参考資料

National Cyber Training Center

ナショナルサイバートレーニングセンターにおける セキュリティ人材育成の取組について

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

参考資料１

CYDER

CYDERの沿革

FY

2013 **総務省の実証実験としてスタート**
NICTは大規模演習環境を提供

2014

2015 **サイバーセキュリティ戦略** (閣議決定)
政府機関、重要インフラ等の実践的な演習・訓練のため、NICTが有する演習基盤や攻撃観測・分析に対する技術的知見を活用することとなった。

2016 **改正NICT法成立** (5 月施行)
CYDERの事業主体をNICTに変更することにより、安定的・継続的な運用を可能にするとともに、演習実施体制の大幅な強化を図ることとなった。

2017 **初級コース新設**　補助金としての総務省事業開始
地方公共団体からの要望を受け、初級Aコースを新設、併せて事前オンライン学習導入による演習日程の短縮を実施

2018 **サイバーセキュリティ戦略改定**（閣議決定）
国や関係機関は、官民の枠を超えた様々な規模の主体の間での訓練・演習を引き続き実施し、必要に応じて対象の拡大や内容の改善を図るなど、発展させていくとされた。

民間企業等からの受講者受け入れ開始
重要インフラを含む民間企業を有料で受け入れ

2019 **国の機関での未受講組織実質ゼロ※を達成**
※「実質ゼロ」は独法等を含まない。

2020 **コロナ禍における緊急的措置として無料で教材を提供**
開催場所に依存しにくい新たな訓練方式（オンライン演習）を段階的に導入開始

2021 **準上級コース新設、オンラインコース正式提供開始**
サイバーコロッセオのレガシーを活用し、準上級Cコースを新設。また、オンライン演習について、クローズドβ、オープンβでのテストを経て、オンラインコースの正式提供を開始した。

受講対象組織一覧

国の機関（30組織）	内閣官房/内閣法制局/人事院/内閣府/宮内庁/公正取引委員会/警察庁/個人情報保護委員会/カジノ管理委員会/金融庁/消費者庁/復興庁/デジタル庁/総務省/法務省/外務省/財務省/文部科学省/厚生労働省/農林水産省/経済産業省/国土交通省/環境省/防衛省/会計検査院/衆議院事務局/参議院事務局/国立国会図書館/最高裁判所/日本銀行	
独立行政法人（87組織）	**内閣府**	国立公文書館、北方領土問題対策協会、日本医療研究開発機構
	消費者庁	国民生活センター
	総務省	情報通信研究機構、統計センター、郵便貯金簡易生命保険管理・郵便局ネットワーク支援機構
	外務省	国際協力機構、 国際交流基金
	財務省	酒類総合研究所、造幣局、国立印刷局
	文部科学省	国立特別支援教育総合研究所/大学入試センター/国立青少年教育振興機構/国立女性教育会館/国立科学博物館/物質・材料研究機構/防災科学技術研究所/量子科学技術研究開発機構/国立美術館/国立文化財機構/教員研修センター/科学技術振興機構/日本学術振興会/理化学研究所/宇宙航空研究開発機構/日本スポーツ振興センター/日本芸術文化振興会/日本学生支援機構/海洋研究開発機構/国立高等専門学校機構/大学改革支援・学位授与機構/日本原子力研究開発機構
	厚生労働省	医薬基盤・健康・栄養研究所/労働者健康安全機構/勤労者退職金共済機構/高齢・障害・求職者雇用支援機構/福祉医療機構/国立重度知的障害者総合施設のぞみの園/労働政策研究・研修機構/国立病院機構/医薬品医療機器総合機構/地域医療機能推進機構/年金積立金管理運用/国立がん研究センター/国立循環器病研究センター/国立精神・神経医療研究センター/国立国際医療研究センター/国立成育医療研究センター/国立長寿医療研究センター
	農林水産省	農林水産消費安全技術センター/家畜改良センター/水産研究・教育機構/農業・食品産業技術総合研究機構/国際農林水産業研究センター/森林研究・整備機構/農畜産業振興機構/農業者年金基金/農林漁業信用基金
	経済産業省	経済産業研究所/工業所有権情報・研修館/産業技術総合研究所/製品評価技術基盤機構/新エネルギー・産業技術総合開発機構/日本貿易振興機構/情報処理推進機構/石油天然ガス・金属鉱物資源機構/中小企業基盤整備機構
	国土交通省	土木研究所/建築研究所/海上・港湾・航空技術研究所/海技教育機構/航空大学校/自動車技術総合機構/鉄道建設・運輸施設整備支援機構/国際観光振興機構/水資源機構/自動車事故対策機構/空港周辺整備機構/都市再生機構/奄美群島振興開発基金/日本高速道路保有・債務返済機構/住宅金融支援機構
	環境省	国立環境研究所、環境再生保全機構
	防衛省	駐留軍等労働者労務管理機構
指定法人（9組織）	サイバーセキュリティ基本法第13条の規定に基づき、サイバーセキュリティ戦略本部が指定する法人 (以下の９法人) 地方公共団体情報システム機構/地方公務員共済組合連合会/地方職員共済組合/都職員共済組合/全国市町村職員共済組合連合会/国家公務員共済組合連合会/日本私立学校振興・共済事業団/公立学校共済組合/日本年金機構	
地方公共団体	都道府県、市町村など	
重要社会基盤事業者	国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生じるものに関する業務を行う者 (以下の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	
民間企業等		

NICTによる実践的サイバー演習の対象となる領域

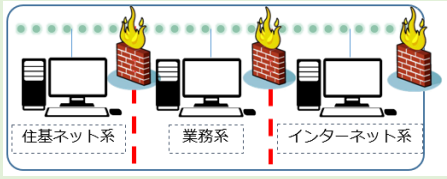
NICTが実施する実践的サイバー演習では、行政機関や民間企業等が講じる必要のある様々なセキュリティ対策のうち、 NICTの有する大規模演習環境及び長年のサイバーセキュリティ研究による知見を活かした実践的なトレーニングを担当

NICTによるセキュリティオペレーターの育成
～①大規模高性能サーバー群StarBED / サイバー演習自動化システムCYDERANGE～

NICT北陸StarBED技術センター (石川県能美市) に設置された大規模高性能サーバー群「StarBED」上に構築した、サイバー演習自動化システム「CYDERANGE」を活用し、サイバートレーニング用に大規模組織のネットワーク環境を再現した仮想ネットワーク環境を自動構築

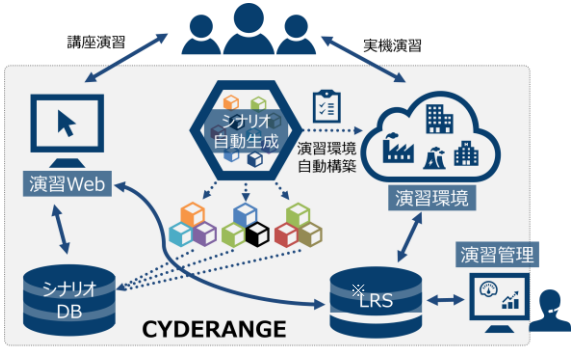
日本国内ではほぼ唯一の、国産の大規模なサイバーレンジ (演習環境)

大規模組織を模したネットワーク環境をサーバー内に構築



仮想自治体「さいだ市」など

StarBED 上に CYDERANGE を構築



※ Learning Record Store (履歴データベース)

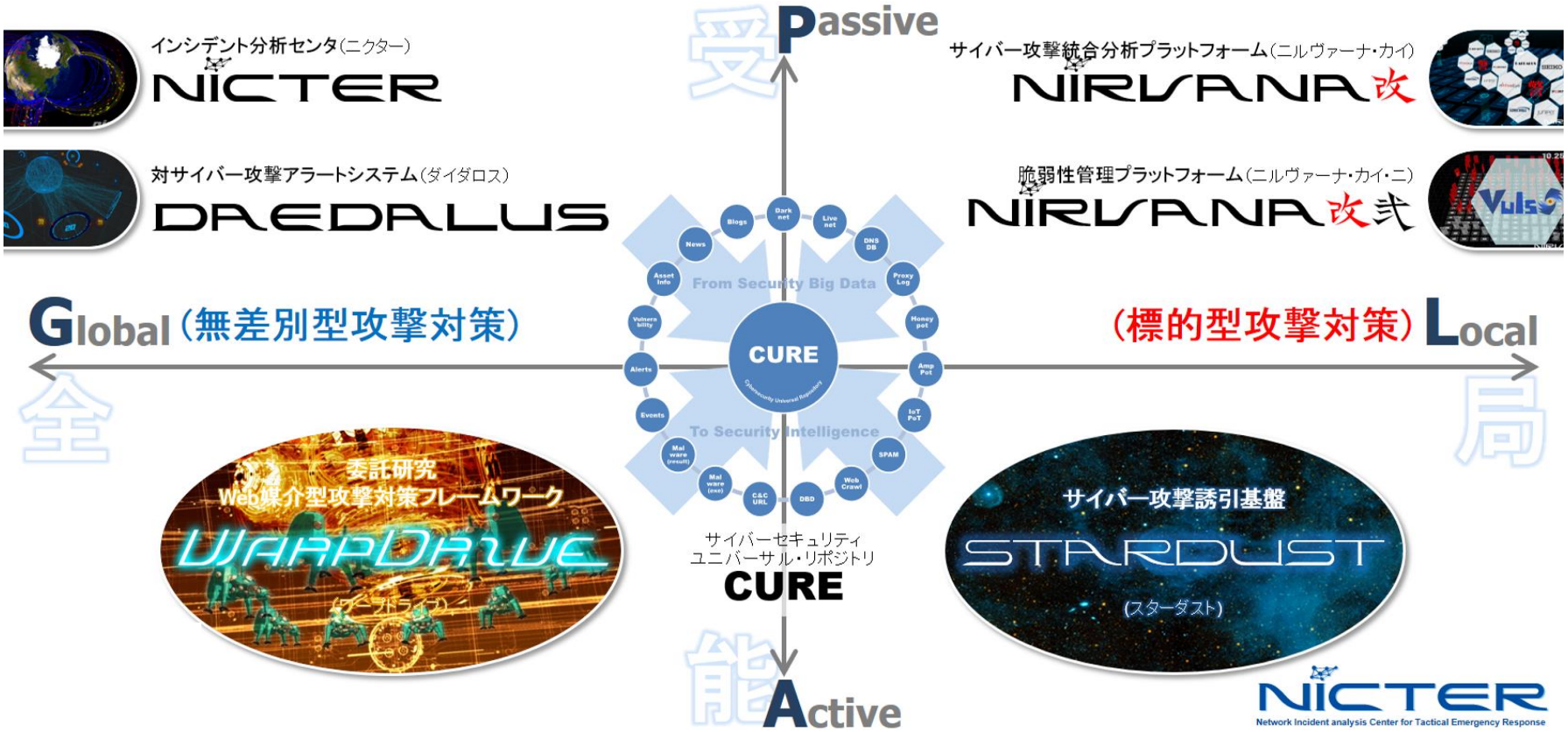
- **大規模性**
  大規模な組織のネットワーク環境を再現した仮想環境を構築するための大規模なサーバー群
- **運営ノウハウの蓄積**
  大規模仮想環境の効率的かつ安定的な運営に関する高度な知見・ノウハウの蓄積
  例) 大規模かつリアルな演習環境の効率的・迅速な環境構築技術、多数端末の同時並行運用技術 等
  2018年度からは、NICTナショナルサイバートレーニングセンターが独自に開発したサイバー演習自動化システム“CYDERANGE”の実運用を開始
- **セキュアな環境**
  インターネット等から隔離された強固な閉鎖環境

※NICTは、2002年から、大規模なネットワークシミュレーション等を行う実験施設として、多数のサーバー群からなる常設のテストベッド環境「StarBED」を構築し、運用開始。その後も順次、規模等を拡大
→StarBED活用事例：P2P型ファイル共有ソフトのトラヒック検知関係実験、クラウドコンピューティング技術の試験環境実験、8K非圧縮対応の映像蓄積配信ノード性能評価実験 等多数

NICTによるセキュリティオペレーターの育成
～②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

※ CYDERは、日本国内ではほぼ唯一の、国産の大規模なサイバーレンジを使用した演習であり、我が国固有のサイバー攻撃事例を踏まえたシナリオを導入することも可能である。例えば、主に日本国内において普及しているソフトウェアの脆弱性を突いた攻撃の実例をベースに演習シナリオを作成するといった取組みも実施している



CYDERANGE（サイダーレンジ）：サイバー演習自動化システム

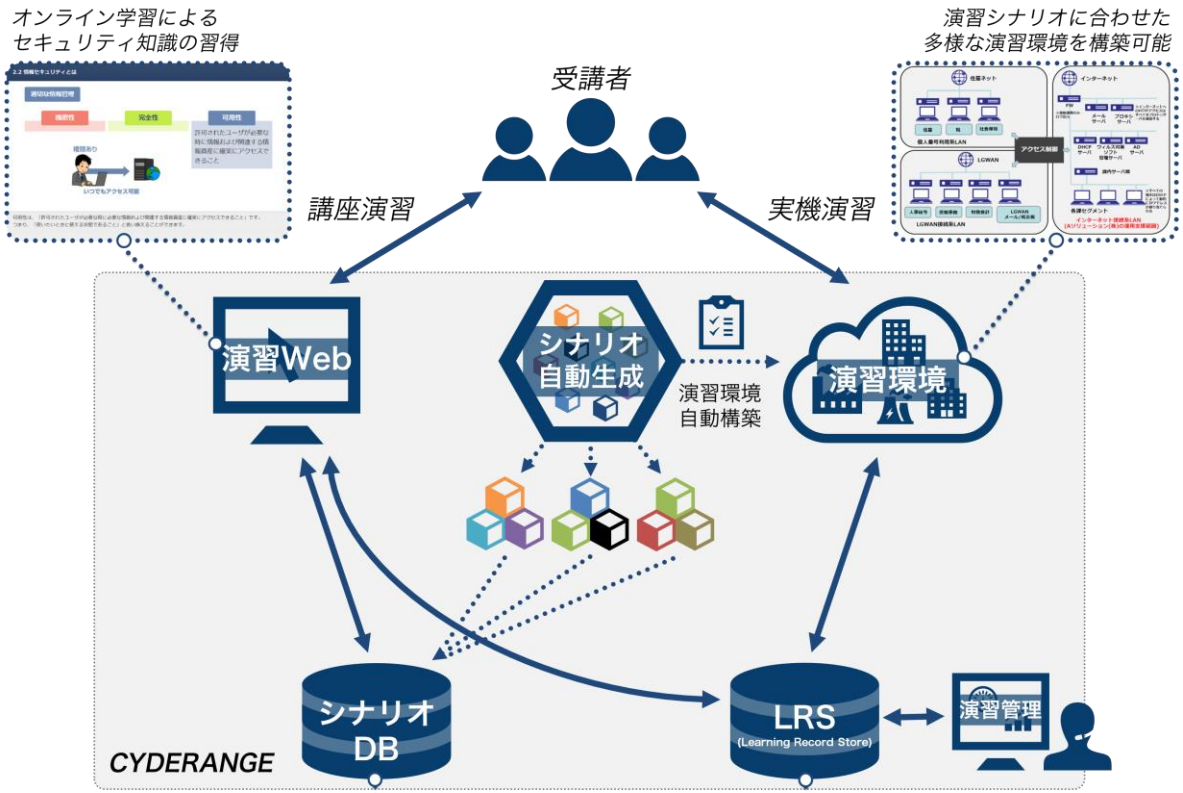
NICTナショナルサイバートレーニングセンターは、より効率的なサイバー演習を実現するサイバー演習自動化システム “CYDERANGE” を独自に開発。これまでのサイバー演習では、演習プログラムの作成ごとにシナリオや演習環境を手作業で作成することが一般的であったが、この CYDERANGE の開発により、演習シナリオの自動生成等が可能となった (2018年度から実運用を開始)

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

CYDERANGE：サイバー演習自動化システム

CYDERANGE (サイダーレンジ) 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行うためのサイバー演習自動化システムを2018年度から導入し、演習を実施



- 各フェーズ (インシデント発見、初動対応等) の要素を組み合わせ、受講者のプロフィール (スキルレベル等) に応じた演習シナリオを自動生成
- 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基づき、演習環境も自動で構築可能

- 教育・演習データ記録方式の世界規格である Experience API (xAPI) を用いたLRSを構築
- 演習時の受講者の行動 (キー入力、マウス操作、ウィンドウ操作等) を収集し、行動分析が可能
- LRSを利用した統一的な演習受講管理を実現

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

CYDER
RPCI
SecHack365

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
Cコース：高いレベルでのインシデントハンドリング/レスポンスをコントロールする能力を身につけたい方

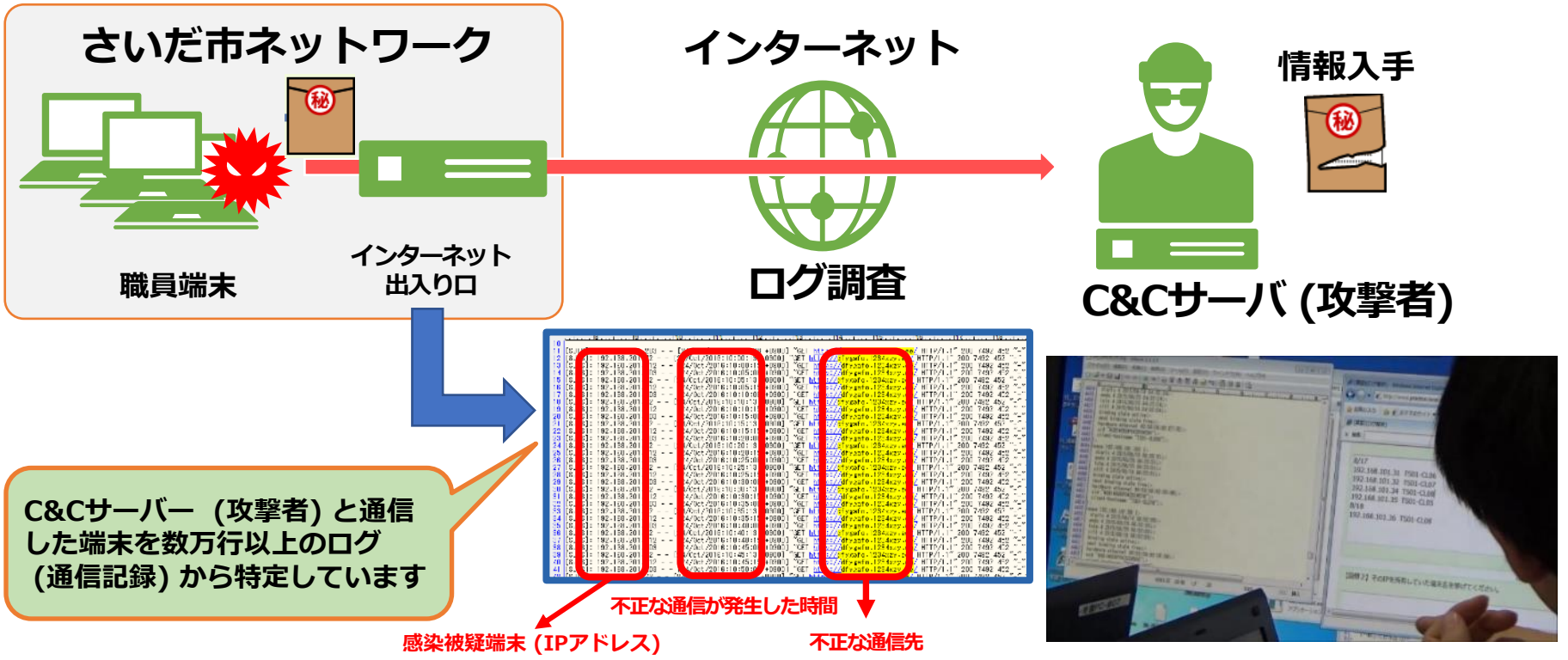
集合演習のマイルストーン: Aコースの例

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。

設問例 「端末特定」

セキュリティ監視業務委託業者から、海外にあるC&Cサーバー (発令サーバー) との通信を検知したとの連絡を受けました。
委託業者より提供された以下のC&Cサーバー情報を基に各種ログを解析し、このサーバーに通信を行った端末を特定してください。
【C&Cサーバー情報】　IPアドレス： x.x.x.x …….

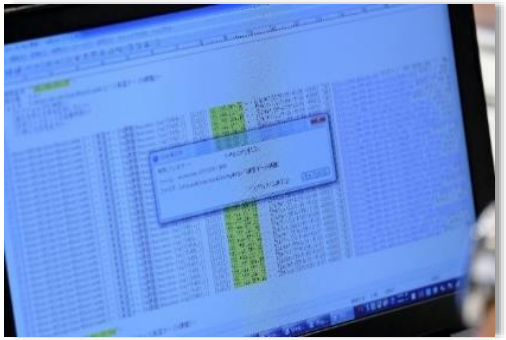


CYDER演習風景

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



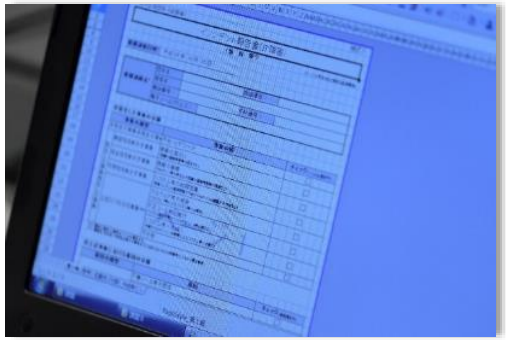
チューターによるサポート

マルウェア挙動調査

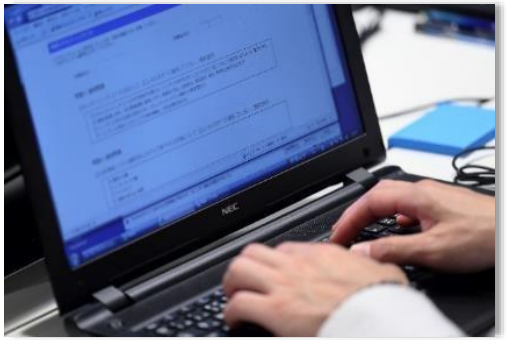
グループワーク

発表

報告書作成



確認テスト



※掲載している写真は、2019年度のものです。

CYDER開催結果 (2021年度)

● 演習申込数/受講決定数/受講者数の実績

◆CYDER演習合計

	集合演習	オンライン演習	合計
申込総数	3,332人	771人	4,103人
受講者数	2,454人	641人	3,095人

集合演習 (コース別) 全105回

コース	申込数 （１回当たりの平均値）	受講者数 （1回当たりの平均値）
A	2,103人 (約31人)	1,656人 (約24人)
B-1	622人 (約30人)	411人 (約19人)
B-2	498人 (約38人)	315人 (約24人)
C	109人 (約36人)	72人 (約24人)

オンライン演習 全67日

	全体数	1回当たりの平均値
申込者数	771人	約12人
受講者数	641人	約9人

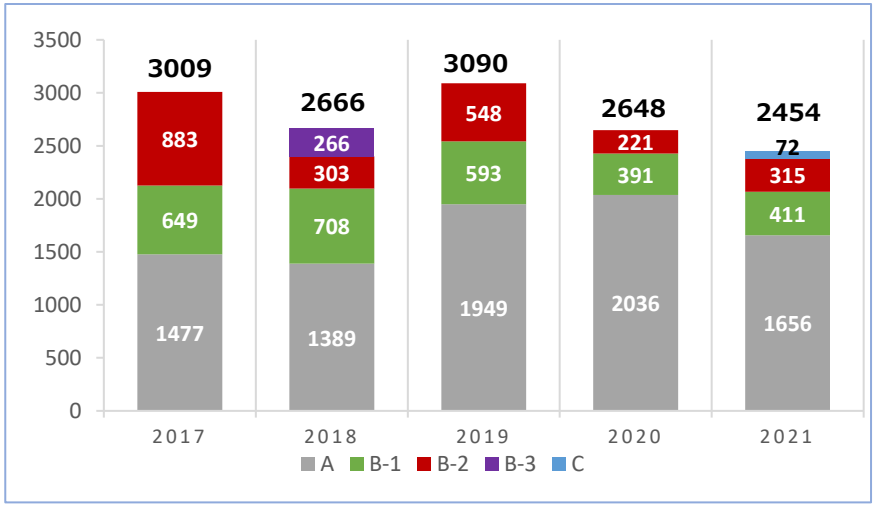
◆オプション演習合計

	全体数	１回あたりの平均値
受講者数	58人	約19人

情報システム統一研修 全3回

	全体数	１回あたりの平均値
受講者数	58人	約19人

集合演習受講者数推移 (2017~2021)



※グラフは集合演習の受講者数を計上。2021年度はこの他オンライン演習を641名が受講。

CYDER実行委員会　委員名簿

実行委員（４名）

菊池 浩明氏（委員長）
明治大学 総合数理学部 先端メディアサイエンス学科
教授

上原 哲太郎氏
立命館大学 情報理工学部
教授

門林 雄基氏
国立大学法人奈良先端科学技術大学院大学
先端科学技術研究科
教授

篠田 陽一氏
国立大学法人北陸先端科学技術大学院大学
情報社会基盤研究センター

推進委員（8名）

猪俣 敦夫氏
国立大学法人大阪大学 情報セキュリティ本部 教授

上野 宣氏
株式会社トライコーダ 代表取締役

岡田 良太郎氏
株式会社アスタリスク・リサーチ 代表取締役

川口 洋氏
株式会社川口設計 代表取締役

中西 克彦氏
株式会社FFRIセキュリティ技術本部
セキュリティサービス部長

寺田 真敏氏
株式会社日立製作所 Hitachi Incident Response Team
チーフコーディネーションデザイナ
東京電機大学 未来科学部 情報メディア学科 教授

与儀 大輔氏
グローバルセキュリティエキスパート株式会社（GSX）
常務取締役

満永 拓邦氏
東洋大学 情報連携学部 准教授

※2022年8月1日現在

参考資料２

実践サイバー演習 RPCI

実践サイバー演習 RPCIの沿革

FY

2016

2016年10月21日
・「サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律」が施行。
・この改正により、**情報処理安全確保支援士（RISS）が法制化**。

2018

IPA/経産省、NICT/総務省との間で方針検討
・IPA とNICTが連携し、情報処理安全確保支援士 (通称 登録セキスペ、RISS) 資格の更新講習 (3 年に1度の集合演習) として、CYDER R コースの提供可否の検討。

2020

2020年5月15日
・「情報処理の促進に関する法律の一部を改正する法律」施行。
・この改正により、**法定講習として一定の条件を満たした民間事業者等の講習（「特定講習」という）も対象に**。

2021

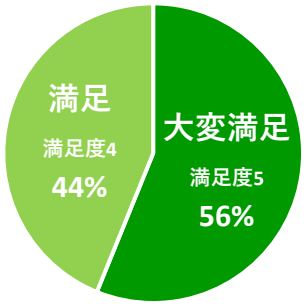
2021年3月31日
・NICTの**「実践サイバー演習（RPCI）」が特定講習として選定**。

2021年4月1日　情報処理安全確保支援士の登録者総数が20,178名となり、2万人突破。
2021年7月14日　プレスリリース＆募集開始

アンケート結果概要（2021年度）

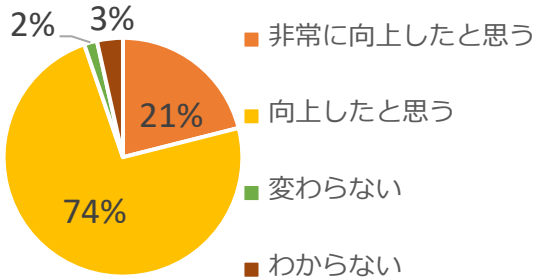
- 受講者の56%が大変満足、と回答（満足度を5段階で評価した結果）
- 選んだ理由は、NICTが実施する講習に興味がある、インシデントハンドリングを学びたかった、が半数以上を占めた
- 大多数の受講者が、自身のスキル向上を実感しており、理解度は、受講者の98%が理解できたと回答
- 速度は、受講者の60%が速いと回答しており、時間が足りないと感じる人が多かった

満足度

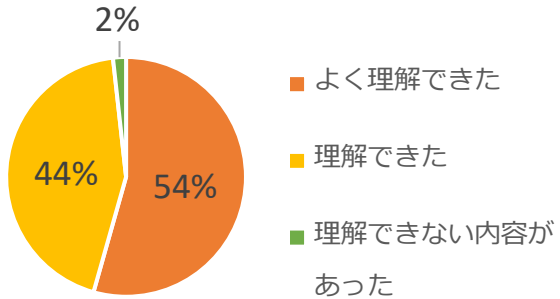


選んだ理由

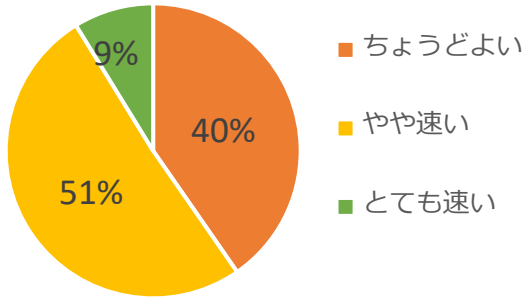
知識やスキルが向上したか



理解度



速度



参考資料３

SecHack365

SecHack365の沿革

FY

2016

2017年1月17日
・総務省「IoTサイバーセキュリティアクションプログラム2017」公表
セキュリティ人材育成のスピードアップの一環として若手セキュリティエンジニアの育成実施を明記

2017年3月
・平成29年度総務省所管予算に「若手セキュリティエンジニアの育成」として計上

2017

2017年4月3日 プレスリリース＆募集開始
・ 成果発表会を実施

2018

・ 3コース制 (表現駆動・思索駆動・開発駆動) 導入
・ 初の修了生イベント「SecHack365 Returns」を開催
・ 成果発表会を一般に向け公開

2019

・ 5コース制 (表現駆動・学習駆動・開発駆動・思索駆動・研究駆動) 導入

2020

2020年５月25日 オンライン開催を決定し、募集開始

2020年7月1日 オンラインでのプログラムスタート
・受講生とトレーナーが期間中非同期に参加する**「イベントウィーク」**と、全員同時に同期参加する**「イベントデイ」**を設定し、実施
・修了生の登用として、各コースのアシスタント制を導入

2021

・修了生の成果収集とコミュニティ継続を目的として「修了生ポータルサイト」を運用開始

SecHack365 実施結果 (2021年度)

2021年度 募集状況

募集期間　：　2021年4月1日 ～ 2021 年4月19日
応募資格　：　日本国内に居住する25歳以下の若手ICT人材
応募数　　：　203名
受講決定数：　45名
（内訳　成年32名/未成年13名、男性43名/女性2名
※2021.5.10受講者決定時点）

SecHack365 年間プログラム

SecHack365年間プログラム【2021】

年間を通して継続開発

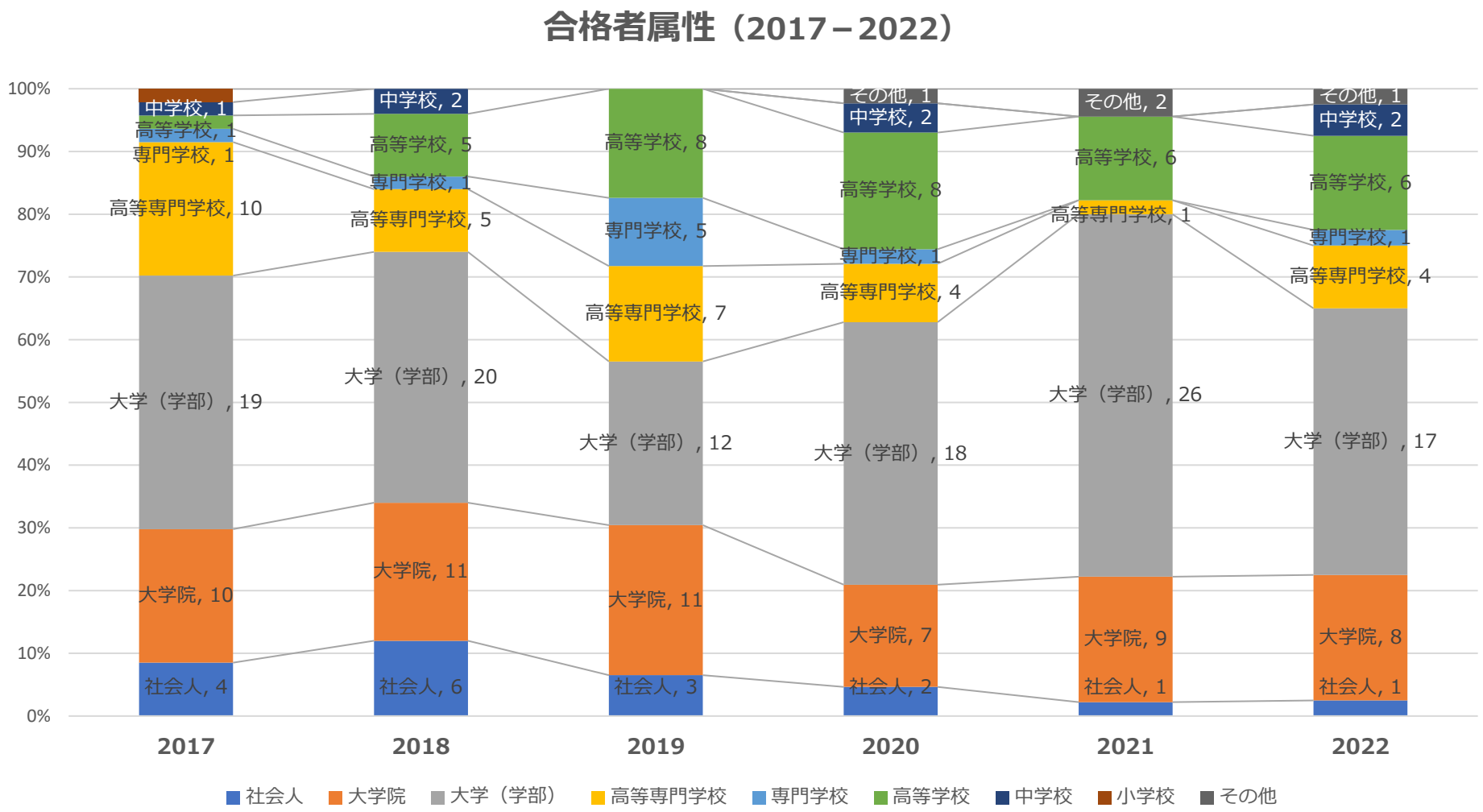
- 第1回 イベントウイーク 【キックオフ】 5/29(sat)・5/30(sun)
  イベントデイ ❶ 5月29日(土) ❷ 5月30日(日)
- 第2回 イベントウイーク 【作品発表・講義・講演等】 6/12(sat)・7/3(sat)
  イベントデイ ❶ 6月26日(土) ❷ 7月3日(土)
- 第3回 イベントウイーク 【作品発表・講義・講演等】 8/7(sat)・8/28(sat)
  イベントデイ ❶ 8月21日(土) ❷ 8月28日(土)
- 第4回 イベントウイーク 【大発表会・レビュー】 9/25(sat)・10/10(sun)
  イベントデイ 10月8日(金)～10月10日(日)
- 第5回 イベントウイーク 【再発表会・レビュー】 11/13(sat)・11/28(sun)
  イベントデイ 11月26日(金)～11月28日(日)
- 第6回 イベントウイーク 【最終発表会】 1/28(fri)・1/30(sun)
  イベントデイ 1月28日(金)～1月30日(日)

■ =オンライン開催　? =場所や実施形態は検討中

2022年3月5日(土) 成果発表会

SecHack365 受講生の属性推移

受講生の属性推移 (2017-2022)



CYDER
RPCI
SecHack365

SecHack365 の成果 (2021年度)

成果発表会 (オンライン)

2021年度優秀グループの発表タイトルと発表者

赤松　宏紀（あかまつ ひろき） 22歳	**開発環境に馴染むWebアプリ向けFuzzingツールSecHackFuzz**

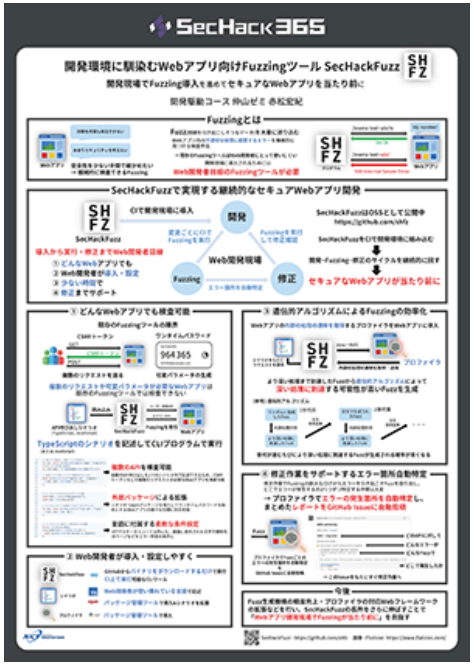
セキュリティが問題になることが多いWebアプリの安全性を機械的に検査するためのFuzzingツール「SecHackFuzz」を制作しました。SecHackFuzzは外部のツールとして検査時のみ使うのではなく、開発環境に組み込み、開発と並行してFuzzingを継続的に実行することで、セキュアなWebアプリを当たり前にできます。また、導入から実行・修正までWebアプリ開発者目線で、検査の高い汎用性と効率・導入の容易さ・修正のサポート機能を実現し、すぐにWebアプリ開発現場に導入できるようになっています。

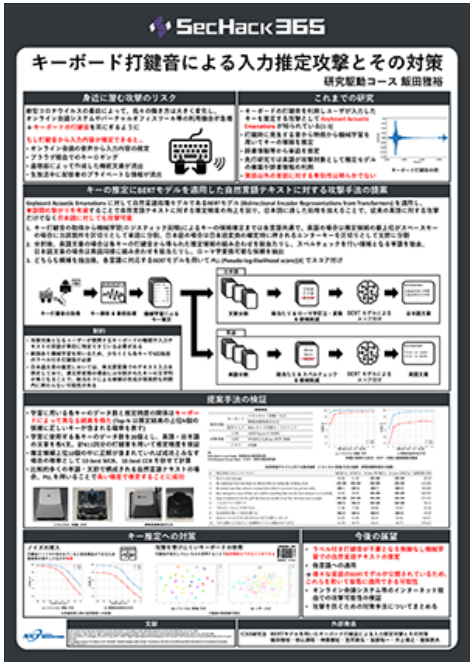
飯田　雅裕（いいだ まさひろ） 22歳	**キーボード打鍵音による入力推定攻撃とその対策**

サイドチャネル攻撃の一種として、キーボードの打鍵音をマイクで録音し入力キーを推定する攻撃である Keyboard Acoustic Emanations があり、様々な研究が行われてきました。 本研究では、Keyboard Acoustic Emanations に対して BERTモデルを適用することで単語間の繋がりを考慮し、自然言語テキストに対する推定精度を向上させる手法を提案します。また、併せて得られた知見に基づく有効な対策方法について提案します。

奥田　宗太（おくだ そうた） 20歳	**GeneSlimeMold_次世代分散型遺伝情報利活用システム**

ゲノム解析が身近になるこれからの世界で、公平な遺伝情報利活用を実現し、特定の事業者による情報独占や望まない利用を防ぐため、分散ネットワーク上で遺伝情報解析結果の保管、利用、利用権取引を一貫して行う未来のシステムです。





SecHack365 の成果 (2021年度)

成果発表会 (オンライン)

2021年度優秀グループの発表タイトルと発表者

平地　浩一（ひらち こういち） 18歳	**Seknot あなただけの暗号資産で新しい世界を**

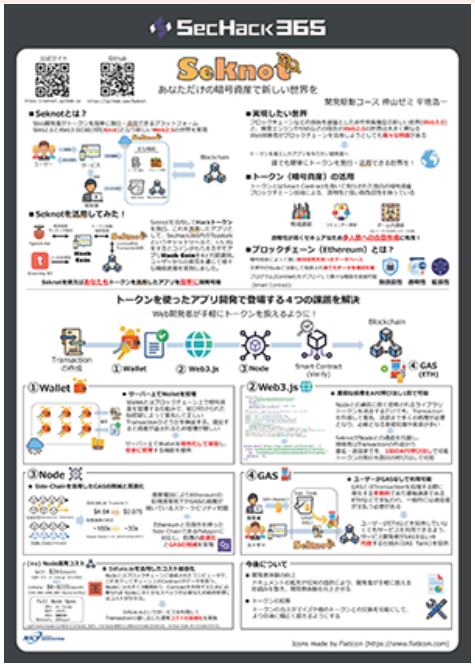
SeknotはWeb開発者が簡単にトークンの発行・活用ができるプラットフォームです。ブロックチェーン技術を用いて発行された独自の暗号資産であるトークンは、透明性や高い耐改竄性を持ち、ゲーム通貨やコミュニティ通貨など幅広い用途へ応用できます。Seknotではこうしたトークンを用いたアプリ開発で登場する問題を解決し、簡単なAPI呼び出しだけでトークンの発行から活用まで行うことが可能にしました。また、10月にはこれを活用したデモアプリとしてチャットツールで動作するHakc Coinをリリースし、4ヶ月間運用していく中で得られたユーザーからの感想を元にして、UX向上のため改善を行ってきました。

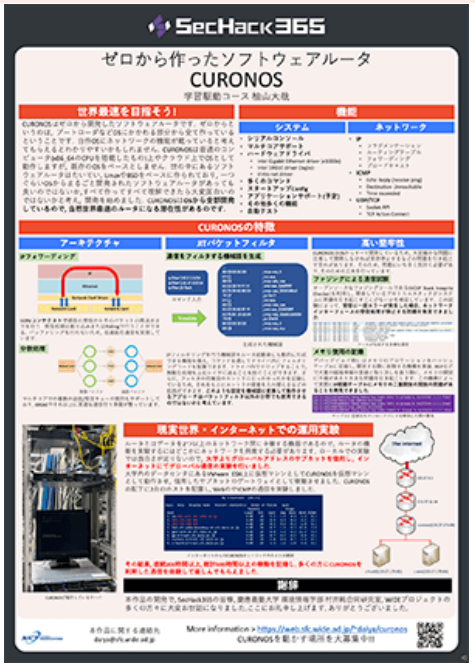
三浦　大輝（みうら だいき）23歳	**Rune ~CPUの特権命令をユーザープログラムへ安全に公開するための仕組み~**

RISC-Vのハイパーバイザー拡張を使って、CPUの特権命令をユーザープログラムへ安全に公開する Rune という仕組みを作りました。また、Runeを使って 起動が高速 かつ システムコールの挙動の高速な差し替えが可能 なサンドボックスを実装しました。

柚山　大哉（ゆやま ひろや）19歳	**接触確認アプリのセキュリティ・プライバシーリスクの評価**

CURONOSはゼロから開発したソフトウェアルータです。ゼロからというのは, ブートローダなどOSにかかわる部分から全て作っているということです。自作OSにネットワークのあれこれが載っていると考えてもらえるとわかりやすいかもしれません。このようにゼロから開発することで、 既存の枠組にとらわれない自由な設計が行えます。CURONOSでは、自由なアーキテクチャを考え, ゼロから開発してるからこそ実現できる機能を追加し、なおかつ堅牢性を保つように様々な施策を行いました。そして現実世界のインターネットにて実際に動作させ、OSから開発したソフトウェアルータが実用に耐える製品であることを確認しました。





海外派遣 の成果

海外派遣SXSW（South by Southwest)への派遣参加

訪問地　　：アメリカ合衆国　オースティン

海外派遣の目的：世界最大級のクリエイティブイベントに参加。海外トップクラスのイノベーター、クリエーターとの意見交換等を実施。今後のキャリア、セキュリティイノベーターに資するマインドセット・スキル習得を目指す。

SXSW Hackathon

SXSWの期間中に開催されるハッカソンイベントのひとつで、イノベーションを生み出す場として、スポンサーが提供するサービスを利用して24時間で作品を製作する。

2017年度　「SXSW2018」

Hackathonスポンサー賞を受賞	
タイトル	「emShare」
コンセプト	人間は言葉になる前の感情、言葉にできない感情を秘めている。emShare はそういう感情を人間がアップロードした動画から読み取り、それに相応しい音楽を選んで動画に差し込むシステム。選んだ音楽が流れる動画を共有することで感情を共有する。
受賞者	木下嵩裕、酒井蓮耀、澤田拓弥、早坂彪流（2017年度修了生）

2018年度　「SXSW2019」

Hackathonスポンサー賞を受賞	
タイトル	「wabisabi」
コンセプト	撮影した物体の情報により、メロディーを生成し、新しい音楽体験により，日常の何気ないものに新しい価値を与えるアプリ。
受賞者	秋田賢、井上勢大、三橋優希（2018年度修了生）
タイトル	「KIZUNA」
コンセプト	ストリートミュージシャンの演奏時の雰囲気の再現、ミュージシャンとリスナーとの音楽的な繋がりを創るサービス
受賞者	小林滉河、室田雅樹、青木克憲（2017年度修了生）

海外派遣 の成果

グローバルイベントへの参加 (CyberTech Grobal)

2018年11月、総務省及びイスラエル国家サイバー総局においてMoC （サイバーセキュリティ分野における協力に関する覚書）が締結。覚書の協力項目として、サイバーセキュリティ政策に関する情報交換、研究開発、人材育成が明記され、SecHack365では日本のセキュリティ人材育成の紹介、修了生のグローバルイベントでの発表を目的として参加。

「CyberTech Tokyo 2019 」2019年11月26日－27日

サイバーセキュリティ分野で世界を代表するBtoBネットワーキングプラットフォームである「CYBERTECH」が主催する、「起業家・投資家」「研究開発者」「政府・自治体」「大企業」「スタートアップ」の5つを繋ぎ、新たなビジネスチャンス・イノベーションを生み出すイベント。

発表者	発表タイトル
横山輝明（NICT）	SecHack365: Introduction of Cybersecurity Human Resource Development
小松聖矢（2018年度修了生）	Analysis of Botnet Cooperative Behavior using Deep Learning on Darknet
山本悠介（2018年度修了生）	Security by design of development kit for CanSat

「CyberTech TelAviv 2020」2020年1月28日－30日

米国外では最も重要とされるサイバー技術の国際会議および展示会。18,000人以上の参加者、180人のグローバルスピーカー、80か国以上からの160の代表団、210の大手企業とスタートアップの参加があり、Cybertech Tel-Aviv 2020には、専門家会議、特別サミット、3日間の展示会、スタートアップパビリオン、B2Bプラットフォームが含まれる。

発表者	発表タイトル
花田智洋（NICT）	SecHack365: Training Young Security Innovators
小松聖矢（2018年度修了生） ※ビデオ参加	Analysis of Botnet Cooperative Behavior using Deep Learning on Darknet
赤間滉星（2018年度修了生） ※ビデオ参加	Security by design of development kit for CanSat
柴﨑研治(2018年度修了生) ※ビデオ参加	Support system for static analysis of malware using CNN

SecHack365 実行委員会　委員名簿

実行委員（６名）

鹿野 利春氏（委員長）
京都精華大学
メディア表現学部
教授

鵜飼 裕司氏
株式会社FFRIセキュリティ
代表取締役社長

砂原 秀樹氏
慶応義塾大学大学院
メディアデザイン研究科
教授

佐藤 健太郎氏
GMOペパボ株式会社
代表取締役社長

田中 英彦氏
情報セキュリティ大学院大学
名誉教授
国立大学法人東京大学
名誉教授

瀧田 佐登子氏
一般社団法人WebDINO Japan
代表理事

※2022年8月1日現在

参考資料４

サイバーコロッセオ・その他

National Cyber Training Center

サイバーコロッセオ

※当事業は2021年度で終了しています。

サイバーコロッセオの沿革

FY

2016 — **総務省事業としてスタート**
東京2020オリンピック・パラリンピック競技大会に向けた演習「サイバーコロッセオ」及びセキュリティ競技大会「サイバーコロッセオ×SECCON」を実施

2017 — **4月　サイバーコロッセオの事業主体をNICTに変更**

12月　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の策定・公表

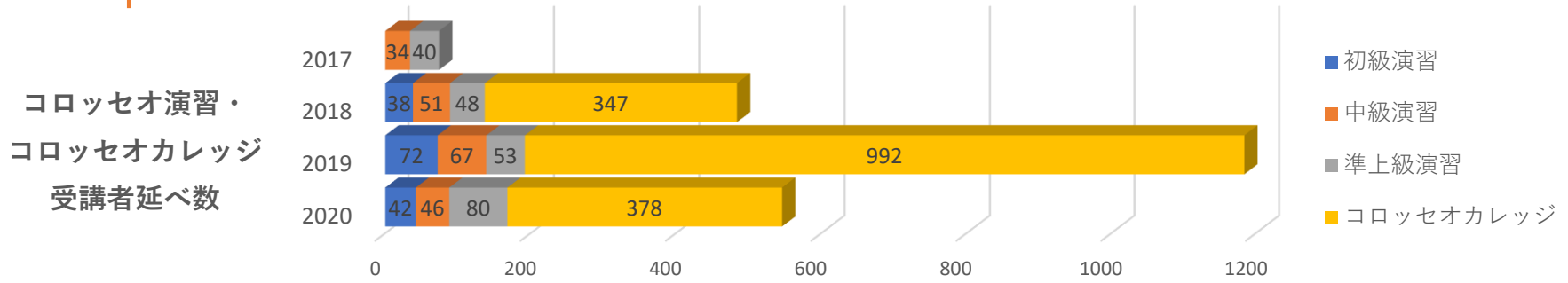
1月　NICT主催最初のコロッセオ演習実施 (中級、準上級)

2018 — **事業を拡充**
初年度の知見に基づき、コロッセオ演習 (初級A/B２コース) を追加、併せてコロッセオカレッジ (15科目) を開設

2019 — **セキュリティの総合的なトレーニング事業へ**
コロッセオ演習、中級B、準上級B、Cのシナリオを追加し、演習の業務カバレッジを拡大。併せてコロッセオカレッジも20科目に整理拡充

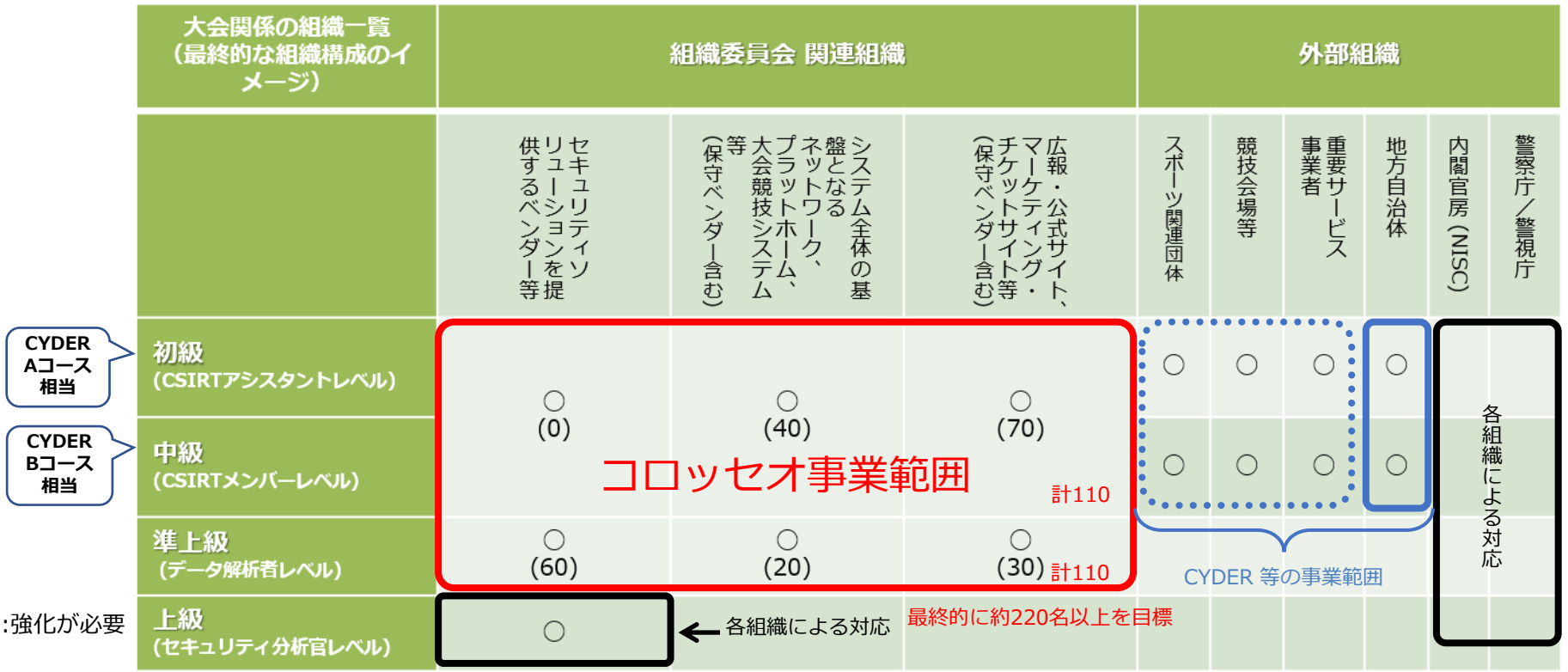
2020 — **人材育成成果の定着に向け最終年度事業を遂行**
セキュリティを取り巻く最新動向、受講者ニーズを汲みカリキュラム内容を一部改修。
新しい生活様式に対応し一部でオンライン受講を導入

12月　4年間で延べ145日(128回)実施、延べ約2300名が受講。事業目標であるセキュリティ人材220名の育成を完遂し事業を終了した。



仮想環境演習実施対象となる大会関係組織の範囲等

NICTが東京2020大会に向けて実施する実践的なトレーニングは、原則として、東京2020大会の関係団体のうち最もコアな団体である、大会組織委員会の組織を対象 (下表の赤枠部分)
それ以外の関係団体の組織についても、トレーニング実施のために必要な予算が追加的に確保される場合には、その範囲で、実践的なトレーニングを実施 (下表の青枠部分)



: サイバーコロッセオによる強化

: 各組織による対応 (NICT による育成事業の範囲外)

: 実践的サイバー防御演習 CYDER による強化

: CYDER 同等レベルの強化が必要 (現状は CYDER 事業の予算措置対象外であるが、必要な予算が追加的に確保される場合には、実施予定)

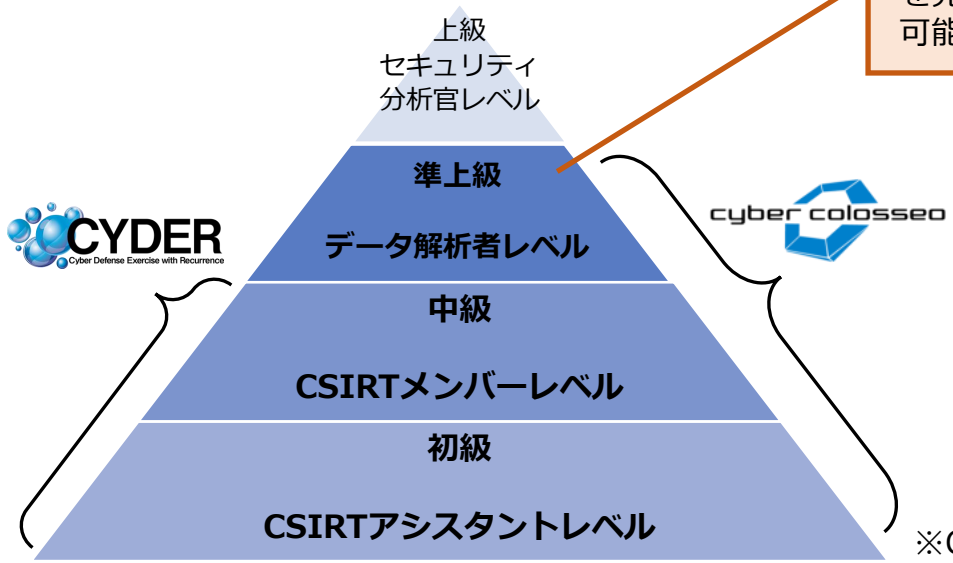
☆ **表中の目標人数は現時点において組織委が想定する数字であり、今後、組織委側のニーズを踏まえつつ、必要に応じて見直しを行う予定。**

サイバーコロッセオとCYDERの相違点①

① 「より高度なスキルを持つ者」に対し、より高度な内容とした「準上級コース」の演習を実施

サイバーコロッセオは、CYDER と同じく、組織内のセキュリティ運用者 (情報システム担当者等) を対象しているが、準上級コースに関しては、CYDER と比較して、より高度なスキルを持つ者に対し、より高度な内容の演習を実施する

運用者全体



【対象者の相違点であるデータ解析者の一例】
ネットワークに侵入したボットやワーム等のマルウェアを発見し、そのデータから、挙動などを解析することが可能なレベルのセキュリティ人材

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

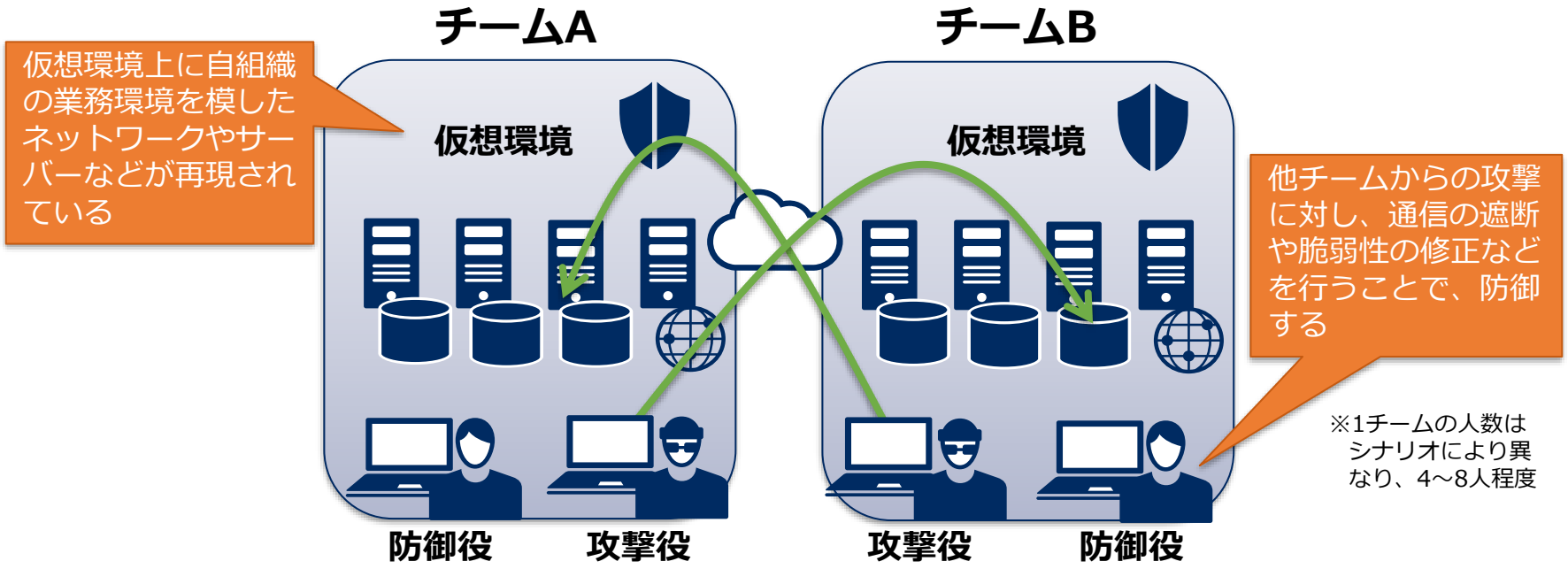
サイバーコロッセオとCYDERの相違点②

② 攻撃者の視点を持つための学習をした上で、 「攻防戦」を実施することで、より実践的な防御能力を育成

2018年度準上級コース (例)

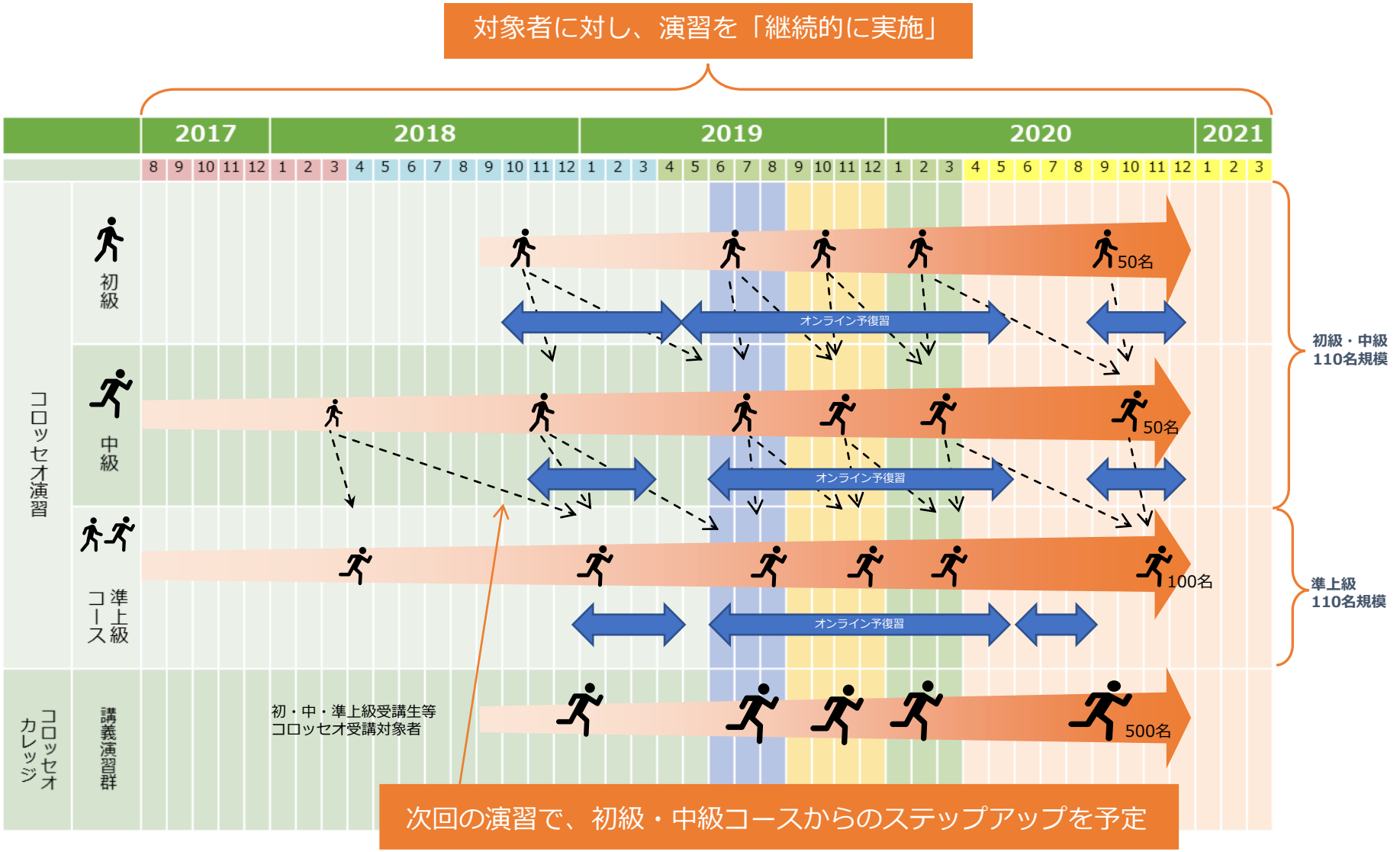
	1 日目：高度セキュリティ講義演習	2 日目：実機演習 (攻防戦等)
AM	オリエンテーション、インシデント・レスポンスの動向	データ解析演習
PM	攻撃手法を学ぶ (ハンズオン)	攻防戦

【演習内容の相違点である攻防戦等の特徴】
攻撃者が使用するツール等の攻撃手法を学習した上で、ツールを使った攻撃とそれに対する防御を実機を操作し行うことで、より実践的な防御能力を身に付ける



サイバーコロッセオとCYDERの相違点③

③ 対象者に対し、演習を「継続的に実施」することで、東京大会までの短期間で大幅なスキル向上を図る

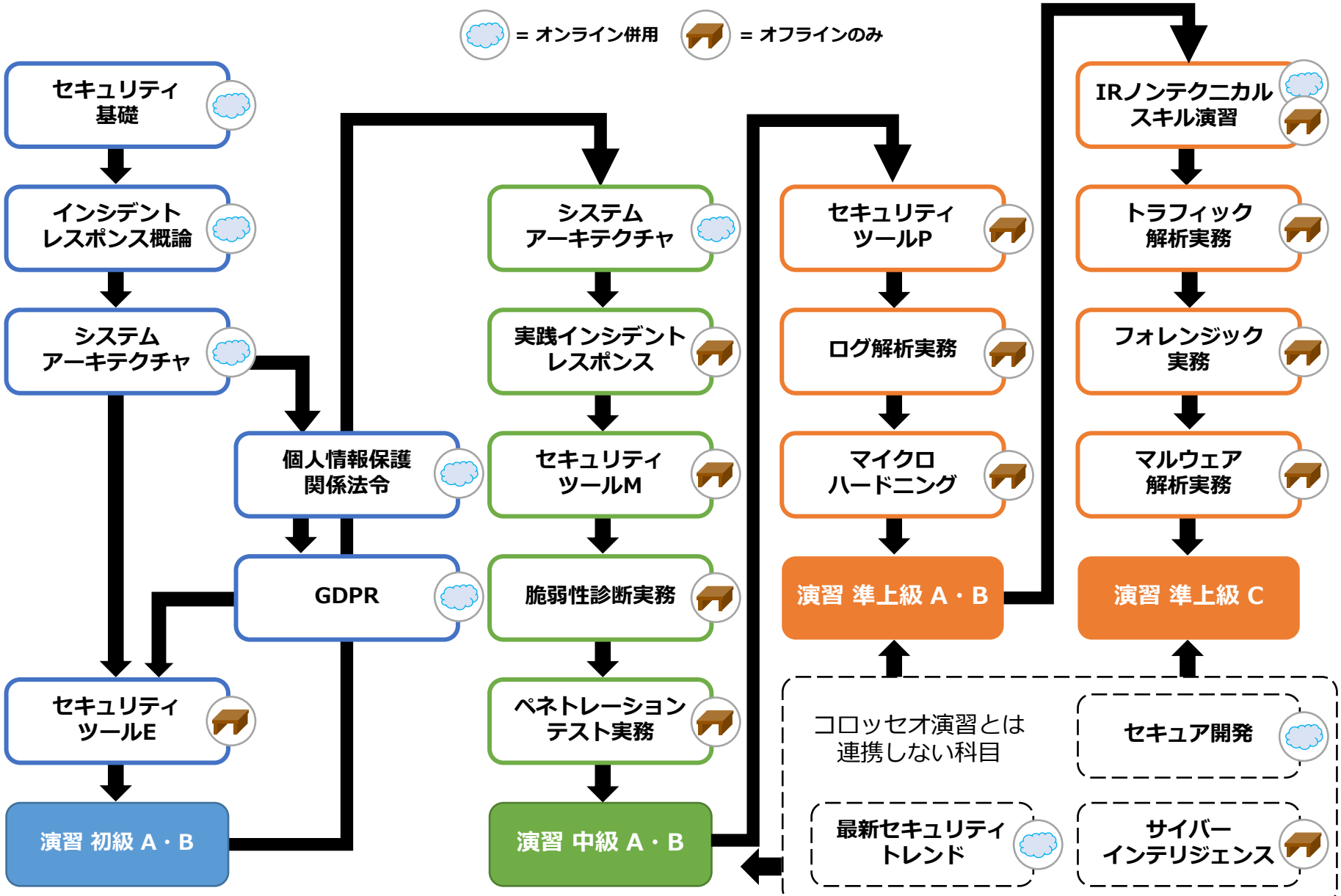


コロッセオカレッジ演習講義別概要

初級・中級・準上級各レベルの、演習受講者に合わせた**カレッジ科目を設定**。
カレッジで得た知識を演習で利活用します。

セキュリティ基礎	【オンライン併用】情報セキュリティの基礎を学びます。セキュリティの脅威についての基礎的なことや、企業ポリシーや情報の扱いなどを学ぶことができます。対象はITに限らないすべての方向けです。
インシデントレスポンス概論	【オンライン併用】インシデントレスポンスの概論を学びます。CSIRTの役割や、インシデントとその対応や具体的な手順について、全体を理解し、説明できるようになります。
個人情報保護関係法令	【オンライン併用】個人データ保護の世界の流れと重要性、プライバシーマークについて理解し、これらを説明できるようになります。データの取扱いや考え方、原則を学びます。
GDPR	【オンライン併用】GDPRは現在国際的にも新しく、影響力のあるプライバシー法として認知されており関心が高まっています。個人情報保護法、GDPR等の法規について理解し、職務に適用できるようになります。
セキュリティツールE	【オフラインのみ】実践的に使える様々なセキュリティツールについて、本格的に学びます。これらのツールを用いて自組織の脆弱性、攻撃の痕跡などを調査することができるようになります。
システムアーキテクチャ	【オンライン併用】システム開発で行う「機能設計、評価・診断、セキュリティマネジメント」の重要性を理解し、包括的なセキュリティ対策として非機能要件をシステムアーキテクチャにどう反映するかを学びます。
実践インシデントレスポンス	【オフラインのみ】インシデントが発生した際の一連の対応をグループワークを通じて、擬似体験します。日常ではなかなか体験できないインシデントレスポンスの流れを習得し、現場で役立てることができます。
セキュリティツールM	【オフラインのみ】セキュリティツールを用いて、安全な環境でサイバー攻撃を擬似体験します。ペネトレーションテストに利用されるツールなどの実体験をして攻撃者側の視点を学び、素早く対応できるようになります。
脆弱性診断実務	【オフラインのみ】毎年大量に発生する脆弱性情報を効率よく分別し、その対処、脆弱性のトリアージをする方法、管理の必要性などを学びます。オープンソースの脆弱性スキャナーツール作者による直接講義です。
ペネトレーションテスト実務	【オフラインのみ】脆弱性診断の概要、Webアプリケーション脆弱性診断、脆弱性再現の演習を行います。アプリケーションの挙動を再現し、報告の内容やリスクについて理解を深めます。
セキュリティツールP	【オフラインのみ】攻撃ツールの利用、OSINT (サイバーインテリジェンス) ツールによる調査、攻撃シナリオを想定した各種ログ調査、フォレンジックツールなど、様々なツールを用いて、包括的に学びます。
ログ解析実務	【オフラインのみ】Web改ざんや脅威インテリジェンス、脅威のハンティングなどをツールを通して学びます。どのような不正アクセスがあったかの痕跡を視覚化し、ハンズオンで学びます。
マイクロハードニング	【オンライン併用】45分を1セットとしたサイバー攻撃対応をチームで複数回繰り返し、攻撃対応能力の向上を目指します。演習では毎回同じ攻撃が行われ、知識を経験として定着させることができます。
IRノンテクニカルスキル演習	【1日目オンライン併用・2日目オフラインのみ】インシデント対応の“ノン・テクニカルスキル”を身につけます。テクニカルではないスキルを身につけることの重要性と必要性を理解することができます。
トラフィック解析実務	【オフラインのみ】ルータやスイッチで生成するデータを収集・蓄積・相関分析を行うツールを利用したシナリオが用意されており、いかに早く攻撃の兆候をつかめるかの演習をハンズオンで行います。
フォレンジック実務	【オフラインのみ】インシデントが発生した際に、侵害された端末を調査するための適切な保全の方法と選択肢を学びます。演習では保全したデータの解析や侵害範囲の確認、重大性などの判断を体験します。
マルウェア解析実務	【オフラインのみ】マルウェアを発見し、組織から追い出すために必要な情報をいかに素早く取得し、対処するかを学びます。マルウェアの動的解析やメモリイメージのフォレンジック調査も取り上げます。
セキュア開発	【オンライン併用】リスクアセスメント、実装、保守、運用までのフェーズでの要件を網羅し、システム開発時に必要な知識を習得。グループワークでは本格的なケーススタディを交え、セキュリティ設計を実践する。
最新セキュリティトレンド	【オンライン併用】近年起こる「攻撃パターン」事例などを通して、システム構築・運用へ適用できる知識習得を目指します。報告書を読むだけでは見えない、脆弱性が作り込まれる過程を解説していきます。
サイバーインテリジェンス	【オフラインのみ】表層ウェブ、ディープウェブ、ダークウェブといったウェブインテリジェンスの定義などを整理し、それぞれでどのような情報収集ができるのかを学び、対策に役立てることができます。

演習受講者によるコロッセオカレッジの標準的な受講例



サイバーコロッセオ実行委員会　委員名簿

実行委員（４名）

安田 浩氏（委員長）
東京電機大学 顧問

篠田 陽一氏（委員長代理）
国立大学法人 北陸先端科学技術大学院大学
情報社会基盤研究センター 教授

青木 眞夫氏
独立行政法人 情報処理推進機構 セキュリティセンター
セキュリティ対策推進部 調査役

洞田 慎一氏
JPCERTコーディネーションセンター 経営企画室 兼
早期警戒グループ兼 サイバーメトリクスグループ
担当部門長

推進委員（2名）

上野 宣氏
株式会社トライコーダ 代表取締役社長

丑丸 逸人氏
株式会社サイバーディフェンス研究所 技術部 バイナリアン

オブザーバ組織（8組織）(順不同)

総務省 サイバーセキュリティ統括官室
内閣官房 内閣サイバーセキュリティセンター
内閣官房 東京オリンピック競技大会・東京パラリンピック競技大会推進本部事務局
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 テクノロジーサービス局
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 警備局
警察庁
東京都 戦略政策情報推進本部 ICT推進部
一般社団法人 ICT-ISAC

その他

National Cyber Training Center

サイバーセキュリティ戦略（2021年9月28日閣議決定）
サイバーセキュリティ戦略の概要（2021年9月27日 サイバーセキュリティ戦略本部資料）抜粋

中長期的

1　2020年代を迎えた日本をとりまく時代認識
1－1　デジタル経済の浸透・デジタル改革の推進、SDGsへの貢献に対する期待、安全保障環境の変化、新型コロナウイルスの影響・経験、東京大会に向けた取組の活用

2　本戦略における基本的な理念
2－1　確保すべきサイバー空間は「自由、公正かつ安全な空間」
2－2　基本原則は従来の戦略で掲げた５つの原則を堅持（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携）

3　サイバー空間をとりまく課題認識
環境変化からみたリスク、国際情勢からみたリスク、近年のサイバー空間における脅威の動向

戦略期間

4　目的達成のための施策
<3つの方向性>（１）デジタル改革を踏まえたデジタルトランスフォーメーション とサイバーセキュリティの同時推進
（２）公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保
（３）安全保障の観点からの取組強化

経済社会の活力の向上及び持続的発展	国民が安全で安心して暮らせるデジタル社会の実現	国際社会の平和・安定及び我が国の安全保障への寄与
１．経営層の意識改革 ２．地域・中小企業におけるDX with Cybersecurity の推進 ３．新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり ４．誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着	１．国民・社会を守るためのサイバーセキュリティ環境の提供 ２．デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保 ３・４・５．経済社会基盤を支える各主体における取組 ①(政府機関等) ②(重要インフラ) ③(大学・教育研究機関等) ６．多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用 ７．大規模サイバー攻撃事態等への対処態勢の強化	１．「自由、公正かつ安全なサイバー空間」の確保 ２．我が国の防御力・抑止力・状況把握力の強化 ３．国際協力・連携

横断的施策

研究開発の推進	人材の確保・育成・活躍促進	全員参加による協働・普及啓発

5　推進体制　「自由、公正かつ安全なサイバー空間」を確保するための政府一体となった推進体制

サイバーセキュリティ2021
(サイバーセキュリティ戦略本部 2021年9月27日決定)

項目	各種施策
1　経済社会の活力の向上及び持続的発展 ～DX with Cybersecurity～ の推進	
2　国民が安全で安心して暮らせるデジタル社会の実現	
2.1 国民・社会を守るためのサイバーセキュリティ環境の提供	
2.2 デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保	
2.3 経済社会基盤を支える各主体における取組① (政府機関等)	**・総務省において、NICT の「ナショナルサイバートレーニングセンター」を通じ、国の行政機関や独立行政法人等におけるサイバー攻撃への対処能力の向上を図るための実践的サイバー防御演習（CYDER）を実施する。【総務省】**
2.4 経済社会基盤を支える各主体における取組② (重要インフラ)	
(1)　官民連携に基づく重要インフラ防護の推進	**・総務省において、NICT の「ナショナルサイバートレーニングセンター」を通じ、重要インフラ事業者におけるサイバー攻撃への対処能力の向上を図るための実践的サイバー防御演習（CYDER）を実施する。【総務省】**
(2)　地方公共団体に対する支援	**・総務省において、NICT の「ナショナルサイバートレーニングセンター」を通じ、受講実績の少ない地方公共団体の受講機会拡大を図るため、都道府県と連携し開催時期等の調整を図るとともに、都道府県ごとに受講計画を策定した上で、当該受講計画を踏まえ、地方公共団体におけるサイバー攻撃への対処能力の向上を図るための実践的サイバー防御演習（CYDER）を実施する。【総務省】**
2.5 経済社会基盤を支える各主体における取組③（大学・教育研究機関等）	
2.6 多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用	
2.7 大規模サイバー攻撃事態等への対処態勢の強化	
3　国際社会の平和・安定及び我が国の安全保障への寄与	
4　横断的施策	
4.1 研究開発の推進	
4.2 人材の確保・育成・活躍促進	
(1)　「DX with Cybersecurity」に必要な人材に係る環境整備	
(2)　巧妙化・複雑化する脅威への対処	**・総務省において、NICT の「ナショナルサイバートレーニングセンター」を通じ、国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等におけるサイバー攻撃への対処能力の向上を図るため、実践的サイバー防御演習（CYDER）を実施する。また、都道府県と緊密に連携し各都道府県におけるCYDER 受講計画の策定などを通じて、未受講である地方公共団体の受講促進を図る。加えて、地理的な要因等により集合演習への参加が困難な団体を対象として、オンラインでの受講を可能とする演習実施環境の整備・高度化を実施する。【総務省】** **・総務省において、NICT の「ナショナルサイバートレーニングセンター」における「SecHack365」の取組を通じて、育成プログラムの質の向上を図りつつ、若年層のICT人材を対象に、セキュリティに関わる技術を本格的に指導し、セキュリティイノベーターの育成に取り組む。【総務省】**
(3)　政府機関における取組	
4.3 全員参加による協働、普及啓発	
5　推進体制	

国立研究開発法人情報通信研究機構法（抜粋）

(平成11年法律第162号)　施行日：令和3年9月1日（令和3年法律第36号による改正）

（業務の範囲）

第十四条　機構は、第四条の目的を達成するため、次の業務を行う。

一　情報の電磁的流通及び電波の利用に関する技術の調査、研究及び開発を行うこと。

二　宇宙の開発に関する大規模な技術開発であって、情報の電磁的流通及び電波の利用に係るものを行うこと。

三　周波数標準値を設定し、標準電波を発射し、及び標準時を通報すること。

四　電波の伝わり方について、観測を行い、予報及び異常に関する警報を送信し、並びにその他の通報をすること。

五　無線設備（高周波利用設備を含む。）の機器の試験及び較こう正を行うこと。

六　前三号に掲げる業務に関連して必要な技術の調査、研究及び開発を行うこと。

七　第一号に掲げる業務に係る成果の普及として**サイバーセキュリティ**（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）**に関する演習その他の訓練を行う**こと。

八　前号に掲げるもののほか、第一号、第二号及び第六号に掲げる業務に係る成果の普及を行うこと。

九　高度通信・放送研究開発を行うために必要な相当の規模の施設及び設備を整備してこれを高度通信・放送研究開発を行う者の共用に供すること。

十　高度通信・放送研究開発の実施に必要な資金に充てるための助成金を交付すること。

十一　海外から高度通信・放送研究開発に関する研究者を招へいすること。

十二　情報の円滑な流通の促進に寄与する通信・放送事業分野に関し、情報の収集、調査及び研究を行い、その成果を提供し、並びに照会及び相談に応ずること。

十三　科学技術・イノベーション創出の活性化に関する法律（平成二十年法律第六十三号）第三十四条の六第一項の規定による出資並びに人的及び技術的援助のうち政令で定めるものを行うこと。

十四　前各号に掲げる業務に附帯する業務を行うこと。

2　機構は、前項の業務のほか、次の業務を行う。

一　特定公共電気通信システム開発関連技術に関する研究開発の推進に関する法律（平成十年法律第五十三号。以下「公共電気通信システム法」という。）第四条に規定する業務

二　基盤技術研究円滑化法（昭和六十年法律第六十五号）第七条に規定する業務

三　通信・放送融合技術の開発の促進に関する法律（平成十三年法律第四十四号）第四条に規定する業務

四　特定通信・放送開発事業実施円滑化法（平成二年法律第三十五号。以下「通信・放送開発法」という。）第六条に規定する業務

五　身体障害者の利便の増進に資する通信・放送身体障害者利用円滑化事業の推進に関する法律（平成五年法律第五十四号。以下「障害者利用円滑化法」という。）第四条に規定する業務

（中長期目標等に関するサイバーセキュリティ戦略本部の意見の聴取）

第二十三条　総務大臣は、通則法第三十五条の四第一項の規定により中長期目標（第十四条第一項第七号に掲げる業務及びこれに附帯する業務に係る部分に限る。）を定め、又は変更しようとするときは、あらかじめ、サイバーセキュリティ戦略本部の意見を聴かなければならない。

2　総務大臣は、通則法第三十五条の五第一項の規定による中長期計画（第十四条第一項第七号に掲げる業務及びこれに附帯する業務に係る部分に限る。）の認可をしようとするときは、あらかじめ、サイバーセキュリティ戦略本部の意見を聴かなければならない。

国立研究開発法人情報通信研究機構第5期中長期目標／第5期中長期計画

(抜粋)

第５期中長期目標（令和３年度～令和７年度）	第５期中長期計画（令和３年度～令和７年度）令和4年2月17日変更
１．重点研究開発分野の研究開発等 **（３）サイバーセキュリティ分野** **③サイバーセキュリティに係る人材育成** 国の機関や地方公共団体等の**サイバー攻撃への対処能力の向上に貢献する**ため、サイバーセキュリティ戦略等の政府の方針を踏まえ、NICT法第14条第１項第７号の規定に基づき、**最新のサイバー攻撃に関する知見を踏まえた実践的な演習**を実施するほか、**若手セキュリティ人材の育成**を行う。	**１－３．サイバーセキュリティ分野** **（３）サイバーセキュリティに関する演習** 国の機関や地方公共団体等のサイバー攻撃への対処能力の向上に貢献するため、国からの補助等を受けた場合には、その予算の範囲内で、サイバーセキュリティ戦略等の政府の方針を踏まえ、機構法第14条第１項第７号の規定に基づき、機構の有する技術的知見を活用して、最新のサイバー攻撃状況を踏まえた実践的なサイバーセキュリティ演習を実施する。演習の実施に当たっては、サイバーセキュリティ基本法第13条及び第14条の規定を踏まえ、全ての国の行政機関、独立行政法人及び指定法人並びに地方公共団体の受講機会を確保するとともに、重要社会基盤事業者及びその組織する団体についても、**より多くの受講機会を確保できるよう配慮する。** また、地理的条件により受講機会が失われることを最小限とするよう、集合演習を全国で実施するほか、**オンライン演習を拡大していくこととし、未受講となる組織・団体に対して積極的な参加を促す。**あわせて、最新のサイバー攻撃情報を踏まえた演習内容の高度化、オンライン演習における学習定着率の向上等、**演習効果の最大化に取り組む。**さらに、**機構におけるサイバーセキュリティ研究と演習業務で得られた知見等を活用し、若手セキュリティ人材の育成を行う。**

【参考】サイバーセキュリティ基本法 より抜粋

第十三条　（国の行政機関等におけるサイバーセキュリティの確保）

国は、国の行政機関、独立行政法人（独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する独立行政法人をいう。以下同じ。）及び特殊法人（法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成十一年法律第九十一号）第四条第一項第九号の規定の適用を受けるものをいう。以下同じ。）等におけるサイバーセキュリティに関し、国の行政機関、独立行政法人及び指定法人（特殊法人及び認可法人（特別の法律により設立され、かつ、その設立等に関し行政官庁の認可を要する法人をいう。第三十二条第一項において同じ。）のうち、当該法人におけるサイバーセキュリティが確保されない場合に生ずる国民生活又は経済活動への影響を勘案して、国が当該法人におけるサイバーセキュリティの確保のために講ずる施策の一層の充実を図る必要があるものとしてサイバーセキュリティ戦略本部が指定するものをいう。以下同じ。）におけるサイバーセキュリティに関する統一的な基準の策定、国の行政機関における情報システムの共同化、情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関、独立行政法人又は指定法人の情報システムに対する不正な活動の監視及び分析、国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する演習及び訓練並びに国内外の関係機関との連携及び連絡調整によるサイバーセキュリティに対する脅威への対応、国の行政機関、独立行政法人及び特殊法人等の間におけるサイバーセキュリティに関する情報の共有その他の必要な施策を講ずるものとする。

第十四条　（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）

国は、重要社会基盤事業者等（※）におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。※ 重要社会基盤事業者及びその組織する団体並びに地方公共団体。

視察実績等

センター発足以来、政界、官界に限らず多数のご視察を受け入れており、今後もセンター事業への関心の高まりとともに、視察希望が多数寄せられる見込み (例　国会議員、中央省庁 (政務関係者含む) 、情報通信関連企業、報道機関、海外要人 等)

➢ 視察実績

H29年度からR3年度の5年間で延べ　398人

(総務省ウェブサイトより)

SecHack365 成果発表会場を視察する
佐藤総務副大臣 (当時) (平成31年3月8日)

(総務省ウェブサイトより)

サイバー防御演習 (CYDER) を視察する
寺田総務副大臣 (当時) (令和元年11月6日)

(総務省ウェブサイトより)

サイバー防御演習 (CYDER) を視察する
木村総務大臣政務官 (当時) (令和元11月22日)

令和 2 年 12月 25日　武田総務大臣 (当時) がサイバー防御演習 (CYDER) を御視察

➢ 研修員受入実績

日本国内外の政府機関からの研修受入れ (複数名)

ナショナルサイバートレーニングセンター・アドバイザリーコミッティー 名簿

NICTは、サイバートレーニング事業の企画・推進、サイバートレーニングの高度化のための研究開発等を審議し、理事長に対し助言を行う組織として、産学の有識者によって構成される「ナショナルサイバートレーニングセンター・アドバイザリーコミッティー」を設置し、併せて事業別の実行委員会を設置

構成員 (7名) (50音順)

座長
後藤 厚宏氏
情報セキュリティ大学院大学 学長

齊藤 忠夫氏
一般社団法人ICT-ISAC 理事長

新野 隆氏
一般社団法人情報通信ネットワーク産業協会 会長
(日本電気株式会社 代表取締役副会長)

安田 浩氏
東京電機大学 顧問

遠藤 信博氏
一般社団法人 日本経済団体連合会　サイバーセキュリティ委員長
(日本電気株式会社 取締役会長)

髙橋 誠氏
一般社団法人電気通信事業者協会 会長
(KDDI株式会社 代表取締役社長)

村井 純氏
慶應義塾大学 教授

※2022年8月1日現在