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

経済産業省　商務情報政策局

サイバーセキュリティ課

サイバーセキュリティ戦略専門官

佐藤　秀紀

１．はじめに
～“サプライチェーン攻撃”と事例

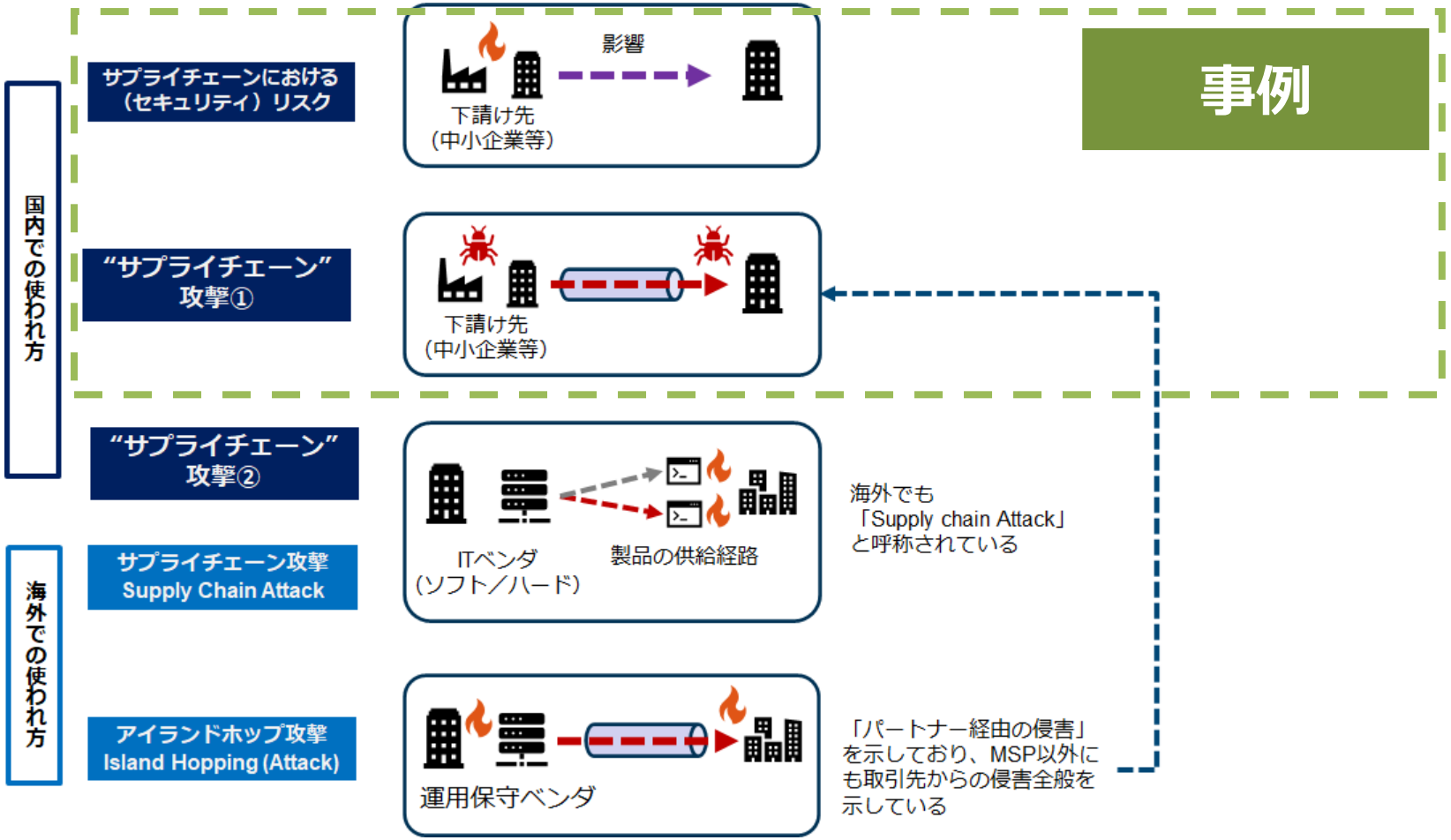
２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．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）

４．サイバーセキュリティ対策の基盤整備
～人材育成

“サプライチェーン”攻撃とは

- サプライチェーン攻撃には、国内では**製品やサービス提供の連鎖への攻撃**、
  海外では**情報のやり取りの連鎖への攻撃**を示しているという違いがある。

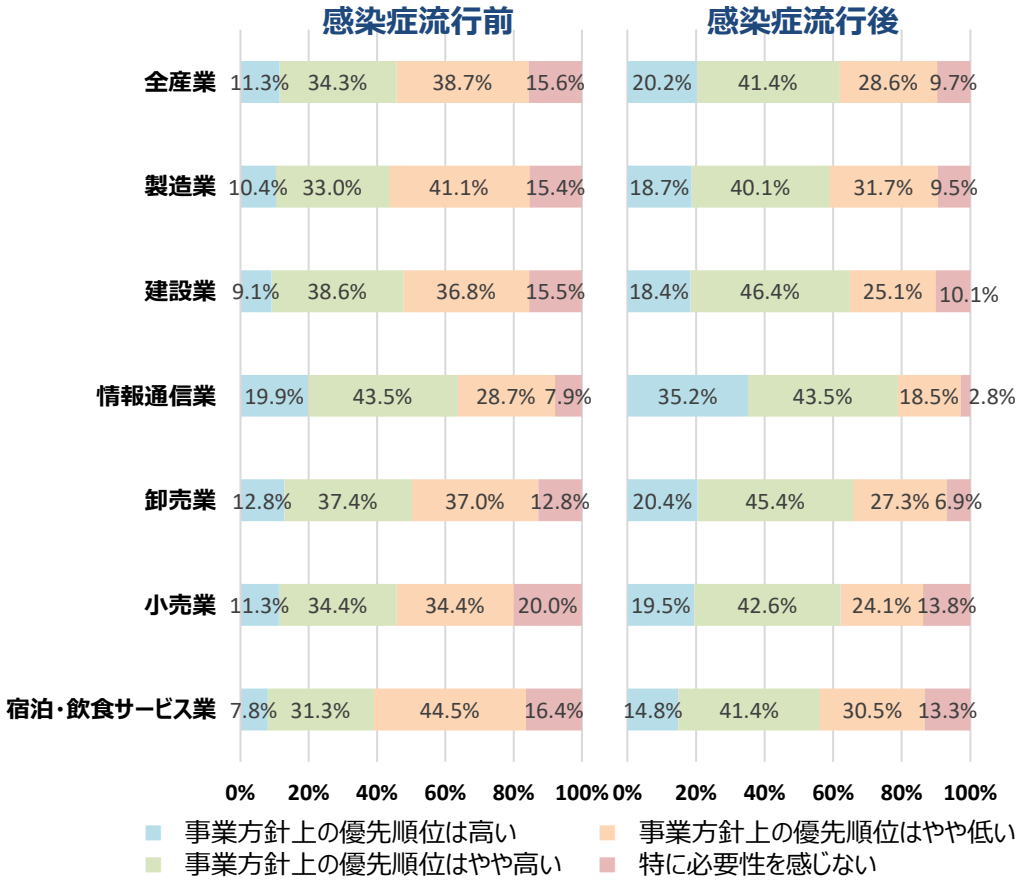


参考：JP-CERT　なぜ、SSL-VPN製品の脆弱性は放置されるのか ～“サプライチェーン”攻撃という言葉の陰で見過ごされている攻撃原因について～
https://blogs.jpcert.or.jp/ja/2022/07/ssl-vpn.html

【事例】デジタル化の進展とサイバーセキュリティ対策の必要性

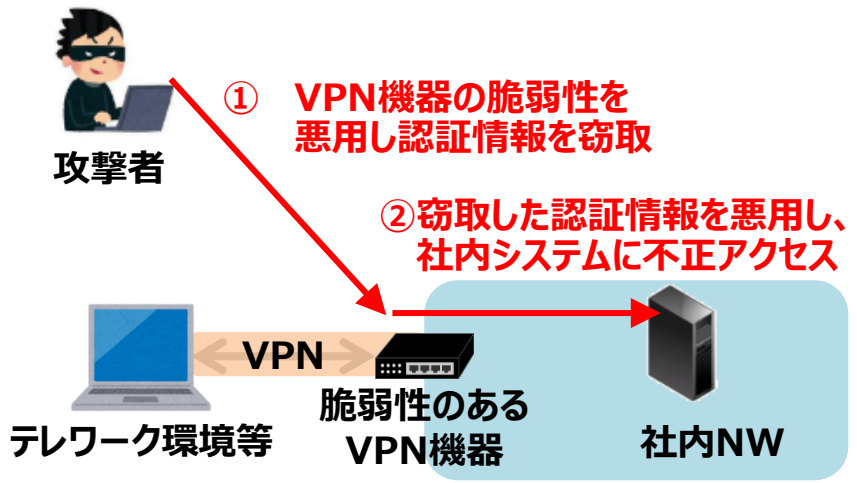
- デジタル化に対する意識は、コロナ禍の前後で、**産業領域を問わず大きく変化**。
- 一方、テレワークの利用等が増える中、VPNの脆弱性を突いたサイバー攻撃が増加するなど、**サイバー攻撃の脅威はあらゆる産業において無縁ではなくなっている**。

デジタル化に対する優先度の変化



（出典）中小企業庁「中小企業白書2021」

VPN機器に対する不正アクセス

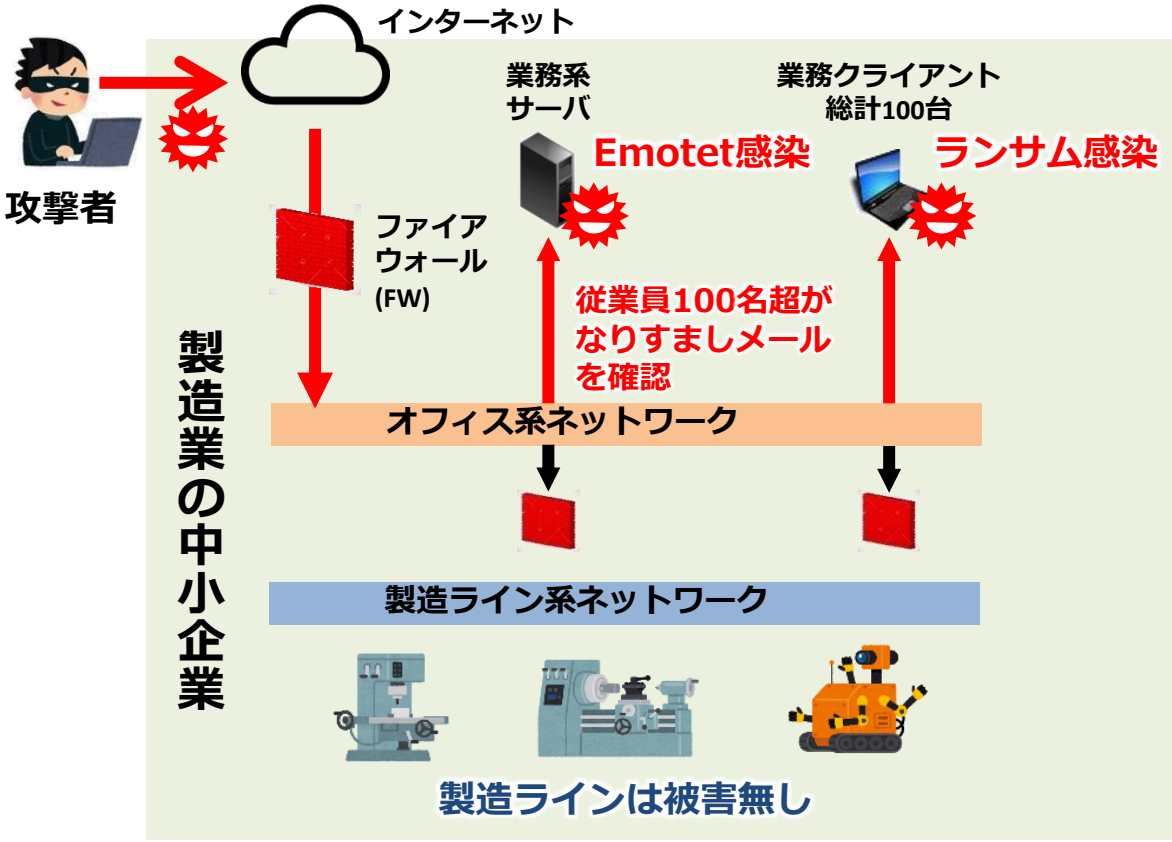


事例：Fortinet製FortiOSの脆弱性

2019年5月	脆弱性情報公開
2019年8月頃	脆弱性の詳細情報公開、悪用やスキャン開始
2020年11月	脆弱性の影響を受ける約5万台の機器情報が公開 IPアドレス、ユーザーアカウント名、平文パスワード等その後追加公開があり、対象が計8.7万台に拡大。

【事例】中小企業におけるサイバー攻撃の事例

- 重要インフラに関連する製造業の中小企業（従業員約200名規模）で、Emotetとランサムウェアに感染。Emotetに感染したメールアカウントは約100名分。原因は、受信メールの添付ファイルを自動実行する環境で開封したことであった。
- サイバーインシデントの初動対応体制や手順、セキュリティポリシーが整備されておらず、業務停止の判断等が困難な状況に陥った。
- 結果として、製造ラインの業務停止はなかったが、取引先へは、製造ラインに被害が無いことを証明する必要があり、影響範囲の特定を行うためフォレンジック調査費だけで500万円程度かかった。



対処時の問題点

- 業務停止の判断基準が整備されておらず、数日間判断が出来ないまま時間が経過。
- インシデント時の初動対応体制の役割分担が不明確であり、適切な人員確保もできず。
- 重要インフラを取り扱う業種で、影響範囲の把握が急務だったが自社内では調べきれず。

業務影響/被害額

- 製造ラインに影響はなかったものの、結果を取引先に報告する必要あり。
- フォレンジック調査費だけで500万円程度を支出。高額な緊急支出に。
- 原因の判明だけでも10営業日程度を要した。
- 設計データなど最重要データが一部消失した。
- 取引先から問合せと苦情が殺到し、数週間にわたって業務がひっ迫した。

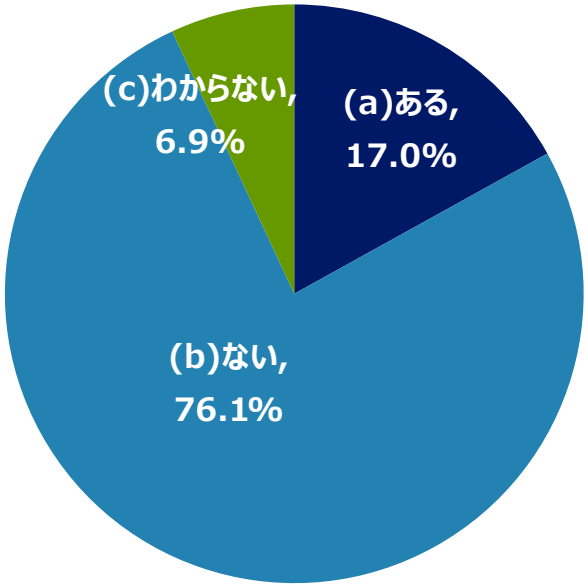
【事例】取引先等を経由した大企業・中堅企業のサイバー攻撃被害

- **取引先企業を含むサプライチェーンのサイバーセキュリティ対策は、自社組織のセキュリティ対策に並び重要な要素となっていること**を踏まえ、大企業・中堅企業を対象に、各企業におけるサプライチェーンのサイバーセキュリティ対策の課題や優良事例を経済産業省が調査（※）。
- **大企業・中堅企業の５社に１社に近い割合で取引先等を経由したサイバー攻撃被害の経験**がある。

取引先等を経由したサイバー攻撃被害の経験

取引先等を経由したサイバー攻撃被害の経験

➢ 過去に取引先等がサイバー攻撃の被害を受け、それが貴社に及んだ経験がありますか（仕入・外注・委託先等の取引先）



(N=1876)

攻撃被害の主な内容

Emotet	● 取引先等がEmotetに感染し、不正なメールを受信
ランサムウェア	● 取引先等がランサムウェアに感染し、自社関連情報が暗号化／外部漏洩 ● 取引先等がランサムウェアに感染、業務停止し、自社業務に影響
不正アクセス	● 取引先等のシステムが不正アクセスをうけ、自社関連の情報が漏洩 ● グループ会社がVPNの脆弱性をついた不正アクセスによりネットワーク侵害をうけ情報が漏洩
ビジネスメール詐欺	● 取引先等がマルウェアに感染し、取引先を装い金銭を要求する詐欺メールを受信
DDoS攻撃	● 委託先のシステムや利用するクラウドサービスがDDoS攻撃を受け、自社業務に影響
その他	● 取引先等のホームページの改ざんによる、不正サイトへの誘導、自社業務への影響 ● 取引先が提供する電子決済サービスの悪用による顧客口座の不正送金 ● 設備業者がメンテナンスのために持ち込んだPCから社内環境にウイルスが侵入　等

（※）令和３年度サイバー・フィジカル・セキュリティ対策促進事業（企業におけるサプライチェーンのサイバーセキュリティ対策に関する調査）

１．はじめに
　～“サプライチェーン攻撃”と事例

２．産学官の検討体制の構築
　～産業サイバーセキュリティ研究会

３．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）

４．サイバーセキュリティ対策の基盤整備
　～人材育成

サイバーセキュリティ戦略2021：「Cybersecurity for All」を踏まえた対応の強化

サイバー空間の課題認識

- あらゆる主体が参画する**公共空間化**
- **サイバー・フィジカルの相互連関・連鎖の深化**
- **サイバー攻撃の複雑化・巧妙化**
- **安全保障上の脅威の増大**

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

個人		組織	
DXに向き合う**地方、中小企業、若年層、高齢者等**	目に見えないリスクと向き合う**個人・組織**	サイバー攻撃による**重要インフラ**停止、知財の窃取、金銭被害等の増大	**国家の関与**が疑われる攻撃

DXとサイバーセキュリティの同時推進

○デジタル改革と一体で：**経営層の意識改革、地域・中小企業の取組促進**
（経営インセンティブ、安価かつ効果的な支援サービス・保険の普及）

○誰も取り残さないリテラシーの向上と定着
（高齢者向けデジタル活用支援講習会との連携、GIGAスクール構想にあわせた普及啓発、サイバー防犯ボランティア）

安全保障の観点からの取組強化

○中露北からの脅威等を踏まえた外交・安全保障上のサイバー分野の優先度向上

○防衛省・自衛隊におけるサイバー防衛能力の抜本的強化

○「妨げる能力」、外交的手段や刑事訴追等を含めた対応、日米同盟の維持・強化

○**国際協力・連携**

公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

○**国民・社会を守るためのサイバーセキュリティ環境の提供**
（**産業横断的なサプライチェーン管理**、サイバー犯罪対策、クラウドサービス利用のための対策の多層的な展開、経済安全保障の視点を含むサイバー空間の信頼性確保）

○深刻なサイバー攻撃から国民生活・経済を守る**包括的なサイバー防御等の展開**
（**情報収集から対処調整、政策措置までの一体的推進の総合調整を担うナショナルサートの機能強化**、政府機関・重要インフラ等の各主体のセキュリティ対策）

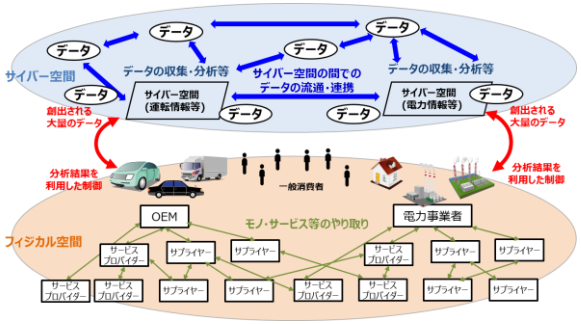
※赤字は経産省が主体的に関与

経済産業省におけるサイバーセキュリティ政策の全体像

- 「Society5.0」では、データの流通・活用を含む、**より柔軟で動的なサプライチェーン**を構成することが可能となる。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要**となる。

①業種別／分野横断的なガイドライン等の作成

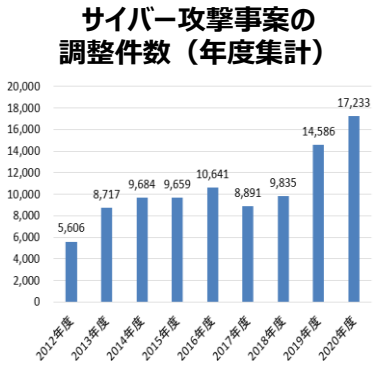
- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）に基づく、セキュリティ対策の提示



- SBOM活用に向けた実証事業の実施

②事案対処に備える基盤の構築

- 国境を越えて行われるサイバー攻撃へのJPCERT/CCの対処能力の向上
- 公的機関や重要インフラ事業者等での事案発生時の初動支援を行うJ-CRATの体制強化
- ICSCoEにおける事故調査体制の構築



③中小企業/地方へのサイバーセキュリティ対策の普及促進

- サイバーセキュリティお助け隊サービスの普及促進
- 地域単位でセキュリティのためのコミュニティ（地域SECUNITY）の創出
- SC3の活動支援を通じた、サプライチェーン全体でのサイバーセキュリティ強化の取組強化

サイバーセキュリティお助け隊

④人材育成/国際貢献

- IPA/産業サイバーセキュリティセンターを中心とした人材・組織・システム・技術の開発
- 重要インフラ等を守る高度セキュリティ人材の育成（中核人材育成プログラム）
- 日米欧によるインド太平洋地域向けの能力構築支援

IPA 産業サイバーセキュリティセンター
Industrial Cyber Security Center of Excellence（ICSCoE）

産業サイバーセキュリティ研究会とWGの設置による検討体制

産業サイバーセキュリティ研究会

第１回：平成29年12月27日　開催
第２回：平成30年　5月30日　開催
アクションプラン（４つの柱）を提示
第３回：平成31年　4月19日　開催
アクションプランを加速化する３つの指針を提示
第４回：令和2年　　4月17日　開催（電話開催）
産業界へのメッセージを発信
第５回：令和2年　　6月30日　開催
サイバーセキュリティ強化運動の展開
第６回：令和３年　　４月２日　開催
アクションプランの持続的発展と、新たな課題へのチャレンジへ
第７回：令和４年　　４月11日　開催
産業界へのメッセージを発信

WG１（制度・技術・標準化）

１．サプライチェーン強化パッケージ

WG２（経営・人材・国際）

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

WG３(サイバーセキュリティビジネス化)

４．ビジネスエコシステム創造パッケージ

産業サイバーセキュリティの加速化指針

１．『グローバル』をリードする
２．『信頼の価値』を創出する~Proven in Japan~
３．『中小企業・地域』まで展開する

泉澤　清次　三菱重工業株式会社取締役社長
遠藤　信博　日本経済団体連合会サイバーセキュリティ委員長、日本電気株式会社取締役会長等
大林　剛郎　日本情報ｼｽﾃﾑ・ﾕｰｻﾞｰ協会会長、株式会社大林組代表取締役会長
櫻田　謙悟　経済同友会代表幹事、ＳＯＭＰＯホールディングスグループＣＥＯ取締役　代表執行役社長
篠原　弘道　日本電信電話株式会社取締役会長
東原　敏昭　株式会社日立製作所代表執行役　執行役会長兼CEO兼取締役
船橋　洋一　アジア・パシフィック・イニシアティブ理事長
村井　純(座長)慶應義塾大学教授
渡辺　佳英　日本商工会議所特別顧問、大崎電気工業株式会社　取締役会長

産業サイバーセキュリティ研究会構成員　（2022年4月11日現在）

１．はじめに
～“サプライチェーン攻撃”と事例

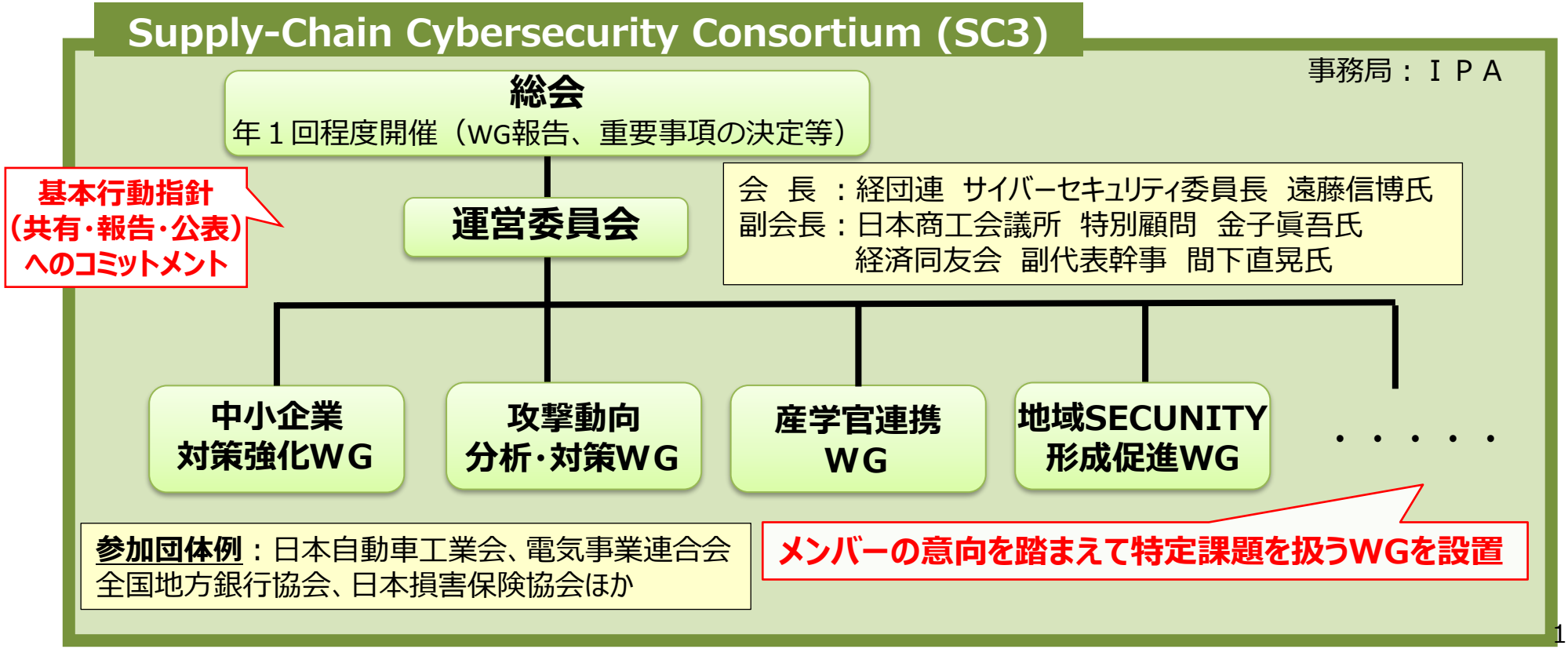
２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．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）

４．サイバーセキュリティ対策の基盤整備
～人材育成

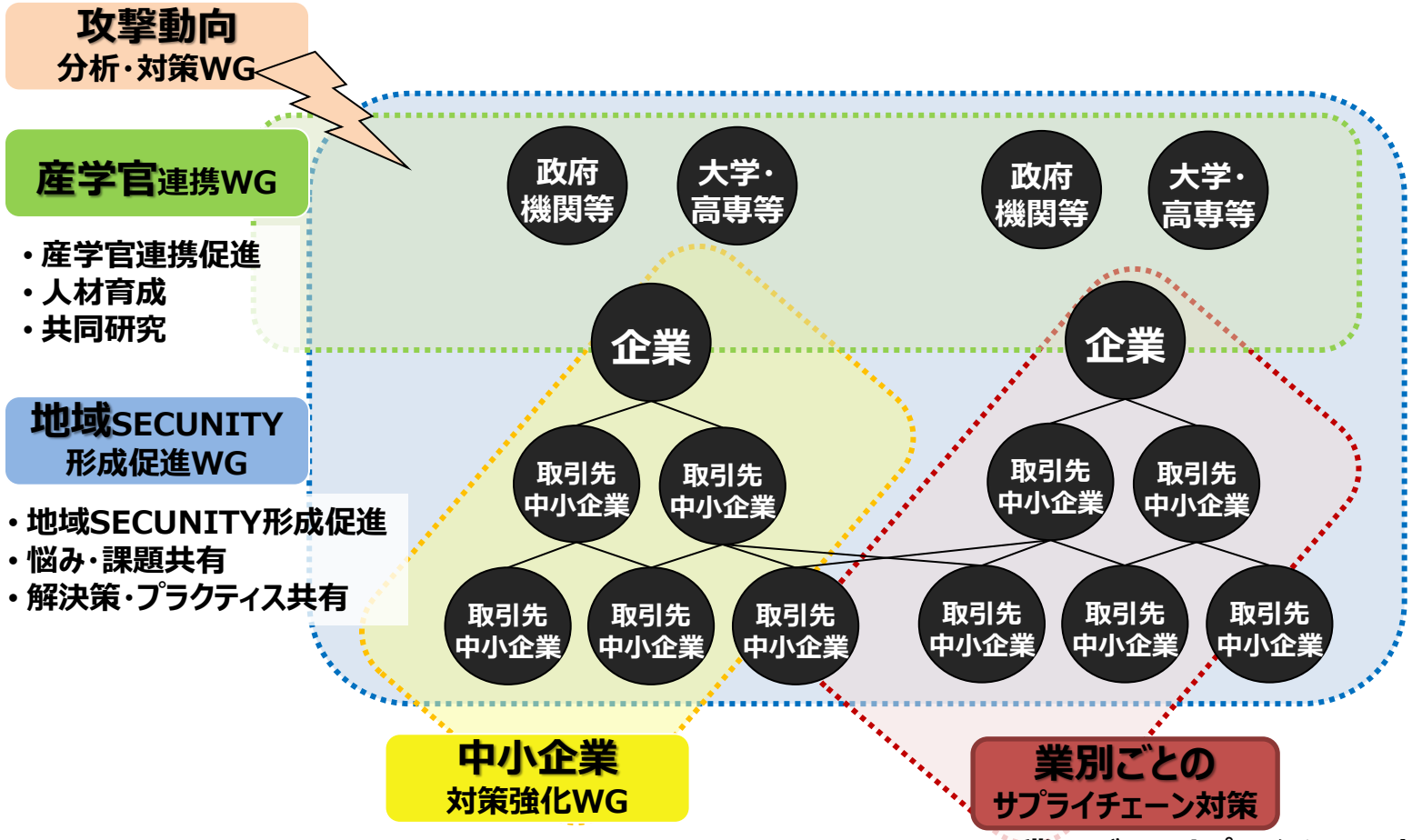
サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）

- **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（2022年10月末時点で175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。



SC3の全体像

- 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議論・浸透のため、SC3に対し、産学官連携や経営層向けの注意喚起、地域・業界別の取組・課題共有等のプラットフォームとしての機能への期待の声が挙がったことを踏まえ、中小企業対策強化WGに加えて、新たに３つのWGを設置。



１．はじめに
　～“サプライチェーン攻撃”と事例

２．産学官の検討体制の構築
　～産業サイバーセキュリティ研究会

３．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）

４．サイバーセキュリティ対策の基盤整備
**　～人材育成**

サイバーセキュリティ経営ガイドラインの改訂の概要

平成27年12月28日策定
平成28年12月8日改訂（Ver1.1）
平成29年11月16日改訂（Ver2.0）

- サイバー攻撃の多様化やサプライチェーンの複雑化により、**サプライチェーン全体を通じたサイバーセキュリティ対策の必要性が高まっており、経営者が自らリーダーシップを発揮して更なる対策の強化や適切な対応が必要**。
- このような実情等を踏まえ、経営者が認識すべき原則及びCISO等に指示すべき事項を記載した本ガイドラインについて、**経営者の責務としてサイバーセキュリティに関する残留リスクを低減すること**等を明記するとともに、**サプライチェーンの多様化・複雑化等の情勢の変化やサイバー・フィジカル空間の融合に対応した対策の必要性**を踏まえた改訂を予定。

＜現行のガイドライン構成＞

1．経営者が認識すべき３原則

（１）経営者が、**リーダーシップを取って対策**を進めることが必要
（２）自社のみならず、**ビジネスパートナーを含めた対策**が必要
（３）平時及び緊急時のいずれにおいても、**関係者との適切なコミュニケーション**が必要

2．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAサイクルの実施
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の対策及び状況把握
関係者とのコミュニケーション	**指示10** 情報共有活動への参加

＜改訂案の概要＞

●取引関係にとどまらず、サプライチェーンでつながる関係者へのセキュリティ対策への目配り、総合的なセキュリティ対策の重要性や社外のみならず、社内関係者とも積極的にコミュニケーションをとることの必要性を記載

●セキュリティ業務従事者のみならず、全ての従業員において、必要かつ十分なセキュリティ対策を実現できるスキル向上の取組の必要性を記載

●サイバーセキュリティリスクの識別やリスクの変化に対応した見直しやクラウド等最新技術とその留意点などを記載

●事業継続の観点から、制御系も含めた業務の復旧プロセスと整合性のとれた復旧計画・体制の整備やサプライチェーンも含めた実践的な演習の実施等について記載

●サプライチェーンリスクへの対応に関しての役割・責任の明確化、対策導入支援などサプライチェーン全体での方策の実行性を高めることについて記載

参考：『サイバーセキュリティ経営ガイドラインVer2.0実践のためのプラクティス集』

- 2019年3月、**「サイバーセキュリティ経営ガイドラインVer2.0実践のための経営プラクティス集」を公開**。経営ガイドラインの重要10項目の実践事例に加え、セキュリティ担当者の日常業務における悩みに対する具体的対応策を提示。プラクティスの拡充と、担当者が抱える課題を追加した**第３版を2022年3月30日に公表**。

＜特徴＞

「情報セキュリティの取組みはある程度進めてきたが、サイバー攻撃対策やインシデント対応は強化が必要。それに向けた体制づくりや対策は何から始めるべきか」と考えている経営者やCISO等、セキュリティ担当者を主な読者と想定し、ガイドラインの「重要10項目」を実践する際に参考となる考え方やヒント、実施手順、実践事例を掲載。

＜イメージ＞

累計20,995DL
（2022年5月末時点）

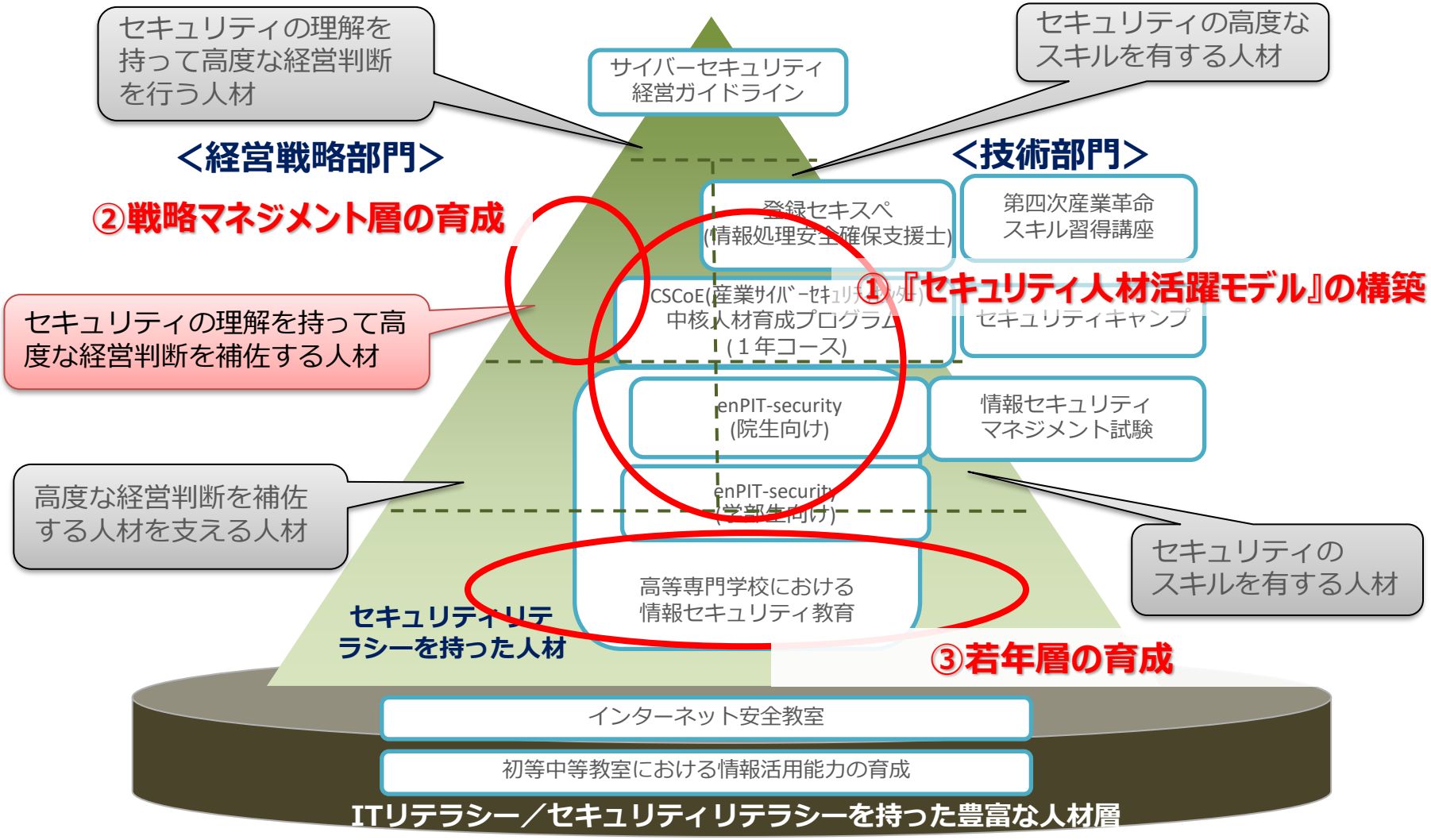
＜構成＞

- **はじめに**
- **第1章　経営とサイバーセキュリティ**
- **第2章　サイバーセキュリティ経営ガイドライン実践のプラクティス**
  サイバーセキュリティ強化のために実践していただきたいファーストステップを、重要10項目ごとにまとめて掲載。
- **第3章　セキュリティ担当者の悩みと取組みのプラクティス**
  事例の妨げとなる課題やセキュリティ担当者の悩みに対し、実際に試みられた工夫の事例を紹介。
- **付録**
  サイバーセキュリティに関する用語集
  サイバーセキュリティ対策の参考情報

https://www.ipa.go.jp/security/fy30/reports/ciso/index.html

サイバーセキュリティ人材育成・活躍促進パッケージの全体像

- **セキュリティ人材の定義や育成・活躍の在り方のモデルが不明確。**
- **「セキュリティの理解を持って高度な経営判断を補佐する人材」の育成が不十分。**
- 教育プログラム策定への貢献など、**産業界の教育への取組の強化が期待される。**



サイバーセキュリティ人材施策の全体像

- セキュリティを本務としない者が自らの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を実現できる能力を身につける「プラス・セキュリティ」の取組を推進するため、SC3での検討や地域での具体的な取組を推進している。

取組の全体像

セキュリティ対策を進めるための体制・人材の考え方

- セキュリティ体制構築・人材確保の手引き（「サイバーセキュリティ経営ガイドライン」付録F）

セキュリティ人材の育成

- ICSCoE中核人材育成プログラム
- 情報処理安全確保支援士
- セキュリティキャンプ

プラス・セキュリティの普及

- SC3産学官連携WGでのプラス・セキュリティ具体化
- NISCにおけるモデルカリキュラム策定
- 地域SECUNITYにおける人材育成

- デジタル人材育成プラットフォームにおけるスキル標準の整理・教育コンテンツ・実践型教育
- 大学・高専等と産業界の連携

今後の方向性

- 手引きの普及による各企業での体制構築の促進と各種セキュリティ人材育成施策を引き続き実施するとともに、プラス・セキュリティの取組を普及させるため、SC3産学官連携WG、デジタル人材育成プラットフォーム、各地域における産学官連携の取組（地域SECUNITY）との連携による取組の具体化・拡大を進めていく。

① 『セキュリティ人材活躍モデル』の構築

② 戦略マネジメント層の育成

③ 若年層の育成

サイバーセキュリティ経営ガイドラインの全体像における手引きの位置付け

企業におけるサイバーセキュリティ対策の推進において、その基盤となる下図の赤枠部分（「リスク管理体制の構築」と「資源（予算、人材等）の確保」）は経営者が積極的に関わって実践すべき取組。『サイバーセキュリティ体制構築・人材確保の手引き』はその具体的検討のための参考文書。※

※ 指示３のうち予算の確保に関する内容は含みません。

経営者が認識すべき３原則

1. 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進め、最終責任者として対応することが必要
2. 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要
3. 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

経営者の積極的な関与のもとで実践

対外的にどの役職者が対応するのかも経営層の判断事項

ACT

PLAN

DO

CHECK

経営者がCISO等に指示すべき10の重要事項（①～⑩）

①サイバーセキュリティ対応方針策定

②リスク管理体制の構築

サイバーセキュリティ
リスク管理体制

◆経営リスク委員会等
他の体制と整合
（ex.内部統制、災害対策）

自社の状況に応じた役割の割当、権限の付与

CISO等の担当幹部・
戦略マネジメント層

セキュリティ担当、CSIRT等
実務者・技術者層

③資源（予算、人材等）の確保

④リスクの把握と対応計画策定

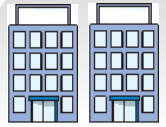
⑤保護対策(防御・検知・分析)の実施

⑥PDCAの実施

⑦緊急対応体制の整備

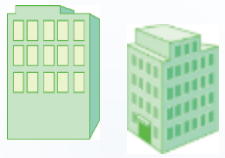
⑧復旧体制の整備

内外に宣言・開示



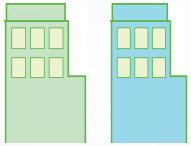
ステークホルダー
（株主、顧客、取引先等）

⑨サプライチェーン
セキュリティ対策



ビジネスパートナー

⑩情報共有活動
への参加



情報共有団体
・コミュニティ

「サイバーセキュリティ体制構築・人材確保の手引き」のポイント

- 手引き書における各項のポイントは次のとおり。
- 責任に見合った権限の付与が重要。特に「プラス・セキュリティ」（＝下表下線部）は組織内における役割の自覚の観点からも重要。

「サイバーセキュリティ体制構築・人材確保の手引き」における検討のポイント

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** **サイバーセキュリティに関して「やるべきこと」の明確化**	①自社で対処すべきサイバーセキュリティリスクを認識し、そのリスクを低減するために具体的に「やるべきこと（タスク）」を明確化していく。 ②ITSS+（セキュリティ領域、次ページ参照）なども参考にしながら、負荷が大きい部分はスモールスタートから始め、継続的に改善する。
	2.2 **セキュリティ統括機能の検討**	① 組織内でサイバーセキュリティ機能をうまく働かせるには、CISO等の経営層を補佐する「セキュリティ統括機能」（次ページ参照）を設置すべき。 ② セキュリティ統括機能には大きく4つの類型があり、自社の状況に合わせて検討する。
	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**	① サイバーセキュリティ体制の具体的な構築にあたっては、ITSS＋（セキュリティ領域）を参考にすることで、関係部署や委託先の役割が明確になる。 ② 実際のところほとんどの企業においてサイバーセキュリティに関する機能の一部を外部委託することが適切であるが、丸投げではない適切な役割分担と、品質の担保されたサービスの選定が重要である。
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** **セキュリティを主たる業務とする人材の確保**	① 外部委託を積極活用していても、サイバーセキュリティリスクの把握と対策を推進する自社要員を割り当てる必要があり、当該人材には役割に応じた知識・スキルが求められる。 ② サイバーセキュリティに関する専門性を有する人材は不足状態にあり、確保には工夫が求められる。
	3.2 **「プラス・セキュリティ」の取組推進**	① 事業部門、管理部門等においてそれぞれの業務に従事する人材が、DX等のデジタル活用を進めるなかで**セキュリティを意識し、業務遂行に伴う適切なセキュリティ対策の実施やセキュリティ人材との円滑なコミュニケーションに必要な能力を育成する**「プラス・セキュリティ」の取組が欠かせない。 ②「プラス・セキュリティ」を担う人材に自らの役割と責任の自覚を促すための意識付けを行う。
	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**	① 各分野に求められる知識・スキルを踏まえ、教育プログラムや試験・資格の活用を検討する。 ② 自社に必要な人材の配置計画をもとに、キャリアデザインを含めた育成計画を検討する。

本書で扱う主要な概念の解説

セキュリティ統括機能

- 企業におけるリスクマネジメント活動の一部として、セキュリティ対策及びセキュリティインシデント対応について、CISOや経営層による意思決定や、事業部門におけるセキュリティ対策の検討及び実施について、専門的な知見や経験をもとにサポートする機能
- 経営層や各事業部門は、セキュリティ統括機能によるサポートを受けつつ、それぞれが責任を負うセキュリティ対策を実践する。
- 「機能」であって「組織」として設置しなくてもよい（企業組織の状況に応じて、最適な形態は異なる：以下は設置方法の例）
  - 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

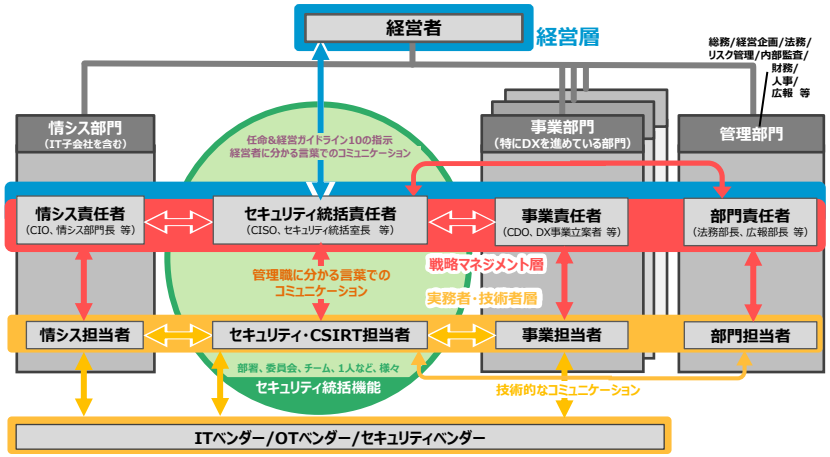
ITSS+（セキュリティ領域）

- 企業のセキュリティ対策に必要となる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している
- DXの取組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、各分野の境界は曖昧化の傾向にある

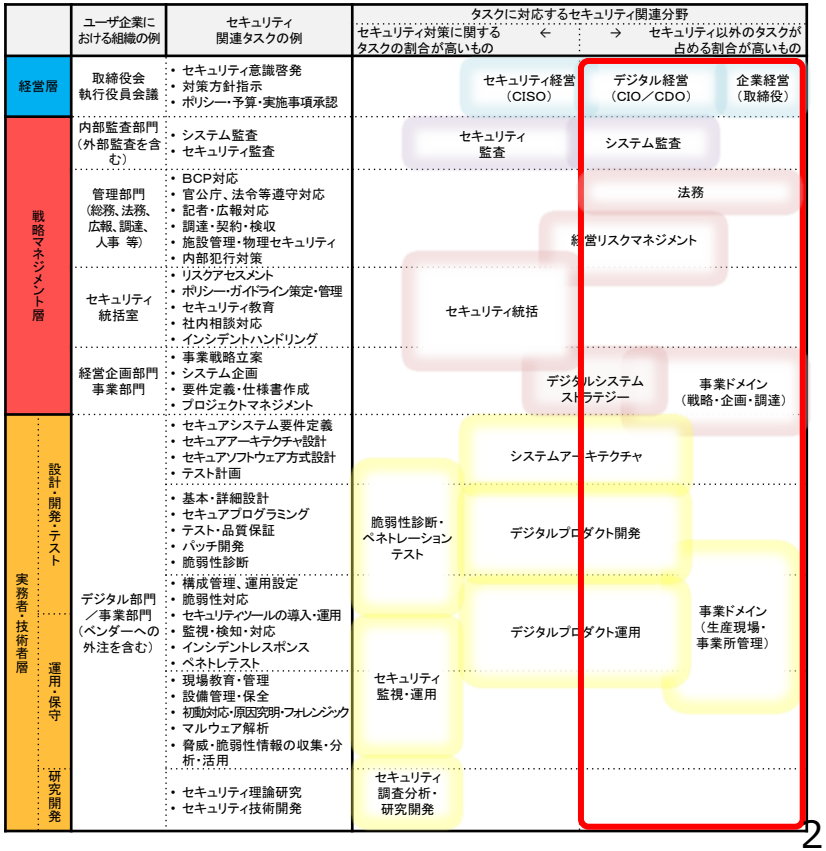
プラス・セキュリティ

- 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」という人材が業務担当者と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
- DXの取り組み有無に関わりなく、ITを活用するすべての企業において実践すべき

セキュリティ統括機能のイメージ



ITSS＋（セキュリティ領域）（赤枠が「プラス・セキュリティ」の分野）



『サイバーセキュリティ体制構築・人材確保の手引き』

- 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。**
- 各組織における検討の流れをステップ・バイ・ステップで整理した**第2.0版を2022年6月15日に公表。**

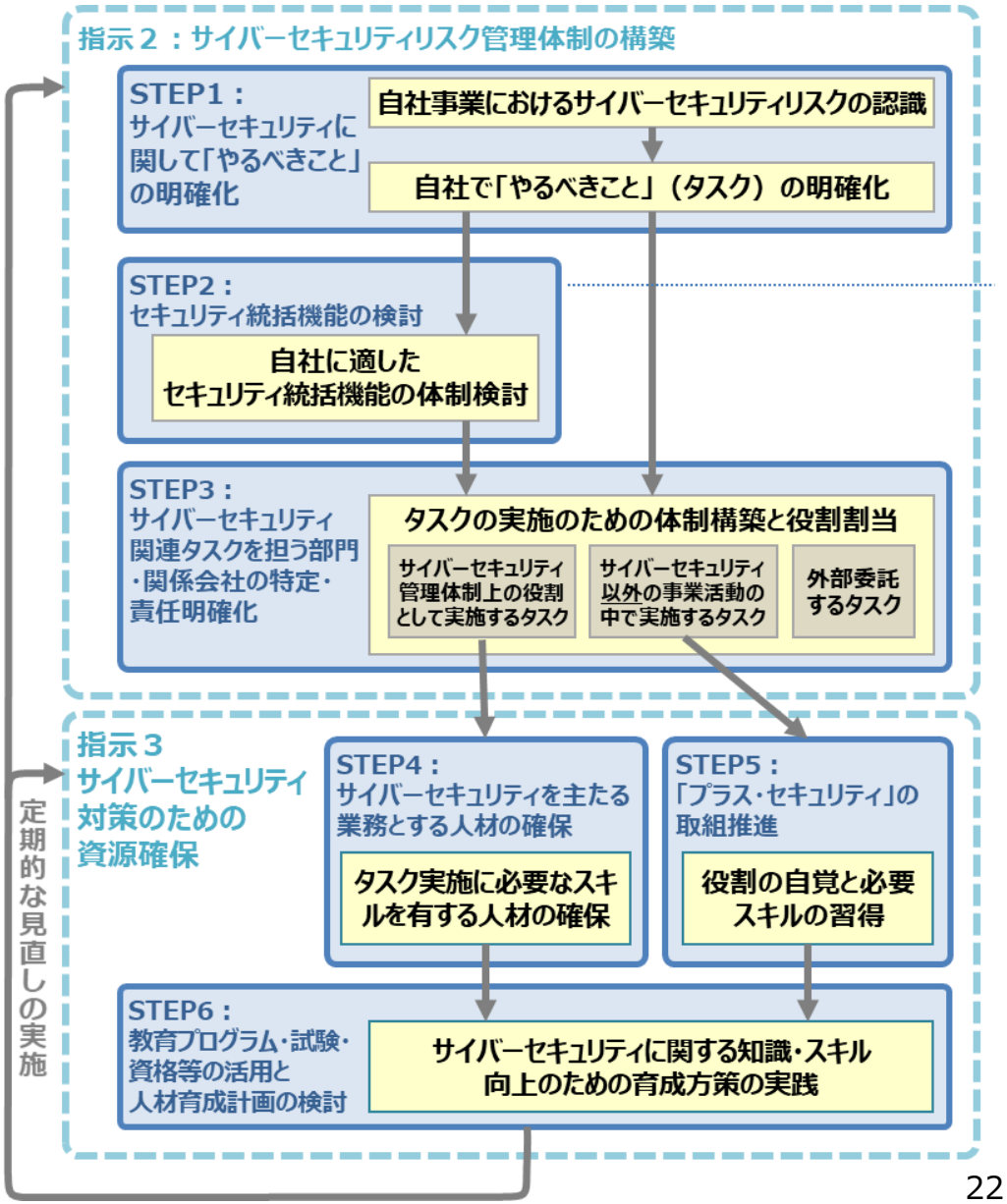
- 2020年9月30日策定、2021年4月15日改訂（Ver.1.1）
- 2022年6月15日改訂（Ver2.0）

第2.0版での更新の主なポイント

- 読みやすさを重視し、step by stepでポイントを記載。
- ITSS+（セキュリティ領域）について、プラス・セキュリティの重要性の増加等を踏まえ、「セキュリティ」「デジタル」「その他」の3分類からセキュリティタスクが占める割合のグラデーションでの表現に変更。
- 人材育成計画について、OT分野とプラス・セキュリティにフォーカスして詳細に解説。

経営者のリーダーシップの下、
手引きのポイントを参照しながら、
適切な体制を検討

検討を実践を効率的に進めるための手順



【STEP1】サイバーセキュリティに関して「やるべきこと」の明確化

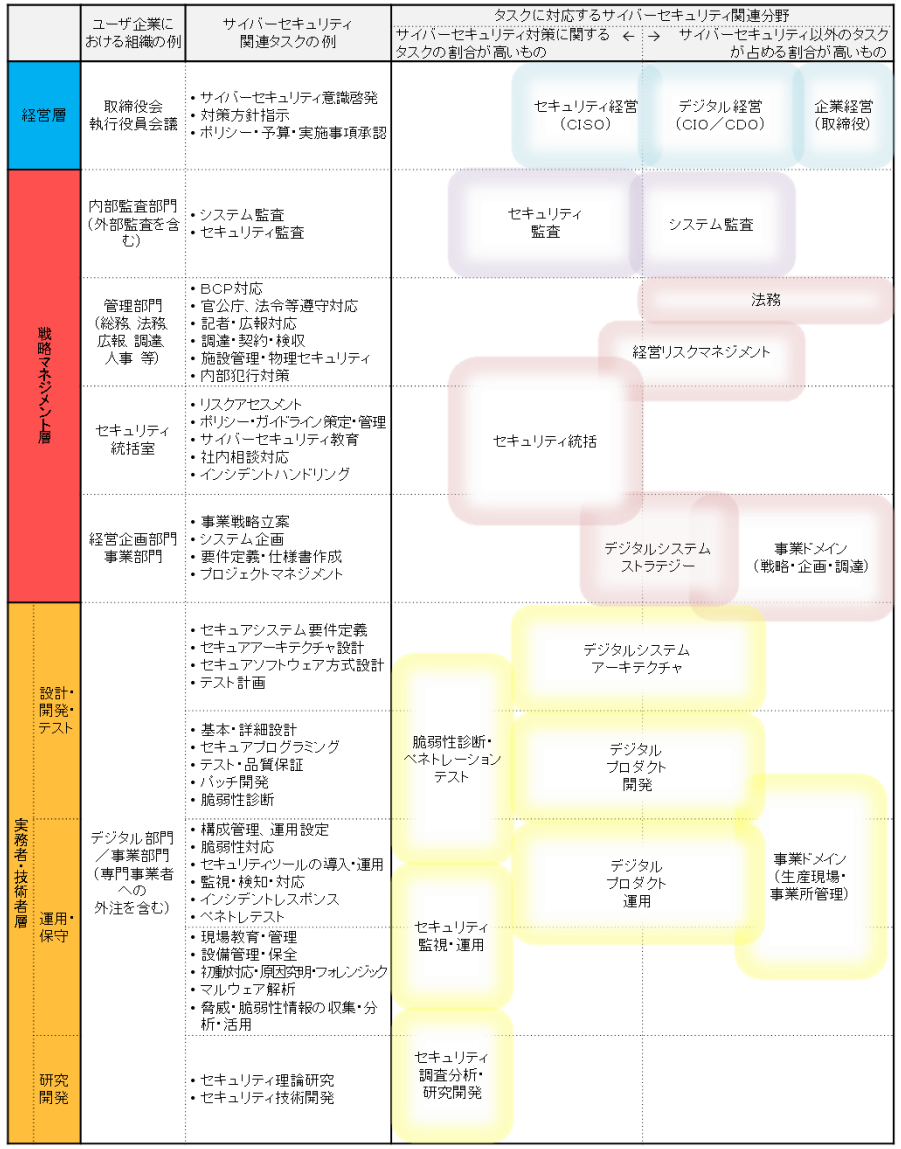
ポイント：
- 自社で対処すべきサイバーセキュリティリスクを認識
- 「やるべきこと（タスク）」を明確化
- ITSS+を用いたタスクの洗い出し
  ※負荷が大きい部分はスモールスタートからはじめ、継続的に改善

サイバーセキュリティに関して自社で具体的にやるべきことの洗い出し手順

	＜具体例＞	＜ポイント＞
①サイバーセキュリティリスクの認識	● マルウェア感染による事業停止 ● 認証不備による情報漏えい ● 内部不正	● デジタル環境活用に伴う事故として、自社で責任もって防ぐべき脅威を抽出します。 ● IPAで簡易的な方法を公表しています。
②実現すべきサイバーセキュリティ機能の明確化	● 自社のIT資産の保全 ● 異常の検知 ● 関係者との調整	● 既存のフレームワークを活用しつつ、必要に応じて追加等を検討します。
③具体的にやるべきこと（タスク）の洗い出し	● IT資産における構成管理 ● 脆弱性対応の実施	● まずやるべきことを洗い出して、次にそれをどこで担当するか割当を検討します。

ITSS+を用いたタスクの洗い出し

ITSS＋（セキュリティ分野）

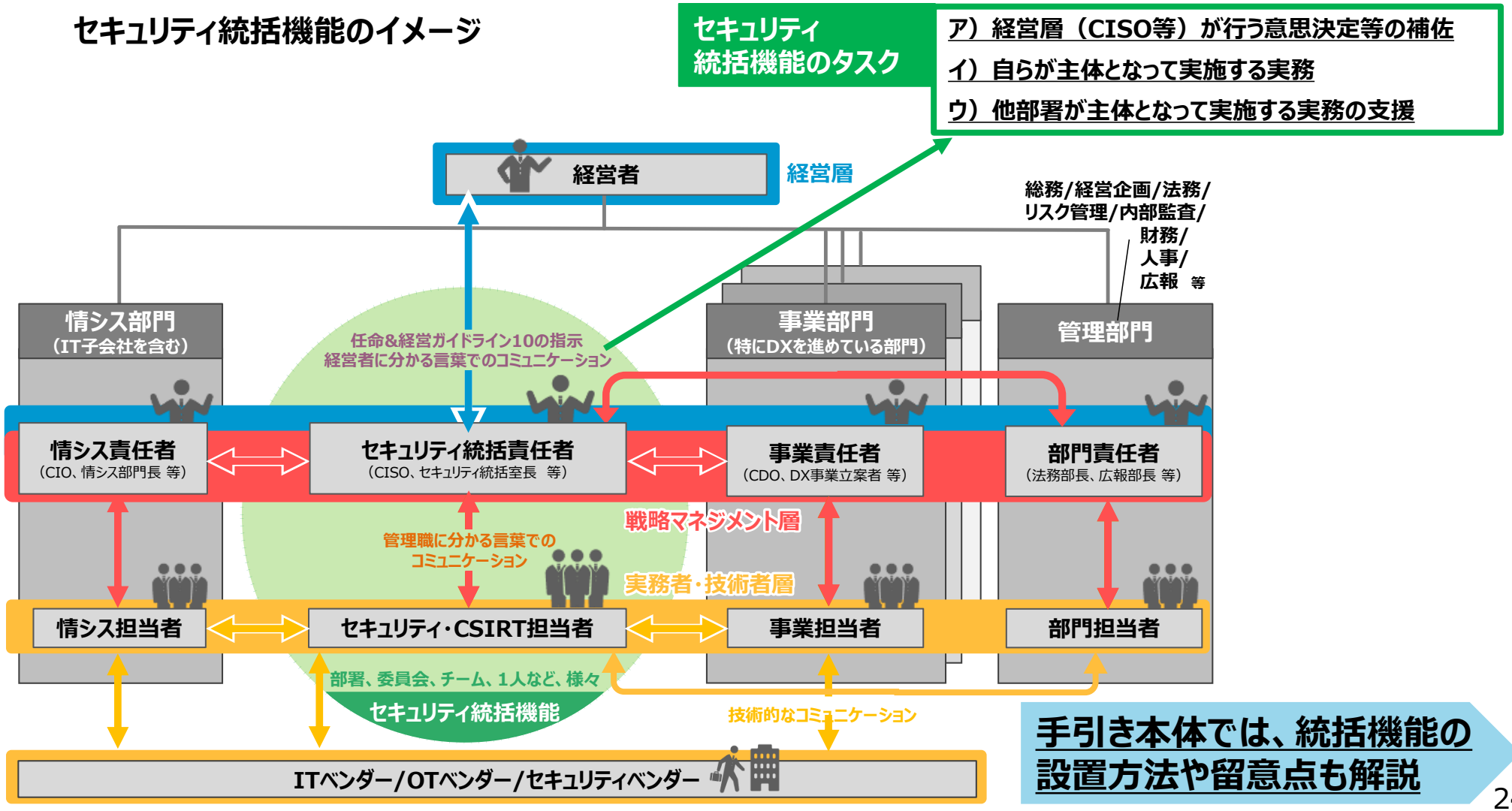


手引き本体では、詳細なタスク例なども例示

【STEP2】セキュリティ統括機能の検討

ポイント：
- CISO等の経営層を補佐する「セキュリティ統括機能」の設置
- セキュリティ統括機能の形態には大きく４つの類型 自社の状況に合わせて検討
（ 専門組織型or委員会型 / 集権型or連邦型 ）

セキュリティ統括機能のイメージ



手引き本体では、統括機能の設置方法や留意点も解説

【STEP3】サイバー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

ポイント：

- ITSS＋（セキュリティ領域）を参考に、セキュリティ統括機能と連携して、関係部署や委託先が、どのような役割を担うかを明確化
- サイバーセキュリティの脅威が高度化する中で、ほとんどの企業においてサイバーセキュリティに関する機能の一部を外部委託することが適切。丸投げではない適切な役割分担と、品質の担保されたサービスの選定が重要。

17分野のサイバーセキュリティ関連タスクと担当部署の割り当て例

	分野名	サイバーセキュリティ関連タスクの例	担当部署／機能の例（青字は社外委託先等）
経営層	セキュリティ経営（CISO） デジタル経営（CIO/CDO） 企業経営（取締役）	サイバーセキュリティ意識啓発、対策方針の指示、セキュリティポリシー・予算・対策実施事項の承認 等	経営者、経営層（CISOを含む）
戦略マネジメント層	セキュリティ監査	情報セキュリティ監査、報告・助言 等	監査部門 セキュリティ専門事業者・監査法人（情報セキュリティ監査サービス）
	システム監査	システム監査、報告・助言 等	監査部門 IT専門事業者・監査法人（システム監査サービス）
	セキュリティ統括	サイバーセキュリティ教育・普及啓発、サイバーセキュリティ関連の講義・講演、サイバーセキュリティリスクアセスメント、セキュリティポリシー・ガイドラインの策定・管理・周知、警察・官公庁等対応、社内相談対応、インシデントハンドリング 等	セキュリティ専門部門、CSIRT セキュリティ委員会 IT・デジタル部門のサイバーセキュリティ対策機能
	デジタルシステムストラテジー	デジタル事業戦略立案、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 等	経営企画部門、IT企画部門、IT・デジタル部門の企画機能 IT/セキュリティコンサルタント
	経営リスクマネジメント	経営リスクマネジメント、BCP／危機管理対応、サイバーセキュリティ保険検討、記者・広報対応、施設管理・物理セキュリティ、内部犯行対策 等	総務部門（リスク管理部門を含む） 経営企画部署、総務部署等のリスクマネジメント機能
	システム監査	システム監査、報告・助言 等	監査部門 IT専門事業者・監査法人（システム監査サービス）
	法務	デジタル関連法令対応、コンプライアンス対応、契約管理 等	法務部門、総務部門の法務担当
	事業ドメイン（戦略・企画・調達）	事業特有のリスクの洗い出し、事業特性に応じたサイバーセキュリティ対応、サプライチェーン管理 等	事業部門の企画機能 事業戦略コンサルタント
実務者・技術者層	脆弱性診断・ペネトレーションテスト	脆弱性診断、ペネトレーションテスト 等	IT・デジタル部門の運用機能、IT子会社 セキュリティ専門事業者（脆弱性診断サービス）
	セキュリティ監視・運用	セキュリティ製品・サービスの導入・運用、セキュリティ監視・検知・対応、インシデントレスポンス、連絡受付 等	IT・デジタル部門の運用機能、IT子会社 セキュリティ専門事業者（セキュリティ監視・運用サービス）
	セキュリティ調査分析・研究開発	サイバー攻撃捜査、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・技術の研究開発、セキュリティ市場動向調査 等	CSIRT/IT・デジタル部門のリサーチ機能、IT子会社 セキュリティ専門事業者（デジタルフォレンジックサービス）
	デジタルシステムアーキテクチャ	セキュアシステム要件定義、セキュアシステム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 等	IT・デジタル部門の設計機能、IT子会社 IT/OT専門事業者
	デジタルプロダクト開発	基本設計、詳細設計、セキュアプログラミング、テスト・品質保証、パッチ開発 等	IT・デジタル部門の開発・保守機能、IT子会社 IT/OT専門事業者
	デジタルプロダクト運用	構成管理、運用設定、利用者管理、サポート・ヘルプデスク、脆弱性対策・対応、インシデントレスポンス 等	IT・デジタル部門の運用機能、IT子会社 IT/OT/セキュリティ専門事業者
	事業ドメイン（生産現場・事業所管理）	現場教育・管理、設備管理・保全、QC活動、初動対応 等	運転、保全、計装、品質管理関連部署、PSIRT OT/セキュリティ専門事業者

【部署間での役割分担】
割当先部署に責任に伴う権限がない場合、他部署による協力が十分に得られず、対策が形骸化

【インシデント対応に備えた機能の確保】
組織内の情報システム等に加え、制御系システムの運用、顧客に販売した製品やサービスでのインシデント対応も視野に

【自社実施と外部委託の切り分け】
戦略マネージメント層以上で決定

手引き本体では、役割分担や外部委託の考え方も解説

【STEP4】 サイバーセキュリティを主たる業務とする人材の確保

ポイント：

- 外部委託を積極活用していても、自社の要員として自社のサイバーセキュリティリスクを把握し、その対策を推進する立場の人材を割り当てる必要あり
- 当該人材にはサイバーセキュリティに関するリスクと対策について理解するのに必要な知識・スキルが求められる
- サイバーセキュリティに関する専門性を有する人材は不足状態にあり、確保には工夫が必要

SETP4では、ITSS＋（セキュリティ領域）において、「セキュリティ経営（CISO）」、「セキュリティ統括」、「セキュリティ監査」、「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」の各分野を担う人材の確保方法を解説。

セキュリティを主たる業務とする人材を確保するための方法例

- リスクマネジメントや経営管理に関する業務経験を有する人材の配置転換及び育成
- ITの管理・運用に関する業務経験を有する人材の配置転換及び育成
- セキュリティ対策関連の業務経験を有する人材の中途採用
- セキュリティを専門とする教育機関を修了した人材の新卒採用
- 兼業や副業で従事する人材の活用

手引き本体では、それぞれの人材確保方法について、メリットや留意点なども解説

【STEP5】「プラス・セキュリティ」の取組推進

ポイント：
- 関連部門の人材が、サイバーセキュリティを意識し、業務遂行に伴うサイバーセキュリティ対策の実施に必要な能力を備えることができるようにする「プラス・セキュリティ」の取組も重要
- 「プラス・セキュリティ」を担う人材に自らの役割と責任の自覚を促すための意識付け

「プラス・セキュリティ」とは？
自らの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を実現できる能力を身につけること、あるいは身につけている状態のこと

例えば・・・以下のような担当者が「プラス・セキュリティ」を実装していないとこんなリスクが生じます。

クラウドを活用した新規事業を立ち上げるプロジェクトの企画担当者

目的にそぐわない不適切なクラウドを選定することや、シャドークラウド化による情報漏えいリスク

製品設計において組込ソフトウェアの機能仕様を設計する担当者

製品にサイバー攻撃に対する脆弱性を生じさせるリスク

自社の電話、インターネット設備、複合機等の保守契約を扱う総務担当者

不適切な設定のまま運用してしまうことによる、当該機器を介した情報漏えいリスク

手引き本体では、それぞれの人材確保方法について、メリットや留意点なども解説

【STEP6】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

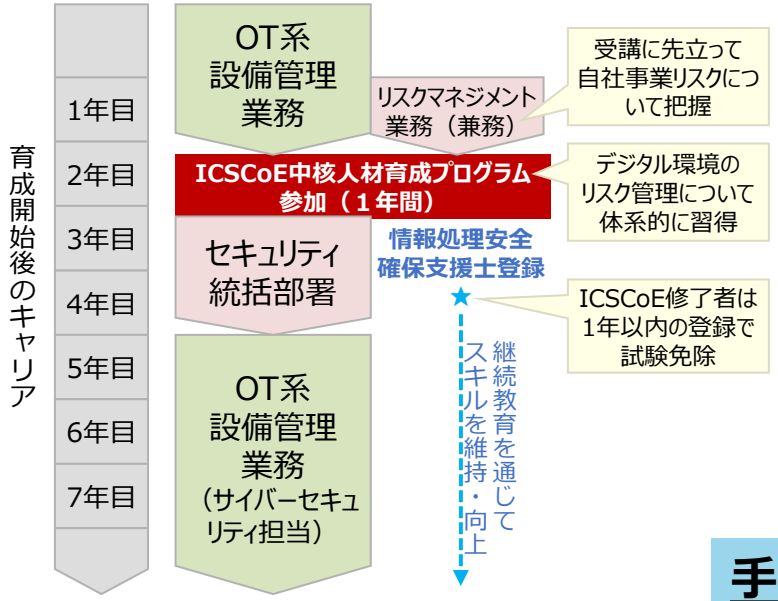
ポイント：
- 各分野に求められる知識・スキルを踏まえ、教育プログラムや試験・資格の活用を検討
- 自社に必要な人材の配置計画をもとに、キャリアデザインを含めた育成計画を検討

STEP6では、各分野に求められる知識・スキルの概観、教育プログラム・コミュニティ活動の活用、資格・試験制度の活用、人材育成計画の検討などについて解説。

人材育成計画の検討（事例）

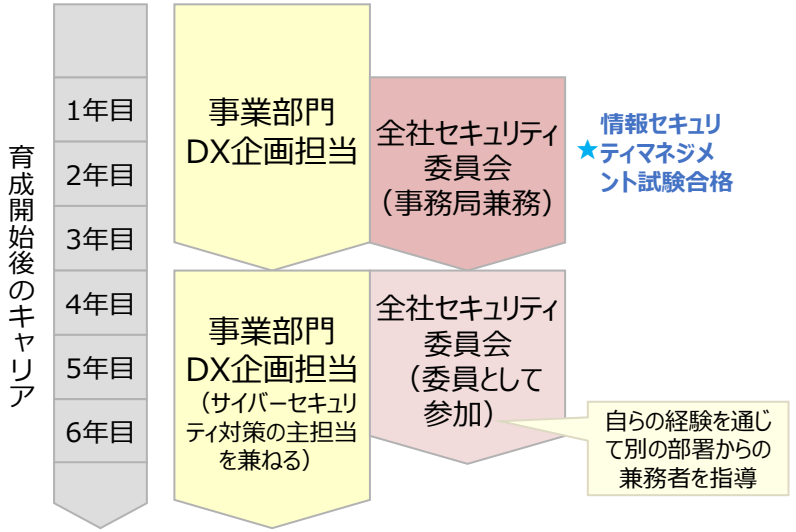
事例1：制御系設備全体のサイバーセキュリティ担当者の育成

工場におけるOT環境に通じた人材がサイバーセキュリティに関する技術とマネジメントを体系的に学び、将来的にOT環境のサイバーセキュリティ対策の中核メンバーとして活躍。ICSCoEで知識・スキルを習得した上で、自社のセキュリティ統括機能に配属。社内の対策に関する実務経験を積むことで効率的な育成を図る。



事例2：「プラス・セキュリティ」を身につけた人材の育成

DXを活用した事業の企画担当者が、そのサイバーセキュリティリスクの対処方針を立案・推進するために必要となる「プラス・セキュリティ」のための知識・スキルを習得するため、自社のセキュリティ統括機能を担う「セキュリティ委員会」の事務局業務を通じて実務経験を積む。



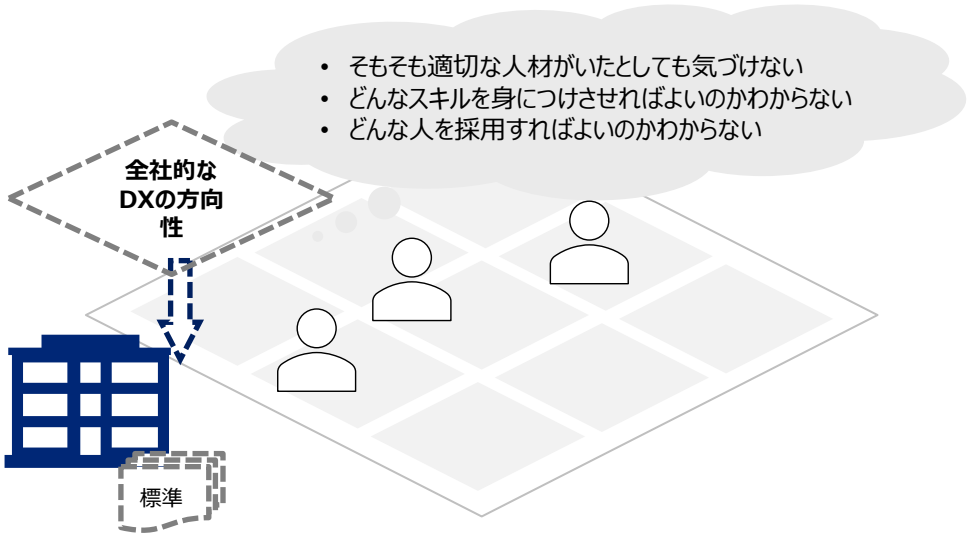
手引き本体では、具体的なプログラム・資格なども解説

DX推進スキル標準の必要性

- 日本企業がDXを推進する人材を十分に確保できていない背景には、自社のDXの方向性を描くことや、自社にとって必要な人材を把握することの難しさに課題があると考えられる。
- 各社がDXを通じて何をしたいのかというビジョン、その推進に向けた戦略を描いた上で、実現に向けてどのような人材を確保・育成することが必要になるか、適切に設定することが重要であり、「DX推進スキル標準」はそのための参考となる。しかし、スキル標準から戦略を描こうとすることや、スキルを闇雲に身につければDXが進むというものではないことには留意が必要である。

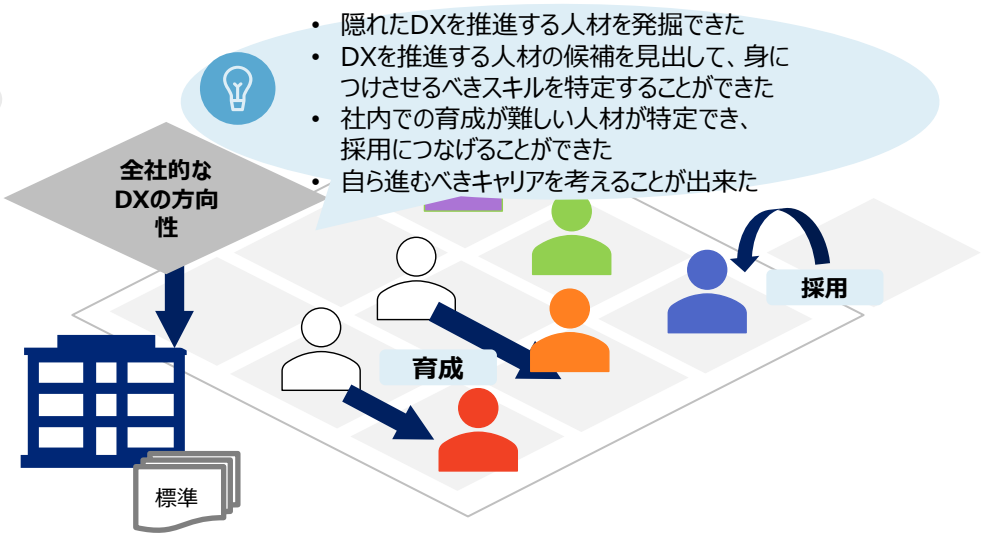
DX推進スキル標準がない場合（イメージ）

- 自社・組織にとって必要な人材の把握が難しいために、DXを推進する人材の確保・育成の取組みに着手できず、人材不足が課題となっている可能性がある



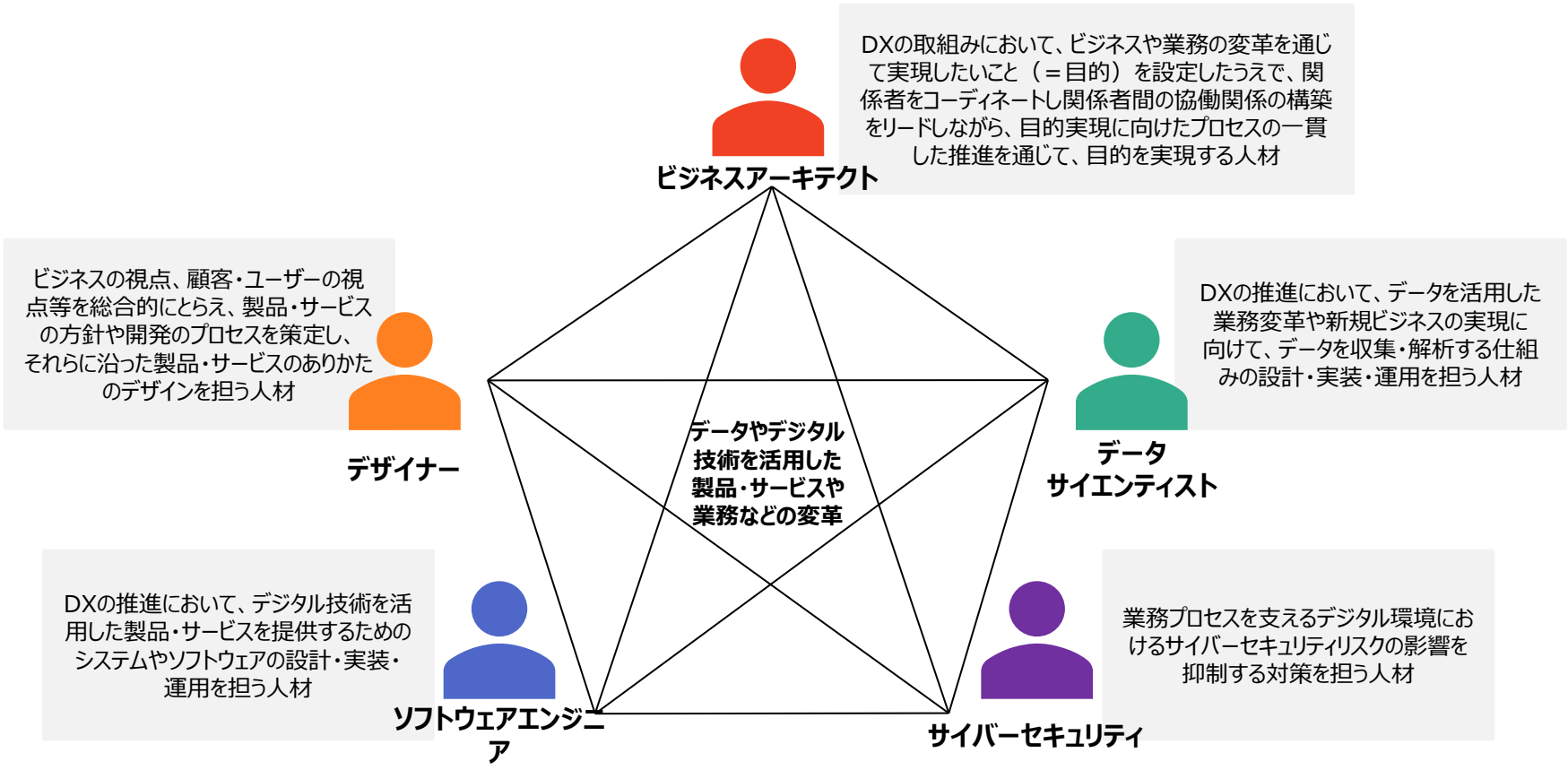
DX推進スキル標準がある場合（イメージ）

- 「DX推進スキル標準」を参考にすることで、自社・組織に必要な人材が明確になり、確保や育成の取組みに着手できている



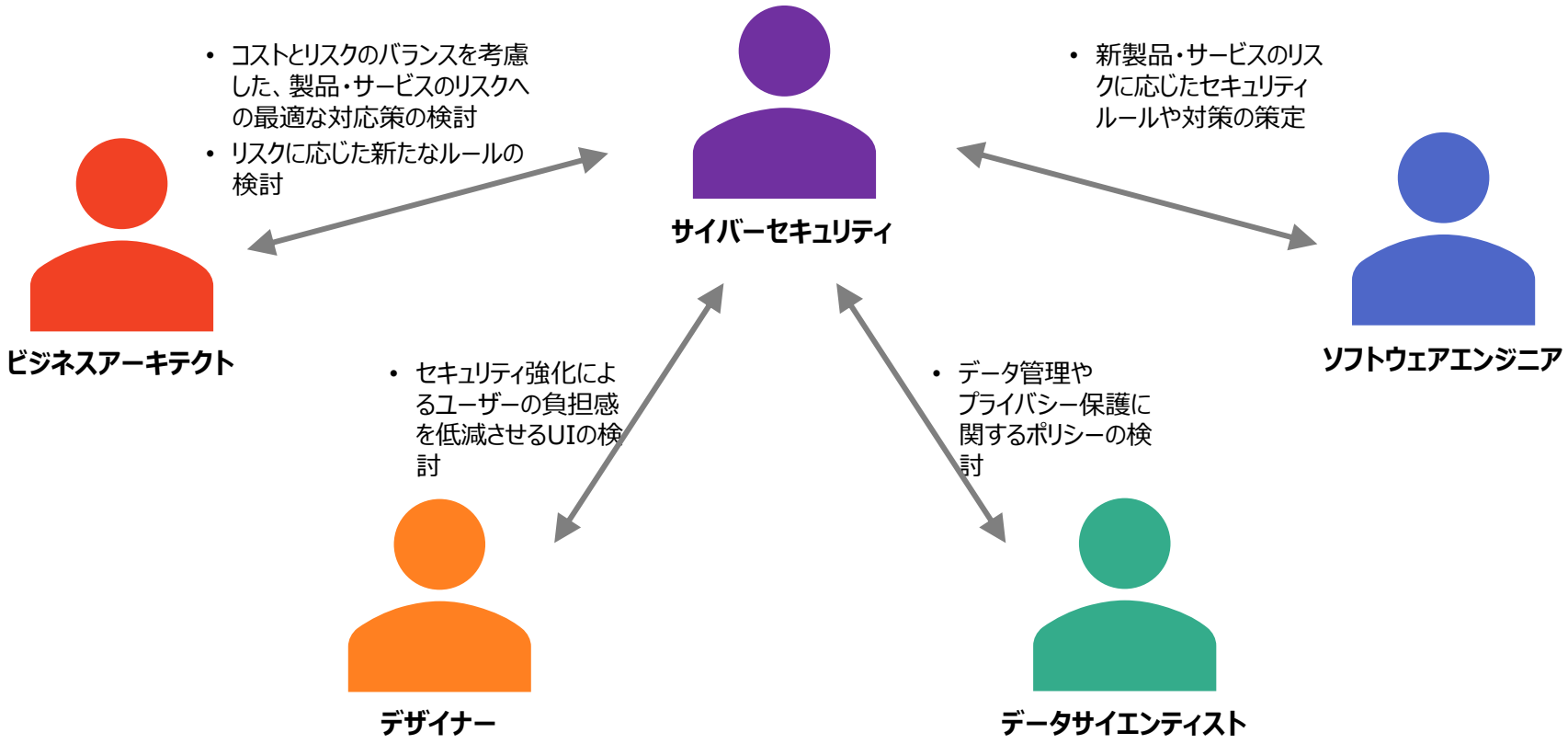
人材類型の定義

- DXを推進する主な人材として5つの人材類型を定義した。
- DXを推進する人材は、他の類型とのつながりを積極的に構築した上で、他類型の巻き込みや他類型への手助けを行うことが重要である。また、社内外を問わず、適切な人材を積極的に探索することも重要である。



サイバーセキュリティとは｜期待される役割

- 「サイバーセキュリティ」と他の人材類型が連携して進める業務の一例を示す。
- どちらかがどちらかに指示をする、又は依頼する、といった形ではなく、様々な場面で二つ（又はそれ以上）の類型が協働関係を構築することを示すために、類型間の関係性を双方向の矢印によって表現している。



参考：ソフトウェアエンジニアのロール｜担う責任・主な業務・スキルの例

人材類型	ソフトウェアエンジニア
ロール	**クラウドエンジニア／SRE（Service Reliability Engineering）**
DXの推進において担う責任	デジタル技術を活用したサービスを提供するためのソフトウェアの開発・運用環境の最適化と信頼性の向上に責任を持つ
主な業務	・デジタル技術を活用したサービスの利用者のニーズを理解し、利用者のニーズを実現するためのソフトウェアの開発・運用環境を実現する ・他の役割を担うソフトウェアエンジニアからのフィードバックを踏まえて、運用環境を最適化する ・サービス運用時に継続的なモニタリングを行い、その結果を踏まえて、サービスの信頼性向上に必要なシステム・ソフトウェア面での対応を行う

必要なスキル

カテゴリー	サブカテゴリー	スキル項目	重要度
ビジネス変革	戦略・マネジメント・システム	ビジネス戦略策定・実行	d
		プロダクトマネジメント	c
		変革マネジメント	d
		システムズエンジニアリング	c
		エンタープライズアーキクチャ	d
		プロジェクトマネジメント	b
	ビジネスモデル・プロセス	ビジネス調査	d
		ビジネスモデル設計	d
		ビジネスアナリシス	d
		検証（ビジネス視点）	d
		マーケティング	d
		ブランディング	d
	デザイン	顧客・ユーザー理解	d
		価値発見・定義	d
		設計	d
		検証（顧客・ユーザー視点）	c
		その他デザイン技術	d

カテゴリー	サブカテゴリー	スキル項目	重要度
データ活用	データ・AIの戦略的活用	データ理解・活用	b
		データ・AI活用戦略	c
		データ・AI活用業務の設計・事業実装・評価	c
	AI・データサイエンス	数理統計・多変量解析・データ可視化	c
		機械学習・深層学習	c
	データエンジニアリング	データ活用基盤設計	b
		データ活用基盤実装・運用	b
テクノロジー	ソフトウェア開発	コンピュータサイエンス	a
		チーム開発	b
		ソフトウェア設計手法	b
		ソフトウェア開発プロセス	b
		Webアプリケーション基本技術	b
		フロントエンドシステム開発	b
		バックエンドシステム開発	b
		クラウドインフラ活用	a
		SREプロセス	a
		サービス活用	c

カテゴリー	サブカテゴリー	スキル項目	重要度
テクノロジー	デジタルテクノロジー	フィジカルコンピューティング	c
		その他先端技術	c
		テクノロジートレンド	c
セキュリティ	セキュリティマネジメント	セキュリティ体制構築・運営	d
		セキュリティマネジメント	c
		インシデント対応と事業継続	c
		プライバシー保護	d
	セキュリティ技術	セキュア設計・開発・構築	b
		セキュリティ運用・保守・監視	a
パーソナルスキル	ヒューマンスキル	リーダーシップ	z
		コラボレーション	z
	コンセプチュアルスキル	ゴール設定	z
		創造的な問題解決	z
		批判的思考	z
		適応力	z

【重要度凡例】
a　高い実践力と専門性が必要
b　一定の実践力と専門性が必要
c　説明可能なレベルで理解が必要
d　位置づけや関連性の理解が必要
z　役割や状況に応じた実践力が必要

① 『セキュリティ人材活躍モデル』の構築

② 戦略マネジメント層の育成

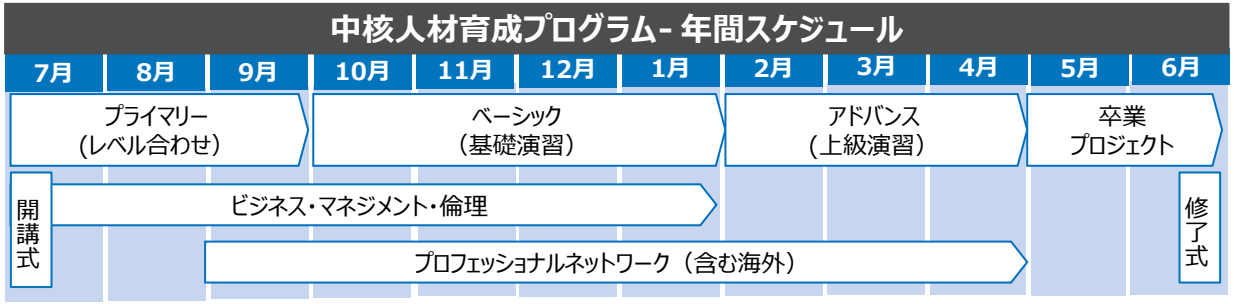
③ 若年層の育成

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6期中核人材育成プログラム（2022年7月開講）には、48名が参加。

ロ　１年を通じた集中トレーニング

ロ　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：46人、第5期：48人）



- 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

ロ　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

産業サイバーセキュリティセンター（ICSCoE）
中核人材育成プログラムにおける模擬プラントを含めた実践的施設（千石、秋葉原）

- 2017年4月、IPAに産業サイバーセキュリティセンターを設置。重要インフラの**セキュリティの中核を担う人材を育成**している。
- 電力、石油、ガス、化学、自動車、鉄道分野等の企業からセキュリティ担当者を1年間派遣させ、制御系セキュリティに精通する講師により、**実機を使った模擬プラントを実際に攻撃して脆弱性を洗い出すなどの実践的なプログラム**を実施している。

千石ー研修・演習施設

＜座学＞

＜基礎演習＞

秋葉原ー模擬プラント

＜実践的プログラム＞

攻撃

模擬プラントを攻撃

①発電模擬プラント

②機械製造模擬プラント

対策を検討

脆弱性を発見

模擬プラント全景

③鉄鋼圧延模擬プラント
④鉄道運行管理模擬プラント
⑤スマートグリッド模擬プラント
⑥施設管理模擬プラント
⑦車載システム
⑧熱資源活用制御システム

受講者

模擬プラント

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

【第４期生　2021年6月】（一部紹介）

➢ **ゼロトラストという戦術の使い方**
～情報系・制御系システムへのゼロトラスト導入～

「ゼロトラスト」で用いられる機能について、実際に環境を構築し、システムへの導入検証を実施。その検証結果と得られたノウハウを「ゼロトラスト導入指南書」としてまとめたもの。

➢ **現場向け制御セキュリティ教育：**
安全・安定操業を脅かした事例10選

近年国内外で発生した制御システムへのサイバー攻撃で、操業の安全・安心を大きく損なった10の事例を、影響の大きい順に紹介。事例の紹介に留まらず、発生する可能性がある被害について解説。

https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project.html

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（11月）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。
- 商工会や地銀と連携、会報や業界紙にセキュリティの啓発記事を掲載。

●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2022に基づき、IPA産業サイバーセキュリティセンターでは、2022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。
  - NISCも「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」の開催、「プラス・セキュリティ」知識を補充するモデルカリキュラムの策定といった取組を推進。

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」

- 2022年11月-12月実施（2018年度から5回目）
- 企業の**「セキュリティ統括責任者」である部課長級の方々**（戦略マネジメント層）、**今後責任者になることが期待される実務者・技術者**、**「プラス・セキュリティ」人材を対象**に、ビジネスのデジタル化・DXに伴うリスクの変化に対応して、組織のセキュリティ対策を推進する者の育成を目指す。
- 2022年度は対面形式の座学コースと、座学・演習コースで開講。座学は有識者講演・講義、演習は組織におけるセキュリティのあり方、課題と対策などをテーマにしたディスカッションで構成。

東京工業大学ＣＵＭＯＴ「サイバーセキュリティ経営戦略コース」

- 2022年11月～2023年3月
  ※新型コロナウィ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ワークショップ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14回実施。

サイバーインシデントに係る事故調査

- サイバー攻撃が現実空間にまで影響を及ぼすようになっていることを踏まえ、プラント等の事故が発生した場合に、**サイバーインシデントの観点からの原因究明調査**（「サイバー事故調査」）を実施。

事故調査のフロー（電力事故の場合）

電力事故発生

電気事業法第106条に基づく事故の報告

①電気関係報告規則に基づく事故の報告
・供給支障（停電等）を発生させた事故
・感電等による死傷事故、電気火災事故
・主要電気工作物の破損事故　等

24時間以内に経済産業大臣に報告しなければならない（30日後に詳細報告）

②①以外の事故で再発防止が特に必要なもの

経済産業大臣は報告を求めることができる

経済産業大臣

報告の結果、サイバーセキュリティに関する重大な事態

電気事業法第105条の２に基づき、サイバーの観点から調査を依頼

産業サイバーセキュリティセンター

ログ(通信履歴)の情報等をもとに事故原因を究明

調査結果を踏まえて、事業者全体のサイバーセキュリティ水準の向上を図るための対策を講じる

＜参考＞改正電気事業法（2022年６月成立）

（調査の要請）

第105条の2　経済産業大臣は、認定高度保安実施設置者その他の保安の確保上特に重要な者として経済産業省令で定める者において保安に係るサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）に関する重大な事態が生じ、又は生じた疑いがある場合において、必要があると認めるときは、独立行政法人情報処理推進機構に対し、その原因究明のための調査を要請することができる。（※）高圧ガス保安法、ガス事業法にも同旨の記載。

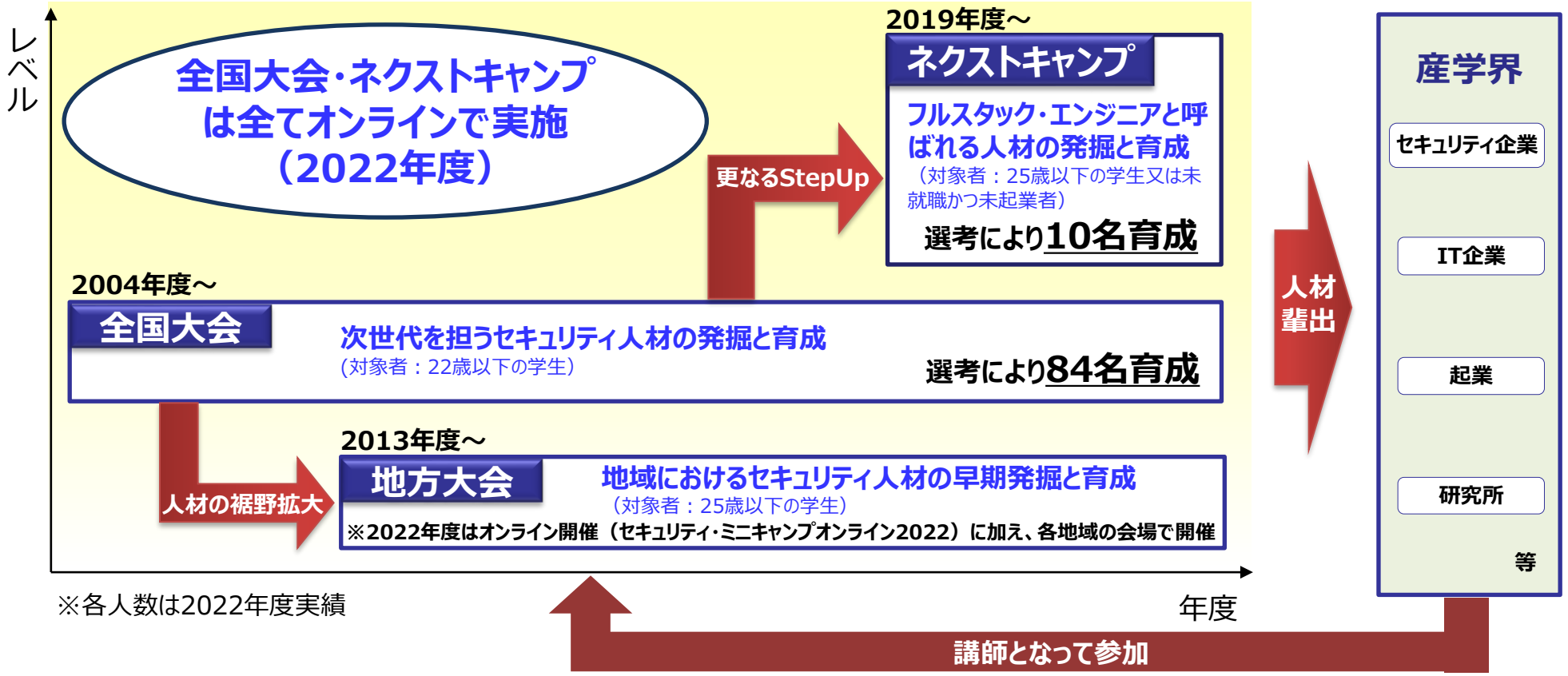
① 『セキュリティ人材活躍モデル』の構築

② 戦略マネジメント層の育成

③ 若年層の育成

セキュリティ・キャンプの概要

- 複雑かつ高度化しているサイバー攻撃に適切に対応するため、**若年層のセキュリティ人材発掘の裾野を拡大し、世界に通用するトップクラス人材を創出**することが必要。
- IPAとセキュリティ・キャンプ協議会は、選抜された22歳以下の学生・生徒を対象とした、次代を担う情報セキュリティ人材発掘・育成する「**セキュリティ・キャンプ全国大会**」を開催。**最新ノウハウも含めたセキュリティ技術を、倫理面と併せ、第一線の技術者から伝授**。**2004年度の開始**からこれまでに、累計で**1,073名**が修了。
- 2019年度からは、全国大会修了生の次のステップとして、選抜された25歳以下の学生・生徒等を対象とした、**情報セキュリティの多様なシーンに対応し新たな価値を生み出していけるトップオブトップの人材（フルスタック・エンジニア）を発掘・育成する「セキュリティ・ネクストキャンプ」**を開催。これまでに累計で**33名**が修了。



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）＞

国立高専機構と産・官との連携促進・具体化

- METI、IPA、JPCERT及び業界団体が国立高専機構と連携し、高専生の専攻（セキュリティ、IT、その他（機械、電気等））に応じた教育コンテンツの提供や講師の派遣等、産学官連携の具体化を推進中。

使用できるインフラ
- 演習設備
- 同時中継
  (全国高専間で配信可)
- 仮想空間

セキュリティスキルレベル

国立高専卒業生 約1万人/年の内訳	コンテンツ開発・授業の提供（パワーポイント、ビデオ等）	セキュリティ合宿に関する協力
約1% トップガンの学生 → 主に**セキュリティ企業**に就職	※トップガンの学生は、全国各校、各学科に散らばっているため、通常の授業時間で集合する機会がない。	・**高専機構がJNSAに講師派遣を依頼できる体制を構築。** ・**METIがセキュリティ専門官を高度セキュリティ合宿に講師として派遣。**
約20% 情報系学科の学生 → 主に**IT企業**に就職	・**JNSAのゲーム形式教材を石川高専と連携してアプリ化。** ※JNSA：NPO日本ネットワークセキュリティ協会 ・**JNSAがオンライン授業環境を利用した現場第一線講師による最新事例授業の開催検討中** ※一度に数十校を対象に同時開催可能。JNSAで実施中の岡山理科大学遠隔授業内容を最新事例中心に発展・展開。 ・**高専機構が四国地域企業のIPA ICSCoE修了生に講師派遣を依頼できる体制を構築。** ・**日立製作所が一関高専生向けに出前授業、インターンシップを実施し、出前授業は全国各校に配信。**	・**JNSAとSECCONビギナーズを石川高専と苫小牧高専で開催。** ・**JNSAがCTFビギナーズfor高専生@木更津高専に講師を派遣。** ・**IPAが高度セキュリティ合宿に講師を派遣し、App Goat（脆弱性体験学習ツール）の講習会を開催。** ・**METIがセキュリティ専門官を高知高専に派遣し、出前授業を実施。**
約80% 非情報系学科の学生 → 主に**ユーザー企業**に就職	・**CRICが高専機構と連携し、業界別（例．機械、電気、建築等）ビデオ教材（20分程度）を作成。** ※CRIC：一般社団法人サイバーリスク情報センター	※セキュリティ合宿のような機会は特段なし。
KOSEN 国立高専専門学校機構 国立高専教員	・**JNSAが教員向けのセキュリティ基礎講座の実施を検討中。** ※神奈川県での高校教員向けセキュリティ基礎講座の実績を展開。	・**IPAが教員向けにAppGoat講習会を開催。** ・**JPCERT/CCが情報担当教員向け研修に講師を派遣。** ・**教員がIPAのセキュリティキャンプ全国大会を見学。** ・**高専機構が、教師向け合宿の機会に、METIにセキュリティ専門官の講師派遣を依頼できる体制を構築。**

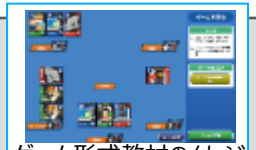
パターン①：90分程度
・高専教員がコンテンツを使って講義 又は 企業等の方が講義
(拠点校から全国各校に同時配信も可)

パターン②：15分程度
授業冒頭や隙間時間でビデオ放映

高度セキュリティ合宿（1泊2日）
年2回程度開催（インシデント対応演習等）参加者：35名程度

KOSENセキュリティコンテスト（1泊2日）
年1回程度開催（CTF）参加者：130名程度

※開催期間中の一部の時間を利用して、一線で活躍するホワイトハッカーから講義を実施可能。


ゲーム形式教材のイメージ


開催の様子@石川高専

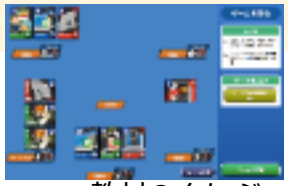

AppGoat講習の様子

（参考）産学連携によるセキュリティ人材育成

- **IPA・産業界が高専に講師を派遣**し、産官が高専のセキュリティ人材を具体的に支援中。
- 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（「**地域SECUNITY**」）の形成を全国において推進。
- 地域間の情報共有や、共通課題の解決に向けた取組の検討／推進を行うため、**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**において、地域間の連携を図るなど、各地の取組をさらに促進中。

高専との連携

- **産業界が教材作成や出前授業、インターンシップ等**を実施。
- **IPA等**が教員向けの講習会に**講師を派遣**。


教材のイメージ


石川高専への講師派遣

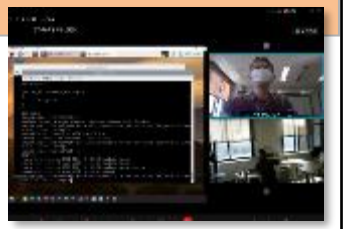
各地域での活動例

北海道の取組（北海道地域情報セキュリティ連絡会（HAISL））

- 経済産業局、総合通信局、道警察の3機関が、**北海道大学等と連携**。
- 道内在住の**学生等を対象にサイバーセキュリティの基礎的な知識を学ぶ勉強会**を開催。（2021年5月～8月に3回開催）

中国地域の取組（中国地域サイバーセキュリティ連絡会）

- 経済産業局、総合通信局が、**岡山大学、広島市立大学等と連携。**
- **地域中小企業との共同研究**や、**中小実務者向けの実践的なオンライン演習等**を含んだ講座等を実施。


オンライン実践演習

活動の横展開

- **各地域のベストプラクティス・課題を共有するワークショップの開催**

ご清聴ありがとうございました。
ご質問等ございましたら、下記の連絡先までお願いします。

経済産業省　商務情報政策局　サイバーセキュリティ課
佐藤 秀紀
sato-hidenori@meti.go.jp

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html


METI
Ministry of Economy, Trade and Industry