# FISCのご紹介

公益財団法人 金融情報システムセンター

# FISCの概要

公益財団法人 金融情報システムセンター
（FISC：The Center for Financial Industry Information Systems）

金融情報システムに関連する各種の課題（技術、利活用、管理態勢、脅威と防衛策等）について総合的な調査研究を行うことを目的として、銀行、証券会社、保険会社、コンピュータメーカー、情報処理会社等の出捐により大蔵大臣（当時）の許可を得て、1984年11月に財団法人として設立。2011年4月に内閣総理大臣の認定を受け公益財団法人に移行しました。

## 会員構成

正会員　530機関（うち金融機関515）

（都市銀行、信託銀行、地方銀行、第二地方銀行、信用金庫、信用組合、労働金庫、農林中央金庫、各都道府県信連、商工組合中央金庫、外国銀行、その他銀行、生命保険会社、損害保険会社、証券会社、銀行系カード会社、電気通信・情報通信会社メーカー、情報システム会社等）

賛助会員　112機関（うち金融機関28）

スタートアップ会員　3機関

合計　645機関（2018年3月31日現在）

# FISCガイドライン

## 金融情報システムに関する自主基準（ガイドライン）策定

会員企業や学識経験者等の皆様の協力を得て、金融情報システムの安全性確保や金融業務の安定的遂行のための自主基準を策定しています。これらは、金融機関や、金融機関に情報システムを提供するコンピュータメーカー等で広く用いられています。

- 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
  （初版1985.12、第9版2018.3）
- 金融機関等のシステム監査指針　（初版1987.7、改訂第3版追補2016.5）
- 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
  （初版1994.1、第３版追補３ 2017.5 ）
- 金融機関等におけるセキュリティポリシー策定のための手引書（初版1999.1、第２版2008.6）
- 金融機関等におけるIT人材の確保・育成計画の策定のための手引書（初版2018.3）

金融情報システムセンター
The Center for Financial Industry Information Systems

# FinTechに関する安全対策の在り方について

2019年3月13日

公益財団法人 金融情報システムセンター
企画部　主任研究員　荒井 孝浩

# 目次

# （１）国内および国外のFinTechに関する動向

近年、金融機関、業界団体及び監督当局等において、FinTechと総称されるITを活用した革新的な金融サービスへの取組みが、急速に活発化している。

国内

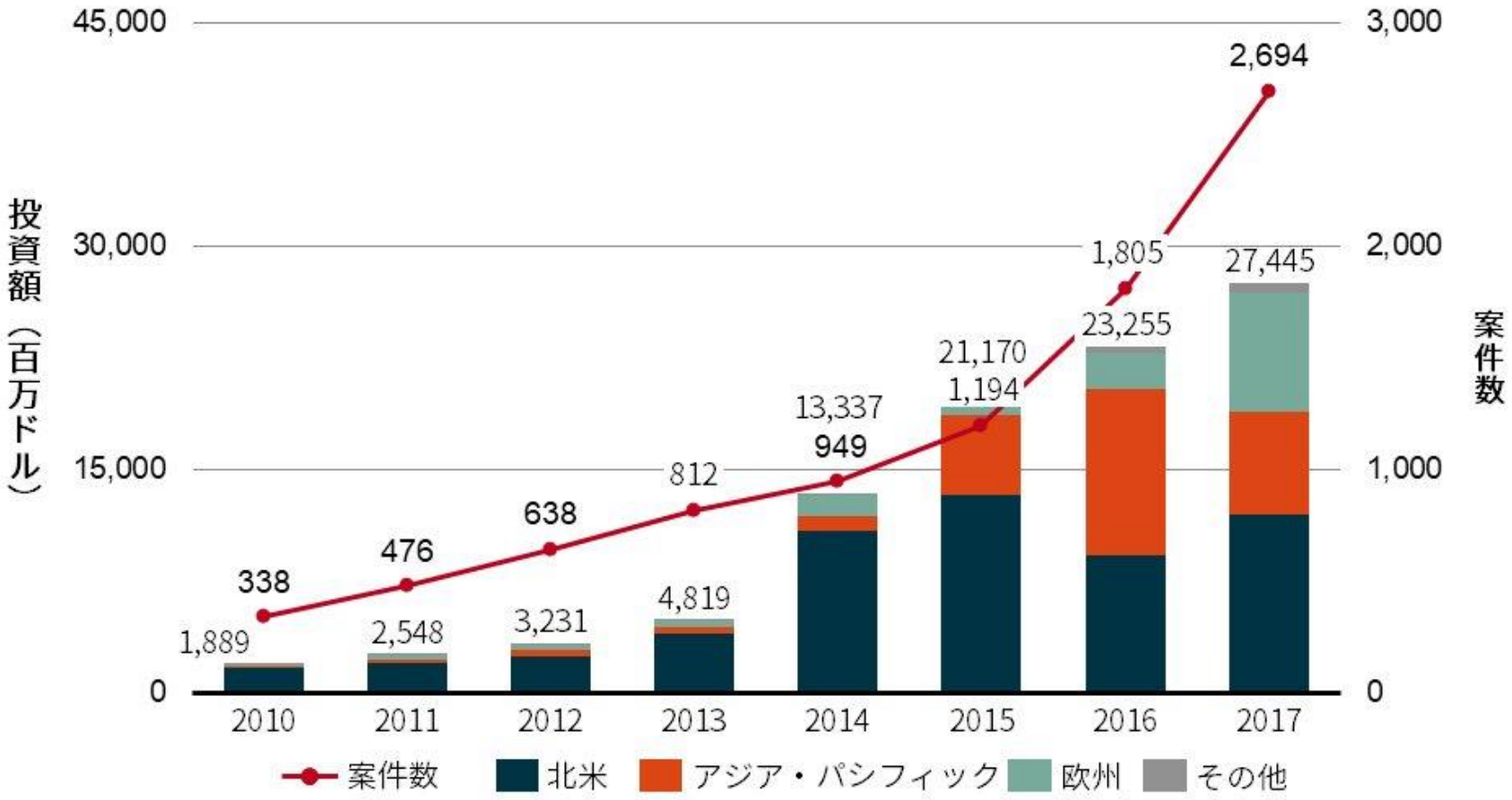
- 市場規模は引き続き拡大
- 金融制度ワーキング・グループ報告（平成28年12月）
- 全国銀行協会の取組み 「オープンAPIのあり方に関する検討会」 等
- Fintech協会の取組み 「API連鎖接続についての検討」 等
- FISCの取組み 「FinTechに関する有識者検討会」、「APIチェックリストに関するWG」 等
- **改正銀行法の施行（平成30年６月）**

海外

- 米国通貨監督庁
  「連邦銀行制度における責任あるイノベーション支援」 （平成28年３月）
  「責任あるイノベーションの枠組みを実行するための勧告および決定」 （平成28年10月）
- 英国 Open Banking Working Group
  「The Open Banking Standard」「The Open Banking Limited」 （平成28年２月）

# （２）FinTech投資の推移

## グローバルフィンテック投資の推移




出典：アクセンチュアによるCB Insightsデータの分析

出典：「フィンテックがもたらす事業社会：社会構造変革への挑戦」　（アクセンチュア　平成30年５月29日）

# （３）「FinTechに関する有識者検討会」の開催

## 有識者検討会とは

有識者検討会とは…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、当センターの理事長の諮問機関として設置するもので、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

（※）過去取り扱ったテーマ

- ・サイバー攻撃対応　金融機関のサイバー攻撃対応の在り方について検討
  （開催時期：2013年６月～2015年７月※途中休会あり）
- ・クラウド利用　クラウド特有の論点や適切なリスク管理・契約管理の在り方について検討
  （開催時期：2014年４月～2014年10月）
- ・外部委託　外部委託管理の在り方についてITガバナンスやリスクベースアプローチの観点も踏まえて抜本的に検討開催時期：2015年10月～2016年6月）

## FinTechに関する有識者検討会　運営体制・日程

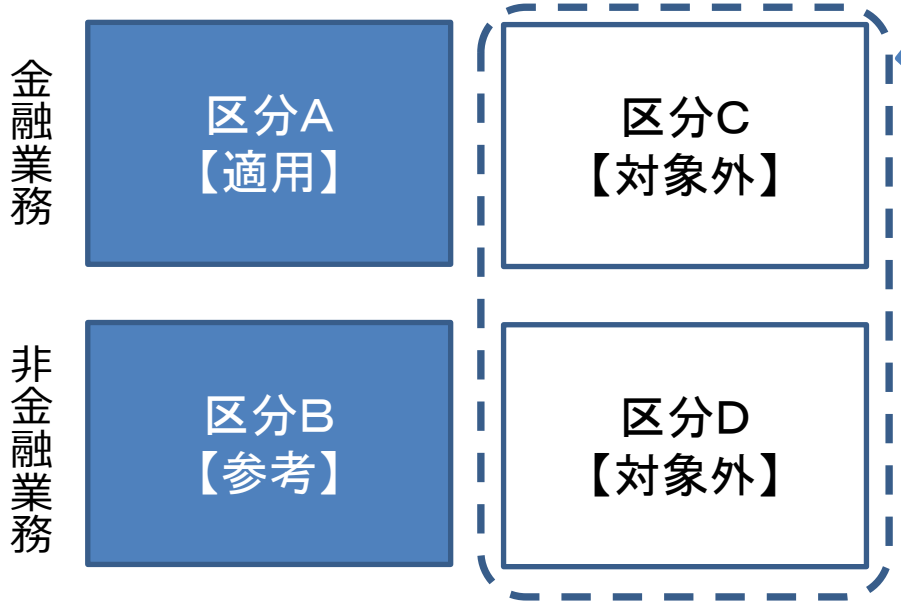
- 2016年10月 「金融機関におけるFinTechに関する有識者検討会」を設置
  - 座長：岩原紳作 早稲田大学大学院法務研究科教授
  - 座長代理：渕崎正弘 株式会社日本総合研究所 代表取締役社長
  - 委員：
    - 学術界：安冨潔　慶應義塾大学名誉教授、國領二郎 慶應義塾常任理事　他
    - 金融業界：都銀、地銀、ネット銀、生保、損保、証券
    - 実務界：FinTech企業、ITベンダー、クラウドベンダー　等
    - オブザーバー：金融庁、日銀、総務省、経産省
- 全６回の会合を開催
  （第1回 2016年10月5日、第2回 同12月1日、
  第3回 2017年2月2日、第4回 同3月23日、第5回 同5月15日、第6回 同6月13日）
- 2017年6月21日 報告書を公表（FISCホームページ https://www.fisc.or.jp/ に掲載）

# （４）安対基準の対象外となるFinTech業務の取扱いに関する議論

＜FinTechに関する有識者検討会における議論＞

安対基準の対象となる情報システムは「金融機関が行う金融業務」を担う情報システムである。利用者の立場に立てば、金融機関と非金融機関のいずれが行う場合においても、シームレスに一体不可分な形で、適切な安全対策が実施されることが期待されている。したがって、非金融機関においても、安対基準の規範性が及んでいることが期待される。

安対基準の適用対象の取扱い




【非金融機関に規範性が生ずる方法】

- 非金融機関であるFinTech企業が個別にFISCの会員となり、安対基準の策定過程に明示的に参画するとともに、FinTechの観点からその基準策定に貢献するとともに、安対基準を遵守する。
- FinTech企業の業界団体がFISC会員となり、業界団体が代表して、安対基準の策定過程に明示的に参画するとともに、FinTech業界の観点からその基準策定に貢献する。また、安対基準と整合的なFinTech業界の自主基準を策定し、業界団体の会員がそれを遵守する。

# （５） FinTech業務における安全対策に関する意見表明

【意見表明】

FISC「金融機関におけるFinTechに関する有識者検討会」は、FinTech業務を実施するのが金融機関であるか否かに関わらず、FinTech業務を担う情報システムにおける安全対策の在り方について、高い関心を持っている。そうしたことから、FinTech業務に携わる事業者においては、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する。

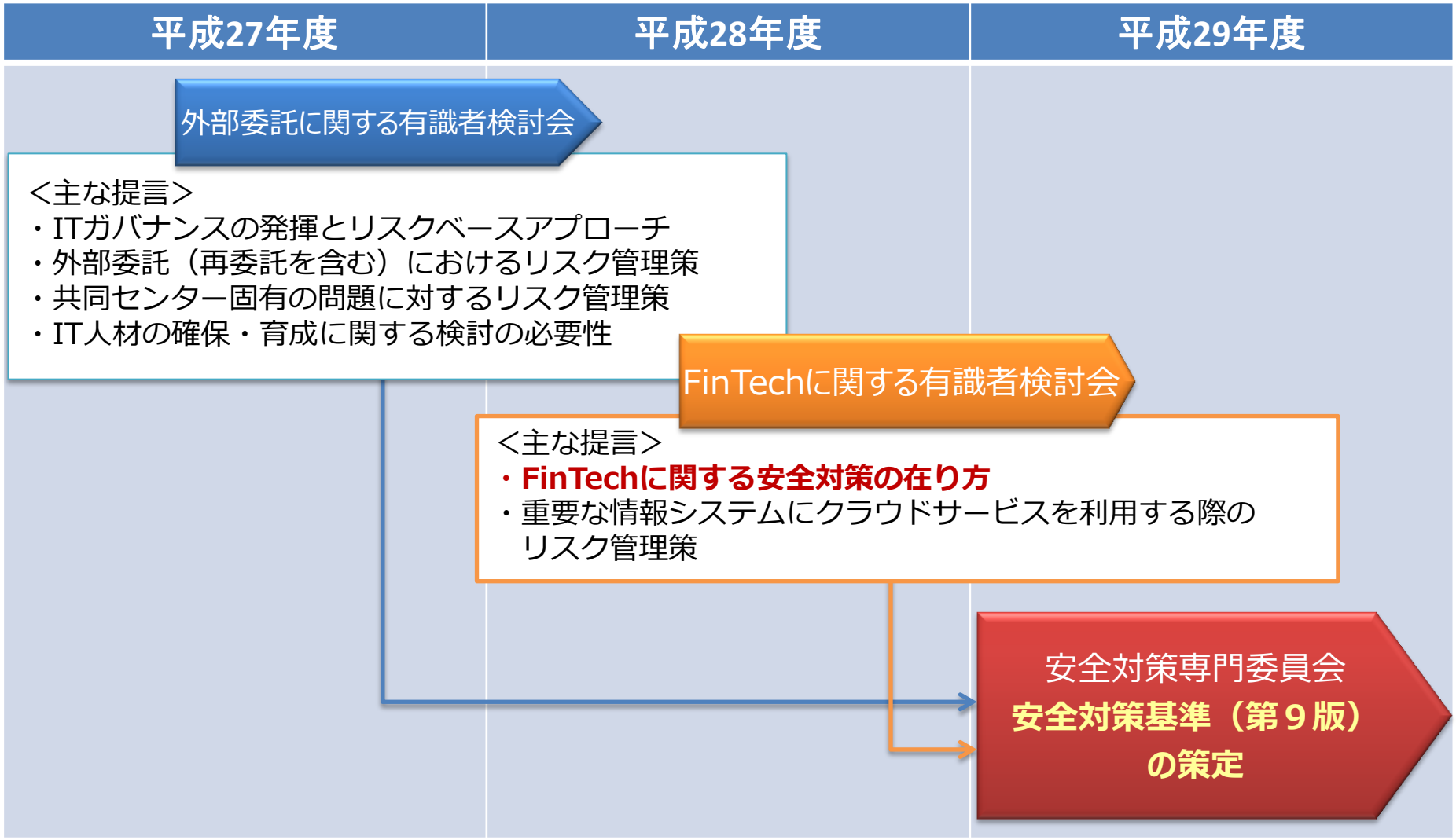
（１）金融関連サービスの提供に携わる事業者は、その利用者が安心してサービスを利用できることを目指し、みずからが管理責任を負う情報システムに対して、**適切な安全対策を実施する**。

（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**。

# （６）有識者検討会を踏まえた安全対策基準の改訂

FinTechに関する有識者検討会等の提言を踏まえ、安全対策基準（第９版）を策定。



# （１）安全対策基準の改訂とFinTechに関する安全対策

安全対策基準（第９版）では、「安全対策の考え方」が見直された。

※　第９版では、FinTechに関する有識者検討会にて整理された「安全対策の在り方（提言）」を踏まえ、FinTechに関する安全対策の在り方についても記載している。

## 安全対策基準（第９版）

**考え方①**

**「ITガバナンスに基づくリスクベースアプローチ」**

**考え方②**

**「金融関連サービスにおける安全対策の在り方」**

**考え方③**

**「３者間構成における外部の統制」**
（金融機関＋ITベンダー＋**FinTech企業**）

**＜FinTechに関する安全対策の在り方＞**

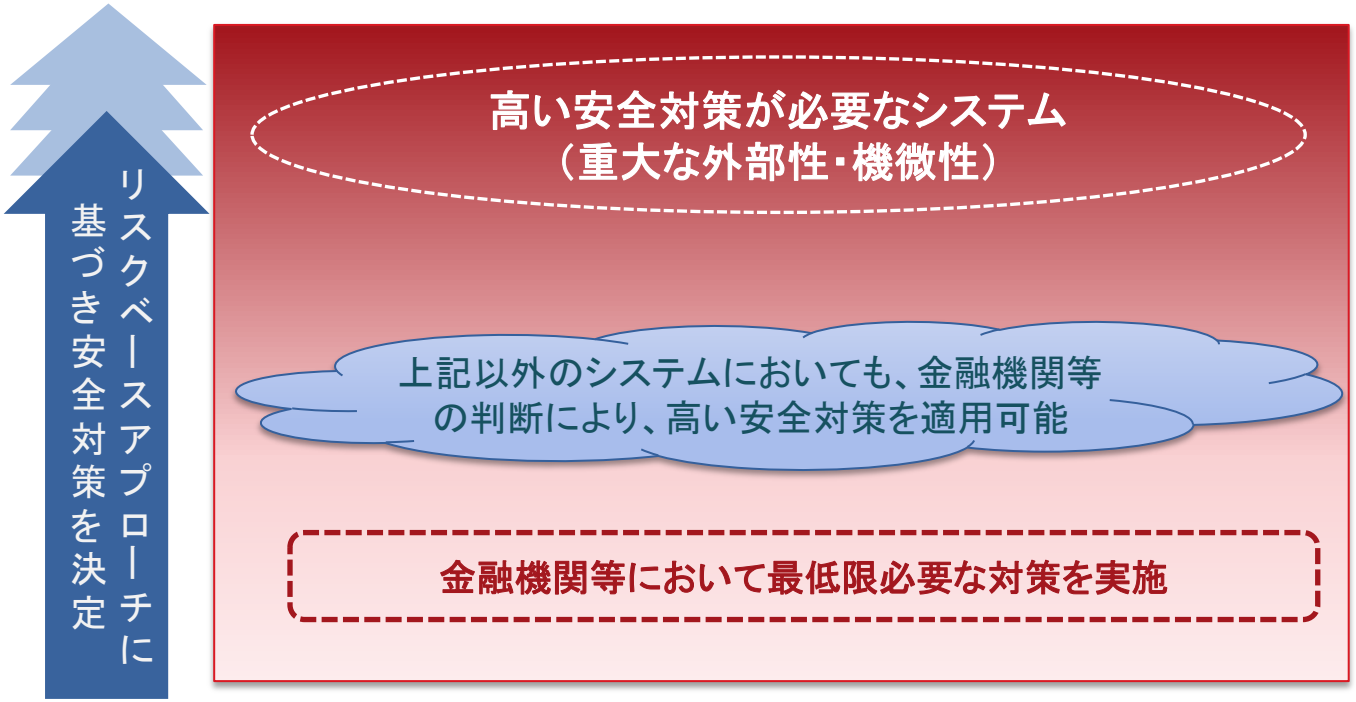
- 安全対策基準の部分適用（外部委託における「準用ルール」）
- 「再配分ルール」
- 「協調性の原則」

# （１）安全対策基準の改訂とFinTechに関する安全対策（つづき）

## 考え方①　ITガバナンスに基づくリスクベースアプローチ

・ リスクの特性を分析し、安全対策実施における意思決定に活用する考え。

⇒ 金融機関等の情報システムとして考慮すべき点（高い安全対策が必要なシステム・最低限必要な安全対策でよいシステム）を押さえ、限られた経営資源のなかで、**過不足なく、**安全対策を決定し実施する。



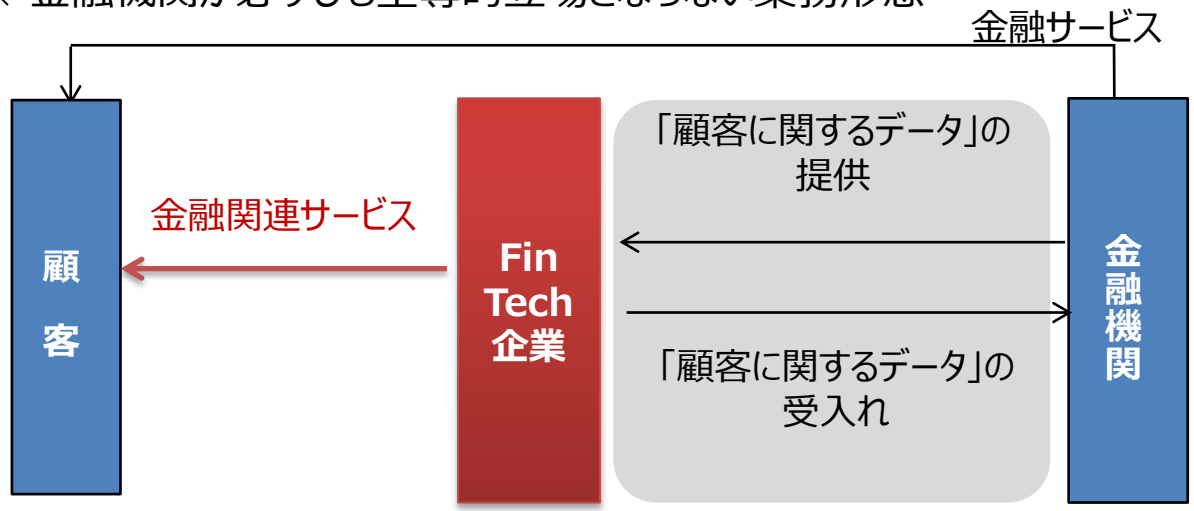
# （１）安全対策基準の改訂とFinTechに関する安全対策（つづき）

## 考え方②　金融関連サービスにおける安全対策の在り方

＜FinTechに関する有識者検討会における議論＞

金融関連サービスの提供において、**金融機関が必ずしも主導的立場とならない業務形態**が登場する。金融機関が部分的にせよ主導性を発揮していれば、安全対策上の責任（責務という）が生じていると解するのが妥当である。

※ 金融機関が必ずしも主導的立場とならない業務形態




リスク特性に着目して安全対策上の在り方を考える

- データの提供の場合　→ データの性質（個人情報、機微情報の有無）
- データの受入れの場合 → 取引の正当性（本人確認の方法）

- 顧客に対し、「誰が」主導的にサービスを提供するのかによって、安全対策上の責任が異なる。
- 金融機関に、データの提供や受入れに関する決定権が存する場合は金融機関に安全対策上の責任が生ずる。
- FinTechが主導性を発揮してサービスを提供する場合の安全対策の在り方の検討が必要。

# （１）安全対策基準の改訂とFinTechに関する安全対策（つづき）

## 考え方②　金融関連サービスにおける安全対策の在り方

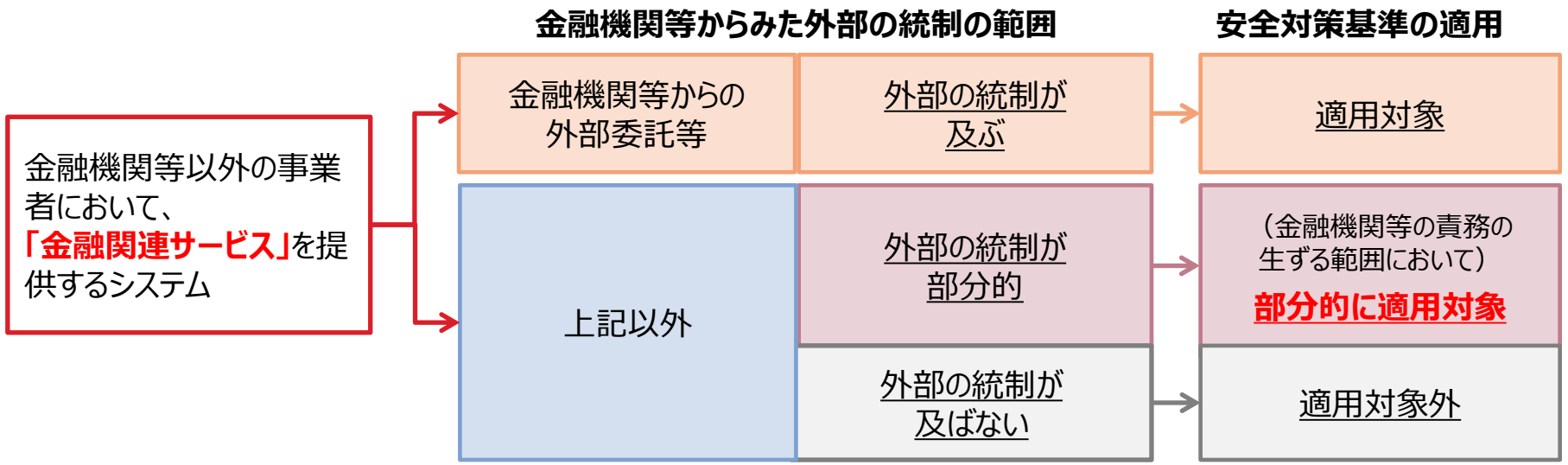
＜FinTechに関する有識者検討会での議論を踏まえ、安全対策基準では以下のように整理＞

### 用語の定義

**金融サービス**　金融機関等（銀行等の預金取扱金融機関、信託会社、証券会社、保険会社、クレジット会社等をいう（ただし、電子決済等代行業者などのFinTech企業等を除く））が業法等に基づき、顧客に提供するサービス

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

### 外部の統制と安全対策基準の適用範囲



# （１）安全対策基準の改訂とFinTechに関する安全対策（つづき）

## 考え方③　3者間構成における外部の統制

＜FinTechに関する有識者検討会における議論＞

FinTechに関する適切な安全対策の実施については、金融機関、ITベンダー及びFinTech企業の３者間の密接な連携、協調が不可欠である。

### 「協調の原則」

- 安全対策に係る情報開示が協調して適切に行えるよう、あらかじめ三者間で合意をしておくことが望ましい。
- 例えば、従来使用しているチェックリストを情報共有の手段として位置づけ、内容を見直し、協調の手段として活用することも有効と考えられる。

### 「再配分ルール」

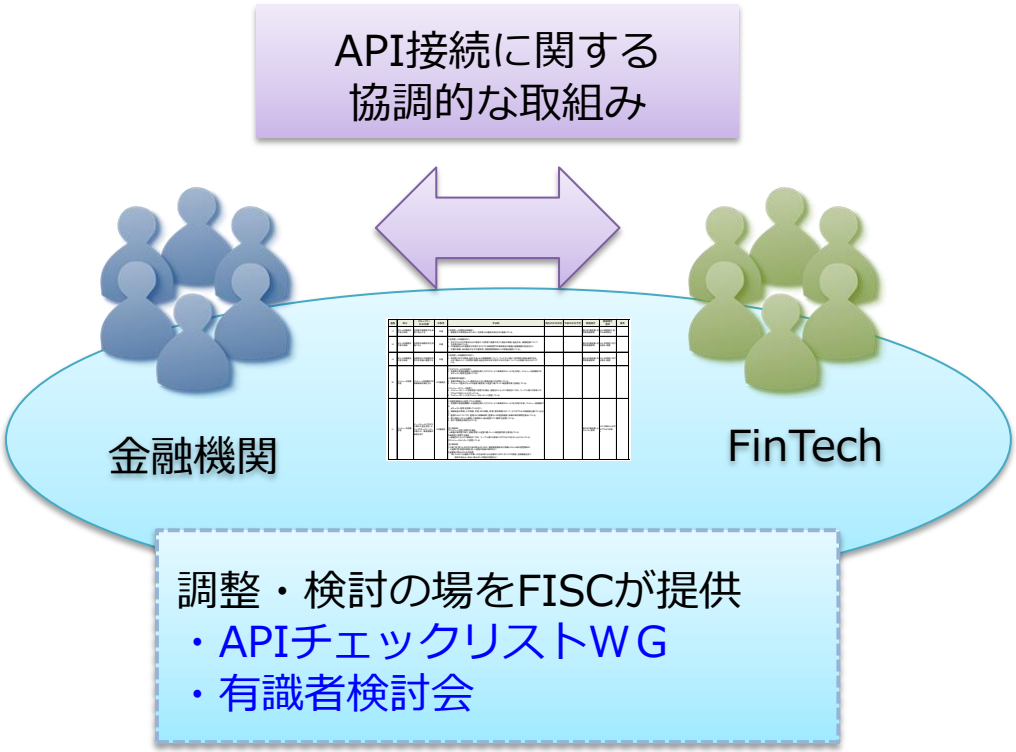
- 必要な安全性を維持するために、従来の安対基準における外部委託の責務を、三者の役割や安全対策遂行能力（保有する経営資源等）に応じて、合理的に再配分する。

### 外部の統制上の考慮事項

**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にする。**
**（過大な負担に応えようとした結果、FinTech業務に関するイノベーションが損なわれる可能性がある。）**

# （２）「オープンAPI」を実現させるための検討

「オープンAPI」においては、「オープン・イノベーション」に対する社会的期待の高まりを受けて、システム連鎖に携わる関係者が多くなることが予想される。
そのため、安全対策に関しては、「FinTech企業と金融機関との相互理解・協力に向けた取組み」を行うことが重要となる。




- 金融機関とFinTech企業のAPI接続が増大すると、結果として、FinTech企業は、複数の金融機関からの要求に応じるため、**膨大な調整事項が発生**する。
- 金融機関の集団とFinTech企業の集団が、両者の負担を最小化することを目指し、**共通のルール作り**を進めていくことが「オープンAPI」の実現にとって有益である。

# （３）「オープンAPI」における安全対策基準の適用

金融機関とFinTech企業の協調的な取組みの結果として、**「API接続チェックリスト（2018年10月版）」**が「安全対策基準」の考え方を踏まえ策定された。

| 章 | 区分 | 各章の目的 | FISC安対基準 | 銀行API報告書※ |
|---|---|---|---|---|
| 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。 | ○ | ○ |
| 2 | 外部委託管理 | API接続先が外部委託を行う場合、外部委託の管理態勢について確認する。 | ○ | |
| 3 | 金融機関・API接続先の協力体制 | 利用者保護の観点から、金融機関及び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。 | | ○ |
| 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。 | | ○ |
| 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。 | ○ | ○ |
| 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。 | ○ | ○ |
| 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。 | | ○ |
| 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。 | | ○ |
| 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。 | | ○ |

※「銀行API報告書」における「セキュリティ原則」または「利用者保護原則」を指す。

# （１）API接続チェックリスト（試行版）の概要

## API接続チェックリスト（試行版）の目的

- **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。**
- **機密性に関する確認項目が中心。**

## 共通確認項目及び構成要素

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

① オープンAPIのあり方に関する検討会（全銀協）
報告書「セキュリティ原則」に基づき作成

② FinTechに関する有識者検討会において
提言された考え方等を踏まえて作成

③ FISC が策定する「必要最低限の安対基準」
又は業界団体の自主基準を踏まえて作成

# （２）API接続チェックリスト（試行版）のイメージ

- **60項目からなる「セキュリティ対応目標」**と、各目標に関する「手法例」を記載。
- 回答欄として、**「現在の対応状況」**と**「今後の対応予定」**を用意。

| 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＞<br>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＞<br>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。<br>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＞<br>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＞<br>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。<br><br>＜設備環境の確認＞<br>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。<br>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。<br><br>＜コンピュータリソース配置＞<br>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。<br>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＞<br>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)。<br>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)。<br>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。<br>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。<br>5. 受付・警備員を常駐させている。<br><br>(注1)具体例<br>①コンピュータ室に設置する場合<br>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<br>②執務室に設置する場合<br>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<br>③コンピュータセンターに設置している<br><br>(注2)具体例<br>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）<br>②盗難等の防止のための措置<br>（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<br>e | |

# （３）API接続チェックリスト（確定版）の策定

**API接続チェックリスト（試行版）は、**
**銀行とAPI接続先の双方において、活用され始めている。**

## API接続チェックリスト確定版の作成（平成30年６月～9月）

- **公表後１年を機に、当該チェックリストの使用状況やユーザーからの要望、FISC安全対策基準の全面改訂等を踏まえて確定版を策定する**ため、平成30年6月に「金融機関におけるオープンAPIに関する有識者検討会」を設立。
- また、当該チェックリストの改訂内容を具体的に検討する場として、同検討会の下にワーキンググループを設置。

【有識者検討会メンバー】

| | |
|---|---|
| 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 | 学界： 安冨潔 慶應義塾大学名誉教授、國領二郎 慶應義塾大学総合政策学部教授　ほか<br>金融界： 都銀、地銀、ネット銀行、生保、損保、証券<br>実務界： FinTech企業、ITベンダー、クラウドベンダー ほか |
| ｵﾌﾞｻﾞｰﾊﾞｰ | 金融庁、日銀、総務省、経産省 |

【WGメンバー】都銀、地銀、第２地銀、信金、ネット銀行、 FinTech企業、ITベンダー（オブザーバー：金融庁、日銀）

# （３）API接続チェックリスト（確定版）の策定（つづき）

○　確定版は、「API接続チェックリスト**＜2018年10月版＞**」として、**10月12日に公表**。

⇒　今後は、年１回程度の頻度で、チェックリストの見直しを検討。

## 利用にあたっての留意事項

- API接続先が提供するサービスの特性や機能固有のリスク等を勘案した結果、「フォーマット」にある確認項目以外に必要なものがある場合には、各金融機関にて独自の確認項目を追加し、一方で、一部の確認項目が不要な場合は、各金融機関にて「フォーマット」から削除する。

  ⇒　いわゆる「リスクベースアプローチ」の考え方を採用。

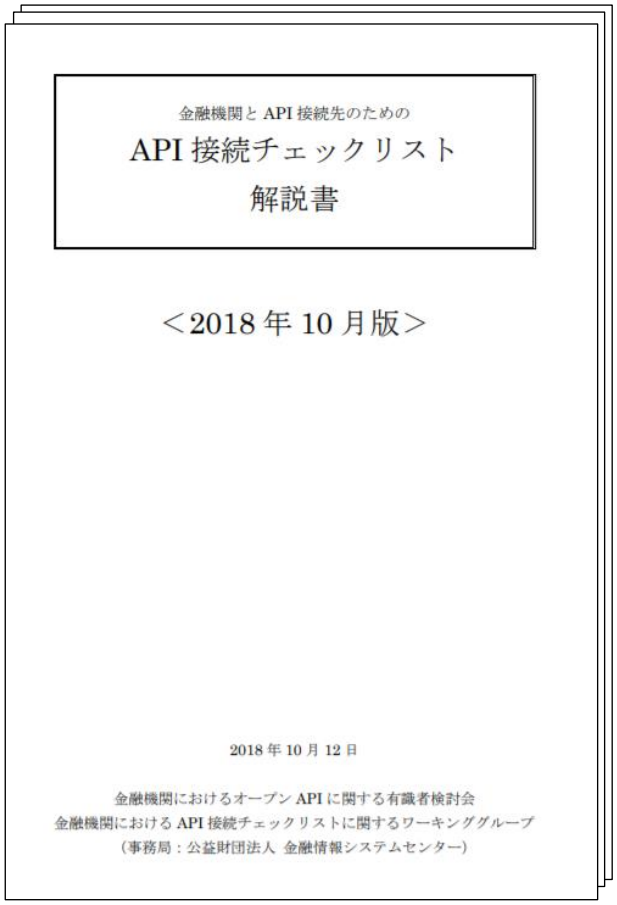
- API 接続先と金融機関は、API 接続先が提供するサービスの特性や機能固有のリスク等を勘案し、セキュリティ対応目標を達成するための適切な手法を協働で検討し選択することができる。

  ⇒　手法例はあくまで例示。

# （４）API接続チェックリストの様式

「API接続チェックリスト」は、使いやすさを高めるとともに手法例の位置づけ等に関する誤解を避けるため、**「API接続チェックリスト解説書」**と**「API接続チェックリスト（フォーマット）」**の２種類の様式で構成。

## ①解説書



金融機関と API 接続先のための

API 接続チェックリスト

解説書

＜2018 年 10 月版＞

2018 年 10 月 12 日

金融機関におけるオープン API に関する有識者検討会
金融機関における API 接続チェックリストに関するワーキンググループ
（事務局：公益財団法人 金融情報システムセンター）

## ②フォーマット

API接続チェックリスト（フォーマット）
＜2018年10月版＞

2018 年10月12日
オープンAPI有識者検討会
API接続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 | 現在の対応状況 | 課題認識 | 課題への対応計画 | 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 | | | | FISC・安対基準 | 統4、統6、統7、統8 | |
| 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 | | | | 銀行API報告書・セキュリティ原則<br>FISC・安対基準 | 3.3.1 API接続先の適格性 d<br>統1、統12 | |
| 3 | 情報・セキュリティ管理態勢 | 役職員に対する情報管理方法の周知やモニタリング等の実施により、セキュリティ管理態勢の定着を図る。 | API接続先 | | | | 銀行API報告書・セキュリティ原則<br>FISC・安対基準 | 3.3.1 API接続先の適格性 d<br>3.3.3 内部からの不正アクセス対策 k<br>統13、統14、監1 | |
| 4 | 情報・セキュリティ管理態勢 | 情報資産の管理を実施する。 | API接続先 | | | | 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 | 役職員による不正への対策を実施する。 | API接続先 | | | | 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 | |

# （５）確認項目

| 通番 | 区分 | セキュリティ対応目標 | 対象者 |
|---|---|---|---|
| 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 |
| 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 |
| 3 | 情報・セキュリティ管理態勢 | 役職員に対する情報管理方法の周知やモニタリング等の実施により、セキュリティ管理態勢の定着を図る。 | API接続先 |
| 4 | 情報・セキュリティ管理態勢 | 情報資産の管理を実施する。 | API接続先 |
| 5 | 情報・セキュリティ管理態勢 | 役職員による不正への対策を実施する。 | API接続先 |
| 6 | 情報・セキュリティ管理態勢 | 自社サービスの解約時及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、防止策を実施する。 | API接続先 |
| 7 | 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、振り返りと対策を実施する。 | API接続先 |
| 8 | 情報・セキュリティ管理態勢 | 連鎖接続における安全性を確保する。 | API接続先 |
| 9 | 情報・セキュリティ管理態勢 | 不正アクセスや障害等の発生を想定した態勢を整備する。 | 共通 |
| 10 | 外部委託管理 | 委託業務が円滑かつ適正に遂行されるよう、必要な対策を実施する。 | API接続先 |
| 11 | 外部委託管理 | クラウドサービス利用にあたってはクラウドサービス固有のリスクを考慮した対策を実施する。 | API接続先 |
| 12 | 金融機関・API接続先の協力体制 | セキュリティ対策の見直しや改善を図る。 | 共通 |
| 13 | 金融機関・API接続先の協力体制 | 利用者からの相談・照会等への対応を適切に実施する。 | 共通 |
| 14 | 金融機関・API接続先の協力体制 | 利用者の被害拡大を防止する。 | 共通 |
| 15 | 金融機関・API接続先の協力体制 | 利用者への補償を適切に実施する。 | 共通 |
| 16 | 金融機関・API接続先の協力体制 | 利用者向けの補償対応窓口を適切に運営する。 | 共通 |
| 17 | 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実施する。 | API接続先 |
| 18 | オフィス設備管理 | 不正な人物の入室を防ぎ、重要情報へのアクセスを制限する。 | API接続先 |
| 19 | 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実施する。 | API接続先 |
| 20 | オフィス設備管理 | ウイルス感染によるシステム侵入等の攻撃を防ぐ。 | API接続先 |

# （５）確認項目（つづき）

| 通番 | 区分 | セキュリティ対応目標 | 対象者 |
|---|---|---|---|
| 21 | システム開発・運用管理 | 情報資産への内部からの不正アクセスを抑止する。 | API接続先 |
| 22 | システム開発・運用管理 | システムアクセス時の認証を実施する。 | API接続先 |
| 23 | 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 |
| 24 | システム開発・運用管理 | 作業担当者による不正行為を防ぐ対策を実施する。 | API接続先 |
| 25 | 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、必要な対策を実施する。 | API接続先 |
| 26 | システム開発・運用管理 | 外部からの不正アクセス対策を実施する。 | API接続先 |
| 27 | システム開発・運用管理 | システムやネットワークに対する脆弱性対策を実施する。 | API接続先 |
| 28 | システム開発・運用管理 | 持ち出された機密情報を管理する。 | API接続先 |
| 29 | 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 |
| 30 | サービスシステムのセキュリティ機能 | 機密情報の漏洩対策を実施する。 | API接続先 |
| 31 | サービスシステムのセキュリティ機能 | 喪失・破損した情報の復旧を可能とする。 | API接続先 |
| 32 | サービスシステムのセキュリティ機能 | 利用者を保護する認証機能を整備する。 | API接続先 |
| 33 | サービスシステムのセキュリティ機能 | 偽アプリケーション対策を実施する。 | API接続先 |
| 34 | 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の被害拡大を最小限に止める。 | 共通 |
| 35 | 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の追跡調査を可能とする。 | 共通 |
| 36 | APIセキュリティ機能 | 認証認可に関する機密情報の漏洩対策を実施する。 | API接続先 |
| 37 | APIセキュリティ機能 | APIの想定外利用を回避する。 | API接続先 |
| 38 | APIセキュリティ機能 | 利用者が認識していないところで、利用者のアカウントがAPI接続に使用されないようにする。 | 金融機関 |
| 39 | APIセキュリティ機能 | 利用者の利便性と、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。 | 金融機関 |
| 40 | APIセキュリティ機能 | 脆弱性への攻撃に対する多層防御を図る。 | 金融機関 |
| 41 | APIセキュリティ機能 | 認証の悪用リスクを可能な限り低減させる。 | 金融機関 |
| 42 | APIセキュリティ機能 | API接続先を含めた全体の認証強度をもって、利用者保護を図る。 | 金融機関 |
| 43 | 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 |
| 44 | 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。 | 金融機関 |

**ご清聴ありがとうございました。**

**本件に関するお問合せは**
**fintech@fisc.or.jp までお願いします。**

公益財団法人 金融情報システムセンター
企画部
〒104-0042
東京都中央区入船2-1-1　住友入船ビル4F
TEL:03-5542-6055　FAX:03-5566-1052
URL:https://www.fisc.or.jp/