IPUT TOKYO

情報セキュリティ応用
第12回　セキュリティマネジメント

愛川 知宏

東京国際工科専門職大学
International Professional University of Technology in Tokyo

授業スケジュール

日時	内容	日時	内容
第１回	ガイダンス	第９回	情報・ネットワークへの脅威と対処
第２回	インターネット上の脅威	第１０回	攻撃を誘発する脆弱性
第３回	攻撃の背景	第１１回	技術と方法に関する確認
第４回	原因の追究（被害を受ける側の限界）および確認	第１２回	セキュリティマネジメント
第５回	認証と認可	第１３回	ソーシャルリスクへの対処
第６回	暗号の基礎（１）	第１４回	セキュリティマネジメント、ソーシャルリスクに関する確認
第７回	暗号の基礎（２）	第１５回	全体のまとめ
第８回	暗号の応用		期末試験

本日の目標（シラバスより）

- 前回までセキュリティに関する技術的な面について述べてきたが、今回は予防や対応といった人的な活動として必要な事項を学ぶ。具体的にはリスクを低減するためのセキュリティマネジメント、および被害が生じた際の対応を担うCSIRTの活動について理解する。

- **重要キーワード**
  - **ISMS、CISO、EDR、ゼロトラスト、サイバーキルチェーン、CSIRT**

リスクと危機

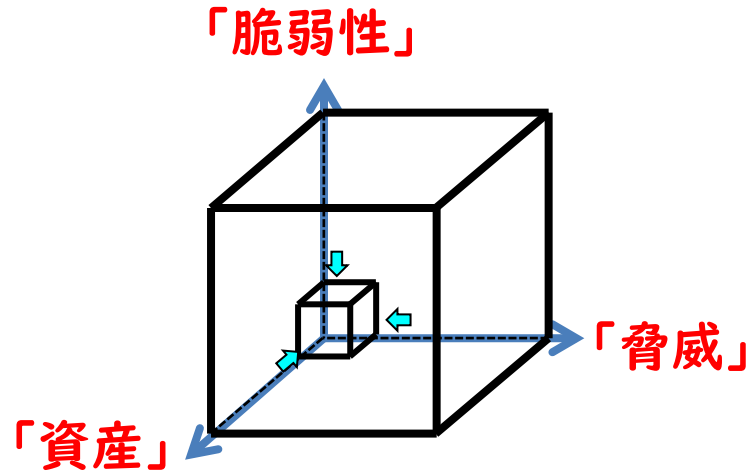
- **リスク(risk)**
  A situation involving exposure to danger
  危険が生じるかもしれない状況（可能性）
  →起きないようにしっかりと備える（リスク管理）

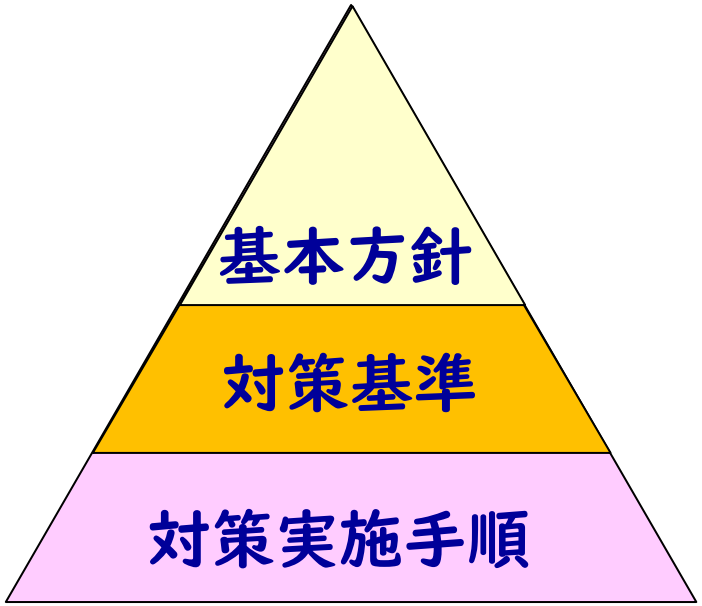
- **危機 (incident)**
  a violent event such as a fracas or assault
  危険が生じてしまった状況（現実化）
  →被害を最小限に抑え、迅速に回復をはかる（危機対応）

セキュリティとはこの2つに対処すること、ともいえる

リスクに備える（マネジメント）

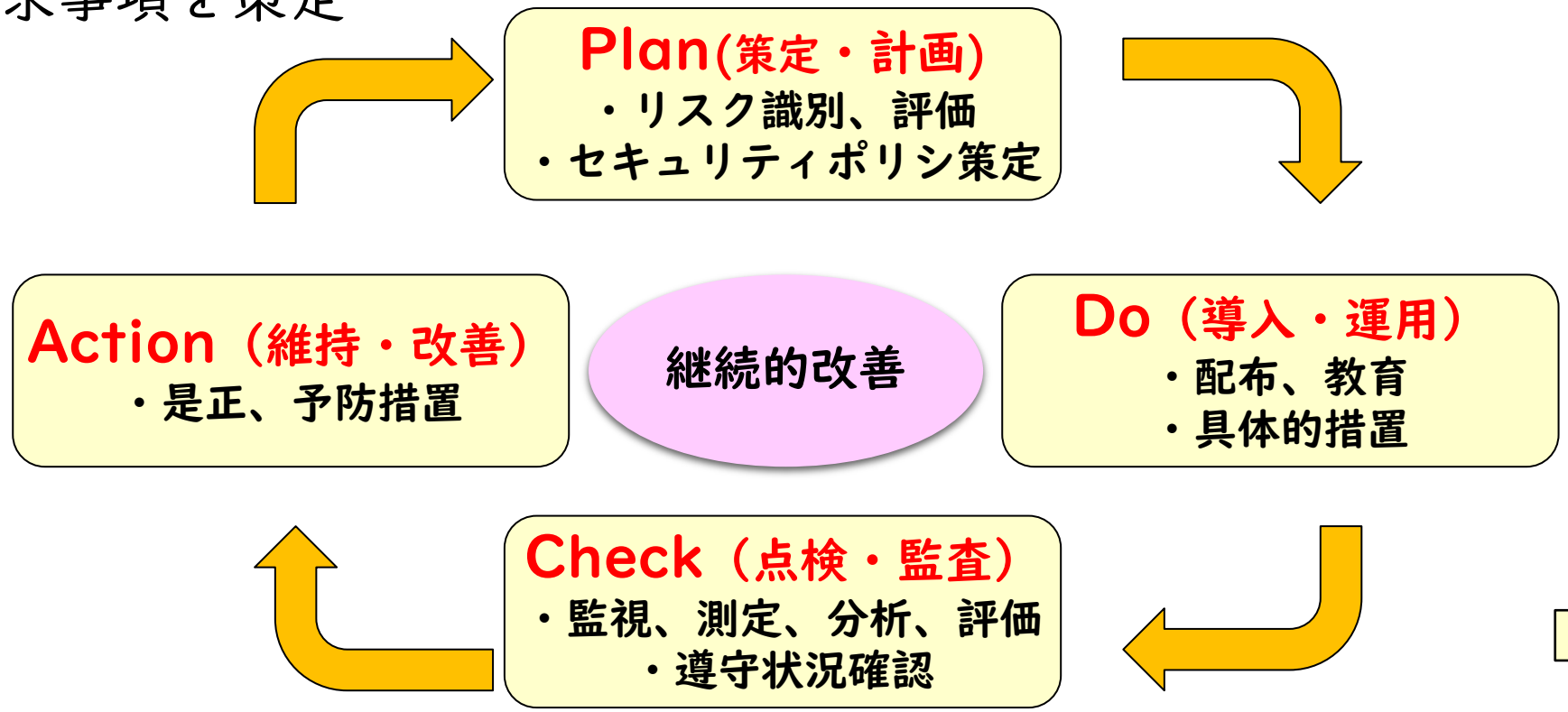
- リスクを識別する
  - 守るべき資産は何か？
  - 想定しうる脅威は何か？
  - 判明している脆弱性は？
- リスクを評価する
  - 情報セキュリティの３要素／７要素
- リスクへの対応方針を決める
  - セキュリティポリシー（方針、基準、手順）





ISMS（情報セキュリティマネジメントシステム）

- Information Security Management System
- 国際規格 ISO/IEC 27001:2013 (日本産業規格JIS Q 27001:2014)として要求事項を策定



認証取得例

認証機関

認証機関の認定機関

ISO/IEC27001の構成

まえがき	
0 序文	0.1 概要 0.2 他のマネジメントシステム規格との両立性
1 適用範囲	
2 引用規格	
3 用語及び定義	
4 組織の状況	4.1 組織及びその状況の理解 4.2 利害関係者のニーズ及び期待の理解 4.3 情報セキュリティマネジメントシステムの適用範囲の決定 4.4 情報セキュリティマネジメントシステム
5 リーダーシップ	5.1 リーダーシップ及びコミットメント 5.2 方針 5.3 組織の役割，責任及び権限
6 計画	6.1 リスク及び機会に対処する活動 6.2 情報セキュリティ目的及びそれを達成するための計画策定
7 支援	7.1 資源 7.2 力量 7.3 認識 7.4 コミュニケーション 7.5 文書化した情報
8 運用	8.1 運用の計画及び管理 8.2 情報セキュリティリスクアセスメント 8.3 情報セキュリティリスク対応
9 パフォーマンス評価	9.1 監視，測定，分析及び評価 9.2 内部監査 9.3 マネジメントレビュー
10 改善	10.1 不適合及び是正処置 10.2 継続的改善
附属書A（規定）	管理目的及び管理策

CISO(Chief Information Security Officer)

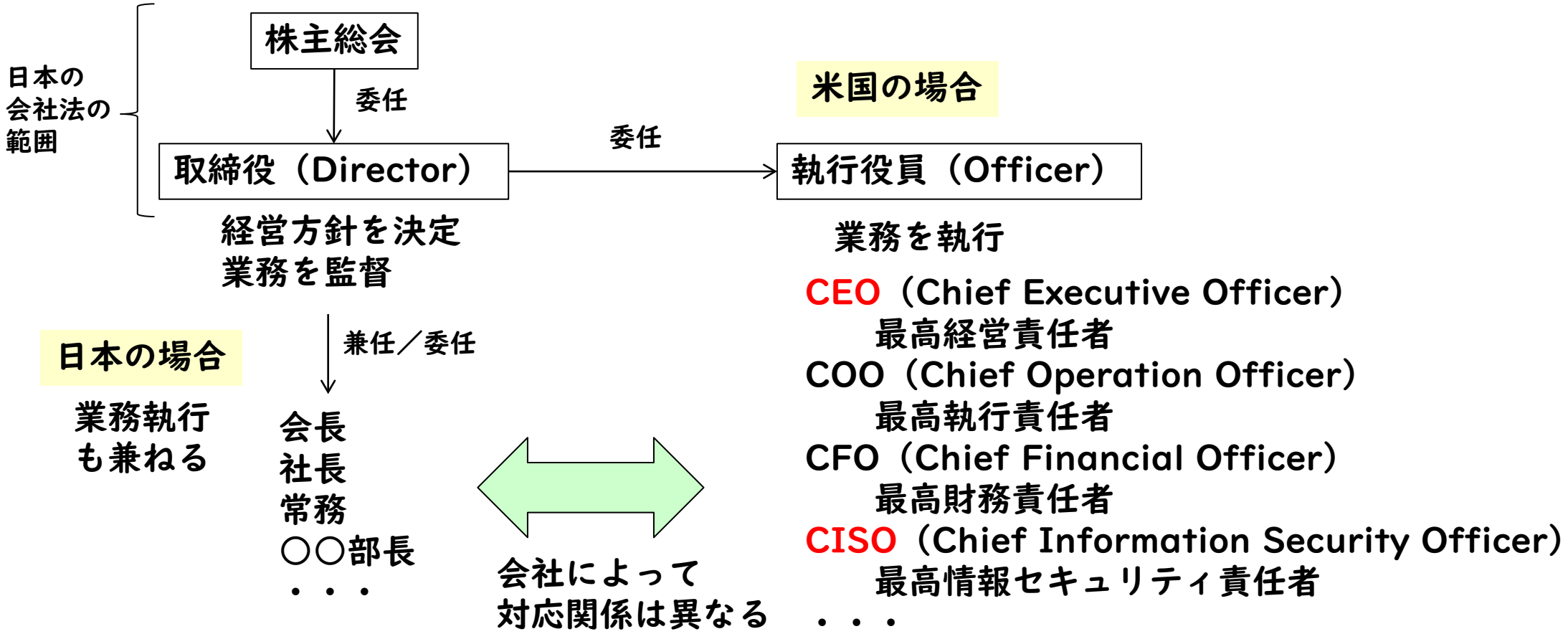
- 企業・組織内において情報管理およびその運用を担当し、情報セキュリティを統括する責任者

求められる役割		内容
マネジメント的側面	Strategist	組織の事業、サイバーリスクに対する戦略を主導し、価値の高い投資によるリスク管理する変革を創造・推進
	Advisor	サイバーセキュリティに対するリスクの観点から事業に対し、教育 / アドバイス / 普及 / 啓発
技術的側面	Guardian	サイバーセキュリティに対する脅威の全体像を理解し、リスクに関するプログラムの有効性を高めることで事業の重要な資産を保護
	Technologist	組織のセキュリティ機能を構築するためのセキュリティ技術及び標準の評価、導入

https://www.lrm.jp/security_magazine/ciso/ より引用

(参考)会社組織について

- 社長と代表取締役とCEOの違い、わかりますか？



セキュリティ管理

- クライアントセキュリティ
- サーバセキュリティ
- ネットワークセキュリティ

リスクの識別・評価に基づいて考える

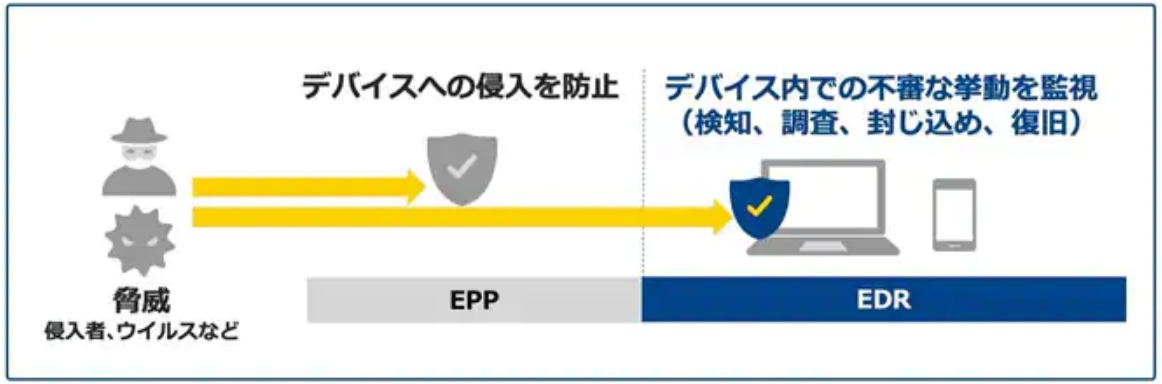
クライアントセキュリティ

- セキュリティパッチの最新化
- アンチウイルスソフトの適用、定義ファイル最新化
- ユーザ教育：セキュリティ意識の向上
- 利用ルールの整備
  - 私物端末の接続禁止
  - Web閲覧先の制限　など
- ヘルプデスク
  - 問合せ対応
  - インシデント報告窓口
- **EDR**の導入
  - デバイスの挙動監視により、脅威を検知・対処

EDR(Endpoint Detection and Response)

- コンピュータシステムのエンドポイント（端末）において脅威を継続的に監視して対応する技術

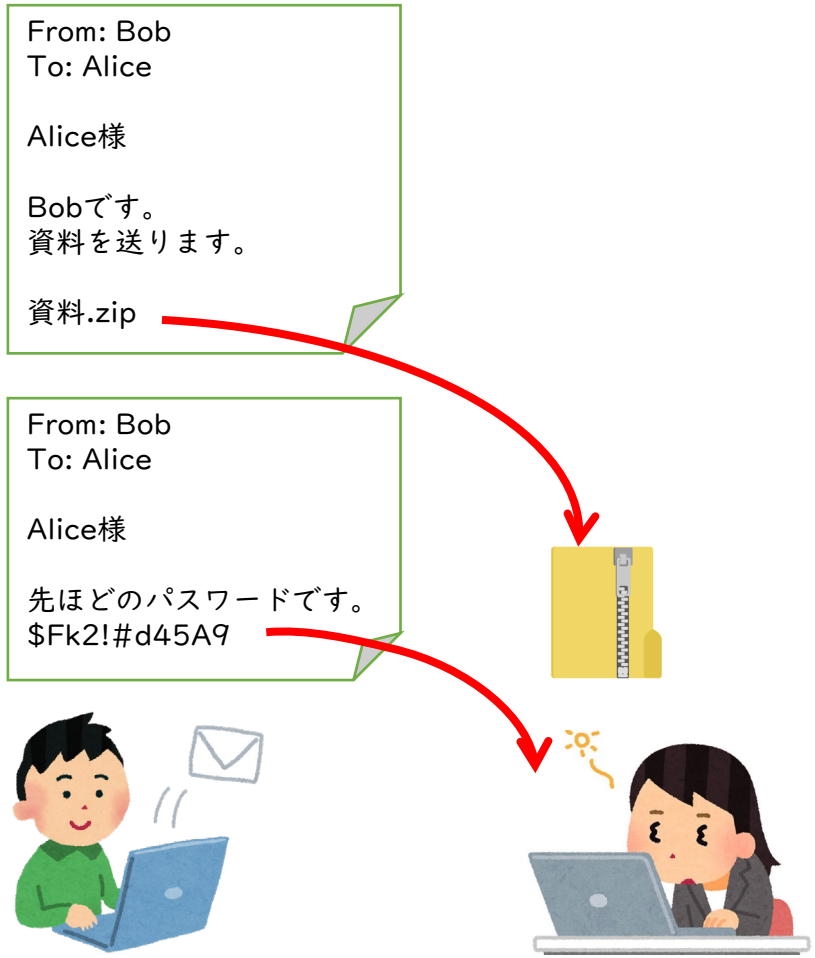
- アンチウイルスソフト(EPP: Endpoint Protection Platform)との違い
  - ネットワーク全体での端末監視
  - 端末のログ解析で攻撃検知
  - 端末の被害状況特定
  - 全端末の状態を可視化



https://www.ntt.com/business/lp/edr.html

PPAP

- P: Password付きZIPファイルを送ります、
- P: Passwordを送ります、
- A: Angouka（暗号化）
- P: Protocol（プロトコル）



多くの企業で取り入れられていましたが、
電子メールのセキュリティ対策としては
悪手とされ、廃止の動きが進みつつあります。
https://twitter.com/hiratakuchan/status/1331150538637938689

サーバセキュリティ

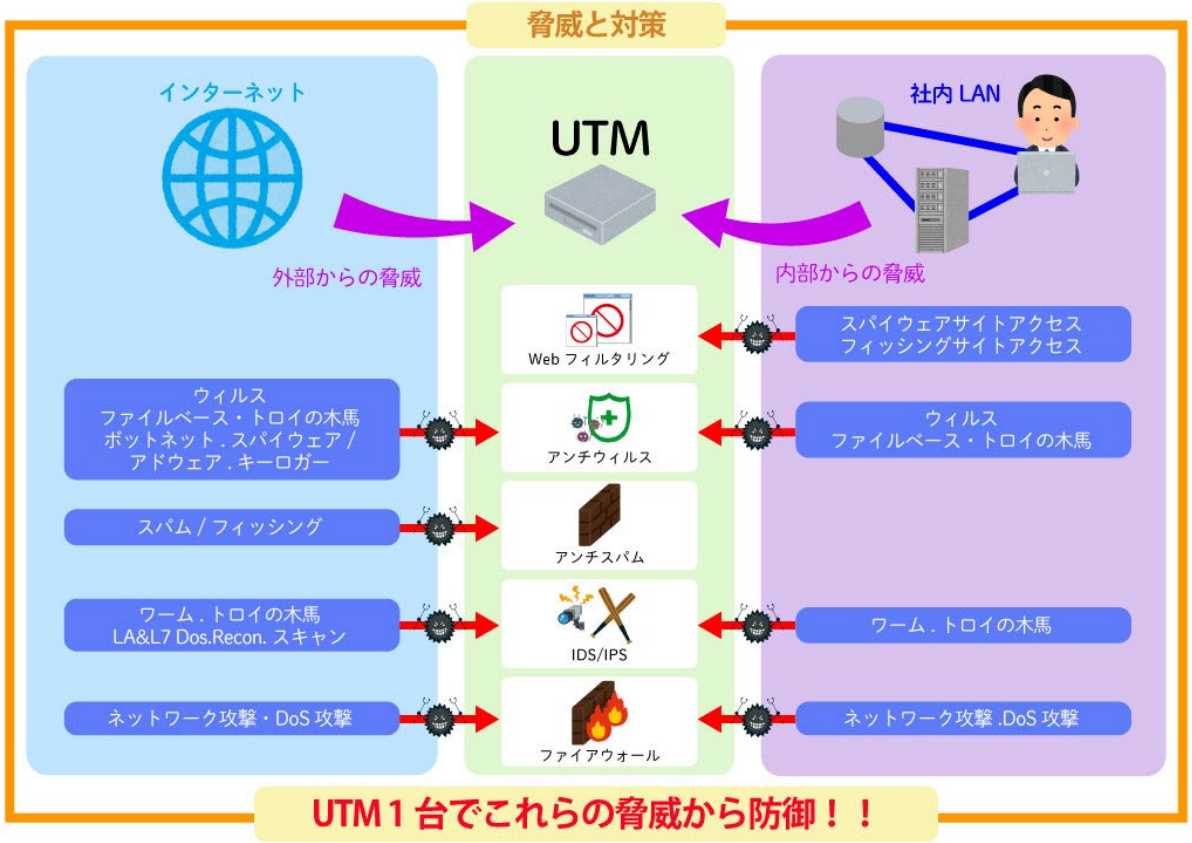
- セキュリティパッチの最新化
- アンチウイルスソフトの定義ファイル最新化
- データの安全性確保
  - バックアップ
  - 暗号化
  - 真正性（改ざん、破壊）チェック
- ログデータのチェック
  - OSログ、サービスログ等
- 脆弱性検査
  - 脆弱性診断
  - ペネトレーションテスト

ネットワークセキュリティ

- Firewall, IDS/IPS等の導入
- ログデータのチェック
  - それぞれの機器が出力するイベントログを統合的にチェック →SIEM
- 脆弱性検査
  - 脆弱性診断
  - ペネトレーションテスト
- 検疫システム
  - 社内LANに繋ごうとする端末を一旦検疫ネットワークに隔離
  - 安全確認後に社内LANへの接続を許可

UTM (Unified Threat Management)

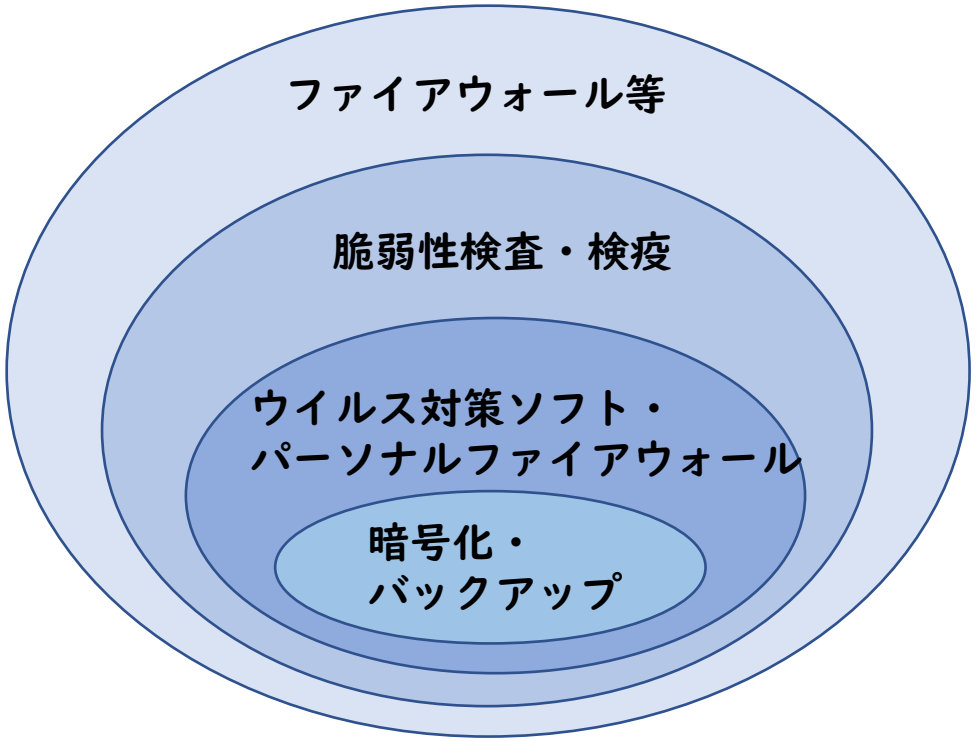
- 複数の異なるセキュリティ製品の機能を統合して集中管理する仕組み

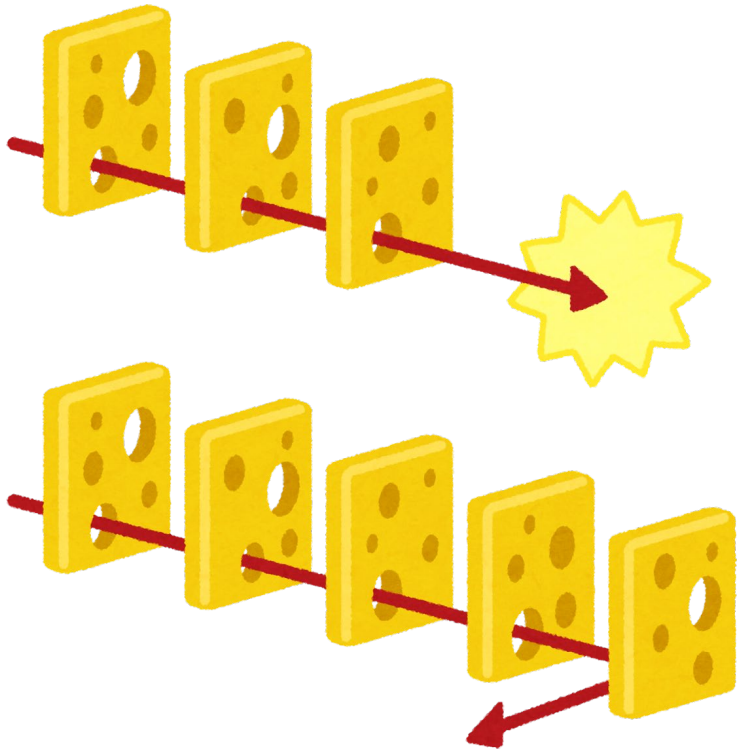


https://cybersecurity-jp.com/utm/utm_01/

多層防御(スイスチーズモデル)

- 一つの対策で全てを賄うのではなく、多層的な防御により安全性を高める





サイバーキルチェーン

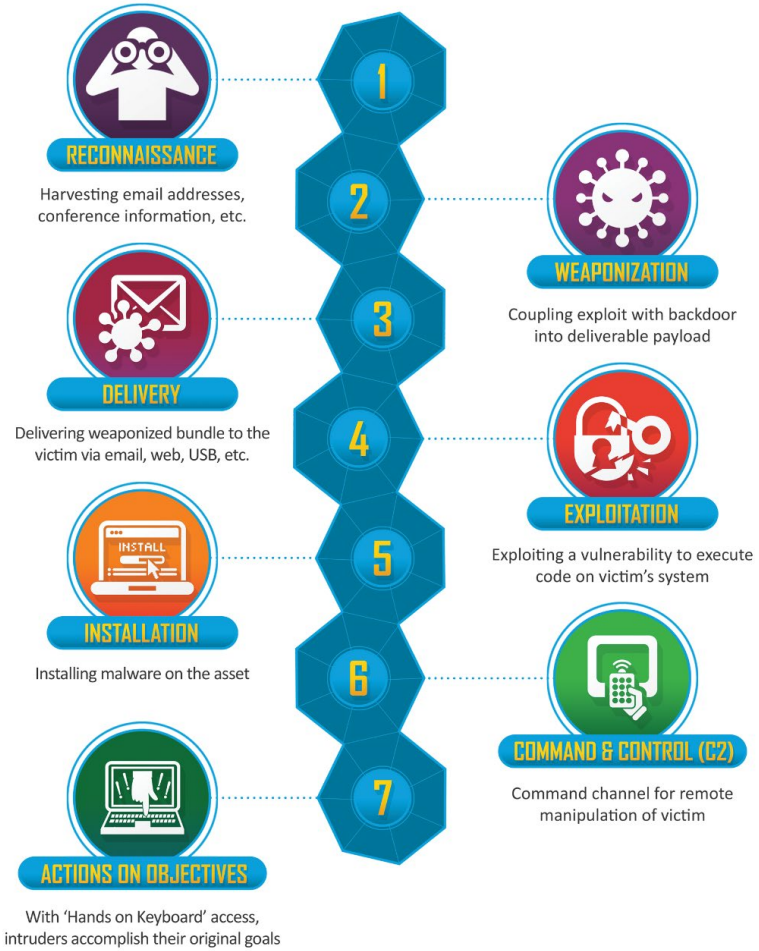
- 2009年にロッキード・マーチン社が作成した、サイバー攻撃の行動段階を整理したもの

- 7つの行動段階
  1. 偵察
  2. 武器化
  3. 配送
  4. 攻撃
  5. インストール
  6. 遠隔制御
  7. 目的達成

入口対策

内部対策

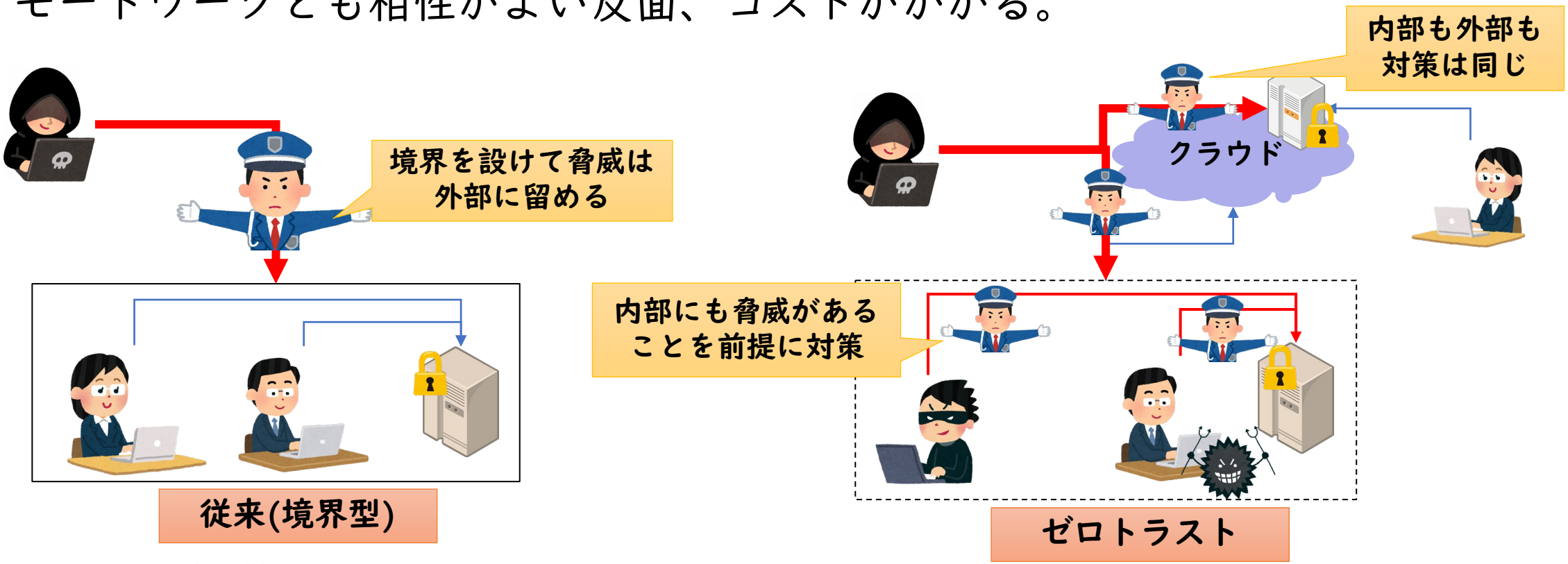
出口対策



https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

ゼロトラスト

- 働き方の多様化や内部犯対策等から注目されるセキュリティモデル
- 境界をおかず全てを「信頼できない」前提で対策を行うため、クラウドやリモートワークとも相性がよい反面、コストがかかる。



リスクと危機

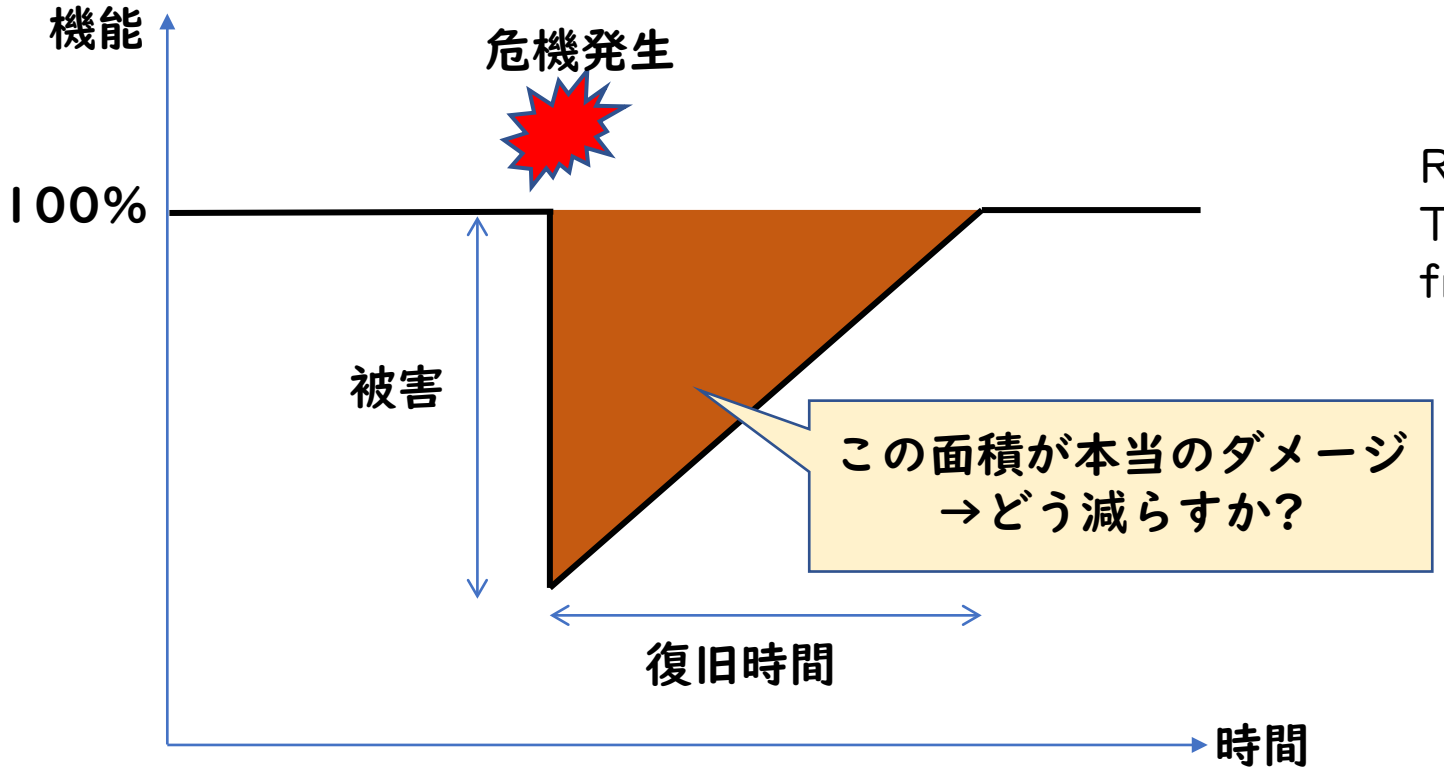
- **リスク(risk)**
  A situation involving exposure to danger
  危険が生じるかもしれない状況（可能性）
  →起きないようにしっかりと備える（リスク管理）

- **危機 (incident)**
  a violent event such as a fracas or assault
  危険が生じてしまった状況（現実化）
  →被害を最小限に抑え、迅速に回復をはかる（危機対応）

セキュリティとはこの2つに対処すること、ともいえる

レジリエンス(Resilience)

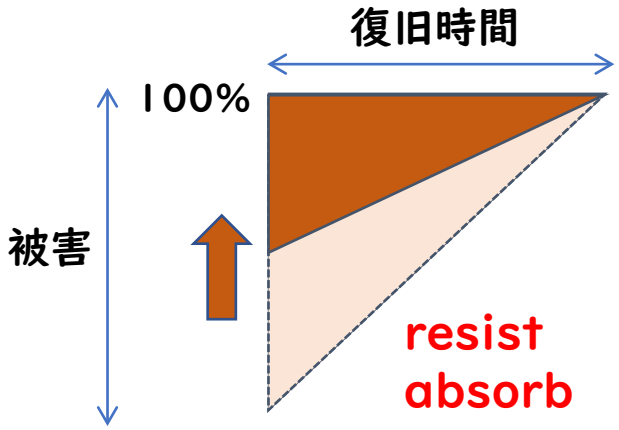
- 危機の発生は避けられないことを前提に、どのようにダメージと向き合うかを考える



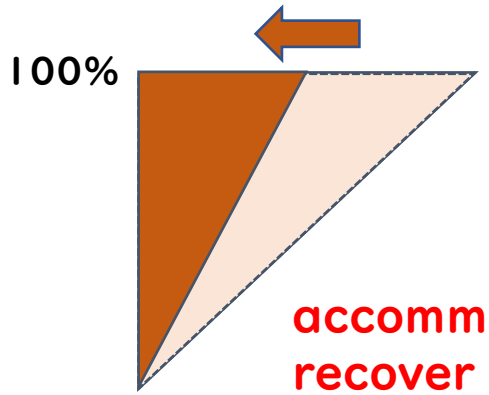
Resilienceの辞書的な意味：
The capacity to recover quickly from difficulties
（困難からすばやく回復する能力）

レジリエンス(Resilience)とは

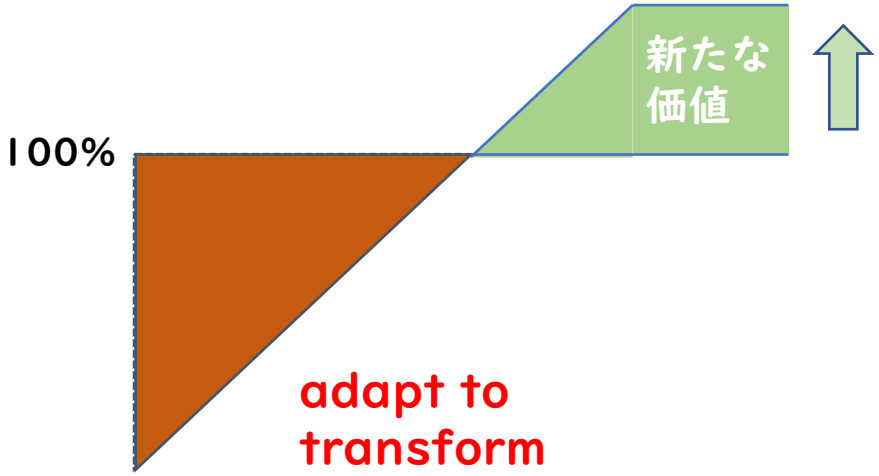
The ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, … (国連UNDRRによる定義)



被害を減らす
→変形を起こさない力
（吸収的対処能力）



復旧を早める
→素早く元に戻る力
（適応的能力）

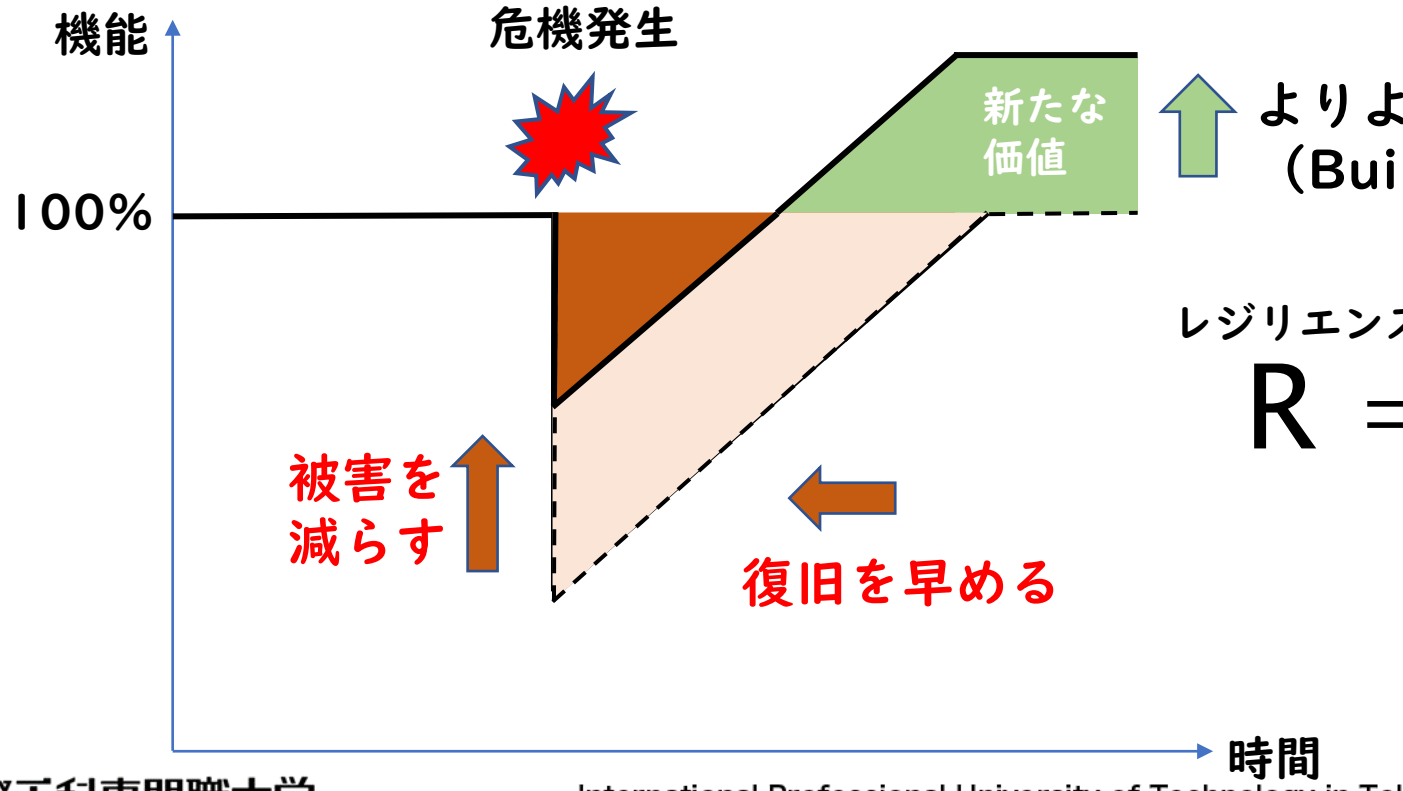


よりよい状態に変える
→Build Back Better
（変革的能力）

参考： しなやかな社会の実現 きたるべき国難の先に(日経BPコンサルティング)

レジリエンス(Resilience)とは

- 総合的な取り組みにより、しなやかに立ち直り、適応・変革を実現していく力



レジリエンス

$$R = f(D,A,T)$$

D: 被害
A: 人間活動
T: 時間

危機対応のポイント

- レジリエンスを高めるには、効果的な対応により被害を食い止め、素早く復旧することが重要
  - その体制がいわゆる「災害対策本部」や「危機管理本部」
  - 情報セキュリティにおいては「**CSIRT**」

- 対応の基本
  - 情報(data, information, intelligence)を正しく扱う
    - Disinformationに惑わされず、限られた情報から状況を把握する
  - 関係者と連携する
    - 単独で抱え込まず、関係者と状況認識を統一する
  - 先を見据えて判断、行動する
    - 様子見や先送りせず、対応計画もどんどんアップデートする

CSIRT (Computer Security Incident Response Team)

- 情報セキュリティインシデントの発生を前提とした対応チームまたは機能

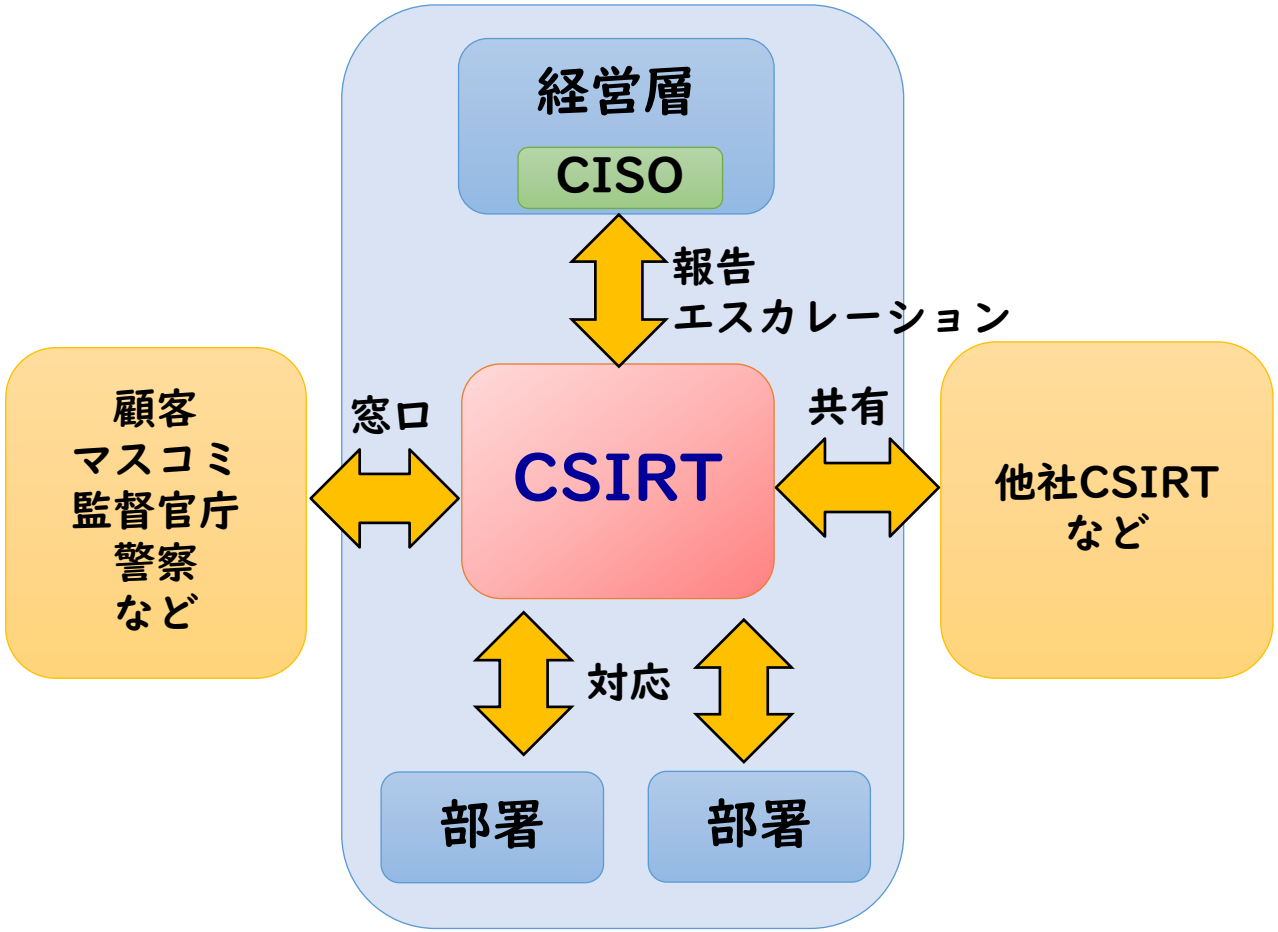
- 情報セキュリティインシデントの窓口
  - 対応に関する情報や経験が集まる場
  - セキュリティに関する外部との情報連携のハブ

- いわば、企業内の「情報セキュリティ消防団」
  - 必ずしも専任組織とは限らない

日本シーサート協議会資料より
https://www.nca.gr.jp/imgs/CSIRT.pdf

CSIRTの位置づけ

- インシデント事後対応
  - インシデントハンドリング
  - 報告・情報公開　など
- インシデント事前対応
  - 監視・検知、イベント分析
  - 脆弱性情報ハンドリング
  - 技術動向調査　など
- セキュリティ品質向上
  - リスク評価・分析
  - コンサル
  - 教育・啓発活動　など



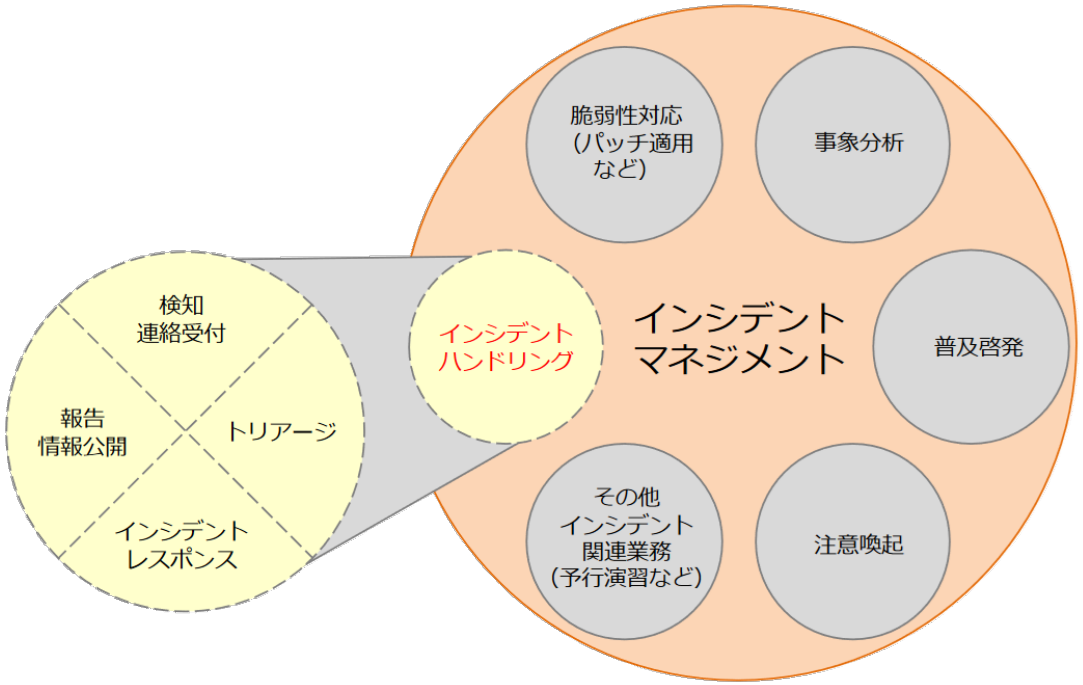
CSIRTとSOC

- **SOC** (Security Operation Center)
  - システム・ネットワークの状態を監視し、サイバー攻撃の検知や分析・対策を行うことで企業の情報資産を守るための組織
  - 常設部署として24時間365日体制でセキュリティ監視
    - サイバー攻撃の検知や分析
    - システム・ネットワークの状態を監視
    - ネットワーク機器やセキュリティ装置・サーバーの監視
    - ログ情報の解析や分析

https://www.gmo.jp/security/cybersecurity/soc/blog/soc-csirt/

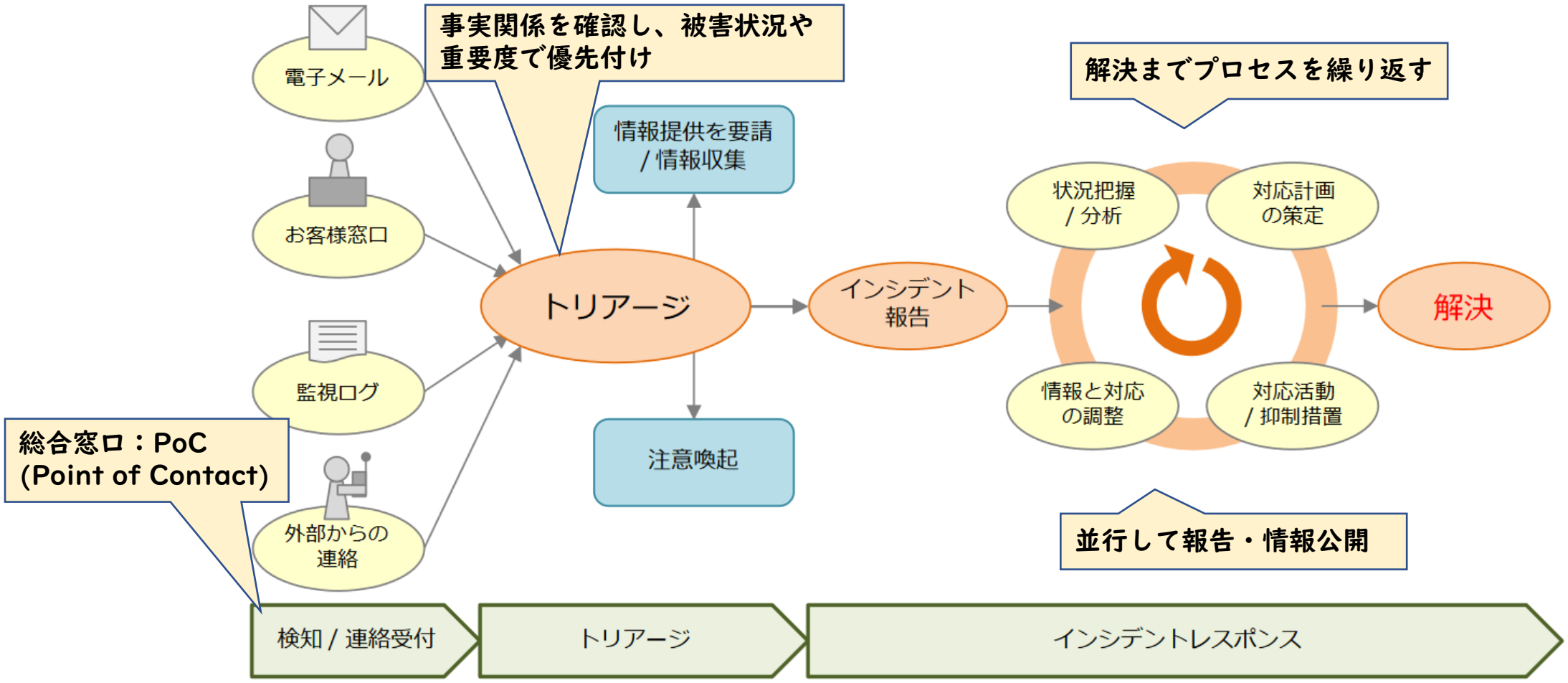
インシデントマネジメント

- **インシデントマネジメント**
  - インシデント全般に対して行う一連の業務
  - 事前、事後、平時対応も含む
- **インシデントハンドリング**
  - 実際に発生したインシデントに対して行う一連の業務
- **インシデントレスポンス**
  - インシデントに実際に対応する業務



https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20151126.pdf

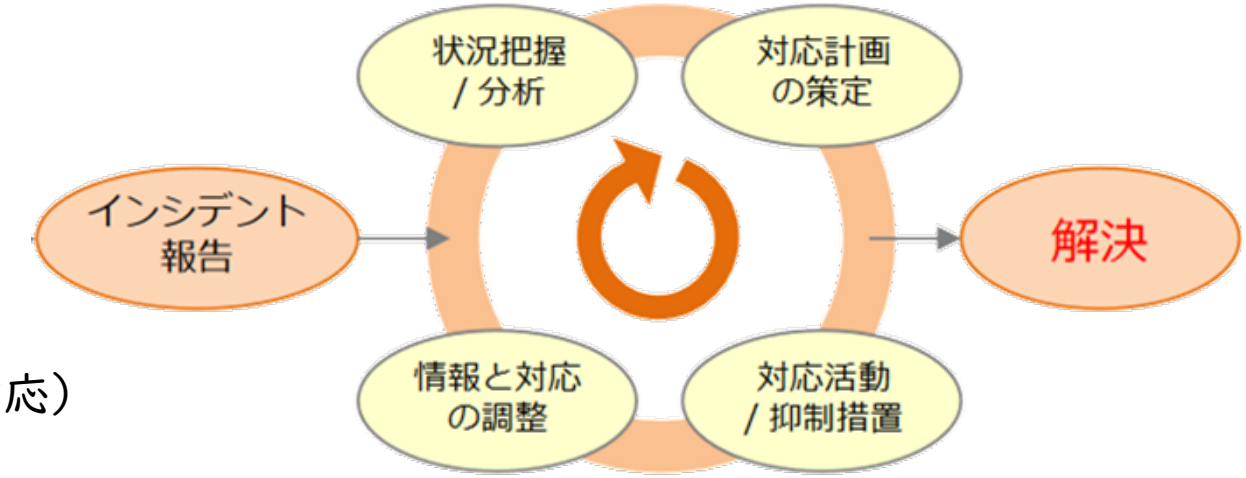
インシデントハンドリング



https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20151126.pdf

インシデントレスポンス

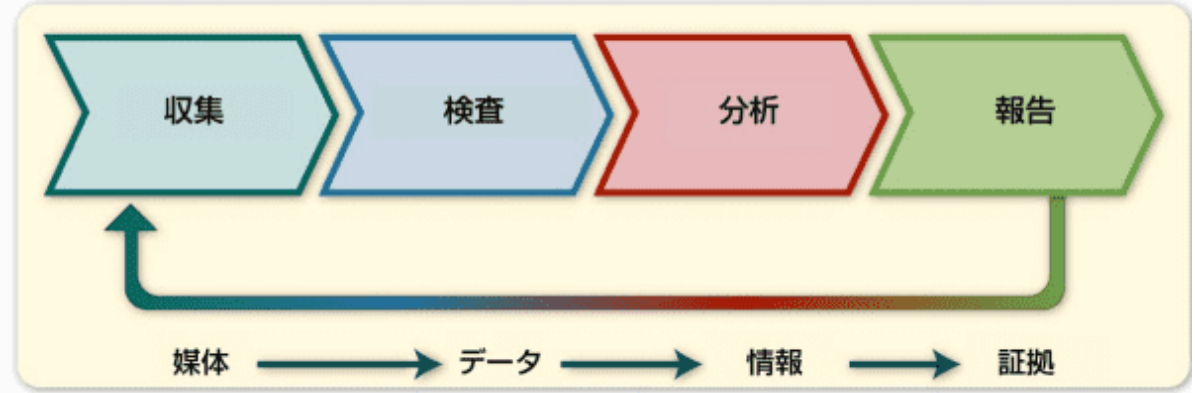
- トリアージ結果を受けて対応を実施
  - 状況把握/分析
    - 証拠保全（フォレンジック）
  - 対応計画策定
    - 方針の決定
  - 対応活動/抑制措置
    - 封じ込め、根絶に向けた作業
    - 復旧（暫定対応）、再発防止（恒久対応）
  - 情報と対応の調整
    - 他機関等との連携、人材支援、情報公開（広報）
  - **事後の振り返り**



https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20151126.pdf

証拠保全（フォレンジック）

- 一般には鑑識や法医学と言われるもの
- IT分野では電子機器から法的証拠や手がかりを探し出す取り組みの総称
- インシデントの原因究明や、訴訟に備えた証拠収集として実施
  - 復旧や初期化を試みるよりも前に、証拠保全をしっかり行うべし！

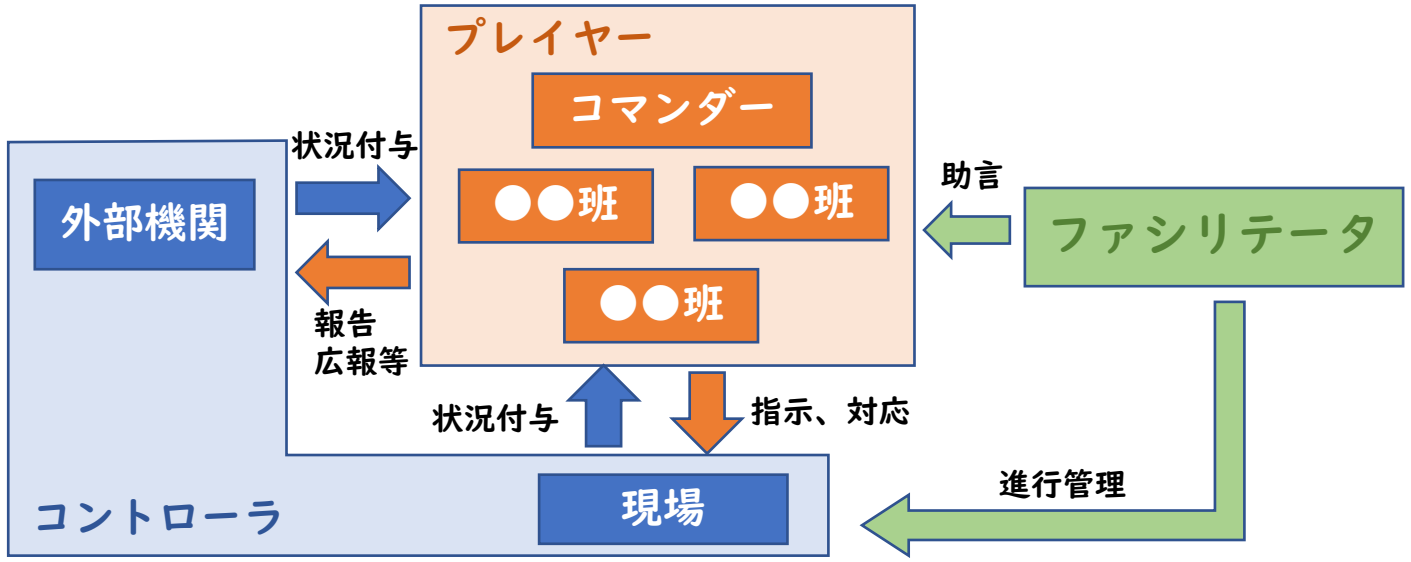


https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025351.pdf

主な保全対象：
・ネットワーク機器の各種ログ
・攻撃を受けた状態のPCやモバイル端末
（のメモリやSSDの内容）
・クラウド上のデータ　など

図上演習（図上訓練）

- 模擬的な状況を想定して机上で行う演習／訓練
- 与えられたストーリーに沿って演じるのではなく、刻々と変化する状況を付与していくことで具体的な災害／インシデントの状況をイメージさせ、対応や意思決定の力を鍛える



サイバー図上演習の例

https://www.youtube.com/watch?v=Cs3mCvAApeo

CSIRTに関する関連組織

- 日本シーサート協議会
  - https://www.nca.gr.jp/
  - CSIRT間の緊密な連携を図り、CSIRTにおける課題解決に貢献するための国内組織
- JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)
  - https://www.jpcert.or.jp/
  - 日本国内に関するインシデント対応の支援や助言などを技術的な立場から行う中立組織
- FIRST (Forum of Incident Response and Security Team)
  - https://www.first.org/
  - 世界中のCSIRTが相互の情報交換やインシデント対応に関する協力関係を構築する目的で設立されたフォーラム

(参考)CSIRTの参考情報

- CSIRT小説「側線」
  - https://www.itmedia.co.jp/enterprise/series/10244/
  - CSIRTでどういう人材がどんな活躍をするのかを連載小説仕立てにしたもの

- 百社百様、我が社のCSIRT
  - https://xtech.nikkei.com/it/atcl/column/16/080500167/
  - 実際の会社でどのようにCSIRTが作られ、運用されているかの事例集