法務・経営のための

サイバーセキュリティ用語「72時間」で読み解く実務地図

架空のA社で起きた一つの事故を追いながら、攻撃・防御・事故対応・規格認証の重要用語を「聞くべき質問」と「法的説明責任」に接続する

弁護士法人三宅法律事務所
弁護士　渡邉雅之

YouTube配信版

OPENING

月曜の朝、この画面が出たら——最初の1時間で何を聞きますか

この動画を見終わるまでに、次の3つの問いに「自分の言葉で」答えられるようになります。

1 どこから入られたのか？

入口の言葉：フィッシング、MFA疲れ、脆弱性、委託先

2 データは持ち出されたのか？

侵入後・防御の言葉：横展開、C2、EDR、DLP

3 誰に、いつまでに、何を報告するのか？

事故対応の言葉：CSIRT、フォレンジック、漏えい等報告

そして事故の後、取締役会と取引先から問われる「何で証明するのか」。

INTRODUCTION

用語は「事故の時間軸」に並べ、「質問」と「法的責任」に変える

暗記はしなくてよい。一つの事故を追いながら、判断に必要な言葉だけを押さえる。

時間軸で覚える

どの局面の言葉かが分かれば、報告書が読める

質問に変換する

「導入済みです」に何を聞き返すかを持ち帰る

法的責任につなぐ

漏えい等報告・内部統制・委託先監督との接点

1 入口	2 侵入後	3 防御	4 事故対応	5 説明責任
どこから入ったか	中で何をされたか	どこで止められたか	誰が何をするか	何で証明するか
フィッシング／BEC MFA疲れ／脆弱性 委託先	横展開／C2 持出し ランサムウェア	IAM／ゼロトラスト EDR・SOC DLP／バックアップ	CSIRT フォレンジック 漏えい等報告	ISO 27001 SOC 2 取締役会

赤＝攻撃者の言葉　緑＝防御の言葉　黄＝事故対応の言葉　紺＝証明と統治の言葉

CASE STUDY

A社の72時間：本日追いかける架空事例

中堅メーカーA社（従業員約800名、顧客データ約5万件）。週末に何が起きたか。

3週間前 — 保守ベンダーのVPN用ID・パスワードが流出。VPN装置には既知の脆弱性が未修正のまま

金 18:10 — 経理担当者が取引先を装うメールのリンクからログイン。深夜の認証要求を誤って承認

土 深夜 — 攻撃者がVPN経由で侵入。管理者権限を奪い、社内を横展開。ファイルサーバから顧客データを持出し

日 深夜 — ランサムウェアを一斉実行。業務サーバとバックアップサーバが暗号化される

月 06:12 — EDRがアラートを出すが、外部SOC（ソック）の監視契約は平日日中のみ。気づいたのは出社後

月 09:00 — 脅迫文を確認。「データを公開する」。社長の下に対策本部を設置

登場人物

- 経理担当者（最初の入口）
- 情報システム課長（現場対応）
- CISO（技術面の統括）
- 法務部長（報告・契約・証拠）
- 広報部長（公表文）
- 保守ベンダー（もう一つの入口）
- 外部SOC・フォレンジック会社

各章の冒頭で、この事例の「続き」を確認します。

INDEX

本日の重要キーワード20：これだけは会議で使えるように

各章4語。網掛けは特に頻出で、報告書・契約書・質問票に必ず出てくる言葉。

1 入口	2 侵入後	3 防御	4 事故対応	5 説明責任
フィッシング	横展開	**IAM／MFA** アイアム	**CSIRT** シーサート	認定と認証
BEC	C2	**EDR／SOC** ソック	トリアージ	**ISO/IEC 27001** アイエスオー・ニーナナゼロゼロイチ
MFA疲れ	**ランサムウェア**	**DLP**	**フォレンジック**	**SOC 2** ソック・ツー
脆弱性／CVE	二重恐喝	RTO／RPO	**漏えい等報告**	リスクアペタイト

概要欄にもこの20語を掲載しています。周辺の略語は各ページで補足します。

CHAPTER 1

攻撃の入口：侵入はどこから始まるか

攻撃者は「システムの穴」だけでなく、人の判断、ID、委託先、設定ミスを狙う。入口の言葉を知ると、原因分析と再発防止の議論が具体的になる。

この章のキーワード

フィッシング　BEC　MFA疲れ　脆弱性　CVE／CVSS　サプライチェーン攻撃

A社の事例（架空）

金曜 18:10

経理担当者のもとに、取引先の担当者名で「請求書の確認」メールが届く。リンク先のログイン画面は本物そっくり。入力後、深夜に何度も届いた認証アプリの通知を、眠気の中で「承認」してしまう。

同じ頃、攻撃者はもう一つの鍵を手にしていた。3週間前に流出した保守ベンダーのVPNアカウントである。

一時停止して考えてみてください

経理担当者の「承認」を、人の注意ではなく仕組みで止める方法はあったでしょうか？

フィッシングとBEC：「だまされた人が悪い」で終わらせない

フィッシングは認証情報を盗む入口。BECは送金・契約という業務プロセスの弱点を突く。

From：取引先 営業部 <sales@examp1e-co.jp>
件名：【至急】振込先口座変更のお願い

いつもお世話になっております。監査対応のため、今月分より下記口座へのお振込みをお願いいたします。本件は社内でも限られた者のみで進めておりますので、ご内密にお願いいたします。

↑ 1文字違いのドメイン、至急性、秘密の強調＝典型的な兆候

フィッシング Phishing
偽メール・偽サイトでID・パスワード等を入力させる手口。

スピアフィッシング Spear phishing
特定の部署・担当者向けに作り込んだ標的型メール。

BEC（ビジネスメール詐欺）
Business Email Compromise
取引先・役員を装い、送金や情報提供を指示させる。

なりすまし／DMARC（ディーマーク） Impersonation
送信元偽装。DMARC等の送信ドメイン認証で対策。

法務・経営が聞くべきこと

- 振込先変更は、メール以外の既知の連絡先で折り返し確認するルールがあるか
- 訓練の実施回数ではなく、「報告しやすい文化」と報告件数を見ているか
- 経理・営業の承認フローをセキュリティ統制として点検しているか

関係法令

- フィッシングサイト設置：不正アクセス禁止法7条（識別符号の入力要求行為の禁止）
- 他人のID・パスワードの不正取得：同法4条
- BECによる送金：刑法246条（詐欺）等

参照：IPA「ビジネスメール詐欺（BEC）対策特設ページ」、フィッシング対策協議会公表資料

ID攻撃：いま最も現実的な侵入口

IDを奪った攻撃者は「正規ユーザー」としてログインしてくる。だから気づきにくい。

クレデンシャル・スタッフィング Credential stuffing
他サービスで漏えいしたID・パスワードの組合せを使い回して試す。

パスワードスプレー Password spraying
多数のIDに「よくあるパスワード」を少しずつ試し、ロックを回避。

MFA疲れ（MFA爆撃） MFA fatigue
認証要求を大量に送り、根負けや誤操作で「承認」させる。A社の手口。

インフォスティーラー Infostealer
端末からID・パスワードやセッション情報を盗むマルウェア。

防御の言葉：耐フィッシング認証

- パスキー／FIDO2（ファイド・ツー）：偽サイトでは認証自体が成立しない方式
- 番号照合（Number matching）：承認時に画面の数字入力を求める
- 条件付きアクセス：端末・場所・リスクで可否を判断

法務・経営が聞くべきこと

- 「MFA導入済み」の対象に、VPN・委託先ID・管理者IDは含まれるか
- 退職者・休眠・共用IDの棚卸しを、いつ誰が行ったか
- 異常ログイン（深夜・海外・短時間の連続失敗）を検知できるか

参照：NIST SP 800-63（Digital Identity Guidelines）、不正アクセス禁止法3条（不正アクセス行為の禁止）

脆弱性の言葉：「脆弱性あり」＝「侵害あり」ではない

ただし、悪用が知られた脆弱性を放置した場合、説明は極めて難しくなる。

緊急度が上がる ↑

自社での侵害 Compromise 自社環境で悪用が確認された

実際の悪用（KEV（ケブ）） Known Exploited 現実に攻撃に使われている

エクスプロイト Exploit 悪用コード・手法が出回る

CVE／CVSS 識別番号／深刻度 公開脆弱性に番号が付き、0～10で深刻度を評価

脆弱性 Vulnerability ソフトや設定上の弱点

法務・経営が聞くべきこと

- CVSSの点数だけでなく、外部公開の有無と悪用実績（KEV掲載等）は
- 修正の公表から適用までの期間と、未適用の理由の記録は
- VPN・ファイアウォール等の境界装置が対象に入っているか

ゼロデイ Zero-day
修正公開前に悪用される脆弱性。

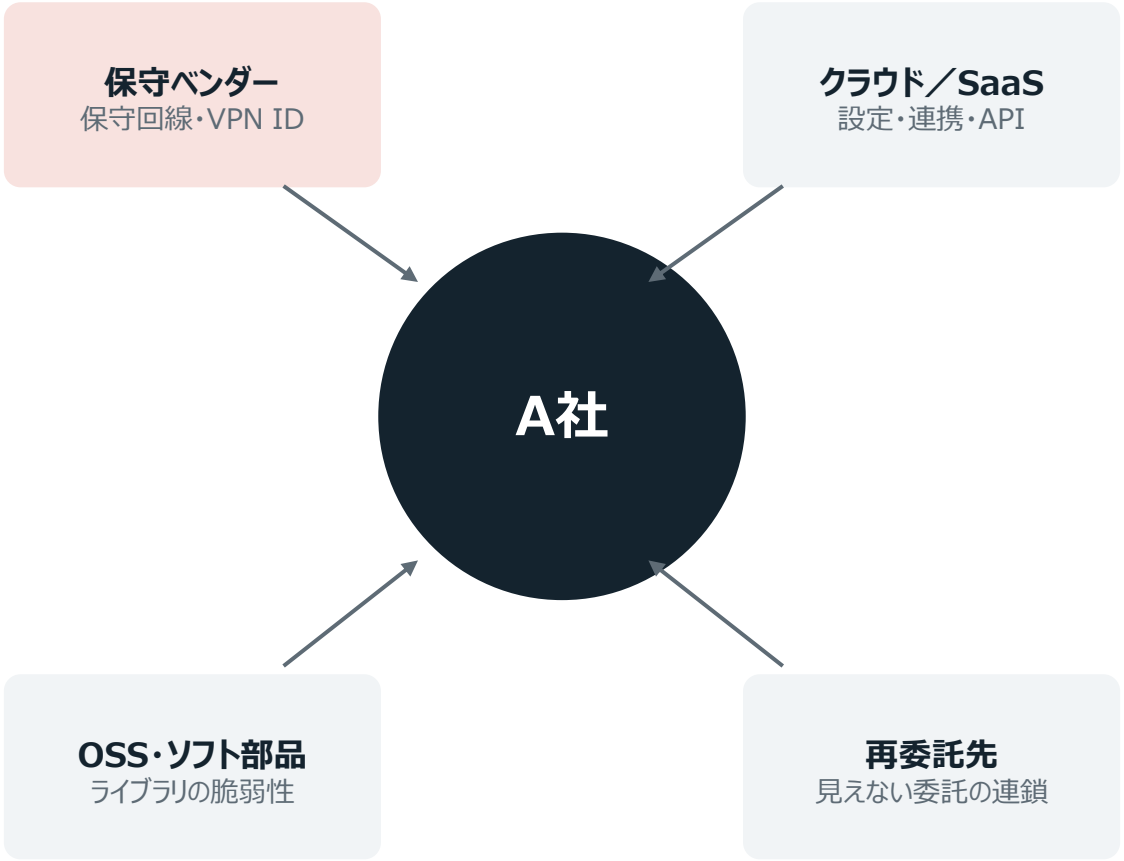
パッチ Patch
修正プログラム。適用記録が重要。

「パッチ未適用」は技術課題であると同時に、安全管理措置（個情法23条）と取締役の善管注意義務の説明課題になる。

参照：NIST NVD／FIRST CVSS v4.0、CISA Known Exploited Vulnerabilities Catalog、JVN（JPCERT/CC・IPA）

サプライチェーン攻撃：自社だけ強くても足りない

攻撃者は、守りの固い本丸ではなく、つながっている取引先・委託先・部品から入る。



サプライチェーン攻撃 Supply chain attack
取引先・委託先・製品供給網を経由する攻撃。

サードパーティ・リスク Third-party risk
委託先・外部サービスに由来するリスク。

SBOM（エスボム） Software Bill of Materials
ソフトウェアの部品表。脆弱性の影響確認に使う。

セキュリティ質問票 Security questionnaire
委託先評価の標準ツール。回答の裏付けが鍵。

関係法令・契約の論点

- 委託先の監督義務：個情法25条（委託先の選定・契約・取扱状況の把握）
- 契約条項：事故報告期限、監査権、再委託の事前承諾、ID管理、削除証明
- 委託元からの責任追及：民法415条（債務不履行）・709条（不法行為）

参照：個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」3-4-4、経済産業省「サイバーセキュリティ経営ガイドラインVer3.0」

CHAPTER 2

侵入後：
攻撃者は中で何をしたか

侵入された瞬間に被害が確定するわけではない。権限を奪い、広がり、盗み、壊す。この流れの言葉を知ると、影響範囲の調査報告が読めるようになる。

この章のキーワード

権限昇格　横展開　C2　データ持出し　ランサムウェア　二重恐喝　生成AIリスク

A社の事例（架空）

土曜 深夜 ～ 日曜 深夜

VPNから入った攻撃者は、管理者のパスワードを窃取してドメイン管理者の権限を得る。数時間かけて社内のサーバを次々に掌握し、外部の指令サーバと通信を確立。

ファイルサーバから顧客データを圧縮して外部へ送信した後、日曜深夜、業務サーバとバックアップサーバで一斉にランサムウェアを実行した。

一時停止して考えてみてください

暗号化に気づいた時点で、まだ「分かっていないこと」は何でしょうか？

攻撃の流れ：侵入から暗号化までの6ステップ

マルウェアは「名前」より「役割」で見る。どの段階の何が実行されたかが影響範囲を決める。

1 → 2 → 3 → 4 → 5 → 6

1 初期アクセス
Initial access
VPN・メール等から最初に侵入

2 権限昇格
Privilege escalation
一般権限から管理者権限へ

3 横展開
Lateral movement
社内の他の端末・サーバへ拡大

4 C2通信
Command & Control
外部の指令サーバと遠隔操作

5 持出し
Exfiltration
データを圧縮し外部へ送信

6 目的実行
Impact
暗号化・破壊・恐喝

マルウェア／ペイロード Malware / Payload
悪意あるソフトの総称／その攻撃本体の機能。

C2（C&C） Command and Control
攻撃者が遠隔から指示を送る通信基盤。痕跡の要。

Living off the Land（リビング・オフ・ザ・ランド） 環境寄生型
正規の管理ツールを悪用し、検知を逃れる手法。

報告書で「感染端末○台」とだけあれば、C2通信・認証情報の窃取・横展開・持出しの有無を必ず確認する。

参照：MITRE ATT&CK Enterprise Tactics

ランサムウェア：いまは「暗号化」だけの攻撃ではない

見るべきは、暗号化の有無より「侵入・窃取・恐喝・復旧不能」の全体像。

従来型	**暗号化して復号と引換えに金銭要求** 復旧できれば被害は限定的
二重恐喝	**暗号化＋窃取データの公開を予告** バックアップで復旧しても漏えい問題が残る
ノーウェアランサム	**暗号化せず、窃取と恐喝のみ** 業務は止まらないが、気づきにくい

リークサイト：窃取データを公開・予告する攻撃者側のサイト。掲載の有無は公表判断にも影響する。

「支払うか」を議論する前に確認すること

- 自力で復旧できるか（バックアップの無事、RTO）
- 支払っても復号・データ削除の保証はない。再恐喝の実例も多い
- 支払先が制裁対象者の場合：外為法16条（支払規制・許可制）等に抵触するおそれ
- 取締役の判断としての合理性：会社法330条・民法644条（善管注意義務）
- 警察・当局・保険会社との連携と記録

攻撃者の行為：刑法234条の2（電子計算機損壊等業務妨害）、168条の2（不正指令電磁的記録作成等）、249条（恐喝）

参照：警察庁「令和7年におけるサイバー空間をめぐる脅威の情勢等について」、IPA「情報セキュリティ10大脅威」

生成AI時代の新しい入口と出口

AIリスクは「入れる情報」「参照させる情報」「AIへの攻撃」「AIによる攻撃」の4つに分けて考える。

入れる情報

シャドーAI

会社が把握・承認していないAI利用。機密や個人データの入力が問題に。

参照させる情報

RAG（ラグ）

社内文書を検索してAIに回答させる構成。権限設定を誤ると閲覧権限のない情報が回答に出る。

AIエージェント

ツールや権限を持ち自律的に操作するAI。プロンプトインジェクションの被害が「情報開示」から「不正な実行」に拡大する。AI自身をID・権限管理の対象にする発想が必要。

AIへの攻撃

プロンプトインジェクション

文書やWebに仕込んだ指示でAIを操り、情報開示や不正操作をさせる。

AIによる攻撃

ディープフェイク

役員の声・映像を偽装した送金指示など。BECの高度化。

法務・経営が聞くべきこと

- 許可サービス一覧と入力禁止情報
- AI利用ログは残るか
- RAGの参照権限は元文書と一致するか
- AIに与えた権限の上限は

参照：OWASP Top 10 for LLM Applications（2025）、IPA「情報セキュリティ10大脅威 2026」、個人情報保護委員会「生成AIサービスの利用に関する注意喚起等」

CHAPTER 3

防御・検知・復旧：どこで止められたか

防御の言葉は「入口で止める」「中で見つける」「出口で止める」「元に戻す」の4つに分ける。製品名ではなく、どの局面を担う言葉かで覚える。

この章のキーワード

IAM（アイアム） MFA ゼロトラスト EDR SOC（ソック） DLP 暗号化 RTO／RPO

A社の事例（架空）

月曜 06:12

端末に導入していたEDRが、不審なプロセスを検知してアラートを出していた。しかし、外部SOCとの監視契約は平日日中のみ。アラートは誰にも見られないまま、出社時刻を迎える。

バックアップは「取っていた」。ただし業務サーバと同じネットワーク上にあり、同じ管理者権限で操作できる状態だった。

一時停止して考えてみてください

A社の対策は「あった」。では、なぜ機能しなかったのでしょうか？

防御は4つの局面で考える：A社はどこで止められたか

「対策をやっています」ではなく、どの局面に、どの管理策が、どの程度効いているかを説明する。

入口で止める

IAM（アイアム）・MFA
ゼロトラスト
脆弱性管理

A社の穴

委託先VPN IDにMFAなし
VPN装置の脆弱性が未修正

中で見つける

EDR・SIEM（シーム）・SOC（ソック）
セグメンテーション

A社の穴

週末のアラートを誰も見ていない
サーバ間の通信が無制限

出口で止める

DLP
通信監視・暗号化

A社の穴

大量データの外部送信を
検知できなかった

元に戻す

バックアップ
BCP・DR

A社の穴

バックアップも同じ権限で
暗号化された

多層防御（Defense in depth）：一つが破られても次で止まるよう、4つの局面すべてに手当てする考え方。

IDは「全館のマスターキー」、ゼロトラストは「毎回確かめる」

クラウド時代には、ネットワークの壁ではなくIDが境界になる。

IAM

アイアム | Identity and Access Management
IDと権限の管理

- 誰が（本人確認）
- どの端末・場所から（条件）
- 何に、どこまで（権限）
- いつまで（入社・異動・退職と連動）

攻撃者が最初に狙うのは管理者権限。

MFA Multi-Factor Auth.
2つ以上の要素で本人確認。

PAM（パム） Privileged Access Mgmt.
特権IDの承認・記録・監視。

最小権限 Least privilege
必要最小限の権限だけ付与。

ゼロトラスト 暗黙の信頼を置かず、アクセスのたびに確かめる考え方

	境界型	ゼロトラスト
信頼の根拠	社内ネットワークの内側	ID・端末・リスクを毎回評価
A社なら	VPNに入れば全サーバへ到達	委託先は保守対象機器だけに接続

法務・監査が聞くべきこと

- 「MFA導入済み」の対象に委託先・管理者・VPNは入るか／特権IDの操作ログと例外承認の記録

参照：NIST SP 800-63、NIST SP 800-207、個人情報保護委員会ガイドライン（通則編）10-6「技術的安全管理措置」

検知の三点セット：EDR・SIEM・SOCを混同しない

センサー、記録と分析の基盤、判断する人。三つがそろって初めて機能する。

センサー
EDR
Endpoint Detection and Response

端末上の不審な挙動を検知し、調査・隔離する。

記録と相関分析
SIEM（シーム）
Security Information and Event Management

各種ログを集約し、関連づけて異常を見つける。

人と判断
SOC（ソック）
Security Operations Center

アラートを監視・分析し、初動対応につなげる。

XDR 横断的な検知
端末・メール・クラウド等を横断。

MDR Managed Detection & Response
検知・対応の外部委託サービス。

SOAR（ソアー） 対応の自動化
定型対応を手順化・自動化。

聞くべきこと：監視の時間帯（24時間365日か）、アラートから連絡までの時間（SLA）、EDRの自動隔離権限を委託先に与えているか。

A社の教訓
EDRは鳴っていた。見る人がいなかった。

アクセス制御とDLP：「見てよいか」と「外に出してよいか」

入口の管理だけでは、正当な権限を持つ人や乗っ取られたIDによる持出しは止められない。

アクセス制御

Access control

問い：見てよいか

- 営業部だけが顧客名簿を閲覧できる
- 退職者アカウントを停止する
- 管理者権限を限定する

DLP

Data Loss Prevention

問い：外に出してよいか

- 顧客名簿の外部メール添付を警告・遮断
- カード番号・マイナンバー様の文字列を検知
- 外部生成AIへの貼付け・アップロードを制限

A社ではどうだったか： 攻撃者は奪った管理者権限で「正当に」ファイルを閲覧できた。アクセス制御上は問題が見えない。深夜に数十GBのデータが外部へ送信された時点で、出口の監視（DLP・通信監視）が働けば止められた可能性がある。

暗号化は「かけたか」より「鍵を誰が持っているか」

鍵が同じ環境にあれば、暗号化の意味は大きく薄れる。

暗号化 Encryption
鍵がなければ読めない形に変換する。保管時・通信時で別。

KMS Key Management System
暗号鍵の生成・保管・ローテーションを管理。

ハッシュ Hash
元に戻せない固定長の値。改ざん検知・パスワード保存に使う。

HSM Hardware Security Module
鍵を安全に保管・操作する専用装置。

トークナイゼーション Tokenization
カード番号等を無意味な代替値に置き換える。

シークレット管理 Secrets management
APIキー・秘密鍵・パスワードの一元管理。

聞くべきこと：「暗号化済み」なら、鍵の保管場所、鍵にアクセスできる人、アクセスログ、鍵が侵害範囲に含まれるか。カード情報を扱うならPCI DSS（第5章）の範囲にも関わる。

漏えい等報告との関係

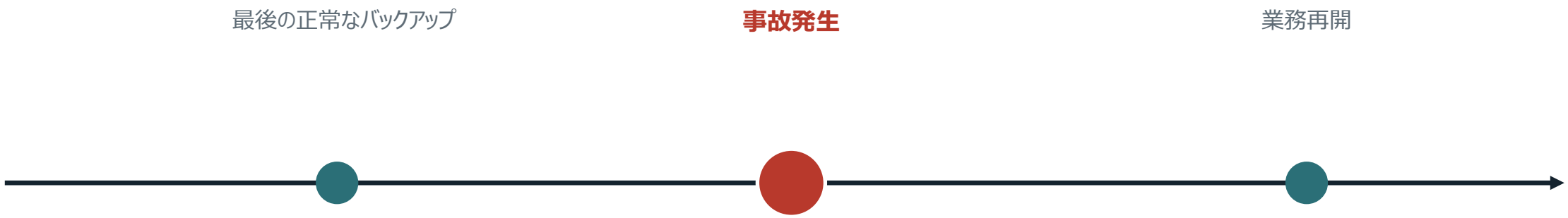
個情法施行規則7条1号は、「高度な暗号化その他の個人の権利利益を保護するために必要な措置」を講じた要配慮個人情報等を、報告対象から除いている（同号括弧書）。

ただし、暗号鍵も一緒に漏えいした場合は、この除外に当たらない。鍵管理が法的判断を左右する。

参照：個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」3-5-3-1

バックアップは「ある」だけでは足りない

戻せるか、どの時点まで戻るか、いつまでに戻るか。平時に決めて試しておく。



RPO（アールピーオー）
目標復旧時点：どの時点のデータまで戻すか
＝どこまでの消失を許容するか

RTO（アールティーオー）
目標復旧時間：どれだけの時間で業務を再開するか
＝停止をどこまで許容するか

イミュータブル Immutable backup
一定期間、変更・削除できないバックアップ。

3-2-1ルール 3コピー・2媒体・1つは遠隔
さらにオフライン1つを加える考え方も。

BCP／DR 事業継続計画／災害復旧
どの業務から戻すかの優先順位を含む。

聞くべきこと

- 復元テストの最終実施日
- 隔離保管と別権限か

今日の用語が「法令の言葉」になる：GL別添の見直し検討

個人情報保護委員会 2026年9月16日資料。安全管理措置（法23条）の手法の例示を現代化する方向。

資料が挙げるキーワードは4つ：ゼロトラスト／横展開対策／クラウド／多要素認証。ただしクラウド利用と多要素認証は、すでに実務の前提。別添の手法の例示として明記される点に意味がある。注目すべきは次の2つ。

ゼロトラストの取り込み

現状の課題：現行の別添10-6（技術的安全管理措置）は境界型セキュリティモデルを念頭に置いたもの。

示される方向：組織内・組織外のアクセスを問わず、アクセス要求ごとに動的コンテキストを評価し、リスクに応じてアクセスの可否を判断すること等を、手法の例として示す方向。

本日の用語：ゼロトラスト／条件付きアクセス／IAM

横展開対策

現状の課題：侵入型ランサムウェアを代表として、ネットワークの奥深くまで侵入する事案が増えている。

示される方向：特権アカウントの利用等を最小限に限定すること。侵害を受けた又はそのおそれがある情報システムの停止・隔離、アカウントの無効化等、被害が広がらない対策を講ずること。

本日の用語：横展開／PAM（特権ID）／封じ込め

もう一つの論点：別添は、従わなければ法違反と判断され得る「講じなければならない措置」と、その実践例である「手法の例示」で構成される。この対応関係・趣旨を整理して再構成し、Q&Aの手法例も別添に一本化。マイナンバーGL等も併せて見直し。

実務：施行は2027年4月予定。それまでに、安全管理措置規程・委託先管理・特権ID運用をこの2つの観点で棚卸ししておく。

2026年9月 方向性の公表 → **11月** 委員会審議 → **12月** パブコメ開始 → **2027年2月** 改正事項の決定 → **2027年4月** 施行

参照：個人情報保護委員会 第369回（2026年9月16日）資料2「ガイドライン（通則編）等における安全管理措置の手法の例示の追加等の検討について」、同「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1月）

CHAPTER 4

事故対応：誰が、いつ、何をするか

初動で混乱する原因は、技術よりも「いまどのフェーズか」「誰が決めるか」の認識違いにある。対応の言葉を時間軸でそろえる。

この章のキーワード

インシデント　トリアージ　封じ込め　根絶・復旧　CSIRT（シーサート）　フォレンジック　漏えい等報告　適時開示

A社の事例（架空）

月曜 09:00 ～ 翌週

社長を本部長とする対策本部が立ち上がる。情報システム課長は「すぐに全サーバを初期化して復旧したい」。法務部長は「証拠が消える。待ってほしい」。広報部長は「取引先から問い合わせが殺到している」。

フォレンジック会社、弁護士、保険会社への連絡順は、誰も決めていなかった。

一時停止して考えてみてください

「すぐ初期化したい」現場と「証拠を残したい」法務。どちらを先にしますか？

対応の流れと体制：「いまどのフェーズか」「誰が決めるか」をそろえる

混乱の原因は技術よりも、フェーズと権限の認識違いにある。

準備	検知・分析	封じ込め	根絶	復旧	事後検証
体制・手順・訓練	トリアージ	隔離・ID停止	原因の除去	安全確認し再開	再発防止

CSIRT（シーサート） Incident Response Team
部署横断の事故対応チーム。

トリアージ Triage
重要度・緊急度の切り分け。

平時に決め、事故時に記録すること
誰が「重大事故」と判断し、誰が公表を決めるか／外部への連絡順（保険の初動ベンダー指定に注意）／「いつ、誰が、何を根拠にインシデントと認定したか」――これが漏えい等報告の起算点の説明になる。

参照：NIST SP 800-61 Rev.3（2025年4月）、JPCERT/CC「CSIRTマテリアル」

フォレンジックと証拠保全：「早く直す」と「正しく調べる」の衝突

初期化してしまうと、侵入経路も持出しの有無も分からなくなる。

復旧を急ぎたい

- 業務停止の損失が日々拡大
- 取引先への影響
- 初期化すれば早く戻る

VS

証拠を残したい

- 侵入経路が不明なら再侵入
- 持出しの有無が漏えい判断に直結
- 保険・訴訟での立証

両立のための原則

- 電源を切る・初期化する前に、専門家に相談する
- ネットワークから切り離して隔離（封じ込め）し、ディスクとメモリを保全
- ログは上書き前に退避。保存期間の短いログを優先
- 保全しながら、別環境で優先業務から復旧する

参照：個人情報保護委員会「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1月公表）

デジタル・フォレンジック Digital forensics
電子的な証拠を保全・解析し、侵入経路・影響範囲を明らかにする。

証拠保全 Preservation
ディスク等の複製（イメージ）を改変なく取得。

揮発性情報 Volatile data
メモリ等、電源断で消える情報。

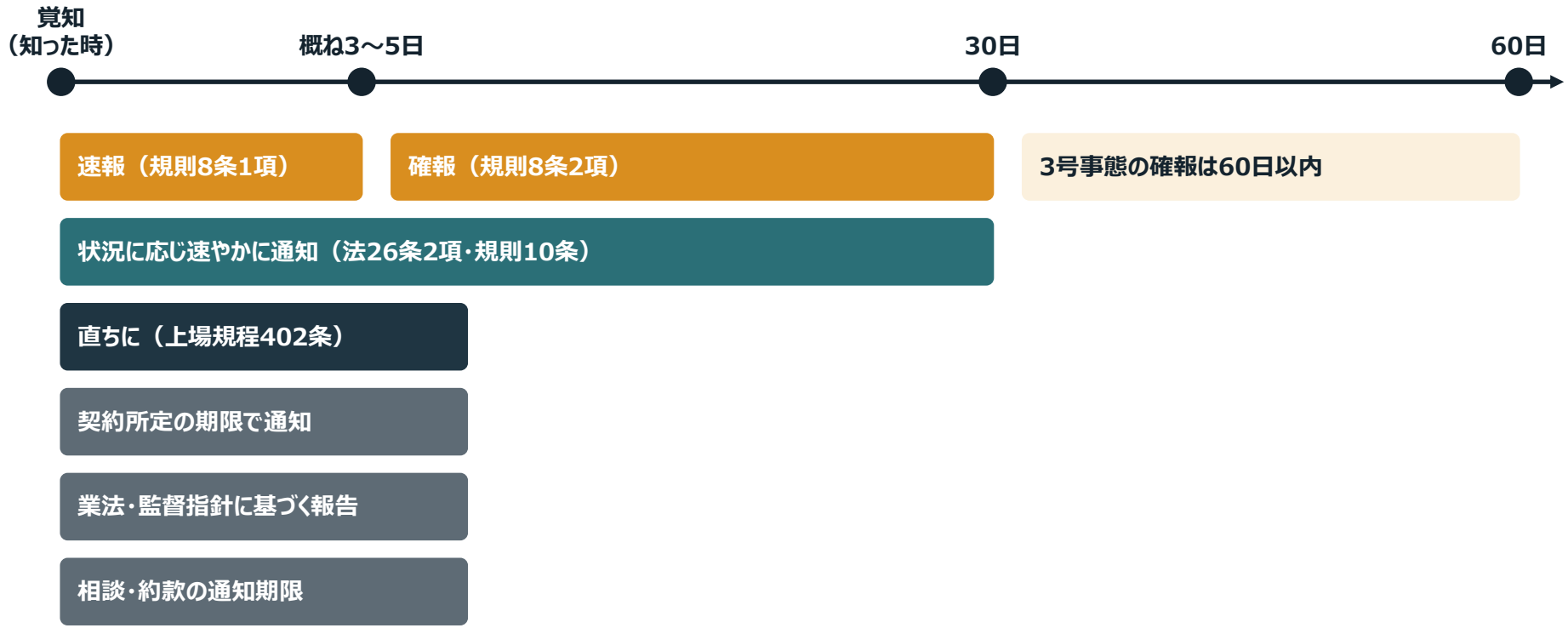
CoC Chain of Custody
証拠の取扱い経過の記録。

タイムライン分析 Timeline analysis
ログを時系列に並べ行動を再構成。

秘匿特権（Legal privilege）への注意：日本法には弁護士・依頼者間通信の秘匿特権の一般的な明文規定はない。海外訴訟が想定される場合は、弁護士経由でのフォレンジック委託を検討する。

報告・通知の時間軸：誰に、いつまでに

「知った時」を起点に、複数の報告ルートが同時に走る。



報告対象（規則7条各号）
①要配慮個人情報 ②財産的被害のおそれ ③不正目的のおそれ ④1,000人超

「おそれ」でも報告対象。A社は不正アクセスによる持出しのおそれ＝3号事態に当たり、確報期限は60日となる。

参照：個人情報保護法26条、同法施行規則7条・8条・10条、個人情報保護委員会ガイドライン（通則編）3-5、東京証券取引所 有価証券上場規程402条

公表・説明の言葉：確定・調査中・対策を混ぜない

早すぎる断定も、遅すぎる沈黙も信頼を損なう。言葉の使い分けで精度を示す。

確定した事実	調査中の事項	講じた・講じる対策
「〇月〇日、当社サーバが第三者による不正アクセスを受け、暗号化されたことを確認しました」	「個人情報が外部に流出したおそれがあり、専門機関と調査を進めています」	「外部接続を遮断し、関係当局へ報告しました。調査結果は判明次第お知らせします」

漏えい	外部に流出したことが確認された状態
漏えいのおそれ	流出した可能性を否定できない状態（報告対象になり得る）
不正アクセス	権限なく侵入された事実。漏えいとは別の概念
影響範囲	対象システム・データ・人数。暫定値か確定値かを明示

⚠ 避けたい表現

- 「被害はありません」（調査前の断定）
- 「高度な攻撃で防ぎようがなかった」（対策不備の検証前）
- 攻撃者との交渉状況の詳細

CHAPTER 5

説明責任：
何で、どう証明するか

「認証を取っています」は出発点にすぎない。何を、誰が、どの基準で、どの期間について確認したのかを読み解く。

この章のキーワード

- 認定と認証
- ISO/IEC 27001（アイエスオー・ニーナナゼロゼロイチ）
- SOC 2（ソック・ツー）
- PCI DSS
- ISMAP（イスマップ）
- NIST（ニスト） CSF 2.0
- リスクアペタイト

A社の事例（架空）

1か月後

取締役会で社外取締役が問う。「当社のリスク管理体制は、どの基準に照らして十分だったのか」。

同じ週、主要取引先からセキュリティ質問票が届く。「ISO/IEC 27001の認証範囲、SOC 2報告書、NIST CSFとの対応表を提出してください」。保守ベンダーには「認証は取っていますか」と聞いていただけだった。

一時停止して考えてみてください

「認証は取っていますか」――この質問には何が足りないでしょうか？

「認証を取っています」を読み解く：何を、誰が、どう確認したか

認定機関は認証機関を見る。認証機関は企業を見る。証明の形式によって重みが違う。

認定機関
例：ISMS-AC、JAB

↓

認証機関
審査し認証書を発行

↓

企業・組織
認証を受ける側

NIST（ニスト） CSF 2.0は認証ではない
統治を中心に6機能で、足りない点を経営に説明する枠組み

	ISO/IEC 27001 アイエスオー・ニーナナゼロゼロイチ	SOC 2 ソック・ツー	PCI DSS	ISMAP イスマップ	質問票回答
形式	認証	保証報告書	準拠評価	登録	自己宣言
確認者	認証機関	監査人	QSA／自己問診	監査機関・運営委員会	なし（自社申告）
対象	組織のISMS	サービスの統制	カード会員データ環境	政府向けクラウド	回答した範囲
見るポイント	認証範囲・適用宣言書	Type II・例外事項・CUEC	対象範囲・AOC	登録サービスの範囲	裏付け資料

SOC 2はType II（一定期間の運用評価）を。CUEC（利用者側に求められる統制）は自社の宿題。

参照：ISMS-AC、日本適合性認定協会（JAB）、AICPA、PCI SSC、ISMAP運営委員会、NIST CSF 2.0

取締役会の言葉：サイバーリスクを「経営リスク」として語る

ゼロリスクはない。残るリスクを、誰が、どこまで引き受けたかを示すことがガバナンスの核心。

リスクアペタイト Risk appetite
組織として許容するリスクの水準。投資判断の物差し。

リスクオーナー Risk owner
リスクを引き受け、対応に責任を持つ者・部門。

残余リスク Residual risk
対策後もなお残るリスク。受容・移転（保険）等を判断。

管理策 Control
リスクを下げる手段。技術・手続・教育を含む。

取締役会で問うべき5つのこと

- 当社にとって重大なサイバーリスクは何か
- 各局面（入口・中・出口・復旧）の対策と例外は
- 重要な委託先の管理状況は
- 事故時の判断権限と連絡順は決まっているか
- 残余リスクと、そのための投資・保険は

関係法令・ガイドライン

- 内部統制システムの整備：会社法362条4項6号・5項（大会社）
- 損失の危険の管理に関する規程その他の体制：会社法施行規則100条1項2号
- 役員の任務懈怠責任：会社法423条1項／第三者に対する責任：同法429条1項
- 個人データの安全管理措置：個情法23条／委託先の監督：同法25条
- 経営者の関与：経済産業省・IPA「サイバーセキュリティ経営ガイドライン Ver3.0」
- 金融機関：金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」（2024年10月）

CASE REVIEW

A社の72時間を振り返る：止められた地点は6つあった

どれか一つが機能していれば、被害の姿は大きく変わった。

1 3週間前
委託先ID
委託先VPN IDへのMFA適用、VPN装置の脆弱性修正
IAM（アイアム）／脆弱性管理

2 金 18:10
人・認証
番号照合型MFA、パスキー、報告しやすい文化
耐フィッシング認証

3 土 深夜
横展開
区画分け、特権IDの管理、委託先の接続先限定
セグメンテーション／PAM（パム）

4 土 深夜
持出し
深夜の大量送信の検知・遮断
DLP／通信監視

5 月 06:12
検知
24時間365日の監視と自動隔離
EDR＋SOC（ソック）／MDR

6 日 深夜
復旧
隔離・変更不能なバックアップと復元訓練
イミュータブル／RTO

さらに事故後：連絡順・判断権限の事前決定（CSIRT（シーサート））と、証拠保全を踏まえた復旧手順（フォレンジック）

CLOSING

用語の暗記ではなく、「事故のときに何を聞くか」を持ち帰る

入口	どこから入ったか。例外のIDや未修正の装置はないか
防御	4つの局面で、何が止め、何が止めなかったか
対応	いつ認定し、誰が決め、何を保全したか
説明	何の基準で、どの範囲を、誰が確認したか

会議で使えるようにしたい10語

1. **BEC**
2. **MFA／IAM**（アイアム）
3. **ゼロトラスト**
4. **EDR**
5. **SOC**（ソック）
6. **DLP**
7. **RTO／RPO**
8. **CSIRT**（シーサート）
9. **ISO/IEC 27001**（アイエスオー・ニーナナゼロゼロイチ）
10. **SOC 2**（ソック・ツー）

主な参照情報

- 個人情報保護法23条・25条・26条、同法施行規則7条・8条・10条、個人情報保護委員会ガイドライン（通則編）
- 会社法362条4項6号・5項、423条1項、429条1項、会社法施行規則100条1項2号／不正アクセス禁止法3条・4条・7条／刑法168条の2・234条の2
- IPA「情報セキュリティ10大脅威 2026」 https://www.ipa.go.jp/security/10threats/
- 経済産業省・IPA「サイバーセキュリティ経営ガイドライン Ver3.0」、金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」
- NIST CSF 2.0／SP 800-61 Rev.3／SP 800-207 https://www.nist.gov/cyberframework ／ CIS Controls v8.1
- ISO/IEC 27001:2022・ISMS-AC https://isms.jp/ ／ OWASP https://owasp.org/ ／ JPCERT/CC https://www.jpcert.or.jp/

注：規格・制度・ガイドラインは改訂されるため、最新版と正式な適用範囲は各原典で確認されたい。本資料の事例は架空である。