

『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）』
に対する当協会による解説
（認証付与事業者向け）



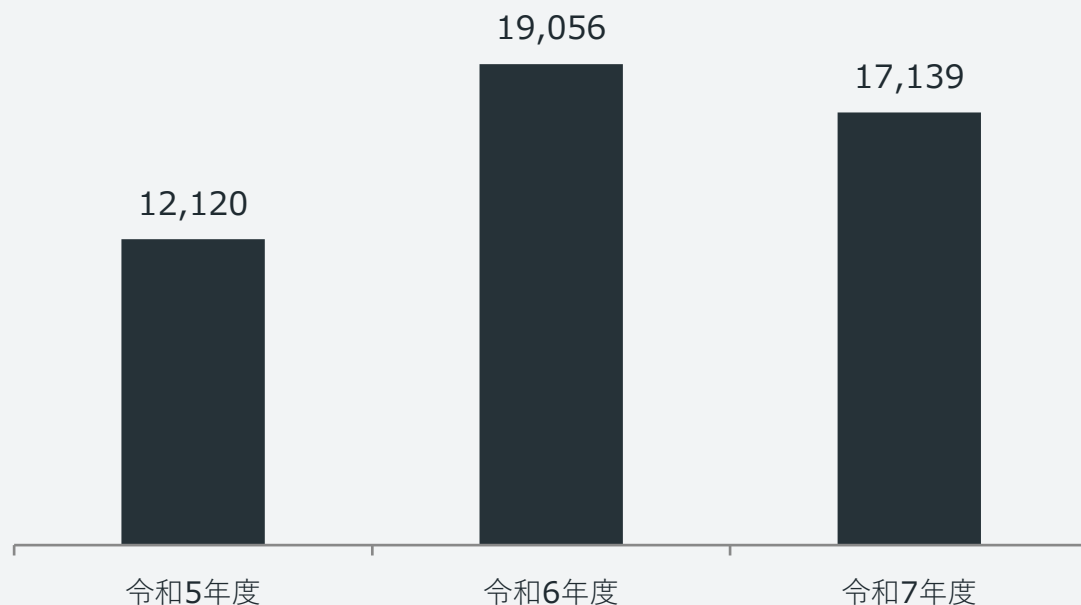
個人情報保護委員会 認定個人情報保護団体
一般社団法人 中小企業個人情報セキュリティ推進協会（SP2）

情報漏えいは「大企業だけの話」ではありません

個人データの漏えい等報告は高水準で推移しています。

2026年10月7日には、近時の大規模な漏えい事案を受けて個人情報保護委員会が注意喚起を公表しました。

民間事業者の漏えい等報告 処理件数（件）



6,101件

令和8年度第1四半期の漏えい等報告の処理件数（個人情報）。前年度の四半期換算4,854件*を大きく上回る。

*行政機関等を含む

26.6%

同期の事業者報告のうち「不正の目的によるおそれ」（不正アクセス等）に該当する割合（1,450件）

58.6%

要配慮個人情報を含む漏えい等の割合。病院・薬局・損害保険業者での誤交付も目立つ

※サイバー攻撃だけでなく誤交付・誤送付などの人的ミスも多い点に注意。件数には委託元・委託先の双方報告による重複が含まれ得るほか、後に改訂される可能性があります（PPC資料注記）。令和7年度は前年度から約1割減少しており、前年度は大型の不正アクセス事案の影響が大きかったとの解説もあります。

報告事案から見える3つの「弱点」

個人情報保護委員会は報告事案を9つの事例に類型化して公表しています。
中小企業にも当てはまる観点で、3つの弱点に整理しました（整理は当協会）。



入口の弱点

事例1～3

VPN装置等の脆弱性が公開・修正済みなのに
放置

保守契約に脆弱性対応が含まれず、担当も不明確

推測されやすいパスワード、ログイン失敗時のロック
なし



つながりの弱点

事例4・5・7・8

海外拠点・子会社を足がかりに侵入され被害が
拡大

会社間で相互にアクセスできる設定にしていた

クラウド利用や親会社への預託を「委託ではない」
と考え監督せず



データ管理の弱点

事例6・9／法22条

個人のデスクトップ等への保存が慣例化

消去すべき古いデータまで漏えいし被害が拡大

APIの設定不備で他人の情報が取得できた

放置するとどうなるか：対策が十分でない場合、安全管理措置（法23条）・従業員の監督（24条）・委託先の監督（25条）の違反と判断される可能性があります。
対策は一つで足りず「多層的」に講じる必要があります。

求められる安全管理措置と見直し予定：5つの技術的安全管理措置

個人情報の保護に関する法律についてのガイドラインの見直し予定内容が先取りで示されました。
別紙には「中小規模事業者における手法の例示」も併記されています。

講じなければならない措置	中小規模事業者向けの例示（要旨）	その他の対策例（標準の例示から抜粋）
(1) アクセス制御	個人データを扱う機器と担当者を明確にし、不要なアクセスを防ぐ	異動・退職時の権限変更、アクセス権限の定期的な棚卸し
(2) 識別と認証	機器に標準装備のユーザー制御機能で利用者を識別・認証	多要素認証、パスワード使い回しの禁止、ログイン失敗時のID停止
(3) 外部からの不正アクセス等の防止	OSを最新に保つ／セキュリティ対策ソフトを導入し自動更新で最新化	ファイアウォール設置、許可していないソフトの導入防止
(4) 使用に伴う漏えい等の防止	メールで個人データを含むファイルを送る際にパスワードを設定	通信の暗号化、テストに本物の個人データを使わない、クラウド上データの確実な消去
(5) 不正アクセス等の検知等	アクセス状況等のログを一定期間保管	ログの定期分析、被害時のシステム停止・隔離・アカウント無効化



あわせて：不要データの消去（法22条・努力義務）
使い終えた個人データは遅滞なく消去。
保有の必要性を法令等の根拠とともに確認する



「措置」と「例示」の違い
措置に従わないと法違反の可能性。
例示は全実施が必須ではなく、リスクに応じて選択

万一、漏えいがあったら：委員会への報告と本人への通知

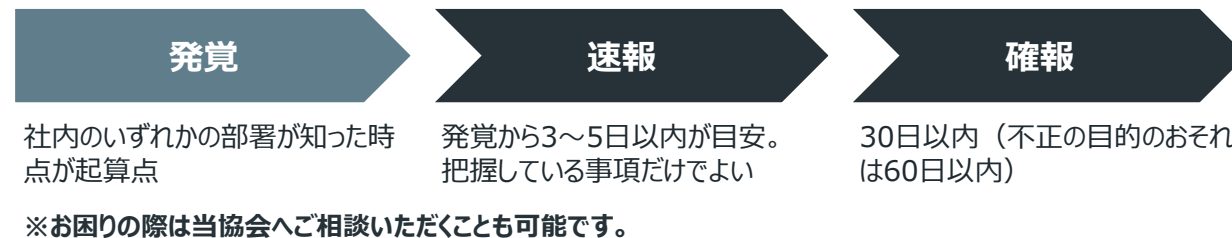
一定の漏えい等（そのおそれを含む）が生じた場合、個人情報保護委員会への報告と本人への通知が法律上の義務です（個人情報保護法第26条）。

報告・通知が必要な4つのケース（施行規則7条）

- 1 要配慮個人情報を含む**
例：従業員の健康診断結果、患者の診療情報
- 2 財産的被害のおそれがある**
例：クレジットカード番号、決済機能のあるサービスのID・パスワード
- 3 不正の目的によるおそれがある**
例：不正アクセス、ランサムウェア、書類の盗難、従業員の持ち出し
- 4 本人の数が1,000人を超える**
例：設定ミスによる公開状態、メールのCC一斉送信

※「おそれ」の段階も対象。高度な暗号化等があれば対象外（個別判断）

報告・通知の流れ



本人への通知：状況に応じて速やかに

通知する内容：概要／漏えいした項目／原因／二次被害のおそれ／その他参考となる事項（本人がとれる対策など）

連絡先が分からない等で通知が困難な場合は、事案の公表や問合せ窓口の設置などの代替措置をとる

報告先

原則は個人情報保護委員会。
権限委任業種は委任先省庁へ。
サイバー攻撃事案は共通様式も可能。

委託先・クラウドで起きたら

原則は委託元・委託先の双方に報告義務。
委託先が委託元へ速やかに通知すれば委託先は免除。

法改正に注意

2026年7月公布の改正法で本人通知の緩和等が予定。
ただし施行前のため、現行ルールで対応。

今日から始める3ステップと注意点



1. 現状を知る

個人データの保管場所、IT資産（VPN装置や借りている機器も含む）、委託先・利用中のクラウドを洗い出す



2. 基本を固める

OS・ソフトの最新化、多要素認証とアカウントロック、個人PCへの保存禁止、不要データの消去



3. 続ける・見直す

保守契約に脆弱性対応が含まれるか確認、ログを保管、漏えい時の報告・通知の手順と担当を決める、2027年4月予定の確定版で社内ルールを見直す



注意したいこと

ガイドライン（通則編）別添の「手法の例示」等の内容はまだ確定前
確定は2027年4月予定。確定版との違いが出る可能性も（推測）

全部やる必要はない

例示はリスクに応じて選択。費用をかける順番を決める

メール添付＋パスワード

中小向け例示に残る一方、内閣府・内閣官房は2020年にPPAPを廃止。
代替手段も検討（当協会見解）

担当者任せにしない

経営層を交えた組織的な対応が必要とされている

セキュリティ対策は、経営/事業運営を安心して進めるための「土台」です