経済産業省　御中

令和4年度サプライチェーン・サイバーセキュリティ対策促進事業

（先進的なサイバー防御機能や分析能力に係る技術動向及びサイバー演習動向等に関する調査）

三菱総合研究所

デジタル・イノベーション本部
サイバーセキュリティ戦略グループ

2023年3月31日

目次

1. 概要

本調査報告書は、『令和4年度サプライチェーン・サイバーセキュリティ対策促進事業（先進的なサイバー防御機能や分析能力に係る技術動向及びサイバー演習動向等に関する調査）』（以下、本事業と呼ぶ）に基づき実施した調査結果をまとめたものである。

本事業の背景・目的は以下の通りである。

- サイバー攻撃は技術の進展とともに巧妙化・高度化しており、例えば、既存のセキュリティ製品による防御に対して AI を活用して回避しシステムへの侵入を試みる攻撃といった新たな攻撃が想定されている。このように将来において起こりうる攻撃に対して先手で対応していくためには、こうした攻撃を想定したサイバー演習シナリオのもと、繰り返しサイバー演習を実施することで、対処・分析能力を向上させていくことが必要である。
- こうした点に関し、我が国の政府方針では、「経済財政運営と改革の基本方針 2022（令和 4 年 6 月 7 日閣議決定）」において「国際情勢の変化等を踏まえたサイバーセキュリティの確保に向けた官民連携や分析能力の強化について、技術開発の推進や制度整備を含めた所要の措置を講ずるべく検討を進める。」との記載があるほか、「新しい資本主義のグランドデザイン及び実行計画（令和4年6月7日閣議決定）」において「サイバー攻撃が高度化・複雑化する中、サイバー攻撃対策やシステムの脆弱性の分析能力を国が主導して強化する。」と記載されている。
- こうした背景のもと、本事業では、先進的なサイバー防御機能や分析能力に係る技術動向及びサイバー演習動向等に関する国内外の事例等の調査や、有識者を交えた研究会の企画・運営を実施することで、我が国のサイバーセキュリティの確保に向けた官民連携や分析能力の強化について検討を行うことを目的とする。

なお、本調査は公開情報（外国政府・国際標準化団体の報告資料、国内外の専門誌等を含む。）、国内外のニュース記事、商用データベース等を範囲とし、また調査対象の国・地域は日本に加えて米国、欧州と対象とした。

2. 国内外のサイバー演習動向の調査

本章では、国内外のサイバー演習動向の調査を以下の観点で実施した。

2.1 節では国内外のサイバー演習について、民間事業者の提供するサービス、公的機関が提供するサービスの各々に対して、演習環境、シナリオ、演習期間、対象者や育成スキル、参加人数、特徴・優位点の観点からサービス内容の調査を行った。

2.2 節では、サイバー演習を企画・運営する主体について、企業沿革、規模、IR 情報、セキュリティ事業における提供製品・サービス・位置づけ、特徴等についての調査を行った。

2.3 節では、国内外のサイバー演習市場について、国内外のサイバー演習に関する市場規模、市場予測、プレイヤー動向等の情報を収集・整理した。

2.1 国内外のサイバー演習

国内外のサイバー演習について、民間事業者の提供するサービス、公的機関が提供するサービスの各々に対して、演習環境、シナリオ、演習期間、対象者や育成スキル、参加人数、特徴・優位点などの観点からサービス内容の調査を行った。

また、各サイバー演習の相違点等について比較を行った。比較の観点は、(1)対象者、育成スキル、(2)対象システム、シナリオ (3)演習目的 等の観点で実施した。

2.1.1 国内のサイバー演習(民間事業者)

国内の民間事業者の提供するサイバー演習の、演習環境、シナリオ、演習期間、対象者や育成スキル、参加人数、特徴・優位点などの観点から以下(1)～(9)のとおり、サービス内容の調査を行った。

(1) Armoris(凸版印刷グループ) :実践的人材育成プログラム「DOJO」

項目	概要
演習環境	・ 提示されたカリキュラムを参加者が実施するための環境(サーバ、ネットワーク機器等)が提供される。 ・ 対面、オンライン、及び出張形式に対応している。
シナリオ	・ 自社システムが狙われたサイバー攻撃を想定し、現実の脅威に対抗する実践的なトレーニングを行う。ユーザのニーズに応じた最適なプログラムを提供可能である。また、脆弱性を突く攻撃、ビジネスメール詐欺など、さまざまなインシデント対応を疑似体験するワークショップも提供している。
演習期間	・ 短期トレーニング 2 日間から要相談
対象者 育成スキル	・ 演習の対象者は、セキュリティ技術者、セキュリティ管理者を想定している。 ・ 育成スキルとしては、テクニカルスキルだけでなく、行動力や問題発見・解決能力といったヒューマンスキルを自主・継続的に学ぶことができる。
参加人数	・ 一組織 5 名まで
特徴、優位点	・ ターゲット／レベル別に多種多様なトレーニングプログラムを提供している。教科書的な知識だけではない、現実の脅威に対抗する実践的なトレーニングとなっている。 ・ トレーニング環境はすべて完全オンラインにも対応している。また、ユーザの要望に応じて、対面・オンライン・出張のいずれの形式でも実施可能となっている。 ・ オーダーメイドのトレーニングメニュー開発も可能で、ユーザのニーズに応じた最適なプログラムを提供することができる。

（2） NEC ：NEC サイバーセキュリティ訓練場演習

項目	概要
演習環境	・同社が独自開発した、企業システムを模した仮想の演習システム環境で実施する。 ・対面・オンライン形式に対応している。
シナリオ	・システム構築フェーズの堅牢化にフォーカスした演習となっており、自らが堅牢化したシステムが攻撃を受けるというシナリオである。「犯行予告型」トレーニングとして、セキュア開発からインシデントレスポンスまで一貫したシナリオとなっている。
演習期間	・2 日間（推奨）
対象者 育成スキル	・演習の対象者は、主にシステム運用／企画（開発・構築）担当者、又はこれから担当する予定の方を想定している。 ・育成スキルとしては、WEB システムにおけるリスクアセスメントおよび堅牢化の実践的なスキルの習得、インシデントハンドリングの初動と基本の理解、セキュリティ・バイ・デザインの考え方をベースにしたセキュア構築の重要性の理解等を習得することができる。
参加人数	・5～30 名まで
特徴、優位点	・システム構築フェーズの演習にフォーカスし、仕込まれた脆弱性の探索や課題解決を実際に体験することができる。 ・自ら堅牢化したシステムがサイバー攻撃の被害に遭うという衝撃的な体験が、受講者への意識浸透につながる。

（3） グローバルセキュリティエキスパート ：Micro Hardening：Enterprise Edition

項目	概要
演習環境	・ 川口設計製の「Micro Hardening」の演習システムの環境を活用する。 ・ 基本オンライン形式だが、対面形式にも対応している。
シナリオ	・ 参加者は与えられた EC サイトのサーバをさまざまな攻撃から守り、制限時間内に最大の売上を目指してサイトを運用する。そのためには、いまサイトに何が起こっているのか見極める目、事象を把握するための知識、攻撃に対処するための技術、EC サイトのサービスを止めない運用力が求められる。 ・ 参加者はチームごとに EC サイト（サーバ）を与えられ、1 日で演習を 4 セット経験する事ができる。各セットは全て同じ攻撃シナリオで行われる。
演習期間	・ 1 日～
対象者 育成スキル	・ 演習の対象は主にエンジニアを想定している。 ・ 育成スキルとしては、EC サイトに何が起こっているのか見極める目、事象を把握するための知識、攻撃に対処するための技術、サービスを止めない運用力など、自ら手を動かすことができるサイバー攻撃対応を習得することができる。
参加人数	・ 最低開講人数：8 名から実施
特徴、優位点	・ シンプルかつ、ゲーム感覚で楽しく経験することができるため、記憶の定着と継続にも有効である。 ・ 忙しいエンジニアにおいても極めて短時間で効率的なスキルアップが可能となる。 ・ 情報処理安全確保支援士の特定講習にも指定されている。

（4） サイバージムジャパン（バルクホールディングスグループ） ：Cyber-Threats and Defense Essentials

項目	概要
演習環境	・ 実戦経験に基づく独自開発のトレーニングプログラムを使用している。IT 環境だけでなく OT 環境に焦点を当てたトレーニングプログラムを保有している。 ・ 事前にプログラム化されたサイバー攻撃ではなく、ホワイトハッカーによるオンタイムの攻撃など、カスタマイズ可能な実践的トレーニングプログラムとなっている。 ・ 基本対面形式を想定している。
シナリオ	・ 実際のサイバー攻撃を受け、複数の検出・監視ツールを駆使してサイバー攻撃を検出し、

	その分析を行う。
演習期間	・2日間
対象者 育成スキル	・演習の対象は、主に IT 担当者、情報セキュリティ担当者、SOC アナリスト、情報処理安全確保支援士を想定している。 ・育成スキルとしては、複数の検出・監視ツールを駆使してサイバーインシデント攻撃を検出、検出したサイバー攻撃インシデントの初期分析等のスキルを習得することができる。
参加人数	・オープン講座は1名から参加可能。単独開催は別途問合せ。
特徴、優位点	・さまざまな重要インフラ分野におけるグローバルかつ高度な知識・ノウハウを有している。 ・実戦経験に基づく独自開発のトレーニングプログラムを有している。 ・IT 環境だけでなく、OT 環境に焦点をあてたトレーニングプログラムを保有している。 ・事前にプログラム化されたサイバー攻撃ではなく、ホワイトハッカーによるオンタイムの攻撃などカスタマイズ可能な実践的トレーニングプログラムを実施することが可能となっている。 ・実戦経験のある多数のホワイトハッカーを活用している。 ・情報処理安全確保支援士特定講習にも指定されている。

（5） サイバーディフェンス研究所 ：サイバー演習

項目	概要
演習環境	・演習用の疑似環境でサイバー攻撃を実際に体験しながらインシデントハンドリングと技術的な解析手法を学ぶ。 ・基本対面形式を想定している。
シナリオ	・企業 WEB への「DoS/DDoS によるサービス停止攻撃」、「正規サイトを模したフィッシングサイトの出現」、「脆弱性攻撃による個人情報などの情報窃取」、「Web 改ざんによるマルウェア配布」等の攻撃に対して、適切な対処方法を習得する「サイバー攻撃　ログ分析・パケット解析演習」コースがある。 ・また、擬似環境に対して、リアルタイムに実施される攻撃（マルウェア感染/遠隔操作/情報の窃取が行われるまでの流れ）を体験しながら、検知と分析の手法を学ぶ「基礎・APT 対処演習」のコースも用意されている。
演習期間	・2 日間
対象者 育成スキル	・演習の対象者は、サイバー犯罪捜査官、サイバーテロ対策担当者、組織の CSIRT メンバー、ネットワーク管理者、システム管理者、インシデントレスポンス担当者を想定している。 ・育成スキルとしては、組織内 CSIRT やインシデントレスポンス担当者の技術力の向上を図ることができる。
参加人数	・定員 16 名（最低開講人数 8 名）
特徴、優位点	・組織内 CSIRT やインシデントレスポンス担当者のみでなく、法執行機関のサイバーテロ対策担当者の技術力の向上への活用も想定した内容となっている。 ・用意されているプランのみでなく、カスタマイズしたサイバー演習も提供可能となっている。

（6） サイバーナレッジアカデミー（大日本印刷グループ） ：サイバーナレッジアカデミー

項目	概要
演習環境	・IT 向けコースでは、一般的な企業システム構成を仮想環境上で構築した上で攻撃が行われる。 ・産業用制御システム向けコースでは、複数種類のシステム構築が可能である。GUI の操作感覚で（プログラミングレスで）仮想的な制御システムの作成が可能である。 ・対面・オンライン・出張形式に対応している。
シナリオ	・標的型攻撃、Ping Flood 攻撃、中間者攻撃、USB からのマルウェア感染などの実際の攻撃手法に対処する。 ・イスラエル IAI 社の演習シミュレータ「Tame Range」を使用している。

演習期間	・ コースは「基礎演習（1 or 2 or 5 日間）」、「実践演習（4 日間）」、「攻撃者視点演習 COP（5 日間）」、「産業制御コース（2 or 5 日間）」がある。
対象者 育成スキル	・ 基礎演習の対象者については、セキュリティ担当者、または IT 分野で 3 年以上の実務経験のある方を想定している。 ・ 育成されるスキルとしては、個人のスキルアップに加え、グループワークによるチーム力とリーダーシップ力を養成することができる。
参加人数	・ 基礎演習・実践演習・産業制御コースは各回 20 名。攻撃者視点演習は各回 10 名。
特徴、優位点	・ TAME Range は、コマンドラインを使用せず、GUI 的な操作によって攻撃可能であるため、講師はコマンドラインへの入力ではなく、受講生のケアに時間を割ける。 ・ 時間帯を調整することで、海外から演習への参加が可能であり、海外サプライチェーンへの攻撃を想定したケースを体験できる。 ・ サイバー攻撃を実際に体験できること、再現性が高いことが強みである。

（7） 日立製作所 ：サイバー防衛訓練サービス

項目	概要
演習環境	・ 大みか事業所（茨城県日立市）内に、サイバー攻撃を想定した防衛訓練施設「NxSeTA」を設置。社会インフラ事業や製造業向けにリモート環境での実践的なインシデント対応訓練を提供している。 ・ 対面・オンライン形式に対応している。
シナリオ	・ 受講者は IT システムまたは OT システムの担当者として、別室からのサイバー攻撃に対処する。シナリオは担当者向けの他に、経営者向けも用意しているため、担当者からの報告をもとに事業継続の可否を判断するような訓練も可能となっている。
演習期間	・ 2 日間（オンラインの場合）
対象者 育成スキル	・ 演習の対象者は、経営層から現場部門までを想定している。 ・ 育成スキルとしては、訓練時の行動記録などをもとに、分析や判断といったスキルだけでなく、人・組織の連携といった視点でも対応力を評価し、教育や訓練計画の策定に生かすことができる。
参加人数	・ 約 20 人
特徴、優位点	・ 訓練対象は経営層から現場部門まで幅広く想定している。 ・ IT/OT を連携させた総合訓練が可能となっている。 ・ 多様で最新のインシデントパターンにも対応している。

（8） 富士通ラーニングメディア ：サイバーレンジによる実践的インシデント訓練

項目	概要
演習環境	・ サイバーレンジによる仮想的に用意された企業ネットワークを使用して、演習を実施する。 ・ 対面・オンライン形式に対応している。
シナリオ	・ システム運用の現場において、セキュリティインシデントが発生した場合、多様な OS やミドルウェア、プロダクト、ネットワーク機器やセキュリティ機器から発生する情報を収集し、セキュリティインシデントかどうかの判断が求められる。本演習では、セキュリティインシデント発生時における初動対応を実現するために、簡易的な調査や分析が行えることを確認する。
演習期間	・ 2 日間
対象者 育成スキル	・ 演習の対象者は、一般的なシステム開発、運用を担当するエンジニアを想定している。 ・ 育成スキルとしては、本演習修了後、次の事項ができることを目標としている。 1. システム構成を理解し影響と暫定対処のシナリオを推論できる 2. 各 OS のコマンドを理解、初動としてのログ採取や保全、一次分析などが行える 3. セキュリティインシデント発生時に現場で初動対応の指示とインシデントのクロージングができる
参加人数	・ 指定なし
特徴、優位点	・ 同社のセキュリティ人材育成ノウハウなど実践的な内容を盛り込んだ研修を最新のテク

	ノロジーとともに学べ、様々な価値観を持った人と意見をぶつけ合い解決策を考え抜くためのリアルな場を提供している。 ・ 実際にサイバー攻撃の脅威を体験し、訓練を通じて新ビジネス創出のチャンスに変えていくための発想力を養う場を提供している。 ・ 仮想環境上に実際の業務データの流れを構築し、攻撃側と防御側に分かれて疑似体験できるコンテンツを豊富に用意している。初心者から専門家の育成まで幅広いニーズに対応可能となっている。

（9） ラック ：ラックセキュリティアカデミー 情報セキュリティ事故対応 2 日コース実機演習編

項目	概要
演習環境	・ 座学でインシデントレスポンスのノウハウを学習した後、ファイアウォールやサーバで構成された実機環境を使用し、演習を実施する。 ・ 対面形式での開催を想定している。
シナリオ	・ 情報セキュリティ事故が発生した際の対応方法、インシデントレスポンスを学ぶコースとなっている。座学でインシデントレスポンスのノウハウを学習した後、ファイアウォールやサーバで構成された実機環境を使用し、演習を実施する。謝罪のタイミング、サービスを止めるか否かなどのハンドリング、ログ調査なども含めたシナリオを想定している。
演習期間	・ 2 日間
対象者 育成スキル	・ 演習の対象者は、一般社員、管理職、IT 技術者（インフラ系・開発系）、情報システム・セキュリティ推進部門担当者、SOC（セキュリティ運用）要員、CSIRT 要員（管理系・技術系）、監査担当を想定している。 ・ 育成スキルとしては、以下のような対応を習得する。 - インシデントレスポンス体制の構築にあたり、必要な準備事項を抽出する - 被害者、顧客、警察など対外対応や、社員に対する社内対応を経験し、具体策を検討する。 - インシデントレスポンスの演習を通して、事故防止を含めたリスクコントロールの方針を検討する。
参加人数	・ 20 名（最低開講人数 5 名）
特徴、優位点	・ 専門性の高い講師陣による実践的な情報セキュリティ教育プログラムを提供することにより人材育成に貢献する。 ・ プログラムは、本講座のような対面型の「集合研修」の他、インターネット受講の「オンライン研修」の講座も用意されており、希望に応じてオーダーメイドトレーニングも行なっている。

2.1.2　国内のサイバー演習（公的機関）

国内の公的機関の提供するサイバー演習の、演習環境、シナリオ、演習期間、対象者や育成スキル、参加人数、特徴・優位点などの観点から以下の（1）～（2）のとおり、サービス内容の調査を行った。

（1）　情報通信研究機構　：実践的サイバー防御演習「CYDER」

項目	概要
演習環境	・ 組織のネットワーク環境を模した仮想環境で擬似的に発生させたサイバー攻撃に対して、具体的な対応の検討を行い、実際にツールを操作して対処を行う実践課題に取り組む。 ・ 対面・オンライン形式に対応している。
シナリオ	・ 例えば USB からのマルウェア感染による事例など、シナリオに基づく課題を通じて、サイバー攻撃の検知から事後対応までの一連の流れを学ぶ。
演習期間	・ 事前学習：2～5時間程度 ・ 演習時間：1～2 日間
対象者 育成スキル	・ 演習の対象者は、情報システムに携わり始めたばかりの方（初級）、情報システム管理者・運用者（中級）、セキュリティ対策・管理業務を統括する責任者（準上級）など、受講者のレベルに合わせて A～C コース及びオンラインコースが用意されている。 ・ 育成スキルとしては、コースのレベルごとに見合った粒度で、インシデント発生～解決までの一通りのセキュリティインシデント対応手順を身に着けることができる。
参加人数	・ 1チーム4名
特徴、優位点	・ 実際のネットワーク環境を再現したリアルな環境で一連の流れを体験できる ・ 現実のサイバー攻撃事例を再現した最新の演習シナリオを用意している。 ・ 座学のみで終わらない本格的なトレーニングとなっている。 ・ 講師・チューターによるサポートも充実している。 ・ 受講目的等に合わせてコース選択が可能となっている。

（2）　情報処理推進機構　産業サイバーセキュリティセンター（ICSCoE）：制御システム向けサイバーセキュリティ演習（CyberSTIX）

項目	概要
演習環境	・ 産業用制御システム（ICS：Industrial Control System）の模擬システムを用いたサイバー攻撃と対応のハンズオン演習により、実践的な防御方法を習得する。 ・ 基本対面での開催を想定している。
シナリオ	・ 模擬プロセス制御ネットワークを使用して、機器の不正な制御に使用されるサイバー攻撃や対応策による防御を体験することで、制御システムのセキュリティについてより深く理解することができる実践的な内容となっている。
演習期間	・ 2 日間
対象者 育成スキル	・ 演習の対象者は、制御システムのサイバーセキュリティを担当している方、又は今後担当を予定されている方を想定している。 ・ 育成スキルとしては、IT と制御システムのアーキテクチャ、セキュリティ脆弱性、および制御システムに固有の対策など、産業用制御システムのセキュリティを習得することができ

	る。
参加人数	・最大 20 名
特徴、優位点	・産業用制御システム（ICS：Industrial Control System）の模擬システムを用いたサイバー攻撃と対応のハンズオン演習により、実践的な防御方法を習得できる。 ・産業用制御システムのセキュリティを、IT におけるセキュリティとの差を認識しながら習得することができる。

2.1.3　海外のサイバー演習（民間事業者）

海外の民間事業者の提供するサイバー演習の、演習環境、シナリオ、演習期間、対象者や育成スキル、参加人数、特徴・優位点などの観点から以下の（1）～（2）のとおり、サービス内容の調査を行った。

（1） SANS Institute（米国）：SANS Cyber Ranges Net Wars Core

項目	概要
演習環境	・ SANS インストラクターによって構築された、仮想的かつインタラクティブで隔離された環境でスキルを適用し、実践的な経験を積むことができる。 ・ ライブオンライン開催（ハイブリッド開催）とオンライン形式に対応。
シナリオ	・ AWS のクラウドコンテンツなどをフィーチャーし、ストーリー仕立てのチャレンジで、サイバーセキュリティの必須スキルの学習と実践を継続的に行うことができる。 ・ トピック例： - 侵入テスト - 高度なデータベースハッキング - 共通管理システムの脆弱性の悪用 - リバースエンジニアリングとデバッグ - ログ分析による脅威検出
演習期間	・ ライブオンライン（Net Wars トーナメント）の場合：2日間 ・ オンライン形式（Net Wars Continuous）の場合：4 ヶ月間、24 時間 365 日アクセス可能
対象者 育成スキル	・ 演習の対象者は、情報セキュリティ初心者～専門家まで想定しており、演習にはスキルに応じてレベル1～5のレベルが含まれており、自分に合ったコースを選ぶことができる。 ・ 育成スキルとしては、IT と制御システムのアーキテクチャ、セキュリティ脆弱性、および制御システムに固有の対策など、産業用制御システムのセキュリティを習得することができる。
参加人数	・ 指定なし
特徴、優位点	・ 競争力とゲーミフィケーションにフォーカスしたコンテンツとなっている。 ・ 個人およびチーム向け双方に対応している。 ・ スキルの練習と評価が可能となっている。 ・ 実環境とは分離された環境で演習できる。 ・ 専門家の戦術、ヒントを得ることができる。 ・ インシデントレスポンスの時間の短縮を実現する。 ・ 受講者のスキルレベルに応じたサイバーレンジコースを用意している。 ・ 常に最新かつ最先端のコースを用意している。

（2） Infosec（米国）：Cyber Ranges

項目	概要
演習環境	・ 仮想化された模擬的な演習環境を使用する。追加のソフトウェア、ハードウェア、サーバスペースを必要としない。

	・基本オンライン形式を想定している。
シナリオ	・MITRE ATT&CK Matrix の戦術とテクニックから身を守る方法、侵入テストを実行する方法、安全なコードを実際に書く方法を学ぶことができる。ビジネスにおける運用環境内の現実的なシナリオを想定している。
演習期間	・指定なし
対象者 育成スキル	・演習の対象者は情報セキュリティ技術者・管理者を想定している。 ・育成スキルとしては、以下の項目についてチームのスキルを高めることができる。 - レッドチームとブルーチーム演習を実行する。 - 安全なコードを作成する。 - 実践的なドメイン知識を習得することにより、数十の技術認定に合格する。 - クラウドベースのアプリケーションへの攻撃と防御を習得する。
参加人数	・指定なし
特徴、優位点	・実践的なトレーニングによって、学習者の関与を深め、チームのスキルアップをより迅速に支援する。 ・ソフトウェア開発チームにソフトウェアの脆弱性を悪用する方法を示し、実用的かつ安全なコーディングスキルでリスクを軽減する方法を教える。 ・52 NICE Framework にマッピングされた役割に関連する実践的なトレーニングで、IT チームのセキュリティの専門知識を強化する。 ・明確な学習目標でサイバーワークをわかりやすく説明する。

2.1.4 海外のサイバー演習（公的機関）

海外の公的機関の提供するサイバー演習の、演習環境、シナリオ、演習期間、対象者や育成スキル、参加人数、特徴・優位点などの観点から以下の（1）～（2）のとおり、サービス内容の調査を行った。

（1） The NATO Cooperative Cyber Defense Centre of Excellence（CCDCOE）：Locked Shields

項目	概要
演習環境	・レッドチーム対ブルーチーム形式でのリアルタイム演習 ・基本的に対面で実施を想定している。（2021 年実績）
シナリオ	・大規模なサイバー攻撃を想定し、仮想的な国の IT システムと重要なインフラストラクチャの保護を実践する。多数のサイバーフィジカルシステムを保護することに加えて、参加チームは、法的問題にも取り組み、IT 運用の危機的状況において、戦術的および戦略的な意思決定、協力、および指揮系統を実践する。
演習期間	・2 日間
対象者 育成スキル	・演習の対象者は、サイバーセキュリティの専門家を想定している。 ・育成スキルとしては、リアルタイム攻撃の下で国の IT システムと重要なインフラストラクチャを保護するスキルを向上させることができる。
参加人数	・32 カ国から 2000 人以上の参加者（2021 年実績）
特徴、優位点	・現実的なシナリオ、最先端のテクノロジー、および戦略的意思決定、法的およびコミュニケーションの側面を含む、大規模なサイバーインシデントの複雑さ全体をシミュレートする

	ことができる。

（2） The Cybersecurity and Infrastructure Security Agency（CISA）：Cyber Storm

項目	概要
演習環境	・ 実際の構成要素を実現するために、シミュレートされ動的に更新されるプラットフォーム上の環境で演習を実施する。
シナリオ	・ 産業制御システム・運用技術に対する攻撃と、従来の企業ネットワークに対する攻撃が含まれる。攻撃者はゼロデイ・エクスプロイトを用いて、標的型攻撃を仕掛けるといったシナリオとなっている。
演習期間	・ 3 日間（2022 年実績）
対象者 育成スキル	・ 演習の対象者は、連邦政府、州・地方政府、民間セクター、国際的なパートナーにおける重要インフラのサイバーセキュリティ関係者、技術専門家、広報担当者、法務担当者、経営層などを想定している。 ・ 育成スキルとしては、参加者は自組織を標的としたサイバー攻撃の解決に取り組む一方で、情報を共有し、インシデント対応を外部と調整する能力を訓練する。
参加人数	・ 2,000 名以上（2022 年実績）
特徴、優位点	・ 国家サイバーセキュリティ計画と政策の有効性を検討する。 ・ サイバーインシデント時における役割と責任を探る。 ・ サイバーインシデント時に使用する情報共有と調整のメカニズムを強化する。 ・ 官民パートナーシップを促進し、パートナー間で関連性のあるタイムリーな情報を共有する能力を向上させる。

2.1.5　各サイバー演習の相違点等についての比較

前項までに提示した各サイバー演習の相違点等について比較を行う。比較の観点は、(1)対象者(2)シナリオ、対象システム (3)演習環境の観点で、以下のとおり整理した。

企業名	サービス名	対象者	シナリオ、 対象システム	演習環境
Armoris (凸版印刷グループ)	実践的人材育成プログラム「DOJO」	・技術者 ・管理者	・ 自社システムへのサイバー攻撃 ・ IT システム	・対面／オンライン ・出張形式
NEC	NEC サイバーセキュリティ訓練場演習	・技術者	・ 自ら堅牢化したシステムへの攻撃 ・ IT システム	・対面／オンライン
グローバルセキュリティエキスパート	Micro Hardening: Enterprise Edition	・技術者	・ EC サイトのサーバへの攻撃 ・ IT システム	・対面／オンライン
サイバージムジャパン	Cyber-Threats and Defense Essentials	・技術者	・ 自社システムへのサイバー攻撃 ・ IT システム	・対面 ・実機訓練あり
サイバーディフェンス研究所	サイバー演習	・技術者 ・管理者 ・犯罪捜査官など	・ 自社 WEB サービスへの攻撃 ・ 自社システムへのサイバー攻撃 ・ IT システム	・対面
サイバーナレッジアカデミー(大日本印刷グループ)	サイバーナレッジアカデミー	・技術者 ・管理者	・ 自社システムへのサイバー攻撃 ・ 産業制御系システムへの攻撃 ・ IT システム／OT システム	・対面／オンライン ・出張形式
日立製作所	サイバー防衛訓練サービス	・技術者 ・管理者 ・経営層	・ 自社システムへのサイバー攻撃 ・ 産業制御系システムへの攻撃 ・ IT システム／OT システム	・対面／オンライン ・実機訓練あり
富士通ラーニングメディア	サイバーレンジによる実践的インシデント訓練	・技術者	・ 自社システムへのサイバー攻撃 ・ IT システム	・対面／オンライン
ラック	ラックセキュリティアカデミー	・一般社員 ・技術者 ・管理者 ・監査担当	・ 自社システムへのサイバー攻撃 ・ IT システム	・対面 ・実機訓練あり

情報通信研究機構	実践的サイバー防御演習「CYDER」	・技術者 ・管理者	・ 自社システムへのサイバー攻撃 ・ IT システム	・対面／オンライン
ICSCoE	制御システム向けサイバーセキュリティ演習（CyberSTIX）	・技術者	・ 産業制御系システムへの攻撃 ・ OT システム	・対面 ・実機訓練あり
SANS Institute	SANS Cyber Ranges Net Wars Core	・技術者 ・管理者	・ 自社システムへのサイバー攻撃 ・ IT システム	・対面／オンライン
Infosec	Cyber Ranges	・技術者	・ 自社システムへのサイバー攻撃 ・ IT システム	・オンライン
CCDCOE	Locked Shields	・技術者	・ 自社システムへのサイバー攻撃 ・ IT システム	・対面
CISA	Cyber Storm	・技術者 ・管理者 ・広報、法務担当 ・経営層	・ 自社システムへのサイバー攻撃 ・ 産業制御系システムへの攻撃 ・ IT システム／OT システム	・対面／オンライン

全体の傾向として、実践性を訴求するサイバー演習というサービスの特性から、演習の対象者はセキュリティ技術者及び管理者向けを対象としたものが多いが、中にはインシデント時の全社的な対応を想定して経営層などのマネジメント層、広報、法務、監査担当などのセキュリティ部門以外のコーポレート職も対象としている演習も存在する。

サイバー演習のシナリオ、対象システムについては、自社 IT システムへのサイバー攻撃を想定したものが主流となっているが、産業制御系システムへの攻撃を想定した演習シナリオに対応したベンダーも出てきている。製造業や重要インフラを狙ったサプライチェーン攻撃の脅威が増している背景から、今後も制御系システムへのサイバー攻撃を想定した演習の需要は拡大していくものとみられる。

演習環境については、2020 年のコロナ禍をきっかけにオンライン形式でのサイバー演習が普及したため、現在では対面とオンライン双方に対応しているサービス提供者が増えている。一方、対面かつハンズオンで講師がレクチャーすることが強みであるサービスも多く、基本的に対面開催を想定しているサービス提供者も一定数存在する。また、ユーザ側の環境に講師が出向いて、遠隔でサイバー演習システムに接続して演習を行う出張形式のサイバー演習サービスを提供可能なサービス提供者もいる。また、顧客の持つ制御システム等を複製した実機を用意する演習も存在している。ユーザ環境と全く同じものを用意することは不可能だが、そのアーキテクチャを再現する。シミュレータではなく実機であることによって、実践性を謳っているサービスとなっている。

2.2　サイバー演習を企画・運営する主体

国内外の民間事業者及び公的機関の沿革、規模、IR 情報、セキュリティ事業における提供製品・サービス・位置づけ、特徴等について、以下のとおり整理した。

2.2.1　国内のサービス提供者（民間事業者）

国内のサイバー演習サービスを提供する民間事業者の沿革、規模、IR 情報、セキュリティ事業における提供製品・サービス・位置づけ、特徴等について、公開情報から把握可能な範囲において以下の（1）～（9）のとおり整理した。

（1）　Armoris（凸版印刷グループ）

項目	概要
沿革	2019 年 9 月　凸版印刷がセキュリティ人勢育成プログラムの提供に特化した新会社 Armoris を設立。 2020 年 1 月　基幹サービス「DOJO」開始 2020 年 6 月　初級者向けサイバー演習「DOJO Lite」 提供開始
規模	＜凸版印刷のデータ＞ 資本金　1,049 億 8,600 万円（2022 年 3 月末現在） 連結従業員数　54,336 名（2022 年 3 月末現在）
IR 情報	売上高　1,547,533（百万円）、 営業利益　72,505（百万円）
提供セキュリティ製品・サービス	サイバーセキュリティ人材育成トレーニング、Web セキュリティ診断サービス、Managed Security Service 等
セキュリティビジネスの位置づけ	凸版印刷においては、情報コミュニケーション事業分野の中の印刷以外の価値を提供するソリューション事業分野としての位置付けとなっている。Armoris としては、サイバー演習サービスを専門に提供する企業として設立されている。
演習サービスの特徴	自社システムが狙われたサイバー攻撃を想定し、現実の脅威に対抗する実践的なトレーニングを行う。

（2）　NEC

項目	概要
沿革	2015 年　北陸先端科学技術大学院大学と連携し、サイバーセキュリティに関する最先端の研究活動と人材育成を目的とした寄附講座「サイバーレンジ構成学」を開設。サイバーレンジ（サイバー空間の演習場）の構築技術を研究開発し、これを用いた教育プログラムを設計・開発。 2021 年 3 月　安全な DX システムを実現するセキュリティ人材の育成と発掘を支援する演習型の教育サービスを提供開始。
規模	資本金　4,278 億円（2022 年 3 月末現在） 連結従業員数　21,350 名（2022 年 3 月末現在）
IR 情報	売上高　3,014,095（百万円）、 経常利益　132,525（百万円）
提供セキュリティ製品・サービス	脆弱性診断などの各種セキュリティソリューションの導入支援といった「テクノロジー」の観点、セキュリティリスクアセスメントやセキュリティ監査などの「組織プロセス」の観点、セキュリティ教育・サイバー演習などの「人材育成啓発」の観点で製品・サービスを展開。
セキュリティビジネスの位置づけ	DX 推進に必要なセキュリティ対策を、「テクノロジー」、「組織プロセス」、「人材育成啓発」の 3 つの観点で用意し、顧客のビジネス継続を支援する。
演習サービスの特徴	システム構築フェーズの演習にフォーカスし、仕込まれた脆弱性の探索や課題解決を実際に体験させることができる。 自ら堅牢化したシステムがサイバー攻撃の被害に遭うという衝撃的な体験が、受講

	者の意識浸透の最後の一押しになる。

（3） グローバルセキュリティエキスパート

沿革	2000 年 4 月 設立 2019 年 1 月 超実践型サイバーセキュリティ演習トレーニングである Micro Hardening：Enterprise Edition をリリース 2020 年 12 月 野村総合研究所との資本提携 2021 年 12 月 東京証券取引所マザーズ市場に上場
規模	資本金 485（百万円） 従業員数 118 名
IR 情報	売上高 4,391（百万円）、 営業利益 439（百万円）
提供セキュリティ製品・サービス	セキュリティコンサルティング・脆弱性診断・各種サイバーセキュリティソリューション等の製品・サービスを展開。
セキュリティビジネスの位置づけ	情報セキュリティ・サイバーセキュリティに特化した専門会社となっている。
演習サービスの特徴	シンプルかつ、ゲーム感覚で楽しく経験でき、楽しさは記憶の定着にも継続にも直結する。 忙しいエンジニアの方にも極めて短時間で効率的なスキルアップが可能。 情報処理安全確保支援士の特定講習にも指定されている。

（4） サイバージムジャパン（バルクホールディングスグループ）

沿革	1994 年 業務プロセスに関するコンサルティング事業及びマーケティングリサーチ事業を目的として設立 2017 年 イスラエル Cyber Gym Control Ltd.と基本合意書を締結 2018 年 サイバーセキュリティトレーニングを行う米国子会社社 Strategic Cyber Holdings LLC を設立 2020 年 サイバージムジャパンを設立
規模	資本金 9 億 8,320 万円（2022 年 3 月末現在） 連結従業員数 61 名（2022 年 3 月末現在）
IR 情報	売上高 1,931,834（千円）、 経常利益 50,053（千円）
提供セキュリティ製品・サービス	・情報セキュリティ認証コンサルティング ・サイバーセキュリティソリューション （サイバーセキュリティトレーニング、脆弱性診断サービス等）
セキュリティビジネスの位置づけ	セキュリティ事業及びマーケティング事業が主であり、特にセキュリティ事業においてもセキュリティトレーニング事業がマーケティング事業（売上高 602,250 千円）と同規模（売上高 586,691 千円）を占める。
演習サービスの特徴	・ 様々な重要インフラ分野におけるグローバルかつ高度な知識・ノウハウを有している。 ・ 実戦経験に基づく独自開発のトレーニングプログラムを有している。 ・ IT 環境だけでなく、OT 環境に焦点をあてたトレーニングプログラムを保有している。 ・ 事前にプログラム化されたサイバー攻撃ではなく、ホワイトハッカーによるオンタイムの攻撃などカスタマイズ可能な実践的トレーニングプログラムを実施することが可能となっている。 ・ 実戦経験のある多数のホワイトハッカーを活用している。 ・ 情報処理安全確保支援士特定講習にも指定されている。

（5） サイバーディフェンス研究所

沿革	2022 年 2 月 オンライン自学自習プラットフォーム「INFINITY CHAMBER」をリリース 2013 年 3 月 NEC の 100%子会社となる

	2008 年 10 月　サイバーディフェンス研究所設立
規模	資本金 100(百万円) 従業員数　非公開
IR 情報	売上高　非公開、 営業利益　非公開
提供セキュリティ製品・サービス	・ セキュリティ診断事業(Web アプリケーション、ネットワークなどのペネトレーションテスト) ・ 教育サービス事業(パブリックコース/プライベートコース) ・ インシデントレスポンス、フォレンジック事業 ・ セキュリティコンサルティング事業(各種ソフトウェア及び組み込み機器へのセキュリティ評価/サイバー演習実施支援) ・ セキュリティ製品販売
セキュリティビジネスの位置づけ	情報セキュリティ・サイバーセキュリティに特化した専門会社となっている。元々は伊藤忠商事の社内のセキュリティ研究所であった。
演習サービスの特徴	・ 組織内 CSIRT やインシデントレスポンス担当者のみでなく、法執行機関のサイバーテロ対策担当者の技術力の向上への活用も想定した内容となっている。 ・ 用意されているプランのみでなく、カスタマイズしたサイバー演習も提供可能となっている。

（6） サイバーナレッジアカデミー(大日本印刷グループ)

沿革	2022 年 5 月　産業制御システムのセキュリティ対策のための教育プログラム、大日本印刷(DNP)と同グループのサイバーナレッジアカデミー(CKA)、三菱電機の 3 社が共同で開発 2020 年 11 月　オンライン演習を開講 2016 年 3 月　サイバーナレッジアカデミー設立、サービス提供開始
規模	＜大日本印刷のデータ＞ 資本金 1,144 億 6,476 万円(2022 年 3 月 31 日現在) 従業員数 36,542 名(連結)(2022 年 3 月 31 日現在)
IR 情報	売上高　1,344,147(百万円)、 営業利益　66,788(百万円)
提供セキュリティ製品・サービス	サイバーセキュリティに関する技術的対策・人的対策・組織的対策の観点で各種サイバーセキュリティソリューション、コンサルティング、教育サービス等を提供
セキュリティビジネスの位置づけ	情報イノベーション事業部部門におけるプラットフォームサービスという位置づけ
演習サービスの特徴	・ TAME Range は、コマンドラインを使用せず、GUI 的な操作によって攻撃可能であるため、講師はコマンドラインへの入力ではなく、受講生のケアに時間を割ける。 ・ 時間帯を調整することで、海外から演習への参加が可能であり、海外サプライチェーンへの攻撃を想定したケースを体験できる。 ・ サイバー攻撃を実際に体験できること、再現性が高いことが強みである。

（7） 日立製作所

沿革	2021 年 6 月　自宅やサテライトオフィスなどから参加できる重要インフラ事業者向けのサイバー防衛訓練サービスの提供を開始 2017 年 8 月　サイバー攻撃対応のための総合訓練・検証施設を開設し、重要インフラ事業者向けのサイバー防衛訓練サービスを提供開始
規模	資本金　461,731 百万円(2022 年 3 月末現在) 従業員数　29,485 名(2022 年 3 月末現在)
IR 情報	売上高　10,264,602 百万円(連結)(2022 年 3 月期)、営業利益　738,236 百万円(連結)(2022 年 3 月期)
提供セキュリティ製品・サービス	セキュリティコンサルティング、教育、各種サイバーセキュリティソリューション、フィジカルセキュリティなど幅広く展開
セキュリティビジネスの位置づけ	社会インフラを支える日立グループとして、サイバー・フィジカル両面からユーザ企業の事業を守るセキュリティソリューションを提供している。
演習サービスの特徴	・ 訓練対象は経営層から現場部門まで幅広く想定している。

	・ IT/OT を連携させた総合訓練が可能となっている。 ・ 多様で最新のインシデントパターンにも対応している。

（8） 富士通ラーニングメディア

沿革	2017 年 CYBERIUM（サイベリウム）/Shinagawa を開設 1994 年 富士通ラーニングメディアに社名変更
規模	資本金 300百万円（2022 年 3 月末現在） 従業員数 633 名（2022 年 3 月末現在）
IR 情報	売上高 151 億円、営業利益 非公表
提供セキュリティ製品・サービス	・法人向け人材育成・研修サービス ・人材育成に関するコンサルティング、人材力診断／適性診断等の提供 ・研修講座（コース、カリキュラム）の企画、開発、実施、運営および運営支援 ・コース教材／マニュアル等の開発、制作、翻訳、出版および販売 ・人材／研修講座の運営／マニュアル制作の管理に関連するソフトウェアの開発および販売
セキュリティビジネスの位置づけ	IT/DX に関する人材育成サービスの内、セキュリティに関するコンテンツも提供している。
演習サービスの特徴	・ 同社のセキュリティ人材育成ノウハウなど実践的な内容を盛り込んだ研修を最新のテクノロジーとともに学べ、様々な価値観を持った人と意見をぶつけ合い解決策を考え抜くためのリアルな場を提供している。 ・ 実際にサイバー攻撃の脅威を体験し、訓練を通じて新ビジネス創出のチャンスに変えてゆくための発想力を養う場を提供している。 ・ 仮想環境上に実際の業務データの流れを構築し、攻撃側と防御側に分かれて疑似体験できるコンテンツを豊富に用意している。初心者から専門家の育成まで幅広いニーズに対応可能となっている。

（9） ラック

沿革	2013 年 12 月 KDDI 株式会社との間で、事業拡大に向けた業務・資本提携を強化 2009 年 4 月 情報セキュリティ教育事業としてラックセキュリティアカデミーを開設 1995 年 4 月 情報セキュリティ事業を開始 1986 年 9 月 ラック設立
規模	資本金 2,648 百万円 従業員数 2,172 名（2022 年 4 月 1 日現在）
IR 情報	売上高 20,382 百万円（2022 年 3 月期）、営業利益 133 百万円（2022 年 3 月期）
提供セキュリティ製品・サービス	・セキュリティソリューションサービス ・ システムインテグレーションサービス ・ 情報システム関連商品の販売およびサービス
セキュリティビジネスの位置づけ	セキュリティ事業及び SI 事業が主事業となっている。
演習サービスの特徴	・ 専門性の高い講師陣による実践的な情報セキュリティ教育プログラムを提供することにより人材育成に貢献する。 ・ プログラムは、本講座のような対面型の「集合研修」の他、インターネット受講の「オンライン研修」の講座も用意されており、希望に応じてオーダーメイドトレーニングも行なっている。

2.2.2　国内のサービス提供者（公的機関）

国内のサイバー演習サービスを提供する公的機関の沿革、規模、IR 情報、セキュリティ事業における提供製品・サービス・位置づけ、特徴等について、公開情報から把握可能な範囲において以下の（1）～（2）のとおり整理した。

（1）　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

沿革	2021年11月　実践的サイバー防御演習 CYDER の「オンライン A コース」を提供開始 2018年4月　同機構が開発したサイバー演習自動化システム「CYDERANGE」（サイダーレンジ）の「CYDER」事業での実運用を開始 2015 年 4 月　国立研究開発法人情報通信研究機構に名称変更
規模	資本金　145,555 百万円（2022 年 3 月末現在） 常勤職員　446名
IR 情報	財源（収入）　73,603　百万円（2022 年 3 月末現在）
提供セキュリティ製品・サービス	サイバーセキュリティ技術の研究開発、産学官連携拠点形成、暗号技術の研究開発と普及促進、IoT 機器の調査、サイバーセキュリティ人材育成
セキュリティ事業の位置づけ	サイバーセキュリティを戦略的に進めるべき 4 つの研究領域の一つとしている。社会（生命・財産・情報）を守る能力を高める技術について、基礎研究から社会実装、人材育成まで幅広く貢献することでイノベーションを促進していくとしている。
演習サービスの特徴	・ 実際のネットワーク環境を再現したリアルな環境で一連の流れを体験できる ・ 現実のサイバー攻撃事例を再現した最新の演習シナリオを用意している。 ・ 座学のみで終わらない本格的なトレーニングとなっている。 ・ 講師・チューターによるサポートも充実している。 ・ 受講目的等に合わせてコース選択が可能となっている。

（2）　情報通情報処理推進機構　産業サイバーセキュリティセンター（ICSCoE）

沿革	2017 年 4 月　産業サイバーセキュリティセンター（ICSCoE）発足 2004 年 1 月　独立行政法人　情報処理推進機構設立
規模	資本金　13,710 百万円（2022 年 3 月末現在） 職員数　517 名（うち非常勤 114 名）（2022 年 4 月 1 日現在）
IR 情報	財源（収入）　20,689 百万円（2022 年 3 月末現在）
提供セキュリティ製品・サービス	・ J-CSIP・J-CRAT ・ 制御システムのセキュリティリスク分析事業 ・ 独立行政法人等のセキュリティ監査・監視事業 ・ 脆弱性対策促進事業 ・ セキュリティ対策の普及啓発事業（IT 利用者向け） ・ セキュリティ対策の普及啓発事業（中小企業向け） ・ セキュリティ製品認証事業 ・ セキュリティ評価事業
セキュリティ事業の位置づけ	サイバー攻撃から企業・組織を守る取り組みや、国民に向けた情報セキュリティ対策の普及啓発、IT 製品・システムの安全性を確保するための制度運用などを推進している。

演習サービスの特徴	・ 産業用制御システム(ICS:Industrial Control System)の模擬システムを用いたサイバー攻撃と対応のハンズオン演習により、実践的な防御方法を習得できる。 ・ 産業用制御システムのセキュリティを、IT におけるセキュリティとの差を認識しながら習得することができる。

2.2.3 海外のサービス提供者(民間事業者)

海外のサイバー演習サービスを提供する民間事業者の沿革、規模、IR 情報、セキュリティ事業における提供製品・サービス・位置づけ、特徴等について、公開情報から把握可能な範囲において以下の(1)～(2)のとおり整理した。

(1) SANS Institute(米国)

沿革	2006 年～ 非同期オンライントレーニング(SANS OnDemand)と仮想同期教室形式(SANS vLive)を提供 1989 年 SANS Institute 設立
規模	資本金 非公開 従業員 約 1,200 名
IR 情報	年間収益 3 百万ドル
提供セキュリティ製品・サービス	・ セキュリティトレーニングや GIAC 試験、出版活動 ・ インターネットストームセンターや SCORE と呼ばれるプロジェクト運営 ・ FBI(米国連邦捜査局)と共同で脆弱性 Top20 などのリストの発表 など
セキュリティ事業の位置づけ	情報セキュリティ、サイバーセキュリティトレーニング、および証明書の販売を専門としている。
演習サービスの特徴	・ 競争力とゲーミフィケーションにフォーカスしたコンテンツとなっている。 ・ 個人およびチーム向け双方に対応している。 ・ スキルの練習と評価が可能となっている。 ・ 実環境とは分離された環境で演習できる。 ・ 専門家の戦術、ヒントを得ることができる。 ・ インシデントレスポンスの時間の短縮を実現する。 ・ 受講者のスキルレベルに応じたサイバーレンジコースを用意している。 ・ 常に最新かつ最先端のコースを用意している。

(2) Infosec(米国)

沿革	2004 年 サイバーセキュリティトレーニングソフトウェアを開発 1998 年 Infosec 設立
規模	資本金:非公開 従業員約 175 名
IR 情報	年間収益 3.1 百万ドル
提供セキュリティ製品・サービス	セキュリティトレーニング(INFOSEC IQ、INFOSEC Skills)

セキュリティ事業の位置づけ	情報セキュリティ及びサイバーセキュリティトレーニングを専門としている。
演習サービスの特徴	・ 実践的なトレーニングによって、学習者の関与を深め、チームのスキルアップをより迅速に支援する。 ・ ソフトウェア開発チームにソフトウェアの脆弱性を悪用する方法を示し、実用的かつ安全なコーディングスキルでリスクを軽減する方法を教える。 ・ 52 NICE Framework にマッピングされた役割に関連する実践的なトレーニングで、IT チームのセキュリティの専門知識を強化する。 ・ 明確な学習目標でサイバーワークをわかりやすく説明する。

2.2.4 海外のサービス提供者（公的機関）

海外のサイバー演習サービスを提供する公的機関の沿革、規模、IR 情報、セキュリティ事業における提供製品・サービス・位置づけ、特徴等について、公開情報から把握可能な範囲において以下の（1）～（2）のとおり整理した。

（1） The NATO Cooperative Cyber Defense Centre of Excellence（CCDCOE）

沿革	2018 年 1 月 CCDCOE は同盟国中のすべての NATO 機関のためにサイバー防衛における教育訓練ソリューションを特定し調整する責任を負っている。 2008 年 5 月 エストニアとドイツ、イタリア、ラトビア、リトアニア、スロバキア、スペインの 6 カ国の主導で CCDCOE 設立
規模	25 の NATO 加盟国が参加している。
IR 情報	非公表
提供セキュリティ製品・サービス	教育、研究開発、教訓、協議により、サイバー防衛における NATO、その加盟国、パートナー間の能力、協力、情報共有を強化する。
セキュリティ事業の位置づけ	サイバー防衛を目的とした組織
演習サービスの特徴	現実的なシナリオ、最先端のテクノロジー、および戦略的意思決定、法的およびコミュニケーションの側面を含む、大規模なサイバーインシデントの複雑さ全体をシミュレートすることができる。

（2） Cybersecurity and Infrastructure Security Agency（CISA）

沿革	2018 年 11 月 Cybersecurity and Infrastructure Security Agency（CISA）設立
規模	人員 2,500 名（2021 年）
IR 情報	年間予算 3.16 億ドル（2020 年）
提供セキュリティ製品・サービス	サイバーセキュリティプログラムの策定、政府主導の演習の実施など
セキュリティ事業の位置づけ	米国国土安全保障省（DHS）の機関であり、政府のサイバーセキュリティとインフラストラクチャ保護を強化し、サイバーセキュリティプログラムを米国の州と調整し、民間および国家のハッカーに対する政府のサイバーセキュリティ保護を改善する責任を負っている。

演習サービスの特徴	・国家サイバーセキュリティ計画と政策の有効性を検討する。 ・サイバーインシデント時における役割と責任を探る。 ・サイバーインシデント時に使用する情報共有と調整のメカニズムを強化する。 ・官民パートナーシップを促進し、パートナー間で関連性のあるタイムリーな情報を共有する能力を向上させる。

2.3　国内外のサイバー演習市場の動向

国内外のサイバー演習やセキュリティ教育・トレーニングに関する市場規模、市場予測、プレイヤー動向等の情報を収集・整理した。

2.3.1　国内のサイバー演習市場の動向

（1）　調査対象市場の定義

- 日本国内でサイバーセキュリティ教育やトレーニングを提供するサービスの内、仮想環境や専用の演習システム上でサイバー攻撃に対する防御の演習を実施し、サイバーセキュリティ技術やインシデント対応を学習するサービスを対象として定義している。
- サービス提供者が独自演習システムを開発して提供するケースと、他社製の演習システムを購入して利用するケースがあるが、今回の動向調査では、両方を対象としている。

（2）　市場概況

世界情勢の変化によるサイバー攻撃被害の増加や、攻撃への事後対処の重要性の認識が浸透してきたことによって、サイバー攻撃への対応力強化を検討する企業は増加傾向にあり、実際の攻撃を受けた場合を想定して訓練できるサイバー演習サービスへの需要が高まっている。

また、従来サイバー攻撃の標的は大手の企業や組織に対するものが中心であったが、近年は大手企業とサプライチェーンを構成するグループ会社や取引先の中小企業を標的とする攻撃が増加していることから、中小企業についてもサイバー演習サービスの受講を検討する企業が増加している。

（3）　市場規模・予測

2021 年から 2027 年にかけてのサイバー演習の日本国内の市場規模の実績と予測については下表 1 のとおりである。

単位：百万円、%

	2021 実績	2022 見込み	2027 予測	CAGR 21/27
金額	3,000	3,500	5,100	9.2
前年比	-	116.7	-	

表 1 国内市場規模推移

出所）富士キメラ総研「2022 ネットワークセキュリティビジネス調査総覧 市場編<サイバーセキュリティ演習サービス>」を基に三菱総合研究所作成

- 2021 年度の市場規模は 3,000 百万円となっており、2027 年に向けて 9.2%の CAGR で推移するものと予測されている。コロナ禍における非対面開催に対するニーズを受けて、各サービス提供者でオンライン形式のサイバー演習のサービス展開が進んだことから、市場規模の成長予測は堅調な推移となっている。
- 2022 年度は、3,500 百万円（前年比 116.7%）に達する見込みとなっており、製造業や金融業界を中心にサプライチェーン攻撃やランサムウェアによる攻撃をはじめとするサイバー攻撃の被害

が増加したことから、サイバー演習への需要が高まっているものとみられる。サービス提供者側も産業制御系システムのシナリオを組み込んだサービスを展開するなど、世の中の攻撃の傾向やニーズに応じた演習シナリオやサービス拡充を図っており、市場の拡大が見込まれている。

- また、近年はサイバー攻撃を完全に防ぎきることは難しいという考えに立ち、攻撃された場合を想定してインシデントレスポンス等の迅速な対応によって被害の拡大を防ぐ「事後対処の重要性」への認識が浸透してきている。そのことから、サイバー攻撃が発生した際の事業継続を可能とする対応力強化に向けて、サイバー演習では実際にサイバー攻撃を受けて受講者が対処する演習を実施することができるため、今後も需要が継続して見込まれる。
- 海外製のサイバー演習システムを活用したサービスを開発して、新規参入するベンダーも増加してきており、今後も市場規模は拡大傾向で推移するものと予測されている。

（4） ユーザ業種/従業員規模別市場動向

2021 年から 2027 年にかけてのユーザ業種/従業員規模別の市場動向については下表 2 のとおりである。

単位：百万円、%

	2021		2027		CAGR		2021		2027		CAGR
	実績	比率	予測	比率	27/21		実績	比率	予測	比率	27/21
超大手	1,600	53.3	2,800	54.9	9.8	製造	700	23.3	1,400	27.5	12.2
大手	1,100	36.7	1,600	31.4	6.4	金融	1,000	33.3	1,600	31.4	8.1
中堅	250	8.3	600	11.8	15.7	流通	100	3.3	200	3.9	12.2
中小	50	1.7	100	2.0	12.2	サービス	100	3.3	250	4.9	16.5
合計	3,000	100.0	5,100	100.0	9.2	情報通信	600	20.0	1,000	19.6	8.9
						公共	400	13.3	500	9.8	3.8
						その他	100	3.3	150	2.9	7.0
						合計	3,000	100.0	5,100	100.0	9.2

表 2 国内ユーザ業種/従業員規模別市場動向（2021 年度実績、2027 年度予測）

出所）富士キメラ総研「2022 ネットワークセキュリティビジネス調査総覧 市場編＜サイバーセキュリティ演習サービス＞」を基に三菱総合研究所作成

- 2021 年度及び 2027 年度共通して、超大手・大手企業の比率を足した割合は 80%～90%程度となっており、非常に高い割合を占めている。サイバー演習はセキュリティトレーニング関連のサービスの中でも比較的高額かつ、ユーザ企業側も人員を一定期間演習時間に充てなければいけないことから、予算及び人的リソースの体力がある超大手・大手企業の比率が高くなっているとみられる。
- サプライチェーン攻撃の増加などの背景から、サイバー攻撃は中小企業が標的となるケースも増加しており、中小企業向けにコストを抑えたプランやサービスが増加していることを背景として、2027 年度にかけて、中堅・中小企業の市場規模が拡大していくと予測されている。
- 業種別では、サプライチェーンを多く持つ製造業や、サイバーセキュリティ意識の高い金融業や情報通信業での実績が大きくなっている。特に製造業においては、近年サプライチェーン攻撃の被害が顕在化していることから、比率が高まっていくものと予測されている。

（5） 主要プレイヤーの動向

- サイバーナレッジアカデミー（大日本印刷グループ）

・ 同社はイスラエル製の実践的サイバー演習システム「TAME Range」を活用し、標的型攻撃や We への攻撃など様々な攻撃手法を想定した演習シナリオによる実践的な演習サービスの提供を強みとしている。
・ 2022 年度は、前年度に引き続きオンラインでのサービス提供を進めているほか、サプライチェーン攻撃やランサムウェア攻撃などのトレンドに合わせたシナリオを拡充している。
・ 顧客層としては、製造業や金融業の大手企業が大半を占めているほか、官公庁や公的機関などの公共向けにも一定の顧客を獲得している。特に工場や重要インフラ向けに産業制御システム向けのコースも提供しており、徐々に高まりつつある OT セキュリティニーズの獲得を図っている。産業制御システム向けのコースは、三菱電機の OT 向けソリューション「サイバーセキュリティソリューション OTGUARD」の教育プログラムのコンテンツの一つとしても提供されている。
・ 攻撃者目線での学習とペネトレーションテストのスキルの習得等を目的とした「サイバーオフェンスプロフェッショナル」等の上級向けコースも提供しており、受講するユーザ企業のレベルに合わせた需要の取り込みを図っている。

- グローバルセキュリティエキスパート

・ 同社は中小企業向けの IT セキュリティに関するサイバー演習やセキュリティエンジニア向けの養成講座、標的型メール訓練サービス等、多岐にわたるセキュリティ教育ソリューションを提供している。
・ 同社の提供する「Micro Hardening：Enterprise Edition」は川口設計製の「Micro Hardening」を活用して提供され、サイバー攻撃に対応する方法をゲーム形式で学ぶハンズオントレーニングによってサイバー攻撃の検知・対処を繰り返し実践することで、企業のセキュリティ人材の育成に必要不可欠な「現場の経験」を提供することを強みとしている。
・ 2022 年度は、中小企業のエンジニア向けの提供を中心に順調に推移し、今後も同社が提供するその他のセキュリティトレーニングサービス等と組み合わせた販促に取り組んでいく方針とみられる。
・ セキュリティ堅牢化競技会である「ハードニング競技会」をデザインし、実現するボランティア・プロジェクトである「Hardening Project」に参画しており、サイバーセキュリティ業界全体でのインシデント対処スキル向上を推進している。

2.3.2　海外のサイバー演習市場の動向

（1）　市場規模・予測

2021 年から 2028 年にかけてのサイバー演習のグローバルの市場規模の実績と予測については下図 2-1 のとおりである。

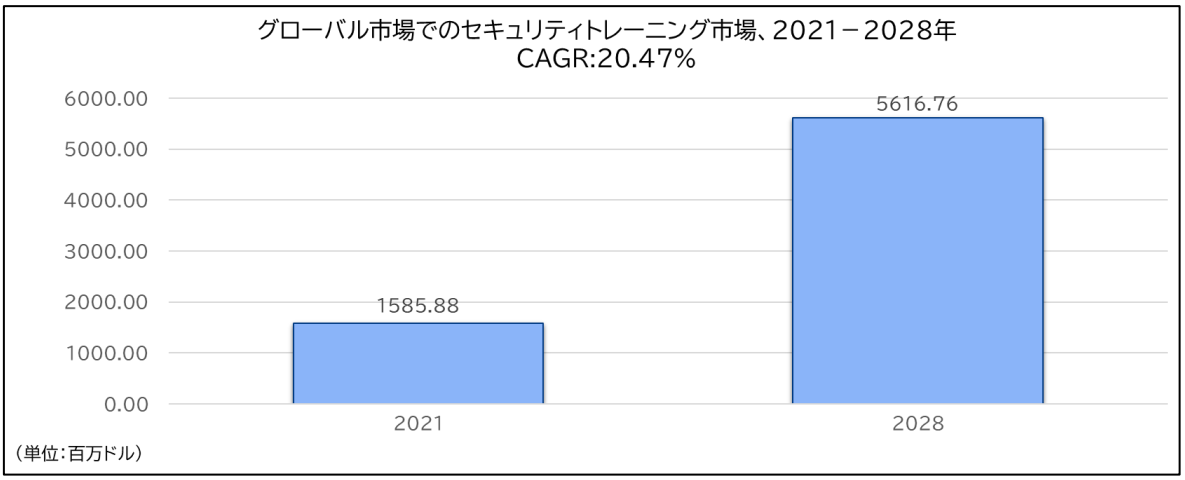

図 2　グローバル市場でのセキュリティトレーニング市場（2021 年度実績、2028 年度予測）

出所）グローバルインフォメーション https://www.gii.co.jp/report/qyrl170456-global-cyber-security-training-market-insights.html（2023 年 3 月 13 日取得）より三菱総合研究所作成

- グローバルのサイバーセキュリティトレーニングの市場規模は、2021 年の 15 億 8,588 万米ドルから、2028 年までに 56 億 1,676 万米ドルに達すると予測されている。また、2022 年から 2028 年の間に 20.47%の CAGR で成長する見込みとなっている。
- 不安定な国際情勢を受け、世界的な経済安全保障及びサイバーセキュリティに対する重要性の高まっていることにより、サイバー技術及びサイバーセキュリティ人材育成の重要性がさらに高まっている。
- また、コロナ禍の影響で、世界中の企業でリモートワークが採用され、サイバーセキュリティの需要が増している。さらに、オンラインバンキングサービスの利用が拡大していることから、世界中の銀行、金融サービス、保険などの金融分野でサイバーセキュリティ技術の導入が進んでおり、技術を使いこなす為の人材を育成するためにグローバル市場においてもサイバー演習を始めとするセキュリティトレーニングの需要が増している。

（2）　主要プレイヤーの動向

- The Cybersecurity and Infrastructure Security Agency（CISA）：Cyber Storm

Cyber Storm は、米国の DHS（国土安全保障省）の機関である CISA のもと、サイバー攻撃による国家レベルの危機が発生した際の対応能力の検証を目的として、2006 年から約 2 年の間隔で実施されている。この演習を通じ、サイバー攻撃への国・州・他国・民間という業界を超えたサイバー攻撃対応及び連携強化を図っている。細かいシナリオは公開されていないが、複数の IT サービスが攻撃を受け、企業、政府、医療、決済のシステムがそれぞれ同時に被害を受ける想定である。攻撃元の IP アドレスをブロックすることがトリガーとなって、マルウェアがシステムに不具合を発生させるなど、実際に発生して

いる攻撃手法を用いた高度な攻撃が展開される。この攻撃に対応するには個社を超えて、政府機関等との連携が必須となるシナリオとなっている。

3. 先進的サイバー防御機能・分析能力に係る技術動向の調査

本章では日本のサイバーセキュリティの確保に向けた官民連携や分析能力の強化について検討を行うことを目的として、先進的サイバー防御機能・分析能力に係る技術動向に関し、研究や民間事業者等が提供するサービスの技術概要や動向の調査結果を記載する。

3.1 調査概要

本事業の背景・目的に鑑み、将来に向けて注意すべき特徴的な攻撃動向についても調査を行った。先進的なサイバー防御機能・分析能力に係る技術動向は米国国立標準技術研究所（NIST※）の「重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1 版」（以下、「NIST CSF」）に沿って整理することで、当該技術がサイバー攻撃対策のどのフェーズに寄与するものかわかるようにした。

※ NIST: National Institute of Standards and Technology

（1） 調査対象とする技術分野

本調査で対象とした主な技術分野は以下の通りである。

- 攻撃検知・解析技術、攻撃者の手口解析、マルウェア・不正アクセスの解析といったサイバー攻撃に関する技術
- 脆弱性検知・評価技術、ペネトレーションテストといった脆弱性検知に関する技術
- アトリビューション技術、偽情報関連技術技術動向の全体的な整理

サイバー攻撃対策のフレームワークである「NIST CSF」と、先進的なサイバー防御機能・分析能力の技術分野の関係をまとめた表を以下に作成した。

表 3 先進的なサイバー防御機能・分析能力の技術

NIST CSF（バージョン 1.1）		先進的なサイバー防御機能・分析能力の技術動向 技術内容
識別	資産管理	・ 脆弱性の評価、管理の自動化に関する技術
	ビジネス環境	
	ガバナンス	
	リスクアセスメント	・ AI を活用したサイバー空間の情報分析技術（OSINT、偽情報分析）
		・ AI を活用したペネトレーションテストの自動化技術
		・ 脆弱性の評価、管理の自動化に関する技術
	リスクマネジメント戦略	
	サプライチェーンリスクマネジメント	・ OSINT 等を活用したリスクのスコア化に関する技術
防御	アイデンティティ管理認証/アクセス制御	・ AI 等を活用した利用者の行動分析に基づくリスクベース認証
		・ マイクロセグメンテーションなどの高度なアクセス制御技術
	意識向上およびトレーニング	
	データセキュリティ	・ 耐量子計算機暗号技術
		・ QNSC や QKD などの量子情報通信技術
	情報を保護するためのプロセスおよび手順	・ データ消去技術（暗号鍵の消去）
		・ 暗号解読やマルウェアによって暗号化されたデータの解読・復号技術
	保守	
	保護技術	・ AI セキュリティ
検知	異常とイベント	・ AI を活用した攻撃の検知・評価技術
		・ xDR などの統合監視技術
	セキュリティの継続的なモニタリング	・ 攻撃動向の詳細を把握するためのデセプション技術
		・ AI を活用したペネトレーションテストの自動化技術
		・ AI を活用した脆弱性の検知・評価技術
	検知プロセス	
対応	対応計画	
	コミュニケーション	
	分析	・ 攻撃者を特定するアトリビューション技術
	低減	
	改善	・ 先進的なセキュリティ対策のアーキテクチャ
復旧	復旧計画	
	改善	
	コミュニケーション	

出所）IPA、「重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1 版（和訳）」を基に三菱総合研究所作成

3.2　将来に向けて注意すべき特徴的なサイバー攻撃

本項では高度化・複雑化するサイバー攻撃の中でも既存のセキュリティ防御機能を回避する攻撃や最新技術を悪用した攻撃など、将来に向けて特に注意すべき特徴的な攻撃について被害事例やサイバー脅威調査・予測レポート及び最新のニュース記事等の調査結果を踏まえて記載する。これらの脅威に対する防御技術や分析能力の強化に向けて継続的に技術開発等に取り組む必要がある。

3.2.1　最新技術を悪用した攻撃

技術の発展に伴い登場した AI などの最新の技術を悪用し、サイバー攻撃に利用する手口が増加している。

（1）　対話型 AI の利用

ChatGPT に代表される AI(人工知能)チャットボットがサイバー攻撃に悪用される可能性が出てきている。ChatGPT は OpenAI が開発した AI チャットボットである。この対話型 AI は「大規模言語モデル(Large Language Model、以下 LLM)」と呼ばれる AI 技術を活用し、インターネット上の膨大なデータを集積し、人間からの質問に的確に回答するよう設計されている。また、質問を通じてプログラミング言語によるソースコードを生成、さらにバグを修正することも可能である。

攻撃者はこれらの機能を悪用し、フィッシング攻撃を成功させるために有効となる自然な文章や回答を生成したり、脆弱性スキャンやエクスプロイト等の作成を行ったりする可能性が考えられる。

参考）
[1] 「ChatGPT とサイバーセキュリティの関係」、https://www.sompocybersecurity.com/column/column/chatgpt-and-cybersecurity、2023年3月11日閲覧
[2] 日経クロステック「サイバー攻撃者が「ChatGPT」に熱視線、AI によるマルウェア作成の可能性が急浮上」、https://xtech.nikkei.com/atcl/nxt/column/18/00676/011900125/、2023年3月11日取得
[3] NEC「ChatGPT とセキュリティに関わる課題」、https://jpn.nec.com/cybersecurity/blog/230227/index.html、2023年3月13日閲覧

（2）　ディープフェイク(deepfake)

機械学習アルゴリズムの一つである深層学習(ディープラーニング)を使用して、2 つの画像や動画の一部を結合させ元とは異なる動画を作成する技術で作成されたフェイク動画、偽動画が、あたかも本物の情報として誤って認知されるなど社会課題になっている[1]。また動画や画像だけでなく、ディープフェイク音声を使ったビジネスメール詐欺(Business Email Compromise、BEC)が増加するとの見込みもある[2]。BEC とは業務上の偽メールで送金を促して金銭をだまし取る詐欺行為であるが、本人確認のための電話の相手が本人にそっくりの偽音声である場合、さらに信ぴょう性が増すため、攻撃者は詐欺をより実効しやすくなる可能性がある。

参考）
[1] NEC ソリューションイノベータ（nec-solutioninnovators.co.jp)、https://www.nec-solutioninnovators.co.jp/ss/insider/security-words/33.html、2023 年 3 月 18 日閲覧
[2] 日経クロステック、https://xtech.nikkei.com/atcl/nxt/mag/nc/18/092400133/020900099/、2023 年 3 月 19 日閲覧

（3）　AI による攻撃対象の探索・侵入・攻撃の自動化

AI が攻撃対象に関係する情報を学習し、適切な攻撃手段を用いた攻撃を自動的に実施する手法の研究開発事例がある。三井物産セキュアディレクションの開発したDeep Exploitは、主要なペネトレーションテストツールである Rapid 7 社の Metasploit に AI による支援機能を掛け合わせることで、ネットワークスキャンの結果やホスト情報等のデータを学習し、自動的に効果的な攻撃コードの選択や生成を行った上で、実行することを可能にしている。本ツールによって、ペネトレーションテストの実施効率の向上が期待できる。

（4） AI ファジングによる未知の脆弱性検出

試験対象に非定型データを入力し未知の脆弱性の発見等を行うファジングテストにおいて、AI の利用によってその効率を向上させた研究事例がある。独フラウンホーファー研究所の AI セキュリティ研究者 Konstantin Böttinger は、深層強化学習によって、ターゲットにより多くの変異を起こすデータを用いたファジングテストを考案、完全なランダムデータによるファジングテストと比較して良好なベンチマーク結果を得ている。

（5） 量子技術を悪用した暗号解読

量子コンピュータの技術開発は急速に進んでいるが、現時点で危険性が指摘されている「RSA 暗号」や「楕円曲線暗号」を解読する能力を持ったものは未だ存在していない[1]。富士通は量子シミュレーターを活用した RSA 暗号の安全性評価として、RSA 暗号を解読する量子アルゴリズム（ショアのアルゴリズム）を用いた暗号解読に必要な量子ビットと量子ゲート数を評価し、それを満足する量子コンピュータの実現は短期的には困難であることを発表している[2]。一方であらかじめデータを盗聴しておき、将来の量子コンピュータで解読する「ハーベスティング攻撃」が懸念されている[3,4]。

参考）
[1] 日経クロステック、https://xtech.nikkei.com/atcl/nxt/column/18/00989/021600110/、2023 年 3 月 19 日閲覧
[2] 富士通、https://pr.fujitsu.com/jp/news/2023/01/23.html、2023 年 3 月 19 日閲覧
[3] 東芝、https://www.global.toshiba/jp/products-solutions/security-ict/qkd/cases/case1.html、2023 年 3 月 19 日閲覧
[4] 量子コンピュータによる暗号解読の可能性 | NTT データ、https://www.nttdata.com/jp/ja/data-insight/2018/0611/、2023年3月13日閲覧

3.2.2　既存のセキュリティ防御機能を回避する攻撃

（1）　AI の悪用による不正メール検知機能の回避

不正メール検知ツールの応答を学習することで、検知機能を回避可能なメール文面を生成する攻撃手法が報告されている。従来攻撃者が人手で行っていた細工を、AI を悪用してより効率的な試行に自動化し、検知回避能力を向上させる 2019 年 9 月 8 日に報告された Proof point Email Protection の検知パイバスに関する脆弱性は、検知ツールの情報を収集し、検知モデルを模倣した機械学習分類モデルを構築することで、検知機能を回避可能な不正メールの作成が可能であるというものであった。

（2）　AI の悪用によるアンチマルウェア機能の回避

アンチウイルスソフトの検知結果を機械学習し、検出を回避するマルウェアの生成手法に関する研究がある。Black Hat USA 2017 で発表された Gym-malware は、アンチウイルスソフトの判定結果を強化学習し、マルウェアの動作に影響しない範囲でコード等の改変を繰り返すことで、悪性判定を受けることを回避するマルウェアの生成に成功している。

（3）　Living off the land 攻撃によるアンチマルウェア機能の回避

攻撃者が対象システムに侵入した後に、さらなる侵害のためにマルウェアやハックツールを追加で送り込むことをせず、侵害したシステム内に正規ファイルとして存在しているツールやバイナリを活用して攻撃を継続する方法であり、ウイルス対策ソフトなどのエンドポイントセキュリティを回避しやすい特徴がある。環境寄生型攻撃や現地調達型攻撃と表現されることもあり、この攻撃手法は検知を逃れることを最優先とする標的型の攻撃者に利用されている。

参考）

1. Living off the land というサイバー攻撃の方法論: NEC セキュリティブログ ｜NEC、https://jpn.nec.com/cybersecurity/blog/220916/index.html、2023年3月13日閲覧
2. Living off the Land（環境に寄生する）手法：ハッカー達はあなたの環境にどうやって紛れ込むのか -Darktrace Blog、https://ja.darktrace.com/blog/living-off-the-land-how-hackers-blend-into-your-environment、2023年3月13日閲覧
3. ウイルス対策ソフトを突破?「ファイルレスマルウェア」｜BizDrive（ビズドライブ）－あなたのビジネスを加速する｜法人のお客さま｜NTT 東日本（ntt-east.co.jp）、https://business.ntt-east.co.jp/bizdrive/column/dr00095-001.html、2023年3月13日閲覧

（4）　先進的なエンドポイントセキュリティ機能「EDR」の回避

振る舞いを検知する EDR を回避する「TrickGate」と呼ばれるサービスの存在が明らかになっている。これは、「Emotet」「Formbook」「Maze」といったマルウェアの拡散に利用されていた。

参考）

[1] 6 年間見つからなかった「サイバー攻撃者のお気に入り」を特定　チェック・ポント、https://atmarkit.itmedia.co.jp/ait/articles/2302/16/news049.html、2023 年 3 月 20 日閲覧

（5）　高度な認証機能の回避

認証機能の回避（バイパス）は、最近の ID とパスワードだけでは認証として不十分なため、多要素認証（MFA）や二段階認証などが採用されているが、これらを回避する攻撃が発生している。

1） CAPTCHA のバイパス

ロボットによるアクセスを拒否するための認証機構の一つである CAPTCHA に対し、事前学習したデータによって認証を突破する手法が見つかっている。ソフトウェアエンジニアの Adam Geitgey 氏が行った検証では、大量の CAPTCHA 画像をディープラーニングによって学習し、CAPTCHA による bot 判定を回避することに成功している。また、GAN を用いてより学習効率を向上し、より少ない数の画像で同様の結果が得られている。

2） 多要素認証（MFA）の回避

認証の強化として使われる多要素認証（MFA）を回避する技術が出ている。

a. MFA 疲労

“他のケースでは、人のエラーによって MFA が破られています。シラキュース大学が内部メールシステムに MFA を実装した後、攻撃者が「MFA 疲労」と呼ばれる攻撃によって学生や職員にスパムを仕掛けようとしました。攻撃者はフィッシングやその他の手口でメールの資格情報にアクセスし、ユーザーデバイスへ複数の MFA リクエストを送信しました。ユーザがリクエストにうんざりして拒否を怠ることを期待したのです。ユーザ認証リクエストを承認してしまうと（たとえそれがうるさい電話通知を止めようとしただけであっても）、攻撃者は大学のリソースやアカウントへさらに深くアクセスできるようになりました。”

出所）多要素認証をバイパス ｜ Cloudflare、https://www.cloudflare.com/ja-jp/learning/insights-bypassing-mfa/、2023年3月13日閲覧

b. Pass-The-Cookie

“Pass-The-Cookie とは、Web アプリケーションのセッション Cookie を攻撃者が何らかの手段で入手し、セッション Cookie を悪用して認証をバイパスする攻撃手法です。有効なセッション Cookie をブラウザに投入するだけで Web アプリケーションにログインすることが可能です。セッション Cookie は、ログイン成功状態を保持しています。そのため、セッション Cookie を入手し、ブラウザに投入することで ID/Password 認証及び多要素認証要求をバイパスし、一気にログイン成功状態に遷移することができます。”

出所）多要素認証のバイパスが可能な攻撃「Pass-The-Cookie」について: NEC セキュリティブログ ｜ NEC、https://jpn.nec.com/cybersecurity/blog/221007/index.html、2023年3月13日閲覧

（6） AI によるサイドチャネル攻撃のための分析実行

暗号化された通信やデータの復号化技術として一般的に次のものがある。

ブルートフォース攻撃

- 正しい鍵が見つかるまで、あらゆる可能な鍵を試す。

辞書攻撃

- パスワードの推測を試みるために単語のリストを使用する。

レインボーテーブル攻撃

- 事前に計算されたハッシュのテーブルを使用して、パスワードを解読する。

サイドチャネル攻撃

・　暗号化システムの弱点（タイミングや消費電力など）を突いて鍵を取り出す。

サイドチャネル攻撃は、暗号を処理するハードウェア等の電力や熱等の物理特性データを計測し、解析することで装置内部の秘匿情報等を不正に読み取る形で行われることが一般的だが、計測データの解析は難易度が高く、多くの労力を要するともいわれている。Google が開発実証した SCAAML という手法では、収集した物理特性データを深層学習することで、ハードウェア内に保存された暗号鍵を効率的に解析することに成功している。

3.2.3　その他、特筆すべきサイバー攻撃

（1）　サービス化された攻撃手段

サイバー攻撃を行うためのハッキングツールやマルウェア、脆弱なネットワークへのアクセス情報などを売買するマーケットは以前から存在していたが、最近、犯罪者のコミュニティが急速に広がっており、防御策を回避する商用セキュリティツールが攻撃に転用されることもある。

「ソフォス脅威レポート2023年版」によると、以下の9つのサービス化された犯罪手段が存在し、サイバー犯罪のためのマーケットが構成されていることがわかる。

1. 侵害されたアカウントやシステムにアクセスするための情報をサービスとして販売。
2. 特定の地域や業界、また、さらに広い範囲にマルウェアを配信するサービスを販売。
3. フィッシングのための偽装サイト、結果を監視する画面など包括的なサービスを販売。
4. 攻撃シミュレーションツールを月額のサブスクリプションサービスなどとして販売。
5. マルウェアを暗号化し、アンチウイルス製品による検出を回避する機能をサービスとして販売。
6. 暗号通貨詐欺に関連した「詐欺用キット」を販売。
7. 標的ユーザが人ではなくボットと対話することを選択できる「AI システム」を販売。
8. SMS やメールなどのさまざまな方法で大量のスパムメールを送信するサービスを販売。
9. 脆弱性を特定するツールをサービスとしてユーザに販売し、スキャンさせる。攻撃者にはスキャンの結果がメールで送信される。

参考）
[1] 2023 年に企業を襲うセキュリティの脅威と傾向について｜サイバーセキュリティ.com（cybersecurity-jp.com）、https://cybersecurity-jp.com/column/76913、2023年3月15日閲覧
[2] ランサムウエアから自社を守れ ～事例から学ぶ企業のセキュリティトレンド～ ｜DATA INSIGHT｜NTT データ - NTT DATA、https://www.nttdata.com/jp/ja/data-insight/2021/0910/、2023年3月13日閲覧
[3] https://sophos.axisjp.co.jp/topics/17341/、2023 年 3 月 19 日閲覧

3.3 先進的な技術の動向

2023 年に経済や社会に影響を与えうるサイバーセキュリティの動向を調査したレポート Global Cybersecurity Outlook 2023[1]では先進的な技術として AI との回答が 20%になる。またマッキンゼーによるレポート[2]では、今後 3 年から 5 年に注目される技術としてユビキタスデータと情報プラットフォームへのオンデマンドアクセス、サイバーAI と自動化技術の台頭、攻撃サーフェスの拡大が含まれている。さらに Deloitte は 3 年以内にサイバーAI と自動化技術が非常に進歩し、インテリジェンスの評価、結論、意思決定が従来よりも 50 倍速くできるようになると予測している[3]。

サイバー空間の情報は非常に多くなり、情報の分析には AI などの最新記述の活用が不可欠になってきている。古典的な OSINT から AI を活用したサイバー空間の情報分析技術のほか、量子技術の活用が考えられる。

参考）
[1] 世界経済フォーラム、Global Cybersecurity Outlook 2023. https://initiatives.weforum.org/global-cyber-outlook/home 2023 年 3 月 18 日閲覧
[2] Cybersecurity trends: Looking over the horizon | McKinsey. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon、2023 年 3 月 18 日閲覧
[3] The future of cybersecurity and AI | Deloitte Insights. https://www2.deloitte.com/us/en/insights/focus/tech-trends/2022/future-of-cybersecurity-and-ai.html、2023 年 3 月 18 日閲覧

3.3.1 AI を活用したサイバー空間の情報分析技術

インターネット上では多様なサービスやコミュニティが形成され、いわば一つの新たな社会領域（「サイバー空間」）となっている[1]。このコンピュータとネットワークからアクセス可能なデジタル化されたサイバー空間に散らばる様々な情報を分析して、「判断・行動するための知識」すなわち「インテリジェンス」とするための取組みはマーケティングを含む様々な分野で積極的に進められており、特に合法的に入手できる公開された情報を分析対象とする OSINT（Open Source Intelligence）の世界市場は大きく成長すると予測されている[2]。

今日では OSINT の対象領域は広く、深くなっており、インターネット上の Web サイトに掲載されている一般公開情報や市販情報のほか、公共情報、ソーシャルメディア、商用データベース、人的情報に加えて、匿名性を持たせるための専用ツールもしくはサービスを利用してしかアクセスでないダークウェブ[3]なども対象に入る。ダークウェブ上には発見された攻撃手法や攻撃者による犯行声明なども掲載されるため、サイバー攻撃対策を効果的に行うにはダークウェブを含めたインテリジェンスは重要である。

組織がサイバー脅威に対して行動を起こし、防御するために利用できる情報、すなわち「サイバー脅威インテリジェンス」を得るには、これら多くのソースから組織にとって重要な情報を膨大な情報を効率的に収集、精査、分析するためには、セキュリティ担当者がよりプロアクティブになるだけでなく、大量のデータを効率的かつ自動的に分析して意味のある情報を抽出する AI 技術の活用が不可欠である[4,5]。

参考）
[1] 総務省、「サイバー空間の在り方に関する国際議論の動向」、https://www.soumu.go.jp/menu_seisaku/ictseisaku/cyberspace_rule/index.html、2023 年 3 月 17 日閲覧
[2] オープンソースインテリジェンス（OSINT）の世界市、https://www.gii.co.jp/report/gmi1223629-open-source-intelligence-market-size-by-security.html、2023 年 3 月 17 日閲覧
[3] トレンドマイクロ、https://news.trendmicro.com/ja-jp/2022-09-06-article-darkweb-overview/、2023 年 3 月

17 日閲覧
［4］ NEC、https://jpn.nec.com/techrep/journal/g17/n02/170217.html、2023 年 3 月 17 日閲覧
［5］ IBM、https://www.ibm.com/downloads/cas/W5XYWEVJ、2023 年 3 月 18 日閲覧

（1） AI 技術を使った OSINT ツールの事例

AI 技術を使った OSINT ツールは膨大な量のデータや会話を検索し、さらなる調査が必要なつながりやリスクを効率的、自動的に特定することなどができる。

Cobwebs Technologies

- 最新の機械学習アルゴリズムを用いてウェブのビッグデータからインテリジェンスを抽出し、重要なインサイトを自動的に生成する。[1]

Rescana

- 人工知能がアセットアトリビューションを行うことで、誤検知を最小限に抑えることができる。[2]

Babel X

- AI を活用した多言語対応のプラットフォーム。あらゆる検索語に対して AI で言語の壁を越える国際検索システム。[3]

espysys

- 自然言語処理（NLP）と機械学習アルゴリズムを使用することで、人間のアナリストが発見することが困難な実用的な洞察を抽出する。[4]

FRONTEO

- オープンソースから得られる、極めて膨大で複雑な情報ネットワークを元に物の流れや、影響力の伝搬度合いを AI で解析し、チョークポイントや隠れた支配を発見する[5]。

参考）
［1］ Cobwebs Technologies、https://cobwebs.com/、2023年3月18日閲覧
［2］ Rescana、https://www.rescana.com/、2023 年 3 月 18 日閲覧
［3］ Babel X、https://www.babelstreet.com/platform/babel-x、2023 年 3 月 18 日閲覧
［4］ espysys、https://espysys.com/blog/ai-for-osint/、2023 年 3 月 18 日閲覧
［5］ FRONTEO、https://osint.fronteo.com/、2023 年 3 月 18 日閲覧

（2） 脅威インテリジェンスへの活用

脅威インテリジェンスとは、攻撃者の意図や能力、設備などに関する情報を整理および分析することで有益な知識を導き出し、使用可能なものに変えたものである。企業は脅威インテリジェンスを活用することで、従来のセキュリティ対策で見逃されるような脅威を事前に把握し、対策を講じることができる。

サプライチェーンリスクマネジメントにおいても、これらのインテリジェンスをスコア化して判断しやすくするレーティング技術の採用が始まっている。

参考）
1. 脅威インテリジェンスとは　種類や内容、利用できる情報源などをわかりやすく解説｜セキュリティの SHIFT（shiftinc.jp）、https://service.shiftinc.jp/column/5541/、2023 年 3 月 13 日閲覧

（3） 偽情報の分析への AI 活用

偽情報キャンペーンは、ソーシャルメディアやその他のチャネルを通じて世論を操作する、いわゆる認知戦（Cognitive Warfare）と呼ばれるものの一部である。その潜在的な影響力から、陸、海、空、宇

宙、サイバー領域に続く紛争領域と見なされるようになってきている。我が国においても国家安全保障戦略（令和 4 年 12 月 16 日　国家安全保障会議・閣議決定）において「偽情報の拡散を含め、認知領域における情報戦への対応能力を強化する」と明記されており、また総務省ではインターネット上のフェイクニュースや偽情報への対策の検討が継続的に進んでおり[1]、同省が設置している「プラットフォームサービスに関する研究会（第 42 回）」において偽情報対策に係る積極的な対策が検討されている[2]。

AI は偽情報を見破るための先進的な技術として活用が検討され、外務省は 2023 年度に AI を活用したシステムを立ち上げ、ソーシャルメディアなどのフェイク情報を収集・分析する予定である[3]。これには AI を活用した OSINT ツールなどの活用が期待される[4]。また、ディープフェイク偽画像の検出手法の開発も進められており[5,6]、さらなる進歩が期待される。

参考）
[1] 総務省、インターネット上のフェイクニュースや偽情報への対策、https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/ihoyugai_05.html、2023 年 3 月 18 日閲覧
[2] プラットフォームサービスに関する研究会、https://www.soumu.go.jp/main_sosiki/kenkyu/platform_service/02kiban18_02000264.html、2023 年 3 月 18 日閲覧
[3] Nikkei Asia、「Japan taps AI to defend against fake news in latest frontier of war」、https://asia.nikkei.com/Business/Technology/Japan-taps-AI-to-defend-against-fake-news-in-latest-frontier-of-war、2023 年 3 月 18 日閲覧
[4] cobwebs、https://cobwebs.com/blog/fake-news-challenges-for-osint/、2023 年 3 月 19 日閲覧
[5] 日本経済新聞、https://www.nikkei.com/article/DGKKZO61483110W2A600C2TEB000/、2023 年 3 月 19 日閲覧
[6] 東京大学、https://www.i.u-tokyo.ac.jp/news/press/2022/202204262039.shtml、2023 年 3 月 19 日閲覧

3.3.2　AI を活用した攻撃検知、対応に関する技術

AI を活用した攻撃検知・対応技術は、サイバーセキュリティの成長分野となっている。AI は悪意のあるファイル、疑わしい IP アドレスのような脅威の関係性をリアルタイムで分析し、セキュリティ担当者が意思決定や脅威への対応にかかる時間を短縮する。また、ネットワーク通信や端末の挙動データ等を AI が学習することで、不正な通信や振舞いを高精度に検知し、必要に応じて遮断等の対応まで実行する。

国内事業者においてもサイバーセキュリティへの AI 活用の取り組みが進んでいる。

情報通信研究機構（NICT）

- AI を用いたサイバーセキュリティオペレーションの自動化技術に関する研究開発。NICT の保有するデータセット、研究開発領域一覧、ハイブリッド脅威分析プラットフォーム等。

三井物産セキュアディレクション株式会社

- AI によるサイバー攻撃の自動化。AI を利用したサイバー攻撃の研究、ペネトレーションテストの自動化、標的型マルウェア攻撃への AI の悪用例等。

KDDI 総合研究所

- トラフィック分析、脆弱性情報解析、ハードウェアセキュリティへの応用、プライバシー保護への活用事例等、セキュリティ対策への AI 利活用等。

（1）　xDR

XDR（Extended Detection and Response）は統合化されたサイバーセキュリティの手段として、

サイバー攻撃、不正アクセス、不正使用といったサイバー脅威を複数のセキュリティ層で可視化、検知、調査、対応を行う新しいアプローチとして登場した技術である。従来のサイロ化されたセキュリティ監視では発見できない脅威に対して、すべてのデータソースを対象として検知と対応を支援する。これにはセキュリティオーケストレーション、オートメーション、レスポンス（Security Orchestration, Automation and Response、SOAR）が含まれる。

AI を搭載した XDR はサイバー攻撃の複雑さを軽減し、検知を迅速化し、レスポンスを調整するよう設計されている。

IBM Security QRadar XDR

- 根本原因の自動分析や MITRE ATT&CK マッピングなどの、専用 AI と事前に構築されたプレイブックを使用して、エンリッチメント、相関、脅威調査の時間を節約する。

（2） AI を活用した未知のマルウェア検知に関する技術

従来型のパターン定義ファイルとの照合方式と異なり、大量のデータからマルウェアの動作を学習することで、未知のマルウェアを検知することを可能とした。アンチウイルスソフト等の高機能化に繋がっている。

（3） 深層学習による DGA で自動生成された悪性ドメインの判別

DGA（Domain Generation Algorism）は、攻撃者がマルウェアから C&C へ向けた通信であるコールバックを隠蔽するための仕組みである。疑似乱数を使ってドメイン名を生成し、侵害したコンピュータと C&C サーバ間で生成されたドメイン名を共有する。攻撃者はこのドメイン名を短時間に変化させることでブラックリストよるセキュリティ防御機能（URL フィルタリング）をすり抜ける。2010年には既にこの仕組みを利用したマルウェアの存在が明らかにサーバたが、最近では深層学習の手法を適用してドメイン名を分析・推測し、C&C サーバとの通信を未然に防ぐ技術が進展し、セキュリティ対策製品への活用が進んでいる。

参考）
[1] マルウェア解析の現場から-06「DGA」｜トレンドマイクロ セキュリティブログ（trendmicro.co.jp）、https://blog.trendmicro.co.jp/archives/3799、2023年3月15日閲覧
[2] DGA マルウェアにより自動生成された悪性ドメインの判別 ｜ CiNii Research、https://cir.nii.ac.jp/crid/1390853649853885824、2023年3月15日閲覧
[3] Efficient Deep Learning Models for DGA Domain Detection（hindawi.com）、https://www.hindawi.com/journals/scn/2021/8887881/、2023年3月15日閲覧
[4] Domain Generation Algorithms（secureworks.com）、https://docs.ctpx.secureworks.com/detectors/dga/、2023年3月15日閲覧

3.3.3 AI を活用した未知の脆弱性への対応技術

（1） SAT ソルバーの応用による未知の脆弱性検出

DARPA による未知の脆弱性検査コンペ Cyber Grand Challenge では、論理命題式 AI ツールである Mayhem が優勝した。本ツールは、SMT ソルバー（SAT ソルバーの拡張）が用いられており、記号実行によりエラーに至る実行パスを論理的・網羅的に検証する。単純なルールベースのファジング

ツールと比較し、一貫してよいベンチマーク性能を実証した。論理型 AI は、アルゴリズム表現に基づいた論理式表現を行うため、事象を網羅的に説明することが可能であり、誤検知が起こらない。結果として Mayhem は米国国防総省から 45 億円を上限に契約を取得した。現在は商用ツールとして一般に流通している。

（2） AI を活用した脆弱性診断

脆弱性診断においても AI 活用が進んでいる。AI を活用した脆弱性診断ではウェブサイトやアプリケーションの脆弱性を、機械学習や RPA などの技術を用いて自動的に広範囲にわたって診断することで、診断時間の短縮、精度の向上が期待される。

AeyeScan は利用者が簡単、高精度に脆弱性診断を行う AI と RPA を活用した自動診断ツールを提供している[1]。Immuniweb は常に最新のガイドラインや攻撃コードを AI が機械学習し、セキュリティスペシャリストとの役割分担により優れたコストパフォーマンスを実現する[2]。

参考）
[1] AeyeScan、https://www.aeyescan.jp/
[2] ImmuniWeb、https://www.immuniweb.jp/

3.3.4 AI を活用したペネトレーションテストの自動化技術

ペネトレーションテストは脅威インテリジェンスやシステムの脆弱性診断を組み合わせて、侵入を試みる攻撃シミュレーションである。単独の脆弱性診断に対して、メールの添付ファイルや URL クリックなどから侵入する攻撃など、実際の攻撃を試みることで組織のセキュリティ対策や被害の大きさを事前に調査できる。攻撃者が実際に行っている攻撃シナリオに沿って侵入や改ざんなどを試みるため、専門的な知識や技術が必要となり、専門の技術者が提供しているサービスを利用するのが一般的である。

BAS（Breach and Attack Simulation）は攻撃者視点からの侵入／攻撃シミュレーションを自動的かつ継続的に行えるソリューションである[1]。これを活用することでペネトレーションテスト技術者の不足および継続的なテストに対応できる。攻撃手法としては、世界中で実際に発生しているサイバー攻撃で使用された膨大な攻撃手法や戦術に関する情報を集約した国際的なフレームワーク MITRE ATT&CK を参考としているものがある。

BAS ソリューションの市場規模は 2020 年の 2 億 1800 万米ドルから、2025 年には 9 億 1500 万米ドルの規模に成長すると予測されている[2]。また、これを提供する主なベンダーには Cymulate、AttackIQ、SafeBreach、Picus Security、XM Cyber 、Keysight、Fortinet などがある[3]。

Pentoma は AI を活用した Web アプリケーションやサーバのセキュリティ脆弱性を効率的に突き止めることができる[4]。NIMIS は Web アプリケーション向けのペネトレーションテストに深層学習と AI 技術をすることで、リスクの高い脆弱性を迅速に発見することが期待されている[5]。

ペネトレーションテストへの AI や機械学習の活用は防衛側にとって有益なものであるが、一方で攻撃者が利用することに注意する。攻撃者は、脆弱性の特定や攻撃ベクトルの生成など、AI の活用で攻撃を自動化することができ、システムをより簡単かつ迅速に侵害できるようになることが懸念される[6]。

参考）
[1] ZDNET「変わり続けるペネトレーションテスト、最新状況を確認する」、https://japan.zdnet.com/storage/2023/03/16/3fa071611a1e795f2fcb8d12204e3d1c/penetrationtest.pdf、2023年3月25日閲覧
[2] GII 市場調査レポート: 自動 BAS（侵害・攻撃シミュレーション）の世界市場（～2025 年）2020年11月13日出版、

https://www.gii.co.jp/report/mama971907-automated-breach-attack-simulation-market-by.html
[3] Gartner、https://www.gartner.com/reviews/market/breach-and-attack-simulation-bas-tools、2023 年 3 月 25 日閲覧
[4] Pentoma、https://pentoma.com/、https://blog.se.works/2018/02/27/the-official-launch-of-our-ai-powered-pen-testing-solution/、2023 年 3 月 19 日閲覧
[5] NIMS、https://nimis.ai/product/、2023 年 3 月 19 日閲覧
[6] https://www.redsentry.com/blog/chatgpt-ai-and-penetration-testing、2023 年 3 月 25 日閲覧

3.3.5 AI を活用した高度な認証技術

金融を含む多くの業界でのインターネットサービス、クラウド利用の拡大に伴い、ID セキュリティ、認証技術の進展がますます必要となっている。

「クレジットカード決済システムのセキュリティ対策強化検討会」の報告書（2023年1月20日）において、利用者の適切な確認に向けた環境整備として、すべての EC 加盟店に対して「利用者であることの適切な確認」としてイシュアーによる本人認証を求めること、及び、その手法としてクレジットカード業界が統一的に推進する対策として現在有力な手法である EMV3DS（*1）の導入を 2024 年度末（2025年3月）を期限として、すべての EC 加盟店に求めることが記載されている。

また、利用者の適切な確認の実効性を担保するためのリスクベース認証のさらなる精度の向上に向けて、AI 等を活用した利用者の行動分析への取組みが期待されている。ユーザのアクセスログ、使用した OS、IP アドレス、ブラウザ等の情報を基に正規ユーザ本人の特徴を学習し、高リスク判定時のみ追加認証要求等を行う。通常の振舞い時の本人認証の効率化、不審なアクセスに対するなりすまし防止等のメリットがある。

参考）
[1] 経済産業省「クレジットカード決済システムのセキュリティ対策強化検討会 報告書」、https://www.meti.go.jp/shingikai/mono_info_service/credit_card_payment/20230120_report.html
[2] OneLogin Blog. https://www.onelogin.com/blog/ai-authentication、2023 年 3 月 17 日閲覧
[3] EMV® 3-D Secure | EMVCo、https://www.emvco.com/emv-technologies/3-d-secure/

3.3.6 攻撃動向の詳細を把握するデセプション技術

攻撃者を発見し被害拡大を防ぐための技術としてハニーポット（Honeypot）がある。これは、サイバー攻撃を受けやすいように設定した機器をおとり（Decoy）としてネットワーク上に公開することで攻撃を誘引し、マルウェアの検体の入手や攻撃手法を分析するものである[1]。主な方法としては OS やアプリケーションの脆弱性を意図的に残した機器をオープンなネットワーク上に配置し、攻撃者の挙動を監視・記録などを行う。

最近の技術の進歩により、攻撃者を欺き、さらに攻撃を遅延・阻止するためのプロアクティブなアプローチとしてデセプション技術（deception、欺瞞技術）という新たな分野が進展している。これは単に脆弱性を意図的に残した機器を設置するという手段ではなく、攻撃者が侵入してくる前提で組織内のネットワークに本物に似せた現実的なおとり（データベース、サーバ、アプリ、ファイル、認証情報など）を配置し、実際の資産と並べておとりとして動作させる。攻撃者がおとりと接触を検知した場合、アラートを発し、セキュリティ担当者に攻撃の早期警告を提供する。この技術を活用することで、セキュリティ態勢の向上、インシデント対応能力の強化、サイバー攻撃の被害が軽減されることが期待される[2]。なお、デセプション技術は既に実施されているセキュリティ対策を強化するもので、それらの対策を突破された時の対策であることに気を付ける必要がある。

MITRE は MITRE ATT&CK に加えて MITRE Engage フレームワークを発表した。このフレーム

ワークでは、積極的な防御のためにデセプション技術を据えている。米国国立標準技術研究所（NIST）もサイバーセキュリティにおけるデセプション技術の役割を強調したガイダンスを発表している。

デセプション技術を使った主な製品は Zscaler、Fortinet、Illusive Networks、LogRythm、Attivo Networks、Rapid7、SEC Technologies、ForeScout、Acalvio、Cymmetria、Allure Security、Fidelis Cybersecurity、GuardiCore などがある[3]。Zscaler は複数のシステムやネットワークに偽の情報を拡散させる分散型デセプションプラットフォーム（DDP）を提供している[4]。この分散型デセプションプラットフォームの市場はサイバーセキュリティ市場の中ではまだ小さいが、活発に成長しており、現在も進化を続けている[5]。また組織がセキュリティ対策としてデセプション技術を導入する場合、攻撃者に本物と思わせるおとりとなる偽情報の設計・展開、および通常業務システムへの干渉の排除など難題も多い。英国のセキュリティベンダ、Lupovis は AI 技術を活用したデセプション製品をより簡単に組織で採用できるようにサービス（Deception as a Service）として展開している[6]。

IT と OT ネットワークが融合する環境におけるセキュリティ対策としてもデセプション技術は効果的に機能するとされており[7]、Fotinet は OT 資産に対応したおとり（Modbus、Bacnet など）を提供している[8]。

参考）
[1] Proofpoint、https://www.proofpoint.com/jp/threat-reference/honeypot、2023 年 3 月 25 日閲覧
[2] https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/ng-csirt01.html、2023 年 3 月 25 日閲覧
[3] Market Tree Research「Global Cyber Deception Market Size, Industry Analysis By Segmentations」、https://markettreeresearch.com/product/global-cyber-deception-market-size-industry-analysis-by-segmentations/、
[4] Zscaler、https://www.zscaler.com/resources/security-terms-glossary/what-is-deception-technology、2023 年 3 月 17 日閲覧
[5] KuppingerCole、https://www.kuppingercole.com/research/lc80340/distributed-deception-platforms-ddps、2023 年 3 月 25 日閲覧
[6] Lupovis、https://www.lupovis.io/challenges-and-opportunities-of-cyber-deception/、2023 年 3 月 25 日閲覧
[7] https://industrytoday.com/securing-iot-ot-systems-with-deception-technology/、2023 年 3 月 25 日閲覧
[8] Fortinet、https://www.fortinet.com/jp/products/fortideceptor、2023 年 3 月 17 日閲覧

3.3.7 攻撃者を特定するアトリビューション技術

アトリビューション（Attribution）とは、サイバー攻撃の犯人を特定することであり、サイバー攻撃やその他のハッキングの加害者を追跡、特定し、責任を負わせるプロセスである。それを行うためには、主に分析者がサイバー攻撃後に証拠を収集し、タイムラインを作成し、証拠をつなぎ合わせることで、誰が、何が侵害の原因かを特定する。

アトリビューションの重要性は、サイバー攻撃者の動機・能力・戦術に関する情報（インテリジェンス）を収集し、将来の起こり得る攻撃に対してより的確な防御策を講じる点、および攻撃の背後にあるグループや個人を特定し、法的または政策的に責任を追及し、サイバー攻撃が容認されないことを明確することで将来の攻撃を抑止する点にある。なお、攻撃元や攻撃対象によっては国際関係に影響を与える可能性がある。

アトリビューションを行う手法には、以下に挙げられた視点での分析を複合的に行い、特定の攻撃者に固有のパターンを特定することがあげられる[3]。

技術的な指標

・ IP アドレス、C&C サーバ、ドメイン、マルウェア、不正ソフトウェアなどの技術的な指標

攻撃者の TTPs

・ 攻撃の戦術、技術、手順（Tactics, Techniques and Procedures）

地政学的な背景

・ 政治的・経済的背景から導かれる動機や要因

デセプション

・ デセプション技術により得られる攻撃者に関する情報

法的な手段

・ 捜査令状や召喚状などの法的手段を用いて得られる情報

フォレンジック

・ 攻撃によって残されたデジタル的な証拠

OSINT

・ ソーシャルメディアの投稿やニュース記事などの公開情報

サイバー攻撃者の特定により不正の兆候を検知して予防措置を講じることは組織にとって共通の課題であるが、民間企業においてはアトリビューションに利用できる情報源や情報量が限られているといった問題もある。

これに対して、MITRE は MITRE ATT&CK フレームワークを提供しており、特定の脅威行為者に関連する通信やインフラのパターンを特定したりすることができる。

参考）

[1] アトリビューション：犯人特定の複雑なパズル（cisco.com）、https://gblogs.cisco.com/jp/2020/08/talos-attribution-puzzle/、2023年3月13日閲覧
[2] AI を活用した不正予防の最前線、PwC アドバイザリーが提供する「デジタルフォレンジックス」｜PwC Japan グループ https://www.pwc.com/jp/ja/knowledge/column/dataanalytics/digital-forensic.html
[3] https://bank-security.medium.com/attribution-in-cyber-threat-intelligence-techniques-and-challenges-6031b85e19ea、2023 年 3 月 26 日閲覧

3.3.8 先進的な量子技術のサイバーセキュリティへの応用

量子コンピュータは AI、バイオテクノロジー、極超音速兵器、宇宙と並んで、米国にとって 5 大外国脅威の 1 つとも言われており、また NATO は、量子を重要な新興技術および破壊的技術の 1 つとして位置づけている。

中国、フランス、ドイツ、英国、米国などの主要企業は、今後数十年にわたって戦略的優位性を獲得するために多額の投資を続けている。量子コンピュータ関連市場が 2030 年には 1250 億ドルにまで成長すると予想もあるが、まだ歴史が浅く、予期せぬ技術革新が起こる可能性があるためあくまで参考程度にとどめておく必要がある。実際のデバイスの販売はまだ限定的であり、現在の主なビジネスは、IBM、Google、Microsoft、Alibaba、Honeywell、IonQ、Rigetti、D-Wave、Amazon などの大手企業が提供するクラウドベースの量子コンピューティングサービス事業の成長にある[1]。

参考）

[1] GlobalData「Quantum Computing in Defense – Thematic Intelligence」、https://www.globaldata.com/store/report/quantum-computing-in-defense-theme-analysis/

（1） 量子技術がサイバーセキュリティにもたらす影響

量子技術は以下の４つの領域でサイバーセキュリティを変革すると期待されている。既存技術では担保されていた安全性を脅かす可能性、量子技術を用いることでさらに高いセキュリティレベルの実現に貢献する可能性がある。

量子鍵配布

- 量子力学を利用して暗号鍵を安全に配布する方法である。量子系を測定すると系が乱れるという原理に基づいている。

ポスト量子暗号

- 量子技術を使うことで現在使われている暗号アルゴリズムの多くが破られる可能性があり、量子コンピュータでも解読困難な新しいアルゴリズムが必要とされている。

量子機械学習

- 量子コンピュータを利用した機械学習である。機械学習アルゴリズムの精度や速度を向上させる可能性があり、サイバー攻撃の検知や予防に活用できる可能性がある。

量子乱数生成

- 従来の乱数生成器は数学的アルゴリズムに基づいているため予測可能であるが、量子乱数生成器は物理法則に基づいているため予測不可能である。

量子コンピュータに関係する技術の進歩は目覚ましく、海外の多くの組織が開発を推進している[1]。IBM は川崎市に国内初の商用量子コンピュータ(27 量子ビット)を 2021 年に設置した。2022 年には 433 量子ビットの QPU(量子プロセッサ)である「Osprey」を発表し、2025 年までに 4,000 量子ビットを超える量子コンピュータの製造を実現する計画である[2]。Google は量子コンピュータ開発において課題となっている量子誤り訂正における重要なマイルストーンしたと発表した[3]。

日本では量子技術イノベーション戦略のロードマップが 2022 年 4 月に改訂されるなど官民連携のもと開発が進められている[4]。理化学研究所量子コンピュータ研究センターらの共同研究グループは量子ゲート方式の超電導量子コンピュータ(64 量子ビット)をインターネットのクラウド公開し、外部からの利用を 2023 年 3 月に開始している[5]。また、NICT の量子 ICT 協創センター[6]は 8 つの量子技術イノベーション拠点のうち「量子セキュリティ拠点」として指定されている。量子 ICT 協創センターは量子暗号に係る国際標準化活動にも積極的に参画し、量子鍵配送ネットワーク(QKDN)及び量子鍵配送装置(QKD 装置)に関する国際標準文書の開発を進めている。

参考)

[1] The Quantum InSIDER「81 Quantum Computing Companies: The Ultimate List for 2023」、https://thequantuminsider.com/2022/09/05/quantum-computing-companies-ultimate-list-for-2022/
[2] 「順調に開発が進む IBM の量子コンピュータ、2023 年以降の展望」、https://texal.jp/2022/12/26/ibms-quantum-computers-in-steady-development-looking-beyond-2023/、2023 年 3 月 27 日閲覧
[3] 「Google の量子コンピュータがエラー訂正のマイルストーンに到達」、https://texal.jp/2023/02/24/googles-quantum-computer-reaches-error-correcting-milestone/、2023 年 3 月 27 日閲覧
[4] 内閣府、量子技術イノベーション、https://www8.cao.go.jp/cstp/ryoshigijutsu/ryoshigijutsu.html
[5] 理研「量子計算クラウドサービス」、https://release.nikkei.co.jp/attach/651815/02_202303241653.pdf、2023 年 3 月 27 日閲覧
[6] NICT・量子 ICT 協創センター、https://www2.nict.go.jp/qictcc/
[7] 量子技術の実用化推進 WG「量子セキュリティ・量子ネットワークの論点等(2022 年 11 月 10 日)」、https://www8.cao.go.jp/cstp/ryoshigijutsu/jitsuyo_wg/2kai/siryo1.pdf

(2) QNSC や QKD などの量子情報通信技術

量子暗号は、共通鍵暗号方式であり復号に必要な鍵情報を、量子力学的な性質を持った光の粒である光子を用いて安全に配送する技術であり、量子鍵配送（Quantum Key Distribution、QKD）と呼ばれる。将来にわたり解読されるリスクがなく超長期的に情報を保護できる暗号方式として、重要な基幹システムなどへの適用が期待されている。送信に必要なビット情報を光子のスピン方向で表し、また送信側と受信側で同じフィルターを用いることで、理論的に安全が確保された鍵配送を行う。量子通信路を用いて安全に共有した乱数の列を使い捨ての暗号鍵として用いることによって，原理的に第三者に解読されない秘匿通信を実現する。量子通信路としては光ファイバーを使用する。光子は量子力学的な性質を持ち、観察されることで挙動が変化してしまうため盗聴を検知できることや、送信側と受信側で共通のフィルターを用いないと復号が正しく行われないという特徴があり、理論的に第三者に解読されないことが特徴である。QKD のプロトコルとしては以下がある。

BB84方式

- 量子鍵配送（QKD）の代表的なプロトコル

デコイ BB84 方式

- BB84 方式を少し複雑にした方式で、絶対安全であることが証明されており、世界中で開発が行われている。NEC が NICT とともに研究開発を進めている。

CV-QKD 方式

- BB84 方式では受信側に必要であった高い性能を有する光子検出器を不要となる。これにより、同じ光ファイバー上で通常の光通信との共存が可能になり、より安価に実現できる。

量子暗号の実用化に向けた実証実験は、顔認証時の特徴データ伝送を量子暗号で秘匿化するシステム、電子カルテのデータの伝送を量子暗号で秘匿化し、ネットワーク経由で安全な伝送を行うシステム、量子暗号の金融分野への適用可能性の検証などが進められている[1]。

Quantum Noise Stream Cipher（QNSC、量子雑音ストリーム暗号）は光ファイバー伝送の安全性を高めるための物理層暗号化方式である。内在する量子ノイズで信号状態をマスクすることでデータを暗号化する方法であり、物理層のセキュリティを実現する。量子暗号の実用化には、QKD、PQC に加えて、量子ストリーミング暗号 QNSC も含めた全体的なセキュリティアーキテクチャの議論が必要とされている[2]。また QNSC に関する技術開発として東北テクノアークにより、以下の研究がなされており、『QNSC は高速通信が実現できる量子暗号として期待されているが、強い光信号を利用するため、量子雑音による完全なマスキング効果が得られず、暗号化に用いる乱数列の一部の情報が盗聴者に漏れてしまう可能性があるという課題があった。本発明は、高速伝送を得意とするQNSC 信号を時間軸にも拡散させ、データの振幅および位相の多値化に用いる乱数列の情報も暗号化することにより、従来の QNSC よりも安全性が高く、かつ高速伝送可能な光秘匿通信システムおよび光秘匿通信装置を提供することが可能になった。』としている[4]。

参考）
[1] NEC、https://jpn.nec.com/techrep/journal/g21/n01/210124.html、2023 年 3 月 27 日閲覧
[2] 量子技術の実用化推進ワーキンググループ（第一回）議事要旨、
https://www8.cao.go.jp/cstp/ryoshigijutsu/jitsuyo_wg/1kai/giji.pdf
[3] 「東北大、量子雑音暗号の光通信システム−70Gbpsで100km先に伝送」、
https://www.nikkan.co.jp/articles/view/00399473
[4] 東北テクノアーチ、https://www.t-technoarch.co.jp/data/anken/T20-1563.pdf、2023 年 3 月 27 日閲覧

（3） 耐量子計算機暗号技術（PQC：Post-Quantum Cryptography）

量子コンピューター技術の進歩により、現在広く使われているRSA暗号を含む非対称暗号が解読されてしまう脅威に対して、将来の量子コンピューターでも復号困難な耐量子暗号技術の検討が進んでいる。

米国では、国家安全保障局（NSA）が対量子暗号アルゴリズムを開発するためのプロジェクトを2015年に始動した。米国立標準技術研究所（NIST）が公募する次世代の公開鍵暗号の最終的な標準化は2024年の見通しだが、2022年7月5日に公表された4回目の選考結果では公開鍵暗号は1方式に絞り込まれ、文書の真正性証明などに用いるデジタル署名は 3 方式が候補となっている［1］。Web サイト暗号通信などに用いられている公開鍵暗号方式としては、格子問題を使った IBM などの「CRYSTALS-Kyber」が標準技術として 1 つに絞られた形となった［2］。インターネットに利用される技術の標準化を推進する団体IETF（Internet Engineering Task Force）もNISTの決定に合わせる方針で、新暗号は事実上の世界標準として規格化される見通しであり、今後、多くの行政などでも使用の義務付けが想定される。

新暗号は電子メールやネット通販、キャッシュレス決済など広範に影響を及ぼすため、IT 業界において新暗号の導入に向けた動きが出始めている。ソフトバンクは実績がある古典暗号と PQC とのハイブリッド方式の実証を完了し、既存のネットワークへの適用できることを確認したとしている［3］。凸版印刷はとNICTはPQCを搭載したICカードを開発し、NICTが運用するテストベッド「保健医療用の長期セキュアデータ保管・交換システム」における医療従事者の IC カード認証と電子カルテデータへのアクセス制御に適用し、その有効性の検証に成功したとしている［4］。

電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである CRYPTREC（Cryptography Research and Evaluation Committees）では、2020 年 2 月に発出した注意喚起情報「現在の量子コンピュータによる暗号技術の安全性への影響」において『CRYPTREC 暗号リスト記載の暗号技術が近い将来に危殆化する可能性は低いと考えています。今後も、本暗号リスト記載の暗号技術の監視活動を引き続き実施していきます。』としているが、2023年3月8日に「CRYPTREC暗号リスト（2013年3月策定）の改定案」に係るパブリックコメントが実施している［5］。

参考）
［1］「量子コンピューターでも解読困難、米政府機関が次世代の暗号標準を絞り込み」、https://xtech.nikkei.com/atcl/nxt/news/18/13260/、2023年3月27日閲覧
［2］「量子時代のネット暗号にIBMの技術 NTT方式は落選」、https://www.nikkei.com/article/DGXZQOUC062L50W2A700C2000000/、2023年3月27日閲覧
［3］ソフトバンク「耐量子計算機暗号アルゴリズムの実用性を確認」2023年2月28日、https://www.softbank.jp/corp/news/press/sbkk/2023/20230228_01/、2023年3月27日閲覧
［4］「凸版印刷とNICT、世界初、米国政府機関選定の耐量子計算機暗号をICカードシステムに実装する技術を確立」、https://www.nict.go.jp/press/2022/10/24-1.html、2023年3月27日閲覧
［5］「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」の改定案に対する意見公募要領、https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000250288、2023年3月27日閲覧

（4） 量子セキュアクラウド

量子セキュアクラウドとは、QKD を利用した量子暗号ネットワーク上に形成された分散ストレージと定義される［1］。分散ストレージには秘密分散技術を用いており、量子暗号ネットワークを利用して、初めて手渡しによらないデータの情報理論的安全な分散保管が可能となる。また秘密分散には保存したデータの秘匿性を担保したうえでそのデータの統計情報などを計算できる秘匿計算機能が実装可能で

もあり、データの安全な伝送、保存、二次利用を可能である。

これらの技術はゲノム解析データ、電子カルテ、さらに生体認証用データの分散保管への活用が検討されている。東芝は、ゲノム解析システムの開発に成功したとしている[2]。NEC は、スマート製造分野での設計情報の最適化の処理・高秘匿伝送・分散保管に成功したとしている[3]。また今後の活用検討が NICT の量子技術の実用化推進 WG でも議論されており[4]、サイバー攻撃に対抗する技術として期待される。

参考）
[1] NICT、https://www.nict.go.jp/publication/shuppan/news/NICT_NEWS486/book/pdf/7.pdf、2023 年 3 月 27 日閲覧
[2] 東芝「量子セキュアクラウドによる高速安全なゲノム解析システムの開発に成功」2022 年 11 月 17 日、https://www.global.toshiba/jp/technology/corporate/rdc/rd/topics/22/2211-04.html
[3] NEC「量子セキュアクラウドシステムを使って次世代レーザー設計の最適化の処理・高秘匿伝送・分散保管を実現」、https://jpn.nec.com/press/202210/20221004_01.html、2023 年 3 月 27 日閲覧
[4] NICT、量子技術の実用化推進 WG「量子セキュリティ・量子ネットワークの実用化戦略（2022 年 11 月 24 日）」、https://www8.cao.go.jp/cstp/ryoshigijutsu/jitsuyo_wg/2kai/siryo2-4.pdf

3.3.9 その他の先進的な技術の動向

（1） 暗号解読やマルウェアによって暗号化されたデータの復号技術

ランサムウェアはファイルを暗号化し、その復号化のために身代金の支払いを要求するマルウェアの一種である。被害者が犯罪者にお金を払うことなく暗号化されたデータを取り戻すのに役立つ復号化ツールがいくつかある。

- Emsisoft Ransomware Decryption Tool
- McAfee Ransomware Recover
- Wildfire Decryptor
- Xorist Decryptor
- No More Ransom

「No More Ransom」はオランダ警察の全国ハイテク犯罪ユニット、ユーロポールの欧州サイバー犯罪センター、Kaspersky、McAfee が主導しており、ランサムウェアの被害者が犯罪者に不当な支払いをすることなく、暗号化されたデータを取り戻すための支援を目的としている。

参考）
1. IPA テクニカルウォッチ「ランサムウェアの脅威と対策」：IPA 独立行政法人 情報処理推進機構
2. ランサムウェア対策特設ページ：IPA 独立行政法人 情報処理推進機構
3. No More Ransom – do you need help unlocking your digital life? | Europol (europa.eu)
4. ランサムウェア対策について | トピックス | 脅威情報 | 一般財団法人日本サイバー犯罪対策センター（JC3）
5. ランサム被害のデータ復元成功 警察庁、暗号化を強制解除 - 産経ニュース（sankei.com）

（2） アタック・サーフェス・マネジメント（ASM）

オンプレミス、クラウド、IoT といった分散したデジタル資産の可視性に加え、これらを対象にした脅威の可視性を高めることで攻撃を未然に防御し、さらには攻撃を受けた際の被害を最小限に抑えるソリューションである。

（3） マイクロセグメンテーションなどの高度なアクセス制御技術

マイクロセグメンテーションとはデータセンターやクラウド環境を個々のワークロードレベルまで細分化するセキュリティ技術である。この手法は、攻撃対象領域を減らし、規制への準拠を実現し、侵害を封じ込めるために使用される。この技術を採用することにより、柔軟なセキュリティポリシーを詳細に展開することができ、各セグメントに独自のセキュリティ制御とアクセス制限を設けることができるため、サイバー脅威のリスクを減らすことが可能になる。

（4） 先進的なセキュリティ対策のアーキテクチャ

ゼロトラストに代表されるシステムのセキュリティ対策のアーキテクチャは、サイバー攻撃への防御にとって重要な要素であり、システムの変遷とともに、多くのアーキテクチャが提示されている。単一の防御技術だけでなく、システム全体を見たセキュリティ対策のアーキテクチャを採用する必要がある。

“「日本企業では、システムを部門単位で導入する形が多く、今後もそうであるなら、システムがモノシリック（一枚岩）にはならないことになる。加えて、クラウドもさまざまなサービスが導入され、マルチクラウド化も進み、1 つのクラウドにはならない。こうしたことを前提とするアーキテクチャを理解していくことが重要になる」。Lovejoy 氏は、現在のシステムやセキュリティの環境や利用状況などを前提として、自社にとって本来あるべきセキュリティ対策のアーキテクチャを考え、それを具現化していく戦略を策定し、行動を起こすべきだと述べる。”

出所）限界が見えてきたセキュリティ対策と打開への道筋 － ZDNET Japan、https://japan.zdnet.com/article/35201129/、2023 年 3 月 15 日閲覧

1） 常時リスク診断・対処（CRSA）アーキテクチャ

デジタル庁においては、次世代セキュリティアーキテクチャに関する技術ガイダンスを具体的に検討するため、次世代セキュリティアーキテクチャ検討会が開催されている。この中で、ゼロトラスト・アーキテクチャーに加えて、システムの挙動やソフトウェアの状況をリアルタイムに監視し対処するための取り組みとして「常時リスク診断・対処（CRSA）」について議論されている。これはサイバーセキュリティリスクを早期に検知し、低減する活動を継続的に実施するための、情報収集・分析を目的としたプラットフォームのアーキテクチャである。

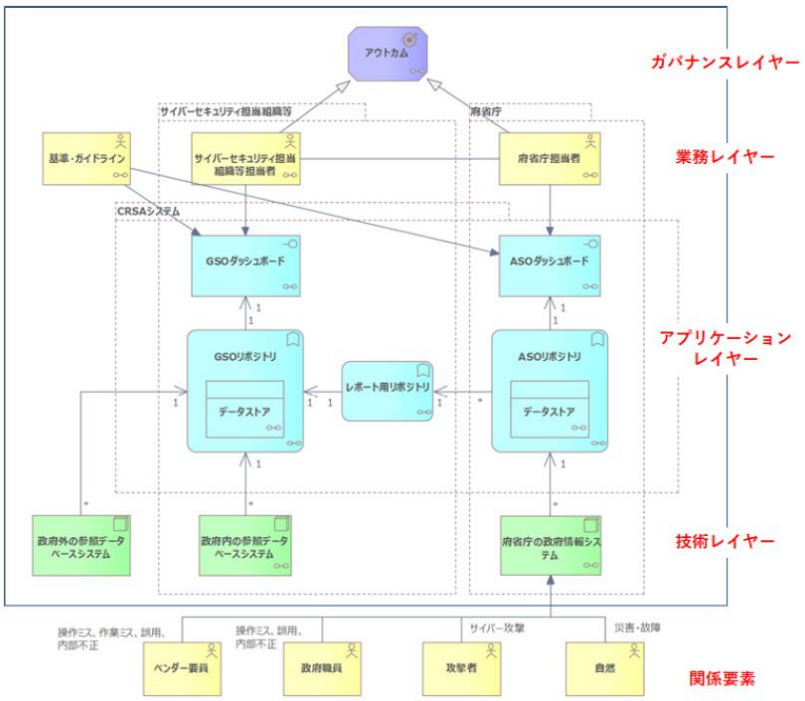

図 1 CRSA システムのアーキテクチャ全体図

出所)「常時リスク診断・対処(CRSA)アーキテクチャ 本文(PDF／1，073KB)」、
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1e024edb/20220630_resources_standard_guidelines_guidelines_07.zip、2023年3月15日

参考)
1. 次世代セキュリティアーキテクチャ検討会｜デジタル庁（digital.go.jp)、
https://www.digital.go.jp/councils/security-architecture/、2023年3月15日閲覧
2. 日本政府に求められるゼロトラスト「常時診断・対応型のセキュリティアーキテクチャ」｜Splunk、
https://www.splunk.com/ja_jp/blog/security/splunk-zerotrust-security-for-government.html、2023年3月15日閲覧

2） サイバーセキュリティメッシュアーキテクチャ

サイバーセキュリティメッシュアーキテクチャ（CSMA：Cybersecurity Mesh Architecture）とはガートナー社が提唱するアーキテクチャアプローチで、「分散型企業が、最も必要な場所にセキュリティを展開し拡張できるようにする、セキュリティアーキテクチャに対する最新の概念的アプローチ」と定義している。

ワークマネジメントオンラインによる説明

各所に散らばった端末や、それらの間で作動するソフトウェアだけではなく、データ内容や接続に関する方式、範囲、アカウントなど多くの要素を考慮して、それぞれの局面における、有効なセキュリティを用意する必要が生じました。その結果、企業は複数のセキュリティソフトを導入し、それぞれ制御しなくてはならない上、セキュリティの更新作業に加えて、使用端末を入れ替える際の、セキュリティソフトの再適用が大きな負担です。そして、言うまでもなくサイバー犯罪者は、こうした負担が招く脆弱性を狙ってきます。そこで、セキュリティを

統合制御し、相互運用性を向上させるプラットフォームとして、サイバーセキュリティメッシュが出現しました。各セキュリティは、脅威インテリジェンスの分析・共有を相互に行いながら、全体でひとつのセキュリティシステムとして動作するよう設計されます。

参考）

1. https://www.gartner.co.jp/ja/articles/the-top-8-cybersecurity-predictions-for-2021-2022
2. 2 つのセキュリティー対策が黎明期に、ガートナーが日本版ハイプ・サイクルを発表 | 日経クロステック（xTECH）(nikkei.com)
3. 攻撃を境界防御ではなく面でブロックする！サイバーセキュリティ・メッシュとは | Secure Station（セキュアステーション）
4. サイバーセキュリティメッシュとは？ アプリケーションとメリット | Fortinet
5. サイバーセキュリティ・メッシュとは？ 解決すべきセキュリティの課題 | ワークマネジメント オンライン（work-management.jp）
6. サイバーセキュリティ・メッシュは分散データを”面”で守る | NTT コミュニケーションズ 法人のお客さま

3.4　関連する組織の取組について

3.4.1　NICT

（1）　サイバーセキュリティ研究室

サイバーセキュリティ研究室は、NICT において進められているサイバーセキュリティに取り組む研究所である「サイバーセキュリティ研究所」に設置された研究室で、サイバー攻撃への対処能力向上に貢献するためのサイバーセキュリティ技術の研究開発に取り組んでいる。

本研究室は、以下の 4 つのチームに分かれ、研究開発を推進している。

研究チーム（大規模データに基づく世界最先端の学術研究）

- サイバー攻撃のトレンドの変化に追従した実践的な研究開発を行うためには、サイバー攻撃の実データを大規模かつ継続的に収集する仕組みが不可欠とし、新たな攻撃に対応した観測技術の研究開発を実施している。また、大規模集約したサイバー攻撃関連情報を活用した自動分析・自動対策技術の研究開発を進めている。さらに、新たに社会に登場する技術に対してセキュリティ課題の抽出や対策に貢献するため、最新の通信機器、IoT 機器、コネクテッドカー等のエマージング技術に対応したセキュリティ検証技術の研究開発を進めるとともに、ヒトを対象としたユーザブルセキュリティの領域にも取り組んでいる。

解析チーム（NICT 内外からの要請に応える異種データ大規模横断解析）

- 本チームは、専門のセキュリティアナリストによって構成され、ダークネット観測・分析による新規マルウェアの発生検知や感染した IoT 機器の発見、ライブネット観測・分析による標的型メールの収集・検知やセキュリティアラートのトリアージ、実際に収集したマルウェア検体の解析や攻撃者の挙動分析等の様々なサイバー攻撃情報の分析を実施している。各種解析結果やノウハウは研究チームや NICT 内の CSIRT へ展開されるだけでなく、NICT 外の組織からの要請に基づいて情報提供を実施している。

開発チーム（観測基盤から可視化までインハウスの組織的開発）

- 大規模な観測・分析基盤から各種可視化エンジン等の研究開発におけるコア技術を本研究室内で開発するための体制を構築している。開発体制を研究室内に構築することで、研究開発のサイクルを迅速に回し攻撃者の進化に追従できるほか、研究成果を活用したシステムを高い完成度で実装・検証し、スムーズな社会展開へ繋げることを目的としている。

インフラチーム（研究開発を支える大規模インフラ設計・構築・運用）

- 本研究室における研究開発のインフラ基盤の維持のため、サーバ・ストレージ・ネットワーク機器等の構築・運用、電源・空調・配線を含むファシリティ整備・運用、DNS・DHCP・仮想化環境等を含む基幹サービスの構築・運用を実施している。他にも、クラウド環境の構築・運用、検証用セキュリティアプライアンスの導入・設定を実施している。

参考）

[1]　サイバーセキュリティ研究室、https://csl.nict.go.jp/ 、2023年3月 24 日閲覧

（2）　セキュリティ基盤研究室

セキュリティ基盤研究室は、NICT の「サイバーセキュリティ研究所」に設置された研究室で、耐量子計算機暗号等を含む新たな暗号・認証技術やプライバシー保護技術の研究開発を実施し、その安全性評価を行うとともに、安全な情報利活用の推進に取り組んでいる。

本研究室では、安全なデータ利活用技術と暗号技術の安全性評価に関して、以下の取り組みを進めている。

安全なデータ利活用技術に関する取り組み

- データの提供・収集・保管・解析・展開の各段階におけるセキュリティやプライバシーを確保するため、匿名認証や検索可能暗号等のアクセス制御技術、秘匿計算等のプライバシー保護解析技術等の研究開発を実施している。
  1. 安全性と利便性との両立（検索可能暗号、平文一致確認可能暗号の研究）
  2. 新たな社会ニーズへの対応（小型宇宙機の乗っ取りを防止し伝送データを保護する暗号技術、ゼロ知識証明と匿名認証への応用の研究）
  3. プライバシー保護基盤技術の研究開発（DeepProtect（プライバシー保護連合学習システム）、ヘルスケア分野で求められるプライバシー保護技術の研究）

暗号技術の安全性評価に関する取り組み

- 秘匿すべき情報を守り、改ざんやなりすましを防ぐため、現代の情報通信システムではあらゆる場面で暗号技術が使用されている環境の下、様々な暗号技術の適切な実装と安全な運用に貢献するため、暗号基盤技術の研究開発を実施している。
  1. 現代暗号に対する量子コンピュータの脅威の評価
  2. 耐量子計算機暗号（多変数公開鍵暗号）の安全性評価
  3. Zoom や Webex 等で導入されているエンドツーエンド暗号化の安全性評価

参考）
[1] セキュリティ基盤研究室、https://sfl.nict.go.jp/ 、2023年3月 24 日閲覧
[2] 検索可能暗号システム、https://searchableenc.nict.go.jp/ 、2023年3月 24 日閲覧
[3] DeepProtect、https://deepprotect.nict.go.jp/ 、2023年3月 24 日閲覧

（3） CYDER プロジェクト

CYDER（Cyber Defense Exercise with Recurrence）は、NICT の「サイバーセキュリティ研究所」に設置されたセンターである「ナショナルサイバートレーニングセンター」が推進している事業で、国の機関、地方公共団体、重要社会基盤事業者等を対象とする実践的なサイバー防御演習である。

CYDER では、サイバー攻撃を受けたことを想定し、「インシデント発生から事後対応までの一連の流れ」をロールプレイ形式で体験できる演習であり、対応手順と具体的な対応を学び、「平時の備え」や「被害を抑えるための対応」等の実務に活かせる内容としている。演習では、課題を通じて、以下の 5 つの対応手順と具体的な対処方法を学習することができる。

1. 検知・連絡受付
   パソコンやサーバ等の不審な動作を検知する。組織内外からの通報を受け付ける。
2. トリアージ（優先順位付け）
   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等を行い、事実関係を確認する。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る。

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等を検討し、「証拠保全」「封じ込め」「根絶」「復旧措置（暫定対応）」を実施する。
4. 報告・公表
   被害の度合いや影響範囲に応じて、報告・公表を実施する。組織内部だけでなく、被害者、監督官庁等の外部関係者にも報告・公表を実施する。
5. 事後対応
   インシデント対応に関わったすべての関係者が参加して「振り返り」を実施する。同様のインシデントを防ぐための今後の対応等を含め、最終報告書に取りまとめる。

なお、CYDER には、受講者のレベル、対象組織、受講形式（集合演習/オンライン演習）によってコースが用意されており、受講目的によってコースを選択することが可能となっている。

参考）
［1］ CYDER、https://cyder.nict.go.jp/index.html 、2023年3月 24 日閲覧
［2］ ナショナルサイバートレーニングセンター、https://nct.nict.go.jp/ 、2023年3月 24 日閲覧

（4） CYNEX プロジェクト

CYNEX（CYBER SECURITY NEXUS）は、NICT の「サイバーセキュリティ研究所」に設置された組織で、「サイバーセキュリティ研究室」が持つ研究成果や「ナショナルサイバートレーニングセンター」が持つ人材育成ノウハウを活用し、産官学の結節点（ネクサス）となる先端的基盤の構築を目的として設立された。サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を開放することで、日本のサイバーセキュリティの対応能力向上を目指している。

CYNEX では、以下の 4 つのサブプロジェクト（Co-Nexus）を推進している。

- Co-Nexus A（Accumulation & Analysis）
  NICTER、STARDUST、WarpDrive 等の各種観測機構を活用し、サイバーセキュリティ情報を収集・蓄積する。また、国内解析者コミュニティを醸成し、共同分析の実現を目指す。
- Co-Nexus S（Security Operation & Sharing）
  解析者と機械学習エンジンの連携で異種データの横断分析を行い、国産の脅威情報の生成と提供を目指す。また、高度 SOC 人材育成プログラムを構築し、SOC 人材の育成拠点を形成する。
- Co-Nexus E（Evaluation）
  NICT のネットワーク環境に国産セキュリティ製品のプロトタイプを導入し、長期運用を通して機能検証と製品へのフィードバックを行い、国産セキュリティ製品の創出と普及を支援する。
- Co-Nexus C（CYDERANGE As An Open Platform）
  国内におけるセキュリティ人材育成のハードルを下げるため、演習シナリオや遠隔演習システムをオープン化し、民間事業者や教育機関におけるセキュリティ人材育成事業の促進を目指す。

参考）
[1] CYNEX、https://cynex.nict.go.jp/ 、2023年3月 24 日閲覧

（5） NOTICE プロジェクト

NOTICE（National Operation Towards IoT Clean Environment）は、NICT の「サイバーセキュリティ研究所」に設置されたセンターである「ナショナルサイバーオブザベーションセンター」が推進している取り組みで、総務省、NICT、インターネットサービスプロバイダ（ISP）が連携し、日本国内に存在するサイバー攻撃に悪用されるおそれのある IoT 機器の調査及び機器利用者への注意喚起を行うプロジェクトである。

NOTICE では、以下の 4 つの取り組みを実施することで、安心・安全に IoT 機器を利用できることを推進している。

1. 機器調査
   NICT は、インターネット上の IoT 機器に容易に推測されるパスワードを入力する等により、サイバー攻撃に悪用されるおそれのある機器を調査し、当該機器の情報を ISP に通知する。
   ※調査対象は、グローバル IP アドレス（IPv4）によりインターネット上で外部からアクセスできる IoT 機器であり、具体的には、ルータ、ウェブカメラ、センサー等である。
2. 注意喚起
   ISP は、NICT から受け取った情報を元に当該機器の利用者を特定し、電子メールや郵送等により注意喚起を行う。
3. 設定変更等
   注意喚起を受けた利用者は、注意喚起の内容や NOTICE サポートセンターサイトの説明等に従い、パスワード設定の変更、ファームウェアの更新など適切なセキュリティ対策を行う。
4. ユーザサポート
   総務省が設置する NOTICE サポートセンターは、ウェブサイトや電話によるお問合せ対応を通じて利用者に適切なセキュリティ対策等を案内する。

参考）
[1] NOTICE、https://notice.go.jp/ 、2023年3月 24 日閲覧
[2] ナショナルサイバーオブザベーションセンター、https://nco.nict.go.jp/ 、2023年3月 24 日閲覧

3.4.2 総務省

（1） AI セキュリティ 情報発信ポータル

AI セキュリティ情報発信ポータルは、AI の開発者や利用者を対象とし、AI に対する攻撃・防御の手法を発信することを目的として、AI の開発時・利用時に認識しておくべきセキュリティのポイントを掲載している。なお、本ポータルにおける AI とは、画像分類や音声認識等のような、通常は人間の知能を必要とする作業を行うことができるコンピュータシステム、機械学習を使用して作成されるシステム全般を指す。また、本ポータルは、総務省の事業である「5G端末等におけるセキュリティ確保のための技術課題の整理と情報発信」の一環として、三井物産セキュアディレクション株式会社によって運用されている。

本ポータルでは、AI に対する攻撃・防御の手法を AI 開発の各工程に合わせて体系化した以下の

「AI セキュリティ・マトリックス」を掲載している。「AI セキュリティ・マトリックス」で掲載されている攻撃分類、攻撃手法、防御手法については、詳細な解説も併せて説明されている。

表 4　AI セキュリティ・マトリックス

開発工程	攻撃分類	攻撃手法	防御手法
学習データの収集/作成 (Data Preparation)	データ汚染	・Convex Polytope Attack ・Feature Collision Attack ・Bullseye Polytope Attack	・トリガーの検知 ・汚染データの検知 ・Neural Cleanse
モデルの学習/作成 (Model Fitting)	モデル汚染	・機械学習フレームワークの悪用	・信頼できる事前学習モデルの利用 ・信頼できる AI 開発会社の利用 ・サンドボックス環境の利用 ・必要最低限の権限による AI の稼働 ・最新バージョンの機械学習フレームワークの利用
		・BadNets	・信頼できる事前学習モデルの利用 ・信頼できる MLaaS の利用 ・モデルの改ざん検知 ・ノード剪定
モデルの設置 (Deployment)	敵対的サンプル	・Fast Gradient Sign Method	・敵対的学習 ・データ拡張 ・ネットワークの蒸留 ・アンサンブルメソッド ・特徴量の絞り込み ・AI による検出
		・Adversarial Patches	
	データ窃取	・Membership Inference Attacks	・過学習の抑制 ・差分プライバシー ・ラベルのみ応答 ・信頼スコアのマスキング
		・Model Inversion Attacks	・勾配情報のマスキング ・信頼スコアのマスキング ・モデルのアクセス制御
	モデル窃取	・Copycat CNN	・モデルのアクセス制御 ・学習データのアクセス制御 ・窃取モデルの検知

参考）

[1]　三井物産セキュアディレクション株式会社、https://www.mbsd.jp/aisec_portal/index.html 、2023年3月 27 日閲覧

3.4.3　科学技術振興機構

（1）　インフォデミックを克服するソーシャル情報基盤技術

インフォデミックを克服するソーシャル情報基盤技術は、科学技術振興機構が推進する戦略的創造研

究推進事業のプログラムである CREST における研究(研究領域:信頼される AI システムを支える基盤技術)である。本研究では、AI により生成されたフェイクメディア(FM)がもたらす潜在的な脅威に適切に対処し、多様なコミュニケーションと意思決定を支援するソーシャル情報基盤技術の確立を目的としている。具体的には、AI により生成されたフェイク映像、フェイク音声、フェイク文書等の多様なモダリティによる FM を用いた高度な攻撃を検出・防御する一方で、信頼性の高い多様なメディアを積極的に取り込むことで人間の意思決定や合意形成を促し、サイバー空間における人間の免疫力を高めるソーシャル情報基盤技術を確立していくとしている。

本研究では、Security(SEC)領域(国立情報学研究所 越前グループ)、Multimedia(MM)領域(大阪大学 馬場口グループ)、Computational Social Science(CSS)領域(東京工業大学 笹原グループ)の 3 つの領域における専門知識を駆使し、領域間の連携を取りながら以下の研究実施項目に取り組んでいる。

1. 多様なモダリティによる高度な FM 生成技術(主担当:MM 領域)
   今後のサイバー社会で脅威となる FM 生成技術を確立する。映像(顔、身体等)、音声、文書等の多様なモダリティに対して、人間または AI 技術を騙す、あるいはその双方を騙すことを目的とした FM 生成技術を確立するとともに、FM 生成の法律的側面についても検討する。
2. FM 検出・防御技術(主担当:SEC 領域)
   1.で生成した多様な FM を対象とした高度な検出・防御技術を確立する。本研究では、FM の検出だけではなく、FM がどのような意図(例:騙す対象は人間か AI 技術か)で生成されたのか、説明可能な形式でユーザに情報を提供することを目指す。
3. FM 無毒化技術(主担当:MM 領域、SEC 領域)
   人間や AI 技術を対象とした、思考誘導・誤動作・誤判定が生じないように FM を無毒化し、通常のメディアとして機械学習モデルの学習データに活用する FM 無毒化技術を確立する。
4. インフォデミックを緩和し多様な意思決定を支援する情報技術(主担当:CSS 領域)
   SEC 領域と MM 領域で開発する FM の生成・検出や無毒化に関する要素技術を最大限に活かし、情報の信頼性を高める社会システムの原理と技術を確立する。

参考)
[1] CREST FakeMedia、http://research.nii.ac.jp/~iechizen/crest/index.html 、2023年3月 27 日閲覧
[2] CREST、https://www.jst.go.jp/kisoken/crest/index.html 、2023年3月 27 日閲覧

3.4.4 MITRE

本項では MITRE が推進しているサイバーセキュリティ関連の研究動向について記載する。

MITRE（The MITRE Corporation）は米国連邦政府が資金提供している非営利組織である。官民パートナーシップや連邦政府から資金提供を受けた研究開発センター（FFRDC）を通じて、政府全体や産業界、学術界と連携して航空、防衛、ヘルスケア、国土安全保障、サイバーセキュリティなどの分野での複雑で長期的な課題に取り組んでいる。FFRDC（Federally Funded Research and Development Centers）とは、連邦政府が民間セクターとの契約により設置する GOCO（Government Owned Contractor Operated）方式の研究組織であり、連邦政府の資金で運用され、運営は大学や企業、非営利機関などの民間セクターが行う産官学が連携した研究組織である。

MITRE は以下の 6 つの FFRDC を運営しており、また独自の研究組織である MITRE Labs および技術財団である MITRE Engenuity のほか、個々の研究開発プログラムを含めてサイバーセキュリティ関連の研究が活発に行われている。

1. National Security Engineering Center（NSEC）
   - Department of Defense（国防総省）
2. Center for Advanced Aviation System Development（CAASD）
   - Federal Aviation Administration（米連邦航空局）
3. Center for Enterprise Modernization（CEM）
   - Department of the Treasury（財務省）and Internal Revenue Service（内国歳入庁）, and co-sponsored by the Department of Veterans Affairs（退役軍人省）and Social Security Administration（社会保障庁）
4. Homeland Security Systems Engineering and Development Institute™（HSSEDI）
   - Department of Homeland Security（国土安全保障省）
5. The Health FFRDC（HEALTH FFRDC）
   - Department of Health and Human Services（米国保健社会福祉省）
6. National Cybersecurity FFRDC（NCF）
   - National Institute of Standards and Technology（米国国立標準技術研究所）

MITRE Labs は2020年 7 月に設立された組織であり、FFRDC の運営を通じて学んだことを生かし、人工知能（AI）や量子コンピュータのような先進的テクノロジーが国家安全保障と経済を大きく変える可能性がある世界において競争力を強化する。

MITRE Engenuity は民間セクターとの協力を促進すべく 2019 年に設立された技術財団である。学際的な専門知識とリソースを応用し、複雑で公益性の高い課題に産業界と協力して取り組み、重要インフラの将来形成に貢献することを目的としている。

参考）
[1] The MITRE Corporation、https://www.mitre.org/who-we-are/
[2] 文部科学省、米国の学術研究推進体制及びファンディングシステム、https://www.mext.go.jp/b_menu/shingi/gijyutu/gijyutu4/008/siryo/attach/1342784.htm、2023 年 3 月 23 日閲覧
[3] MITRE Labs Fact Sheet、https://www.mitre.org/news-insights/fact-sheet/mitre-labs
[4] MITRE Engenuity、https://mitre-engenuity.org/who-we-are/

（1） National Cybersecurity FFRDC（NCF）

NCF は、米国国立標準技術研究所（NIST）とナショナル・サイバーセキュリティ・センター・オブ・エクセレンス（NCCoE）からの資金提供を受け、サイバーセキュリティと技術安全のための規格開発に特化した連邦政府出資の研究開発センターである。絶えず変化するデジタル環境を調査し、新たな予期せぬ問題を発見することで、重要な役割を果たしている。MITRE は NCF を通じて、重要なインフラとそれらが支える複雑なエコシステムを研究・分析し、サイバーセキュリティの脆弱性を軽減するための詳細なガイダンスとプレイブックを開発している。

主な活動領域は、人工知能、モノのインターネット、5G ネットワーク、衛星通信、そして商業宇宙旅行である。

Artificial Intelligence（人工知能）

- 産学共同で、機械学習モデルの誤作動を引き起こす可能性のある敵対的な機械語に関する概念と用語の分類法を開発した。

IoT

- 家庭用 IoT 機器のインターネット製品のセキュリティについて、これを悪用するサービス拒否攻撃（DDoS）を緩和するのに役立つガイダンスを提供している。

Election Integrity（選挙の完全性）

- サイバー攻撃が選挙の完全性を脅かし、国家安全保障損なわれる懸念に対して、投票システムをより安全にするための阻害要因を分析している。

Securing Space（安全な宇宙空間）

- 地球低軌道の商業衛星コンステレーションのサイバー脆弱性に関する知識の必要性が高まっており、NCF の主導で宇宙情報共有分析センター（Space ISAC）を創設した。
-

[1] https://www.mitre.org/our-impact/rd-centers/national-cybersecurity-ffrdc
[2] National Cybersecurity FFRDC Fact Sheet（2022.1.5）、https://www.mitre.org/news-insights/fact-sheet/national-cybersecurity-ffrdc

（2） Homeland Security Systems Engineering and Development Institute™（HSSEDI）

主なサイバーセキュリティに関する活動内容は以下の通り。

- 重要インフラを保護するシステムを含む連邦政府システムに対するサイバーハイジャックキャンペーンの疑いをデータに基づいて分析し、サイバースペースを保護する。
- MITRE の ATT&CK®フレームワークを活用し、政府のモバイルデバイスのセキュリティを向上させる。
- 国土安全保障専門家グループのような関係者間のコラボレーションを促進する。
- 選挙や COVID-19 の対応に悪影響を与えるソーシャルメディア上の誤報・偽情報に対抗する。

（3） MITRE Engenuity

MITRE Engenuity は、民間部門とのコラボレーションを促進するために MITRE によって設立された非営利の技術財団である。

[1] https://www.mitre.org/news-insights/news-release/mitre-establishes-engenuity-foundation-foster-private-sector
[2] https://impact.mitre.org/mitre-engenuity/

a. The Center for Threat-Informed Defense（CTID、脅威情報防御センター）

The Center for Threat-Informed Defense は、脅威情報に基づく防御能力の実践的強化と成果の公益的な無償共有を行うべく、MITRE Engenuity が2019年に設立した民間資金を原資とする非営利の研究開発組織である[1]。これには Bank of America、Microsoft、Siemens、Verizon、AttackIQ らとともに富士通が本組織の創設メンバーになっている [2]。

同センターはサイバーセキュリティ企業が利害関係にとらわれず自発的に協力して共通の問題に取り組むことができる場となっており、そのナレッジやリソース、人材を結集して産業界が結束することで、サイバー攻撃者が攻撃ツールやナレッジの共有を行うことで防御側より有利な立場になっている現状に対抗する。本組織には設立後もブラックベリーやサイバーリーズンなどグローバルなセキュリティ企業が参画し[3,4]、活動しており、2022 年の活動レポート[5]では脅威情報に基づく防衛を実施するのに役立つ 9 つの先進的なリソースが紹介され、これらは無償で利用できる。

Defending IaaS with ATT&CK

- パブリッククラウドを含む IaaS 環境で使用される可能性のある ATT&CK 攻撃技術を理解し、防御するための支援ツールを備えた方法論。

Attack Flow

- 攻撃者の一連の行動を記述するためのツールや例を含むデータモデル。防御者がサイバー攻撃における一連の行動を理解し、共有し、脅威を考慮した意思決定を行うのに役立つ。

Micro Emulation Plans

- レッドチームを持たない組織でも侵入・攻撃シミュレーションを実行し、改善を行い、改善を検証できるようにする攻撃者エミュレーションライブラリ。

Cloud Analytics

- クラウド特有の攻撃者の行動に関するリファレンスとして MITRE ATT&CK® Cloud Matrix を使用し、クラウド環境固有の攻撃者の行動を検出するための分析を行う。

Security Stack mappings – Google Cloud Platform

- Google Cloud Platform で利用可能なセキュリティ機能を ATT&CK 攻撃技術にマッピング。

Top ATT&CK Techniques

- 利用者が自分の組織に合わせた最も懸念すべき攻撃技術リスト TOP10 を作成できる。

Sightings Ecosystem

- 実世界のデータとそのデータから得られる洞察を防衛側の意思決定プロセスに入れることで、優先度の高い問題にリソースを集中させることを可能にする。

Insider Threat TTP knowledge base

・ IT 環境における内部関係者が使用する戦術、技術、手順に関するオープンなナレッジベース。

NIST 800-53 Controls to ATT&CK mappings

・ NIST800-53 のコントロールと ATT&CK の攻撃技術の間のマッピング。

参考）
[1] https://www.linkedin.com/pulse/announcing-launch-mitre-engenuitys-center-defense-richard-struse/
[2] https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/participants/
[3] https://blogs.blackberry.com/ja/jp/2022/03/blackberry-joins-center-for-threat-informed-defense、2023 年 3 月 23 日閲覧
[4] https://www.cybereason.co.jp/blog/security/6301/、2023 年 3 月 23 日閲覧
[5] 2022 IMPACT REPORT、https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/

b. ATT&CK Evaluations（攻撃技術に基づくセキュリティソリューションの評価）

サイバーセキュリティ企業が提供するマネージドサービスについて、ATT&CKⓇ攻撃技術に基づく透明性の高い評価と結果の公開を行うことで、利用者が攻撃者の行動を正しく理解し、適切なソリューションを選択できるようにしている。

同センターでは既知のサイバー攻撃者が使用する戦術や技術を防衛側が再現できる攻撃者エミュレーションプランの公開ライブラリを持っている。例えば、少なくとも 2018 年 8 月以降で大手企業から病院まで、さまざまな組織に対してランサムウェアキャンペーンを実施している犯罪グループである「Wizard Spider」の攻撃行動を再現し、各セキュリティソリューションの検知状況を評価して開示している[2]。

参考）
[1] https://attackevals.mitre-engenuity.org/
[2] https://attackevals.mitre-engenuity.org/enterprise/wizard-spider-sandworm/

（4） フレームワークの活用

MITRE では MITRE ATT&CK フレームワークをはじめとして、サイバー攻撃者の行動を分析した結果を基にした様々なサイバーセキュリティ対策に有効なフレームワーク等を提供している。

1） MITRE ATT&CK

ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge)はサイバー攻撃者が使用する攻撃を戦術と手法、手順の視点で分類したものであり、サイバー攻撃の手法を体系化したフレームワークである。企業や組織が防御の弱点を特定するのに役立つ。

Roadmap 2023

[1] MITRE 2023 Roadmap to focus on targeted growth and integration, while improving ATT&CK’s current platforms - Industrial Cyber、https://industrialcyber.co/analysis/mitre-2023-roadmap-to-focus-on-targeted-growth-and-integration-while-improving-attcks-current-platforms/

2） MITRE Decider

CISA Releases New Tool Mapping Adversary Behavior to MITRE ATT&CK |

MITRE、MAR 1, 2023

[1] CISA Releases New Tool Mapping Adversary Behavior to MITRE ATT&CK® | Business Wire、https://www.businesswire.com/news/home/20230301005251/en/CISA-Releases-New-Tool-Mapping-Adversary-Behavior-to-MITRE-ATTCK%C2%AE

3） MITRE ATT&CK Defender（MAD）

MITRE Engenuity により 2021 年 3 月に提供開始されたサイバーセキュリティの専門家を教育および認定するためトレーニングプログラムである。

参考）
[1] https://mitre-engenuity.org/cybersecurity/mad/enterprise/

4） MITRE ATLAS

MITRE ATLAS（Adversarial Threat Landscape for Artificial-Intelligence Systems）は、現実世界の観察、ML レッドチームやセキュリティグループからの実証、学術研究からの可能性の状態に基づいて、機械学習（ML）システムに対する敵の戦術、技術、事例をまとめた知識ベースです。ATLAS は MITRE ATT&CK®フレームワークをモデルとしており、その戦術とテクニックは ATT&CK のものを補完するものである。

参考）
[1] https://atlas.mitre.org/

5） MITRE Arsenal

このツールは MITRE ATLAS（MITRE Adversarial Threat Landscape for Artificial-Intelligence Systems）のプラグインとして開発されており、サイバーセキュリティ犯罪者の戦術や技術、手順の作成、保存および自動的なサイバーセキュリティ攻撃のエミュレートを可能にする。Arsenal は GitHub のリポジトリで公開されている。

[1] AI や ML モデルのセキュリティツール「Arsenal」登場 Microsoft および Mitre が公開 - ITmedia エンタープライズ、https://www.itmedia.co.jp/enterprise/articles/2303/08/news037.html
[1] New research, tooling, and partnerships for more secure AI and machine learning - Microsoft Security Blog、https://www.microsoft.com/en-us/security/blog/2023/03/02/new-research-tooling-and-partnerships-for-more-secure-ai-and-machine-learning/

6） MITRE CALDERA

MITRE CALDERA は、MITRE が開発した攻撃エミュレーションツールである。特定の攻撃者のプロファイルを構築し、ネットワーク内でそれを起動させて、どこに影響を受けやすいかを確認することができるため、防御のテストや、特定の脅威を検出する方法についてセキュリティ担当者の訓練に役立つものである。

[2] CALDERA’s documentation、https://caldera.readthedocs.io/en/latest/

7） MITRE SHIELD／MITRE ENGAGE

MITRE SHIELD はアクティブディフェンスを実現するためのフレームワークとして 2020 年 8 月に

発表された。このフレームワークには能動的に攻撃者の活動を検出したり、攻撃者を騙すことで自分の組織で発見される攻撃者の TTPs(戦術、手法と手順)を収集したり、攻撃者の目的を妨害したりするなど、多岐に渡る能動的な防御手法がまとめられている。そしてその発展形である MITRE Engage[2]は 2022 年 3 月に発表されたフレームワークである。

参考)
[1] https://security.macnica.co.jp/blog/2020/09/mitre-shield.html
[2] MITRE Launches Engage Framework to Defend Against Cyber Attacks | MITRE、https://www.mitre.org/news-insights/news-release/mitre-launches-engage-framework-defend-against-cyber-attacks
[3] https://www.countercraftsec.com/blog/integrated-the-new-mitre-engage/

8) MITRE D3FEND

MITRE D3FEND は米国家安全保障局(NSA)の資金援助を受けて作られたもので、2021 年 6 月に発表されたセキュリティフレームワークである。サイバー攻撃に対する防御的な戦術と手法が提供される。D3FEND ではセキュリティ製品固有の用語や専門用語ではなく、標準的な防御手法の用語群を確立し、防御と攻撃の手段についての関係を明確にしている。

参考)
[1] https://d3fend.mitre.org/
[2] What Is MITRE D3FEND、https://thenewstack.io/what-is-mitre-d3fend-and-how-do-you-use-it/
[3] https://d3fend.mitre.org/resources/D3FEND.pdf
[4] https://qualias.net/toward-a-knowledge-graph-of-cybersecurity-countermeasures/
https://project.nikkeibp.co.jp/idg/atcl/19/00220/080600001/
https://project.nikkeibp.co.jp/idg/atcl/19/00220/080600002/?ST=idg-cio-security&P=1

9) MITRE RE&CT

MITRE RE&CT Framework は、実用的なインシデントレスポンス技術を蓄積、記述、分類するために設計されている。セキュリティチームのスキルアップ、技術対策の計画、社内手順の整備などインシデントレスポンス能力開発の優先順位付けや、既存のインシデントレスポンス能力で対応できる範囲を理解するのに役立つ。

参考)
[1] https://atc-project.github.io/atc-react/

10) MITRE CREF Navigator

MITRE CREF(Cyber Resiliency Engineering Framework) Navigator は 2023 年 2 月にサイバー・レジリエンス・システムを設計するための可視化ツールとして公表された。多くの組織において攻撃の防止から、攻撃を受けても重要なビジネス機能を維持し、ダウンタイムを最小限にするための回復力の重要性に対する認識が高まっていることを受けて開発されたものである。

参考)
[1] MITRE Launches Cyber Resiliency Engineering Framework Navigator | MITRE、FEB 2, 2023(https://crefnavigator.mitre.org/navigator)
[2] MITRE CREF Navigator empowers enterprises to improve cyber resiliency strategies - Help Net Security、https://www.helpnetsecurity.com/2023/02/04/mitre-cref-navigator/
[3] https://iototsecnews.jp/2023/02/03/mitre-releases-tool-to-design-cyber-resilient-systems/

3.5　関連する海外政府の取組について

3.5.1　米国

(1) Federal Cybersecurity Research and Development Strategic Plan

「Cybersecurity Enhancement Act of 2014(2014 年サイバーセキュリティ強化法)」では、National Science and Technology Council(国家科学技術会議)及び Networking and Information Technology Research and Development Program(NITRD:ネットワーキング・情報技術研究開発プログラム)に対して、サイバーセキュリティ研究開発(R&D)戦略計画を 4 年毎に作成・維持・更新することを義務付けている。

これに従い、「Federal Cybersecurity Research and Development Strategic Plan(2019 年版連邦サイバーセキュリティ研究開発戦略計画)」が発表されている。

この計画では、以下 5 項目の研究開発目標が掲げられている。

・サイバーセキュリティの人的側面の理解
・効果的かつ効率的なリスク管理の提供
・悪意のあるサイバー活動を抑止し、対抗するための効率的かつ効率的な手法の開発
・統合的な安全、セキュリティ、プライバシーのフレームワークと手法の開発
・持続可能なセキュリティのためのシステム開発・運用の改善

また、安全なサイバー空間の目標を達成するために、「抑止」「保護」「検知」「対応」の相互に依存する 4 つの防御機能のフレームワークを組み込んだ 2016 年の計画の基本的な概念を引き継いでいる。

さらには、「2018 National Cyber Strategy of the United States of America(2018 年米国国家サイバー戦略)」及び「FY 2021 Research and Development Budget Priorities Memorandum(2021 年度研究開発予算優先事項覚書)」に示された目的を推進するために、次の優先分野における研究目標の概要を示している。

・人工知能
・量子情報科学
・信頼できる分散型デジタルインフラ
・プライバシー
・安全なハードウェア・ソフトウェア
・教育・人材開発

2023 年の計画策定に向けては、2023 年 2 月～3 月に NITRD、National Coordination Office(NCO)、National Science Foundation(NSF)により意見照会が行われている。質問項目のうちの 1 つには、「デジタルエコシステム(データ、コンピューティング、ネットワーク、サイバーフィジカルシステム、人々などの参加エンティティを含むが、これらに限定されない)のセキュリティ、信頼性、回復力、トラスト、およびプライバシー保護を大幅に強化する可能性のある新しいイノベーション及び組織は何か」との質問項目が挙げられている。

（2） National Cybersecurity Strategy

2023 年 3 月、バイデン政権が「National Cybersecurity Strategy（国家サイバーセキュリティ戦略）」を発表している。この戦略では、サイバー空間における役割・責任・リソース配分を根本的に転換する必要があるとしており、以下の 2 点を示している。

・サイバー空間の防護責任の再配分：

サイバーセキュリティの負担は、個人・中小企業・自治体から切り離し、最高の能力・最適な立場を備えた組織に移す

・長期的な投資を促進するインセンティブの再調整：

喫緊の脅威からの防護と、未来に向けた戦略的計画・投資のバランスを取る

また、アプローチとして以下の 5 本の柱を掲げている。

・重要インフラの防護

・脅威ある行動者への対応

・安全と強靭性を促進させる市場形成

・強靭な未来への投資

・共通する目標を追求する国際パートナーシップの構築

このうち、「強靭な未来への投資」おいては、優先する研究開発として、ポスト量子暗号、デジタル個人認証、クリーンエネルギーインフラなど次世代技術のためのサイバーセキュリティが挙げられている。

（3） NSF

NSF の研究開発プログラムには以下がある。

・Secure and Trustworthy Cyberspace（SaTC）プログラム（NSF 22-517）：

セキュリティとプライバシーの確保

・Cybersecurity Innovation for Cyberinfrastructure（CICI）プログラム（NSF 21-512）：

多層サイバーセキュリティのためのモデルと予測に基づく動的な事業継続と復旧の方法論

接続機器用のオープンソース・オープンスペックのハードウェアにおけるセキュリティの向上

サイバーセキュリティ強化のための AI

個人情報を含む欧州の国境を越えたフェデレーション計算のためのプライバシー保護技術

3.5.2 EU

（1） EU Cybersecurity Strategy

2020 年、「EU Cybersecurity Strategy（EU サイバーセキュリティ戦略）」が策定されている。

セキュリティ研究開発としては、次期長期 EU 予算、特に Digital Europe Program や Horizon Europe 等を通じて、EU のデジタル移行に伴うサイバーセキュリティ戦略の支援に取り組むこととしている。加盟国は、サイバーセキュリティを強化し、EU レベルの投資に見合うべく EU の復興・強靭化のための設備を最大限に活用することが推奨されている。

また、EU と各国予算による共同プロジェクトを通じて、サイバーセキュリティにおける産業・技術的能

力の強化も目指しており、デジタルサプライチェーン（データとクラウド、次世代プロセッサ技術、超安全な接続、6G ネットワークなど）全体でサイバーセキュリティのリーダーシップを推進している。

（2） Horizon Europe

Horizon Europe は、EU の研究・イノベーション枠組みプログラムである。個別プログラムとして 3 つの柱「第 1 の柱：卓越した科学」「第 2 の柱：グローバル・チャレンジ・欧州の産業競争力」「第 3 の柱：イノベーティブ・ヨーロッパ」があり、このうち「第 2 の柱：グローバル・チャレンジ・欧州の産業競争力」において、設定されているクラスター（社会課題）の 1 つである「社会のための市民安全クラスター」において、サイバーセキュリティをテーマとした研究開発公募が実施されている。

＜目標＞

1. 犯罪・テロリズムから EU と EU 市民をよりよく保護する
2. EU 外国境の効率的な管理
3. 強靱なインフラ
4. サイバーセキュリティ強化
5. 欧州のための災害に強い社会
6. セキュリティ研究・イノベーション強化

（3） Digital Europe Program

欧州のデジタルトランスフォーメーション（DX）を加速するためのプログラムである。スーパーコンピューター、AI、サイバーセキュリティ等の機能強化に必要な、インフラ構築に資金を提供するものである。「高性能コンピューティング」「人工知能（AI）」「サイバーセキュリティ・トラスト」「先端デジタルスキル」「経済・社会全体におけるデジタルの幅広い利用」の 5 分野があり、そのうち「サイバーセキュリティ」では、「量子通信インフラによる光通信・サイバーセキュリティ分野の能力強化」「ネットワーク・情報システムの均一な高レベルのセキュリティ実現のため、加盟国と民間部門の先端スキル・能力強化」が示されている。

4. 先進的サイバー防御機能・分析能力に係る制度的課題

2 章で示したような実際に行われているサイバー演習では、演習用に閉じた模擬的な環境や仮想環境での演習がほとんどであり、より実際の状況に近い攻撃や防御について経験することには限界がある。

また、3 章で示したような各種技術についても、より攻撃の内容に近づこうとするほど制度や法規制等による制約を受け、実装が難しくなるという問題がある。

本章では、より先進的な演習や技術を実装するにあたっての制度的課題について整理を行った。具体的には、先進的な取組において制度等が実際に制約や障害となった事例を調査し、その法令や制度の概要を整理するとともに、先進的なサイバー演習や技術開発を進める際の課題について整理を行った。

また、これらの課題への対応策についても、参考となりうる事例収集を行い、対応策に関する検討を実施した。

4.1 調査概要

調査対象とする法令・政策・対応策、国内外の事例を選定し、主に公開情報により、法令・政策等については、目的、対象、特徴等を抽出した。また、国内外の事例については、発生時期、発生事象、論点等を抽出した。調査結果を踏まえ、サイバー防御機能・分析技術に関わる政策等について検討を行った。

4.2 サイバーセキュリティの法令や制度に関連する事例整理

サイバーセキュリティに関する法令や制度は、基本的には、憲法に基づく個人の人権保護の観点から古くより制定されているものや、サイバー攻撃による被害防止の観点から整備されてきたものである。

しかし、先進的なサイバー防御の実装に当たっては、これらの法令や制度が制約となるケースも存在する。以下では、サイバー犯罪やサイバー対策に法令等が係る事案、事例について整理する。

4.2.1 マルウェア研究等がサイバー犯罪に該当した国内外の事例

刑事法的なリスクについては、法令の構成要件の範囲や明確性が論点となる。そのため、事例収集にあたって、刑罰法規およびその論点を意識する必要がある。

(1) セキュリティベンダ社員がウイルス保管容疑で逮捕された事例(2017 年)

P2P ファイル共有ソフト「Share」を介して得た情報流出型のマルウェアを業務用 PC に保管していたことで、セキュリティ会社社員が不正指令電磁的記録保管の疑いで京都府警サイバー犯罪対策課などに 2017 年 10 月に逮捕された事案である。

当該セキュリティ会社は、Shareで構築されたP2Pネットワークに顧客企業の情報が流出していないかを監視する業務を請け負っており、その過程で収集し、保管していたファイルにウイルスが含まれていたもの。ファイルはShareをインストールした業務用PCにキャッシュとして保管されていたが、他のShareユーザに対して公開状態となっており、他のユーザがウイルスを入手可能な状態にあったため、ウイル

ス取得・保管の容疑で担当社員の逮捕に至ったものである。警察の調査の結果、業務用PCにはウイルスを含むファイルが約 2,000 個保管されていたことがわかっている。

これに対して当該セキュリティ会社はウイルス取得・保管罪の要件である「正当な理由がないのに、その使用者の意図とは無関係に勝手に実行されるようにする目的で、コンピュータ・ウイルスやコンピュータ・ウイルスのソースコードを取得、保管する行為」のうち、理由と目的に関して罪に当たらないと広報で主張している。

セキュリティ会社社員は逮捕から 2 週間程度で釈放されており、翌年 3 月には「犯罪事実を立証できるような証拠が集められなかった」として不起訴となっている。

この事案は結果的に不起訴処分となったが、セキュリティ業界に幾つかの教訓と疑念を与える結果となり、セキュリティ対策への取組をより慎重なものとさせる要因になっている。

- Shareにはキャッシュの共有を防ぐパッチや設定があるにも関わらずその適用を怠っていたということで、研究や対策ソフト開発の用途でウイルス等を扱う場合には、その流出を防ぐための慎重な取り扱いや防護策の徹底が必要とされる（事故で流出させてしまった場合でも罪に問われる危険があるとの指摘もある）。
- セキュリティ研究の用途でサイバー攻撃を敢えて受けることを目的に故意に脆弱性のあるシステムをインターネット上に公開するハニーポットがある。攻撃手法の分析やマルウェアの収集に使われるが、適切に運用をしないと却って不正アクセスの踏み台にされてしまったり、不正なファイル交換の場所として利用される可能性もある。結果的にサイバー犯罪者の手助けをし、自身がサイバー犯罪に加担してしまうリスクが存在する。
- サイバーセキュリティに関するガイドライン等では、攻撃者にヒントを与えないように、対策の詳細を隠すことが多い。サイバーセキュリティを高めるためには、攻撃手法等の情報を共有し、対策の推進を後押しすることが重要であるが、これらの知見の共有や公開が、罪に問われる可能性があるのではとの懸念から、サイバーセキュリティに関する技術的な情報共有を躊躇する事態も発生している。これらの懸念の払しょくのため、業界としての取組が大事であり、この取組は後述の「サイバーセキュリティ業務における倫理行動宣言」にもつながるものとなっている。

（2） Coinhive 事件（2018 年）

自身のウェブサイトに Coinhive を設置し、閲覧者の許可を得ずに無断で暗号資産のマイニングを行わせたとして、ウェブデザイナーの男性が不正指令電磁的記録保管罪の疑いで神奈川県警に2018年2月に逮捕された事案である。Coinhiveに関しては同時期に各地で摘発が進んでおり、2018 年末までに全国で合計 28 件 21 人が検挙されたという報告がある。通常は簡易裁判により罰金や科料の略式命令が出され結審することが多いが、当該ウェブデザイナーは横浜簡易裁判所の罰金 10 万円の略式命令を不服として、正式裁判で争われることとなった。

検察側は、ウェブサイトの閲覧者はマイニングに気が付かないまま意図に反してプログラムが実行される形であり、閲覧者の同意は推定される状況にないとして、Coinhiveは不正指令電磁的記録にあたるとし、さらにウェブサイトにCoinhiveを設置することで閲覧者のパソコンでプログラムが動作することは認識しており、未必の故意があったとして、不正指令電磁的記録保管罪にあたると主張している。一方、ウェブデザイナー及び弁護側は、一般的なウェブサイトの広告と同様のもので、サイト広告は社会的にも認識されており、そもそも不正指令電磁的記録にあたらないと主張している。当該ウェブデザイナー

はCoinhiveの存在を知り、技術的面白さとともに、画面広告が表示されるよりもウェブサイトが見やすくなる点から、ウェブサイト運営の新たな収益源になり得る可能性があるとして、実験的にウェブサイトのソースコードのJavaScriptにCoinhiveのプログラムを書き加えた。しかしその後、サイト閲覧者よりユーザの同意がないままCoinhiveを動かすのはグレーではないかとの指摘を受け、また収益性も低いとの判断から約1ヶ月でプログラムを削除している。

裁判は最高裁まで争われ、2022年1月に無罪が確定した。この間、1審では反意図性は認めたが、Coinhiveが社会的に許容されていなかったとは断定できないとして不正性を否定して無罪、2審では反意図性とともに不正性も認めて有罪、最高裁においては反意図性は認めたが、サイト閲覧中に閲覧者のCPUを使用する割合も閲覧者が気が付くほどではなく、広告表示と比較しても優位な差異は認められず、社会的に許容し得る範囲内だとして不正性は認めず、不正指令電磁的記録とは認められないとして2審判決を破棄した。この事案の論点をまとめると以下のようになると思われる。

- 不正指令電磁的記録保管罪において、何が不正指令電磁的記録に当たるかの明確な基準がない。警視庁のサイトでは刑法第168条3に基づくウイルスの取得・保管について「正当な理由がないのに、その使用者の意図とは無関係に勝手に実行されるようにする目的で、コンピュータ・ウイルスやコンピュータ・ウイルスのソースコードを取得、保管する行為」としており、不正性や反意図性への判断が焦点となるが、その基準が明確ではない。今回の最高裁判決では、不正性の判断基準として「社会的に許容しえないプログラムが該当する」として一歩踏み込んだが、どういう場合に社会的に許容しえないのかは1件1件判断していくことに変わりはない。
- 一般的な視点として、不正指令電磁的記録というのはコンピュータウイルスのことを指すと考えられており、新たな技術の利用がある日突然に不正指令電磁的記録と解釈されて摘発されるような事態が続発することにより、新たな技術の利用やその情報共有を自粛する動きにつながっている。実際、2013年から継続してきたコミュニティレベルのセキュリティ勉強会を2019年に休止するという動きも発生している。

（3） Wizard Bible 事件（2018 年）

情報セキュリティに関する技術情報を投稿できる情報提供サイト「Wizard Bible」において、ウイルスのプログラムを公開したとして、サイトの管理者が不正指令電磁的記録提供の罪で2018年3月に摘発、略式起訴され、罰金 50 万円の略式命令を受けた事案である。サイトは2018年4月に閉鎖に追い込まれている。

問題とされたプログラムはトロイの木馬型マルウェアの解説記事に含まれていたもので、ネットワーク経由で送信されたコマンドをそのまま実行するというものだったが、サーバの遠隔管理等に使う一般的な機能であり、プログラムは入門書にも載っているような簡単なサンプルコードレベルのものだったとされている。また、このサンプルコードにはファイアウォールを越える機能はないため、高度な技術がなければ悪用も難しいものだった。サイト管理者もこの程度の内容のものがウイルスとして摘発されたと驚いており、摘発される基準がわからず、草の根レベルのセキュリティ研究が難しくなると発言していた。

警察庁によると不正アクセスの検挙件数は年々増加しており、研究目的や情報提供目的で本人が悪意を持っていない状況でも摘発されるケースも含まれており、この状況を課題であると指摘するセキュリティ関係者は多い。

（4） 岡崎市立中央図書館事件（2010年）

岡崎市立図書館の蔵書検索システムにアクセス障害が発生、同システムに高頻度の検索リクエストを送り付けたとして、利用者の男性1名が2010年5月に愛知県警に偽計業務妨害の容疑で逮捕された事案である。男性は蔵書検索システムの使い勝手に不満をもち、独自にクローラを実行して蔵書情報を収集していたが、この結果、蔵書検索システムに障害が発生し、逮捕に至ったものである。その後、取り調べの結果として業務妨害の意図は認められないとして、翌6月に起訴猶予処分となっている。

クローラ自身は、1秒間に1リクエスト程度しかしないように調整されており、常識的な動作をするものであったが、蔵書検索システム側に不具合があり、障害が発生していた。

- ウェブサイトから情報を自動で収集するクローラは広く使われているが、相手サイトに障害を与えたり、攻撃と受け取られないように、リクエストの頻度を調整するなど、注意が必要である。
- セキュリティ関係のサービス等においても、ポートスキャンや外部からのウェブサイト診断は広く行われており、攻撃と受け取られたり、法令違反に問われることのないよう、注意が必要となっている。

4.2.2 通信の秘密等のその他の法令や制度に関する議論

マルウェア研究等を含めてサイバーセキュリティに関する研究や情報提供等は、主に刑法における不正指令電磁的記録に関する罪との関係で事案化されているケースが多いが、サイバーセキュリティに関する法令や制度は、それ以外にも様々な議論がされている。

- 日本国憲法第九条（戦争の放棄とその解釈としての専守防衛）、第二十一条（表現の自由と通信の秘密）により、日本が武力攻撃を受けて防衛出動が発令されない限り、攻撃の兆候があることだけを理由として、相手のシステムに侵入したり、反撃行為を行うのは困難とされている。
- 仮にサイバー攻撃のアトリビューションや攻撃を抑止する意図であっても、攻撃元のシステムに侵入することは不正アクセス禁止法への違反を問われる可能性がある。同様の目的で攻撃元のIDやパスワード等を何らかの方法で入手し、本来は利用権限のない機器を動かすことも不正アクセス禁止法に違反する可能性がある。
- また攻撃元の無力化するために相手のシステムやファイルに改編や破壊を加えたり、そのためのマルウェアを作成すること等も刑法に違反する可能性がある。

4.3 国内外の関連法令や制度の概要

法律等のハードローの他、ガイダンス等のソフトロー的な取り組みは主体が多岐にわたる（当局や業界団体の他、オンライン人権団体等）ため、各主体の立ち位置を意識する必要がある。

（1） 関連法令・制度

1） 不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）

不正アクセス行為を禁止するとともに、これについての罰則及びその再発防止のための援助措置等を定める法律である。

不正アクセス行為の禁止（第三条）、他人の識別符号を不正に取得する行為の禁止（第四条）、不正アクセス行為を助長する行為の禁止（第五条）、他人の識別符号を不正に保管する行為の禁止（第六条）、識別符号の入力を不正に要求する行為の禁止（第七条）、アクセス管理者による防御措置（第八条）等について定めている。

2） 特許法

発明の保護やその利用促進を図る法律である。サイバーセキュリティ技術の対象となるようなプログラムについては、物の発明の一部として定義されている。

主に特許の出願から審査、特許に基づく権利、意義や審判等に関する手続きが定められているが、サイバーセキュリティとの関係では、定義（第二条）、特許を受けることができない発明（第三十二条）、特許の効力が及ばない範囲（第六十九条）等について定めている。

3） 著作権法

プログラムを含む著作物や演奏、放送等に関し著作者の権利及び隣接する権利の保護をし、文化の発展に寄与することを目的とした法律である。

サイバーセキュリティとの関係では、著作物に表現された思想又は感情の享受を目的としない利用（第三十条の四）、差止請求権（第百十二条）、侵害とみなす行為（第百十三条）等を定めている。

4） ライセンス・使用許諾

法令ではないが、プログラムやサービスの利用にあたって、利用者との間の合意を定めたものであり、契約に相当する効力を発揮する。従ってライセンス・使用許諾に違反した利用は、契約違反として責任を問われることがある。

5） 刑法（不正指令電磁的記録に関する罪）

情報処理の高度化等に対処するための刑法等の一部を改正する法律（平成 23 年法律第 74 号）が 2011 年 6 月 24 日に公布され、新たに「不正指令電磁的記録に関する罪」が設けられが設けられた。

不正指令電磁的記録作成等（第百六十八条の二）、不正指令電磁的記録取得等（第百六十八条の三）について定めており、「正当な理由がないのに、人の電子計算機における実行の用に供する目的で、人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録、不正な指令を記述した電磁的記録その他の記録を作成し、又は提供し、又は実行の用に供し、又は未遂の者への罰則」を定めている。

その他、サイバーセキュリティとの関係では、電磁的記録不正作出及び供用（第百六十一条の二）、電子計算機損壊等業務妨害（第二百三十四条の二）、電子計算機使用詐欺（第二百四十六条の二）等についても定めている。

6） 電気通信事業者における事業法や電気通信事業法施行規則等

いわゆる通信の秘密について定めているもので、電気通信事業法においては、秘密の保護（第四条）、

罰則（第百七十九条）、有線電気通信法においては、有線電気通信の秘密の保護（第九条）、罰則（第十三条、第十四条、第十五条）、電波法においては、秘密の保護（第五十九条）、罰則（第百九条）等を定めている。

7） サイバー行動に適用される国際法に関する日本政府の基本的な立場

国連において、国際法がサイバー行動にどのように適用されるかについて議論するため、「国際安全保障の文脈における情報通信分野の発展に関する政府専門家グループ」が設置され、2019 年 5 月に国連憲章全体を含む既存の国際法がサイバー行動にも適用されることを確認するコンセンサスが採択されている。これを受けて、日本政府としての立場を外務省より公表したものである。

それによると、「国連憲章全体を含む既存の国際法はサイバー行動にも適用される」、「国家は、サイバー行動によって他国の主権を侵害してはならず、他国の国内管轄事項に干渉してはならない」、「サイバー空間における国家による国際違法行為は当該国家の国家責任を伴う」、「サイバー行動が関わるいかなる国際紛争も、国連憲章第 2 条 3 に従って平和的手段によって解決されなければならず、サイバー行動であっても、一定の場合には、国連憲章第 2 条 4 が禁ずる武力による威嚇又は武力の行使に当たり得る」等とされている。国家、又は国家を背景としたサイバー攻撃は武力攻撃とみなしうるとしていることになる。

（2） その他の取組

1） サイバーセキュリティ業務における倫理行動宣言（日本ネットワークセキュリティ協会）

サイバーセキュリティ事業にはサイバー犯罪と見做されて誤認逮捕等を引き起こす事業固有リスクがある。この宣言は、業界全体として共通的に取り組むべきリスク管理指針を定めたものであり、本宣言に則って業務を遂行することを対外的に宣言することで、適切なセキュリティ活動を実施していることをアピールすることができるとしている。

宣言では、サイバーセキュリティ事業に携わる者の行動規範として次の 5 項目を定めている。

- 情報社会の安全を向上させ、安心の醸成に努めます。
- 法令等の正しい理解に努め、これを遵守します。
- 高度化する脅威に備え技術の向上に努めます。
- 自らの製品およびサービスの安全確保に努めます。
- 倫理観を持ち、正当な目的のために業務を遂行します。

そのうえで事業遂行の基本指針として、リスク管理の考え方や管理策の実施方法について整理しており、各事業者はこの方針に基づいて事業を実施するとしている。

2023 年 3 月時点の宣言参加企業は 16 社である。

4.4 先進的なサイバー防御機能や分析能力の推進・向上に向けた関連法令等の課題及び対応策

サイバー演習やセキュリティに関する技術開発を進める際の制度的課題を検討するにあたり、関連法

令等の概要及び想定される課題を挙げる。

表 5　サイバー演習やセキュリティ関連技術開発を行う際の関連法令等の概要及び想定される課題、対応策

法令等	概要及び課題	対応策
不正アクセス禁止法	電気通信回線(インターネット等)を経由し、第三者のアクセス制御機能を有する特定電子計算機に対して無断で他人の識別符号(ID、パスワード等)を使う他、アクセス制御機能を回避してアクセスすること(不正アクセス)を禁止した法律。	脆弱性検証を行う場合には、機器やシステムの開発者・利用者の同意や、機器やシステムに対するアクセス手法について留意する必要がある。
特許法	プログラムは特許法によって知的財産として保護される場合があるが、特許法 69 条 1 項において「試験又は研究のためにする特許発明の実施」については許可を明記している。	脆弱性検証の目的や明示の仕方に関して留意する必要がある。
著作権法	機器のファームウェアをリバースエンジニアリングのために逆コンパイルして調査・解析を行うことは、対象となるプログラムの著作権を侵害する行為となりえたが、2019 年 1 月 1 日に施行された「著作権法の一部を改正する法律」によって、著作権法第三十条の四「技術の開発又は実用化のための試験の用に供するための利用」の改正が規定された。具体的には、技術の開発等のための試験の用に供する場合、情報解析の用に供する場合等にはその必要と認められる限度において利用することができると規定しており、文化庁の Web サイトにおいても「プログラムの調査解析を目的としてプログラムの著作物を利用する行為(いわゆる「リバース・エンジニアリング」)」は権利制限の対象として挙げられることが記載されている。	技術開発等のための機器に対するリバースエンジニアリングは可能であるが、必要と認められる限度に留意する必要がある。
ライセンス・使用許諾	多くのソフトウェア製品では、ライセンス契約や使用許諾契約においてリバースエンジニアリングを禁止する条項が記載されている。機器においても、ファームウェアの利用について使用許諾契約やライセンス契約に同意したことを前提に利用することになっているものがある。	リバースエンジニアリングは法令としては認められる行為であっても、機器・ソフトウェアのライセンス・使用許諾条項において問題がないか留意する必要がある。
不正指令電磁的記録に関する罪 (ウイルス製造罪)	情報処理の高度化等に対処するための刑法等の一部を改正する法律(平成 23 年法律第 74 号)が平成 23 年 6 月 24 日に公布され、改正法により、刑法に新たに「不正指令電磁的記録に関する罪(いわゆるコンピュータ・ウイルスに関する罪」)」が制定、同年 7 月 14 日に施行。ウイルスの作成、提供、供用、取得、保管行為が罰せられる。「正当な理由がないのに（正当な理由の不存在）」「人の電子計算機における実行の用に供する目的で（目的）」「 第 1 号又は第 2 号)に掲げる電磁的記録その他の記録を（客体)を 」「作成し, 又は提供した（行為）」場合に成立する。	サイバー演習や研究開発においては、罪が成立する条件に合致しないよう正当な理由の存在等に留意する必要がある。
電気通信事業者における事業法や電気通信事業法施行規則等	電気通信事業者の取扱中に係る通信の秘密については電気通信事業法第4条、第179条、有線電気通信における通信の秘密は有線電気通信法第9条、第14条、無線通信における通信の秘密は、電波法第59条、第109条により保護されている。	サイバー演習や研究開発において、利用する組織等のネットワークについては、電気通信事業法上の通信の秘密の保護が及ぶものではないが、有線電気通信法の適用を受ける可能性がある。プライバシー保護への配慮も必要となる。

また、サイバーセキュリティ対策の実施に当たって、実際に法令や規則等を変更した例もあり、参考と

して紹介する。

- 国立研究開発法人情報通信研究機構法の改正による特定アクセスの認可と IoT 機器調査業務実施

  2017 年頃よりIoT機器を乗っ取るMiraiマルウェアやその亜種によるボットネット等が大きく問題となり、それに付随して、IoT機器のセキュリティ確保が大きな課題となった。この課題に対応するため、パスワード設定等に不備のあるインターネットにつながれたIoT機器を特定し、注意喚起をするため、IoT機器の調査業務を国立研究開発法人情報通信研究機構（NICT）が実施することとなった。

  調査に当たっては、インターネット上に接続されたIoT機器に実際にアクセスし、初期パスワード等で実際にアクセスを試みて、アクセスが成功すればパスワード設定が不適切なものとして注記喚起の対象とするというもので、不正アクセスと捉えられかねない方法である。このため、5 年間の時限措置として、NICTの法定業務としてパスワード設定等に不備のあるIoT機器の調査を追加する法改正を行い、このような調査アクセスを特定アクセス行為として法的に認める方法をとった。

5. 研究会の運営

本調査の実施及び取りまとめにあたり、専門的な見地からの検討、分析、助言を得ることを目的に、研究会を開催する。

5.1 第 1 回研究会の運営

(1) 開催概要

日時 2023 年 1 月 30 日(月)18:00～19:00
場所 Teams 会議(Web 会議)

5.2 第 2 回研究会の運営

(1) 開催概要

日時 2023 年 3 月 7 日(火)9:00～10:30
場所 Teams 会議(Web 会議)

令和4年度サプライチェーン・サイバーセキュリティ対策促進事業
（先進的なサイバー防御機能や分析能力に係る技術動向及びサイバー演習動向等に関する調査）
報告書

2023 年 3 月

株式会社三菱総合研究所
デジタル・イノベーション本部
サイバーセキュリティ戦略グループ
TEL 03-6858-3578