平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

第 54 回　安全対策専門委員会　議事次第

Ⅰ　日時

平成 29 年 7 月 11 日（火）　15:00～17:00

Ⅱ　場所

FISC 会議室

Ⅲ　議事次第

１．	15:00	開会
		理事長挨拶
		次第説明
２．	15:15	【議案１】改訂原案（前説）に関する検討
		・各委員からのご意見反映について（FISC 事務局）
３．	16:15	【議案２】基礎基準に関する検討
		・基礎基準の選定にあたっての考え方について（FISC 事務局）
４．	16:55	事務連絡
５．	17:00	閉会

Ⅳ　資料

【資料１－１】	改訂原案（前説）に対する各委員からのご意見（対応方針）
【資料１－２】	改訂原案（安全対策基準前説）
【資料２－１】	基礎基準に関する検討について
【資料２－２】	基準本文の記述様式（例）
【資料２－３】	基準一覧（基礎基準案）
【資料３－１】	検討事項に関するご意見（メール回答用）
【参考資料】	基準本文（統制・実務・監査）

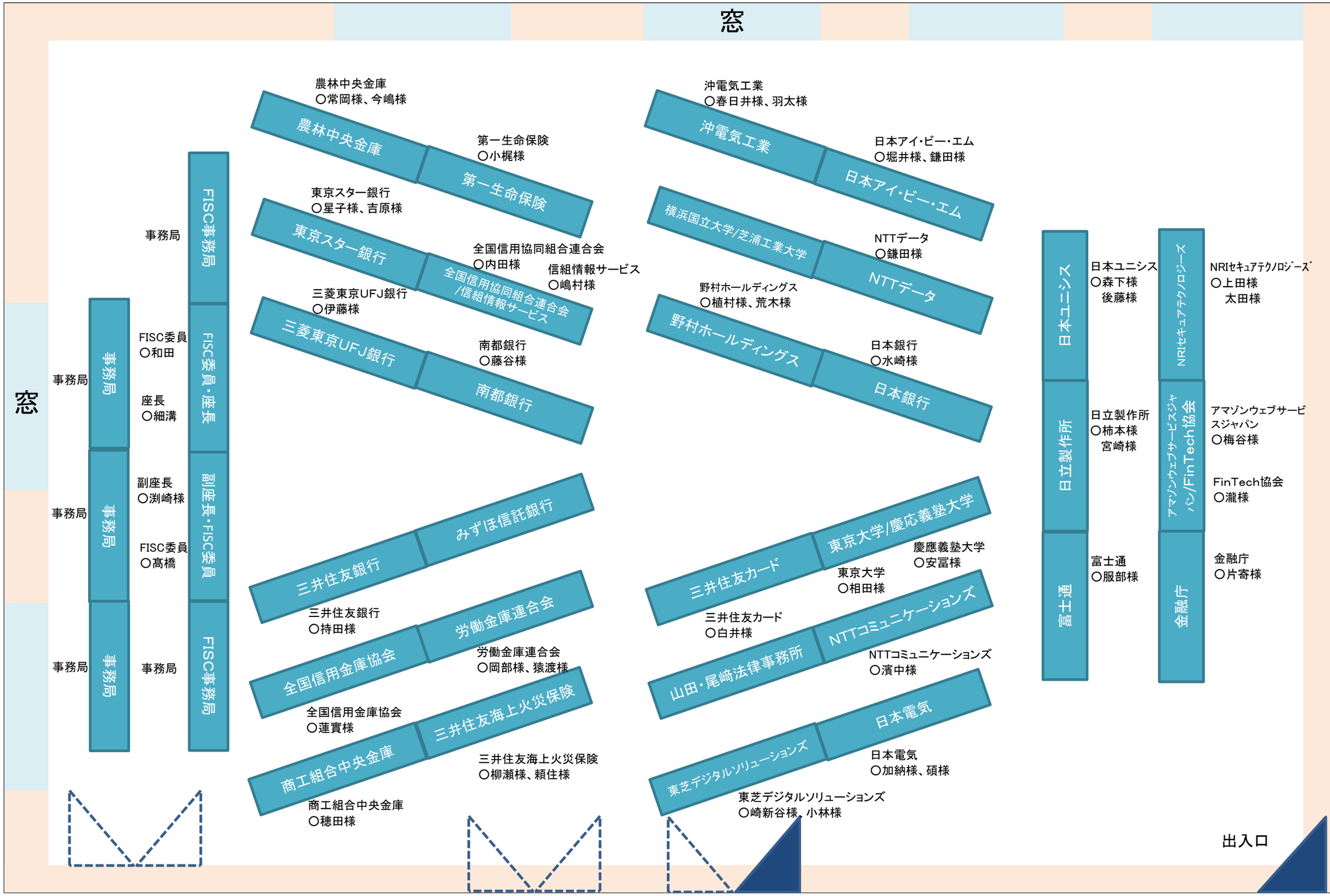
Ⅴ　今後の予定

○第 55 回　安全対策専門委員会
（予定）平成 29 年 8 月 8 日（火）15:00～17:00　FISC 会議室

以上

第54回「安全対策専門委員会」座席表

平成29年7月11日



【資料1－1】
平成29年7月11日
公益財団法人　金融情報システムセンター

■改訂原案（前説）に対する各委員からのご意見（対応方針）

	No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
★	3	p0	（全般）	システムリスクの評価についてはこれまで各金融機関が個別に評価してきたものであるが、各金融機関が改めて「リスクベースアプローチの考え方」に基づくシステムリスクの評価を行うには相応の時間を要することが予想される。ついては、新しい安全対策基準の公表・発刊にあたっては、全金融機関が「リスクベースアプローチの考え方」を「一律的に、一斉に適用する」等の表現は避けていただきたい。	南都銀行 山田様(専) 藤谷様（検）	外部委託に関する有識者検討会の報告書でも述べられているように、リスクベースアプローチの考え方を導入するにあたっては、一律的、一斉に適用することは想定していません（激変緩和措置の必要性が述べられています）。例えば、システム更新の際に、順次適用していくことを想定しています。従って、新しい安全対策基準の記述においても、また対外公表に当たっても、その点を留意しながら作業を進めていくことを考えております。	要	未
★	24	p1	Ⅰ概説 1．安全対策基準の意義	「あるべき姿」について、これは会員が実施することを強制する意味合いなのか。だとすると、安対基準は規制の程度が強くなると思われるが、その理解でよいか。その上で、以下のように修正いただきたい。 【そこで、『金融機関等コンピュータシステムの安全対策基準・解説書』（以下、「本書」とする）では、金融機関等のよりどころとなる安全対策基準の適用において、リスクベースアプローチを取り入れた考え方を示すこととした。ただし、その考え方については、全金融機関への一律の適用を求める物ではない。	全国信用金庫協会 蓮實様(検)	安対基準は「自主基準」として策定され、金融機関等の安全対策の拠り所として活用されてきました。ご指摘頂いた点は、自主基準に選択と適用の幅を持たせることを確保したいとの趣旨と理解いたしました。従って、他の委員から提示（No25）された「現実的かつ効果的な安全対策の考え方を示すこととした」という表現が、現在の安全対策基準についての考え方の記載とも通じるものがあると考えられますので、この表現に修正いたしました。	要	済
	25	p1	Ⅰ概説 1．安全対策基準の意義	安対基準が金融機関等の安全対策を考えるうえでの拠り所となっている現状と、各金融機関では既にリスク管理対象やリスク度合いに応じて、安対基準をアレンジして利用している実態を踏まえると、ここで「あるべき姿」と表現するのではなく、「現実的かつ効果的な安全対策の考え方」とした方が相応しいのではないか。	三井住友銀行 持田様(専)	No24参照	要	済
★	19	p0	（全般）	【必要十分】という言葉が複数個所で用いられているが、「必要」は例えば、最低限の基準としてこれまでの安対基準でも使われてきた概念である。対して、「十分」については、その判断に明確の基準はなく、振れ幅が大きくなることが想定される。これは、今後も「ここまでやれば十分」と基準が示せるものではなく、また、何かの事象が発生し、結果を見た上で金融機関の意思決定が「十分」ではなかったと評価されるなど、結局は、結果が全てとなるのではないか。	全国信用金庫協会 蓮實様(検)	「必要十分」という表現は、p6で記載されているように、形式的に安全性に偏った安全対策を行ってしまうこと（=リスクゼロを追及するがために過剰な安全対策を行ってしまうこと）のないように安全対策を行うことを指し示す表現として使われています。そうした意図にも関わらず、「必要十分」といった表現が、「リスクゼロとなるのに十分な」と誤解される可能性が高いのであれば、他の適切な表現に変更することが考えられます（例えば、「適切な」や「過不足なく」といった表現が考えられます）。	要	済
	73 （追加）	p6	Ⅰ概説 2．安全対策の考え方 (2)リスクベースアプローチ ①安全対策基準を取り巻く環境の変化 ②リスクベースアプローチの意義	「どこまで対策を講じるかは、リスクや経営資源等を踏まえて各社の経営がしっかり判断すべき」つまり「どこまでやれば十分かは各社で異なる」と理解してます。 一方「必要十分」との記述が、「必要十分な対策（リスクゼロの対策）というものが一意に定められる」とも読めます。 （2）①「‥必要十分ではない安全‥」の「必要十分」は削除した方がよいかと思います。 （2）②リスクベース‥‥、の文中に「十分」という語を書き、「十分」とは各社それぞれのリスクに応じた水準であるということがわかるようにしていただけたらと思います。	東京海上日動火災保険 佐々木様(検)	No19参照	要	済

No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
39	p7	Ⅰ概説 2. 安全対策の考え方 (3)安全対策における基本原則	質問・基本原則の4つ目の項目に【〇上記原則が遵守されたうえで、妥当な意思決定等が行われ、適切に運営されている限りにおいては、安全対策は独自決定することが可能である。】とあるが、 原則に当てはまらない場合には、だれが安全対策を決めるのか？	全国信用金庫協会 蓮實様(検)	金融機関は、従来より安全対策基準に基づき、各々が独自に判断して安全対策を決定・実施してきました。ご指摘の文章は、金融機関の自主的な判断により、リスクの特性に合った安全対策を決定できることを強調した文章ですが、その趣旨が誤解される可能性があるのであれば、〇の4つ目を一番上に配置し直した上で、No19,23も踏まえて、以下のように修正いたしました。	要	済
★					〇情報システムに対する安全対策は、以下の考え方に基づき、適切な意思決定が行われ、運営されるべきである。 〇情報システムに対する安全対策の達成目標は、個々の情報システムのリスク特性に応じて、適切な内容で決定されるべきである。 〇情報システムに対する安全対策への経営資源配分は、リスク顕在化後の事後対策と比較衡量したうえで、情報システムに係る予算内における新規開発等との調整のみならず、経営資源全体も視野に入れ、顧客の利便性向上や企業価値の最大化を目指して、決定されるべきである。 〇ただし、重大な外部性を有する情報システム及び機微性を有する情報システムにおいては、その社会的・公共的な観点から、このシステムの外部性や保有情報の機微性を考慮に入れた安全対策の達成目標が設定されなければならない。		
38	p7	Ⅰ概説 2. 安全対策の考え方 (3)安全対策における基本原則	「金融機関等の情報システムの安全対策における基本原則」の次行より表記されている内容について、保有する情報システムだけでなく、クラウド形式などの利用による情報システムに対する統制についても、必要に応じて求めることが望まれることから、以下の表現にしてはどうか。 「基本原則は、金融機関等が利用する情報システムの安全対策について、ITガバナンスが適切に発揮されている限りにおいて、リスクベースアプローチの考え方に基づき、必要十分な内容で、みずから決定することを可能としている。」	日本ユニシス 後藤様(検)	ご指摘およびNO39を踏まえ、以下のとおり修正いたしました。 「基本原則では、金融機関等は、ITガバナンスを適切に発揮し、リスクベースアプローチの考え方に基づき、保有する情報システムに対する適切な安全対策を、みずからが決定することができるとしている。」	要	済
69	p8	Ⅰ概説 2. 安全対策の考え方 (3)安全対策における基本原則 (参考)「外部性」の考え方	基本原則中の「重大な」の範囲を分かりやすくできないか。外部性を持つシステムはいくつも考えられるため、「重大」の境界線によって安全対策の考え方が変わるとした場合、その境界線に対する明確な根拠、例示を示して欲しい。	東京スター銀行 星子様(専)	「重大な外部性」について限定列挙に読めるような表現にすると、選択の幅が狭まってしまう可能性があります。 そこで、「重大な外部性」の例として、「他の金融機関や、他の金融機関の顧客に対し広く影響を及ぼし、社会全体に経済的損失を与える可能性のある為替・預金を取り扱うシステム」を取り上げたうえで、「ATMやインターネットバンキング等が、これらと同質のリスクを有する場合もあり」とし、「重大な外部性を持つシステム」を特定する際に選択の幅を持たせる表現としました。	要	済
★							
9	p8	Ⅰ概説 2. 安全対策の考え方 (3)安全対策における基本原則 (参考)「外部性」の考え方	【例えば、決済システムは個別金融機関等で深刻なシステム障害が発生した場合、他金融機関等への信用不安に発展し、経済的損失が拡大する可能性のある性質を有する。】 とあるが、金融機関が破綻した場合などなら適切な例かもしれないが、システム障害から他金融機関の信用不安は例として無理があるのではないか。 また、4つ目の【また～可能性もある。】も極端すぎて例として不適切ではないか。 全体として外部性の定義が良くわからない。	全国信用金庫協会 蓮實様(検)	ご指摘およびNo69を踏まえ、表現を修正しました。	要	済
★							
74 (追加)	p8	Ⅰ概説 2. 安全対策の考え方 (3)安全対策における基本原則 (参考)「外部性」の考え方	「外部性を有する」「外部の統制」「外部のシステム」のそれぞれの指す「外部」が別の意味であるので、やや分かりにくい（読み手が間違える）と感じました。また、「重大な外部性を有するシステム」について、ここで想定している対象システムよりも広く対象であると誤解されないよう、表現を工夫（何等か補注するなど）いただいた方がよいかと思います。	東京海上日動火災保険 佐々木様(検)	「外部の統制」については、「外部（委託先等の他組織）の統制」と表現を変更。「外部のシステム」は、この文言がなくても文章の意味が通じるので削除。2つの「外部」について、変更・削除することで、「外部性を有する」と区別ができるように修正いたしました。 なお、「重大な外部性」についての表現方法の工夫についてはNo69を参照してください。	要	済

	No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
★	8	p7 p14	Ⅰ概説 2. 安全対策の考え方 (3)安全対策における基本原則 Ⅱフレームワーク 1. 総論 (2)基準の分類	7頁において、重大な外部性がある場合、機微情報の場合を「高い安全対策」が必要な場合としつつも、14頁においては、特定システムでない通常システムにおける機微情報の扱いについて注釈で可用性について安全対策を一部適用しない場合について規定しております。7頁の言い回しについては、基準改訂の大きなテーマの一つにはなると考えておりますが、機微情報と重要な外部性がある場合とを一つにまとめて「高い安全対策が必要」として留保しないことが整理として適切かご検討ください。	FinTech協会 瀧様(専)	ご指摘を踏まえ、P14「(2)基準の分類」をわかりやすく修正いたしました。	要	済
★	70	p14 P20	Ⅱフレームワーク 1. 総論 (2)基準の分類(図8) (4)安全対策基準の適用方法(図11)	特定システムに関わる付加基準の選択が「全て適用」となっており、誤解を生じさせやすい内容となっている。 今回の改訂では、「情報の外部性」と「情報の機微性」に着目し、リスクベースアプローチの考え方に基づいて安全対策基準を考えよう、というものであると認識しているが、「情報の外部性」と「情報の機微性」では求められる安全対策は異なることが通常であるから、「付加基準の分割」を検討してもよいのではないか。	東京スター銀行 星子様(専)	No8参照(「全て適用」は修正しました) なお、「重大な外部性」と「機微性」の特徴は異なるものの、金融機関等における特定システムの重要性を鑑みた場合、安全対策をこれらの特徴により明確に2分して提示することは難しいのではないか考えております。	要	済
★	47	p14 p20	Ⅱフレームワーク 1. 総論 (2)基準の分類(図8) (4)安全対策基準の適用方法(図11)	「全て適用」という表現を用いると、「原則として」の意味合いが排除されてしまう。このため、図8においては言葉ではなく、「〇」「△」等の表記とし、注釈にて 「〇:リスク特性に応じて原則適用」 「△:リスク特性に応じて選択適用」 のようにしてはどうか。併せて本文中も「最低限原則適用する基準」等に表現を見直してはどうか。	三井住友銀行 持田様(専)	No8参照 「原則として適用」として表現を統一しました。	要	済
★	56	p20	Ⅱフレームワーク 1. 総論 (4)安全対策基準の適法方法 ③リスク特性の評価・基準の選択	図8と平仄をとるため、以下のように修正してはいかがか。 ・「特定システムにおいては～全ての対策を選択実施する」として注釈17で一部省略も可とする ・「ただし、～原則として選択不可とする」の記述は注釈17で、リスク特性に応じて選択も可とする	三井住友銀行 持田様(専)	No8参照 また、④安全対策の目標設定の本文中に左記を参考に説明文を追加しました。	要	済
★	71	p16	Ⅱフレームワーク 1. 総論 (2)基準の分類 (補足2)外部の統制における・・	「可能である」という表現の使い方に何通りもあるように読めるため、全体として意味が理解しにくい。表現上の問題だけでなく、必要最低限の考え方も混入しているため、整理して分かりやすくした方がよい。	全国信用金庫協会 蓮實様(検)	ご指摘の通り、「可能である」には、必要最低限と位置付けられるものが混在しているため、全体として意味が分かりづらくなっています。「可能である」という表現は、主に「クラウドサービス利用」の基準において使用されていますが、当該基準は、8月8日専門委員会のテーマである「外部委託管理基準の検討」において審議していただく予定ですので、それまでに対応方針を整理したいと考えております。	要	未
	54	p18	Ⅱフレームワーク 1. 総論 (4)安全対策決定のプロセス	「対象システムの特定」を行う段階自体、リスクベースアプローチの一部にあたる。 すなわち、対象システムの特定を行うにあたって、一定の評価基準でシステムリスク評価を行うのであるから、これをリスクベースアプローチから外すことは不適切である。また、「リスク特定の評価」も「対象システムの特定」をカバーの範囲とすることになる。	日本銀行 水崎様(検)	ご指摘を踏まえ、「対象システムの特定」についても、リスクベースアプローチに含まれるように修正しました。	要	済
★	55	p18	Ⅱフレームワーク 1. 総論 (4)安全対策決定のプロセス	現行の安全対策基準をみると、基準の解説部分に、具体的な対策として最低限のものから高い水準のものやベストプラクティスが含まれている。この場合、基礎基準となる部分と選択的に適用される部分とを区分することが必要となる。	事務局	基準と一体となって利用されている解説部分については、No8で述べたような各種の記述が混在していますので、各論において、基礎基準とその解説に当たる部分、付加基準に当たる部分、ベストプラクティスに当たる部分等を明確に区分したいと考えております。	要	未

	No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
★	57	p18	Ⅱフレームワーク 1．総論 ⑷安全対策決定のプロセス ③安全対策の目標設定 ④安全対策の決定	安全対策の選択と安全対策の設定との違いがわかりにくい。また、安全対策の目標の設定は、基準の選択、安全対策の選択と同時に決定されるものではないか。	事務局	「安全対策の適用方法」を「安全対策決定のプロセス」に改め、以下の工程に整理しました。さらに、各工程の内容を見直したうえ、原案を修正しました。 ⑷安全対策決定のプロセス ①リスク特性の洗い出し ②対象システムの特定 ③安全対策の目標設定（基準の選択・安全対策の選択） ④安全対策の決定 ⑤コンティンジェンシープランの策定	要	済
★	68	p1	Ⅰ概説 1．安全対策基準の意義	「決済代行業者等」という言葉を利用することとなった経緯は判ったが、この「決済代行業者等」に含まれる業者の事業内容には幅が有りすぎる。例えば、「決済代行」のように金融機関側システムに対し更新を指示するケースもあれば、単に金融機関側システムから情報を参照するケースもある（更に、参照する情報にも機密性について幅がある）。 こうした中、（補足3）において、「決済代行業者等」に対し、何が「一部」なのかはっきりしないため、その後「基礎的基準を満たすことが期待される」とした場合、情報を参照するケース（例えば、為替相場照会、店舗・ATM所在地照会、金利、手数料紹介、店頭混雑状況照会など）などにおいて、過度の対策を求めることになる可能性がある。	日本銀行 水崎様(検)	まず、言葉の使い方について、FinTechに関する有識者検討会において、「FinTech企業」という用語を用いましたが、法整備等の進む中、FinTech企業という言葉が今後も継続的に使用されない可能性があるとの指摘を受けて、「決済代行業者等」という用語を用いました。「決済代行業等」が、一部の特定業務のみをイメージさせるのであれば、「FinTech企業」との表現に戻すか、他の適切な表現を考案することも考えられますので、委員の皆様のご意見をお聞きしたいと考えます。また、補足3の記述について、ご指摘の通り、決済代行業者等のサービス内容は多岐にわたっているにもかかわらず、一律に基礎的基準を踏まえた安全対策を実施するとの誤解を招く惧れがあります。そこで、FinTechに関する有識者検討会報告書の記述を踏まえて「決済代行業者等が金融関連サービスを提供するシステムの安全対策を策定する場合には、安全対策基準の基礎基準などを踏まえたうえで適切な安全対策が実施されることが期待される」といった表現に変更しました。また、この記述については、基礎基準の具体的な検討やオープンAPIチェックリストの策定等を勘案しながら、再度検討することとしたいと考えています。	要	済
★	21	p0	（全般）	・金融サービスと金融関連サービス ・外部委託先と決済代行業者等 今回の改訂を機に新たなプレーヤーが基準を参照していく中で、上記の違いが明瞭な表現となることが必要と考えています。例えばAPIを活用する事業者は外部委託事業者ではないため、過度な統制を回避するためにも、個別の定義の記載を修正していく必要を感じております。	FinTech協会 瀧様(専)	「金融関連サービス」はFinTech企業等が提供する金融に関連するサービスであることを明確化するために、脚注（p1）に説明を加えました。また、本文中、金融サービスおよび金融関連サービスの語句については、実施主体を意識して必要な修正を加えています。 さらに、決済代行業者は、「FinTech企業」という名称に暫定的に戻していますが、外部委託先＝FinTech企業とはならないケース（API連携など）を考慮し、関連する箇所に修正・補記を行っております。 今後の議論を踏まえ、よりわかりやすい定義としていきます。	要	済
★	1	p11	Ⅰ概説 2．安全対策の考え方 ⑹安全対策基準における「統制」のあり方 ②外部に対する「統制」のあり方	「外部に対する統制」について、既存の外部委託先とは異なる形での外部連携先（例えばAPI連携先）が出てきております。外部委託とそれに含まれない外部連携先があることについて、より明確な記載をお願いいたします。 （修正文例） 金融機関等においては、【外部委託→外部委託先あるいはAPIによる接続先等】やサービスの利用が拡大 また外部委託先とは異なる形での外部連携先（例えばAPI連携先）は、一般論としては、外部委託先ほどの管理が求められない場合があることを意識した記載にして頂ければと思います。	FinTech協会 瀧様(専)	ご指摘を踏まえ、以下の内容に修正いたしました。 なお、FinTech企業との契約形態には、外部委託とは性質の異なるものが存在する 。金融機関等は、当該サービスを提供するシステムが、安全対策基準の適用範囲であるかを考慮のうえ、適切な水準で外部の統制を行うことが必要となる。 （脚注） FinTech企業が金融関連サービスを提供するシステムを運用し、金融機関等との接続を行う場合、運用主体であるFinTech企業と、接続される金融機関との間には外部委託とは異なる性質の契約関係が存在する。金融機関等は、FinTech企業に対して外部委託先に対する統制をそのまま適用できない場合を考慮する必要がある。	要	済

	No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
★	61	P22	Ⅱフレームワーク 2．統制 (2)外部の統制	決済代行業者がいわゆる外部委託先と同じように書かれていますため、外部委託に関する概念は説明ないし整理が必要と思われます。外部委託ではないAPI連携等の場合の統制の考え方も内部、外部と並べて（しない場合ならその旨も明らかに）記載すべきと考えます。	FinTech協会 瀧様(専)	ご指摘を踏まえ、外部委託の関係にあるか否かを明示的に示すことで、サービス内容が多岐にわたるFinTech企業と金融機関等との関係を分かりやすく表記することが適切であると考えました。2者間・3者間構成を表した模式図を修正し、外部委託関係の有無を表記したいと考えております。	要	未
★	5	p0	（全般）	今般、API接続事業者のチェックリストの策定が行われましたが、これらに対応したプレーヤーが、安全対策基準によって別のスタンダードでの対応を迫られるケースを回避することは必須であり、そのための配慮を今後の検討の中でも行っていくべきと考えております。	FinTech協会 瀧様(専)	APIチェックリストは安対基準（基礎基準）を踏まえながら、チェックリストの試行結果等も勘案して、今後完成バージョンを策定する予定となっています。その検討の中で、ダブルスタンダードにならない配慮を行っていくものと考えております。	否	現時点では前説へ反映しない考えです。
★	16	p17	Ⅱフレームワーク 1．総論 (3)安全対策基準の適用対象	一例として、API接続事業者がFISCのチェックリストを満たした場合には、別途安全対策基準についての対策を検討する必要がない状態を担保することが重要と考えています。そのためにも、APIチェックリストを超えないように基礎基準が策定されることを明記して頂ければと考えます。	FinTech協会 瀧様(専)	No5参照	否	現時点では前説へ反映しない考えです。
★	51	p16	Ⅱフレームワーク 1．総論 (2)基準の分類 (補足3)決済代行業者等における・・	（補足3）決済代行会社等の文末で、「基礎基準を満たすことが期待される」とありますが、この「期待される」＝それ以下でも良いという表現になりますでしょうか。文言上は、例えばAPIのチェックリストとは関係なく基礎基準を適用とも取ることができます。また、この基準は26頁の最後にある「準用」とは異なるのでしょうか Fintech企業は「金融機関等が提供するサービスと同等」の対策が常に求められる訳では無く、より柔軟な安全対策が許容されると思いますので、この点は「期待」ほどに現実が追いつかない場合もありえることを前提として、表現にご反映頂きたいと思います。	FinTech協会 瀧様(専)	ご指摘を踏まえ、当該箇所を「(3)安全対策基準の適用対象」に移動したうえで、以下の内容に修正いたしました。 金融機関等以外の事業者が金融機関等の外部委託先として金融関連サービスを提供する場合、金融機関等による外部の統制を受けることとなり、当該金融関連サービスを提供する情報システムは、結果として安全対策基準の適用対象となる。 一方で、金融機関等以外の事業者が、金融機関等の外部委託先とはならず、主導的に金融関連サービスを提供する場合、金融機関等による外部の統制が及ばないか、又は部分的となることが考えられる。金融機関等による外部の統制が及ばない場合は、当該金融関連サービスを提供する情報システムは、安全対策基準の適用外となる。また、金融機関等における外部の統制が部分的となる場合、当該金融関連サービスを提供する情報システムは、金融機関等に責務が生じる範囲において、結果として安全対策基準が部分的に適用 されることとなる。	要	済
	4	p0	（全般）	基準の構成や分類、適用に関する記載は、実際の基準が示されていない中で、判断ができない。	全国信用金庫協会 蓮實様(検)	今後、基準内容の各論について整理を行った後、必要に応じて、基準の構成や分類、適用に関する記載部分を見直していく予定です。	要	未
	20	p0	（全般）	個々の考え方や内容は理解できるが、実際の安全対策基準利用での全体感（どの様に具体的に適用されるや図7、図8、図11、図12の関連性が判る等）が整理された図や一覧等があると良いが。	野村ホールディングス 荒木様(検)	ご指摘の点について、検討を行いたいと考えております。	要	未
	22	p1	Ⅰ概説 1．安全対策基準の意義	「一方で、金融機関等が、企業価値を高めるために」について、金融機関側からの視点だけではなく、利用者視点から「顧客の利便性を向上させるため」について述べた方がよいのではないか。	全国信用金庫協会 蓮實様(検)	ご指摘を踏まえ、No23のように修正いたしました。	要	済
	23	p1	Ⅰ概説 1．安全対策基準の意義	顧客の視点を入れて、「この中で」以降を以下のように修正してはいかがか。 「したがって、金融機関等は、顧客利便性と企業価値の向上を目的に、新規開発等に適切に資源配分していくことは重要であるが、一方で、金融機関等は、信用秩序を維持し、利用者が安心してサービスを享受するために、ITガバナンスを発揮し、安全対策に対する資源配分を経営資源全体の中で適切に調整していくことが不可欠である。」	三井住友銀行 持田様(専)	No22のご指摘とも共通している点もありますが、強調したい部分が「限りある経営資源を新規開発に適切に配分していく」であることから、以下のとおり修正いたしました。 元文 「こうした中、金融機関等が信用秩序を維持し、利用者が安心してサービスを享受するためには、十分な安全対策の実施が不可欠であるが、一方で、金融機関等が、企業価値を高めるために、限りある経営資源を、安全対策のみならず、新規開発等にも適切に配分していくことが重要となってくる。」 修正文 「こうした中、金融機関等が信用秩序を維持し、利用者が安心してサービスを享受するためには、十分な安全対策の実施が不可欠であるが、一方で、金融機関等が顧客の利便性や企業価値を高めるために、限りある経営資源を、安全対策のみならず、新規開発等にも適切に配分していくことが重要となってくる。」	要	済

No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
6	p1	Ⅰ概説 1. 安全対策基準の意義	「学識経験者、金融機関、保険会社、証券会社、、、」において、保険会社や証券会社は一般的には金融機関に含まれると思われるが、見直すべきか検討頂きたい。	三井住友銀行 持田様(専)	ここに記載されている「金融機関」は、預金取扱い金融機関を指しています（狭義の定義）。そのうえで、保険会社、証券会社、クレジット会社等を含め「金融機関等」としています。記載箇所は、「金融機関」のみならず、保険会社、証券会社、クレジット会社や、コンピュータメーカー等が改訂に参加していることを明示的に示したいと考えたため、こうした表現としております。 一方で、その下にある「金融、保険、証券、、、当金融業務を提供する」となっている部分については、文章の冗長感を避けるため、「金融業務を営む業界の各社」との表現に見直しました。	要	済
26	p1	Ⅰ概説 1. 安全対策基準の意義	「非金融機関等」は「金融機関等」の対義語で使用しているのか？「等」の示す部分など、指示している範囲が曖昧であると感じる。（他数箇所あり）	全国信用金庫協会 蓮實様(検)	「金融機関等」の対義語としてご指摘通り、一旦「金融機関等以外の事業者」と修正いたしました。ただし、「金融機関等以外の事業者」の定義が曖昧なため、今後、各論の検討結果等を踏まえて、用語の整理を行っていくことといたします。	要	暫定的に修正しています。
7	p2	Ⅰ概説 2. 安全対策の考え方 安全対策基準改訂の考え方	本改訂における大方針の一つである「リスクベースアプローチ」の導入に際し、リスクベースアプローチの一般的な定義・効用、次期安対への導入目的について前説で分かり易い補記が欲しい。 P2にて経緯（外部委託に関する有識者検討会の提言）、またP6でリスクベースアプローチの意義について触れられているが、散在して記載されており読み易さ・理解し易さの観点で再考いただきたい。	NTTデータ 鎌田様 (専)、鈴木様（検）	ご指摘を踏まえ、(p6)「(2)②リスクベースアプローチの意義」に、リスクベースアプローチの考え方を示すよう、以下のように修正いたしました。 リスクベースアプローチとは、金融機関等の安全対策の決定にあたり、リスク特性を分析した結果を、安全対策の優先順位等の合理的な意思決定に活用するとともに、金融機関等の経営資源が有限である点を踏まえ、安全対策に対する資源配分を経営資源全体の中で調整する<u>考え方を言う。</u>	要	済
27	p2	Ⅰ概説 2. 安全対策の考え方 安全対策基準改訂の考え方	L6「決済代行業等と連携した金融関連サービス」について、文中の主語が「金融機関等の情報システム」であり、文脈的に主従が一致していない。	全国信用金庫協会 蓮實様(検)	ご指摘を踏まえ、修正いたしました。	要	済
29	p2	Ⅰ概説 2. 安全対策の考え方 安全対策基準改訂の考え方	L12「サービス利用等において、外部委託への依存度が」について、サービスの利用はそもそも外部委託なので、この文脈では意味がおかしい。	全国信用金庫協会 蓮實様(検)	ご指摘を踏まえ、修正いたしました。	要	済
30	p3	Ⅰ概説 2. 安全対策の考え方 (1)ITガバナンスとITマネジメント ①安全対策上必要となるITガバナンスの意義	今回は安全対策に関してなので必須ではないが、以前より中長期計画やシステム戦略方針策定においては「経営戦略やビジネス戦略との整合性」がより重要になってきているので、その記載もあってもいいかもしれない。	野村ホールディングス 荒木様(検)	ご指摘を踏まえ、修正いたしました。	要	済
31	p4	Ⅰ概説 2. 安全対策の考え方 (1)ITガバナンスとITマネジメント ①安全対策上必要となるITガバナンスの意義	経営層は、業務執行とモニタニング体制の整備方針の決定を担っているが、経営層を含む担い手は分離・独立しているものと思われるので、次のとおり別々の章としたらよいのではないか。 b. ⅰ 安全対策に携わる業務執行 ⅱ モニタリング体制の整備方針の決定	南都銀行 山田様(専) 藤谷様（検）	ご指摘を踏まえ、それぞれが分離独立していることを考慮し、左記を参考に修正いたしました。	要	済
32	p5	Ⅰ概説 2. 安全対策の考え方 (1)ITガバナンスとITマネジメント ②安全対策上必要となるITマネジメント	PDCAサイクルを意識して書かれたものと考えるが、列挙されている「・内部規程・組織体制等の整備」と「・内部規程・組織体制等の見直し」の違いは小さく、まとめて記載してもよいのではないか。	東京スター銀行 星子様(専)	ご指摘を踏まえ、以下のとおり修正いたしました。 ・内部規程・組織体制等の整備・見直し ・個々の情報システムに対する安全対策の決定 ・安全対策上必要となる情報の経営層への報告	要	済
33	p5	Ⅰ概説 2. 安全対策の考え方 (1)ITガバナンスとITマネジメント ②安全対策上必要となるITマネジメント	管理者の役割についての箇条書き部分は以下の様に修正していただきたい。 ・内部規程・組織体制等の整備、見直し ・個々の情報システムに対する安全対策の決定 ・ITガバナンス上必要となる情報の経営層への報告	全国信用金庫協会 蓮實様(検)	ご指摘の通り、修正いたしました。（No32参照）	要	済
34	p5	Ⅰ概説 2. 安全対策の考え方 (1)ITガバナンスとITマネジメント ②安全対策上必要となるITマネジメント	図4について、経営企画担当（部門）の役割の説明と平仄を合わせるため、経営層に向けて「支援」の矢印が必要。	三井住友銀行 持田様(専)	ご指摘の通り、修正いたしました。	要	済

No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
75（追加）	p6	Ⅰ概説 2. 安全対策の考え方 ⑵リスクベースアプローチ	リスクベースアプローチにおいて、各社におけるリスクというものは、時間の経過によって変わることがあると思います。リスク特性の分析を各社が定期的にしっかりやるべきであるということを、どこかに明記いただいた方がよいかと思います。	東京海上日動火災保険 佐々木様(検)	ご指摘を踏まえ、「安全対策決定のプロセス」において、リスク評価の定期的な見直しが必要である旨、記載を追加いたしました。	要	済
35	p6	Ⅰ概説 2. 安全対策の考え方 ⑵リスクベースアプローチ ①安全対策基準を取り巻く環境の変化	意味をより分かりやすくするために、以下の言葉を補足してはどうか。 「大きな比率を占めてきたその他情報システムについては、適用する安全対策の具体的な考え方がしめされないまま」	三井住友銀行 持田様(専)	ご指摘の通り、修正いたしました。	要	済
28	p2	Ⅰ概説 2. 安全対策の考え方 安全対策基準改訂の考え方	L11現時点の安全対策基準は、基幹業務系以外のシステムに対する基準適用に関して、演繹的及び帰納的な考え方に基づき、適用を求めていると理解している。 しかし、昨今の多様性に対して、「現在の安全対策基準の想定している適用要件、背景が、追従しきれない情況とならないように改善していく事が求められている」と理解している。 このことから、以下の表現にしてはどうか。 「多様化する基幹業務系以外のシステムにおいては、その適用基準に想定されていた適用要件、背景の不一致などにより、」	日本ユニシス 後藤様(検)	他の同様のご意見も参考に、当該文章を「多様化する基幹業務系以外のシステムにおいては、適用の考え方が具体的に示されず」と修正いたしました。	要	済
36	p6	Ⅰ概説 2. 安全対策の考え方 ⑵リスクベースアプローチ ②リスクベースアプローチの意義	L11「企業価値の最大化」について、前説中に数回登場してくるため、価値の多様性について同様の認識がなされるよう、他の箇所も含め、本文中の表現を見直せないか。	全国信用金庫協会 蓮實様(検)	「企業価値の最大化」については、原則として「顧客の利便性向上」と並列して記載するように見直しており、それとP1の脚注を合わせて読めば、価値の多様性は十分に認識されるものと考えております。	否	－
37	p7	Ⅰ概説 2. 安全対策の考え方 ⑶安全対策における基本原則	L6「プライバシーなど個人の人権を侵害する場合」について、人権等を侵害する以外の影響も考えられるが、表現されていないと感じる。また、「侵害する」ではなく「侵害される」が正しいのでは？	全国信用金庫協会 蓮實様(検)	プライバシー以外、例えば漏えい等により不当な差別が発生する場合があり得るため、「人権等」として表現させて頂きました。この部分は原案とおりとさせて頂きたいと考えます。 また、「侵害する」ではなく、「人権等が侵害される」が正しいため、ご指摘の通り修正いたしました。	要	済
40	p8	Ⅰ概説 2. 安全対策の考え方 ⑶安全対策における基本原則 (参考)「情報の機微性」の考え方	L9「「重大な外部性を有する」システムと同様に」について、「同様」の指すものが曖昧である。同様の対策なのか？同様のレベルの安全対策なのか？を明確にした方がよい。	東京スター銀行 星子様(専)	ご指摘を踏まえ、「同様」の指す内容が明確になるよう、本文を修正いたしました。	要	済
41	p8	Ⅰ概説 2. 安全対策の考え方 ⑶安全対策における基本原則 (参考)「情報の機微性」の考え方	L11「これらが同一に扱われてしまった場合」について、「これら」の指す内容が曖昧であるため、表現の見直しをした方がよい。	東京スター銀行 星子様(専)	ご指摘を踏まえ、「これら」の指す内容が明確になるよう、本文を修正いたしました。	要	済
42	p9	Ⅰ概説 2. 安全対策の考え方 ⑷基本原則に従ったITガバナンス	「新規投資等を含むその効率の最大化」について、「その」を具体的に示した方が分かりやすいのでは。	三井住友銀行 持田様(専)	ご指摘を踏まえ、「投資効率の最大化」と修正いたしました。	要	済
10	p9	Ⅰ概説 2. 安全対策の考え方 ⑸安全対策における経営責任のあり方	L3「安全対策の基本原則の遵守に当たって」について、「現在の認識は、過去からの積み上げで求められている基本要件と認識、この要件を認識した後、今回検討している基本原則に対する危惧の関係を示す」事が分かりやすく表現されるべきと考える。このため、表現をより平易にすべく、以下のようにしてはどうか。 「ひとたび重大なシステム障害が発生した場合、その事実をもって、結果責任を追及されかねない立場にあることから、高い安全対策を求めない訳にはいかない」といった共通認識が存在する。この認識から生まれる危機感が、安全対策の基本原則に示される「リスクベースアプローチに基づき安全対策を決定」の考え方に対する阻害要因とならぬようにすることが、重要と認識する。」	日本ユニシス 後藤様(検)	ご提案頂いた「危機感」も含め、「共通認識」という文言によりマイルドに表現しています。	否	原案のとおりとさせて頂きたいと考えております。

No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
43	p10	Ⅰ概説 2. 安全対策の考え方 (6)安全対策基準における「統制」のあり方 ①「統制」と「実務」の区分	今回の検討においては、過去を踏襲する事を否定していないが、その前提は、既存の考え方に縛られない、より的確な対応を基本とすること理解していることから、以下の表現としてはどうか。 「経営層が、既存の考え方に縛られることなく」	日本ユニシス 後藤様(検)	ご指摘を踏まえ、修正いたしました。	要	済
45	p11	Ⅰ概説 2. 安全対策の考え方 (6)安全対策基準における「統制」のあり方 ①「統制」と「実務」の区分	図6「実務」の説明を以下のように修正してはいかがか。 「管理者がリスク管理対象やリスク度合いに応じて」	三井住友銀行 持田様(専)	ご指摘を踏まえ、「管理者がリスクの管理対象やリスクの程度に応じて 」と修正いたしました。	要	済
44	p11	Ⅰ概説 2. 安全対策の考え方 (6)安全対策基準における「統制」のあり方 ①「統制」と「実務」の区分	図6「外部の統制」の内容説明について「外部への統制を具体化した施策」が判り難い。 P12に記載の「外部へ委託する上で必要となる統制」等が表現が良い。	野村ホールディングス 荒木様(検)	ご指摘を踏まえ、修正いたしました。	要	済
2	p11	Ⅰ概説 2. 安全対策の考え方 (6)安全対策基準における「統制」のあり方 ②外部に対する「統制」のあり方	外部に対する統制の特徴について記載されている箇所について、リーガルエンティティとして別個となる委託先に対する統制という側面を具体的に表現してはどうか。 「内部（自組織）に対する統制に比して、外部（委託先などの他組織）に対して、内部に求める統制と同等の期待、要求は、一般的に及びにくくなる傾向にある。さらに、外部が再委託を行う場合は、その再委託先に対して内部が求める「統制」は、さらに及びにくくなる事が考えられる。」	日本ユニシス 後藤様(検)	内部、外部が指すものが理解しやすいよう、左記を参考に修正いたしました。	要	済
76 （追加）	p11	Ⅰ概説 2. 安全対策の考え方 (6)安全対策基準における「統制」のあり方 ②外部に対する「統制」のあり方	外部に対する統制のあり方について、外部センターのシステムと自社センター内部のシステムと、具体的にどの基準について差を設けるかは、今後基準それぞれについて以下の観点でよく検討が必要と感じました。 ・リスクベースで考えると、障害発生時の影響は、外部センターのシステムか自社センターのシステムかによらない。 ・一方で、外部センターに対し、すべてにおいて自社内部と同等の統制を行うことが可能とは限らない。	東京海上日動火災保険 佐々木様(検)	ご指摘の点につきましては、今後「外部委託管理の検討」の中で整理させて頂きたいと考えます。	要	未
46	p12	Ⅱフレームワーク 1. 総論 (1)安全対策基準における定義	「I. 安全対策の考え方」で述べた「基幹業務系システム以外の基準が不明確～」を受け、「1.総論」の後に、過去の課題を解消するために、どのような策を施したか説明を入れた方がよいのではないか。	三井住友銀行 持田様(専)	ご指摘の内容を受け、考え方を具体的に示すものとして、一文を説明として加えました。	要	済
11	p12	Ⅱフレームワーク 1. 総論 (1)安全対策基準における定義 ②特定システム・通常システム	「なお、特定システムの一部を～」について、具体的なシステム例を示した方が分かりやすいのではないか。	三井住友銀行 持田様(専)	例示として、「例えば、システム全体では、顧客情報が保有されているが、当該サブシステム内には顧客情報が保有されていない場合等が考えられる」（FinTech有識者検討会報告書P23脚注34）を脚注として追加しました。	要	済
12	p13	Ⅱフレームワーク 1. 総論 (1)安全対策基準における定義 ③安全対策基準の構成	「統制基準」に人材育成・訓練等に関する対策を含める理由を教えていただきたい。	南都銀行 山田様(専) 藤谷様（検）	システム開発、運用やシステムリスク管理等に従事する人材の確保、育成は、安全対策の水準を維持・向上するにあたり、組織的な取り組みとして実施されるものであり、内部の統制の一要素として位置付けているためです。	否	原案のとおりとさせて頂きたいと考えております。

No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
13	p13 p14	Ⅱフレームワーク 1．総論 (1)安全対策基準における定義 ③安全対策基準の構成	現行の安全対策基準は、「設備基準」→「運用基準」→「技術基準」の順番で並べられている。改訂後の安全対策基準を使いやすいものとするため、「統制基準」→「設備基準」→「実務基準」→「監査基準」の順番で並べてほしい。また、現行の安全対策基準の「運用基準」は保守・運用担当、「技術基準」は開発担当が参照しており、各担当が参照すべき安全対策が一目で分かる構成となっているが、改訂案の「実務基準」は、各担当が参照しにくいものになることが懸念される。こうしたことを踏まえ、「実務基準」を整理する際は、基準が現行の「運用基準」または「技術基準」のいずれに該当するものなのかが分かるような整理をしてほしい。	南都銀行 山田様(専) 藤谷様(検)	金融機関等が共通して利用する統制に据えた構成を考えており、統制を実現する方法としての実務を次に配置しました。監査は全体を監査するという意味から、最後に配置したため、このような構成となっています。各基準には、統制、実務、設備、監査ごとに現在と同様のインデックスを付ける予定です（従って「設１」は「設１」のまま）。なお、今回の改訂では、基準一覧上に旧基準番号を記載し、現在の運用基準もしくは技術基準が、どの実務基準となるか参照できるよう配慮したいと考えております。	否	原案のとおりとさせて頂きたいと考えております。
14	p13 p14	Ⅱフレームワーク 1．総論 (1)安全対策基準における定義 ③安全対策基準の構成	「コンビニATM」および「デビットカード」の安全対策基準について、地銀の中には、「コンビニATM」の安全対策はセブン銀行やイオン銀行などコンビニATM設置行、「デビットカード」の安全対策は日本デビットカード推進協議会が行っているとして、銀行は（「コンビニATM」および「デビットカード」の安全対策を自ら実施するのではなく）コンビニATM設置行や日本デビットカード推進協議会の安全対策を確認する態勢を整備するものと考えるところがある。こうしたことから、これら項目は「実務基準」ではなく、「統制基準」として整理するのがよいと考える。「統制基準」として整理することが難しいならば、これら項目の順番を「実務基準」の一番最後にするのがよい。	南都銀行 山田様(専) 藤谷様(検)	「コンビニATM」および「デビッドカード」の安全対策基準に関しては、ビジネスモデル等も踏まえ、今後、「外部委託管理基準の検討」の中で整理させて頂きたいと考えております。	要	未
48	p14 p19	Ⅱフレームワーク 1．総論 (2)基準の分類（図8） (4)安全対策決定のプロセス（図11）	図表8で登場する「特定システム、通常システム」と図表10で登場する「情報システム、金融情報システム、上記以外のシステム」の関係性が判りにくいので、一体で整理してほしい。	日本銀行 水崎様(検)	金融情報システムをリスク特性の評価を踏まえ、「特定システム」「通常システム」および、「上記以外のシステム」に分類されることが分かるよう修正いたしました。	要	済
50	p16	Ⅱフレームワーク 1．総論 (2)基準の分類 (補足3)非金融機関等における・・	内容が分かりづらいと思われる。サービス提供主体が金融機関でない場合にあっても金融関連サービスを提供する業者はシステムの安全対策を策定する場合云々ということを言いたいのではないかと考えます。そう書けば多分ほかの解釈はないし、この一部の非金融機関の中のさらに業者とは一体何を指しているだろうということにはならないのではないかと思います。	全国信用金庫協会 蓮實様(検)	ご指摘を踏まえ、修正いたしました。	要	済
52	p17	Ⅱフレームワーク 1．総論 (3)安全対策基準の適用対象	【金融機関等がベンダーと契約するものや、協同組織等を通じてベンダーと～】とあるが共同組織等を運営組織等に変更していただきたい。	全国信用金庫協会 蓮實様(検)	ご指摘を踏まえ、修正いたしました。	要	済
53	p12 p17	Ⅱフレームワーク 1．総論 (3)安全対策基準の適用対象 (補足)金融機関等における特定システムと通常システムの分類	これはp12（1）②の補足とした方がよいのではないか。ご検討いただきたい。	三井住友銀行 持田様(専)	ご指摘を踏まえ、構成を一部見直しました。	要	済
15	p18	Ⅱフレームワーク 1．総論 (4)安全対策決定のプロセス ① リスク特性の洗い出し	なお、対象システムの特定などシステムリスク評価の方法については、評価方法のサンプルを提供することを検討してはどうか。	日本銀行 水崎様(検)	システムリスク評価の方法については、これまで当センター発刊の「金融機関等のシステムリスク管理入門」など、既に多くの文献が存在しています。リスク評価の方法については、こちらをサンプルとして脚注に記載することとしました。	要	済

No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
17	p19	Ⅱフレームワーク 1．総論 (4)安全対策決定のプロセス	リスクが低く安全対策基準が適用されない場合とは、具体的にどのような場合か、書いて頂いたほかにどのような考え方で「リスク」をとらえるべきかご記載頂きたく思います。適用外になるような評価ができる場合がわかることは、FinTech事業者にとっても有益と考えます。 （適用されない例） ・外部接続なし ・顧客データなし ・＿＿＿＿（他の例）	FinTech協会 瀧様(専)	リスクが極めて低いと判断する根拠は様々であり、一律に定義することは困難と考えられます。そうした中で、共通項として想定される「顧客データを保有しないなど」という例示を挙げました。また、限定列挙に読めるような表現にしてしまうと選択の幅が狭まってしまう可能性があると考えております。	否	原案のとおりとさせて頂きたいと考えております。
58	p20	Ⅱフレームワーク 1．総論 (4)安全対策決定のプロセス ③安全対策の目標設定（基準の選択・安全対策の選択）	各システムの安全対策目標の設定ではなく、目標設定方針の決定に経営層が関与する方が、実態として相応しいのではないか。	三井住友銀行 持田様(専)	ご指摘を踏まえ、修正いたしました。	要	済
59	p21	Ⅱフレームワーク 1．総論 (4)安全対策決定のプロセス ⑤コンティンジェンシープランの策定	残リスクに対して必ずCPが必要との書きぶりになっているが、単純に許容できるリスクや補完的な統制対応もあるのではないか。（＝CPを必須としたら逆に負担が増える可能性がある）	野村ホールディングス 荒木様(検)	ご指摘を踏まえ、修正いたしました。	要	済
60	p21	Ⅱフレームワーク 1．総論 (4)安全対策決定のプロセス ⑤コンティンジェンシープランの策定	対象物を明確化するために、「なお、安全対策基準においては～およぶことからコンティンジェンシープランについてはコンピュータシステムを中心に言及している」とした方がよいのではないか。	三井住友銀行 持田様(専)	ご指摘いただいた文章「なお、安全対策基準～を中心に言及している」は、当該パラグラフの中で冗長感があるため、削除しました。	要	済
62	p23	Ⅱフレームワーク 2．統制 (2)外部の統制 ①外部委託の管理におけるITガバナンス	[図13]「経営層以外」の「層」の文字の右横に両矢印があるが、何を指しているのか判読しづらい。恐らく「委託業務が低リスクな場合は～」を指していると思われるが、吹き出し線の色が周囲とほぼ同色で判読しづらい。（他、数名「分かりにくい」との意見あり）	NTTデータ 鎌田様(専)、鈴木様（検）	他の委員からのご指摘もあり、図13について、見やすさを改善します。	要	未
63	p25	Ⅱフレームワーク 2．統制 (2)外部の統制 ③基本形（2者間構成）における各論 b.共同センター	【主に勘定系システムなど、高い可用性が求められる～】とあるが、勘定系システムであれば機密性、可用性、完全性の全てが高いレベルで求められるので可用性はセキュリティや、安全対策などの用語の方が適切ではないか。	全国信用金庫協会 蓮實様(検)	ご指摘を踏まえ、該当箇所を「高い安全対策」に修正いたしました。	要	済
18	p25	Ⅱフレームワーク 2．統制 (2)外部の統制 ③基本形（2者間構成）における各論 b.共同センター	APIの共通基盤を作成した場合にはbの類型に含まれるのであれば、その旨の記載をお願いいたします。	FinTech協会 瀧様(専)	現時点では明確に分類できませんので、原文のままとさせて頂きたいと考えております。（今後、API共通基盤がITベンダー等によって運用される場合、それが金融機関等からみて共同センターと同様の委託関係が発生する場合には、その取扱いを改めて整理することが必要と考えております。）	否	原案のとおりとさせて頂きたいと考えております。
64	p25	Ⅱフレームワーク 2．統制 (2)外部の統制 ③基本形（2者間構成）における各論 c.クラウドサービス	クラウドサービスについては、外部委託に要求するような、安対遵守、監査受入、改善要求などは期待できない場合、安対によるコントロールでなくSLA等でもよいと言っているのでしょうか。（実際、数万台のサーバ設置拠点を監査することは現実的には不可能であるが）	三井住友銀行 持田様(専)	ご指摘頂いた箇所につきましては、誤解される可能性があることから「SLA等を契約するなど」という文言を削除しました。	要	済

No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針	原案の修正要否	反映状況コメントNo
77（追加）	p26	Ⅱフレームワーク 2．統制 (2)外部の統制 ④派生形（3者間構成）における通則 b.再配分ルール	FinTechに関する有識者検討会報告書の内容が反映されていないため、b.再配分ルールの最後に以下の一文を追加していただきたい。 （追加部分） なお、中立性及び有効性といった観点から、再配分によって、金融機関及びITベンダー等の負担が必要な範囲を超えて増加することがないよう留意することが重要である。 ※金融機関におけるFinTechに関する有識者検討会報告書 「Ⅱ．1．(1)目標とすべき安全対策の効果」の後半抜粋部分	日立製作所 宮崎様(検)	ご指摘を踏まえ、報告書の内容を正しく反映する観点で修正を加えました。	要	済
65	p26	Ⅱフレームワーク 2．統制 (2)外部の統制 ⑤派生形（3者間構成）における各論	3者間構成の各論について、タイプA、タイプBと各々文章での説明が続く。図式を用いるなど理解のし易さを考慮いただきたい。	NTTデータ 鎌田様(専)、鈴木様（検）	視覚的に理解しやすい図のアイディアがあれば、取り入れたいと考えております。	要	未
66	p27	Ⅱフレームワーク 2．統制 (2)外部の統制 ⑤派生形（3者間構成）における各論 b.タイプB	タイプAは従来通り決済代行業者等が金融機関の委託先、または再委託先の場合を指し、タイプBは決済代行業者等が顧客の委託先の場合を指していると思うが、【預取金融機関の勘定系システムに対して入出金の指示を行うなど、金融機関等に変わり、決済代行業者等が金融関連サービスを提供するため～】の「金融機関等にかわり」は決済代行業者が金融機関の委託先の様にもとれるため、削除していたたきたい。	全国信用金庫協会 蓮實様(検)	ご指摘の点のほかに、読みやすさの観点から修正しました。	要	済
72	p27	Ⅱフレームワーク 2．統制 (2)外部の統制 ⑤派生形（3者間構成）における各論 b.タイプB	最後の段落の記載（新設部分）につき、銀行の参照系ないし更新系のAPIに接続する事業者が本人確認義務を負うシチュエーションは現状の業務と即していません。利用する口座は金融機関において開設されたものであり、二重の確認が発生する本記載は修正が必要と考えております。一方で、口座開設や取引の実行等、本来あるべき認証が必要なケースへの対応であれば、その旨が明らかとなる記載として頂ければと思います。	FinTech協会 瀧様(専)	ご指摘の点については、各論等を議論する中で、改めて整理させて頂きたいと考えております。	要	未
67	p27	Ⅱフレームワーク 2．統制 (2)外部の統制 ⑤派生形（3者間構成）における各論 b.タイプB	タイプBの説明文の中で「例えば、～指す。」が5行に渡る長文である。文章を区切るなど読み易さを考慮いただきたい。	NTTデータ 鎌田様(専)、鈴木様（検）	ご指摘を踏まえ、読みやすさの観点で修正を加えました。	要	済

【資料１－２】
平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

改訂原案（安全対策基準前説）

削除: 基準の適用方法

【資料１－２】
平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

Ⅰ．概説

１．安全対策基準の意義

わが国の金融機関等のコンピュータシステムは、企業間・個人間におけるネットワーク化を前提とした新たな技術・サービスの急速な展開や、クラウド事業者、あるいは FinTech 企業[1]と呼ばれる革新的な金融関連サービスを提供する事業者の出現に伴う関係者の拡大を反映し、新たな局面を迎えつつある。また、IT の進展等により、システムに障害が生じた場合の影響が広域化・深刻化するおそれがあること、顧客データや企業の重要なデータ等を侵害するサイバー攻撃をはじめとする犯罪が巧妙化・大規模化するおそれがあることなどから、安全対策には多くの経営資源が必要とされている。

こうした中、金融機関等が信用秩序を維持し、利用者が安心してサービスを享受するためには、十分な安全対策の実施が不可欠であるが、一方で、金融機関等が顧客の利便性や企業価値[2]を高めるために、限りある経営資源を、安全対策のみならず、新規開発等にも適切に配分していくことが重要となってくる。

金融機関等のコンピュータシステムの安全対策は、第一義的には、システムを用いて金融サービスを提供する金融機関等の経営判断に基づいて実施されるべきである。その上で、リスク[3]が顕在化した場合に社会的に重大な影響を及ぼすシステムと、それ以外のシステムにおいては、それぞれのリスク特性に応じた安全対策の目標を設定することが妥当と考えられる。そこで、『金融機関等コンピュータシステムの安全対策基準・解説書』（以下、「本書」とする）では、金融機関等のよりどころとなる安全対策基準の適用において、リスクベースアプローチの考え方を取り入れ、現実的かつ効果的な安全対策の考え方を示すこととした。

また、システムに対する安全対策の実施主体が外部の委託先等にも拡大している中、FinTech 企業等との新たな関係や、重要な情報システムにクラウドサービスを用いた場合の安全対策のあり方を改めて考える必要がある。本書では、これらの金融機関の外部に対する統制のあり方を改めて示すとともに、金融機関内部の統制及び、これら統制のもとで実施する実務的な基準等との関係を示している。

本書は、公益財団法人 金融情報システムセンター（以下、「当センター」とする）内に設置された学識経験者、金融機関、保険会社、証券会社、クレジット会社及びコンピュータメーカー、クラウドサービス事業者、FinTech 企業等の専門的知識を有する安全対策専門委員及び、検討委員において審議・作成されたものである。

金融業務を営む業界の各社においては、本書が業務内容やその重要度に応じて実施すべき安全対策の指針となること、各社がコンピュータシステムの状況等に即し漸次実施しうる内容となっていること等を勘案し、各社が本書を参考にしながら適切な安全対策を実施することが期待される。

[1] 電子決済等代行業など、IT 技術を活用した革新的な金融に関連するサービスは、将来において更に多様化することが想定されるが、事業もしくは事業者に対し、現時点ではこれらを定義した画一的な名称が存在しない。本書においては、これら革新的な金融関連サービスを提供する事業者を「FinTech 企業等」と表現している。

[2] 相互扶助の精神から、地域の繁栄等を目的とする金融機関など、「企業価値の最大化」には多様な目的が含まれる。

[3] 本書では、金融機関等が情報システムの導入・利用等で実現しようとする経営目標の達成を阻害する不確実性及び、情報システムの障害等によって社会的な影響・損失を引き起こす不確実性をリスクとしている。

コメント [FISC1]: No.68

コメント [FISC2]: No.21
「金融関連サービス」は金融機関等以外が提供するサービスであり、定義を用語集に記載する。

コメント [FISC3]: No.36
「企業価値」についての説明（脚注）について、各委員の意見を踏まえ見直す。

コメント [FISC4]: No.22,23
顧客利便性の観点を入れ、再度内容を見直した。

コメント [FISC5]: No.24,25
改訂の趣旨を表す表現として見直した。

削除: あるべき安全対策

削除: 非金融機関等における決済代行業者等

コメント [FISC6]: No.26,68

コメント [FISC7]: No.6

削除: 金融、保険、証券、クレジット等

【資料１－２】
平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

２．安全対策の考え方

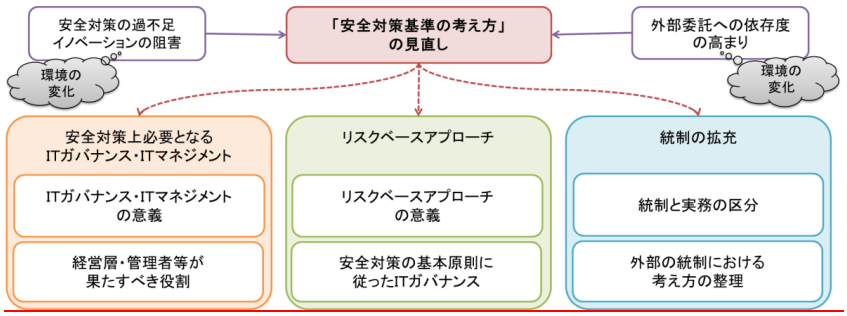
安全対策基準を取り巻く環境変化と対応

安全対策基準が作られた当初は、金融機関等の情報システムと言えば、基幹業務系のコンピュータシステムであった。そのため、安全対策基準の初版では、その適用対象とする情報システムを、「金融機関等のオンラインシステム」としていた。その後、情報化の進展に伴い、金融機関等の情報システムは、基幹業務系にとどまらず、情報系システムや部門システム等その範囲が広がり、基幹業務系以外のシステムがある程度大きなウエイトを占めるようになってきた。また、その形態や利用するサービスもホストコンピュータからクライアントサーバー、クラウドサービス、FinTech 企業等と連携した金融関連サービスなど、多様化してきている。

その過程で、安全対策基準は、基幹業務系システムの安全確保と安定運用という、当初の目的を果たしてきたものの、多様化する基幹業務系以外のシステムにおいては、適用の考え方が具体的に示されず、その結果、安全対策の程度に過不足が生じ、場合によっては、新規開発等への投資が抑制されるなど、経営資源が適切に配分されないといった懸念が生じている。また、金融機関等においては、システム開発・運用等における、外部委託への依存度が高まっているほか、金融関連サービスの利用が広がりをみせるなど、外部に対する統制の重要度が増している。

そうした状況を受けて、当センターにおいて、「金融機関における外部委託に関する有識者検討会」が開催され、外部への統制の拡充のほか、リスクベースアプローチの考え方に従った IT ガバナンスなど、安全対策基準の抜本的な見直しを含む提言が行われた。さらに、つづく「金融機関における FinTech に関する有識者検討会」では、革新的な金融関連サービスが登場する中、金融機関等がシステムの安全性を確保しつつ、企業価値を高めることを目指して、安全対策のあり方について提言が行われた。

これらの有識者検討会の提言内容を踏まえ、以下では、安全対策の考え方・利用方法等について理解いただくことを目的に、安全対策上必要となる IT ガバナンス・IT マネジメントについて解説した上で、リスクベースアプローチに基づく安全対策の基本原則及び、統制の拡充についての考え方を示すこととする（[図 1] を参照）。



[図 1] 安全対策基準を取り巻く環境変化と対応（概念図）

削除: 改訂の考え方

コメント [FISC8]: No.27
「利用するサービス」はシステムの形態と並列であり、文章を全体的に見直した。

コメント [FISC9]: No.68

削除: 決済代行業等

コメント [FISC10]: No.28

削除: 基準が不明確なままであり

コメント [FISC11]: No.29

削除: 多岐にわたる決済代行業等

コメント [FISC12]: 事務局
用語等の統一ならびに、レベル等に関して全体的に見直しを行った。

削除: 改訂の考え方

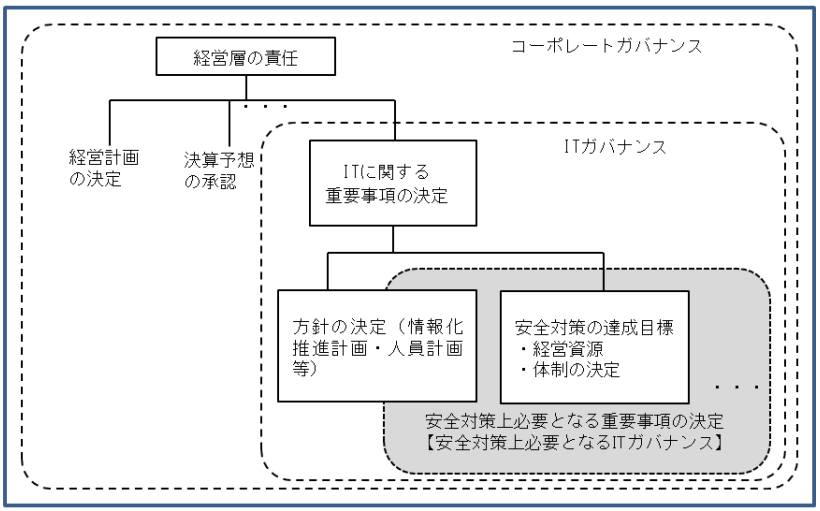
【資料１－２】
平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

(1) IT ガバナンスと IT マネジメント

金融機関等の活動は情報システムに大きく依存しており、その安全・安定の確保は、金融機関等の重要な経営課題である。

① 安全対策上必要となる IT ガバナンスの意義

一般的に IT ガバナンスとは、コーポレートガバナンスの中で、特に IT に関する重要事項について経営層が意思決定を行うための仕組みのことをいう。そうした IT に関する重要事項の中でも特に情報システムに対するセキュリティ対策をはじめとした安全対策は、金融機関等の活動の根幹に関わるため、優先度高く取り扱われるべき事項である（［図 2］を参照）。したがって、システム担当役員に限らず金融機関等の経営層は、安全対策上必要となる IT ガバナンスを機能させる責任を有する。



［図 2］IT ガバナンスの階層構造

社会的使命を担う金融機関等において、経営層は、顧客や株主等のステークホルダーに対し責任を有しており、情報システムに対する安全対策の重要性を十分認識するとともに、その重要事項の決定を行い、情報システムの安全・安定の確保を推進していく（［図 3］を参照）。

1) 中長期計画等における安全対策に係る重要事項の決定

a. 安全対策に係る方針の決定

ⅰ. システム戦略方針の決定

経営層は、中長期計画（経営戦略・ビジネス戦略等）との整合性を踏まえたうえで、システム戦略方針を決定する。

コメント [FISC13]: No.30

ⅱ. システムリスク管理方針の決定

iii. 安全対策の達成目標の決定

経営層は、金融機関等として、リスク特性に応じ達成すべき安全対策の目標を決定する。また、その場合でも、大きなセキュリティ上の脆弱性を残さないことに考慮する。

iv. 安全対策へ投下する経営資源の決定

経営層は、安全対策の達成目標の決定と同時に、達成目標を実現するために必要となる経営資源の投下（費用・配分方針等）を決定する。経営層は、経営資源が有限であることを踏まえて、あらかじめ、保有する経営資源を踏まえた達成目標を検討するとともに、リスク特性に応じた資源配分を決定することが重要である。

b. 安全対策に携わる業務執行体制及びモニタリング体制の決定

ⅰ. 安全対策に携わる業務執行体制の決定

経営層は、安全対策の達成目標及び投下する経営資源の内容を踏まえ、必要に応じて、システム部門等の業務執行体制を決定する。

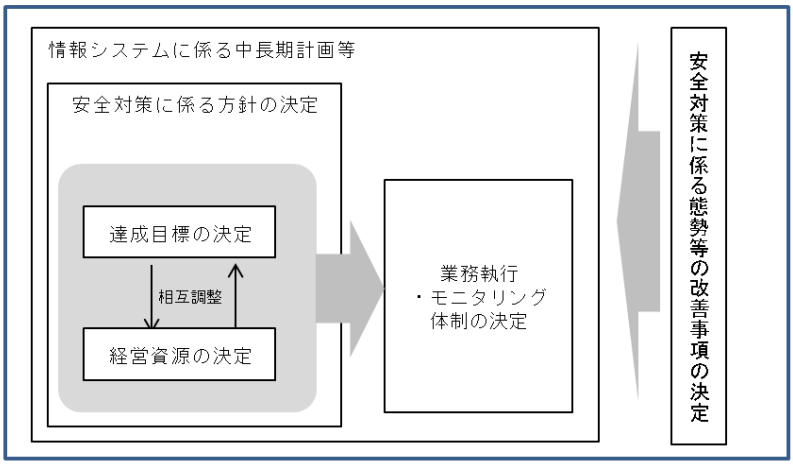
ⅱ. モニタリング体制の整備方針の決定

経営層は、安全対策の達成目標及び投下する経営資源の内容を踏まえ、必要に応じて、システム監査等のモニタリング体制の整備方針を決定する。

コメント [FISC14]: No.31

2) 安全対策に係る態勢等の改善事項の決定

経営層は、管理者（後述②1）を参照）からの報告やシステム監査報告等を通じて、みずからが決定した重要事項を踏まえて IT マネジメントが十分機能しているか検証したうえで、必要に応じて改善事項を決定し、安全対策に係る態勢等を継続的に改善していく。



［図 3］経営層が決定すべき安全対策に係る重要事項

【資料１－２】
平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

② 安全対策上必要となる IT マネジメント

IT マネジメントとは、経営層による IT ガバナンスのもとで、管理者が、情報システムの執行部門（システム担当・システムリスク管理担当等）に対して、IT に関する業務執行の管理等を行うことをいう。IT マネジメントにおいて、管理者等の関係者は以下の役割と責任を果たすことが求められる（［図 4］を参照）。

1）管理者

管理者は、経営層による IT ガバナンスのもとで、システム担当（部門）やシステムリスク管理担当（部門）等を統括し、安全対策上必要となる IT マネジメントを推進する。また、経営層に対しては、IT ガバナンスにおいて必要となる情報を、迅速かつ正確に提供する。

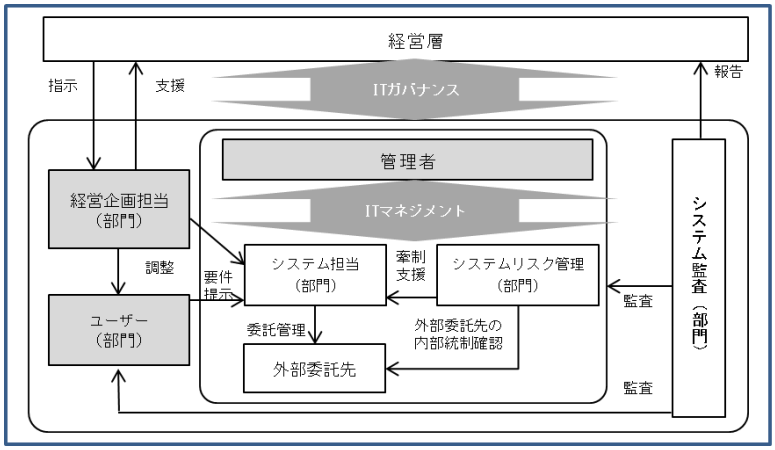
・内部規程・組織体制等の整備・見直し
・個々の情報システムに対する安全対策の決定
・安全対策上必要となる情報の経営層への報告

2）経営企画担当（部門）

安全対策を含むシステム化事案の決定において、部門間の調整結果をもとに、必要に応じて経営資源投下に関する優先度を評価する等、経営層の意思決定をサポートする。

3）ユーザー（部門）

金融機関等の本社主管部署で、経営戦略実現のために、ビジネスモデル（商品・サービス・事務）等の企画に携わるとともに、管理者等に対してシステム化の有用性・経営戦略への目的適合性等の説明を行い、システム開発着手時には、システム担当に対して業務要件を提示する。



［図 4］情報システムの安全対策に携わる関係者（例）

コメント [FISC15]: No.32

コメント [FISC16]: No.33

削除: ・内部規程・組織体制等の見直し

コメント [FISC17]: No.34

【資料１－２】
平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

(2) リスクベースアプローチ

① 安全対策基準を取り巻く環境の変化

これまでの安全対策基準では、「基幹業務のオンラインコンピュータ・システム」に適用する基準を明確化しているが、「基幹業務のオンラインコンピュータ・システム以外の情報システム」については、安全対策基準を「適宜取り入れる」あるいは「そのシステムによって提供されるサービスや扱う情報の重要性によって、個別に判断する」としてきた。

しかし、金融機関等を取り巻く環境変化の中で、大きな比率を占めてきたその他情報システムについては、適用する安全対策の考え方が具体的に示されないまま、不確実性を含む環境となっているため、以下の状況が生じていることが危惧される。

- 「基幹業務のオンラインコンピュータ・システム以外の情報システム」に対する安全対策を「基幹業務のオンラインコンピュータ・システム」に設定されているのと一律に設定しておけば安心する、といった形式的で安全性に偏った選択を行ってしまう。
- 「安全対策基準の考え方」に、安全対策への経営資源配分や、安全対策と新規開発との経営資源配分の調整といった観点が示されていないことから、金融機関等の経営層の経営資源配分に係る決定プロセス等によっては、そのシステムにおいて適切ではない安全対策が最終的にそのまま実施されてしまう。
- 経営層の立場では、ひとたび重大なシステム障害が発生すれば、その事実だけをもって、直ちにその結果責任を追及されかねないといった懸念から、経営層は、システム障害を極力ゼロとするために、そのシステムにおいて適切な水準を超えた安全対策を承認する、あるいはみずから追求してしまう。

② リスクベースアプローチの意義

従来の安全対策基準が内包する上記の課題を解決するためには、海外先進諸国の動向も踏まえ、一般的に「リスクベースアプローチ」と総称される考え方を取り入れることが有益である。リスクベースアプローチとは、金融機関等の安全対策の決定にあたり、リスク特性を分析した結果を、安全対策の優先順位等の合理的な意思決定に活用するとともに、金融機関等の経営資源が有限である点を踏まえ、安全対策に対する資源配分を経営資源全体の中で調整する考え方を言う。つまり、限られた経営資源の中では、リスクゼロを追求することは合理的ではないという基本的な考え方を金融機関等の経営層が理解し、BCP 等の事後対策を手当てしたうえで、リスクを受容する判断も取りうることを意味する。

次に、こうした、リスクベースアプローチの考え方を導入する際には、「金融機関等がみずから」その安全対策の達成目標を決定することが前提となる。つまり、安全対策の達成目標は、一義的には、金融機関等がシステムの安全性を確保しつつ、顧客の利便性向上や企業価値の最大化を目指し、IT ガバナンスを発揮して、決定されることが重要である。

コメント [FISC18]: No.35

削除: の安全対策が過不足な状態を残したまま

コメント [FISC19]: 事務局
整合性の観点から修正した。

コメント [FISC20]: 事務局
整合性の観点から修正した。

削除: 適正な水準以上の

コメント [FISC21]: No.7

削除: こととなる

【資料１－２】
平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

(3) 安全対策における基本原則

金融機関等は、リスクベースアプローチの考え方に従い、IT ガバナンスを発揮しつつ、リスク特性を踏まえた安全対策を実施することが期待される。

ただし、金融機関等は、社会性・公共性を有していることから、リスクの顕在化による影響が、個別金融機関等による統制可能な範囲を超えて外部に及ぶ場合（以下、「外部性を有する」という）や、機微情報（要配慮個人情報を含む）等の流出により、プライバシーなど個人の人権等が侵害される場合（以下、「機微性を有する」という）を考慮に入れるべきである。

以上を踏まえて、金融機関等の情報システムに対する安全対策における基本原則を以下のとおり定めるとともに、本基本原則を安全対策基準の前提として位置付ける。

金融機関等の情報システムの安全対策における基本原則

○情報システムに対する安全対策は、以下の考え方に基づき、適切な意思決定が行われ、運営されるべきである。
○情報システムに対する安全対策の達成目標は、個々の情報システムのリスク特性に応じて、適切な内容で決定されるべきである。
○情報システムに対する安全対策への経営資源配分は、リスク顕在化後の事後対策と比較衡量したうえで、情報システムに係る予算内における新規開発等との調整のみならず、経営資源全体も視野に入れ、顧客の利便性向上や企業価値の最大化を目指して、決定されるべきである。
○ただし、重大な外部性を有する情報システム及び機微性を有する情報システムにおいては、その社会的・公共的な観点から、このシステムの外部性や保有する情報の機微性を考慮に入れた安全対策の達成目標が設定されなければならない。

基本原則では、金融機関等は、IT ガバナンスを適切に発揮し、リスクベースアプローチの考え方に基づき、保有する情報システムに対する適切な安全対策をみずからが決定することができるとしている。

一方で、金融機関等の情報システムが、金融インフラの一部を構成している点を考慮し、重大な外部性や機微性を有するシステムについては、社会的・公共的な性質を持つことから、社会的に合意されたガイドライン等[4]を踏まえた「高い安全対策」が必要であるとしている。

コメント [FISC22]: No.37

コメント [FISC23]: No.19,39, 73
基本原則において、「上記を遵守のうえ」とした表現を削除し、「以下の考え方に基づき」とした。また「必要十分」については、「適切な」とし、企業価値向上に「顧客の利便性向上」を追記した。

削除: 、適切に運営されている限りにおいては、安全対策は独自に決定することが可能である

削除: 必要十分

削除: での

削除: 金融機関等が保有する

コメント [FISC24]: No.38

削除: 基本原則では、

[4] 監督当局の示すガイドラインや、業界団体等によって定められたガイドライン等を指す。本書に記載される安全対策基準も、金融機関等や関連するベンダー各社が定めるガイドラインとして、ここに含まれる。

【資料１－２】
平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

（参考）「重大な外部性」の考え方

・まず「外部性」とは、例えば、個別金融機関等におけるシステム障害等によって、個別金融機関等のみならず、他の金融機関やその顧客に影響を与える可能性のある性質をいう。中でも、金融機関等における為替や預金を取り扱うシステムは、深刻なシステム障害が発生した場合、他の金融機関やその顧客に対し広く影響を及ぼし、社会全体に経済的損失を与える「重大な外部性を有する」システムである。

・「外部性」には、当該金融機関等の顧客への影響は含まれない。なぜなら、これらの顧客に対しては、相手を個別に認識し個別に対処可能であり、損失額を内部的に算定できるからである。

・リスクベースアプローチに従って、適切に IT ガバナンスを発揮できる金融機関等であっても、「外部性を有する」情報システムに関する損害額等を正確には把握できない。特に、「重大な外部性を有する」システムの障害等に伴う影響を正確に把握し、障害を防止するためのコストを事前に算定・内部化して、安全対策の立案に的確に反映させることは困難である。

・こうしたことから、金融機関等では「重大な外部性を有する」システムには、「高い安全対策」を適用することが必要となる。

・なお、金融機関等における決済システムのうち、一般的には為替や預金を取り扱うシステムは、「重大な外部性を有する」と解されるが、例えば ATM やインターネットバンキング等を、これらと同様のシステムとして取り扱うかどうかは各金融機関等の判断によるものと考えられる。各金融機関等は保有するシステムのリスク評価を通じ、「重大な外部性を有する」システムを特定することが必要となる。

（参考）「情報の機微性」の考え方

・個人情報については、個人情報保護法等の法的規制のフレームワークがあり、金融機関等がシステムの安全対策を行う際に、これらを遵守する必要がある。

・しかしながら、金融機関等が取り扱う個人情報は多種多様で、住所や氏名等の情報から、病歴を含む生活履歴等極めて機微にわたるものまである。こうした機微性を有する情報に関しては、一般の個人情報と区別せず取り扱うことは適当でない。

・なぜなら、「機微情報（要配慮個人情報を含む）」は、本人等の許諾なく流出した場合、経済的損失に留まらず、プライバシー等、個人の人権等の侵害といった広範かつ甚大な損失を被る可能性を有するからである。

・仮に、一般の個人情報と機微情報（要配慮個人情報を含む）が同一に扱われてしまった場合には、金融機関等のほとんどすべてのシステムに存在している個人情報が、この機微情報（要配慮個人情報を含む）に影響されて適切な水準を超えた安全対策目標が設定され、資源の過剰配分が行われるおそれがある。

・このような事態を避けるためには、個人情報を「機微情報（要配慮個人情報を含む）」と「その他の個人情報」に分け、「機微情報（要配慮個人情報を含む）」については、「重大な外部性を有する」システムと同様、「高い安全対策」を適用することが必要となる。

コメント [FISC25]: No.9, 69

削除: 社会全体に経済的損失

削除: 個別

削除: 可能である

コメント [FISC26]: No.9,69

削除: ・金融機関等では、特にリスクが高い「重大な外部性を有する」システムにおいて、金融機関等共通の規範となるルール（＝高い安全対策）を適用することが必要となる。

削除: その取扱いは社会的・公共的な性質を有するものとも考えられることからも、「重大な外部性を有する」システムと同様に取り扱うことには合理性がある。

コメント [FISC27]: No.40,41

削除: これら

削除: 適正

削除: 以上の

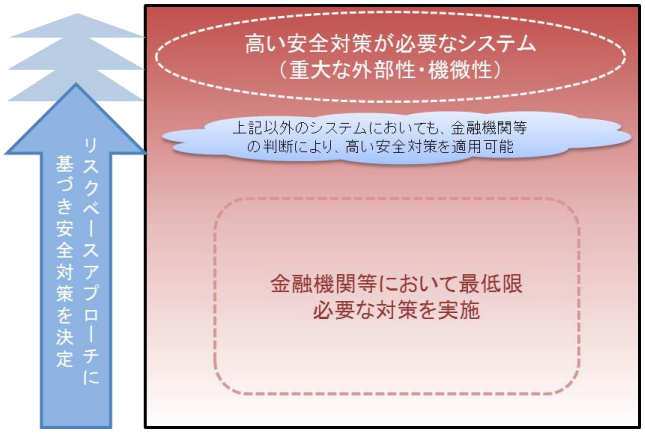
削除: のうち、その保護のために最上位の安全対策目標が設定されるべき

コメント [FISC28]: No.40

(4) 基本原則に従った IT ガバナンス

金融機関等の経営層は、情報システムのリスク特性を評価し、その評価された結果に基づき、新規投資等含め、投資効率の最大化を追求した経営資源配分を考慮したうえで、安全対策の目標を適切かつ包括的に決定する。この際、重大な外部性や機微性を有するシステムや、それらと同様の取扱いをする必要があると判断されるシステム[5]に対しては、「高い安全対策」を適用する。金融機関等の業務が情報システムに大きく依存している状況を踏まえ、経営資源配分の観点も含め、原則として、経営層みずからが、対象となるシステムを決定することが求められる。

「高い安全対策」が必要なシステム以外のシステムに対しては、金融機関等は、安全対策の達成目標を適切な水準で決定することとなるが、顧客データの漏えい防止等、金融機関等のシステムが満たすべき最低限の対策は、多くのシステムに共通すると考えられる。そこで、最低限の対策を予め設定することは、金融機関等が、リスクベースアプローチの考え方に基づき安全対策を決定する際、その不確実性を低減することに繋がると期待される（[図 5] を参照）。



[図 5] 基本原則に従った安全対策の考え方

(5) 安全対策における経営責任のあり方

経営層においては、「ひとたび重大なシステム障害が発生した場合、その事実をもって、結果責任を追及されかねない立場にあることから、高い安全対策を求めない訳にはいかない」といった共通認識が存在することから、安全対策の基本原則の遵守に当たっては、そうした認識が阻害要因となることが危惧される。

わが国の将来の金融ビジネスにおける優位性を確保するためには、監督当局と金融機関等において、必ずしもリスクゼロを追求しないといったリスクベースアプローチの考え方を共通の認識とするとともに、リスクベースアプローチを実施した結果として、リスクが残存し、

[5] 例えば、法人取引等に関する重要な機密情報を取り扱うシステムなどは、機微性を有するシステムと同等に扱うケースが想定される。

コメント [FISC29]: No.42

削除: 必要十分な

コメント [FISC30]: No.19

コメント [FISC31]: 事務局
高い安全対策が必要なシステムに対し、これらを超越したリスクを有するシステムはないことから、リスクの高低ではなく、「同様に扱うと判断されるシステム」として、表現を見直した。

削除: 同等以上のリスクを有する

削除: 必要十分な内容をもって、

コメント [FISC32]: No.19

さらにそれが顕在化した場合においても、監督当局が金融機関等に対して、障害や事故が発生してリスクが顕在化したという結果だけをもってその責任を追及することは、リスクベースアプローチの考え方と整合的ではない、という認識まで含めて、共有されるべきものと考える。

以上の考え方を踏まえて、安全対策における経営責任の在り方を以下のとおり示す。

金融機関等の情報システムの安全対策における経営責任のあり方

○経営層の使命は、顧客の利便性向上や企業価値の最大化であり、このことは、必ずしもリスクゼロを目指した安全対策の追求を意味するものではない。
○顧客の利便性向上や企業価値の最大化を目指した結果として、残るリスクについては、これを正当に認識したうえで、これに対応するために、その程度に応じて、コンティンジェンシープランを策定するとともに、環境変化に応じて見直すことが必要である。
○経営層が、諸法令を遵守するとともに、安全対策基準等の社会的に合意されたガイドライン（前述の安全対策における基本原則を含む）等を踏まえて、安全対策や残存リスクに対するコンティンジェンシープラン等を用意し、かつ、有事においては、これらを踏まえつつ臨機応変に対応している限りにおいては、客観的立場から見れば、法的責任を果たしているものと評価されるべきである。

(6) 安全対策基準における「統制」のあり方

「統制」とは、IT ガバナンスや IT マネジメントを行うための管理態勢の整備のことを言う。金融機関等における経営層は、基本原則に従って IT ガバナンスを発揮していくことが求められる。また、金融機関等において、外部委託への依存度が高まる中、安全対策基準は統制面での対策を拡充させていくことが求められる。これらの課題を解決していくには、安全対策基準において、統制面の対策を明示的に示すことが有効である。

① 「統制」と「実務」の区分

IT ガバナンス及び IT マネジメントを適切かつ効果的に発揮していくためには、経営層が、既存の考え方に縛られることなく、多様で主体的な創意工夫を発揮し、安全対策における、統制と実務の適切なバランスを確保することが望ましい。

そこで、安全対策基準では、「統制」に関する基準と、「実務」に関する基準を明確に分離し、さらに、統制に関連した基準を自組織内に対する「内部の統制」と、外部委託管理等を通じて外部（委託先等の他組織）への統制を発揮していくための基準である「外部の統制」に分けている。一方、「実務」に関する基準は、新たなテクノロジーの出現等により、常に変化していく部分であり、IT マネジメントを具体的に実行するための基準として、対象とするシステムや、各局面等に応じたリスク管理策を設けている（［図 6］を参照）。

コメント [FISC33]: No.43

書式変更：リスト段落，インデント ： 左 3 字，最初の行 ： 1 字

コメント [FISC34]: No.2

コメント [FISC35]: No.2, 74（追加）

【資料１－２】
平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

区分		基準の内容
統制	内部（自組織内）の統制	金融機関等において、セキュリティポリシーの策定や、教育・訓練を含む、管理態勢等を整備するために実施する対策
	外部（委託先等の他組織）の統制	契約締結や業務管理など、外部へ委託するうえで実施する対策
実　務		管理者がリスクの管理対象やリスクの程度に応じて、具体的に実施する対策

［図 6］「統制」と「実務」の区分

② 外部に対する「統制」のあり方

金融機関等においては、外部委託やサービスの利用が拡大しており、外部に対する「統制」の重要性が増している。

内部に対する統制に対し、外部に対しては、一般的には「統制」が及びにくくなるといった特性があり、再委託においては、そうした特性がいっそう顕著となるものと考えられる。また、委託業務が分割され複数の先に再委託され、さらに、再委託先からその先にも再委託が進めば、委託先を通じた「統制」の構造が複雑化し、「統制」の難易度は極めて高くなることが危惧される。

当然のことながら、金融機関等が、外部に対して、「統制」を全く行わないことは、社会的・公共的な観点から適当でないことは自明であるものの、金融機関等の内部に求められるものと同程度まで完全な「統制」を行うと、コスト削減や先進技術の利用を目指して行われる外部委託本来の目的が損なわれるおそれがある。したがって、金融機関等の社会的・公共的な観点や委託目的を総合的に勘案した結果として、委託先及び再委託先との接点において、最適な「統制」を決定することが重要であり、これは、リスクベースアプローチや「安全対策における経営責任の在り方」で示した内容と何ら異ならない。すなわち、金融機関等においては、顧客の利便性向上や企業価値の最大化を目指して経営資源配分と最適な安全対策が決定され、残存リスクに対し適切に対応されている限りにおいては、その責任は果たされていると解される。

金融機関等と委託先との間では、統制と実務において、各々が果たすべき役割（以下、責務という）が存在[6]し、安全対策の達成目標は、これら責務の分担と各々の責務の確実な遂行によって実現される。なお、FinTech 企業との契約形態には、外部委託とは性質の異なるものが存在する[7]。金融機関等においては、金融関連サービスを提供する FinTech 企業等によって運用される情報システムに対し、金融機関等に安全対策上の責務が生じる範囲において、適切な水準で外部の統制を行うことが必要となる。

[6] 一般には、金融機関等において、委託先に対する「統制」の責務が発生することになるが、委託先が再委託先を管理するための「統制」についても考慮する必要がある。

[7] FinTech 企業等が金融関連サービスを主導するシステムを運用し、金融機関等との接続を行う場合、運用主体である FinTech 企業等と、接続される金融機関との間には外部委託とは異なる性質の契約関係が存在する。金融機関等は、FinTech 企業等に対して外部委託先に対する統制をそのまま適用できない場合を考慮する必要がある。

コメント [FISC36]: No.74（追加）
コメント [FISC37]: No.44
コメント [FISC38]: No.45
削除: 委託先等
削除: 等企業価値の最大化
コメント [FISC39]: No.50,68
削除: 外部委託の一形態である「クラウドサービス」や、決済代行業等を営む事業者
コメント [FISC40]: No.1
削除: これらの考え方と整合性が保たれることが
コメント [FISC41]: No.1

【資料１－２】
平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

Ⅱ．フレームワーク

１．総論

ここでは、安全対策基準の考え方を踏まえ、リスクベースアプローチの考え方に基づき安全対策基準を具体的に適用していくにあたり、対象システムや、基準の構成、分類、適用対象など、安全対策の決定に必要な定義やプロセスを示す。

(1) 安全対策基準における定義

① 金融情報システム

金融機関等が、業法等に基づき、顧客に商品・サービスを提供するために利用する情報システムを、「金融情報システム」と定義する。

② 特定システム・通常システム

金融情報システムのうち、重大な外部性を有するシステム（システム障害等が発生した場合の社会的な影響が大きく、個別金融機関等では影響をコントロールできない可能性があるシステム）や、機微情報（要配慮個人情報を含む）を有するシステム（機微情報（要配慮個人情報を含む）の漏えい等により顧客に広範な損失を与える可能性があるシステム）を、「特定システム」と定義する[8]。「特定システム」には、「高い安全対策」を適用する必要がある。

特定システム以外の金融情報システムを、「通常システム」と定義する。通常システムにおいては、そのリスク特性に応じた基準を適用することが可能である。

なお、特定システムの一部を、サブシステムとして独立して管理することが可能であり、かつ当該サブシステムにおいて発生したリスク事象がシステム全体へ影響を及ぼすことを防止できる場合や、当該サブシステムが停止する等の障害が発生した際、業務停止を回避するための代替策が可能な場合には、当該サブシステムを特定システムから切り離し、「通常システム」として安全対策を適用することが可能である[9]。

[8] 安全対策基準における「特定システム」とは、必ずしも監督当局等への報告対象となるシステムを指すものではない。「特定システム」は、あくまでその社会的影響を考慮して個別金融機関等が設定すべきものである点を補足しておく。

[9] 例えば、システム全体では、顧客情報が保有されているが、当該サブシステム内には顧客情報が保有されていない場合等が考えられる。

コメント [FISC42]: No.46
フレームワーク編の位置付けを明確にするため説明を加えた。（暫定案）

削除: 運用または

コメント [FISC43]: 事務局
考え方で示した「高い安全対策」が必要なシステムについて、分かりやすさの観点から具体的な内容を追記した。

コメント [FISC44]: 事務局
コメント FISC41 のとおり。

削除: 性の確保を必要と

削除: 安全対策

削除: 設定

コメント [FISC45]: No.11
特定システムの一部について、脚注にて例示を示した。

削除: 設定

（参考）金融機関等における特定システムと通常システムの分類

個別金融機関等におけるシステムの分類は、業態ごと[10]、または個別金融機関等における取扱い業務の重要度の位置付けによって様々であり、それらを一律に特定し、列挙することは難しいため、どのシステムが「通常システム」または「特定システム」に分類されるかは、個別金融機関等が実態に則して判断することとなる。安全対策基準を適用するに当たっては、経営層が適切な IT ガバナンスを発揮したうえで、個別金融機関等におけるリスク評価や、経営資源配分等の観点を考慮したうえで対象となるシステムを決定することが求められる。

コメント [FISC46]: No.53
安全対策基準の適用対象に記載していたが、システムの定義に対する補足であるため、ここに移動した。

削除: 補足

削除: 共通的な

削除: 困難であり

③ 安全対策基準の構成

安全対策基準は、その目的や利用場面に応じて体系化しており、「統制基準」「実務基準」「設備基準」「監査基準」の４編で構成される（[図 7] を参照）。

a. 統制基準

IT ガバナンスや IT マネジメントを行ううえで必要な管理態勢の整備のための「内部の統制」及び「外部の統制」に関する基準・解説等から構成される。内部の統制は、社内体制の整備や、方針の策定、人材育成・訓練等に関する対策を記載している。外部の統制は、契約手続きや委託先の業務管理等、金融情報システムを外部へ委託するうえで必要となる対策を記載している（詳細は「２．統制」を参照）。

b. 実務基準

金融情報システムの信頼性・安全性の向上を図るために必要となる、システム企画・開発、運用、防災・防犯等に関する実務的な対策に関する基準・解説等から構成される。実務基準には、オペレーション等、管理者や作業者等が主体となる対策と、関連する技術的対策が含まれる。

なお、技術の進展が著しい環境下においては、その対策を字義通りに適用することが適当ではない場合があり、最新の技術動向等を踏まえ、金融機関等において適用の可否を判断されるべきものが含まれることに留意する必要がある。

c. 設備基準

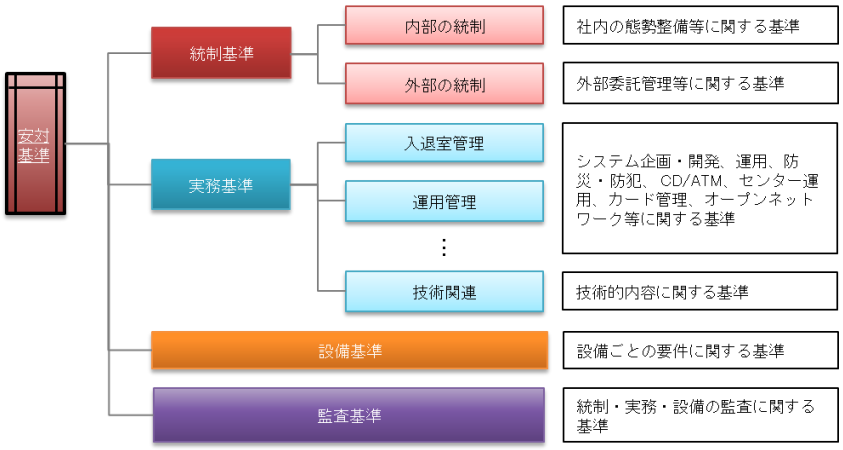
コンピュータシステムが収容される建物や設備を自然災害、不正行為等から守るための対策に関する基準・解説等から構成される。

10 一般に、預金取扱金融機関における為替システム、預金システム等は、重大な外部性を有すると想定され、生命保険会社等における、給付金査定等を行うシステムは、機微性を有すると想定される（Ⅰ.2.(3)「安全対策における基本原則（参考）」を参照）。証券会社におけるトレーディングシステムや、インターネットバンキングを主なチャネルとする預金取扱金融機関におけるインターネットバンキングシステムなどは、特定システムと同等に扱うことが考えられる。一方で、類似のシステムを有する金融機関等においても、そのシステム構成や、利用形態を鑑み、特定システムと判断しないことも考えられる。

コンピュータセンターの建物・付帯施設及び設備、本部・営業店等の建物・付帯施設及び設備、流通・小売店舗等と提携してサービスを提供する場合の建物・付帯施設及び設備に関する対策を記述する。

d. 監査基準

統制、実務及び設備に対する監査を行ううえで必要となる、監査体制の整備や手順について記載している。



［図 7］安全対策基準の構成

(2) 基準の分類

本書では、金融機関等がリスク特性に応じた安全対策の目標を設定するにあたり、不確実性を低減させることを目的に、「基礎基準」を設定している。一方で、「基礎基準」以外の基準は、リスク特性に応じて追加・選択する「付加基準」としている。

「基礎基準」は、特定システム、通常システムによらず、金融情報システムが最低限適用する基準として、以下の考え方に基づき設定している。

全てのシステムにおいて安全対策を決定、実施していくためには、セキュリティポリシーや、外部委託に関する方針等が整備され、必要な人員が確保・教育されるなど、IT ガバナンスが適切に発揮されていることが必要である。このため、内部及び外部の統制並びに監査に関する基準は、これらをまず「基礎基準」としている。

また、一般に金融情報システムは、商品・サービスを顧客に提供するため、顧客データを保有または、顧客データに接続していると想定されることから、顧客データの漏えい防止に関する基準についても「基礎基準」としている。顧客データには、個人データ以外の重要なデータ[11]が含まれる場合があるが、この場合も顧客データ漏えい防止に関する基準が有効と考えられる。

また、近年において重要性が増しているサイバー攻撃対策に関する基準も、顧客データの

[11] 企業の公開前決算情報など、金融機関等において高い機密性が求められる情報を指す。

削除: 最低限の安全対策として、安全対策基準の中から

削除: 「基礎基準」は、特定システム、通常システムによらず、金融情報システムにおける適用基準であり、統制基準、実務基準及び、監査基準のうち顧客データの漏えい防止等の観点から抽出した一部の基準で構成されている。

コメント [FISC47]: 事務局
統制・監査を基礎基準として根拠を追加。

書式変更: 下線

書式変更: 下線

削除: なお、金融情報システムには、

削除: おける対策

漏えい防止に関する基準に含めている。

さらに、リスクベースアプローチの考えでは、必ずしもリスクゼロを追求しないことから残存リスクへの対応を考慮する必要がある。このため、コンティンジェンシープラン策定に関する基準についても、「基礎基準」としている。

「基礎基準」の選定にあたっての考え方

○統制・監査に関する基準
○顧客データの漏えい防止に関する基準
○コンティンジェンシープラン策定に関する基準

上記以外の観点で必要となる基準については、各金融機関等が、システム構成やリスク評価の結果等を考慮のうえ、適宜、必要に応じて選択する「付加基準」となる。例えば、通常システムにおいて高い可用性が求められる場合は、可用性を確保するための安全対策の目標を定め、「付加基準」の中から適宜、必要な基準を選択・追加することで、安全対策の水準を高めることとなる。

なお、「設備基準」については、収納するコンピュータシステムに求められる基準を一意に定めることが困難であることから、「基礎基準」及び「付加基準」を区分していない。

「基礎基準」は、特定システム、通常システムによらず、金融情報システムにおける最低限の基準として設定しているが、システム構成や、リスク特性の観点から全てが適用されないことを考慮し、「原則として適用[12]」としている。

通常システムでは原則として「基礎基準」を適用するとともに、リスク特性を踏まえ、「付加基準」から必要な基準を選択・追加する。特定システムでは、「基礎基準」及び、「付加基準」を「原則として適用[13]」としている（[図 8]を参照、詳細は、(4)安全対策決定のプロセスを参照）。

	基礎基準	付加基準
特定システム	原則として適用	原則として適用
通常システム		リスク特性に応じて選択追加可

［図 8］基礎基準と付加基準

[12] 安全対策基準の中には、特定のシステムや業務（外部接続管理や渉外端末の管理に関する基準等）のみを対象とした基準が含まれており、これらは最低限の基準であっても、システムによっては適用除外となる。こうした点を考慮して、「原則として適用」との表現を使用している。

[13] 重大な外部性を有するシステムと、機微性を有するシステムでは、適用する基準が異なることが想定される。また、特定のシステムや業務のみを対象とした基準が含まれる。こうしたことを考慮して、特定システムにおいても、すべての付加基準を適用するわけではないため、「原則として適用」との表現を使用している。

削除: 安全対策

削除: 安全対策の設定において、

書式変更: 下線

コメント [FISC48]: 事務局
タイトルを「基礎基準」の選定にあたっての考え方に修正。

コメント [FISC49]: 事務局
読みやすさの観点から、文章の位置を基礎基準の条件の下に移動した。

削除: の観点で必要となる安全対策について

削除: システム毎のリスク特性に差異があり、

削除: で、適切な水準の安全対策となるよう決定することになる

削除: 「設備基準」は、既に、コンピュータセンターに求められる基準と、本部・営業店等、各拠点に求められる基準を区分して記載しているため

削除: 安全対策

コメント [FISC50]: No.8,47,70

削除: 全ての

コメント [FISC51]: No.8,47,70

削除: 全て

コメント [FISC52]: No.8,47,70
「全て適用」を「原則として適用」に修正

【資料１－２】
平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

コメント [FISC53]: No71
（補足２）については、外部委託基準の検討の中で整理する。

コメント [FISC54]: No.50,51
(3)安全対策基準の適用対象に移動させ、外部委託または外部委託と異なる場合の安全対策基準の適用の考え方として内容を見直した。

削除: （補足３）決済代行業者等における安全対策基準の適用について

【資料１－２】
平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

(3) 安全対策基準の適用対象

安全対策基準は金融情報システムに適用される。共同センター等[14]、金融機関等が統制を行うシステムは、外部委託と同等の性質を有するものとして、必要となる安全対策を設定する。

なお、金融機関相互のシステム・ネットワーク等[15]は、金融機関等が共同して運営するものであり、個別金融機関等が負う管理責任が部分的となるシステムとして区分している。これらは、主にサービスの利用者の視点で実施すべき対策等、外部委託の統制面において必要となる安全対策を設定する。

金融機関等における、金融情報システム以外のシステムについては、安全対策基準の適用対象外であるが、その技術基盤（セグメント等）の共通性や、金融情報システムとのリスク特性の類似性がある場合は、必要となる対策を適宜取り入れることとする。

金融機関等以外の事業者が金融機関等の外部委託先として金融関連サービスを提供する場合、金融機関等による外部の統制を受けることとなり、当該金融関連サービスを提供する情報システムは、結果として安全対策基準の適用対象となる。

一方で、金融機関等以外の事業者が金融機関等の外部委託先とはならず、主導的に金融関連サービスを提供する場合、金融機関等による外部の統制が及ばないか、または部分的となることが考えられる。金融機関等による外部の統制が及ばない場合は、当該金融関連サービスを提供する情報システムは、安全対策基準の適用外となる[16]。また、金融機関等における外部の統制が部分的となる場合、当該金融関連サービスを提供する情報システムは、金融機関等に責務が生じる範囲において、結果として安全対策基準が部分的に適用対象[17]となる。

コメント [FISC55]: No.52

コメント [FISC56]: No.74（追加）

削除: 「外部の

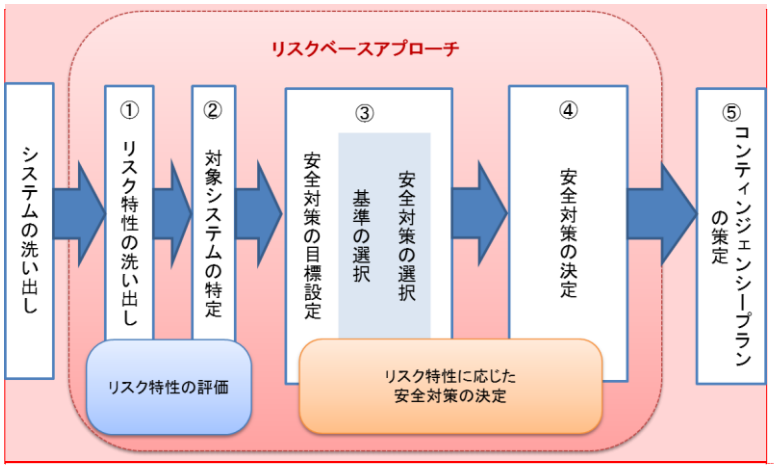
削除: 」

コメント [FISC57]: No.26,50,51

[14] 金融機関等がベンダーと契約するものや、運営組織等を通じてベンダーと契約するものなどが含まれる。
[15] 全銀ネット、CAFIS、統合 ATM、協同組織金融機関為替中継システム、SWIFT、LINC、損保ネット等は外部のシステムと定義している。その他、日銀ネット、でんさいネット、ほふりシステム、証券取引所システム等も、ここに分類される。
[16] 金融機関等以外の事業者においては、各業界等で定める基準・ガイドライン等に従うことが想定されるものの、その際、金融機関等が最低限満たすべき「基礎基準」を踏まえた安全対策が選択・運用されることが期待される。
[17] 金融関連サービスにおいて、金融機関等に安全対策上の部分的な責任が生じる場合、金融機関等は金融機関等以外の事業者に対し、その責任が生じる範囲において有効な安全対策が実施され、その効果が発揮されていることを検証していくこととなり、これを外部委託基準の「準用」と呼んでいる。例えば、預金取扱金融機関における勘定系システムに対し、オープン API 等による接続が行われる場合は、当該システムはインターネットバンキングに類似するリスク特性を有していると解され、金融機関等は、FinTech 企業等に対し、「データの保全」または「本人認証」に係る安全対策の実施状況や、その効果について検証を行うこととなる。

(4) 安全対策決定のプロセス

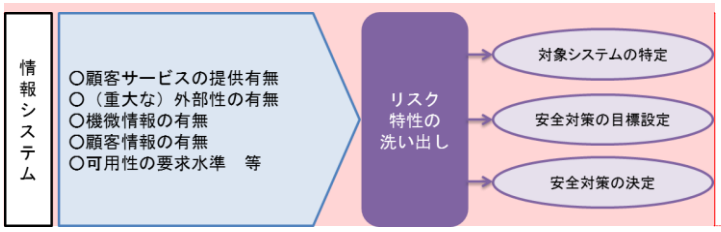
リスクベースアプローチでは、その経営資源配分の効果が最大となるよう、適切な内容で安全対策を決定していくこととなる。金融機関等は、安全対策基準の適用対象となる各システムのリスク特性を洗い出し、対象システムを特定した後、安全対策の目標を定め、必要となる基準及び安全対策の選択を行ったうえ、安全対策の目標に対し、安全対策費用とその効果、新規開発投資とその効果、それぞれについて、効率が最大化されるよう考慮し、最終的に安全対策を決定していく。その結果、残存リスクが発生する場合は、必要に応じて、コンティンジェンシープランを策定する（[図 9]を参照）。



［図 9］安全対策決定のプロセス

① リスク特性の洗い出し

金融機関等は、利用する金融情報情報システムを洗い出した後、リスク特性の評価[18]に必要となる、各システムのリスク特性の洗い出しを行う。リスク特性の洗い出しは、まず、金融サービスを顧客に提供するものかどうか、（重大な）外部性、機微情報、顧客情報の有無、可用性の要求水準等の観点に基づき行っていく（[図 10]を参照）。



［図 10］リスク特性の評価

18 リスク評価の手法については、当センター発行の『金融機関等のシステムリスク管理入門』などを参考に、各金融機関等の実態を考慮のうえ、各金融機関等において有効な方法が選択されることを想定しており、本書では具体的な手法については示していない。

コメント [FISC58]: 事務局
タイトルを「安全対策基準の適用方法」から変更し、図９の工程（修正後）に従って、以下の構成を全体的に見直した。

削除: ① リスクベースアプローチに従った安全対策の決定 .

削除: 経営資源配分の効果を最大化するためには、

コメント [FISC59]: No.54

コメント [FISC60]: No.15

削除: 保有または

コメント [FISC61]: No.48

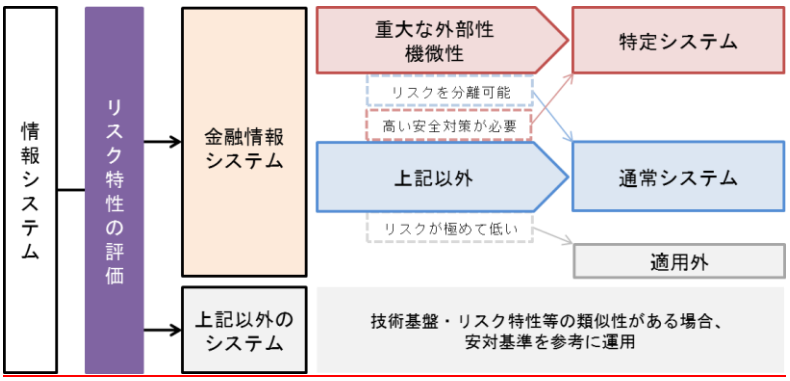
② 対象システムの特定

洗い出されたリスク特性を評価し、利用する金融情報システムから、安全対策基準の適用対象となる金融情報システムを特定する。金融情報システム以外のシステムについては、その技術基盤やリスク特性に類似性がある場合、安全対策基準を適宜取り入れることとする。

次に、金融情報システムを、重大な外部性または機微情報を有する特定システムと、それ以外の通常システムに区分する。この際、各金融機関等の判断により、通常システムの中から、高い安全対策が必要なシステムを独自に選択することも可能である。一方で、特定システムの一部において、リスクが低いと判断されるサブシステムは、リスク管理上、当該サブシステムを分離することが可能な場合、これを通常システムとして取り扱うことも可能である（1.(1)②「特定システム・通常システム」を参照）。

また、金融情報システムにおいて、内部だけで利用されるシステムや、顧客データを保有しないシステムなど、リスクが極めて低いと判断される場合は、安全対策基準の適用対象外とすることも可能である（[図 11]を参照）。

金融機関等においては、システムの区分を更に細分化する等の方法も考えられるため、金融機関等のセキュリティポリシー等を踏まえた創意工夫によって、よりリスクベースアプローチの考えを反映した方法とすることも可能である。



［図 11］対象システムの特定

金融機関等を取り巻く環境変化等により、保有するリスクの種類や程度は変動していくことが想定される。このため、金融機関等では、リスク特性の洗い出し及びリスク特性の評価を定期的に実施するとともに、適宜、対象システムの特定の結果を見直すことが必要となる。

③ 安全対策の目標設定（基準の選択・安全対策の選択）

対象システムを特定した後、個々のシステムのリスク特性の評価結果に応じ、安全対策の目標を設定する。個々のシステムに対する安全対策の目標設定では、例えば、保有する

削除: 保有または

コメント [FISC62]: No.75（追加）

データの種類や稼働率など、システムのリスク特性に応じて、選択した基準からどの対策を実施すべきかを選択していくことが考えられる。適切な目標を設定するためには、例えば、リスク事象ごとに定められた障害発生件数の抑制など、目標設定の方針が定められていることが必要である。目標設定の方針は、システムリスク管理方針や、セキュリティポリシー、経営資源配分等の観点を踏まえ、経営層の関与のもと決定されることとなる。

IT マネジメントを担う管理者等は、設定された安全対策の目標を達成するために、必要となる基準及び対策を選択する。

特定システムにおいては、原則として、基礎基準に示された対策及び付加基準に示された対策の中から必要な対策を選択する。

通常システムは、原則として、基礎基準に示された対策を選択した後、個々のシステムのリスク特性等を考慮のうえ、必要に応じ付加基準を追加していく。

なお、基準の選択及び対策の選択において、システム構成やリスク特性から、明確に不要な基準及び対策は適用除外となる[19]。

④ 安全対策の決定

安全対策を選択した後、経営資源配分の観点等を踏まえ、最終的な安全対策を決定する。安全対策の決定においては、安全対策を実施した場合とリスクを受容した場合における費用等を比較衡量のうえ、安全対策の選択を見直すことも可能である。また、リスク特性や経営資源配分の観点から、実施する安全対策の程度[20]についても検討し、セキュリティ上の大きな脆弱性を残さないよう、安全対策を決定していく。この結果、残存リスクが発生する場合は、原則としてコンティンジェンシープランを策定し、適切にリスクに対応できる態勢を整備しておくことが必要となる。

⑤ コンティンジェンシープランの策定

コンティンジェンシープランとは、金融機関等のコンピュータセンター、営業店、本部機構等が、不慮の災害や事故、あるいは障害等により重大な損害を被り、業務の遂行が果たせなくなった場合に、各種業務の中断の範囲と期間を極小化し、迅速かつ効率的に必要な業務を復旧するために、あらかじめ策定された「緊急時対応計画」のことである。

残存リスクに対するコンティンジェンシープランの策定は、金融機関等が策定する必要最低限の安全対策と位置付けている。ただし、リスク自体を単純に受容できるなど、コンティジェンシープランを策定する必要がない場合もあるため、残存リスクの特性に応じて、適切に策定されることが必要である。

また、近年、自然災害以外の脅威として、サイバー攻撃や感染症のパンデミック災害等についても体制の整備や要員の確保の観点から考慮することが必要となっている。

コンティンジェンシープランの目的は、従来から推進されている安全対策の積み重ねを

19 「1.(2)基準の分類」を参照。

20 安全対策を実現する技術や手法について、難易度や品質の程度を決定することを指す。例えば、本人確認において、生体認証方式や、ワンタイムパスワードを採用するなど、リスク特性に応じてより高度で優れた技術を採用する場合などが考えられる。

コメント [FISC63]: No.58

削除: が望ましい

コメント [FISC64]: No.56

削除: に応じ

削除: （[図 12]を参照）

コメント [FISC65]: No.56

削除: を予め選択しないことも可能

コメント [FISC66]: 事務局
図 8 にて基準の適用方法を示していることと、上記説明文があるため、システムごとの基準の適用をしめした図は削除した。

削除: .
.
［図 12］基準の選択・安全対策の選択

コメント [FISC67]: No.59

コメント [FISC68]: No.60

削除: .
なお、安全対策基準においては、金融業務が情報システムに深く依存しており、その不具合が業務全般に及ぶことから、コンピュータシステムを中心に言及している。

削除: 外部ネットワークに接続しないシステムにおいて、外部ネットワークの機器設定に関する基準等は省略することも可能である。

前提に、これらの対策では防ぐことのできなかった緊急事態に際して、可能な限り影響を軽減し、早期に業務を復旧させることにある。

影響範囲が限定された障害等の発生については、あらかじめ計画された回復措置等により、処置できるケースが多く、安全対策基準の「障害時・災害時対応策」の中でその対応手順を述べている。しかし広域災害のような、影響が広範囲にわたり金融機関等として統一された行動計画による対応が必要となる場合には、システム部門内にとどまらず、全社的にまとめられた、事前に十分に準備された計画が不可欠となる。

このための緊急時対応計画として、コンティンジェンシープランを事前に策定しておくことが必要であり、コンティンジェンシープラン構築の必要性を安全対策基準の中で記述し、金融機関等が実施すべき最低限の安全対策の一つと位置づけている。

コンティンジェンシープランの詳細については、当センター発刊の『金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書』を参照されたい。

【資料１－２】
平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

２．統制

金融機関等においては、安全対策を決定するうえで、基本原則に従った IT ガバナンスを発揮することが前提となる。このため、これら統制に関する基準は「基礎基準」としている。統制には「内部の統制」と「外部の統制」があり、両者は「統制」の対象や統制の方法が異なる。ここでは、これら「統制」の内容と、ルールの導出に至る考え方について解説する。

(1) 内部の統制

安全対策基準上の「内部の統制」とは、金融機関等が、安全対策を策定・推進していくために自組織内で実施すべき対策を指す。具体的には、セキュリティポリシーの策定、規程等の整備、セキュリティ管理態勢等の組織の整備、要員の教育・管理、訓練等を指す。

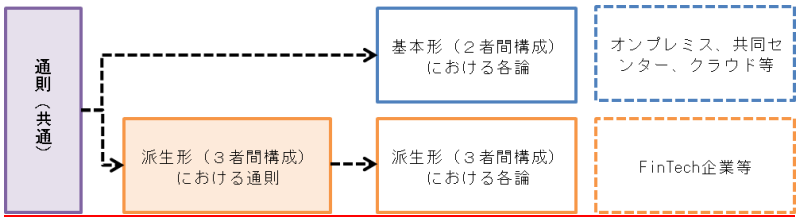
安全対策基準上は、内部の統制を、以下のカテゴリーに分類している。

a. 方針・規程
b. 組織体制
c. サイバー攻撃対応態勢
d. 人材（要員・教育）

内部の統制に関する方針・対策の決定には、多くの部門が関係することが一般的である。このため、内部の統制に実効性をもたせるためには、人員計画（ローテーション、キャリアパスの策定等）や経営資源配分など、経営層による意思決定が求められる。

(2) 外部の統制

金融情報システムにおける「外部の統制」は、以下のように体系化される。まず、IT ベンダー等とのシステムの開発・運用の委託や、クラウドベンダー等の利用など、２者間で構成される委託関係がある。次に、委託先に加えて、FinTech 企業等のように、必ずしも委託関係にあるとは限らない企業が関与する３者間構成がある。以下では、それぞれについて、「外部の統制」における考え方を解説する（[図 12] を参照）。



［図 12］外部の統制における体系

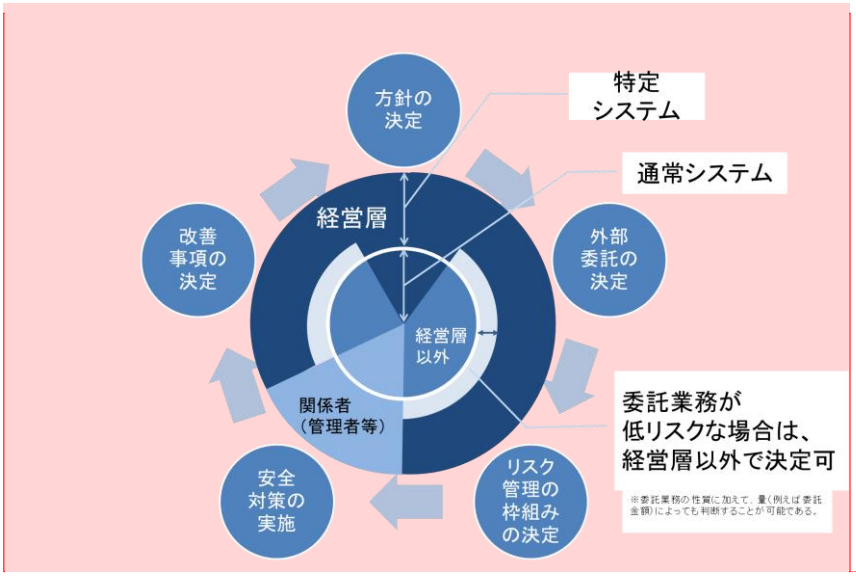
削除: 対策
削除: 、原則として全て
削除: 21
削除: に関する対策が含まれるが
コメント [FISC69]: No.68
削除: 決済代行業者等
削除: IT ベンダーと金融関連サービスを提供する性質を併せ持つ関係者を含む
コメント [FISC70]: No.61
FinTech と金融機関等の関係では、これまでの外部委託の考え方と異なる、それ以外の形態を意識した記載が必要である。(API 連携先等との関係)
削除: について
削除: における考え方

① 外部委託の管理における IT ガバナンス

IT の進展や金融機関等の業務範囲の拡大等に伴い、国内の金融機関等では、コスト削減や先進技術の利用等により、顧客の利便性向上や企業価値の最大化を目指した結果、情報システムにおいて年々外部委託への依存度が高まっている現状にある。金融機関等は、外部委託に関する管理責任や説明責任を、より一層求められるものと考える。

外部委託全般における管理プロセスには、次のものが考えられる。これらのプロセスは、基本形である２者間構成のみでなく、後述の派生形となる３者間構成においても、共通で適用されるべきものである。これらのプロセスにおける決定は、委託業務の重要性等を考慮し、経営層等が実施することが望ましい（[図 13] を参照）。

a. 情報システムの外部委託に関する方針の決定
b. 個別情報システムの外部委託の決定
c. 個別情報システムの外部委託におけるリスク管理の枠組みの決定
d. 各枠組みにおける安全対策の実施
e. 外部委託におけるリスク管理に係る改善事項の決定



［図 13］外部委託の管理プロセスにおける IT ガバナンス

コメント [FISC71]: No.62
図については、分かりやすさの観点から修正する。

② 通則（基本形・派生形共通）

金融機関等は、委託先の選定から契約終了まで、その管理責任を有する。これには再委託を含む業務委託の全体を把握することが必要である。また、再委託先の統制の責任は一義的には委託先にあることから、金融機関等の再委託に関する主な責任は、委託先が再委託先を適切に管理しているかどうかをチェックすることにある。

外部委託における共通の管理項目は次のものが考えられる。

・委託先の選定要件の策定と事前審査の実施
・委託先への監査権の明記
・有事対応

上記について、外部委託管理における考え方を解説する。

a. 委託先の選定要件の策定と事前審査の実施

金融機関等は、委託先の選定に当たって、専門性（例えば資格保有状況等）や信頼性（例えば過去に問題を起こしたことが無いか等）等とともに、委託業務の内容に応じて必要となる相互牽制等の内部的なリスク管理態勢を整備する能力の有無を考慮することが必要である。なお、そうした管理態勢の整備が困難な委託先であっても、専門性等の理由により、委託せざるをえない場合には、勤務場所を管理可能な場所に限定するといった条件を付すことが考えられる。これは再委託先に対する確認の場合も同様であるが、再委託の場合は、委託先がそれら再委託先への評価を適切に実施しているかを金融機関等が確認することとなる。再委託先との接点が限られる場合、委託先への確認を通じて、再委託先を評価することとなるため、例えば情報セキュリティに関する管理状況など、その評価はリスク特性等に応じて、適切に実施する必要がある。ただし、委託先の再委託先に対する審査・管理プロセスが金融機関等のそれと同等か、それ以上実効的であるとみなされる場合には、金融機関等が、あらかじめ委託先の審査・管理プロセスの整備・運用状況の適切性を検証することで、個別の再委託先の事前審査に代替させることが可能である。

b. 委託先への監査権の明記

金融機関等は、契約期間中において、委託先及び再委託先における業務遂行状況のみならず、セキュリティ管理状況等を確認する必要がある。このため、委託先との契約締結時には、委託先のみならず再委託先への監査権に関する条項を盛り込むことが必要であり、これらは委託業務の内容等に応じて、金融機関等が適切に判断することが必要である。

監査人の選定に当たっては、FISC『金融機関等のシステム監査指針（改訂第３版追補）』で定められた監査人の選定要件と整合的であることが必要である。

c. 有事対応

システムの運用等を委託する場合、再委託先も含めた委託先におけるコンティンジェンシープランは、個別金融機関等のものと完全に整合し、相互補完的な内容とすることが必要である。また、金融機関等は、平時は、委託先及び再委託先と共同で、定期的に訓練を実施することも重要である。

委託先や再委託先は、システム障害等が発生し、金融インフラ全体に深刻な影響を与える可能性があることを認識した場合には、その状況を即時に金融機関等に報告し、金融機関等のコンティンジェンシープランの発動に係る意思決定を支援することが期待さ

れる。

③ 基本形（２者間構成）における各論

以下は、外部の統制における２者間構成の代表的な形態におけるリスク管理策の考え方である。

a. オンプレミス

金融機関等が情報システムを自社で保有し、自社の施設においてシステムの開発や運用、サービスの一部または全部を、外部の企業などに委託する外部委託の形態である。外部の高度な専門能力やノウハウ、技術などを有効に活用し、コスト削減や業務の効率化を図ることが主な目的となるが、情報セキュリティに対する態勢を確認するなど、適切な委託先の選定、契約、管理が求められる。

b. 共同センター

共同センターは、外部委託の一形態として、複数の金融機関等が共同で委託している。多くの金融機関等が、勘定系システム等を中心に共同化を進めている状況にある。

共同センターにおいては、主に勘定系システムなど、高い安全対策が求められるシステムを運用しており、有事における初動対応は極めて重要なものとなる。このため、共同センター固有のリスクとして、有事の際、利用者間における意思決定に時間がかかることで、対応の遅れが発生しうるリスク（時間性の問題）を認識しておくことが重要である。そのうえで、利用金融機関等の経営層は、委託先及び他の利用金融機関等との間で、有事を踏まえた対応態勢を整備しておくことが求められる。

コメント [FISC72]: No.63

削除: 可用性

c. クラウドサービス

クラウドサービスは、外部委託の一形態として位置付けられ、いくつかの利用形態[22]が存在する。クラウドサービスの特徴として、複数の事業者が単一のクラウド事業者に委託する場合に、利用者間で何らコミュニケーションが無いという「匿名の共同性」や、情報処理拠点が複数の国や地域にまたがる「情報処理の広域性」、そして仮想化技術や、データの秘匿性等における「技術の先進性」などが挙げられる。

クラウドサービスにおいて、安全対策を決定する役割がクラウド事業者に帰属する場合は、クラウド事業者が金融機関等からの個別監査要求や改善要望に応えられない可能性があるため、金融機関等においては、クラウド事業者との責任分界点を理解したうえで、必要な統制が行えるかどうかを確認することが重要となる。

コメント [FISC73]: No64

削除: SLA 等を締結するなど、

④ 派生形（３者間構成）における通則

FinTech 企業等は、IT ベンダーと類似の技術的な性質を有するとともに、金融関連サー

コメント [FISC74]: No.68

削除: 決済代行業者等

22 一般的にクラウドサービスには、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）、SaaS（Software as a Service）等があり、利用者のニーズによりサービス内容を選択する。各形態ごとに提供されるサービスや利用上の制約が異なる。

ビスといったビジネスモデルの企画実施等を行う業務的な性質もあわせて有しており、こうした技術的な性質と業務的な性質を同時に有する関係者を含めた、金融機関、IT ベンダー、FinTech 企業等を加えた３者構成の場合には、安全対策上、２者間構成である基本形とは異なる点に留意する必要がある。金融機関等の経営層は、イノベーションの発揮によって得られるメリットと、リスク管理上の考慮事項を比較衡量のうえ、外部への統制を適切に実施することが求められる。

a. 同等性の原則

安全対策基準の対象となる金融情報システムについて、その安全対策の在り方を検討するに当たっては、金融機関と IT ベンダーに FinTech 企業等を加えた３者間構成を前提することとなるが、顧客の立場に立てば、安全対策上の関係者が変わろうと、安全対策の効果が同程度で確保されることが期待されていると考えられる。

したがって、FinTech 企業等という新たな関係者が登場する場合であっても、その安全対策の効果は、従来の安全対策基準において実現される２者間構成における効果と比較して、同程度（同等）となるよう留意することが重要である。

b. 再配分ルール

金融機関等は、FinTech 企業等の安全対策遂行能力を確認したうえで、仮に FinTech 企業等の能力を超える過大な責務があれば、その部分については、金融機関や IT ベンダーが分担することで、FinTech 企業等の革新性を損なわずに安全対策の効果を達成できるよう、３者間にて責務の再配分を行なうことが可能である。すなわち、２者間構成を念頭に置いた従来の安全対策基準において求められる責務の水準を維持しつつ、その責務を、３者の各類型における役割や、３者の安全対策遂行能力（保有する経営資源等）に応じて、合理的に再配分することができる。

c. リスク特性に合う管理策の適用

金融機関等の FinTech 企業等と接続する金融情報システムが、特定システムをはじめとする重要なシステムと連動する場合においても、それ自体一つのシステムとして完結性を有し、さらにそのリスク特性が金融機関等の特定システムのリスク特性と顕著に異なり、リスク事象を特定システム本体に波及させないことが可能な場合は、当該システムを通常システムとして扱うことが可能である。

⑤ 派生形（３者間構成）における各論

以下は、外部の統制における３者間構成の代表的な形態におけるリスク管理策の考え方である。

a. タイプＡ（金融機関等が安全対策の決定を主導するケース）

タイプＡは、FinTech 企業等が、金融機関等の委託先となる形態である（IT ベンダーが金融機関等の委託先となり、FinTech 企業等が再委託先となる場合を含む）。

コメント [FISC75]: No.68

削除: 決済代行業者等

削除: 決済代行業等に関する

コメント [FISC76]: No.68

削除: 決済代行業者等

コメント [FISC77]: No.68

削除: 決済代行業者等

コメント [FISC78]: No.68

削除: 望ましい

削除: この問題を解決するには、

コメント [FISC79]: No.77（追加）

削除: との整合性

コメント [FISC80]: No.68

削除: 決済代行業者等の

コメント [FISC81]: No.65
３者間構成について、分かりやすさの観点から図表等を用いるか検討する。

金融機関等は、FinTech 企業等の安全対策遂行能力を確認し、IT ベンダー及び FinTech 企業等と合意の上、安全対策に係る責務を、３者間で再配分することが可能である（「再配分ルール」）。責務の再配分に当たっては、「同等性の原則」にしたがって、関係者の負担が必要以上に増加しないよう留意する。

なお、FinTech 企業等が金融機関等の子会社となる形態も、タイプＡに含まれる。この場合、子会社に対する責任が金融機関等に付加される点を除いては、タイプＡのそれ以外の形態と安全対策上の差異はなく、金融機関等は、同等性の原則及び責務の再配分ルールを踏まえた統制を行うことが必要となる。

b. タイプＢ（金融機関等が安全対策の決定において部分的に責務を負うケース）

タイプＢは、FinTech 企業等が、金融関連サービスを主導して提供するケースである。金融機関等の安全対策上の責務が部分的となる点が、基本形またはタイプＡとは異なる。

例えば、FinTech 企業等が、顧客からの依頼に基づき預金取扱金融機関の勘定系システムに入出金の指示を行う場合、原則として、FinTech 企業等が、当該サービスに用いるシステムの安全対策を担うこととなる。この場合、金融機関等の責務は、本人確認及び FinTech 企業における顧客に関するデータの保全に係る部分に限定される。金融機関等は、当該責務を果たすため、基礎基準で示した安全対策を準用することが可能であり、FinTech 企業等が運用するシステムに対し、本人確認手続きや顧客に関するデータの保全を求めることとなる。

タイプＢにおいても、同等性の原則、責務の再配分などを踏まえた安全対策を行うことが必要となる。

コメント [FISC82]: No.68

コメント [FISC83]: 事務局
FinTech 報告書と整合性を保つよう、全体を見直した。

コメント [FISC84]: No.68

コメント [FISC85]: No.72
本人確認に関しては現在検討中の内容であり、動向を見定めたうえで、改めて記載方法を検討する。

コメント [FISC86]: No66,.67,.68
FinTech 報告書と整合性を保つよう、全体を見直した。

【資料２－１】
平成 29 年 7 月 11 日
公益財団法人 金融情報システムセンター

基礎基準に関する検討について

Ⅰ 「基礎基準」の考え方

金融機関等がリスクベースアプローチの考え方に基づき、リスク特性に応じた安全対策の目標を設定するにあたり、不確実性を低減させることを目的に、「基礎基準」を設定する。

「基礎基準」は、特定システム、通常システムによらず、金融情報システムにおける最低限適用する基準として設定する。もっとも安全対策基準の中には、特定のシステムや業務（外部接続管理や渉外端末の管理に関する基準等）のみを対象とした基準が含まれており、これらは最低限の基準であっても、システムによっては適用除外となる。

<table>
<tr><th></th><th>基礎基準</th><th>付加基準</th></tr>
<tr><td>特定システム</td><td rowspan="2">原則として適用</td><td>原則として適用</td></tr>
<tr><td>通常システム</td><td>リスク特性に応じて選択追加可</td></tr>
</table>

Ⅱ 「基礎基準」の選定について

１． 「基礎基準」の選定にあたっての考え方

○ 統制・監査に関する基準

全てのシステムにおいて安全対策を決定、実施していくためには、セキュリティポリシーや、外部委託に関する方針等が整備され、必要な人員が確保・教育されるなど、IT ガバナンスに基づく統制・監査が適切に発揮されていることが必要であるため。

○ 顧客データの漏えい防止に関する基準

一般に金融情報システムは、商品・サービスを顧客に提供するために、顧客データを保有または、顧客データに接続していると想定されるため。

○ コンティンジェンシープラン策定に関する基準

リスクベースアプローチの考えでは、安全対策の設定において、必ずしもリスクゼロを追求しないことから、金融機関等においては残存リスクへの対応のために、コンティンジェンシープランを策定する必要があるため。

２． 「基礎基準」の選定方法

○ 『金融機関等コンピュータシステムの安全対策基準・解説書』における「基準小項目」単位で選定した。

○ 「基準小項目」※、「適用にあたっての考え方」※及び「基準項目の目的、内容説明、具体例等の解説」※において「統制・監査」、「顧客データ漏えい防止」、「コンティンジェンシープラン策定」に関連する基準を「基礎基準」として選定した。

※【資料２－２】「基準本文の記述様式（例)」

３． 選定した「基礎基準」

【資料２－３】「『基準一覧』（基礎基準案)」及び【参考資料】「基準本文（統制・実務・監査)」を参照。

Ⅲ 今後の検討について

１． 検討の進め方

本日ご説明した「（１）『基礎基準』の選定にあたっての考え方」、「（２）『基礎基準』の選定方法」及び、それを踏まえた「（３）選定した『基礎基準』」について、本日の委員会後ご意見等をいただき、次回以降の専門委員会で検討してまいりたいと考えております。

２． 本検討のスケジュール

日程（予定）	内容
7 月 20 日（木）	意見の締切※1
8 月 8 日（火）	第 55 回安全対策専門委員会審議※2
8 月 22 日（火）	第 55 回安全対策専門委員会事後意見の締切
9 月 12 日（火）	第 56 回安全対策専門委員会審議※2
9 月下旬	第 56 回専門委員会事後意見の締切
10 月 17 日（火）	第 57 回安全対策専門委員会審議※2

※1 意見等は、第 57 回安全対策専門委員会まで随時受付けます。

※2 他の案件と併せて行う予定です。

以上

【資料２－２】
平成 29 年 7 月 11 日
公益財団法人　金融情報システムセンター

基準本文の記述様式（例）

基準大項目	内部の統制
基準中項目	方針・規定

適　用　区　分				
共	セ	本	提	ダ
◎				

基準小項目	統１	セキュリティ管理方法を具体的に定めた文書を整備すること。

適用にあたっての考え方

セキュリティ管理を適切に行うため、セキュリティ管理の具体的手順、責任等を明確にした文書を整備すること。

基準項目の目的、内容説明、具体例等の解説

1. セキュリティ管理を適切に行うためには、会社（もしくは組織）の情報資産を適切に保護するための基本方針である「セキュリティポリシー（基本方針）」と、これを実行に移すための具体的対策を記述した「セキュリティスタンダード（自社の安全対策基準）」及び「マニュアル」や「手順書」等のセキュリティ関連文書を整備することが必要である。セキュリティ関連文書は以下のように分類される。
   (1) セキュリティポリシー（基本方針）
   全社統一の基本方針として、保護されるべき情報資産、保護する理由と責任の所在を定めたもの。
   (2) セキュリティスタンダード（自社の安全対策基準）
   セキュリティポリシー（基本方針）を実行に移すための具体的な対策であり、社内部門別に作成してもよい。
   (3) マニュアルや手順書
   セキュリティポリシー（基本方針）及びセキュリティスタンダード（自社の安全対策基準）を具体的な業務の手順に反映したものであり、社内部門別や個々のシステム別のものであってもかまわない。

   なお、全社（もしくは全組織）のセキュリティ管理の方針や対策に重大な影響を与えるセキュリティ関連文書の策定にあたっては、経営層が指示し、承認すること。

2. セキュリティ関連文書は、全役職員（外部要員を含む）に対して、組織内における安全対策に関する役割と責任に応じて適切に周知、教育する必要がある。セキュリティ教育については【運 80】を参照のこと。

3. セキュリティポリシーの文書に定めるべき事項は主に以下の 3 点である。
   (1) 保護されるべき情報資産
   (2) 保護を行うべき理由
   (3) 保護にあたっての責任の所在

【資料２－３】
平成29年7月11日
公益財団法人　金融情報システムセンター

基準一覧（基礎基準案）

構成	基準大項目	基準中項目	新基準番号（暫定）	基準小項目	基礎基準			旧基準番号
					統制・監査	顧客データ漏洩防止	コンティンジェンシープラン	
Ⅰ　統制基準	1　内部の統制	(1) 方針・規定	統1	セキュリティ管理方法を具体的に定めた文書を整備すること。	○			運1
			統2	セキュリティ管理方法を具体的に定めた文書の評価と改訂を行うこと。	○			運2
			統3	システム開発計画は中長期計画との整合性を確認するとともに、承認を得ること。	○			技7
			統4	各種規定を整備すること。	○			運10
			統5	セキュリティ遵守状況を確認すること。	○			運10-1
		(2) 組織体制	統6	セキュリティ管理体制を整備すること。	○			運3
			統7	システム管理体制を整備すること。	○			運4
			統8	データ管理体制を整備すること。	○			運5
			統9	ネットワーク管理体制を整備すること。	○			運6
			統10	防災組織を整備すること。	○			運7
			統11	防犯組織を整備すること。	○			運8
			統12	業務組織を整備すること。	○			運9
		(3) サイバー攻撃対応態勢	統13	サイバー攻撃対応態勢を整備すること。	○			運113
		(4) 人材（要員・教育）	統14	セキュリティ教育を行うこと。	○			運80
			統15	要員に対するスキルアップ教育を行うこと。	○			運81
			統16	オペレーション習熟のための教育および訓練を行うこと。	○			運82
			統17	障害時・災害時に備えた教育・訓練を行うこと。	○			運83
			統18	防災・防犯訓練を行うこと。	○			運84
			統19	要員の人事管理を適切に行うこと。	○			運85
			統20	要員の健康管理を行うこと。	○			運86
	2　外部の統制	(1) 方針・計画	外部委託検討の中で整理する。	システムの開発や運用、サービス利用等で外部委託を行う場合は、事前に目的や範囲を明確にすること。				外部委託関連基準として再編の予定
				外部委託先の選定手続きを明確にすること。				
		(2) 契約・業務管理		安全対策に関する項目を盛り込んだ委託契約を締結すること。				
				外部委託先（再委託先を含む）の要員にルールを遵守させ、その遵守状況を管理、検証すること。				
				外部委託にあたって、データ漏洩防止策を講ずること。				
				外部委託における業務組織の整備と業務の管理、検証を行うこと。				
				外部委託契約終了時の情報漏洩防止策を講ずること。				
		(3) 金融機関相互のシステム・ネットワークのサービス	統28	金融機関相互のシステム・ネットワークのサービス利用にあたっては、適切なリスク管理を行うこと。	○			運90-1
Ⅱ　実務基準	1　入退管理	(1) 入退館（室）管理	実1	資格付与および鍵の管理を行うこと。		○		運11
			実2	入退館管理を行うこと。		○		運12
			実3	入退室管理を行うこと。		○		運13
	2　運用管理	(1) マニュアルの整備	実4	通常時マニュアルを整備すること。				運14
			実5	障害時・災害時マニュアルを整備すること。			○	運15
		(2) アクセス権限の管理	実6	各種資源、システムへのアクセス権限を明確にすること。		○		運16
			実7	パスワードが他人に知られないための措置を講じておくこと。		○		運17
			実8	各種資源、システムへのアクセス権限の付与、見直し手続きを明確化すること。		○		運18
		(3) オペレーション管理	実9	オペレータの資格確認を行うこと。		○		運19
			実10	オペレーションの依頼・承認手続きを明確にすること。				運20
			実11	オペレーション実行体制を明確にすること。				運21
			実12	オペレーションの記録、確認を行うこと。				運22
			実13	クライアントサーバー・システムにおける作業の管理を行うこと。				運23
		(4) 入力管理	実14	データの入力管理を行うこと。				運24
		(5) データファイル管理	実15	授受・管理方法を定めること。		○		運25
			実16	修正管理方法を明確にすること。				運26
			実17	バックアップを確保すること。			○	運27
		(6) プログラムファイル管理	実18	管理方法を明確にすること。				運28
			実19	バックアップを確保すること。			○	運29
		(7) コンピュータウイルス対策	実20	コンピュータウイルス対策を講ずること。		○		運30
		(8) ネットワーク設定情報管理	実21	設定情報の管理を行うこと。				運31
			実22	設定情報のバックアップを確保すること。			○	運32
		(9) ドキュメント管理	実23	保管管理方法を明確にすること。				運33
			実24	バックアップを確保すること。			○	運34
		(10) 帳票管理	実25	未使用重要帳票の管理方法を明確にすること。				運35
			実26	重要な印字済帳票の取扱方法を明確にすること。		○		運36
		(11) 出力管理	実27	出力情報の作成、取扱いについて、不正防止および機密保護対策を講ずること。		○		運37
		(12) 取引の管理	実28	各取引の操作権限を明確にすること。				運38
			実29	オペレータカードの管理を行うこと。				運39
			実30	取引の操作内容を記録・検証すること。				運40
			実31	顧客からの届出の受付体制を整備し、事故口座の管理を行うこと。				運41
			実32	機器および媒体の盗難、破損等に伴い、利用者が被る可能性がある損失および責任を明示すること。				運42
		(13) 暗号鍵の管理	実33	暗号鍵の利用において運用管理方法を明確にすること。		○		運43
		(14) 厳正な本人確認の実施	実34	本人確認を行うこと。				運44
			実35	CD・ATM等の機械式預貯金取引における正当な権限者の取引を確保すること。				運44-1
		(15) CD・ATM等及び無人店舗の管理	実36	運用管理方法を明確にし、かつ不正払戻防止の措置を講ずること。				運45
			実37	監視体制を明確にすること。				運46
			実38	防犯体制を明確にすること。				運47
			実39	障害時・災害時の対応方法を明確にすること。				運48
			実40	関係マニュアルの整備を行うこと。				運49
		(16) 渉外端末の管理	実41	運用管理方法を明確にすること。		○		運50
		(17) カード管理	実42	カードの管理方法を明確にすること。		○		運51
			実43	顧客に対して犯罪に関する注意喚起を行うこと。				運51-1
			実44	指定された口座のカード取引監視方法を明確にすること。				運52
		(18) 顧客データ保護	実45	顧客データの保護策を講ずること。		○		運53
			実46	生体認証における生体認証情報の安全管理措置を講ずること。		○		運53-1
		(19) 資源管理	実47	能力及び使用状況の確認を行うこと。				運54
		(20) 外部接続管理	実48	接続契約内容を明確にすること。		○		運55
			実49	外部接続における運用管理方法を明確にすること。		○		運56
		(21) 機器の管理	実50	管理方法を明確にすること。		○		運57
			実51	ネットワーク関連機器の保護措置を講ずること。				運58
			実52	保守方法を明確にすること。				運59
		(22) 運行監視	実53	監視体制を整備すること。		○		運60
		(23) コンピュータ室・データ保管室の管理	実54	入室後の作業を管理すること。		○		運61
		(24) 障害時・災害時対応策	実55	関係者への連絡手順を明確にすること。			○	運62
			実56	障害時・災害時復旧手順を明確にすること。			○	運63
			実57	障害の原因を調査・分析すること。				運64
		(25) コンティンジェンシープランの策定	実58	コンティンジェンシープランを策定すること。			○	運65

基準一覧（基礎基準案）

構成	基準大項目	基準中項目	新基準番号（暫定）	基準小項目	基礎基準			旧基準番号
					統制・監査	顧客データ漏洩防止	コンティンジェンシープラン	
	3 システム開発・変更	(1) ハードウェア・ソフトウェア管理	実59	ハードウェア、ソフトウェアの管理を行うこと。				運66
		(2) システム開発・変更管理	実60	開発・変更手順を明確にすること。				運67
			実61	テスト環境を整備すること。		○		運68
			実62	本番への移行手順を明確にすること。				運69
		(3) ドキュメント管理	実63	作成手順を定めること。				運70
			実64	保管管理方法を明確にすること。				運71
		(4) パッケージの導入	実65	評価体制を整備すること。				運72
			実66	運用・管理体制を明確にすること。				運73
		(5) システムの廃棄	実67	廃棄計画、手順を策定すること。		○		運74
			実68	情報漏洩防止対策を講ずること。		○		運75
	4 各種設備管理	(1) 保守管理	実69	管理方法を明確にすること。				運76
			実70	保守方法を明確にすること。				運77
		(2) 資源管理	実71	能力および使用状況の確認を行うこと。				運78
		(3) 監視	実72	監視体制を整備すること。				運79
	5 インストアブランチ	(1) インストアブランチ	実73	出店先の選定基準を明確にすること。				運92
	6 コンビニATM	(1) コンビニATM	実74	出店先の選定基準を明確にすること。				運93
			実75	現金装填等メンテナンス時の防犯対策を講じること。				運94
			実76	障害時・災害時対応手順を明確にすること。				運95
			実77	ネットワーク関連機器、伝送データの安全対策を講ずること。				運96
			実78	所轄の警察および警備会社等関係者との連絡体制を確立すること。				運97
			実79	顧客に対して犯罪に関する注意喚起を行うこと。				運98
	7 デビットカード	(1) デビットカード・サービスの安全性確保	実80	デビットカード・サービスにおける安全対策を講ずること。				運99
			実81	口座番号、暗証番号等の安全性を確保すること。				運100
		(2) 顧客保護	実82	デビットカード利用時の顧客保護の措置を講ずること。				運101
		(3) 顧客への注意喚起	実83	デビットカード利用上の留意事項を顧客に注意喚起すること。				運102
	8 オープンネットワークを利用した金融サービス	(1) インターネット、モバイル	実84	不正使用を防止すること。		○		運103
			実85	不正使用を早期発見すること。		○		運104
			実86	安全対策に関する情報開示をすること。				運105
			実87	顧客対応方法を明確にすること。				運105-1
			実88	インターネットやモバイル等を用いた金融サービスの運用管理方法を明確化すること。				運106
		(2) 電子メール	実89	電子メールの運用方針を明確にすること。				運107
	9 共同センター	(1) 共同センター	外部委託検討の中で整理する。	共同センターにおける有事対応方針を明確にすること。				新設予定
	10 FinTech・クラウド関連	(1) FinTech・クラウド関連		（現時点では勘定系クラウドとオープンAPIが入る想定）				
	11 ハードウェアの信頼性向上対策	(1) ハードウェアの障害予防策	実92	予防保守を実施すること。				技1
		(2) ハードウェアの予備	実93	本体装置の予備を設けること。				技2
			実94	周辺装置の予備を設けること。				技3
			実95	通信系装置の予備を設けること。				技4
			実96	回線の予備を設けること。				技5
			実97	端末系装置の予備を設けること。				技6
	12 ソフトウェアの信頼性向上対策	(1) 開発時の品質向上対策	実98	必要となるセキュリティ機能を取り込むこと。				技8
			実99	設計段階でのソフトウェアの品質を確保すること。				技9
			実100	プログラム作成段階での品質を確保すること。				技10
			実101	テスト段階でのソフトウェアの品質を確保すること。				技11
			実102	プログラムの配布を考慮したソフトウェアの信頼性を確保すること。				技12
			実103	パッケージ導入にあたり、ソフトウェアの品質を確保すること。				技13
		(2) メンテナンス時の品質向上対策	実104	定型的変更作業時の正確性を確保すること。				技14
			実105	機能の変更、追加作業時の品質を確保すること。				技15
	13 運用時の信頼性向上対策	(1) 運用時の信頼性向上対策	実106	オペレーションの自動化、簡略化を図ること。				技16
			実107	オペレーションのチェック機能を充実すること。				技17
			実108	負荷状態の監視制御機能を充実すること。				技18
			実109	CD・ATM等の遠隔制御機能を設けること。				技19
	14 障害の早期発見・早期回復	(1) 障害の早期発見	実110	システム運用状況の監視機能を設けること。				技20
			実111	障害の検出および障害箇所の切り分け機能を設けること。				技21
		(2) 障害の早期回復	実112	障害時の縮退・再構成機能を設けること。				技22
			実113	取引制限機能を設けること。				技23
			実114	リカバリ機能を設けること。				技24
	15 災害時対策	(1) バックアップサイト	実115	バックアップサイトを保有すること。				技25
	16 データ保護	(1) 漏洩防止	実116	暗証番号・パスワード等は他人に知られないための対策を講ずること。		○		技26
			実117	相手端末確認機能を設けること。		○		技27
			実118	蓄積データの漏洩防止策を講ずること。		○		技28
			実119	伝送データの漏洩防止策を講ずること。		○		技29
		(2) 破壊・改ざん防止	実120	ファイルに対する排他制御機能を設けること。				技30
			実121	ファイルに対するアクセス制御機能を設けること。		○		技31
			実122	不良データ検出機能を充実すること。				技32
		(3) 検知策	実123	伝送データの改ざん検知策を講ずること。				技33
			実124	ファイル突合機能を設けること。				技34
	17 不正使用防止	(1) 予防策(アクセス権限確認)	実125	本人確認機能を設けること。		○		技35
			実126	生体認証の特性を考慮し、必要な安全対策を検討すること。		○		技35-1
			実127	IDの不正使用防止機能を設けること。		○		技36
			実128	アクセス履歴を管理すること。		○		技37
		(2) 予防策(利用範囲の制限)	実129	取引制限機能を設けること。				技38
			実130	事故時の取引禁止機能を設けること。				技39
		(3) 予防策(不正・偽造防止対策)	実131	カードの偽造防止対策のための技術的措置を講ずること。				技40
			実132	電子的価値の保護機能、または不正検知の仕組みを設けること。				技41
			実133	電子化された暗号鍵を蓄積する機器、媒体、またはそこに含まれるソフトウェアには、暗号鍵の保護機能を設けること。				技42
			実134	電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること。				技42-1
		(4) 外部ネットワークからのアクセス制限	実135	外部ネットワークからの不正侵入防止機能を設けること。		○		技43
			実136	外部ネットワークからアクセス可能な接続機器は必要最小限にすること。		○		技44
		(5) 検知策	実137	不正アクセスの監視機能を設けること。		○		技45
			実138	異常な取引状況を把握するための機能を設けること。				技46
			実139	異例取引の監視機能を設けること。				技47
		(6) 対応策	実140	不正アクセスの発生に備えて対応策、復旧策を講じておくこと。		○		技48
	18 不正プログラム防止	(1) 防御策	実141	コンピュータウイルス等不正プログラムへの防御対策を講ずること。		○		技49
		(2) 検知策	実142	コンピュータウイルス等不正プログラムの検知対策を講ずること。		○		技50
		(3) 復旧策	実143	コンピュータウイルス等不正プログラムによる被害時対策を講ずること。			○	技51
Ⅲ 設備基準								
Ⅳ 監査基準	1 システム監査	(1) システム監査	監1	システム監査体制を整備すること。	○			運91

【資料３－１】
平成29年7月11日
公益財団法人 金融情報システムセンター

平成29年度第54回安全対策専門委員会
検討事項に関するご意見（メール回答用）

電子メールにて、ご連絡願います。（fisc40@fisc.or.jp）

〆切　7/20(木)（改訂原案（前説）／基礎基準に関するご意見）

会社名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

お名前：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

資料番号	項番 （基準番号）	ご意見
（例） 資料２－１	（例） Ⅱ．１． （２）	・・・

内部の統制	適　用　区　分				
方針・規定	共	セ	本	提	ダ
	◎				

統 1	セキュリティ管理方法を具体的に定めた文書を整備すること。

セキュリティ管理を適切に行うため、セキュリティ管理の具体的手順、責任等を明確にした文書を整備すること。

1. セキュリティ管理を適切に行うためには、会社（もしくは組織）の情報資産を適切に保護するための基本方針である「セキュリティポリシー（基本方針）」と、これを実行に移すための具体的対策を記述した「セキュリティスタンダード（自社の安全対策基準）」及び「マニュアル」や「手順書」等のセキュリティ関連文書を整備することが必要である。セキュリティ関連文書は以下のように分類される。
   (1) セキュリティポリシー（基本方針）
   全社統一の基本方針として、保護されるべき情報資産、保護する理由と責任の所在を定めたもの。
   (2) セキュリティスタンダード（自社の安全対策基準）
   セキュリティポリシー（基本方針）を実行に移すための具体的な対策であり、社内部門別に作成してもよい。
   (3) マニュアルや手順書
   セキュリティポリシー（基本方針）及びセキュリティスタンダード（自社の安全対策基準）を具体的な業務の手順に反映したものであり、社内部門別や個々のシステム別のものであってもかまわない。

   なお、全社（もしくは全組織）のセキュリティ管理の方針や対策に重大な影響を与えるセキュリティ関連文書の策定にあたっては、経営層が指示し、承認すること。

2. セキュリティ関連文書は、全役職員（外部要員を含む）に対して、組織内における安全対策に関する役割と責任に応じて適切に周知、教育する必要がある。セキュリティ教育については【運 80】を参照のこと。

3. セキュリティポリシーの文書に定めるべき事項は主に以下の 3 点である。
   (1) 保護されるべき情報資産
   (2) 保護を行うべき理由
   (3) 保護にあたっての責任の所在

削除: 管理体制の確立

削除: セキュリティ管理と責任の明確化

削除: 運　1

4.　セキュリティ関連文書の整備を行ううえでの留意事項として、以下のようなものがある。

(1) セキュリティ管理の実施計画策定は、コンピュータシステムで扱う情報の重要性を判断して、コンピュータシステムが提供しているサービスの優先順位を決定することから始まる。このためには取り扱っている情報をすべて洗い出し、会社（もしくは組織）として情報を保護するレベルを決定することが必要である。

　重要な情報資産についてはセキュリティポリシーに則って、機密性、完全性、可用性の観点から、その重要性に応じた適切な保護、管理を行うことが必要である。

　また、セキュリティを確保するための手段として保険の適用を検討することが望ましい。

(2) 機器及びソフトウェアを導入あるいは更新する場合には、セキュリティ機能がセキュリティポリシーに適合していることを確認することが必要である。

(3) セキュリティを確保するためには、システムを計画する段階からセキュリティ対策を考慮しておくことが必要である。

　システム計画時のセキュリティ対策の考慮については、以下の基準項目を参照のこと。

　・必要となるセキュリティ機能を取り込むこと【技 8】

(4) セキュリティ管理を適切に行うにあたって、セキュリティに関する法令等も考慮する必要がある。

(5) セキュリティポリシーを策定する際は、社内各部門の意見・状況を把握し、適切に反映することが望ましい。

(6) 情報システムの外部委託に関しては、企業価値の最大化や健全性の確保を踏まえて、外部委託を選択するに当たっての考え方（利用目的等）、例えば、外部委託が可能となる業務、リスク管理の枠組み、更に、再委託が可能となる業務、業務に応じた再委託の階層や数の制限等を、方針として明確に定める必要がある。

（注）・機密性（Confidentiality）　…… アクセスを許されていない者から守ること
　　・完全性（Integrity）　…… 改ざん等されないように完全な形態で保持すること
　　・可用性（Availability）　…… いつでも利用できるように保持すること

5.　セキュリティポリシーを策定するにあたっては、当センター発刊の『金融機関等におけるセキュリティポリシー策定のための手引書』等を参照のこと。

内部の統制	適　用　区　分				
方針・規定	共	セ	本	提	ダ
	◎				

統 2	セキュリティ管理方法を具体的に定めた文書の評価と改訂を行うこと。

セキュリティ管理の方法を最適なものとするため、作成された文書については、業務の実態にあっているかを定期的に評価し、必要に応じて改訂すること。

1. セキュリティ管理を適切に行うためには、管理や運用方法などを具体的に定めたセキュリティ関連文書が業務の実態にあっていなければならない。この文書の見直しのきっかけには以下のようなものがあり、これらに応じて改訂する必要がある。

   なお、全社（もしくは全組織）のセキュリティ管理の方針や対策に重大な影響を与えるセキュリティ文書の改訂にあたっては、経営層の承認を得ること。

   ・組織の運営の変化
   ・ビジネス環境の変化
   ・法令の制定、改正
   ・情報・通信技術の進歩
   ・業務組織や人員・就業場所の変化
   ・扱う情報資産に関する変化
   ・セキュリティに関する事故や犯罪
   ・セキュリティ関連文書に定められた事項の遵守状況の確認結果

   なお、共通的なものについては、主管部署等で改訂したものを全社に配布することで対応すればよい。

2. 対象となるのは以下のような文書であるが、場合によってはこれらの基本となっているセキュリティポリシー（基本方針）の見直しが必要なこともある。
   ・セキュリティスタンダード（自社の安全対策基準）
   ・マニュアルや手順書

3. 合併等により異なるセキュリティポリシーを持つ複数の企業がひとつの企業となる場合は、システム統合に先立ち統合金融機関の間でセキュリティポリシーの違いを認識し、見直すことが必要である。

削除: 管理体制の確立
削除: セキュリティ管理と責任の明確化
削除: 運　2
削除: ィ

内部の統制	適　用　区　分				
方針・規定	共	セ	本	提	ダ
	◎				

削除: ソフトウェアの信頼性向上対策

削除: 開発時の品質向上対策

統 3	システム開発計画は中長期計画との整合性を確認するとともに、承認を得ること。

削除: 技　7

コンピュータシステム全体の信頼性向上のため、システム開発計画は、中長期のシステム化計画と整合性が取れており、かつ内外の技術調査を実施していること、また開発責任者（システムを企画、開発する部門の長）の承認を得ていること。

1. 開発するコンピュータシステムは、関連する他のコンピュータシステムと役割を分担し、全体として機能する必要があるため、システム開発計画は中長期のシステム化計画との整合性を考慮して策定することが必要である。

2. 幅広く情報技術の適用を検討するため、開発計画を策定するにあたっては、内外の情報技術を調査することが望ましい。

   なお、開発を外部に委託する場合には、採用技術の正当性について委託先から十分な説明を受けることが必要である。

   調査のポイントとしては、以下のようなものがある。

   ・技術の特徴、適用条件
   ・将来採用可能となる技術までを含めた拡張性
   ・技術の性能評価
   ・費用対効果の評価

3. システム開発計画が中長期のシステム化計画に基づいていること、採用技術も適切なことを確認し、計画を実行に移すためには開発責任者が承認することが必要である。

削除: <オブジェクト>

削除: <オブジェクト>

内部の統制	適　用　区　分				
方針・規定	共	セ	本	提	ダ
	◎				

統 4	各種規定を整備すること。

コンピュータシステムを円滑かつ適正に運用、管理するため、防災、防犯、業務の各組織における責任と権限を明確にした規定を整備すること。

1.　ここでいう規定とは、防災、防犯、業務の各組織に関する事務分掌、職掌ならびに責任と権限を定めたものを指しており、以下の内容を含んだ各種規定を定めることが必要である。
(1) 入退管理
(2) コンピュータシステムの通常時、障害時・災害時運用
(3) コンピュータ処理に係わる業務の通常時、障害時・災害時運用
(4) データ、プログラム及びドキュメント（サーバー、パソコン、フロッピーディスク、CD-ROM等に蓄積されたものも含む）の管理
(5) カード管理
(6) システム開発・変更
(7) 電源設備、空調設備、防災設備、防犯設備の管理
(8) 防犯・警備
(9) 監視

2.　データ、プログラム及びドキュメントの管理については、顧客データや秘密鍵等の重要で機密を要するデータの取扱いに関する規定を必要に応じて定めることが必要である。

3.　規定の内容については、以下の基準項目を参照のこと。
(1) 入退管理　【運 11～13】
(2) コンピュータシステムの通常時、障害時・災害時運用
【運 14～24、運 31、運 32、運 54～65】
(3) コンピュータ処理に係わる業務の通常時、障害時・災害時運用　【運 37～50、運 53】
(4) データ、プログラム及びドキュメントの管理　【運 25～30、運 33～36】
(5) カード管理　【運 51、運 52】
(6) システム開発・変更　【運 66～75】
(7) 電源設備、空調設備、防災設備、防犯設備の管理　【運 76～78】
(8) 防犯・警備　【運 4～9】
(9) 監視　【運 79】

削除: 管理体制の確立
削除: 各種規定の整備
削除: 運　10
削除: およ
削除: およ
削除: およ

内部の統制	適　用　区　分				
方針・規定	共	セ	本	提	ダ
	◎				

統 5	セキュリティ遵守状況を確認すること。

セキュリティ関連文書に定められた事項の遵守状況を確認し、全役職員（外部要員を含む）のセキュリティポリシーに対する意識やセキュリティレベルの向上を図ること。

1. コンピュータシステムを円滑かつ適正に運用するため、セキュリティ関連文書に定められた事項の遵守状況を確認し、全役職員（外部要員を含む）のセキュリティポリシーに対する意識やセキュリティレベルの向上を図ることが必要である。

2. セキュリティ遵守状況を確認するタイミングとしては、以下のようなものがある。
   (1) 新しいシステム及びサービスの導入時
   (2) 既存のシステム及びサービスに対して定期、不定期
   (3) セキュリティ関連文書に変更があった時
   (4) 異動等により人員の配置変更があった時

3. セキュリティ遵守状況を確認する者は、建屋内の点検や職員面接等の手段により、セキュリティ対策及びセキュリティ遵守状況を把握しておくことが望ましい。

4. セキュリティ遵守状況の確認結果を評価し、セキュリティ関連文書の改訂に反映することが必要である。【運２】

5. セキュリティ遵守状況の確認結果を評価し、セキュリティ教育の内容等を見直すことが必要である。【運 80】

削除: 管理体制の確立
削除: セキュリティ遵守状況の確認
削除: 運　10-1
削除: およ
削除: およ
削除: およ

内部の統制	適　用　区　分				
組織体制	共	セ	本	提	ダ
	◎				

削除: 管理体制の確立

削除: セキュリティ管理と責任の明確化

統 6	セキュリティ管理体制を整備すること。

削除: 運　3

セキュリティ管理を適切に行うため、セキュリティ管理の責任者等を定め、その職務範囲と権限及び責任について定めること。

1.　全社のセキュリティが、定められた方針、基準、指針及び手順に従って確保されていることを、適正に管理するための体制（組織、職務範囲、権限等）を確立すること。

　また、全社的にセキュリティを統括する責任者を明確にし、統一的なセキュリティ管理を行うこと。

　上記体制の確立にあたっては経営層が指示し、承認すること。

2.　全社的にセキュリティを統括する責任者のもと、組織の規模や体制等に応じて、セキュリティ管理者を定めるなど、セキュリティ管理体制を整備することが必要である。

　なお、セキュリティ管理の体制整備及び管理者の設置にあたっては、以下の基準項目も参照のこと。

・システム管理体制（システム管理者）【運 4】
・データ管理体制（データ管理者）【運 5】
・ネットワーク管理体制（ネットワーク管理者）【運 6】

3.　セキュリティ管理者の業務としては、以下のようなものがある。

(1) システムの企画から開発、運用、保守、廃棄にわたるすべてのフェーズのセキュリティの統制、管理

(2) 重大な障害・事故・犯罪等に関するセキュリティ上の問題について、全社的にセキュリティを統括する責任者及び経営層への迅速な報告

(3) セキュリティの障害・事故・犯罪等について、情報収集、分析、評価、及びセキュリティ関連文書への反映

4.　外部委託を行う場合においても、外部委託業務におけるセキュリティ管理体制を整備することが必要である。

参照法令	不正アクセス行為の禁止等に関する法律　第２条～第５条

内部の統制	適　用　区　分				
組織体制	共	セ	本	提	ダ
	◎				

統 7	システム管理体制を整備すること。

システムの安全かつ円滑な運用と不正防止のため、システムの管理手順を定め、管理体制を整備すること。

1. システムの運用、管理及び利用承認手続き等を管理手順として定め、関係者に周知徹底させることにより、システムの安全で円滑な運用を行うことが必要である。

2. ハードウェア、ソフトウェアの維持、管理を行うとともに、システムの運用管理を行うためにシステム管理者を置くことが必要である。
　なお、システム管理者はシステム単位あるいは業務単位に設置することが望ましい。さらに、それぞれのシステム管理者の間で、相互に連携を図った体制を整えることが望ましい。

3. システム管理者の業務としては、以下のようなものがある。
(1) システムに関するセキュリティ対策の実施
(2) ハードウェア、ソフトウェアの導入、管理、保守
(3) システム構成、設定情報の管理、保守
(4) バックアップの確保
(5) システムを利用するための ID の登録
(6) システム利用状況の管理
(7) コンピュータウイルス等不正プログラムへの対応
(8) システムに関するセキュリティ違反についてのセキュリティ管理者への報告と対応
(9) 障害、事故対応
　なお、システム管理者に権限が集中することによる不正行為の発生を防ぐため、システム管理者を複数名任命して担当する業務を分けるなど、各機関の実態に合わせて権限を適切に分散し、相互牽制機能が働くようにしておくことが望ましい。

4. データ管理者やネットワーク管理者と、適切に職能が分離されていることが望ましい。

削除: 管理体制の確立

削除: セキュリティ管理と責任の明確化

削除: 運　4

内部の統制	適　用　区　分				
組織体制	共	セ	本	提	ダ
	◎				

統 8	データ管理体制を整備すること。

データの安全かつ円滑な運用と不正防止のため、データ管理手順を定め、管理体制を整備すること。

1. データの管理手順、及び利用承認手続き等を管理手順として定め、関係者に周知徹底させることにより、データの安全で円滑な運用を行うことが必要である。

2. データについて機密性、完全性、可用性の確保を行うために、データ管理者を置くことが必要である。
   なお、データ管理者はシステム単位あるいは業務単位で設置することが望ましい。

3. データ管理者の業務としては、以下のようなものがある。
   (1) データに関するセキュリティ対策の実施
   (2) データ管理手順の遵守状況の監視
   (3) データ利用に関する承認
   (4) データに関するユーザーアクセス権限の決定
   (5) データ利用状況の管理
   (6) データに関するセキュリティ違反についてのセキュリティ管理者への報告と対応
   (7) 障害、事故対応

4. システム管理者やネットワーク管理者と、適切に職能が分離されていることが望ましい。

削除: 管理体制の確立
削除: セキュリティ管理と責任の明確化
削除: 運　5
削除: およ

内部の統制	適　用　区　分				
組織体制	共	セ	本	提	ダ
	◎				

統 9	ネットワーク管理体制を整備すること。

コンピュータネットワークの適切かつ効率的な運用と不正アクセス等の防止のため、ネットワークの管理手順を定め、管理体制を整備すること。

1. ネットワークの管理手順、及び利用承認手続き等を管理手順として定め、関係者に周知徹底させることにより、ネットワークの適切かつ効率的で安全な運用を行うことが必要である。

2. ネットワーク稼働状況の管理、アクセスコントロール、及びモニタリング等を行うために、ネットワーク管理者を置くことが必要である。

3. ネットワーク管理者の業務としては、以下のようなものがある。
   (1) ネットワークに関するセキュリティ対策の実施
   (2) ネットワーク関連のハードウェア、ソフトウェアの導入、管理、保守
   (3) ネットワーク構成、設定情報の管理、保守
   (4) ネットワーク設定情報のバックアップ確保
   (5) ネットワークに関するアクセス権限の登録
   (6) ネットワークトラフィック状況の管理
   (7) アクセス状況の管理
   (8) ネットワークに関するセキュリティ違反についてのセキュリティ管理者への報告と対応
   (9) 障害、事故対応

削除: 管理体制の確立
削除: セキュリティ管理と責任の明確化
削除: 運　6
削除: およ
削除: およ

内部の統制	適　用　区　分				
組織体制	共	セ	本	提	ダ
		◎	◎		

統 10	防災組織を整備すること。

災害の予防及び被害軽減のため、防災組織を整備し、責任者を明確にすること。

削除: 管理体制の確立

削除: 組織の整備

削除: 運　7

削除: およ

1.　災害の発生を予防・予知するとともに、万一災害が発生した場合の被害を軽減するため、迅速に対応できる防災組織を整備することが必要である。特に、コンピュータセンターやコンピュータ設備等のシステム資源を保有する部門においては、それらの資源の重要性を配慮した防災組織とすることが必要である。

　なお、防災組織の実効性を高めるため、業務組織に則した組織とし、役割分担ごとに責任者を明確にすることが必要である。

　防災組織の例を図 1 に示す。

2.　コンピュータセンターにおいて共同ビルを利用している場合は、ビル全体の管理組織を踏まえ、コンピュータセンターとして独立した防災組織を整備することが必要である。

3.　防災組織を整備する際の具体的な留意点として、以下のようなものがある。

(1) 防災組織を整備し、関連部門に周知徹底する。

　防災組織に係わる責任者、分担、避難経路等を関連部門の人に周知徹底することが必要である。なお、他社の勤務者についても、必要な範囲において周知徹底することが必要である。

(2) 防災組織の形骸化を防ぐため、組織の定期的な周知徹底、及び見直しを行う。

　作成された防災組織が有効であるためには、関係者に対する当該組織図の定期的な周知徹底と定期的な見直しとが必要である。また、人事異動等により担当者が変更になった場合にも、再度組織図の周知徹底が必要である。

(3) 災害に備えて防災機関との連絡方法、想定される連絡内容を明確にする。

　ここでいう防災機関とは、消防署等の防災機関を指している。

　なお、災害時には、被害の状況を迅速、的確に連絡する必要があるので、想定される連絡内容を明確化しておくことが必要である。

(4) 災害発生時の緊急連絡網を整備する。

　災害発生時における緊急連絡網を整備し、かつ当該連絡網の有効性を定期的に点検することが必要である。また、夜間、休日の災害発生に備えて関係者等への連絡体制を明確にしておくことが必要である。

(5) 地震等の自然災害に備えて災害予報機関等からの情報収集に努める。

　災害予報機関としては、気象庁、日本気象協会等があるが、災害に関する予報、警報等はテ

レビ（衛星放送、ケーブルテレビを含む）、ラジオ等を通じて報道されるとともに、市区町村等からも、サイレン、広報車等により伝達される。

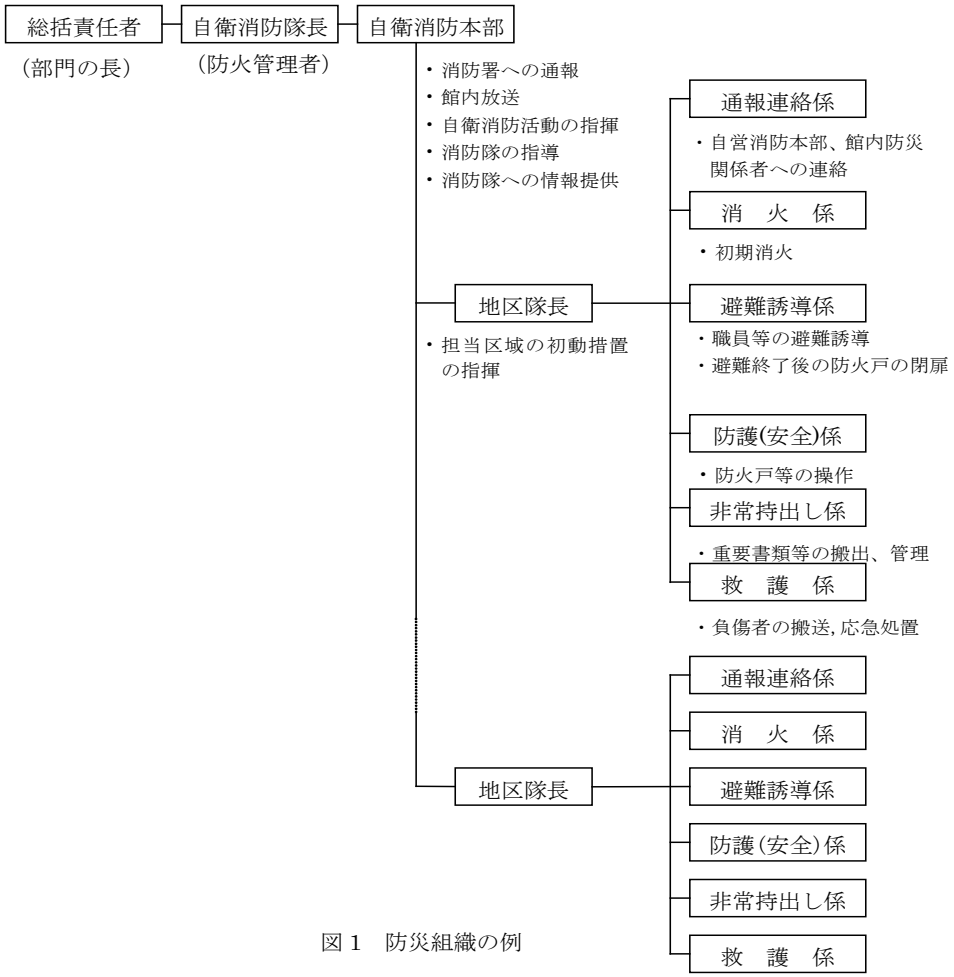


図１　防災組織の例

参照法令	消防法第８条、消防法施行規則第１条～第４条

内部の統制	適　用　区　分				
組織体制	共	セ	本	提	ダ
		◎	◎		

統 11	防犯組織を整備すること。

犯罪を防止するため、防犯組織を整備し、責任者を明確にすること。

1.　不法侵入、危険物持込み、不法持出し等コンピュータシステムの安全性を脅かす行為を防止するため、入退管理を行うとともに、警備員が巡回監視するなど、建物の内外の不審者・不審物に気を配ることが必要である。また、万一犯罪が発生した場合、被害の影響を最小限にとどめることが必要である。そのため、迅速に対応できるよう業務組織に則した防犯組織を整備し、役割分担ごとに責任者を明確にすることが必要である。

　特に、コンピュータセンターやコンピュータ設備等のシステム資源を保有する部門においては、それらの資源の重要性を考慮した防犯組織とすることが必要である。

　防犯組織の例を図１に示す。

2.　コンピュータセンターにおいて、共同ビルを利用している場合は、ビル全体の管理組織を踏まえ、コンピュータセンターとして独立した防犯組織を整備することが必要である。

3.　防犯組織を整備する際の具体的な留意点として、以下のようなものがある。

(1) 防犯組織を整備し、関連部門や店内に周知徹底する。

　防犯組織に係わる責任者、分担等を関連部門や店内の人に周知徹底することが必要である。なお、警備会社等他社の勤務者についても、必要な範囲において周知徹底することが必要である。

(2) 防犯組織の形骸化を防ぐため、組織の定期的な周知徹底を図るとともに犯罪の高度化に備え、必要に応じた当該体制の見直しを行う。

　防犯組織の形骸化を防ぐため、組織の定期的な周知徹底を図るとともに犯罪の高度化に備え、必要に応じた当該体制の見直しを行うことが必要である。特に、人事異動等により担当者が異動となった場合には、再度組織図の周知徹底が必要である。

(3) 犯罪に備えて防犯機関との連絡方法を明確にする。

　ここでいう防犯機関とは、警察署を指している。

4.　なお、防犯対策のための設備基準としては以下の項目がある。

削除: 管理体制の確立

削除: 組織の整備

削除: 運　8

(1) コンピュータセンター

内　　容	該当する項目番号
①　建物	
・看板等を外部に出さないこと。	設 6
・防犯措置を講ずること。	設 15
・常時利用する出入口は１カ所とし、出入管理設備、防犯設備を設置すること。	設 16
・出入口の扉は、十分な強度を持たせるとともに、錠を付けること。	設 19
②　コンピュータ室・データ保管室	
・外部から容易に入れない位置に設置すること。	設 23
・室名等の表示は付さないこと。	設 24
・常時利用する出入口は１カ所とし、前室を設けること。	設 27
・出入口の扉は、十分な強度を持たせるとともに、錠を付けること。	設 28
・非常時の連絡装置を設置すること。	設 38
・出入口には出入管理設備、防犯設備を設置すること。	設 45
③　電源室・空調機械室	
・無窓とし、錠を付けた扉を設置すること。	設 55
④　電源設備	
・防災、防犯設備用の予備電源を設置すること。	設 71
⑤　空調設備	
・空調設備には侵入、破壊防止対策を講ずること。	設 77
⑥　監視制御設備	
・監視制御設備を設置すること。	設 80
・中央管理室を設置すること。	設 81
⑦　回線関連設備	
・回線関連設備には錠を付けること。	設 82
・回線関連設備の設置場所の表示は付さないこと。	設 83
・回線は、専用の配線スペースに設けること。	設 83-1

(2) 本部・営業店等

内　　容	該当する項目番号
①　開口部	
・窓・扉には防犯措置を講ずること。	設 90
・通用口には、入室者の識別装置を設置すること。	設 92
②　設備	
・防犯措置を講ずること。	設 103
③　回線関連設備	
・回線関連設備の設置場所の表示は付さないこと。	設 104
・回線関連設備には錠を付けること。	設 105
④　電源設備	
・防災、防犯設備用の予備電源を設置すること。	設 108
⑤　自動機器室	
・非常通報装置を設置すること。	設 112
・防犯措置を講ずること。	設 113
・照明設備、及び非常用照明設備を設置すること。	設 114
・扉は、一部を素通しにすること。	設 115
⑥　サーバー設置場所	
・外部から容易に入れない位置に設置すること。	設 122
・室名等の表示は付さないこと。	設 123
・専用の区画とすること。	設 124
・サーバーを設置した室の出入口には出入管理設備、防犯設備を設置すること。	設 130

削除: およ

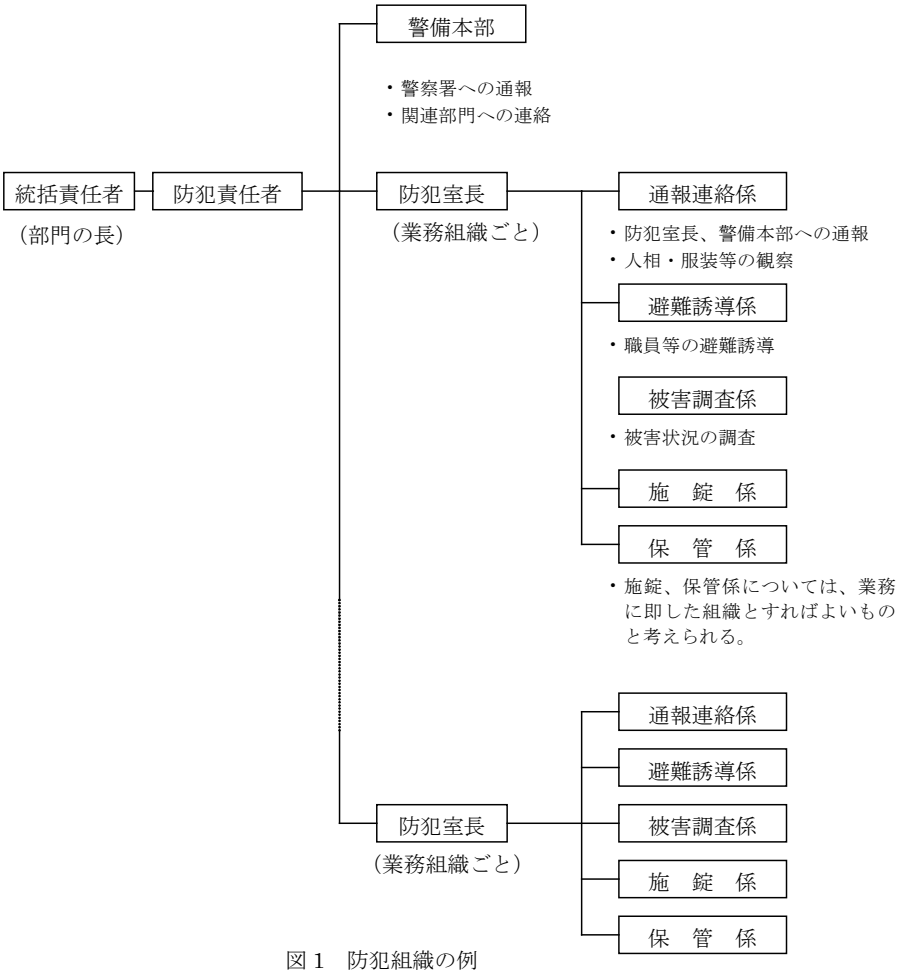

警備本部
・警察署への通報
・関連部門への連絡
統括責任者
防犯責任者
（部門の長）
防犯室長
（業務組織ごと）
通報連絡係
・防犯室長、警備本部への通報
・人相・服装等の観察
避難誘導係
・職員等の避難誘導
被害調査係
・被害状況の調査
施　錠　係
保　管　係
・施錠、保管係については、業務に即した組織とすればよいものと考えられる。
防犯室長
（業務組織ごと）
通報連絡係
避難誘導係
被害調査係
施　錠　係
保　管　係

図１　防犯組織の例

内部の統制	適　用　区　分				
組織体制	共	セ	本	提	ダ
		◎	◎		

統 12	業務組織を整備すること。

コンピュータシステムに係わる業務を円滑かつ適正に運営するとともに、不正を防止するため、業務範囲及び責任と権限を明確にし、相互牽制体制を整備すること。

1.　コンピュータシステムに係わる業務の遂行にあたっては、業務範囲及び責任と権限を明確にするとともに、適切な業務組織の分離、業務の分担が行われ、相互にチェックできる体制が整備されていることが必要である。

なお、業務組織の分離が困難な場合には、少なくとも担当者を定期的にローテーションすることなどで相互牽制が働く仕組みとすることが必要である。

2.　コンピュータセンターにおける具体的事例として、以下のようなものがある。

(1) 業務組織を分離・分担する。

プログラムの作成、入力データの作成、コンピュータシステムの運転、ライブラリ管理等を分担することにより、相互牽制を図ることが必要である。

なお、業務組織によっては、さらに以下のように職務を分離・分担することが考えられる。

・プログラムの作成‥‥‥‥‥‥‥‥‥‥‥設計者・プログラマー等
・入力データの作成‥‥‥‥‥‥‥‥‥‥‥起票者・検証者・入力者
・コンピュータシステムの運転‥‥オペレータ・オペレーション依頼者・オペレーション承認者・オペレーション検討者等
・ライブラリ管理‥‥‥‥‥‥‥‥‥‥‥‥‥プログラムライブラリ管理者・データファイル管理者等

(2) 業務処理権限、及び管理の明確化を図る。

上記の具体的な実施にあたっては、業務処理権限（担当部門の権限や役割分担）の明確化を図ることが必要である。

(3) 業務組織の分離・分担にあたっては、以下のように両方からの観点を考慮することが不正防止策として有効である。

・開発担当者が本番環境を利用できないこと（不正プログラムの投入防止、本番データへのアクセス防止）
・運用担当者が開発環境を利用できないこと（本番データの不正解析の防止）

削除: 管理体制の確立
削除: 組織の整備
削除: 運　9
削除: およ
削除: およ
削除: およ

1　内部の統制

(3)　サイバー攻撃対応態勢の整備

削除: （ＸＶ）

金融機関においても、サイバー攻撃対応態勢の整備が必要である。

安全対策基準におけるサイバー攻撃は、金融機関又はその利用者の情報システムや情報通信ネットワーク等に対し、インターネットや電磁的記録媒体等を経由して不正侵入、不正プログラムの実行、その他の攻撃等を行うことにより、情報を窃取、改ざん、破壊し、もしくは情報システムや情報通信ネットワーク等を誤作動、停止させることなどにより機能不全に陥らせる行為を企図し、または実行することをいう。

内部の統制
サイバー攻撃対応態勢

適　用　区　分				
共	セ	本	提	ダ
◎				

削除: サイバー攻撃対応態勢の整備

統 13	サイバー攻撃対応態勢を整備すること。

削除: 運　113

サイバー攻撃の手口は高度化かつ巧妙化しているため、サイバー攻撃対応態勢の整備にあたっては、手口の高度化や巧妙化にあわせて見直すことが必要である。

1. サイバー攻撃に伴うシステムの停止や、不正な資金移動に対する、未然防止策・事前対策、検知策、対応策を検討し、態勢を整備することが必要である。また、以下に示す例の他に、各金融機関等でも有効と考えられるセキュリティ対策について検討することが必要である。

2. 未然防止策・事前対策には、以下のような例がある。
   (1) 外部の第三者によるセキュリティ評価を行うこと。不正侵入防止における評価については【技 43】を参照のこと。
   (2) 業務委託先、業務提携先等のうち、重要な関係先のサイバー攻撃対応態勢の整備状況を確認すること。特に、外部委託先に対するサイバー攻撃対応態勢の整備状況確認については、監査の一環として行うことが有効であるため、【運 88】【運 90】【運 91】を参照のこと。
   (3) インシデント発生時における部署間の連携や、外部との連絡窓口の機能を担い、経営陣への報告並びに経営陣からの指示を実施することができる組織を整備すること。例として CSIRT（Computer Security Incident Response Team）の設置等がある。【技 43】（参考 4）
   (4) 大規模な攻撃が行われた場合も含め、サイバー攻撃発生時の外部ベンダー等のフォレンジックなどに関するサービス提供能力を把握すること。
   (5) 顧客が必要とする機能、並びに利用環境や IT リテラシー等のセキュリティレベルを踏まえて、利用可能な機能や限度額を設定すること。取引制限については【技 38】を参照のこと。
   (6) インターネット取引を求める顧客に対し、不正プログラム対策ソフトの導入有無等、利用者が利用するパソコン環境の事前告知を求めること。

3. 検知策には、以下のような例がある。
   (1) インシデントレスポンス態勢を整備すること。その前提として、システム全体の監視を行うことが必要となるため、【運 60】を参照のこと。
   (2) アクセス履歴を監査すること。アクセス履歴の監査については【技 37】の 2.を参照のこと。
   (3) 不正アクセス監視の一環として、侵入検知システム等による自動監視等、ネットワークの監視を行うこと。詳細については、【技 45】を参照のこと。

4.　対応策には、以下のような例がある。

(1) サイバー攻撃の発生直後はシステム障害と区別ができない可能性も想定されるため、システム障害時にサイバー攻撃の可能性を考慮すること。システム障害時の対応手順の整備については【運 63】、連絡手順については【運 62】を参照のこと。

(2) 利用者（顧客）への説明を行うこと。顧客への対応方針については、【運 105-1】を参照のこと。

(3) システムの全部または一部を、一時的に停止すること。不正アクセスの拡大防止については、【技 48】を参照のこと。

(4) 侵入経路及び手口、情報流出の痕跡及び範囲などを分析するフォレンジックを実施すること。ただし、サイバー攻撃の高度化及び複雑化に伴い、フォレンジックに必要なデータの取得対象、範囲及び期間並びに事象発生時の証拠保全方法は変化することから、実施にあたっては、専門的な知識や技術を持つ外部業者に委託することも有効である。

5.　教育・訓練には、以下のような例がある。

(1) サイバー攻撃を想定した対応訓練を実施すること。

(2) サイバー攻撃対応の意識を高めるためにも、データやファイル交換を行う当事者同士が必要に応じて相互のサイバー攻撃対応態勢について確認すること。

(3) 教育・訓練の実施に際しては、コンピュータセンターと本部・営業店等との連携を行うこと。また、業界団体が訓練を開催する場合には参加すること。

(4) サイバー攻撃を受けるリスクや、受けた場合の対応手順は、関係する役職員、外部委託先に対して周知、啓発を行い、訓練を実施すること。関係する役職員に対しては【運 80】、外部委託先に対しては【運 89】をそれぞれ参照のこと。

(5) 顧客に対して、サイバー攻撃を受けるリスクや防止策を周知し、注意喚起を行うこと。注意喚起すべき内容については【運 105-1】を参照のこと。

6.　サイバー攻撃に対応するためには、事前の情報収集並びに攻撃発生時の相談先として、セキュリティ対応機関を利用することが望ましい。

1　内部の統制

削除: （VI）

削除: 教育・訓練

(4)　人材（要員・教育）

削除: 1.

削除: 教育･訓練

コンピュータシステムの運用を安全かつ円滑に行うため、システムの開発・変更および運用に携わる要員の人事管理ならびに健康管理を適切に行うことが必要である。

また、配置にあたってはスキルを正しく評価するとともに、職務権限を適切に分離し、職責を明確にすることが必要である。

さらに、コンピュータシステムの運用を安全かつ円滑に行うため、要員に対しセキュリティ教育をはじめとした各種の教育および訓練を行うことが必要である。また、教育・訓練の目的を明確にし、計画の策定および実施を行う体制を整備することが必要である。

内部の統制	適　用　区　分				
人材（要員・教育）	共	セ	本	提	ダ
	◎				

統 14	セキュリティ教育を行うこと。

セキュリティ意識の向上を図るため、全役職員（外部要員を含む）に対するセキュリティポリシーの周知徹底と、具体的なセキュリティ対策実施に関するセキュリティ教育を、担当する業務内容等を勘案のうえで行うこと。

1. 会社（もしくは組織）として定めた、セキュリティポリシーに関する教育を、セキュリティ関連文書（セキュリティポリシー（基本方針）、セキュリティスタンダード（自社の安全対策基準）、及びこれに基づいて作成されたマニュアルや手順書等）により行い、これらを理解させ、責任と義務及び懲罰等について周知徹底を図ることが必要である。

2. 教育・訓練は定期的、計画的に行うこと。新入社員あるいは中途採用者であっても確実にセキュリティ教育が受けられる体制にしておくことが必要である。なお、セキュリティに関する事故が発生した時などにも、教育・訓練を行うことが望ましい。

3. 教育にあたっては、以下の重要性を明確にすることが必要である。
   (1) コンピュータシステムが果たす役割
   (2) 機密保護、顧客データの保護
   (3) システムの安全運用等についての対策

4. 教育テーマとしては、以下のような例がある。
   (1) セキュリティポリシー
   (2) システム利用に係わる手順、手続き
   　特に、・ユーザーID、パスワードの管理
   　　・利用権限の認識
   　　・ドキュメントや出力物の整理、整頓
   　　・異常事態発見時の対応
   (3) 機密保護
   (4) セキュリティを守るためのユーザーの責任と義務
   (5) 顧客情報保護
   (6) セキュリティ違反時の懲罰等
   (7) コンピュータウイルスへの対応
   (8) 不正アクセスへの対応
   (9) 著作権保護

削除: 教育・訓練
削除: 教育・訓練
削除: 運　80
削除: およ
削除: およ

(10) 情報倫理
(11) ソーシャルエンジニアリング対策
(12) 電子メール、ホームページ閲覧等の運用方針 【運 107、技 42-1】

（注）「ソーシャルエンジニアリング」とは、不正侵入するのに必要なシステム情報を、正規のユーザーあるいはその同僚などから聞き出したり、ごみ箱に捨てられた記録紙から推測したりする手法のことである。対策としては、アカウント、パスワード、ネットワークアドレス等のシステム情報の厳重管理や、擬似ソーシャルエンジニアリングによる訓練等がある。

内部の統制	適　用　区　分				
人材（要員・教育）	共	セ	本	提	ダ
	◎				

統 15	要員に対するスキルアップ教育を行うこと。

システムとその開発対象となる適用業務に関する知識、及び技能の向上を図るための教育を、担当する業務内容等を勘案のうえで行うこと。

1.　コンピュータシステムの開発、運用、及び利用に携わる要員（外部要員を含む）に対し、職種、職責、経験年数等を考慮した社内教育、社外教育を行うことが必要である。

2.　教育の具体例としては、以下のようなものがある。

(1) 社内教育

①　システム技術研修
②　システム利用研修
③　適用業務システム研修
④　適用業務に関する研修
⑤　システム管理者研修
⑥　情報処理技術者認定試験研修
⑦　OJT

(2) 社外教育

①　メーカー・ベンダー研修
②　外部セミナー・講習会
③　教育機関派遣

3.　教育実施後、金融機関等における教育の責任者は、教育担当者から教育結果について報告を受け、要員の習得状況を把握することが必要である。

削除: 教育・訓練

削除: 教育・訓練

削除: 運　81

削除: およ

削除: およ

内部の統制	適　用　区　分				
人材（要員・教育）	共	セ	本	提	ダ
	◎				

統 16	オペレーション習熟のための教育および訓練を行うこと。

コンピュータシステムに係わる通常時運用の円滑化および営業店事務処理に係わる端末機器の操作習熟のため、オペレーションの教育および訓練を行うこと。

1.　コンピュータシステムのオペレーションの教育および訓練については、以下の点に留意すること。

(1) コンピュータシステムに係わる通常時の運用（自動運行方式を導入している場合を含む）においては、システム進行状況の的確な把握、正確・迅速な運用対応等を円滑に行うため、新人配属時、新機種導入時、ソフトウェア変更時等に、オペレーションの教育および訓練を行うこと。なお、教育および訓練の実施に際しては、責任者、訓練範囲、訓練内容、所要時間等の訓練体制を明確にして実施することが必要である。

(2) 営業店事務処理に係わる端末機器の操作に関しては、研修モードを利用した研修等により、新人配属時、新端末導入時等に担当、職責、経験年数等を考慮した教育および訓練を、責任者を明確にして継続的に行うことが必要である。

2.　訓練実施結果については、分析・評価のうえ、次回訓練に反映させることが必要である。なお、訓練実施結果の分析・評価に際しては、理解度テスト等の客観的な指標を用いることも有効である。

削除: 教育・訓練

削除: 教育・訓練

削除: 運　82

内部の統制	適　用　区　分				
人材（要員・教育）	共	セ	本	提	ダ
	◎				

統 17	障害時・災害時に備えた教育・訓練を行うこと。

削除: 教育・訓練

削除: 教育・訓練

削除: 運　83

障害時・災害時に備えるため、コンピュータシステムの運用に係わるオペレーション等の教育・訓練を行うこと。

1. 障害時・災害時におけるコンピュータシステムの運用を円滑に行うため、障害時・災害時マニュアル及びコンティンジェンシープランに基づいたオペレーションの教育・訓練を定期的に行うことが必要である。

また、訓練結果については、責任者を明確にし、分析・評価のうえ、次回訓練及びコンティンジェンシープランに反映することが必要である。

なお、教育・訓練の実施に際しては、コンピュータセンターと本部・営業店等との連携が必要である。

部門内に閉じているコンピュータシステムにおいては、その重要性に応じた教育・訓練を実施することが必要である。教育・訓練の実施にあたっては、全社的なコンティンジェンシープランと整合を図ることが必要である。

2. 訓練としては、以下のような例がある。

(1) 訓練範囲

コンピュータシステムの運用を担当する要員(コンピュータセンター等における外部要員を含む）に対し、職責、経験年数等を考慮した訓練を実施する。なお、必要に応じ、本部・営業店等におけるユーザーについても訓練に参加させることが必要である。

(2) 訓練内容

① オンライン回復・再始動訓練

② 代替機、代替回線、バックアップシステム（バックアップサイト設置分を含む）等への切替え及び切戻し訓練

③ オンライン障害発生時の業務縮退等の訓練

④ 自動運行システム障害時の業務縮退、マニュアル運用等の訓練

⑤ 障害時・災害時の代替手段を想定した事務処理の教育・訓練

(3) 所要時間

障害・災害発生時には迅速な行動が要求されるため、目標時間を設定した訓練を行うとともに、コンピュータ運転スケジュールとの調整を図ること。

3.　訓練上の考慮点としては、以下のようなものがある。

(1) 障害時・災害時に迅速な対応がとれるよう、訓練はできるだけ本番環境に近い状態で実施する。ただし、実施困難な場合には、本番環境との差異を洗い出したうえで、テスト環境等で訓練を実施する。また、環境が準備できない場合には、机上訓練によって訓練内容をレビューすることも有効である。

(2) 担当者の交替や機器構成の変更等に合わせて行うなど、訓練効果を考えて実施する。

4.　訓練実施時には本番環境に戻した後、本番稼働に支障がないことを確認する必要がある。

5.　障害時・災害時マニュアルの整備については、【運 15、運 62～運 64】を参照のこと。

内部の統制	適　用　区　分				
人材（要員・教育）	共	セ	本	提	ダ
	◎				

削除: 教育・訓練

削除: 教育・訓練

統 18	防災・防犯訓練を行うこと。

削除: 運　84

非常時に備えて防災・防犯訓練を行うこと。

1. 防災組織、防犯組織が十分機能するよう、非常時を想定した防災・防犯訓練を行うことが必要である。
　ただし、実施困難な場合には、机上訓練によって訓練内容をレビューすることも有効である。

2. 防災・防犯訓練は、訓練範囲、訓練内容、所要時間等の訓練体制を明確にして行うことが必要である。
(1) 訓練範囲
　コンピュータセンター及び本部・営業店等における役職員、外部要員（委託先や再委託先（再委託には二以上の段階にわたる再委託を含む））等の関係者を対象とする。
(2) 訓練内容
　① 防災・防犯設備の操作訓練
　② 防災・防犯機関との連絡訓練
　③ 緊急連絡網の機能訓練
　④ 避難訓練
　なお、訓練内容は、通信途絶時等を想定した複数の連絡手段を用いた訓練を行うことが必要である。【運 62】
(3) 所要時間
　災害・犯罪発生時には迅速な行動が要求されるため、目標時間を設定した訓練を行うことが必要である。

3. 訓練実施結果については分析・評価のうえ、次回の訓練に反映させることが必要である。
　また、コンティンジェンシープランに反映させるべき事項があれば、当該プランにも反映させることが必要である。

参照法令	消防法第 8 条、消防法施行令第 4 条

内部の統制	適　用　区　分				
人材（要員・教育）	共	セ	本	提	ダ
	◎				

統 19	要員の人事管理を適切に行うこと。

システムの円滑な運用のため、要員の配置、交替等人事管理を適切に行うこと。

1. コンピュータシステムの運用に携わる人員（パートタイマー、派遣等外部要員を含む）の配置、交替等は、スキル、経験年数、人事面接等とセキュリティ、及び効率面を考慮して、適切に行うことが必要である。

2. 職務権限の分離、及び職責に対するスキルの評価を行うことが必要である。

削除: 要員管理

削除: 要員管理

削除: 運　85

削除: およ

削除: およ

内部の統制	適　用　区　分				
人材（要員・教育）	共	セ	本	提	ダ
	◎				

削除: 要員管理

削除: 要員管理

統 20	要員の健康管理を行うこと。

削除: 運　86

作業環境の整備や定期的に健康診断を実施するなど要員の健康管理を適切に行うこと。

1. コンピュータシステムの運用に携わる人員（パートタイマー、派遣等外部要員を含む）の健康管理は、要員の勤務体制、作業内容、コンピュータ室内の環境等を考慮して定期的な健康診断、及びカウンセリングを行うことが必要である。

削除: およ

2. 要員の健康管理上注意すべき事項には、以下のようなものがある。
(1) 配置及びローテーションの適切化
(2) 残業時間、夜間勤務、休日勤務、休暇取得状況等勤務体制
(3) 業務的緊張感からくる精神的ストレス
(4) システム開発・運用業務に適した作業環境の維持・改善

削除: およ

（参考）
1. VDT 作業の増加に伴う作業環境の整備の観点から行う対策として以下のような例がある。
(1) ディスプレイ画面のグレア防止対策
① 作業者の視野内に高輝度の照明器具、窓、壁面や点滅する光源等がない場所への設置
② 高輝度の照明器具、窓、壁面や点滅する電源等がディスプレイ画面に映り込まない場所への設置
③ 低輝度型照明器具の使用（ルーバー等を取り付ける）
④ ディスプレイ画面にフードまたはフィルターの取付け

2. VDT 作業環境については、厚生労働省が平成 14 年 4 月に定めた「VDT 作業における労働衛生管理のためのガイドライン」を参照のこと。

※グレアとは、視野内で過度に輝度が高い点や面が見えることによっておきる不快感や見にくさのことで、光源から直接または間接に受けるギラギラしたまぶしさなどをいう。

外部の統制	適　用　区　分				
金融機関相互のシステム・ネットワークのサービス	共	セ	本	提	ダ
	◎				

統 28	金融機関相互のシステム・ネットワークのサービス利用にあたっては、適切なリスク管理を行うこと。

金融機関相互のシステム・ネットワークは、金融機関相互の金融取引の決済や CD/ATM オンライン提携などを行うえで、基幹インフラとしての機能を担っている。仮にシステム・ネットワークにおいて、障害が発生した場合は、その影響は決済システム全体及び顧客サービス全般に及びかねないことから、適切なリスク管理を行うこと。

1.　金融機関がその業務を営むために必要な事務を第三者に「委託」する場合は、金融機関みずからが、委託先の選定や委託内容（提供されるサービスの内容やレベル等）を取り決めることができるのが一般的である。

一方で、金融機関相互のシステム・ネットワーク(注1)の「サービス利用」については、当該サービスの提供元が限定されており、加えて数多くの金融機関が共同で利用しているという特徴がある。

このため、各金融機関が、外部委託の管理と全く同様に、サービスの提供元を複数の中から選定することや、独自にリスク管理を行うことは難しく、また非効率な場合が多い。

したがって、当該サービスの利用にあたっては、以下の観点で管理することが必要である。

(1) 金融機関は、当該サービスの管理者(注2)に対して、システム上の適切な対応がなされていることを確認すること。

具体的には、金融機関は、①サービスの管理者から監査報告を受ける、②金融機関みずからが利用している範囲で、障害の発生を確認できる体制を構築する、などが考えられる。

なお、サービスの管理者が IT ベンダーの場合には、金融機関の代表組織等が組織運営に関わることが多い。その際には、代表組織等が、金融機関に代わり、当該サービスの管理者に対して、システム上の適切な対応がなされていることを確認し、各金融機関に報告することも考えられる（以下、(2)、(3)も同様の扱い）。

(2) 当該サービスにおいてシステム更改を行う場合には、金融機関みずからも、システム上の適切な対応がなされていることを、必要に応じて十分に評価・確認すること。

具体的には、①当該サービスとの接続テストにより、金融機関みずからのシステムのほか、当該サービスの更改後のシステムが正常に稼働することを確認する、②当該サービスの管理者から、プロジェクト管理体制やシステム品質状況等、システム更改の内容に応じた必要な報告を受けること、などが考えられる。

削除: 外部委託管理
削除: 外部委託業務管理
削除: 運　90-1
削除: 上
削除: 自ら
削除: 自ら
削除: 自ら
削除: 自ら

(3) 特に、当該サービスの運営、及び更改に係る意思決定において、金融機関が主導的な役割を果たしている場合には、金融機関は、当該サービスの管理者とともに、十分なリスク管理態勢、プロジェクトマネジメント態勢等を整備すること。

具体的には、金融機関みずからによる当該サービスのシステム・ネットワーク構成の確認、進捗会議等への参加、問題点への対処などを行うことが考えられる。

削除: およ

削除: 自ら

（注 1）統合 ATM スイッチングサービス、全国銀行データ通信システム、信用金庫業界の ATM・為替のシステム、信用協同組合業界の ATM・為替のシステム、労働金庫業界の ATM・為替のシステム、農業協同組合業界の ATM・為替のシステム。

なお、金融機関が上記以外のシステム・ネットワークサービスを対象とすることを妨げない。

（注 2）金融機関が利用する当該サービスを管理する組織。金融機関により組成された組織のほか、サービスを提供する IT ベンダーとなる場合などがある。

1　入退管理

削除：（Ⅱ）

(1)　入退館（室）管理

削除：1．

不法侵入、危険物持込み、不法持出し等を防止するため、コンピュータセンターやコンピュータ室等重要な室へ出入りする人・物を管理することが必要である。

入退管理
入退館(室)管理

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実1	資格付与、及び鍵の管理を行うこと。

コンピュータセンターへの入館者、及びコンピュータ室、データ保管室等重要な室への入室者を特定するため、資格付与と鍵の管理を行うこと。

1. コンピュータセンターへの入館者を特定するため、写真入り入館許可証を発行する等、資格の付与を行うことが必要である。また、コンピュータセンターへの入館が許可された者であっても、コンピュータ室、データ保管室、中央管理室（中央監視室、防災センター等）、コンピュータ関連設備室、及び重要なサーバー設置場所への入室者を特定するため、所属、立入場所等を判別できる識別章を発行することが必要である。また、本部・営業店等における重要なサーバーの設置場所への出入についても、入室者への資格付与や鍵の管理を行うことが必要である。

   なお、プログラム開発場所についても十分な管理を行うことが望ましい。

2. ここでいうコンピュータ関連設備室、及び重要なサーバー設置場所とは、以下の室を指す。
   (1) コンピュータ関連設備室
      ① 電源室
      ② 空調機械室
   (2) 重要なサーバーの設置場所については、以下の基準項目を参照のこと。
      ① 重要なサーバー設置場所　位置 【設 121～124】
      ② 重要なサーバー設置場所　構造・内装 【設 125～127】

3. 資格付与の具体例として、以下のようなものがある。
   (1) 常駐者（コンピュータセンター業務に従事する役職員・他社の勤務者、コンピュータセンター業務に係わりの深い他部門の役職員等。以下同じ）に対しては、写真入り入館許可証の発行（機械により入退管理を行う場合は、資格の登録・磁気カードの発行、及び識別コードの付与等）及び所属、立入場所等を判別できる識別章の発行を行う。なお、所属、立入場所等が明示された写真入り入館許可証は識別章を兼ねることができる。
      ① 本基準項目の趣旨を踏まえて資格付与されたことが確認できるものであれば、ここでいう写真入り入館許可証に該当すると考えられる。
      ② ここでいう識別章とは、名札、バッジ、腕章等を指しているが、所属、立入場所が容易に判別できる方法としては、例えば、これら識別章の色分けが考えられる。
      ③ ここでいう機械とは、あらかじめ設定された入退資格を識別し、扉の開閉（施錠、解錠）を行う出入管理設備を指している。【設 16】参照

削除: 運　11
削除: およ
削除: およ
削除: およ
削除: およ
削除: およ
削除: およ

(2) 資格喪失時には、写真入り入館許可証、及び識別章を回収する。

削除: およ

4. 資格付与にあたっては、コンピュータ室、データ保管室、電源室、空調機械室、中央管理室、及び重要なサーバー設置場所への入室者を特定することが必要である。

削除: およ

特定者の例としては、表１のようなものが考えられる。

なお、ここに示した者以外にも、必要に応じ入室を許可することが考えられるので、その際の資格付与方法についても明確にしておくことが必要である。

5. 鍵管理の具体的事例としては、以下のようなものがある。

(1) 出入口の鍵は定められた場所に保管し、管理は特定者が行う。

なお、鍵の複製を要する場合は、所定の方法により行うことが必要である。

(2) 鍵の受渡者の氏名、及び受渡時の時刻を記録する。

削除: およ

記録の目的は鍵の授受の明確化により責任の所在を明らかにするとともに、管理の徹底を図ることにある。なお、貸出用の磁気カード等についても、この項目を適用し、管理の徹底を図ることが必要である。

(3) 磁気カードの発行管理、識別コード等の管理は特定者が行う。

① 入退管理用磁気カードの発行管理は特定者が定められた方法によって行うとともに、有資格者が資格を喪失した場合は、磁気カードを速やかに回収することが必要である。

② 入退管理用磁気カードの紛失には十分注意して保管管理することが必要である。

③ 入退管理用識別コードの登録・変更・抹消は特定者が定められた方法によって行うとともに、必要に応じ変更することが必要である。なお、入退管理用識別コードの登録・変更にあたっては、容易に推測できない番号を選択することが必要である。

④ 入退管理用磁気カード等の紛失、毀損、不携帯等の場合の手続きを明確にしておくことが必要である。

⑤ 入退管理用テンキーは、定期的に清掃またはテンキー保護カバーを交換するなど、外見的にパスワードが推測できない措置を講ずることが必要である。

⑥ 磁気カード、識別コード、パスワード以外による資格確認については、【設 16】を参照のこと。

表１　入室者の特定例

室	入室資格者
コンピュータ室 データ保管室 電源室 空調機械室 中央管理室 重要なサーバー設置場所	オペレータ、コンピュータシステムの管理者 ライブラリ管理者、データの保管管理者、プログラムの保管管理者 電源設備の管理者 空調設備の管理者 電源設備、空調設備、及び防災・防犯設備の管理者 サーバーの管理者

削除: およ

入退管理
入退館(室)管理

適　用　区　分				
共	セ	本	提	ダ
	◎			

実 2	入退館管理を行うこと。

削除: 運　12

不法侵入、危険物持込み、不法持出し等を防止するため、入退館者の資格確認により、コンピュータセンターの入退館管理を行うこと。

1. 共同ビルを利用しているコンピュータセンターでは、入退館管理を行うことができない場合が考えられる。そのような場合は、入退室において、入退館管理と同等の管理ができるようにしておくことが必要である。

2. 入退館管理の具体的事例として、以下のようなものがある。
   (1) 常駐者に対しては、写真入り入館許可証（機械により入退管理を行う場合は、磁気カード、識別カード等）により入退館の資格を確認する。また、館内にあっては、識別章を常時着用させる。
   (2) 訪問者（常駐者以外の役職員、写真入り入館許可証未発行の他社の勤務者を含む。以下同じ）に対しては、身元及び用件を確認のうえ、入退館を許可する。また、訪問者用の識別章を貸与し、館内にあっては常時着用させ、退館時に回収する。
   (3) 訪問者については、来訪者名簿に氏名、勤務先、電話番号、用件、訪問先、入館時刻、退館時刻、貸与識別章番号等を記録する。
   (4) 訪問者に対しては、面会場所を特定し、被面会者が訪問者を確認のうえ、案内する。
   (5) 必要に応じ入退館者の所持品検査を行う。
   (6) 搬出入物品は、納品書・受渡し書、許可証等で確認を行う。
   (7) 警備員を配置する。

3. 入退資格が付与されている者であっても、夜間、休日の入退館については、入退館者名を入館受付に事前通知することや、入退館記録の事後チェックなど、手続きを明確にしておくことが必要である。

入退管理
入退館(室)管理

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実 3	入退室管理を行うこと。

削除: 運　13

不法侵入、危険物持込み、不法持出し等を防止するため、コンピュータ室及びデータ保管室等重要な室については、資格確認により入退室管理を行うこと。

1.　コンピュータ室及びデータ保管室、中央管理室（中央監視室、防災センター等）並びに重要なサーバー設置場所は、コンピュータ処理の中枢を占める機器、データファイル、プログラムファイル等が設置・保管されているため、入館を許可されたものであっても、再度、資格確認を行うことが必要である。

2.　具体的事例として、以下のようなものがある。

(1) 入退室者の資格確認は識別章等により行う。

コンピュータ室及びデータ保管室、中央管理室並びに重要なサーバー設置場所への入退室は、以下のような方法で行うことが考えられる。

①　機械により入退室管理を行っている場合は、磁気カードに付与されている資格の確認または識別コードの確認等により、自動的に入室許可を与える。

②　入室受付窓口で、受付係等が識別章を確認のうえ、入室許可を与える。

③　管理者が、入室の際に資格確認を行い、入室許可を与える。

(2) 入退室者の氏名、入退室時刻、危険物や可搬型記録媒体等の持込み物、及び持出し物の記録をする。

記録の目的は、在室時間を明確にし、障害及び不正使用等が発生した場合の原因究明を容易にするためであり、当該記録については一定期間保管することが必要である。

なお、機械により自動的に記録することも考えられる。

(3) コンピュータ室への用紙等可燃物の持込みは、必要最小限にする。

(4) 保守または工事の目的以外、危険物または燃焼器具をコンピュータ室及びデータ保管室、中央管理室へ持ち込まない。

(5) コンピュータ室への可搬型記録媒体の持込み及び持出しは、必要最小限とし、管理者が許可を与える。

なお、管理者が持込み及び持出しを行う場合は、別の管理者が許可を与える等、相互牽制が働くような仕組みを考慮する。

(6) 訪問者による作業については、必要に応じて管理者または管理者の指示を受けた者の監視下に置くことが望ましい。

3.　本部・営業店等における重要なサーバー設置場所については、上記に準じて入退室管理を行

うことが望ましい。

4. 入退室を許可された者の搬出入物品であっても、不審な場合は内容を確認することが必要である。

2　運用管理

削除: （Ⅲ）

(1)　マニュアルの整備

削除: 1．

コンピュータシステムを正確かつ安全に運用するため、通常時の各種運用手順を標準化し、マニュアルを整備することが必要である。また、障害・災害による影響を極小化し早期復旧させるため、障害時・災害時の操作手順を明確化し、マニュアルを整備することが必要である。

運用管理
マニュアルの整備

適　用　区　分				
共	セ	本	提	ダ
◎				

実 4	通常時マニュアルを整備すること。

削除: 運　14

コンピュータシステムを正確かつ安全に運用するとともに、本部・営業店等設置の端末機器の誤操作を予防し、事務処理を円滑に行うため、通常時における各種手順（含む操作手順）を定めたマニュアルを整備すること。

1.　ここでいう通常時マニュアルとは、コンピュータシステムの通常時運用に必要な手順、手続き、及び本部・営業店等における端末機器等の操作手順を定めたものを指している。

削除: およ

なお、マニュアルはシステム変更等が発生した都度見直しを行い、常に最新の状態にしておくことが必要である。

2.　通常時マニュアルとして整備すべき事項については、以下の基準項目を参照のこと。
(1) アクセス権限の管理　【運 16～18】
(2) オペレーション管理　【運 19～23】
(3) データファイル管理　【運 25～27】
(4) プログラムファイル管理　【運 28、運 29】
(5) ドキュメント管理　【運 33、運 34】
(6) 帳票管理　【運 35、運 36】
(7) 出力管理　【運 37】
(8) カード管理　【運 51、運 52】
(9) 資源管理　【運 54】
(10) 外部接続管理　【運 55、運 56】
(11) 機器の管理　【運 57～59】
(12) 運行監視　【運 60】

3.　上記の他、本部・営業店等における通常時マニュアルには、以下のような内容を含んでいることが必要である。
(1) 端末機器のオペレーション
(2) 事務手続き

4.　通常時マニュアルの整備に係わる具体的事例として、以下のようなものがある。
(1) 通常時マニュアルを整備し、遵守について関連部門に周知徹底させる。
(2) 追加・変更等が発生した場合は、定められた手続きに従い更新する。

5. マニュアルに盛り込む要件としては、以下のようなものがある。

(1) 記述内容

① 職務遂行に必要な基本事項について、その基準・手続き等の記述

② 特定の事務処理について、その具体的な流れ・手続きの記述

③ ①または②に記載している事項について、その作業方法を具体的にわかり易く示して、作業担当者の職務遂行上の手引となる記述

(2) 記述項目

① 表題

② 改訂履歴

③ 目次

④ 前文、総則（目的、趣旨、基本方針、適用範囲等）

⑤ 本文

⑥ 雑則（適用の特例、施行時期、経過措置等）

⑦ 様式（書式、記入事項）

⑧ 付表（参考資料等）

(3) 文書の制定と承認

(4) 文書の配布と管理

(5) 文書の整理、保管、保存

(6) 文書変更の手続き

(7) その他例外規定等

運用管理
マニュアルの整備

適　用　区　分				
共	セ	本	提	ダ
◎				

実 5	障害時・災害時マニュアルを整備すること。

削除: 運　15

障害・災害によるコンピュータシステムへの影響の極小化と早期復旧ならびに本部・営業店等における業務継続のため、障害時・災害時における代替措置、復旧手順及び対応方法等について定めたマニュアルを整備すること。

1.　障害時・災害時マニュアルとして整備すべき事項については、以下の基準項目を参照のこと。
　なお、障害時・災害時マニュアルの整備にあたっては、コンティンジェンシープランとの整合性を保つことが必要である。また、マニュアルは組織的な管理のもと、定期的に見直し等を行い、最新の状態にしておくことが必要である。マニュアルの記載内容については、経験の浅い要員でも理解できるよう、作業手順等を明確にすることが望ましい。
(1) 障害時・災害時対応策　【運 62～運 64】
(2) コンティンジェンシープランの策定　【運 65】

2.　特に、本部・営業店等における業務継続のため、障害時・災害時マニュアルには、以下のような内容を含んでいることが必要である。【運 62～運 64】
(1) 端末機器の取扱い
(2) 事務手続き

2　運用管理

削除: （Ⅲ）

(2)　アクセス権限の管理

削除: 2．

　コンピュータシステムを構成する機器、ファイル等各種資源に対する破壊、及び不正使用を防止するため、その重要度に応じたアクセス権限を設定し、管理することが必要である。

削除: およ

運用管理
アクセス権限の管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 6	各種資源、システムへのアクセス権限を明確にすること。

削除: 運　16

無資格者によるアクセスを防止するため、コンピュータシステムと、システムの運用上及び業務上重要なファイルは、アクセス権限所有者を特定すること。

1.　ここでいうコンピュータシステムの運用上もしくは業務上重要なファイルとは、金融機関等が顧客にサービスを提供するうえで必要となるデータ、プログラム等を指し、これらのファイルについては不正使用、改ざん等を防止するため、アクセス権限所有者を特定するとともに、必要最小限に限定することが必要である。アクセス権限の特定は以下の点からも行うことが必要である。

(1) 重要な還元帳票ファイル等の不正使用を防止する。
(2) システムの開発・変更作業に係わるテスト用データの漏洩を防止する。
(3) アプリケーションプログラムへのアクセス管理を行うことによるプログラムの改ざん防止及び内容の漏洩を防止する。

アクセス権限の確認に利用される機能については、以下の基準を参照のこと。
【技 26、技 31、技 35、運 17】
また、アクセス手段を特定するとともに、必要最小限に限定することも考えられる。

2.　不正アクセスが行われた場合の早期発見と原因究明のため、アクセス記録の取得を行うことが必要である。また、正当な権限のない者のアクセスに対しては、アクセス権限がない旨の警告を表示することが望ましい。【技 37】

3.　アクセス権限管理の具体的な注意点は、【運 18】参照のこと。

運用管理
アクセス権限の管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 7	パスワードが他人に知られないための措置を講じておくこと。

パスワード等の漏洩防止のため、他人に知られないための注意喚起等の措置を講じておくこと。

1. パスワード等については、以下の事項を使用者に注意喚起する等の対策が必要である。
   ・推測されやすいパスワードを設定しないこと
   ・パスワード等を他人に知られないようにすること
   ・他人のパスワード等を使用しないこと
   ・パスワードをメモ等に残した場合、メモ等の盗難・紛失により他人にパスワードが漏洩するおそれがあること
   また、初期設定されるパスワード等についても推測されやすいパスワードを設定しない等の運用によって、漏洩するリスクを軽減することが必要である。

2. 推測されやすいパスワードとは、例えば以下のようなものがある。
   ・桁数の短いパスワード
   ・ID と同一のパスワード
   ・生年月日、電話番号、住所（地番）、自分の車のナンバー等の個人の生活に関連した情報
   ・自分、及び自分の知っている人（配偶者、友人、ペット、有名人等）の名前や愛称
   ・123456 等の単純な文字列や英字のみのものまたは数字のみのもの
   ・よく使われる英語の単語
   ・上記の逆読みやそれらの組合せ

3. 社内で使用するパスワード等については、長期にわたって同じパスワードを使用し続けることがないよう、適宜変更することとし、変更されないまま一定期間が経過した場合、当該 ID を使用不可とする措置を講ずることが望ましい。なお、個人データを扱うシステムにおいては、この措置は必要である。

4. パスワード等を他人に知られないための技術的対策については【技 26】参照のこと。

削除: 運　17

削除: およ

運用管理
アクセス権限の管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実８	各種資源、システムへのアクセス権限の付与、見直し手続きを明確化すること。

削除: 運　18

各種資源、システムへのアクセスを管理するため、アクセス権限を与えるにあたってその手続きを明確に定めることが必要である。さらに、アクセス権限を適切に保つため、見直しの手続きを明確化することが必要である。

1.　各種資源やシステムへのアクセスを管理するためには、アクセス権限の付与方法を明確に定めておく必要がある。職制、所属部署等によって、ユーザーにアクセス権限を与えるまでの承認者や、相互牽制が働く承認手順を定めることが必要である。

なお、アクセスに用いる ID はグループ等で共有せず、1 つの ID に対して 1 人を対応させることが望ましい。また、個人データを扱うシステムにおいては、漏洩等の発生に備え、アクセス権限所有者の範囲が把握できることが必要である。

2.　アクセス権限の付与は、例えば以下のような手順に従って行われることが考えられる。

(1) 従業員等利用希望者が利用するデータへのアクセス権の取得を申請する。

(2) 所属長が業務上適切か審査のうえ承認し、当該データ管理者にアクセス権の付与を申請する。

(3) データ管理者が所属部署、職制、利用目的等を審査のうえ承認する。

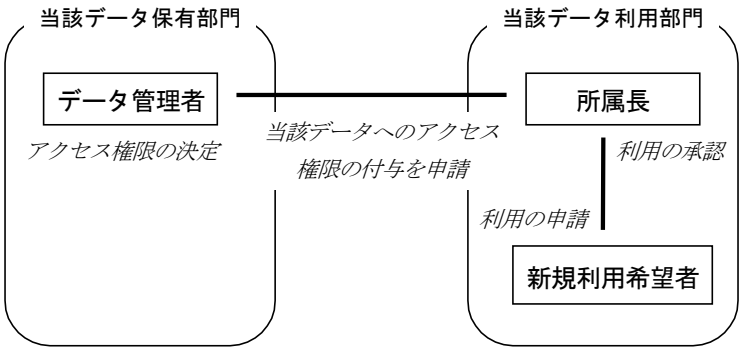


図１　アクセス権限の取得承認例

3.　人事異動等によるアクセス権限の見直しを速やかかつ適切に行うため、アクセス権限の見直し手続きを明確化する必要がある。アクセス権限の見直しは人事異動等に合わせ適宜行う措置を講ずることが望ましい。なお、個人データを扱うシステムにおいては、この措置は必要である。

4.　アクセス権限見直しのタイミングとしては、以下のようなものがある。

・所属、職制、組織変更時
・入社時、退職時
・長期出張、長期留学、休職
・新システム稼働時
・一定期間経過時

5.　アクセス権限管理の具体的な注意点は、以下のようなものがある。

(1) ID 等の登録・変更等の管理者を明確にしておく。
(2) ID 等の付与に際しての依頼・承認、及び発行手続きを明確にしておく。
(3) ユーザーが業務上アクセスする必要がなくなった場合、そのアクセス権限は速やかに抹消する。
(4) ベンダーから購入したパッケージソフト、アプリケーションソフト等は、導入時にベンダーが登録したアクセス権限を抹消する。
(5) システムに特権 ID（スーパーユーザー等）が設定されている場合は、管理者を限定し特別に留意する。
(6) システムに初期設定されている特権 ID（スーパーユーザー等）は、削除あるいはリネームする。
(7) アクセス権限は、必要最小限の者に対して有効期限を限って与え、期限満了に伴う延長は、その必要性を再度確認して与える。
(8) ユーザーのパスワード失念時にパスワードを通知する場合には、ユーザーの本人確認などの手続きを明確にしておく。

削除: およ

2　運用管理

削除：（Ⅲ）

(3)　オペレーション管理

削除：３．

コンピュータシステムの不正使用を防止し、運用の円滑化を図るため、オペレーションについては依頼、承認、実行、記録、結果確認等の管理を行うことが必要である。

運用管理
オペレーション管理

適　用　区　分				
共	セ	本	提	ダ
	◎			

実9	オペレータの資格確認を行うこと。

削除: 運　19

コンピュータシステムの不正使用を防止するため、オペレータの資格確認を行うこと。

1.　不正操作によるデータ漏洩、障害の発生を防止するため、コンピュータシステムのオペレーションにあたっては、運用管理責任者がオペレータの資格確認を行うことが必要である。

　また、臨時処理やトラブル発生の際に、例外的に開発担当者等にオペレーション資格を付与する場合には、運用管理責任者が承認し、処理の重要度によっては立ち会うことが必要である。

2.　資格確認の具体的事例として、以下のようなものがある。

(1) オペレーションにあたり、運用管理責任者はオペレータ勤務予定表等に基づいて、正当なオペレータであることを確認する。

(2) 正当なオペレータであることが確認できるように、コンピュータ室に常時勤務するオペレータには、制服等を着用させる。

　正当なオペレータであることが確認できる方法として、以下のような例がある。

　①　制服の着用

　②　腕章の着用

　③　名札の着用

運用管理
オペレーション管理

適　用　区　分				
共	セ	本	提	ダ
	◎			

実 10	オペレーションの依頼・承認手続きを明確にすること。

削除: 運　20

コンピュータシステムの不正使用を防止するため、オペレーションの依頼・承認手続きを明確にすること。

1. コンピュータシステムの不正使用を防止するため、オペレーションの依頼、承認は、オペレーション依頼票等を用いて行うなど、定められた手続きに従って行うことが必要である。

2. オペレーションが自動化されている場合は、スケジュールの作成、承認、及び自動スケジューリングプログラムへの登録等に関する手続きを明確に定めることが必要である。

削除: およ

3. 臨時処理やトラブル発生にともなう例外処理についても、手続きが明確に定められていることが必要である。なお、処理を実行する際は、他処理への影響等を踏まえスケジュールに留意すること。

運用管理
オペレーション管理

適　用　区　分				
共	セ	本	提	ダ
	◎			

実 11	オペレーション実行体制を明確にすること。

削除: 運　21

コンピュータシステムの誤操作、及び不正使用を防止するため、オペレーション実行体制を明確にすること。

削除: およ

1.　ここでいうオペレーション実行体制とは、オペレーションにあたってのオペレータチーム編成、及びオペレーション手順を指している。

削除: およ

2.　オペレーション実行体制に係わる具体的事例として、以下のようなものがある。

(1) オペレーション依頼票等により、承認されたオペレーション依頼であることを確認する。

(2) オペレータは専任とし、オペレーションは複数のオペレータが行う。

オペレータの専任とは、運用規定によりあらかじめ定められた者を指し、専任とする目的として、以下のようなことが考えられる。

①　責任の明確化

②　不正使用防止

また、操作を複数のオペレータが行う目的として、以下のようなことが考えられる。

①　オペレータ相互間の牽制効果による不正使用防止

②　非常時対応

(3) 重要コマンド投入にあたっては相互確認を行う。

重要コマンド投入にあたって相互確認を行わせる目的は、誤操作による障害発生を防止することにある。なお、重要コマンドとして、以下のようなものが考えられる。

①　オンライン開局処理

②　オンライン閉局処理

③　障害発生装置の切離し（中央処理装置、主記憶装置、チャネル装置、ファイル装置等）【技 22】

④　回線の論理的切替え

(4) ジョブの実行者を明確にする。

ジョブの実行者を明確にする目的は、責任を明確にするとともに、障害が確認された際の原因究明を容易に行えるようにすることにある。なお、ここでいうジョブの実行者とは、コンソールから操作もしくは運行状況確認を行うオペレータまたはオペレータチームを指している。

3.　事故や障害が発生した場合には、事故・障害状況等を速やかにオペレータを統括する担当責任者、システム運用部門の責任者等に報告することが必要である。

4. 誤操作によるコンピュータシステムの障害発生を防止し、業務を円滑に行うため、以下のような操作手順の標準化を図り、マニュアルとして常備することが必要である。
   (1) 各機器の操作方法
   (2) コマンドの使用法
   (3) コンピュータシステム運転手順

5. 機密性の高いオペレーションを行う際は、要員を限定するなど特別な注意が必要である。

6. オペレーションの自動化、簡略化については、【技 16】参照のこと。

運用管理
オペレーション管理

適　用　区　分				
共	セ	本	提	ダ
	◎			

実 12	オペレーションの記録、確認を行うこと。

削除: 運　22

オペレーションの正当性を検証するため、オペレーションの記録、確認を行うこと。

1.　オペレーションの正当性を確保するため、オペレーション実行時の運行状況を確認するとともに、依頼されたオペレーションが指示どおり処理されたことを確認できるよう、オペレーション記録を残すことが必要である。

2.　オペレーション記録の具体的事例として、以下のようなものがある。

(1) 運行状況を確認するチェックリストを作成する。

運行状況を確認するチェックリストとして、以下のようなものが考えられる。

①　オペレーション実施記録
②　オペレーション予定・実績比較表
③　オペレーション進捗状況表

(2) オペレータ交替時の未処理、重複処理を防止するため、オペレーションを引き継ぐときの引継事項を明確にする。

引継事項としては、以下のようなものがある。

①　ジョブ処理状況
②　障害発生状況
③　その他連絡事項

(3) オペレーション記録を残し、オペレーション結果を検証する体制を明確にする。

オペレーション結果の検証方法としては、以下のようなものがある。

①　運行状況チェックリストによる確認、検証
②　自動運行確認リストによる確認、検証
③　処理レコード件数の確認

なお、確認、検証時に重大な不備等を発見した場合、オペレータを統括する担当責任者は速やかに運用管理部門の責任者に報告することが必要である。

運用管理
オペレーション管理

適　用　区　分				
共	セ	本	提	ダ
	○	○		

実 13	クライアントサーバー・システムにおける作業の管理を行うこと。

削除: 運　23

クライアントサーバー・システムにおける不正使用等を防止するため、依頼、承認等の手続きを明確にし、実行、記録、結果確認等を適切に管理することが望ましい。

1.　操作管理方法としては、以下のようなものがある。

(1) 作業によって作業者を特定し、作業体制を明確にする。【運 21】

・データ、プログラムのバックアップ

・アクセス権限の登録

・システムのメンテナンス作業

(2) 作業の依頼・承認手続きを明確にする。【運 20】

(3) 作業記録をつける。【運 22】

・データ、プログラムのバックアップの取得

・システムのバージョンアップ作業

2　運用管理

削除：（Ⅲ）

(4)　入力管理

削除：４．

システムに入力するデータの完全性を確保するため、データの入力管理ルールを作成し関連部門で遵守することが必要である。

運用管理
入力管理

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実14	データの入力管理を行うこと。

削除:運　24

データの正確な処理と不正防止のため、入力手順を定めること。

1.　情報システムに入力するデータを正確に処理するとともに完全性を確保し、機密を保護し、不正を防止するために、データの入力手続き、承認等の手順を定め、遵守することが必要である。

2.　入力管理ルールの制定項目としては、以下のような例がある。

(1) 入力管理の責任者の設置、職務の明示

(2) 入力データ作成の手続き

・原始データの作成要領

・入力指示

(3) 入力データの授受

・手続き

・担当者

・授受の記録

－授受者

－日付

－データ件数

－授受データの形状とラベル内容

(4) 重要データ、機密データの取扱者の限定、確認のタイミング

(5) 入力承認（入力データの承認者）

(6) 承認時期（入力前、入力後）

(7) データのチェック

・データ内容の確認

・データ原票と入力データの照合

(8) 入力の取消し、修正、追加

(9) 入力記録の取得、管理、保存

2　運用管理

削除：（Ⅲ）

(5)　データファイル管理

削除：５．

データファイルの不正使用、改ざん、紛失等を防止するため、データファイルの授受、保管は特定者が定められた方法によって行うことが必要である。また、障害や災害等の発生に備えてバックアップを確保することが必要である。

運用管理
データファイル管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 15	授受・管理方法を定めること。

削除: 運　25

データファイルの不正使用、改ざん、紛失等を防止するため、データファイルの授受、保管は定められた方法によって行うこと。

1. ここでいうデータファイルとは、サーバー・パソコン等を含むコンピュータの磁気ディスク内のファイル、フロッピーディスク、光ディスク、磁気テープ、カートリッジ磁気テープ、DAT等を指す。

2. データファイルはその重要度に応じた保管・管理方法を明確にする必要がある。

3. データファイルの授受・保管管理方法として、以下のような例がある。

(1) 受渡し、持出し及び廃棄方法を定めるとともに、責任者を明確にする。

削除: およ

① データファイルの受渡しにおいては、不正使用、改ざん、紛失等を防止するため、以下のような項目を明確にして行うことが必要である。

a. 使用目的
b. 使用日時
c. 使用者名
d. 責任者の承認
e. 入出庫日時
f. 入出庫担当者名

② データファイルを外部に持ち出す場合、データ漏洩を防止するため、データの持出しに関する制限や管理方法を明確に定めておくことが必要である。

③ データファイルの廃棄においては、誤消去、データ漏洩等を防止するため、以下のような項目を明確にして行うことが必要である。【運 74、運 75】

a. ファイル管理簿等による保存期間
b. データファイルの機密度に応じた廃棄方法（消磁、裁断等）
c. 廃棄確認方法
d. 廃棄理由
e. 廃棄日時
f. 廃棄責任者

④ 磁気ディスクの障害等でディスクを交換または廃棄する場合は、適切な情報漏洩防止策を講ずることが必要である。【運 74、運 75】

(2) コピーを必要とする場合は、定められた方法によって行う。
　無断コピー等によるデータ漏洩を防止するため、コピーが必要な場合の依頼、承認、コピー手続き及びコピーファイルの授受、廃棄手続きを明確にしておくことが必要である。
(3) ファイルごとの保管方法を明確にする。
　データファイルの誤消去を防止するため、データファイルの重要度に応じ、保存期間等保管方法を明確にしておくことが必要である。
(4) ファイル管理簿等により、在庫管理を行う。
　データファイルの不正使用、紛失等の防止、及び早期発見のため、ファイル管理簿等により定期的にまたは随時に在庫管理を行うことが必要である。
(5) データファイルは、データ保管室等定められた場所に保管する。
　データファイルの不正使用、紛失等を防止するとともに、障害時、災害時の対応を容易にするため、定められた場所に保管することが必要である。
・コンピュータセンター
　データ保管室に管理することが必要である。
・本部・営業店
　防火区画内の施錠可能なキャビネット等で保管することが望ましい。防火区画がない場合は、耐火金庫、耐火キャビネット等で保管することが必要である。
(6) データファイルのラベル等への内容表示は記号化する。
　データファイルの不正使用等を防止するため、ラベルへの内容表示は記号等により最小限の項目にとどめることが必要である。

削除: およ

削除: およ

運用管理
データファイル管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実16	修正管理方法を明確にすること。

削除: 運　26

不正使用・改ざんを防止するため、データファイルに不整合が生じた場合のデータファイルの修正および管理は、定められた方法で行うこと。

1. プログラム障害等により、データファイルに不整合が生じた場合、ファイルの修正が必要になる場合があるが、データファイルの修正は通常の業務処理とは異なるため、修正作業の依頼・承認、及び処理手続きを明確にするとともに、結果の確認・検証を行うことが必要である。

削除: およ

2. 修正結果は、以下のような点について確認、検証することが必要である。
   (1) 処理手続きに基づいた処理の正当性の確認
   (2) 修正後のファイル内容の正当性の確認・検証

3. ファイルの重要度に応じてドキュメント（修正記録、及び修正依頼書等）を所定期間保存すること。

削除: およ

運用管理
データファイル管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 17	バックアップを確保すること。

重要なデータファイルの障害や災害等への対応のため、バックアップを取得し、管理方法を明確にすること。

1. 障害や災害等の発生により重要なデータファイルに破損等が発生した場合、そのファイルを早期に回復させる必要があるため、バックアップを取得し、保管管理方法を明確にすることが必要である。

なお、バックアップの取得、保管管理方法については、コンティンジェンシープランと整合性のとれたものとすること。

2. バックアップを取得するにあたっては、以下のような点に留意する必要がある。

(1) 適切な世代管理レベル（二世代前、三世代前まで等）を設定すること。

(2) 回復に要する時間、及びその間の影響を考慮して、取得サイクルを定めておくこと。

(3) バックアップが正常に取得できていることを確認すること。

(4) 必要に応じてバックアップ取得対象範囲の見直しを行うこと。例えば、データベースの拡張やファイルの新設を行った場合等がある。

3. バックアップを取得するにあたっては、データファイルの種類や更新タイミング等に応じて適切な保管サイクルを設定すること。保管にあたっては以下の方法がある。

(1) 分散保管

バックアップファイルを同一建物内もしくは比較的近距離の場所で保管する（火災等、局所災害に有効）。

(2) 隔地保管

バックアップファイルを遠距離の場所で保管する（地震等、大規模災害に有効）。

保管場所の選定にあたっては、本番ファイル保管場所（現有システム保有場所）とリスク要因（火災、地震、停電等）を共有しないこと、及び被災時の復旧に際しての現有システムへのファイル移送時間の考慮等も含め、総合的に判断することが望ましい。特に経営存続のために重要なデータファイルについては、大規模災害も想定して検討することが必要である。

また、保管を外部に委託する場合は、信頼性、安全性、利用体制（保管データを必要時にいつでも利用可能か、等）についても考慮する必要がある。

なお、定められた保管期間前の持出しにあたっては部門責任者の承認を得て行い、持出し記

削除: 運　27

削除: およ

削除: およ

録については所定期間保存する必要がある。

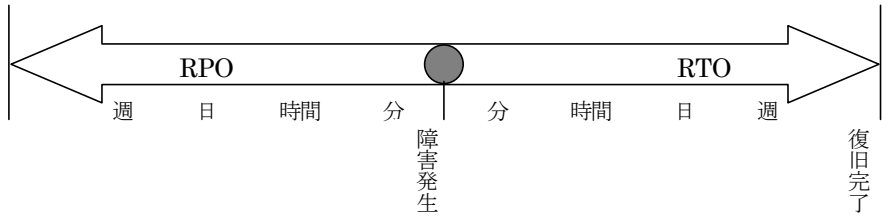
4. バックアップデータの保管方法については、【運 25】も参照のこと。

5. イントラネットへの業務の依存度が高まっていることから、これらネットワーク上のデータについても、重要度を勘案し、バックアップを確保することが望ましい。

（参考 1）

バックアップの取得サイクルを検討する際、目安となるものにRPO（Recovery Point Objective）と RTO（Recovery Time Objective）がある。RPO とは、どのくらい前の時点のデータを保存しておくのかを表し、RTO とは、どのくらいの時間でデータを復旧できるかを表す。

データの重要度等を考慮し、RPO、RTO を設定されることが多い。



（参考 2）

バックアップファイルの保管場所については、コンピュータセンターの立地条件に準じて考える必要があるため【設 1】を参照のこと。

2　運用管理

削除: （Ⅲ）

(6)　プログラムファイル管理

削除: 6．

プログラムの改ざん、破壊等を防止するため、プログラムファイルは特定者が定められた方法によって管理することが必要である。また、障害や災害等の発生に備えてバックアップを確保することが必要である。

運用管理
プログラムファイル管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実18	管理方法を明確にすること。

プログラムの改ざん、破壊等を防止するため、プログラムファイルの管理は、定められた方法によって行うこと。

1. ここでいうプログラムファイルとは、パッケージプログラム、自社開発プログラム等のソースプログラムやロードモジュールを指す。

2. 本番プログラムの改ざん、破壊、誤消去を防止するため、本番ライブラリへのプログラム登録、抹消等については、プログラムライブラリを管理する者が定められた方法によって管理するとともに、開発中または修正中のプログラムファイルと本番ファイルは分けて管理することが必要である。ライブラリとは、特定の分野で汎用的に使用されるプログラムをひとまとめにしたものを指す。

3. プログラムの管理方法として、以下のような例がある。
   (1) プログラム管理簿等を整備して管理する。
   管理内容については、【運 66】参照のこと。
   (2) コンピュータセンターにおいてプログラムライブラリへの登録等は、定められた手続きに基づいて行う。
   本番ライブラリへの新規登録、修正後の再登録、及び本番ライブラリからの抹消については、以下のような項目を明確にした登録依頼票、抹消依頼票等により行うことが必要である。
   ① プログラム番号及び名称
   ② 作業内容（新規、変更、廃棄等）
   ③ 作業理由（変更理由等）
   ④ バージョン番号
   ⑤ 本番移行予定日
   ⑥ 担当者名
   ⑦ 責任者の承認
   (3) OS・コンパイラ等を含め、プログラムのバージョン管理を行う。

削除: 運　28

削除: およ

削除: およ

運用管理
プログラムファイル管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 19	バックアップを確保すること。

削除: 運　29

プログラムの障害や災害等への対応のため、バックアップを取得し、管理方法を明確にすること。

1. コンピュータウイルス等不正プログラムによるプログラムの改ざん、破壊、及び障害や災害等の発生による破損等に対応するため、本番プログラム等重要なプログラムはバックアップを取得し、保管管理方法を明確にすることが必要である。

削除: およ

削除: 、

2. バックアップを取得するにあたっては、品質の確保も考慮して適切な世代管理方法を定めるとともに、回復に要する時間、及びその間の影響を考慮して、取得間隔を定めておくことが必要である（品質確保に関しては【技 15】、取得サイクルに関しては【運 27】参照）。

削除: およ

3. バックアップの保管には以下の方法がある。

(1) 分散保管

バックアップファイルを同一建物内もしくは比較的近距離の場所で保管する（火災等、局所災害に有効）。

(2) 隔地保管

バックアップファイルを遠距離の場所で保管する（地震等、大規模災害に有効）。

なお、保管場所の選定にあたっては、本番ファイル保管場所（現有システム保有場所）とリスク要因（火災、地震、停電等）を共有しないこと、及び被災時の復旧に際しての現有システムへのファイル移送時間の考慮等も含め、総合的に判断することが望ましい。

削除: およ

また、保管を外部に委託する場合は、信頼性、安全性、利用体制（保管プログラムを必要時にいつでも利用可能か、等）についても考慮する必要がある。

なお、定められた保管期間前の持出しにあたっては部門責任者の承認を得て行い、持出し記録については所定期間保管する必要がある。

（参考）
バックアップファイルの保管場所については、コンピュータセンターの立地条件に準じて考える必要があるため【設 1】を参照のこと。

2　運用管理

削除：（Ⅲ）

(7)　コンピュータウイルス対策

削除：7．

コンピュータウイルス等不正プログラムによるプログラムの改ざん、破壊等を防止するため、不正プログラムの侵入防止策や侵入した場合の検知策を講ずる必要がある。また、不正プログラムに感染した場合に備え、バックアップを確保しておく等、復旧対策についても講じておく必要がある。

運用管理
コンピュータウイルス対策

適　用　区　分				
共	セ	本	提	ダ
◎				

実 20	コンピュータウイルス対策を講ずること。

削除: 運　30

コンピュータウイルス等の侵入、及び感染に備えて、防御、検知、復旧の手順を明確にしておくこと。

削除: およ

1. コンピュータウイルス等の不正プログラムについては、侵入を事前に防止することが必要である。また、侵入した場合には、これを速やかに検知できるような対策を講ずることが必要である。

ATM 等の専用端末においては、メンテナンス時にウイルスが混入しないようメンテナンス用パソコン等についてもウイルス対策を講ずることが必要である。

(1) 防御対策については【技 49】参照のこと。

(2) 検知対策については【技 50】参照のこと。

2. コンピュータウイルス等不正プログラムに感染した場合に備え、速やかな復旧が行えるように事前の対策を行うことが必要である。事前対策としては、以下のような例がある。

(1) プログラムやデータのバックアップを取得し、プログラムのオリジナルファイルにはライトプロテクトを施して保管する。

(2) システムの変更履歴をとる（構成情報を保管する）。

【技 49】参考の「コンピュータウイルス対策の例」参照のこと。

3. コンピュータウイルス等不正プログラムに感染した場合、被害の拡大防止、システムの復旧、及び再発を防止するための事後対策を行うことが必要である。

削除: およ

復旧策については【技 51】参照のこと。

4. コンピュータウイルスによるデータ、ハードウェア、ソフトウェアの破壊や復旧に要した費用、損害賠償責任等について、保険の適用を検討することが望ましい。

（参考）「コンピュータウイルス対策基準」（平成 12 年通商産業省告示 952 号）

2　運用管理

削除: （Ⅲ）

(8)　ネットワーク設定情報管理

削除: 8.

ネットワーク設定情報が不正に改ざんされないように管理することが必要である。また、障害や災害等の発生に備えてネットワーク設定情報のバックアップを確保することが必要である。

運用管理
ネットワーク設定情報管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 21	設定情報の管理を行うこと。

ネットワーク機器の設定情報が不正に変更されないように管理を行うこと。

1. ルータ等ネットワーク機器の設定は正式な手続きを踏まえて変更されなければならない。また、設定が不正に変更されたり、障害などで設定情報が失われたりする場合に備えて、コンフィグレーション情報等を適切に管理することが望ましい。
   ネットワーク管理については、以下の基準項目を参照のこと。
   ・ネットワーク管理体制を整備すること　【運 6】

2. 特に、公衆回線（ATM、ISDN など）が接続されているネットワーク機器についてはモニタリングを行うなど、適切な管理を行うことが望ましい。

3. なお、ルータへのアクセスについては、ID、パスワードで保護するなどの不正アクセス対策が必要である。
   不正アクセス対策については、以下の基準項目を参照のこと。
   ・本人確認機能を設けること　【技 35】
   ・暗証番号・パスワード等は他人に知られないための対策を講ずること　【技 26】

削除: 運　31

削除: フレームリレー、

運用管理
ネットワーク設定情報管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 22	設定情報のバックアップを確保すること。

削除: 運　32

ネットワーク設定情報の不正な変更、障害や災害等への対応のため、バックアップを取得し、管理方法を明確にすること。

1. ルータ等ネットワーク機器の設定が不正に変更されたり、障害や災害等の発生により設定情報が失われたりする場合に備えて、コンフィグレーション情報等のバックアップを適切に行うことが必要である。

   バックアップの方法については、以下の基準項目を参照のこと。

   ・授受、保管管理方法を定めること　【運 25】
   ・修正管理方法を定めること　【運 26】
   ・バックアップを確保すること　【運 27】

2　運用管理

削除：（Ⅲ）

(9)　ドキュメント管理

削除：９．

ドキュメントの不正使用、紛失等を防止するため、定められた方法によって管理することが必要である。また、障害時・災害時の復旧に必要なドキュメントはバックアップを取得し、管理方法を明確にすることが必要である。

運用管理
ドキュメント管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 23	保管管理方法を明確にすること。

削除: 運　33

不正使用、改ざん、紛失等を防止するため、ドキュメントは定められた方法によって管理すること。

1. ここでいう運用管理におけるドキュメントとは、コンピュータセンターにおける運用管理に必要なオペレーションフロー、操作指示書、システム関連資料、及び端末操作マニュアル等を指している。

削除: およ

2. ドキュメントの管理方法として、以下のような例がある。
   (1) システム開発部門から業務を引き継ぐ場合は、定められた手続きに従いドキュメントの引渡しを受ける。
   (2) 追加、変更等が発生した場合は、定められた手続きに従い更新する。
   (3) 各種ドキュメントは、管理簿等で管理を行う。
   (4) 重要なドキュメントは、定められた手続きに従い、施錠可能なキャビネット等に保管する。
   (5) 他部門からの閲覧依頼に対しては、定められた手続きに従い行う。
   (6) ユーザーへ引渡しを行う場合は、定められた手続きに従い行う。
   (7) ドキュメントごとの保存期間を明確にする。

3. ペーパーによらないドキュメント（フロッピーディスク等）についても、上記 2.と同様に取り扱うことが必要である。

4. 重要なドキュメントの複写・複製については、管理方法を明確にしておくことが必要である。

運用管理
ドキュメント管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 24	バックアップを確保すること。

削除: 運　34

災害時の復旧対応のため、復旧に必要なドキュメントはバックアップを取得し、管理方法を明確にすること。

1.　災害時の復旧対応のために必要なドキュメントは、バックアップを取得し、管理方法を明確にすることが必要である。なお、火災等の災害に備えたドキュメントのバックアップの保管方法としては、以下のようなものがある（取得サイクルに関しては【運 27】参照）。

(1) 分散保管

システムの復旧に必要なドキュメントを同一建物内もしくは比較的近距離の場所で保管する（火災等、局所災害に有効）。

(2) 隔地保管

システムの復旧に必要なドキュメントを遠距離の場所で保管する（地震等、大規模災害に有効）。

保管場所の選定にあたっては、本番ファイル保管場所（現有システム保有場所）とリスク要因（火災、地震、停電等）を共有しないこと、及び被災時の復旧に際しての現有システムへのドキュメント移送時間の考慮等も含め総合的に判断することが望ましい。

削除: およ

また、保管を外部に委託する場合は信頼性、安全性、利用体制（保管されているドキュメントを必要時にいつでも利用可能か等）についても考慮する必要がある。

なお、定められた保管期間前の持出しにあたっては部門責任者の承認を得て行い、持出し記録については所定期間保存する必要がある。

2.　システムの復旧に必要なドキュメントのバックアップは定期的に整備する必要がある。また、重要な変更については、変更の都度整備する必要がある。

3.　災害時の復旧対応のために必要なドキュメント（ペーパーによらないドキュメント、例えばフロッピーディスク等も含む）としては、以下のようなものが考えられる。

(1) 基本設計書、詳細設計書（フローチャート、ファイルレイアウト、トランザクションコード、システムプログラム説明等）

(2) オペレータ指示書

(3) ユーザーマニュアル

(4) オペレーティングシステムのオプションと変更点

(5) システム構成（ハード及びOS）
(6) ネットワーク構成
(7) コンティンジェンシープラン（緊急時対応計画）

削除: およ

（参考）
　バックアップファイルの保管場所については、コンピュータセンターの立地条件に準じて考える必要があるため【設 1】を参照のこと。

2　運用管理

削除: （Ⅲ）

(10) 帳票管理

削除: 10.

帳票の不正使用、内容漏洩を防止するため、重要な帳票は管理方法、廃棄手続きを明確にすることが必要である。

運用管理
帳票管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実25	未使用重要帳票の管理方法を明確にすること。

削除: 運　35

不正使用を防止するため、未使用重要帳票の在庫管理、及び廃棄は定められた方法によって行うこと。

削除: およ

1.　重要帳票とは、例えば社長印、頭取印等代表者印や社印の押印された領収証、支払通知書、証券等金銭を受領できる帳票、及び契約に係わる帳票、通帳・証書（預金通帳等）を指している。

削除: およ

2.　在庫管理、及び廃棄にあたっては、使用枚数、廃棄枚数等を管理することが必要である。管理方法の具体的事例として、以下のことが考えられる。

削除: およ

(1) 重要帳票は防火区画内の施錠可能なキャビネット等で保管、格納することが望ましい。防火区画がない場合は、耐火金庫、耐火キャビネット等で保管、格納することが必要である。

(2) 入出庫は責任者立会いのもとに行い、受渡簿等を使用し授受の記録を明確にする。

(3) 処理後は次により残存枚数を確認する。

残存枚数＝印刷前在庫枚数－印刷枚数－印刷失敗枚数－プリンター紙送り廃棄枚数

(4) 在庫は帳票・用紙在庫管理簿により記録・管理するとともに適宜在庫確認を行う。

3.　印刷ミス、印刷不鮮明、及び帳票改訂等による廃棄にあたっては、責任者が立ち会う等により裁断、焼却、溶解等を確認することが必要である。

削除: およ

運用管理
帳票管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実26	重要な印字済帳票の取扱方法を明確にすること。

削除: 運　36

不正使用を防止するため、重要な印字済帳票の受渡し、及び廃棄は定められた方法によって行うこと。

削除: およ

1.　ここでいう重要な印字済帳票とは、【運 35】にいう帳票に所定の事項が印字されたもの、顧客データ、取引情報等重要なデータが印字されたコンピュータセンターから配布された帳票、端末から出力された帳票、COM フィッシュ、及びマイクロフィルム等の媒体種別には係わらず、コンピュータの処理結果として作成されたすべてのものをいう。

削除: および

削除: および

2.　重要な印字済帳票の不正使用を防止するため、授受、廃棄は定められた方法によって特定者が行い、管理責任者等がその状況を確認できることが必要である。
　また、授受の過程で一時保管が必要な場合は、厳重に保管することが必要である。

3.　授受方法について
　印字された重要帳票の授受は、授受伝票、授受管理簿、発送管理表、印刷枚数一覧表等により確認することが必要である。

4.　管理方法について
　帳票を保管する場合、定められた場所に保管する。また、障害時・災害時に使用する帳票は、防火区画内の施錠可能なキャビネット等で保管することが望ましい。防火区画がない場合は、耐火金庫、耐火キャビネット等で保管することが必要である。

5.　廃棄方法について
　使用済みもしくは回収されたものの廃棄にあたっては、責任者が立ち会う等により、裁断、焼却、溶解等を確認することが必要である。

2　運用管理

削除: （Ⅲ）

(11) 出力管理

削除: 11.

出力情報の不正使用、漏洩等を防止し、機密性、プライバシー等を保護するため、出力情報の管理ルールを定め、遵守することが必要である。

運用管理
出力管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 27	出力情報の作成、取扱いについて、不正防止、及び機密保護対策を講ずること。

出力情報の改ざん、盗難、漏洩等を防止するため、作成、取扱い等にあたっては不正防止、及び機密保護対策を講ずること。

1. 重要な出力情報の作成、授受、保管、管理及び廃棄については、改ざん、盗難、漏洩等の不正防止対策、及び機密保護対策を講ずることが必要である。

ここでいう出力情報とは、帳票、COM フィッシュ、マイクロフィルム、磁気テープ、フロッピーディスク等の媒体種別には係わらず、コンピュータシステムの処理結果として作成されたすべてのものを指す。

2. 対策のポイントとしては、以下のようなものがある。
(1) 出力情報の作成手順は、不正を防止する内容である。
(2) 不正な複写、複製等を防止する対策を講ずる。
(3) 出力情報の機密度に応じて取扱者を限定する。

3. 対策の具体例としては、以下のようなものがある。
(1) 出力情報の作成手順と取扱い
① 端末、パソコン等への情報出力
・操作者のアクセス資格の確認ならびに使用機器に適用業務の設定を行う。
・長時間の継続表示は行わない。
・社外に設置した機器への情報出力は、取扱いルールを契約や取引規定等によって明確にしておく。
② コンピュータセンター処理における情報出力
・オペレーション指示書等により、出力処理を行う。
・複数のオペレータによるオペレーション作業を行う。
・オペレーション日報等に作業結果を記録する。
・出力情報を確実に依頼者に引き渡す。
・処理途中における機密の漏洩、紛失を防止するために、プリンターなどの使用する機器及び取扱者を限定する。
(2) 不正防止対策
① 端末、パソコン等への表示
・権限のない者による操作、画面の覗き込み、ハードコピー取得を防止する。
・長時間の継続表示は行わない。

削除: 運　37
削除: およ
削除: およ
削除: およ
削除: およ
削除: およ

② 出力情報のプリント
・プリント処理者を限定する。
・情報出力の量、範囲を限定する。
規定以上の部数、量が出力された場合に発見できるようにしておく。

(3) 複写、複製の取扱い
・重要なデータの複写、複製は記録を残す。

(4) 出力の記録
① 情報出力に関する記録を残しておく。
② ネットワーク等を介する端末、パソコンへのデータ出力の記録を取得しておく。
③ 出力記録を作成する。項目例としては以下のようなものがある。
・処理業務
・処理日時
・処理結果（正常、異常）
・処理担当者
・処理依頼者
・出力量

(5) 出力情報のチェック
① 誤った処理が行われていないことを確認する。
② 確認項目の例としては、以下のものがある。
・レコードID
・パスワードによる資格確認
・データ件数
・レコード項目の合計（トータルチェック）

(6) 保管と廃棄
① 責任者を定める。
② 保管場所、及び管理方法を定める。
③ 廃棄方法を定める。
【運36】参照のこと。

削除: およ

（参考）
平成17年4月に「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（以下、e-文書法）が施行された。
e-文書法の施行により、それまでの法令で書面による保存を義務づけられていた文書が原則として電子データによる保存を容認されることとなった。
具体的に電子データによる保存が認められる対象の文書と保存方法は、保存を要求しているそれぞれの法令の主務省令で指定されるので、文書ごとに確認が必要である。
保存方法を要求する例としては、電子署名【技35】やタイムスタンプを必要とする文書や、紙文書を電子化する際のイメージスキャナの解像度を指定している文書があげられる。
なお、電子署名が必要な場合においては、署名の有効期限に留意する必要がある。
（注）タイムスタンプ：電子データが特定時刻より前に存在したことの証明と、その内容が当該時刻以降に変更・改ざんされていないことを証明するための技術。

2　運用管理

削除: （Ⅲ）

(12) 取引の管理

削除: 12.

端末機操作による不正、不当取引を防止するため、取引の操作内容を記録・検証することが必要である。また、顧客からの届出の受付体制の整備も必要である。

運用管理
取引の管理

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実 28	各取引の操作権限を明確にすること。

削除: 運　38

端末機操作による不正、不当取引を防止するため、取引内容ごとに端末機操作者等が操作できる権限の範囲を明確にすること。

1.　不正、不当取引を防止するため、取引の重要度等により端末機操作者等が操作できる権限の範囲を明確にすることが必要である。

　また、営業店以外の場所で 1 人で端末機操作が行える渉外端末等については、権限の範囲を明確にしておくことが特に重要である。

2.　異例取引を行う場合には、オペレーションに先立ち、当該取引権限保持者の承認を得ることが必要である。

運用管理
取引の管理

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実 29	オペレータカードの管理を行うこと。

削除: 運　39

端末機操作による不正取引を防止するため、オペレータカードは管理者を定め管理すること。

1. オペレータカードは端末機の操作にあたり操作権限者であることを確認するためのものであり、ここではオペレータキー、ID 等を含むものとする。

2. オペレータカードの管理は、以下のような方法によって行うことが考えられる。
(1) オペレータカードの管理者を明確にするとともに端末機操作者にオペレータカードを貸与する場合は貸与簿等により管理する。
(2) 異例取引を実行できる役席カード（監査カード）は役席者が管理し、使用記録を残す。
(3) 有資格者が使用資格を失った場合、その者に貸与したオペレータカードは速やかに回収する。

3. ID 等の管理は、以下のような方法によって行うことが考えられる。
(1) ID 等の登録、変更、抹消に際しての依頼手続きを明確にしておく。
(2) ID 等の登録、変更、抹消の処理にあたる責任者を明確にするとともに管理簿等により管理する。
(3) 有資格者が使用資格を失った場合、その者に付与されていた ID 等は速やかに抹消する。

運用管理
取引の管理

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実 30	取引の操作内容を記録・検証すること。

削除: 運　40

端末機操作による不正取引を防止するため、取引明細表、端末機操作記録等により、取引内容が検証できる体制を整備すること。

1.　取引内容等が記録された端末機のジャーナル、センターから還元される取引明細表等を使用した検証方法を定めておくことが必要である。

2.　具体的事例としては、以下のようなものがある。

(1) 端末機操作者等を記録する措置を講ずる。

端末機操作記録等に記録する内容として、取引内容のほか以下のような項目が考えられる。

①　端末機操作者
②　端末番号
③　処理通番
④　処理時刻

端末機操作記録等とは、営業店における伝票、端末機のジャーナル、コンピュータセンター及び営業店におけるジャーナルファイルなどが考えられる。

削除: およ

なお、端末機から入力された取引の正当性を検証するため、取引通番の管理を行うことが考えられる。

(2) 異例取引は取引記録を当該取引権限保持者が検証する。

検証の方法としては、以下のような方法がある。【技 47】

①　還元帳票による方法
②　オンライン照会による方法
③　モニター専用（指定）端末による方法

(3) 端末機操作記録等の保存期間を定め保存する。

運用管理
取引の管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 31	顧客からの届出の受付体制を整備し、事故口座の管理を行うこと。

削除: 運　41

事故による不正使用を防止するため、口座とリンクして顧客資産の移動を可能とする機器及び媒体の盗難等の届けを受け付けられる体制を整備すること。また、事故届のあった口座の管理は定められた方法により行うこと。

削除: およ

1.　「偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律」（以下、預金者保護法）により、預金者は真正カード等が盗取されたと認めた後、速やかに、当該金融機関に対し盗取された旨の通知を行うことが求められている。

金融機関等においては、顧客からの届出を速やかに受け付ける体制を整備し、事故による不正使用を防止することが必要である。

なお、顧客の不安を防ぐためには、届出の受付は有人対応とすることが望ましい。

ここでいう事故とは、金融機関等が顧客に提供した機器やICカード、磁気ストライプ付カード、通帳、印鑑、証書、証券等の盗難、紛失等を指している。

（参考1）
預金者保護法
第五条（盗難カード等を用いて行われた不正な機械式預貯金払戻し等の額に相当する金額の補てん等）　預貯金者は、自らの預貯金等契約に係る真正カード等が盗取されたと認める場合において、次の各号のいずれにも該当するときは、当該預貯金等契約を締結している金融機関に対し、当該盗取に係る盗難カード等を用いて行われた機械式預貯金払戻しの額に相当する金額の補てんを求めることができる。
一　当該真正カード等が盗取されたと認めた後、速やかに、当該金融機関に対し盗取された旨の通知を行ったこと。
二　当該金融機関の求めに応じ、遅滞なく、当該盗取が行われるに至った事情その他の当該盗取に関する状況について十分な説明を行ったこと。
三　当該金融機関に対し、捜査機関に対して当該盗取に係る届出を提出していることを申し出たことその他当該盗取が行われたことが推測される事実として内閣府令で定めるものを示したこと。

2.　事故届を受け付けた場合は、受付時刻等を記録しておくとともに、直ちに登録管理することが必要である。なお、盗難等の電話連絡を受けた場合、書面による届出を受領するまでの間、

適切な措置を講ずることのできる体制を整備しておくことも必要である。【技 39】

3.　夜間、休日においても CD・ATM 等のサービス提供時間帯においては、例えば管理センター等において顧客からの届出を受け付け、即時に支払停止等の処置を行う必要がある。

また、CD・ATM 等のサービス提供時間帯外に顧客からの届出を受け付けた場合は、CD・ATM 稼働開始前までに支払停止等の処置が必要である。

なお、個別金融機関が受け付けしない時間帯の受付窓口を、共同で運営する方式もある。

（参考 2）

預金者保護法第五条第一項において、預金者が被害額の補償を受けるための条件として、『当該真正カード等が盗取されたと認めた後、速やかに、当該金融機関に対し盗取された旨の通知を行ったこと。』が定められており、金融機関においては、預金者から速やかに通知を受けるための体制を整備することが、立法過程や、金融庁「偽造キャッシュカード問題に関するスタディグループ」の議論等において求められている。

「偽造キャッシュカード問題に関するスタディグループ最終報告書」

http://www.fsa.go.jp/

4.　事故登録等の解除にあたっては、規定や事務手続き上でも問題のないことを確認する等、特に注意を払うことが必要である。

5.　事故届の受付窓口が、事務センター、コンピュータセンター、及び外部委託先である場合も同様の措置を講ずることが必要である。

削除: およ

6.　顧客に対し、事故届の受付窓口（連絡先電話番号等）を周知する必要がある。

周知方法としては以下のようなものがある。

(1) 配布パンフレット、ホームページ、店頭ポスター等に掲載

(2) カード、通帳等に掲載

7.　事故届の受付窓口を電話会社の電話番号案内サービスに登録する際には、オペレータが検索しやすいように適切な名称で連絡先を登録することが必要である。

参照法令	偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律（平成 17 年法律第 94 号）

運用管理
取引の管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 32	機器および媒体の盗難、破損等に伴い、利用者が被る可能性がある損失及び責任を明示すること。

削除: 運　42

削除: およ

利用者に責任と注意を喚起するため、電子的価値を蓄積する媒体、及び通信等に使用する機器の盗難、破損等に伴い、利用者が被る可能性がある損失、及び利用者側の責任についてもわかり易く明示すること。

削除: およ

削除: およ

1.　電子的価値を蓄積する媒体等の紛失、盗難、破損に関し、利用者が被る可能性のある損失及び責任を利用者に対して明示すること。

削除: およ

2.　明示する場所としては、以下のようなものがある。
(1) 契約時の取引規定
(2) 電子的価値を蓄積する媒体の裏面

3.　明示する項目としては、以下のようなものがある。
(1) 電子的価値の保証について
(2) 紛失、盗難、破損時の届出について
(3) 盗難にあった媒体・機器により発生した損害に対する責任について

2　運用管理

削除: （Ⅲ）

(13) 暗号鍵の管理

削除: 13.

金融機関等が暗号鍵を管理する場合には、情報漏洩や不正使用を防止するために登録･変更手順を明確にし、厳正な管理を行う必要がある。

運用管理
暗号鍵の管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実33	暗号鍵の利用において運用管理方法を明確にすること。

削除:　運　43

不正行為を防止するため、暗号鍵の利用において暗号鍵の生成、配布、使用及び保管等に係わる手続きを定めておくこと。また、その管理書類等は役席者が厳重に管理すること。

削除: およ

1.　金融機関等で利用する暗号鍵のユーザーへの配布と使用、鍵の紛失・損失時の回復、鍵の回収、有効期限等について手続きを定めておくことが必要である。

2.　金融機関等で利用する暗号鍵（共通鍵暗号方式あるいは公開鍵暗号方式の秘密鍵）において、鍵の生成、配布、保管、失効、更新、廃棄等に係わる作業が必要な場合は、それらの処理が円滑かつ適正に行われるために作業の手続きを定めておくことが必要である。また、その作業記録等の管理書類等は、不正行為への悪用を防止するため、役席者が厳重に管理することが必要である。

なお、暗号鍵失効後の保存が必要な場合は、保存についての手続きも明確にし、保存に関する管理書類等も役席者が厳重に管理することが必要である。

3.　生成、配布、保管、失効、更新、廃棄、保存等の手続きの明確化においては、以下の点に留意すること。

(1) 作業は、権限をもった特定の者のみが行えること。

(2) 作業にあたっては、役席者の承認を得るとともに誤操作防止等のため権限をもった複数の者が実施することにより相互牽制体制をとること。

(3) 作業の記録（作業者、作業日時、作業内容等）を残し、一定期間保管すること。

2　運用管理

削除: （Ⅲ）

(14) 厳正な本人確認の実施

削除: 14.

ネットワークを介した取引が増加の一途をたどり、ほとんどの業務が可能となりつつある。これらの業務は非対面であることから、特に取引の始まりである口座開設時の本人確認や個々の取引における本人認証が重要となる。

運用管理
厳正な本人確認の実施

適　用　区　分				
共	セ	本	提	ダ
		◎		

実 34	本人確認を行うこと。

削除:　運　44

口座開設等を行う場合は適切な方法により本人確認を行うこと。

1. インターネットバンキング等の非対面取引において、口座開設等を行う場合は不正取引防止のために、以下の手順等により本人を確認することが必要である。
(1) 公的証明書の原本またはコピーの送付を受ける。
(2) 顧客の住居に取引関連書類（キャッシュカード等）を書留郵便等で返送する。

2. 利用者からの暗証番号等の照会において、対面・非対面にかかわらず、十分な本人確認ができない場合には、直ちに回答するのではなく、別途、登録されている顧客情報をもとに、金融機関から電話連絡や書留郵便等の手段で本人であることを確認したうえで、回答する必要がある。

3. 不正取引を防止する策として、【運 103】を参照のこと。

参照法令	犯罪による収益の移転防止に関する法律 （旧 金融機関等による顧客等の本人確認等及び預金口座等の不正な利用の防止に関する法律）

運用管理
厳正な本人確認の実施

適　用　区　分				
共	セ	本	提	ダ
◎				

実 35	CD・ATM 等の機械式預貯金取引における正当な権限者の取引を確保すること。

削除:　運　44-1

不正払戻し防止のための措置を講ずることにより機械式預貯金払戻し等が正当な権限を有する者に対して適切に行われることを確保すること。

1. 「偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律」（以下、預金者保護法）により、できるだけ速やかに認証の技術の開発並びに情報の漏洩の防止、及び異常な取引状況の早期の把握のための情報システムの整備その他の措置を講ずることにより、機械式預貯金払戻し等が正当な権限を有する者に対して適切に行われることを確保することが求められている。

削除: およ

対策としては、以下のようなものがある。

(1) 認証技術の開発としては、IC カード、生体認証技術の導入等がある。【技 35】

(2) 情報漏洩の防止としては、自動機器室等における覗き見防止設備の設置、IC カードの導入、CD・ATM の伝送データの暗号化等がある。【設 113】【設 137】【技 29】【技 35】

(3) 異常な取引状況の早期の把握のための措置としては、異常取引検知技術の導入等がある。【技 46】

(4) その他不正払戻し防止の措置としては、カードの偽造防止対策や携帯電話による CD・ATM の取引ロック機能の導入等がある。【技 38】【技 40】

（参考）
預金者保護法
第九条第一項（偽造カード等又は盗難カード等を用いて行われる不正な機械式預貯金払戻し等の防止のための措置等）
金融機関は、偽造カード等又は盗難カード等を用いて行われる不正な機械式預貯金払戻し等の発生を防止するため、できるだけ速やかに、機械式預貯金払戻し等に係る認証の技術の開発並びに情報の漏えいの防止及び異常な取引状況の早期の把握のための情報システムの整備その他の措置を講ずることにより、機械式預貯金払戻し等が正当な権限を有する者に対して適切に行われることを確保することができるようにするとともに、預貯金者に対するこれらの措置についての情報の提供並びに啓発及び知識の普及、容易に推測される暗証番号が使用されないような適切な措置の実施その他の必要な措置を講じなければならない。

参照法令	偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律（平成 17 年法律第 94 号）

2　運用管理

削除: （Ⅲ）

(15) CD･ATM 等及び無人店舗の管理

削除: 15.

CD･ATM 等及び無人店舗の円滑な稼働ならびに安全対策のため、必要な措置を講じておくとともに、犯罪発生時や障害時・災害時等の対応方法を明確にしておく必要がある。なお、無人店舗とは CD･ATM 等の無人運用を行う店舗をいう。

削除: およ

削除: およ

運用管理
CD・ATM 等および無人店舗の管理

適　用　区　分				
共	セ	本	提	ダ
		◎	◎	

実 36	運用管理方法を明確にし、かつ不正払戻防止の措置を講ずること。

削除:　運　45

CD・ATM および無人店舗の安全性を確保し、円滑に稼働させるため、運用管理方法を明確に定めること。

1.　CD・ATM 等は設置場所や所有者、運用方法、稼働時間によりさまざまな運用形態が考えられるため、それぞれの運用形態に合わせた運用管理方法を定めておくことが必要である。

具体的項目としては、以下のようなものがある。

(1) 現金の装填手順
(2) CD・ATM 等の操作記録の保存（保存期間を定めておく）
(3) 故障時の対応方法
(4) 防犯監視体制

防犯監視体制については、【設 113】【設 137】【運 47】を参照のこと。

2.　店舗外 CD・ATM 等については、母店等での運用管理方法を定めておくことが必要である。

3.　無人店舗では以下のような事項を考慮して、運用管理方法を定めるとともに、関係者に周知徹底することが必要である。

(1) 現金切れを極力少なくするために、適正量の現金を装填しておく必要がある。
(2) ジャーナル等、CD・ATM 等で必要とする用紙等についても十分に装填しておく必要がある。
(3) 現金切れ、機械故障等に備え、無人店舗での機械設置は複数台とすることが望ましい。
(4) 現金切れ、機械故障等に備え、近隣無人店舗の地図をコーナーに掲示することも考えられる。

4.　犯罪に対しては、防犯カメラおよび防犯ビデオが抑止策となるとともに、犯罪解決には有効な手段であるため、その運用、管理方法を明確にし実施することが必要である。【設 103】

なお、ビデオとジャーナルの時刻の不一致度合いを極力少なくするため、定期的に時刻合わせを実施するとともに、テープ等の記録媒体の交換やレンズの清掃を実施することが望ましい。

また、犯罪解決や同様の被害防止の観点から、犯罪手口の特定化のために防犯カメラ、防犯ビデオおよび CD・ATM ジャーナル等の提供など、積極的な捜査協力が必要である。加えて、捜査依頼に対して迅速かつ適切に協力する観点から、あらかじめ捜査協力に関する手順等を定め、従業者に教育・周知しておくことが必要である。

（参考）
捜査協力時の個人データ提供についての根拠は
・令状による捜査に協力する場合：個人情報の保護に関する法律　第 16 条第 3 項第 1 号、第 23 条第 1 号
・任意捜査に協力する場合：個人情報の保護に関する法律　第 16 条第 3 項第 4 号、第 23 条第 4 号を参照のこと（個人情報の目的外利用の制限の除外事項として、規定あり）

5. 防犯カメラ、防犯ビデオおよび CD･ATM ジャーナルの運用、管理に関して明確にする項目としては、以下のようなものがある。
(1) CD･ATM ジャーナルおよびテープ等の保存期間および保存場所
(2) 責任者
(3) 運用方法
防犯ビデオは顧客からの届出状況等に応じて一定期間の保存を考慮することが望ましい。例えば警察庁の「金融機関の防犯基準」においては「少なくとも、3 月を下回るような短期間の保存は避けること」の記述がある。
なお、ハードディスク等を使用して集中管理する場合は、捜査協力を想定してダビングの容易性についても考慮することが必要である。

6. 防犯カメラおよび防犯ビデオに関する運用実施策としては、以下のようなものがある。
(1) 金融機関等による運用および管理
(2) 警備会社等の外部委託を利用した運用および管理
また、コンビニ ATM の防犯カメラおよび防犯ビデオは、コンビニエンスストアで運用および管理を行う場合もある。

7. ATM 利用明細書から、口座番号を他人に知られないための対策を講ずる必要がある。
具体的には、以下のようなものがある。
(1) ATM 利用明細書の口座番号等の一部あるいはすべてを非表示とする。
(2) 照会等の一部取引において ATM 利用明細書を出力しない。
(3) ATM 利用明細書を持ち帰るように注意喚起する。
(4) ゴミ箱を設置する場合は、鍵やシュレッダー付のものを選択する。
(5) コンビニ ATM に設置したゴミ箱に捨てられた ATM 利用明細書の扱いについて、関係者間で確認する。

運用管理
CD・ATM 等および無人店舗の管理

適　用　区　分				
共	セ	本	提	ダ
		◎		

実37	監視体制を明確にすること。

削除:　運　46

無人店舗における異常状態を発見するため、監視体制を明確にすること。

1. 無人店舗における異常状態を発見するため、管理センター等で監視することが望ましい。
   管理センター等での対応内容としては、以下のようなものがある。
   (1) CD・ATM 等の障害、破壊等のオンライン監視
   (2) 直通電話による顧客の操作誘導
   (3) 警備会社への必要な対応依頼（障害時顧客対応、犯罪発生時対応等）
   (4) 犯罪発生時の警察への通報
   (5) 障害・災害発生時における母店等関係者への連絡

2. 管理センター等を設置できない場合、並びに管理センターでの監視では不十分と考えられる場合には、代替策として警備会社による定期的巡回等の方法が考えられる。
   巡回にあたっては、ATM 設置場所の環境を考慮して、巡回時間を特定されないよう配慮することが必要である。また、設置場所等の環境を考慮して、巡回・点検頻度を上げることが望ましい。

3. なお、最低限の措置として顧客が連絡を取れる先を表示しておくとともに、顧客からの連絡を受ける責任者を定めておき、連絡が必ず取れるようにしておくことが必要である。

運用管理
CD・ATM 等および無人店舗の管理

適　用　区　分				
共	セ	本	提	ダ
		◎		

実 38	防犯体制を明確にすること。

削除:　運　47

無人店舗における犯罪を防止するため、防犯方法および犯罪発生時の対応方法を明確にすること。

1.　無人店舗では、CD・ATM 等の破壊による現金盗難や隠しカメラ設置による暗証番号盗撮等の犯罪が行われる可能性が高くなるため、周辺地域の犯罪発生状況を把握することに努め、事前に防犯方法および発生時の対応方法を明確に定めておくことが必要である。

(1) 防犯具体例としては、以下のようなものがある。

①　契約された警備会社による巡回

②　警察にあらかじめ依頼することによる警察官の巡回

③　防犯カメラによる監視　【設 103】

なお、巡回時に CD・ATM 機、その周囲および出入口付近に隠しカメラやカード情報の不正な読取装置等の不審な装置がないか確認することが必要である。また、ゴミ箱が荒らされていないか確認することも対策として有効である。

(2) 犯罪発生時の対応具体例としては、以下のようなものがある。

①　警報装置による警報鳴動（自動鳴動、遠隔監視による鳴動指示等が考えられる）

②　警備会社、警察等への管理センター等からの連絡

③　警備員等の迅速な駆けつけ

④　防犯ビデオへの犯人像の記録　【設 103】

2.　現金装填を行う場合には必ず複数名により行うことが必要である。

また、職員が行う場合には警備会社等に立会いを依頼することも有効である。

現金装填は直接現金が人目に触れない方式とし、短時間でできるようにすること。

CD・ATM 等は後面装填型が望ましいが、前面装填型 CD・ATM 等の現金装填については、装填者の背後が無防備になるため、特に配慮が必要である。

運用管理
CD・ATM 等および無人店舗の管理

適　用　区　分				
共	セ	本	提	ダ
		◎		

実 39	障害時・災害時の対応方法を明確にすること。

削除:　運　48

無人店舗の円滑な運営のため、障害時・災害時の対応方法を明確にすること。

1.　無人店舗における障害時の対応方法を明確にしておくことが必要である。
　具体的に検討、整理しておく項目としては、以下のようなものがある。
(1) 利用客への状況連絡方法、説明方法
(2) 利用客へのカード等の返却方法
　自動返却、職員、警備会社等による個別手作業返却が考えられる。
(3) 特定店に障害が限定されている場合における他店への誘導
(4) 自社ホストに係わる障害でない場合に最寄の CD・ATM への誘導
(5) 回復後のサービス時間延長への対応
(6) 関係者（営業店、本部、コンピュータセンター、警備会社等）の招集方法および役割

2.　災害時における対応方法についても、障害時の対応方法を参考にして検討、整理しておくことが必要である。

運用管理
CD・ATM 等および無人店舗の管理

適　用　区　分				
共	セ	本	提	ダ
		◎		

実 40	関係マニュアルの整備を行うこと。

削除:　運　49

無人店舗の円滑な運営、安全確保のため、各種対応を想定した関係マニュアルを整備しておくこと。

1. 無人店舗での各種対応を想定した関係マニュアルを整備しておくことが必要である。
   マニュアルの具体例としては、以下のようなものが考えられる。
   (1) 管理センター等での監視対応マニュアル
   (2) 防犯マニュアル
   (3) 障害時対応マニュアル
   (4) 災害時対応マニュアル
   (5) 母店における店舗外 CD・ATM 等管理マニュアル
   (6) 警備会社、警察等との連絡方法マニュアル
   (7) 現金、ジャーナル等の装填マニュアル

2. マニュアルは本部、コンピュータセンター、管理センター、営業店、警備会社等にそれぞれ必要なものを作成し、常備しておくことが必要である。

2　運用管理

削除: （Ⅲ）

(16) 涉外端末の管理

削除: 16.

安全性の確保および処理の円滑化のため、涉外端末等の可搬型端末は、定められた方法によって管理することが必要である。また、涉外端末の不正使用の防止および破損、紛失、盗難等に備えた対策を講じておく必要がある。

運用管理
涉外端末の管理

適　用　区　分				
共	セ	本	提	ダ
		◎		

実 41	運用管理方法を明確にすること。

削除:　運　50

涉外端末の不正使用を防止するため、運用管理方法を明確にすること。

1.　ここでいう涉外端末は、ハンディ端末、スマートデバイス、携帯型パソコン等可搬型端末をいう。

2.　涉外端末には各々識別 ID を付与し、その取扱者を明確にする必要がある。

3.　涉外端末は可搬型の端末であるため、定められた場所に保管し、その保管方法を明確にする必要がある。　【運 57】

4.　盗難、紛失等を早期に発見するため、涉外端末の管理者を明確にし、定期的に台数の確認をする必要がある。また、盗難、紛失等の届出・受付体制を整備しておく必要がある。　【運 3】

5.　涉外端末が使用不可能になった場合に備え、取引の記録またはデータファイルのバックアップを取得する必要がある。
　バックアップの方法としては、以下のようなものがある。
(1) ジャーナル（明細票等）の保管
(2) 記録媒体によるバックアップの取得

6.　涉外端末の盗難、紛失等が発生した場合に備え、データ保護のための対策を講じておく必要がある。
　データ保護のための対策としては、以下のようなものがある。
(1) 起動時に識別コード、パスワード等の入力、または特殊操作による起動等により不正アクセスを防止する。
(2) 端末内または着脱可能な記録媒体にあるデータファイルは、その重要度に応じて暗号化またはデータファイルへのパスワード設定など、適切な漏洩防止策を講ずることが望ましい。【技 28】
(3) データファイルを端末に保存する際は、その重要度に応じた保管・管理方法を明確にする必要がある。　【運 25】

7.　データ漏洩、不正アクセス、コンピュータウイルスの侵入等を防止するため、社内ネットワークへの接続やリモートアクセスの利用は、定められた方法によって行うことが必要である。
(1) 外部接続の運用管理については、【運 56】参照のこと。
(2) ウイルス対策については、【運 30】参照のこと。

8. 端末機器操作の権限管理については【運 38】を参照のこと。

9. 使用しない機能は停止、もしくは使用を制限するとともに、使用しないソフトウェアを搭載しない等、セキュリティを考慮した設定とする必要がある。

10. 涉外端末の廃棄方法を明確にする必要がある。 【運 66】

（参考）

1. スマートデバイスの業務利用に関わる考慮点

スマートデバイスは、業務利用で必要となるセキュリティ機能を実装することが困難な場合がある。また、パソコンと異なる「機器の特性」、「アプリケーションの特性」、「ネットワークの特性」を理解して以下の点を考慮することが求められる。

(1) 端末へのデータ保存

導入しているアプリケーションのデータ保存の仕組みを理解し、情報漏洩の原因とならないよう考慮する。例えば、利用者がインターネット上のサービス等を利用する場合、端末データがサービス等に同期されることで、外部環境にもデータが保存され、情報が漏洩するリスクがある。

(2) MDM（Mobile Device Management）の導入

スマートデバイスを制御する仕組みとして、MDM があり、デバイスの利用制限、アプリケーションのインストール制限、端末の状態監視等の管理を行うことができる。このような MDM を導入する場合には、サービス機能が異なるため、提供される機能を調査し、自社の要件を満たす最適な製品を選択する。

(3) 紛失・盗難対策

紛失や盗難時に MDM 等の機能を利用した遠隔操作によるデータ消去の対策はあるが、通信圏外や SIM カードが抜き取られた場合には、遠隔操作でデータ消去はできないことを考慮した運用が求められる。

(4) 機種または OS の選択

スマートデバイスは機種や OS の種類が様々にあり、システムやセキュリティに関わる仕様も一様ではないため、会社（もしくは組織）のセキュリティポリシーに基づき、最適な機種・OS を選択することが求められる。例えば、パソコンと異なり脆弱性に対するセキュリティパッチの適用の遅れも発生しており、セキュリティパッチの適用等が十分な機種を選択することが望ましい。

(5) 通信機能の利用

スマートデバイスは通信機能を備えており、企業内無線 LAN、携帯電話回線網、または公衆無線 LAN 等の複数の経路で社内ネットワークへアクセス可能であり、不正認証（なりすまし）、盗聴、情報漏洩といったセキュリティ上の脅威に対して、経路別に様々な対処（無線 LAN 使用時に利用可能なアクセスポイントを制限する等）の考慮が求められる。

（【技 29】【技 35】【技 43】参照）

(6) 抗ウイルスソフト

抗ウイルスソフトは、コンピュータウイルス等不正プログラムの防御対策として一定程度有効であるが、アプリケーションの一種として動作をしており、管理者権限を持たないため、システム領域における対策は困難であり、パソコン用の抗ウイルスソフトと同等の効果は期待できないことを理解した運用が求められる。

2. スマートデバイス特有のセキュリティに関わる留意点

自社のセキュリティポリシーに基づいて、利用する業務や保持するデータの重要性に応じて、会社（もしくは組織）として必要なセキュリティ対策を講じることが重要である。

(1) テザリング

スマートデバイスの一部には、スマートデバイスを無線ネットワークのルータとして利用し、パソコン等をインターネットに接続させるテザリングという機能を有する機器がある。社内ネットワークへの接続を承認されたスマートデバイスのテザリング機能を有効とした場合、未承認のパソコン等が社内ネットワークに接続されるリスクがある。

(2) 管理者権限の不正取得（特権解除）

通常、スマートデバイスの利用者は管理者権限を有しないが、OS のセキュリティホールを突くなどの方法で、管理者権限を不正に取得することを特権解除という。これが行われた機器は、コンピュータウイルスの侵入、端末 ID やユーザーID 等の認証子が盗難・改ざんされる等のリスクが増大する。

(3) アプリケーションの Web サイトからの導入

スマートデバイスへのアプリケーション等の導入は、パソコンと異なり Web サイトから行われることが多い。Web サイトからアプリケーションを導入する場合、アプリケーションの安全性が審査されていないケースがあるため、コンピュータウイルスに感染するリスクがある。【技 49】（参考 1）「コンピュータウイルス対策の例」を参照し、対応することが求められる。

(4) 組込み機能に対する制御

スマートデバイスには、カメラ、GPS 等の組込みの機能がある。これら機能の使用により、利用者の意図しない操作・動作による情報漏洩のリスクがある。

3. スマートデバイスのセキュリティ対策や利用者に周知すべき情報を公開しているガイドラインを以下に示す。

・「スマートフォン&タブレットの業務利用に関するセキュリティガイドライン【第一版】」（2012 年 10 月 26 日）

http://www.jssec.org/activities/index.html

一般社団法人 日本スマートフォンセキュリティ協会

なお、スマートデバイスの業務利用の 1 つの形態として、個人所有の端末機器を業務に利用する「BYOD（Bring Your Own Device）」がある。ただし、BYOD が原因で情報漏洩が生じる可能性もあるので、個人所有の端末を業務で利用する場合は、十分な検討が求められる。

2　運用管理

削除: （Ⅲ）

(17) カード管理

削除: 17.

カードの不正使用を防止するため、カードの発行、保管および交付は、特定者が定められた方法によって行うことが必要である。また、指定された口座に対するカード取引監視方法を明確にすることが必要である。

なお、金銭の支払、貸出、情報の授受等に係わる呼称の異なるカードの管理についても本基準項目を準用し、状況に即した安全性を確保することが必要である。さらに、顧客に対してカード犯罪に対する注意喚起を行うことも必要である。

運用管理
カード管理

適　用　区　分				
共	セ	本	提	ダ
	◎	◎	◎	

実 42	カードの管理方法を明確にすること。

削除:　運　51

安全性の確保及び処理の円滑化のため、カードの発行、保管、交付、回収及び廃棄は定められた方法によって行うこと。

1.　不正行為を防止するとともに、不正行為に対する牽制効果を目的として、カードの発行（再発行も含む）、保管、交付、回収及び廃棄は定められた方法によって行うことが必要である。

2.　カード発行責任者及び担当者の特定

カード発行業務に携わる責任者及び担当者を特定することが必要である。

3.　カード発行依頼書に暗証番号が記入されている場合は、役席者が厳重に当該依頼書を管理することが必要である。

4.　カードの発行

(1) 発行依頼書に基づき作成する場合の確認事項としては、以下のようなものが考えられる。

①　発行カードの正当性（エンコード、エンボス内容）の確認

②　発行カード枚数とカード発行依頼枚数の一致確認

(2) カード発行時に暗証番号の登録が必要な場合は、暗証番号の漏洩防止に万全の措置を講ずることが必要である。

漏洩防止措置の例としては、以下のものがある。

①　登録時等にやむを得ず暗証番号の印字が必要となるような場合は、登録票に印字し管理を厳重に行う。

②　金融機関職員が暗証番号登録に介在しない方式とする。具体的な方法として以下の例がある。

1) 顧客が暗証番号を直接キーパッドから入力する方法

2) 顧客が暗証番号を設定するのではなく、金融機関が初期暗証番号を割り当て顧客に暗証番号を変更させる方式

5.　カードの保管管理

カードの保管管理内容として、以下のようなものが考えられる。

(1) カード（未使用、送付待ち、郵送返却、廃棄待ち）は金庫または施錠可能なキャビネットに厳重に保管する。

(2) 未使用カードの授受は、授受簿等に記録し、その事実を明確にする。

(3) カード発行後は下記方法により在庫を確認する。
　在庫枚数＝作成前在庫枚数－作成枚数－作成失敗枚数

6. カードの交付方法

顧客へのカードの送付は、原則として書留等受領の記録が残る郵便物により行い、発送管理簿等に記録を残しておくことが必要である。なお、やむを得ず営業店外で作成したカードを営業店で顧客に対し交付する際は、カード作成部署から社内書留等重要物件送付方法によりカードの送付を受け、十分な本人確認を行い、授受の明確化（受領書等の徴求）を行った後に交付することが必要である。

また、金融機関から顧客に送付し、窓口で本人確認後に使用可能とすることや、店頭交付の際の複数職員によるダブルチェックも有効である。

7. 郵送返却カードの取扱い

書留等で郵送したカードが返送されてきた場合、役席者が保管管理簿等を用いて厳重に管理するなど、定められた方法で管理することが必要である。

なお、返却理由が「居所不明」のものは、原則として廃棄処分することが必要である。

8. 廃棄方法

作成ミスやデザイン変更等により使用できなくなったカード及び長期未交付または口座解約等で回収したカードは、責任者立会いのもとで裁断、焼却等により廃棄する等、廃棄手続きを明確にしておくことが必要である。

9. 暗証番号の変更

顧客本人が暗証番号を安全かつ容易に変更できる方法を顧客に明示することが必要である。暗証番号の変更の方法としては、以下のようなものがある。

(1) 本部・営業店等の届出用紙等により、顧客の本人確認のうえ、用紙により申請する方法
(2) 本部・営業店等の CD・ATM 等により、顧客本人が暗証番号を直接入力する方法

10. 顧客への注意喚起

顧客からカードの発行依頼があった場合、他人にわかり難い暗証番号を選定するように勧めることが必要である。その際、生年月日等の推測されやすいものを暗証番号として認めない仕組みがあることが望ましい。また、併せて暗証番号の重要性や適切な管理方法について説明するか、カード送付時に同様の内容を明示した文書を添付することが必要である。【運 51-1】

11. 非ゼロ暗証化カードの対応

磁気ストライプ上には、暗証番号並びに暗証番号が推測されるおそれのある情報は書き込まないことが必要である。

ゼロ暗証化されていない磁気キャッシュカードが残っている場合は、新規カードへの切替やゼロ暗証化の手続きを顧客に促す等の適切な処置を講ずること。

12.　テスト用カードの作成や使用にあたっては、その目的を明確にするとともに、カードの作成時や使用開始から終了まで管理する体制を整備することが必要である。

　なお、管理体制の整備にあたっては、管理者も含め相互牽制が働くようにしておくことが望ましい。

(参考)

　多機能カード発行においては、カードの盗難、破損等に伴い利用者が被る可能性がある損失等について、機能別にサービス提供者を特定するなど、責任の所在を明確化することが重要である。【運 42】

運用管理
カード管理

適　用　区　分				
共	セ	本	提	ダ
		◎	◎	

実 43	顧客に対して犯罪に関する注意喚起を行うこと。

削除:　運　51-1

顧客並びに取引の安全性を確保するため、犯罪に関する注意喚起を行うこと。

1.　顧客を狙った犯罪に対しては、サービスを提供する側の設備、運用だけでは限界があり、顧客に対する注意喚起も重要な犯罪抑止策となる。よって顧客に対して犯罪に対する注意喚起を行うことが必要である。

2.　カード取引等に関する犯罪の例としては以下のものがある。
(1) CD・ATM 利用後店舗内外で襲われる。
(2) 盗難カードや偽造カードにより預金を不正に引き出される。

3.　カードや暗証番号の適切な管理方法について顧客に注意喚起すること。喚起すべき事項としては以下のものがある。
(1) カードを安易に第三者に渡さないこと
(2) カード上に暗証番号を記入しないこと
(3) 他人に暗証番号を知らせないこと
(4) 推測されやすい暗証番号を使用しないこと
(5) キャッシュカードの暗証番号を他のパスワードと共用しないこと（貴重品ロッカー等のパスワードに使用しない等）
(6) 不特定多数の者が使用するパソコンでは金融機関との取引を行わないこと（スパイウェアにより暗証番号・パスワード等が盗まれる危険性がある）
(7) 警察官や金融機関の職員が、暗証番号等を直接顧客に照会することは無いこと（警察官や金融機関の職員を詐称し、暗証番号等を聞きだす犯罪行為があること）
(8) 暗証番号は定期的に変更することが望ましいこと
(9) ATM 利用明細書の取扱いに注意すること
その他最新の犯罪事例をもとに必要な対策を周知すること。

4.　CD・ATM 取引時の安全のため必要な事項を顧客に注意喚起すること。喚起すべき事項としては以下のものがある。
(1) 不審者の有無等、周囲の安全に気を配ること
(2) 暗証番号等の覗き見に注意すること
(3) CD・ATM 周辺に見慣れないカード読取機等があった場合には気を付けること

5.　不正使用の早期発見のため、定期的（できれば毎月）に残高照会や通帳記帳により取引内容を確認するよう顧客に推奨することが望ましい。

6.　顧客に対する注意喚起の方法としては、以下のものがある。
(1) 口座開設時に説明およびパンフレット等への明記
(2) 配布パンフレット、ホームページ、店頭ポスター、CD・ATM 画面等へ注意事項等の情報掲載
(3) DM 送付時に犯罪対処に関する情報を提供

7.　推測されやすい暗証番号を使用している顧客に対しては変更するよう、個別具体的に対応することが望ましい。対応方法の例としては以下のものがある。
(1) 窓口対応
(2) 電話対応
(3) ダイレクトメール　等
なお、ダイレクトメール等を用いる場合には、当該顧客が推測されやすい番号を使用しているという情報が漏洩するリスクを考慮することが必要である。対策の例としては、通知内容に口座番号を記載しないことがあげられる。

8.　推測されやすい暗証番号の例としては以下のものがある。
(1) 生年月日
(2) 自宅の電話番号
(3) 職場の電話番号
(4) 自宅の住所
(5) 自家用自動車のナンバー　等

（参考）
国会での審議によると、盗難カード等による被害の場合、暗証番号を生年月日等の推測されやすいものとしていただけで、直ちに預金者の過失を問うことはできないとしている。そのためには、まず、金融機関から預金者に対し、生年月日等の推測されやすい暗証番号から別の番号に変更するよう、複数回にわたる働きかけが行われることが前提となるとしている。加えて、この働きかけは、推測されやすい暗証番号を使用している預金者に対して、電話やダイレクトメール等により個別的、具体的に行う必要があり、ポスター等による預金者一般に向けた広報では、ここに言う働きかけには該当しないとしている。

参照法令	偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律（平成 17 年法律第 94 号）

運用管理
カード管理

適　用　区　分				
共	セ	本	提	ダ
	◎	◎	◎	

実 44	指定された口座のカード取引監視方法を明確にすること。

削除:　運　52

不正使用を防止するため、指定された口座のカード取引を監視できる方法を明確にすること。

1. ここでいう指定された口座のカード取引とは、犯罪に絡んで犯人の所在を把握するために捜査当局から依頼のあった口座のカード取引を指しているが、休眠口座についても監視対象とすることが望ましい。

2. 監視方法としては、当該口座に対しカード取引があった場合、取引のあった端末もしくは端末の設置場所を特定する情報等をコンソール上に表示するのが一般的である。
   なお、実際に取引のあった場合の連絡手続きを定めることも必要である。

3. 監視方法については、【運 60】参照のこと。

4. 監視機能については、【技 47】参照のこと。

2　運用管理

削除: （Ⅲ）

(18) 顧客データ保護

削除: 18.

金融機関等は、業務の性格上、顧客に関するさまざまなデータ（顧客データ）を取り扱うが、顧客データの取扱い・保護に関し、適切に対応していくことが必要である。

特に認証手段として生体認証を用いる場合は、生体認証情報の管理手順を定め、安全管理措置を講ずることが必要である。

運用管理
顧客データ保護

適　用　区　分				
共	セ	本	提	ダ
◎				

実 45	顧客データの保護策を講ずること。

削除: 運　53

顧客データを保護し、適正に利用するため、管理･取扱い方法を定めること。

1.　「顧客データ」とは、金融機関等が取引等において収集、蓄積し、業務上利用する顧客に関するすべての情報を意味する。

2.　金融機関等は顧客に関する厳密な守秘義務に基づき、顧客データの取扱いに関しては、管理責任者、管理方法および取扱い方法を定め適正に管理することが必要である。また、顧客データに関しては、【運 10、運 36、運 80、運 88】を参照のこと。

3.　不正アクセス等で顧客データが漏洩して顧客が被害を受けることを想定し、損害賠償責任等についての保険の適用を検討することが望ましい。

4.　機微（センシティブ）情報を取り扱う場合は、以下の点を考慮する必要がある。なお、生体認証情報については【運 53-1】を参照のこと。

機微（センシティブ）情報とは、「個人情報の保護に関する法律第２条第３項に定める要配慮個人情報並びに労働組合への加盟、門地、本籍地、保健医療及び性生活（これらのうち要配慮個人情報に該当するものを除く。）に関する情報（本人、国の機関、地方公共団体、個人情報の保護に関する法律第 76 条第１項各号若しくは個人情報の保護に関する法律施行規則第６条各号に掲げる者により公開されているもの、又は、本人を目視し、若しくは撮影することにより取得するその外形上明らかなものを除く。）」である。（個人情報保護委員会・金融庁「金融分野における個人情報保護に関するガイドライン」第５条）

削除:「政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報」で

削除: 6

(1) 各管理段階において、「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」の 1−2 および（別添 1）に掲げる措置を実施することが必要である。なお、各管理段階とは、「取得・入力」「利用・加工」「保管・保存」「移送・送信」「消去・廃棄」のことをいう。

(2) 機微（センシティブ）情報の「取得・入力」「利用・加工」「移送・送信」は、「金融分野における個人情報保護に関するガイドライン」第５条第１項各号に定める場合に限定すること。

削除: 6

(3) 各管理段階において取扱者、アクセス権限の設定は必要最小限に限定するとともに、「利用・加工」「保管・保存」「移送・送信」の各段階においてはそれを担保するアクセス制御を実施することが必要である。

(4) 「取得・入力」および「利用・加工」の段階にあたっては、本人同意が必要である場合に

は、機微（センシティブ）情報の利用目的および利用範囲について本人に明示し、同意を得ることが必要である。

(5) 機微（センシティブ）情報に該当する生体認証情報を取り扱う場合は上記(2)(3)(4)に加えて、【運 53-1】を実施することが必要である。

5. 匿名加工情報（匿名加工情報データベース等を構成するものに限る。）を作成するときは、個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）」の３－２に定める「匿名加工情報の適正な加工（法 36 条第１項関係）」に従い、当該個人情報を加工することが必要である。

参照法令	・個人情報の保護に関する法律 ・個人情報の保護に関する法律についてのガイドライン ・金融分野における個人情報保護に関するガイドライン ・金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針

運用管理
顧客データ保護

適　用　区　分				
共	セ	本	提	ダ
◎				

実 46	生体認証における生体認証情報の安全管理措置を講ずること。

顧客を認証する手段として、生体認証を用いる場合に、生体認証情報を安全に管理するための手順を定めること。

1. 本項の対象となる生体認証と生体認証情報は、以下のとおり。

生体認証　・・・生体認証情報を、本人の同意に基づき用いて、本人確認手段として実施する機械による自動認証。

生体認証情報　・・・機械による自動認証に用いられる身体的特徴の情報のうち、非公知の情報を、コンピュータ等で扱えるデータに変換したもの。

（ここで身体的特徴の情報は、「金融分野における個人情報保護に関するガイドライン」第5条の機微（センシティブ）情報に該当するもの。）

（注１）①　生体認証情報の例としては、静脈・虹彩等がある。

②　一方、公知な情報としては、一般的な顔写真等があげられる。（ただし、医療用に撮影された顔写真等は除く）

③　行動的特徴（キーストローク、筆順、筆速、筆圧、声紋等）は、非公知であるとしても、身体的特徴の情報ではないため、本基準でいう生体認証情報には含まない。

（注２）一般的に、「個人の身体的特徴及び行動的特徴を識別情報とした本人確認技術」や「身体的特徴及び行動的特徴の情報そのもの」を「バイオメトリクス」と呼ぶことがある。本項目においては、この概念から対象を上記のとおり絞って、「生体認証」および「生体認証情報」という用語を用いる。

2. 生体認証情報を取り扱う各段階について、安全に管理するための手順を定めること。

各段階において、取扱者は必要最小限に限定することが必要である。【運 53】を参照のこと。

削除: 運　53-1

削除: 6

削除: .
<オブジェクト>.
.
.

(1) 取得

① 顧客の同意

事前に金融機関等は、顧客に対し、生体認証情報の利用目的、利用範囲、生体認証のシステム利用手順等について説明し、顧客より同意を得ることが必要である。

本人の同意に基づかない、もしくは、本人確認の目的以外で、生体認証情報を取得することは、「金融分野における個人情報保護に関するガイドライン」第5条に反する。

削除: 若しくは

削除: 6

② 厳正な本人確認の実施

生体認証に使用する生体認証情報を取得する場合は、「犯罪による収益の移転防止に関する法律」（旧「金融機関等による顧客等の本人確認等及び預金口座等の不正な利用の防止に関する法律」）に定める手段に準拠し、なりすましによる登録を防止し、本人であることを厳格に確認すること。

（例：口座開設時の手続きの一環として、公的証明書（パスポートや運転免許証等）により、対面で確かに本人であることを確認したうえで、生体認証情報を取得すること等があげられる）

③ 本人確認に必要な最小限の生体認証情報のみの取得

生体認証情報の取得にあたっては、本人確認に必要な最小限の生体認証情報のみに限定することが必要である。具体的には、raw（生）データそのものを登録して使用することなく、特徴点を抽出して用いることが求められる。

(2) 入力

① テンプレートの登録

・テンプレートの登録時には、新たに生成したテンプレートが、被登録者本人の認証に適合することを、利用開始に先立ち、確認すること。

・金融機関等がテンプレートをコンピュータ上に登録する場合は、テンプレートの作成場所から保存場所への、安全な移送・伝送手順を明確にすること。（例、暗号の使用など）

・顧客が保持する記録媒体（以下、トークンという）にテンプレートを登録する場合は、トークンへテンプレートを安全に格納する手順、および顧客への安全な発行手順を明確にすること。

・伝送データの漏洩防止に関しては、【技29】を参照のこと。

・蓄積データの漏洩防止に関しては、【技28】を参照のこと。

・データ保護、破壊・改ざん防止に関しては、【技31】を参照のこと。

・外部ネットワークからのアクセス制限については、【技43】を参照のこと。

（注）テンプレート・・・認証時に参照するために、事前に登録する生体認証情報のこと。

② 顧客への通知

取引開始に先立ち、テンプレートの登録が完了した旨、顧客への通知を行うことが望ましい。（例：その場で本人に通知する。または、登録が完了した時点で、メールやはがきを出状する。）

③ サンプル・データの消去

テンプレートを作成するために、顧客から取得したサンプル・データについては、その消去の条件と方法が明確になっており、安全な管理のもとに速やかに消去することが必要である。

（注）サンプル・データ　・・・認証の都度（日常取引や登録時等）、センサー等の機器を

介して取得する生体認証情報のこと。

(3) 利用

① 暗号化

a. 生体認証情報の不正利用等を防止するため、生体認証情報を移送、伝送する場合は暗号化することが必要である。

（例：ここで対象となる生体認証情報とは、
・テンプレート
・サンプル・データ
・ログに含まれる生体認証情報
など）

b. また、テンプレートの改ざん検知策を講ずることが望ましい。

（例：メッセージ認証コードの使用など）

・改ざん検知策について、【技 33】を参照のこと。

② 暗号鍵の管理

利用する暗号鍵の管理方法を明確にし、運用することが必要である。

・暗号鍵の管理について、【運 43】を参照のこと。

③ サンプル・データの消去

日常取引において、顧客から取得したサンプル・データについては、その消去の条件と方法が明確になっており、安全な管理のもとに速やかに消去することが必要である。

(4) 保存

① テンプレートの保存

a. 金融機関等が、テンプレートを保存する場合、安全に保存するための手順を定めることが必要である。

b. 金融機関等が、テンプレートをサーバー等の検索可能なデータベースに保存する場合は、「氏名等の個人情報」と「生体認証情報」を分別管理することが望ましい。ここで、「氏名等」とは、「氏名や顧客番号のように顧客を容易に特定できる情報」を指す。

（例：具体的には、データベースを分ける。サーバーを分ける。バックアップ先の媒体を分ける。等）

・伝送データの漏洩防止に関しては、【技 29】を参照のこと。
・蓄積データの漏洩防止に関しては、【技 28】を参照のこと。
・データ保護、破壊・改ざん防止に関しては、【技 31】を参照のこと。
・外部ネットワークからのアクセス制限については、【技 43】を参照のこと。

② 暗号化

登録された生体認証情報の不正利用等を防止するため、生体認証情報を移送、伝送、保管する場合は暗号化することが必要である。

（例：ここで対象となる生体認証情報とは、
・テンプレート
・ログに含まれる生体認証情報
など）

③ 暗号鍵の管理

利用する暗号鍵の管理方法を明確にし、運用することが必要である。

・暗号鍵の管理について、【運 43】を参照のこと。

(5) 消去

生体認証情報、およびそれを記録した記憶媒体等を、本人確認に用いる必要性がなくなった場合、および本人から消去の申し入れがあった場合には、速やかにこれらを消去するための手順が明確になっており、安全な管理のもとに、実施することが必要である。

(6) トークンの取扱管理

① 顧客が保持するトークンにテンプレートを保存する場合

・トークンを顧客に安全に発行するための、手順を明確にすることが必要である。

・また、発行後のトークンの使用停止、使用停止解除、再発行、消去を、安全に実施するための手順、およびトークンの紛失、盗難、汚損時等の取扱手順を明確にすることが必要である。

・トークンを本人確認に用いる必要性がなくなった場合、および本人から消去の申し入れがあった場合には、速やかにこれを消去するための手順が明確になっており、安全な管理のもとに、実施することが必要である。

（例：顧客との授受や登録手続きを窓口で対面で確実に行う。受領確認を行い、そのログを記録する。顧客がトークンを保有する際は、生体認証情報の漏洩防止対策がなされている。等）

② 不正アクセス技術の向上等に対応し、必要かつ適切な安全管理措置を実施する観点から、トークンの使用期限を考慮することが望ましい。

・カードの管理方法の明確化については、【運 51】も参照のこと。

・テンプレートの再発行については、【技 35-1】を参照のこと。

参照法令	・個人情報の保護に関する法律 ・個人情報の保護に関する法律についてのガイドライン ・金融分野における個人情報保護に関するガイドライン ・金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針

「生体認証情報」を取り扱ううえで、安全対策基準に「重要」データ、「機密」データ等として記述がある下記の基準を参考にされたい。

【設 23、設 24、設 26、 設 31、 設 93、設 101、設 106、設 122、設 123】

【運 1、運 5、運 10、運 11、運 13、運 16、運 21、運 24、運 25、運 27、運 29、運 33、運 36、 運 37、運 57、運 58、運 61、運 71、運 74、運 75、運 76、運 79、運 80、運 87-1、運 88、運 90、運 107】

【技 8、技 11、技 13、技 16、技 17、技 28、技 29、技 31、技 33、技 43、技 50】

2　運用管理

削除: （Ⅲ）

(19) 資源管理

削除: 19.

コンピュータシステムの障害および処理能力の低下を回避するため、各種資源の容量および性能の限界を把握する等、適切な管理を行うことが必要である。

運用管理
資源管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 47	能力及び使用状況の確認を行うこと。

削除: 運　54

コンピュータシステムの障害及び処理能力の低下を回避するため、各種資源の能力及び使用状況の確認を行い、適切な措置を講ずること。

1. コンピュータシステムを構成する各種資源の性能や容量には限界があり、それに起因するコンピュータシステムの障害及び処理能力の低下を回避するため、能力及び使用状況の確認を行うことが必要である。

また、使用状況確認結果を継続的に分析し、システムの性能強化や機能強化、組合せの再検討等を行うことが必要である。

(1) ハードウェア資源
- ① 本体装置
- ② 周辺装置
- ③ 通信系装置

(2) ソフトウェア資源
- ① 各種プログラム
- ② 各種ファイル
- ③ 入出力バッファ、キュー等の緩衝エリア

(3) ネットワーク資源

2. 資源管理を実施するにあたっては、以下の手順を明確にしておくことが必要である。

なお、新たなサービスの提供や環境変化が想定される場合には、その内容に応じて、業務部署と連携して事務量の変動を加味することが必要である。

(1) 計画
管理対象資源の設定、使用状況の確認方法と確認頻度等の資源管理計画の策定

(2) 実施
統計プログラム、モニタリング等による各種資源の利用率、使用容量等のデータ収集、分析、評価の実施

(3) 検証・報告
資源容量等の設定内容の妥当性検証、資源不足等によりシステム運行に支障が見込まれる場合の対応策の検討及びまとめ

3.　能力及び使用状況の確認として、以下のような例がある。

(1) レスポンス時間及びバッチ処理時間は、許容範囲であることを確認する。

レスポンス時間とは、オンラインシステムで取引 1 件を処理する時間を指し、バッチ処理時間とは、バッチシステムにおけるジョブのスタートからエンドまでの所要時間を指している。

なお、オンライン処理においては単位時間当たりの処理件数、バッチ処理においてはオンライン処理に影響を与えないことを確認することも必要である。

(2) 各種資源の能力限界を把握し、定期的に使用状況の確認を行う。

各種資源の使用状況を確認し、能力限界との比較を行うことにより、あらかじめ対応策を考えておくことが必要である。

また、システム処理における上限（同時アクセス数、1 日における最大値等）を設定している場合には、その設定内容の定期的な確認と事務量等の管理を行うことが望ましい。

なお、Web システムにおいて、想定事務量を超えた際には、アクセスの制限（流量制限）等を行うことも有効である。

(3) 各ファイルの使用可能容量を把握し、定期的に使用状況の確認を行う。

(4) 新規システムの追加、ネットワークの拡大、接続形態の変更などを行った際には、ネットワークの能力と使用状況を確認し、レスポンス時間等の処理能力が許容範囲内であることの確認を行う。

（参考）

勘定系オンライン運行中は、使用する資源やオンラインシステムとの競合等について確認がなされ、オンラインに影響を与えないことが確認されているプログラム以外の走行を禁止することが必要である。

2　運用管理

削除: （Ⅲ）

(20) 外部接続管理

削除: 20.

外部との接続を安全かつ正確に行い、データ漏洩、不正アクセス等を防止するため、接続先が正当であることを確認するとともに、外部接続時の運用方法等を明確に定め、適切に管理することが必要である。

運用管理
外部接続管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 48	接続契約内容を明確にすること。

削除: 運　55

外部との接続を安全かつ正確に行うため、回線接続によるデータ授受に係わる契約締結にあたっては、接続の方法、データフォーマット、データ内容等を明確にすること。

1.　回線接続によるデータ授受に係わる契約を締結するにあたっては、契約に盛り込まれた内容を十分把握し、誤接続等のないようにすることが必要である。このため、接続条件確認書を作成するなど標準化を図っておくことが考えられる。

2.　接続契約にあたっては、次のような事項を明確にすることが必要である。

(1) 利用回線

①　公衆回線（共同利用型通信回線）

a.　電話回線

b.　ISDN 回線

c.　回線交換回線

d.　パケット交換回線

e.　ATM 回線

f.　インターネット回線

g.　その他

削除: e.　フレームリレー回線

削除: f

削除: g

削除: h

②　専用回線（専用に利用できる回線）

a.　（一般）専用回線

b.　高速デジタル回線

c.　衛星通信回線

(2) 接続機器

①　音声伝送

a.　電話

b.　音声蓄積

c.　音声転送

②　データ伝送

a.　ファクシミリ

b.　コンピュータ

c.　パソコン

d.　その他

削除: b.　テレックス

削除: c

削除: d

削除: e

(3) 伝送制御手順

① 全銀協手順
② JCA 手順
③ FTAM（OSI「開放型システム間相互接続」におけるファイル転送の国際標準規格）
④ その他

(4) 送受信データフォーマット

(5) データ内容
① 給与振込
② 総合振込
③ 公共料金
④ 年金
⑤ 株式配当金
⑥ 保険料
⑦ その他

(6) 相手先確認方法
① 公衆回線による電話、ファクシミリ等の接続
a. 初回申込および変更時の通話による電話番号確認
b. 初回申込および変更時のデータ送信による電話番号確認
c. 発信者番号通知サービスによる接続相手確認
d. コールバックによる接続相手確認
e. ID・パスワード等による接続相手確認
② コンピュータ、パソコン、家庭用簡易端末等の接続
a. 相手先確認コードによる接続相手確認
b. ID・パスワードによる接続相手確認
c. ファイルアクセスキーによる接続相手確認

(7) 伝送不能等障害時の対応方法

運用管理
外部接続管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 49	外部接続における運用管理方法を明確にすること。

削除: 運　56

データ漏洩、不正アクセス等を防止するため、外部接続時には運用管理方法を明確にし、相手先確認、接続条件（パスワード等）の登録・変更管理などを適切に行うこと。

1.　回線接続によりデータ授受を行う場合には、契約や定められた規定などにより接続相手先の本人確認や端末確認の方法を明確にし、適切な管理を行うことが必要である。

2.　特にインターネットの利用や公衆回線網によるリモートアクセスの利用など、不特定多数の者による社内システムへの侵入の危険性が高いネットワークと接続する場合には、接続に関する運用管理方法を明確にし、適切な管理を行うことが必要である。

3.　運用管理方法には、例えば以下のようなものがある。

(1) 接続先の確認、制限

①　接続する際は相手の本人確認、端末確認を行う。確認方法については【技 27、技 35】参照のこと。

②　確認に使用するパスワード等の登録・変更は定められた方法によって行い、その結果については確認検証を行う。管理方法については【技 26】、【運 17】参照のこと。

(2) 外部接続の利用管理

社内システムとインターネットとの接続や、出張先からのリモートアクセス等を行う場合以下の点を定め、場合によっては制限を設ける。

①　利用可能者

②　利用可能時間

③　利用目的

(3) 接続の監視

不正アクセスや情報漏洩防止のため、接続記録を取得し以下の監視を行う。

①　外部から内部への接続監視

②　内部から外部への接続監視

監視方法については【技 37、技 45】参照のこと。

(4) 認証デバイス紛失時の対応

接続先の本人確認に使用する認証デバイス（アクセストークン、IC カード等）を本人が紛失した際の対応策を定める。

(5) セキュリティホール等への対応

外部と接続するサーバーやルータ等に搭載されているソフトウェアについて、セキュリティホール等の情報を収集し、適切なバージョンアップを行うなどの対応策を定める。

なお、不正アクセスや不正プログラム等の対策として、ベンダーから頻繁にセキュリティ対策のための修正プログラムが提供されている。これらの修正プログラム等を利用する際には、正規のプログラムであることを検証する電子署名が付いたデータを入手し、電子署名の内容や改ざんされていないこと等を確認することが望ましい。

これらの修正プログラムは、業務やシステムに対する緊急度や重要度を考慮し、適用することが望ましい。

緊急度や重要度の判断の例として、以下のものがある。

・外部ネットワークとの接続部分の機器

不特定多数の人がアクセスする可能性のある外部ネットワークとの接続部分にあるファイアウォール、公開サーバー、ルータ等の機器においては、インターネットから不正アクセスや攻撃を受ける危険性を考慮し、速やかに適用する。

・それ以外の機器

不正アクセスの可能性や業務への影響を考慮し、十分に確認してから適用する。

また、修正プログラムの適用後は、修正の影響範囲を適切に判断し、正常に稼働することを確認する必要がある。

削除: ー

削除: ー

4. 外部からの不正アクセス等により生じた損害賠償責任、逸失利益、業務継続に要した費用等について、保険の適用を検討することが望ましい。

(参考)
スマートデバイスに関わる考慮点については、【運 50】を参照のこと。

2　運用管理

削除: （Ⅲ）

(21) 機器の管理

削除: 21.

コンピュータシステムを構成する各機器の障害、不正使用、破壊、盗難等の防止策を的確に講ずるため、管理責任者を明確にし、各機器の重要性に応じて、管理方法、保守方法を明確に定めることが必要である。

運用管理
機器の管理

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実50	管理方法を明確にすること。

削除: 運　57

コンピュータシステムを構成する各機器の不正使用、破壊、盗難等を防止するため、定められた方法によって管理すること。

1.　機器については、管理責任者を明確にするとともに、以下のような点から管理することが必要である。
(1) 関係者以外容易に接近できない。
(2) 入力機器（端末機など）、出力機器（プリンターなど）及び重要なサーバー等は、許可された人のみ操作ができる。

なお、システムの構成、使用形態、使用状況、設置台数等を把握しておくことも重要である。

2.　1.で述べた事項の具体的な実施方法としては、以下のような例が考えられる。
(1) 関係者以外の接近防止
①　コンピュータ室や重要なサーバーの設置場所への入室資格付与【運 11】
②　施錠による管理【運 11】
(2) 機器の操作資格の付与
①　操作者の資格確認【運 19】
②　ID の付与や鍵の貸与などによるアクセス権限の付与【運 16、運 18】
端末権限規制機能の設定【技 38】
(3) 持出しが容易な機器類の盗難防止
①　ワイヤー等により設置機器の固定
②　鍵付ラックへの収納
(4) 記録媒体の使用制限【技 28】
①　持出し、持込み許可
②　使用許可

3.　機器を修理等で外部に持ち出す時、情報漏洩等がなされないように、修理時等の管理方法についても定めておくことが必要である。

4.　機器の不正使用、破壊、盗難等により生じた損害や業務上の逸失利益、業務の継続に要した費用等について保険の適用を検討することが望ましい。

（参考）
スマートデバイスに関わる考慮点については、【運 50】を参照のこと。

運用管理
機器の管理

適　用　区　分				
共	セ	本	提	ダ
	○	○	○	

実 51	ネットワーク関連機器の保護措置を講ずること。

削除: 運　58

不正使用、破壊、盗難等を防止するため、重要なデータを扱うシステムを構成するネットワーク機器等は、適切な保護措置が講じられていることが望ましい。

1. 重要なデータを扱うシステムの場合、MDF、IDF、ルータやファイアウォール等のネットワーク機器に関しても不正使用、破壊、盗難等された場合の影響が大きい。このため、ネットワーク機器も、必要に応じてサーバー設置場所に準ずる機器管理を行うことが望ましい。

削除: ー

2. サーバーの機器管理については【運 57】参照のこと。

3. ネットワーク機器の設定情報管理については【運 31、32】参照のこと。

運用管理
機器の管理

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実 52	保守方法を明確にすること。

削除: 運　59

コンピュータシステムを構成する各機器の障害を防止するため、保守点検を実施し、点検内容および結果を把握すること。

1. コンピュータシステムの保守には、定期保守と随時保守があり、保守の計画は対象機器ごとの使用状況および緊急度とメーカー側の体制を勘案し作成することが必要である。その場合、以下のような点について取り決めておくことが必要である。【技 1】
   また、保守点検実施後、その内容と結果について把握することが必要である。
   (1) 点検対象
   (2) 点検周期
   (3) 点検内容

2. 機器の盗難や破壊、情報の持出し等がなされないように、機器の重要性に応じて、当該機器を管理する部署の者が立ち会うことが必要である。

3. 連絡等に備えてメーカー側の保守体制、責任者・担当者の氏名、電話番号、保守担当範囲等を十分に把握しておくことが必要である。なお、メーカー側には、保守専門会社を含んでいる。

4. 保守要員の確保については、以下のような方法がある。
   (1) 必要時に電話等での連絡による招集
   (2) メーカー保守要員の常駐

5. 保守点検については、以下の点について管理運用することが必要である。
   (1) 保守内容の報告制度
   (2) 保守連絡会議
   (3) 保守についての統計分析
   (4) 保守計画の策定
   (5) 前回の保守点検以降のエラーログ解析結果

6. 保守点検のスケジュールについては、以下のような点を考慮することが必要である。
   (1) 設備関連工事と保守点検スケジュールを調整しておくこと。
   (2) CD･ATM 等の休日稼働、夜間稼働等を考慮し、保守点検スケジュールを調整しておくこと。

2　運用管理

削除: （Ⅲ）

(22) 運行監視

削除: 22.

異常状態早期発見のため、コンピュータシステムの運行状況を監視することが必要である。

運用管理
運行監視

適　用　区　分				
共	セ	本	提	ダ
◎				

実 53	監視体制を整備すること。

削除: 運　60

異常状態早期発見のため、監視対象、監視内容及び監視方法を定めること。

1.　システムの異常状態を早期発見するとともに、不正使用を発見、防止するため、例えば、以下のような事項について明確にした監視体制を整備することが必要である。

なお、異常状態や不正使用を発見したときの対応方法を明確にしておくことも必要である。

(1) 監視対象・内容

①　システム異常状態早期発見のための監視

a.　オンライン稼働状況

b.　中央処理装置、チャネル装置、ファイル装置等の稼働状況

c.　各業務オンラインに関する通信制御装置、回線及び営業店端末機の稼働状況

d.　CD･ATM 等の稼働状況

e.　バッチの進捗状況

f.　待機系システムの稼働状況（切り替え時に必要なプログラム等）

②　不正使用発見・防止のための監視

コンソールログ、システムログ等の分析または監視により、以下のような点について把握することが必要である。

a.　ジョブ稼働状況の確認

(a) 実行予定ジョブ以外のジョブ実行有無確認

(b) オペレータコマンドによるジョブ実行状況確認

b.　異常な使用時間や使用頻度のジョブ確認

c.　ファイルに関するアクセス状況の確認

(a) アクセスエラー多発者

(b) アクセス権限に基づいたアクセス状況

(2) 監視方法

監視者を定め、集中監視システム等により一元的に監視することが望ましい。また、オペレーションを外部に委託している場合は、定期報告や異常状態及び不正発見時のタイムリーな報告を受けるように取り決めておくことが必要である。

①　システム異常早期発見

a.　コンソールまたはパネルによるモニタリング

b.　システム異常時のアラームによる監視

c. 監視ツールの使用
d. ベンダーによる遠隔監視システムの活用

② 不正使用発見・防止のための監視

a. 不正アクセス検知時のコンソールまたはパネルによるプログラム名称等のモニタリング
b. 不正アクセス検知時のアラームによる監視
c. 監視ツールの使用

2. 監視機能については、【技 18、技 20、技 45】参照のこと。

3. 障害検出機能については、【技 21】参照のこと。

4. 障害時・災害時の対応策については、【運 62、運 63、運 64】参照のこと。

5. 異常取引検知機能については、【技 46】参照のこと。

2　運用管理

削除: （Ⅲ）

(23) コンピュータ室・データ保管室の管理

削除: 23.

不法侵入、危険物持込み、不法持出し等を防止するため、コンピュータ室およびデータ保管室等重要な室における入室者の作業を管理することが必要である。

運用管理
コンピュータ室・データ保管室の管理

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実 54	入室後の作業を管理すること。

削除:　運　61

不法侵入、危険物持込み、不法持出し等を防止するため、コンピュータ室およびデータ保管室等重要な室における入室者の作業を管理すること。

1.　コンピュータ室およびデータ保管室、中央管理室（中央監視室、防災センター等）ならびに重要なサーバー設置場所への入室を認めた場合には、入室後の作業を管理することが必要である。

2.　入室後の作業管理の具体的事例として以下のようなものがある。
(1) 重要な室へ入室して行われる作業には監督者を配置する。
(2) 許可された区画以外に立ち入らないよう制限する。
(3) 未使用区画は施錠し、定期的に確認する。
(4) カメラ、ビデオ、パソコン等の記録用機器を許可なく使用させない。

3.　本部・営業店等における重要なサーバー設置場所等については、上記に準じて入室者の作業の管理を行うことが望ましい。

2　運用管理

削除: （Ⅲ）

(24) 障害時・災害時対応策

削除: .

コンピュータシステムの障害時・災害時における顧客、本部・営業店等への影響を最小限にとどめ、かつ、早期復旧を図るため、障害時・災害時対応策を講ずることが必要である。

運用管理
障害時・災害時対応策

適　用　区　分				
共	セ	本	提	ダ
◎				

実 55	関係者への連絡手順を明確にすること。

削除: 運　62

障害時・災害時に関係者へ迅速かつ確実に連絡を行うため、連絡手順を定めておくこと。

1.　障害時・災害時に連絡を行い、招集する関係者には以下のような対象者をあらかじめ整理しておき、定期的に見直すことが必要である。

　また、各関係者は必ず正副 2 名以上を決め、連絡のつかないことが無いようにするとともに、関係部署及び店内に定められた連絡手順を周知徹底させることが必要である。

　特に重大な障害、災害については、想定される最大リスク等を含め、経営層への報告を適宜行う必要がある。

(1) コンピュータセンターにおける関係者
　① コンピュータセンター運営担当者及び管理者
　② システム担当者及び管理者
　③ コンピュータメーカー及び UPS 等の設備関連業者の担当者
　④ 本部・営業店等への連絡責任者
　⑤ 外部共同システム（全銀センター、統合 ATM システム、共同 CMS 等）への連絡責任者
　⑥ 広報責任者

(2) 本部・営業店等における関係者
　① 本部・営業店等の責任者
　② コンピュータセンターへの連絡責任者
　③ メーカー等の保守部門担当者
　④ 警備会社

(3) 重要なシステムを委託している外部委託先

2.　連絡手段としては、以下のようなものが考えられるが、複数の連絡網を定めておくことが必要である。

(1) 電話（携帯電話、自動車電話、衛星電話を含む）
(2) ファクシミリ
(3) 別系統オンラインシステムの一斉通報機能
(4) 無線
(5) パソコン（インターネット等の利用）
(6) ボイスボックス

3.　CD･ATM 等への障害を考慮して、無人監視による時間帯（夜間、土曜日、日曜日、祝祭日等）の連絡網、連絡方法を別途作成しておくとともに、定期的な見直しを行うことが必要である。

4.　顧客へ正しい情報提供を行うため、広報窓口をあらかじめ一本化して取り決めておくことが必要である。提供する情報の例として、障害の内容・発生原因、復旧見込等が考えられる。
　また、広報窓口に対する各種情報の提供責任者もあらかじめ決めておくことが必要である。

5.　顧客受付窓口は、広報窓口と連携して、整合性がとれた情報を顧客に提供する必要がある。
　また、顧客受付窓口として、必要に応じてコールセンター等を開設することも有効である。

（参考）
(1) ボイスボックス
　ボイスメールセンターを利用して複数のメンバー間で音声メッセージをやりとりできるサービスである。パスワード等を入力することにより、メンバー間でメッセージの録音や再生等ができ、音声用掲示板として情報提供が可能である。
(2) 災害時優先電話
　正しくは「災害時優先通信」といい、災害の復旧等や公共の秩序を維持するため、法令に基づき、防災関係等各種機関等に対し、固定電話及び携帯電話の各電気通信事業者が提供しているサービスである。災害等で電話が混み合うと、発信規制や接続規制といった通信制限により、通常の電話は被災地からの発信や被災地への接続は制限されるが、優先電話はこうした制限を受けずに発信や接続を行うことが可能となっている。また、「優先」するものであって必ずつながることを保証しているものではない。

運用管理
障害時・災害時対応策

適　用　区　分				
共	セ	本	提	ダ
◎				

実 56	障害時・災害時復旧手順を明確にすること。

削除: 運　63

障害または災害等によりコンピュータシステムが正常に稼働しなくなった場合の復旧手順を明確にすること。なお、当該手順については、コンティンジェンシープランと整合性のとれた内容にすること。

1.　障害時・災害時復旧手順とは、障害または災害等により正常に稼働しなくなったコンピュータシステムを復旧させるための手続きを明確にしたものである。

コンピュータシステムの復旧手順を作成する障害の例としては以下のものがある。

(1) コンピュータ装置の故障
(2) 端末機器等の故障
(3) 関連設備（電源、空調、給排水設備等）の故障
(4) 通信回線の障害
(5) ソフトウェアの障害

2.　障害時・災害時の復旧手順を明確にするにあたって、以下のようなことを考慮することが必要である。

(1) 業務開始時の手順（システム立上げ時等）
(2) 影響を局所化する縮退等
(3) バックアップシステム（バックアップサイト設置分を含む）への切替え（強制切替え、システム運用時の諸制約等を踏まえた切替え判断及び運用手順、共同センターにおける切替え判断等を含む）
(4) バックアップシステム（バックアップサイト設置分を含む）への切替えによる社内のシステムへの影響確認（周辺システム、EUC システム等）
(5) ファイルの不整合や取引データの欠落の有無の確認手順
(6) 対応要員の確保と当該要員への必要な権限委任
(7) 本部・営業店等への業務影響範囲、復旧見込み等の連絡手順
(8) 社外のシステムへの影響確認（全銀センター、統合 ATM システム、共同 CMS 等の関連会社等）
(9) 稼働に必要な ID・パスワードの取得方法の明確化　【運 18】
(10) バックアップシステム（バックアップサイト設置分を含む）からの切戻しが必要な場合の対応方針、手順等

また、業務やシステム運用を外部に委託している場合に、外部委託先が契約どおりに委託業務を遂行できない場合の対応策についても、事前に考慮しておくことが望ましい。

3.　障害時・災害時に使用するバックアップシステム（バックアップサイト設置分を含む）が正常に稼働することを定期的に確認すること。

　なお、冗長構成によって信頼性を確保しているシステムにおいては、冗長構成の機器が正常に稼働していることを定期的に確認すること。

4.　障害時・災害時復旧については、【技 22～技 24】を参照のこと。

運用管理
障害時・災害時対応策

適　用　区　分				
共	セ	本	提	ダ
◎				

実 57	障害の原因を調査・分析すること。

削除: 運　64

すばやく復旧するため、障害の原因を調査する手法を講じておくこと。また、障害の発生原因を記録し、傾向分析等を通じて再発防止に役立てること。

1. すばやく復旧するためにも障害の原因を調査する手法を講じておくことが必要である。
   具体例としては、【技 20、技 21】を参照のこと。

2. コンピュータメーカーによる障害事前検知、障害発生後の早期原因把握のため、メーカー社内からシステムの診断が可能な遠隔診断システムの導入も原因調査の手段として考えられる。

3. 障害の発生を防止するため、発生した障害に係わる各種データを収集・分析し、障害発生原因を調査のうえ、根本原因を究明し、当該障害についての対策を講ずることが必要である。
   根本原因を究明する際は、システム的要因だけではなく、人的要因等からも究明する必要がある。なお、人的要因には操作者の過誤、要員の繁忙による集中力の低下、要員不足等が挙げられる。

4. 障害の未然防止の観点から、可能な範囲で社内及び社外（同業他社、他業態）の障害等の情報を収集・分析し、必要に応じて対策を講ずることが望ましい。

5. 障害の再発防止や未然防止に向けた施策については、障害件数の上限目標値等の障害管理の指標を用いて、その施策の実効性を客観的に評価することが望ましい。また、障害管理の指標は、システムの重要度及び障害の影響範囲に応じて、システム別・発生原因別等に定めることが有効である。
   障害の傾向分析などを継続的に行い、類似障害を事前防止できるよう態勢を整え運用することが望ましい。
   なお､障害の分析結果を定期的に経営層へ報告することも考慮して態勢を整備することが望ましい。

6. EUC システムについても、取り扱う業務の重要度や障害発生時の影響度に応じて、障害情報の収集・分析・障害対応・報告を行うための管理体制を整備すること。

2　運用管理

削除: （Ⅲ）

(25) コンティンジェンシープランの策定

削除: .

災害時・障害時等の緊急時に早期に業務の復旧を図るため、あらかじめ想定されるケースに基づいたコンティンジェンシープラン（緊急時対応計画）を作成しておくことが必要である。

運用管理
コンティンジェンシープランの策定

適　用　区　分				
共	セ	本	提	ダ
◎				

実 58	コンティンジェンシープランを策定すること。

削除: 運　65

不慮の災害や事故、あるいは障害等により重大な損害を被り、業務の遂行が困難になった場合の損害の範囲と業務への影響を極小化し、早期復旧をはかるために、あらかじめコンティンジェンシープラン（緊急時対応計画）を策定しておくこと。

1.　本基準におけるコンティンジェンシープランとは、金融機関等のコンピュータシステムが、不慮の災害や事故・犯罪、障害等により重大な損害を被り業務の遂行が果たせなくなった場合に、各種業務の中断の範囲と期間を極小化し、迅速かつ効率的に必要な業務の復旧を行うためにあらかじめ策定された緊急時対応計画のことである。（「Ⅱ.1(3)⑤コンティンジェンシープランの策定」参照）

削除: Ⅰ.2

削除: 4

削除: の必要性

2.　不慮の災害や事故、あるいは障害時に、あらかじめ想定される複数のケースに応じてコンティンジェンシープランを策定しておくことが必要である。

想定される緊急事態としては、以下のような例がある。

(1) コンピュータセンター、本部・営業店等の全面被災、一部被災
(2) コンピュータ装置の破壊、損傷
(3) 端末機器等の破損、損傷
(4) 関連設備（電源、空調、給排水設備等）の破壊、損傷
(5) 回線の切断、通信設備の損傷
(6) 公共インフラの障害（停電、断水、交通遮断等）
(7) ソフトウェアの障害
(8) サイバー攻撃

なお、集中豪雨、降雪等による交通遮断や感染症のパンデミック発生などから生じる職員不在等の不測の事態についても、要員確保の観点から考慮することが必要である。

また、障害等が発生した時期、曜日、時間帯やシステム環境の違いにより対応する範囲や方法が異なる場合には、これらの対応を考慮する必要がある。

特に、広範囲に重大な影響を及ぼすような資金決済システム等の障害については、時限性や社内関連システム及び社外への影響等にも留意する必要がある。

3.　コンティンジェンシープランの策定に際して考慮すべき内容としては、以下のようなことが考えられる。

なお、具体的なコンティンジェンシープランとしては、(3)～(6)に掲げた内容を手順書として

文書化することが必要である。

(1) 緊急事態を想定し、自社の業務や各種施設に対してどのような影響が起こるかを評価する。
(2) 緊急時における業務の継続の優先順位を評価する。
(3) 被災拠点及び対策本部における緊急時対応組織の体制（コンティンジェンシープラン発動権限も含む）や要員等を明確にする。
(4) 緊急事態発生時における、顧客・職員の安全確保、資産の保全、被災状況の把握等の措置を明確にする。
(5) 業務、顧客サービスの中断あるいは、中断による損失を極小化するために、業務の通常的な継続が困難な緊急事態のもとで、重要と判断される業務の暫定的継続を図るために必要な措置を明確にする。
(6) 早期に事態を収拾して、平常業務への復旧を図るために必要な措置を明確にする。
(7) 緊急時における要員の移動、機器等の物資の搬送手段及びルートを決めておく。
(8) プランの維持管理体制の確立を行い、定期的な訓練の実施とその結果に基づくプランの見直し等の維持管理を明確にする。
(9) 業務が外部委託されている場合は、委託先や再委託先（２段階以上の委託先を含む）の役割等も明確にする。

コンティンジェンシープランの策定に関する詳細内容については、当センター発刊の『金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書』を参照のこと。

4. コンティンジェンシープランが策定された後においても、適宜見直しをすることが必要である。

見直しが必要となる契機としては以下のようなものがある。

(1) 重要な業務についてその内容に変更が生じた場合。
(2) 従来、コンティンジェンシープランでは考慮していなかった業務についてその重要度が高まった場合。
(3) 上記業務遂行の前提となる組織や拠点施設、インフラ、システム構成等の条件に変更が生じた場合。
(4) 政府の取組みやガイドライン等が変更された場合。

なお、見直しを行う際は、事務手続き等の変更点にも考慮する。

5. 組織図や緊急連絡網等については、最新の情報を維持するとともに、組織内に周知することが必要である。

6. コンティンジェンシープランの策定及び重要なプラン内容の見直しを行うにあたっては、経営層の承認を得ることが必要である。

7. コンティンジェンシープランは、対策本部、各拠点、バックアップサイトにおいて、必要な部分が常時保管され、全役職員が必要な部分を閲覧できる状態を保つことが必要である。

8.　障害時・災害時等におけるシステムの復旧やバックアップサイトへの切替えを行う際は、セキュリティ管理のレベルが低下するおそれがある。当該事象が発生した場合のセキュリティについても通常時と同等のレベルを維持することが必要である。

9.　障害・災害によって生じる可能性のある損害賠償責任、逸失利益、業務継続に要する費用等に備えて、保険の適用を検討することが望ましい。

10.　設備及び技術面の復旧策、並びに災害時・障害時等に備えた運用訓練については、以下の基準項目を参照のこと。

削除: ならびに

(1) 環境　【設 1】
(2) 周囲　【設 2～設 4、設 7～設 9】
(3) 構造　【設 10～設 13、設 31～設 36】
(4) 開口部　【設 14、設 17～設 19、設 28～設 30】
(5) 内装等　【設 20、設 21】
(6) 位置　【設 22、設 25、設 26】
(7) 設備　【設 37～設 44】
(8) コンピュータ機器、什器、備品　【設 48、設 50、設 51】
(9) 電源室、空調機械室　【設 52、設 54～設 60】
(10) 電源設備　【設 62～設 71】
(11) 空調設備　【設 74～設 79】
(12) 監視制御設備　【設 80、設 81】
(13) 回線関連設備　【設 82、設 83、設 83-1】
(14) ハードウェアの予備　【技 2～技 6】
(15) 障害の早期回復　【技 22～技 24】
(16) 災害時対策　【技 25】
(17) 教育、訓練　【運 80～運 84】

11.　コンティンジェンシープランを変更する際は、必要に応じて上記の基準項目を参照のこと。

3　システム開発･変更

削除: （Ⅳ）

(1)　ハードウェア・ソフトウェア管理

削除: 1．

システム開発・変更に際し、導入するハードウェア、ソフトウェアの把握をするとともに、システムの構成変更などに対応するため必要事項を台帳等で管理することが必要である。

システム開発・変更
ハードウェア・ソフトウェア管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 59	ハードウェア、ソフトウェアの管理を行うこと。

削除: 運　66

システムの導入、変更、廃棄を確実に行うため、ハードウェア、ソフトウェアの構成管理、版数管理などを行うこと。

1. システム開発や導入時においては、下記項目について、考慮し把握していることが望ましい。
   ・製品入手可能期間（販売終了予定日等）
   ・サポート期間（サポート終了予定日、サポート期間延長の可否）
   特にサポート期間については、製品、バージョンにより異なるので、注意が必要である。

2. ハードウェア、ソフトウェアを適切に管理するため、台帳等を作成することが必要である。
   なお、本部・営業店等に設置されているハードウェア、ソフトウェアを主管部署が一括管理する場合には、主管部署で作成した台帳を配布し、当該部室店においても識別管理できるようにしておくことが望ましい。
   また、主管部署においては、当該システムのシステム構成図、ネットワーク接続図等を整備し、システム構成変更などに的確に対応できるようにしておくことが必要である。

3. 管理する項目としては、以下のようなものがある。
   (1) ハードウェア
   ① ハードウェア名称
   ② 製造会社名と型式名（型式番号）
   ③ 識別用シリアル番号
   ④ 費用
   ⑤ 導入日
   ⑥ 資産管理番号もしくはリース契約番号
   ⑦ 当初の配備先
   ⑧ 現在の配備先
   ⑨ 使用責任を持つユーザー名
   ⑩ 保守契約先
   (2) ソフトウェア
   ＜自社開発ソフトウェア＞
   ① プログラム名
   ② 当初開発年月日
   ③ 最終更新年月日
   ④ 利用部署名もしくはユーザー名

＜購入ソフトウェア＞
① 製品名
② 製造会社名および契約代理店名
③ 買取り、あるいはライセンス契約の区別
④ 費用
⑤ 導入日
⑥ 資産管理番号
⑦ バージョン番号
⑧ シリアル番号
⑨ 利用ユーザー名
⑩ サーバーソフトウェアとして導入された場合のライセンス数
⑪ 保守契約先

4. システム運用時においてもサポート確保やバージョンアップ、脆弱性対策を可能とするために、サポート期間（サポート終了予定日、サポート期間延長の可否等）について考慮し把握すること望ましい。

5. コンピュータセンターやシステム主管部署などにおいては、オペレーティングシステムなどの基本ソフトウェアについてベンダー等から修正情報を収集し、適切なバージョンのものを導入することが必要である。

6. オペレーティングシステムなどの基本ソフトウェアやソフトウェア製品（ミドルウェアを含む）については、ベンダー等から修正情報を収集し、対策を検討することが必要である。対策としては、脆弱性に対応する適切な修正プログラムの適用や修正プログラムを適用しない場合には運用による回避策、代替策等が挙げられる。また、発見された脆弱性の業務への影響度に応じて、業務の継続可否等の検討が望まれる。

7. パソコン等を別の用途に再利用するときには、コンピュータウイルスや不正プログラムが混入されていないかチェックすることが必要である。
コンピュータウイルスについては、以下の基準項目を参照のこと。
・コンピュータウイルス等不正プログラムへの防御対策 【技 49】
・コンピュータウイルス等不正プログラムの検知対策 【技 50】

8. ハードウェアの損害やソフトウェアのバグ、不正プログラムによるシステムの障害により生じた損害賠償責任、逸失利益、業務継続に要した費用等について保険の適用を検討することが望ましい。

3　システム開発･変更

削除: （Ⅳ）

(2)　システム開発･変更管理

削除: 2.

システム開発・変更における内容の正当性と本番システムの安全性を確保するため、システム開発・変更手順を明確にし、テスト環境を整備するなど総合的に管理することが必要である。

システム開発・変更
システム開発・変更管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実60	開発・変更手順を明確にすること。

削除: 運　67

システム開発・変更における内容の正当性を確保するため、開発・変更手順を明確にすること。

1.　システムの信頼性を向上させるとともに、内容の正当性を確保するため、システム開発・変更の各段階における確認、検証等は定められた手順によって行うことが必要である。

開発・変更手順とは、以下のようなものを指している。

(1) 新規システムの開発または既存システムの変更における要件検討、企画の承認手順
(2) 設計、プログラム作成、テスト等各段階における検証・承認手順
(3) 開発・変更作業完了時における検証・承認手順
(4) 障害時、災害時対応手順等への反映の検証・承認手順　【運 15、運 65】

2.　システム開発工程を適切に管理するため、プロジェクトごとに責任者を明確にし、効率的な開発手法を確立して、プロジェクト管理を実施することが必要である。

ここでいうプロジェクト管理とはシステム開発・変更作業を与えられた時間と資源（人、物、金等）の範囲内で合理的に進め、確実かつ効率的に目的を達成するために、定められた方法にしたがってプロジェクトの状況を十分に把握し、適切な対応をとることを指す。

適切なプロジェクト管理の実施には、プロジェクトの支援環境を整備することも有効である。

3.　システムの信頼性向上を図るうえで、ソフトウェアの信頼性向上対策を講ずることが重要である。ソフトウェアの品質確保については、【技 7～技 15】参照のこと。

（参考 1）

開発の各段階における管理ポイントとして、以下のような例がある。

1. システム要件検討、企画

(1) 社内の組織横断的な審議機関を設置し、案件の開発可否を審議しているか。

(2) 情報システムの投資効果とそのリスクが開発案件の検証・承認ルールの中で評価され、必要に応じ、経営層に報告されているか。 なお、この投資効果の計測にあたって考慮する要素としては、以下の例がある。

・システム開発コスト

・開発により得ることができる収益の向上、事務量の削減効果などの「定量効果」

・その他、定量的に計測することのできない「定性効果」

(3) ユーザー要件の確認は十分か。また、依頼文書は受付簿等で管理されているか。

2. システム設計

(1) 各段階で作成した設計書等のドキュメント類は標準化ルールにそった内容となっているか。

(2) 設計内容等のチェック・レビューは行われているか。

3. プログラム作成

(1) プログラム作成作業等を外部に委託するにあたっては、詳細作業指示、ドキュメント授受・内容の検証等、受渡票等により、ドキュメント類の受渡しの事実が明らかになっているか。

(2) プログラム仕様の検証、承認は定められた手続きに従い、適切に行われているか。また、仕様変更は必ず権限者の承認を受けて行われているか。

4. テスト

(1) テスト方法や確認の手順が確立しており、かつ遵守されているか。

(2) バグ管理表等により、未解決バグ、問題点・懸案事項等の把握、管理、対策が行われているか。

(3) 必要に応じ、ユーザー部門によるテストデータの作成や出力結果の確認等が行われているか。

(4) ピーク処理時の性能評価、及び許容最大件数を考慮した負荷評価が行われているか。

5. システム運用

(1) 運用部門（運用担当者）への引継ぎ資料、説明、初期運用時のフォローは十分か。

(2) システムの維持管理体制、維持管理用ドキュメント等は適切に整備されているか。

(3) システムのリスクの評価を継続的に行い、その維持・改善のための投資が計画的に行われているか。

6. 開発の段階全般

(1) システム開発・変更スケジュールが明確化され、進捗管理が行われているか。また、遅延した場合の問題解決が行われているか。

(2) 特に重要なシステムの開発プロジェクトにおいては、業務部門や顧客対応部門等の状況を把握するための社内の組織横断的な検証体制が整備されているか。また、その整備や状況チェックには経営層が関与しているか。

（参考 2）

システム開発を効率化するためにはプロジェクトマネジメントが重要であり、その基礎プロセスを明確にして、プロジェクトの計画・遂行管理を成功に導くための知識体系を整備することが有効である。この知識体系の一例として、プロジェクトマネジメントの知識体系 PMBOK（Project Management Body of Knowledge）がある。

（参考 3）

プロジェクトの支援環境整備の一例として、プロジェクトを横断的に支援する組織 PMO（Project Management Office）の設置がある。

システム開発・変更
システム開発・変更管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実61	テスト環境を整備すること。

削除: 運　68

本番システムの安全性を確保するため、本番環境へ影響を与えないようなテスト環境を整備すること。

1. システムの開発・変更作業に係わるテストにおいては、本番環境へ影響を与えずに十分なテストが実施できることが必要である。また、本番環境とテスト環境の差異についても把握しておくことが必要である。
   なお、本番機と開発機はできる限り分離することが望ましい。

2. テスト環境整備の具体的事例として、以下のようなものがある。
   (1) 本番環境へ影響を与えないテスト環境の設定
   ① テスト用ファイルと本番用ファイルを分離する。
   テストを行う際は、本番用ファイルを参照、更新及び破壊しないよう、本番用ファイルと分離したテスト用ファイルを用意することが必要である。
   ② テスト用端末からの本番ファイルへのアクセス防止策を講ずる。
   不正アクセス防止については、【運 16～運 18】を参照のこと。
   また、テスト用端末ではログオン手順や ID 体系を変更したり、メニュー画面を変更するなどの対策を行い、本番端末との混同を避けることが望ましい。
   ③ 本番システム稼働中のテスト等を回避する。
   本番システム稼働中のテスト等の実施は極力回避し、やむを得ず実施する場合は、テストによる影響度を明らかにし、それに対するテスト制限を設ける必要がある。
   ④ 本番機器を使用したテストを行う場合は、テスト後の戻し、切替え手順を明確にする。
   本番機器を使用したテストを行う場合、機器を本番システムの環境に戻す手順を明らかにしておき、本番システムに影響が出ないことを確認する。
   ⑤ 営業店側での事務処理上の留意点について連絡、徹底する。
   営業店を含むテストを実施する場合には、現行システムとの関連で混乱が発生しないよう、以下のような点の取扱いについて連絡し、周知徹底しておく必要がある。
   a. 端末ハードウェア・ソフトウェアの入替え
   b. 使用帳票等の分離、管理
   c. 事務手続き・マニュアル類の分離、管理等
   ⑥ 開発用 ID と本番用 ID を明確に区別する。
   本番移行後に開発用 ID がセキュリティホールとならないように開発用 ID と本番用 ID を明確に区別し、本番移行時には不要な開発用 ID を抹消すること。

(2) 本番稼働へ向けて十分なテストが実施できる環境の設定

① 開発・テスト用資源等を確保する。

開発・テスト用のコンピュータ等の資源は十分に確保する望ましい。その際、使用する媒体やテスト用ファイル等がコンピュータウイルスに感染していないかをチェックすること。

② 外部システム（全銀センター、共同 CMS センター等）との接続テストの予約を行う。

外部システムとの接続テストを実施する場合には、事前にテスト日程、テスト範囲・分担、テスト内容等を十分に検討し、調整しておくことが必要である。

③ 本番想定でのテストを実施する。

テストの種類については、【技 11】参照のこと。

(3) オープンネットワークを使用したテストを行う際の留意点

オープンネットワークと接続する必要のあるテストを行う場合は、不正侵入防止機能を設けておくことが必要である。【技 43】

3. テストデータの漏洩防止

本番データをもとにテストデータを作成する場合、個人を識別できる情報を削除またはスクランブル化することが必要である。

やむをえず本番データを使用する場合には、次のような漏洩防止策を講ずることが必要である。

(1) データ管理者への本番データコピー借用依頼、承認

(2) アクセスできる要員の必要最小限化

(3) 使用後（借用期日到来時）のデータ管理部門への返却、及び開発・テスト環境からの削除

(4) テスト結果の出力リスト等の保管、廃棄　等

システム開発・変更
システム開発・変更管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実62	本番への移行手順を明確にすること。

削除: 運　69

本番システムの安全性を確保するため、本番への移行に際しては、各システムの特性を考慮し、移行手順を明確にするとともに、関連する各部門の手順の整合性を確認すること。

1.　本番への移行は、移行時における障害を防止することが重要であり、本番システムへの切替えを安全・確実に行うためのシステムの特性に応じた移行手順を明確にすることが必要である。

また、円滑な運用に移行するため、運用部門（運用担当者）への引継ぎ、説明及びユーザーへの説明を十分に行い、準備状況を確認することが重要である。

2.　本番への移行手順で考慮するものとして、以下のような例がある。

(1) 移行方法の明確化

移行作業手順及びカットオーバー可否の判断基準等を明確にする。判断基準については、数値化等による客観的な指標を用いることも有効である。

また、以下のような事項も考慮しておく。

・移行に支障が生じた場合の対処として、旧システムを継続稼働させるために必要な対応等（制度対応等のシステム変更、保守、契約期限の延長等）を実施すること。

・待機系システムがある場合、現用系システムと同様に移行作業手順等を明確化すること、また現用系システムと待機系システムの設定値の整合性確認をすること。

・外部接続がある場合、カットオーバー判断のため外部接続先の要件等の十分な調査・調整を実施すること。

(2) 運用部門及びユーザーへの説明や準備状況の確認等

円滑な運用に移行するため、運用部門に対し、システムの運用に必要なドキュメント類を引き継ぐとともに十分に説明を行う。また、ユーザーに対しては移行のタイミングや変更点及び制約事項等を十分に説明するとともに、事務処理や顧客周知等の準備状況を確認する。

(3) 移行リハーサルの実施

システムの移行にあたっては、必要に応じて事前に移行のリハーサルを行い、安全・確実に移行できることを確認するとともに、移行処理時間の測定や正当性確認のためのチェックポイントなどを明確にする。

なお、具体的には以下のようなものが考えられる。

・ファイル移行確認テスト

・移行手順確認テスト

・回線接続確認テスト

・オペレーション確認テスト

・残高照合等確認テスト

(4) 移行判定

カットオーバー可否の判断基準に照らして準備状況を確認し、移行判定を行う。また、特に重要なシステムにおいては、社内横断的に関連する部門（業務部門、顧客対応部門等）の準備状況等を確認し、リスク管理部門等の評価も踏まえたうえで経営層が判定する。

(5) 移行作業の実施

移行のための組織・体制を整備し、移行手順書に従いデータファイル（環境設定ファイル等を含む）及びプログラム等の移行作業を実施する。移行作業については、(3)移行リハーサルの実施等において、正確性（移行順序やタイミング等）を確認する必要がある。また、必要に応じて新旧の比較により変更箇所を確認することも有効である。

なお、異常時に備えて、作業中止・復旧作業に移るための判断ポイントを設定し、速やかに復旧作業ができるように関連する各部門の手順の整合性を確認のうえ、準備しておくことも必要である。

(6) 最終確認

移行実施後は、ユーザーと協力のうえ、残高照合等のデータの整合性を確認するテストを行い、既存システムを含めた本番稼働に支障がないことを確認する必要がある。

また、開発用に使用したコマンド、JCL、ツール、開発用 ID 等については、本番移行に伴い不要なものを削除することが重要であり、本番環境に持ち込む場合には、オペレータの誤操作等で起動されることがないように措置されている必要がある。

3. 特にコンピュータセンターの移転に際しては、1、2 の対策に加え、データの運搬に関して発生するリスクを考慮して、十分な対策を講じる必要がある。対策の例としては以下のようなものがある。

(1) 運搬中の事故、紛失、破損、盗難等への対策

・電磁波、塵埃などに留意した安全な経路の確保、天候・道路周辺事情の把握、警備

・データの保存時の暗号化

・運搬経路の多重化

(2) バックアップデータの保存もれ、保存時のエラー、紛失への対策

・バックアップの多重化

3　システム開発･変更

削除: （Ⅳ）

(3)　ドキュメント管理

削除: 3．

開発・変更作業を円滑にし、改ざん、不正使用を防止するため、システム開発・変更に係わるドキュメントの作成手順および管理方法を定めることが必要である。

システム開発・変更
ドキュメント管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 63	作成手順を定めること。

削除: 運　70

システムドキュメントを適切に作成するため、作成対象とするものを決め、それらについての作成手順を定めること。

1.　一貫した適切なドキュメントを作成するため、作成対象とするシステムドキュメントの範囲、体系、様式、記述内容等について明文化した手順を定め、遵守することが必要である。
　また、ドキュメントは、その品質を確認し、共有できるシステム資産とするために、作成部門および利用部門の責任者の承認を得ておくことが必要である。
　なお、定められた手順は開発方法の変更や運用形態などに応じて適時見直す必要がある。

2.　ドキュメント作成手順については、ドキュメントの作成者、利用者および管理者等の関係者に周知徹底させることが必要である。

3.　ドキュメント作成手順の遵守状況を、ドキュメントの作成、利用および管理の各責任者が確認していることが必要である。

4.　ドキュメント作成手順における制定項目としては、以下のようなものがある。
(1) 作成範囲
　作成するドキュメントの種類
(2) 作成方法
　ドキュメント作成の手段や方法
(3) 分類方法
　開発用、保守用、運用用など、ドキュメントの分類
(4) 記述要領
　標準様式、記述項目、記入要領、事例集
(5) 変更手順
　システムの変更に伴うドキュメントの変更方法、更新履歴の管理方法
(6) 作成部門
　ドキュメントの作成担当部門
(7) 保守部門
　ドキュメントの保守担当部門
(8) 利用部門
　ドキュメントの利用部門

(9) 承認手続き

ドキュメントのレビューから承認に至るまでの手続き

システム開発・変更
ドキュメント管理

適　用　区　分				
共	セ	本	提	ダ
◎				

実 64	保管管理方法を明確にすること。

削除: 運　71

円滑な利用および改ざん、不正使用等の防止のため、システムドキュメントの保管管理を適正に行うこと。

1. ドキュメントの保管管理は、その利用を円滑にし、かつ不正使用防止や機密保護のために、定められた手順に従って適正に行うことが必要である。

2. コンピュータシステムの内容と整合したドキュメントを維持するためには、一元管理することが望ましい。

3. 管理の具体的事例としては、以下のようなものがある。
   (1) ドキュメントの管理は管理簿にて行い、管理記録を整備する。
   (2) ドキュメントごとの保管期間を明確にする。
   (3) 管理責任者を明確にする。
   (4) 重要なドキュメントは定められた保管場所（施錠可能な保管室やキャビネット等）に保管する。
   (5) 重要なドキュメントは閲覧者を特定するとともに、コピーの制限を設けるなどの措置を講ずる。

4. ペーパーによらないドキュメント（電子媒体上の文書ファイル等）の保管管理についても、同様に取り扱うことが必要である。

3　システム開発･変更

削除: （Ⅳ）

(4)　パッケージの導入

削除: 4．

パッケージを導入する場合のシステム開発・変更を円滑に行うため、パッケージの信頼性、生産性、既存システムとの親和性などを評価する体制を整備するとともに、パッケージの運用・管理体制を明確にすることが必要である。

システム開発・変更
パッケージの導入

適　用　区　分				
共	セ	本	提	ダ
◎				

実65	評価体制を整備すること。

削除: 運　72

パッケージを導入する場合のシステム開発・変更を円滑に行うため、パッケージの有効性、信頼性、生産性等を評価する体制を整備すること。

1. パッケージ導入に際しては、システム開発部門、運用部門および利用部門（本部・営業店等）による総合的評価が必要である。

2. パッケージ導入に際しての評価項目としては、以下のようなものがある。
(1) パッケージ自体の評価項目
① 業務機能の充足性
② 性能（レスポンス、処理時間等）
③ 運用の容易性
④ ドキュメントの整備状況
⑤ 拡張性
⑥ 柔軟性
⑦ セキュリティ機能
⑧ パッケージ供給元の保守・支援体制（脆弱性への対応体制を含む）
⑨ 使用実績、導入実績
⑩ カスタマイズの可否と範囲
(2) 既存システム等との整合性に関する評価項目
① OS や DBMS、ミドルウェア等との親和性
・既存プラットフォームで実現できる性能
・バージョン相違などによる不整合等
② 入出力仕様
・データ入力方法や出力形式等（帳票、伝票、ファイル仕様）
③ コード体系
・漢字コード、フォント、外字の取扱い等

3. 必要なカスタマイズや将来の案件対応のために、パッケージのソースコード開示の可否を確認することも必要である。

システム開発・変更
パッケージの導入

適　用　区　分				
共	セ	本	提	ダ
◎				

実66	運用・管理体制を明確にすること。

削除: 運　73

パッケージの導入後のトラブル対応、機能拡張等を円滑に行うため、パッケージの運用・管理体制を明確にすること。

1.　パッケージの運用管理項目には以下のようなものがあり、その運用・管理体制を明確にすることが必要である。

(1) トラブル発生時の影響を最小にするため、パッケージ供給元の連絡窓口と保守体制および確認事項（トラブル現象の把握方法、応急措置方法等）の明確化

(2) 不正使用やトラブルの発生を抑制するための、ライセンス管理、バージョン管理体制の明確化

(3) システムの運用を円滑に行うためのメンテナンス体制とパッケージ供給元の支援体制（脆弱性への対応体制を含む）の明確化

(4) パッケージに関する教育、問合わせ等の体制の明確化

(5) パッケージの主要な設定内容等（各種設定値、有効期限等）管理の明確化

3　システム開発・変更

削除：（Ⅳ）

(5)　システムの廃棄

削除：５．

システムの廃棄時における機密保護、プライバシー保護、不正防止等のため、廃棄計画、手順を定めて遵守することが必要である。

システム開発・変更
システムの廃棄

適　用　区　分				
共	セ	本	提	ダ
◎				

実 67	廃棄計画、手順を策定すること。

削除: 運　74

システムの廃棄を円滑、確実かつ安全に実施するため、運用およびユーザー責任者の承認を得て不正防止、機密保護対策を含めた計画、手順を策定すること。

1. コンピュータシステムの廃棄を円滑、確実かつ安全に実施するために、廃棄計画、廃棄手順を策定し、運用および利用部門の責任者の承認を得て廃棄することが必要である。

2. コンピュータシステムを廃棄するにあたっては、あらかじめ、ユーザー、システム資産の管理部署および廃棄作業にあたる部署などの関係先に確実に連絡しておくことが必要である。
   また、廃棄作業に着手する前に、当該システムの運用が完全に終結していることを確認する必要がある。

3. 廃棄計画の内容としては、以下のようなものがある。
   (1) 廃棄の目的
   (2) 廃棄の対象範囲
   (3) 廃棄する時期
   (4) 廃棄する方法
   (5) 計上資産の処分方法

4. 廃棄にあたっては、機密保護等の措置を講ずることが必要である。【運 75】

システム開発・変更
システムの廃棄

適　用　区　分				
共	セ	本	提	ダ
◎				

実 68	情報漏洩防止対策を講ずること。

削除: 運　75

機密保護や不正防止等のため、システムの廃棄にあたっては機器等から情報漏洩が生じないように防止策を講ずること。

1. コンピュータシステムを廃棄するにあたっては、当該コンピュータシステムの重要度を考慮し、機密保護、プライバシー保護および不正防止のための対策を講ずることが必要である。

2. 廃棄が確実に行われるよう、廃棄方法および廃棄時期を明確にし、廃棄作業完了後には廃棄記録について責任者の承認を得ておくことが必要である。

3. ハードウェアを廃棄する場合には、内部の重要なデータを読み出し不可能とすることが必要である。具体的な対策としては以下の例がある。
   なお、リース契約期限切れに伴うリース会社への機器の返却等においても必要に応じて以下の例を参照すること。
   (1) パソコン等のハードディスクのデータを消去するツールを使用したデータの完全消去
   (2) IC カード等の破壊
   (3) 記録媒体の消磁もしくは破壊
   (4) ATM 等に内蔵している暗号化・復号装置等の破壊

4. ソフトウェアを廃棄する場合の対策としては、以下の例がある。
   (1) システムからのアンインストール
   (2) 記録媒体の消磁もしくは破壊
   (3) ドキュメントの廃棄
   なお、ライセンス契約上、廃棄時の定めがある場合はそれに従うことが必要である。

5. ドキュメントを廃棄する場合の対策としては、以下のようなものがある。
   (1) 焼却、細断
   (2) 記録媒体の消磁もしくは破壊

6. 第三者に廃棄を委託する場合においては、上記に準じて行うことが必要である。また、秘密保持契約を締結することが望ましい。

4　各種設備管理

削除：（V）

(1)　保守管理

削除：1．

コンピュータシステムを円滑に運用するため、電源、空調、給排水、防災、防犯、監視、回線関連等の設備の管理方法、保守方法を明確にすることが必要である。

各種設備管理
保守管理

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実 69	管理方法を明確にすること。

削除: 運　76

コンピュータシステムを円滑に運用するため、設備の管理責任者および管理方法を明確にし、定められた方法によって管理すること。また、障害時・災害時の対応方法を明確にすること。

1. コンピュータシステム（含む端末機器等）に係わる電源、空調、給排水、防災、防犯、監視および回線関連の設備は、コンピュータシステムの円滑な運用を確保するため、各設備の管理責任者を明確にするとともに、定められた方法によって管理することが必要である。

　また、コンピュータシステムへの影響を最小限にとどめるために、障害時・災害時の対応方法を明確にすることが必要である。

2. 端末機器、CD・ATM 等の自動機器等を円滑に運用するためには、電源設備、各種センサー、カメラ等防災・防犯設備等の管理方法を明確にすることが必要である。

　また、災害の発生に備えて、消火設備、監視設備等が正常に稼働するよう適切な管理を行うことが必要である。

　さらに、電源容量等各設備の能力を把握し、OA 機器、パソコン等の増設に備える必要がある。

3. 管理方法としては、以下のようなものがある。

(1) 各設備の操作手順書を備える。

　各設備の誤操作を防止するとともに、障害・災害発生時の対応を適切かつ迅速に行うため、各設備の操作手順書を備えることが必要である。

(2) 障害時の切替手順を定める。

(3) 障害時における保守要員の緊急招集体制を定める。

(4) 非常時における関係者への連絡方法および連絡内容を明確にする。

　コンピュータシステムへ影響を及ぼす障害・災害発生時の対応を迅速に行うため、コンピュータシステムの管理責任者等への連絡方法および連絡内容を明確にすることが必要である。

(5) 非常時の稼働に必要な燃料等を把握する。

　障害・災害発生時にもコンピュータシステムを円滑に運用するため、各設備で使用する重油、水等の管理を適切に行うことが必要である。

(6) 定期的な設備の機能点検・確認の計画を立て実施する。

　例えば、バックアップサイトへの切替えや復旧等の大掛かりな障害テスト、毎月の自家発電テスト、空調バックアップテストおよび絶縁テスト等を行うことが必要と考えられる。

削除: たと

(7) 設備関連機器の保守・運用を外部業者に委託する場合は、特に管理責任を明確にし、安全

指導を徹底する。

(8) 夜間、休日サービス等無人化運転で使用される設備を明確にし、管理を行う。

(9) 設備の操作盤等の鍵は、鍵の管理責任者が管理する。

(10) 携帯電話等から放射される電波により、コンピュータ関連機器が誤動作するおそれがあるため、コンピュータ室および重要なサーバー設置場所における携帯電話等の機器の使用については、メーカーと協議のうえ、当該機器の使用を制限する等の対策を講ずることが必要である。

(11) 障害原因を把握し、対策を講ずるとともに、障害記録を整理保存し、障害発生原因を時系列的に分析することにより、問題点の改善を図る。

各種設備管理
保守管理

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実 70	保守方法を明確にすること。

削除: 運　77

コンピュータシステムを円滑に運用するため、保守点検を実施し、点検内容および結果を把握すること。

1. コンピュータシステム（含む端末機器等）に係わる電源、空調、給排水、防災、防犯、監視および回線関連等の設備の保守点検にあたっては、コンピュータシステム運転スケジュールとの調整を図り、点検対象、点検周期、点検内容等を明確にして行うことが必要である。
　なお、保守点検にあたっては、事前の作業内容および事後の作業結果について各々書面にて報告を求め、検収後記録として保管することが必要である。

2. 防災設備の保守については規定を設け、定期的に点検を実施することが必要である。防災設備については、【設 80】参照のこと。

3. 設備を長時間停止した場合の再稼働にあたっては、保守点検を実施することが必要である。

4. 代替機等常時稼働しない設備は、正常稼働することを定期的に確認しておくことが必要である。

5. 設備保守にあたっては、設備管理責任者とコンピュータ運用管理者の連絡を密にし、システム運用に影響を与えないようにすることが必要である。

6. 電源設備や空調設備のようなコンピュータシステムに直接影響を与える可能性のある設備の保守作業は、オンライン時間帯を避けて行うことが望ましい。

7. システム稼働中に一部機器を保守する場合には、稼働中のシステムに影響を与えないための手順を徹底するとともに、当該機器の責任者立会いのもとに作業を行うことが必要である。

8. 電源および監視装置の接続系統を正確に把握するとともに、変更増設工事後も接続系統を整備されたものにしておくことが必要である。

参照法令	消防法第 8 条、第 17 条の 3 の 3、消防法施行規則第 31 条の 4

4　各種設備管理

削除：（V）

(2)　資源管理

削除：2.

コンピュータシステムを円滑に運用するため、各種設備の容量および性能の限界と使用状況を把握することが必要である。

各種設備管理
資源管理

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実 71	能力および使用状況の確認を行うこと。

削除: 運　78

異常状態早期発見のため、各種設備の容量および性能の限界を把握し、使用状況の確認を行うこと。

1.　コンピュータシステムの安定稼働を維持し、各種設備の異常状態を早期に発見するため、管理者は各設備の容量および性能を把握するとともに、以下のような点に留意することが必要である。

(1) コンピュータシステムを構成する各機器の増設

現在の各種設備の限界容量を超えないか､各種設備の容量も増設する必要がないかを検討する。

(2) コンピュータ室内のレイアウト変更

レイアウト変更後も通路、保守スペースの確保、床加重等の安全性確認が必要である。

2.　ここでいう設備としては、以下のようなものを指している。

(1) 受電設備（契約容量に留意すること）
(2) 定電圧定周波装置（CVCF）
(3) 蓄電池設備
(4) 自家発電設備
(5) 水冷装置
(6) 空調設備
(7) 給・排水設備
(8) 消火設備
(9) 監視設備
(10) 回線関連設備（障害時対応の DDX 等）
(11) 非常用通信設備（無線、自動車電話、衛星通信等）

4　各種設備管理

削除：（V）

(3)　監視

削除：3.

異常状態早期発見のため、コンピュータシステムの稼働に必要な各種設備の稼働状況を監視することが必要である。

各種設備管理
監視

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実 72	監視体制を整備すること。

異常状態早期発見のため、監視対象、監視内容および監視方法を定めること。

1.　各種設備の異常状態を早期に発見し、コンピュータシステムへの影響を軽減させるため、監視対象、監視内容および監視方法等の監視体制を整備することが必要である。

(1) コンピュータセンターにおける監視体制

①　監視対象、内容

a.　コンピュータシステムの正常稼働のための監視

対象：電源、空調、給・排水設備

b.　防災、防犯のための監視

対象：火災警報装置、センサー警報装置、入退館チェックシステムおよび遠隔監視モニター装置等

②　監視方法

異常状態を発見する方法としては、以下のような例がある。

a.　操作盤、バルブ等に正常値または正常位置を明示し、巡回監視の際に確認する。

b.　警告灯または警告ブザーにより、異常状態を中央管理室に通報する。

c.　中央管理室（中央監視室・防災センター）等において、電源、空調、給排水、防犯設備等の集中監視を行う。

(2) 本部・営業店等における監視体制

本部・営業店等に設置された重要なサーバーについては、運用状況に合った最適な監視方法をベンダー等と相談し、コンピュータセンターに準じた監視体制を整備することが望ましい。

2.　異常状態を発見した場合の対応方法を設備ごとに明確にしておくことが必要である。

対応方法を決定する要素として以下のようなものがある。

(1) 各種設備の容量および停止可能時間　【設 61】

(2) 代替機の有無

削除: 運　79

削除: に

5　インストアブランチ

削除: （X）

インストアブランチは、開放的なレイアウトおよび少人数での運営等、従来の本部・営業店等の運営と異なる点がある。インストアブランチの安全性を確保するため、出店先地域やストアの選定基準を明確にすることが必要である。

インストアブランチ

適　用　区　分				
共	セ	本	提	ダ
		◎		

実 73	出店先の選定基準を明確にすること。

削除: 運　92

インストアブランチの安全性を確保するため、出店先地域やストアの選定基準を明確にすること。

1. インストアブランチは、開放的なレイアウトおよび少人数での運営等、従来の本部・営業店等の運営と異なる点がある。インストアブランチの安全性を確保するため、出店先地域やストアの選定基準を明確にすることが必要である。

2. 明確にする選定基準としては、以下のようなものがある。
   (1) ストアの経営体質、警備方針
   (2) 出店先地域における過去の犯罪発生履歴等

3. インストアブランチの出店にあたっては、出店先の設備状況についても考慮する必要がある。

4. インストアブランチでは、出店先の設備状況およびインストアブランチの要員体制に応じた安全対策が必要である。インストアブランチの安全対策としては、以下のようなものがある。
   (1) 防犯カメラおよび防犯ビデオ 【設 103】【設 113】
   (2) 警察、警備会社のステッカー
   (3) 警察官の立ち寄り
   (4) 警備員の巡回
   (5) 非常押ボタンの設置、非常押ボタンの携帯 【設 113】

6　コンビニ ATM

削除: （ＸＩ）

コンビニ ATM は自動機器室に設置された CD・ATM とは異なり、コンビニエンスストアという不特定多数の人が行き来する場所で自動機器室、機械室がなく単体で設置されることが多い。このため、コンビニ ATM、利用者およびメンテナンス要員等の安全性に考慮した運用を行うことが必要である。

コンビニ ATM

適　用　区　分				
共	セ	本	提	ダ
			◎	

実 74	出店先の選定基準を明確にすること。

削除: 運　93

コンビニ ATM および利用者の安全性を確保するため、出店先地域やコンビニエンスストアの選定基準を明確にすること。

1. コンビニ ATM および利用者の安全性を確保するため、出店先地域やコンビニエンスストアの選定基準を明確にすることが必要である。

2. 明確にする選定基準としては、以下のようなものがある。
   (1) コンビニエンスストアの経営体質、警備方針
   (2) 出店先地域における過去の犯罪発生履歴等

3. コンビニ ATM の出店にあたっては、出店先の設備状況についても考慮する必要がある。

4. コンビニ ATM では、出店先の設備状況およびコンビニエンスストアの店員に対する安全対策が必要である。コンビニ ATM および利用者の安全対策としては、以下のようなものがある。
   (1) 防犯カメラおよび防犯ビデオ 【設 103】【設 137】
   (2) 警察、警備会社のステッカー
   (3) 警察官の立ち寄り
   (4) 警備員の巡回
   (5) 駐車場の照明
   (6) 非常押ボタンの設置、非常押ボタンの携帯 【設 137】

コンビニ ATM

適　用　区　分				
共	セ	本	提	ダ
			◎	

実 75	現金装填等メンテナンス時の防犯対策を講じること。

削除: 運　94

コンビニ ATM のメンテナンス時の安全性を確保するため、防犯体制および防犯方法を明確にすること。

1. コンビニ ATM は開放的な場所に設置されるため、現金装填等メンテナンス時の防犯体制および防犯方法を明確にすることが必要である。

2. 現金装填等メンテナンス時の具体的な防犯対策としては、以下のようなものがある。
(1) 犯罪が発生しやすい深夜等の装填は行わない。
(2) 現金装填は直接現金が人目に触れない方式とし、短時間で実施できるようにする。
(3) 現金装填は警備会社等防犯の専門家に委託する。
(4) 本体扉の内側に非常通報装置等を設置する。

3. コンビニ ATM の鍵をコンビニエンスストアに置くことは店員が犯罪に巻きこまれる可能性が高くなる。このため、コンビニエンスストアではコンビニ ATM の鍵を管理せず、警備会社または金融機関等の専門家が管理することが望ましい。

4. カード情報の不正な読取装置等の設置を防ぐなどの防犯上の観点から、巡回時等にコンビニ ATM 等の周囲に不審な装置がないか確認することが必要である。また、最新の犯罪状況等を踏まえ、カード情報の不正な読取装置などに関する情報を巡回者に適宜教育・周知することが必要である。

コンビニ ATM

適　用　区　分				
共	セ	本	提	ダ
			◎	

実 76	障害時・災害時対応手順を明確にすること。

削除: 運　95

コンビニ ATM の障害時・災害時に迅速な対応を行うため、その対応手順を明確にすること。

1.　コンビニ ATM の障害時・災害時の対応手順を明確にしておくことが必要である。

2.　具体的なコンビニ ATM の障害時の対応項目としては、以下のようなものがある。
(1) 顧客への状況連絡方法、説明方法
(2) 顧客へのカード等の返却方法
　自動返却、警備会社等による個別手作業返却が考えられる。
(3) 特定店に障害が限定されている場合における他店への誘導
(4) 自社ホストに係わる障害でない場合に最寄の CD･ATM への誘導
(5) 回復後のサービス時間延長への対応
(6) 関係者（営業店、本部、コンピュータセンター、警備会社等）の招集方法および役割
(7) コンビニ ATM の電源設備等の障害対策状況の確認とその対策
(8) コンビニ ATM の回線設備等の状況の確認とその対策

3.　災害時における対応方法についても、障害時の対応手順を参考にして検討、整理しておくことが必要である。

コンビニ ATM

適　用　区　分				
共	セ	本	提	ダ
			◎	

実 77	ネットワーク関連機器、伝送データの安全対策を講ずること。

削除: 運　96

伝送データの安全性、信頼性を確保し、また不正使用、破壊、改ざん等を防止するため、ネットワーク関連機器の適切な保護措置および伝送データの安全対策を講ずること。

1.　ネットワーク関連機器は、適切な保護措置を講ずることが必要である。【運 58】

2.　伝送データの安全対策を講ずることが必要である。回線は、コンビニエンスストア等の回線とは別の回線であることが望ましい。

3.　伝送データの安全対策としては、以下のようなものがある。
(1) 伝送データの重要性に応じた適切な漏洩防止策　【技 29】
(2) 伝送データの不正な破壊や改ざん等を早期に発見するための適切な検知策　【技 33】

コンビニ ATM

適　用　区　分				
共	セ	本	提	ダ
			◎	

実 78	所轄の警察および警備会社等関係者との連絡体制を確立すること。

削除: 運　97

犯罪発生時に関係者へ迅速に連絡を行うため、所轄の警察および警備会社等関係者との連絡体制の確立および訓練を行うこと。

1. 犯罪発生時に警察および警備会社等への迅速に連絡できる体制の確立および訓練を行うことが必要である。

2. 出店時および日頃から所轄の警察等に認識してもらうとともに連絡を取ることが望ましい。

3. 犯罪抑止策として、出入口等に警察や警備会社等のステッカーを貼ることが望ましい。例えば、警官立ち寄り所、警備会社等のステッカー等がある。

4. 迅速で簡素化された連絡体制の確立および訓練としては、以下のようなものがある。
   (1) 店舗警備と連動した一括した管理
   (2) 非常押ボタンが押下されたときの運用の明確化および訓練
   (3) 運用マニュアル
   (4) 店員に対する教育および訓練

5. 迅速な連絡を行うための装置としては、以下のようなものがある。
   (1) 非常押ボタン
   (2) リモート監視装置

コンビニ ATM

適　用　区　分				
共	セ	本	提	ダ
			◎	

実 79	顧客に対して犯罪に関する注意喚起を行うこと。

削除: 運　98

顧客ならびに取引の安全性を確保するため、犯罪に関する注意喚起を行うこと。

1.　内容は【運 51-1】参照のこと。

7　デビットカード

削除: （ＸⅡ）

デビットカード・サービスの安全性を確保するためには、顧客（口座保有者）、カード発行金融機関等、加盟店金融機関等、加盟店等が各々、そして共に協力する必要がある。ここではデビットカード・サービスの安全対策として金融機関等が留意すべき事項を記述する。

なお、日本デビットカード推進協議会が会員向けに策定したセキュリティガイドラインが存在する。（本ガイドラインは、会員の金融機関、情報処理センター、加盟店等に対して端末、ネットワーク等の機能、運用等について、遵守を義務づけている。）

(1)　デビットカード・サービスの安全性確保

削除: １．

デビットカード・サービスの安全性を確保するため、金融機関等はサービスの提供形態に応じて、情報処理センターや加盟店等と共に総合的な安全対策を実施することが必要である。

デビットカード
デビットカード・サービスの安全性確保

適　用　区　分				
共	セ	本	提	ダ
			◎	

実 80	デビットカード・サービスにおける安全対策を講ずること。

削除: 運 99

デビットカード・サービスの安全性を確保するため、金融機関等はサービスの提供形態に応じて、情報処理センターや加盟店等と共に安全対策を講ずること。

1. デビットカード・サービスの安全性を確保するため、金融機関等はサービスの提供形態に応じて、情報処理センターや加盟店等と共に総合的な安全対策を講ずることが必要である。

2. サービスの提供形態に応じて検討する安全対策としては、以下のようなものがある。
   (1) 顧客データの適切な保護 【運 53】
      ・口座番号等のカード情報が記載された印刷物の適切な管理
   (2) 顧客への注意喚起 【運 102】
   (3) 口座番号、暗証番号等の安全性の確保 【運 100】
   (4) デビットカードの不正使用の防止策
      ・加盟店の店員によるカード券面の確認による不正なカードの検知 【技 40】
      ・カードの不正使用取引の検知 【技 46】
   (5) デビットカードをデビットカード端末で読み取る際の安全対策上の配慮
      ・加盟店の店員による顧客の目の届く範囲でのカードの読取り
      ・顧客本人によるカードの読取り
   (6) 犯罪抑止ならびに犯罪者を特定しやすくする措置
      ・適切な利用限度額の設定等 【運 101】
      ・加盟店への防犯カメラ等の設置 【設 103】
      ・デビットカード端末が正当な加盟店に設置されていること
   (7) セキュリティ管理と責任の明確化 【運 1～運 6】
   (8) セキュリティ教育の実施 【運 80】

デビットカード
デビットカード・サービスの安全性確保

適　用　区　分				
共	セ	本	提	ダ
			◎	

実 81	口座番号、暗証番号等の安全性を確保すること。

削除: 運　100

口座番号、暗証番号等の安全性を確保するため、金融機関等はサービスの提供形態に応じて、情報処理センターや加盟店等と共に安全対策を講ずること。

1.　口座番号、暗証番号等の安全性を確保するため、金融機関等はサービスの提供形態に応じて、情報処理センターや加盟店等と共に総合的な安全対策を講ずることが必要である。

2.　口座番号等の安全性の確保としては、以下のようなものがある。
(1) デビットカード端末からの盗難防止策
・端末の耐タンパー性による保護
・カード情報の暗号化による保護
(2) 伝送データからの漏洩防止策　【技 29】
(3) 利用明細書等からの口座情報等の漏洩防止策
・利用明細書への口座番号等のカード情報を一部あるいはすべて非印字
・端末への口座番号等のカード情報を一部あるいはすべて非表示
(4) デビットカードの偽造防止策　【技 40】

3.　暗証番号の安全性の確保としては、以下のようなものがある。
(1) デビットカード端末からの盗難防止策
・端末の耐タンパー性による保護
・カード情報の暗号化による保護
(2) 伝送データからの漏洩防止策　【技 29】
(3) 蓄積データからの漏洩防止策　【技 28】
(4) 暗証番号の盗み見防止策
・暗証番号入力用のキーパッドへのかざしの設置
・暗証番号を入力する場所のパーティション等の設置
・加盟店に防犯カメラ等を設置する場合は、暗証番号を入力する際の顧客の手元が映らないような配置の工夫
(5) 他人に推測されにくい暗証番号の使用　【運 17】
(6) 顧客本人による暗証番号の変更　【運 51、運 101】
(7) 顧客への注意喚起　【運 17、運 51-1】

7　デビットカード

削除：（ⅩⅡ）

(2)　顧客保護

削除：２．

顧客がデビットカードを利用する際の安全性を確保するために、適切な顧客保護の措置を講ずる必要がある。

デビットカード
顧客保護

適　用　区　分				
共	セ	本	提	ダ
			◎	

実 82	デビットカード利用時の顧客保護の措置を講ずること。

削除: 運　101

デビットカード利用時の安全性を確保するため、適切な顧客保護の措置を講ずること。

1.　顧客がデビットカードを利用する際の安全性を確保するために、適切な顧客保護を講ずることが必要である。

2.　デビットカード利用における顧客保護の措置としては、以下のようなものがある。

(1) デビットカード利用上の留意事項を顧客に注意喚起する。【運 102】

(2) 1 日当たりの利用限度額等を設ける。

・利用限度額を一律に設定する。

・利用限度額を顧客本人が選択、変更可能とする。

(3) デビットカードとして利用する要否を顧客本人が選択、変更可能とする。

(4) デビットカードの紛失、盗難、偽造等により発生した顧客の損失を補償するための適切な対策を講ずる。

(5) CD･ATM 等により顧客本人が暗証番号を変更可能とする。【運 51】

7　デビットカード

削除：（Ⅹ Ⅱ）

(3)　顧客への注意喚起

削除：３．

デビットカードは、従来のキャッシュカードに新しい機能が付加される形態をとるため、顧客に対してサービス内容や安全性等の留意事項をわかり易く明示することが必要である。

デビットカード
顧客への注意喚起

適　用　区　分				
共	セ	本	提	ダ
			◎	

実 83	デビットカード利用上の留意事項を顧客に注意喚起すること。

削除: 運　102

顧客に注意を喚起するため、デビットカード利用上の留意事項を顧客に明示すること。

1. デビットカードは、従来のキャッシュカードに新しい機能が付加される形態をとるため、顧客に対してサービス内容や取扱い上の留意事項をわかり易く明示することが必要である。

2. デビットカードのサービス内容や留意事項の顧客への周知方法としては、以下のようなものがある。
   (1) 取引規定への記載
   (2) カードの裏面等への記載
   (3) デビットカードや CD・ATM の利用明細書への記載
   (4) DM への記載
   (5) 店頭や自動機器コーナーのポスターへの記載
   (6) 金融機関等のホームページへの記載
   (7) 新聞広告等

3. 周知する留意事項としては、以下のようなものがある。
   (1) デビットカードとして利用できるカードの種類と特徴
   (2) デビットカードのサービス利用可能時間帯
   (3) 暗証番号を他人に知られないようにすること 【運 17】
   (4) 本人が暗証番号をデビットカード端末に入力すること
   (5) 利用明細書を持ち帰るようにすること
   (6) 通帳記帳時等の日付、利用金額、残高の確認
   (7) デビットカード利用口座の限定等
   (8) 暗証番号の変更方法 【運 51、運 101】
   (9) 利用限度額等の利用条件や変更届けの有無や届出方法
   (10) デビットカードの利用停止届けの有無や届出方法
   (11) 紛失、盗難、破損時の届出方法
   (12) 紛失、盗難、偽造等により発生した損害に対する責任や補償

8　オープンネットワークを利用した金融サービス

削除: （ⅩⅢ）

(1)　インターネット、モバイル

削除: 1．

利用者との取引を安全に実施するために、オープンネットワークに関するさまざまな脅威に対する安全対策を講ずることが必要である。

オープンネットワークでのビジネス展開に対する脅威としては、例えば盗聴、なりすまし、情報の改ざん、不正侵入のうえでのホームページの書換え等がある。これらの脅威に対応するために、必要な情報システムへの安全対策を実施することが望ましい。

削除: 上

また、サービス利用に関する注意喚起等、顧客対応方法を明確にする必要がある。

オープンネットワークでのビジネスとしては、銀行取引、証券取引、生損保取引等の金融サービスがある。

オープンネットワークを利用した金融サービス
インターネット、モバイル

適　用　区　分				
共	セ	本	提	ダ
				◎

実84	不正使用を防止すること。

削除: 運　103

オープンネットワークを利用した金融サービスの安全性を確保するため、接続相手先が本人であることを確認する予防策やアクセス制限、検知策等の不正使用防止機能を設けること。

1.　不正使用防止策として、厳正な本人確認を実施することが必要である。特に資金移動及び注文等の取引に関しては、より厳正な本人確認を実施することが必要である。

2.　不正使用防止策としては、以下のような例がある。また、必要に応じて複数の対策を組み合わせることが望ましい。

(1) 予防策

①　パスワード　【技 35】
②　パスワードの入力失敗回数の制限及び監視　【技 36】
③　ログイン時の本人認証に加え、資金移動、注文等の取引確定時や、ID・パスワード、住所、登録メールアドレス等重要な登録事項の変更時等における更なる本人認証の実施
④　指紋などバイオメトリクス　【技 35】
⑤　同時ログオンの禁止
⑥　前回の最終ログオフ日時の明示　【技 36】
⑦　無アクセス時間による自動ログオフ　【技 36、技 37】
⑧　コールバックによる端末、本人確認　【技 35】
⑨　クライアント証明書の導入　【技 35】
⑩　通常使用している端末以外からのログイン時や、通常とは異なる取引が行われた時等、取引のリスクに応じた更なる本人確認　【技 35】
⑪　暗号化　【技 35】
⑫　電子署名　【技 35】
⑬　Web アプリケーションの脆弱性対策　【技 43】
⑭　フィッシング対策　【技 49】(参考２)
⑮　利用者機器（パソコンなど）のシステム環境チェック機能
⑯　取引内容をモニタリングし、疑わしい取引や異常を検知した場合は取引を一時的に中断する仕組み
⑰　ハードウェアトークン等を利用したトランザクション認証

(2) 外部ネットワークからのアクセス制限

①　プロバイダー（ドメイン）限定　【技 43】

② プロバイダーとの専用線接続【技 43】
③ 登録済み IP アドレスのみ接続を許可する 【技 35】

(3) 検知策
① 不正侵入検知時、ログオン失敗を検知した場合のアラーム鳴動 【技 45】
② 前回の最終ログオフ日時の明示 【技 45】
③ 暗号技術を活用した認証、並びに暗号技術を活用した改ざん検知 【技 33】
④ 送金等の取引や重要事項の変更があった際の顧客への通知 【技 46】
⑤ 同一 IP アドレスからの複数アカウントによるログインの検知

なお、既に発見され、公表されている不正行為（侵入や組込みの手口）の事例は、防御対策、検知対策に対する有益な情報となることが多い。したがって、これらについて記載されている文献や、ガイド等を参考にすることも有用である。

3. 脆弱性が発見または報告された場合の手順を決めておくことが必要である。

4. 不正を検知した場合の手順を決めておくことが必要である。

（参考 1）
サイバーテロの脅威とその対策
(1) サイバーテロとは、重要インフラの基幹をなす重要な情報システムに対して、情報通信ネットワークや情報システムを利用した電子的な攻撃のことを言う。サイバーテロにより国民生活や社会経済活動に重大な影響を及ぼす可能性があることが懸念される。
(2) 外国においては、金融機関等の情報システムが被害を受けた事例や、個人がいわゆるハッカーとして、重要インフラ等の情報システムに対する侵入、サービス不能攻撃（DoS 攻撃）、コンピュータウイルスの流布等によって重大な被害を起こした事例もある。
(3) 政府では、内閣官房を中心として、官民の緊密な連携の下、「情報セキュリティ対策に係る行動計画」等の実施に努めている。
(4) 個別金融機関等においては、サイバーテロによる被害の可能性を極力少なくするために、外部ネットワークからのアクセス廻りの強化を行う等、ネットワークセキュリティ対策を強化することが望まれる。

（参考 2）
重要インフラ防護のための政府のサイバーテロ対策
・重要インフラの情報セキュリティ対策に係る第 2 次行動計画（平成 24 年 4 月 26 日改定）
http://www.nisc.go.jp/

（参考 3）
不正アクセス対策、Web アプリケーションの脆弱性、セキュアプログラミング等については、独立行政法人情報処理推進機構（IPA）セキュリティセンターに詳しい情報があるので参照されたい。
・独立行政法人情報処理推進機構（IPA）セキュリティセンター
http://www.ipa.go.jp/security/index.html

（参考 4）
フィッシング対策の参考文献として、以下のものがある。
・「フィッシング対策ガイドライン」フィッシング対策協議会

（参考 5）
スマートデバイスを用いたインターネットバンキングサービス提供時の考慮点
(1) スマートデバイスは携帯性に優れている反面、紛失・盗難のリスクが高く、Web サイトにおける不正使用対策の充実が求められる。この対策として、【技 35】を参照されたい。
(2) スマートデバイスは、画面サイズの制約により接続した URL が一部しか表示できないため、不正な URL に気づかずフィッシングサイトにアクセスするリスクがある。 このようなフィッシング詐欺への対策については、（参考 4）にある「フィッシング対策ガイドライン」を参照されたい。

オープンネットワークを利用した金融サービス
インターネット、モバイル

適　用　区　分				
共	セ	本	提	ダ
				◎

実85	不正使用を早期発見すること。

削除: 運　104

利用者を不正使用から守るため、利用者自身が使用状態を確認する機能を設けること。

1.　ユーザーID 等が不正使用されていないか、利用者自身で確認可能にすることが必要である。特に資金移動および注文等の取引に関しては、不正使用の早期発見のため、処理結果が確認できる機能を提供することが重要である。

　なお、不正に使用されていないかの確認を利用者自身が行うことを注意喚起することも重要である。

2.　不正使用の早期発見対策としては、以下のようなものがある。

(1) ログイン日時とログオフ日時の履歴表示　【技 45】
(2) 資金移動、注文処理結果等の取引結果表示
(3) 資金移動、注文処理結果等を郵送または登録アドレスへ電子メールで通知
(4) ID・パスワード、登録メールアドレス等重要な登録事項の変更処理結果等を郵送または登録アドレスへ電子メールで通知、住所変更の場合は登録アドレスへ電子メールで通知

　なりすましによるメールアドレスの変更を検知するため、登録アドレスの変更の際は、新旧登録アドレスに変更通知を出すことも有効である。通知する内容としては、変更受付日時、変更に心当たりがない場合の連絡先がある。

　なお、電子メール等を用いる際は顧客データが漏洩しないよう文面等に注意すること。例として、取引があったことだけを記載し、取引内容は記載しない文面とすることなどが考えられる。

オープンネットワークを利用した金融サービス
インターネット、モバイル

適　用　区　分				
共	セ	本	提	ダ
				○

実86	安全対策に関する情報開示をすること。

削除: 運　105

利用者が適切に取引機関や金融サービスの選択を行うため、安全対策に関する情報を開示することが望ましい。

1. 利用者が適切に取引機関や金融サービスの選択を行えるよう、金融機関等はセキュリティ方針等を開示することが望ましい。

2. 開示内容としては、以下のようなものがある。
(1) 情報漏洩防止のために暗号化していること。
(2) なりすまし防止のために認証（パスワード、電子認証）を行っていること。
(3) 顧客に関する厳密な守秘義務に基づき、顧客データを保護していること。

3. 開示方法としては、以下のようなものがある。
(1) DM への記載
(2) 店頭や自動機器コーナーのポスターへの記載
(3) 金融機関等ホームページへの記載
(4) 新聞広告等
(5) 電子メール

4. 開示にあたっては図等を使用し、利用者に理解しやすいように工夫することが望ましい。

5. 利用者からの問合せおよび苦情に対応することが望ましい。
(1) 相談窓口の設置
(2) パンフレット、ホームページ等に連絡先を明記

6. 利用者への安全対策に関する情報開示を実施するにあたっては、当センター発刊の「安全対策に関する情報開示研究会報告書」等を参照のこと。

オープンネットワークを利用した金融サービス
インターネット、モバイル

適　用　区　分				
共	セ	本	提	ダ
				◎

実87	顧客対応方法を明確にすること。

削除: 運 105-1

インターネット、モバイル等を用いた金融サービスにおいて、注意喚起や受付対応等の顧客対応方法を明確にすること。

1.　サービスの利用に関して顧客に周知すべき事項としては、以下のような例がある。
(1) サービス内容・規約
(2) 操作方法
(3) 顧客対応窓口
(4) 金融機関等が実施している安全対策の概要等
(5) 顧客の利用環境（利用可能な機種やブラウザ等）
なお、顧客の利用環境を周知する場合には、以下の内容を Web サイトに掲載、またはインターネット利用取引の開始案内で利用者に通知することが必要である。
・OS（必須パッチが含まれる場合はその内容を含む）
・ブラウザとその設定
・必要となるプラグイン
・専用ソフトがある場合はそのバージョン 等

2.　口座が不正に利用されることを防止するため顧客に注意喚起すべき事項としては、以下のような例がある。
(1) 他人に ID やパスワード、乱数表、トークンといった本人確認用の情報や媒体を渡さないこと
(2) 推測されやすいパスワードを使用しないこと
(3) パスワードを他のパスワードと共用しないこと
(4) 不特定多数の者が使用するパソコンでは金融機関との取引を行わないこと（スパイウェアによりパスワード等が盗まれる危険性がある）
(5) 警察官や金融機関の職員がパスワードを直接顧客に照会することはないこと（警察官や金融機関の職員を詐称し、パスワードを聞きだす犯罪行為があること）
(6) パスワードは定期的に変更することが望ましいこと
(7) パスワードをメモ等に残した場合のリスクを認識すること（紙に書いた場合やパソコンやスマートデバイスにファイルで保管した場合には盗難のリスクがある）
(8) 使用するパソコンやスマートデバイス等への市販または金融機関が配布する抗ウイルスソフトやセキュリティパッチ等の適用と、その最新化
(9) 基本ソフト（OS）やウェブブラウザ等、インストールされている各種ソフトウェアを最新の状態に更新しておくこと
(10) 金融機関の正当なサイトであることの確認手段（不用意に ID・パスワード等の本人確認

用情報を入力すると、フィッシング等の詐欺を目的とした偽サイトに入力している場合がある）
(11) 金融機関からの正当なメールであることの確認手段
(12) （金融機関が利用者向けアプリケーションを提供している場合）アプリケーションが正式なものであることの確認手段【技 49】
(13) 不審な CD-ROM 等の受領時は、金融機関の公式ホームページ等で確認すること
(14) 使用するパソコンを廃棄する際には、ツールの使用等によりハードディスク内のデータを完全に消去すること
(15) 金融機関が乱数表の全内容の入力を求めることはないこと
(16) ワンタイムパスワードの利用を推奨すること
(17) 可能であれば、インターネットバンキングへのログイン等に使用するパソコンの利用目的を限定し、使用していないときには電源を切ること【技 44】。また、法人であれば取引の申請者と承認者とで異なるパソコンを利用することも有効であること。
(18) 取引明細や取引通知メール等から、身に覚えのない取引がないか確認すること
(19) 電子証明書は、金融機関等が指定した正規の手順以外では利用しないこと
(20) （顧客ごとに振込等の限度額の設定が可能な場合）限度額については取引上の必要性に応じてできるだけ低く設定すること【技 38】

3. 顧客への周知の方法としては、以下のような例がある。
(1) 口座開設時における説明及びパンフレット等への明記
(2) 電話による通知
(3) ホームページへの掲載
(4) メールによる通知
なお、ホームページへの掲載に際しては、改ざん防止策を実施すること。
また、メールによる通知時にはそれ自体が情報の漏洩につながらないよう、文面には注意するとともに、なりすまし防止、改ざん防止策を実施すること。

4. 不正使用の早期発見のため、定期的に残高や取引履歴を確認するよう顧客に推奨することが望ましい。

5. 顧客からの問合せや相談、届出に対応する窓口を整備すること。また、届出を受け付けた場合は定められた方法により対応すること。
顧客からの届出を速やかに受け付ける体制の整備が必要な時間帯としては、インターネットバンキングでのサービスの場合、例えば振込が可能な時間帯及びその前の一定の時間帯とすること等が考えられる。

6. 顧客からの問合せや届出としては、以下の例がある。
(1) サービス内容や規約に関する照会
(2) 操作方法の照会
(3) 取引に用いる携帯電話や IC カード等の紛失による利用停止等の届出
(4) 口座残高や取引履歴に疑義が生じた場合の利用停止等の届出
(5) フィッシングメールや偽サイト（フィッシングサイト）に関する通報
(6) 不正取引の届出

(7) インターネットバンキング利用中に、利用マニュアル等に記載されているものとは異なる画面が表示された場合の照会

7. 被害の拡大防止のため、犯罪が発生した際の対応方針を定めておくこと。具体的な内容としては以下の例がある。

(1) 被害に遭った口座のインターネット取引を停止する。

(2) スパイウェアやフィッシングなどにより不正取引が発生した場合には、ホームページ上での公表に加え、個別メールによる周知を行う。

また、犯罪手口についても可能な限り公表する。

なお、公表・周知の時間帯としては、個人顧客は夕刻以降にアクセスすることが多いなど、顧客の利用傾向も踏まえ、多くの顧客が利用開始する時間帯までに可能な限り公表・周知を行う。

(3) フィッシングにより不正取引が発生した場合には、当該フィッシングサイトの閉鎖等の対応を行う。なお、閉鎖に際しては専門機関との連携やフィッシングサイト閉鎖サービス事業者の利用も有効である。

(4) 原因究明・捜査協力のため、被害に遭った顧客が特定できる場合には、当該顧客に対して使用したパソコン等の現状を保全し、警察に連絡するよう要請する。

(参考 1)

コンピュータウイルス等の不正プログラム対策やフィッシング対策等、利用者に周知すべき事項に関する情報を公開している公的な Web サイトを以下に示す。

独立行政法人情報処理推進機構（IPA）セキュリティセンター
http://www.ipa.go.jp/security/index.html

警察庁サイバー犯罪対策
http://www.npa.go.jp/cyber/

警察庁セキュリティポータルサイト@police
http://www.cyberpolice.go.jp/

フィッシング対策協議会
https://www.antiphishing.jp/

(参考 2)

フィッシングサイト閉鎖の協力を行う専門機関としては以下が挙げられる。

一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
http://www.jpcert.or.jp/form/

オープンネットワークを利用した金融サービス
インターネット、モバイル

適　用　区　分				
共	セ	本	提	ダ
				◎

実 88	インターネットやモバイル等を用いた金融サービスの運用管理方法を明確化すること。

削除: 運 106

インターネットやモバイル等を用いた金融サービスにおいて、利用者を保護し、安全性を確保し円滑に稼働させるため、運用管理方法を明確化すること。

1.　不正な取引を防止する対策としては、以下のようなものがある。
(1) 伝送データの漏洩防止策　【技 29】
(2) 本人確認機能　【技 35】
・認証機関が発行する電子的な証明書等による認証（【技 35】参考 1 項番 6）
・取引の重要度に応じた、ログインパスワードとは異なるパスワード設定
・パスワードの入力失敗回数の制限と監視
・パスワード再発行時の本人確認の厳格化（リマインダー機能において回答が推測できる質問を提供しない　等）
(3) アクセス履歴の管理　【技 37】
(4) 取引制限機能　【技 38】
・顧客より資金移動先や限度額の登録を受け、取引を制限する
(5) 事故時の取引禁止機能　【技 39】
(6) 暗号鍵の保護機能　【技 42】
(7) 不正侵入防止機能　【技 43】
(8) 不正アクセス監視機能　【技 45】
(9) 異常な取引状況の把握機能　【技 46】
・取引履歴や取引結果を利用者自身が確認可能とする
(10) 異例取引監視機能　【技 47】
(11) 不正アクセス時の復旧策　【技 48】
(12) DNS サーバーの登録状況の管理
・TLD（Top Level Domain）レジストリへの登録情報が正しいこと
・ドメイン名の設定情報が正しいこと

2.　顧客の誤操作や誤認を防止する対策としては、以下のようなものがある。
(1) リンク等による利用者の誤認・混同防止策
(2) 取引確定前に確認のための画面を表示する等の操作支援機能

3.　サービスの信頼性を向上させる対策としては、以下の例がある。
(1) 予想される取引量に対するインターネットサービス・プロバイダーとの間の十分な回線容

量の確保や予備の設置 【運 54】【技 5】
(2) 予想される取引量に対し十分な性能を持つサーバーの導入や予備サーバーの設置【技 2～4】
(3) システムの負荷状態の監視、制御やトラフィック制御機能の設定 【技 18】

4. 障害時・災害時対応手順を明確にすることが必要である。【運 63】

（参考 1）
コンピュータウイルス等の不正プログラム対策やフィッシング対策等、利用者に周知すべき事項に関する情報を公開している公的な Web サイトを以下に示す。

独立行政法人情報処理推進機構（IPA）セキュリティセンター
http://www.ipa.go.jp/security/index.html

警察庁サイバー犯罪対策
http://www.npa.go.jp/cyber/

警察庁セキュリティポータルサイト@police
http://www.cyberpolice.go.jp/

フィッシング対策協議会
https://www.antiphishing.jp/

（参考 2）
フィッシングサイト閉鎖の協力を行う専門機関としては以下が挙げられる。

一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
http://www.jpcert.or.jp/form/

参照法令	金融商品の販売等に関する法律、消費者契約法

8　オープンネットワークを利用した金融サービス

削除：（ⅩⅢ）

(2)　電子メール

削除：２．

電子メールを利用し、利用者に対して取引通知、情報提供および問合せ等のサービスを行う場合には、電子メールの特徴等を考慮し、対象業務の判断およびその運用方針を明確にすることが必要である。

オープンネットワークを利用した金融サービス
電子メール

適　用　区　分				
共	セ	本	提	ダ
				◎

実89	電子メールの運用方針を明確にすること。

削除: 運　107

電子メールの運用にあたっては、信頼性、安全性を確保するため、その運用方針を明確にすること。

1.　電子メールを利用し、利用者に対して取引通知、情報提供および問合せ等のサービスを行う場合には、電子メールの危険性を考慮する必要がある。考慮する電子メールの危険性とは、以下のようなものがある。
(1) 盗聴およびなりすましの可能性
(2) 情報漏洩に利用される可能性
(3) 送信先を間違い、誤った宛先に送信する可能性
(4) コンピュータウイルスに感染する可能性
(5) コンピュータウイルスに感染した添付ファイルを送信する可能性
(6) 遅延および紛失する可能性
(7) 同一ネットワークを利用する他業務システムのレスポンスに影響を与える可能性
(8) システム障害による業務中断の可能性

2.　電子メールの危険性を考慮し、電子メールの運用方針を明確にする必要がある。明確にする電子メールの運用方針としては、以下のようなものがある。
(1) 不正アクセス防止のための方策　【運 17】【技 35】
(2) 機密漏洩防止のための方策
(3) コンピュータウイルスチェック　【技 49～51】
(4) 添付ファイルの取扱い
(5) 送受信容量の制限
(6) なりすまし防止の方策
フィッシング等によるなりすましを防止する方策としては、以下のものがある。
・電子署名の使用
・メール本文中には URL を記述しない。
・メールの形式は、HTML をできるだけ使用しない。

3.　取引通知、情報提供および問合せ等で電子メールを利用する場合は、その運用方針を明確にすることが必要である。明確にする運用方針としては、以下のようなものがある。
(1) 取引データの保護策
(2) 取引等に必要な情報の保管

(3) メッセージ受領確認の方策
(4) 障害発生時における業務継続策
(5) 施設面における保護対策

なお、取引データ等の保護のため、電子メールには取引時の情報を記載せず、金融機関のホームページでの照会を依頼するような文言とすることも考えられる。

また、登録アドレスへの電子メールの通知を確実なものとするため、登録アドレスの変更の際は、新旧登録アドレスに変更通知を出すことも有効である。通知する内容としては、変更受付日時、変更に心当たりがない場合の連絡先、がある。

4. 運用方針の管理を行う体制を明確にする必要がある。

11 ハードウェアの信頼性向上対策

削除: Ⅰ．システム信頼性向上対策

削除: （Ⅰ）

コンピュータシステムの信頼性を向上させるためには、まずシステムの構成要素であるハードウェアの信頼性向上が重要である。それには、コンピュータ本体および関連機器の障害発生を極力減少させることが必要である。

次に、ハードウェアの構成要素の一部に障害が生じても、システム全体に影響が及ばないような対策を講ずることが重要である。これらの対策は個々のハードウェアの特性や重要性に応じ実施されなければならない。

ハードウェアの信頼性向上対策
ハードウェアの障害予防策

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実92	予防保守を実施すること。

削除: 技　1

ハードウェアの障害を予防するため、装置の特性や重要度に応じ、予防保守を定期的または随時実施すること。

1.　コンピュータシステムの信頼性を向上させるためには、まずシステムの構成要素であるハードウェアの信頼性向上が重要であり、ハードウェアの障害の発生を極少化させるため、予防保守を実施することが必要である。

2.　予防保守の具体的事例として、以下のようなものがある。【運 59】

(1) 定期保守

定期保守とは、装置の特性や重要度に応じ、あらかじめ定められた点検項目および周期に従って、障害を未然に防止するために行うもので次の 2 つの形態がある。

①　全体保守

システム全体を停止して、総合的に行う予防保守である。

②　個別保守

システム運転時も含め、運用に影響を与えない範囲で、装置個別に行う予防保守である。なお、オペレータが始業前に行うクリーニング等も重要な項目である。

(2) 随時保守

随時保守とは、装置個別の使用状況、障害発生状況やエラーログ情報の収集・分析から今後の障害発生の可能性を察知し、障害を未然に防止するために随時行うものである。例えばオープン系の機器については、定期保守の対象外となっていることが多いため、随時保守を実施することが考えられる。

3.　特に、24 時間稼働システム等の長時間連続稼働システムにおいては、当該システムの機能および制約に応じた適切な予防保守を行うことが必要である。

ハードウェアの信頼性向上対策
ハードウェアの予備

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実93	本体装置の予備を設けること。

削除: 技 2

本体装置の障害時に迅速に対応するため、重要な本体装置には予備を設けること。

1. コンピュータシステムの中核となる重要な本体装置は、予備を設ける必要がある。
　また、物理的な予備装置を設けることのほか、並列処理装置や同一筐体内の複数の中央処理装置による継続運転の仕組みにより同等の効果を持たせることも可能である。

2. 本体装置とは、中央処理装置、主記憶装置、チャネル装置の総称であり、クライアントサーバー・システムの場合は、システムの中核となるサーバーを指す。

3. システムの目的や重要性に応じ、必要な予備（能力の余裕）を確保できるようにシステムを構築することが望ましい。
　特に、24 時間稼働システム等の長時間連続稼働システムにおいては、当該システムの機能及び制約に応じた予備（能力の余裕）を設けることが望ましい。
　なお、コンピュータシステムは本体装置のほか、周辺装置・通信系装置・回線・端末系装置等から構成されるため、障害が発生した場合に、それらの予備を含めたシステム全体が有効に機能することを確認しておく必要がある。

4. 本体装置の予備の持ち方には、以下のような例がある。
(1) デュプレックスシステム
　待機系の本体装置を備えておき、現用系に障害が発生した場合、待機系に切り替えて業務を続行できるシステムである。待機系の本体装置は、待機中ほかの業務で使用しても構わないが、現用系と同程度の能力を持っていることが望ましい（図 1）。
　なお、待機の形態によって以下の方式がある。
　①　ホットスタンバイ方式
　　事前にプログラムロード等の事前処理を一部行っておき、現用系に障害が発生したときに、直ちに業務を続行できるように待機している方式である。
　②　コールドスタンバイ方式
　　事前の処理は特に行っていないが、現用系に障害が発生したときに、切り替えて業務を続行できるように待機している方式である。

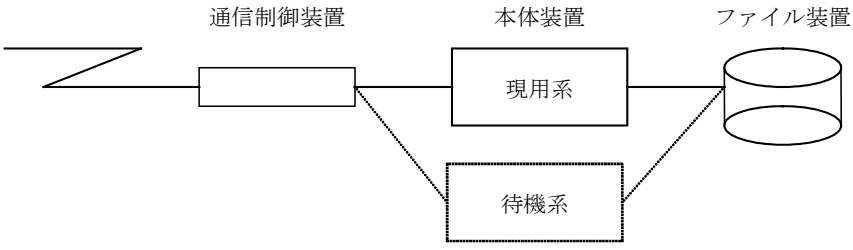


図１　デュプレックスシステムの例

(2) デュアルシステム

２つの系の本体装置を常時並列で運転して、互いに監視し合い、一方の系に障害が発生した場合は残りの系だけで運転を継続するシステムである。

(3) フォールトトレラントシステム

誤りもしくは障害となり得る状態にかかわらず、外部からみる限り、一定の性能を維持する能力を備えたシステムである。一般にはシステムの中の本体系装置、磁気ディスク装置等の主要なハードウェアを多重化することによってシステムが停止しない設計となっているフォールトトレラントシステム・コンピュータをメインフレームやサーバーに用いて構成したシステムである。

(4) マルチプロセッサシステム

性能と信頼性の向上をねらって、複数の中央処理装置（プロセッサ）を結合したシステム。

信頼性を向上させるため、ある中央処理装置に障害が発生しても、その中央処理装置を切り離して継続運転を行うことが可能な仕組みを持つ。

なお、切り離して運用する場合でも、ある程度の能力が確保できるように、中央処理装置の能力には余裕があることが望ましい（図２）。

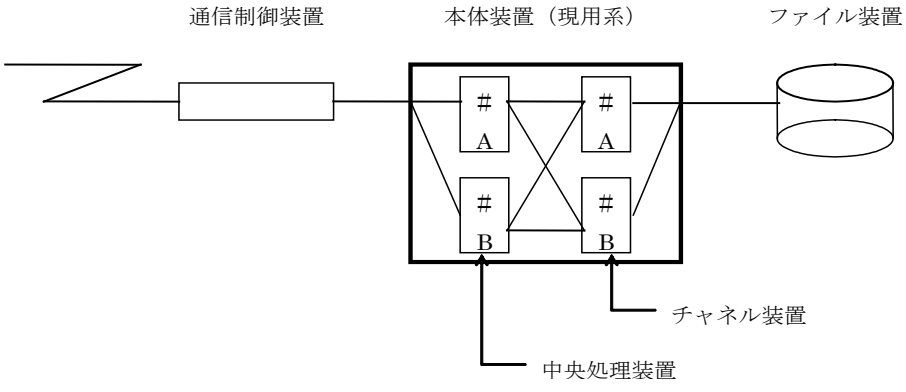


図２　マルチプロセッサシステムの例

(5) フェールオーバー機能

クライアントサーバー・システムにおいて、1つのサーバーが停止したときに別のサーバーが処理を代行する機能（図 3）。

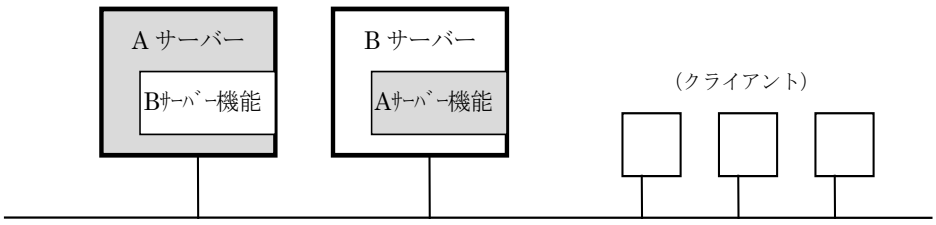


図 3　フェールオーバー機能の例

(6) 待機系セグメント構成（レプリカ構成）

クライアントサーバー・システム等において、重要なサーバーを含む LAN 構成そのものを二重化し、一方を待機系として持つ構成（図 4）。

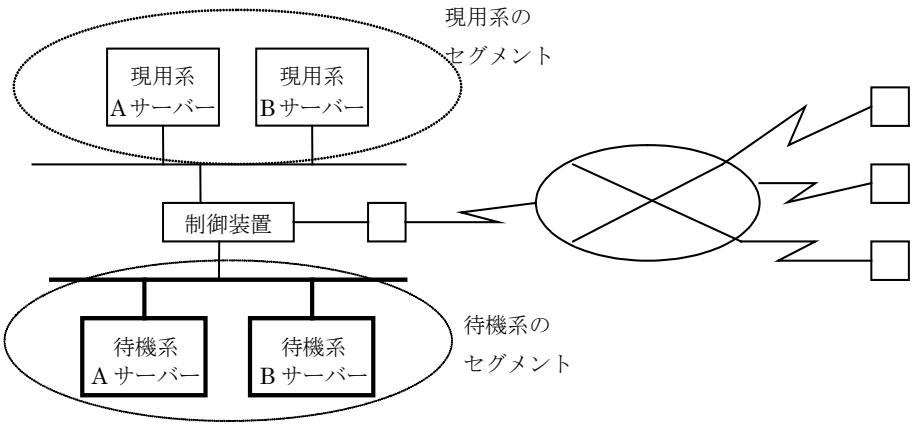


図 4　待機系セグメント構成の例

ハードウェアの信頼性向上対策
ハードウェアの予備

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実94	周辺装置の予備を設けること。

削除: 技 3

周辺装置の障害時に迅速な対応を行うため、重要な周辺装置は予備または代替機能を設けること。

1. 周辺装置には、ファイル装置（磁気ディスク装置、半導体ディスク装置、光磁気ディスク装置、磁気テープ装置等）、コンソールディスプレイ等の種類がある。
（サーバーの場合は、筐体内部のディスク装置も周辺装置に該当するものとする。）

2. 重要な周辺装置の予備または代替機能を設ける方法としては、以下のような例がある。
(1) 複数台の周辺装置ごとに予備を設ける。
なお、ファイル装置においては、通常はバッチ業務等で使用していて、障害発生時にオンライン用に切り替え、ファイルのリカバリ等を行い業務を続行させる方法もある。また、装置としての予備ばかりでなく、空き容量を持つことにより予備とする方法もある。
(2) 複数台設置により予備機装置と同様の効果を持たせる。
(3) 異種装置により代替させる。
ジャーナル情報を半導体ディスク装置に記録している場合､障害時に磁気ディスク装置に代行記録するような事例がある。
(4) ネットワーク上の他のサーバーのファイル装置に代替させる。
ネットワーク上の他のサーバーのファイル装置を自身のファイル装置の予備とする方法もある。
(5) 冗長構成を持ったディスクアレイを、ファイル構成装置として利用する。
（注）ディスクアレイとは、データを分解し、複数のディスクドライブに対して並列にリード＋ライトすることで、大容量、高性能、データの保護、無停止運転を可能にした磁気ディスク装置。RAID（Redundant Arrays of Inexpensive Disks）とも呼ばれる。
冗長性を持つディスクアレイの種類としては以下のようなものがある。
・RAID1（ミラーリング方式）
・RAID5（パリティ付ストライピング方式）

3. 重要なファイル装置と本体装置との間のアクセスパス（接続経路）について
重要なファイル装置については、代替パスを設け、アクセスパスの障害時に一群のファイル装置が使用不能となる事態の発生を回避する手段を講じておくことが考えられる。
アクセスパス構成法には、以下のような例がある（図 1）。

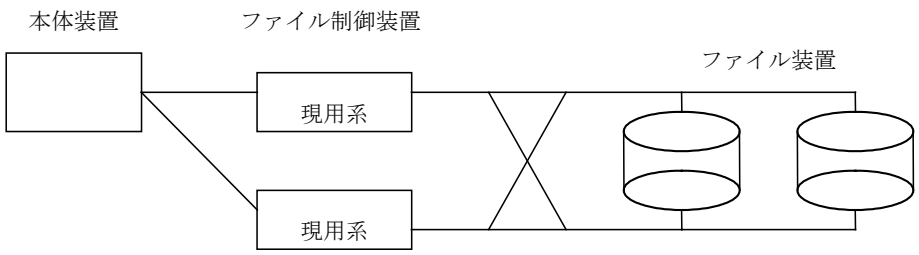


図１　アクセスパス構成例

4.　さらに高い信頼性が必要となるファイルは二重化を考慮することが望ましい。二重化の対象となる重要なファイルとしては、以下のような例がある。

・主要業務ファイル
・ジャーナルファイル
・その他システム系制御ファイル等

5.　【技 2】3. を参照。

ハードウェアの信頼性向上対策
ハードウェアの予備

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実95	通信系装置の予備を設けること。

削除: 技　4

通信系装置の障害時の迅速な対応のために、重要な通信系装置は予備を設けること。

1.　予備が必要な通信系装置には、以下のようなものがある。

(1) 通信制御装置

・通信制御部の予備構成例（図 1）

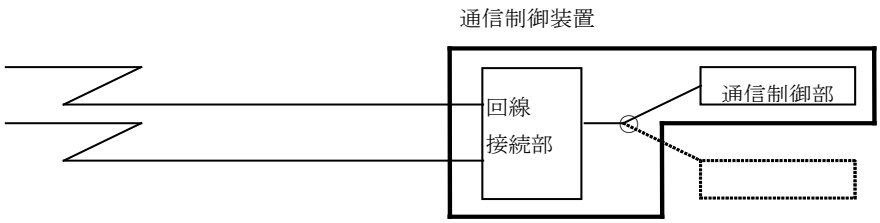


図 1　通信制御部の予備構成例

・通信制御部・回線接続部の予備構成例（図 2）

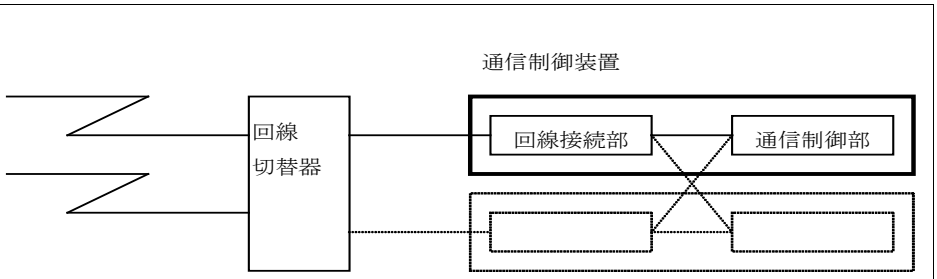


図 2　通信制御部・回線接続部の予備構成例

なお、複数台の通信制御装置ごとに予備を設置することも考えられる。また、回線切替器の設置等、それぞれの実情に応じた切替方法を検討することが必要である。

(2) 回線終端装置等

回線終端装置等についても、重要なものについては予備を設ける等、あらかじめ障害時に速やかな対応がとれるようにしておくことが必要である。なお、ここでいう回線終端装置等には時分割多重装置（TDM）やデジタル回線終端装置（DSU）等も含むものとする。

(3) ルータ等

ルータや HUB についても障害時の速やかな対応のために、重要なものについては予備が必要である。

なお、フィルタリング情報等のネットワーク設定情報を持つものについては、装置の予備だけでなく、設定情報のバックアップやリカバリの手順を含めて信頼性の向上対策が必要である。【運 31、運 32】

(4) 交換装置等

交換装置等についても障害時の速やかな対応のために、重要なものについては予備が必要である。なお、ここでいう交換装置等には、非同期転送モード（ATM）装置等も含むものとする。

（ATM：Asynchronous Transfer Mode）

削除: 及びフレームリレーユニット

2. 回線終端装置やルータ等の予備の持ち方として、自社で保有することのほかにベンダーとの保守契約において必要時に代替機の提供を依頼できるようにすることも有効である。

3. 【技 2】3. を参照。

ハードウェアの信頼性向上対策
ハードウェアの予備

適　用　区　分				
共	セ	本	提	ダ
	○	○		

実96	回線の予備を設けること。

削除: 技５

回線障害時の迅速な対応のために、重要な回線は予備を設けることが望ましい。

1.　回線の予備については、以下の点を考慮すること。

(1) 地点間（構外）の重要な回線は複数化するか、またはバックアップ回線を確保しておくことが望ましい。なお、回線を複数化する際は、物理的別ルート化（別の収容交換設備等（旧電話局）を経由するもの）を図ることが望ましい。また、回線のルートや回線容量等は、通信事業者に該当の回線の利用目的等を明示し、適切な設計・構築を図ることが望ましい。

(2) 構内回線についても、コンピュータセンター内の構内配線や、重要な部門 LAN については予備を設けることが望ましい。

2.　地点間（構外）の回線について

(1) 予備の具体的事例として、以下のようなものがある。

①　専用回線の複数化の例

・端末系装置を 2 つのグループに分け、それぞれ別々の回線に接続する方法

・回線の一方を予備とし、必要に応じて切り替える方法

②　電話回線（xDSL を含む）、 ISDN 回線、回線交換回線、パケット交換回線、ATM 回線、衛星通信回線、光ファイバー通信網等を利用したバックアップ回線の確保（図 1）。

削除: 、フレームリレー回線

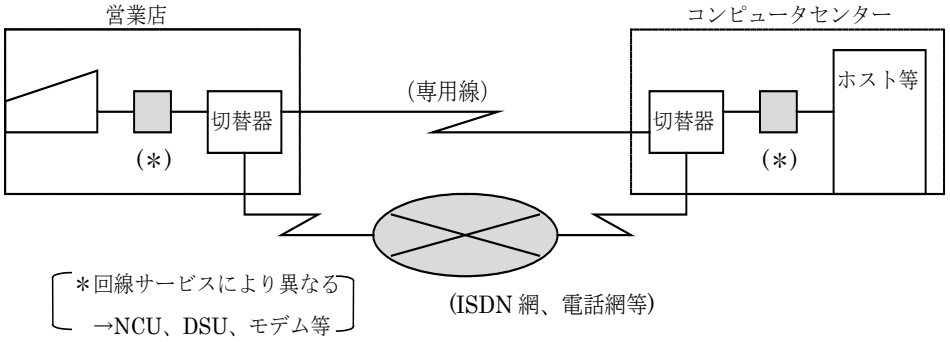


図 1　バックアップ回線の例

(2) 回線の別ルート化

回線ルートに障害が発生した場合に、全回線が同時に使用できなくなる事態を防ぐため、複数の回線により別々に接続し、並行して危険分散を図るための方法である。

単一の通信事業者を利用し、中継局を分ける（物理的に別ルートにする）方法と、複数の通信事業者を利用する方法がある（図 2、図 3）。

① 単一の通信事業者の利用

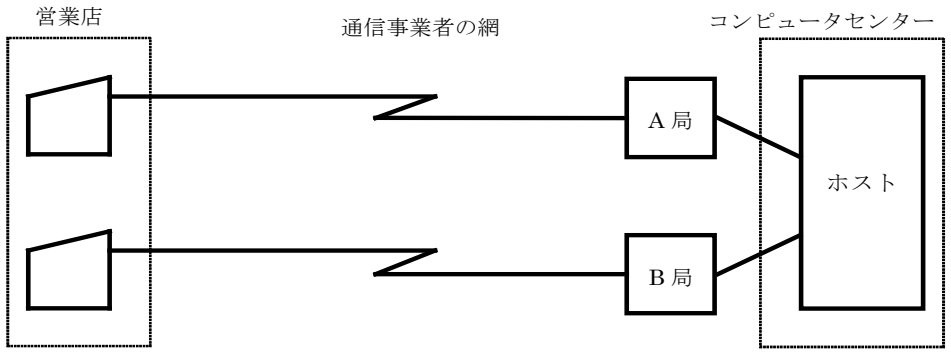


図 2　単一の通信事業者の利用例

② 複数の通信事業者の利用

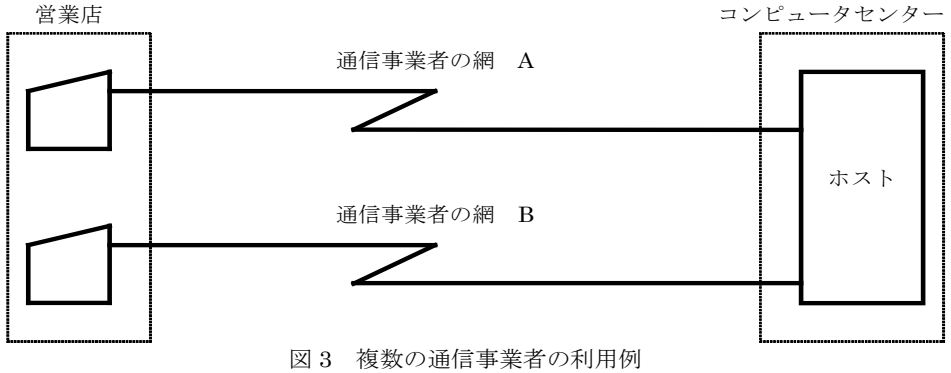


図 3　複数の通信事業者の利用例

(3) データ伝送経路の構成と留意点

代表的なデータ伝送経路の構成には、スター型構成（コンピュータセンター等の主要拠点と営業店等の拠点を 1 対 1 で接続する構成）や、ツリー型構成（コンピュータセンター等の主要拠点より事務センターや基幹営業店等の中継結節点を経由し、複数の営業店等の拠点を接続する構成）等がある。構成によって、障害時の影響範囲、通信量及びコスト等について留意する必要があり、選択にあたっては、各種構成の特徴を踏まえ、業務への影響等を勘案することが必要である（図 4、図 5）。

① スター型の構成

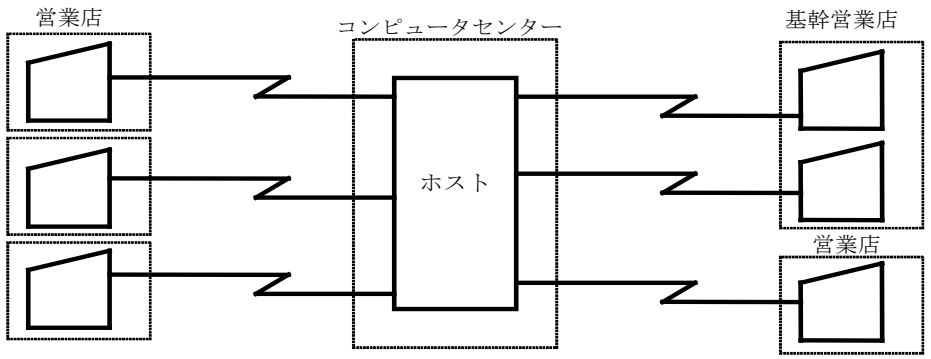


図 4　スター型の構成の例

② ツリー型の構成

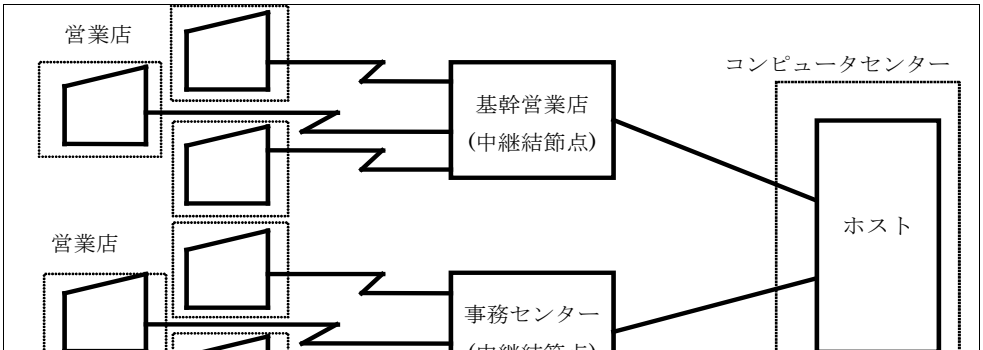


図 5　ツリー型の構成の例

3. 構内回線について

(1) コンピュータセンターにおける留意点

コンピュータセンターにおいては､回線関連設備から重要な各機器までの配線は二重化することが望ましい。特に、建物外の回線を二重化した場合、コンピュータセンター内において、MDF から通信制御装置等の重要な各機器までの配線を二重化することが望ましい。

(2) 構内 LAN の予備

構内 LAN についても、重要性に応じて予備を持つことが望ましい。予備の例として、以下のようなものがある（図 6）。

① 基幹 LAN の多重化（図 6）

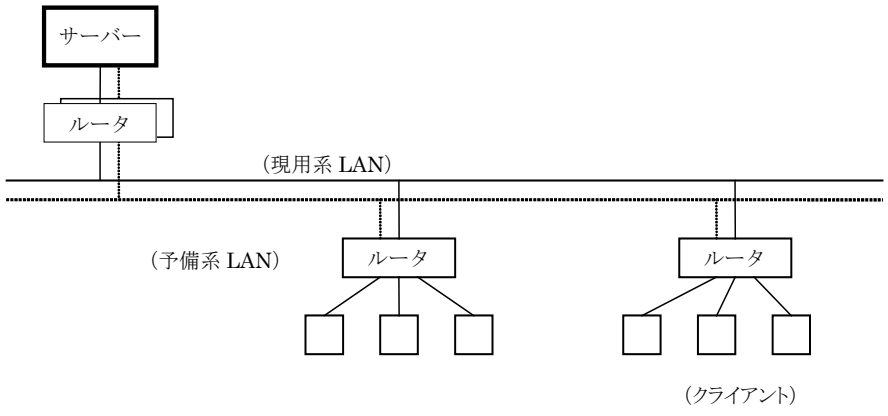


図 6　LAN の多重化の例

4. 【技 2】3. を参照。

ハードウェアの信頼性向上対策
ハードウェアの予備

適　用　区　分				
共	セ	本	提	ダ
	◎	◎		

実97	端末系装置の予備を設けること。

削除: 技　6

端末系装置の障害時の迅速な対応のため、端末系装置は予備または代替機能を設けること。

1. 端末制御装置（TC 等）、端末装置、クライアント機の予備または代替機能の持ち方として、以下のような方法がある。
   (1) 規模などにより、地域ごと、主要営業店ごと、またはコンピュータセンターに予備を保有する。
   (2) 複数台設置することにより、予備と同様の効果を持たせる。
   (3) 端末制御装置に障害が発生したときに、配下の端末を他店等の端末制御装置に接続して使用する。
   （制御装置内にローカルファイルを有する場合、このファイルの障害に対する復旧対策及び予備の保有について考慮する必要がある。）
   (4) ベンダーとの保守契約により代替機の提供を受ける。
   (5) 端末装置の障害の場合、異なる種類の端末装置や他の業務で使用している端末装置で代替する。
   ・CD・ATM、イメージ OCR 等の専用端末装置の障害時に汎用端末装置で代替する。
   ・汎用端末装置の障害時に渉外端末装置で部分的な代替を行う。
   ・業務系端末装置と情報系端末装置で相互に部分的な代替を行う。
   (6) 他店またはコンピュータセンター等の端末で代行入出力する機能を設けておく。

2. 【技 2】3. を参照。

12 ソフトウェアの信頼性向上対策

削除: Ⅰ．システム信頼性向上対策

削除: （Ⅱ）

システムの信頼性向上を図るうえで、ソフトウェアの信頼性向上対策を講ずることが重要である。技術的には、ソフトウェアの信頼性を向上するための技法やツールが数多く提唱されているが、利用に際しては開発の各工程でどのような技法やツールを使用するか、あるいはその使用目的を明確にするなどの計画立案が重要である。さらに、開発作業の標準化または作業の自動化を図るなど、ソフトウェアの信頼性を向上させるための対策を講ずることが重要である。

また、パッケージ等の利用にあたっては、既存システムとの整合性、親和性に留意する必要がある。本部・営業店等におけるユーザー部門による開発においても、システム部門の手法を参考にするなど、信頼性を確保するための留意が必要である。

ソフトウェアの信頼性向上対策
開発時の品質向上対策

適　用　区　分				
共	セ	本	提	ダ
◎				

実 98	必要となるセキュリティ機能を取り込むこと。

削除: 技　8

セキュリティ対策を確実に実施するため、システム計画段階において必要となるセキュリティ機能が取り込まれていることを明確にすること。

1.　開発するシステムが具備すべきセキュリティ機能、およびそれらを実現するために必要となる技術については、システム計画段階から考慮することが必要である。

2.　セキュリティ対策は、全体のシステム開発計画と整合性が取られ、処理する業務やデータの重要性およびリスクに応じて決定されることが必要である。

（参考）OECD 理事会勧告のセキュリティガイドライン（1992 年）における
情報システムセキュリティの目的

「情報システムセキュリティの目的は、情報システムに依存するものの利益を可用性（Availability）、機密性（Confidentiality）、完全性（Integrity）の欠如に起因する危害から保護することである」

・可用性（Availability）　……ハードウェア、ソフトウェア、情報をいつでも利用できるように保持すること
・機密性（Confidentiality）　…アクセスを許されていない者からハードウェア、ソフトウェア、情報を守ること
・完全性（Integrity）……改ざん等されないようにハードウェア、ソフトウェア、情報を完全な形態で保持すること

ソフトウェアの信頼性向上対策
開発時の品質向上対策

適　用　区　分				
共	セ	本	提	ダ
◎				

実 99	設計段階でのソフトウェアの品質を確保すること。

削除: 技　9

設計段階でのソフトウェアの信頼性向上のため、開発の前提となる要件を明確にするとともに、信頼度設計の考慮や設計作業の標準化等を行い、ソフトウェアの品質を確保すること。

1.　ソフトウェアの品質を確保するためには、まず設計段階から品質を高めることが重要である。そのために考慮すべき点として、以下のものがある。

(1) セキュリティ機能の組込み

セキュリティに関する品質を確保するためには､設計段階において必要なセキュリティ機能を組み込むことがポイントであり、以下の点に留意すること。

・セキュリティポリシーに基づいて、会社（もしくは組織）として必要な機能を組み込む。

・ユーザー要件としてのセキュリティ機能を組み込む。

(2) 品質向上のための設計技法やツールの活用

設計技法やツールは技術の進歩にあわせて常に新しいものが提案されており、それらの検討とあわせて、組織体制の整備、標準化の推進、教育の実施等を行うことが必要である。

2.　品質確保のための具体的事例として、以下のようなものがある。

(1) システム開発の前提となる要件の明確化

① セキュリティ要件の明確化

セキュリティ要件の明確化については、以下の点に留意すること。

・セキュリティポリシーを満足すること。

・ユーザー要件としてのセキュリティ機能を満足すること。

・システムの開発においては、既に開発・導入済のシステムについて発見されたセキュリティ上の弱点を解決すること。また、開発時点で広く知られているセキュリティ上の弱点を解決すること。【技 10】

・監査証跡（処理内容の履歴を跡付けできるジャーナル等の記録）の作成機能の要件を明確化すること。

② ユーザー要件の明確化

開発対象システムのユーザー要件となるものに入出力要件、主要機能要件（業務処理内容）、ハードウェア要件等がある。これらのユーザー要件について漏れのないようにするため、要件定義書やシステム設計書のユーザーインタフェース仕様等についてユーザー側責任者の承認を得る手続きを明確にし、遵守すること。

（ユーザー側の責任者は、そのシステムの利用に関して責任を負う人であり、部門の長や

プロジェクトリーダー等を指す。）

③　開発目標の設定

ユーザー要件に基づく安全性の確保及びソフトウェアの品質確保に関して、次のような目標を設定するものである。

・信頼性、機能、性能、操作性、拡張性、保守性等

(2) 設計作業の標準化

設計作業の標準化の対象として、以下のようなものがある。

①　設計工程

設計の各工程ごとに行うべき作業、内容、範囲等。

②　ドキュメント

設計内容を記述するドキュメントの内容、作成手順等。

③　レビュー

レビューの手順、実施基準等。

(3) 信頼度設計の考慮

エラーを少なくするための努力をする一方で､エラー発生時のことを考慮して設計しておくことも重要であり、以下のような例がある。

①　エラー局所化ルーチンの設計

ソフトウェアにエラーが発生しても、その影響が広がらないように影響範囲を局所化する。

②　異常ケースの洗出しと対処策の設計（回避または代行）

異常ケースの洗出しを行い、その対処策を体系的に行う。

(4) レビューの実施

レビューとは、システムの完成度を高めるために、開発の各フェーズごとに検討会を開き設計書の検証を他人の目で行うことである。また、レビューを実施する際には、テストのしやすさ、読みやすさ、保守容易性等さまざまな観点から検証することも必要である。

（参考 1）

システムの信頼性を高め、開発の効率化を推進する例として、以下のものがある。

1. ソフトウェア開発形態、ソフトウェア開発手法

(1) ソフトウェア開発形態

① ウォーターフォールモデル

ソフトウェアのライフサイクルをいくつかのフェーズ（要求分析フェーズ、設計フェーズ等）に分け、各々のフェーズを滝とみなして、全体を上流から下流に至る滝の連なりと見なして開発していく形態。

② スパイラルモデル

目的とするソフトウェアを開発する前に、その一部を試作の形態で早期に動作させて評価し、その結果を本番ソフトウェアの開発にフィードバックする、プロトタイプ開発→評価→フィードバックという流れをステップごとに繰り返して開発を進めていく形態。

(2) ソフトウェア開発手法

① プロセス中心設計

プロセスを中心にとらえ、データをそれに付随するものとする考え方に基づく設計法。

② データ中心設計

データを中心にとらえ、プロセスをそれに付随するものとする考え方に基づく設計法。

③ オブジェクト指向設計

プロセスとデータを一体化して独立したオブジェクトとしてとらえ（一体化することをカプセル化という）、オブジェクト間のインタフェースはメッセージ送受信のみで行う手法。

2. CASE（Computer Aided Software Engineering）ツールを利用したソフトウェア設計作業の効率化

(1) 設計情報の統合管理

データ項目の属性（長さ、タイプ等）、内容等を一元管理するための辞書及びツール等を利用し設計情報を統合管理する。

(2) 仕様記述言語の利用による後工程への活用

コンピュータ処理が可能なように作られた、仕様を記述する言語を利用して、後工程の作業へ活用する。

(3) 設計情報を再利用するための機能辞書システム

よく使う機能をパターン化し辞書に登録しておいて、それを再利用する。

3. 「共通フレーム 2007（SLCP-JCF）経営者、業務部門が参画するシステム開発及び取引のために」等を参照し、開発要員の間で作業内容を共有することがソフトウェアの開発の効率化に有効である。

4.　発注者視点での設計書等ドキュメントの記述やレビューに関する考慮点については、独立行政法人情報処理推進機構（IPA）ソフトウェア・エンジニアリング・センターに詳しい情報があるので参照されたい。

・独立行政法人情報処理推進機構（IPA）ソフトウェア・エンジニアリング・センター
http://sec.ipa.go.jp/reports/20080710.html

（参考 2）

スマートデバイスのアプリケーション設計に関する留意点

利用者情報の取扱いにおいては、総務省より公開されている「スマートフォン プライバシー イニシアティブ」の「第５章　スマートフォンにおける利用者情報の取扱いの在り方　１ スマートフォン利用者情報取扱指針」に参考となる情報が記載されているので参照されたい。

・「スマートフォン　プライバシー　イニシアティブ
－利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－」の公表
（平成 24 年８月）
http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html
総務省 利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会

ソフトウェアの信頼性向上対策
開発時の品質向上対策

適　用　区　分				
共	セ	本	提	ダ
◎				

実100	プログラム作成段階での品質を確保すること。

削除: 技　10

プログラム作成段階での、ソフトウェアの信頼性向上のため、プログラム仕様書に基づいたプログラミングを行うとともにプログラム作成作業の標準化・自動化等を行い、ソフトウェアの品質を確保すること。

1. プログラムの作成段階において、ソフトウェアの品質を確保するための方法として、以下のような標準化・自動化の例がある。

(1) 標準化

① 適切な言語の選択

全体的な効率性を考慮し、目的にあった言語を選択することが必要である。

② プログラム検証のルール化（インスペクション）

作成されたプログラムがプログラム仕様書に基づいたものであるかを、他人が検証するものである。中核的なプログラムや、新人等の技術及び標準化について経験の浅いプログラマーが作成したプログラムを対象に検証をルール化することはエラーの早期発見に有効である。

また、検証結果に基づくフォローアップを実施することも、その後のエラー削減に有効である。

③ 部品化、パターン化の有効活用

よく使う典型的なプログラムをパターンプログラムとして登録したり、使用頻度の高いコーディング部分を部品プログラムとして登録しておき、それを活用する方法である。

④ その他

a. コーディング規約の作成

プログラマー間の個人差を解消し、他人に見やすくするようにするとともに、プログラムの誤りを少なくするために行うものである。

b. 構造化プログラミングの利用

3つの基本制御構造（命令を連続して実行する単純構造、命令のいずれかを実行する分岐構造、命令を繰り返し実行するループ構造）及びその組合せを使用してプログラムを作成する方法で、プログラムの誤りを発生しにくくするものである。

(2) プログラム作成の自動化

① プログラム自動作成ツールの活用

以下のようなプログラム自動作成ツール等の活用も有効である。

a. 仕様記述言語の利用による半完成プログラムの作成ツール

b. 会話形式による画面定義作成ツール

c. 設計仕様とコーディングの整合性をチェックするツール

② ドキュメント作成ツールの活用

以下のようなドキュメント作成ツール等の活用も有効である。

a. プログラム詳細処理説明書（フローチャート等）の作成ツール

b. 日本語仕様書作成ツール

2. プログラム作成段階においてもコンピュータウイルス等の不正プログラムの侵入を防ぐことが必要である。特に、ネットワーク環境での開発において開発者同士がファイルを共有するケースや、市販パッケージソフトを使用する場合等は、コンピュータウイルスの侵入機会が多いと考えられるため、抗ウイルスソフトによる監視が必要である。【技 49、技 50】

3. Web システムについては、Web アプリケーションの脆弱性対策を考慮してシステムを構築することが望ましい。

(1) 脆弱性の例

現在知られている Web アプリケーションで考慮すべき脆弱性として、以下のようなものがある。

① SQL インジェクションの脆弱性
② OS コマンド・インジェクションの脆弱性
③ ディレクトリ・トラバーサルの脆弱性
④ セッション管理機構の脆弱性
⑤ クロスサイト・スクリプティングの脆弱性
⑥ CSRF（クロスサイト・リクエスト・フォージェリ）の脆弱性
⑦ HTTP ヘッダ・インジェクションの脆弱性
⑧ アクセス制御と認可制御の脆弱性

(2) 脆弱性対策の例

実装上の対策として、以下のようなものがある。

① 入力データを元に処理（SQL、スクリプト、シェル等）をアプリケーションで生成し実行する場合は、意図しない処理が実行されないような、各脆弱性に対応した適切な実装を行う。追加的対策として、入力項目及び入力パラメータについて、値の属性やデータ長、制御文字の有無等の確認を行い不正なデータを排除することも望ましい。

② ユーザーを特定する情報は推測困難なものとし、暗号化を施して送受信するなど漏洩しない方法で受け渡しする。また、なりすましの予防としてユーザーを特定する情報の発行をログイン成功後にするなどの実装を行う。

③ データベースやシステムファイル等の重要な資源に対し、適切なユーザー認証機能や認可制御を設けて必要最小限の権限・アクセスのみを許可するような実装を行う。

（参考 1）

Web システムの脆弱性対策の参考文献として、以下のものがある。

(1)「安全なウェブサイトの作り方 改訂第５版」

独立行政法人情報処理推進機構（IPA）セキュリティセンター

(2)「安全な Web サイト利用の鉄則」

独立行政法人産業技術総合研究所情報セキュリティ研究センター

(3)「フィッシング対策ガイドライン」

フィッシング対策協議会

（参考 2）

スマートデバイスのアプリケーション開発に関する留意点

スマートデバイスのアプリケーション開発においては、セキュリティを確保するコーディングのガイドとして、日本スマートフォンセキュリティ協会（JSSEC）より「Android アプリのセキュア設計・セキュアコーディングガイド」が公開されている。このガイドには Android に依存しない一般的な基礎知識の情報も記載されているので参照されたい。

・「Android アプリのセキュア設計・セキュアコーディングガイド」

http://www.jssec.org/activities/index.html

一般社団法人 日本スマートフォンセキュリティ協会

ソフトウェアの信頼性向上対策
開発時の品質向上対策

適　用　区　分				
共	セ	本	提	ダ
◎				

実101	テスト段階でのソフトウェアの品質を確保すること。

削除: 技　11

テスト段階でのソフトウェアの信頼性向上のために、テスト計画の策定、テスト環境・体制の整備、テストサポート機能の活用、テスト実施段階での各種管理等を行い、ソフトウェアの品質を確保すること。

1.　ソフトウェアに内在する欠陥を事前に発見・除去するとともに、ソフトウェアの正確性を十分に検証することが必要である。

2.　ソフトウェアの品質を確保するために、以下のような事項に留意することが必要である。

(1) テスト計画書の作成

システムに求められる要件が多様化するにつれ、開発すべきシステム自体が複雑になり、信頼性の評価などソフトウェアの品質を検証するためのテストも複雑になってきている。こうした状況において重要となるのは、テスト段階を円滑に行うための計画書である。

テスト計画書で明確にしておかなければならない主要項目は以下のとおりである。

①　実施方針
　テストの分類と目的、完了基準、テスト・スケジュール等

②　実施体制
　実施体制と役割分担、要員選出等（詳細下記）

③　実施方法
　テストツール及びその使用方法、検証方法、作業の依頼方法等

④　実施資源
　テスト環境、リソース見積等

⑤　実施管理
　プログラム管理（ライブラリ管理、資源管理等）、トラブル管理、ドキュメント管理、進捗管理、品質管理、外部委託管理等

(2) テスト体制の整備

テスト項目の量が膨大なシステムの場合には、テストの効率性、ソフトウェアの品質確保等を鑑み、テスト実施の専任体制を敷き、分業化を図ることも必要である。

テスト結果の検収は、内容を十分理解できる要員によって実施される必要がある。

また、要員の選出にあたっては、利用部門、運用部門などの参画も有効な場合が考えられる。

(3) テスト工程の分類

テスト工程の分類には、さまざまな考え方があるが、例として以下に挙げるものがある。

①　単体テスト

モジュール単位等のある特定のプログラム範囲の機能を検証するテスト

② 結合テスト（統合テスト）

モジュールを結合した（プログラム単位、サブシステム単位など）機能を検証するテスト

③ システムテスト（総合テスト、総合運転テスト）

設計段階で計画したシステムの要件が計画のとおり機能することをシステム全体で検証するテスト

なお、ソフトウェアの品質を検証するため、システムテスト用ツール、過負荷テスト用ツール、異常テスト用ツール等によるシステムテストに加えて、本番に近い状態でのシステムテストを行うことも有効である。

a. 性能テスト（ピーク処理時の性能評価を含む）
b. 例外処理テスト
c. リカバリ・テスト
d. システムの利用者も参加したリハーサル
e. 限界値テスト（許容最大件数を考慮した評価を含む）
f. 連続運転テスト（閏日等の実際の日付構成や連続運用に即したテストを含む）
g. 接続テスト（全銀システム、統合 ATM システム、共同 CMS 等の他システムとの回線接続、記録媒体授受を含む）
h. 機密保護等のセキュリティ機能テスト
i. 脆弱性テスト（Web アプリケーション、外部ネットワークとの接続部分の機器等）

(4) 各種テストツールの活用

テストを効率的に行うためのテストツールにはさまざまなものが考えられるが、具体的事例として、以下のようなものがある。

① 単体テスト、結合テスト（統合テスト）工程でのテストツール事例

a. ドライバー等（下位モジュールテスト実行ツール）
コンパイルの最小単位を実行するためのテスト用ツール

b. スタブ・シミュレーター等（未完成モジュール代理実行ツール）
プログラムをテスト実行するときに、未完成下位モジュールをシミュレートするテストツール

c. デバッガー
プログラム等のテスト実行において、デバッグを支援するテストツール

d. カバレージ等（テスト範囲管理ツール）
プログラムの全ルートのうち、どの程度のルートをテストしたか、その割合を測定するためのツールであり、テストの十分性評価の指標を与えるのに有効であるとともに、テストの進捗管理にも使えるツール

e. テストデータ・ジェネレータ
豊富なテストデータを作成するために、ひな型テストケースを基に詳細なケースに分かれたテストデータを自動的に作り出すツール

② システムテスト（総合テスト、総合運転テスト）工程でのテストツールの事例

a. システムテスト用ツール
システムを総合的に動作させてテストするためのテスト環境、テストデータの発生機

能、テスト結果のロギング機能等を備えたツール

b. 過負荷テスト用ツール

過負荷状態を作り出す機能等を備えたツール

c. 異常テスト用ツール

異常状態を作り出す機能等を備えたツール

d. 脆弱性テスト用ツール

アプリケーションの脆弱性やネットワークの設定不備等のシステムの潜在的なセキュリティホールを発見するために、擬似攻撃（不正リクエストや不正パケットを送信して実際の攻撃手法のシミュレートを行う）の機能等を備えたツール

(5) テスト実施段階での各種管理の例

テスト実施段階での各種管理の例として、以下のものがある。また、テスト終了後は、テスト結果報告書を作成し、開発責任者へ報告することが必要である。

① プログラム管理

プログラム等の作成、変更、削除が容易に行えるように、プログラムを管理するためのものである。このなかには、次の管理も含む。

a. ライブラリ管理

テスト段階では、テスト、バグ（欠陥）発見、プログラム修正（欠陥除去）という作業を繰り返し行うが、それらの作業を効率的に行うため、単体テスト、結合テスト（統合テスト）、システムテスト（総合テスト、総合運転テスト）等の工程ごと、または業務ごとにライブラリを分ける等の保有手段を提供し、その管理を行うものである。

b. データ・ディクショナリー管理

プログラム等で参照するデータ及びプログラムの相互関係等を一元的に管理することにより、テスト段階の変更を漏れなく行うためのものである。

c. 変更管理

新規要件の追加、要件の変更等に対し、ドキュメント、プログラム等の変更管理を明確にするとともにそれを管理し、関係者に周知されるようにするためのものである。

② トラブル管理

トラブルの原因を解明し、そのトラブルの迅速かつ確実な解決を行うとともに、トラブルの発生状況及び発生傾向を把握・管理し、同一・類似トラブルの再発を未然に防ぐためのものである。　【運 64】

③ ドキュメント管理

テスト仕様書（テストケース一覧表、テスト項目等）、テストデータ、テスト結果報告書、カバレージ報告書等のテストドキュメントを各テスト工程ごとに整備し、その管理を行うものである。

④ 進捗管理

テストで発生する問題の早期発見と対策の早期実現を図り、テスト計画に基づき遅滞なくテストが実施されていることを管理するものである。

⑤ 品質管理

テストで得られた結果が、品質管理基準値を満たしているかを検証、管理するものである。なお、テスト環境（テストツールやテスト用媒体）からのコンピュータウイルス等の不正プログラムの侵入を防止することもテスト段階における品質管理である。

ソフトウェアの信頼性向上対策
開発時の品質向上対策

適　用　区　分				
共	セ	本	提	ダ
◎				

実102	プログラムの配布を考慮したソフトウェアの信頼性を確保すること。

削除: 技　12

配布時のソフトウェアの信頼性を確保するため、配布先の稼働環境との整合性確認やウイルスチェックを行うこと。

1.　業務用アプリケーション等のプログラムを配布する際は、プログラムを開発し検証した環境と、稼働する機器の環境の違いを考慮し、整合性を確認することが必要である。

考慮すべき例として、以下のものがある。

・ハードウェア環境（マイクロプロセッサ、メモリ容量等）の相違

・OS、ミドルソフト等の相違、それらのバージョンの相違

また、これらの原因により正常に稼働しないケースを想定し、リカバリ手順を含めた更新手順を取り決めておくことが望ましい。

2.　ウイルスチェック等による安全性の確保

プログラム開発時やテスト時にコンピュータウイルス等の不正プログラムが混入するケースを想定し、プログラムの配布前にチェックを行うこと。

コンピュータウイルス等の不正プログラムの防止については【技 49、技 50】を参照すること。

ソフトウェアの信頼性向上対策
開発時の品質向上対策

適　用　区　分				
共	セ	本	提	ダ
◎				

実103	パッケージ導入にあたり、ソフトウェアの品質を確保すること。

削除: 技　13

パッケージソフトウェアの品質を確保するために、機能および自社システムとの整合性を十分確認すること。

1.　業務システムパッケージ導入時の品質確保の具体的事例として、以下のようなものがある。

(1) パッケージ導入の前提となる要件の明確化

①　ユーザー要件の明確化

購入するパッケージのユーザー（利用者）の要件となるものに入出力要件、主要機能要件（業務処理内容）、ハードウェア要件などがある。

②　目標の設定

ユーザー要件に基づいて、安全性確保やソフトウェアの品質確保に関して、次のような目標を設定するものである。

・信頼性、機能、性能、操作性、拡張性、保守性等

(2) 機能について記載された仕様書、設計書、テスト確認書等のドキュメントの確保

安全性確保やソフトウェアの品質確保およびメンテナンスのため必要となるものである。

(3) 自社によるテスト

機能、性能、操作性等を確認するためのテストについては【技 11】に準じて行うこと。

（参考 1）

契約により、販売者と購入者の責任を明確にすべき例として、以下のようなものがある。

・パッケージのソフトウェアを使用する装置等の使用条件
・ソフトウェアについてのバグ（欠陥）その他の瑕疵を発見した場合の責任所在
・障害発生時の支援体制
・メンテナンスの範囲、期限等（脆弱性の修正パッチの提供を含む）

（参考 2）

パッケージ購入にあたり、留意すべき事項として、以下のようなものがある。

特にクライアントサーバー・システムの場合、インストールする機器ごとに OS のバージョンやハード要件等の環境が相違することもあるため十分に留意すること。

1. オペレーティングシステムのバージョンレベルの確認
   パッケージのソフトウェアが動作可能なオペレーティングシステムであることを確認するものである。
2. アプリケーションパッケージ間の連係時のバージョンレベルの確認
   すでに導入しているアプリケーションパッケージとの連係や、同時に購入する複数のパッケージ間の連係について、バージョンレベルの確認を行うものである。
3. 最大利用記憶容量等の必要資源の確認
   自社システムの記憶容量等がパッケージのソフトウェアを稼働させるのに十分であることを確認するものである。
4. コード体系の確認
   自社システムとパッケージのソフトウェアにおけるコード体系の整合性を確認するものである。
5. 機密保護への対応
   機密保護等のセキュリティ機能がパッケージに組み込まれていること。また、必要に応じてカスタマイズが可能であること。
6. コンピュータウイルスのチェック
   購入パッケージそのものにコンピュータウイルスが潜むケースもあるため、導入時のウイルスチェックが必要である。

ソフトウェアの信頼性向上対策
メンテナンス時の品質向上対策

適　用　区　分				
共	セ	本	提	ダ
◎				

実104	定型的変更作業時の正確性を確保すること。

削除: 技　14

営業店新設、機器増設等の定型的変更作業時における正確性を確保するため、変更作業の合理化等の必要な対策を講ずること。

1.　定型的変更作業の例として、営業店新設、機器の増設等があるが、それらの変更作業時における正確性を確保するための対策として、以下のような例がある。

(1) 変更作業の合理化

①　定義の一元化

テーブル化またはデータベース化することなどにより、営業店、機器等の定義を一元化し、1項目の変更のための修正が複数箇所とならないようにするものである。

②　変更手順の簡略化

変更作業の信頼性向上のため、各種テーブルまたはデータベースに関する変更、追加、削除の手順の簡略化を進めるものである。

(2) 変更内容と作業手順のドキュメント化

定型的変更に伴い変更やテストを要するプログラム等のすべてが、最新の状態で把握でき、かつ変更箇所や変更方法が記述してあるドキュメントが必要である。

これを使用して変更作業に抜け落ちがないかを確認し、正確性の確保を図るものである。

(3) テストおよび検証手順の確立

変更結果の整合性および妥当性をチェックするためのツールを作成（変更部分のテスト、副作用テスト、チェックリスト等）したり、手順のマニュアル化を図り、変更作業の正確性を確保するものである。

ソフトウェアの信頼性向上対策
メンテナンス時の品質向上対策

適　用　区　分				
共	セ	本	提	ダ
◎				

実105	機能の変更、追加作業時の品質を確保すること。

削除: 技　15

機能の変更、追加作業時におけるソフトウェアの品質を確保するため、開発時の品質向上対策を準用すること。

1.　機能の変更、追加作業時においては、変更、追加に伴うほかへの影響をチェックし、極小化することが重要であり、以下のような例がある。

(1) 変更、追加箇所の確認

①　ドキュメント生成支援ツールの活用

プログラムのドキュメント生成支援ツールを有効活用し、変更箇所をドキュメントで検証・確認するものである。

②　プログラムの新旧比較ツールの活用

変更、追加作業前後のプログラムを比較し、目的のとおりに作業されていること、および不要な箇所が変更されていないことを確認し、新たなバグの発生、不正ロジックの組込みを防止するものである。

(2) 影響度の検証

①　テスト環境、テストデータ等の整備

変更前のテストデータを用い、変更箇所以外の部分について、テスト結果が変更前と一致することを確認するため、テスト環境、テストデータ等を整備して活用する方法である。

②　影響度確認支援ツールの活用

プログラムとプログラム、プログラムとファイル、プログラムとデータ等、それぞれの間のクロスリファレンスを作成しておき、機能の変更、追加がどのプログラムやファイル等に影響を与えるか確認するものである。

(3) 機能の変更、追加作業時の障害対策

①　バックアップ

機能の変更、追加時の品質確保に努める一方で、機能の変更、追加による障害対策として、変更前のシステムをバックアップとして準備しておくことである。

②　障害時回復手順の作成

障害発生に備えて、その回復のための手順の確立、テスト、訓練等をしておくものである。

13 運用時の信頼性向上対策

削除: Ⅰ．システム信頼性向上対策

削除: （Ⅲ）

コンピュータシステムの信頼性向上を図るうえで、ハードウェア・ソフトウェアの信頼性向上とともに、人が行う操作または作業の信頼性向上も重要な要素である。

運用時の信頼性を向上させるため、オペレーションの自動化、簡略化等の対策を講ずるとともに、妥当性、正当性のチェック機能を充実することが重要である。

運用時の信頼性向上対策
運用時の信頼性向上対策

適　用　区　分				
共	セ	本	提	ダ
○				

実106	オペレーションの自動化、簡略化を図ること。

削除: 技　16

オペレーションの信頼性を向上させるため、オペレーションの自動化、簡略化を図ることが望ましい。

1.　汎用機、サーバーのオペレーション

コンピュータセンターおよび本部・営業店等におけるオペレーションの信頼性を向上させるため、ハードウェアやソフトウェアを利用してオペレーションの自動化、簡略化を図ることが重要であり、以下のような例がある。

(1) コンピュータセンターでのオペレーション

①　自動化

システムの起動や業務の開始を自動的に行う機能、ジョブの起動やジョブと記憶装置の対応を自動化する機能等、各種自動運転機能を活用する、またはそれぞれの実情に応じた機能を開発することなどによりセンターオペレーションの自動化を図るものである。

削除: が整備されてきており、これら

また、運用スケジュールの規模に応じてシステムの電源投入を自動的に行う機器、テープハンドリングを自動的に行う機器を活用することもオペレーションの信頼性、安全性、情報の機密保護を向上させるうえで有効である。

削除: も開発されており、これら

スケジュール化されたジョブグループのジョブシーケンスに従ったジョブの自動起動やタイマーによるジョブの時間起動のほかに以下のような自動化の例がある。

a.　電源投入からシステムの立上げ、オンラインジョブの起動、端末の開局等、業務が開始できるまでの一連処理の自動化

b.　平常日、繁忙日、月末日、土曜日等パターンごとにスケジュール化された一斉同報通知の送出や端末モード変更の自動化

c.　取引ジャーナル等のファイルのバッチジョブへの引継ぎの自動化

d.　取引ジャーナル等のファイルの他システム（系）への引継ぎの自動化

e.　端末の閉局からオンラインジョブの停止までの一連の処理の自動化

f.　システム停止の自動化

g.　テープハンドリングの自動化

なお、自動運用の注意事項として処理の順序や運転状況、条件の変更が生じた際にも、システム全体の運用に支障を来さぬよう、自動化を変更できる機能を充実しておくことが重要であり、変更内容として、以下のようなものがある。

・一斉同報通知や端末モード変更を行う時刻の変更
・システム（系）の変更（現用系から待機系への変更、またはその逆）
・自動運用からマニュアル運用への変更
・ジョブネットワークへのジョブの追加、変更

・ボリュームの追加、変更
・実行 JCL（ジョブ制御言語）の変更

② 簡略化

コマンド体系の一元化を図ったり出力メッセージの日本語化を図るなどして、オペレータインタフェースを平易化すること。さらに、運用をケースによりパターン化し、一連のコマンド列を一括実行できるように準備しておくことなどにより、オペレーションを単純化、簡略化するものであり、以下のような例がある。

a. コマンド入力の極少化
b. テープハンドリングの極少化
c. 異常終了後再開オペレーションのパターン化

③ 自動化、簡略化の留意点

センターオペレーションの自動化の推進は、オペレーションの信頼性向上のために有効であるが、過度の自動化は、機械運行の安全性を阻害する可能性もある。そのような場合には、単にオペレータへの通報にとどめる等、オペレータによる判断の余地を残しておくことも必要である。

オペレータの応答を必要とするメッセージやオペレータに注意を喚起する必要があるメッセージ等は、高輝度出力、赤字出力やブザーを鳴らす（オペレータの応答で解除）方法等で重要メッセージの見落としを防ぐ工夫も必要である。さらに、大量メッセージによるシステム停止等を防ぐため、冗長なメッセージを抑止する等の仕組みを合わせて構築することも必要である。

(2) 本部・営業店等におけるオペレーション

本部・営業店等における重要なサーバーのオペレーションは、コンピュータセンターでのオペレーションに倣って自動化、簡略化を図ることが望ましい。さらに、本部・営業店等でコンピュータ運用に必要な知識や技能を持つ専門のオペレータを配置することが困難な場合には、自動化等の運用をリモート操作で行う機能を持つことが望ましい。

① 自動化

本部・営業店等のサーバーオペレーションの自動化として、以下のような例がある。

a. 電源の投入やシステムの立上げ、業務アプリケーションの起動
b. バックアップの取得やデータベース更新手順
c. 障害発生時の縮退運転の手順やシャットダウン手順

② 簡略化

簡略化の例として、以下のものがある。

a. オペレーション用のインタフェースを平易化（ユーザーフレンドリなインタフェースの採用）
b. 一連のコマンドを一括実行しコマンド入力を極少化
c. 異常終了時の再開オペレーションの単純化

2. データ入力作業（端末オペレーション）

(1) 自動化

磁気ストライプ読取装置、現金処理機、OCR 等の活用により、手入力操作を減少させたり、無くしたりするものである。

(2) 簡略化

オペレーションガイダンス機能の活用等により、入力判断の平易化やコード入力による簡略化を行うものである。

運用時の信頼性向上対策
運用時の信頼性向上対策

適　用　区　分				
共	セ	本	提	ダ
◎				

実107	オペレーションのチェック機能を充実すること。

削除: 技　17

オペレーションミスを防止するため、チェック機能を充実すること。

1.　汎用機、サーバーのオペレーション

オペレーションミスの防止、早期発見のために、チェック機能を充実することが必要である。

(1) コンピュータセンターでのオペレーション

コンピュータセンターにおいてオペレータの作業をチェックする機能として、以下の例がある。

①　コマンド入力の再確認機能

センターオペレーションについて、誤操作により重大なシステム障害を起こす可能性のあるコマンドの再確認機能を設ける方法である。

②　妥当性チェック機能

処理の順序性や運転状況、条件（時間帯、曜日等）により、入力されたコマンドが妥当なものであるかどうかをチェックする機能を組み込んでおく方法である。

③　テープ使用時のラベルチェック機能

使用する磁気テープの妥当性をチェックするため、ジョブとボリュームラベルの対応チェック機能を有効活用するものである。

(2) 本部・営業店等におけるオペレーション

本部・営業店等で重要なサーバーのオペレーションを行う場合には、コンピュータセンターに準ずるチェック機能を備えることが必要である。

2.　データ入力作業（端末オペレーション）

コンピュータシステムの端末操作者が入力したデータについてチェックする機能として、以下の例がある。

(1) 入力のチェック機能

入力するデータ項目ごとのチェック（桁数オーバーの検出、省略不可の検出等）や項目間の関連性チェック、または口座番号などのチェックディジットの検出等により、チェック機能を充実するものである。

(2) 各種合計突合機能

個々の入力データのチェックだけでなく、端末の取り扱った件数・金額等の合計を突合する機能（精査カウンター等）を設けておくものである。【技 32】

（参考）本部・営業店等でのオペレーションチェックについて

オペレーションのチェックは、第一義的には処理目的の正当性や操作者の権限を確認することが重要である。本部･営業店等において、この点の確認を確実に行うためには、以下のような機能を持つこと、および手順を策定しておくことが望ましい。

1. 処理目的や根拠を責任者がチェックし、作業そのものの妥当性を確認する手順
2. 作業手順や実施タイミングの正当性を確認する手順
3. 処理結果を責任者がチェックするためのレポート出力機能や、作業履歴を取得し、保存する機能

運用時の信頼性向上対策
運用時の信頼性向上対策

適　用　区　分				
共	セ	本	提	ダ
◎				

実108	負荷状態の監視制御機能を充実すること。

削除: 技　18

コンピュータシステムの安定稼働のために、各種資源の能力や容量の限界を超えないように負荷状態を監視し、必要に応じて制御する機能を充実すること。

1.　負荷状態の監視制御機能の例として、以下のようなものがある。

(1) 監視機能

①　負荷状態表示機能

中央処理装置、チャネル装置、ファイル装置、通信制御装置、回線等の負荷状態が把握できるような表示機能である。

②　使用状況照会機能

主記憶装置、ファイル装置等の資源の使用状況（バッファ、ファイル容量等）を把握するため、照会機能を設けておく方法である。

さらに、使用率が限界値に近づいた場合、警告を発する機能を設けておく方法もある。

③　統計分析機能

各種資源の使用状況について、平均値、最大値等の統計データが得られるようにしておき、それを定期的にチェックし、対策を事前に講じておくという方法である。

(2) トラフィック制御機能

メッセージの待ち行列やシステムコントロール上重要なカウンター類等の使用状況が限界に近づいた場合、コンピュータシステムへの入力を抑える制御機能を設けておき、コンピュータシステムを安定的に稼働させるものである。

また、トラフィック制御はジョブの優先度･多重度を変更することによって行うこともある。

2.　本部・営業店等に分散配置された機器等については、リモートによる集中監視・制御が有効である。

なお、分散環境における負荷状態の監視機能としては、SNMP 等の監視用プロトコルを使用することによって、分散したシステムのノード装置の管理情報データベース（MIB）を定期的に収集したり、しきい値を超えたノードがアラームを自動送出したり、ノード装置のリモート制御が可能になる。

（SNMP：Simple Network Management Protocol）

（MIB：Management Information Base）

（参考）

過負荷発生のトラフィック制御のミスにより、重大な故障に発展したケースがあるので参考までに事例を以下に取りまとめた。

過負荷トラブルはオンラインシステムを構成する各種資源が、さまざまな要因で不足することに起因して発生する。

1. 資源不足の具体例としては、以下のようなものがある。
   - CPU 能力の不足（マルチプロセッサの片側 CPU 故障時等）
   - ファイル装置またはチャネル装置の使用率オーバー（パス系故障による片パス運用時の考慮洩れ等）
   - 主記憶装置容量不足（業務追加に伴うメモリ不足等）
   - 回線容量不足（部分的回線故障に起因等）
   - タスク数不足（トラフィック増加に伴う使用率増大等）
   - 一部の主記憶上のカウンター類への負荷集中（異常なトラフィックによる使用率増大等）
2. 主な障害の現象としては、タイムオーバーを繰り返す場合と、バッファ負荷となり過負荷通知はするが、負荷制御機能が働かずシステム異常になる場合とがある。

   前者のケースは、レスポンスタイムの悪化により、システム異常にみえるが、システムとしては、正常な動作をしているので、入力電文を減少させれば回復する場合が多い。

   後者のケースは、以下のような要因によるものであり、回復措置としてシステムの初期化を要する場合が多い。
   - バッファ過負荷発生の限界値の指定ミス（タイムオーバー等の同一エラーの繰返し、負荷通知用のバッファ不足等）
   - 負荷制御処理タスク（または入力キュー）の優先順位の設定ミス
   - スタック容量の不足（OS のテーブルチューニングにより設定）

運用時の信頼性向上対策
運用時の信頼性向上対策

適　用　区　分				
共	セ	本	提	ダ
	◎	◎	◎	

実 109	CD・ATM 等の遠隔制御機能を設けること。

削除: 技　19

無人店舗における CD・ATM 等の安定運用のために、運用状況を集中監視し、必要に応じて遠隔制御を行う機能を設けること。

1.　無人店舗の CD・ATM 等の運用状況を集中監視する場合、設備基準に加え、以下のような技術面にも考慮した安全対策を行う必要がある。【設 111～設 117】

(1) 異常状態（現金切れ、ジャム、機器異常、回線断等）の検知機能を設けること。

(2) 現金、ジャーナル等のニアエンドを検知して、適切な処置を行うこと。

(3) 装置等の稼働状況を検知（エラー等の集計）し、適切な予防保守を行うこと。

14 障害の早期発見・早期回復

削除：Ⅰ．システム信頼性向上対策

削除：（Ⅳ）

障害が発生した際には、早急に障害状況を検出し、その影響を最小限に抑え、速やかに回復するための対策が重要である。

障害の早期発見・早期回復
障害の早期発見

適　用　区　分				
共	セ	本	提	ダ
◎				

実 110	システム運用状況の監視機能を設けること。

削除: 技　20

障害の早期発見・回復のために、コンピュータシステムの運用状況（稼働状態、停止状態、エラー状態）を監視する機能を設けること。

1. コンピュータシステムの運用状況は、システムの重要性に応じた適切な監視がなされる必要がある。なお、個人データを取り扱うシステムにおいては、この措置は必要である。また、待機中の機器についても、本番環境に接続されている等により監視可能な場合には、本番機と同様の扱いとすることが必要である。具体的事例として、以下のようなものがある。

(1) ソフトウェアによる監視
　一定時間ごとに装置へのアクセスを行い状態把握を行うものである。

(2) コンソールからのステータスディスプレイ機能による表示
　オペレータからの照会コマンドにより各機器の状態を表示するものである。

(3) 遠隔監視盤等によるリモート監視
　システムの運転状況やエラーメッセージ等を表示するディスプレイ装置により、コンピュータ室から離れた室で監視を行うものである。

(4) サービスプロセッサによる監視
　保守診断専用の独立したプロセッサであり、リアルタイムにシステムの運転状況を把握するものである。

2. システムの規模が大きくなるにつれ、集中監視が重要になってくる。
　具体的事例として、以下のようなものがある。

(1) コンピュータシステムの監視については中央処理装置、チャネル装置、各種ファイル装置等の運転状況を集中監視する方法がある。

(2) ネットワークの監視については、回線、マルチメディア変換装置、時分割多重装置、モデム、TA、ルータ、HUB、端末等の運用状況を集中監視する方法がある。

3. その他
　システムの重要度により、本部・営業店等に設置されたサーバーの監視も必要である。本部・営業店等において必要な技能を持った担当者を置くことが困難な場合には、リモートによる集中監視のみならず以下のようなリモート制御の機能を持つことが望ましい。

・サーバーのパワーコントロール（リモート電源 ON／OFF）
・DBMS 等のミドルソフトウェアや業務アプリケーションの起動・終了
・システム環境の最適化

・データアクセスの分散化やトランザクションのプライオリティ制御

（参考）本部・営業店等に設置されたサーバー・システムにおける考慮点

本部・営業店等に設置されたサーバー・システムの安全性・信頼性に関しては、以下の点を考慮する必要がある。

(1) コンピュータセンター以外の場所に設置された機器等については、熱、振動、水、煙、埃、電圧変化などの脅威に晒される機会が増加する。

(2) LAN 等のネットワークの大規模化、複雑化が進展し、障害発生時の原因究明を困難にしている。

このようなことから、危険な兆候や業務処理に支障の起こる可能性のある状態（例えば、磁気ディスクの I/O エラーの増加や局所的なトラフィックの集中）を早期に発見し、しかるべき対処を行うことも必要である。そのため、システムの運用状況を監視することが重要であり、監視・制御専用のネットワークサーバー等を用いた集中監視・制御が有効である。

障害の早期発見・早期回復
障害の早期発見

適　用　区　分				
共	セ	本	提	ダ
◎				

実 111	障害の検出および障害箇所の切り分け機能を設けること。

削除: 技　21

迅速な障害回復に役立てるため、コンピュータシステムに発生する各種障害を的確に検出し、障害箇所を切り分ける機能を設けること。

1.　障害を検出し、障害箇所の切り分けを行うために、以下のような機能がある。

(1) 異常検出機能

迅速な障害回復に役立てるための異常を検出する機能であり、具体的事例として、以下のようなものがある。

①　中央処理装置、主記憶装置、ファイル装置、回線、端末装置等の障害検出機能

②　ソフトウェア障害検出機能

(2) ロギング機能

迅速な障害箇所切り分けに役立てるためのロギング機能であり、具体的事例として、以下のようなものがある。

①　エラー発生時の状態に関する詳細情報のロギング機能

②　コンソールメッセージのロギング機能

③　障害発生までの稼働状況がトレースできるような情報をロギングする機能

（例：I/O トレース、モジュールトレース等）

(3) テスト機能

迅速な障害箇所切り分けに役立てるためのテスト機能であり、具体的事例として、以下のようなものがある。

①　障害箇所を切り分けるための折返しテスト機能

②　障害箇所を切り分けるための診断テスト機能

障害の早期発見・早期回復
障害の早期回復

適　用　区　分				
共	セ	本	提	ダ
◎				

実112	障害時の縮退・再構成機能を設けること。

削除: 技　22

障害時に、一部の処理を中断しても、システム全体を停止させることなく運転を続行させるため、機能を縮小し、システムを再構成する機能を設けること。

1.　縮退・再構成機能の例として、以下のようなものがある。

(1) 障害が発生した部分に関する取引を閉塞する機能

(2) 障害が発生した部分の切離しを行う機能

オンラインシステムに影響を与えないで修理できるようにすると、さらに有効である。

削除: 更

(3) 正常な構成要素で運転が続行できるように構成しなおす機能

障害復旧後、再組込みができるようにしておくと、更に有効である。

2.　対象となる構成要素として、ハードウェア、ソフトウェアの両面があるが、ハードウェア対象例として、以下のようなものがある。

・マルチプロセッサシステム等における中央処理装置
・主記憶装置
・チャネル装置
・ファイル装置
・通信制御装置
・回線、端末系装置

なお、縮退・再構成時のオペレーションについてもパターン化し、極力オペレータの介入を少なくしておくことも有効である。

障害の早期発見・早期回復
障害の早期回復

適　用　区　分				
共	セ	本	提	ダ
◎				

実113	取引制限機能を設けること。

削除: 技　23

ファイル障害やプログラムミス等による影響を極小化するため、ファイル単位、科目単位等による取引制限機能を設けること。

1.　障害の影響を局所化するため、障害の状況に応じ一部取引を稼働中のシステムから切り離すなどの措置がとれるような取引制限機能を設けておくことが必要である。

2.　具体的な取引制限の単位として、以下のような例がある。

・業務
・科目
・提供サービス・商品
・稼働プログラムの制御単位
・営業店等の営業地域
・端末装置
・取引相手、取引口座

障害の早期発見・早期回復
障害の早期回復

適　用　区　分				
共	セ	本	提	ダ
◎				

実 114	リカバリ機能を設けること。

削除: 技　24

障害が発生した場合は、速やかにシステムを回復させ業務を支障なく続行させるために必要なリカバリ機能を設けること。

1. 障害による業務への影響時間を短縮し業務への支障を少なくするため、リカバリのための機能が必要である。

2. 複数サーバーで構成される分散処理システム等、複数のコンピュータで構成されるシステムの場合は、各コンピュータ間のシステム的な整合性を維持して復旧できるリカバリ手順を決定しておく必要がある。

3. リカバリ機能としては、例えば以下のようなものがある。

削除: たと

(1) リカバリ用ジャーナル機能
　各種リカバリに役立たせるため、データ処理の過程を記録しておく機能である。
(2) チェックポイント機能
　迅速なリカバリを行うため、主記憶装置に展開している重要カウンターおよび端末テーブル等を一定時間ごとまたは一定取引量ごとに外部記憶装置に記録しておく機能である。
(3) 部分リカバリ機能
　プログラムやタスク等が異常終了した場合、他のプログラムやタスクには影響を与えず（システムダウンさせず）、ジャーナル情報を基に回復させる機能である。
(4) ダウンリカバリ機能
　システムダウンに至った場合、ジャーナル情報を基に回復させる機能である。
　そのためには、取引の成立基準を定めておくとともに、再開始時に最終成立取引が把握できるようにしておくことも重要である。
(5) ファイルリカバリ機能
　ファイルに障害が発生した場合、バックアップファイルやジャーナルに基づき、ファイルを回復させる機能である。
　なお、迅速なファイルリカバリのため、装置の特性に応じて、例えばユニット単位、シリンダー単位等により回復範囲の極小化を図る方法もある。

削除: たと

4. 24 時間オンライン運転を行う場合は、リカバリに必要なデータをオンライン運転中にオンラインサービスに支障を与えることなく取得できる機能もしくは仕組みを考慮しておく必要がある。

該当する機能としては、例えば以下のようなものがある。

(1) ファイルの復旧においては通常、元帳ファイル等のバックアップファイルを起点としてジャーナル情報により回復させる。そのためには、元帳のバックアップファイルが必要となる。

これら元帳のバックアップをオンライン運転中にも取得できるように元帳ファイルのスワップを行う機能等を考慮しておくことが必要である。

(2) プログラム修復においては、プログラム内容に起因する障害が発生した場合、システムを停止させることなく、該当プログラムの修正を行う。

なお、分散処理システムのプログラムを修復させる方法としては、オフラインによるメンテナンスやオンラインによるリモートメンテナンス機能等がある。

15 災害時対策

削除：Ⅰ．システム信頼性向上対策 .

削除：（V）

削除：.

コンピュータセンター等が災害等により機能しなくなった場合に備えて、リスクの分散の意味で、別の地域にバックアップサイトを設置することが望ましい。

災害時対策
バックアップサイト

適　用　区　分				
共	セ	本	提	ダ
	○			

実115	バックアップサイトを保有すること。

削除: 技　25

コンピュータセンター等が災害等により機能しなくなった場合に備えて、業務の優先度を考慮してバックアップサイトを保有することが望ましい。

1. コンピュータセンター等が災害等により機能しなくなった場合に備えて、リスク分散の意味で、別の地域にバックアップサイトを保有することが望ましい。

特に、資金決済等を行う重要なシステムについては、原則としてバックアップサイトを保有することが必要である。

ただし、バックアップサイトを保有しない場合は、障害による社会への影響を十分に検討のうえ、他に代替する方法による業務継続態勢を整備し、経営層が承認する必要がある。

バックアップサイトの運営形態としては、以下のものがある。

(1) 自営センター

自社専用の代替施設として利用する。

(2) 共同利用センター

複数企業が共同で代替センターを設立し、必要時に利用する。

(3) 相互利用センター

別地域にある同一企業（グループ）内の事業部門と相互に被災時等にバックアップし合う。代替施設提供部門は、被災時等には緊急度の低い業務は一時運用を止めて対応する。他企業（協力企業）間でバックアップし合う場合もある。

(4) 代行処理センター

第三者にバックアップを委託し、必要時に利用する。

2. バックアップサイトを外部に委託している場合、複数の委託元で同時に緊急事態が発生するケースを想定して、バックアップを受ける優先順位、最低保証の範囲などのサービスを確認し、事務量の変化に対応して定期的に見直すことが必要である。

3. バックアップサイトの保有にあたっては、以下の事項を考慮し、総合的に判断することが望ましい。

(1) コンピュータセンターと同一のリスク要因（火災、地震、停電等）を共有しないこと。

(2) 被災時の要員、データ、物資等の移動・移送時間を含む復旧時間を確認しておくこと。

（参考）
バックアップサイトの立地条件については、コンピュータセンターの立地条件と同様に考える必要があるため【設1】を参照のこと。

16 データ保護

削除: Ⅱ.安全性侵害対策 .

削除: （Ⅰ）

機密データや重要データは、漏洩、破壊、改ざんなどによる影響が極めて大きい。また、これらのデータへのアクセスに必要な暗証番号、パスワード等が漏れた場合、影響は多大なものになる。そのため、これらのデータに対する保護対策を講ずることが必要である。

(1) 漏洩防止

削除: 1.

重要なデータに関しては、その重要性などに応じて、蓄積データ、伝送データともに適切な漏洩防止策を講ずる必要がある。

データ保護
漏洩防止

適　用　区　分				
共	セ	本	提	ダ
◎				

実 116	暗証番号・パスワード等は他人に知られないための対策を講ずること。

削除: 技　26

暗証番号・パスワード等の漏洩防止のため、非表示、非印字等の必要な対策を講ずること。

1.　端末機における漏洩防止として、暗証番号・パスワード等は、他人に知られないように、非表示、非印字、記号などへの置換え、覗き見防止等の対策を講ずることが必要である。また、媒体上に暗証番号・パスワード等をそのまま記憶させない等の対策を講ずることが必要である。

磁気ストライプ方式のキャッシュカードにおいては磁気ストライプ上に暗証番号を持たない方式（ゼロ暗証方式）を採用することが必要であり、ホスト上の暗証番号を参照し本人確認を行う必要がある（ホスト照合方式）。

また、磁気ストライプ上の暗証番号を消去する機能を有することが必要である。

2.　暗証番号・パスワードの利用等にあたっての安全対策上の機能としては、例えば以下のようなものがある。

(1) 暗証番号・パスワードには NULL または少ない桁数を認めない機能

(2) 暗証番号・パスワードの使用に有効期間を設定し、有効期限近接時は、事前に変更要求を行う機能

(3) パスワードの変更にあたって前回もしくは以前と同一のパスワードの使用を認めない機能

(4) 特定の予測可能なパスワード（自分の会社名等）や不適切なパスワードを排他的に定義することができる機能

(5) アクセスの都度、アクセスに使用するパスワードを変更するワンタイムパスワードの機能

ワンタイムパスワードの機能を実現するには、以下のようなものが考えられる。

①　端末以外の機器（IC カードやパスワード生成機等）でワンタイムパスワードを生成させる方式

なお、下記の点に留意すること。

・ワンタイムパスワードはランダムに生成されること

・ワンタイムパスワードは生成させる機器ごとにユニークであること

・ワンタイムパスワードを生成させる機器は耐タンパー性などを有すること

②　前もって複数の乱数をパスワードとして顧客に渡しておき、利用の都度パスワードを使い捨てにする方式

③　サーバーで生成したワンタイムパスワードを電子メールで利用者に通知する方式

ただし、通知先については取引に利用している機器とは別の機器で利用者が受信することを強く推奨すること。

(6) 新規ユーザーの初回ログオン時に、初期設定されたパスワードからユーザー自身のパスワ

ードに強制的に変更をうながす機能

(7) ソフトウェアキーボードを使用し、キーロガーによる暗証番号・パスワードの盗取を防止する。

なお、ソフトウェアキーボードは画面キャプチャーや暗号化前の電文を盗取するようなタイプのスパイウェアの対策にはならないことに留意する必要がある。

(8) 盗撮カメラが発する電波をもとに不正な設置を検知する機能

(9) 暗証番号の登録・変更時に推測されやすい暗証番号の登録を認めない機能

3. 暗証番号・パスワード等を他人に知られないための運用における対策については【運 17】参照のこと。

4. テレホンバンキング等、パスワードで本人確認を行うサービスを提供する場合、以下のような安全対策上の機能を設けることが望ましい。

(1) CD･ATM 等によるパスワードを変更する機能

(2) 個々のサービス別に異なるパスワードを設定する機能

5. CD・ATM 等の覗き見防止の対策としては、以下のような例がある。

(1) 画面の表示（画面の視野角制限、文字の大きさ、文字の色合い、表示内容）

(2) 端末機の画面上におけるテンキーの利用者に応じた配列方式の採用

6. 暗証番号・パスワード等を他人に知られないためには、データ伝送について暗号化等の必要な対策の検討を行う必要がある。伝送データの暗号化策は【技 29】を参照のこと。

7. 推測されやすい暗証番号を利用している顧客に対して、ATM 等において個別に警告を行い、暗証番号の変更を誘導する機能を設けることが望ましい（推測されやすい暗証番号については、【運 51-1】参照）。

データ保護
漏洩防止

適　用　区　分				
共	セ	本	提	ダ
○				

実 117	相手端末確認機能を設けること。

公衆通信網を通じて自動着信端末に出力する場合には、誤接続を防止するため、確認可能なものについては相手端末を確認する機能を設けることが望ましい

1. 公衆通信網を通じて金融機関等から顧客に対して振込入金等の種々の金融情報を、自動着信機能を持ったファクシミリ端末を介して連絡する場合には、暗証番号等による本人確認ができないため電話番号の登録ミス等により誤った相手に出力する可能性がある。

2. 相手確認が可能な端末については、相手端末確認機能を用いることが望ましい。
接続相手端末確認の例としては以下のようなものがある。
(1) 電話の発信者情報通知サービス、携帯電話の識別番号等の利用
(2) ファクシミリの端末 ID の利用
(3) 認証機関が発行する電子的な証明書【技 35】

3. 公衆通信網を通じてパソコンやコンピュータへ種々の資金移動や金融情報を通知する場合、接続する際に端末 ID や発信者確認コードの確認を行う等の機能を設けることが望ましい。
【技 35】

削除: 技　27

削除: テレックス端末や

削除: (3) テレックスのアンサーバックの利用 .

削除: 4

データ保護
漏洩防止

適　用　区　分				
共	セ	本	提	ダ
○				

実 118	蓄積データの漏洩防止策を講ずること。

削除:　技　28

ファイルのコピーや盗難等による漏洩を防止するため、重要なデータについては暗号化等の対策を講ずることが望ましい。

1.　ファイルの不正コピーや盗難の際にも、データの内容がわからないようにするため、重要なデータについては暗号化することが望ましい。特に個人データを蓄積する場合には、暗号化・パスワード設定等ファイルの不正コピーや盗難の際にもデータの内容がわからないようにするための対策を講ずることが必要である。また、電子的取引において蓄積されるデータについても暗号化・パスワード設定等の対策を講ずることが必要である。

パスワード設定の例としては、以下のようなものがある。

①　データベース　：DBMS の備えるパスワード【技 31】
②　文書ファイル　：文書そのものにかけるパスワード
③　ハードディスク：ハードディスクドライブにかけるパスワード。パスワードが知られない限り他の機器に接続しても読み取り不可能となる。

なお、外部持ち出しや他の媒体へのコピーが物理的に不可能なコンピュータ機器内の個人データの漏洩防止策としては、上記対策の他、本人確認機能を設けることにより、許可された者以外の者が当該データを判別できないようにする仕組みも有効である。（本人確認機能については【技 35】参照。）

また、ホストコンピュータ等でのみ読み出し可能な個人データを媒体に蓄積する際には、フィジカルダンプ等で断片化させて蓄積することにより、特定のソフトウェア・ハードウェアを用いなければ判別できないようにする方法も有効である。

（注 1）ホストコンピュータ等：ホストコンピュータ、またはそれに準じるコンピュータ
（注 2）フィジカルダンプ　　：ファイルレイアウト等論理的な構成を無視し、ディスクの先頭から順番にコピーすることにより、個別にファイルを復帰することができないようにすること。

2.　暗号の使用にあたっては、CPU 負荷の増大、業務処理遅延等の影響にも留意して、信頼のおける適切な技術を選択することが必要である。なお、適用する技術は、情報処理技術の発展とともにその強度が変化することに留意するとともに、その使用にあたっては、複数の方式を適切に組み合わせて使用することが望ましい。

また新規にシステムを構築する、あるいはシステムを更新する際には、技術の進歩により暗

号は脆弱になることや暗号技術も日々進化していることを踏まえ、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」等に記載されている、安全性が継続的に検証されている暗号方式を採用することが望ましい。

3. IC カードにおける漏洩防止策としては耐タンパー性、その他蓄積媒体上の漏洩防止策としては暗号化が考えられる。

蓄積媒体上の暗号化として、以下のレベルがある。

(1) ファイルの中の重要な項目だけ暗号化
（例：暗証番号、パスワード、電子的価値情報等）

(2) 重要ファイルについて全項目を暗号化
（例：パスワードファイル、個人情報ファイル、電子的価値情報ファイル等）

4. 渉外端末の盗難・紛失時に備えた対策として、渉外端末内に重要なデータを蓄積する場合には、暗号化することが望ましい。なお、個人データを蓄積する場合には、暗号化・パスワード設定等の対策を講じる必要がある。

（参考 1）
暗号化の方式としては、例えば以下のようなものがある。
(1) 共通鍵暗号方式
暗号化する時に使用した鍵と同じ鍵で復号する方式。
(2) 公開鍵暗号方式
ペアになった 2 つの鍵でデータを暗号化、復号する方式で、どちらか一方の鍵を公開する。

5. 端末機器からの漏洩防止策としては、以下のようなものがある。

(1) 封印ラベル等による周辺機器との接続部分の固定や物理的封鎖、外部記憶装置の取り外し、ソフトウェアによる記録媒体の使用制限

(2) 使用する記録媒体内のデータの暗号化

(3) CD・ATM 等を含む端末機器内部のデータに対するアクセス権限の制限【運 16】

なお、一時的な使用制限の解除が認められる場合には、使用制限の再設定手続きと定期的な制限の確認が必要である。

6. コンピュータ端末及び周辺機器から漏れる電磁波が盗聴され再現される危険性（テンペスト）があることから、対策としては以下のようなものがある。

(1) 電磁遮蔽カバーの採用

機器そのものをカバーする例として、筐体全体を金属で覆う、導電性塗料を塗布する、導電性メッシュを一体成型した非透過性シールドを CRT 映像面に装着する等がある。

機器が設置されている部屋をシールドする例として、電磁波を通しにくいシールドフィルム等を壁紙に使用する、窓ガラスに非透過性シールドを貼る等がある。

(2) 電磁波防止フィルターの採用

各種ケーブルのコネクター部に装着し、ケーブルから発生する電磁波を減少させるものが市販されている。

(3) 保護対象機器の設置場所から一定範囲内の侵入制限を行う

7. システム処理中に重要なデータを含む一時データファイルが生成される場合、重要なデータの漏洩を防止するため、利用状況に応じ不要となった時点で消去する機能を設けることが望ましい。

（参考 2）

1. 技術の進歩により暗号の脆弱性が増す事例には以下のものがある。
   (1) コンピュータの処理能力の向上により、解読に要する時間が現実的な時間に収まる。
   (2) 暗号アルゴリズムの脆弱性が発見される。
   （注）内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）において、政府機関における SHA-1 及び RSA1024 の移行についての指針等を打ち出している事例がある。
   （検討状況の参照 URL）
   http://www.nisc.go.jp/conference/seisaku/dai20/pdf/20siryou0502.pdf
   （指針の参照 URL）
   http://www.nisc.go.jp/conference/seisaku/dai17/pdf/17siryou0101.pdf

2. 総務省と経済産業省が中心となって選定した「電子政府推奨暗号リスト」は平成 15 年 2 月に発刊されている。
   また、平成 25 年 3 月には「電子政府推奨暗号リスト」を改定した「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」が策定されている。
   （CRYPTREC：URL）
   http://www.cryptrec.go.jp/

3. 「電子政府推奨暗号」の利用方法に関しては、CRYPTREC から「電子政府推奨暗号の利用方法に関するガイドブック」が平成 20 年 7 月に公開されている。
   （参照 URL）
   http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf
   （注）CRYPTREC とは Cryptography Research and Evaluation Committees の略で、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。総務省及び経済産業省が共同で運営する暗号技術検討会と、独立行政法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で運営する暗号方式委員会、暗号実装委員会及び暗号運用委員会で構成されている。

削除: <オブジェクト>

データ保護
漏洩防止

適　用　区　分				
共	セ	本	提	ダ
○				

実 119	伝送データの漏洩防止策を講ずること。

削除: 技　29

データ伝送時の盗聴等による漏洩を防止するため、重要なデータについては暗号化の対策を講ずることが望ましい。

1.　データ伝送時に盗聴された場合にもデータの内容がわからないようにするため、重要なデータについては、暗号化することが望ましい。特に個人データを伝送する場合には、暗号化・パスワード設定等データ伝送時に盗聴された場合にもデータの内容がわからないようにするための対策を講ずることが必要である。

　また、個人データを伝送する場合には、上記以外の対策として、以下の条件を満たしセキュアな環境とすることで、光ファイバーの専用線を用いることも有効である。

(1) 建物内に不正な機器が接続されていないことの確認
(2) 切断などにより、漏洩のおそれがある場合にその分析ができること
(3) 通信事業者における漏洩防止策を確認・評価していること

　オープンネットワークや無線を利用して重要なデータを伝送する場合は、通信事業者と協力するなど暗号化対策を図り、十分な漏洩防止対策を講じておくことが必要である。開発時のドキュメント、ソースコード等もその重要性に配慮した伝送方式を考えること。

　なお、構内 LAN においては、ネットワーク構成機器への未承認機器の論理的・物理的な接続を不可能とする仕組みも有効である。

（参考 1）

無線 LAN を使用する際には、以下のような点を考慮する必要がある。

(1) 従来の無線 LAN 機器で使用されている、WEP (Wireless Equivalent Privacy) の RC4 という暗号化方式は、脆弱性を回避する手段がないことから、業務システムにおいては使用しない。

(2) 平成 24 年 10 月現在で望ましいとされる暗号化方式は、IEEE802.11i 通信規格の WPA（Wi-Fi Protected Access）または WPA2 の AES（Advanced Encryption Standard）と呼ばれる共通鍵暗号方式とされている。なお、WPA または WPA2 には TKIP（Temporal Key Integrity Protocol）と呼ばれる共通鍵暗号方式も存在する。この方式に確認されている脆弱性に対応するために、安全な設定値を利用すること。

(3) 無線 LAN が使用している電波が社外に漏れることを防ぐための対策として電波遮断シートの利用が挙げられる。

(4) 参照 URL として、以下のものがある。

・「無線 LAN セキュリティ要件の検討」
http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/dai65/65lan_kentou.pdf
首相官邸各府省情報化統括責任者（CIO）補佐官等連絡会議

・「WPA の脆弱性の報告に関する分析（技術編）」
http://www.rcis.aist.go.jp/TR/2009-01/wpa-compromise.html
独立行政法人産業技術総合研究所 情報セキュリティ研究センター

・「一般利用者が安心して無線 LAN を利用するために」
http://www.soumu.go.jp/main_content/000183224.pdf
総務省

2. 暗号の使用にあたっては、CPU 負荷の増大、業務処理遅延等の影響にも留意して、信頼のおける適切な技術を選択することが必要である。なお、適用する技術は、情報処理技術の発展とともにその強度が変化することに留意するとともに、その使用にあたっては、複数の方式を適切に組み合わせて使用することが望ましい。

また、新規にシステムを構築する、あるいはシステムを更新する際には、技術の進歩により暗号は脆弱になることや暗号技術も日々進化していることを踏まえ、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」等に記載されている、安全性が継続的に検証されている暗号方式を採用することが望ましい。

（参考 2）

1. インターネットバンキング等における暗号技術は SSL（Secure Socket Layer）プロトコルが一般的になっている。SSL の暗号鍵は、数種類の鍵長が選択可能であるが、安全性を考慮すると 128 ビット以上の鍵長を使用することが望ましい。

2. SSL の暗号技術の適切な利用方法については、CRYPTREC 公開の「電子政府推奨暗号の利用方法に関するガイドブック」に記載がある。
（参照 URL）
http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf

3. Web アプリケーションの設計及び実装において、SSL を適切に使用し、重要な情報を漏れなく暗号化することが必要である。
例として以下のようなものがある。
(1) ID・パスワードや個人情報等の情報を入力させる際には、SSL を使用した画面（「https://」で始まる画面）とすること。
(2) 複数フレームを使用する際には、利用者が Web ブラウザのアドレスバーで、表示中のページが SSL で保護されていることを確認できる画面構成とすること。
(3) セッション ID 等ユーザーを特定するようなデータは常に SSL 通信を使用し、特にデータを cookie に格納する場合には、「secure」属性を付与するなどの実装を行うこと。

4. 参考文献として、以下のものがある。
(1)「安全なウェブサイトの作り方 改訂第５版」
独立行政法人情報処理推進機構（IPA）セキュリティセンター
(2)「安全な Web サイト利用の鉄則」
独立行政法人産業技術総合研究所情報セキュリティ研究センター

3. データ伝送上の暗号化の例として、以下のようなものがある。
(1) 暗号化対象範囲によるレベル
① 伝送データの一部のみ暗号化
（例：暗証番号、口座番号、電子的価値情報等）
② 伝送データ全体の暗号化
（例：伝送するレコード全体を暗号化する）
(2) 伝送路上における暗号化レベル
① 伝送回線上の暗号化
（例：伝送回線の両端に暗号化・復号装置を設置する方法）
② 端末間の暗号化
（例：端末上の暗号化ソフトにより端末間の伝送データを暗号化する方法）
(3) (1)、(2)を組み合わせた暗号化
（例：暗証番号、口座番号、電子的価値情報等の暗号化をしたうえで、さらに暗号化装置を

設置する方法）

（参考 3）

1.　技術の進歩により暗号の脆弱性が増す事例には、以下のものがある。

(1) コンピュータの処理能力の向上により、解読に要する時間が現実的な時間に収まる。

(2) 暗号アルゴリズムの脆弱性が発見される。

（注）内閣サイバーセキュリティセンター（NISC : National center of Incident readiness and Strategy for Cybersecurity）において、政府機関における SHA-1 及び RSA1024 の移行についての指針等を打ち出している事例がある。

（検討状況の参照 URL）

http://www.nisc.go.jp/conference/seisaku/dai20/pdf/20siryou0502.pdf

（指針の参照 URL）

http://www.nisc.go.jp/conference/seisaku/dai17/pdf/17siryou0101.pdf

2.　総務省と経済産業省が中心となって選定した「電子政府推奨暗号リスト」は平成 15 年 2 月に発刊されている。

また、平成 25 年 3 月には「電子政府推奨暗号リスト」を改定した「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」が策定されている。

（CRYPTREC：URL）

http://www.cryptrec.go.jp/

3.　「電子政府推奨暗号」の利用方法に関しては、CRYPTREC から「電子政府推奨暗号の利用方法に関するガイドブック」が平成 20 年 7 月に公開されている。

（参照 URL）

http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf

（注）CRYPTREC とは Cryptography Research and Evaluation Committees の略で、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。総務省及び経済産業省が共同で運営する暗号技術検討会と、独立行政法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で運営する暗号方式委員会、暗号実装委員会及び暗号運用委員会で構成されている。

削除: .

.

改ページ

<オブジェクト>

16 データ保護

削除: Ⅱ.安全性侵害対策 .

削除: （Ⅰ）

(2) 破壊・改ざん防止

削除: 2.

プログラムミスや不正なアクセスによってデータが破壊・改ざんされることを防ぐため、適切な破壊・改ざん防止策を講ずる必要がある。

データ保護
破壊・改ざん防止

適　用　区　分				
共	セ	本	提	ダ
◎				

実 120	ファイルに対する排他制御機能を設けること。

削除: 技　30

ファイル内容の矛盾発生防止のため、ファイルに対する排他制御機能を設けること。

1. 同一ファイルに複数のプログラムから同時更新がある場合は、データ内容に矛盾を起こし、結果的にファイル破壊となる。これを防止するため、ファイルに対する排他制御機能を設けることが必要である。

2. 同一システム内の複数のプログラムでファイルを共用する場合

同一ファイルに対する同時アクセスが起こり得ることから、一方がアクセス中は、その処理が終了し、ファイルを解放するまで要求中のプログラムを待たせる排他制御機能を設けることが必要である。

なお、排他制御のレベルの例として以下のようなものが考えられる。

(1) ファイルレベル
(2) ブロックレベル
(3) レコードレベル

3. 複数システム間でファイルを共用する場合

複数システムで共用されるファイルは、各システムから排他制御をかける対策が必要である。その事例として、以下のようなものがある。

(1) システム間での排他制御情報の伝達、確認
(2) ファイル制御装置の排他制御機能の活用

4. デッドロックによる待ち状態の回避策

ファイルに対する排他制御機能組込みにより、デッドロックが発生することがある。このためデッドロックによる待ち状態を回避する対策が必要である。その具体的事例として以下のようなものがある。

(1) デッドロックの検知と解除

デッドロックの発生を検知し､デッドロックが発生したトランザクションの一方をいったん無効とし、デッドロック状態を解除したうえで当該トランザクションを再処理する。

データ保護
破壊・改ざん防止

適　用　区　分				
共	セ	本	提	ダ
◎				

実 121	ファイルに対するアクセス制御機能を設けること。

削除: 技　31

不正アクセス等からデータを保護するため、プログラムとファイル間のアクセス権限チェック機能等を設けること。

1.　故意または過失によるファイルの破損、または不正アクセスからデータを保護するため、重要なファイルについては、アクセス制御機能を設けることが必要である。

2.　アクセス制限の方法としては、一般に以下のものが考えられる。
(1) OS の備えるアクセス制限の方法を使用する手法
(2) DBMS の備えるアクセス制限の方法を使用する手法
(3) アクセス制御専用のソフトウエアを使用する手法

3.　ファイルに対するアクセス制御のため、ネットワークによるアクセス制御を行うことも有効である。
ネットワークによるアクセス制御の例としては、ネットワーク機器による、IP アドレスやポートのフィルタリング等がある。

4.　具体的事例として、以下のようなものが考えられる。
(1) プログラムとファイル間のアクセス権限チェック
プログラムに、ファイルアクセス権限（参照のみ可、更新可等）を与えて、これをチェックすることによりファイル保護を行う。
(2) ユーザー（含む端末）とファイル間のアクセス権限チェック
アクセス可能なファイルの範囲、アクセスのレベル（参照のみ可、更新可等）等のユーザーに与えたファイルアクセス権限をチェックすることによりファイル保護を行う。
(3) ユーザー（含む端末）とプログラム間のアクセス権限チェック
ユーザーがアクセスできるプログラムの範囲をチェックすることにより、間接的にファイル保護を行う。

データ保護
破壊・改ざん防止

適　用　区　分				
共	セ	本	提	ダ
◎				

実 122	不良データ検出機能を充実すること。

削除: 技　32

システムへの不良データの混入を防止するため、不良データの検出・除外機能を充実すること。

1.　故意または過失により発生する不良データを検出する対策として、以下のようなものがある。

(1) 入力データのチェック

入力データの内容が論理的、形式的に不完全なものを検出する機能であり、具体的事例として、以下のようなものがある。

①　フォーマットチェック

データの各項目がその性質に応じた数字あるいは文字であり、必要なすべての項目が入力されているか。

②　範囲チェック

データの各項目の値が論理的に許される範囲内のものか。

③　チェックディジットによるチェック

顧客コード等にあらかじめ付加した検証数字について、入力された数字と定められたロジックによる計算結果とが一致するか。

削除: 予

④　妥当性チェック

データ項目の組合せ、相互関連から見て有り得ないデータまたは論理的に矛盾しているデータはないか。

⑤　通番チェック

付加された処理通番が同一のデータはないか。

⑥　マスターファイルとの照合チェック

データの各項目がマスターファイルの内容と整合しているか。

（注）データの論理的、形式的条件のチェックを主とするものであり、データ内容の本質的誤謬までは検出できないものもあるため、入力データの事前検証等、管理運用面の対策も併せて行うことが必要である。

(2) 処理履歴の確保

論理的、形式的条件のチェックで判別できなかった不良データ処理過程等を明らかにする対策として、処理履歴の確保が考えられる。これはオンライン処理業務において特に重要な意味を持つ対策であり、一般的にはリカバリ用ジャーナル等にデータ処理日時、端末、入力者の識別コード等の要件を付加することによって行われる。なお、処理履歴を記録したファイルは、

アクセス保護機能等によって保護することが望ましい。

処理履歴を記録したファイルのアクセス保護については、【技 37】を参照のこと。

16 データ保護

削除: Ⅱ.安全性侵害対策 .

削除: （Ⅰ）

(3) 検知策

削除: 3.

データの不正な破壊や改ざんなどを早期発見するために、適切な検知策を講ずる必要がある。

データ保護
検知策

適　用　区　分				
共	セ	本	提	ダ
○				

実 123	伝送データの改ざん検知策を講ずること。

削除: 技　33

重要なデータの伝送においては、改ざん検知のための対策を講じておくことが望ましい。

1. データ伝送において、重要なデータについては、改ざん検知のための対策を講じておくことが望ましい。特にオープンネットワークを介してデータを伝送する場合は、伝送途中におけるデータ改ざんを検知するための対策が講じられている必要がある。

2. 暗号技術を活用した認証機能、改ざん検知機能としては、例えば以下のようなものがある。
   ・メッセージ認証コード
   ・電子署名

参照法令	電子署名及び認証業務に関する法律

データ保護
検知策

適　用　区　分				
共	セ	本	提	ダ
◎				

実 124	ファイル突合機能を設けること。

削除: 技　34

故意または過失により起きたファイル間の不整合を早期に発見するため、元帳、精査表、ジャーナル等のファイル間の突合機能を設けること。

1. 故意または過失により起きたファイル間の内容不整合、論理エラー等を早期に発見するため、元帳、精査表、ジャーナル等のファイル間の内容を突合、検証する機能を設けることが必要である。

2. 不整合の原因として、以下のようなものが考えられる。
(1) データの改ざんによる不整合
(2) プログラムのミスによる不整合
(3) システム障害時、仕掛かり中取引のリカバリ不備による不整合

3. ファイル突合機能として、例えばトータルチェック等がある。
トータルチェックは、元帳ファイルと精査表を合計数値により突合するものである。
さらに、元帳ファイルと取引ジャーナルとの突合を行うことは、整合性の精度を高めることに役立つ。

4. 分散処理においてファイルを分散している場合には、ファイル間の整合性に留意することが必要である。

17 不正使用防止

削除: Ⅱ.安全性侵害対策 .
削除: （Ⅱ）

ネットワークの広がりにより種々の端末からアクセスが可能となり、権限を持たない者による不正取引またはデータやソフトウェアの改ざん等の増加が考えられるため、アクセス権限確認、利用範囲の制限等の対策を講ずることが重要である。

なお、不正使用防止策については、各機関において機器・端末種類、用途等により不正行為を分類し、チェック項目を定めることが重要である。

予防策

削除: 1.

(1) 予防策（アクセス権限確認）

削除: 1-1.

コンピュータシステムの不正使用を防止するため、本人確認、端末確認や媒体の正当性確認など、アクセス権限の確認をすることが重要である。

(2) 予防策（利用範囲の制限）

削除: 1-2.

アクセス権限確認が十分でない場合や不正アクセスの危険性が高いと認められる場合には、利用範囲を制限する対策を講ずることが必要である。

(3) 予防策（不正・偽造防止対策）

削除: 1-3.

カード犯罪を防止し、カードを利用したサービスを安全に提供するため、カードの偽造防止対策を講ずることが望ましい。また、電子的価値データや暗号鍵には、そのデータの保護機能もしくは偽造･改ざんを防止・検知する対策を講ずることが必要である。

不正使用防止
予防策（アクセス権限確認）

適　用　区　分				
共	セ	本	提	ダ
◎				

実 125	本人確認機能を設けること。

削除: 技　35

不正使用防止のため、業務内容や接続方法に応じ、接続相手先が本人もしくは正当な端末であることを確認すること。

1. コンピュータシステムの不正使用及びネットワーク拡大による種々の端末を使用した不特定多数の者からの不正アクセスを防止するため、正当な権限を保有した本人であるか、もしくは正しい端末に接続されているかなど、接続相手先の正当性を確認することが重要である。

2. インターネットを介した電子的な取引や支払指図の受付等を行う場合は特に、なりすまし等を防止するため、通信相手が正当な権限を持った者であることを確認できる仕組みが必要である。

3. 本人確認の方法として、以下のようなものがある。

(1) 広義のパスワード
- 暗証番号
- ID・パスワード
- イメージ連想
- ワンタイムパスワード
- チャレンジ・レスポンス方式　　等

(2) 暗号利用
- 共通鍵方式
- 公開鍵方式
- 電子署名
- 認証機関が発行する電子的な証明書　　等

(3) バイオメトリクス（個人の身体的特徴を識別情報とした本人確認技術）
- 指紋
- 声紋
- 掌紋
- 網膜パターン
- 虹彩
- 筆跡
- 顔　　等

(4) 所有物
- 磁気カード（キャッシュカード、オペレータカード、役席カード 等）
- IC カード

・パスワード生成機
・携帯電話の識別番号　　等
(5) これらの併用

なお、キャッシュカードのICカード化に当たっては、「全銀協ICキャッシュカード標準仕様」に要求される要件を満たすこと（セキュリティや互換性など）。また、ICカードの運用面や技術面について、セキュリティ対策上、以下のような点に注意することが必要である。
・ICカードの有効期限（電子証明書の有効期限）
・電子証明書の認証機関の信頼性（運用規定等）
・使用される暗号の強度
・耐タンパー性
【運43】【技40】を参照のこと

4. 端末確認の方法として、以下のようなものがある。
(1) 端末ID確認
(2) 電話番号確認
(3) コールバック
(4) 認証機関が発行する電子的な証明書等による接続先サーバーの認証
(5) IPアドレス等で利用場所を制限する方式

5. 本人確認のために使用される手段の管理運用方法については、以下の基準を参照のこと。
【運16～運18、運39、運51】【技26】

6. たとえ端末の操作や画面の情報が盗取された場合でも、当該情報だけではなりすまされる可能性が少ない方式とすることが望ましい。
上記の例としては、以下の方式がある。なお、セキュリティ強化の観点から、固定パスワードと下記方式を組み合わせることも有効である。
ただし、個人顧客を対象とするインターネットバンキングにおいては、ログイン時と重要取引時の少なくともどちらか一方で、固定式のID・パスワードのみに頼らない認証方法の導入が必要である。
(1) 乱数表
(2) ICカード
(3) パスワード生成機、またはメール等によるワンタイムパスワードの通知
(4) 携帯電話等による取引のON／OFF
(5) 電子証明書　　等
電子証明書については、他の媒体に電子証明書を保存することも、インターネットバンキングの利用時以外は利用者が当該媒体を外すことにより、証明書を利用できない状況となるため、被害の予防に有効である。
乱数表等本人認証に用いる媒体については、キャッシュカードと同様に、発行、保管、交付、回収及び廃棄の管理方法を明確にすることが必要である。その際に、有効期限があるものや、取引回数とともにリスクが増加するものは、その特性を考慮して管理方法を検討することが必要である。【運51】

7. ID・パスワードを用いて携帯電話の識別番号を金融機関に登録する方式においては、ID・パスワード漏洩時に、第三者の携帯電話の識別番号を、不正に登録されるリスクがあるため、登録時には異なる認証を用いることが望ましい。

（参考 1）

1. ワンタイムパスワード

不正アクセスを防ぐため、ユーザーを認証する際に使用するパスワードをアクセスのたびに変更する仕組み。ワンタイムパスワードの実現方式として、タイムシンクロナス方式とチャレンジ・レスポンス方式がある。タイムシンクロナス方式は、サーバーと同期のとれたパスワード生成機でワンタイムパスワードを生成させる方式。チャレンジ・レスポンス方式は、サーバーがチャレンジ・コード（一種の乱数）をユーザーに送信し、それを元に乱数表等を用いてワンタイムパスワードを生成させる方式。

また、前もって複数の乱数をパスワードとして顧客に渡しておき、利用の都度パスワードを使い捨てにすることにより、ワンタイムパスワードの機能を実現する方法もある。

なお、「IC カード」「電子証明書」については内部的に毎回異なるパスワードを生成させているため、広義のワンタイムパスワードとも位置づけられる。

2. トランザクション認証

取引に使用するパソコンとは別の機器（ハードウェアトークン等）に振込先口座番号や振込金額を入力し、口座番号と金額等を元に計算された認証コードを取引時に入力することで、中間者攻撃を防ぐ仕組み。仮に、第三者が通信経路上で振込先や振込金額を改ざんした場合でも、計算結果である認証コードが不一致となるため不正送金対策に有効である。

3. 共通鍵暗号方式

暗号化する時に使用した鍵と同じ鍵で復号できるタイプの暗号方式。鍵を 2 者間で共有する必要があるため、通信相手ごとに別々の鍵が必要となる。

4. 公開鍵暗号方式

2 種類の鍵（秘密鍵と公開鍵）を使用する方式で、一方の鍵を使って暗号化し、復号にはもう一方の鍵を使用する。片方の鍵を公開し片方を秘密にすることで、通信相手が複数であっても一組の鍵を管理するだけでよい。

5. 電子署名

電子情報の真正性を確保するための技術であり、現在、公開鍵暗号方式に依拠したデジタル署名が一般的である。本人確認の他、改ざんの防止、取引否認の防止にも有効である（図 1）。なお、鍵長等により暗号強度（暗号解読の困難性）が変わるなどに留意することが必要である。

6. 証明書

公開鍵が本人のものであることを証明する、認証機関によって発行されるデータ。公開鍵と鍵の持ち主の情報等が記載されており、これらの情報に対して認証局が電子署名をすることで証明書の正当性を保証している。証明書のフォーマットの国際標準は ITU-T（ International Telecommunication Union Telecommunication Standardization Sector：国際電気通信連合 電気通信標準化部門）の X.509 で規定されている。インターネットバンキングにおいては、電子証明書に対して申請者や承認者といった権限情報を付与することが必要となることが多いが、再発行時に電子証明書を盗取するマルウェアが存在した場合でも、再発行時に権限情報が付与されていないことで、不正送金の被害を防ぐことができる。

7.　送信者認証技術

メールの送信元が信頼できるものかどうか確認する技術。以下のような方式がある。

(1) DNS の仕組みを利用し、送信者がメール送信に利用しているメールサーバーを特定し、送信元アドレスで示されるドメインと同じ場所から送信されているかどうかを確認する方式（送信ドメイン認証）

(2) 差出人の秘密鍵を使って暗号化した署名をメールのヘッダに埋め込み、受信側のサーバーが公開鍵を使って署名を認証し、メール送信者の身元を識別する方式（電子署名付メール）

8.　サイト認証（サーバー証明書）

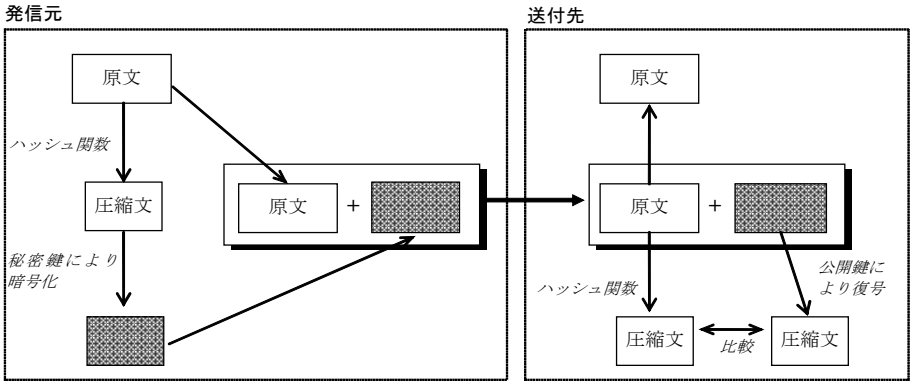
Web サーバーに対して発行される電子証明書であり、クライアントからサーバーの実在を確認する技術。信頼できる第三者機関に申請し発行される証明書を使用することが望ましい。なおその証明書として、発行者によるサイト運営組織・企業の審査に一定の基準を設けた EV SSL 証明書（注 1）がある。

（注 1）EV SSL（Extended Validation SSL）証明書

アメリカの CA/Browser Forum によって標準化された発行・運用プロセスに従った SSL サーバー証明書。証明書の発行にあたってはドメイン名の所有権や、組織・企業の実在性、申請責任者の権限が厳格に検証される。

9.　ネットワーク認証（IEEE802.1X 等）

ネットワークを利用してユーザーを認証する技術。事実上の標準規格である IEEE802.1X を利用することで、ユーザーの認証が成功するまで認証データ以外の通信をすべて遮断することができる。有線 LAN での適用も可能であるが、無線 LAN での利用が進んでいる。ただし、この規格では通信データの暗号化が行われないため、別途暗号化が必要になる場合がある。



・発信者の公開鍵で復号できるということは、確かに秘密鍵を保有している本人が作ったということ。
・原文の圧縮文と、復号した圧縮文が一致した場合は、伝送途中で第三者により改ざんされなかったということ。

図１　電子署名の利用例

（参考 2）
「リスク分析に基づく認証方式の選択」
認証方式によってリスクに対する耐性が異なる。
各金融機関で認証方式を採用するにあたっては、こうしたリスクに対する耐性を分析したうえで、一つの手口のみで破られない認証方式を採用することが求められる。
リスクに対する耐性を分析するにあたり留意する点としては、以下のようなものがある。

(1) パスワードは一般的に記憶に頼るものであるため紛失・盗難、コピーには強いが、固定パスワードの場合はスパイウェア、フィッシングによる情報の詐取に対するリスク耐性は弱いと考えられる。
(2) 固定パスワードの桁数を長くすると利用者が覚えにくくなりメモ等に記録してしまうため、盗難や紛失・コピーの危険性が生じる。
(3) 乱数表やパスワード生成機は盗難・紛失の危険性があるが、認証情報が可変であるため、スパイウェア、フィッシングによって詐取された認証情報の再利用を防ぐ効果がある。
(4) 乱数表を使用する場合、使用回数が増えるにつれ、乱数表が解明されるリスクが高くなることに留意が必要である。以下の対策を組み合わせることがより有効な対策となる。
・十分に複雑な乱数表を用いる。
・一定期間（取引回数）ごとに乱数表を更新する。

参照法令	電子署名及び認証業務に関する法律

不正使用防止
予防策（アクセス権限確認）

適　用　区　分				
共	セ	本	提	ダ
◎				

実 126	生体認証の特性を考慮し、必要な安全対策を検討すること。

削除:　技　35-1

生体認証の導入と運用にあたっては、技術の最新動向等に留意し、その特性を十分考慮し、必要な安全対策を検討すること。

生体認証の導入と運用にあたって、考慮すべき特性として、以下のものがある。

1. 認証精度

認証精度設定等の適切性の確認を行うことが必要である。（認証のしきい値を厳しく設定すると、一般に本人拒否率が高くなり、利用者はフラストレーションを引き起こすため、実務においては、これをゆるく設定しがちになる。しかし、しきい値をゆるく設定すると、他人受入率の上昇につながり、他人によるなりすまし等の可能性を高める。この観点から、両者のトレードオフを、（生体認証の結果が適用される）アプリケーションの特性を考慮し、調整することが重要となる。）

また、テンプレートを生成・発行する際は、テンプレートが十分なデータ・ポイントを有し、設定した精度を充足するよう、考慮することが必要である。

なお、顧客に対して認証精度を提示している時は、実装されている認証精度が提示値を充足することが必要である。

2. 代替措置手続き

生体認証が機能しない場合（例、正当なアクセス権限を有する顧客から「認証時に拒否される旨」申告された場合等）に備えて、代替措置手続き、手段を明確にすることが必要である。

なお、具体的策定にあたっては、代替措置手続き、手段がセキュリティ・ホールとならないようにすることが必要である。

3. 否認防止

「顧客による否認」防止の機能を用いる場合には、以下の点を考慮することが望ましい。

(1) 生体認証の結果を記録し、事後に検証する手段、手順、あるいは運用上の措置。

（例：・ IC カード発行時に、その IC カードが本人の認証に適合したことを、顧客本人に確認してもらいその記録を残す。

・ 防犯カメラによる日常の監視　等。【設 103】）

(2) 認証判定に使用された、サンプル・データとテンプレートの照合結果を記録する。

（注）「顧客による否認」・・・ここで想定している状況とは、悪意を持った顧客や勘違いをしている顧客が、その本人の口座から、生体認証にて預金の

払戻しをした後、その行為を否認して被害を訴え補償を求める場合等である。

4. 不正認証（なりすまし）等防止

(1) 生体認証情報の登録時、および日常取引における認証時に、センサー等の機器を介して取得する、「真正な顧客」のサンプル・データに関して、本人ではない者による、その

① 不正入手

② 偽造

③ 不正使用

等を防ぐ手段、運用上の措置を講ずることが必要である。

リスクと対応策の一例を以下にあげる。

・偽 ATM（偽センサー機器等）の設置による、生体認証情報のだまし取り。また、センサー部分の残存情報からの指紋等のコピー。対応策としては、防犯カメラでの監視、職員による巡回点検、利用者への注意喚起等。【設 103】

・人工的に合成してつくった偽造生体を使った不正認証（なりすまし）。対応策としては、生体検知装置での確認、職員による対面確認等。

・ホスト照合の場合には、センサーで取得した生体認証情報をホストへ送信する際にスパイウェア、フィッシングなどにより詐取され、悪用される可能性がある。対応策としては、ホストへの送信時に、暗号化や生体認証情報の読み取り日時等の情報を付加するなど、照合時にチェック可能とすることにより詐取された情報の再利用を防ぐなどが考えられる。

(2) テンプレートの不正利用を防ぐ手段、運用上の措置を講ずることが必要である。

リスクと対応策の一例を以下にあげる。

・悪意を持った内部者や、ネットワークを経由等した外部者が、「真正な顧客」のテンプレートを、不正に入手・使用して、それをサンプル・データ等に不正流用し、認証をパスする。対応策として、そもそもテンプレートは、サンプル・データに流用できない設計とする。ほかに、テンプレートとサンプル・データの類似度が極端に高い場合は、認証をパスさせない。（センサー機器等へかざす生体の位置・角度やぶれ等により、100%の一致は、認証方式によっては不自然な場合がある。）

5. テンプレート保護技術

テンプレートのデータ保護について、「取り消し可能なバイオメトリクス認証」（Cancellable biometrics）など技術動向を考慮することが望ましい。

（参考）

取り消し可能なバイオメトリクス認証とは、何らかの原因でテンプレートが流出した場合等に、以前のテンプレートを無効として新規のテンプレートを再発行できる方式である。取り消し可能なバイオメトリクス認証では、サンプル・データと変換パラメータを入力として、不可逆関数を用いて変換し、テンプレートを作成する。不可逆関数を用いて変換した場合、元のサンプル・データを復元することは不可能である。加えて、変換パラメータは必要に応じ変更可能なので、万一テンプレートの信頼性が失われた場合には、変換パラメータを変更することによりテンプレートの再発行が可能となる。

不正使用防止
予防策（アクセス権限確認）

適　用　区　分				
共	セ	本	提	ダ
◎				

実 127	ID の不正使用防止機能を設けること。

削除:　技　36

不正アクセス防止のため、システムやデータ等へのアクセスに用いる ID の不正使用防止機能を設けること。

1.　システムやデータへのアクセス権を不正使用される危険性を考慮し、不正使用を防止するための機能を組み込むことが必要である。また、暗証番号等についても、同様に不正使用を防止する機能を整備することが必要である。（暗証番号の不正使用防止策については【技 45】参照。）

2.　具体的な方法として、例えば以下のようなものがある。

(1) ログオン中のタイムアウト

システムにログオンしたまま一定時間操作が行われない ID を、強制的にログオフもしくは画面をロックする。

(2) 使用されていない ID の使用停止

一定期間システムに対してアクセスがない ID は、使用停止とする。

(3) ユーザーにログオン履歴情報を提供する

システムへのログオン時、ユーザーに以下の情報を提供する。

・前回のアクセス日付、時刻、状況

・前回ログオン以降、ログオンが連続失敗していた場合、そのアクセス状況

(4) パスワード入力失敗の回数制限

パスワードの入力を一定回数失敗した場合は、当該 ID を一時的に使用不可とする。

(5) パスワードを他人に知られないための対策を講ずる。

パスワードを他人に知られないための対策としては、【技 26】参照のこと。

(6) 総当り攻撃（ブルートフォース攻撃）への対策を講ずる。

単にパスワード入力時のリトライ制限を設けるだけでなく、認証方式の特性を分析し、総当り攻撃が可能となるリスクに対応する。例えば想定されるリスクとして、パスワードを固定しユーザーID を次々変化させてログオンを繰り返すことによるパスワードのリトライ制限の回避が考えられる。

(7) チャレンジレスポンス方式での不正使用対策を講ずる。

例えば、チャレンジレスポンス方式の乱数表の一部が流出した場合において、ログオン操作の中断・再開の回数制限が無い認証方式では、流出した情報に対応したチャレンジ値となるまで中断・再開を繰り返すことにより、不正なログオンが可能となるリスクが考えられる。上記のケースには、以下のような対策が考えられる。

・一定回数ログオン操作を中断・再開した場合、ロックする。

・ログオン操作を中断・再開した際は、チャレンジ値を変更しない。

チャレンジレスポンス方式は【技 35】参照

(8) エラーメッセージからの推測を防止する。

エラーメッセージの文面からパスワード等を推測できないようにする。

(9) ログオン後は画面に必要な場合を除き ID を表示しない。

ログオン後は画面に必要な場合を除き ID を表示しないことで、覗き見での漏洩を防止する。

(10) プログラム等に ID・パスワードを記述しない。

パスワード変更が必要な際に容易な対応ができるよう、プログラム等に ID・パスワードを直接記述しない。ID・パスワードをプログラム等で使用する場合には、別ファイルに記述し、さらに容易に閲覧されないよう、当該ファイルの参照権限を限定する等の対策を講ずることが必要である。

なお、アプリケーションの制約等により、ID・パスワードをプログラム等に直接記述する必要がある場合には、当該プログラムの参照権限を限定する等の対策を講ずることが必要である。

不正使用防止
予防策（アクセス権限確認）

適　用　区　分				
共	セ	本	提	ダ
◎				

実128	アクセス履歴を管理すること。

削除:　技　37

アクセス状況を管理するため、システムやデータへのアクセス履歴を取得し、監査証跡として必要期間保管するとともに定期的にチェックすること。

1.　アクセス履歴を取得し監査証跡として保管する必要がある。また、アクセス記録を定期的にチェックして正当なアクセスなのかどうかを調査していることを周知させることによって、不正アクセス行為を牽制することが必要である。

記録として取得する具体的な内容としては、以下のような例がある。

・ログインとログオフ状況（指示端末、時刻、ID、回線種別、使用したシステムもしくはデータ、行った処理）
・不正なアクセス要求（指示端末、時刻、ID）
・システムによって失効とされた ID
・システムにログインしたまま一定時間操作が行われないために、強制的にログオフされた ID
・特権 ID の利用履歴（成功時及び失敗時）

なお、不正アクセス対策については、以下の基準項目を参照のこと。

・本人確認機能を設けること【技 35】
・暗証番号、パスワード等は他人に知られないための対策を講ずること【技 26】

2.　監査証跡に基づいて、許可されていないアクセスの分析、報告を可能とすることが望ましい。なお、個人データを扱うシステムにおいては、この措置は必要である。

3.　監査証跡、オペレーション記録、運転記録等は、改ざんや不正アクセスを防ぐために、正当なアクセス権限者以外のものから適切に保護される必要がある。

具体的な対策としては、以下のような例がある。

・暗号化して保管する。
・書換え不能メディアに記録し、保護された場所に保管する。
・ネットワーク経由の不正アクセスや改ざんを防止するために、オフライン媒体に記録する。

4.　後日アクセス履歴を参照する場合に備え、複数システムの時刻を、基準となる時刻に同期させておくことが望ましい。

分散システムにおけるシステム間の時間の同期方法としては、NTP（Network Time Protocol）を用いる方法がある。

5.　インターネット等を利用した取引においては、他人による不正使用から利用者を守るため、利用者みずからがその使用状態（前回ログオン日時、取引履歴等）を確認できる機能を設けることが望ましい。

削除: 自ら

6.　インターネット等を利用した取引においては、他人による不正使用が発生した場合に備え、当該取引を特定できる情報をログとして取得し保存できる機能を設けることが必要である。

取得すべき情報としては、以下のようなものが考えられる。

・口座番号
・ユーザーID
・取引日時
・取引先口座
・取引金額
・取引時の IP アドレス
・取引時のポート番号
・画面遷移

なお、不正取引の特定に有用であることから、取引に失敗した際のアクセス情報（不正な取引を試みた痕跡）も、ログとして取得しておくことが必要である。

7.　CD・ATM 等を利用した取引においては、偽造・盗難カード等による不正使用が発生した場合に備え、取引情報等を記録・管理できる機能を設けることが望ましい。

当該取引を特定できる情報としては、以下のようなものが考えられる。

・取引日時
・CD・ATM 等の端末情報
・取引の種類
・口座番号
・取引金額

なお、払戻し取引や振込取引だけでなく、照会取引、暗証番号入力誤りや、偽造・盗難カードの挿入等の事象も、記録・管理することが望ましい。

（参考）
政府機関が構築するシステムにおいては 1 年以上のログ保存が推奨されている。
「平成 23 年度　政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書（1.1 版）」（内閣官房情報セキュリティセンター）平成 24 年 10 月 1 日

不正使用防止
予防策（利用範囲の制限）

適　用　区　分				
共	セ	本	提	ダ
◎				

実 129	取引制限機能を設けること。

削除:　技　38

不正アクセスを防止するため、端末等取引に使用する機器・媒体の種類、設置場所、用途等により、取引内容の制限機能を設けること。

1.　アクセス権限確認が十分に行われない場合、または不正アクセスの危険性が高いと認められる場合には、端末等取引に使用する機器・媒体の種類、設置場所、用途等により、取引や業務内容の制限機能を設けること。なお、取引制限機能を設ける際には、取引や業務内容の特徴を勘案したうえで、顧客保護の視点からの検討も行うことが望ましい。

2.　CD・ATM、インターネットバンキングによる引出金額及び振込金額については限度額を設けることが必要である。

１日あたりの限度額及び一定期間の限度額を、顧客の希望により変更できる仕組みを導入することが望ましい。

なお、上記変更のうち、限度額の引上げについては当該チャネル以外で実施できることが望ましい。

（参考）

１日あたりの限度額を制限する機能を導入するにあたり、システム対応に一定の時間を要する場合には、限度額が無制限であることに伴うリスクを顧客に対して説明する等、必要な措置をとること。

限度額を引き上げる場合は、窓口等での本人確認を実施すること。また、限度額を引き下げる場合は、その分窓口における取引量が増加し待ち時間も増加する可能性があること等、顧客対応には十分に配慮すること。

3.　取引・業務内容の制限要因として、例えば以下のようなものがある。

(1) 端末の種類によって業務を制限する。

・開発用端末
・窓口端末
・CD・ATM
・渉外端末

(2) 端末の設置場所によって取引を制限する。

・CD・ATM

・渉外端末
・顧客・企業設置端末

4. 取引制限の内容として、例えば以下のようなものがある。
・取引金額を制限する。
・電子的価値の蓄積可能額を制限する。
・サービス内容を照会業務に限定する。
・資金移動取引において、振込先を限定する。
・顧客が振込指示をしてから実際に処理されるまでの間を一定時間空ける。
・インターネットバンキングにおいては、資金移動先としての事前登録先口座の追加や変更の指示をしてから処理されるまでの間を一定時間空ける。また、事前登録先口座の追加や変更については、インターネットバンキング以外の郵送や窓口等で実施することも考えられる。
・パスワード入力失敗回数の制限と監視が実施されていない場合、パスワード入力失敗時の再入力不可時間を確保する。

5. 取引制限機能を設ける際には、当該取引やサービスの特性（取引限度額、利用頻度、利用者層等）を踏まえて決定する必要がある。

不正使用防止
予防策（利用範囲の制限）

適　用　区　分				
共	セ	本	提	ダ
◎				

実 130	事故時の取引禁止機能を設けること。

削除:　技　39

カード、通帳、印鑑等の盗難・紛失等の事故に対処するため、その口座に対する当該媒体による取引を禁止する機能を設けること。また、渉外端末の盗難・紛失等の事故に対処するため、端末ごとの取引禁止機能を設けること。

1. 取引を禁止する具体的事例として、以下のようなものがある。

カード、通帳、印鑑については当該口座の元帳に、渉外端末については当該端末の端末 ID ファイルに、事故内容に応じた注意コードまたは支払禁止コード等を登録し、盗難・紛失等に対応した取引を排除する。【運 41】

不正使用防止
予防策（不正・偽造防止対策）

適　用　区　分				
共	セ	本	提	ダ
	○	○	○	

実 131	カードの偽造防止対策のための技術的措置を講ずること。

削除:　技　40

不正使用防止のため、カードの偽造防止のための技術的措置を講ずることが望ましい。

1.　カード犯罪を防止し、カードを利用したサービスを安全に提供するため、カードの偽造防止のための技術的措置を講ずることが望ましい。

2.　カードの偽造防止対策としては、IC カード化等の高セキュリティ技術の導入がある。

磁気ストライプ付きキャッシュカードの偽造防止対策としては、偽造を判別するためのコードを磁気ストライプに記録することが必要である。なお、当該コードは、容易に推察されない仕組みとすることが望ましい。

利用者の利便性を考慮して IC と磁気ストライプを併用したカードを導入する場合、IC 単独のカードに比べ安全性が低いことに十分留意する必要がある。例えば、IC を使用した場合と磁気ストライプを使用した場合とで、利用できる取引の種類や金額を区別することが考えられる。

また、その他のカードの偽造防止対策としては、以下のようなものがある。

(1) カードへ有効期限を設定し、期限経過時に更新

(2) 顔写真、ホログラム等の券面への印刷

3.　キャッシュカードの IC カード化に当たっては、「全銀協 IC キャッシュカード標準仕様」に要求される要件を満たすこと（セキュリティや互換性など）。また、IC カードの運用面や技術面について、セキュリティ対策上、以下のような点に注意し、定期的に見直すことにより時々の技術水準を反映することが必要である。

・IC カードの有効期限（電子証明書の有効期限）
・電子証明書の認証機関の信頼性（運用規定等）
・使用される暗号の強度
・耐タンパー性

不正使用防止
予防策（不正・偽造防止対策）

適　用　区　分				
共	セ	本	提	ダ
○				

実 132	電子的価値の保護機能、または不正検知の仕組みを設けること。

削除:　技　41

電子的価値のコピー、二重使用等の不正行為に対処するため、データの保護機能を具備するか、あるいはその発生を検知できる仕組みを構築しておくことが望ましい。

1.　電子的価値を蓄積する機器、媒体あるいはそれに含まれるソフトウェアには、価値を保護する機能を具備することが望ましい。

2.　上記の機能がない場合には、改ざん、不正コピーによる二重使用等の不正行為を検出できる仕組みを用意することが望ましい。

3.　セキュリティ確保のためには、以下のような手段を組み合わせて総合的に対応する必要がある。

なお、セキュリティ技術は最新の技術の動向に留意し、その安定性、互換性、実装の容易さなどを適切に評価したうえで採用することが必要である。

- IC カード型電子マネーでの耐タンパー性のような保護機能
- IC カード等には有効期限を設定するなどの偽造抑止対策
- シリアルナンバー方式による不正検知
- 証拠センター方式による不正検知

（注）・耐タンパー性　　：こじ開けや不正アクセスなどで情報を無理に取り出そうとした場合に、その情報を消去する等で不正を防止する技術。
・シリアルナンバー方式：電子的価値の使用単位ごとに固有の識別番号を付与し、同一番号のものが二重に使用されないようにチェックする方式。
・証拠センター方式　　：付与された電子的価値の総額に対して、実際の使用額と残額とを突合して不正使用をチェックする方式。証拠センターにおいて使用額と残額とが突合されるため、事後的なチェックとなる。

不正使用防止
予防策（不正・偽造防止対策）

適　用　区　分				
共	セ	本	提	ダ
◎				

実 133	電子化された暗号鍵を蓄積する機器、媒体、またはそこに含まれるソフトウェアには、暗号鍵の保護機能を設けること。

削除:　技　42

暗号鍵が他人に知られることによる不正行為を防止するため、暗号鍵の保護機能を機器、媒体またはソフトウェアに具備すること。

1.　電子化された共通鍵、秘密鍵を蓄積する IC カード等の機器、媒体あるいはそれに含まれるソフトウェアには、共通鍵、秘密鍵を保護する機能を具備することが必要である。

　パソコン等を利用する場合においては、共通鍵、秘密鍵は別の機器および媒体に確保し、必要時にその機器、媒体を接続して使用する。

2.　共通鍵、秘密鍵をパソコン等の端末機器側に蓄積する場合は、他人に解読されないような措置を講ずることが必要である。

3.　セキュリティ確保のためには、以下のような手段を組み合わせて総合的に対応する必要がある。

　なお、セキュリティ技術は最新の技術の動向に留意し、その安定性、互換性、実装の容易さなどを適切に評価したうえで採用することが必要である。

・IC カードにおける耐タンパー性のような保護機能
・ID、パスワード等によるアクセス制限
・暗号を用いた蓄積

不正使用防止
予防策（不正・偽造防止対策）

適　用　区　分				
共	セ	本	提	ダ
○				

実 134	電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること。

削除:　技　42-1

業務目的以外の電子メールの送受信やホームページの閲覧等に対処するため、不正使用防止対策を講ずることが望ましい。

1.　業務目的以外の電子メールの送受信やホームページの閲覧等に対処するため、セキュリティポリシーと整合性がある不正使用防止対策を講ずることが望ましい。なお、個人データを扱う場合には、この措置は必要である。

2.　業務目的以外の電子メールの送受信やホームページの閲覧等としては、以下のようなものがある。

(1) 電子メールの送受信

①　業務に関係しない私的な情報の交換・連絡

②　業務上適切な範囲を逸脱した電子メールの利用（不適切なメーリングリストやメールマガジンの利用等）

③　公序良俗に反する情報の送信

(2) ホームページの閲覧

①　業務に関係しないホームページの閲覧

②　ホームページへの業務上適切な範囲を逸脱したコメントの掲載（掲示板等への公序良俗に反するコメント掲載等）

3.　業務目的以外の電子メールの送受信やホームページの閲覧等の不正使用防止対策としては、以下のようなものがある。

(1) 電子メールの送受信やホームページの閲覧が可能な利用者を適切な範囲に限定する。【運 16】

(2) メールフィルタリング等を導入し、電子メールの内容を判断し、不適切な情報の送受信を防止する。また、不適切な電子メールを送受信した利用者に対して適切な措置を行う。

(3) 社外に送信された電子メールを自動的に送信者の管理者等に転送する。

(4) コンテンツフィルタリング等を導入し、ホームページのコンテンツの内容を判断し、不適切な情報の閲覧を防止する。また、不適切なホームページを閲覧した利用者に対して適切な措置を行う。

4.　なお運用面においても、全役職員（外部要員を含む）に対するセキュリティ教育を行い、責任と義務および懲罰等について周知徹底を図ることが必要である。【運 80】

（参考）
メールフィルタリング：電子メールの内容を判断し、不適切な情報の送受信を防ぐ目的で利用されるソフトウェアであり、利用者が受信したくないメールアドレスを設定しスパムメールの着信を拒否できる機能も含めることがある。
コンテンツフィルタリング：ホームページのコンテンツの内容を判断し、不適切な情報の閲覧を防ぐ目的で利用されるソフトウェアであり、不適切なホームページを閲覧した利用者のアクセスログを取得する機能も含めることがある。

17 不正使用防止

削除: Ⅱ.安全性侵害対策 .

削除: （Ⅱ）

(4) 外部ネットワークからのアクセス制限

削除: 2.

コンピュータシステムをオープンネットワークなど外部ネットワークと接続した場合、ネットワークを介した外部からの不正侵入によるコンピュータシステムの不正使用を防止するため、外部からのアクセスを制限することが必要である。

不正使用防止
外部ネットワークからのアクセス制限

適　用　区　分				
共	セ	本	提	ダ
◎				

実 135	外部ネットワークからの不正侵入防止機能を設けること。

削除:　技　43

不正侵入を防止するため、重要なデータやプログラムを扱うシステムについては、外部ネットワーク（オープンネットワーク、リモートアクセス等）と内部ネットワークの接続部分に適切な不正侵入防止策を講ずること。

1.　ここでいう外部ネットワークとは、不特定多数の人がアクセスする可能性のあるネットワークであり、主にインターネット、公衆回線網等はこれに該当する。専用線の利用により相手接続先が特定できる場合は本項の対象外である。ただし、途中まで専用線接続し、その先で不特定多数の人がアクセスする可能性のあるネットワークとの接続を目的とした場合（例えばインターネットサービス・プロバイダーとの専用線接続）は、本項の対象とする。

2.　外部ネットワークとの接続部分より、社内のシステムへ不正侵入される危険性がある。このため、重要なデータやプログラムを扱うシステムを外部ネットワークと接続する場合は、接続部分に不正侵入防止策を講じる必要がある。

3.　不正侵入の防止策並びに検知策を検討する場合は、外部からの攻撃の予防・防御を目的とした入口対策(ファイアウォール、抗ウイルスソフトの導入等)のほか、侵入したウイルスの検知、バックドアの構築防止や機密情報の流出防止等を目的とした出口対策(通信ログ、イベントログ等の分析による、不適切な通信の検知・遮断等)があるが、具体的対策を講じる際には、これらを組み合わせた多層防御の形を取ることが有効である。

4.　外部ネットワークからの不正侵入の防止と早期発見のため、内部ネットワークへのアクセスを監視し、アクセス履歴のチェックを行うことが必要である。

　情報漏洩防止の観点から、外部への通信を検知する仕組み（プロキシ経由等）を導入することも有効である。

　また、サーバー等のセキュリティホール対策を行うことが必要である。【運 56】【技 37、技 45】

削除: システムへ

削除: システム

5.　不正侵入防止策として、例えば以下のようなものがある。

(1) ファイアウォール

　インターネットと接続する場合はファイアウォールを設置し､インターネットを介した社内ネットワークへの侵入を制限する。

(2) アクセスサーバー

ダイヤルアップによるリモートアクセスの受け口にアクセスサーバーを設置する。その際、コールバック、アクセス認証を行うことで、安全性を確保する。

(3) 非武装セグメント（DMZ: De-Militarized Zone）

ファイアウォールにより設けられた特別なセグメント上に公開サーバー(外部にホームページなどを公開しているサーバー）を設置し、社内ネットワークへの不正アクセスを防止する。非武装セグメントを設けることにより､外部ネットワークから社内ネットワークを隠蔽するとともに、詳細なアクセス制御が可能となる。非武装セグメントの構成として、図1のような例がある。

(4) その他

サービス妨害攻撃（DoS 攻撃: Denial of Service）等を早期に検知するための侵入検知システム（IDS: Intrusion Detection System）や SQL インジェクション等を検知するためのウェブアプリケーションファイアウォールなどにより Web サイト等へのアクセス要求等のトランザクション量やアクセス要求元の正当性、要求内容などを監視する。

6. ファイアウォールまたはアクセスサーバーはコンピュータ室内もしくはサーバー設置場所と同等の設備基準を満たす場所に設置することが必要である。

7. ファイアウォールまたはアクセスサーバーは最新の技術動向を踏まえ適宜評価（定期確認及びシステム変更等を実施したときの確認・評価）を行い、セキュリティ上の効果を確認するとともに、その結果に応じてメンテナンスを行うことが必要である。【技 49】

外部ネットワークと社内ネットワークの間等に、多重にファイアウォールを設置しアクセス制御を実施している場合には、外部ネットワーク側からのセキュリティ評価を行うことが必要であることに加え、制御をより確実にするため、社内ネットワーク側のファイアウォールのセキュリティ評価を行なうことが望ましい。ファイアウォールのセキュリティ評価の箇所としては図 1 のような例がある。なお、多重に設置したファイアウォールを異なる機種とすることも有効である。

ファイアウォールまたはアクセスサーバーのセキュリティ評価の手法の一例として、侵入検査（ペネトレーションテスト）がある。これは外部からの攻撃を想定して、サーバー（Web サーバー、メールサーバー等）及びネットワーク機器（ルータ、ファイアウォール等）に対しポートスキャンや擬似アタックを行うことで、脆弱性（セキュリティホール）の有無や程度を検証する手法である。

なお、最近は内部からの情報漏洩対策として、ネットワーク内部からの攻撃の検証（アクセスコントロールされている重要情報に対して、無権限者がアクセスできるようになっていないかどうか等の検証）の有効性も認識されている。

8. 外部ネットワークに接続するネットワークと、接続しないネットワークを物理的に分離することや、接続用仮想環境等による遮断措置を利用したネットワーク構成を検討することも必要である。

9. 本人確認機能等アクセス権限の確認と併せて本項の対策を行うことが重要である。【技 35】

10.　インターネットに接続する場合のセキュリティ技術は、最新のセキュリティ技術の動向に留意し、その安定性、互換性、実装の容易さなどを適切に評価したうえで採用することが必要である。

11.　Web アプリケーションの脆弱性を利用した不正侵入や不正使用の防止策の実施にあたっては、既に発見され、公表されている不正行為（侵入や組込みの手口）の事例は、防御対策、検知対策に対する有益な情報となることが多い。したがって、これらについて記載されている文献や、ガイド等を参考にすることも有用である。【運 103】（参考 3）

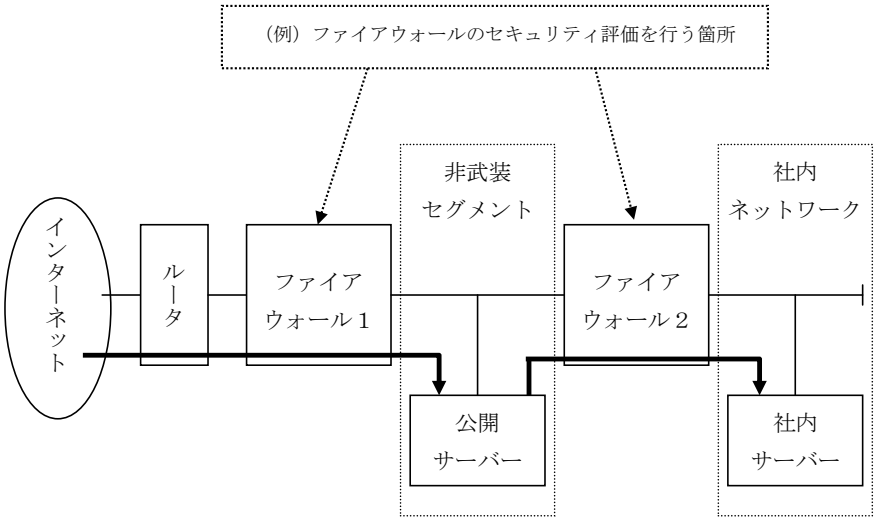


図１　非武装セグメントの構成例

（参考 1）
　各部門内にて管理するデータの機密性を維持するため、業務内容やデータの重要性に応じて、内部ネットワークにおいても部門ごとにファイアウォールを設置する等の不正侵入防止策を講じることも有効である。
　また、外部ネットワーク経由での侵入検査をはじめとした不正侵入防止策の診断をするサービスを利用することも有効である。

（参考 2）

無線 LAN 技術の不正アクセス防止対策としては、適切な方式で暗号化することが必要である。【技 29】（参考 1）

それに加え、対策としては例えば以下のようなものがある。

(1) MAC アドレスフィルタリング

無線 LAN クライアントのネットワークインタフェースが持つ MAC アドレスによってアクセスを制御する認証方式である。無線 LAN アクセスポイント側で登録された MAC アドレスを持つ機器が、無線 LAN アクセスポイントへ通信を行った場合のみ接続することができる。

(2) ESSID の ANY 接続拒否

無線 LAN アクセスポイントの設定において ESSID（Extended Service Set ID）が「ANY」や空欄の設定になっている無線 LAN クライアントを拒否する対策をいう。

(3) ESSID のステルス化

無線 LAN アクセスポイントから定期的に送信している Beacon 信号を停止する対策をいう。正規のユーザーは ESSID を無線 LAN アクセスポイントからの配信以外の手段で入手し、無線 LAN クライアントに設定する必要がある。

(4) 無線アナライザ

無線 LAN 上のデータをモニターして、そのデータの内容を解析する機器やソフトウェアをいう。この無線アナライザの定期的な利用により、使用中のすべての無線装置を識別して、認可されていない無線装置を経由した不正アクセスを検知できる。（対応策については【技 48】を参照。）

（参考 3）

標的型攻撃は絶えず高度化するため、情報（組織内外のインシデント）収集に努め、定期的に対策を見直し、上記の技術的対策のほか、組織（関係先等も含む）においても標的型メール訓練や各種教育等を定期的に実施することが望ましい。

（参照 URL）

内閣サイバーセキュリティセンター（NISC）

http://www.nisc.go.jp/

独立行政法人情報処理推進機構（IPA）

http://www.ipa.go.jp/

（参考４）

サイバー攻撃対応態勢の整備のため、組織内 CSIRT（Computer Security Incident Response Team）を整備することは、迅速かつ適切な対応や、収集した情報の一元化による早期警戒体制の構築、及び関係者間での情報共有に有効と考えられる。

なお、CSIRT には、さまざまな形態が考えられ、必ずしも常設であることは必要ではなく、専属の人員を置くことや、「CSIRT」という名称を名乗ることが必須というわけではない。また、CSIRT 設置後も、インシデント対応の全てを組織内で行うことが求められているわけではなく、CSIRT を窓口として外部に支援を要請することも考えられる。金融機関は、その規模や組織態勢に即して、最適な CSIRT の形態や機能を選択することが適切である。

（参照 URL）

一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
http://www.jpcert.or.jp/

日本コンピュータセキュリティインシデント対応チーム協議会（日本シーサート協議会）
http://www.nca.gr.jp/

参照法令	不正アクセス行為の禁止等に関する法律　第２条～第５条

不正使用防止
外部ネットワークからのアクセス制限

適　用　区　分				
共	セ	本	提	ダ
◎				

実 136	外部ネットワークからアクセス可能な接続機器は必要最小限にすること。

削除:　技　44

不正アクセスによるコンピュータシステムへの侵入を防ぐため、外部からアクセス可能な通信経路、通信関連機器等は最小限とし、不必要な機器は接続しないこと。

1. 外部ネットワークからのアクセス経路は、不正アクセスを防止するため、必要最小限にすることが必要である。これにより、侵入された経路の特定や、管理および監視がしやすくなる。
   アクセス経路を必要最小限にする例には、以下のようなものがある。
   (1) 長期にわたって使用しない機器（コンピュータ、回線終端装置等）のネットワークからの切断
   不正使用を防止したり、システム上の障害防止のため、ネットワークから物理的に切断する、または機器の電源を切る。
   (2) 使用しないポートを塞ぐ
   使用しないポートは、外部からの不正アクセスの脅威にさらされやすいためポートを塞ぐ。

2. 外部ネットワークと接続するコンピュータは、セキュリティを考慮した設定とする。
   セキュリティを考慮した設定にする例には、以下のようなものがある。
   (1) 基本ソフトウェアの提供する機能の選択
   基本ソフトウェアのセキュリティホールを最小限にするため、基本ソフトウェアが提供する機能（telnet, ftp, finger 等）のうち、使用しない機能は停止、あるいは使用を制限する。
   (2) 搭載ソフトウェアの制限
   ソフトウェアには、セキュリティホールが発見される可能性があるため、外部ネットワークと接続するコンピュータに、使用予定のないソフトウェアは搭載しない。

17 不正使用防止

削除: Ⅱ.安全性侵害対策 .

削除: （Ⅱ）

(5) 検知策

削除: 3.

不正アクセスを早期に発見するため、不正アクセスを監視する機能や異例取引を監視する機能を設けることが必要である。

また、不正取引による被害発生の防止等のため、不正取引を検知する機能を設けることが望ましい。

不正使用防止
検知策

適　用　区　分				
共	セ	本	提	ダ
◎				

実 137	不正アクセスの監視機能を設けること。

削除:　技　45

不正アクセスを早期に発見するため、アクセスの失敗や不正アクセスを監視する機能を設けること。

1.　アクセスの失敗を監視する機能として、以下のものを設けること。
・アクセスの失敗を記録する機能を設けること。
・連続した何回かのアクセスの失敗に対しては、強制終了・取引禁止等を行う機能を設けること。

2.　不正アクセスの監視機能の使用例として、以下のようなものがある。
(1) パソコン、電話等を利用した資金移動取引、残高照会取引等については、パスワードが規定回数誤入力された場合、その時点で自動的に取引を禁止する。
(2) CD・ATM 等自動機器やデビットカード端末を利用したカード取引においては、暗証番号が規定回数誤入力された場合、以後のカード取引を禁止する。
(3) 偽造を判別するためのコードにより異常を検知した場合は、取引停止等の措置を講ずる。
(4) 遠隔診断システムを導入している場合、社外に設置されている遠隔診断用の端末からのアクセスは、必要時以外禁止する。また、アクセスが必要な時は都度許可を行い、さらに不正アクセスの有無をチェックするため、アクセス履歴を記録する。
(5) 他人が不正にアクセスしたかを利用者が確認できるために、表示器等に、前回アクセス日時を表示する。
(6) 不正アクセス等の異常を検知した場合には、セキュリティ管理者など、あらかじめ定められた者に自動的に通知する。
(7) Web サイトを外部に公開している場合は、侵入検知システム（IDS: Intrusion Detection System）や専用ソフトウェア等により、改ざんやサービス妨害攻撃（DoS 攻撃: Denial of Service）等の不正アクセスを自動監視または早期に検知する。

不正使用防止
検知策

適　用　区　分				
共	セ	本	提	ダ
◎				

実 138	異常な取引状況を把握するための機能を設けること。

削除:　技　46

不正取引による被害発生の防止等のため、異常な取引状況を早期に把握するための機能を検討し実施すること。

1.　ATM 等による取引が正当な権限を有する者に対して適切に行われることを確保するため、異常な取引状況を早期に把握するための機能をできるだけ速やかに整備すること。【運 44-1】

不正取引によるマネーロンダリング防止のため、異常な取引状況を把握するための機能を設けることが望ましい。

2.　異常な取引状況を把握するための機能の例としては以下のものがある。

(1) カードの異常取引

・顧客の一般的な取引パターンから逸脱した取引を検知する。

・資金移動を伴う取引について顧客があらかじめ登録したあて先に通知する。

・偽造を判別するためのコードの相違をリアルタイムで検知する。

払戻しだけでなく照会取引でもコード相違を検知する、また、カード取引を停止したり、警察への通報と連動することも考えられる。

(2) マネーロンダリングの疑いのある取引

・短期間のうちに頻繁に行われる取引で、現金または小切手による入出金の総額が多額であるケースを検知する。

（参考）

マネーロンダリングの疑いのある取引については、JAFIC（Japan Financial Intelligence Center）のホームページから疑わしい取引の参考事例を参照のこと。

http://www.npa.go.jp/sosikihanzai/jafic/index.htm

JAFIC とは、マネーロンダリングに対処するため、犯罪に起因すると疑われる取引情報や、疑わしい資金の動きを取り扱った金融機関等からの通報を国内で一元的に受理、分析し、捜査機関等に情報を提供する責任を有する国の機関。

3.　オープンネットワークを利用した金融サービスにおいても異常な取引状況を把握するための機能を設けることが望ましい。

異常な取引状況を把握するための機能としては、以下のようなものが考えられる。

・顧客の一般的な取引パターンから逸脱した取引などの検知
・前回の取引日時をログオン時に表示する
・送金等の取引や重要な登録事項の変更の発生時に顧客に通知する
・過去の取引履歴について顧客から参照可能とする
・資金移動に必要なパスワード入力失敗時等、不正な取引が未遂に終わったと考えられる場合に顧客に通知する

参照法令	犯罪による収益の移転防止に関する法律

不正使用防止
検知策

適　用　区　分				
共	セ	本	提	ダ
◎				

実 139	異例取引の監視機能を設けること。

削除:　技　47．

不正アクセスを早期に発見するため、異例取引の監視機能を設けること。

1.　事故届の解除、通帳・証書の再発行、暗証番号照会等の異例な取引については、役席カードを使用するとともに、その使用記録を確認させる機能を設ける必要がある。
　使用記録の確認方法の例として、以下のようなものがある。
(1) 還元帳票による方法
(2) オンライン照会による方法
(3) モニター専用（指定）端末による方法

　役席カードは端末機の操作にあたり役席操作権限者であることを確認するためのものであり、ここでは役席キー、ID 等を含むものとする。

2.　特定口座への取引を端末番号も含めて監視する機能として、特定口座にアクセスがあった場合、直ちに端末番号等を出力できる機能を設けることが必要である。

3.　顧客端末、企業端末、外部センター等からの異例取引について取引規制機能を設けること。

17 不正使用防止

削除: Ⅱ.安全性侵害対策 .

削除: （Ⅱ）

(6) 対応策

削除: 4.

不正アクセス、不正使用を検知した場合は、迅速に被害の範囲を調査・特定し被害の拡大を防止するとともに、システムの復旧を行う必要があり、そのための対応策を講じておくことが望ましい。また、被害状況、原因を調査・分析し、再発防止策を講じておくことが必要である。

不正使用防止
対応策

適　用　区　分				
共	セ	本	提	ダ
◎				

実 140	不正アクセスの発生に備えて対応策、復旧策を講じておくこと。

削除:　技　48

不正アクセスを検知した場合に備えて、不正アクセスの拡大防止のための対応策、復旧手順を明確にしておくことが望ましい。不正アクセスを検知した場合、その被害の有無にかかわらず、不正アクセスの拡大防止策、復旧策を講ずること。また、不正アクセスの原因を分析後、再発防止策を講ずること。

1.　不正アクセスの拡大防止のための対応策、復旧策を明確にしておくことが必要である。対応策、復旧策においては以下の対応が必要である。

なお、対応にあたっては、関係者との協力のもとに進めることが必要である。

(1) 不正アクセスの拡大防止

不正アクセスは多くの場合、一つの機器・経路に侵入後、その機器・経路を経由してその周辺に不正アクセスの範囲を拡大してゆく。不正アクセスを検知した場合の対応としては、例えば以下のようなものがある。

①　侵入されたシステムの緊急停止を行う。

②　侵入経路であるネットワークとの接続を切断する。

(2) 不正アクセス被害に対する復旧

①　不正アクセスによる被害に対する復旧のために事前に復旧手順を明確にしておくことが必要である。

事前に復旧手順を明確化すべき事例としては以下のようなものがある。

a.　サービス妨害攻撃（DoS 攻撃）により通信不能となった場合

b.　サーバーの特権的アクセス権（ルート権限等）が奪われた場合

c.　サーバーが不正な処理を開始した場合

d.　サーバーへの侵入の痕跡を発見した場合

e.　サーバーが通信不能となった場合

f.　ホームページの改ざんが発見された場合

事前に作成した復旧策で対応できない事象の場合は、関係者の協力のもとで復旧策を検討すること。

②　また、ファイル等が破壊された場合の復旧のために、データ・ファイル、プログラム・ファイル等のバックアップを確保しておく必要がある。

復旧の対応としては、例えば以下のようなものがある。

a.　消去または破壊されたファイルを復旧する。

b.　侵入された機器を含む周辺機器のアクセス履歴を調べ、他のシステムに不正アクセスの範囲が及んでいないことを確認する。

c.　不正なプログラムが潜伏していないことを確認する。

なお、復旧作業にあたっては、不正アクセスの原因究明・分析のために必要と思われるデータを取得しておくことが望ましい。

2.　不正アクセスの再発防止のためには以下のような対応が必要である。

(1) 侵入経路、侵入時刻、被害範囲等の状況を把握する。

(2) 原因究明・分析を行う。

(3) 究明された原因に対する再発防止のための対策を講ずる。

再発防止策としては、例えば以下のようなものがある。

・アクセス制限を強化する。

・不正アクセスに使用された ID および他の ID のパスワードを変更する。

・システムにセキュリティホールがあった場合、それに対する対応策を講ずる。

18 不正プログラム防止

削除: Ⅱ.安全性侵害対策 .

削除: （Ⅲ）

システムの安全性の侵害対策を講じるにあたって、不正プログラムのシステムへの侵入や組込みを防止することが重要である。

(1) 防御策

削除: 1 .

コンピュータシステムへの不正プログラムの侵入や組込みによる機密情報（パスワード、重要ファイルの内容等）の漏洩やシステムの破壊（ファイルの破壊やシステム機能の停止等）、および故意による安全性侵害に対してその対策を総合的に講じる必要がある。

不正プログラム防止
防御策

適　用　区　分				
共	セ	本	提	ダ
◎				

実 141	コンピュータウイルス等不正プログラムへの防御対策を講ずること。

削除:　技　49

開発、保守、運用時におけるコンピュータウイルス等不正プログラムによる被害を防ぐため、防御対策を講ずること。

1.　不正プログラムからシステムを守るため、コンピュータウイルスの侵入や、不正アクセスによるプログラムの改ざんを防止する対策を講ずることが必要である。

　また、システムに不正プログラムが組み込まれないよう、プログラム（自機関開発プログラム、外部開発委託プログラム、パッケージプログラム及びダウンロードプログラム等を含む）をシステムに組み込む場合には、事前に十分な検証を行うことが必要である。

2.　コンピュータウイルス侵入、プログラム改ざん及び不正プログラム組込みの手段としては、以下の例がある。

(1) コンピュータウイルスの侵入
- 電子メールの添付ファイルから侵入
- インターネットのダウンロードプログラムから侵入
- パッケージプログラムから侵入
- 可搬型記録媒体等の媒体から侵入
- 故障通知や保守要求、リモートメンテナンス等、メンテナンス時に利用するネットワークの接続先からの侵入【技 43】

(2) 不正アクセスによるプログラムの改ざん
- トロイの木馬を使った改ざん
- アクセス権限チェック機能のバイパス処理による改ざん
- システムのテスト機能等を無権限利用した改ざん
- ロギングデータから ID やパスワード等を取得して改ざん
- OS 等のセキュリティホールを突いた改ざん
- 端末等のシステムのテスト機能等を利用した組込み
- システムデモや研修用 ID を利用した組込み
- Web アプリケーションの脆弱性を利用した改ざん

(3) 不正プログラムの組込み
- 取引プログラムへの不正処理の組込み
- 端末パソコン等に搭載するプログラム改ざんによる組込み
- パソコン等のシステム立上げプログラム改ざんによる組込み

3.　防御策としては、以下のようなものがある。

(1) コンピュータウイルスの侵入

①　抗ウイルスソフト（ワクチンソフト）の導入

抗ウイルスソフトは、端末・サーバーへの導入のほか、外部ネットワークと内部ネットワークを接続するゲートウェイ等に導入し、データ送受信の都度チェックする仕組みとすることが望ましい。

抗ウイルスソフトを有効とするには、最新のウイルスパターンファイルを利用することが必要であり、そのための仕組みを構築することが望ましい。

②　ファイル管理の実施

出所が不明のプログラムは導入しない、ダウンロードしたファイルや電子メールの添付ファイル等は必ずウイルスチェックを行う、オリジナルプログラムにはライトプロテクトをかける等の対策が必要である。

(2) 不正アクセスによるプログラムの改ざん

①　アクセス管理の実施

ファイルに対するアクセス制御機能を設けること。【技 31】

本人確認機能を設けること。【技 35】

ID の不正使用防止機能を設けること。【技 36】

②　不正侵入防止機能の導入

外部ネットワークからの不正侵入防止機能を設けること。【技 43】

③　不正アクセスの要因除去

・ID、パスワード等の漏洩防止

暗証番号、パスワード等が他人に知られないための対策を講ずること。【技 26】

蓄積データの漏洩防止策を講ずること。【技 28】

伝送データの漏洩防止策を講ずること。【技 29】

・OS 等のセキュリティホールへの対応

・Web アプリケーションの脆弱性への対応

Web アプリケーションの脆弱性に関する監査（評価）を、定期的あるいはシステム変更時に実施することが効果的である。

(3) 不正プログラムの組込み

開発の各段階において、十分な検証を行い、システムに不正プログラムを組み込ませないことが必要である。

・必要となるセキュリティ機能を取り込むこと。【技 8】

・設計段階でのソフトウェアの品質を確保すること。【技 9】

・プログラム作成段階での品質を確保すること。【技 10】

・テスト段階でのソフトウェアの品質を確保すること。【技 11】

・パッケージ導入にあたり、ソフトウェアの品質を確保すること。【技 13】

特に外部に配布するアプリケーションにおいては、以下のような対策も有効である。

・アプリケーションを難読化すること。

・出荷時に電子署名等を付与し、出荷後の改ざんを防止すること。

4. OS 等のセキュリティホールや Web アプリケーションの脆弱性に関する最新情報を常に把握することが望ましい。

（参考 1）

コンピュータウイルスとは、『コンピュータウイルス対策基準』（平成 12 年通商産業省告示第 952 号）（最終改定）で「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラム」であり、「自己伝染機能」、「潜伏機能」、「発病機能」のうち「1 つ以上有するもの」と定義されている。すなわち正常なプログラムファイルやデータファイルに寄生して、自分自身を勝手に他のシステムに複写することにより増殖し、ある時突然に、データを破壊する、正常なプログラムに悪影響を及ぼす、フロッピーディスクやハードディスクを読めなくする、入力したものとは違う命令を実行するプログラムのことである。

インターネットを利用したサービスの進展により、コンピュータウイルスの脅威は増大しており、コンピュータウイルスは、ネットワークやフロッピーディスク等の媒体を介して容易にシステムに「侵入」したり「組込」まれたりして、不正処理を行うことができる状況にある。特に電子メールの添付ファイルからコンピュータウイルスに感染する事例があり、その被害も感染したパソコンのみならずネットワークで接続されているサーバー上のファイルを削除する等、悪質化している。また、電子メールのアドレス帳に登録されているすべてのメールアドレス宛に、コンピュータウイルスを埋め込んだメールを送信するようなワーム（Worm）型と呼ばれる感染力が強いタイプもあり、電子メールを通じたコンピュータウイルスの感染防止には特に注意が必要である。

コンピュータウイルス対策の例は表 1 のとおりである。最も重要なことはコンピュータウイルスをパソコンに入り込ませないことである。システム利用者に対しては、感染防止が第一であることを理解させ、感染したことを知らないまま他人にファイルを渡すなどして被害者が新たな加害者にならないよう、教育を行っていくことが必要である。

（表1）コンピュータウイルス対策の例

感染防止	・ソフトウェアは販売者または配付責任者の連絡先及び更新情報が明確なものを入手する（出所不明のソフトウェア、インターネット等を利用して信頼性の低いソフトウェアを勝手に導入したり、不用意に実行しない）。 ・オリジナルプログラムはライトプロテクト措置、バックアップの確保等安全な方法で保管する。 ・予防、検査の機能を持つ抗ウイルスソフト（ワクチンソフト）を導入し外部より入手したファイル及び媒体は、必ず検査する。 なお、抗ウイルスソフトで使用するウイルスパターンファイルは定期的に更新し、最新のものを利用することが重要である。 ・不正アクセスによる感染を防止するためのアクセス管理を行う。 ・電子メールの添付ファイルは、ウイルスチェック後に開く。
データ等の保護	・被害に備えるため、ファイルのバックアップを定期的に行い、一定期間保管する。 ・被害に備えるため、システムに導入した全ソフトウェアの構成情報を保存する。
感染の検査	・感染を早期に発見するため、最新の抗ウイルスソフトの利用等によりコンピュータウイルスを常時監視する。 ・電子メールで添付ファイルを送信する前に、添付ファイルのウイルスチェックを行う。 ・マクロ機能を有するファイルに対してもウイルスチェックを必ず行う。
感染が発見された場合の処置	・直ちに感染したシステムの使用を中止する。 ・被害状況を記録し、感染経路及び影響範囲を調べ関係先に連絡する。 ・被害を「独立行政法人　情報処理推進機構（IPA）」に届け出る。 ・駆除及びシステム復旧を行う。 ・再発防止対策を講じる。

（参考 2）

フィッシングとは、金融機関等からのメールを装い、メールの受信者に偽のホームページにアクセスするよう仕向け、そのページにおいて個人の金融情報（クレジットカード番号、ID、パスワード等）を入力させるなどして、個人情報を不正に入手する詐欺的な行為である。

phishing は、手の込んだ（sophisticated）手法により個人情報を釣り上げる（fishing）ことから作られた造語とも言われている。

ファーミングとは、hosts ファイルや DNS 情報の書き換え（DNS ID スプーフィングや DNS キャッシュポイズニング）などにより、インターネットの利用者を偽サイトへ誘導するオンライン詐欺の一種。広義のファーミングには、キーロガーなどを使って個人情報を収集し、悪用するオンライン詐欺行為も含まれる。フィッシングとは異なり、偽メールを大量送信したり、偽の URL をクリックさせる必要がない（ユーザーが正規の URL を入力しても偽サイトへ誘導されてしまう）。Pharming は、farming（農業）をもじったもの。

フィッシングの現状及びISPによるフィッシング対策の方向性（総務省総合通信基盤局電気通信事業部消費者行政課）平成17年8月10日

1. フィッシング対策としては、以下のようなものがある。

(1) Webサーバーでの対策

利用者がアクセスしているサイトが真正なサイトであることを確認できるような措置を講じること、及びフィッシングにつながる重要情報を保護するために機密性を維持すること。

① EV SSLサーバー証明書を取得し、証明書に記載の組織名にはサイト運営者である金融機関等の名称を示す。

② Webサイトの URLにはサイト運営者である金融機関等が所有するドメイン名を使用する。

③ ID・パスワードや個人情報等の情報を入力させる際には、SSL を使用した画面（「https://」で始まる画面）とする。

④ 重要な告知の掲載や連絡先を掲示する画面は、SSLを使用した画面とする。

⑤ ポップアップウィンドウを使用しない。アドレスバーやステータスバーを隠さない。右クリック機能を無効化しない。

(2) メールでの対策（金融機関等における考慮点）

① メールには電子署名を付与する。

② メールの差出人のメールアドレスは、運営者である金融機関等が所有するドメイン名のメールアドレスとする。

③ 差出人のメールアドレスに使用するドメイン名は、Webサーバーのドメイン名と同じものとすることが望ましい。

④ メールにURLを記載しない。やむを得ずメールにURLを記載する場合は、運営者である金融機関等が所有するドメイン名のURLのみを記載する。

⑤ HTML形式のメールをできるだけ使用しない。

⑥ メールサーバーを送信ドメイン認証に対応させる。

⑦ 顧客にメールを送信する契機を事前に周知しておく。

(3) ドメイン名についての対策

① Webサーバーの URLやメールアドレスで使用するドメイン名や用途を顧客に周知する。

② ドメイン名の悪用を防ぐため、類似性の高いドメイン名を事前に保有しておく。

2. フィッシング対策の参考文献として、以下のものがある。

(1)「安全なWebサイト利用の鉄則」
独立行政法人産業技術総合研究所情報セキュリティ研究センター

(2)「フィッシング対策ガイドライン」フィッシング対策協議会

3. DNSキャッシュポイズニングの対策

DNSキャッシュポイズニングの新たな手法が平成20年7月に発見・公開され、重大な脅威となっている。DNS キャッシュポイズニングへの有効な対処としては、DNSSEC（DNS Security Extension：DNSセキュリティ拡張）の導入がある。

（参考 3）

1.　スパイウェアとは、定義として明確なものは存在しないが、各種定義の共通的なものとして、以下が挙げられる。

・利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム等。（独立行政法人情報処理推進機構（IPA）と日本ネットワークセキュリティ協会（JNSA）スパイウェア対策啓発 WG による共同の定義）

2.　スパイウェアを構成する機能として、以下のものがある。

(1) キー入力情報を記録する機能（キーロガー）
(2) マウスの操作情報を記録する機能（マウスロガー）
(3) 端末画面を記録する機能（画面キャプチャ）
(4) 端末のファイル等を取得する機能
(5) 上記により収集した情報のファイル保存や外部へ送信する機能

独立行政法人情報処理推進機構（IPA）セキュリティセンター
http://www.ipa.go.jp/security/index.html
日本ネットワークセキュリティ協会（JNSA）スパイウェア対策啓発 WG
http://www.jnsa.org/spyware/index.html

参照法令	・不正アクセス行為の禁止等に関する法律 ・情報処理の高度化等に対処するための刑法等の一部を改正する法律

18 不正プログラム防止

削除: Ⅱ.安全性侵害対策 .

削除: （Ⅲ）

(2) 検知策

削除: 2.

コンピュータウイルスや不正プログラムの侵入を検知し、ユーザーおよびシステム管理者が適切に対応できることが必要である。

不正プログラム防止
検知策

適　用　区　分				
共	セ	本	提	ダ
◎				

実 142	コンピュータウイルス等不正プログラムの検知対策を講ずること。

削除:　技　50

システムの信頼性を確保・維持するため、コンピュータウイルス等の不正プログラムの侵入や組込みの有無を検証する検知対策を講ずること。

1.　コンピュータシステムに対する不正行為（不正アクセス、不正プログラムの侵入や組込み等）に対する防御策を講じていても技術の進展やサービス環境の変化、システムの拡張や変更等により、防御対策を乗り越えシステムに不正プログラム等が侵入してしまうことが想定される。

ソフトウェアの信頼性を確保・維持するうえからもこれら不正プログラムの検知策や、その他システムの正当性を検証する対策を講ずることが必要である。

不正プログラム等に対する検知は、1 つの技術やソフトウェアによってカバーできるものではなく、対象とするプログラムや機器構成、利用している OS 等により個別の対策が必要とされるが、それぞれの対応策をとるに際して、既に発見され、公表されている不正行為（侵入や組込みの手口）の事例は、防御対策、検知対策に対する有益な情報となることが多い。したがって、これらについて記載されている文献や、ガイド等を参考にすることも有用である。

2.　検知対策としては、以下のようなものがある。

(1) 抗ウイルスソフト等による検知

・コンピュータウイルスやスパイウェアに対しては、スパイウェア検知機能を盛り込んだ抗ウイルスソフト（ワクチンソフト）や、スパイウェア対策ソフトにて検知する。

また、抗ウイルスソフト等の使用にあたっては、最新のパターンファイルを利用することが必要である。

なお、現時点ではスパイウェアの定義が確定していないことから、個別の抗ウイルスソフト等ごとに検知対象とするスパイウェアが異なる場合があるので、利用の際は注意すること。

(2) アクセス履歴による検知

・システムの運転状況を監視したり、稼働履歴内容の分析を行うことにより、運転状況の異常やどこから重要ファイルへのアクセスがあったか、パスワードエラーの内容、回数等により、不正行為を検知する。

－アクセス履歴を管理すること。【技 37】

(3) 資源管理による検知

・システム資源（ファイル容量やメモリ容量、CPU 使用時間等）の使用状態をチェックし異常や特異な傾向を検知することにより、不正処理プログラムの侵入や組込みを検知する。

(4) ライブラリ管理などによる検知

・ファイル更新履歴を管理することにより、不正更新や不正プログラムの追加を検知する。

・オリジナルライブラリファイル（パソコン等で開発したプログラムや購入したプログラム原本ファイル）と運用中のファイルとを比較し不正プログラムの侵入や組込みを検知する。

・ドキュメント生成支援ツール等を利用し、目視により不正ロジックを検知する。

18 不正プログラム防止

削除: Ⅱ.安全性侵害対策 .

削除: （Ⅲ）

(3) 復旧策

削除: 3.

コンピュータウイルス被害から復旧する手順を整備するとともに、再発防止対策を講じることが必要である。

不正プログラム防止
復旧策

適　用　区　分				
共	セ	本	提	ダ
◎				

実 143	コンピュータウイルス等不正プログラムによる被害時対策を講ずること。

削除:　技　51

コンピュータウイルス等の不正プログラムによる被害を最小限にするため、発見時からシステム復旧までの対策を講ずること。

1.　コンピュータウイルスの感染が検知されたり発病した場合、あるいは不正プログラムが発見された場合に備えた対策を講ずることが必要である。

詳細内容については、当センター発刊の『金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書』を参照のこと。

削除: 当該システムやネットワークではすべての処理を停止させ、利用者個人の判断や方法によるのではなく、あらかじめ定められた手順に従って復旧させることが必要である。

2.　コンピュータウイルスの感染が発見されたり、発病した場合の対応手順としては、以下のような例がある。

(1) 感染したシステム（あるいは端末装置やパソコン）の切離し
(2) 関係先への連絡
(3) 感染の疑いのある他のシステムの検査
(4) コンピュータウイルスの駆除
(5) プログラムの再インストール（必要に応じて）
(6) バックアップデータの再ロード（必要に応じて）
(7) 当該システムのコンピュータウイルスの再検査
(8) 再発防止策の実施
(9) 当該システム（あるいは端末装置やパソコン）の再接続

3.　その他の不正プログラムによる被害発生の場合も、上記に準じて行うことが必要である。

1　システム監査

削除: （Ⅸ）システム

(1)　システム監査

削除: 1．

　コンピュータシステムの開発・変更、運用等においては、コンピュータシステムの有効性、効率性、信頼性、遵守性、及び安全性を確保するため、システム監査体制を整備することが必要である。

削除: およ

システム監査
システム監査

適　用　区　分				
共	セ	本	提	ダ
◎				

監1	システム監査体制を整備すること。

コンピュータシステム及びその管理について、有効性、効率性、信頼性、遵守性、及び安全性の面から把握、評価するため、システム監査体制を整備すること。

1. コンピュータシステムの運用、システム開発・変更等においては、コンピュータシステムの有効性、効率性、信頼性、遵守性、及び安全性を確保するため、コンピュータ部門から独立したシステム監査人がシステムの総合的な監査・評価を行い、経営層に監査結果を報告する必要がある。

   なお、被監査部門としては、コンピュータシステムに関して、その開発及び運用を担当する部門が該当するが、本部各部門や営業店などの利用部門、EUC（エンドユーザーコンピューティング）実施部門等においてもシステム監査もしくはそれに準じた監査を受けることが望ましい。特に、個人データを取り扱う情報システムの利用及び個人データへのアクセスの監視状況については、システム監査もしくはそれに準じた監査を受けることが必要である。

2. システム監査の実施手段の 1 つとして、内部者による監査に加え、外部の専門機関を活用することが望ましい。特に機微（センシティブ）情報を取り扱う場合は、外部の専門機関を活用することが望ましい。なお、機微（センシティブ）情報に該当する生体認証情報を取り扱う場合は、より客観性が求められることから、外部の専門機関を活用することが必要である。

3. システム監査実施結果による指摘事項については、システム監査部門と被監査部門の間で、事実確認、及び十分な意見交換を行い、問題があると認められた点について適切な改善を行うことが必要である。

4. システム監査を実施するにあたっては、当センター発刊の「金融機関等のシステム監査指針」、及び金融庁告示の「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」等を参照のこと。

5. システム監査人として、コンピュータシステムに精通した人材を確保する必要がある。

6. 外部委託先の監査の方法としては、以下のようなものがある。

(1) 委託元が委託先の監査を行う。

   なお、共同センター等委託元が複数の場合は、複数の委託元が共同で監査を行い個別の監査を代替することも可能である。

削除: 運　91
削除: およ
削除: およ
削除: およ
削除: およ
削除: およ
削除: およ

(2) 委託先の内部監査部門、または委託先みずからが依頼する外部の第三者による監査を受け、監査結果を委託元に報告する。

なお、共同センター等委託元が複数の場合は、監査結果を複数の委託元に報告することも可能である。

削除: 自ら