資料2－3

「API接続チェックリスト原案（フォーマット）」（A3横Excel版）サンプル

平成30年8月2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	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	役職員に情報管理方法を周知し、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 e --------- 統13、監1	
4	情報・セキュリティ管理態勢	情報資産の取扱管理態勢を整備する。	API接続先				銀行API報告書・セキュリティ原則	3.3.3 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	役職員の不正対策を整備する。	API接続先				銀行API報告書・セキュリティ原則	3.3.3 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講じる。	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	
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、振り返りと対策を行う体制を確立する。	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	

「API接続チェックリスト原案（フォーマット）」（A3横Excel版）サンプル

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
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対応態勢を整備する。	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	委託業務が円滑及び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	
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20、統21、 統22、統23、 統24	
12	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				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	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				銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得	
14	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				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（フォーマット）」（A3横Excel版）サンプル

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
15	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				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	
16	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				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	
17	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				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	
18	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				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	執務室に不正な人物の入室を防ぐとともに重要情報へのアクセスを制限して、業務情報の漏洩を防ぐ。	API接続先						
20	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				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	
21	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				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原案（フォーマット）」（A3横Excel版）サンプル

通番	区分	セキュリティ対応目標	対象者	現在の対応状況	課題認識	課題への対応計画	関連規定	関連規定箇所	備考
22	システム開発・運用管理	システムや情報資産への不正アクセスを抑止し、顧客情報の漏洩や改竄の防止を図る。	API接続先				銀行API報告書・セキュリティ原則 --------- FISC・安対基準	3.3.3 内部からの不正アクセス対策 e --------- 実27、実29	
23	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				FISC・安対基準	実1、実8、実16、実26	
24	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	
25	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態勢を整備する。	API接続先						
26	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						
27	システム開発・運用管理	システムの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						
28	システム開発・運用管理	外部からの不正アクセスへの的確な対策や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 t、y	

「API接続チェックリスト原案（フォーマット）」（A3横Excel版）サンプル

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
29	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				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	
30	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 y	
31	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				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	
32	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				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	
33	サービスシステムのセキュリティ機能	利用者を適切に保護する認証機能を整備する。	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、必要な対策を実施する。	API接続先						
35	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				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原案（フォーマット）」（A3横Excel版）サンプル

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
36	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				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 3.3.4 不正アクセス発生時の対応 b	
37	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				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	
38	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						
39	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				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	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				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	
41	APIセキュリティ機能	脆弱性やそれの攻撃に対する多層防御を図る。	銀行						
42	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				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原案（フォーマット）」（A3横Excel版）サンプル

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
43	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				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	
44	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	
45	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				銀行API報告書・利用者保護原則	3.4.2 説明・表示、同意取得	