資料７－７

総務省

７　サイバーセキュリティ関係の取組状況について

令和4年3月

総務省
サイバーセキュリティ統括官室

政府全体のサイバーセキュリティ推進体制

- 「サイバーセキュリティ戦略本部」（本部長：内閣官房長官）が政府全体の司令塔（「サイバーセキュリティ基本法」に基づき、平成27年に設置）。総務大臣も、同戦略本部の構成員。
- 「サイバーセキュリティ戦略」の策定・改定を始め、政府横断的にセキュリティ対策を推進することが役割。

サイバーセキュリティ戦略本部（2015.1.9 サイバーセキュリティ基本法により設置）

本部長　内閣官房長官
副本部長　サイバーセキュリティ戦略本部事務を担当する国務大臣
本部員　国家公安委員会委員長
デジタル大臣
総務大臣
外務大臣
経済産業大臣
防衛大臣
経済安全保障担当大臣
東京オリンピック競技大会・パラリンピック競技大会担当大臣

本部有識構成員（８名）

遠藤　信博	日本電気株式会社代表取締役会長
後藤　厚宏	情報セキュリティ大学院大学学長
田中　孝司	KDDI株式会社代表取締役会長
中谷　和弘	東京大学大学院法学政治学研究科教授
野原佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英	日本大学大学院法務研究科教授
宮澤　栄一	株式会社デジタルハーツホールディングス取締役会長
村井　純	慶應義塾大学環境情報学部教授 大学院政策・メディア研究科委員長

（事務局）
内閣官房　内閣サイバーセキュリティセンター（NISC）

デジタル庁

デジタル社会の形成に向けた司令塔としてデジタル改革を推進

緊密連携

国家安全保障会議（NSC）

我が国の安全保障に関する重要事項を審議

緊密連携

閣僚本部員6省庁

- 警察庁（サイバー犯罪・攻撃の取締り）
- デジタル庁（デジタル改革）
- **総務省**（通信・ネットワーク政策）
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
- 防衛省（国の防衛）

重要インフラ（14分野）
情報通信、地方公共団体(=**総務省所管**)、金融機関、医療、水道、電力、ガス、化学、クレジット、石油、鉄道、航空、物流、空港

協力

協力

重要インフラ事業者等　政府機関（各府省庁）　企業　個人

サイバーセキュリティと総務省の役割

- **サイバー空間**は、あらゆる主体が利用する公共空間であり、その**根幹は情報通信ネットワーク。**
- **サイバー攻撃**等により、**情報通信ネットワークの機能停止や情報の漏えい等**が生ずれば、**国民の生活**や**我が国の経済社会**に**甚大な影響**が発生するおそれ。

⇒総務省の役割：社会経済活動を支える情報通信ネットワークの安全を確保し、サイバー空間を利用する全ての国民のサイバーセキュリティの向上を図ること。

「ICTサイバーセキュリティ総合対策2021」(総務省サイバーセキュリティタスクフォース)

➢ 総務省においては、情報通信分野におけるサイバーセキュリティの確保に向け、毎年取組方針を整理し、公表（直近は「ICTサイバーセキュリティ総合対策2021（令和3年7月）」）

＜政策課題に対処するための主な施策＞

＜電気通信事業者における安全かつ信頼性の高いネットワークの確保＞

電気通信事業者のネットワークや電気通信サービスにおけるリスクの高まりに応じた適切なセキュリティ対策を講じる必要

＜COVID-19への対応を受けたセキュリティ対策の推進＞

COVID-19感染拡大が続く中、中小企業等におけるテレワーク推進のためセキュリティ対策が急務。コロナ後も視野に、トラストサービスの推進も重要。

＜デジタル改革・DX推進の基盤となるサービス等のセキュリティ対策＞

IoT、クラウド、スマートシティについて、それぞれの課題に応じた適切な対策を推進していくことが必要。

＜サイバーセキュリティ情報に関する産学官での連携・共有等の促進＞

有効な技術や知見の共有による社会全体での対策の底上げ等が重要。

「ICTサイバーセキュリティ総合対策2021」の構成

Ⅰ 改定に当たっての主要な政策課題

Ⅱ 情報通信サービス・ネットワークの個別分野に関する具体的施策

1. 電気通信事業者における安全かつ信頼性の高いネットワークの確保のためのセキュリティ対策の推進
- (1) 安全かつ信頼性の高いネットワークの確保
- (2) サイバー攻撃に対する電気通信事業者の積極的な対策の実現
- (3) 5Gの本格的な普及に向けたセキュリティ対策の強化

2. COVID-19への対応を受けたセキュリティ対策の推進
- (1) テレワークセキュリティの確保
- (2) トラストサービスの制度化と普及促進

3. デジタル改革・DX推進の基盤となるサービス等のセキュリティ対策の推進
- (1) IoTのセキュリティ対策
- (2) クラウドサービスの利用の進展を踏まえた対応
- (3) スマートシティのセキュリティ対策

4. 分野別の具体的施策
- (1) 無線LANのセキュリティ対策
- (2) 放送分野のセキュリティ対策
- (3) 地域の情報通信サービスのセキュリティの確保

Ⅲ 横断的施策

1. サイバーセキュリティ情報に関する産学官での連携・共有等の促進
- (1) 我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速
- (2) サイバー攻撃被害情報の適切な共有及び公表の促進
- (3) その他の情報共有・情報開示の促進

2. ICTサイバーセキュリティに係る横断的施策
- (1) 国際連携の推進
- (2) 研究開発の推進
- (3) 人材育成・普及啓発の推進

別添：プログレスレポート2021（総合対策2020の各施策の進捗状況）

（参考）サイバーセキュリティタスクフォースの概要

趣旨

- 2020年東京オリンピック・パラリンピック競技大会における成果や「サイバーセキュリティ戦略」（2021年９月28日閣議決定）を踏まえつつ、サイバー攻撃の複雑化・巧妙化や脆弱性の拡大などの動向に対応したサイバーセキュリティに係る課題を整理するとともに、情報通信分野において講ずべき対策や既存の取組の改善など幅広い観点から検討を行い、必要な方策を推進することを目的として、サイバーセキュリティタスクフォースを開催（2017年１月～）。

体制

- 本タスクフォースは座長１名、座長代理１名、委員14名
- 事務局は、サイバーセキュリティ統括官室が行う。

議題

- サイバーセキュリティに係る動向把握
- サイバーセキュリティを支える基盤・制度の在り方
- サイバーセキュリティを担う人材育成や普及啓発の在り方
- サイバーセキュリティ確保に向けた国際連携の在り方

タスクフォース構成員（敬称略）

鵜飼　裕司	株式会社FFRIセキュリティ　代表取締役社長
宇佐美　理	日本テレビ放送網株式会社ICT戦略本部　専任部長
岡村　久道	英知法律事務所 弁護士、京都大学大学院医学研究科　講師
後藤　厚宏	情報セキュリティ大学院大学　学長　(座長)
小山　覚	NTTコミュニケーションズ情報セキュリティ部　部長、ICT-ISAC　ステアリング・コミッティ運営委員長
篠田　佳奈	株式会社BLUE　代表取締役
園田　道夫	国立研究開発法人情報通信研究機構（NICT）、ナショナルサイバートレーニングセンター　センター長
辻　伸弘	SBテクノロジー株式会社　プリンシパルセキュリティリサーチャー
戸川　望	早稲田大学理工学術院　教授
徳田　英幸	国立研究開発法人情報通信研究機構（NICT）理事長、慶應義塾大学 名誉教授 (座長代理)
中尾　康二	ICT-ISAC　顧問、国立研究開発法人情報通信研究機構（NICT）　主管研究員
名和　利男	サイバーディフェンス研究所　専務理事/上級分析官
林　紘一郎	情報セキュリティ大学院大学前学長・名誉教授
藤本　正代	情報セキュリティ大学院大学　教授、GLOCOM客員研究員
吉岡　克成	横浜国立大学大学院環境情報研究院/先端科学高等研究院　准教授
若江　雅子	株式会社読売新聞東京本社　編集委員

オブザーバ：内閣官房内閣サイバーセキュリティセンター、デジタル庁、経済産業省、地方公共団体情報システム機構

総務省のサイバーセキュリティに関する取組の大枠

情報通信分野におけるサイバーセキュリティの確保

＝ なりすましやサイバー攻撃による**情報・データの流出・改ざん・サービスの停止を防止**

⇒ 以下の施策を推進することで、**安全で信頼できる情報通信インフラ、機器・サービスを実現**

電気通信事業者による積極的セキュリティ対策

・フロー情報(※1)の分析によるC&Cサーバ(※2)の検知に向けた取組

５Ｇのセキュリティ

・5Gのサプライチェーンリスク対策を含むセキュリティ担保

テレワークのセキュリティ

・テレワークセキュリティガイドライン
・中小企業等向けのチェックリスト

トラストサービス

・タイムスタンプ、eシール等のトラストサービスの制度整備及びその普及に向けた取組

ＩｏＴ(※3)のセキュリティ

・パスワード設定に不備のあるIoT機器の調査（NOTICE）等

クラウドのセキュリティ

・クラウド提供におけるセキュリティ対策ガイドライン
・ISMAP

(※1) IPアドレスやポート番号、タイムスタンプ等の付随情報
(※2) 各感染端末（ボット）にサイバー攻撃の指示を出す管理サーバ

(※3)「Internet of Things」ネットに接続された監視カメラ等

研究開発

・NICTのサイバー攻撃観測技術（「NICTER」）等を用いた高度な分析技術の研究開発 など

人材育成

・「ナショナルサイバートレーニングセンター」における取組 など

「統合知的・人材育成基盤（CYNEX）」の構築

国際連携

・米国との連携、ASEANとの連携（「日ASEANサイバーセキュリティ能力構築センター（AJCCBC）」） など

■ 主な取組

1.　サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証

①フロー情報分析によるC&Cサーバ検知技術の実証
②悪性Webサイトの検知技術・共有手法の実証
③ISPにおけるネットワークセキュリティ技術の導入実証等

2-1. セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

①実践的サイバー防御演習　（CYDER）
②SecHack365

2-2. セキュリティ人材の育成（地域におけるIoTセキュリティ人材の確保）

2-3. 地域に根付いたセキュリティコミュニティ（地域SECUNITY）の形成促進

3.　サイバーセキュリティに関する産学官の結節点『CYNEX』

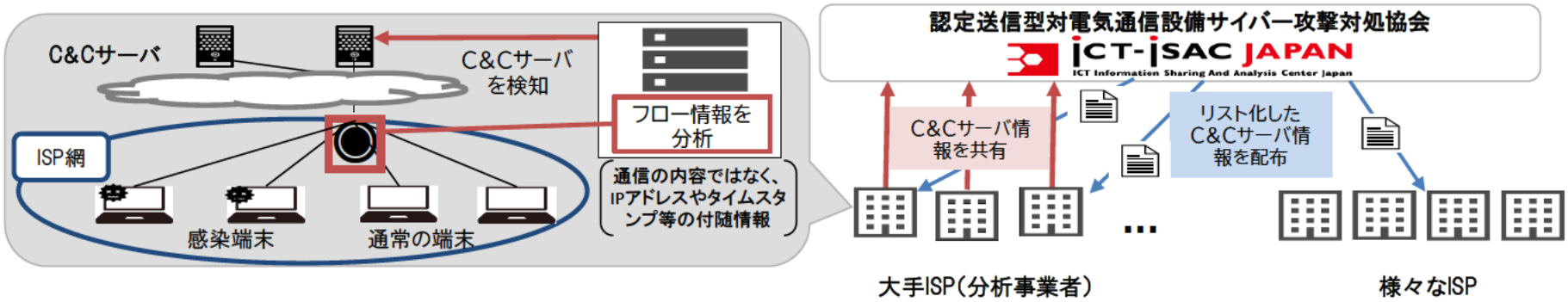
4.　サイバーセキュリティ対策の強化についての注意喚起

1. サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証

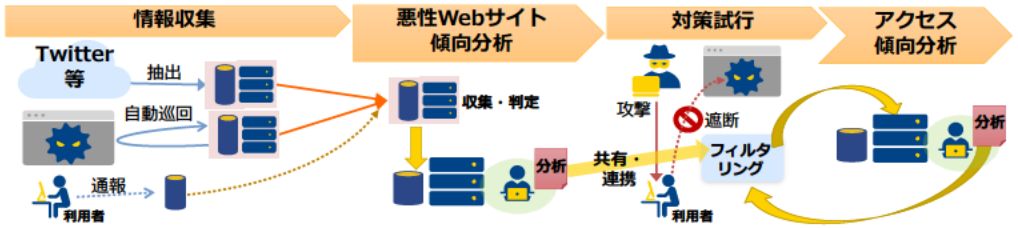
➢ 大規模化・巧妙化・複雑化するサイバー攻撃・脅威に、電気通信事業者が技術的手法を活用して効率的・積極的に対処できるようにするため、①フロー情報分析によるC&Cサーバ検知技術の実証、②悪性Webサイトの検知技術・共有手法の実証、③ネットワークセキュリティ技術の円滑な導入のための実証を実施。

①フロー情報分析によるC&Cサーバ検知技術の実証

※C&C(Command and Control)サーバ：各感染端末（ボット）にサイバー攻撃の指示を出す管理サーバ

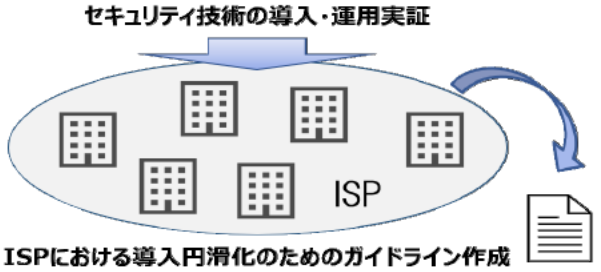


② 悪性Webサイトの検知技術・共有手法の実証



※悪性Webサイト：IDやパスワードなど個人情報の窃取に使用される、正規の金融機関等に偽装したWebサイト（フィッシングサイト） など

③ ネットワークセキュリティ技術の導入実証



※ ネットワークセキュリティ技術: BGPハイジャックに対するRPKI、DNSハイジャックに対するDNSSEC、なりすましメールに対するDMARC 等

①フロー情報分析によるC&Cサーバ検知技術の実証

- 大規模化・巧妙化・複雑化するサイバー攻撃・脅威に、電気通信事業者が積極的に対処できるようにするため、フロー情報の分析を通じて、サイバー攻撃の指令元であるC&Cサーバを検知する技術の実証を行う。具体的には、電気通信事業者におけるフロー情報分析によるC&Cサーバ検知技術の有効性の検証や、事業者間の共有に当たっての運用面の課題整理のための実証事業を実施予定。

（※）フロー情報：通信トラフィックに係るデータのうち、IPアドレス及びポート番号等のヘッダ情報並びにルータでヘッダ情報を抽出する際に付与されるタイムスタンプ等の情報

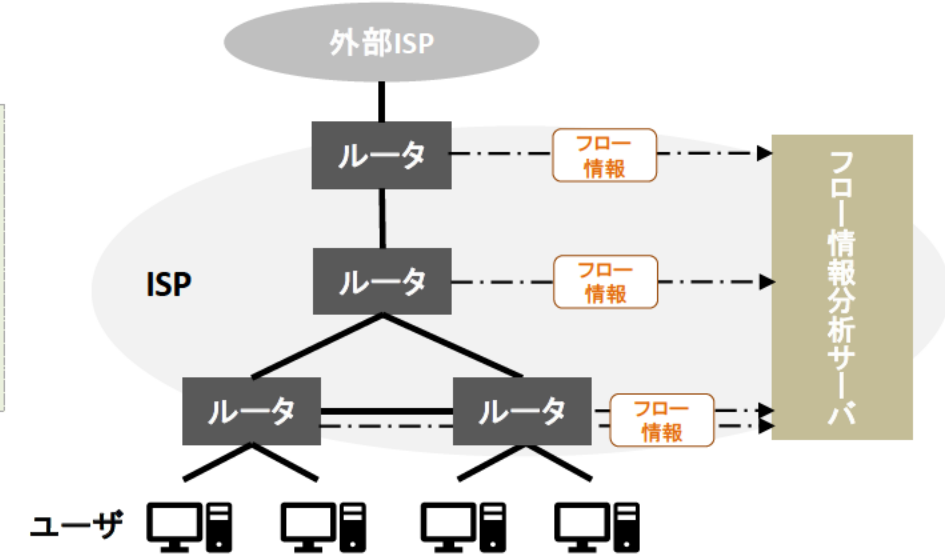
C&Cサーバ：Command and Controlサーバの略で、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者から指令を送り、制御を行うサーバコンピュータ

- なお、有識者による研究会において、昨年11月に通信の秘密に係る法的整理を実施。

1）フロー情報の収集・蓄積

- ISPのネットワーク内の各所に設置されているルータから、当該ルータを通過するユーザの通信トラフィックに係るデータの一部（IPアドレス、ポート番号等）を収集・蓄積する。

※大手ISP等においては、通信の傾向を把握し、ネットワークの設計や輻輳対策、DDoS攻撃対策等に活用するべく、平時からフロー情報の収集を行っており、これをC&Cサーバ検知に活用する。

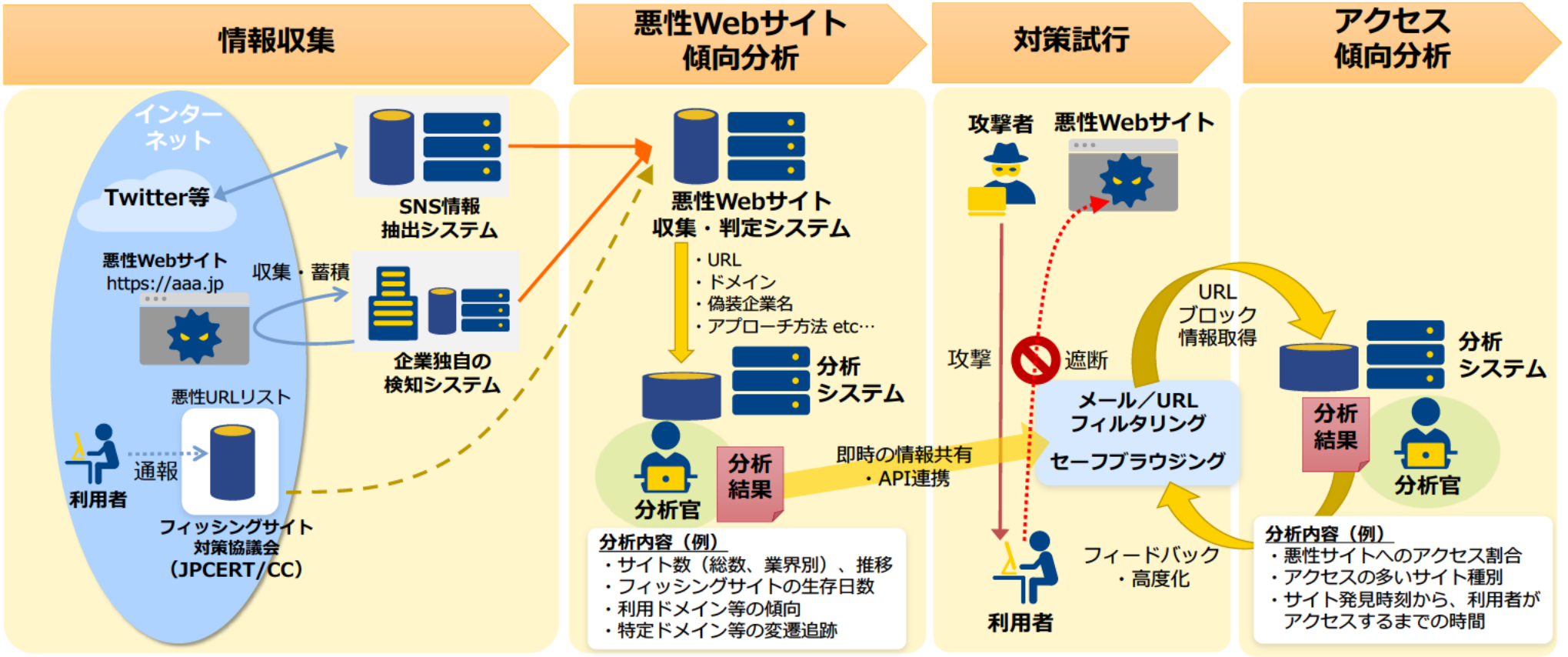


2）フロー情報の分析・C&Cサーバの検知

- 踏み台となる感染端末を用いたサイバー攻撃においては、複数の感染端末が共通の相手方（＝標的、C&Cサーバ等）と通信を行ったり、共通のふるまい（例えば、同種・同サイズのパケットを同時期に大量送信する等）をすることから、フロー情報の中からこうした通信の特徴を抽出し、C&Cサーバの検知を行う。

②悪性Webサイトの検知技術・共有手法の実証

- SNS等への投稿、企業独自の悪性Webサイト検知システム、また利用者による通報等をもとに、自動巡回による機械的処理を活用して悪性Webサイト情報の収集・分析を行い、利用者の被害実態把握および課題について整理し、悪性Webサイトを検知する手法の有効性実証、検知結果を活用し継続的な対策を講じるための必要事項を整理する実証事業を行う。



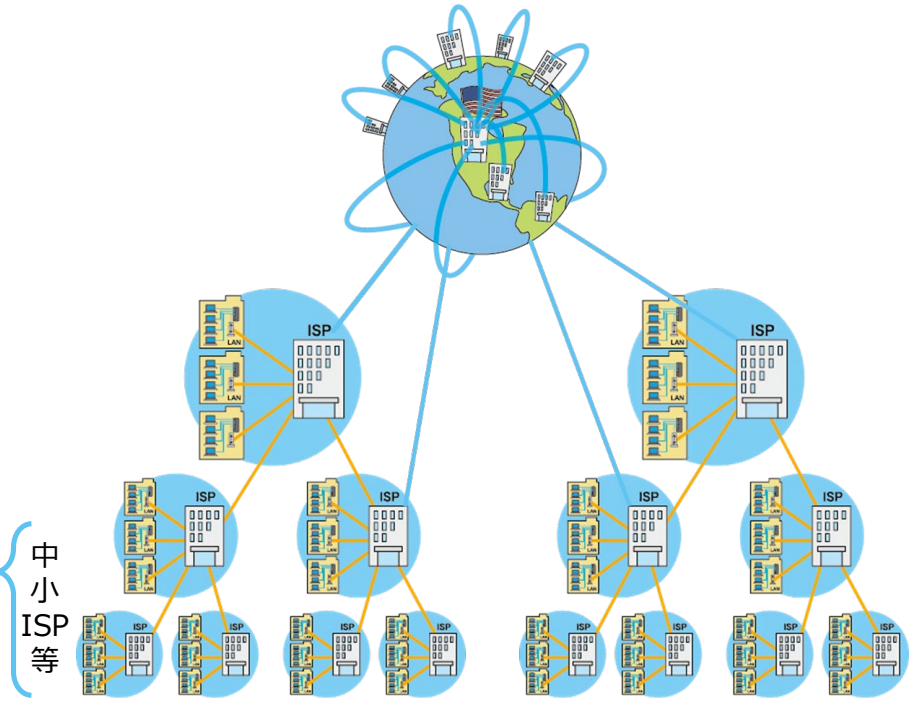
自社偽装サイト検知の仕組みの各種企業への提供、URLフィルタリング・迷惑メール対策・セーフブラウジングの高度化およびJPCERTと連携し悪性Webサイトのテイクダウンに貢献

③ISPにおけるネットワークセキュリティ技術の導入実証等

- インターネットの一部の脆弱な仕様を悪用するサイバー攻撃に対しては、電子認証技術を活用したネットワークセキュリティ技術が国際標準化*されており、それらを実装することで通信ネットワーク側で抑え込むことが可能。
  *例: BGPハイジャックに対するRPKI、DNSハイジャックに対するDNSSEC、なりすましメールに対するDMARC等がIETFでRFC化されている。
- これらの実装には、各ISP等が管理する通信ネットワークに、対応ソフトウェア・ハードウェアを組み込み、継続運用していく必要があるところ、国内においては以下のような事情もあり、いまだ普及率が上がらないのが実情。
  - ✓ 通信ネットワークの再構築を要するとともに、導入後は電子認証技術の運用に関する知見や能力が求められる。
  - ✓ ユーザが、各ISPを選定する際、対策状況が分からない・判断が難しいなど、ISPが苦労して導入・運用しても競争優位に繋がるか不透明。
  - ✓ ネットワークセキュリティ技術の実装に関する特段の規制も存在しない。
- 本事業では、中小ISP等の通信ネットワークを実証環境とし、ネットワークセキュリティ技術の導入実証を実施。得られた知見等に基づき、ISPにおける導入円滑化のためのガイドラインを作成するとともに、対策を実装したセキュアな通信ネットワークがユーザから評価される仕組みの在り方検討等を進める。

- ネットワークセキュリティ技術の導入実証（想定される対象技術: RPKI, DNSSEC, DMARC等）
- 実証結果に基づき:
  - ISPにおける導入円滑化のためのガイドラインを作成
  - セキュアな通信ネットワーク・ISPがユーザから評価される仕組みの在り方検討 等

- インターネットの一部の脆弱な仕様を悪用するサイバー攻撃に対する、通信ネットワーク側での積極的対処を推進
- 自律・分散・協調のもと、我が国サイバー空間の安全性と信頼性の強化とユーザの保護を実現



2-1. セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

➢ 巧妙化・複雑化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、平成29年4月より、情報通信研究機構（ＮＩＣＴ）の「ナショナルサイバートレーニングセンター」において演習等を実施。

CYDER（サイダー）

国・地方公共団体・独法・重要インフラ事業者等を対象とした実践的サイバー防御演習

⇒ **年間100回、計3,000名規模**で実施（**１日**コース＆**全都道府県**で開催）
2017年度以降で、延べ**13,867名**が受講
2021年度から、オンラインコースを開設するとともに、準上級コースを開設

cyber colosseo（サイバーコロッセオ）

2020年東京大会関連組織のセキュリティ担当者等を対象とした実践的サイバー演習

⇒ 2017年度から開始し、2020年12月で事業完了
期間中に、**演習形式**で延べ**571**名、**講義形式**で延べ**1,717名**の人材を育成

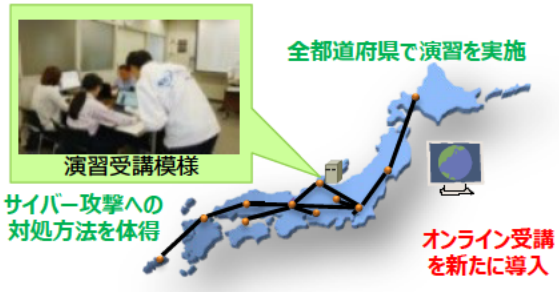
サイバーコロッセオのレガシーとして、準上級コースを制作

SecHack365（セックハック365）

25歳以下の若手セキュリティイノベーターの育成

⇒ **年間50名程度**の受講者を選定し、**１年間のトレーニング**コースを実施
2017年度以降で、計**212名が修了**

新たな手法のサイバー攻撃にも対応できる演習プログラム・教育コンテンツを開発



実事案に対処可能な人材育成
CYDER

高度な攻撃に対処可能な人材育成
サイバーコロッセオ

ハイレベル層の人材育成
SecHack365

①実践的サイバー防御演習（CYDER）

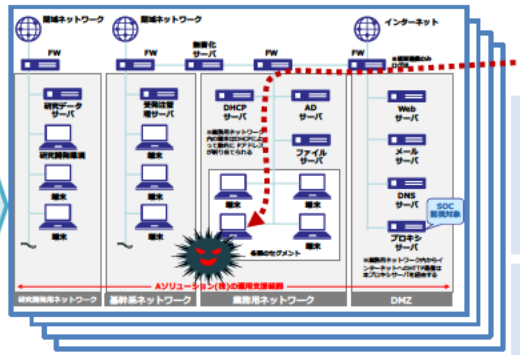
- 総務省は、情報通信研究機構(NICT)を通じ、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習**(**CYDER**)を実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って、**外部のセキュリティ事業者の支援を受けることを前提としてサイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回・計3,000名規模**で実施。 参加申込 → https://cyder.nict.go.jp
  ※2017年度:100回・3,009名、2018年度:107回・2,666名、2019年度:105回・3,090名、2020年度:106回・2,648名、2021年度:105回・2454名

CYDER: CYber Defense Exercise with Recurrence

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうる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。

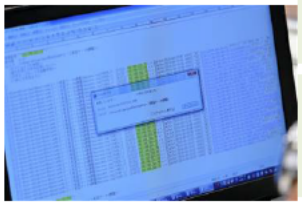
北陸StarBED技術センターの大規模高性能サーバ群を活用



擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**



演習模様 **専門指導員**による補助

チーム内での議論を通じた相互理解

本番同様のデータを使用した演習

インシデント（事案）対処能力の向上

令和３年度の実施計画

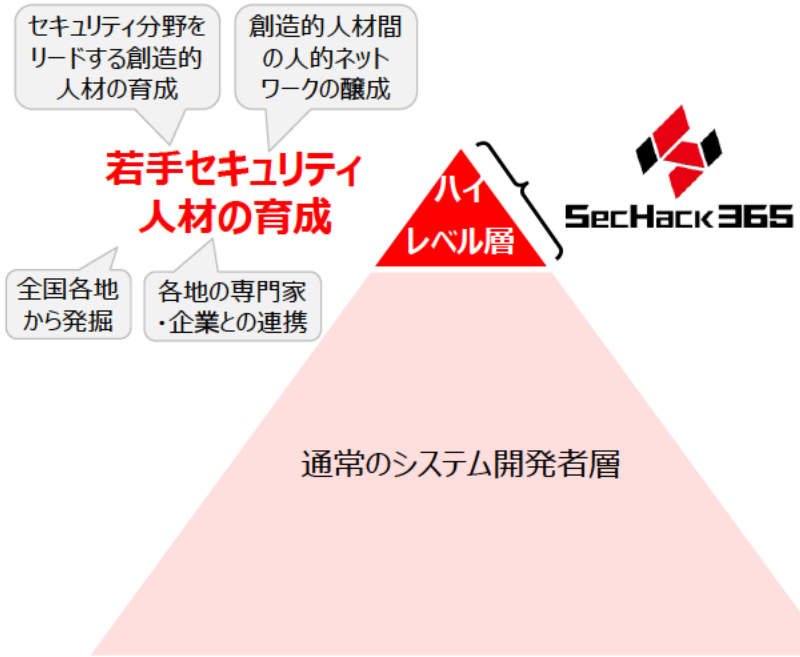
コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムに携わり始めた者（事案発生時の対応の流れ）	全組織共通	４７都道府県	６８回	７月～翌年２月
B-1		中級	システム管理者・運用者（主体的な事案対応・ｾｷｭﾘﾃｨ管理）	地方公共団体	全国１１地域	２１回	10月～翌年２月
B-2				地方公共団体以外	東京・大阪・名古屋・福岡	１３回	翌年１月～２月
C		準上級	セキュリティ専門担当者（高度なｾｷｭﾘﾃｨ技術）	全組織共通	東京	３回	翌年１月～２月
オンラインA	ｵﾝﾗｲﾝ演習	初級	システムに携わり始めた者（事案発生時の対応の流れ）	全組織共通	（受講者職場等）	随時	11月～翌年２月（6~8月に試験提供）

令和３年度から新規開設

②SecHack365

- 日本国内に居住する**25歳以下の若手ICT人材を対象**として、新たなセキュリティ対処技術を生み出しうる**最先端のセキュリティ人材（セキュリティイノベーター）**を育成。
- NICTの持つサイバーセキュリティの研究資産を活用し、実際のサイバー攻撃関連データに基づいたセキュリティ技術の研究・開発を、**第一線で活躍する研究者・技術者が１年かけて継続的かつ本格的に指導。**
  （2017年度:39名, 2018年度:46名, 2019年度:45名, 2020年度:41名, 2021年度:41名, 合計212名が修了）
- 受講者は、NICTの有する遠隔開発環境※を活用し、**年中どこからでも遠隔開発実習が可能。**また、集合イベントとして、**座学講座（研究倫理）**や**ハッカソン等**を実施。

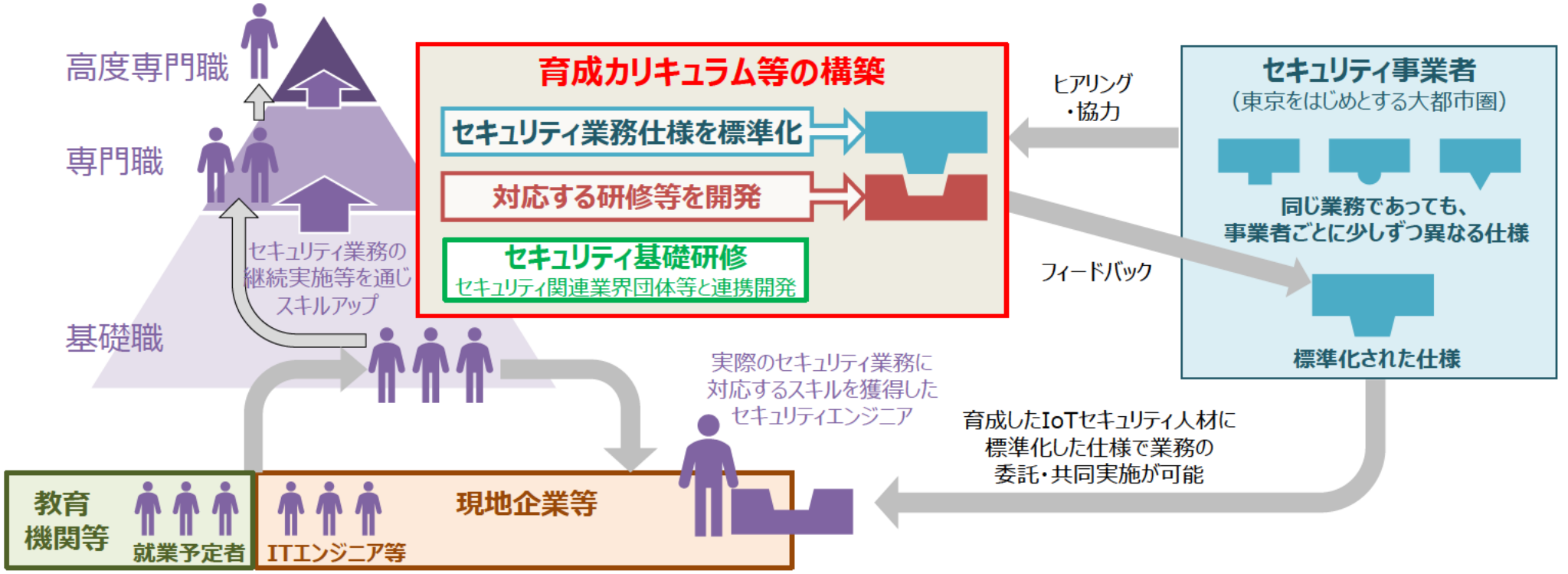
※ NONSTOP（NICTER Open Network Security Test-out Platform）では、NICTの長年にわたるサイバーセキュリティ研究によって得られた膨大なセキュリティ関連データを活用することができ、NONSTOP内に整備された様々な研究開発・解析用ツール類と、他では触れることのできない貴重なデータを用いて研究・開発に取り組むことが可能。



年６回の集合研修（座学講座等）、
成果発表会・OB交流会＋通年の遠隔開発実習
の組合せによる総合的な人材育成プログラム

2-2. セキュリティ人材の育成（地域におけるIoTセキュリティ人材の確保）

- **地域コミュニティにおいてIoTセキュリティに関して活躍可能な人材を自立的に育成するエコシステムを構築。**
  - ✓ セキュリティ事業者ごとに異なる業務仕様を、業務ごとに標準化し、対応する研修等を開発。
  - ✓ 地方を拠点に、現地のITエンジニアや若年層に集中的に研修等を提供し、業務遂行できるスキルを身につけたIoTセキュリティエンジニアを育成。
  - ✓ セキュリティ事業者は、標準化した業務仕様に基づき業務委託が可能。
- **エコシステム構築に必要となる、育成カリキュラム等の育成モデルを構築する。**



2-3. 地域に根付いたセキュリティコミュニティ（地域SECUNITY）の形成促進

➢ 総務省、経済産業省が互いに連携しつつ、地域単位の事業者のセキュリティ対策の強化のため、地域に根付いたセキュリティコミュニティ（地域SECUNITY（セキュニティ））の形成の促進を図る。

● 全国規模で事業展開する企業に比べ、地域の企業や地方公共団体などについては、有効なサイバーセキュリティ対策をとるための人材育成・普及啓発の機会や情報共有の枠組みなどが不足しているおそれ。

➡

● 地域の企業や地方公共団体については、各者とも単独で有効なサイバーセキュリティ対策をとることは困難であり、地域レベルでのコミュニティを形成して情報共有等を強化する必要がある。

地域に根付いたセキュリティコミュニティ

セキュリティ関連の情報共有

定期的なセミナーや演習等の実施

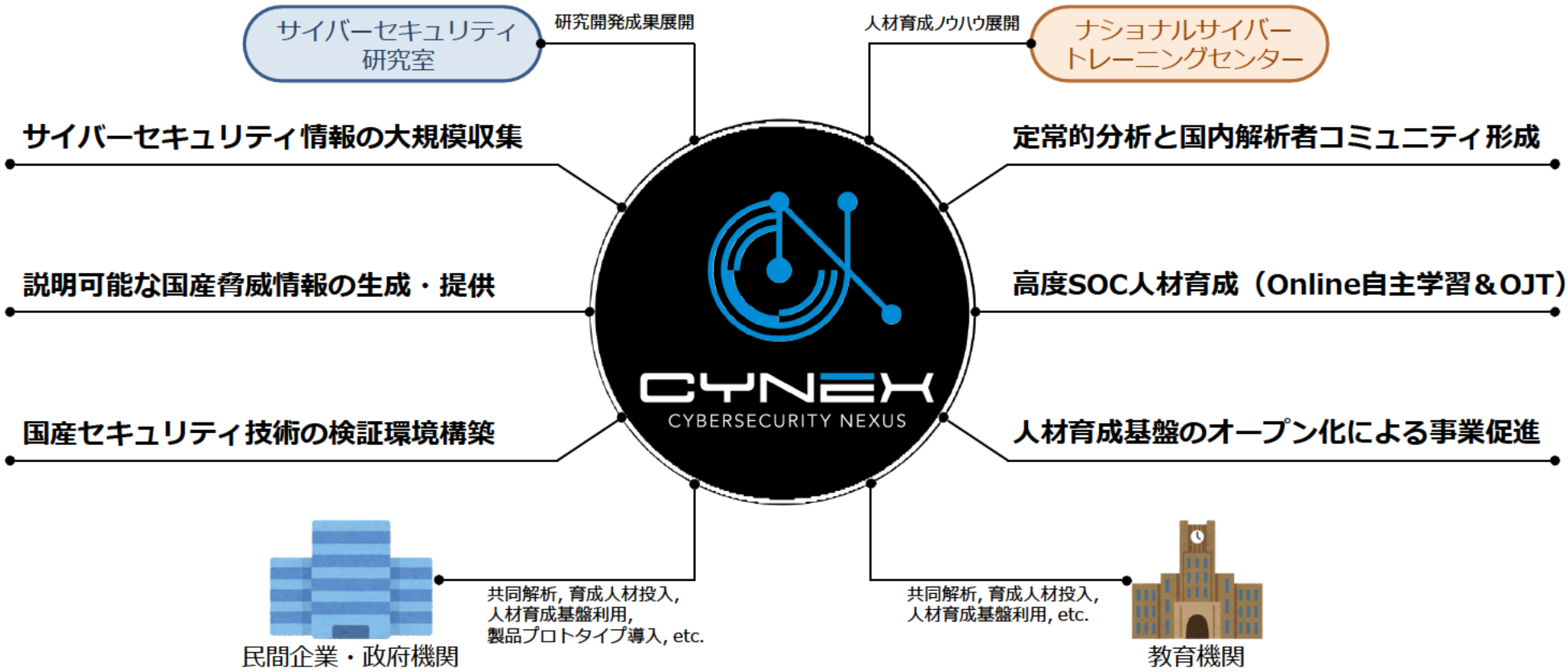
セキュリティコミュニティの形成の促進

●①当該地域における大手事業者、②業界団体（地方支部など）、③都道府県警、④サイバーセキュリティ関係事業者・機関、⑤地方公共団体、⑥有識者などによる地域のサイバーセキュリティ向上のための推進体制を構築する。なお、情報共有体制がすでに存在している地域においては、既存の体制を活用していくことが望ましい。

●地域の企業等向けに①定期的なセミナーやインシデント演習の実施、②セキュリティ関連の情報共有の枠組みなどを構築。

3. サイバーセキュリティに関する産学官の結節点『CYNEX』

➢ 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構築し、産学官の結節点として開放



3. 4つのサブチーム“Co-Nexus” によるプロジェクト推進

A **Co-Nexus A** (Accumulation & Analysis)
- ✓各種観測機構によるデータ収集・蓄積
- ✓解析者コミュニティ醸成と共同分析の実現

S **Co-Nexus S** (Security Operation & Sharing)
- ✓高度SOC人材育成（Online自主学習＆OJT）
- ✓国産脅威情報の生成・提供

E **Co-Nexus E** (Evaluation)
- ✓国産セキュリティ製品の長期運用・検証
- ✓国産セキュリティ製品へのフィードバック

C **Co-Nexus C** (CYROP*)
- ✓人材育成基盤のオープン化
- ✓パイロットコンテンツ開発

*CYROP: CYDERANGE as an Open Platform

4. サイバーセキュリティ対策の強化についての注意喚起①

➢ 昨今の情勢を踏まえ、サイバー攻撃事案のリスクは高まっていると考えられることから、総務省では、関係省庁と連携して、電気通信事業者、放送事業者及び地方公共団体等に対して、サイバーセキュリティ対策の強化について、令和４年２月23日、３月１日及び3月24日に注意喚起を実施。

・「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について」
（経済産業省、２月23日）

昨今の情勢を踏まえるとサイバー攻撃事案の潜在的なリスクは高まっていると考えられます。

各企業・団体においては、経営者のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、国外拠点等についても、国内の重要システム等へのサイバー攻撃の足掛かりになることがありますので、国内のシステム等と同様に具体的な支援・指示等によりセキュリティ対策を実施するようお願いいたします。

不審な動きを把握した場合は、早期対処のために速やかに経済産業省やセキュリティ関係機関に御相談ください。

１．リスク低減のための措置
- ○パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化する。
- ○IoT 機器を含む情報資産の保有状況を把握する。特に VPN 装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。　※下記 URL 参照
- ○メールの添付ファイルを不用意に開かない、URL を不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内に周知する。

２．インシデントの早期検知
- ○サーバ等における各種ログを確認する。
- ○通信の監視・分析やアクセスコントロールを再点検する。

３．インシデント発生時の適切な対処・回復
- ○データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。
- ○インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制等を準備する。

https://www.meti.go.jp/press/2021/02/20220221003/20220221003.html

・「サイバーセキュリティ対策の強化について」
（経済産業省、金融庁、総務省、厚生労働省、国土交通省、警察庁、内閣官房内閣サイバーセキュリティセンター、３月１日）

昨今の情勢を踏まえるとサイバー攻撃事案のリスクは高まっていると考えられます。本日、国内の自動車部品メーカーから被害にあった旨の発表がなされたところです。

政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、中小企業、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施するようお願いいたします。

さらに、国外拠点等についても、国内の重要システム等へのサイバー攻撃の足掛かりになることがありますので、国内のシステム等と同様に具体的な支援・指示等によりセキュリティ対策を実施するようお願いいたします。

実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、早期対処のために速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にもご相談ください。

１．リスク低減のための措置
- ○パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化する。
- ○IoT 機器を含む情報資産の保有状況を把握する。特に VPN 装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。
- ○メールの添付ファイルを不用意に開かない、URL を不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内に周知する。

２．インシデントの早期検知
- ○サーバ等における各種ログを確認する。
- ○通信の監視・分析やアクセスコントロールを再点検する。

３．インシデント発生時の適切な対処・回復
- ○データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。
- ○インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制等を準備する。

https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000470.html

4. サイバーセキュリティ対策の強化についての注意喚起②

「現下の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）」

（令和4年3月24日　経済産業省、総務省、警察庁、内閣官房内閣サイバーセキュリティセンター）

昨今のサイバー攻撃事案のリスクの高まりを踏まえ、政府においては、２月 23 日に「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について（別添１）」、３月１日に「サイバーセキュリティ対策の強化について（別添２）」注意喚起を行っております。

その後も、国内では、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事案の報告が続いており、また、エモテットと呼ばれるマルウェアの増加も見られるところです。また、米国では、３月 21 日に、バイデン大統領が、国内の重要インフラ事業者等に対して、ロシアが潜在的なサイバー攻撃の選択肢を模索しており警戒を呼びかける声明を発表するとともに、企業等に対してサイバーセキュリティ対策を強化する具体策を提示しています。

このような現下の情勢を踏まえ、政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、上記の２月 23 日及び３月１日の注意喚起にある対策（①リスク低減のための措置、②インシデントの早期検知、③インシデント発生時の適切な対処・回復）の徹底をあらためてお願いいたします。また、ランサムウェアやエモテットについては、これまで専門機関等において公表している情報・サイトを確認の上、対応を講じるようお願いいたします。あわせて、不審な動き等を検知した場合は、速やかに所管省庁、セキュリティ関係機関に対して情報提供いただくとともに、警察にもご相談ください。

https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000472.html

今後の主な課題等（総務省サイバーセキュリティタスクフォースにおける検討）

➢ **政府全体のサイバーセキュリティ戦略（2021年9月28日閣議決定）を踏まえつつ、総務省サイバーセキュリティタスクフォースにおいて、サイバー攻撃の複雑化・巧妙化や脆弱性の拡大などの最近の動向に対応した、課題の整理、講ずべき対策等を検討。**

【主な課題】

■ **最近のサイバー攻撃の動向等を踏まえた、情報通信ネットワークのさらなる安全性・信頼性の確保**
- 全てのインターネットユーザーのセキュリティを守るためのネットワーク環境整備
- 脆弱なIoT機器対策の更なる強化
- サプライチェーンリスク対応の重要性の高まりを踏まえた取組の検討　等

■ **我が国のサイバーセキュリティ情報の収集・分析と人材育成の向上**
- 「サイバーセキュリティ統合知的・人材育成基盤」(CYNEX)の早期の本格稼働に向けた環境整備
- 地域におけるセキュリティ人材の育成・セキュリティコミュニティの活性化　等

■ **Cybersecurity for ALLに向けた普及啓発の実施**
- 最近のフィッシングの急増等の現状を踏まえた取組
- 子ども・高齢者・中小企業等のセキュリティリテラシー向上が必要な層向けのサイバーセキュリティ普及啓発に向けた施策の検討　等

上記課題も含め、総務省サイバーセキュリティタスクフォースにおいて取組方針の策定（ICTサイバーセキュリティ総合対策2021の改定）を今夏を目途に行い、サイバーセキュリティ戦略本部で取りまとめられる次期年次計画に反映。