企業に求められるレジリエンス要件とセキュリティ投資の考え方

成熟度マトリクスで読み解く現在地とステップアップ方針

Incident Lake

Agenda

01 レジリエンスは「要望」から「要件」へ変わる

02 現場は対応できる状態にあるか

03 自社診断 — 8観点×5段階の成熟度マップ

04 国内企業に多い Level 2〜3 の典型状態

05 Level 2〜3 のままだと何が起きるか
— 国内大手の事例

06 先進企業はどこまで進んでいるか
— 先進企業の事例

07 Level 2〜3 から Level 4〜5 へ進むための
具体的アクション

08 セキュリティ投資の目安
— JCIC の目安値で投資水準を考える

09 現場の対応を支える実装基盤
— Incident Lake

10 社内で議論すべき5つの問い

Appendix

CHAPTER 01

レジリエンスは「要望」から「要件」へ変わる

企業に求められるレジリエンス水準

レジリエンスへの要求はグローバル規制や国内所管庁の動きなど、複数の層から同時に求められている。
また、近年のサイバーセキュリティは、現場の技術課題から、経営が説明責任を負う経営課題へと位置づけが変わりつつある。

	所管／枠組み	主な内容
国内	経済産業省	経済産業省が公表する「サイバーセキュリティ経営ガイドライン Ver3.0」。サイバーセキュリティリスクを企業リスクマネジメント上の重要課題として位置づけ、経営者のリーダーシップのもと、体制整備、必要な投資、サプライチェーンを含む対策を進める考え方を示している。企業は、経営層がリスクを把握し、体制・資源配分・対応方針を判断できる状態を整えることが重要となる。
	総務省	電気通信事業法令に基づく電気通信事故の報告制度と、総務省による事故検証の取組み。報告対象となる重大な事故等について、電気通信事業者には総務大臣への報告が求められる。サイバー攻撃を含む様々な要因による事故を念頭に、原因・影響範囲・復旧措置・再発防止策を整理し、報告・利用者周知・再発防止につなげられる体制が重要となる。
	経済産業省／IPA	経済産業省・国家サイバー統括室の制度構築方針に基づき、IPAが運営する「サプライチェーン強化に向けたセキュリティ対策評価制度」。発注者は取引先・委託先に必要な対策水準を示し、実施状況を確認する。企業には、発注者として相手先を確認し、受託者として自社の対策を説明できる状態を整えることが重要となる。
	会社法・民法	取締役の善管注意義務や、内部統制システム構築に関わる法的枠組み。会社法・民法がサイバーインシデント対応を直接・一律に義務づけるものではないが、合理的な備えや、判断・復旧・説明・改善を行える体制が欠けている場合には、善管注意義務や内部統制システム構築の適切性との関係で問題となり得る。企業は、対応体制と判断・対応の証跡を整えることが重要である。
	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」。ガバナンス、特定、防御、検知、対応・復旧、サードパーティリスク管理の観点を整理している。金融機関等には、規模・特性や、自ら直面するリスクの重要性・緊急性を踏まえつつ、委託先管理を含む管理態勢を整備・運用し、インシデント時の対応・復旧を含めて説明できる状態を整えることが求められる。
海外	EU DORA	EU金融セクターを対象とするデジタル・オペレーショナル・レジリエンス規則。ICTリスク管理、重大ICTインシデント報告、レジリエンステスト、ICTサードパーティリスク管理を求める。EU金融機関のICT委託先となる企業は、委託元のDORA対応を通じて、復旧・報告・委託先管理に関する情報提供や契約上の要求を受ける可能性がある。
	NIST CSF 2.0	サイバーセキュリティ管理の国際的なベストプラクティスとして広く参照される任意のフレームワーク。従来の5機能に「Govern（統治）」が追加され、ガバナンスが中核要素として明確化された。組織は、サイバーリスクを現場任せにせず、責任分界・判断権限・方針・監督のあり方を明確にすることが重要となる。
	米国 SEC サイバー開示規則	米国SECのサイバーセキュリティ開示規則。Form 8-K提出義務のある米国国内登録企業には、重要なサイバーインシデントについて、重要性判断後4営業日以内の開示を求める。あわせて、リスク管理・戦略・ガバナンスの年次開示も求める。企業は、影響把握、経営報告、開示判断を迅速に行える体制を整える必要がある。

日本企業がレジリエンスを高めにくい4つの理由

日本企業がレジリエンスを高めにくい理由は、対策の必要性を理解していないからではない。内製志向、復旧責任の部門依存、経営優先度の低さ、文書整備止まりによって、現場の努力が組織的な対応能力へ転換されにくいからである。

01

内製志向による停滞

自社で作ろうとするが、
設計・運用の複雑さの前で止まりやすい

02

復旧責任の部門依存

復旧判断が情報システム部門やSREに閉じ、
経営判断につながりにくい

03

経営優先度の低さ

現場では課題が見えていても、平時には効果が
見えにくく、経営アジェンダになりにくい

04

文書整備止まり

ポリシーやBCPは整備されているが、
訓練・検証・改善まで落とし込まれていない

CHAPTER 02

現場は対応できる状態にあるか

経営課題として取り組むべき属人化の解消

実態調査では、インシデント対応が退職懸念のあるキーパーソンに依存している実態が見えた。属人化が解消されないのは「組織として優先度が上がらないため」と出ており、事業継続に関わるトラブルが現場任せになっている状態が明らかになった。

インシデント対応が特定の1〜2名に集中・依存していると感じるか？

72.0%
依存している

依存している人材が直近1〜2年以内に退職・転職・異動する可能性はあるか

88.9%
可能性がある

属人化が集中している業務はどこか

56.1% 障害の原因調査・ログ解析

51.7% 一次アラートの受け・トリアージ判断

属人化解消に向けた取り組みを実施したことがあるか

※**32.4%**
取り組んだが改善しなかった

属人化解消に取り組めない最大の理由は何か

※**32.0%**
組織として優先度が上がらない
（経営の関心が低い）

属人化解消を支援する専用ツール／基盤があれば導入を検討したいか

69.6% 前向き

89.2% 興味あり含む

インシデント対応の属人化に関する実態調査2026（n=250 / システム障害対応に関わる企業担当者を対象）
※「取り組んだが改善しなかった」「組織として優先度が上がらない」は、それぞれの設問における最多回答

要求水準と実態のギャップから生じる事業リスク

求められるレジリエンス水準は、経営判断・説明責任・サプライチェーン対応・報告開示まで広がっているが、対応は属人化している。このギャップにより、復旧・説明遅延による企業評価の低下や再発防止の遅れという事業リスクが生じ得る。

求められる水準	現場の実態	生じ得るリスク
経営判断・説明責任が求められる	重大時の判断が特定人材に依存	初動判断や経営報告が遅れ、事業停止の長期化や経営責任の問題に発展
取引先・委託先を含むサプライチェーン上の説明責任が問われる	影響範囲や依存関係の把握が、特定人材の経験に依存	取引先・顧客への影響説明が遅れ、契約継続・委託先評価・顧客信頼に影響
影響範囲・判断理由・復旧状況を記録できることが求められる	ログ解析・原因調査が属人化	原因特定や復旧判断が遅れ、復旧長期化・再発防止不全につながる
文書整備だけでなく、体制の実効性が問われる	文書はあるが、訓練記録・対応証跡・改善履歴が不十分	重大時に手順が機能せず、対応ばらつき・復旧遅延・改善サイクル形骸化に
インシデント報告・開示の迅速性が求められる場面が増えている	社内外への状況報告・エスカレーションが属人化している	報告・開示の遅延や説明不備により、当局・顧客・市場からの信用低下を招く

CHAPTER 03

自社診断 ―― 8観点×5段階の成熟度マップ

レジリエンス成熟度マトリクス

国内外の指針・制度が求める要件に、どの程度対応できているか把握するための成熟度マトリクスを作成。
各種規制の共通要素とソフトウェア成熟度モデルのCMMIの発想を基に、独自の成熟度モデルを整理した。

8つの観点 ＼ 5段階のレベル	Level.1 無管理 決まった手順・担当がなく対応が場当たり的	Level.2 個人依存 特定人材の経験と勘で回っている	Level.3 部門管理 部門内では整備されているが、組織横断・経営層への接続が弱い	Level.4 組織管理 経営層を含めて、責任・判断・訓練が組織的に整備されている	Level.5 持続的管理 記録・分析・改善が継続的に回り、対応能力が更新され続けている
① ガバナンスと責任分界	重大時の判断者・経営報告ライン・部門横断の責任分担が定義されているか				
② 資産・重要業務・依存関係の特定	重要業務と、それを支えるシステム・委託先・クラウド・認証基盤の関係が把握されているか				
③ 攻撃面最小化	外部公開資産・特権ID・脆弱性・設定不備が棚卸し・優先対応されているか				
④ 可観測性	ログ・アラート・対応記録が集約され、影響範囲や類似事例を追えるか				
⑤ 証跡性・監査可能性	対応の記録が、後から監査・リスク管理・当局・顧客に説明できる証跡になっているか				
⑥ 対応基盤の可用性	本番障害時にも、連絡・記録・意思決定の手段が使える状態か				
⑦ 復旧可能性	RTO/RPO・復旧優先順位・手動継続手順が定義され、訓練・検証されているか				
⑧ 判断理由の記録性と継続改善	判断理由、再発防止策、未解決リスクが構造化され、経営報告・改善サイクルに接続されているか				

※ 8観点と公的・国際フレームワークの対応の詳細は巻末 Appendix B に掲載。

CHAPTER 04

国内企業に多い Level 2〜3 の典型状態

成熟度Level 2〜3の企業に見られやすい状態

ネット調査の結果から、多くの企業・現場では『仕組みではなく人で回す状態にある』ことが確認できている。以下の『Level 2〜3企業に見られる典型状態』と自社の状況を見比べ、ステップアップが必要な観点はないのか確認していただきたい。

8つの観点	Lv.2〜3 典型状態	内容
① ガバナンスと責任分界	重大時の判断者・責任分担が定まっていない	ポリシーや規程は整備されていても、重大インシデント時に誰が判断し、どの部門がどの責任を負うかが取り決められておらず、実際には機能しない
② 資産・重要業務・依存関係の特定	重要業務と依存関係が結びついていない	システムの一覧はあるが、重要業務を支える委託先・クラウド・認証基盤との関係が整理されておらず、障害時にどの業務が止まり、どこへ波及するかを追えない
③ 攻撃面最小化	攻撃面の棚卸しが部門任せになっている	外部公開資産・特権ID・脆弱性・設定不備の棚卸しが部門ごとにばらつき、全社横断の優先度づけがないため、未適用パッチや過剰な権限が放置されやすい
④ 可観測性	可観測性が個人に依存する	ログ解析や影響範囲の特定が、特定人材の経験に依存している
⑤ 証跡性・監査可能性	対応記録が監査・説明に耐えない	対応の記録が個人メモやチケットに散在し、いつ誰が何を判断したかを後から監査・当局・顧客に独立して説明できる証跡になっていない
⑥ 対応基盤の可用性	障害時の代替手段が用意されていない	連絡・記録・意思決定をふだんのツールに頼っており、本番障害でそれらが同時に止まった場合に動ける代替手段が決まっていない
⑦ 復旧可能性	復旧手順が訓練・検証されていない	復旧手順やBCPは文書としてあるが、RTO/RPO・復旧優先順位を実際に動かして訓練・検証したことがない
⑧ 判断理由の記録性と継続改善	振り返りが改善・KPIに回らない	ポストモーテムが現場内で終わり、判断理由・再発防止策が構造化されず、経営の改善サイクルやKPIにつながらない

※本図は典型的な現在地のイメージであり、実測値ではない。実際の位置は組織により異なる。

企業の成熟度がLevel 2〜3で止まりやすい理由

Level 2〜3 の企業は、現場が何の対応もしていないわけではない。課題なのは、現場の努力が、組織能力・経営判断・説明責任の仕組みへと転換できていないことにある。

Level 2〜3企業によくある5つの壁

現場が優秀だから回ってしまう

障害のたびに「あの人に聞けば解決する」が積み重なり、属人化が“優秀さの副産物”として強化される。問題が顕在化しないまま、依存度だけが上がっていく。

文書があることで安心してしまう

第1章で挙げた「文書整備に留まる」状態は、現場では“作って終わり”として現れる。BCPや手順書が監査・規程対応のために整備された結果、最後に手順を実際に動かしたのがいつか、すぐに答えられないケースも少なくない。

予算化しにくい

第1章で触れた「平時には効果が見えにくい問題」は、予算プロセスでより具体的な壁になる。レジリエンス投資は“何も起きなかったこと”が成果でありROIを数値で示しにくいため、売上に直結する施策に予算が優先される。

部門横断しにくい

第1章の「復旧責任が情シス・SREに閉じる」構造は、重大時に部門間の溝として現れる。インシデントは技術・法務・広報・経営の判断を同時に要するが、平時に連携線が引かれていないため、有事になって初めて「誰が何を決めるのか」を検討することになる。

外部説明を想定していない

社内復旧を優先するあまり、顧客・当局・取引先への説明に必要な情報（影響範囲・時系列・対応根拠）が、後から再構成できない形でしか残らない。これらは事後にまとめようとしても再現できないため、対応の最中に記録できる仕組みをあらかじめ設計しておく必要がある。

CHAPTER 05

Level 2〜3 のままだと何が起きるか ― 国内大手の事例

Level 2〜3 のままだと何が起きるか ― 国内大手のトラブル事例

事故原因は各社異なるが、攻撃か障害かを問わず共通していたのは「異常に気づけない／障害時に動けない／復旧が長引く」という観点だった。自社においても同じ観点がLevel 2〜3の状態であれば、同種の事態は起こりうるという警鐘になる。

企業名 （業界）	企業規模 （連結売上／従業員数）	トラブル内容	被害規模
アサヒグループHD （食品・飲料）	約2.9兆円 約2.8万人	2025年9月29日朝、ランサムウェア攻撃でシステム障害が発生（侵入は約10日前）。受注・出荷・コールセンター業務が停止。受注・出荷業務のシステム利用再開まで約2カ月、配送リードタイムを含む物流業務全体の正常化まで約5カ月（〜2026年2月）	個人情報漏えい115,513件。 サイバー攻撃関連の特別損失は未開示（2026年7月8日 通期決算で開示予定）
KADOKAWA （出版・メディア）	約2,779億円 約8千人	2024年6月8日に発覚。フィッシングで窃取した認証情報を起点とするランサムウェア攻撃で、ニコニコ等Webサービス・出版製造/物流・経理が広範に停止。主要サービス再開まで約2カ月	個人情報漏えい確認 254,241人分。 特別損失 24億13百万円、 通期業績影響 売上▲83億円・営業利益▲47億円
みずほ銀行・FG （金融）	約3.2兆円 約5.4万人	2021年2月28日〜9月30日に自社システム障害が続発（対象8事案）。ATM網の広範停止、外為送金の遅延、外為法上の確認義務の履行が不十分とされた。報道では、業務改善命令に基づく定期報告が不要となるまで約3年を要したとされる	2/28に ATM最大4,318台停止・通帳/カード取込 5,244件・5,000人超の顧客負担。金融庁 業務改善命令2回＋財務省 是正措置命令、経営陣4名辞任。金銭被害額の公表は中心でなく、行政処分・経営責任が主たる帰結
KDDI （通信）	約5.4兆円 約4.9万人	2022年7月2日 1:35、全国中継網ルータのメンテナンス作業での経路誤設定を起点に、VoLTE交換機・加入者DBの輻輳が連鎖（攻撃ではない）。全国規模で 7/2 1:35〜7/4 15:00、合計61時間25分の通信障害	のべ3,091万人以上に影響（総務省発表ベース。緊急通報・物流・交通・金融・IoT・MVNOに波及）。総務省厳重注意＋行政指導。返金・補償 総額約73億円（沖縄セルラー含む業績影響見込み約75億円）
アスクル （流通・EC）	約4,811億円 約4千人	2025年10月19日、委託先向け管理者アカウントの認証情報漏えい・MFA未適用を突破口とするランサムウェア攻撃を検知。同日 ASKUL／ソロエルアリーナ／LOHACO の受注・出荷を停止。本格復旧フェーズ移行（12/12）まで約2カ月	個人情報流出確認 約74万件。無印良品・ロフト等の委託元ECや医療・介護等の供給に波及（3PL下流波及）。2026年5月期第2四半期に、ランサムウェア関連の影響額 約120億円、システム障害対応費用として特別損失52億円を計上

※各事例の詳細は巻末 Appendix Cを参照。

CHAPTER 06

先進企業はどこまで進んでいるか ― 先進企業の事例

レジリエンスの高い企業のトラブル対応力

レジリエンスのある企業でも、トラブルを完全に防ぐことはできない。公開情報から見える共通点はトラブル後の対応にあり、影響範囲を把握し切り分け、代替手段による業務遂行、速やかな復旧と改善策の実行などに顕著な差が見られる。

	JAL	トヨタ自動車／小島プレス工業	Norsk Hydro
企業・業界	航空・運輸業 1兆8,440億円／約4万人	自動車・製造業／サプライチェーン業 48兆367億円 ／約40万人	アルミ・素材／再生エネ 約3.6兆円／約3万人
トラブル内容	2024年12月26日、社内外接続用のネットワーク機器が外部からの大量通信により過負荷となり、社外連携システムに不具合が発生。国内線・国際線の一部遅延、同日出発便の航空券販売停止など、予約・販売・運航関連業務に影響が波及した。	2022年2月26日、主要サプライヤーである小島プレス工業が不正アクセス被害を受け、部品供給関連システムに障害が発生。トヨタは3月1日に国内14工場28ラインを停止し、サプライヤー起点の障害が完成車メーカー本体の生産停止に直結した。	2019年3月19日、ランサムウェア攻撃により、グローバル全体のIT環境・生産関連業務に影響。特にExtruded Solutions事業では生産・受発注処理に大きな支障が出て、操業影響と財務損失が発生。サイバー攻撃の被害額は約8億NOK（約136億円）と推定。
復旧	原因となった社内外接続ルーターを遮断し、システムを順次復旧。同日中に航空券販売を再開し、空港業務は有人対応などの代替運用で継続した。	小島プレスは紙・手作業による代替運用に切り替え、部品供給業務を継続。トヨタは国内14工場28ラインを1日停止した後、翌日から稼働を再開した。	攻撃後、影響拡大を防ぐためにネットワーク・システムを切り離し、拠点・業務ごとに手作業や代替手順へ切り替えた。社内外の専門家を投入した24時間体制で、PC・サーバーの確認、洗浄、バックアップからの再構築を進め、全社復旧につなげた。
成熟度観点	④可観測性 ⑥対応基盤の可用性 ⑦復旧可能性	①ガバナンスと責任分界 ②依存関係の特定 ⑥対応基盤の可用性 ⑦復旧可能性	①ガバナンスと責任分界 ④可観測性 ⑥対応基盤の可用性 ⑦復旧可能性 ⑧継続改善
レジリエンスポイント	障害の原因となった社内外接続ルーターを特定し、当該機器を一時遮断することで影響を切り分け、システムを順次復旧できた点がポイント。加えて、航空券販売の再開や空港での有人対応など、影響範囲を限定しながら業務を継続・復旧する運用が機能した。	サプライヤー起点の障害でも、完成車メーカー側で国内全工場停止・再開を判断できる意思決定体制があった点が肝。加えて、小島プレス側では紙かんばん・図面・手作業による代替運用で、納入先・納入時刻・必要部品の確認を継続。完全なシステム復旧を待つのではなく、供給継続に必要な最低限の運用基盤を確保、翌日再開につなげた点がレジリエンス上のポイント。	身代金を払わず、外部専門家を即時投入し、手作業運用・バックアップ復元・段階的復旧を並行させたことで、全社的な攻撃下でも一部事業は通常に近い生産を維持した。復旧後にセキュリティチームを再編し、検知・対応力の強化まで行った点も、単なる復旧ではなく改善まで含むレジリエンスとして評価できる。

※ 本資料は各社の総合的な成熟度を評価・格付けするものではない。公開情報から、トラブル発生後にレジリエンスが機能した局面を整理したものである。

CHAPTER 07

Level 2〜3 から Level 4〜5 へ進むための具体的アクション

レジリエンスを高めるステップアップアクション

先進企業との差は「観点ごとの具体的アクションを組織として回しているか」にある。自社の現状を可視化し、次のステップに行くために必要なアクションを組織で推進することで、着実にレジリエンスは高まっていく。

8つの観点	Lv.2〜3 の状態	Level 4〜5 へのステップアップアクション
① ガバナンスと責任分界	重大インシデント時の判断が情シス・SREに依存し、経営層の関与基準が曖昧。いざという時に「誰が止め、誰が公表し、誰が報告するか」が決まっておらず、判断と対外対応が遅れる。	重大インシデントの判定基準・最終判断者・経営報告ライン・法務・広報・事業部門のRACIを1枚に整理、机上演習で検証。
② 資産・重要業務・依存関係の特定	システム一覧はあるが、重要業務・委託先・クラウド・認証基盤との関係が見えない。障害時にどの業務が止まり、どこから波及するかが分からず、影響範囲の把握が遅れる。	重要業務トップ10 を選び、関連システム・データ・委託先・クラウド・認証基盤・代替手段を紐づけた依存関係マップを作成
③ 攻撃面最小化	脆弱性・権限・外部公開資産の棚卸しが部門ごとにばらつく。未適用パッチや過剰な権限が放置され、侵入の入り口になりやすい。	外部公開資産・特権ID・未適用パッチ・設定不備を月次で棚卸しし、重要業務に紐づくリスクから優先対応。
④ 可観測性	ログ解析や影響範囲特定が特定人材の経験に依存している。その人がいないと何が起きたか追えず、検知も復旧も属人化・長期化する。	重要システムのログ・アラート・対応記録を共通基盤に集約し、過去類似インシデント・影響範囲・判断履歴を検索可能に
⑤ 証跡性・監査可能性	対応記録が個人メモやチケットに散在しており、第一線の対応を第二線・第三線・内部監査が後から独立して検証できない。結果として「いつ誰が何を判断したか」を、監査・当局・顧客に説明しにくい。	対応時刻・判断者・判断理由・実施内容・承認履歴を改ざん困難な形で保存。内部監査・リスク管理・法務・外部説明に利用可能な監査証跡として整備。
⑥ 対応基盤の可用性	障害時に使うチャット・チケット・監視・連絡手段も同時に使えなくなる可能性がある。対応や連絡そのものが止まり、初動が遅れる。	障害時にも使える代替連絡手段・記録手段・意思決定ログの保存場所を決め、訓練で実際に利用。
⑦ 復旧可能性	復旧手順やBCPはあるが、実際に訓練・検証されていない。いざ障害が起きると手順どおりに動かず、復旧が想定外に長引く。	重要業務ごとに RTO/RPO・復旧優先順位・手動業務継続手順を定義し、机上演習・実地訓練で復旧可能性を検証。
⑧ 判断理由の記録性と継続改善	ポストモーテムが現場内で終わり、経営報告や改善 KPI につながらない。同じ失敗が繰り返され、再発防止が定着しない。	インシデントごとに原因・判断理由・再発防止策・未解決リスク・改善期限を構造化し、月次の経営報告・改善 KPI に接続。

レジリエンス強化はまず1つの重要業務から始める

レジリエンスの強化は、8観点を最初から一斉に整備する必要はない。まずは事業影響の大きい業務を1つ選び、その業務に関わる依存関係・判断基準・復旧手順・報告ラインを整理し、インシデント時に実際に機能するかを検証することから始める。

step1
重要業務の選定

止まると売上、顧客対応、社会的責任、法規制対応に大きな影響が出る業務を1つ選定。たとえば、決済、受注・出荷、請求、予約、本人認証、会員基盤、給電・通信など、停止時に顧客影響や対外説明が必要になる業務を対象に。

整理事項

- 停止時の売上・顧客・社会・規制影響を確認
- 業務・システム責任者、経営報告先を明確化
- どの状態で重大インシデントと判断するか

成果物

対象業務の選定理由／影響評価メモ／責任者・報告ライン／重大判定基準　など

step2
影響範囲と復旧必要情報整理

選んだ重要業務が、どのシステム、データ、委託先、クラウド、認証基盤に支えられているかを整理。あわせて、障害時に確認すべきログや対応記録、連絡手段、復旧手順がどこにあるかを確認。見るべきなのは、単なるシステム構成ではなく、「どこが止まると業務影響が出るか」「復旧判断に必要な情報は見つかるか」

整理事項

- 重要業務に紐づくシステム、データ、委託先、クラウド、認証基盤の洗い出し
- ログ、アラート、対応記録、連絡手段、復旧手順の所在を確認
- RTO/RPO、代替手段、単一障害点を確認

成果物

依存関係マップ／ログ・記録所在一覧／復旧手順一覧／RTO・RPO整理／単一障害点リスト　など

step3
演習で検証し改善方針決定

整理した内容をもとに、重大インシデントが起きた想定で机上演習を実施。発生検知から、重大判定、影響範囲の把握、復旧判断、経営報告、顧客・取引先への説明までを一連で確認。演習で見つかった不足点は、現場の反省で終わらせず、改善テーマとして整理し、責任者・期限・予算を決定。

整理事項

- 重大判定、復旧判断、社内外報告まで通し確認
- 判断理由、対応記録、報告内容は説明可能か
- 不足ログ、手順、体制、権限、予算の洗い出し
- 改善テーマ毎に責任者、期限、必要予算を決定

成果物

演習シナリオ／演習記録／判断・報告記録／未解決リスク一覧／改善計画／経営報告サマリ　など

CHAPTER 08

セキュリティ投資の目安 ―
JCIC の目安値で投資水準を考える

JCIC基準で見るレジリエンスを高める投資目安

JCICが示す目安値は、セキュリティ投資を「高い／安い」の感覚論ではなく、連結売上高や従業員数に対する比率で議論するための共通言語である。重要なのは、自社の企業規模・業種・リスク特性に照らして、現在の投資水準が十分か、どこまで引き上げるべきかを経営層と判断できる状態にすることである。

企業規模	業種	投資目安※	セキュリティ人員数※
大企業 連結売上高 1,000 億円以上	金融	0.6%	0.8%
	IT・情報通信	0.5%	0.6%
	社会インフラ	0.3%	0.3%
	製造	0.2%	0.2%
	小売・サービス・その他	0.1%	0.1%
中堅企業 連結売上高 100〜1,000 億円	業種横断	0.3%	0.2%

出典：JCIC「企業規模・業種別に見るセキュリティ投資・人員数の目安値」
＊投資額は連結売上高に対する割合、投資には人件費を含む。セキュリティ人員数は全従業員数に対する割合、専任・兼務・外部委託まで含めたFTEベース。

ポイントは「防御」に偏らないセキュリティ投資

近年の規制・フレームワークは「防ぐ」だけでなく「起きた後にどう持ちこたえ、立ち直るか」を重視している。
インシデント対応・復旧・記録・報告・改善と、セキュリティ投資は配分バランスが重要になっている。

投資配分で見る4つの領域

起きる前の投資 ／ 起きた後に、持ちこたえ・立ち直るための投資

① 防御・検知

発生可能性を下げ、
兆候を早く捉える

主な投資対象

EDR／WAF／脆弱性管理
監視／SIEM／認証強化

② 対応・判断

発生後に状況を把握し、
判断を遅らせない

主な投資対象

インシデント管理／判定基準
エスカレーション／対応記録

③ 復旧・継続

重要業務を止め続けず、
早期に戻す

主な投資対象

BCP／DR／バックアップ
代替手段／復旧訓練

④ 記録・報告・改善

説明責任を果たし、
再発防止につなげる

主な投資対象

報告書／監査証跡
ポストモーテム／改善KPI

防御・検知はあくまでも大前提。レジリエンスを高めるには、
発生後に 判断できる 戻せる 説明できる 改善できる 状態へ**投資を配分**する必要がある。

CHAPTER 09

現場の対応を支える実装基盤
— Incident Lake

Level 2〜3の典型状態は人手・個別ツール運用では再発しやすい

第4章で見たLevel 2〜3の典型状態は、方針や手順を決めるだけでは解消しにくい。代替手段や復旧手順、改善サイクルが個別ツールや人の記憶に分散したままでは、対応経験は組織知にならず、属人化や改善停止が繰り返されやすい。

第4章で見た典型状態	人手・個別ツール運用での現れ方
【1】重大時の判断者・責任分担が定まっていない	有事に誰が停止判断・復旧優先順位・顧客連絡を決めるのかが曖昧になり、初動判断が遅れる
【2】重要業務と依存関係が結びついていない	システム・委託先・クラウド・認証基盤と業務影響が別々に管理され、影響範囲の特定に時間がかかる
【3】攻撃面の棚卸しが部門任せになっている	外部公開資産・特権ID・脆弱性・設定不備の情報が部門ごとに散在し、優先順位が揃わない
【4】可観測性が個人に依存する	ログ・チケット・チャットが分散し、原因調査や影響範囲の特定を特定人材に頼る
【5】対応記録が監査・説明に耐えない	時系列、判断理由、承認履歴、対応根拠が整理されず、監査・当局・顧客向けに再構成が必要になる
【6】障害時の代替手段が用意されていない	本番環境や通常の連絡手段が止まった際に、連絡・記録・意思決定を継続できない
【7】復旧手順が訓練・検証されていない	復旧優先順位やRTO/RPOを実際に動かして検証しておらず、有事にどの業務から戻すべきか判断できない
【8】振り返りが改善・KPIに回らない	ポストモーテムで出た課題が、改善タスク・責任者・期限・KPIに落ちず、次回対応に反映されない

第2章で取り上げた属人化調査では、属人化が集中する業務は「障害の原因調査・ログ解析」が56.1%で最多となり、
全体の32.4%が「属人化解消に取り組んだが改善しなかった」と回答している。
この結果は、第4章で見たLevel 2〜3の典型状態と重なる。従来の「防御・検知」への投資だけでは、
インシデント発生後に必要な「判断・記録・報告・改善」のレベルまで上げることができないことを示唆している。

インシデント対応を1基盤で支えるIncident Lake

Incident Lakeは、散在する対応情報・判断履歴・過去事例を統合し、インシデント発生後の状況把握、意思決定、報告、改善を一気通貫で支える基盤。既存の監視・チケット・チャット・ドキュメントを活用・統合するインテリジェンスレイヤー。

INPUT
既存運用ツール／散在する運用データ

- Slack
- Teams のメッセージ
- GitHub の Issue
- PR
- Datadog
- Sentry のアラート
- ログ
- メトリクス
- トレース
- ポストモーテム
- 手順書

ツール跨ぎで分断され、
全体像の把握が困難な状態

Incident Lake
AI インシデント・インテリジェンス層

01 リアルタイム・データ統合
散在する情報を AI が束ね、
「今何が起きているか」を全員が把握

02 暗黙知の構造化・資産化
LLM ×蓄積された自社の対応ログを基に、
AI が次の一手を提示

03 AIによる意思決定支援
意思決定プロセスをデータ化し、組織知として蓄積
社内レポート・当局報告・ポストモーテムを
宛先別に自動作成

OUTPUT
意思決定の高速化

リアルタイムな状況要約
「今、何が起きているか」を即把握

類似事例のサジェスト
過去事例から初動判断を支援

ポストモーテム自動生成
監査・顧客報告に耐える品質を担保

重大度の自動判定
特許出願中（特願2025-202718）

カバー領域	対象インシデント：システム障害 ／ セキュリティ事故 ／ オペミス ／ コンプラ違反（業種・職種を問わず）
特化領域	NIST CSF 2.0 「復旧（Recover）」領域に特化 — 監視・チケット・内製ツールが届かない空白地帯／認証：SOC 2 Type 1 取得

観点別に見るIncident Lake の支援領域

Incident Lakeは、記録集約、判断理由の保存、証跡保全、自動レポート、ポストモーテム管理、改善タスク管理などを通じて、Level 2〜3からLevel 4〜5への移行を支援し得るSaaSプロダクトである。

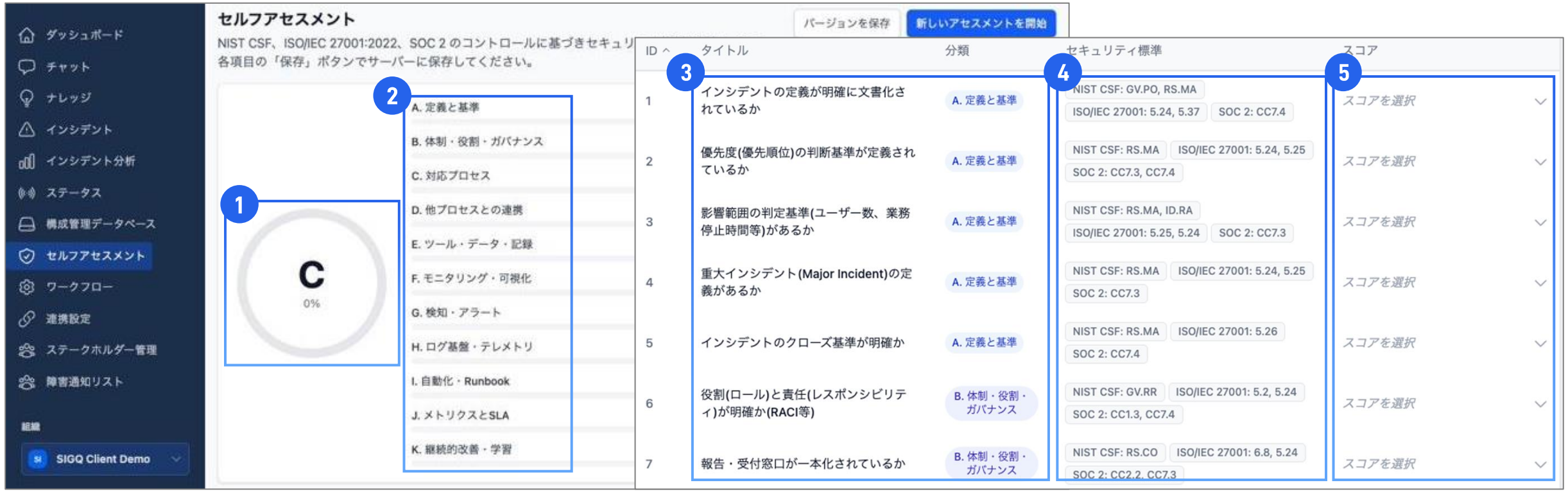
8つの観点	Incident Lake 対応機能	機能説明
① ガバナンスと責任分界	判断履歴の記録 ・経営報告支援	重大時の判断者や責任分担が曖昧になりがちな場面でも、Incident Lakeに対応記録・判断履歴を残すことで、誰が何を判断したのかを後から確認し、経営への報告につなげやすくなる。
② 資産・重要業務・依存関係の特定	Real-time RAG （関連情報の集約）	普段は、どの業務がどのシステム・委託先・クラウドに支えられているか散らばって見えづらい。 Incident Lakeに対応履歴や関連情報が蓄積されることで、過去にどこで何が止まり、どの業務に影響したのかが参照しやすくなる。
③ 攻撃面最小化	改善タスク ・類似事象の参照	Incident Lakeは、脆弱性スキャンや権限管理を直接代替するものではないが、インシデント後の原因・対応・再発防止策を記録し、改善タスクや類似事例として参照できる。そのため、同じ事象を繰り返さない備えにつなげやすくなる。
④ 可観測性	Real-time RAG （横断検索）	インシデント対応時に、Slack、Jira、Datadog、Notionなどに散在する対応情報・手順・過去事例・判断履歴を横断的に参照できる。これにより、担当者ごとの経験に頼らず、今何が起きているかを組織で把握しやすくなる。
⑤ 証跡性・監査可能性	証跡保全 ・Auto-Reporting	対応記録・判断履歴・証跡をIncident Lake上に整理して残すことで、監査・顧客・当局に対して、いつ誰が何を判断し、どのように対応したのかを説明しやすくなる。ポストモーテムや社内外向け報告書の作成も支援できる。
⑥ 対応基盤の可用性	独立した代替記録 ・連絡基盤	障害時には、対応情報や連絡内容がチャット・チケット・個人メモに分散し、後から状況を追いにくくなる。Incident Lakeは既存ツール上の対応情報を集約・構造化し、対応中・対応後に参照しやすい記録基盤として機能する。
⑦ 復旧可能性	Decision Support （復旧判断支援）	復旧手順や過去の対応履歴がIncident Lakeに蓄積されることで、類似事例や確認すべき観点を参照しながら復旧判断を進めやすくなる。復旧作業そのものを自動化するのではなく、判断に必要な情報を揃え、復旧の遅れを防ぎやすくする。
⑧ 判断理由の記録性と継続改善	Auto-Reporting ・Data Moat	インシデント対応の中で発生した判断理由・対応履歴・暗黙知を蓄積し、ポストモーテムや改善点の整理に活用できる。対応を一度きりの反省で終わらせず、類似事例の参照や改善タスク管理を通じて、組織学習につなげやすくなる。

※ 本マトリクスは Incident Lake がどのような支援を成し得るか概念的に示したもので、実際の導入や適用には各社の状況により異なるため個別の確認が必要。

Incident Lakeで行うアセスメント

Incident Lake のアセスメント機能を使えば、NIST CSF・ISO/IEC 27001:2022・SOC 2 のコントロールに沿い、自社のセキュリティ体制を客観的に自己評価できる。それにより、現在地の可視化と、改善すべきポイントの特定がしやすくなる。

実際のツールUI



画面で確認できること

① 総合スコア・グレード：セキュリティ体制の総合評価を可視化
② 評価カテゴリ／スコア：11の領域で自社の強み・弱みを見極め
③ カテゴリ別設問：各カテゴリの実態把握のための設問
④ 設問に紐づく規格コントロール：世界基準の規格との紐づきを解説
⑤ 回答スコア：プルダウンでスコア入力。バージョン保存で再評価・進捗を確認

CHAPTER 10

社内で議論すべき5つの問い

社内で議論すべき5つの問い

自社の現在地を把握し、経営層・情報システム部門・リスク管理部門が同じ物差しで議論を始めることが、レジリエンス強化の第一歩である。読んで終わりにせず、次の経営会議・社内会議で、そのまま議題にできる5つの問いを示す。

01 8観点において、自社は Level 1〜5 のどこにあるか

02 8観点内の弱い領域において、事業継続リスクに最も影響を与えるのはどれか

03 第5章で取り上げた重大インシデントのうち、自社に最も近いのはどれか

04 第6章で取り上げた先進企業のうち、自社が近づきたいレジリエンスの水準はどれか

05 最初に改善する観点について、責任者・予算・期限を誰が、いつ決めるか

重要なのは、経営層・現場・リスク管理が同じ物差し（8観点×5段階）で自社の現在地を語り、
最もリスクの高い観点から最初の一歩を決めることである。レジリエンスは、特定の誰かの頑張りではなく、
組織として備える仕組みによって高まる。その議論を、今日から始めていただきたい。

Appendix

Appendix A：規制・認定制度の概要

制度・枠組み	法令・ガイドライン・評価制度	主に求められること	日本企業への示唆
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。経営者向けの指針。	経営者が認識すべき3原則と、経営者がCISO等に指示すべき重要10項目。体制・予算・人材・インシデント対応・復旧・改善を含む。	情シス任せではなく、経営判断・予算・人材・復旧・改善のテーマとして扱う必要がある。
総務省	電気通信事業法令に基づく電気通信事故報告制度および、事業用電気通信設備の安全・信頼性確保に関する制度。	法令上の報告対象となる重大な事故等の把握・報告、復旧、再発防止。サイバー攻撃に起因する通信障害も、報告基準に達すれば対象となり得る。	電気通信事業者等では、障害時の把握・報告・復旧手順と記録性が必要。
経済産業省・国家サイバー統括室／IPA	経済産業省・国家サイバー統括室が制度構築方針を公表し、IPAが運営する「サプライチェーン強化に向けたセキュリティ対策評価制度」。	★3・★4は、2026年度末頃の制度開始（申請受付開始）を目指す。発注者が受注者に必要な★を提示し、対策実施と実施状況を確認する任意制度。	取引先から求められる対策水準や★3・★4の評価取得の文脈で、自社および委託先の対策状況を説明できる状態を整えることが重要となる。
会社法・民法	取締役の善管注意義務および内部統制に関する法的枠組み。	企業規模・業態・保有するリスクに応じた合理的な備えと、復旧・説明・改善を行える体制の有無が、善管注意義務・内部統制の観点から問題となり得る。	サイバー対策が不十分であることを直ちに「違法」と断定するのではなく、合理的な備え、判断過程、証跡、改善状況を説明できる体制の有無として整理するのが安全。
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。金融機関等向け。2024/10/4適用、2025/7一部改正。	ガバナンス、特定、防御、検知、対応・復旧、サードパーティリスク管理。	委託先を含むサードパーティリスクを管理し、対応・復旧を説明できる体制が求められる。委託先も、取引を通じ情報提供や体制整備が求められ得る。
EU DORA	EUの金融事業体を主な直接対象とする規則。ICT第三者サービス提供者との契約・管理を含み、重要ICT第三者サービス提供者は監督枠組みの対象。	ICTリスク管理、重大インシデント報告、レジリエンステスト、ICTサードパーティリスク管理。	EU金融機関のICT委託先となる場合、契約を通じて復旧・報告・監査協力・再委託管理等を求められ得る。
NIST CSF 2.0	法的義務ではない任意フレーム。2024/2公表。重要インフラに限らず全組織が参照可能。	Governを加えた6機能（統治・特定・防御・検知・対応・復旧）でリスク管理を整理。	自社診断、取引先説明、経営報告の共通言語として活用しやすい。特にガバナンスと復旧能力を説明する際の参照枠組みになる。
米国 SEC サイバー開示規則	SECへの定期報告義務を負う国内登録企業および外国私募発行体に対するサイバーセキュリティ開示規則。2023年採択。	国内登録企業は、重大と判断したサイバーインシデントを、原則として重要性判断後4営業日以内にForm 8-K Item 1.05で開示。	SEC報告対象の日本企業には、重要性判断、影響範囲把握、経営報告、開示判断を迅速に行う記録・判断プロセスが必要となる。

※ 各制度は直接適用範囲が異なるため、「直接対象」と「日本企業への示唆」を分けて整理。NIST CSF 2.0は任意フレームワーク、DORAはEUの金融事業体を主な直接対象とする規則、SEC規則はSECへの定期報告義務を負う国内登録企業および外国私募発行体を対象とする開示規則。主な出典：経済産業省、IPA、総務省、金融庁、EUR-Lex、NIST、SEC（2026年6月確認）

Appendix B-1：主要フレームワーク共通要素を診断用に8項目に整理

本マトリクスの8観点は、NIST CSF 2.0、DORA、金融庁・経済産業省ガイドライン、ISO 22301、FCA Operational Resilience等で共通して重視される要素を、企業が自社診断しやすい粒度に再整理したものである。特定規制の公式評価基準ではなく、レジリエンス態勢の現在地を把握するための本WP独自の整理である。

8つの観点	主に参照する考え方	本WPでの落とし込み
① ガバナンスと責任分界	NIST CSF 2.0「GOVERN」／経産省ガイドライン／金融庁ガバナンス／DORAの経営体責任	重大時の判断者、経営報告ライン、部門横断の責任分担
② 資産・重要業務・依存関係の特定	NIST「IDENTIFY」／金融庁「特定・サードパーティ管理」／DORA／FCA mapping	重要業務と、それを支えるシステム・委託先・クラウド・認証基盤の関係把握
③ 攻撃面最小化	NIST「PROTECT」／金融庁「防御」／CIS Controls／経産省ガイドライン	外部公開資産、特権ID、脆弱性、設定不備の棚卸しと優先対応
④ 可観測性	NIST「DETECT」／金融庁「検知」／CIS Controlsの監査ログ管理・ネットワーク監視	ログ、アラート、対応記録を集約し、影響範囲や類似事例を追跡
⑤ 証跡性・監査可能性	NIST「GOVERN／Oversight」／金融庁モニタリング／DORAの監査・検査権／ISO 22301	対応記録を、監査・リスク管理・当局・顧客に説明できる証跡として保持
⑥ 対応基盤の可用性	NIST「RESPOND／RECOVER」／金融庁「対応・復旧」／ISO 22301／FCA Impact Tolerances	本番障害時にも、連絡・記録・状況把握・意思決定の手段を維持
⑦ 復旧可能性	NIST「RECOVER」／ISO 22301／DORAの復旧・バックアップ／FCAシナリオテスト	RTO/RPO、復旧優先順位、手動継続手順を定義し、訓練・検証
⑧ 判断理由の記録性と継続改善	NISTのImprovement／経産省ガイドラインのPDCA／ポストモーテム／SEC開示における説明責任	判断理由、再発防止策、未解決リスクを記録し、経営報告・改善に接続

※ 本表は公的・国際フレームワークの概念対応を示したものであり、条文単位の厳密なマッピングではない。

Appendix B-2：属人対応から継続改善へ進む5段階の成熟度モデル

本マトリクスの5レベルは、CMMIに代表される成熟度モデルの発想を参考に、レジリエンス態勢を「場当たり的・属人的な対応」から「部門管理」「組織管理」「持続的改善」へ進む段階として整理したものである。CMMIの公式評価を行うものではなく、各社が自社の現在地を把握するための独自モデルである。

本WPでの名称	本WPでの状態	成熟度モデル上の考え方
Lv.01 無管理	手順・責任者・記録が定まらず、場当たり的に対応している	反応的で、結果が予測しにくい状態
Lv.02 個人依存	特定人材の経験・勘・暗黙知により、個別には対応できている	実行はされるが、再現性・標準化が弱い状態
Lv.03 部門管理	部門内では手順や記録が整っているが、組織横断・経営報告には弱い	プロセスは定義され始めるが、組織全体ではばらつきが残る状態
Lv.04 組織管理	経営層を含む責任分担、報告ライン、訓練、証跡が整備されている	組織的に管理され、測定・統制される状態
Lv.05 持続的管理	記録・分析・再発防止・訓練結果が改善サイクルに接続されている	学習と改善により、対応能力が継続的に更新される状態

※ Levelは企業全体の格付けではなく、8観点ごとの状態を把握するための目安。観点ごとにばらつきが出る前提で、Level 2〜3からLevel 4〜5へ近づくための改善論点を特定する。
※ CMMI等の成熟度モデルの発想を参考にした独自整理であり、CMMIの公式評価・認定を意味しない。

Appendix C：国内大手のインシデント事例詳細

事例（観点）	観点別の根拠（公開情報からの整理）	主な出典
アサヒグループHD	① ガバナンス：再発防止策として独立セキュリティ組織・専任役員・取締役会監督強化を掲げる。 ③ 攻撃面：拠点のネットワーク機器を経由して侵入され、パスワードの脆弱性から管理者権限を奪取された。攻撃面・認証の管理に課題があった可能性。 ④ 可観測性：障害の約10日前からの潜伏・偵察を検知できなかった。 ⑥ 対応基盤の可用性：データセンター完全隔離・約300拠点遮断で全業務システムが使えず、受注・出荷を手作業で対応。 ⑦ 復旧可能性：受注・出荷停止 約2カ月、物流正常化まで約5カ月。	アサヒグループHD「調査完了内容と再発防止策」（2026/2/18）／同社リリース（2025/10/3・10/14・11/27）／同社企業情報
KADOKAWA	② 依存関係：オンプレの仮想化基盤に多数のサービスを集約し、基盤の侵害がグループ横断の同時停止に波及。 ③ 攻撃面：従業員アカウント情報がフィッシングで窃取されたことが侵入の起点。 ④ 可観測性：複数サーバーへアクセスできない障害として顕在化し、調査で大規模攻撃と確認。 ⑥ 対応基盤の可用性：ニコニコ等グループ主要サービスがほぼ全停止。 ⑦ 復旧可能性：主要サービス再開まで約2カ月。	KADOKAWA「2025年3月期 決算短信」「決算リリース」「情報漏えいに関するお知らせ」（特損24.13億・通期▲83/▲47億・漏えい254,241人分）※侵入手口の詳細は報道・OSINTより取得
みずほ銀行／みずほFG	本件は外部攻撃ではなく自社のシステム障害。 ① ガバナンス：金融庁が「経営管理（ガバナンス）態勢の整備」を命令、特別調査委が真因を組織力・IT統制・顧客目線・企業風土の4課題と総括。 ③攻撃面は対象外。 ④ 可観測性／予兆管理：過去のATM取り込みトラブル（2018年1,821件・2019年187件）を経営報告せず。 ⑥ 対応基盤の可用性：ATM等が広範に停止。8/20は冗長系への自動切替が動作せず。 ⑦ 復旧可能性：8/20の二重障害で復旧が長時間化。正常化まで約3年。 ⑧ 記録性・継続改善：2002年・2011年の障害に通底する真因が指摘され、継続改善が十分に回っていなかった可能性。	金融庁・財務省「行政処分について」（2021/11/26）／システム障害特別調査委員会「調査報告書（公表版）」（2021/6/15）／みずほFG 2021年3月期 決算短信
KDDI	本件は外部攻撃ではなくメンテナンス作業を起点とする通信障害。 ① ガバナンス／作業統制：根本原因は作業手順書の不備（ルーティング変更手順が指示されず）＝変更管理・事前検証の統制に課題があった可能性。 ② 依存関係（社会インフラ）：緊急通報・物流・交通・金融・IoT・MVNO等への波及。 ④ 可観測性：VoLTE交換機・加入者DBの輻輳・データ不一致の連鎖を早期に抑えられず、影響が長時間化。 ⑥ 対応基盤の可用性：全国規模・合計61時間25分の通信サービス停止。 ⑦ 復旧可能性：過剰信号送出の原因となったVoLTE交換機（18台中6台）の特定・切り離しまで時間を要した。	総務省「電気通信事故検証報告書」（2022年10月）／KDDI 障害報告資料・リリース（2022/7/29）／KDDI 2023年3月期 決算短信（補償・業績影響）
アスクル	① ガバナンス：侵入口が委託先（第三者）アカウント＝委託先リスク管理の責任分界に課題があった可能性。 ② 依存関係：自社（ASKUL LOGIST）が無印良品・ロフト等の物流を受託する3PLの結節点であり、自社停止が委託元のEC・医療/介護の供給まで波及。 ③ 攻撃面：委託先向け管理者アカウントにMFA未適用で、認証情報漏えいが侵入に直結（公式第13報）。 ④ 可観測性：公式第13報が「侵入検知の遅れ（EDR未導入・24時間監視なし）」を課題として明記。 ⑥ 対応基盤の可用性：高度に自動化された基幹物流システムの停止で出荷が全面停止。 ⑦ 復旧可能性：バックアップデータも暗号化・削除され、本格復旧フェーズ移行まで約2カ月。	アスクル「影響調査結果…ご報告（第13報）」（2025/12/12）ほか第1〜10報／良品計画「顧客情報流出について」（2025/11/14）