Draft

API接続チェックリスト（フォーマット）
＜2018年10月版＞

資料2－3

2018 年10月12日
オープンAPI有識者検討会
API接続チェックリストワーキンググループ

通番	区分	セキュリティ対応目標	対象者	現在の対応状況	課題認識	課題への対応計画	関連規定	関連規定 箇所	備考
1	情報・セキュリティ管理態勢	セキュリティ管理責任の所在と対象範囲を明確にする。	API接続先				FISC・安対基準	統4、統6、 統7、統8	
2	情報・セキュリティ管理態勢	セキュリティ管理ルールを整備する。	API接続先				銀行API報告書・セキュリティ原則 --------- FISC・安対基準	3.3.1 API接続先の適格性 d --------- 統1、統12	
3	情報・セキュリティ管理態勢	役職員に対する情報管理方法の周知やモニタリング等の実施により、セキュリティ管理態勢の定着を図る。	API接続先				銀行API報告書・セキュリティ原則 --------- FISC・安対基準	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 g --------- 統13、統14、監1	
4	情報・セキュリティ管理態勢	情報資産の管理を実施する。	API接続先				銀行API報告書・セキュリティ原則	3.3.3 内部からの不正アクセス対策 e	
5	情報・セキュリティ管理態勢	役職員による不正への対策を実施する。	API接続先				銀行API報告書・セキュリティ原則	3.3.3 内部からの不正アクセス対策 c	
6	情報・セキュリティ管理態勢	自社サービスの解約時及びシステムの廃棄にあたっては機器等から情報漏洩が生じないよう、防止策を実施する。	API接続先				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（フォーマット）
＜2018年10月版＞

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
7	情報・セキュリティ管理態勢	セキュリティ不祥事案の発生に対して、振り返りと対策を実施する。	API接続先				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	情報・セキュリティ管理態勢	連鎖接続における安全性を確保する。	API接続先						
9	情報・セキュリティ管理態勢	不正アクセスや障害等の発生を想定した態勢を整備する。	共通				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	
10	外部委託管理	委託業務が円滑かつ適正に遂行されるよう、必要な対策を実施する。	API接続先				FISC・安対基準	統20、統21、統22、統23、監1	
11	外部委託管理	クラウドサービス利用にあたってはクラウドサービス固有のリスクを考慮した対策を実施する。	API接続先				FISC・安対基準	統24、監1	
12	金融機関・API接続先の協力体制	セキュリティ対策の見直しや改善を図る。	共通				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	
13	金融機関・API接続先の協力体制	利用者からの相談・照会等への対応を適切に実施する。	共通				銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得 i、j	

API接続チェックリスト（フォーマット）
＜2018年10月版＞

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
14	金融機関・API接続先の協力体制	利用者の被害拡大を防止する。	共通				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 d	
15	金融機関・API接続先の協力体制	利用者への補償を適切に実施する。	共通				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 c	
16	金融機関・API接続先の協力体制	利用者向けの補償対応窓口を適切に運営する。	共通				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 d	
17	コンピュータ設備管理	コンピュータ設備面での情報漏洩対策を実施する。	API接続先				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	
18	オフィス設備管理	不正な人物の入室を防ぎ、重要情報へのアクセスを制限する。	API接続先				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	
19	オフィス設備管理	内部関係者による情報漏洩の出口対策を実施する。	API接続先				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 -------- 実14	
20	オフィス設備管理	ウイルス感染によるシステム侵入等の攻撃を防ぐ。	API接続先				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	

API接続チェックリスト（フォーマット）
＜2018年10月版＞

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
21	システム開発・運用管理	情報資産への内部からの不正アクセスを抑止する。	API接続先				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 --------- 実27、実29	
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16、実26	
23	システム開発・運用管理	システムアクセスとその作業についてのログを保管し、有事の際に調査が可能なようにする。	API接続先				FISC・安対基準	実10	
24	システム開発・運用管理	作業担当者による不正行為を防ぐ対策を実施する。	API接続先						
25	システム開発・運用管理	システム変更時に著しく品質が低下しないよう、必要な対策を実施する。	API接続先						
26	システム開発・運用管理	外部からの不正アクセス対策を実施する。	API接続先				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	
27	システム開発・運用管理	システムやネットワークに対する脆弱性対策を実施する。	API接続先				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	

API接続チェックリスト（フォーマット）
＜2018年10月版＞

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
28	システム開発・運用管理	持ち出された機密情報を管理する。	API接続先				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	
29	サービスシステムのセキュリティ機能	データの種類・内容に応じた管理策を実施する。	API接続先				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	
30	サービスシステムのセキュリティ機能	機密情報の漏洩対策を実施する。	API接続先				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	
31	サービスシステムのセキュリティ機能	喪失・破損した情報の復旧を可能とする。	API接続先				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	
32	サービスシステムのセキュリティ機能	利用者を保護する認証機能を整備する。	API接続先				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	
33	サービスシステムのセキュリティ機能	偽アプリケーション対策を実施する。	API接続先						
34	サービスシステムのセキュリティ機能	不正アクセス発生時の被害拡大を最小限に止める。	共通				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	

API接続チェックリスト（フォーマット）
＜2018年10月版＞

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
35	サービスシステムのセキュリティ機能	不正アクセス発生時の追跡調査を可能とする。	共通				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 3.3.4 不正アクセス発生時の対応 b	
36	APIセキュリティ機能	認証認可に関する機密情報の漏洩対策を実施する。	API接続先				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	
37	APIセキュリティ機能	APIの想定外利用を回避する。	API接続先						
38	APIセキュリティ機能	利用者が認識していないところで、利用者のアカウントがAPI接続に使用されないようにする。	金融機関				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	
39	APIセキュリティ機能	利用者の利便性と、リスクに見合った利用者保護を実現する認証強度とする。	金融機関				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	
40	APIセキュリティ機能	脆弱性への攻撃に対する多層防御を図る。	金融機関				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	
41	APIセキュリティ機能	認証の悪用リスクを可能な限り低減させる。	金融機関				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（フォーマット）
＜2018年10月版＞

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
42	APIセキュリティ機能	API接続先を含めた全体の認証強度をもって、利用者保護を図る。	金融機関				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	
43	API利用セキュリティ	API利用に関わる利用者説明責任を果たす。	API接続先				銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得 d	
44	API利用セキュリティ	利用者のAPI接続に関する誤認・誤解を防ぐ。	金融機関				銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得 c	