

各省庁における 普及啓発・人材育成に係る取組について

令和3年6月

内閣サイバーセキュリティセンター（NISC）
基本戦略第1グループ

目次

内閣官房 内閣サイバーセキュリティセンター（NISC）・・・	2
経済産業省・・・・・・・・・・・・・・・・・・・・・・・・	7
総務省・・・・・・・・・・・・・・・・・・・・・・・・	2 0
文部科学省・・・・・・・・・・・・・・・・・・・・・・・・	3 3
厚生労働省・・・・・・・・・・・・・・・・・・・・・・・・	3 8
警察庁・・・・・・・・・・・・・・・・・・・・・・・・	3 9
防衛省・・・・・・・・・・・・・・・・・・・・・・・・	4 1
内閣官房 IT総合戦略室・・・・・・・・・・・・・・・・	4 5

※資料3における施策の掲載順

1. 背景・問題認識

- サイバー攻撃が巧妙化・複雑化する中、国内ではサイバー犯罪が増加傾向にあり、また、民間ベンダの調査によれば回答企業の約8割でインシデント発生※するなど、サイバー空間における脅威は深刻な情勢。報道においても、日々、個別のインシデントが取り上げられているものの、風評被害等をおそれて、当事者からは、サイバー攻撃の実情は対外的に公表されないことが多く、サイバー攻撃を受けた際の経験が共有されがたい状況。
- 他方、我が国のサイバーセキュリティのレベルを向上させるためには、経験を共有すべきとの声も聞かれ、一部の企業からは積極的に知見の共有を図りたいとの意見も寄せられている。本年3月、NISCが主催したオンラインセミナーにおいて、サイバー攻撃を受けた企業より実体験を紹介したところ、アンケート回答者の98%が内容に満足するなど、対応事例の知見へのニーズが高いことが見て取れた。

(※) トレンドマイクロ株式会社「2020年度法人組織のセキュリティ動向調査」

2. 対応案

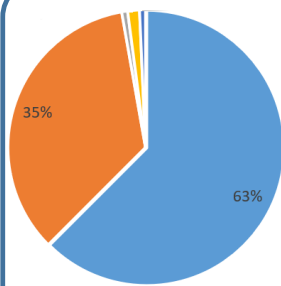
- サイバー攻撃を受けた組織からヒアリング等の協力を得た上で、サイバー攻撃を受けた際の実際の対応や、体制強化、人材確保等について調査研究を行い、様々な組織でのサイバーセキュリティ対策に役立ててもらうべく、(個社が特定されない形で) 事例集を作成・公表することを検討中。

(参考) NISC主催「戦略マネジメント層向けサイバーセキュリティセミナー」について

セミナーの概要

- ◆ 2021年3月18日(木) オンラインで開催
- ◆ プログラムの内容は以下のとおり。最後にアンケートを実施。
 - 経済産業省
「産業分野におけるサイバーセキュリティ政策」
 - NTTコミュニケーションズ(株)
「NTT Comへのサイバー攻撃が残した教訓」
 - (株) 日立製作所
「WannaCry被害の学びとサイバーレジリエンス強化への取り組み」
 - NISC
「サイバー攻撃事案からの学び」

アンケート結果概要



- セミナー内容に関して、十分満足している
- セミナー内容に関して、どちらかというと満足している

- 視聴者数232名(アンケート回答者数144名)
- セミナーに対する満足度は98%
- 意見の例(概要)
 - ・各社の生々しい実インシデントを知ることが出来たとともに、今後を見据えた対策も発表されていたので、自社へのフィードバックにしやすいと感じた。
 - ・自社の現状と照らし合わせながら、事例の教訓を社内に共有したいと思った。
 - ・他社での先行事例を詳細に示して頂けたので、当社のサイバーセキュリティ体制構築の参考になった。

- 2016年に「政府機関におけるセキュリティ・IT人材育成総合強化方針」を策定・公表し、同方針に沿った取組を推進。
- 各府省庁は、2016年度から「サイバーセキュリティ・情報化審議官」等を設置し、司令塔機能を抜本的に強化。
- 優秀な人材が、各府省庁、地方公共団体、民間企業、独立行政法人を行き来しながらキャリアを積める環境の整備が重要であることから、外部の高度専門人材を活用する仕組みの検討や、新設される国家公務員採用試験「デジタル区分」合格者の積極的な採用、デジタル化の進展を踏まえた研修の充実・強化等に向け、2021年度前半に同方針を改定する。

現行方針に基づく主な取組

1. 人材確保・育成計画の作成 【計画的な取組】

- ✓ 各府省庁は、サイバーセキュリティ・情報化審議官等の主導の下、採用・人材育成等にわたる具体的な取組方策を定めた「**セキュリティ・IT人材確保・育成計画**」を作成。
- ✓ 毎年度、見直しを実施。

2. 体制の整備 【人員の確保】

- ✓ 各府省庁は、統括部局・システム所管部局等の体制整備を図るため、政府全体の方針等に従って、**機構・定員を要求**。

3. 研修の実施 【質の維持・向上】

- ✓ 役職段階別（補佐、係長、係員）のスキルレベルのモデルを設定。これに応じた**研修**（総務省の「情報システム統一研修」）の**受講を、原則必須化**。

4. スキル認定の推進 【能力の評価】

- ✓ 一定の実務経験と研修修了を要件とする、橋渡し人材のスキル認定を行うための**全府省庁共通の基準を策定**（2018年1月）。
- ✓ 同基準に基づき、各府省庁は、手続規程を整備し、**対象職員の認定を推進**。

5. 適切な処遇の確保 【俸給の調整額】

- ✓ スキル認定された人材を専門性・特殊性の高い業務に充てる場合に、適切な処遇を確保するため、政府全体の方針等に従って、**「俸給の調整額」を要求**。

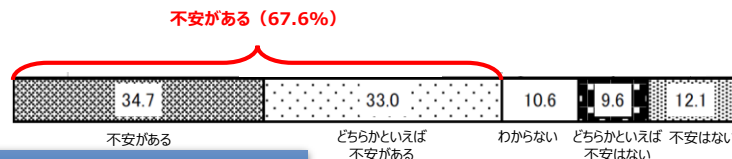
1 はじめに

「サイバーセキュリティ戦略」(2018年7月閣議決定)に基づき、普及啓発について、2020年東京オリンピック・パラリンピック競技大会を見据えつつ、産学官民の関係者が円滑かつ効果的に活動し、有機的に連携できるよう、本プログラムを策定。

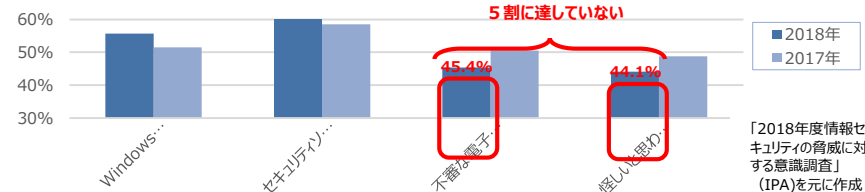
2 現状

- ①個人：**AIやIoTの「生活」への浸透**に伴い、インターネット利用への**不安感が拡大**。一方、**具体的な対策の実施に十分に結びついていない**。
- ②企業：**中小企業では、特に規模の小さい企業ほど**担当者が置かれなない場合も多いなど、**取組が遅れている**。

＜インターネットの利用に関連するトラブルへの不安感＞



＜セキュリティ対策の実施状況＞



3 今後の取組の基本的な考え方

- ・対策に関する情報が国民一人一人や中小企業に必ずしも行き届いていない、いわば「**サイバーセキュリティのラストワンマイル**」の状況。
- ・「3つの視点」から取組を推進：**①継続的な実施、②対象に合わせた適切なツール・コンテンツの提供、③関係者間の連携の促進**

4 具体的取組の推進

(1) 基本的な対策の徹底

- ・個人や企業が**取組の必要性を自覚し、当たり前のこととして取組を講じる状態**を目指し、**必要な対策を継続的に伝える**

(取組の一例)
「インターネットを安全に利用するための情報セキュリティ対策9か条」(2015年2月 NISC・IPA)の各種取組への浸透



(2) 重点的な対象とその内容

- ・様々な対象に幅広く実施することを前提としつつ、以下の対象について、**重点的に取組を実施**

- ①**中小企業** 中小企業向けガイドラインの作成・普及、「SECURITY ACTION」活用の促進、中小企業支援ネットワークによる啓発等
- ②**若年層** 無自覚なまま加害者になることを防ぐためのリテラシー向上の取組、先端的人材育成施策の推進
- ③**地域における取組の支援** 産学官連携型の取組の活性化、高専学生によるボランティア活動等



高専学生によるボランティア活動(提供: 富山県庁)

(3) 情報発信・相談窓口の充実

- ・最新の脅威の情報・対策の適時かつ迅速な発信や相談できる窓口の確保等、自ら取り組むための環境を整備

(取組の一例) NISCにおけるSNSによる情報発信



5 連携体制の強化

- ・**NISCをはじめとした関係機関が連携し、ラストワンマイルに情報が行き着くよう配慮しつつ取組を推進**
①ポータルサイトによる取組の見える化・連携推進 ②ツール・コンテンツの共有 ③サイバーセキュリティ月間の推進 ④国際的連携の強化、⑤PDCAによる継続的改善
- ・**官民の様々な取組を集約するポータルサイトを構築し、対象となる層や伝達手法の見える化及び連携を推進**
- ・個別施策の実施状況に加え、**個人や企業の対策の実施状況等**を分析し、本プログラムの**内容・効果の定期的な評価、見直しを実施**

⇒ 取組状況をフォローアップし、継続的な改善に取り組む。また、高齢者への対応を含め、見直しを検討する。 5

「サイバーセキュリティ月間」の取組

- 2010年より、毎年2月1日から3月18日を「サイバーセキュリティ月間」に設定。各種啓発主体と連携し、インターネットを介してサイバーセキュリティに関する普及啓発活動を集中的に実施。
- 2021年は、感染症の状況を踏まえ、**SNSや動画配信を用いたオンラインでの周知広報を積極的に実施し、地域を問わず幅広い層に訴求。**
- また、サイバーセキュリティに関する**意識や行動の強化**に繋げるべく、1人1人が気を付けてほしいことを国民の皆様によりわかりやすくまとめた**9つの標語**をもとにして、**様々なコンテンツを用いて発信。**

認知度の高いコンテンツとのタイアップ

- ・『ラブライブ！サンシャイン!!』とタイアップし、様々なコンテンツを用いて発信。
- ◆**全体ポスター**：キャッチコピー「みんなで叶えるセキュリティ！」を訴求
- ◆**標語ポスター**：9人の主要キャラクターが9つの標語を各々担当し発信
- ◆**パンフレット**：4コマ漫画で身近な事例を扱い、9つの標語を紹介
- ◆他、**イベント動画**（右下の欄を参照）・**短編アニメ**をインターネットで配信
また、**Webラジオ**でも発信
- ・インターネット上での**アンケート結果**（任意回答：1,241件）
 - －月間を機会に意識や行動が強化された人：回答者中の**約95%**
例：同じパスワードを使い回していたが、パターンを変えた。/メールのURLを開かず、検索エンジンから開くようにした。
 - －月間を機会に身の回りの人にサイバーセキュリティの重要性などを伝えた人：回答者中の**約66%**
例：ファイルやリンクをすぐに開かないよう家族や友人に周知した。/子供にSNSを使用する際の注意喚起をした。



標語ポスター
(例 パスワード関係、二要素認証関係)

9つのセキュリティの標語

- 1 パスワードは長くて複雑にしよう
- 2 二要素認証を導入しよう
- 3 ウイルス対策ソフトを導入して、常に最新に（アップデート）しておこう
- 4 ファイルやリンクはすぐには開かない
- 5 フィッシングサイトに注意しよう
- 6 個人情報をもやみに発信しない
- 7 情報の真偽はきちんと確認しよう
- 8 相手を傷つけるような発信はしない
- 9 「心の隙」を作らないようにしよう

情報発信の強化

- ・月間の開始にあわせて、**加藤官房長官によるトップメッセージ**を発信。
- ・NISC Webサイトで、11名の有識者によるコラム「**サイバーセキュリティ ひとつ言いたい！**」を発信。
- ・「**インターネットの安全・安心ハンドブック**」をパンフレットとともに全国の公立図書館に配布。
- ・各種啓発主体の実施する行事を、**サイバーセキュリティ月間関連行事**と位置付けて募集し、NISCのWebサイトやSNSで案内を実施。
→ オンライン開催を中心に**127件**を実施



官房長官トップメッセージ

NISC主催のイベント・行事の開催

- ・**NISC-CTF (2/17)** (CTF: Capture The Flag、セキュリティ技術の競技)
各府省庁・独法等の職員がサイバーセキュリティに関する幅広い技術・能力を競うオンライン競技会を開催。
- ・**オンライン普及啓発イベント動画 (2/21、28、3/6)**
楽しみながらサイバーセキュリティを学べる動画を配信。
→一時、約4,000人が同時視聴し、Twitterトレンド入り。
- ・**戦略マネジメント層向けWebセミナー (3/18)**
サイバー攻撃の被害を受けた企業から被害経験を通じて得られた気づき等を講演。参加者232名。



NISC-CTF表彰式の様子



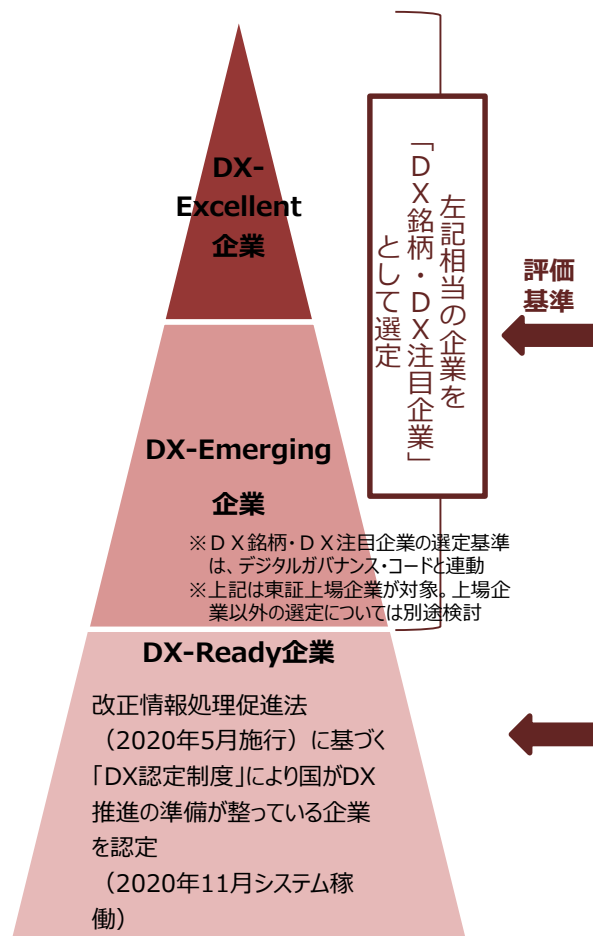
普及啓発イベント動画の様子
(コンテンツの声優らによるセキュリティ講座)

DX with Cybersecurity経営の推進：経営層によるリスク把握・企業情報開示

- デジタル化の進展等に伴い、DX(デジタルトランスフォーメーション)とサイバーセキュリティ対策の不可分性が増す中で、DX銘柄選定等によるインセンティブづけの下、「可視化ツール」の活用を通じた経営層による自社リスクの可視化/把握を推進するとともに、企業情報開示のプラクティスを普及させる。

DX経営の推進

◆DX企業の体系



※「DX認定」は、「DX投資促進税制」の要件の一つとなっている。

◆デジタルガバナンス・コード(2020年11月策定)

経営者が企業価値向上に向け実践すべき事項

1. 経営ビジョン・ビジネスモデル
2. 戦略
3. 成果と重要な成果指標
4. ガバナンスシステム (セキュリティ)

望ましい方向性に係る取組例より：

○経営者がサイバーセキュリティリスクを経営リスクの1つとして認識し、CISO等の責任者を任命するなど管理体制を構築するとともに、サイバーセキュリティ対策のためのリソース(予算、人材)を確保。

○情報処理安全確保支援士(登録セキスペ)の取得を会社として奨励。

○サイバーセキュリティを経営リスクの一つと捉え、その取組を前提としたリスクの性質・度合いに応じて、サイバーセキュリティ報告書、CSR報告書、サステナビリティレポートや有価証券報告書等への記載を通じて、開示を行っている。

認定基準：

○戦略の実施の前提となるサイバーセキュリティ対策を推進していること。

※サイバーセキュリティ経営ガイドライン等に基づき対策を行い、セキュリティ監査(内部監査を含む)を行っていることの説明文書等が提出されることをもって確認する。

※中小企業においては、SECURITY ACTION制度に基づき自己宣言(二つ星)を行っていることを確認する方法でも可とする。

評価
基準

サイバーセキュリティ経営の推進

1st Step サイバーセキュリティ経営の明確化

➢「サイバーセキュリティ経営ガイドライン」(2017年10月Ver2.0)の普及・定着【累計10万DL】

2nd Step サイバーセキュリティ経営の定着

➢「プラクティス集」(2020年6月第2版)「体制構築・人材確保の手引き」(2021年4月第1.1版)の整備により、サイバーセキュリティ経営を現場レベルで推進

3rd Step セキュリティの高い企業であることの可視化

➢「可視化ツール」の普及によるサイバーセキュリティ経営の可視化の推進

活用
推奨

活用
推奨

◆Web版「可視化ツール」※

※経営ガイドライン実践状況の可視化ツールV1.0(2021年夏頃リリース予定。Excel形式のβ版公開中)

→①経営層による自社リスクの可視化/把握
②ステークホルダー(取引先、投資家、損保会社)とのコミュニケーションに活用



中小企業のセキュリティ対策

● 中小企業の情報セキュリティ対策ガイドライン（第3版 2019年3月）

- － 中小企業が情報セキュリティ対策に取り組む際の経営者が認識し実施すべき指針、社内において対策を実践する際の手順や手法をまとめたもの。
- － 第3版より、付録6として、クラウドサービスを安全に利用するための留意事項やチェック項目を記載した手引きを追加。

中小企業の情報セキュリティ対策ガイドライン



**経営者向けの
解説**

経営者が認識すべき3原則と実施すべき重要7項目を解説

**実践者向けの
解説**

企業のレベルに合わせて段階的にステップアップできるような構成で解説

付録6:クラウドサービス安全利用の手引き



- 【クラウドサービス導入時の考慮ポイントの例】**
- ✓ クラウドで扱う情報と業務の重要性（情報漏洩、改ざん、サービス停止した際の影響等）
 - ✓ 自社・事業者間でのセキュリティルール・水準の整合性（データアップデート時の暗号化やパスワード強度の警告等）
 - ✓ 利用者の範囲、権限の管理（利用目的に合わせ利用者、権限を設定等）
 - ✓ クラウド事業者・サービスの安全・信頼性（セキュリティ対策の開示状況等）

● 「SECURITY ACTION」

- － 中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度（IPA）。
- － IT導入補助金の申請において、「SECURITY ACTION」の宣言を必須要件化したことにより、宣言数が大幅に増加。
- － 11万者を超える中小企業が宣言（2021年2月末時点）



情報セキュリティ
5か条に取り組む



情報セキュリティ自
社診断を実施し、基
本方針を策定

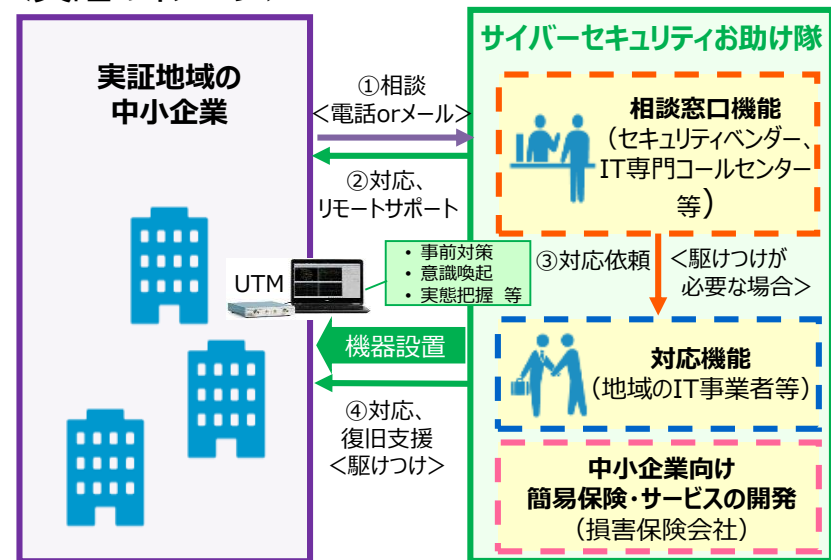
サイバーセキュリティお助け隊実証事業(2019・2020年度)

- 地域の団体、セキュリティ企業、保険会社がコンソーシアムを組み、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした実証事業を実施（2019年度：全国で8件、2020年度：全国で15件）。のべ2,181社の中小企業が参加。
- 2年間にわたる実証事業を通して、サイバーセキュリティに関する中小企業の実態を把握。2021年度より簡易サイバー保険を含むサイバーセキュリティお助け隊の民間自走化を促進すべく、お助け隊サービス基準を策定し、同基準を満たすサービスの審査登録制度の運営を開始。

<2020年度の実証地域>



<実証のイメージ>



実証結果

中小企業 側

- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上 等

保険会社、セキュリティベンダー 側

- 中小企業のセキュリティ対策状況の把握
- 中小企業の被害実態の把握
- 中小企業が求めるサービスの把握 等

※2019年度実証地域（全8地域、1064社の中小企業が参加）：

①宮城、岩手、福島②新潟③長野、群馬、栃木、茨城、埼玉④神奈川⑤石川、富山、福井⑥愛知⑦大阪、京都、兵庫⑧広島、山口

サイバーセキュリティお助け隊ブランドの使用開始

- 実証事業で得られた知見に基づき、中小企業向けのセキュリティサービス（お助け隊サービス）が満たすべき基準を整理、パブコメを経て2月末にIPAより公開。
- 2021年3月に第1回審査を行い、4月15日にお助け隊マークが付与された民間サービスが「サイバーセキュリティお助け隊サービス※」として登録され、市場に展開。

※中小企業のサイバーセキュリティ対策支援サービスに不可欠な各種サービス内容（相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など）の基準を満たした民間による支援サービス事業

<https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html>



2019年度
(実証1年目)

2020年度
(実証2年目)

2021年度以降
(民間で自走)

攻撃実態の
把握

ニーズを踏まえた
サービスのスリム化

地域特性・産業特性
の考慮

実証事業：
中小企業が利用しやすい安価なセキュリティサービスの開発

意識啓発

事前対策とのセット
によるリスク低減

導入・運用負荷を
下げる方法の検討

お助け隊サービス審査登録制度：
一定の基準を満たすサービスにお助け隊の商標利用権を付与。

お助け隊サービスA
お助け隊サービスB
お助け隊サービスC

サービス
提供

中小企業

自社の信頼性を
アピール

取引先
(大企業等)

お助け隊サービス利用の推奨等の
中小企業の取組支援

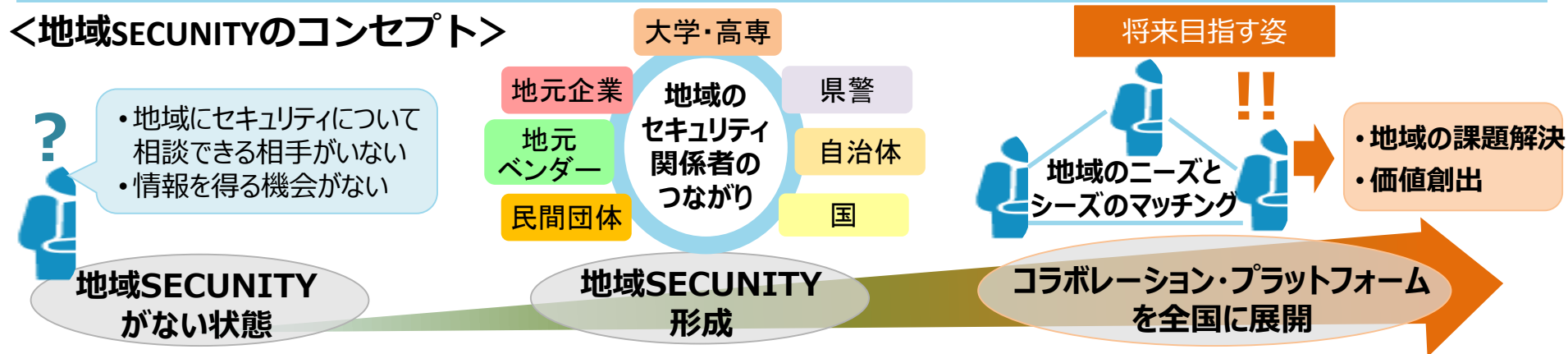
SC3(サプライチェーン・サイ
バーセキュリティ・コンソーシアム)

→SC3（業種別業界団体が参加）で利用推奨を行うことで、より多くの中小企業がお助け隊サービスを活用し、万が一の際に早急に正しい対処が行える状態を目指す。

地域に根付いたセキュリティ・コミュニティ（地域SECURITY）の形成促進

- 地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ活動を、「地域SECURITY」と命名。
- まずは各地域で経済産業局や総合通信局を中心に地域SECURITYの形成を促進し、将来的には、地域のニーズとシーズのマッチングによる課題解決・付加価値創出の場（コラボレーション・プラットフォーム）へと発展することを目指す。

<地域SECURITYのコンセプト>



（取組例）中国地域サイバーセキュリティ連絡会

事務局：中国総合通信局、中国経済産業局

参加機関：中国地域5県、2政令市、通信・放送事業者、金融機関、業界団体、産業支援機関、大学等）76機関



地域SECURITY形成のためのプラクティス集

各地域におけるセキュリティ・コミュニティの形成を促進するため、モデルとなるようなコミュニティへのヒアリングを実施し、プラクティスとして公開。

<https://www.meti.go.jp/press/2020/02/20210217001/20210217001.html>



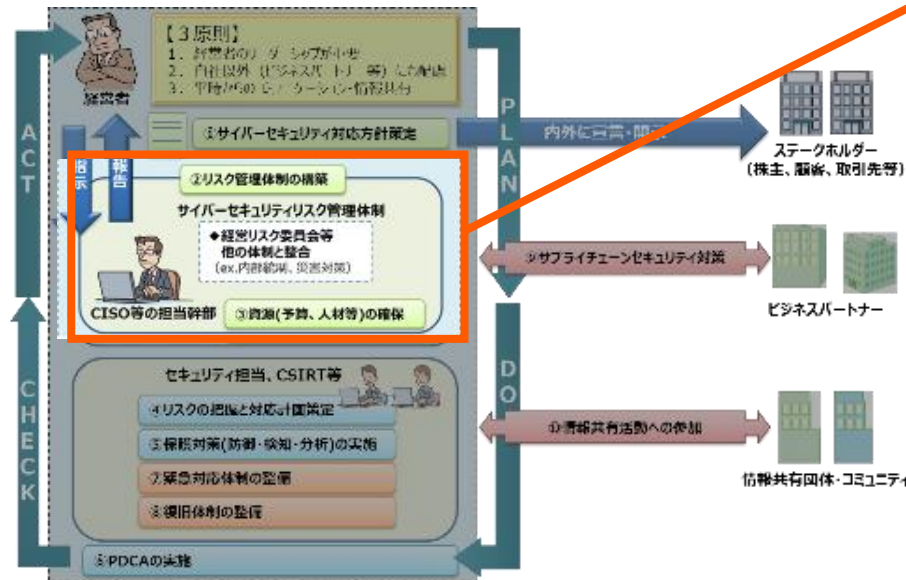
『セキュリティ体制構築・人材確保の手引き』の開発

累計**5,158**ダウンロード
(2021年3月末時点)

- サイバーセキュリティ経営ガイドラインの付録Fとして**2020年9月30日に第1版を公表**。
今後の課題としていた箇所を更新した**第1.1版を2021年4月15日に公表**。

サイバーセキュリティ経営ガイドライン（10の指示）

手引きの構成（指示2、3の深掘り）



指示2 サイバーセキュリティ リスク管理体制 の構築

- 2.1 経営者のリーダーシップの下でのセキュリティ体制の検討
- 2.2 セキュリティ統括機能の検討
- 2.3 セキュリティ関連タスクを担う部門・関係会社の特定・責任明確化

指示3 サイバーセキュリティ 対策のための 資源確保

- 3.1 セキュリティ人材の確保
- 3.2 プラス・セキュリティ人材の確保
- 3.3 教育プログラム・試験・資格等の活用と人材育成計画の検討

第1.1版での更新ポイント（例）：

- サイバーセキュリティ対策に従事する人材の確保
- ユーザー企業で必要となるスキルの習得に活用可能な資格制度
- ユーザー企業でサイバーセキュリティ対策に従事する人材の育成パスのイメージ

(参考)『セキュリティ体制構築・人材確保の手引き』で扱う主要な概念の解説

セキュリティ統括機能

- セキュリティ対策及びインシデント対応において、CISOや経営層を補佐してセキュリティ対策を組織横断的に統括することにより、企業におけるリスクマネジメント活動の一部を担う
- 「機能」であって「組織」として設置しなくてもよい（状況に応じて、最適な形態は異なる）
 - 独立した組織として設置
 - 管理部門の1機能として割当
 - 情シス部門の1機能として割当
 - 組織横断的な委員会形態で運用

ITSS+（セキュリティ領域）

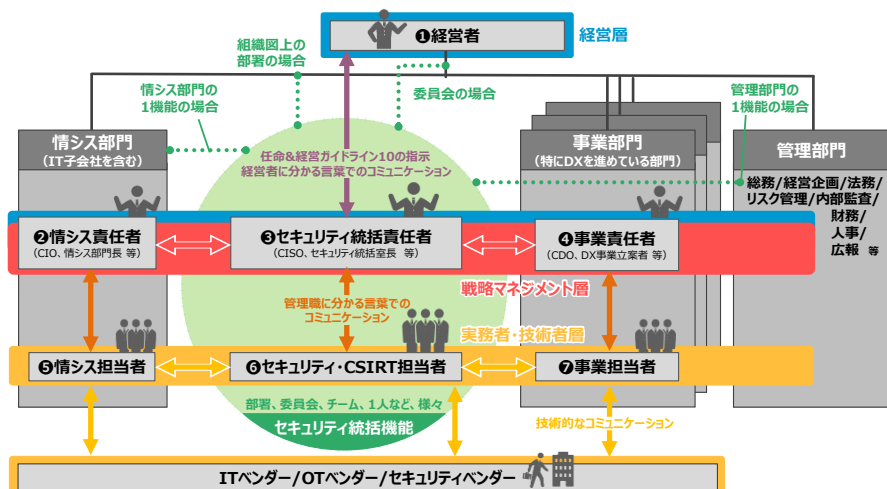
- 企業のセキュリティ対策に必要な関連業務のまとまりを17分野に整理したもの
- セキュリティの専門性の高い分野だけでなく、経営層や法務部門、事業ドメインまで、サイバーセキュリティ対策に関わる幅広い領域を網羅
- DXの取り組みを通じたクラウド化、アジャイル開発、開発・セキュリティ対策・運用の一体化（DevSecOps）等の動きの中、ITSS+で定める各分野の境界は曖昧化の傾向

プラス・セキュリティ

- セキュリティ対策を本務としないが、業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策の実践が求められる業務が「プラス・セキュリティ」の対象
- 「プラス・セキュリティ」人材が業務担当者として別に存在するわけではなく、これまでの業務担当者がサイバーセキュリティの知識・スキルを習得し、実践することを通じて対策を担う

セキュリティ統括機能のイメージ

企業の組織構造や事業内容に応じて下図の緑色部分の実現方法の検討が必要



ITSS+（セキュリティ領域）（赤枠が「プラス・セキュリティ」の分野）

	経営層		戦略マネジメント層			実務者・技術者層					
						設計・開発・テスト		運用・保守		研究開発	
ユーザ企業における組織の例	取締役会 執行役員会議		内部監査部門 (外部監査を含む)		管理部門 (総務、法務、広報、 調達、人事 等)	セキュリティ 統括室	経営企画部門 事業部門	デジタル部門/事業部門 (ベンダーへの外注を含む)			
セキュリティ関連タスクの例	・セキュリティ意識 啓発 ・対策方針指示 ・ポリシー・予算、 実施事項承認		・システム監査 ・セキュリティ監査		・BCP対応 ・官公庁等対応 ・法令遵守対応 ・記者・広報対応 ・調達・契約・検収 ・施設管理・物理 セキュリティ ・内部犯行対策	・リスクアセスメント ・ポリシー・ガイド ライン策定・管理 ・セキュリティ教育 ・社内相談対応 ・インシデントハン dling	・事業戦略立案 システム企画 ・要件定義・仕様 書作成 ・プロジェクトマネ ジメント	・セキュアシステム 要件定義 ・セキュアアーキテ クチャ設計 ・セキュアソフト ウェア方式設計 ・テスト計画	・構成管理 ・運用設定 ・脆弱性対応 ・セキュリティツ ールの導入・運用 ・監視・検知・対応 ・インシデントレ スポンス ・ペネトレーション テスト	・現場教育・管理 ・設備管理・保全 ・初期対応・原因 究明・フォレンジ ック ・マルウェア解析 ・脅威、脆弱性情 報の収集・分析・ 活用	・セキュリティ理論 研究 ・セキュリティ技術 開発
セキュリティを推進する組織のあり方	デジタル (IT/IoT/OT)	デジタル経営 (CIO/CDO)	システム監査	事業戦略策定において サイバーセキュリティ リスクを 織り込んだ立案ができる			デジタル システム ストラテジー	Security by designを自力でできる			セキュリティに配慮した 監視・保守等ができる
	セキュリティ	セキュリティ経営 (CISO)	セキュリティ 監査				セキュリティ統括	システム アーキテクチャ	デジタル プロダクト 開発	デジタル プロダクト 運用	
	その他	企業経営 (取締役)	担当業務において サイバーセキュリ ティリスクを他リス クと同様に捉える	経営リスク マネジメント	法務	事業ドメイン (戦略・企画・調達)	脆弱性診断・ ペネトレーションテスト	セキュリティ 監視・運用	セキュリティ 調査分析・研究開発	セキュリティ 調査分析・研究開発	事業遂行において、他部署やベンダーと 連携してセキュリティ対策を行える

産業サイバーセキュリティセンター（ICSCoE）（2017年4月設置）

- 世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ1年程度のトレーニング等を実施。
- 第4期中核人材育成プログラム（2020年7月開講）には、47名が参加。

□ 1年を通じた集中トレーニング

- 電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：47人）

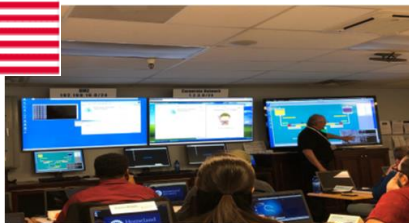
中核人材育成プログラム- 年間スケジュール											
7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月
プライマリー (レベル合わせ)			ベーシック (基礎演習)			アドバンス (上級演習)			卒業 プロジェクト		
ビジネス・マネジメント・倫理											
プロフェッショナルネットワーク (含む海外)											
開講式											修了式

- IT系・制御系に精通した専門人材の育成
- 模擬プラントを用いた対策立案
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析

現場を指揮・指導する
リーダーを育成



□ 米・英・仏等の海外とも協調したトレーニングを実施



- DHSが開催する高度なサイバーセキュリティトレーニングである301演習への参加



- 政府機関、自動車業界、スタートアップ企業の代表者等からの講義や意見交換を実施



- 政府機関、産業界等のセキュリティ専門家との意見交換や研究機関の施設見学等を実施

など

中核人材育成プログラムの成果と修了者の活動

中核人材育成プログラム受講者は、1年間のプログラムで学んだ技術や人脈を業界の課題に当てはめていくことを主眼に、プログラムの最後にチーム別の**卒業プロジェクト**に取り組む。業界のあるべき姿と現状のギャップを分析し、成果を公表。また、修了者の知見をアップデートし、また、その知見やノウハウを産業界や社会へ還元していくため、**業種横断の修了者コミュニティ「叶会」**で**情報共有システムを運用**、経済産業省や情報処理推進機構の取組に貢献。

最近の卒業プロジェクトの成果物

➤ 制御システムにおける資産管理ガイドライン（2020年6月）

資産管理はセキュリティ対策の土台であると考え、制御システム向けの資産管理ガイドライン、自動化ツール、製品検証結果をまとめた成果物を作成。

➤ 「経営者のキモチ」冊子（2020年6月）

経営者のサイバーセキュリティに対する考え（キモチ）をできるだけ短く簡潔に、かつ網羅的に集約。また、経営者へのセキュリティ提言時に注意すべきアドバイスも記載。

➤ CSIRTカードゲーム制作（2020年6月）

CSIRTの初期教育現場で共通の課題を解決すべく、CSIRT教育のはじめの一歩として「短時間（30分程度）」で「参加者同士が楽しく」、「CSIRT業務に特化」して学べる3種類のカードゲームを制作。

修了者コミュニティ 叶会

【目的】

- 卒業後も知見をアップデート
- 卒業年次・業種を超えた人脈形成
- 修了者の知見の社会還元



【主な活動】

- 年1回年次総会（今年度は11月5日に開催）で最新動向と修了者の近況の活躍を発表
- サイバーセキュリティ情報提供活動
→情報共有ツール「SIGNAL」を使い、ICSCoEが入手した脆弱性情報等を修了者に提供
- 東京以外の地域（関西・中京等）でも修了者がコミュニティを形成、各地でセミナー等を開催、またセキュリティ対応等のノウハウをシェア

●修了者の技術や知見の活用：「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」作成への貢献

中核人材育成プログラムでビルが直面するセキュリティの課題と解決手法を学んだ受講者が、有志で経済産業省のビルSWGに参加。カリキュラムのアウトプットとして、経済産業省が2019年6月にリリースした「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」をより分かりやすく理解できる“解説書”を作成するとともに、ビル関係者向けの脆弱性情報やその解説の配信にも協力。

サイバーセキュリティ経営を進める戦略マネジメント層の育成

- 経営層が示す戦略の下、事業継続と価値創出に係るリスクマネジメントを中心となって支える立場である「戦略マネジメント層」の育成が急務。以下の取組を推進中。
 - － サイバーセキュリティ2020に基づき、IPA産業サイバーセキュリティセンターでは、2019年度に引き続き2020年度も戦略マネジメント層向けのセミナーを実施。
 - － 東京工業大学CUMOTは「サイバーセキュリティ経営戦略コース」を開催。

産業サイバーセキュリティセンター 「戦略マネジメント系セミナー」



- ・ 2021年2月実施（2018年度から3回目）
- ・ サイバーセキュリティは経営課題であること及び経営層をはじめ関係者が認知すべきセキュリティ機能の重要性の理解を目指す。
- ・ 2020年度はオンライン（オンデマンド形式）で開講。講演・パネルディスカッション・講義（約10時間分収録）により、先進事例・課題や解決策・ノウハウなどを体系的に学ぶプログラムを提供。



東京工業大学CUMOT 「サイバーセキュリティ経営戦略コース」



- ・ 2021年2月～6月
※新型コロナウイルス感染症対策で原則オンライン開催。
- ・ サイバーセキュリティ経営及びその戦略立案に求められる知識・能力を備え、企業・組織を先導する人材の育成を目的とする。
- ・ 座学だけでなく、受講生同士による議論やグループ課題によって理解を深める実践的なスタイルの講義を1回2時間、全20回実施。



国立高専機構と産・官との連携促進・具体化に向けて

- 国立高専におけるセキュリティ教育が産業界の求める人材像とも整合していくためには、産学官の継続的な協力関係が必要。
- これまで国立高専機構がIPAや業界団体（CRIC CSF、JNSA）等と進めてきた連携を効果的かつ継続的なものとするために、SC3の場の活用も含め、産学官連携を推進していく。

<高専・産・官の対話の場（イメージ）>



サプライチェーンセキュリティ確保のための産業界一丸となった対応 ～サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）～

- **趣 旨:** 大企業と中小企業がともにサイバーセキュリティ対策を推進するためのコンソーシアムを立ち上げ、「基本行動指針※」の実践と中小企業・地域を含めたサプライチェーンのサイバーセキュリティ対策を産業界全体の活動として展開していく。
※サイバー攻撃事案発生時における、「共有、報告、公表」によるリスクマネジメントの徹底。
- **参加者:** 経済団体、業種別業界団体 等（2021年4月末時点で171会員）
- **設立日:** 2020年11月1日（設立総会：2020年11月19日）
- **活 動:** 特定の課題についてWGを設置し、具体的アクションを展開。

Supply-Chain Cybersecurity Consortium (SC3)

事務局：IPA

総会

年1回程度開催（WG報告、重要事項の決定等）

運営委員会

会 長：経団連 サイバーセキュリティ委員長 遠藤信博氏
副会長：日本商工会議所 特別顧問 金子眞吾氏
経済同友会 副代表幹事 間下直晃氏

中小企業
対策強化WG

地域SECURITY
形成促進WG（案）

産学官連携
WG（案）

.....

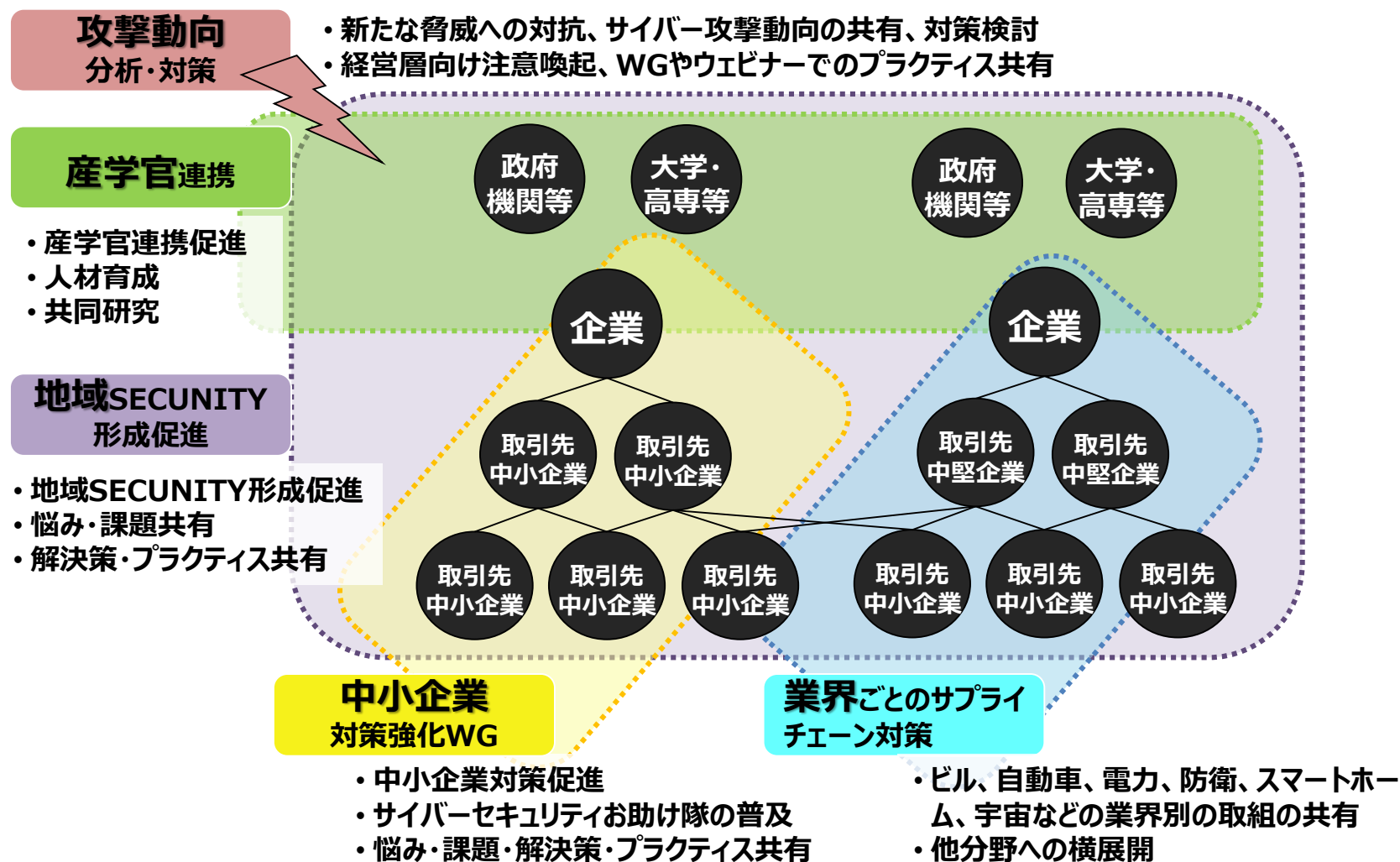
参加団体例：日本自動車工業会、電気事業連合会
全国地方銀行協会、日本損害保険協会ほか

メンバーの意向を踏まえて特定課題を扱うWGを設置

**基本行動指針
（共有・報告・公表）
へのコミットメント**

サプライチェーンセキュリティ確保のための産業界一丸となった対応 ～Supply-Chain Cybersecurity Consortium (SC3) の今後の活動方針

- 産業界全体で取り組むべきサプライチェーンセキュリティ対策の浸透のため、産学官連携や経営層の啓発、地域・業界別の取組等を加速するプラットフォームとしての機能に期待。



- 民間企業のサイバーセキュリティ対策の情報開示の促進のため、民間企業にとって参考となり得る情報開示の事例等をまとめた手引きを策定し、令和元年6月に公表。
- 今後、情報開示をステークホルダーに伝達する主体を含めた産業界全体における情報開示の取組を促進。
→(一社)日本IT団体連盟「サイバーセキュリティに関する企業公開情報の調査」(令和2年11月)において活用

背景

- ✓ サイバー攻撃が深刻化する中、民間企業においてサイバーセキュリティ対策は重要な経営課題となっているが、企業としての社会的責任を果たしステークホルダーからの信頼を得るためには、サイバーセキュリティ対策の実施のみならず、その内容について適切な情報開示が重要。

目的

- ✓ 民間企業によるサイバーセキュリティ対策やその対策の情報開示の重要性の認識を促進。
- ✓ 民間企業にとって参考になり得るような既存の情報開示の実例を事例集として示す。

活用主体

- ✓ サイバーセキュリティ対策の情報開示に一定の関心のある民間企業の開示の実務担当者等を想定。

対象とする情報開示

- ✓ 開示書類を通じた情報開示を取り扱う。
- ✓ 開示書類の読み手は、投資家、融資元、顧客・契約者・取引先、従業員、競合他社等を含む、社会全体の広範なステークホルダーを想定。

本編 サイバーセキュリティ対策情報開示の手引き

1. 本手引きの趣旨・目的

- ✓ サイバーセキュリティリスクの増大と対策の必要性
- ✓ サイバーセキュリティ対策の情報開示の意義
- ✓ 本手引きの目的、想定参照主体、及び内容・構成等

2. 情報開示の手段

- ✓ 代表的な開示書類の紹介

3. 企業における情報開示の在り方

- ✓ 企業において実施されるのが望ましいサイバーセキュリティ対策
- ✓ 開示にあたってのポイントと記載例

4. 今後の方向性について

- ✓ 手引きの改定の在り方等の今後の方向性

参考資料① 関連施策等の紹介

- ✓ 本手引きに関連した様々な施策やガイドライン等について紹介

参考資料② 開示書類の事例集

- ✓ 情報開示にかかる実際の開示書類の例について紹介

地域に根付いたセキュリティコミュニティの形成促進

総②

※経⑤と連携

- 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の形成の促進を図る。総務省においては、総合通信局等（全11管区）の内、令和元年度は3地域、令和2年度は5地域で実施し、令和3年度はより多くの地域で実施予定。

- 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。

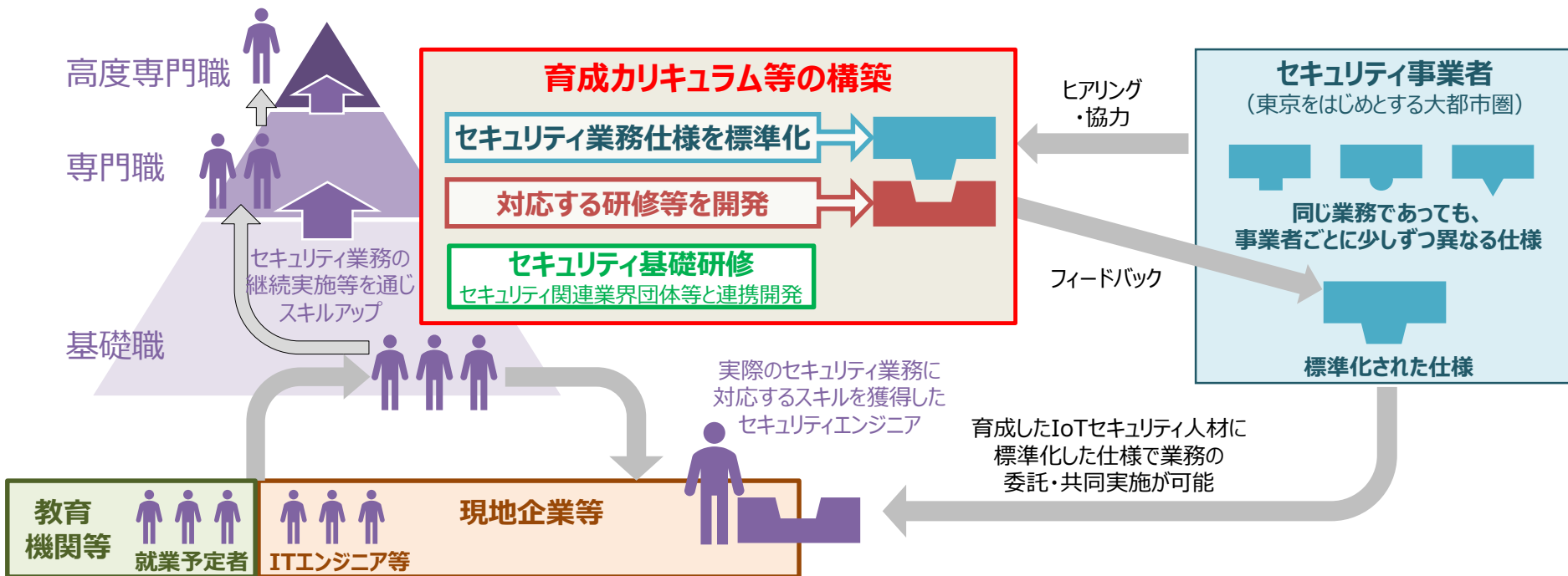
地域に根付いたセキュリティコミュニティ



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。

- 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。



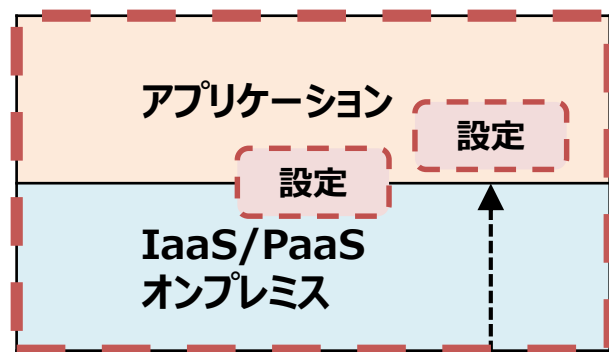
クラウドサービスの設定ミスの防止・軽減に向けた取組の検討

総④

➤ クラウドサービス利用時の設定ミスの防止・軽減のため、以下の取組を検討中。

- ① サービス利用者としてのクラウドサービス事業者（CSP）における対策（セキュリティベンダによるアセスメントの利用等）を促す取組
- ② サービス提供者としてのクラウドサービス事業者（CSP）における、サービス利用者に対するサポート（情報提供やツール提供等）を促す取組

【サービス利用者としてのCSP】

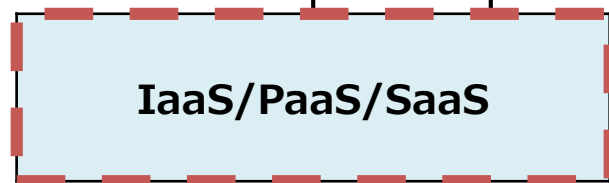


利用

エンドユーザ

① サービス利用者としてのクラウドサービス事業者における対策（セキュリティベンダによるアセスメントの利用等）を促す取組

【サービス提供者としてのCSP】



② サービス提供者としてのクラウドサービス事業者における、サービス利用者に対するサポート（情報提供やツール提供等）を促す取組

※サービス利用者としてのCSP：他のクラウドサービスを基盤として利用する等し、エンドユーザに対してクラウドサービスを提供するCSP
サービス提供者としてのCSP：他のCSPやエンドユーザに対してクラウドサービスを提供するCSP

実践的サイバー防御演習 (CYDER)

総⑤

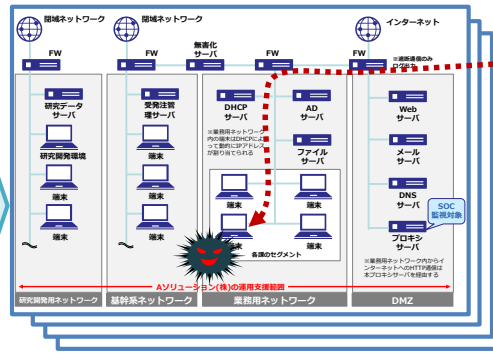
CYDER: CYber Defense Exercise with Recurrence

- 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

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



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	65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	2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月に試験提供予定)

令和3年度から新規開設

CYDER開催スケジュール（令和3年度）

Aコース（初級）（全組織共通）

地域	開催県	開催日	
北海道	北海道	10/14 札幌	11/05 釧路
	青森県	9/22 青森	
東北	岩手県	9/14 盛岡	
	宮城県	8/17 仙台	10/26 仙台
	秋田県	10/22 秋田	
	山形県	10/01 山形	
	福島県	10/08 郡山	
関東	茨城県	10/19 水戸	
	栃木県	9/17 宇都宮	
	群馬県	7/27 前橋	
	埼玉県	8/20 さいたま	
	千葉県	9/14 習志野	
	東京都	7/20 東京	9/22 東京
		10/13 東京	10/21 東京
		11/10 東京	12/09 東京
		1/21 東京	2/16 東京
	神奈川県	10/05 横浜	1/28 横浜
信越	山梨県	9/07 甲府	
	新潟県	9/17 新潟	
北陸	長野県	8/24 松本	11/12 佐久
	富山県	11/19 富山	
東海	石川県	8/31 金沢	
	福井県	11/09 福井	
	岐阜県	10/15 岐阜	
	静岡県	11/17 静岡	
	愛知県	7/30 名古屋	10/29 名古屋
	三重県	12/03 名古屋	
		8/05 津	

オンラインAコース（初級）（全組織共通）

オンラインにより受講可能なコースを2021(令和3)年秋から開始予定
※試験的なオープンβ版を6月中旬から実施予定

B-1コース（中級）（地公体向け）

開催地域	開催日	
北海道	11/25 札幌	
東北	11/25 仙台	12/22 盛岡
関東	10/14 東京	11/11 東京
	1/14 東京	2/17 東京
信越	12/24 新潟	
北陸	11/30 金沢	
東海	10/19 名古屋	1/25 名古屋
近畿	10/26 大阪	11/16 大阪
	12/21 大阪	2/04 大阪
中国	1/19 岡山	2/09 広島
四国	2/15 松山	
九州	12/14 熊本	2/15 福岡
沖縄	2/04 那覇	

B-2コース（中級）（国・重要インフラ）

開催地域	開催日	
関東	1/13 東京	1/20 東京
	1/26 東京	1/28 東京
	2/01 東京	2/03 東京
	2/08 東京	2/10 東京
	2/18 東京	2/25 東京
東海	2/01 名古屋	
近畿	1/21 大阪	
九州	2/10 福岡	

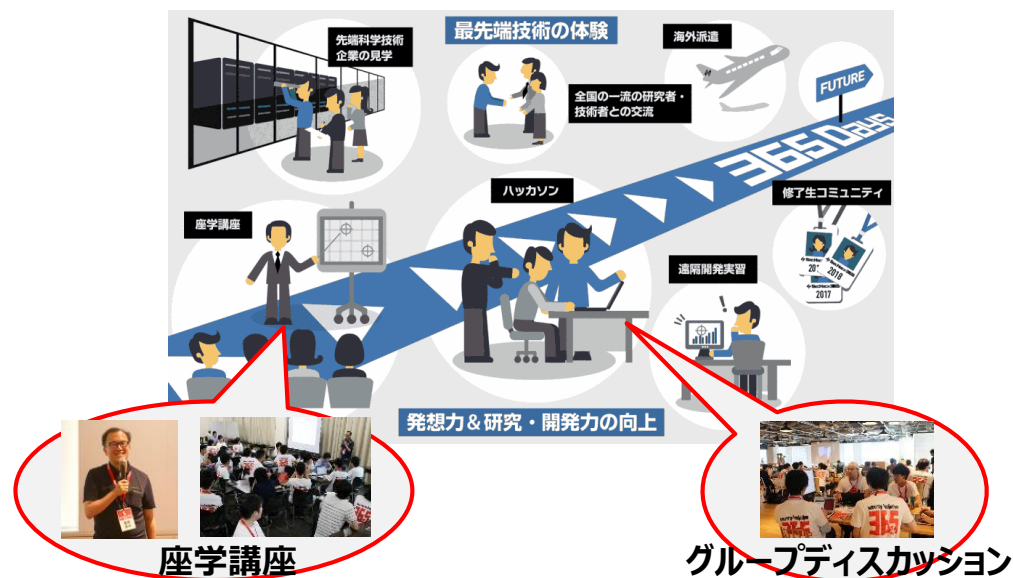
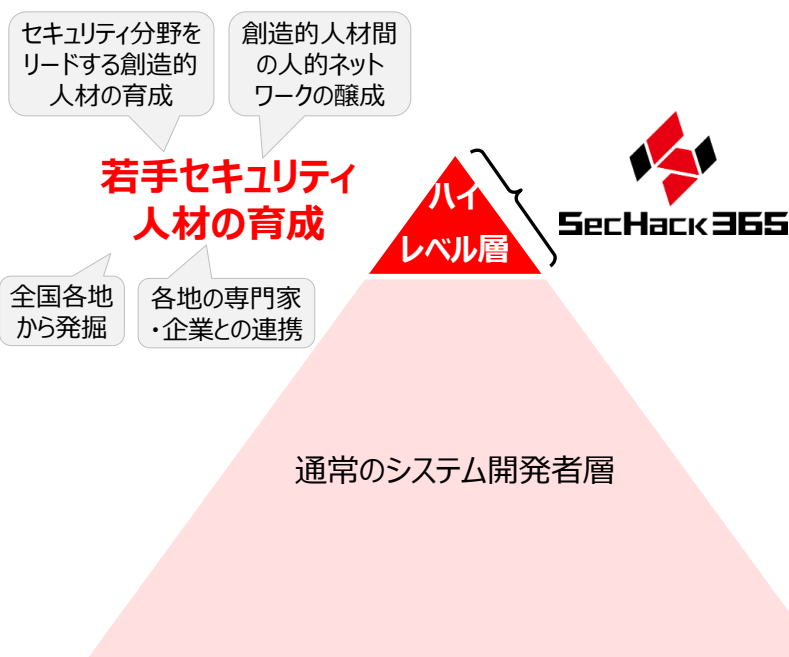
Cコース（準上級）（全組織共通）

開催地域	開催日	
関東	1/18 ~19	2/21 ~22 東京

- 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さう**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、合計171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。

毎年4月頃に受講者を募集
詳細は「**SecHack365**」で検索

※ 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。

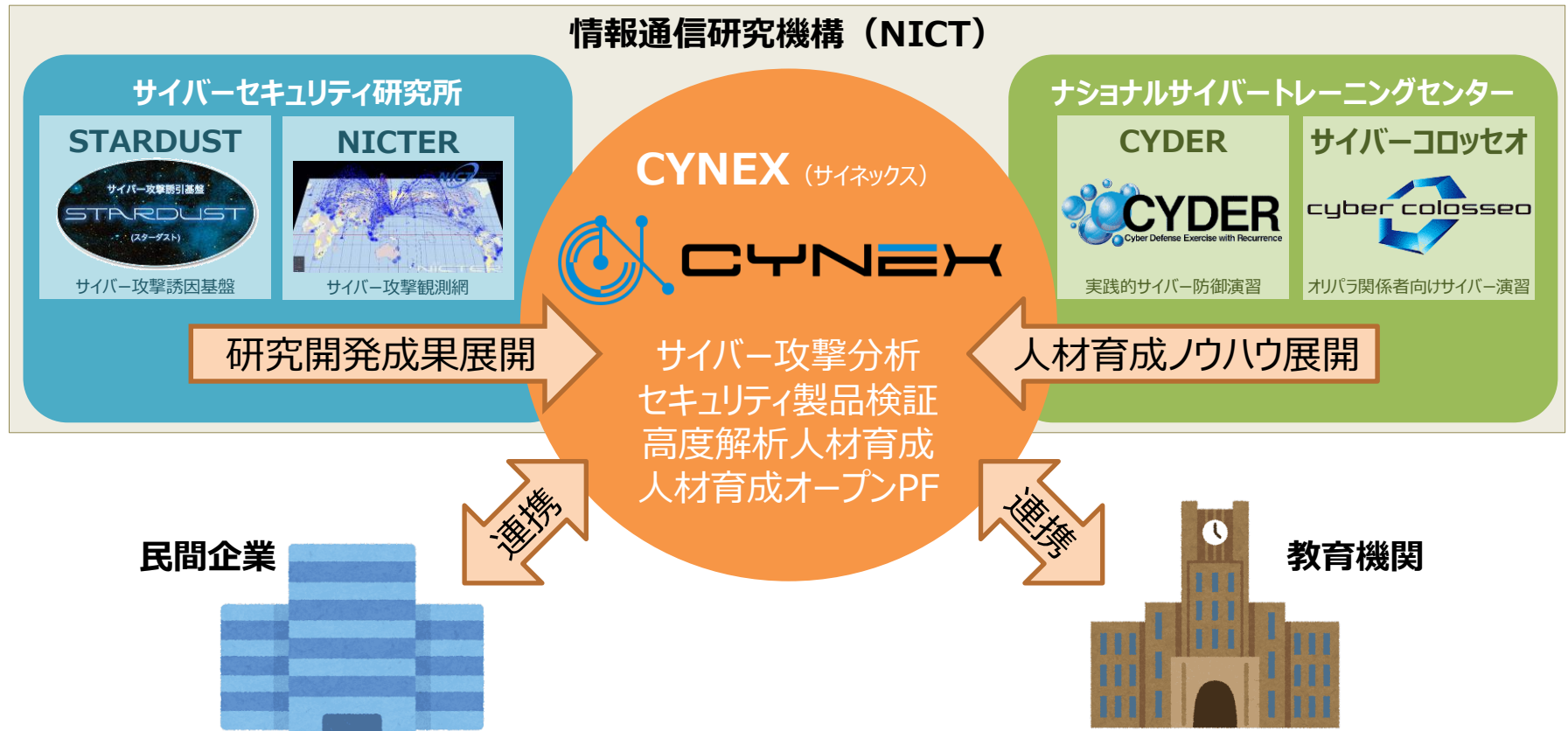


年6回の集合研修（座学講座等）、
成果発表会・OB交流会＋通年の遠隔開発実習
の組合せによる総合的な人材育成プログラム

サイバーセキュリティに関する産学官の結節点『CYNEX』

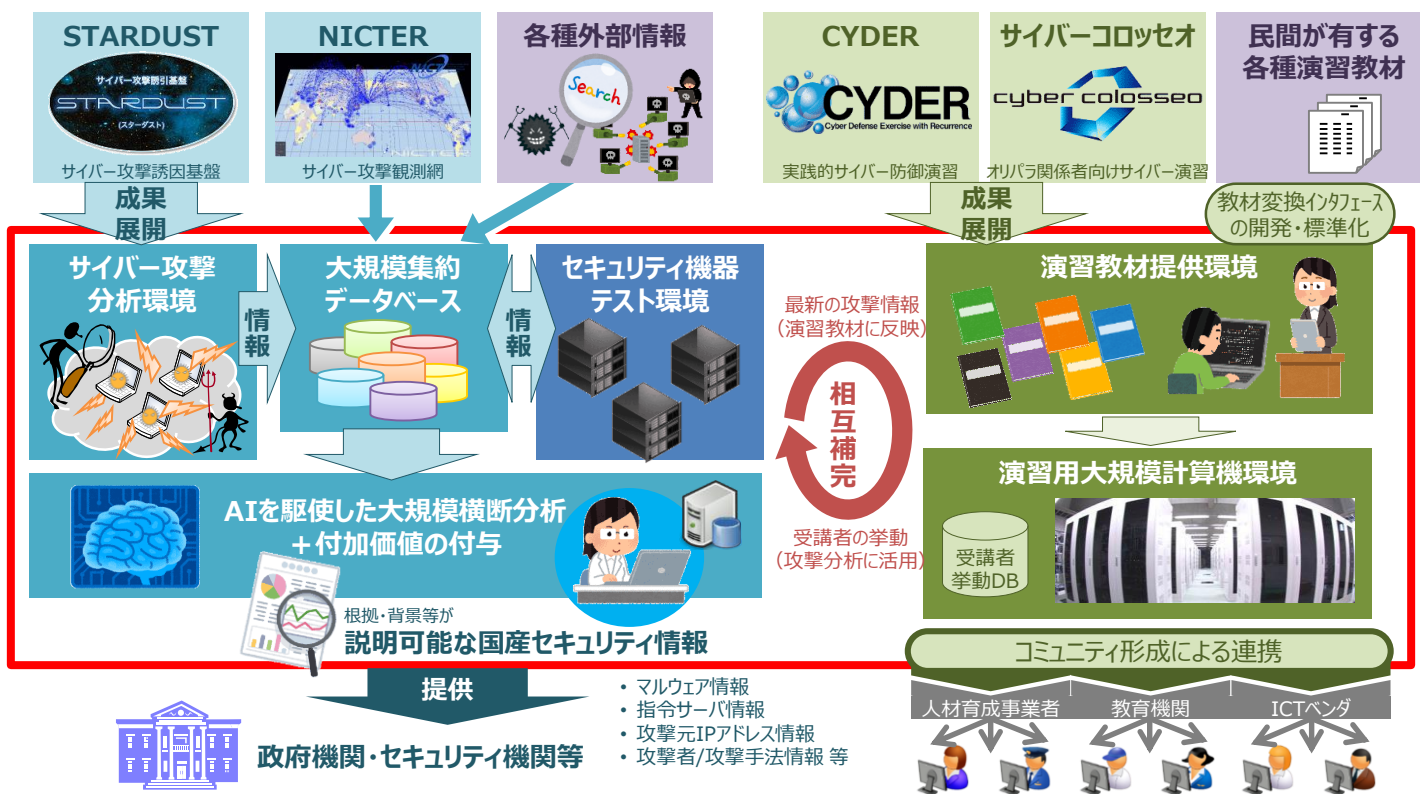
総⑦

- 情報通信研究機構（NICT）では、これまでも次のような取組を実施
 - サイバーセキュリティ研究所・・・最先端のサイバーセキュリティ関連技術の研究開発を実施
 - ナショナルサイバートレーニングセンター・・・実践的サイバー防御演習等による人材育成を実施
- これらの知見を活用し、サイバーセキュリティに関する産学官の巨大な結節点となる先端的基盤として
CYNEX（CYbersecurity NEXus：サイネックス） を構築



サイバーセキュリティ統合知的・人材育成基盤（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NICTに構築し、産学の結節点として開放することで、サイバーセキュリティ対応能力の向上を図る。



次のとおり活用可能な基盤をNICTに構築。

➤ 国産セキュリティ情報の収集・蓄積・分析・提供

幅広くサイバーセキュリティ情報を収集・蓄積し、AIを駆使して横断的に分析することで、高信頼で即時的なセキュリティ情報を生成し、政府・セキュリティ機関等に提供。

➤ セキュリティ機器テスト環境

セキュリティ製品・サービスの開発を推進するため、最新のサイバー攻撃情報を活用し、その対応状況をセキュリティ事業者がテストできる環境を提供。

➤ 高度解析人材の育成

収集したセキュリティ情報を活用し高度なサイバー攻撃を迅速に検知・分析できる卓越した人材を育成。

➤ 人材育成のための基盤提供

NICTが有する人材育成に関する環境・知見を民間・教育機関等に開放し、自立的な人材育成を推進。



- 総務省では従来から「**テレワークセキュリティガイドライン**」を策定し、セキュリティ対策の考え方を示してきた。
→ テレワークを取り巻く環境やセキュリティ動向の変化に対応するため**2021年5月**に**全面的に改定**
- ガイドラインを補完するものとして、セキュリティの専任担当がいらないような中小企業等においても、テレワークを実施する際に**最低限のセキュリティを確実に確保**してもらうための**チェックリスト**についても策定。

公表URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

テレワークセキュリティガイドライン (2021年5月 第5版)

2004年12月初版
2006年4月第2版
2013年3月第3版
2018年4月第4版



- ✓ テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針
- ✓ 中小企業を含む全企業を対象
- ✓ システム管理者のほか経営層や利用者(勤務者)を幅広く対象

ガイドラインに記載の内容について、理解や検討が難しい場合

中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト) (2021年5月 第2版) 2020年9月初版

中小企業等に向け**最低限のセキュリティを確実に確保**してもらうためのものに限定

【想定読者像】

- ✓ システム管理担当者向け
- ✓ 専任の担当・部門は存在しない
- ✓ 基本IT用語は聞いたことがあるレベル
- ✓ 設定作業は検索しながら実施可能



テレワークで活用される代表的なソフトについて、**設定解説資料**を作成し、具体的な設定を解説

【設定解説資料の対象】

CiscoWebexMeetings / Microsoft Teams / Zoom / Windows / Mac / iOS / Android / LanScope An / Exchange Online / Gmail / Teams_chat / LINE / OneDrive / Googleドライブ / Dropbox / YAMAHA VPNルータ / CiscoASA / Windowsリモートデスクトップ接続 / Chromeリモートデスクトップ / Microsoft Defender / ウイルスバスター ビジネスセキュリティサービス

テレワークセキュリティガイドラインの改定 (2021年5月)

【テレワーク環境・セキュリティ動向の変化】

- ✓ テレワークは「一部の従業員」が利用するものから、Web会議を含め、一般的な業務・勤務形態に進むなど、システム構成や利用形態が多様化
- ✓ クラウドサービスの普及やスマートフォン等の活用が進むなど、システム構成や利用形態が多様化
- ✓ 標的型攻撃等の高度な攻撃が増え、従来型のセキュリティ対策では十分対応できない状況も発生

【ガイドライン改定の主要なポイント】

- ✓ **テレワーク方式を再整理**し、適した方式を選定するフローチャートや特性比較を掲載
- ✓ クラウドやゼロトラスト等のセキュリティ上のトピックについても記載
- ✓ 経営者・システム管理者・勤務者の立場それぞれにおける役割を明確化
- ✓ 実施すべきセキュリティ**対策の分類や内容を全面的に見直し**
- ✓ テレワークセキュリティに関連する**トラブルについて、具体的事例を含め全面見直し**(事例紹介のほか、セキュリティ上留意すべき点や、採るべき対策についても明示)

テレワークセキュリティに関する周知啓発

▶ テレワークセキュリティに関する各種取組について、周知啓発を実施。

- ✓ 総務省広報誌に掲載（2020年11月号）
- ✓ 専門紙6紙＋専門雑誌12誌に掲載（2020年11月～翌年1月）
- ✓ インターネット検索サイト（Yahoo）に掲載（テキスト：2020年10月27日～翌年3月12日、バナー：2020年11月9日～12月8日）
- ✓ 二次実態調査（3万社対象）の調査票郵送時にリーフレットを同封（2020年12月発送）
- ✓ テレワークサポートネットワークが開催するセミナーでリーフレットを配布（2020年8月～）

専門紙・専門雑誌周知内容

テレワークを安心して利用するために 無料で相談できる窓口を開設しました。

総務省では、企業・団体・自治体などの皆さまのテレワーク推進をサポートする事業として「テレワークのセキュリティ あんしん無料相談窓口」を開設しました。

テレワーク導入でお悩みはありませんか？

テレワークを導入したけど
セキュリティ的に大丈夫かしら？



情報漏えいが心配だけど
何をすればいいの？

テレワークセキュリティに関する不安、対策方法、ルール作りなど、
信頼できるセキュリティの専門家が

皆さんのお悩みを無料で解決します！

④ テレワークのセキュリティあんしん無料相談窓口

テレワークセキュリティの『ガイドライン』と『チェックリスト』を公表しています。



テレワークを安心して導入するための
『セキュリティガイドライン』
テレワーク導入にあたってのセキュリティ対策に
ついての考え方や対策例を示しています。

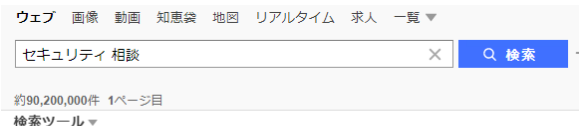


最低限のセキュリティを確保する
テレワーク『チェックリスト』
中小企業等でテレワークを実施する際に、最低限の
セキュリティを確保するためのチェックリストです。

総務省 テレワークにおけるセキュリティ確保へ▶

総務省 テレワーク セキュリティ 検索

Yahoo（テキスト）掲載内容



[【総務省】無料相談 | テレワークのセキュリティ | 安全な...](#)

[\(広告\) www.soumu.go.jp/総務省/テレワーク](#)

テレワーク導入・利用時のセキュリティについて無料で相談を受け付けています。（総務省事業）専門家がアドバイスをいたします。少しでも気になることがあれば、まずは一度ご相談ください。無料で相談いただけます。安心安全なテレワーク・専門家がアドバイス・テレワーク推進をサポート・セキュリティの不安を払拭・セキュリティ相談の専門家・サービス：総務省事業、オンライン相談、お悩み相談、専門家による情報提供。
先月のsoumu.go.jpの閲覧回数：10万回以上

※「テレワーク」「リモートワーク」「テレワーク セキュリティ」「セキュリティ 相談」等のキーワードで検索した際に表示(10,000クリック)

Yahoo（バナー）掲載内容

**『テレワークのセキュリティ
あんしん無料相談窓口』を開設**



**セキュリティの専門家が
テレワークに関する
お悩みを
無料で解決します。**

総務省

※「テレワーク」と検索した際に常に表示(1ヶ月間)

- 総務省では、無線LANの利用者・提供者向けにガイドラインを作成しており、周知啓発に活用。
- 新技術や最新のセキュリティ動向に対応するため、内容を見直し2020年5月に改定版を公表。
- 改定版については、Wi-Fi提供者（医療機関、宿泊施設、教育機関等を含む）等に幅広く周知。
https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

「Wi-Fi利用者向け 簡易マニュアル」のポイント

- ✓ セキュリティ対策の訴求点を明確にするため、**セキュリティ対策のポイントを整理**
 - ① **接続するアクセスポイントをよく確認**（偽アクセスポイント対策として接続URL等を確認）
 - ② **正しいURLでHTTPS通信をしているか確認**（Wi-Fi暗号化等に関わらず通信内容を保護）
 - ③ **自宅に設置している機器の設定を確認**（管理用パスワードの変更やファームウェアアップデート等）
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を紹介



「Wi-Fi提供者向け セキュリティ対策の手引き」のポイント

- ✓ ガイドラインの対象者の明確化（**自店利用者のみへ提供する者も対象**）
- ✓ 近年懸念されている**偽アクセスポイント対策**（認証画面のURLの周知等）を追記
- ✓ 暗号化のための**パスフレーズを公開している場合**解読の**リスクが高まる**ことを明示
- ✓ 状況に応じたセキュリティ対策の選択と**利用者への周知が必要**であることを明確化
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を紹介



無線LAN（Wi-Fi）の利用に関する周知啓発

- 総務省では、無線LANの利用者のセキュリティ対策に関する周知啓発を継続的に実施。
- 令和2年度も、**オンライン動画講座**を開講するとともに、**ショートムービー**を作成し**SNS**を通じて周知。

オンライン動画講座

- ✓ 無線LAN利用時のリスクや、適切なセキュリティ対策を**有識者が動画**（全11回）により説明
- ✓ オンライン講座プラットフォーム「gacco」にて配信
<https://gacco.org/wifi-security/>
- ✓ 2021年2月12日～3月24日に開講し、
3,161名が受講（前年度は3,164名：2020.2.10～3.23）

SNSを用いた周知啓発

- ✓ 無線LANのセキュリティ周知啓発に関し、
20秒程度の動画コンテンツを配信（全5種）
- ✓ SNSを通じて配信するとともに、動画クリック時に
上記オンライン動画講座にリンクすることにより誘導
（Instagram、Facebook、YouTube）
- ✓ 2021年2月12日～3月23日に
配信し、216万インプレッション
（3.3万クリック）
※前年度は102万インプレッション
（1.3万クリック）（2020.3.2～3.22）



第1回：もっとつながる・使える公衆無線LAN＜Wi-Fiの技術＞

第2回：とっても危険！「野良Wi-Fi」

第3回：そのWi-Fi、本物ですか？

第4回：さまざまな公衆無線LANサービスを知ろう

第5回：Wi-Fiの接続と暗号化の仕組み

第6回：安全なWeb利用の方法

第7回：自分で重要な通信内容を守る

第8回：より安全・安心にWi-Fiを使うために

第9回：Wi-Fi規格の最新動向

第10回：無線LAN利用時に注意すべき3つのポイント

（令和2年度新規→無線LANの利用者向けガイドラインをベースにした動画講座）

第11回：提供者視点からみた無線LANセキュリティ

（令和2年度新規→無線LANの提供者向けガイドラインをベースにした動画講座）

＜動画例：知らない接続先を使わない＞



Society 5.0に対応した高度技術人材育成事業

成長分野を支える情報技術人材の育成拠点の形成(enPiT)

enpit

令和3年度予算額 110百万円

背景

- サイバーセキュリティ、IoT、ビッグデータ、人工知能、組み込みシステムなど、情報技術を高度に活用して、社会の具体的な課題を解決することのできる人材の育成は急務であり、我が国の極めて重要な課題
- 今後のIT需要の拡大にもかかわらず、労働人口の減少から、**IT人材不足が今後一層深刻化する可能性が高い**

例えば、東京オリンピック・パラリンピック競技大会を成功に導くためにもセキュリティ技術者等の高度のIT技術者の育成は不可欠
Society5.0を実現するためには、ビッグデータ、人工知能等の情報技術の利活用が重要な鍵を握る
また、長期的視点からも、学部教育でのアクティブラーニングの推進や、大学における社会人学び直し機能の強化は喫緊の課題

高等教育機関の役割

- 学生に対する実践的教育の推進**：大学教育改革により、質の高い情報技術人材を多く輩出すること
- 社会人学び直しの推進**：個々の情報技術人材の生産性を高めるための学び直しに貢献すること

改革の
好循環

<産業界に期待する役割(例)>

- ✓ 産業の魅力向上(処遇・キャリア)
- ✓ 流動性向上により高付加価値領域への人材配置
- ✓ 高い競争力の実現→企業収益の確保→優秀な情報技術者に対する高い処遇という好循環の実現

第四次産業革命や
働き方改革に貢献

enPiTの概要

Education Network for Practical Information Technologies (エンピット)

産学連携による課題解決型学習(PBL)等の実践的な教育の推進により、大学における情報技術人材の育成機能強化を目指す取組

① 学生に対する実践的教育の推進

大学院生に対する第1期enPiT

平成24～28年度(5年間)
15大学連携による取組

学部生に対する第2期enPiT

平成28～令和2年度(5年間)
34大学+αの連携による取組連携
協力

- 大学間連携により、PBL中心の実践的な情報教育を行う
- 教育ネットワークを構築し、開発した教育方法や知見を広く全国に普及させる
- 産業界と強力な連携体制を構築する

② 社会人学び直しの推進

社会で活躍するIT技術者の学び直しを推進するenPiT-Pro

複数大学協働(36大学)+産業界(平成29～令和3年度[5年間])



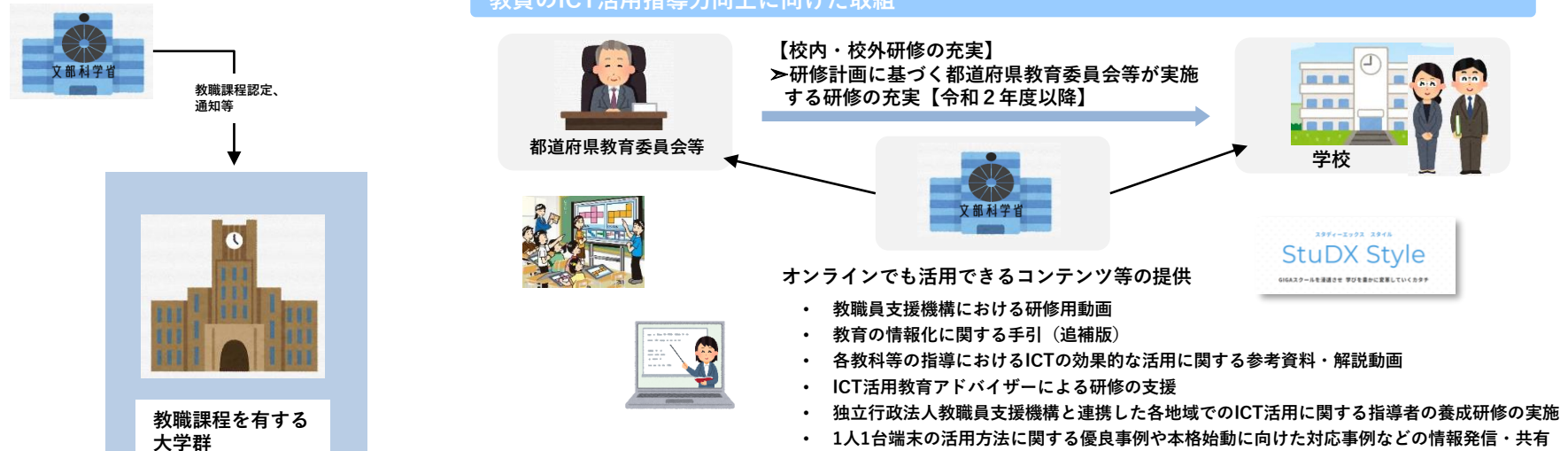
- 大学が有する最新の研究の知見に基づき、情報科学分野を中心とする高度な教育(演習・理論等)を提供する
- 拠点大学を中心とした産学教育ネットワーク構築し、**短期の実践的な学び直しプログラムを開発・実施**する

1人1台環境における教員のICT活用指導力の向上及び指導体制の充実を図るために、教員養成段階において教員志望者が身に付けるべき資質・能力の修得を狙うとともに、研修段階においてもオンラインでも活用できるコンテンツ等を活用した指導力向上を図ることに加え、指導体制を充実させるためにICT支援員の配置の促進やICT活用教育アドバイザーによる支援等を行う。

教員養成

現職教員

教員のICT活用指導力向上に向けた取組



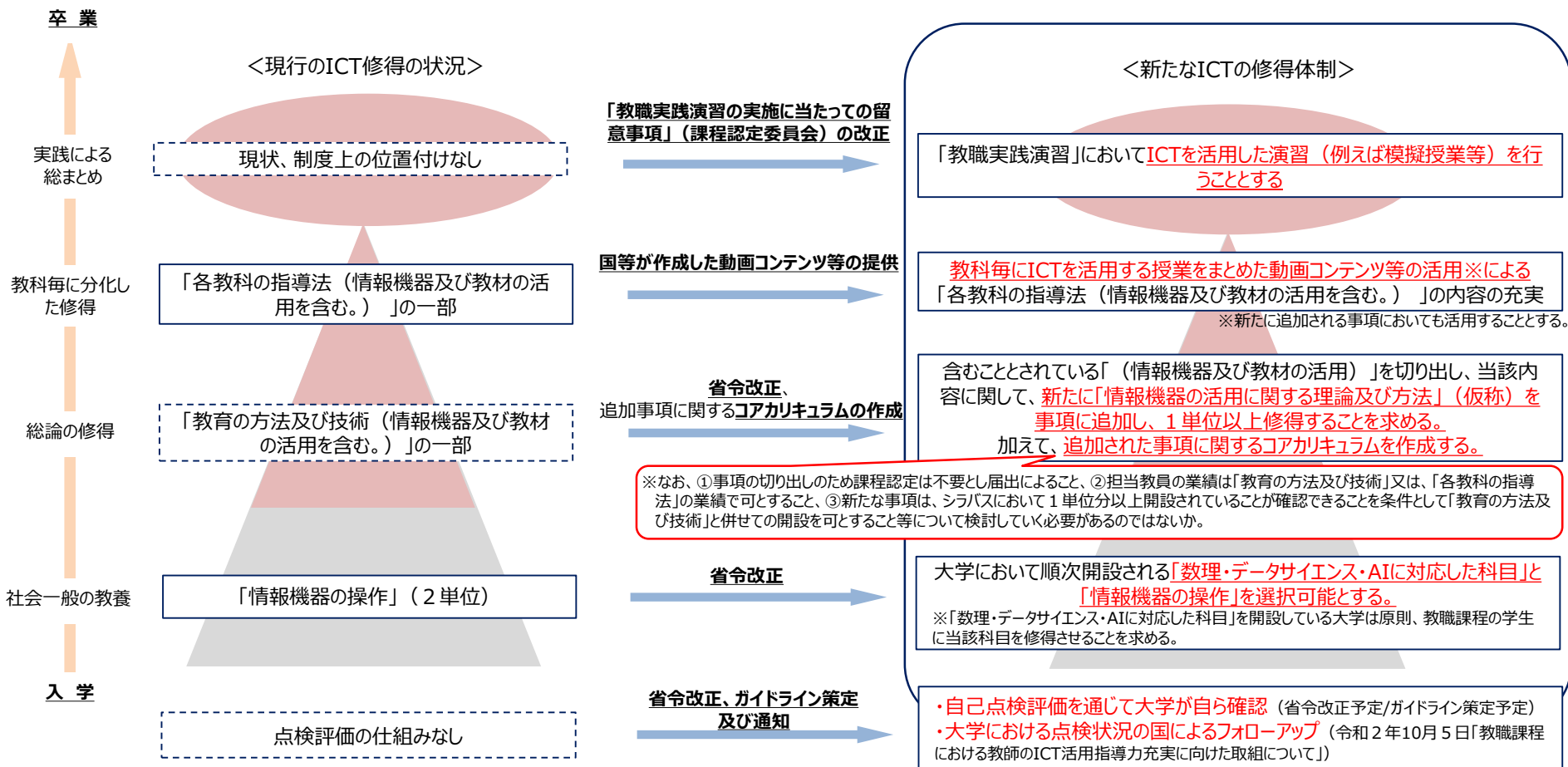
外部人材の活用等による指導体制の充実

【共通的な教員養成】

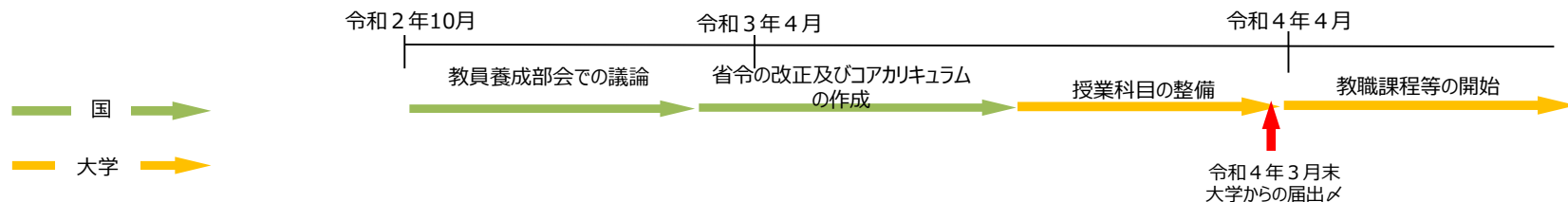
- ・ 教職課程においてICTを活用した各教科等の指導法を必修化【令和元年度から実施】
- ・ ICTに特化した科目を新設し、ICT機器を活用する授業の設計や授業の方法等の総論について1単位以上の修得を義務化【令和3年度：制度改正、令和4年度：課程の開始】
- ・ 国が作成したICTの活用に係るコンテンツを大学の授業で活用するとともに、「教員のICT活用指導力チェックリスト」等を活用して教職課程全体を検証すること等を求める通知を发出。今後大学の取組のフォローアップを実施【令和2年度実施】



教職課程におけるICT活用に関する内容の修得促進に向けた取組（案）



＜今後のスケジュール＞



ICT活用教育アドバイザー

＜令和2年度予算額：「新時代の学びにおける先端技術導入実証研究事業」（4.5億円）の内数＞

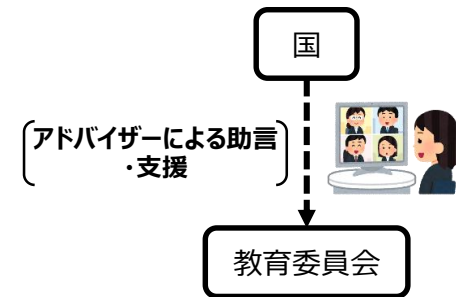
＜令和3年度予算額（案）：「GIGAスクールにおける学びの充実」（4億円）の内数＞

＜事業の流れ＞

国がアドバイザーを手配し、**各教育委員会等**に対し、派遣やオンラインで環境整備やICTを活用した指導方法など、教育の情報化に関する全般的な助言・支援を行う
※ アドバイザー：大学教員や先進自治体職員など、教育の情報化の知見を有する者

＜主な業務内容＞

ICT環境整備の計画、端末・ネットワーク等の調達方法、セキュリティ対策、ICT活用（遠隔教育含む）に関する助言 等



GIGAスクールサポーター

＜令和2年度補正予算額：105億円（自治体に対し、国が1/2補助）＞

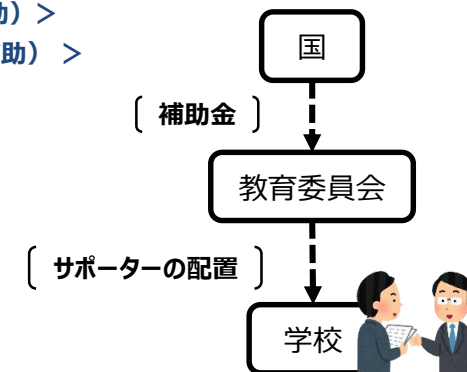
＜令和3年度予算額（案）：10億円（自治体に対し、国が1/2補助）＞

＜事業の流れ＞

各教育委員会等が国の補助金等を活用して、サポーターを募集・配置し、学校におけるICT環境整備の初期対応を行う
※ サポーター：ICT関係企業OBなど、ICT環境整備等の知見を有する者

＜主な業務内容＞

オンライン学習時のシステムサポート、ヘルプデスクによる遠隔支援、通信環境の確認、端末等の使用マニュアル・ルールの作成 等



ICT支援員

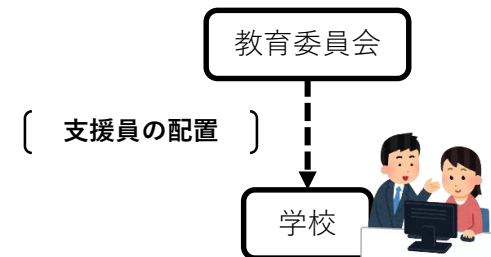
＜4校に1人分、地方財政措置＞

＜事業の流れ＞

各教育委員会等が地方財政措置を活用して支援員を募集・配置し、日常的な教員のICT活用の支援を行う
※ 支援員：業務に応じて必要な知見を有する者

＜主な業務内容＞

授業計画の作成支援、ICT機器の準備・操作支援、校務システムの活用支援、メンテナンス支援、研修支援 等



情報モラル教育の一層の充実に向けて

携帯電話・スマートフォンやSNSが子供たちにも急速に普及し、それらの利用に伴う犯罪被害等も生じている。

児童生徒に情報モラルを身に付けさせることが一層重要

※学習指導要領において、情報活用能力(情報モラルを含む)を、言語能力と同様に「学習の基盤となる資質・能力」と位置付け

1. 教師用指導資料の改訂や 動画教材の改善・充実

『情報社会の新たな問題を考えるための教材
～安全なインターネットの使い方を考える～』
(平成25年度、27年度、30年度、令和元年度)
・すぐに授業に活用できるようモデル指導案、
ワークシート例、アンケート例等を添付

文部科学省ホームページにて18の動画教材と指導の手引きを公開

http://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1416322.htm

①スマートフォンやタブレットなどの利用マナー

◆教材のねらい◆
対象:小学1年生～小学4年生
スマートフォンやタブレットなどの利用者の低年齢化に伴い、使いすぎるとともに問題となるのが、歩きながらのスマートフォン利用、



音漏れ、迷惑な写真撮影などの「マナー」の問題である。本教材では、他者のマナー違反を考えることで、スマートフォンやタブレットなどの利用マナーについて児童自身に考えさせる。

②著作物を公開するためには

◆教材のねらい◆
対象:小学5年生～中学1年生
最近はSNSなどで自分の著作物を公開する子供も増えており、「自分の著作物をどのように公開するか」という送り手側の意識に



着目することも必要である。本教材では受け手・送り手両方の立場から、著作物を取り扱う際の注意点、公開範囲の違いによる法律やマナーの違いなどを考えさせる。



2. 児童生徒向けリーフレットの 作成・配布

『ちょっと待ってスマホ時代のキミたちへ』
(小学校低学年用、小学校高学年・中学生用、高校生用)
・令和元年度は小学3年生、6年生全員に配布
・教育委員会を通じて全学校に1部ずつ配布

3. 情報モラル教育指導者 セミナーの実施

・対象は各学校において情報モラル教育を推進するに
当たり中核となる教員等
・令和元年度は全国4か所で開催し、238名が受講



労働者が費用負担し、厚生労働大臣が指定する教育訓練を受けた場合に、その費用の一部を「教育訓練給付」として雇用保険により支援。

	専門実践教育訓練給付 (2014年10月制度開始) ＜特に労働者の中長期的キャリア形成に資する教育訓練受講を対象＞	特定一般教育訓練給付 (2019年10月制度開始) ＜特ご労働者の速やかな再就職及び早期のキャリア形成に資する教育訓練受講を対象＞	一般教育訓練給付 (1998年12月制度開始) ＜活めひの雇用の安定・就職の促進に資する教育訓練受講を対象＞
給付内容	○ 受講費用の 50% (上限年間 40万円) を6か月ごとに支給。 ○ 訓練修了後1年以内に、資格取得等し、就職等した場合には、受講費用の 20% (上限年間 16万円) を追加支給。	○ 受講費用の 40% (上限 20万円) を受講修了後に支給。	○ 受講費用の 20% (上限 10万円) を受講修了後に支給。
支給要件	在職者又は離職後1年以内(妊娠、出産、育児、疾病、負傷等で教育訓練給付の対象期間が延長された場合は最大20年以内)の者 + 雇用保険の被保険者期間3年以上(初回の場合は2年以上)		
対象講座数	2,531講座 (2021年4月時点) 累計新規指定講座数 4,102講座 ※平成29年4月時点の給付対象講座数に、その後新規指定された講座数を加えた数	464講座 (2021年4月時点)	11,067講座 (2021年4月時点)
受給者数	23,251人 (2019年度実績) / 71,442人 (制度開始～2019年度) ※いずれも初回受給者数。	126人 (2019年度実績)	90,776人 (2019年度実績)
対象講座指定要件 (講座の内容に関する主なもの)	次の①～⑦の類型のいずれかに該当し (【 】内は講座期間・時間要件) かつ、類型ごとの講座レベル要件 を満たすものを指定。 ① 業務独占資格又は名称独占資格に係るいわゆる養成施設の課程 受給率、合格率及び就職・在職率の実績が一定以上 (看護師、准看護師、社会福祉士の養成課程等) [原則1年以上3年以内で、かつ取得に必要な最短期間(法令上の最短期間が4年の管理栄養士の課程及び法令上の最短期間が3年の養成課程であって定時制により訓練期間が4年となるものを含む。)] ② 専門学校等の職業実践専門課程等(キャリア形成促進プログラムを含む)※ 就職・在職率の実績が一定以上 文部科学省連携 (商業実務、経理・簿記等) 【2年(キャリア形成促進プログラムは120時間以上2年未満)】 ③ 専門職大学院 (MBA等) 【2年以内(資格取得につながるものは、3年以内で取得に必要な最短期間)】 就職・在職率、認証評価結果、定員充足率等の実績が一定以上 ④ 職業実践力育成プログラム (子育て女性のリカレント課程等)※ 文部科学省連携 [正規課程: 1年以上2年以内、特別の課程: 時間が120時間以上かつ期間が2年以内] 就職・在職率 (正社員等) かつ、就職・在職率及び定員充足率の実績が一定以上 ⑤ 一定レベル以上の情報通信技術に関する資格取得を目標とする課程 (情報処理安全確保支援士等)※ 経済産業省連携 【時間が120時間以上 (ITSSLレベル相当4以上のものに限り30単位以上) かつ期間が2年以内】 受給率、合格率及び就職・在職率の実績が一定以上 ⑥ 第四次産業革命スキル習得講座 (AI、IoT等)※ 経済産業省連携 【時間が30時間以上かつ期間が2年以上】 就職・在職率の実績が一定以上 ⑦ 専門職大学・専門職短期大学・専門職学科の課程※ 【専門職大学・学科: 4年、専門職短期大学・学科: 3年以上】 就職・在職率、認証評価結果、定員充足率等の実績が一定以上 ※1: 2016年4月から適用 ※2: 2016年10月から適用 ※3: 2017年10月から適用 ※4: 2018年4月から適用 ※5: 2019年4月から適用	次の①～③の類型のいずれかに該当しかつ、類型ごとの講座レベル要件 を満たすものを指定。 ① 業務独占資格、名称独占資格若しくは必置資格に係るいわゆる養成施設の課程(※)又はこれらの資格の取得を訓練目標とする課程等 (介護職員初任者研修、生活援助従事者研修、特定行為研修等を含む) ※ 専門実践教育訓練の①に該当するものを除く。 受給率、合格率及び就職・在職率の実績が一定以上 ② 情報通信技術に関する資格のうちITSSL 2以上の情報通信技術に関する資格取得を目標とする課程 (120時間未満のITSSLレベル3を含む) ※ 専門実践教育訓練の②に該当するものを除く。 受給率、合格率及び就職・在職率の実績が一定以上 ③ 短時間のキャリア形成促進プログラム及び職業実践力育成プログラム ※ 専門実践教育訓練の②、④に該当するものを除く。 就職・在職率の実績が一定以上 文部科学省連携 ※ 趣味的・教養的な教育訓練、入門的・基礎的な水準の教育訓練、職業能力を評価するものとして社会一般に認知されていない免許資格・検定に係る教育訓練は、対象外。 ※ 講座時間・期間要件 通学制: 期間が1ヶ月以上1年以内であり、かつ時間が50時間以上、通信制: 3ヶ月以上1年以内 サイバーセキュリティを含む情報関係講座等実績 講座数: 360講座 修了者数: 3,551人 ※講座数は令和3年4月時点、修了者数は令和元年度実績	次の①又は②のいずれかに該当する教育訓練を指定。 ① 公的職業資格又は修士若しくは博士の学位等の取得を訓練目標とするもの ② ①に準じ、訓練目標が明確であり、訓練効果の客観的な測定が可能なもの (民間職業資格の取得を訓練目標とするもの等) ※ 趣味的・教養的な教育訓練、入門的・基礎的な水準の教育訓練、職業能力を評価するものとして社会一般に認知されていない免許資格・検定に係る教育訓練は、対象外。 ※ 講座時間・期間要件は原則として以下のとおり。 ・ 通学制: 期間が1ヶ月以上1年以内であり、かつ時間が50時間以上 ・ 通信制: 3ヶ月以上1年以内 指定講座例 ○ 輸送・機械運転関係 (大型自動車、建設機械運転等) ○ 医療・社会福祉・保健衛生関係 (同行援助従事者研修等) ○ 専門的サービス関係 (社会保険労務士、税理士、司法書士等) ○ 情報関係 (プログラミング、CAD、ウェブデザイン等) ○ 事務関係 (簿記、英語検定等) ○ 営業・販売・サービス関係 (宅地建物取引主任者等) ○ 技術関係 (建築施工管理技術検定、電気主任技術者等) ○ 製造関係 (技能検定等) ○ その他 (大学院修士課程等)

警察のサイバー人材

人材の確保

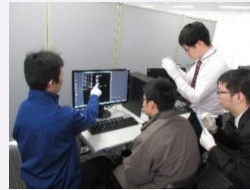
都道府県警察捜査員
約2万名

専門捜査員
約1,500名

連携

警察庁採用技術系職員
約900名

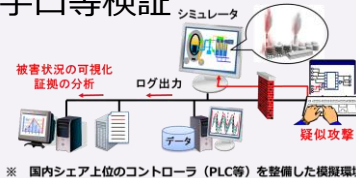
捜査支援



不正プログラム解析



手口等検証



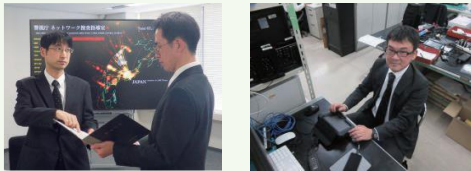
サイバーフォース



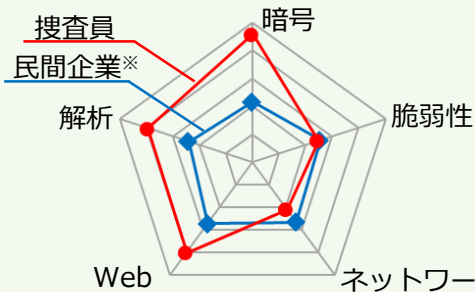
補完

技術系人材の登用

特別採用・中途採用 約400名



【参考】ベンダー提供CTF結果



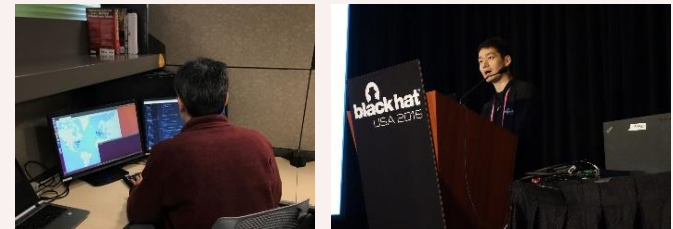
高度な訓練環境

サイバーレンジ

- 実事案の犯行手口や状況を再現できる仮想環境を構築し、演習を実施。
- 攻撃側と防御側に分かれた攻防戦も可能。

民間研修・学術研究機関等への派遣

- パデュー（米）、カーネギーメロン（米）、情報セキュリティ大学院大学（日）等
- 日本サイバー犯罪対策センター、金融機関、ITベンダー等



【参考】

セキュリティスペシャリスト等の資格保有状況
都道府県警察捜査員・警察庁技術系職員
約400名

警察の強みを活かした地域社会における安全教育・普及啓発活動の推進

【警察の強み①：幅広い情報を保有】

- オープンソースはもとより、捜査により得た情報や全国の事業者、外国治安機関等から提供された情報などを幅広く保有



【警察の強み②：大規模な技術部隊が各都道府県に満遍なく存在】

- 警察（国）は約4千人の技術集団を擁しており、数百人規模の解析の専門家を全国に配置
- 都道府県警察の捜査支援に従事する一方、セキュリティ人材が不足しがちな地方においては貴重な存在



【警察の強み③：地域における幅広いネットワーク】

- 全国の都道府県警察（警察本部、警察署等）は、協議会等を通じて地域住民、事業者等とのネットワークを形成
- 交通安全教室等を通じて青少年への教育にもコミット



取組

- 青少年や教育機関関係者等を対象とした講演
- 各地の協議会等を通じた関係者への情報提供や意見交換
- サイバー防犯ボランティアと連携したイベントやサイバーパトロール等

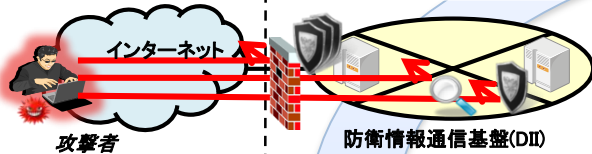
【事例：産学官連携による安全教育活動】



防衛省・自衛隊におけるサイバー攻撃対処のための各種施策

① 情報システムの安全性確保

- ・ファイアウォール、ウィルス検知ソフトの導入
- ・ネットワークをDIIオープン系・クローズ系と分離
- ・システム監査の実施 等



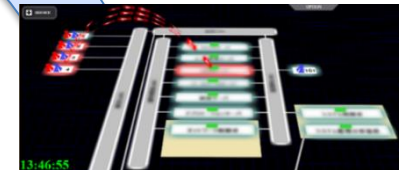
② 専門部隊によるサイバー攻撃対処

- ・サイバー防衛隊(統)、システム防護隊(陸)、保全監査隊(海)、システム監査隊(空)によるネットワーク・情報システムの24時間監視、高度なサイバー攻撃対処(マルウェア解析)



③ サイバー攻撃対処態勢の確保・整備

- ・サイバー防衛演習の実施
- ・サプライチェーン・リスク対応の措置
- ・サイバー攻撃発生時の対処態勢の整備



サイバー攻撃対処6本柱

⑥ 他機関等との連携

- ・内閣サイバーセキュリティセンター、米軍、関係各国等との情報共有
- ・NATOサイバー防衛協力センター(CCDCOE)への防衛省職員派遣
- ・米陸軍サイバー教育機関への連絡官の派遣
- ・官民人事交流



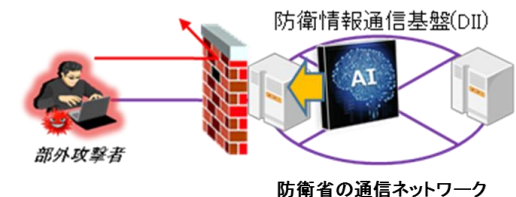
⑤ 人材育成

- ・人材育成のため、米国カーネギーメロン大学付属機関、国内大学院への留学や各自衛隊の専門課程における教育の実施
- ・セキュリティ意識の醸成のため、職場における教育、防衛大学校における専門教育の実施
- ・部外教育の実施



④ 最新技術の研究

- ・AIの活用に関する研究



防衛省・自衛隊におけるサイバー攻撃対処態勢

■ サイバー防衛隊はDIIを、陸海空のサイバー関連部隊等（陸：サイバー防護隊、海：保全監査隊、空：システム監査隊等）はそれぞれが管理するシステム・ネットワークを24時間態勢で監視し、サイバー攻撃に対処。

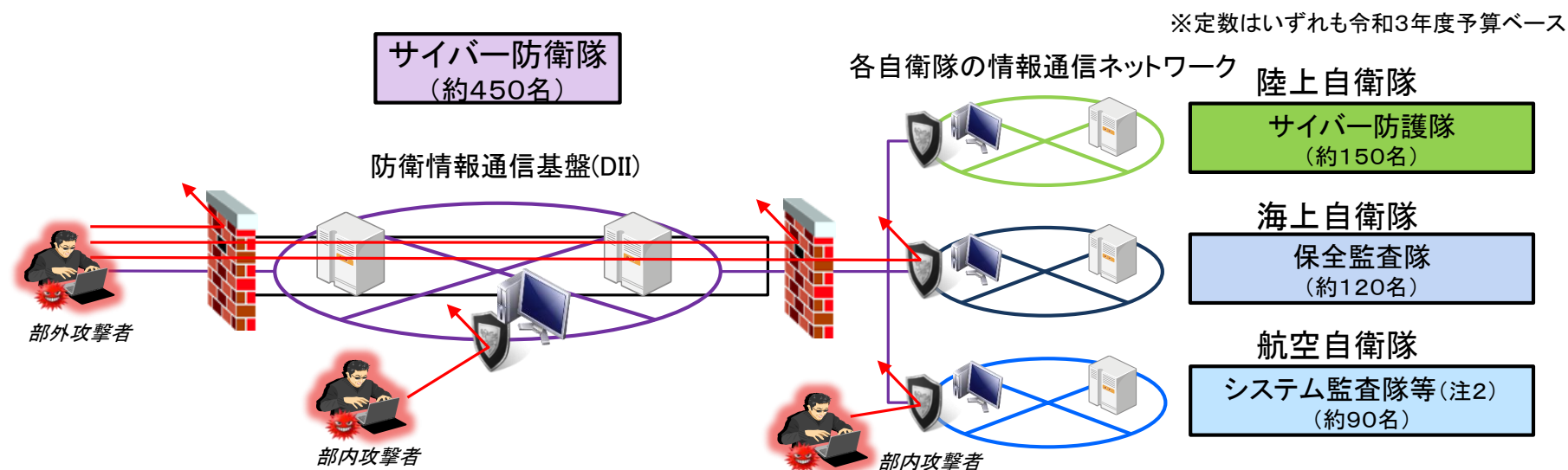
■ サイバー防衛隊及び陸海空のサイバー関連部隊等の規模は、以下のとおり。

平成30年度末時点：合計約430名（うち、サイバー防衛隊は約150名）

令和元年度末時点：合計約580名（うち、サイバー防衛隊は約220名）

令和2年度末時点：合計約660名（うち、サイバー防衛隊は約290名）

⇒ 令和3年度予算：合計約800名（うち、サイバー防衛隊等は約450名（注1））



(注1) 自衛隊サイバー防衛隊(仮称)の隊本部及び同隊隷下のサイバー防衛隊の定員の合計

(注2) システム監査隊のほか、空自の作戦システム等に係るサイバー防護のための要員

防衛省・自衛隊におけるサイバー人材の確保・育成

人材確保・育成の現状(イメージ)

スキル
レベル

Lv7

部外人材の活用

(企業が擁する人材の契約による活用、
隊員としての採用等)

Lv6

Lv5

部外教育による育成

(企業研修、国内外教育機関への留学、
国際訓練等)

Lv4

Lv3

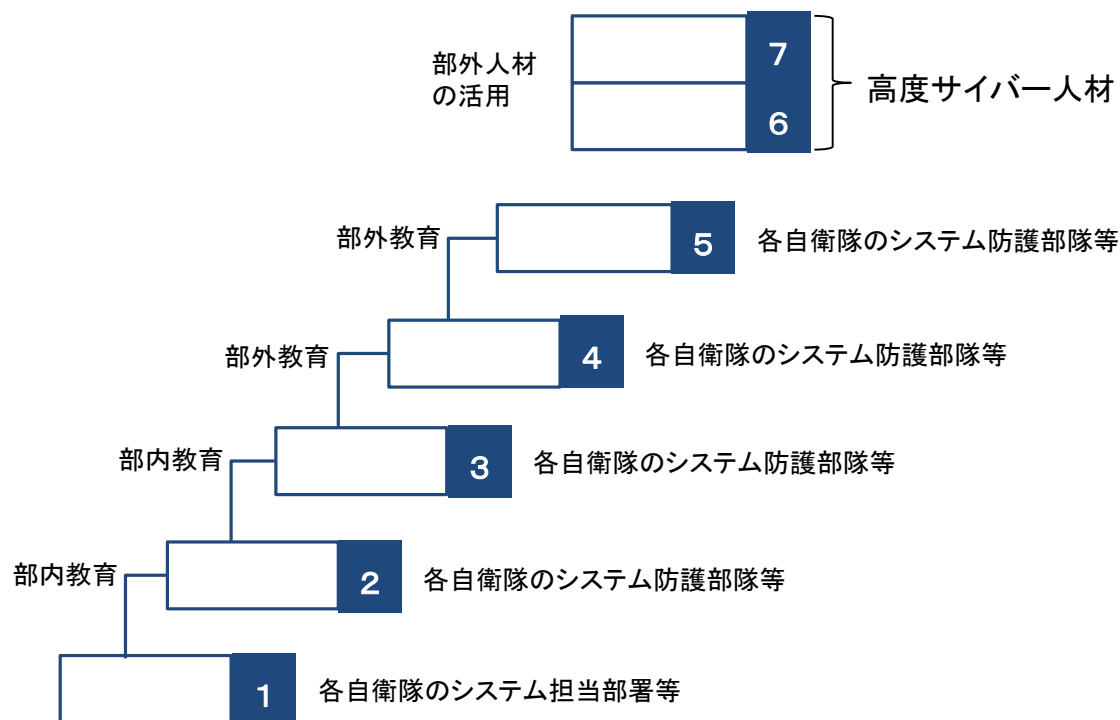
部内教育による育成

(統幕・陸海空自の教育課程)

Lv2

Lv1

高度な技能を修得・維持できるよう、
サイバー関連部署に継続的かつ段階的に配属



※スキルレベルは、IPA(Information-technology Promotion Agency:
独立行政法人情報処理推進機構)のITスキル標準に準拠

サイバー人材の確保・育成の施策

■ 部内教育

- 令和元年度から実施している陸海空自衛隊の共通教育である「サイバー共通課程」の規模を令和3年度に拡充し、一元的な人材育成を強化予定(器材整備等の経費を令和2年度予算(約0.9億円)及び令和3年度予算(約0.8億円)に計上)
- 令和3年度から、陸自高等工科学校においてサイバー等に関する基礎的な教育を行う「システム・サイバー専修コース」を開始

■ 部外教育

- 令和元年度から、米国防大学のサイバー戦指揮官要員課程に、サイバー戦における指揮官の意思決定要領等に関する知見を習得させるため、隊員(1佐)を派遣
- 令和3年度予算において、サイバーセキュリティに関する高度な知識・技能を有するハイスキル人材の育成を加速化すべく、部外教育機関を活用した教育を実施するために必要な経費(約7百万円)を計上

■ 部外の高度人材の活用

- 令和3年度予算において、サイバー領域における最新技術やサイバー攻撃の最新動向等サイバーセキュリティに関する高度な知見を有する民間の高度サイバー人材を採用するために必要な経費(約0.2億円)を計上
- 官民人事交流制度による民間企業のサイバー人材の活用を検討

デジタル社会の実現に向けた改革の基本方針

IT室①

IV. デジタル庁設置の考え方

2. デジタル庁の業務

(6) サイバーセキュリティの実現

- デジタル庁が作成する情報システムの整備・管理の基本的な方針において、サイバーセキュリティに関する基本的な方針を示すこととし、当該部分については、サイバーセキュリティ戦略本部と緊密に連携して作成する。
- デジタル庁にセキュリティの専門チームを置き、デジタル庁が整備・運用するシステムの検証・監査を実施するとともに、内閣サイバーセキュリティセンター（NISC）がその体制を強化しつつ、デジタル庁が整備・運用するシステムを含めて国の行政機関等のシステムに対するセキュリティ監査等を行う。
- これらにより、国民の重要な情報資産を保護する。

「デジタル社会の実現に向けた改革の基本方針」（令和2年12月25日閣議決定）
<https://www.kantei.go.jp/jp/singi/it2/dgov/201225/siryou1.pdf>

デジタル庁設置に向けたセキュリティ人材の確保

- 4月27日～5月10日(月)公募を実施、現在、選考中。
- 9月1日のデジタル庁設置より前倒しで(IT総合戦略室に)採用予定。セキュリティを始め、各専門分野毎に「ジョブ・ディスクリプション」を明確にし、対応すべき分野やプロジェクトを担う方々を募集。
- セキュリティ分野では、セキュリティ・ストラテジスト、脆弱性診断士、インシデントハンドラーなどの業務ごとに必要なスキル・経験を示して公募。
- 今後も、幹部クラスの常勤職員やデジタル庁で必要となる非常勤職員等を順次募集していく予定。

デジタル庁 (準備中) トップ デジタル庁について 法令 新卒採用 中途採用 お知らせ

中途採用

デジタル庁の創設に向けて 人材募集中。

デジタル庁は、デジタルの活用により、一人一人のニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会（誰一人取り残さない、人に優しいデジタル化）を目指します。

内閣官房 情報通信技術（IT）総合戦略室では、デジタル庁の創設に当たり、能力と志の両方を併せ持つ人材の採用を進めていきたいと考えています。デジタル庁の組織文化を形作る想いのある人材に、是非門戸を叩いてほしいと考えています。

デジタル庁は、社会全体のデジタル化を推進し、Move Agile、Scale Fastの精神で、行政におけるデジタル・トランスフォーメーションを加速させ、継続的にアップデートしていく仕組みづくりを行います。

国民との信頼関係を構築し、日本のデジタル・インフラを描き、実行していく。多様な経験や豊富な専門性を活かし、ともに大きな挑戦に取り組みましょう。

中途採用

志高いプロフェッショナル人材を広く募集しております。

応募期間
2021（令和3）年4月27日～5月10日
※受付は終了しました。

選考プロセス
書類選考の後、複数回の面接（※専門性を見極めるための面接）と書類選考通過者へのみ、応募書類の提出を求めます。

セキュリティ

- 【受付終了】 セキュリティストラテジスト（全体設計）
- 【受付終了】 セキュリティストラテジスト（監査）
- 【受付終了】 脆弱性診断士
- 【受付終了】 インシデントハンドラー

デジタル庁 中途採用ページ

<https://www.digital.go.jp/recruit/career>

関連：次期サイバーセキュリティ戦略 骨子

4 目的達成のための施策

4. 2 国民が安全で安心して暮らせるデジタル社会の実現

4. 2. 3 経済社会基盤を支える各主体における取組①（政府機関等）

- 各政府機関においては、統一的な基準を踏まえた情報セキュリティ対策が講じられるとともに、当該基準に基づいた監査やGSOCによる不正な通信の監視等の取組を通じて、政府機関全体としての対策の水準の向上を推進している。セキュリティは、社会全体のデジタル化の車の両輪として、情報システムの開発・構築段階も含めたあらゆるフェーズでの対策を強化していく。
- 特に、各府省庁が共通で利用する重要なシステムについては、デジタル庁が自ら又は各府省と共同で整備・運用し、セキュリティも含めて安定的・継続的な稼働を確保する。

次期サイバーセキュリティ戦略 骨子

4. 2 国民が安全で安心して暮らせるデジタル社会の実現（緑パート）

<https://www.nisc.go.jp/conference/cs/dai28/pdf/28shiryoku01.pdf>