令和7年度
中小企業サイバーセキュリティ
実践力強化プログラム

第9回

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

講師紹介

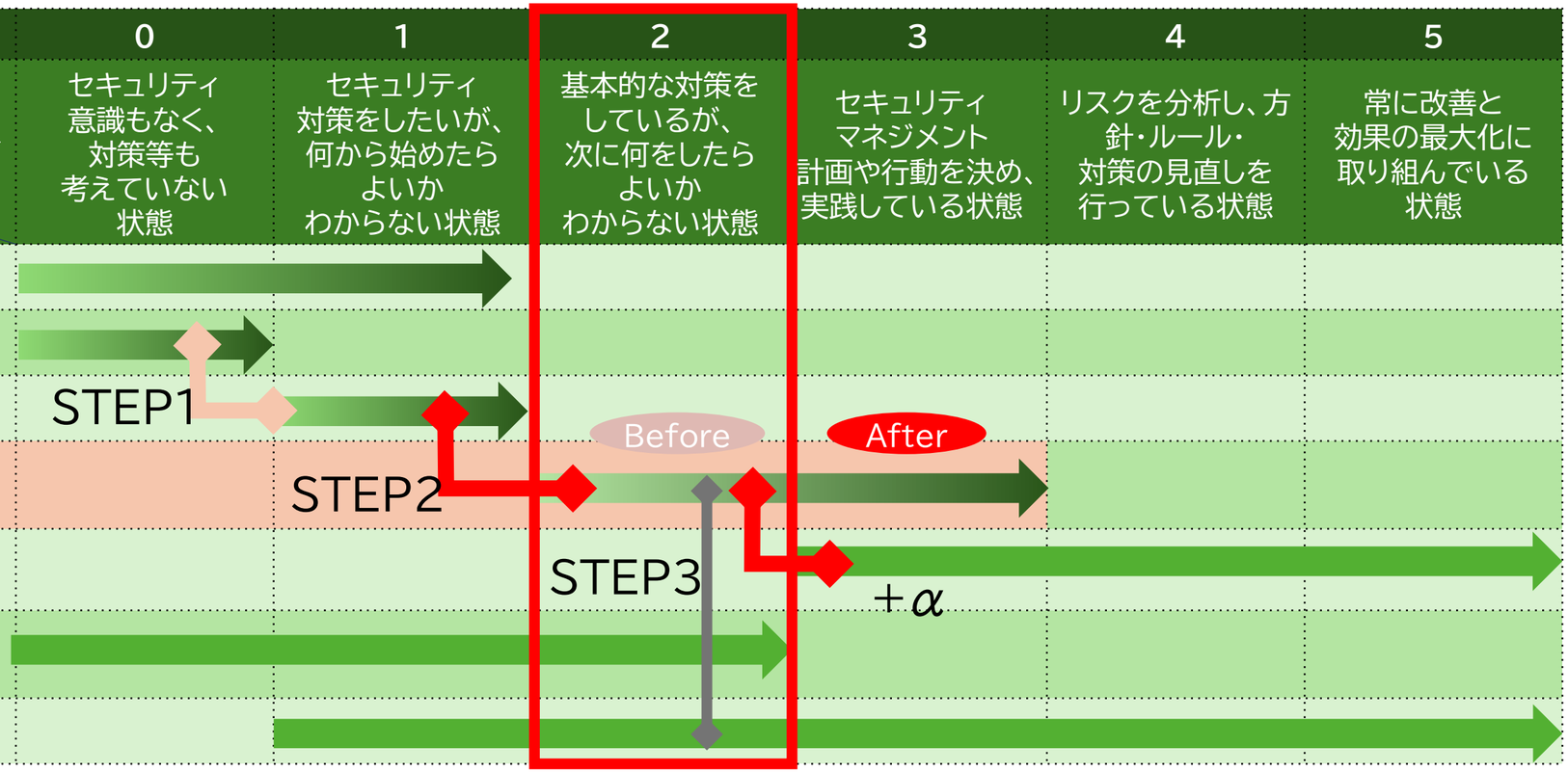
氏名	矢野　泰広（やの　よしひろ）
業務経歴	26年（セキュリティ経験：15年）
専門分野	情報セキュリティ、DX、ICT、クラウド技術、 ネットワーク技術、DB設計・構築、プロジェクト マネジメント、WEBシステム設計・構築、 サーバ設計・構築
保有資格	情報処理安全確保支援士（第004005号） 経済産業省認定 情報処理技術者試験 プロジェクトマネージャ、 情報処理技術者第一種、情報処理技術者第二種 インターネット検定 .com Master ADVANCE★★ 生成AIパスポート 家電製品アドバイザー（AV情報家電・生活家電）
コメント	中小企業を中心にDX、ネットワーク、クラウド技術および情報セキュリティに関する構築や導入支援やコンサルティングの経験が豊富。併せて長年にわたり大手通信事業者のSE（技術営業）を対象に指導を行ってきた事から、幅広い業種、業態の企業の状況を認識しており、中小企業の課題点を的確に捉え、各企業が取り組みやすい解決策を提示する対応力に定評がある。

目的

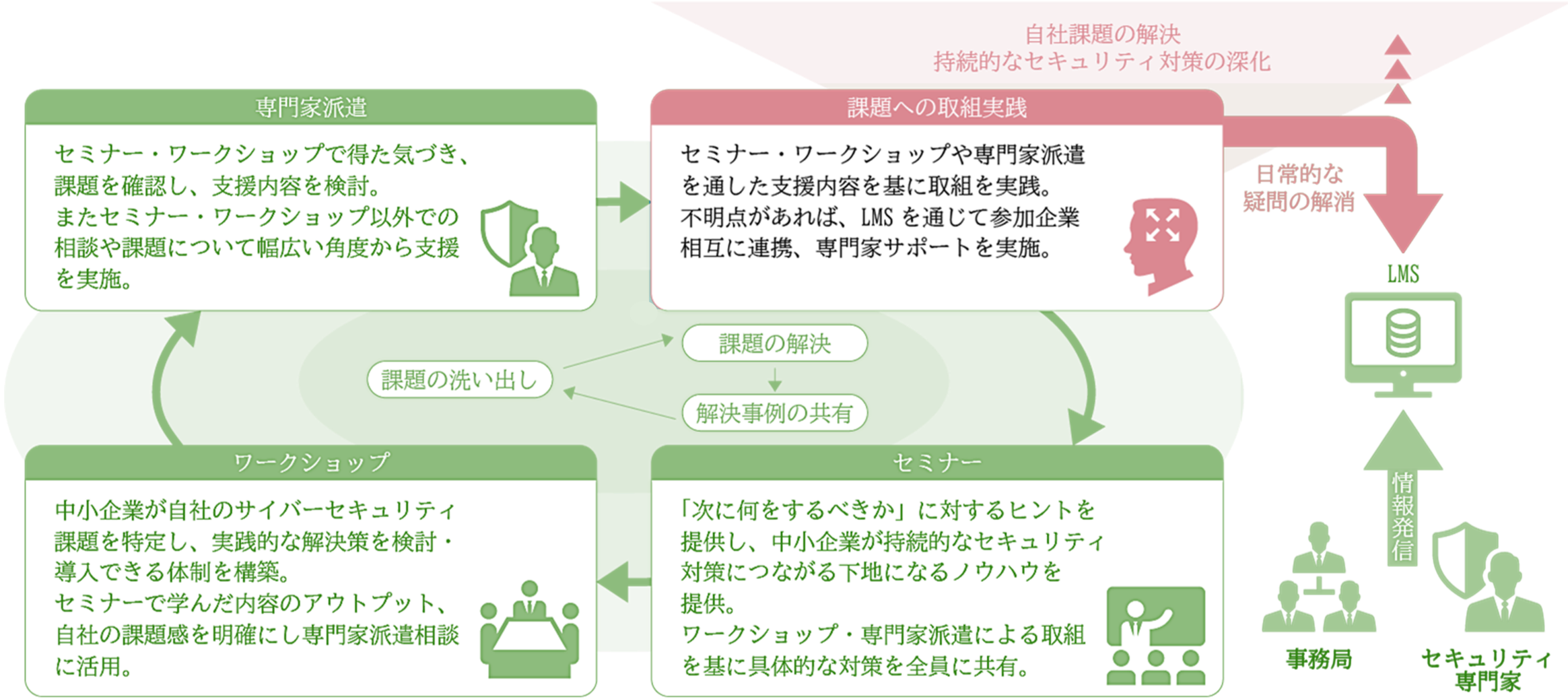
- 継続的なセキュリティ対策の実施を支援する。
- 人材の育成と実践的な課題解決を通じて、サプライチェーン全体のセキュリティ強化を図る。

東京都他事業と本事業の位置づけ

成熟度レベル　※COBITを援用し設定	0	1	2	3	4	5
ステータス / 事業と主な支援領域	セキュリティ意識もなく、対策等も考えていない状態	セキュリティ対策をしたいが、何から始めたらよいかわからない状態	基本的な対策をしているが、次に何をしたらよいかわからない状態	セキュリティマネジメント計画や行動を決め、実践している状態	リスクを分析し、方針・ルール・対策の見直しを行っている状態	常に改善と効果の最大化に取り組んでいる状態
中小企業サイバーセキュリティの極意						
中小企業サイバーセキュリティ 啓発事業						
中小企業サイバーセキュリティ 基本対策事業						
中小企業サイバーセキュリティ実践力強化プログラム（本事業）						
中小企業サイバーセキュリティインシデント対応力強化						
Tcyss（東京中小企業サイバーセキュリティ支援ネットワーク）						
サイバーセキュリティ対策促進助成金						



支援内容の全体像


自社課題の解決
持続的なセキュリティ対策の深化
専門家派遣
セミナー・ワークショップで得た気づき、課題を確認し、支援内容を検討。
またセミナー・ワークショップ以外での相談や課題について幅広い角度から支援を実施。
課題への取組実践
セミナー・ワークショップや専門家派遣を通した支援内容を基に取組を実践。
不明点があれば、LMS を通じて参加企業相互に連携、専門家サポートを実施。
日常的な
疑問の解消
LMS
課題の解決
課題の洗い出し
解決事例の共有
ワークショップ
中小企業が自社のサイバーセキュリティ課題を特定し、実践的な解決策を検討・導入できる体制を構築。
セミナーで学んだ内容のアウトプット、自社の課題感を明確にし専門家派遣相談に活用。
セミナー
「次に何をするべきか」に対するヒントを提供し、中小企業が持続的なセキュリティ対策につながる下地になるノウハウを提供。
ワークショップ・専門家派遣による取組を基に具体的な対策を全員に共有。
情報発信
事務局
セキュリティ専門家

スケジュール

支援内容	7月	8月	9月	10月	11月	12月	1月	2月	3月
セミナー・ワークショップ（全10回）	7/25（金）	8/8（金）	8/27（水）	9/11（木）	9/25（木）	10/10（金）	10/27（月）	11/17（月）	12/12（金）	1/16（金）		
専門家派遣（全4回）	1回目		2回目		3回目			4回目				
事例集								ご参加いただいた企業様への取材	事例集作成期間	公表3月下旬～		

セミナー内容

実施回	編	テーマ
第1回 7/25 （金）	第0編	はじめに
	第1編	サイバーセキュリティを取り巻く背景
	第2編	中小企業に求められるデジタル化の推進とサイバーセキュリティ対策
第2回 8/8 （金）	第3編	これからの企業経営に必要なIT活用とサイバーセキュリティ対策
	第4編	セキュリティ事象に対応して組織として対策すべき対策基準と具体的な実施
	第5編	各種ガイドラインを参考にした対策の実施

セミナー内容

実施回		編	テーマ
第3回	8/27(水)	第6編	ISMSなどのフレームワークの種類と活用法の紹介
第4回 第5回	9/11(木) 9/25(木)	第7編	ISMSの構築と対策基準の策定と実施手順
第6回 第7回	10/10(金) 10/27(月)	第8編	具体的な構築・運用の実践
第8回	11/17(月)	第9編	中小企業が組織として実践するためのスキル・知識と人材育成
第9回	12/12(金)	第10編	サイバーレジリエンス能力の育成
第10回	2026年 1/16(金)	第11編	全体総括

第26章. サイバーレジリエンスの必要性

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
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
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
サイバーレジリエンス能力の育成に向けた体系項立て

サイバーレジリエンスの必要性と情報セキュリティ戦略上の位置づけ

【参照:テキスト26-1.】P2～P5

サイバーレジリエンスの基本定義と戦略価値

- サイバーレジリエンスとは、サイバー攻撃やシステム障害及び自然災害に直面しても事業を継続し、迅速に復旧する能力を指す
- 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が重点ポイント
- 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なため、被害発生を前提とした事業継続力が必要

サイバーレジリエンスの必要性と情報セキュリティ戦略上の位置づけ

【参照:テキスト26-1.】P2～P5

サイバーレジリエンスにおける中小企業の弱点

脅威	影響	中小企業の弱点
ランサムウェア	• 暗号化による業務停止 ➢ IPA「情報セキュリティ10大脅威 2025」	• 復旧体制不足 （専門人材・予算の不足）
サプライチェーン攻撃	• 取引先・委託先への波及被害 • 信頼失墜 ➢ IPA「情報セキュリティ10大脅威 2025」	• 監視体制不足 （委託先管理の不十分さ）
情報漏えい	• 信頼失墜 • 損害賠償リスク ➢ IPA「中小企業のセキュリティ対策に関する実態調査（2024）」	• 初動対応経験不足 • 手順書整備不足 ➢ 新たな脅威の社内共有が不十分（37.9%）
自然災害 （地震・水害・火災・停電）	• 物理設備の損壊・データ破損 • 長期操業停止 • ネットワーク障害 ➢ 経済産業省「中小企業BCP策定状況（2024）」 ➢ 内閣府「業務継続計画（BCP）に関する実態調査」	• 耐災害性の低さ （バックアップの多重化不足） • 停電・浸水などの物理的対策の遅れ • 冗長化・多拠点化が難しい

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

【参照：テキスト26-1.】 P2～P5

ISO/IEC 27001・27002におけるサイバーレジリエンスの基礎

- サイバーレジリエンスの概念は ISO/IEC 27001の要求事項と密接に関連
- 情報セキュリティの3要素のうち「可用性」の維持がポイント
- ISMSのPDCAにおいて、「改善（Act）」がレジリエンス強化の基盤となる
- 可用性維持の具体的な実装例
  - 情報セキュリティインシデント対応
  - 事業継続計画（BCP）策定
- **ISO/IEC 27002の管理策**の多くは**サイバーレジリエンス能力の中核**をなす

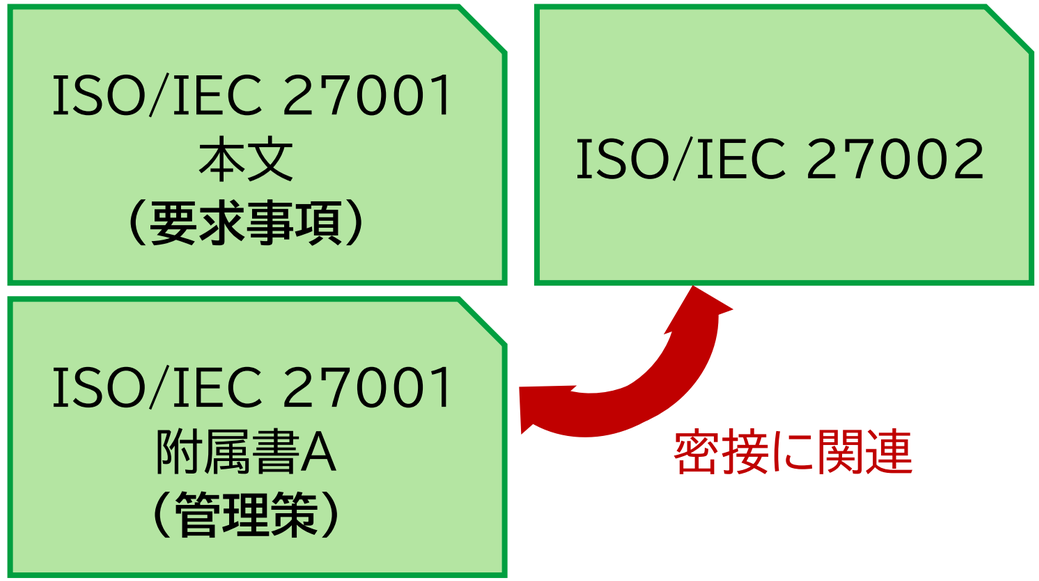


図1. ISO／IEC 27001とISO/IEC 27002の関係図
東京都 「【詳細解説】AI活用とセキュリティガバナンスのための統合規格マネジメント：ISO/IEC 27001, 27002 & 42001 詳細分析レポート」をもとに作成
https://www.cybersecurity.metro.tokyo.lg.jp/security/KnowLedge/656/index.html

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

【参照:テキスト26-1.】P2～P5

サイバーレジリエンスの実践策

1. 事前準備
   - 5.9　情報及びその他の関連資産の目録
   - 5.12　情報分類
   - 8.8　技術的ぜい弱性の管理
   - 8.13　情報のバックアップ

2. 対応
   - 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
   - 5.26　情報セキュリティインシデントへの対応
   - 8.15　ログ取得
   - 5.6　専門組織との連絡

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

【参照:テキスト26-1.】P2～P5

サイバーレジリエンスの実践策

3. 回復
   - 5.29　事業の中断・阻害時の情報セキュリティ
   - 5.30　事業継続のための情報セキュリティ
   - 8.14　情報処理施設・設備の冗長性

4. 学習と改善
   - 5.27　情報セキュリティインシデントからの学習
   - 6.3　情報セキュリティの意識向上、教育及び訓練

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

【参照:テキスト26-1.】P2～P5

サイバーレジリエンスの実践策のイメージ

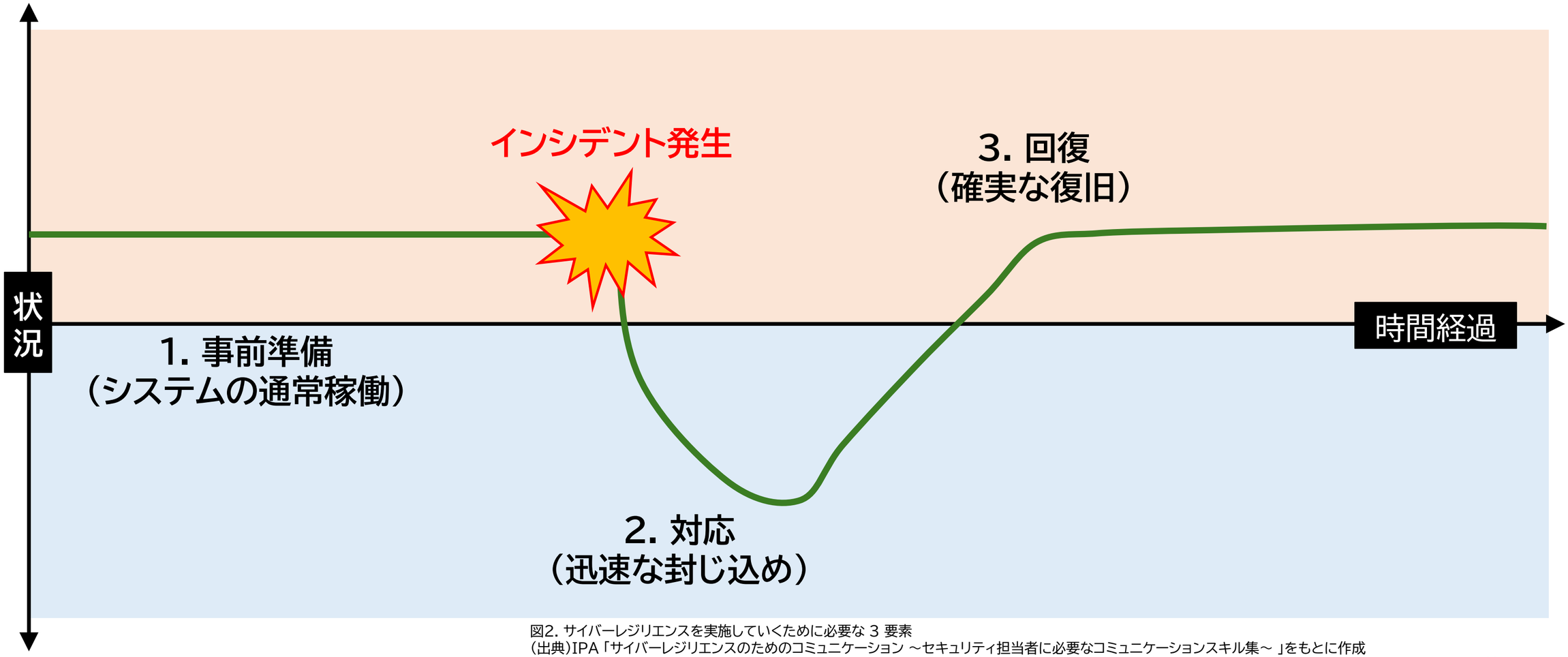


図2. サイバーレジリエンスを実施していくために必要な 3 要素
(出典)IPA「サイバーレジリエンスのためのコミュニケーション ～セキュリティ担当者に必要なコミュニケーションスキル集～ 」をもとに作成
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/f55m8k00000070u7-att/f55m8k000000710q.pdf

ISO/IEC 27002に基づく情報セキュリティインシデント管理策

【参照:テキスト26-2.】P6

情報セキュリティインシデント対応

情報セキュリティインシデント対応の位置づけ

- 情報セキュリティインシデント対応は組織的対策であり、サイバーセキュリティフレームワーク(CSF2.0)の Respond／Recover 機能に対応している

管理策で求められる対応内容

- 対応手順の整備、事象分析、証拠保全、関係者への報告を実施する
- 対応後は教訓を反映し、再発防止策を改善に繋げる

技術的対策

- バックアップや冗長化は Recover の基盤となる
- 有効性は RTO／RPO や訓練結果で評価する

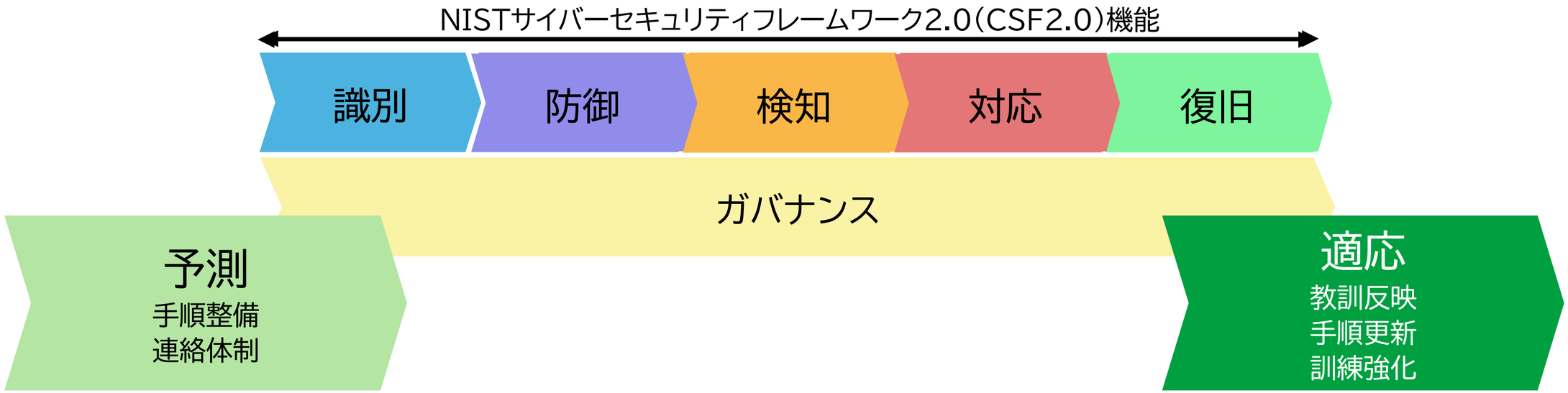
ISO/IEC 27002に基づく情報セキュリティインシデント管理策

【参照:テキスト26-2.】P6

情報セキュリティインシデント対応

マネジメントと改善

- 経営層の統制とリスク判断が不可欠である
- インシデント経験を学習し、手順や教育を継続的に改善することで、レジリエンスの「予測・適応」機能が定着する



情報セキュリティインシデント対応イメージ

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
https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf

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

【参照:テキスト26-3.】P7～P9

サイバーセキュリティフレームワーク(CSF)2.0

NIST CSF 2.0とサイバーレジリエンス

- Govern／Identify／Protect／Detect／Respond／Recover の6機能
- サイバーレジリエンスの中心は Respond(対応) と Recover(復旧)
- Govern は、サイバー対策を経営の責任として組織全体に統合する役割を持つ

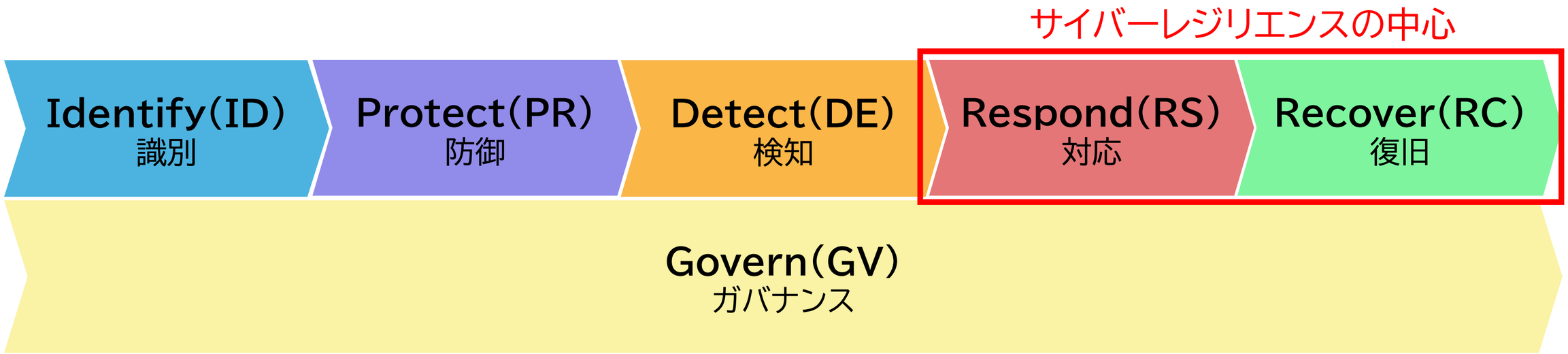


図4. NIST　CSF2.0におけるサイバーレジリエンスの中心
IPA「The NIST Cybersecurity Framework (CSF) 2.0(2024年2月)」の翻訳版をもとに作成
https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf

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

【参照:テキスト26-3.】P7～P9

中小企業におけるCSF 2.0活用の実践指針

中小企業では、限られたリソースを考慮し、段階的に重点領域を整備することが現実的

CSF Tier	段階	重点機能	主な取り組み	目標
Tier 1～2	初期段階	Identify・Protect	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・Respond	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、定期的な訓練と連絡網の整備、遠隔環境を含む監視強化	迅速な対応体制の整備
Tier 4	成熟段階	Govern・Recover	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

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

【参照:テキスト26-3.】P7～P9

中小企業におけるCSF 2.0活用の実践指針

　中小企業では、特にTier1～2を基盤に整備し、段階的にTier3及びTier4へ拡張していくと過度な負担なく現実的な体制を構築できる。

ガバナンス機能(Govern・GV)

- リスク評価やインシデント状況を定期的に経営層へ報告
- 経営層はリスク許容度・投資方針を決定し、IT計画に反映
- CSFをISMSや経営方針に組み込み、レジリエンスを定着

サイバーレジリエンスの有効性確認のための指標例

- 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

サイバーレジリエンス能力の育成に向けた体系項立て

【参照:テキスト26-4.】P10～P11

主要フレームワークの機能比較と統合

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と主たる目的

サイバーレジリエンス ライフサイクル	CSF2.0機能	主たる目的
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
防御	Protect（PR）	脅威に対する予防的コントロールの実装
検知	Detect（DE）	異常およびインシデントの早期発見
対応	**Respond（RS）**	**被害の封じ込め、根絶、コミュニケーション**
復旧	**Recover（RC）**	**事業の迅速な回復、サービスの復元**
改善・適応	Govern（GV） Recover（RC）	教訓の反映、体制の強化、継続的改善

サイバーレジリエンス能力の育成に向けた体系項立て

【参照:テキスト26-4.】P10～P11

NIST CSF2.0に基づく段階的育成モデル例

CSF	段階・目標	重点機能	主な取り組み
Tier 1	**Partial** **（部分的対応）** 重大被害の回避	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）
Tier 2	**Risk-Informed** **（リスク認識段階）** 継続的対策の開始	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
Tier 3	**Repeatable** **（再現的運用段階）** 継続的運用の確立	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
Tier 4	**Adaptive** **（適応的高度段階）** 自律的なレジリエンス経営	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

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

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

NIST CSF 2.0 Respond（RS）機能に基づく対応基準

NIST CSF 2.0 Recover（RC）機能に基づく復旧基準

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

【参照:テキスト27-1.】P13～P14

サイバーレジリエンス・ライフサイクルと対応計画策定

総合的な対応計画(IRPとIT-BCPの統合)

- インシデント対応計画(IRP)とIT-BCPを一体化して策定し効率的に運用できる
- サイバーレジリエンスは、予防から復旧までのPDCAサイクルとして能力を強化
- ISO/IEC 27002組織的対策とNIST CSFのRespond・Recoverが基盤となる

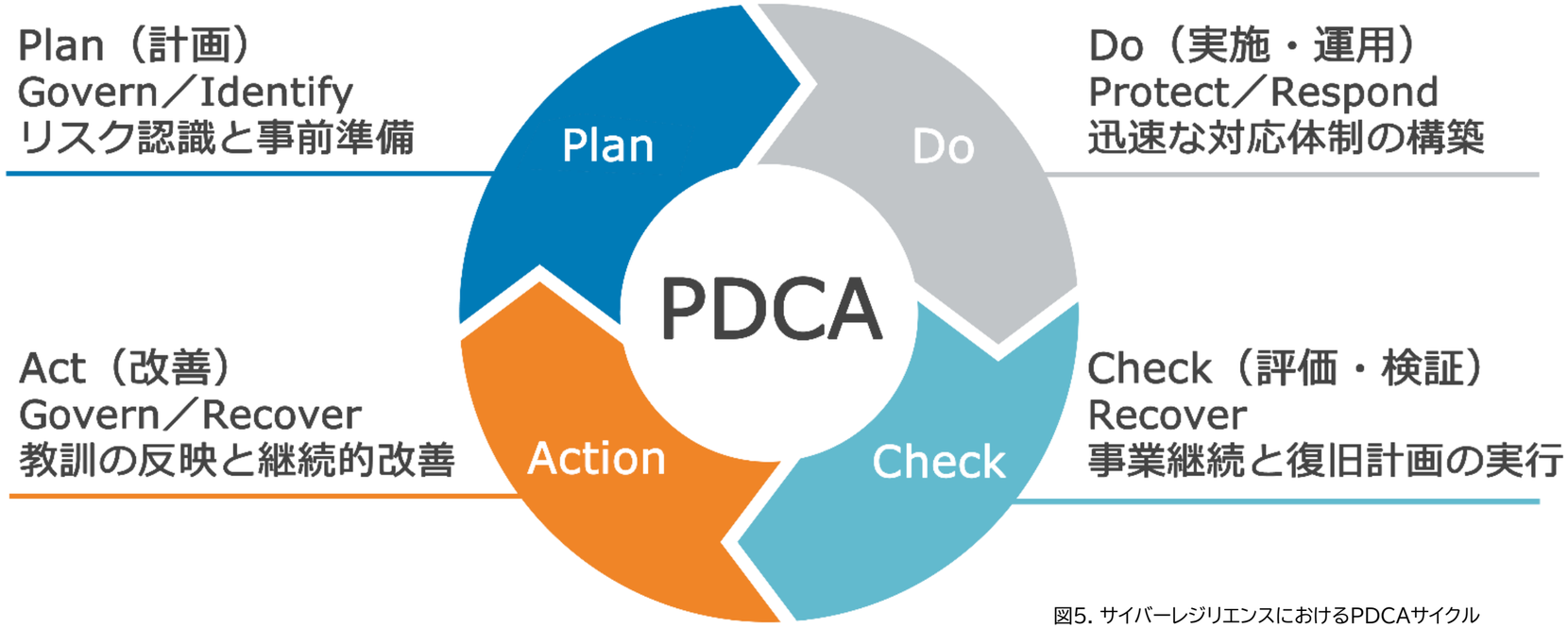


図5. サイバーレジリエンスにおけるPDCAサイクル

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

【参照:テキスト27-1.】 P13～P14

サイバーレジリエンス・ライフサイクルモデル例

フェーズ	CSF機能対応と主な目的	実施の要点
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、NISC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のライフサイクルと対応計画の策定

【参照:テキスト27-1.】 P13～P14

サイバーレジリエンス確立のための3要素

経営層の関与

- レジリエンスは経営リスクであり、トップが方針・優先度・体制を主導する
- NIST CSF 2.0 の Govern機能を組織に定着させる

計画と対応の統合

- IRPとIT-BCPを1つの「総合的対応計画」として統合することで、判断・行動の一貫性と効率的運用を確保する

継続的な改善

- 対応・復旧の教訓を手順書や訓練へ反映する
- PDCAを回し続けることで、レジリエンスが組織文化として定着させる

経営判断、計画統合、継続改善の3つが揃うことで、持続的な事業継続力を高められる。

NIST CSF 2.0 Respond（RS）機能に基づく対応基準

【参照:テキスト27-2.】P15～P16

インシデント管理体制の確立(RS.IM)

RS機能はインシデント発生時に迅速に行動し、影響を封じ込めるための機能であり、混乱を防ぎ組織的に対応するために 初動対応の手順と役割分担の明確化が必須である

対応フロー

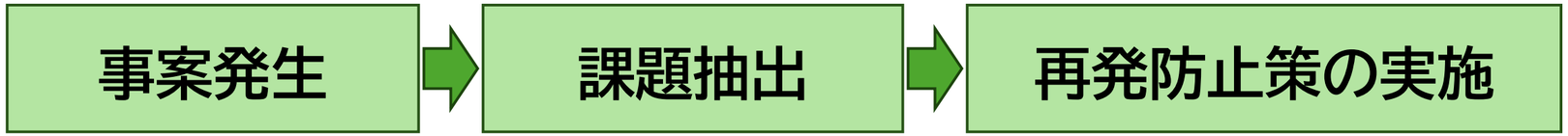


図6. 検知後の対応フロー

中小企業が整備すべきRS.IMにおける4つの領域

- 役割分担の明確化(経営層／IT／現場)
- 報告・判断プロセスの文書化
- 外部機関との連携整備(IPA、JPCERT、ベンダ等)
- 訓練と改善の継続(年1回の机上演習、手順改善)

事後レビューの実施により得られた知見から組織の危機対応力を継続的に強化することで、RS.IMは単なる手順書ではなく、実践的なレジリエンス向上の仕組みとなる。

NIST CSF 2.0 Respond（RS）機能に基づく対応基準

【参照:テキスト27-2.】 P15～P16

インシデントの分析と軽減策(RS.AN、RS.MI)

RS.AN(分析能力)におけるインシデント初期対応では、原因究明・影響範囲の特定・証拠保全が最重要となる。分析には ログ(記録)の存在が必須であり、事後分析(フォレンジック)の基盤となるため、長期保存と保護が必要となる。

RS.MI(軽減策)においては、被害拡大を防ぐための封じ込め行動が中心となり、ランサムウェア対策として多要素認証(MFA)やジャンプサーバ経由のアクセス制御などの技術的対策が有効である。

中小企業が整備すべき3つの段階

- 記録　　適切なログ取得と保全
- 封じ込め　　侵入経路遮断・横展開防止
- 改善　　対応後の見直しと継続的強化

NIST CSF 2.0 Recover（RC）機能に基づく復旧基準

【参照:テキスト27-3.】P17～P21

復旧計画の実行(RC.RP)と事業復旧目標の設定

復旧計画(RC.RP)

- 事業継続計画(BCP)の一環としてRTO(目標復旧時間)とRPO(目標復旧時点) を明確に設定する
- RTO/RPO の設定は、経営層がビジネス要件とリスク許容度に基づいて行う戦略的判断となる

復旧の技術基盤

- バックアップと冗長化 が復旧計画の核心である
- 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、成功可否を左右する
- CSF 2.0 は、復旧しやすいシステム設計を重視する

RC.RPはバックアップ中心の対策ではなく、経営判断と技術対策を統合したレジリエンス戦略の要であり、中小企業もRTO／RPOの文書化と復旧手順検証が必要である。

NIST CSF 2.0 Recover（RC）機能に基づく復旧基準

【参照:テキスト27-3.】P17～P21

復旧計画の実行(RC.RP)と事業復旧目標の設定

中小企業が整備すべき4つの視点

1. 目標設定(RTO／RPO)

- 業務影響度分析(BIA)に基づき、業務ごとにRTO／RPOを設定し、経営層が承認

2. 優先順位付け・復旧責任

- 全システム同時復旧は困難なため、重要度で復旧順序と代替手段を決定する

3. バックアップ・冗長化

- 3-2-1ルール(3世代・2媒体・1つはオフライン)を基本とする
- 定期的なリストアテストを実施し、クラウドは復旧支援範囲・保持期間を確認する

4. 検証と改善

- 復旧手順演習を年1回以上実施により、PDCAに組み込み継続的に改善させる

NIST CSF 2.0 Recover（RC）機能に基づく復旧基準

【参照:テキスト27-3.】 P17～P21

復旧のためのコミュニケーション(RC.CO)

RC.CO(復旧コミュニケーション)の目的

- 復旧時に、内部(従業員・経営)と外部(顧客・規制当局・IPA等)との情報調整を行い、透明性を確保するための機能である
- インシデントの被害状況・初動対応・復旧状況を適切なタイミングで正確に通知することが求められる
- 適切なコミュニケーションは 信頼維持に直結する

NIST CSF 2.0 Recover（RC）機能に基づく復旧基準

【参照:テキスト27-3.】P17～P21

CSF 2.0 対応・復旧機能に基づく対応計画の基準

CSF機能	カテゴリー（RC/RS）	機能の目的	対応基準
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
	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
	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
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
	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
	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

NIST CSF 2.0 Recover（RC）機能に基づく復旧基準

【参照:テキスト27-3.】P17～P21

復旧のためのコミュニケーション(RC.CO)

中小企業が整備すべきRC.COの3要素

責任体制の明確化

- 技術・広報・顧客対応の責任者を事前に指定する
- 緊急連絡先リストを作成し、オフラインでも参照可能にしておく

外部調整と情報発信

- クラウド・委託先との連絡体制を契約書やSLAに明記し、窓口を共有する
- 顧客・取引先への報告は 事実のみ、推測なしで行う

訓練と改善

- 年1回以上、情報伝達を想定した訓練(報告・連絡・公表)を実施する
- 演習結果を手順書へ反映し、役割理解と精度を向上させる

第28章. IT-BCPの一環としてのインシデントに対応する体制

情報システム継続計画（IT-BCP）の基本要素と体制
インシデント対応体制の確立と初動対応の具体的手順
復旧・回復プロセスと教訓の反映（継続的改善）
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

情報システム継続計画（IT-BCP）の基本要素と体制

【参照：テキスト28-1.】
P22～P23

サイバーレジリエンスとIT-BCP

　サイバーレジリエンスは IT-BCP（情報システム継続計画）と不可分であり、両者を一体として整備することが重要である。また、IT-BCPはサイバー攻撃を含む障害を想定し、事業の早期再開を目的とする組織的対策である。

経営層の役割と計画統合

- レジリエンス体制の構築は経営層のリーダーシップが不可欠である
- CSIRT等の役割・責任を明確化し、インシデント発生時は 経営者が指揮を執る
- 中小企業では、リソース効率化のためIT-BCPとIRPの統合が推奨される

情報システム継続計画（IT-BCP）の基本要素と体制

【参照：テキスト28-1.】
P22～P23

サイバーレジリエンスとIT-BCP

中小企業におけるIT-BCPの3要素

体制の明確化

- 経営層（統括）、IT担当者（技術）、総務（連絡）、外部ベンダ（支援）の役割を整理する

復旧優先順位の設定

- システムの重要度に応じて RTO・RPO を設定し、復旧責任者を決定しておく

訓練と見直し

- NCOや日本シーサート協議会（NCA）の演習資料を活用し、訓練と改善を継続する

【参考】演習資料例

NCA：　「サイバー攻撃演習訓練実施マニュアル」
IPA：　「セキュリティインシデント対応机上演習教材」
NCO：　普及啓発ポータル「みんなで使おうサイバーセキュリティ・ポータルサイト」

インシデント対応体制の確立と初動対応の具体的手順

【参照:テキスト28-2.】
P24～P27

初動対応のフェーズと実践(Respond機能の実装)

- 初動対応は 被害拡大防止・迅速復旧のため極めて重要である。
- 中小企業では専任担当者が不足するため、簡潔・実践的な行動指針を3フェーズの初動対応について整備することが必要である。

初動対応の3フェーズ

図7. 初動対応の3フェーズ

① 検知と報告

- EDR、ログ監視、従業員通報などで異常を検知したら即座に責任者へ報告
- 「インシデント報告書」に日時・対象・事象・対応状況を記録して共有
- 重大な場合は IPA・JPCERT/CC、個人情報漏えい時は規制当局へ報告

インシデント対応体制の確立と初動対応の具体的手順

【参照:テキスト28-2.】
P24～P27

初動対応のフェーズと実践(Respond機能の実装)

② 封じ込め(Containment)

- 攻撃拡大を防ぐため、感染端末の隔離・ネットワーク遮断を実施
- 証拠保全のため、ログ・記録を消さずに保存
- 必要に応じて、外部ベンダーやクラウド事業者へ支援依頼

③ 根絶(Eradication)

- マルウェア・不正設定・脆弱性などの原因を完全に除去
- 感染ファイル削除、パッチ適用、アカウント再発行、再スキャンで安全性を確認
- 作業記録は「インシデント対応記録」として保存し、復旧計画や再発防止策に活用

根絶後の対応として、事業継続の観点でIT-BCP／IRPに反映し、対応ログをもとに、初動・封じ込め・連絡手順の有効性をレビューし、年次更新を行う。

インシデント対応体制の確立と初動対応の具体的手順

【参照:テキスト28-2.】P24～P27

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

ランサムウェアからの確実な復旧には、具体策をサイバーレジリエンスの必須要件として組み込むことが重要である。

多要素認証(MFA)の適用　**アクセス制御の強化**　**バックアップと冗長化**

多要素認証(MFA)の重要性

- VPN・クラウド管理画面など全リモート接続に多要素認証(MFA)を適用し、ID・パスワード漏洩による侵入を遮断する
- 特に、管理者アカウントは必須と考えるべき
- スマートフォンアプリによるワンタイムパスワード(TOTP:Time-based One Time Password)方式や緊急コードの安全管理を推奨する

インシデント対応体制の確立と初動対応の具体的手順

【参照:テキスト28-2.】
P24～P27

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

アクセス制御の強化

- 重要サーバへの接続はジャンプサーバ経由に限定し、横展開を防止する
- 不要なポート閉鎖、共有アカウント廃止、権限分離、アクセスログ保存などを実施する

バックアップと冗長化

- ランサムウェア後の復元には バックアップの完全性の確保が不可欠である
- オフラインバックアップ、クラウド版の過去バージョン保持、複数保存先を確保する
- バックアップデータ保管責任者の明確化が重要である

復旧・回復プロセスと教訓の反映（継続的改善）

【参照：テキスト28-3.】
P28～P30

復旧・回復プロセスと教訓の反映（継続的改善）

　復旧後は、根本原因に基づく恒久的な対策を実施することが不可欠であり、特権アカウント管理や脆弱性確認などの運用改善を手順化し、PDCAで継続強化する。

原因分析と改善策の立案　**改善の実行と記録**　**再発防止計画とレビュー**

原因分析と改善策

- インシデントの原因を 技術的・組織的・人的の3視点で分析。
  - 技術的：　設定不備、脆弱性、更新漏れ
  - 組織的：　連絡体制の不備
  - 人的：　教育不足
- 改善策を明確化し、IT-BCPや対応記録に反映。

インシデント対応体制の確立と初動対応の具体的手順

【参照:テキスト28-3.】
P28～P30

復旧・回復プロセスと教訓の反映（継続的改善）

改善の実行と記録

- 対策は担当・期限・確認方法を決めて実行する
- 技術・運用・教育・外部委託の分類で整理し、効果を記録して見直す

再発防止計画とレビュー

- 改善結果を半期・年次で点検し、未完了項目は翌年へ繰り越す
- 必要に応じて外部専門家の助言を活用する
- 経営層に報告し、IT-BCPの更新に反映する

インシデント対応体制の確立と初動対応の具体的手順

【参照:テキスト28-3.】
P28～P30

教訓の反映と継続的改善（RC.IM）

サイバーレジリエンス向上の基本的な考え方として、インシデント対応で得た 教訓を体系化し改善につなげることが不可欠であり、ISMS の「改善」プロセスを活用し、復旧後の事後評価を必ず実施する。

また、RC.IMは、復旧プロセスに過去の教訓を反映することを要求されており、ポリシー見直し、設計改善、訓練更新を通じてレジリエンスを継続的に向上させる。

- 成功点と課題の明確化及び教訓の整理
- 改善項目の管理と反映
- 継続的改善の仕組み化

インシデント対応体制の確立と初動対応の具体的手順

【参照:テキスト28-3.】
P28～P30

教訓の反映と継続的改善（RC.IM）

成功点・課題の整理（事後レビュー）

- 復旧後に初動～復旧までを振り返り、成功点と課題を明確化する
- 手順・技術・体制の観点で教訓を整理し、「改善記録表」にまとめる

改善項目の管理と反映

- 各改善項目に 担当・期限・確認方法 を設定して管理する
- 改善結果は IT-BCP・手順書・関連文書へ反映し、経営層とも共有する

継続的改善の仕組み化

- 改善効果を確認し、未実施項目は次年度計画へ繰り越す
- 教訓を定例会や研修で共有し、組織全体の意識を向上させる

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

【参照:テキスト28-4.】 P31～P33

サイバーレジリエンス能力向上のための演習と訓練

　文書化された IT-BCP／IRP を実効的にするには、定期的な訓練・演習が必須であり、訓練は、計画の有効性検証、役割の明確化、習熟度向上に直結する。

対象別の訓練の推奨

- 経営層向け:　　サイバーリスク判断や対外説明のシミュレーション訓練
- 実務担当者向け:　CYDER・RPCIなどの実践的演習で封じ込め・復旧手順を習得

人材育成の統合

- 非専門人材も初期対応（報告・連絡・封じ込め補助）を行えるよう、「プラス・セキュリティ」などの基礎教育を継続する
- 中小企業では、これが外部専門家との橋渡し役として重要である

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

【参照:テキスト28-4.】P31～P33

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)	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	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	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、恒久対策の実施	タイムリーな事業の再開
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	組織全体のレジリエンス向上と適応性の獲得

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

【参照:テキスト28-4.】P31～P33

訓練・教育のおける定着のための実践的な手順

訓練・教育の実施方法

- 組織の成熟度に合わせて 机上 → 模擬 → 外部演習 を段階的に導入する
- 訓練目的・対象・頻度(年1回以上)を明確化する

訓練結果の活用

- 訓練後は評価表で改善点(連絡体制・判断・文書整合性)を整理する
- 結果を IT-BCP に添付し、次回改善サイクルへ反映 → レジリエンス向上に直結する

外部支援の活用

- IPA:サイバー演習教材・CYDER
- NCO:演習モデル・訓練シナリオ
- 地域組織:商工会等との合同訓練

外部支援の活用で、小規模でも現実的な訓練環境を構築できる。

令和7年度
中小企業サイバーセキュリティ
実践力強化プログラム

東京都産業労働局