
AMT/NEWSLETTER

Digital Trust, Security & Governance

2026 年 10 月 23 日

企業の運命を分けるサイバーセキュリティ～平時のガバナンスと有事の危機管理(下)

—有事編:混乱を封じ込める「初動の鉄則」と「関係当局連携」—

弁護士 佐野 裕子

Contents

- I. 発覚時の初動措置と緊急対応体制
- II. デジタル・フォレンジックによる証拠保全
- III. 警察その他の関係当局への報告・届出
- IV. 对外広報
- V. 事後対応において特に留意すべき点
 - 1. 警察・専門家を交えない「身代金の独断支払い」～反社会的勢力への利益供与と再攻撃のリスク
 - 2. 証拠保全前の「疑惑者への不用意な事情聴取・即座の解雇」
- VI. 再発防止策の公表
- VII. 終わりに

I. 発覚時の初動措置と緊急対応体制

サイバーインシデントが発生した際には、事前の計画に基づき情報システム部門や法務部門が即座に連携する緊急対応チーム(CSIRT 等)を稼働させる必要がある¹。緊急対応チームの立上げ・運用については、実務上、初期から専任者を何名も配置することは難いため、過去の好事例²を参考に、情報システム・法務・総務各部門の兼任メンバーによる「ハイブリッド型・兼任型」の仮想組織として、各企業の規模に応じた無理のないもので始動すること(ミニマルスタート)が成

¹ 内閣官房 内閣サイバーセキュリティセンター(NISC)・サイバーセキュリティ戦略本部「サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0」27 頁等 [LAW_HANDBOOK_2.PDF](#)

² ネットワンシステムズ株式会社(NetOne-CSIRT)等

功の秘訣とされている。

また、現場からの報告がためられる環境では被害が拡大するため、「インシデントは起きて当たり前」という認識を常日頃から組織内で共有するとともに、「報告者を責めない」運用方針を徹底し、いわゆる「悪い報告」が速やかに組織に上がるよう、被害情報を迅速に経営陣へ一元管理する体制を整えなければならない³。実際に、社内の雰囲気や風通しの悪さゆえに、発生後の報告・初動対応に遅れが生じ、後々まで深刻な影響を残した事例は少なくない。

II. デジタル・フォレンジックによる証拠保全

法的責任の確定や原因究明において、システム内のアクセスログや電子データを改変させずに保全する「デジタル・フォレンジック」が極めて重要となる⁴。インシデントが発生した際、日ごろからの訓練や基礎知識が不十分であると、安易に電源を入切したり、ファイルを操作したり、システムを再起動させたりということが往々にして起こるが、これは、決して行ってはならない。これらの操作によって、メモリ上にもみ残されている攻撃者の痕跡や実行プロセス、最終更新時刻等のアクセスログが上書き・消去されてしまい、事後の追跡・捜査を困難・不可能にしてしまいかねない。

専門家の指示を受けるまで機器の状態を現状維持することが鉄則である⁵。

III. 警察その他の関係当局への報告・届出

サイバー攻撃を受けた場合、事業者は、所在地を管轄する警察署へ速やかに被害申告を行うべきである。

サイバーインシデントの発生は、それ自体が当該企業のサイバーセキュリティ対策の不十分さを示すと見られることを恐れ、時に被害申告や公表をためらう傾向が見られる。実際にも、筆者が警察のサイバー担当部署の幹部の立場にあった時に、グローバル展開する企業において、相当数の顧客情報の漏洩・流出や、相当額の暗号資産被害が発生したとして、メディアで大きく報じられた際に、当局への一応の相談と断片的な情報共有はなされたものの、最終的に事件化は望まないとして、被害届が提出されることはなく、顧客への個別の対応で終わらせたと見られるケースが複数存在した。

しかし、警察への相談や情報提供は、警察が保有する攻撃者情報の還元を受けることにつながるほか、社会的責任を果たす上でも大きな意義を持つ⁶。実際、発生後直ちに関係当局に報告するとともに、その後の継続的な情報共有が円滑になされたために、被害を最小限に抑えることができた事例も多い。

なお、2025 年 10 月からは、ランサムウェア事案等に関する関係省庁・警察への報告様式が統一・一元化される運用が開始されている⁷。

また、個人データの漏えい等が発生した場合は、個人情報保護法に基づき、個人情報保護委員会へ「速やかに(概ね 3 ～5 日以内)」速報を行い、30 日(不正目的の場合は 60 日)以内に確報を提出する義務がある⁸。

3 サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会(警察庁・総務省・経済産業省・NISC 等)「サイバー攻撃被害に係る情報の共有・公表ガイダンス」(2023 年 3 月) [guidance2022_honbun.pdf](https://www.police.go.jp/guidance2022_honbun.pdf)

4 個人情報保護法サイバーセキュリティ連絡会(個人情報保護委員会・警察庁・NCO・IPA 等)「不正アクセス発生時のフォレンジック調査の有効活用に向けた着眼点」[不正アクセス発生時のフォレンジック調査の有効活用に向けた着眼点-個人情報保護委員会-](#)

5 独立行政法人情報処理推進機構(IPA)「中小企業のためのセキュリティインシデント対応の手引き」[付録 8 中小企業のためのセキュリティインシデント対応の手引き 説明資料](#)

6 警察大学校編集『警察学論集 2023 年 8 月号』(立花書房、2023 年) 警察学論集 2023 年 8 月号

7 個人情報保護法サイバーセキュリティ連絡会「不正アクセス発生時のフォレンジック調査の有効活用に向けた着眼点」(2026 年)[不正アクセス発生時のフォレンジック調査の有効活用に向けた着眼点-個人情報保護委員会-](#)

8 個人情報保護委員会・厚生労働省『健康保険組合等における個人情報の適切な取扱いのためのガイダンス』を補完する事例集(Q&A)』(2018 年)、個人情報の保護に関する法律第 26 条

IV. 対外広報

被害公表に当たっては、不正確な情報の公表による混乱を避けるため想定問答集を用意し、対外メッセージを統一して段階的に開示することが重要である。

また、法的義務がない場合であっても、被害の拡大防止のために必要と認められる場合や、社会的な影響が大きい場合は、タイムリーな公表を検討することが求められる。

ここで留意すべきは、十分なフォレンジック調査が完了していない初動段階で、未確認の事実や原因、被害の有無を、推測や先入観に基づいて断定し、不用意に発表してはならないということである。後に調査が進んで被害の全容が判明した場合、発表内容が二転三転して「二重の虚偽発表」とみなされ、ステークホルダーに大きな混乱を与えかねない。初報では不確定な事実を断定せず、「現在詳細を調査中であり、判明次第公表する」と伝えることが原則である。

なお、当然ながら、被害を隠蔽する姿勢は、後に発覚した際の社会的信用失墜のリスクが極めて高いため、透明性のある情報発信と、責任ある立場の者による真摯かつ誠実な説明及び質疑対応が推奨される⁹。

V. 事後対応において特に留意すべき点

1. 警察・専門家を交えない「身代金の独断支払い」～反社会的勢力への利益供与と再攻撃のリスク

ランサムウェア攻撃等を受けた際、警察や外部専門家に相談せず独断で身代金を支払う対応は推奨されない。身代金を支払ったとしても暗号化されたデータが復元される保証はなく、むしろ犯罪組織・反社会的勢力への資金提供問題を生じさせかねない。さらに、「身代金を支払う易しいターゲット」と認識され、同じ攻撃者や別のハッカー集団から繰り返し攻撃対象にされ得るリスクを抱えることになる。

2. 証拠保全前の「疑惑者への不用意な事情聴取・即座の解雇」

社内不正や退職者による情報持ち出しが疑われる際、アクセスログや端末データのバックアップを水面下で確保する前に本人を問い詰めることは禁物である。疑われていると察知した本人が、端末データを完全消去・初期化して証拠隠滅を図る恐れがあるほか、関与を認めたからといって直ちに解雇してしまうと、その後の詳細調査や全容解明に向けた本人の協力が一切得られなくなる。

VI. 再発防止策の公表

インシデント収束後は、フォレンジック調査で判明した侵入経路や体制上の課題を踏まえ、反省と教訓を生かした実効性のある再発防止策を講じ、評価と改善を継続する体制を再構築しなければならない。

VII. 終わりに

先に述べたように、サイバーインシデントを未然に 100 パーセント防止することは不可能であり、いつでも発生し得るという認識の下、一旦発生した際に初動を誤ることなく対応すること、そして、インシデントを機に、職員・従業員一人一

⁹ 独立行政法人情報処理推進機構(IPA)「中小企業の情報セキュリティ対策ガイドライン第 4.0 版」[中小企業の情報セキュリティ対策ガイドライン 第 4.0 版](#)

人の意識向上を図り、将来に向けた組織の強さ・レジリエンスにつなげること、いわばピンチをチャンスに変えていくことが極めて大切である。

そのためには、組織のトップが自身の言葉で発信し働きかけていく、真のリーダーシップの発揮が求められる。

以上

-
- 本ニュースレターの内容は、一般的な情報提供であり、具体的な法的アドバイスではありません。お問い合わせ等ございましたら、下記弁護士までご遠慮なくご連絡下さいますよう、お願いいたします。
 - 本ニュースレターの執筆者は、以下のとおりです。
弁護士 佐野 裕子 yuko.sano[at]amt-law.com
※メールを送信する際には、[at]を@に変更してお送りください。
 - ニュースレターの配信停止をご希望の場合には、お手数ですが、[お問い合わせ](#)にてお手続き下さいますようお願いいたします。
 - ニュースレターのバックナンバーは、[こちら](#)にてご覧いただけます。