National Institute of Information and Communications Technology

CYDER
Cyber Defense Exercise with Recurrence

実践的サイバー防御演習「CYDER」のここがスゴい！

～NICTナショナルサイバートレーニングセンターの取り組み～

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

#CYDER

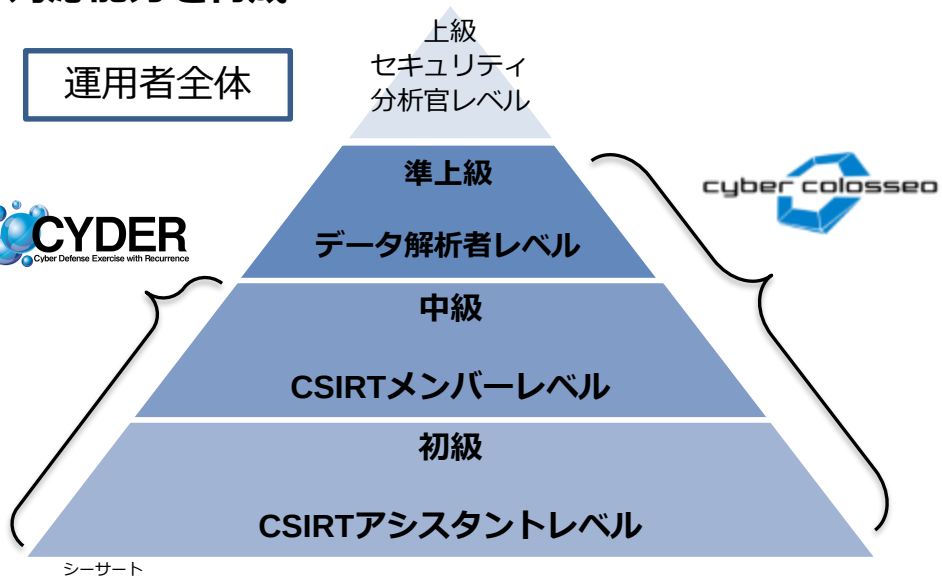
「ナショナルサイバートレーニングセンター」の概要

○ 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**する組織として、「ナショナルサイバートレーニングセンター」を設置（2017年4月1日）

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**

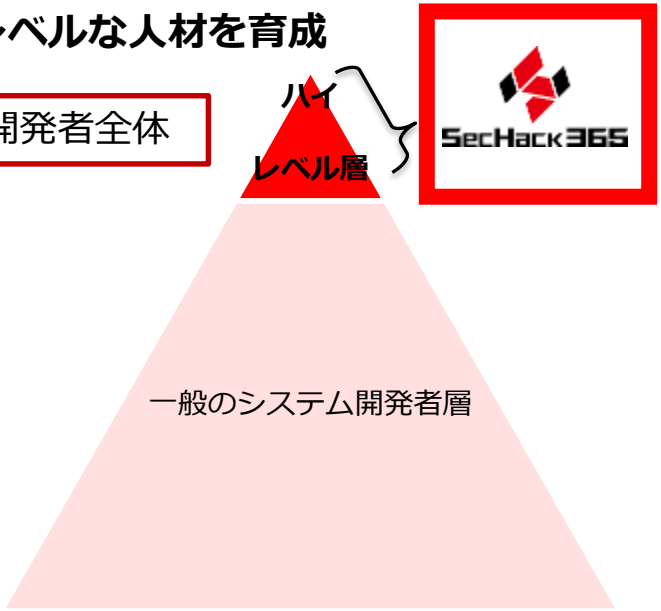
運用者全体



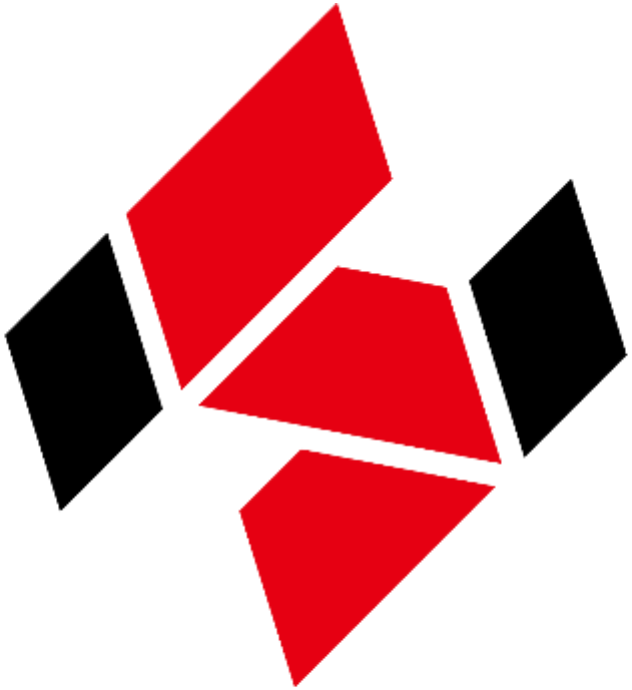
セキュリティイノベーター（革新的研究・開発者）の育成

- ✓ **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**

開発者全体



※CSIRT：Computer Security Incident Response Team



SecHack365

#SecHack365

セキュリティイノベーター育成プログラム「SecHack365」の概要

（セックハックサンロクゴ）

セキュリティに関わる新たなモノづくりができる人材（**セキュリティイノベーター**）の創出に向けて、若年層のICT人材を対象に、NICTの持つ長年の研究開発のノウハウや、実際のサイバー攻撃関連データとそれらを安全に利用して研究開発を行うことができる環境を活かした、1年をかけて本格的にセキュリティ関連技術の指導を行うプログラム

対象者

- ✓ **学生、若手社会人**を対象とした早期人材育成
- ✓ 対象者は、**日本国内に居住する25歳以下の若手ICT人材**
- ✓ 2018年度は応募者数345名のうち50名の受講生を選定。
  （選定時内訳　成年37名/未成年13名・男性46名/女性4名）

受講生属性

2018年度受講生

属性	人数
社会人	6
大学院生	11
大学(学部)生	20
専門学校生	1
高等専門学校生	5
高校生	5
中学生	2
合計	50名

2017年度修了生

属性	人数
社会人	4
大学院生	9
大学(学部)生	16
専門学校生	1
高等専門学校生	7
高校生	1
小学生	1
合計	39名

ハッカソンのテーマ例 (2017年度実績)
AI (深層学習) による不正 Web サイト検知
広範なマシン環境で動作可能なプログラム解析エンジン
仮想空間でサイバー攻撃を体験できるゲーム
自動車データのクラウド解析によるドライバーアシスト
レーザポインタによる家電の「指揮」
不正 Web サイトの統合分析プラットフォーム

「SecHack365」のプログラム内容

NICTの強みを生かした育成事業

アイデアソン・ハッカソンイベント
開催地を変えて複数回実施し、継続的に開発指導。
オフラインで議論、検討、相談、発表を行う。

受講生への支援
長時間の学業との両立についての助言、指導。
作る→見せる を習慣化し作品のイメージを早期に具体化。

最先端技術の体験
先端企業の見学による社会体験で発想力を強化。
講演を聞くことでプレゼンテーションスキルにつなげる。

オンラインでの指導・遠隔開発演習
自宅などの遠隔地から開発環境へアクセス可能。
チャットやタスク管理ツールを活用した持続的な指導を実施。

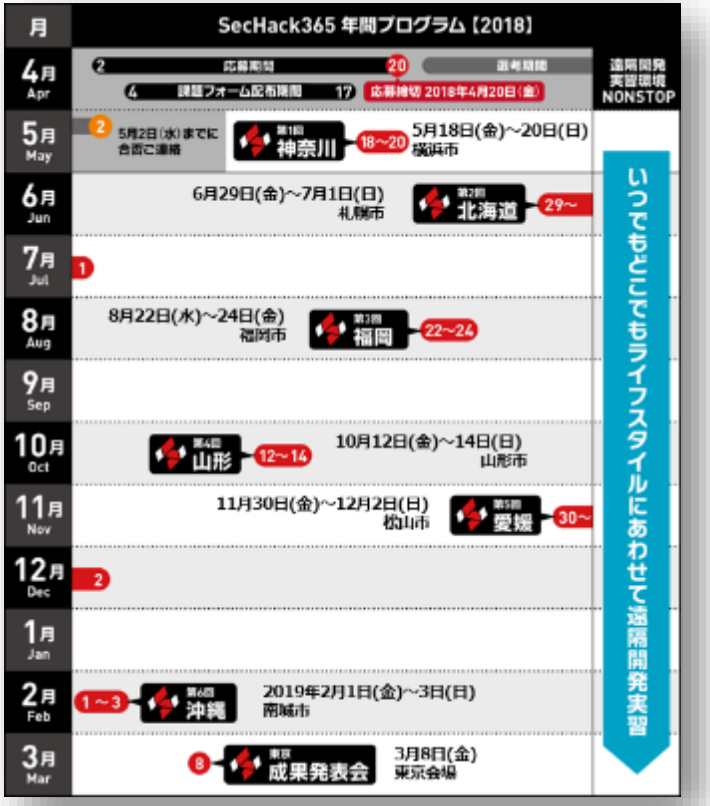
豊富な研究資産
NICTの知見・人的資源、研究開発のノウハウ、
攻撃データ等の活用。

作品づくりを支援する３つのコース（2018年度）
応募時に自らが望むコースを選択することでミスマッチを抑制

開発駆動コース
作りたいモノ、方法、アプローチがはっきりしている人向け。
実装などのアウトプットをすることを重視

表現駆動コース
作りたいテーマはあるが、成果物そのものや、
それを作り出す方法、アプローチを工夫したい人向け。
発表など他者への表現とフィードバックを重視

思索駆動コース
大きなテーマや社会的課題について本質的な検討をしながら、
課題解決するために必要なモノを導き出す頭を整えたい人向け。
取り扱う問題や対象について深く考えることを重視



SecHack365実施風景

現地企業訪問・見学

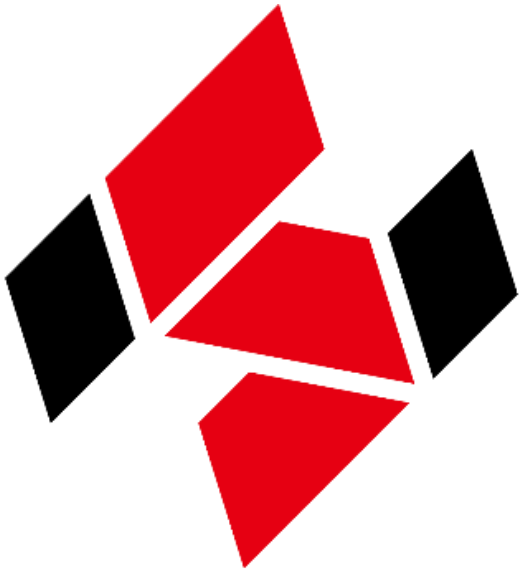
講義

ポスター展示

デモ

コースワーク

成果発表会



SecHack365

3/8(金)成果発表会@秋葉原

ぜひ会場で成果をご覧ください

#SecHack365

「ナショナルサイバートレーニングセンター」の概要

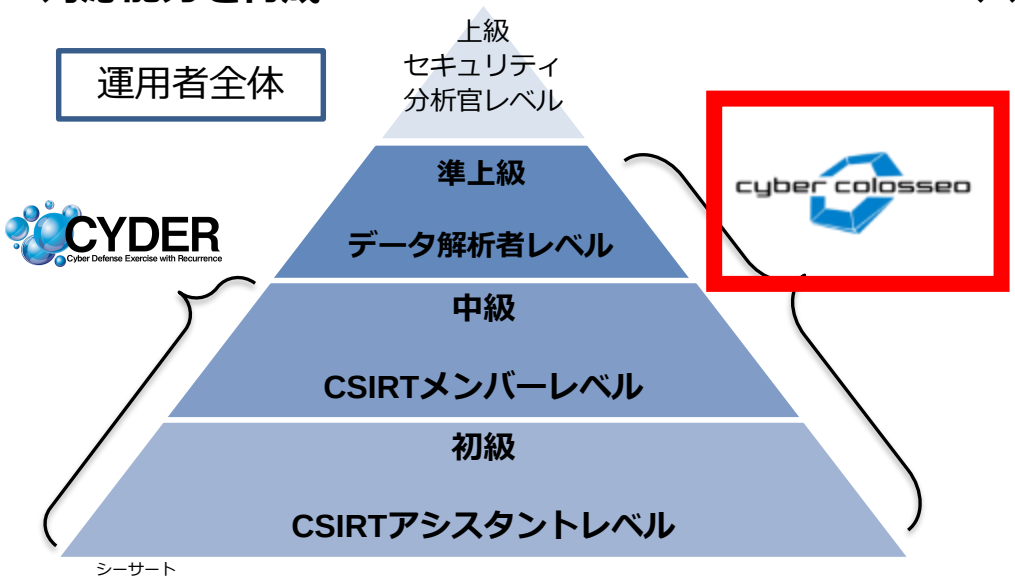
○ 情報通信分野を専門とする我が国唯一の公的研究機関である**NICTの技術的知見、研究成果、研究施設等を最大限に活用し、実践的なサイバートレーニングを企画・推進**する組織として、「ナショナルサイバートレーニングセンター」を設置（2017年4月1日）

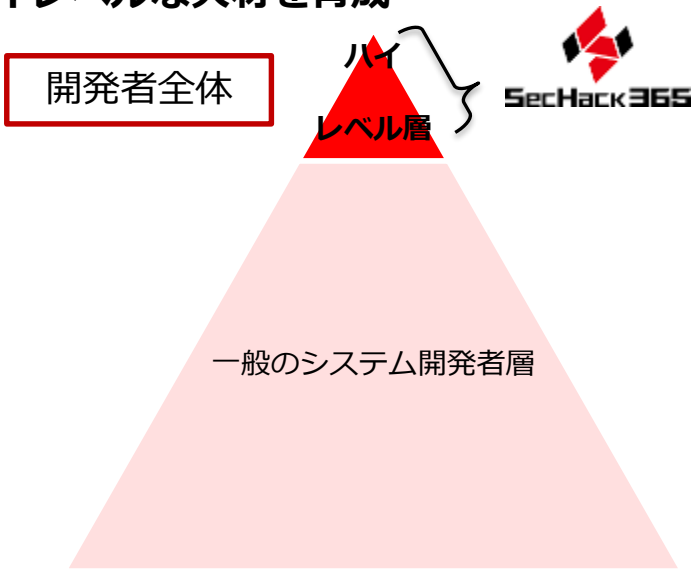
セキュリティオペレーター（実践的運用者）の育成

- ✓ **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**

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**





※CSIRT：Computer Security Incident Response Team


cyber colosseo

東京2020大会開催に向けた実践的サイバー演習「サイバーコロッセオ」の概要

東京2020オリンピック・パラリンピック競技大会関連組織のセキュリティ関係者が、
大会開催時を想定した模擬環境で攻撃・防御双方の実践的な演習を行うことにより、
高度な攻撃に対処可能な高度な能力を有するサイバーセキュリティ人材を育成

サイバーコロッセオ実施計画の策定・公表（2017年12月7日）

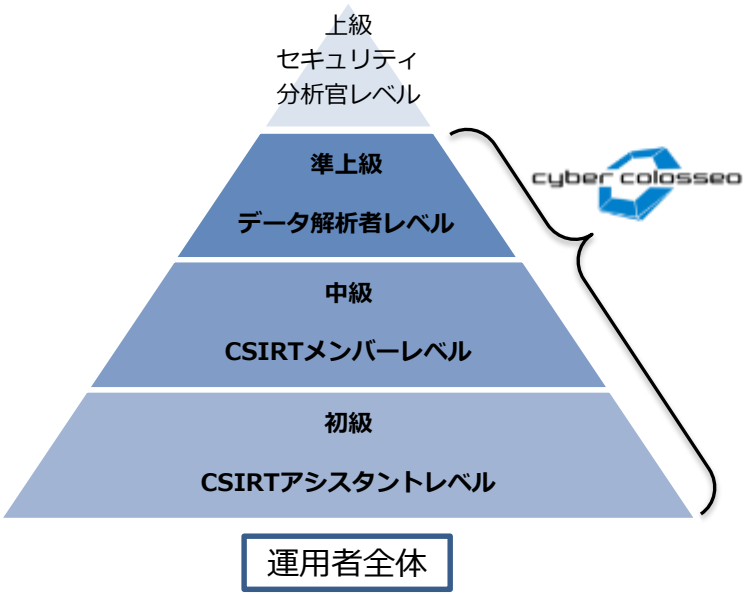
東京2020オリンピック・パラリンピック競技大会まで3年を切る中、必要な能力を兼ね備えた人材を大会開催までに段階的・計画的に育成していくことを目的として、NICTは、関係省庁・関係団体等と協議の上、2017年12月7日「東京2020オリンピック・パラリンピック競技大会に向けたサイバーコロッセオ実施計画」を策定・公表

コース概要

◆コロッセオ演習
受講者の習熟度や業務の性質等に合わせて、
初級A/B・中級・準上級コースを設定

・初級A/B（CSIRTアシスタントレベル）
　業務内容によってA、Bの2コース
　事前オンライン学習（1 時間程度）、実機演習・グループワーク（1日）
・中級コース（CSIRTメンバーレベル）
　事前オンライン学習（1 時間程度）、実機演習・グループワーク（1日）
・準上級コース（データ解析者レベル）
　高度セキュリティ講義（1日）、実機演習・グループワーク（1日）

◆コロッセオカレッジ
コロッセオ演習と連携する15科目20コマの講義演習（選択受講制）



サイバーコロッセオは、(ISC)[2]が提供する資格の認定継続に必要なCPEクレジット(継続教育単位)付与対象の演習。

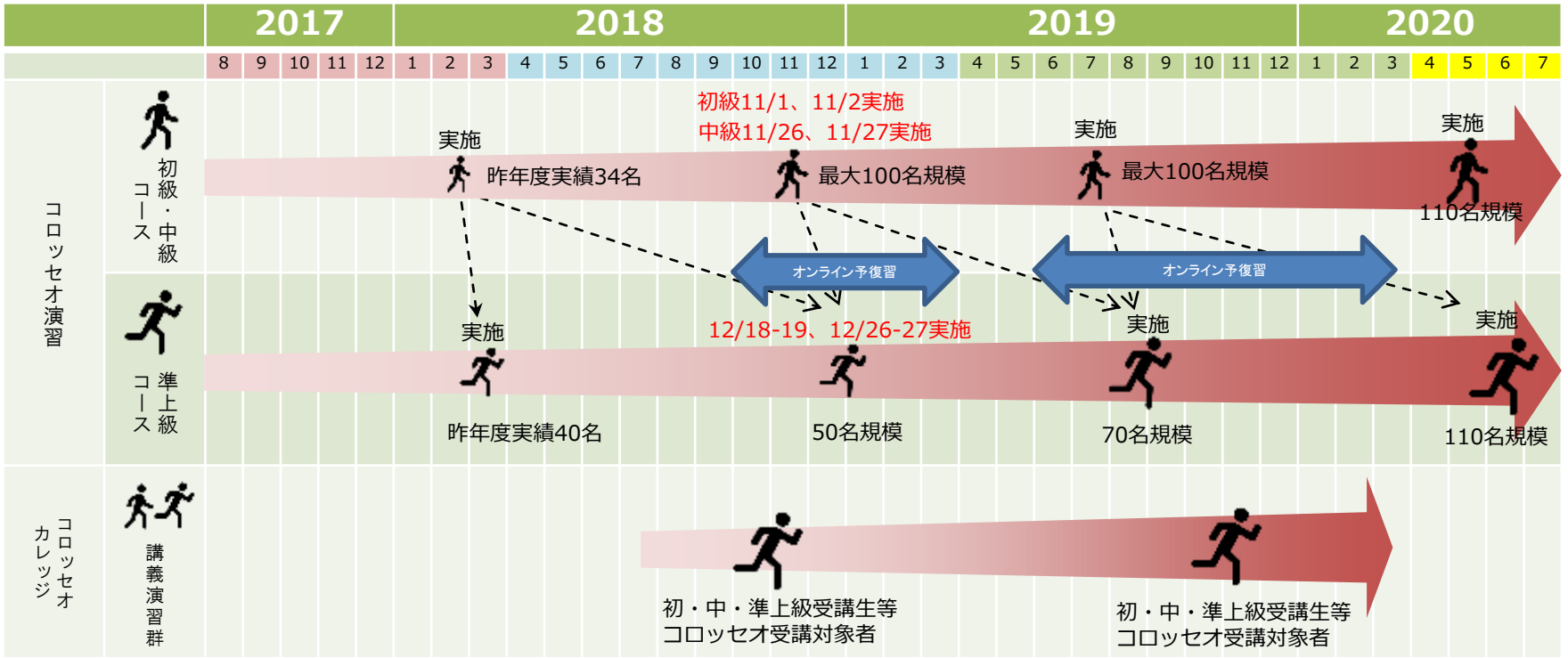
(ISC)[2] (International Information Systems Security Certification Consortium)は、ベンダーフリーであり、知名度と信頼の高いセキュリティ国際資格の一つ、CISSP (Certified Information Systems Security Professional)などの国際資格を提供している。

サイバーコロッセオの対象組織及び開催規模

大会開催時には高度かつ多様なサイバー攻撃を集中的に受けるおそれがあることを考慮し、
サイバーコロッセオは、大会関係団体のうち最もコアな役割を担う、
公益財団法人東京オリンピック・パラリンピック競技大会組織委員会を対象

開催規模等

- ○ 東京大会開催までの3年間を通じて継続的なトレーニングを実施
- ○ 最終的に約220人のセキュリティ担当者等を育成予定（段階的に規模を拡大）
- ○ NICTイノベーションセンター（大手町）にて実施



※ 表中の目標人数は現時点において組織委が想定する数字であり、今後、組織委側のニーズを踏まえつつ、必要に応じて見直しを行う予定

サイバーコロッセオのトレーニング内容

コロッセオ演習

- 演習舞台設定
  サイバーコロッセオの演習舞台（仮想ネットワーク）は、東京大会の公式サイト、大会運営システム等のネッワーク環境を再現して構築
- 演習イメージ（準上級コース）
  大会開催時に想定されるサイバー攻撃を擬似的に発生させることができるようにし、本格的な攻防戦等を繰り返し実施
  ※ 攻防戦のほかに、フォレンジックやバイナリ解析の速さ等を競うコンテスト形式の演習などを開発予定
  - 攻防戦
    受講者が複数チームに分かれ、自組織のネットワークの守備と他チームのネットワークへの攻撃を両方体験することで、攻撃者側の視点をも踏まえたハイレベルな防御手法の検証及び訓練を行う演習

コロッセオカレッジ

- コロッセオ演習内でカバーできない広範な講義演習を開講
- 選択受講制
  - 受講者が自身のスキルマップに基づき不足している領域の講義演習を選択

科目群	科目名	対応コロッセオ演習コース（レベル）
標準科目群	セキュリティ基礎	初級A/B
	セキュリティツールE	初級A/B、中級
	インシデントレスポンス概論	初級A/B
	個人情報保護法令	初級B
	システムアーキテクチャ	初級A/B、中級
	セキュリティツールM	中級、準上級
	実践インシデントレスポンス１、２	中級、準上級
補助系/実務系科目群	セキュア開発	中級、全コース
	最新セキュリティトレンド	中級、全コース
	マルウェア解析実務１、２	中級、準上級
	フォレンジックス実務１、２	中級、準上級
	Micro Hardening１、２	中級、準上級
	ログ・パケット解析実務	中級、準上級
	サイバーインテリジェンス	中級、準上級
	脆弱性診断実務１	中級、準上級
	脆弱性診断実務２	中級、準上級

「ナショナルサイバートレーニングセンター」の概要

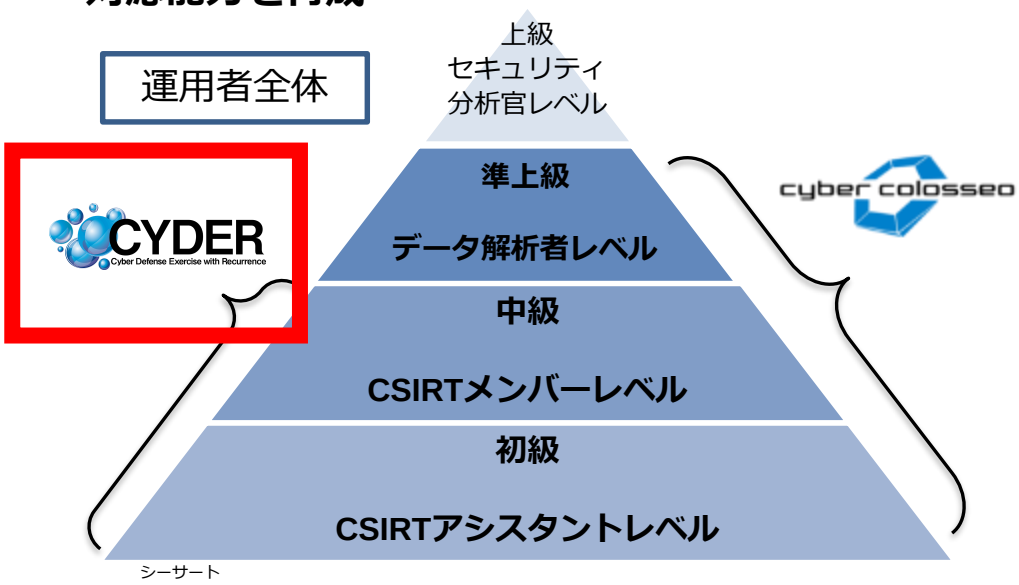
○ 情報通信分野を専門とする我が国唯一の公的研究機関である**NICTの技術的知見、研究成果、研究施設等を最大限に活用し、実践的なサイバートレーニングを企画・推進**する組織として、「ナショナルサイバートレーニングセンター」を設置（2017年4月1日）

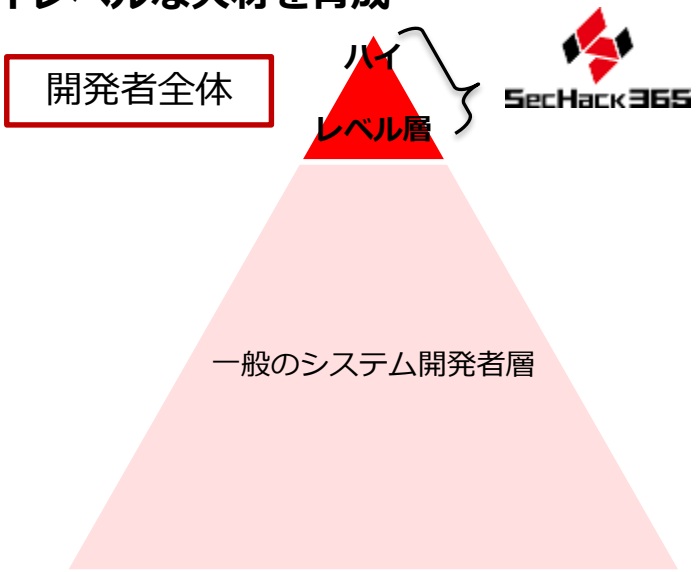
セキュリティオペレーター（実践的運用者）の育成

- ✓ **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**

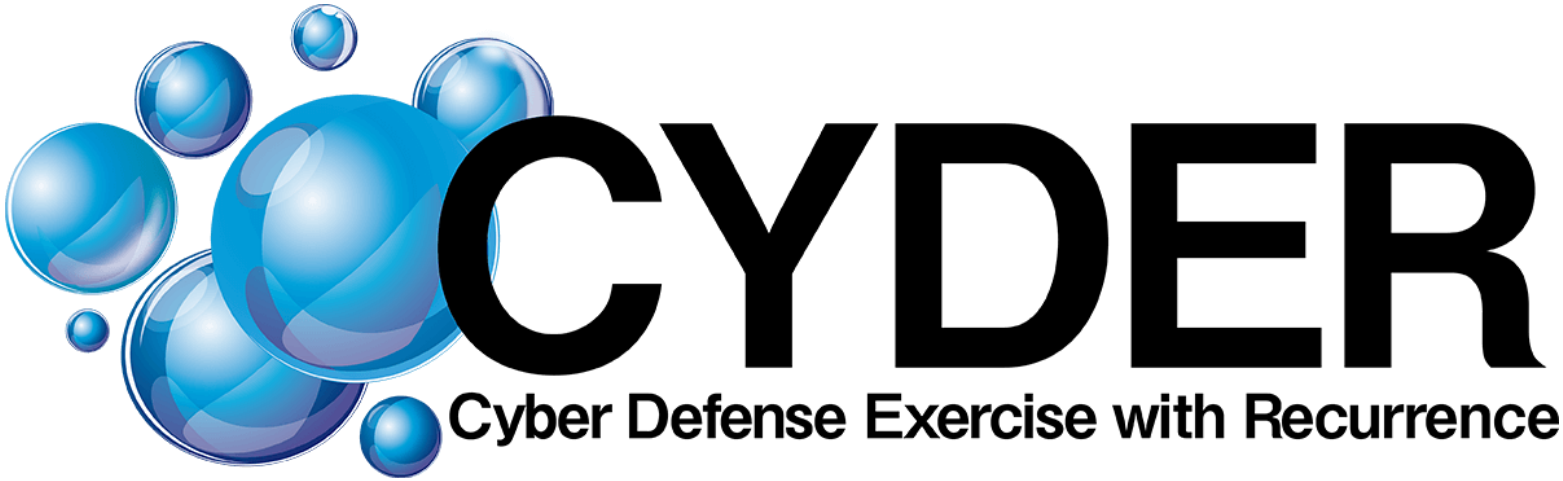
セキュリティイノベーター（革新的研究・開発者）の育成

- ✓ **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**



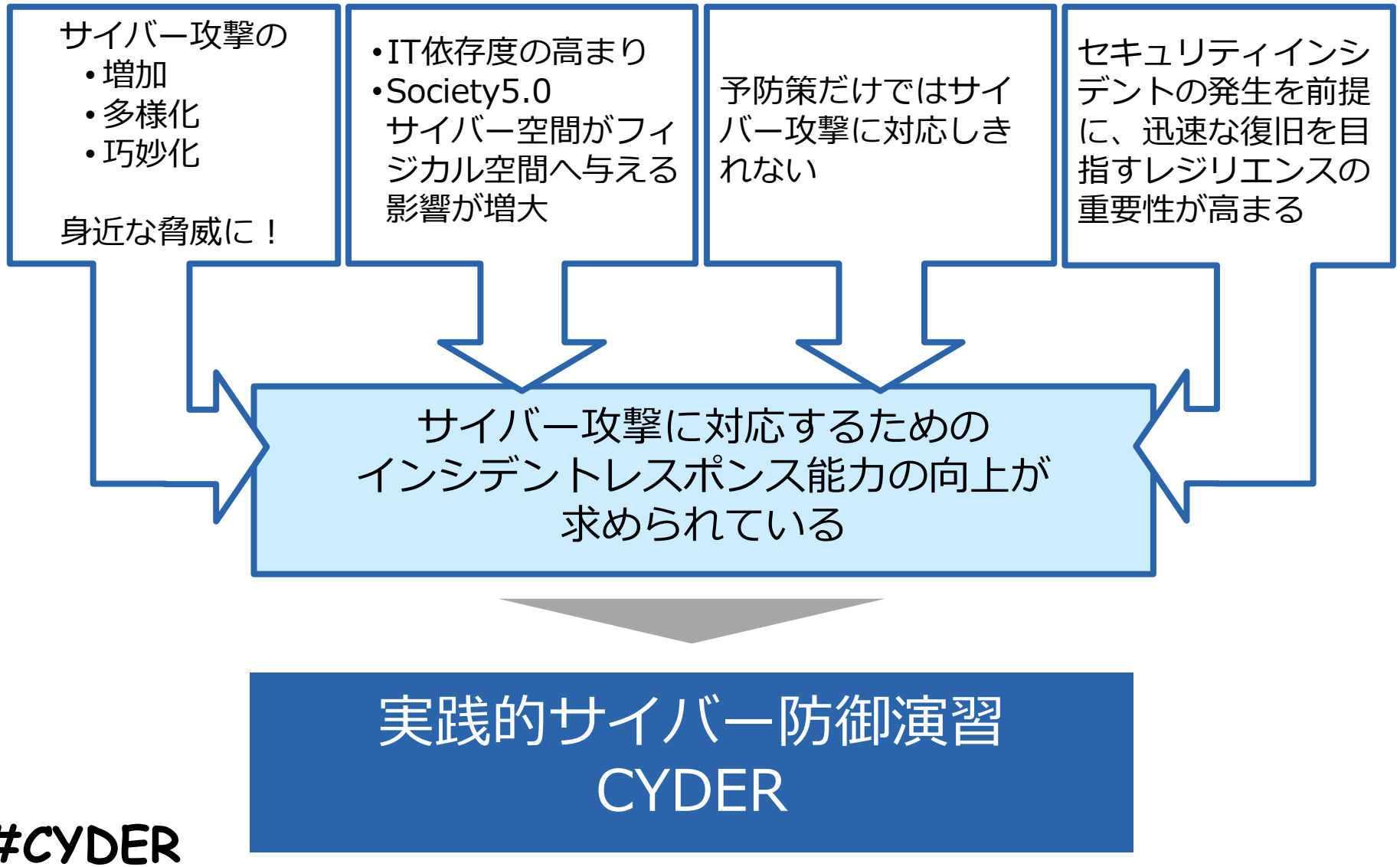


※CSIRT：Computer Security Incident Response Team



#CYDER

近年のサイバー攻撃に関する背景



#CYDER

実践的サイバー防御演習「CYDER（サイダー）」の概要

(CYDER：CYber Defense Exercise with Recurrence)

行政機関、重要インフラ等の情報システム担当者等が、組織のネットワーク環境を模擬した環境で、実践的な防御演習を行うことができるプログラムを提供することにより、数千人規模でセキュリティオペレーターを育成

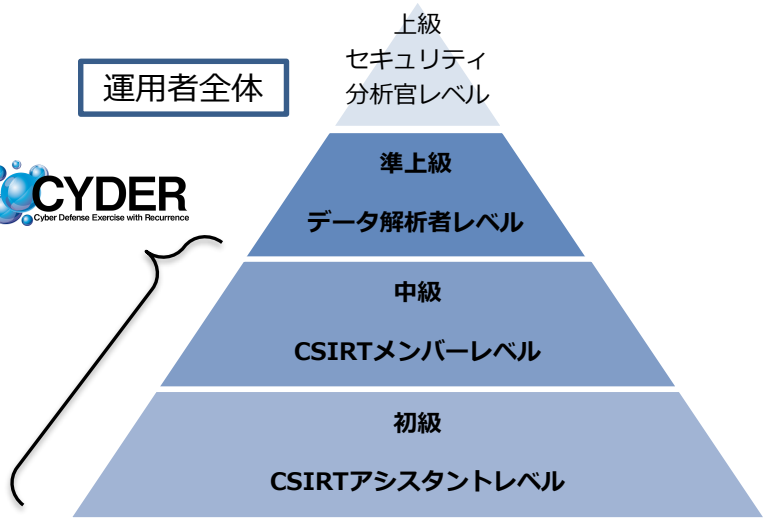
2018年度コース概要

受講者の習熟度に応じて**Aコース及びBコースを開催**

- ◆ 事前オンライン学習（１時間程度）
- ◆ 実機演習・グループワーク（１日間）

年間100回程度開催、3,000人以上の受講が可能

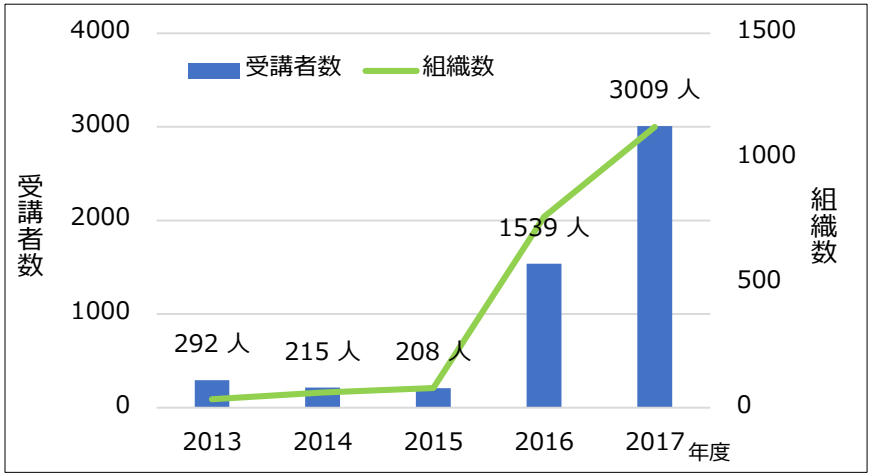
- ◆ **Aコース**（CSIRTアシスタントレベル）
  47都道府県において開催
- ◆ Bコース（CSIRTメンバーレベル）
  - ・**B-1コース**（地方公共団体向け）
  - ・**B-2コース**（国の行政機関等向け）
  - ・**B-3コース**（重要社会基盤事業者等向け）



対象組織

※サイバーセキュリティ基本法にて規定

- ✓ 国の行政機関等
  - ・国の行政機関（28組織）
  - ・独立行政法人（87法人）
  - ・指定法人（特殊法人・認可法人のうちサイバーセキュリティ戦略本部が指定する9法人）
- ✓ 地方公共団体
- ✓ 重要社会基盤事業者（14分野）
  情報通信、金融、航空、空港、鉄道、電力、ガス、医療、水道、物流、化学、クレジット、石油　等
- ✓ 一般企業等



CYDER受講者数の推移

CYDERは、(ISC)²が提供する資格の認定継続に必要なCPEクレジット(継続教育単位)付与対象の演習

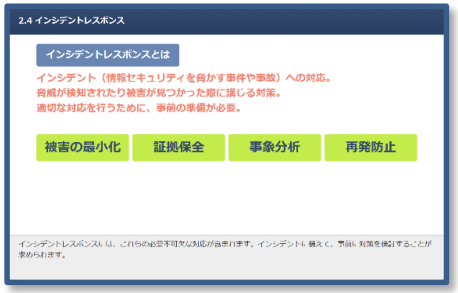
CYDER演習内容

Aコース：初心者向け
Bコース：コンピューター及びネットワーク並びにサイバーセキュリティに関する基礎知識を持つ者向け

事前学習（約１時間）

事前オンライン学習（講義演習編）

- ✓ 最近のサイバー攻撃の傾向や対策を理解
- ✓ 事件対応の心得について学ぶ



会場演習（１日）

実習（実機演習編）

- ✓ チーム毎に事件対応を一通り体験
- ✓ 報告書を作成

グループワーク

- ✓ 運用基準等の課題を明確化
- ✓ 対策を検討する議論を実施

体験のみで終わらない本格的な訓練を受けることが可能！

#CYDER

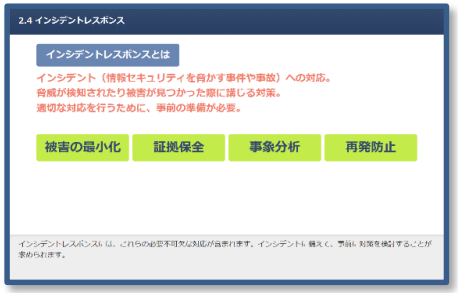
CYDER演習内容

Aコース：初心者向け
Bコース：コンピューター及びネットワーク並びにサイバーセキュリティに関する基礎知識を持つ者向け

事前学習（約１時間）

事前オンライン学習（講義演習編）

- ✓ 最近のサイバー攻撃の傾向や対策を理解
- ✓ 事件対応の心得について学ぶ



会場演習（１日）

実習（実機演習編）

- ✓ チーム毎に事件対応を一通り体験
- ✓ 報告書を作成

グループワーク

- ✓ 運用基準等の課題を明確化
- ✓ 対策を検討する議論を実施

体験のみで終わらない本格的な訓練を受けることが可能！

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

※ 例えば地方公共団体向けのB-1コース（仮想自治体「さいだ市」）では、総務省が示す自治体情報システム強靭性向上モデルに沿った強靭性向上後の庁内システムを再現

○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

演習シナリオ例

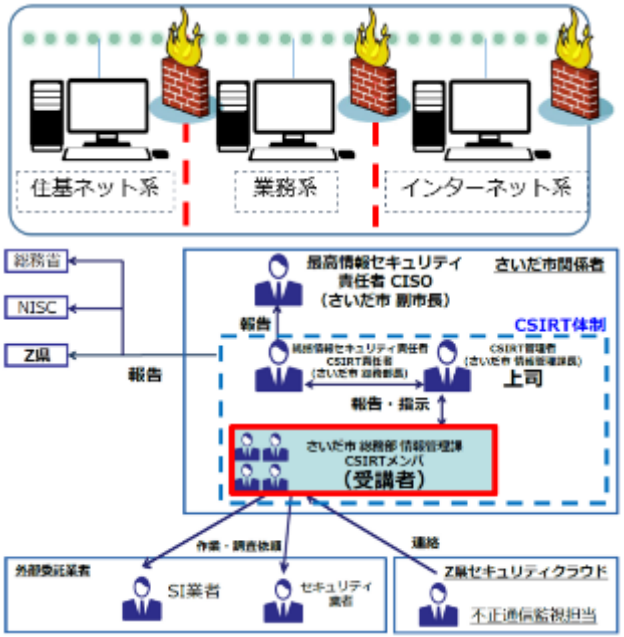
※ 演習シナリオは、最新のサイバー攻撃事例をふまえて、毎年度、最新のものを準備

Aコース（2017年度）
- 職員が標的型メールを開き、ウイルスに感染
- その職員の端末から庁内の他の複数のネットワーク機器へ感染が拡大

B-1コース（2017年度）
- さいだ市が住民向けサービスを提供しているWebサイト(Webアプリケーションフレームワーク)の脆弱性を突かれ、管理者ページの改ざんが発生
- それを起点とし、庁内システム内にマルウェアが感染拡大

B-2コース（2017年度）
- さいだ省職員が組織外部にて持ち出し用PCからインターネットにアクセス その際にPC内のソフトの脆弱性を突かれ、端末がマルウェアに感染
- その後、当該端末が省内ネットワークに接続され、省内システム内にマルウェアが感染拡大

演習舞台設定例（B-1コース）

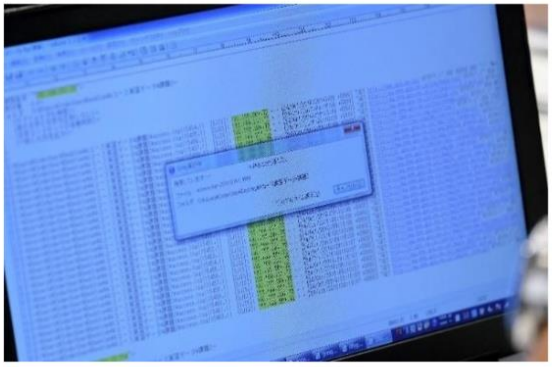


CYDER演習風景

演習

演習フロー説明

端末特定

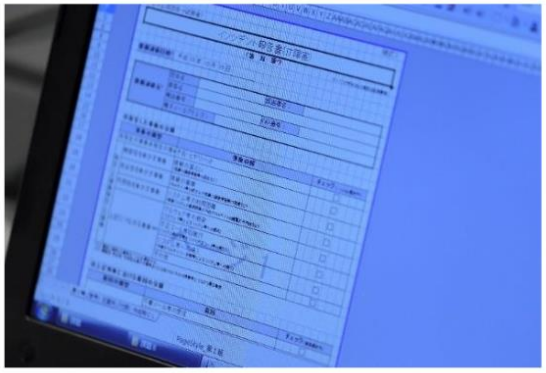


マルウェア挙動調査

グループワーク

発表

報告書作成



集合演習の目的

- サイバー攻撃に対応するため情報システム担当者の**インシデントレスポンス能力の向上を目的**としています。

- インシデントハンドリングを体験することで、**サイバー攻撃について理解**を深め、事業継続を脅かす攻撃への対応を学ぶことができます。

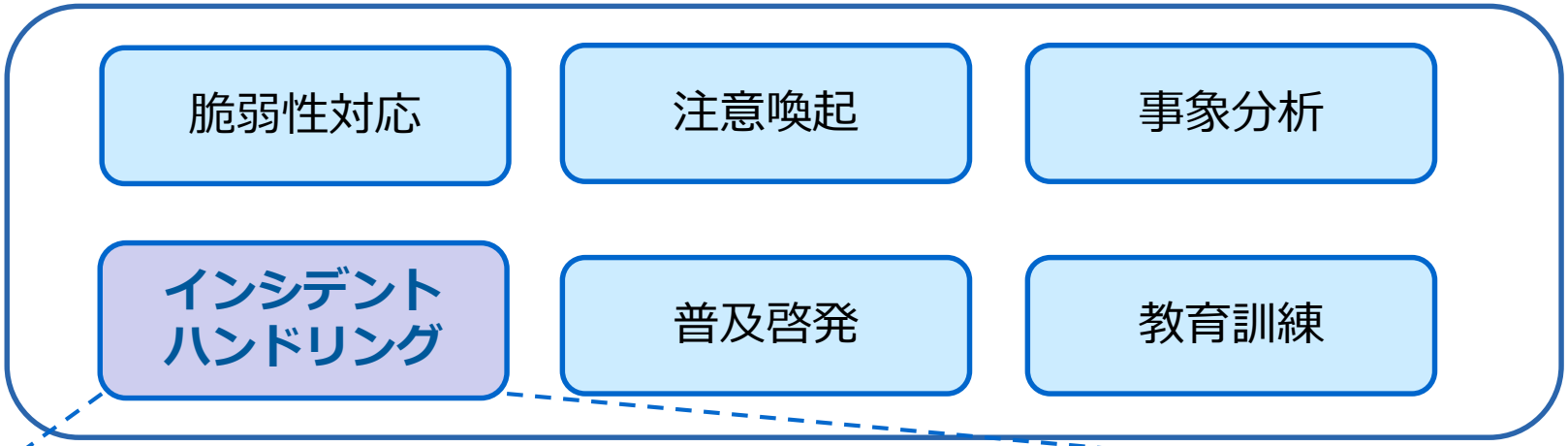
- 演習を通じて、以下の**気づき（ヒント）を得る**ことができます。
  「平時からどのような**備え**が必要か」
  「被害を最小化するためにどんな対応をすればよいのか」

習得できるスキル

- インシデントの予兆を認知した後、事実確認を実施できる（検知確認）
- 関係者（ステークホルダ）への適切な報告が実施できる（報告）
- インシデント現場の端末利用者に対する
適切なヒヤリング内容を理解する（情報収集）
- 各種ログサーバから必要な情報を検索し、
情報漏洩の可能性等を調査できる（調査）
- インシデントに合わせ、適切な封じ込めを実施できる（封じ込め）
- 保全対象となる端末の選択が実施できる（証拠の保全）
- 外部機関と連携して、
保全対象となった端末の適切なフォレンジック調査依頼を実施できる
- 所定のフォーマットを用いて、報告書作成が実施できる（報告書作成）

インシデントマネジメント

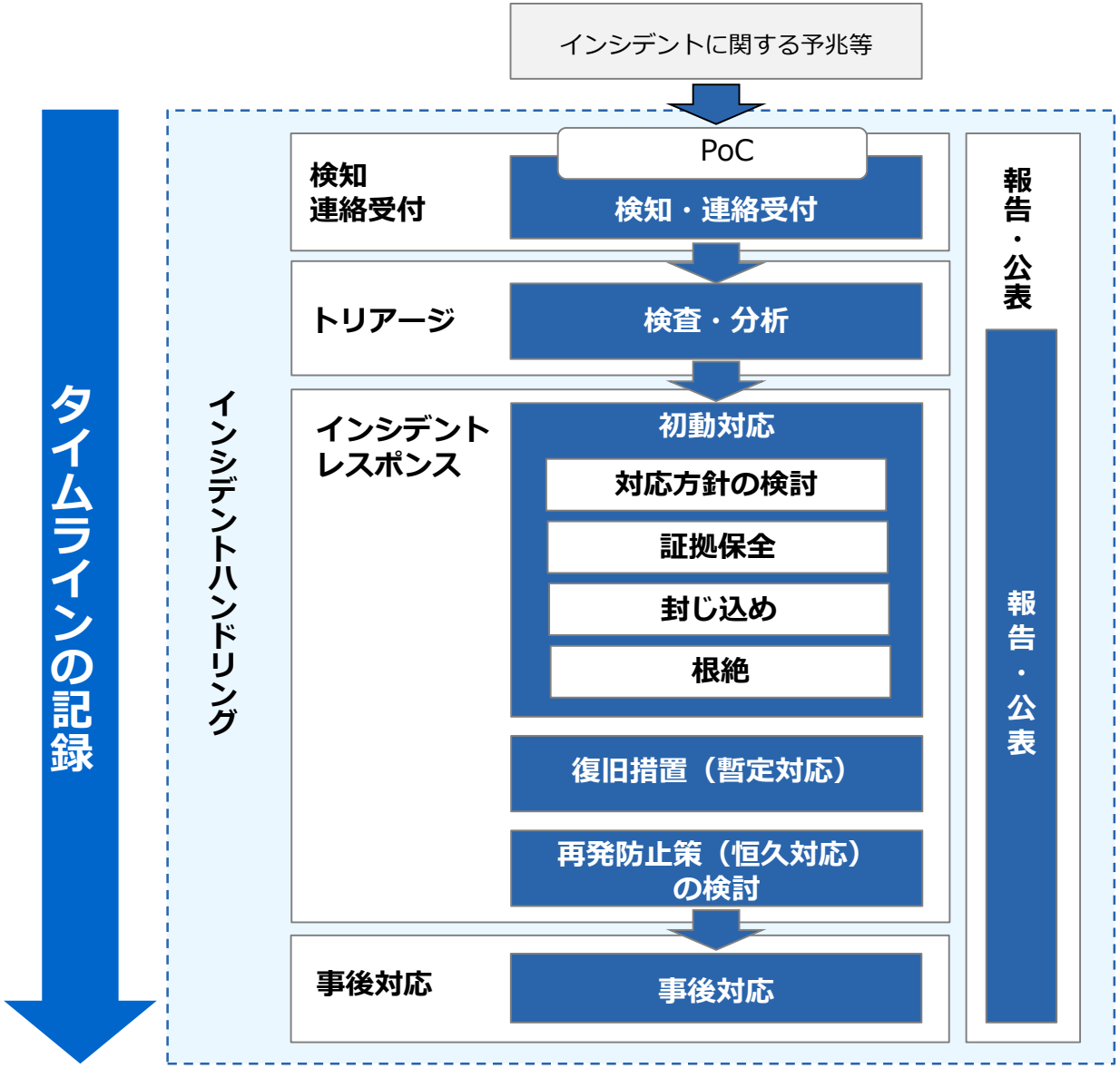
CSIRTが「事前」の準備を含めたインシデントに対して行う一連の業務



■インシデント発生から解決までの一連の業務

集合演習ではインシデントマネジメントの内、インシデントハンドリングについて学習します。

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。

集合演習舞台設定: Aコースの例

- みなさんは株式会社サイダーの従業員で、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。
- 情報システムのネットワーク運用、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。

株式会社サイダー

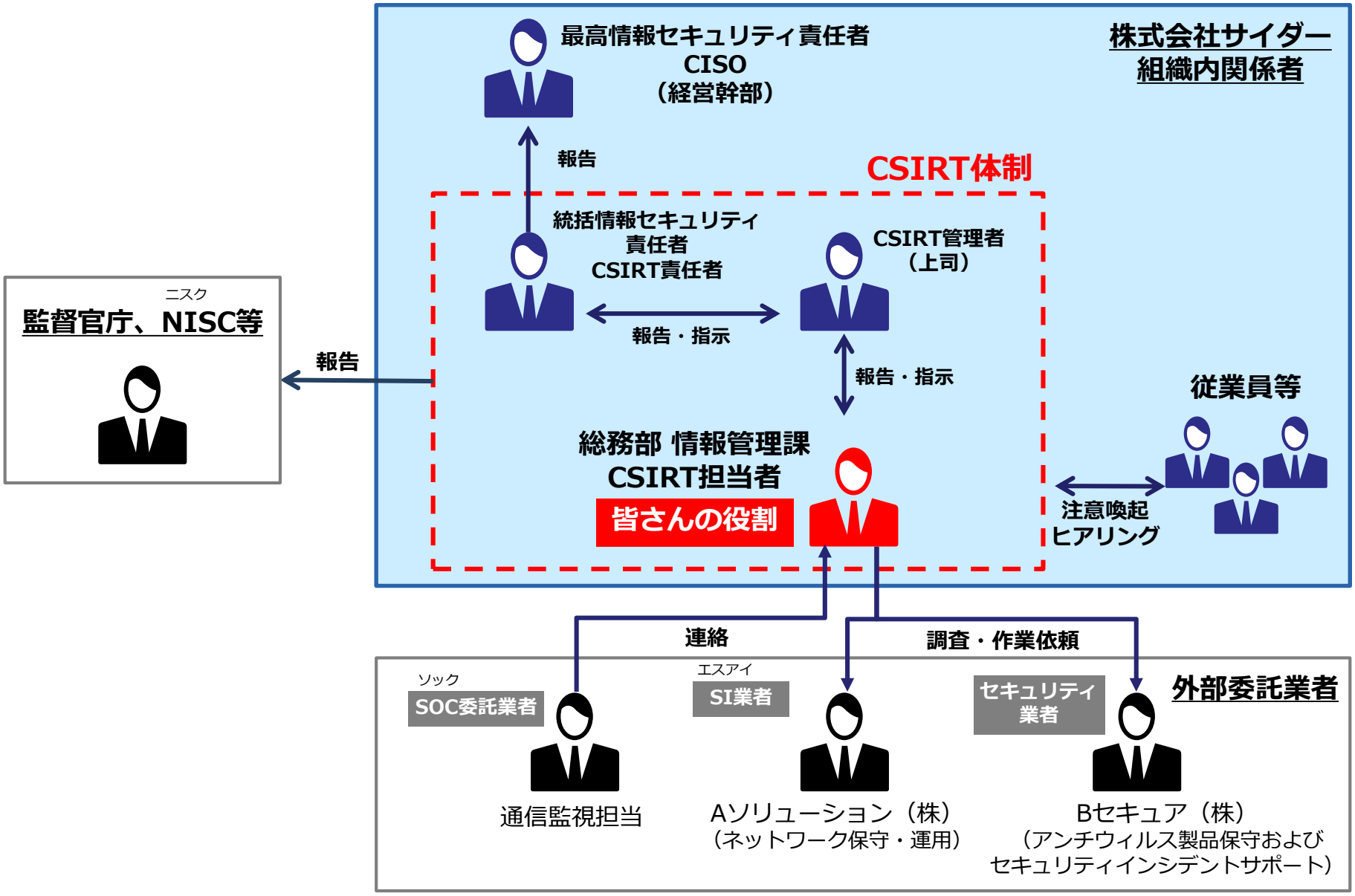
売上：16億円　従業員：245 人

株式会社サイダーは、日本国内で清涼飲料水の販売を行っており、昨今のサイバー攻撃の脅威の高まりを受け、内部ネットワークを3分割するネットワークの更改を完了したところである。

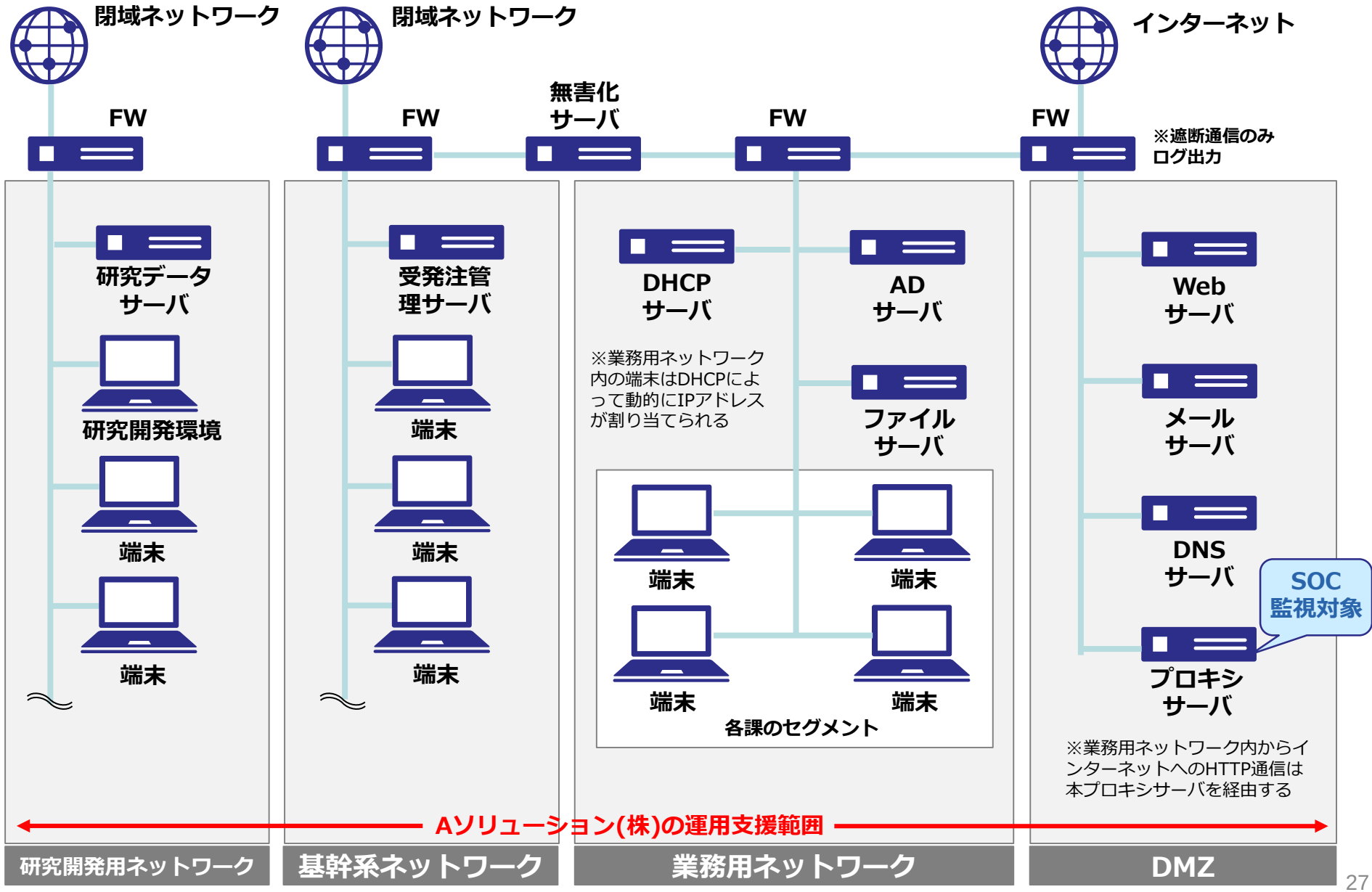
株式会社サイダーでは、仕入れを必要とする複数の商品の情報をシステムに入力し、取引先（卸売業やメーカーなど）に配送する。そのため、配送先顧客の個人情報など多くの機密情報を保有している。

また最近では、飲料水ボトルの研究開発に注力しており、国内複数の研究機関とも共同研究を行っている。

登場人物相関

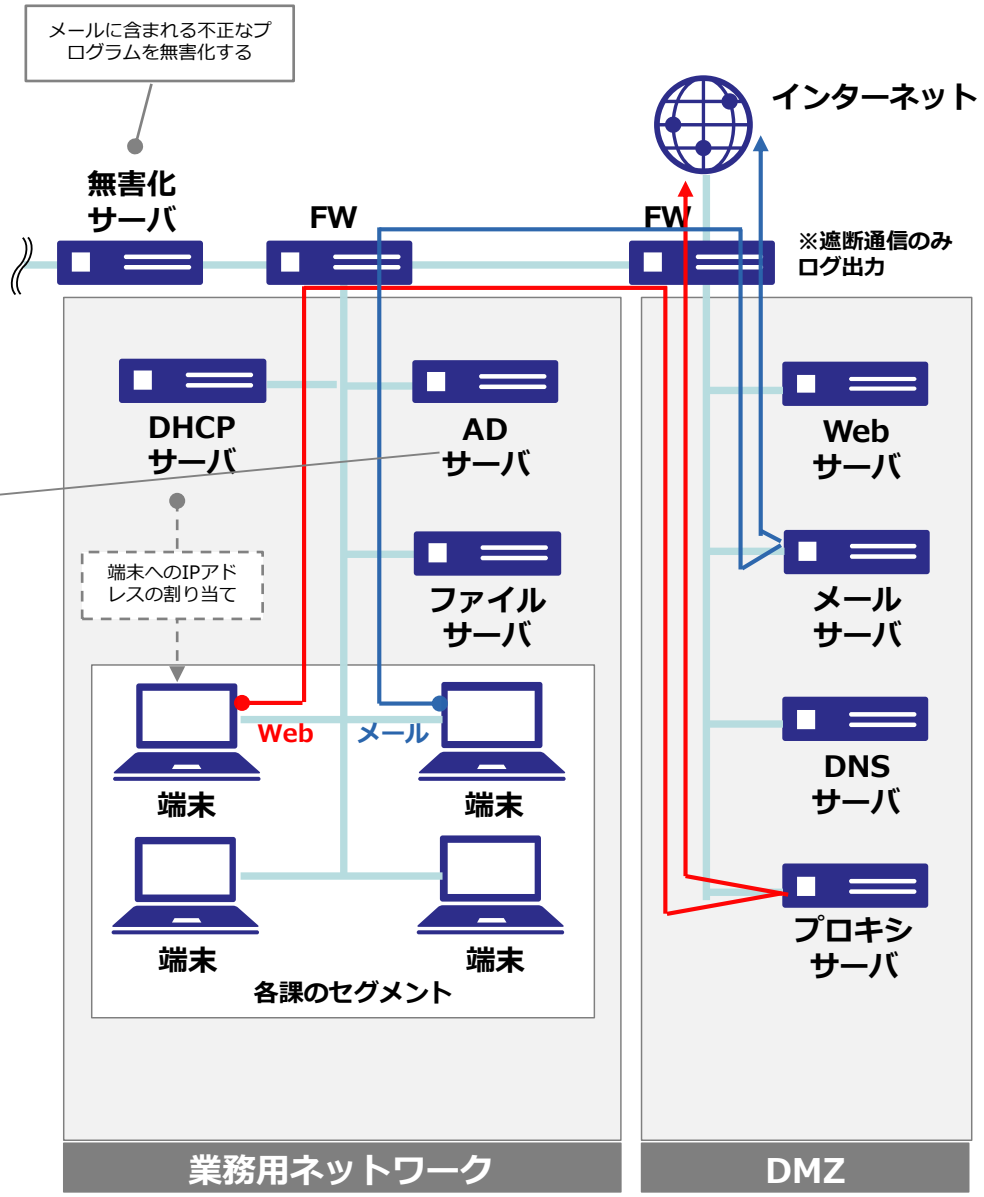

株式会社サイダー
組織内関係者
最高情報セキュリティ責任者
CISO
（経営幹部）
報告
CSIRT体制
統括情報セキュリティ
責任者
CSIRT責任者
CSIRT管理者
（上司）
報告・指示
報告・指示
監督官庁、NISC等
ニスク
報告
総務部 情報管理課
CSIRT担当者
皆さんの役割
従業員等
注意喚起
ヒアリング
連絡
調査・作業依頼
外部委託業者
ソック
SOC委託業者
通信監視担当
エスアイ
SI業者
Aソリューション（株）
（ネットワーク保守・運用）
セキュリティ
業者
Bセキュア（株）
（アンチウィルス製品保守および
セキュリティインシデントサポート）

ネットワーク構成


閉域ネットワーク
閉域ネットワーク
インターネット
FW
FW
無害化
サーバ
FW
FW
※遮断通信のみ
ログ出力
研究データ
サーバ
研究開発環境
端末
端末
受発注管
理サーバ
端末
端末
端末
DHCP
サーバ
AD
サーバ
※業務用ネットワーク
内の端末はDHCPによ
って動的にIPアドレス
が割り当てられる
ファイル
サーバ
端末
端末
端末
端末
各課のセグメント
Web
サーバ
メール
サーバ
DNS
サーバ
SOC
監視対象
プロキシ
サーバ
※業務用ネットワーク内からイ
ンターネットへのHTTP通信は
本プロキシサーバを経由する
Aソリューション(株)の運用支援範囲
研究開発用ネットワーク
基幹系ネットワーク
業務用ネットワーク
DMZ

サーバの役割

プロキシサーバ	クライアント端末の代わりにWebサーバなどに代理でアクセスするサーバ。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。
メールサーバ	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。
ADサーバ	同一のドメイン内にあるPCや機器を一括管理するサーバ。株式会社サイダー内のユーザやリソース、セキュリティポリシーなどを一括管理している。
DHCPサーバ	IPアドレスなどのネットワークの設定に必要な情報を自動的に割り当てるサーバ。業務用ネットワーク内の端末は、DHCPで動的にIPが割り当てられる。
DNSサーバ	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。
無害化サーバ	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プログラムを無害化するサーバ。



講師・チューターによるサポート

演習環境の不具合、課題に関する疑問・質問があった場合は、スタッフジャンパーを着用したチューターがサポートします。

例）

- ネットワークが不安定
- テキスト等の印刷物に不備がある
- ツールの使い方がわからない　等

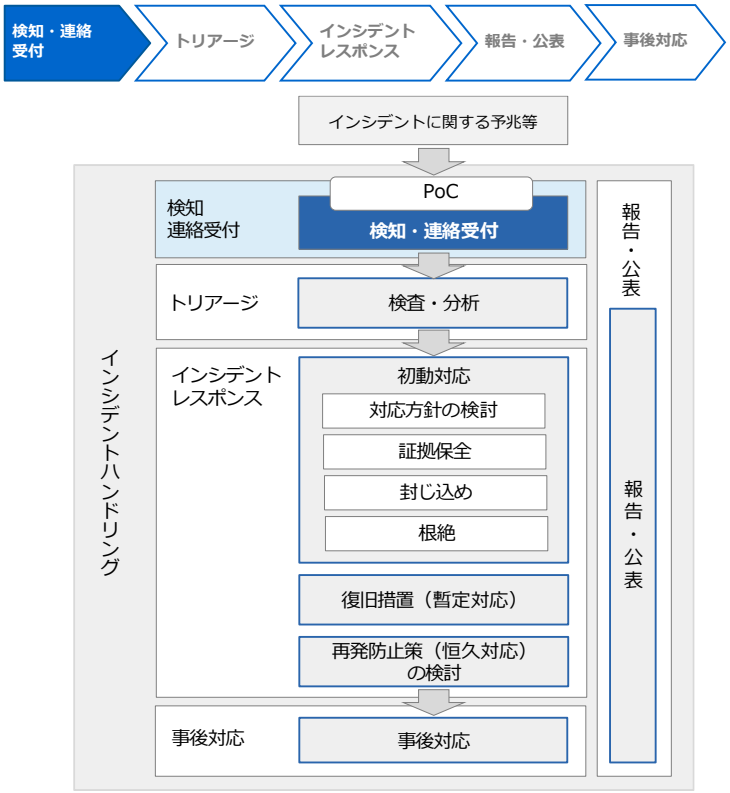
集合演習のマイルストーン: Aコースの例

課題	テーマ	課題概要
1	検知・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。

Aコースはステップ・バイ・ステップで進めていきます

検知・連絡受付



検知・連絡受付では

インシデント発生に関する予兆等の検知や連絡を受け付ける。

■検知・連絡の発信源（例）
- 監視システムからの異常検知アラーム
- SOC等、通信を監視している業者
- 組織内外からの通報（電話、メール）
- 組織外の例：JPCERT/CC、NISC

■ PoC(Point of Contact)
セキュリティに関する統一的な窓口

POINT

- 正しい発信源から通知されたか確認すること。
- 上位者へ第一報を報告すること。
- 従業員が予兆等を検知／発見したとき、あるいは外部から連絡を受けたときは、PoCへ伝達することを日頃から従業員に周知、理解させておくこと。
- ホームページなどでPoCの連絡先を公表してくこと。

検知・受付フェーズの課題例

状況説明

現在2019/02/08 12:00です。

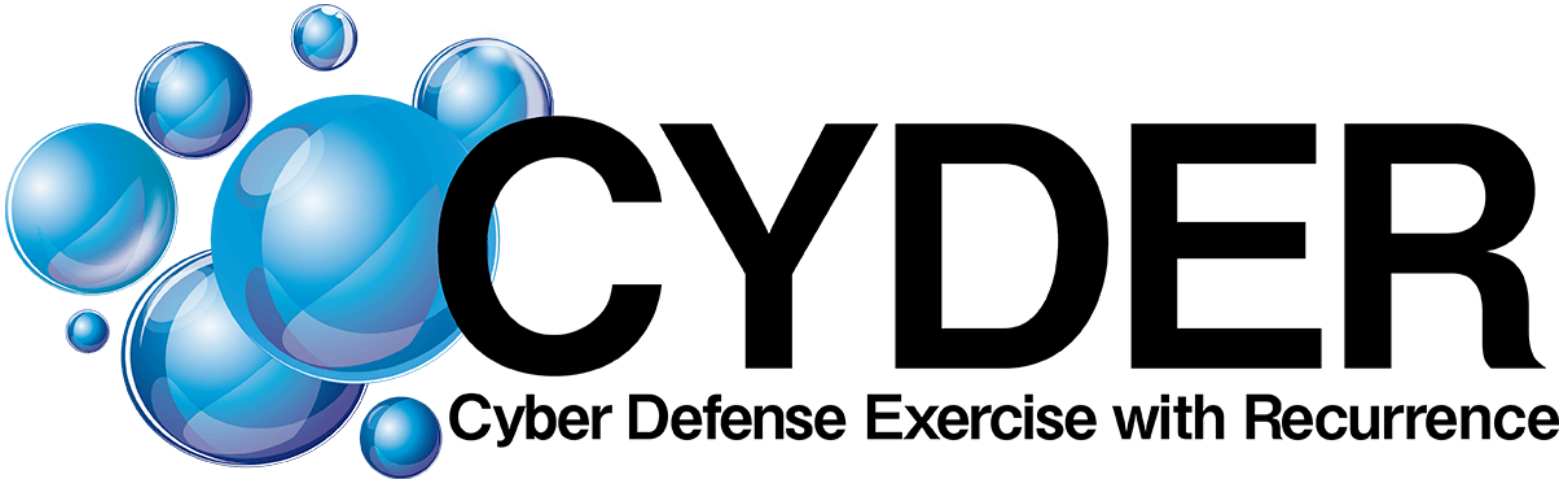
職員伊藤からCSIRTのPoCに、情報通信研究機構の職員を名乗る不審なメールを受信したとの通報メールが届きました。

それを受けてCSIRT管理者である上司から、不審なメールが情報通信研究機構から送信されたものであるかをすぐに確認してほしいと指示されました。

また、「CSIRT情シス担当」は、上司からの指示を受けて、メールの送受信経路について運用マニュアルを確認しました。

課題

不審メールが情報通信研究機構から送信されたものであるかを確認するために、どのような対応を取るべきかグループでディスカッションし、まとめてください。



集合演習体験

#CYDER

ディスカッション課題
【体験課題1】検知・受付

連絡受付に対する事実確認および対処

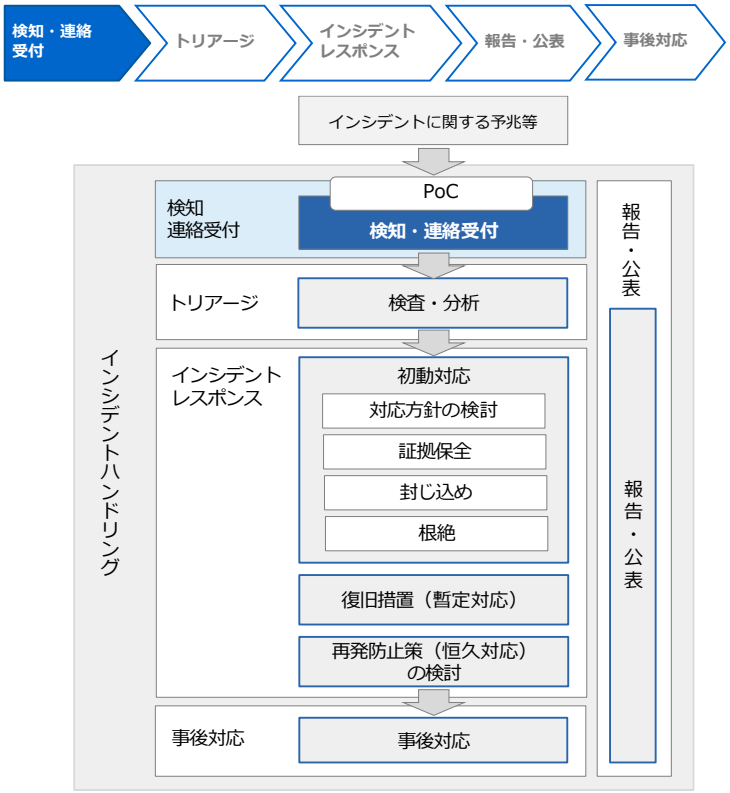
#CYDER

マイルストーン

課題	テーマ	課題概要
1	検知・受付	連絡受付に対する事実確認および対処 今ココ！
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。

検知・連絡受付



検知・連絡受付では

インシデント発生に関する予兆等の検知や連絡を受け付ける。

■検知・連絡の発信源（例）
- 監視システムからの異常検知アラーム
- SOC等、通信を監視している業者
- 組織内外からの通報（電話、メール）
- 組織外の例：JPCERT/CC、NISC

■ PoC(Point of Contact)
セキュリティに関する統一的な窓口

POINT

- 正しい発信源から通知されたか確認すること。
- 上位者へ第一報を報告すること。
- 従業員が予兆等を検知／発見したとき、あるいは外部から連絡を受けたときは、PoCへ伝達することを日頃から従業員に周知、理解させておくこと。
- ホームページなどでPoCの連絡先を公表してくこと。

【体験課題1】検知・受付

状況

現在2019/02/12 09:30です。
SOC委託業者の通信監視担当者から、一通の連絡メールが届きました。

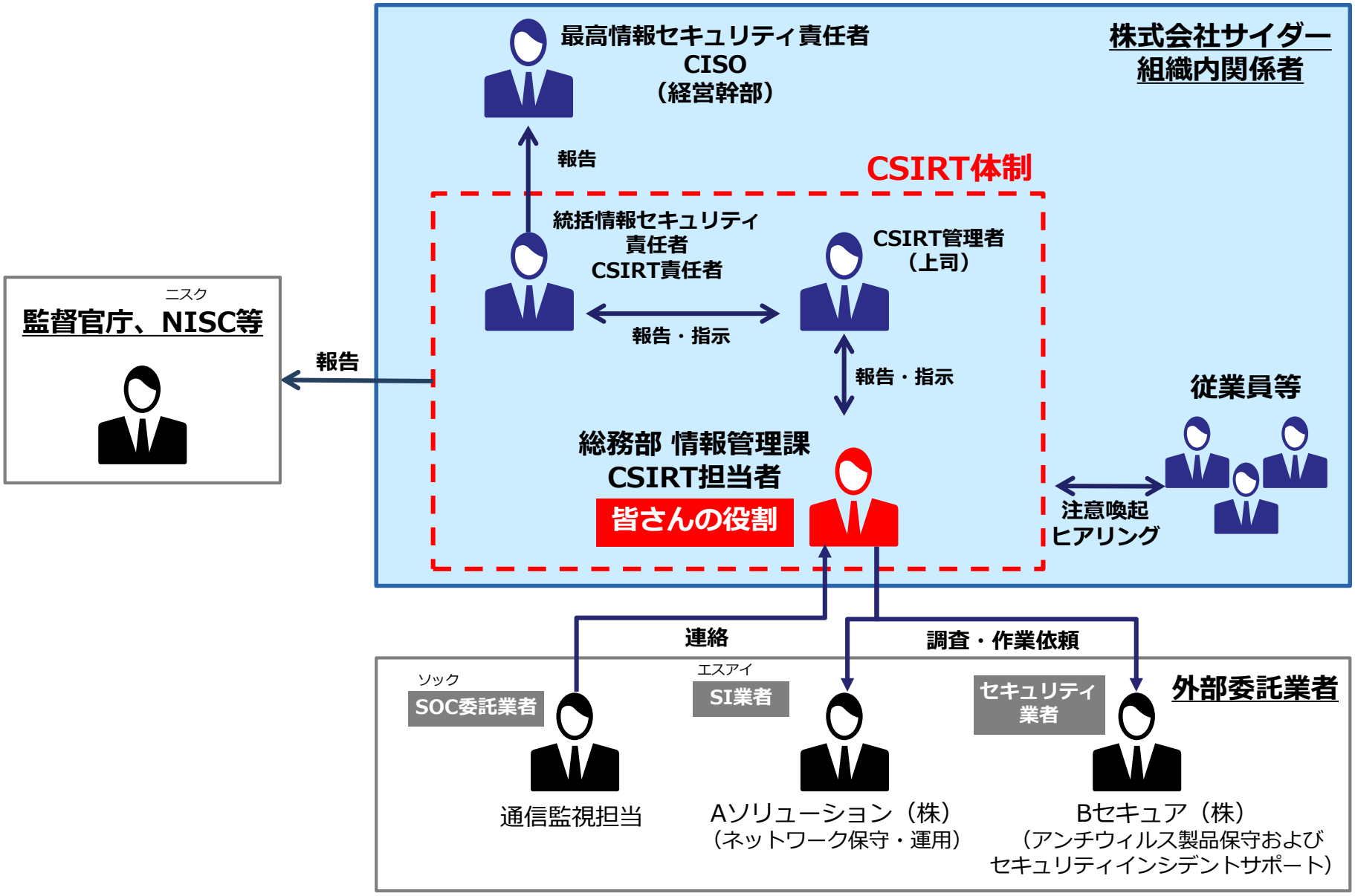
■SOCから連絡メール（抜粋）
貴組織のネットワークから C&C(Command & Control)サーバへの
通信を検知しました。通信の宛先を以下に示します。
マルウェア感染等のインシデント発生が懸念されますので、
早急な対処をお勧めいたします。
通信先 vulnerability.shop ポート番号 80

この連絡メールに関してインシデントハンドリングを開始します。

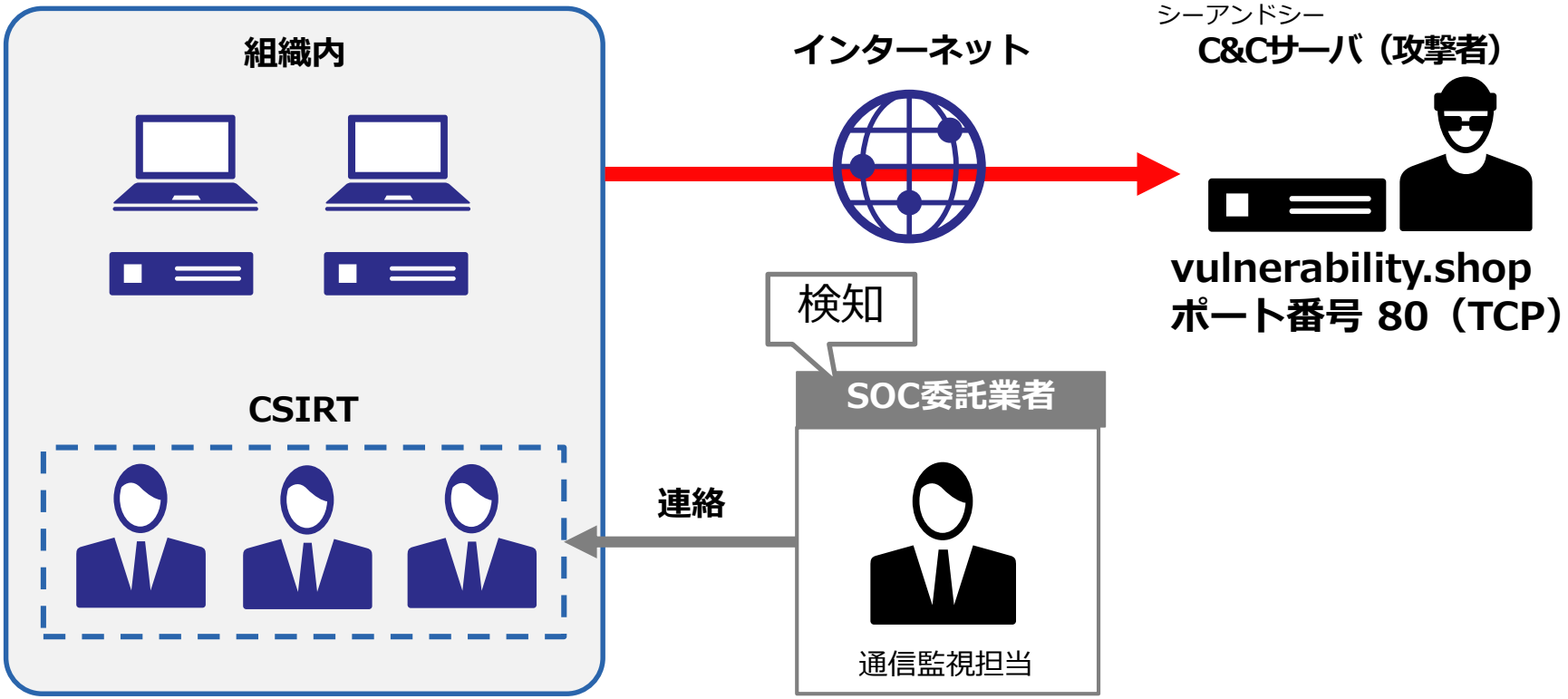
課題

この連絡メールに対して
CSIRTでどのような対応を行う必要があるか検討してください。

登場人物相関


株式会社サイダー
組織内関係者
最高情報セキュリティ責任者
CISO
（経営幹部）
報告
CSIRT体制
統括情報セキュリティ
責任者
CSIRT責任者
CSIRT管理者
（上司）
報告・指示
報告・指示
監督官庁、NISC等
ニスク
報告
総務部 情報管理課
CSIRT担当者
皆さんの役割
従業員等
注意喚起
ヒアリング
連絡
調査・作業依頼
外部委託業者
ソック
SOC委託業者
通信監視担当
エスアイ
SI業者
Aソリューション（株）
（ネットワーク保守・運用）
セキュリティ
業者
Bセキュア（株）
（アンチウィルス製品保守および
セキュリティインシデントサポート）

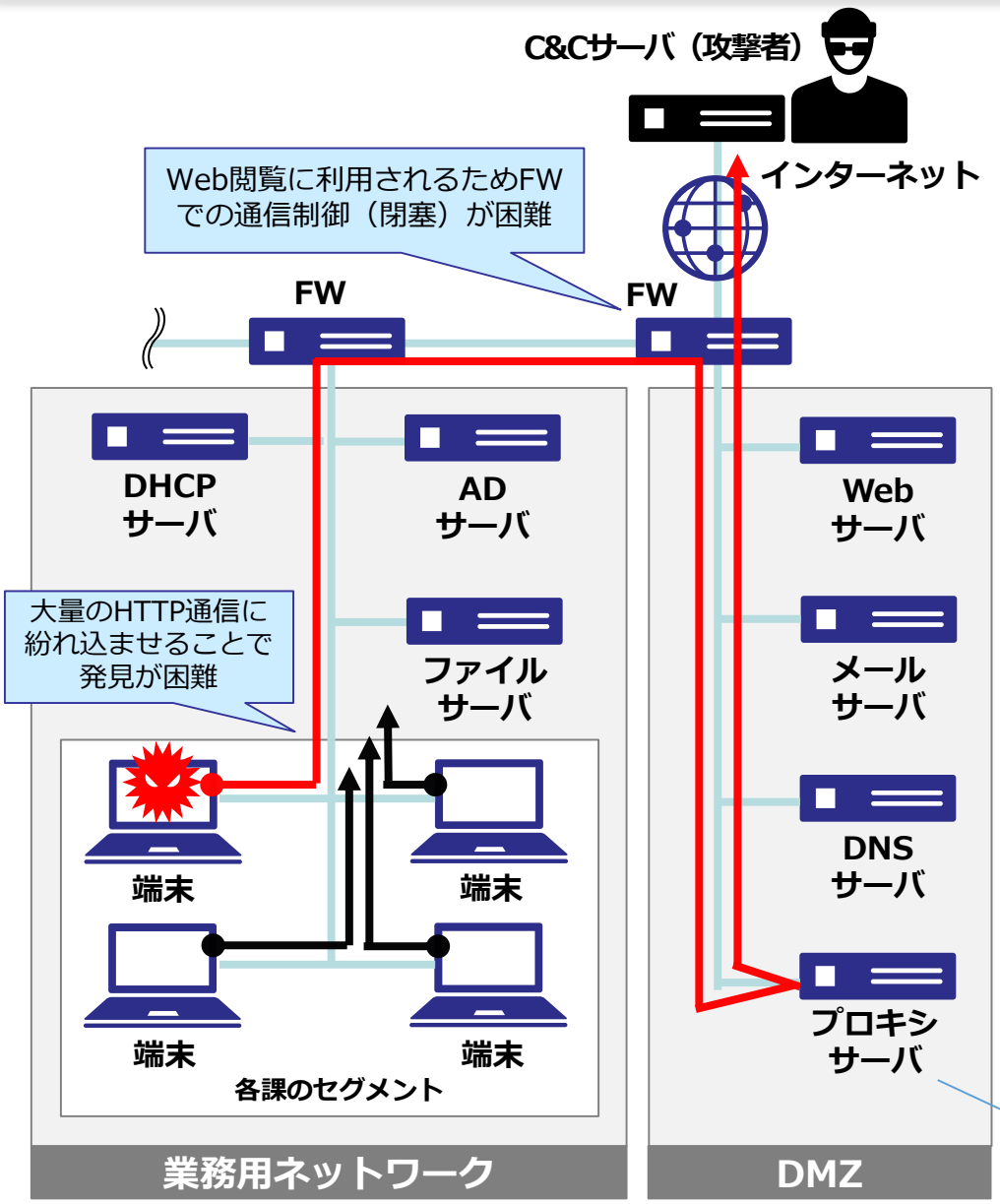
状況の整理



C&Cサーバ

「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のこと。「C2サーバ」と呼ばれることもある。

ポート80番によるC&Cサーバとの接続



なぜ攻撃者はC&Cとの接続に80/TCPを利用するのか？

TCPポート番号 **“80/TCP”** はWebサイトを閲覧する際に利用するプロトコル（HTTP）であり、併せてマルウェアがC&Cサーバとの通信に多く利用するポート番号である。

理由①
通常の業務でWebサイトへの接続が必要であることから、当該ポートをファイアウォールで閉塞することは困難であり、マルウェアとC&Cサーバとの接続が成功する可能性が高いため。

理由②
業務上行われる大量のHTTP通信にマルウェアからの通信を紛れ込ませることで発見を困難にする。

プロキシサーバ
内部ネットワークのセキュリティを守るために、クライアント端末の代わりにWebサーバなどに代理でアクセスするサーバ。また、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。

【体験課題1】検知・受付

状況

お席が近くの方とディスカッションしてみましょう！

現在2019/02/12 09:30です。
SOC委託業者の通信監視担当者から、一通の連絡メールが届きました。

■SOCから連絡メール（抜粋）
貴組織のネットワークから C&C(Command & Control)サーバへの
通信を検知しました。通信の宛先を以下に示します。
マルウェア感染等のインシデント発生が懸念されますので、
早急な対処をお勧めいたします。
通信先 vulnerability.shop ポート番号 80

この連絡メールに関してインシデントハンドリングを開始します。

課題

この連絡メールに対して
CSIRTでどのような対応を行う必要があるか検討してください。

解答・解説

【体験課題1】検知・受付（解答例1）

解答例

- **SOCからの連絡メールが「なりすまし」や「いたずら」ではないこと(真正性)について確認する。メールに書かれた連絡先ではなく、代表電話番号などに問い合わせる。**

- **上司(CSIRT管理者)へ、第一報として報告する。**
  - 連絡メールの真正性について確認後、上司に第一報として通報の内容と次のアクションについて報告します。
  - 検知や通報の内容によっては、すぐに「封じ込め」の対応を行うことも検討します。

【体験課題1】検知・受付（解答例2）

解答例

- **C&Cサーバへ通信している機器を特定する。**
  - C&Cサーバと通信している機器を特定する場合、プロキシサーバログを調査します。
    - 連絡メールによると、外部への通信はポート80を利用して行われています。当組織では、外部へのHTTP通信はすべてDMZに設置されたプロキシサーバを経由します。そのため、プロキシサーバログにて通信記録を確認することで、送信元IPアドレスを特定することができます。
    - 当組織では、各課セグメントにおいてDHCPサーバにより動的にIPアドレスが割り当てられているため、IPアドレスから端末を特定するためには、DHCPサーバのログと照合する必要があります。

【体験課題1】検知・受付（解答例3）

解答例

- **C&Cサーバへの通信を遮断する。**
  (ファイアウォールまたはプロキシサーバ)

  - マルウェア感染への対処として、既に判明している事実から対応策を検討します。
    この場合、C&Cサーバへの通信を遮断します。

【体験課題1】検知・受付（解答例4）

解答例

- **CSIRTで対応可能な範囲外は外部委託業者に協力を要請する。**
  - 連絡メールの事実関係について確認するため、Aソリューションにプロキシサーバログの調査を依頼する。
  - 被害状況や影響範囲等の事態の全体を把握し、優先順位を判断して対応します。このプロセスを「トリアージ」と呼びます。
    CSIRTで対応が困難であると判断した場合、まずは当該システムを開発、運用、保守している外部委託業者に協力を要請します。
    システムの開発、運用、保守を行っている業者では対応が困難である場合は、すみやかに外部の専門家(セキュリティベンダ)に協力を要請します。

【体験課題1】検知・受付（補足）

【インシデント発生時の窓口（PoC)】

- 「検知・連絡受付」を行うセキュリティに関する統一的な窓口は、PoC(Point of Contactの略)と呼ばれ、内外に周知、公表することが重要です。公表すべき内容は、所在地、対応時間、電話番号、FAX番号、メールアドレス等です。
- PoCには、CSIRTの「顔」として他のCSIRTとの信頼関係を構築したり、コミュニティとの情報共有の窓口としての役目も果たすとともに、あらかじめCSIRT間で取り決めたフローでは対応できないような「想定外の事態」が発生した場合の「柔軟性のある」連絡窓口としての役目もあります。
- JPCERT/CCなどの第三者から通報を受け付ける場合は、WHOISデータベースに登録されている技術連絡担当者、登録担当者のメールアドレス宛に連絡されることが通例となっています。

【参考情報】

- URLの調査活動は、攻撃者が調査活動に気づき活動を活発化させたり、攻撃に関わるサーバを破棄する事象があります。

他組織からの連絡

■ 組織内の機器がサイバー攻撃の被害に遭っていることが疑われる場合、他の組織から連絡が来る場合があります。

代表的な連絡元	説明
ジェーピーサートコーディネーションセンター JPCERT/CC	インターネットを介して発生する侵入やサービス妨害などのコンピュータセキュリティインシデントについて、日本国内を対象とする報告の受け付け、対応の支援や助言などを、技術的な立場から行う。
IPA サイバーレスキュー隊 ジェイ・クラート （J-CRAT）	サイバー攻撃の被害の発生が予見され、その対策の対応遅延が社会や産業に重大な影響を及ぼすと判断される組織などに対してエスカレーションや支援を行う。
ニスク NISC （内閣サイバーセキュリティセンター）	監視活動により認知された脅威を分析した結果、攻撃が行われたと認識され、当該政府機関等において対応が推奨される事案について、通報を行う。
ジェイリス J-LIS （地方公共団体情報システム機構）	地方公共団体が運営する組織として、住民基本台帳法、電子署名等に係る地方公共団体の認証業務及び行政手続における特定の個人を識別するための番号の利用等に関する事務、並びにその他の地方公共団体の情報システムに関する事務及び支援を行う。

※上記のような第三者から通報を受け付ける場合は、WHOISデータベースに登録されている技術連絡担当者、登録担当者のメールアドレス宛に連絡されることが通例となっています。

WHOIS
IPアドレスやドメイン名の登録者などに関する情報を、インターネットユーザーが誰でも参照できるサービス。

ハンズオン課題
【体験課題2】トリアージ（ログ調査）

事実確認のためのログ調査

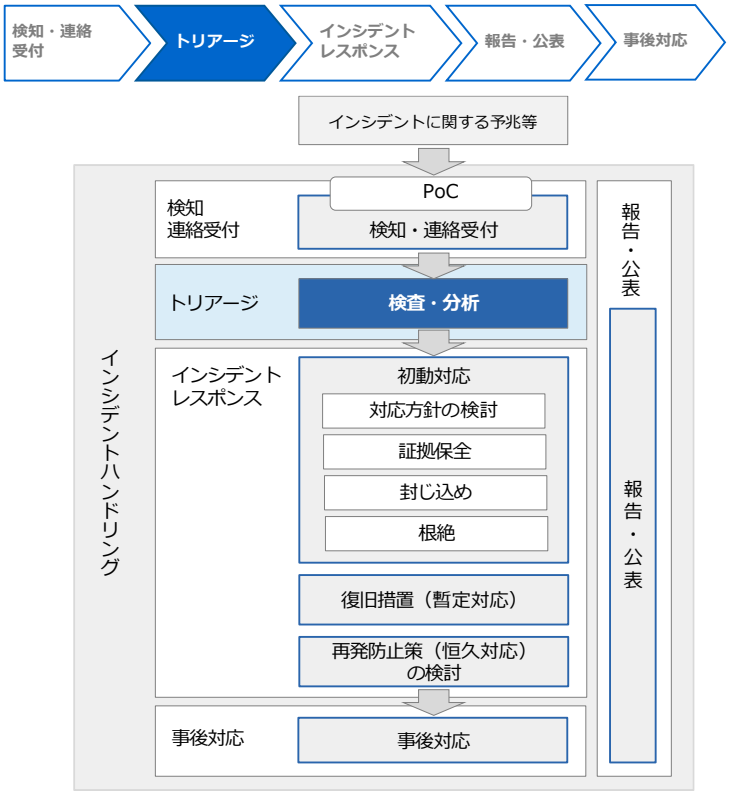
#CYDER

マイルストーン

課題	テーマ	課題概要
1	検知・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 今ココ！
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。

トリアージ（検査・分析）



トリアージ（検査・分析）では

ヒアリング、ログ検査・分析などで事実関係を確認する。
インシデントと判断した場合、被害状況と重要度に基づいて、対処の優先順位を付ける。

（例）複数のシステムから不審な通信が発生していることが発覚し、顧客情報を保有するシステムから優先して詳細を調査する。

➔優先順位を付けた後、
組織内の上位者へ状況報告する

POINT

- ヒアリングでは正確な情報を得られるよう、5W1Hを意識した質問項目を事前に用意する。
- ログ調査の依頼時、対象とするログと現時点で判明している情報（ドメイン、IPアドレス等）を明示し、何を確認したいのか目的を具体的に伝える。

【体験課題2】トリアージ（ログ調査）

状況

現在2019/02/12 15:30です。
上司への報告、およびAソリューションへのプロキシサーバログ調査依頼を行いました。
その後、Aソリューションより、ログの調査結果が報告されました。

■Aソリューションからのプロキシサーバログ調査結果要約
プロキシサーバログを調査した結果、C&Cサーバと通信しているIPアドレスは以下の通りでした。これらのIPアドレスから端末と、その使用者を特定する作業を早急に進めます。

通信元IPアドレスリスト

```
XXX.XXX.XXX.XXX
…
XXX.XXX.XXX.XXX
XXX.XXX.XXX.XXX
…
```

課題

■ハンズオン
Aソリューションが行ったプロキシサーバログ調査を行います。
C&Cサーバと通信しているIPアドレスをすべて特定してください。

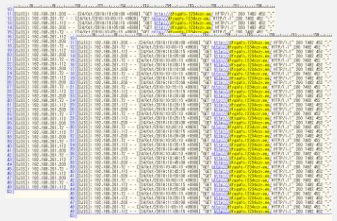
ログ調査

プロキシサーバのログ

- プロキシサーバを導入している場合、
  外部とのHTTP通信（Webを閲覧するための通信）はプロキシサーバを経由します。
- 多くの攻撃者は、マルウェアとC&Cサーバとの通信にHTTP通信を使用します。

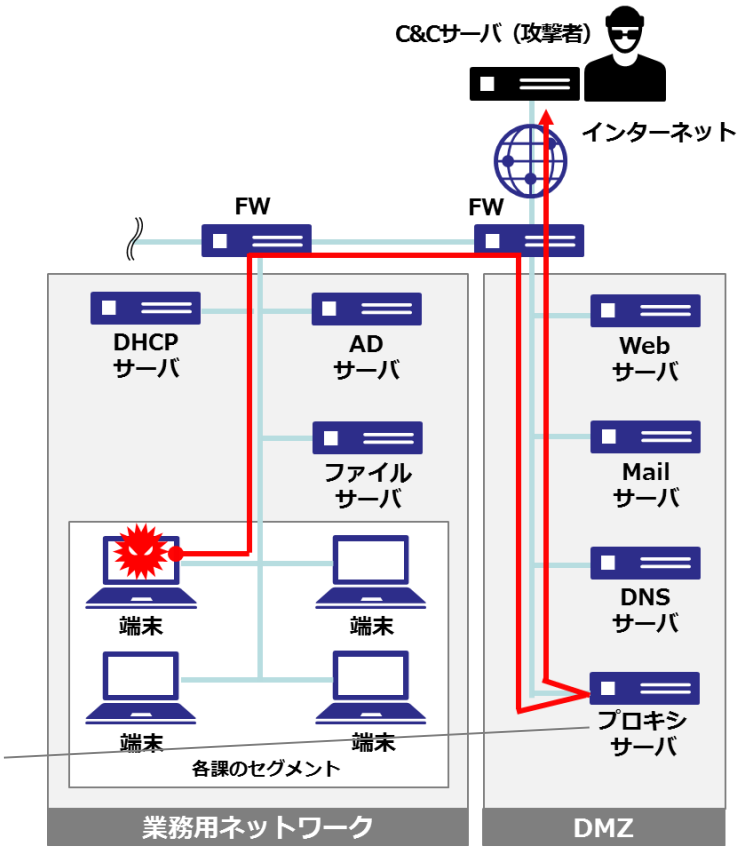
■ログの利用例

- **不正サイトへの通信の有無**
- **不正プログラム等からのアクセス有無**
- **外部サイトへのファイル等の**
  アップロードの有無



組織内から不審な通信が発生している場合、
プロキシサーバを経由して通信している場合は
当該端末を特定することができます。

プロキシサーバ
内部ネットワークのセキュリティを守るために、クライアント端末の代わりにWebサーバなどに代理でアクセスするサーバ。また、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。



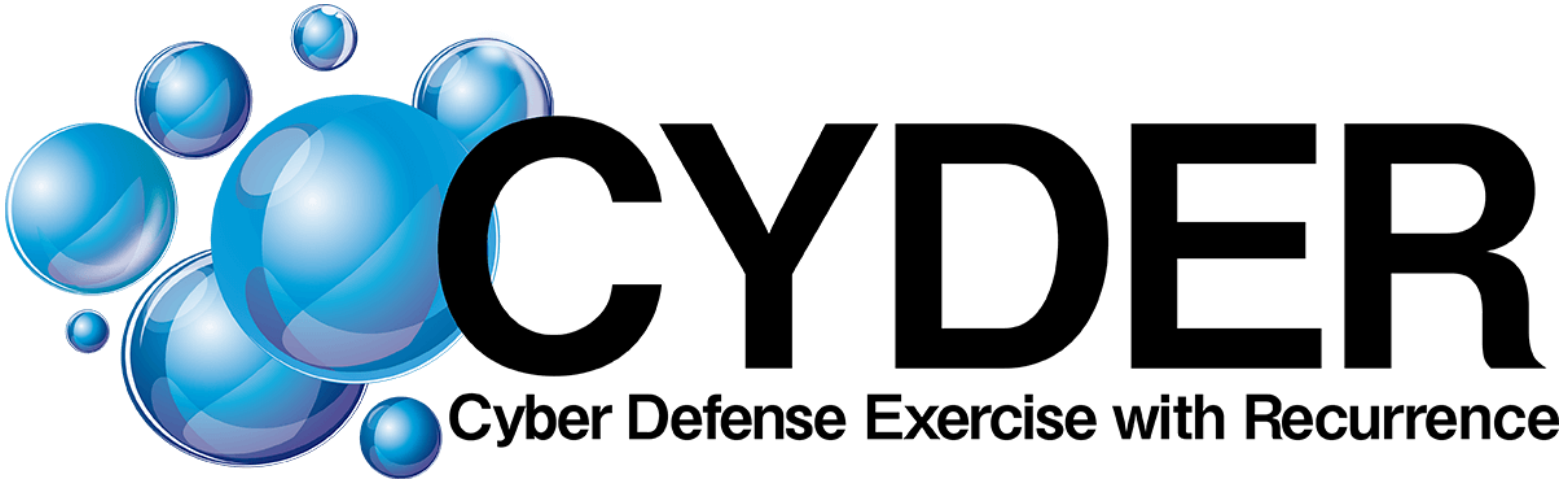
【体験課題2】トリアージ（ログ調査）

#CYDER

以降のフェーズは、集合演習を是非ご受講ください

課題	テーマ	課題概要
1	検知・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。



を支えるNICTの「強み」

#CYDER

Why NICT ?

NICTの「強み」

1. 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

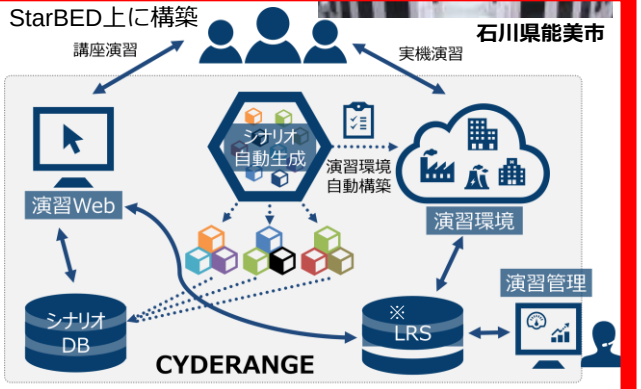
2. 大規模高性能サーバー群 NICT北陸StarBED技術センター

- **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の知見・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

3. 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

サイダーレンジ

CYDERANGE：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、かつ低コストな
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。

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

CYDERANGEの主要な機能

①演習シナリオ自動生成機能

- 演習シナリオをフェーズごとに分解し、フェーズ要素をシナリオのモジュールと見立て、モジュールを組み合わせて新たなシナリオを組み上げる仕組みにより、受講生のプロフィール (スキルレベル、産業分野等) にあわせたシナリオを自動生成する

②演習環境自動構築機能

- シナリオ自動生成機能によって生成された環境構築情報にもとづき、演習シナリオの舞台となる演習環境 (問題サーバ等も含む) を自動構築する

③最新の学習情報管理データベース対応

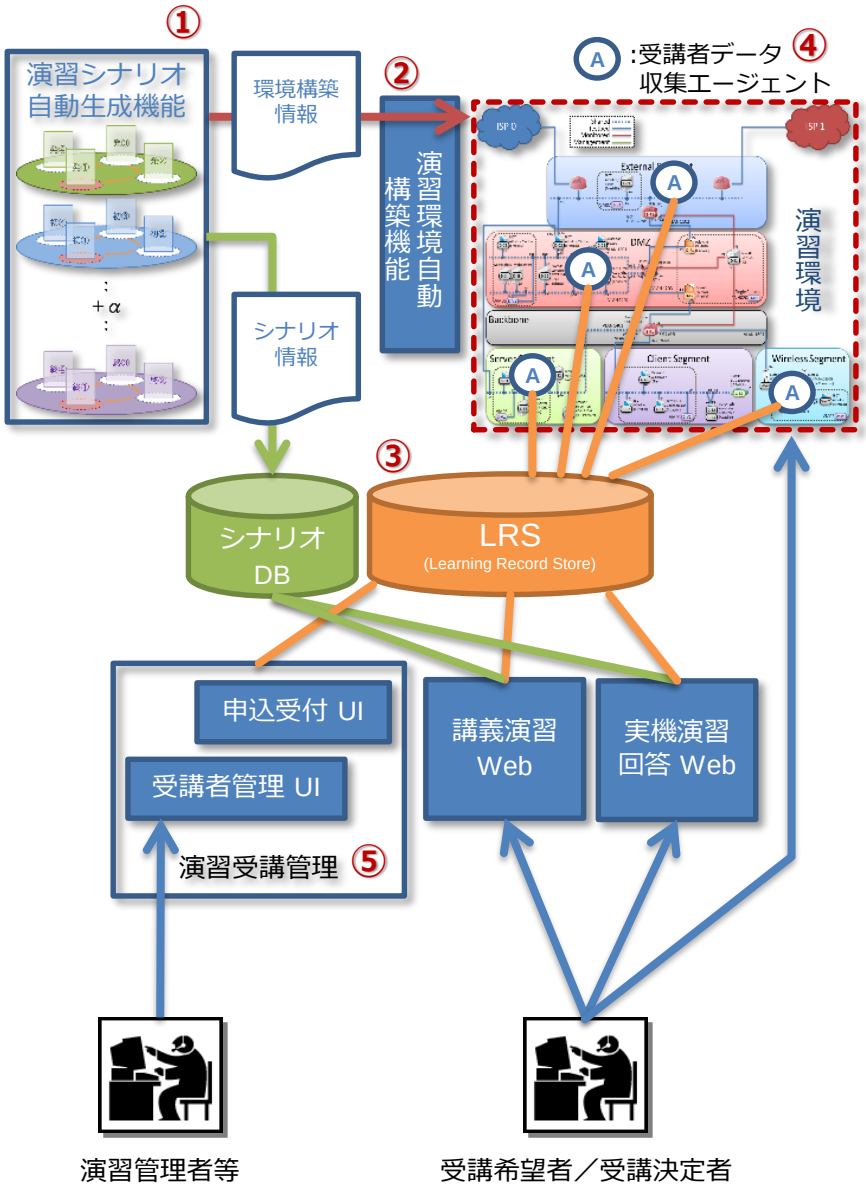
- 次世代の業界標準となる Learning Record Store (LRS) にいち早く対応し、詳細な受講者情報を収集・分析可能とする

④受講者データ収集エージェント

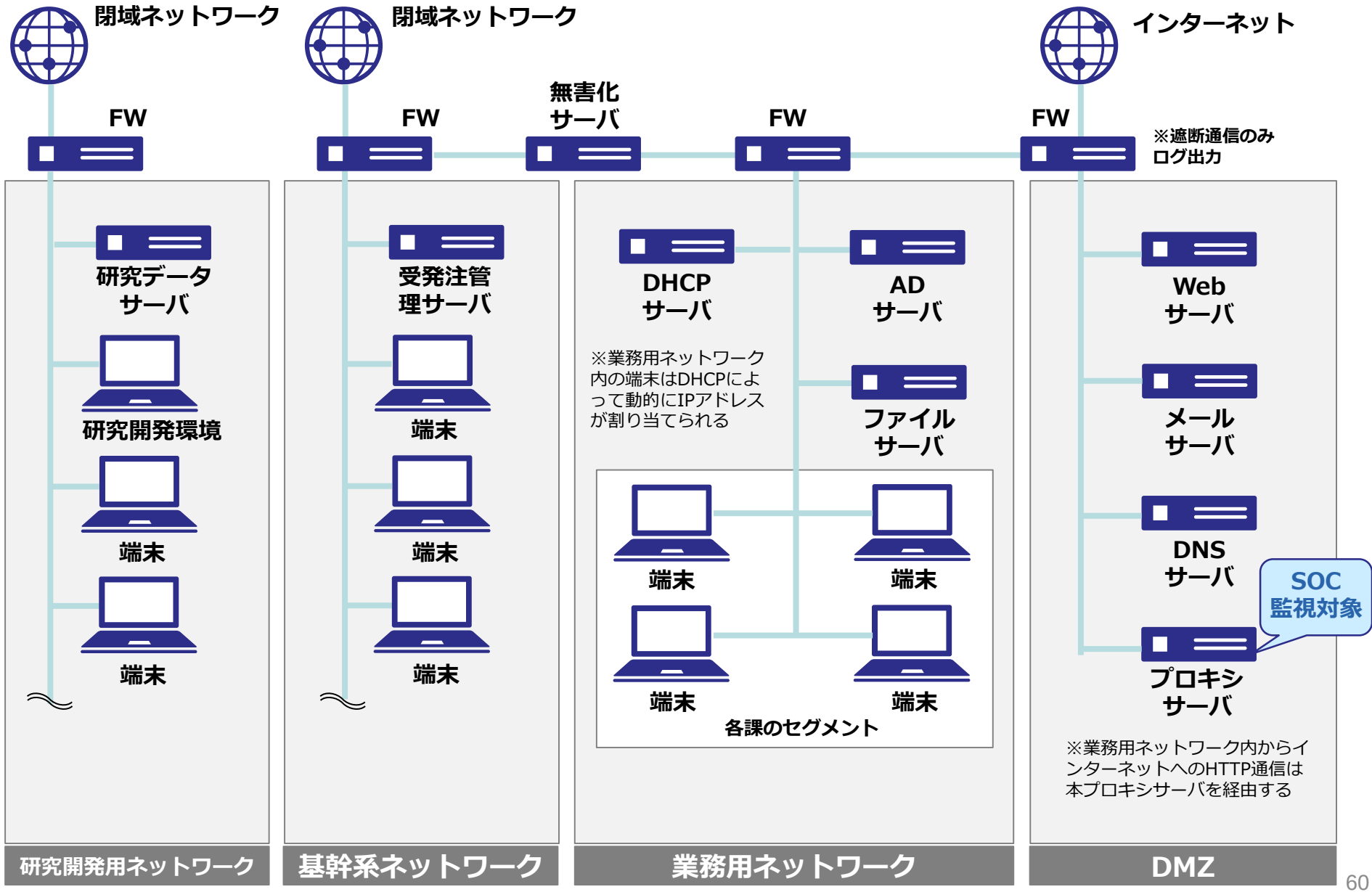
- キーロギング、マウス操作等、演習環境内における受講者のあらゆる行動をパーソナルデータの適切な取り扱いに配慮しつつ収集し、 LRS に蓄積するエージェント。ここで蓄積された情報を元に、受講者の行動分析を行う

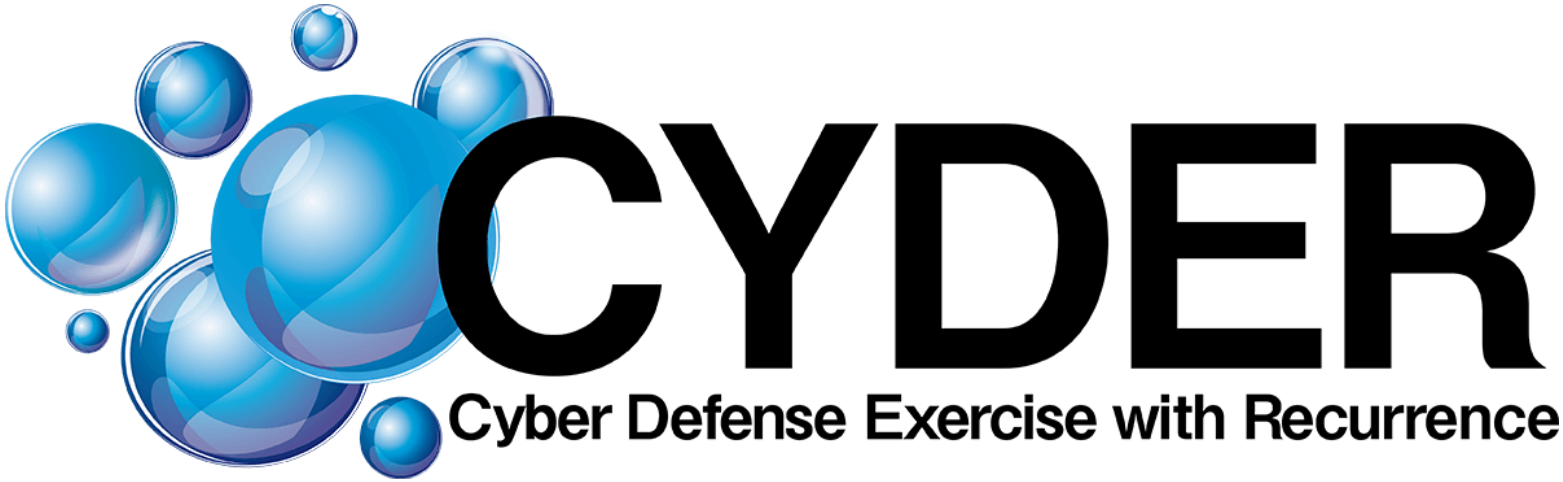
⑤演習受講管理機能

- 受講者を受付時点から LRS 上で統一的に管理する機能。受付を起点に複数年にまたがる受講者の追跡を可能とすることで、継続的な受講支援を行う



各グループに提供するネットワーク構成





よくあるご質問

#CYDER

質問1

Q.

- 以前CYDERを受講しました。内容は同じですか。

A.

- CYDER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**を準備しています。
  毎年受講していただくことにより、最新かつ様々な攻撃に対する対処法を学ぶことができます。

#CYDER

質問2

Q.

- 今年度までのCYDER を受講したことがあります。
  もう受講しなくてもよいですか。

A.

- 「有事」の対処能力は、日常業務を行っているだけでは、なかなか身につきません。
  インシデントが発生した際、「直ちに」「的確な」対応ができるように、「平時」からインシデント対応能力を十分に高めておく必要があります。
  インシデントハンドリングに必要な能力を習得できる
  「CYDER」を、繰り返し受講することをお勧めします。

#CYDER

質問3

Q.

- 時間が無くて受講できません。

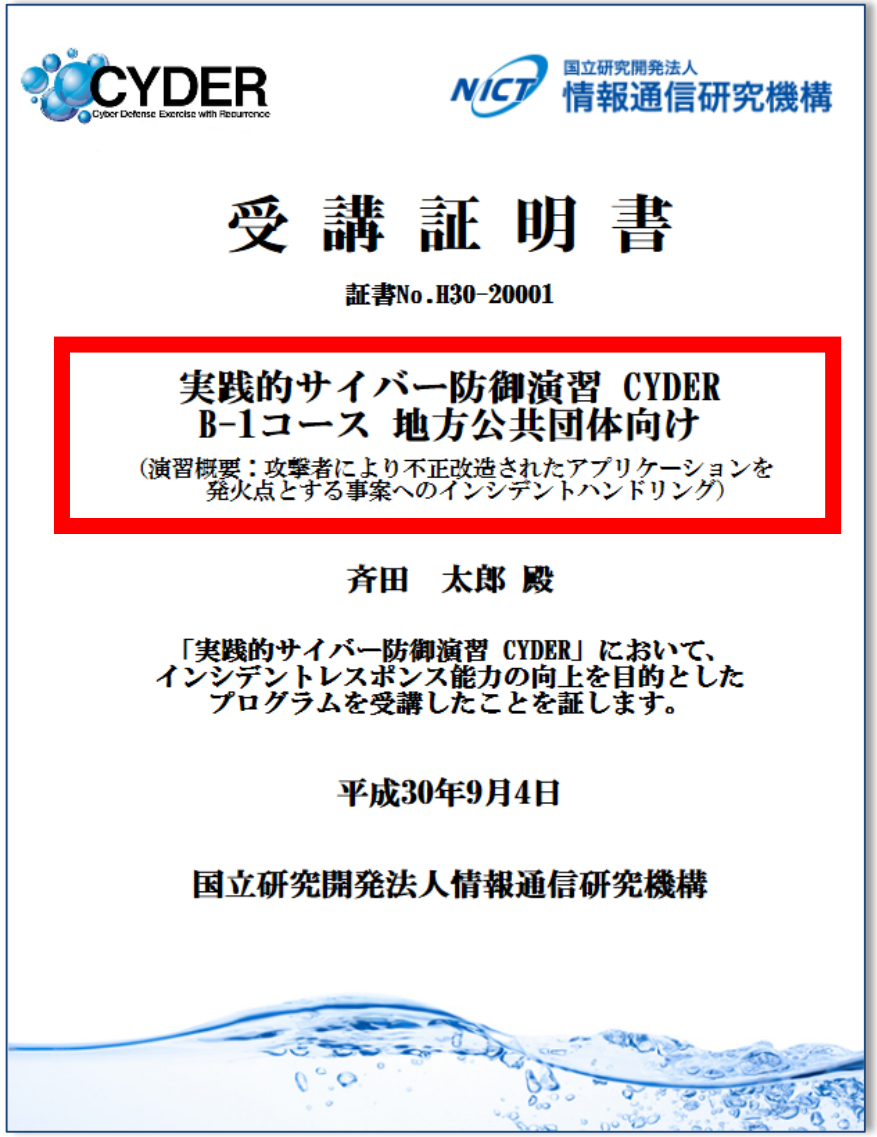
A.

- CYDERは、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**を構成しています。
  事前オンライン学習で1時間、集合演習で1日間、これで体験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。

CYDER受講証明書

CYDER受講後には、
- ●受講したコース
- ●演習の概要

を記載した**受講証明書**を発行します



CYDER
Cyber Defense Exercise with Recurrence

国立研究開発法人 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
B-1コース 地方公共団体向け
（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

「実践的サイバー防御演習 CYDER」において、
インシデントレスポンス能力の向上を目的とした
プログラムを受講したことを証します。

平成30年9月4日

国立研究開発法人情報通信研究機構

#CYDER

繰り返し受講の勧め

インシデントハンドリングはさまざま

セキュリティポリシー

導入システム

インシデント種類

絶対的な正解はない

集合演習の解説で行うこと

- 演習のインシデントに沿った課題についての解答例及び解説
- 演習だけでは伝えきれなかった補足説明
- 所属組織でインシデントハンドリングの準備をする際の参考情報

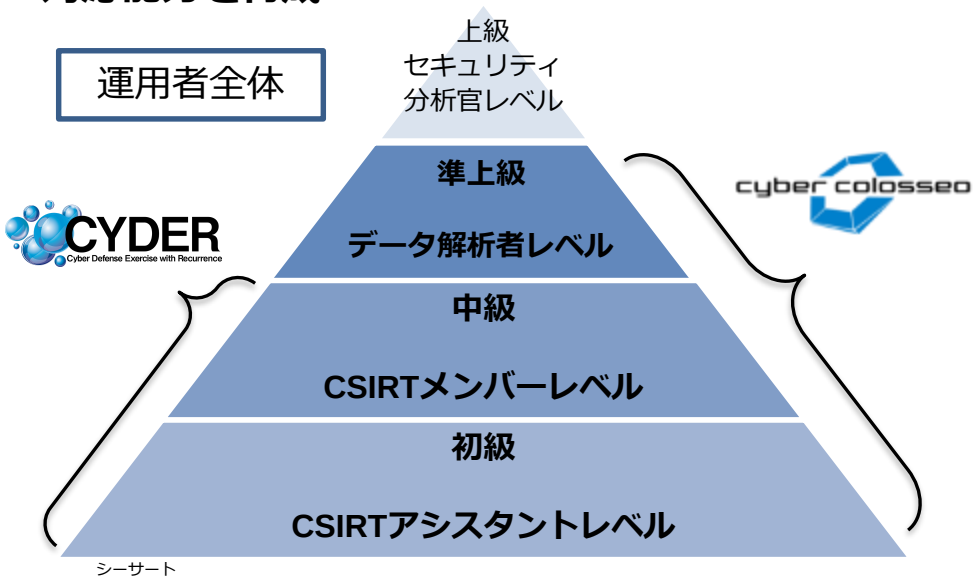
年度毎に学んだ内容を持ち帰り「組織の力」に！

まとめ:「ナショナルサイバートレーニングセンター」の取り組み

○ 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**する組織として、「ナショナルサイバートレーニングセンター」を設置（2017年4月1日）

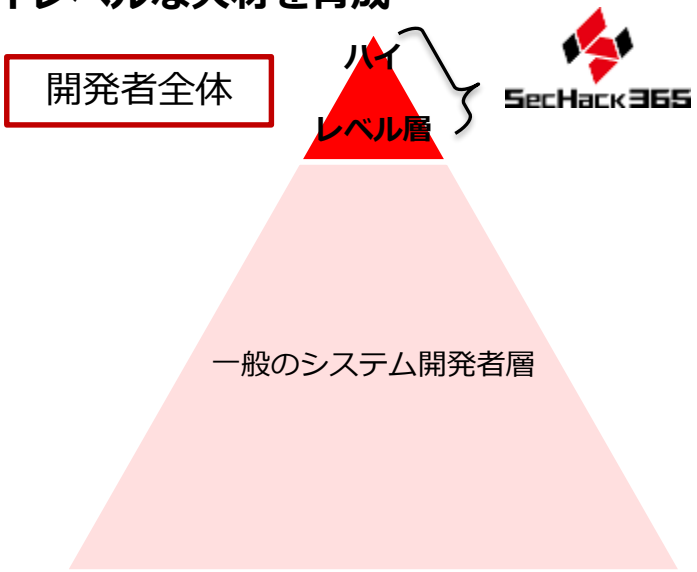
セキュリティオペレーター（実践的運用者）の育成

- ✓ **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**



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**



※CSIRT：Computer Security Incident Response Team

CYDER Webサイト - http://cyder.nict.go.jp/