平成 29 年 11 月 21 日
公益財団法人 金融情報システムセンター

第 59 回　安全対策専門委員会　議事次第

Ⅰ　日時

平成 29 年 11 月 21 日（火）　15:00～17:00

Ⅱ　場所

FISC 会議室

Ⅲ　議事次第

１．　15:00　開会
２．　15:10　【議案１】外部委託基準改訂の検討結果について
３．　15:30　【議案２】基礎基準及び付加基準の対応・方針について
４．　15:50　【議案３】安全対策基準改訂原案（全編）について
５．　16:20　【議案４】会員意見募集について
６．　16:50　事務連絡（次回開催予定など）
７．　17:00　閉会

Ⅳ　資料

【資料１－１】　外部委託基準改訂の検討結果について
【資料１－２】　外部委託関連基準に対する各委員からのご意見・対応方針
【資料１－３】　改訂原案（外部委託関連）
【資料２－１】　基礎基準及び付加基準の対応・方針について
【資料３－１】　安全対策基準改訂原案（全編）について
【資料３－２】　前説に対する各委員からのご意見・対応方針
【資料３－３】　読みやすさ対応に対する各委員からのご意見・対応方針
【資料４－１】　平成 29 年度『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』改訂原案に対する FISC 会員企業への意見募集実施について
【資料４－２】　安全対策基準（第９版）の改訂概要
【資料４－３】　改訂原案（全編）
【資料４－４】　『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』改訂原案に関するよくあるご質問（FAQ）

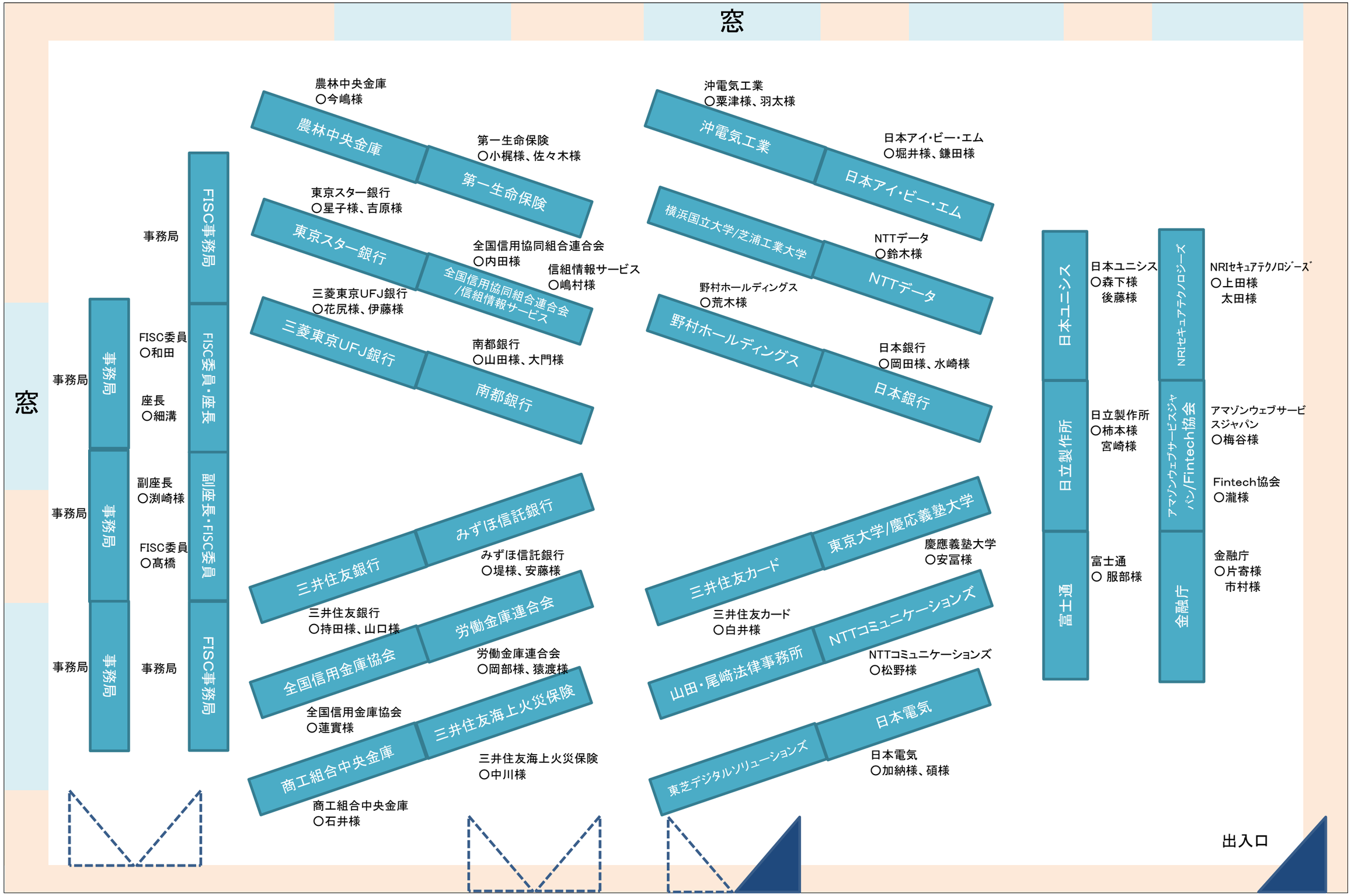
Ⅴ　今後の予定

○第 61 回　安全対策専門委員会　（※第 60 回は IT 人材のみとし、1 月に開催する予定）
（予定）平成 30 年 2 月 23 日（金）15:00～17:00　FISC 会議室

以上

第59回「安全対策専門委員会」座席表

平成29年11月21日



【資料１－１】
平成 29 年 11 月 21 日
公益財団法人 金融情報システムセンター

外部委託基準改訂の検討結果について

○ 前回ご提示した論点４（クラウド固有の管理策に関する基準の位置付け）について、各委員との意見交換を行った。

○ 意見交換の内容を踏まえ、事務局にて検討した結果、外部の統制に関する基準はすべて「基礎基準」と位置付けたうえで、クラウド固有の管理策に関する基準については、FinTech 有識者検討会の提言を反映する形で原案を修正することとした。

○ なお、その他基準を含め、いただいたご意見については【資料１－２】外部委託関連基準に対する各委員からのご意見・対応方針に一覧として掲載した。

上記の結果、論点４については以下のとおり対応している（基準再編後の番号を記載）。

論点４ （再掲）	クラウド固有の管理策とした基準【統 24】について、「基礎基準」・「付加基準」のいずれに整理するのが適当か。
主なご意見	・外部の統制に関する基準はすべて「基礎基準」に位置づけるべきであり、クラウドサービスを利用するシステムが多様化する状況においても、分離すべきではない。 ・【統 24】には、特定システム以外でもリスク特性に応じて実施すべき（あるいは考慮すべき）内容が含まれると考えられるため、注意喚起を行う意味でも基礎基準とすべきではないか。
対応方針	・外部の統制に関する基準はすべて[1]「基礎基準」と位置付けたうえで、【統 24】は、FinTech報告書の内容を反映し、「クラウドサービスを利用する場合、利用するサービスの内容及びリスク特性等に応じて・・・が必要である。」としたうえで、「なお、特定システムにおいては、この措置は必要である。」とする。

以上

[1] 【統 24】のほか、【統 25】（共同センター）、【統 26】（金融機関相互のシステム・ネットワークサービスの利用）も基礎基準と位置付ける。

【資料1－2】
平成29年11月21日
公益財団法人　金融情報システムセンター

■外部委託関連基準に対する各委員からのご意見・対応方針

	No.	記載箇所	項番 （基準番号）	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
*	1	資料３－１（第57回）	II.改訂方針に関する論点	・外部の統制に関する基準はすべて「基礎基準」に位置づけるべきであり、クラウドサービスを利用するシステムが多様化する状況においても、分離すべきではない。 ・【統24】には、特定システム以外でもリスク特性に応じて実施すべき（あるいは考慮すべき）内容が含まれると考えられるため、注意喚起を行う意味でも基礎基準とすべきではないか。	三菱東京UFJ銀行 伊藤様(検)	クラウドサービスの利用における安全管理策は、クラウド以外の外部委託の統制の拡張部分と位置付け、改めて「外部の統制」として整理することが有益と考えました。ご意見を踏まえ、クラウド固有の管理策は、【統24】として整理することとし、各委員のご意見を伺いたいと考えております。 また、FinTech報告書の提言では、「重要なシステムにおける」という条件があることから、当該基準については個別の業務・サービスに関する基準、即ち「外部の統制における付加基準」と整理することとし、各委員のご意見を伺いたいと考えております。（No.20参照） →委員会でのご意見を踏まえ、外部の統制に関する基準はすべて(*)「基礎基準」と位置付けたうえで、【統24】は、FinTech報告書の内容を反映し、「クラウドサービスを利用する場合、利用するサービスの内容及びリスク特性等に応じて・・・が必要である。」としたうえで、「なお、特定システムにおいては、この措置は必要である。」としました。 (*)【統24】のほか、【統25】（共同センター）、【統26】（金融機関相互のシステム・ネットワークサービスの利用）も基礎基準と位置付ける。	要	済
*	16	資料３－３（第57回）	統2０．３	３．外部委託先（再委託先を含む）を客観的に評価することが必要である。 当該評価内容は、再委託先までに及ぶ内容として検討された結果でしょうか。 外部委託有識者検討会で、提言された「再委託先の選定要件をあらかじめ定めること」の内容と必ずしも同一にする必要はないと思いますが、例えば、損害賠償などは委託先であって、再委託先を直接評価する内容として妥当ではないものと思料します。	富士通 服部様(検)	ご意見を踏まえ、「外部委託先」を用語として定義したうえで、外部の統制に関する基準を適用する際、用語の定義を認識しやすいよう、【統20】に解説を追加することとしました。 用語の定義（【統20】の解説として再掲） ここでいう外部委託先には再委託先を含む。また、再委託先には再々委託以下の階層を含む（以下同じ）。 また、委託先の選定要件の策定については、外部委託報告書の内容に沿って、特定システムと通常システムにおいて実施すべき対策（あるいは代替可能な対策）を整理し、基準原案に反映いたしました。【統20.3】 また、委託先に対する統制が、全て再委託先に対する統制とはならないことから、以下の記載を追加することとしました。（【統20.1】にも、例示の対策は選択的である点を明記しました） 「なお、委託する業務の全部または一部が再委託される場合、再委託される業務の内容及びリスク特性に応じ、再委託先と外部委託先とで評価する事項が異なる点に留意する必要がある。」	要	済
*	20	資料３－１（第57回）	II.改訂方針に関する論点	該当箇所と意見 論点2、「統制24が個別サービスを利用する場合の実務基準として整理することも考えられる」という記述がありますが、これは個別の業務で限定されたアプリケーションとして利用されるSaaSのような特定のクラウドサービスを指した場合には当てはまるかもしれません。しかしIaaS、PaaSなどより業務基盤そのものに広範囲に利用されるクラウドサービスの利用形態を考えると、FISC様で実施されたFinTech有識者検討会の実例でもコア業務を含めた業務システムがすべてクラウドサービスで実行されるような例が出てきているという調査例が提示されており、そのような最新の状況を考慮しリスクを客観的に把握した上で将来にわたって定めた統制が有効であるような方向性で統制基準の見直しができるような内容にするためには、今後も技術の発展に関わらず有効で抽象度の高い内容を残したほうが良いと思われるため、統制24を残すことを提案します。	アマゾンウェブサービスジャパン 梅谷様(専)	No.1の整理と同様、クラウド固有の管理策は、外部の統制における「基礎基準」として整理したいと考えております。	要	済
*	30	資料３－１（第57回）	II.改訂方針に関する論点	（論点４）について 「【統24】～【統26】については、外部の統制における「個別の業務・サービスに関する基準」として位置付け、外部の統制における「付加基準」として整理する。また、前説における「基礎基準」の選定にあたっての考え方に所要の修正を行う。」との提案内容について賛同します。	三井住友海上火災保険 中川様(検)	前回委員会の後、事務局にて意見交換をしてまいりました。結論としては、外部の統制として「基礎基準」として整理させていただきたいと考えております。（No.1参照）	否	ー
*	31	資料３－３（第57回）	統2０　1.	外部委託先に「共同センター」を含めているが、例えば勘定系の共同センターの場合、よほどの大手金融機関でなければ、オーダーメイドの外部委託ということは難しく、既にある共同センターを比較し、その中から条件等の良いところを選ぶということも事実多いのではないか。また、その選択も頻繁に発生するわけではないため、条件や手順をあらかじめ定めること自体が難しいのではないか。共同センターについては、利用、加盟の検討あたり、通常の外部委託とは異なる対応が考えられる点について、補足を入れていただきたい。	全国信用金庫協会 蓮實様(検)	ご意見を踏まえ、【統20】及び、前説の共同センターに関する記述（p24）に左記の考慮点を追記いたしました。 【統20.1】 「外部委託（共同センター、クラウドサービスの利用を含む）を行う場合は、事前に目的、範囲等を明確にすることが必要である。ただし、外部委託には、勘定系システムの共同化など、当該金融機関等の全体に大きな影響が生じるものがある。こうした場合、外部委託の決定にあたっては、経営計画、中長期システム計画等を踏まえ総合的に評価することが考えられる。」 【前説p24共同センター】 「共同センターに対するリスク管理策は、システムが共同化されている程度や、利用金融機関相互の関係等を踏まえて検討されるべきものであるが、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、インシデント発生時における初動対応は極めて重要なものとなる。」	要	済

2 外部の統制
(1) 外部委託管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　20	外部委託を行う場合は、事前に目的、範囲等を明確にするとともに、外部委託先選定の手続きを明確にすること。

適切な外部委託先を選定するため、外部委託を行う場合は、事前に目的、範囲等を明確にするとともに、選定手続きを明確にし、外部委託先を客観的に評価すること。また、外部委託先の決定にあたっては、責任者の承認を得ること。

ここでいう外部委託先には再委託先を含む。また、再委託先には再々委託以下の階層を含む（以下同じ）。

1. 外部委託（共同センター、クラウドサービスの利用を含む）を行う場合は、事前に目的、範囲等を明確にすることが必要である。ただし、外部委託には、勘定系システムの共同化など、当該金融機関等の全体に大きな影響が生じるものがある。こうした場合、外部委託の決定にあたっては、経営計画、中長期システム計画等を踏まえ総合的に評価することが考えられる。

外部に委託する業務としては、以下の例がある。
(1) オペレーション（バックアップサイトにおけるオペレーションを含む）
(2) システムの開発、変更
(3) ソフトウェアの開発、変更
(4) プラットフォーム、アプリケーション等に関するサービスの利用
(5) ハードウェア及び回線の設置、入替、撤去
(6) 入力データの作成（端末オペレーションを含む）
(7) 記録媒体、ドキュメント及び帳票等の作成、保管、配送、廃棄
(8) 館内、構内及び店内の警備
(9) 電源、空調、防犯等設備の管理、保守
(10) 集中監視（CD・ATM 等）
(11) CD・ATM 等の現金の管理

明確にすべき外部委託に関する事項としては、以下の例がある。
(1) 委託目的
(2) 委託業務範囲
(3) 委託形式
(4) 委託期間
(5) 委託費用

削除: 21

削除: 外部委託先の選定に際しては

削除: （再委託先を含む）

削除: を選定するにあたっては

削除: 明確にしたうえで、選定手続きを

コメント [A1]: 大規模なシステム移行を伴う外部委託においては、開発や運用といった一部の業務を委託する場合と比較し、より総合的な判断を伴うことが想定されるため、考慮事項を追加した。

削除: .

なお外部委託には、共同センター、クラウドサービスの利用も含まれる。.

削除: なお、これら金融機関等の情報システムに関する業務を全面的に委託する場合もある。.

(6) リスクの管理方法
(7) 外部委託先の選定要件
(8) 外部委託に関する自社窓口と役割 等

2. 外部委託先の選定要件を策定することが必要である。
委託する業務に求められる可用性・機密性等の観点及び自社の経営の視点から、リスクを分析・認識し、当該業務に求められるリスク管理レベルを検討のうえ、外部委託先の選定要件を策定する必要がある。

3. 外部委託先を客観的に評価することが必要である。
特定システムを委託する場合、外部委託先に対し金融機関等みずからが評価を行う必要がある。この際、委託する業務の範囲及び外部委託先のサービスの性質、利用形態に関する金融機関等と外部委託先の責任分界点を考慮のうえ、外部委託先の資質・業務遂行能力に関する情報、内部統制、及びリスク管理に関する状況等をもとに評価を行うことが必要である。また、評価にあたっては、外部委託先の情報開示における条件等を考慮し、必要に応じ機密保持契約を事前に締結したうえで開示を求めることが望ましい。委託する業務の全部または一部が再委託される場合、金融機関等は委託先が再委託先を選定することを前提として、その妥当性を検証するために、再委託先の評価を行う必要がある。

通常システムを委託する場合、外部委託先の公開情報、業界における評判、実績等をもとに客観的な評価を行うことも可能である。再委託先については、委託先における再委託先の審査・管理プロセス及びその運用状況が実効的であるかを検証することで、個別の再委託先の評価に代替することも可能である。

外部委託先を評価する事項としては、以下の例がある。
なお、委託する業務の全部または一部が再委託される場合、再委託される業務の内容及びリスク特性に応じ、再委託先と外部委託先とで評価する事項が異なる点に留意する必要がある。

(1) 外部委託を想定する業務に係る実績、技術レベル
①信頼度及び受託実績（類似システムの開発実績、他のプロジェクトやサービスにおける評判等）
②技術レベル（業務内容の理解度、業界に関する知識（金融機関等が委託する業務に関する専門性）、情報収集能力、プロジェクト管理能力（外部委託先が安定して業務に係る開発・運用をしているか等）、導入サポート力等）
(2) 事業継続性（経営方針、経営体力・収益力、人的基盤、被災時の BCM・データのバックアップ）
(3) サービスの可用性・データの安全性（機密性保護）・完全性の確保のための態勢、セキュリティ対策の実施状況（機密保護状況を含む）
(4) 内部統制やリスク管理等に関する状況（委託先における再委託先管理を含む）、外部監査の受検、各種公的認証の取得状況及び組織体制（コンプライアンス体制を含む）
(5) 情報開示における条件

削除: （または再委託先）

コメント [A2]: 外部委託報告書の提言内容を受け、重要・それ以外の場合において、外部委託先及び再委託先に対する評価の方法にメリハリを付けて示すこととした。

削除: （再委託先を含む）

削除: 金融機関等と同等かそれ以上に

削除: 業務が

特に情報セキュリティに関する事項は、十分に把握しておく。

①データの入力・保管・処理・バックアップ・出力といった一連のフロー
②暗号方式、暗号化領域、非暗号化領域
③ログ（システムログ、業務ログ、操作ログ等）の取得範囲・取得頻度・保存期間・開示範囲
④バックアップを含むデータコピーの取得内容・保管場所・保管期間
⑤インフラのバージョンアップ作業及びネットワーク設定情報の変更　等

(6) 監査の受入に関する方針、訪問調査の受入スタンス、コミュニケーションルート
(7) 既存システムとの連携・新システムへのデータ移行の容易性
(8) 保守体制・サポート体制（サポートデスク、問題発生時の対応力（障害発生時におけるトレーサビリティの確保等）、日本語による対応）

なお、外部委託先が提供するアプリケーション、サービス等の導入に際しては【実80、実81】も参照のこと。

(9) インシデントが発生した場合の想定損害額（直接損害・間接損害）と外部委託先側が提示する損害賠償・補償上限額とのバランス
(10) 契約終了時の対応（ベンダーロックインリスク対応、データ消去等）

契約の中断・終了に伴い発生する可能性があるシステム移行作業（移行データの抽出方法と実際の移行作業内容）など

(11) 個人データの取扱い

個人データの取扱いの全部または一部を外部委託先に行わせることを内容とする契約を締結する場合、「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Ⅲに定める「個人データ保護に関する委託先選定の基準」に対する準拠対応可否

(12) 委託費と支払い条件
(13) 係争等に関する国外における裁判に関する事項

外部委託先との間で係争が生じた場合の準拠法及びこれを取り扱う裁判所に関する取決めが国外である場合に評価すべき事項など

国外での裁判に関する事項として評価すべきリスクとしては、以下の例がある。

①現地の各種法制及び裁判制度の把握並びに分析
②現地における活動資格を有する弁護士の確保
③地理不案内な遠隔地での打合せや出廷などに伴う経済的、人的負担
④上記すべてについての外国語による対応

4. 外部委託先の選定に関する手続きを明確にすることが必要である。具体的には、規程等により、外部委託先の選定手続きを定めることが考えられる。また、委託する業務の全部または一部が再委託される場合、再委託される業務の内容及びリスク特性に応じ、再委託先の評価及び委託先に再委託を承認する手続きについても明確にすることが必要である。

5. 外部委託先の決定については、責任者の承認を得ることが必要である。また、システム開発、システム運用、サービスの利用等に関する計画の承認時に、外部委託に関する事項についても責任者の承認を得ることが必要である。

削除: ことが重要である
削除: 情報セキュリティに関する事項としては、以下の例がある。
削除: 65
削除: 66
削除: 他国
削除: 他国
削除: 他国における
削除: 3
削除: 方法として
削除: やガイドライン
削除: 4
削除: （または再委託先）

6. 契約期間中においても、継続的に外部委託先を評価することが望ましい。

削除: 5

削除: （または再委託先）

2 外部の統制
(1) 外部委託管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　21	外部委託先と安全対策に関する項目を盛り込んだ契約を締結すること。

安全性確保のため、機密保護、安定的なシステム運用等に関する項目を盛り込んだ契約を締結すること。

1. 金融機関等は委託した業務が安全に遂行されるよう、機密保護及びシステムの安定的な運用等に関する事項を盛り込んだ契約を外部委託先と締結する必要がある。また、委託契約に加え「機密保持に関する契約」または「リスク管理に関する契約」を締結することも考えられる。

契約締結時に考慮すべき事項としては以下の例がある。なお、委託する業務の内容、リスク特性及び再委託の有無等によって、考慮すべき事項が異なることに留意する必要がある。

(1) 基本的な事項
①用語の定義、役割分担、責任範囲、債務不履行時の損害賠償範囲、準拠法、裁判管轄等
②検収及び納品の条件並びに手順及び権利の移転の時期
③品質の保証及び確認手順
④作業時間、立入場所等
⑤指示目的外使用
⑥契約変更の場合の手順
⑦仕様変更の取扱い

(2) 個別契約条件、サービス仕様、データ保護の管理策
①利用する業務の期限、費用
②外部委託先（複数の外部委託先が業務の委託を受けた場合も含む）への業務委託範囲、外部委託先のサービスの性質及び利用形態を考慮した金融機関等と外部委託先との間の管理境界や責任分界点に関する取決め
③サービス仕様（リソースの割当て等（仕様上の制限や変更に必要な時間等））
④機密保護
⑤金融機関等が守るべき法令や金融機関等のセキュリティポリシー等、外部委託先の要員が遵守するべきルール
⑥セキュリティ管理方法及び体制
外部委託先におけるデータ漏洩防止に関する対策（暗号化等）及び管理体制（暗号鍵の管理体制等）【実3、実4、実8、実30】
⑦データのバックアップ

削除: 22

コメント [A1]: 統 23 の内容であり削除

削除: とともに、その契約の遵守状況を定期的に確認することが

削除: とは別に

削除: 3

削除: 118

削除: 119

削除: 技

削除: 35

(3) サービスレベル未達の場合の対応
(4) 情報開示範囲、監督当局による検査等への協力義務、金融機関等と外部委託先間の報告・連絡等の運営ルール、インシデントレスポンスの取扱い
①作業の報告方法と報告形式
②作業の指示に関する取決め
③委託業務における問題発生時の解決体制
④保守及び障害時等の回復作業・復旧手順、マニュアル整備及び教育・訓練
⑤目標復旧時間（RTO：Recovery Time Objective）
⑥事故発生時における報告
⑦情報漏洩等のインシデントが発生、または発生が疑われる場合のトレーサビリティ確保のための調査協力義務
⑧委託業務に関するコンティンジェンシープラン（緊急時対応計画）【統16、統17】
(5) 反社会的勢力・テロ組織と関わりがないことの表明・確約
(6) 契約の解除条件、契約終了時のデータの返却・消去等及び、契約終了時の原状回復・新システム移行時における協力義務
①契約の解除条件（外部委託先の業務遂行に問題がある場合に、他の外部委託先等と契約する権利等）
②契約終了時における外部委託先によるデータ消去の実施（物理的消去または論理的消去等の方法、開発端末等の消去の範囲）及び実施時期、消去証明書等の発行（または消去プロセスの有効性に関する外部の第三者による検証）、文書等の廃棄・回収【実83】
③契約終了時における原状回復・データ移行作業等の協力義務
(7) 損害が発生した場合の協議及び賠償に関する取決め
(8) 委託業務の成果の知的財産権、使用権等の権利の帰属
(9) 外部委託先からの情報開示
①平常時の標準的な情報開示内容の明記
契約または SLA 等による情報開示の範囲に関する合意、開示請求の対象情報の機密性が高い場合における機密保持契約の締結
②リスク顕在化時の情報開示
リスク事象が発生した際や、各種の資料により情報漏洩リスクが高まった、または外部委託先側の内部統制状況が悪化したと判断される場合の金融機関等からの請求内容に応じた情報開示
(10) 複数の外部委託先への委託
金融機関等と外部委託先間における責任関係の明確化、一元的な窓口機能、外部委託先間の相互調整機能を担う事業者の選定
(11) 再委託管理
①再委託先に対する金融機関等の事前審査の実施
再委託先の選定要件の策定、評価、選定プロセス
選定要件の策定及び、評価については【統20】を参照のこと。
②損害賠償も含めた責任の明確化
再委託先が問題を発生させた際の委託先の管理責任及び、損害賠償の上限に関する条項

削除: 17
削除: 18
削除: ＰＣ
削除: 68
削除: 1

③外部委託先・再委託先間の義務の明確化
外部委託先との契約において、外部委託先が金融機関等に対して負う義務（報告、内部統制確保など）に関する内容と同等の条項が外部委託先・再委託先間の契約上に明記されていることの確認

④再委託の中止の扱い
各種の報告資料等を踏まえ、再委託先の業務遂行能力に対し、問題視し得る状況が生じた場合、金融機関等は外部委託先に対し、再委託の中止を求めることができる条項、外部委託先が中止の求めに応じない場合の委託契約の解除に関する条項の設置

(12) 監査・モニタリング

①監査等の権利
金融機関等が、外部委託先に対し監査等を実施する権利の明記
なお、監査の方法については【監 1】を参照のこと。

②監査等の受入対応費用
監査等の受入対応の費用負担に関する取り決めの明記

③監査等の指摘事項の扱い
監査等により判明した指摘事項への対応に関する取り決め（費用負担・対応期間等）の明記

(13) インシデント発生時等の立入調査

①委託業務において重要な脆弱性が判明した場合、情報漏洩等のインシデントが発生した場合、外部委託先が他の顧客から受託した業務において重大なインシデントが発生した場合、または第三者において委託業務と関連性を有する社会的に重大なインシデントが発生した場合、もしくはこれらの発生が疑われる具体的な懸念が生じた場合等において、金融機関等みずから、または金融機関等が指定するセキュリティ業者・デジタルフォレンジック業者が立入調査することについて外部委託先とあらかじめ協議しておくことが考えられる。

②インシデント発生時において調査に必要なデータの収集範囲及び分析に必要なツール等の提供（提供されない場合は、分析に係る費用等）について、外部委託先とあらかじめ協議しておくことが考えられる。

③外部委託先の経営不安が発生した場合、金融機関等みずから、または金融機関等が指定する専門業者が、必要に応じ、外部委託先施設に立ち入り、顧客データや関連著作物・成果物の保全を行うことについて、外部委託先とあらかじめ協議しておくことが考えられる。

(14) 記憶装置等の障害・交換
記録媒体等を障害、交換等の事情により施設外へ持ち出す場合には、記録済データをあらかじめ復元が不可能または著しく困難な状態とする。また、記憶装置等の障害・交換におけるデータ消去については、消去証明書の発行・取得または外部委託先に対する情報提出要請や、監査等の方法で消去・破壊プロセスの実効性を検証する。

(15) 国外におけるデータ保管時の留意点
金融機関等における障害対応要員の現地の語学力が十分でない場合、日本語によるサポート、外部委託先の日本法人等の障害対応窓口設置を明確にする。

(16) トレーサビリティの確保

削除: 【監 1】

コメント [A2]: 「監査等の権利行使」の内容は、インシデント発生時（13)に集約した。

削除: 監査等の権利行使 .
<#>委託業務において重要な脆弱性が判明した場合及び金融機関等への影響が懸念される場合において監査等を実施する権利の明記 .
③

削除: ④

削除: に関わる領域で

削除: 他事業者

削除: 海外

障害や情報漏洩等のインシデントが発生した際には、流出・毀損したデータの特定や原因究明のための作業が複雑化する場合があることが想定されるため、トレーサビリティ確保のための方策を準備する。

2. SLA の締結または SLO の確認により、サービスレベルについて合意することが望ましい。

SLA 及び SLO に記載される指標としては、以下の例がある。

(1) システム運用（可用性（注）、信頼性、性能、拡張性、稼働時間、ネットワークを含む管理体制、オンラインシステムの稼働開始時限）に関する事項

（注）システム運用の可用性に関する指標の評価にあたって考慮する事項としては、以下の例がある。

①障害等に伴うシステムの停止時間

②システムの更新・保守（緊急的なセキュリティパッチ対応を含む）、新サービスの追加などシステムの品質・セキュリティ向上のための計画停止期間

(2) サポート（障害対応、問合せ対応）に関する事項

(3) データ管理（利用者データの管理等）に関する事項

(4) 統制環境（委託先における再委託先管理、機密保護の維持、統制環境の維持）に関する事項

(5) 開発業務を委託する場合の開発に要する人員や開発期間及び期限に関する事項

なお、広域災害等の影響により外部委託先が SLA 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. サービスレベル合意の違反のほか、外部委託先または金融機関等の方針変更によって外部委託先との契約の続行が困難になるような場合でも、業務の継続を可能とする対策を講ずることが望ましい。

具体的な対策としては、以下の例がある。

(1) 外部委託先による移行すべきデータの抽出方法の提供及び移行作業への協力義務に関する契約書への明記

(2) 契約の解約時におけるシステム移行作業にかかる費用負担の契約書への明記

削除: 万一

削除: （再々以下の階層の先を含む）

削除: .

.

.

.

参照法令

2 外部の統制
(1) 外部委託管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　22	外部委託先の要員にルールを遵守させ、その遵守状況を確認すること。

削除: 23

セキュリティ管理を適切に行うため、外部委託先の要員に対し、委託業務の内容や作業の範囲に応じて、セキュリティポリシーをはじめとした各種ルールの遵守を義務づけ、その遵守状況を確認すること。

削除: （再委託先を含む。以下同じ）

1. 外部委託先の要員が委託業務を遂行するにあたっては、金融機関等のセキュリティポリシーをはじめとした、外部委託先の要員が遵守すべきルールを委託業務の内容及び作業の範囲に応じて明確にし、これを遵守させる必要がある。

   具体的な取り組みとしては、以下の例がある。

   (1) 外部委託先の要員が遵守すべきルールの明示

   業務遂行のマネジメントを含む委託の場合には、業務体制、監査等のセキュリティ要件を外部委託先と合意のうえで契約するか、あるいはそれに準じた文書の中で列挙する。

   なお、外部委託先の要員が遵守すべきルールとしては、以下の例がある。

   ①金融機関等のセキュリティポリシー

   ②コンピュータセンターの入退館管理ルール、機器管理ルール

   ③各種情報へのアクセス権限の管理ルール（ID やパスワードの付与、抹消ルール等）

   ④開発工程において作成されたドキュメントや磁気媒体の管理手順

   (2) 外部委託先の要員が遵守すべきルールの周知徹底

2. 外部委託先の要員に与える金融機関等の各種資源及びシステムへのアクセス権限は、委託業務の遂行のために必要な範囲に限定する必要がある。なお、アクセス権限の取得及び見直しの手順については【実 27】を参照のこと。

削除: 8

3. 金融機関等は、上記のルールの遵守状況を確認する必要がある。そのためには、金融機関等は委託業務の内容及び作業の範囲に応じて、外部委託先における業務の遂行状況について監査を行うこと、または外部委託先からの業務報告を受けるなどの対策を講ずる必要がある。監査については【監 1】を参照のこと。

2 外部の統制
(1) 外部委託管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　23	外部委託における管理体制を整備し、委託業務の遂行状況を確認すること。

外部委託先のセキュリティ管理状況及び、委託した業務が適切に遂行されているかを確認するため、委託業務の内容または作業の範囲に応じて、外部委託管理体制を整備するとともに、委託契約に基づき委託業務の遂行状況を確認すること。

1. 委託した業務を円滑及び適正に運営する観点から、委託業務の内容または作業の範囲に応じて、外部委託管理体制を整備するとともに、委託契約に基づき委託業務の遂行状況を確認する必要がある。また、金融機関等と外部委託先の業務範囲及び責任について、委託契約の内容に応じ、相互牽制を有効に機能させる必要がある。
   なお、組織の整備及び相互牽制については【統 12】を参照のこと。

   業務遂行状況の確認方法としては、以下の例がある。
   (1) 外部委託先の管理状況を把握する。
      ①管理責任者より状況を聴取する。
      ②定期的に作業状況の報告を受ける。また、定められた場所以外で作業が行われていないことを確認する。
      ③作業の機密管理状況の報告を受ける。また、定められた場所以外には情報が持ち出されていないことを確認する。
      ④外部委託先における業務遂行に関する重要な事項の変更（管理責任者の交替、システム更新など）の報告を受ける。
      ⑤セキュリティに関する事故及び犯罪の報告を受ける。
   (2) 外部委託先における業務の遂行状況について監査等を行う。
      確認した結果及び認識した問題点については、その影響度に応じて、経営層へ適切な報告を行う。なお、監査については【監 1】を参照のこと。
   (3) 外部委託先における業務の遂行状況を定期的にモニタリングする。
      金融機関等は、担当要員を選定するなど、外部委託先における顧客データ等の管理状況、データ漏洩防止に関する対策の遂行状況及び開発・運用状況等について把握する。

2. 金融機関等は、外部委託先による業務の成果が金融機関等の求めるレベルに達しているかを把握する必要がある。例えば、システム開発を委託する場合は、機能要件の充足度、標準化遵守状況の確認及び異例処理等を含んだ検証テストを行うことなどが考えられる。
   なお、この業務の成果を計測するために、ベンチマークである SLA をあらかじめ外部委託契

削除: 24

削除: （再委託先を含む。以下同じ）

コメント [A1]: 委託元と委託先の責任については契約締結時に明確にするものであり、ここでは「委託契約の内容に応じ」と修正した。

削除: を明確にし

約の１つとして金融機関等と外部委託先の間で締結し、これに対する評価を定期的に行うことが有効である。SLA の締結については【統 21】を参照のこと。
また、認識された問題点については、外部委託先と連携して速やかに対応することが必要である。

削除: 2

2 外部の統制
(2) クラウドサービスの利用

適用区分					基準分類
共	セ	本	提	ダ	
◎					基礎

統 24	クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること。

クラウド事業者に対する統制を十分かつ実効的に機能させるため、クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること。

1. クラウドサービスを利用する場合、クラウド事業者の選定時に、利用するサービスの内容及びリスク特性等に応じて、統制対象クラウド拠点（注）を把握する必要がある。なお、統制対象クラウド拠点は、実質的な統制が可能となる地域（国、州等）に所在することが必要である。なお、特定システムにおいては、この措置は必要である。

（注）統制対象クラウド拠点とは、データやシステムに対する実効的なアクセスを行う拠点のことを指している。そのため、クラウドサービスにおける情報処理の広域性を勘案し、金融機関等が統制を行うべき対象となる。統制対象クラウド拠点は、クラウド事業者のデータセンター、オペレーションセンター、本社、営業所等様々な拠点が候補となるが、金融機関等によって、利用するクラウドサービスの内容やクラウド事業者の内部管理状況等を踏まえ、金融機関等が個別に特定することとなるため、上記の候補以外が対象となる場合もある。

2. 金融機関等は、統制対象クラウド拠点に対して必要となる権利（監査権等）を確保するために、利用するサービスの内容及びリスク特性等に応じて、クラウド事業者と交わす契約書等にその権利を明記する必要がある。なお、特定システムにおいては、この措置は必要である。

3. 監査の実施にあたっては、技術の先進性などを考慮し、クラウド事業者が監査人に保証型監査を委託（または同等の効力を有する監査を実施）し、その監査報告書を利用することが望ましい。なお、特定システムにおいてクラウドサービスを利用する場合、定期的に監査を実施する必要がある。監査の方法については【監 1】を参照のこと。

4. 特定システムにおいてクラウドサービスを利用する場合、クラウド事業者に対する監査及びモニタリングを実効的に実施するため、クラウド事業者において採用されている技術など専門知識を有する人材を配置する必要がある。ただし、金融機関等内部で確保・育成することが困難な場合においては、専門性を有する第三者監査人等を利用することで代替することも可能である。

5. クラウドサービスの利用にあたっては、新しい技術によってサービス内容及び利用形態が変化す

削除: 付加

削除: 27

削除: （データの切片化、記録保管場所が時間軸に沿って流動的となる等の特徴）

削除: とともに、

削除: するか、

削除: 3

削除: ことが望ましい

削除: も考えられる

削除: 4

る可能性があるため、検討時点から広義の IaaS，PaaS，SaaS 等のクラウドサービスの利用形態を考慮し、金融機関等とクラウド事業者との責任範囲を明確にした上で利用を開始することが望ましい。

削除: に関する定義を参考に

2 外部の統制
(3) 共同センター

適　用　区　分					基準分類
共	セ	本	提	ダ	
◎					基礎

統　25	共同センターにおける緊急事態の発生に備えて安全対策を講ずること。

勘定系システムにおいて共同センターを利用する場合、緊急事態の発生時に迅速な初動対応が取れるよう、適切な安全対策を講ずること。

1. 勘定系システムにおいて共同センターを利用する場合、緊急事態の発生に備えて適切な安全対策を講ずることが必要である。
   共同センターにおいては、緊急事態が発生した際の関係者が複数金融機関等にまたがり、対応方針を相互に合意するのに時間を要する可能性がある。そこで、対応に関する意思決定を迅速化するため、コンティンジェンシープランには初動対応を決定するための手順を盛り込み、利用金融機関等及び共同センターと合意しておくことが考えられる。
   想定される緊急事態については、【実73】を参照のこと。

   ここでいう共同センターには、勘定系システムにおいて共同利用型のクラウドサービスを利用する場合も含まれる。

   迅速な初動対応を可能とする手順としては、以下の例がある。
   (1) 利用金融機関等の利益を代表する共同運営組織が緊急事態発生の際の初動対応を決定する。
   (2) 緊急事態発生時に初動対応を決定する金融機関等を事前に定める。
   (3) 一定の影響範囲内の障害においては、共同センター側があらかじめ合意された対応を実施したうえ、利用金融機関等に事後報告する。
   (4) 初動対応の定期的な訓練（机上訓練含む）を行う。
   (5) コンティンジェンシープランの定期的な見直しを行う。　等

2. 安全対策の検討にあたっては、緊急事態の発生等に備えて必要となる IT 人材を、継続して配置するために、利用金融機関等または、利用金融機関等と共同センターとの間で人員計画を策定することが望ましい。

削除: 付加
削除: 28
削除: 有事の際時の
削除: 58
削除: 対象となる
削除: 有事
削除: 有事
削除: 有事
削除: 外部委託先
削除: 共同で、

2 外部の統制
(4) 金融機関相互のシステム・ネットワークのサービス

適用区分					基準分類
共	セ	本	提	ダ	
◎					基礎

統 26	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、CD･ATM オンライン提携などを行ううえで、基幹インフラとしての機能を担っている。仮に当該システム・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、金融機関等は適切なリスク管理を行うこと。

削除: 付加

削除: 29

1. 金融機関等が業務を外部委託する場合は、金融機関等みずからが、外部委託先の選定及び委託内容（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等が共同で利用しているという特徴がある。
このため、各金融機関等が、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及び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) 金融機関等は、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。
具体的には、金融機関等は、①サービスの管理者から受領した監査報告を評価する、②金融機関等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 ベンダーであり、サービスを利用する金融機関の代表組織等が組織運営に関わる際には、代表組織等が、金融機関等に代わり、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、各金融機関等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、金融機関等みずからも、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。
具体的には、①当該サービスとの接続テストにより、金融機関等のシステム（外部委託するシステムを含む）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、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。

(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、金融機関等が主導的な役割を果たしている場合には、金融機関等は、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。
具体的には、金融機関等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。

(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、金融機関等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も考えられる。

(注 2) 金融機関等が利用する当該サービスを管理する組織。金融機関等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 システム監査
(1) システム監査

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

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監査人がシステムの総合的な評価・検証を行い、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（外部委託先を含む）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また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、システム監査またはそれに準じた監査を受けることが必要である。
   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』等を参照のこと。

2. 監査人として、コンピュータシステムに精通し、監査スキルを保有する人材を確保する必要がある。

3. 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。

4. システム監査におけ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改善のための措置を講ずることが必要である。また、改善策の実施状況について、定期的にフォローアップすることが望ましい。

5. 金融機関等が外部委託を行う場合には、委託する業務の遂行状況及び、外部委託先の要員によるルールの遵守状況等について、評価・検証することが必要である。
   また、提出された情報のみで委託業務の適切性の評価・検証が十分にできない場合は、外部

削除: 運　91

削除: システム

削除: 監査・

削除: 、個人情報保護委員会並びに金融庁が策定した「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」

削除: 2

削除: 3

削除: 適切な改善を行うこと

削除: 。
4. システム監査人として、コンピュータシステムに精通し、監査スキルを保有する人材を確保する必要がある。 。

削除: ・監査

委託先のオフィスまたはデータセンターへの監査・モニタリング等により実地で確認することが必要である。なお、特定システムが再委託される場合には、再委託先に対しても金融機関等の責任において監査を行う必要がある。

外部委託先の監査の方法としては、以下の例がある。

(1) 金融機関等がみずから外部委託先の監査を行う。また、複数の金融機関等が同一の共同センター等を利用する場合は、金融機関等が共同で監査を行うことも考えられる。なお、金融機関等による監査等が実効的でない場合には、第三者監査等（注１）により代替することも考えられる。なお、監査を行う際に、外部委託先から提供されたデータ抽出のツールを利用したデータ検証を行うことも考えられる。

（注１）金融機関等が監査法人を利用した監査を行う場合、監査の対象期間において外部委託先の会計監査に従事していない監査法人とし、また、選定した監査法人が外部委託先の SOC2、IT7 号の保証業務に従事している場合には、外部委託先の保証業務に直接従事していない監査責任者を選定するなどにより、外部委託先との利益相反に疑義が生じないような外観とすることが考えられる。なお、第三者監査人の適格性の担保のため、監査人(監査法人)が日本公認会計士協会等の指導や指針等に基づいて、適切な品質管理体制の整備、運用を実施することも考えられる。また、外部委託先のリスク特性を踏まえた検証、金融機関等の検証ニーズに則った検証を行う。

(2) 外部委託先の内部監査部門の監査結果報告について確認を行う。なお、共同センター等、委託元となる金融機関等が複数の場合は、監査結果を複数の金融機関等に報告することも考えられる。

(3) 第三者保証による報告書（注２）または第三者認証に関する情報（注３）について確認を行う。

（注２）SOC1、SOC2、監査・保証実務委員会実務指針第 86 号、IT 委員会実務指針 7 号等に基づく第三者保証による報告書。

（注３）情報セキュリティ体制やプライバシー保護体制の基準等に係る認証。代表的なものとして、ISMS(ISO27001、ISO27017)や PCI DSS level1、プライバシーマーク等に関する情報。

(4) 外部委託先が作成したセキュリティ及びコンプライアンスに係るホワイトペーパーについて確認を行う。

削除: 外部委託先同様、

削除: 監査

削除: (注２)のレポート

削除: 、または外部委託先が作成したセキュリティに係るホワイトペーパー

削除: ２

削除: 各国の公認会計士協会や業界団体等が定める事業者等の

削除: がある

【資料２－１】
平成 29 年 11 月 21 日
公益財団法人 金融情報システムセンター

基礎基準及び付加基準の対応・方針について

Ⅰ. 前回提示した論点と対応

１．「論点１」について

論点	「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」を廃止し、「実 10」「実 11」「実 12」（※）に統合する。また、安全対策基準で示すコンピュータシステムの定義に、クライアントサーバーが含まれるように用語解説を修正することについて。
主なご意見	賛同
対応方針	「実 13」を廃止し、「実 10」「実 11」「実 12」（※）に統合する。安全対策基準で示すコンピュータシステムの定義に、クライアントサーバーが含まれるように用語解説を修正する。

※「Ⅳ安全対策基準一覧表　2．基準一覧」では「実 36」「実 37」「実 38」に基準番号を変更。

２．「論点２」について

論点２	基礎基準候補の中で、下表に示した３つの基準については、個別のシステムや業務に関する基準に該当することから、「付加基準」とすることについて。
主なご意見	賛同
対応方針	下表の３基準を「付加基準」とする。

○ 以下の基準を「基礎基準」から「付加基準」へ変更する。

基準中項目	番号（※）	基準小項目
インターネット・モバイルサービス	実 34	インターネット・モバイルサービスにおいて口座開設等を行う場合は、本人確認を行うこと。
生体認証	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。
	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。

※「Ⅳ安全対策基準一覧表　2．基準一覧」では「実 34」→「実 117」、「実 46」→「実 140」、「実 126」→「実 141」に基準番号を変更。

３．「論点３」について

論点３	前回提示した方針案及び前回の論点を基に「基礎基準」案を更新し、「新基準構成案」を確定することについて。
主なご意見	ご意見なし
対応方針	前回提示した方針案及び前回の論点を基に「基礎基準」案を更新し、「Ⅳ安全対策基準一覧表　2．基準一覧」を確定する。

II. 基礎基準及び付加基準に関する委員会原案

これまでの審議の結果、基礎基準及び付加基準に関する方針を以下のとおりとし、会員より意見を募集することとする。

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、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及びシステムの不正使用防止に関する基準	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、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。
システムの運行管理に最低限必要な基準	システムの運行管理に最低限必要な対策として考えられるため。

２． 基礎基準・付加基準における「解説部分」の位置付け

基礎基準や付加基準において、「解説部分」で「必要である」と記載されている対策をすべて各基準の「必須対策」と位置付け、「解説部分」で「望ましい」と記載されている対策、例示されている対策は、すべてリスクベースアプローチによって選択的に適用されるものと位置付ける。

なお、以下を本文や表の脚注および前説「Ｉフレームワーク 1. 総論 (4) 安全対策決定のプロセス」に記載する。

システム構成等の観点から適用する必要がない、あるいは適用できない場合には「必須対策」であっても適用は不要である（例えば、外部接続しないシステムについて、外部接続管理に関する安全対策の適用は不要である）。また、「必須対策」には、「個人データを扱うシステムにおいては～することが必要である。」などのように、一定の条件の下において適用が必須である対策も含まれている点に留意する必要がある。

３． 「適用にあたっての考え方」が「望ましい」と記載されている基準について

「適用にあたっての考え方」の末文「望ましい」と記載がある基準は「付加基準」と位置付け、「望ましい」は修文し「～すること」に統一する。なお「解説部分」に「必須対策」が示されていない基準は、そのままの表現とする。

４． 個別のシステムや業務に関する実務基準の位置付けについて

実務基準のうち、個別のシステムや業務に関する基準は、すべての金融情報システムには適用されないことから、「付加基準」と位置付ける。

５． 基準の内訳

○ 「Ⅳ安全対策基準一覧表 ２.基準一覧（設備基準を除く）」に基づき基準の内訳は以下のとおりとなる。

項目	合計	統制		実務	監査
		内部の統制	外部の統制		
基準総数	**168**	19	7	141	1
基礎基準	**106**	19	7	79	1
付加基準	**62**	－	－	62	－

【資料３－１】
平成 29 年 11 月 21 日
公益財団法人 金融情報システムセンター

安全対策基準改訂原案（全編）について

Ⅰ. 安全対策基準改訂原案（全編）について

これまでの議論・ご意見を踏まえ、安全対策基準改訂原案（全編）をとりまとめた（【資料４－３】）。なお、第８版と第９版（案）における構成上の新旧対比は以下のとおりとなる。

第８版	第９版（案）
改訂にあたって	改訂にあたって
Ⅰ.安全対策基準の考え方 1.基準の意義 2.個別金融機関等の安全対策の実施手順 3.本基準の対象 4.本基準の構成と記載内容 5.主要用語	Ⅰ.概説 1.安全対策基準の意義 2.安全対策の考え方
Ⅱ.本書の利用にあたって 1.効果的な利用 2.本書の記述様式 3.参照法令・参考文献等	Ⅱ.フレームワーク 1.総論 2.統制 第8版の「個別金融機関等の安全対策の実施手順」は全面的に内容を見直した
Ⅲ.安全対策基準一覧表 （基準小項目一覧）	Ⅲ.本書の利用にあたって 1.安全対策基準の構成について 2.基準・解説書の記述仕様 (参考)安全対策基準適用における経過的措置について 3.用語の解説 4.参考文献等
Ⅳ.設備基準 （中扉） （前文）	Ⅳ.安全対策基準一覧表 1.構成一覧 ※大項目・中項目の概要 2.基準一覧 ※小項目一覧（旧番号付記）
Ⅴ.運用基準 （中扉） （前文）	Ⅴ.統制基準
Ⅵ.技術基準 （中扉） （前文）	Ⅵ.実務基準
（資料編） 1.セキュリティポリシーについて 2.改訂項目一覧表	Ⅶ.設備基準
（付表）	Ⅷ.監査基準 安全対策の考え方の見直しに伴い、資料編は削除する予定 （付表）

ＩＩ. 改訂原案に対するご意見への対応について

前説（Ⅰ.概要・Ⅱ.フレームワーク・Ⅲ.本書の利用にあたって）、Ⅳ.安全対策基準一覧表、基準本文（Ⅴ.統制基準～Ⅷ.監査基準）に対する各委員からのご意見及び対応方針については、【資料３－２】及び【資料３－３】のとおりとなる。対応方針は、ご意見

をいただいた委員を中心に事前確認を行っており、適宜、改訂原案（全編）に反映している。
今後は、広く会員への意見を募集するとともに、各委員からの意見等を踏まえ、原案への修正を行っていく予定である。なお、内容に影響しない軽微な修正については、事務局一任として対応することでご了承いただきたい。

以上

【資料３－２】
平成29年11月21日
公益財団法人　金融情報システムセンター

■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
*	21	p1	（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」は金融機関等以外の事業者が金融サービスを補完する目的で提供するサービスであることを明確化するため、定義を用語解説に追加したいと考えております。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企業等」という名称（No68参照）に暫定的に戻していますが、FinTech企業が外部委託先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。 併せて、用語定義に以下を追加しました。 金融機関等…… 銀行等の預金取扱金融機関、信託会社、保険会社、証券会社、クレジット会社等をいう。ただし、電子決済等代行業者などのFinTech企業等を除く。 金融サービス…… 金融機関等が業法に基づき顧客に提供するサービス 金融関連サービス…… 金融サービスを補完するため、金融機関等以外の事業者が提供するサービス	要	済
*	72	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 b.タイプB	最後の段落の記載（「本人確認」に関する部分）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、銀行等において口座開設の際に実施するのと同じ本人確認を行うことは実体に即さないものと考えております。 FinTech有識者検討会においても議論された部分となりますが、現状において更新系API接続における本人確認義務の整理が並行して行われる中、API接続を行う際の金融機関側の責務とAPI接続先事業者（FinTech企業）における責務に関する記載については修正が必要と考えております。	FinTech協会 瀧様(専)	ご意見を踏まえ、金融機関等とFinTech企業等の責務に関する記載について、FinTech有識者検討会の報告書に基づき、原案を修正いたしました。 「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みずからのシステムの安全対策を担うこととなる。 タイプBにおいて金融機関等が行う外部の統制の内容は、FinTech企業等が金融機関等から提供された顧客に関するデータを適切に管理しているか、または金融機関等がFinTech企業等から受け入れるデータに対し、これが顧客の依頼に基づくものであることをFinTech企業等が適切に確認しているかという部分に限定される。金融機関等は、当該責務を果たすため、外部の統制に関する基準を準用することとなる。」	要	済
*	78	p16	Ⅱ.フレームワーク 1.総論 (3) 安全対策基準の適用対象	本件と「API接続先チェックリスト」の運用を行う際に、基礎基準を踏まえた安全対策を行うことが前説において定義されていますが、既に実効的なチェックリストの運用が行われている中で、基礎基準と「API接続先チェックリスト」とが2重に参照され実務上の混乱が生じないよう、前説に改めて、チェックリストに照らして適切な検討は、基礎基準との関係でも必要十分な検討であることに関し、言及をして頂きたく考えております。	FinTech協会 瀧様(専)	FinTech有識者会議における議論を踏まえ、内容を検討させて頂きたいと考えております。 →金融機関とFinTech企業等の間で、二者間にとどまらず広く共通的なチェックリストが存在する場合、チェックリストに基づく自主基準を策定することが可能であるとして、脚注に以下（下線部）を追加いたしました。 「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。例えば金融関連サービスの利用（API接続等含む）検討時に行われる安全対策の策定に関して、「基礎基準」を踏まえ、あらかじめ金融機関等と金融機関等以外の企業等との間で二者間に留まらず広く合意形成された共通のチェックリスト等があれば、その内容を踏まえて安全対策の自主基準を策定することも可能である。」	要	済
*	94	ー	（全般）	記述中に「等」や「など」が多数使われており、文意が不明確になっているかもしれないため、これらが何を指すかを明確にするか、使用箇所によっては「等」という表現を削除した方がよいのではないか？	慶應義塾大学 安冨様(専)	個別に確認のうえ、「等」・「など」の表現が不要な箇所があれば、見直しをさせていただきたいと考えております。 →委員からのご意見・アドバイス及び事務局内での指摘を精査のうえ、原案の修正をさせていただきました。	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
*	112	p9	Ⅰ.概説 2. 安全対策の考え方 (5) 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、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。」について、 共有されるべき範囲には監督当局だけではなく、広くステークホルダーも含まれると思料します。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、「認識を共有する範囲」については、再検討する必要があると考えております。すなわち、金融機関等の立場からすれば、ステークホルダーや社会全般においても認識が共有されることが重要であるため、この点を追加できないかどうか、検討させていただきたいと考えております。 →「当局やステークホルダーと金融機関等の間において、‥‥という認識が共有されるべきである」として、当局のみならず、広くステークホルダーとの間で認識が共有されるものとして、文章を修正させていただきました。	要	済
*	114	p10	Ⅰ.概説 2. 安全対策の考え方 (5) 経営責任のあり方	「〇経営層が、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。」は、 「…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、適宜見直しをし、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、経営責任は十分に果たしているとの立場をとる。なお、金融機関等は社会性・公共性を有していることから、これらの考え方は、ステークホルダーはもちろん、広く社会と共有していくべきである。」としてはいかがか。	農林中央金庫 常岡様(専) 今嶋様(検)	ご意見を踏まえ、今一度表現方法等について検討することとします。 →ここで使われる「法的責任」は、裁判所の最終的な司法判断に限定しているものではなく、ご意見にていただいた内容を広く含むことが示されるよう、脚注に補足を入れるとともに、「法的責任」という言葉を、より解釈の幅が持たせられるよう「法的な責任」と修正させていただきました。 「脚注6 ここで「法的な責任」とは、裁判所の最終的な司法判断に限らず、コーポレートガバナンス・コードに準拠した対応や、金融規制上の行動規範に準拠するなど、経営層が広く日常において果たすべき行動や姿勢を尽くすことをいう。」	要	済
*	121	p3-4	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	文末の表現が一部「する」ではなく「していく」になっています。「していく」に特に意味合いがなければ、「する」に統一でもよいのではないでしょうか。 ⇒P3、a. の直前とP4　b. の最後	日本電気 加納様(専)	ご意見を踏まえ、語尾を「する」に変更いたしました。	要	済
*	122	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	8行目に「以上を踏まえて」とありますが、これは(3)のそれ以前の文書だけではなく、「2. 」以降もすべて受けての流れと思われますので、一行空けてはどうでしょうか（あるいは「以上を踏まえ」を(3)の冒頭に移動し「金融機関等は、リスクベース～」と続くようにする？）。	日本電気 加納様(専)	ご意見を踏まえ、「以上を踏まえて」の前に一行挿入し、範囲が限定的とならないよう修正させていただきました。	要	済
*	123	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	真ん中の「金融機関等の～基本原則」の最初に「〇」以下は、直前の「～基本を以下のとおり～」と重複している（二つ目以下の「〇」の前置き）ように思われますので、削除してはどうでしょうか。 ⇒P10では特にこのページの最初の「〇」に相当する文書は入っていません。	日本電気 加納様(専)	ご意見を踏まえ、基本原則の直前の文章から「以下のとおり」を削除させていただきました。（基本原則の内容は変更せず）	要	済
*	124	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	下の部分の「基本原則では、～」以下の文書は、基本原則の解説の様で、書き振りが第三者的で、やや曖昧な印象です。例えば「したがって、金融機関はITガバナンスを適切に発揮し、～安全対策をみずから決定するとともに、金融機関等の情報システムが～重大な外部性や～高い安全対策も求められる」というような文章にされてはどうでしょうか。	日本電気 加納様(専)	ご意見を踏まえ、以下のとおり修正させていただきました。 「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決定することが求められる。ただし、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対しては、社会的に合意されたガイドライン等 に基づく「高い安全対策」を決定することが求められる。」	要	済
*	125	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）	機微性に関する（参考）ですが、本項の主旨を明確にするには「しかしながら」、「仮に」がしっくりこない気がしました。最初の「・」以下にある法的規制があるものは法規制（特定個人情報等）に従うしかなく、リスクベースが入る余地がないのであれば 「しかしながら」は削除し、「仮に」を「しかしながら」や「しかし」とした方が良いのではないでしょうか。	日本電気 加納様(専)	ご意見を踏まえ、修正させていただきました。	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
*	126	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	冒頭の（参考）の下から二行目ですが、「通常システム」と「特定システム」の記載場所は入れ替えた方が良いように思いました。	日本電気 加納様(専)	ご意見を踏まえ、修正させていただきました。	要	済
*	127	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	下のほうの「また、一般に金融情報システムは、商品、～」から始まる段落ですが、「顧客データ」「個人データ以外の重要なデータ」とい言葉が使われています。かたや、P8では「個人情報」「一般の個人情報」「機微情報」「その他個人情報」という言葉が使われています。整合や関連付けがあったほうが良いのではないでしょうか。	日本電気 加納様(専)	ご意見を踏まえ、以下のとおり修正させていただきました。 「顧客データには、個人情報以外の重要な情報 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。」 前説については、原則として「顧客データ」「個人情報」で統一しました。	要	済
*	128	p28 p31	（全般）	前説で全体に係る重要な部分にも関わらず、図が横になっており見辛い。縦配置のまま工夫して記載できないか。	NTTデータ 鎌田様(専) 鈴木様(検)	ここは極力図表を大きく表示したいため、敢えて横に表示させていただきました。会員意見にて、同様のご意見が多数ある場合は、縦配置への変更について検討させていただきたいと考えております。（安全対策基準の対象となる金融機関のコンピュータシステムについては、適用区分の説明文との重複感があるため、図を削除いたしました。）	否	原案のとおりとさせて頂きたいと考えております。
*	129	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）	（参考）「重大な外部性」の考え方については、「金融機関等」が「重大な外部性を有する」システムを特定することと明確に記載されている。 一方、（参考）「情報の機微性」の考え方については、主語が記載されていないため、「重大な外部性」と同様に、「金融機関等」が「情報の機微性」を特定することと明確に記載いただきたい。 （修正案） ・このような事態を避けるためには、金融機関等は、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。	日立製作所 宮崎様(検)	ご意見を踏まえ、以下のとおり修正させていただきました。 「このような事態を避けるために、金融機関等は、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。」	要	済

【資料3－3】
平成29年11月21日
公益財団法人　金融情報システムセンター

■「読みやすさ」に対する各委員からのご意見・対応方針

No.	記載箇所（新基準番号）	記載箇所（従来の基準番号）	項番（基準番号）	ご意見の概要	ご意見者	対応方針（案）	分類	原案の修正要否	反映予定
7	全般	全般	－	「運」「技」の記載を「実」「統」に定めたにも関わらず参照先として「運」「技」が出てくる。「運」「技」の基準は今後も使われるのか？	農林中央金庫 常岡様(専) 今嶋様(検)	参照先の「運」「技」については基準番号が確定次第、「統」「実」に更新します。	⑤表現の統一・見直し	要	11/14 反映済
17	統9	統12	1	開発担当者が本番環境を利用できないことは、不正防止策として有効であるとあるとして、(1)～(3)が併記されているが、それぞれが例になっているわけではない。特に(3)は(1)の具体的事例では？ 開発環境と本番環境の完全分離は難しく、望ましいであることを明記した方がよい。	三井住友銀行 持田様(専) 山口様(検)	(1)の具体的な考慮点としての記載となるため、(1)に紐づけて記載します。（例示内の記載のため、語尾は原案のままとします）	⑤表現の統一・見直し	要	11/14 反映済
29	実26	実7		米国ではNIST SP800-63の改正により、パスワードにランダムな文字列を強要することや、パスワードの定期変更を行うことがむしろ推奨されなくなってきているが、こうした情勢が踏まえられていないのではないか?	農林中央金庫 常岡様(専) 今嶋様(検)	NISTの改正から日も浅く、基準への反映に当たっては十分な調査と検証が必要になると考えます。今後調査を実施したうえで改訂の要否を検討いたします。	②対策・例示の変更	否	－
31	実27	実8		「各種資源」とは何を指しているのか、分かりづらくないか。	三井住友銀行 持田様(専) 山口様(検)	「各種資源」は、「コンピュータシステムを構成する機器、ファイル等」を指しますが、本基準においてはその記載がないため、追記します。	⑤表現の統一・見直し	要	11/14 反映済
39	実28	実15	1	「ここでいうデータファイルとは、・・・DAT等を指す。」について、この並びで言うと、今日的にUSBメモリ、フラッシュストレージ等も加えた方が良いのではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	記憶媒体やストレージ等を含む表現に変更します。	⑤表現の統一・見直し	要	11/14 反映済
40	実28	実15	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等を指している」となっており、前半はファイルを、後半はフロッピーディスクなどのハードウェア媒体を指しています。全体を通じてファイルを指すように、「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、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等の中のファイルを指している」等の表現とした方が良いかと思います。	日本銀行 岡田様(専)	「～の中のファイル」を追記するよう変更します。	⑤表現の統一・見直し	要	11/14 反映済
41	実28	実15	1	USBメモリ等、最近の保存媒体について言及しなくてよいか。	三井住友銀行 持田様(専) 山口様(検)	記憶媒体やストレージ等を含む表現に変更します。	⑤表現の統一・見直し	要	11/14 反映済
43	実41	実19	2	「バックアップを取得するにあたっては・・・取得間隔を定めておくことが必要である。」について、プログラムファイルのバックアップであり、「取得間隔を定めておく」は表現として適切では無いと考えられる。	農林中央金庫 常岡様(専) 今嶋様(検)	ご指摘のとおり表現として適切ではないため、「取得タイミングを定める」等の表現に変更しま	⑤表現の統一・見直し	要	11/14 反映済
46	実42	実21	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。」のモニタリングは何をモニタリングするのか分かりにくい。今日的に、公衆回線に限定する意味も分かりにくい。	農林中央金庫 常岡様(専) 今嶋様(検)	現在の実態を踏まえ適切な表現に見直します。	④時代背景に沿った見直し	要	11/14 反映済
47	実42	実21	2	ATM（Asynchronous Transfer Mode）は伝送方式の種類であるため、公衆回線に限らず、専用回線でも使用される場合があると思います。したがって、「公衆回線（ISDNなど）」と「ATM、」を削除しては如何でしょうか。	日本銀行 岡田様(専)	現在の実態を踏まえ適切な表現に見直します。	④時代背景に沿った見直し	要	11/14 反映済
48	実42	実21	3	「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。」について、極めて重要なセキュリティであり、通常のID、パスワードだけでなく、特権IDや可変パスワードとその管理、アクセスモニタリング、操作ログモニタリングなどもっと対処が必要ではないか。	農林中央金庫 常岡様(専) 今嶋様(検)	現在の記載は、ID、パスワードで保護すれば良いと誤認される表現となっているため、それ以外の対策も必要であることがわかるように表現を見直します。	⑤表現の統一・見直し	要	11/14 反映済
52	実68	実26	1	「ここでいう重要な印字済帳票とは、・・・、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。」とあるが、「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」と定義してしまうと、2.～4.の管理において実現不能とならないか。	農林中央金庫 常岡様(専) 今嶋様(検)	「すべてのもの」の記載表現を見直し対象範囲を明確にします。	⑤表現の統一・見直し	要	11/14 反映済
54	実66	実27	1	「ここでいう出力情報とは、・・・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。」について、ポイントや具体策はベストプラクティクスベースの記載とはいえ、実現不能とならないか。	農林中央金庫 常岡様(専) 今嶋様(検)	「すべてのもの」の記載表現を見直し対象範囲を明確にします。	⑤表現の統一・見直し	要	11/14 反映済
68	実34、実20他	実49、141他		セキュリティホールという語句は、脆弱性が適切な場合が散見。	三井住友銀行 持田様(専) 山口様(検)	例えば、実141の「OS等のセキュリティホールを・・・」は、ご指摘の通り「脆弱性」が適切と考えます。他の箇所についても調査のうえ適切な表現に見直します。	⑤表現の統一・見直し	要	11/14 反映済
113	実91	実100	3	Webシステムだけでなく、スマートデバイス向けの脆弱性対策を明記しなくてよいか。	三井住友銀行 持田様(専) 山口様(検)	スマートデバイスに関する基準については調査、検討中であり今後の改訂に反映する予定です。	②対策・例示の変更	否	－
120	実101	実108	1	「負荷状態の監視制御機能」の例のうち、(1)③は資源使用状況に関するデータを蓄積し、分析するというものなので、（リアルタイムでの）「(1)監視機能」の1項目ではなく、1.の本文に記載することとしては如何でしょうか。 例えば、「1.コンピュータシステムの安定稼働のため、『各種資源の使用状況に関する統計データを定期的にチェックし、事務量の変化等の傾向分析結果をもとに能力増強などの対策を事前に講じるとともに、』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が必要である。」としては如何でしょうか。	日本銀行 岡田様(専)	ご指摘のとおり(1)③は「機能」の説明とは言い難く、記載を見直した方が良いと考えます。ただし例示であることから提案いただいた対策への記載ではなく、選択的に適用可能な例示として記載すべきと考えます。	⑤表現の統一・見直し	要	11/14 反映済
125	実4	実119	参考2	SSL3.0でさえほぼ使われない現状では、「SSL」は「TLS」と改めるべき。	農林中央金庫 常岡様(専) 今嶋様(検)	現状ではSSLの方が一般的に認知されていることから記載はそのままとさせていただきますが、 今後の状況を踏まえ、調査および改訂の要否を検討していきたいと考えております。	②対策・例示の変更	否	－

No.	記載箇所（新基準番号）	記載箇所（従来の基準番号）	項番（基準番号）	ご意見の概要	ご意見者	対応方針（案）	分類	原案の修正要否	反映予定
132	全体	全体		安全対策基準一覧表【基準一覧】にて、新基準番号→旧基準番号の紐づけが記載されているが、旧基準番号→新基準番号の紐づけも付録／別表等でご検討願いたい。（旧基準ベースでチェックリスト等作成している場合の移行／読み替え措置として）	NTTデータ 鎌田様(専) 鈴木様(検)	現在のところ、旧基準番号→新基準番号の紐づけを収録することは想定しておりませんが、会員意見募集等で要望が多い場合は検討したいと考えております。	その他（確認等）	－	－
133	統3	統3		基準中項目が、「(2)組織体制」となっているが、内容は中長期計画となっており、「(1)方針・計画」と整理するほうがよいと思われます。	三井住友海上火災保険株式会社 中川様(検)	本基準の内容としては個別のシステム開発計画を指しており、開発責任者の承認といった体制面についての記載のため、基準中項目は原案のとおりとさせて頂きたいと考えます。	①基準構成の変更	否	－
134	統13	統5		「システムのセキュリティ対策の実施状況ではなく、役職員の遵守状況を確認することが本基準の目的となります。」とのことですが、役職員の遵守状況を確認することを明確にわかるようにするため、タイトル（基準小項目）を修正してはいかがでしょうか。 例）役職員のセキュリティ遵守状況を確認すること。	三井住友銀行 持田様(専) 山口様(検)	基準小項目では全てを表現できないことから、「適用にあたっての考え方」に「～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」と記載しております。役職員を対象とした基準は多数あるため整合性を踏まえ、小項目についても原案とおりとさせて頂きたいと考えます。	⑤表現の統一・見直し	否	－
135	統14	統14		セキュリティ関連文書（・・・・・）を削除しているが、その結果セキュリティポリシーから、マニュアルまですべての文書を周知徹底させるべき様に取られてしまわないか。	全国信用金庫協会 蓮實様(検)	現行の「セキュリティ関連文書」はマニュアル・手順書まで含んでいましたが、マニュアル・手順書は、より実務に関連する文書であることから、「セキュリティ関連文書」という文言は削除しています。ご指摘を踏まえ、表現を「マニュアルや手順書等により行い」を「～に沿って実施し」に見直し、文書そのものを周知徹底という解釈とならないようにします。	⑤表現の統一・見直し	要	11/14 反映済
136	統14,15	統14,15		統14、統15の記載内容で、今回の安全対策基準更改とほぼ同時期に検討、公表が進められている、IT人材育成手引書の関係について記載がないが、今回の基準の改定においては、考慮はされませんか？	日本ユニシス 後藤様(検)	各基準と、IT人材育成手引書との関係の記載については、手引書発刊後に、必要に応じて調査し、委員会にて検討いただくものと考えております。	その他（確認等）	－	－
137	統21他	統22他		「AまたはB」という場合、「または」の後に読点はつけないのが原則ではないかと思われます。 ・統22　1.(14) 「消去証明書の発行・取得または、外部委託先」 ・実142　1.（1）① 「抗ウイルスソフト（ワクチンソフト）または、スパイウェア対策ソフト」 ・P. 279　2行目 「外部委託先のオフィスまたは、データセンター」	三井住友海上火災保険株式会社 中川様(検)	ご指摘の通り読点を付けるのは適切ではないため削除しました。 （該当は指摘いただいた3箇所）	⑤表現の統一・見直し	要	11/14 反映済
138	統22	統19	23	スキル評価のイメージがわくように、どういったスキルを評価することが考えられるのか例示することは難しいでしょうか。	三井住友銀行 持田様(専) 山口様(検)	スキル評価に関する有益な情報を掲載するためには、そのテーマに関する調査・研究・検討が必要となります。今後調査を実施したうえで改訂の要否を検討いたします。	②対策・例示の変更	否	－
139	実1	実116	1.(2)	パスワードの定期変更の効果は最近否定論が主流となりつつあり、例示とは言えこのまま残すべきなのか。	全国信用金庫協会 蓮實様(検)	NISTの改正から日も浅く、基準への反映に当たっては十分な調査と検証が必要になると考えます。今後調査を実施したうえで改訂の要否を検討いたします。	②対策・例示の変更	否	－
140	実12	実130		基準分類はこの一覧表付加を正と理解で良いでしょうか。当該の基準書本体の記載は基礎基準となっていますが、この一覧表は付加基準と記載されています。	日本ユニシス 後藤様(検)	ご指摘のとおり、原案の修正漏れで一覧表が正となります。基準原案の基準分類を修正いたします。	⑤表現の統一・見直し	要	11/14 反映済
141	実14	実135	7	7. の「重要である」は、「必要である」に変更すべきではないか。 （理由） 重要なデータやプログラムを扱うシステムが、外部ネットワークと接続する際には、必ず本人確認等の方法によってアクセス制御を行うことが適当であると考えるため。	日立製作所 宮崎様(検)	ご意見としていただいた内容（必ず併せて実施することが適当）については、その通りかと思いますが、本項の対策のみを実施することを妨げない点を踏まえ、「望ましい」としています。	②対策・例示の変更	否	－
142	実3	実118		基準分類はこの一覧表の付加を正と理解で良いでしょうか。当該の基準書本体の記載は基礎基準となっていますが、この一覧表は付加基準と記載されています。	日本ユニシス 後藤様(検)	ご指摘のとおり、原案の修正漏れで一覧表が正となります。基準原案の基準分類を修正いたします。	⑤表現の統一・見直し	要	11/14 反映済
143	実4	実119	3	「なお、構内LAN・・・」のセンテンスは、4.として独立させるべきではないか。	全国信用金庫協会 蓮實様(検)	前回改訂時における不備と考えられるため、該当文を対策1の最後に移動します。	②対策・例示の変更	要	11/14 反映済
144	実30	実33		暗号鍵に関する対象となる範囲の定義に関する記載を検討願います。 仮想通貨のアドレスと暗号鍵（ハッシュ値）の場合と混同されないようにする事が必要ではないかと考えます。	日本ユニシス 後藤様(検)	本基準は、金融機関が生成、配布、使用及び保管等をおこなう暗号鍵について記載しており、現時点においては、仮想通貨と明確に区別するものではないと考えます。よって、原案とおりとさせて頂きたいと考えます。	②対策・例示の変更	否	－
145	実30	実33		他の基準と同様に、関連する基準の参照を記載していただく事を検討願います。	日本ユニシス 後藤様(検)	基準内の文章において他の基準を参照する必要がある場合に限り、「参照先」として基準番号等を記載しております。全ての基準において関連する基準を記載しているものではありません。	その他（確認等）	－	－
146	実31	統16		「コンピュータシステムに係わる通常時運用の円滑化及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及び訓練を行うことが必要である」等、1～3で必須項目が設定されていますが、教育や訓練の必要性は、システムの用途、使い勝手、重要性等に応じて実施の必要性が異なるかと思います。"重要なシステムについては、"と追記する等、対策を求めるべきシステムを限定すべきかと思います。	三井住友銀行 持田様(専) 山口様(検)	対策の強度は変更していないため、金融情報システムにおいては、コンピュータシステムにおけるオペレーションの教育及び訓練は既に実施されているものと考えます。よって、原案とおりとさせて頂きたいと考えます。	②対策・例示の変更	否	－
147	実33	実48		社内システム等の限定された環境のみで利用するシステムにおいては接続契約内容を明確にする必要は無いと思います。	三井住友銀行 持田様(専) 山口様(検)	システム構成等の観点から適用する必要がない、あるいは適用できない場合には「必須対策」であっても適用は不要であることが前提となっており、本文中（前説）で示されています。当該基準は、外部との接続を安全かつ正確に行うことが目的のため、社内システムに限定された環境のシステムにおいては、必ずしも適用が必要ない場合も考えらえます。よって、原案とおりとさせて頂きたいと考えます。	②対策・例示の変更	否	－

No.	記載箇所（新基準番号）	記載箇所（従来の基準番号）	項番（基準番号）	ご意見の概要	ご意見者	対応方針（案）	分類	原案の修正要否	反映予定
148	実34、実20他	実49、141他	2(5)	①が「外部ネットワークとの接続部分の機器」となっていることについて申し上げております。①にパソコンも含めるべきという意見です。	三井住友銀行 持田様(専) 山口様(検)	パソコンは例示における②に該当し、業務への影響等を考慮し十分に確認したうえで修正プログラム等を適用することになると考えます。	②対策・例示の変更	否	ー
149	実4	実119		基準分類はこの一覧表の付加を正と理解で良いでしょうか。当該の基準書本体の記載は基礎基準となっていますが、この一覧表は付加基準と記載されています。	日本ユニシス 後藤様(検)	ご指摘のとおり、一覧表が正となります。基準原案の基準分類を修正いたします。	⑤表現の統一・見直し	要	11/14 反映済
150	実48	実59	3	3. の語尾に脱字がある。(が)の抜けている。 「(誤)考慮し把握すること望ましい。」 →「(正)考慮し把握することが望ましい。」	三井住友海上火災 保険株式会社 中川様(検)	ご指摘のとおり、変更時の脱字のため修正いたします。	⑤表現の統一・見直し	要	11/14 反映済
151	実51	実52		基準分類はこの一覧表の基礎を正と理解で良いでしょうか。当該の基準書本体の記載は付加基準となっていますが、この一覧表は基礎基準と記載されています。	日本ユニシス 後藤様(検)	ご指摘のとおり、原案の修正漏れで一覧表が正となります。基準原案の基準分類を修正いたします。	⑤表現の統一・見直し	要	11/14 反映済
152	実64	実31		基準分類は基礎、付加のどちらとなりますか。当該の基準書本体の記載は付加基準となっていますが、この一覧表は表記がありません。	日本ユニシス 後藤様(検)	付加基準となります。ご指摘のとおり一覧表上空欄となっておりましたので修正いたします。	⑤表現の統一・見直し	要	11/14 反映済
153	実78	実63	1	1行目の「システムドキュメント」は、「システム」が削除漏れではないでしょうか。	三井住友海上火災 保険株式会社 中川様(検)	現行通りの記載であり削除漏れではありませんが、表現を統一し「システム」を削除します。	⑤表現の統一・見直し	要	11/14 反映済
154	実79	実64		「基準分類」の箇所が、「基礎」ではなく、「付加」のままとなっており修正が漏れていると思われます。	三井住友海上火災 保険株式会社 中川様(検)	ご指摘のとおり修正漏れとなりますので、基準分類を修正いたします。	⑤表現の統一・見直し	要	11/14 反映済
155	実79	実64		基準分類はこの一覧表の基礎を正と理解で良いでしょうか。当該の基準書本体の記載は付加基準となっていますが、この一覧表は基礎基準と記載されています。	日本ユニシス 後藤様(検)	ご指摘のとおり、原案の修正漏れで一覧表が正となります。基準原案の基準分類を修正いたします。	⑤表現の統一・見直し	要	11/14 反映済
156	実92	実101		2項に「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。」とありますが、"以下のような事項"と書かれている(1)～(5)は必須対策でしょうか。それとも留意する例であり、必須対策ではないと考えてよいでしょうか。	三井住友銀行 持田様(専) 山口様(検)	「留意することが必要である」は必須対策となりますが、(1)～(5)については「気に留める必要があるが、実際に行うかどうかは判断が分かれる」という意味合いとなります。	その他（確認等）	ー	ー
157	実99	実106		基準分類はこの一覧表の付加を正と理解で良いでしょうか。当該の基準書本体の記載は基礎基準となっていますが、この一覧表は付加基準と記載されています。	日本ユニシス 後藤様(検)	ご指摘のとおり、原案の修正漏れで一覧表が正となります。基準原案の基準分類を修正いたします。	⑤表現の統一・見直し	要	11/14 反映済
158	実100	実107	1	「汎用機、サーバー・・・・」は「汎用機、重要なサーバー・・・・」と限定しないと範囲が広くなりすぎるのではないか。	全国信用金庫協会 蓮實様(検)	基準内の構成、文意を踏まえ、「1. コンピュータセンターにおける汎用機、サーバーのオペレーションミスの防止～」と変更いたします。	⑤表現の統一・見直し	要	11/14 反映済
159	実100	実107		「汎用機、サーバーの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」「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、チェック機能を充実することが必要である。」とありますが、全てのシステムに対して充実化を求める必要はないと思います。"重要なシステムについては、"と追記する等、対策を求めるべきシステムを限定すべきかと思います。	三井住友銀行 持田様(専) 山口様(検)	ご指摘及び基準内の構成、文意を踏まえ、「コンピュータセンターの」汎用機、サーバーにおいては、チェック機能を「充実」するとし、入力したデータについてはチェック機能を「設ける」とします。	②対策・例示の変更	要	11/14 反映済
160	実107	実42		基準分類はこの一覧表の付加を正と理解で良いでしょうか。当該の基準書本体の記載は基礎基準となっていますが、この一覧表は付加基準と記載されています。	日本ユニシス 後藤様(検)	ご指摘のとおり、原案の修正漏れで一覧表が正となります。基準原案の基準分類を修正いたします。	⑤表現の統一・見直し	要	11/14 反映済
161	実112	実84		基準分類はこの一覧表の付加を正と理解で良いでしょうか。当該の基準書本体の記載は基礎基準となっていますが、この一覧表は付加基準と記載されています。	日本ユニシス 後藤様(検)	ご指摘のとおり、原案の修正漏れで一覧表が正となります。基準原案の基準分類を修正いたします。	⑤表現の統一・見直し	要	11/14 反映済
162	実112	実84	2.(3)⑤	例示に「複数IPアドレスからの同一アカウントによるログインの検知」も記載すべき。 当方も、過去のアカウント乗っ取りによる事故の発生を踏まえ追加するものです。	三井住友銀行 持田様(専) 山口様(検)	例示として、「複数IPアドレスからの同一アカウントによるログインの検知」を追加いたします。	②対策・例示の変更	要	11/14 反映済
163	実118（他）	実41（他）		「基準分類」の箇所が、「付加」ではなく、「基礎」のままとなっており修正が漏れていると思われます。	三井住友海上火災 保険株式会社 中川様(検)	ご指摘のとおり修正漏れとなりますので、基準分類を修正いたします。	⑤表現の統一・見直し	要	11/14 反映済
164	実118（他）	実41（他）		基準分類はこの一覧表の付加を正と理解で良いでしょうか。当該の基準書本体の記載は基礎基準となっていますが、この一覧表は付加基準と記載されています。	日本ユニシス 後藤様(検)	ご指摘のとおり、原案の修正漏れで一覧表が正となります。基準原案の基準分類を修正いたします。	⑤表現の統一・見直し	要	11/14 反映済
165	実132他	実80他		デビットカードについてはJ－Debitもブランドデビットも含まれるとの事でしたが、J－Debitについては「実42」も適用されると思います。また、BANKカードとして、クレジット機能付きのキャッシュカードも一般的になっている中で、デビットカードをｶｰﾄﾞ取引と　分けて記載する必要はありますでしょうか。キャッシュアウトサービス等、多様なカード取引も視野に「カード取引」等で統一的にカバーしてはどうでしょうか。	日本電気 加納様(専)	安対基準におけるデビットカードは、J－Debit、クレジット機能付きの区別はなく、「利用代金を顧客の口座から即時に引き落とし、利用店の口座に入金する即時決済サービスを提供可能なカードサービス」と定義されています。よってカードの種類ではなく機能に応じて基準を適用することとなります。	その他（確認等）	ー	ー

【資料４－１】
平成 29 年 11 月 21 日
公益財団法人 金融情報システムセンター

平成 29 年度『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』改訂原案に対する FISC 会員企業への意見募集実施について

今般、『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『安対基準』という）の改訂原案の取りまとめが終了したことから、広く意見を取り入れるために、FISC 会員企業からの意見募集（以下「意見募集」という）を下記のとおり実施することについてご承認いただきたい。

なお、次回の第 61 回安全対策専門委員会では、FISC 会員企業からの意見を取り入れた改訂原案についてご審議いただき、確定稿といたしたい。

記

Ⅰ 意見募集対象

平成 29 年度安全対策専門委員会（以下「専門委員会」という）にて取りまとめた『安対基準』の改訂原案に対し意見募集を実施する。

意見募集の実施にあたっては、以下の資料を当センターホームページの会員向け Web サイトへ掲載する。

① 【資料１】安全対策基準（第９版）の改訂概要（本日配付した【資料４－２】）
② 【資料２】改訂原案（全編）（本日配付した【資料４－３】）
③ 【資料３】改訂原案（改訂履歴付）（本日配付なし）
④ 【資料４】『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』改訂原案に関するよくあるご質問（FAQ）（本日配付した【資料４－４】）

Ⅱ 意見募集要領

１．募集期間（予定）

平成 29 年 11 月 28 日（火）～平成 30 年１月 12 日（金）17 時必着

２．提出方法

所定の意見提出書式に会社名・部署、氏名、意見等を記入のうえ、電子メール又は郵送により、FISC 事務局までご提出いただく。

３．意見に対する回答

当センターホームページの会員向け Web サイトに掲載する。

Ⅲ 意見募集後の対応

頂いたご意見に対する回答案及び改訂原案（修正版）を FISC 事務局にて作成し、次回の専門委員会でご審議いただく。

※ 誤植・脱字等、軽微な字句・語句の修正については、事務局の判断にて適宜行うこととしたく、ご了承いただきたい。

平成 29 年 11 月 21 日
公益財団法人 金融情報システムセンター

【参考】意見募集から発刊までのスケジュール（予定）

１．意見募集（Web サイト掲載）　【平成 29 年 11 月 28 日（火）～平成 30 年 1 月 12 日（金）】

・当センターホームページの会員向け Web サイトへⅠ.①～④の資料を掲載し、FISC 会員企業から意見募集を行う。

２．意見に対する回答案等作成【平成 30 年 1 月 15 日（月）～平成 30 年 2 月 13 日（火）】（予定）

・FISC 事務局にて、意見に対する回答案及び改訂原案（修正版）を作成する。

３．第 61 回安全対策専門委員会　【平成 30 年 2 月 23 日（金）】（予定）

・意見に対する回答案及び改訂原案（修正版）についてご審議いただく。

・『安対基準』（第９版）の発刊についてご審議いただく。

４．意見に対する回答公開（Web サイト掲載）　【平成 30 年 2 月 27 日（火）】（予定）

・当センターホームページの会員向け Web サイトへ意見に対する回答を掲載する。

５．『安対基準』PDF 版の発刊　【平成 30 年 3 月 30 日（金）】

・当センターホームページの会員向け Web サイトにてダウンロード可能とする。

６．『安対基準』冊子版の発刊　【平成 30 年 5 月】（予定）

・FISC 事務局にて、編集・製本を行い、会員企業に配付する。

以　上

安全対策基準（第９版）の改訂概要

平成29年11月28日

公益財団法人　金融情報システムセンター

安全対策基準（第９版）改訂までの流れ

これまでの安全対策基準の改訂について

- 『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、安全対策基準という）は、昭和60年に初版が発刊された後、ＩＴの進展や新たなサービスの登場など、金融機関等を取り巻く環境の変化に応じ、改訂を行ってきた。
- 直近では、クラウドサービスの利用及びサイバー攻撃対応等に関する有識者検討会を開催し、その検討結果を第８版追補改訂（平成27年6月発刊）に反映している。
- 発刊以来、安全対策基準は、金融機関等の情報システムの安定運用に寄与してきたものの、多様化する基幹業務系以外のシステムに対し、安全対策を一律に実施するのではなく、リスクに応じて安全対策が策定されるよう、安全対策基準の改訂を行うこととした。

昭和60年度	・・・	平成23年度	平成25年度	平成27年度	平成29年度（予定）
初版発刊		第8版	第8版追補	第8版追補改訂	第9版
決済オンライン化に伴い、主に勘定系システムの安全対策に関する自主基準として策定	ＩＴの進展、新たなサービスなど状況の変化に応じ、安全対策基準の改訂を実施		大震災への対応、Ｗｅｂ化の進展、クラウドサービスの利用、サイバー攻撃対応を踏まえた改訂を実施		安全対策に対する考え方の見直し＝リスクベースアプローチの導入

安全対策基準（第９版）改訂までの流れ

有識者検討会の提言を踏まえた安全対策基準の改訂

外部委託に関する有識者検討会及び、FinTechに関する有識者検討会の提言内容を安対基準改訂に反映。

平成27年度	平成28年度	平成29年度

外部委託有識者検討会

＜主な提言＞
- **リスクベースアプローチの導入とITガバナンスの発揮**
- 外部委託（再委託を含む）におけるリスク管理策
- 共同センターにおける固有のリスクへの対応

金融機関等の情報システムを取り巻く状況の変化を捉え、安全対策の方向性や課題をテーマに有識者検討会を開催。
検討会の提言を踏まえ、安全対策専門委員会にて、より分かりやすく、実態に即した安全対策となるよう、安全対策基準の改訂作業を実施してきた。

FinTech有識者検討会

＜主な提言＞
- FinTechに関する安全対策の在り方
- 重要な情報システムにクラウドサービスを利用する際のリスク管理策

安全対策専門委員会
安全対策基準の改訂

安全対策基準（第９版）改訂の概要

改訂のポイント

各検討会における提言内容の反映箇所は次のとおり。

改訂に向けた提言

外部委託に関する有識者検討会

- ◆ リスクベースアプローチの導入とITガバナンスの発揮
- ◆ 委託先（再委託先を含む）におけるリスク管理
- ◆ 共同センターにおける固有のリスクへの対応

FinTechに関する有識者検討会

- ◆ FinTechに関する安全対策の在り方
- ◆ 重要な情報システムでクラウドサービスを利用する場合のリスク管理策
- ◆ 「オープンAPI」における安全対策の在り方
- ◆ 今後の安対基準改訂の考え方

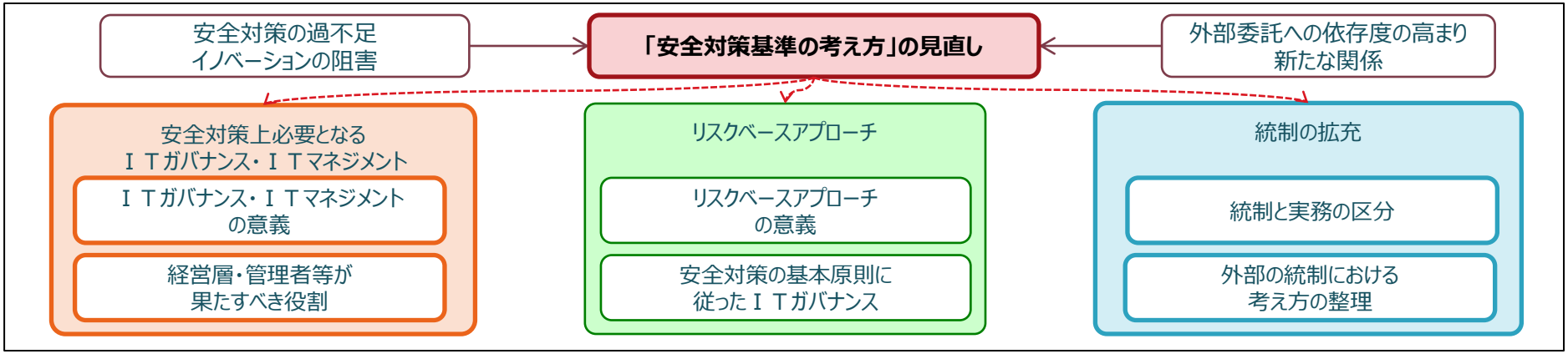
提言内容を安対基準（第９版）に反映

- リスクベースアプローチ導入に伴う改訂
  - 「金融情報システム」の分類
  - 「基準の分類」の設定
  - 「必須対策」の設定
- 外部の統制基準の整理
  - 外部の統制に関する整理
  - 外部委託基準とクラウド基準の整理・統合
  - 共同センター固有基準の新設
- 基準構成の変更・基準の分類
  - 新基準構成
  - 基準の並び替え
- 読みやすさの対応
  - 様式の再定義
  - 語尾の曖昧さ排除

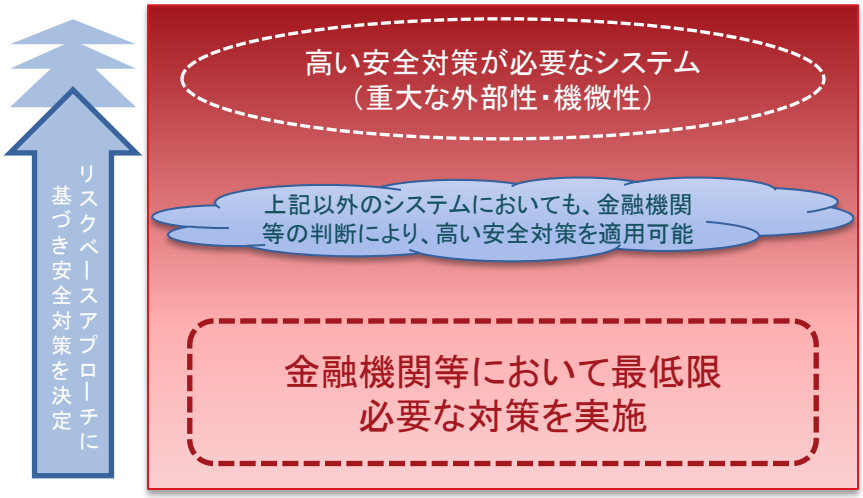
安全対策基準（第９版）改訂の概要

リスクベースアプローチ導入に伴う改訂

ITガバナンスの下、金融情報システムに対してリスク評価を実施し、リスク特性に応じた安全対策基準を適用。



基本原則に従った安全対策の考え方



金融情報システムの分類

「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

特定システム

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）。

通常システム

特定システム以外の金融情報システム。なお、特定システムの一部について、リスクの影響が限定的である場合、特定システムから切り離し、「通常システム」とすることも可能。

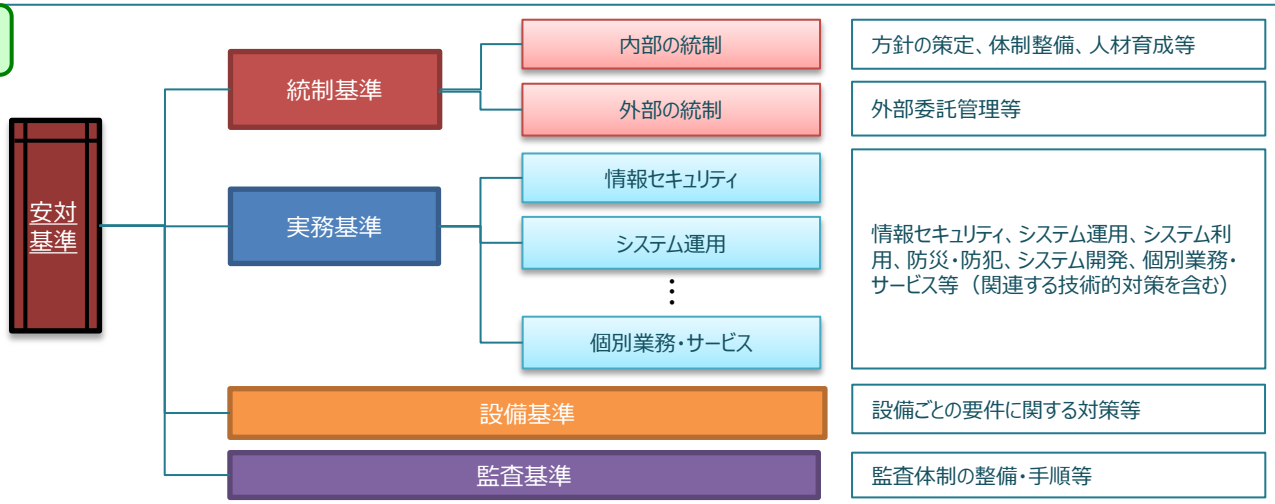
安全対策基準（第９版）改訂の概要

基準構成の変更

基準の構成を「統制基準」「実務基準」「設備基準」「監査基準」に変更。

金融機関の経営層はITガバナンスを発揮していくことが求められ、また、金融機関等においては外部委託やサービス利用への依存度が高まる中、安対基準は統制面での対策を拡充していくことが求められる。これらの要求に応えていくには、安対基準において、**統制面の対策を明示的に示す**ことが有効。

新基準構成



基準項目の並べ替え

基準項目（大項目・中項目・小項目）をシステム共通の視点・利用者の視点に沿って変更。

これまでの基準項目の構成は、基幹業務系システムにおける安全対策を効果的に実施することを前提としていたが、情報システムが多様化し、外部委託やサービス利用への依存度が高まる中、金融機関等はもちろん、FinTech企業等の新たな利用者にとっても、利用しやすい構成へ変更。

第8版追補改訂

・勘定系システムを前提とした構成
・作業の流れをイメージ（入退室管理・・・・）した構成

⇒

第９版改訂案

・様々なシステムを想定した構成
・利用者の目的（セキュリティ対策・・・・）をイメージした構成

安全対策基準（第９版）改訂の概要

「基準の分類」・「必須対策」の設定

ITガバナンスの下、金融情報システムに対して自らリスク評価を実施し、リスク特性に応じた安全対策基準を適用。

「基準の分類」の設定

基礎基準	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
付加基準	「基礎基準」以外で、リスク特性に応じて追加・選択する基準 ※特定システムは適用する基準

「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及びシステムの不正使用防止に関する基準
○コンティンジェンシープラン策定に関する基準
○システムの運行管理に最低限必要な基準

「必須対策」の設定

必須対策	基礎基準や付加基準において、「解説部分」で「必要である」と記載されている対策をすべて各基準の「必須対策」と位置付ける。
その他の対策	「解説部分」で「望ましい」と記載されている対策、例示されている対策は、すべてリスクベースアプローチによって選択的に適用されるものと位置付ける。

基準の適用方法	基礎基準		付加基準	
	必須対策	その他の対策	必須対策	その他の対策
特定システム	○	△	○	△
通常システム	○	△	△	△

【凡例】○：適用　　△：選択的に適用

システム構成等の観点から適用する必要がない、あるいは適用できない場合には「必須対策」であっても適用は不要である（例えば、外部接続しないシステムについて、外部接続管理に関する安全対策の適用は不要である）。
また、「必須対策」には、「個人データを扱うシステムの場合には～することが必要である。」などのように、一定の条件の下において適用が必須である対策も含まれている点に留意する必要がある。

安全対策基準（第９版）改訂の概要

外部の統制の範囲

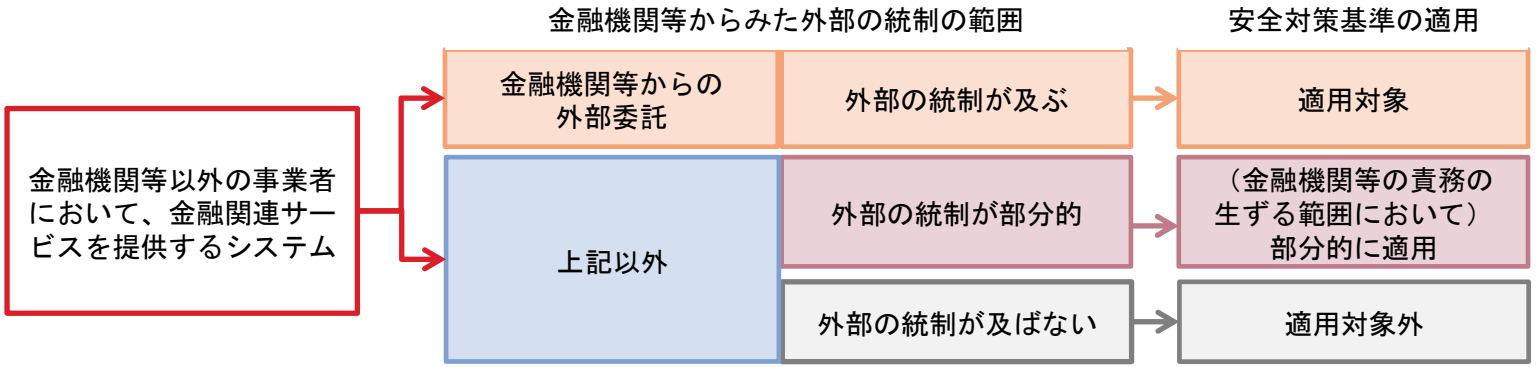
金融機関等以外の事業者が、金融関連サービスを提供する場合の安対基準の適用の考え方を整理。

外部の統制と安対基準の適用範囲の整理

用語の定義

金融サービス	金融機関等（銀行等の預金取扱金融機関、信託会社、証券会社、保険会社、クレジット会社等をいう（ただし、電子決済等代行業者などのFinTech企業等を除く））が業法等に基づき、顧客に提供するサービス
金融関連サービス	金融サービスを補完するため、金融機関等以外の事業者が提供するサービス

FinTech企業等の登場により、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ケースが生じている。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場合の安全対策基準適用方法の考え方を示した。



安全対策基準（第９版）改訂の概要

外部統制基準の整理

外部委託基準（運【87～90】）、クラウド基準（【運108～111】）及び、監査に関する基準（【運91】、【運112】）の内容を統合・整理し、クラウド固有基準と共同センターに関する基準を新設。

外部委託基準とクラウド基準の整理・統合　監査基準の整理・統合　クラウド固有基準の新設

第8版追補改訂（H27.6発刊）

	外部委託	クラウド
利用検討時	運87 運87-1	運108
契約締結時	運88	運109
運用時	運89 運90	運110
契約終了時	運90内	運111
監査	運91内	運112

第9版改訂案

	新基準番号	ポイント
利用検討時	【統20】	記載の重複・冗長を排除し再構成
契約締結時	【統21】	記載の重複・冗長を排除し再構成
運用・モニタリング時	【統22】 【統23】	・記載の重複・冗長を排除し再構成 ・データ漏洩防止基準「運110」は、【統21】へ統合。
契約終了時	–	【統21】へ統合
監査	【監1】	記載の重複を排除し、監1へ統合
クラウド固有	【統24】 （新設）	・クラウド固有のリスク管理策 （「クラウド拠点の把握」「監査権の明記」等）

共同センター固有基準の新設

第9版改訂案

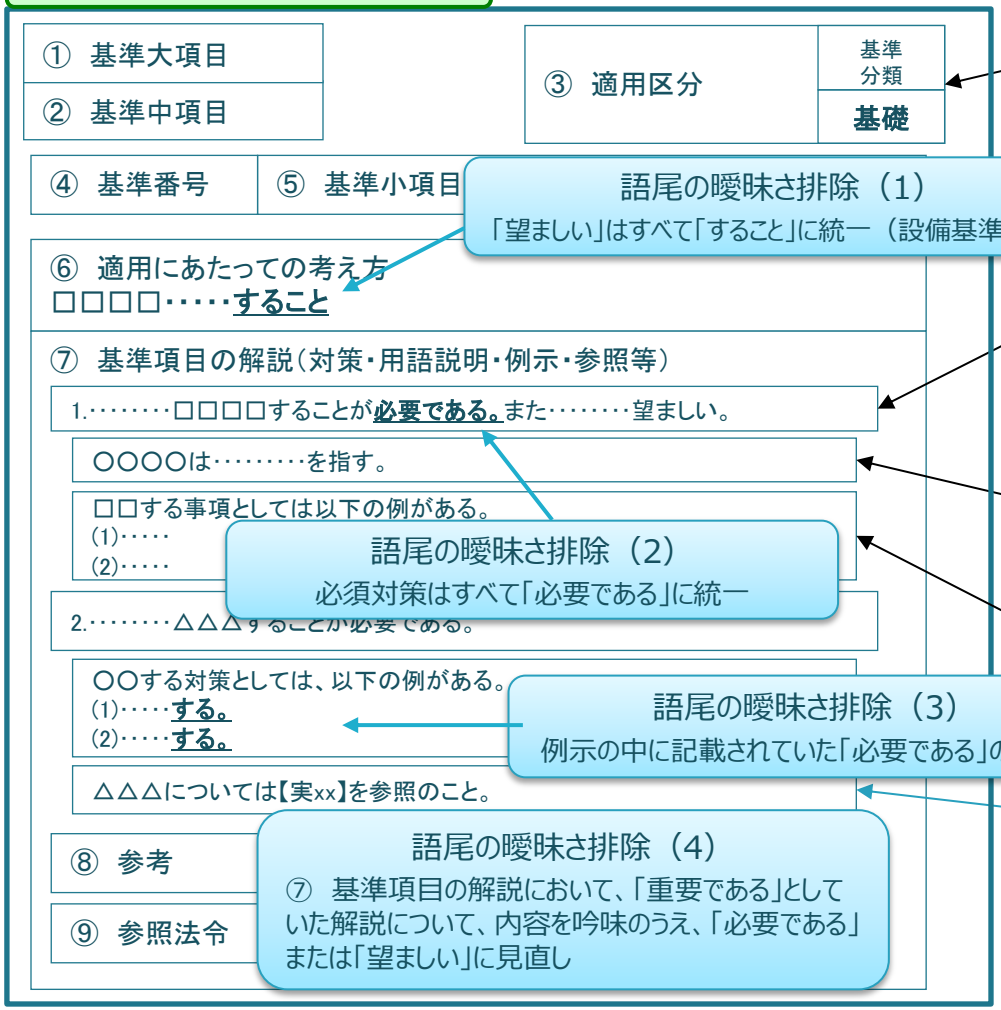
	新基準番号	ポイント
共同センター固有	【統25】 （新設）	・共同センター固有のリスクに対する安全対策 （緊急事態発生時における「時間性」の問題）

安全対策基準（第９版）改訂の概要

読みやすさの対応（記述様式の再定義・標準化）

「読みやすさの向上」を目的とし、様式、記述ルールを再定義するとともに、基準本文（主に解説部分）の変更を実施。

様式・記述ルールの再定義



語尾の曖昧さ排除（1）
「望ましい」はすべて「すること」に統一（設備基準除く）

語尾の曖昧さ排除（2）
必須対策はすべて「必要である」に統一

語尾の曖昧さ排除（3）
例示の中に記載されていた「必要である」の見直し

語尾の曖昧さ排除（4）
⑦ 基準項目の解説において、「重要である」としていた解説について、内容を吟味のうえ、「必要である」または「望ましい」に見直し

【基準分類】
基礎基準・付加基準のいずれであるかを表示する。
（設備基準にはない）

【対策】
実施する「対策」を記載する。

- 「～必要である」 ・・・必須対策
- 「～可能である」 ・・・必須対策に対する代替策
- 「～望ましい」 ・・・選択可能な対策（ベストプラクティス）
- 「～考えられる」 ・・・選択可能な対策

※番号は「対策」のみに付され、例示、用語説明は、関連する「対策」の下に記載している。

【用語説明】
基準中で使用される用語についての説明を記載する。

【例示】
対策に対する具体的な実施方法等を記載する。
例示の内容は、リスク特性等に応じて選択可能な対策となる。
（例示以外の方法等を選択することも可能）

【参照】
対策に関連する基準番号を記載する。

安全対策基準（第９版）改訂の概要

改訂版安対への移行措置

安全対策基準適用における経過的措置を掲載。

（参考）安全対策基準適用における経過的措置について

第9版改訂は、それ以前の改訂と異なり、安全対策基準の適用の考え方から抜本的に変更を行うことから、安全対策基準を使用する金融機関等においては、社内規程の見直しや、場合によっては組織体制等の見直しが発生するなど、その影響が大きいことが予想される。

そのため、現状で安定的に運営されている金融情報システムについては、従来どおりの取扱いを継続することとし、所要の社内体制や規程等の整備を行ったうえで、システムの更改時や新システムの導入時に、変更後の安全対策基準を適用するなど、順次移行を図ることとする。

【資料４－３】
平成29年11月21日
公益財団法人　金融情報システムセンター

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

第９版

平成 30 年 3 月

公益財団法人 金融情報システムセンター

改訂にあたって

　XXX。

平成 30 年 3 月

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

目　　次

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に伴う新たな技術・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]と呼ばれる金融関連サービスを提供する事業者の出現による関係者の拡大を反映し、新たな局面を迎えつつある。一方で、ITの進展により、インシデントの発生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、顧客データ等の金融機関等が保有する重要なデータへのサイバー攻撃が巧妙化・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、利用者に安心して利用できるサービスを提供するためには、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、新たなサービスを展開するための新規開発等にも適切に配分していくことが重要となる。

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。そのうえで、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」という。）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金融機関等にとどまらず、外部の委託先にも拡大していることから、クラウドサービスを重要な情報システムで利用する場合や、FinTech 企業等が提供する金融関連サービスとの新たな関係を踏まえた安全対策の在り方を考える必要がある。本書では、金融機関の内部に対する統制と外部に対する統制の在り方を示すとともに、これらの統制のもとで実施すべき実務的な基準との関係を提示している。

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」という。）に設けられた学識経験者、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、検討委員によって審議され、その結果をとりまとめて作成されたものである。

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として作成され、各社がコンピュータシステムの状況に即して漸次実施しうる内容となっていることを勘案し、金融業務を営む各社においては、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 技術を活用した新たな金融に関連するサービスは、将来においてさらに多様化することが想定されるが、本書においては、金融機関等以外の事業者が上記のサービスを提供する場面を想定し、当該事業者を「FinTech 企業等」と表現している。（Ⅲ.4 用語の解説参照）

[2]「企業価値の最大化」には、ステークホルダーへの還元のみならず、相互扶助の精神から地域の繁栄を実現するという目的もあり、多様な目的を含めて使用している。

[3] 本書では、金融機関等が情報システムの導入・利用により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。

２．安全対策の考え方

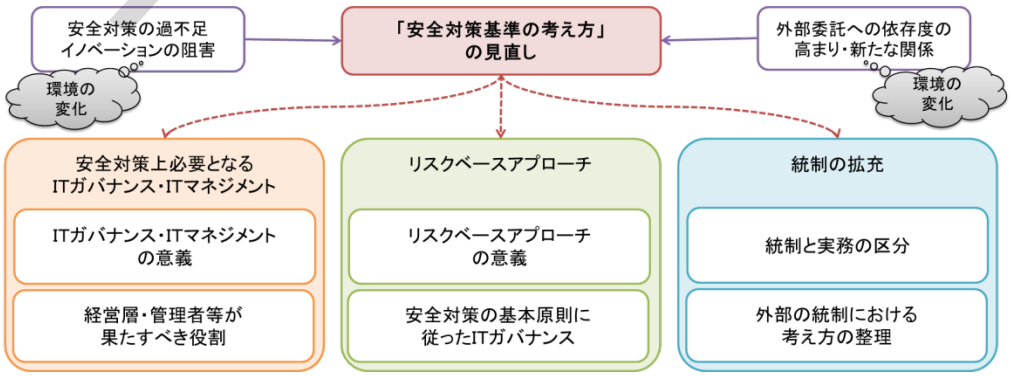
安全対策基準を取り巻く環境変化と対応

安全対策基準が作られた当時、金融機関等の主要な情報システムは、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、IT の進展に伴い、金融機関等の情報システムはその範囲が広がり、基幹業務系以外の情報システムが大きなウエイトを占めるようになってきた。また、システム形態については、ホストコンピュータ中心からクライアントサーバ等の分散処理型のシステムへの移行が進み、サービス利用についても、共同センターやクラウドサービス利用の増加、FinTech 企業等と連携した金融関連サービスの登場等、多様化してきている。

以上の変化の過程で、安全対策基準は、基幹業務系のコンピュータ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たものの、多様化する基幹業務系以外の情報システムにおいては、安全対策基準の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、新規開発への投資が抑制される等、経営資源が適切に配分されないといった懸念が生じてきた。また、金融機関等においては、システム開発・運用業務の外部委託への依存度が高まっているほか、クラウドサービスや FinTech 企業等と連携した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すとともに、統制の在り方も多様化してきている。

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 ガバナンス等、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、これに続く「金融機関における FinTech に関する有識者検討会」では、従来の概念にない新た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、安全対策の在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・利用方法についての理解を目的に、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（[図表 1] を参照）。



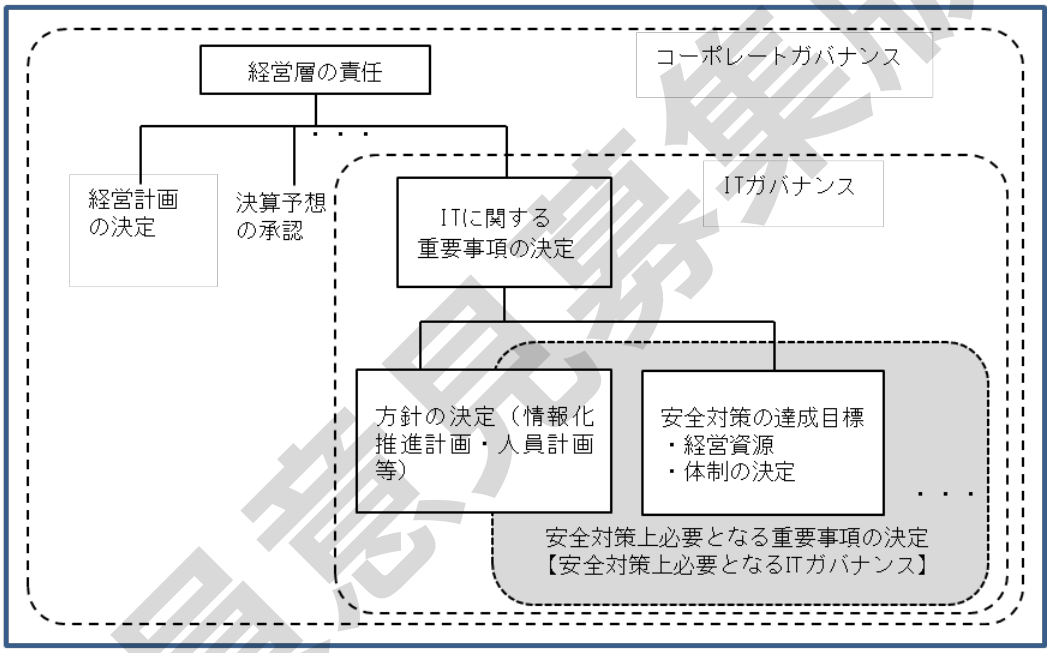
［図表 1］安全対策基準を取り巻く環境変化と対応（概念図）

(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、高い優先度で取り扱われるべき事項である（［図表 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。



［図表 2］IT ガバナンスの階層構造

金融機関等の経営層は、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・安定の確保を推進する（［図表 3］を参照）。

a. 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。

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、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

際には、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、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・人材等の配分方針）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

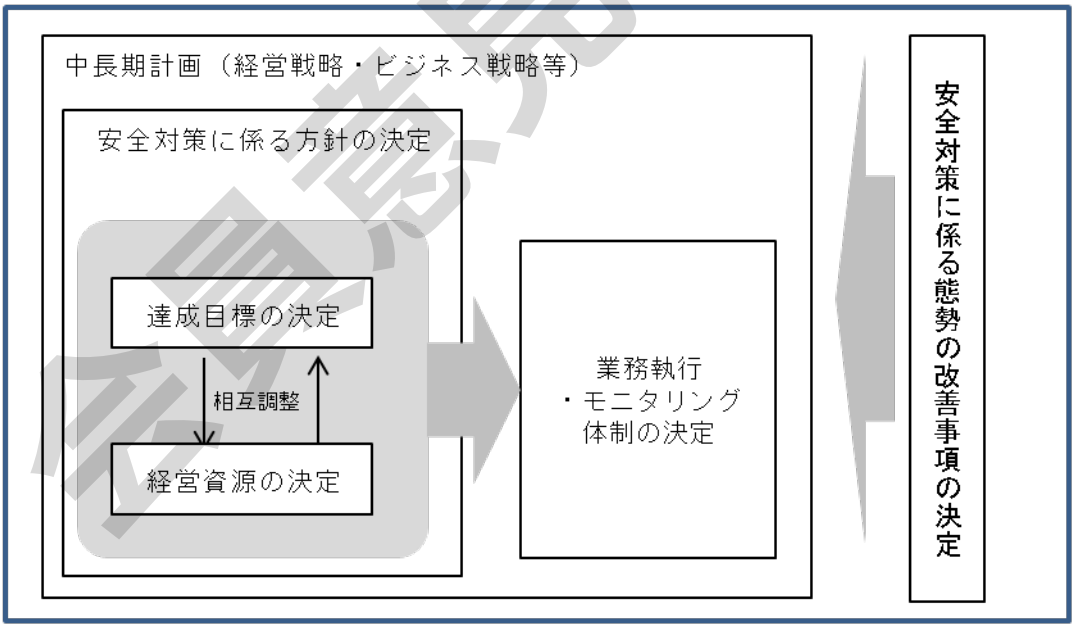
経営層は、安全対策の達成目標及び投下する経営資源の内容を踏まえ、必要に応じて、システム部門等の業務執行体制を決定する。

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。

b. 安全対策に係る態勢の改善事項の決定

経営層は、管理者（後述②a）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を継続的に改善する。



［図表 3］経営層が決定すべき安全対策に係る重要事項の決定

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（［図表 4］を参照）。

a. 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、迅速かつ正確に報告する。

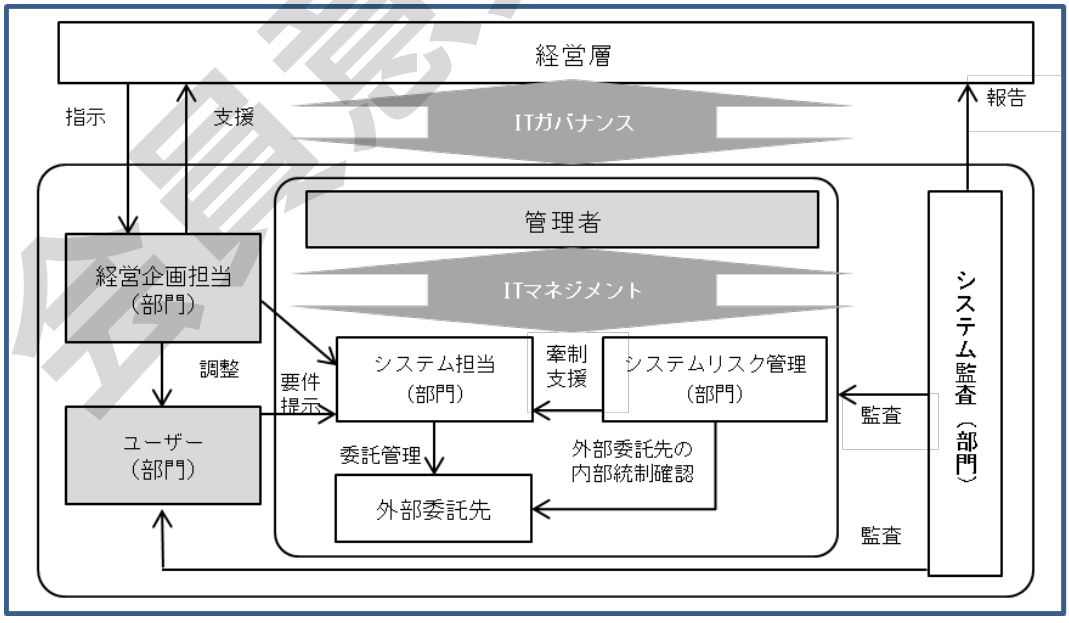
・内部規程・組織体制等の整備・見直し
・個々の情報システムに対する安全対策の決定
・安全対策上必要となる情報の経営層への報告

b. 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。

c. ユーザー（部門）

経営戦略実現のために、ビジネス（商品・サービス・事務）等の企画に携わるとともに、管理者等の関係者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。



［図表 4］情報システムの安全対策に携わる関係者（例）

(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、「基幹業務系のコンピュータ・システム」に適用する基準を明確化しているが、「基幹業務系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、大きな比率を占めるようになってきた基幹業務系以外の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ておらず、以下の状況が生じていることが危惧される。

- 「基幹業務系以外の情報システム」に対する安全対策を「基幹業務系のコンピュータ・システム」に設定しているのと同じレベルに設定しておけば安心である、といった一律に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によっては、そのシステムのリスク特性と比較し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、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、リスク特性の分析結果を安全対策の優先順位など金融機関等が安全対策を決定するため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、リスクゼロを追求することは必ずしも合理的ではないという認識に基づき、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いう。つまり、限られた経営資源の中では、コンティンジェンシープラン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。安全対策の達成目標を決定するためには、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 ガバナンスが適切に発揮されることが重要となる。

(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事態（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）の流出により、プライバシーなど個人の人権が侵害される事態（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づける。

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

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。

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決定することが求められる。ただし、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対しては、社会的に合意されたガイドライン等[4]に基づく「高い安全対策」を決定することが求められる。

[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。

（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等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、影響や損失額等を内部的に把握できるからである。

・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影響や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等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のシステムを、これらと同等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。

・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、病歴等の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）」[5]は、本人の許諾なく流出した場合、経済的損失にとどまらず、プライバシーなど個人の人権の侵害といった広範かつ甚大な損失を発生させる可能性を有するからである。

・しかしながら、一般の個人情報と機微情報（要配慮個人情報を含む）が同一に扱われた場合、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に対し、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。

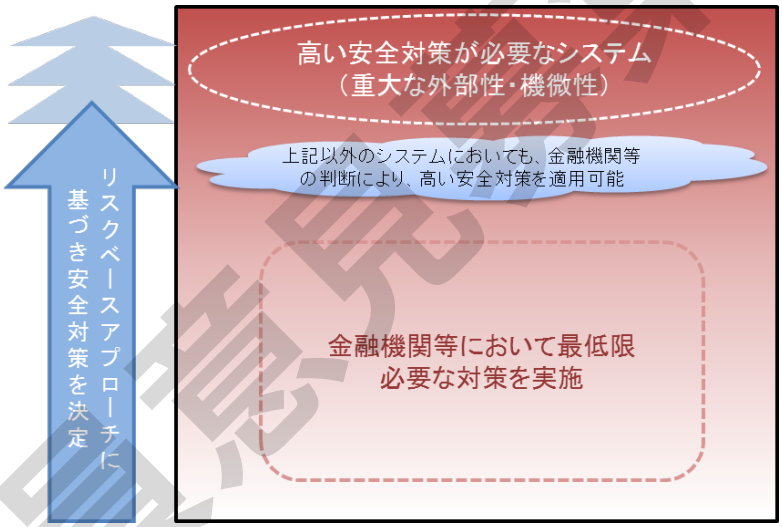
・このような事態を避けるために、金融機関等は、個人情報を「機微情報（要配慮個人情報を含む）」と「その他の個人情報」に分け、「機微情報（要配慮個人情報を含む）」については、「重大な外部性を有する」システムと同様、「高い安全対策」を適用することが必要となる。

[5] 『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６条（機微（センシティブ）情報について）参照。

(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踏まえた評価結果に基づき、安全対策の目標を決定する。さらに、新規投資を含め、顧客の利便性向上や企業価値の最大化を追求した経営資源配分を考慮したうえで、実施する安全対策を決定する。また、重大な外部性や機微性を有するシステムや、それらと同等の取扱いをする必要があると判断されるシステム[6]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、対象となるシステムの決定については、原則として経営層の判断が求められる。

「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、最低限の対策をあらかじめ設定することは、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つながると期待される（[図表 5] を参照）。



[図表 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在り方

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あたっては、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、監督当局やステークホルダーと金融機関等との間において、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、さらにそれが顕在化した場合においても、監督当局やステークホルダー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

6 例えば、法人取引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。

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在り方

〇経営層の使命は、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。

〇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。

〇経営層が、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、インシデントが発生した場合においては、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、法的な責任[7]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」の在り方

「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体制の整備・モニタリングのことをいう。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、外部委託やサービス利用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、安全対策基準を、「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、テクノロジーの進展により、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、各局面に応じたリスク管理策を設けている（［図表 6］を参照）。

7 ここで「法的な責任」とは、裁判所の最終的な司法判断に限らず、コーポレートガバナンス・コードに準拠した対応や、金融規制上の行動規範に準拠するなど、経営層が広く日常において果たすべき行動や姿勢を尽くすことをいう。

区分		基準の内容
統制	内部（自組織内）の統制	中長期システム計画及びセキュリティポリシーの策定、教育・訓練を含む、管理体制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	契約管理や業務管理等、外部委託または外部のサービスを利用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

［図表 6］「統制」と「実務」の区分

② 外部に対する「統制」の在り方

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」と比較し、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。したがって、金融機関等においては、これらのリスクに対して外部に対する「統制」を行うことが必要となる。

さらに、委託先に対し、金融機関等の内部に求められるものと同程度に「統制」を行うことで、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可能性について考慮する必要がある。したがって、委託する業務の内容や委託先の評価結果を把握したうえで、そのリスク特性に応じた統制を行うことが必要であり、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[8]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企業等との契約形態には、外部委託とは性質の異なるものが存在する[9]。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、適切な水準で外部に対する「統制」を行うことが必要となる。

[8] 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。

[9] FinTech 企業等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、サービスの運用主体である 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し、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。

Ⅱ．フレームワーク

１．総論

ここでは、「安全対策の考え方」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、基準の構成、基準の分類、適用方法等、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）からの情報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[10]。「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安全対策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等が可能な場合には、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[11]。

（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[12]、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づ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「特定システム」または「通常システム」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。

---

10 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。

11 例えば、システム全体では、機微情報が保有されているが、当該サブシステム内には機微情報が保有されていない場合が考えられる。

12 一般に、預金取扱金融機関における為替システム、預金システムは、重大な外部性を有すると想定され、生命保険会社における、給付金査定を行うシステムは、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。

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（[図表 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体制の整備のための「内部の統制」及び「外部の統制」に関する基準項目から構成される。内部の統制は、方針の策定や、社内体制の整備、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「Ⅱ.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、情報セキュリティ、システム運用等に関する基準項目から構成される。実務基準には、オペレーション等、管理者や作業者が主体となる対策や、個別の業務・サービスに関する対策、関連する技術的対策が含まれる。

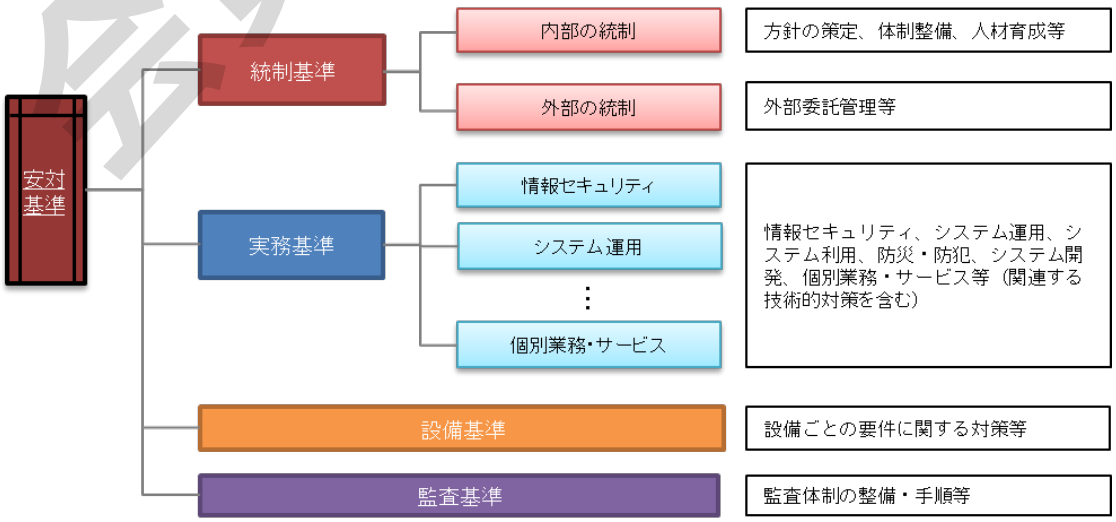
なお、技術の進展が著しい環境下においては、技術的な対策を字義どおりに適用することが適当ではない場合があり、最新の技術動向等を踏まえ、金融機関等において適用の可否を判断されるべきものが含まれることに留意する必要がある。

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、不正行為等から防護するための基準項目から構成される。設備基準には、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載している。

d. 監査基準

統制、実務及び設備に対する監査に関する基準項目から構成される。監査基準には、監査体制の整備や手順等について記載している。



［図表 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。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」・「付加基準」の区分を行っていない。

「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。

すべ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、まず内部及び外部の統制並びに監査に関する基準を「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及びシステムの不正使用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、個人情報以外の重要な情報[13]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を適用することが有効と考えられる。

なお、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、顧客データの漏えい防止及びシステムの不正使用防止に関する基準に含めている。

また、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。

さらに、システムの運行管理に最低限必要な基準についても、これを「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及びシステムの不正使用防止に関する基準
○コンティンジェンシープラン策定に関する基準
○システムの運行管理に最低限必要な基準

上記以外の基準については、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。実務基準のうち個別の業務やサービス等において実施する基準[14]についても、すべての金融情報システムにおいて適用されないことから、これらは「付加基準」としている。

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、システムの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。一方、特定システムでは、「高い安全対策」が求

[13] 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。
[14] インストアブランチ、コンビニ ATM、インターネットの利用に関する基準など。

められることから、「基礎基準」に加え、「付加基準」を適用することとなる。

次に、「基礎基準」の「解説部分」において、すべての金融情報システムに適用されるべき最低限必要な対策を「必須対策」[15]とする。具体的には、「必要である」と 記載している対策を「必須対策」とする。「必須対策」以外の対策は、システム特性やリスク特性等によって選択的に適用 するものとする（「Ⅲ.２.本書の記述仕様」を参照）。

「付加基準」の「解説部分」において、当該基準を適用する場合に必須となる対策 を「付加基準」の「必須対策」[14]とする。具体的には、「必要である」と記載して いる対策を「必須対策」とする(特定システムでは、「付加基準」の「必須対策」を必ず適用するものとする。「必須対策」以外の対策は、システム特性やリスク特性によって選択的に適用 するものとする。

この結果、特定システム・通常システムへの基準の適用方法は、[図表 8] のとおりとなる。

	基礎基準		付加基準	
	必須対策	その他の対策	必須対策	その他の対策
特定システム	○	△	○	△
通常システム	○	△	△	△

・「○」は、適用。

・「△」は、選択的に適用。

[図表 8] 特定システム、通常システムへの基準の適用方法

(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。金融機関等が金融サービスを提供するために外部委託するシステム（クラウドサービス、共同センター等[16]を含む）については、金融機関等が外部の統制を通じて当該システムの安全対策を実施する責務が生じることから、結果として安全対策基準が適用される。なお、金融機関相互のシステム・ネットワーク等[17]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等が共同で利用しているという特徴がある。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基準を適用する。

---

15 システム構成等の観点から適用する必要がない、あるいは適用できない場合には「必須対策」であっても適用は不要である（例えば、外部接続しないシステムについて、外部接続管理に関する安全対策の適用は不要である）。また、「必須対策」には、「個人データを扱うシステムにおいては～することが必要である。」などのように、一定の条件の下において適用が必須である対策も含まれている点に留意する必要がある。

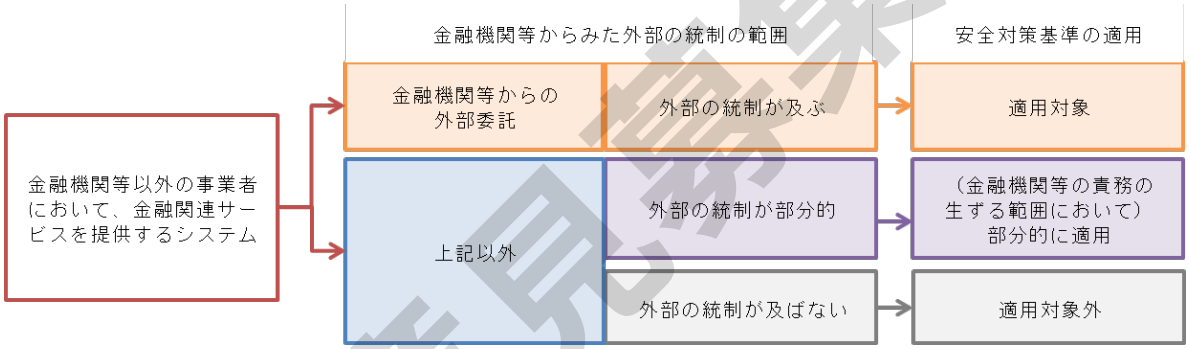
16 金融機関等がベンダーと契約するものや、運営組織等を通じてベンダーと契約するものなどが含まれる。

17 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委託とは別の形態として整理している。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。

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（[図表 9]を参照）。

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[18]。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[19]となる。



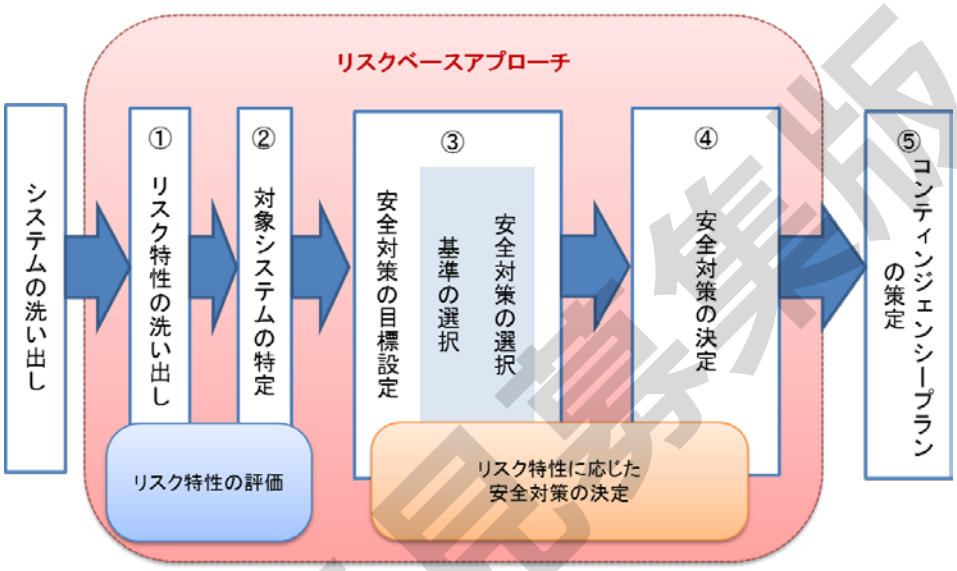
［図表 9］金融関連サービスにおける安全対策基準適用の考え方

18 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。例えば金融関連サービスの利用（API 接続等含む）検討時に行われる安全対策の策定に関して、「基礎基準」を踏まえ、あらかじめ金融機関等と金融機関等以外の事業者との間で二者間にとどまらず広く合意形成された共通のチェックリスト等があれば、その内容を踏まえて安全対策の自主基準を策定することも可能である。

19 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」や「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

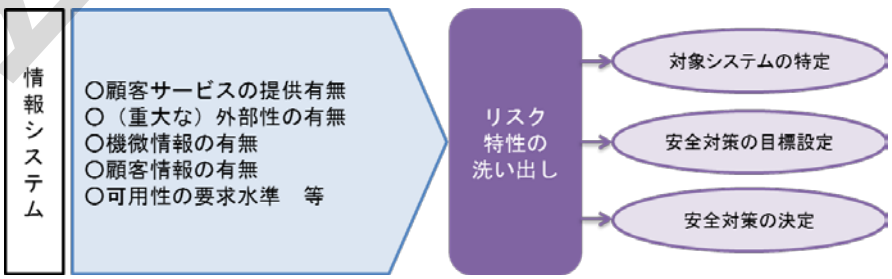
リスクベースアプローチでは、その経営資源配分の効果が最大となるよう、適切な内容で安全対策を決定していくこととなる。金融機関等は、安全対策基準の適用対象となる各システムのリスク特性を洗い出し、対象システムを特定した後、安全対策の目標を定め、必要となる基準及び安全対策の選択を行う。安全対策の目標に対し、安全対策費用とその効果、新規開発投資とその効果、それぞれについて、効率が最大化されるよう考慮し、最終的に安全対策を決定していく。その結果、残存するリスクを踏まえ、必要に応じてコンティンジェンシープランを策定する（[図表 10]を参照）。



［図表 10］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、利用する情報システムを洗い出した後、リスク特性の評価[20]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、顧客データの有無、可用性等の要求水準の観点に基づき行っていく（[図表 11]を参照）。



［図表 11］リスク特性の評価

[20] 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。

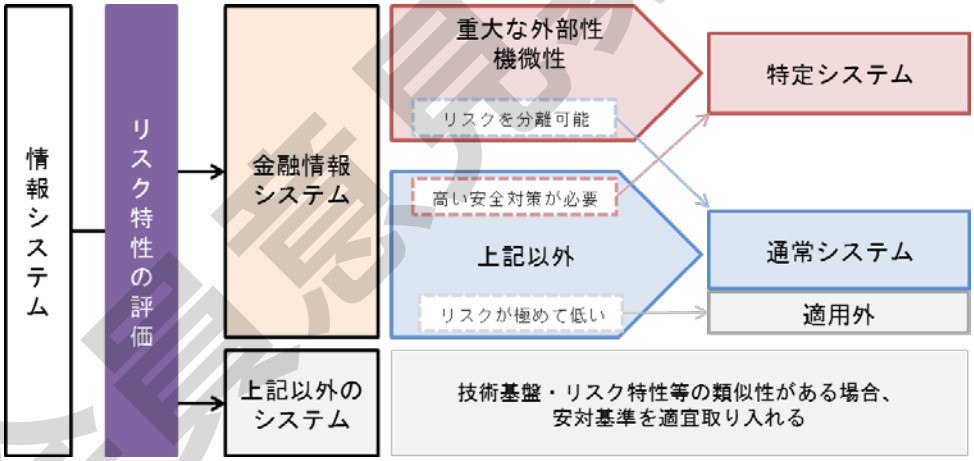
② 対象システムの特定

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（Ⅱ.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等、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（[図表 12]を参照）。

金融機関等においては、システムの区分をさらに細分化するなどの方法も考えられ、金融機関等の実態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。



［図表 12］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、保有するデータの種類や必要となる稼働率など、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等、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、基礎基準及び付加基準に示された対策の中から、必須対策を適用する。併せて、個々のシステムのリスク特性を考慮のうえ、必要な対策を選択して適用する。

通常システムにおいては、基礎基準に示された対策の中から、必須対策を適用する。併せて、個々のシステムのリスク特性を考慮のうえ、必要に応じ基礎基準における必須対策以外の対策及び付加基準に示された対策を選択して適用する。

なお、システム構成等の観点から適用する必要がない、あるいは適用できない場合には「必須対策」であっても適用は不要である（例えば、外部接続しないシステムについて、外部接続管理に関する安全対策の適用は不要である）。

また、「必須対策」には、「個人データを扱うシステムにおいては～することが必要である。」などのように、一定の条件の下において適用が必須である対策も含まれている点に留意が必要である（「Ⅰ.1.(2)基準の分類」を参照）。

④ 安全対策の決定

安全対策を選択した後、経営資源配分等の観点を踏まえ、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、安全対策の実施時期や、安全対策の程度[21]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。

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、本部・営業店等が、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づけている。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。

[21] 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。

コンティンジェンシープランの目的は、安全対策の決定の結果として生じる残存リスクへの対応や、従来から推進されている安全対策の積み重ねを前提に、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、実務基準の「6 緊急時の対応」の中でその対応手順の策定について述べている。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。

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、安全対策基準においても、統制に関する基準を区分している（「Ⅰ.1.(6) 安全対策基準における「統制」の在り方」を参照）。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

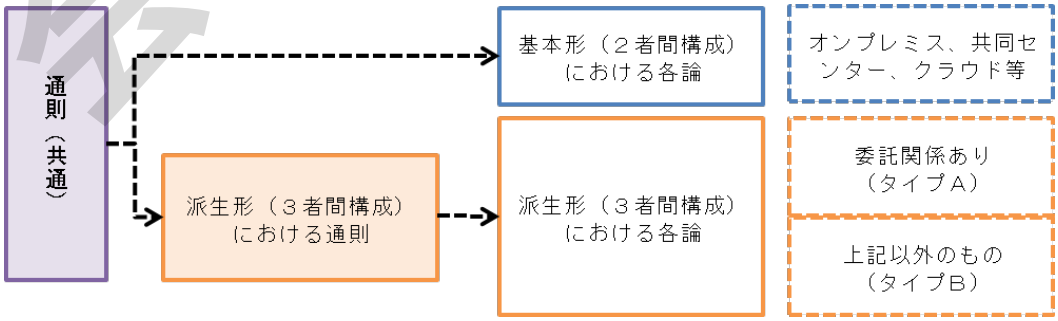
安全対策基準上の「内部の統制」とは、金融機関等が、安全対策を策定・推進していくために自組織内で実施すべき対策を指す。

a. 方針・計画
b. 組織体制
c. 管理状況の評価
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）[22]や経営資源配分等、経営層による意思決定が求められる。

(2) 外部の統制

安全対策基準上の「外部の統制」は、以下のように体系化される。まず、IT ベンダーへのシステムの開発・運用の委託や、クラウドベンダーの利用など、金融機関等と委託先との２者間で構成される関係がある。次に、IT ベンダーやクラウドベンダー等の委託先に加えて、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、外部委託管理における IT ガバナンスの考え方を示したうえで、「外部の統制」における通則及び各論について解説する（[図表 13] を参照）。



[図表 13] 外部の統制における体系

[22] 当センター発行の『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』を参照。

① 外部委託管理における IT ガバナンス

金融機関等は、情報システムの安全性を確保するために、外部委託管理を適切に実施していくことが求められる。

外部委託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（[図表 14]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

	方針の決定	外部委託の決定	リスク管理の枠組みの決定	安全対策の実施	改善事項の決定
特定システム	経営層	経営層	経営層	安全対策に携わる関係者（管理者等）	経営層
上記のうち、委託業務が低リスクな場合※	経営層	経営層以外	経営層以外		経営層以外
通常システム	経営層	経営層以外	経営層以外		経営層以外

※委託業務の性質に加えて、量（例えば委託金額）によっても判断することが可能である。

[図表 14] 外部委託の管理プロセスにおける IT ガバナンス

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（再々委託先以下の層を含む。以下同じ）に対する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
・インシデント発生時の対応

なお、再委託先に対しては、委託する業務の範囲や重要度に応じて、外部委託先に対して実施する管理上の項目から必要な部分を選択し、実施することが考えられる。

以下に、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、委託先の選定にあたって、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、あるいは、発生した問題に対し再発防止を含め適切に対応しているか等）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。また、委託先が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で、再委託先の評価に代替することも考えられる。特に、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については、委託先の情報セキュリティに関する管理状況について評価を行い、その妥当性をもって再委託先の管理状況を評価することも考えられる。

ただし、重要な業務が再委託される場合、例えば、特定システムの運用業務等が再委託される場合は、リスクが顕在化することで、直ちに重大な障害・影響が発生しかねない。このため、金融機関等は委託先における再委託先の審査・管理プロセスの整備・運用状況の適切性を検証するためには、金融機関等がみずから再委託先の審査を行うことが求められる。

b. 委託先に対する統制

金融機関等は、契約期間中において、委託業務の遂行状況のみならず、委託する業務内容や取り扱うデータ等に応じ、セキュリティ管理状況についても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、金融機関等は委託する業務のリスク特性や、統制の形態等を適切に判断し、必要に応じ、委託先への実質的な統制を行うにあたって必要となる権利（監査権等）を契約書の条項に盛り込むこととなる。特に重要な業務が再委託される場合（特定システムの運用業務等）、金融機関等は委託先との契約締結にあたって、再委託先に対する監査権を明記することが求められる。

なお、監査人の選定にあたっては、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. インシデント発生時等の対応

金融機関等は、残存するリスクに対するコンティンジェンシープランを策定することとなるが、重要な業務を委託する場合、コンティンジェンシープランは、委託先を含めて（再委託される場合は再委託先を含めて）策定される必要がある。また、委託先でコンティンジェンシープランを個別に策定する場合は、金融機関等が策定した内容と整合し補完的な内容となっているかを確認することが求められる。さらに、金融機関等は、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となる。訓練では、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委託先や再委託先が認識した場合、金融機関等は、その状況について即時に報告を受けられる体制となっているかを確認し、緊急事態においてコンティンジェンシープランの

発動に係る意思決定を速やかに行える状態にしておくことが重要である。

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上の考慮事項である。

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対応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。

共同センターに対するリスク管理策は、システムが共同化されている程度や、利用金融機関相互の関係等を踏まえて検討されるべきものであるが、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、インシデント発生時における初動対応は極めて重要なものとなる。このため、共同センターの利用においては、インシデントが発生した際、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、インシデントの発生を踏まえた対応態勢を整備しておくことが求められる。

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づけられ、いくつかの利用形態[23]が存在する。クラウドサービスの特徴として、複数の利用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」が挙げられる。また、利用者が広域に及ぶことにより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方法等における「技術の先進性」も挙げられる。

クラウド事業者が、サービスの安全対策を決定する場合には、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想定される。そこで、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、利用するクラウドサービスのリスクの特性に応じた適切な統制が行えるかどうかを確認することが重要となる。

[23] 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。

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、金融関連サービスといったビジネスモデルの企画実施等の業務的な性質もあわせて有しており、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

金融関連サービスの提供に用いる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あたっては、金融機関と IT ベンダーに FinTech 企業等を加えた３者間構成を前提とすることとなるが、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を維持しつつ、類型や３者の安全対策遂行能力（保有する経営資源等）に応じて、役割を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

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（[図表 15] を参照）。

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）。

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」）。責務の再配分にあたっては、「同等性の原則」に従って、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「再配分ルール」を踏まえた統制を行うことが必要となる。

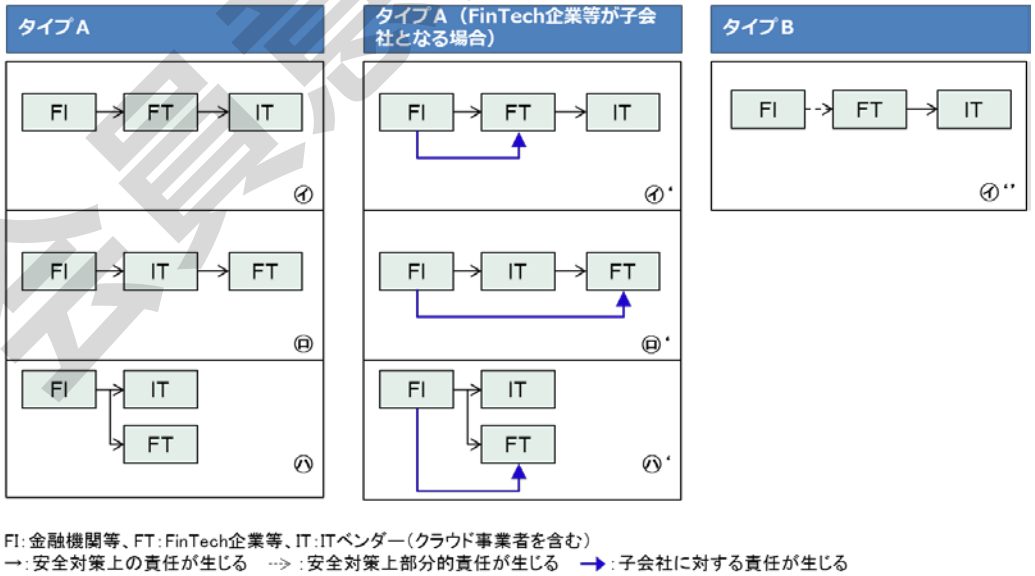
b. タイプＢ（金融機関等が安全対策の決定において部分的に責務を負うケース）

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みずからのシステムの安全対策を担うこととなる。

タイプＢにおいて金融機関等が行う外部の統制の内容は、FinTech企業等が金融機関等から提供された顧客に関するデータを適切に管理しているか、または金融機関等がFinTech企業等から受け入れるデータに対し、これが顧客の依頼に基づくものであることをFinTech企業等が適切に確認しているかという部分に限定される。金融機関等は、当該責務を果たすため、外部の統制に関する基準を準用[24]することとなる。

なお、タイプＢにおいても、「同等性の原則」、「再配分ルール」などを踏まえた安全対策を行うことが必要となる。



［図表 15］派生形（３者間構成）における安全対策実施上の関係者のタイプ別類型

[24] 脚注 19 参照。

Ⅲ．本書の利用にあたって

１．安全対策基準の構成について

安全対策基準は、統制基準、実務基準、設備基準、監査基準から成り、それぞれが基準大項目、基準中項目及び、基準小項目によって構成されている。

安全対策基準の構成については、「Ⅳ. 安全対策基準一覧表」を参照のこと。

２．基準・解説の記述仕様

(1) 基準・解説の記述仕様

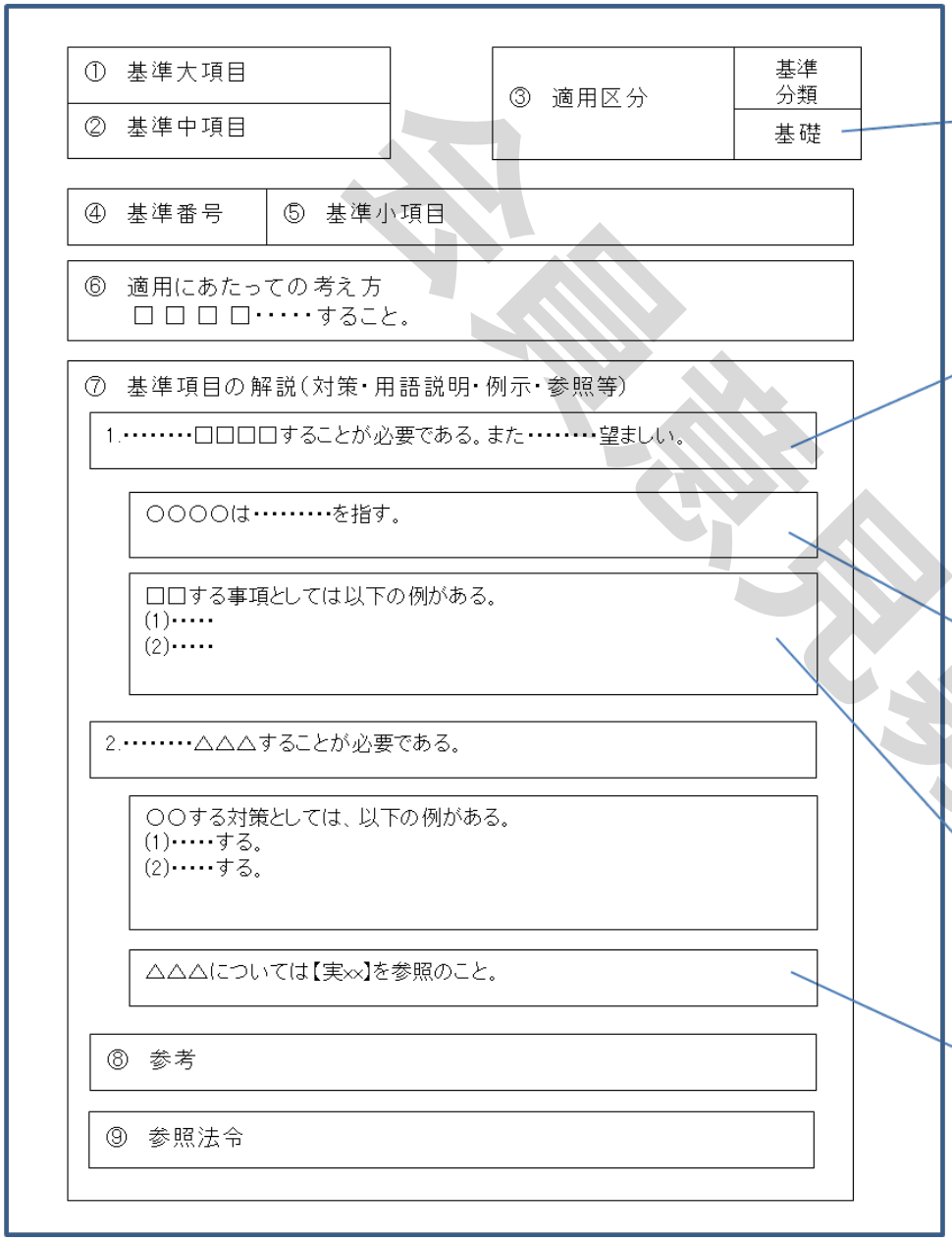
各基準は、以下の内容で構成されている。各欄の意味は以下のとおり（[図表 16] を参照）。

① ：基準大項目、当該基準項目がどの大項目に分類されるかを示す
② ：基準中項目、当該基準項目がどの中項目に分類されるかを示す
③ ：適用区分・基準分類（設備基準には基準分類欄はない）
④ ：統制・実務・設備・監査の各基準内における当該基準項目の項番
⑤ ：基準小項目
⑥ ：適用にあたっての考え方
⑦ ：基準項目の解説（対策・用語説明・例示・参照等）
⑧ ：当該基準項目の解説に関連する参考事項
⑨ ：当該基準項目と関連の深い法令

「適用にあたっての考え方」について

基準小項目の目的及び、実施すべき内容を記載している。なお、設備基準においては、適用が「望ましい」とした基準がある。（統制基準・実務基準・監査基準については、リスクベースアプローチの考え方に基づき実施する対策を選択するため、当該欄はすべて「すること」としている。）

[図表16] 安全対策基準・解説の記述仕様



【基準分類】
基礎基準・付加基準のいずれであるかを表示する。
（設備基準にはない）

【対策】

実施する「対策」を記載する。

- 「～必要である」 ・・・必須対策
- 「～可能である」 ・・・必須対策に対する代替策
- 「～望ましい」 ・・・選択可能な対策（ベストプラクティス）
- 「～考えられる」 ・・・選択可能な対策

※番号は「対策」のみに付され、例示、用語説明は、関連する「対策」の下に記載している。

【用語説明】

基準中で使用される用語についての説明を記載する。

【例示】

対策に対する具体的な実施方法等を記載する。
例示の内容は、リスク特性等に応じて選択可能な対策となる。
（例示以外の方法等を選択することも可能）

【参照】

対策に関連する基準番号を記載する。

「基準項目の解説（対策・用語説明・例示・参照等)」について

基準小項目に対する具体的な対策を記載している。各対策は、以下のように分類される。必須対策以外は、リスクベースアプローチの考えに基づき、選択的に適用する対策となる。([図表 17］を参照

語尾	摘要
・「必要」	必ず実施すべき対策（必須対策）
・「可能」	必須対策に対する代替策
・「望ましい」	選択的に適用する対策（ベストプラクティス）
・「以下の例がある」「考えられる」「有効である」	選択的に適用する対策（例示・参考）

［図表 17］基準項目の解説（対策・用語説明・例示・参照等）

(2) 適用区分

本書では、基準の対象箇所を明確にするため、「適用区分」欄を設けている（[図表 18]参照)。本欄では各基準及び解説が、以下の箇所を対象とするか否かを◎ないし○で示している。

各記号の意味は以下のとおりである。

◎：基準及び解説が当該箇所を対象としていることを示す。(全基準共通)

○：当該箇所を対象とするが、金融機関等の業務の実態に照らし、必要に応じて取り入れる基準及び解説であることを示す。したがって「適用にあたっての考え方」の欄を、「…望ましい」と記述する（設備基準のみ)。

適用区分				
建物、チャネルに依存せず適用 「共」と略記	コンピュータセンター・共同センター 「セ」と略記	本部・営業店等 「本」と略記	ダイレクトチャネル 「ダ」と略記	流通・小売店舗等との提携チャネル 「提」と略記
	◎	◎		

※設備基準においては、「建物、チャネルに依存せず適用」の欄はない。

［図表 18］適用区分の例

各業界・業態によって本部・営業店等の運用形態や提供サービスの内容が異なる場合は、それぞれの実態に合わせて本書に記載の安全対策を適宜取り入れることとする。

以下にモデル化された 5 つの機能要素について述べる。

①コンピュータセンター・共同センター

コンピュータシステムを用いて金融機関等の業務を集中して処理しデータを蓄積する機能を有す。コンピュータ本体やそれを収容する建物、ソフトウェア、開発・維持組織や要員等から構成される。共同センターの場合、建物等の一部構成要素について、金融機関等の管理対象外となる場合がある。

②本部・営業店等

a. 本部

コンピュータセンター以外の本部機能を指す。企画部門、営業店支援部門、システム開発部門等の組織、事務センターや地区センター等から構成される。

b. 営業店等

顧客にサービスを提供する店舗機能を指す。有人の店舗（テラーが顧客対応する窓口で、CD・ATM が併設されている場合を含む）、CD・ATM が設置されている無人店舗、ショッピングセンターやスーパーマーケット等にインストアブランチとして設置された CD・ATM、及び有人の店舗で勤務している要員等から構成される。

③ダイレクトチャネル等

「営業店等」を介さずに、サービスを直接顧客に提供するデリバリーチャネル機能を指す。電話やインターネット、モバイル（携帯電話）による金融サービスの提供を想定している。

④流通・小売店等との提携チャネル

金融機関等が、流通・小売店等と提携して顧客へのサービスを提供するデリバリーチャネル機能である。小売店舗を通じてサービスを提供する場合（デビットカードなど）や流通業を通じてサービスを提供する場合（コンビニエンス ATM など）を対象としている。

(3) 基準分類

当該基準が基礎基準・付加基準のいずれであるかを示している（「基礎」または「付加」と記載する。設備基準には当欄はない。）（[図表 19] を参照）。

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

［図表 19］基準分類の表示例

（参考）安全対策基準適用における経過的措置について

第９版改訂は、それ以前の改訂と異なり、安全対策基準の適用の考え方から抜本的に変更を行うことから、安全対策基準を使用する金融機関等においては、社内規程の見直しや、場合によっては組織体制等の見直しが発生するなど、その影響が大きいことが予想される。

そのため、現状で安定的に運営されている金融情報システムについては、従来どおりの取扱いを継続することとし、所要の社内体制や規程等の整備を行ったうえで、システムの更改時や新システムの導入時に、変更後の安全対策基準を適用するなど、順次移行を図ることとする。

３．用語の解説

(1) 安全対策基準における「重要な」の意味

安全対策基準において、「重要な本体装置」「重要なデータ」等、「重要な…」と表記されている場合の「重要な」とは、「当該…に障害が発生した場合、金融サービス機能（現金引出、資金決済等）の提供という面で多数の顧客に影響を与え、かつ効果的な代替手段を講ずることが難しいと想定される…」、あるいは「当該…に破壊・改ざん等が発生した場合にコンピュータシステムの運転に重大な支障を来す…」、あるいは「顧客データそのもの」を意味する。

(2) 安全対策基準において用いる主要用語の定義または範囲は、以下のとおりである。

CSIRT…… コンピュータセキュリティインシデントに関する報告を受け取り、調査・対応活動を行う組織の総称（Computer Security Incident Response Team の略称）

CVCF…… 電源の入力変動や出力負荷の変化に関係なく、コンピュータシステムへ供給する電圧及び周波数を一定に保つ装置、または電圧・周波数を安定化した電源のこと。以前は単独の装置だったが、現在では UPS（無停電装置）に機能として組み込まれることが多い。（Constant Voltage Constant Frequency Power Supply: 定電圧定周波装置の略称）

DoS 攻撃 …… コンピュータやネットワーク機器に対して無意味なデータを短時間に大量に送りつけるもので、システムを混乱させ、正常な接続を妨げる攻撃。DoS 攻撃が単一のコンピュータからの攻撃なのに対して、DDoS 攻撃では複数のコンピュータが一斉に単一の標的にパケットを送信することで、攻撃者の特定を困難としている。

EUC システム…… 情報システム部門以外の部門が管理するシステム

IDF…… 回線がフロアに入る最初の場所に設置されるフロア配線盤（Intermediate Distributing Frame の略称）

MDF …… 回線が建物に入る最初の場所に設置される主配線盤（Main Distributing Frame の略称）

SLA …… 委託先から提供を受けるサービスの品質を明確にし、約束するために取り交わす契約書。システムの可用性、障害時の復旧時間、オンラインシステムの稼働開始時限、システム性能などに関する指標を決めておく。（Service Level Agreement の略称）

SLO …… サービス事業者がサービスの品質について目標を定めたもの。SLA を達成するための具体的な施策、手続きと指標。（Service Level Objective の略称）

UPS…… 商用電源が短時間停電しても蓄電池から電力を供給し、運転を継続させる機能とともに CVCF（定電圧定周波装置）の機能を備えた装置（Uninterruptible Power Supply: 無停電電源装置の略称）

インシデント…… 事件や事故のことをいうが、IT の分野ではサイバー攻撃や内部不

正行為といった、コンピュータやネットワークのセキュリティを脅かす事象をいう。

インストアブランチ…… ショッピングセンターやスーパーマーケット等のストア（店舗）の中に設置してある金融機関等の店舗

オープンネットワーク…… インターネットに代表される、不特定多数の相手との自由な接続、通信が可能なネットワーク

オペレータ…… コンピュータセンターにおけるコンピュータ操作者

オンプレミス…… 情報システムを自社で保有し、自社の設備において運用すること。

クラウド…… 米国の NIST（National Institute of Standards and Technology：国立標準技術研究所）におけるクラウドの定義を採用する。

【NIST におけるクラウドの定義】

最小限の管理負荷やプロバイダー交渉だけで、迅速に提供され稼働する構成変更自在のコンピュータ資源（ネットワーク、サーバー、記憶装置、サービス等）の共有プールに対する、ネットワークを通じた便利で随時のアクセスを可能とするモデル。代表的なサービスの提供形態としては、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）、SaaS（Software as a Service）などが挙げられる。

コンビニ ATM …… 金融機関がコンビニエンスストア内に設置した ATM

コンピュータシステム…… コンピュータ、端末機器、周辺装置、通信系装置、回線及びプログラム等の全部または一部により構成されるデータを処理するためのシステム。非中央集中型の分散処理システム（クライアント・サーバーシステム等）を含む。

サイバー攻撃…… 重要インフラの基幹をなす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いう。

手法としては、コンピューターウイルスやスパムの大量送信、ネットワークへの不正侵入と破壊、ウェブサイトの改ざんなどが挙げられる。

サーバー…… LAN 等のネットワークで接続されたシステムにおいて、他のコンピュータにファイルやデータ、プログラム等（サービス）を提供するコンピュータ

スマートデバイス…… スマートフォン及び同様の機能を具備するタブレット型端末の総称

セキュリティホール…… 本来の接続手順を踏まずにアクセスを許してしまうなどの、システムやネットワーク管理ソフトウェア等におけるセキュリティ上の弱点（穴）

セキュリティポリシー…… 全社統一の基本方針として、保護すべき情報資産、保護する目的及び責任の所在を定めたもの。

セキュリティスタンダード… セキュリティポリシーを実行に移すための具体的対策を記述したもの。自社の安全対策基準。

セグメント…… 物理的、論理的に区切ることのできるネットワークの単位。セグメントに設置されたネットワーク機器（ルーター、ハブ等）に、ユーザーのアクセス権限等の条件を設定しておくことにより、ネットワークを効率的に運用したり、無権限者のアクセスを排除したりすることができる。

ゼロ暗証化…… スキミング（カードの磁気に記録されている各種データ（会員番号や口座番号など）を不正に読み取る行為）への対策として、暗証番号を磁気カードから取り除いたカードへの切り替や、カードの磁気データの一部を NULL 等に置き換える対応をいう。

ダイレクトチャネル…… オープンネットワークを利用したインターネットやモバイル、または電話などにより、金融サービスを営業店等を通さずに顧客に直接提供する方法の総称

デジタルフォレンジック[25]… 電子機器や電子記録媒体内にある電子データを分析して、不正行為等の証拠を見つけ出す手法のこと。（単に「フォレンジック」または「フォレンジクス」として使用される場合もある）

デビットカード…… 利用代金を顧客の口座から即時に引き落とし、利用店の口座に入金する即時決済サービスを提供可能なカードサービス

トークン化…… ある数列を元の数列と全く関連のない数列に置き換える技術のこと。トークン化されたデータ自体は無意味な数列にすぎず、数学的な解析処理がなされて復号されてしまうようなリスクがない。

トレーサビリティ…… 追跡可能性のこと。インシデント発生時に、後から要因を追跡できる状態にあること。

パスワード…… ネットワークやシステム等を利用する際に使用する、本人を認証するための、本人しか知り得ない文字列

パターンファイル…… 抗ウイルスソフトなどがコンピュータウイルスを検出するために必要とする、コンピュータウイルスの特徴等の情報が記述されているファイルのこと。最新のコンピュータウイルスに対応するために、頻繁に更新することが必要。

パッケージ…… 特定の業務用にあらかじめ作成され、市販されているソフトウェア

パッチ…… メインフレーム、サーバー、パソコン等の機器にインストールされている OS やパッケージソフトウェア等のソフトウェア製品に対して、不具合の修正や機能変更を行うためにプログラムの一部を更新するデータのこと。同義語として PTF（Program Temporary Fix）、ホットフィックス、アップデータ等がある。特に、セキュリティの脆弱性を修正するためにリリースされるパッチについては、セキュリティパッチまたは修正パッチと呼ばれて

[25] 「犯罪の立証のための電磁的記録の解析技術及びその手続」（平成 26 年警察白書）より。なお、サイバー攻撃の実態解明を目的に、ログ等の解析を通して攻撃プロセスを特定していく「ネットワークフォレンジック」と呼ばれる手法もある。（『改訂版デジタル・フォレンジック事典』デジタル・フォレンジック研究会（平成 12 年））

いる。

ファイアウォール…… インターネット等の外部ネットワークから内部ネットワークに対する侵入を防ぐために設置されるハードウェア、又はその機能を実現するソフトウェア

ファイル…… 記録媒体、または記憶装置に記録されているデータ及びプログラム

ブルートフォース攻撃…… 暗号やパスワードを解読、解析するための手法のひとつ。特定のIDに対し、パスワードに使用され得る文字列を総当り的に入力して、有効な組み合わせを発見しようとする(総当たり攻撃)。なお、パスワードを固定してユーザーIDを変更することで、不正ログインを試みる手法をリバースブルートフォース攻撃という。

ベンダーロックイン…… 特定事業者の独自技術に依存した製品、サービス、システム等を採用し、他の事業者への乗換えが困難な状態になること。

ホワイトペーパー…… ベンダーみずからが作成するセキュリティに関する情報の開示・レポート等

暗号鍵…… データ等を暗号化する際、暗号化方式が定める計算手順に与えるパラメータのこと。

暗証番号…… ATMやパソコン、モバイル端末で本人確認のために入力する数字

外部委託…… システム開発、システム運用、情報処理等の業務の全部または一部を外部の事業者に委託すること。なお、共同センターやクラウドサービスの利用も外部委託に含まれる。

外部委託先…… 業務を委託する事業者または、サービスを提供する事業者。なお外部委託先には再委託先を含む。また、再委託先には再々委託以下の階層を含む。

可搬型記憶媒体…… パソコン又はその周辺機器に挿入又は接続して情報を保存. することができる媒体又は機器のうち、可搬型のものをいう。
CD-ROM、USBメモリ、ポータブルハードディスク等

金融サービス…… 金融機関等が業法に基づき顧客に提供するサービス

金融関連サービス…… 金融サービスを補完するため、金融機関等以外の事業者が提供するサービス

金融機関等…… 銀行等の預金取扱金融機関、信託会社、保険会社、証券会社、クレジット会社等をいう。ただし、電子決済等代行業者などのFinTech企業等を除く。

空調設備…… コンピュータ室等の空気調和（温度・湿度・清浄度などの室内環境の調節）をするための空気調和機、冷却塔及びその付属設備

経営層…… 取締役会（理事会）等

顧客データ…… 業務上収集、蓄積、利用される顧客に関するデータ
データの範囲は、保有するすべての個人情報（氏名、生年月日、取引内容等）及び法人情報（代表者、決算内容、取引内容等）

個人情報[26]……	生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日、その他の記述等により特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別できるものを含む）をいう。
個人データ……	個人情報データベース[27]等を構成する個人情報
自動機器室……	CD・ATM などの現金自動支払機等を設置するコーナー、室
周辺装置……	磁気ディスク装置、磁気テープ装置、コンソールディスプレイ、プリンター等の総称
渉外端末……	ハンディ端末、スマートデバイス、携帯型パソコン等、主に渉外担当者が携帯し、店舗外で利用されるコンピュータ機器
端末機器……	コンピュータに接続される、窓口装置、自動機器、ワークステーション、パソコン等の機器
端末系装置……	コンピュータシステムを利用するための入出力インタフェースとなる窓口装置、パソコン、渉外端末等の機器及びそれらを制御する装置の総称
通信系装置……	ホストコンピュータを中心とするシステムでは通信制御装置等、サーバを中心とするシステムではルーター等
提携チャネル……	デビットカード及びコンビニ ATM 等の総称
電源設備……	コンピュータシステム等を作動させるための受電設備、UPS（無停電装置）、自家発電設備等の設備及びその付属設備
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、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。電子署名は、本人確認のほか、改ざんの防止、取引否認の防止にも有効である。なお、電子署名法上の電子署名はデジタル署名に限られない。
匿名加工情報[28]……	特定の個人を識別できる記述等から全部又はその一部を削除するあるいは他の記述等に置き換えることによって、特定の個人が識別されないよう加工されたもの。
なりすまし……	他人のユーザーID やパスワード等を使い、本人であると偽ってネットワーク又はコンピュータシステムに侵入したり、ネットワークを介した商取引等を行ったりすること。
防犯カメラ……	状況監視を行うためのテレビカメラ
防犯ビデオ……	防犯カメラの映像、音声等の記録
不正アクセス[29]……	不正な手段により、ユーザー以外の者が行うアクセスまたはユーザーが行う権限外のアクセス
本体装置……	中央処理装置、主記憶装置、チャネル装置等の総称

[26] 「個人情報」、「個人データ」の定義の詳細については、金融庁告示『金融分野における個人情報保護に関するガイドライン』を参照。
[27] 「個人情報データベース」とは、個人情報を含む情報の集合物であって、特定の個人情報をコンピュータを用いて検索できるように体系的に構成したもの。
[28] 個人情報保護法（法 36 条 1 項）及び個人情報保護委員会規則（19 条）に準拠。
[29] 不正アクセス行為の禁止等に関する法律（平成 12 年 2 月 13 日施行。平成 25 年 5 月 31 日改正。）に準拠。

無人店舗…… CD・ATM 等の自動機器のみで運用を行う店舗

４．参考文献等

安全対策基準を作成するにあたって参考とした文献等は以下のとおりである。

(1) 「金融分野における個人情報保護に関するガイドライン」　金融庁 平成 16 年 12 月
「金融分野における個人情報保護に関するガイドライン」の一部改正　個人情報保護委員会、金融庁 平成 29 年 2 月

(2) 「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関する実務指針」　金融庁 平成 17 年 1 月
「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関する実務指針」の一部改正　個人情報保護委員会、金融庁 平成 29 年 2 月

(3) 「金融検査評定制度（預金等受入機関に係る検査評定制度）」　金融庁 平成 17 年 7 月

(4) 「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～偽造・盗難キャッシュカード被害発生の予防策・被害拡大の抑止策を中心として～」　金融庁 平成 17 年 6 月

(5) 「金融機関における情報セキュリティの重要性と対応策」　日本銀行 平成 12 年 4 月

(6) 「金融機関業務のアウトソーシングに際してのリスク管理」　日本銀行 平成 13 年 4 月

(7) 「わが国金融機関におけるシステムリスクの管理状況と留意点」　日本銀行 平成 13 年 9 月

(8) 「金融機関の拠点被災を想定した業務継続計画のあり方」　日本銀行 平成 14 年 3 月

(9) 「金融機関における業務継続体制の整備について」　日本銀行 平成 15 年 7 月

(10) 「金融機関の防犯基準」　警察庁 平成 11 年 10 月

(11) 「コンビニエンスストア・スーパーマーケットの防犯基準」　警察庁 平成 15 年 12 月

(12) 「単体で設置される現金自動預支払機（ATM）等の防犯基準」　警察庁 平成 15 年 7 月

(13) 「現金自動支払機等の防犯基準」　警察庁 平成 3 年 6 月

(14) 「情報システム安全対策指針」　警察庁 平成 11 年 11 月

(15) 「CD 等の技術的防犯対策について」　日本自動販売機工業会 金融システム部会 平成 2 年 6 月

(16) 「ガラスの防犯性能に関する板硝子協会基準」　板硝子協会 平成 14 年 3 月

(17) 「VDT 作業における労働衛生管理のためのガイドライン」　厚生労働省 平成 14 年 4 月

(18) 「情報通信ネットワーク安全・信頼性のガイドライン」　平成 7 年 4 月
（編集）郵政省電気通信局電気通信事業部電気通信技術システム課
（発行）財団法人 日本データ通信協会

(19) 「情報通信ネットワーク安全・信頼性基準」　郵政省 平成 6 年郵政省告示第 638 号
「情報通信ネットワーク安全・信頼性基準」の一部改正　総務省 平成 16 年総務省告示第 244 号

(20) 「重要インフラの情報セキュリティ対策に係る行動計画」　内閣官房情報セキュリティセンター 平成 17 年 12 月

(21) 「コンピュータウイルス対策基準解説書」　平成 7 年 7 月
（監修）通商産業省機械情報産業局 （発行）財団法人 日本情報処理開発協会
（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）

(22) 「システム監査基準解説書」　平成 16 年 10 月
（監修）経済産業省商務情報政策局 （発行）財団法人 日本情報処理開発協会

(23)「システム管理基準解説書」　平成 16 年 10 月
（監修）経済産業省商務情報政策局 （発行）財団法人 日本情報処理開発協会
(24)「コンピュータ不正アクセス対策基準解説書」　平成 8 年 11 月
（監修）通商産業省機械情報産業局 （発行）財団法人 日本情報処理開発協会
（コンピュータ不正アクセス対策基準：平成 12 年通商産業省告示第 950 号）
(25)「コンピュータセキュリティ基本要件」　社団法人 電子情報技術産業協会 平成 9 年 8 月
(26)「金融機関向け防犯カメラの性能基準」　社団法人 日本防犯設備協会 平成 16 年 3 月
(27)「情報システムの設備ガイド」　社団法人 電子情報技術産業協会 平成 26 年 3 月
(28)「IS(Information Systems)検査ハンドブック」　FFIEC（米国連邦金融機関検査協議会）2002 年
(29)「電子バンキングにおけるリスク管理の原則」　バーゼル銀行監督委員会 2003 年 7 月
(30)「BIOVISION, Privacy Best Practices in Deployment of Biometric Systems」 2003 年 8 月
(31)「全銀協 IC キャッシュカード標準仕様」　全国銀行協会 平成 13 年 3 月
(32)「暗号技術検討会　2002 年度報告書」　暗号技術検討会 平成 15 年 3 月
(33)「金融機関等のシステム監査指針」　財団法人 金融情報システムセンター 平成 19 年 3 月
(34)「ATM 等の技術的防犯対策について」　日本自動販売機工業会 金融システム委員会 平成 12 年 12 月
(35)「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」　内閣官房情報セキュリティセンター 平成 21 年 2 月
(36)「電子政府推奨暗号の利用方法に関するガイドブック」 独立行政法人 情報通信研究機構、独立行政法人 情報処理推進機構 平成 20 年 3 月
(37)「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 平成 22 年 4 月
(38)「共通フレーム 2007―経営者、業務部門が参画するシステム開発および取引のために」 独立行政法人 情報処理推進機構ソフトウェア・エンジニアリング・センター 平成 21 年 10 月
(39)「安全なウェブサイトの作り方」独立行政法人 情報処理推進機構セキュリティセンター 平成 22 年 1 月
(40)「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 平成 19 年 3 月
(41)「バックアップ・コンピュータセンターの実効性確保にかかる課題と対応策」 日本銀行 平成 22 年 3 月
(42)「金融機関におけるサイバー攻撃対応に関する有識者検討会報告書」 公益財団法人 金融情報システムセンター 平成 26 年 2 月
(43)「金融機関におけるクラウド利用に関する有識者検討会報告書」 公益財団法人 金融情報システムセンター 平成 26 年 11 月
(44)「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 改定版」 内閣官房情報セキュリティセンター 平成 24 年 4 月
(45)「金融機関等防犯カメラシステムの設計基準・解説」 公益社団法人 日本防犯設備協会 平成 26 年 11 月

(46)「金融機関における外部委託に関する有識者検討会報告書」 公益財団法人 金融情報システムセンター 平成 28 年 6 月
(47)「金融機関における FinTech に関する有識者検討会報告書」 公益財団法人 金融情報システムセンター 平成 29 年 6 月
(48)「金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書」公益財団法人 金融情報システムセンター 平成 30 年 3 月

Ⅳ．安全対策基準一覧表

１．構成一覧

Ⅰ　統制基準

基準大項目		基準中項目	
1 内部の統制	内部の統制を行うために必要となる規程・体制の整備等に関する基準項目。	(1)方針・計画	システムの安全対策を適切に実施するために必要となる基本方針の整備及び、必要な経営資源を考慮した中長期のシステム計画の策定に関する基準項目。
		(2)組織体制	システムの安全対策を適切に実施するために必要な組織体制の整備（責任者の選任、所管部署の整備、各種規則の整備等）に関する基準項目。
		(3)管理状況の評価	セキュリティ関連文書に定められた事項について、その遵守状況の確認及び評価に関する基準項目。
		(4)人材（要員・教育）	システムの開発・変更及び運用に携わる要員の人事管理、健康管理及び、要員に対し実施するセキュリティ教育及び訓練に関する基準項目。
2 外部の統制	外部の統制を行うために実施すべき外部委託管理等に関する基準項目。	(1)外部委託管理	外部委託管理を適切に行うために必要な、利用検討時、契約時、運用時における対策、管理体制の整備に関する基準項目。
		(2)クラウドサービスの利用	クラウドサービスを利用する場合における、金融機関等が実施すべき対策及び、考慮すべき事項に関する基準項目。
		(3)共同センター	勘定系システムで共同センターを利用する場合における、緊急事態の発生に備えた安全対策に関する基準項目。

基準大項目		基準中項目	
2 外部の統制		(4)金融機関相互のシステム・ネットワークのサービス	金融機関相互のシステム・ネットワークのサービスを利用する場合において実施すべき対策及び考慮すべき事項に関する基準項目。

Ⅱ　実務基準

基準大項目		基準中項目	
1 情報セキュリティ	顧客データ漏えい防止、改ざんの防止、システムの不正使用の防止等、情報セキュリティに関する基準項目。	(1)データ保護	データの漏えい、破壊、改ざんの防止及び、暗号鍵の適切な管理等、データ保護に関する基準項目。
		(2)不正使用防止	不正取引、データやソフトウェアの改ざん等の防止、アクセス権限の確認、利用範囲の制限等、システムの不正使用防止に関する基準項目。
		(3)外部ネットワークからの不正アクセス防止	ネットワークを介した外部からの不正アクセスの防止等、外部からのアクセスにおいて実施すべき対策に関する基準項目。
		(4)不正検知策	不正アクセスを早期に発見するための監視機能や、異例取引・不正取引の監視・検知等に関する基準項目。
		(5)不正発生時の対応策	不正アクセス、不正使用を検知した際、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ために実施すべき対策に関する基準項目。
		(6)不正プログラム対策	システムの安全性確保を目的に、不正プログラム等のシステムへの侵入または組込みを防止するための対策に関する基準項目。
2 システム運用共通	システムの運用部門（主に委託先）及び利用部門（金融機関等）が実施すべき基準項目。	(1)マニュアルの整備	システムを正確かつ安全に運用するための通常時及び障害・災害時における各種運用手順等のマニュアルの整備に関する基準項目。

基準大項目		基準中項目	
2 システム運用共通	システムの運用部門（主に委託先）及び利用部門（金融機関等）が実施すべき基準項目。	(2)アクセス権限の管理	システムを構成する機器、データ等の各種資源に対する破壊及び、不正使用を防止するためのアクセス権限の設定等に関する基準項目。
		(3)データ管理	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に実施すべきデータファイルの授受・保管における管理手順及び、暗号鍵等の管理手順等に関する基準項目。
		(4)オペレーション習熟	システムや端末の誤操作による事故を防止するために実施すべき、コンピュータセンター等におけるシステムのオペレーション及び、営業店等における端末操作に関する教育及び訓練に関する基準項目。
		(5)コンピュータウイルス対策	コンピュータウイルス等の不正プログラムによる情報漏えい、プログラムの改ざん、破壊等を防止するために実施すべき、不正プログラムの侵入防止策及び、侵入した場合の検知策に関する基準項目。
		(6)外部接続管理	不正アクセス、データ漏えい等を防止を目的とした、接続先の正当性の確認及び、外部接続管理等に関する基準項目。
3 運行管理	日々のシステム運行にあたり、システムの運用部門（主に委託先）が実施すべき基準項目。	(1)オペレーション管理	システムの運用を安全・円滑に行うために必要となるオペレーション管理（作業依頼、承認、実行、記録、結果確認等）に関する基準項目。
		(2)データファイル管理	障害・災害、サイバー攻撃等による破壊・改ざんに備えて実施すべき、データファイルのバックアップ等に関する基準項目。
		(3)プログラムファイル管理	プログラムファイルの適切な管理及び、障害・災害等の発生に備えたプログラムのバックアップ等に関する基準項目。

基準大項目		基準中項目	
3 運行管理	日々のシステム運行にあたり、システムの運用部門（主に委託先）が実施すべき基準項目。	(4)ネットワーク設定情報管理	ネットワーク設定情報の不正な改ざんを防止するために実施すべき、ネットワーク設定情報の管理、障害・災害等の発生に備えたバックアップの確保に関する基準項目。
		(5)運用時ドキュメント管理	不正使用、紛失等を防止するために実施すべき、ドキュメントの管理、障害・災害等の発生に備えたバックアップの確保に関する基準項目。
		(6)運行監視	異常状態の早期発見のために実施すべき、システムの運行監視に関する基準項目。
4 各種設備管理	コンピュータ機器や能力の管理を行うために、システムの運用部門（主に委託先）が実施すべき基準項目	(1)資源管理	システムの障害、処理能力の低下を回避するために実施すべき、各種資源の容量・能力等の把握に関する基準項目。
		(2)機器の管理	ハードウェア・ソフトウェア等の障害及び不正使用・破壊・盗難等の防止など、システムの信頼性向上のために実施すべき、コンピュータ本体及び周辺機器の障害発生を抑制に関する基準項目。
		(3)コンピュータ関連設備の保守管理	コンピュータシステムを円滑に運用するために実施すべき、電源、空調、給排水、防災、防犯、監視、回線関連等の設備の管理及び、各種設備の容量・性能及び使用状況の把握に関する基準項目。
		(4)入退館（室）管理	不法侵入、危険物持込み、不法持出し等を防止するために実施すべき、コンピュータセンターやコンピュータ室等重要な室における入退室管理及び、入室者の作業管理に関する基準項目。
		(5)監視	異常状態の早期発見のために実施すべき、システムの稼働に必要な各種設備の稼働状況の監視等に関する基準項目。

基準大項目		基準中項目	
5 システムの利用	システムの適切な利用及び顧客データを保護するために利用部門（金融機関）が実施すべき基準項目	(1)取引の管理	端末機操作による不正、不当取引を防止するために実施すべき、取引の操作内容の記録・検証及び、顧客からの届出の受付体制の整備に関する基準項目。
		(2)入出力管理	データの完全性を確保するために必要となるデータの入力管理ルールの作成及び、出力情報の不正使用の防止及び、顧客データを保護するために必要となる出力情報の管理ルールの作成に関する基準項目。
		(3)帳票管理	帳票の不正使用及び漏えいを防止するために実施すべき、帳票の管理及び廃棄手続きに関する基準項目。
		(4)顧客データ保護	顧客データを保護するために実施すべき、管理手順の策定及び管理体制の整備等に関する基準項目。
6 緊急時の対応	システムの管理部門、運用部門及び利用部門において、緊急事態の発生に備え実施すべき基準項目。	(1)障害時・災害時対応策	システムの障害や災害時に顧客、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に実施すべき、障害・災害時対応策に関する基準項目。
		(2)コンティンジェンシープランの策定	障害・災害が発生した際に必要となる、コンティンジェンシープラン（緊急時対応計画）の策定に関する基準項目。
		(3)バックアップサイト	コンピュータセンターが災害等により機能しなくなった場合に備えた、バックアップサイトの設置に関する基準項目。

基準大項目		基準中項目	
7 システム開発・変更	システム開発部門が、システムの安全性を確保するために実施すべき基準項目。	(1)システム開発・変更管理	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に実施すべき、システム開発・変更手順及びテスト環境の整備に関する基準項目。
		(2)開発・変更時ドキュメント管理	システム開発及び変更作業を円滑に行うとともに、改ざん、不正使用を防止するために実施すべき、システム開発・変更に係わるドキュメントの管理に関する基準項目。
		(3)パッケージの導入	パッケージを導入する場合に実施すべき、パッケージの信頼性・生産性・既存システムとの親和性等の評価及び、パッケージの運用・管理体制の整備に関する基準項目。
		(4)システムの廃棄	システムの廃棄時における情報漏えい及び不正防止等のために実施すべき、廃棄計画の作成及び廃棄手順に関する基準項目。
8 システムの信頼性向上対策	システムの安定運用及び品質向上など、システムの信頼性向上のために実施すべき基準項目。	(1)ハードウェアの予備	コンピュータシステムの信頼性を向上させるために実施すべき、ハードウェア構成の冗長化等に関する基準項目。
		(2)ソフトウエアの品質向上対策	システムの信頼性向上のために実施すべき、設計工程や製造工程及び本番適用段階におけるソフトウェアの品質向上に関する対策及び、パッケージ等の利用にあたり検討すべき事項に関する基準項目。
		(3)運用時の信頼性向上対策	システムの運用時における信頼性向上を図るために実施する、オペレーションの自動化・簡略化及び、システムの処理結果の妥当性・正当性のチェック機能等の充実に関する基準項目。
		(4)障害の早期発見・回復機能	障害が発生した際に、障害状況を検知・把握し、その影響を最小限に抑え、速やかに回復するための機能及び管理方法に関する基準項目。

基準大項目		基準中項目	
9 個別業務・サービス	個別業務・サービスにおいて実施すべき基準項目。	(1)カード取引サービス	カード取引サービスに係る事故・犯罪を防止し、安心・安全なサービスを提供するために実施すべき、カード管理及びカード取引の監視に関する基準項目。
		(2)インターネット・モバイルサービス	利用者との取引の安全性を確保するために実施すべき、インターネット・モバイルサービスにおける脅威への対策及び、サービス利用における顧客への注意喚起等の対策に関する基準項目。
		(3)渉外端末の管理	顧客データ保護及びシステム機器保護の観点から実施すべき、渉外端末等の可搬型端末の管理（端末の破損、紛失、盗難等に備えた対策等）に関する基準項目。
		(4) CD・ATM 等及び無人店舗の管理	CD･ATM 等及び無人店舗における犯罪の未然防止、システム機器等の保護に必要となる各種予防策及び、障害・災害や犯罪発生時の対応方法を定めたマニュアル等の整備に関する基準項目。
		(5)インストアブランチ	インストアブランチにおける安全性を確保するために実施すべき、出店先地域やストアの選定基準等に関する基準項目。
		(6)コンビニ ATM	コンビニ ATM の利用者及びメンテナンス要員等の安全確保に関する基準項目。
		(7)デビットカード・サービス	デビットカード・サービスの安全性を確保するために実施すべき、サービスの提供形態に応じた情報処理センターや加盟店等との総合的な対策及び、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の顧客保護に関する基準項目。

基準大項目		基準中項目	
9 個別業務・サービス	個別の業務・サービスにおいて実施すべき基準項目。	(8)前払式支払手段	プリペイドカード等の前払式支払手段を利用する際の安全性を確保するために実施すべき、不正検知等の対策及び、不正利用に関する利用者への注意喚起等に関する基準項目。
		(9)電子メール・イントラネットの利用	電子メールを利用したサービスを行う場合において必要となる運用方針の策定及び、電子メールの送受信やホームページの閲覧等によりデータ漏えい等の発生を防止するために必要な対策に関する基準項目。
		(10)生体認証	生体認証を用いる場合に必要となる、生体認証情報の入手・保管における安全管理及び、生体認証の導入・運用において必要な対策に関する基準項目。

Ⅲ　設備基準

基準大項目		基準中項目	
1 コンピュータセンター	コンピュータセンターの建物・付帯施設及び設備に関する基準項目。	(1)建物(環境)	コンピュータセンターの建物において、災害、障害が発生した場合に被害を最小限にとどめ迅速に復旧させるために必要となる、立地環境の調査、建物周囲の状況ごとに講ずるべき対策等に関する基準項目。
		(2)建物(周囲)	
		(3)建物(構造)	
		(4)建物(開口部)	
		(5)建物(内装等)	
		(6)コンピュータ室・データ保管室(位置)	コンピュータ室・データ保管室に収容されているネットワーク機器及び、データ記録媒体等の安全性を確保するために実施すべき、自然災害または不正行為等に対する対策に関する基準項目。
		(7)コンピュータ室・データ保管室(開口部)	

基準大項目		基準中項目	
1 コンピュータセンター	コンピュータセンターの建物・付帯施設及び設備に関する基準項目。	(8)コンピュータ室・データ保管室(構造・内装等)	コンピュータ室・データ保管室に収納されているネットワーク機器及び、データ記録媒体等の安全性を確保するために実施すべき、自然災害及び不正行為等に対する対策に関する基準項目。
		(9)コンピュータ室・データ保管室(設備)	
		(10)コンピュータ室・データ保管室(コンピュータ機器、什器・備品)	
		(11)電源室・空調機械室	電源室及び空調機械室における障害等の早期発見と被害を最小限にとどめるための対策に関する基準項目。
		(12)電源設備	停電、異常電圧、異常周波数、電源の瞬断、過電流、漏電及び電源設備自体の障害によりシステムの運用に影響を及ぼさないために、異常検知や災害等に対する対策に関する基準項目。
		(13)空調設備	空調設備を安定的に運用するための対策及び、空調設備が建物外に設置されることを想定した外部からの侵入防止等の対策に関する基準項目。
		(14)監視制御設備	監視制御設備において必要となる、電源設備、空調設備、防災設備、防犯設備等の監視機能及び、異常等の速やかな発見・通報等を可能とするために必要となる機能に関する基準項目。
		(15)回線関連設備	回線関連設備において必要となる、通信回線の保護策及び、システムへの不正アクセス等を防止するための対策に関する基準項目。

基準大項目		基準中項目	
2 本部 ・営業店等	本部・営業店等の建物・付帯施設及び設備に関する基準項目	(1)建物(周囲)	システムの安定稼働のために、本部・営業店等において実施すべき、設備面の対策、及び自動機器等の無人運用を行う場合（店舗外現金自動設備を含む）における、周辺環境を考慮した防犯・防災対策に関する基準項目。
		(2)建物(構造)	
		(3)建物(開口部)	システムの安定稼働のために、本部・営業店等において実施すべき、設備面の対策、及び自動機器等の無人運用を行う場合（店舗外現金自動設備を含む）における、周辺環境を考慮した防犯・防災対策に関する基準項目。
		(4)建物(内装等)	
		(5)建物(設備)	
		(6)建物(回線関連設備)	
		(7)建物(電源設備)	
		(8)建物(空調設備)	
		(9)建物(自動機器室)	
		(10)建物(端末機器)	
		(11)サーバー設置場所（位置）	コンピュータ室外（本部・営業店等）に設置されるシステムにおいて、サーバーを主体とした装置構成の盗難・破壊等を想定した、サーバー設置等において考慮すべき事項に関する基準項目。
		(12)サーバー設置場所（構造・内装等）	
		(13)サーバー設置場所（設備）	
		(14)インストアブランチ	インストアブランチにおいて、ストアの既設設備の利用または、ストア等との営業時間が異なる場合があることを想定した、設備の防犯対策、破壊侵入等の防御に関する基準項目。
3 流通・小売店舗との提携チャネル	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基準項目。	(1)コンビニ ATM	コンビニ ATM の特性として、不特定多数の人が行き来する場所に機器が単体で設置されることが多い点を踏まえた、強化すべき防犯対策に関する基準項目。

Ⅳ　監査基準

基準大項目		基準中項目	
1 システム監査	システムの監査体制の整備に関する基準項目。	(1)システム監査	システムの有効性、効率性、信頼性、遵守性、安全性を確保するために必要となる、システム監査体制の整備に関する基準項目。

２. 基準一覧

Ⅰ　統制基準

◎：適用が必要
○：適用が望ましい

基準大項目	基準中項目	基準番号	基準小項目	旧基準番号（第８版）	基準分類	適用区分				
						共通（建物、チャネルに依存せず適用）	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
1 内部の統制										
	(1)方針・計画	統 1	システムの安全対策に係る重要事項を定めた規程を整備すること。	運 1・2	基礎	◎				
		統 2	中長期的視点に立ったシステムの企画・開発・運用に関する計画を策定すること。	（新設）	基礎	◎				
	(2)組織体制	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	基礎	◎				
		統 4	セキュリティ管理体制を整備すること。	運 3	基礎	◎				
		統 5	サイバー攻撃対応態勢を整備すること。	運 113	基礎	◎				
		統 6	システム管理体制を整備すること。	運 4	基礎	◎				
		統 7	データ管理体制を整備すること。	運 5	基礎	◎				
		統 8	ネットワーク管理体制を整備すること。	運 6	基礎	◎				
		統 9	業務組織を整備すること。	運 9	基礎		◎	◎		
		統 10	防災組織を整備すること。	運 7	基礎		◎	◎		
		統 11	防犯組織を整備すること。	運 8	基礎		◎	◎		
		統 12	各種業務の規則を整備すること。	運 10	基礎	◎				
	(3)管理状況の評価	統 13	セキュリティ遵守状況を確認すること。	運 10-1	基礎	◎				
	(4)人材（要員・教育）	統 14	セキュリティ教育を行うこと。	運 80	基礎	◎				
		統 15	要員に対するスキルアップ教育を行うこと。	運 81	基礎	◎				
		統 16	障害時・災害時に備えた教育・訓練を行うこと。	運 83	基礎	◎				
		統 17	防災・防犯訓練を行うこと。	運 84	基礎	◎				
		統 18	要員の人事管理を行うこと。	運 85	基礎	◎				
		統 19	要員の健康管理を行うこと。	運 86	基礎	◎				
2 外部の統制										
	(1)外部委託管理	統 20	外部委託を行う場合は、事前に目的や範囲等を明確にするとともに、外部委託先選定の手続きを明確にすること。	運 108 他	基礎	◎				
		統 21	外部委託先と安全対策に関する項目を盛り込んだ契約を締結すること。	運 109 他	基礎	◎				
		統 22	外部委託先の要員にルールを遵守させ、その遵守状況を確認すること。	運 89	基礎	◎				
		統 23	外部委託における管理体制を整備し、委託業務の遂行状況を確認すること。	運 90	基礎	◎				

基準大項目	基準中項目	基準番号	基準小項目	旧基準番号（第８版）	基準分類	適用区分				
						共通（建物、チャネルに依存せず適用）	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
	(2)クラウドサービスの利用	統 24	クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること。	新設	基礎	◎				
	(3)共同センター	統 25	共同センターにおける緊急事態の発生に備えて安全対策を講ずること。	新設	基礎	◎				
	(4)金融機関相互のシステム・ネットワークのサービス	統 26	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	基礎	◎				

Ⅱ　実務基準

基準大項目	基準中項目	基準番号	基準小項目	旧基準番号（第８版）	基準分類	適用区分				
						共通（建物、チャネルに依存せず適用）	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
1 情報セキュリティ										
	(1) データ保護	実 1	他人に暗証番号・パスワード等を知られないための対策を講ずること。	技 26	基礎	◎				
		実 2	相手端末確認機能を設けること。	技 27	付加	◎				
		実 3	蓄積データの漏洩防止策を講ずること。	技 28	付加	◎				
		実 4	伝送データの漏洩防止策を講ずること。	技 29	付加	◎				
		実 5	ファイルに対するアクセス制御機能を設けること。	技 31	基礎	◎				
		実 6	不良データ検出機能を充実すること。	技 32	基礎	◎				
		実 7	伝送データの改ざん検知策を講ずること。	技 33	付加	◎				
	(2) 不正使用防止	実 8	本人確認機能を設けること。	技 35	基礎	◎				
		実 9	ID の不正使用防止機能を設けること。	技 36	基礎	◎				
		実 10	アクセス履歴を管理すること。	技 37	基礎	◎				
		実 11	取引制限機能を設けること。	技 38	基礎	◎				
		実 12	事故時の取引禁止機能を設けること。	技 39	付加	◎				
		実 13	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	付加	◎				
	(3) 外部ネットワークからの不正アクセス防止	実 14	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	基礎	◎				
		実 15	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	基礎	◎				
	(4) 不正検知策	実 16	不正アクセスの監視機能を設けること。	技 45	基礎	◎				
		実 17	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	付加	◎				
		実 18	異例取引の監視機能を設けること。	技 47	付加	◎				

基準大項目	基準中項目	基準番号	基準小項目	旧基準番号（第８版）	基準分類	適用区分				
						共通（建物、チャネルに依存せず適用）	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
	(5) 不正発生時の対応策	実 19	不正アクセスの発生に備えて対応策、復旧策を講ずること。	技 48	基礎	◎				
	(6) 不正プログラム対策	実 20	コンピュータウイルス等の不正プログラムへの防御対策を講ずること。	技 49	基礎	◎				
		実 21	コンピュータウイルス等の不正プログラムの検知対策を講ずること。	技 50	基礎	◎				
		実 22	コンピュータウイルス等の不正プログラムによる被害時対策を講ずること。	技 51	基礎	◎				
2 システム運用共通										
	(1) マニュアルの整備	実 23	通常時マニュアルを整備すること。	運 14	基礎	◎				
		実 24	障害時・災害時マニュアルを整備すること。	運 15	基礎	◎				
	(2) アクセス権限の管理	実 25	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	基礎	◎				
		実 26	パスワードが他人に知られないための措置を講ずること。	運 17	基礎	◎				
		実 27	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にすること。	運 18	基礎	◎				
	(3) データ管理	実 28	データファイルの授受・管理方法を明確にすること。	運 25	基礎	◎				
		実 29	データファイルの修正管理方法を明確にすること。	運 26	基礎	◎				
		実 30	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	基礎	◎				
	(4) オペレーション習熟	実 31	オペレーション習熟のための教育及び訓練を行うこと。	運 82	基礎	◎				
	(5) コンピュータウイルス対策	実 32	コンピュータウイルス対策を講ずること。	運 30	基礎	◎				
	(6) 外部接続管理	実 33	接続契約内容を明確にすること。	運 55	基礎	◎				
		実 34	外部接続における運用管理方法を明確にすること。	運 56	基礎	◎				
3 運行管理										
	(1) オペレーション管理	実 35	オペレータの資格確認を行うこと。	運 19	基礎		◎			
		実 36	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	基礎		◎	◎		
		実 37	オペレーション実行体制を明確にすること。	運 21	基礎		◎	◎		
		実 38	オペレーションの記録、確認を行うこと。	運 22	基礎		◎	◎		
	(2) データファイル管理	実 39	データファイルのバックアップを確保すること。	運 27	基礎	◎				
	(3) プログラムファイル管理	実 40	プログラムファイルの管理方法を明確にすること。	運 28	基礎	◎				
		実 41	プログラムファイルのバックアップを確保すること。	運 29	基礎	◎				
	(4) ネットワーク設定情報管理	実 42	ネットワークの設定情報の管理を行うこと。	運 31	基礎	◎				
		実 43	ネットワークの設定情報のバックアップを確保すること。	運 32	基礎	◎				
	(5) 運用時ドキュメント管理	実 44	運用時のドキュメントの保管管理方法を明確にすること。	運 33	基礎	◎				
		実 45	ドキュメントのバックアップを確保すること。	運 34	基礎	◎				
	(6) 運行監視	実 46	システムの運行状況の監視体制を整備すること。	運 60	基礎	◎				

基準大項目	基準中項目	基準番号	基準小項目	旧基準番号（第８版）	基準分類	適用区分				
						共通（建物、チャネルに依存せず適用）	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
4 各種設備管理										
	(1) 資源管理	実 47	各種資源の能力及び使用状況の確認を行うこと。	運 54	基礎	◎				
	(2) 機器の管理	実 48	ハードウェア及びソフトウェアの管理を行うこと。	運 66	基礎	◎				
		実 49	機器の管理方法を明確にすること。	運 57	基礎		◎	◎		
		実 50	ネットワーク関連機器の保護措置を講ずること。	運 58	付加		◎	◎	◎	
		実 51	機器の保守方法を明確にすること。	運 59	基礎		◎	◎		
		実 52	機器の予防保守を実施すること。	技 1	付加		◎	◎		
	(3) コンピュータ関連設備の保守管理	実 53	コンピュータ関連設備の管理方法を明確にすること。	運 76	基礎		◎	◎		
		実 54	コンピュータ関連設備の保守方法を明確にすること。	運 77	基礎		◎	◎		
		実 55	コンピュータ関連設備の能力および使用状況の確認を行うこと。	運 78	基礎		◎	◎		
	(4) 入退館（室）管理	実 56	入館（室）の資格付与、及び鍵の管理を行うこと。	運 11	基礎		◎	◎		
		実 57	入退館管理を行うこと。	運 12	基礎		◎			
		実 58	入退室管理を行うこと。	運 13	基礎		◎	◎		
		実 59	入室後の作業を管理すること。	運 61	基礎		◎	◎		
	(5) 監視	実 60	各種設備の監視体制を整備すること。	運 79	基礎		◎	◎		
5 システムの利用										
	(1) 取引の管理	実 61	各取引の操作権限を明確にすること。	運 38	基礎		◎	◎		
		実 62	オペレータカードの管理を行うこと。	運 39	付加		◎	◎		
		実 63	取引の端末機操作の内容を記録・検証すること。	運 40	基礎		◎	◎		
		実 64	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	付加	◎				
	(2) 入出力管理	実 65	データの入力管理を行うこと。	運 24	基礎		◎	◎		
		実 66	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。	運 37	基礎	◎				
	(3) 帳票管理	実 67	未使用重要帳票の管理方法を明確にすること。	運 35	付加	◎				
		実 68	重要な印字済帳票の取扱方法を明確にすること。	運 36	基礎	◎				
	(4) 顧客データ保護	実 69	顧客データの保護策を講ずること。	運 53	基礎	◎				
6 緊急時の対応										
	(1) 障害時・災害時対応策	実 70	障害時・災害時の関係者への連絡手順を明確にすること。	運 62	基礎	◎				
		実 71	障害時・災害時復旧手順を明確にすること。	運 63	基礎	◎				
		実 72	障害の原因を調査・分析すること。	運 64	基礎	◎				
	(2) コンティンジェンシープランの策定	実 73	コンティンジェンシープランを策定すること。	運 65	基礎	◎				
	(3) バックアップサイト	実 74	バックアップサイトを保有すること。	技 25	付加		◎			

基準大項目	基準中項目	基準番号	基準小項目	旧基準番号（第８版）	基準分類	適用区分				
						共通（建物、チャネルに依存せず適用）	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
7 システム開発・変更										
	(1) システム開発・変更管理	実 75	システムの開発・変更手順を明確にすること。	運 67	基礎	◎				
		実 76	テスト環境を整備すること。	運 68	基礎	◎				
		実 77	本番への移行手順を明確にすること。	運 69	基礎	◎				
	(2) 開発・変更時ドキュメント管理	実 78	開発・変更時のドキュメントの作成手順を明確にすること。	運 70	付加	◎				
		実 79	開発・変更時のドキュメントの保管管理方法を明確にすること。	運 71	基礎	◎				
	(3) パッケージの導入	実 80	パッケージの評価体制を整備すること。	運 72	付加	◎				
		実 81	パッケージの運用・管理体制を明確にすること。	運 73	付加	◎				
	(4) システムの廃棄	実 82	システムの廃棄計画を策定するとともに、廃棄手順を明確にすること。	運 74	基礎	◎				
		実 83	システム廃棄時の情報漏洩防止対策を講ずること。	運 75	基礎	◎				
8 システムの信頼性向上対策										
	(1) ハードウェアの予備	実 84	本体装置の予備を設けること。	技 2	付加		◎	◎		
		実 85	周辺装置の予備を設けること。	技 3	付加		◎	◎		
		実 86	通信系装置の予備を設けること。	技 4	付加		◎	◎		
		実 87	回線の予備を設けること。	技 5	付加		◎	◎		
		実 88	端末系装置の予備を設けること。	技 6	付加		◎	◎		
	(2) ソフトウエアの品質向上対策	実 89	必要となるセキュリティ機能を取り込むこと。	技 8	基礎	◎				
		実 90	設計段階におけるソフトウェアの品質を確保すること。	技 9	基礎	◎				
		実 91	プログラム作成段階における品質を確保すること。	技 10	基礎	◎				
		実 92	テスト段階におけるソフトウェアの品質を確保すること。	技 11	基礎	◎				
		実 93	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	基礎	◎				
		実 94	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	基礎	◎				
		実 95	定型的な変更作業時の正確性を確保すること。	技 14	基礎	◎				
		実 96	機能の変更、追加作業時の品質を確保すること。	技 15	基礎	◎				
		実 97	ファイルに対する排他制御機能を設けること。	技 30	付加	◎				
		実 98	ファイル突合機能を設けること。	技 34	基礎	◎				
	(3) 運用時の信頼性向上対策	実 99	オペレーションの自動化、簡略化を図ること。	技 16	付加	◎				
		実 100	オペレーションのチェック機能を充実すること。	技 17	基礎	◎				
		実 101	負荷状態の監視制御機能を充実すること。	技 18	基礎	◎				

基準大項目	基準中項目	基準番号	基準小項目	旧基準番号（第８版）	基準分類	適用区分				
						共通（建物、チャネルに依存せず適用）	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
	(4) 障害の早期発見･回復機能	実 102	システム運用状況の監視機能を設けること。	技 20	基礎	◎				
		実 103	障害の検出及び障害箇所の切り分け機能を設けること。	技 21	付加	◎				
		実 104	障害時の縮退･再構成機能を設けること。	技 22	付加	◎				
		実 105	障害時の取引制限機能を設けること。	技 23	付加	◎				
		実 106	障害時のリカバリ機能を設けること。	技 24	基礎	◎				
9	個別業務・サービス									
	(1) カード取引サービス	実 107	カードの管理方法を明確にすること。	運 51	付加		◎	◎	◎	
		実 108	カード取引等に関する犯罪について注意喚起を行うこと。	運 51-1	付加			◎	◎	
		実 109	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	付加	◎				
		実 110	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	付加		◎	◎	◎	
		実 111	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	付加		◎	◎	◎	
	(2) インターネット･モバイルサービス	実 112	インターネット・モバイルサービスの不正使用を防止すること。	運 103	付加					◎
		実 113	インターネット・モバイルサービスの使用状況を利用者が確認できるようにすること。	運 104	付加					◎
		実 114	インターネット・モバイルサービスの安全対策に関する情報開示をすること。	運 105	付加					◎
		実 115	インターネット・モバイルサービスの顧客対応方法を明確にすること。	運 105-1	付加					◎
		実 116	インターネット・モバイルサービスの運用管理方法を明確にすること。	運 106	付加					◎
		実 117	インターネット・モバイルサービスにおいて口座開設等を行う場合は、本人確認を行うこと。	運 44	付加			◎		◎
	(3) 渉外端末の管理	実 118	渉外端末の運用管理方法を明確にすること。	運 50	付加			◎		
	(4) CD・ATM 等及び無人店舗の管理	実 119	CD･ATM 等及び無人店舗の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	付加			◎	◎	
		実 120	無人店舗の監視体制を明確にすること。	運 46	付加			◎		
		実 121	無人店舗の防犯体制を明確にすること。	運 47	付加			◎		
		実 122	無人店舗の障害時・災害時の対応方法を明確にすること。	運 48	付加			◎		
		実 123	無人店舗の関係マニュアルの整備を行うこと。	運 49	付加			◎		
		実 124	CD・ATM 等の遠隔制御機能を設けること。	技 19	付加		◎	◎	◎	
	(5) インストアブランチ	実 125	インストアブランチの出店先の選定基準を明確にすること。	運 92	付加			◎		

基準大項目	基準中項目	基準番号	基準小項目	旧基準番号（第８版）	基準分類	適用区分				
						共通（建物、チャネルに依存せず適用）	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
	(6) コンビニ ATM	実 126	コンビニ ATM の出店先の選定基準を明確にすること。	運 93	付加				◎	
		実 127	コンビニ ATM の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	付加				◎	
		実 128	コンビニ ATM の障害時・災害時対応手順を明確にすること。	運 95	付加				◎	
		実 129	コンビニ ATM の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	付加				◎	
		実 130	コンビニ ATM の所轄の警察及び警備会社等関係者との連絡体制を確立すること。	運 97	付加				◎	
		実 131	コンビニ ATM の顧客に対して犯罪に関する注意喚起を行うこと。	運 98	付加				◎	
	(7) デビットカード・サービス	実 132	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	付加				◎	
		実 133	デビットカード利用時の口座番号、暗証番号等の安全性を確保すること。	運 100	付加				◎	
		実 134	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	付加				◎	
		実 135	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	付加				◎	
	(8) 前払式支払手段	実 136	前払式支払手段における機器及び媒体の盗難、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。	運 42	付加	◎				
		実 137	前払式支払手段における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	付加	◎				
	(9) 電子メール・イントラネットの利用	実 138	電子メールの運用方針を明確にすること。	運 107	付加					◎
		実 139	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	付加	◎				
	(10) 生体認証	実 140	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	付加	◎				
		実 141	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	付加	◎				

Ⅲ　設備基準

基準大項目	基準中項目	新基準番号（暫定）	基準小項目	適用区分 コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
1 コンピュータセンター							
	(1) 建物(環境)	設 1	各種災害、障害が発生しやすい地域を避けること。	○			
	(2) 建物(周囲)	設 2	立地環境の変化に伴う災害および障害の発生の可能性を調査し、防止対策を講ずること。	○			
		設 3	敷地には通路を確保すること。	◎			
		設 4	隣接物との間隔を十分に取ること。	○			
		設 5	塀または柵および侵入防止装置を設けること。	○			
		設 6	看板等を外部に出さないこと。	○			
		設 7	建物には避雷設備を設置すること。	○			
		設 8	建物はコンピュータシステム関連業務専用、または建物内においてコンピュータシステム関連業務専用の独立区画とすること。	○			
		設 9	敷地内の通信回線・電力線は、切断・延焼の防止措置を講ずること。	○			
	(3) 建物(構造)	設 10	耐火建築物であること。	◎			
		設 11	構造の安全性を有すること。	◎			
		設 12	外壁、屋根等は十分な防水性能を有すること。	◎			
		設 13	外壁等に強度を持たせること。	○			
	(4) 建物(開口部)	設 14	窓には防火措置を講ずること。	◎			
		設 15	防犯措置を講ずること。	◎			
		設 16	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 17	非常口を設けること。	◎			
		設 18	防水措置を講ずること。	○			
		設 19	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。	◎			
	(5) 建物(内装等)	設 20	不燃材料および防炎性能を有するものを使用すること。	◎			
		設 21	地震による内装等の落下・損壊の防止措置を講ずること。	○			
	(6) コンピュータ室・データ保管室(位置)	設 22	災害を受けるおそれの少ない位置に設置すること。	◎			
		設 23	外部から容易に入れない位置に設置すること。	◎			
		設 24	室名等の表示は付さないこと。	◎			
		設 25	必要空間を確保すること。	◎			
		設 26	専用の独立した室とすること。	◎			

基準大項目	基準中項目	新基準番号（暫定）	基準小項目	適用区分			
				コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
	(7) コンピュータ室･データ保管室(開口部)	設 27	常時利用する出入口は 1 カ所とし、前室を設けること。	○			
		設 28	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 29	窓に防火、防水、破損防止措置を講じ、外部から室内の機器等が見えない措置を講ずること。	◎			
		設 30	非常口、避難器具、誘導灯等を設置すること。	◎			
	(8) コンピュータ室･データ保管室(構造・内装等)	設 31	独立した防火区画とすること。	◎			
		設 32	漏水防止対策を講ずること。	◎			
		設 33	静電気の防止措置を講ずること。	◎			
		設 34	内装等には不燃材料および防炎性能を有するものを使用すること。	◎			
		設 35	地震による内装等の落下・損壊の防止措置を講ずること。	◎			
		設 36	フリーアクセス床は地震時に損壊しない構造とすること。	◎			
	(9) コンピュータ室･データ保管室(設備)	設 37	自動火災報知設備を設置すること。	◎			
		設 38	非常時の連絡装置を設置すること。	◎			
		設 39	消火設備を設置すること。	◎			
		設 40	ケーブルの難燃化、延焼防止措置を講ずること。	◎			
		設 41	排煙設備を設置すること。	◎			
		設 42	非常用照明設備、携帯用照明器具を設置すること。	◎			
		設 43	水使用設備を設置しないこと。	◎			
		設 44	地震感知器を設置すること。	○			
		設 45	出入口には出入管理設備、防犯設備を設置すること。	○			
		設 46	温湿度自動記録装置または温湿度警報装置を設置すること。	◎			
		設 47	ネズミの害を防止する措置を講ずること。	○			
	(10) コンピュータ室・データ保管室(コンピュータ機器、什器・備品)	設 48	什器・備品は不燃性とすること。	◎			
		設 49	静電気防止措置を講ずること。	◎			
		設 50	耐震措置を講ずること。	◎			
		設 51	運搬車等に固定装置を取り付けること。	◎			
	(11) 電源室・空調機械室	設 52	災害を受けるおそれの少ない場所に設置すること。	◎			
		設 53	保守点検に必要な空間を確保すること。	◎			
		設 54	専用の独立した室とすること。	○			
		設 55	無窓とし、錠を付けた扉を設置すること。	◎			
		設 56	耐火構造とすること。	◎			
		設 57	自動火災報知設備を設置すること。	◎			
		設 58	ガス系消火設備を設置すること。	○			
		設 59	空調設備の漏水防止措置を講ずること。	◎			
		設 60	ケーブル、ダクトからの延焼防止措置を講ずること。	◎			

基準大項目	基準中項目	新基準番号（暫定）	基準小項目	適用区分			
				コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
	(12) 電源設備	設 61	電源設備の容量には余裕を持たせること。	◎			
		設 62	電源は複数回線で引き込むこと。	○			
		設 63	良質な電力を供給する設備を設置すること。	◎			
		設 64	自家発電設備、蓄電池設備を設置すること。	◎			
		設 65	電源設備には避雷設備を設置すること。	◎			
		設 66	電源設備には耐震措置を講ずること。	◎			
		設 67	分電盤からコンピュータ機器への電源の引込みは専用とすること。	◎			
		設 68	負荷変動の激しい機器との共用を避けること。	◎			
		設 69	コンピュータシステムのアースは適切に施工すること。	◎			
		設 70	過電流、漏電により各機器に障害を及ぼさないよう措置を講ずること。	◎			
		設 71	防災、防犯設備用の予備電源を設置すること。	◎			
	(13) 空調設備	設 72	空調設備の能力には余裕を持たせること。	◎			
		設 73	空調設備は安定的に空気調和できる措置を講ずること。	◎			
		設 74	空調設備はコンピュータ室専用とすること。	◎			
		設 75	空調設備の予備を設置すること。	○			
		設 76	空調設備には自動制御装置、異常警報装置を設置すること。	◎			
		設 77	空調設備には侵入、破壊防止対策を講ずること。	◎			
		設 78	空調設備には耐震措置を講ずること。	◎			
		設 79	空調設備の断熱材料、給排気口は不燃材料とすること。	◎			
	(14) 監視制御設備	設 80	監視制御設備を設置すること。	◎			
		設 81	中央管理室を設置すること。	○			
	(15) 回線関連設備	設 82	回線関連設備には錠をつけること。	◎			
		設 83	回線関連設備の設置場所の表示は付さないこと。	◎			
		設 83-1	回線は、専用の配線スペースに設けること。	○			
2 本部・営業店等							
	(1) 建物(周囲)	設 84	敷地内の通信回線・電力線の切断・延焼の防止措置を講ずること。		○		
	(2) 建物(構造)	設 85	耐火建築物であること。		○		
		設 86	構造の安全性を有すること。		◎		
		設 87	外壁、屋根等は十分な防水性能を有すること。		◎		
		設 88	外壁等の強度を確保すること。		○		
	(3) 建物(開口部)	設 89	窓には防火措置を講ずること。		◎		
		設 90	窓・扉には防犯措置を講ずること。		◎		
		設 91	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 92	通用口には、入室者の識別設備を設置すること。		◎		
		設 93	出入口には防水措置を講ずること。		○		

基準大項目	基準中項目	新基準番号（暫定）	基準小項目	適用区分			
				コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
	(4) 建物(内装等)	設 94	天井および壁は、遮熱、吸音機能を持たせること。		○		
		設 95	地震による内装等の落下・損壊の防止措置を講ずること。		◎		
		設 96	床表面は、塵埃や静電気が発生しにくい材質のものとすること。		○		
		設 97	端末機器への回線等は、切断のおそれのない措置を講ずること。		◎		
		設 98	端末機器に接続している回線、電源ケーブル等への漏水防止対策を講ずること。		○		
	(5) 建物(設備)	設 99	自動火災報知設備および消火器を設置すること。		◎		
		設 100	設備等の耐震措置を講ずること。		○		
		設 101	耐火金庫を設置すること。		◎		
		設 102	避雷設備を設置すること。		○		
		設 103	防犯措置を講ずること。		◎		
	(6) 建物(回線関連設備)	設 104	回線関連設備の設置場所の表示は付さないこと。		◎		
		設 105	回線関連設備には錠を付けること。		◎		
		設 106	回線関連設備から各端末機器までの配線を二重化すること。		○		
	(7) 建物(電源設備)	設 107	電源ケーブルは、端末機器等に支障を来さないよう布設すること。		◎		
		設 108	防災、防犯設備用の予備電源を設置すること。		◎		
		設 109	自家発電設備等を設置すること。		○		
	(8) 建物(空調設備)	設 110	空調設備を設置すること。		◎		
	(9) 建物(自動機器室)	設 111	通話装置を設置すること。		◎		
		設 112	非常通報装置を設置すること。		◎		
		設 113	防犯措置を講ずること。		◎		
		設 114	照明設備および非常用照明設備を設置すること。		◎		
		設 115	扉は、一部を素通しにすること。		◎		
		設 116	自動機器の現金の装填と保守のための必要な空間を確保すること。		○		
		設 117	自動運行設備を設置すること。		○		
	(10) 建物(端末機器)	設 118	端末機器には耐震措置を講ずること。		○		
		設 119	機器のアースを確実に取ること。		◎		
		設 120	漏水および塵埃等に対する保護措置をとること。		○		
	(11) サーバー設置場所(位置)	設 121	災害を受けるおそれの少ない位置とすること。		○		
		設 122	外部から容易に入れない位置とすること。		○		
		設 123	室名等の表示は付さないこと。		○		
		設 124	専用の区画とすること。		○		
	(12) サーバー設置場所(構造・内装等)	設 125	防火区画に設置すること。		○		
		設 126	漏水防止対策を講ずること。		○		
		設 127	フリーアクセス床は地震に備えて耐震措置を講ずること。		○		

基準大項目	基準中項目	新基準番号（暫定）	基準小項目	適用区分			
				コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
	(13) サーバー設置場所(設備)	設 128	消防設備を有すること。		○		
		設 129	地震感知器を設置すること。		○		
		設 130	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 131	温湿度自動記録装置または温湿度警報装置を設置すること。		○		
		設 132	空調設備を設置すること。		○		
		設 133	ネズミの害を防止する措置を講ずること。		○		
		設 134	電源コンセントの抜け防止対策を講ずること。		◎		
	(14) インストアブランチ	設 135	他の区画からの侵入防止措置を講ずること。		◎		
		設 136	使用するストアの設備状況に応じて、適切な補強策を講ずること。		◎		
3 流通・小売店舗との提携チャネル							
	(1) コンビニ ATM	設 137	防犯措置を講ずること。			◎	

Ⅳ　監査基準

基準大項目	基準中項目	新基準番号（暫定）	基準小項目	旧基準番号（第８版）	基準分類	適用区分				
						共通（建物、チャネルに依存せず適用）	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル
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	基礎	◎				

V. 統 制 基 準

1 内部の統制
(1) 方針・計画

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　1	システムの安全対策に係る重要事項を定めた規程を整備すること。

システムの安全対策を適切に実施するための組織体制、関係者の役割及び管理すべき事項を明確にした規程を策定すること。また、環境変化に対応するため、策定した規程を適宜改訂すること。

1. システムの安全対策を実行に移すために必要な以下の事項を定めた規程を整備することが必要である。
   (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、保護すべき情報資産、保護する目的及び責任の所在を定めたものである。
   なお、セキュリティポリシーの策定にあたっては、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』を参照のこと。
   (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を実行に移すための具体的な対策を定めたものであり、社内部門別に作成することもある。

2. 当該規程の整備にあたっては、システムリスク管理方針等の上位規程に示された安全対策に係る方針との整合をとることが必要である。

3. 全社（もしくは全組織）の安全対策の方針及び実施に重大な影響を与える規程の策定及び改訂にあたっては、経営層が指示し、承認することが必要である。

4. 環境変化に対応し、当該規程を適宜見直し改訂することが必要である。

   規程を見直すタイミングとしては、以下の例がある。
   (1) 組織運営の変化
   (2) ビジネス環境の変化
   (3) 法令の制定、改正
   (4) 情報・通信技術の進歩
   (5) 業務組織及び人員・就業場所の変化
   (6) 扱う情報資産の変化
   (7) セキュリティに関する事故及び犯罪の発生
   (8) 当該規程に定められた事項の遵守状況の確認結果

5. 当該規程の内容を、安全対策の関係者（外部要員を含む）に対して、その役割と責任に応じて周知、教育することが必要である。セキュリティ教育については【統 14】を参照のこと。

6. 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金融機関等が統合する場合は、システム統合に先立ち相互の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。

1 内部の統制
(1) 方針・計画

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　2	中長期的視点に立ったシステムの企画・開発・運用に関する計画を策定すること。

有効なシステムを長期的かつ安定的に維持するため、中長期的視点に立って、システムの企画・開発・運用に関する計画を策定すること。

1. システムの整備には多くの経営資源及び期間が必要となることを考慮し、中長期的視点に立って、システムの企画・開発・運用に関する計画（以下「中長期システム計画」という）を策定することが必要である。

2. 中長期システム計画は、計画遂行に必要となる人材を含む経営資源を考慮し、中長期の経営計画と整合をとって策定または経営計画の一部として策定し、経営層の承認を得ることが必要である。

   中長期システム計画の策定にあたり検討する事項としては、以下の例がある。
   (1) 今後の重点投資分野及び達成目標
   (2) 基幹業務のシステムの方向性
   (3) 重要設備の更改計画
   (4) 重要な外部委託先との関係
   (5) 新技術・サービスの導入方針
   (6) 計画遂行に必要となる人材の確保

1 内部の統制
(2) 組織体制

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

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

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、中長期システム計画と整合性がとれており、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システム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、システム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、以下の例がある。
   (1) 技術の特徴、適用条件
   (2) 将来採用可能となる技術までを含めた拡張性
   (3) 技術の性能評価
   (4) 費用対効果の評価

3. システム開発計画が中長期システム計画に基づいており、採用技術も適切なことを確認することが必要である。また、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。

1 内部の統制
(2) 組織体制

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　4	セキュリティ管理体制を整備すること。

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、定められた規程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）を確立することが必要である。
   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の統制、管理を行うことが必要である。
   上記体制の確立にあたっては経営層が指示し、承認することが必要である。

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、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。

   セキュリティ管理者の業務としては、以下の例がある。
   (1) システムの企画から開発、運用、保守及び廃棄にわたるすべてのフェーズのセキュリティの管理
   (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) セキュリティ上の問題により発生した障害・事故・犯罪等について、情報収集、分析、評価、及びセキュリティポリシー、セキュリティスタンダード等の規程への反映

   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。
   (1) システム管理体制（システム管理者）【統 6】
   (2) データ管理体制（データ管理者）【統 7】
   (3) ネットワーク管理体制（ネットワーク管理者）【統 8】

3. 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

1 内部の統制
(2) 組織体制

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　5	サイバー攻撃対応態勢を整備すること。

サイバー攻撃への対応のため、サイバー攻撃対応態勢を整備するとともに、手口の高度化及び巧妙化にあわせて見直すこと。

1. サイバー攻撃に伴うシステムの停止及び不正な資金移動に対応するために、未然防止策・事前対策、検知策及び対応策を検討し、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、各金融機関等は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。
未然防止策・事前対策、検知策及び対応策としては、以下の例がある。

(1) 未然防止策・事前対策

①外部の第三者によるセキュリティ評価を行う。不正侵入防止における評価については【実 14】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。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、【統 21】【統 23】【監 1】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及び外部との連絡窓口の機能を担い、経営層への報告並びに経営層からの指示を実施することができる組織を整備する。例として CSIRT（Computer Security Incident Response Team）の設置等がある。【実 14】（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、外部ベンダー等におけるフォレンジック業務等のサービス提供能力を事前に把握する。

⑤インターネット取引において、顧客が必要とする機能、並びに顧客の利用環境や 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。取引制限については【実 11】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、顧客が利用するパソコン環境の事前告知を求める。

(2) 検知策

①インシデントレスポンス態勢を整備する。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、【実 46】を参照のこと。

②アクセス履歴を監査する。アクセス履歴の監査については【実 10】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。詳細については【実 16】を参照のこと。

(3) 対応策

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。システム障害時の対応手順の整備については【実 71】、連絡手順については【実 70】を参照のこと。

②利用者（顧客）への説明を行う。顧客への対応方針については【実 115】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。不正アクセスの拡大防止については【実 19】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。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。

教育・訓練としては、以下の例がある。

(1) サイバー攻撃を想定した対応訓練を実施する。

(2) サイバー攻撃対応の意識を高めるために、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。

(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。また、業界団体が開催する訓練に参加する。

(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。関係する役職員に対しては【統 14】、外部委託先に対しては【統 22】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。注意喚起すべき内容については【実 115】を参照のこと。

2. サイバー攻撃に対応するためには、国内外のサイバー攻撃動向・事例、脆弱性などに関する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
(2) 組織体制

適　用　区　分					基礎分類
共	セ	本	提	ダ	基礎
◎					

統　6	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。

   システム管理者の業務としては、以下の例がある。
   (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

3. 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することが望ましい。

4. システム管理者は、データ管理者及び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。

1 内部の統制
(2) 組織体制

適　用　区　分					基礎分類
共	セ	本	提	ダ	基礎
◎					

統　7	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。さらに、それぞれのデータ管理者の間で、相互に連携を図った体制を整えることが望ましい。

   データ管理者の業務としては、以下の例がある。
   (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

3. データ管理者は、システム管理者及び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。

1 内部の統制
(2) 組織体制

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　8	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、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。

　ネットワーク管理者の業務としては、以下の例がある。
　(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

3. ネットワーク管理者は、システム管理者及びデータ管理者と、適切に職能が分離されていることが望ましい。

1 内部の統制
(2) 組織体制

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

統　9	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、業務範囲並びに責任及び権限を明確にし、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、業務範囲並びに責任及び権限を明確にするとともに、適切な業務組織の分離及び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。

   コンピュータシステムに係わる業務組織を整備する際の具体的な留意点としては、以下の例がある。

   (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。
   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。
   ①プログラムの作成‥‥‥‥‥‥‥‥‥‥‥‥設計者・プログラマー等
   ②入力データの作成‥‥‥‥‥‥‥‥‥‥‥‥起票者・検証者・入力者
   ③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・オペレーション検証者等
   ④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
   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。
   ①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）
   ②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）

   (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。

1 内部の統制
(2) 組織体制

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

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。

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、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が共同ビル内にある場合は、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。

   防災組織を整備する際の留意点としては、以下の例がある。
   (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。
   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。
   (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を行う。また、人事異動等により担当者が変更になった場合にも、再度組織図を周知徹底する。
   (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ため、想定される連絡内容を明確にする。
   (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。
   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する。
   (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。

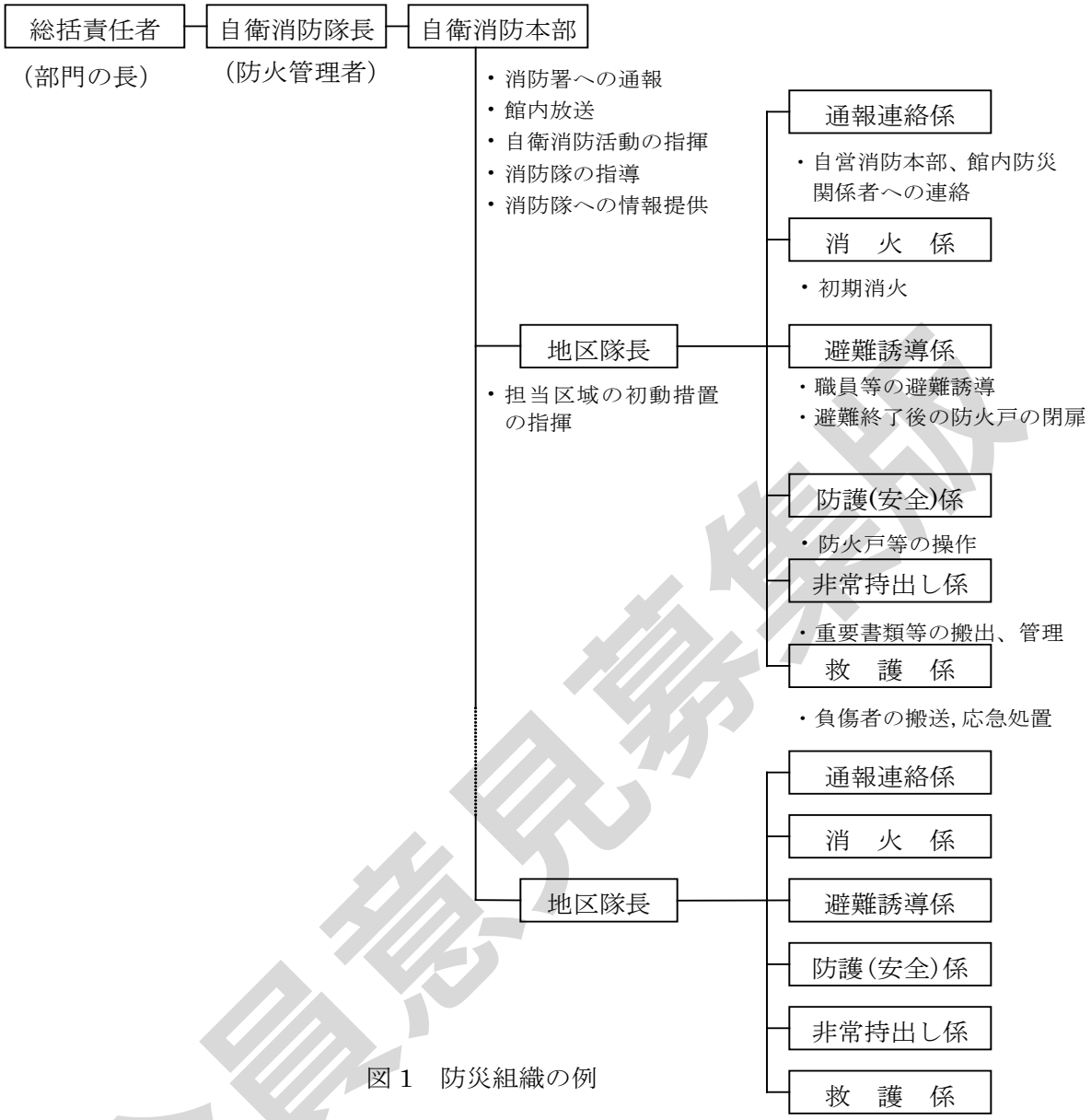


図１　防災組織の例

参照法令	消防法第８条、消防法施行規則第１条～第４条

1 内部の統制
(2) 組織体制

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

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、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が共同ビル内にある場合は、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。

   防犯組織を整備する際の留意点としては、以下の例がある。
   (1) 防犯組織に係わる責任者、分担等を関連部門及び店内の人に周知徹底する。
   　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。
   (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。特に、人事異動等により担当者が異動となった場合には、再度組織図を周知徹底する。
   (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。

   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。

(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

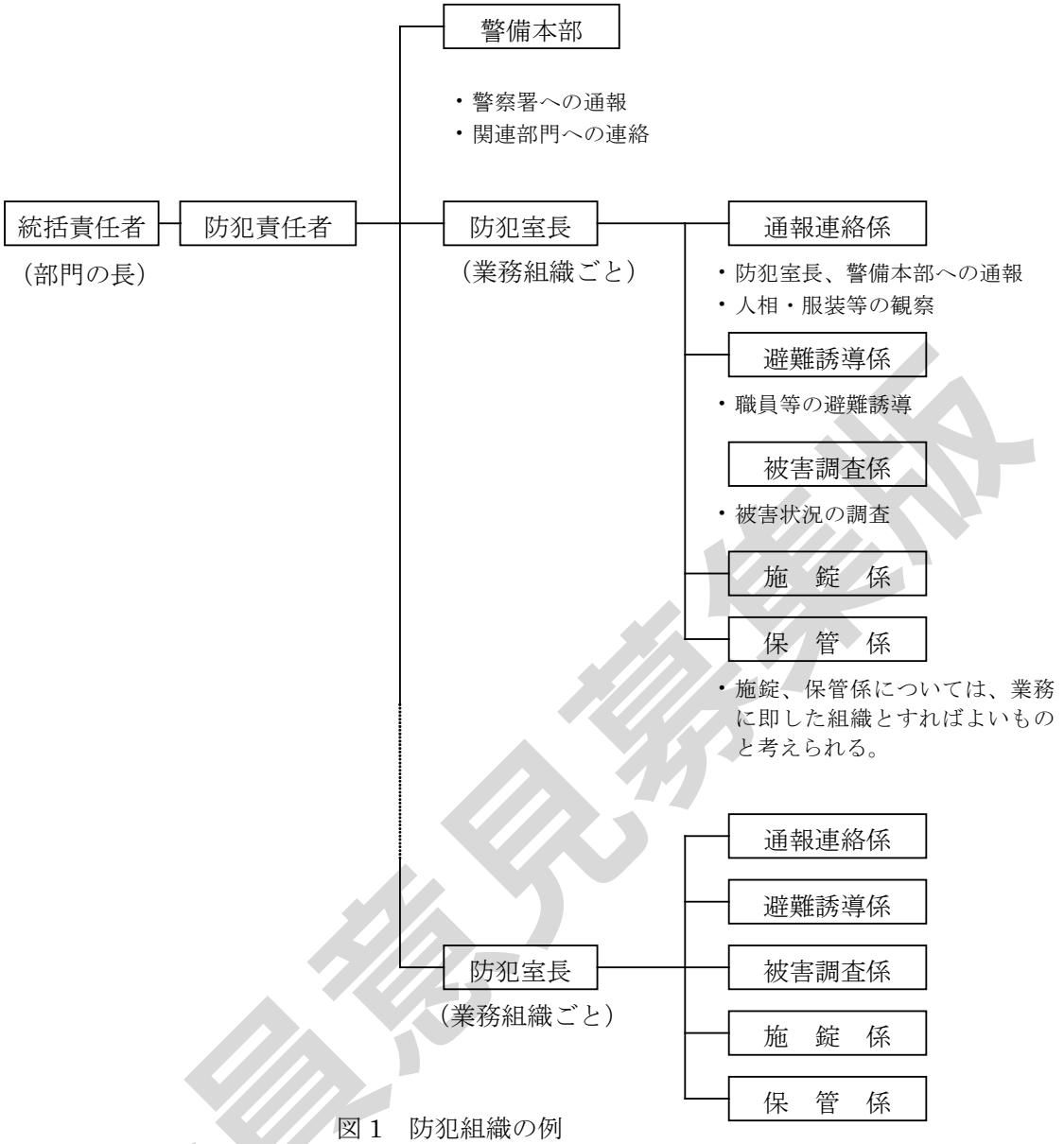


図１　防犯組織の例

1 内部の統制
(2) 組織体制

適 用 区 分					基準分類
共	セ	本	提	ダ	基礎
◎					

統 12	各種業務の規則を整備すること。

システムを円滑かつ適正に運用、管理するため、業務の各組織における責任及び権限を明確にした規則を整備すること。

1. システムを円滑かつ適正に運用、管理するため、上位規程であるセキュリティポリシー、セキュリティスタンダード等の規程と整合をとって、業務の各組織における責任及び権限を明確にした規則を整備することが必要である。

   ここでいう規則とは、業務の各組織に関する事務分掌、職掌並びに責任及び権限を定めたものを指している。また、手順書及びマニュアルは、本規則に基づいて作成されるものである。

   規則の内容に含まれる業務としては、以下の例がある。
   (1) 入退管理【実 56～58】
   (2) コンピュータシステムの通常時、障害時・災害時運用【実 23～27、実 33～38、実 42、実 43、実 46、実 47、実 49～51、実 59、実 65、実 70～73】
   (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【実 30、実 61～64、実 66、実 69、実 117～123、実 136】
   (4) データ、プログラム及びドキュメントの管理【実 28、実 29、実 32、実 39～41、実 44、実 45、実 67、実 68】
   (5) カード管理【実 107、実 110】
   (6) システム開発・変更【実 48、実 75～83】
   (7) 電源設備、空調設備、防災設備、防犯設備の管理【実 53～55】
   (8) 防犯・警備【統 6～11】
   (9) 監視【実 60】

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、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則を必要に応じて定めることが必要である。

1 内部の統制
(3) 管理状況の評価

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　13	セキュリティ遵守状況を確認すること。

コンピュータシステムを円滑かつ適正に運用するため、セキュリティポリシー、セキュリティスタンダード等の規程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及びセキュリティレベルの向上を図ること。

1. セキュリティポリシー、セキュリティスタンダード等の規程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及びセキュリティレベルの向上を図ることが必要である。

   セキュリティ遵守状況を確認するタイミングとしては、以下の例がある。
   (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) セキュリティポリシー、セキュリティスタンダード等の規程に変更があった時
   (4) 異動等により人員の配置変更があった時

2. セキュリティ遵守状況を確認する者は、建屋内の点検、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することが望ましい。

3. セキュリティ遵守状況の確認結果を評価し、セキュリティポリシー、セキュリティスタンダード等の規程の改訂に反映することが必要である。【統 1】

4. セキュリティ遵守状況の確認結果を評価し、セキュリティ教育の内容等を見直すことが必要である。【統 14】

1 内部の統制
(4) 人材（要員・教育）

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

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して、担当する業務内容等を勘案したうえでセキュリティ教育を行うこと。

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、セキュリティポリシー、セキュリティスタンダード、及びこれに基づいて作成されたマニュアル、手順書等に沿って実施し、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、計画的に行うことが必要である。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することが必要である。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

   教育テーマとしては、以下の例がある。
   (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
      ①ユーザーID、パスワードの管理
      ②利用権限の認識
      ③ドキュメントや出力物の整理、整頓
      ④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

(10) 情報倫理
(11) ソーシャルエンジニアリング対策（注）
(12) 電子メール、ホームページ閲覧等の運用方針 【実 138、実 139】

（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等がある。

1 内部の統制
(4) 人材（要員・教育）

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

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、担当する業務内容等を勘案した教育を行うこと。

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。

   教育の内容としては、以下の例がある。

   (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
   ⑦OJT

   (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

2. 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。

1 内部の統制
(4) 人材（要員・教育）

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　16	障害時・災害時に備えた教育・訓練を行うこと。

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。
   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。

   障害時・災害時マニュアルの整備については、【実 24、実 70～72】を参照のこと。

   訓練を計画するにあたり明確にするべき事項としては、以下の例がある。
   (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。
   (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。

訓練上の考慮点としては、以下の例がある。

(1) 障害時・災害時に迅速な対応がとれるように、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の記載内容をレビューする。

(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。

2. 訓練終了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。

3. 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。

1 内部の統制
(4) 人材（要員・教育）

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　17	防災・防犯訓練を行うこと。

防災組織、防犯組織を十分に機能させるため、非常時に備えた防災・防犯訓練を行うこと。

1. 防災組織、防犯組織を十分に機能させるために、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、防災・防犯組織の役割・コンティンジェンシープランの記載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。【実 70】
   (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等に反映させるべき事項があれば、当該プラン等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

1 内部の統制
(4) 人材（要員・教育）

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　18	要員の人事管理を行うこと。

システムの円滑な運用のため、要員の配置、交替等の人事管理を行うこと。

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。

1 内部の統制
(4) 人材（要員・教育）

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　19	要員の健康管理を行うこと。

要員の健康維持及びシステムの円滑な運用のため、作業環境の整備、定期的な健康診断の実施などの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。

   要員の健康管理上注意すべき事項としては、以下の例がある。
   (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

（参考）

1. VDT(Visual Display Terminals)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（注）
   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、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。

（注）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。

2 外部の統制
(1) 外部委託管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　20	外部委託を行う場合は、事前に目的、範囲等を明確にするとともに、外部委託先選定の手続きを明確にすること。

適切な外部委託先を選定するため、外部委託を行う場合は、事前に目的、範囲等を明確にするとともに、選定手続きを明確にし、外部委託先を客観的に評価すること。また、外部委託先の決定にあたっては、責任者の承認を得ること。

ここでいう外部委託先には再委託先を含む。また、再委託先には再々委託以下の階層を含む（以下同じ）。

1. 外部委託（共同センター、クラウドサービスの利用を含む）を行う場合は、事前に目的、範囲等を明確にすることが必要である。ただし、外部委託には、勘定系システムの共同化など、当該金融機関等の全体に大きな影響が生じるものがある。こうした場合、外部委託の決定にあたっては、経営計画、中長期システム計画等を踏まえ総合的に評価することが考えられる。

外部に委託する業務としては、以下の例がある。
(1) オペレーション（バックアップサイトにおけるオペレーションを含む）
(2) システムの開発、変更
(3) ソフトウェアの開発、変更
(4) プラットフォーム、アプリケーション等に関するサービスの利用
(5) ハードウェア及び回線の設置、入替、撤去
(6) 入力データの作成（端末オペレーションを含む）
(7) 記録媒体、ドキュメント及び帳票等の作成、保管、配送、廃棄
(8) 館内、構内及び店内の警備
(9) 電源、空調、防犯等設備の管理、保守
(10) 集中監視（CD・ATM 等）
(11) CD・ATM 等の現金の管理

明確にすべき外部委託に関する事項としては、以下の例がある。
(1) 委託目的
(2) 委託業務範囲
(3) 委託形式
(4) 委託期間
(5) 委託費用

(6) リスクの管理方法
(7) 外部委託先の選定要件
(8) 外部委託に関する自社窓口と役割 等

2. 外部委託先の選定要件を策定することが必要である。
委託する業務に求められる可用性・機密性等の観点及び自社の経営の視点から、リスクを分析・認識し、当該業務に求められるリスク管理レベルを検討のうえ、外部委託先の選定要件を策定する必要がある。

3. 外部委託先を客観的に評価することが必要である。
特定システムを委託する場合、外部委託先に対し金融機関等みずからが評価を行う必要がある。この際、委託する業務の範囲及び外部委託先のサービスの性質、利用形態に関する金融機関等と外部委託先の責任分界点を考慮のうえ、外部委託先の資質・業務遂行能力に関する情報、内部統制、及びリスク管理に関する状況等をもとに評価を行うことが必要である。また、評価にあたっては、外部委託先の情報開示における条件等を考慮し、必要に応じ機密保持契約を事前に締結したうえで開示を求めることが望ましい。委託する業務の全部または一部が再委託される場合、金融機関等は委託先が再委託先を選定することを前提として、その妥当性を検証するために、再委託先の評価を行う必要がある。

通常システムを委託する場合、外部委託先の公開情報、業界における評判、実績等をもとに客観的な評価を行うことも可能である。再委託先については、委託先における再委託先の審査・管理プロセス及びその運用状況が実効的であるかを検証することで、個別の再委託先の評価に代替することも可能である。

外部委託先を評価する事項としては、以下の例がある。
なお、委託する業務の全部または一部が再委託される場合、再委託される業務の内容及びリスク特性に応じ、再委託先と外部委託先とで評価する事項が異なる点に留意する必要がある。

(1) 外部委託を想定する業務に係る実績、技術レベル
①信頼度及び受託実績（類似システムの開発実績、他のプロジェクトやサービスにおける評判等）
②技術レベル（業務内容の理解度、業界に関する知識（金融機関等が委託する業務に関する専門性）、情報収集能力、プロジェクト管理能力（外部委託先が安定して業務に係る開発・運用をしているか等）、導入サポート力等）
(2) 事業継続性（経営方針、経営体力・収益力、人的基盤、被災時の BCM・データのバックアップ）
(3) サービスの可用性・データの安全性（機密性保護）・完全性の確保のための態勢、セキュリティ対策の実施状況（機密保護状況を含む）
(4) 内部統制やリスク管理等に関する状況（委託先における再委託先管理を含む）、外部監査の受検、各種公的認証の取得状況及び組織体制（コンプライアンス体制を含む）
(5) 情報開示における条件

特に情報セキュリティに関する事項は、十分に把握しておく。
①データの入力・保管・処理・バックアップ・出力といった一連のフロー
②暗号方式、暗号化領域、非暗号化領域
③ログ（システムログ、業務ログ、操作ログ等）の取得範囲・取得頻度・保存期間・開示範囲
④バックアップを含むデータコピーの取得内容・保管場所・保管期間
⑤インフラのバージョンアップ作業及びネットワーク設定情報の変更　等

(6) 監査の受入に関する方針、訪問調査の受入スタンス、コミュニケーションルート
(7) 既存システムとの連携・新システムへのデータ移行の容易性
(8) 保守体制・サポート体制（サポートデスク、問題発生時の対応力（障害発生時におけるトレーサビリティの確保等）、日本語による対応）
なお、外部委託先が提供するアプリケーション、サービス等の導入に際しては【実 80、実 81】も参照のこと。
(9) インシデントが発生した場合の想定損害額（直接損害・間接損害）と外部委託先側が提示する損害賠償・補償上限額とのバランス
(10) 契約終了時の対応（ベンダーロックインリスク対応、データ消去等）
契約の中断・終了に伴い発生する可能性があるシステム移行作業（移行データの抽出方法と実際の移行作業内容）など
(11) 個人データの取扱い
個人データの取扱いの全部または一部を外部委託先に行わせることを内容とする契約を締結する場合、「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Ⅲに定める「個人データ保護に関する委託先選定の基準」に対する準拠対応可否
(12) 委託費と支払い条件
(13) 係争等に関する国外における裁判に関する事項
外部委託先との間で係争が生じた場合の準拠法及びこれを取り扱う裁判所に関する取決めが国外である場合に評価すべき事項など
国外での裁判に関する事項として評価すべきリスクとしては、以下の例がある。
①現地の各種法制及び裁判制度の把握並びに分析
②現地における活動資格を有する弁護士の確保
③地理不案内な遠隔地での打合せや出廷などに伴う経済的、人的負担
④上記すべてについての外国語による対応

4. 外部委託先の選定に関する手続きを明確にすることが必要である。具体的には、規程等により、外部委託先の選定手続きを定めることが考えられる。また、委託する業務の全部または一部が再委託される場合、再委託される業務の内容及びリスク特性に応じ、再委託先の評価及び委託先に再委託を承認する手続きについても明確にすることが必要である。

5. 外部委託先の決定については、責任者の承認を得ることが必要である。また、システム開発、システム運用、サービスの利用等に関する計画の承認時に、外部委託に関する事項についても責任者の承認を得ることが必要である。

6. 契約期間中においても、継続的に外部委託先を評価することが望ましい。

2 外部の統制
(1) 外部委託管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　21	外部委託先と安全対策に関する項目を盛り込んだ契約を締結すること。

安全性確保のため、機密保護、安定的なシステム運用等に関する項目を盛り込んだ契約を締結すること。

1. 金融機関等は委託した業務が安全に遂行されるよう、機密保護及びシステムの安定的な運用等に関する事項を盛り込んだ契約を外部委託先と締結する必要がある。また、委託契約に加え「機密保持に関する契約」または「リスク管理に関する契約」を締結することも考えられる。

   契約締結時に考慮すべき事項としては以下の例がある。なお、委託する業務の内容、リスク特性及び再委託の有無等によって、考慮すべき事項が異なることに留意する必要がある。

   (1) 基本的な事項
   ①用語の定義、役割分担、責任範囲、債務不履行時の損害賠償範囲、準拠法、裁判管轄等
   ②検収及び納品の条件並びに手順及び権利の移転の時期
   ③品質の保証及び確認手順
   ④作業時間、立入場所等
   ⑤指示目的外使用
   ⑥契約変更の場合の手順
   ⑦仕様変更の取扱い

   (2) 個別契約条件、サービス仕様、データ保護の管理策
   ①利用する業務の期限、費用
   ②外部委託先（複数の外部委託先が業務の委託を受けた場合も含む）への業務委託範囲、外部委託先のサービスの性質及び利用形態を考慮した金融機関等と外部委託先との間の管理境界や責任分界点に関する取決め
   ③サービス仕様（リソースの割当て等（仕様上の制限や変更に必要な時間等））
   ④機密保護
   ⑤金融機関等が守るべき法令や金融機関等のセキュリティポリシー等、外部委託先の要員が遵守するべきルール
   ⑥セキュリティ管理方法及び体制
   外部委託先におけるデータ漏洩防止に関する対策（暗号化等）及び管理体制（暗号鍵の管理体制等）【実 3、実 4、実 8、実 30】
   ⑦データのバックアップ

(3) サービスレベル未達の場合の対応

(4) 情報開示範囲、監督当局による検査等への協力義務、金融機関等と外部委託先間の報告・連絡等の運営ルール、インシデントレスポンスの取扱い

①作業の報告方法と報告形式

②作業の指示に関する取決め

③委託業務における問題発生時の解決体制

④保守及び障害時等の回復作業・復旧手順、マニュアル整備及び教育・訓練

⑤目標復旧時間（RTO：Recovery Time Objective）

⑥事故発生時における報告

⑦情報漏洩等のインシデントが発生、または発生が疑われる場合のトレーサビリティ確保のための調査協力義務

⑧委託業務に関するコンティンジェンシープラン（緊急時対応計画）【統 16、統 17】

(5) 反社会的勢力・テロ組織と関わりがないことの表明・確約

(6) 契約の解除条件、契約終了時のデータの返却・消去等及び、契約終了時の原状回復・新システム移行時における協力義務

①契約の解除条件（外部委託先の業務遂行に問題がある場合に、他の外部委託先等と契約する権利等）

②契約終了時における外部委託先によるデータ消去の実施（物理的消去または論理的消去等の方法、開発端末等の消去の範囲）及び実施時期、消去証明書等の発行（または消去プロセスの有効性に関する外部の第三者による検証）、文書等の廃棄・回収【実 83】

③契約終了時における原状回復・データ移行作業等の協力義務

(7) 損害が発生した場合の協議及び賠償に関する取決め

(8) 委託業務の成果の知的財産権、使用権等の権利の帰属

(9) 外部委託先からの情報開示

①平常時の標準的な情報開示内容の明記

契約または SLA 等による情報開示の範囲に関する合意、開示請求の対象情報の機密性が高い場合における機密保持契約の締結

②リスク顕在化時の情報開示

リスク事象が発生した際や、各種の資料により情報漏洩リスクが高まった、または外部委託先側の内部統制状況が悪化したと判断される場合の金融機関等からの請求内容に応じた情報開示

(10) 複数の外部委託先への委託

金融機関等と外部委託先間における責任関係の明確化、一元的な窓口機能、外部委託先間の相互調整機能を担う事業者の選定

(11) 再委託管理

①再委託先に対する金融機関等の事前審査の実施

再委託先の選定要件の策定、評価、選定プロセス

選定要件の策定及び、評価については【統 20】を参照のこと。

②損害賠償も含めた責任の明確化

再委託先が問題を発生させた際の委託先の管理責任及び、損害賠償の上限に関する条項

③外部委託先・再委託先間の義務の明確化

外部委託先との契約において、外部委託先が金融機関等に対して負う義務（報告、内部統制確保など）に関する内容と同等の条項が外部委託先・再委託先間の契約上に明記されていることの確認

④再委託の中止の扱い

各種の報告資料等を踏まえ、再委託先の業務遂行能力に対し、問題視し得る状況が生じた場合、金融機関等は外部委託先に対し、再委託の中止を求めることができる条項、外部委託先が中止の求めに応じない場合の委託契約の解除に関する条項の設置

(12) 監査・モニタリング

①監査等の権利

金融機関等が、外部委託先に対し監査等を実施する権利の明記

なお、監査の方法については【監 1】を参照のこと。

②監査等の受入対応費用

監査等の受入対応の費用負担に関する取り決めの明記

③監査等の指摘事項の扱い

監査等により判明した指摘事項への対応に関する取り決め（費用負担・対応期間等）の明記

(13) インシデント発生時等の立入調査

①委託業務において重要な脆弱性が判明した場合、情報漏洩等のインシデントが発生した場合、外部委託先が他の顧客から受託した業務において重大なインシデントが発生した場合、または第三者において委託業務と関連性を有する社会的に重大なインシデントが発生した場合、もしくはこれらの発生が疑われる具体的な懸念が生じた場合等において、金融機関等みずから、または金融機関等が指定するセキュリティ業者・デジタルフォレンジック業者が立入調査することについて外部委託先とあらかじめ協議しておくことが考えられる。

②インシデント発生時において調査に必要なデータの収集範囲及び分析に必要なツール等の提供（提供されない場合は、分析に係る費用等）について、外部委託先とあらかじめ協議しておくことが考えられる。

③外部委託先の経営不安が発生した場合、金融機関等みずから、または金融機関等が指定する専門業者が、必要に応じ、外部委託先施設に立ち入り、顧客データや関連著作物・成果物の保全を行うことについて、外部委託先とあらかじめ協議しておくことが考えられる。

(14) 記憶装置等の障害・交換

記録媒体等を障害、交換等の事情により施設外へ持ち出す場合には、記録済データをあらかじめ復元が不可能または著しく困難な状態とする。また、記憶装置等の障害・交換におけるデータ消去については、消去証明書の発行・取得または外部委託先に対する情報提出要請や、監査等の方法で消去・破壊プロセスの実効性を検証する。

(15) 国外におけるデータ保管時の留意点

金融機関等における障害対応要員の現地の語学力が十分でない場合、日本語によるサポート、外部委託先の日本法人等の障害対応窓口設置を明確にする。

(16) トレーサビリティの確保

障害や情報漏洩等のインシデントが発生した際には、流出・毀損したデータの特定や原因究明のための作業が複雑化する場合があることが想定されるため、トレーサビリティ確保のための方策を準備する。

2. SLA の締結または SLO の確認により、サービスレベルについて合意することが望ましい。

SLA 及び SLO に記載される指標としては、以下の例がある。

(1) システム運用（可用性（注）、信頼性、性能、拡張性、稼働時間、ネットワークを含む管理体制、オンラインシステムの稼働開始時限）に関する事項

（注）システム運用の可用性に関する指標の評価にあたって考慮する事項としては、以下の例がある。

①障害等に伴うシステムの停止時間

②システムの更新・保守（緊急的なセキュリティパッチ対応を含む）、新サービスの追加などシステムの品質・セキュリティ向上のための計画停止期間

(2) サポート（障害対応、問合せ対応）に関する事項

(3) データ管理（利用者データの管理等）に関する事項

(4) 統制環境（委託先における再委託先管理、機密保護の維持、統制環境の維持）に関する事項

(5) 開発業務を委託する場合の開発に要する人員や開発期間及び期限に関する事項

なお、広域災害等の影響により外部委託先が SLA 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. サービスレベル合意の違反のほか、外部委託先または金融機関等の方針変更によって外部委託先との契約の続行が困難になるような場合でも、業務の継続を可能とする対策を講ずることが望ましい。

具体的な対策としては、以下の例がある。

(1) 外部委託先による移行すべきデータの抽出方法の提供及び移行作業への協力義務に関する契約書への明記

(2) 契約の解約時におけるシステム移行作業にかかる費用負担の契約書への明記

2 外部の統制
(1) 外部委託管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　22	外部委託先の要員にルールを遵守させ、その遵守状況を確認すること。

セキュリティ管理を適切に行うため、外部委託先の要員に対し、委託業務の内容や作業の範囲に応じて、セキュリティポリシーをはじめとした各種ルールの遵守を義務づけ、その遵守状況を確認すること。

1. 外部委託先の要員が委託業務を遂行するにあたっては、金融機関等のセキュリティポリシーをはじめとした、外部委託先の要員が遵守すべきルールを委託業務の内容及び作業の範囲に応じて明確にし、これを遵守させる必要がある。

   具体的な取り組みとしては、以下の例がある。

   (1) 外部委託先の要員が遵守すべきルールの明示

   業務遂行のマネジメントを含む委託の場合には、業務体制、監査等のセキュリティ要件を外部委託先と合意のうえで契約するか、あるいはそれに準じた文書の中で列挙する。

   なお、外部委託先の要員が遵守すべきルールとしては、以下の例がある。

   ①金融機関等のセキュリティポリシー
   ②コンピュータセンターの入退館管理ルール、機器管理ルール
   ③各種情報へのアクセス権限の管理ルール（ID やパスワードの付与、抹消ルール等）
   ④開発工程において作成されたドキュメントや磁気媒体の管理手順

   (2) 外部委託先の要員が遵守すべきルールの周知徹底

2. 外部委託先の要員に与える金融機関等の各種資源及びシステムへのアクセス権限は、委託業務の遂行のために必要な範囲に限定する必要がある。なお、アクセス権限の取得及び見直しの手順については【実 27】を参照のこと。

3. 金融機関等は、上記のルールの遵守状況を確認する必要がある。そのためには、金融機関等は委託業務の内容及び作業の範囲に応じて、外部委託先における業務の遂行状況について監査を行うこと、または外部委託先からの業務報告を受けるなどの対策を講ずる必要がある。監査については【監 1】を参照のこと。

2 外部の統制
(1) 外部委託管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　23	外部委託における管理体制を整備し、委託業務の遂行状況を確認すること。

外部委託先のセキュリティ管理状況及び、委託した業務が適切に遂行されているかを確認するため、委託業務の内容または作業の範囲に応じて、外部委託管理体制を整備するとともに、委託契約に基づき委託業務の遂行状況を確認すること。

1. 委託した業務を円滑及び適正に運営する観点から、委託業務の内容または作業の範囲に応じて、外部委託管理体制を整備するとともに、委託契約に基づき委託業務の遂行状況を確認する必要がある。また、金融機関等と外部委託先の業務範囲及び責任について、委託契約の内容に応じ、相互牽制を有効に機能させる必要がある。
   なお、組織の整備及び相互牽制については【統 12】を参照のこと。

   業務遂行状況の確認方法としては、以下の例がある。
   (1) 外部委託先の管理状況を把握する。
      ①管理責任者より状況を聴取する。
      ②定期的に作業状況の報告を受ける。また、定められた場所以外で作業が行われていないことを確認する。
      ③作業の機密管理状況の報告を受ける。また、定められた場所以外には情報が持ち出されていないことを確認する。
      ④外部委託先における業務遂行に関する重要な事項の変更（管理責任者の交替、システム更新など）の報告を受ける。
      ⑤セキュリティに関する事故及び犯罪の報告を受ける。
   (2) 外部委託先における業務の遂行状況について監査等を行う。
      確認した結果及び認識した問題点については、その影響度に応じて、経営層へ適切な報告を行う。なお、監査については【監 1】を参照のこと。
   (3) 外部委託先における業務の遂行状況を定期的にモニタリングする。
      金融機関等は、担当要員を選定するなど、外部委託先における顧客データ等の管理状況、データ漏洩防止に関する対策の遂行状況及び開発・運用状況等について把握する。

2. 金融機関等は、外部委託先による業務の成果が金融機関等の求めるレベルに達しているかを把握する必要がある。例えば、システム開発を委託する場合は、機能要件の充足度、標準化遵守状況の確認及び異例処理等を含んだ検証テストを行うことなどが考えられる。
   なお、この業務の成果を計測するために、ベンチマークである SLA をあらかじめ外部委託契

約の１つとして金融機関等と外部委託先の間で締結し、これに対する評価を定期的に行うことが有効である。SLA の締結については【統 21】を参照のこと。
また、認識された問題点については、外部委託先と連携して速やかに対応することが必要である。

2 外部の統制
(2) クラウドサービスの利用

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　24	クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること。

クラウド事業者に対する統制を十分かつ実効的に機能させるため、クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること。

1. クラウドサービスを利用する場合、クラウド事業者の選定時に、利用するサービスの内容及びリスク特性等に応じて、統制対象クラウド拠点（注）を把握する必要がある。なお、統制対象クラウド拠点は、実質的な統制が可能となる地域（国、州等）に所在することが必要である。なお、特定システムにおいては、この措置は必要である。

   （注）統制対象クラウド拠点とは、データやシステムに対する実効的なアクセスを行う拠点のことを指している。そのため、クラウドサービスにおける情報処理の広域性を勘案し、金融機関等が統制を行うべき対象となる。統制対象クラウド拠点は、クラウド事業者のデータセンター、オペレーションセンター、本社、営業所等様々な拠点が候補となるが、金融機関等によって、利用するクラウドサービスの内容やクラウド事業者の内部管理状況等を踏まえ、金融機関等が個別に特定することとなるため、上記の候補以外が対象となる場合もある。

2. 金融機関等は、統制対象クラウド拠点に対して必要となる権利（監査権等）を確保するために、利用するサービスの内容及びリスク特性等に応じて、クラウド事業者と交わす契約書等にその権利を明記する必要がある。なお、特定システムにおいては、この措置は必要である。

3. 監査の実施にあたっては、技術の先進性などを考慮し、クラウド事業者が監査人に保証型監査を委託（または同等の効力を有する監査を実施）し、その監査報告書を利用することが望ましい。なお、特定システムにおいてクラウドサービスを利用する場合、定期的に監査を実施する必要がある。監査の方法については【監 1】を参照のこと。

4. 特定システムにおいてクラウドサービスを利用する場合、クラウド事業者に対する監査及びモニタリングを実効的に実施するため、クラウド事業者において採用されている技術など専門知識を有する人材を配置する必要がある。ただし、金融機関等内部で確保・育成することが困難な場合においては、専門性を有する第三者監査人等を利用することで代替することも可能である。

5. クラウドサービスの利用にあたっては、新しい技術によってサービス内容及び利用形態が変化す

る可能性があるため、検討時点から広義の IaaS，PaaS，SaaS 等のクラウドサービスの利用形態を考慮し、金融機関等とクラウド事業者との責任範囲を明確にした上で利用を開始することが望ましい。

2 外部の統制
(3) 共同センター

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　25	共同センターにおける緊急事態の発生に備えて安全対策を講ずること。

勘定系システムにおいて共同センターを利用する場合、緊急事態の発生時に迅速な初動対応が取れるよう、適切な安全対策を講ずること。

1. 勘定系システムにおいて共同センターを利用する場合、緊急事態の発生に備えて適切な安全対策を講ずることが必要である。
   共同センターにおいては、緊急事態が発生した際の関係者が複数金融機関等にまたがり、対応方針を相互に合意するのに時間を要する可能性がある。そこで、対応に関する意思決定を迅速化するため、コンティンジェンシープランには初動対応を決定するための手順を盛り込み、利用金融機関等及び共同センターと合意しておくことが考えられる。
   想定される緊急事態については、【実 73】を参照のこと。

   ここでいう共同センターには、勘定系システムにおいて共同利用型のクラウドサービスを利用する場合も含まれる。

   迅速な初動対応を可能とする手順としては、以下の例がある。
   (1) 利用金融機関等の利益を代表する共同運営組織が緊急事態発生の際の初動対応を決定する。
   (2) 緊急事態発生時に初動対応を決定する金融機関等を事前に定める。
   (3) 一定の影響範囲内の障害においては、共同センター側があらかじめ合意された対応を実施したうえ、利用金融機関等に事後報告する。
   (4) 初動対応の定期的な訓練（机上訓練含む）を行う。
   (5) コンティンジェンシープランの定期的な見直しを行う。　等

2. 安全対策の検討にあたっては、緊急事態の発生等に備えて必要となる IT 人材を、継続して配置するために、利用金融機関等または、利用金融機関等と共同センターとの間で人員計画を策定することが望ましい。

2 外部の統制
(4) 金融機関相互のシステム・ネットワークのサービス

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

統 26	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、CD･ATM オンライン提携などを行ううえで、基幹インフラとしての機能を担っている。仮に当該システム・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、金融機関等は適切なリスク管理を行うこと。

1. 金融機関等が業務を外部委託する場合は、金融機関等みずからが、外部委託先の選定及び委託内容（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等が共同で利用しているという特徴がある。
   このため、各金融機関等が、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及び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) 金融機関等は、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。
   具体的には、金融機関等は、①サービスの管理者から受領した監査報告を評価する、②金融機関等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 ベンダーであり、サービスを利用する金融機関の代表組織等が組織運営に関わる際には、代表組織等が、金融機関等に代わり、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、各金融機関等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、金融機関等みずからも、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。
   具体的には、①当該サービスとの接続テストにより、金融機関等のシステム（外部委託するシステムを含む）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、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。

(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、金融機関等が主導的な役割を果たしている場合には、金融機関等は、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。
具体的には、金融機関等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。

（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、金融機関等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も考えられる。

（注 2）金融機関等が利用する当該サービスを管理する組織。金融機関等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。

VI. 実　務　基　準

1 情報セキュリティ
(1) データ保護

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　1	他人に暗証番号・パスワード等を知られないための対策を講ずること。

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。

暗証番号・パスワードの利用等における安全対策上の機能としては、以下の例がある。
(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り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) 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
(5) 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
(6) 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機能
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。
(7) アクセスの都度、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方式としては、以下の例がある。
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。
a.ワンタイムパスワードはランダムに生成されること
b.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
c.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。

(8) 盗撮カメラ等が発する電波をもとに不正な機器の設置を検知する機能

CD・ATM 等の覗き見防止の対策としては、以下の例がある。

(1) 画面の表示上の対策（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

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【実 26】参照のこと。

2. インターネットバンキングや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、安全対策上の機能を設けることが望ましい。

安全対策上の機能としては、以下の例がある。

(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

3. 暗証番号・パスワード等をデータ伝送する場合は、他人に知られないように、暗号化等の対策を検討する必要がある。伝送データの暗号化策については【実 4】を参照のこと。

4. 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【実 108】を参照のこと。

1 情報セキュリティ
(1) データ保護

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実　2	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。

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。
   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。

   接続相手端末確認としては、以下の例がある。
   (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【実 8】

2. 公衆通信網を通じてパソコン、コンピュータ等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。【実 8】

1 情報セキュリティ
(1) データ保護

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実　3	蓄積データの漏洩防止策を講ずること。

ファイルの不正コピー、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データ保護の対策を講ずること。

1. ファイルの不正コピー、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データ保護の対策を講ずることが必要である。
   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。

   パスワード設定の内容としては、以下の例がある。
   (1) データベース　：DBMS の備えるパスワード【実 5】
   (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。

2. 外部持ち出し及び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、【実 8】を参照のこと。
   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。

3. 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、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、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。

4. 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）

5. 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。

端末機器からの漏洩防止策としては、以下の例がある。
(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。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を行う。
(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【実 25】

（参考 1）
暗号化の方式としては、以下の例がある。
(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。

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、対策を講じることが考えられる。

電磁波の盗聴対策としては、以下の例がある。
(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。

1 情報セキュリティ
(1) データ保護

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実　4	伝送データの漏洩防止策を講ずること。

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データ保護の対策を講ずること。

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、データ保護の対策を講ずることが必要である。
   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。

   個人データを伝送する場合には、上記以外の対策としては、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
   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。

2. 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。

3. 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が望ましい。

4. 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、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。

   データ伝送上の暗号化としては、以下の例がある。
   (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 1）

無線 LAN を使用する際に考慮する点としては、以下の例がある。

(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 29 年８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。

①「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

②「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

③「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

（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考えられる。

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考えられる。

暗号化の方法としては、以下の例がある。

(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 7 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

1 情報セキュリティ
(1) データ保護

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　5	ファイルに対するアクセス制御機能を設けること。

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。

   アクセス制限の方法としては、以下の例がある。
   (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

2. 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。

   アクセス権限チェックの内容としては、以下の例がある。
   (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。

1 情報セキュリティ
(1) データ保護

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　6	不良データ検出機能を充実すること。

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. 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が必要である。

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は、以下の例がある。

(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としては、以下の例がある。

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。

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。

なお、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。

(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。
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【実 10】を参照のこと。

1 情報セキュリティ
(1) データ保護

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実　7	伝送データの改ざん検知策を講ずること。

データの改ざんを早期に発見するため、重要なデータの伝送において、改ざん検知のための対策を講ずること。

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ずることが望ましい。
   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を講ずることが必要である。

   暗号技術を活用した認証機能、改ざん検知機能としては、以下の例がある。
   (1) メッセージ認証コード
   (2) 電子署名

参照法令	電子署名及び認証業務に関する法律

1 情報セキュリティ
(2) 不正使用防止

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　8	本人確認機能を設けること。

不正使用防止のため、業務内容、接続方法等に応じ、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必要である。

2. インターネットを介した電子的な取引、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。

本人確認の方法としては、以下の例がある。

(1) 広義のパスワード
- ①暗証番号
- ②ID・パスワード
- ③イメージ連想
- ④ワンタイムパスワード
- ⑤チャレンジ・レスポンス方式

(2) 暗号利用
- ①共通鍵方式
- ②公開鍵方式
- ③電子署名
- ④認証機関が発行する電子的な証明書

(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）
- ①指紋
- ②声紋
- ③掌紋
- ④網膜パターン
- ⑤虹彩
- ⑥筆跡
- ⑦顔

(4) 所有物
- ①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）
- ②IC カード（注）

③パスワード生成機
④携帯電話の識別番号
(5) これらの併用

端末確認の方法としては、以下の例がある。
(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

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、【実 1、実 25～27、実 62、実 107】を参照のこと。

3. 端末の操作、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。

上記の方式としては、以下の例がある。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。
(1) 乱数表
(2) IC カード
(3) パスワード生成機、または電子メール等によるワンタイムパスワードの通知
(4) スマートフォン等パソコン以外からの端末からの取引制限機能
(5) 電子証明書
USB メモリー等、操作を行う端末以外の媒体に電子証明書を保存し、取引利用時以外は当該媒体を用いないことも被害の予防に有効である。

4. 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。

5. 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、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。【実 107】

6. 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。

(1) タイムシンクロナス方式

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。

(2) チャレンジ・レスポンス方式

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）

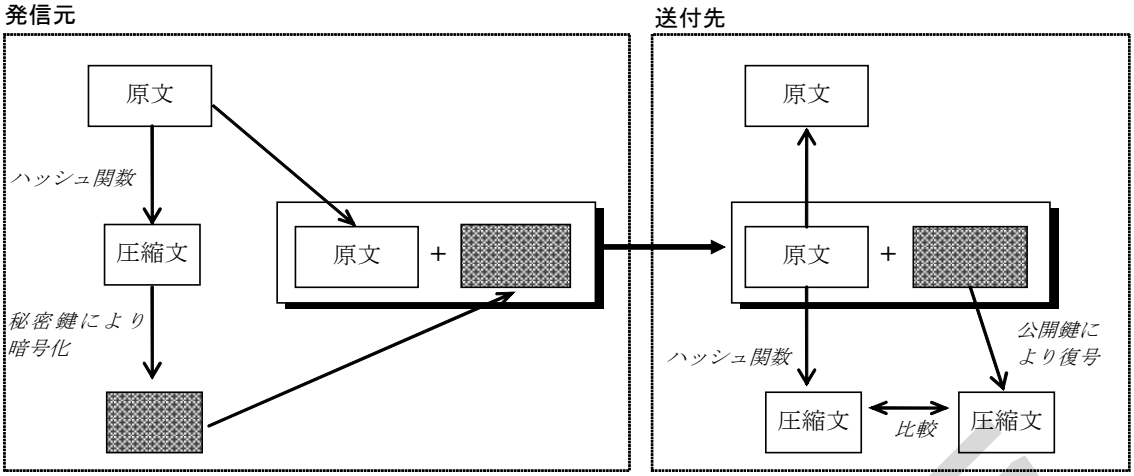
Web サーバーに対して発行される電子証明書であり、クライアントからサーバーの実在を確認する技術。信頼できる第三者機関に申請し発行される証明書を使用することが望ましい。なおその証明書として、発行者によるサイト運営組織・企業の審査に一定の基準を設けた EV SSL 証明書がある。

（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 による適用も可能であるが、無線 LAN による利用が進んでいる。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及び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。
①十分に複雑な乱数表を用いる。
②一定期間（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

1 情報セキュリティ
(2) 不正使用防止

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　9	ID の不正使用防止機能を設けること。

不正使用防止のため、システム、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、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、ID の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【実 16】を参照のこと。

   不正使用防止のための機能としては、以下の例がある。
   (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。
   ①前回のアクセス日付、時刻、状況
   ②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については【実 1】を参照のこと。
   (6) 総当り攻撃（ブルートフォース攻撃及びリバース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による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。

①一定回数ログオン操作を中断・再開した場合、ロックする。

②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については【実 8】を参照のこと。

(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、覗き見による漏洩を防止する。

(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に、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。

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。

1 情報セキュリティ
(2) 不正使用防止

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　10	アクセス履歴を管理すること。

アクセス状況を管理するため、システム及び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内容としては、以下の例がある。
   (1) 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）
   (2) 不正なアクセス要求（指示端末、時刻、ID）
   (3) システムによって失効とされた ID
   (4) 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
   (5) 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。
   (1) 本人確認機能を設けること【実 8】
   (2) 他人に暗証番号・パスワード等を知られないための対策を講ずること【実 1】

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、改ざん及び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、以下の例がある。
   (1) 暗号化して保管する。
   (2) 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。
   (3) 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。

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。
   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、ログとして取得することが必要である。

   取得すべき情報としては、以下の例がある。
   (1) 口座番号
   (2) ユーザーID
   (3) 取引日時
   (4) 取引先口座
   (5) 取引金額
   (6) 取引時の IP アドレス
   (7) 取引時のポート番号
   (8) 画面遷移

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。
   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、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。

   当該取引を特定できる情報としては、以下の例がある。
   (1) 取引日時
   (2) CD・ATM 等の端末情報
   (3) 取引の種類
   (4) 口座番号
   (5) 取引金額

（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

1 情報セキュリティ
(2) 不正使用防止

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　11	取引制限機能を設けること。

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が必要である。
   なお、取引制限機能を設ける際には、取引及び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等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。
   また、1日当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日当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、窓口等における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。

取引・業務内容の制限要因としては、以下の例がある。
(1) 端末の種類によって業務を制限する。
　①開発用端末
　②窓口端末
　③CD・ATM 等
　④渉外端末
(2) 端末の設置場所によって取引を制限する。

①CD・ATM 等
②渉外端末
③顧客・企業設置端末

取引制限の内容としては、以下の例がある。

(1) 取引金額を制限する。
(2) 電子的価値の蓄積可能額を制限する。
(3) サービス内容を照会取引に限定する。
(4) 資金移動取引において、振込先を限定する。
(5) 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。
(6) 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。
(7) 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。

3. 取引制限機能を設ける際には、当該取引及びサービスの特性（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。

1 情報セキュリティ
(2) 不正使用防止

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実　12	事故時の取引禁止機能を設けること。

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. 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が必要である。
   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が必要である。

   取引を禁止する対策としては、以下の例がある。
   (1) 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。【実 64】

1 情報セキュリティ
(2) 不正使用防止

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実　13	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。

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、秘密鍵は別の機器及び媒体に確保し、必要時にその機器、媒体を接続して使用することが必要である。

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、複数の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。

   セキュリティ確保のための手段としては、以下の例がある。
   (1) IC カードにおける耐タンパー性のような保護機能
   (2) ID、パスワード等によるアクセス制限
   (3) 暗号を用いた蓄積

1 情報セキュリティ
(3) 外部ネットワークからの不正アクセス防止

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 14	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。

不正侵入を防止するため、重要なデータ及び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. 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、重要なデータ及び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。

   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、公衆回線網等を指している。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、途中まで専用線で接続し、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接続する場合（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. 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、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。

3. 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、サーバー等の脆弱性対策を行うことが必要である。【実 10、実 16、実 34】

   不正侵入防止策としては、以下の例がある。

   (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。

4. 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。

5. 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。【実 20】
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。さらに、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、脆弱性の有無や程度を検証する手法である。

なお、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）も有効である。

6. 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。

7. 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望ましい。【実 8】

8. 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。

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。【実 112】（参考 3）

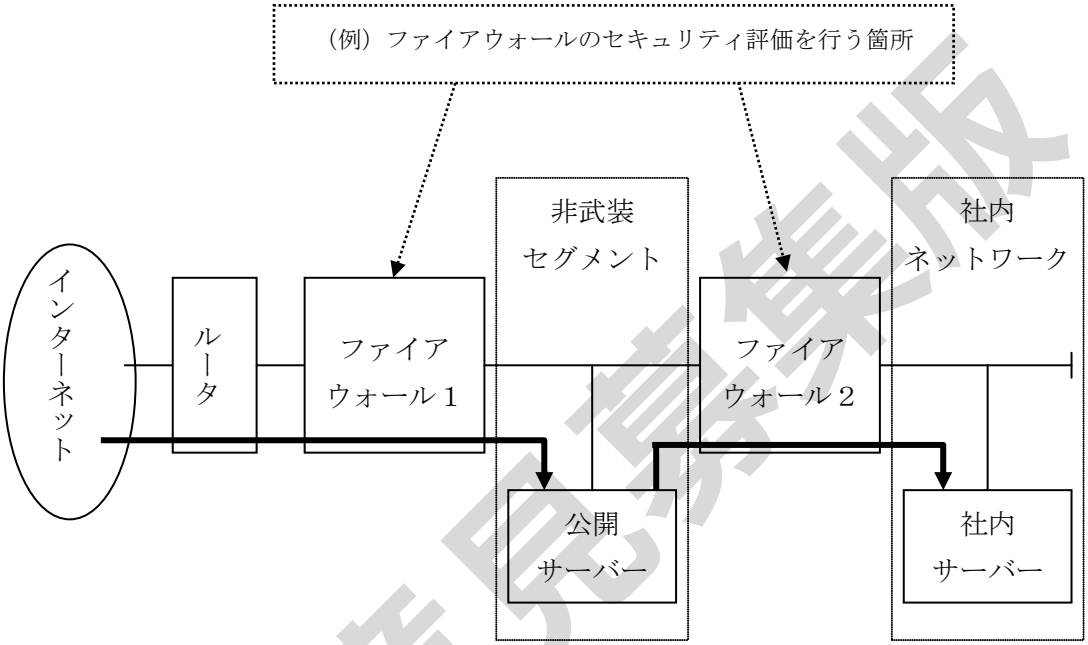


図１　非武装セグメントの構成例

（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による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に加え、以下の例がある。【実 4】（参考 1）

(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。

(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【実 19】を参照のこと。

（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、及び関係者間における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

1 情報セキュリティ
(3) 外部ネットワークからの不正アクセス防止

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　15	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。

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、管理及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方法としては、以下の例がある。

   (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）は、不正使用の防止、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ことが必要である。

   セキュリティを考慮した設定としては、以下の例がある。

   (1) 基本ソフトウェアの脆弱性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) ソフトウェアには、脆弱性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。

1 情報セキュリティ
(4) 不正検知策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　16	不正アクセスの監視機能を設けること。

不正アクセスを早期に発見するため、アクセスの失敗及び不正アクセスを監視する機能を設けること。

1. 不正アクセスを早期に発見するため、アクセスの失敗及び不正アクセスを監視する機能を設けることが必要である。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が必要である。
   (1) アクセスの失敗を記録する機能を設けること。
   (2) 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。

   不正アクセスの監視機能を使用した対策としては、以下の例がある。
   (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。

1 情報セキュリティ
(4) 不正検知策

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実　17	異常な取引状況を把握するための機能を設けること。

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整備することが必要である。【実 109】
   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。

   異常な取引状況を把握するための機能としては、以下の例がある。
   (1) カードの異常取引
   ①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。
   ②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。
   ③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、カード取引の停止、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。

2. 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、以下の例がある。

(1) 顧客の一般的な取引パターンから逸脱した取引などを検知する

(2) 前回の取引日時をログオン時に表示する

(3) 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

(4) 過去の取引履歴について顧客から参照可能とする

(5) 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

1 情報セキュリティ
(4) 不正検知策

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実　18	異例取引の監視機能を設けること。

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としては、以下の例がある。
   (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

   ここでいう役席カードとは、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を指し、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が必要である。

1 情報セキュリティ
(5) 不正発生時の対応策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　19	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。

不正アクセスの拡大防止のため、対応策、復旧手順を明確にするとともに、不正アクセスが発生した場合は、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、復旧策を明確にすることが必要である。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、以下の例がある。
   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。
   ③不正アクセス元からのアクセスを遮断する。

   (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することが必要である。
   なお、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が必要である。

   事前に復旧手順を明確にすべき事象としては、以下の例がある。
   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

   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する必要がある。

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することが望ましい。

復旧の対応としては、以下の例がある。

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。

2. 不正アクセスの再発防止のためには以下の対応が必要である。

(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、以下の例がある。

①アクセス制限を強化する。

②不正アクセスに使用された ID 及び他の ID のパスワードを変更する。

③システムに脆弱性があった場合、それに対する対応策を講ずる。

1 情報セキュリティ
(6) 不正プログラム対策

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 20	コンピュータウイルス等の不正プログラムへの防御対策を講ずること。

開発、保守、運用時における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及び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に、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。

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
①電子メールの添付ファイルからの侵入
②インターネットのダウンロードプログラムからの侵入
③パッケージプログラムからの侵入
④可搬記憶媒体からの侵入
⑤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【実 14】

(2) 不正アクセスによるプログラムの改ざん
①トロイの木馬を使った改ざん
②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
③システムのテスト機能等を無権限利用した改ざん
④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
⑤OS 等の脆弱性を突いた改ざん
⑥端末等のシステムのテスト機能等を利用した改ざん
⑦システムデモや研修用 ID を利用した改ざん
⑧Web 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
①取引プログラムへの不正処理の組込み
②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
③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

防御策としては、以下の例がある。

(1) コンピュータウイルスの侵入

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。

抗ウイルスソフトを有効とするために、最新のウイルスパターンファイルを利用する仕組みを構築する。

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

a.ファイルに対するアクセス制御機能を設けること。【実 5】

b.本人確認機能を設けること。【実 8】

c.ID の不正使用防止機能を設けること。【実 9】

②不正侵入防止機能の導入

a.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。【実 14】

③不正アクセスの要因除去

a.ID、パスワード等の漏洩防止

(a) 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。【実 1】

(b) 蓄積データの漏洩防止策を講ずること。【実 3】

(c) 伝送データの漏洩防止策を講ずること。【実 4】

b.OS 等の脆弱性への対応

c.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ための対策を行う。

①必要となるセキュリティ機能を取り込むこと。【実 89】

②設計段階におけるソフトウェアの品質を確保すること。【実 90】

③プログラム作成段階における品質を確保すること。【実 91】

④テスト段階におけるソフトウェアの品質を確保すること。【実 92】

⑤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。【実 94】

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。

①アプリケーションを難読化すること。

②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。

2. OS 等の脆弱性及び 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に、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、金融機関等からの電子メールを装い、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。

①EV 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。

②Web 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。

③ID・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) 電子メールの対策（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。

⑤HTML 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

①Web 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。
   (1) 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

1 情報セキュリティ
(6) 不正プログラム対策

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 21	コンピュータウイルス等の不正プログラムの検知対策を講ずること。

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及び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、組込み等）に対する防御策を講じていても、技術の進展、サービス環境の変化、システムの拡張及び変更等により、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及び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、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、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（侵入及び組込みの手口）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、ガイド等を参考にすることも有用である。

   検知対策としては、以下の例がある。

   (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及び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）またはスパイウェア対策ソフトにて検知する。なお、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し、定期的にウイルスチェックを行う。また、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。

   (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、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。
   アクセス履歴の管理については【実 10】を参照のこと。

   (3) 資源管理による検知
   システム資源（ファイル容量、メモリ容量、CPU 使用時間等）の使用状態をチェックし異常、特異な傾向等を検知することにより、不正処理プログラムの侵入、組込みを検知する。

(4) ライブラリ管理などによる検知

①ファイル更新履歴を管理することにより、不正更新及び不正プログラムの追加を検知する。

②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、購入したプログラム原本ファイル等）と運用中のファイルとを比較し不正プログラムの侵入、組込みを検知する。

③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。

1 情報セキュリティ
(6) 不正プログラム対策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　22	コンピュータウイルス等の不正プログラムによる被害時対策を講ずること。

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を検知または発病、あるいは不正プログラムを発見した場合に備えた対策を講ずることが必要である。
   当該システム及び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、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。

   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。

   コンピュータウイルスの感染が発見、または発病した場合の対応手順としては、以下の例がある。
   (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

2. 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。

2 システム運用共通
(1) マニュアルの整備

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　23	通常時マニュアルを整備すること。

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. 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が必要である。
   なお、マニュアルはシステム変更等が発生した都度、定められた手続きに従って見直しを行い、常に最新の状態にすることが必要である。
   また、通常時マニュアルの整備後、遵守について関連部門に周知徹底させることが必要である。

   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。

   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 【実 25～27】
   (2) オペレーション管理 【実 35～38】
   (3) データファイル管理 【実 28、実 29、実 39】
   (4) プログラムファイル管理 【実 40、実 41】
   (5) 運用時ドキュメント管理 【実 44、実 45】
   (6) 帳票管理 【実 67、実 68】
   (7) 出力管理 【実 66】
   (8) カード管理 【実 107、実 110】
   (9) 資源管理 【実 47】
   (10) 外部接続管理 【実 33、実 34】
   (11) 機器の管理 【実 49～51】
   (12) 運行監視 【実 46】

2. 本部・営業店等における通常時マニュアルには、上記の他、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

マニュアルに盛り込む要件としては、以下の例がある。

(1) 記述内容

①職務遂行に必要な基本事項に関する基準・規則・手続き

②特定の事務処理に関する具体的な流れ・手続き

③①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) その他例外規則等

2 システム運用共通
(1) マニュアルの整備

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　24	障害時・災害時マニュアルを整備すること。

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並びに本部・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が必要である。

   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。
   (1) 障害時・災害時対応策　【実 70～72】
   (2) コンティンジェンシープランの策定　【実 73】

2. 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、最新の状態にすることが必要である。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に、作業手順等を明確にすることが望ましい。

3. 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、以下の内容を含んでいることが必要である。【実 70～72】
   (1) 端末機器の取扱い
   (2) 事務手続き

2 システム運用共通
(2) アクセス権限の管理

適 用 区 分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 25	各種資源、システムへのアクセス権限を明確にすること。

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. 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。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。
   (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。

   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ている。

   アクセス権限の確認に利用される機能については【実 1、実 5、実 8、実 26】を参照のこと。また、アクセス権限管理の具体的な注意点は【実 27】を参照のこと。

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。【実 10】

2 システム運用共通
(2) アクセス権限の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　26	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。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。
   (1) 推測されやすいパスワードを設定しないこと
   (2) パスワード等を他人に知られないようにすること
   (3) 他人のパスワード等を使用しないこと
   (4) 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

   推測されやすいパスワードとしては、以下の例がある。
   (1) 桁数の短いパスワード
   (2) ID と同一のパスワード
   (3) 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
   (4) 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
   (5) 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
   (6) よく使われる英語の単語
   (7) 上記の逆読みやそれらの組合せ

2. 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に、適宜変更することが必要である。また、パスワードが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。
   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【実 1】を参照のこと。

2 システム運用共通
(2) アクセス権限の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　27	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にすること。

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。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にすること。

1. 各種資源、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、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。

   ここでいう各種資源とは、コンピュータシステムを構成する機器、ファイル等を指す。

   アクセス権限の付与手順としては、以下の例がある。
   (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。

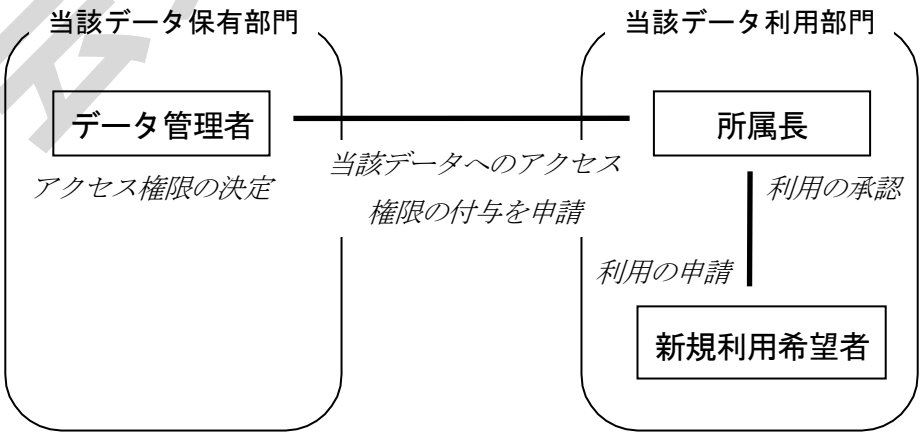


図 1　アクセス権限の取得承認例

2. 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にする必要がある。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。

アクセス権限見直しのタイミングとしては、以下の例がある。

(1) 所属、職制、組織変更時
(2) 入社時、退職時
(3) 長期出張、長期留学、休職
(4) 新システム稼働時
(5) 一定期間経過時

アクセス権限管理の注意点としては、以下の例がある。

(1) ID 等の登録・変更等の管理者を明確にする。
(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する。
(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、利用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再発行する場合には、ユーザーの本人確認などの手続きを明確にする。

2 システム運用共通
(3) データ管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　28	データファイルの授受・管理方法を明確にすること。

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

ここでいうデータファイルとは、サーバー・パソコン・ストレージ等を含むコンピュータの磁気ディスク内のファイル、及び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 等の記憶媒体内のファイルを指している。

データファイルの授受・保管管理方法としては、以下の例がある。

(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。

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、以下の項目を明確にする。

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する。

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する。【実 82、実 83】

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。【実 82、実 83】

(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、廃棄の手続きを明確にする。

(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する。

(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。

(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。

①コンピュータセンター

データ保管室に保管する。

②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。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。

(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。

2 システム運用共通
(3) データ管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　29	データファイルの修正管理方法を明確にすること。

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及び管理は、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。

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) 処理手続きに従っ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が必要である。

2 システム運用共通
(3) データ管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　30	暗号鍵の利用において運用管理方法を明確にすること。

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ること。また、その管理書類等は役席者が厳重に管理すること。

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、有効期限等について手続きを定めることが必要である。

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ることが必要である。
   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、保存等の手続きを明確にするにあたっては、以下の点に留意することが必要である。
   (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 システム運用共通
(4) オペレーション習熟

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　31	オペレーション習熟のための教育及び訓練を行うこと。

コンピュータシステムに係わる通常時運用の円滑化及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及び訓練を行うこと。

1. コンピュータシステムに係わる通常時運用の円滑化及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及び訓練を行うことが必要である。

2. コンピュータシステムのオペレーションの教育及び訓練については、以下の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及び訓練を行うことが必要である。なお、教育及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及び訓練を、責任者を明確にして継続的に行うことが必要である。

3. 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。

2 システム運用共通
(5) コンピュータウイルス対策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　32	コンピュータウイルス対策を講ずること。

コンピュータウイルス等の侵入、及び感染に備えるため、防御、検知、復旧の手順を明確にすること。

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、侵入を事前に防御する対策を講ず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。
   CD･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【実 20】参照のこと。
   (2) 検知対策については【実 21】参照のこと。

2. コンピュータウイルス等の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）。
   【実 20】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の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。
   復旧策については【実 22】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、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 システム運用共通
(6) 外部接続管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　33	接続契約内容を明確にすること。

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、以下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
      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
   (3) 伝送制御手順

①全銀協手順
②JCA 手順
③FTAM（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.初回申込及び変更時の通話による電話番号確認
b.初回申込及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) 伝送不能等の障害時の対応方法

2 システム運用共通
(6) 外部接続管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　34	外部接続における運用管理方法を明確にすること。

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、定められた規則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. インターネットの利用、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。

運用管理方法としては、以下の例がある。

(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【実 2、実 8】を参照のこと。

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【実 1、実 26】を参照のこと。

(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は以下の点を定め、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【実 10、実 16】を参照のこと。

(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) 脆弱性等への対応

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、脆弱性等の情報を収集し、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。

緊急度や重要度の判断としては、以下の例がある。

①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。

②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。

3. 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【実 118】を参照のこと。

3 運行管理
(1) オペレーション管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎				

実　35	オペレータの資格確認を行うこと。

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、臨時処理及び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。

資格確認の具体的な内容としては、以下の例がある。

(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は、以下の例がある。

①制服の着用
②腕章の着用
③名札の着用

3 運行管理
(1) オペレーション管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実　36	オペレーションの依頼・承認手続きを明確にすること。

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。

3. 臨時処理及びトラブル発生にともなう例外処理についても、手続きを明確に定め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必要がある。

3 運行管理
(1) オペレーション管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実　37	オペレーション実行体制を明確にすること。

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。

1. 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必要がある。

ここでいうオペレーション実行体制とは、オペレーションにおける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。

オペレーション実行体制に係わる対策としては、以下の例がある。

(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、運用業務の規則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）【実 104】

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。

2. 事故及び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。

3. 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
   オペレーションの自動化、簡略化については【実 99】参照のこと。

4. 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。

3 運行管理
(1) オペレーション管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実　38	オペレーションの記録、確認を行うこと。

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に、オペレーション記録を残すことが必要である。

   オペレーション記録の方法としては、以下の例がある。

   (1) 運行状況を確認するため、以下のチェックリストを作成する。
   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に以下の引継事項を明確にする。
   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、以下の例がある。
   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部門の責任者に報告する。

3 運行管理
(2) データファイル管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　39	データファイルの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及び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. 障害及び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、その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必要がある。

   バックアップを取得するにあたっての留意事項としては、以下の例がある。
   (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。

2. 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、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が必要である。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）。

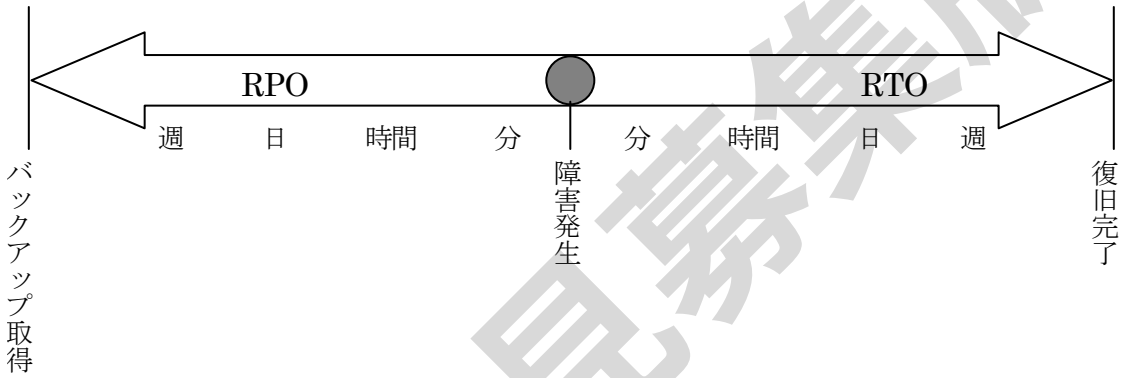
3. 保管場所の選定にあたっては、本番ファイル保管場所（現有システム保有場所）とリスク要因（火災、地震、停電等）を共有しないこと、及び被災時の復旧に際しての現有システムへのファイル移送時間の考慮等も含め、総合的に判断することが望ましい。
   特に業務または組織の存続のために重要なデータファイルについては、大規模災害も想定して検討することが必要である。
   また、保管を外部に委託する場合は、信頼性、安全性、可用性（保管データを必要時にいつでも利用可能か、等）についても考慮する必要がある。
   なお、バックアップされたデータの持出しにあたっては部門責任者の承認を得て行い、持出

し記録については所定期間保存する必要がある。

バックアップデータの保管方法については【実 28】を参照のこと。

4. イントラネット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。

3 運行管理
(3) プログラムファイル管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　40	プログラムファイルの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. 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プログラムファイルは分けて管理することが必要である。

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及びロードモジュールを指し、また、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している。

プログラムの管理方法としては、以下の例がある。

(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【実 48】を参照のこと。

(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従って行う。
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。
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。

3 運行管理
(3) プログラムファイル管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　41	プログラムファイルのバックアップを確保すること。

プログラムの障害、災害等への対応のため、プログラムファイルのバックアップを取得し、保管管理方法を明確にすること。

1. コンピュータウイルス等の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、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ファイル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。

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、取得タイミングを定めておくことが必要である。品質確保については【実 96】を参照のこと。
   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）。

3. 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。
   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。

4. バックアップされたプログラムファイル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。

3 運行管理
(4) ネットワーク設定情報管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　42	ネットワークの設定情報の管理を行うこと。

ネットワーク設定情報の不正な変更への対応のため、設定情報を適切に管理すること。

1. ルータ等ネットワーク機器の設定は、定められた手続きに従って変更することが必要である。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【統 8】を参照のこと。

2. 外部ネットワーク（インターネット・公衆回線網等）に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. ルータ等へのアクセスについては、ID、パスワード等による保護、アクセス履歴を管理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。
   (1) 本人確認機能を設けること 【実 8】
   (2) 他人に暗証番号・パスワード等を知られないための対策を講ずること 【実 1】

3 運行管理
(4) ネットワーク設定情報管理

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　43	ネットワークの設定情報のバックアップを確保すること。

ネットワーク設定情報の不正な変更、障害、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. ルータ等のネットワーク機器の設定が不正に変更されたり、障害、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取得し、管理方法を明確にすることが必要である。

   バックアップの方法については【実 39】を参照のこと。

3 運行管理
(5) 運用時ドキュメント管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　44	運用時のドキュメントの保管管理方法を明確にすること。

不正使用、改ざん、紛失等を防止するため、運用時の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. 不正使用、改ざん、紛失等を防止するため、運用時のドキュメントは定められた方法によって管理することが必要である。

   ここでいう運用時のドキュメントとは、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。なお、ドキュメントの形態には、印刷物のみならず電子媒体上の文書ファイル等も含んでいる。

   ドキュメントの管理方法としては、以下の例がある。
   (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。

2. 重要なドキュメントの複写・複製については、管理方法を明確にすることが必要である。

3 運行管理
(5) 運用時ドキュメント管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　45	ドキュメントのバックアップを確保すること。

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。

   災害時の復旧対応のために必要なドキュメント（印刷物のみならず電子媒体上の文書ファイル等も含む）としては、以下の例がある。

   (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）

   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、以下の例がある。取得サイクルについては【実 39】を参照のこと。

   (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）。

2. 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。
   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、バックアップされたドキュメント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。

3. 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。

（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。

3 運行管理
(6) 運行監視

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　46	システムの運行状況の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、監視対象、監視内容及び監視方法等の監視体制を整備することが必要である。
なお、異常状態及び不正使用を発見したときの対応方法を明確にすることも必要である。

監視体制の整備にあたり明確にすべき事項としては、以下の例がある。

(1) 監視対象・内容

①システムの異常状態を早期発見するための監視

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不正使用の発見・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、以下の点を把握する。

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。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。

①システム異常早期発見のための監視

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

監視機能については【実 16、実 101、実 102】を参照のこと。
障害検出機能については【実 103】を参照のこと。
障害時・災害時の対応策については【実 70～72】を参照のこと。
異常取引検知機能については【実 17】を参照のこと。