

個人情報保護委員会 注意喚起(2026年10月7日公表)

# 大規模漏えいの 「意外な犯人」とは？

なぜ万全のはずの会社から、大量の個人データが漏れるのか

注意喚起

「検知」を新設

WARNING改訂

弁護士法人三宅法律事務所 弁護士 渡邊 雅之

今日の問い

# あなたの会社にも、ありませんか？

海外子会社

本社が把握していない  
VPN機器がある

親会社・クラウド

「身内だから」「クラウド  
だから」と任せきり

社員のPC

古い顧客データが個人フ  
ォルダに残っている

1つでも当てはまれば、それが「意外な犯人」

= 誰も責任を持っていない「管理の空白」

## 今日のポイントは3つ

- ① 「検知」が安全管理措置の柱に  
技術的安全管理措置に「(5)不正アクセス等の検知等」
- ② 多要素認証は「フィッシング耐性」まで  
組織外からのアクセス・管理者権限・重要な個人データ
- ③ グループ・クラウド・APIまで面で守り、不要データは消す  
WARNINGは9事例に拡充、法22条の消去も改めて注意喚起

数字で見る

## 漏えい等の報告は、1日あたり約47件

17,139  
件

民間事業者等の漏えい等報告(令和7年度)

3,822件

うち「不正の目的」によるおそれ(22.3%)

121件

1件で5万人超が漏えい等

不正アクセスの漏えい等元: 報告者自身 533件 / 委託先 328件

入口は「自社の外」にもある

出典: 個人情報保護委員会「令和7年度年次報告」

弁護士法人三宅法律事務所 弁護士 渡邊 雅之

**背景** 攻撃者はAIで何をしている？

# AIで脆弱性は見つけられるのか？

答え:もう見つけている

2024.11

Googleの「Big Sleep」が、広く使われるデータベースSQLiteの未知の脆弱性を発見。従来の自動検査では見つからなかった

2025.7

攻撃者だけが知っていた脆弱性をAIが先回りで発見し、悪用を阻止(AIによる初の事例と発表)

2026.1

IPA「情報セキュリティ10大脅威2026」組織編で、「AIの利用をめぐるサイバーリスク」が初選出・3位

守る側のAIにできることは、攻める側のAIにもできる

背景 | 攻撃者はAIで何をしている？

## 実際の手口: 攻撃の8~9割をAIが実行

### AIが実行した工程

- ① 偵察(攻撃対象の洗い出し)
  - ② 脆弱性の発見・検証
  - ③ 侵入
  - ④ 認証情報の窃取・横展開
  - ⑤ データの収集・選別、持ち出し
- 人間は標的選びと要所の判断だけ

2025年9月の事案(AI企業が同年11月に公表)

国家支援とされる集団が、大手IT・金融・化学・政府機関など約30組織を標的に。一部で侵入成功

「正規のセキュリティ検査」と偽り、作業を細切れにしてAIの安全装置をすり抜けた

弱点も: 存在しない認証情報をでっち上げるなどのミス

他にも: AIエージェントが34セッション・5,317コマンドを実行した政府機関への攻撃(Check Point)  
被害者PC内のAI開発ツールに「秘密情報を探させる」マルウェア(2025年8月)

背景 | 攻撃者はAIで何をしている？

## 結果:「穴」の公開から攻撃まで1日足らず

# 22時間

脆弱性の公開から攻撃コード作成までの平均(2023年は約4か月)

Check Point(2026年7月)

# 24時間 未満

脆弱性の発見から武器化までの中央値

Microsoft(2026年10月)

# +51%

新たに公表された脆弱性(2026年上半期、前年同期比)

Forescout(2026年7月)

脆弱性が公開されたら、翌日には攻撃に使われる前提で

パッチは「月1回」では間に合わない時代に

※ 注意喚起・WARNING自体はAIに言及していない。背景の可能性として各社レポート等をもとに解説

弁護士法人三宅法律事務所 弁護士 渡邊 雅之

## AIが真っ先に見つけるのは、こんな「穴」

### 狙われやすいもの

- 公開済みなのに放置された脆弱性(容疑者①)
- 台帳にないVPN・ネット接続機器(容疑者②)
- 「認可」チェックのないAPI(容疑者④)
- 推測しやすい・使い回しのパスワード(事例3)

### 企業の打ち手

- ① ネット接続機器から「日」単位でパッチ
- ② 外から見える資産を棚卸し
- ③ 侵入を前提に、検知・隔離(新設の(5))
- ④ 守る側もAIで自社を点検

AIが変えたのは攻撃の「速さ」と「量」。狙われるのは今も「管理の空白」

## PART 1 10月7日、委員会は何を出した？

# 公表されたのは「注意喚起」と「WARNING」

### 本体＋別紙

## 大規模な漏えい等事案を踏まえた対応について(注意喚起)

- 宛先は「個人情報取扱事業者の皆様へ」
- 見直し後の技術的安全管理措置を先取り(別紙)
- 不要データの消去(法22条)を再確認

### 参考資料

## WARNING 不正アクセスによる個人データ漏えい防止のための注意喚起

- 令和6年12月11日版を10月7日に改訂
- 8事例 → 9事例(API悪用を追加)
- 原因・対策例を具体化

**注意** 新たな法改正や一律の義務の施行を発表したものではない(見直し内容の確定は来年4月予定)

## 特に呼びかけられた5つの事業者像

① **大量保有** 国民の多くが利用し業界内で高いシェアのサービス、又は顧客が事業者を選びにくいサービスで大量の個人情報を保有

② 機微性の高い個人情報を保有

③ 財産的被害につながるおそれのある個人情報を保有

④ 詐欺などに利用されるおそれのある個人情報を保有

⑤ その他、漏えい時に権利利益侵害の蓋然性が高い個人情報を保有

「漏れたら被害が大きい」事業者ほど、手法の例示の上位まで求められる

# WARNINGの9事例から、容疑者は4人

容疑者① 事例1・2

「契約した」「指示した」

容疑者② 事例4・5

台帳にない海外VPN

容疑者③ 事例7・8

「身内」と「クラウド」

容疑者④ 事例9(改訂で新設)

「認可」のないAPI

残る事例3(不正ログイン)はPART3、事例6(個人領域への保存)はPART4で

クイズ① ○か×か

社内ネットワークでしか使っていないなら、サポート切れの機器を使い続けてもよい？

ヒント:WARNING 事例2

## 容疑者① 「契約した」「指示した」

**クイズ①の答え：×** 社内の機器も「外から侵入される」前提で対策を

### 契約(事例1)

改訂で追加

保守契約の業務に脆弱性対応が入っていない  
→ 脆弱性対策を含む保守契約に

### 指示(事例2)

親会社がパッチ適用を指示。人手不足の子会社が未対応  
→ 適用状況までグループで一元管理

### サポート切れ(事例2)

改訂で追加

「社内だけだから」と使い続けた  
→ 社内機器も脆弱性対策の対象に

「契約した」「指示した」≠「直った」

## 容疑者② 台帳にない海外VPN

海外拠点の子会社



親会社のデータセンター



グループ全体に被害

### 手口(事例4・5)

- 貸与品のVPN装置が台帳になく、存在を把握できず(改訂で追加)
- 子会社と親会社の間のアクセス制御が不適切
- 利便さ優先でグループ会社間を相互アクセス可能に

### 対策例

- 貸与品も含め、海外拠点のIT資産を洗い出す
- 拠点間の通信は業務上必要な範囲だけ
- 同じデータセンターでも会社ごとに分離

グループ共通システムは便利。しかし事故のときは「延焼経路」になる

クイズ② ○か×か

子会社が親会社に個人データの処理を任せているなら、子会社は親会社を監督しなくてよい？

ヒント:WARNING 事例7

## 容疑者③ 答えは×。身内もクラウドも委託先

### 親会社(事例7)

子会社が親会社に給与計算等の人事データ処理を委託。「身内だから委託ではない、監督不要」と誤認

→ 通常の外部委託先と同じ基準で監督(法25条)

例:親会社の自己点検・第三者検査の結果を子会社がモニタリング

### クラウド(事例8)

「クラウド利用は委託ではない」と考え、取扱状況を監督せず。提供事業者への不正アクセスで多数の顧客企業のデータが暗号化

→ 利用規約・安全性評価資料で確認して選定

委託に当たる場合は取扱状況を把握

## PART 2 | 大規模漏えいの真犯人は誰？

# 「クラウド例外」でも逃げられない

クラウド事業者が個人データを取り扱う

→ 「委託」に当たる

委託先の監督が必要(法25条)

取り扱わないこととなっている(Q&A7-53)

→ 例外でも「**自社の漏えい**」

自ら安全管理措置(法23条、Q&A7-54)／漏えい時は利用者が報告(法26条1項、Q&A6-22)

### 実例:エムケイシステム事案(社労士向けクラウド「社労夢」)

2023年6月ランサムウェア被害。漏えい等報告3,067件・本人数計約750万人

保守用IDでデータにアクセス可能 → 例外は適用されず「委託」と判断(2024年3月 行政指導)

どちらに転んでも、利用者自身の安全管理措置の問題

PART 2 | 大規模漏えいの真犯人は誰？

容疑者④ 「認可」のないAPI



| 原因               | 対策例                   |
|------------------|-----------------------|
| 管理対象から漏れたAPIがあった | 定期的にAPIを棚卸し           |
| 書き換えで他人のデータに届いた  | 認証に加え認可を都度確認          |
| 会員IDが連番、応答に不要な情報 | UUID等のランダム値、不要情報は返さない |
| 大量アクセスの制御がなかった   | レートリミットで検知・遮断         |

認証＝本人か？    認可＝そのデータを見てよいか？

# 真犯人は「管理の空白」

4人の共通点:「誰の担当か」が決まっていなかった

① 誰が直すか(契約・指示)

② 何があるか(台帳)

③ 誰が見張るか(監督)

④ 誰に見せるか(認可)

措置が不十分なら、**安全管理措置(法23条)・従業員の監督(法24条)・委託先の監督(法25条)**違反と判断される可能性

## PART 3 解決編:見直し後のルールは何を求める？

# どこからが違反？ いつ確定？

### 講じなければならない措置

従わなければ法23条違反と判断される可能性

### 手法の例示

あくまで例。ただし、漏えい時の被害が大きいほど上位まで求められる(リスクベース)

9月16日

ガイドライン別添の見直しを決議

10月7日

見直し後の技術的安全管理措置を先取り  
公表

来年4月(予定)

内容を確定

確定前でも、漏えい後の調査・指導の「目線」になり得る

個人情報の保護に関する法律についてのガイドライン(通則編)「10(別添)講ずべき安全管理措置の内容」

弁護士法人三宅法律事務所 弁護士 渡邊 雅之

## 技術的安全管理措置が「4本柱」→「5本柱」へ

(1)

アクセス制御

(2)

アクセス者の識別と認証

(3)

外部からの不正アクセス等の防止

(4)

情報システムの使用に伴う漏えい等の防止

(5) 新設

不正アクセス等の検知等

### (5)「講じなければならない措置」の内容(別紙)

不正アクセス等が発生した場合に**早期に検知等**するための措置を**平時から**講じ、組織内ネットワークにおける**被害拡大を防止**できるよう適切に運用

現行ガイドライン(通則編)10-6は(1)～(4)の4項目。注意喚起の別紙は見直し予定の内容(来年4月確定予定)

## 「検知等」で求められる3つのこと

### ① 定期的な分析

認証・アクセス・操作・通信のログを一定期間保管し、改ざん等から保護

定期分析で発生・兆候を早期検知

### ② 常時監視

IDS/IPS、EDR等の仕組みを導入

「定期的に見る」から「常に見ている」へ

### ③ 被害拡大の防止

侵害を受けた(おそれのある)システムの停止・隔離

アカウントの無効化

中小規模事業者の例示でも「ログ等を一定期間保管」は必須の目安。WARNING事例3でも、ログ保存・監視のルールがなく検知が遅れたことが原因に

## PART 3 | 見直し後のルールは何を求める？

# MFA・EDR・ログ分析を一言で

### MFA

鍵を1本盗まれても、もう1つの確認がないと入れない

### EDR

パソコンやサーバーの怪しい動きを見つけ、調べ、止める

### IDS / IPS

ネットワークの不審な通信を見つけ、遮断する

### ログ分析

足跡を後から見るだけでなく、異常の兆候を早くつかむ

製品を買うだけでは不十分。誰が見て、誰が止めるかまで決める

## 「パスワード+SMS」は、もう古い？

### この3場面は多要素認証

- ① 組織外ネットワークから
- ② 管理者権限で
- ③ 重要な個人データへ

「フィッシングに耐性のあるもの」を含む(例: パスキー等)。顧客側の認証にも例示

### 見直し後の例示のポイント

特権アカウントは人・端末・場面を最小限に、権限は定期的に棚卸し

アクセスのたびに場所・時間・端末の状態でリスク判断(ゼロトラスト)

基準を満たした許可端末からだけアクセス

**事例3(不正ログイン)** 推測されやすいパスワード、ロックなし、漏えいしたパスワードを放置

## PART 4 「念のため保存」が被害を広げる？

# 持っていないデータは、漏れない

### 法22条(努力義務)

利用する必要がなくなった個人データは、遅滞なく消去するよう努める

例: 利用目的を達成し保有の合理的理由がなくなった／前提の事業が中止になった(法令で保存期間が定まるものを除く)

**事例6** 各自の端末に残った古いデータまで漏えいし、被害範囲が拡大

**対応** 保有データごとに保存の法令等の根拠を確認し、根拠がなければ消す

## PART 5 明日、何から手をつける？

# 実務チェックリスト10

- |                                      |                                |
|--------------------------------------|--------------------------------|
| ① 台帳に貸与品・VPN装置・APIまで載っているか           | ⑥ 特権アカウント・権限を定期的に棚卸ししているか      |
| ② 保守契約に脆弱性対応が含まれているか                 | ⑦ ログの種類・保存期間・分析頻度が決まっているか      |
| ③ パッチ適用状況をグループで一元管理しているか             | ⑧ 侵害時の隔離・アカウント無効化の手順があるか       |
| ④ サポート切れ機器が社内に残っていないか                | ⑨ 親会社・クラウドも委託先として監督しているか(法25条) |
| ⑤ 組織外・管理者・重要データにフィッシング耐性のある多要素認証があるか | ⑩ 不要な個人データを消しているか(法22条)        |

PART 5 | 明日、何から手をつける？

それでも漏れたら：不正アクセスは人数を問わず報告

| 場面   | 内容                                | 根拠            |
|------|-----------------------------------|---------------|
| 報告対象 | 不正の目的によるおそれのある漏えい等(おそれ含む)は1人分でも対象 | 法26条1項、規則7条3号 |
| 速報   | 知った後、速やかに(概ね3～5日以内)               | 規則8条1項        |
| 確報   | 60日以内(他の類型は30日以内)                 | 規則8条2項        |
| 本人通知 | 状況に応じて速やかに                        | 法26条2項        |
| その後  | 報告徴収・立入検査、指導・助言、勧告・命令             | 法146～148条     |

ログがなければ、漏えいの範囲も人数も特定できず、報告も再発防止策も書けない

現行法・現行規則に基づく。令和8年改正法(公布後2年以内施行)で漏えい等報告の規律も見直し予定

## 社長・法務・情シスの「宿題」

### 社長・経営層

漏えい時の損害を評価し、予算・体制を決める

グループ・海外拠点まで責任範囲に  
来年4月の確定を待たず今期から

### 法務

保守・委託契約の業務範囲を確認  
親会社・クラウドの委託該当性と監督(法25条)

保存根拠の確認と不要データ消去  
(法22条)

漏えい時の報告体制(法26条)

### 情シス

IT資産台帳(貸与品・VPN・API)  
パッチの一元管理、サポート切れ  
機器

フィッシング耐性MFA、権限の棚  
卸し

ログ・EDR・隔離の手順

WARNINGも、技術対応だけでなく経営層を交えた組織的対応を求めている

まとめ

# 防御 × 監督 × データ削減

- ① 防ぐだけでなく、早く気づき、広げない(検知等の新設)
- ② 多要素認証はフィッシング耐性まで
- ③ 親会社・海外拠点・クラウド・APIの管理の空白をなくし、不要データは消す

事故ゼロを前提にせず、侵入後の被害を小さくする設計を

ご相談・お問い合わせ

## 弁護士法人三宅法律事務所 弁護士 渡邊 雅之

個人情報保護法・漏えい等事案への対応・委託先管理・社内規程の整備

TEL 03-5288-1021 / m-watanabe@miyake.gr.jp / <https://www.miyake.gr.jp/>

### 出典

個人情報保護委員会「大規模な漏えい等事案を踏まえた対応について(注意喚起)」(令和8年10月7日)、「WARNING～不正アクセスによる個人データ漏えい防止のための注意喚起～」(令和6年12月11日、令和8年10月7日改訂)、「令和7年度年次報告」、ガイドライン(通則編)10(別添)、同Q&A 6-22・7-53・7-54、「株式会社エムケイシステムに対する個人情報の保護に関する法律に基づく行政上の対応について」(2024年3月) IPA「情報セキュリティ10大脅威2026」/Google「Big Sleep」公表資料(2024年11月・2025年7月)/Anthropic「Disrupting the first reported AI-orchestrated cyber espionage campaign」(2025年11月)/Check Point「AI Security Report 2026」/Microsoft「Digital Defense Report 2026」/Forescout「2026H1 Threat Review」  
[https://www.ppc.go.jp/news/press/2026/261007\\_houdou/](https://www.ppc.go.jp/news/press/2026/261007_houdou/)