2013.07 投稿

特集 【 月例研究会報告 】

■第 181 回月例研究会報告

日時:2013 年 5 月 21 日(火曜日) 18 時 30 分～20 時30 分

演題:『金融機関等コンピュータシステムの安全対策基準・解説書』及び
『金融機関等におけるコンティンジェンシープラン策定のための手引書』の
改訂に伴う追補版について

講師: 財団法人 金融情報システムセンター(FISC)
監査安全部 西村 敏信 部長 様
鬼頭 克巳 総括主任研究員 様
岡田 昌一主任研究員 様

報告者 №0148 木村 裕一

【概要】

『金融機関等コンピュータシステムの安全対策基準・解説書』(以下「安全対策基準」とも表示:第Ⅰ部とする)、及び『金融機関等におけるコンティンジェンシープラン策定のための手引書』(以下「コンテ手引書」とも表示:第Ⅱ部とする)の改訂に伴い、去る3月1日にそれぞれ発刊した追補版についてご説明いただきました。この記録は資料からの引用を主としました。

なお、資料からの引用は明朝字体で、記録者による記述は当字体で表示します。

＜第Ⅰ部＞

「安全対策基準」:クラウドサービスに関わる現状の留意点、スマートデバイスの業務利用における留意点、インターネットバンキングにおけるセキュリティの確保、また、金融庁によるシステムリスク総点検の結果、及び東日本大震災やシステム障害に関する日本銀行のレポート等を踏まえ見直した内容について。

＜第Ⅱ部＞ (→P6から)

「コンテ手引書」:東日本大震災での被災から復旧に至る過程において、業務継続態勢整備として有効と考えられる施策や、政府や各省庁等からの防災・減災対策に対する検討結果等を踏まえ見直した内容について。

＜第Ⅰ部＞

テーマ:『金融機関等コンピュータシステムの安全対策基準・解説書』の改訂

経緯

平成23年3月に実施した『金融機関等コンピュータシステムの安全対策基準・解説書』(以下『FISC安全対策基準』という)全面改訂後、金融機関等におけるコンピュータシステムをとりまく様々な情勢の変化を受け、「安全対策基準改訂に関する検討部会」にて継続検討を行い、『第8版追補』を発刊することとなった。

今回の主な検討事項は次のテーマである。

●クラウド利用に関わる課題、留意点
●スマートデバイスの業務利用における留意点
●東日本大震災やシステム障害に関する各種ガイドライン・レポートとの比較分析
全体の構成（改訂の有無など）は次のとおり。

No	主要テーマ	改訂有無	No	その他のテーマ	改訂有無
1	**クラウドサービスを対象とした安全対策基準の対応付け**	**有**	1	【運50】の渉外端末の管理を対象とした安全対策の十分性の確認	有
2	**セキュリティ脅威の実情に照らした 記述内容の見直し**	**有**	2	CSIRTの整備に係る調査及び検討	有
3	**システム障害に関するリスク管理態勢**	**有**	3	関連法制の動向を踏まえての対応	無
4	**東日本大震災を踏まえた安全対策基準の検証**	**有**	4	PCIDSS(Ver2.0)と安全対策基準とのギャップ分析	無
5	**スマートフォンのセキュリティ**	**有**	5	関連ガイドライン等の最新動向を 踏まえての対応	無
6	**NISCの「安全基準等」への対応**	**無**	6	暗号関連（電子政府推奨暗号リストの改訂）	無
7	**通信技術の動向への対応**	**有**	7	事故犯罪事例に係る調査及び検討	無
8	**外部委託管理（オフショア開発）**	**無**			

以下は今回の改訂の主要テーマの中で取り上げられた特徴的な項目である。改訂の例として次の項目の取り上げ考え方を紹介する。詳細は配布資料を参照願いたい。

1．クラウドサービスを対象とした安全対策基準の対応付け

(1)検討の背景
①金融機関のクラウドサービスの利用にあたっては、従来のシステムとは異なる様々なリスクが懸念されている。
クラウドサービスの利用は、金融機関においても個別業務システムの分野では、既に普及段階に入りつつある。
一方で、基幹系システムや個人情報を扱うシステムへの適用については、従来のコンピュータシステムとは異なる様々なリスクが懸念されており、そのメリットには魅力を感じつつも、導入に踏み切れないでいる金融機関等もあるものと思料された。
②今後の安全対策のあり方の検討
以上のような背景のもと、金融機関等におけるクラウドサービスの利用の現状を踏まえ、セキュリティに関する懸念及び対策、関係法令や各種ガイドライン等について幅広く調査分析を行った。
調査の結果として「顕在化している課題・問題点」が散見されたことから、その課題・問題点について FISC 安全対策基準への反映の必要性も含め、検討することとした。

(2)検討内容

FISC安全対策基準の対象に関する基本的な考え方（本基準の対象）
1　顧客にオンラインサービスを提供するコンピュータシステム
2　他の金融機関等との決済業務に使用するコンピュータシステム
3　顧客データを扱うコンピュータシステム
4　サービスを提供するために金融機関等が顧客に提供するハードウェア・ソフトウェア
上記以外の主要なコンピュータシステムについては、主管部門を問わず、各金融機関の業務の実態に即して、本基準を適宜取り入れる。

（3）検討の経緯

①クラウド利用状況調査として金融機関等及びクラウド事業者にクラウドサービスの利用状況のヒアリングを実施した結果、 以下のような課題・問題点が明らかとなった。

分類	課題・問題点（主なもの）
契約・SLA	契約書チェックが疎か、SLAの扱いが区々
セキュリティ	外部にデータを預けることへの不安
内部統制	クラウドが外部委託契約ではないという認識
監査	データセンターの所在を開示しない例

②同課題・問題点に対するFISC安全対策基準上の管理の考え方と、該当する基準項目を整理した。

③改訂の要否及び内容の検討

該当するFISC 安全対策基準の改訂の要否を検討し、さらに、改訂が必要となる事項をどのような形でFISC 安全対策基準に盛り込むのかを検討した。

（4）主な論点

①委託契約ではないクラウドサービスの利用も外部委託に相当するのか？

実態として業務を委託していれば、外部委託に該当する。他の外部委託と同様に適切な外部委託管理が必要。

②クラウドサービスを利用している業務のうち、検討の対象とするのはどの業務か？

「FISC安全対策基準の対象に関する基本的な考え方」で対象としているものとする。

③今回の検討はクラウドサービスに関するリスク全般を網羅していないのでは？

今回の検討対象は、調査によって明らかとなった「既に顕在化している課題・問題点」について

検討したもの。

④参照の利便性を考慮すべきでないのか？

対象となる基準項目を各々改訂するのではなく、基準を新設し、必要事項をまとめることとした。ただし、既存の基準項目についても、必要に応じて参照することとする。

（5）検討結果

クラウドサービスに関し、「既に顕在化している課題・問題点」について、対応が必要な項目をまとめ、基準項目を新設

した。
なお、クラウドサービスについては、今後も引き続き検討を行う予定である。

新設基準

【運108】クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。

主な内容	狙い
クラウドサービスの利用にあたっては、**外部委託管理**の考え方に準じて適切なリスク管理が必要	クラウドサービスの利用は業務の外部委託であることの明確化
契約には、クラウド事業者との間の**管理境界・責任分界点**に関する取り決めを盛り込むこと	利用者・事業者双方が責任をもって管理する範囲の明確化
本基準項目で参照していない基準についても必要に応じて参照すること	当基準だけを参照すれば良いということではないことの明確化
参照基準に「委託契約」の文言がある場合、サービスを利用するための契約に読み替えて参照すること	契約形態に関わらず外部委託管理が必要であることの明確化

2. セキュリティ脅威の実情に照らした 記述内容の見直し
(1)検討内容
安全対策実施状況調査の結果から浮き彫りになったセキュリティ脅威等として次がある。
① 本人確認機能における認証方式
② 標的型攻撃に対する対策の有効性
③ 各種法改正の動向

(2)主な論点と検討結果
今回の改訂においては、特に、預金等の不正払い戻しが発生している「個人顧客を対象とする」「インターネットバンキング」に限定して、認証方式を強化するよう記載することとする。
改訂基準として、運用項目1件、技術項目3件の改定を行った。

3. システム障害に関するリスク管理態勢
(1)検討の経緯
金融庁の監督指針、金融検査マニュアル等の改正に伴うFISC安全対策基準の十分性の検証及び改訂の必要性の検討を行った。そのギャップ分析の結果、次のような改定を行った。

(2)検討結果

主な改訂基準	内容
【運1】セキュリティ管理方法を具体的に定めた文書を整備すること。	セキュリティ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**とした。

3】セキュリティ管理体制を整備すること。	体制の確立にあたっては**経営層が指示し、承認すること**とした。
【運62】関係者への連絡手順を明確にすること。	重大な障害、災害については、**想定される最大リスク等を含め**、経営層への報告を適宜行う必要があるとした。
	障害・災害時の連絡、召集対象に**「重要なシステムを委託している外部委託先」**を追加した。
【運90】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。	委託先の業務の点検または監査の結果として認識した問題点について、**「その影響度に応じて、経営層へ適切な報告を行う必要がある」**ことを追記した。

4．東日本大震災を踏まえた安全対策基準の検証

（1）主な論点

①非常時のコンピュータシステムの継続稼働については、自家発電装置の稼動時を想定した記載が必要ではないか？

非常時に備えた自家発電設備の定期点検の内容として、「燃料容量や冷却水の確保による、非常時の運転可能時間」を考慮することが必要であるとする。

②障害時・災害時の連絡手順を定めるにあたって、通信途絶時等の対応を考慮すべきではないか？

通信途絶時の対応例として、災害時優先通信を連絡手段の例に含めることとする。

③外部委託契約の締結について考慮点を記載すべきではないか？

目標復旧時間やSLAどおりに委託業務を遂行できない場合の対応策を事前に考慮しておくことが望ましいとする。

④障害時・災害時の復旧手順を見直すべきではないか？

バックアップシステム（バックアップサイトを含む）への切替え時の社内システムへの影響確認、切戻しについての考慮が必要であるとする。

⑤バックアップサイト保有の必要性について、より一段高いレベルの記載が必要ではないか？

資金決済等の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とする。ただし、保有しない場合は、代替手段について経営層による承認を必要とすることとする

その他、つぎの主要テーマ（P2に表示）についても説明がなされた。（記録は省略）

5.スマートフォンのセキュリティ

6．NISCの「安全基準等」への対応

7．通信技術の動向への対応

8．外部委託管理（オフショア開発）

なお、Q&Aについては第2部　5項に記載

＜第Ⅱ部＞

テーマ:『金融機関等におけるコンティンジェンシープラン策定のための手引書』の改訂に伴う
追補版について　（東日本大震災の教訓を反映）

1. 発刊の経緯

『コンティンジェンシープラン策定のための手引書（第3版追補2）』発刊の目的

平成 23 年3月の東日本大震災の経験を踏まえ、わが国全体として防災・減災対策への関心が大きく高まっており、この経験を将来へ向けた貴重な教訓として役立てていこうとする動きが活発化している。

当センター（FISC）では、「東日本大震災影響調査プロジェクトチーム」を設置し、東日本大震災によって金融機関等が受けた被害や対応状況などの事実関係、その後に金融機関等で検討された諸施策などを調査し、今後の業務継続態勢に関する論点について整理を行い、機関誌などで報告してきた。

機関誌に掲載の震災レポート

「東日本大震災における金融機関等の対応状況について」『金融情報システム』平成24年春号
「東日本大震災を踏まえた業務継続態勢整備の方向性」『金融情報システム』平成24年秋号

また、上記の震災レポートの他、第1部で説明した「安全対策基準改訂に関する検討部会」における2つの検討テーマ（「システム障害に関するリスク管理態勢」「東日本大震災を踏まえた安全対策基準の検証」）における検討結果も合わせ、金融機関等が有効に活用することを目的として、『金融機関等におけるコンティンジェンシープラン策定のための手引書（第3版）』（『コンテ手引書』）の『追補2』を発刊した。

今回の改訂により、『コンテ手引書』の構成は次のようになる。

第3版 ＋ 第3版追補 ＋ 第3版追補2

2. 改訂の概要

今回の改訂は、東日本大震災の影響をテーマとし、『震災レポート』の内容と他団体等のガイドライン等とのギャップ分析結果をもとに行った。

《検討テーマ》

（1）震災レポート

（2）他団体等のガイドライン等とFISCガイドラインとのギャップ分析

《改訂の範囲》

『コンテ手引書』 の各編	改訂のポイント	『コンテ手引書』との関係
第1編	改訂の背景や事業影響度分析の考え方を追記	読替え
第2編	「3. 本手引書の構成」について全体の構成を追記	読替え
第3編	「停電対策」「関連先の考慮」「業務継続態勢整備」「経営層の関与」「障害対応」について更新・追記	読替え

第4編	「バックアップサイトの実効性」「関連先の考慮」「業務継続態勢整備」「長期間拠点使用不可リスク」「帰宅困難者対応」「障害対応」について更新・追記	読替え
第5編	「障害対応」「具体例」について更新・追記	読替え
第6編	自然災害以外のリスク 「障害対応」「具体例」について更新・追記	読替え
第7編	資料編として、『震災レポート』2編と事業影響度分析の手法に関する国内外の動向を調査したレポートを追加	追加

3. 改訂内容の紹介

主な改訂内容について、以下に紹介する。

(1)策定にあたって

① 検討内容

『震災レポート』にて紹介した事業影響度分析(BIA)の考え方は、新たな考え方として、今後のコンティンジェンシープラン策定に際し有効な考え方であるため、『コンテ手引書』のプロセスに影響を与えず、この考え方を紹介するため、第1編に記載することを検討。

② 検討結果

コンティンジェンシープラン策定のプロセス説明の中で、リスク洗い出しの際の新たな視点として、重要業務が停止した場合のリスクを先に考える事業影響度分析の考え方を追記した。

(2)緊急事態 (リスク) の洗い出し

① 検討内容

・外部委託先との契約の際、不確実性の想定についての追記を検討

・停電の影響が長時間、断続的、広範囲におよぶ場合の追記

② 主な論点

・緊急事態(リスク)の考慮について、一定の地域への立入禁止リスクなども明記すべきではないか？

③ 検討結果

・緊急事態(リスク)が長時間、広範囲にわたる場合の考慮として、計画停電だけでなく、コンピュータセンター等が立入禁止になる場合などを、例示として追記

・緊急事態(リスク)発生時に外部委託が契約どおりに対応できない可能性の考慮を追記

(3)緊急時対応策の骨子の決定

① 検討内容

・外部委託先のサービス供給が不可能である場合の考慮の追記を検討

・目標復旧時間の検討について追記を検討

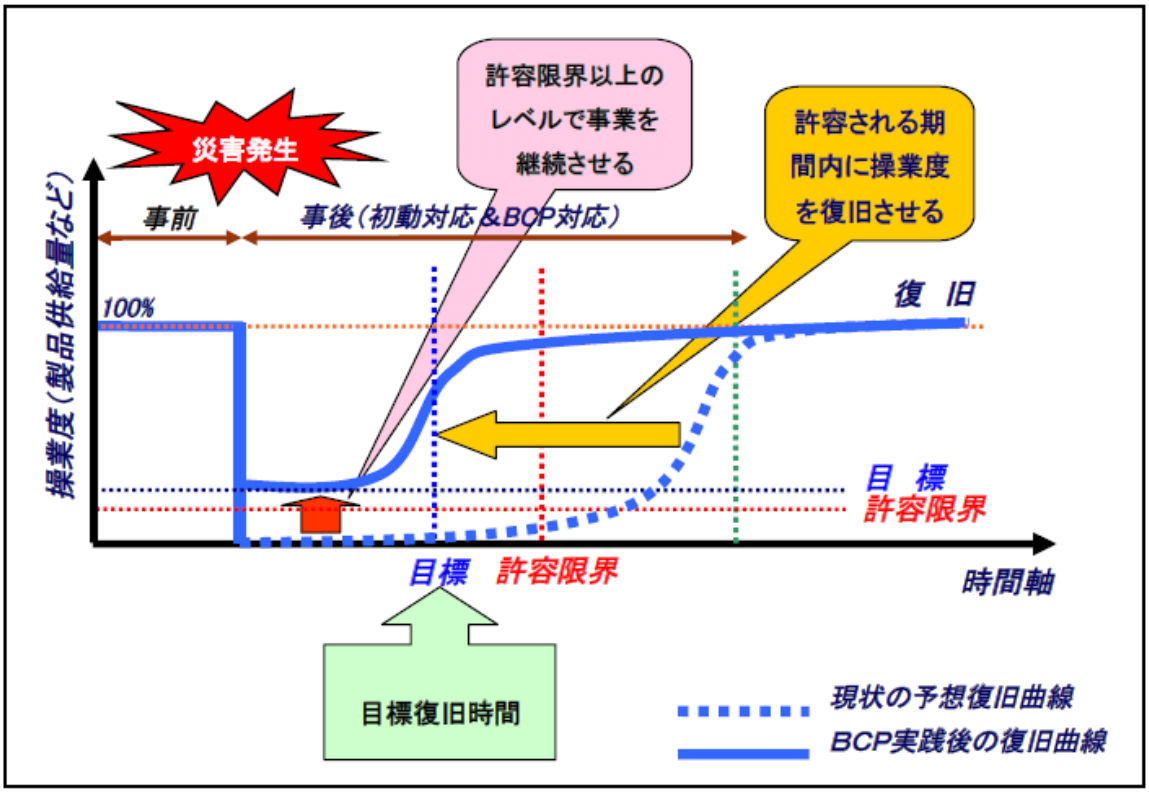
② 検討結果

・外部委託先に依存する代替手段が機能しなくなる可能性の考慮を追記

・業務の目標復旧時間の設定検討について追記

・業務の目標復旧時間のイメージ図について追記

図表２　事業継続計画（BCP）の概念



（内閣府編「事業継続ガイドライン　第二版」（平成 21 年 11 月）をもとに FISC にて作成）

(4)コンティンジェンシープラン策定の基本方針の決定

① 検討内容

・経営層がコンティンジェンシープランの重要性を認識することについて追記を検討

・経営層がシステムやシステムリスクを把握していることについて追記を検討

② 検討結果

・経営層がコンティンジェンシープランの基本方針決定（承認）する際のシステムリスク認識について追記

・コンティンジェンシープラン更新を経営層が承認する際、状況変化に応じてシステムリスクなどが見直されていることを確認することを追記

5. 質疑応答　（鬼頭氏、西村氏により回答を頂いた。）

(1)質問1　安全対策の改訂　配布資料　第1部　P12

「クラウドサービスを対象とした安全対策基準の対応付け（3／5）」

＜質問＞

クラウドサービスを利用する際に監査がしづらいという話があった。実際現場で悩ましい問題である。大きな

クラウドサービス事業者には実質的認証があったりする。それで監査を省略できるか、信用できる会社との契約を締結するなどが考えられる。これについて、ガイドラインなどの議論があるのか。

＜回答＞

今回の改訂においては、クラウドサービスの利用について、外部委託の範疇と捉えられることから、監査は外部委託同様に必要であるとしている。

クラウドサービスの利用についての課題は、今後も出てくると認識しており、今後も継続的に検討が必要と考えている。

(2)質問 2　安全対策 配布資料 P24 (当記録P5 参照)

「システム障害に関するリスク管理態勢」において、〔運1〕〔運3〕。

＜質問＞

“経営層が指示し、承認すること とした。”とある。

リスク管理態勢をボトムアップからトップダウンにしたとのことである。主旨は分かるが、“経営層が指示し”は、それが出来ていると想定しているのか、あるいはあるべき姿としているものか。

＜回答＞

“経営層が指示し”の主旨は、大規模システム障害が発端になっている。

内容についてリスク管理態勢は経営層が主体的にやらなければならないという認識であり、それがあるべき姿であると考えている。

(3)質問 3「コンテ手引書」 配布資料　P40

「緊急時における要員確保について」

＜質問＞

“緊急対応する代替要員を検討することも望ましい“と記載されている。

大規模災害では、キーマンが被災することもありうる。

考え方としてキーマンの代替の考え方は分かるが、現実的に考えられるか疑問。

＜回答＞

議論の中で代替要員を確保することは、目指すべき姿としてあげた。

現実には難しいこともあるが、目指すべきは、一人の人が欠けて業務が止まることが無いように、事前に準備をしてもらいたい、というのが主旨である。

(4)質問 4　安全対策　配布資料 P30

「東日本大震災を踏まえた安全対策基準の検証(4／5)」

＜質問＞

バックアップ体制については、以前は60Km ほど離れていれば OK という記述があった。広域災害が起こったことを踏まえてどれくらい離れていれば OK であろうか。

＜回答＞

相当以前の安全対策の中には、距離60Km 離れていればという記述があったが、現状は距離の記載はない。

今回の大規模災害でも関西や九州は被害が無かったことを考えると、距離は離れていたほうが良いが、中央防災会議などでも一概に安全な距離というものはないとしているため、各種リスクをメインサイトとバックアップサイトで共有しないようにするという観点で、できることを行う必要がある。例えば、管轄が違う電力会社や地域にサイトを持つといったことも考えられる。また、バックアップサイトを保有することは原則であるが、保有すること自体が現実的ではない場合、代替手段をいかに確保するかを、予め検討して先に取り決めしておくことが重要である。

＜記録者の感想＞

非常に盛り沢山の内容を短時間に報告・説明していただいた。配布資料は細かく丁寧に作成されているので、資料だけでも参考に出来るようになっているのは大変ありがたい。

その中で考え方がきちんと表現されていることは参考になる。われわれはよく理解しておきたいものである。また、短時間であったが、質疑応答でシステムの管理者や監査人から見ての疑問が出され、まだこれからの検討課題であることや、今回の改訂の考え方が回答されて意義深いものになった。

講師としてご来場を頂いた西村部長、鬼頭総括主任研究員、岡田主任研究員の皆さんには、深くお礼を申し上げます。有難うございました。

以上

■ 第 182 回月例研究会報告

日時:2013 年 6 月 17 日(月曜日) 18 時 30 分～20 時30 分

場所:機械振興会館　地下 2 階　ホール

演題:「個人情報影響評価 PIA の要諦とシステム監査との関係」

講師:公立大学法人首都大学東京　産業技術大学院大学

教授　瀬戸洋一　氏

報告者 Ｎｏ．1186　宮下重美

1. 講演要旨

プライバシーなど個人情報を利用するシステムの構築にあたり、プライバシーリスクを事前評価することにより、適切なコストで安全なシステムを構築することが可能である。プライバシーリスクの事前評価に関する世界的な規準としてプライバシー影響評価(Privacy Impact Assessment)がある。保護対象とするデータは機微情報だけではなく、いわゆる個人情報であるため、日本や韓国では、個人情報影響評価(Personal information Impact Assessment:PIA)と呼んでいる。本講演では、プライバシー影響評価、個人情報影響評価の2つの言葉を同じ意味で使う。一般的な専門用語として利用する場合はプライバシー影響評価、日本や韓国における状況の説明の場合は個人情報影響評価と使い分ける。

個人情報保護の体系的な対策としてプライバシーバイデザイン(計画的なプライバシー対策)PbD のコンセプトが提案されている。この PbD における PIA の位置づけを明確にし、システム監査との比較における PIA の要諦を紹介する。

なお、項目構成は次のとおりである。　　(講演資料の項番を詳細化し、項目を再設定している)