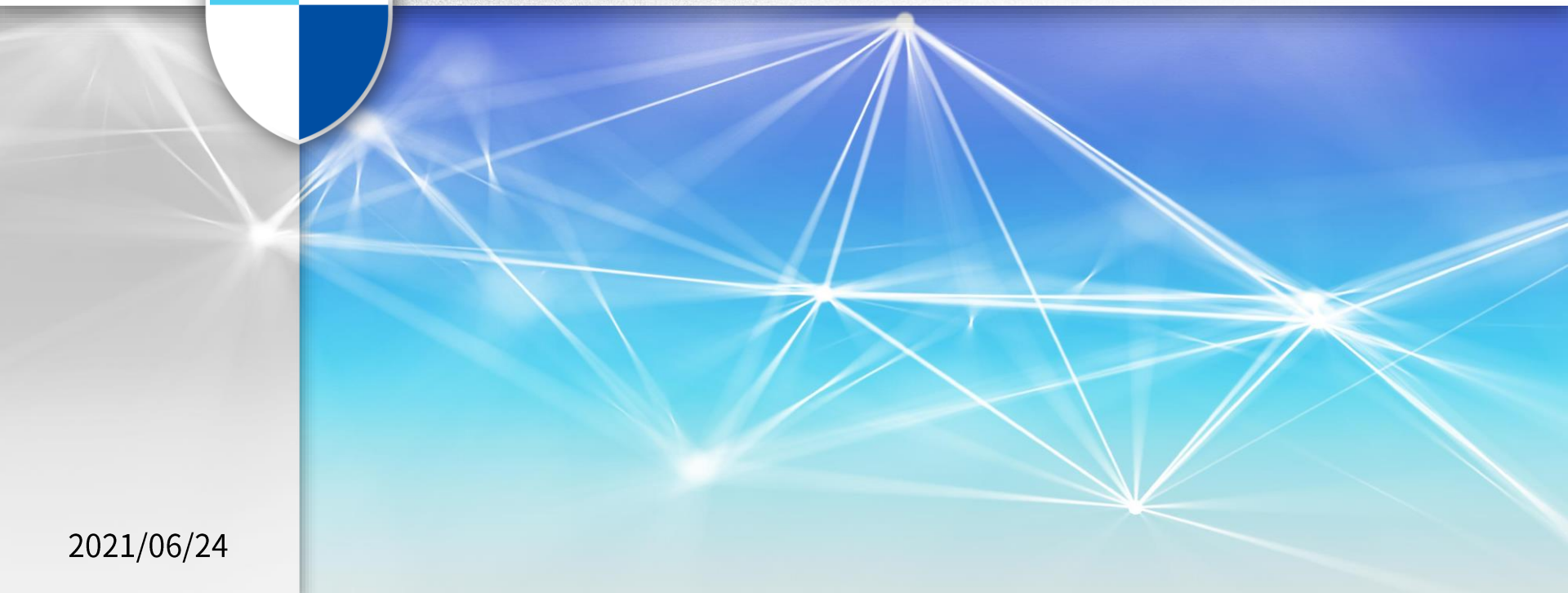
国立研究開発法人 情報通信研究機構
ナショナルサイバートレーニングセンター

2021情報通信月間講演会

【講演3】サイバーセキュリティを巡る最新動向
～実践的サイバー防御演習、ナショナルサイバートレーニングセンター紹介～

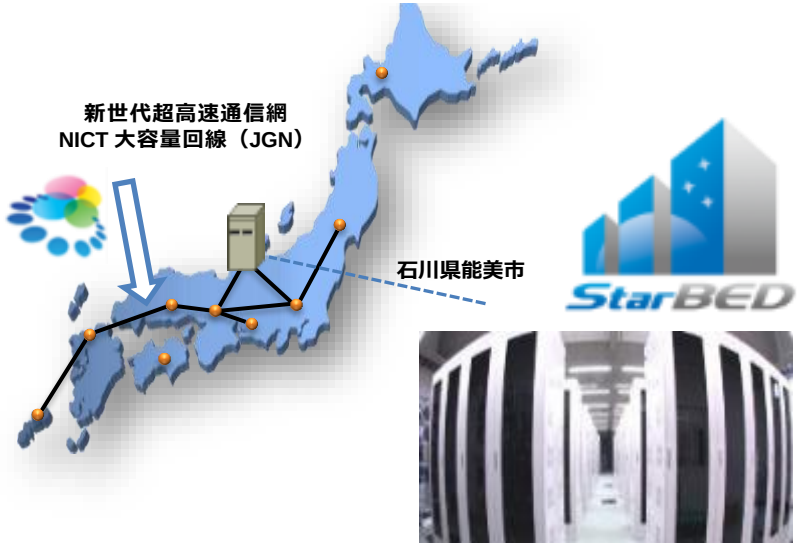
花田 智洋 (Tomohiro Hanada)



2021/06/24

国立研究開発法人 情報通信研究機構(NICT)

情報通信分野を専門とする我が国唯一の公的研究機関



自己紹介

- 氏名: 花田 智洋 (Tomohiro Hanada)
- 勤務先: 2017年1月～
  - NICTナショナルサイバートレーニングセンター(通称: ナショトレ)
  - 主任研究技術員
  - CYDER, RPCI, SecHack365, CYDERANGE開発等に携わる
- 前職: ～2016年12月末
  - 銀行システムのプロマネ
- 業務外活動:
  - 情報セキュリティコミュニティ運営

2021年の気になるイベント

東京2020大会

- 7/23-8/8 オリンピック競技大会
- 8/24-9/5 パラリンピック競技大会

9/1 デジタル庁発足予定

夏頃「サイバーセキュリティ戦略」に代わる新たな戦略の策定

-10/21 第49回衆議院議員総選挙

「地方公共団体における情報セキュリティポリシーに関するガイドライン」等の改定に関連した各種対応　等

沖縄関連

- 7月末 沖縄最大の木質バイオマス発電所が稼働予定　等

クイズ: この数字は何?

25,150,047人
88社、103件

2020年に
個人情報の漏えい・紛失事故を
公表した上場企業とその子会社

「上場企業の個人情報漏えい・紛失事故」調査（2020年） ： 東京商工リサーチ
https://www.tsr-net.co.jp/news/analysis/20210115_01.html

参考

キーワードで振り返る 2020年以降のセキュリティニュース

ランキング形式で振り返る 2020年以降のセキュリティニュース

	情報セキュリティ安心相談窓口の相談状況	情報セキュリティ10大脅威 2021		情報セキュリティ監査人が選ぶ2021年の情報セキュリティ十大トレンド	2020年セキュリティ十大ニュース
	2021年第1四半期（1月～3月）	個人	組織		
1	「ウイルス検出の偽警告」に関する相談	スマホ決済の不正利用	ランサムウェアによる被害	テレワークニーズに追いつかないセキュリティ対策	新型コロナウイルス感染症　七都府県に緊急事態宣言
2	「宅配便業者をかたる偽SMS」に関する相談	フィッシングによる個人情報等の詐取	標的型攻撃による機密情報の窃取	史上最悪の天災やパンデミックなどに対応できるIT-BCPへ	ドコモ口座サービスで不正利用発覚
3	「仮想通貨で金銭を要求する迷惑メール」に関する相談	ネット上の誹謗・中傷・デマ	テレワーク等のニューノーマルな働き方を狙った攻撃	止まらない、安全なクラウドサービスへ広がる要求	「デジタル庁」21年に設置へ
4	「iPhoneに突然表示される不審なカレンダー通知」に関する相談	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	サプライチェーンの弱点を悪用した攻撃	標的型攻撃の侵入パターンが多様化	東証システム障害で終日売買停止
5	「不正ログイン」に関する相談	クレジットカード情報の不正利用	ビジネスメール詐欺による金銭被害	頻発する大規模システム障害への対応	進化を続けるマルウェア「Emotet」の感染急増
6	「ワンクリック請求」に関する相談	インターネットバンキングの不正利用	内部不正による情報漏えい	在宅勤務のセキュリティ対策に求められる説明責任	防衛関連企業、不正アクセス事案の調査結果 を公開
7	「Emotet関連」に関する相談	インターネット上のサービスからの個人情報の窃取	予期せぬIT基盤の障害に伴う業務停止	手法の高度化が進む金銭目的のサイバー攻撃	GoTo利用し無断キャンセル 千葉のホテル、被害63万円分
8	「Facebookのメッセンジャーに届く動画」に関する相談	偽警告によるインターネット詐欺	インターネット上のサービスへの不正ログイン	在宅勤務者を踏み台にして組織を狙うフィッシング詐欺の横行	期待のISMAP運用開始
9	-	不正アプリによるスマートフォン利用者への被害	不注意による情報漏えい等の被害	EasyなネットサービスのEasyな拡大がなりすましの温床に	カプコン、標的型ランサムウェアで最大35万人の個人情報流出か
10	-	インターネット上のサービスへの不正ログイン	脆弱性対策情報の公開に伴う悪用増加	ニューノーマルに対応した新たな情報セキュリティ監査	経産省、IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）を策定
	情報セキュリティ安心相談窓口の相談状況［2021年第1四半期（1月～3月）］：IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/security/txt/2021/q1outline.html		情報セキュリティ10大脅威 2021：IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/security/vuln/10threats2021.html	監査人の警鐘- 2021年 情報セキュリティ十大トレンド	JASA (Japan Information Security Audit Association) https://www.jasa.jp/seminar/sec_trend2021/	NPO日本ネットワークセキュリティ協会 https://www.jnsa.org/active/news10/index.html
	2021/4/20		2021/1/27	2021/1/6	2020/12/25	

[Pick up]インシデント事例

VPN狙うサイバー攻撃で露見　既知の穴塞がぬ日本企業

2021年5月23日 2:00

日経XTECH 日経クロステック

セキュリティー対策機器大手の米フォーティネットの製品を巡り、脆弱性を突くサイバー攻撃が相次ぎ問題となっている。ただし、攻撃に使われたのは1年以上前に既知の脆弱性で、修正プログラムも提供済み。脆弱性対策のバージョンアップにさえも消極的な日本企業が、被害拡大の一因となる構図が浮き彫り

VPN狙うサイバー攻撃で露見　既知の穴塞がぬ日本企業: 日本経済新聞
https://www.nikkei.com/article/DGXZQOUC138DE0T10C21A5000000/

ランサムウェア

営業/プロジェクト管理
ストレージ権限/脆弱性
ウィルスチェックサービス
業務/個人用混同

重要インフラにサイバー攻撃　20年、世界で1.5倍の468件

2021年5月10日 15:00

Think! 多様な観点からニュースを考える

給油したくてもガソリンがない――。米国で起きた石油パイプラインへのサイバー攻撃は、こんな事態にもつながりかねないリスクを米国人に感じさせた。エネルギー供給網から工場や水道まで。経済や生活を支える重要インフラへのサイバー攻撃は急増

重要インフラにサイバー攻撃　20年、世界で1.5倍の468件: 日本経済新聞
https://www.nikkei.com/article/DGXZQOUC1923L0Z10C21A4000000/

サイバー攻撃はどこからやってくるのか？

攻撃経路例:

- メール
- USBメモリ
- Web, ドライブバイダウンロード
- 汚染ソフトウェア、アプリ
- 持ち込み機器、持ち出しPC
- リモートエクスプロイト
- クラウド　等

攻撃フェーズ

攻撃段階

攻撃例

- OSINT
- ソーシャルエンジニアリング
- 公開サーバーに対する調査

- メール
- Web, ドライブバイダウンロード
- (その他は攻撃経路例参照)

- 追加機能ダウンロード
- ソフトウェア設定変更
- 悪性コード注入

- バックドア(通信経路確保)
- 権限昇格
- 認証情報窃取

- 内部探索
- 挙動監視
- 機種・バージョン調査

- 横展開
- 機密情報収集、パッケージ化、暗号化
- 機密情報漏洩

C2:
C2(C&C)はCommand And Controlの略。攻撃者が感染した端末上のマルウェアに遠隔操作のための指令を送るサーバーのこと。
「C2サーバー」と呼ばれることもある。
OSINT:
オープン・ソース・インテリジェンス(Open Source INTelligence)の略。一般的に公開されている情報を収集する手法のこと。

クイズ: 正しいのはどれ？

わたしたちは

事実をありのままに見ているのか

あやまりがあっても理解できてしまうる能力

- ×：みさなん、こんちには
- ○：みなさん、こんにちは

知っている文字・単語だと思い込んでしまう

- 思い込み、勘違い、うっかり
- 過信、うぬぼれ、そんなつもりは無かった
- 情報過多、注意力散漫

どのように対峙するか

人的・組織的対策

- **計画**: インシデントレスポンスプランニング
- **対処**: インシデントハンドリング

技術的対策

- 事**前**対策
- 事**後**対策

人的・組織的対策: インシデントレスポンスプランニング

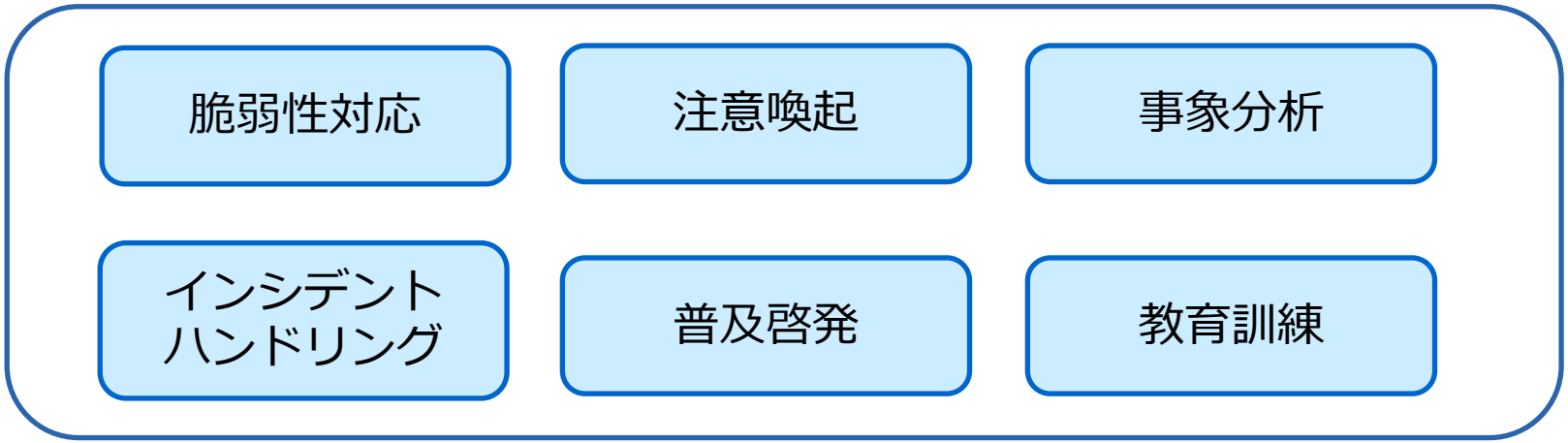
インシデント発生時に**確実**かつ**迅速**に
ハンドリングできるよう**計画を策定**する

参考 プランニングのプロセス

1. 参考文献調査、情報収集
2. (経営層からの)体制構築承認獲得
3. 組織内の現状把握及び関係部門との調整
4. CSIRT体制の設置及び簡易的な演習
5. CSIRT活動に係る文書作成と定期レビュー

インシデントマネジメント

「事前」の準備を含めたインシデントに対して行う一連の業務



インシデントハンドリング

インシデントマネジメント

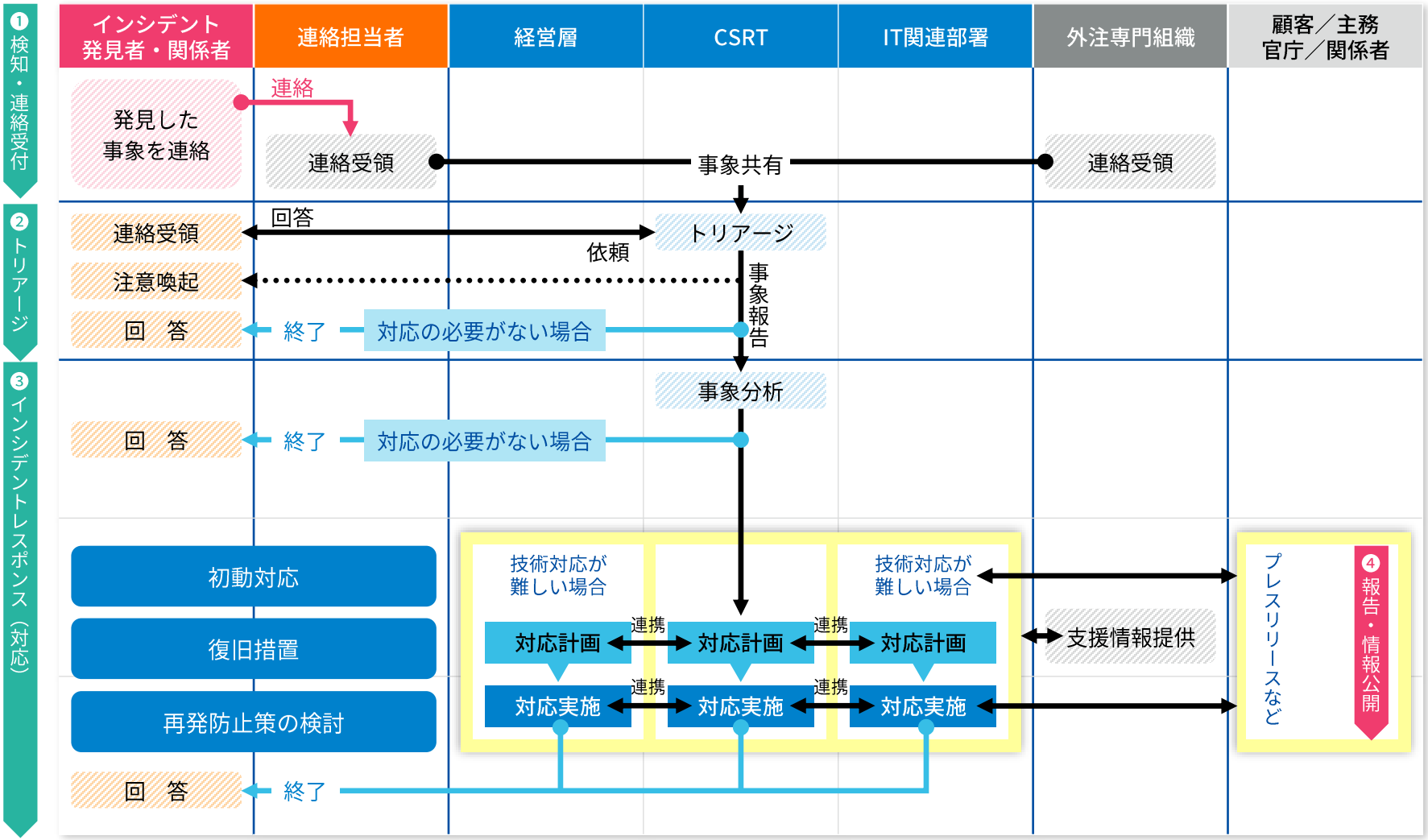
「事前」の準備を含めたインシデントに対して行う一連の業務

■インシデント発生から解決までの一連の業務

参考

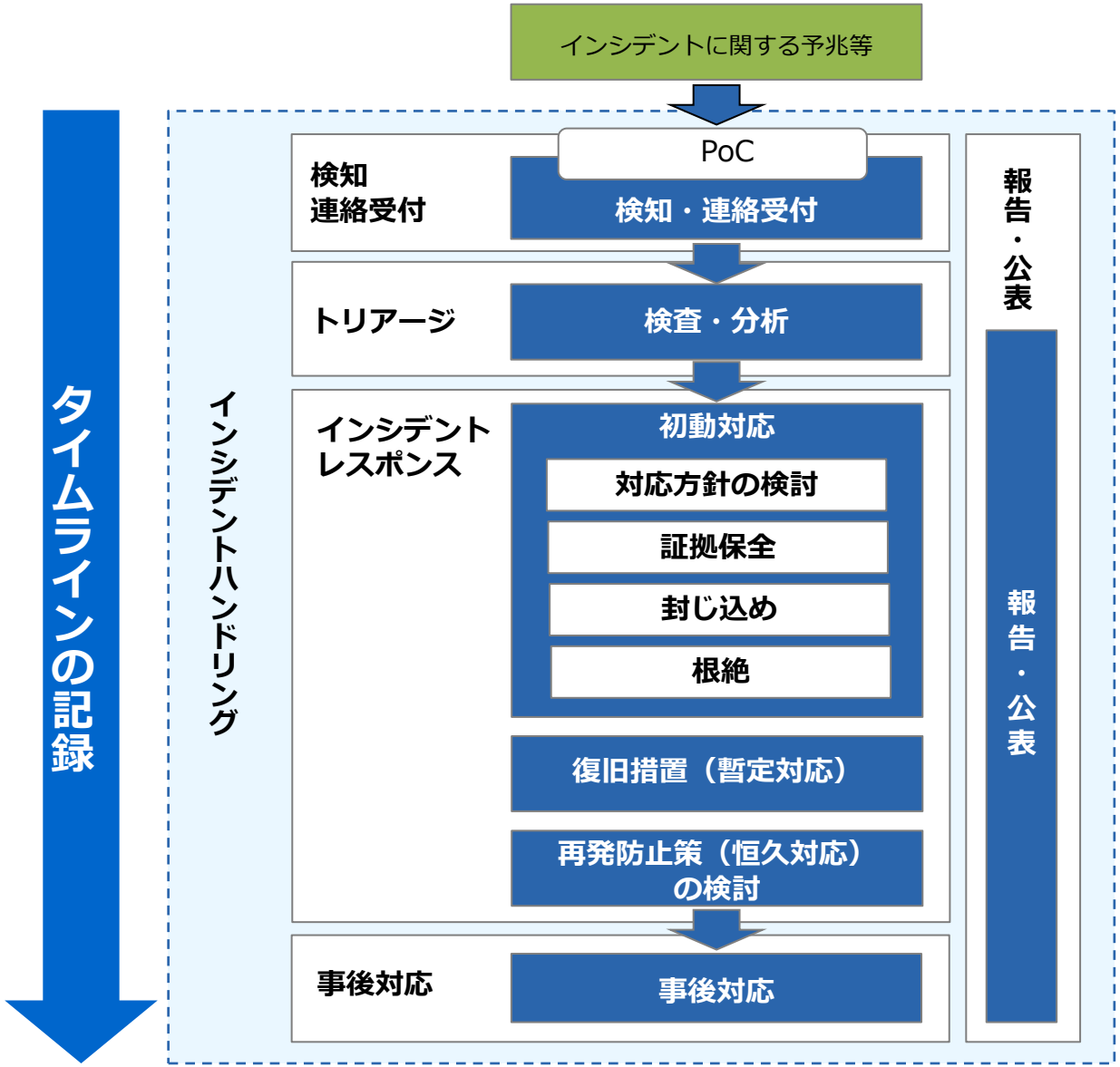
インシデントハンドリングの流れ

インシデントハンドリングのフロー例



参考

インシデントハンドリングの流れ



※実際のインシデントハンドリングにおいては、各組織のルールに則った対応をしてください。

技術的対策: 事前対策

- 被害を未然防止する
- 攻撃者の攻撃コストを高める
- 被害に遭いにくい環境を実現する

- 参考 代表的な事前対策
  - アプリケーションの利用制限(ホワイトリスト化)
  - セキュリティパッチ適用(OS, アプリケーション最新化)
  - 権限最小化(最小特権)
  - (定期的なバックアップ)

技術的対策: 事後対策

- 被害拡大の防止・抑制
- 証拠保全
- 被害全貌の把握

参考 事後(起きてしまった後)に実施すること

- トリアージ
- インシデントレスポンス
  - 初動対応
  - 復旧措置(暫定対応)
  - 再発防止策(恒久対応)の検討　等

原因分析(特定)の難しさ

- 技術的に追い詰める難しさ
- 証拠不足の難しさ
- 証拠保全に要する膨大な時間
- 影響範囲の見極めの難しさ

- さらに
  - サービス再開タイミング判断の難しさ
  - 利用者への説明構成の難しさ

ではどうすれば良いのか？

教育

訓練

人的・組織的対策: 教育訓練

インシデントマネジメント

教育訓練の例

- ワークショップ
- 机上演習
- 実機演習

- 正常時の状態把握
- 堅牢な運用管理体制
- 経営と現場の認識合わせ
- ギャップの洗い出し
- ヒヤリハット体験の共有

National Cyber Training Center

人材育成

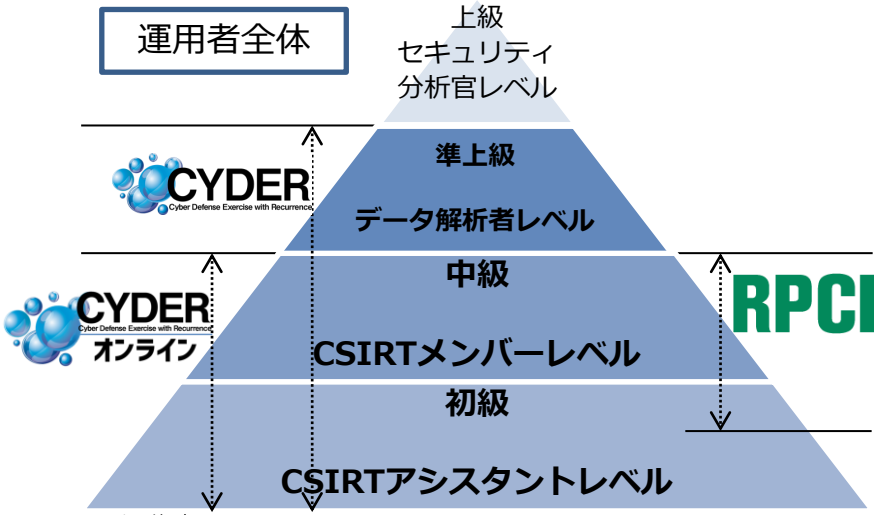
参考

「ナショナルサイバートレーニングセンター」の概要

情報通信分野を専門とする我が国唯一の公的研究機関である**NICTの技術的知見、研究成果、研究施設等を最大限に活用し、実践的なサイバートレーニングを企画・推進**

セキュリティオペレーター（実践的運用者）の育成

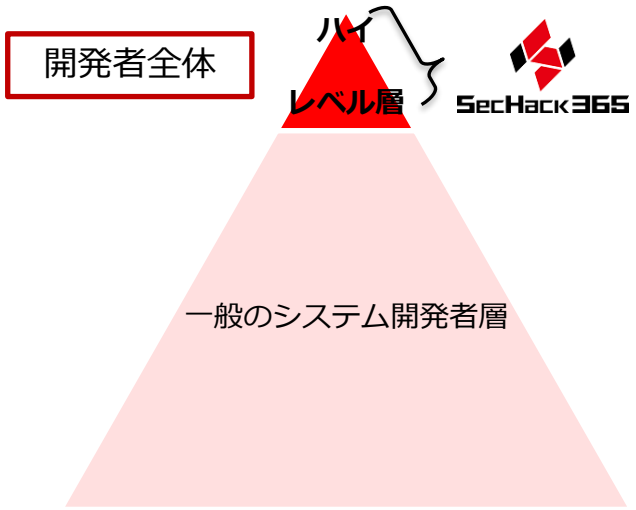
- **行政機関や民間企業等の組織内のセキュリティ運用者（情報システム担当者等）を対象**
- **所属組織が深刻なサイバー攻撃を受けた段階等（＝「有事」）における実践的なインシデント対応能力を育成**



シーサート
※CSIRT：Computer Security Incident Response Team

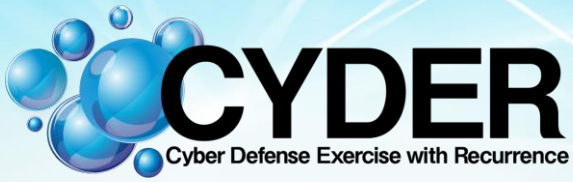
セキュリティイノベーター（革新的研究・開発者）の育成

- **セキュリティマインドを持ち、既存ツールを単に「ユーザー」として利用するだけではなく、革新的なセキュリティソフトウェア等を自ら「研究・開発」していくことができるハイレベルな人材を育成**



NICT National Institute of Information and Communications Technology

実践的サイバー防御演習
「CYDER」



たった1ページで分かる CYDER

Cyber Defense Exercise with Recurrence

初級、 中級、準上級、オンライン

- 最大4名のグループワーク、ハンズオン　等

演習環境CYDERANGE

- 1グループに1仮想組織環境
- 各種操作記録機能
- シナリオ自動生成用機能
- **NICTの強み① 大規模計算機環境＆StarBED**

そのときどきの旬なシナリオの提供

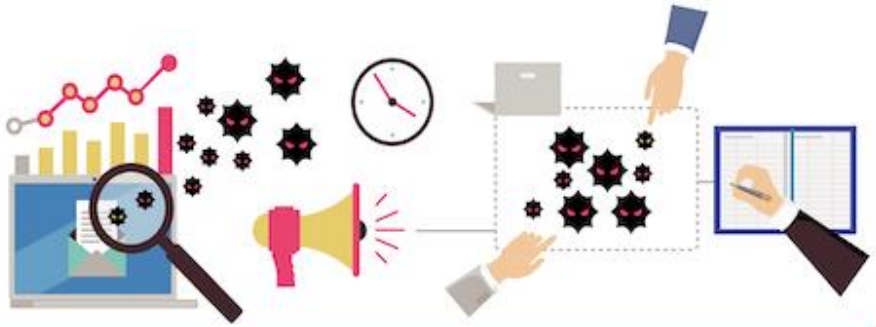
- **NICTの強み② 研究実績と攻撃観測データの蓄積**

CYDER演習内容

Aコース：初心者向け
Bコース：コンピュータやネットワーク、サイバーセキュリティに関する基礎知識を既にお持ちの方

「事前オンライン学習」と「集合演習（ハンズオン&グループワーク）」により、座学のみで終わらない本格的なトレーニングを受けることができます。

事前オンライン学習により攻撃手法や対策技術に対する理解を深め、集合演習（ハンズオン＆グループワーク）を通じて、グループによる一連のインシデントハンドリング（セキュリティ事故への対応）を体験することにより、インシデントレスポンスの手法はもとより、組織で役立つセキュリティポリシー（セキュリティ対応方針）、コミュニケーションの重要性を学びます。



事前オンライン学習
標準学習時間 1時間程度

最近のサイバー攻撃の傾向や対策を理解し、集合演習に必要なインシデントハンドリングの心得について学びます。

集合演習
1日間/回（例）10:00～18:00

ハンズオン
端末を用いて、インシデントの検知・報告・影響範囲の特定・隔離、分析・解析、被害状況の確認等を行い、技術的な知識を身につけます。

グループワーク
役割を決め、演習を行うことによって、セキュリティポリシーやインシデントレスポンスの手順などさまざまな気づきの共有を行い、学びを深めます。

参考

事前オンライン学習 サンプル1

第４章　実機演習に必要な知識（使用するツールの紹介）

（標準学習時間：25分）

第４章では、実機演習で必要な知識、使用するツール、使用方法等について紹介します。集合演習当日に利用するツールのためしっかり学んでおきましょう。これからご紹介するソフトウェアは全てフリーです。可能であればソフトウェアをインストールし、触れてみると理解が深まります。

4.1　リモート接続
Windows端末からリモートのLinux端末やWindows端末へアクセスするツールや、ファイルの送受信するツールを学習します。

4.2　メールヘッダ解析
メールヘッダの見方やメールヘッダの詐称の可能性を解説し、不正なメールの見分け方を学習します。

4.3　SPFレコード調査
メールの送信ドメイン認証であるSPFレコードを確認することでメールが詐称されていないことの確認方法を学習します。

4.4　DNS通信ログと出力設定
DNSプロトコルで通信するマルウェアの調査を前提にログ出力の設定方法とログの見方を学習します。

4.5　IOC Finderを使った感染調査
IOCを利用してサイバー攻撃の調査方法の紹介とツールの使い方を学習します。

次ページへ進んで、学習を開始してください。

参考

事前オンライン学習 サンプル2

参考1.1 最近のセキュリティ事件・事故

日本語のランサムウェアの登場で国内での被害が増加しています。また、ワナクライのように、ワームとして感染拡大できるランサムウェアが出現し、組織への被害が深刻な事例も増えています。

多様化する脅威　～攻撃の傾向（その２）～

ランサムウェアの被害が増加中

- PC内のファイルの暗号化や、スマートフォンの画面のロックを行い、その復元に身代金を要求
- 検出件数が増加、日本語表記のものも確認されており被害が拡大
- Webサイトの脆弱性等を悪用してランサムウェアに感染させるケースが増加中
- 「WannaCrypt(WannaCry、WannaCryptor、Wcry)」（通称：ワナクライ）のように、ワームとして感染拡大する事例が確認された
- 感染したPCだけではなく、共有サーバ等のファイルが暗号化されることも

参考：ランサムウェア「WannaCry(WannaCryptor)」画面

定期的なバックアップと脆弱性対策が重要

CYDER演習内容

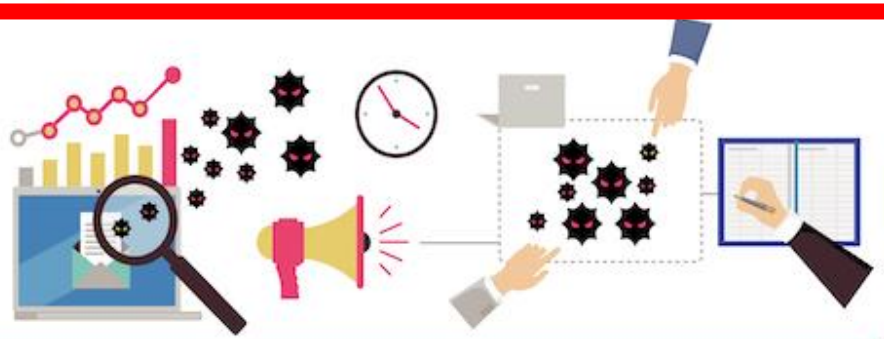
Aコース：初心者向け
Bコース：コンピュータやネットワーク、サイバーセキュリティに関する基礎知識を既にお持ちの方

「事前オンライン学習」と「集合演習（ハンズオン&グループワーク）」により、座学のみで終わらない本格的なトレーニングを受けることができます。

事前オンライン学習により攻撃手法や対策技術に対する理解を深め、集合演習（ハンズオン＆グループワーク）を通じて、グループによる一連のインシデントハンドリング（セキュリティ事故への対応）を体験することにより、インシデントレスポンスの手法はもとより、組織で役立つセキュリティポリシー（セキュリティ対応方針）、コミュニケーションの重要性を学びます。

事前オンライン学習
標準学習時間 1時間程度

最近のサイバー攻撃の傾向や対策を理解し、集合演習に必要なインシデントハンドリングの心得について学びます。



集合演習
1日間/回（例）10:00～18:00

ハンズオン
端末を用いて、インシデントの検知・報告・影響範囲の特定・隔離、分析・解析、被害状況の確認等を行い、技術的な知識を身につけます。

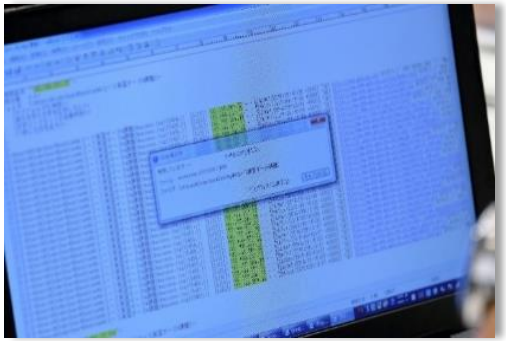
グループワーク
役割を決め、演習を行うことによって、セキュリティポリシーやインシデントレスポンスの手順などさまざまな気づきの共有を行い、学びを深めます。

CYDER演習風景: Aコース（2019年度）

オリエンテーション

演習フロー説明

インシデント発生～事実確認



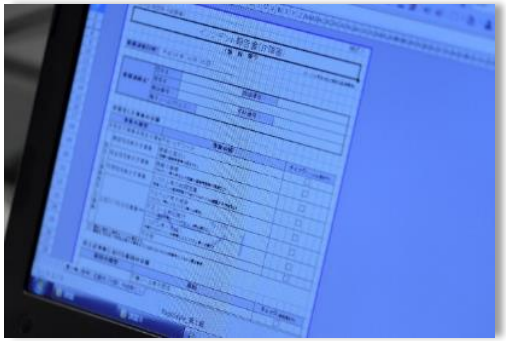
チューターによるサポート

マルウェア挙動調査

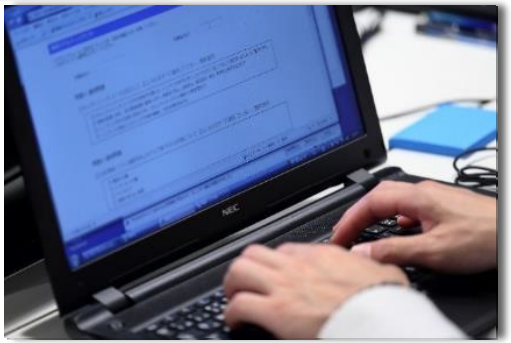
グループワーク

発表

報告書作成



確認テスト



集合演習の流れ

インシデント発生から解決、事後対応までを体験

Flow 1

― 検知・連絡受付

パソコンやサーバーなどの不審な動作を検知。組織内外からの通報を受け付けます。

Flow 2

― トリアージ（優先順位付け）

セキュリティインシデントが疑われる事象に対して、情報収集やログ調査などを行い、事実関係を確認します。インシデントと判断した場合には、被害状況を把握した上で重要度によって対応に優先順位を付けていきます。

Flow 3

― インシデントレスポンス（対応）

組織として、どのように対応すべきか、外部に協力を求める必要があるかなどを検討します。「証拠保全」「封じ込め」「根絶」「復旧措置（暫定対応）」を行います。

Flow 4

― 報告・公表

被害の度合いや影響を及ぼしている範囲に応じて、報告・公表します。組織内部への報告に加えて、被害者、監督官庁や警察機関などの外部関係者にも併せて報告します。

Flow 5

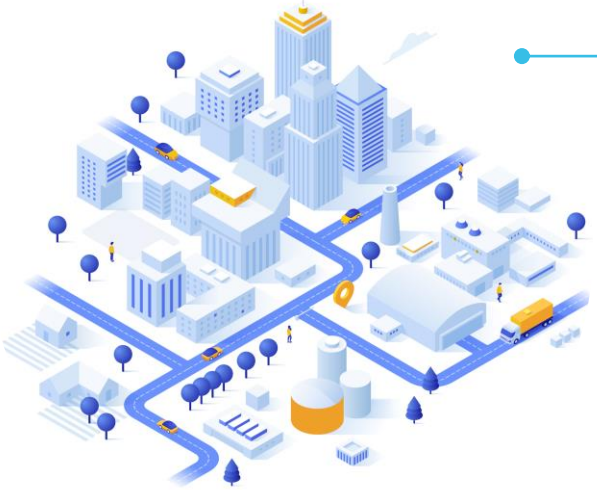
― 事後対応

インシデントに関わったすべての関係者が参加して「振り返り」を実施します。同様のインシデントを防ぐための今後の対応などを含め、最終報告書に取りまとめます。

Aコース	Bコース
説明	実習
実習	
解説	
説明	実習
実習	
解説	
説明	実習
実習	
解説	
説明	実習
実習	
解説	
	全体解説

参考

集合演習舞台設定例



みなさんは「さいだ市」の職員です。

みなさんは「さいだ市」の職員で、組織内の情報システムネットワークを管理する総務部情報管理課に所属しています。情報システムを扱う部署としてネットワーク運用、保守はもとより、CSIRTとして組織内で発生したセキュリティインシデントに対応するミッションを持っています。

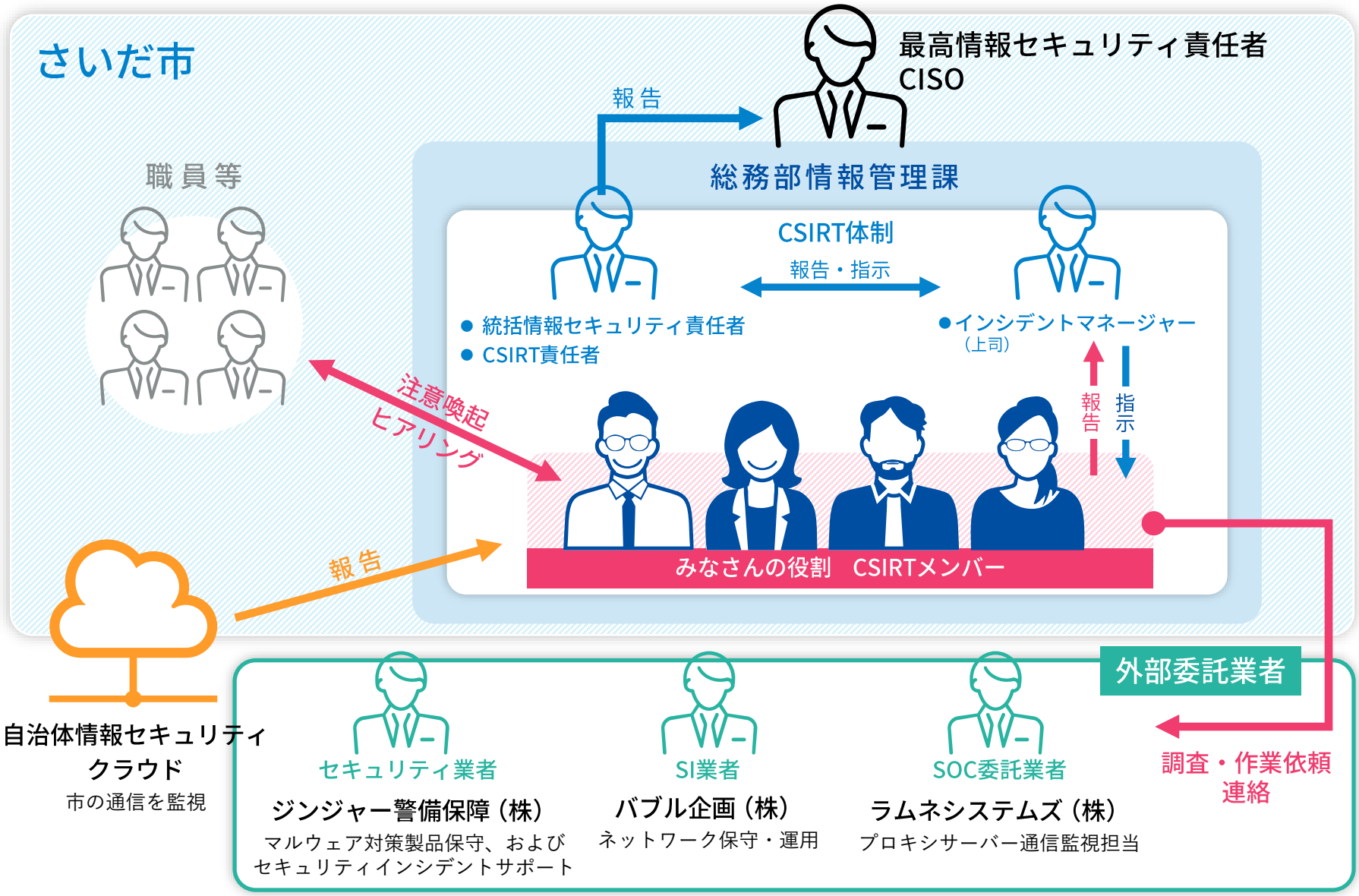
さいだ市データ

面積：84.87 km^2　人口：168,245 人

- 県北部に位置し、県庁所在地から北東約40kmに位置し、中心地域は県北部の中心都市としての性格を有している。
- 総務省のインターネット分離に関するガイドラインを受け、内部ネットワークをより強固にするために、自治体情報システム強靭性向上モデルに基づく組織内ネットワークの3分割および適切な強靭化の施策は完了している。
- 昨年度、調達を実施。県内有数のSI業者であるバブル企画（株）によってネットワークの3分割は実現された。また更なる強靭化を図るため、端末からの情報持ち出し対策、二要素認証などを検討中で、来年度には実現する予定である。なお職員が利用する端末は、インターネット接続系およびLGWAN接続系ともに、現時点は全台物理端末を利用している。
- 自治体情報セキュリティクラウドについては、県側と連携しながら利用中である。

参考

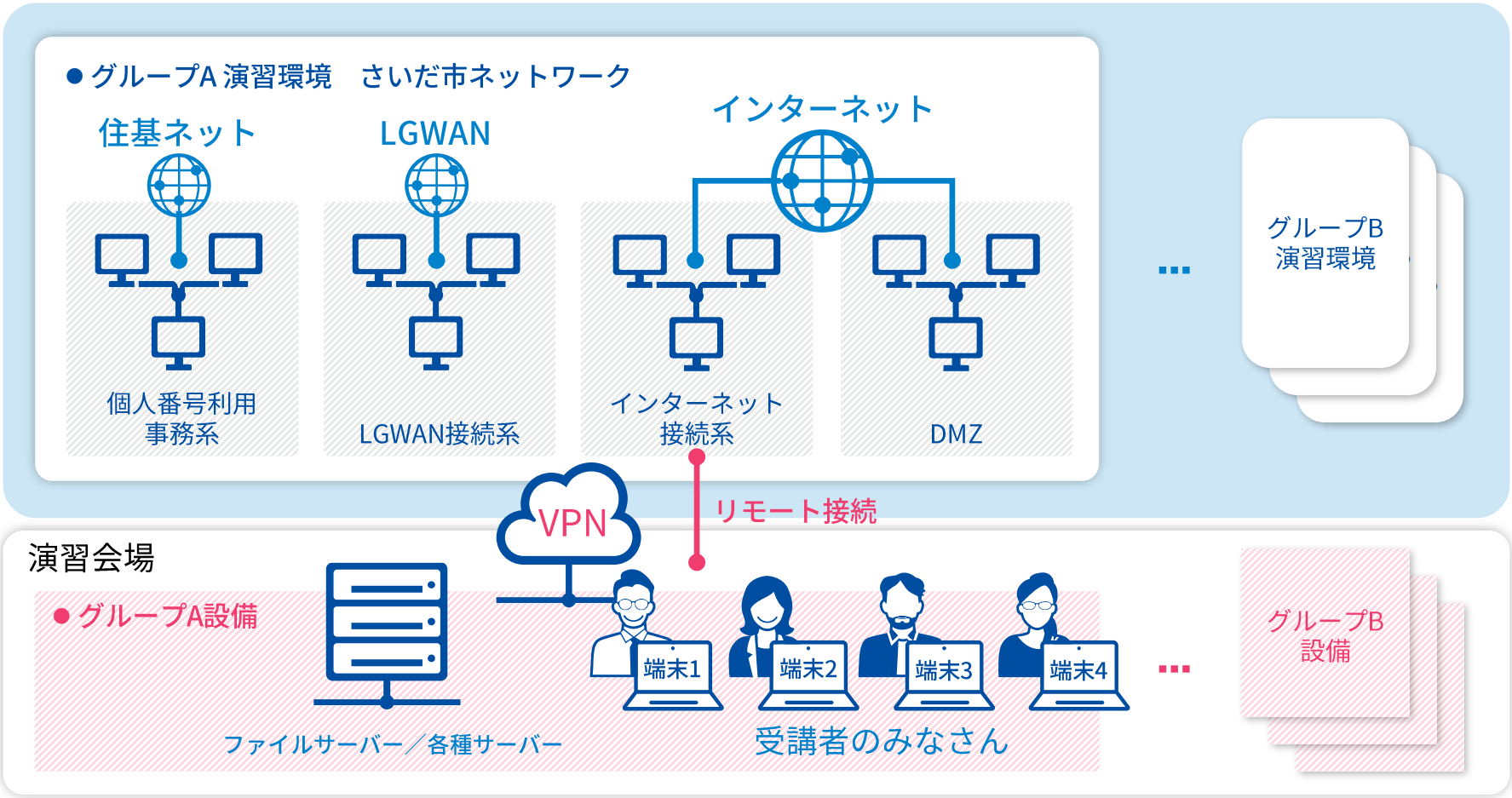
登場人物相関: B-1コースの例



各グループそれぞれに提供するネットワーク構成例

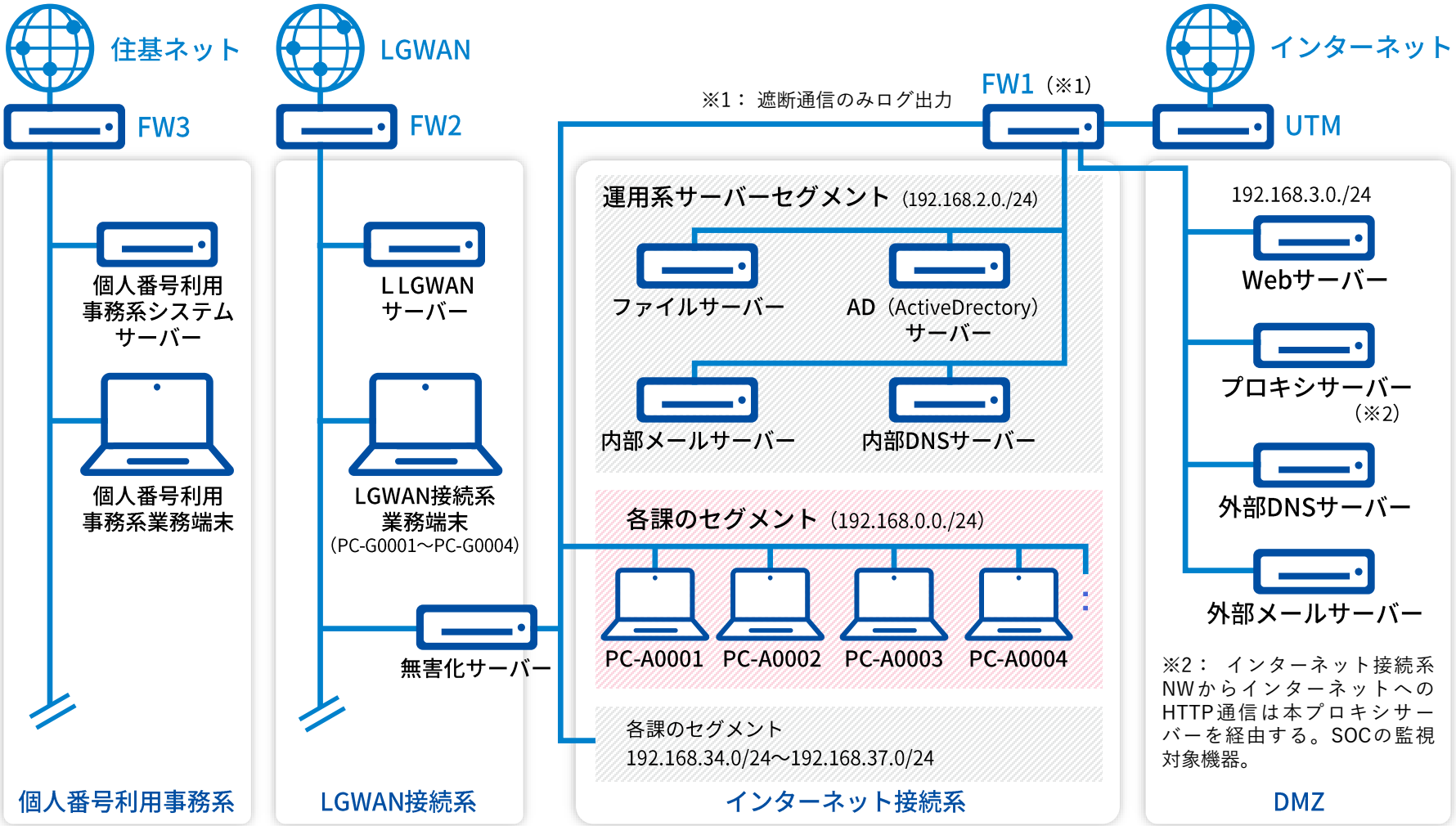
演習環境［StarBED］

※StarBED：NICTが構築した、大規模なシミュレーションを実施できる計算機群です。本演習では、さいだ市のネットワークをシミュレーションし、演習環境として利用しています。



参考

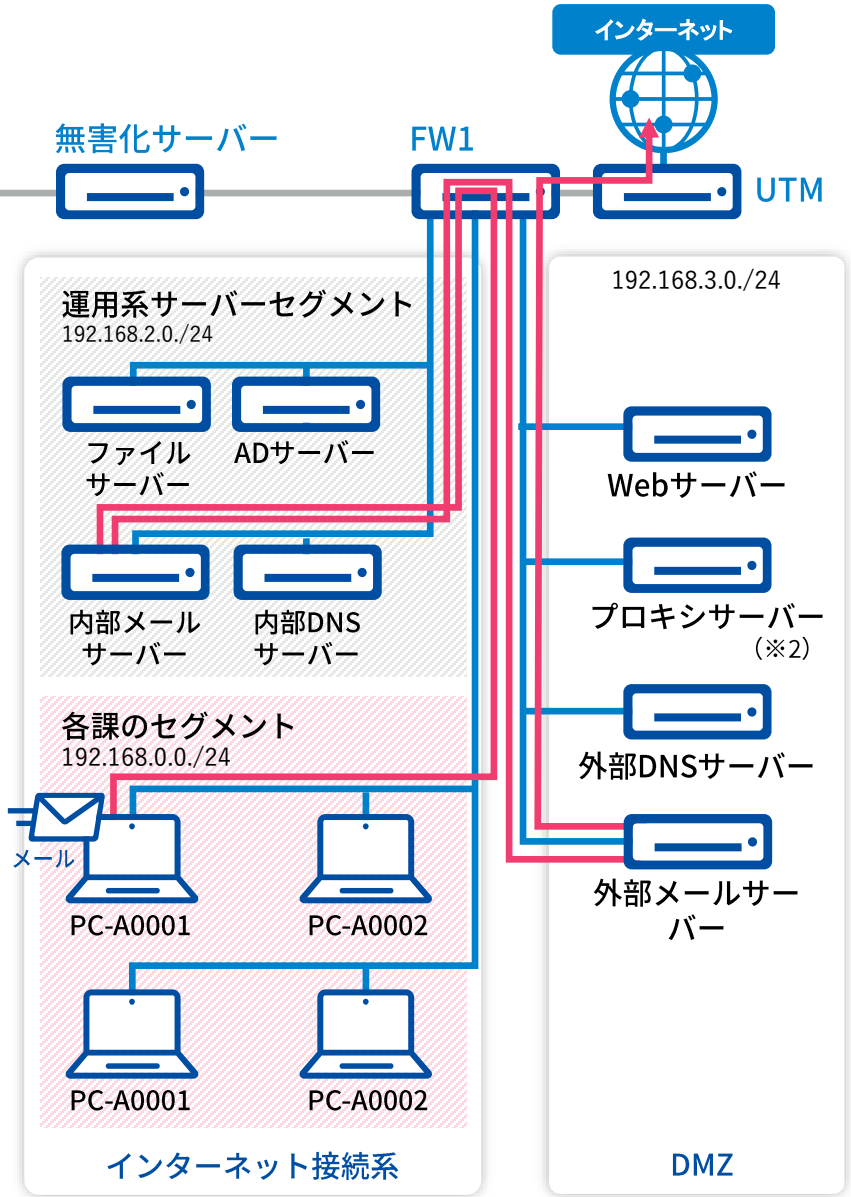
演習環境例


住基ネット
FW3
個人番号利用
事務系システム
サーバー
個人番号利用
事務系業務端末
個人番号利用事務系
LGWAN
FW2
L LGWAN
サーバー
LGWAN接続系
業務端末
(PC-G0001～PC-G0004)
無害化サーバー
LGWAN接続系
※1： 遮断通信のみログ出力
FW1（※1）
運用系サーバーセグメント（192.168.2.0./24）
ファイルサーバー
AD（ActiveDrectory）
サーバー
内部メールサーバー
内部DNSサーバー
各課のセグメント（192.168.0.0./24）
PC-A0001
PC-A0002
PC-A0003
PC-A0004
各課のセグメント
192.168.34.0/24～192.168.37.0/24
インターネット接続系
インターネット
UTM
192.168.3.0./24
Webサーバー
プロキシサーバー
（※2）
外部DNSサーバー
外部メールサーバー
※2： インターネット接続系NWからインターネットへのHTTP通信は本プロキシサーバーを経由する。SOCの監視対象機器。
DMZ

参考

リアリティのある演習環境をご提供

外部 / 内部 メールサーバー	ネットワークを通じた電子メールの送受信を管理するサーバー。 ※さいだ市では、外部メールサーバーを経由して送受信します。組織内のメールは内部サーバーで送受信します。
外部 / 内部DNS サーバー	ネットワーク上におけるドメイン名とIPアドレスの対応関係を管理するためのサーバー。 ※さいだ市では、端末から名前解決する際、内部DNSサーバーに問い合わせます。
プロキシサーバー	クライアント端末の代わりにWebサーバーなどに代理でアクセスするサーバー。取得したWebコンテンツをキャッシュすることによってアクセスを高速化する。 ※さいだ市では、インターネット接続系NWからインターネットへのHTTP通信は本プロキシサーバーを経由します。
ADサーバー	「ActiveDirectory」の略。同一のドメイン内にある端末や機器を一括管理するWindowsサーバー。さいだ市内のユーザーやリソース、セキュリティポリシーなどを一括管理している。
無害化 サーバー	メールの本文やメールに添付されているファイルに含まれるマルウェアなどの不正なアプリケーションを無害化するサーバー。



継続的な教育訓練の必要性

インシデントハンドリングはさまざま。

絶対的な正解はない

[次ページ参照]

- 共通要素はあるが部分的に違うシナリオを体験
- 共通要素の洗練
- 「想定内」の想定範囲が広くなれば、多少のことでは慌てなくなる

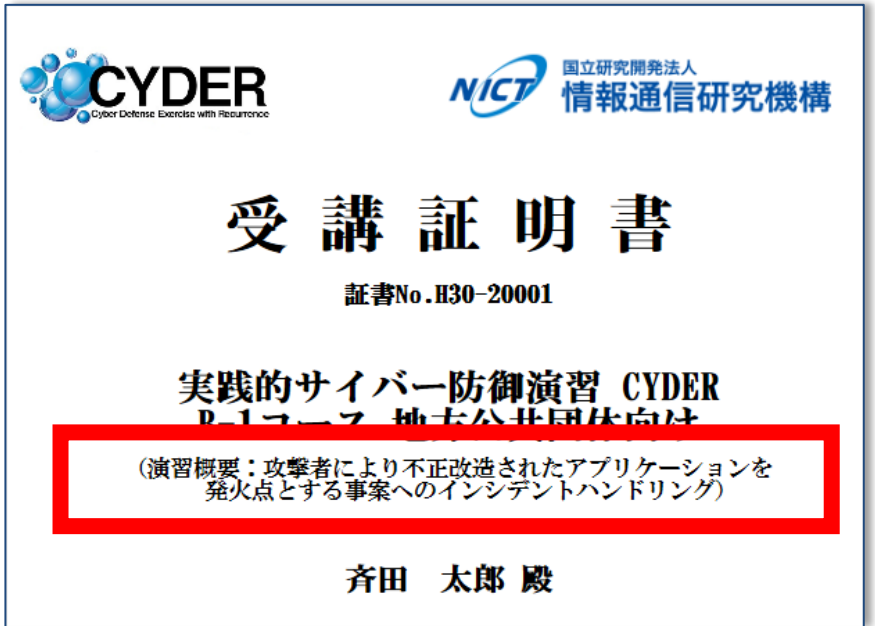
繰り返し、違うシナリオを体験

共通要素はあるが部分的に違うシナリオを体験

- 個別要素の意味や効果、影響を見極める力
- 必要な要素を想起できるようになる

共通要素の洗練

「想定内」の想定範囲が広くなれば、多少のことでは慌てなくなる


CYDER
Cyber Defense Exercise with Recurrence

国立研究開発法人
NICT 情報通信研究機構

受 講 証 明 書

証書No.H30-20001

実践的サイバー防御演習 CYDER

（演習概要：攻撃者により不正改造されたアプリケーションを
発火点とする事案へのインシデントハンドリング）

斉田　太郎 殿

セッションのまとめ

2021年の気になるイベント

2020年以降のセキュリティニュース

サイバー攻撃の理解

インシデントとの対峙

申し込み開始時期が異なるためご注意ください

■ A, B-1, B-2コース
- 7~9月の実施分：　現在申込受付中
- 10月以降の実施分：　8月中旬より申込受付開始

※Aコース@沖縄10/29, B-1コース@沖縄2/4

■ Cコース
- [予定]11月中旬より申込受付開始

■ オンラインAコース
- [予定]9月中旬より申込受付開始

実践的サイバー防御演習CYDER のご紹介

参考

インシデント対応時のマニュアル・チェックリスト(入門)

- **情報漏えい発生時の対応ポイント集　第3版（IPA）**
  - インシデント対応の内容が記載されています。絵が多く見やすく構成されています。
  - https://www.ipa.go.jp/security/awareness/johorouei/

- **中小企業向けサイバーセキュリティ対策の極意ガイドブック（東京都）**
  - サイバー攻撃に関する情報や、攻撃に対する対応方法などがマンガ形式として描かれています。サイバー攻撃への対処方法などを楽しく学ぶことができる内容です。
  - https://cybersecurity-tokyo.jp/security/guidebook/index.html

参考

インシデント対応時のマニュアル・チェックリスト(中級)

- **インシデントハンドリングマニュアル（JPCERT/CC）**
  - インシデントハンドリングの対応フローや各フェーズでの対応方法についての記載があり、インシデントハンドリングのマニュアルづくりに参考となる資料です。
  - https://www.jpcert.or.jp/csirt_material/operation_phase.html
- **サイバー攻撃（標的型攻撃）対策防御モデルの解説（総務省）**
  - インシデントハンドリングの対応情報が記載されています。さらに、チェックすべきログ情報や対処内容などがリスト化されている資料が、別冊として用意されています。
  - https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000125.html
- **情報セキュリティ事故対応ガイドブック（情報セキュリティ大学院大学）**
  - 中・小規模の組織向けのインシデント対応ガイドブックです。インシデントに対する準備やインシデントの対応フローなどが記載されています。
  - http://lab.iisec.ac.jp/~hiromatsu_lab/sub07.html
- **組織対応力ベンチマークシート（一般社団法人オープンガバメント・コンソーシアム）**
  - 事前準備やインシデント対応に関する内容がチェックシート形式で記載されています。
  - https://ogc.or.jp/article/1525
- **セキュリティ対応組織の教科書　v2.1（日本セキュリティオペレーション事業者協議会）**
  - インシデントに対する準備やインシデントの対応フローなどが記載されています。人材育成を観点とした内容も含まれています。
  - https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html
- **証拠保全ガイドライン　第8版（デジタル・フォレンジック研究会）**
  - インシデントに関わる証拠保全の内容が記載されています。証拠保全で使用されるツールの一覧なども記載されています。
  - https://digitalforensic.jp/home/act/products/home-act-products-df-guideline-8th/
- **Incident Handler's Handbook（SANS）**
  - インシデントハンドラーのハンドブックです。フェーズごとの対応内容についてのチェックリストが記載されています。WindowsとUNIXのコマンドに関する内容も資料に含まれています。
  - 英語の資料です。
  - https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

参考

インシデント対応時のマニュアル・チェックリスト(上級)

- **コンピュータセキュリティインシデント対応ガイド**
  米国立標準技術研究所による勧告（IPA）
  - インシデントハンドリングに関するガイドラインです。
    技術的な部分も含めて、非常に詳細な情報が記載されています。
    NIST（800-61）の資料の翻訳版です。
  - https://www.ipa.go.jp/security/publications/nist/

- **インシデント対応へのフォレンジック技法の統合に関するガイド**
  米国国立標準技術研究所による勧告（IPA）
  - インシデントに関わるデジタルフォレンジックの内容が記載されています。技術的な内容が多く含まれています。
    NIST（800-86）の資料の翻訳版です。
  - https://www.ipa.go.jp/security/publications/nist/

参考

テレワーク環境のリスクと対策

テレワーク固有のリスクを理解した適切な対応

新型コロナ対応で、十分な準備もできないままリモートワークを実施する組織も多いようです。テレワーク固有のリスクを理解して適切な対応を行う必要があります。

テレワークに関連する事故例

- 大学のリモート授業時に配信したメッセージに、学生の個人情報を誤って添付
- 高校教諭がテレワークのために生徒の個人情報を保存したUSBメモリを紛失
- IT企業が、トラフィック増大等によって障害が多発したため リモートアクセスサービスを終了
- 通信事業者が、リモートアクセスを利用したBYOD端末を経由して VDIサーバーへ不正アクセスを受け、内部情報が流出

テレワークのリスク

- 宅内端末からの情報流出
- 宅内端末を踏み台にした社内への不正侵入
- 宅内端末へのポリシー適用不全による脆弱性の残留
- 宅内端末の通信監視不全による脅威検知の遅延
- 宅内端末への障害対応やインシデント対応の遅延（遠隔対応、端末の回収、代替機送付等）

テレワークのセキュリティ対策例

- 多要素認証によるVPNアクセス認証の厳格化
- VPNアクセスの監視の強化
- 端末へのエンドポイントセキュリティ(EDR等)の実装による、ネットワークアクセス制限の厳格化、インストール制限、セキュリティパッチ管理の強化、操作監視、インシデント発生時の遠隔分析と隔離
- テレワーク環境の管理と利用の規定の整備

*1：BYOD（Bring Your Own Device）
私有デバイスの業務利用

*2：VDI（Virtual Desktop Infrastructure）
仮想的なデスクトップ環境

参考

2020年以降のセキュリティニュースで参照したサイト

- 情報セキュリティ安心相談窓口の相談状況［2021年第1四半期（1月～3月）］：IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/security/txt/2021/q1outline.html
- 情報セキュリティ10大脅威 2021：IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/security/vuln/10threats2021.html
- 監査人の警鐘- 2021年 情報セキュリティ十大トレンド | JASA (Japan Information Security Audit Association) https://www.jasa.jp/seminar/sec_trend2021/
- NPO日本ネットワークセキュリティ協会 https://www.jnsa.org/active/news10/index.html
- Software ISACが選ぶ開発者（企業）が注目すべき10大ニュース | CSAJ 一般社団法人コンピュータソフトウェア協会 https://www.csaj.jp/NEWS/committee/security/210122_softwareisac10.html
- マカフィー、2020年の10大セキュリティ事件ランキングを発表 第7回「2020年のセキュリティ事件に関する意識調査」を実施| McAfee Press Release https://www.mcafee.com/enterprise/ja-jp/about/newsroom/press-releases/press-release.html?news_id=2020121501

参考

サイバー空間における犯罪事例

ランサムウェア

2018年、交通事業者の業務用ファイルサーバーがマルウェアに感染し、業務の一部に支障が生じていると発表された。当該サーバーに保存された全ファイルへのアクセスが不能になった。

【攻撃の手口】

ランサムウェアの攻撃方法は、マルウェアで感染させた後ファイルを暗号化することでデータアクセスを不能にさせる。このデータを身代金やビットコインと引き換えに復旧させるという金銭獲得が主な目的となっている。

Web改ざん

2013年、市立総合病院のWebサイトが不正アクセスを受け、改ざんされていたことが確認された。改ざんされたWebサイトを閲覧した場合、マルウェアに感染する可能性があった。

【攻撃の手口】

Webページを改ざんしたり、不正プログラムを組み込むことでユーザー情報の搾取または悪質なウイルスのばら撒きなどを目的としたもの。

標的型メール攻撃

2018年、国家政策の指針となる基本計画の策定メンバーである、複数の大学の教授数人に対し、政府職員になりすました偽装メールが送信された（本事例での情報流出は起きていない）。

【攻撃の手口】

偽装メールの添付ファイルを開くとマルウェアに感染し、情報を盗み取られる仕組みとなっていた。中国のハッカー集団が関与したとみられている。

DDoS攻撃

2016年、地方公共団体のWebサーバーが閲覧できない障害が発生した。また、同機関のWebサーバー以外にも複数のサイトで障害が発生した。Webサーバーが閲覧できなくなったことに伴い、利用者からの問い合わせの受け付けも一時不可となった。

【攻撃の手口】

複数のコンピューターから標的のサーバーに、ネットワークを介し大量の処理要求を送ることでサービスを停止させたもの。攻撃のあった同日に、ハッカー集団がTwitter上で、同機関のWebサーバーをサービス不能にしたとする投稿があった。

参考

CYDERのトレーニング内容

- 演習舞台設定
  CYDERの演習舞台 (仮想組織のネットワーク) は、コース別に最適化された仮想環境を構築
- 攻撃・対処シナリオ
  CYDERの演習で使用されるサイバー攻撃や、それに対処する検知、解析、封じ込め、報告、復旧等の流れは、現実に起きたサイバー攻撃事例の最新動向を徹底的に分析し、コース別に、毎年最新のシナリオを準備。繰り返し受講することにより、最新かつ様々な攻撃に対する対処法を学ぶことが可能

過去の演習シナリオ例

Aコース

① 標的型攻撃メールを受信した株式会社サイダーの職員が、添付されていたドキュメントファイルを開いて、マルウェアに感染
② その職員の端末から社内の他の端末へ感染が拡大

B-1コース

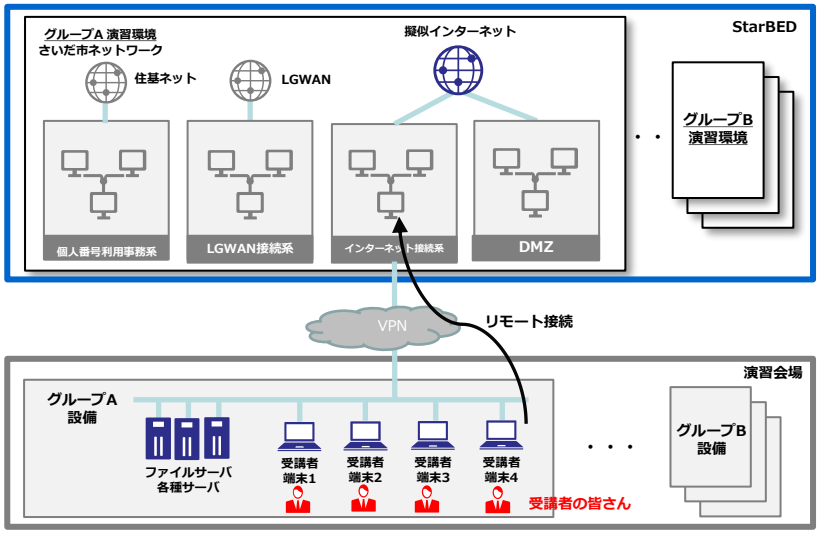
① CMS (コンテンツ・マネジメント・システム) の脆弱性を用いて侵入・改ざんされたWebサイトにさいだ市の職員がアクセスした結果、マルウェアに感染
② その職員の端末から、庁内システム内にマルウェア感染が拡大、機密ファイルが漏洩しメールサーバーにマイニングツールが設置される

B-2コース

① さいだ省の職員が、悪意のある広告 (マルバタイジング) を含んだ一般のニュースサイトにアクセスし、マルウェアに感染
② その職員の端末から、省内システム内にマルウェアが感染拡大、機密ファイルが漏洩する

演習舞台設定例 (B-1コース)

各グループそれぞれに提供するネットワーク構成



参考

集合演習のマイルストーン例

課題	テーマ	課題概要
1	検知・連絡受付	連絡受付に対する事実確認および対処
2	トリアージ（ログ調査） Hands-on	事実確認のためのログ調査
3	トリアージ（ヒアリング）	現場当事者への指示・依頼
4	対応方針の検討	事実関係の整理、今後の対応方針の検討
5	証拠保全 （ディスクイメージ調査） Hands-on	事象の詳細調査（１）
6	証拠保全 （マルウェア解析） Hands-on	事象の詳細調査（２）
7	封じ込め・根絶／報告・公表	事実関係の整理、封じ込め・根絶策検討
8	復旧措置・報告書作成	報告書作成
9	再発防止策の検討	改善点の洗い出し

- Hands-on はハンズオン課題、それ以外はディスカッション課題です。
※ディスカッションで検討した内容について、数チームに発表していただきます。その他チームからの質問、助言等の意見交換を行います。

参考

セキュリティ人材に必要とされる能力とNICTが行う実践的サイバー演習の対応関係

行政機関や民間企業の現場で働く情報システム担当者等は、日常業務が忙しく、訓練に長時間を割くことが難しい
NICTの実践的サイバー防御演習では、「ベンダーお任せ」では済まない、インシデント発生時の即応的な対処のために最低限必要なスキルを厳選して凝縮し、１日程度のコンパクトで効率的な実機演習を実施している

セキュリティ人材に必要とされる、スキルおよび知識の一覧 (※1)

総合的なセキュリティ人材は、インシデントマネジメント技術のみならず、セキュリティの基礎知識から、計算機やネットワーク等の専門性の高い分野や、事業運営、情報倫理、法制度までを含む、幅広いスキルと知識が必要となる

※1 「セキュリティ知識分野(SecBoK)人材スキルマップ 2017年版 (JNSA)」を基に作成

：演習で集中的に得られる技術分野

：演習で部分的に触れる技術分野 (インシデント発生時の即応的な対処能力の習得に焦点を絞れば、必ずしも、演習で集中的に取り組む必要まではない技術分野)

技術領域	具体的な技術分野の例
ICT 基礎	ハードウェア、OS、ネットワーク、システム開発
工学基礎	プロセス工学、フォールトトレランス、数学
セキュリティガバナンス	情報セキュリティアーキテクチャシステム
セキュアシステム設計・構築	システムライフサイクルマネジメント、構成管理
暗号・認証・電子署名	暗号化アルゴリズム、認証手法、一方向性ハッシュ
セキュリティ運用	**セキュリティ運用と事業の衝突回避**
	インシデント対応
	セキュリティ技術に関する知識
セキュリティ基礎	CIA、セキュリティ問題・リスクおよび脆弱性
サイバー攻撃手法	脅威、攻撃手法、脆弱性、マルウェア、ハッキング
デジタルフォレンジックス	データの保全・解析・保管、ライブデータの解析
セキュリティマネジメント	教育、啓発、ポリシー、セキュリティ対策
システムセキュリティ	システムの脅威と脆弱性、バイナリ解析
ネットワークセキュリティ	トラフィック解析、侵入検知、アクセス制御
	フィルタリング、ペネトレーション、脆弱性診断
ビジネス基礎	コミュニケーション能力、組織評価、アセスメント
法・制度・標準	国内外関連法・標準、コンプライアンス、ポリシー

セキュリティ運用と事業の衝突回避
- 運用上のセキュリティに関する知識
- 新興の情報技術と情報セキュリティ技術に関する知識
- システム診断ツールと障害識別技法に関する知識
- 自組織内部の構造とプロセスについて報告するコンピュータネットワーク防御 (CND) サービスの提供者に関する知識
- 主要ベンダの製品と用語及びエクスプロイト／脆弱性にどのように作用するかの相違点に関する知識
- セキュリティ運用と事業の衝突回避に関するスキル
- リスク脅威の評価に関する知識

インシデント対応
- インシデントのカテゴリ、インシデントレスポンス及び応答のタイムラインに関する知識
- インシデントレスポンスとハンドリングの方法論に関する知識
- インシデントハンドリング手法の利用に関するスキル
- インシデントの根本原因分析に関する知識
- インシデントに関連したネットワークセキュリティの報告のためのプロセスに関する知識
- 企業のインシデントレスポンスプログラム、役割及び責任に関する知識
- インシデントの根本原因分析の実施に関するスキル
- 報告されたインシデントの文書化と問い合わせに用いられるデータベース手続きに関する知識

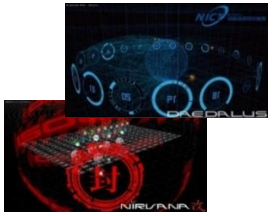
セキュリティ技術に関する知識
- 内部不正の検出、報告、検出ツール及び法規制に関する知識と経験
- セキュアな取得に関する知識
- セキュリティイベント (事象) の相関ツールに関する知識

参考

NICTによるセキュリティオペレーターの育成

NICTの「強み」

長年のサイバーセキュリティ研究による技術的知見



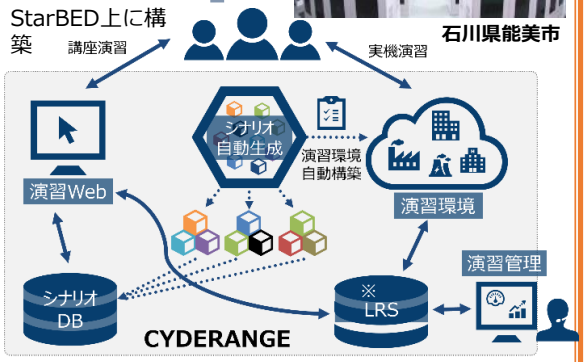
- NICTの長年にわたるサイバーセキュリティ研究で得られた技術的知見を活用し、我が国固有のサイバー攻撃事例を徹底分析した最新の実機演習シナリオを作成
- インシデントハンドリングに最低限必要なスキルを厳選して凝縮し、コンパクトで効率的なカリキュラムを構成

大規模高性能サーバー群 NICT北陸StarBED技術センター

- **大規模性**
  大規模な組織のネットワーク環境を再現した仮想環境を構築するための大規模なサーバー群
- **運営ノウハウの蓄積**
  大規模仮想環境の効率的かつ安定的な運営に関する高度な知見・ノウハウが蓄積
- **セキュアな環境**
  インターネット等から隔離された強固な閉鎖環境

サイバー演習自動化システム CYDERANGE (サイダーレンジ)

- CYDERANGEはサイバー演習の運営に係るコストの削減と受講者のプロファイルに合わせた効果的な演習プログラムの提供を目指すサイバー演習自動化システムを2018年度から導入



※ Learning Record Store (履歴データベース)

活用

CYDER
Cyber Defense Exercise with Recurrence

サイバー攻撃への対処方法を体得

仮想空間で再現された大規模ネットワーク環境

参考

CYDERANGE（サイダーレンジ）：サイバー演習自動化システム

NICTナショナルサイバートレーニングセンターは、より効率的なサイバー演習を実現するサイバー演習自動化システム “CYDERANGE” を独自に開発。これまでのサイバー演習では、演習プログラムの作成ごとにシナリオや演習環境を手作業で作成することが一般的であったが、この CYDERANGE の開発により、演習シナリオの自動生成等が可能となった (2018年度から実運用を開始)

ポイント

- **世界初の機能**
  - 演習「シナリオ」の自動生成は、既存技術にはない、世界で初めての機能
- **運用性の向上とコストの削減**
  - 演習環境を自動構築することで、演習環境の運用性の向上や演習実施に係る費用の低減を実現
- **次世代の業界標準技術にいち早く対応**
  - フライトシミュレーター等でも用いられる次世代の演習データ記録方式の世界規格である Experience APIを用いたLRS (Learning Record Store) を構築
    → より詳細な受講者データの取得・分析を可能に
- **演習の効果を精密に測定**
  - 膨大な受講者データを機械学習等の技術によって分析することで、演習による学習効果を精密に測定することが可能

Webサイト https://cyder.nict.go.jp/