【資料５】

2025 年 12 月４日
金融情報システムセンター

2025 年度 API 接続チェックリスト見直し要否 対応方針

【対応方針】API 接続チェックリストの見直しは「要」とする。

チェックリスト関連規程（FISC「安全対策基準」）において、API が関連する記載が追記されたため、API 接続チェックリストの内容を変更する。なお、金融機関・電子決済等代行業者のニーズ、全銀協「オープン API のあり方に関する検討会報告書」）改訂、更新系 API のサービス提供状況においては当センターが確認する限り、API 接続チェックリストの見直しを要するような事象は発生していない。

1 見直しに関するルール

API 接続チェックリスト（以下、チェックリスト）の維持管理方法については、チェックリスト解説書 P2 に下記の通り規定されている。

今後の維持管理方法

FISC は、「API 接続チェックリスト」が常に有益なものであるよう、「API 接続チェックリスト連絡会」を設置し、以下の事項を踏まえて年１回、チェックリストの見直しについて検討する。また、チェックリストを大幅に見直す等、重要な判断が必要な場合は、別途、有識者検討会等を開催し審議することとする。

(1) ユーザーの使用状況や要望
(2) オープン API に関するインシデントの発生状況
(3) オープン API に関する標準化の動向
(4) 認定電子決済等代行事業者協会の自主基準　等

なお、インシデントの発生等に伴い、金融機関及び API 接続先に対して速やかに注意喚起等を行う必要がある場合には、FISC 事務局がウェブサイト等を通じて行う。

また、過去の「API 接続チェックリスト連絡会」（以下、連絡会）において、下記事項の動向についても継続的に確認している。

・ チェックリスト関連規定
（FISC「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」、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」）

・ 更新系 API のサービス提供状況

2　各検討事項の評価

(1) ユーザーの使用状況や要望

昨年度連絡会の議事要旨公表以降、複数の金融機関、電子決済等代行業者等と意見交換を行ってきたなかで、チェックリストの改訂にかかる具体的なニーズは確認できていない。

(2) オープン API に関するインシデントの発生状況

当センターが情報収集する限り、これまでチェックリストの改訂を要するようなインシデントの発生は確認できていない。

(3) オープン API に関する標準化の動向

当センターが情報収集する限りでは、これまで、チェックリストの改訂を要するような標準化の動向は確認できていない。

(4) 認定電子決済等代行事業者協会の自主基準

2020 年 12 月、電子決済等代行事業者協会は、会員向けの自主基準を制定しているが、その後、チェックリストの見直しを要する改訂等は行われていない。

(5) チェックリストの関連規程等の改訂

当センターは、2025 年 3 月に、「金融機関等コンピュータシステムの安全対策基準・解説書」（以下、「安全対策基準」という。）を改訂し、「第 13 版」として公表した[1]。第 13 版では、チェックリストにおける確認項目において、関連規定として敷衍されている安全対策基準の一部の基準項目が改訂されている。

〔図表 1〕のとおり、安全対策基準の実務基準 9 において、第 2 項「機器（API に認証情報を組み込むことを含む）及びユーザーの ID 及び認証情報を適切に管理することが必要」が追加された。ここでの機器は、デバイスに加えてアプリケーションも指していると理解し、API に認証情報を組み込むという記述から、人ではなく機械やプログラムが自動的にアクセスする際の認証情報の管理を意味しているため、API チェックリストにおいてもシステムアクセス時の認証を対象とする通番 22 に実務基準 9 を紐づけることとする。

[1] https://www.fisc.or.jp/publication/book/006660.php

〔図表 1〕チェックリストに関連規定と明記されている安全対策基準第 13 版の項目うち、取り込みが必要な改訂内容

チェックリストの通番	安全対策基準の主な改訂内容	
通番 22 システム開発・運用管理	実 9 ID の不正防止機能を設けること。	2　機器（API に認証情報を組み込むことを含む）及びユーザーの ID 及び認証情報を適切に管理することが必要である。 対応としては、以下の項目がある。 (1)初期設定されたパスワードの変更 (2)パスワード強度の要件 (3)ID の自動失効 (4)システム責任者による定期的なアクセスレビュー 【追加】 ・「サイバーガイドライン」に関する改訂

3. 2025 年度のチェックリスト見直し方針

以上のとおり、見直しのルールとして規定されている 4 項目にはチェックリストの見直しが必要となる事項がないが、関連規定等にチェックリストに加えるべき事項があるため、〔図表 2〕のとおり 2025 年度のチェックリストの見直しを実施したい。

〔図表 2〕チェックリスト改訂内容（赤字記載）

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
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				FISC・安対基準	実1、実8、実9、実16、実26	

〔参考〕API チェックリストに関連規定として明記されている、安全対策基準（第 13 版）該当項目の主な改訂内容

チェックリスト	安全対策基準	主な改訂内容
2. 情報・セキュリティ管理体制	統 1 システムの安全対策に係る重要事項を定めた規程を整備すること。	7. 法令上の責任や組織の資産としての情報の重要性に従って、データ・ガバナンスに関する方針及び規程等を策定することが望ましい。 【追加】 ・「サイバーガイドライン」に関する改訂
1. 情報・セキュリティ管理態勢	統 1 システムの安全対策に係る重要事項を定めた規程を整備すること。	統 1-1　サイバーセキュリティ対策に関する基本方針を整備すること。 【追加】 ・「サイバーガイドライン」の安全対策取込みに伴う基準小項目の新設
1. 情報・セキュリティ管理態勢	統 1 システムの安全対策に係る重要事項を定めた規程を整備すること。	統 1-2　サイバーセキュリティ対策に関する規程等及び業務プロセスを整備すること。 【追加】 ・「サイバーガイドライン」の安全対策取込みに伴う基準小項目の新設
－	統 3 システム開発計画は中長期システム計画との整合性を確認するとともに、承認を得ること。	参考 2　経済安全保障推進法に基づく制度のひとつ「特定社会基盤役務の安定的な提供の確保」では、金融機関等の各業態の主要事業者が「特定社会基盤事業者」に指定され、その事業者が「特定重要設備の導入」を行う際には、事前に金融庁に届出を行い、審査を受けることが求められている。 【追加】 ・経済安全保障推進法に関する改訂
1. 情報・セキュリティ管理態勢	統 4 セキュリティ管理体制を整備すること。	4　セキュリティを統括する部門、ユーザー部門等から独立した立場でセキュリティ管理体制が有効に機能していることを監視・牽制する組織としてリスク管理部門（注 1）を置くことが必要である。リスク管理部門は、セキュリティ管理の実施状況について、リスク管理を統括する責任者及び経営層へ報告を行うことが必要である。 【追加】 ・「サイバーガイドライン」に関する改訂

通番 1、3	統 4 セキュリティ管理体制を整備すること。	5　セキュリティを統括する部門、ユーザー部門のみならずリスク管理部門からも独立した立場で内部監査を実施する部門（注 2）を置き、セキュリティ及びサイバーセキュリティに関する監査を実施することが必要である。【監 1、監 1-1】 【追加】 ・「サイバーガイドライン」に関する改訂
1. 情報・セキュリティ管理態勢	統 4 セキュリティ管理体制を整備すること。	1　サイバーセキュリティを管理するための経営資源及び人材に関する計画を策定すること。 【追加】 ・「サイバーガイドライン」の安全対策取込みに伴う基準小項目の新設
1. 情報・セキュリティ管理態勢	統 4 セキュリティ管理体制を整備すること。	2　サイバーセキュリティ管理態勢の監視及び牽制を行うこと。 【追加】 ・「サイバーガイドライン」の安全対策取込みに伴う基準小項目の新設
－	統 5 サイバー攻撃対応態勢を整備すること。	1　サイバーセキュリティリスクを特定するため、情報資産を適切に管理すること。 【追加】 ・「サイバーガイドライン」の安全対策取込みに伴う基準小項目の新設
－	統 5 サイバー攻撃対応態勢を整備すること。	2　サイバーセキュリティリスクの特定・評価及びリスク対応計画を策定すること。 【追加】 ・「サイバーガイドライン」の安全対策取込みに伴う基準小項目の新設
－	統 5 サイバー攻撃対応態勢を整備すること。	3　ハードウェア・ソフトウェア等の脆弱性管理に関する手続き等を策定すること。 【追加】 ・「サイバーガイドライン」の安全対策取込みに伴う基準小項目の新設
－	統 5 サイバー攻撃対応態勢を整備すること。	4　サイバーセキュリティに関する演習・訓練を行うこと。 【追加】 ・「サイバーガイドライン」の安全対策取込みに伴う基準小項目の新設

−	統 5 サイバー攻撃対応態勢を整備すること。	5　サイバーセキュリティに係る教育・研修を行うこと。 【追加】 ・「サイバーガイドライン」の安全対策取込みに伴う基準小項目の新設
−	統 7 データ管理体制を整備すること。	データ管理者の業務としては、以下の項目がある。 (5)データ利用状況の管理（アクセスしたユーザーを特定できる措置を講じ、処理内容をログに記録し、ユーザーの操作内容と対応させる等） 【追加】 ・「サイバーガイドライン」に関する改訂
通番 2 情報・セキュリティ管理態勢	統 12 各種業務の規則を整備すること。	2　データ、プログラム及びドキュメントの管理については、顧客データ、秘密鍵等の重要で機密を要するデータの取扱いに関する規則を必要に応じて定めることが必要である。なお、データの取扱いに関する管理規則には、データの管理、データの保存、適切な暗号化方式を採用することや、暗号鍵と電子証明書を、そのライフサイクルを通じて管理し、保護すること、危殆化時の対応などを含めることが必要である。【実 3、実 28、実 30】 【追加】 ・下線部追加。「サイバーガイドライン」に関する改訂
通番 2 情報・セキュリティ管理態勢	統 12 各種業務の規則を整備すること。	3　認証及びアクセス権の付与に係る方針及び規則等を策定し、定期的に見直すことが必要である。その際、以下の観点を踏まえること。 【追加】 ・「サイバーガイドライン」に関する改訂
通番 2 情報・セキュリティ管理態勢	統 12 各種業務の規則を整備すること。	4　ログの取得・監視・保存のための手続きを策定し、定期的にレビューすることが必要である。手続きには、例えば、以下の事項を含むこと。【実 10】 【追加】 ・「サイバーガイドライン」に関する改訂

通番 10 外部委託管理	統 20 外部委託を行う場合は、事前に目的、範囲等を明確にするとともに、外部委託先選定の手続きを明確にすること。	2　外部委託先の選定要件を策定することが必要である。 委託する業務に求められる可用性・機密性等の観点及び自社の経営の視点から、リスクを分析・認識し、当該業務に求められるリスク管理レベルを検討のうえ、外部委託先の選定要件を策定する必要がある。この時、セキュリティ・バイ・デザインを実施できる体制となっているかを確認することが必要である。 【追加】 ・「サイバーガイドライン」に関する改訂
通番 10 外部委託管理	統 20 外部委託を行う場合は、事前に目的、範囲等を明確にするとともに、外部委託先選定の手続きを明確にすること。	参考　経済安全保障推進法に基づく制度のひとつ「特定社会基盤役務の安定的な提供の確保」では、金融機関等の各業態の主要事業者が「特定社会基盤事業者」に指定され、その事業者が「重要維持管理等の委託」を行う際には、事前に金融庁に届出を行い、審査を受けることが求められている。 「重要維持管理等」には、信頼性向上のために実施すべき障害、不正使用、破壊、盗難等の防止などの対応（維持管理）、並びに特定重要設備に当たる金融情報システムの運用業務（操作）が該当する。 【追加】 ・経済安全保障推進法に関する改訂
通番 10 外部委託管理	統 21 外部委託先と安全対策に関する項目を盛り込んだ契約を締結すること。	1-(1)基本的な事項 ⑤目的外使用の禁止 【追加】 ・脆弱性に関する対策基準の改訂
通番 10 外部委託管理	統 21 外部委託先と安全対策に関する項目を盛り込んだ契約を締結すること。	1-(2)個別契約条件、サービス仕様、データ保護の管理策 ⑥セキュリティ管理方法及び体制 外部委託先におけるデータ漏えい防止に関する対策（暗号化等）及び管理体制（暗号鍵の管理体制等）【実 3、実 4、実 8、実 30、実 83】、脆弱性に対するバージョンアップ適用状況等、脆弱性情報の管理状況と関連する管理体制 【追加】 ・脆弱性に関する対策基準の改訂

通番 10 外部委託管理	統 23 外部委託における管理体制を整備し、委託業務の遂行状況を確認すること。	1　業務遂行状況の確認方法としては、以下の例がある。 (1)外部委託先の管理状況を把握する。 ⑥脆弱性に対するバージョンアップ適用状況等、脆弱性情報の管理状況の報告を受ける。 【追加】 ・業務遂行状況の確認方法に関する対策例の改訂
通番 11 外部委託管理	統 24 クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること。	8　妥当性の確認においては、専門家によるシステム監査や誤設定の自動検知等の診断サービス（CSPM 等）、クラウド事業者の提供する適切なアーキテクチャを設計するための原則や実務的なベストプラクティス等を利用することも有効である。 【追加】 ・妥当性の確認方法に関する対策基準の改訂
－	統 28 サプライチェーンを考慮したサイバーセキュリティリスクを適切に管理すること。	【追加】 ・「サイバーガイドライン」の安全対策取込みに伴う基準小項目の新設
－	実 3 蓄積データの漏えい防止策を講ずること。	参考 2-1.技術の進歩により暗号の脆弱性が増す事例には、以下のものがある。 （省略） (2)暗号アルゴリズムの脆弱性が発見される。 （注）内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）において、政府機関における SHA-1 及び RSA1024 からの移行についての指針等を打ち出している事例がある。また、CRYPTREC「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」（2022 年 3 月）では、RSA2048 の利用期限（移行完遂期間）は 2030 年 12 月 31 日までとなっている。 【追加】 ・RSA2048 の利用期限に関する参考例の改訂

－	実 4 伝送データの漏えい防止策を講ずること。	1　データ伝送時に盗聴された場合にもデータの内容がわからないようにするため、重要なデータについては、暗号化、パスワード設定等のデータ保護の対策を講ずることが必要である。 その際には、例えば以下のような階層別の対策を複数組み合わせて実施することが必要である。 【追加】 ・伝送データの漏えい防止に関する対策基準の改訂
－	実 4 伝送データの漏えい防止策を講ずること。	2　データ伝送時のデータ保護の対策として暗号化を行う場合は、暗号化の適用範囲を適切に設定する必要がある。暗号化を施さない範囲については、想定されるリスクを受容できるか評価し、必要に応じて代替策を検討することが望ましい。 暗号化の適用範囲の切り口としては、以下の例がある。 【追加】 ・伝送データの漏えい防止に関する対策基準の改訂
－	実 4 伝送データの漏えい防止策を講ずること。	6　重要なデータを伝送するネットワーク（通信回線、LAN、その構成機器等を含む）については、以下のような対策を講ずることが望ましい。 (1)ネットワークへの未承認機器の論理的・物理的な接続の防止・検知 (2)ケーブルの切断、機器の取外しなどを検知し、情報漏えいのおそれのある不審な処置が施されていないか確認すること (3)建物内、ケーブル等に不正な機器の設置、取り付けが行われていないか確認すること (4)通信事業者における漏えい防止策を確認・評価すること 【追加】 ・伝送データの漏えい防止に関する対策基準の改訂
－	実 4 伝送データの漏えい防止策を講ずること。	参考 1　構内 LAN として無線 LAN を使用する際に考慮する点としては、以下の例がある。 【追加】 ・分かりやすい表現に見直し

通番 22 システム開発・運用管理	実 8 本人確認機能を設けること。	2　インターネットを介した電子的な取引、支払指図の受付等を行う場合は特に、なりすまし等を防止するため、通信相手が本人もしくは正当な端末であることを確認できる仕組みが必要である。その仕組みは、複数の方法を組み合わせることが望ましい。FIDO 認証やパスキー認証などを利用することも考えられる。 【追加】 ・認証方式に関する対策基準の改訂
通番 22 システム開発・運用管理	実 8 本人確認機能を設けること。	7　シングルサインオンや外部認証連携等、システム間又はセキュリティ境界にまたがる認証及び認可における機密性、完全性及び真正性等を確保することが必要である。 【追加】 ・「サイバーガイドライン」に関する改訂
-	実 8 本人確認機能を設けること。	参考 1-1.ワンタイムパスワード 1-2.トランザクション認証 1-3.FIDO 認証（Fast IDentify Online 認証） 1-4.パスキー認証 【追加】 ・認証方式に関する参考例の改訂
通番 22 システム開発・運用管理	実 9 ID の不正防止機能を設けること。	2　機器（API に認証情報を組み込むことを含む）及びユーザーの ID 及び認証情報を適切に管理することが必要である。 対応としては、以下の項目がある。 (1)初期設定されたパスワードの変更 (2)パスワード強度の要件 (3)ID の自動失効 (4)システム責任者による定期的なアクセスレビュー 【追加】 ・「サイバーガイドライン」に関する改訂

－	実 14 外部ネットワークからの不正侵入防止策を講ずること。	3　外部ネットワークからの不正侵入の防止と早期発見のため、内部ネットワークへのアクセスを監視し、アクセス履歴のチェックを行うことが必要である。 情報漏えい防止の観点から、外部への通信を検知する仕組み（プロキシ経由等）を導入することも有効である。 サービス妨害攻撃（DDoS/DoS）を早期に検知するため、攻撃対策、DNS に係るサイバーセキュリティ対策、代替通信経路の制御などによって、組織の通信及びネットワークサービスの耐性度を強化することが望ましい。（参考 6） また、サーバー等の脆弱性対策を講ずることが必要である。【実 10、実 16、実 34】 【追加】 ・「サイバーガイドライン」に関する改訂
－	実 14 外部ネットワークからの不正侵入防止策を講ずること。	3-(4)その他 サービス妨害攻撃（DDoS/DoS）等を早期に検知するための侵入検知システム（IDS:Intrusion Detection System）や 【変更】 ・より適切な表現に見直し（サービス妨害攻撃例の追加）
－	実 14 外部ネットワークからの不正侵入防止策を講ずること。	4　無線 LAN ネットワークへのアクセスは、適切な認証機能及びアクセス制御機能を実装し、不正利用を防止する必要がある。（参考 2） 【追加】 ・「サイバーガイドライン」に関する改訂
－	実 14 外部ネットワークからの不正侵入防止策を講ずること。	8　ネットワークセグメントを細分化し、マルウェアの水平移動（ラテラルムーブメント）を阻止することなどにより、サイバー攻撃の被害拡大防止を図ることが望ましい。 【追加】 ・「サイバーガイドライン」に関する改訂
－	実 14 外部ネットワークからの不正侵入防止策を講ずること。	9　情報システムのイベントログや運用担当者の作業ログの適切性を定期的又は必要に応じて都度確認することが必要である。 【追加】 ・「サイバーガイドライン」に関する改訂

－	実 14 外部ネットワークからの不正侵入防止策を講ずること。	参考 6　DDoS/DoS 攻撃への対策としては、以下の例がある。 ①海外に割り当てられた IP アドレスからの通信の遮断（サービス対象者が国内に限られる Web サイトの場合） ②CDN（注）、WAF の導入 ③サーバー設定の見直し（同一 IP アドレスからのアクセス回数制限、タイムアウト設定の見直し等） ④ソーリーページ等の設定 ⑤インターネットサービス・プロバイダー側での対策可否の検討（通信流量抑制可否の確認、DDoS/DoS 防御サービスへの加入検討等） （省略）
－	実 14 外部ネットワークからの不正侵入防止策を講ずること。	1　サイバー攻撃の端緒を検知するための監視・分析などの対策を講ずること。 【追加】 ・「サイバーガイドライン」の安全対策取込みに伴う基準小項目の新設
－	実 14 外部ネットワークからの不正侵入防止策を講ずること。	2　脆弱性診断及びペネトレーションテストを行うこと。 【追加】 ・「サイバーガイドライン」の安全対策取込みに伴う基準小項目の新設
通番 22 システム開発・運用管理	実 16 不正アクセスの監視機能を設けること。	1-(7)Web サイト等を外部に公開している場合は、侵入検知システム（IDS）や侵入防御システム（IPS）等の専用ソフトウェア等により、改ざんやサービス妨害攻撃（DDoS/DoS）等の不正アクセスを自動監視又は早期に検知する。 【変更】 ・より適切な表現に見直し（サービス妨害攻撃例の追加）
－	実 17 異常な取引状況を把握するための機能を設けること。	1　CD/ATM 等による取引が正当な権限を有する者に対して適切に行われることを確保するため、異常な取引状況を早期に把握するための機能を整備することが必要である。【実 109】 不正取引によるマネー・ローンダリング及びテロ資金供与の防止のため、異常な取引状況を把握するための機能を設けることが望ましい。

		【変更】 ・より適切な表現に見直し（不正取引例の追加）
－	実 17 異常な取引状況を把握するための機能を設けること。	1-(2)マネー・ローンダリング及びテロ資金供与の疑いのある取引 システムを利用して異常な取引を検知するには、金融庁「疑わしい取引の参考事例」等を参照のうえ、自らが直面するリスクに見合った情報を収集し、シナリオの検討・しきい値の設定等を行う必要がある。 【変更】 ・より適切な表現に見直し（不正取引例の追加）
－	実 19 不正アクセスの発生に備えて対応策、復旧策を講じておくこと。	1-(1)不正アクセスの拡大防止 ④サービス対象者が国内に限られる Web サイトの場合は、海外に割り当てられた IP アドレスからのアクセスを制限する。 【追加】 ・不正アクセス拡大防止に関する対策基準の改訂
－	実 19 不正アクセスの発生に備えて対応策、復旧策を講じておくこと。	1-(2)不正アクセス被害に対する復旧 ①不正アクセスによる被害に対する復旧のために事前に復旧手順を明確にすることが必要である。 a.サービス妨害攻撃（DDoS/DoS）により通信不能となった場合 【変更】 ・より適切な表現に見直し（サービス妨害攻撃例の追加）

－	実 25 各種資源、システムへのアクセス権限を明確にすること。	3-(3)外部事業者が提供するアクセス権限の設定のためのツール等を導入する場合の条件や制約 金融機関等においては、上記の確認結果をもとに職務分掌に応じたアクセス権限の設定を行うことが必要である。なお、アクセス権限の種類に不足がある場合には、ツールの導入等により機能を補うことが考えられる。 また、クラウドの設定誤りや不正なセキュリティ設定変更の早期発見のため、クラウドの設定状態を自動で監視するツール（CSPM 等）を利用することも有効である。 【追加】 ・クラウドサービスの適切な設定に関する対策基準の改訂
通番 21 システム開発・運用管理	実 27 各種資源、システムへのアクセス権限の付与、見直し手続きを明確にすること。	1　各種資源、システムへのアクセスを管理するためには、アクセス権限の付与方法を明確に定めておく必要がある。システムへのアクセス権限は、正当な業務上の要請があり、承認され、適切に教育・研修を受け、管理監視されている個人に対してのみ付与することが必要である。また、ユーザーによる機器及びシステムへのアクセス権限は、システムや情報の重要度を考慮して付与することが必要であり、職制、所属部署等によって、ユーザーにアクセス権限を与えるまでの承認者、相互牽制が働く承認手順を定めることが必要である。 【追加】 ・「サイバーガイドライン」に関する改訂
通番 21 システム開発・運用管理	実 27 各種資源、システムへのアクセス権限の付与、見直し手続きを明確にすること。	2　アクセス権限管理の注意点としては、以下の項目がある。 【変更】 ・「サイバーガイドライン」に関する改訂 ・項番 7 の追加 ・項番の振直し（順序の入れ替え） (5)→(8) (6)→(9) (7)→(5) (8)→(6)
通番 21 システム開発・運用管理	実 28 データファイルの授受・管理方法を明確にすること。	2　外部記憶媒体の保護と使用（使用制限、暗号化、マルウェアスキャンなど）に係る管理手続を策定し、実施することが必要である。【実 3】

		【追加】 ・「サイバーガイドライン」に関する改訂
－	実 30 暗号鍵の運用管理方法を明確にすること。	2　暗号鍵の管理手続きにおいては、採用している暗号鍵の適切性を維持し、危殆化時の対応等を定めることが必要である。 【追加】 ・暗号鍵の運用管理方法に関する対策基準の改訂
－	実 30 暗号鍵の運用管理方法を明確にすること。	3　暗号鍵の生成、配布、保管、失効、更新、廃棄、保存等の手続きを明確にするに当たっては、以下の点に留意することが必要である。 (3)作業の記録（作業者、作業日時、作業内容等）を残し、一定期間保管すること。作業記録等の管理書類等は、不正行為への悪用を防止するため、役席者が厳重に管理すること。 【追加】 ・項番 2 から移設
－	実 30 暗号鍵の運用管理方法を明確にすること。	参考　暗号鍵の運用管理方法を設計する際の参考として、CRYPTREC 公開の「暗号鍵管理システム設計指針（基本編）」及び「暗号鍵管理ガイダンス」がある。 【追加】 ・文献の最新化
－	実 34 外部接続における運用管理方法を明確にすること。	4　テレワークやベンダーによる保守等においてリモートアクセスの対象とするシステムを制限し、適切に管理する必要がある。また、重要なシステムについては、多要素認証や暗号化接続を使用する必要がある。 【追加】 ・「サイバーガイドライン」に関する改訂
－	実 39 データファイルのバックアップを確保すること。	1　障害及び災害等の発生により重要なデータファイルに破損等が発生した場合、そのファイルを早期に回復させる必要があるため、システム及び情報の重要度に応じたバックアップ要件、バックアップデータの隔離と保護、整合性の検証、復旧テストの実施等を含む、バックアップに関する規程等を整備のうえ、バックアップを取得し、その保管管理方法を明確にすることが必要であ

		る。 【追加】 ・「サイバーガイドライン」に関する改訂
－	実 39 データファイルのバックアップを確保すること。	2　バックアップを取得するに当たっては、データファイルの種類、更新タイミング等に応じて適切な保管期間及び保管場所を設定することが必要である。 特に、ランサムウェア攻撃のリスクを考慮して、バックアップの期間や頻度を検討することが必要である。また、同一ネットワーク内のバックアップファイルを探索して削除するランサムウェアのタイプがあることを踏まえて、改ざん耐性バックアップシステムの利用、組織内ネットワークから切り離した複数の環境での保管や媒体等へのバックアップを実施することも必要である。【実 20】（参考 3） 【追加】 ・「サイバーガイドライン」に関する改訂
－	実 41 プログラムファイルのバックアップを確保すること。	1　コンピュータウイルス等の不正プログラムによるプログラムの改ざん、破壊及び障害、災害等の発生による破損等に対応するため、本番プログラム等重要なプログラムファイルはシステム及び情報の重要度に応じたバックアップ要件、バックアップデータの隔離と保護、整合性の検証、復旧テストの実施等を含む、バックアップに関する規程等を整備のうえ、バックアップを取得し、保管管理方法を明確にすることが必要である。 【追加】 ・「サイバーガイドライン」に関する改訂

－	実 41 プログラムファイルのバックアップを確保すること。	2　バックアップを取得するに当たっては、品質の確保も考慮して適切な世代管理方法を定めるとともに、取得タイミングを定めておくことが必要である。 特に、ランサムウェア攻撃のリスクを考慮して、バックアップの期間や頻度を検討することが必要である。また、同一ネットワーク内のバックアップファイルを探索して削除するランサムウェアのタイプがあることを踏まえて、改ざん耐性バックアップシステムの利用、組織内ネットワークから切り離した複数の環境での保管や媒体等へのバックアップを実施することも必要である。【実 20】（参考 3） 【追加】 ・「サイバーガイドライン」に関する改訂
－	実 48 ハードウェア及びソフトウェアの管理を行うこと。	4　サポートの終了に伴うハードウェア・ソフトウェアの廃止・更改を計画的かつ安全に実施することが必要である。なお、ソフトウェアについてサポート対象バージョンへの更新が困難な場合には、補完的な措置を講じるとともに、迅速にサポートが得られるソフトウェアを利用したシステム・ビジネスプロセスへの移行計画を立て、着実に実行することが必要である。 【追加】 ・「サイバーガイドライン」に関する改訂
－	実 48 ハードウェア及びソフトウェアの管理を行うこと。	7　サプライチェーンのリスク評価の中で、ハードウェアに関するサイバーセキュリティリスク（不正なファームウェア導入のリスク等）を評価対象とすることが望ましい。 【追加】 ・「サイバーガイドライン」に関する改訂
－	実 48 ハードウェア及びソフトウェアの管理を行うこと。	8　ハードウェア（機器、ファームウェア、BIOS（注 1）又は UEFI（注 2）等）の真正性を確保し、また、不正な書き換えを防止するための対策（改ざん検知など）を導入することが望ましい。 【追加】 ・「サイバーガイドライン」に関する改訂

−	実 48 ハードウェア及びソフトウェアの管理を行うこと。	9　ハードウェアの調達基準等にセキュアな調達のための基準を設けることが望ましい。調達基準や取引基準の中で、調達先又は取引先の法令順守、自組織のセキュリティ基準又は倫理基準などの社内基準の遵守を求めること。法令、社内基準、国連制裁等を踏まえたサプライヤーリスト又は制裁対象リストを作成、維持し、これらを踏まえた調達を実施することが望ましい。 【追加】 ・「サイバーガイドライン」に関する改訂
−	実 48 ハードウェア及びソフトウェアの管理を行うこと。	10　必要な機能（ポート、プロトコル、サービス等）のみを提供するようにシステムを構成することが必要である。 【追加】 ・「サイバーガイドライン」に関する改訂
−	実 51 機器の保守方法を明確にすること。	6　システムの保守におけるサイバーセキュリティを確保するための手続きを定めること（リモート保守やオンサイト保守時の保守要員、作業手順、作業に用いるツール・交換部品を承認する手続きなど）が必要である。 【追加】 ・「サイバーガイドライン」に関する改訂
−	実 57 データセンターの入退管理を行うこと。	1-(3)訪問者に対しては、事前の届出を求め、入館の申請・承認の手続きを整備する。 【追加】 ・入退管理に関する対策基準の改訂
−	実 71 障害時・災害時復旧手順を明確にすること。	3　サイバー攻撃の発生直後はシステム障害と区別ができない可能性も想定されるため、システム障害時にサイバー攻撃の可能性を考慮することが必要である。 【追加】 ・統 5 から移設
−	実 73 コンティンジェンシープランを策定すること。	1-(3)緊急事態におけるコンティンジェンシープランの発動基準及びサービス停止の判断基準を明確にする。 【追加】 ・コンティンジェンシープランに関する対策基準の改訂
−	実 73 コンティンジェンシープランを策定すること。	1　サイバー攻撃を想定したインシデント対応計画及びコンティンジェンシープランを策定すること。 【追加】

		・「サイバーガイドライン」の安全対策取込みに伴う基準小項目の新設
－	実 75 システムの開発・変更手順を明確にすること。	4　システムで利用するサードパーティのライブラリやミドルウェア、ハードウェアについては、不正侵入の経路となるバックドア等が含まれることのないように、セキュリティ・バイ・デザインやセキュリティ・バイ・デフォルト等の安全な開発手法を製品開発に取り入れている事業者から提供される安全なプロダクトを選定することが望ましい。 【追加】 ・「サイバーガイドライン」に関する改訂
－	実 75 システムの開発・変更手順を明確にすること。	5　セキュリティ・バイ・デザインにかかる管理プロセスを、以下の点も考慮のうえ、整備し、運用することが望ましい。 【追加】 ・「サイバーガイドライン」に関する改訂
－	実 76 テスト環境を整備すること。	1-(2)本番稼働へ向けて十分なテストが実施できる環境の設定 ①開発・テスト用資源等を確保する。 開発・テスト用のコンピュータ等の資源は十分に確保する。また、本番環境での障害発生を想定し、テスト用に本番に近い環境（資源やソフトウェア、テストデータ等）を確保する。確保が難しい場合は、本番環境とテスト環境の差異及び差異に伴う障害時のリスクを把握しておく。 【追加】 ・より適切な表現に見直し（テスト環境に関する例示を追加）
－	実 89 必要となるセキュリティ機能を取り込むこと。	3　金融商品・サービスの企画・設計段階から、セキュリティ要件を組み込む「セキュリティ・バイ・デザイン」を実践することが必要である。また、サービス全体の流れの中で、重要なサードパーティも含めてリスクを検証し対策を講ずることが必要である。また、自組織にシステムを提供する重要なサードパーティにおいて、セキュリティ・バイ・デザインを実施できる体制となっているかを確認すること。

		【追加】 ・「サイバーガイドライン」に関する改訂
－	実 107 カードの管理方法を明確にすること。	11　顧客が暗証番号を失念した場合の手続きを定めることが必要である。 【追加】 ・暗証番号、パスワードに関する対策基準の改訂
－	実 112 インターネット・モバイルサービスの不正使用を防止すること。	2-(1)⑧着信電話番号と届出電話番号との一致確認、コールバックによる端末、本人確認【実 8】 【追加】 ・本人確認の方法に関する対策基準の改訂
－	実 112 インターネット・モバイルサービスの不正使用を防止すること。	⑪インターネット取引において、顧客が必要とする機能、並びに顧客の利用環境や IT リテラシー等のセキュリティレベルを踏まえて、利用可能な機能や限度額を設定【実 11】 【追加】 ・統 5 から移設
－	実 112 インターネット・モバイルサービスの不正使用を防止すること。	⑰インターネット取引を求める顧客に対し、不正プログラム対策ソフトの導入有無等、顧客が利用するパソコン環境の事前告知を求める 【追加】 ・統 5 から移設
－	実 112 インターネット・モバイルサービスの不正使用を防止すること。	2-(2)①インターネットサービス・プロバイダー（ドメイン）限定【実 14】 ②インターネットサービス・プロバイダーとの専用線接続【実 14】 【追加】 ・分かりやすい表現に見直し

－	実 112 インターネット・モバイルサービスの不正使用を防止すること。	参考 1-(2)外国においては、金融機関等の情報システムが被害を受けた事例や、個人がいわゆるハッカーとして、重要インフラ等の情報システムに対する侵入、サービス妨害攻撃（DDoS/DoS）、コンピュータウイルスの流布等によって重大な被害を起こした事例もある。 【変更】 ・より適切な表現に見直し（サービス妨害攻撃例の追加）
－	実 113 インターネット・モバイルサービスの使用状況を利用者が確認できるようにすること。	1-(4)ID・パスワード、住所、電話番号、登録メールアドレス等の重要な登録事項の変更処理結果等を郵送又は登録アドレスへ電子メールで通知、住所変更の場合は登録アドレスへ電子メールで通知 【追加】 ・より適切な表現に見直し（重要な登録事項に関する例示を追加）
－	実 115 インターネット・モバイルサービスの顧客対応方法を明確にすること。	3　顧客がパスワードを失念した場合の手続きを定めることが必要である。顧客がパスワードを失念した場合の手続きとしては、対面又は非対面による十分な本人確認を実施し、「新しいパスワードの再登録」又は「パスワードの再発行」等を受け付ける等がある。 なお、インターネット・モバイルサービスのパスワードについては、金融機関等の職員による専用端末等からの照会を不可とすることが必要である。 【追加】 ・暗証番号、パスワードに関する対策基準の改訂（パスワード失念時の対応方法を追加）
－	実 150 AI の利用に係る方針の策定と態勢の整備を行うこと。	【追加】 ・AI の安全対策に関する改訂に伴う基準小項目の新設
－	実 151 AI の適切な運用管理方法を定めること。	【追加】 ・AI の安全対策に関する改訂に伴う基準小項目の新設
－	実 152 AI に係る安全対策を講ずること。	【追加】 ・AI の安全対策に関する改訂に伴う基準小項目の新設

－	実 153 AI の利用に係る教育、注意喚起等を行うこと。	【追加】 ・AI の安全対策に関する改訂に伴う基準小項目の新設
－	設 19 出入口は、不法侵入・危険物の投込み・延焼などの防止措置を講ずること。	防犯・防災のため、データセンター又はコンピュータシステム関連業務専用区画の出入口には十分な強度と防火性能を有する扉を設置し、錠を付けること。 【追加】 ・用語の見直し
通番 3 情報・セキュリティ管理態勢	監 1	1　サイバーセキュリティを対象とした内部監査を行うこと。 【追加】 ・「サイバーガイドライン」に関する改訂

以 上