経済産業省

資料３

事務局説明資料

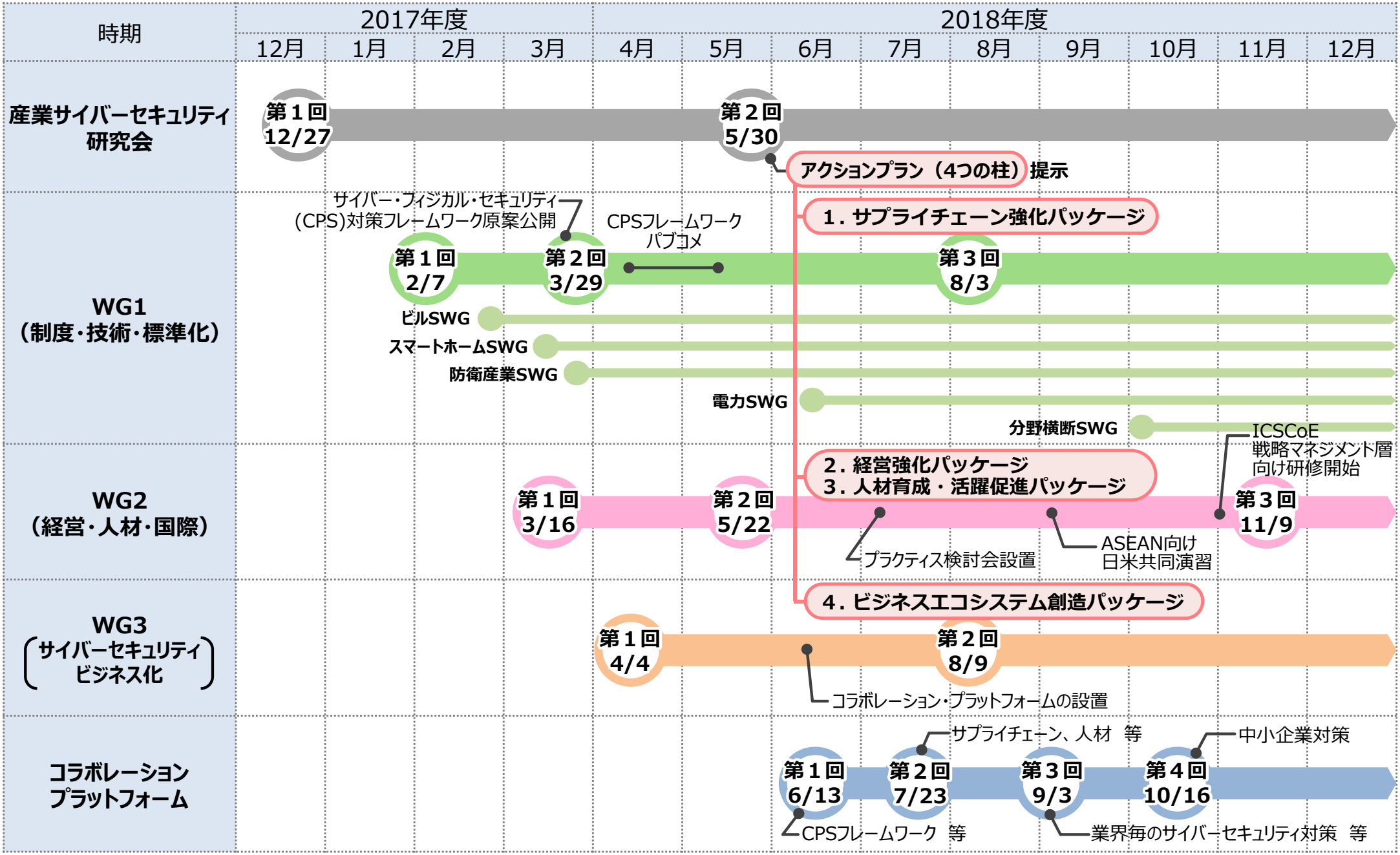
経済産業省

商務情報政策局

サイバーセキュリティ課

産業サイバーセキュリティ研究会の開催状況

- 産業サイバーセキュリティ研究会で政策全体の方向性を提示し、各WGで詳細な議論を実施。各WGを通じて顕在化したニーズとシーズをコラボレーションプラットフォームでマッチング。



ニーズとシーズをマッチングする『コラボレーション・プラットフォーム』の設置

- 各WGの活動などを通じて顕在化したニーズとシーズをマッチングする“場”となる**『コラボレーション・プラットフォーム』をIPAに設置し、6月から活動を開始。**

コラボレーション・プラットフォームの開催状況

- 各回、予定定員以上の申込みがあり、参加者からは政府との意見交換、最新動向の情報収集、人脈形成等、様々な視点で有益との声。

	日にち	参加人数(*)	主なテーマ
第一回	6月13日	179名（99名）	経済産業省の政策動向、パネルディスカッション（サイバーセキュリティビジネス、サプライチェーンセキュリティ）
第二回	7月23日	104名（74名）	IoTの発展に潜むリスクと対策、グループディスカッション（サプライチェーン、人材、つながる世界の脅威と対策）
第三回	9月3日	132名（69名）	経済産業省の新政策、企業の取り組み事例（資生堂）、グループディスカッション（業界別セキュリティ対策、セキュリティ検証基盤、サイバーセキュリティ経営）
第四回	10月16日	151名（56名）	中小企業におけるサイバーセキュリティリスク、ウイルス感染デモ、中小企業向けサイバーセキュリティ対策

(*)括弧内の人数はコラボレーション・プラットフォーム後に開催した情報交換会の出席者数


富田理事長(IPA)ご挨拶

三角審議官(経済産業省)ご挨拶


パネルディスカッション(第一回)


グループディスカッション(第二回)

コラボレーション・プラットフォームの今後の進め方

- 今後も参加者からより多くの意見を引出し、ビジネスマッチングの場として有効活用できるよう、テーマ、実施方法等について検討を重ねていく。

参加目的(*)	議論したい内容(*)
● ビジネスマッチング	● 産業IoT(Connected Industries)
● 人脈形成	● サプライチェーン
● 最近のサイバーセキュリティ動向の把握	● データ利活用・流通
● 自社のセキュリティ対策の向上	● 人材/教育
● 政策に対する意見表明　など	● 保険(サイバー保険、契約書保険条項)　など

結果をもとに今後の進め方を検討

開催頻度、参加人数
講演やディスカッションのテーマ
業種や参加目的を絞って開催を検討
地方開催の必要性

(*)コラボレーション・プラットフォームのアンケート結果より抜粋

１．経営

２．人材

３．国際

前回の主なご意見と今後の方向性

前回WGでの主なご意見	今後の方向性
（特に中小企業においては）セキュリティを意識すればするほどITを使わなくていいという考えになりイノベーションを止めることが懸念される。イノベーションのためにセキュリティが必要であるとのバランス感覚が重要。	・サイバー・フィジカル・セキュリティ対策フレームワーク －Society5.0、Connected Industriesを実現するためのセキュリティの取組と位置付け －レベル別の対策例も作成
保険会社の顧客は中小企業が圧倒的に多いが、中小企業はサイバー攻撃によるリスクを深刻に捉えていないところも散見される。	・コラボレーションプラットフォーム（中小企業編） ・中小企業サイバーセキュリティお助け隊の創設
サイバーセキュリティ経営ガイドライン等は具体性が不十分。「どこまでやるか」についてのモデルケースが充実するとよい。	・サイバーセキュリティ経営プラクティス検討会（IPA）
セキュリティに対する意識は企業規模、業種によって大きく異なることも念頭に置いた上で、プラクティス作りを進めた方がよい。	
可視化ツールについては一つの物差しで測るのはフィットしない可能性がある。様々な物差しで測ることができるとよい。	

サイバーセキュリティ経営における全体像

第二回WGの再掲

- 経営層向け、現場向け、中小企業向けの３つの視点で、サイバーセキュリティ経営を促進するための施策を検討。

経営層向け

サイバーセキュリティ経営ガイドラインを軸として経営者の意識向上を図るとともに、将来的にセキュリティの高い企業が投資家の評価を受けられる枠組みの構築を支援する。

現場向け

サイバーセキュリティ経営ガイドラインの実践規範となるプラクティスや、対策状況の可視化ツールの提供により対策の実行を支援する。

中小企業向け

サイバー保険との連動も検討しつつ、中小企業におけるセキュリティに関するトラブルの相談対応を支援する。

（１）経営層向けの施策

（２）現場向けの施策

（３）中小企業向けの施策

段階的なサイバーセキュリティ経営の実現

第二回WGの再掲

- 以下の3Stepにより、サイバーセキュリティ経営の定着を目指す。

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の普及・定着

2nd Step

サイバーセキュリティ経営の実践

- CGSガイドラインにサイバーセキュリティを反映
- IRの観点から、サイバーリスクを経営リスクとして認識・自己確認することの重要性を啓発
- 取締役会実効性評価の項目にサイバーリスクを位置づけ
- 投資家に対してもサイバーセキュリティの重要性を啓発

3rd Step

セキュリティの高い企業であることの可視化

- セキュリティの高い企業であることを投資家が評価できるようにするための、サイバーセキュリティ経営に関する情報の開示の在り方の検討

コーポレート・ガバナンス・システム（CGS）研究会における検討状況

- CGS研究会（第２期）において、子会社を含めた「グループガバナンス」の実効性向上等に向け、ベストプラクティスの収集整理を通じた検討を行っている。
- コーポレート・ガバナンス・システム（CGS） に関するガイドラインのとりまとめに向け、「守り」のリスク管理の一環として、サイバーセキュリティ対策を位置づけることを検討。

ＣＧＳ研究会（第二期）スケジュール
＜平成29年＞
第１回 （12/8） 問題意識、論点整理
＜平成30年＞
第２回 （1/16） 論点整理
第３回 （2/22） フォローアップ
第４回 （3/29） フォローアップ、中間整理①
第５回 （4/24） フォローアップ、中間整理②
第６回 （5/25） グループの全体設計、アンケート結果報告
第７回 （6/22） グループガバナンス「守り」の論点①
第８回 （7/24） グループガバナンス「守り」の論点②
第９回 （9/5） ＣＧＳガイドライン改訂案について 等
第10回（10/10）グループガバナンス「攻め」の論点
第11回（11/12）経営幹部の選任
第12回（12/13）経営幹部の報酬設計
＜平成31年＞
第13回（1/21） その他論点、とりまとめ骨子案
第14回（2/12） ガイドライン素案
第15回（3/15） ガイドラインとりまとめ

グループガバナンス「守り」の論点の議論

- サイバーセキュリティ対策を含むグループガバナンス「守り」の論点について、第2回産業サイバーセキュリティ研究会資料（アクションプラン）を紹介しつつ議論。
- サイバーセキュリティ対策についても、統括する取締役等を置き、現場から社長までのホットライン構築が必要との指摘があった。

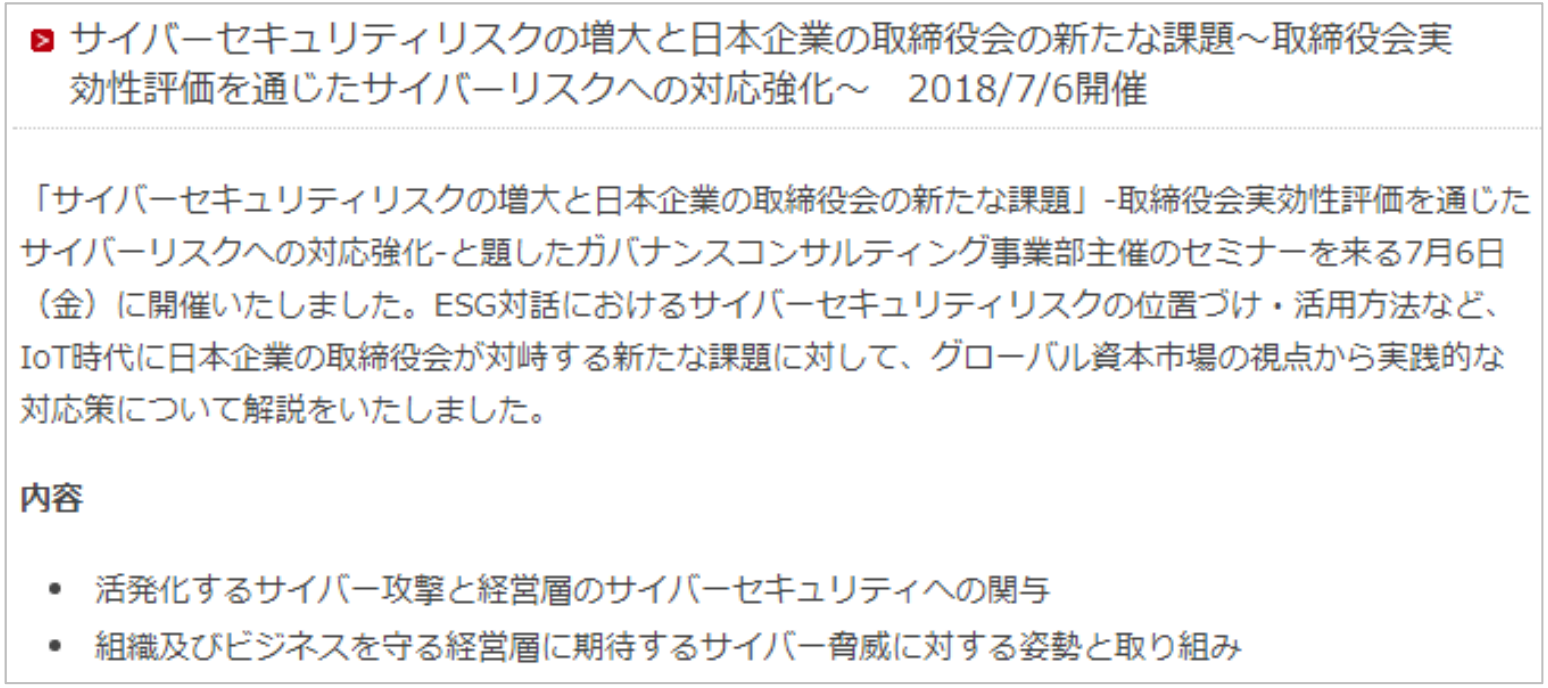
CGSに関するガイドラインのとりまとめ

CGSに関するガイドラインのとりまとめに向け、サイバーセキュリティを位置付けることを検討。

投資家向けの普及啓発活動

- コンサル会社（株式会社アイ・アールジャパン）が主催する投資家向けセミナーにて、サイバーセキュリティ対策の重要性について啓発を実施（2018/7/6開催、85名参加）。

講演内容	登壇者
サイバーセキュリティ経営ガイドラインを中心に、経営者視点でのサイバーセキュリティの重要性について解説	経済産業省　奥家
サイバーセキュリティを巡る日本企業の危機的実態について解説	サイバーディフェンス研究所　名和氏
投資家の視点からサイバーセキュリティリスクの対応についての日本企業への期待・要望	ブラックロック　江良氏



サイバーセキュリティリスクの増大と日本企業の取締役会の新たな課題～取締役会実効性評価を通じたサイバーリスクへの対応強化～　2018/7/6開催

「サイバーセキュリティリスクの増大と日本企業の取締役会の新たな課題」-取締役会実効性評価を通じたサイバーリスクへの対応強化-と題したガバナンスコンサルティング事業部主催のセミナーを来る7月6日（金）に開催いたしました。ESG対話におけるサイバーセキュリティリスクの位置づけ・活用方法など、IoT時代に日本企業の取締役会が対峙する新たな課題に対して、グローバル資本市場の視点から実践的な対応策について解説をいたしました。

内容

- 活発化するサイバー攻撃と経営層のサイバーセキュリティへの関与
- 組織及びビジネスを守る経営層に期待するサイバー脅威に対する姿勢と取り組み

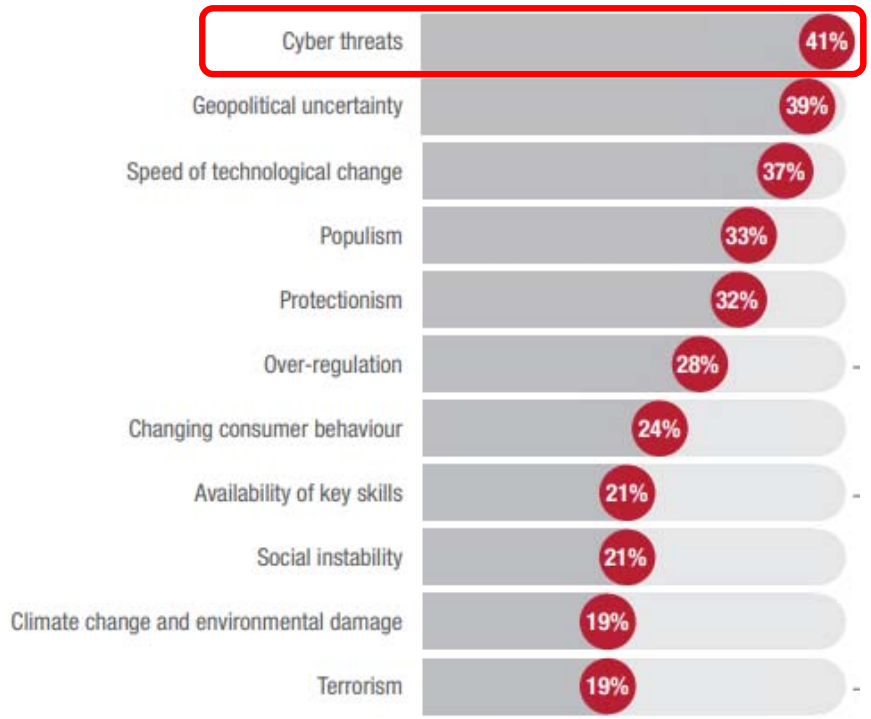
（出典）株式会社アイ・アールジャパン　実務者向けセミナー実績一覧より　https://www.irjapan.net/seminar/s_seminar.html#s_seminar_21

サイバーセキュリティ経営に関する米国の状況

- 投資家がサイバーセキュリティをビジネス上の大きな脅威と考えるようになっている。
- SECは、企業が投資家に適切なタイミングでサイバーセキュリティに関わる情報を開示すること促進。

2018 Global Investor Survey ＜PwC調査レポート＞

投資家が考えるビジネス上の脅威のトップはサイバーセキュリティ。



（出典）2018 Global Investor Survey（PwC）

Commission Statement and Guidance on Public Company Cybersecurity Disclosures＜SEC（米国証券取引委員会）＞

サイバーインシデントとリスクに関する情報開示等の指針を2018年2月に公開。
インシデントへの開示に関する手続きの整備や、インサイダー取引の禁止の重要性を強調。

本指針は法的強制力はないものの、投資家への影響が大きいインシデントの不開示についてはSECから摘発された事例あり。
（事例：米の情報通信業が大規模な情報漏えいを起こした際、インシデントに関する情報開示を怠ったとして、SECが当該企業を摘発し、3,500万ドルの罰金を課した）

（参考）英国の投資家団体の動向

- 英国の投資家団体であるThe Investment Association（IA）とKPMGは、サイバーセキュリティに投資することを経営層に求める報告書（Building Cyber Resilience in Asset Management）を作成。
- IAはこれらの取組を支援するために、企業、規制当局、公的機関と協力してCyber Security Committeeを設立。

英国の投資家は、経営層がサイバーセキュリティに関与しているかどうかを重要視している。

報告書においては、「取締役会はサイバーセキュリティリスクを理解し、説明責任をはたすべき」、「サイバーセキュリティリスクはサプライチェーン全体で管理されるべき」、等について言及

（１）経営層向けの施策

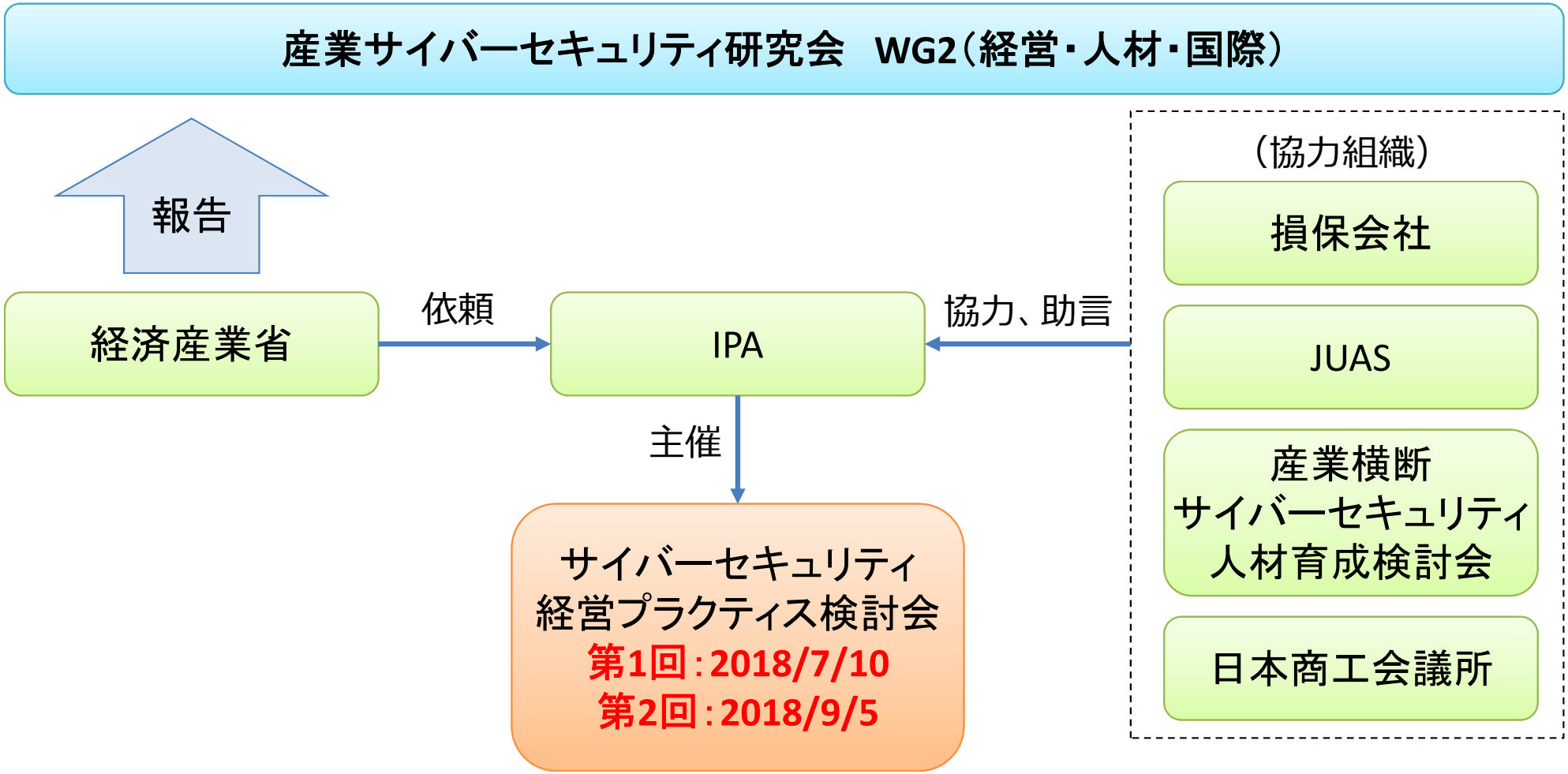
（２）現場向けの施策

（３）中小企業向けの施策

サイバーセキュリティ経営プラクティスと可視化ツールの作成

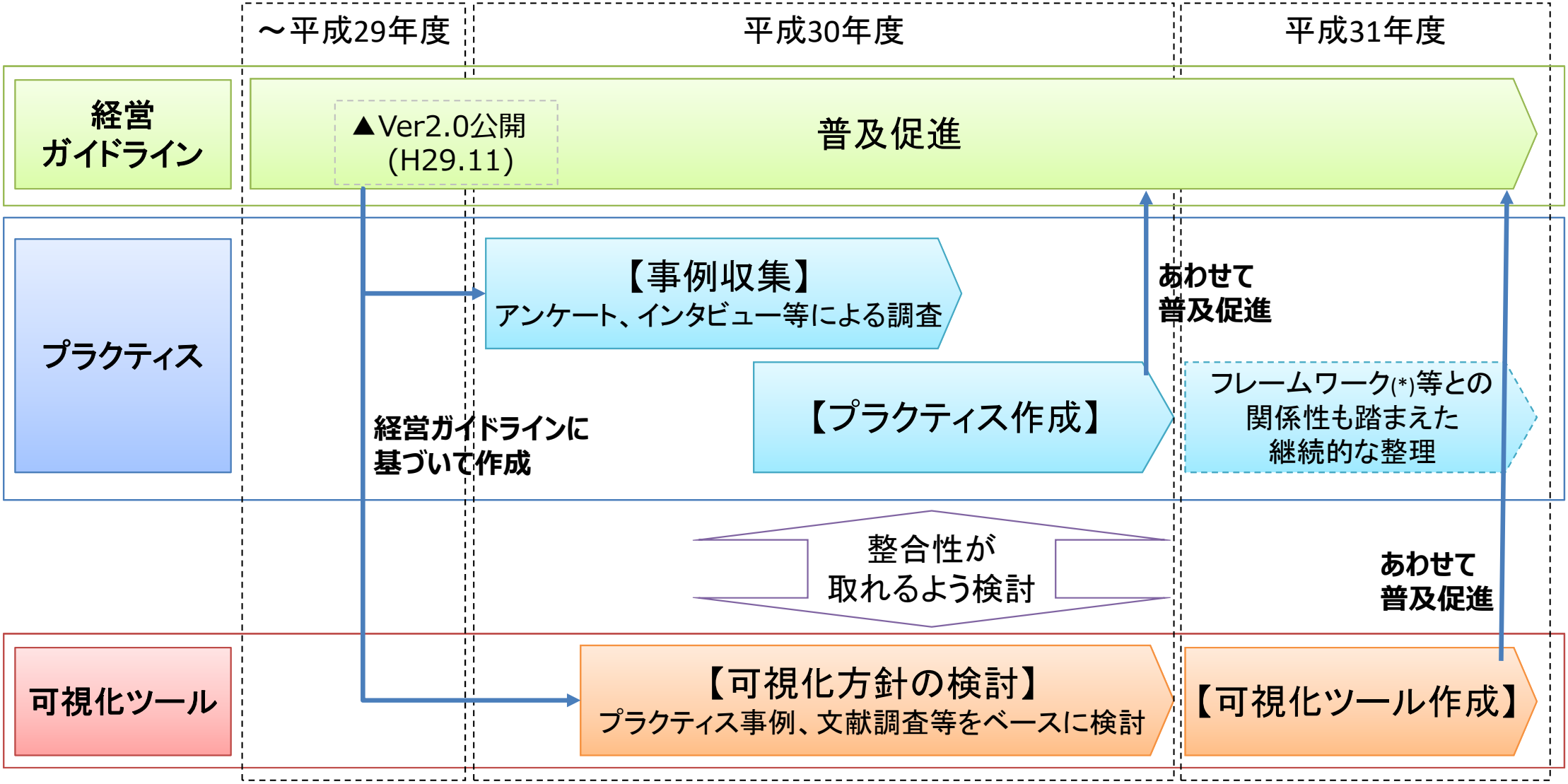
- サイバーセキュリティ経営ガイドラインのプラクティスと、セキュリティ対策の実施状況を可視化するツールを作成するためにサイバーセキュリティ経営プラクティス検討会をIPAに設置し、これまで2回開催（2018/11/9現在）。

＜作成体制＞



プラクティスと可視化ツールの作成について

- 企業へのインタビュー等によりプラクティス事例を収集し、企業の取り組み状況をベースとして可視化の方向性を定めていく予定。



(*)サイバー・フィジカル・セキュリティ対策フレームワーク（経済産業省）

サイバーセキュリティ経営プラクティス検討会での主な検討内容

主なご意見	対応方針（案）
● サイバーセキュリティ経営ガイドラインの重要10項目について、他の企業が具体的にどのような対策を実施しているかが読者に伝わるような内容にできるとよい。一方で、会社が特定されるような形での事例公開は難しい。	● インタビューで適切な事例を収集する。その際、企業が特定されないような内容での事例公開であることを前提に、企業へのインタビュー協力を依頼する。
● 重要インフラに課せられたセキュリティレベルは高いなど、社会的要求度によって求められるセキュリティレベルが異なる。 ● 企業規模によってもセキュリティレベルは異なる。	● 業種や企業規模等の条件の違いを考慮してプラクティスを作成する。
● サプライチェーン全体にまたがる基準を出し、どこまでやるべきか明らかにする必要がある。	● WG1及び各SubWGにて検討する。

（１）経営層向けの施策

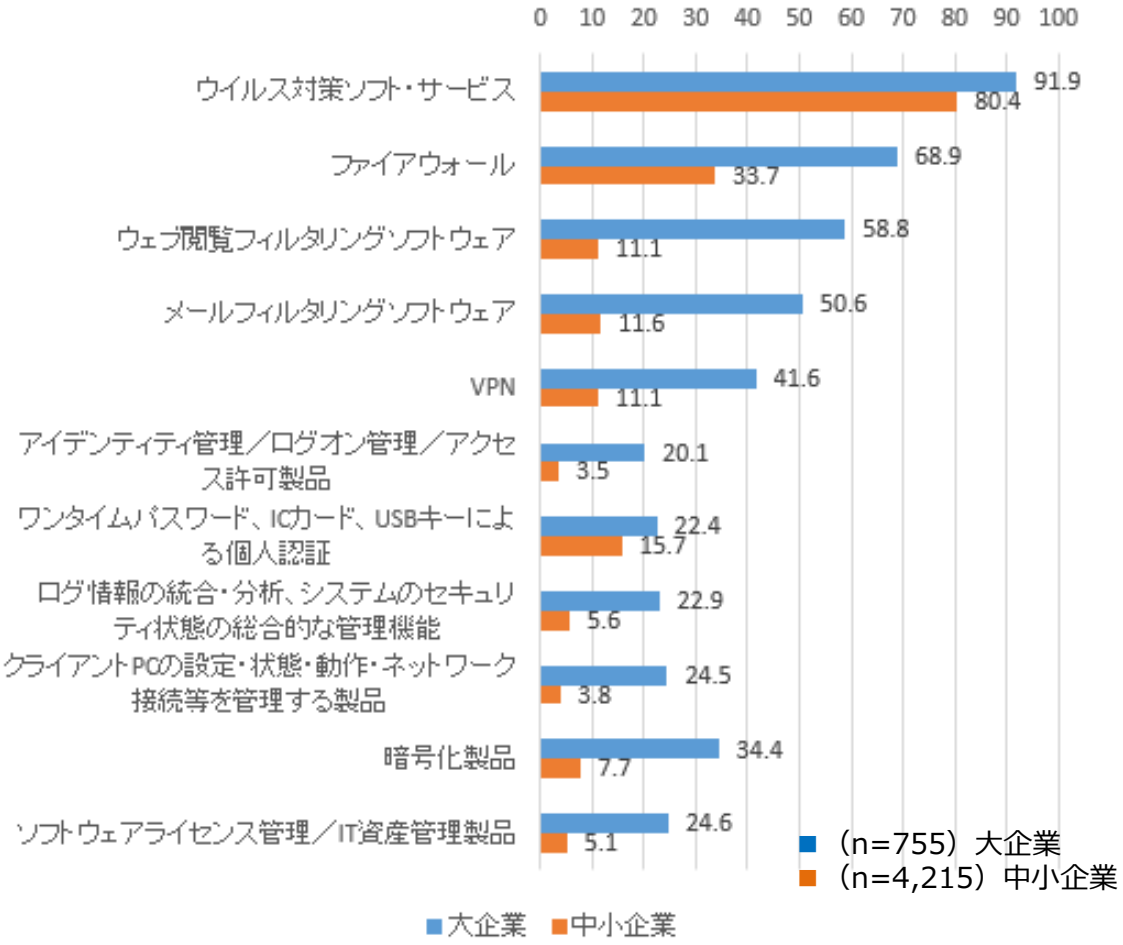
（２）現場向けの施策

（３）中小企業向けの施策

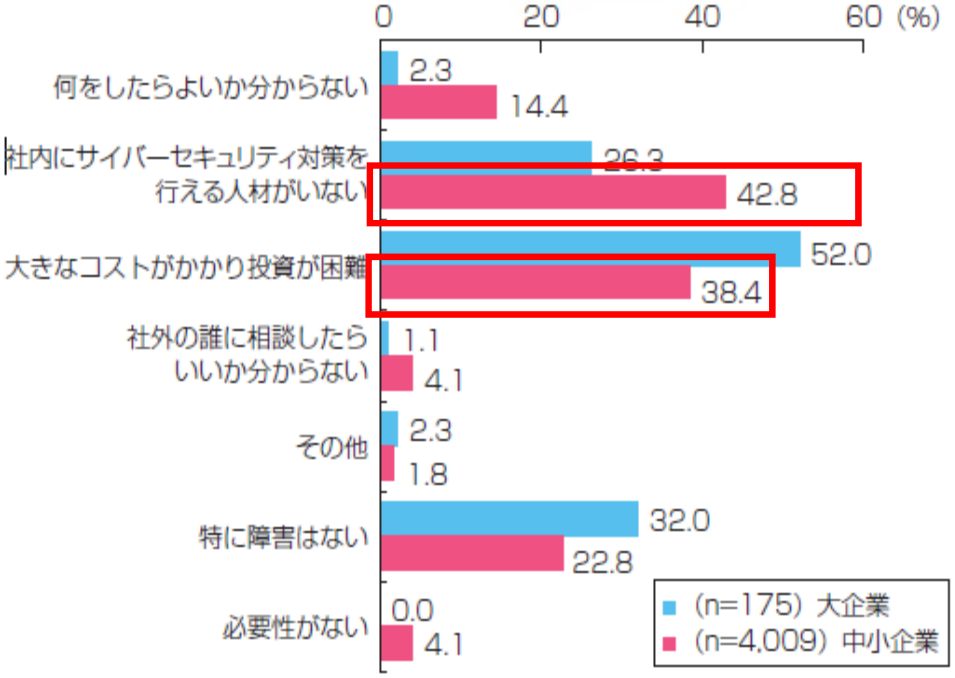
中小企業のサイバーセキュリティ対策の実施状況

- 中小企業のセキュリティ対策は、大企業と比較しても大きく遅れを取っている。中小企業では**セキュリティ人材の不足**が課題。また、**コスト**の大きさも大きな課題となっている。

【大企業と中小企業の対策状況の比較】



【セキュリティ対策を実施する際の障害】



（出典）経済産業省　2018年版ものづくり白書

（出典）IPAが実施した「企業のCISOやCSIRTに関する実態調査」、
「中小企業における情報セキュリティ対策に関する実態調査」より作成

中小企業向けセキュリティサービスの現状

- 中小企業自身で対策を進めるには限界がある一方、中小企業におけるニーズ把握が進んでいない。特に事後対策については、中小企業向けセキュリティサービスの提供が進んでいないのが実情。
- 中小企業向けサービスが創出される上でのボトルネックを解消し、**持続可能なサービスに結びつけること**が必要。

＜中小企業＞

- 人材不足であり自社でのセキュリティ事案への対応は困難。
- できるだけ**セキュリティに費用はかけたくない。**

ニーズに合致したサービスは存在しない

＜支援側（損保会社、ベンダー等）＞

- **専門性が必要であり、**損保等の窓口やIT営業では、**現状対応が困難。**
- 事案対応は常時対応が発生するわけではなく、**安価なサービスの提供が困難。**

公的支援で支え続けることはコスト的な課題有り

＜公的支援側＞

- 事案対応については、**迅速な対応が求められるため、緊急対応を行う面的な体制が必要だが、限られた公的資金での継続的な対応は容易ではない。**

中小企業サイバーセキュリティ対策支援促進事業

主に事後対策

平成31年度概算要求額　２．２億円（新規）

事業の内容

事業目的・概要

- 「Society5.0」へ向け、様々なデータのつながりが価値を生む一方、サイバーセキュリティの面では、サプライチェーン全体での対策の必要性が高まっています。
- また、グローバルサプライチェーンの中で、我が国企業が競争力を確保するためにも、中小企業を含めて諸外国の規制動向も踏まえながら、サイバーセキュリティ対策を推進していく必要があります。
- このため、サプライチェーンを構成する中小企業のサイバーセキュリティ対策の強化に向け、中小企業のニーズに合致した支援体制の構築が急務です。
- 本事業では、損害保険会社、ITベンダーの連携や、ITベンダー等における職務経験を有するITシルバー人材の「サイバーセキュリティお助け隊」としての活用等により、中小企業に対する専門的なアドバイス等を実施する支援体制のモデルを構築し、地域実証を行います。
- 実証を通じ、中小企業のサイバーセキュリティ対策の実態を把握し、実態に即したサービス内容やこれに求められる人材のスキル、支援体制等を明らかにすることにより中小企業が活用しやすいサイバーセキュリティサービスの創出を目指します。

成果目標

- 平成31年度から平成32年度まで全国5か所程度における実証を通じて、中小企業の実態に即したサービス内容やこれに必要な人材、体制等を明らかにすることを目指します。

条件（対象者、対象行為、補助率等）

国 → 委託 → 民間企業

事業イメージ

中小企業のサイバーセキュリティ対策支援体制のモデル構築

【中小企業が悩んでいること、課題】

- 助言だけではなく技術的な対応までしてほしい。【支援内容】
- 相談しやすい窓口がほしい。何かあれば迅速に対応してほしい。【支援体制】
- できるだけ費用はかけたくない。【コスト】

中小企業のサイバーセキュリティ対策支援の地域実証

- 全国５か所程度※で、支援体制モデルを構築し、中小企業支援の地域実証を実施。実態に即したサービスに必要な人材、体制等を明確化。

＜中小企業向け支援体制モデル＞

国
委託
サービス設計
相談窓口
損害保険会社、ITベンダー　等
必要に応じ対応依頼
サイバーセキュリティお助け隊
ITベンダー等のITシルバー人材
再教育プログラム
サイバーセキュリティに関する相談
アドバイス、復旧、調査等
中小企業

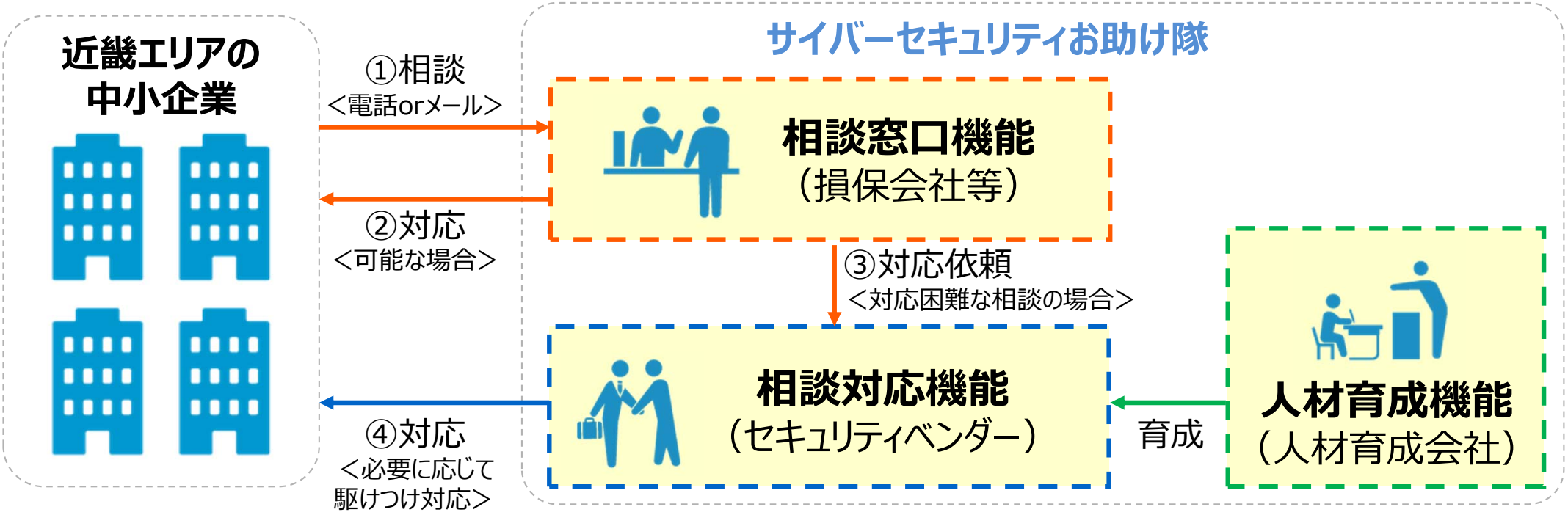
中小企業が活用しやすいサイバーセキュリティサービスの創出

サイバーセキュリティお助け隊

主に事後対策

- 中小企業において事案が発生した際の**相談窓口を設置**し、**迅速に対応の支援を行う体制を構築**。本窓口の活用・展開を通じて、**事前対策についても普及促進。**
- **来年度、地域（近畿エリア等）を絞って実証事業(*)**を行う予定。

＜実証事業のイメージ＞



実証により、「中小企業におけるサイバー攻撃の実態把握」を行うとともに、「中小企業支援のための必要な人材スキル・ツール等」を明らかにし、「迅速かつ効率的に支援対応を行うための体制」を検証する。

(*)地域での実証事業の普及啓発に関しては、地域の大企業や団体等と連携することも検討。

（参考）中小企業における課題と SOMPO CYBER SECURITYの中小企業向けサービスの展開

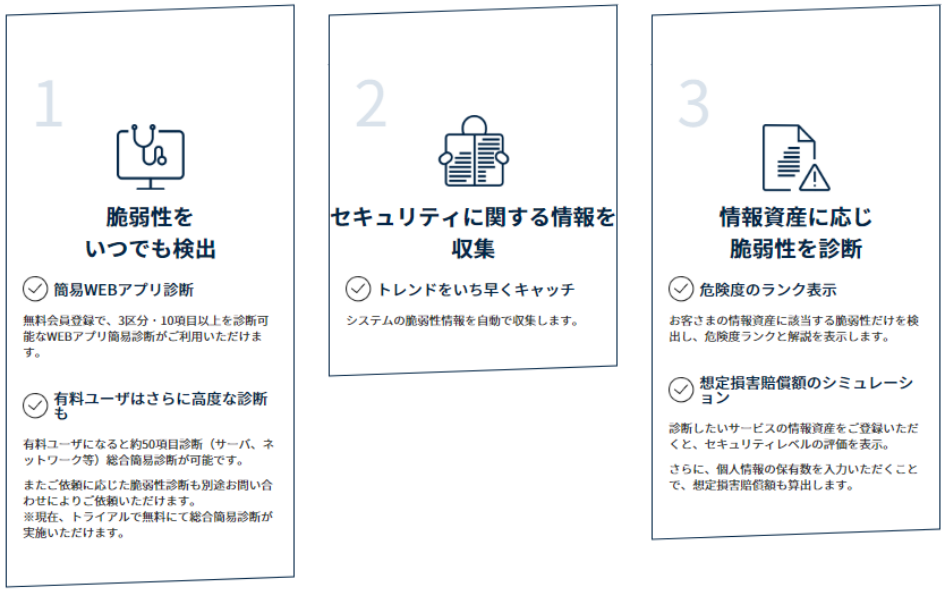
中小企業の多くが抱える課題

- **セキュリティ予算が潤沢ではない。**また、サイバーセキュリティ事業者の多くは大企業向けのサービス展開に注力し、**中小企業の予算に見合ったセキュリティサービスを入手しにくい。**
- **サイバーリスクに関するリスクアセスメントを十分に実施できていない。**このため、経営層が自社のサイバーリスクに関して影響の範囲や程度を適切に評価・認識できておらず、適切な資源配分もできていない。
- **サイバーインシデントを適切に監視・検知できていない。**このため、サイバー攻撃を受けた場合などに適切に対応するための対処態勢を整えられていない。

中小企業向けサイバーセキュリティ対策プラットフォームの構築 及び これを通じたリーズナブルな診断サービスや監視サービスの提供

SOMPO DEFNAVI

ウェブサイト等に対するサイバー攻撃について、各種脆弱性診断等を通じて適切なリスク対策をナビゲートするためのサービスです。



診断結果を踏まえた
監視サービス等の提案

SOMPO CYBER SECURITY

監視・検知サービス

WAF	UTM	・・・

中小企業に向けた主な特長

- ✓ 中小企業向けに機能をカスタマイズして<u>わかりやすさと低価格</u>を実現
- ✓ クラウド又は機器レンタルによるSaaS型サービスとして、<u>導入に係る購買・導入負荷を低減</u>
- ✓ サイバー保険を付帯し、<u>インシデント対応時に必要な費用負担を低減</u>

（参考）中小企業向けサービスの展開（東京海上日動）

- サイバー保険の契約者を対象とし、サイバーリスクに関するトラブルを直接相談できる窓口（緊急時ホットラインサービス）を設置。（ 2019年1月1日よりサービス開始予定）
- ウィルス感染等の簡易なトラブル相談から不正アクセス等の重大トラブル時の専門事業者紹介まで幅広いサービスを展開。

【サービスのポイント】
- 365日対応（受付時間は9:00-18:00）
- 簡易なトラブルから専門性を要するトラブルまで幅広く対象に。

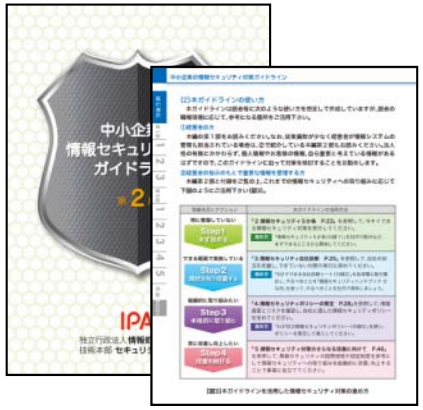
（出典）緊急時ホットラインサービスのご案内（東京海上日動火災保険株式会社）

中小企業の情報セキュリティ対策ガイドラインの改訂

事前対策

- 中小企業の経営者やIT担当者が、セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドラインの第2版をIPAより公開中。
- 政策動向や市場のニーズ(*)を踏まえて**平成30年度中に作成を目指す**。

(*)サイバーセキュリティの経営ガイドラインの改訂（平成29年11月）といった政策動向や、クラウドサービスの安全な利用方法に関するニーズ等



経営者向けの解説

サイバーセキュリティ経営ガイドラインの内容を中小企業向けに整理し、**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

管理者向けの解説

管理者が具体的にセキュリティ対策を実施していくための方法を、**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

＜主な改訂ポイント＞

- サイバーセキュリティ経営ガイドラインVer2.0との整合性の改善
  （「検知」、「復旧」の観点について、中小企業の実態に即した対応策を提示）
- 各種ITツールの利用方法に関する対策を追加
  （クラウドサービスの安全な利用方法等）
- 中小企業向けによりわかりやすい表現や記述の改善

（参考）サイバーセキュリティ経営ガイドラインVer2.0の主な改訂ポイント（１／２）

- 米国のサイバーセキュリティフレームワークでも事前対策だけでなく、事後（**検知、対応、復旧**）対策を要求。
- 一方で、経営ガイドラインVer1.1は、CSIRTの構築などの「対応」に関する項目はあるものの、「検知」や「復旧」に関する内容が弱かったため、**国際的な整合性を考慮し、「検知」「復旧」に関する項目を追加**。

サイバーセキュリティ経営ガイドラインVer2.0 重要10項目
（平成29年11月16日改訂）

(1)	セキュリティポリシーの策定
(2)	サイバーセキュリティリスク管理体制の構築
(3)	セキュリティ対策のための資源確保
(4)	リスクの把握、対策目標と計画の策定
(5)	リスク対応策（防御・検知・分析）の実施
(6)	PDCAの実施と対策の開示
(7)	緊急時の対応体制の整備
(8)	復旧体制の整備
(9)	サプライチェーンセキュリティ対策の実施
(10)	情報共有活動への参加

対応

Framework for Improving Critical Infrastructure Cybersecurity(NIST)

（参考）サイバーセキュリティ経営ガイドラインVer2.0の主な改訂ポイント（２／２）

- 重要項目　指示5として「攻撃の検知」に関する、「サイバーセキュリティリスクに対応するための仕組みの構築」を追加

サイバー攻撃による被害を最小限にするためには早期に検知することが重要であるが、約半数の企業が外部からの指摘によりサイバー攻撃による被害が発覚している状況であり、**サイバー攻撃を自分たちで気づけていない**ケースが多い（≒**企業において「検知」の対策が十分ではない**と想定）。

- 重要項目　指示8 として「復旧」に関する、「サイバーセキュリティリスクに対応するための仕組みの構築」を追加

企業においてBCPの策定・訓練の実施が進んでいるが、自然災害対策等を想定しており、**サイバー攻撃についての復旧が意識されていない**ケースが多い（ランサムウェアのように、可用性に影響を与える攻撃も増加している状況において、復旧に関する対策は重要）。

- 重要項目　指示9の「サプライチェーンのビジネスパートナーや委託先等を含めたサイバーセキュリティ対策の実施及び状況把握」において、委託先におけるリスクマネーの確保や委託先の組織としての活用の把握（ISMSやSECURITY ACTION）等の留意点を追記

日本企業の自社のセキュリティ点検は欧米にやや遅れる程度だが、委託先等へのケアは大幅に遅れている。

セキュリティ対策自己宣言「SECURITY ACTION」

事前対策

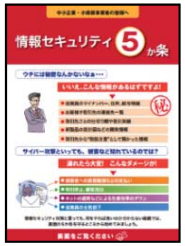
- 中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度（IPA）。
- IT導入補助金の申請において、「SECURITY ACTION」の宣言を必須要件化。

★ 一つ星

SECURITY ACTION ★

セキュリティ対策自己宣言

情報セキュリティ5か条に取り組む企業

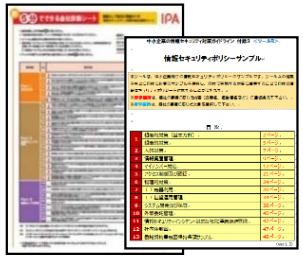


★★ 二つ星

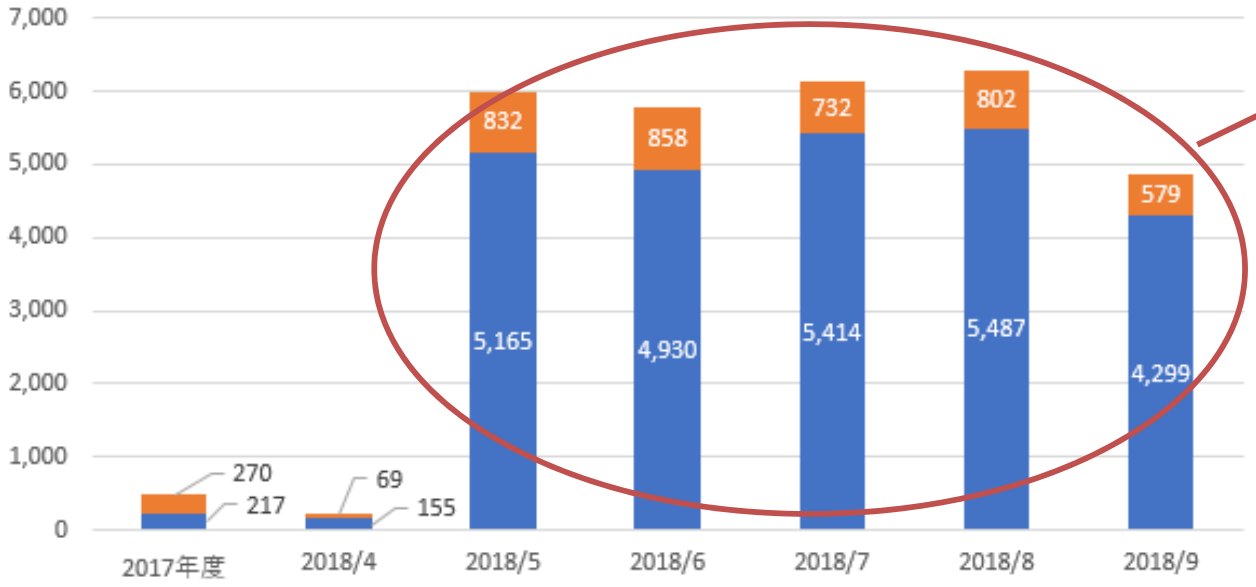
SECURITY ACTION ★★

セキュリティ対策自己宣言

情報セキュリティ自社診断の実施及びセキュリティポリシーを策定する企業



※IPAにて、一般社団法人中小企業診断士協会、全国社会保険労務士会連合会、全国商工会連合会、全国中小企業団体中央会、特定非営利活動法人日本ネットワークセキュリティ協会、特定非営利活動法人ITコーディネータ協会、独立行政法人中小企業基盤整備機構、日本商工会議所、日本税理士会連合会と連携した普及促進活動を実施



IT導入補助金の申請要件となったことにより、**宣言数が大幅に増加**

二つ星	4,142
一つ星	25,667
Total	29,809

(2018年9月末時点)

地域におけるセキュリティ対策向上の取組（講習能力養成セミナー）

- 中小企業に対してセキュリティ対策を支援する方に対して、実戦的な知識を学んでいただくために、地域の団体と連携して全国で講習能力養成セミナーを開催（IPA）

都道府県	共催団体	開催日	参加人数
北海道	北海道ソフトウェア技術開発機構	2018/12/10	―
福島県	ITCふくしま	2018/11/20	―
埼玉県	埼玉ITコーディネータ	2018/7/17	84
千葉県	ちば経営応援隊	2018/9/18	86
東京都	東京商工会議所	2018/8/7	105
	中小企業基盤整備機構	2018/9/5	34
神奈川県	情報セキュリティフォーラム、ITCはまさき	2018/11/13	―
長野県	長野県ITコーディネータ協議会	2018/10/3	36
富山県	富山商工会議所	2018/10/23	―
石川県	石川県情報化支援協会	2018/9/26	31
岐阜県	ソフトピアジャパン	2018/10/2	47
愛知県	ITC中部、東海インターネット協議会	2018/8/1	70
三重県	ITC三重	2018/11/9	―

都道府県	共催団体	開催日	参加人数
京都府	ITコーディネータ京都、近畿経済産業局、近畿総合通信局	2018/11/20	―
大阪府	ITC近畿会、近畿経済産業局、近畿総合通信局	2018/8/30	52
兵庫県	ヒューリット経営研究所、近畿経済産業局、近畿総合通信局	2018/8/30	50
山口県	アイティコーディネータやまぐち協同組合	2018/11/6	―
香川県	高松商工会議所	2018/7/24	20
愛媛県	愛媛情報サービス産業協議会	2018/11/26	―
大分県	ハイパーネットワーク社会研究所	2018/9/4	97
鹿児島県	鹿児島印ファーメーション	2018/10/30	―

※10/22時点で712名が参加

地域におけるセキュリティ対策向上の取組（インターネット安全教室）

- 家庭や学校からインターネットにアクセスする一般利用者を対象として、基礎的なセキュリティ知識を習得することを目的としたセミナーを全国で開催（IPA）。

都道府県	共催団体	開催日	参加人数
北海道	くるくるねっと	2018/7/5	301
	旭川情報産業事業協同組合	2018/7/18	320
岩手県	盛岡情報ビジネス専門学校	全2回	78
宮城県	地域情報モラルネットワーク	2018/12/1	―
栃木県	栃木シニアセンター	全8回	132
群馬県	おおたIT市民ネットワーク	2018/6/5	14
埼玉県	―	2018/7/13	219
東京都	―	全3回	542
神奈川県	情報セキュリティフォーラム	全5回	356
山梨県	―	2018/10/13	426
長野県	グループHIYOKO	全2回	53
	岡谷市教育委員会	2018/12/9	―
岐阜県	岐阜市消費生活センター	2018/5/26	46
三重県	PCシエル	2018/9/23	106
京都府	―	2018/7/3	408

都道府県	共催団体	開催日	参加人数
大阪府	―	2018/11/10	―
兵庫県	―	2018/9/28	39
島根県	島根県隠岐の島警察署	2018/11/7	―
岡山県	岡山県情報セキュリティ協議会	2018/9/28	21
徳島県	e-とくしま推進財団	全7回	421
福岡県	スキルアップサービス	全5回	59
大分県	ハイパーネットワーク社会研究所、東部・佐賀関地区PTA	2018/6/23	100
	ハイパーネットワーク社会研究所、由布私立狭間小学校PTA	2018/6/28	33

※10/22時点で3,674名が参加
※本リストに掲載している以外の地域でも開催を予定

1．経営

2．人材

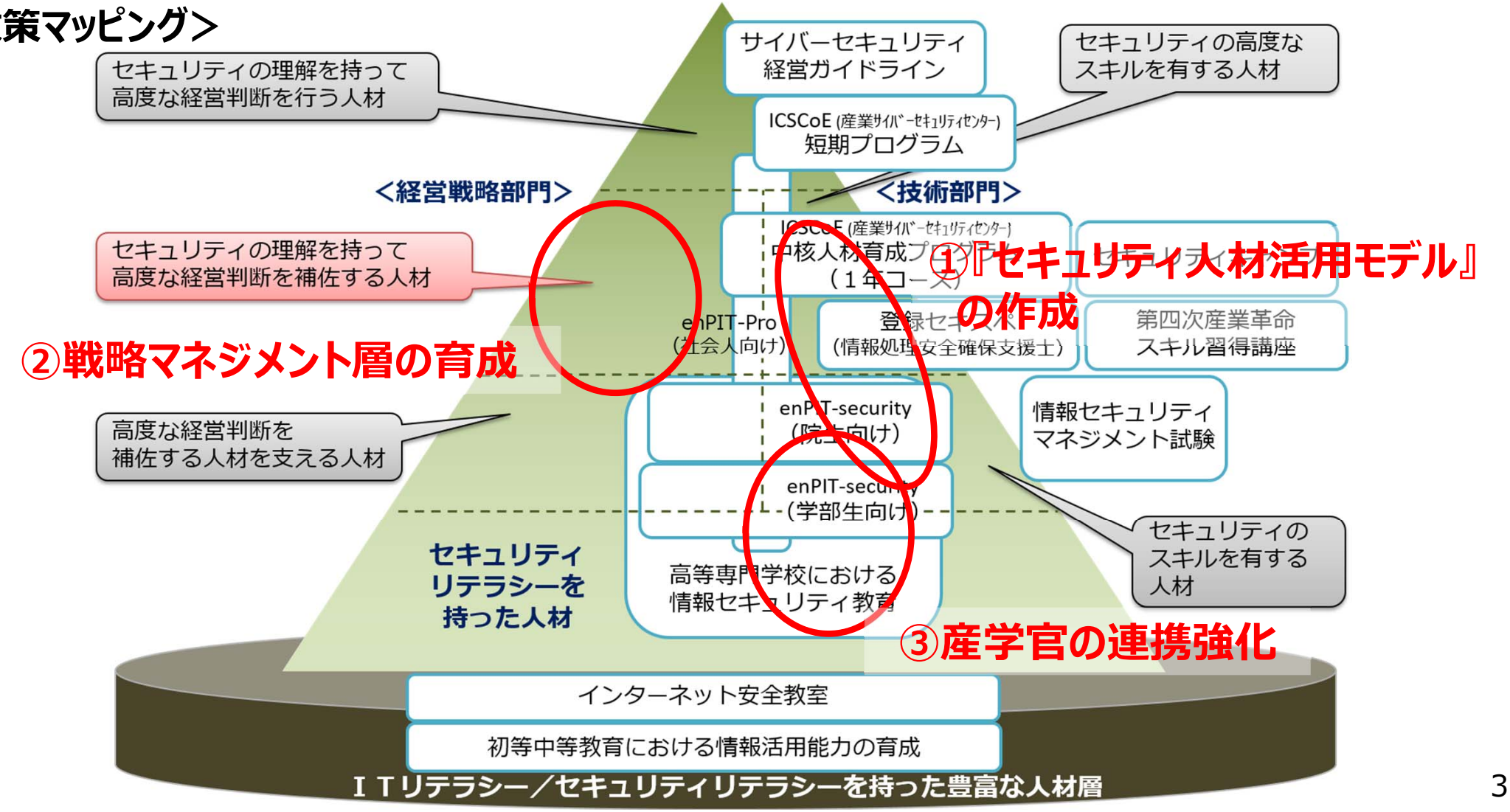
3．国際

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

第二回産業サイバーセキュリティ研究会資料より再掲

- ユーザー企業において必要となる**セキュリティ人材の定義、評価指標が不明確。**
- **「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。**

＜政策マッピング＞



（参考）米国大統領令に基づくサイバーセキュリティ人材育成に関する報告書

- 2017年5月の「連邦政府のネットワーク及び重要インフラのサイバーセキュリティ強化に関する大統領令」に基づき、米国の商務省・国土安全保障省が共同で、サイバーセキュリティ人材の育成に関する大統領への報告書を策定（2017年11月）、公表（2018年5月）。

(1) 現状

○ 米国内では約30万人のサイバーセキュリティ人材の求人（2017年8月現在）。また、グローバルには、2022年には約180万人の不足が発生するとの試算もあり。
○ 初級者的レベルから高度な知識・技能を必要とするレベルまで幅広い人材が求められており、人材獲得の競争も激しくなっている。
○ 経営層は、サイバーセキュリティに関する能力と併せ、事業分野に関する知識・スキルも有する人材を求めている。

(2) 主な課題

○ 米国は、サイバーセキュリティ人材の育成に関する、速やか、かつ、持続的な取組を推進することが重要。
○ 具体的には、経営層のニーズに合致する人材を育成・確保するための教育プログラムの提供、社会人等の学び直し、初等中等教育の充実、求人や教育・研修プログラムに関する包括的かつ信頼性の高いデータ提供等を推進することが必要。

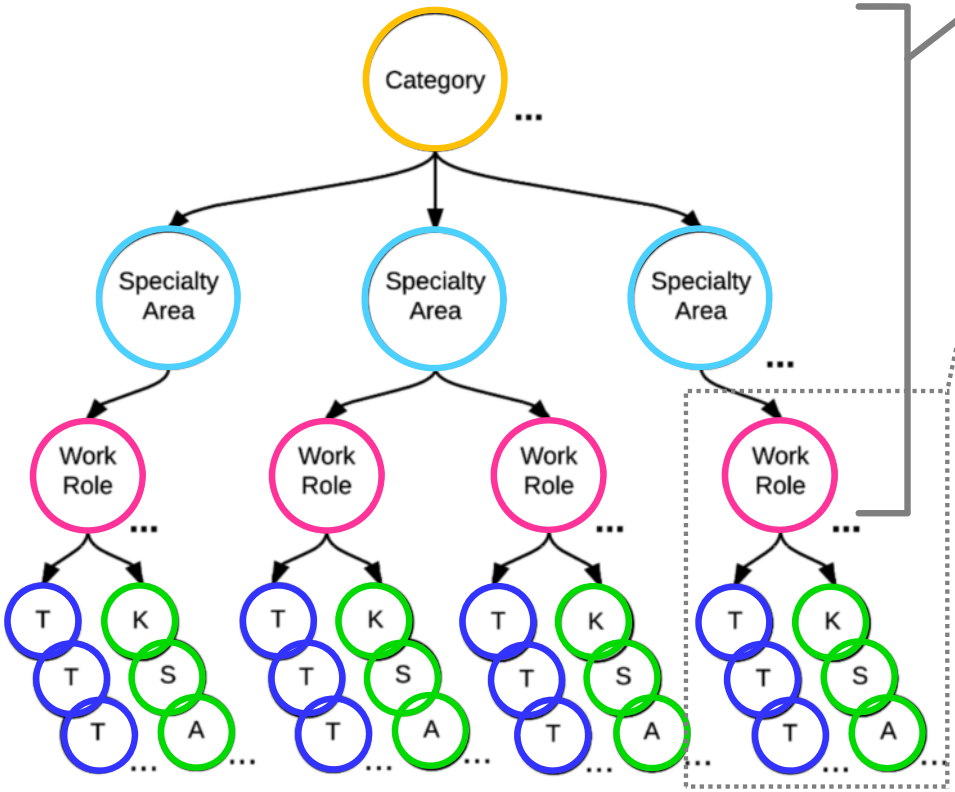
(3) 推進すべき主な取組

➢ 安全保障及び経済的発展に資する人材の育成・強化に係るビジョン及びアクションプラン、官民連携のための「行動規範（Call for Action）」の策定
➢ 高品質かつ効果的な教育プログラム等を提供するための予算の確保
➢ 政府機関におけるサイバーセキュリティ人材の採用・育成・確保に関する取組の推進
➢ 学び直しの推進（例：ハンズオン演習、オンライン学習、教員・講師の確保、必要な予算の確保）
➢ 官民連携の下、経営層のニーズに合致する人材の育成・強化の推進（例：**NICEフレームワークの活用**、キャリアパスやカリキュラムのモデル化、州ごとに一つ以上の連合（alliance）の整備、人材育成に関する情報ハブ（clearing house）の整備）
➢ 人材育成への投資効果を定量的に把握するための手法の開発・活用

(参考) NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework (SP800-181)

- NIST（国立標準技術研究所）が中心となり産学官で策定したサイバーセキュリティ人材に関するフレームワーク。（2013年4月策定、2017年8月改訂）
- サイバーセキュリティ業務に関する52種類の役割と、各役割に求められるタスクや知識・技能・能力の関係を明確化。

＜NICEフレームワークの構成＞



タスク: 1007項目　**スキル**: 374項目
知識: 630項目　**能力**: 176項目

7種類の**カテゴリ**、33種類の**専門分野 (Specialty Area)**、52種類の**役割 (Work Role)** から構成

各役割には、達成される**作業(T:Task)**と、役割を果たすために必要な**知識 (K:Knowledge)**、**技能 (S:Skill)**、**能力 (A:Ability)** が紐付いている

Work Roleの例（Authorizing Official）

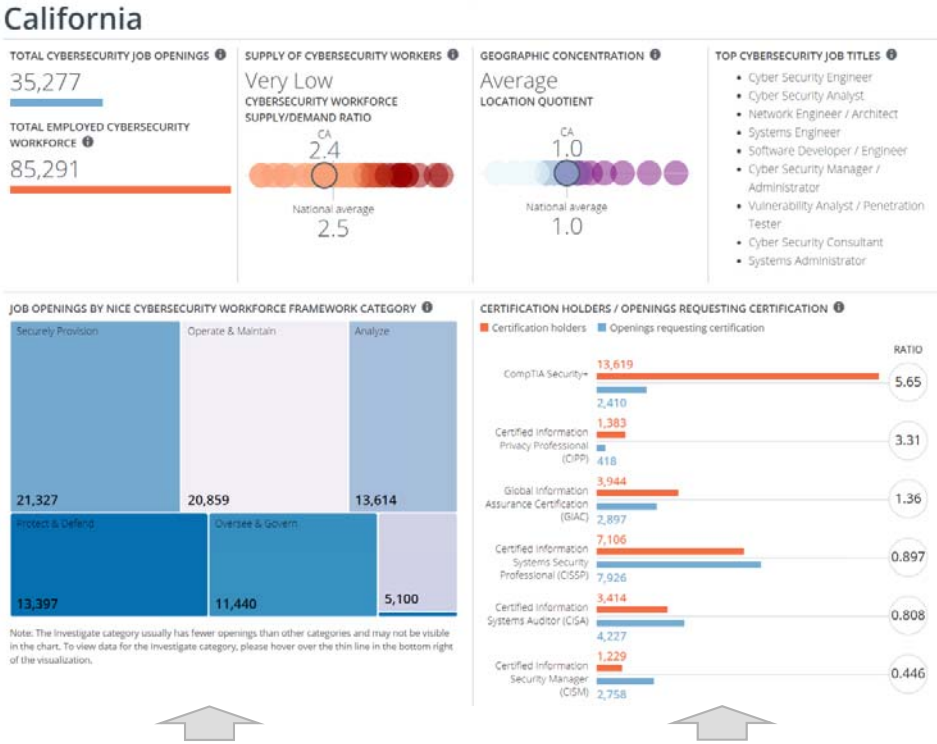
Work Role Name	Authorizing Official
Work Role ID	SP-RSK-001
Specialty Area	Risk Management (RSK)
Category	Securely Provision (SP)
Work Role Description	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).
Tasks	T0145, T0221, T0371, T0495
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0027, K0028, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0059, K0070, K0084, K0089, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0295, K0322, K0342, K0622, K0624
Skills	S0034, S0036
Abilities	A0028, A0033, A0077, A0090, A0094, A0111, A0117, A0118, A0119, A0123, A0170

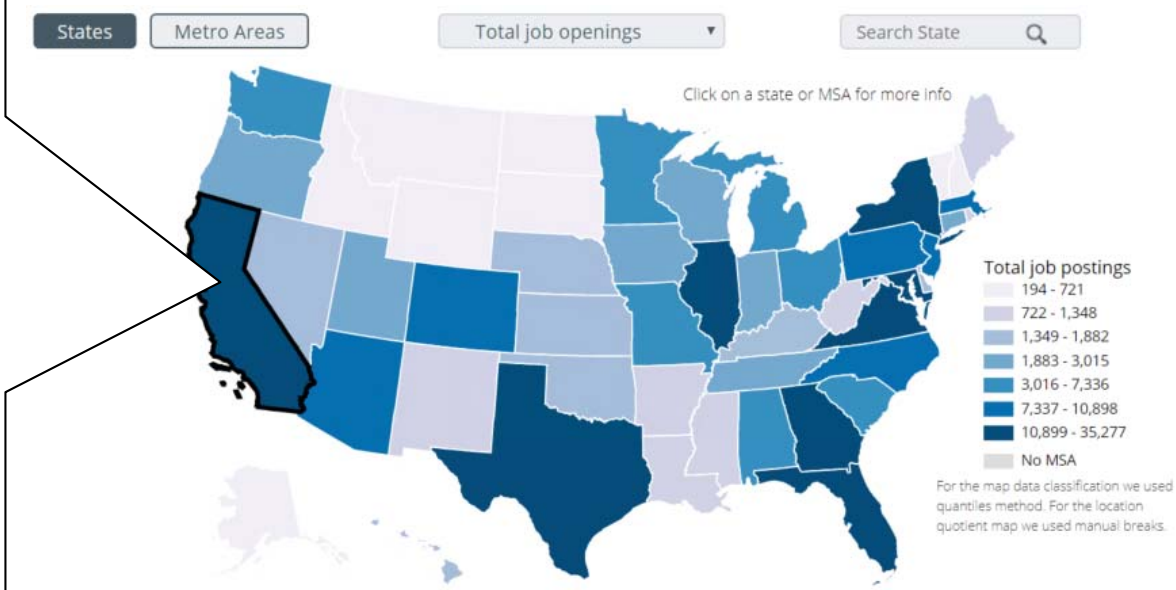
T0495	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.

出典： NIST SP800-181

（参考）NISTによるCyberSeekプロジェクト

- NIST（国立標準技術研究所）が支援するオンラインサイト。米国の各地域におけるオンライン求人状況等の情報を、NICEフレームワークや民間団体が提供する資格と紐づけて視覚的に提供。
- 役割とスキルを紐づけ共通言語化することにより、こういった取組が可能になる。





NICEフレームワークの７カテゴリーの分類で求人数を表示。
- Securely Provision
- Operate & Maintain
- Analyze
- Protect & Defend
- Oversee & Govern
- Collect & Operate
- Investigate

民間団体が提供するそれぞれの資格の保有者の数と求人要件となっている数を提示。
上記のカリフォルニア州の例だと、CISSP資格は保有者よりも求人数の方が多いことが分かる。

＜プロジェクトパートナー＞

NICE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION
→ NISTによるセキュリティ人材に関する産官学のプロジェクト

burningglass CAREERS IN FOCUS
→ 労働市場のデータ分析に強みを持つ民間企業

CompTIA
→ Security+, Network+等のIT資格を開発・提供している業界団体

出典：https://www.cyberseek.org/

サイバーセキュリティ対策を支える基盤となる
サイバーセキュリティ人材育成・活躍促進パッケージ

①『セキュリティ人材活用モデル』の作成

- 役割定義の整理
- 委託調査

② 戦略マネジメント層の育成

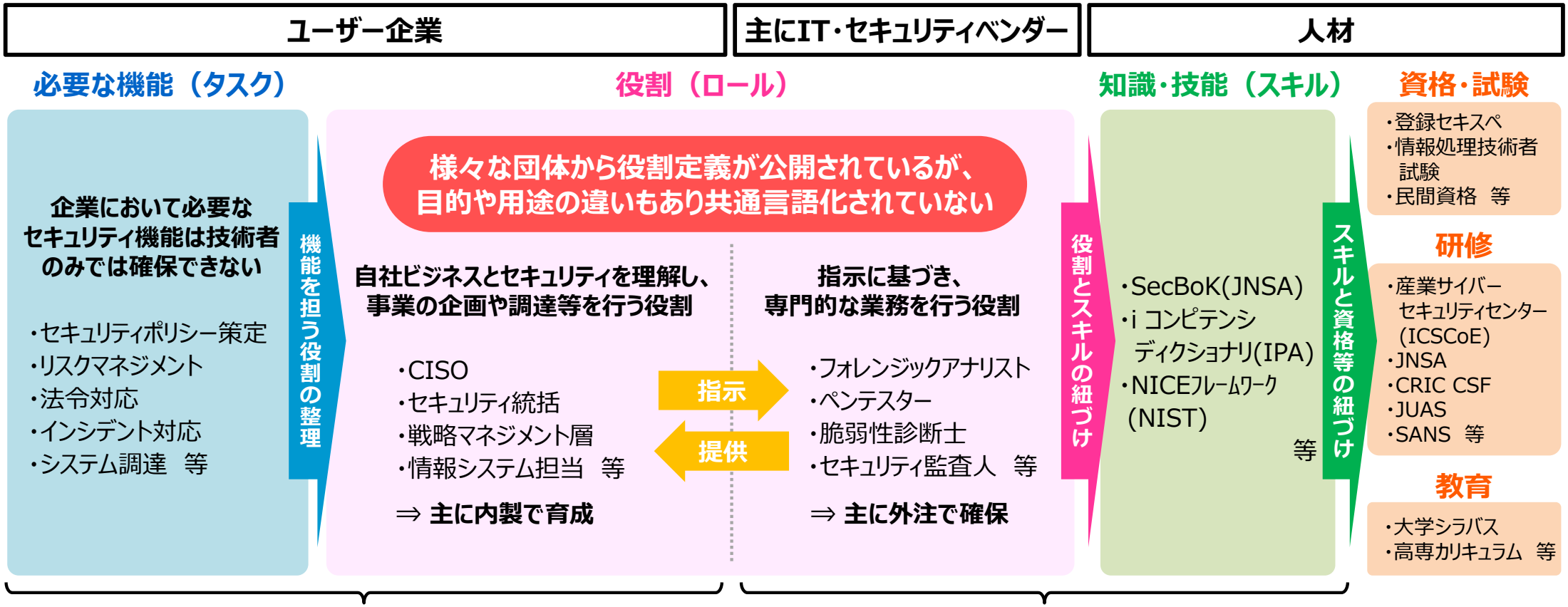
- 育成プログラムの提供

③ 産学官の連携強化

- 高専との連携の具体化
- 地域的取組の促進

セキュリティ人材の流動化に対応できる『セキュリティ人材活用モデル』の構築

- 企業に求められるセキュリティ機能を果たす人材の役割（肩書き）を、必要な知識・技能（スキル）と紐づけ、共通言語化することにより、人材の雇用・配置・外注等における企業と人材の間のコミュニケーションコストを減らし、マッチングを促進。
- 人材のニーズとシーズの見える化により、セキュリティ人材の最適活用、処遇改善につなげる。



論点1　ユーザー企業によって機能・体制・役割の在り方は様々

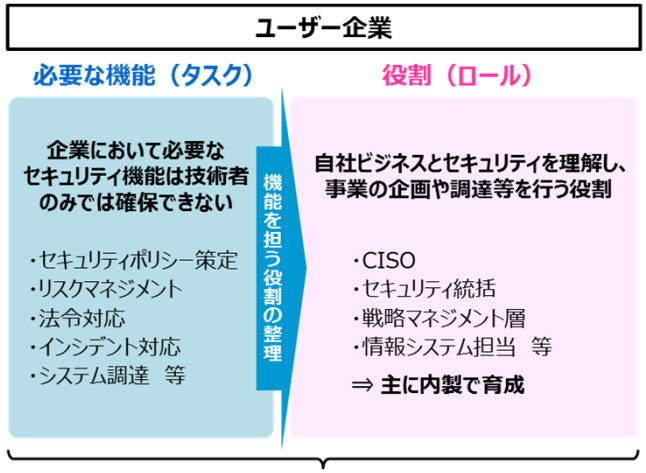
⇒ ユーザー企業の規模・業種・成熟度等に応じたセキュリティ体制や人材確保の関係について調査を実施

論点2　専門性が高い役割は比較的共通言語化しやすい

⇒ SecBoK(JNSA)、ITSS+(METI/IPA)、統合セキュリティ人材モデル(サイバーセキュリティ人材育成スキーム策定共同プロジェクト)等における既存の役割定義・専門分野の関係を整理・明確化

ユーザー企業におけるセキュリティ体制・人材確保に関する調査の実施

- 29年度の調査では、米国・英国のCISO等に対し、人材の確保・配置状況や企業のセキュリティ体制の成熟度等に関するアンケートを実施。成熟度を高める上で効果的な取組は、企業規模に応じて異なる可能性がある。
- 30年度の調査では、規模・業種・成熟度等に応じた様々なセキュリティ体制や人事・教育体制が存在する国内ユーザー企業を対象にヒアリング等を実施し、セキュリティ担当と事業部門の連携の在り方や、セキュリティ担当や戦略マネジメント層等のキャリアパス・活躍イメージ（ロールモデル）等、企業が人材戦略を考える上で参考となるプラクティスを抽出。



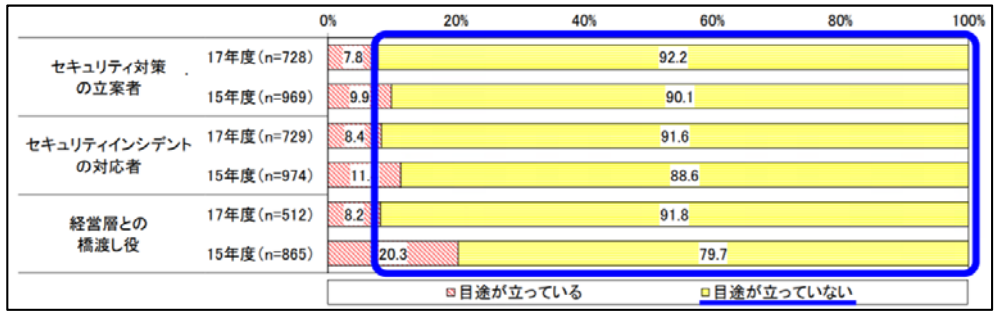
論点1 ユーザー企業によって機能・体制・役割の在り方は様々

⇒ ユーザー企業の規模・業種・成熟度等に応じたセキュリティ体制や人材確保の関係について調査を実施

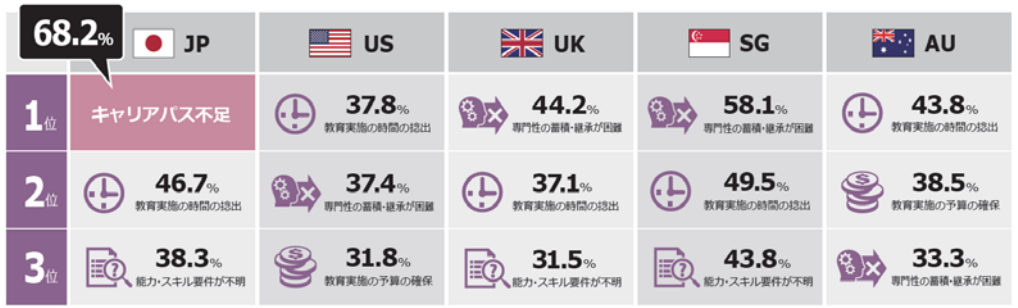
＜委託調査の概要＞

- ユーザー企業に対するヒアリング（30社程度）により、企業の規模・業種・成熟度等と組織体制・人材確保の関係について調査
- セキュリティ担当と事業部門の連携の在り方に関するプラクティスを抽出
- セキュリティ担当・戦略マネジメント層等のキャリアパス（ロールモデル）を抽出
- 海外動向等文献調査
- 有識者ヒアリング（10名程度）
- 報告書の作成

（背景１）日本の多くのユーザー企業では、内製すべきセキュリティ人材が不足。（背景２）人材育成・教育に係る課題のうち、日本ではキャリアパス不足が突出。



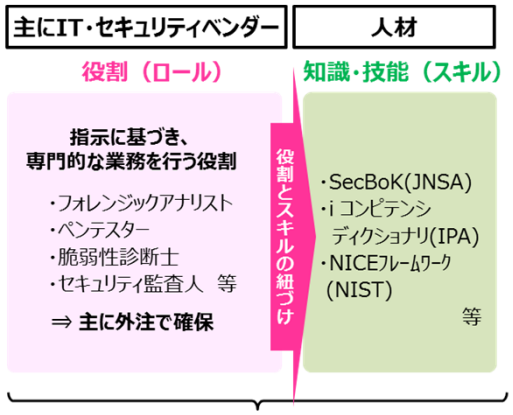
出典：(一社)日本情報システム・ユーザー協会『企業IT動向調査2018』
（ユーザー企業 1,078社に調査）



出典：NRIセキュアテクノロジーズ株式会社『NRI Secure Insight 2018』
（ユーザー企業 計1,110社に調査）

専門性が高い分野における役割定義の関係整理

- 専門性が高い役割については、比較的共通言語化しやすいと思われるが、目的や用途に応じ、様々な役割定義が存在。
- NICEフレームワーク等の海外の規格も参照しつつ、国内における既存の様々な役割定義の関係整理に向け、関係団体（IPA、JNSA、産業横断サイバーセキュリティ人材育成検討会（以下、CRIC CSF）等）と継続的に議論を実施。（9月27日、10月26日に、関係団体との議論を実施。）



論点2　専門性が高い役割は比較的共通言語化しやすい

⇒ SecBoK(JNSA)、ITSS+(METI/IPA)、統合セキュリティ人材モデル(サイバーセキュリティ人材育成スキーム策定共同プロジェクト)等における既存の役割定義・専門分野の関係を整理・明確化

目的や用途の違いから、役割の名称・定義の粒度はそれぞれ異なる

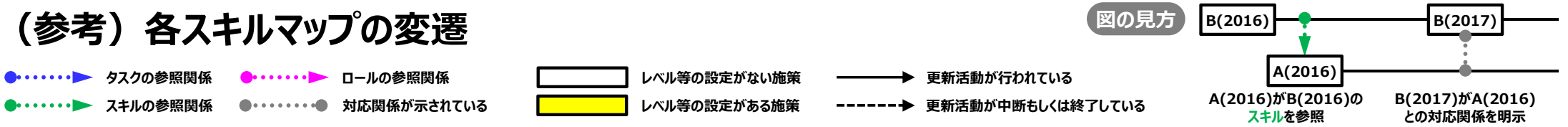
例として、既存のそれぞれの役割定義に沿ってインシデント対応に関係する役割を塗りつぶしたものが右表。

（※なお、塗りつぶし箇所以外にも広い意味でインシデント対応に関係する役割は存在。）

＜各団体による役割・専門分野の定義の例＞

ITSS+ (セキュリティ領域)【METI / IPA】	SecBoK【JNSA】	人材定義リファレンス【CRIC CSF】	統合セキュリティ人材モデル【サイバーセキュリティ人材育成スキーム策定共同プロジェクト】	NICEフレームワーク (Specialty Areas)【NIST】
情報リスクストラテジ	CISO	CISO/ CRO/ CIO等	セキュリティコンサルタント	Risk Management
情報セキュリティデザイン	POC (Point of Contact)	サイバーセキュリティ統括（室等）	セキュアシステムプランナー	Software Development
セキュア開発管理	ノーティフィケーション	システム部門責任者	セキュアシステムデベロッパー	Systems Architecture
脆弱性診断	コマンダー	システム管理者	セキュアアプリケーションデベロッパー	Technology R&D
情報セキュリティアドミニストレーション	トリアージ	ネットワーク管理者	セキュリティマネージャー	Systems Requirements Planning
情報セキュリティアナリシス	インシデントマネージャー	CSIRT責任者	セキュリティオーディター	Test and Evaluation
CSIRTキュレーション	インシデントハンドラー	サイバーセキュリティ事件・事故担当	システムリスクアセッサー	Systems Development
CSIRTリエゾン	キュレーター	セキュリティ設計担当	ペネトレーションテスター	Data Administration
CSIRTコマンド	リサーチャー	構築系サイバーセキュリティ担当	ネットワークリスクアセッサー	Knowledge Management
インシデントハンドリング	ソリューションアナリスト	運用系サイバーセキュリティ担当	リサーチャー	Customer Service and Technical Support
デジタルフォレンジクス	セルフアセスメント	CSIRT担当	フォレンジックエンジニア	Network Services
情報セキュリティインベスティゲーション	脆弱性診断士	SOC担当	インテリジェンスアナリスト	Systems Administration
情報セキュリティ監査	教育・啓発	ISMS担当	インシデントレスポンダー	Systems Analysis
	フォレンジックエンジニア	システム企画担当	セキュアオペレーター	Legal Advice and Advocacy
	インベスティゲーター	基幹システム構築担当		Training, Education, and Awareness
	リーガルアドバイザー	基幹システム運用担当		Cybersecurity Management
	IT企画部門	WEBサービス担当		Strategic Planning and Policy
	ITシステム部門	業務アプリケーション担当		Executive Cyber Leadership
	情報セキュリティ監査人	インフラ担当		Program/Project Management
		サーバ担当		Cyber Defense Analysis
		DB担当		Cyber Defense Infrastructure Support
		ネットワーク担当		Incident Responder
		サポート・教育担当		Vulnerability Assessment and Management
		ヘルプデスク担当		Threat Analysis
		監査責任者		Exploitation Analysis
		監査担当		All-Source Analysis
		特定個人情報取扱責任者		Targets
		特定個人情報取扱担当		Language Analysis
		個人情報取扱責任者		Collection Operations
		個人情報取扱担当		Cyber Operational Planning
				Cyber Operations
				Cyber Investigation
				Digital Forensics

（参考）各スキルマップの変遷



名称	概要	2014以前	2015	2016	2017	2018
情報処理技術者試験・情報処理安全確保支援士試験（METI）	**情報処理技術者試験：** 「情報処理の促進に関する法律」に基づき経済産業省が、情報処理技術者としての「知識・技能」が一定以上の水準であることを認定している国家試験。 **情報処理安全確保支援士：** 最新のセキュリティに関する知識・技能を備えた、高度かつ実践的な人材に関する国家資格。 https://www.jitec.ipa.go.jp/	情報セキュリティアドミニストレータ試験 2001年～2008年 テクニカルエンジニア（セキュリティ）試験 2006年～2008年 2009年　春試験より 情報セキュリティスペシャリスト試験 2009年～2016年 CCSF		2016年　春試験より 情報セキュリティマネジメント試験	2017年　春試験より 情報処理安全確保支援士試験 情報処理安全確保支援士（登録） 支援士の想定業務を専門分野として具体化	
iコンピテンシディクショナリ(iCD)（IPA）	企業においてITを利用するビジネスに求められる業務（タスク）と、それを支えるIT人材の能力や素養（スキル）を「タスクディクショナリ」、「スキルディクショナリ」として体系化したもの。 **タスク: 50(大分類)、スキル：4(カテゴリ)** **タスク参照例: 6分類、99種類** https://icd.ipa.go.jp/icd/	2007年： 情報処理技術者試験と3スキル標準の統合を企図 2009年： CCSFに準拠した試験体系 CCSF・追補版 2012年：公開 2014年：iCDに名称変更 「情報セキュリティ人材の育成指標等の策定事業(経産省)」成果	6/30 iCD2015 ITSS等で定義される職種とスキルDの職種を対応付け	6/6 iCD2016	iCDのタスク/スキルDを参照 6/20 iCD2017 2017年度で普及活動終了 → タスク/スキルD保持 8/17 iCD2018 ITSS+で定義される専門分野とスキルDを対応付け	
ITSS（METI/IPA）	各種IT関連サービスの提供に必要とされる能力を明確化、体系化した指標。 **タスク: 11職種・35専門分野　※職種は役割ではない** **スキル: 5カテゴリ** https://www.ipa.go.jp/jinzai/itss/download_V3_2011.html	ITSS、ETSS、UISS ITSS：2011年度以降、更新無し UISS：2011年度以降、更新無し ETSS：2013年度から民間移管				
ITSS＋（セキュリティ分野）（METI/IPA）	ITSSが対象としている情報サービスの提供や、ユーザー企業のIS部門に関わっている人材が「セキュリティ領域」等のスキル強化を図るための学び直しの指針として活用。 **専門分野: 13、タスク、スキルはiCDを参照** ※専門分野は専門的なセキュリティ業務の役割の観点により設定 https://www.ipa.go.jp/jinzai/itss/itssplus.html			IT人材の“学び直し”方向性を提示	4/7 ITSS+ ロールの対応関係をマッピング ITSS+（セキュリティ領域）における専門分野とSecBoKの役割（ロール）との関連を明確化	
SecBoK（JNSA）	情報セキュリティに関する業務に携わる人材が身に付けるべき知識とスキルを整理。 **役割: 16、スキル: 400弱** https://www.jnsa.org/result/2017/skillmap/	2003年：情報セキュリティスキルマップとして登場 2007年：SecBoKに名称変更 SecBoK2009以降、更新無し	NICE、iCDの双方に存在しないが、必要と思われるスキルは独自に追加 4/19 SecBoK 2016 ユーザー企業における人材の定義はNCAを参照 ベンダー企業における人材の定義はNRIで活用されているものを参照		8/21 SecBoK 2017	2018年度内 SecBoK 2018
CSIRT人材の定義と確保（NCA）	各企業のCSIRTにおいて必要な機能、体制、人材を明確化。 **機能: 4、役割: 15** **各役割ごとに任用前提/追加教育スキルを定義** http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf	2014年10月 CSIRT人材WG設立	11/16 Ver. 1.0 SecBoKの16の役割から、開発系を抜いた13の役割を参照		3/13 Ver. 1.5	
NICEフレームワーク（NIST）	サイバーセキュリティ業務の役割・専門分野と必要とされる知識・能力に関する共通言語と分類法を提供。 **7種類のカテゴリ、33専門分野に紐づくロール: 52** **各ロールに以下が紐づく** **タスク: 1007、スキル: 374、知識: 630、能力: 176** https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework	2010年 NICE立ち上げ 2013年4月 Ver. 1.0 2014年4月 Ver. 2.0			8月 Ver. 3.0	NICEフレームワークの改訂に適合
人材定義リファレンス（CRIC CSF）	企業におけるサイバーセキュリティ対策に必要とされる機能を明らかにし、それらの機能を遂行するために必要な人材が果たす役割を定義。 **機能: 29、役割: 30（IT領域）** **対応するスキルセットを定義** http://cyber-risk.or.jp/sansanren/xs_20160914_01_Report_1.0.pdf	2014年10月 経団連傘下に「サイバーセキュリティに関する懇談会」発足 2015年2月 経団連「サイバーセキュリティ対策の強化に向けた提言」公開	2015年6月 提言を受け「産業横断サイバーセキュリティ人材育成検討会（CSF）」が発足 9/14 人材定義リファレンス（IT領域） タスク、ロールは独自に定義		2017年4月 CSFを（一社）サイバーリスク情報センター（CRIC）の委員会として組織改編	11/21発表予定 人材定義リファレンス（OT領域） NICEフレームワークが定めるセキュリティ対策への対応がベース
統合セキュリティ人材モデル（サイバーセキュリティ人材育成スキーム策定共同プロジェクト）	セキュリティ事故対応やサイバー攻撃監視などといった、各セキュリティ人材として習得すべきスキルセットを体系化し、共通的に利用できる統合セキュリティ人材モデルを策定 **役割: 14、対応するスキルセットを定義** https://jpn.nec.com/press/201810/20181024_03.html				2017年1月 NEC、富士通、日立の3社で検討開始 2017年12月 プロジェクト発足(ニュースリリース)	10/24 統合セキュリティ人材モデル

サイバーセキュリティ対策を支える基盤となる
サイバーセキュリティ人材育成・活躍促進パッケージ

① 『セキュリティ人材活用モデル』の作成

- **役割定義の整理**
- **委託調査**

② 戦略マネジメント層の育成

- **育成プログラムの提供**

③ 産学官の連携強化

- **高専との連携の具体化**
- **地域的取組の促進**

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育成の取組み状況

- IPA産業サイバーセキュリティセンターにおいて、企業におけるリスク管理に関わる責任者クラス向けに「戦略マネジメント系セミナー」を本年11月から実施。
- 一橋ビジネススクールICSの協力で、カリキュラムにサイバーセキュリティを組み込んだ「デジタル・トランスフォーメーション時代における経営人材育成プログラム」を本年9月から実施。

	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」	一橋ビジネススクールICS協力「デジタル・トランスフォーメーション時代における人材育成プログラム」
対象者	• CISO、CIOに相当する役割を担っている方 • 総務部門、生産部門等の統括責任者・マネージャークラスの方 • その他、企業においてリスク管理に関わる方全般	• 30代後半～40代の社会人 • 所属組織で次世代の経営を担うことを期待される方 • 現在も経営トップへのアドバイスが期待される方
実施期間	• 平成30年11月～12月（全７回）	• 平成30年9月～（全17回） ※修了式を除く。
カリキュラム	• 「企業におけるサイバーセキュリティ対策の機能」をメインテーマに講義・演習・ケースディスカッションを通じて熟議	• 経営戦略・知識経営等のコアコース • 世界の先進的IT戦略の集中講義 • サイバーセキュリティ、個人情報保護等の講義
受講者実績	• 17名（中核人材プログラム3名を含む。）	• 30名

サイバーセキュリティ対策を支える基盤となる
サイバーセキュリティ人材育成・活躍促進パッケージ

① 『セキュリティ人材活用モデル』の作成

- 役割定義の整理
- 委託調査

② 戦略マネジメント層の育成

- 育成プログラムの提供

③ 産学官の連携強化

- 高専との連携の具体化
- 地域的取組の促進

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。
- このため、高専機構、NISC、経産省、IPA、CRIC CSF、JNSA、JUASが参加し、高専の抱えるニーズに基づき、各関係機関の協力内容を具体化していくための議論をスタート。

＜高専・産・官の対話の場（イメージ）＞

継続的な協力体制

学　高専機構　等
- ■高度セキュリティ人材、情報系人材、非情報系人材
- ■教員　等

産　企業・業界団体
- ■CRIC CSF、JUAS、JNSA
- ■ユーザー企業、IT・セキュリティベンダー　等

ニーズ・シーズの整理・具体化 ▶ 協力の検討 ▶ 産業界に求められるセキュリティ人材の育成・輩出

- ・トップガンの育成支援
- ・キャリア教育
- ・機械・建築・生物等の分野別教材の開発・素材提供
- ・セキュリティ教員向けのFD（Faculty Development）
- ・講師派遣
- ・産業界に求められるセキュリティ人材像の共有
- ・適切なプレイヤーとのマッチング

官　関係省庁・独法等
- ■NISC、文科省
- ■IPA、JPCERT/CC　等

国立高専におけるセキュリティ教育の現状と産学官連携強化の方向性

- 既に開発済みの教材・演習等もあるが、特に応用的内容・分野別のものについては産業界等から協力を得つつ継続的にアップデートされることが望ましい。
- 学生の専攻やセキュリティスキルレベル等によって、求められる教材・演習等やマッチングすべき団体は様々であるため、今後、個別に具体的協力についての議論を深める。

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

約 1 %
トップガンの学生
→ 主に**セキュリティ企業**に就職

約20%
情報系学科の学生
→ 主に**IT企業**に就職

約80%
非情報系学科の学生
→ 主に**ユーザー企業**に就職

KOSEN 国立高等専門学校機構
国立高専教員

文科省予算等で開発された教材・演習等

- 情報モラル教材・情報リテラシー教材（全学科）
- 各専門分野別教材（各学科）
- セキュリティ基礎教材（情報系・一部学科）
- 情報セキュリティ管理者教材（情報系学科）
- 高度人材向け講義教材（情報系学科）
- ・高度セキュリティ合宿（2日間）
  ・KOSENセキュリティコンテスト（3日間）等
- ・情報系教員向け研修（3日間）
  ・高度セキュリティ研修（２日間）
  ・サイバー攻撃対策演習（5日間）等

産・官との連携の具体化の方向性

高専機構のニーズ①：
産業界の第一線で活躍するトップガンやホワイトハッカーからの講義・キャリア教育　等
⇒ IPA、JNSA等と協力の具体化について協議

高専機構のニーズ②：
セキュリティ知識を活かして働くITベンダー社員からのキャリア教育、教材提供　等
⇒ IPA、JNSA、ITベンダー等と協力の具体化について協議

高専機構のニーズ③：
機械・建築・材料・化学等の分野ごとの特徴に応じた教材の開発・素材提供　等
⇒ CRIC CSF、JUAS等と協力の具体化について協議

高専機構のニーズ④：
教員のFaculty Development (FD)
⇒11月15日の情報担当教員向け研修にJPCERT/CCから講師を派遣。IPA、JNSA等と協力の具体化について協議

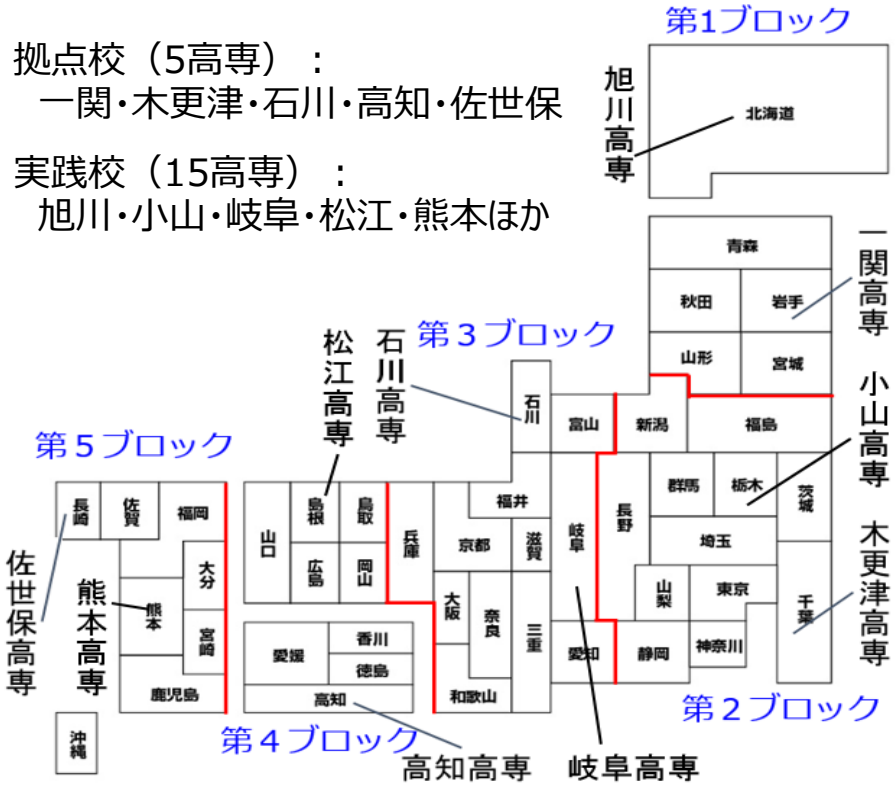
（参考）高専制度の概要

- 高専は、国立51校、公立3校、私立3校が存在。15歳から5年一貫（より高度な教育を実施する専攻科の場合はさらに２年）の技術者教育を行う。
- 各高専ごとに設置されている学科は様々であるが、高知高専等20か所の国立高専において、情報セキュリティ人材の発掘・育成が重点的に実施されている。
- 国立高専では、本科（1～5年生）に約50,000名、専攻科（1～2年生）に約3,000名の学生が在籍しており、毎年約1万人の技術者を輩出。なお、就職先の上位はユーザー企業となっている。

＜国立高専における情報セキュリティ教育重点校＞

拠点校（5高専）：
一関・木更津・石川・高知・佐世保

実践校（15高専）：
旭川・小山・岐阜・松江・熊本ほか



出典：文部科学省提供資料から

＜国立高専生　就職先ランキング（2018年度）＞

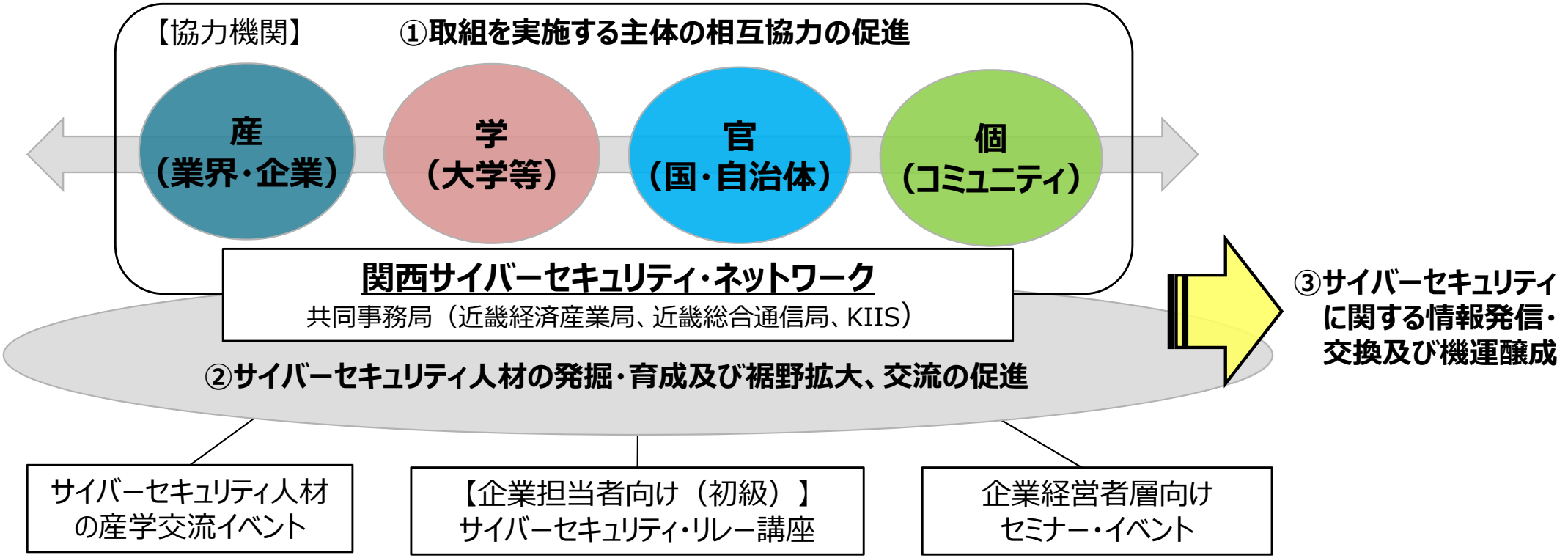
就職先の上位はユーザー企業（非ICT企業）

順位	企業名	採用人数（人）	前年度比（人）
1	JR東海	80	8
2	サントリーグループ（※グループ会社含む）	66	6
3	花王	65	10
4	旭化成	60	8
5	ダイキン工業	57	4
6	三菱電機ビルテクノサービス	49	▲ 3
7	中部電力	48	5
	関西電力	48	2
	JXTGエネルギー	48	2
10	東京ガス	45	4
	メンバーズ	45	14

出典：日経産業新聞　2018年10月19日付
(https://www.nikkei.com/article/DGXMZO36700480191020 18X11000/)より経済産業省作成

地域的取組の推進：関西サイバーセキュリティ・ネットワーク

- 近畿経済産業局、近畿総合通信局、(一財)関西情報センター(KIIS)が共同事務局となり、関西のサイバーセキュリティ人材発掘・育成及び裾野拡大に関心を有する産学官等の相互協力を促進。
- 関西におけるサイバーセキュリティの重要性についての認識の醸成及び情報交換の活性化を図るとともに、人材の発掘・育成及び裾野拡大の円滑化を進める。
- 11月12日にキックオフ。その後、リレー講義、企業経営者層向けセミナー等を実施予定。



（参考）関西サイバーセキュリティ・ネットワークの体制

【協力機関】※以下の機関等はあくまで発足時であり、順次拡大を想定。

カテゴリ		主な機関等
産	業界団体・ 経済団体	関西経済連合会、関西経済同友会、大阪商工会議所、神戸商工会議所、京都商工会議所、 関西ものづくりIoT推進連絡会議関係団体（18団体：IT・電気計測器・電子電機・電子部品）、 近畿情報通信協議会、日本ネットワークセキュリティ協会（JNSA）西日本支部、ISACA（情報システムコントロール協会）大阪支部
	セキュリティベンダー	神戸デジタル・ラボ、ファイア・アイ、ラック
	情報通信企業	NTT西日本、オージス総研、NEC、富士通、日立製作所、さくらインターネット
	ユーザー企業	パナソニック、関西電力、大阪ガス、ダイキン工業、毎日放送、朝日放送テレビ、読売テレビ放送
学	大学・大学院	神戸大学、兵庫県立大学、和歌山大学、大阪経済大学、立命館大学情報理工学部上原研究室、 奈良先端科学技術大学院大学サイバーレジリエンス構成学研究室
	研究機関	産業技術総合研究所（AIST）、情報通信研究機構（NICT）
官	国関係機関	内閣官房内閣サイバーセキュリティセンター（NISC）、情報処理推進機構（IPA）
	自治体	大阪府、大阪市
個	セキュリティコミュニティ	総関西サイバーセキュリティLT大会、OWASP Kansai、tktkセキュリティ勉強会

（順不同）現在40機関

【共同事務局】

近畿経済産業局、近畿総合通信局、一般財団法人関西情報センター（KIIS）

（参考）関西サイバーセキュリティ・ネットワーク　平成30年度 取組内容（予定）

（１）関西サイバーセキュリティ・ネットワーク　キックオフフォーラム

●日時：11月12日（月）13:30～17:00
●会場：グランフロント大阪　タワーC8階会議室（C03+C04）
●参加者数：200名程度（想定）
●内容：　**※講演テーマは予定**
○主催者挨拶　森 清（近畿経済産業局長）
○基調講演　大橋 秀行（近畿総合通信局長）
○特別講演
・伊東 寛（ファイア・アイ CTO、前経済産業省サイバーセキュリティ・情報化審議官、元陸上自衛隊システム防護隊隊長）
○パネルディスカッション
「サイバーセキュリティの普及と人材の発掘・育成について」
・（コーディネータ）森井 昌克（神戸大学大学院 教授）
・（パネラー）
【学】上原 哲太郎（立命館大学　教授）
申 吉浩（兵庫県立大学大学院 教授）
【産】黒田 吉広（西日本電信電話株式会社 代表取締役副社長）
吉村 宏之（パナソニック株式会社　製品セキュリティセンター 製品セキュリティ行政部 部長）
【官】奥山 剛（近畿経済産業局　地域経済部長、元内閣サイバーセキュリティセンター参事官）
○閉会挨拶　森下 俊三（一般財団法人関西情報センター会長）
○交流会（17:30～）

（２）【企業担当者向け(初級)】サイバーセキュリティ・リレー講座

●日時：11下旬～1月下旬 16:30～18:00（予定）
●会場：KIIS会議室
●参加者数：40名程度（想定）
●対象者：企業でサイバーセキュリティを担当する者（初級者）
●内容：　**※講演テーマは予定**
「サイバーセキュリティの専門性を高めるにあたっての心得」
① 11/29【申先生】AIとサイバーセキュリティ
② 12/3　【上原先生】フォレンジック技術
③ 12/5　【五十部先生】暗号技術に基づくサイバーセキュリティ
④ 12/21【川橋先生】ネットワーク運用とそのセキュリティ対策
⑤ 1/10　【森室長】サイバーフィジカルシステムにおけるセキュリティ
⑥ 1/22　【金子先生】サイバーセキュリティマネジメント
⑦ 1/28　【森井先生】無線LAN及びLPWAにおけるセキュリティ
（又はマルウェア（コンピュータウィルス）総論）及び総括

○受講修了証：
原則全講義に参加し、一定水準以上の理解が認められる場合（各回の講義後に簡単なテストを出題し理解度を確認）、関西サイバーセキュリティ・ネットワーク事務局から受講修了証を授与（自主認証）し、希望者については事務局機関HP等に所属・氏名等を掲示する。

（３）企業経営者層向けセミナー・イベント

●日時：11月以降　※サイバーセキュリティ月間（2/1～3/18）も念頭
●内容：　①大企業経営者向け、中小企業経営者向けセミナーやイベントコラボ（経済団体・業界団体との連携）
②サイバーセキュリティ人材をテーマとした、企業経営者層との対話企画等

1．経営

2．人材

3．国際

ASEAN等向け日米サイバー共同演習　概要

- 多くの日本企業がサプライチェーンを共有するASEAN各国等のサイバーセキュリティ対応能力の向上のため、**米国国土安全保障省（DHS）と連携**し、**ASEAN等向けの日米共同演習を今年初めて開催。**

■**開催日時**：2018年9月10～14日(以降毎年9月に開催)

■**開催場所**：東京

■**内　　容**：重要インフラにおける制御システムのセキュリティに関する5日間の講義・演習

■**参 加 者**：IPA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 83名
ASEAN10ヶ国、韓、台、印、豪、NZ 36名
DHS/NCCIC 講師5名　ほか

■**開講挨拶**：武藤容治　経済産業副大臣
ウィリアム・F・ハガティ 駐日米国大使
富田達夫 IPA理事長

武藤副大臣ご挨拶（フジTVより）

ハガティ大使ご挨拶（大使のTwitterより）

＜日米以外の参加国＞

ASEAN等向け日米サイバー共同演習　概要

- DHS/NCCICによる講義や日本人講師による実機を用いた講義等を5日間にわたり実施。

■2018年9月10～11日　■2018年9月12～14日

OTセキュリティの基礎を学習
101, 201演習（NCCIC講師）

制御システムを用いた演習
J202演習（ICSCoE講師）

模擬プラントを用いた講義
（ICSCoE講師）

プラクティス共有等
（DHS/METI/日米の企業）

【ASEAN等からの参加者の声】

・全体を通してとても情報量が多く包括的だった。
・演習前はOTはセキュアだと思っていたが、演習後、ハッカーがどのようにシリアル通信やPLCを攻撃するのか理解できた。
・自企業でITとOTを統合しているところであり、良いタイミングで学ぶことが出来た。
・得られた情報を国に持ち帰り共有したい。

【日本人参加者（ICSCoE研修生）からの声】

・取組の進んでいる米国がICSセキュリティをどう考えているか分かりとても有意義だった。
・全てにおいて内容が濃くとても参考になった。
・米国やASEAN等の方々との交流も充実しており有益な議論が出来た。

（参考）インド太平洋地域の維持・促進に向けた日米協力の例

- 9月26日の日米首脳会談において示された「インド太平洋地域の維持・促進に向けた日米協力の例」において、日米サイバー共同演習が取り上げられた。

出典：ホワイトハウスHP

FACT SHEETS

President Donald J. Trump and Prime Minister Shinzo Abe Are Working Together to Maintain a Free and Open Indo-Pacific

ECONOMY & JOBS | Issued on: September 28, 2018

★ ★ ★

"Let us work together for a peaceful, prosperous, and free Indo-Pacific."

President Donald J. Trump

⋮

ENERGY: The United States and Japan are cooperating to promote energy security and access in the Indo-Pacific, including through the Japan-United States Strategic Energy Partnership.

⋮

INFRASTRUCTURE AND DEVELOPMENT FINANCE: The United States and Japan seek to ensure that infrastructure knits the Indo-Pacific region together, generates local wealth, and leads to sustainable growth.

⋮

DIGITAL ECONOMY AND CYBERSECURITY: Cyberspace increasingly will be an engine of economic growth and innovation in the Indo-Pacific.

⋮

MARITIME SECURITY AND DISASTER RISK REDUCTION: The United States and Japan are building capacity to advance the region's rules-based maritime order, and to boost resiliency to natural disasters that threaten lives and property and disrupt commercial activity.

DIGITAL ECONOMY AND CYBERSECURITY: Cyberspace increasingly will be an engine of economic growth and innovation in the Indo-Pacific.

- The United States and Japan are working together to foster a vibrant and resilient Indo-Pacific digital economy and ensure a secure cyber future.
- To bolster the cybersecurity defenses of critical infrastructure and promote focus on industrial control system security, the U.S. Department of Homeland Security and METI conducted joint training on industrial control systems for ASEAN member countries and other Indo-Pacific partners in September 2018.
- The United States is cooperating with Japan in providing capacity building and technical support to the Pacific Islands.

米国国土安全保障省（DHS）と経済産業省（METI）は、重要インフラのサイバーセキュリティの促進と制御システムセキュリティの推進のため、ASEANや他のインド太平洋諸国向けに、2018年9月に制御システムセキュリティに関する共同演習を実施。

マルチ・バイを通じた国際協調への取り組み

- **「サイバー・フィジカル・セキュリティ対策フレームワーク」**を軸に、各国のステークホルダーと議論、マルチの会議で紹介し、サイバー・フィジカル・セキュリティに関する共通の認識を醸成。

- **Broad Band for All (BB4ALL)（2018年6月@スウェーデン・ストックホルム）**
  - Ericsson主催の国際会議においてサイバー・フィジカル・セキュリティ対策フレームワークを紹介。
- **RSA Conference 2018 Asia Pacific & Japan（2018年7月@シンガポール）**
  - サイバー・フィジカル・セキュリティ対策フレームワークを含む当省の取組について紹介。
- **APEC TEL57（第57回電気通信・情報作業部会）（2018年6月@PNG）**
  - Security and Prosperity Steering Group (SPSG)の「IoT Security Workshop」で、サイバー・フィジカル・セキュリティ対策フレームワークについて紹介。
- **APEC TEL58（第58回電気通信・情報作業部会）（2018年10月@台湾・台北）**
  - デジタルエコノミーにおける戦略と対策に関するシンガポール主催のWSにおいて、サイバー・フィジカル・セキュリティ対策フレームワークについて紹介。
- **2nd Global Cyber Dialogue（米国商工会議所主催）（2018年10月@DC）**
  - 米（DHS、NIST、国務省、商務省）、英、仏、EC等37の国・地域における影響力のある政策担当者や代表的な民間企業と、サイバーセキュリティ政策について議論。
- **Asia-Pacific Conference of German Business（2018年11月@ジャカルタ）**
  - ドイツの産業団体が主催。NTTセキュリティから我が国のセキュリティ技術等について紹介。