BRANDEFENSE COUNTRY REPORT · JAPAN 2026

# Brandefense 日本サイバー脅威動向レポート 2026

認証情報、共有サービス、確認された影響の範囲

Odin by Brandefense
調査対象期間: 2026 年 1 月 1 日〜11 月 22 日
バージョン 1.0 · 公開調査版 · TLP:CLEAR · 2026 年 11 月 8 日〜22 日

**85 / 250**
確認時点で認証情報の販売掲載があった選定組織

**6**
詳細に扱う主張の事例。それぞれの証拠の範囲を区別

**146**
日本のラベルが付いたランサムウェア掲載。いずれも犯罪者の主張を記録したもの

**30 / 60 / 90**
責任者を定めた対応計画の確認日

目次

# 目次

**Translated with AI**

この版は英語の原版からAIで翻訳しました。内容に相違がある場合は英語版を優先します。


| | | |
|---|---|---|
| 01 | 要旨 | 05 |
| | 本報告の構成 | 09 |
| 02 | 日本の事業環境 | 10 |
| 03 | 国全体の露出状況と選定組織群 | 14 |
| 04 | 地下フォーラムの活動と投稿から分かること | 23 |
| 05 | 公表された事案と分野別の対応 | 39 |
| 06 | 可用性と接続機器のリスク | 73 |
| 07 | 脅威アクター、攻撃活動、裏付けのある関係 | 77 |
| 08 | 詐欺が狙う業務手順と委任されたアクセス | 90 |
| 09 | 銀行と金融サービスの依存関係 | 94 |
| 10 | 規制対応と報告 | 99 |
| 11 | 見通しと条件付きシナリオ | 104 |
| 12 | 行動計画 | 108 |
| A | Appendix A. 調査範囲と証拠の境界 | 114 |
| B | Appendix B. 証拠一覧 | 117 |
| C | Appendix C. 出典 | 122 |
| D | Appendix D. 用語集 | 132 |



| | |
|---|---|
| 経営層 | 01 05 11 12 |
| CISO・対応責任者 | 03 04 07 12 |
| SOC・認証管理 | 04 07 08 09 |
| 運用・委託先管理 | 02 05 06 12 |
| 法務・個人情報・不正対策 | 05 08 09 10 |

# 本版について

AIによる翻訳。内容に相違がある場合は英語版を優先する。

日本の公表事案と地下市場の主張は、異なる対応判断を求めている。認証情報を検証し、重要サービスを維持し、影響を受けた情報の範囲を特定する必要がある。

**146**

日本関連のランサムウェア掲載。犯罪者側の主張

**51/100 (B)**

選定対象群の全国Atlas代表値

**101**

DMARCのquarantineまたはrejectを指定する評価対象ドメイン

**85 / 250**

現在の認証情報販売掲載がある組織

# 目次と読み進め方

| 章 | 問い |
| --- | --- |
| 1 要旨 | どの判断を優先すべきか |
| 2 運用環境 | 日本の対応優先順位を変える依存関係は何か |
| 3 組織の露出 | 選定した対象群から何が分かるか |
| 4 地下市場の活動 | 販売、購入希望、再投稿は何を示すか |
| 5 公表された事案 | どの公表が分野別の判断を変えるか |
| 6 可用性と機器 | ウェブサイトと運用設備のリスクはどう違うか |
| 7 実行主体とキャンペーン | どの関係に出典の裏付けがあるか |
| 8 詐欺 | 連絡手段、同意、保管された本人確認情報はどう被害につながるか |
| 9 銀行 | 委託先、顧客、取引のリスクをどう分けるか |
| 10 規制 | どの義務と報告経路が適用されるか |
| 11 見通し | どの条件付きシナリオに備えるべきか |
| 12 行動計画 | 誰が対応し、何を完了の証拠とするか |
| 付録 A–D | 範囲、証拠一覧、出典、用語集 |

章 01

# 要旨

01

この章で答える問い

日本の組織にどの対応が求められるか

**4**

認証情報、継続性、データ保管、報告の判断


経営層が行う 4 つの判断 07

主な数値 07

章 01

# 要旨

概要

証拠からは、認証情報の検証、委託先を含む継続性、データの最小化、正確な報告を優先すべきと考えられる。公表事案には、システム境界を越える認証情報、共有サービスの停止、機微な過去データが登場する。地下市場の販売投稿は検証すべき主張であり、全国の事案数ではない。Ransompediaの日本関連掲載は 146 件である。DNSでは評価対象 250 ドメインのうち 101 がDMARCの強制処理を指定していた。認証情報アラートの責任者を定め、重要サービスの代替手段を試し、保管情報を見直し、最初の信頼できる認知時点から報告を訓練する。

本報告は、Odin by Brandefenseが保有する地下市場の投稿、Ransompediaの掲載、選定ドメインの観測、公表された原資料を組み合わせている。対象群は別々である。投稿、掲載、公表事案、認証情報のレコード、影響を受けた人を合算して全国の攻撃件数とはしない。[S1][S2][S3][S4]

対象期間の終日は 11 月 22 日である。調査中も当日は進行しており、出典の確認は 11 月 23 日まで行った。公表、検知、初期侵入、その後の範囲更新は異なる日付である。各事例ではこの違いを保っている。

1. **委託先の事案は、顧客側の認証情報と継続性の判断にも及ぶ。** RIKENの更新では、収集または移動の痕跡がある外部システム用認証情報 430 件が示された。クラウド事業者の事例では、顧客組織 495 が影響を受けた。決済基盤の事案では、利用先ごとの確認と段階的な再開が必要になった。これらは異なる影響であり、共通の侵入経路を示すものではない。[S6][S8][S12]

2. **当初の目的を終えた保管情報が、被害を広げることがある。** 11 月のレンタカー関連の注意喚起は、顔写真付き本人確認書類の画像を扱っている。教育機関の事例には、委託先に残った過去の移行データが含まれる。他の公表では、退会者、未完了の口座申込み、残存したテストデータが区別されている。アクセス管理とともに、保管目的と削除の判断が必要である。[S71][S16][S31][S50]

3. **犯罪者の販売投稿から導ける結論は、見出しより狭い。** 11 月の不動産関連の投稿には、弁護士登録に関する項目が並んでいる。別の交通関連の販売投稿も、大量の行数を掲げているが内容は認証されていない。商取引データの再投稿は、元の取得時期を 2024 年と述べている。出所とアカウントの確認は必要だが、投稿ごとに新たな事案が起きたとはいえない。[S1]

4. **恐喝掲載は復旧準備に役立つが、全国の攻撃件数ではない。** Ransompediaの 2026 年対象期間内の日本関連掲載は 146 件である。2025 年の通年では 105 件だった。比較期間の長さは異なる。警察庁の 2026 年 1〜6 月のランサムウェア報告 123 件は、同じ警察報告対象群における 2025 年 1〜6 月の 116 件と比較できる。掲載と警察統計は報告対象群が異なり、合算や相互確認には使えない。[S2][S66][S254]

5. **DNSポリシーから分かるのは、限られた設定の観測結果である。** 評価対象 250 ドメインのうち 101、40.4%がDMARCのquarantineまたはrejectを指定していた。残る 149 は監視用ポリシーか、ポリシーが観測されなかった対象である。選定対象は全国を代表しない。[S4][S3]

**6. 現在の認証情報販売掲載には、自組織のアカウント検証が必要である。** 選定組織 250 件のうち 85 件に、確認時点で認証情報の販売掲載があった。全国Atlas代表値は 51/100 (B)である。端末との関連は少なくとも 247,993 件、過去の認証情報レコードとの関連は 17,488,907 件ある。重複する観測であり、現在の侵入や全国の割合を示さない。[S3]

## 経営層が行う 4 つの判断

1. **接続先を含めて認証情報の証拠を検証する。** 関連するアラートをアカウント責任者へ送り、権限とセッションを確認し、必要な無効化が各サービスで反映されたことを確かめる（§3、§7、§12）。
2. **委託先と重要サービスの継続を実証する。** 製品、テナント、業務依存を特定し、事業者が停止している間の最小限の運用手段を試す（§5–6、§9）。
3. **現在の目的がないデータとアクセスを除去する。** テスト環境、移行時のコピー、本人確認画像、契約終了後の連携を見直す。残す情報の法的・業務上の根拠を記録する（§2、§8、§10）。
4. **調査の完了前に報告できるよう備える。** 部署をまたぐ認知時点を記録し、現行の様式を使い、サービス、情報、顧客保護の判断を整合させる（§10、§12）。

## 主な数値

### 1,073,099

出典で日本関連のラベルが付いた投稿

**示さないもの**

確認済みの標的化、攻撃、重複のない人数

### 146

2026 年の対象期間に日本関連として掲載されたランサムウェアの主張

**示さないもの**

確認済み侵入や重複のない被害者数

### 105

2025 年通年の日本関連掲載

**示さないもの**

同じ長さの比較期間

### 43

日本関連の掲載で使われたグループ名

**示さないもの**

実行者の人数や国籍

### 55 / 146

The Gentlemen、Qilin、Everestの名称による掲載

**示さないもの**

共通組織や共通の攻撃経路

### 73 / 122 / 110 / 169

韓国、台湾、シンガポール、オーストラリアの対象期間内掲載

**示さないもの**

人口差などを調整した国別リスク

## 123 / 116

警察庁の 2026 年 1〜6 月と 2025 年 1〜6 月のランサムウェア報告

**示さないもの**

対象期間全体の報告や全国の完全な集計

## 51/100 (B)

選定対象群の全国Atlas代表値

**示さないもの**

侵入の割合や業種の順位

## 85 / 250

確認時点で認証情報の販売掲載があった組織

**示さないもの**

有効な認証情報、販売の成立、確認済み侵入

## 250

主なドメインで表す選定組織の項目数

**示さないもの**

独立した企業グループ数や全国の割合

## 101 / 250

DMARCの強制処理を求める評価対象ドメイン

**示さないもの**

フィッシング防止の実効性や受信側の遵守

## 26 + 11

事例カードと追加の詳しい公表事例

**示さないもの**

独立した侵入の合計件数

比較対象国は、背景を示すための例としてのみ選定したものであり、順位付けや政治的評価を意味するものではありません。

公開する証拠には、未検証の地下市場の主張を扱う 6 事例と、公表資料に基づく 31 件の詳しい事例が含まれる。キャンペーンの調査や影響範囲の更新を扱うものもあり、すべてが新規侵入ではない。第 5.5 節には、時系列順の短い事例を 137 件掲載する。どちらの掲載件数も、独立した事案の件数を示すものではない。公表日や更新日は、必ずしも攻撃日ではない。

要点

**01**

管理する認証情報とサービスを検証してから封じ込めを選ぶ。

**02**

委託先の代替手段を試し、不要な過去情報を見直す。

**03**

犯罪者の主張、公的な公表、報告の対象群を分ける。

# 本報告の構成

12 章で証拠と判断をつなぐ。担当する責任に合う経路を選び、各知見の制約を保って読む。

| | | |
|---|---|---|
| **経営層** | 継続性、保管、復旧への投資 | 移動先 1 5 11 12 |
| **CISO・対応責任者** | アラートの範囲と責任分担 | 移動先 3 4 7 12 |
| **SOC・認証管理** | アクセス、セッション、不審な配布経路の検証 | 移動先 4 7 8 9 |
| **運用・委託先管理** | 重要サービスと安全な設備運用の維持 | 移動先 2 5 6 12 |
| **法務・個人情報・不正対策** | 影響情報と報告義務の評価 | 移動先 5 8 9 10 |

**01要旨**
今すぐ何を行う根拠があるか

**02日本の事業環境**
サービス、情報、物理プロセスに異なる証拠が必要な理由

**03国全体の露出状況と選定組織群**
利用できるドメイン観測と、裏付けのない結論

**04地下フォーラムの活動と投稿から分かること**
購入希望、保有の主張、再流通の違い

**05公表された事案と分野別の対応**
公表と更新が対応をどう変えるか

**06可用性と接続機器のリスク**
ウェブ停止が運用システムへのアクセスを意味しない理由

**07脅威アクター、攻撃活動、裏付けのある関係**
各名称、キャンペーン、関係線の根拠

**08詐欺が狙う業務手順と委任されたアクセス**
支払権限、遠隔操作、アプリ権限の悪用

**09銀行と金融サービスの依存関係**
取引、情報、サービスの論点の分け方

**10規制対応と報告**
報告の範囲、認知、日付と判断の関係

**11見通しと条件付きシナリオ**
想定シナリオを開始・変更する兆候

**12行動計画**
責任者が何を実証するか

章 02

# 日本の事業環境

02

この章で答える問い

日本のデジタル経済のどの特徴が、インシデント時の判断を左右するか？

## 3

事業継続に関する確認事項：認証情報、サプライヤー、物理的な運用


2.1 相互依存を前提に運用する 11

2.2 証拠に関する三つの確認事項 11

2.3 制度の変更は日付を正確に扱う 12

2.4 地域の表示だけでは帰属は分からない 12

2.5 情報の保存もセキュリティの一部 12

章 02

# 日本の事業環境

概要

日本でのインシデント対応は、顧客認証、外部で運用する業務システム、物流、研究環境へのアクセスなど、相互につながるサービスに左右される。サプライヤーの障害でサービスが停止しても、すべての顧客への侵入が確認されたことにはならない。盗まれたアカウントから情報が露出しても、物理的なプロセスへのアクセスが立証されたわけではない。規制上の報告と顧客保護も、別々に判断する必要がある。依存関係を把握し、代替の業務経路を定め、各確認事項の責任者を決める。

## 2.1 相互依存を前提に運用する

対応の実務上の単位は、複数の組織が利用する共通サービスとなることが多い。第 5 章の公表事例には、ホスティング、顧客対応、モビリティ、研究向けのサービスが含まれる。同じ上流の事象でも、利用者への影響は異なる。サービスが利用できなくなる顧客もいれば、認証情報の更新や個人データへの影響評価が必要な顧客もいる。これらの結果は分けて記録する。

調達時にも、この区別が重要になる。稼働率を約束する契約だけでは、誰がインシデントのログを提供し、特権を持つシステム連携を解除し、アクセスされた情報を顧客に説明できるかは分からない。サプライヤーで事象が起きる前に確認する。調査の途中でも事業継続の判断を下せるよう、社内のサービス責任者を決めておく。

依存関係の台帳には、業務機能、サプライヤーのアクセス権、共有する情報、代替手段を記載する。目的は、障害時の判断を支えることにある。サプライヤー名を多数並べても、こうした関係がなければ、受注、決済、一般からの問い合わせを継続できるかは分からない。

## 2.2 証拠に関する三つの確認事項

公表通知や犯罪者の主張を対応チームが受け取ったときは、次の点を確認する。

| 確認事項 | 確保する証拠 | 担当責任者 |
| --- | --- | --- |
| サービスは利用可能か？ | 利用者の取引記録、サービスの状態、検証済みの代替手段 | 業務運用 |
| 情報へのアクセスや開示があったか？ | 関連するアカウント、アプリケーション、データ出力の記録 | インシデント対応とデータ管理責任者 |
| 物理的なプロセスに変化があったか？ | 運転員の計測値、変更履歴、技術担当者の評価 | 設備運用と安全管理 |

ある確認事項の答えを、別の答えの代わりにはできない。公開ウェブサイトの停止は、OTへのアクセスを立証しない。ログインの成功も、すべての記録へのアクセスを意味しない。調査でデータの持ち出しが確認されていないことは、持ち出しが不可能だったという証明にはならない。

事例カードも、この区別に従う。各カードでは、組織の発表、未解明の点、証拠に基づく初動を分ける。公表日は、情報が公開された日を示す。活動が始まった日を自動的に示すものではない。

## 2.3 制度の変更は日付を正確に扱う

国家サイバー統括室（NCO）は、本報告書で国の調整機能と分野横断の注意喚起に用いる現行の公式情報源である。過去の資料には、NISCの名称が残っていることがある。現在の組織名に置き換えても、過去の注意喚起が新しいインシデントになるわけではない。

内閣府の公式説明では、サイバー対処能力強化に関する法律のうち、官民連携とアクセス・無害化に関する特定の規定が 2026 年 10 月 1 日に施行されたとしている。これは一部の規定の施行に関する説明である。法律の成立日や、すべての規定の施行日としては扱わない。[S88]

企業が行うべきことは、報告先と連携先の一覧を最新に保つことである。適用される監督機関、インシデント対応窓口、警察への連絡経路、個人情報保護の所管機関を特定する。新しい様式や調整の仕組みは対応計画に反映する。ただし、他の義務に置き換わるとは想定しない。

## 2.4 地域の表示だけでは帰属は分からない

本報告書は、領土問題、歴史上の論争、選挙、政府の決定について立場を取らない。投稿、アカウント、掲載情報に付された国名は、運用者の国籍や国家の関与を立証しない。キャンペーン名は、情報源が活動を識別するために用いる名称である。

国家との関連に関する評価は、引用元による帰属評価としてのみ示し、その範囲と不確実性を保つ。使用言語、政治的な標語、公開標的が共通していても、運用者が同一とは限らない。防御側の対応は、報告された手法と自組織の証拠に基づく。

地域比較には、産業、金融、物流、サービス上の依存関係がある韓国、台湾、シンガポール、オーストラリアを、四つの比較対象として用いる。掲載件数が示すのは、観測された掲載情報の集団である。国の防御能力、政治的地位、個別の組織が攻撃される可能性を順位付けするものではない。

比較対象国は、背景を示すための例としてのみ選定したものであり、順位付けや政治的評価を意味するものではありません。

## 2.5 情報の保存もセキュリティの一部

PPCが 11 月に公表したレンタルサービスの本人確認画像に関する注意喚起は、データの最小化とインシデント被害の関係を示す。確認目的を果たした後も画像を保存すれば、後から漏えいする可能性が残る。法律で必要な記録と、便宜のための画像コピーは別である。[S71]

データ管理責任者は、サービス提供に必要な情報、法律上必要な情報、現在の目的がないまま保存する情報を区別する。区分ごとに保存方針を決める。適用される証拠保全などの義務を踏まえ、本番環境とサプライヤー側のコピーの両方で削除を検証する。

同じ考え方は、終了した顧客契約、古いシステム連携キー、退職者のアカウントにも当てはまる。現在の業務上の価値が小さくても、別のシステムを露出させる力が残っている場合がある。契約終了を削除の証拠とせず、アクセス権と保存の見直しに含める。

要点

01

サプライヤーを、その管理下にあるサービス、情報、権限と対応付ける。

02

サービスの可用性、情報へのアクセス、物理的なプロセスの証拠を分ける。

03

過去の記録と終了済み契約のアクセス権を見直し、新たな対応課題になる前に整理する。

章 03

# 国全体の露出状況と選定組織群

この章で答える問い

組織の標本から何が分かり、どの露出に関する判断には自組織の証拠が必要か？

**85 / 250**

確認時点で認証情報の販売掲載があった選定組織


3.1 対象集団 15
3.2 業種別の露出の兆候 16
3.3 端末と認証情報の対象群 17
3.4 現在の認証情報の販売投稿 20
3.5 公開メールとウェブの観測 20
3.6 全国代表値と判断の境界 21

章 03

# 国全体の露出状況と選定組織群

概要

選定組織 250 件のうち 85 件で、確認時点に認証情報の販売掲載があった。この対象群の全国Atlas代表値は 51/100 (B)である。端末との関連は少なくとも 247,993 件、過去の認証情報レコードとの関連は 17,488,907 件ある。これらは重複する観測であり、現在の侵入や全国の割合を示さない。有効なアカウントを検証し、関係する従業員端末の証拠とメール認証を確認する。

## 3.1 対象集団

選定対象は、重要な組織を分析用にまとめたものである。日本の大企業を規模順に並べた公開ランキングではない。各項目を一つの主ドメインで表している。公共サービスの責任、または業種内での主要な役割を踏まえて選定している。[S3]

| 項目 | 対象範囲 |
| --- | --- |
| 対象集団 | 十業種から選定した主ドメイン 250 件 |
| 業種ごとの規模 | 各区分 25 件 |
| 選定 | 公的機関、金融機関、インフラ事業者、主要なサービス・産業・研究組織を目的に沿って選定 |
| 単位 | 主ドメインで表した、選定組織の一項目 |
| 露出の観測日 | 2026-11-22。選定した 250 ドメインを評価 |
| 時間の範囲 | 端末と認証情報は累積記録。現在の掲載は観測時点の状態 |
| 文脈の期間 | 言及：2025-11-23〜2026-11-22。類似ドメインの観測：2026-10-19〜2026-11-18 |
| 代表性 | この対象群から、国全体での露出の割合は推定しない |

ドメインは、分析上の参照点である。主ドメインだけでは、グループ内のすべての子会社、顧客向けサービス、ホストされたアプリケーション、独立した法人の範囲は分からない。企業再編、共有インフラ、別の顧客向けブランドにより、対応すべき範囲が変わる場合がある。

この標本は、公開された事故の一覧とも異なる。選定されていない組織が、公的な事故通知に登場する場合がある。選定組織について、関係する事故の公表がない場合もある。どちらも、侵入の有無を立証するものではない。

## 3.2 業種別の露出の兆候

**250 組織のうち 85 件に、確認時点で認証情報の販売掲載があった。** 端末との関連は 209 ドメイン、過去の認証情報レコードは 241 ドメインで観測された。これらの対象群には重複がある。[S3]

各業種の選定対象は 25 件である。表は観測された兆候の件数と分母を示す。現在の掲載は広告であり、販売の成立、有効な認証情報、確認済み侵入を意味しない。

### 選定した 250 組織のうち 85 件に認証情報の販売掲載がある

| | 現在の販売掲載 | 端末との関連 | 従業員端末 | 認証情報 | 文書との関連 |
|---|---|---|---|---|---|
| 行政 | 13/25 | 21/25 | 16/25 | 24/25 | 14/25 |
| 銀行 | 12/25 | 22/25 | 10/25 | 25/25 | 13/25 |
| 保険・資本市場 | 6/25 | 24/25 | 14/25 | 23/25 | 17/25 |
| 大学・研究 | 14/25 | 25/25 | 22/25 | 25/25 | 14/25 |
| 医療・ライフサイエンス | 2/25 | 14/25 | 9/25 | 25/25 | 16/25 |
| 工業・製造 | 4/25 | 22/25 | 17/25 | 25/25 | 17/25 |
| 技術・通信 | 17/25 | 24/25 | 21/25 | 24/25 | 23/25 |
| エネルギー・公益 | 4/25 | 20/25 | 12/25 | 25/25 | 17/25 |
| 運輸・物流 | 8/25 | 22/25 | 12/25 | 23/25 | 11/25 |
| 小売・サービス | 5/25 | 15/25 | 11/25 | 22/25 | 12/25 |

業種別の現在の認証情報販売掲載（コーラル色）。各セルは兆候のある組織数／選定組織数。区分は重複する。 出典：選定した日本の組織の露出観測、2026年11月22日。[S3] 選定対象は250組織。関連は重複し、過去の情報を含む場合がある。現在の侵入や全国の割合を示さない。

| 業種 | ドメイン | 現在の掲載 | 掲載履歴（期間不明） | 従業員端末の兆候 | 文書の兆候 |
|---|---|---|---|---|---|
| 行政 | 25 | 13 | 13 | 16 | 14 |
| 銀行 | 25 | 12 | 12 | 10 | 13 |
| 保険・資本市場 | 25 | 6 | 6 | 14 | 17 |
| 大学・研究 | 25 | 14 | 14 | 22 | 14 |
| 医療・ライフサイエンス | 25 | 2 | 2 | 9 | 16 |
| 工業・製造 | 25 | 4 | 4 | 17 | 17 |

| 業種 | ドメイン | 現在の掲載 | 掲載履歴（期間不明） | 従業員端末の兆候 | 文書の兆候 |
|---|---|---|---|---|---|
| 技術・通信 | 25 | 17 | 16 | 21 | 23 |
| エネルギー・公益事業 | 25 | 4 | 4 | 12 | 17 |
| 交通・物流 | 25 | 8 | 8 | 12 | 11 |
| 小売・サービス | 25 | 5 | 5 | 11 | 12 |
| 合計 | 250 | 85 | 84 | 144 | 154 |

84 ドメインに関する掲載履歴の指標は、対象期間と現在の掲載との重複範囲が明示されていない。全期間を通じた総数や、現在の掲載を除いた件数としては解釈できない。二つの数値から、時間の経過に伴う増減は判断できない。[S3]

従業員端末との関連は 144 ドメイン、文書との関連は 154 に認められる。文書は公開資料、重複資料、事故と無関係な資料の場合がある。内容と想定読者を検証する。[S3]

2026-10-19〜2026-11-18 の類似ドメインの観測は、選定した 223 ドメインに関係する。年間のチャット言及は 46、ウェブ言及は 37 ドメインにある。類似や議論だけでは、なりすましや不正アクセスは確認できない。所有関係と実際の利用を検証する。[S3]

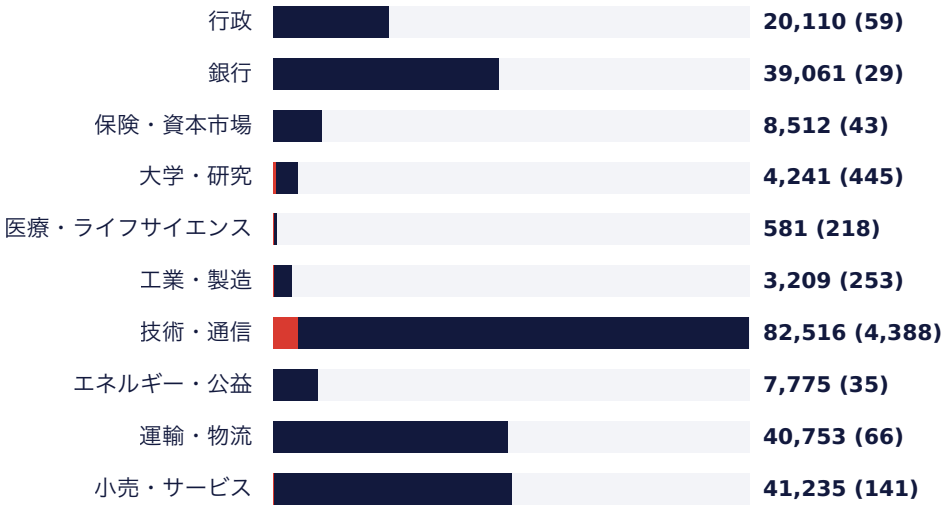
## 3.3 端末と認証情報の対象群

選定対象群には、少なくとも 247,993 件の端末との関連があり、うち 5,677 件は従業員端末との関連である。過去の認証情報レコードとの関連は 17,488,907 件、文書との関連は 1,025 件ある。対象群は異なり、ドメイン間で重複する場合もある。[S3]

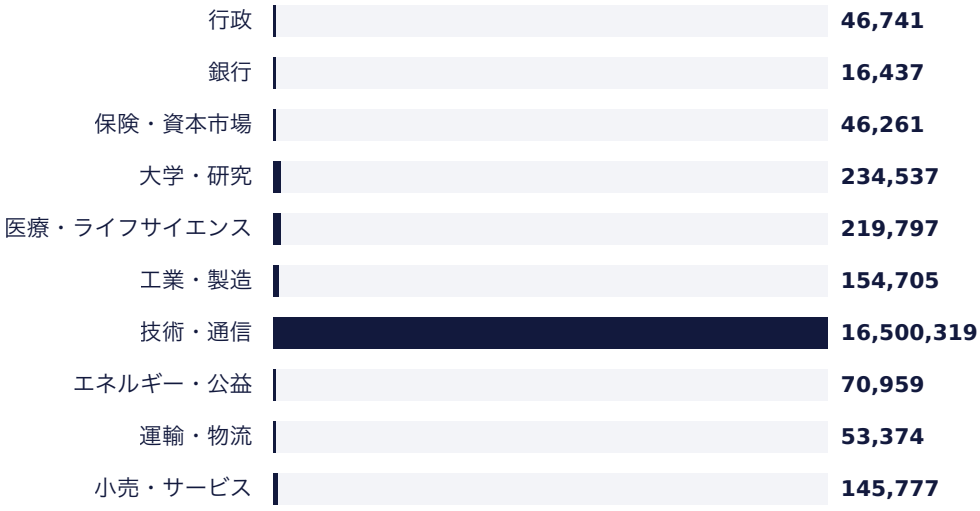
### 技術・通信の端末および認証情報との関連総数が最も多い

■従業員端末　■その他の端末・レコードとの関連

端末との関連総数、少なくとも（括弧内は従業員端末）




過去の認証情報レコードとの関連（別の目盛り）




出典：選定した日本の組織の露出観測、2026年11月22日。[S3] 選定対象は250組織。関連は重複し、過去の情報を含む場合がある。現在の侵入や全国の割合を示さない。

| 業種 | 端末、少なくとも | 従業員端末 | 認証情報レコード | 文書 |
|---|---|---|---|---|
| 行政 | 20,110 | 59 | 46,741 | 187 |
| 銀行 | 39,061 | 29 | 16,437 | 44 |
| 保険・資本市場 | 8,512 | 43 | 46,261 | 38 |
| 大学・研究 | 4,241 | 445 | 234,537 | 33 |
| 医療・ライフサイエンス | 581 | 218 | 219,797 | 50 |
| 工業・製造 | 3,209 | 253 | 154,705 | 78 |
| 技術・通信 | 82,516 | 4,388 | 16,500,319 | 351 |

| 業種 | 端末、少なくとも | 従業員端末 | 認証情報レコード | 文書 |
|---|---|---|---|---|
| エネルギー・公益事業 | 7,775 | 35 | 70,959 | 40 |
| 交通・物流 | 40,753 | 66 | 53,374 | 31 |
| 小売・サービス | 41,235 | 141 | 145,777 | 173 |
| 合計 | 247,993 | 5,677 | 17,488,907 | 1,025 |

技術・通信は、認証情報レコードとの関連 16,500,319 件を占め、対象群全体の 94.3%に当たる。端末との関連は少なくとも 82,516 件である。この集中は観測記録の特徴であり、業種の侵入率ではない。[S3]

従業員端末との関連は端末全体の内数であり、加算しない。残る 242,316 件は従業員関連と表示されていないが、所有者が誰かは確定しない。

## 露出の兆候を正確に読む

組織単位の警告と集計の文脈には、以下の区別を添える必要がある。

| 兆候 | 裏付けられる内容 | まだ検証が必要な問い |
|---|---|---|
| 認証情報の販売投稿 | 観測した販売投稿が、認証情報をドメインに関連付けている | 自組織に有効なアカウントが存在し、何にアクセスできるか？ |
| 端末との関連 | 取得された情報が、端末をサービスやドメインに関連付けている | 端末の所有者は誰か、情報はいつ取得され、アクセスは今も使えるか？ |
| 過去の認証情報の記録 | 保存された過去の資料に、アカウントへの言及がある | 現在も有効か、使い回されているか、すでに対処済みか？ |
| 文書中の言及 | 文書が組織やドメインに言及している | 機微な内容か、本物か、意図して公開されているか？ |
| 類似ドメインの候補 | ドメインが保護対象のブランドに似ている | 関係するドメインか、正当なものか、だますために使われているか？ |
| 地下フォーラムでの言及 | 投稿が組織に言及している | 具体的な主張か、通常の議論か、繰り返しの広告か？ |

一人が複数のアカウントを持ち、複数の過去の資料に登場し、複数組織のサービスを使う場合がある。端末や認証情報との関連は、それらのサービスの間で重複する場合がある。合算しても、重複のない人数や影響組織数にはならない。

従業員に関連付けられた情報は、速やかに確認する必要がある。従業員アカウントと検証できれば、内部の権限を持っている場合があるためである。ラベルだけでは、管理対象の業務端末、現在の感染、雇用元の環境への侵入は確認できない。大学や共有サービスの組織では、アカウントの利用者が特に多様な場合がある。

## 3.4 現在の認証情報の販売投稿

現在の販売投稿は、関係するアカウントを調べる理由になる。売買の成立、認証情報の有効性、組織自身のシステムが流出元であることを示す証拠ではない。影響の大きな封じ込めを行う前に、所有者と対象範囲を確認すること。

正当な警告から具体的な自組織のIDが分かる場合は、そこから始める。アカウントの存在、最後の正当な利用、権限、過去のリセットや失効を確認すること。関係するセッション、アプリケーション、遠隔アクセスの動作を調べる。廃止済みのアカウントであっても、結果を記録すること。

有効な特権アカウント、不審なセッション、不正な操作を確認した場合は、対応の段階を引き上げること。封じ込めには、セッションの失効、連携用秘密情報の更新、アクセス経路の制限などがある。適切な措置は、検証できた証拠と業務への影響によって変わる。

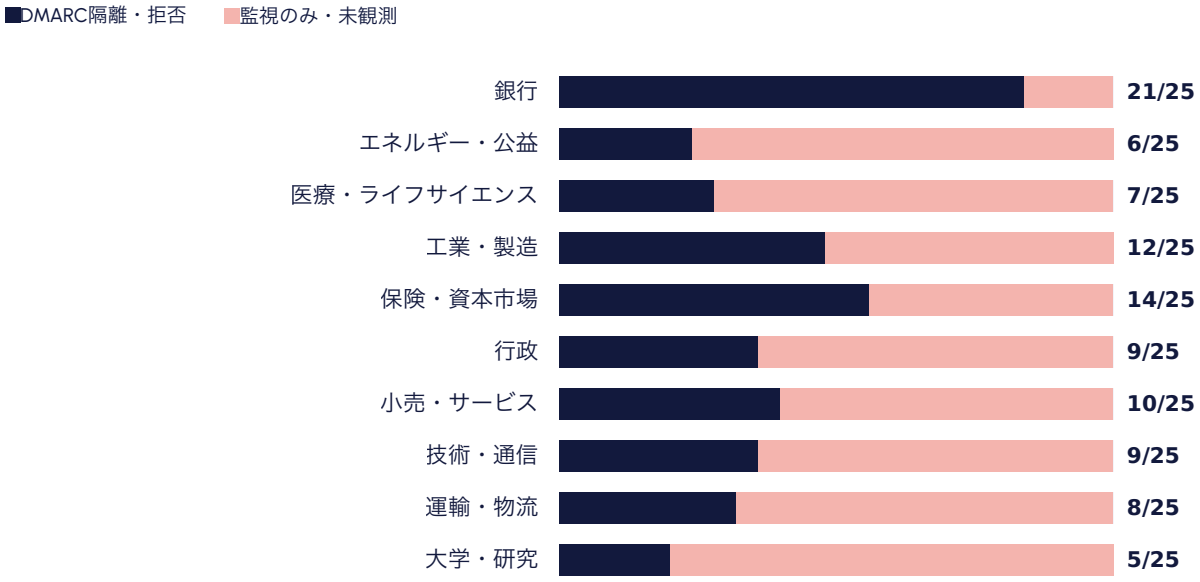
見える範囲に販売投稿がないことを理由に、別の調査を終えないこと。公開市場や監視対象の市場で分かるのは、活動の一部だけである。情報は非公開、誤ったラベル付き、過去のもの、または一度も広告されていない場合がある。

## 3.5 公開メールとウェブの観測

DNSだけのデータには、選定した 250 ドメインすべてについて、解釈可能な応答がある。101 件でDMARCのquarantineまたはrejectポリシーを記録しており、評価できた対象の 40.4%である。残る 149 件は、監視用のポリシー、またはポリシーが観測されなかったものである。[S4]

図c05 は、評価できたドメインを示す。フィッシングメールの到達や、詐欺の成功を測るものではない。

### 評価できた 250 ドメインのうち 101 件が、DMARCの隔離・拒否ポリシーを公開




出典：公開DNSポリシーの観測、評価対象250ドメイン、2026年11月22日。[S4] 公開されたポリシーは、受信側の遵守やフィッシング防止の実効性を証明しない。

| 業種 | 評価できたドメイン | quarantineまたはreject | 監視用または未観測 |
|---|---|---|---|
| 銀行 | 25 | 21 | 4 |
| エネルギー・公益事業 | 25 | 6 | 19 |
| 医療・ライフサイエンス | 25 | 7 | 18 |
| 工業・製造 | 25 | 12 | 13 |
| 保険・資本市場 | 25 | 14 | 11 |
| 行政 | 25 | 9 | 16 |
| 小売・サービス | 25 | 10 | 15 |
| 技術・通信 | 25 | 9 | 16 |
| 交通・物流 | 25 | 8 | 17 |
| 大学・研究 | 25 | 5 | 20 |
| 合計 | 250 | 101 | 149 |

評価できた対象全体では、rejectを求めるポリシーが 58 件、quarantineを求めるものが 43 件である。ほかに、監視用が 109 件、ポリシー未観測が 40 件ある。これはポリシーの観測結果であり、配信時の管理が有効に働いている証拠ではない。[S4]

本版には、TLS、ホームページのヘッダー、基本設定の状態をまとめた指数について、完全なデータがない。それらの割合や指数は推定していない。DNSの観測は、不足しているこれらの結果の代わりにはならない。

メールのポリシーは、認証結果を受信側にどのように扱ってほしいかを示す。すべての受信側が従うことや、すべての正当な送信元が正しく設定されていることを立証するものではない。適用方針を変える前に送信元の一覧を確認し、その後、正当なメールの配信を監視すること。

証明書やホームページの観測は、確認したサービスに対するものである。すべてのアプリケーションを説明するものでも、アプリケーションの安全な動作を保証するものでもない。観測できなかったものは不明のままである。安全な結果にも、確認済みの弱点にも数えるべきではない。

## 3.6 全国代表値と判断の境界

**全国Atlas代表値は 51/100 (B)である。** 優先順位を考えるための指標であり、侵入を受けた割合、今後の侵入確率、管理策の有効性の認証ではない。[S3]

公表する評価値は全国代表値のみである。業種表は匿名の兆候の件数を示し、業種別や組織別の評価値は示さない。評価は観測時点に対応する。累積した過去の記録が、すべて 2026 年に初めて現れたとは限らない。

過去の関連、現在の販売掲載、事案の対象期間を区別する。公式公表、犯罪者の広告、受動的な設定の観測は異なる問いに答える。過去の観測が残っていても、個別アカウントの対応完了には組織側の証拠が必要である。

実用的な判断は具体的である。外部の警告を、認証情報、アプリケーション、業務の責任者へつなぐ。検証結果、対象サービス、証拠を解消した対応を記録する。全国代表値は組織固有の検証に代わるものではない。

要点

**01**

250 件の選定対象は範囲を定めるもので、日本全体の割合を推定するものではない。

**02**

端末、認証情報、文書、言及の各対象集団は、別々に解釈する必要がある。

**03**

封じ込めを選ぶ前に、自組織のIDとアクセス経路を検証すること。

章 04

# 地下フォーラムの活動と投稿から分かること

この章で答える問い

どの販売投稿を調べるべきで、どの結論は証拠の範囲を超えるか？

6

詳細に扱う主張の事例。それぞれの証拠の範囲を区別


4.1 対象集団 24
4.2 保存した情報から見える範囲と制約 25
4.3 最近の活動：11 月 8〜22 日 27
4.4 詳細に扱う主張の事例 29
4.5 需要、古い情報、国際的な販売 35
4.6 価格、ファイル容量、アクター間の関係 37
4.7 警告からリスクに見合う措置へ 38

章 04

# 地下フォーラムの活動と投稿から分かること

概要

保存した地下フォーラムの投稿には、日本の情報への需要、具体的なデータの販売、銀行の未確認の脆弱性、再流通する情報が現れる。国全体の事故総数を示すものではない。最近の一つの販売投稿は不動産データをうたいながら、弁護士登録の項目を記している。別の国際的な旅行情報の販売では、日本の分量を示していない。保有と需要、現在のアクセスと宣伝上の能力、新しい投稿と過去の事故を分けること。自組織の情報とアクセスの記録に基づき、関係する警告を検証すること。

## 4.1 対象集団

資料の対象集団は、Odin by Brandefenseが保存した地下フォーラムの投稿である。主な対象期間は投稿時刻に基づき、2026 年 1 月 1 日〜11 月 22 日である。投稿日は、侵入日、入手日、実行日を意味しない。[S1]

| 項目 | 対象範囲 |
|---|---|
| 証拠 | 保存したフォーラム、メッセージサービス、関連する地下フォーラムの投稿 |
| 日本との関係 | 日本に関連する議論、販売、需要。一部の投稿は複数の地域に言及 |
| 時間 | 指定期間内の投稿時刻 |
| 国関連の件数 | 出典のラベル付き投稿 1,073,099 件。確認済みの標的化ではない |
| 保存した対象集団 | 報告書の本文で扱う、重複しない投稿 17,529 件 |
| 意味 | 観測したメッセージと主張。確認済みの事故や、重複のない被害者ではない |
| 制約 | 資料ごとの見え方に偏りがあり、非公開・未公表の活動は対象外 |

保存した対象集団は、日本に関する地下フォーラムの活動を全数調べたものではない。その量から、年間の攻撃発生率は分からない。広告の繰り返し、国際的な販売、通常の議論によって、日本への新たな侵入がなくても多数のメッセージが生じる。

公開用の事例カードには、実際の短い引用を残し、何が未解決かを記している。機微な識別情報と連絡先は非公開である。ファイル容量、行数、価格、アクセスに関する主張は、別に確認できない限り、投稿者の主張として扱う。

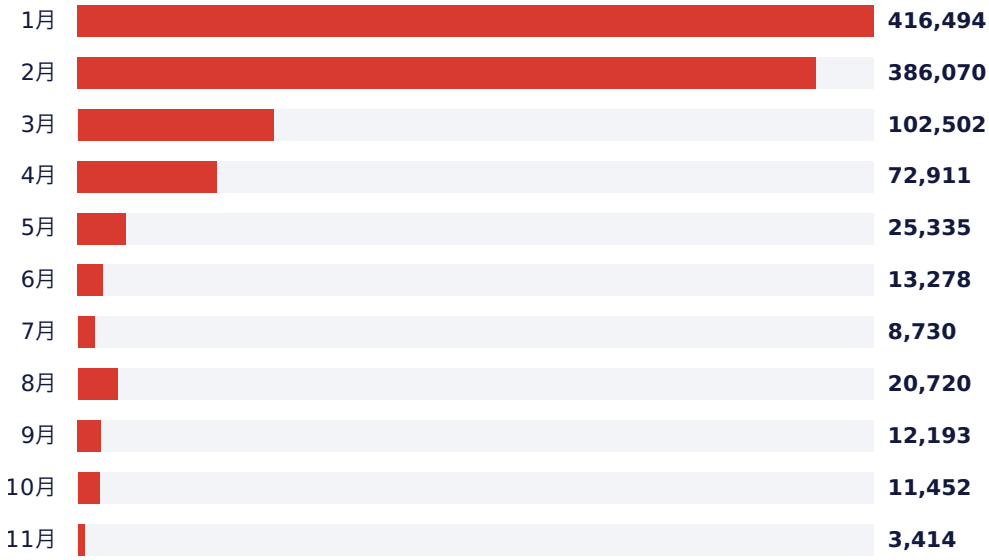
## 4.2 保存した情報から見える範囲と制約

この観測には　17,529　件の投稿が含まれる。これは保有する対象群の件数であり、日本全国の年間総数ではない。[S1]

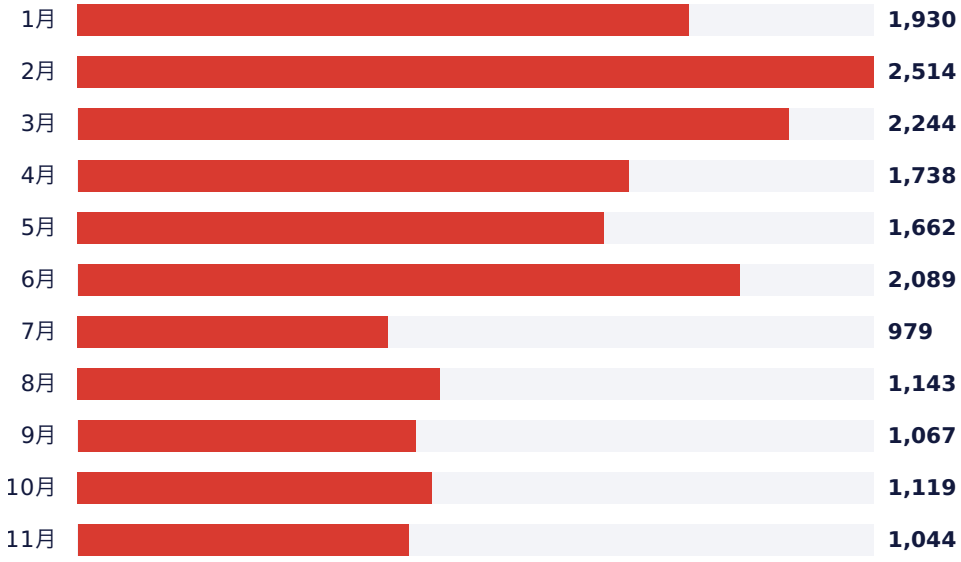
出典の日本関連ラベル付き投稿は 1,073,099 件である。国関連の集計と、内容を扱う保有投稿群は異なる観測範囲である。一方を他方の完全な部分集合とはみなさない。1 投稿が複数の地域を扱う場合もある。[S1]

### 国関連の投稿量は時期によって異なり、攻撃頻度の系列ではない

国関連のラベル付き投稿




保存した投稿の観測（別の目盛り）




出典：Odin by Brandefense、日本関連の投稿観測、2026年1月1日〜11月22日（終日は途中まで）。国関連のラベル付き投稿と保存した投稿は別の対象集団であり、攻撃件数ではない。[S1]

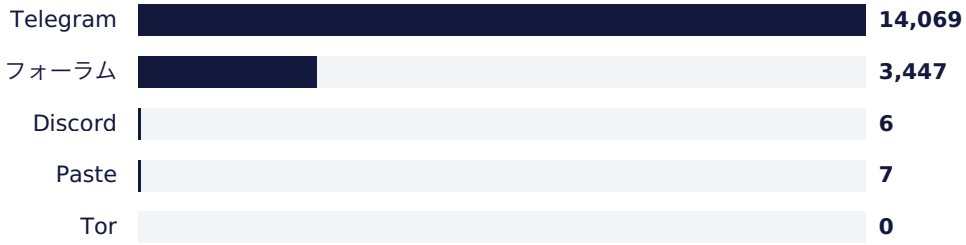
図c01 は国関連ラベル付きの月別件数を示す。以下の配信先と言語の表は、保有する投稿群を対象とする。投稿量の変化から、全国の脅威の増減は推定しない。

| 種類 | 投稿数 | 全保有投稿に占める割合 |
|---|---|---|
| telegram | 14,069 | 80.3% |
| forum | 3,447 | 19.7% |
| paste | 7 | 0.0% |
| discord | 6 | 0.0% |

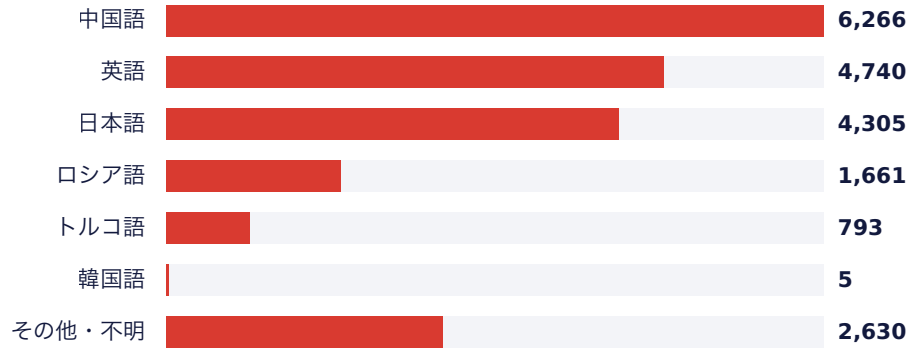
次の表は、明確な言語名を持つカテゴリーと、その他・不明のラベルを示す。後者には不明、地理的なラベル、解釈が確定しないラベルが含まれる。件数はラベルの出現件数であり、その他・不明の欄は一意の投稿数を示さない。割合の分母は保有投稿 17,529 件で、ラベルは重複し得る。[S1]

## 言語と配信先の違いは、実行者の国籍や事案数を示さない

保存した投稿の配信先




言語の関連（重複する場合がある・別の目盛り）




出典：Odin by Brandefense、日本関連の投稿観測、2026年1月1日〜11月22日（終日は途中まで）。国関連のラベル付き投稿と保存した投稿は別の対象集団であり、攻撃件数ではない。[S1]

| 言語カテゴリー | ラベル出現件数 | 全保有投稿に対する割合 |
|---|---|---|
| 中国語 | 6,266 | 35.7% |
| 英語 | 4,740 | 27.0% |
| 日本語 | 4,305 | 24.6% |

| 言語カテゴリー | ラベル出現件数 | 全保有投稿に対する割合 |
|---|---|---|
| ロシア語 | 1,661 | 9.5% |
| トルコ語 | 793 | 4.5% |
| 韓国語 | 5 | 0.0% |
| その他・不明のラベル | 2,630 | 15.0% |

投稿の言語から、アクターの国籍を推定しないこと。日本語の項目一覧は、データからコピーされた可能性がある。中国語や英語の広告が、多くの市場の一つとして日本を扱う場合もある。言語は保存したメッセージの特徴であり、投稿者や想定する買い手を特定するものではない。

掲載場所についても、同じ注意が必要である。フォーラムには、具体的なデータの販売、古いアップロードの再投稿依頼、世界各地の販売一覧が混在する。対応を決めるのは、主張とそれを支える証拠である。プラットフォームの名前だけでは判断できない。

## 4.3 最近の活動：11 月 8〜22 日

以下の締切間際の例は、異なる二つの内容を示している。11 月 18 日には、買い手が情報を求めている。11 月 16 日には、売り手が業種の説明に不整合のあるデータを販売している。どちらの投稿も、日本の組織が新たに被害を受けたことを立証しない。[S1]

| 日付 | 観測した主張 | 証拠の範囲 | カード |
|---|---|---|---|
| 2026-11-18 | 日本を含む、価値の高い政府・技術分野の情報を求める投稿 | 需要は、保有や引き渡しを立証しない | B01 |
| 2026-11-16 | 不動産の説明と弁護士関係の項目定義を伴う、48,000 件の記録の販売 | 真正性、由来、業種の特定さえ未解決 | B02 |
| 2026-11-15 | 旅行系ポイントプログラムを名目に、48,000,000 件を 550 ドル（投稿表記）で販売する投稿 | 主張された行数、所有者、真正性、現在のアクセスは未検証 | B12 |
| 2026-11-14 | 交通を題材に、約 19,210,000 件を 400 ドル（投稿表記）で販売する投稿 | 宣伝上の総数は、日本の影響人数として検証された値ではない | B11 |

具体的な不整合は、宣伝上の量より重要である。ラベルが間違っていても、それだけで販売内容全体が捏造だとは分からない。同様に、詳しい項目定義だけでは、ファイルが本物だと確認できない。対応チームは矛盾を記録し、影響するサービスを名指しする前に、自組織の証拠を確認する必要がある。

証拠カード B01 2026年11月18日

[別名非公開] フォーラム フォーラム 英語

原文
I am looking to obtain high-value intelligence and data

翻訳
価値の高い情報やデータの入手を求めている。

**注記.** 日本は、求める情報の対象国の一つである。データの保有主張ではなく、需要を示す投稿である。

**確認事項**
投稿者は、政府、軍事、半導体などの価値が高い資料を求めている。日本は、対象とする複数の国の一つである。

**未確認事項**
これは入手の募集である。情報の保有、販売者との関係、受け渡し、日本での侵害は示されていない。

証拠カード B02 2026年11月16日

[別名非公開] フォーラム フォーラム 日本語

原文
弁護士登録番号 氏名 氏名カナ 氏名ローマ字 生年月日

翻訳
弁護士登録番号、氏名、氏名カナ、氏名ローマ字、生年月日。

**注記.** 説明と項目一覧の矛盾が所見であり、不動産分野の事案は確認されていない。

**確認事項**
11月16日の販売投稿は、不動産関連との説明で48,000件を宣伝している。一方、日本語の項目一覧には、弁護士登録、弁護士会への所属、法律事務所に関する項目が並ぶ。

**未確認事項**
この投稿の記録からは、ファイル、行数、出所、情報の新しさ、不動産分野という説明の正しさは確認できない。

証拠カード B11 2026年11月14日

[別名非公開] フォーラム フォーラム 英語

原文
records: 19.21M

翻訳
レコード数は1,921万と記載。

**注記.** 11月16日の48,000件の販売投稿とは別である。件数は広告上の数字であり、独立して確認されていない。

**確認事項**
投稿者は、日本の交通事業者に由来すると称するデータセットを、19,210,000件、広告価格$400で宣伝している。

**未確認事項**
ファイルの真正性、重複のない人数、元の侵害日、販売の成立、継続的なアクセスは確認されていない。元のサンプルにある身元情報と値は非公開としている。

証拠カード B12 2026年11月15日

[別名非公開] フォーラム フォーラム 英語

原文
Records - 48M

翻訳
レコード数は4,800万と記載。

**注記.** 11月16日の48,000件の販売投稿とは別である。件数は広告上の数字であり、独立して確認されていない。

**確認事項**
投稿者は、日本の旅行系ポイントプログラムに由来すると称するデータセットを、48,000,000件、広告価格$550で宣伝している。

**未確認事項**
ファイルの真正性、重複のない人数、元の侵害日、販売の成立、継続的なアクセスは確認されていない。元のサンプルにある身元情報と値は非公開としている。

交通を題材にした二つの販売投稿は、顧客保護に関する問いも生じさせる。自組織に関係する情報との一致を裏付けられた場合は、実際の情報に見える内容を使ったなりすましに備え、予約、会員制度、アカウント復旧の手順を確認すること。広告だけでは、国全体の影響人数を示す根拠にならない。

第 5 章では、11 月の公式な公表を別に扱う。投稿と公表の時期が近いだけでは、同じ情報を扱っているとは判断できない。これらの例と公式公表の間に、一致するファイル、アカウント、独立に裏付けられた関係は確認されていない。

## 4.4 詳細に扱う主張の事例

各事例では、観測した主張、時系列、分かること、別の可能性、リスクに見合う対応を区別している。確認済みの侵入として示すものはない。警察への報告、ランサムウェアの掲載、公開された事故の対象集団に、これらの事例を加算していない。

A

事例 A

### 題名と項目定義が異なる業種を示す

証拠カード B02 | 2026年11月16日 | フォーラム | 業種不確定／専門サービス

主張は未確認

| | |
|---|---|
| **主張** | 11 月 16 日のフォーラムの販売投稿は、不動産に関する説明で 48,000 件の記録を宣伝している。一方、日本語の項目定義には、弁護士登録、弁護士会への所属、法律事務所に関する項目がある。 |
| **時系列** | 日付は、保存した資料にこの販売投稿が現れた時点を示す。情報の収集時期や、別の場所に以前の販売投稿があったかは分からない。 |
| **分かること** | 投稿の説明と記載された項目には、内部的な不整合がある。これは、データの正体が不確かであることを裏付ける。不動産業種での事故が確認されたことにはならない。 |
| **別の可能性** | 誤ったラベル、広告の使い回し、複数情報の混在、本物のファイルに対する不正確な説明などが考えられる。投稿は、どれに当たるかを解決していない。 |
| **制約** | ファイルの真正性、主張された行数、由来、新しさは未検証である。登録に関する項目は、正当な名簿ですでに公開されている情報を指す場合もある。 |
| **対応** | 関係するデータの責任者は、記載された項目を、承認済みの出力情報や公開情報と照合すること。封じ込めや事故の通知を選ぶ前に、自組織の情報との信頼できる一致を調べる必要がある。 |

**結論**

対象サービスを特定する前に、示された項目定義を、許可された出力や公開情報と照合する。

事例 B

B

## 段階的な公開をうたう説明で圧力をかけ、件数も不確か

証拠カード B03 | 2026年11月6日 | フォーラム | サービス事業者

主張は未確認

| | |
|---|---|
| **主張** | 11 月 6 日の投稿は、公開サイトと、専門職 50 人に関する第一弾の情報の準備ができたと述べている。さらに専門職と顧客の情報を出すと予告している。 |
| **時系列** | 投稿文は、自らの説明の中で以前の報告に言及している。その言及は、以前の情報、侵入の順序、公開の完了を示す独立した証拠ではない。 |
| **分かること** | あるアカウントが、恐喝のような情報公開の主張を行った。投稿だけでは、保有、対象となる人、公開の完了、支払を立証できない。 |
| **別の可能性** | 本物の情報、コピーされた情報、繰り返される圧力、裏付けのない要求の可能性がある。過去の報告への言及では、どれが正しいか分からない。 |
| **制約** | 範囲、入手経路、元の本人の識別情報は、独立に確認されていない。すべての利用者を対象とするという説明も、投稿者の主張である。 |
| **対応** | サービス責任者は、関係する警告を保全し、正当な情報との一致を検証し、顧客保護の計画を調整すること。対外説明では、要求と確認できた事実を区別する必要がある。 |

**結論**

関連する警告を保存し、自社情報との一致を確認したうえで、確認済みの事実に基づき顧客保護を調整する。

証拠カード B03 2026年11月6日

[別名非公開] フォーラム フォーラム 英語

原文

full disclosure of all users since September 2026 is ready

翻訳

2026年9月以降の全利用者データを全面公開する準備ができている。

**注記.** 未確認の恐喝に関する説明であり、独立して確認された侵害ではない。

**確認事項**

投稿者は、新たな公開サイト、業務従事者50人を対象とする初回の公開、その後の業務従事者と顧客の記録の公開を主張している。

**未確認事項**

投稿者の保有、件数、公開の完了、対象者の身元、侵害の手段は、独立して確認されていない。和解金の要求は、支払いがあった証拠ではない。

事例 C

## C ■ 脆弱性の販売はアクセスの販売とは異なる

証拠カード B04 2026年3月2日 フォーラム 銀行

主張は未確認

| | |
|---|---|
| **主張** | 3 月 2 日のフォーラムの投稿は、日本の銀行に影響する、内容不明の脆弱性を 5,000 USDで販売している。文面によると、買い手がそれを悪用する必要がある。 |
| **時系列** | 観測した事象は、その日の広告である。保存した主張には、発見日、影響するソフトのバージョン、過去の悪用履歴は記載されていない。 |
| **分かること** | アカウントは、あるとする能力を宣伝した。その文面は、有効なアカウントの保有、システムの制御、主張する問題の悪用済みという事実を立証しない。 |
| **別の可能性** | 実在する脆弱性、誇張された弱点、コピーした販売投稿、捏造した能力の可能性が残る。価格は技術的な主張の真正性を示さない。 |
| **制約** | 技術的な証明、影響が確認された製品、銀行への侵入は、いずれも確認されていない。対象の財務状況に関する売り手の説明も未検証である。 |
| **対応** | 関係する正当な警告を受けた銀行は、アプリケーションのセキュリティ責任者へ連絡すること。重大度の判断や影響の大きな措置の前に、自組織の証拠を確認し、許可された範囲で検証すること。 |

**結論**

関連する警告をアプリケーションセキュリティ担当へ回し、主張された弱点を許可された範囲で検証する。

証拠カード B04 2026年3月2日

[別名非公開] フォーラム フォーラム 英語

原文

Selling a critical vulnerability on a bank from Japan

翻訳

日本の銀行に関する重大な脆弱性を販売する。

**注記.** 能力があると称する販売投稿であり、アクセスの保有や銀行の侵害は確認されていない。

**確認事項**

投稿は、特定されていない銀行の脆弱性を広告価格$5,000で販売するとし、購入者自身が悪用する必要があると述べている。

**未確認事項**

技術的な証拠、対象製品、アクセス、悪用、銀行の侵害は示されていない。投稿が述べる銀行の利益も、独立して確認されていない。

D

事例 D

## 登録記録は信じやすいなりすましに使われ得る

証拠カード B05 2026年2月3日 フォーラム 余暇・イベント

主張は未確認

| | |
|---|---|
| **主張** | 2 月 3 日の販売投稿は、スポーツ大会の登録・出席記録 457,000 件を宣伝している。記載された項目には、大会識別子、氏名、連絡先、生年月日、参加状況が含まれる。 |
| **時系列** | 投稿日は、報告書の対象期間に広告されたことを示す。登録システムへの現在の侵入や、記録の対象期間は分からない。 |
| **分かること** | 宣伝された項目の組み合わせは、あり得る大会登録の手順を表している。内容の真正性や、各行が別々の人を表すことを立証しない。 |
| **別の可能性** | 本物の出力情報、古い登録情報、集約した情報、誤解を招く販売投稿でも、同じ説明が可能である。詳しい項目一覧では、由来を確定できない。 |
| **制約** | 情報全体、売り手の入手への関与、主張された件数、新しさは未検証である。本章では、影響する組織を名指ししていない。 |
| **対応** | 大会やサービスの責任者は、自組織の情報との信頼できる一致について、出力記録と委託先のアクセスを確認すること。漏えいが裏付けられた場合は、実際の大会や出席情報を引用するなりすましを想定すること。 |

**結論**

主張された登録情報が裏付けられる場合は、自社の出力記録と委託先のアクセスを点検する。

証拠カード B05 2026年2月3日

[別名非公開] フォーラム フォーラム 英語

原文

Data contents: id, registration_date, event_id, event_name, user_id, first_name, last_name, email, phone, birthday, gender, postal_code, address, entry_category, status, attendance_flag.

翻訳

データ項目：レコード・イベントの識別子、氏名、メール、電話、生年月日、性別、住所、申込状況、出席フラグ。

**注記.** 具体的なデータ販売の主張である。示された項目と主張された行数を記載し、検証済みの影響件数には置き換えない。

**確認事項**

販売者は、日本の連絡先を含む16項目を示し、スポーツイベントの登録・出席記録457,000件を宣伝している。

**未確認事項**

内容の真正性は確認されていない。重複のない人数、元の侵害日、販売者の作成関与、完全なファイルは確認されていない。

事例 E

E

## 再配布の主張では元の侵入者は分からない

証拠カード B06 2026年8月22日 フォーラム ソフトウェア

主張は未確認

| | |
|---|---|
| **主張** | 8 月 22 日のあるアカウントは、日本のソフトウェア企業のソースコードなど 74 GBを公開すると主張している。元の入手に関わったとする、ほかの別名アカウントを挙げている。 |
| **時系列** | 投稿は再配布を説明している。その日付は、元のアクセスの時期や、挙げられたアカウントの関与を立証しない。 |
| **分かること** | アカウントは、情報を共有していると述べ、他のアカウントに以前の役割を帰属させた。これは、主張された関連であり、確認済みの移転や共通の運営者ではない。 |
| **別の可能性** | 情報は、本物、一部のみ、以前から公開済み、過去のもの、誤って説明されたものの可能性がある。別名への謝辞は、正確な場合も、宣伝のための場合もある。 |
| **制約** | ソースコードの真正性、完全性、入手日、顧客への影響は未解決である。説明だけでは、製品の脆弱性や露出した連携は確認できない。 |

| | |
|---|---|
| **対応** | 関係する責任者は、正当なファイルとの一致を特定し、実際の機微性を評価すること。検証した情報から関係が分かる場合に限り、認証情報や連携を確認する必要がある。 |

**結論**

機微なコード、認証情報、連携先を評価する前に、自社の真正な資料を特定する。

証拠カード B06 — 2026年8月22日

[別名非公開] フォーラム フォーラム 英語

原文

74GB of source codes, and other stuff

翻訳

74GBのソースコードとその他の資料。

**注記.** 再配布の主張であり、投稿したアカウントが侵入を実行した証拠ではない。

**確認事項**

投稿者は、日本のソフトウェア事業者のソースコードなど74GBを公開すると主張している。元の取得を実行したとされる主体には、別のアカウント名を挙げている。

**未確認事項**

ソースコードの真正性、完全性、侵害日、元の攻撃者との関係、顧客への影響は確認されていない。

事例 F

F

## 保険の行数は販売投稿上の対象集団にとどまる

証拠カード B09 | 2026年5月13日 | フォーラム | 保険

主張は未確認

| | |
|---|---|
| **主張** | 5 月 13 日のフォーラムの販売投稿は、CSV形式の日本の保険記録 10,000,000 件を宣伝している。説明には、本人情報、連絡先、保険契約に関係する項目が並んでいる。 |
| **時系列** | この販売投稿は、本報告書で扱う後の公表の一部より前である。ファイルや独立に裏付けられた関係は確認されていないため、それらの事故に帰属させていない。 |
| **分かること** | 投稿は、件数と項目の種類を主張する、保険を題材にしたデータを販売している。保険会社への侵入や、影響した人数を立証しない。 |
| **別の可能性** | 過去の情報、集約した見込客データ、誤ったラベルのファイル、新たな漏えいなどが考えられる。保存した文面では区別できない。 |

| | |
|---|---|
| **制約** | 内容、行数、重複の有無、由来、入手日は、独立に確認されていない。CSVは形式の説明であり、真正性の検証方法ではない。 |
| **対応** | 保険会社は、自組織の情報との信頼できる一致を調べ、契約変更やアカウント復旧の手順を確認すること。顧客への通知や、対象全体のアカウントへの措置を選ぶ前に、漏えいを裏付ける必要がある。 |

**結論**

自社情報との一致を確認し、契約変更、アカウント復旧、顧客通知の判断を見直す。

証拠カード B09 — 2026年5月13日

[別名非公開] フォーラム フォーラム 英語

原文

Type: Japan Insurance Format: CSV Records: 10M

翻訳

種別：日本の保険。形式：CSV。レコード数：1,000万という。

**注記.** 日本を対象とする具体的な販売の主張である。行数は、広告上の件数として扱う。

**確認事項**

販売者は、日本の保険に関するCSV記録10,000,000件のデータセットを宣伝している。本人情報、連絡先、保険契約に関する項目を挙げている。

**未確認事項**

データセット、規模、出所、日付、重複の有無、保険会社の侵害は、独立して確認されていない。

## 4.5 需要、古い情報、国際的な販売

追加のカードは、投稿を事故として数えられない理由を示している。防御側に役立つが、それぞれから分かることは限定されている。[S1]

| 観測した投稿 | 分かること | 立証しないこと | カード |
|---|---|---|---|
| 元の入手を 2024 年 2 月 22 日とし、18,653,758 行を記す、1 月の再アップロード | 2026 年中に再流通が宣伝された | 2026 年の新たな侵入や、現在のパスワードの有効性 | B07 |
| 日本出身の宿泊客を含む、世界全体で 16,000,000 行と主張する、11 月のホテル予約情報の販売 | 国際的な販売投稿が日本に言及している | 日本の分量や、日本のサービス提供者への侵入 | B08 |
| 複数の地域の政府情報を求める、1 月の中国語の投稿 | 情報を買いたいという意思 | 保有、入手の成功、日本政府への侵入 | B10 |

証拠カード B07 2026年1月13日

[別名非公開] フォーラム フォーラム 英語

原文
contains 18,653,758 lines

翻訳
18,653,758 行が含まれるという。

**注記.** 2026年に観測された再流通であり、2026年の新規事案ではない。

**確認事項**
2026年1月の投稿は、再アップロードと自称し、元の取得日は2024年2月22日だったと記載している。

**未確認事項**
2026年の投稿日は、2026年の侵入、新たな被害者、重複のない人数、パスワードの有効性を示すものではない。

証拠カード B08 2026年11月5日

[別名非公開] フォーラム フォーラム 英語

原文
database consisting of 16 million rows

翻訳
16,000,000 行からなるデータベースだという。

**注記.** 世界・複数国を対象とする販売投稿であり、16,000,000件や対象ホテルは日本に帰属しない。

**確認事項**
販売者は、ホテル予約のデータセットを宣伝し、新たな記録が継続して追加されていると主張している。顧客の出身国として挙げた複数の国には、日本も含まれる。

**未確認事項**
16,000,000行という数字は、世界全体に関する主張である。日本の割合、対象ホテル、データの真正性、継続的なアクセスの主張は未確認である。

証拠カード B10 2026年1月1日

[別名非公開] フォーラム フォーラム 中国語

原文
政府的内部情报，包括政策、报告、机密文件、军事情报

翻訳
政府の内部情報。政策、報告書、機密文書、軍事情報を含む。

**注記.** 複数国に対する需要であり、政府データの販売投稿ではない。

**確認事項**
中国語の広告は、日本を含む複数の国から、政府内部、政策、機密、軍事に関する情報を求めている。

**未確認事項**
投稿が示すのは、購入の意向だけである。保有、取得の成功、日本政府の侵害を示すものではない。

古い情報でも、本物であれば本人情報を使った詐欺に役立つ場合がある。価値が続いていても、入手が最近だったことにはならない。対応チームは、観測した広告日と、主張された元の対象期間の両方を記録すること。未検証の情報の古さは、投稿者の主張として維持する必要がある。

国際的な販売では、国との関係を区切る必要がある。日本の顧客、海外にある日本のブランド、日本で運用するシステムは、それぞれ異なる関係である。広告が多数の宿泊客や顧客の出身地に日本を含めただけで、世界全体の行数を日本に割り当てるべきではない。

需要にも、別の意味がある。買い手の関心は、機微情報や内部通報の経路に注意を向ける理由になる。売り手、アクセス経路、入手、成立した取引が存在することを立証しない。

ほかの業種別の主張は、以下に示す。日付は投稿日であり、内容は未検証のままである。国全体の事故件数には加算していない。[S1]

| 日付 | 広告上の内容 | 証拠の境界 |
|---|---|---|
| 2026-01-01 | ラジオ・音楽サービスのデータ。3,016,221 レコードとの主張 | ファイルの真正性や流出は確認していない |
| 2026-01-02 | ホテル関連データ。約 720,000 レコードとの主張 | 依頼形式の題名だが、本文は販売の申し出 |
| 2026-01 to 2026-10 | 教育関連データ。約 98,000 行 | 日付をまたぐ類似広告を、その都度の新規事案とは数えない |
| 2026-02 to 2026-04 | 管理・サポート関連データ。約 468,000 行 | 別の購入者は自動生成の識別子だと主張。いずれもデータを認証しない |
| 2026-04-02 | 従業員・給与関連資料。約 672,000 レコード | 内容と影響対象は未検証 |
| 2026-04-02 to 2026-04-22 | 利用者・連絡先の資料。約 437,000 レコード | 説明の繰り返しは、別々の事案を示さない |
| 2026-04-07 | 住宅検索の資料。約 2,400,000 レコード | 出所、重複の有無、現在のアクセスは未確認 |
| 2026-04-07 | 通信サービスのアカウントと活動。250 GB超との主張 | 容量の主張であり、人数ではない |
| 2026-04-18 | 小売・注文情報。約 1,700,000 レコード | データの真正性や現在の侵入は未確認 |
| 2026-09-17 | 製薬事業のファイル。約 4 TBとの主張 | 投稿が言及する組織側の声明を独立には確認していない |
| 2026-09-18 | 過去の余暇サービス関連資料。2,137,062 行、流出日を 2022 年と記載 | 2026 年の再流通。元の日付と内容は投稿者の主張 |
| 2026-01-11 | 約 850,000 件の日本の電話情報をめぐる販売上の争い | 購入者は虚偽だと主張。争いだけでは真正性は判断できない |

## 4.6 価格、ファイル容量、アクター間の関係

脆弱性の価格 5,000 USDは、広告上の希望価格である。コード 74 GBという説明は、主張された容量である。どちらも、成立した取引、商業的な価値、確認済みの保有を示さない。そのため、本報告書は、これらの販売投稿から市場の収益を推定していない。[S1]

似た文面は、広告同士が似ているという判断を裏付ける場合がある。同一のファイル、元の作者、アカウント間の移転は立証できない。投稿に記された別名との関係も、具体的な共通要素が限定した結論を支えるまでは、主張された関係にとどまる。

対応チームが最初に確認するのは、情報やアクセスが自組織に属するかどうかである。次に、今も関係し、使えるかを確認する。IDの責任者、アプリケーションの責任者、データの管理者では、判断に必要な証拠が異なる場合がある。

## 4.7 警告からリスクに見合う措置へ

関係する警告について、判断を明確に記録すること。主張、観測日、主張された範囲を保全する。検証または否定に使った自組織の証拠、判断の責任者、次の見直し時点も加えること。

有効なアカウントを確認した場合は、権限と関係する動作を調べる。情報の一致が裏付けられた場合は、影響する種類と保護措置を評価すること。警告が古い情報や無関係の情報を扱っていた場合は、不確かさを安全の宣言に変えることなく、終了する理由を記録すること。

公開の説明にも、同じ規律が必要である。広告は広告、依頼は依頼として記し、公的な公表は、その明示された範囲で説明すること。付録で慎重なラベルを付けても、確信しすぎた見出しを修正することはできない。

要点

01

六つの事例が示すのは、観測した主張であり、確認済みの侵入件数ではない。

02

需要、再配布、国際的な範囲、主張されたアクセスを区別すること。

03

自組織の証拠との一致に基づき、ID、データ保護、サービス対応の措置を選ぶこと。

章 05

# 公表された事案と分野別の対応

この章で答える問い

どの事案が業務上の判断を変えるか

## 2026

公表事案と攻撃活動の調査


5.1 公表された事案 41
5.2 追加の公表事例 54
5.3 業種ごとの判断 58
5.4 匿名の事案と広がる情報流出への注意 58
5.5 原文の公表に基づく追加事例 58

章 05

# 公表された事案と分野別の対応

概要

各事案では、サービス停止、確認済みの持ち出し、漏えい可能性を区別する。11 月の通知は、機微なテストデータ、委託先の保有記録、保存された認証情報で対応が異なることを示す。後日の範囲修正が、新たな攻撃を意味するとは限らない。金融ではセッションと口座開設の管理、製造では復旧検証、顧客基盤では出力制限と連絡の代替策が必要になる。封じ込めや顧客案内を決める前に、対象項目と依存関係を確認する。

**サービス復旧とデータ漏えいの判断には、別々の証拠が必要である。** アプリケーションが復旧しても、コピーされた記録や認証情報の疑問は残り得る。反対に、大きな影響可能性が示されても、全アカウントからの持ち出しが確認されたとは限らない。以下では、この区別と最新の重要な修正を示す。

| 業種 | 事案から生じる判断 | 優先する対応 |
| --- | --- | --- |
| 銀行・証券・保険 | 機微なデータはテスト、照会、口座開設の環境に残り得る | 保存データを減らし、出力を制限し、必要に応じて有効なセッションを無効化する |
| 通信・ホスティング・デジタルサービス | 一つの委託先の制御が、多くの利用企業のサービスに影響する | 顧客ごとの範囲、共通の管理権限、顧客連絡の代替策を把握する |
| 製造・研究 | 暗号化と認証情報の露出では、復旧範囲が異なる | 復旧を検証し、接続先環境へのアクセスを調べる |
| 医療・教育 | 補助システムや委託先の古いコピーに、機微な履歴が残り得る | 周辺システム、委託先権限、不要となった記録を点検する |
| 交通・小売・飲食 | 本人確認画像、購入履歴、決済画面では危険が異なる | 実際のデータ区分に合わせて、保存と顧客案内を調整する |

## 5.1 公表された事案

事例 G

### G 理化学研究所：外部システムの認証情報にも対応が必要

研究

公式更新

| | |
|---|---|
| **概要** | 理化学研究所は、富岳を支える計算環境への不正アクセスを公表した。11 月 20　日の更新により、全国報道が始まった時点よりも対応範囲が大きく広がった。[S7] [S6] |
| **時系列** | 11 月 12 日に不審な通信が見つかり、11 月 13 日に侵入を確認した。11 月 14 日にサービスを停止した。初回公表は 11 月 16 日で、詳細な更新は 11 月 20 日だった。[S6] |
| **確認事項** | 更新では、利用者 4,222 人の情報へのアクセス痕跡を確認した。秘密鍵を含む外部システム用認証情報　430 件には、収集または移動の痕跡があった。このうち　233 件はパスフレーズなし、197 件はパスフレーズ付きだった。[S6] |
| **限界** | 一部の認証情報には外部への接続痕跡があったが、より広い不正利用は確認されていなかった。研究成果が持ち出された具体的な証拠も見つかっていない。認証情報の移動と、すべての外部システムへのアクセス成功は別の事象である。[S6] |
| **対応** | 防御側は、対象の認証情報を交換し、接続先機関の認証履歴を調べる必要がある。鍵の利用状況を検証してから信頼関係を復旧すべきである。研究基盤の対応には、利用者が保存した秘密情報で接続できるシステムも含める必要がある。 |

**結論**

収集または移動の痕跡がある研究用認証情報を無効化し、接続先すべての認証履歴を確認する。

事例 H

### H IDCフロンティア：共用クラウドで暗号化による障害

クラウドサービス

ランサムウェアを確認

| | |
|---|---|
| **概要** | IDCフロンティアは、IDCFクラウドの顧客仮想マシンに影響するランサムウェア被害を確認した。当時の報道は、企業や自治体の顧客への障害を伝えた。共用インフラ事業者の障害が及ぶ範囲を示している。[S9] |

| | |
|---|---|
| **時系列** | 障害は 10 月 7 日午前 3 時 40 分ごろ、日本時間で始まった。10 月 27 日の第 7 報は調査結果と対応をまとめた。東日本リージョン 1 の 4 ゾーンが影響を受けた。[S8] |
| **確認事項** | 事業者は、ポータル認証で使うオープンソースソフトウェアの弱点を侵入経路と特定した。攻撃者は仮想マシンを暗号化または停止させた。影響を受けたサービスの顧客は 495 組織だった。[S8] |
| **限界** | 495 という数字は、影響を受けた顧客組織数である。人数や、データ窃取が確認された被害組織数ではない。10 月 27 日の報告では、顧客仮想マシンのデータが外部に持ち出されたとは確認されていなかった。[S8] |
| **対応** | 防御側は、クラウド内の分離、独立した復旧用コピー、事業者停止時の代替策を一緒に検証すべきである。調達部門は、管理基盤への侵入、仮想マシンの暗号化、確認済みの持ち出しを区別した更新報告を求める必要がある。 |

**結論**

被害を受けた事業者の管理基盤に依存しない復旧を検証する。

事例 I

## プレイド：顧客向け基盤の停止が長期化

デジタルサービス

公式調査結果

| | |
|---|---|
| **概要** | プレイドのKARTEで発生した事案は、複数の組織が使う顧客接点基盤に影響した。11 月 20 日の調査結果と再開見通しにより、委託先の停止が利用企業の事業継続に直結する課題となった。[S11] |
| **時系列** | 同社は攻撃日を 11 月 13 日とし、同日に全サービスを停止した。提供側の影響範囲調査を 11 月 19 日に終え、11 月 20 日にまとめを公表した。[S10] |
| **確認事項** | 内部処理の不備により、外部からデータへアクセスできる経路が生じた。そこから得た情報と認証情報を使い、管理画面にアクセスされた。確認された範囲には、現契約先と過去の契約先が含まれた。[S10] |
| **限界** | 同社は、アカウントのメールアドレス 79,249 件と、営業・サポートの連絡先 45,816 件を別々に示した。これらから利用企業側の影響人数を一つの合計にすることはできない。顧客ごとに同じ項目が含まれたともいえない。[S10] |
| **対応** | 公表された再開目標は 2027 年 1 月中旬だった。防御側は、顧客連絡の代替手段を用意し、接点基盤に不要な過去データを残さないようにすべきである。再開計画では、技術的な修正や顧客別通知に加え、業務責任者による確認も必要となる。 |

**結論**

委託先の長期停止を前提に、顧客連絡の代替手段を計画する。

J

事例 J

## 決済事業者：復旧を個別に判断

金融

公式公表

| | |
|---|---|
| **概要** | 決済事業者は、顧客情報に関係する不正アクセスを確認した。 [S12] [S13] |
| **範囲** | 事業者は、影響する環境と、確認後に再開できる環境を区別した。 [S12] |
| **確認されたこと** | 公表された範囲は個人情報に関するものであった。記録の対象集団は、必ずしも実人数を示さない。 [S12] |
| **限界** | 一部の再開だけでは、全面復旧やすべての調査の終了は裏付けられない。 [S12] |
| **対応** | 顧客ごとの証拠に基づいて再開を判断し、現在のサービス状況を説明する。 |

**結論**

顧客ごとの証拠に基づいて再開を判断し、現在のサービス状況を説明する。

K

事例 K

## ニトリ：大規模な影響可能性と確認済み被害を区別

小売

漏えいの可能性

| | |
|---|---|
| **概要** | ニトリは、システムへの不正アクセスに伴う個人情報漏えいの可能性を公表した。全国向けの経済報道でも取り上げられたが、公表規模を解釈する際には同社の留保を維持する必要がある。 [S15] |
| **時系列** | 同社は 11 月 6 日に問題を検知し、11 月 9 日に公表した。10 月中旬から下旬に不正アクセスがあった可能性を示した。 [S14] |
| **確認事項** | 対象となる可能性のある範囲は、約 37,620,000 件に達した。同様の小売システムを点検する組織には、顧客データの保存と過去の記録の扱いが重要な論点となる。通知では、パスワードとカード情報を対象外とした。 [S14] |
| **限界** | この数字は、影響の可能性がある記録の最大範囲である。窃取が確認された件数、重複のない顧客数、後の不正利用が立証された数として言い換えてはならない。 [S14] |

| | |
|---|---|
| **対応** | 防御側は、保存する顧客データが現在の業務に必要かを照合し、公表された期間のアプリケーションアクセスを調べるべきである。利用者への説明では、漏えいの可能性と確認済みの持ち出しを区別し、具体的な保護策を示す必要がある。 |

**結論**

漏えいの可能性という留保を維持し、不要な顧客データの保存を減らす。

L

事例 L

## 教育機関：委託先の露出と業務障害を区別

教育

公式更新

| | |
|---|---|
| **概要** | 教育機関は、委託先に関係する情報漏えいと自組織のシステム障害を公表した。 [S16] |
| **範囲** | 調査では、委託先が保管する情報と、教育機関の業務システムを個別に扱った。 [S16] |
| **確認されたこと** | サービスの委託関係全体で、保存情報と特権アクセスの確認が必要となった。 [S16] |
| **限界** | 教育機関は、自組織のシステムから個人情報が直接持ち出された具体的な証拠を確認していなかった。 [S16] |
| **対応** | 不要となった委託先のコピーを削除し、管理アクセスを作業と時間で制限する。 |

**結論**

不要となった委託先のコピーを削除し、管理アクセスを作業と時間で制限する。

M

事例 M

## タイムズカー：本人確認画像の調査結果を更新

交通

影響範囲を更新

| | |
|---|---|
| **概要** | タイムズカーの事案は、顧客アカウント情報と本人確認書類の画像に関係した。10 月 23 日の第 5 報を扱う報道は、画像件数の修正、利用者支援、保存方法の大きな変更を伝えた。 [S18] |
| **時系列** | 異常なアクセスは 9 月 25 日に検知された。9 月 28 日の通知は当初の顧客範囲を示した。10 月 23 日の更新は、本人確認画像の以前の推計を、より具体的な調査結果に置き換えた。 [S17] |

| | |
|---|---|
| **確認事項** | 最新のアカウント範囲は約 6,600,000 件だった。暗号化された本人確認書類画像約 1,460,000 件に、アクセスと外部送信の痕跡があった。別の画像区分には、アクセス痕跡はあったが、外部送信の痕跡は確認されなかった。[S17] |
| **限界** | 画像の件数を、別の重複のない人数として加えてはならない。暗号化画像の外部送信は、直ちに読める状態になったことを意味しない。ただし、復号の危険は完全には否定できなかった。アクセスと送信は別の区分として報告された。[S17] |
| **対応** | 運営会社は本人確認画像の保存方法を変更した。防御側は、登録後も書類全体の保管が必要かを見直すべきである。調査報告では、アカウント記録、暗号化データ、アクセス痕跡、確認された移動を分ける必要がある。 |

**結論**

本人確認書類は、確認手続きに必要な期間だけ保存する。

N

事例 N

## KDDI：訂正後のメール基盤の件数を使用

通信

公表数値を訂正

| | |
|---|---|
| **概要** | KDDIの共用インターネット接続事業者向けメール基盤の事案は、複数のサービス運営者に及んだ。その後の行政指導に関する報道も、対象基盤の利用者と同社の他の消費者向けサービスを区別する重要性を示した。[S20] |
| **時系列** | 一部の対象事業者では、不正な活動が 5 月に始まった。KDDIは 6 月 17 日に問題を検知し、6 月に初めて公表した。7 月 6 日の報告は 7 月 21 日に訂正された。[S19] |
| **確認事項** | 訂正後の範囲は、利用者　12,231,954　人のメールアドレスと、パスワード 7,616,173 件だった。パスワードの対象は、より大きな影響範囲の中に含まれる。別の人数として加えてはならない。[S19]　個人情報保護委員会も、この共有基盤の認証情報流出を確認し、是正を指導した。[S83] |
| **限界** | 訂正により、当初のより大きな推計は置き換えられた。KDDIは、明示した主要な消費者向けサービスを影響なしとした。同じ企業ブランドを使う全サービスに、影響を広げて解釈すべきではない。[S19] |
| **対応** | 防御側は、対象事業者間で認証情報の交換を調整し、パスワードの使い回しを確認すべきである。各アカウントが実際に使うメール基盤も特定する必要がある。通知、窓口説明、利用企業の更新情報では、古い数字を一貫して訂正すべきである。 |

**結論**

訂正後の範囲を使用し、対象事業者間でパスワード対応を調整する。

事例 O

## ■ アフラック生命：大量照会を捉える監視が課題

保険

最新の公式範囲

| | |
|---|---|
| **概要** | アフラック生命は、アプリケーション環境を通じた顧客情報の漏えいを公表した。広範な報道は日本法人の事案を確認した。その後の同社の更新により、活動期間と対象情報が修正された。[S22] |
| **時系列** | 最新の説明では、不正アクセスの期間は 6 月 10 日から 25 日で、検知日は 6 月 25 日となる。初回公表は 6 月 30 日だった。事案のFAQは 11 月 13 日にも更新された。[S21] |
| **確認事項** | 修正後の範囲は顧客約 4,400,000 人で、その中に銀行口座情報が関係する約 220,000 人が含まれた。同社は、データ照会の制御が不十分で、要求が通常利用に見える場合があったと説明した。大量照会の監視が必要となる。[S21] |
| **限界** | 以前の顧客数と銀行口座情報の推計は置き換えられた。同社は、カード情報やウェブサイトのパスワードなど、他の機微な項目を対象外とした。海外の別のアフラック事案に関する報道は、日本の事案の帰属根拠にはならない。[S21] |
| **対応** | 防御側は、正規のアプリケーション機能を使う要求でも、照会権限と異常な取得量の警告を点検すべきである。保険会社の対応計画では、本人情報、銀行口座情報、顧客窓口のなりすましを別々に扱う必要がある。 |

**結論**

不審なログインに加え、異常なデータ照会量も検知する。

事例 P

## ■ 日本医科大学武蔵小杉病院：ナースコールシステムに機微情報が保存されていた

医療

ランサムウェアと漏えい

| | |
|---|---|
| **概要** | 日本医科大学武蔵小杉病院は、ナースコール環境に影響するランサムウェア事案を公表した。初期の全国報道は、少ない暫定患者数を使っていた。その数字は、後の病院の調査結果で大きく修正された。[S24] |
| **時系列** | |

病院は、1 月 26 日にVPNの弱点を通じた侵入があり、1 月 29 日にナースコールのデータベースから情報が盗まれたと特定した。障害の検知は 2 月 9 日だった。2 月 27 日の第 5 報が調査結果を更新した。[S23]

| | |
|---|---|
| **確認事項** | 修正後の影響可能性は、患者約 130,000 人と職員・学生約 1,700 人だった。病院は、盗まれたナースコールのデータが後に公開されたと確認した。その情報は、中央の電子カルテ環境とは別の場所にあった。[S23] |
| **限界** | 当初の患者約 10,000 人という数字は、最新値ではない。病院は通常診療の継続を報告し、電子カルテシステムからの漏えいは確認しなかった。周辺の臨床システムにも、多くの機微情報が保存され得る。[S23] |
| **対応** | 防御側は、病床周辺、通信、設備関連のシステムにあるデータを把握し、遠隔保守のアクセスを分離すべきである。診療継続の演習には、補助システムの停止と、そこにコピーされた情報の公開を含める必要がある。 |

**結論**

アクセス点検では、診療を支える周辺システムも機微情報の保存先として扱う。

事例 Q

## アドバンテスト：後日の通知で持ち出しを確認

製造

ランサムウェアを確認

| | |
|---|---|
| **概要** | アドバンテストの当初のランサムウェア対応と後日の個別通知は、同じ事案の異なる段階を示す。その後の報道は、個人情報の窃取が後に確認された点を明確にした。[S27] |
| **時系列** | 同社は 2 月 15 日に不審な活動を検知し、2 月 19 日に初回通知を公表した。カリフォルニア州司法長官に届け出た 10 月 6 日の個別通知は、より具体的な調査結果を示した。[S26] [S25] |
| **確認事項** | 後日の通知では、2 月の事案で情報が持ち出され、通知先本人の個人情報が含まれたと確認した。当初の説明を補強するものであり、10 月の別の侵入を確認したものではない。[S25] |
| **限界** | 通知書のひな型にある情報区分は、受取人ごとに異なり得る。全員から同じ項目が盗まれたと説明すべきではない。確認した通知から、影響人数の全体像を確定することもできない。[S25] |
| **対応** | 防御側は、後日の当局向け報告や個別通知まで、同じ事案の時系列を維持すべきである。製造業の対応計画では、暗号化からの復旧とともに持ち出しの証拠を保全する必要がある。遅れて判明した事実を、顧客と従業員への説明に正確に反映すべきである。 |

**結論**

後日の通知で持ち出しが確認された場合、元の事案記録を更新する。

事例 R

R

## マネーフォワード：リポジトリのコピーと本番アクセスを区別

金融技術

調査完了

| | |
|---|---|
| **概要** | マネーフォワードは、GitHubリポジトリの不正なコピーを公表した。報道と同社の調査は、開発資料内の情報露出と、本番データベースの侵害を区別した。[S29] |
| **時系列** | 同社は 5 月 1 日に事案を初めて発表した。6 月 23 日の第 4 報で詳細調査を終え、コピーされた資料内の追加情報を特定した。銀行連携機能にも一時的な停止の影響があった。[S28] |
| **確認事項** | 最終更新では、追加の顧客氏名・メールアドレス、取引先連絡先、従業員情報を特定した。同社は、顧客 60,449 名分の内部識別子も報告した。これらの識別子だけでは個人を直接特定できず、氏名やメールアドレスを含まず、ログインIDとも異なっていた。[S28] |
| **限界** | 同社は、本番データベースへの不正アクセスを確認しなかった。リポジトリのコピー、秘密情報の露出、その秘密情報で到達できるシステムへのアクセスは、別々に確認する必要がある。公表区分を根拠なく一つの合計にすべきではない。[S28] |
| **対応** | 防御側は、開発資料に本番由来のデータがないかを調べ、露出した秘密情報を無効化し、交換後の認証情報でアクセスを検証すべきである。サービス停止の判断は、封じ込める依存先と、安全な再接続に必要な証拠に基づく必要がある。 |

**結論**

本番由来のデータをリポジトリから除き、再接続前に交換後の認証情報を検証する。

事例 S

## S ■ オンライン基盤：不完全なログが結論を制約

デジタルサービス

漏えいの可能性

| | |
|---|---|
| **概要** | オンライン基盤は、開発環境とクラウド環境に関係する不正アクセスを公表した。 [S30] |
| **範囲** | 認証情報の露出により、当初確認した環境以外も調査する必要があった。 [S30] |
| **確認されたこと** | 個人情報が、アクセスされた可能性のある範囲に含まれた。 [S30] |
| **限界** | 不完全なログのため漏えいを断定的に否定できなかったが、データベース全体の窃取が確認されたわけでもない。 [S30] |
| **対応** | 露出した認証情報を失効させ、機微なクラウド情報のクエリ単位の証拠を保存する。 |

**結論**

露出した認証情報を失効させ、機微なクラウド情報のクエリ単位の証拠を保存する。

事例 T

## T ■ 金融サービス事業者：残されたテストデータが露出

金融サービス

公式調査結果

| | |
|---|---|
| **概要** | 金融サービス事業者は、テスト環境への不正アクセスを確認した。 [S31] |
| **範囲** | 調査では、アカウント認証情報の不正利用を確認した。 [S31] |
| **確認されたこと** | 保存されていた業務情報が影響範囲に含まれた。 [S31] |
| **限界** | 調査結果は、取引処理の侵害を裏付けていない。 [S31] |
| **対応** | 不要なテスト環境を廃止し、テスト終了時に複製した業務情報を削除する。 |

**結論**

不要なテスト環境を廃止し、テスト終了時に複製した業務情報を削除する。

事例 U

## U メーカー：外部送信後もファイルの範囲は不明

製造

最終調査結果

| | |
|---|---|
| **概要** | メーカーは、リモートアクセスの認証情報に関係する侵入を公表した。[S32] |
| **範囲** | その後の調査結果では、情報の外部送信を確認した。[S32] |
| **確認されたこと** | 外部に送信された個別のファイルは特定されていなかった。[S32] |
| **限界** | 送信の確認だけでは、露出したすべてのファイルの内容や、その後の公開は裏付けられない。[S32] |
| **対応** | リモートアクセスの認証を見直し、外部送信のログを保存する。 |

**結論**

リモートアクセスの認証を見直し、外部送信のログを保存する。

事例 V

## V 日本交通：業務記録と過去の個人情報で範囲が異なる

交通

公式範囲を更新

| | |
|---|---|
| **概要** | 日本交通は、マルウェアの侵入とハイヤー関連システムの停止を公表した。後の報道と同社通知は、サービス停止と、影響を受けた過去の個人情報の保有範囲を区別した。[S35] |
| **時系列** | 侵入は 7 月 11 日に検知され、7 月 13 日に初めて公表された。10 月 30 日の第 6 報は、先行する調査更新を受けて対象区分を修正した。一つの事案について説明が更新されている。[S34] [S33] |
| **確認事項** | 対象には、個人ハイヤー利用者、従業員、応募者、親族、取引先連絡先、事故の相手方が含まれた。各区分のおおよその件数には大きな差があった。区分によって、本人確認、金融、健康に関する項目が含まれた。[S33] |
| **限界** | 区分間に重複があり得るため、人数として合計してはならない。同社は、タクシーの乗車・配車利用者データを対象外とした。ハイヤーの停止から、全タクシー業務の侵害を導くことはできない。[S33] |

| | |
|---|---|
| **対応** | 防御側は、採用と事故の記録を現在の配車業務から分離し、保存量を減らし、電話による代替手段を演習すべきである。交通事業の継続計画では、被害環境の隔離中に、どの予約・配車業務を継続できるかを特定する必要がある。 |

**結論**

保存する人事・事故記録を、稼働中の配車システムから分離する。

事例 W

## W ■ 運輸事業者：業務アプリに個人情報を保存

運輸

公式公表

| | |
|---|---|
| **概要** | 運輸事業者は、業務アプリケーションからの情報持ち出しを確認した。[S36] |
| **範囲** | アプリケーションの復旧と保存情報の評価は、別々の対応作業であった。[S36] |
| **確認されたこと** | 影響する情報には、人事情報と業務上の連絡先情報が含まれた。[S36] |
| **限界** | 確認した通知は、ランサムウェアや攻撃者の帰属を裏付けていない。[S36] |
| **対応** | 補助的なアプリケーションの個人情報を棚卸しし、復旧中もアクセスログを保存する。 |

**結論**

補助的なアプリケーションの個人情報を棚卸しし、復旧中もアクセスログを保存する。

事例 X

X

## 技術サービス事業者：環境を個別に調査

技術サービス

漏えいの可能性

| | |
|---|---|
| **概要** | 技術サービス事業者は、別々の環境における不正アクセスを調査した。[S37] |
| **範囲** | 各調査では、アクセスの履歴と情報の範囲が異なった。[S37] |
| **確認されたこと** | 流出の可能性がある範囲には、アカウント情報と保存された認証情報が含まれた。[S37] |
| **限界** | 対象となり得る集団全体の外部持ち出しは確認されていない。単一の攻撃経路も裏付けられていない。[S37] |
| **対応** | 露出した可能性のある秘密情報を更新し、環境ごとの証拠に基づいて評価する。 |

**結論**

露出した可能性のある秘密情報を更新し、環境ごとの証拠に基づいて評価する。

事例 Y

Y

## ブックオフ：漏えいを確認し、対象項目を訂正

小売

公式調査結果

| | |
|---|---|
| **概要** | ブックオフは、会員管理システムへの不正アクセスを公表し、個別通知を始めた。その後の公式調査結果は、会員データ件数と影響人数を正確に区別した。[S39] |
| **時系列** | 同社は 10 月 6 日にアクセスを確認し、10 月 4 日から 6 日に情報が取得されていたとした。初回公表は 10 月 9 日だった。11 月 6 日の第 3 報が、調査結果と現在の対応をまとめた。[S38] |
| **確認事項** | 公表範囲は、元会員を含む 6,383,279 人に関する会員データ 6,427,735 件だった。システムの一部機能にあるアクセス制御上の問題が悪用された。公表された情報項目には、パスワードのハッシュ値と顧客の連絡先が含まれた。[S38] |
| **限界** | 10 月の訂正では、以前の一覧から漏れた項目を追加したが、人数は変わらなかった。最新通知では、外部公開、ポイント不正利用、会員情報の改変は確認されなかった。決済情報と銀行情報は対象外だった。[S38] |

| | |
|---|---|
| **対応** | 防御側は、通知前に対象項目を確認し、アカウント記録と人数を区別すべきである。小売の対応計画では、直接連絡と利用者自身による照会を用意する必要がある。FAQと窓口案内でも、訂正内容を一貫して管理すべきである。 |

**結論**

顧客通知前に、影響人数、会員記録件数、対象項目を照合する。

Z

事例 Z

## ANA：委託先の旅客データを項目別に区分

航空

公式公表

| | |
|---|---|
| **概要** | ANAは、予約システムの提供会社に関係する旅客データの事案を確認した。全国報道は対象利用者を伝えた。同社通知は、基本的な予約データと、より少ない人数に関する追加情報を区別した。[S41] |
| **時系列** | 確認した同社通知の日付は 10 月 30 日で、10 月 29 日の報道に続いた。対象の予約記録は、2023 年 8 月から 2026 年 9 月のものだった。この予約期間は、侵入期間を示してはいない。[S40] |
| **確認事項** | 対象は顧客約 37,800 人だった。約 36,100 人は基本的な予約情報で、約 1,700 人にはパスポートや連絡先などの追加項目が含まれる可能性があった。区分は、保存する旅客情報の違いを反映していた。[S40] |
| **限界** | 同社は、カード情報とパスワードを対象外とした。すべての旅客に、より機微な追加項目が露出したとは確認されていない。委託先の事案を、すべての航空会社アプリケーションへの直接侵入として説明すべきではない。[S40] |
| **対応** | 防御側は、提供会社と項目の機微性に応じて旅客情報を把握し、区分ごとの通知を準備すべきである。航空の演習には、予約を装うなりすましを含める必要がある。運航、予約の可用性、機密性への影響は区別して扱うべきである。 |

**結論**

委託先にある各記録の実際の項目に応じて、旅客への通知を分ける。

## 5.2 追加の公表事例

### 追加事例 AA: OpJapan：攻撃主張と実証された停止は別

- **概要。** セキュリティ研究者は、OpJapanの名称を使った攻撃活動の再活発化を報告した。確認した調査は、攻撃者の主張と標的の傾向を分析する材料となる。一方、各標的の業務への影響は未確定のままである。[S42] [S43]
- **時系列。** S2Wは、2 月 14 日から 16 日の主張の波を報告した。Check Pointの 9 月 7 日の調査は、8 月 24 日から 30 日の再活発化を扱った。公表日と、主張された活動期間は別の時系列情報である。[S42] [S43]
- **確認事項。** Check Pointは、後の波で 26 組織に関する 66 件の主張を記録した。調査は主に分散型サービス妨害を扱い、監視機器へのアクセス主張も含んだ。これらは、同社が数えた主張と、名指しされた標的の件数である。[S42]
- **限界。** 調査は、名指しされた標的全体の内部システム侵害やデータ漏えいを確認していない。主張の合計は、確認済み事案の合計ではない。攻撃者の画面画像やサービスエラーの観測だけで、全国規模の継続的な停止を確認することもできない。[S42]
- **対応。** 防御側は、対応を引き上げる前に、主張を可用性監視、事業者ログ、顧客影響と照合すべきである。サービス妨害への対処能力と連絡計画を維持し、アクセスや盗難データの主張は別の証拠確認で評価する必要がある。

### 追加事例 AB: CoGUI：日本を重視するフィッシング基盤への妨害

- **概要。** Proofpointは、日本を強く意識した中国語のフィッシングキットに対する 10 月の妨害活動を説明した。Microsoftの関連する民事手続きの通知は、その手続きに関する別の記録となる。[S44] [S45]
- **時系列。** 確認した二つの資料は、いずれも 10 月 14 日に公表された。調査が扱うのは既存のフィッシング基盤への介入であり、日本の特定の銀行や小売企業に対する新たな侵害の特定ではない。[S44]
- **確認事項。** Proofpointは、共通の起源や利用者の活動を含め、CoGUI、CoAceV、CoFish_wsの関係を評価した。これらのキットは、消費者向けブランドへの大量のなりすましを支えた。その関係は研究者の評価であり、ここで独立して確認した所有関係ではない。[S44]
- **限界。** 調査の大きな送信量は、より広い活動を対象とする。日本の被害者数や詐欺の成功件数として言い換えてはならない。妨害の実施は、キットや運営者が恒久的に排除されたことを意味しない。[S44]
- **対応。** 防御側は、ブランド監視、決済詐欺の兆候、利用者からの通報を組み合わせるべきである。妨害後は代替ドメインと変更された誘導文を確認する必要がある。強い認証と、認証情報窃取の疑いへの迅速な対応も継続すべきである。

## 追加事例 AC: メーカー：ランサムウェアで生産停止

- **概要。** メーカーは、ランサムウェアにより生産が停止したと公表した。[S46]
- **範囲。** 公表後も、調査と復旧計画の策定が続いた。[S46]
- **確認されたこと。** リモートアクセスの認証とバックアップの保護を確認する必要があった。[S46]
- **限界。** 生産停止だけでは、顧客が使用する製品の侵害は裏付けられない。[S46]
- **対応。** 多要素認証を適用し、再開計画を承認する前に隔離した環境での復旧を検証する。

## 追加事例 AD: 楽天証券：テスト環境の対象は二つの口座区分

- **概要。** 楽天証券は、テストシステムに関係する不正アクセスを公表した。全国向けの経済報道は情報露出の可能性を伝えた。その後の同社通知は、金融庁による報告徴求を確認した。[S49] [S48]
- **時系列。** 同社は 11 月 16 日に不正アクセスの疑いを検知した。その後の調査で、11 月 11 日に情報が漏えいした可能性があると判明した。初回通知は 11 月 17 日だった。報告徴求に関する通知は 11 月 19 日に続いた。[S47] [S48]
- **確認事項。** 一つの区分では、最大 4,470,000 口座について詳細な個人情報と金融情報が対象となった。別の区分では、最大 11,250,000 口座の顧客コードとログイン識別子が対象だった。過去に閉鎖された口座も含まれた。[S47]
- **限界。** 発表は区分間の重複を確定していないため、合計してはならない。パスワードや取引暗証番号の漏えい、関連する不正取引は確認されなかった。テストデータの露出可能性と、確認済みの口座不正取引は異なる。[S47]
- **対応。** 防御側は、テスト環境から不要な本番由来情報を削除すべきである。機微な項目を残す場合は、同等のアクセス管理を適用する必要がある。対応では、本人情報の露出と取引用秘密情報の侵害を、それぞれに適した証拠で別々に評価すべきである。

## 追加事例 AE: マネックス証券：口座開設書類に委託先のリスク

- **概要。** マネックス証券の 11 月 13 日の中間報告は、口座開設の委託先からの漏えい可能性を説明した。全国テレビ報道は、申込未完了の情報を含む更新後の範囲を伝えた。[S51]
- **時系列。** 委託先は 10 月 18 日に事案を検知し、10 月 19 日に不正アクセスを遮断した。11 月 13 日は、先行する事案の範囲更新であり、11 月の新たな攻撃を示すものではない。[S50]
- **確認事項。** 最大範囲には、重複や未完了の申込みを含むメールアドレス約 1,130,000 件があった。さらに、本人確認書類画像 1,592 件に影響の可能性があった。同社は、対応する人数の確認を続けていた。[S50]
- **限界。** メールアドレスの記録と書類画像を、人数として加えてはならない。ログインと取引の認証情報は別のデータベースにあり、漏えいしていなかった。委託先の調査中、一部の口座開設機能は停止が続いていた。[S50]
- **対応。** 防御側は、未完了の申込データと本人確認画像の保存を最小限にし、委託先の分離を検証すべきである。証券会社の継続計画では、窓口が口座開設の停止と取引の可用性を区別できるようにする必要がある。情報区分ごとに保護策が異なる理由も説明すべきである。

## 追加事例 AF: SBCメディカル：顧客履歴と職員情報の範囲が重複

- **概要。** SBCメディカルグループは、日本のシステムに影響する不正アクセスを公表した。日本語の企業発表とその後の報道は、顧客情報と職員記録を説明し、別のクリニック管理サービスの事案も示した。[S52] [S54]
- **時系列。** グループは 11 月 16 日に事案を検知した。投資家向け通知の日付は米国の 11 月 18 日で、日本の発表は 11 月 19 日に続いた。これらは、同じ公表の流れにおける日付である。[S53]
- **確認事項。** 基本情報の区分は 1,624,000 人を対象とした。予約、相談、口コミ、モニター関連のメタデータの区分には重複があった。企業発表は、職員アカウントと人事書類も特定した。また、過去の顧客パスワードが暗号化されずに保存されていたと説明した。[S52]
- **限界。** モニター区分はメタデータとファイル名に関するもので、写真の漏えいではなかった。電子カルテとMySBCの窃取は確認されていない。別のクリニック管理サービスへのアクセスから、共通の攻撃者や同じ対象集団を導くことはできない。[S52] [S53]
- **対応。** 防御側は、診療、予約、マーケティング、人事のシステムを分離すべきである。平文の秘密情報が確認された場合は、パスワードの使い回しに対応する必要がある。通知では、重複区分を説明し、誤解を招く顧客総数を作らないようにすべきである。

## 追加事例 AG: 六花亭：カードを保存しなくても決済画面から露出

- **概要。** 六花亭は、オンラインショップの決済画面の改ざんを公表した。初回通知の報道後、11 月 21 日の公式更新は、情報漏えいの可能性がある範囲を広げ、不正利用の報告例を説明した。[S56]
- **時系列。** 対象の入力期間は、10 月 21 日 21:00 から 11 月 18 日 11:00 までだった。初回通知は 11 月 18 日に公表された。カードの不正利用に関する報告は、11 月 20 日に確認された。[S55]
- **確認事項。** 改ざんされた決済画面のソフトウェアは、顧客の入力情報を取得できる状態だった。店舗側にカード番号のデータベースがなくても起こり得る。第 2 報は、氏名、住所、連絡先の漏えい可能性を追加した。[S55]
- **限界。** 現在の調査結果は、対象となる可能性があるすべての入力情報が、持ち出されたり悪用されたりしたとは確認していない。確認された不正利用報告 1 件を、影響可能性のある全体の結果として説明すべきではない。[S55]
- **対応。** 同社はカード再発行を依頼した。防御側は、決済画面のスクリプトとブラウザー側の変更を監視し、外部の決済連携を検証すべきである。顧客向け案内は、カードの危険と、購入時に入力する個人情報の両方を扱う必要がある。

## 追加事例 AH: アララ：メールアドレス件数を人数と区別

- **概要。** アララは、メール配信基盤に影響する不正アクセスを確認した。全国報道は、公表されたメールアドレス件数を伝えた。[S58]
- **時系列。** 第 3 報は、10 月 27 日を偵察、10 月 28 日から 31 日を活動期間とした。全サービスは 10 月 31 日に停止した。確認した提供会社の最新更新は 11 月 6 日で、直近の対象期間より前だった。[S57]
- **確認事項。** アララは、メールアドレス 81,329,467 件が外部に持ち出されたことを確認したと報告した。この件数は、重複のない人数を示すものではない。顧客ごとの属性情報も一部で関係した。提供会社は最大 380 社と、配信機能の悪用を調べていた。[S57]
- **限界。** メールアドレス件数は、重複のない人数ではない。同じ期間に追加のクラウドデータが見つかったことは、新たな攻撃の確認にはならない。この事案は、本章の別のメール配信事業者や決済基盤の事案とは別である。[S57]
- **対応。** 防御側は、顧客環境ごとの項目を点検し、送信権限を制限し、予期しない送信を監視すべきである。委託先の通知は、数字の単位がアドレス、メッセージ、記録、人数のどれかを示す必要がある。確認済みの事項と未解明の点も区別すべきである。

## 追加事例 AI: メッセージ配信事業者：共有基盤の露出が顧客に波及

- **概要。** メッセージ配信事業者は共有基盤の事案を更新し、その後、顧客が下流での影響を公表した。[S59] [S60] [S61]
- **範囲。** 事業者と顧客の公表は、サービスの関係における異なる範囲を説明していた。[S59]
- **確認されたこと。** 事業者が保管する顧客の記録に情報漏えいの影響が生じた。[S59]
- **限界。** 事業者と顧客の対象集団は重複する可能性があり、実人数として合算してはならない。[S59]
- **対応。** 一括出力を制限し、顧客との連絡に使う代替経路を用意する。

## 追加事例 AJ: GMOインターネット：仮想デスクトップに取引セッションのリスク

- **概要。** GMOインターネットは、取引ツールの利用者が使う顧客向け仮想デスクトップでマルウェアを確認した。報道は、恐喝の脅しと顧客自身の端末への影響可能性に対する同社の対応を伝えた。[S64]
- **時系列。** 顧客からの問い合わせは 10 月 19 日に届いた。マルウェアは 10 月 20 日に確認され、影響の可能性があるサーバーは 10 月 21 日に停止された。後の通知は、10 月 27 日の顧客情報の公開を説明した。[S62] [S63]
- **確認事項。** 影響の可能性がある範囲は 26,739 サーバーだった。取引ツールに保存された認証情報が盗まれ、不正利用された可能性があった。顧客からは身に覚えのない取引が報告された。同社は、認証情報の変更とともに、既存の取引セッションの終了も案内した。[S62] [S63]
- **限界。** 影響の可能性があるサーバー数は、侵害が確認された件数や人数ではない。顧客端末に関する攻撃者の脅しは、すべての端末が暗号化された証拠にならない。通知は、全顧客に同じ結果が起きたとは確認していない。[S63]
- **対応。** 防御側は、自動実行用ホストの調査、有効なセッションの無効化、保存された取引用認証情報の交換を一緒に行うべきである。金融対応部門は、個別の不正取引を基盤の事案に結び付ける前に、取引記録とホストの調査結果を照合する必要がある。

### 追加事例 AK: 消費者向けアプリ：利用情報の保護が必要

- **概要。** 消費者向けアプリの運営者は、顧客関連情報への不正アクセスを確認した。 [S65]
- **範囲。** 公表内容は、不正な活動の開始時点や終了時点を裏付けていない。 [S65]
- **確認されたこと。** 利用に関係する情報が影響範囲に含まれた。 [S65]
- **限界。** 通知は、外部への持ち出しを確認しておらず、影響する実人数も示していない。 [S65]
- **対応。** 利用情報のデータ群を保護し、顧客への案内では確認済みのアクセスと持ち出しを区別する。

## 5.3 業種ごとの判断

共通して必要なのは、何を封じ込めるか、その依存関係を正確に特定することである。予約サービス、返金フォーム、委託先アカウント、保存された研究用の鍵によって、対応が検知元のシステムの外に広がることがある。対象組織は、その依存関係に技術と業務の両方の責任者を置く必要がある。

顧客の対応は、情報区分に応じて決めるべきである。本人確認書類画像、暗号化されていないパスワード、暗号化データ、顧客識別子、購入履歴では、意味が異なる。件数が変わった場合も、利用企業が後日更新を公表した場合も、通知はこの区別を維持すべきである。

## 5.4 匿名の事案と広がる情報流出への注意

警察庁の上半期報告には、2026 年 1 月に飲料メーカーで発生したランサムウェア事案が記載されている。社名は公表されていない。警察はLockBitを特定し、1 TBを超えるデータを復元した。復元日は示されていない。この公的な事例は、証拠の保全と復旧支援の相談の重要性を示す。被害組織名や復旧期限を推定する根拠にはならない。 [S66]

JPCERT/CCの 10 月の注意喚起は、国内の情報流出で複数の手口を区別している。APIの悪用、アプリケーションサーバー上のシェル、既知の脆弱性、管理上の弱点などである。更新が加わっても、全事例に共通の実行主体、欠陥、侵入経路があったとはいえない。自組織の公開アプリケーションとアクセスの証拠を調べる必要がある。 [S73]

警察庁は 11 月 6 日、2026 年に確認された大規模な個人情報流出について合同捜査を発表した。捜査を共有することは、本章の全事案に共通の実行者がいる証拠ではない。各事案の日付と範囲を別々に保つ。 [S82]

## 5.5 原文の公表に基づく追加事例

以下の 137 件の短い説明は、上記の詳細事例を補う。組織の特定につながる日付、数値、サービスの詳細は非公開とした。委託先と顧客の通知には重複する対象集団が含まれる場合がある。行数は全国のインシデント数や被害組織数を示さない。

N001

ある組織はバックアップ媒体の紛失を公表した。外部への漏えいは確認されていない。媒体の保管と棚卸しを徹底する。 [S163]

### N002

ある組織はアプリケーションへのアクセスを通じた情報漏えいを確認した。認可を検証し、一括取得を制限する。 [S167]

### N003

公的機関は、リモートアクセス機器を経由した不正アクセスにより、職員・委託先の記録が流出した可能性を公表した。リモートアクセスの管理を見直し、影響を受けた保守用アカウントを失効させる。 [S114]

### N004

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S169]

### N005

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S173]

### N006

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S164]

### N007

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S122]

### N008

ある組織は情報の不正閲覧を確認した。閲覧だけでは外部への複製は裏付けられない。認可を検証し、アクセスログを確認する。 [S120]

### N009

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S168]

### N010

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S176]

### N011

ある組織はランサムウェアによる障害を公表した。サービス停止だけでは情報窃取は裏付けられない。隔離した環境での復旧を試し、代替経路を維持する。 [S166]

### N012

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S193]

### N013

ある組織は委託先に関係する情報流出の可能性を公表した。影響する顧客の範囲を確認し、委託先のアクセスを見直す。 [S177]

### N014

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S121]

### N015

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S175]

### N016

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S165]

### N017

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S201]

### N018

ある組織はランサムウェアによる障害を公表した。サービス停止だけでは情報窃取は裏付けられない。隔離した環境での復旧を試し、代替経路を維持する。 [S95] [S96]

### N019

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S191]

### N020

ある組織はアプリケーションへのアクセスを通じた情報取得の可能性を公表した。認可を検証し、不審な一括取得を調べる。 [S179]

### N021

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S186]

### N022

ある組織は認証情報を含む情報漏えいを確認した。影響する認証情報を失効させ、依存するサービスへのアクセスを調べる。 [S195]

### N023

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S196]

### N024

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S178]

### N025

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S185]

### N026

ある組織は認証情報を含む情報漏えいを確認した。影響する認証情報を失効させ、依存するサービスへのアクセスを調べる。 [S184]

### N027

ある組織は認証情報を含む情報漏えいを確認した。影響する認証情報を失効させ、依存するサービスへのアクセスを調べる。 [S183]

### N028

ある組織は個人情報を含むファイルの不正ダウンロードを確認した。機微なファイルへのアクセスを制限し、取得ログを保存する。 [S119]

### N029

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S188]

### N030

ある組織は委託先に関係する情報漏えいを確認した。委託先の保管するコピーを見直し、影響する顧客への通知を調整する。 [S194]

### N031

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S204]

### N032

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S198]

### N033

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S172]

### N034

ある組織は委託先に関係する情報漏えいを確認した。委託先の保管するコピーを見直し、影響する顧客への通知を調整する。 [S180]

### N035

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S199]

### N036

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S187]

### N037

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S117]

### N038

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S118]

### N039

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S132]

### N040

ある組織は委託先に関係する情報流出の可能性を公表した。影響する顧客の範囲を確認し、委託先のアクセスを見直す。 [S182]

### N041

ある組織は認証情報を含む情報漏えいを確認した。影響する認証情報を失効させ、依存するサービスへのアクセスを調べる。 [S102] [S103] [S104]

### N042

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S150]

### N043

ある組織はアプリケーションへのアクセスを通じた情報漏えいを確認した。認可を検証し、一括取得を制限する。 [S151]

### N044

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S152]

### N045

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S153]

### N046

ある組織は認証情報を含む情報漏えいを確認した。影響する認証情報を失効させ、依存するサービスへのアクセスを調べる。 [S154]

### N047

ある組織は個人情報を含むファイルの不正ダウンロードを確認した。機微なファイルへのアクセスを制限し、取得ログを保存する。 [S155]

### N048

ある組織はアカウントへの不正アクセスを確認した。アカウントの不正利用だけではサーバー侵入は裏付けられない。認証を強化し、影響するセッションを失効させる。 [S156]

### N049

ある組織はクラウド認証情報の不正利用を確認した。影響するキーを失効させ、サービスの権限を制限する。 [S157]

### N050

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S158]

### N051

ある組織は委託先に関係する情報漏えいを確認した。委託先の保管するコピーを見直し、影響する顧客への通知を調整する。 [S243]

### N052

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S171]

### N053

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S181]

### N054

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S197]

### N055

ある組織は委託先に関係する情報流出の可能性を公表した。影響する顧客の範囲を確認し、委託先のアクセスを見直す。 [S130]

### N056

ある組織は決済ページの改ざんと決済情報の流出の可能性を公表した。決済スクリプトを点検し、決済事業者と対応を調整する。 [S146]

### N057

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S147]

### N058

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S148]

### N059

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S149]

### N060

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S189]

### N061

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S128]

### N062

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S144]

### N063

ある組織は認証情報を含む情報漏えいを確認した。影響する認証情報を失効させ、依存するサービスへのアクセスを調べる。 [S145]

### N064

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S244]

### N065

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S99]

### N066

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S115]

### N067

ある組織は認証情報を含む情報流出の可能性を公表した。露出した可能性のある認証情報を失効させ、関連するアクセスを見直す。 [S116]

### N068

ある組織は情報の不正閲覧を確認した。閲覧だけでは外部への複製は裏付けられない。認可を検証し、アクセスログを確認する。 [S140]

### N069

ある組織は認証情報を含む情報漏えいを確認した。影響する認証情報を失効させ、依存するサービスへのアクセスを調べる。 [S141]

### N070

ある組織はアカウントへの不正アクセスを確認した。アカウントの不正利用だけではサーバー侵入は裏付けられない。認証を強化し、影響するセッションを失効させる。 [S142]

### N071

ある組織はアプリケーションへのアクセスを通じた情報漏えいを確認した。認可を検証し、一括取得を制限する。 [S143]

### N072

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S170]

### N073

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S134]

### N074

ある組織はアカウントへの不正アクセスを確認した。アカウントの不正利用だけではサーバー侵入は裏付けられない。認証を強化し、影響するセッションを失効させる。 [S135]

### N075

ある組織は認証情報を含む情報漏えいを確認した。影響する認証情報を失効させ、依存するサービスへのアクセスを調べる。 [S136]

### N076

ある組織はアカウントへの不正アクセスを確認した。アカウントの不正利用だけではサーバー侵入は裏付けられない。認証を強化し、影響するセッションを失効させる。 [S137]

### N077

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S138]

### N078

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S139]

### N079

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S229] [S230]

### N080

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S240]

### N081

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S245]

### N082

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S247]

### N083

ある組織は報酬に関する不正な活動を公表した。アクセスの管理を見直し、アカウントの不正利用を調べる。 [S248]

### N084

ある組織はアプリケーションへのアクセスを通じた情報取得の可能性を公表した。認可を検証し、不審な一括取得を調べる。 [S174]

### N085

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S190]

### N086

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S100] [S101]

### N087

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S94]

### N088

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S98]

### N089

ある組織は委託先に関係する情報漏えいを確認した。委託先の保管するコピーを見直し、影響する顧客への通知を調整する。 [S111]

### N090

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S123]

### N091

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S228]

### N092

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S112]

### N093

ある組織は不正アクセスと保存情報の変更を確認した。認可を見直し、アクセスを復旧する前に情報の完全性を検証する。 [S131]

### N094

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S219] [S220]

### N095

地方公共団体は、住民向け通知システムがランサムウェアで停止したと公表した。復旧は目標段階であり完了ではない。緊急情報の代替経路を検証する。 [S246]

### N096

ある組織は委託先に関係する情報流出の可能性を公表した。影響する顧客の範囲を確認し、委託先のアクセスを見直す。 [S105] [S106] [S107]

### N097

ある組織は、調査した顧客システムからの情報持ち出しを示す証拠はなかったと公表した。委託先側のすべての露出が解明されたわけではない。対象環境を個別に検証する。 [S161]

### N098

ある組織は情報の不正閲覧を確認した。閲覧だけでは外部への複製は裏付けられない。認可を検証し、アクセスログを確認する。 [S108]

### N099

ある組織は認証情報を含む情報流出の可能性を公表した。露出した可能性のある認証情報を失効させ、関連するアクセスを見直す。 [S110]

### N100

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S129]

### N101

ある組織は業務文書への不正アクセスを確認した。文書へのアクセスを制限し、監査ログを保存する。 [S160]

### N102

ある組織は委託先に関係する情報流出の可能性を公表した。影響する顧客の範囲を確認し、委託先のアクセスを見直す。 [S223] [S224]

### N103

ある組織は認証情報を含む情報流出の可能性を公表した。露出した可能性のある認証情報を失効させ、関連するアクセスを見直す。 [S227]

### N104

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S231] [S232] [S233]

### N105

ある組織は委託先に関係する情報漏えいを確認した。委託先の保管するコピーを見直し、影響する顧客への通知を調整する。 [S241]

### N106

ある組織は委託先に関係する情報流出の可能性を公表した。影響する顧客の範囲を確認し、委託先のアクセスを見直す。 [S242]

### N107

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S202]

### N108

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S205]

### N109

通知サービス事業者は、認証情報を含む情報漏えいを確認した。影響する認証情報を更新し、セッションを終了し、保存パスワードの保護を検証する。 [S109]

### N110

ある組織は決済ページの改ざんと決済情報の流出の可能性を公表した。決済スクリプトを点検し、決済事業者と対応を調整する。 [S125]

### N111

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S126]

### N112

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S127]

### N113

ある組織は委託先に関係する情報流出の可能性を公表した。影響する顧客の範囲を確認し、委託先のアクセスを見直す。 [S206]

### N114

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S216]

### N115

ある組織は認証情報を含む情報漏えいを確認した。影響する認証情報を失効させ、依存するサービスへのアクセスを調べる。 [S217]

### N116

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S218]

### N117

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S221]

### N118

ある組織はアカウントへの不正アクセスを確認した。アカウントの不正利用だけではサーバー侵入は裏付けられない。認証を強化し、影響するセッションを失効させる。 [S222]

### N119

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S225] [S226]

### N120

ある組織は委託先に関係する情報流出の可能性を公表した。影響する顧客の範囲を確認し、委託先のアクセスを見直す。 [S238]

### N121

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S239]

### N122

通知サービス事業者は、不正な送信と連携アクセスの不正利用を公表した。連携用の秘密情報を失効させ、送信の管理を検証する。 [S200]

### N123

公的機関は、ファイル共有で意図した受領者以外のアクセスと情報漏えいの可能性を公表した。共有権限を見直し、露出したリンクを失効させ、安全な代替経路を用意する。 [S97]

### N124

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S113]

### N125

ある組織はアカウントへの不正アクセスを確認した。アカウントの不正利用だけではサーバー侵入は裏付けられない。認証を強化し、影響するセッションを失効させる。 [S124]

### N126

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S207]

### N127

ある組織は委託先に関係する情報漏えいを確認した。委託先の保管するコピーを見直し、影響する顧客への通知を調整する。 [S208] [S209] [S210]

### N128

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S211] [S212]

### N129

ある組織は、委託先に関係する情報漏えいの可能性が高いと公表した。連携用の認証情報を見直し、外部ツールが利用できる情報を最小限にする。 [S213] [S214]

### N130

ある組織は情報の外部送信を確認した。送信された個別の記録は特定されていない。露出した可能性のある認証情報を更新し、保存するコピーを減らす。 [S215]

### N131

ある組織は不正アクセスと保存情報の変更を確認した。認可を見直し、アクセスを復旧する前に情報の完全性を検証する。 [S234]

### N132

ある組織は委託先に関係する情報流出の可能性を公表した。影響する顧客の範囲を確認し、委託先のアクセスを見直す。 [S235]

### N133

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S236]

### N134

ある組織は不正アクセスと保存情報の変更を確認した。認可を見直し、アクセスを復旧する前に情報の完全性を検証する。 [S237]

### N135

ある組織は認証情報を含む情報流出の可能性を公表した。露出した可能性のある認証情報を失効させ、関連するアクセスを見直す。 [S162]

### N136

ある組織は不正アクセス後の情報漏えいを確認した。影響する情報を確認し、アクセスを制限したうえでサービスを復旧する。 [S192]

### N137

ある組織は情報流出の可能性を公表した。対象となり得る範囲全体の持ち出しが確認されたわけではない。アクセスと保存情報を見直す。 [S203]

要点

01

テスト環境、委託先の保存先、過去のコピーから、不要な機微情報を削除する。

02

信頼を復旧する前に、接続先環境も含めて露出した認証情報とセッションを無効化する。

03

確認済み項目、現在の範囲、実際のサービス依存に基づき、復旧と顧客案内を決める。

---

章 06

# 可用性と接続機器のリスク

この章で答える問い

公的な発表は、サービス障害と接続機器について何を裏付け、
どのような運用判断につながるか？

## 4

対象範囲の異なる公的発表の節目


6.1 ウェブサイトの障害は影響を具体的に示す 74
6.2 国内からに見える通信にも注意する 74
6.3 運用上のシナリオと確認済みの事案を分ける 75
6.4 調査締切までの公的発表 75
6.5 主張と公的な証拠の範囲 76

章 06

# 可用性と接続機器のリスク

概要

日本の警察は、2 月のDDoS攻撃により、政府、交通、金融のウェブサイトに障害が生じたと報告した。接続機器は、攻撃元を隠すためにも悪用された。公開サービスの可用性とアクセスの信頼性は、別々に判断する必要がある。ウェブサイトの障害だけでは、情報窃取や産業プロセスの停止は裏付けられない。サービスの責任者を定め、復旧手順を試し、運用ネットワークへの不要な経路を取り除くこと。

## 6.1 ウェブサイトの障害は影響を具体的に示す

**障害の確認には、対象サービスと期間の特定が必要である。**

警察庁の9 月の報告書は、2026 年 2 月に複数の重要インフラ組織がDDoS攻撃を受けたと記している。ウェブサイトの閲覧障害を報告し、攻撃者を親ロシア系ハクティビストとみられるグループとしている。[S66]

この説明は、可用性への影響を裏付ける。それだけで、交通の運行、決済システム、工場の制御への干渉が確認されたことにはならない。公開ウェブサイトと、その背後のサービスでは、依存するシステムが異なる場合がある。

CISOが確認すべきなのは、公開サービスのそれぞれが、顧客のどの手続きに必要かという点である。案内ページの短時間の停止と、旅客情報、仕入先の受発注、事故連絡への障害では、影響が異なる。

対策を選ぶ前に、影響を定義すること。サービス責任者は、遅延を許容できる要求、照合が必要な取引、代替経路を必要とする利用者を特定する必要がある。これらは、事業部門も参加して行う運用上の判断である。

外部からの障害の主張は、時刻、対象機能、実際の顧客影響を示す証拠とともに、対応対象として扱うこと。攻撃者の発言は調査のきっかけになるが、事故の説明は組織自身の確認結果に基づく必要がある。

対応チームは、要求の失敗、アプリケーションの性能低下、サービスの利用不能も区別すること。それぞれ、必要な判断が異なる場合がある。すべてのエラーを全面停止と表現しないこと。

## 6.2 国内からに見える通信にも注意する

**国内のアドレスだけでは信頼性を判断できない。**

7 月に、警察庁、総務省、NICTは、家庭用機器がレジデンシャルプロキシとして第三者の通信を中継する仕組みを説明した。実際の攻撃者が別の場所にいても、接続先には家庭のアドレスが見える場合がある。[S72]

これは、国内の通信元を安心材料としている組織に関係する。見慣れた国や個人向け回線からの接続であっても、アカウント管理、取引確認、利用者の通常の行動との整合性を確かめる必要がある。

同じ注意喚起は、未承認の機器を業務ネットワークに接続させず、IoTのネットワークを業務システムから分離することを推奨している。これらは、自組織の環境が犯罪に悪用されるリスクへの対策である。[S72]

機器の所有者と攻撃者の区別も重要である。通信を中継している機器の所有者が、その動作を知らない場合がある。責任を判断する前に、その機器が担った役割を調べる必要がある。

管理対象の環境では、各機器を責任者と業務上の目的にひも付けること。管理されていない動画視聴端末、カメラ、ルーターも、サーバーと同様に確認が必要である。必要性がなくなっても、ネットワークへの接続が残る場合があるためである。

保守を続けられない機器については、交換、分離、撤去のいずれかを明確に決めること。責任者のいない恒久的な例外は、一時的な制約を、ネットワークに残り続ける経路へと変えてしまう。

## 6.3 運用上のシナリオと確認済みの事案を分ける

本章で用いた閲覧可能な公的資料は、ウェブサイトの障害と接続機器の悪用を記録している。これらの資料だけでは、日本の冷凍・冷蔵設備の故障や産業プロセスの停止は確認できない。

以下は分析上のシナリオであり、日本で報告された事案ではない。産業用の制御機器が一般の業務端末と接続を共有し、保守事業者から遠隔保守を受けている。許可されていないセッションにより、運転状態が変更される。

この場合の影響は、公開ウェブサイトの障害とは異なる。可用性の対策では、対象プロセス、安全な状態、復旧を担当する人を考慮する必要がある。一律にインターネット接続を遮断すると、運用に影響する場合がある。

IT部門と運用部門は、遠隔アクセスを承認できる人、終了できる人、通信が失われてもプロセスを安全に保つ方法を、一緒に確認すること。事故の前に、仕入先の責任も合意しておく必要がある。

運用担当者の立ち会いの下で、復旧を試すこと。バックアップが役立つのは、必要な設定を復元し、安全な動作を確認できる場合である。受け入れの判断は、サービスまたはプロセスの責任者が行う。

## 6.4 調査締切までの公的発表

以下の日付は、公的資料の公開日である。9 月の報告書が記す2 月の活動については、報告書の公開日が攻撃日を意味するわけではない。

**2026年7月21日** — **警察庁、総務省、NICT**
レジデンシャルプロキシとして悪用される家庭用IoT機器への対策を公表。対象は、攻撃元の見え方と機器の管理である。[S72]

**2026年9月10日** — **警察庁**
1〜6 月の報告書で、2 月のDDoSによる政府、交通、金融のウェブサイト障害を報告。本章の証拠からは、物理的なサービスの停止は確認されていない。[S66]

**2026年10月15日** — **警察庁**
10 月 8 日の米国裁判所の命令に基づく、日本向けフィッシング基盤の停止を発表。これは、別個の法執行対応である。[S74]

**2026年11月16日** **警察庁**
資産管理、公開範囲の縮小、APIの管理、委託先の監督を重視。この通知は対策の指針であり、被害組織を追加で数える事案ではない。[S75]

## 6.5 主張と公的な証拠の範囲

| 論点 | 攻撃者の主張 | 公的な説明 | 解釈 |
|---|---|---|---|
| ウェブサイトの障害 | 本評価では、攻撃者の主張を証拠として用いていない。 | 警察は、2月のDDoS活動でウェブサイトの閲覧障害が生じたと報告している。[S66] | 可用性への影響は裏付けられる。情報窃取には別の証拠が必要である。 |
| 情報窃取 | 本章では、攻撃活動全体で情報を窃取したという攻撃者の主張を採用していない。 | JPCERT/CCは、複数の手口による不正アクセスと情報漏えいの、別の一連の事案を説明している。[S73] | 事案を結び付ける証拠がない限り、この一連の事案をDDoSと一括りにしないこと。 |
| 物理的な影響 | 本章では、日本の産業設備を停止させたという攻撃者の主張を採用していない。 | 引用した資料の対象は、ウェブサイトの障害とレジデンシャルプロキシの悪用である。[S66][S72] | §6.3 の例は分析上のシナリオであり、日本で確認された事案ではない。 |

こうした区別により、事故の責任者は、証拠が増える途中でも正確に説明できる。関係のない主張を、単一の攻撃活動の説明にまとめてしまうことも防げる。

要点

**01**
公開サービスごとに、業務上の責任者、影響の基準、検証済みの代替連絡経路を定めること。

**02**
家庭向け回線からの通信元は参考情報として扱い、管理されていない接続機器を業務システムから分離すること。

**03**
OTについては、アクセス終了、安全な状態、復旧に関する判断を、プロセスの責任者と合意すること。

章 07

# 脅威アクター、攻撃活動、裏付けのある関係

この章で答える問い

証拠によって裏付けられるアクターと攻撃活動の関係は何か？

**146**

日本のラベルが付いたランサムウェア掲載。いずれも犯罪者の主張を記録したもの


7.1 関係図 78
7.2 APT-C-60 と正規サービスを使う配布 79
7.3 WaterPlumと採用を使うアクセス経路 80
7.4 DDoSとフィッシングのラベル 81
7.5 ランサムウェア掲載と地域比較 82
7.6 掲載の業種と月別分布 86
7.7 記録された配布経路の動作表 87
7.8 最近の技術的な注意喚起は製品ごとに判断する 88

章 07

# 脅威アクター、攻撃活動、裏付けのある関係

概要

日本の証拠には、恐喝活動のラベル、ベンダーが報告したDDoSの主張、公的に記録されたマルウェア攻撃が含まれる。これらは別々の集団である。Ransompediaは、指定期間に日本の掲載 146 件を記録し、ラベルは 43 種類あった。JPCERT/CCは、正規サービスを悪用したAPT-C-60 の配布を説明している。共同注意喚起はWaterPlumの採用を装う誘導を記している。各資料の証拠と帰属判断に沿い、自組織で対応するアクセス管理と復旧手順を検証すること。

## 7.1 関係図

この図は、資料と、その資料が裏付けるラベルや活動を結び付ける。線があるだけで、別々の攻撃活動に共通の運営者がいると判断するものではない。ランサムウェアに関する線は、Brandefense自身の掲載データを表す。公的資料とベンダーの報告は、それぞれ異なる種類の線で示している。[S2][S77][S78][S42][S44]

本人の投稿　転載　公式発表　公表資料　観測



本章では、恐喝のラベル、採用を装う攻撃、DDoSの主張、フォーラムの販売投稿を結び付ける運用上の関係は確認されていない。これらを単一の犯罪エコシステムとして扱う場合は、分析モデルとなる。本報告書では、サービスの復旧、本人確認、マルウェアの封じ込め、可用性に関する主張の評価を、別々の対応課題として扱う。

## 7.2 APT-C-60 と正規サービスを使う配布

JPCERT/CCの7 月 13 日の調査は、2026 年も日本の組織に対する攻撃が続いたと説明している。事例は、クラウドに置かれた圧縮ファイルへのスピアフィッシングのリンク、または不正な添付ファイルから始まる。圧縮ファイルには、次の配布処理を始めるショートカットが含まれる。JPCERT/CCは、その結果使われるマルウェアをSpyGlaceと特定している。[S77]

資料は、後の段階で正規の開発サービスやコンテンツ配信サービスが使われたと記している。Windowsの標準プログラムからJavaScriptを開始する動作も説明している。許可済みの接続先や署名付きのツールだけでは、一連の動作が安全だと判断できない理由が分かる。サービス提供者を、この攻撃活動の運営者と特定したものではない。[S77]

防御側は、不審なダウンロードの前後関係を保全すること。元のメッセージ、ダウンロードした圧縮ファイル、利用者の操作、子プロセス、その後の通信が対象である。後の接続先が正規サービスでも、通常と異なるショートカットからスクリプトへの連続した動作を調べること。アプリの方針を変更する前に、正当な業務上の必要性を確認し、リスクに見合う制限を適用すること。

### APT-C-60

JPCERT/CCが整理したキャンペーン | 帰属は引用元が述べる範囲に限る

日本、2026年

2026-07-13
標的型メール、圧縮ファイル、ショートカット、正規サービスを使う配布経路からSpyGlaceへつながる。

主張された標的

引用元が扱う範囲に限る

公表資料での記載

[S77] 標的型メール、圧縮ファイル、ショートカット、正規サービスを使う配布経路からSpyGlaceへつながる。

評価

キャンペーンの識別はJPCERT/CCの評価である。本報告は独自の国家帰属を行わない。

確度
出典がその活動を報告したことへの確信度は高い。未解決の制約は残る

## 7.3 WaterPlumと採用を使うアクセス経路

9 月 18 日の共同注意喚起は、WaterPlumが採用やコーディング課題を装い、日本の人を含むIT技術者を狙っていると説明している。参加当局は、この活動を北朝鮮に帰属させている。これは当局の判断であり、本報告書が独自に国家への帰属を認定したものではない。[S78]

注意喚起は、不正なリモート就労と、日本でのラップトップファームの摘発も説明している。対象の活動期間は、2025 年 12 月〜2026 年 7 月である。国際的な端末、ウォレット、暗号資産の数値は、日本の被害総数ではない。採用の接触やリモート就労者がすべて悪意を持つ、という主張に読み替えないこと。[S78]

採用担当と技術担当は、知らないコードをどのように評価するか合意すること。本番環境へのアクセスや、再利用できる業務用認証情報のない、分離した環境を使うこと。採用担当者や応募者の本人確認は、既存の経路で行う。コーディング課題に悪意が疑われる場合は、関係する端末とアカウントの証拠を保全し、影響し得る連携先を確認すること。

### WaterPlum

合同当局が帰属を示したキャンペーン　帰属は引用元が述べる範囲に限る

日本、2026年

2026-09-18
日本を含むIT専門家を狙う採用やコーディング課題の誘い。

主張された標的

引用元が扱う範囲に限る

公表資料での記載

[S78] 日本を含むIT専門家を狙う採用やコーディング課題の誘い。

評価

北朝鮮への帰属は当局の評価である。国際的な件数は日本の被害者数ではない。

確度
出典がその活動を報告したことへの確信度は高い。未解決の制約は残る

2026 年の観測期間より前の公的なスパイ活動の注意喚起は、2026 年の事案数ではなく過去の背景情報として扱う。2025 年 2 月に警察庁とNISCは、2019 年頃から同注意喚起時点までに日本の政府関連、シンクタンク、学術、半導体、製造分野などを狙った一連の攻撃を整理した。[S256] 当局はこれらの攻撃をMirrorFaceによる、中国の関与が疑われる組織的なサイバー攻撃と評価した。[S256] 同注意喚起は不正な添付ファイルやダウンロードリンクを含むメールと、インターネットに接続された機器の脆弱性の悪用を説明しており、2026 年の対象期間より前の公表であるため 2026 年のプロファイルからは除外している。[S256]

## 7.4 DDoSとフィッシングのラベル

Check Pointの9 月の調査は、NoName057(16)が再開した攻撃活動で、8 月 24〜30 日に日本の組織 26 社・団体に対する 66 件の主張があったと報告している。説明の中心はDDoSの主張で、監視設備へのアクセスの主張も一件ある。これは、独立に確認された障害 66 件や、侵入が立証された組織 26 社・団体を意味しない。[S42]

Proofpointの10 月の調査は、日本を狙う三つのフィッシングキットと、その共通の起源や重複するアフィリエイトを説明している。言語や活動基盤に関する評価は、ベンダーによるものである。キットを使ったすべてのメッセージについて、国籍、国家の指示、共通の運営者を立証するものではない。警察庁は、別に、攻撃基盤の停止への関与を報告している。[S44][S74]

ブランドがかたられただけでは、そのブランドの組織で情報漏えいが起きたことにはならない。最初の対応は、実際のサインインや支払の手順を守り、利用者に正当性を確認できる報告経路を用意することである。基盤の停止の発表は、活動が恒久的になくなった証拠ではない。

### NoName057(16)

ベンダー報告に登場するDDoS主張の名称 | 帰属は引用元が述べる範囲に限る

日本、2026年

2026-09-07
8月24–30日の日本関連の主張を対象とする。

主張された標的

引用元が扱う範囲に限る

公表資料での記載

[S42] 8月24–30日の日本関連の主張を対象とする。

評価

主張の件数は、停止時間、データ窃取、物理プロセスへのアクセスを確認した件数ではない。

確度
出典がその活動を報告したことへの確信度は高い。未解決の制約は残る

## Japan-focused phishing kits

ベンダーが整理したフィッシングキットの関係　帰属は引用元が述べる範囲に限る

日本、2026年

2026-10-14
消費者・金融ブランドのなりすましと犯罪インフラの停止措置。

主張された標的

引用元が扱う範囲に限る

公表資料での記載

[S44] 消費者・金融ブランドのなりすましと犯罪インフラの停止措置。

評価

キットの系統、協力者、使用言語の評価は出典のベンダーによる。国籍や国家の指示を示すものではない。

確度
出典がその活動を報告したことへの確信度は高い。未解決の制約は残る

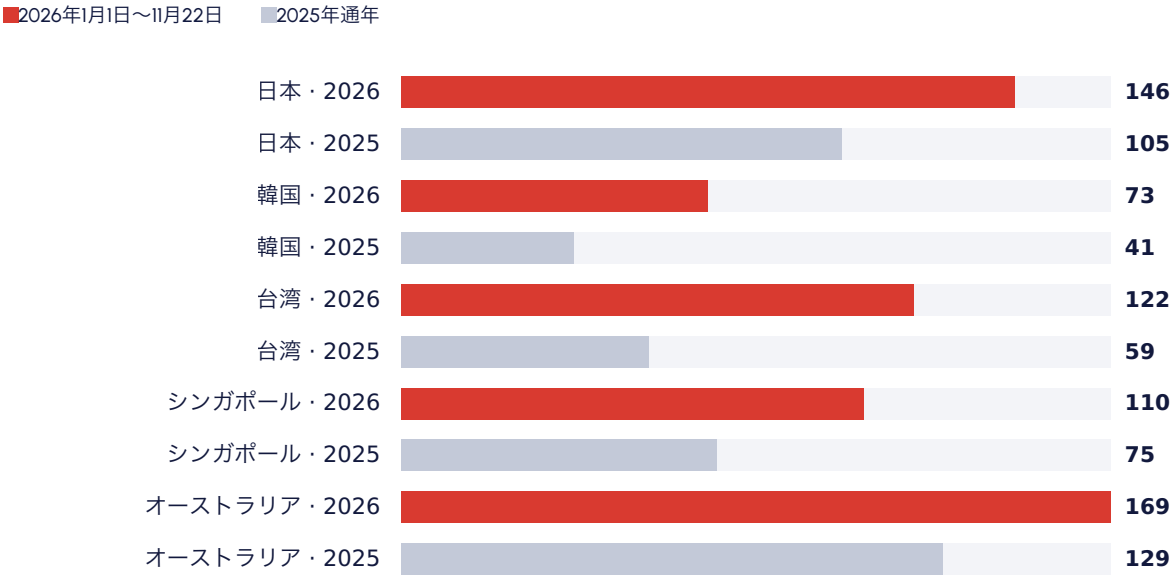
## 7.5 ランサムウェア掲載と地域比較

Ransompediaは、2026 年 1 月 1 日〜11 月 22 日の間に、日本のラベルが付いた掲載 146 件を記録している。2025 年の通年は 105 件であった。年の途中までと通年の比較であり、同じ期間で算出した増加率ではない。掲載は犯罪者による公開の主張で、同じ組織が繰り返し登場する場合がある。[S2]

図c08 は、日本の集計を、選定した比較対象と並べている。違いには、犯罪活動だけでなく、公表の慣行、国のラベル、資料の見え方も影響し得る。国の対策の有効性を測るものではない。

比較対象国は、背景を示すための例としてのみ選定したものであり、順位付けや政治的評価を意味するものではありません。

## 日本の観測掲載は 146 件。地域比較が示すのは主張であり、攻撃される確率ではない




出典：Ransompediaの国関連ラベル付き掲載（犯罪者側の主張）。[S2] 2026年は1月1日〜11月22日（終日は途中まで）、2025年は通年。期間と出典から見える範囲が異なり、国別リスクの順位ではない。

| 比較対象 | 指定期間 | 2025 年通年 | 比較する理由 |
|---|---|---|---|
| 日本 | 146 | 105 | 本報告書の対象 |
| 韓国 | 73 | 41 | 近隣の技術・産業分野との依存関係 |
| 台湾 | 122 | 59 | 半導体・製造業のサプライチェーン |
| シンガポール | 110 | 75 | 地域の金融・物流サービス |
| オーストラリア | 169 | 129 | 地域のサービス・重要インフラとの依存関係 |

日本の掲載には 43 種類のラベルがある。The Gentlemen、Qilin、Everestを合わせると 55 件、37.7%である。残るラベルは 91 件である。ラベルの頻度だけでは、個別の運営者、侵入方法、成功率は分からない。[S2]

| 掲載ラベル | 掲載件数 | 構成比 |
|---|---|---|
| The Gentlemen | 24 | 16.4% |
| Qilin | 19 | 13.0% |
| Everest | 12 | 8.2% |
| SafePay | 8 | 5.5% |
| NightSpire | 7 | 4.8% |

| 掲載ラベル | 掲載件数 | 構成比 |
|---|---|---|
| その他のラベル | 76 | 52.1% |
| 合計 | 146 | 100.0% |

掲載件数から、ラベルごとの侵入方法を推定していない。防御側は、自組織の初期侵入の証拠、復旧の準備状況、影響する情報の範囲を確認する必要がある。公表された一つの手法に対応する製品を購入しても、これらのラベルが表すあらゆる状況を解決できるわけではない。

## The Gentlemen

恐喝掲載のグループ名　国家への帰属は評価していない

日本、2026年

2026
対象期間に日本関連の掲載 24 件

主張された標的

掲載された対象群。被害組織名は記載しない

公表資料での記載

[S2] 保有する掲載件数：24。

評価

件数が示すのは確認した犯罪者側の主張である。実行者の人数、侵入の成功、暗号化、窃取、支払いは確認できない。

確度
保有する掲載件数への確信度は高い。個々の主張は未検証

## Qilin

恐喝掲載のグループ名　国家への帰属は評価していない

日本、2026年

2026
対象期間に日本関連の掲載 19 件

主張された標的

掲載された対象群。被害組織名は記載しない

公表資料での記載

[S2] 保有する掲載件数：19。

評価

件数が示すのは確認した犯罪者側の主張である。実行者の人数、侵入の成功、暗号化、窃取、支払いは確認できない。

確度
保有する掲載件数への確信度は高い。個々の主張は未検証

## Everest

恐喝掲載のグループ名　国家への帰属は評価していない

日本、2026年

2026
対象期間に日本関連の掲載 12 件

主張された標的

掲載された対象群。被害組織名は記載しない

公表資料での記載

[S2] 保有する掲載件数：12。

評価

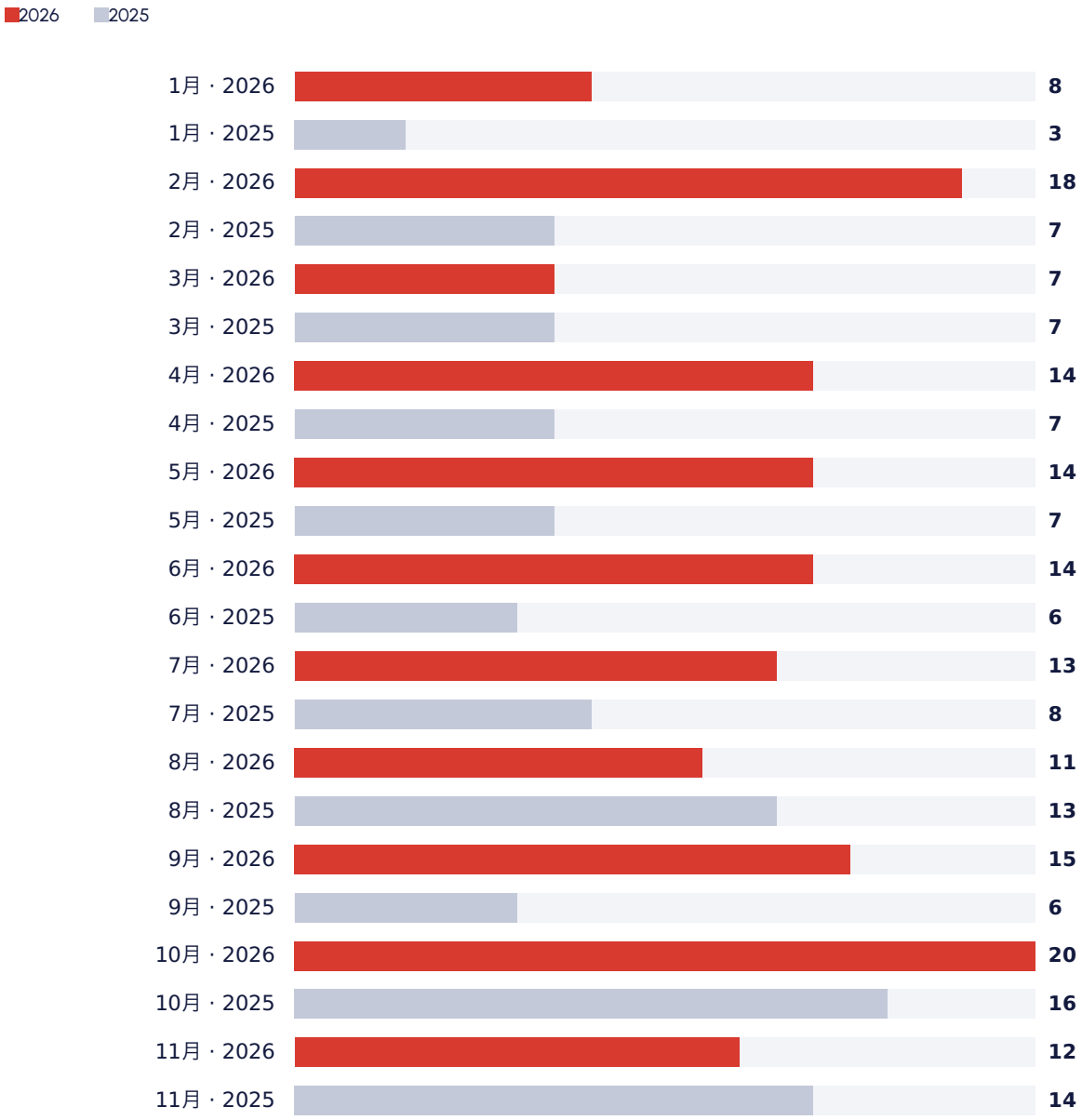
件数が示すのは確認した犯罪者側の主張である。実行者の人数、侵入の成功、暗号化、窃取、支払いは確認できない。

確度
保有する掲載件数への確信度は高い。個々の主張は未検証

## 7.6 掲載の業種と月別分布

図c10 は、掲載日を示している。10 月は 20 件、11 月の途中までの期間は 12 件である。これらの日付は、集計対象の掲載が公表された日を表す。侵入日や、実測した月ごとの攻撃頻度の変化を示すものではない。[S2]

### 掲載は年間を通じて存在。10 月は 20 件、11 月は途中までの集計




出典：Ransompediaの日本関連掲載（犯罪者側の主張）。[S2] 両年の1〜11月。2026年11月は1〜22日（終日は途中まで）、2025年11月は全月。同じ長さの期間による増加率ではない。

2025 年の棒は対応する月の全期間を示す。2026 年 11 月は途中までである。

以下の大きな業種区分では、小さな分類をまとめている。業種のラベルは、元の資料による説明である。掲載対象の具体的な事業や、企業の境界を独立に確認するものではない。

| 大きな業種区分 | 掲載件数 | 構成比 |
|---|---|---|
| 製造、建設、生産 | 40 | 27.4% |
| その他・複合的な活動 | 27 | 18.5% |
| 技術・通信 | 21 | 14.4% |
| 交通・旅行 | 19 | 13.0% |
| 医療・健康 | 14 | 9.6% |
| 教育 | 12 | 8.2% |
| 専門サービス | 7 | 4.8% |
| 小売・商業 | 6 | 4.1% |
| 合計 | 146 | 100.0% |

業種別の表示は、関係する事業継続上の要件を確かめるために使うこと。製造と物流には、事業部門と現場の参加が必要である。医療には、安全な代替診療手順が必要である。教育・技術分野の組織は、研究開発への特権アクセスを確認すること。掲載だけでは、どのシステムに影響があったかは分からない。

## 7.7 記録された配布経路の動作表

この表は、JPCERT/CCが説明した動作を、分析者がATT&CKの用語に対応付けたものである。資料の帰属判断の方法ではなく、すべての日本の組織で各手法が使われた証拠でもない。記載した動作は、資料中の事例によって裏付けられている。[S77][S90][S91][S92]

出典の調査で示された技術（戦術別）

| 初期アクセス | 実行 | 隠密化 |
|---|---|---|
| T1566.002<br>標的型メールのリンク。JPCERT/CCの記述に基づく分析上の対応付け | T1204.002<br>悪性ショートカット。JPCERT/CCの記述に基づく分析上の対応付け | T1218.005<br>Mshtaによるスクリプト処理。JPCERT/CCの記述に基づく分析上の対応付け |

出典が記述する挙動の分析上の対応付け。帰属の手法でも、全対象での実施を示す証拠でもない。[S77]

| 戦術または段階 | 資料に記された動作 | 防御側の証拠 |
| --- | --- | --- |
| 初期アクセス | ホストされた圧縮ファイルへのスピアフィッシングのリンク | 元のメッセージとダウンロード履歴 |
| 実行 | 利用者が圧縮ファイル内の不正なショートカットを開く | ファイルの入手元とプロセス生成の証拠 |
| ステルス（Stealth、隠密化） | Windowsの標準ツールが、埋め込まれたスクリプトの動作を開始する | 親子プロセスの連鎖とスクリプトの記録 |
| 後続段階の配布（ATT&CKの戦術ではない） | 後続のファイルが正規の開発サービスから届く | 接続先、プロセス、要求された内容を組み合わせた状況 |

提供者のドメインだけを一律に信頼しないこと。一方、報告書に悪用が記されただけで、正規プラットフォーム全体を遮断することも避けること。組織に関係するアカウント、内容、プロセスの順序を調べる必要がある。

## 7.8 最近の技術的な注意喚起は製品ごとに判断する

JPCERT/CCの11月18日の注意喚起は、高速化されたBase64デコード処理のCVE-2026-114938を扱う。OpenJDK 17.0.6以降の脆弱なビルドが含まれる。悪用には、x86-64のAVX-512 VBMI対応と、細工されたデータが脆弱な高速化処理に渡ることなどの条件が必要である。ARM64は影響を受けないとされる。[S89]

JPCERT/CCは11月18日時点で悪用を確認していなかった。この注意喚起は、日本での被害事案を示す証拠ではない。同梱ランタイムも含め、配備されたディストリビューション、完全なビルド、動作条件を確認する。[S89]

次の表は、影響を受ける上流ビルドの参照例とUbuntuでの修正例を示す。修正例は、基本バージョン、パッチ、ビルド、Ubuntuのリビジョンを分けて示す。導入したディストリビューションとパッケージの完全なリビジョンを確認する。同梱ランタイムでは、アプリケーションの提供元がサポートする修正を確認する。[S249] [S250] [S251]

| 系統 | 脆弱な参照ビルド | Ubuntuの修正例 |
| --- | --- | --- |
| OpenJDK 17 | 17.0.21.0.3 | Ubuntu 24.04: openjdk-17 基本版 17.0.21、パッチ 1、ビルド 2、リビジョン 1~24.04.1 |
| OpenJDK 21 | 21.0.13.0.3 | Ubuntu 24.04: openjdk-21 基本版 21.0.13、パッチ 1、ビルド 2、リビジョン 1~24.04.1 |
| OpenJDK 25 | 25.0.5.0.3 | Ubuntu 24.04: openjdk-25 基本版 25.0.5、パッチ 1、ビルド 2、リビジョン 1~24.04.1 |
| OpenJDK 27 | 27.0.1.0.3 | Ubuntu 26.10: openjdk-27 基本版 27.0.1、パッチ 1、ビルド 4、リビジョン 1~26.10.1 |

アプリケーション責任者は、更新後に稼働中のサービスを確認する。ビルドと設定を記録し、サポートされる暫定措置を終了する前にサービスの動作を試験する。

IPAの11月20日のPHP通知は、バージョン、機能、設定によって条件が異なる複数の脆弱性を扱う。次は系統別の確認範囲であり、適用の判断には個別の注意喚起を使う。The PHP Groupは、記載した11月のセキュリティリリースを確認している。[S80] [S252]

| PHP系統 | 確認が必要なバージョン | 修正版または対応 |
|---|---|---|
| 8.1 | 同系統の8.1.34以前 | サポート対象の系統へ移行するか、提供元の保守対象の修正を入手する |
| 8.2 | 同系統の8.2.36より前 | 8.2.36 |
| 8.3 | 同系統の8.3.37より前 | 8.3.37 |
| 8.4 | 同系統の8.4.28より前 | 8.4.28 |
| 8.5 | 同系統の8.5.13より前 | 8.5.13 |

この系統別一覧は、すべての脆弱性が記載されたすべてのバージョンに影響するという意味ではない。提供元のバックポートと組み込み製品は個別に確認する。既定の設定だけで安全とは判断せず、個別の注意喚起の条件と修正後の稼働アプリケーションを確認する。[S80]

要点

01
掲載ラベルと、資料が帰属判断を示した攻撃活動を分けること。

02
正規サービスが関わる場合でも、不審なプロセスやアカウントの連続した動作を調べること。

03
技術的な注意喚起への対応を完了とする前に、影響する製品、ビルド、設定を確認すること。

---

章 08

# 詐欺が狙う業務手順と委任されたアクセス

この章で答える問い

詐欺は連絡手段や委任されたアクセスをどのようにまたぎ、組織はどこで止めるべきか？

## 3

管理上の判断：支払権限、遠隔アクセス、アプリへの同意


8.1 経営者のなりすましは会話の場を移す 91
8.2 電話が従業員をアクセス経路に変える 91
8.3 アプリへの同意も復旧の対象にする 92
8.4 個人向けの経路から組織にも影響する 92
8.5 本人確認書類の保管が漏えいの影響を変える 93
8.6 決済カードの観測とその限界 93

章 08

# 詐欺が狙う業務手順と委任されたアクセス

概要

日本の公的な注意喚起は、経営者のなりすまし、銀行や税務サービスを装う電話、不正な決済アプリ、クラウドの同意機能の悪用を説明している。これらは複数の連絡手段を使い、従業員自身にアクセス権を与えさせる場合がある。対応には、支払権限、遠隔操作、アプリの権限、保管する本人確認書類を含める必要がある。支払やアクセスの変更は別の経路で確認し、従業員が不審な動作をすぐ止められる連絡経路を整えること。

## 8.1 経営者のなりすましは会話の場を移す

**見慣れた名前でも、指示に正当な権限があるとは限らない。**

IPAの3 月の注意喚起は、経営者名や会社名を使うメッセージを説明している。従業員にLINEグループを作らせ、招待コードを返信するよう求めていた。その後、業務上の指示を装って送金を求める場合がある。[S68]

この注意喚起の相談集計は、2025 年 12 月から始まっている。106 件の相談は、2026 年の被害件数ではない。別に、警察は 2026 年1〜6 月の経営者なりすまし詐欺について、認知件数 127 件、被害額約 3,880,000,000 円と報告している。[S66]

業務上の弱点は、連絡手段が変わる際に、権限の確認が引き継がれないことである。電子メールで緊急性を示した後、通常の確認が働きにくい少人数のグループへ会話を移す。

連絡手段が変わっても、承認の要件は変えるべきではない。経理部門には、通常と異なる指示を、権限のある本人に確認する既存の経路が必要である。不審な会話の中で返信しても、独立した確認にはならない。

新しい送金先の承認、口座残高の開示、経理担当者を含む業務グループの作成についても、誰に権限があるか明確にすること。幹部の表示名だけで、これらの規則を省略すべきではない。

従業員には、実際に手続きを止められる仕組みが必要である。詐欺かどうかを確定する前でも、送金を保留し、既知の同僚に確認し、不審な依頼を報告できるようにすること。

## 8.2 電話が従業員をアクセス経路に変える

警察庁の6 月の通知は、電話、遠隔操作ソフト、窃取した銀行認証情報を組み合わせる、法人口座を狙ったボイスフィッシングを警告している。犯罪者は、更新作業に見せながら、組織自身の端末を操作できる場合がある。[S67]

IPAの第二四半期の報告書にも、税務サービスの更新を装う、似た相談事例がある。電話の相手は電子メールアドレスを聞き出し、リンクを送り、ソフトをインストールさせた。別の従業員が不審に思い、やり取りを止めた。[S69]

これらの事例から、対応範囲を最初の電話だけに限定できないことが分かる。そのセッションで何にアクセスできたか、その端末からどのアカウントを使えたかを考慮する必要がある。安心させる更新画面が表示されても、無害だった証拠にはならない。

依頼していないソフトのインストール要求は、承認が必要な変更として扱うこと。従業員は、組織がすでに把握している連絡先で確認する必要がある。電話の相手が示した番号やリンクを、確認経路にしないこと。

すでに遠隔操作が行われた場合は、対応担当者へ明確な経路で連絡できるようにすること。端末の分離、証拠の保全、アカウントの保護、送金取消しに関する判断には連携が必要である。セッションが続いている間に、従業員がその場の判断で復旧を完結させようとすべきではない。

復旧計画では、確認した動作と、起きた可能性のある影響を区別すること。遠隔セッションは、アクセスの機会があったことを示す。すべての文書、ブラウザー内の秘密情報、金融口座が窃取されたと自動的に証明するものではない。

## 8.3 アプリへの同意も復旧の対象にする

**復旧では、アプリに委任された権限も確認する必要がある。**

IPAの第三四半期の報告書は、アプリへの同意が付与された後、従業員のMicrosoftアカウントから大量のメールが送信された事例を説明している。組織は、侵入経路と情報漏えいの有無を、まだ調査していた。[S70]

クラウドのアプリは、付与された権限で動作できるため、この事例は重要である。事故の調査では、アカウントのサインインやメールの動作とともに、同意とアプリの活動も確認する必要がある。

IPAは、監査ログ、サインインログ、付与された権限、メッセージトレース、転送設定、メールボックスのルールの確認を勧めている。利用者による同意の制限や、管理者によるアプリ承認も説明している。[S70]

CISOは、アプリのアクセス権に責任を持つ人を定める必要がある。アカウントの復旧はサービスデスクが担当し、企業向けアプリは別の管理者が管理している場合がある。対応手順で、これらの責任をつなげること。

アプリが承認済みか、何を実行できるか、そのアクセスが今も必要かを確認すること。利用者の問い合わせを完了しても、説明のつかない権限付与を有効なまま残すべきではない。

この考え方は、日常の管理にも当てはまる。委任されたアクセスを定期的に見直すと、根拠となったプロジェクト、従業員、仕入先との関係が終了した後も残る権限を見つけられる。例外には、責任者と見直し日を定めること。

## 8.4 個人向けの経路から組織にも影響する

9 月に、警察は、不正なスマートフォンアプリによる遠隔操作や、キャッシュレス決済サービスの不正送金を警告した。配布経路には、SNSの広告、メッセージ内のリンク、オンラインで知り合った相手が含まれる。[S81]

組織は、どの業務が従業員のスマートフォンに依存しているかを確認する必要がある。支払の承認、アカウントの復旧、業務連絡が、私用アプリと同じ端末で行われる場合がある。そのリスクに見合う規則が必要である。

規則では、許可するインストール元、報告経路、不正操作が疑われる端末の扱いを説明すること。従業員が、影響を受けた端末を信頼し続けることなく、必要な業務へのアクセスを維持する方法を知っている必要がある。

## 8.5 本人確認書類の保管が漏えいの影響を変える

個人情報保護委員会の11 月 18 日の注意喚起は、名称を公表していないレンタカー事業者への不正アクセスで、保管していた顔写真付き本人確認書類の画像が漏えいした事案を受けたものである。本人確認への使用後に画像を消去するよう求め、保存が必要な免許証番号の記録と区別した。[S71]

データの責任者が確認すべき点は明確である。組織に今も必要なのは、書類の画像だろうか。それとも、確認済みの属性と取引記録だけだろうか。

保存の判断では、利用目的、法的な要件、消去の責任を結び付けること。便利だからという理由でコピーを残すと、後の不正アクセスの影響が大きくなる場合がある。

本人確認書類を持っているだけで、応募者が正当な本人だと判断しないこと。9　月のWaterPlum共同注意喚起は、窃取した本人確認書類の画像が、技術職の不正な採用活動でなりすましに使われ得ると警告している。当局は、この攻撃活動を北朝鮮に帰属させている。[S78]

## 8.6 決済カードの観測とその限界

**カードの数値の対象範囲**

この限定的な観測から、現在の有効性、重複のないカード保有者数、全国のカード盗難の発生状況、不正利用の損失は分からない。

本報告書には、日本に関連する決済カードの観測が 303 件ある。記録の存在だけでは、カードが今も有効か、現在の顧客のものか、成立した取引に使われたかは分からない。この観測から、銀行への侵入は特定できない。[S5]

関係する正当な警告を受けた発行会社は、通常の不正利用対応の手順を通じて、実際のカードと口座の証拠を検証すること。観測件数だけでは、一斉再発行の根拠にならない。措置を選ぶ前に、実際の不正利用、口座の状態、顧客保護の必要性を確認すること。

要点

**01**
会話が電子メール、電話、チャットの間を移っても、支払の承認と別経路での確認を維持すること。

**02**
アカウント復旧の判断には、遠隔操作とクラウドアプリへの権限付与も含めること。

**03**
組織に適用される保存義務を確認し、利用目的が終了した本人確認書類の画像を消去すること。

章 09

# 銀行と金融サービスの依存関係

この章で答える問い

金融機関は、顧客への詐欺、委託先のリスク、自行のシステムをどう区別すべきか？

## 3

対応の軸：取引、情報、サービス継続


9.1 銀行分野の対象範囲 95
9.2 非本番システムにも実際の被害につながる情報が残る 95
9.3 リポジトリへのアクセスとデータベースへのアクセスは異なる 96
9.4 共有の決済サービスは提供先ごとに範囲を確認する 96
9.5 顧客への詐欺とアカウント復旧 97
9.6 監督と合同演習 97

章 09

# 銀行と金融サービスの依存関係

概要

金融分野の証拠は、残されたテスト環境、開発リポジトリ、委託先が提供する決済、顧客向けの詐欺など、異なる事象にまたがる。委託先の事故だけでは、すべての顧客の基幹システムへのアクセスは確認できない。データの記録だけでは、不正送金も確認できない。取引の完全性、情報漏えい、サービスの可用性は、別々の責任者が扱うこと。共通の原因を裏付ける自組織の証拠がある場合に、対応を結び付けること。

## 9.1 銀行分野の対象範囲

選定した銀行対象群は、主ドメイン 25 件である。端末との関連は少なくとも 39,061 件、うち従業員端末との関連は 29 件ある。過去の認証情報レコードとの関連は 16,437 件、現在の認証情報販売掲載は 12 ドメインで観測された。銀行インフラへの侵入を立証するものではない。[S3]

銀行の対象群は 25 の主要ドメインを含む。うち 22 に従業員関連と表示されていない端末との関連があり、10 に従業員端末との関連がある。従業員関連と表示されていない関連は 39,032 件である。顧客が端末を所有すると確定するものではない。[S3]

日本関連の決済カード観測 303 件のうち、本ポートフォリオの銀行に関係するものはごく一部である。認証情報や端末の観測と共通の出所を持つとは確認できない。銀行業種の評価値は公表しない。[S3][S5]

公開事例は、それぞれ異なる問いに答える。金融サービス事業者のテスト環境には、顧客と株主の記録があった。ソフトウェア企業グループのリポジトリに関する公表では、開発情報に影響があった。決済プラットフォームの事故はサービス提供先に影響し、顧客ごとの確認が必要であった。これらを、同じ種類の銀行への侵入と言い換えるべきではない。[S31][S28][S12]

§8 の決済カードの観測は、別の限定的な対象集団を示している。銀行の顧客口座、企業の認証情報、成立した不正取引を数えるものではない。

## 9.2 非本番システムにも実際の被害につながる情報が残る

金融サービス事業者は、残されていたテスト環境への不正アクセスを確認した。調査結果は、取引処理の侵害を裏付けていない。保存された業務情報とアカウントのアクセスを見直す。[S31]

対策上の教訓は、一つの環境にとどまらない。テストシステムには、プロジェクト終了後も、実際の連絡先、株主、顧客の情報や、有効なアクセス経路が残る場合がある。運用上の重要度が低くても、内容のリスクまで低いとは限らない。

実際の情報を含む非本番環境には、責任者、目的、終了日を定めること。認証とアクセスの記録は、情報の機微性に見合う注意を払って確認すること。元の目的が終了した場合は、適用される義務に従い、削除または個人を識別できなくする処理を行った証拠を示すこと。

完了を示す証拠には、対象環境、保管する情報の種類、アクセスに関する判断を含める必要がある。開発が終了したという説明だけでは、サーバー、コピー、アカウントを削除したことは分からない。

## 9.3 リポジトリへのアクセスとデータベースへのアクセスは異なる

金融ソフトウェアに関する公表は、個人情報の漏えいについての評価を、リポジトリの内容に限定している。本番データベースへのアクセスや漏えいはなかったと説明し、個人情報と内部の利用者識別子も区別している。対応の説明でも、これらの範囲を維持する必要がある。[S28]

それでも、リポジトリには、次の段階に役立つ情報が含まれる場合がある。設定、連携先の参照情報、配備の詳細、秘密情報などである。関係する委託先から通知を受けた組織は、自組織のどの連携に影響し得るか確認すること。関係する認証情報だけを更新し、接続先のサービスで結果を確認すること。

委託先のリポジトリの事故を、その金融機関の取引データベースに関する、裏付けのない主張に変えないこと。正当な経路で、影響するリポジトリ、情報の種類、連携の範囲を確認する。未解決の問いは、アプリケーション責任者と委託先管理の責任者が把握できるようにすること。

## 9.4 共有の決済サービスは提供先ごとに範囲を確認する

決済事業者は、影響する環境と、確認後に再開できる環境を区別した。復旧の判断には顧客ごとの証拠が必要となる。[S12]

顧客は、プラットフォーム全体の数値を自組織の通知に転記する前に、実際に利用する製品、環境、情報の流れを確認する必要がある。事実がまだ不十分な間のサービス停止は、保護のための措置である場合がある。一つの提供先の再開だけでは、すべての提供先が同じ状態だとは判断できない。

| 対応の軸 | 初期に確認する証拠 | 完了を示す証拠 |
| --- | --- | --- |
| 取引の完全性 | 正当な支払記録、決済の不一致、関係するアクセス | 取引の照合と不一致の解決 |
| 情報漏えい | 該当する製品、テナント、データの種類 | 文書化した範囲と報告義務の評価 |
| サービスの可用性 | 停止した機能、提供先の状態、代替手段 | 業務で検証した動作と、受け入れた残る制約 |

共有サービスに関する複数の通知に、同じ人や記録が含まれる場合がある。対象集団が別々だという証拠がない限り、下流の公表を合算して全国の総数にしないこと。共通の事故を参照できるようにしつつ、各金融機関の義務の評価は個別に維持すること。

## 9.5 顧客への詐欺とアカウント復旧

顧客情報だけでは取引を承認できなくても、詐欺の電話やメッセージに説得力を与える場合がある。詐欺対策チームは、影響する業務手順を確認すること。パスワードの復旧、連絡先の変更、遠隔サポートの要求、支払先の変更などが対象である。対応は、実際に悪用されている経路に合わせる必要がある。

支払の変更は、既存の信頼できる経路で確認すること。漏えいした可能性のある情報に依存する復旧判断を見直す。不審なメッセージのリンクをたどらなくても、顧客が注意喚起を確認できる明確な方法を用意すること。

漏えいの後に報告された送金が、すべてその漏えいに起因すると考えないこと。金融機関の正当な事案記録に、時刻、連絡先、口座上の操作、その他の関連証拠を保全する。因果関係の主張には、時期が近いという事実以上の根拠が必要である。

金融庁のインターネット取引に関する注意喚起ページは 2025 年 4 月に初回公表され、2026 年 11 月 13 日に更新された。認証の強化と関係金融機関への速やかな連絡を呼びかけている。[S79]

金融庁の 2026 年 11 月 13 日時点の月別集計表は、2025 年 1 月〜2026 年 10 月の証券会社等からの暫定報告をまとめている。この表は不正アクセス件数と、そのうち不正取引が行われた件数（不正取引件数）を記録している。[S255] 月別件数は 2025 年 4 月に不正アクセス 5,490 件、不正取引 3,033 件で最多となった。2026 年 1〜10 月は月間 18〜340 件の不正アクセスで推移し、10 月は不正アクセス 168 件、不正取引 139 件であった。期間累計は不正アクセス 19,427 件、うち不正取引 10,782 件であり、不正売買の総額は顧客の実際の損失額とは一致しない。[S255]

## 9.6 監督と合同演習

金融機関は、§10 の報告手順を最新に保つ必要がある。金融庁の 2026 年の報告様式の変更は、個人データに関する報告の要否の評価とは別である。適用される経路で報告しながら、運用、詐欺対策、プライバシー、技術対応の各担当が、一貫した説明を維持できるか、一つの演習で確認すること。[S87]

共有プラットフォームで、データの範囲が不確かなシナリオを使うこと。チームには、取引を継続するか、顧客情報に影響するか、いつ初期報告が必要かを判断させる。その後、これらの答えの一つだけを変更する、委託先の追加情報を提示すること。

責任者が区別を説明し、判断を更新できれば、演習の目的を達成できる。顧客情報と取引に関する問いが未解決なら、「復旧済み」「封じ込め済み」といった単一の状態表示だけでは不十分である。

要点

01

残されたテストデータと委託先のリポジトリを、別々の露出面として扱うこと。

02

支払の完全性、顧客情報、サービス継続は、それぞれの証拠で判断すること。

03

提供先ごとの通知と報告義務を、共有サービスの実際の影響範囲に合わせること。

章 10

# 規制対応と報告

10

この章で答える問い

日本の対応チームは、どの義務と報告経路を準備すべきか？

## 30 / 60

個人情報保護法の確報期限。報告対象の事象によって異なる


10.1 個人情報保護法に基づく報告 100

10.2 金融分野の監督 101

10.3 サイバー対処能力に関する法律 101

10.4 保存期間と本人確認画像の注意喚起 102

10.5 初期段階で使える報告資料 102

章 10

# 規制対応と報告

概要

報告の起点は、調査の完了ではなく、事実と認知にある。PPCの指針は、報告対象となる個人データの事象、速やかな速報、確報期限、本人への通知を示す。金融機関には、現行の監督上の手続も必要になる。サイバー対処に関する特定の規定は、法律の成立とは別に、10 月に施行された。法務担当と報告義務の一覧を作り、認知時刻を記録する。技術調査の間も顧客保護を続ける。

これは運用上の要約であり、法的助言ではない。

## 10.1 個人情報保護法に基づく報告

次の表は、民間事業者向けの個人情報保護委員会（PPC）の現行の指針を要約したものである。適用される義務を示しており、2026 年の新法として扱うものではない。対応チームは、自組織の法的な立場と、業種別の取扱いを確認する必要がある。[S84]

| 要件 | 対象または時期 | 対応上の意味 |
| --- | --- | --- |
| 報告対象の事象 | 所定の類型に該当する漏えい、滅失、毀損、またはそのおそれ | 最終的な帰属評価を待たず、信頼できる懸念をエスカレーションする |
| 所定の類型 | 要配慮個人情報、財産的被害が生じるおそれ、不正の目的によるおそれ、または 1,000 人超 | 情報の種類、リスク、影響する人数を別々に判断する |
| 監督機関への速報 | 速やかに。指針では一般に、認知後おおむね 3–5 日以内を目安とする | 判明した事実と未解明の点を含む初期報告を準備する |
| 監督機関への確報 | 30 日以内。不正の目的による行為が疑われる場合は 60 日以内 | 更新と期限計算の担当者を決める |
| 本人への通知 | 状況に応じて速やかに | すべての詳細を待たず、関連する事実と保護のための対応を説明する |

行政機関等は、PPCの行政機関等向けの指針に基づいて報告の要否を判断する必要がある。人数による報告要件は、保有個人情報に係る本人の数が 100 人を超える漏えい、滅失、毀損、またはそのおそれである。その人数以下でも、ほかの報告対象の類型に該当する場合がある。[S253]

法人について、PPCの指針は、いずれかの部署が認知した時点を基準とする。速報の起点は、中央のセキュリティチームに完成した調査報告書が届く時点ではない。顧客対応、不正対策、業務運用、サプライヤー管理の担当者に、信頼できる証拠を速やかに報告するよう教育する。受領した部署が何をいつ把握したかを記録する。[S84]

報告対象の類型には、条件や例外がある。一定の安全措置により、報告対象から外れる場合がある。報告先はPPC、または権限の委任を受けた主務大臣となる場合がある。本人への直接通知が困難な場合には、保護のための代替措置が認められることもある。これらは、自動的な公表ではなく、記録を残した評価に基づいて判断する。[S84]

委託先は、指針に定める状況で責任を負う委託元に速やかに通知した場合、監督機関への直接報告と本人への通知を免除されることがある。委託元の義務までなくなるわけではない。誰が事実を提供し、開示のおそれを委託元がどう把握するかを契約で定める。[S84]

目安となる 3–5 日は、社内でのエスカレーションを先送りしてよい期間ではない。法務とプライバシーの担当者は、暦日などの取扱いも含め、実際に適用される規則に従って確報期限を計算する。この表は対応の補助資料であり、その評価に代わるものではない。

## 10.2 金融分野の監督

金融庁（FSA）のサイバーセキュリティに関するガイドラインと関連する監督指針の改正は、2024 年 10 月 4 日から適用された。本報告書では、2026 年にすでに適用されていた基準として扱う。FSAの 2026 年 2 月の公表資料では、追加の監督指針改正は、公表日である 2 月 27 日から適用されたとしている。[S85][S86]

FSAは 9 月 18 日、報告手続の追加変更を公表した。改正後の監督指針は 2026 年 10 月 1 日から適用された。既存のDDoSとランサムウェアの様式に加え、共通様式はその他のサイバーインシデントも対象とする。この手続変更は、個人情報保護法の報告要件や期限とは別である。[S87]

| 項目 | 日付の区別 | 準備事項 |
| --- | --- | --- |
| サイバーセキュリティの基準となるガイドライン | 2024 年 10 月 4 日から適用 | 現在適用されるガイドラインと監督指針を確認する |
| 追加の監督指針改正 | 2026 年 2 月 27 日に公表、同日適用 | 自機関に関係する規定を確認する |
| 共通報告様式 | 9 月 18 日に公表。2026 年 10 月 1 日から適用 | 対応手順書の旧様式を置き換える |

この公表資料から確認できるのは、日付と手続の範囲である。それだけを根拠に、特定の管理策が日本のすべての企業に義務付けられるとは言えない。金融機関は、適用される詳細な指針を、自機関のサービス、委託業務、経営上の責任と対応付ける必要がある。

## 10.3 サイバー対処能力に関する法律

内閣府の説明は、特定の規定が 2026 年 10 月 1 日に施行されたことを確認している。対象は、官民連携の強化とアクセス・無害化措置に関する規定である。この説明から、他の日付や法令上の規定を推測しない。[S88]

企業の当面の課題は、適用範囲の確認である。自社のサービスが、関連する指定や分野別の仕組みに該当するかを特定する。所管機関への正しい連絡経路と情報共有窓口を確認する。個人情報が関係する可能性があれば、プライバシー上の評価も別に行う。

本報告書は、政府の方針への賛否を示さず、公式の枠組みを説明する。民間組織が所有しないシステムを調査したり、その動作に干渉したりする権限を、この法律が与えるとは推論しない。防御のための検証は、自組織に認められた環境の範囲内で行う。

## 10.4 保存期間と本人確認画像の注意喚起

PPCの 11 月 18 日の注意喚起は、レンタカー事業者が保存していた写真付き本人確認書類の画像が、外部からの不正アクセスを受けて漏えいしたと報告している。確認目的を果たした後の削除を促している。この注意喚起では、免許証番号を二年間記録することと、貸渡手続後も画像を保存することを区別している。[S71]

これは、あらゆる業種のすべての文書に共通する保存期限ではない。画像コピーが引き続き必要かを見直す、具体的な契機である。データ管理責任者は、保存する各区分について、目的、適用される義務、サプライヤー側のコピー、削除の証拠を特定する。

## 10.5 初期段階で使える報告資料

インシデントの前に、簡潔な報告資料一式を準備する。規制当局、顧客、警察、サプライヤーに示す事実は整合させる。一方で、経路ごとに必要な情報が異なることも踏まえる。

| 項目 | 初期段階の内容 | 更新担当者 |
| --- | --- | --- |
| 認知 | 最初の信頼できる証拠と受領部署 | インシデント調整担当 |
| サービスへの影響 | 利用できないと確認された機能と代替手段 | 業務運用 |
| 情報 | 確認済みまたは疑いのある情報区分と影響範囲 | データ管理責任者とプライバシー担当 |
| 封じ込め | 実施した対応、保全した証拠、残存するアクセス | 技術対応 |
| 報告 | 適用される経路、報告要件、期限、次の更新 | 法務とコンプライアンス |

不明な項目を、犯罪者の投稿が主張する数字で埋めない。主張は調査の手掛かりとして保存する。報告された停止、アクセスの疑い、確認済みの開示を区別して説明する。後の更新で範囲が狭まったり広がったりしても、最初の認知記録は書き換えない。

JPCERT/CCが 11 月 18 日に公表した調査報告書の確認表は、結論と証拠の関係、調査対象外の範囲、ログの不足、調査結果に対応する対策の確認を求めている。報告書は、単に事案を終了と記すのではなく、次の判断を支える必要がある。[S76]

要点

01

部署を問わず認知の時点を記録し、報告対象となる疑いのある事象を速やかにエスカレーションする。

02

個人情報保護法の義務と金融分野の報告手続を分ける。

03

保存する本人確認画像を見直し、各コピーが必要な理由を記録する。

章 11

# 見通しと条件付きシナリオ

11

この章で答える問い

どの変化に備える必要があり、何が評価を変えるか？

## 4

観測可能な発動条件を持つ計画シナリオ


11.1 主要な評価 105
11.2 サプライヤーのサービス停止 105
11.3 認証情報やセッションの悪用 106
11.4 情報を利用した顧客への不正 106
11.5 運用システムの露出 106
11.6 再評価の契機 107

章 11

# 見通しと条件付きシナリオ

概要

証拠は、サプライヤーの障害、アカウントの悪用、情報を利用した不正、運用システムの露出への備えを支持する。日本の攻撃件数や損失額を数値で予測する根拠にはならない。以下の各シナリオには、発動条件と責任者を設ける。今から訓練できる判断を検証し、自組織の証拠によって異なる範囲が確認されたら、対応を見直す。

## 11.1 主要な評価

ここでの確信度は、明示した命題に対するものである。将来のインシデント発生確率、国の評価、攻撃者全般への評価を示すものではない。

| 評価 | 確信度と根拠 | 評価を変える証拠 |
|---|---|---|
| サプライヤーのインシデントには、顧客ごとの判断が必要 | 公表事例から得られる運用上の教訓として高い | 当該サービスや情報に影響しないとする、検証済みのサプライヤーの範囲説明 |
| アカウントとシステム連携の証拠は、迅速な検証が必要 | 対応の必要性について高い。個々のアラートは未検証 | 自組織のログ、アカウント状態、是正記録によるアラートの解明 |
| 保存された本人確認情報は、復旧後も被害を長引かせる可能性がある | リスクの仕組みとPPCの注意喚起を根拠に高い | 検証済みの削除、または当該情報を含まないとする開示範囲の評価 |
| 公開された主張だけでは、物理的なプロセスへのアクセスは立証されない | この証拠の限界について高い | プロセスの変化を示す技術記録、または運用者の確認済みの評価 |

個別のインシデント件数が変わっても、これらの評価は有用である。確保すべき証拠と、判断すべき部門を示すためである。国の順位や、すべてのサプライヤー、従業員、顧客が影響を受けたという主張に置き換えてはならない。

## 11.2 サプライヤーのサービス停止

**計画上の想定。** 共通の業務基盤が利用できなくなり、提供元が不正アクセスを調査している。一部の顧客に必要なのは、サービスの代替手段だけである。他の顧客では、情報やシステム連携の確認も必要になる。調査の進展に伴い、復旧予定日は変わり得る。

**発動条件。** サプライヤーの公式通知が、自組織の製品、テナント、システム連携を、影響を受けた可能性がある対象に含めている。サービス責任者が、契約または技術資産台帳で依存関係を確認する。

**判断。** 最低限のサービスを維持する経路に切り替える。サプライヤーの通知と、自組織の取引に関する証拠を保全する。顧客情報、過去の契約、他のシステムへのアクセスを可能にする認証情報について、それぞれ確認する。

**完了条件。** 業務責任者がサービスの動作を実証し、セキュリティ責任者が特権アクセスの扱いを確定する。プライバシー責任者は、情報への影響評価を記録する。提供元の一般的な稼働状況の通知だけでは、この三つの判断は完了しない。

## 11.3 認証情報やセッションの悪用

**計画上の想定。** 関連するアラートや公表情報が、自組織のサービスに関係するアカウント、キー、セッションを示している。当初は、現在の有効性と影響範囲が不明である。継続的なアクセスがなくても、過去の情報が関係する場合がある。

**発動条件。** 認証管理の責任者が、アカウントやシステム連携が自組織のものであると確認する。ログ、権限、過去の是正記録を確認できる。

**判断。** 有効な特権アクセスと、システムをまたぐキーを優先する。証拠から必要と判断できる場合に、関係するセッションや認証情報を失効させる。アカウントの変更とデータ出力を確認し、証拠が示す範囲で調査を広げる。

**完了条件。** アカウントの判断結果が記録され、必要な失効が検証されている。責任者が、影響するサービス上の操作を確認している。パスワードを変更しても、既存のセッションやシステム連携がすべて解除されたことにはならない。

## 11.4 情報を利用した顧客への不正

**計画上の想定。** 開示された連絡先、予約、本人確認、取引の情報が、後の不正メッセージに信憑性を持たせるために使われる。技術的に復旧しても、すでに開示された情報は消えない。

**発動条件。** データ管理責任者が関連する開示を確認する。または顧客対応部門が、影響した情報を使う信頼できる不正メッセージの報告を記録する。販売者の主張だけであれば、引き続き調査の手掛かりとして扱う。

**判断。** 顧客対応担当に、分かりやすい注意事項と、正規と確認できる相談経路を提供する。影響する業務について、アカウント復旧時の確認と支払先変更の検証を強化する。通知は法務とプライバシーの担当者と調整する。

**完了条件。** 顧客対応担当がこの手口を見分けられ、顧客に実行可能な保護手順が提供されている。不正監視の責任者が決まっている。今後の不正をすべて防いだと主張せず、観測された悪用に照らして対策を評価する。

## 11.5 運用システムの露出

**計画上の想定。** 公開された主張や公式の注意喚起により、遠隔から到達可能な産業機器への懸念が生じる。ウェブサイトの可用性、操作画面のスクリーンショット、物理的なプロセスの変化は、異なる種類の証拠である。

**発動条件。**　設備運用部門が、関連する資産や保守経路が自組織の環境に存在すると確認する。安全上の懸念は、定められた技術上の手続でエスカレーションする。

**判断。**　プロセスの計測値を検証し、遠隔アクセスを見直す。不要な直接公開は、承認された変更により解消する。変更履歴を保全する。対応は、機器の安全性と可用性の要件に見合うものとする。

**完了条件。**　運用部門が物理的な状態を検証し、アクセスが承認済みの経路に限定されている。担当技術者が結果を承認する。一般的なITアカウントのリセットだけでは、未確認の産業機器の保守経路は解決しない。

## 11.6 再評価の契機

提供元が影響する製品の一覧を変更した場合、規制当局が新しい要件を示した場合、自組織のログからより広いアクセス経路が確認された場合は、シナリオを見直す。元の評価を残し、判断を変えた理由を記録する。公開投稿の量が変わっただけでは、攻撃頻度の変化は立証されない。

要点

01

条件付きシナリオで判断を訓練し、全国の攻撃件数の予測には使わない。

02

認証、サービス継続、顧客保護には、それぞれ別の完了証拠を求める。

03

自組織の証拠や権威ある更新情報で範囲が変わったら、再評価する。

章 12

# 行動計画

12

この章で答える問い

誰がどの順序で行動し、何をもって完了とするか？

## 30 / 60 / 90

責任者を定めた対応計画の確認日


12.1 三十日、六十日、九十日の確認事項 109
12.2 役割ごとの着手点 111
12.3 簡潔な経営向け評価表 111
12.4 Brandefenseによる支援 112

章 12

# 行動計画

**概要**

最初に、証拠の受領経路、有効な認証情報の露出、継続が必要なサービスを確認する。次に、過去のデータとシステム連携の認証情報を含め、サプライヤーと顧客の業務を検証する。その後、訓練で復旧と経営の監督を実証する。この日程は計画の枠組みであり、法定期限を示すものではない。すべての行動に責任者を置き、他のチームが確認できる証拠を求める。

## 12.1 三十日、六十日、九十日の確認事項

以下の区分は、推奨する確認時点を示す。進行中のインシデント、安全上の問題、適用される報告義務があれば、直ちに対応する必要がある。チームは、確認済みの露出とサービスの依存関係に応じて日程を調整する。

### 11–30 日

関連する認証情報、サプライヤー、犯罪者の主張に関するアラートの受領経路を整える

責任者
CISOとサービスデスク

完了の証拠
受領チーム、エスカレーション基準、検証済みの例

自組織のアカウントに関係するアラートを検証し、有効な特権アクセスを優先する

責任者
認証管理とインシデント対応

完了の証拠
所有者、情報の新しさ、権限、判断結果の記録

検証で封じ込めが必要と判断した場合、関連するセッションやキーを失効させる

責任者
認証管理とアプリケーション責任者

完了の証拠
影響するサービスでの失効確認

個人データのインシデントが疑われる場合の認知時点と報告経路を記録する

責任者
法務、プライバシー、コンプライアンス

完了の証拠
現行の義務一覧、様式、期限、机上訓練での認知の時系列

重要サービスを、ホスティング、認証、業務基盤のサプライヤーと対応付ける

責任者
調達と業務運用

完了の証拠
サービスの依存関係、データ区分、権限、代替手段の責任者

### 産業用インターフェースへの不要な直接アクセスを見直す

責任者
設備運用とOTセキュリティ

完了の証拠
承認済みのアクセス経路と技術担当者の承認

### 外部に公開している自組織の製品を、適用されるベンダーの注意喚起と照合する

責任者
インフラとアプリケーション責任者

完了の証拠
影響するバージョンの判定、是正、検証の記録

## 31–60 日

### 重要なサプライヤーの停止を想定し、代替の業務経路を検証する

責任者
事業継続とサービス責任者

完了の証拠
最低限のサービスの実証と復旧の障害の記録

### 古いシステム連携の認証情報と、終了済み契約のアクセス権を見直す

責任者
アプリケーション責任者と調達

完了の証拠
必要なアクセスの承認と、不要なアクセスの削除の実証

### 本人確認画像など、漏えい時の被害が大きい情報の保存を見直す

責任者
データ管理責任者とプライバシー担当

完了の証拠
目的、法的根拠、保存方針、削除の証拠

### 開示された情報区分を使い、信憑性のある顧客向け不正メッセージへの対応を訓練する

責任者
不正対策、顧客対応、広報

完了の証拠
正規と確認できる相談経路と担当者の対応の実証

### メール認証と正規の送信サービスを見直す

責任者
メール運用とドメイン責任者

完了の証拠
送信元の台帳とポリシー検証の証拠

## 61–90 日

### 分離した環境で重要サービスを復旧する

責任者
インフラと業務責任者

完了の証拠
復旧テスト、データ完全性の確認、業務側の受入れ

| | |
|---|---|
| 影響に争いがある主張と、その後の範囲更新への対応を訓練する | |
| 責任者<br>広報、法務、インシデント対応 | 完了の証拠<br>主張、確認済みの事実、不明点、次回更新の説明を分けた発表文 |
| 認証、サプライヤー、保存に関する未決の判断を経営と確認する | |
| 責任者<br>CISOと責任を負う経営幹部 | 完了の証拠<br>リスク受容、または予算を伴う是正措置と見直し日 |

## 12.2 役割ごとの着手点

**取締役会と経営幹部。** 通常のサプライヤーや認証基盤が使えなくても、どのサービスを継続できるかを確認する。方針の一覧ではなく、実証を求める。予算、契約上の支援、リスク受容が必要な未決事項を確認する。

**CISOとインシデント対応。** 証拠の記録を一元化しつつ、主張、サービス、情報、プロセスの評価は分ける。従業員が部分的な情報でもエスカレーションできるようにする。アラートが証拠で解明されたのか、出所が不確かという理由だけで終了したのかを確認する。

**SOCと認証管理チーム。** 封じ込めを広げる前に、自組織のアカウントとアクセス経路を検証する。必要に応じて、管理上の変更、セッションの付与、データ出力、システム連携を調べる。実施した対応とその限界の両方を説明できる証拠を残す。

**インフラと業務運用。** 現行の注意喚起の対象となる自組織のシステムについて、バージョンと公開状況を確認する。復旧と代替経路を検証する。産業環境では、物理的な安全性とプロセスの可用性を理解する技術者と、セキュリティ上の変更を調整する。

**不正対策と顧客対応。** 開示されたどの情報が、なりすましに信憑性を持たせるかを特定する。その情報だけに頼らず顧客を確認できる、一貫した手順を担当者に示す。支払先の変更は、以前から把握している連絡経路で確認する。

**法務、プライバシー、コンプライアンス。** 認知時点、適用される要件、報告の判断を、その都度記録する。初期段階の事実と最終的な範囲を分ける。自組織の義務に対する責任を維持しながら、サプライヤーからの通知を調整する。

## 12.3 簡潔な経営向け評価表

判断が完了したことを示す指標を用いる。確認したアラートの件数を、リスクがなくなった証拠として報告しない。

| 指標 | 進捗の証拠 | エスカレーションの契機 |
| --- | --- | --- |
| 関連する認証アラート | 自組織のアカウントについて、根拠のある判断結果がある | 有効な特権アクセスが未解決 |
| 重要サプライヤーへの備え | 依存関係と代替手段を実証済み | 利用できる代替経路がないサービスがある |
| 被害が大きいデータの保存 | 各区分に現在の目的と保存方針がある | 責任者がいないまま画像やコピーが残る |
| 報告の準備状況 | 認知と速報の訓練を完了 | エスカレーションを始める時点について、チーム間の認識が異なる |
| 復旧の準備状況 | 業務責任者が実際の復旧テストを受け入れている | 技術的な復旧で最低限のサービスを維持できない |

## 12.4 Brandefenseによる支援

Brandefenseは、Cyber Threat Intelligence、Digital Risk Protection、External Attack Surface Managementを組み合わせる。本報告書に関係する用途は、外部のアラートを責任者のいる判断につなげることである。アカウントの検証、主張の評価、サプライヤーの確認、公開サービスの調査などが該当する。

本報告書の集計結果だけでは、読者の有効なアカウントを特定したり、侵入を立証したりすることはできない。有用な支援は、組織が利用を認めたドメイン、サービスの依存関係、対応責任者の確認から始まる。責任者が評価し、行動に移せる証拠を得ることを成果とする。

必要な監視と対応の範囲について、Brandefenseに相談できる。検証、封じ込め、報告、業務上の判断の責任は、引き続き組織が負う。

要点

01

自組織のアカウント、報告経路、重要サービスの依存関係から着手する。

02

次の確認時点では、代替手段、保存、復旧の判断を実証する。

03

責任を負う業務責任者が確認できる証拠で、各行動を完了する。

付録

# 付録

A–D

この章で答える問い

対象群と証拠の区分から、どこまで結論を導けるか

## 2026

主な観測期間。過去の背景情報は別に示す


Appendix A. 調査範囲と証拠の境界 114
Appendix B. 証拠一覧 117
Appendix C. 出典 122
Appendix D. 用語集 132

# Appendix A. 調査範囲と証拠の境界

比較対象国は、背景を示すための例としてのみ選定したものであり、順位付けや政治的評価を意味するものではありません。

## A.1 期間と日付

主な対象期間は 2026 年 1 月 1 日〜11 月 22 日である。地下市場の情報は投稿日時を基準とする。最近の動向は 11 月 8 日〜22 日を扱う。公表資料には、過去の活動、後日の検知、現在の更新が含まれる場合がある。これらの日付を区別する。

確認時も締切日は進行中だった。終日を終えた完全な集計ではない。過去の法律、古い事案の資料、以前の年の統計には、その期間を明記する。新たな公表が新たな侵入を示すとは限らない。

## A.2 出典ごとの対象群

出典の種類ごとに、単位と範囲が異なる。各章の制約とともに読む必要がある。

| 対象群 | 単位 | 境界 |
|---|---|---|
| 地下市場の観測 | 保有する投稿 | 固有の広告、確認済み事案、影響を受けた人の数ではない |
| ランサムウェア掲載 | 犯罪者による掲載 | 暗号化、抽出、支払い、重複のない組織数を確認したものではない |
| 選定組織群 | 主なドメインで表す項目 | 独立した企業グループや全国を代表する標本ではない |
| DNS観測 | 評価対象ドメインとポリシー | 配信の実効性やアプリケーション全体の安全性ではない |
| 公表事案 | 出典の範囲内の公表と調査 | 全国の事案を網羅する集計ではない |
| 公的統計 | 当局が定める報告・事案 | 明記された期間と対象群に限る |
| 決済カードの観測 | 決済カードの観測 | 全国のカード窃取や不正利用の損失ではない |

Atlasは、2026-11-22 時点の選定した 250 ドメインについて、全国代表値 51/100 (B)を示す。匿名の業種別集計は観測された兆候を示し、業種別や組織別の評価値は公表しない。過去の認証情報レコードは累積であり、ドメイン間で重複する場合がある。掲載履歴の対象期間と現在の掲載との重複範囲は明示されていない。[S3]

DNSポリシーの観測対象は 250 ドメインである。TLS、ホームページのヘッダー、総合的な衛生指数の完全なデータはない。観測がない項目は不明である。[S4]

決済カードの観測は限定的な対象集団に関するものである。現在の有効性、重複のないカード保有者数、全国のカード盗難の発生状況、不正利用の損失を示すものではない。[S5]

## A.3 証拠の表現と確信度

観測は、保有する出典に何が書かれているかを示す。犯罪者の主張は、その出典内の言い分である。外部の裏付けは、組織によるアクセスや停止の確認など、特定の命題を支える。分析上の推論は、元の主張を事実へ格上げせず、起こり得る影響を説明する。

確信度は、その命題に付ける。広告が存在する確信度と、内容が正しい確信度は異なる。詳しい項目一覧、サンプルの主張、価格、有名な別名は、ファイルの真正性を保証しない。一方、確認がないことも虚偽の証明ではない。

公表された調査は、後に範囲が変わることがある。抽出が観測されなかったことと、抽出が不可能だったことは異なる。出典が示す留保、ログの制約、後日の更新を保って記載する。

## A.4 関係とシナリオ

関係図の線は、裏付ける出典と関係の種類を示す。自社の掲載データ、公的発表、公表調査を分ける。ある出典が実行主体を報告したことは、図内の別キャンペーンとの関係を示さない。

広告の類似から分かるのは、表現の繰り返しである。同じファイル、販売成立、最初の侵入者、共通の実行者は確認できない。裏付けのない広い括りは分析モデルとなる。第 11 章の条件付きシナリオは、開始条件と完了の証拠を備えた計画上の想定である。

## A.5 名称と公開範囲

事案の対象組織は、公式確認と広い報道がある場合に限り実名を使う。それ以外は広い役割で表す。出典の題名にも同じ境界を適用する。非公開の当事者は所在を示さずに出典を記載する。報道機関や中立的な開示基盤については、記事URLを伏せてルートアドレスを示す場合がある。

国家や政治的な帰属は、出典の評価として記載する。使用言語やインフラの場所から国籍を推定しない。領土問題、歴史的論争、選挙、政府の判断について、本報告は立場を取らない。

## A.6 対象範囲の制約

可視の投稿と公表資料が捉えるのは、脅威環境の一部である。非公開の販売、未公表の事案、原文を確認できない通知は含められない。国や分野のラベルが誤っている場合もある。選定対象から全国の割合や攻撃確率を推定しない。

事例カード 26 件と追加事例 11 件は、編集上の単位である。未検証の販売、更新を伴う組織の公表、キャンペーン調査を含む。共通の事案件数の分母ではない。各事例には出典固有の制約を添えている。

付録

# 付録

A–D

この章で答える問い

各カードと詳しい事例はどこに掲載されているか

## 12

識別情報を伏せた地下市場の投稿カード


Appendix A. 調査範囲と証拠の境界 114

Appendix B. 証拠一覧 117

Appendix C. 出典 122

Appendix D. 用語集 132

# Appendix B. 証拠一覧

## B.1 投稿カード

カードIDは両言語版で共通である。日付は投稿の日付である。連絡先として使える別名は非公開とする。抜粋が示すのは主張であり、真正性を確認したデータではない。[S1]

| カード | 日付 | 場所 | 別名 | 言語 | 章 |
|---|---|---|---|---|---|
| B01 | 2026-11-18 | フォーラム | 非公開 | 英語 | 4 |
| B02 | 2026-11-16 | フォーラム | 非公開 | 日本語 | 4 |
| B03 | 2026-11-06 | フォーラム | 非公開 | 英語 | 4 |
| B04 | 2026-03-02 | フォーラム | 非公開 | 英語 | 4 |
| B05 | 2026-02-03 | フォーラム | 非公開 | 英語 | 4 |
| B06 | 2026-08-22 | フォーラム | 非公開 | 英語 | 4 |
| B07 | 2026-01-13 | フォーラム | 非公開 | 英語 | 4 |
| B08 | 2026-11-05 | フォーラム | 非公開 | 英語 | 4 |
| B09 | 2026-05-13 | フォーラム | 非公開 | 英語 | 4 |
| B10 | 2026-01-01 | フォーラム | 非公開 | 中国語 | 4 |
| B11 | 2026-11-14 | フォーラム | 非公開 | 英語 | 4 |
| B12 | 2026-11-15 | フォーラム | 非公開 | 英語 | 4 |

## B.2 詳しい事例

最初の 6 カードは地下市場の主張を扱う。次の 20 カードは公表資料を扱う。さらに 11 の詳しい事例で、追加の公表とキャンペーン調査を扱う。更新や下流の影響を、自動的に別の新規侵入と数えない。出典が示す事案の一部として扱う。

| ID | 対象または主張 | 証拠 | 章 |
|---|---|---|---|
| A | 説明と項目一覧の不一致 | 未検証の投稿上の主張。B02 | 4 |
| B | 段階的な公開の主張 | 未検証の投稿上の主張。B03 | 4 |
| C | 銀行の脆弱性とする販売 | 未検証の投稿上の主張。B04 | 4 |
| D | スポーツ登録データの販売 | 未検証の投稿上の主張。B05 | 4 |
| E | ソースコード再配布の主張 | 未検証の投稿上の主張。B06 | 4 |

| ID | 対象または主張 | 証拠 | 章 |
|---|---|---|---|
| F | 保険データの販売 | 未検証の投稿上の主張。B09 | 4 |
| G | 理化学研究所：外部システムの認証情報にも対応が必要 | 出典の範囲内の公表事例 [S6][S7] | 5 |
| H | IDCフロンティア：共用クラウドで暗号化による障害 | 出典の範囲内の公表事例 [S8][S9] | 5 |
| I | プレイド：顧客向け基盤の停止が長期化 | 出典の範囲内の公表事例 [S10][S11] | 5 |
| J | 決済事業者：復旧を個別に判断 | 出典の範囲内の公表事例 [S12][S13] | 5 |
| K | ニトリ：大規模な影響可能性と確認済み被害を区別 | 出典の範囲内の公表事例 [S14][S15] | 5 |
| L | 教育機関：委託先の露出と業務障害を区別 | 出典の範囲内の公表事例 [S16] | 5 |
| M | タイムズカー：本人確認画像の調査結果を更新 | 出典の範囲内の公表事例 [S17][S18] | 5 |
| N | KDDI：訂正後のメール基盤の件数を使用 | 出典の範囲内の公表事例 [S19][S20] | 5 |
| O | アフラック生命：大量照会を捉える監視が課題 | 出典の範囲内の公表事例 [S21][S22] | 5 |
| P | 日本医科大学武蔵小杉病院：ナースコールシステムに機微情報が保存されていた | 出典の範囲内の公表事例 [S23][S24] | 5 |
| Q | アドバンテスト：後日の通知で持ち出しを確認 | 出典の範囲内の公表事例 [S25][S26][S27] | 5 |
| R | マネーフォワード：リポジトリのコピーと本番アクセスを区別 | 出典の範囲内の公表事例 [S28][S29] | 5 |
| S | オンライン基盤：不完全なログが結論を制約 | 出典の範囲内の公表事例 [S30] | 5 |
| T | 金融サービス事業者：残されたテストデータが露出 | 出典の範囲内の公表事例 [S31] | 5 |
| U | メーカー：外部送信後もファイルの範囲は不明 | 出典の範囲内の公表事例 [S32] | 5 |
| V | 日本交通：業務記録と過去の個人情報で範囲が異なる | 出典の範囲内の公表事例 [S33][S34][S35] | 5 |
| W | 運輸事業者：業務アプリに個人情報を保存 | 出典の範囲内の公表事例 [S36] | 5 |

| ID | 対象または主張 | 証拠 | 章 |
|---|---|---|---|
| X | 技術サービス事業者：環境を個別に調査 | 出典の範囲内の公表事例 [S37] | 5 |
| Y | ブックオフ：漏えいを確認し、対象項目を訂正 | 出典の範囲内の公表事例 [S38][S39] | 5 |
| Z | ANA：委託先の旅客データを項目別に区分 | 出典の範囲内の公表事例 [S40][S41] | 5 |
| AA | OpJapan：攻撃主張と実証された停止は別 | 出典の範囲内の公表事例 [S42][S43] | 5 |
| AB | CoGUI：日本を重視するフィッシング基盤への妨害 | 出典の範囲内の公表事例 [S44][S45] | 5 |
| AC | メーカー：ランサムウェアで生産停止 | 出典の範囲内の公表事例 [S46] | 5 |
| AD | 楽天証券：テスト環境の対象は二つの口座区分 | 出典の範囲内の公表事例 [S47][S48][S49] | 5 |
| AE | マネックス証券：口座開設書類に委託先のリスク | 出典の範囲内の公表事例 [S50][S51] | 5 |
| AF | SBCメディカル：顧客履歴と職員情報の範囲が重複 | 出典の範囲内の公表事例 [S52][S53][S54] | 5 |
| AG | 六花亭：カードを保存しなくても決済画面から露出 | 出典の範囲内の公表事例 [S55][S56] | 5 |
| AH | アララ：メールアドレス件数を人数と区別 | 出典の範囲内の公表事例 [S57][S58] | 5 |
| AI | メッセージ配信事業者：共有基盤の露出が顧客に波及 | 出典の範囲内の公表事例 [S59][S60][S61] | 5 |
| AJ | GMOインターネット：仮想デスクトップに取引セッションのリスク | 出典の範囲内の公表事例 [S62][S63][S64] | 5 |
| AK | 消費者向けアプリ：利用情報の保護が必要 | 出典の範囲内の公表事例 [S65] | 5 |

## B.3 関係図と挙動の対応表

自社データの線は掲載の存在を示す。公的発表の線は、当局と報告対象のキャンペーンを結ぶ。公表調査の線は、ベンダー調査と取り上げた名称を結ぶ。全ノードに共通の実行者がいることを示す線ではない。[S2][S77][S78][S42][S44]

挙動の対応表は、記述された行動をATT&CKの用語に対応付けた分析である。出典の帰属手法ではない。初期アクセス、実行、隠密化の区分は、対応付けた挙動に適用する。日本の全事案に適用するものではない。[S90] [S91][S92]

付録

# 付録

A–D

この章で答える問い

各命題をどの出典が支えるか

## 2026

観測締切は 11 月 22 日、出典は 11 月 22〜23 日に確認


Appendix A. 調査範囲と証拠の境界 114
Appendix B. 証拠一覧 117
Appendix C. 出典 122
Appendix D. 用語集 132

# Appendix C. 出典

欠番の出典番号はレビュー中に廃止されており、引用されていない。観測対象期間は 2026 年 11 月 22 日を締切とし、出典の確認は 2026 年 11 月 23 日まで実施した。自社出典は、本報告が保有する証拠を示す。外部出典は、原資料を確認した情報を示す。非公開の当事者は所在を示さずに出典を記載する。報道機関や開示基盤のルートアドレスは、根拠となる記事の代わりにはならない。


**S1:** Odin by Brandefense. Retained Japan-related underground post observations. 自社保有の証拠. Verified on 2026-11-22.

**S2:** Ransompedia. Japan and four regional-peer ransomware listing aggregates. 自社保有の証拠. Verified on 2026-11-22.

**S3:** Atlas. Selected Japan organisation exposure snapshot and national headline. 自社保有の証拠. Verified on 2026-11-22.

**S4:** Odin by Brandefense. Public DNS policy observations for selected Japanese domains. 自社保有の証拠. Verified on 2026-11-22.

**S5:** Odin by Brandefense. Japan-associated payment-card observations. 自社保有の証拠. Verified on 2026-11-22.

**S6:** RIKEN. Investigation update, second report. https://www.riken.jp/pr/news/2026/20261120_1/index.html. Verified on 2026-11-22.

**S7:** news.tv-asahi.co.jp. TV Asahi reports Fugaku unauthorized access. https://news.tv-asahi.co.jp/news_society/articles/000548214.html. Verified on 2026-11-22.

**S8:** IDC Frontier. IDCF seventh report: investigation results and response. https://www.idcf.jp/news/topics/20261027001. Verified on 2026-11-22.

**S9:** itmedia.co.jp. IDCF ransomware affects 495 corporate and municipal customers. https://www.itmedia.co.jp/news/article/2610/07/2000002107/. Verified on 2026-11-22.

**S10:** PLAID. KARTE investigation results and service-restart outlook. https://plaid.co.jp/news/20261120/. Verified on 2026-11-22.

**S11:** watch.impress.co.jp. KARTE inquiry complete, restart targeted for January 2027. https://www.watch.impress.co.jp/docs/news/2158411.html. Verified on 2026-11-22.

**S12:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S13:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S14:** Nitori. Nitori notice of potential personal-information leakage. https://www.nitorihd.co.jp/news/items/2b702dbe4d438f7fef74945d68e5bd27_3.pdf. Verified on 2026-11-22.

**S15:** watch.impress.co.jp. Nitori possible 37.62 million-record leak. https://www.watch.impress.co.jp/docs/news/2154952.html. Verified on 2026-11-22.

**S16:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S17:** Times Car. Times Car fifth report and revised scope. https://park24.co.jp/news/2026/10/20261023-1.html. Verified on 2026-11-22.

**S18:** ascii.jp. Times Car fifth report covered by ASCII. https://ascii.jp/elem/000/004/445/4445381/. Verified on 2026-11-22.

**S19:** KDDI. KDDI July6 report, corrected July21. https://newsroom.kddi.com/news/assets/2026/kddi_nr_s-73_4619/kddi_nr_s-73_4619_pdf_01.pdf. Verified on 2026-11-22.

**S20:** k-tai.watch.impress.co.jp. MIC administrative guidance after ISP mail incident. https://k-tai.watch.impress.co.jp/docs/news/2129178.html. Verified on 2026-11-22.

**S21:** Aflac Japan. Aflac incident FAQ updated November13. https://www.aflac.co.jp/info/yorisou_faq.html. Verified on 2026-11-22.

**S22:** bleepingcomputer.com. Aflac discloses Japan subsidiary breach. https://www.bleepingcomputer.com/news/security/insurance-giant-aflac-discloses-data-breach-after-subsidiary-hack/. Verified on 2026-11-22.

**S23:** Nippon Medical School Musashikosugi Hospital. Hospital fifth report with revised scope and route. https://www.nms.ac.jp/kosugi-h/news/_28850.html. Verified on 2026-11-22.

**S24:** news.tv-asahi.co.jp. National TV report of ransomware and initial patient leak. https://news.tv-asahi.co.jp/news_society/articles/000485236.html. Verified on 2026-11-22.

**S25:** Advantest. Advantest October6 notice filed with California AG. https://oag.ca.gov/system/files/Advantest%20Corporation%20-%20Notice%20of%20Data%20Breach%20-%20Individual%20Letter.pdf. Verified on 2026-11-22.

**S26:** Advantest. Advantest responds to cybersecurity incident. https://www.advantest.com/en/news/2026/20260219.html. Verified on 2026-11-22.

**S27:** bleepingcomputer.com. Advantest confirms information theft. https://www.bleepingcomputer.com/news/security/advantest-confirms-personal-information-stolen-in-ransomware-attack/. Verified on 2026-11-22.

**S28:** Money Forward. GitHub detailed investigation complete, fourth report. https://corp.moneyforward.com/news/info/20260623-mf-press-1/. Verified on 2026-11-22.

**S29:** itmedia.co.jp. Money Forward production-database assessment. https://www.itmedia.co.jp/news/article/2605/11/1260511106/. Verified on 2026-11-22.

**S30:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S31:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S32:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S33:** Nihon Kotsu. Sixth notice with affected groups. https://www.nihon-kotsu.co.jp/news/20261030-3479/. Verified on 2026-11-22.

**S34:** Nihon Kotsu. Initial unauthorized-access and system-suspension notice. https://www.nihon-kotsu.co.jp/news/20260713-3334/. Verified on 2026-11-22.

**S35:** internet.watch.impress.co.jp. Nihon Kotsu confirms some file leakage. https://internet.watch.impress.co.jp/docs/news/2133999.html. Verified on 2026-11-22.

**S36:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S37:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S38:** BOOKOFF. BOOKOFF third report, linked from corporate news page. https://ssl4.eir-parts.net/doc/9278/tdnet/2906882/00.pdf. Verified on 2026-11-22.

**S39:** game.watch.impress.co.jp. BOOKOFF begins individual breach notices. https://game.watch.impress.co.jp/docs/news/2148433.html. Verified on 2026-11-22.

**S40:** ANA. ANA notice on reservation-system-provider access. https://www.ana.co.jp/ja/jp/special-notice/001612.html?p1=top&p2=ja&p3=global. Verified on 2026-11-22.

**S41:** news.tv-asahi.co.jp. ANA confirms provider incident. https://news.tv-asahi.co.jp/news_economy/articles/000543786.html. Verified on 2026-11-22.

**S42:** blog.checkpoint.com. Check Point: renewed OpJapan claim wave. https://blog.checkpoint.com/exposure-management/noname05716-renews-opjapan/. Verified on 2026-11-22.

**S43:** s2w.inc. S2W February third-week claim report. https://s2w.inc/ja/resources/1022. Verified on 2026-11-22.

**S44:** proofpoint.com. Proofpoint: Japanese-focused phishing-kit disruption. https://www.proofpoint.com/us/blog/threat-insight/disruption-targets-major-chinese-language-phishing-kits-japanese-focus. Verified on 2026-11-22.

**S45:** CoGUI phishing disruption. Microsoft DCU action docket. https://www.microsoft.com/en-us/corporate-responsibility/customer-security-trust/digital-crimes-unit/notice-of-pleadings/yam-cogui-ironman/. Verified on 2026-11-22.

**S46:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S47:** Rakuten Securities. Unauthorized access and possible test-system information leak. https://www.rakuten-sec.co.jp/web/info/info20261117-02.html. Verified on 2026-11-22.

**S48:** Rakuten Securities. Corporate notice of Financial Services Agency reporting order. https://www.rakuten-sec.co.jp/web/company/newsrelease/pdf/press2026111901.pdf. Verified on 2026-11-22.

**S49:** watch.impress.co.jp. Rakuten Securities test-environment disclosure. https://www.watch.impress.co.jp/docs/news/2157207.html. Verified on 2026-11-22.

**S50:** Monex. Monex corporate interim report PDF. https://prtimes.jp/a/?c=5159&f=d5159-595-9f0a3826f4b4d2d6569f7c0693728a0b.pdf&r=595. Verified on 2026-11-22.

**S51:** news.tv-asahi.co.jp. National television reports Monex contractor incident. https://news.tv-asahi.co.jp/news_economy/articles/000547701.html. Verified on 2026-11-22.

**S52:** SBC Medical Group. SBC corporate Japan incident notice. https://prtimes.jp/main/html/rd/p/000000416.000097803.html. Verified on 2026-11-22.

**S53:** SBC Medical Group. Group notice of Japan cybersecurity incidents. https://ir.sbc-holdings.com/ja/sbc-medical-group-reports-cybersecurity-incidents-in-japan/. Verified on 2026-11-22.

**S54:** itmedia.co.jp. SBC incident scope and separate clinic-management access. https://www.itmedia.co.jp/news/article/2611/20/2000003355/. Verified on 2026-11-22.

**S55:** Rokkatei. Online-shop incident second notice. https://www.rokkatei.co.jp/news/info/20261121-25796/. Verified on 2026-11-22.

**S56:** itmedia.co.jp. Rokkatei online-shop card exposure notice. https://www.itmedia.co.jp/news/article/2611/19/2000003316/. Verified on 2026-11-22.

**S57:** Arara. Messaging-platform incident third report. https://www.arara.com/dcms_media/other/arara_20261106.pdf. Verified on 2026-11-22.

**S58:** news.tv-asahi.co.jp. National report on Arara messaging incident. https://news.tv-asahi.co.jp/news_economy/articles/000545959.html. Verified on 2026-11-22.

**S59:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S60:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S61:** FNN. Incident notice. https://www.fnn.jp/ (article URL withheld). Verified on 2026-11-22.

**S62:** GMO Internet. Hosted desktop incident third report. https://internet.gmo/news/article/248. Verified on 2026-11-22.

**S63:** GMO Internet. Hosted desktop incident fifteenth report. https://internet.gmo/news/article/261/. Verified on 2026-11-22.

**S64:** itmedia.co.jp. GMO response to actor threats and customer endpoint impact. https://www.itmedia.co.jp/news/article/2610/27/2000002624/. Verified on 2026-11-22.

**S65:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S66:** National Police Agency. 令和８年上半期におけるサイバー空間をめぐる脅威の情勢等について. https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf. Verified on 2026-11-22.

**S67:** National Police Agency. 巧妙化するボイスフィッシング被害に注意. https://www.npa.go.jp/bureau/cyber/pdf/R8_Vol.6cpal.pdf. Verified on 2026-11-22.

**S68:** IPA. 社長等をかたる詐欺メールに注意. https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20260312.html. Verified on 2026-11-22.

**S69:** IPA. サイバーセキュリティ相談窓口の相談状況2026年第2四半期. https://www.ipa.go.jp/security/support/reports/2026q2outline.html. Verified on 2026-11-22.

**S70:** IPA. サイバーセキュリティ相談窓口の相談状況2026年第3四半期. https://www.ipa.go.jp/security/support/reports/2026q3outline.html. Verified on 2026-11-22.

**S71:** PPC. 運転免許証等の顔写真付きの公的身分証明書の画像の消去について. https://www.ppc.go.jp/files/pdf/261118_houdou.pdf. Verified on 2026-11-22.

**S72:** National Police Agency. 家庭用IoT機器を悪用するレジデンシャルプロキシの現状. https://www.npa.go.jp/bureau/cyber/pdf/20260721-1_residentialproxy.pdf.pdf. Verified on 2026-11-22.

**S73:** JPCERT/CC. 直近で相次いでいる国内組織における不正アクセスに関する注意喚起. https://www.jpcert.or.jp/at/2026/at260030.html. Verified on 2026-11-22.

**S74:** National Police Agency. マイクロソフト・ＪＣ３と連携した犯罪インフラのテイクダウンについて. https://www.npa.go.jp/bureau/cyber/pdf/20261015.pdf. Verified on 2026-11-23.

**S75:** National Police Agency. 事業者に求められる不正アクセス対策のポイント. https://www.npa.go.jp/bureau/cyber/pdf/R8_Vol.22cpal.pdf. Verified on 2026-11-22.

**S76:** JPCERT/CC. インシデント調査報告書受領時のチェックリスト. https://blogs.jpcert.or.jp/ja/2026/11/ir_report_checklist.html. Verified on 2026-11-22.

**S77:** JPCERT/CC. APT-C-60による2026年の攻撃. https://blogs.jpcert.or.jp/ja/2026/07/apt-c-60_2026.html. Verified on 2026-11-23.

**S78:** National Police Agency. WaterPlum joint advisory. https://www.npa.go.jp/bureau/cyber/pdf/20260918_e.pdf. Verified on 2026-11-22.

**S79:** FSA. インターネット取引サービスへの不正アクセス・不正取引にご注意ください. https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html. Verified on 2026-11-23.

**S80:** IPA. PHPの脆弱性対策について（2026年11月）. https://www.ipa.go.jp/security/security-alert/2026/alert20261120.html. Verified on 2026-11-23.

**S81:** National Police Agency. 不正アプリによる不正送金被害が発生. https://www.npa.go.jp/bureau/cyber/pdf/R8_Vol.18cpal.pdf. Verified on 2026-11-22.

**S82:** National Police Agency. 大規模な個人情報等の流出事案に係る警察庁長官の指示. https://www.npa.go.jp/news/release/2026/20261106news.pdf. Verified on 2026-11-22.

**S83:** PPC. 共有メールシステムに関する行政上の対応. https://www.ppc.go.jp/files/pdf/260819_01_houdou.pdf. Verified on 2026-11-22.

**S84:** PPC. APPI breach reporting and affected-person notification. https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/. Verified on 2026-11-22.

**S85:** FSA. FSA cybersecurity guidelines. https://www.fsa.go.jp/news/r6/sonota/20241004/20241004.html. Verified on 2026-11-22.

**S86:** FSA. FSA 2026 supervisory amendments. https://www.fsa.go.jp/news/r7/sonota/20260227/20260227.html. Verified on 2026-11-22.

**S87:** FSA. FSA common cyber incident report forms. https://www.fsa.go.jp/news/r8/sonota/20260918/20260918.html. Verified on 2026-11-22.

**S88:** Cabinet Office. Cyber response legislation partial commencement. https://www.cao.go.jp/minister/2609_t_furukawa/photo/2026_005.html. Verified on 2026-11-22.

**S89:** JPCERT/CC. OpenJDK urgent update review. https://www.jpcert.or.jp/newsflash/2026111801.html. Verified on 2026-11-22.

**S90:** MITRE. ATT&CK Spearphishing Link. https://attack.mitre.org/techniques/T1566/002/. Verified on 2026-11-22.

**S91:** MITRE. ATT&CK User Execution: Malicious File. https://attack.mitre.org/techniques/T1204/002/. Verified on 2026-11-22.

**S92:** MITRE. ATT&CK System Binary Proxy Execution: Mshta. https://attack.mitre.org/techniques/T1218/005/. Verified on 2026-11-22.

**S93:** RFC Editor. RFC 7489: Domain-based Message Authentication, Reporting, and Conformance. https://www.rfc-editor.org/rfc/rfc7489.html. Verified on 2026-11-22.

**S94:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S95:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S96:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S97:** Organisation notice. Public-sector incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S98:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S99:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S100:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S101:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S102:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S103:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S104:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

**S105:** Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S106: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S107: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S108: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S109: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S110: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S111: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S112: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S113: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S114: Organisation notice. Public-sector incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S115: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S116: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-23.

S117: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S118: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S119: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S120: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S121: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S122: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S123: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S124: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S125: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S126: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S127: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S128: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S129: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S130: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S131: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S132: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S134: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S135: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S136: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S137: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S138: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S139: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S140: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S141: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S142: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S143: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S144: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S145: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S146: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S147: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S148: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S149: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S150: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S151: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S152: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S153: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S154: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S155: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S156: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S157: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S158: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S160: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S161: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S162: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S163: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S164: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S165: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S166: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S167: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S168: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S169: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S170: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S171: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S172: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S173: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S174: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S175: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S176: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S177: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S178: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S179: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S180: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S181: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S182: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S183: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S184: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S185: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S186: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S187: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S188: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S189: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S190: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S191: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S192: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S193: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S194: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S195: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S196: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S197: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S198: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S199: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S200: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S201: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S202: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S203: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S204: Organisation notice. Incident notice. https://data.swcms.net/ (article URL withheld). Verified on 2026-11-22.

S205: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S206: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S207: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S208: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-23.

S209: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-23.

S210: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-23.

S211: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S212: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S213: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S214: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S215: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S216: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S217: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S218: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S219: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S220: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S221: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S222: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S223: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S224: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S225: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S226: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S227: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S228: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S229: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S230: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S231: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S232: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S233: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S234: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S235: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S236: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S237: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S238: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S239: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S240: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S241: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S242: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S243: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S244: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S245: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S246: Organisation notice. Public-sector incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S247: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S248: Organisation notice. Incident notice. 公式発表（記事URL非公開）. Verified on 2026-11-22.

S249: CVE Program. CVE-2026-114938 record. https://cveawg.mitre.org/api/cve/CVE-2026-114938. Verified on 2026-11-22.

S250: OpenJDK. OpenJDK Vulnerability Advisory 2026-11-17. https://openjdk.org/groups/vulnerability/advisories/2026-11-17. Verified on 2026-11-22.

S251: Ubuntu. CVE-2026-114938 package status and fixes. https://ubuntu.com/security/CVE-2026-114938. Verified on 2026-11-22.

S252: The PHP Group. PHP November security releases in the 2026 news archive. https://www.php.net/archive/2026.php. Verified on 2026-11-22.

S253: PPC. APPI reporting guidance for private businesses and administrative bodies. https://www.ppc.go.jp/personalinfo/legal/leakAction/. Verified on 2026-11-22.

**S254:** National Police Agency. 令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について (18 September 2025). https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf. Verified on 23 November 2026.

**S255:** FSA. インターネット取引サービスへの不正アクセス・不正取引の発生状況 (13 November 2026). https://www.fsa.go.jp/ordinary/chuui/chuui_phishing/20261113.pdf. Verified on 23 November 2026.

**S256:** National Police Agency and NISC. Alert: Cyberattacks by MirrorFace (Provisional Translation) (4 February 2025). https://www.npa.go.jp/bureau/cyber/pdf/20250204_mf.pdf. Verified on 23 November 2026.

付録

# 付録

A–D

この章で答える問い

証拠を対応へつなげるために、どの用語を理解すべきか

## 3

観測、主張、推論の区別


Appendix A. 調査範囲と証拠の境界 114
Appendix B. 証拠一覧 117
Appendix C. 出典 122
Appendix D. 用語集 132

# Appendix D. 用語集

| 用語 | 平易な説明 |
| --- | --- |
| APPI | 日本の個人情報保護法。適用と通知の判断には、実際の範囲と状況の確認が必要である。[S84] |
| API | ソフトウェアが機能や情報を要求する窓口。要求する操作とデータに認可が必要である。[S73] |
| 認証情報 | アカウントや連携の認証に使う情報。販売された認証情報が現在も使えるとは限らない |
| DMARC | ドメイン単位のメールポリシーと報告の仕組み。quarantineやrejectは認証失敗時の扱いを要求する。[S93] |
| DDoS | 分散型サービス妨害。サービスの資源や可用性を損なう試み |
| 露出 | 検証が必要な観測結果や関連付け。確認済み侵入の同義語ではない |
| 連携キー | 他のシステムとの通信に使う認証情報。利用範囲は受信側のシステムによる |
| IoT | カメラや家庭用機器などの接続機器。通信の中継に悪用される場合がある。[S72] |
| MFA | 複数の要素を使う認証。セッション、連携、アプリ権限のすべてを解決するものではない |
| OAuthの同意 | 利用者や管理者が、付与した範囲でアプリの動作を認めること。[S70] |
| OT | 物理プロセスの監視や制御に使う運用技術 |
| ランサムウェア掲載 | 犯罪者が対象を名指しする掲載。窃取や暗号化を独立に確認したものではない |
| レコード・行 | データの1件の記録。同じ人に複数の記録が対応する場合がある。 |
| リポジトリ | ソースコードや開発資料の保管先。本番データベースとは異なる |
| レジデンシャルプロキシ | 家庭用回線を経由して通信を中継する仕組み。通信元を分かりにくくする場合がある。[S72] |
| セッション | 認証されたやり取り。パスワード変更後も確認が必要な場合がある |
| 委託先の対象範囲 | 事業者の調査結果が実際に扱う製品、環境、情報、顧客 |
| ビッシング | 音声で欺き、情報の提供や操作を促す行為。[S67] |

| 用語 | 平易な説明 |
| --- | --- |
| SpyGlace | JPCERT/CCがAPT-C-60 の配布経路の調査で示したマルウェア。[S77] |
| WaterPlum | 採用と不正な就労活動に関する合同注意喚起で使われたキャンペーン名。[S78] |

## 本報告について

Odin by Brandefenseは、セキュリティ、不正対策、個人情報保護、事業継続の担当者向けに本公開版を作成した。明記した範囲で、証拠に基づく判断を支援する。読者自身の現在の露出を特定するものではない。個別事案の技術、法務、運用上の評価に代わるものでもない。

日本語版は英語の原版からAIで翻訳した。意味に相違がある場合は英語版を優先する。両版で証拠IDと数値を共通にしている。配布区分はTLP:CLEARである。

ABOUT BRANDEFENSE

# Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS

**4.7** / 5

COVERAGE

**3** pillars

CTI, DRPS, EASM

MONITORING

**24** / 7

Open, deep and dark web

REQUEST A DEMO

## Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

# Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.




### Top InfoSec Innovator

2026




### Deloitte Technology Fast 500 EMEA

2024




### Global InfoSec Awards

2025




### Cybersecurity Excellence Awards

2025

## See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

# See what attackers see. Before they act.


UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO