Deloitte.
デロイト トーマツ

サイバー攻撃・情報漏洩発生時のファーストステップガイド

July 2025

サイバー攻撃・情報漏洩発生時の初動対応

□ 不正アクセス、ランサムウェアの感染などによって、個人情報等の情報流出の恐れや企業内のITシステムが利用不可能になった場合など

● サイバー攻撃・情報漏洩の発生時においては、侵入経路の閉鎖、マルウェア等の除去を迅速に行うとともに、被害範囲を調査し、被害者を含むステークホルダーへ迅速に連絡する必要があります。

タイムライン　　ステップ

事象検知

情報収集フェーズ　発生直後

1.　発生事象の確認と情報収集

① 事実（いつ、どこで、何が起きたのか）の把握
② 情報の保全（ログの確認）
③ 拠点間ネットワーク構成等のシステム全体像の把握
④ クライシスマネジメント、サイバーインシデントの専門家への相談　など

2.　封じ込め

① ネットワークの遮断
② 社内への情報共有および注意喚起
③ ネット上の漏洩情報のモニタリング開始　など

体制構築

体制構築フェーズ　即日～2日以内

3.　有事対応体制の構築

① 対策本部の立ち上げ（責任者の任命・事務局の設置）
② 情報集約、エスカレーションルートの確定　など

4.　有事対応方針検討

① 通常業務の継続可否・縮退業務の判断
② 侵入経路・公的手口・被害範囲の調査方針の決定
③ 封じ込め・除去・回復方針の結滞
④ 情報発信方法の決定（個別連絡／プレス／HP掲載等）　など

初報発信

対外対応フェーズ　速やかに対応

5.　被害者・取引先等のステークホルダー対応

① 個人情報保護委員会への報告（速報）
② 本人への報告
③ 取引先等、その他ステークホルダーへの連絡
④ 問い合わせ対応体制の構築（コールセンター設置など）など

インシデント緊急相談窓口

TEL ：0120-123-281 (平日9:00-17:00受付)
Mail：dt_emergency@tohmatsu.co.jp

対応時のポイント

- 事案の詳細に加えて、侵害調査に不可欠であるログを確保する
- 被害の拡大抑制、二次被害の防止のために封じ込めを確実に行う
- サイバーインシデントは全社的な危機であるとの認識のもと対応体制を整える
- IT部門、法務、広報、リスクマネジメント等の複数タスクを同時施行で推し進める
- 外部専門家を活用し個人情報保護法の定める義務を果たす

個人情報保護法の定める報告義務

規則第 8 条（第 1 項）

1 個人情報取扱事業者は、法第 26 条第 1 項本文の規定による報告をする場合には、前条各号に定める事態を知った後、速やかに、当該事態に関する次に掲げる事項（報告をしようとする時点において把握しているものに限る。次条において同じ。）を報告しなければならない。

(1) 概要
(2) 漏えい等が発生し、又は発生したおそれがある個人データの項目
(3) 漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数
(4) 原因
(5) 二次被害又はそのおそれの有無及びその内容
(6) 本人への対応の実施状況
(7) 公表の実施状況
(8) 再発防止のための措置
(9) その他参考となる事項

規則第 8 条（第 2 項）

前項の場合において、個人情報取扱事業者は、当該事態を知った日から 30 日以内（当該事態が前条第 3 号に定めるものである場合にあっては、60 日以内）に、当該事態に関する前項各号に定める事項を報告しなければならない。

※ 報告期限の起算点となる「知った」時点については、個別の事案ごとに判断されるが、法人の場合は、いずれかの部署が当該事態を知った時点を基準とする。
※ 「速やか」の日数の目安については、個別の事案によるものの、個人情報取扱事業者が当該事態を知った時点から概ね 3～5 日以内である。
※ 個人情報保護委員会への漏えい等報告については、原則として、個人情報保護委員会のホームページの報告フォームに入力する方法により行う。
※ 速報時点での報告内容については、報告をしようとする時点において把握している内容を報告すれば足りる

個人情報保護法ガイドライン（通則編）より

Deloitte.
デロイト トーマツ

※貴社および貴社の関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合等、
本サービス内容がご提供できない可能性があります。詳細はお問合せください。

デロイト トーマツ ファイナンシャルアドバイザリー合同会社
フォレンジック＆クライシスマネジメントサービス
〒100-8363 東京都千代田区丸の内 3-2-3　丸の内二重橋ビルディング
Tel: 03-6213-1180　Fax: 03-6213-1085
E-mail: dt-cm@tohmatsu.co.jp

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301