参考資料1

API接続チェックリスト（試行版）

平成29年6月28日
API接続先チェックリストワーキンググループ

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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

API接続チェックリスト（試行版）

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