

あさませキュリティニュースレター



個人情報保護法改正、漏えい報告・本人通知義務化について

(2022年5月13日)

改正

漏えい等*が発生した場合に、個人の権利利益を害するおそれ大きい事態については、個人情報保護委員会への報告及び本人への通知を義務化。

*漏えい等...漏えい、滅失又は毀損

改正前 個人情報保護委員会に報告し、本人に通知するよう努める。

個人情報保護委員会への報告が必要となる事態
(委員会規則で定める事態)

- 要配慮個人情報の漏えい等
- 財産的被害のおそれがある漏えい等
- 不正の目的によるおそれがある漏えい等
- 1,000件を超える漏えい等

※各事態につき、漏えい等の「おそれ」がある場合も対象

漏えい等
事態が
発生

個人情報取扱事業者

報告

個人情報保護委員会

通知

本人

他の個人情報取扱事業者から委託を受けた場合において漏えい等の事態が発生したとき、委託元と委託先の双方が個人情報保護委員会への報告義務を負う。ただし委託先が委託元に報告した場合、委託先は同委員会への報告義務を免除される。

令和4年4月1日から、個人データの漏えい等が発生し、個人の権利利益を害するおそれがあるときは、**個人情報保護委員会への報告及び本人への通知が義務化**されました。不注意、故意による漏えい、サイバー攻撃による被害などを想定して、対策および対処方法のご確認を！



出典 改正個人情報保護法 特集 https://www.ppc.go.jp/news/kaiseihou_feature/

報告対象となる事態

出典 漏えい等の対応とお役立ち資料 | 個人情報保護委員会 <https://www.ppc.go.jp/personalinfo/legal/leakAction/>

(1) 要配慮個人情報に含まれる個人データの漏えい等 (又はそのおそれ)

(2) 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等 (又はそのおそれ)

(3) 不正の目的をもって行われたおそれがある個人データの漏えい等 (又はそのおそれ)

① 病院における患者の診療情報や調剤情報を含む個人データを記録したUSBメモリを紛失した場合



② 従業員の健康診断等の結果を含む個人データが漏えいした場合



① ECサイトからクレジットカード番号を含む個人データが漏えいした場合



※ クレジットカード番号の下4桁のみとその有効期限の組合せの漏えいであれば、直ちに報告対象事態には該当しない。

② 送金や決済機能のあるウェブサービスのログインIDとパスワードの組み合わせを含む個人データが漏えいした場合



① 不正アクセスにより個人データが漏えいした場合

- 個人データを格納しているサーバー等において、外部からの不正アクセスによりデータが窃取された場合
- マルウェアに感染したコンピュータに不正な指令を送り、IPアドレス等への通信が確認された場合
- 不正検知を行う専門家等の第三者から漏えいのおそれについて連絡を受けた場合



② ランサムウェア等により個人データが暗号化され、復元できなくなった場合



③ 個人データが記載又は記録された書類・媒体等が盗難された場合



④ 従業員が顧客の個人データを不正に持ち出して第三者に提供した場合



(1)～(3) は、件数に関わりなく漏えい報告・本人通知対象

(4) 個人データに係る本人の数が1,000人を超える漏えい等 (又はそのおそれ)

① システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となり、当該個人データに係る本人の数が1,000人を超える場合



② 自社の会員 (1,000人超) ヘメールマガジンの配信を行う際、本来メールアドレスをBCC欄に入力して送信すべきところをCC欄に入力にして一括送信した場合



対策

- ・ ソフトウェアアップデート 脆弱性対策
- ・ 初期パスワードの見直し
- ・ ウィルス対策ソフトの更新確認 ネットワーク全体のセキュリティ対策
- ・ 在宅勤務やテレワークへの対策
- ・ 上司もしくは社長への報告体制の確認
- ・ データのバックアップ
- ・ 外部からのサイバー攻撃の対策、内部の情報管理の見直し
- ・ USBメモリの管理、持ち出すデータの確認や取扱の見直し

情報源

個人情報保護委員会 <https://www.ppc.go.jp/>

動画 政府インターネットテレビ 個人データの漏えい等事案と発生時の対応について https://www.ppc.go.jp/news/kaiseihou_feature/roueitouhoukoku_gimuka/