平成 29 年 6 月 28 日
公益財団法人 金融情報システムセンター

第 53 回　安全対策専門委員会　議事次第

Ⅰ　日時

平成 29 年 6 月 28 日（水）　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（FISC 事務局）
２．　15:15　【報告】
　　・『FinTech 有識者検討会報告書』公表について（FISC 企画部）
３．　15:40　【議案】改訂原案（前説）に関する検討
　　・各委員からのご意見について（FISC 事務局）
４．　16:55　事務連絡
５．　17:00　閉会

Ⅳ　資料

【資料１－１】　「金融機関における FinTech に関する有識者検討会」報告書の公表について
【資料１－２】　「API 接続チェックリスト（試行版）」 利用にあたって
【資料１－３】　「API 接続チェックリスト（試行版）」
【資料２－１】　改訂原案（前説）に対する各委員からのご意見まとめ
【資料２－２】　改訂原案（前説）に対する各委員からのご意見（対応方針案）
【資料２－３】　改訂原案（安全対策基準前説）
【資料３－１】　検討事項に関するご意見（メール回答用）

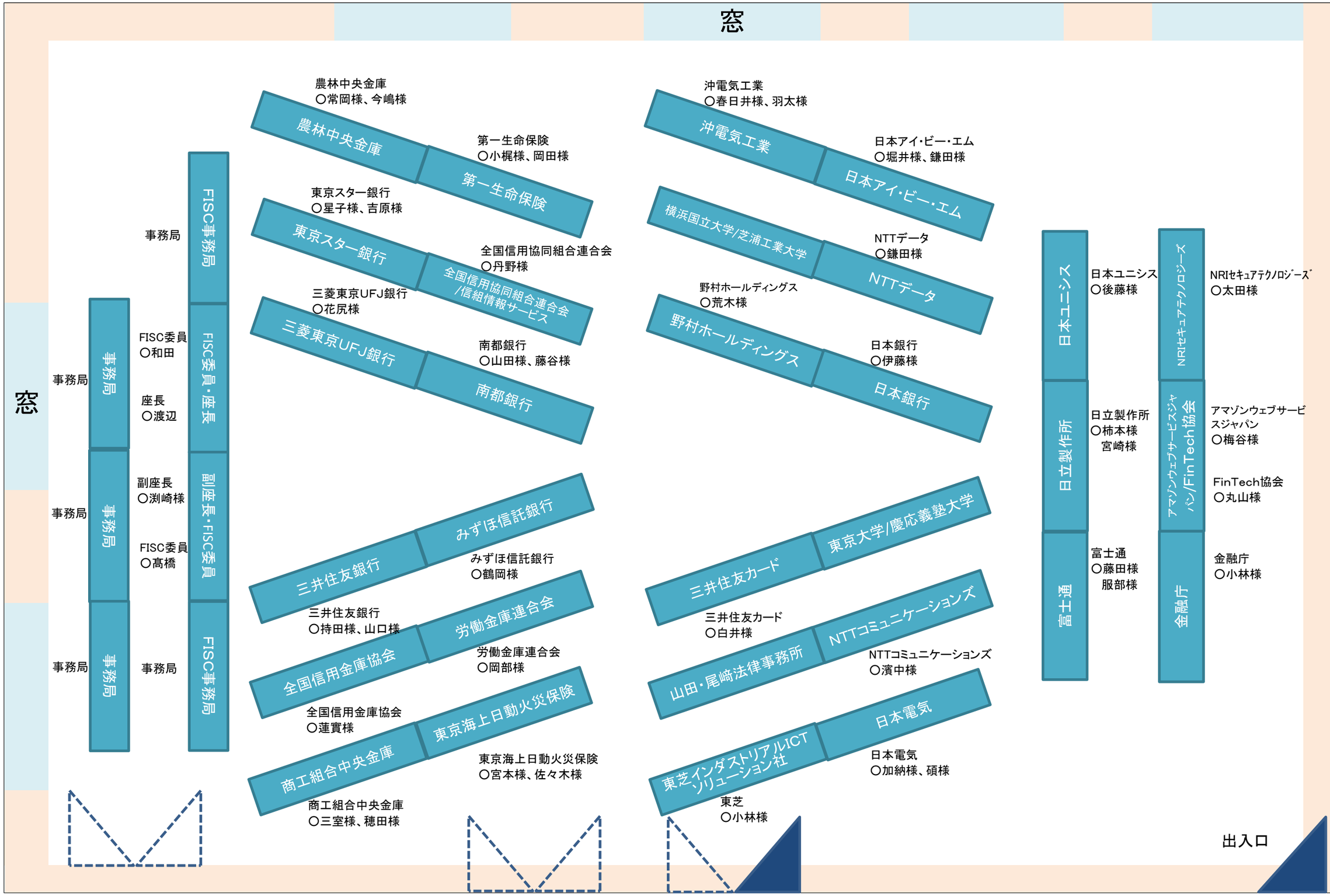
Ⅴ　今後の予定

○第 54 回　安全対策専門委員会
　（予定）平成 29 年 7 月 11 日（火）15:00～17:00　FISC 会議室

以上

第53回「安全対策専門委員会」座席表

平成29年6月28日



【資料１－１】
平成29年6月28日
公益財団法人 金融情報システムセンター

平成 29 年 6 月 21 日
公益財団法人 金融情報システムセンター（FISC）

「金融機関における FinTech に関する有識者検討会」報告書の公表について

当センターで開催しておりました「金融機関における FinTech に関する有識者検討会」の報告書を公表いたします。

「有識者検討会」とは、わが国金融機関の情報システムの安全対策推進に資することを目的に、当センター理事長の諮問機関として設置し、学識経験者及び各業界団体並びに各金融機関の代表等で構成される検討会です。検討の成果を報告書として公表するとともに、最終的には当センター発刊の「金融機関等コンピュータシステムの安全対策基準・解説書」（以下「安対基準」という）等各種ガイドラインにその内容を反映し、金融機関をはじめとして金融情報システムに携わられている多くの皆様にご利用いただいております。

これまでに、「サイバー攻撃対応」「クラウド利用」「外部委託」をテーマに開催してきましたが、これらに続いて、昨年１０月から、近年、金融機関、業界団体及び監督当局等において取り組みが急速に活発化している「FinTech」をテーマに取り上げました。計６回にわたる検討会（座長は岩原紳作早稲田大学 大学院法務研究科 教授）での議論を経て、報告書をとりまとめ、今般、当センターホームページ（https://www.fisc.or.jp）で公表いたします。

【報告書のポイントと特徴】・・・（別紙１）参照
【検討会名簿】　　・・・（別紙２）参照

なお、当センターでは、既に安対基準の改訂に着手しており、『外部委託』『FinTech』に関する両有識者検討会報告書での提言内容に基づく改訂を、来年３月末を目途に完了させる予定です。

以上

＜本件に関する問い合わせ先＞
公益財団法人　金融情報システムセンター　企画部　小林、大澤、柴田
(03-5542-6055)

（別紙１）

【報告書のポイント】

１．イノベーションとシステムの安全性を両立させるための原則・ルールの提言

わが国金融機関が、FinTech に取組む中で、システムの安全性を確保しつつも、顧客のニーズに適応しイノベーションの成果を最大限享受しうることを目指し、以下の原則・ルールを提言した。

- 同等性の原則

  FinTech で目標とされるべき安全対策の効果は、FinTech 企業が加わったからといって増減されることなく、従来のサービスと同等に維持されるべきとする考え方。

- 協調の原則

  FinTech において適切な安全対策を実施するためには、関係する金融機関、IT ベンダー及び FinTech 企業の３者が、互いに協調することが不可欠とする考え方。

- 再配分ルール

  イノベーションの成果を享受するために、FinTech 企業の安全対策遂行能力によっては、金融機関等の関係者が、本来 FinTech 企業が実施すべき安全対策を補完することを可能とするルール。

- 外部委託基準の準用ルール

  FinTech 企業が自ら主導するサービスに、金融機関が API 等を通じてデータの提供・受入れを行う場合には、金融機関は FinTech 企業に対して、従来からある外部委託基準を部分的に準用して統制を行うことを可能とするルール。

２．FinTech に携わる幅広い事業者に向けた意見表明

FinTech 業務に携わる事業者においては､安対基準の適用対象であるか否かに関わらず、本検討会が策定する以下の「金融関連サービスの提供に携わる事業者を対象とした原則」を踏まえたうえで、適切な安全対策が実施されることを期待し、意見表明を行った。

（１）金融関連サービスの提供に携わる事業者は、その利用者が安心してサービスを利用できることを目指し、みずからが管理責任を負う情報システムに対して、適切な安全対策を実施する。

（２）金融関連サービスの提供に携わる事業者は、安全対策の実施に当たっては、イノベーションの成果が利用者の利便性向上に資するよう留意するとともに、金融機関とその他事業者がそれぞれ独自の優位性を活かせることを目指し、安全対策においても協調が促進されるよう留意する。

（３）金融関連サービスの提供に携わる事業者は、互いに協調して安全対策を実施するに際し、FISC 安対基準を含め、安全対策に関して社会的に合意されたルールが形成されるよう努める。

３．重要な情報システムでクラウドサービスを利用する際のリスク管理策の提言

FinTech ではクラウドサービスが利用される場合が多いことから、従来のクラウド基準に対して補足的検討を行った。具体的には、金融機関におけるクラウドサービスの歴史的意義を明らかにするとともに、クラウドサービス固有の性質（匿名の共同性・情報処理の広域性・技術の先進性）を明確にした。そのうえで、重要な情報システムでクラウドサービスが利用される場合を想定し、以下のリスク管理策を提言した。

【リスク管理策】

・統制対象クラウド拠点の把握
・監査権等の明記
・監査の実施（保証型監査報告書の利用）
・監査人等モニタリング人材の配置

４．「オープン API」における安全対策の在り方の提言

FinTech 企業集団と金融機関集団が、安全対策に関する協議を開始し、総体的な安全性を確保しつつ関係者の負担を最小化することを目指して、両者で協調した取組みが進められていくことを提言した。

５．今後の安対基準等の改訂の考え方

外部委託検討会及び FinTech 検討会の提言を受けて、以下のような考え方に基づき、安対基準等のガイドラインの改訂を進める。

・リスクベースアプローチを踏まえた基本原則の導入
・基本原則に基づいた安対基準の明確化
・外部委託等に対する統制基準の拡充

【報告書の特徴】

- 問題を論理的に特定し対策を効果的に導出するため、FinTech をタイプ別に類型化している。
- FinTech に留まらず、FISC が既に行った外部委託検討会の提言（リスクベースアプローチ・IT ガバナンス）から一貫した議論がなされ、広範かつ相互に整合的一体的な形で、金融情報システムに携わる全ての関係者にとって参考となる提言内容となっている。
- FISC が 30 年以上にわたり涵養してきた「関係者が協調し集合的検討を行う土壌」により、多様な関係者が携わる FinTech に関しても、短期間での合意形成が可能となっている。（他国であまり類を見ないこの「土壌」は、今後発生する諸問題に対処していくにあたっても有効。）

以上

（別紙２）

「金融機関における FinTech に関する有識者検討会」委員・オブザーバー名簿

（敬称略）

座長	岩原 紳作	早稲田大学 大学院法務研究科　教授
座長代理	渕崎 正弘	株式会社日本総合研究所 代表取締役社長
委員	安冨 潔	慶應義塾大学名誉教授 京都産業大学法務研究科客員教授・ 法教育総合センター長 弁護士（渥美坂井法律事務所・外国法共同事業）
	國領 二郎	慶應義塾常任理事、慶應義塾大学総合政策学部教授
	上山 浩	日比谷パーク法律事務所　パートナー弁護士
	田中 秀明	株式会社みずほフィナンシャルグループ IT・システム企画部　システムリスク管理室　室長 （第４回まで）
	持田 恒太郎	株式会社三井住友銀行 システム統括部　システムリスク統括室　室長 （第５回から）
	山田 満	株式会社南都銀行 システム部　部長
	吉本 憲文	住信 SBI ネット銀行株式会社 FinTech 事業企画部長
	真田 博規	住友生命保険相互会社 情報システム部 担当部長
	久井 敏次	東京海上日動火災保険株式会社 理事　IT 企画部長（第４回まで）
	黒山 康治	東京海上日動火災保険株式会社 IT 企画部　参与（第５回から）
	植村 元洋	野村ホールディングス株式会社　IT 統括部 次長 兼 IT 管理課長(エグゼクティブディレクター)
	Mark Makdad	一般社団法人 FinTech 協会 理事
	瀧 俊雄	株式会社マネーフォワード 取締役　Fintech 研究所長
	轟木 博信	株式会社 Liquid 経営管理部長　弁護士
	村上 隆	株式会社ＮＴＴデータ 第四金融事業本部　企画部　ビジネス企画担当 シニア・スペシャリスト
	長 稔也	株式会社日立製作所 金融システム営業統括本部　事業企画本部 金融イノベーション推進センタ　センタ長

	岩田 太地	日本電気株式会社 事業イノベーション戦略本部 FinTech 事業開発室　室長
	梅谷 晃宏	アマゾンウェブサービスジャパン株式会社 セキュリティ・アシュアランス本部　本部長 日本・アジア太平洋地域担当
	内田 克平	日本マイクロソフト株式会社 クラウド＆ソリューションビジネス統括本部 金融インダストリー担当部長 （第２回まで）
	平原　邦久	日本マイクロソフト株式会社 金融サービス営業本部 シニアインダストリーマネージャー （第３回から）
	荻生 泰之	デロイトトーマツコンサルティング合同会社 執行役員
オブザーバー	神田 潤一	金融庁 総務企画局　企画課　信用制度参事官室　企画官
	片寄 早百合	金融庁 検査局　総務課　システムモニタリング長 主任統括検査官
	中井 大輔	日本銀行 金融機構局　考査企画課 システム・業務継続グループ企画役
	師田 晃彦	経済産業省 商務情報政策局 サイバーセキュリティ課長
	大森 一顕	総務省 情報通信国際戦略局 参事官（サイバーセキュリティ戦略担当）

【資料１－２】
平成 29 年 6 月 28 日

「API 接続チェックリスト（試行版）」 利用にあたって

１．目的

「API 接続チェックリスト（試行版）」（以下「チェックリスト」という）は、銀行と API 接続先が効率的にコミュニケーションを行うためのツールとして、「API 接続先チェックリスト ワーキンググループ」（以下「チェックリスト WG」という）において、機密性に関して共通的に確認する項目を中心に策定したものである。

（注）オープン API のあり方に関する検討会（事務局：一般社団法人全国銀行協会）「オープン API のあり方に関する検討会報告書－オープン・イノベーションの活性化に向けて－【中間的な整理（案）】」には、「複数の銀行と API 接続する企業等における審査対応負担を軽減する観点から、銀行が API 接続先の適格性を審査する際に使用する、必須確認項目と独自確認項目からなる「API 接続先チェックリスト」（仮称）を制定することが期待される」と記載されている。

２．共通確認項目及び構成要素

共通確認項目は、大きく分けると以下の２つである。

（１）安全対策の遂行能力の確認

①オープン API のあり方に関する検討会が定める安全対策の遂行能力

オープン API のあり方に関する検討会報告書「セキュリティ原則」に基づき作成

②FISC 安対基準（FinTech 関連項目）の遂行能力

FinTech 検討会で提言された考え方等を踏まえて作成

③基礎的な安全対策の管理・運営能力

FISC が策定する「必要最低限の安対基準」（注）又は業界団体の自主基準

（注）「必要最低限の安対基準」は、API 接続先を含む金融関連サービスの提供に携わる事業者において、踏まえられるべき基準としても制定される。その制定までの間は、少なくとも「安全対策遂行能力のうち基礎的な部分」を踏まえて検討されることが望ましい。

（２）その他の確認

利用者保護態勢等

共通確認項目				独自確認項目
（１）安全対策関連			（２）その他	
① API 検討会が定める安全対策の遂行能力	② FISC 安対基準(FinTech 関連)の遂行能力	③ 基礎的な安全対策の管理・運営能力	利用者保護態勢等	

３．全体構成

チェックリストには 60 個の確認項目がある。

章	区分	各章の目的	項番
1	情報・セキュリティ管理態勢	API 接続先の情報・セキュリティ管理態勢について確認する。	1-10
2	外部委託管理	API 接続先が外部事業者に委託して開発する場合の管理態勢について確認する。	11-13
3	銀行・API 接続先の協力体制	利用者保護の観点から、銀行及び API 接続先における責任分界点や役割分担について確認する。	14-19
4	コンピュータ設備管理	API 接続先がサービスを提供するシステムが実装されているコンピュータ設備のセキュリティについて確認する。	20-22
5	オフィス設備管理	API 接続先がサービスを提供するシステムにアクセスする機器が設置されているオフィスのセキュリティについて確認する。	23-26
6	システム開発・運用管理	API 接続先の基本的な開発及び運用の管理態勢について確認する。	27-40
7	サービスシステムのセキュリティ機能	API 接続先が提供するサービスシステムのセキュリティ実装要件について確認する。	41-49
8	API セキュリティ機能	利用者保護の観点から、API アクセスを管理するシステムについて確認する。	50-57
9	API 利用セキュリティ	利用者への説明義務について確認する。	58-60

４．取扱方法

（１）各項目の説明

チェックリストの各項目に関する説明は、以下の通り。

通番：通し番号

区分：テーマ別分類

セキュリティ対応目標：安全対策を実施する目標

対象者：安全対策を実施する主体

手法例：安全対策の例示

現在の対応状況：対象者が現在実施している安全対策の状況を記載する

今後の対応予定：対象者が今後実施予定の安全対策について記載する

関連規定：参照先（全銀協「セキュリティ原則」又は FISC「安対基準」）

関連規定箇所：全銀協「セキュリティ原則」及び FISC「安対基準」の参照箇所

（２）使用タイミング及び用途

チェックリストの使用タイミング及び用途は、API 接続先の任意である。

なお、API 接続先が銀行との API 接続を検討する際、チェックリストの「現在の対応状況」及び「今後の対応予定」を予め記載しておくことにより、銀行が実施する API 接続先の適格性審査において、双方の対応負担が軽減されることとなる。

（３）留意事項

チェックリストを利用するにあたっては、以下について留意する必要がある。

・チェックリストは機密性に関する確認項目を中心に策定し、各銀行の独自確認項目が多くならないよう幅広に用意した。しかし、各銀行が必要とする確認項目の全てを網羅したものではない。他に必要な確認項目がある場合は、各銀行にて独自の確認項目を付加する場合がある。

・記載されている手法例はあくまで例示であり、業務特性やリスク等を勘案し各銀行にて取捨選択する。なお、各銀行の判断により、例示以外の手法を選択することを妨げるものではない。

・チェックリストはコミュニケーション・ツールとして活用することを想定している。各銀行は必要に応じて「今後の対応予定」等の欄を用いて、API 接続先から「○」又は「×」の回答を単に受けるだけではなく、API 接続先と十分に会話するよう努める。

・チェックリストの確認項目のいずれかにおいて、API 接続先の回答が「×」であったとしても、各銀行は業務特性やリスク等を踏まえて総合的に判断する。

・チェックリストは、銀行、IT ベンダー、そして大小様々な規模の API 接続先においても利用しやすく、理解しやすいものとなるよう、見直しが行われる予定である。

５．今後の予定

チェックリスト（試行版）の見直しの時期および方法については、チェックリスト WG メンバーを含む関係者の意見を踏まえ、引き続き FISC にて検討を行う。

なお、チェックリストへの反映が予定されている「必要最低限の安対基準」については、その原案が FISC 安全対策専門委員会において 2017 年 10 月を目途に確定される予定のため、チェックリストの見直しの時期は少なくともそれ以降となる見込みである。

以上

参考

【資料１－２】
平成 29 年 6 月 28 日

API 接続先チェックリスト検討の経緯

１．検討メンバー

チェックリスト WG は、API 接続に携わる関係者 10 社（全銀協から銀行 3 行、FinTech 協会から FinTech 企業 3 社、IT ベンダー3 社、FISC 監査安全部 1 名）を委員とし、金融庁及び日本銀行にもオブザーバーとして参加いただいた（事務局は FISC 企画部が担当）。

（敬称略）

区分	氏名	所属・役職
銀行 （3 名）	奥野　瑞穂	株式会社みずほ銀行 e-ビジネス営業部　法人プロダクト開発チーム 調査役
	小原　彰	株式会社三井住友銀行 システム統括部　統括グループ　グループ長
	原田　一雪	株式会社三菱東京 UFJ 銀行 デジタル企画部　事業開発グループ　次長
FinTech 企業 （3 名）	土佐　鉄平	freee 株式会社 開発本部　チーフセキュリティアーキテクト
	大目　晃弘	マネーツリー株式会社 ビジネスディベロップメント　マネージャー
	内波　生一	株式会社マネーフォワード アカウントアグリゲーション本部　本部長
IT ベンダー （3 名）	村上　隆	株式会社エヌ・ティ・ティ・データ 第四金融事業本部　企画部　シニア・スペシャリスト
	鎌田　美樹夫	日本アイ・ビー・エム株式会社 グローバル・ビジネス・サービス事業部 金融インダストリー・ソリューション　担当部長
	谷内　圭	富士通株式会社 金融システム事業本部　デジタルビジネス開発室 シニアマネージャー

【資料１－２】
平成 29 年 6 月 28 日

区分	氏名	所属・役職
FISC （1 名）	亀水　宏次	公益財団法人金融情報システムセンター 監査安全部　次長
オブザーバー （4 名）	小林　侑剛	金融庁 総務企画局　企画課　信用制度参事官室　課長補佐
	市村　雅史	金融庁 検査局　総務課　システムモニタリングチーム 専門検査官
	中井　大輔	日本銀行 金融機構局　考査企画課　企画役
	宮　　将史	日本銀行 決済機構局　FinTech センター 決済高度化グループ長　企画役

２．開催実績

回数	日時	主な内容
第 1 回	2 月 7 日（火） 10 時～12 時	API 接続先チェックリスト検討の前提（FinTech 有識者検討会における議論）の内容確認
第 2 回	2 月 20 日（月） 15 時～17 時	API チェックリスト検討のたたき台（FinTech 企業の委員による発表）等をもとに議論
第 3 回	3 月 3 日（金） 15 時～17 時	API 接続先チェックリスト作成手順案（事務局案）等をもとに議論
第 4 回	3 月 17 日（金） 15 時～17 時	同上
第 5 回	4 月 11 日（火） 15 時～17 時	API 接続先チェックリスト（案）等をもとに議論
第 6 回	4 月 25 日（火） 15 時～17 時	同上
第 7 回	5 月 11 日（木） 15 時～17 時	同上
第 8 回	5 月 25 日（木） 15 時～17 時	同上
第 9 回	6 月 6 日（火） 15 時～17 時	同上
第 10 回	6 月 20 日（火） 15 時～17 時	API 接続チェックリスト（試行版）の最終確認

３．検討にあたっての前提

オープン API は、FISC において開催している「金融機関における FinTech に関する有識者検討会」（以下「FinTech 検討会」という）におけるタイプⅢ（FinTech 企業が金融関連サービスを主導する形態で、金融機関の安全対策上の責任が部分的となる場合）の実現方法の１つであることから、チェックリスト WG の検討は、FinTech 検討会におけるタイプⅢに関する提言内容と整合的に進められることが必要である。すなわち、タイプⅢにおける「外部委託基準の準用ルール」及び「必要最低限の安対基準」を踏まえつつ、FinTech に関する安全対策を検討している集団の相互関係を考慮した検討が行われることが必要である。

チェックリスト WG において、FinTech 検討会におけるタイプⅢに関する提言内容と整合的な検討が行われた結果として作成されたチェックリスト等は、FinTech 検討会の提言内容の一部として取り扱われることとなる。

（参考）「金融機関における FinTech に関する有識者検討会」報告書

【資料９】API接続にあたって使用されるチェックリストに関する集合的な検討

全銀協が公表した「オープンAPIのあり方に関する検討会報告書－オープン・イノベーションの活性化に向けて－【中間的な整理（案）】」において，「複数の銀行とAPI接続する企業等における審査対応負担を軽減する観点から，情報セキュリティ関連機関において，銀行がAPI接続先の適格性を審査する際に使用する，必須確認項目と独自確認項目からなる「API接続先チェックリスト」（仮称）を制定することが期待される」と整理された。

こうした整理を受けて，平成29年2月，FISCが事務局となり，「API接続先チェックリストワーキンググループ」（以下「チェックリストWG」という）を設置し，入口の管理フェーズで行われる統制の内容，すなわち，API接続先に対する客観的評価で使用されるチェックリスト（以下「チェックリスト」という）の共通部分に関する検討等を行っている。

オープンAPIは，FinTech検討会におけるタイプⅢの実現方法の１つであることから，チェックリストの検討は，FinTech検討会におけるタイプⅢに関する提言内容と整合的に進められることが必要である。すなわち，タイプⅢにおける「外部委託基準の準用ルール」，及び「必要最低限の安対基準」[79]を踏まえつつ，FinTechに関する安全対策を検討している集団の相互関係を意識した検討が行われることが必要である。

また，FinTech企業の負担軽減の観点から，社会的規範性をもったチェックリストが制定されることが望ましく，そのためには，金融機関，FinTech企業，ITベンダーといったAPI接続に携わる関係者が，合意形成を目指して，チェックリストの検討過程に参画することが望ましい。

チェックリストの制定に当たって，以上の集合的な検討が行われ，その結果として，成果物が取りまとめられた場合には，その成果物は，FinTech検討会の提言内容の一部として取り扱われることとなる。また，環境変化等が生じた場合にも，以上の集合的な検討が行われ，成果物の内容が継続的に見直され，実装・運用されることが期待される。

API接続に携わる関係者においては，その成果物を，有用なものとして，金融機関の実態に応じて利用し，総体的な安全性の確保とイノベーションの両立が目指されることを期待する。

[79]「必要最低限の安対基準」は，API接続先を含む金融関連サービスの提供に携わる事業者において，踏まえられるべき基準としても制定される。その制定までの間は，少なくとも「安全対策遂行能力のうち基礎的な部分」（脚注26）を踏まえて検討されることが望ましい。

４．主な議論（要旨）

チェックリスト WG における主な議論（要旨）は、以下の通り。

・「参照系」（注 1）と「更新系」（注 2）の別は、サービスの内容が個々で、かつ、これから拡がりをみせることから、二者の区別が現段階では難しいこと、また、一律に二者のどちらがリスクが高い又は低いとは断定できない（注 3）ことから、確認項目を分けず、銀行が案件の都度、個別に判断することとする。

・チェック項目は、独自確認項目がたくさんあるよりも、できるだけ共通項目として開示する（その上で、利用する確認項目は案件の都度、銀行が決める）方が、事前に API 接続先が安全対策を準備するのに資するとの考えから、幅広に用意する。

・チェックリストの「セキュリティ対応目標」に対し、「手法例」（注 4）を用意する。目標に対し、単に「○」又は「×」の回答だけではなく、具体的な対応状況を銀行側に伝えることができる仕組みとする。また、「現状」及び「今後の対応状況」欄も設けることにより、銀行及び API 接続先双方の‘コミュニケーション・ツール’としての活用を期待する。

・基本的にチェックリストは銀行が API 接続先を審査する際に使用するリストであるが、二者間の‘コミュニケーション・ツール’を目指す観点から、API 接続先から銀行に確認する項目も含める。また、銀行及び API 接続先の双方にて確認する項目も含める。

・チェックリストは、安全対策関連の機密性に関する確認項目をほぼ網羅し、機密性に関する独自確認項目は基本的にはない想定である。また、利用者保護に関する確認項目は、関係者で合意した項目を掲載する。

・「必要最低限の安対基準」は現時点でまだ決定されていない。決定次第、API 接続に関する実態等も踏まえて、チェックリストの見直しを行う予定とする。

（注 1）「参照系」とは、銀行が API 接続先へデータを提供する場合をいう。

（注 2）「更新系」とは、銀行が API 接続先からデータを受入れる場合をいう。

（注 3）例えば、金額 10 万円の更新系（決済指示）のリスクと、100 万人の顧客情報の漏洩が生じて 1 人 1 千円の慰労金を配布するケース（@1 千円×100 万人=10 億円）におけるリスクを比べた場合、どちらかが高いとは一概に言えないのではないか、との意見があった。

（注 4）当初、チェックリストは「最低限の目線」あるいは「松・竹・梅のようなレベル別の目線」を示す案であったが、これから多様なサービスの拡がりが見込まれる中、現実的な対応としては、複数の具体例を列挙する形式とした。また、「手法例」はあくまで例示であり、いずれかを満たせば、その確認項目のセキュリティ対応目標をクリアしていると一義的に判断できるものではない。

５．関連団体への展開

委員としてチェックリスト WG に参加していない他業態の預金取扱金融機関（以下「関連団体」という）には、チェックリストの位置づけを十分ご理解いただき、参考として利用していただくことを期待する。

（注）関連団体は以下の通り。

- 一般社団法人 全国地方銀行協会
- 一般社団法人 第二地方銀行協会
- 全国信用協同組合連合会
- 農林中央金庫
- 株式会社ゆうちょ銀行
- 一般社団法人 信託協会
- 一般社団法人 全国信用金庫協会
- 労働金庫連合会
- 株式会社 商工組合中央金庫
- 一般社団法人 国際銀行協会

API接続チェックリスト（試行版）

【資料1－3】

平成29年6月28日
API接続先チェックリストワーキンググループ

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
1	情報・セキュリティ管理態勢	セキュリティ管理責任の所在と対象範囲を明確にする	API接続先	＜責任者の設置＞ 1. セキュリティ管理に関する責任者を明確化し、セキュリティ管理の職務範囲を認識している。 2. 情報資産の安全管理に係る業務遂行の総責任者である「情報管理に係る統括責任者」を設置している。 3. 情報資産を取扱う部署における「情報資産管理に係る責任者」を設置している。 ＜体制の整備＞ 4. セキュリティ等の管理体制を整備している（責任範囲対象毎に責任者を任命する）。 ＜統括責任者・責任者の業務＞ 5. セキュリティ管理に係る統括責任者は、情報管理に関する各種対策を実施している(注1)。 6. API利用サービスを所管する部署の「セキュリティ管理に係る責任者」は、情報管理に関する各種対策を実施している(注2)。 (注1)具体例 ①情報資産の安全管理に関する規程及び委託先の選定基準の承認及び周知 ②「セキュリティ管理に係る責任者」及び情報資産利用者に係る「本人確認に関する情報」の管理者の任命 ③「セキュリティ管理に係る責任者」からの報告徴収及び助言・指導 ④情報資産の安全管理に関する教育・研修の企画 ⑤その他事業者内全体における情報資産の安全管理に関すること (注2)具体例 ①情報資産の取扱者の指定及び変更等の管理 ②情報資産の利用申請の承認及び記録等の管理 ③情報資産を取り扱う保管媒体の設置場所の指定及び変更等 ④情報資産の管理区分及び権限についての設定及び変更の管理 ⑤情報資産の取扱状況の把握 ⑥委託先における情報資産の取扱状況等の監督 ⑦情報資産の安全管理に関する教育・研修の実施 ⑧「セキュリティ管理に係る統括責任者」に対する報告 ⑨その他所管部署における情報資産の安全管理に関すること			FISC・安対基準	運3、運4、運5、運6	
2	情報・セキュリティ管理態勢	セキュリティ管理ルールを整備する	API接続先	＜セキュリティ関連文書の整備＞ 1. 情報資産の安全管理措置に係る基本方針・取扱規程を整備している(注1)。 2. 情報資産の安全管理措置、点検および監査に関する規程について定期的に評価・改訂を行っている(注2)。 ＜アクセス管理の実施＞ 3. データ管理者の設置及び顧客データにアクセスできる者の人数とアクセス管理の仕組み、アクセス管理ルールを整備している。 ＜エビデンスの確保＞ 4. 組織文化醸成の中で、セキュリティの文脈も踏まえたディスカッションを経営陣も交えて継続的に実施している。そこでの議論はプレゼン資料やチャット等に残し、エビデンスとして提示している。 5. 業界団体が策定した自主基準に則る前提でセキュリティ運用を行い、業界団体の指導・教育を受けたエビデンスを提示している。 (注1)具体例 ①以下の事項を定めた基本方針の整備 a.事業者の名称 b.安全管理措置に関する質問及び苦情処理窓口 c.安全管理に関する宣言 d.基本方針の継続的改善の宣言 e.関係法令等遵守の宣言 ②各管理段階に係る取扱規程の整備 a.取得・入力段階 b.利用・加工段階 c.保管・保存段階 d.移送・送信段階 e.消去・廃棄段階 f.漏えい事案等への対応の段階 ③情報資産の取扱状況の点検および監査に関する規程の整備 (注2)具体例 ①情報資産の安全管理措置、点検および監査に関する規程を、定期的に評価・改訂を行う			銀行API報告書・セキュリティ原則 --------- FISC・安対基準	3.3.1 API接続先の適格性 d --------- 運1、運2、運10	

API接続チェックリスト（試行版）

【資料1－3】

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
3	情報・セキュリティ管理態勢	セキュリティ管理態勢の定着を図る	API接続先	＜周知・意識啓発の徹底＞ 1. セキュリティ運用に関する周知・注意喚起を全役職員向けメールで行っている。経営者（セキュリティ管理責任者）も宛先に入っており、運用状況の把握を行っている。またメールがログとして後から精査可能な状態としている。 2. 役職員が情報分類の取扱いルールを確認できるよう、イントラネットや社内掲示板等で広く周知している。 3. 役職員向けに個人情報保護に係るトレーニングや意識啓発を図っている。 ＜モニタリングの実施＞ 4. セキュリティ遵守状況を定期的に点検し、改善を行っている。 5. 情報資産を取扱う部署が自ら行う点検体制を整備し、規程違反事項の有無等の点検を実施している(注1)。 6. 取扱規程(に規定する)の規定事項の遵守状況の記録及び確認を行っている。 ＜体制の整備＞ 7. 情報資産の安全管理に係る取扱規程に従った体制を整備し、運用を行っている。 8. 本サービスに関する情報管理ルールを制定し、遵守されるよう運用を行っている。 ＜監査の実施＞ 9. 当該部署以外の者による監査体制を整備し、規程違反事項の有無等の監査を実施している(注2)。 (注1)具体例 ①情報資産取扱部署の点検責任者・点検担当者の選任 ②点検計画の策定による体制整備 ③定期的及び臨時の点検の実施 ④点検の実施後において、規程違反事項等を把握したときは、その改善の実施 (注2)具体例 ①情報資産取扱部署以外からの監査責任者・監査担当者の選任 ②監査計画の策定による監査体制整備 ③定期的及び臨時の監査の実施 ④監査の実施後において、規程違反事項等を把握したときは、その改善の実施			FISC・安対基準	運10-1	
4	情報・セキュリティ管理態勢	役職員に情報管理方法を周知し、セキュリティに対するモラルを高める	API接続先	＜教育・研修の実施＞ 1. 役職員への安全管理措置の周知徹底、教育及び訓練を行っている(注1)。 2. セキュリティ管理に関し、定期的（年1回以上）な勉強会の開催等、周知徹底・教育を実施している。 またその中で、従事する社員が個人的に利用するSNS等インターネット上に、委託業務で知り得た情報の記載をしないことの周知徹底を図っている。 3. 役職員に対する定期的あるいは、必要に応じた教育・研修の実施を行っている。 (注1)具体例 ①役職員に対する採用時の教育及び定期的な教育・訓練 ②提供する情報資産の取扱いに関する研修 ③情報資産の安全管理に係る就業規則等に違反した場合の懲戒処分の周知 ④役職員に対する教育・訓練の評価及び定期的な見直し			銀行API報告書・セキュリティ原則	3.3.3 内部からの不正アクセス対策e	
5	情報・セキュリティ管理態勢	情報資産の取扱態勢を確認する	API接続先	＜情報資産の台帳管理＞ 1. 情報資産に関する台帳等を整備している(注1)。 (注1)具体例 ①取得項目 ②利用目的 ③保管場所・保管方法・保管期限 ④管理部署 ⑤アクセス制御の状況			銀行API報告書・セキュリティ原則	3.3.3 内部からの不正アクセス対策e	
6	情報・セキュリティ管理態勢	役職員との情報資産の非開示契約等の締結・就業規則等における安全管理措置を整備する	API接続先	＜内部役職員の不正対策＞ 1. 役職員等との間で採用時等に情報資産の非開示契約等を締結している(注1)。 2. 就業規則等に「情報資産の取扱に関する役職員の役割・責任や、非開示契約違反時の懲戒処分」を定めている。 (注1)具体例 ①非開示契約（業務上知りえた秘密に関する守秘義務を含む）締結時に、以下内容を含む締結内容を十分に説明している a.非開示義務に反した場合の責任の規定 b.役職員の退職後における非開示義務遵守の規定 ②派遣社員を従事させる場合の、派遣社員本人との契約、覚書、念書等（電子的手段含む）による守秘義務の規定			銀行API報告書・セキュリティ原則	3.3.3 内部からの不正アクセス対策c	

API接続チェックリスト（試行版）

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
7	情報・セキュリティ管理態勢	サービスの解約時およびシステムの廃棄にあたっては機器等から情報漏洩が生じないように防止策が講じられている	API接続先	＜解約時のデータポータビリティ及び消去＞ 1. 解約時のデータの返却有無及び方法を定めている(注1)。 2. サービス解約後のデータ消去の実施有無／タイミング、保管媒体の破棄の実施有無／タイミング、 利用者に所有権のあるデータの消去方法及び第三者証明の有無について事前に取り決めている。 ＜情報資産の廃棄計画＞ 3. 情報資産の廃棄計画を取り決めている(注2)。 (注1)具体例 ①機密情報の完全消去 ②監査権の行使 ③情報システムの廃棄手続きを明確化することで、安全かつ効率的な対応が求められる ④廃棄手続を規定している (注2)具体例 ①廃棄計画の例 a.廃棄の目的 b.廃棄の対象範囲 c.廃棄する時期 d.廃棄する方法 e.計上資産の処分方法			銀行API報告書・セキュリティ原則	3.3.3 内部からの不正アクセス対策 e	
8	情報・セキュリティ管理態勢	セキュリティ不祥事案の発生に対して、振り返りと対策を行う体制を確立する	API接続先	＜不祥事案への対応＞ 1. 過去に発生したセキュリティ関連の不祥事案の内容と対策状況を記録し保管している。 2. 重大な不祥事案については、第三者にて対策や改善状況の妥当性や統制プロセスを評価している。			銀行API報告書・セキュリティ原則	3.3.1 API接続先の適格性 b	
9	情報・セキュリティ管理態勢	セキュリティ管理態勢が整備されていることを客観的に証明する	API接続先	＜認証の取得＞ 1. プライバシーマーク、TRUSTe、ISMS（JIS Q 27001など）、ITSMS（JIS Q 20000-1など）の認証を取得している。 （取得している場合は、認証番号を明記） 2. 内部統制保証報告書〔SOC1（SSAE16･ISAE3402）・SOC2・IT委員会実務指針7号〕または情報セキュリティ監査 報告書を取得している。 （報告書がある場合は、報告書の名称（年次で最新の報告書を確認）を明記） 3. クラウドセキュリティ推進協議会のCSマークやISMSクラウドセキュリティ認証（ISO27017）を取得している。			銀行API報告書・セキュリティ原則 --------- FISC・安対基準	3.3.1 API接続先の適格性 d --------- 運112	
10	情報・セキュリティ管理態勢	不正アクセス発生を想定した対応準備ができている	共通	＜不正アクセス(情報漏えい事案等）発生時の体制整備＞ 1. 不正アクセス発生時における必要な対応については、予め取り決めて明確にしておく(注1)。 2. 関係対応部署（共同で対応する場合等、複数の場合は複数記入のこと）との連絡・社内報告体制を整備している(注2)。 3. 不正アクセスで発生した漏えい事案等の影響・原因等に関する調査を行う体制としている。 4. 再発防止策・事後対策の検討を行う体制としている。 5. 金融機関への報告を行う体制としている。 (注1)具体例 ①双方の連絡先 ②対象利用者を双方で特定・共有する方法 ③関係先への連絡方法・範囲 ④被害拡大を防ぐ対応範囲の確認 ⑤利用者への周知方法 (注2)具体例 金融機関側の連絡先の例： ①コンピュータセンター運営担当者および管理者 ②システム担当者および管理者 ③コンピュータメーカーおよびUPS等の設備関連業者の担当者 ④本部・営業店等への連絡責任者 ⑤外部共同システム（全銀センター、統合ATMシステム、共同CMS等）への連絡責任者 ⑥広報責任者 ⑦本部・営業店等の責任者 ⑧コンピュータセンターへの連絡責任者 ⑨メーカー等の保守部門担当者 ⑩警備会社			銀行API報告書・セキュリティ原則	3.3.4 不正アクセス発生時の対応 c	

API接続チェックリスト（試行版）

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
11	外部委託管理	システム運用における安全性を確保する	API接続先	＜委託先の選定＞ 1. 委託する場合、委託先に対して選定基準を提示している。 2. 委託する際の規程を整備している。 ＜委託契約の締結＞ 3. 委託した業務が安全に遂行されるために、必要に応じて機密保護契約あるいはサービスレベルアグリーメントなどを締結している。 4. クラウドサービスが提供されているデータセンターの所在地、データの保存場所の把握を行い、紛争が生じた際にどの国の法律が適用されるのか、および裁判所がどこであるのかを把握している。 ＜体制の整備＞ 5. システム障害の発生時に備えて、国内、オフショアを含む開発拠点との連絡先や対応体制等を構築している。			FISC・安対基準	運108、運109、運110、運111	
12	外部委託管理	外部委託事業者における委託業務の実施内容に問題がないことを確認する	API接続先	＜委託先の選定＞ 1. クラウドサービスを利用する際に、その事業者を利用して良いか判断するためのチェックシートにてチェックしている。チェックリストでシステム導入時にリスクを評価し、利用可否のチェックを行っている。 ＜委託状況の確認＞ 2. 運用中のリスクについて、クラウドサービスのリスクを洗い出している。 3. 契約時に利用サービスのホワイトペーパーをチェックしている。 4. 保証型監査報告書の内容を検証した結果について、社内の責任者に報告している。			FISC・安対基準	運3、運4、運5、運6	
13	外部委託管理	外部委託事業者における委託業務の実施状況を確認する	API接続先	＜委託状況の確認＞ 1. 外部委託事業者から保証型監査報告書を受領し、内容について説明を受けている。			FISC・安対基準	運89、運90、運91、運112	
14	銀行・API接続先の協力体制	セキュリティ対策の高度化を図る	共通	＜協力体制の整備＞ 1. セキュリティ対策の改善・見直し・高度化に向けて、銀行・API接続先双方で協力して取り組む態勢を整備している。 2. 想定する外部脅威や内部脅威を特定の上、発生したサイバーインシデントを記録するルールを整備している。			銀行API報告書・セキュリティ原則	3.3.4 不正アクセス発生時の対応c	
15	銀行・API接続先の協力体制	利用者からの照会対応を的確に行う	共通	＜利用者からの照会対応＞ 1. 利用者からの相談・照会・苦情・問い合わせがあった場合の役割分担、業務フローをあらかじめ取り決めている。			銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得	
16	銀行・API接続先の協力体制	利用者からの相談等対応を的確に行う	共通	＜利用者への連絡先表示＞ 1. 利用者からの相談・照会・苦情・問い合わせのための連絡先を表示している。			銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得	

API接続チェックリスト（試行版）

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
17	銀行・API接続先の協力体制	利用者の被害拡大を未然に防止する	共通	＜利用者への連絡手段確保＞ 1. 被害拡大の未然防止のために、利用者との連絡手段を予め確保している。			銀行API報告書・利用者保護原則	3.4.4 被害発生・拡大の未然防止	
18	銀行・API接続先の協力体制	利用者の補償対応を的確に行う	共通	＜利用者への補償対応＞ 1. 不正アクセスや不具合などが原因で、利用者に損害が生じた場合の補填・返金方法、補償範囲について予め取り決めている。 2. API接続先とAPI接続先が利用するクラウド事業者間での事故責任の範囲と補償範囲が記述された文書の有無、有る場合はその文書名称、損害賠償保険加入の有無を確認している。			銀行API報告書・利用者保護原則	3.4.5 利用者に対する責任・補償	
19	銀行・API接続先の協力体制	利用者向けの補償対応窓口を的確に運営する	共通	＜利用者への補償窓口対応＞ 1. 利用者に対する補填・返金方法とその補償範囲について、ウェブサイト等にて利用者が常時確認できるように表示したり、利用者が補償・返金を求める対応窓口やその方法について十分認識できるようにしている。			銀行API報告書・利用者保護原則	3.4.5 利用者に対する責任・補償	
20	コンピュータ設備管理	コンピュータ設備面での情報漏洩対策を行う	API接続先	＜クラウドサービスの活用＞ 1. 各種第三者認証機関による認証を得たクラウドサービス事業者のサービスを利用し、コンピュータ設備面でのセキュリティ態勢を担保している。 ＜設備環境の確認＞ 2. 重要な物理セキュリティ境界の出入口に破壊対策ドアを設置している。 3. コンピュータ室及びラックの施錠・鍵管理（入退室に鍵・カード・暗証番号要）を実施している。 ＜コンピュータリソース配置＞ 4. コンピュータリソースを執務室に設置する場合、施錠されたラックに格納されており、ケーブル類にも簡易にはアクセスできないようになっている。 5. コンピュータリソースをコンピュータセンターに設置している。					
21	コンピュータ設備管理	サーバルームに不正な人物の入室を防ぎ、セキュアなネットワークへの侵入や、業務情報の漏洩を防ぐ	API接続先	＜内部役職員の入退室・アクセス管理＞ 1. 各種第三者認証機関による認証を得たクラウドサービス事業者のサービスを利用する等、コンピュータ設備面でのセキュリティ態勢を担保している(注1)。 2. 情報資産の取得・入力段階、利用・加工段階、保管・保存段階において、以下のアクセス制御策を講じている(注2)。 3. 監視カメラについては、監視カメラ稼働時間、監視カメラの監視範囲、映像の保存期間を提示している。 4. 個人認証システムと連動した物理的入退出装置（ドア・柵等）を設置している。 5. 受付・警備員を常駐させている。 (注1)具体例 ①コンピュータ室に設置する場合 a.部屋が専用室であり、施錠管理（入退室に鍵・カード・暗証番号要）を実施している ②執務室に設置する場合 a.施錠されたラックに格納されており、ケーブル類にも簡易にはアクセスできないようになっている ③コンピュータセンターに設置している (注2)具体例 ①入館（室）者による不正行為の防止のための、業務実施場所及び情報システム等の設置場所の入退館（室）管理の実施（例：入退館の記録の保存など） ②盗難等の防止のための措置 （例：カメラによる撮影や作業への立会等による記録またはモニタリングの実施、記録機能を持つ媒体の持込み・持出し禁止または検査の実施など）			銀行API報告書・セキュリティ原則	3.3.3 内部からの不正アクセス対策e	

API接続チェックリスト（試行版）

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
22	コンピュータ設備管理	政治状況、法規制の変化に対応しやすい状況下におく	API接続先	＜データに関する確認＞ 1. データセンター所在地（含む隔地保管）を把握し、リスク・制約がないことを確認している(注1)。 ＜海外法規制の確認＞ 2. 開発担当国の規制等を考慮して開発されたシステムを他国の拠点で利用する場合、利用拠点国の規制に水準が合わないリスクが存在するため対策が必要。利用各国の金融当局ガイドラインを調査し、リスク・制約がないことを確認している。 ＜クラウドサービスの活用＞ 3. 各種第三者認証機関による認証を得た、クラウドサービス事業者のサービスを利用し、コンピュータ設備面でのセキュリティ態勢を担保している。 (注1)具体例 ①国名（日本の場合は地域ブロック名（例：関東、東北））、全データ経由国の名称 ②データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する解約条件の有無 ③日本の個人情報を取り扱う場合は、個人情報保護法を踏まえた個人情報の管理態勢になっていることを確認する					
23	オフィス設備管理	執務室に不正な人物の入室を防ぎ、セキュアなネットワークへの侵入や、業務情報の漏洩を防ぐ	API接続先	＜アクセス制御策の実施＞ 1. 情報資産の取得・入力段階、利用・加工段階、保管・保存段階において、以下のアクセス制御策を講じている(注1)。 (注1)具体例 ①入館（室）者による不正行為の防止のための、業務実施場所及び情報システム等の設置場所の入退館(室)管理の実施 （例：入退館の記録の保存、保存期間など） ②盗難等の防止のための措置 （例：カメラによる撮影や作業への立会等による記録またはモニタリングの実施、記録機能を持つ媒体の持込み・持出し禁止または検査の実施など） ③執務室が他社と同居するビルの場合は、エレベータ・階段から直接入れる位置には設置しない （設ける場合は、事務室等の前室を設けること）これらの設備がある上下階は危険が多いので避ける					
24	オフィス設備管理	重要情報にアクセスできる人間を制限する	API接続先	＜入室制限の実施＞ 1. 重要情報を格納した機器を保管している部屋への入室を制限している(注1)。 (注1)具体例 ①重要な物理的セキュリティ境界からの入退出を管理するための手順書を作成している ②他社と同居するビルの場合は、エレベータ・階段から直接入れる位置には設置しない （設ける場合は、事務室等の前室を設けること） ③これらの設備がある上下階は危険が多いので避ける					

API接続チェックリスト（試行版）

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
25	オフィス設備管理	内部関係者による情報漏洩の出口対策を行う	API接続先	＜情報資産の書込禁止・持出制限＞ 1．PCは、外部記憶媒体やスマートデバイスを介した通信手段(テザリング）による情報漏えいリスクへの対策を講じている(注1)。 2．システムに保有する情報資産(電子データ)の取扱状況を管理している(注2)。 3．社内規程に基づきパソコンの管理（情報資産の漏えい、き損等防止策）を行っている(注3)。 4．媒体の保管を行っている(注4)。 5．情報資産の書出し・持出し等の管理を厳格に行っている(注5)。 (注1)具体例 ①管理者によるレジストリ設定でUSBの書き出し制限を実施している ②書出し制御SWによる制限（MTP転送対策制限、テザリング制限含む） ③物理的な媒体挿入口ロック装置(FDD用鍵など)を設置 ④封印シール(封印確認およびシール在庫管理要） ⑤電子メールのルール違反のモニタリングの実施、および重要情報送信に対しての盗聴・改竄などを考慮すること ⑥業務用メールの運用規程を策定すること (注2)具体例 ①記録媒体への書き出しが可能な場合、書き出し行為に関する制御を行っている （例：システムによる許可制、ログ取得および事後監査USB鍵等による封印、USBポートの無効化など。 また自らの行為を自らが承認できない仕組みとなっていること） ②オンラインストレージの利用が可能な場合（＊）、アップロード行為に関する制御を行っている （利用権限付与制や、ログ取得と監査等） ＊…インターネット接続がない場合や、webフィルタリングにより接続不可等の場合は本項目は「対象外」 (注3)具体例 ①次に掲げる措置により、情報資産の保護策を講じている a.私有PC、私有記録媒体等の執務室内における持込禁止や、機器の接続の制限 b.業務で使用するPCへの無断インストール禁止 ②情報資産の漏えい等のため、以下の監査またをは措置等行っている a.電子メールでの自己の個人保有PCアドレスへの業務情報の送信禁止 b.送信メールに対する監査の実施、または本サービスにて取得する情報が電子メールにて送信できないようなシステム制御 (注4)具体例 ①紙、磁気テープ、光メディア等の媒体の保管手順書及び保管方法 ②紙、磁気テープ、光メディア等の媒体の廃棄手順書有無及び廃棄方法 (注5)具体例 ①可搬性媒体への書き出しを機能的に禁止 ②外部WEBへの不正な情報持ち出しを禁止 ③メール経由での不正な情報持ち出しを禁止 ④可搬性媒体への書き出しを機能的に抑止 ⑤外部WEBへの不正な情報持ち出しを監視・抑制 ⑥メール経由での不正な情報持ち出しを監視・抑制			銀行API報告書・セキュリティ原則 ＿＿＿＿＿＿ FISC・安対基準	3.3.3 内部からの不正アクセス対策e ＿＿＿＿＿＿ 技43	
26	オフィス設備管理	ウィルス感染によるシステム侵入等の攻撃を防ぐ	API接続先	＜ウイルス対策の実施＞ 1．業務利用しているPC等にウィルス対策ソフトが導入され、パターンファイルが随時更新されている他、可搬性記憶媒体にウィルスチェックを行っている。 2．メール、ダウンロードファイル、サーバー上のファイルアクセス及び運用管理端末に対するウイルスチェックを行っている(ウイルス対策ソフト名、パターンファイルの更新間隔を提示）。 3．ウィルス感染を検知した場合の対応手順を定め、定期的に見直しを行っている。 4．ウィルス感染を検知した場合の対応手順を、システム復旧プランに明記し、定期的(年1回以上）に見直しを行っている。			銀行API報告書・セキュリティ原則	3.3.2 外部からの不正アクセス対策t	

API接続チェックリスト（試行版）

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
27	システム開発・運用管理	システムアクセスできる担当者の権限を適切に設定して、不正な作業を防ぐ	API接続先	＜役割・責任に応じたアクセス権限の設定＞ 1. 役職員の役割・責任に応じた管理区分及びアクセス権限の設定について以下の通り実施している(注1)。 2. アクセス権限に応じた各種IDはアクセス管理ルールを定め以下を例に適切な管理を行っている(注2)。 (注1)具体例 ①アクセス権限所有者を特定し、漏えい等の発生に備えアクセスした者の範囲が把握できるような対応の実施 ②事業者内部における権限外者に対するアクセス制御 ③データ管理者の設置及び顧客データにアクセスできる者の人数とアクセス管理の仕組み・アクセス管理ルールを制定 (注2)具体例 ①特権ID(Admin権限) a.原則、システム開発・運用時において使用することのない権限として管理し、社内のごく限られたメンバーに限定した管理とする ②運用ID a.運用部門・開発部門からの依頼書によって、運用部門にてIDを作成している b.開発・運用部門の不正を防止するため、開発部署、運用部署を分離独立している体制が望ましい					
28	システム開発・運用管理	システムアクセスに際しての特権権限の付与を可能な限り限定して、不正な作業、誤った作業の発生を防ぐ	API接続先	＜アクセス管理の実施＞ 1. データ管理者の設置及び顧客データにアクセスできる者の人数とアクセス管理の仕組み・アクセス管理ルールを制定している。 2. 情報資産へのアクセス権限を付与する役職員数を必要最小限に限定するとともに、役職員に付与するアクセス権限を必要最小限に限定している。 ＜特権IDの管理＞ 3. 特権IDについては、原則、システム開発・運用時において使用することのない権限として管理し、社内のごく限られたメンバーに限定した管理としている。 4. root、Administratorなど特権IDの付与が、セキュリティの管理責任者（部長級）の権限としている。 5. 特権IDにおいて、アクセス権限の変更が行われた場合は、当日中にセキュリティの管理責任者（部長級）あるいはセキュリティの管理者がモニター出力等で、変更結果を確認している。			FISC・安対基準	運18	
29	システム開発・運用管理	システムアクセス時の認証を適切に行い、不正なシステムアクセスを防ぐ	API接続先	＜本人確認の実施＞ 1. 情報資産の利用者の識別及び認証にあたり、以下の措置を講じている(注1)。 ＜関連規程や本人確認方法の構築＞ 2. IDやパスワード（暗号鍵含む）の運用管理方法の規程を制定している。 3. ユーザー（利用者側）のアクセスを管理するための認証方法、特定の場所及び装置からの接続に限定して接続・認証する仕組みを構築している。 ＜ID・パスワードの管理＞ 4. 本人確認に関するパスワード総当り攻撃によるID悪用を防止している(注2)。 5. 埋め込みIDのパスワードが漏洩しないための対策を行っている(注3)。 6. DB内やシェル内、プログラム間にて使用するIDは、人が利用するIDとは別の管理としている(注4)。 7. システムログイン時のパスワードについて、十分推測されにくい文字数、文字種類とする運用とすることでパスワードの漏洩を防いでいる。 8. システムログイン時のパスワードを、申請・承認による都度発行とし、その申請作業内のみの有効期限を設定している。 ＜証明書による認証＞ 9. 証明書による認証とし、端末とその端末を利用できる担当者の認証を行っている。 10. ログイン時にワンタイムトークンを利用する多要素認証としている。 ＜ネットワークの限定＞ 11. 接続端末について一般的なネットワークアクセスを不可とし、接続元ネットワークを限定している。 (注1)具体例 ①本人確認機能の整備 ②本人確認に関する情報の不正使用防止機能の整備 ③本人確認に関する情報が他人に知られないための対策 (注2)具体例 ①情報システムに対してパスワード入力を連続して一定回数失敗した場合は一時的に使用不可とする機能を設ける (注3)具体例 ①プログラムや運用ジョブ内で使用するパスワードが見られないための対策を実施する (注4)具体例 ①システム用のIDとしてログイン禁止とすることで、運用面での不正防止を強化することが求められる			FISC・安対基準	運17、技26、技35、技45	

API接続チェックリスト（試行版）

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
30	システム開発・運用管理	システムアクセスとその作業についてのログを保管し、有事の際に調査が可能なようにする	API接続先	＜情報資産へのアクセス記録＞ 1. 情報資産へのアクセスを記録するとともに、当該記録の分析・保存は以下の通りに実施している(注1)。 ＜ログ情報の提供＞ 2. 利用者の利用状況、例外処理及びセキュリティ事象の記録（ログ等）を利用者に提供している。 （記録（ログ等）はその種類及び保存期間） (注1)具体例 ① 情報資産へのアクセス及び情報資産を取扱う情報システムの稼動状況についての記録・分析 （例：ログインとログオフの状況、不正なアクセス要求、システムによって失効とされたIDなど(注2)） ② 取得した記録について、漏えい等防止の観点から適切な安全管理措置を実施 ③ 取得した記録について、特に漏えいリスクの高い時間帯(例:休日や深夜時間帯等)におけるアクセス頻度の高いケースについて重点的な分析を実施 (注2)具体例 ①システムログを取得し、内容を確認している ②業務IDを保有しておらず、運用IDについてはパスワード管理システムとアクセス実績管理システムによるアクセス履歴管理を実施している ※システムログの取得・・・OS機能や業務アプリケーションにて作業結果を記録 ③望まれる水準の例： a.OS、ミドルウェアの起動と終了がログに記録される、監視画面に上がる b.OS、ミドルウェアへのログインが記録される（成功/失敗/ログアウト） c.ユーザ環境からのアプリケーションの操作日時が記録される d.以下の内容が記録されること－OS起動/終了,DBMS起動/終了、ミドルウエア起動/終了、ディスク装置や論理ボリュームのマウント/アンマウント、ログ取得プログラムの起動/停止 ④ログの取得と対応するIDについて ログ取得の対象となるIDとリスク評価項目の(a)(b)について整理すると以下のとおり これらについてログ取得されているかを評価する a.OS、ミドルウェアの起動終了・・・運用IDによるコマンド操作およびOSイベント等のログが対象 b.ログインの成功失敗・・・・・・・・・・業務利用（顧客利用含む）時のログイン、運用IDでのOS、ミドルウェアへのログインおよびそれらのログアウトが対象 c.ログトレース用の日付と時刻（タイムサーバーによる時刻同期） d.アカウント管理・・・・・・・・・・・・・・・業務ID（顧客ID含む）および運用IDの登録、修正、失敗のログが対象			FISC・安対基準	技37	
31	システム開発・運用管理	担当者単独のシステムアクセスの発生を抑止し、不正な作業を防ぐ	API接続先	＜単独作業の防止＞ 1. ログイン時に部署内に自動全体周知されるのと、ログイン前に作業内容を事前全体周知することで、部署内のメンバーが作業内容を確認できる運用を行い、単独作業による不正を抑止している。 2. 常に、申請・承認ベースの作業とすることで、単独作業が発生しない状態を作っている。 ＜改ざん防止対応＞ 3. 顧客宛に表示するデータについて、利用部署、担当者による改ざんを防止する対策（ユーザーを特定可能とする体系、出力制限、出力記録、保管・廃棄方法の明確化）が講じられている。					
32	システム開発・運用管理	システム変更の単独作業を抑止し、不正なシステム変更を防ぐ	API接続先	＜単独作業の防止＞ 1. 申請・承認ベースのシステム変更作業とすることで、単独作業を抑止している。 2. ソースコードの変更をリポジトリに反映させる際に、必ず他者の承認を必要とする運用とすることで、単独作業を抑止している。 ＜第三者監査の実施＞ 3. 外部監査や部内検査を定期的（年1回以上）に実施し、不正な行為を排除できる運用となっている事を確認している。					
33	システム開発・運用管理	システム変更時に著しく品質が低下しないような対策を行う	API接続先	＜システムの品質確保＞ 1. ソースコードの変更をリポジトリに反映させる際に、自動テストを行うことで不測の品質低下を防いでいる。 2. システム変更時には必ずシステム停止を行い、打鍵確認による品質チェックを行っている。					

API接続チェックリスト（試行版）

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
34	システム開発・運用管理	システム変更に伴う脆弱性の埋め込みや、利用技術に対する脆弱性発覚に対する対策を行う	API接続先	＜脆弱性テスト・侵入テストの実施＞ 1．以下の通りに脆弱性テスト・侵入テストを実施している(注1)。 2．以下の場合にネットワークの脆弱性テストを実施している(注2)。 (注1)具体例 ①脆弱性テスト/侵入テスト等の第三者(専門業者)による診断の対象範囲（アプリケーション、OS、ハードウェア等） ②ツールベースの自動脆弱性テスト ③脆弱性テスト・侵入テストの実施インターバル（第三者診断は年1回、ツールは日次等） ④テスト結果の報告頻度、テストの結果から対策が必要となった部分に対する対応を実施 (注2)具体例 ①インターネットを利用してお客さまのパソコンからサービスを利用する ②インターネットVPNを使用して、特定のお客さまにサービスを提供する ③専用線を介してお客さまにサービスを提供する					
35	システム開発・運用管理	システムに対する外部からの不正な通信を検知する	API接続先	＜不正アクセス対策の実施＞ 1．WAFなどの導入によって、改ざん検知や不正侵入検知を行っている(注1)。 2．脆弱性による不正アクセスを防止している(注2)。 3．外部からの不正アクセスに対して、以下の防止措置を実施している(注3)。 (注1)具体例 ①インターネット接続のWebサイトで、ファイアウォールでステートフルインスペクション機能チェックを行い、DMZ内にWAF（Webアプリケーションファイアウォール）を設置している ②専用線接続でWebサーバ公開をおこなっており、ファイアウォールでのステートフルインスペクション機能チェックを行っているが、DMZ内にWAFは設置せずWebアプリケーションのセキュアコーディングで対応し、Web診断で脆弱性対策を確認している (注2)具体例 ①ファイアウォールやサーバーを新たに設置する場合やネットワークに大規模な変更を行なった場合は、ネットワーク構成や設定条件等を評価し、事前に脆弱性の有無を検査する (注3)具体例 ①アクセス可能な通信経路の限定 ②外部ネットワークからの不正侵入防止機能の整備 ③不正アクセスの監視機能（IDS/IPS）の整備（シグニチャ（パターンファイル）の更新間隔：〇〇） ④ネットワークによるアクセス制御機能の整備 （セキュリティ監視装置の設置・インターバルは〇〇）			銀行API報告書・セキュリティ原則	3.3.2 外部からの不正アクセス対策y	
36	システム開発・運用管理	システムに対する外部からの不正な通信を防ぐ	API接続先	＜ファイアウォール等の設置＞ 1．ファイアウォール等の設定により、外部からの不正な侵入を防ぐ措置を講じている。 2．外部からの不正アクセスに対して、以下の防止措置を用意している(注1)。 （注1）具体例 ①アクセス可能な通信経路の限定 ②外部ネットワークからの不正侵入防止機能の整備 ③不正アクセスの監視機能の整備 ④ネットワークによるアクセス制御機能の整備 ⑤ファイアウォール、リバースプロキシ設置等の不正アクセスを防止する仕組み及びファイアウォールの縦列多重化、アプリケーションへの攻撃対策			銀行API報告書・セキュリティ原則	3.3.2 外部からの不正アクセス対策t	

API接続チェックリスト（試行版）

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
37	システム開発・運用管理	システムで利用する技術で発覚する脆弱性に対する対策を行う	API接続先	＜脆弱性対策の実施＞ 1. 外部公開しているサーバーについて、セキュリティパッチ適用などの脆弱性対策を行っている。 2. セキュリティ診断・監査等を行っている(注1)。 3. ネットワーク関連機器の管理を行っている(注2)。 4. ソフトウエア管理を行っている(注3)。 5. セキュリティパッチの適用を行っている(注4)。 ＜サイバー脅威関連情報の収集＞ 6. 日頃からメーカー、セキュリティベンダー、外部団体（金融ISAC、JPCERT、警視庁、JC3等）等より、サイバー脅威情報を収集し、適切な分析（自社システムへの影響、即時対応が必要であるかの判断、過去に収集済みの情報で何等かの対応を行った履歴があるか）を行っている。 (注1)具体例 ①定期的に外部の専門会社等に委託してWebアプリケーション検査およびネットワーク検査を実施する a. 不正な侵入や、DoS攻撃への耐久性を診断 b. 侵入された際にそこを踏み台にして他のネットワークを攻撃できるかどうかを診断 c. Web診断とプラットフォーム脆弱性診断（外からF/W、内部ネットワーク内）の実施 (注2)具体例 ①外部ネットワークと接続しているシステムにおいて、不要なポートを閉じておいたり、常時使用していない機器（含むネットワーク機器)の電源を切断してアクセス経路を必要最小限にするなど、不正アクセスの防止策を講じる ②インターネットからの接続が可能となるサーバ上で稼動するネットワークサービスは、必要最小限とし、外部からの侵入手段を制限している （TELNET, rlogin, rsh, rexec, FTP, RFS, NFS等リモートでサーバを操作することが可能となるサービスは無効とする。 またSMTP等の上記以外のサービスについても、システムの機能上不必要である場合は無効とする等の対応を行なう） (注3)具体例 ①不正アクセス、マルウェア対策のため、SWの適切な管理 ②サポート停止となったOSやミドルウェア等を使用していない (注4)具体例 ①サーバー・運用管理端末へのセキュリティパッチの適用方針（ベンダーリリース情報収集の仕組み、ベンダーリリースからパッチ更新開始までの時間）を定める ②パッチ情報の適用可否については、パッチの重要度に応じて決定し、CVSS(Common Vulnerability Scoring System)深刻度レベル3のパッチは漏れなく適用している ※CVSS深刻度レベル3とは、以下のようなものをいう リモートからシステムを完全に制御されるような脅威、・大部分のデータを改ざんされるような脅威、 例えば、OSコマンド・インジェクション、SQLインジェクション、バッファオーバフローによる任意の命令実行など			銀行API報告書・セキュリティ原則	3.3.2 外部からの不正アクセス対策t	
38	システム開発・運用管理	機密情報へのアクセスを制限して、不正な作業、誤った作業の発生を防ぐ	API接続先	＜ユーザーID管理＞ 1. 役職員に対してシステムアクセス権限を割り当てる場合は、必要最小限に限定している。アクセス権限は、業務プロセスの職務分離に応じたアクセス権限を適切に付与している。 2. アクセス権限の登録・登録変更・削除の正式な手順を制定している。 3. 役職員の異動、退職等変更がある場合は、異動・退職後速やかに削除等の手続きを行っている。 4. アクセス権限設定・監理として、次に掲げる措置等を講じている(注1)。 5. ユーザー（利用者側）のアクセスを管理するための認証方法、特定の場所及び装置からの接続に限定して接続・認証する方法等を導入している。 (注1)具体例 ①各管理段階における情報資産の取扱いに関する役職員の役割・責任の明確化 ②情報資産の管理区分に応じたアクセス権限の設定 ③ユーザーIDは原則個人単位に設定し、共有しない ④退職や異動により不要となったユーザIDがないか、役割や職責に応じたアクセス権限が適切に付与されているかを定期的に確認する ⑤必要に応じた規程等の見直し			銀行API報告書・セキュリティ原則	3.3.3 内部からの不正アクセス対策e	

API接続チェックリスト（試行版）

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
39	システム開発・運用管理	問題発生時の原因・経緯を特定可能な状態にして、不正アクセスを抑止する	API接続先	＜情報資産へのアクセスを記録、当該記録の分析・保存＞ 1. 情報資産へのアクセス及び情報資産を取扱う情報システムの稼動状況についての記録・分析。 （例：ログインとログオフの状況、不正なアクセス要求、システムによって失効とされたIDなど） 2. 取得した記録について、漏えい等防止の観点から適切な安全管理措置を実施。 3. 取得した記録について、特に漏えいリスクの高い時間帯(例:休日や深夜時間帯等)におけるアクセス頻度の高いケースについて重点的な分析を実施。 ＜ログによる運用ID・特権IDの使用履歴確認＞ 4. 開発/運用部署での運用ID（本番アクセス時の運用ID、特権ID）の使用について、異例扱いや特権ID利用の申請に無い操作が操作ログ上に無いことを検証している(注1)。 5. 休日や深夜時間帯等の漏洩リスクが高い時間帯におけるアクセス等を分析し検証している(注2)。 ＜情報資産を取り扱う情報システムの監視及び監査＞ 6. 情報資産を取り扱う情報システムの利用状況及び情報資産へのアクセス状況を監視している。 7. 監視状況についての点検及び監査を行っている。 (注1)具体例 ①アクセス実績の検証例：ログが還元される、ログを(本番アクセスすることなく)参照可能である、異常時に監視画面に上がる ②「検証」の例:不審なアクセスがないかログを目視確認している ③アクセスログの記録・保存し、特定条件のログ出力を検知して周知運用を行う ④アクセスログの記録・保存、定期的な査閲を行う (注2)具体例 ①アクセス実績の検証例：ログが還元される、ログを(本番アクセスすることなく)参照可能である、異常時に監視画面に上がる ②「検証」の例:不審なアクセスがないかログを目視確認している			銀行API報告書・セキュリティ原則	3.3.3 内部からの不正アクセス対策e	
40	システム開発・運用管理	持ち出された機密情報を適切に管理する	API接続先	＜情報の持出・削除・廃棄管理に関する取扱＞ 1. 重要な機密情報・顧客情報の可搬性媒体へのデータコピーの持ち出し・削除・廃棄管理をログで記録し、定期的に査閲している。 2. 廃棄を業者に依頼する場合は、業者間との契約ならびに社内ルール（一般物と機密情報の分類等）に則り実施している。 ＜管理方法の取決め＞ 3. 電子記憶媒体の入手・作成、利用、複製、保管、持出し、廃棄など現物管理全般についての管理方法（管理簿の作成など）を取り決めている。			銀行API報告書・セキュリティ原則	3.3.3 内部からの不正アクセス対策e	
41	サービスシステムのセキュリティ機能	データの種類・内容に応じた管理策を実施する	API接続先	＜データの管理レベルの設定＞ 1. 自サービスで取り扱われるデータの内、公開されるべきではないデータを列挙可能で、それらに対して求められるべきセキュリティレベルを整理している。			銀行API報告書・セキュリティ原則	3.3.2 外部からの不正アクセス対策y	

API接続チェックリスト（試行版）

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
				＜安全管理措置の実施＞ 1. クレジットカード番号やパスワード等の機密性の高いデータを取り扱う場合、そのデータを安全に通信・保管するための仕組みを導入している(注1)。 ＜データの保護・管理＞ 2. コンピュータ機器内や外部媒体に個人情報、認証方法等重要なデータを蓄積する場合、暗号化またはパスワードによる保護を行っている(注2)。 3. お客さまが使用するパスワードや暗証番号、乱数表部分の全てのデータをハッシュ化している(注3)。 4. 一時的に生成されるファイルに重要情報が含まれる場合、暗号化されていない状態の情報が漏えいするリスクが存在するため、対策が求められることから、一時ファイルが不要になった時点で消去する機能を設けている。 5. DB内やシェル内、プログラム間にて使用するIDは、運用IDとは別の管理としている。 6. 運用部署は、開発部署の管理者の承認を確認したうえでデータの参照許可や引渡しを実施している。 7. 情報資産の保護策を講じている(注4)。 ＜暗号化処理＞ 8. 暗号化アルゴリズム、チェックデジット仕様、認証仕様、個人情報マスキング仕様などの秘匿性の高い重要プログラムは、開発担当者以外の者が使用、参照できない手段を講じている。 9. 暗号鍵は、システム部門の担当者でも参照できないような対策と期日管理など厳正な管理を行っている。暗号鍵は厳重な管理・保管を行っている。また暗号鍵の生成、配布、保管、失効、更新、廃棄に関する作業手順を定めている。 10. 回線の暗号化有無と暗号化している場合の暗号化方法（プロトコル・暗号化方式等）と強度（暗号化キーの長さ等）を管理している。 ＜不正アクセス検知＞ 11. IDS（侵入検知システム）/IPS（侵入防止システム）を導入し、管理者が定期的にモニタリング・分析できる仕組みとしている。 12. 社内のシステム利用者による大量顧客データ漏えいリスクを検知する対策を実施している。 13. 顧客情報のダウンロード実績を取得し、不審な利用がないか検証する機能を設ける等不正アクセスが無いことを確認している。 14. 第三者による悪用を検知するため、当該IDによる前回アクセスの日時、状況等のログオン履歴情報を当該IDのユーザーに提供している。 （パスワード使用者にログイン情報履歴を提供している）					
42	サービスシステムのセキュリティ機能	機密性の高いデータの漏洩対策がとられている	API接続先	＜テストデータの取扱い＞ 15. テストに利用する本番データに含まれる顧客情報について、マスキング等により、顧客を特定できない形式に変更する手続を定め、実施している(注5)。 16. 開発者による本番データの参照や借用（開発・テストでの利用）は、例外運用であり、厳格な管理下で実施し、情報漏洩等の事故が発生しないよう細心の注意を払って運用している。 17. 本番環境以外で使用する場合は、取引先情報の漏えい防止策として、取引先を特定可能なデータ項目、マイナンバーおよびクレジットカード番号をマスク化している。 (注1)具体例 ①データ保管時に暗号化する ②パスワードやクレジットカード番号など機密性の高い情報を画面などに表示する場合は、一部をマスクする ③パスワードやクレジットカード番号など機密性の高い情報がログなどに出力されないようにする ④暗号化通信を用いることで通信傍受を防ぐための対策を行っている (注2)具体例 ①データベース：DBMSの備えるパスワード設定 ②文書ファイル：文書そのものまたは格納フォルダにかけるパスワード設定 ③ハードディスク：ハードディスクドライブの暗号化機能の実施またはパスワード設定 ④バックアップデータ：暗号化機能の実施またはパスワード設定 (注3)具体例 ①ハッシュ化推奨だが暗号化でも可、②二要素認証の場合は両方対象、③暗号アルゴリズムはNST推奨暗号等を使用している (注4)具体例 ①ファイルの不正コピーや盗難の際にも情報資産の内容が分からないようにするための蓄積データの漏えい防止措置 ②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伝送データの漏えい防止策 ③コンピュータウイルス等不正プログラムへの防御対策 ④記録媒体もしくは電子ファイル形式で保存・保管する場合、パスワード・暗号化等の措置を講じている ⑤データの暗号化方法（暗号化方式等） (注5)具体例 ①手続には以下の条件を含むこと a.承認権限がセキュリティの管理責任者（部長級）になっていること b.アクセスできる要員を必要最小限とすること c.データの消去・廃棄管理要領を定めていること			銀行API報告書・セキュリティ原則	3.3.2 外部からの不正アクセス対策t	

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
43	サービスシステムのセキュリティ機能	情報喪失・破損からの復旧を可能とする	API接続先	＜バックアップの実施＞ 1. データのバックアップと、その世代管理、復旧手段の確保を行っている。 2. バックアップにあたっては以下の措置により、障害発生時の技術的対応・復旧手続を整備している(注1)。 3. 早期復旧が不可能な場合の代替措置（別サイトからのバックアップデータの提供有無やデータ形式等）を制定している。 (注1)具体例 ①不正アクセスの発生に備えた対応・復旧手続の整備 ②コンピュータウイルス等不正プログラムによる被害時の対策 ③リカバリー機能の整備			銀行API報告書・セキュリティ原則	3.3.2 外部からの不正アクセス対策 t	
44	サービスシステムのセキュリティ機能	必要な認証機能を適切に把握できている	API接続先	＜認証機能の管理＞ 1. 自サービスが提供する認証機能がどのような役割を果たしており、それを前提としたサービスとなっている場合、その構成が整理されている(注1)。 (注1)具体例 ①自社サービス内で提供している重要な機能（例：銀行情報の照会、銀行振込、等）について、その利用のためにどのような認証（例：ID/PW＋ワンタイムトークン）をエンドユーザに対して課しているかを漏れなく整理し、認識している					
45	サービスシステムのセキュリティ機能	ユーザを保護する適切な認証機能を見直す	API接続先	＜認証機能の見直し＞ 1. 認証を前提とした機能がある場合、その認証が求められるセキュリティレベルに応じて適切な状態であることを確認する仕組みを整備している(注1)。 (注1)具体例 ①認証レベルが劣化することの把握 a. 例：ID/PW認証やソーシャルログインを始め、自サービスにログイン可能な全ての認証方式を網羅・整理しており、それらの方式に脆弱性が無いことを定期的に確認している					
46	サービスシステムのセキュリティ機能	ユーザを適切に保護する認証機能を提供する	API接続先	＜認証機能の提供＞ 1.ユーザを適切に保護する認証機能を提供している(注1)。 2.セキュリティ事故の発生を想定して以下の対策を行っている(注2)。 (注1)具体例 ①最低限やるべき項目 a.PW入力を一定回数間違うとアカウントロック b.PW文字数の最低数制限 ・パスワード変更は利用者本人および管理者が画面から行い第3者（オペレータ等）を介さない ・Windowsの場合、パスワードポリシー設定で「複雑さの要件を満たす必要があるパスワード」の設定がされている場合、要件を満たすと評価してよい ②サービスのリスクに応じてやるべき項目 a.ログイン履歴の確認画面の提供 b.2段階認証 c.リスクベース認証 (注2)具体例 ①不正認証検知の仕組み（リスト型攻撃への対策） ②システム脆弱性検知の仕組み					

API接続チェックリスト（試行版）

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
47	サービスシステムのセキュリティ機能	スマートデバイス利用時の顧客保護として、動作するアプリケーションに対して、不正な偽アプリケーションが出回らないよう、必要な対策を実施している	API接続先	＜アプリケーションの管理＞ 1．スマートデバイス利用時の顧客保護として、動作するアプリケーションに対して、不正な偽アプリケーションが出回らないよう、必要な対策を実施している(注1)。 (注1)具体例 ①配布時に電子署名を付与 ②アプリに対する署名の検証など、偽のアプリによるシステムアクセスを防止する ③スマートフォンアプリをリバースされた場合でも、暗号化キーや個人情報を抽出できない対策を行う					
48	サービスシステムのセキュリティ機能	不正アクセス時の被害拡大を最小限に止める	共通	＜不正アクセスの拡大防止＞ 1．不正アクセス検知後、サービス利用の制限、停止を行うことができる運用体制を整備している。			銀行API報告書・セキュリティ原則	3.3.4 不正アクセス発生時の対応 a	
49	サービスシステムのセキュリティ機能	不正アクセス発生時に追跡調査を実施する	共通	＜ログの記録・保存＞ 1．不審な資金移動等に関する利用者からの照会対応や、不正アクセス発生時の原因調査・対策の検討のため、アクセスログを記録・保存している(注1)。 2．利用者の利用状況、例外処理及びセキュリティ事象の記録（ログ等）取得の有無と利用者への提供。 （ログ種類：〇、保存期間：〇） (注1)具体例 ①システムログを取得し、内容を確認している ②パスワード管理システムとアクセス実績管理システムによるアクセス履歴管理を実施している ※システムログの取得・・・OS機能や業務アプリケーションにて作業結果を記録 ③望まれる水準の例： a.OS、ミドルウェアの起動と終了がログに記録される、監視画面に上がる b.OS、ミドルウェアへのログインが記録される（成功/失敗/ログアウト） c.ユーザ環境からのアプリケーションの操作日時が記録される d.以下の内容が記録されること－OS起動/終了,DBMS起動/終了,ミドルウエア起動/終了,ディスク装置や論理ボリュームのマウント/アンマウント、ログ取得プログラムの起動/停止 e.ネットワーク監視機能（アクセスログの取得や、不正アクセス時のアラーム等）を組み込んでいる f.運用者によって、アラーム報知等を監視している			銀行API報告書・セキュリティ原則	3.3.4 不正アクセス発生時の対応 b	
50	APIセキュリティ機能	認証に関わる機密情報の漏洩対策を行う	API接続先	＜トークンの有効期限管理＞ 1．利用するAPIのセキュリティリスクに応じた適切なトークン管理を実施している。 （例えば1時間など一定時間以上の有効期限を持ったトークンについて暗号化保存） ＜暗号化対象の取決め＞ 2．暗号化の対象を取り決めている（注1）。 (注1)具体例 ①OAuth認証で使用する認証コード、アクセストークン			銀行API報告書・セキュリティ原則	3.3.2 外部からの不正アクセス対策 h	

API接続チェックリスト（試行版）

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
51	APIセキュリティ機能	APIの想定外利用回避のための原則を把握する	API接続先	＜APIの想定外利用の回避＞ 1. 利用するAPIのscopeや、取得するトークンによって実現できる機能を理解している(注1)。 2. APIの想定外利用回避のための原則を把握し、以下の脅威に対策を実施している(注2)。 (注1)具体例 ①OAuth2.0の仕組みを理解しており、それに関連する項目の意味を説明することができる ②API提供元で最低限果たすべきセキュリティ原則がなにかを理解しており、そうなっていることをAPI提供元に対して確認することができる (注2)具体例 ①URIの一部を改ざんして、サーバーにアクセスし不正に他社のデータを取得する ②APIリクエストを偽造して、不正にデータ取得等をする ③悪意のある会社・第三者がアクセストークンを乗っ取り、他社の個人情報を不正に入手したり、利用者に損害を与える ④悪意のある第三者がインターネット上又は広域LAN情報の通信をハイジャックし、個人情報を不正に入手したり、利用者に損害を与える					
52	APIセキュリティ機能	API利用実績の追跡調査を可能にする	API接続先	＜ログの取得・保管＞ 1. 利用するAPIのセキュリティリスクに応じた適切な実行ログの保管を行っている。 （実行ログが常に出力されるFWの導入） 2. ログに出力されるメッセージコードを登録し、該当メッセージが出力された場合に通知される仕組みとしている。			銀行API報告書・セキュリティ原則	3.3.2 外部からの不正アクセス対策t	
53	APIセキュリティ機能	利用者の認識していないところで、該当アカウントのAPI接続先との接続が行われることがないようにする	銀行	＜本人確認の実施＞ 1. API接続先に対するアクセス権限の付与（認可）を利用者の申請に基づき行い、その際利用者の本人認証を行っている。			銀行API報告書・セキュリティ原則	3.3.2 外部からの不正アクセス対策c	
54	APIセキュリティ機能	利用者のAPI接続先サービス利用の利便性と、API接続のリスクに見合った利用者保護を実現する認証強度とする	銀行	＜アクセス範囲に応じた認証の実施＞ 1. API接続先に対するアクセス権限の付与に関する利用者の認証は、利用者の属性や付与するアクセス権限の内容とそのリスクに応じた強度としている。 2. API接続先に対するアクセス権限の付与に関する利用者の認証方式の選択にあたっては、インターネット・バンキングの認証方式(注1)の水準を一つの目安として、以下の点に留意している（注2)。 ＜アクセス範囲の限定＞ 3. API接続先に付与するアクセス権限について、API接続先が提供するサービスに必要な範囲に限定している。 (注1)具体例 ①ログイン時にID+パスワード、振込時にワンタイムパスワードを用いている ②通常使用しているPCと異なる機器で取引処理を実施する場合に、追加認証機能を実装している (注2)具体例 ①API接続先に対するアクセス権限の付与に関する利用者の認証は、個々の取引に係る認証ではなく、アクセス権限の「認可」に係る認証とする ②APIを通じて指図を受ける個々の取引に係る認証方式も勘案した全体の不正アクセスリスクに応じた認証強度とする			銀行API報告書・セキュリティ原則	3.3.2 外部からの不正アクセス対策d	

API接続チェックリスト（試行版）

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
55	APIセキュリティ機能	認証機構以外にも全体システム機構として、万が一の脆弱性やそれの攻撃に対すする多層防御を図る	銀行	＜多層防御の実施＞ 1. 認証機構以外にも全体システム機構として、万が一の脆弱性やそれの攻撃に対する多層防御を図っている(注1)。 (注1)具体例 ①API接続先とのサーバー間接続を原則として、接続間のパラメーター情報が参照されない機構の導入 ②API接続先のIPアドレスなどを限定して、それ以外からのアクセスを許容しない機構の導入 ③API接続先にクライアント証明書の導入を求めて、証明書による接続元認証を行う機構の導入					
56	APIセキュリティ機能	API接続先との接続への認証を、第三者に悪用されるリスクを可能な限り低減させる	銀行	＜トークンの管理＞ 1. API接続先に発行するトークンには、適切な有効期限を設定している。 （例えば、1回限りとする、1ヶ月から数ヶ月で失効する） 2. アクセス権限の内容に応じたトークンの偽造・盗用対策を行っている。 3. 不正アクセス検知後、すみやかにアクセス権限の制限・停止・取消が可能な仕組みとしている。 ＜暗号化対象の取決め＞ 4. 暗号化の対象を取り決めている（注1)。 (注1)具体例 ①OAuth認証で使用する認証コード、アクセストークン			銀行API報告書・セキュリティ原則	3.3.2 外部からの不正アクセス対策 h	
57	APIセキュリティ機能	銀行単体ではなく、API接続先を含めた全体の認証強度を以って、利用者保護を図る	銀行	＜利用者保護の実施＞ 1. 利用者からAPI経由で銀行に対して行われる個々の取引指図について、銀行側で行う認証強度に対して、API接続先で行う認証強度が劣後することが想定し、その方が利用者利便性のために適切だと考えられる場合は、他の仕組みによって利用者保護を図っている。			銀行API報告書・セキュリティ原則	3.3.2 外部からの不正アクセス対策 n	
58	API利用セキュリティ	API利用に関わる利用者説明責任を果たす	API接続先	＜利用者の誤認防止＞ 1. 認可形式のAPIの利用において、利用者に対し、そのトークンを使って何を行うかを説明している。			銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得	

通番	区分	セキュリティ対応目標	対象者	手法例	現在の対応状況	今後の対応予定	関連規定	関連規定箇所	備考
59	API利用セキュリティ	API利用に関わる利用者説明責任を果たす	API接続先	＜利用者への説明＞ 1. 認可形式のAPIの利用において、利用者に対し、その機能が利用不可能となる状況や可能性について説明している。			銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得	
60	API利用セキュリティ	利用者のAPI接続に関する誤認・誤解を防ぐ	銀行	＜重要情報の表示、利用者からの同意取得＞ 1. トークン発行にあたって、API接続に関する情報についてわかりやすく画面表示のうえ、利用者の同意を求めている(注1)。 (注1)具体例 ①アクセス権限を付与するAPI接続先の名称 ②API連携するサービス等の名称 ③付与する権限の内容・範囲 ④付与する権限の有効期限 ⑤付与した権限の削除、解除方法 ⑥その他注意喚起が必要な事項 ⑦情報漏洩防止のために暗号化していること ⑧サービス規約、問い合わせ窓口、安全対策の概要、緊急時の連絡窓口			銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得	

【資料2－1】
平成29年6月28日
公益財団法人　金融情報システムセンター

■改訂原案（前説）に対する各委員からのご意見まとめ

	No.	頁	記載箇所	ご意見の概要	ご意見者
★	1	p11	Ⅰ概説 2．安全対策の考え方 ⑹安全対策基準における「統制」のあり方 ②外部に対する「統制」のあり方	「外部に対する統制」について、既存の外部委託先とは異なる形での外部連携先（例えばAPI連携先）が出てきております。外部委託とそれに含まれない外部連携先があることについて、より明確な記載をお願いいたします。 （修正文例） 金融機関等においては、【外部委託→外部委託先あるいはAPIによる接続先等】やサービスの利用が拡大 また外部委託先とは異なる形での外部連携先（例えばAPI連携先）は、一般論としては、外部委託先ほどの管理が求められない場合があることを意識した記載にして頂ければと思います。	FinTech協会 瀧様(専)
	2	p11	Ⅰ概説 2．安全対策の考え方 ⑹安全対策基準における「統制」のあり方 ②外部に対する「統制」のあり方	外部に対する統制の特徴について記載されている箇所について、リーガルエンティティとして別個となる委託先に対する統制という側面を具体的に表現してはどうか。 「内部（自組織）に対する統制に比して、外部（委託先などの他組織）に対して、内部に求める統制と同等の期待、要求は、一般的に及びにくくなる傾向にある。さらに、外部が再委託を行う場合は、その再委託先に対して内部が求める「統制」は、さらに及びにくくなる事が考えられる。」	日本ユニシス 後藤様(検)
★	3	p0	（全般）	システムリスクの評価についてはこれまで各金融機関が個別に評価してきたものであるが、各金融機関が改めて「リスクベースアプローチの考え方」に基づくシステムリスクの評価を行うには相応の時間を要することが予想される。ついては、新しい安全対策基準の公表・発刊にあたっては、全金融機関が「リスクベースアプローチの考え方」を「一律的に、一斉に適用する」等の表現は避けていただきたい。	南都銀行 山田様(専) 藤谷様（検）
	4	p0	（全般）	基準の構成や分類、適用に関する記載は、実際の基準が示されていない中で、判断ができない。	全国信用金庫協会 蓮實様(検)
★	5	p0	（全般）	今般、API接続事業者のチェックリストの策定が行われましたが、これらに対応したプレーヤーが、安全対策基準によって別のスタンダードでの対応を迫られるケースを回避することは必須であり、そのための配慮を今後の検討の中でも行っていくべきと考えております。	FinTech協会 瀧様(専)
	6	p1	Ⅰ概説 1．安全対策基準の意義	「学識経験者、金融機関、保険会社、証券会社、、、」において、保険会社や証券会社は一般的には金融機関に含まれると思われるが、見直すべきか検討頂きたい。	三井住友銀行 持田様(専)
	7	p2	Ⅰ概説 2．安全対策の考え方 安全対策基準改訂の考え方	本改訂における大方針の一つである「リスクベースアプローチ」の導入に際し、リスクベースアプローチの一般的な定義・効用、次期安対への導入目的について前説で分かり易い補記が欲しい。 P2にて経緯（外部委託に関する有識者検討会の提言）、またP6でリスクベースアプローチの意義について触れられているが、散在して記載されており読み易さ・理解し易さの観点で再考いただきたい。	NTTデータ 鎌田様(専) 鈴木様（検）
★	8	p7 p14	Ⅰ概説 2．安全対策の考え方 ⑶安全対策における基本原則 Ⅱフレームワーク 1．総論 ⑵基準の分類	7頁において、重要な外部性がある場合、機微情報の場合を「高い安全対策」が必要な場合としつつも、14頁においては、特定システムでない通常システムにおける機微情報の扱いについて注釈で可用性について安全対策を一部適用しない場合について規定しております。7頁の言い回しについては、基準改訂の大きなテーマの一つにはなると考えておりますが、機微情報と重要な外部性がある場合とを一つにまとめて「高い安全対策が必要」として留保しないことが整理として適切かご検討ください。	FinTech協会 瀧様(専)
★	9	p8	Ⅰ概説 2．安全対策の考え方 ⑶安全対策における基本原則 (参考)「外部性」の考え方	【例えば、決済システムは個別金融機関等で深刻なシステム障害が発生した場合、他金融機関等への信用不安に発展し、経済的損失が拡大する可能性のある性質を有する。】 とあるが、金融機関が破綻した場合などなら適切な例かもしれないが、システム障害から他金融機関の信用不安は例として無理があるのではないか。 また、4つ目の【また～可能性もある。】も極端すぎて例として不適切ではないか。 全体として外部性の定義が良くわからない。	全国信用金庫協会 蓮實様(検)
	10	p9	Ⅰ概説 2．安全対策の考え方 ⑸安全対策における経営責任のあり方	L3「安全対策の基本原則の遵守に当たって」について、「現在の認識は、過去からの積み上げで求められている基本要件と認識、この要件を認識した後、今回検討している基本原則に対する危惧の関係を示す」事が分かりやすく表現されるべきと考える。このため、表現をより平易にすべく、以下のようにしてはどうか。 「ひとたび重大なシステム障害が発生した場合、その事実をもって、結果責任を追及されかねない立場にあることから、高い安全対策を求めない訳にはいかない」といった共通認識が存在する。この認識から生まれる危機感が、安全対策の基本原則に示される「リスクベースアプローチに基づき安全対策を決定」の考え方に対する阻害要因とならぬようにすることが、重要と認識する。」	日本ユニシス 後藤様(検)
	11	p12	Ⅱフレームワーク 1．総論 ⑴安全対策基準における定義 ②特定システム・通常システム	「なお、特定システムの一部を～」について、具体的なシステム例を示した方が分かりやすいのではないか。	三井住友銀行 持田様(専)
	12	p12	Ⅱフレームワーク 1．総論 ⑴安全対策基準における定義 ③安全対策基準の構成	「統制基準」に人材育成・訓練等に関する対策を含める理由を教えていただきたい。	南都銀行 山田様（専） 藤谷様(検)

No.	頁	記載箇所	ご意見の概要	ご意見者
13	p13	Ⅱフレームワーク 1．総論 (1)安全対策基準における定義 ③安全対策基準の構成	現行の安全対策基準は、「設備基準」→「運用基準」→「技術基準」の順番で並べられている。改訂後の安全対策基準を使いやすいものとするため、「統制基準」→「設備基準」→「実務基準」→「監査基準」の順番で並べてほしい。 また、現行の安全対策基準の「運用基準」は保守・運用担当、「技術基準」は開発担当が参照しており、各担当が参照すべき安全対策が一目で分かる構成となっているが、改訂案の「実務基準」は、各担当が参照しにくいものになることが懸念される。こうしたことを踏まえ、「実務基準」を整理する際は、基準が現行の「運用基準」または「技術基準」のいずれに該当するものなのかが分かるような整理をしてほしい。	南都銀行 山田様(専) 藤谷様(検)
14	p13	Ⅱフレームワーク 1．総論 (1)安全対策基準における定義 ③安全対策基準の構成	「コンビニATM」および「デビットカード」の安全対策基準について、地銀の中には、「コンビニATM」の安全対策はセブン銀行やイオン銀行などコンビニATM設置行、「デビットカード」の安全対策は日本デビットカード推進協議会が行っているとして、銀行は(「コンビニATM」および「デビットカード」の安全対策を自ら実施するのではなく)コンビニATM設置行や日本デビットカード推進協議会の安全対策を確認する態勢を整備するものと考えるところがある。 こうしたことから、これら項目は「実務基準」ではなく、「統制基準」として整理するのがよいと考える。「統制基準」として整理することが難しいならば、これら項目の順番を「実務基準」の一番最後にするのがよい。	南都銀行 山田様(専) 藤谷様(検)
15	p18	Ⅱフレームワーク 1．総論 (4)安全対策基準の適用方法 ③リスク特性の評価・基準の選択	リスクが低く安全対策基準が適用されない場合とは、具体的にどのような場合か、書いて頂いたほかにどのような考え方で「リスク」をとらえるべきかご記載頂きたく思います。適用外になるような評価ができる場合がわかることは、FinTech事業者にとっても有益と考えます。 （適用されない例） ・外部接続なし ・顧客データなし ・＿＿＿＿（他の例）	FinTech協会 瀧様(専)
★ 16	p16	Ⅱフレームワーク 1．総論 (3)安全対策基準の適用対象	一例として、API接続事業者がFISCのチェックリストを満たした場合には、別途安全対策基準についての対策を検討する必要がない状態を担保することが重要と考えています。そのためにも、APIチェックリストを超えないように基礎基準が策定されることを明記して頂ければと考えます。	FinTech協会 瀧様(専)
17	p18	Ⅱフレームワーク 1．総論 (4)安全対策基準の適用方法 Ⅰリスクベースアプローチに基づく安全対策基準の適用	なお、対象システムの特定などシステムリスク評価の方法については、評価方法のサンプルを提供することを検討してはどうか。	日本銀行 水崎様(検)
18	p24	Ⅱフレームワーク 2．統制 (2)外部の統制 ③基本形における各論 b.共同センター	APIの共通基盤を作成した場合にはbの類型に含まれるのであれば、その旨の記載をお願いいたします。	FinTech協会 瀧様(専)
★ 19	p0	（全般）	【必要十分】という言葉が複数個所で用いられているが、「必要」は例えば、最低限の基準としてこれまでの安対基準でも使われてきた概念である。対して、「十分」については、その判断に明確の基準はなく、振れ幅が大きくなることが想定される。これは、今後も「ここまでやれば十分」と基準が示せるものではなく、また、何かの事象が発生し、結果を見た上で金融機関の意思決定が「十分」ではなかったと評価されるなど、結局は、結果が全てとなるのではないか。	全国信用金庫協会 蓮實様(検)
20	p0	（全般）	個々の考え方や内容は理解できるが、実際の安全対策基準利用での全体感（どの様に具体的に適用されるや図7、図8、図11、図12の関連性が判る等)が整理された図や一覧等があると良いが。	野村ホールディングス 荒木様(検)
★ 21	p0	（全般）	・金融サービスと金融関連サービス ・外部委託先と決済代行業者等 今回の改訂を機に新たなプレーヤーが基準を参照していく中で、上記の違いが明瞭な表現となることが必要と考えています。例えばAPIを活用する事業者は外部委託事業者ではないため、過度な統制を回避するためにも、個別の定義の記載を修正していく必要を感じております。	FinTech協会 瀧様(専)
22	p1	Ⅰ概説 1．安全対策基準の意義	「一方で、金融機関等が、企業価値を高めるために」について、金融機関側からの視点だけではなく、利用者視点から「顧客の利便性を向上させるため」について述べた方がよいのではないか。	全国信用金庫協会 蓮實様(検)
23	p1	Ⅰ概説 1．安全対策基準の意義	顧客の視点を入れて、「この中で」以降を以下のように修正してはいかがか。 「したがって、金融機関等は、<u>顧客利便性と企業価値の向上を目的に</u>、新規開発等に適切に資源配分していくことは重要であるが、一方で、金融機関等は、信用秩序を維持し、利用者が安心してサービスを享受するために、ITガバナンスを発揮し、安全対策に対する資源配分を経営資源全体の中で適切に調整していくことが不可欠である。」	三井住友銀行 持田様(専)

	No.	頁	記載箇所	ご意見の概要	ご意見者
★	24	p1	Ⅰ概説 1. 安全対策基準の意義	「あるべき姿」について、これは会員が実施することを強制する意味合いなのか。だとすると、安対基準は規制の程度が強くなると思われるが、その理解でよいか。その上で、以下のように修文いただきたい。 【そこで、『金融機関等コンピュータシステムの安全対策基準・解説書』(以下、「本書」とする)では、金融機関等のよりどころとなる安全対策基準の適用において、リスクベースアプローチを取り入れた考え方を示すこととした。ただし、その考え方については、全金融機関への一律の適用を求める物ではない。	全国信用金庫協会 蓮實様(検)
	25	p1	Ⅰ概説 1. 安全対策基準の意義	安対基準が金融機関等の安全対策を考えるうえでの拠り所となっている現状と、各金融機関では既にリスク管理対象やリスク度合いに応じて、安対基準をアレンジして利用している実態を踏まえると、ここで「あるべき姿」と表現するのではなく、「現実的かつ効果的な安全対策の考え方」とした方が相応しいのではないか。	三井住友銀行 持田様(専)
	26	p1	Ⅰ概説 1. 安全対策基準の意義	「非金融機関等」は「金融機関等」の対義語で使用しているのか？「等」の示す部分など、指示している範囲が曖昧であると感じる。(他数箇所あり)	全国信用金庫協会 蓮實様(検)
	27	p2	Ⅰ概説 2. 安全対策の考え方 安全対策基準改訂の考え方	L6「決済代行業等と連携した金融関連サービス」について、文中の主語が「金融機関等の情報システム」であり、文脈的に主従が一致していない。	全国信用金庫協会 蓮實様(検)
	28	p2	Ⅰ概説 2. 安全対策の考え方 安全対策基準改訂の考え方	L11現時点の安全対策基準は、基幹業務系以外のシステムに対する基準適用に関して、演繹的及び帰納的な考え方に基づき、適用を求めていると理解している。 しかし、昨今の多様性に対して、「現在の安全対策基準の想定している適用要件、背景が、追従しきれない情況とならないように改善していく事が求められている」と理解している。 このことから、以下の表現にしてはどうか。 「多様化する基幹業務系以外のシステムにおいては、その適用基準に想定されていた適用要件、背景の不一致などにより、」	日本ユニシス 後藤様(検)
	29	p2	Ⅰ概説 2. 安全対策の考え方 安全対策基準改訂の考え方	L12「サービス利用等において、外部委託への依存度が」について、サービスの利用はそもそも外部委託なので、この文脈では意味がおかしい。	全国信用金庫協会 蓮實様(検)
	30	p3	Ⅰ概説 2. 安全対策の考え方 (1)ITガバナンスとITマネジメント ①安全対策上必要となるITガバナンスの意義	今回は安全対策に関してなので必須ではないが、以前より中長期計画やシステム戦略方針策定においては「経営戦略やビジネス戦略との整合性」がより重要になってきているので、その記載もあってもいいかもしれない。	野村ホールディングス 荒木様(検)
	31	p4	Ⅰ概説 2. 安全対策の考え方 (1)ITガバナンスとITマネジメント ①安全対策上必要となるITガバナンスの意義	経営層は、業務執行とモニタニング体制の整備方針の決定を担っているが、経営層を含む担い手は分離・独立しているものと思われるので、次のとおり別々の章としたらよいのではないか。 b. ⅰ 安全対策に携わる業務執行 　ⅱ モニタリング体制の整備方針の決定	南都銀行 山田様(専)
	32	p5	Ⅰ概説 2. 安全対策の考え方 (1)ITガバナンスとITマネジメント ②安全対策上必要となるITマネジメント	PDCAサイクルを意識して書かれたものと考えるが、列挙されている「・内部規程・組織体制等の整備」と「・内部規程・組織体制等の見直し」の違いは小さく、まとめて記載してもよいのではないか。	東京スター銀行 星子様(専)
	33	p5	Ⅰ概説 2. 安全対策の考え方 (1)ITガバナンスとITマネジメント ②安全対策上必要となるITマネジメント	管理者の役割についての箇条書き部分は以下の様に修正していただきたい。 ・内部規程・組織体制等の整備、見直し ・個々の情報システムに対する安全対策の決定 ・ITガバナンス上必要となる情報の経営層への報告	全国信用金庫協会 蓮實様(検)
	34	p5	Ⅰ概説 2. 安全対策の考え方 (1)ITガバナンスとITマネジメント ②安全対策上必要となるITマネジメント	図4について、経営企画担当(部門)の役割の説明と平仄を合わせるため、経営層に向けて「支援」の矢印が必要。	三井住友銀行 持田様(専)
	35	p6	Ⅰ概説 2. 安全対策の考え方 (2)リスクベースアプローチ ①安全対策基準を取り巻く環境の変化	意味をより分かりやすくするために、以下の言葉を補足してはどうか。 「大きな比率を占めてきたその他情報システムについては、適用する安全対策の具体的な考え方がしめされないまま」	三井住友銀行 持田様(専)
	36	p6	Ⅰ概説 2. 安全対策の考え方 (2)リスクベースアプローチ ②リスクベースアプローチの意義	L11「企業価値の最大化」について、前説中に数回登場してくるため、価値の多様性について同様の認識がなされるよう、他の箇所も含め、本文中の表現を見直せないか。	全国信用金庫協会 蓮實様(検)
	37	p7	Ⅰ概説 2. 安全対策の考え方 (3)安全対策における基本原則	L6「プライバシーなど個人の人権を侵害する場合」について、人権等を侵害する以外の影響も考えられるが、表現されていないと感じる。また、「侵害する」ではなく「侵害される」が正しいのでは？	全国信用金庫協会 蓮實様(検)

	No.	頁	記載箇所	ご意見の概要	ご意見者
	38	p7	Ⅰ概説 2. 安全対策の考え方 (3)安全対策における基本原則	「金融機関等の情報システムの安全対策における基本原則」の次行より表記されている内容について、保有する情報システムだけでなく、クラウド形式などの利用による情報システムに対する統制についても、必要に応じて求めることが望まれることから、以下の表現にしてはどうか。 「基本原則は、金融機関等が利用する情報システムの安全対策について、ITガバナンスが適切に発揮されている限りにおいて、リスクベースアプローチの考え方に基づき、必要十分な内容で、みずから決定することを可能としている。」	日本ユニシス 後藤様(検)
★	39	p7	Ⅰ概説 2. 安全対策の考え方 (3)安全対策における基本原則	質問・基本原則の4つ目の項目に【〇上記原則が遵守されたうえで、妥当な意思決定等が行われ、適切に運営されている限りにおいては、安全対策は独自決定することが可能である。】とあるが、 原則に当てはまらない場合には、だれが安全対策を決めるのか？	全国信用金庫協会 蓮實様(検)
	40	p8	Ⅰ概説 2. 安全対策の考え方 (3)安全対策における基本原則 (参考)「情報の機微性」の考え方	L9「「重大な外部性を有する」システムと同様に」について、「同様」の指すものが曖昧である。同様の対策なのか？同様のレベルの安全対策なのか？を明確にした方がよい。	東京スター銀行 星子様(専)
	41	p8	Ⅰ概説 2. 安全対策の考え方 (3)安全対策における基本原則 (参考)「情報の機微性」の考え方	L11「これらが同一に扱われてしまった場合」について、「これら」の指す内容が曖昧であるため、表現の見直しをした方がよい。	東京スター銀行 星子様(専)
	42	p9	Ⅰ概説 2. 安全対策の考え方 (4)基本原則に従ったITガバナンス	「新規投資等を含むその効率の最大化」について、「その」を具体的に示した方が分かりやすいのでは。	三井住友銀行 持田様(専)
	43	p10	Ⅰ概説 2. 安全対策の考え方 (6)安全対策基準における「統制」のあり方 ①「統制」と「実務」の区分	今回の検討においては、過去を踏襲する事を否定していないが、その前提は、既存の考え方に縛られない、より的確な対応を基本とすること理解していることから、以下の表現としてはどうか。 「経営層が、既存の考え方に縛られることなく」	日本ユニシス 後藤様(検)
	44	p11	Ⅰ概説 2. 安全対策の考え方 (6)安全対策基準における「統制」のあり方 ①「統制」と「実務」の区分	図6「外部の統制」の内容説明について「外部への統制を具体化した施策」が判り難い。P12に記載の「外部へ委託する上で必要となる統制」等が表現が良い。	野村ホールディングス 荒木様(検)
	45	p11	Ⅰ概説 2. 安全対策の考え方 (6)安全対策基準における「統制」のあり方 ①「統制」と「実務」の区分	図6「実務」の説明を以下のように修正してはいかがか。 「管理者がリスク管理対象やリスク度合いに応じて」	三井住友銀行 持田様(専)
	46	p12	Ⅱフレームワーク 1. 総論 (1)安全対策基準における定義	「I. 安全対策の考え方」で述べた「基幹業務系システム以外の基準が不明確～」を受け、「1.総論」の後に、過去の課題を解消するために、どのような策を施したか説明を入れた方がよいのではないか。	三井住友銀行 持田様(専)
★	47	p14 p18	Ⅱフレームワーク 1. 総論 (2)基準の分類（図8） (4)安全対策基準の適用方法（図11）	「全て適用」という表現を用いると、「原則として」の意味合いが排除されてしまう。このため、図8においては言葉ではなく、「〇」「△」等の表記とし、注釈にて 「〇:リスク特性に応じて原則適用」 「△:リスク特性に応じて選択適用」 のようにしてはどうか。併せて本文中も「最低限原則適用する基準」等に表現を見直してはどうか。	三井住友銀行 持田様(専)
	48	p14 p17	Ⅱフレームワーク 1. 総論 (2)基準の分類（図8） (4)安全対策基準の適用方法（図10）	図表8で登場する「特定システム、通常システム」と図表10で登場する「情報システム、金融情報システム、上記以外のシステム」の関係性が判りにくいので、一体で整理してほしい。	日本銀行 水崎様(検)
	49	p14	Ⅱフレームワーク 1. 総論 (2)基準の分類 (補足1)「基礎基準」とした安全対策について	より分かりやすくするために、以下の内容に修正してはどうか。 ・タイトル「基礎基準」の対象となる安全対策について ・(p15L4)上記を踏まえ、「基礎基準の対象とする安全対策」は、、、 ・(p14L13)「上記以外の、、、」を、p15の枠囲みの後に移動 ・統制・監査を対象とした説明の追加	事務局
	50	p15	Ⅱフレームワーク 1. 総論 (2)基準の分類 (補足3)決済代行業者等における・・	内容が分かりづらいと思われる。サービス提供主体が金融機関でない場合にあっても金融関連サービスを提供する業者はシステムの安全対策を策定する場合云々ということを言いたいのではないかと考えます。そう書けば多分ほかの解釈はないし、この一部の非金融機関の中のさらに業者とは一体何を指しているだろうということにはならないのではないかと思います。	全国信用金庫協会 蓮實様(検)

	No.	頁	記載箇所	ご意見の概要	ご意見者
★	51	p15	Ⅱフレームワーク 1．総論 (2)基準の分類 (補足3)決済代行業者等における・・	(補足3)決済代行会社等の文末で、「基礎基準を満たすことが期待される」とありますが、この「期待される」＝それ以下でも良いという表現になりますでしょうか。文言上は、例えばAPIのチェックリストとは関係なく基礎基準を適用とも取ることができます。また、この基準は26頁の最後にある「準用」とは異なるのでしょうか Fintech企業は「金融機関等が提供するサービスと同等」の対策が常に求められる訳では無く、より柔軟な安全対策が許容されると思いますので、この点は「期待」ほどに現実が追いつかない場合もありえることを前提として、表現にご反映頂きたいと思います。	FinTech協会 瀧様(専)
	52	p16	Ⅱフレームワーク 1．総論 (3)安全対策基準の適用対象	【金融機関等がベンダーと契約するものや、協同組織等を通じてベンダーと～】とあるが共同組織等を運営組織等に変更していただきたい。	全国信用金庫協会 蓮實様(検)
	53	p16	Ⅱフレームワーク 1．総論 (3)安全対策基準の適用対象 (補足)金融機関等における特定システムと通常システムの分類	これはp12(1)②の補足とした方がよいのではないか。ご検討いただきたい。	三井住友銀行 持田様(専)
	54	p17	Ⅱフレームワーク 1．総論 (4)安全対策基準の適用方法 Ⅰリスクベースアプローチに基づく安全対策基準の適用	「対象システムの特定」を行う段階自体、リスクベースアプローチの一部にあたる。 すなわち、対象システムの特定を行うにあたって、一定の評価基準でシステムリスク評価を行うのであるから、これをリスクベースアプローチから外すことは不適切である。また、「リスク特定の評価」も「対象システムの特定」をカバーの範囲とすることになる。	日本銀行 水崎様(検)
★	55	p18	Ⅱフレームワーク 1．総論 (4)安全対策基準の適用方法 ③リスク特性の評価・基準の選択	現行の安全対策基準をみると、基準の解説部分に、具体的な対策として最低限のものから高い水準のものやベストプラクティスが含まれている。この場合、基礎基準となる部分と選択的に適用される部分とを区分することが必要となる。	事務局
★	56	p18	Ⅱフレームワーク 1．総論 (4)安全対策基準の適用方法 ③リスク特性の評価・基準の選択	図8と平仄をとるため、以下のように修正してはいかがか。 ・「特定システムにおいては～全ての対策を選択実施する」として注釈17で一部省略も可とする ・「ただし、～原則として選択不可とする」の記述は注釈17で、リスク特性に応じて選択も可とする	三井住友銀行 持田様(専)
★	57	p18	Ⅱフレームワーク 1．総論 (4)安全対策基準の適用方法 ④安全対策の選択	安全対策の選択と安全対策の設定との違いがわかりにくい。また、安全対策の目標の設定は、基準の選択、安全対策の選択と同時に決定されるものではないか。	事務局
	58	p19	Ⅱフレームワーク 1．総論 (4)安全対策基準の適用方法 ⑤安全対策の目標設定	各システムの安全対策目標の設定ではなく、目標設定方針の決定に経営層が関与する方が、実態として相応しいのではないか。	三井住友銀行 持田様(専)
	59	p19	Ⅱフレームワーク 1．総論 (4)安全対策基準の適用方法 ⑦コンティンジェンシープランの策定	残リスクに対して必ずCPが必要との書きぶりになっているが、単純に許容できるリスクや補完的な統制対応もあるのではないか。(＝CPを必須としたら逆に負担が増える可能性がある)	野村ホールディングス 荒木様(検)
	60	p20	Ⅱフレームワーク 1．総論 (4)安全対策基準の適用方法 ⑦コンティンジェンシープランの策定	対象物を明確化するために、「なお、安全対策基準においては～およぶことからコンティンジェンシープランについてはコンピュータシステムを中心に言及している」とした方がよいのではないか。	三井住友銀行 持田様(専)
★	61	p21	Ⅱフレームワーク 2．統制 (2)外部の統制	決済代行業者がいわゆる外部委託先と同じように書かれていますため、外部委託に関する概念は説明ないし整理が必要と思われます。外部委託ではないAPI連携等の場合の統制の考え方も内部、外部と並べて(しない場合ならその旨も明らかに)記載すべきと考えます。	FinTech協会 瀧様(専)
	62	p22	Ⅱフレームワーク 2．統制 (2)外部の統制 ①外部委託の管理におけるITガバナンス	[図13] 「経営層以外」の「層」の文字の右横に両矢印があるが、何を指しているのか判読しづらい。恐らく「委託業務が低リスクな場合は～」を指していると思われるが、吹き出し線の色が周囲とほぼ同色で判読しづらい。(他、数名「分かりにくい」との意見あり)	NTTデータ 鎌田様(専) 鈴木様(検)
	63	p24	Ⅱフレームワーク 2．統制 (2)外部の統制 ③基本形における各論 b.共同センター	【主に勘定系システムなど、高い可用性が求められる～】とあるが、勘定系システムであれば機密性、可用性、完全性の全てが高いレベルで求められるので可用性はセキュリティや、安全対策などの用語の方が適切ではないか。	全国信用金庫協会 蓮實様(検)
	64	p24	Ⅱフレームワーク 2．統制 (2)外部の統制 ③基本形における各論 c.クラウドサービス	クラウドサービスについては、外部委託に要求するような、安対遵守、監査受入、改善要求などは期待できない場合、安対によるコントロールでなくSLA等でもよいと言っているのでしょうか。(実際、数万台のサーバ設置拠点を監査することは現実的には不可能であるが)	三井住友銀行 持田様(専)

No.	頁	記載箇所	ご意見の概要	ご意見者
65	p25	Ⅱフレームワーク 2. 統制 (2)外部の統制 ⑤3者間構成における各論	3者間構成の各論について、タイプA、タイプBと各々文章での説明が続く。図式を用いるなど理解のし易さを考慮いただきたい。	NTTデータ 鎌田様(専) 鈴木様(検)
66	p26	Ⅱフレームワーク 2. 統制 (2)外部の統制 ⑤3者間構成における各論 b.タイプB	タイプAは従来通り決済代行業者等が金融機関の委託先、または再委託先の場合を指し、タイプBは決済代行業者等が顧客の委託先の場合を指していると思うが、【預取金融機関の勘定系システムに対して入出金の指示を行うなど、金融機関等に変わり、決済代行業者等が金融関連サービスを提供するため～】の「金融機関等にかわり」は決済代行業者が金融機関の委託先の様にもとれるため、削除していたたきたい。	全国信用金庫協会 蓮實様(検)
67	p26	Ⅱフレームワーク 2. 統制 (2)外部の統制 ⑤3者間構成における各論 b.タイプB	タイプBの説明文の中で「例えば、～指す。」が5行に渡る長文である。文章を区切るなど読み易さを考慮いただきたい。	NTTデータ 鎌田様(専) 鈴木様(検)
68	p1	Ⅰ概説 1. 安全対策基準の意義	「決済代行業者等」という言葉を利用することとなった経緯は判ったが、この「決済代行業者等」に含まれる業者の事業内容には幅が有りすぎる。例えば、「決済代行」のように金融機関側システムに対し更新を指示するケースもあれば、単に金融機関側システムから情報を参照するケースもある（更に、参照する情報にも機密性について幅がある）。こうした中、（補足3）において、「決済代行業者等」に対し、何が「一部」なのかはっきりしないため、その後「基礎的基準を満たすことが期待される」とした場合、情報を参照するケース（例えば、為替相場照会、店舗・ATM所在地照会、金利、手数料紹介、店頭混雑状況照会など）などにおいて、過度の対策を求めることになる可能性がある。	日本銀行 水崎様(検)
69	p7	Ⅰ概説 2. 安全対策の考え方 (3)安全対策における基本原則	基本原則中の「重大な」の範囲を分かりやすくできないか。外部性を持つシステムはいくつも考えられるため、「重大」の境界線によって安全対策の考え方が変わるとした場合、その境界線に対する明確な根拠、例示を示して欲しい。	東京スター銀行 星子様(専)
70	p14 p18	Ⅱフレームワーク 1. 総論 (2)基準の分類（図8） (4)安全対策基準の適用方法（図11）	特定システムに関わる付加基準の選択が「全て適用」となっており、誤解を生じさせやすい内容となっている。 今回の改訂では、「情報の外部性」と「情報の機微性」に着目し、リスクベースアプローチの考え方に基づいて安全対策基準を考えよう、というものであると認識しているが、「情報の外部性」と「情報の機微性」では求められる安全対策は異なることが通常であるから、「付加基準の分割」を検討してもよいのではないか。	東京スター銀行 星子様(専)
71	p15	Ⅱフレームワーク 1. 総論 (2)基準の分類 (補足2)外部の統制における・・	「可能である」という表現の使い方に何通りもあるように読めるため、全体として意味が理解しにくい。表現上の問題だけでなく、必要最低限の考え方も混入しているため、整理して分かりやすくした方がよい。	全国信用金庫協会 蓮實様(検)
72	p26	Ⅱフレームワーク 2. 統制 (2)外部の統制 ⑤3者間構成における各論 b.タイプB	最後の段落の記載（新設部分）につき、銀行の参照系ないし更新系のAPIに接続する事業者が本人確認義務を負うシチュエーションは現状の業務と即していません。利用する口座は金融機関において開設されたものであり、二重の確認が発生する本記載は修正が必要と考えております。一方で、口座開設や取引の実行等、本来あるべき認証が必要なケースへの対応であれば、その旨が明らかとなる記載として頂ければと思います。	FinTech協会 瀧様(専)

【資料2－2】
平成29年6月28日
公益財団法人　金融情報システムセンター

■改訂原案（前説）に対する委員からの主なご意見とその対応方針案

		No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針案	備考
1	激変緩和措置に関するもの	3	p0	（全般）	システムリスクの評価についてはこれまで各金融機関が個別に評価してきたものであるが、各金融機関が改めて「リスクベースアプローチの考え方」に基づくシステムリスクの評価を行うには相応の時間を要することが予想される。ついては、新しい安全対策基準の公表・発刊にあたっては、全金融機関が「リスクベースアプローチの考え方」を「一律的に、一斉に適用する」等の表現は避けていただきたい。	南都銀行 山田様(専) 藤谷様(検)	外部委託に関する有識者検討会の報告書でも述べられているように、リスクベースアプローチの考え方を導入するにあたっては、一律的、一斉に適用することは想定されていません（激変緩和措置の必要性が述べられています）。例えば、システム更新の際に、順次適用していくことを想定しています。従って、新しい安全対策基準の記述においても、また対外公表に当たっても、その点を留意しながら作業を進めていくことを考えています。	広報については、委員会終了までに適切な方法を検討します。
2	安全対策基準の意義に関するもの	24	p1	Ⅰ概説 1．安全対策基準の意義	「あるべき姿」について、これは会員が実施することを強制する意味合いなのか。だとすると、安対基準は規制の程度が強くなると思われるが、その理解でよいか。その上で、以下のように修正いただきたい。 【そこで、『金融機関等コンピュータシステムの安全対策基準・解説書』（以下、「本書」とする）では、金融機関等のよりどころとなる安全対策基準の適用において、リスクベースアプローチを取り入れた考え方を示すこととした。ただし、その考え方については、全金融機関への一律の適用を求める物ではない。】	全国信用金庫協会 蓮實様(検)	安対基準は「自主基準」として策定され、金融機関等の安全対策の拠り所として活用されてきました。ご指摘頂いた点は、自主基準に選択と適用の幅を持たせることを確保したいとの趣旨と理解いたしました。従って、他の委員から提示（No25）された「現実的かつ効果的な安全対策の考え方を示すこととした」という表現が、現在の安全対策基準についての考え方の記載とも通じるものがあると考えます。	
3	基本原則に関するもの	19	p0	（全般）	【必要十分】という言葉が複数個所で用いられているが、「必要」は例えば、最低限の基準としてこれまでの安対基準でも使われてきた概念である。対して、「十分」については、その判断に明確の基準はなく、振れ幅が大きくなることが想定される。これは、今後も「ここまでやれば十分」と基準が示せるものではなく、また、何かの事象が発生し、結果を見た上で金融機関の意思決定が「十分」ではなかったと評価されるなど、結局は、結果が全てとなるのではないか。	全国信用金庫協会 蓮實様(検)	「必要十分」という表現は、p6で記載されているように、形式的に安全性に偏った安全対策を行ってしまうこと（=リスクゼロを追及するがために過剰な安全対策を行ってしまうこと）のないように安全対策を行うことを指し示す表現として使われています。そうした意図にも関わらず、「必要十分」といった表現が、「リスクゼロとなるのに十分な」と誤解される可能性が高いのであれば、他の適切な表現に変更することが考えられます（例えば、「適切な」や「過不足なく」といった表現が考えられます）。	使用箇所が複数あるため、それぞれの内容、文脈等を確認のうえ対応します（7箇所）。
4		39	p7	Ⅰ概説 2．安全対策の考え方 (3)安全対策における基本原則	質問・基本原則の4つ目の項目に【〇上記原則が遵守されたうえで、妥当な意思決定等が行われ、適切に運営されている限りにおいては、安全対策は独自決定することが可能である。】とあるが、 原則に当てはまらない場合には、だれが安全対策を決めるのか？	全国信用金庫協会 蓮實様(検)	金融機関は、従来より安全対策基準に基づき、各々が独自に判断して安全対策を決定・実施してきました。ご指摘の文章は、金融機関の自主的な判断により、リスクの特性に合った安全対策を決定できることを強調した文章ですが、その趣旨が誤解される可能性があるのであれば、〇の4つ目を一番上に配置し直した上で、以下のように修正することが考えられます。 〇情報システムに対する安全対策は、以下の考え方に基づき、適切な意思決定が行われ、運営されるべきである。 〇情報システムに対する安全対策の達成目標は、個々の情報システムのリスク特性に応じて、必要十分な内容で決定されるべきである。 〇情報システムに対する安全対策への経営資源配分は、リスク顕在化後の事後対策と比較衡量したうえで、情報システム予算内での新規開発等との調整のみならず、経営資源全体も視野に入れ、企業価値の最大化を目指して、決定されるべきである。 〇ただし、金融機関等が保有する重大な外部性を有する情報システム及び機微情報（要配慮個人情報を含む）を保有する情報システムにおいては、その社会的・公共的な観点から、このシステムの外部性や保有情報の機微性を考慮に入れた安全対策の達成目標が設定されなければならない。	
5	「外部性」の説明に関するもの	69	p7	Ⅰ概説 2．安全対策の考え方 (3)安全対策における基本原則	基本原則中の「重大な」の範囲を分かりやすくできないか。外部性を持つシステムはいくつも考えられるため、「重大」の境界線によって安全対策の考え方が変わるとした場合、その境界線に対する明確な根拠、例示を示して欲しい。	東京スター銀行 星子様(専)	決済システムは個別金融機関で深刻なシステム障害が発生した場合、他金融機関等への信用不安へ発展し、経済的損失が拡大する可能性のある性質を有すると位置づけられることから、「重大な外部性」を有するシステムとして例示しました。「重大な外部性」の意義をイメージしやすくするために、システムを例示することが必要と考えられるのであれば、委員の皆様のご意見・ご提案をいただき、取り入れたいと考えています。	
6		9	p8	Ⅰ概説 2．安全対策の考え方 (3)安全対策における基本原則 (参考)「外部性」の考え方	【例えば、決済システムは個別金融機関等で深刻なシステム障害が発生した場合、他金融機関等への信用不安に発展し、経済的損失が拡大する可能性のある性質を有する。】 とあるが、金融機関が破綻した場合などなら適切な例かもしれないが、システム障害から他金融機関の信用不安は例として無理があるのではないか。 また、4つ目の【また～可能性もある。】も極端すぎて例として不適切ではないか。 全体として外部性の定義が良くわからない。	全国信用金庫協会 蓮實様(検)	リスク事象による影響が甚大で、個別金融機関においてその損失等を算出することが困難な場合を「重大な外部性」としており、最大のリスクを想定すると、（参考）に記載した内容になると考えられます。No69のご意見も踏まえ、重大な外部性を有するシステムが持つリスク事象についても、より具体的かつ現実的な例示ができれば、それを取り入れたいと考えています。	
7	安全対策の基準の分類・適用に関するもの	8	p7 p14	Ⅰ概説 2．安全対策の考え方 (3)安全対策における基本原則 Ⅱフレームワーク 1．総論 (2)基準の分類	7頁において、重要な外部性がある場合、機微情報の場合を「高い安全対策」が必要な場合としつつも、14頁においては、特定システムでない通常システムにおける機微情報の扱いについて注釈で可用性について安全対策を一部適用しない場合について規定しております。7頁の言い回しについては、基準改訂の大きなテーマの一つにはなると考えておりますが、機微情報と重要な外部性がある場合とを一つにまとめて「高い安全対策が必要」として留保しないことが整理として適切かご検討ください。	FinTech協会 瀧様(専)	現在の記載内容では、特定システムに対して、現行の安全対策基準を一律すべて適用するという趣旨に捉えられてしまう惧れがあり、修正が必要と考えています。安全対策基準の中には、例えば、個々のシステムへの適用を行う場合、その性質上、適用対象外になるものが含まれていたり、水準の異なる対策が含まれていたり、ベストプラクティスの対策等が含まれていたりします。従って、現時点では「全て適用」を「原則として適用」とし、これに関連する箇所を修正したうえで、今後、各論を整理しながら、適切な表現に修正していきたいと考えています。	
8		70	p7 p14	Ⅱフレームワーク 1．総論 (2)基準の分類（図8） (4)安全対策基準の適用方法（図11）	特定システムに関わる付加基準の選択が「全て適用」となっており、誤解を生じさせやすい内容となっている。 今回の改訂では、「情報の外部性」と「情報の機微性」に着目し、リスクベースアプローチの考え方に基づいて安全対策基準を考えよう、というものであると認識しているが、「情報の外部性」と「情報の機微性」では求められる安全対策は異なることが通常であるから、「付加基準の分割」を検討してもよいのではないか。	東京スター銀行 星子様(専)	No8参照	
9		47	p14 p18	Ⅱフレームワーク 1．総論 (2)基準の分類（図8） (4)安全対策基準の適用方法（図11）	「全て適用」という表現を用いると、「原則として」の意味合いが排除されてしまう。このため、図8においては言葉ではなく、「〇」「△」等の表記とし、注釈にて 「〇：リスク特性に応じて原則適用」 「△：リスク特性に応じて選択適用」 のようにしてはどうか。併せて本文中も「最低限原則適用する基準」等に表現を見直してはどうか。	三井住友銀行 持田様(専)	No8参照	
10		56	p18	Ⅱフレームワーク 1．総論 (4)安全対策基準の適法方法 ③リスク特性の評価・基準の選択	図8と平仄をとるため、以下のように修正してはいかがか。 ・「特定システムにおいては～全ての対策を選択実施する」として注釈17で一部省略も可とする ・「ただし、～原則として選択不可とする」の記述は注釈17で、リスク特性に応じて選択も可とする	三井住友銀行 持田様(専)	No8参照	
11		71	p15	Ⅱフレームワーク 1．総論 (2)基準の分類 (補足2)外部の統制における・・	「可能である」という表現の使い方に何通りもあるように読めるため、全体として意味が理解しにくい。表現上の問題だけでなく、必要最低限の考え方も混入しているため、整理して分かりやすくした方がよい。	全国信用金庫協会 蓮實様(検)	ご指摘のとおり、「可能である」には、必要最低限と位置付けられるものが混在しているため、全体として意味が分かりづらくなっています。「可能である」という表現は、主に「クラウドサービス利用」の基準内で使われている表現ですが、当該基準は、8月8日専門委員会のテーマである「外部委託管理基準の検討」において審議していただく予定ですので、それまでに整理したいと考えています。	
12		55	p18	Ⅱフレームワーク 1．総論 (4)安全対策基準の適用方法 ③リスク特性の評価・基準の選択	現行の安全対策基準をみると、基準の解説部分に、具体的な対策として最低限のものから高い水準のものやベストプラクティスが含まれている。この場合、基礎基準となる部分と選択的に適用される部分とを区分することが必要となる。	事務局	基準と一体となって利用されている解説部分については、No8で述べたような各種の記述が混在していますので、各論において、基礎基準とその解説に当たる部分、付加基準に当たる部分、ベストプラクティスに当たる部分等を明確に区分したいと考えています。	

		No.	頁	記載箇所	ご意見の概要	ご意見者	対応方針案	備考
13		57	p18	Ⅱフレームワーク 1．総論 (4)安全対策基準の適用方法 ④安全対策の選択	安全対策の選択と安全対策の設定との違いがわかりにくい。また、安全対策の目標の設定は、基準の選択、安全対策の選択と同時に決定されるものではないか。	事務局	再度整理のうえ、修正案をご提示させて頂きたいと考えています。	
14	「決済代行業者等」に関するもの	68	p1	Ⅰ概説 1．安全対策基準の意義	「決済代行業者等」という言葉を利用することとなった経緯は判ったが、この「決済代行業者等」に含まれる業者の事業内容には幅が有りすぎる。例えば、「決済代行」のように金融機関側システムに対し更新を指示するケースもあれば、単に金融機関側システムから情報を参照するケースもある（更に、参照する情報にも機密性について幅がある）。 こうした中、（補足3）において、「決済代行業者等」に対し、何が「一部」なのかはっきりしないため、その後「基礎的基準を満たすことが期待される」とした場合、情報を参照するケース（例えば、為替相場照会、店舗・ATM所在地照会、金利、手数料紹介、店頭混雑状況照会など）などにおいて、過度の対策を求めることになる可能性がある。	日本銀行 水崎様(検)	まず、言葉の使い方について、FinTechに関する有識者検討会において、「FinTech企業」という用語を用いましたが、法整備等の進む中、FinTech企業という言葉が今後も継続的に使用されない可能性があるとの指摘を受けて、「決済代行業者等」という用語を用いました。「決済代行業」が、却って一部の特定業務をイメージさせるのであれば、「FinTech企業」とするか他の適切な表現を考案することも考えられますので、委員の皆様のご意見をお聞きしたいと考えます。また、補足3の記述について、ご指摘の通り、決済代行業者等のサービス内容は多岐にわたり、一律に基礎的基準を適用すると過度の対策を求めることにもなりかねません。そこで、FinTechに関する有識者検討会報告書の記述を踏まえて「決済代行業者等が金融関連サービスを提供するシステムの安全対策を策定する場合には、安全対策基準の基礎基準などを踏まえたうえで適切な安全対策が実施されることが期待される」といった表現に変更したいと考えています。また、この記述については、基礎基準の具体的な検討やオープンAPIチェックリストの策定等を勘案しながら、再度検討することとしたいと考えています。	
15		21	p0	（全般）	・金融サービスと金融関連サービス ・外部委託先と決済代行業者等 今回の改訂を機に新たなプレーヤーが基準を参照していく中で、上記の違いが明瞭な表現となることが必要と考えています。例えばAPIを活用する事業者は外部委託事業者ではないため、過度な統制を回避するためにも、個別の定義の記載を修正していく必要を感じております。	FinTech協会 瀧様(専)	決済代行業者等が金融関連サービスを提供する場合に、安全対策基準の全てをストレートに適用することは、そもそも想定されていません。金融関連サービスの特徴に照らして、安全対策基準を参考にして適切な安全対策を実施することが期待されています。従って、そうした趣旨がよりわかるような記述に心掛けたいと考えています。例えば、外部委託事業者ではないFinTech企業については、外部委託先としての統制が直接適用されるわけではないことをより明確に記載することとしたいと考えています。	決済代行業について、個別の記載状況を確認のうえ対応します。（33箇所）
16		1	p11	Ⅰ概説 2．安全対策の考え方 (6)安全対策基準における「統制」のあり方 ②外部に対する「統制」のあり方	「外部に対する統制」について、既存の外部委託先とは異なる形での外部連携先（例えばAPI連携先）が出てきております。外部委託とそれに含まれない外部連携先があることについて、より明確な記載をお願いいたします。 （修正文例） 金融機関等においては、【外部委託→外部委託先あるいはAPIによる接続先等】やサービスの利用が拡大 また外部委託先とは異なる形での外部連携先（例えばAPI連携先）は、一般論としては、外部委託先ほどの管理が求められない場合があることを意識した記載にして頂ければと思います。	FinTech協会 瀧様(専)	No21参照	
17		61	p21	Ⅱフレームワーク 2．統制 (2)外部の統制	決済代行業者がいわゆる外部委託先と同じように書かれていますため、外部委託に関する概念は説明ないし整理が必要と思われます。外部委託ではないAPI連携等の場合の統制の考え方も内部、外部と並べて（しない場合ならその旨も明らかに）記載すべきと考えます。	FinTech協会 瀧様(専)	No21参照	
18		5	p0	（全般）	今般、API接続事業者のチェックリストの策定が行われましたが、これらに対応したプレーヤーが、安全対策基準によって別のスタンダードでの対応を迫られるケースを回避することは必須であり、そのための配慮を今後の検討の中でも行っていくべきと考えております。	FinTech協会 瀧様(専)	APIチェックリストは安対基準（基礎基準）を踏まえながら、チェックリストの試行結果等も勘案して、今後完成バージョンを策定する予定となっています。その検討の中で、ダブルスタンダードにならない配慮を行っていくものと考えております。	
19		16	p18	Ⅱフレームワーク 1．総論 (3)安全対策基準の適用対象	一例として、API接続事業者がFISCのチェックリストを満たした場合には、別途安全対策基準についての対策を検討する必要がない状態を担保することが重要と考えています。そのためにも、APIチェックリストを超えないように基礎基準が策定されることを明記して頂ければと考えます。	FinTech協会 瀧様(専)	No5参照	
20		51	p15	Ⅱフレームワーク 1．総論 (2)基準の分類 (補足3)決済代行業者等における・・	（補足3）決済代行会社等の文末で、「基礎基準を満たすことが期待される」とありますが、この「期待される」＝それ以下でも良いという表現になりますでしょうか。文言上は、例えばAPIのチェックリストとは関係なく基礎基準を適用とも取ることができます。また、この基準は26頁の最後にある「準用」とは異なるのでしょうか Fintech企業は「金融機関等が提供するサービスと同等」の対策が常に求められる訳では無く、より柔軟な安全対策が許容されると思いますので、この点は「期待」ほどに現実が追いつかない場合もありえることを前提として、表現にご反映頂きたいと思います。	FinTech協会 瀧様(専)	No5参照	

【資料２－３】
平成 29 年 6 月 28 日更新
公益財団法人 金融情報システムセンター

改訂原案（安全対策基準前説）

削除: 基準の適用方法

【資料２－３】
平成 29 年 6 月 28 日更新
公益財団法人 金融情報システムセンター

Ⅰ．概説

１．安全対策基準の意義

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

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

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

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

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

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

コメント [FISC1]: 6/28 確認
「FinTech 企業」もしくは、それに代わる名称はないか？

コメント [FISC2]: 6/28 確認
「金融サービス」と「金融関連サービス」または、「外部委託先」と「決済代行業者」の明確な使い分けが必要。オープンＡＰＩ連携先は外部委託以外の位置付けであることも説明が必要。

コメント [FISC3]: 6/28 修正案
今回の改訂の趣旨を表す表現として、この表現に見直した。

削除: あるべき安全対策

[1] 電子決済代行業など、IT 技術を活用した革新的な金融関連サービスは、将来において更に多様化することが想定されるため、事業もしくは事業者に対し、現時点で画一的な名称を与えることが適当ではない。本書においては、便宜上、これら革新的な金融サービスを「決済代行業等」、それらを提供する事業者を「決済代行業者等」としている。

２．安全対策の考え方

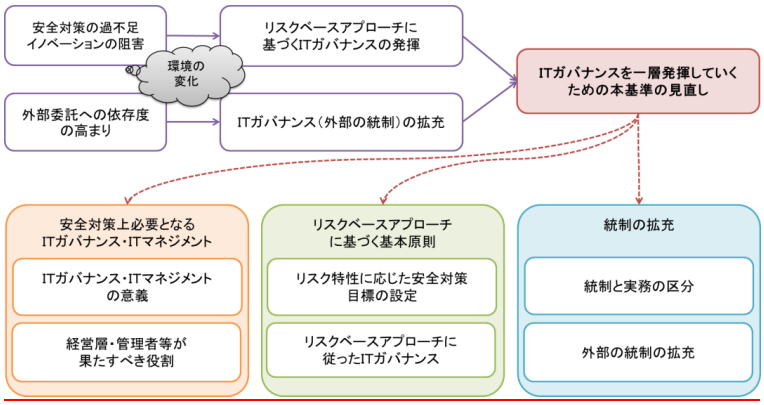
安全対策基準改訂の考え方

安全対策基準が作られた当初は、金融機関等の情報システムと言えば、基幹業務系のコンピュータシステムであった。そのため、安全対策基準の初版では、その適用対象とする情報システムを、「金融機関等のオンラインシステム」としていた。その後、情報化の進展に伴い、金融機関等の情報システムは、基幹業務系にとどまらず、情報系システムや部門システム等その数が増加し、全体の中ではある程度大きな比率を占めるようになるとともに、その形態もホストコンピュータからクライアントサーバー、クラウドサービス、決済代行業等と連携した金融関連サービスなど、多様化してきている。

その過程で、安全対策基準は、基幹業務系システムの安全確保と安定運用という、当初の目的を果たしてきたものの、多様化する基幹業務系以外のシステムにおいては、その適用基準が不明確なままであり、その結果、安全対策の程度に過不足が生じ、場合によっては、新規開発等への投資が抑制されるなど、経営資源が適切に配分されないといった懸念が生じている。また、金融機関等において、システム開発・運用、サービス利用等において、外部委託への依存度が高まる中、外部に対する統制の重要度が増してきている。

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

本書では、以上の有識者検討会の提言内容を踏まえて、安全対策の考え方・利用方法等について理解頂くことを目的に、安全対策上必要となる IT ガバナンス・IT マネジメントについて解説した上で、リスクベースアプローチに基づく安全対策の基本原則及び、統制の拡充について安全対策の考え方を示していく。（[図 1] を参照）



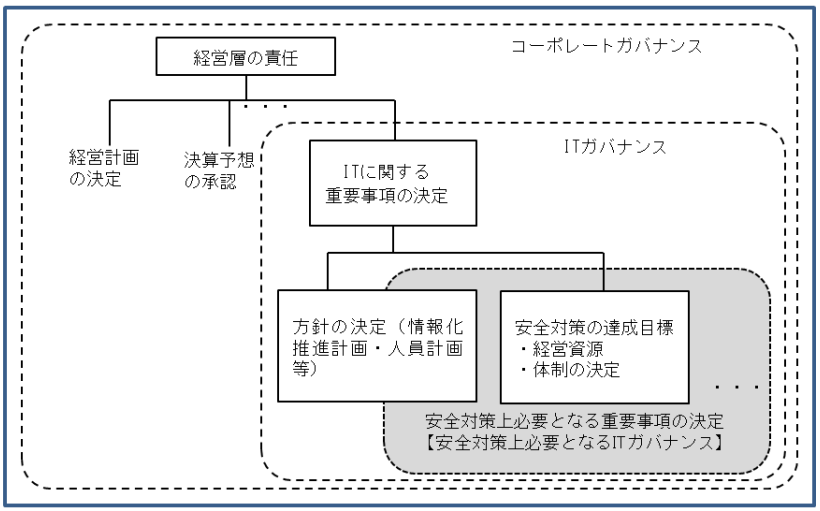
［図 1］安全対策基準改訂の考え方（概念図）

(1) IT ガバナンスと IT マネジメント

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

① 安全対策上必要となる IT ガバナンスの意義

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



［図 2］IT ガバナンスの階層構造

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

1）中長期計画等における安全対策に係る重要事項の決定

a. 安全対策に係る方針の決定

ⅰ. システム戦略方針の決定

ⅱ. システムリスク管理方針の決定

ⅲ. 安全対策の達成目標の決定

経営層は、金融機関等として、リスク特性[2]に応じ達成すべき安全対策の目標を決定する。また、その場合でも、大きなセキュリティ上の脆弱性を残さないことに考慮する。

ⅳ. 安全対策へ投下する経営資源の決定

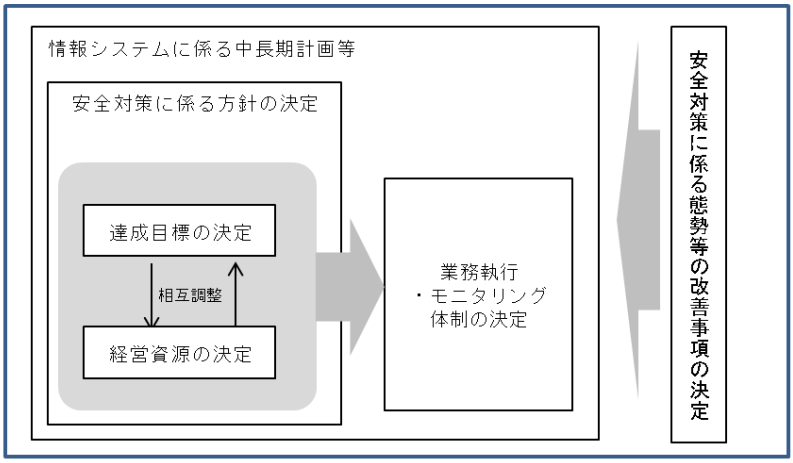
経営層は、安全対策の達成目標の決定と同時に、達成目標を実現するために必要となる経営資源の投下（費用・配分方針等）を決定する。経営層は、経営資源が有限であることを踏まえて、あらかじめ、保有する経営資源を踏まえた達成目標を検討するとともに、リスク特性に応じた資源配分を決定することが重要である。

b. 安全対策に携わる業務執行及びモニタリング体制の決定

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

2）安全対策に係る態勢等の改善事項の決定

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



［図 3］経営層が決定すべき安全対策に係る重要事項

② 安全対策上必要となる IT マネジメント

IT マネジメントとは、経営層による IT ガバナンスのもとで、管理者が、情報システム

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

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

1）管理者

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

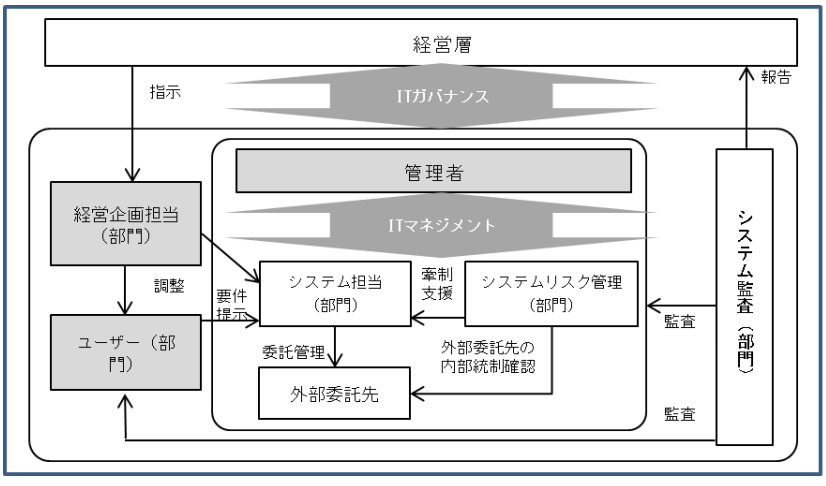
・内部規程・組織体制等の整備
・個々の情報システムに対する安全対策の決定
・内部規程・組織体制等の見直し
・安全対策上必要となる情報の経営層への報告

2）経営企画担当（部門）

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

3）ユーザー（部門）

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



［図 4］情報システムの安全対策に携わる関係者（例）

(2) リスクベースアプローチ

① 安全対策基準を取り巻く環境の変化

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

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

・「基幹業務のオンラインコンピュータ・システム以外の情報システム」に対する安全対策を「基幹業務のオンラインコンピュータ・システム」に設定されているのと一律に設定しておけば安心する、といった形式的で安全性に偏った選択を行ってしまう。
・「安全対策基準の考え方」に、安全対策への経営資源配分や、新規開発との経営資源配分の調整といった観点が示されていないことから、金融機関等の経営層の経営資源配分に係る決定プロセス等によっては、そのシステムにおいて必要十分ではない安全対策が最終的にそのまま実施されてしまう。
・経営層の立場では、ひとたび重大なシステム障害が発生すれば、その事実だけをもって、直ちにその結果責任を追及されかねないといった懸念から、経営層は、システム障害を極力ゼロとするために、そのシステムにおいて適正な水準以上の安全対策を承認する、あるいはみずから追求してしまう。

② リスクベースアプローチの意義

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

つぎに、こうした、リスクベースアプローチの考え方を導入する際には、「金融機関等がみずから」その安全対策の達成目標を決定することが前提となる。つまり、安全対策の達成目標は、第一義的には、金融機関等がシステムの安全性を確保しつつ、企業価値の最大化[3]を目指し、IT ガバナンスを発揮して、決定されることが重要である。

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

(3) 安全対策における基本原則

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

ただし、その一方で、金融機関等は、社会性・公共性を有していることから、リスクの顕在化による影響が、個別金融機関等による統制可能な範囲を超えて外部に及ぶ場合（以下、「外部性を有する」という）や、機微情報（要配慮個人情報を含む）等の流出により、プライバシーなど個人の人権等を侵害する場合（以下、「機微性を有する」という）を考慮に入れるべきである。

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

金融機関等の情報システムの安全対策における基本原則

○情報システムに対する安全対策の達成目標は、個々の情報システムのリスク特性に応じて、必要十分な内容で決定されるべきである。
○情報システムに対する安全対策への経営資源配分は、リスク顕在化後の事後対策と比較衡量したうえで、情報システム予算内での新規開発等との調整のみならず、経営資源全体も視野に入れ、企業価値の最大化を目指して、決定されるべきである。
○ただし、金融機関等が保有する重大な外部性を有する情報システム及び機微情報（要配慮個人情報を含む）を保有する情報システムにおいては、その社会的・公共的な観点から、このシステムの外部性や保有情報の機微性を考慮に入れた安全対策の達成目標が設定されなければならない。
○上記原則が遵守されたうえで、妥当な意思決定等が行われ、適切に運営されている限りにおいては、安全対策は独自に決定することが可能である。

コメント [FISC4]: 6/28 確認
「必要十分」の表現を見直すべきか？

コメント [FISC5]: 6/28 修正案

○情報システムに対する安全対策は、以下の考え方に基づき、適切な意思決定が行われ、運営されるべきである。
○情報システムに対する安全対策の達成目標は、、、である。
○情報システムに対する安全対策への経営資源配分は、、、である。
○ただし、金融機関等が保有する、、、されなければならない。

基本原則では、金融機関等は、IT ガバナンスが適切に発揮されている限りにおいては、リスクベースアプローチの考え方に基づき、保有する情報システムに対する安全対策を、必要十分な内容で、みずから決定することが可能としている。

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

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

【資料２－３】
平成 29 年 6 月 28 日更新
公益財団法人 金融情報システムセンター

（参考）「外部性」の考え方

・「外部性」とは、例えば、個別金融機関等の決済システムにおけるシステム障害等によって、他金融機関等社会全体に経済的損失を与える可能性のある性質をいう。例えば、決済システムは個別金融機関等で深刻なシステム障害が発生した場合、他金融機関等への信用不安に発展し、経済的損失が拡大する可能性のある性質を有する。

・「外部性」には、個別金融機関等の顧客は含まれない。なぜなら、顧客に対しては、相手を個別に認識し個別に対処可能であり、損失額を内部的に算定可能であるからである。

・一方、リスクベースアプローチに従って、適切に IT ガバナンスを発揮できる金融機関等であっても、「外部性を有する」情報システムに関する損害額等は正確には把握できない。つまり、個別金融機関等がシステム障害等に伴い社会全体に及ぼす損失額を正確に把握し、障害を防止するためのコストを事前に算定・内部化して、安全対策の立案に的確に反映させることは困難である。

・また、金融機関等の中には、インセンティブ上の問題（モラルハザード）等から、自社のシステム障害が引き起こす社会的影響の全部または一部を考慮の外に置いて、安全対策に係る意思決定を行う可能性もある。

・これらの問題に適切に対処するためには、特にリスクが高い「重大な外部性を有する」システムにおいては、金融機関等共通の規範となるルール（＝高い安全対策）が必要となる。

コメント [FISC6]: 6/28 確認
「重大な外部性」を有する具体的なシステムにおけるリスクについて、具体的なシステム名など、例示が可能か？

（参考）「情報の機微性」の考え方

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

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

・なぜなら、「機微情報（要配慮個人情報を含む）」は、本人等の許諾なく流出した場合、経済的損失に留まらず、プライバシー等、個人の人権等の侵害といった広範かつ甚大な損失を被る可能性がある。その取扱いは社会的・公共的な性質を有するものとも考えられることからも、「重大な外部性を有する」システムと同様に取り扱うことには合理性がある。

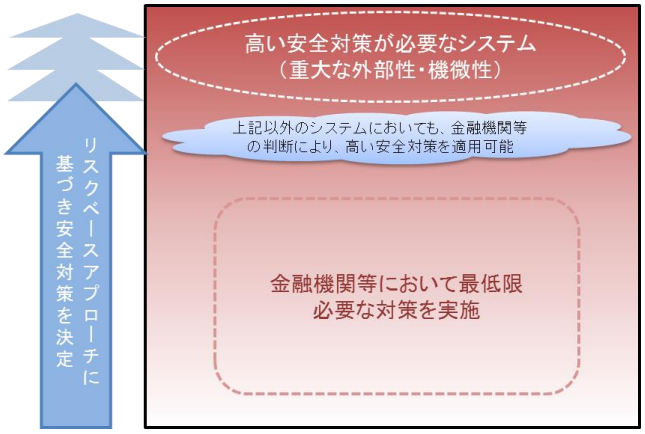
・仮に、これらが同一に扱われてしまった場合には、金融機関等のほとんどすべてのシステムに存在している個人情報が、この機微情報（要配慮個人情報を含む）に影響されて適正な水準以上の安全対策目標が設定され、資源の過剰配分が行われるおそれがある。

・このような事態を避けるためには、個人情報のうち、その保護のために最上位の安全対策目標が設定されるべき「機微情報（要配慮個人情報を含む）」と「その他の個人情報」を分け、「機微情報（要配慮個人情報を含む）」については、「高い安全対策」を適用することが妥当である。

(4) 基本原則に従った IT ガバナンス

金融機関等の経営層は、情報システムをそのリスク特性に応じて区分し、その評価された結果に基づき、新規投資等含めその効率の最大化を追求した経営資源配分を考慮したうえで、必要十分な安全対策の目標を包括的に決定する。この際、重大な外部性や機微性を有するシステムや、それらと同等以上のリスクを有するシステム[5]に対しては、「高い安全対策」を適用する。金融機関等の業務が情報システムに大きく依存している状況を踏まえ、経営資源配分の観点も含め、原則として、経営層みずからが、対象となるシステムを決定することが求められる。

「高い安全対策」が必要なシステム以外のシステムに対しては、金融機関等は、必要十分な内容をもって、安全対策の達成目標を決定することとなるが、顧客データの漏えい防止等、金融機関等のシステムが満たすべき最低限の対策は多くのシステムで共通すると考えられる。そこで、最低限の対策を予め設定することは、金融機関等が、リスクベースアプローチの考え方に基づき安全対策を決定する際、その不確実性を低減することに繋がると期待される。（[図 5] を参照）



[図 5] 基本原則に従った安全対策の考え方

(5) 安全対策における経営責任のあり方

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

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

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

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

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

金融機関等の情報システムの安全対策における経営責任のあり方

〇経営層の使命は、企業価値の最大化であり、このことは、必ずしもリスクゼロを目指した安全対策の追求を意味するものではない。
〇企業価値の最大化を目指した結果として、残るリスクについては、これを正当に認識したうえで、これに対応するために、その程度に応じて、コンティンジェンシープランを策定するとともに、環境変化に応じて見直すことが必要である。
〇経営層が、諸法令を遵守するとともに、安全対策基準等の社会的に合意されたガイドライン（前述の安全対策における基本原則を含む）等を踏まえて、安全対策や残存リスクに対するコンティンジェンシープラン等を用意し、かつ、有事においては、これらを踏まえつつ臨機応変に対応している限りにおいては、客観的立場から見れば、法的責任を果たしているものと評価されるべきである。

(6) 安全対策基準における「統制」のあり方

金融機関等における経営層は、基本原則に従って IT ガバナンスを発揮していくことが求められる。また、金融機関等において、外部委託への依存度が高まる中、安全対策基準は統制面での対策を拡充させていくことが求められる。これらの課題を解決していくには、安全対策基準において、統制面の対策を明示的に示すことが有効である。

① 「統制」と「実務」の区分

IT ガバナンス及び、 IT マネジメントを適切かつ効果的に発揮していくためには、経営層が、過去のやり方を機械的に継続するのではなく、多様で主体的な創意工夫を発揮し、安全対策における、統制と実務の適切なバランスを確保することが望ましい。

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

区分		基準の内容
統制	内部の統制	金融機関等において、セキュリティポリシーの策定や、教育・訓練を含む、管理態勢等を整備するために実施する対策
	外部の統制	外部委託管理等に関する基準として、外部への統制を具体化した対策
実　務		管理者が場面やリスク管理対象に応じて、具体的に実施する対策

［図 6］「統制」と「実務」の区分

② 外部に対する「統制」のあり方

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

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

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

金融機関等と委託先との間では、統制と実務において、各々が果たすべき役割（以下、責務という）が存在する[6]。安全対策の達成目標は、これら責務の分担と各々の責務の確実な遂行によって実現されるものであり、外部委託の一形態である「クラウドサービス」や、決済代行業等を営む事業者との新たな契約形態においても、これらの考え方と整合性が保たれることが必要である。

コメント [FISC7]: 6/28
オープン API 連携先など、既存の外部委託先とは異なる形での外部連携先などを考慮した内容に修正する予定。

[6] 一般には、金融機関等において、委託先に対する「統制」の責務が発生することになるが、委託先が再委託先を管理するための「統制」についても考慮する必要がある。また、決済代行業者等が、顧客への金融関連サービスを提供するシステムを運用し、その一部が金融機関等との接続を行う場合、運用主体である非金融機関と、接続される金融機関との間で、「統制」に係る責務の分担が発生すると想定される。

Ⅱ．フレームワーク

１．総論

(1) 安全対策基準における定義

① 金融情報システム

金融機関等が、業法等に基づき、顧客に商品・サービスを提供するために運用または利用[7]する情報システムを、「金融情報システム」と定義する。

② 特定システム・通常システム

金融情報システムのうち、システム障害等が発生した場合の社会的な影響が大きく、個別金融機関等では影響をコントロールできない可能性や、機微情報（要配慮個人情報を含む）の漏えい等により広範な損失を与える可能性があるシステムを、「特定システム」と定義する[8]。「特定システム」は、高い安全性の確保を必要とする。

特定システム以外の金融情報システムを、「通常システム」と定義する。通常システムにおいては、そのリスク特性に応じた安全対策を設定することが可能である。

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

③ 安全対策基準の構成

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

a. 統制基準

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

b. 実務基準

金融情報システムの信頼性・安全性の向上を図るために必要となる、システム企画・開発、運用、防災・防犯等に関する実務的な対策に関する基準・解説等から構成される。

---

[7] 金融業及び、それに関連するサービスを共同センター等の形態で運用する場合、金融機関等は、そのシステムを利用する側面を持つため、「運用」以外の形態の一つとして、「利用」を記した。

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

実務基準には、オペレーション等、管理者や作業者等が主体となる対策と、関連する技術的対策が含まれる。

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

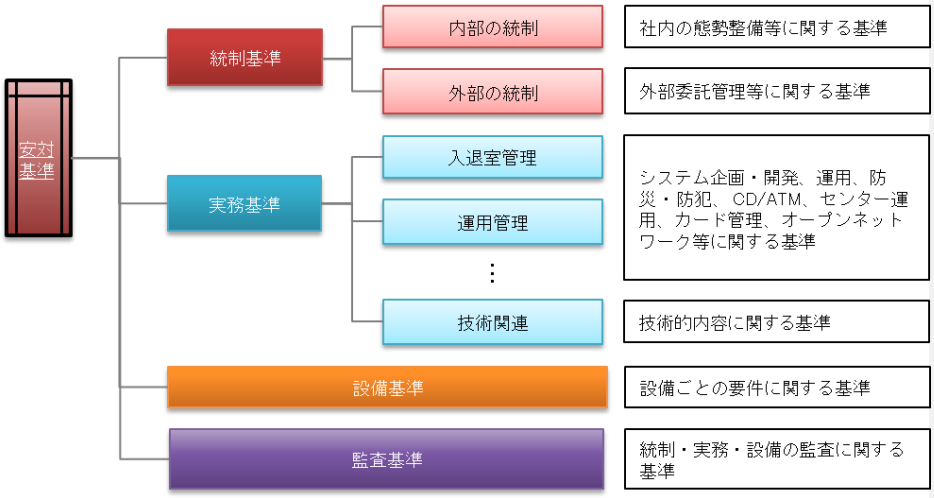
c. 設備基準

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

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

d. 監査基準

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



［図 7］安全対策基準の構成

(2) 基準の分類

本書では、金融機関等がリスク特性に応じた安全対策の目標を設定するうえで、最低限の対策が実施されないといった不確実性を低減するために、安全対策基準の中から「基礎基準」を選定している。

基礎基準は、特定システム、通常システムによらず、金融情報システムに最低限適用する基準であり、統制基準、監査基準及び、実務基準のうち顧客データの漏えい防止等の観点から抽出した一部の基準で構成されている。

「付加基準」は、「基礎基準」以外の基準として、リスク特性に応じて追加・選択する基準である。

通常システムでは原則として「基礎基準」を適用するとともに、リスク特性を踏まえ、「付加基準」から必要な基準を選択・追加する。特定システムでは、「基礎基準」及び、「付加基準」を原則として適用する[9]。（[図 8]を参照）（詳細は、(4)安全対策決定のプロセスを参照）

削除: 全ての

削除: 全て

コメント [FISC8]: 6/28 修正案
「全て適用」を「原則として適用」に修正。

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

［図 8］基礎基準と付加基準

なお、設備基準は、既に、コンピュータセンターに求められる基準と、本部・営業店等、各拠点に求められる基準を区分して記載しているため、「基礎基準」及び「付加基準」を区分しない。

（補足１）「基礎基準」とした安全対策について

金融情報システムのリスク特性は、多岐にわたり、全てのシステムが最低限満たすべき安全対策を一意に決定することは困難であるものの、一般に金融情報システムは、商品・サービスを顧客に提供するため、顧客データを保有または、顧客データに接続していると想定されることから、顧客データの漏えい防止に関する対策を、最低限の安全対策と位置付けている。なお、金融情報システムには、顧客データ以外の重要なデータ[10]が含まれる場合があるが、この場合も顧客データ漏えい防止の対策が有効と考えられる。

また、近年において、サイバー攻撃対策の重要性が増してきていることから、顧客データの漏えい防止に関する安全対策には、サイバー攻撃対策として必要な対策を含めている。

さらに、リスクベースアプローチの考えでは、安全対策の設定において、必ずしもリスクゼロを追求しないことから、金融機関等においては残存リスクへの対応を考慮する必要がある。このため、コンティンジェンシープラン策定に関して実施すべき対策についても、基礎基準を設定するための条件としている。

上記以外の観点で必要となる安全対策については、システム毎のリスク特性に差異があり、各金融機関等が、システム構成やリスク評価の結果等も考慮のうえ、適宜、必要な対策を選

9 例えば機微性を有するシステムにおいて、可用性に関する安全対策を一部選択しないことも考えられる。各金融機関等は、みずから定めた安全対策の目標に応じて、基準を選択・適用していく。
10 法人情報や企業の公開前決算情報など、金融機関等において高い機密性が求められる情報を指す。

択することとなる。例えば、通常システムにおいて高い可用性が求められる場合は、可用性を確保するための安全対策の目標を定め、「付加基準」の中から適宜、必要な対策を選択・追加することで、必要十分な安全対策となるよう考慮することが必要となる。

上記を踏まえ、「基礎基準とした安全対策」を以下に示す。

・統制・監査に関する対策
・顧客データの漏えい防止において実施すべき対策[11]
・コンティンジェンシープラン策定に関して実施すべき対策[12]

（補足２）外部の統制における「基礎基準」について

外部の統制における一部の基準には、ベストプラクティス（努力目標）としての対策が示されており、必ずしもすべてのシステムで実施すべき対策とはなっていない。このため、同基準には代替策として、「～することも可能である。」といった必要最低限の対策を示している。これらの代替策は、リスクベースアプローチの考えに基づき、通常システムにおいて選択可能としている。

コメント [FISC9]: 6/28
外部委託に関する基準整理の検討の中で、記述の修正あるいは削除を検討する。

（補足３）決済代行業者等における安全対策基準の適用について

決済代行業者等を含む一部の非金融機関が、金融関連サービスを提供するシステムの安全対策を策定する場合、サービスの利用者からは、金融機関等が提供するサービスと同等の安全性確保が求められる。このため、これらの事業者によって実施される安全対策は、基礎基準を満たすことが期待される。

コメント [FISC10]: 6/28
FinTech 有識者検討会の報告内容を反映する形で、記載内容の見直しを行う。

[11] ハードウェアの保守等、対策を実施しないことで、ただちにリスク事象の発生に繋がらない予防的に実施する対策については、基礎基準としていない。
[12] システムごとの障害復旧マニュアル等は、コンティンジェンシープランの内容に応じて適宜必要性を判断するものであり、基礎基準としていない。

(3) 安全対策基準の適用対象

安全対策基準は金融情報システムに適用される。共同センター等[13]、金融機関等が統制を行うシステムは、外部委託と同等の性質を有するものとして、必要となる安全対策を設定する。

なお、金融機関相互のシステム・ネットワーク等[14]は、金融機関等が共同して運営するものであり、個別金融機関等が負う管理責任が部分的となる「外部のシステム」として区分している。これらは、主にサービスの利用者の視点で実施すべき対策等、外部委託の統制面において必要となる安全対策を設定する。

金融機関等における、金融情報システム以外のシステムについては、安全対策基準の適用対象外であるが、その技術基盤（セグメント等）の共通性や、金融情報システムとのリスク特性の類似性がある場合は、必要となる対策を適宜取り入れることとする。また、非金融機関等が金融関連サービスを提供するシステムについては、各業界等で定める基準・ガイドライン等に従うことが想定されるものの、その際、安全対策基準を参考として運用されることが期待される。

（補足）金融機関等における特定システムと通常システムの分類

個別金融機関等における共通的なシステムの分類は、業態ごと[15]、または個別金融機関等における重要度によって様々であり、それらを一律に特定し、列挙することは困難であり、どのシステムが「通常システム」または「特定システム」に分類されるかは、個別金融機関等の実態に則して判断することが必要となる。安全対策基準を適用するに当たっては、経営層が適切な IT ガバナンスを発揮したうえで、個別金融機関等におけるリスク評価や、経営資源配分等の観点を考慮した上で対象となるシステムを決定することが求められる。

[13] 金融機関等がベンダーと契約するものや、協同組織等を通じてベンダーと契約するものなどが含まれる。
[14] 全銀ネット、CAFIS、統合 ATM、協同組織金融機関為替中継システム、SWIFT、LINC、損保ネット等は外部のシステムと定義している。その他、日銀ネット、でんさいネット、ほふりシステム、証券取引所システム等も、ここに分類される。
[15] 一般に、預取金融機関における為替システム、預金システム等は、重大な外部性を有すると想定され、生命保険会社等における、給付金査定等を行うシステムは、機微性を有すると想定される。証券会社におけるトレーディングシステムや、インターネットバンキングを主なチャネルとする預取金融機関におけるインターネットバンキングシステムなどは、特定システムと同等に扱うことが可能である。一方で、類似のシステムを有する金融機関等においても、そのシステム構成や、利用形態を鑑み、特定システムとしない判断も可能である。

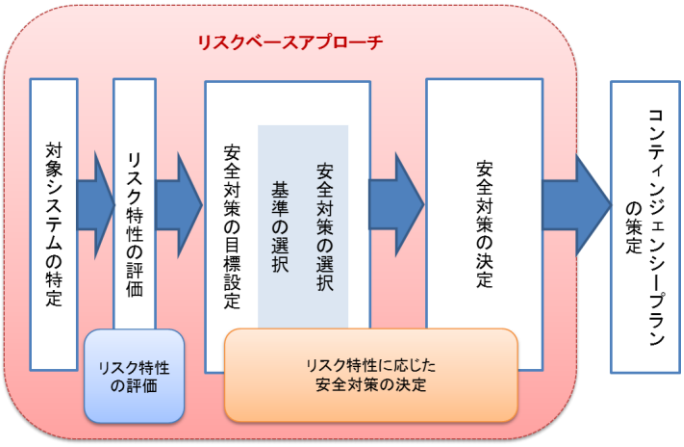
(4) 安全対策決定のプロセス

コメント [FISC11]: 6/28 修正案
タイトルを「安全対策基準の適用方法」から変更し、図９の工程（修正後）に従って、以下の構成を全体的に見直した。

削除: 安全対策基準の適用方法

① リスクベースアプローチに基づく安全対策基準の適用

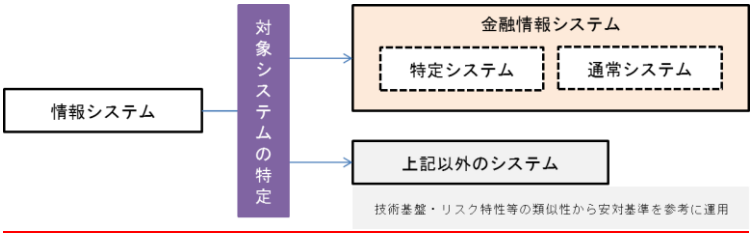
リスクベースアプローチでは、その経営資源配分の効果が最大となるよう安全対策を決定していく。経営資源配分の効果を最大化するためには、安全対策基準の適用対象となるシステムを特定した後、各システムのリスク特性を分析し、安全対策の目標を定め、必要なる基準及び、安全対策の選択を行う。さらに、安全対策の目標に対し、安全対策費用とその効果、及び新規開発投資とその効果、それぞれについて、効率が最大化されるよう考慮のうえ、最終的に安全対策を決定する。その結果、残存リスクが発生する場合は、必要に応じて、コンティンジェンシープランを策定する。([図 9]を参照)



［図 9］安全対策基準適用のプロセス

② 対象システムの特定

金融機関等は、保有または利用する情報システムから、安全対策基準の適用対象となる金融情報システムを特定する。金融情報システム以外のシステムについては、その技術基盤の共通性や、リスク特性に類似性がある場合、安全対策基準を適宜取り入れる。([図 10]を参照)



［図 10］対象システムの特定

③ リスク特性の評価

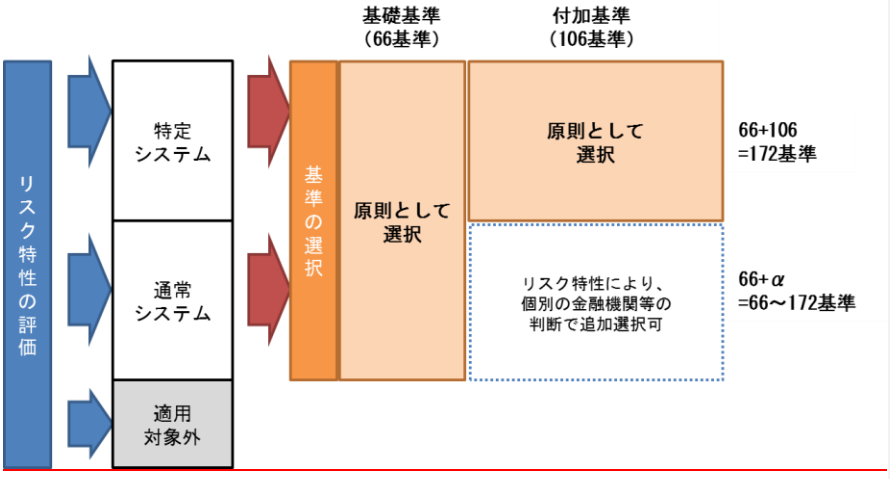
適用対象となるシステムを特定した後、システムのリスク特性を評価し、社会的・公共的に高い安全対策が求められる特定システムと、それ以外の通常システムを区分する。この際、各金融機関等の判断により、通常システムの中から、高い安全対策が必要なシステムを独自に選択することも可能である。一方で、特定システムの一部において、リスク特性が低いと判断されるサブシステムにおいて、リスク管理上、当該サブシステムを分離することが可能な場合等、これを通常システムとして取り扱うことも可能である。

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

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

④ 安全対策の目標設定（基準の選択・安全対策の選択）

リスク特性の評価結果[16]に応じ、安全対策の目標を設定する。個々のシステムに対する安全対策の目標設定とは、リスク特性に応じて選択した基準から、どの対策を実施すべきか選択することである。IT ガバナンスを適切に発揮し、適切な目標を設定するためには、目標設定の方針が定められていることが望ましい。目標設定の方針は、システムリスク管理方針や、セキュリティポリシー等を踏まえ、経営層の関与のもと決定されることが望ましい。IT マネジメントを担う管理者等は、設定された安全対策の目標を達成するために、必要となる基準および対策を選択する。



［図 11］システムの区分・基準の選択

16 リスク評価に関する手法は様々であり、一律に示すことは困難である。一般的な手法については、当センター発行の『金融機関等のシステムリスク管理入門』などを参考に、各金融機関等の状況等に応じて検討されるものであり、安全対策基準では、具体的手法については示していない。

安全対策の目標設定では、システム障害件数の低減や、システムの稼働率など、具体的な数値目標等に基づき決定することも考えられる。

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

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

なお、基準の選択および対策の選択において、システム構成や、リスク特性から、明確に不要な対策を予め選択しないことも考えられる[17]

⑤ 安全対策の決定

安全対策の目標が設定された後、経営資源配分の観点等を踏まえ、最終的な安全対策を決定する。安全対策の決定においては、実施する安全対策の程度[18]や、実施時期等についても検討し、セキュリティ上の大きな脆弱性を残さないことが求められる。安全対策を決定した結果、残存リスクが発生する場合は、コンティンジェンシープランを策定し、適切にリスクに対応できる態勢を整備しておくことが求められる。

⑥ コンティンジェンシープランの策定

残存リスクに対するコンティンジェンシープランの策定は、金融機関等が策定する必要最低限の安全対策と位置付けている。

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

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

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

コンティンジェンシープランの目的は、従来から推進されている安全対策の積み重ねを前提に、これらの対策では防ぐことのできなかった緊急事態に際して、可能な限り影響を軽減し、早期に業務を復旧させることにある。

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

17 外部ネットワークに接続しないシステムにおいて、外部ネットワークの機器設定に関する基準等、システム構成やリスク特性から判断し、明確に不要な対策を省略することも可能である。

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

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

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

２．統制

金融機関等においては、安全対策を決定するうえで、基本原則に従った IT ガバナンスを発揮することが前提となる。このため、これら統制に関する対策は、原則として全て「基礎基準」としている[19]。統制には「内部の統制」と「外部の統制」に関する対策が含まれるが、両者は「統制」の対象や、統制の方法が異なる。ここでは、これら「統制」の内容と、ルールの導出に至る考え方について解説する。

(1) 内部の統制

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

安全対策基準上は、内部の統制を、以下のカテゴリーに分類している。

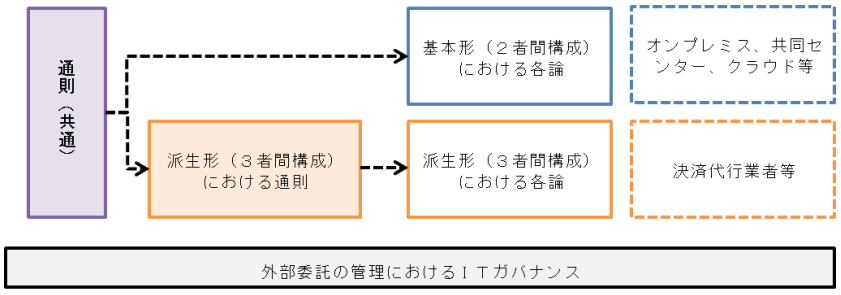
a. 方針・規程
b. 組織体制
c. サイバー攻撃対応態勢
d. 人材（要員・教育）

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

(2) 外部の統制

金融情報システムにおける「外部の統制」は、以下のように体系化される。IT ベンダー等とのシステムの開発・運用や、クラウドベンダー等との２者間構成の委託に加え、決済代行業者等のように、IT ベンダーと金融関連サービスを提供する性質を併せ持つ関係者を含む、３者間構成について、「外部の統制」における考え方を解説する。（[図 12] を参照）

コメント [FISC12]: 6/28
決済代行業者の中でも、外部委託先とは異なる場合を考慮する必要がある。



[図 12] 外部の統制における考え方

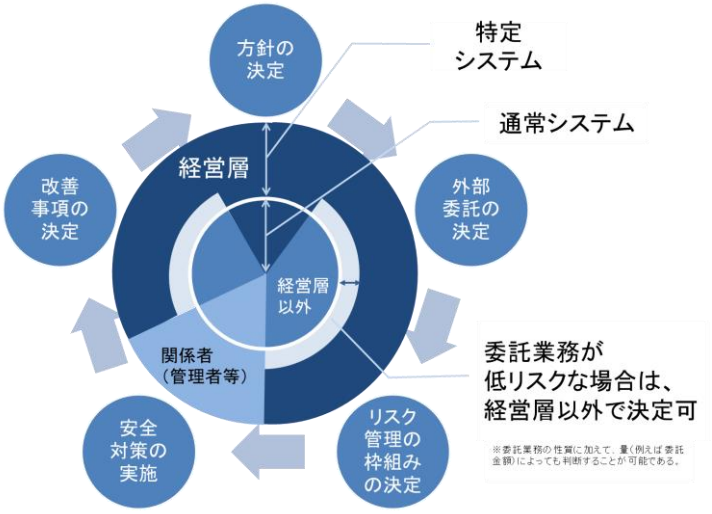
[19] 基礎基準のうち、「～することも可能である」として軽減策を示している場合、特定システムを除き、「可能である」とした内容を実施することができる（統制基準・実務基準共通）。

① 外部委託の管理における IT ガバナンス

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

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

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



[図 13] 外部委託の管理プロセスにおける IT ガバナンス

② 通則（基本形・派生形共通）

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

外部委託における共通の管理項目は次のものが考えられる。
・委託先の選定要件の策定と事前審査の実施
・委託先への監査権の明記
・有事対応
上記について、外部委託管理における考え方を解説する。

a. 委託先の選定要件の策定と事前審査の実施

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

b. 委託先への監査権の明記

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

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

c. 有事対応

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

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

③ 基本形（２者間構成）における各論

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

a. オンプレミス

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

b. 共同センター

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

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

c. クラウドサービス

クラウドサービスは、外部委託の一形態として位置付けられ、いくつかの利用形態[20]が存在する。クラウドサービスの特徴として、複数の事業者が単一のクラウド事業者に委託する場合に、利用者間で何らコミュニケーションが無いという「匿名の共同性」や、情報処理拠点が複数の国や地域にまたがる「情報処理の広域性」、そして仮想化技術や、データの秘匿性等における「技術の先進性」などが挙げられる。

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

④ 派生形（３者間構成）における通則

決済代行業者等は、IT ベンダーと類似の技術的な性質を有するとともに、金融関連サービスといったビジネスモデルの企画実施等を行う業務的な性質もあわせて有しており、

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

こうした技術的な性質と業務的な性質を同時に有する関係者を含めた、金融機関、IT ベンダー、決済代行業者等を加えた３者構成について、安全対策上、２者間構成である基本形とは異なる点に留意する必要がある。金融機関等の経営層は、イノベーションの発揮によって得られるメリットと、リスク管理上の考慮事項を比較衡量のうえ、外部への統制を適切に実施することが求められる。

a. 同等性の原則

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

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

b. 再配分ルール

金融機関等は、決済代行業者等の安全対策遂行能力を確認したうえで、仮に決済代行業者等の能力を超える過大な責務があれば、その部分については、金融機関や IT ベンダーが分担することで、決済代行業者等の革新性を損なわずに、安全対策の効果を達成できるよう、３者間にて責務の再配分を行なうことが望ましい。すなわち、この問題を解決するには、２者間構成を念頭に置いた従来の安全対策基準において求められる責務との整合性を維持しつつ、その責務を、３者間構成の各類型における役割や、安全対策遂行能力（保有する経営資源等）に応じて、合理的に再配分することを指す。

c. リスク特性に合う管理策の適用

決済代行業者等のシステムが、金融機関等の特定システムをはじめとする重要なシステムと連動する場合においても、それ自体一つのシステムとして完結性を有し、さらにそのリスク特性が金融機関等の特定システムのリスク特性と顕著に異なり、リスク事象を金融機関等の特定システム本体に波及することを防止が可能な場合は、当該システムを通常システムとして扱うことが可能である。

⑤ 派生形（３者間構成）における各論

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

a. タイプＡ（金融機関等が安全対策の決定を主導するケース）

タイプＡは、金融機関等が IT ベンダーへ委託する形態において、決済代行業者等または、IT ベンダーが委託先となる形態である。この場合、委託先が IT ベンダー、再委託先が決済代行業者等という形態もあり得る。基本形における、オンプレミスと同様の考

え方に、派生形の通則を付加した形態として整理できる。

このため、タイプＡの安全対策の在り方としては、まず、金融機関等は、決済代行業者等の安全対策遂行能力を確認したうえで、IT ベンダー及び、決済代行業者等と合意の上、従来の安全対策基準における外部委託に関する責務を、３者間で再配分することを考慮する必要がある。再配分に当たっては、「同等性の原則」にしたがって、必要な範囲を超えて関係者の負担が増加することがないよう留意する必要がある。

また、決済代行業者等が金融機関等の子会社となる形態も考えられる。この場合、金融機関等において、子会社に対する責任が付加される点を除いては、考慮点に差異はなく、同等性の原則ならびに責務の再配分ルールを踏まえた統制を行うことが必要となる。

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

タイプＢは、金融機関等以外の事業者が、金融関連サービスを主として提供するケースである。この場合、金融機関等が担う金融関連サービスに対する安全対策上の責務が部分的となる点が、基本形またはタイプＡとは異なる。例えば、決済代行業者等が、利用者からの決済指示を受け、預取金融機関の勘定系システムに対し入出金の指示を行うなど、金融機関等に代わり、決済代行業者等が金融関連サービスを提供するため、システムの安全対策は原則的には決済代行業者等が担うものの、顧客データの保護など、一部の責務について金融機関等がその安全対策の確保を決済代行業者等に求めるなど、部分的な責務が金融機関等において発生する場合を指す。

タイプＢにおいて、対象となるシステムは決済代行業者等が運用することを想定しているものの、金融機関等においても部分的な責務が発生することから、これらは金融情報システムに準じて取り扱うことが妥当である。この場合、同等のリスク特性を持つ金融情報システムにおける安全対策に対し、同等性の原則、責務の再配分などを踏まえ、金融機関等が実施する金融関連サービスと比較し、安全対策の水準において整合性が保たれることが必要となる。

なお、決済代行業者等が運用するシステムが、金融機関等のシステムと接続する場合、本人確認手続きや、顧客情報の保全等は必要最低限実施すべき対策と考えられる。このため、これらの金融関連サービスを適用する場合においては、基礎基準で示した安全対策を準用[21]することが求められる。

[21] 「準用」とは、安全対策基準の中で、限定的な一部の安全対策について実施することを言う。例えば、預取金融機関機関における勘定系システムに対し、オープン API 等による接続が行われる場合は、当該システムはインターネットバンキングに類似するリスク特性を有していると解され、「情報の保全」「認証」に関連する安全対策を中心に、安全対策を選択することが求められる。

【資料３－１】
平成２９年６月２８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53回安全対策専門委員会
検討事項に関するご意見（メール回答用）

電子メールにて、ご連絡願います。（fisc40@fisc.or.jp）

〆切　7/4（火）（改訂原案（前説）・対応方針案に対する事後意見）

会社名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

お名前：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

資料番号	項番	ご意見
（例） 資料２－３	（例） Ⅱ．１． （３）	・・・