平成 29 年 9 月 12 日
公益財団法人 金融情報システムセンター

第 56 回　安全対策専門委員会　議事次第

Ⅰ　日時

平成 29 年 9 月 12 日（火）　15:00～17:00

Ⅱ　場所

FISC 会議室

Ⅲ　議事次第

１．	15:00	開会
		次第説明
２．	15:10	【議案１】基礎基準・付加基準の整理
３．	15:50	【議案２】外部委託管理関連基準の改訂について
４．	16:20	【議案３】「読みやすさ対応」統制基準の一部再編・見直しについて
５．	16:50	事務連絡
		委員会開催日程について
６．	17:00	閉会

Ⅳ　資料

【資料１－１】　基礎基準・付加基準の整理
【資料１－２】　基準解説部分の解釈例
【資料１－３】　基礎基準案のベストプラクティス基準
【資料１－４】　付加基準案のベストプラクティス基準
【資料２－１】　外部委託管理関連基準の改訂について
【資料２－２】　外部委託管理関連基準改訂原案
【資料３－１】　「読みやすさ対応」統制基準の一部再編・見直しについて
【資料３－２】　改訂原案（統制基準再編）
【資料３－３】　統制基準再編（内容一覧）
【資料３－４】　新基準構成案（再編後）
【資料４－１】　平成 29 年度 安全対策専門委員会開催日程（改訂）
【資料４－２】　検討事項に関するご意見（メール回答用）

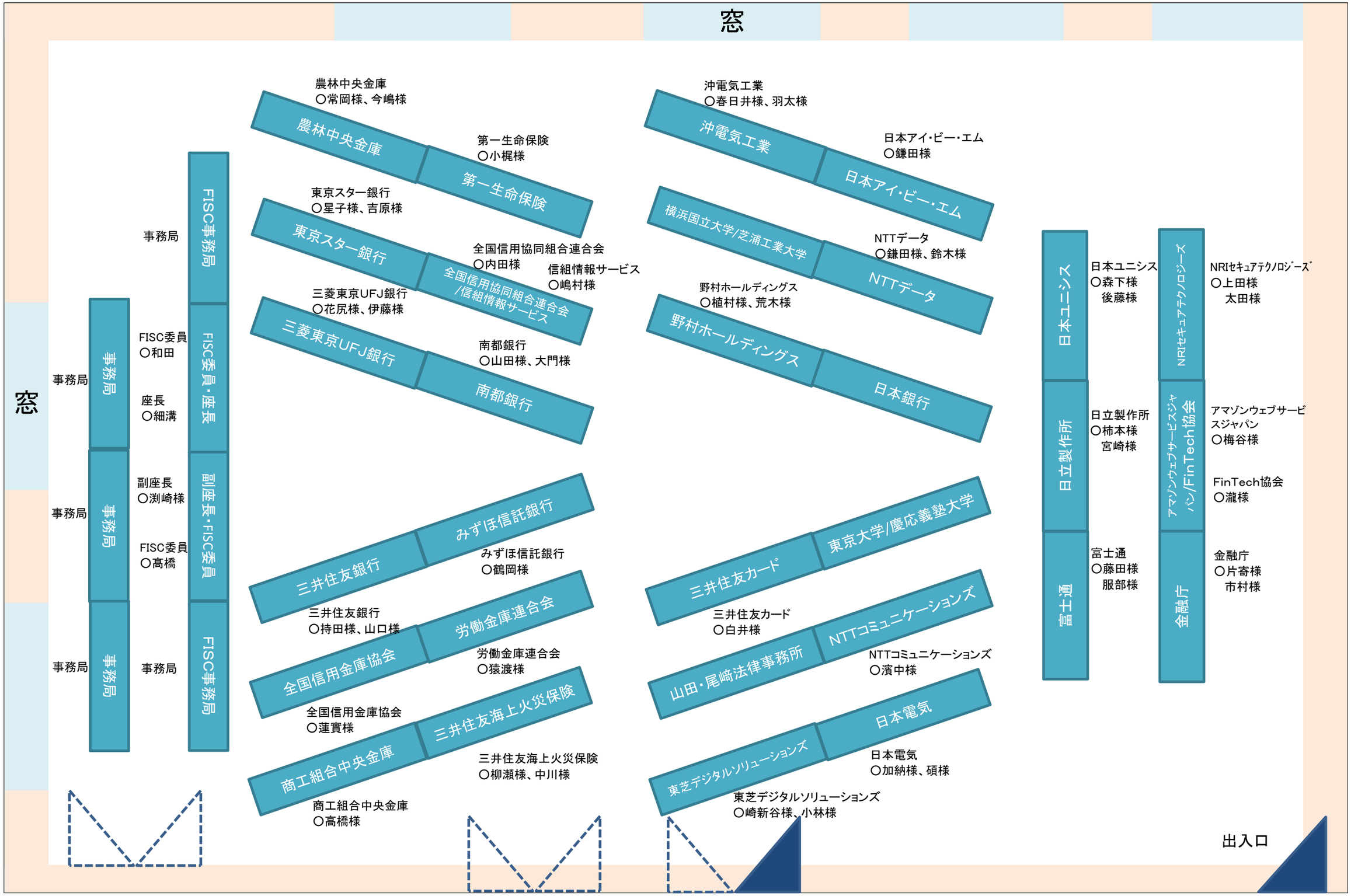
Ⅴ　今後の予定

○第 57 回　安全対策専門委員会
（予定）平成 29 年 10 月 17 日（火）15:00～17:00　FISC 会議室

以上

第56回「安全対策専門委員会」座席表

平成29年9月12日



【資料１－１】
平成 29 年 9 月 12 日
公益財団法人 金融情報システムセンター

基礎基準・付加基準の整理

Ⅰ. 課題認識

○　「基礎基準」の選定に当たっては、４つの考え方[1]に沿って、「安全対策基準」の「基準項目の目的、内容説明、具体例等の解説」（以下「解説部分」という）において、すべての金融情報システムについて最低限必要な対策が記載されているものを選定することが適当と考えられる。

ただし、「解説部分」には、実施が必要な対策（「必要である」と記載されている対策）、ベストプラクティス（「望ましい」と記載されている対策）、例示として示されているものが併記されている状態にある。

こうした基準内容をリスクベースアプローチの考え方に沿って、明確に整理する必要がある。

○　また、「付加基準」の「解説部分」についても、同様の整理を行う必要がある。

Ⅱ. 方針案

- 「基礎基準」の「解説部分」の中で、すべての金融情報システムにおいて適用されるべき最低限必要な対策を「必須対策」と呼ぶ。具体的には、「必要である」と記載されている対策を「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。
- 「付加基準」の「解説部分」の中で、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」と呼ぶ。具体的には、「必要である」と記載されている対策を「必須対策」とする（特定システムでは、「付加基準」の「必須対策」は、必ず適用されることとなる）。
  「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。

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、下表のとおりとなる。

	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（ただし、システムの特性等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、適用は不要）。
・「△」は、選択的に適用。

[1] ①統制・監査に関する基準
②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
③コンティンジェンシープラン策定に関する基準
④システムの運行管理に最低限必要な基準

III. 論点

論点１：「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」と位置付けて良いか。

・「必須対策」から除外すべきもの、記載内容の修正が必要なものはないか。

論点２：「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て良いか。

・「必須対策」と位置付けることが適当なもの、記載内容の修正が必要なものはないか。

論点３：「基礎基準」の候補のうち、「適用にあたっての考え方」が「望ましい」と記載されているものがあるが、その取扱いをどうするか。

・以下の２案のいずれをとるか（それ以外の選択肢はあるか）

第１案

「付加基準」と位置付け、「適用に当たっての考え方」の文末を「～すること」に修正する。また、「解説部分」のうち「必要である」と記載されている対策は「必須対策」とし、それ以外にも「必須対策」とすべき対策については文末を「必要である」に修正する（「必須対策」が示されていないものについては、新規に「必須対策」を記載することが必要か否かを検討する）。

第２案

基準の策定当時は、技術的困難さ等に配慮し、ベストプラクティスとしたものと考えられる。従って、現在では「基礎基準」とすることに支障がない基準については、「基礎基準」として位置付け、それ以外は「付加基準」として位置づける。また、いずれについても、第１案と同様の考え方で、「適用に当たっての考え方」、「解説部分」に所要の修正を行う。

・具体的には、暫定的に「基礎基準」として位置付けた以下の基準が対象となる。修正原案は、別紙【資料１－３】を参照。

番号	基準小項目
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。
実 51	ネットワーク関連機器の保護措置を講ずること。
実 106	オペレーションの自動化、簡略化を図ること。
実 117	相手端末確認機能を設けること。
実 118	蓄積データの漏洩防止策を講ずること。
実 119	伝送データの漏洩防止策を講ずること。
実 123	伝送データの改ざん検知策を講ずること。
実 131	カードの偽造防止対策のための技術的措置を講ずること。
実 132	電子的価値の保護機能、または不正検知の仕組みを設けること。
実 134	電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること。

論点４：「基礎基準」の候補のうち、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」と位置付けることとしてはどうか。

・ 具体的には、暫定的に「基礎基準」として位置づけた以下の基準が対象となる。

基準中項目	番号	基準小項目
渉外端末	実 41	運用管理方法を明確にすること。
カード管理	実 42	カード不正使用を防止すること。管理方法を明確にすること。
ｲﾝﾀｰﾈｯﾄ、ﾓﾊﾞｲﾙ	実 84	不正使用を防止すること。
	実 85	不正使用を早期発見すること。
予防策（不正・偽造防止策）	実 131	カードの偽造防止対策のための技術的措置を講ずること。
	実 132	電子的価値の保護機能、または不正検知の仕組みを設けること。
	実 134	電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること。

・ 実 131、132、134 は、論点３の対象ともなっており、論点４の考え方を取るのであれば、いずれも「付加基準」として位置付けられる。

論点５： 「付加基準」の候補のうち、「適用にあたっての考え方」が「望ましい」と記載されているものがあるが、その取扱いをどうするか。

・ 「適用に当たっての考え方」の文末を「～すること」に修正する。そのうえで、「解説部分」には「必須対策」が示されていないもの（「望ましい」または例示のみを記載）があるが、そのままの表現で良いか（ベストプラクティスのみの基準とすることで良いか）。

・ 具体的には、以下の基準が対象となる。修正原案は、別紙【資料１－４】を参照。

番号	基準小項目
実 86	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。
実 96	回線の予備を設けること。
実 115	バックアップサイトを保有すること。

Ⅳ. 今後の予定

本日ご説明した上記論点について、9/22（金）までに事後意見をいただきたい。事後意見をもとに基準原案の修正を行い、次回委員会において修正原案を提示する予定。「基礎基準」については、論点の検討結果をもとに確定していく。

日程（予定）	内容
9 月 12 日（火）	第 56 回安全対策専門委員会審議（本日論点説明）
9 月 22 日（金）	第 56 回専門委員会事後意見の締切
10 月 17 日（火）	第 57 回安全対策専門委員会審議（修正原案提示）
11 月 21 日（火）	第 58 回安全対策専門委員会審議（「基礎基準」の確定）

以　上

【資料１－２】
平成 29 年 9 月 12 日
公益財団法人 金融情報システムセンター

運用管理
障害時・災害時対応策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 56	障害時・災害時復旧手順を明確にすること。

障害時・災害時におけるコンピュータシステムの早期復旧のため、復旧手順を明確にするとともに、コンティンジェンシープランとの整合性を図ること。

1. 障害時・災害時におけるコンピュータシステムの早期復旧のため、復旧手順を明確にするとともに、コンティンジェンシープランとの整合性を図ることが必要である。

必須対策

復旧手順とは、障害または災害等により正常に稼働しなくなったコンピュータシステムを復旧させるための手続きを明確にしたものである。

用語説明

コンピュータシステムの復旧手順を作成する障害としては、以下の例がある。

例示

(1) コンピュータ装置の故障
(2) 端末機器等の故障
(3) 関連設備（電源、空調、給排水設備等）の故障
(4) 通信回線の障害
(5) ソフトウェアの障害

なお、障害時・災害時の復旧手順において考慮すべき事項としては、以下の例がある。

例示

(1) 業務開始時の手順（システム立上げ時等）
(2) 影響を局所化する縮退等
(3) バックアップシステム（バックアップサイト設置分を含む）への切替え（強制切替え、システム運用時の諸制約等を踏まえた切替え判断及び運用手順、共同センターにおける切替え判断等を含む）
(4) バックアップシステム（バックアップサイト設置分を含む）への切替えによる社内のシステムへの影響確認（周辺システム、EUC システム等）
(5) ファイルの不整合や取引データの欠落の有無の確認手順
(6) 対応要員の確保と当該要員への必要な権限委任
(7) 本部・営業店等への業務影響範囲、復旧見込み等の連絡手順
(8) 社外のシステムへの影響確認（全銀センター、統合 ATM システム、共同 CMS 等の関連会社等）
(9) 稼働に必要な ID・パスワードの取得方法の明確化　【運 18】
(10) バックアップシステム（バックアップサイト設置分を含む）からの切戻しが必要な場合の対応方針、手順等

【資料１－２】
平成 29 年 9 月 12 日
公益財団法人 金融情報システムセンター

2. 業務やシステム運用を外部に委託している場合に、外部委託先が契約どおりに委託業務を遂行できない場合の対応策についても、事前に考慮しておくことが望ましい。

ベストプラクティス

3. 障害時・災害時に使用するバックアップシステム（バックアップサイト設置分を含む）が正常に稼働することを定期的に確認することが必要である。
なお、冗長構成によって信頼性を確保しているシステムにおいては、冗長構成の機器が正常に稼働していることを定期的に確認することが必要である。

必須対策

障害時・災害時復旧については、【技 22～技 24】を参照のこと。

参照

運用管理
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 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。

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

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

操作管理方法としては、以下の例がある。

(1) 作業によって作業者を特定し、作業体制を明確にする。【運 21】
　①データ、プログラムのバックアップ
　②アクセス権限の登録
　③システムのメンテナンス作業
(2) 作業の依頼・承認手続きを明確にする。【運 20】
(3) 作業記録をつける。【運 22】
　①データ、プログラムのバックアップの取得
　②システムのバージョンアップ作業

削除: ○
削除: ○
削除: 運　23
削除: なお、
削除: ようなもの

運用管理
機器の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎	◎		

実 51	ネットワーク関連機器の保護措置を講ずること。

不正使用、破壊、盗難等を防止するため、重要なデータを扱うシステムを構成するネットワーク機器等は、適切な保護措置が講じられていることが望ましい。

1. 重要なデータを扱うシステムの場合、MDF、IDF、ルータやファイアウォール等のネットワーク機器に関しても不正使用、破壊、盗難等された場合の影響が大きい。このため、ネットワーク機器も、必要に応じてサーバー設置場所に準ずる機器管理を行うことが望ましい。必要である。

(1) サーバーの機器管理については【運 57】参照のこと。
(2) ネットワーク機器の設定情報管理については【運 31、32】参照のこと。

削除: ○
削除: ○
削除: ○
削除: 運　58
削除: 2.
削除: .
3.

運用時の信頼性向上対策
運用時の信頼性向上対策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実106	オペレーションの自動化、簡略化を図ること。

オペレーションの信頼性を向上させるため、オペレーションの自動化、簡略化を図ることが望ましい。

1. 汎用機、サーバーのオペレーション

コンピュータセンター及び本部・営業店等におけるオペレーションの信頼性を向上させるため、ハードウェアやソフトウェアを利用してオペレーションの自動化、簡略化を図ることが望ましい必要である。

オペレーションの自動化、簡略化としては、以下の例がある。

(1) コンピュータセンターにおけるオペレーション

①自動化

システムの起動や業務の開始を自動的に行う機能、ジョブの起動やジョブと記憶装置の対応を自動化する機能等、各種自動運転機能を活用する、またはそれぞれの実情に応じた機能を開発することなどによりセンターオペレーションの自動化を図るものである。

また、運用スケジュールの規模に応じてシステムの電源投入を自動的に行う機器、テープハンドリングを自動的に行う機器を活用することもオペレーションの信頼性、安全性、情報の機密保護を向上させるうえで有効である。

スケジュール化されたジョブグループのジョブシーケンスに従ったジョブの自動起動やタイマーによるジョブの時間起動のほかに自動化としては、以下の例がある。

a.電源投入からシステムの立上げ、オンラインジョブの起動、端末の開局等、業務が開始できるまでの一連処理の自動化

b.平常日、繁忙日、月末日、土曜日等パターンごとにスケジュール化された一斉同報通知の送出や端末モード変更の自動化

c.取引ジャーナル等のファイルのバッチジョブへの引継ぎの自動化

d.取引ジャーナル等のファイルの他システム（系）への引継ぎの自動化

e.端末の閉局からオンラインジョブの停止までの一連の処理の自動化

f.システム停止の自動化

g.テープハンドリングの自動化

なお、自動運用の注意事項として処理の順序や運転状況、条件の変更が生じた際にも、システム全体の運用に支障を来さぬよう、自動化を変更できる機能を充実しておくことが重要であり、変更内容としては、以下の例がある。

削除: ○

削除: 技　16

削除: 重要であり

削除: ような

削除: での

削除: が整備されてきており、これら

削除: も開発されており、これら

削除: 以下のような自動化の

削除: ようなものがある

(a) 一斉同報通知や端末モード変更を行う時刻の変更
(b) システム（系）の変更（現用系から待機系への変更、またはその逆）
(c) 自動運用からマニュアル運用への変更
(d) ジョブネットワークへのジョブの追加、変更
(e) ボリュームの追加、変更
(f) 実行 JCL（ジョブ制御言語）の変更

②簡略化

コマンド体系の一元化を図ったり出力メッセージの日本語化を図るなどして、オペレータインタフェースを平易化する。さらに、運用をケースによりパターン化し、一連のコマンド列を一括実行できるように準備しておくことなどにより、オペレーションを単純化、簡略化する。

オペレーションの単純化、簡略化としては、以下の例がある。

a.コマンド入力の極少化
b.テープハンドリングの極少化
c.異常終了後再開オペレーションのパターン化

③自動化、簡略化の留意点

センターオペレーションの自動化の推進は、オペレーションの信頼性向上のために有効であるが、過度の自動化は、機械運行の安全性を阻害する可能性もある。そのような場合には、単にオペレータへの通報にとどめる等、オペレータによる判断の余地を残しておく。

オペレータの応答を必要とするメッセージやオペレータに注意を喚起する必要があるメッセージ等は、高輝度出力、赤字出力やブザーを鳴らす（オペレータの応答で解除）方法等で重要メッセージの見落としを防ぐ工夫も必要である。さらに、大量メッセージによるシステム停止等を防ぐため、冗長なメッセージを抑止する等の仕組みを合わせて構築する。

(2) 本部・営業店等におけるオペレーション

本部・営業店等における重要なサーバーのオペレーションは、コンピュータセンターでのオペレーションに倣って自動化、簡略化を図ることが~~望ましい。~~必要である。さらに、本部・営業店等でコンピュータ運用に必要な知識や技能を持つ専門のオペレータを配置することが困難な場合には、自動化等の運用をリモート操作で行う機能を持つことが望ましい。

①自動化

本部・営業店等のサーバーオペレーションの自動化としては、以下の例がある。

a.電源の投入やシステムの立上げ、業務アプリケーションの起動
b.バックアップの取得やデータベース更新手順
c.障害発生時の縮退運転の手順やシャットダウン手順

②簡略化

簡略化としては、以下の例がある。

a.オペレーション用のインタフェースを平易化（ユーザーフレンドリなインタフェースの採用）
b.一連のコマンドを一括実行しコマンド入力を極少化

削除: こと
削除: ものであり、以下のような
削除: ことも必要である
削除: ことも必要である
削除: ような
削除: の例として、以下のものがある

c.異常終了時の再開オペレーションの単純化

2. データ入力作業（端末オペレーション）

コンピュータセンター及び本部・営業店等におけるオペレーションの信頼性を向上させるため、ハードウェアやソフトウェアを利用してデータ入力作業（端末オペレーション）の自動化、簡略化を図ることが~~望ましい~~。必要である。

オペレーションの自動化、簡略化としては、以下の例がある。

(1) 自動化

磁気ストライプ読取装置、現金処理機、OCR 等の活用により、手入力操作の一部またはすべてを削減する。

(2) 簡略化

オペレーションガイダンス機能の活用等により、入力判断の平易化やコード入力による簡略化を行う。

削除: を減少させたり、無くしたりするものである

削除: ものである

データ保護
漏洩防止

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 117	相手端末確認機能を設けること。

公衆通信網を通じて自動着信端末に出力する場合には、誤接続を防止するため、確認可能なものについては相手端末を確認する機能を設けること~~が望ましい~~。

1. 公衆通信網を通じて金融機関等から顧客に対して振込入金等の種々の金融情報を、自動着信機能を持ったファクシミリ端末を介して連絡する場合には、暗証番号等による本人確認ができないため電話番号の登録ミス等により誤った相手に出力する可能性がある。
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。~~必要である。

   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【技 35】

2. 公衆通信網を通じてパソコンやコンピュータへ種々の資金移動や金融情報を通知する場合、接続する際に端末 ID や発信者確認コードの確認を行う等の機能を設けることが望ましい。【技 35】

削除: ○
削除: 技　27
削除: テレックス端末や
削除: 2.
削除: の例としては以下のようなものがある
削除: (3) テレックスのアンサーバックの利用 .
削除: 4
削除: 3

データ保護
漏洩防止

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

削除: ○

実 118	蓄積データの漏洩防止策を講ずること。

削除:　技　28

ファイルのコピーや盗難等による漏洩を防止するため、重要なデータについては~~暗号化等の~~データ保護の対策を講ずること~~が望ましい~~。

1. ファイルの不正コピーや盗難の際にも、データの内容がわからないようにするため、重要なデータについては暗号化することが望ましい。特に個人データを蓄積する場合には、暗号化・パスワード設定等ファイルの不正コピーや盗難の際にもデータの内容がわからないようにするための対策を講ずることが必要である。また、電子的取引において蓄積されるデータについても暗号化・パスワード設定等の対策を講ずることが必要である。

パスワード設定の内容としては、以下の例がある。

削除: の例としては、以下のようなもの

(1) データベース　：DBMS の備えるパスワード【技 31】
(2) 文書ファイル　：文書そのものにかけるパスワード
(3) ハードディスク：ハードディスクドライブにかけるパスワード。パスワードが知られない限り他の機器に接続しても読み取り不可能となる。

2. 外部持ち出しや他の媒体へのコピーが物理的に不可能なコンピュータ機器内の個人データの漏洩防止策としては、上記対策の他、本人確認機能を設けることにより、許可された者以外の者が当該データを判別できないようにする仕組みも有効である。（本人確認機能については【技 35】参照。）

削除: なお、

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、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。

削除: 2

また、新規にシステムを構築する、あるいはシステムを更新する際には、技術の進歩により暗号は脆弱になることや暗号技術も日々進化していることを踏まえ、「電子政府における調

達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」等に記載されている、安全性が継続的に検証されている暗号方式を採用することが望ましい。

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. 涉外端末の盗難・紛失時に備えた対策として、涉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

(3) CD・ATM 等を含む端末機器内部のデータに対するアクセス権限の制限【運 16】

（参考 1）
暗号化の方式としては、例えば以下のようなものがある。
(1) 共通鍵暗号方式
暗号化する時に使用した鍵と同じ鍵で復号する方式。
(2) 公開鍵暗号方式
ペアになった 2 つの鍵でデータを暗号化、復号する方式で、どちらか一方の鍵を公開する。

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

削除: 3

削除: 4

削除: 5.

削除: ようなもの

削除: なお、一時的な使用制限の解除が認められる場合には、使用制限の再設定手続きと定期的な制限の確認が必要である。

削除: ことから、

削除: ようなものがある

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。

データ保護
漏洩防止

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

削除: ○

実 119	伝送データの漏洩防止策を講ずること。

削除: 技　29

データ伝送時の盗聴等による漏洩を防止するため、重要なデータについては~~暗号化の~~データ保護の対策を講ずること~~が望ましい~~。

1. データ伝送時に盗聴された場合にもデータの内容がわからないようにするため、重要なデータについては、暗号化することが望ましい。特に個人データを伝送する場合には、暗号化・パスワード設定等データ伝送時に盗聴された場合にもデータの内容がわからないようにするための対策を講ずることが必要である。

   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

削除: また、

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。なお、構内 LAN においては、ネットワーク構成機器への未承認機器の論理的・物理的な接続を不可能とする仕組みも有効である。

（参考 1）
無線 LAN を使用する際には、以下のような点を考慮する必要がある。
(1) 従来の無線 LAN 機器で使用されている、WEP (Wireless Equivalent Privacy) の RC4 という暗号化方式は、脆弱性を回避する手段がないことから、業務システムにおいては使用しない。
(2) 平成 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。
・「無線 LAN セキュリティ要件の検討」
http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/dai65/65lan_kentou.pdf
首相官邸各府省情報化統括責任者（CIO）補佐官等連絡会議
・「WPA の脆弱性の報告に関する分析（技術編）」
http://www.rcis.aist.go.jp/TR/2009-01/wpa-compromise.html
独立行政法人産業技術総合研究所 情報セキュリティ研究センター
・「一般利用者が安心して無線 LAN を利用するために」
http://www.soumu.go.jp/main_content/000183224.pdf
総務省

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や暗号技術も日々進化していることを踏まえ、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」等に記載されている、安全性が継続的に検証されている暗号方式を採用することが望ましい。

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

削除: 24
削除: 10
削除: 2
削除: 3.
削除: の例として、以下のようなものがある

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 2）

1. インターネットバンキング等における暗号技術は SSL（Secure Socket Layer）プロトコルが一般的になっている。SSL の暗号鍵は、数種類の鍵長が選択可能であるが、安全性を考慮すると 128 ビット以上の鍵長を使用することが望ましい。

2. SSL の暗号技術の適切な利用方法については、CRYPTREC 公開の「電子政府推奨暗号の利用方法に関するガイドブック」に記載がある。
（参照 URL）
http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf

3. Web アプリケーションの設計及び実装において、SSL を適切に使用し、重要な情報を漏れなく暗号化することが必要である。
例として以下のようなものがある。
(1) ID・パスワードや個人情報等の情報を入力させる際には、SSL を使用した画面（「https://」で始まる画面）とすること。
(2) 複数フレームを使用する際には、利用者が Web ブラウザのアドレスバーで、表示中のページが SSL で保護されていることを確認できる画面構成とすること。
(3) セッション ID 等ユーザーを特定するようなデータは常に SSL 通信を使用し、特にデータを cookie に格納する場合には、「secure」属性を付与するなどの実装を行うこと。

4. 参考文献として、以下のものがある。
(1) 「安全なウェブサイトの作り方 改訂第 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

削除: 5

（参考 3）

1. 技術の進歩により暗号の脆弱性が増す事例には、以下のものがある。

(1) コンピュータの処理能力の向上により、解読に要する時間が現実的な時間に収まる。

(2) 暗号アルゴリズムの脆弱性が発見される。

（注）内閣サイバーセキュリティセンター（NISC : National center of Incident readiness and Strategy for Cybersecurity）において、政府機関における SHA-1 及び RSA1024 の移行についての指針等を打ち出している事例がある。

（検討状況の参照 URL）

http://www.nisc.go.jp/conference/seisaku/dai20/pdf/20siryou0502.pdf

（指針の参照 URL）

http://www.nisc.go.jp/conference/seisaku/dai17/pdf/17siryou0101.pdf

2. 総務省と経済産業省が中心となって選定した「電子政府推奨暗号リスト」は平成 15 年 2 月に発刊されている。

また、平成 25 年 3 月には「電子政府推奨暗号リスト」を改定した「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」が策定されている。

（CRYPTREC：URL）

http://www.cryptrec.go.jp/

3. 「電子政府推奨暗号」の利用方法に関しては、CRYPTREC から「電子政府推奨暗号の利用方法に関するガイドブック」が平成 20 年 7 月に公開されている。

（参照 URL）

http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf

（注）CRYPTREC とは Cryptography Research and Evaluation Committees の略で、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。総務省及び経済産業省が共同で運営する暗号技術検討会と、独立行政法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で運営する暗号方式委員会、暗号実装委員会及び暗号運用委員会で構成されている。

データ保護
検知策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 123	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じておくことが望ましい。

1. データ伝送において、重要なデータについては、改ざん検知のための対策を講じておくことが望ましい。特にオープンネットワークを介してデータを伝送する場合は、伝送途中におけるデータ改ざんを検知するための対策が講じられている必要がある。

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

削除: ○

削除: 技　33

削除: は

削除: 2.

削除: 例えば以下のようなものがある

不正使用防止
予防策（不正・偽造防止対策）

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎	◎		

実 131	カードの偽造防止対策のための技術的措置を講ずること。

不正使用防止のため、カードの偽造防止の技術的措置を講ずることが~~望ましい~~。

1. カード犯罪を防止し、カードを利用したサービスを安全に提供するため、カードの偽造防止のための技術的措置を講ずることが~~望ましい。~~必要である。

カードの偽造防止対策としては、以下の例がある。

(1) IC カード化

(2) 磁気ストライプに偽造を判別するコードを記録する。

なお、当該コードは、容易に推察されない仕組みとする。

利用者の利便性を考慮して IC と磁気ストライプを併用したカードを導入する場合、IC 単独のカードに比べ安全性が低いことに十分留意する。例えば、IC を使用した場合と磁気ストライプを使用した場合とで、利用できる取引の種類や金額を区別することが考えられる。

(3) カードへ有効期限を設定し、期限経過時に更新

(4) 顔写真、ホログラム等の券面への印刷

2. キャッシュカードの IC カード化に当たっては、「全銀協 IC キャッシュカード標準仕様」に要求される要件を満たすこと（セキュリティや互換性など）が必要である。また、IC カードの運用面や技術面について、セキュリティ対策上注意し、定期的に見直すことにより時々の技術水準を反映することが必要である。

IC カードの運用面や技術面について、セキュリティ対策上注意すべき事項としては、以下の例がある。

(1) IC カードの有効期限（電子証明書の有効期限）

(2) 電子証明書の認証機関の信頼性（運用規定等）

(3) 使用される暗号の強度

(4) 耐タンパー性

削除: ○
削除: ○
削除: ○
削除:　技　40
削除: のため
削除: 2.
削除: 等の高セキュリティ技術の導入がある。
削除: 磁気ストライプ付きキャッシュカードの偽造防止対策としては、偽造を判別するためのコードを磁気ストライプに記録することが必要である。
削除: ことが望ましい
削除: 必要がある
削除: また、その他のカードの偽造防止対策としては、以下のようなものがある。
削除: 3
削除: 、以下のような点に

不正使用防止
予防策（不正・偽造防止対策）

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 132	電子的価値の保護機能、または不正検知の仕組みを設けること。

電子的価値のコピー、二重使用等の不正行為に対処するため、データの保護機能を具備するか、あるいはその発生を検知できる仕組みを構築しておくことが望ましい。

1. 電子的価値を蓄積する機器、媒体あるいはそれに含まれるソフトウェアには、価値を保護する機能を具備することが~~望ましい。~~必要である。

2. 上記の機能がない場合には、改ざん、不正コピーによる二重使用等の不正行為を検出できる仕組みを用意することが望ましい。

3. セキュリティ確保のためには、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 カード型電子マネーでの耐タンパー性を向上させる保護機能
(2) IC カード等には有効期限を設定するなどの偽造抑止対策
(3) シリアルナンバー方式による不正検知
(4) 証拠センター方式による不正検知

（注）・耐タンパー性　：ソフトウェアやハードウェアの内部構造や記憶しているデータなどの解析の困難な状態。
・シリアルナンバー方式：電子的価値の使用単位ごとに固有の識別番号を付与し、同一番号のものが二重に使用されないようにチェックする方式。
・証拠センター方式　：付与された電子的価値の総額に対して、実際の使用額と残額とを突合して不正使用をチェックする方式。証拠センターにおいて使用額と残額とが突合されるため、事後的なチェックとなる。

削除: ○
削除: 技　41
削除: 以下のような
削除: のような
削除: こじ開けや不正アクセスなどで情報を無理に取り出そうとした場合に、その情報を消去する等で不正を防止する技術

不正使用防止
予防策（不正・偽造防止対策）

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 134	電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること。

業務目的以外の電子メールの送受信やホームページの閲覧等に対処するため、不正使用防止対策を講ずることが望ましい。

1. 業務目的以外の電子メールの送受信やホームページの閲覧等に対処するため、セキュリティポリシーと整合性がある不正使用防止対策を講ずることが望ましい。なお、個人データを扱う場合には、この措置は必要である。

業務目的以外の電子メールの送受信やホームページの閲覧等としては、以下の例がある。

(1) 電子メールの送受信
　①業務に関係しない私的な情報の交換・連絡
　②業務上適切な範囲を逸脱した電子メールの利用（不適切なメーリングリストやメールマガジンの利用等）
　③公序良俗に反する情報の送信

(2) ホームページの閲覧
　①業務に関係しないホームページの閲覧
　②ホームページへの業務上適切な範囲を逸脱したコメントの掲載（掲示板等への公序良俗に反するコメント掲載等）

また、業務目的以外の電子メールの送受信やホームページの閲覧等の不正使用防止対策としては、以下の例がある。

(1) 電子メールの送受信やホームページの閲覧が可能な利用者を適切な範囲に限定する。【運 16】

(2) メールフィルタリング等を導入し、電子メールの内容を判断し、不適切な情報の送受信を防止する。また、不適切な電子メールを送受信した利用者に対して適切な措置を行う。

(3) 社外に送信された電子メールを自動的に送信者の管理者等に転送する。

(4) コンテンツフィルタリング等を導入し、ホームページのコンテンツの内容を判断し、不適切な情報の閲覧を防止する。また、不適切なホームページを閲覧した利用者に対して適切な措置を行う。

2. 運用面においても、全役職員（外部要員を含む）に対するセキュリティ教育を行い、責任と義務及び懲罰等について周知徹底を図ることが必要である。【運 80】

削除: ○
削除:　技　42-1
削除: 2.
削除: ようなもの
削除: 3.
削除: ようなもの
削除: 4
削除: なお、

（参考）
メールフィルタリング：電子メールの内容を判断し、不適切な情報の送受信を防ぐ目的で利用されるソフトウェアであり、利用者が受信したくないメールアドレスを設定しスパムメールの着信を拒否できる機能も含めることがある。
コンテンツフィルタリング：ホームページのコンテンツの内容を判断し、不適切な情報の閲覧を防ぐ目的で利用されるソフトウェアであり、不適切なホームページを閲覧した利用者のアクセスログを取得する機能も含めることがある。

オープンネットワークを利用した金融サービス
インターネット、モバイル

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
				◎	

実86	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。

利用者が適切に取引機関や金融サービスの選択を行うため、安全対策に関する情報を開示することが望ましい。

1. 利用者が適切に取引機関や金融サービスの選択を行えるよう、金融機関等はセキュリティ方針等を開示することが望ましい。

開示内容としては、以下の例がある。

(1) 情報漏洩防止のために暗号化していること。
(2) なりすまし防止のために認証（パスワード、電子認証）を行っていること。
(3) 顧客に関する厳密な守秘義務に基づき、顧客データを保護していること。

また、開示方法としては、以下の例がある。

(1) DM への記載
(2) 店頭や自動機器コーナーのポスターへの記載
(3) 金融機関等ホームページへの記載
(4) 新聞広告等
(5) 電子メール

2. 開示にあたっては図等を使用し、利用者に理解しやすいように工夫することが望ましい。

3. 利用者からの問合せ及び苦情に対応することが望ましい。

(1) 相談窓口の設置
(2) パンフレット、ホームページ等に連絡先を明記

利用者への安全対策に関する情報開示を実施するにあたっては、当センター発刊の「安全対策に関する情報開示研究会報告書」等を参照のこと。

削除: ○
削除: 運　105
削除: 2.
削除: ようなもの
削除: 3.
削除: ようなもの
削除: 4
削除: 5
削除: 6.

ハードウェアの信頼性向上対策
ハードウェアの予備

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎	◎			

実 96	回線の予備を設けること。

回線障害時の迅速な対応のため、重要な回線は予備を設けることが望ましい。

1. 回線障害時の迅速な対応のため、重要な回線は予備を設けることが望ましい。
また、回線の予備については、以下の点を考慮することが望ましい。
(1) 地点間（構外）の重要な回線は複数化するか、またはバックアップ回線を確保しておくことが望ましい。なお、回線を複数化する際は、物理的別ルート化（別の収容交換設備等（旧電話局）を経由するもの）を図ることが望ましい。また、回線のルートや回線容量等は、通信事業者に該当の回線の利用目的等を明示し、適切な設計・構築を図ることが望ましい。
(2) 構内回線についても、コンピュータセンター内の構内配線や、重要な部門 LAN については予備を設けることが望ましい。

2. 地点間（構外）の回線について
(1) 予備の具体的な内容としては、以下の例がある。
①専用回線の複数化の例
a. 端末系装置を 2 つのグループに分け、それぞれ別々の回線に接続する方法
b. 回線の一方を予備とし、必要に応じて切り替える方法
②電話回線（xDSL を含む）、 ISDN 回線、回線交換回線、パケット交換回線、ATM 回線、衛星通信回線、光ファイバー通信網等を利用したバックアップ回線の確保（図 1）。

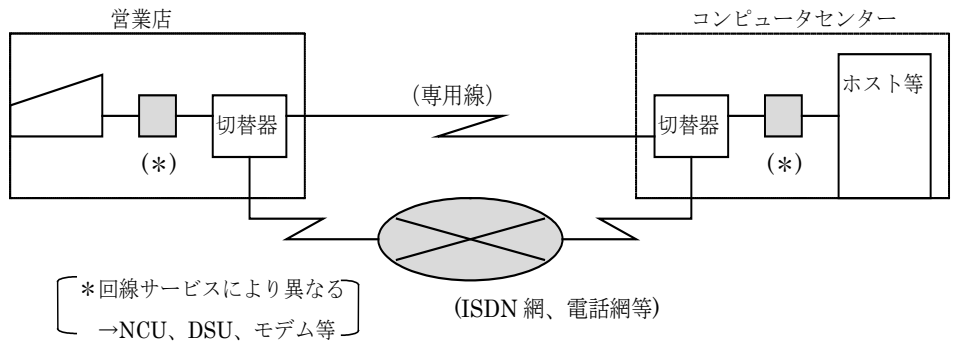


図 1　バックアップ回線の例

(2) 回線の別ルート化
回線ルートに障害が発生した場合に、全回線が同時に使用できなくなる事態を防ぐため、

削除: ○
削除: ○
削除: 技 5
削除: に
削除: 事例として、以下のようなものがある
削除: 、フレームリレー回線

複数の回線により別々に接続し、並行して危険分散を図るための方法である。
単一の通信事業者を利用し、中継局を分ける（物理的に別ルートにする）方法と、複数の通信事業者を利用する方法がある（図 2、図 3）。
①単一の通信事業者の利用

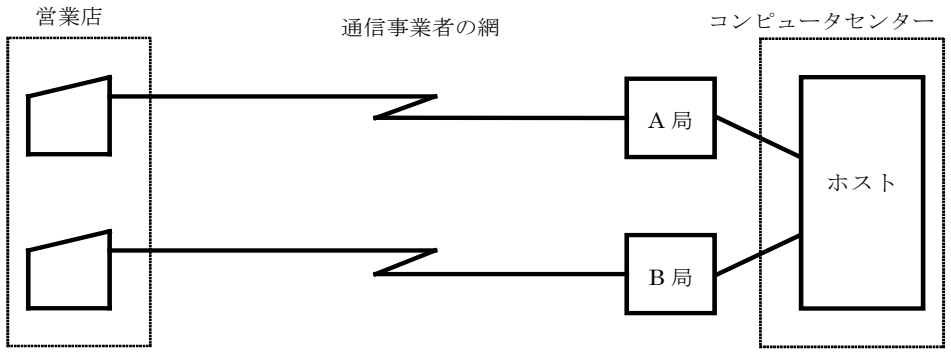


図 2　単一の通信事業者の利用例

②複数の通信事業者の利用

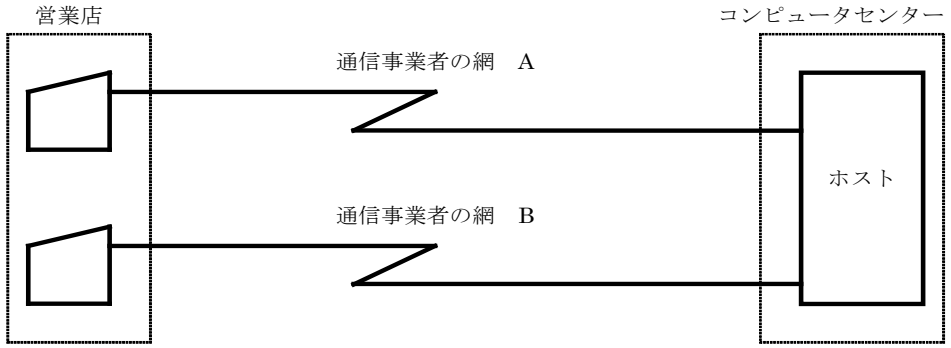


図 3　複数の通信事業者の利用例

(3) データ伝送経路の構成と留意点
代表的なデータ伝送経路の構成には、スター型構成（コンピュータセンター等の主要拠点と営業店等の拠点を 1 対 1 で接続する構成）や、ツリー型構成（コンピュータセンター等の主要拠点より事務センターや基幹営業店等の中継結節点を経由し、複数の営業店等の拠点を接続する構成）等がある。構成によって、障害時の影響範囲、通信量及びコスト等について留意する必要があり、選択にあたっては、各種構成の特徴を踏まえ、業務への影響等を勘案することが必要である（図 4、図 5）。

書式変更: インデント : 左　4 字

①スター型の構成

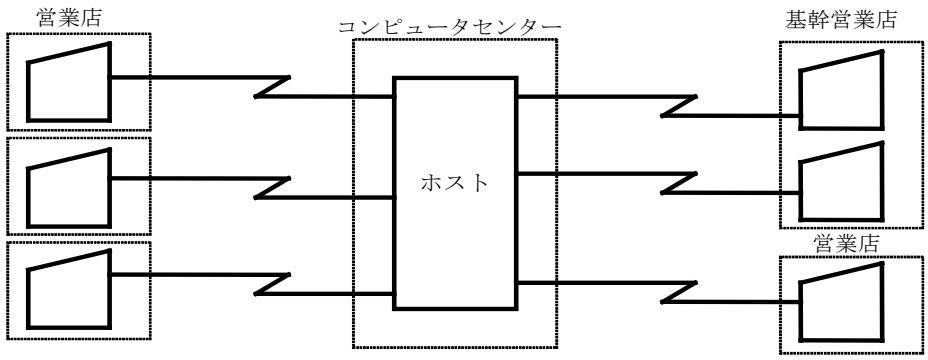


図４　スター型の構成の例

②ツリー型の構成

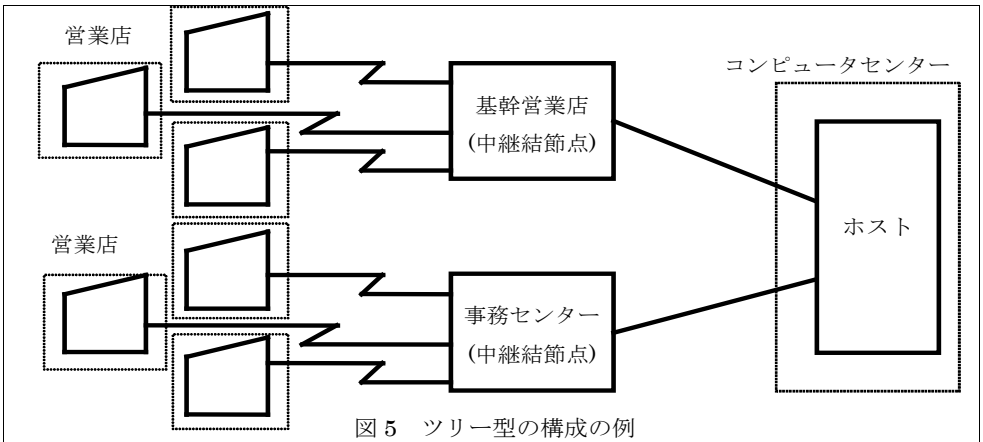


図５　ツリー型の構成の例

3.　構内回線について

(1) コンピュータセンターにおける留意点

コンピュータセンターにおいては、回線関連設備から重要な各機器までの配線は二重化することが望ましい。特に、建物外の回線を二重化した場合、コンピュータセンター内において、MDF から通信制御装置等の重要な各機器までの配線を二重化することが望ましい。

(2) 構内 LAN の予備

構内 LAN についても、重要性に応じて予備を持つことが望ましい。構内 LAN の予備としては、以下の例がある（図 6）。

削除: の例として、以下のようなものがある

①基幹 LAN の多重化（図 6）

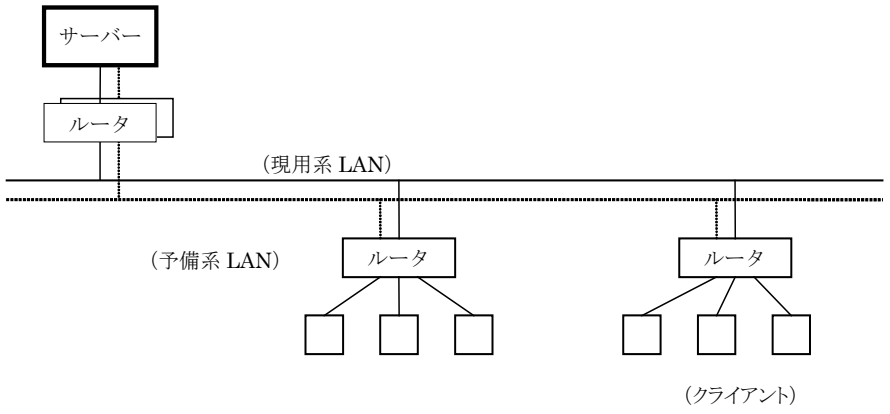


図 6　LAN の多重化の例

4. システムの目的や重要性に応じ、必要な予備（能力の余裕）を確保できるようにシステムを構築することが望ましい。
特に、24 時間稼働システム等の長時間連続稼働システムにおいては、当該システムの機能及び制約に応じた予備（能力の余裕）を設けることが望ましい。
なお、コンピュータシステムは本体装置のほか、周辺装置・通信系装置・回線・端末系装置等から構成されるため、障害が発生した場合に、それらの予備を含めたシステム全体が有効に機能することを確認しておく必要がある。

削除: 【技 2】3. を参照。

災害時対策
バックアップサイト

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎				

実 115	バックアップサイトを保有すること。

コンピュータセンター等が災害等により機能しなくなった場合に備えるため、業務の優先度を考慮したバックアップサイトを保有することが望ましい。

1. コンピュータセンター等が災害等により機能しなくなった場合に備えて、リスク分散の意味で、別の地域にバックアップサイトを保有することが望ましい。
   特に、資金決済等を行う重要なシステムについては、原則としてバックアップサイトを保有することが必要である。
   ただし、バックアップサイトを保有しない場合は、障害による社会への影響を十分に検討のうえ、他に代替する方法による業務継続態勢を整備し、経営層が承認する必要がある。

   バックアップサイトの運営形態としては、以下のものがある。
   (1) 自営センター
   　自社専用の代替施設として利用する。
   (2) 共同利用センター
   　複数企業が共同で代替センターを設立し、必要時に利用する。
   (3) 相互利用センター
   　別地域にある同一企業（グループ）内の事業部門と相互に被災時等にバックアップし合う。代替施設提供部門は、被災時等には緊急度の低い業務は一時運用を止めて対応する。
   　他企業（協力企業）間でバックアップし合う場合もある。
   (4) 代行処理センター
   　第三者にバックアップを委託し、必要時に利用する。

2. バックアップサイトを外部に委託している場合、複数の委託元で同時に緊急事態が発生するケースを想定して、バックアップを受ける優先順位、最低保証の範囲などのサービスを確認し、事務量の変化に対応して定期的に見直すことが必要である。

3. バックアップサイトの保有にあたっては、以下の事項を考慮し、総合的に判断することが望ましい。
   (1) コンピュータセンターと同一のリスク要因（火災、地震、停電等）を共有しないこと。
   (2) 被災時の要員、データ、物資等の移動・移送時間を含む復旧時間を確認しておくこと。

（参考）
バックアップサイトの立地条件については、コンピュータセンターの立地条件と同様に考える必要があるため【設 1】を参照のこと。

削除: ○
削除: 技　25
削除: て
削除: して

【資料２－１】
平成 29 年 9 月 12 日
公益財団法人 金融情報システムセンター

外部委託管理関連基準の改訂について

I. 改訂原案作成のポイント

○ 前回ご説明した考え方に基づき、各委員に訪問のうえ、現在の基準との差異を中心に改訂原案作成のポイントをご説明させて頂きました。（頂いたご意見については、資料「外部委託管理関連基準の事前意見まとめ」を参照）

○ 改訂原案作成の主なポイントについて整理し、改訂原案検証の補助資料としてご確認頂きたい。（資料「外部委託管理関連基準　改訂原案作成の主なポイント」参照）

II. 改訂方針に関する論点

改訂に関する共通の項目として、以下の論点についてご議論いただきたい。

論点１	クラウド基準新設時に記載された、「クラウドサービス利用における考慮点」等について、現時点では不要となった箇所については、新基準に記載しない（削除する）ことでよいか。

○クラウド事業者に対し「情報開示に消極的である」（運 108）など、基準新設当時において懸念されていた事項のうち、現在は解消されたもの等については、新基準には記載しない。

○例示部分について、「必要に応じて」や「通常システムでは」といった表現が使用されているが、リスクベースアプローチの考え方を徹底するのであれば、こうした表現は不要であると考えられるため、原則として削除し、「読みやすく」する。

論点２	クラウド固有の安全対策として新設した【統 27】において、システムの重要度に関する表現（例えば、「特定システムでクラウドサービスを利用する場合には」といった表現）を記載しない（削除する）ことでよいか。 また、統制基準ではなく、実務基準として整理することが適切と考えられるがどうか。

○FinTech 有識者検討会では「クラウド固有のリスク管理策」は、「重要な情報システム」（安対改訂案では「特定システム」）についてクラウドを利用する場合を対象に策定されている。また、個別の業務・サービスを対象とする基準に該当するため、この基準は「付加基準」として位置付けられる。

○こうしたことから、クラウド固有の安全対策を基準化するにあたっては、システムの重要度に関する記載は不要であるため、これを削除する。

○なお、この基準については、統制基準というよりは、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がどうか。

論点３	実務基準との重複部分や、記載箇所が複数の基準に分散している内容を統合・整理することでよいか。

○クラウド基準には、情報漏洩に関する基準として【運 110】【運 111】がある。これらは、クラウド基準が策定された際に、それ単独で利用することができるように他の基準（【実 118】【実 119】）を織り込みながら策定された経緯がある。従って、今回の改訂作業では、他の基準と内容が重複するものを削除する必要がある。

○同様に、監査に関する記載については、【統 22】（契約締結時に監査権を契約書に明記）、【統 27】（クラウド事業者に対する監査）、【監 1】（監査の実施等）と記載箇所が複数に跨ることから、利便性を考慮して記載箇所を整理していくべきか。

III. 改訂原案について

改訂原案については、【資料２－２】として本日配布している。資料は以下の構成としており、修正箇所は原案本文中にコメント及び修正履歴として表示した。改訂内容を検証するうえで、参照いただきたい。

基準 No	頁	内容
【運 108】【運 109】	1	クラウド基準（現基準）
【統 21】	11	外部委託利用検討時（新基準）
【統 22】	14	契約締結時（新基準）
【統 23】～【統 26】	19	その他外部委託管理基準
【統 27】～【統 29】	26	クラウド基準、共同センターほか
【監 1】	30	システム監査体制
【実 58】	33	コンティンジェンシープランの策定

IV. 今後の予定

本日ご説明した内容について、9/22（金）までに事後意見をいただきたい。事後意見をもとに基準原案の修正を行い、次回委員会にて修正原案を提示する予定である。

（第 55 回安全対策専門委員会資料より再掲・一部加筆修正）

日程（予定）	内容
9 月 12 日（火）	第 56 回安全対策専門委員会審議（本日原案提示）
9 月 22 日（金）	第 56 回専門委員会事後意見の締切
10 月 17 日（火）	第 57 回安全対策専門委員会審議（修正原案提示）

以上

【別紙1】外部委託管理関連基準の事前意見まとめ

1．外部委託管理基準とクラウド基準の統合・整理

基準	概要	No	主なご意見	対応方針
全般	―	1	統合の考え方については問題ないと考える	―
		2	監査に関する対策は複数個所に記載されているため、利便性を考慮した方がよい	【統22】、【統27】および【監1】の監査に関する記載を統合・整理したいと考えます。（論点３）
		3	時代の変化を捉え、見直すべき部分があれば今回修正を加えた方がよいのでは	委員からのご意見を踏まえ、必要な箇所があれば対応したいと考えます。
【統21】 【統22】	利用検討時 契約締結時	4	クラウド基準新設時の考慮点のうち、基準として不要と判断できる部分を削除するという方針は問題なし	削除した原案を提示し、委員の皆様にご確認いただこうと考えています。（論点１）
		5	利用形態に応じて委託先との責任分界点を考慮する考え方を記載した方がよい（例IaaS、PaaSなど）	責任分界点に関する考慮は監査指針にも記載があり、ご意見を踏まえ明記するようにします。
		6	例示の中で重みづけ等の表現は極力排除した方がよく、「十分な」や「重要な」といった表現は例示の中である以上、排除しても問題ないと考える	No4とも関連しますが、各委員からは「過去の知見を継承すべきでは？」との意見もあり、改訂原案をご提示し、より適切な内容となるよう、ご検討いただこうと考えています。（論点１）
		7	「必要に応じて」という表現は、例示であれば不要では？	
【統23】 【統24】	要員へのルール徹底 委託先組織の整備	8	クラウドサービスの利用に当てはまらない内容だと思われるが、そもそも契約書に含まれない内容であれば、基準も選択されないと思われるので、「委託する業務内容に応じて…」とした条件文は不要では？	「原則として適用」の考え方に基づくと、この条件文は不要とも言えますが、各委員からのご意見を踏まえ、最終的に表現を残すべきか検討したいと思います。
		9		
【統25】	情報漏洩防止	10	情報漏洩防止について、別の基準（【実118】【実119】）では「暗号化等の対策を講ずることが望ましい」となっているが、ここでは「講ずること」となっており矛盾するのでは？	実務基準との冗長化を排し、基準間のギャップをなくすことが必要だと考えます。このため、統25自体を廃止し、残すべき要素については、【統22】へ移動させることを考えています。（論点３）
		11	暗号化を含む漏洩防止策は、別の基準に記載されていることもあり、かつ委託先の評価や契約締結時に明らかにすべき内容であり、基準自体の位置付けを見直すべきでは？	No10と同じく、【統22】に統合することを検討したいと考えています。（論点３）
【統26】	契約終了時	12	情報漏洩防止は【実118】【実119】の他、実務基準にある内容と重複することになるのでは？	No10と同じく、【統26】についても統合（または廃止）を検討したいと考えています。（論点３）
		13	物理的消去と論理的消去に差を付ける必要はないと思われる	記述を簡素化し、両者に差のある記述を排除したいと思います。（廃止の場合は別途検討）
		14	消去証明書は必須と考えているため、「望ましい」という表現は変えた方がよい	消去証明かそれに代替するものが必要として記述を見直したいと思います。（同上）
【統27】	クラウド固有の管理策	15	特定システムに限定した内容ではないと思われるため、通常システムでも適用すべき内容について、対策の漏れが生じないように記載を工夫した方がよい	委員からのご意見を踏まえ、通常システムでも適用すべき内容について記載を見直すべきか検討します。（論点２）
		16	クラウド基準は個別の業務・サービスとなるため、実務基準とすべきでは？	ご意見を踏まえ、クラウド基準を実務基準（付加基準）として整理したいと考えています。（論点２）
		17	第三者監査や外部の監査報告書で代替可能である旨が欠落している	報告書の内容を踏まえ、記載を一部修正しています。

2．その他の基準の統合・整理

基準	概要	No	主なご意見	対応方針
【統28】	共同センター	18	共同センターの示す範囲を明確にした方がよい	小項目および適用の考え方に「勘定系システム等で共同センターを利用する場合」と記載しようと思います。
		19	協同利用型クラウドはここに含まれるのか	含まれないため、No17に沿って適用範囲を限定するよう、記載を見直したいと思います。
【統29】	金融機関相互のシステム・ネットワーク	20	誰が実施する管理策なのか、主語を明確にした方がよい	安全管理策を講ずるのはあくまで金融機関であり、主語を明確にしたいと考えています。
【監1】	監査	21	SOC2に関する記載については、報告書の内容を反映してもらいたい	外部委託報告書の内容が反映されているか改めて確認したいと思います。
		22	監査に関する記載が複数に渡り、使いづらさに繋がらないか	No2と併せて整理したいと思います。（論点３）
【実58】	コンティンジェンシープランの策定	23	特になし	

【別紙2】外部委託管理関連基準　改訂原案作成の主なポイント

1. 全般

・「クラウドサービスの利用」については、全て「外部委託」に表現を統一。（外部委託にクラウドサービス利用が含まれることは、基準の中扉（カテゴリ単位に挿入する説明文）に記載する予定）
・例示の中で示されている条件や、システムの重要度等の判断根拠を簡素化または省略。

2. 各個別基準

フェーズ	旧基準	旧区分	基準の内容（概要）	改訂要領	新基準	主な修正点	考慮すべき事項
利用検討時	【運87】	外部委託	外部委託する目的・範囲を明確にすること	統合による廃止			・これまで外部委託基準を利用していた場合に、例示される項目数が増加（選択肢が増加）する
	【運87-1】		外部委託先を評価すること	統合による廃止			
	【運108】	クラウド	外部委託する目的・範囲を明確にするとともに、外部委託先を評価すること	見直し	【統21】	・クラウド事業者に対する固有の考慮事項の削除	・過去に検討された考慮事項を削除することにより知見やノウハウが喪失する懸念
						・クラウド固有の管理策（データ所在の把握）の削除	
						・例示部分の表現簡素化・統一（「必要である」、「可能である」の削除）	・過去に検討された考慮事項を削除することにより知見やノウハウが喪失する懸念
契約締結時	【運88】	外部委託	契約時に明確にすべき事項を検討すること	統合による廃止			・これまで外部委託基準を利用していた場合に、例示される項目数が増加（選択肢が増加）する
	【運109】	クラウド	契約時に明確にすべき事項を検討すること	見直し	【統22】	・クラウド事業者に対する固有の考慮事項の削除	・過去に検討された考慮事項を削除することにより知見やノウハウが喪失する懸念
						・例示部分の表現簡素化・統一（「必要である」、「可能である」の削除）	・過去に検討された考慮事項を削除することにより知見やノウハウが喪失する懸念
運用・モニタリング	【運89】	外部委託	委託先の要員がルール等を遵守しているかを確認すること	見直し	【統23】	・委託する業務や内容によって選択できるよう、条件を追記する	・リスクベースアプローチで考えた場合、条件文は不要か？
	【運90】	外部委託	外部委託にあたって、安全管理に関する体制が整備され、機能しているか確認すること	見直し	【統24】		
	【運110】	クラウド	外部委託先のデータ漏洩防止策が講じられていること（暗号化含む）	見直し or 廃止	【統25】	・実務基準と内容が重複するため、冗長化を排し、記載を極小化する	・契約締結時の考慮事項とも考えられるため、基準自体を廃止し、内容を移動させた方がよいか？
契約終了時	【運111】	クラウド	契約終了時のデータ漏洩防止策を講ずること	見直し or 廃止	【統26】	・実務基準と内容が重複するため、冗長化を排し、記載を極小化する	・基準の廃止も考えられるが、終了時の基準が存在しないこととなり、バランスとしてよいか？
―	なし	―	クラウドサービスを利用する場合の安全管理策を講ずること	新設	【統27】	・クラウド固有の管理策を記載する	・システムの重要度に関する記載は不要か？（FinTech報告書では、「重要な情報システム」という条件が付けられているが）

クラウドサービスの利用

適　用　区　分				
共	セ	本	提	ダ
◎				

運　108	クラウドサービスの利用を行う場合は、事前に利用目的や範囲等を明確にするとともに、事業者選定の手続きを明確にすること。

クラウドサービスの利用を行う場合は、事前に目的や範囲等を明確にするとともに、クラウド事業者の選定に際しては手続きを明確にし、事業者を客観的に評価すること。
また、事業者の決定にあたっては、責任者の承認を得ること。

1. クラウド事業者を選定するにあたっては、事前に目的や範囲等を明確にしたうえで、選定手続きを明確にすることが必要である。

2. 明確にすべきクラウドサービスの利用に関する事項としては以下の例がある。
(1) 利用目的
(2) 利用業務範囲
(3) 利用形式
(4) 利用期間
(5) 利用費用
(6) リスクの管理方法
(7) クラウド事業者の選定条件
(8) クラウドサービスに関する自社窓口と役割 等

3. クラウド事業者を客観的に評価すること。
クラウドサービスを利用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、その実現が可能なクラウド事業者を選定すること。その際、クラウド事業者の資質・業務遂行能力に関する情報や、クラウド事業者の内部統制や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（注）。評価にあたっては、クラウド事業者によって契約前の情報開示に消極的なケースもあるが、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。
（注）資源共有型であるパブリッククラウドの場合、クラウド事業者によっては、標準的な契約・SLA 等の内容に関し個社からの変更要求に応じないことも想定されるため、各金融機関が特に重要であると判断した事項については、こうした変更要求の交渉が可能であるかを事前に確認しておくことが必要である。
ただし、金融機関等において業務の特性を十分検討した上で、委託する業務の重要度が高くないと判断し得る場合は、クラウド事業者の公開情報や、業界における評判や実績等による客観的な評

コメント [A1]: 外部委託に関する基準の通則化のため、クラウドに関する記載を外部委託に変更
以下、同様

コメント [A2]: 外部委託に関する基準の通則化のため、「利用」の表現を「委託」に変更

コメント [A3]: 「読みやすさ」の修正に伴い、「必要である」に変更。

コメント [A4]: 外部委託に関する有識者検討会報告書の提言に従い、「再委託先」を含む記載に変更

コメント [A5]: 通則化に伴い、記載内容を変更。「外部委託先の情報開示における条件等を考慮し」

コメント [A6]: 前説 p25
２．統制
(2) 外部の統制
③ 基本形（２者間構成）における各論
c. クラウドサービス
に記載の内容のため、削除

価を行うことも可能である。

評価する事項としては、以下のような例がある。

(1) クラウド利用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、他プロジェクトやサービスでの評判等）
　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（クラウド事業者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（再委託先管理も含む）、外部監査の受検や各種公的認証の取得状況、組織体制（コンプライアンス体制を含む）
(5) 情報開示姿勢
(6) 立入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) データの所在（データが保管される場所、または保管の可能性がある場所）
(8) 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
(9) 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）、日本語での対応）
(10) 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）とクラウド事業者側が提示する損害賠償・補償上限額とのバランス
(11) サービス利用廃止時の対応（ベンダーロックインリスク対応、データ消去等）
　ただし、契約の中断・終了に伴うシステム移行作業（移行データの抽出方法と実際の移行作業内容）については、サービス利用前に把握することが望ましい。
(12) 個人データの取扱いの全部または一部を事業者に行わせることを内容とする契約を締結する場合は、「金融分野における個人情報保護に関するガイドライン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」に準拠対応可能か
(13) 委託費と支払い条件

なお、(5)情報開示姿勢の中でも、リスク管理に直結する事項（注）については、十分に把握しておくことが必要である。このため、こうした情報の開示が必ずしも十分でないクラウド事業者と契約してよいか、慎重な判断が必要である。

（注） リスク管理に直結する事項には以下のようなものがある。
　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 等

4. 紛争が生じた際にどの国の法律が適用されるのか、また、現地の公権力による捜査目的で、

コメント [A7]: 「読みやすさ」対応で、表現を統一する。「以下の例がある」

コメント [A8]: 「情報開示における条件」に変更。

コメント [A9]: 外部委託に関する有識者検討会報告書の提言に従い削除

コメント [A10]: 「読みやすさ」「通則化」に伴い、文書を見直し（番号繰り上げ）。
「(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」

コメント [A11]: 通則化に伴い、クラウド事業者に対する考慮点を見直す。
「特にリスク管理に直結する事項は、十分に把握しておくことが重要である。リスク管理に直結する事項には以下の例がある。」

コメント [A12]: 記載箇所の変更
上記(5)の内容のため、(5)の直下に移動

データが差し押えられるといった場合に、業務の継続性に影響がないかといった点には十分に配慮する必要がある。特に、重要業務を委ねる場合には、データが分散格納されている場合を含めて、データの所在を把握することが重要になる。

高い可用性が求められる業務処理を行ったり、機密性の高い顧客情報の処理・蓄積・保管を行ったりする場合には、当該クラウドサービスに適用される法令が特定できる範囲で所在地域（国、州等）を把握する必要がある。

勘定系システム等の極めて高い可用性・信頼性が求められるシステムについては、データセンターの立地状況等を見極める観点から、詳細な所在地まで把握する必要がある。

インシデント発生時にデータセンターへの立入が必要になる場合や立入監査を行う際には、具体的な所在地を把握する必要がある。

ただし、委託する業務の重要度に応じて、データの所在について把握する必要性や把握の詳細度に差異が生じることはあり得る。したがって、金融機関等において業務の特性を十分検討した上で、委託する業務の重要度が高くないと判断し得る場合には、データの所在地に関する情報の把握について省略することも可能である。

5. クラウド事業者との間で係争が生じた場合の準拠法やこれを取り扱う裁判所に関する取決めが他国である場合に、クラウド事業者の選定にあたって評価すべきリスクとしては、以下のようなものがある。

(1) 現地の各種法制や裁判制度の把握と分析
(2) 現地での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での対応

6. クラウド事業者の決定には、責任者の承認を得ることが必要である。

7. クラウド事業者が提供するサービス等の導入に際しては、必要に応じて【運 72、運 73】も参照のこと。

【関連ガイドライン等】

システム監査指針	10-1-A　10-1-B　10-1-C　10-2-A
検査マニュアル　システムリスク編	顧保護Ⅱ.4.(1)　Ⅱ.4.(2)　ｵﾍﾟﾘⅢ.3　Ⅲ.5.(1)　Ⅲ.5.(2)
検査マニュアル　システム統合編	

コメント [A13]: 外部委託に関する有識者検討会報告書の提言に従い削除
なお、監査に関する内容については、監１において記載されている

コメント [A14]: 例示の一部として組み入れる。
「(13)外部委託先との間で係争が生じた場合の準拠法やこれを取り扱う裁判所に関する取決めが他国である場合に、外部委託先の選定にあたって評価すべきリスクとしては、以下の例がある。」

コメント [A15]: 外部委託に関する基準の通則化のため、サービス利用に関する内容以外の記載を追記

コメント [A16]: 「読みやすさ」対応として、参考部分を明確化する。

クラウドサービスの利用

適　用　区　分				
共	セ	本	提	ダ
◎				

運　109	クラウド事業者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.　クラウドサービスを利用する業務の種類や範囲に応じて、クラウド事業者と契約を締結すること。

契約時に考慮すべき事項については、以下のような例がある。

なお、クラウド事業者との契約やSLAの締結、SLO（Service Level Objective、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）の確認にあたっては、以下の例の他に、各金融機関が委託する業務のプロファイルに応じて必要と判断する事項を追加、変更することも考えられる。さらに、必要に応じて「サービスを利用するための契約」とは別に「リスク管理に関する契約」を締結することも考えられる。

(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、納品の条件と手順、及び権利の移転の時期
- ③　品質の保証と確認手順
- 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　クラウド事業者（複数のクラウド事業者がサービスの委託を受けた場合も含む）との間の管理境界や責任分界点に関する取決め（注）

（注）クラウドサービスには、複数のクラウド事業者がサービス業務の委託を受けることがある。こうした状況下では、特定のクラウド事業者外部委託先が所管するリソースにおける性能面のボトルネックや障害がクラウドサービス全体の品質に甚大な影響を与え得ることに留意する必要がある。インシデントが発生した場合に、それぞれのクラウド事業者が自らの責任の所在を認めず、責任の擦り付け合いが生じ、その結果、障害の状況把握や復旧対応が遅延するといった事態を回避しなければならない。

- 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

コメント [A17]: 外部委託に関する基準の通則化のため、クラウドに関する記載を外部委託に変更
以下、同様

コメント [A18]: 「読みやすさ」対応として修正。「必要がある」

コメント [A19]: 「読みやすさ」対応として、文章を例示の前に移動。

コメント [A20]: 外部委託に関する基準の通則化のため、クラウド利用に特化した記載を削除

コメント [A21]: クラウド基準新設時の補足事項のため削除

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、クラウド事業者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
⑦　クラウドサービスを利用するための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、監督当局等による検査等への協力義務、金融機関による監査受入、事業者と利用者間の報告・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　利用する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、もしくは発生が疑われる場合における、トレーサビリティ確保のための調査協力義務
⑧　利用する業務におけるクラウド事業者での対策を含むコンティンジェンシープラン（緊急時対応計画）

(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) 利用終了時の原状回復・新システム移行時の協力義務、データの返却・消去等
①　契約の解除条件（クラウド事業者の業務遂行に問題がある場合に、他のクラウド事業者等と契約する権利等）
②　サービス契約終了時におけるクラウド事業者によるデータの消去の実施、将来的なハードウェア更改・撤去時におけるデータの物理的消去の実施、データ消去の実施時期や消去証明書の発行時期【運 111】3.
③　サービス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や賠償に関する取決め

(8)クラウド事業者のサービスを利用した結果の知的財産権や使用権等の権利の帰属

ただし、以下の事項は契約に明記することが望ましい。

(9) クラウド事業者からの情報開示
①　平常時における標準的な情報開示内容の明記
クラウド事業者が複数の委託元金融機関から多種多様な開示請求を受けた場合、対応負担が増す可能性がある。このため、事前にある程度標準的な情報開示の範囲を契約またはSLA 等で定めることによりクラウド事業者の負担軽減を図り、金融機関からの情報開示の請求に対応しやすくする等の配慮をすることが望ましい。クラウド事業者によっては一般に公開している内容以上の情報提供について、その機密性の保全目的もあり消極的なケースがあるものの、金融機関による情報開示請求があった場合には、その必要性の説明が合理的である限り、金融機関とクラウド事業者が協議のうえ、必要な情報をクラウド事業者が提供することを契約上明記すること。開示請求の対象情報の機密性が高い場合には、両者の間で機密保持契約を締結したうえで提供すること。
②　リスク顕在化時の情報開示

コメント [A22]: (9)以降は、クラウド基準新設時に「望ましい」としていたが、外部委託契約の締結時に記載すべき事項は RBA が適用されるべきであるため削除

コメント [A23]: クラウド事業者に対する考慮点であったが、有効性等を鑑み、文書から削除するのが適当。また、例示の一部であるため、「読みやすさ」の観点から、文書の見直しを行った。
「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など」

リスク事象が発生した際、または各種の資料により情報漏洩リスクが高まった、もしくはクラウド事業者側の内部統制状況が悪化したなどと判断される場合、平常時における標準的な情報開示の前提に関わらず、金融機関からの開示請求を受けたときには、請求内容に応じた情報開示を行っていくべきことを契約やSLAに明記すること。

なお、金融機関等において、業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断し得る場合には、クラウド事業者に対し、リスク管理に直結する事項等の情報を詳細かつ厳格に求めないことも可能である。この場合には、クラウド事業者が提示する標準的な情報開示の内容で十分であり、さらに付加的な情報を求めないことも考えられる。

(10) 複数のクラウド事業者への委託

クラウドサービスには、複数のクラウド事業者がサービスの委託を受けることがある。こうした状況下では、特定のクラウド事業者が所管するリソースにおける性能面のボトルネックや障害がクラウドサービス全体の品質に甚大な影響を与えうることに留意すること。インシデントが発生した場合に、それぞれのクラウド事業者が自ら責任の所在を認めず、責任の擦りつけ合いが生じ、その結果、障害の状況把握や復旧対応が遅延するといった事態を回避しなければならない。

このため、障害発生時等の迅速な対応のため、委託元金融機関の管理能力を踏まえ、委託元金融機関・クラウド事業者間での責任関係を明確にし、一元的な窓口機能やクラウド事業者間の相互調整機能を担う事業者をあらかじめ決めておくこと。なお、この役割を委託元金融機関が担える場合においては、クラウド事業者側の相互調整機能を担う事業者は必要ではない。

なお、金融機関等において、業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断し得る場合、かつリスク分析の結果として、障害発生時の影響範囲が限定的である、もしくは復旧自体が遅れてもその影響が軽微であると判断し得る場合は、相互調整を担う事業者を置かないことも可能である。

(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

金融機関等は、安定したサービスの確保や情報保護等のために、直接の委託先であるクラウド事業者のみならず、再委託先についても同様に実態把握し適切なリスク管理を行うこと。

ただし、通常システムにおける再委託を行う場合、委託先の再委託先に対する審査・管理プロセスが金融機関等のそれと同等かそれ以上実効的であるとみなされる場合には、金融機関等が、あらかじめ委託先の審査・管理プロセスの整備・運用状況の適切性を検証し、確認することで、個別の再委託先の事前審査に代替させることが可能である。

・委託の状況を把握し、不適切な再委託先が介在することを排除するため、委託業務を再委託する場合、再委託先に対する適切な事前審査を行うこと（注１）。

（注１）金融機関が自ら事前審査を行う場合、事前審査作業を効率化するため、クラウド事業者側と金融機関側の合意により、あらかじめ、再委託先の候補先企業群に対し事前審査を行うという工夫を講じることも考えられる。

・再委託先に対する事前審査については、例えば、クラウド事業者による再委託先の審査・

コメント [A24]: 同上。「読みやすさ」の観点からも文章を見直した。
「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、もしくは外部委託先側の内部統制状況が悪化したなどと判断される場合の委託元金融機関からの請求内容に応じた情報開示など」

コメント [A25]: 外部委託に関する基準の通則化のため、クラウド利用に特化した記載を削除

コメント [A26]: クラウド基準新設時の補足事項のため削除

コメント [A27]: クラウド利用に特化した記載と「読みやすさ」の観点から文書を見直した。
「委託元金融機関・外部委託先間での責任関係の明確化、一元的な窓口機能や外部委託先間の相互調整機能を担う事業者の選定など」

コメント [A28]: クラウド基準新設時の補足事項のため削除

コメント [A29]: 再委託管理全般を指す内容であるため、場所を(11)再委託管理のしたいに移動。（「直接の委託先である」の文言は不要と判断し削除）

コメント [A30]:
外部委託に関する有識者検討会報告書の提言に従い、「再委託先の事前審査」に関する内容を反映
＜参考＞【運 88】
4.(4)再委託（再委託にかかる責任の所在の明確化・金融機関等の事前承認の必要性等）

管理プロセスが金融機関のそれよりも実効的であるとみなされる場合には、クラウド事業者側での事前審査が最善策となり得る点には留意が必要である（注２）。なお、勘定系システムや機密性の高い顧客データを保管するシステム等、特に重要な業務を再委託する場合には、金融機関等自らが事前審査をすること。

（注 2）クラウド事業者側での再委託先の審査については、金融機関のリスク管理ポリシー等と照らし、金融機関自らが行う審査と比較して、その範囲・深度について同等かそれ以上である必要がある。これが満たされる場合は、個別の再委託先（既存分、新規追加・変更分）に係る事前報告や承諾を必ずしも要しない。

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、速やかな復旧回復の責任を負うことと同時に、委託先が損害賠償上限条項に定められた範囲内で賠償責任を負うことを明確にすること。

③　委託先・再委託先間の義務の明確化

委託先が金融機関に対して負う義務報告・内部統制確保義務などの各種義務を再委託先も負う扱いとするため、委託先・再委託先間の契約に必要な義務に関する条項を設けることを金融機関と委託先との契約に明記すること。

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、金融機関はクラウド事業者に対し、再委託の中止を求めることができることを明確にし、契約上明記することが望ましい。クラウド事業者が中止の求めに応じない場合は、サービス利用の停止も検討すること。

なお、金融機関等において、業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断し得る場合は、再委託先における委託元金融機関による事前の審査や日常のモニタリング等のリスク管理を簡易化することも可能である（注）。例えば、再委託する対象業務が重要な業務ではなく、サイバー攻撃対策や内部不正による情報漏洩対策などのリスク管理及びログの取得・分析を含めたインシデント発生時の緊急対応を直接の委託先であるクラウド事業者側で行うといった場合などが該当するという判断も可能である。

（注）リスク管理の簡易化については、例えば、チェック項目や頻度、深度の軽減化が考えられる（ただし、反社会的勢力等については、社会的に厳格な対応が求められていることに留意すること）。

(12) 委託元金融機関による立入監査・モニタリング【運 112】

①　立入監査等の権利の明記

業務委託契約に、委託元及び再委託先に対し金融機関等の立入監査等を実施する権利を明記すること。

②　立入監査等の代替手段

委託元金融機関が直接、立入監査等を実施するのではなく、平常時には立入監査等のスキルのある外部の第三者による検証により代替することも可能とすること。

③　立入監査等の権利行使

クラウド技術に関する重要な脆弱性が判明した場合、クラウド事業者における他の顧客

コメント [A31]: 上記コメント[A14] を追加したため、重複する内容を削除のうえ、全体を以下の文書に見直した。
「金融機関等は委託業務が再委託される際、再委託先に対する事前審査を実施する。ただし、通常システムに…（中略）適切性を検証し、確認することで、個別の再委託先の事前審査に代替させることも考えられる」

コメント [A32]: 「読みやすさ」の観点から、例示内の文章として見直し。
「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など」

コメント [A33]: 「読みやすさ」の観点から、例示内の文章として見直し。
「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）に関する条項が委託先・再委託先間の契約上に設けられることを、金融機関等と委託先の契約に明記する。」

コメント [A34]: 「読みやすさ」の観点から、例示内の文章として見直し。
「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や、外部委託先が中止の求めに応じない場合の、業務委託契約の解除に関する条項の設置な…

コメント [A35]: 再委託管理全般を指す内容であるため、場所を(11)再委託管理のしたいに移動。

コメント [A36]: 外部委託に関する基準の通則化のため、「立入監査」の表現を「監査」に変更
以下、同様

コメント [A37]: 外部委託に関する有識者検討会報告書の提言に従い、「再委託先に対する監査権の明記」に関する内容を反映

に関わる領域でインシデントが発生した場合、他事業者でインシデントが発生した場合等に、委託元金融機関への影響を確認するため、臨時の第三者監査を行うことが可能となっていること。

なお、立入監査等に代替する第三者監査が行われない、または依拠できないと判断される場合に限定して立入監査等を行う運用形態を取る場合は、立入監査等の権利行使の条件を必要に応じ書面化し、委託元金融機関とクラウド事業者の両者が認識を共有することも可能である。

④　立入監査等の受入対応費用

立入監査を受けるクラウド事業者側の受入対応の費用については、委託元金融機関、クラウド事業者側のいずれが負担するか、あらかじめ両者で協議しておくこと。

⑤　再委託先への立入監査等

再委託する業務が重要な場合、再委託先等に対して、委託元金融機関とクラウド事業者間の契約に、金融機関による再委託先への立入監査を実施する権利を明記すること。

⑥　立入監査等の指摘事項の扱い

立入監査等により判明した指摘事項については、対応の是非を含め、委託元金融機関とクラウド事業者の両者で協議のうえ、合理的な対応期間を定め、期間内に対応する旨をあらかじめ契約上明確にすること。

(13) 金融監督当局の検査等

金融監督当局は、当該金融機関の業務の健全性について、委託業務も含めて検証する公益上の要請がある。当局の要請があった場合、クラウド事業者としては立入検査等を受け入れることが法律上求められる。

①　当局検査等への協力義務

当局の立入り検査等の円滑な実施を担保するため、委託元金融機関とクラウド事業者との間の契約に、クラウド事業者の当局検査等への協力義務を明記すること。

②　再委託先への立入り検査等

業務委託の再委託先（再々委託先を含む）に対しても、金融機関と元請け事業者との間の契約に、当局検査等への協力義務を明記すること。

③　検査等後の指摘事項の扱い

当局検査等の指摘事項については、速やかに改善を図る旨の条項を契約に明記すること。

(14) インシデント発生時の立入調査

①　情報漏洩等のインシデントが発生した場合、もしくは発生が疑われる場合に、クラウド事業者が情報提供に応じない、提供しても迅速性に問題があると金融機関が判断した場合、もしくは提出情報の網羅性に疑義が有る場合は、委託元金融機関自ら、もしくは委託元金融機関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の立入調査が実施できることについて、契約上明記すること。

②　調査時に収集の対象となる証跡の範囲（クラウド事業者の他の顧客にかかわる証跡のため委託元金融機関に一般的には開示できないものも含む）及び抽出ツールの開発・検証のために必要となる費用負担（注）について、契約締結時に合意を得ること。

（注）クラウド事業者側が自らのポリシーにより、委託元金融機関の立入調査人や金融機関の指定するセキュリティ業者・デジタルフォレンジック事業者による機器操作のための調査受入を避けたい場合は、トレーサビリティを確保するため、委託元金融機関の施設、クラウド事業者側の施設、または外部施設の何れかにおいて解析に必要な

コメント [A38]: クラウド基準新設時の補足事項であり、「委託元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についても明記することが考えられる」と修正する。

コメント [A39]: 「読みやすさ」対応として、例示の一項目となるよう修正する。「協議しておくことが考えられる」

コメント [A40]: 上記コメント[A11]の修正内容のとおり、委託先ならびに再委託先に対する「監査権の明記」に関する記載を統合したため削除

コメント [A41]: 「読みやすさ」対応として、例示内の文章に修正する。

コメント [A42]: 法令に定めるものであり、削除

コメント [A43]: クラウド基準新設時の補足事項であり、「委託業務の範囲等に応じ、インシデント発生時に立入調査を行う場合について、明記することも考えられる」という文書に見直す。

情報を抽出することのできるツールが必要となる。また、これらの抽出ツールが適切に作動することに関する外部の第三者による検証を受けることが必要である。こうしたデータ抽出の機能は、アプリケーションの一部機能としてユーザーに提供されるケースもあるが、提供されていない、ないし網羅性に問題がある場合は、別途、抽出ツールの開発・検証が必要になる。この場合、委託元金融機関としては、収集の対象となる証跡の範囲（当該クラウド事業者の他の顧客にかかわる証跡のため委託元金融機関に一般的には開示できないものも含む）や抽出ツールの開発・検証のために必要となる費用負担について、契約締結時にクラウド事業者とあらかじめ合意を得る必要がある。

③　クラウド事業者の経営不安が発生した場合、委託元金融機関自らもしくは委託元金融機関が指定する専門業者が、必要に応じ、クラウド事業者施設に立ち入り、顧客データや関連著作物・成果物の保全を行うことを認めるよう契約に明記すること。

なお、金融機関等において、業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断し得る場合は、費用対効果を踏まえた管理策を講じることで立入に代替することも可能である。【運 112】4.

(15) 記憶装置等の障害・交換

記録媒体等を障害や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にしておくこと。【運 110】

(16) 海外でのデータ保管時の留意点

金融機関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、日本語でのサポート、クラウド事業者の日本法人等の障害対応窓口設置を明確にすること。

(17) トレーサビリティの確保

クラウドは、仮想化され、かつ動的に変化する環境であるため、万一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こと。

2. SLA の締結や SLO の確認により、サービスレベル（注）について合意することが望ましい。SLA 及び SLO に記載すべき指標には以下のような例がある。

（注）　クラウド事業者との契約の中には SLA が含まれるのが通例であるが、多くの標準的な SLA では、基準となる月間稼働率などを定めたうえで、実際の稼働率が基準を下回った場合にサービスの利用料を減額するといった内容にとどまっている。そのため、例えば、勘定系システムのオンライン処理など高い稼働率が求められる場合では、こうした標準的な SLA による契約締結では不十分な可能性がある。

クラウド事業者の顧客は金融機関をはじめ、さまざまな業種にわたる。その中で各顧客企業との間で個別の内容の契約を準備するのは効率的ではないとの考えから、クラウド事業者は SLA を個別に締結することに対し消極的な場合もある。一方で、金融機関が特に重要な業務を委託する場合においては、その社会的な重要性に鑑み、相応の高いサービスレベルが求められる。

コメント [A44]: クラウド基準新設時の補足事項であり、通則化にあたり「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や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、予め委託先と協議しておくことも考えられる」と修正する。

コメント [A45]: クラウド基準新設時の補足事項であり、通則化にあたり「保全を行うことについて、委託先と予め協議しておくことが考えられる」と修正する。

コメント [A46]: 通則化にあたり、「立入調査に代替することも考えられる」と修正。

コメント [A47]: 「読みやすさ」対応として、例示内の文章に修正。

コメント [A48]: 「読みやすさ」対応として、例示内の文章に修正。

コメント [A49]: 「読みやすさ」対応として、例示内の文章に修正。

コメント [A50]: クラウド基準新設時の補足事項のため削除

(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）の保証

（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は、以下のような事項を考慮する必要がある。

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）や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

なお、上記②に関して、グローバルベースでサービスが提供されるパブリッククラウドでは、緊急的なセキュリティ対策等に係る計画停止作業について、ユーザー全体の安定性を優先するため、必ずしも個々のユーザーの要望（作業のタイミングや時間等）に沿わない形で実施される可能性があることにも留意する必要がある。

(2) サポート（障害対応、問合せ対応）の保証

(3) データ管理の保証（利用者データの保証）

(4) 統制環境（再委託先管理（再々以下の階層の先を含む）、機密保護の維持、統制環境の維持）の保証

3. 委託する業務の重要度に応じて、契約や SLA に盛り込まれる内容や基準値が異なるほか、内容自体の必要性も変わり得る。したがって、金融機関等において業務の特性を十分検討した上で、委託する業務の重要度が高くないと判断し得る場合には、必ずしも上記 1.～2.のすべてを必要とせず、クラウド事業者が提示する標準的な SLA を締結することや一般的な契約の締結のみを行い、SLA の締結を省略することも可能である。

4. サービスレベル合意の違反のほか、クラウド事業者や金融機関の方針変更によってクラウド事業者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ため、事前に代替のクラウドサービスや一般のアウトソーシングに移行する、もしくはオンプレミスの環境に移行することができるような対策を講ずることが望ましい。

例えば、以下のような例がある。

(1) クラウド事業者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

ただし、金融機関等において業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断し得る場合は、クラウド事業者の協力を前提とせず、別のクラウド事業者に移行するための準備をあらかじめ行っておくことをもって代替することが可能である。例えば、コンピューティング資源のみを委託する IaaS（Infrastructure as a Service）の場合では、クラウド事業者の協力がなくても比較的容易に別のクラウドサービス基盤に移行することが可能であるため、こうしたケースに該当すると考えられる。

コメント [A51]: 「読みやすさ」対応として、例示内の文章に修正。
「評価にあたって考慮する事項には、以下の例がある。」

コメント [A52]: クラウド基準新設時の補足事項のため削除

コメント [A53]: クラウド基準新設時の補足事項のため削除

コメント [A54]: クラウド基準新設時の補足事項のため削除

コメント [A55]: 「読みやすさ」対応として、「実施する対策には以下の例がある」と修正。

コメント [A56]: クラウド基準新設時の補足事項のため削除

外部の統制
利用検討時

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　21	外部委託を行う場合は、事前に利用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。

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、外部委託先の選定に際しては手続きを明確にし、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。

1.　外部委託先を選定するにあたっては、事前に目的や範囲等を明確にしたうえで、選定手続きを明確にすることが必要である。

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) ハードウェア及び回線の設置、入替、撤去
(5) 入力データの作成（端末オペレーションを含む）
(6) 記録媒体、ドキュメント及び帳票等の作成、保管、配送、廃棄
(7) 館内、構内及び店内の警備
(8) 電源、空調、防犯等設備の管理、保守
(9) 集中監視（CD・ATM 等）
(10) CD・ATM の現金等の管理

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。

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（再委託先を含む）の選定条件
(8) 外部委託に関する自社窓口と役割 等

コメント [A1]: 【運 87】、【運 87-1】及び【運 108】の「基準小項目」を統合

コメント [A2]: 【運 87】、【運 87-1】及び【運 108】の「適用にあたっての考え方」を統合

コメント [A3]: 【運 87】1.【運 87-1】1.及び【運 108】1. を統合

コメント [A4]: 「外部委託」には「クラウドサービスの利用」を含むため、中扉（基準中項目の冒頭説明）にて、「クラウドサービスの利用を含め」と記載する。

削除: .

2

コメント [A5]: 【運 88】2.

コメント [A6]: 【運 87】2.及び【運 108】2. を統合

削除: 3.

2. システムの開発や運用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。

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。

外部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、適切な外部委託先を選定する必要がある。その際、委託業務範囲（クラウドサービスにおける IaaS、PaaS、SaaS 等によって委託先の責務に差異が生じること等）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。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。

ただし、金融機関等において業務の特性を十分検討した上で、委託する業務の重要度が高くないと判断し得る場合は、外部委託先の公開情報や、業界における評判や実績等による客観的な評価を行うことも可能である。

評価する事項としては、以下の例がある。

(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、他プロジェクトやサービスでの評判等）
　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（再委託先管理も含む）、外部監査の受検や各種公的認証の取得状況、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
　特にリスク管理に直結する事項は、十分に把握しておくことが重要である。リスク管理に直結する事項には以下の例がある。
　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 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）、日本語での対応）
(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

コメント [A7]: 【運 87】3.

削除: 4

コメント [A8]: 【運 87-1】2.及び【運 108】3.を統合したうえで、整理・通則化

削除: 5

コメント [A9]: 「その実現が可能な」という表現が具体的に示すものが不明確なため、「適切な」と表現を見直した。

削除: その実現が可能

削除: こと

コメント [A10]: 委託業務の内容によって責務に差異が生じる場合を追記した。

コメント [A11]: 左記下線部分が該当

＜参考＞【運 87-1】

2. 外部委託先を客観的に評価すること。評価する項目としては、以下のような例がある。

(1) 安定性（財務内容）、健全性
(2) 組織体制（コンプライアンス体制含む）
(3) 信頼度および受託実績（類似システムの開発実績、他プロジェクトでの評判等）
(4) 技術レベル（業務内容の理解度、業界に関する知識、情報収集能力、プロジェクト管理能力、導入サポート力等）
(5) 委託費と支払い条件
(6) セキュリティ対策の実施状況（機密保護状況含む）
(7) 問題発生時の対応力
(8) 保守体制等
(9) 各種公的認証の取得状況

(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) 係争時等における他国での裁判に関する事項

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

他国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 現地の各種法制や裁判制度の把握と分析
② 現地での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での対応

4 外部委託先の決定には、責任者の承認を得ることが必要である。

＜参照先＞

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、【運 72、運 73】も参照のこと。

削除: 可能か

コメント [A12]: 【運 108】5. を通則化

削除: 外部委託先の選定にあたって

コメント [A13]: 【運 87-1】3.

削除: 6

外部の統制
契約締結時

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統　22	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.　金融機関等が外部委託した業務が安全に遂行されるために、機密保護や安定的なシステム運用等を契約として外部委託先と締結するとともに、その契約の遵守状況を定期的に確認することが必要である。また、委託契約とは別に「機密保持に関する契約」や、「リスク管理に関する契約」を締結することも考えられる。

契約時に考慮すべき事項としては以下の例がある。

(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、納品の条件と手順、及び権利の移転の時期
- ③　品質の保証と確認手順
- 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）との間の管理境界や責任分界点に関する取決め（例えばクラウドサービスの利用にあたっては、利用形態（IaaS、PaaS、SaaS など）によって責任分界点の考え方に差異が生じる場合がある）
- 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
- 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、監督当局等による検査等への協力義務、金融機関による監査受入、事業者と利用者間の報告・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

コメント [A1]: 【運 88】1.

削除: 安全な業務の遂行

コメント [A2]: 目的と内容が重複しているため、前説の「適用の考え方」を踏まえ、記載を見直した。

コメント [A3]: 実態を踏まえ、「機密保持に関する契約」を追加した。

コメント [A4]: 【統 25】と統合すべきか？（論点３）

コメント [A5]: 「クラウドサービスには IaaS や PaaS など、開発・運用を委託する場合と比較して、委託先の責務が異なる（小さい）場合が想定される。そういった考慮事項を明示すべき」との意見を踏まえ、文章を追加。

② 作業の指示に関する取決め
③ 利用する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、もしくは発生が疑われる場合における、トレーサビリティ確保のための調査協力義務
⑧ 利用する業務における外部委託先での対策を含むコンティンジェンシープラン（緊急時対応計画）

(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) 契約終了時の原状回復・新システム移行時の協力義務、データの返却・消去等
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の消去の実施、データ消去の実施時期や消去証明書等の発行時期【統 26】3.
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や賠償に関する取決め
(8) 外部委託業務の成果の知的財産権や使用権等の権利の帰属
(9) 外部委託先からの情報開示
① 平常時における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など
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、もしくは外部委託先側の内部統制状況が悪化したなどと判断される場合の委託元金融機関等からの請求内容に応じた情報開示など
(10) 複数の外部委託先への委託
委託元金融機関等・外部委託先間での責任関係の明確化、一元的な窓口機能や外部委託先間の相互調整機能を担う事業者の選定など
(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
委託先の再委託先に対する審査・管理プロセスが金融機関等のそれと同等かそれ以上実効的であるとみなされる場合には、金融機関等が、あらかじめ委託先の審査・管理プロセスの整備・運用状況の適切性を検証し、確認することで、個別の再委託先の事前審査に代替させることも考えられる。
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など
③ 委託先・再委託先間の義務の明確化
委託先との契約において、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）に関する条項が委託先・再委託先間の契約上に明記される内容となっているか
④ 再委託の中止の扱い

削除: 将来的なハードウェア更改・撤去時におけるデータの物理的消去の実施、

コメント [A6]: 【統 26】と統合すべきか？（論点３）

削除: 運 111

削除: 金融機関等は委託業務が再委託される際、再委託先に対する事前審査を実施する。ただし、通常システムにおいて再委託を行う場合は、

削除: 設けられることを、金融機関等と委託先の契約に明記する

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や、外部委託先が中止の求めに応じない場合の、業務委託契約の解除に関する条項の設置など

(12) 監査・モニタリング【監 1】

① 監査等の権利の明記

委託先及び再委託先に対する委託元金融機関等の監査等を実施する権利の明記

② 監査等の代替手段

委託元金融機関等が直接、監査等を実施するのではなく、平常時には監査等のスキルのある外部の第三者が検証を代替する等の手段の明記

③ 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や、委託元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

④ 監査等の受入対応費用

監査を受ける外部委託先側の受入対応の費用負担に関する取り決め

⑤ 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（対応期間など）

(13) インシデント発生時の立入調査

① 情報漏洩等のインシデントが発生した場合、外部委託先における他の顧客に関わる領域でインシデントが発生した場合、または他事業者において委託業務と関連性を有するインシデントが発生した場合、もしくは発生が疑われる場合等において、委託元金融機関等みずから、もしくは委託元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旨の明記

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や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、予め委託先と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、委託元金融機関等みずからもしくは委託元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保全を行うことについて、委託先と予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

記録媒体等を障害や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。【統 26】

(15) 海外でのデータ保管時の留意点

金融機関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、日本語でのサポート、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

万一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 の締結や 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。

削除: 委託元金融機関等による

削除: 運 112

コメント [A7]: 【運 88】4.の一部について、外部委託有識者検討会の議論を踏まえ、【運 109】の内容を反映。
＜参考＞【運 88】
4.(15) 監査の権利（外部委託先を監査する権利あるいは外部の専門機関により監査を実施する権利等）

削除: 外部委託先における他の顧客に関わる領域でインシデントが発生した場合、または他事業者において委託業務と関連性を有するインシデントが発生した場合など、

削除: については、委託元金融機関等、外部委託先側のいずれが

削除: するか、あらかじめ両者で協議しておくことが考えられる。

削除: については、対応の是非を含め、委託元金融機関等と外部委託先の両者で協議のうえ、合理的な対応期間を定め、期間内に対応する旨をあらかじめ契約上明確にする。

削除: を

削除: することも考えられる。

コメント [A8]: リスクベースアプローチの考え方に基づくと、実施の要否は金融機関等によって判断されるものであり、「費用対効果を踏まえ」とした文章は不要と判断して削除した。

コメント [A9]: 【統 25】と統合すべきか？（論点３）

削除: 運 110

コメント [A10]: 【運 88】5. 、【運 109】2. を統合

削除: 4

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）の保証

（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）や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）の保証

(3) データ管理の保証（利用者データの保証）

(4) 統制環境（再委託先管理（再々以下の階層の先を含む）、機密保護の維持、統制環境の維持）の保証

(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、期限の保証

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. 委託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。

4. サービスレベル合意の違反のほか、外部委託先や金融機関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。

実施する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: すべき

コメント [A11]: ＜参考＞【運 88】5.
・運用業務を委託する場合の例：システムの可用性（Availability）の保証、オンラインシステムの稼働開始時限の保証

コメント [A12]: 統合に伴い、【運 88】5. の一部の記載方法を変更
＜参考＞【運 88】5.
・開発業務を委託する場合の例：開発に要する人員や開発期間、期限の保証

コメント [A13]: 【運 88】5.

コメント [A14]: 【運 88】6.

削除: 5

コメント [A15]: 【運 109】4.

削除: 6

（参考）

外部委託の形式について

(1) 派遣（労働者派遣）とは、派遣元事業主が自己の雇用する労働者を、派遣先の指揮命令を受けて、この派遣先のために労働に従事させることを言う。派遣労働者と派遣元事業主との間には雇用関係が、派遣労働者と派遣先との間には指揮命令関係がある。なお、派遣形態での契約における労働者の管理については、「労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律」を参照のこと。

(2) 請負とは、請負者（企業）が労務提供の結果として請負った仕事を完成させ、注文者（企業）がその成果に対して報酬を支払うことを、約束する契約形態である。請負では請負者が従業員等をみずから指揮命令し、請負った仕事を完成させる。（請負の意義　民法第 632 条参照）

(3) 委任は、請負者が従業員等をみずから指揮命令し、労務を提供する点で、請負と同じである。しかし、請負では仕事の完成に対し報酬が支払われるが、委任では委任された労務の提供自体に対し報酬が支払われる点が異なっている。（委任の意義　民法第 643 条参照）

参照法令	労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律、民法第 632 条、643 条

外部の統制
外部委託管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統 23	外部委託先の要員にルールを遵守させ、その遵守状況を管理、検証すること。

外部委託先（再委託先を含む）の要員のセキュリティ管理を適切に行うため、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、その遵守状況を管理、検証すること。

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、委託業務の内容や作業の範囲に応じて、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に応じて明確にし、これを周知徹底する必要がある。

   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、業務体制や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、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やシステムへのアクセス権限は、業務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と見直しの手順については【運 18】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管理、検証する必要がある。そのためには、金融機関等は外部委託業務の内容や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や、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。

コメント [A1]: 【運 89】を変更

コメント [A2]: 外部委託に関する有識者検討会報告書の提言に従い、「再委託先」を含む記載に変更

削除: 教育、監査

削除: を行うこと

コメント [A3]: 「教育」「監査」という表現は、基準小項目および、解説の内容と乖離するため見直した。

削除: 遵守させる

削除: を金融機関等が外部委託先に明確に提示する

削除: 特に、

削除: し、遵守を義務づけることが望ましい考えられる

コメント [A4]: 関連する内容が分離されていたため、記載箇所を（2）の下から移動させた。

コメント [A5]: 委託先への教育ではなく、実質的には周知徹底させるという意味と解されるため、表現を見直した。

削除: に対し、

削除: に関する教育がなされることの実施

コメント [A6]: 適用にあたっての考え方と内容が不整合であり、文章を見直した。

削除: ことが望ましい

削除: 運 91

外部の統制
外部委託管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統 24	外部委託における業務組織の整備と業務の管理、検証を行うこと。

外部委託先（再委託先を含む）に委託した業務内容の実施状況を確認するため、委託業務の内容や作業の範囲に応じて、業務組織の整備を行うとともに、委託契約に基づき管理、検証を行うこと。

1.　外部委託の対象の業務を円滑、適正に運営する観点から、委託業務の内容や作業の範囲に応じて委託業務を遂行する業務組織（金融機関等自身と外部委託先の両者により構成される組織）の、業務範囲及び責任と組織を明確にし、相互牽制が有効に機能する体制とする必要がある。
　なお、組織の整備と相互牽制については【統 12】を参照のこと。

　業務組織の整備に関する具体的事例としては以下の例がある。

(1) 委託先の管理状況を把握する。
　管理状況の把握方法としては以下の例がある。
　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　業務処理体制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や犯罪の報告を受ける。

(2) 委託先における業務の実施状況について、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) 委託先における業務の実施状況を定期的にモニタリングする。
　委託元は、担当要員を選定等して、委託先における顧客データ等の管理状況や開発・運用状況等について把握する。

~~(5) 委託業務終了後、関連重要資料、文書等を回収する。~~
　~~機密保護と不正使用防止のため、委託業務終了後、委託先に貸し出した関連重要資料、文書等もしくはそのコピーを回収することが必要である。~~

2.　外部委託先の業務の成果が金融機関等が求めるレベルに達しているか、金融機関等が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

コメント [A1]: 【運 90】を変更

コメント [A2]: 外部委託に関する有識者検討会報告書の提言に従い、「再委託先」を含む記載に変更

削除: 外部

削除: 運 9

削除: 2.

削除: の場所には情報が持ち出されないことを確認する。

コメント [A3]: 「点検」は「監査等」に含めるため、【統 22】の内容と整合性を取って文章を見直した。

削除: 点検または

削除: ここでいう点検とは、外部委託業務に関わる委託元部門が、委託先の管理状況を直接確認することを指す。また、

削除: 必要がある

削除: 運 91

削除: (3) 委託先が作成したシステム設計書、プログラム等の検証を行う。 .
機能要件の充足度、標準化遵守状況の確認及び異例処理を含んだ検証テストを行う必要がある。 .

削除: 4

削除: 必要がある

コメント [A4]: 委託業務終了時の情報漏洩防止対策であり、【統 26】へ移動する

削除: 3

確認及び異例処理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（Service Level Agreement）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 22】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。

コメント [A5]: 2.(3)に記載されていたが、業務の成果を把握する内容であり、3 に移動した。なお、「システム設計書」および「プログラムの検証」は「機能要件の充足度」や「標準化遵守状況の確認」に含まれると判断したため、例示から削除した。

削除: 運 88

外部の統制
外部委託管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統 25	外部委託にあたって、データ漏洩防止策を講ずること。

外部委託先（再委託先を含む）によるファイルのコピーや盗難等による漏洩を防止するための対策を講ずること。

1.　外部委託先に重要なデータの管理を委託する場合、データ漏洩防止策を講ずることが必要である。

暗号化を含むデータ保護に関する管理策としては、以下の例がある。【技 28】【技 29】

(1) 蓄積・伝送データの暗号化

暗号化の仕様（処理プロセスにおいてどの部分が暗号化されておりどの部分がされていないか、暗号方式、暗号鍵の管理態勢等）を把握し、自社のセキュリティポリシー等に合致しているかどうかを確認する。

(2) 暗号鍵の管理主体

外部委託先に暗号鍵の管理を委ねる場合には、その管理策の詳細を十分に把握し、自社のセキュリティポリシー等に合致していることを確認する。【運 43】

(3) 暗号化の代替策

暗号化の代替策として、元データは金融機関側で持ち、外部委託先環境下にあるデータは無作為な乱数（トークン）に置き換え、実質的に無意味化するとしたトークン化技術を利用することも考えられる。ただし、トークン化を管理策として採用する場合には、金融機関におけるトークンマッピング（対応表）の管理についても相応の管理策を整備しておく。

2.　記憶装置の故障等により、機器・部品を交換する場合には、交換対象の記憶装置等の機器・部品に金融機関等やその顧客の情報等の機密性の高いデータが残存している可能性があるため、これらの記憶装置等に対しても、データ消去も含めた十分な管理を行う必要がある。

ただし、契約中の記憶装置等の障害・交換における消去証明書の発行・取得については、外部委託先に対して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ことで代替することも可能である。

管理策としては、以下のような例がある。

(1) 交換された元の記憶装置等において実際にデータが格納されていた可能性のある記憶媒体上のデータの物理的または論理的消去を実施する（回転部や論理回路等の機器故障により論理的消去の操作ができない場合は、物理的消去を実施）。

(2) 外部委託先の施設外に搬出される前に物理的消去を実施する。

(3) 復元を不可能または著しく困難な状態にしたうえで持ち出すといった点をあらかじめ契約

コメント [A1]: 【運 110】を変更

コメント [A2]: 外部委託に関する基準の通則化のため、クラウドに関する記載を外部委託に変更し、「再委託先を含む」とした以下、同様

コメント [A3]: 実 118（技 28）、実 119（技 29）と整合的となるよう見直す。

削除: 、重要なデータについては暗号化等

削除: ただし、暗号化やトークン化等の代替策は、顧客データ等の重要なデータを保全するための管理策であり、金融機関等において、情報の機密性や業務におけるリスクプロファイルにより重要なデータでないと判断し得る場合は、暗号化やトークン化等の管理策を省略することも可能である。

削除: 機密性の高い個人データ等が含まれているデータについては、暗号化等の管理策を講じることが必要である。
なお、仕様上の制約から暗号化が不可能な部分（平文で処理される部分）でのデータ覗き見リスクを把握するため、

削除: リスク管理の

削除: 判断する必要がある

削除: 概要

削除: リスク管理の

削除: 判断する必要がある

削除: とトークンを

削除: が可能である

削除: が必要となる

コメント [A4]: 重要なデータにおいても代替可能と読み取れる内容であり、ご意見があれば、記載を見直す。

書または SLA 等に明記する。
(4) データの消去の方法として、必要に応じて【運 75】も参照のこと。

検証のポイント
案１　上記内容としたうえで、【統 25】を残すべきか。

案２　上記内容は契約締結時に確認する事項として、【統 22】に移動させ、【統 25】を廃止すべきか。

案３　上記内容は契約締結時に確認する事項として、【統 22】に以下を追加し、【統 25】を廃止すべきか。

【統 22】
1.(2) 個別契約条件、サービス仕様、データ保護の管理策
⑥セキュリティ管理方法及び体制
委託先におけるデータ漏洩防止策（暗号化等）の対策、管理体制（暗号鍵の管理体制等）を確認する。【技 28】【技 29】【運 43】

1.(14) 記憶装置等の障害・交換
記憶装置等の障害や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など、漏洩防止に関する事項を委託先と合意しておくことが考えられる。【運 75】
また、記憶装置等の障害・交換における消去証明書の発行・取得については、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ことも考えられる。【統 26】

案４　その他

コメント [A5]: リスクベースアプローチの考えに基づき判断される部分であり、場合分けは不要と判断した。

削除: 。
ただし、重要なデータを扱わない場合は、記憶装置等の交換に際し、データの消去・破壊を実施しないことも可能である。

書式変更: インデント ： 最初の行 ： 1.3 字

外部の統制
外部委託管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統 26	外部委託契約終了時のデータ漏洩防止策を講ずること。

機密保護や不正防止等のため、外部委託契約の終了にあたっては当該システム・機器等からデータの漏洩が生じないように防止策を講ずること。

1. 外部委託の契約を終了する場合、金融機関等がみずからデータを消去することが困難な場合であっても、外部委託先とともに機密保護、プライバシー保護及び不正防止のための対策を講ずることが必要である。【運 75】

2. 外部委託契約の終了時には、委託先が保有するデータの消去を行うことが必要である。

データ消去の方法としては、以下の例がある。

(1) 物理的消去（消磁や破壊）

(2) 論理的消去

① データ管理領域とデータ保存領域におけるリンク情報の不可逆的な切断

② 全データの保存領域の上書き（意図的で無意味なデータもしくは他のユーザーのデータによる上書き）

③ 保管データが暗号化されている場合における暗号鍵の廃棄

3. 外部委託先がデータ消去を実行する場合は、消去証明書等を受領することが必要である。

なお、外部委託契約終了時において、外部委託先が論理的消去も含めたデータ消去を実施することを契約書に記載し、かつ外部の第三者が監査等において、消去プロセスの適切性を検証することにより、消去証明書の発行・取得の代替とすることも可能である。

4. 顧客データ等の機密情報を扱わない業務を外部委託先に委ねる場合は、契約終了時のデータ消去プロセスを簡略化または不要とすることも考えられ、消去証明書を不要とすることも可能である。

5. 委託業務終了後、関連重要資料、文書等を回収する。

機密保護と不正使用防止のため、委託業務終了後、委託先に貸し出した関連重要資料、文書等もしくはそのコピーを回収などの対策を講ずることが必要である。

コメント [A1]: 【運 111】を変更

コメント [A2]: 外部委託に関する基準の通則化のため、クラウドに関する記載を外部委託に変更
以下、同様

削除: にあたっては、

削除: 以下の方法が考えられるは物理的消去と論理的消去などの方法が考えられる。なお、将来的なハードウェア更改・撤去時に物理的消去を行うことが望ましい。

削除: 以下のいずれかによる

コメント [A3]: 【統 25】の記載内容と整合性が取れていないため、「消去証明書等が必要」としたうえで、消去証明以外の方法についても記載した。

削除: 望ましい

コメント [A4]: 【統 24】から移動し、対策が明確となるよう一部見直し。

検証のポイント

案１　上記内容としたうえで、【統 26】を残すべきか。

案２　上記内容はデータ漏洩防止に関する基準として、以下の基準と統合を行うべきか。

【運 75】システムの廃棄　情報漏洩防止策を講ずること

案３　上記内容は契約締結時に確認する事項として、【統 22】の内容を見直し、【統 26】を廃止すべきか。

【統 22】

1.(6) 契約終了時の現状回復・新システム移行時の協力義務・データの返却・消去等

② 契約終了時における外部委託先によるデータの消去の実施（物理的消去、論理的消去等）、データ消去の実施時期や消去証明書の発行時期、文書等の回収など

案４　その他

外部の統制
クラウドサービス

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統 27	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. 金融機関等は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、統制対象クラウド拠点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。

（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であり、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、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とともに、定期的に監査を実施する必要がある。監査の実施にあたっては、金融機関みずからが監査を実施する方法以外にも、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し、その監査報告書を利用することも考えられる。なお、監査の実施にあたっては【監 1】を参照のこと。

3. 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ことが望ましい。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の利用を考慮することも考えられる。

コメント [A1]: 「特定システム」に限定しなくてもよいのではないか？そもそも「データの所在」を確認する負担を軽減（実効性を持たせるため）し、「統制対象クラウド拠点の把握」としているのだから、通常システムが適用されるとしてもよいのでは？

削除: 特定システムにおいて

コメント [A2]: FinTech 有識者検討会報告書よりクラウド固有のリスク管理策を基準化

※現在のクラウド基準上にある、クラウドサービス利用時の考慮点のうち、固有のリスク管理策として基準に追加するものは無い想定。

削除: するよう

削除: 特定システムで

削除: 特定システムで

削除: （※）

削除: ※

削除: 本社、営業所、

削除: 必ずしもデータセンターが候補とならない

削除: 特定システムでクラウドサービスを利用する場合

削除: 特定システムでクラウドサービスを利用する場合、一般的にクラウド事業者が採用する技術が先進的であることを考慮し、

削除: 必要となる能力を有した

削除: が望ましい

外部の統制
共同センター

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統 28	共同センターにおける有事の際の安全管理策を講ずること。

勘定系システムにおいて共同センターを利用する場合、迅速に初動対応が取れるよう有事発生に備えた適切な安全管理策を講ずること。

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、有事発生に備えて適切な安全管理策を講ずることが必要である。

　共同センターにおいては、有事の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。

　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有事の際の初動対応を決定する。
(2) 有事に初動対応を決定する金融機関等を事前に定めておく。
(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。

2. 安全管理策の検討にあたり、有事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、利用金融機関等もしくは委託先と共同で、人員計画を策定することが望ましい。

コメント [A1]: 外部委託有識者検討会報告書より。
ただし、「有事対応責任者の設置」については、基準として明記しない。

コメント [A2]: 共同センターの定義が具体的にされていないため、当基準の対象を明確化するため、「勘定系システムにおいて共同センターを利用する場合」と明記した。

削除: の

削除: にあたっては

削除: 関係

削除: できるよう

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

金融機関相互のシステム・ネットワークは、金融機関相互の金融取引の決済や CD･ATM オンライン提携などを行うえで、基幹インフラとしての機能を担っている。仮に当該システム・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、金融機関は適切なリスク管理を行うこと。

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

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

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

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

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

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

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

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

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

コメント [A1]: 【運 90-1】を変更

削除: 上

削除: 自ら

削除: こと

削除: 自ら

削除: 自ら

削除: こと

削除: 自ら

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

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

削除: およ

削除: こと

削除: 自ら

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

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

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

システム監査
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システム監査人がシステムの総合的な監査・評価を行い、経営層に監査結果を報告する必要がある。

なお、被監査部門としては、コンピュータシステムに関して、その開発及び運用を担当する部門（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もしくはそれに準じた監査を受けることが望ましい。特に、個人データを取り扱う情報システムの利用及び個人データへのアクセスの監視状況については、システム監査もしくはそれに準じた監査を受けることが必要である。

2. システム監査の実施手段の１つとして、内部者による監査に加え、外部の専門機関を活用することが望ましい。特に機微（センシティブ）情報を取り扱う場合は、外部の専門機関を活用することが望ましい。なお、機微（センシティブ）情報に該当する生体認証情報を取り扱う場合は、より客観性が求められることから、外部の専門機関を活用することが必要である。

3. システム監査実施結果による指摘事項については、システム監査部門と被監査部門の間で、事実確認、及び十分な意見交換を行い、問題があると認められた点について適切な改善を行うことが必要である。

4. システム監査を実施するにあたっては、当センター発刊の「金融機関等のシステム監査指針」、及び金融庁告示の「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」等を参照のこと。

5. システム監査人として、コンピュータシステムに精通した人材を確保する必要がある。

6. 金融機関等は、自らの業務処理を自社の責任で適正に行い、顧客データ等の重要情報を適切に管理するため、業務委託を行う場合には、当該委託業務が適切に運営されているかを検証することが必要である。

コメント [A1]: 【運 91】及び【運 112】の「基準小項目」を統合

コメント [A2]: 【運 91】及び【運 112】の「適用にあたっての考え方」を統合

コメント [A3]: 【運 91】1. 及び【運 112】1. を統合

コメント [A4]: 外部委託に関する有識者検討会報告書の提言に従い、「外部委託先」を含む記載に変更

コメント [A5]: 【運 91】2.

コメント [A6]: 【運 91】3.

コメント [A7]: 【運 91】4.

コメント [A8]: 【運 91】5.

コメント [A9]: 【運 91】6. 及び【運 112】2. 3. 4. を統合したうえで、整理・通則化

コメント [A10]: 【運 112】2. を通則化

削除: 必要がある

削除: 求められる

この点について、提出された情報のみで委託業務の適切性の検証が十分にできない場合は、外部委託先のオフィスや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、委託業務が再委託され、金融機関等がシステム監査を行う場合には、委託先同様、再委託先にも金融機関等の責任において監査を行う必要がある。

(1) 外部委託先の監査の方法としては以下の例がある。

① 委託元が委託先の監査を行う。

なお、共同センター等委託元が複数の場合は、複数の委託元が共同で監査を行い個別の監査を代替することも可能である。

② 委託先の内部監査部門、または委託先みずからが依頼する外部の第三者による監査（注）を受け、監査結果を委託元に報告する。

なお、共同センター等委託元が複数の場合は、監査結果を複数の委託元に報告することも可能である。

（注）第三者監査人を利用した監査人の選定は、顧客に対して責任を負う金融機関として、直接関わっていない者から見た際に、委託先との利益相反に疑義が生じるような外観を呈していない監査法人を選定することが必要である。そのために、委託元金融機関等は、監査の対象機関において、委託先の会計監査に従事していない監査法人を選定することが必要である。また、委託先の SOC2、IT7 号の保証業務に従事している監査法人を選定する場合には、委託先の SOC2、IT7 号の保証業務に従事していない監査責任者を選定することが必要である。

(2) 委託元金融機関等の監査等が実効的でない場合などには、第三者監査により代替することも可能である。その際に考慮すべき事項としては、以下の例がある。

① 検証項目については、外部委託先のリスク特性を踏まえた検証、委託元金融機関等の検証ニーズに則った検証を行うこと。なお、委託元金融機関等が単独、または他の金融機関と共同で第三者監査人と監査契約を締結し、外部委託先に対する監査を行う場合、既に外部委託先が受検している監査結果の内容を検証し、疑問点や不足する監査項目を中心に外部委託先に対する実地検証を行うことが有効である。

② 委託元金融機関等が、単独または共同で第三者監査人と外部委託先に対する監査に関する契約を締結し、外部委託先に対する監査を行う体制も選択可能とすること。

③ 委託元金融機関等が、第三者監査に関する費用を負担(または分担)する体制に移行すること。

④ 同一の監査責任者が長期間にわたり監査を行うことによる外観的独立性に対する疑念を払拭するため、適切なサイクルで交代すること。

⑤ 監査の品質を引き上げるために、SOC2 等、監査人側の損害賠償責任が契約書上明確化されている監査スキームを活用すること。

⑥ 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。

⑦ 第三者監査を効率的に行うため、複数の委託元金融機関等が共同で第三者に監査実施を委託すること。

⑧ 海外でのデータ保管時において、当該データセンターへの往査に必要な時間やコスト等を考慮すること。

コメント [A11]: 外部委託に関する有識者検討会報告書の提言に従い、「再委託先」を含む記載に変更

コメント [A12]: 【運 91】6.

削除: ようなもの

コメント [A13]: 外部委託に関する有識者検討会報告書の提言に従い、第三者監査人の選定に関する注釈を追記

コメント [A14]: 外部委託報告書の内容を精査し、見直しを行う予定。

コメント [A15]: 【運 112】3. を通則化

削除: ようなことが考えられる

削除: プロファイル

(3) 金融機関等において、業務の特性を十分に検討したうえで、委託する業務の重要度が高くないと判断し得る場合には、費用対効果を踏まえた管理策を講じることで、監査等に代替することも可能である。
例えば、以下のような方法が考えられる。

① その業務の必要とする監査等の項目をカバーし、内容が十分と判断できる第三者認証(注)のレポートの活用
（注）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)やPCI DSS level1、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、プライバシーマーク等がある。

② 外部委託先が準備するセキュリティに係るホワイトペーパーの確認またはレビュー

③外部委託先側が提供するリスク管理に必要なデータ抽出のツールを利用したデータ検証

コメント [A16]: 【運112】4. を通則化

削除: リスク管理に必要なデータ抽出のツールを

削除: から

削除: 準備・提供する。

運用管理
コンティンジェンシープランの策定

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 58	コンティンジェンシープランを策定すること。

削除: 運　65

不慮の災害や事故、あるいは障害等により重大な損害を被り、業務の遂行が困難になった場合の損害の範囲と業務への影響を極小化し、早期復旧を図るため、あらかじめコンティンジェンシープラン（緊急時対応計画）を策定しておくこと。

1. 不慮の災害や事故、あるいは障害時に、あらかじめ想定される複数のケースに応じてコンティンジェンシープランを策定しておくことが必要である。
なお、集中豪雨、降雪等による交通遮断や感染症のパンデミック発生などから生じる職員不在等の不測の事態についても、要員確保の観点から考慮することが必要である。
また、障害等が発生した時期、曜日、時間帯やシステム環境の違いにより対応する範囲や方法が異なる場合には、これらの対応を考慮する必要がある。
特に、広範囲に重大な影響を及ぼすような資金決済システム等の障害については、時限性や社内関連システム及び社外への影響等にも留意する必要がある。

本基準におけるコンティンジェンシープランとは、金融機関等のコンピュータシステムが、不慮の災害や事故・犯罪、障害等により重大な損害を被り業務の遂行が果たせなくなった場合に、各種業務の中断の範囲と期間を極小化し、迅速かつ効率的に必要な業務の復旧を行うためにあらかじめ策定された緊急時対応計画のことである。（「Ⅱ.1(3)⑤コンティンジェンシープランの策定」参照）

想定される緊急事態としては、以下の例がある。
(1) コンピュータセンター、本部・営業店等の全面被災、一部被災
(2) コンピュータ装置の破壊、損傷
(3) 端末機器等の破損、損傷
(4) 関連設備（電源、空調、給排水設備等）の破壊、損傷
(5) 回線の切断、通信設備の損傷
(6) 公共インフラの障害（停電、断水、交通遮断等）
(7) ソフトウェアの障害
(8) サイバー攻撃

また、コンティンジェンシープランの策定に際して考慮すべき内容としては、以下の例がある。
(1) 緊急事態を想定し、自社の業務や各種施設に対してどのような影響が起こるかを評価す

る。
(2) 緊急時における業務の継続の優先順位を評価する。
(3) 被災拠点及び対策本部における緊急時対応組織の体制（コンティンジェンシープラン発動権限も含む）や要員等を明確にする。
(4) 緊急事態発生時における、顧客・職員の安全確保、資産の保全、被災状況の把握等の措置を明確にする。
(5) 業務、顧客サービスの中断あるいは、中断による損失を極小化するために、業務の通常的な継続が困難な緊急事態のもとで、重要と判断される業務の暫定的継続を図るために必要な措置を明確にする。
(6) 早期に事態を収拾して、平常業務への復旧を図るために必要な措置を明確にする。
(7) 緊急時における要員の移動、機器等の物資の搬送手段及びルートを決めておく。
(8) プランの維持管理体制の確立を行い、定期的な訓練の実施とその結果に基づくプランの見直し等の維持管理を明確にする。
(9) 業務が外部委託されている場合は、委託先や再委託先（再委託には二以上の段階にわたる再委託を含む）の役割等も明確にする。

設備及び技術面の復旧策、並びに災害時・障害時等に備えた運用訓練については、以下の基準項目を参照のこと。また、コンティンジェンシープランを変更する際も、必要に応じて以下の基準項目を参照のこと。
(1) 環境　【設 1】
(2) 周囲　【設 2～設 4、設 7～設 9】
(3) 構造　【設 10～設 13、設 31～設 36】
(4) 開口部　【設 14、設 17～設 19、設 28～設 30】
(5) 内装等　【設 20、設 21】
(6) 位置　【設 22、設 25、設 26】
(7) 設備　【設 37～設 44】
(8) コンピュータ機器、什器、備品　【設 48、設 50、設 51】
(9) 電源室、空調機械室　【設 52、設 54～設 60】
(10) 電源設備　【設 62～設 71】
(11) 空調設備　【設 74～設 79】
(12) 監視制御設備　【設 80、設 81】
(13) 回線関連設備　【設 82、設 83、設 83-1】
(14) ハードウェアの予備　【技 2～技 6】
(15) 障害の早期回復　【技 22～技 24】
(16) 災害時対策　【技 25】
(17) 教育、訓練　【運 80～運 84】

なお、コンティンジェンシープランの策定に関する詳細内容については、当センター発刊の『金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書』を参照のこと。

2. 上記、コンティンジェンシープランの策定に際して考慮すべき内容(1)～(9)のうち、(3)～(6)に揚げた内容については手順書として文書化することが必要である。

3. コンティンジェンシープランが策定された後においても、適宜見直しをすることが必要である。見直しを行う際は、事務手続き等の変更点にも考慮することが必要である。

   見直しが必要となる契機としては、以下の例がある。
   (1) 重要な業務についてその内容に変更が生じた場合
   (2) 従来、コンティンジェンシープランでは考慮していなかった業務についてその重要度が高まった場合
   (3) 上記業務遂行の前提となる組織や拠点施設、インフラ、システム構成等の条件に変更が生じた場合
   (4) 政府の取組みやガイドライン等が変更された場合

4. 組織図や緊急連絡網等については、最新の情報を維持するとともに、組織内に周知することが必要である。

5. コンティンジェンシープランの策定及び重要なプラン内容の見直しを行うにあたっては、経営層の承認を得ることが必要である。

6. コンティンジェンシープランは、対策本部、各拠点、バックアップサイトにおいて、必要な部分が常時保管され、全役職員が必要な部分を閲覧できる状態を保つことが必要である。

7. 障害時・災害時等におけるシステムの復旧やバックアップサイトへの切替えを行う際は、セキュリティ管理のレベルが低下するおそれがある。当該事象が発生した場合のセキュリティについても通常時と同等のレベルを維持することが必要である。

8. 障害・災害によって生じる可能性のある損害賠償責任、逸失利益、業務継続に要する費用等に備えて、保険の適用を検討することが望ましい。

【資料３－１】
平成 29 年 9 月 12 日
公益財団法人 金融情報システムセンター

「読みやすさ対応」統制基準の一部再編・見直しについて

前回の専門委員会「【議案３】安全対策基準「読みやすさ」対応について」（前回【資料３－２】のⅣ）を踏まえ、以下のとおり統制基準の再編を行うとともに、併せて内容を見直す。

※添付資料
【資料３－２】改訂原案（基準本文）
【資料３－３】統制基準再編（内容一覧）
【資料３－４】新基準構成案（再編後）

Ⅰ.「セキュリティ関連文書」に関する基準の見直し

セキュリティ関連文書の階層としては、下表に記載した４種類に分類（１が最上位）できるが、それぞれの関連性（上下関係）が明確になっていない点、および記載内容が重複している点を解消する。

No	対象	現行基準	再編後基準	再編・見直し内容
1	システムリスク管理方針等	－	【統 1】（【統 2】は【統 1】に統合）	安全対策に係る重要事項を定めたセキュリティポリシーとセキュリティスタンダードの策定について記載。その際、上位規程であるシステムリスク管理方針との関連についても追記。
2	セキュリティポリシー・セキュリティスタンダード	【統 1】【統 2】		
3	業務規則	【統 4】	【統 4】	セキュリティポリシー・スタンダード等を踏まえた、システムを管理するための業務規則の策定について記載
4	マニュアル・手順書	【統 1】【実 4】	【実 4】	業務規則の内容を、実行レベルまで具体化した、マニュアル・手順書の策定について記載（変更なし）

Ⅱ.「システム開発計画」に関する基準の見直し

現状では、個別システム開発計画はシステム中期計画を踏まえ策定すべきとの記載はあるが、システム中期計画の策定に関する記載はない。

システムの安全・安定稼働を実現するためには、中長期的視点に立って開発・維持管理を計画する必要があることから、システム中期計画の策定についての基準を新設し、その上で各計画の関連性（上下関係）を明確にする。

【資料３－１】
平成 29 年 9 月 12 日
公益財団法人 金融情報システムセンター

No	対象	現行基準	再編後基準	再編・見直し内容
1	中期経営計画	－	基準を新設し【統 2】とする。	・システム中期計画の策定について記載。 ・システム中期計画とその上位にある中期経営計画の関連について記載。
2	システム中期計画	－		
3	システム開発計画	【統 3】	【統 3】	変更なし。

Ⅲ．今後の予定

本日ご説明した内容について、9/22（金）までに事後意見をいただきたい。事後意見をもとに基準原案の修正を行い、次回委員会にて修正原案を提示する予定である。

日程（予定）	内容
9 月 12 日（火）	第 56 回安全対策専門委員会審議（本日原案提示）
9 月 22 日（金）	第 56 回専門委員会事後意見の締切
10 月 17 日（火）	第 57 回安全対策専門委員会審議（修正原案提示）

以　上

内部の統制
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、安全対策実施のための組織体制及び関係者の役割、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、策定した規程を必要に応じて改訂すること。

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、保護する理由と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. 全社（もしくは全組織）の安全対策の方針や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。

3. 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。

4. 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【運 80】を参照のこと。

5. 環境変化に対応し、当該規程を適宜見直すことが必要である。見直す場合には当該規程の策定権限者の承認を得ることが必要である。

コメント [A1]: 再編・内容見直し

コメント [A2]: 上位規程との関連性について追記

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) 業務組織や人員・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や犯罪の発生
(8) セキュリティ関連文書に定められた事項の遵守状況の確認結果

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。

内部の統制
方針・計画

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統 2 【新設】	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。

コメント [A3]: 新設

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され、経営層の承認を得ることが必要である。

   中期システム計画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と達成目標
   (2) 基幹業務のオンラインコンピュータ・システムシステムの方向性
   (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

3. 個別のシステム計画は、中期システム計画との整合性を考慮して策定されることが必要である。

内部の統制
方針・規定

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、中長期のシステム化計画と整合性が取れており、かつ内外の技術調査を実施していること、また開発責任者（システムを企画、開発する部門の長）の承認を得ていること。

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

2. 幅広く情報技術の適用を検討するため、開発計画を策定するにあたっては、内外の情報技術を調査することが望ましい。
   なお、開発を外部に委託する場合には、採用技術の正当性について委託先から十分な説明を受けることが必要である。

   調査のポイントとしては、以下の例がある。
   (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のシステム化計画に基づいていること、採用技術も適切なことを確認し、計画を実行に移すためには開発責任者が承認することが必要である。

コメント [A4]: 変更なし

内部の統制
組織体制

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

統 4	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と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やセキュリティスタンダード等と整合をとって、業務の各組織における責任と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、職掌ならびに責任と権限を定めたものを指している。また、手順書やマニュアルは、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【運 11～13】
   (2) コンピュータシステムの通常時、障害時・災害時運用【運 14～24、運 31、運 32、運 54～65】
   (3) コンピュータ処理に係わる業務の通常時、障害時・災害時運用【運 37～50、運 53】
   (4) データ、プログラムおよびドキュメントの管理【運 25～30、運 33～36】
   (5) カード管理【運 51、運 52】
   (6) システム開発・変更【運 66～75】
   (7) 電源設備、空調設備、防災設備、防犯設備の管理【運 76～78】
   (8) 防犯・警備【運 4～9】
   (9) 監視【運 79】

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

コメント [A5]: 内容見直し

コメント [A6]: 上位規程との関連性について追記

運用管理
マニュアルの整備

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実４	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見直しを行い、常に最新の状態にしておくことが必要である。

   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 【運 16～18】
   (2) オペレーション管理 【運 19～23】
   (3) データファイル管理 【運 25～27】
   (4) プログラムファイル管理 【運 28、運 29】
   (5) ドキュメント管理 【運 33、運 34】
   (6) 帳票管理 【運 35、運 36】
   (7) 出力管理 【運 37】
   (8) カード管理 【運 51、運 52】
   (9) 資源管理 【運 54】
   (10) 外部接続管理 【運 55、運 56】
   (11) 機器の管理 【運 57～59】
   (12) 運行監視 【運 60】

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

コメント [A7]: 変更なし

通常時マニュアルの整備に係わる具体的な対策としては、以下の例がある。

(1) 通常時マニュアルを整備し、遵守について関連部門に周知徹底させる。

(2) 追加・変更等が発生した場合は、定められた手続きに従い更新する。

また、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ついて、その基準・手続き等

②特定の事務処理について、その具体的な流れ・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) その他例外規定等

【資料３－３】
平成29年9月12日
公益財団法人　金融情報システムセンター

【統1】	原文	改訂案	改訂内容
基準小項目	**セキュリティ管理方法を具体的に定めた文書を整備すること。**	**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。**	安全対策実施の根拠となる規程類の整備に関する基準項目とする。
適用にあたっての考え方	セキュリティ管理を適切に行うため、セキュリティ管理の具体的手順、責任等を明確にした文書を整備すること。	システムの安全対策を適切に実施するため、安全対策実施のための組織体制及び関係者の役割、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、策定した規程を必要に応じて改訂すること。	他の基準と記載内容の整合性をとるため、規程の「策定」（統1【運1】）に加えて、「改訂」（統2【運2】）の内容を含める。
基準本文（解説） 【統1】	1. セキュリティ管理を適切に行うためには、会社（もしくは組織）の情報資産を適切に保護するための基本方針である「セキュリティポリシー（基本方針）」と、これを実行に移すための具体的対策を記述した「セキュリティスタンダード（自社の安全対策基準）」及び「マニュアル」や「手順書」等のセキュリティ関連文書を整備することが必要である。セキュリティ関連文書は以下のように分類される。 (1) セキュリティポリシー(基本方針) 全社統一の基本方針として、保護されるべき情報資産、保護する理由と責任の所在を定めたもの。 (2) セキュリティスタンダード(自社の安全対策基準) セキュリティポリシー(基本方針)を実行に移すための具体的な対策であり、社内部門別に作成してもよい。 (3) マニュアルや手順書 セキュリティポリシー（基本方針）及びセキュリティスタンダード（自社の安全対策基準）を具体的な業務の手順に反映したものであり、社内部門別や個々のシステム別のものであってもかまわない。	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、保護する理由と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。	【一部削除】 原文の1. および1(3)の、マニュアルや手順書については、（実4【運14】）「通常時マニュアルを整備すること。」で対象としており、本基準の対象外とする。（削除）
	なお、全社（もしくは全組織）のセキュリティ管理の方針や対策に重大な影響を与えるセキュリティ関連文書の策定にあたっては、経営層が指示し、承認すること。	2. 全社（もしくは全組織）の安全対策の方針や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	【継承】 同内容を継承する。
		3. 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。	【追加】 上位規程である「システムリスク管理方針」についての記載を追記する。
	2. セキュリティ関連文書は、全役職員(外部要員を含む)に対して、組織内における安全対策に関する役割と責任に応じて適切に周知、教育する必要がある。セキュリティ教育については【運80】を参照のこと。	4. 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【運80】を参照のこと。	【継承】 同内容を継承する。
	3. セキュリティポリシーの文書に定めるべき事項は主に以下の3点である。 (1) 保護されるべき情報資産 (2) 保護を行うべき理由 (3) 保護にあたっての責任の所在		【削除】 改訂案の1(1)に記載しており、重複しているため削除する。
	4. セキュリティ関連文書の整備を行ううえでの留意事項として、以下のようなものがある。 (1) セキュリティ管理の実施計画策定は、コンピュータシステムで扱う情報の重要性を判断して、コンピュータシステムが提供しているサービスの優先順位を決定することから始まる。このためには取り扱っている情報をすべて洗い出し、会社(もしくは組織)として情報を保護するレベルを決定することが必要である。 重要な情報資産についてはセキュリティポリシーに則って、機密性、完全性、可用性の観点から、その重要性に応じた適切な保護、管理を行うことが必要である。 また、セキュリティを確保するための手段として保険の適用を検討することが望ましい。 (2) 機器及びソフトウェアを導入あるいは更新する場合には、セキュリティ機能がセキュリティポリシーに適合していることを確認することが必要である。 (3) セキュリティを確保するためには、システムを計画する段階からセキュリティ対策を考慮しておくことが必要である。 システム計画時のセキュリティ対策の考慮については、以下の基準項目を参照のこと。 ・必要となるセキュリティ機能を取り込むこと【技8】 (4) セキュリティ管理を適切に行うにあたって、セキュリティに関する法令等も考慮する必要がある。 (5) セキュリティポリシーを策定する際は、社内各部門の意見・状況を把握し、適切に反映することが望ましい。		【削除】 原文の4(1)(2)(3)は、以下基準と内容が重複しているため、削除する。 ※・（実18【技8】）「必要となるセキュリティ機能を取り込むこと。」 ・（実99【技9】）「設計段階でのソフトウェアの品質を確保すること。」 原文の4(4)、4(5)については、改訂案の1(1)記載の『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』により詳細な内容が記載されており、他にも留意すべき事項は多数あることから、継承は不要と判断した。
	(注) ・機密性(Confidentiality)……アクセスを許されていない者から守ること ・完全性(Integrity)……改ざん等されないように完全な形態で保持すること ・可用性(Availability)……いつでも利用できるように保持すること		【削除】 ・（実18【技8】）に、同様の解説があるため削除する。 ※（実18【技8】）「必要となるセキュリティ機能を取り込むこと。」
	5. セキュリティポリシーを策定するにあたっては、当センター発刊の『金融機関等におけるセキュリティポリシー策定のための手引書』等を参照のこと。		【継承】 改訂案の1(1)に記載する。
基準本文（解説） 【統2】 ※【統1】に統合	1. セキュリティ管理を適切に行うためには、管理や運用方法などを具体的に定めたセキュリティ関連文書が業務の実態にあっていなければならない。この文書の見直しのきっかけには以下のようなものがあり、これらに応じて改訂する必要がある。 なお、全社(もしくは全組織)のセキュリティ管理の方針や対策に重大な影響を与えるセキュリティ文書の改訂にあたっては、経営層の承認を得ること。 ・組織の運営の変化 ・ビジネス環境の変化 ・法令の制定、改正 ・情報・通信技術の進歩 ・業務組織や人員・就業場所の変化 ・扱う情報資産に関する変化 ・セキュリティに関する事故や犯罪 ・セキュリティ関連文書に定められた事項の遵守状況の確認結果 なお、共通的なものについては、主管部署等で改訂したものを全社に配布することで対応すればよい。	5. 環境変化に対応し、当該規程を適宜見直すことが必要である。見直す場合には当該規程の策定権限者の承認を得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。 ・組織運営の変化 ・ビジネス環境の変化 ・法令の制定、改正 ・情報・通信技術の進歩 ・業務組織や人員・就業場所の変化 ・扱う情報資産の変化 ・セキュリティに関する事故や犯罪の発生 ・セキュリティ関連文書に定められた事項の遵守状況の確認結果	【一部削除し、統1に統合】 原文の「なお、共通的なものについては、主管部署等で改訂したものを全社に配布することで対応すればよい。」は、全社統一の文書に関する記載ではないため、削除する。
	2. 対象となるのは以下のような文書であるが、場合によってはこれらの基本となっているセキュリティポリシー(基本方針)の見直しが必要なこともある。 ・セキュリティスタンダード(自社の安全対策基準) ・マニュアルや手順書		【一部削除し、統1に統合】 改訂案の1に記載する。マニュアルや手順書については、（実4【運14】）「通常時マニュアルを整備すること。」で対象としており、本基準の対象外とする。（削除）
	3. 合併等により異なるセキュリティポリシーを持つ複数の企業がひとつの企業となる場合は、システム統合に先立ち統合金融機関の間でセキュリティポリシーの違いを認識し、見直すことが必要である。	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。	【継承し、統1に統合】 同内容を継承する。

【資料３－３】
平成29年9月12日
公益財団法人　金融情報システムセンター

【統4】	原文	改訂案	改訂内容
基準小項目	**各種規定を整備すること。**	**各種業務の規則を整備すること。**	【統1】の「規程」、【実4】の「マニュアル」と明確に区別するため、「規則」とした。
適用にあたっての考え方	コンピュータシステムを円滑かつ適正に運用、管理するため、防災、防犯、業務の各組織における責任と権限を明確にした規定を整備すること。	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と権限を明確にした規則を整備すること。	防災、防犯を削除。業務の一部に含める。
基準本文（解説） 【統4】	1. ここでいう規定とは、防災、防犯、業務の各組織に関する事務分掌、職掌ならびに責任と権限を定めたものを指しており、以下の内容を含んだ各種規定を定めることが必要である。 (1) 入退管理 (2) コンピュータシステムの通常時、障害時・災害時運用 (3) コンピュータ処理に係わる業務の通常時、障害時・災害時運用 (4) データ、プログラムおよびドキュメント(サーバー、パソコン、フロッピーディスク、CD-ROM等に蓄積されたものも含む)の管理 (5) カード管理 (6) システム開発・変更 (7) 電源設備、空調設備、防災設備、防犯設備の管理 (8) 防犯・警備 (9) 監視	1. 上位規程であるセキュリティポリシーやセキュリティスタンダード等と整合をとって、業務の各組織における責任と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、職掌ならびに責任と権限を定めたものを指している。 また、手順書やマニュアルは、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【運11～13】 (2) コンピュータシステムの通常時、障害時・災害時運用【運14～24、運31、運32、運54～65】 (3) コンピュータ処理に係わる業務の通常時、障害時・災害時運用【運37～50、運53】 (4) データ、プログラムおよびドキュメント(電子媒体)の管理【運25～30、運33～36】 (5) カード管理【運51、運52】 (6) システム開発・変更【運66～75】 (7) 電源設備、空調設備、防災設備、防犯設備の管理【運76～78】 (8) 防犯・警備【運4～9】 (9) 監視【運79】	【継承】【追加】 同内容を継承する。 また、上位規程との関係性を追記し、下位文書である手順書やマニュアルとの関係性も追記する。
	2. データ、プログラムおよびドキュメントの管理については、顧客データや秘密鍵等の重要で機密を要するデータの取扱いに関する規定を必要に応じて定めることが必要である。	2. データ、プログラムおよびドキュメントの管理については、顧客データや秘密鍵等の重要で機密を要するデータの取扱いに関する規則を必要に応じて定めることが必要である。	【継承】 同内容を継承する。
	3. 規定の内容については、以下の基準項目を参照のこと。 (1) 入退管理【運11～13】 (2) コンピュータシステムの通常時、障害時・災害時運用【運14～24、運31、運32、運54～65】 (3) コンピュータ処理に係わる業務の通常時、障害時・災害時運用【運37～50、運53】 (4) データ、プログラムおよびドキュメントの管理【運25～30、運33～36】 (5) カード管理【運51、運52】 (6) システム開発・変更【運66～75】 (7) 電源設備、空調設備、防災設備、防犯設備の管理【運76～78】 (8) 防犯・警備【運4～9】 (9) 監視【運79】		【一部削除】 1と内容が重複している。1に各々の参照先の基準番号を記載する。

統2（新設）	原文	改訂案	内容
基準小項目		**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。**	システムのリスク特性を評価する際には、現状のリスクを評価することに加え、中長期的視点にたって、システムの将来形を考慮し、リスクを評価することが重要であることから、「中期システム計画 の策定」を基準として新設する。
適用にあたっての考え方		有効なシステムを長期的かつ安定的に維持するために、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。	
基準本文（解説）		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「中期システム計画」という）を策定することが必要である。	【追加】 中期経営計画に沿った「中期システム計画」を中長期的視点にたって策定することについて記載する。
		2. 中期システム計画は、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され、経営層の承認を得ることが必要である。 中期システム計画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と達成目標 (2) 基幹業務のオンラインコンピュータ・システムシステムの方向性 (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を含む経営資源	【追加】 業務の継続性の観点から必要となる考慮事項を記載したもの。システム対応には時間を要することから、システムを安定的に運用するためには、先を見越した対応が必要となる。 また、「金融機関における外部委託に関する有識者検討会」にて提言された「人材の把握、確保」を踏まえ、「人材を含む経営資源」も考慮事項とする。
		3. 個別のシステム計画は、中期システム計画との整合性を考慮して策定されることが必要である。	【追加】 個別のシステム計画（【統3】）との関連性を記載する。

【資料３－４】
平成29年９月12日
公益財団法人　金融情報システムセンター

新基準構成案（再編後）

構成	修正案　基準大項目	修正案　基準中項目	新基準番号（暫定）	基準小項目	旧基準番号	基礎基準 ○：当初案 △：追加案	適用区分				
							建屋、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
Ⅰ　統制基準	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	○	◎				
			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	○	◎				
		(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	○	◎				
			統6	セキュリティ管理体制を整備すること。	運3	○	◎				
			統13	サイバー攻撃対応態勢を整備すること。	運113	○	◎				
			統7	システム管理体制を整備すること。	運4	○	◎				
			統8	データ管理体制を整備すること。	運5	○	◎				
			統9	ネットワーク管理体制を整備すること。	運6	○	◎				
			統12	業務組織を整備すること。	運9	○		◎	◎		
			統10	防災組織を整備すること。	運7	○		◎	◎		
			統11	防犯組織を整備すること。	運8	○		◎	◎		
			統4	各種業務の規則を整備すること。	運10	○	◎				
		(3)　管理状況の評価	統5	セキュリティ遵守状況を確認すること。	運10-1	○	◎				
		(4)　人材（要員・教育）	統14	セキュリティ教育を行うこと。	運80	○	◎				
			統15	要員に対するスキルアップ教育を行うこと。	運81	○	◎				
			統17	障害時・災害時に備えた教育・訓練を行うこと。	運83	○	◎				
			統18	防災・防犯訓練を行うこと。	運84	○	◎				
			統19	要員の人事管理を適切に行うこと。	運85	○	◎				
			統20	要員の健康管理を適切に行うこと。	運86	○	◎				
	2　外部の統制	(1)　外部委託管理	統21	システムの開発や運用、サービス利用等で外部委託を行う場合は、事前に目的や範囲を明確にすること。	運108他		◎				
			統22	安全対策に関する項目を盛り込んだ委託契約を締結すること。	運109他		◎				
			統23	外部委託先（再委託先を含む）の要員にルールを遵守させ、その遵守状況を管理、検証すること。	運89		◎				
			統24	外部委託における業務組織の整備と業務の管理、検証を行うこと。	運90		◎				
			統25	外部委託にあたって、データ漏洩防止策を講ずること。	運110		◎				
			統26	外部委託契約終了時の情報漏洩防止策を講ずること。	運111		◎				
		(2)　クラウドサービス	統27	重要なシステムにおけるクラウドサービス利用時の管理策を講ずること。 →【実144】に移動			◎				
		(2)　共同センター	統28	共同センターにおける有事の際の安全管理策を講ずること。	新設	○	◎				
		(3)　金融機関相互のシステム・ネットワークのサービス	統29	金融機関相互のシステム・ネットワークのサービス利用にあたっては、適切なリスク管理を行うこと。	運90-1	○	◎				
Ⅱ　実務基準	1 情報セキュリティ	(1)　データ保護	実116	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	○	◎				
			実117	相手端末確認機能を設けること。	技27	○	○				
			実118	蓄積データの漏洩防止策を講ずること。	技28	○	○				
			実119	伝送データの漏洩防止策を講ずること。	技29	○	○				
			実121	ファイルに対するアクセス制御機能を設けること。	技31	○	◎				
			実122	不良データ検出機能を充実すること。	技32	△	◎				
			実123	伝送データの改ざん検知策を講ずること。	技33	△	○				
		(2)　不正使用防止	実125	本人確認機能を設けること。	技35	○	◎				
			実126	生体認証の特性を考慮し、必要な安全対策を検討すること。	技35-1	○	◎				
			実127	IDの不正使用防止機能を設けること。	技36	○	◎				
			実128	アクセス履歴を管理すること。	技37	○	◎				
			実129	取引制限機能を設けること。	技38	△	◎				
			実130	事故時の取引禁止機能を設けること。	技39	△	◎				
			実133	電子化された暗号鍵を蓄積する機器、媒体、またはそこに含まれるソフトウェアには、暗号鍵の保護機能を設けること。	技42		◎				
		(3)　外部ネットワークからの不正アクセス防止	実135	外部ネットワークからの不正侵入防止機能を設けること。	技43	○	◎				
			実136	外部ネットワークからアクセス可能な接続機器は必要最小限にすること。	技44	○	◎				
		(4)　不正検知策	実137	不正アクセスの監視機能を設けること。	技45	○	◎				
			実138	異常な取引状況を把握するための機能を設けること。	技46		◎				
			実139	異例取引の監視機能を設けること。	技47		◎				
		(5)　不正発生時の対応策	実140	不正アクセスの発生に備えて対応策、復旧策を講じておくこと。	技48	○	◎				
		(6)　不正プログラム対策	実141	コンピュータウイルス等不正プログラムへの防御対策を講ずること。	技49	○	◎				
			実142	コンピュータウイルス等不正プログラムの検知対策を講ずること。	技50	○	◎				
			実143	コンピュータウイルス等不正プログラムによる被害時対策を講ずること。	技51	○	◎				
	2　システム運用共通	(1)　マニュアルの整備	実4	通常時マニュアルを整備すること。	運14	△	◎				
			実5	障害時・災害時マニュアルを整備すること。	運15	○	◎				
		(2)　アクセス権限の管理	実6	各種資源、システムへのアクセス権限を明確にすること。	運16	○	◎				
			実7	パスワードが他人に知られないための措置を講じておくこと。	運17	○	◎				
			実8	各種資源、システムへのアクセス権限の付与、見直し手続きを明確化すること。	運18	○	◎				
		(3)　データ管理	実15	データファイルの授受・管理方法を定めること。	運25	○	◎				
			実16	データファイルの修正管理方法を明確にすること。	運26	△	◎				
			実33	暗号鍵の利用において運用管理方法を明確にすること。	運43	○	◎				
		(4)　オペレーション習熟	統16	オペレーション習熟のための教育および訓練を行うこと。	運82	○	◎				
		(5)　コンピュータウイルス対策	実20	コンピュータウイルス対策を講ずること。	運30	○	◎				
		(6) 外部接続管理	実48	接続契約内容を明確にすること。	運55	○	◎				
			実49	外部接続における運用管理方法を明確にすること。	運56	○	◎				
	3　運行管理	(1)　オペレーション管理	実9	オペレータの資格確認を行うこと。	運19	○		◎			
			実10	オペレーションの依頼・承認手続きを明確にすること。	運20	△		◎			
			実11	オペレーション実行体制を明確にすること。	運21	△		◎			
			実12	オペレーションの記録、確認を行うこと。	運22	△		◎			
			実13	クライアントサーバー・システムにおける作業の管理を行うこと。	運23	△		○	○		
		(2)　データファイル管理	実17	データファイルのバックアップを確保すること。	運27	○	◎				
		(3)　プログラムファイル管理	実18	プログラムファイルの管理方法を明確にすること。	運28	△	◎				
			実19	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	○	◎				
		(4)　ネットワーク設定情報管理	実21	ネットワークの設定情報の管理を行うこと。	運31	△	◎				
			実22	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	○	◎				
		(5)　ドキュメント管理	実23	ドキュメントの保管管理方法を明確にすること。	運33	△	◎				
			実24	ドキュメントのバックアップを確保すること。	運34	○	◎				
		(6) 運行監視	実53	システムの運行状況の監視体制を整備すること。	運60	○	◎				
	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	△	◎				
		(2) 機器の管理	実59	ハードウェア、ソフトウェアの管理を行うこと。	運66	△	◎				
			実50	機器の管理方法を明確にすること。	運57	○		◎	◎		
			実51	ネットワーク関連機器の保護措置を講ずること。	運58	△		○	○	○	
			実52	機器の保守方法を明確にすること。	運59			◎	◎		
			実92	機器の予防保守を実施すること。	技1			◎	◎		
		(3)　コンピュータ関連設備の保守管理	実69	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	△		◎	◎		
			実70	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	△		◎	◎		
			実71	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	△		◎	◎		
		(4)　入退館（室）管理	実1	入館（室）の資格付与、及び鍵の管理を行うこと。	運11	○		◎	◎		
			実2	入退館管理を行うこと。	運12	○		◎			
			実3	入退室管理を行うこと。	運13	○		◎	◎		
			実54	入室後の作業を管理すること。	運61	○		◎	◎		

【資料３－４】
平成29年９月12日
公益財団法人　金融情報システムセンター

新基準構成案（再編後）

構成	修正案　基準大項目	修正案　基準中項目	新基準番号（暫定）	基準小項目	旧基準番号	基礎基準 ○：当初案 △：追加案	適用区分 建屋、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) 監視	実72	各種設備の監視体制を整備すること。	運79	△		◎	◎		
	5 システムの利用	(1) 取引の管理	実28	各取引の操作権限を明確にすること。	運38	△		◎	◎		
			実29	オペレータカードの管理を行うこと。	運39			◎	◎		
			実30	取引の操作内容を記録・検証すること。	運40	△		◎	◎		
			実31	顧客からの届出の受付体制を整備し、事故口座の管理を行うこと。	運41		◎				
		(2) 入出力管理	実14	データの入力管理を行うこと。	運24	△		◎	◎		
			実27	出力情報の作成、取扱いについて、不正防止および機密保護対策を講ずること。	運37	○	◎				
		(3) 帳票管理	実25	未使用重要帳票の管理方法を明確にすること。	運35		◎				
			実26	重要な印字済帳票の取扱方法を明確にすること。	運36	○	◎				
		(4) 厳正な本人確認の実施	実34	口座開設等を行う場合は、本人確認を行うこと。	運44	△			◎		
		(5) 顧客データ保護	実45	顧客データの保護策を講ずること。	運53	○	◎				
			実46	生体認証における生体認証情報の安全管理措置を講ずること。	運53-1	○	◎				
	6 緊急時の対応	(1) 障害時・災害時対応策	実55	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	○	◎				
			実56	障害時・災害時復旧手順を明確にすること。	運63	○	◎				
			実57	障害の原因を調査・分析すること。	運64	△	◎				
		(2) コンティンジェンシープランの策定	実58	コンティンジェンシープランを策定すること。	運65	○	◎				
		(3) バックアップサイト	実115	バックアップサイトを保有すること。	技25			○			
	7 システム開発・変更	(1) システム開発・変更管理	実60	システムの開発・変更手順を明確にすること。	運67	△	◎				
			実61	テスト環境を整備すること。	運68	○	◎				
			実62	本番への移行手順を明確にすること。	運69	△	◎				
		(2) システムドキュメント管理	実63	システムドキュメントの作成手順を定めること。	運70		◎				
			実64	システムドキュメントの保管管理方法を明確にすること。	運71		◎				
		(3) パッケージの導入	実65	パッケージの評価体制を整備すること。	運72		◎				
			実66	パッケージの運用・管理体制を明確にすること。	運73		◎				
		(4) システムの廃棄	実67	システムの廃棄計画、手順を策定すること。	運74	○	◎				
			実68	システム廃棄時の情報漏洩防止対策を講ずること。	運75	○	◎				
	8 システムの信頼性向上対策	(1) ハードウェアの予備	実93	本体装置の予備を設けること。	技2			◎	◎		
			実94	周辺装置の予備を設けること。	技3			◎	◎		
			実95	通信系装置の予備を設けること。	技4			◎	◎		
			実96	回線の予備を設けること。	技5			○	○		
			実97	端末系装置の予備を設けること。	技6			◎	◎		
		(2) ソフトウエアの品質向上対策	実98	必要となるセキュリティ機能を取り込むこと。	技8	△	◎				
			実99	設計段階でのソフトウェアの品質を確保すること。	技9	△	◎				
			実100	プログラム作成段階での品質を確保すること。	技10	△	◎				
			実101	テスト段階でのソフトウェアの品質を確保すること。	技11	△	◎				
			実102	プログラムの配布を考慮したソフトウェアの信頼性を確保すること。	技12	△	◎				
			実103	パッケージ導入にあたり、ソフトウェアの品質を確保すること。	技13	△	◎				
			実104	定型的変更作業時の正確性を確保すること。	技14	△	◎				
			実105	機能の変更、追加作業時の品質を確保すること。	技15	△	◎				
			実120	ファイルに対する排他制御機能を設けること。	技30		◎				
			実124	ファイル突合機能を設けること。	技34	△	◎				
		(3) 運用時の信頼性向上対策	実106	オペレーションの自動化、簡略化を図ること。	技16	△	○				
			実107	オペレーションのチェック機能を充実すること。	技17	△	◎				
			実108	負荷状態の監視制御機能を充実すること。	技18	△	◎				
		(4) 障害の早期発見・回復機能	実110	システム運用状況の監視機能を設けること。	技20	△	◎				
			実111	障害の検出および障害箇所の切り分け機能を設けること。	技21		◎				
			実112	障害時の縮退・再構成機能を設けること。	技22		◎				
			実113	障害時の取引制限機能を設けること。	技23		◎				
			実114	障害時のリカバリ機能を設けること。	技24	△	◎				
	9 個別業務・サービス	(1) カード取引サービス	実42	カードの管理方法を明確にすること。	運51	○		◎	◎	◎	
			実43	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				◎	◎	
			実35	CD・ATM等の機械式預貯金取引における正当な権限者の取引を確保すること。	運44-1		◎				
			実44	指定された口座のカード取引監視方法を明確にすること。	運52			◎	◎	◎	
			実131	カードの偽造防止対策のための技術的措置を講ずること。	技40	△		○	○	○	
		(2) インターネット・モバイルサービス	実84	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	○					◎
			実85	インターネット・モバイルサービスの不正使用を早期発見すること。	運104	○					◎
			実86	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						○
			実87	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						◎
			実88	インターネットやモバイル等を用いた金融サービスの運用管理方法を明確化すること。	運106						◎
		(3) 渉外端末の管理	実41	渉外端末の運用管理方法を明確にすること。	運50	○			◎		
		(4) CD・ATM等及び無人店舗の管理	実36	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				◎	◎	
			実37	無人店舗の監視体制を明確にすること。	運46				◎		
			実38	無人店舗の防犯体制を明確にすること。	運47				◎		
			実39	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				◎		
			実40	無人店舗の関係マニュアルの整備を行うこと。	運49				◎		
			実109	CD・ATM等の遠隔制御機能を設けること。	技19			◎	◎	◎	
		(5) インストアブランチ	実73	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				◎		
		(6) コンビニATM	実74	コンビニATMの出店先の選定基準を明確にすること。	運93					◎	
			実75	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					◎	
			実76	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					◎	
			実77	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					◎	
			実78	コンビニATMの所轄の警察および警備会社等関係者との連絡体制を確立すること。	運97					◎	
			実79	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					◎	
		(7) デビットカード・サービス	実80	デビットカード・サービスにおける安全対策を講ずること。	運99					◎	
			実81	デビットカードの口座番号、暗証番号等の安全性を確保すること。	運100					◎	
			実82	デビットカード利用時の顧客保護の措置を講ずること。	運101					◎	
			実83	デビットカード利用上の留意事項を顧客に注意喚起すること。	運102					◎	
		(8) 前払式支払手段	実32	機器および媒体の盗難、破損等に伴い、利用者が被る可能性がある損失および責任を明示すること。	運42		◎				
			実132	電子的価値の保護機能、または不正検知の仕組みを設けること。	技41	△	○				
		(9) 電子メール・イントラネットの利用	実89	電子メールの運用方針を明確にすること。	運107						◎
			実134	電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること。	技42-1	△	○				
		(10) クラウドサービスの利用	実144	クラウドサービス利用時の管理策を講ずること。	新設		◎				
Ⅲ 設備基準											
Ⅳ 監査基準	12 システム監査	(1) システム監査	監1	システム監査体制を整備すること。	運91	○	◎				

【資料４－１】
平成29年９月12日
公益財団法人 金融情報システムセンター

平成２９年度　安全対策専門委員会開催日程（改訂案）

	日程		時間	テーマ		議案（予定）	参加者
				安対	IT		
第５２回	6月16日	（金）	15:00-17:00	●		・改訂原案（前説Ⅰ・Ⅱ）に関する検討	安対専門委員・検討部会委員
第５３回	6月28日	（水）	15:00-17:00	●		・改訂原案（前説Ⅰ・Ⅱ）に関する委員意見に対する検討	安対専門委員・検討部会委員
第５４回	7月11日	（火）	15:00-17:00	●		・改訂原案（前説Ⅰ・Ⅱ）に関する検討 ・基礎基準・基準改訂に関する検討	安対専門委員・検討部会委員
第５５回	8月8日	（火）	15:00-17:00	●		・基礎基準・基準改訂に関する委員意見に対する検討 ・外部委託管理に関する検討 ・「読みやすさ」に関する検討（追加）	安対専門委員・検討部会委員
第５６回	9月12日	（火）	15:00-17:00	●		・基礎基準・付加基準における対策の整理 ・外部委託管理に関する検討（原案提示） ・「読みやすさ」に関する検討（統制基準の一部再編）	安対専門委員・検討部会委員
第５７回	10月17日	（火）	15:00-17:00	●	○	・基礎基準・付加基準に関する委員意見に対する検討 ・外部委託管理に関する委員意見に対する検討（修正案提示） ・「読みやすさ」に関する委員意見に対する検討 ・改訂原案（前説Ⅲ）に関する検討（原案提示） ・最終原案の承認・会員意見募集実施の承認（ＩＴ人材のみ）	安対専門委員・検討部会委員
第５８回	11月21日	（火）	15:00-17:00	●		・「読みやすさ」に関する委員意見に対する検討 ・改訂原案（前説Ⅲ）に関する委員意見に対する検討 ・最終原案の承認・会員意見募集実施の承認（安対基準のみ）	安対専門委員・検討部会委員
第５９回	１月中旬			●		・会員意見に対する回答案についての承認 ・発刊の最終承認	安対専門委員・検討部会委員
第５9回	1月中旬		15:30-17:00		○	・会員意見に対する回答案についての承認 ・発刊の最終承認	安対専門委員

運営要領についてIT人材と調整する予定

※IT人材のテーマが「○」については、書面による審議とさせていただく場合があります。

※会場は、全日程ともFISC会議室で行う予定です。

※日程等については、進度、状況によって、追加・変更となる場合があります。

【資料４－２】
平成29年９月12日
公益財団法人 金融情報システムセンター

平成29年度第56回安全対策専門委員会
検討事項に関するご意見（メール回答用）

電子メールにて、ご連絡願います。（fisc40@fisc.or.jp）

〆切　9/22（金）17:00（基礎基準、外部委託、読みやすさ）

会社名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

お名前：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

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