2022年春、サイバー被害情報漏洩時の報告が「義務化」されます。

2022年春に情報漏洩事案の公表義務化が決定。違反業者には最大1億円の罰金が課せられることになりました。

情報漏洩発生時の企業報告対応

【改正前】努力義務

個人への報告を怠ったり、ホームページで情報漏洩の事実のみを公開するなど、十分とはいえない対応を取るケースが目立っていた。

【改正後】義務化

不正アクセスによる情報漏洩など、悪用の危険性が高い事案については、個人情報保護委員会および個人への詳細な報告が義務付けられます。

● 報告を怠ると･･･最大1億円の罰金・悪質な場合は社名公表も

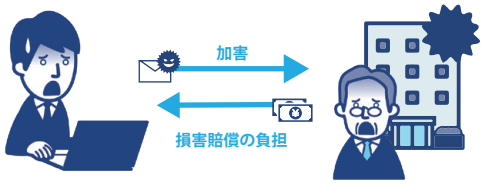
個人情報を一つでも把握していたら、その取扱いについての責任が生じます。

■氏名　■住所　■電話番号　■パスポートの番号　■基礎年金番号　■免許証の番号　■住民票コード
■個人番号（マイナンバー）　■保険証の番号　■在留カードの番号　■特別永住者証明書の番号　等

情報漏洩があった場合に想定される企業の不利益

企業の信用低下

損害賠償の負担



被害状況調査や報告にかかるコスト

各調査内容

※ 被害状況調査と報告を怠った場合は、**罰則適用**（最大1億円の罰金）

御社の情報漏洩対策、万全ですか？
Check Point の UTM も情報漏洩対策に有効です。

UTM とは？

UTMとは、Unified Threat Managementの略で日本語にすると「統合脅威管理」。
様々な脆弱性を突いてくる脅威に対抗するためには、**複数のセキュリティ機能** が必要となります。
今まで主流だったファイアウォールは通信のアドレスと種類だけで防御していましたが、
昨今の標的型攻撃や外部から社内PCを乗っ取る攻撃に対しては無力です。
UTMは **通信の内容までチェック** するため、**ファイアウォールを通過してしまう攻撃もブロック** することができます。

ファイアウォールとの違いは？

ファイアウォール　自動改札機のイメージ
宛先のみをチェックするため悪意のある通信も通過可能

UTM　空港の手荷物検査のイメージ
通信の中身を確認し、悪意のある通信を遮断

ウイルス対策ソフトとの違いは？

ウイルス対策ソフト

PC個々に保護します。
ウイルスファイルは 社内ネットワークを通過 します。
PCが感染した場合は 社外にウイルスが流出 します。

UTM

外側からの攻撃・侵入を防ぎ、ウイルスファイルを 社内ネットワークに入れません。感染したPCが持ち込まれた場合でも 内側からのウイルス流出を防ぎます。

■ お問い合わせ