

「API接続チェックリスト原案(新旧比較表)」

平成30年9月27日
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	手法例	関連規定	関連規定箇所	通番	セキュリティ対応目標	解説文	手法例 / 具体例	関連規定	関連規定箇所
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	<p><責任者の設置></p> <ol style="list-style-type: none"> 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。 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。 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。 <p><体制の整備></p> <ol style="list-style-type: none"> 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)。 <p><統括責任者・責任者の業務></p> <ol style="list-style-type: none"> 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)。 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)。 <p>(注1)具体例</p> <ol style="list-style-type: none"> 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 「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 「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 情報資産の安全管理に関する教育・研修の企画 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 <p>(注2)具体例</p> <ol style="list-style-type: none"> 情報資産の取扱者の指定及び変更等の管理 情報資産の利用申請の承認及び記録等の管理 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 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 情報資産の取扱状況の把握 委託先における情報資産の取扱状況等の監督 情報資産の安全管理に関する教育・研修の実施 「セキュリティ管理に係る統括責任者」に対する報告 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	1	セキュリティ管理責任の所在と対象範囲を明確にする。	<p>セキュリティに関する適切な対策を実施するため、セキュリティ管理に関する責任者を決定し、職務範囲を明確にする。</p> <p>(注1)</p> <ol style="list-style-type: none"> 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 セキュリティ管理に関する責任者及び情報資産利用者に「<u>本人確認</u>」に関する情報の管理者の任命 セキュリティ管理に関する責任者からの報告徴収及び助言・指導 情報資産の安全管理に関する教育・研修の企画 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 <p>(注2)</p> <ol style="list-style-type: none"> 情報資産の取扱者の指定及び変更等の管理 情報資産の利用申請の承認及び記録等の管理 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 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 情報資産の取扱状況の把握 委託先における情報資産の取扱状況等の監督 情報資産の安全管理に関する教育・研修の実施 セキュリティ管理に関する最高責任者に対する報告 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 	<p>FISC・安 対基準</p> <p>統4 統6 統7 統8</p>		
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	<p><セキュリティ関連文書の整備></p> <ol style="list-style-type: none"> 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)。 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)。 <p><アクセス管理の実施></p> <ol style="list-style-type: none"> 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。 <p><エビデンスの確保></p> <ol style="list-style-type: none"> 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。 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。 <p>(注1)具体例</p> <ol style="list-style-type: none"> 以下の事項を定めた基本方針の整備 <ol style="list-style-type: none"> 事業者の名称 安全管理措置に関する質問及び苦情処理窓口 安全管理に関する宣言 基本方針の継続的改善の宣言 関係法令等遵守の宣言 各管理段階に係る取扱規程の整備 <ol style="list-style-type: none"> 取得・入力段階 利用・加工段階 保管・保存段階 移送・送信段階 消去・廃棄段階 漏えい事案等への対応の段階 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 <p>(注2)具体例</p> <ol style="list-style-type: none"> 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	3.3.1 API 接続先の 適格性 d	2	セキュリティ管理ルールを整備する。	<p>セキュリティ管理態勢を維持、継続するため、セキュリティ管理の方針や規程を整備する。</p> <p>(注1)</p> <ol style="list-style-type: none"> 以下の事項を定めた基本方針の整備 <ol style="list-style-type: none"> 事業者の名称 安全管理措置に関する質問及び苦情処理窓口 安全管理に関する宣言 基本方針の継続的改善の宣言 関係法令等遵守の宣言 各管理段階に関する取扱規程の整備 <ol style="list-style-type: none"> 取得・入力段階 利用・加工段階 保管・保存段階 移送・送信段階 消去・廃棄段階 漏えい事案等への対応の段階 情報資産の取扱状況の点検及び監査に関する規程の整備 	<p>銀行API 報告書・ セキュリ ティ原則</p> <p>FISC・安 対基準</p> <p>3.3.1 API 接続先の 適格性 d</p> <p>統1 統12</p>		

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ対応目標	対象者	手法例	関連規定	関連規定箇所	通番	セキュリティ対応目標	解説文	手法例 / 具体例	関連規定	関連規定箇所		
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	<p><周知・意識啓発の徹底></p> <p>1. セキュリティ運用に関する周知・注意喚起を全従業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。</p> <p>2. 従業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。</p> <p>3. 従業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。</p> <p><モニタリングの実施></p> <p>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。</p> <p>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)。</p> <p>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。</p> <p><体制の整備></p> <p>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。</p> <p>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。</p> <p><監査の実施></p> <p>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)。</p> <p>(注1)具体例</p> <p>①情報資産取扱部署の点検責任者・点検担当者の選任</p> <p>②点検計画の策定による体制整備</p> <p>③定期的及び臨時的点検の実施</p> <p>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</p> <p>(注2)具体例</p> <p>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</p> <p>②監査計画の策定による監査体制整備</p> <p>③定期的及び臨時的監査の実施</p> <p>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</p>	FISC・安 対基準	連10-1	3	<p>全社的にセキュリティ管理態勢を定着させるため、従業員に対してセキュリティ教育を実施し、遵守状況について定期的にモニタリング等を実施する。</p>	<p><周知・意識啓発の徹底></p> <p>1. セキュリティ運用に関する周知・注意喚起を全従業員向けに行っている。</p> <p><教育・研修の実施></p> <p>1. 従業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)</p> <p><体制の整備></p> <p>1. 情報資産の安全管理に関する取扱規程に従った体制を整備し、運用を行っている。</p> <p>2. 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。</p> <p><エビデンスの確保></p> <p>1. 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、エビデンスとして提示している。</p> <p>2. 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。</p> <p><モニタリングの実施></p> <p>1. 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。</p> <p>2. 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。</p> <p>3. 取扱規程の規定事項の遵守状況の記録及び確認を行っている。</p> <p><監査の実施></p> <p>1. 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)</p> <p><第三者認証の利用></p> <p>1. 提供するサービスや目的に合致した第三者認証を取得(注3)してセキュリティ管理態勢が整備されていることを示すことが考えられるが、第三者認証を取得していなければならない訳ではない。</p> <p>(注1)</p> <p>① 従業員に対する採用時の教育及び定期的な教育・訓練</p> <p>② 提供する情報資産の取扱いに関する研修</p> <p>③ 情報資産の安全管理に関する就業規則等に違反した場合の懲戒処分の周知</p> <p>④ 従業員に対する教育・訓練の評価及び定期的な見直し</p> <p>(注2)</p> <p>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</p> <p>② 監査計画の策定による監査体制整備</p> <p>③ 定期的及び臨時的監査の実施</p> <p>④ 監査の実施後において、規程違反事項等を把握した時は、その改善の実施</p> <p>(注3)</p> <p>① プライバシーマーク、ISMS(JIS Q 27001等)、ITSMS(JIS Q 20000-1等)の認証を取得している。</p> <p>② 内部統制保証報告書[SOC1(SSAE16・ISAE3402)、SOC2、IT委員会実務指針7号]や情報セキュリティ監査報告書を取得している。</p> <p>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。</p>	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 d	3.3.3 内 部からの 不正アク セス対策 e	FISC・安 対基準	統13 統14 監1
4	情報・セキュリティ管理態勢	従業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	<p><教育・研修の実施></p> <p>1. 従業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)。</p> <p>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。</p> <p>3. 従業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。</p> <p>(注1)具体例</p> <p>①従業員に対する採用時の教育及び定期的な教育・訓練</p> <p>②提供する情報資産の取扱いに関する研修</p> <p>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</p> <p>④従業員に対する教育・訓練の評価及び定期的な見直し</p>	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原案(新旧比較表)」

通番	区分	セキュリティ対応目標	対象者	手法例	関連規定	関連規定箇所	通番	セキュリティ対応目標	解説文	手法例 / 具体例	関連規定	関連規定箇所
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	<p><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)。</p> <p>(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</p>	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	4	情報資産の管理を実施する。	<p>情報漏洩等が発生した場合、影響範囲を速やかに把握し、適切な対応を行うため、情報資産の管理を実施する。</p>	<p><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)</p> <p>(注1) 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</p>	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	<p><内部従業員の不正対策> 1. 役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従業員の役割・責任や、非開示契約違反時の懲戒処分」を定めている。</p> <p>(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.従業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</p>	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	役員による不正への対策を実施する。	<p>社内から無断で情報が持ち出されること等がないよう、役員に対して不正対策を実施する。</p>	<p><従業員の不正対策> 1. 役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従業員の役割・責任や、非開示契約違反時の懲戒処分を定めている。</p> <p>(注1) ① 非開示契約(業務上知り得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. 従業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に、派遣社員本人との契約、覚書、念書等(電子的手段含む)による守秘義務を規定している。</p>	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
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	<p><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の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の有無/タイミング、保管媒体の破棄の実施の有無/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。</p> <p><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)。</p> <p>(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</p> <p>(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</p>	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	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に防止策を実施する。	<p>自社サービスの解約後及びシステムの廃棄後に情報漏洩を発生させないため、機器等に保存されている情報を消去する等の対策を実施する。</p>	<p><自社サービス解約時・解約後のデータポータビリティ及び消去> 1. 自社サービス解約時のデータの返却の有無及び方法を定めている。(注1) 2. 自社サービス解約後のデータ消去の実施の有無及びタイミング、保管媒体の破棄の有無及びタイミング、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。</p> <p><情報資産の廃棄計画> 1. 情報資産の廃棄計画を取り決めている。(注2)</p> <p>(注1) ① 機密情報の完全消去 ② データ廃棄の完了を確認するための監査権の行使 ③ 情報システムの廃棄手続きの明確化</p> <p>(注2) ① 廃棄の目的 ② 廃棄の対象範囲 ③ 廃棄する時期 ④ 廃棄する方法 ⑤ 計上資産の処分方法</p>	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原案(新旧比較表)」

通番	区分	セキュリティ対応目標	対象者	手法例	関連規定	関連規定箇所	通番	セキュリティ対応目標	解説文	手法例 / 具体例	関連規定	関連規定箇所
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	<p><不祥事案への対応></p> <p>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。</p> <p>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。</p>	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	7	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。	<p>セキュリティ不祥事案の再発を防止するため、発生した不祥事案の原因分析を行い、必要な対策を実施する。</p>	<p><不祥事案への対応></p> <p>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。</p> <p>2. 重大な不祥事案については、第三者が対策や改善状況の妥当性、統制プロセスを評価している。</p>	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
-	-	-	-	-	-	-	8	連鎖接続における安全性を確保する。 【対象者】API接続先	<p>連鎖接続先においてセキュリティ不祥事案が発生しないよう、連鎖接続先における安全性確保のための施策を実施する。</p>	<p><連鎖接続先の安全対策></p> <p>1. 連鎖接続先が遵守すべき安全対策の内容を踏まえた契約を締結している。</p> <p>2. 連鎖接続先における安全対策の実施状況を把握している。</p> <p>3. 連鎖接続先が決められた安全対策を実施していない場合は改善を求め等、必要な対応を実施している。</p>	-	-
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	<p><認証の取得></p> <p>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)</p> <p>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)</p> <p>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。</p>	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d	-	-	-	-	-	-
					FISC・安対基準	運112						

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所
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 備ができています	共通	<p><不正アクセス(情報漏えい事案等)発生時の体制整備></p> <ol style="list-style-type: none"> 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)。 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)。 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。 再発防止策・事後対策の検討を行う体制としている。 金融機関への報告を行う体制としている。 <p>(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</p> <p>(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</p>	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	9	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。	不正アクセスやシ ステム障害等の発 生時に適切な対 応ができるよう、 態勢を整備する。	<p><不正アクセス(情報漏えい事案等)の発生を想定した対応態勢の整備></p> <ol style="list-style-type: none"> 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) 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) 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を整備している。 再発防止策、事後対策の検討を行う体制を整備している。 <p><障害等発生時の連絡体制></p> <ol style="list-style-type: none"> 障害等の発生に備えて緊急時の連絡体制を決めている。 緊急時の連絡体制を定期的に見直している。 <p>(注1) ① 通知手段の確保 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</p> <p>(注2) 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及び管理者 ② システム担当者及び管理者 ③ コンピュータメーカー及び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</p>	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
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	<p><委託先の選定></p> <ol style="list-style-type: none"> 委託する場合、委託先に対して選定基準を提示している。 委託する際の規程を整備している。 <p><委託契約の締結></p> <ol style="list-style-type: none"> 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。 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。 <p><体制の整備></p> <ol style="list-style-type: none"> 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	10	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。	外部委託(クラウド サービスの利用を 含む) ⁸ を行う場 合、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。	<p><委託先の選定></p> <ol style="list-style-type: none"> 外部委託する場合、委託先の選定基準を策定している。 外部委託する際の規程を整備している。 規程等に基づいて委託先を評価し、委託先の決定について責任者の承認を得ている。 <p><委託契約の締結></p> <ol style="list-style-type: none"> 外部委託した業務の安全な遂行を確保するため、必要に応じて機密保持契約あるいはサービスレベルアグリーメント等を締結している。 <p><委託状況の確認></p> <ol style="list-style-type: none"> 委託先の管理状況を把握している。(注1) 委託先における業務の遂行状況について監査等を行っている。 委託先における業務の遂行状況を定期的にモニタリングしている。 <p>(注1) ① 管理責任者より状況を聴取する。 ② 定期的に作業状況の報告を受ける。 ③ 作業の機密管理状況の報告を受ける。 ④ 委託先における業務遂行に関する重要な事項の変更の報告を受ける。 ⑤ セキュリティに関する事故及び犯罪の報告を受ける。</p> <p>⁸ 外部委託には、金融機関やAPI接続先とITベンダー等との関係が委託関係にある場合(システム開発や運用等)だけでなく、委託関係にあるとは限らない場合(クラウドサービスの利用等)も含む。</p>	FISC・安 対基準	統20 統21 統22 統23 監1

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ対応目標	対象者	手法例	関連規定	関連規定箇所	通番	セキュリティ対応目標	解説文	手法例 / 具体例	関連規定	関連規定箇所
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	<p><委託先の選定></p> <p>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。</p> <p><委託状況の確認></p> <p>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。</p> <p>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。</p> <p>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。</p>	FISC・安 対基準	運3 運4 運5 運6	11	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て、必要な対策を実施する。	<p>クラウドサービスを利用する際は自社サービスの内容やクラウドサービス固有のリスクを考慮して、必要な対策を実施する。</p> <p><委託先の選定></p> <p>1. <u>利用するサービスの内容及びリスク特性に応じて、クラウド事業者の選定時に、統制対象クラウド拠点を把握している。</u></p> <p>2. <u>統制対象クラウド拠点が実質的な統制が可能となる地域に所在していることを確認している。</u></p> <p>3. クラウドサービスを利用する際に、<u>チェックリスト等を用いて、その事業者を利用して良いか判断している。</u></p> <p><契約の締結></p> <p>1. <u>利用するサービスの内容及びリスク特性に応じて、統制対象クラウド拠点に対して必要となる権利(監査権等)を確保するために、クラウド事業者と交わす契約書等にその権利を明記している。</u></p> <p>2. 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。</p> <p><委託状況の確認></p> <p>1. <u>利用するサービスの内容及びリスク特性に応じて、クラウド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。</u></p> <p>2. 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。</p> <p>3. <u>監査の実施にあたっては、技術の先進性等を考慮し、クラウド事業者が委託した保証型監査の報告書を利用している。</u></p> <p>4. 運用中のサービスについて、クラウドサービスが内包するリスクを確認している。</p>	FISC・安 対基準	統24 監1	
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	<p><委託状況の確認></p> <p>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。</p>	FISC・安 対基準	運89 運90 運91 運112	-	-	-	-	-	-
14	銀行・API接続先の協力量体制	セキュリティ対策の高度化を図る	共通	<p><協力量体制の整備></p> <p>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。</p> <p>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。</p>	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	12	新たな手口によるセキュリティ不祥事案を防止するため、セキュリティ対策の見直しや改善を実施する。	<p><協力量体制の整備></p> <p>1. セキュリティ対策の<u>見直し・改善</u>・高度化に向けて、<u>金融機関</u>・API接続先双方で協力して取り組む態勢を整備している。</p> <p>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。</p>	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原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所
15	銀行・API接続先協力体制	利用者からの照会対応を的確に行う	共通	<p><利用者からの照会対応></p> <p>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。</p>	銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得	13	利用者からの相談・照会等への対応を適切に実施する。	<p>利用者保護の観点から、利用者の相談・照会、苦情、問い合わせ等に対して適切に対応する。</p> <p><利用者からの相談・照会等への対応></p> <p>1. 利用者からの相談・照会、苦情、問い合わせ等があった場合の役割分担、業務フローを予め取り決めている。</p> <p><利用者への連絡先表示></p> <p>1. 利用者からの相談・照会、苦情、問い合わせ等のための連絡先を表示している。</p>	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接続先協力体制	利用者からの相談等対応を的確に行う	共通	<p><利用者への連絡先表示></p> <p>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。</p>	銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得	-	-	-	-	-	-
17	銀行・API接続先協力体制	利用者の被害拡大を未然に防止する	共通	<p><利用者への連絡手段確保></p> <p>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。</p>	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	14	利用者の被害拡大を防止する。	<p>利用者の被害が拡大しないよう、必要な対策を実施する。</p> <p>(注1)</p> <p>① 電子メール ② 電話 ③ ウェブサイト ④ SNS</p>	<p><利用者への連絡手段確保></p> <p>1. 被害拡大の防止のために、利用者との連絡手段(注1)を予め確保している。</p>	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

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所
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	<p><利用者への補償対応></p> <p>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。</p> <p>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。</p>	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	15	利用者への補償を適切に実施する。	<p>利用者保護の観点から、利用者に補償する必要がある場合には、補償を適切に実施する。</p>	<p><利用者への補償対応></p> <p>1. 不正アクセスや不具合等が原因で、利用者に損害が生じた場合の補償・返金方法、補償範囲について予め取り決めている。</p> <p>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。</p>	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	<p><利用者への補償窓口対応></p> <p>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。</p>	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	16	利用者向けの補償対応窓口を適切に運営する。	<p>利用者保護の観点から、利用者向けの補償窓口を設置し、適切な運営を実施する。</p>	<p><利用者への補償窓口対応></p> <p>1. 利用者に対する補償・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。</p>	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	<p><クラウドサービスの活用></p> <p>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。</p> <p><設備環境の確認></p> <p>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。</p> <p>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。</p> <p><コンピュータリソース配置></p> <p>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。</p> <p>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。</p>			17	コンピュータ設備面での情報漏洩対策を実施する。	<p>(クラウドサービスを利用する場合は、通番11を参照のこと)</p> <p><設備環境の確認></p> <p>1. 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。</p> <p>2. 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・暗証番号が必要)を実施している。</p> <p><コンピュータリソース配置></p> <p>1. 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。</p> <p>2. 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。</p> <p><役職員の入退室・アクセス管理></p> <p>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、アクセス制御策を講じている。(注1)</p> <p>2. 監視カメラについては、稼働時間、監視範囲、映像の保存期間を定めている。</p> <p>3. 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。</p> <p>4. 受付に警備員を常駐させている。</p> <p>(注1)</p> <p>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:入退館記録の保存等)</p> <p>(例:入退館記録の保存等)</p> <p>② 盗難等の防止のための措置(例:カメラによる記録又は作業への立会等によるモニタリングの実施、記録機能を持つ媒体の持込み・持出し禁止又は検査の実施等)</p>	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	

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所
21	コンピュータ設備管理	サーバー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	<p><内部役職員の入室・アクセス管理></p> <ol style="list-style-type: none"> 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)。 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)。 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。 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。 受付・警備員を常駐させている。 <p>(注1)具体例</p> <ol style="list-style-type: none"> ①コンピュータ室に設置する場合 <ol style="list-style-type: none"> a.部屋が専用室であり、施錠管理(入室に鍵・カード・暗証番号)を実施している ②執務室に設置する場合 <ol style="list-style-type: none"> 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 <p>(注2)具体例</p> <ol style="list-style-type: none"> 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	-	-	-	-	-	-
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	<p><データに関する確認></p> <ol style="list-style-type: none"> 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)。 <p><海外法規制の確認></p> <ol style="list-style-type: none"> 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。 <p><クラウドサービスの活用></p> <ol style="list-style-type: none"> 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。 <p>(注1)具体例</p> <ol style="list-style-type: none"> 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	<p><アクセス制御策の実施></p> <ol style="list-style-type: none"> 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)。 <p>(注1)具体例</p> <ol style="list-style-type: none"> 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 	-	-	18	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。	<p>業務上入手した重要情報の漏洩を防止するため、執務室への入室管理やアクセス管理を適切に実施する。</p>	<p><入室制限の実施></p> <ol style="list-style-type: none"> 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) <p><アクセス制御策の実施></p> <ol style="list-style-type: none"> 1. 情報資産の取得・入力段階、利用・加工段階、保管・保存段階、移送・送信段階、消去・廃棄段階において、アクセス制御策を講じている。(注2) <p>(注1)</p> <ol style="list-style-type: none"> 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。 <p>(注2)</p> <ol style="list-style-type: none"> 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:入退館記録の保存等) ② 盗難等の防止のための措置 (例:カメラ撮影による記録又は作業への立会等によるモニタリングの実施、記録機能を持つ媒体の持込み・持出し禁止又は検査の実施等) 	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原案(新旧比較表)」

通番	区分	セキュリティ対応目標	対象者	手法例	関連規定	関連規定箇所	通番	セキュリティ対応目標	解説文	手法例 / 具体例	関連規定	関連規定箇所
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	<p><入室制限の実施></p> <p>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)。</p> <p>(注1)具体例</p> <p>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</p> <p>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)</p> <p>③これらの設備がある上下階は危険が多いので避ける</p>								
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	<p><情報資産の書き込み禁止・持出し制限></p> <p>1. PCは、外部記憶媒体やスマートデバイスを経た通信手段(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)。</p> <p>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)。</p> <p>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)。</p> <p>4. 媒体の保管を行っている(注4)。</p> <p>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)。</p> <p>(注1)具体例</p> <p>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</p> <p>②書出し制御SWIによる制限(MTP転送対策制限、テザリング制限含む)</p> <p>③物理的な媒体挿入口ロック装置(FDD用鍵など)を設置</p> <p>④封印シール(封印確認およびシール在庫管理要)</p> <p>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</p> <p>⑥業務用メールの運用規程を策定すること</p> <p>(注2)具体例</p> <p>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)</p> <p>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)</p> <p>*…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」</p> <p>(注3)具体例</p> <p>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</p> <p>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</p> <p>b. 業務で使用するPCへの無断インストール禁止</p> <p>②情報資産の漏えい等のため、以下の監査またはは措置等を行っている</p> <p>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</p> <p>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</p> <p>(注4)具体例</p> <p>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</p> <p>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</p> <p>(注5)具体例</p> <p>①可搬性媒体への書き出しを機能的に禁止</p> <p>②外部WEBへの不正な情報持ち出しを禁止</p> <p>③メール経由での不正な情報持ち出しを禁止</p> <p>④可搬性媒体への書き出しを機能的に抑制</p> <p>⑤外部WEBへの不正な情報持ち出しを監視・抑制</p> <p>⑥メール経由での不正な情報持ち出しを監視・抑制</p>	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	19	内部関係者による情報漏洩の出口対策を実施する。	<p><情報資産の書き込み禁止・持出し制限></p> <p>1. PCは、外部記憶媒体やスマートデバイスを経た通信手段(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)</p> <p>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)</p> <p>3. 社内規程に基づきPCの管理(情報資産の漏洩、き損等防止策)を行っている。(注3)</p> <p>4. 媒体の保管を行っている。(注4)</p> <p>5. 情報資産の書出し・持出し等の制限を行っている。(注5)</p> <p>(注1)</p> <p>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。</p> <p>② 書出し制御SWIによる制限(MTP転送対策制限、テザリング制限含む)を実施している。</p> <p>③ 物理的な媒体挿入口ロック装置(USB用鍵等)を設置している。</p> <p>④ 封印シールを利用して(封印確認及びシール在庫管理を行っている)。</p> <p>⑤ 電子メールのルール違反のモニタリングの実施及び重要情報送信に対しての盗聴、改竄等を考慮している。</p> <p>⑥ 業務用メールの運用規程を策定している。</p> <p>(注2)</p> <p>① 記録媒体への書出しが可能な場合、書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、ログ取得及び事後監査USB鍵等による封印、USBポートの無効化等。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)</p> <p>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)</p> <p>※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</p> <p>③ システムのメンテナンスや重要情報(トークン、認証コード等)を扱えるPCでは、電子メールや業務上必要のないウェブサイトの閲覧を行わない。</p> <p>(注3)</p> <p>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。</p> <p>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</p> <p>b. 業務で使用するPCへの無断インストール禁止</p> <p>② 情報資産の漏洩等のため、以下の監査又は措置等を行っている。</p> <p>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</p> <p>b. 送信メールに対する監査の実施、又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</p> <p>(注4)</p> <p>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</p> <p>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</p> <p>(注5)</p> <p>① 可搬性媒体への書き出しを機能的に禁止</p> <p>② 外部Webへの不正な情報持ち出しを禁止</p> <p>③ 電子メール経由での不正な情報持ち出しを禁止</p> <p>④ 可搬性媒体への書き出しを機能的に抑制</p> <p>⑤ 外部Webへの不正な情報持ち出しを監視・抑制</p> <p>⑥ 電子メール経由での不正な情報持ち出しを監視・抑制</p>	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	
26	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	<p><ウイルス対策の実施></p> <p>1. 業務利用しているPC等にウイ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イルスチェックを行っている。</p> <p>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)。</p> <p>3. ウイ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。</p> <p>4. ウイ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。</p>	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	20	ウイルス感染によるシステム侵入等の攻撃を防ぐ。	<p>ウイルス感染による不正なシステム侵入が発生して、情報が外部に漏洩したり改竄されることがないように、必要な対策を実施する。</p>	<p><ウイルス対策の実施></p> <p>1. 業務利用しているPC等にウイ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ほか、可搬性記憶媒体にウイルスチェックを行っている。</p> <p>2. 業務利用しているPCのOS、アプリケーションについて、最新版へのアップデートを実施している。</p> <p>3. 電子メール、ダウンロードファイル、サーバ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)</p> <p>4. ウイ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。</p>	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

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所
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	<p><役割・責任に応じたアクセス権限の設定></p> <p>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)。</p> <p>(注1)具体例</p> <p>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</p> <p>②事業者内部における権限外者に対するアクセス制御</p> <p>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</p> <p>(注2)具体例</p> <p>①特権ID(Admin権限)</p> <p>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</p> <p>②運用ID</p> <p>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</p> <p>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</p>			21	情報資産への内 部からの不正アク セスを抑制する。	<p>顧客情報が外部 に漏洩したり改竄 されたりすること がないよう、顧客 情報が含まれる情 報資産に対する不 正アクセスを抑制 する対策を実施す る。</p>	<p><アクセス管理の実施></p> <p>1. 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。</p> <p><役割・責任に応じたアクセス権限の設定></p> <p>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実施している。(注1)</p> <p>2. アクセス権限に応じた各種IDについては、アクセス管理ルールを定め適切な管理を行っている。(注2)</p> <p><ユーザーID管理></p> <p>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。</p> <p>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。</p> <p>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。</p> <p>4. アクセス権限設定、監理に必要な措置等を講じている。(注3)</p> <p>5. ユーザー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。</p> <p><アクセス記録の分析・保存></p> <p>1. 情報資産へのアクセス及び電子データを取り扱う情報システムの稼動状況についての記録・分析を 行っている。(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等)</p> <p><ログによる運用ID・特権IDの使用履歴の確認></p> <p>1. 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 利用の申請が行われていない操作が操作ログ上に無いことを検証している。(注4)</p> <p>2. 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5)</p> <p><電子データを取り扱う情報システムの監視及び監査></p> <p>1. 電子データ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。</p> <p>2. 監視状況についての点検及び監査を行っている。</p> <p><顧客情報の改竄防止></p> <p>1. 顧客情報の取扱いに関する管理ルールを定めている。</p> <p>2. 顧客情報に関する管理ルールの遵守状況を把握している。</p> <p>3. 管理ルールの遵守状況に応じて、必要な改善を行っている。</p> <p>4. 顧客情報の改竄防止のために必要な対策を実施している。(注6)</p> <p>(注1)</p> <p>① アクセス権限所有者を特定し、漏洩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</p> <p>② 事業者内部における権限外者に対するアクセス制御</p> <p>(注2)</p> <p>① 特権ID(Administrator権限)</p> <p>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している。</p> <p>b. 特権IDの付与は、責任者の権限としている。</p> <p>c. 特権IDにおいて、アクセス権限の変更が行われた場合は、当日中に変更結果を確認している。</p> <p>② 運用ID</p> <p>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。</p> <p>b. 開発・運用部門の不正を防止するため、開発部門、運用部門を分離独立している。</p> <p>(注3)</p> <p>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・責任を明確化している。</p> <p>② 情報資産の管理区分に応じてアクセス権限を設定している。</p> <p>③ ユーザーIDは原則個人単位に設定し、共有しない。</p> <p>④ 退職や異動により不要となったユーザー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している。</p> <p>⑤ 必要に応じて規程等を見直している。</p> <p>(注4)</p> <p>① アクセスログを記録・保存し、特定条件のログ出力を検知して周知運用を行う。</p> <p>② アクセスログの記録・保存、定期的な査閲を行う。</p> <p>(注5)</p> <p>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。</p> <p>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。</p> <p>(注6)</p> <p>① TLS相互認証を行っている。</p> <p>② 電子署名技術(HTTP Signature MessagesやJSON Web Signature)を用いた要求電文への署名を検証し ている。</p> <p>③ 暗号技術(JSON Web Encryption)を用いた要求電文の暗号化を採用している。</p>	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
											FISC・安 対基準	実27 実29

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所
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	<p><アクセス管理の実施></p> <ol style="list-style-type: none"> 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。 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。 <p><特権IDの管理></p> <ol style="list-style-type: none"> 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。 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。 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	<p><本人確認の実施></p> <ol style="list-style-type: none"> 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)。 <p><関連規程や本人確認方法の構築></p> <ol style="list-style-type: none"> 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。 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。 <p><ID・パスワードの管理></p> <ol style="list-style-type: none"> 本人確認に関するパスワード総当たり攻撃によるID悪用を防止している(注2)。 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)。 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)。 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。 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有効期限を設定している。 <p><証明書による認証></p> <ol style="list-style-type: none"> 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。 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。 <p><ネットワークの限定></p> <ol style="list-style-type: none"> 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。 <p>(注1)具体例</p> <ol style="list-style-type: none"> 本人確認機能の整備 本人確認に関する情報の不正使用防止機能の整備 本人確認に関する情報が他人に知られないための対策 <p>(注2)具体例</p> <ol style="list-style-type: none"> 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 <p>(注3)具体例</p> <ol style="list-style-type: none"> 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 <p>(注4)具体例</p> <ol style="list-style-type: none"> 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	22	システムアクセス 時の認証を 実施 する。 不正アクセスによ る情報漏洩や改 竄、システム障害 等が発生させない ため、システムへ のアクセス時の本 人確認を適切に 実施する。	<p><関連規程や本人確認方法の構築></p> <ol style="list-style-type: none"> 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。 ユーザー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。(注1) <p><ID・パスワードの管理></p> <ol style="list-style-type: none"> 本人確認に関するパスワード総当たり攻撃によるID悪用を防止している。(注2) システム不正アクセスに繋がるようなIDの埋め込みを行っていない。(注3) 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) 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でパスワードの漏洩を防いでいる。 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し、その申請作業内のみ有効期限を設定している。 <p><証明書による認証></p> <ol style="list-style-type: none"> 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。 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。 <p><ネットワークの限定></p> <ol style="list-style-type: none"> 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。 <p>(注1)</p> <ol style="list-style-type: none"> 本人確認機能の整備 本人確認に関する情報の不正使用防止機能の整備 本人確認に関する情報が他人に知られないための対策 <p>(注2)</p> <ol style="list-style-type: none"> 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。 <p>(注3)</p> <ol style="list-style-type: none"> 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。 <p>(注4)</p> <ol style="list-style-type: none"> システム用のIDとしてログイン禁止としている。 	FISC・安 対基準	案1 案8 案16 案26	

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所
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となるようにする	API接続先	<p><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)。</p> <p><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)</p> <p>(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</p> <p>(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ーOS起動/終了、DBMS起動/終了、ミドルウェア起動/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</p>	FISC・安 対基準	技37	23	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となるようにする。	<p>情報漏洩やシステム障害等が発生した場合、原因を調査することができるよう、アクセスログ等を保管する。</p>	<p><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・保存を実施している。(注1)</p> <p><ログ情報の提供> 1. 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(ログ等の種類及び保存期間)を利用者に提供している。</p> <p>(注1) ① 情報資産へのアクセス及び電子データを取り扱う情報システムの稼動状況についての記録・分析を行っている。 (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等) ② 取得した記録について、漏洩防止等の観点から適切な安全管理措置を実施している。 ③ 取得した記録について、特に漏洩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している。</p>	FISC・安 対基準	実10
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制し、不正な作業を防ぐ	API接続先	<p><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制している。 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。</p> <p><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。</p>			24	作業担当者による不正行為を防ぐ対策を実施する。	<p>無断で情報を外部に持ち出す等、作業担当者が不正な行為を行うことがないよう、必要な対策を実施する。</p>	<p><単独作業の防止> 1. ログイン時に部署全体に自動的に周知されることに加えて、ログイン前に作業内容を部署全体に周知することで、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制している。 2. 作業については、常に申請・承認を行うことで、単独作業が発生しない状態を作っている。 3. 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、単独作業を抑制している。</p> <p><改ざん防止対応> 1. 利用者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(担当者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。</p> <p><第三者監査の実施> 1. 外部監査や内部検査を定期的(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。</p>		

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所
32	システム 開発・運 用管理	システム変更の単 独作業を抑制し、 不正なシステム変 更を防ぐ	API 接続先	<p><単独作業の防止></p> <ol style="list-style-type: none"> 1. 申請・承認ベースのシステム変更作業とすることで、単独作業を抑制している。 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、単独作業を抑制している。 <p><第三者監査の実施></p> <ol style="list-style-type: none"> 3. 外部監査や社内検査を定期的(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	<p><システムの品質確保></p> <ol style="list-style-type: none"> 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。 			25	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。	<p>システム変更時に 発生しがちな品質 低下を防ぐため、 必要な対策を実施 する。</p>	<p><システムの品質確保></p> <ol style="list-style-type: none"> 1. 設計書等のドキュメントやソースコード、テスト結果についてレビューする体制を整備し、実施している。 2. ソースコードの変更をリポジトリに反映させる際に、自動テストを行うことで不測の品質低下を防いでいる。 3. システム変更時には必要に応じて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。 		
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	<p><脆弱性テスト・侵入テストの実施></p> <ol style="list-style-type: none"> 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)。 <p>(注1)具体例</p> <ol style="list-style-type: none"> 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 <p>(注2)具体例</p> <ol style="list-style-type: none"> 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 			26	外部からの不正ア クセス対策を実施 する。	<p>外部からの不正ア クセスによって、 情報が漏洩したり 改竄されたりする ことがないよう、必 要な対策を実施す る。</p>	<p><不正アクセス対策の実施></p> <ol style="list-style-type: none"> 1. 不正侵入検知・防御システム(IDS・IPS)及びWebアプリケーションファイアウォール(WAF)等の導入によって、不正侵入検知や改竄検知を行っている。(注1) 2. 外部からの不正アクセスに対して、各種の防止措置を実施している。(注2) <p><サイバー脅威関連情報の収集></p> <ol style="list-style-type: none"> 1. 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、警察庁、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。 <p>(注1)</p> <ol style="list-style-type: none"> ①インターネット接続のウェブサイトで、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を設置している。 ②専用線接続でWebサーバ公開を行っており、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。 <p>(注2)</p> <ol style="list-style-type: none"> 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 (例:シグニチャ(パターンファイル)の更新間隔等) ④ネットワークによるアクセス制御機能の整備 (例:セキュリティ監視装置の設置、インターバル等) 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

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所
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	<p><不正アクセス対策の実施></p> <p>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)。</p> <p>(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</p> <p>(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</p> <p>(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)</p>	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	27	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。	<p>情報漏洩等が発 生することがない よう、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。</p>	<p><システムにおける脆弱性対策の実施></p> <p>1. システムにおける脆弱性対策(診断)を行っている。(注1) 2. 外部公開しているサーバについて、脆弱性対策を行っている。 3. セキュリティ診断、監査等を行っている。(注2) 4. ネットワーク関連機器の管理を行っている。(注3) 5. ソフトウェア管理を行っている。(注4) 6. セキュリティパッチの適用を行っている。(注5)</p> <p><脆弱性テスト・侵入テストの実施></p> <p>1. 継続的に脆弱性テストを実施している。(注6) 2. 継続的に侵入テストを実施している。(注7) 3. ネットワークの脆弱性テストを実施している。</p> <p>(注1) ① セキュリティ対策基準(セキュアコーディングルール等)の策定 ② セキュリティ診断実施ルールの策定 ③ システム新規構築、変更時の実施 ④ 定期的な診断の実施 ⑤ 診断結果に基づく対応</p> <p>(注2) 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及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する。 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する。 c. Web診断とプラットフォーム脆弱性診断を実施する。</p> <p>(注3) 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(ネットワーク機器を含む)の電源を切断してアクセス経路を必要最小限にする等、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、login、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う)。</p> <p>(注4) ① 不正アクセス、マルウェア対策のため、ソフトウェアを適切に管理している。 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。</p> <p>(注5) ① サーバ・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竄されるような脅威 (例:OSコマンド・インジェクション、SQLインジェクション、バッファオーバーフローによる任意の命令実行等)</p> <p>(注6) ① 診断の対象範囲(アプリケーション、プラットフォーム等) ② 診断の手法(ツールベース診断、手動診断又はその組み合わせ) ③ 実施インターバル(第三者による診断は年1回、ツールによる自動診断は日次等) 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の実施</p> <p>(注7) ① 診断の対象範囲(システム、データ、人、設備等) ② 第三者(専門業者)による診断 ③ 実施インターバル(年1回等) 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の実施</p>	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

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所	
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	<p><ファイアウォール等の設置></p> <ol style="list-style-type: none"> 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。 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)。 <p>(注1)具体例</p> <ol style="list-style-type: none"> アクセス可能な通信経路の限定 外部ネットワークからの不正侵入防止機能の整備 不正アクセスの監視機能の整備 ネットワークによるアクセス制御機能の整備 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	-	-	-	-	-	-	
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	<p><脆弱性対策の実施></p> <ol style="list-style-type: none"> 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。 セキュリティ診断・監査等を行っている(注1)。 ネットワーク関連機器の管理を行っている(注2)。 ソフトウェア管理を行っている(注3)。 セキュリティパッチの適用を行っている(注4)。 <p><サイバー脅威関連情報の収集></p> <ol style="list-style-type: none"> 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。 <p>(注1)具体例</p> <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 不正な侵入や、DoS攻撃への耐久性を診断 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 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 <p>(注2)具体例</p> <ol style="list-style-type: none"> 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 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) <p>(注3)具体例</p> <ol style="list-style-type: none"> 不正アクセス、マルウェア対策のため、SWの適切な管理 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 <p>(注4)具体例</p> <ol style="list-style-type: none"> 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 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 <p>※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、バッファオーバーフローによる任意の命令実行 など</p>	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	-	-	-	-	-	-	-

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所		
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、誤つ た作業の発生を防 ぐ	API 接続先	<p><ユーザーID管理></p> <ol style="list-style-type: none"> 1. 従業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. 従業員の異動、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。 <p>(注1)具体例</p> <ol style="list-style-type: none"> ①各管理段階における情報資産の取扱いに関する従業員の役割・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ー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	-	-	-	-	-	-		
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	<p><情報資産へのアクセスを記録、当該記録の分析・保存></p> <ol style="list-style-type: none"> 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働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。 <p><ログによる運用ID・特権IDの使用履歴確認></p> <ol style="list-style-type: none"> 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)。 <p><情報資産を取り扱う情報システムの監視及び監査></p> <ol style="list-style-type: none"> 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。 <p>(注1)具体例</p> <ol style="list-style-type: none"> 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 <p>(注2)具体例</p> <ol style="list-style-type: none"> 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	<p><情報の持出し・削除・廃棄管理に関する取扱い></p> <ol style="list-style-type: none"> 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。 <p><管理方法の取決め></p> <ol style="list-style-type: none"> 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	28	持ち出された機密 情報を管理する。 社外に持ち出され た機密情報が漏 洩しないよう、管 理方法を定めて、 情報管理を実施 する。	<p><情報の持出し・削除・廃棄管理に関する取扱い></p> <ol style="list-style-type: none"> 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、業者間との契約並びに社内ルール(一般物と機密情報の分類等)に則り実施している。 <p><管理方法の取決め></p> <ol style="list-style-type: none"> 1. 電子記憶媒体の入手・作成、利用、複製、保管、持出し、廃棄等現物管理全般についての管理方法(管理簿の作成等)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	<p><データの管理レベルの設定></p> <ol style="list-style-type: none"> 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	29	データの種類・内 容に応じた管理策 を実施する。 データの種類や内 容により、漏洩し た場合の影響度 が異なるため、そ れに応じた管理方 法を定めて、デー タ管理を実施す る。	<p><データの管理レベルの設定></p> <ol style="list-style-type: none"> 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 x			

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所
42	サー ビス シ ス テ ム の セ キ ユ 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	<p><安全管理措置の実施></p> <p>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)。</p> <p><データの保護・管理></p> <p>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)。</p> <p>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)。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>7. 情報資産の保護策を講じている(注4)。</p> <p><暗号化処理></p> <p>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。</p> <p>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。</p> <p>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。</p> <p><不正アクセス検知></p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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)</p> <p><テストデータの取扱い></p> <p>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)。</p> <p>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。</p> <p>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。</p> <p>(注1)具体例</p> <p>①データ保管時に暗号化する</p> <p>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</p> <p>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</p> <p>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</p> <p>(注2)具体例</p> <p>①データベース:DBMSの備えるパスワード設定</p> <p>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</p> <p>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</p> <p>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</p> <p>(注3)具体例</p> <p>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</p> <p>(注4)具体例</p> <p>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</p> <p>②データ伝送時に盗聴された場合にもデータの内容が分からないようにするための伝送データの漏えい防止策</p> <p>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</p> <p>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</p> <p>⑤データの暗号化方法(暗号化方式等)</p> <p>(注5)具体例</p> <p>①手続には以下の条件を含むこと</p> <p>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</p> <p>b.アクセスできる要員を必要最小限とすること</p> <p>c.データの消去・廃棄管理要領を定めていること</p>	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	30	機密情報の漏洩 対策を実施する。	<p><安全管理措置の実施></p> <p>1. クレジットカード番号やパスワード等の機密情報を取り扱う場合、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)</p> <p><データの保護・管理></p> <p>1. 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、暗号化又はパスワードによる保護を行っている。(注2)</p> <p>2. 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)</p> <p>3. 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洩するリスクが存在するため、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。</p> <p>4. 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。</p> <p>5. 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。</p> <p>6. 情報資産の保護策を講じている。(注4)</p> <p><暗号化処理></p> <p>1. 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等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。</p> <p>2. 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等、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。</p> <p>3. 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。</p> <p><不正アクセス検知></p> <p>1. 社内のシステム利用者による大量の顧客情報の漏洩リスクを検知する対策を実施している。</p> <p>2. 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。</p> <p>3. 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)。</p> <p><テストデータの取扱い></p> <p>1. 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)</p> <p>2. 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。</p> <p>3. 本番環境以外で使用する場合は、取引先情報の漏洩防止策として、取引先を特定可能なデータ項目、マイナンバー及びクレジットカード番号をマスク化している。</p> <p>(注1)</p> <p>①データ保管時に暗号化する。</p> <p>②パスワードやクレジットカード番号等、機密情報を画面等に表示する場合は、一部をマスクする。</p> <p>③パスワードやクレジットカード番号等、機密情報がログ等に出力されないようにする。</p> <p>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。</p> <p>(注2)</p> <p>①データベース:DBMSの備えるパスワード設定</p> <p>②文書ファイル:文書そのもの又は格納フォルダにかけるパスワード設定</p> <p>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又はパスワード設定</p> <p>④バックアップデータ:暗号化機能の実施又はパスワード設定</p> <p>(注3)</p> <p>①ハッシュ化推奨だが暗号化でも可とする。</p> <p>②二要素認証の場合は双方を対象としている。</p> <p>③暗号アルゴリズムはCRYPTREC暗号リストに記載された暗号等を使用している。</p> <p>(注4)</p> <p>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洩防止措置</p> <p>②データ伝送時に盗聴された場合にもデータの内容が分からないようにするための伝送データの漏洩防止策</p> <p>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</p> <p>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・暗号化等の措置の実施</p> <p>⑤データの暗号化方法(暗号化方式等)</p> <p>(注5)</p> <p>①手続には以下の条件が含まれる。</p> <p>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。</p> <p>b.アクセスできる要員を必要最小限とすること。</p> <p>c.データの消去・廃棄管理要領を定めていること。</p>	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	

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所
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	<p><バックアップの実施></p> <p>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。</p> <p>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)。</p> <p>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。</p> <p>(注1)具体例</p> <p>①不正アクセスの発生に備えた対応・復旧手続の整備</p> <p>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</p> <p>③リカバリー機能の整備</p>	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	31	喪失・破損した情 報の復旧を可能と する。	<p>情報が喪失したり 破損した場合にお いて、その情報を 復旧することがで きるよう、必要な 対策を実施する。</p> <p><バックアップの実施></p> <p>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。</p> <p>2. バックアップにあたっては、障害発生時の技術的対応、復旧手続を整備している。(注1)</p> <p>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の有無やデータ形式等) を制定している。</p> <p>(注1)</p> <p>① 不正アクセスの発生に備えた対応、復旧手続の整備</p> <p>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</p> <p>③ リカバリー機能の整備</p>	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 s	
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	<p><認証機能の管理></p> <p>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)。</p> <p>(注1)具体例</p> <p>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</p>			32	利用者を保護する 認証機能を整備 する。	<p>リスクに応じた適 切な認証機能によ り、利用者の利便 性とセキュリティと を両立させる。</p> <p><認証機能の管理></p> <p>1. 自社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)</p> <p><認証機能の提供></p> <p>1. 利用者を適切に保護する認証機能を提供している。(注2)</p> <p>2. セキュリティ事故の発生を想定した対策を行っている。(注3)</p> <p><認証機能の見直し></p> <p>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4)</p> <p>(注1)</p> <p>① 自社サービス内で提供している重要な機能(例:情報照会、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)を利用者に対して課しているかを漏れなく整理 し、認識している。</p> <p>(注2)</p> <p>① パスワード入力を一定回数間違えた場合のアカウントロック</p> <p>② パスワード文字数の最低数制限</p> <p>a. パスワード変更は利用者本人及び管理者が画面から行い、第三者(オペレータ等)を介さない。</p> <p>b. Windowsの場合、パスワードポリシー設定において、複雑さの要件を満たすパスワードを使用する ようにしている。</p> <p>③ ログイン履歴の確認画面の提供</p> <p>④ 2段階認証</p> <p>⑤ リスクベース認証</p> <p>(注3)</p> <p>① 不正認証検知の仕組み(リスト型攻撃への対策)</p> <p>② システム脆弱性検知の仕組み</p> <p>(注4)</p> <p>① 認証レベルが劣化することの把握</p> <p>(ID/PW認証やソーシャルログインを始め、自社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等)</p>	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 m	

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所
45	サー ビス シ ス テ ム の セ キ ユ 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	<p><認証機能の見直し></p> <p>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)。</p> <p>(注1)具体例</p> <p>①認証レベルが劣化することの把握</p> <p>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</p>								
46	サー ビス シ ス テ ム の セ キ ユ 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	<p><認証機能の提供></p> <p>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)。</p> <p>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)。</p> <p>(注1)具体例</p> <p>①最低限やるべき項目</p> <p>a.PW入力を一定回数間違えるとアカウントロック</p> <p>b.PW文字数の最低数制限</p> <p>・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</p> <p>・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</p> <p>②サービスのリスクに応じてやるべき項目</p> <p>a.ログイン履歴の確認画面の提供</p> <p>b.2段階認証</p> <p>c.リスクベース認証</p> <p>(注2)具体例</p> <p>①不正認証検知の仕組み(リスト型攻撃への対策)</p> <p>②システム脆弱性検知の仕組み</p>								
47	サー ビス シ ス テ ム の セ キ ユ 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	<p><アプリケーションの管理></p> <p>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)。</p> <p>(注1)具体例</p> <p>①配布時に電子署名を付与</p> <p>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</p> <p>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</p>			33	偽アプリケーション 対策を実施す る。	<p>偽アプリケーションによる情報漏洩 等が発生すること のないよう、必要 な対策を実施す る。</p>	<p><アプリケーションの管理></p> <p>1. スマートデバイスにおけるアプリケーション利用時の顧客保護のため、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)</p> <p>(注1)</p> <p>① アプリ作成時に電子署名を付与する。</p> <p>② スマートフォンアプリをリバースエンジニアリングされた場合に備えて、暗号化や難読化等の対策を行う。</p> <p>③ アプリ内部に個人情報を保存しない。</p> <p>④ アプリ提供サイトのパトロールを実施する。</p>		

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ対応目標	対象者	手法例	関連規定	関連規定箇所	通番	セキュリティ対応目標	解説文	手法例 / 具体例	関連規定	関連規定箇所
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	<p><不正アクセスの拡大防止></p> <p>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。</p>	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	34	不正アクセス発生時の被害拡大を最小限に止める。	不正アクセスが発生した場合、被害の拡大を最小限にするため、必要な対策を実施する。	<p><不正アクセスの拡大防止></p> <p>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。</p>	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	<p><ログの記録・保存></p> <p>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)。</p> <p>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:○、保存期間:○)</p> <p>(注1)具体例</p> <p>①システムログを取得し、内容を確認している</p> <p>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</p> <p>※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</p> <p>③望まれる水準の例:</p> <p>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</p> <p>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)</p> <p>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</p> <p>d.以下の内容が記録されること-OS起動/終了,DBMS起動/終了,ミドルウェア起動/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</p> <p>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</p> <p>f.運用者によって、アラーム報知等を監視している</p>	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	35	不正アクセス発生時の追跡調査を可能とする。	不正アクセスが発生した場合、原因や対策を検討するための追跡調査ができるよう、必要な対策を実施する。	<p><ログの取得・保管></p> <p>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、アクセスログを取得・保管している。(注1)</p> <p>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(ログ等の種類や保存期間)を取得する。</p> <p>3. 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ファイアウォールの導入等)。</p> <p>4. 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。</p> <p>5. 外部団体(デジタル・フォレンジック研究会等)から公表されるガイドライン等に則った初動対応及び証拠保全を行っている。</p> <p>(注1)</p> <p>①システムログを取得(※)し、内容を確認している。</p> <p>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。</p> <p>③その他:</p> <p>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。</p> <p>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)。</p> <p>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。</p> <p>d.以下の内容が記録される。</p> <ul style="list-style-type: none"> - OSの起動及び終了 - DBMSの起動及び終了 - ミドルウェアの起動及び終了 - ディスク装置や論理ボリュームのマウント及びアンマウント - ログ取得プログラムの起動及び停止 <p>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。</p> <p>f. 運用者によって、アラーム報知等を監視している。</p>	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 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	<p><トークンの有効期限管理></p> <p>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)</p> <p><暗号化対象の取決め></p> <p>2. 暗号化の対象を取り決めている(注1)。</p> <p>(注1)具体例</p> <p>①OAuth認証で使用する認証コード、アクセストークン</p>	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	36	認証認可に関する機密情報の漏洩対策を実施する。	認証認可に関する機密情報が漏洩することがないように、必要な対策を実施する。	<p><トークンの適切な管理></p> <p>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の管理を実施している。(注1)</p> <p><暗号化対象の取決め></p> <p>1. 暗号化の対象を取り決めている。(注2)</p> <p>(注1)</p> <p>①1時間等、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する。</p> <p>(注2)</p> <p>① OAuth2.0で使用する認可コード、アクセストークン、リフレッシュトークン</p>	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 ^g

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ対応目標	対象者	手法例	関連規定	関連規定箇所	通番	セキュリティ対応目標	解説文	手法例 / 具体例	関連規定	関連規定箇所
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	<p><APIの想定外利用の回避></p> <p>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)。</p> <p>(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</p> <p>(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</p>			37	APIの想定外利用を回避する。	<p>APIが想定外に利用されないよう、必要な対策を実施する。</p>	<p><APIの想定外利用の回避></p> <p>1. 利用するAPIの範囲や、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(注2)を回避するための原則を把握し、対策を実施している。 3. 外部団体(金融ISAC、JPCERT、警察庁、JC3等)から発行されるセキュリティリファレンス等に則った認可機能・APIリクエスト機能の開発を行っている。</p> <p>(注1) ① OAuth2.0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。 ② API提供元に求められる最低限のセキュリティ原則を理解しており、API提供元においてそれが満たされていることを確認することができる。</p> <p>(注2) APIの想定外利用とは、以下のようなものを指す。 ① URIの一部を改ざりして、サーバーにアクセスし不正に他社のデータを取得する。 ② API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に乗っ取り、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。</p>		
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	<p><ログの取得・保管></p> <p>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。</p>	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ないようにする	銀行	<p><本人確認の実施></p> <p>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。</p>	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	38	<p>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。</p>	<p>利用者が認識していないにも関わらず、利用者のアカウントがAPI接続に使用されないよう、必要な対策を実施する。</p>	<p><本人確認の実施></p> <p>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。</p>	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b

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ対応目標	対象者	手法例	関連規定	関連規定箇所	通番	セキュリティ対応目標	解説文	手法例 / 具体例	関連規定	関連規定箇所
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	<p><アクセス範囲に応じた認証の実施></p> <ol style="list-style-type: none"> 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。 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)。 <p><アクセス範囲の限定></p> <ol style="list-style-type: none"> 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。 <p>(注1)具体例</p> <ol style="list-style-type: none"> 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 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 <p>(注2)具体例</p> <ol style="list-style-type: none"> 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、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 API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	39	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。	<p>利用者にとって、API接続先が提供するサービスの利便性と、API接続に関するリスクに見合った利用者保護の双方を実現するため、最適な認証強度を確保する。</p>	<p><アクセス範囲に応じた認証の実施></p> <ol style="list-style-type: none"> 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。 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、実施している。(注2) <p><アクセス範囲の限定></p> <ol style="list-style-type: none"> 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。 <p>(注1)</p> <ol style="list-style-type: none"> ログイン時にIDとパスワード、振込時にワンタイムパスワードを用いている。 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。 <p>(注2)</p> <ol style="list-style-type: none"> 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、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。 API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e
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の攻撃に対する多層防御を図る	銀行	<p><多層防御の実施></p> <ol style="list-style-type: none"> 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の攻撃に対する多層防御を図っている(注1)。 <p>(注1)具体例</p> <ol style="list-style-type: none"> API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 API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 API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 			40	脆弱性への攻撃に対する多層防御を図る。	<p>脆弱性への攻撃によって情報漏洩等が発生することがないよう、多層防御を実施する。</p>	<p><多層防御の実施></p> <ol style="list-style-type: none"> 認証機構以外にも全体システム機構として、<u>予期していない脆弱性への攻撃</u>に対する多層防御を図っている。(注1) <p><既知の脆弱性への対応></p> <ol style="list-style-type: none"> 外部団体(金融ISAC、JPCERT、警察庁、JC3等)から発行されるセキュリティリファレンス等に則った認可機能・APIの開発を行っている。 <p>(注1)</p> <ol style="list-style-type: none"> 多層防御とは一般的に<u>侵入前対策(入口対策)</u>と、<u>侵入後(出口対策)</u>と<u>内部対策</u>を組み合わせる対策を行うものである。 <ol style="list-style-type: none"> 侵入前対策(入口対策): ウイルスやマルウェア等がネットワークに侵入する脅威から防ぐ。 侵入後対策(出口対策): ネットワークの不正通信を検出し、情報の外部流出等を防ぐ。 内部対策: 利用端末やサーバにおけるデータを監視し、異常発生時に速やかに対処する。 API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を導入する。 API接続先のIPアドレス等を限定して、それ以外からのアクセスを許容しない機構を導入する。 API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を導入する。 	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s
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	<p><トークンの管理></p> <ol style="list-style-type: none"> 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) 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。 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。 <p><暗号化対象の取決め></p> <ol style="list-style-type: none"> 暗号化の対象を取り決めている(注1)。 <p>(注1)具体例</p> <ol style="list-style-type: none"> OAuth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	41	認証の悪用リスクを可能な限り低減させる。	<p>API接続先との接続における認証が、第三者に悪用されるリスクを可能な限り低減させるため、必要な対策を実施する。</p>	<p><トークンの適切な管理></p> <ol style="list-style-type: none"> 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。(注1) 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。 不正アクセス検知後、速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。 <p><暗号化対象の取決め></p> <ol style="list-style-type: none"> 暗号化の対象を取り決めている。(注2) <p>(注1)</p> <ol style="list-style-type: none"> 1回限りとする。 1ヶ月から数ヶ月で失効する。 <p>(注2)</p> <ol style="list-style-type: none"> OAuth2.0で使用する認可コード、アクセストークン、リフレッシュトークン 	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g,m

「API接続チェックリスト原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所
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	<p><利用者保護の実施></p> <p>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。</p>	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	42	API接続先を含めた全体の認証強度をもつて、利用者保護を図る。	<p>利用者保護の観点から、金融機関はAPI接続先も含めた認証強度を適切に整備する。</p> <p><認証強度の確認・確保></p> <p>1. 利用者からAPI経由で金融機関に対して行われる個々の取引指図について、API接続先で実施している認証強度が金融機関側の認証強度に劣後しないか確認している。</p> <p>2. 金融機関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される場合、その方が利用者利便性のために適切だと考えられる取引は、他の仕組みによって利用者保護を図っている。</p>	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	
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	<p><利用者の誤認防止></p> <p>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。</p>	銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得	43	API利用に関わる利用者説明責任を果たす。	<p>利用者がAPIを利用するにあたって、重要となる事項を説明する。</p> <p><利用者の誤認防止></p> <p>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。</p> <p><利用者への説明></p> <p>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。</p>	銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得	
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	<p><利用者への説明></p> <p>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。</p>	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原案(新旧比較表)」

通番	区分	セキュリティ 対応目標	対象者	手法例	関連 規定	関連 規定 箇所	通番	セキュリティ 対応目標	解説文	手法例 / 具体例	関連 規定	関連 規定 箇所
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	<p><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)。</p> <p>(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</p>	銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得	44	利用者のAPI接続に関する誤認・誤解を防ぐ。	<p>利用者がAPI接続に関する誤認や誤解をしないよう、必要な対策を実施する。</p> <p>(注1) ① アクセス権限を付与するAPI接続先の名称 ② API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の実施 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</p>	銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得	