



API 提供事業者と API 利用事業者の農機データ連携のための

API 接続チェックリスト

解説書

2022 年 3 月版

農機 API 共通化コンソーシアム

API 提供事業者と API 利用事業者の農機データ連携ための
農機 OpenAPI 接続チェックリスト解説書

目 次

1. 位置づけ	1
2. 全体構成	4
3. 利用にあたっての留意事項等	9
4. 用語解説	10
5. 確認項目一覧表	15

1. 位置づけ

(1) 目的

オープン API (Application Programming Interface) は、API 提供事業者¹が API 利用事業者²に API を提供し、利用者（農業者等）の同意に基づいて API 提供事業者のシステムへのアクセスを許諾することをいう。その際、安全なデータ連携を行うため、API 提供事業者と API 利用事業者はセキュリティに関する確認を行うことになるが、双方は多対多の関係であるため、効率的に行うことが重要となる。

このため、API 接続が行われる際に、双方が効率的にコミュニケーションを行うためのツールとして、農機 API 共通化コンソーシアムでは、「農業分野におけるオープン API の整備に関するガイドライン（農林水産省策定）」の趣旨を踏まえ、農機・機器メーカー、ICT ベンダー等の協力を得て、「API 接続チェックリスト」を策定した。関係者がこのチェックリストを活用することにより、効率的で安全な API 接続が広く普及していくことが期待される。

なお、「API 接続チェックリスト」は、API 接続後のモニタリングにおけるコミュニケーション・ツールとしても活用することができる。

(2) 本解説書の基本的な考え方およびオープン API の主なリスクについて

1) 基本的な考え方

- 農業分野におけるオープン API の活用は、現在、世界的にも試行錯誤のフェーズにあり、考え方の整理が必要な論点が多い。とりわけ、セキュリティ対策、利用者（農業者等）保護は、オープン API を活用したサービスに対する利用者（農業者等）の信頼を確保し、オープン API の普及、活用促進・円滑化を図るうえで、重要な論点である。
- オープン API では、利用者（農業者等）からの申請・同意にもとづいて行われるとはいえ、API 提供事業者が保有する秘匿性の高い利用者（農業者等）の情報（利用者個人を特定しうる情報等）が API 利用事業者に提供され、当該 API 利用事業者において蓄積・保存されることになる。それゆえ、オープン API に取り組むに当たっては、関係者において十分なセキュリティ対策、利用者（農業者等）保護が図られることが必要となる。
- こうした認識の下、当コンソーシアムでは、他業界（銀行業界等）の事例も参考にしつつ、API の機能や連携するデータの種類・秘匿性等に応じたリスクベースアプロー

¹ 本 API 接続チェックリスト解説書における「API 提供事業者」とは、主に農機・機器メーカーを指す。

² 本 API 接続チェックリスト解説書における「API 利用事業者」とは、主に ICT ベンダーを指す。

チにもとづいて、利用者（農業者等）の利便と保護のバランスを踏まえた、農業分野のオープン API における主な確認項目³を取りまとめた。

- 取りまとめに当たっては、API 提供事業者、API 利用事業者双方に対して対応水準の目安を示すことで、API 提供事業者と API 利用事業者の協業・連携の円滑化に資するものとすることを意識した。
- なお、オープン API は、オープン・イノベーションを実現していくためのキー・テクノロジーの一つであり、今後、本技術を活用して、様々なビジネスモデルやサービスが提供されることが期待される。それゆえ、ビジネスモデルやサービスによって異なるリスクと対策の全てを網羅的に検討することは困難であり、本解説書では、様々なビジネスモデルやサービスに共通すると思われる主なリスクを想定した確認項目を取りまとめている。
- 具体的な確認項目については、各 API 提供事業者のポリシーや、個別のビジネス、各サービスのリスク、API 利用事業者の態様等に応じて個々に判断されるものであり、利用者（農業者等）保護の観点から、関係当事者において本解説書の趣旨を十分に踏まえつつ、検討されることを期待する。例えば、リスクの内容等を勘案して本解説書では挙げていない追加的な対策を講じることも考えられる。他方で、リスクが小さいと考えられるビジネスやサービス等についてはセキュリティ対策を軽減することも考えられる。

2) オープン API の主なリスク

オープン API では、API 提供事業者のシステムに新たな通信路を設けて他の企業等を経由した新たなサービスを利用者（農業者等）に提供することになるため、当該通信路を悪用したデータの漏洩・改竄や不正取引等が生じるリスクがある。これらオープン API において想定される主なリスクを列挙すれば、以下のとおり。

2) —1 セキュリティ上の脅威とリスク

- API 利用事業者のログイン ID／パスワード等が何らかの原因で漏洩し、第三者によって、API 利用事業者が不正にアクセスされるリスク
- API 利用事業者のシステムが第三者から攻撃を受けて、API 利用事業者のサービス機能の停止や、API 利用事業者からの大規模な情報流出、情報改竄／消失等が発生するリスク
- トークン⁴の発行を管理する API 提供事業者側の API 連携システムが第三者によって不正に認証され、トークンが不正に取得されるリスク
- トークンの流出や偽造等により、API 提供事業者からの大規模な情報流出、情報改竄／消失等が発生するリスク

³ API 提供事業者と API 利用事業者が安全にデータ連携を行うために確認することが想定される事項のこと。

⁴ OAuth2.0 において、API 提供事業者と他の企業等のアプリケーションを連携するための認証情報を保持した「許可証」。

- ルータ等の通信経路へのハッキング、無線通信等の傍受等により、情報流出、情報改竄／消失等が発生するリスク
- API 利用事業者のプログラム不備等により、API 提供事業者のシステムがダウンするリスク
- API 提供事業者のオープン API の通信路に不必要に大量のデータが送信され、API 提供事業者側システムの負荷が増加するリスク
- 内部の役職員が利用者情報を不正に利用（転売、私的利用を含む）するリスク

2) ー2 利用者保護上のリスク

- API 利用事業者の事業内容や社会的信用に疑義があり、API を利用したサービスによって、利用者に被害や混乱が生じるリスク
- API 利用事業者の利用者保護態勢、経済的信用、資力等に疑義があり、利用者が十分な保護を受けられないリスク
- API 利用事業者が利用者との緊急時の連絡方法を有しておらず、十分な利用者（農業者等）保護対応ができないリスク
- 利用者が、誰に何の権限を与えているのか、それにどのようなリスクがあるのか、API 利用事業者に取得される情報の利用目的は何か等について、十分に理解しないまま、API を活用したサービスを利用するリスク
- トラブルが発生した場合に、利用者がどこに問い合わせたら良いかわからなくなるリスク
- 十分な説明、表示を尽くしても、利用者がよく読まずに手続きを行うリスク
- API 利用事業者のシステムにおいて不具合、バグ等が発生し、API 提供事業者から提供された情報が正しく表示されないリスク

2. 全体構成

「API 接続チェックリスト」は、「API 接続チェックリスト解説書」（以下「解説書」という）と「API 接続チェックリスト（フォーマット）」（以下「フォーマット」という）で構成されている。それぞれの概要は以下の通り。

（1）解説書

「解説書」は、チェックリストの目的や利用方法、確認項目毎の詳細内容（セキュリティ対応目標及び手法例等）を記述したもので、チェックリストを利用するにあたって必ず読んでおくものである。

確認項目は、以下の 10 区分、46 項目で構成されている。

章	区分	各章の目的	通番
1	情報・セキュリティ管理態勢	API 利用事業者の情報・セキュリティ管理態勢について確認する。	1-8
2	外部委託管理	API 利用事業者が外部委託を行う場合、外部委託の管理態勢について確認する。	9-10
3	API 提供事業者・API 利用事業者の協力体制	利用者保護の観点から、API 提供事業者及び API 利用事業者における責任分界点や役割分担について確認する。	11-15
4	コンピュータ設備管理	API 利用事業者がサービスを提供するシステムが実装されているコンピュータ設備のセキュリティについて確認する。	16
5	オフィス設備管理	API 利用事業者がサービスを提供するシステムにアクセスする機器が設置されているオフィスのセキュリティについて確認する。	17-19
6	システム開発・運用管理	API 利用事業者の基本的な開発及び運用の管理態勢について確認する。	20-27
7	サービスシステムのセキュリティ機能	API 利用事業者が提供するサービスシステムのセキュリティ実装要件について確認する。	28-34
8	API セキュリティ機能	利用者保護の観点から、API アクセスを管理するシステムについて確認する。	35-41
9	API 利用セキュリティ	利用者への説明義務について確認する。	42-43
10	API ドキュメント管理	API 仕様に関するドキュメントとソースコードの紐づけやバージョン管理方法について確認する。	44-46

各確認項目は、以下の内容で記述されている。各欄の意味は以下の通り。

- ①区分：テーマ別分類
- ②対象者：セキュリティ対策を実施する主体
- ③通番：通し番号
- ④セキュリティ対応目標：実施すべきセキュリティ対策上の目標
- ⑤セキュリティ対応目標の説明：目標についての説明
- ⑥手法例：セキュリティ対策の例示
- ⑦注記：手法例の補足

【確認項目の記述仕様】

10 区分から該当するテーマを記載している。

- ・セキュリティ対策を実施する主体に「○」を表示している。
- ・「共通」の場合、API 利用事業者及び API 提供事業者の双方が主体となる。

① 区分	②対象者		
.....	API利用事業者	API提供事業者	共通
	○		

③ 通番...	④ 実施すべきセキュリティ対策上の目標を記載している。
---------	-----------------------------------

⑤	セキュリティ対応目標についての説明を記載している。
------------------	---------------------------

⑥ 本項目に関連して実施する手法例は、以下が考えられる。

<○○○○>

1.
2.

- ・手法例はあくまで例示として記載している。
- ・API 利用事業者と API 提供事業者は、API 利用事業者が提供するサービスの特性や機能固有のリスク等を勘案し、セキュリティ対応目標を達成するための適切な手法を協働で検討し選択することができる。

<△△△△>

1. (注 1)
2. (注 2)

⑦ (注 1)

- ①
- ②
- ③

注記は手法例の補足として記載している。
(※) 該当がない場合は記載なし

(注 2)

- ①
- ②

(2) フォーマット

「フォーマット」は、確認項目毎に現在の対応状況や課題認識等を入力できるようになっており、関係者間でコミュニケーションを行う際に利用するものである。

表頭の意味は以下の通り。

- ①通番：通し番号
- ②区分：テーマ別分類
- ③セキュリティ対応目標：実施すべきセキュリティ対策上の目標
- ④対象者：セキュリティ対策を実施する主体
- ⑤現在の対応状況：対象者が現在実施しているセキュリティ対策の状況を記載する
- ⑥課題認識：対象者が現在認識している課題を記載する
- ⑦課題への対応計画：対象者が現在認識している課題への対応計画を記載する

【フォーマットの記述仕様】

① 通番	② 区分	③ セキュリティ対応目標	④ 対象者	⑤ 現在の対応状況	⑥ 課題認識	⑦ 課題への対応計画	備考
1			⑤ 【現在の対応状況】 対象者がセキュリティ対応目標に関して、現在の対応状況を記述する。				
2			⑥ 【課題認識】 対象者が現在の対応状況を踏まえ、課題として認識していることを記述する。				
			⑦ 【課題への対応計画】 対象者が課題認識に基づき、今後の対応計画を記述する。				
3							
4							

3. 利用にあたっての留意事項等

「解説書」及び「フォーマット」を利用するにあたっては、以下について留意する。

○確認項目について

- ・ 確認項目は機密性に関するものを中心に幅広く用意した。しかし、必ずしも各 API 提供事業者が必要とする確認項目の全てを網羅したものではない。
- ・ 確認項目の「対象者」は、セキュリティ対策を実施する主体（「フォーマット」への記載者）であり、「API 利用事業者」、「API 提供事業者」、「共通」の 3 種類がある。「共通」の場合は、API 利用事業者と API 提供事業者が協働して「フォーマット」に記載する。
- ・ API 利用事業者が提供するサービスの特性や機能固有のリスク等を勘案した結果、「フォーマット」にある確認項目以外に必要なものがある場合は、各 API 提供事業者にて独自の確認項目を追加し、一方で、一部の確認項目が不要な場合は、各 API 提供事業者にて「フォーマット」から削除する（「リスクベースアプローチ」の考え方を採用する）。
- ・ API 利用事業者は、第三者認証等を取得していなければならない訳ではない。もっとも、取得している場合には、各 API 提供事業者は、効率的なコミュニケーションを行う観点や API 利用事業者から必要以上に重要情報を取得しないという観点から、エビデンス等の提出に代え、第三者認証等の活用を積極的に検討する。例えば、次の確認項目等で活用を検討することが考えられる（通番 3、通番 8、通番 9、通番 13、通番 14、通番 21、通番 24、通番 27、通番 33 等）。

○手法例について

- ・ 「解説書」に記載されている手法例はあくまで例示であり、API 利用事業者と API 提供事業者は、API 利用事業者が提供するサービスの特性や機能固有のリスク等を勘案し、セキュリティ対応目標を達成するための適切な手法を協働で検討し選択することができる。

○回答及び判断について

- ・ 「フォーマット」はコミュニケーション・ツールとして活用することを想定しているため、API 利用事業者と API 提供事業者の双方において、自社のセキュリティ実態を正しく、できるだけ具体的に回答する。
- ・ API 利用事業者が API 提供事業者との間で API 接続を検討する際、「現在の対応状況」等を予め記載して API 提供事業者に提示することにより、API 提供事業者が実施する API 利用事業者の適格性審査における双方の対応負担が軽減されるものと考えられる。
- ・ 各 API 提供事業者は API 利用事業者から対応の有無の回答を単に受けるだけでなく、「現在の対応状況」等の欄を用いて API 利用事業者と十分に会話するよう努める。
- ・ 各 API 提供事業者は、API 利用事業者が「フォーマット」に記載されている確認項目のいずれかにおいて未対応であったとしても、API 利用事業者が提供するサービスの特性や機能固有のリスク等を踏まえて、API 接続の適否を総合的に判断する。

○モニタリングにおける活用について

- ・ API 接続後のモニタリングの実施時期は、年度ごとや確認項目に変化が生じた場合等、API 利用事業者、API 提供事業者の双方で取り決めることが適当である。
- ・ API 接続後のモニタリングの方法や深度等についても、API 利用事業者、API 提供事業者の双方で取り決めることが適当である。

4. 用語解説

チェックリストにおいて用いる主要な用語の説明等は、以下の通り。

用語	説明等
API 利用事業者	API 提供事業者と API 接続する ICT ベンダー等の事業者。
CVSS	特定のベンダーに依存せず、情報システムの脆弱性に対する汎用的な評価手法の一つで、Common Vulnerability Scoring System の略称。
DBMS	コンピュータのデータベースを構築するために必要となるデータベース運用・管理のシステムのことで、データベース管理システム (Database Management System) の略称。
DMZ	インターネット等に接続されたネットワークで、ファイアウォール等の機器を用いて外部と内部の両ネットワークの間に設けられたネットワーク領域で、非武装地帯 (DeMilitarized Zone) の略称。
FTP	特定のコンピュータ間でファイルを転送するためのプロトコルの一つで、File Transfer Protocol の略称。
IDS	ネットワークやサーバについて、外部との通信を監視し、攻撃や侵入等の不正アクセス検知及び管理者に通知する機能を持つ侵入検知システム (Intrusion Detection System) の略称。
IPS	ネットワークやサーバについて、外部との通信を監視し、攻撃や侵入等の不正アクセスを検知し未然に防ぐ機能を持つ侵入防止システム (Intrusion Prevention System) の略称。
JC3	産業界、学術機関、法執行機関等それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を共有することにより、サイバー空間全体を俯瞰した上で、サイバー犯罪等のサイバー空間の脅威の大本を特定、軽減及び無効化し、以後の事案発生の防止に資するための活動を行うことを目的とした一般財団法人日本サイバー犯罪対策センター (JC3 : Japan Cybercrime Control Center) の略称。

用語	説明等
JPCERT	インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内のサイトに関する報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言等を技術的な立場から行う一般社団法人 JPCERT (Japan Computer Emergency Response Team) コーディネーションセンターの略称。
MTP	PC とスマートフォンやデジタルオーディオプレーヤー等を USB ケーブルで結んで音声や動画等のメディアファイルを転送する通信規約 (プロトコル) の一つで、メディア転送プロトコル (Media Transfer Protocol) の略称。
NFS	ネットワークを介してファイルを共有するシステムの一つで、Network File System の略称。
OAuth2.0	インターネット技術の標準化団体である IETF (Internet Engineering Task Force) の OAuth WG (ワーキンググループ) が策定した API アクセス認可の標準仕様群で、IETF が公開している技術文書「RFC (Request For Comments) 6749」に記述されている。
OS コマンド・インジェクション	Web アプリケーションの脆弱性を悪用し、OS を不正に操作する攻撃。
rexec	ネットワーク経由で別のコンピュータ上のプログラムを実行することを可能とするプログラム。
RFS	ネットワークに接続されている他のコンピュータのファイルシステムで、Remote File System の略称。
rlogin	ネットワーク経由で遠隔のサーバにログインすることを可能とするプログラム。
rsh	ネットワーク経由で別のコンピュータ上のシェルを操作することを可能とするプログラムのことで、remote shell の略称。
SMTP	電子メールを伝送するためのプロトコルの一つで、Simple Mail Transfer Protocol の略称。

用語	説明等
SQL インジェクション	Web アプリケーションの脆弱性を悪用し、SQL（データベースを操作するための言語で、Structured Query Language の略称）文を用いてデータを改竄する攻撃。
SW	ソフトウェア（software）の略称。OS とアプリケーションソフトに大別される。
TELNET	インターネット等を介して遠隔にあるネットワークに接続された機器を操作するためのプロトコルの一つで、Teletype network の略称。
URI	情報やサービス、機器等、何らかの資源（リソース）を一意に識別するためのデータ書式を定義した標準の一つで、Uniform Resource Identifier の略称。
アプリ提供サイト	安心・安全なアプリケーションを流通させるため、OS ベンダーや移動体通信事業者が運営するアプリケーション提供サイト。
アンマウント	コンピュータに接続した外部装置を、安全に取り外し可能な状態にすること。
クラウドサービス	一般的に IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）、SaaS（Software as a Service）等、いくつかの利用形態が存在する。なお、米国国立標準技術研究所（NIST）は、「最小限の管理負荷やプロバイダー交渉だけで、迅速に提供され稼働する構成変更自在のコンピュータ資源（ネットワーク、サーバ、記憶装置、サービス等）の共有プールに対する、ネットワークを通じた便利で随時のアクセスを可能とするモデル」と定義している。
コンピュータリソース	コンピュータにおいてシステムを動作させるために必要なハードウェアやネットワーク。
シェル	利用者が入出装置を操作した情報を、コンピュータに入出力するためのプログラム。
ステートフルインスペクション	ネットワークの状態を監視、記録し、通信の内容や方向等を考慮して、通信を許可あるいは遮断する機能。
ソーシャルログイン	ソーシャルメディア（Facebook 等の SNS）のアカウントを活用して、利用者の本人確認を行う認証方法。

用語	説明等
ソースコード	人間が理解し、記述しやすい言語やデータ形式を用いて記述された文字列。
チェックデジット	数値の誤り検出や捏造防止のため、一定の計算手順で付加される数値や記号。
ツールベース	手作業によるのではなく、ソフトウェアの機能を活用した方法。
トークン	API 接続において、API 提供元（農機・機器メーカー）が API 利用事業者に対して発行する文字列。認証済情報や利用元の限定、API 実行種類の制限（許可）等を利用する。
ハッシュ化	元データをハッシュアルゴリズムに従って固定長のハッシュ値（同じ長さで規則性のない値）を算出して置換すること。
バッファオーバーフロー	プログラムの不具合の一つで、コンピュータ上で確保した記憶領域を超えてデータが入力された場合に発生する事象。
マウント	コンピュータに外部装置を接続し、利用可能な状態にすること。
リスト型攻撃	予め用意した ID とパスワードがセットになったリストを基に、不正なログインを試行する攻撃。
リバースプロキシ	特定のサーバの代理として、外部からの全ての接続を中継し、データの暗号化や復号、データの圧縮等、様々な機能を設定するために利用されるサーバ。
リポジトリ	アプリケーション開発において、システムの設計情報やプログラムやデータ等の情報を記録し保管するデータベース。
レジストリ	コンピュータにおいて、ハードウェア又はソフトウェアの各種設定に関する情報を保存しているデータベース。
運用ジョブ	コンピュータ上で定期的に行われるプログラムを実行させる処理。

用語	説明等
機密情報	暗証番号、パスワード等、秘密にする情報。
重要情報	社外に漏洩した場合、ステークホルダーに多大な影響を及ぼす可能性がある機密情報や利用者（農業者等）情報等。
情報資産	企業が事業を遂行することで蓄積された一定量の価値ある情報と、情報を収集、処理、保管等を行うための装置。
多要素認証	「知識情報（パスワード等）」、「所持情報（ワンタイムパスワード等）」、「生体情報（指紋等）」といった複数の要素のうち、二つ以上の要素を組み合わせ、本人確認を行う認証方式。 二つの要素による認証は「二要素認証」とも呼ばれる。
統制対象クラウド拠点	データに対する実効的なアクセスを行う拠点であり、クラウドサービスにおける情報処理の広域性を勘案し、API 利用事業者等が統制を行うべき対象の拠点。クラウド事業者のデータセンター、オペレーションセンター、本社、営業所等さまざまな拠点が候補となるが、API 利用事業者等によって、利用するクラウドサービスの内容やクラウド事業者の内部管理状況等を踏まえ、API 利用事業者等が個別に特定することとなるため、上記の候補以外が対象となる場合もある。
農機データ	ほ場農業機械、穀物乾燥調製施設、施設園芸機器等の農機・機器から得られる各種データ。
不祥事案	個人又は団体等が起こした、社会的な信頼を失わせるような出来事。
役職員	役員及び職員。
利用者	API 利用事業者が提供するサービスに関する利用規約に同意し、API 利用事業者と利用契約を締結した者。 農機データ連携においては、当該農機を所有する農業者や農業法人が主な利用者となる。

5. 確認項目一覧表

区分	通番	セキュリティ対応目標	対象者
情報・セキュリティ管理態勢	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。	共通
	2	セキュリティ管理ルールを整備する。	共通
	3	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。	共通
	4	情報資産の管理を実施する。	共通
	5	役職員による不正への対策を実施する。	共通
	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。	共通
	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。	共通
	8	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
外部委託管理	9	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。	共通
	10	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。	共通
API 提供事業者・API 利用事業者の協力体制	11	セキュリティ対策の見直しや改善を図る。	共通
	12	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
	13	利用者の被害拡大を防止する。	共通
	14	利用者への補償を適切に実施する。	共通

区分	通番	セキュリティ対応目標	対象者
API 提供事業者・API 利用事業者の協力体制	15	利用者向けの補償対応窓口を適切に運営する。	共通
コンピュータ設備管理	16	コンピュータ設備面での情報漏洩対策を実施する。	共通
オフィス設備管理	17	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。	共通
	18	内部関係者による情報漏洩の出口対策を実施する。	共通
	19	ウイルス感染によるシステム侵入等の攻撃を防ぐ。	共通
システム開発・運用 管理	20	情報資産への内部からの不正アクセスを抑止する。	共通
	21	システムアクセス時の認証を実施する。	共通
	22	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。	共通
	23	作業担当者による不正行為を防ぐ対策を実施する。	共通
	24	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。	共通
	25	外部からの不正アクセス対策を実施する。	共通
	26	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。	共通
	27	持ち出された機密情報を管理する。	共通
サービスシステムの セキュリティ機能	28	データの種類・内容に応じた管理策を実施する。	共通
	29	機密情報の漏洩対策を実施する。	共通
	30	喪失・破損した情報の復旧を可能とする。	共通
	31	利用者を保護する認証機能を整備する。	共通

区分	通番	セキュリティ対応目標	対象者
サービスシステムのセキュリティ機能	32	偽アプリケーション対策を実施する。	API 利用事業者
	33	不正アクセス発生時の被害拡大を最小限に止める。	共通
	34	不正アクセス発生時の追跡調査を可能とする。	共通
API セキュリティ機能	35	認証認可に関する機密情報の漏洩対策を実施する。	共通
	36	API の想定外利用を回避する。	API 利用事業者
	37	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。	共通
	38	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。	共通
	39	脆弱性への攻撃に対する多層防御を図る。	共通
	40	認証の悪用リスクを可能な限り低減させる。	共通
	41	API 利用事業者を含めた全体の認証強度をもって、利用者保護を図る。	共通
API 利用セキュリティ	42	API 利用に関わる利用者説明責任を果たす。	API 利用事業者
	43	利用者の API 接続に関する誤認・誤解を防ぐ。	API 提供事業者
API ドキュメント管理	44	標準形式に準拠した API ドキュメントを公開する。	API 提供事業者
	45	API 仕様、ソースコード等の関連ドキュメントはバージョンで関連性を明確にする。	API 提供事業者
	46	変更履歴を明確にするため API ドキュメントのバージョン管理を行う。	API 提供事業者

6. 確認項目

区分
情報・セキュリティ管理態勢

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 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。
------	---------------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

<責任者の設置>

1. セキュリティ管理に関する最高責任者を明確化し、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関する業務遂行の責任者を設置している。
3. 情報資産を取り扱う部署における情報資産管理に関する責任者を設置している。

<最高責任者・責任者の業務>

1. セキュリティ管理に関する最高責任者は、情報管理に関する各種対策を実施している。
(注 1)
2. API 利用サービスを所管する部署のセキュリティ管理に関する責任者は、情報管理に関する各種対策を実施している。(注 2)

(注1) 対策の例：

- 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関する責任者」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関す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) 対策の例：

- 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関する最高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

区分
情報・セキュリティ管理態勢

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 2	セキュリティ管理ルールを整備する。
------	-------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

<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関する基本方針、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、点検及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。

<アクセス管理ルールの整備>

1. データ管理者の設置及び利用者（農業者等）情報にアクセスできる者の特定と、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。

(注1) 基本方針、取扱規定の例：

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 各管理段階に関する取扱規程の整備

- 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. 漏洩事案等への対応の段階

③ 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

区分
情報・セキュリティ管理態勢

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 3	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。
------	--

全社的にセキュリティ管理態勢を定着させるため、役職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。

本項目に関連して実施する手法例は、以下が考えられる。

<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に行っている。

<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)

<体制の整備>

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。
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。

<エビデンスの確保>

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。

<モニタリングの実施>

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。
2. 情報資産を取り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。
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。

<監査の実施>

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)

＜第三者認証等の利用＞

1. API 接続に関するセキュリティ管理態勢を含めた第三者認証を取得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、第三者認証等未取得していなければならない訳ではない。

（注１） 教育、訓練等の例：

- 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関す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

（注２） 監査体制の例：

- 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時は、その改善の実施

区分
情報・セキュリティ管理態勢

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 4	情報資産の管理を実施する。
------	---------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

<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) 台帳の記載項目の例：

- 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

区分
情報・セキュリティ管理態勢

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 5	役職員による不正への対策を実施する。
------	--------------------

社内から無断で情報が持ち出されること等がないよう、役職員に対して不正対策を 実施する。

本項目に関連して実施する手法例は、以下が考えられる。

< 役職員の不正対策 >

1. 役職員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い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) 開示契約等の例：

- 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. 役職員の退職後における非開示義務遵守の規定
- ② 派遣社員に従事させる場合に、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。

区分
情報・セキュリティ管理態勢

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 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。
------	--

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。

本項目に関連して実施する手法例は、以下が考えられる。

<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。

<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)

(注1) 情報漏洩防止策の例：

- 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

(注2) 廃棄計画の項目例：

- 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

区分
情報・セキュリティ管理態勢

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 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。
------	---------------------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

＜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。

区分	対象者		
	API 利用事業者	API 提供事業者	共通
情報・セキュリティ管理態勢			○

通番 8	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。

本項目に関連して実施する手法例は、以下が考えられる。

＜不正アクセス（情報漏洩事案等）の発生を想定した対応態勢の整備＞

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洩事案等の影響、原因等に関する調査を行う体制を整備している。
4. 再発防止策、事後対策の検討を行う体制を整備している。

＜障害等発生時の対応態勢の整備＞

1. 障害等の発生に備えて緊急時の連絡体制を決めている。
2. 緊急時の連絡体制を定期的に見直している。
3. 障害検知後、事業責任者に通知するまでの時間や利用者の連絡窓口へ通知するまでの時間などを予め取り決めている。

(注1) 不正アクセス発生時の対応例：

- 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

(注2) API 提供事業者側の連絡先の例：

- 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

区分	対象者		
外部委託管理	API 利用事業者	API 提供事業者	共通
			○

通番 9	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）⁵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。

本項目に関連して実施する手法例は、以下が考えられる。

<委託先の選定>

1. 外部委託する場合、委託先の選定基準を策定している。
2. 外部委託する際の規程を整備している。
3. 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。

<委託契約の締結>

1. 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。

<委託状況の確認>

1. 委託先の管理状況を把握している。（注1）
2. 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。
3. 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。

（注1）管理状況の把握方法の例：

- 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。

外部委託には、API 提供事業者や API 利用事業者と ICT 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。

区分	対象者		
	API 利用事業者	API 提供事業者	共通
外部委託管理			○

通番 10	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。
-------	---

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。

本項目に関連して実施する手法例は、以下が考えられる。

<委託先の選定>

1. 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。
2. 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。
3. クラウドサービスを利用する際に、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。

<契約の締結>

1. 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。
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。

<委託状況の確認>

1. 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、内容について確認している。
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。
3. 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。
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。

区分
API 提供事業者 ・ API 利用事業者の協力体制

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 11	セキュリティ対策の見直しや改善を図る。
-------	---------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

<協力体制の整備>

1. セキュリティ対策の見直し・改善・高度化に向けて、API 提供事業者・API 利用事業者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。

区分
API 提供事業者 ・ API 利用事業者の協力体制

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 12	利用者からの相談・照会等への対応を適切に実施する。
-------	---------------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

＜利用者からの相談・照会等への対応＞

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。

＜利用者への連絡先表示＞

1. 利用者からの相談・照会、苦情、問い合わせ等のための連絡先を表示している。

区分
API 提供事業者 ・ API 利用事業者の協力体制

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 13	利用者の被害拡大を防止する。
-------	----------------

利用者の被害が拡大しないよう、必要な対策を実施する。

本項目に関連して実施する手法例は、以下が考えられる。

<利用者への連絡手段確保>

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。

（注1） 連絡手段の例

- ① 電子メール
- ② 電話
- ③ ウェブサイト
- ④ SNS

区分
API 提供事業者 ・ API 利用事業者の協力体制

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 14	利用者への補償を適切に実施する。
-------	------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

<利用者への補償対応>

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。
2. API 利用事業者と API 利用事業者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。

区分
API 提供事業者 ・ API 利用事業者の協力体制

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 15	利用者向けの補償対応窓口を適切に運営する。
-------	-----------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

<利用者への補償窓口対応>

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。

区分	対象者		
コンピュータ設備管理	API 利用事業者	API 提供事業者	共通
			○

通番 16	コンピュータ設備面での情報漏洩対策を実施する。
-------	-------------------------

コンピュータ設備に情報資産（電子データ）が保管されている場合、情報資産（電子データ）の漏洩を防止するため、コンピュータ設備面での対策を実施する。

本項目に関連して実施する手法例は、以下が考えられる（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）。

<設備環境の確認>

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。
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。

<コンピュータリソース配置>

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。
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。

<役職員の入退室・アクセス管理>

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）
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。
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。
4. 受付に警備員を常駐させている。

（注 1）アクセス制御策の例：

- 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：入退館記録の保存等）
- 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）

区分	対象者		
オフィス設備管理	API 利用事業者	API 提供事業者	共通
			○

通番 17	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。
-------	------------------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

<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)

<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、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)

(注1) 入室制限の例：

- 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。

(注2) アクセス制限策の例：

- 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)

区分	対象者		
	API 利用事業者	API 提供事業者	共通
オフィス設備管理			○

通番 18	内部関係者による情報漏洩の出口対策を実施する。
-------	-------------------------

内部関係者による情報の無断持出しを防止するための対策を実施する。

本項目に関連して実施する手法例は、以下が考えられる。

<情報資産の書込み禁止・持出し制限>

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）による情報漏洩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 PC の管理（情報資産の漏洩、毀損等防止策）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・持出し等の制限を行っている。（注5）

（注1） 情報漏洩リスク対策の例：

- ① 管理者によるレジストリ設定で USB の書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）を実施している。
- 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。
- ④ 封印シールを利用している（封印確認及びシール在庫管理を行っている）。
- 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。
- ⑥ 業務用メールの運用規程を策定している

(注2) 情報資産の取扱状況の管理例：

- 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。)
- 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
- 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。

(注3) PC 管理の例：

- 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み禁止や、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 情報資産の漏洩等のため、以下の監査又は措置等を行っている。
 - 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、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

(注4) 記憶媒体の保管方法例：

- 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) 情報資産の書出し・持出し等の制限例：

- ① 可搬性媒体への書出しを機能的に禁止
- ② 外部 Web への不正な情報持出しを禁止
- ③ 電子メール経由での不正な情報持出しを禁止
- ④ 可搬性媒体への書出しを機能的に抑止
- ⑤ 外部 Web への不正な情報持出しを監視、抑制
- ⑥ 電子メール経由での不正な情報持出しを監視、抑制

区分	対象者		
	API 利用事業者	API 提供事業者	共通
オフィス設備管理			○

通番 19	ウイルス感染によるシステム侵入等の攻撃を防ぐ。
-------	-------------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

＜ウイルス対策の実施＞

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。
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。
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)
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。

区分	対象者		
システム開発・運用管理	API 利用事業者	API 提供事業者	共通
			○

通番 20	情報資産への内部からの不正アクセスを抑止する。
-------	-------------------------

利用者（農業者等）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に、利用者（農業者等）情報が含まれる情報資産に対する不正アクセスを抑止する対策を実施する。

本項目に関連して実施する手法例は、以下が考えられる。

＜アクセス管理の実施＞

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。

＜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実施している。
(注1)
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)

＜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、監理に必要な措置等を講じている。(注3)
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。

＜アクセス記録の分析・保存＞

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)

＜ログによる運用ID・特権IDの使用履歴の確認＞

1. 開発・運用部門での運用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）
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）

＜電子データを取り扱う情報システムの監視及び監査＞

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。
2. 監視状況についての点検及び監査を行っている。

＜利用者（農業者等）情報の改竄防止＞

1. 利用者（農業者等）情報の取扱いに関する管理ルールを定めている。
2. 利用者（農業者等）情報に関する管理ルールの遵守状況を把握している。
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。
4. 利用者（農業者等）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）

（注1） アクセス制限の対策例

- 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
- ② 事業者内部における権限外者に対するアクセス制御

(注2) アクセス管理ルール例:

① 特権 ID (Administrator 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している。
- b. 特権 ID の付与は、責任者の権限としている。
- 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。

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、開発部門、運用部門を分離独立している。

(注3) アクセス権限設定、監理に必要な措置例:

- 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・責任を明確化している。
- 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。
- 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している。
- ⑤ 必要に応じて規程等を見直している。

(注4) アクセス分析・検証例:

- 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。
- ② アクセスログの記録・保存、定期的な査閲を行う。

(注5) 漏洩リスクが高い時間帯におけるアクセス分析・検証例:

- 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。

(注6) 利用者情報の改竄防止対策例:

- ① TLS 相互認証を行っている。
- 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。
- 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。

区分	対象者		
システム開発・運用管理	API 利用事業者	API 提供事業者	共通
			○

通番 21	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、システム障害等を発生させないため、システムへのアクセス時の本人確認を適切に実施する。

本項目に関連して実施する手法例は、以下が考えられる。

＜関連規程や本人確認方法の構築＞

1. 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。
2. 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）

＜ID・パスワードの管理＞

1. 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）
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）
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）
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。
5. 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の有効期限を設定している。

＜証明書による認証＞

1. 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。
2. 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＞

1. 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) 本人確認方法に係る対策の例

- 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) ID 悪用防止策の例：

- 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) 不正アクセス防止策の例：

- 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) ID の管理例：

- ① システム用の ID としてログイン禁止としている。

区分		対象者		
システム開発・運用管理		API 利用事業者	API 提供事業者	共通
				○
通番 22	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。			

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。

本項目に関連して実施する手法例は、以下が考えられる。

<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)

<ログ情報の提供>

1. 情報資産利用者の利用状況、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）を情報資産利用者に提供している。

(注1) 記録の分析・保存方法の例：

- 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。

区分	対象者		
	API 利用事業者	API 提供事業者	共通
システム開発・運用管理			○

通番 23	作業担当者による不正行為を防ぐ対策を実施する。
-------	-------------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

<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止している。
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、単独作業を抑止している。

<改竄防止対応>

1. 利用者宛に表示するデータについて、利用部署、担当者による改竄を防止する対策（担当者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。

<第三者監査の実施>

1. 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ことを確認している。

区分	対象者		
	API 利用事業者	API 提供事業者	共通
システム開発・運用管理			○

通番 24	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。
-------	-----------------------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

＜システムの品質確保＞

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。

区分	対象者		
システム開発・運用管理	API 利用事業者	API 提供事業者	共通
			○

通番 25	外部からの不正アクセス対策を実施する。
-------	---------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

<不正アクセス対策の実施>

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）

<サイバー脅威関連情報の収集>

1. 日頃からメーカー、セキュリティベンダー、外部団体（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。

(注1) 不正侵入検知方法の例：

- 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。

(注2) 不正アクセス防止措置の例：

- 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
(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

区分
システム開発・運用管理

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 26	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。
-------	----------------------------

情報漏洩等が発生することがないように、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。

本項目に関連して実施する手法例は、以下が考えられる。

＜システムにおける脆弱性対策の実施＞

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）

＜脆弱性テスト・侵入テストの実施＞

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。

(注1) 脆弱性対策の例：

- 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

(注2) セキュリティ診断、監査等の例：

- 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。

(注3) ネットワーク関連機器の管理例：

- 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（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、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う）。

(注4) ソフトウェア管理の例：

- 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。

(注5) セキュリティパッチの適用方法例：

- 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）

(注6) 脆弱性テストの例：

- 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

(注7) 侵入テストの例：

- 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

区分	対象者		
	API 利用事業者	API 提供事業者	共通
システム開発・運用管理			○

通番 27	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。

本項目に関連して実施する手法例は、以下が考えられる。

<情報の持出し・削除・廃棄管理に関する取扱い>

1. 重要な機密情報、利用者（農業者等）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。

<管理方法の取決め>

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。

区分
サービスシステムのセキュリティ機能

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 28	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。

本項目に関連して実施する手法例は、以下が考えられる。

＜データの管理レベルの設定＞

1. 自社サービスで取り扱われるデータのうち、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。

区分
サービスシステムのセキュリティ機能

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 29	機密情報の漏洩対策を実施する。
-------	-----------------

機密情報が漏洩しないよう、必要な漏洩対策を実施する。

本項目に関連して実施する手法例は、以下が考えられる。

<安全管理措置の実施>

1. 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)

<データの保護・管理>

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)
2. お客さまが使用するパスワードのデータをハッシュ化している。(注3)
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。
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。
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。
6. 情報資産の保護策を講じている。(注4)

<暗号化処理>

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。
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。
3. 回線の暗号化の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>

1. 社内のシステム利用者による大量の利用者（農業者等）情報の漏洩リスクを検知する対策を実施している。
2. 利用者（農業者等）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。
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）。

<テストデータの取扱い>

1. テストに利用する本番データに含まれる利用者（農業者等）情報について、マスキング等により、利用者（農業者等）を特定できない形式に変更する手続きを定め、実施している。（注5）
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。
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をマスク化している。

(注1) 安全管理措置の例：

- ① データ保管時に暗号化する。
- ② パスワード等、機密情報を画面等に表示する場合は、一部をマスクする。
- ③ パスワード等、機密情報がログ等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) パスワードによる保護の例：

- 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：文書そのもの又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又はパスワード設定
- ④ バックアップデータ：暗号化機能の実施又はパスワード設定

(注3) 利用者パスワード暗号化の例：

- ① ハッシュ化推奨だが暗号化でも可とする。
- ② 二要素認証の場合は双方を対象としている。
- 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。

(注4) 情報資産保護策の例：

- 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洩防止措置
- ② データ伝送時に盗聴された場合にもデータの内容が分からないようにするための伝送データの漏洩防止策
- 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・暗号化等の措置の実施
- ⑤ データの暗号化方法（暗号化方式等）

(注5) 利用者情報の取扱い手続きの例：

- ① 手続きには以下のような条件が含まれる。
 - 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。

区分
サービスシステムのセキュリティ機能

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 30	喪失・破損した情報の復旧を可能とする。
-------	---------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

＜バックアップの実施＞

- 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。
- 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)
- 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。

(注1) 障害発生時の技術的対応、復旧手続を整備例：

- 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

区分	対象者		
	API 利用事業者	API 提供事業者	共通
サービスシステムのセキュリティ機能			○

通番 31	利用者を保護する認証機能を整備する。
-------	--------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

<認証機能の管理>

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)

<認証機能の提供>

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)
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)

<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4)

(注1) サービス構成の整備例：

- 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。

(注2) 認証機能の提供例：

- 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
- ② パスワード文字数の最低数制限
 - 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。
 - 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。
- ③ ログイン履歴の確認画面の提供
- ④ 2段階認証
- ⑤ リスクベース認証

(注3) セキュリティ事故の発生を想定した対策の例：

- 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

(注4) 認証レベルの見直し例：

- ① 認証レベルが劣化することの把握
(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)

区分	対象者		
	API 利用事業者	API 提供事業者	共通
サービスシステムのセキュリティ機能	○		

通番 32	偽アプリケーション対策を実施する。
-------	-------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

<アプリケーションの管理>

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利用者保護のため、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)

(注1) アプリケーションの管理例：

- ① アプリ作成時に電子署名を付与する。
- 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。
- ③ アプリ内部に個人情報を保存しない。
- ④ アプリ提供サイトのパトロールを実施する。

区分
サービスシステムのセキュリティ機能

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 33	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。

本項目に関連して実施する手法例は、以下が考えられる。

<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。

区分
サービスシステムのセキュリティ機能

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 34	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。

本項目に関連して実施する手法例は、以下が考えられる。

<ログの取得・保管>

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)
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。
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)。
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。
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。

(注1) ログの取得・管理の例：

① システムログを取得（※）し、内容を確認している。

※OS 機能や業務アプリケーションにて作業結果を記録

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。

③ その他：

- 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. ユーザー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。
 - 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
- 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。

区分
API セキュリティ機能

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 35	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。

本項目に関連して実施する手法例は、以下が考えられる。

<トークンの適切な管理>

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の管理を実施している。

(注 1)

<暗号化対象の取決め>

1. 暗号化の対象を取り決めている。(注 2)

(注 1) トークン管理の例：

- ① 1 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。

(注 2) 暗号化対象の例：

- 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

区分
API セキュリティ機能

対象者		
API 利用事業者	API 提供事業者	共通
○		

通番 36	API の想定外利用を回避する。
-------	------------------

API が想定外に利用されないよう、必要な対策を実施する。

本項目に関連して実施する手法例は、以下が考えられる。

<API の想定外利用の回避>

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、セキュリティ対策を実施している。
3. 外部団体（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。
4. 利用する API のサービスレベル（注 3）を理解している。

(注1) 理解が必要な項目の例：

- 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。

(注2) API の想定外利用とは、以下のようなものを指す。

- ① URI の一部を改竄して、サーバ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。

(注3) API のサービスレベルとは、以下のようなものを指す。

- ① システム稼働日
- ② サービス提供時間帯
- ③ API のオンライン応答時間

区分
API セキュリティ機能

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 37	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。
-------	--

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。

本項目に関連して実施する手法例は、以下が考えられる。

<本人確認の実施>

1. API 利用事業者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。

区分
API セキュリティ機能

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 38	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。
-------	-------------------------------------

利用者にとって、API 利用事業者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。

本項目に関連して実施する手法例は、以下が考えられる。

<アクセス範囲に応じた認証の実施>

1. API 利用事業者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。

<アクセス範囲の限定>

1. API 利用事業者に付与するアクセス権限について、API 利用事業者が提供するサービスに必要な範囲に限定している。

区分	対象者		
API セキュリティ機能	API 利用事業者	API 提供事業者	共通
			○

通番 39	脆弱性への攻撃に対する多層防御を図る。
-------	---------------------

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に、多層防御を実施する。

本項目に関連して実施する手法例は、以下が考えられる。

<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、予期していない脆弱性への攻撃に対する多層防御を図っている。(注1)

<既知の脆弱性への対応>

1. 外部団体（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。

(注1) 多層防御の例：

- ① 多層防御とは一般的に侵入前対策（入口対策）と、侵入後対策（出口対策）と内部対策を組み合わせで対策を行うものである。
 - a. 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。
 - b. 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。
 - c. 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。
- ② API 利用事業者とのサーバ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。
- ③ API 利用事業者の 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。
- ④ API 利用事業者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。

区分
API セキュリティ機能

対象者		
API 利用事業者	API 提供事業者	共通
		○

通番 40	認証の悪用リスクを可能な限り低減させる。
-------	----------------------

API 利用事業者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。

本項目に関連して実施する手法例は、以下が考えられる。

<トークンの適切な管理>

1. API 利用事業者が発行するトークンには、適切な有効期限を設定している。
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、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。

<暗号化対象の取決め>

1. 暗号化の対象を取り決めている。(注1)

(注1) 暗号化対象の例：

- 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

区分	対象者		
API セキュリティ機能	API 利用事業者	API 提供事業者	共通
			○

通番 41	API 利用事業者を含めた全体の認証強度をもって、利用者保護を図る。
-------	------------------------------------

利用者保護の観点から、API 提供事業者は API 利用事業者も含めた認証強度を適切に整備する。

本項目に関連して実施する手法例は、以下が考えられる。

<認証強度の確認・確保>

1. 利用者から API 経由で API 提供事業者に対して行われる個々の指図について、API 利用事業者で実施している認証強度が API 提供事業者側の認証強度に劣後しないか確認している。
2. API 提供事業者側で行う認証強度に対して、API 利用事業者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。

区分	対象者		
API 利用セキュリティ	API 利用事業者	API 提供事業者	共通
	○		

通番 42	API 利用に関わる利用者説明責任を果たす。
-------	------------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

<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。

<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。

区分	対象者		
API 利用セキュリティ	API 利用事業者	API 提供事業者	共通
		○	

通番 43	利用者の API 接続に関する誤認・誤解を防ぐ。
-------	--------------------------

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。

本項目に関連して実施する手法例は、以下が考えられる。

＜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できる限り分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） 重要情報の項目例：

- ① アクセス権限を付与する API 利用事業者の名称
- 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

区分
API ドキュメント管理

対象者		
API 利用事業者	API 提供事業者	共通
	○	

通番 44	標準形式に準拠した API ドキュメントを公開する。
-------	----------------------------

API がより広く活用されるため、RFC、ISO などで規定している標準を可能な範囲で適用する。

本項目に関連して実施する手法例は、以下が考えられる。

<標準形式への準拠>

1. ステートレスやリソース指向等、REST の API 設計原則に可能な限り従う。
2. 標準フォーマットである Swagger の仕様に準じてドキュメントを管理する。(注1)

(注1) Swagger の詳細：

①Swagger は、RESTful API を構築するためのオープンソースのフレームワークで、「Open API Initiative」という団体が RESTful API のインターフェイスの記述をするための標準フォーマットとして推進。

区分
API ドキュメント管理

対象者		
API 利用事業者	API 提供事業者	共通
	○	

通番 45	API 仕様、ソースコード等の関連ドキュメントはバージョンで関連性を明確にする。
-------	--

API のバージョンコントロールと下位互換性を保証するため、API 仕様、ソースコードの関連ドキュメントをバージョン管理する。

本項目に関連して実施する手法例は、以下が考えられる。

<API 仕様等のバージョン管理>

1. API 仕様は、〈メジャー〉．〈マイナー〉．〈修正〉 の3つの要素でバージョンを表現する。
2. API 仕様は、Swagger を利用してバージョンを管理する。
3. API のバージョンは URI 構造で定義する。

区分
API ドキュメント管理

対象者		
API 利用事業者	API 提供事業者	共通
	○	

通番 46	変更履歴を明確にするため API ドキュメントのバージョン管理を行う。
-------	-------------------------------------

API ドキュメントのバージョン管理により、新しいデータまたは機能が追加されたときに、既存の仕様および利用者に影響するかどうかを確認できるようにする。

本項目に関連して実施する手法例は、以下が考えられる。

<バージョンによる変更履歴の管理>

1. API 標準のドキュメント<メジャー>、<マイナー>、<修正>の3つの要素でバージョンを表現する。
 - メジャー：大きな変更要素の為、別の実装が必要な場合。例えばセキュリティの仕組みの変更等。
 - マイナー：変更が行われるが同じメジャーバージョン内では下位互換性が担保される場合。
 - 修正：ドキュメント内容の表現の修正や説明を分かりやすくするための追加