中小企業向け

サイバーセキュリティ実践ハンドブック

中小企業も安心！セキュリティ対策で DX を加速

第 10 編　　サイバーレジリエンス能力の育成

東京都産業労働局

第26章. サイバーレジリエンスの必要性

章の目的
第 26 章では、中小企業におけるサイバーレジリエンスの必要性とその定義を理解し、ISO/IEC 27001/27002 や NIST CSF 2.0 との関係を把握することで、自組織の情報セキュリティ戦略や IT-BCP と統合したレジリエンスを段階的に構築するための基礎を身につけることを目的とします。

主な達成目標

- サイバーレジリエンスの概念と、防御だけでなく回復・適応を重視する戦略的必要性を理解すること
- ISO/IEC 27001/27002 および ISMS の PDCA との関連を踏まえ、可用性維持と継続的改善がレジリエンスの基盤であることを説明できること
- NIST CSF 2.0 の 6 機能、とくに Respond／Recover の重要性を理解し、中小企業向けの段階的導入方法を整理できること
- サイバーレジリエンスライフサイクル（準備・防御・検知・対応・復旧・改善）を体系的に把握し、自社の取り組みへ適用できること

26-1. サイバーレジリエンスの定義と情報セキュリティ戦略上の位置づけ

26-1-1. サイバーレジリエンスの基本定義と戦略価値

関連項目
0-1-1、6-3、

サイバーレジリエンス（CR: Cyber Resilience）は、組織のミッションや目標達成を阻害するサイバー攻撃、システム障害、または自然災害といった多様な事態に直面しても、その影響を最小限に食い止め、迅速に回復し、事業を継続する能力を指す概念です。従来のサイバーセキュリティ対策が「侵入を水際で防ぐ」（防御）に重点を置いていたのに対し、サイバーレジリエンスは、防御が完全ではないという現実を前提とし、「侵害を許容しつつ、いかに迅速に立ち直り、事業を継続できるか」（回復と適応）に戦略の重点を置きます。

今日の攻撃は巧妙化しており、あらゆる予防策を講じても、セキュリティ侵害を完全に防ぐことは不可能であるという認識が広まっています。この「防御の限界」という前提のもと、企業の存続能力、すなわち可用性と信頼性の確保は、事態発生後の生存能力を高める戦略的なアプローチが必須となります。サイバーレジリエンス能力の向上は、攻撃によって業務が停止した場合の大きな経済的損失を回避し、企業の経営リスクを許容可能なレベルに抑えるための必須戦略となります。特に中小企業においては、セキュリティ対策のリソースが限られていることが多く、一度の攻撃で事業継続が困難になることも考えられるため、サイバーレジリエンスの確保はビジネスの存続にとって極めて重要な要素です。

26-1-2. ISO/IEC 27001/27002 におけるサイバーレジリエンスの基礎

関連項目
13-2-7、13-2-8、15-2-5、15-2-6

サイバーレジリエンスの概念は、情報セキュリティマネジメントシステム（ISMS）の国際規格である ISO/IEC 27001 の要求事項と密接に関連しています。ISMS が目指す情報セキュリティの 3 要素である機密性、完全性、可用性のうち、サイバーレジリエンスは特に、情報を必要なときに使える状態を保つ 可用性（Availability）の維持に直接的に深く関連しています。

ISMS は、情報セキュリティの継続的改善を PDCA（計画、実行、点検、改善）サイクルを通じて行うことを求めており、この「改善」（Act フェーズ）の要求が、サイバーレジリエンスの核となる組織の適応能力の基盤を提供します。インシデント発生後、ISMS の「パフォーマンス評価」を通じて、活動が情報セキュリティ目標の達成に繋がっているかを確認し、課題を改善することに焦

点を当てます。これにより、過去のインシデント対応から得られた教訓を体系的に組み込み、組織全体のサイバーレジリエンス能力を持続的に強化することが可能となります。

また、ISO/IEC 27002 に基づき策定される管理策の多くは、サイバーレジリエンス能力の中核をなします。ハンドブックにおいて組織的対策として示されている「情報セキュリティインシデント対応」や「事業継続計画策定」（BCP）といった項目は、可用性をサイバー脅威から守るための組織的な準備体制の具体的な実装例であり、サイバーレジリエンスの基礎を成す要素となります。

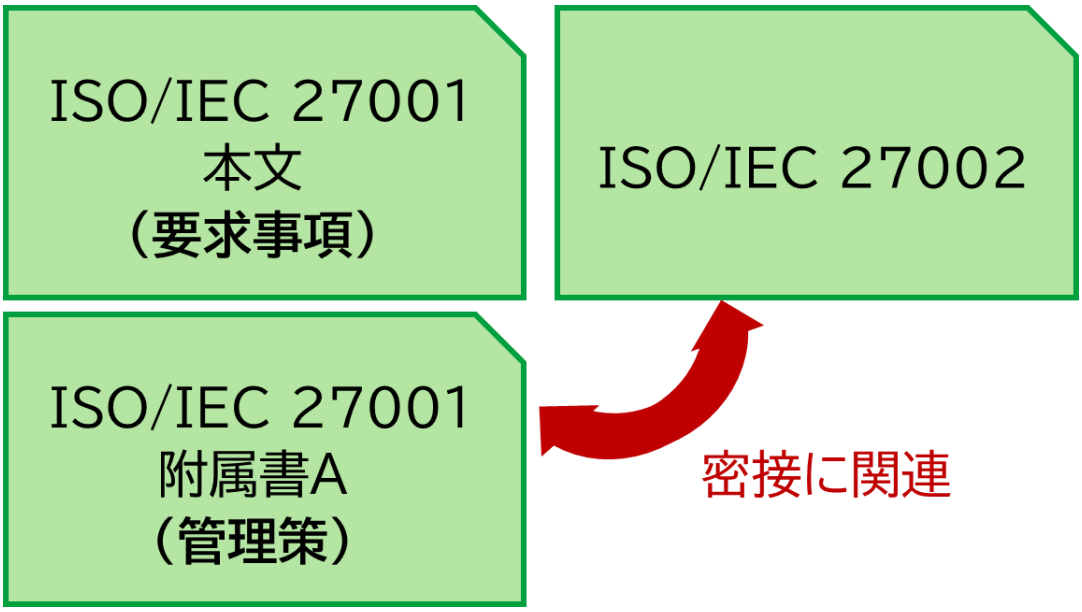

図 1. ISO／IEC 27001 と ISO/IEC 27002 の関係図

東京都　「【詳細解説】AI 活用とセキュリティガバナンスのための統合規格マネジメント：ISO/IEC 27001, 27002 & 42001 詳細分析レポート」をもとに作成

ISO/IEC 27002 に基づくサイバーレジリエンスの実践策

サイバーレジリエンスを効果的に構築するためには、ISO/IEC 27002 の管理策を計画的に導入し、組織の実情に合わせて段階的に実践することが必要です。

事前準備

管理策 5.9 情報及びその他の関連資産の目録

管理策 5.12 情報分類

- 自社が保有する情報資産を網羅的に把握する。
- 各資産の重要度と責任者を明確に定義する。
- サイバー攻撃や障害発生時に優先的に保護・復旧すべき資産を判断できる体制を確立する。

管理策 8.8 技術的ぜい弱性の管理

- ソフトウェアの更新管理を定期的に行い、パッチ適用状況を可視化する。
- 一定期間未対応の端末が存在する場合には、管理者へ通知が行われる体制を整える。

管理策 8.13 情報のバックアップ

- 重要な業務データを異なる環境へ定期的にバックアップする。
- 年 1 回以上の復元試験を行い、実際に復旧できることを確認する。

対応

管理策 5.24 情報セキュリティインシデント管理の計画策定及び準備

管理策 5.26 情報セキュリティインシデントへの対応

- インシデント発生時に備え、対応手順を明文化する。
- 報告経路・判断基準・対応責任者を明確にする。
- 初動カードや報告テンプレートを全従業員に共有する。

管理策 8.15 ログ取得

- システムやネットワーク機器の操作記録を一定期間（90 日以上）保存する。
- 改ざん防止のためアクセス制御を実施する。
- クラウドサービス利用時はログ保存機能を確認し、自社要件を満たすように設定する。

管理策 5.6 専門組織との連絡

- IPA、JPCERT/CC、警察など外部機関と連絡できる体制を確立する。
- 定期的な訓練で連絡手順を検証する。

回復

管理策 5.29 事業の中断・阻害時の情報セキュリティ

管理策 5.30 事業継続のための情報セキュリティ

- 被害を最小限に抑え、早期業務再開するための復旧方針を確立する。
- IT 担当者は、業務継続計画(BCP)と統合された復旧手順書を作成する。
- 重要システムごとに復旧時間目標（RTO)と復旧時点目標（RPO)を明確にする。

管理策 8.14 情報処理施設・設備の冗長性

- クラウド環境や外部バックアップを活用して冗長化を確保する。
- 復旧時には感染ファイルや不正変更の有無を確認し、安全確保後に再稼働する。
- 通信障害や停電などの非常事態に備え、代替通信手段や手作業による暫定業務プロセスを準備しておく。

学習と改善

管理策 5.27 情報セキュリティインシデントからの学習

- インシデント対応記録を残し、原因分析と改善策を文書化する。
- 得られた教訓を訓練や手順書更新に反映させ、対応力を継続的に強化する。

管理策 6.3 情報セキュリティの意識向上、教育及び訓練

- 全社員を対象とした教育を計画的に実施する。
- 年 1 回以上の演習で初動対応・連絡体制・復旧判断を確認し、実践的な対応力を維持する。
- 中小企業では E ラーニングや簡易シミュレーションを活用することでコストを抑えながら効果的な教育が可能です。

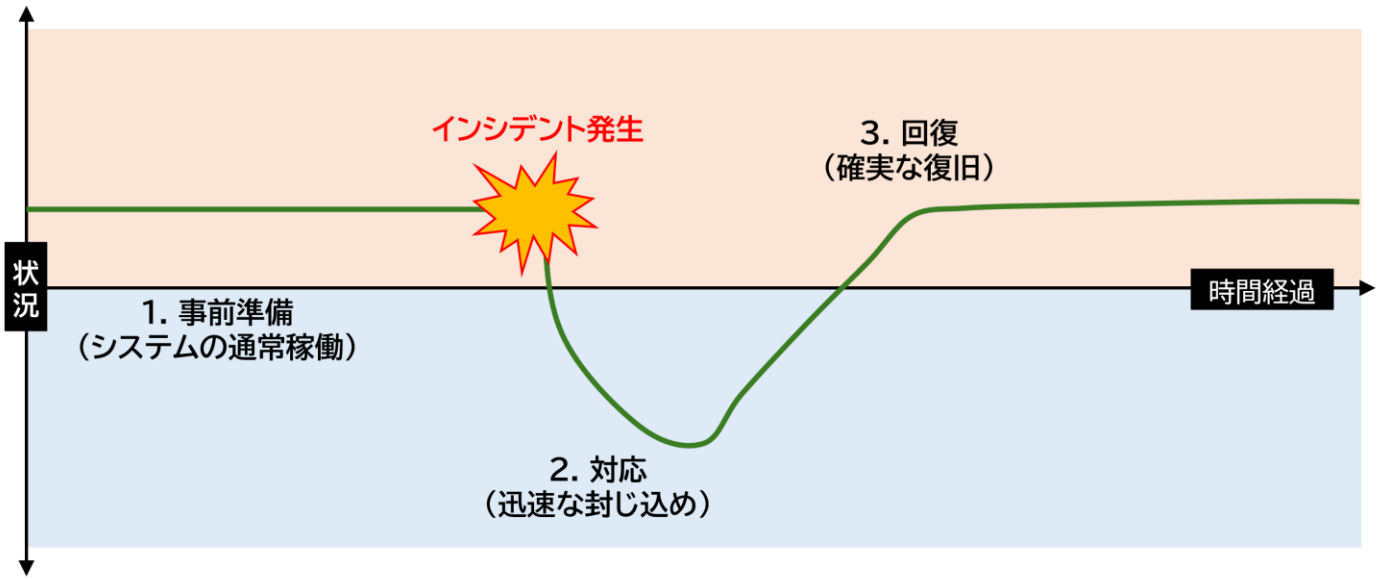

図 2. サイバーレジリエンスを実施していくために必要な 3 要素

（出典）IPA 「サイバーレジリエンスのためのコミュニケーション ～セキュリティ担当者に必要なコミュニケーションスキル集～ 」をもとに作成

詳細理解のため参考となる文献（参考文献）	
経済産業省「サイバーセキュリティ経営ガイドライン Ver.3.0」	https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf
IPA「中小企業の情報セキュリティ対策ガイドライン（第 3.1 版）」	https://www.ipa.go.jp/security/guide/sme/about.html
総務省「テレワークセキュリティガイドライン（第 5 版）	https://www.soumu.go.jp/main_content/000752925.pdf
IPA サイバーレジリエンスのためのコミュニケーション ～セキュリティ担当者に必要なコミュニケーションスキル集～	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/f55m8k00000070u7-att/f55m8k000000710q.pdf

26-2. ISO/IEC 27002:2022 に基づく情報セキュリティインシデント管理策

関連項目
5-2-3、5-2-4、13-2-7、15-2-5、15-2-6、18-2-11、18-2-12

ハンドブックの「情報セキュリティインシデント対応」の記述は、組織的対策に該当します。これは、サイバーレジリエンスの Respond/Recover 機能の基準として活用可能です。この管理策では、インシデント発生を検知した場合に備え、対応手順の整備を求めており、また、疑わしい事象の分析、証拠の収集・保全、および関係者への報告と対応を規定しています。インシデント対応完了後、教訓の収集と反映を通じて、再発防止策を検討し、組織全体の改善（RC.IM）に反映することが求められます。

インシデント対応の具体的な実行には、バックアップや冗長化といった技術的対策が必須となります。これらの技術的要素は、Recover 機能の基盤を形成します。インシデント対応体制の有効性は、対応・復旧の所要時間（RTO/RPO）や、インシデント対応訓練の実施頻度と結果によって測定されるべきであり、これは ISMS のパフォーマンス評価の重要な指標となります。

なお、インシデント対応を効果的に実施するためには、経営層による統制とリスク判断が不可欠です。情報セキュリティマネジメントシステム（JIS Q 27001）に基づき、組織はインシデントの経験を通じて学習し、対応手順や教育内容を継続的に改善する必要があります。これにより、サイバーレジリエンスの「予測・適応」機能が組織に定着します。

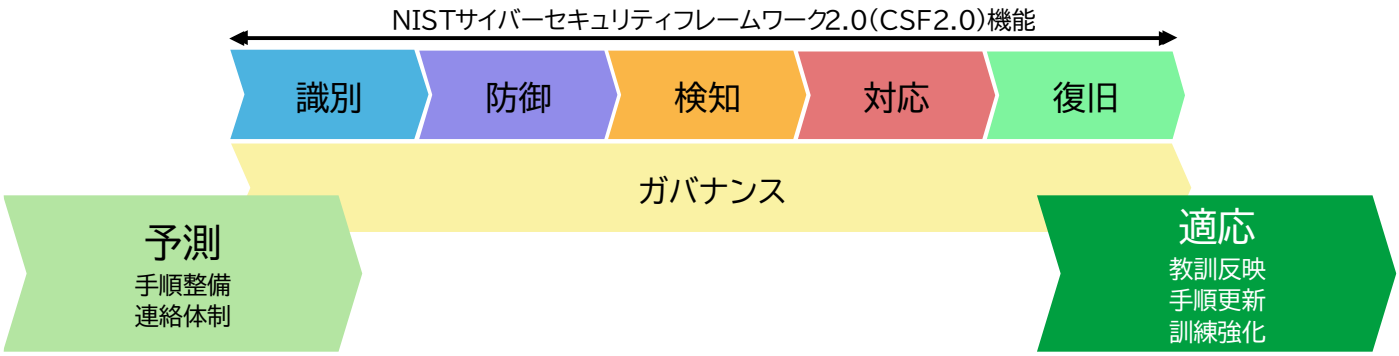

図 3. 情報セキュリティインシデント対応イメージ

IPA 「The NIST Cybersecurity Framework (CSF) 2.0（2024 年 2 月）」 の翻訳版をもとに作成

詳細理解のため参考となる文献（参考文献）	
NIST Cybersecurity Framework（CSF）2.0（2024）	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf
経済産業省「サイバーセキュリティ経営ガイドライン Ver.3.0」	https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf
総務省「テレワークセキュリティガイドライン（第 5 版）	https://www.soumu.go.jp/main_content/000752925.pdf

26-3. サイバーレジリエンス戦略としての NIST CSF 2.0 フレームワーク

関連項目
6-3-2、11-3、11-3- 1

NIST サイバーセキュリティフレームワーク（CSF）2.0 は、あらゆる組織がサイバーセキュリティリスクを管理するための指針であり、サイバーレジリエンス戦略に不可欠な体系を提供します。CSF 2.0 は、Govern, Identify, Protect, Detect, Respond, Recover の 6 つの機能で構成されます。

サイバーレジリエンス能力の核となるのは、インシデント発生後の迅速な行動と回復を支援する Respond（RS）と Recover（RC）機能です。RS 機能は、インシデントの封じ込めと分析に焦点を当て、被害の拡大防止を担います。RC 機能は、事業の復旧とサービス復元に焦点を当てます。

特に CSF 2.0 で新設された ガバナンス（Govern, GV） 機能は、サイバーレジリエンスが IT 部門の業務に留まらず、組織のミッションやリスク管理戦略に統合されるためのトップダウンの指示を確実にします。サイバーレジリエンス戦略が IT 部門任せではなく、経営層の責任であることを明確に位置づけ、組織全体のリスク管理体制に組み込むことを求めています。

中小企業における NIST CSF 2.0 活用の実践指針

NIST CSF 2.0 を中小企業が効果的に導入するためには、限られたリソースの中で、段階的な導入と重点領域の明確化が重要です。すべての機能を同時に整備するのではなく、自社の状況に応じて優先度を設定することが現実的です。

CSF2.0 Tier	段階	NIST CSF 2.0 における主な機能	主な取組内容	目標
Tier 1～2	初期段階	Identify(ID)／Protect(PR)	情報資産の把握、アクセス権限の整理、バックアップの確保、クラウドやリモートアクセス環境の安全設定、端末管理と多要素認証の導入	最小限の防御体制の確立
Tier 3	発展段階	Detect(DE)／Respond(RS)	ログ監視やアラート体制の構築、インシデント報告と対応手順の明文化、	迅速な対応体制の整備

			定期的な訓練と連絡網の整備、遠隔環境を含む監視強化	
Tier 4	成熟段階	Govern(GV)／Recover(RC)	経営層の定期レビュー、復旧計画と外部連携の統合、復旧訓練の定期化と教訓の反映、KPI に基づく継続改善の仕組みづくり	全社的レジリエンスの定着

中小企業では、特に Identify（資産とリスクの把握） と Protect（予防的管理策） を基盤に整備し、段階的に Respond／Recover へ拡張していくことで、過度な負担なく現実的な体制を構築できます。

Govern 機能は、経営層の関与を制度化することにより、レジリエンスを「組織文化」として根付かせるものです。IT 担当者は、以下のような手順で経営との連携を強化します。

- リスク評価結果やインシデント報告を、月次または四半期単位で経営層に報告する。
- 経営層は「リスク許容度」「優先順位」「投資方針」を決定し、IT 部門がそれを実装計画に反映する。
- CSF 機能を経営方針（Govern）に組み込み、ISMS または内部統制の一部として管理する。

サイバーレジリエンスの有効性を確認するために、以下のようなシンプルな指標を設定します。

- 訓練実施頻度：年 2 回以上のインシデント対応訓練を実施。
- 復旧時間（MTTR）：主要システムの平均復旧時間を前年より短縮。
- 改善策実施率：年度内に計画した改善項目の 80%以上を実施。

これらの評価は、NIST CSF の成熟度（Implementation Tiers）に対応し、継続的改善（Continuous Improvement）の成果を定量的に把握するための基礎となります。

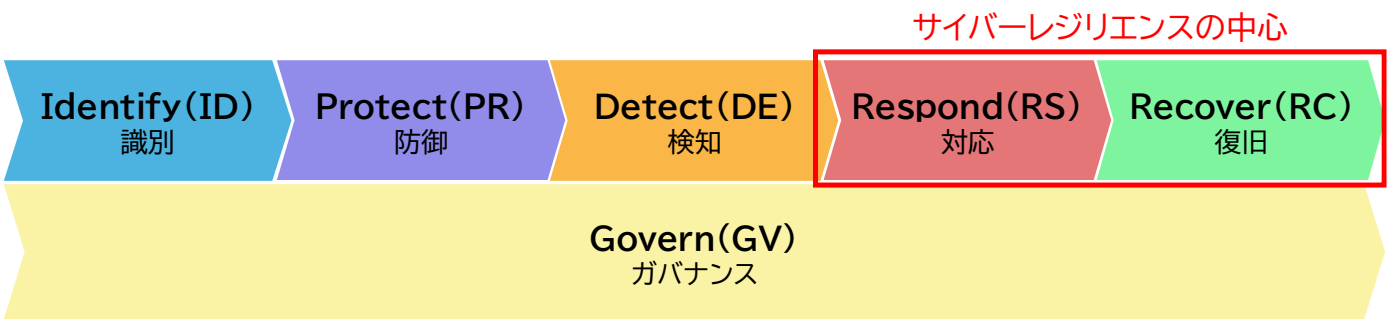

図 4. NIST　CSF2.0 におけるサイバーレジリエンスの中心

IPA 「The NIST Cybersecurity Framework (CSF) 2.0（2024 年 2 月）」の翻訳版をもとに作成

詳細理解のため参考となる文献（参考文献）	
NIST Cybersecurity Framework（CSF）2.0（2024 年版）	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf
経済産業省「サイバーセキュリティ経営ガイドライン Ver.3.0」	https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf
IPA「中小企業の情報セキュリティ対策ガイドライン（第 3.1 版）」	https://www.ipa.go.jp/security/guide/sme/about.html
JISC「JIS Q 27000：情報セキュリティマネジメントシステム－用語」	https://kikakurui.com/q/Q27000-2019-01.html

26-4. サイバーレジリエンス能力の育成に向けた体系項立て

関連項目
11-1-1

サイバーレジリエンスは、防御から復旧、そして改善に至る包括的なライフサイクルとして捉えることが重要です。この体系的なアプローチを採用することで、組織はセキュリティ対策の抜け漏れを防ぎ、特にリソースに制約のある中小企業においても、効率的にサイバーレジリエンス能力を育成することが可能となります。このライフサイクルは、CSF 2.0 の 6 機能をベースに、ハンドブックの既出の記述内容を統合することで体系的に整理されます。

サイバーレジリエンスを構成する主要フレームワークの機能比較と統合

サイバーレジリエンスライフサイクル	NIST CSF 2.0 機能	主たる目的（サイバーレジリエンス視点）	ハンドブック関連章節項
準備・計画	Govern (GV) / Identify (ID)	経営戦略との整合性確保、リスクと資産の特定	6-3. 経営投資としてのセキュリティ対策、12-2. リスクアセスメント
防御	Protect (PR)	脅威に対する予防的コントロールの実装	18 章. 技術的対策 16 章. 人的対策
検知	Detect (DE)	異常およびインシデントの早期発見	2-1. EDR の動作 18-2-14. 監視
対応	**Respond (RS)**	**被害の封じ込め、根絶、コミュニケーション**	**15-2-5. 情報セキュリティインシデント対応、5-2-3. 事案発生→課題の抽出…**
復旧	**Recover (RC)**	**事業の迅速な回復、サービスの復元**	**15-2-6. 事業継続計画策定、18-2-11. バックアップ**
改善・適応	Govern (GV) / Recover (RC)	教訓の反映、体制の強化、継続的改善	5-2-4. インシデントから得た気づきと取組、13-2-8. ISMS:10.改善

このように、NIST CSF 2.0 の 6 機能を中核とした体系的なライフサイクルを採用することで、組織は「防御」「検知」「対応」「復旧」「改善」を一連の流れとして継続的に回すことが可能になります。特に中小企業では、個別のセキュリティ施策を点として導入するのではなく、経営戦略と整合した統合的なサイバーレジリエンス体制の確立が鍵となります。

NIST CSF2.0 に基づく段階的育成モデル例

CSF2.0 Tier	段階	段階的特徴	主な取組内容	目的
Tier 1	Partial（部分的対応）	対策が断片的で、明文化された方針が存在しない。	最低限の防御・復旧体制を整備（バックアップ、EDR 導入、緊急連絡網整備）	重大被害の回避
Tier 2	Risk-Informed（リスク認識段階）	リスクを理解し、方針と責任が限定的に共有されている。	重要システムのリスク評価を実施し、インシデント通報経路を整備	継続的対策の開始
Tier 3	Repeatable（再現的運用段階）	手順やルールが組織として整備され、訓練とレビューが定期化されている。	年 2 回以上の訓練実施、ログ監視の標準化、定期的な復旧テスト	継続的運用の確立
Tier 4	Adaptive（適応的高度段階）	経営層が主導し、学習と改善を通じて動的にレジリエンスを維持している。	改善活動を組織文化に定着させ、経営層が KPI に基づき意思決定	自律的なレジリエンス経営

詳細理解のため参考となる文献（参考文献）	
NIST Cybersecurity Framework (CSF) 2.0（2024 年版）	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf
経済産業省「サイバーセキュリティ経営ガイドライン Ver.3.0」	https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf
IPA「中小企業の情報セキュリティ対策ガイドライン（第 3.1 版）」	https://www.ipa.go.jp/security/guide/sme/about.html
デジタル庁「デジタル・ガバメント推進標準ガイドライン（2025 年 5 月）」	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d4e68a9b/20250619_resources_standard_guidelines_guideline_01.pdf

第27章. サイバー攻撃を含む様々な事態に対する総合的な対応計画

章の目的
第 27 章では、インシデント対応計画（IRP）と IT-BCP を統合し、ISO/IEC 27002 および NIST CSF 2.0 を基盤とした、予防から対応・復旧・改善まで一体となった総合的な対応計画とサイバーレジリエンス・ライフサイクルの構築方法を学ぶことを目的とします。

主な達成目標
◘ IRP と IT-BCP を連携させた総合的対応計画の枠組みを理解すること
◘ NIST CSF 2.0 の Respond／Recover 機能に基づく対応・復旧基準を把握すること
◘ RTO・RPO 設定やバックアップ等による事業復旧プロセスを設計できること
◘ RC.CO による復旧時のコミュニケーションと信頼維持の要点を理解すること

27-1. サイバーレジリエンスのライフサイクルと対応計画の策定

関連項目
15-2-5、15-2-6、

総合的な対応計画の策定にあたっては、インシデント対応計画（IRP）と IT システムに特化した継続計画（IT-BCP）を、リソース効率化の観点から一体として扱うことが重要です。サイバーレジリエンスは、この IRP と IT-BCP を連携させ、予防（Protect）から回復（Recover）までを包含する PDCA サイクルとして能力を高めていきます。

計画策定の基軸となるのは、ISO/IEC 27002 の管理策、特に組織的対策と、NIST CSF 2.0 の Respond (RS) および Recover (RC) 機能が提供する体系的な基準です。

サイバーレジリエンス・ライフサイクルモデル（中小企業向け）例		
フェーズ	**NIST CSF 機能対応と主な目的**	**実施の要点（主な目的を含む）**
Plan（計画）	Govern／Identify リスク認識と事前準備	経営層と IT 担当者が共同でリスクアセスメントを実施し、重要業務・資産・システムを特定する、IRP と IT-BCP を一体化し、RTO（復旧時間目標）と RPO（復旧時点目標）を設定する
Do（実施・運用）	Protect／Respond 迅速な対応体制の構築	インシデント発生時に初動対応を確実に実行するため、手順書と連絡網を整備する、被害の封じ込め、影響分析、証拠保全を含む対応プロトコルを確立し、クラウド・リモート環境にも適用する
Check（評価・検証）	Recover 事業継続と復旧計画の実行	定期的なバックアップと冗長化を確保し、復旧手順に従ってサービスを再開する、関係者への報告や外部連携（取引先、顧客、IPA、NCO など）を実施し、復旧後の確認テストを行う
Act（改善）	Govern／Recover 教訓の反映と継続的改善	対応後の評価会議を実施し、再発防止策を策定する、ISMS の「パフォーマンス評価」と連携し、ポリシーや手順書の更新、従業員訓練の見直しを定期的に実施する

サイバーレジリエンスを確立するためには、経営層の関与、計画の統合、そして改善の継続という 3 つの要素が重要です。

まず、経営層の関与と責任を明確にすることが必要です。サイバーレジリエンスは技術的課題にとどまらず、経営リスクとして捉えるべきものです。経営層がリスクを判断し、方針と体制を主導することで、NIST CSF の「Govern」機能に対応した経営レベルのセキュリティ統合が実現します。

次に、計画と対応を一体化することが効果的です。インシデント対応計画（IRP）と IT システムに特化した継続計画（IT-BCP）を統合し、「総合的対応計画」として策定します。これにより、限られた人員でも効率的かつ迅速に対応でき、緊急時の判断や行動の一貫性が確保されます。

最後に、改善の継続が欠かせません。対応や復旧の結果を定期的に評価し、教訓を手順書や訓練に反映します。PDCA サイクルを継続して運用することで、サイバーレジリエンスは一時的な対策ではなく、組織文化として定着します。

このように、経営層による判断、計画と対応の統合、継続的な改善という 3 つの要素を通じて、組織は新たな脅威や環境変化に柔軟に対応し、持続的な事業継続力を高めることができます。

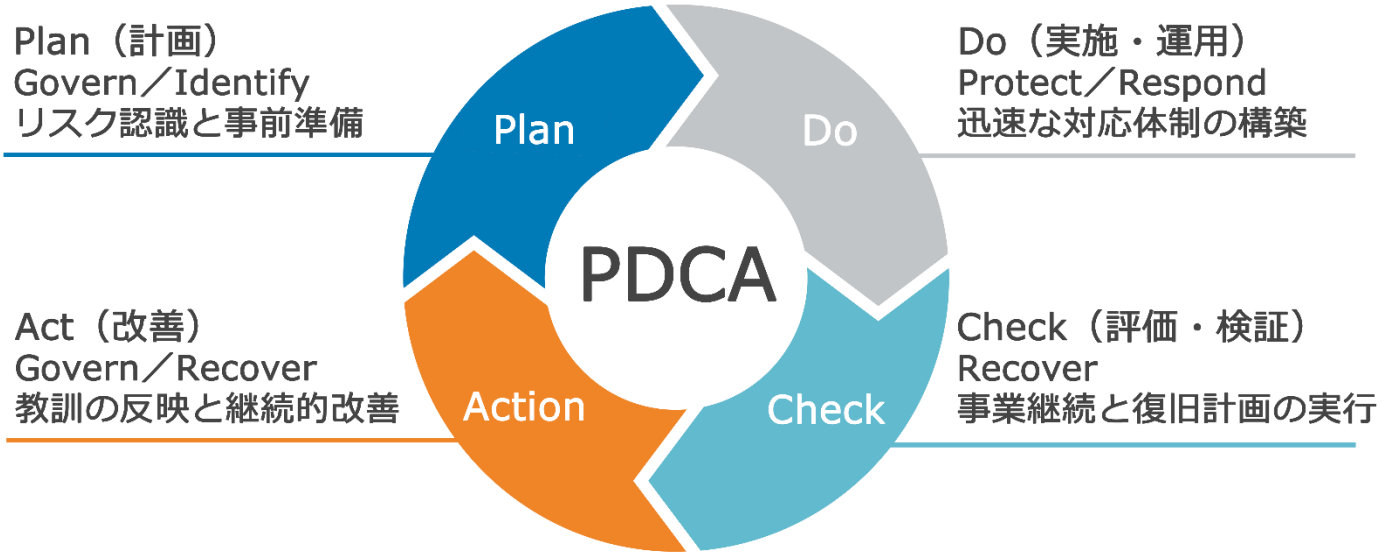

図 5. サイバーレジリエンスにおける PDCA サイクル

詳細理解のため参考となる文献（参考文献）	
NIST Cybersecurity Framework（CSF）2.0（2024 年版）	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf
IPA「中小企業の情報セキュリティ対策ガイドライン（第 3.1 版）」	https://www.ipa.go.jp/security/guide/sme/about.html

27-2. NIST CSF 2.0 Respond (RS) 機能に基づく対応基準

Respond (RS) 機能は、検知されたサイバーセキュリティインシデントに対して行動を起こし、その影響を封じ込める能力を支援します。

27-2-1. インシデント管理体制の確立（RS.IM）

関連項目
5-2-3、15-2-5、

インシデント発生時の混乱を最小限に抑え、組織的な対応を可能にするために、初動対応のプロトコルと役割分担を明確に定義しなければなりません。ハンドブックの「情報セキュリティインシデント対応」は、この体制を組織的に構築するための基準です。

検知後の対応フローは、ハンドブックの「事案発生→課題の抽出→再発防止策の実施までの流れ」に基づき具体化されます。初動対応では、検知後、速やかに情報セキュリティ責任者へ報告し、被害の拡大を防ぐための措置（封じ込め）を迅速に行う必要があります。

図６．検知後の対応フロー

中小企業が RS.IM を効果的に実施するためには、役割分担・外部連携・訓練・改善の 4 点を重点として体制を整備することが重要です。

- 経営層、IT 担当者、現場担当者それぞれの役割を明文化する。
- 報告と判断の流れを文書化する。
- 外部支援先（IPA、JPCERT/CC、セキュリティベンダ等）との連携を平時から整備する。
- 年 1 回程度の訓練（机上演習）を実施し手順の有効性を検証、改善に反映する。
- 事後レビューを行い、得られた知見を手順や教育に反映し継続的な改善を図る。

これらの取組を継続することで、RS.IM は単なる対応手順の整備にとどまらず、組織の危機対応力を高める実践的な仕組みとなります。

詳細理解のため参考となる文献（参考文献）	
NIST Cybersecurity Framework (CSF) 2.0（2024 年版）	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf
IPA「中小企業の情報セキュリティ対策ガイドライン（第 3.1 版）」	https://www.ipa.go.jp/security/guide/sme/about.html
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」	https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf
JPCERT/CC「インシデント対応依頼フォーム」	https://www.jpcert.or.jp/form/

27-2-2. インシデントの分析と軽減策（RS.AN, RS.MI）

関連項目
5-2-3、5-3-3、18-2-13、

インシデント対応の初期段階で最も重要となるのは、原因究明と影響範囲の特定、そして攻撃者が残した痕跡（証拠）の保全です。この分析能力（RS.AN）を担保するためには、システムにおけるログ（記録）の存在が不可欠となります。技術的対策における「ロギング」は、分析能力を支える前提要件であり、事後分析（フォレンジック調査）の成功に不可欠な証拠を保護するために、ログの長期保存と保護を確実に行う必要があります。

軽減策（Mitigation, RS.MI）の実行は、被害の拡大を防ぐために決定的な役割を果たします。ランサムウェア攻撃などに対する軽減策として示された、VPN 接続への多要素認証（MFA）実装や、重要なサーバへの接続をジャンプサーバ経由に制限するといった技術的対策は、攻撃者の侵入経路や横展開を断ち切る上で、サイバーレジリエンス能力に直結する重要な基準となります。

中小企業が RS.AN および RS.MI を実践的に運用するためには、「記録」「封じ込め」「改善」の 3 段階を明確に整備することが重要です。RS.AN と RS.MI は単なる事後対応の手順ではなく、組織全体のサイバーレジリエンス強化プロセスとして機能します。

詳細理解のため参考となる文献（参考文献）	
NIST Cybersecurity Framework（CSF）2.0（2024 年版）	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf
IPA「中小企業の情報セキュリティ対策ガイドライン（第 3.1 版）」	https://www.ipa.go.jp/security/guide/sme/about.html
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」	https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf
JPCERT/CC「インシデント対応依頼フォーム」	https://www.jpcert.or.jp/form/

27-3. NIST CSF 2.0 Recover (RC) 機能に基づく復旧基準

Recover (RC) 機能は、インシデントの影響を受けた資産と業務を復旧させ、通常運用に迅速に回復する能力を支援します。この RC 機能の確立が、サイバーレジリエンス戦略の成功を決定づけます。

27-3-1. 復旧計画の実行（RC.RP）と事業復旧目標（RTO/RPO）の設定

関連項目
6-3-2、18-2-11、18-2-12、18-3-1

RC.RP（復旧計画の実行）の基準として、復旧の迅速性を測る指標である RTO（目標復旧時間）と RPO（目標復旧時点）を事業継続計画（BCP）の一環として明確に設定しなければなりません。これらの指標は、経営層がビジネス要件とリスク許容度に基づいて決定する戦略的判断となります。

復旧計画の物理的・技術的な基盤は、確実なバックアップと冗長化の確保です。特にバックアップは、ランサムウェア対策として不可欠であり、復旧の成否を決定づけます。また、CSF 2.0 では、システムを最初からインシデントに耐え、迅速に復旧できるよう設計する技術インフラのレジリエンスの重要性が強調されています。これは、企画・設計段階からセキュリティを考慮する Security by Design の考え方を復旧プロセスに統合することを意味します。

中小企業が RC.RP（復旧計画）を効果的に運用するためには、「目標設定」「優先順位付け」「バックアップ」「検証」の 4 つの視点で計画を整理することが重要です。

目標設定（RTO/RPO）

各業務システムについて、停止しても許容できる時間（RTO）と、失っても許容できるデータの範囲（RPO）を明確にします。これらの数値は、業務影響度分析（BIA）の結果をもとに設定し、経営層が承認します。

優先順位付けと復旧責任

全システムを同時に復旧することは困難であるため、重要度に応じて復旧順序を定めます。また、各システムの復旧責任者を指定し、代替手段（クラウド利用、紙記録運用等）をあらかじめ定義しておくことが望ましいです。

バックアップと冗長化の実施

バックアップは「3-2-1 ルール」（3 世代・2 媒体・1 つをオフライン保管）を基本とし、定期的にリストアテスト（復旧試験）を実施します。クラウド環境を利用する場合は、事業者側のバックアップ保持期間と復旧支援範囲を確認し、契約書に明記することが必要です。

検証と改善

復旧手順やシステム切替手順の有効性を年 1 回以上検証し、演習結果を反映して計画を更新します。この活動を ISMS の PDCA サイクルに組み込み、継続的に IT-BCP の改善を行うことで、復旧能力の成熟度を高めます。

このように、RC.RP の運用は単なるバックアップ体制の整備にとどまらず、経営判断と技術的手段を統合したサイバーレジリエンス戦略の中核を成します。中小企業においても、実現可能な範囲から RTO・RPO を文書化し、手順の実効性を検証する取り組みが求められます。

詳細理解のため参考となる文献（参考文献）	
NIST Cybersecurity Framework（CSF）2.0（2024 年版）	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf
経済産業省「サイバーセキュリティ経営ガイドライン Ver.3.0」	https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf
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」	https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf
IPA「情報セキュリティ 10 大脅威 2025」	https://www.ipa.go.jp/security/10threats/

27-3-2. 復旧のためのコミュニケーション（RC.CO）

関連項目
0-1-1、5-2-3

復旧プロセスにおいては、内部（従業員、経営層）と外部（顧客、規制当局、警察/IPA/NCO）のステークホルダーとの間で情報を調整し、透明性をもって伝達するための明確なプロトコルが必要です。RC.CO（復旧のためのコミュニケーション）は、インシデント発生時の公表手順を確立し、適切なタイミングと内容での情報開示を支援することで、企業の信頼の維持に貢献します。インシデント発生時には、被害状況、初動対応、復旧の進捗状況を関係者全員に適切なタイミングと内容で通知することが求められます。

NIST CSF 2.0 対応・復旧機能に基づく対応計画の基準

CSF2.0 機能	カテゴリー (RC/RS)	機能の目的（サイバーレジリエンス能力）	対応基準（ハンドブック対応）	参照基準
Respond (RS)	インシデント管理 (RS.IM)	封じ込め、インシデントの管理と追跡	初動対応の実施、ネットワーク遮断措置	15-2-5. 情報セキュリティインシデント対応 5-2-3. 事案発生→課題の抽出...
	インシデント分析 (RS.AN)	原因究明と影響範囲の特定、証拠保全	証拠保全手順の確立、フォレンジック対応	5-2-3. 事案発生→課題の抽出...
	インシデント軽減 (RS.MI)	被害拡大防止と根絶策の実行	特権 ID 管理、多要素認証、ジャンプサーバ利用	5-3-3. 具体的な対応策
Recover (RC)	復旧計画の実行 (RC.RP)	事業継続計画に基づくサービスの復元	RTO/RPO の策定、定期的なバックアップと冗長化	15-2-6. 事業継続計画策定 18-2-11. バックアップ

	復旧のためのコミュニケーション (RC.CO)	復旧状況の調整と外部ステークホルダーへの説明責任	関係者への適切な通知と公表手順の確立	5-2-3. 事案発生→課題の抽出...
	改善 (RC.IM)	復旧計画とプロセスへの教訓の反映	事後評価に基づく再発防止策の実施、ポリシー改訂	5-2-4. インシデントから得た気づきと取組 13-2-8. ISMS:10.改善

RC.CO（復旧のためのコミュニケーション）は、復旧活動時の信頼維持と情報調整を目的とする機能であり、中小企業においては、特に「責任体制の明確化」「外部調整」「訓練と改善」の 3 つの要素を中心に整備することが有効です。

責任体制と連絡経路の明確化

重大なインシデントが発生した際には、技術対応、広報、顧客対応の責任者を事前に定め、それぞれの代行体制と緊急連絡先を「インシデント対応連絡リスト」にまとめておくことが重要です。また、通信障害や停電などに備えて、オフラインでも参照可能な紙媒体の一覧を保管しておくことが望まれます。

外部連携と情報発信

クラウドサービスや外部委託先を利用する場合は、障害発生時の連絡体制を契約書や SLA に明記し、平常時から担当窓口を共有しておきます。復旧過程での顧客・取引先への報告は、事実確認を優先し、推測情報を含まない正確な内容で実施します。

訓練と改善

復旧時の情報伝達手順について、年 1 回以上、連絡・報告・公表を想定した訓練を行い、演習記録を残して次回の手順書に反映します。この活動を通じて、関係者の役割理解と実行精度を高めることができます。

このような RC.CO の取り組みは、単なる広報対応ではなく、経営上の透明性とステークホルダー信頼の確保に直結します。中小企業では、限られた人員の中で、IT 担当者が技術対応と情報発信を兼務する場合が多いため、あらかじめ手順と責任範囲を文書化しておくことが、サイバーレジリエンス強化の鍵となります。

詳細理解のため参考となる文献（参考文献）	
NIST Cybersecurity Framework (CSF) 2.0（2024 年版）	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf
経済産業省「サイバーセキュリティ経営ガイドライン Ver.3.0」	https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf
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」	https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf
IPA「情報セキュリティ 10 大脅威 2025」	https://www.ipa.go.jp/security/10threats/

第28章. 情報システム継続計画（IT-BCP）の一環としてのインシデントに対応する体制

章の目的
第 28 章では、サイバーレジリエンス確保に不可欠な情報システム継続計画（IT-BCP）を独立した柱として位置づけ、その中にインシデント対応体制・復旧プロセス・教訓の反映および訓練を一体的に組み込み、中小企業でも現実的に運用可能な仕組みとして定着させることを目的とします。

主な達成目標
◘ IT-BCP と IRP を統合したインシデント対応体制の基本構造を理解すること ◘ RTO・RPO 設定や復旧優先順位に基づく復旧・回復プロセスを設計できること ◘ ランサムウェア対策を含む技術的対策と証拠保全・記録の実務要点を把握できること ◘ 教訓の反映と継続的改善サイクルを運用し、訓練・演習及び外部支援を活用しながら IT-BCP を日常業務に定着させる方法を理解すること

28-1. 情報システム継続計画（IT-BCP）の基本要素と体制

関連項目
5-2-3、13-2-3、15-2-6、

サイバーレジリエンスの確保は、IT システムとデータに特化した継続計画（IT-BCP）の能力と不可分です。IT-BCP は、サイバー攻撃を含むあらゆる事態を想定し、事業の早期再開を目指す組織的対策であり、ハンドブックにおいても組織的対策として重要項目とされています。

サイバーレジリエンス体制の構築は、経営層のリーダーシップのもとで推進されなければなりません。インシデント発生時の対応を担うセキュリティ担当者や組織（CSIRT など）の役割と責任を明確にし、インシデント発生時には事前に策定した対応方針に従い、経営者が指揮を執ることが必要となります。特にリソースに制約がある中小企業においては、IT-BCP とインシデント対応計画（IRP）を統合し、リソースを効率的に活用できる体制を構築することが推奨されます。

中小企業における IT-BCP は、限られた人員・設備でも現実的に運用できるよう、「体制の明確化」「復旧優先順位の設定」「訓練と見直し」の 3 要素を中心に設計することが重要です。

IT-BCP 体制例

区分	役割	主な任務	代行者
経営層	IT-BCP 統括責任者	方針承認 全社対応指揮	副経営者 または管理部長
IT 担当者	技術対応責任者	バックアップ 復旧対応 外部連携	外部 IT 支援企業
総務担当	連絡・記録管理	被害報告 連絡網の運用 記録保持	経営管理担当者
外部ベンダ	技術支援	復旧支援 クラウド再構築支援	代替委託先 または協力企業

復旧優先順位と目標設定例

業務システム	業務重要度	許容停止時間（RTO）	許容データ損失（RPO）	復旧責任者
会計・給与システム	高	12 時間	1 日	IT 担当者
顧客・受発注管理	高	24 時間	1 日	IT 担当者
社内文書共有	中	48 時間	3 日	外部ベンダ
広報・メール	低	72 時間	7 日	総務担当

IT-BCP の訓練および改善手順例

訓練実施にあたっては、国家サイバー統括室（NCO）の分野横断的演習報告や、日本シーサート協議会（NCA）の公開演習マニュアルなど、実務的な訓練資料を参照すると効果的です。詳細は「28-4.サイバーレジリエンス能力向上のための実践的な演習と訓練」を参照のこと。

IT-BCP は、BCP の下位概念ではなく、情報システムの継続を担保する独立した柱として位置づけられるべきです。中小企業では、経営層の指揮のもとで IT 担当者と外部専門家が連携し、実現可能な範囲から体制・復旧目標・演習計画を文書化することが、サイバーレジリエンス強化の出発点となります。

詳細理解のため参考となる文献（参考文献）	
NIST Cybersecurity Framework（CSF）2.0（2024 年版）	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf
IPA「中小企業の情報セキュリティ対策ガイドライン（第 3.1 版）」	https://www.ipa.go.jp/security/guide/sme/about.html
中小企業庁「中小企業 BCP 策定運用指針」	https://www.chusho.meti.go.jp/bcp/
国家サイバー統括室（NCO）「2023 年度 分野横断的演習 実施報告」	https://www.cyber.go.jp/pdf/policy/infra/NISC_enshu_20240327.pdf
日本シーサート協議会「サイバー攻撃演習訓練実施マニュアル」	https://www.nca.gr.jp/activity/pub_doc/drill_manual.html
CSIRT スタータキット	https://www.nca.gr.jp/activity/pub_doc/csirtstarterkit.html
CSITR スタータキット ver3.0	https://www.nca.gr.jp/activity/pub_doc/imgs_u/CSIRTstarterkit_v3.pdf

28-2. インシデント対応体制の確立と初動対応の具体的手順

28-2-1. 初動対応のフェーズと実践（Respond 機能の実装）

関連項目
2-1、5-2-3、5-3-3、18-2-11、18-2-12、18-2-13

インシデント発生時の初動対応は、被害の拡大を防ぎ、迅速な復旧を可能にするために極めて重要です。ハンドブックの「事案発生→課題の抽出→再発防止策の実施までの流れ」に基づき、以下の初動対応が実行されます。

また、中小企業では、専任のセキュリティ担当者がいない場合や、外部委託に依存する体制が一般的です。そのため、Respond 機能（RS）を効果的に運用するには、以下の 3 フェーズごとに簡潔で実践的な行動指針を明確化することが必要です。

図 7. 初動対応の 3 フェーズ

①検知と報告

EDR やログ監視を通じてインシデントを検知した後、直ちに情報セキュリティ責任者に報告し、対応体制を立ち上げます。

中小企業における実践指針

検知の手段

EDR・アンチウイルス警告・ログ監視・従業員からの通報などを活用し、異常を確認した場合には速やかに報告体制に従い連絡を行う。

報告の流れ

検知者は「インシデント報告書（簡易様式）」に以下の項目を記載し、IT 管理責任者・経営層・外部 IT 支援事業者へ通知する。

- 検知日時
- 対象システム・端末
- 事象内容（例：不正メール開封、ファイル暗号化など）
- 現在の対応状況
- 連絡者氏名

外部機関への通報

被害が重大または広範な場合は、IPA「情報セキュリティ安心相談窓口」や JPCERT/CC への報告を検討する。個人情報漏えいの可能性がある場合は、法令に基づく所轄官庁への届出も必要である。

②封じ込め（Containment）

被害の拡大を防ぐため、ネットワークの遮断やシステムの停止などの適切な措置を講じます。この際、事後分析のための証拠保全が必須であり、システムの記録（ログ）を消去しないよう注意を払わなければなりません。

中小企業における実践指針

封じ込めの目的

攻撃の拡大を防ぎ、他システムへの感染を遮断する。
過剰な停止は業務影響を拡大させるため、影響範囲の特定と段階的対応が重要である。

実施手順

- 感染・不正アクセスを受けた機器をネットワークから切り離す
  （LAN ケーブル抜線、Wi-Fi 無効化など）
- サーバやクラウド環境では、対象インスタンスの隔離・停止を実施する
- ログ・証拠（システムイベント・アクセス履歴）を削除せずに保全する
- ディスクイメージやログファイルを安全な外部媒体にバックアップする

外部支援要請

封じ込め作業を自社で完結できない場合は、契約しているシステムベンダーやクラウドサービス事業者、ISP などに速やかに支援を依頼する。これらの連絡先は「緊急連絡リスト」に登録し、IT-BCP 文書の付録として管理しておく。

③根絶（Eradication）

攻撃の根本原因を特定し、悪意のあるプログラムや不正アクセス経路を完全に排除します。この作業が復旧後の再発を防ぐための鍵となります。

中小企業における実践指針

根絶の目的

攻撃の原因（マルウェア、不正設定、脆弱性など）を排除し、再発を防止することである

主な作業

- 感染ファイルや不正スクリプトの削除、レジストリ修正、アクセス権再設定を実施

- セキュリティパッチ適用やアカウント再発行を行い、再侵入経路を遮断
- システム復旧前に全端末のスキャンと監視を行い、再感染がないことを確認

対応記録と報告

各作業の実施時間・担当者・結果を記録し、「インシデント対応記録」として保存します。記録内容は後続の RC（Recover）フェーズでの復旧計画や再発防止策策定（RC.IM）に活用します。

根絶フェーズ完了後は、事業継続観点でレビューを実施し、IT-BCP および IRP に反映します。対応ログを基に初動判断・連絡経路・封じ込め手順の有効性を分析し、年次更新を行うことが推奨されます。

詳細理解のため参考となる文献（参考文献）	
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」	https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf
IPA「中小企業の情報セキュリティ対策ガイドライン（第 3.1 版）」	https://www.ipa.go.jp/security/guide/sme/about.html
国家サイバー統括室（NCO）「2023 年度 分野横断的演習 実施報告」	https://www.cyber.go.jp/pdf/policy/infra/NISC_enshu_20240327.pdf

28-2-2. ランサムウェア被害からの回復を確実にする技術的対策の実装

ランサムウェア攻撃からの回復を確実にするため、ハンドブックの具体的な対応策をサイバーレジリエンス体制の必須要件として組み込むべきです。

多要素認証（MFA）の適用

VPN 接続の認証に多要素認証を実装し、接続する個人の身元を証明することは、ID/パスワード漏洩による不正侵入経路を遮断する上で最も重要な技術的対策です。

具体的な実装例

- すべてのリモート接続（VPN・クラウド管理画面など）に MFA を適用する
- スマートフォンアプリによるワンタイムパスワード方式（TOTP 方式）は管理負担が少なく推奨される
- 管理者アカウントの MFA は必須とし、代替認証手段（緊急コード）を安全に保管する

アクセス制御の強化

重要なサーバへのリモートデスクトップ接続は、ジャンプサーバからの接続のみに制限するなど、アクセス制御を強化する。これにより、攻撃者が内部に侵入した後の横展開のリスクを軽減できます。

具体的な実装例

- 外部からの接続を原則 VPN 経由に限定し、不要な RDP ポート（TCP 3389）を閉鎖する
- 共有アカウントを廃止し、権限分離（管理者／一般ユーザー）を徹底する
- 重要データフォルダは「変更権限を持つユーザー」を限定し、アクセスログを自動保存する

バックアップと冗長化

定期的なバックアップは、攻撃を受けた後のデータ復元に不可欠であり、冗長化は、システムの可用性を確保し、RTO の達成を支援します。バックアップデータの完全性の確保がサイバーレジリエンスの成否を決定づけます。

具体的な実装例

- 本番データとは物理的・論理的に分離されたバックアップ（オフラインバックアップ）を毎日または週次で取得する
- クラウドバックアップを利用する場合は「過去バージョン復元」機能を有効化し、暗号化攻撃への備えとする
- バックアップの保存先は複数（社内 NAS＋クラウド）とし、保管責任者を明確にする

ランサムウェア対策は技術を導入するだけでなく、継続的に検証し、実際に技術が機能する状態を保つことが重要です。

詳細理解のため参考となる文献（参考文献）	
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」	https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf
IPA「中小企業の情報セキュリティ対策ガイドライン（第 3.1 版）」	https://www.ipa.go.jp/security/guide/sme/about.html
国家サイバー統括室（NCO）「2023 年度 分野横断的演習 実施報告」	https://www.cyber.go.jp/pdf/policy/infra/NISC_enshu_20240327.pdf
IPA「情報セキュリティ 10 大脅威 2025」	https://www.ipa.go.jp/security/10threats/

28-3. 復旧・回復プロセスと教訓の反映（継続的改善）

28-3-1. 復旧（Recover）後の再発防止策の実施

関連項目
5-2-3、5-3-3、

インシデントの修復が確認され、計画（IT-BCP）に基づいてシステムとデータが正常な状態に戻された後、恒久的な再発防止策を立案・実施することがサイバーレジリエンス能力向上に不可欠です。この際、単なる場当たり的な修正ではなく、根本的な原因に基づいた対策を実施することが求められます。例えば、特権アカウントのパスワード定期変更や、脆弱性情報の定期確認といった運用手順を組み込みます。

再発防止策は、復旧後に発生原因を整理し、改善を日常業務へ定着させることが目的です。一時的な対応で終わらせず、継続的な改善サイクルとして運用することが求められます。

原因分析と改善策の立案

復旧後は、インシデントを技術的・組織的・人的要因に分けて分析します。

- 技術的：設定不備、脆弱性、未更新ソフト
- 組織的：連絡体制の遅延、手順の不備
- 人的：教育不足、注意喚起の欠如

それぞれに対して改善策を明確化し、IT-BCP やインシデント対応記録に反映します。

改善の実施と記録

立案した対策は、担当・期限・確認方法を明示して実施します。改善内容を「技術」「運用」「教育」「外部委託」の区分で整理し、完了後は IT 管理責任者が効果を確認して記録します。この運用を定期的に見直すことで、PDCA サイクルが継続的に機能します。

再発防止計画とレビュー

改善結果は半期または年次で点検し、未完了項目は次年度に繰り越します。必要に応じて外部専門家の助言を得て、対策の実効性を高めます。レビュー結果は経営層にも共有し、IT-BCP 更新時に反映させます。

詳細理解のため参考となる文献（参考文献）	
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」	https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf
IPA「中小企業の情報セキュリティ対策ガイドライン（第 3.1 版）」	https://www.ipa.go.jp/security/guide/sme/about.html
国家サイバー統括室（NCO）「2023 年度 分野横断的演習 実施報告」	https://www.cyber.go.jp/pdf/policy/infra/NISC_enshu_20240327.pdf

28-3-2. 教訓の反映と継続的改善（RC.IM）

関連項目
5-2-4、13-2-8

サイバーレジリエンス能力を動的に高めるためには、インシデント対応から得られた「気づきと取組」を体系化し、組織の適応能力に変換することが不可欠です。ISMS の「改善」プロセスを活用し、インシデント対応後の事後評価を必ず実施します。

NIST CSF 2.0 の RC.IM（Improvements - 改善）カテゴリーは、復旧計画とプロセスが、過去のイベントから得られた教訓を組み込んでいることを確実にするよう明確に要求しています。この体系的な改善サイクルを通じて、組織はセキュリティポリシーの改訂、システム設計の改善（Security by Design）、および訓練内容の見直しを行い、将来の脅威に対する組織全体のレジリエンスを動的に向上させます。

復旧後に得られた教訓を組織に定着させ、継続的に改善するための手順を示します。「再発防止策の実施」で抽出した改善項目を、運用・文書・教育へ反映することを目的とします。

成功点と課題の明確化及び教訓の整理

インシデント対応の終了後、初動から復旧までを振り返り、対応上の成功点と課題を明確化します。IT 管理担当者と関係部門が参加する簡易レビュー会を実施し、教訓を次の観点で整理します。

- 手順面：報告経路や判断の遅延など
- 技術面：設定不備や監視の不足
- 体制面：役割の不明確さや外部連携の不備

結果は「改善記録表」としてまとめ、再発防止計画の基礎資料とします。

改善項目の管理と反映

改善項目には担当・期限・確認方法を設定し、進捗を定期的に確認します。内容は「技術」「運用」「教育」「委託管理」などに区分して管理すると効果的です。改善結果は、IT-BCP や手順書などの関連文書へ反映し、更新時には経営層にも共有します。

継続的改善の仕組み化

改善の効果を確認し、未実施項目は次年度の改善計画に繰り越します。この PDCA 型の改善サイクルを通じて、IT-BCP を「継続的に成長する計画」として運用できます。また、共有可能な教訓は定例会や社内研修で報告し、組織全体の意識向上につなげます。

詳細理解のため参考となる文献（参考文献）	
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」	https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf
IPA「中小企業の情報セキュリティ対策ガイドライン（第 3.1 版）」	https://www.ipa.go.jp/security/guide/sme/about.html
国家サイバー統括室（NCO）「2023 年度 分野横断的演習 実施報告」	https://www.cyber.go.jp/pdf/policy/infra/NISC_enshu_20240327.pdf

28-4. サイバーレジリエンス能力向上のための実践的な演習と訓練

関連項目
5-2-3、22-3-4、24-1、24-1-1、

文書化された IT-BCP/IRP の実効性を確保するためには、定期的な訓練と演習が必須です。訓練は、計画が緊急時に機能するかを検証し、全関係者の役割の明確化と習熟度向上に寄与します。

対象別訓練の推奨

【経営層向け】

サイバーリスクを伴う経営判断や、対外的なコミュニケーションをシミュレーションする訓練が必要です。

【実務担当者向け】

実践的サイバー防御演習（CYDER、RPCI など）を活用し、インシデント封じ込めや復旧の具体的な技術手順を習得させます。

人材育成の統合

セキュリティ専門人材以外の全従業員がインシデント発生時の初期対応（報告、連絡、封じ込め支援）を適切に行えるよう、「プラス・セキュリティ」知識補充講座などを活用した継続的なスキル育成が必要です。この非専門人材の育成は、リソースが限定的な中小企業にとって、外部の専門家との連携を円滑にする「橋渡し役」の確保につながります。

IT-BCP におけるインシデント対応（IR）体制の実践ステップと教訓の反映

ステップ	実践内容の概要（サイバーレジリエンス視点）	ハンドブック内参照基準	サイバーレジリエンス能力への貢献
準備・計画（Plan）	IT-BCP/IRP 策定、RTO/RPO 設定、体制構築、演習実施	15-2-6. 事業継続計画策定 24-1. 知識補充講座カリキュラム例	事態発生時の対応能力と迅速性の確保
検知・分析（Detect/Analyze）	脅威の早期検知と影響範囲の特定、ログ保全	5-2-3. 事案発生→課題の抽出… 18-2-13. ロギング	被害拡大の防止（封じ込め）
復旧・回復（Recover）	システムの復元、サービス再開、恒久対策の	5-3-3. 具体的な対応策	タイムリーな事業の再開

	実施	18-2-11. バックアップ	
改善・教訓 (Improve)	事後評価に基づく再発防止策の実施、ポリシー改訂、訓練見直し	5-2-4. インシデントから得た気づきと取組 13-2-8. ISMS:10. 改善	組織全体のレジリエンス向上と適応性の獲得

IT-BCP の訓練・教育を定着させる実践的な手順

IT-BCP（情報システム継続計画）における訓練と教育を、日常業務に定着させるための実践的な手順を示します。

訓練・教育実施案の立案

訓練は組織の成熟度に応じ、段階的に導入します。初期は「計画理解と連携確認」を目的とした机上訓練を実施し、その後、模擬訓練や外部演習（CYDER 等）へ発展させます。

- 机上訓練（基本）：報告手順・判断ルートの確認
- 模擬訓練（応用）：シナリオに沿った実践的対応
- 外部演習（発展）：他機関との合同訓練による対応力強化

この段階的アプローチにより、無理のない訓練体制を構築できます。

訓練計画と役割分担例

訓練実施にあたっては、目的・対象・頻度を明確に設定します。

- 目的：初動対応の確認、連絡体制検証、復旧手順の確認
- 対象：経営層、IT 担当者、従業員など役割に応じて区分
- 頻度：年 1 回以上を基本とし、体制変更時に追加実施

訓練の進行・記録は IT 担当者が兼務しても構いません。小規模組織でも実施しやすい形に簡略化することが重要です。

結果の記録と改善への反映

訓練後は、評価表や実施記録を作成し、改善点を整理します。

- 連絡体制の有効性（報告遅延や情報漏れの有無）
- 判断・指示の妥当性（優先度や対応順の適切さ）
- 文書整合性（計画書との乖離）

結果は IT-BCP 文書に添付し、次回の改善サイクルに反映します。この継続的な記録が、組織のレジリエンス向上に直結します。

外部支援の活用

自組織のみでの訓練実施が困難な場合は、外部支援を積極的に利用します。

- IPA：中小企業向けサイバー演習教材、CYDER プログラム
- NCO：演習モデル・訓練シナリオの提供
- 地域：商工会・情報セキュリティ連携組織との合同訓練など

これらの支援を組み合わせることで、継続的で現実的な訓練環境を整備できます。

詳細理解のため参考となる文献（参考文献）	
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」	https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf
国家サイバー統括室（NCO）「2023 年度 分野横断的演習 実施報告」	https://www.cyber.go.jp/pdf/policy/infra/NISC_enshu_20240327.pdf
セキュリティインシデント対応机上演習教材	https://www.ipa.go.jp/security/sec-tools/ttx.html
中小企業支援セミナー（IPA 主催）	https://www.ipa.go.jp/security/seminar/sme/supportseminar.html?utm_source=chatgpt.com

編集後記

第 10 編では、サイバーレジリエンスを実務に落とし込むうえで中心的な位置づけとなる IT-BCP とインシデント対応計画（IRP）の統合、復旧プロセスの確立について紹介しました。特に、中小企業が限られたリソースの中で現実的に取り組むためには、予防から復旧までのプロセスを一貫した体系として扱うことが重要である点を改めて確認しました。本編では、この 2 つの計画を一体として整理し、実務に即した体制として構築するための視点を中心に解説しています。

さらに、Respond 機能に基づく初動対応の重要性についても取り上げました。検知・報告・封じ込め・根絶という流れは、どの組織においてもインシデント対応の共通の骨格となります。その実効性を支えるのは、日常的なログ管理や役割分担の明確化といった基本的な仕組みです。外部機関との連携、机上訓練の実施、発生時の記録の徹底など、平常時に整えるべき要素が多く存在することもお伝えしています。さらに、復旧段階では、RTO 及び RPO を事前に設定しておくことが企業活動の再開速度を大きく左右すること、バックアップの取得だけでなく、復元可能性を確認するための定期的な検証、復旧後の教訓をどのように手順書や訓練へ反映していくかについても触れ、改善のプロセスが組織の適応力そのものにつながることを解説しています。

サイバーレジリエンスの強化は、計画の文書化、連絡体制の整備、訓練の実施、バックアップ検証、教訓の反映といった、ひとつひとつの取り組みを確実に積み上げることで、組織の復旧力と継続力は大きく向上します。本編が、皆さまの組織で取り組むべき項目を見直すきっかけとなり、日常の業務からサイバーレジリエンスに取り組むきっかけとなれば幸いです。

引用文献

中小企業向けサイバーセキュリティの実践ハンドブック2024

https://www.cybersecurity.metro.tokyo.lg.jp/security/docs/Tokyo_CyberSecurity_HandBook_2024_Text.pdf

NIST Cybersecurity Framework 2.0: Resource & Overview Guide

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf

Breaking Down NIST CSF 2.0: Categories and Sub-Categories (with Real-World Examples) | by Brittney Ginther | Medium

https://medium.com/@brittneyaginther/breaking-down-nist-csf-2-0-categories-and-sub-categories-with-real-world-examples-9bc611c87eab

The NIST Cybersecurity Framework (CSF) 2.0

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

サイバーレジリエンスとは？事業継続性向上やBCPに必須な対策 - NTTドコモビジネス

https://www.ntt.com/business/lp/cyber-resilience.html

Breaking Down the NIST Cybersecurity Framework: Recover - CyberSaint

https://www.cybersaint.io/blog/nist-function-recover

NIST Cybersecurity Framework 2.0: Key changes to CSF - Acronis

https://www.acronis.com/en/blog/posts/nist-cybersecurity-framework-20-key-changes-to-csf/

参考文献

経済産業省「サイバーセキュリティ経営ガイドライン Ver.3.0」
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

IPA「中小企業の情報セキュリティ対策ガイドライン（第3.1版）」
https://www.ipa.go.jp/security/guide/sme/about.html

総務省「テレワークセキュリティガイドライン（第5版）
https://www.soumu.go.jp/main_content/000752925.pdf

NIST Cybersecurity Framework (CSF) 2.0（2024）
https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf

JISC「JIS Q 27000：情報セキュリティマネジメントシステム－用語」
https://kikakurui.com/q/Q27000-2019-01.html

デジタル庁「デジタル・ガバメント推進標準ガイドライン（2025年5月）」
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d4e68a9b/20250619_resources_standard_guidelines_guideline_01.pdf

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」
https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf

JPCERT/CC「インシデント対応依頼フォーム」
https://www.jpcert.or.jp/form/

IPA「情報セキュリティ10大脅威 2025」
https://www.ipa.go.jp/security/10threats/

中小企業庁「中小企業 BCP策定運用指針」
https://www.chusho.meti.go.jp/bcp/

国家サイバー統括室（NCO）「2023年度 分野横断的演習 実施報告」
https://www.cyber.go.jp/pdf/policy/infra/NISC_enshu_20240327.pdf

日本シーサート協議会「サイバー攻撃演習訓練実施マニュアル」
https://www.nca.gr.jp/activity/pub_doc/drill_manual.html

CSIRTスタータキット
https://www.nca.gr.jp/activity/pub_doc/csirtstarterkit.html

CSITRスタータキットver3.0
https://www.nca.gr.jp/activity/pub_doc/imgs_u/CSIRTstarterkit_v3.pdf

セキュリティインシデント対応机上演習教材
https://www.ipa.go.jp/security/sec-tools/ttx.html

中小企業支援セミナー（IPA主催）

https://www.ipa.go.jp/security/seminar/sme/supportseminar.html?utm_source=chatgpt.com

■BCP

Business Continuity Plan（事業継続計画）の略。企業が災害やテロ攻撃などの緊急事態に直面した際に、被害を最小限に抑え、企業の存続に関わる最も重要な事業を継続または早期復旧するための計画。

26-1-2

■IRP

Incident Response Plan：インシデント対応計画の略。サイバー攻撃や情報漏洩などのセキュリティインシデントが発生した際に、被害を最小限に抑え、迅速な復旧と再発防止を図るための文書化された計画。誰が・何を・どの順序で・どのように対応するかを明確に定め、組織が混乱なく行動できるようにすることを目的とする。企業や組織にとって不可欠な文書であり、事前の準備と定期的な見直しが重要とされる。

27-1

■IT-BCP

IT Business Continuity Plan の略。企業の事業継続計画（BCP）の一部として策定する、災害やサイバー攻撃、システム障害などによってITシステムが停止した場合でも、業務を継続・早期復旧できるようにするための計画。企業の重要な情報資産やシステムの保護、損失の最小化を目的とし、復旧目標（RTO/RPO）や代替手段、バックアップ、システムの冗長化、クラウド活用などの対策が含まれる。IT への依存度が高まる現代において、定期的な見直しと訓練を通じて実効性を高めることが求められる。

27-1

■MTTR

Mean Time To Recovery の略。システム障害の発生からサービスが正常に復旧するまでの平均所要時間を示す指標。復旧速度や運用体制の成熟度を測る際に用いられ、数値が低いほどシステムの信頼性や可用性が高いと評価される。

26-3

■RPO

Recovery Point Objective の略。システム障害やサイバー攻撃などのインシデント発生時に、どの時点までのデータを復旧対象とするかを定める指標。

インシデント発生前のどれだけのデータ損失を許容できるかを示し、バックアップの頻度や保管方法、データ保全の厳格さを決める基準となる。

適切な RPO の設定により、データ損失の影響を最小限に抑え、迅速な復旧と事業継続を支えるための重要な指標として、サイバーレジリエンスの領域でも重視されている。

26-1-2

■RTO

システム障害やサイバー攻撃などのインシデント発生後、業務やサービスを再開するまでに許容される最大の停止時間を定める指標。復旧に必要な時間の上限を示し、システム構成、復旧手順、代替手段の設計における重要な基準となる。 適切な RTO の設定により、業務への影響を最小限に抑え、迅速なサービス復旧と事業継続を実現する。RPO（Recovery Point Objective）と併せて、可用性やサイバーレジリエンスを評価する際の重要な指標とされる。

26-1-2

■インシデント

情報セキュリティの分野において、システム障害、サイバー攻撃、情報漏えい、不正アクセス、マルウェア感染、設定ミ

スなど、業務に影響を及ぼす、またはその恐れがある予期しない事象を指す。

これらはシステムの「機密性・完全性・可用性」に影響を与え、サービス停止や業務中断、信用失墜、経済的損失を招く可能性がある。

インシデント発生時には、迅速な検知と対応、被害の最小化、原因の特定、再発防止といった適切な対応が求められる。

26-1-2

■サイバーレジリエンス

サイバー攻撃やシステム障害が発生しても、業務の継続性を維持しながら影響を最小限に抑え、迅速に回復・適応できる能力を指す。

従来の「防御中心」のサイバーセキュリティに対し、攻撃を受けることを前提に「備える・耐える・回復する・適応する」といった一連の対応力を含む概念であり、組織の事業継続性と信頼性を高めるための重要な要素として NIST CSF2.0 でも位置づけられている。

26-1-1

■ジャンプサーバ

外部ネットワークや社内環境から、機密性の高いサーバや重要なシステムへ安全にアクセスするための中継点となる専用サーバ。別名「踏み台サーバ」とも呼ばれ、直接の接続を制限し、ジャンプサーバ経由に限定することで、アクセス経路の統制、認証強化、操作ログの一元管理が可能となる。

不正アクセスや内部不正のリスクを低減できるため、セキュリティ向上やゼロトラストの観点から、重要システムの管理運用において広く採用されている。

27-2-2

■多要素認証

多要素認証は、サービス利用時において利用者の認証を行うために、3 つの要素（①利用者だけが知っている情報②利用者の所有物③利用者の生体情報）のうち、少なくとも 2 つ以上の要素を組み合わせて認証する安全性が高い認証方法。例えば、利用者が知っている情報としてはパスワード、利用者の所有物としては、スマートフォンの電話番号を用いたメッセージ認証、利用者の生体情報としては指紋認証や顔認識などがある。また、近年では FIDO2 と呼ばれる、デバイスを使用したパスキーによる認証により、パスワードレスでの認証が広まっている。

28-2-2

■フォレンジック

犯罪捜査における分析や鑑識を意味する言葉。サイバーセキュリティの分野で使われる「フォレンジック」とは、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取組を指す。「デジタル・フォレンジック」や「コンピュータ・フォレンジック」などと呼ばれる。

27-2-2

■ログ（記録）

ログとは、コンピュータシステム、ネットワーク機器、アプリケーションなどで発生する操作履歴やイベント情報を時系列で記録したデータのこと。

ユーザー操作、アクセス履歴、認証情報、設定変更、エラーや障害などを把握でき、インシデントの原因調査や不正アクセスの検知、監査証跡として活用される。

適切なログの取得・保管・分析は、インシデントの早期発見や原因特定、再発防止に不可欠であり、サイバーセキュリティ対策の基盤となる。

27-2-2

東京都産業労働局