経済産業省

資料３

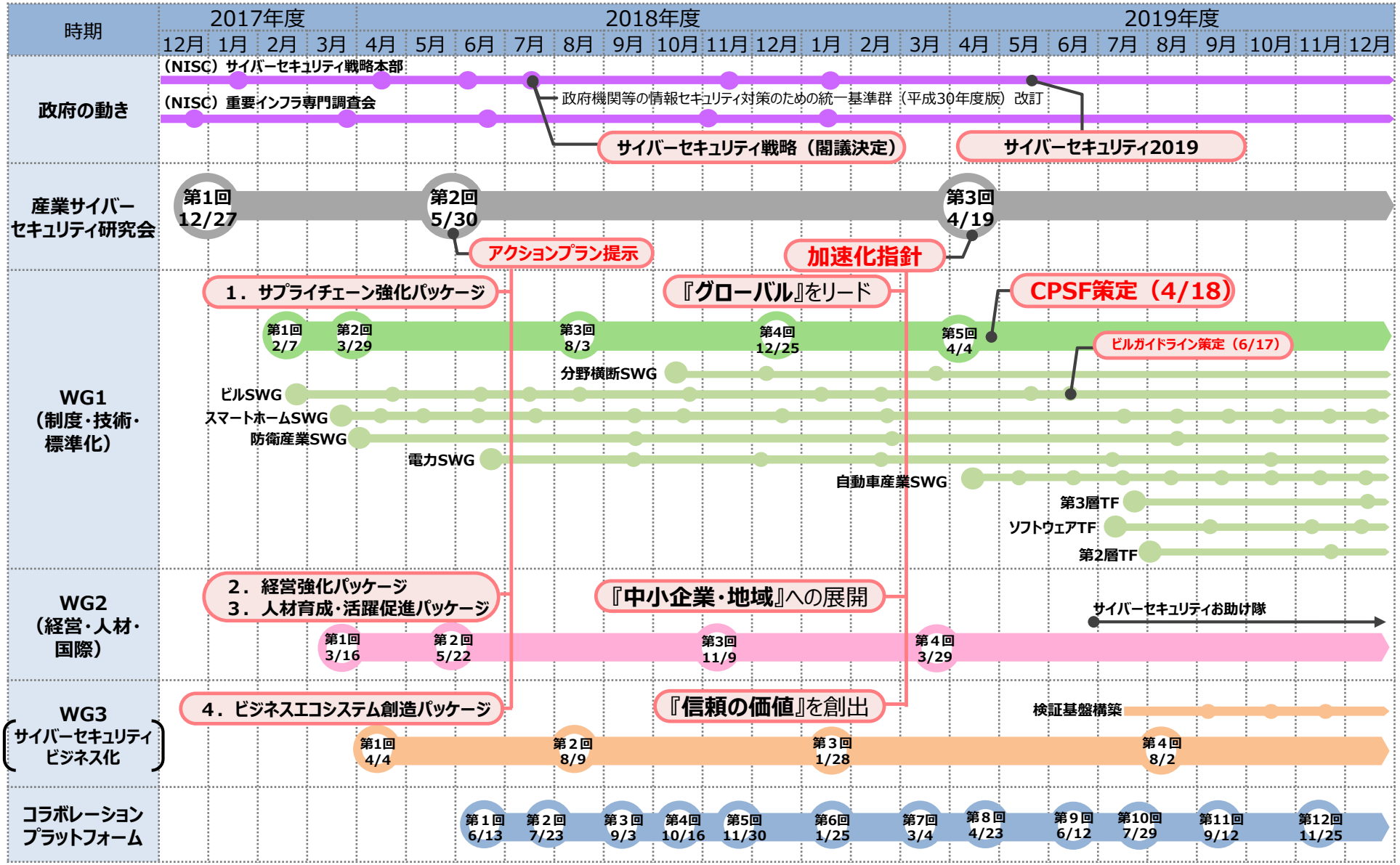
事務局説明資料

経済産業省

商務情報政策局

サイバーセキュリティ課

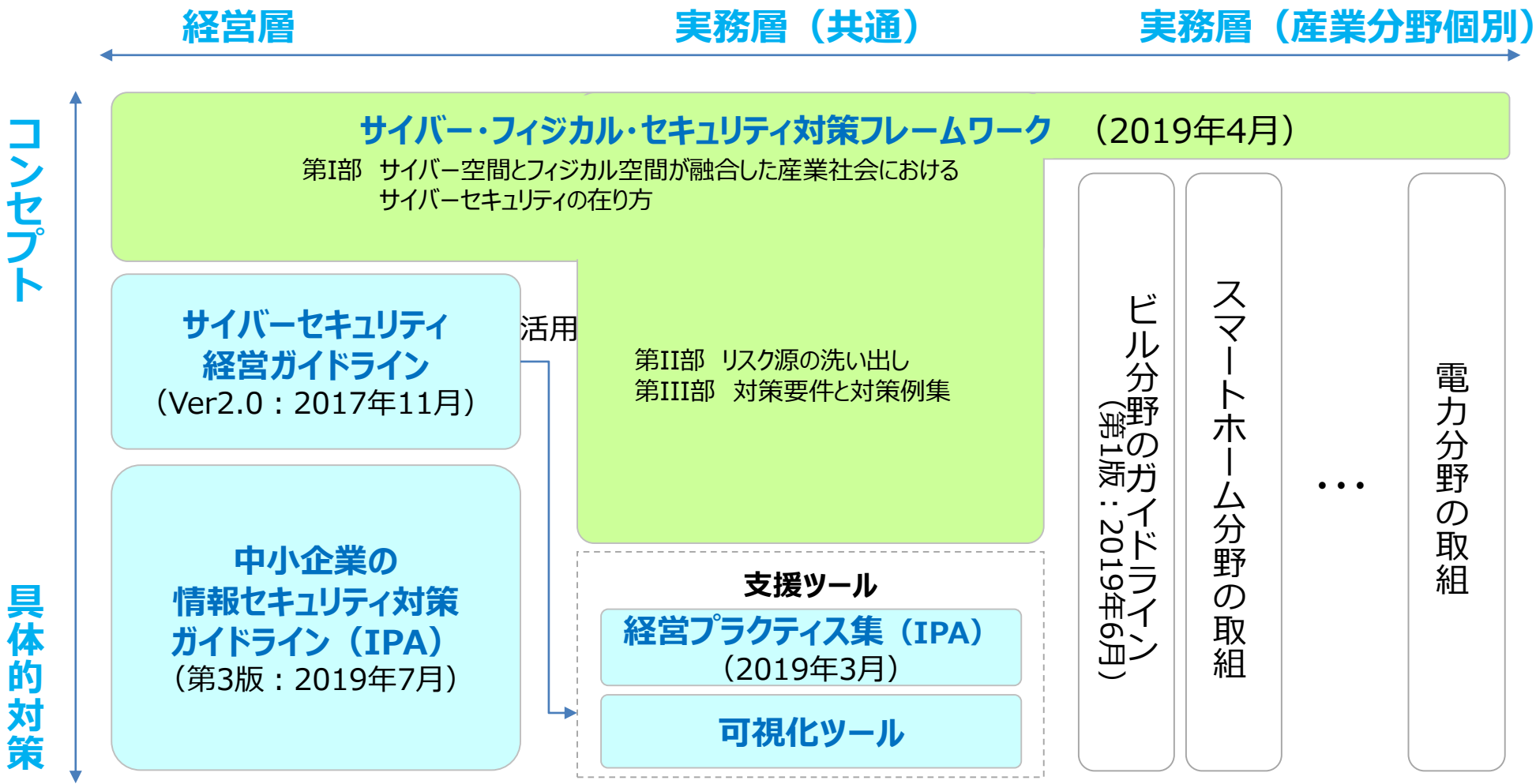
産業サイバーセキュリティ研究会関連の動き



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とした各種取組

- **「サイバー・フィジカル・セキュリティ対策フレームワーク」では、Society5.0における産業社会でのセキュリティ対策の全体枠組みを提示。**
- 全体の枠組みに沿って、対象者や具体的な対策を整理し、『サイバーセキュリティ経営ガイドライン』や産業分野別のガイドラインなどの実践的なガイドラインを整備。

＜各種取組の大まかな関係＞



1．経営

2．中小･地域

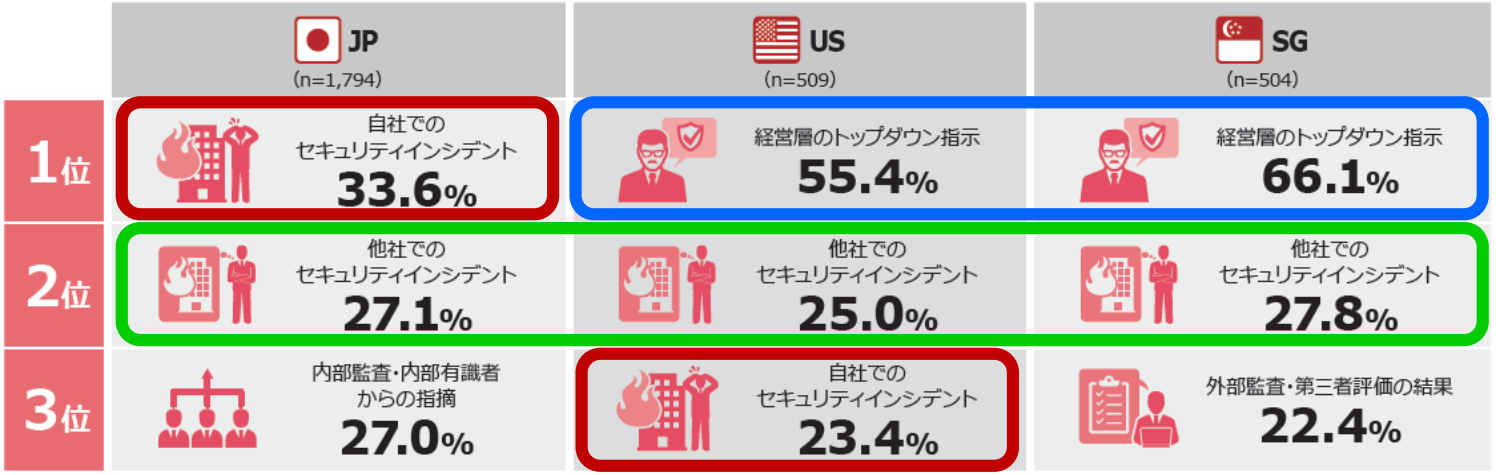
3．人材

4．国際

サイバーセキュリティ経営に関する各国企業の実態

- セキュリティ対策実施のきっかけや理由が、米・星では**経営層からの指示**であるのに対して、日本では**インシデント**が上位を占めている。一層のサイバーセキュリティ経営の促進が必要。

情報セキュリティ対策実施のきっかけや理由



※ 他選択肢:株主や取引先からの要請 / 関連法規の改定 / 監督省庁からのセキュリティ対策の要請

- 米/星の1位は共通して「経営層のトップダウン指示」であり、経営層がリーダーシップを発揮し、セキュリティ対策を実施する企業の割合が高かった。なお、日本の「経営層のトップダウン指示」の割合は23.7%で4位であった。
- 日本の1位は「自社でのセキュリティインシデント」で、発見した事象に対する事後的な対応である。日本企業のセキュリティ対策実施の位置づけは依然「コスト」であり、インシデントが発生したことでようやく経営層が対策の必要性を認識したといったケースが多いのではないかと考えられる。
- なお、各国共に2位は共通して「他社でのセキュリティインシデント」であった。対策のきっかけとなる外的要因として、他社のセキュリティインシデントが最も影響を与えていることがわかる。

（出典）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2019」
調査対象：日本、アメリカ、シンガポール企業の情報システム/情報セキュリティ担当者　回答企業：計2,807社（日本：1,794社、アメリカ：509社、シンガポール：504社）

段階的なサイバーセキュリティ経営の実現

- 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(コーポレート・ガバナンス・システム)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

2nd step

サイバーセキュリティ経営の実践（2nd step）の取組

- 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(コーポレート・ガバナンス・システム)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

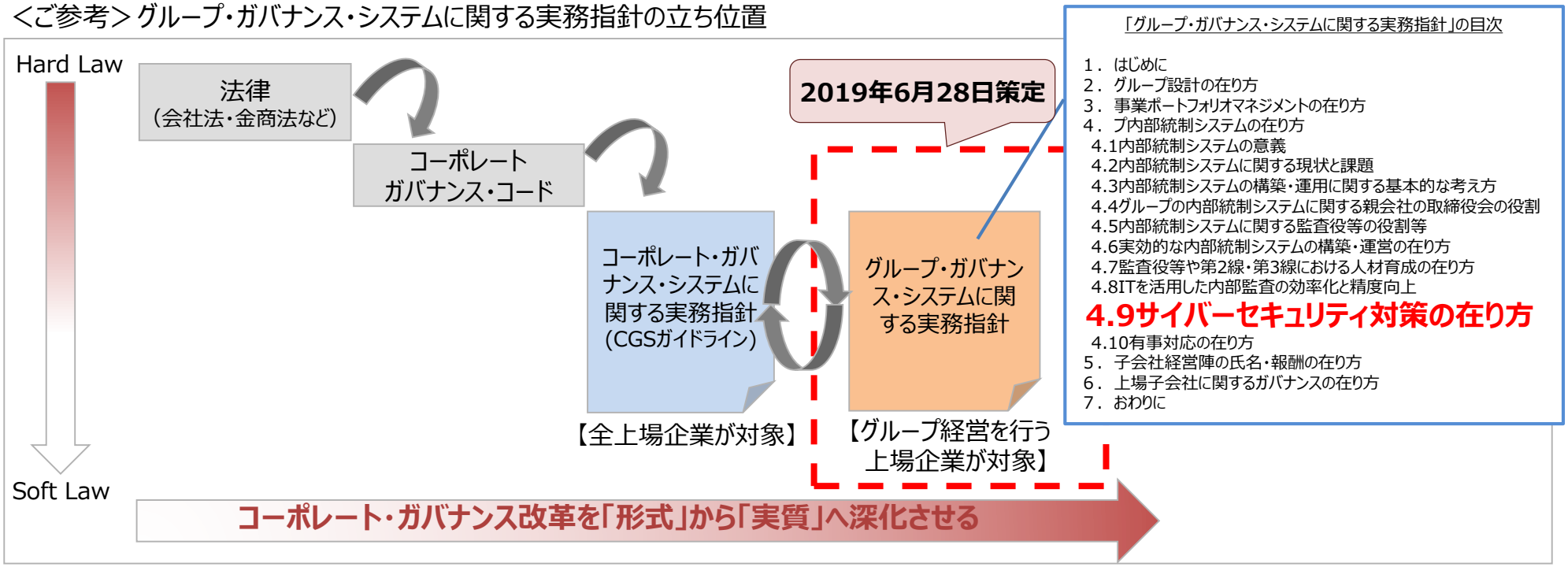
- セキュリティの高い企業であることを投資家が評価できるようにするための、サイバーセキュリティ経営に関する情報の開示の在り方の検討

2nd step

コーポレートガバナンスの一環として、サイバーセキュリティ経営を位置づけ

- **海外では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認識**しており、経営層のサイバーセキュリティへの関わりを重要視。
- 「グループ・ガバナンス・システムに関する実務指針(グループガイドライン)」において、**グループ内部統制システムの一つとして、サイバーセキュリティ対策の在り方を位置づけ**。(2019年6月公表)
- 親会社の**取締役会レベルで、子会社も含めたグループ全体、更には関連するサプライチェーンも考慮に入れてセキュリティ対策を行うことを検討すべき**ことを明記。

<ご参考> グループ・ガバナンス・システムに関する実務指針の立ち位置



（出典）第13回CGS研究会資料より抜粋

2nd ～ 3rd step

サイバーセキュリティ経営ガイドラインベースの可視化ツール

- 自社の可視化、投資家等ステークホルダー向けの可視化を段階的に実現することにより、2nd step と 3rd step をつなぐ。

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(コーポレート・ガバナンス・システム)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

可視化ツール

- **自社内の可視化**
- **投資家等ステークホルダー向けの可視化**

3rd Step

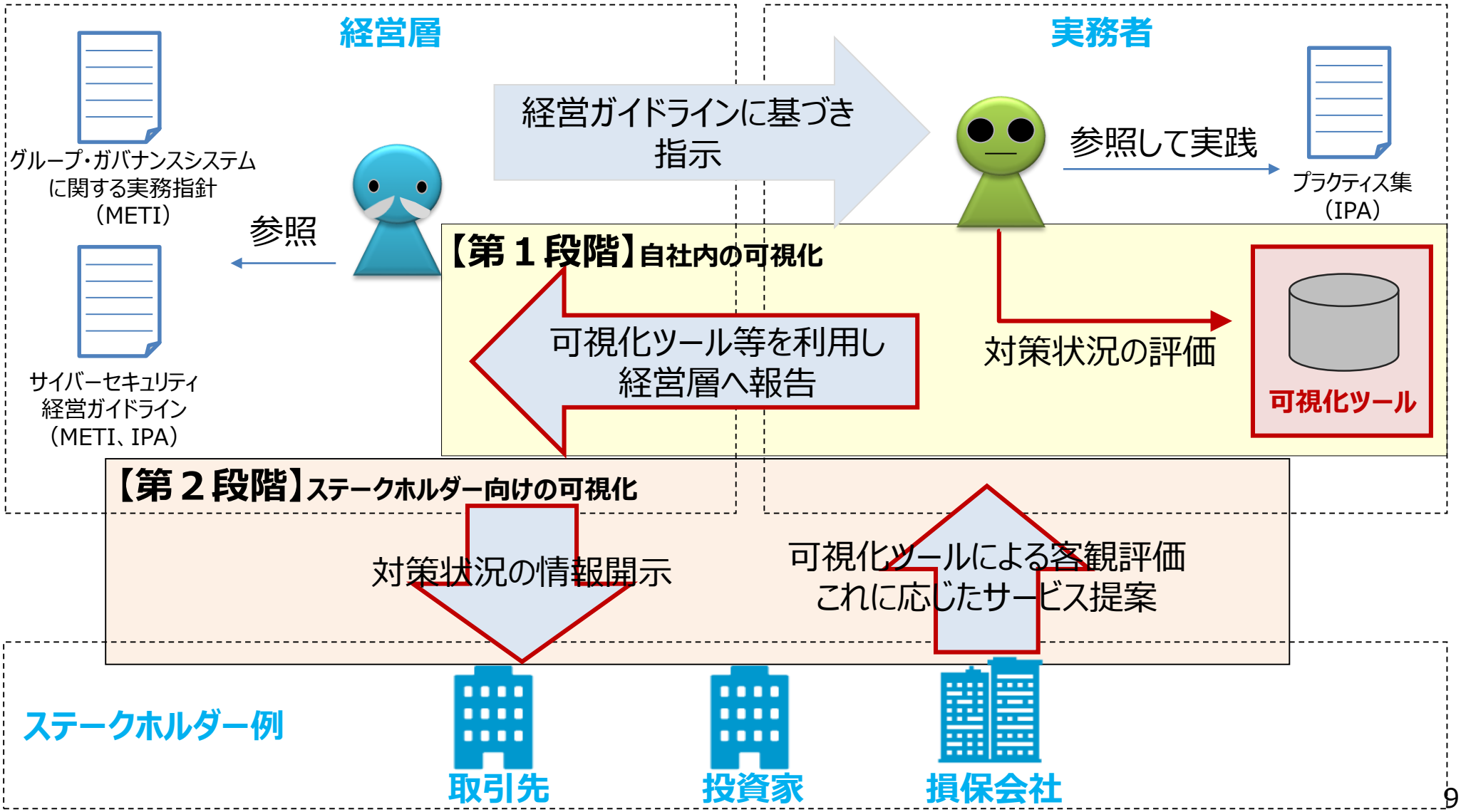
セキュリティの高い企業であることの可視化

- 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

可視化ツールの作成により目指すサイバーセキュリティ経営

2nd ～ 3rd step

- 経営ガイドライン、プラクティス集、可視化ツールを活用することで、実践的かつステークホルダーの信頼にも結び付くサイバーセキュリティ経営につながる。



段階的なβテストを経た可視化ツールの展開

2nd ～ 3rd step

- 今年度中に可視化ツールのβ版を用意し、来年度以降、ユーザ企業、投資家等ステークホルダーにそれぞれβテストを行う。
- βテストを踏まえた修正後、可視化ツールV1.0をリリースし、広く展開する。

2019年度中	**可視化ツールβ版（Excel）**の策定、公開
2020年度	【第１段階】**ユーザ企業**においてβ版をテスト - JUAS等と連携し、ユーザ企業のフィードバックを収集
2020年度以降	【第２段階】**投資家等ステークホルダー**においてβ版をテスト - 機関投資家、保険会社等のフィードバックを収集
2020年度以降	可視化ツール**V1.0リリースと本格展開** - マスプロモーション

- 自社及び自社グループ、サプライチェーン内の可視化
- 業界他社との比較（2020年度 Web版開発予定）
- セキュリティ対策レベルをステークホルダー向けに可視化
- 2nd stepと3rd stepをつなぎ、サイバーセキュリティ経営を実現

可視化ツールの策定に向けた基本方針とイメージ

2nd ～ 3rd step

- 可視化ツールのメインターゲットユーザー及び要件の案は以下のとおり。

<ターゲットユーザー>

- 従業員３００名以上の企業

  ※大企業が自社と取引する中小企業を対象とすることは可。それ以外の中小企業は『中小企業の情報セキュリティ対策ガイドライン』、『5分でできる！情報セキュリティ自社診断』を利用する。

- 経営層やステークホルダーに対する自社の対策状況の説明に活用
- 簡易に自己診断を行いたい企業

  ※詳細なアセスメントについてはコンサル等による民間のサービスの活用を想定

<要件>

1．セルフチェック方式

① 経営ガイドライン【付録Ａ】をベースに、NIST Cybersecurity Framework等を踏まえて見直し

② 質問数は50項目以下（ユーザ負担を考慮。なお、現在の付録Ａは41項目）

③ 回答は３～５段階で、主観や曖昧さをできるだけ排除し、クリアに回答できるように

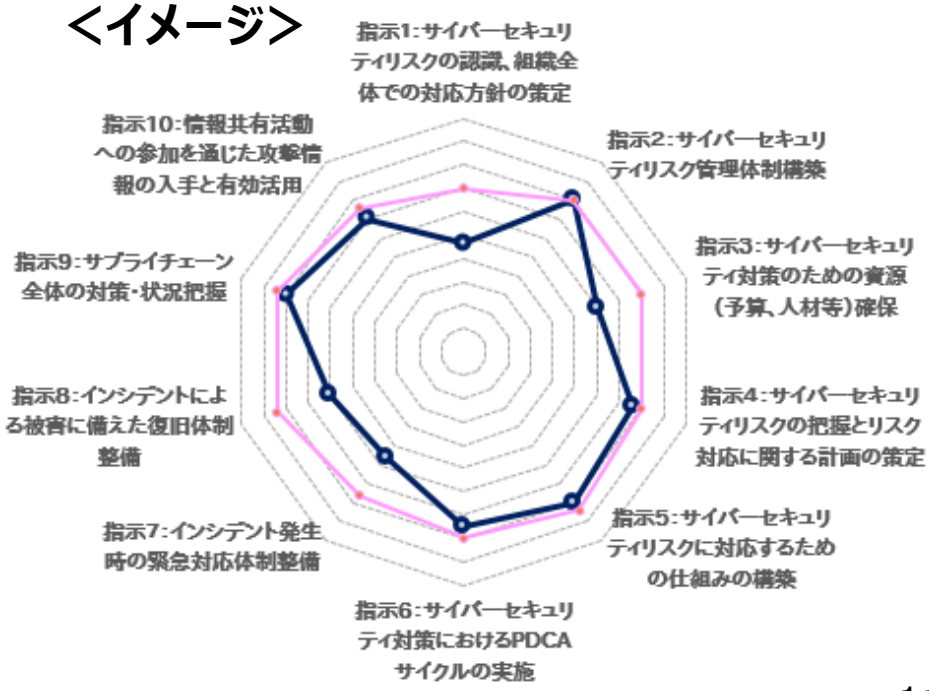
2．定量的な可視化

全体を通しての設問粒度の整合

3．他社比較が可能

業種・業界に特化しない共通の評価項目

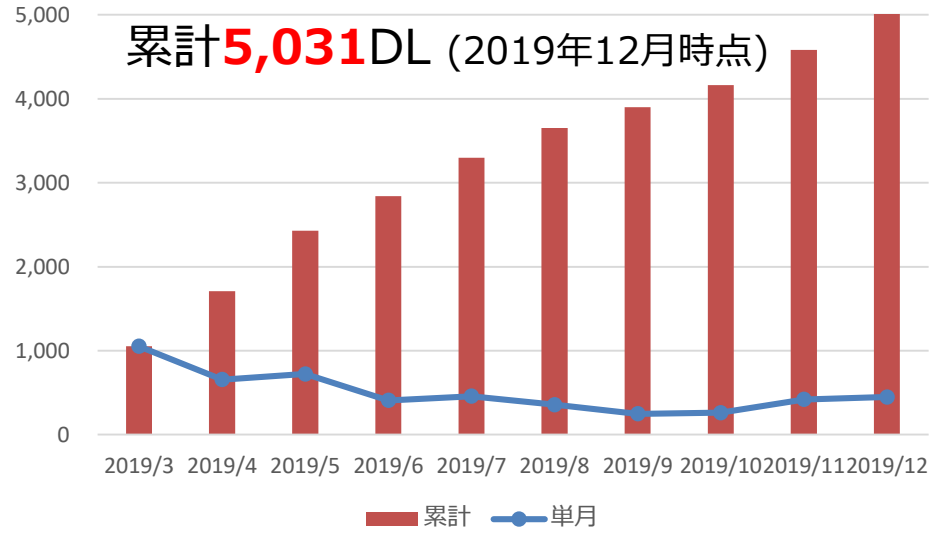
<イメージ>



（参考）『サイバーセキュリティ経営ガイドラインVer2.0実践のための経営プラクティス集』のアップデート状況

- 2019年3月25日にIPAより公開した「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」について、昨年度収集していない指示項目を中心にプラクティスを収集中であり、**今年度中にアップデート版を公開予定。**

<プラクティス集のダウンロード数推移>



【参考】上場企業数　第一部　2,157社
　　第二部　488社
（日本取引所グループ公表 2019年12月17日時点）

【参考】プラクティス集　目次

第一章：経営とサイバーセキュリティ

<経営者、CISO等向け>
なぜサイバーセキュリティが経営課題となるのか等を解説

第二章：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

<CISO等、セキュリティ担当者向け>
企業の具体事例をベースとした重要10項目の実践手順、実践内容、取り組む際の考え方を解説

第三章：サイバーセキュリティ対策を推進する担当者の悩みと解決のプラクティス

<セキュリティ担当者向け>
サイバーセキュリティ対策を実践する上での悩みに対する、企業の具体的な取組事例を紹介

<今年度アップデート予定の指示項目>

- 指示4　リスクの把握と対応計画策定（リスクアセスメント手法）
- 指示6　PDCAの実施（リスク管理に関するKPIの定め方、是正措置の実施方法、情報開示の手法）
- 指示10　情報共有活動への参加（情報の提供方法、入手した情報の活用方法）

１．経営

２．中小･地域

３．人材

４．国際

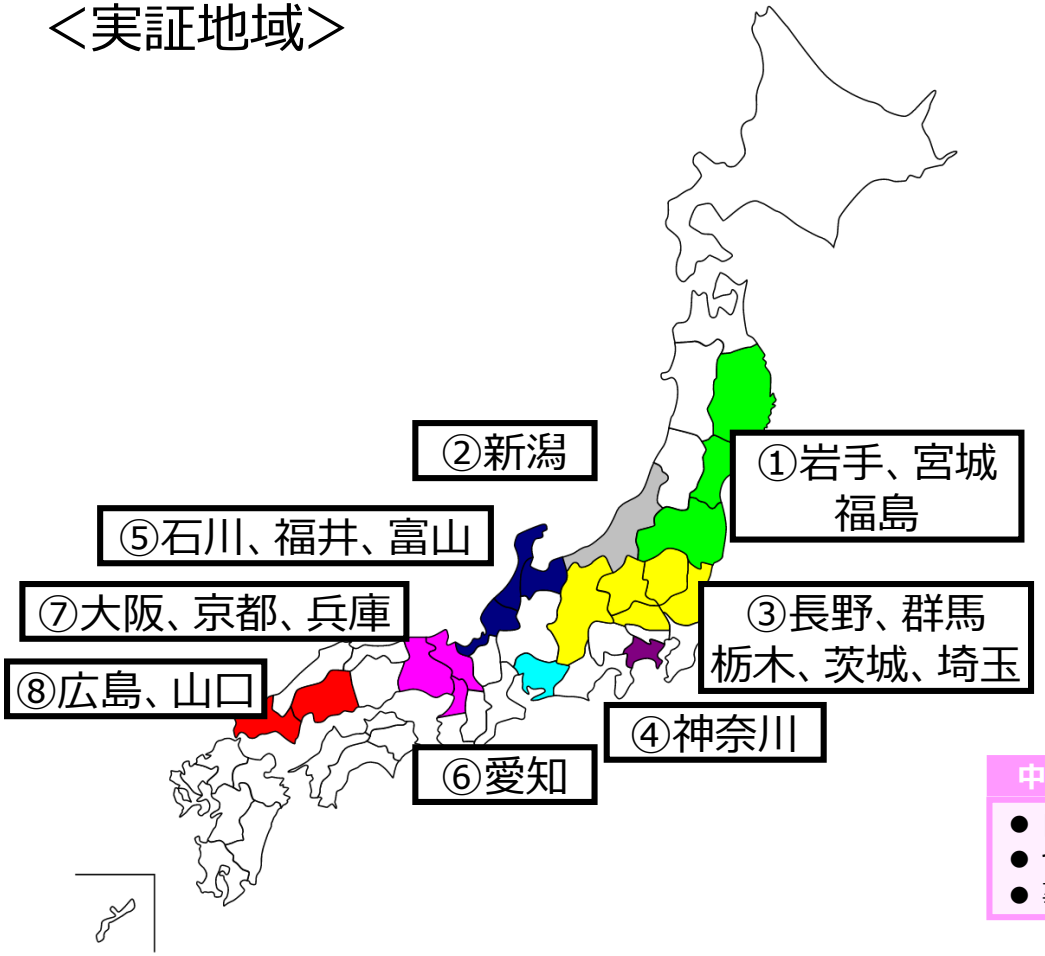
（１）サイバーセキュリティお助け隊

（２）地方版コラボレーション・プラットフォーム

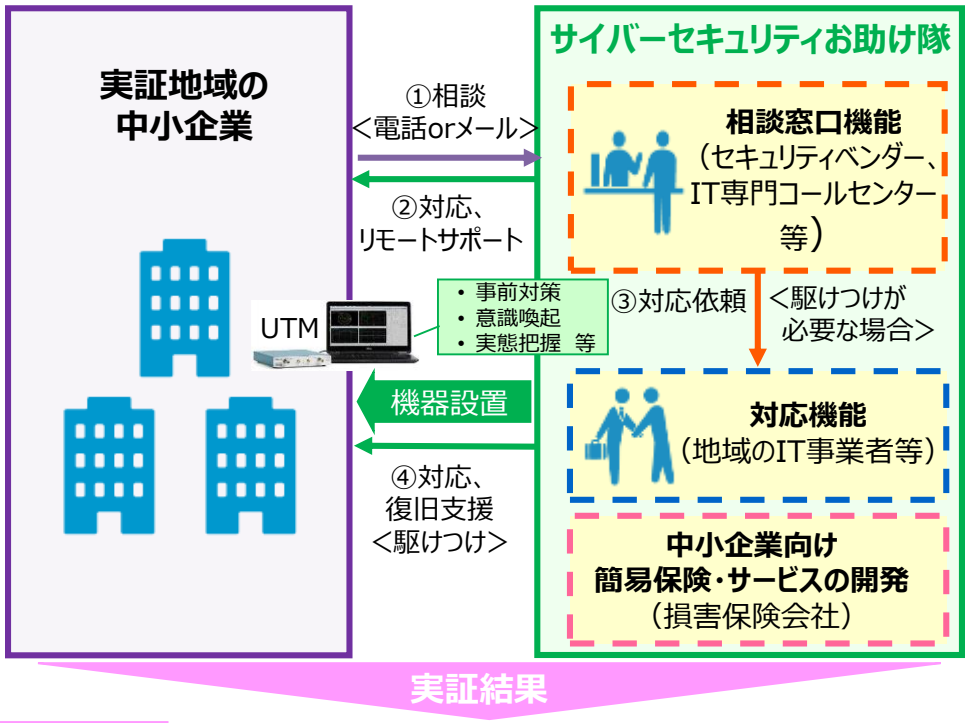
サイバーセキュリティお助け隊実証事業

- 全国**8地域**において、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。
- 本事業により、中小企業の事前対策の促進や意識喚起、攻撃実態や対策ニーズの把握を行い、**民間による中小企業向けのセキュリティ簡易保険サービスの実現を目指す。**

＜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

（参考）サイバーセキュリティお助け隊コンソーシアムリスト

地域名	実施主体	実施体制
宮城、岩手、福島	株式会社デジタルハーツ	**損害保険ジャパン日本興亜株式会社** 株式会社アライブ 地元関係団体多数
新潟	東日本電信電話株式会社	**東京海上日動火災保険株式会社** 東京海上日動リスクコンサルティング株式会社
長野、群馬、栃木、茨城、埼玉	富士ゼロックス株式会社	**東京海上日動火災保険株式会社**
神奈川	SOMPOリスクマネジメント株式会社	**損害保険ジャパン日本興亜株式会社** 日本PCサービス株式会社 株式会社コムネットシステム 株式会社サイバーセキュリティクラウド 株式会社ラック 学校法人岩崎学園
石川、福井、富山	株式会社PFU	アイパブリッシング株式会社 **損害保険ジャパン日本興亜株式会社**　金沢支店 北陸先端技術大学院大学 PFU西日本株式会社
愛知	MS&ADインターリスク総研株式会社	**三井住友海上火災保険株式会社** **あいおいニッセイ同和損害保険株式会社** NTTアドバンステクノロジ株式会社 綜合警備保障株式会社 デロイトトーマツサイバー合同会社
大阪、京都、兵庫	大阪商工会議所	**東京海上日動火災保険株式会社** 日本電気株式会社 キューアンドエー株式会社
広島、山口	株式会社日立製作所	**損害保険ジャパン日本興亜株式会社** SOMPOリスクマネジメント株式会社 株式会社日立システムズ 広島県情報産業協会

サイバーセキュリティお助け隊　今年度実証事業の状況①

- 多くの中小企業に参加いただき、駆けつけ事例も発生している状況。

受託事業者	地域	参加 中小企業数
株式会社デジタルハーツ	宮城県、岩手県、福島県	111
東日本電信電話株式会社	新潟県	148
富士ゼロックス株式会社	長野県、群馬県、栃木県、茨城県、埼玉県	112
SOMPOリスクマネジメント株式会社	神奈川県	150
株式会社PFU	石川県、富山県、福井県	120
MS&ADインターリスク総研株式会社	愛知県	201
大阪商工会議所	大阪府、京都府、兵庫県	112
株式会社日立製作所	広島県、山口県	110

計**1,064**社
の
中小企業が
参加

(2020年1月10日時点)

お助け隊で観測されたサイバー攻撃の実例

お助け隊設置のUTMが不審な通信を観測。ボットネットへの通信が疑われた。
原因は、従業員がマルウェア感染が疑われる**私物のスマートフォン**を社内の無線アクセスポイントに接続したこと。
お助け隊が**駆けつけ対応を実施し、対処した**。

お助け隊による対処が行われず放置した場合・・・

スマートフォンに感染しているマルウェアがWi-Fiを経由して社内LANに侵入し、社員全員の業務用PC全25台に感染、業務停止や機密情報が漏洩する事態が考えられた。
この場合の保険会社算出の被害想定額※は、

約4,925万円

※初動対応、調査対応、復旧費用、事業停止による損失等。

出典：MS&ADインターリスク総研株式会社　2019年10月16日「サイバーセキュリティお助け隊実証事業（愛知県）」中間報告会資料

サイバーセキュリティお助け隊　今年度実証事業の状況②

- 全国８地域合計でインシデントが48件既に発生しており、そのうち駆けつけ対応が17件発生している状況である。（12/6時点）

<コールセンター稼働及び駆け付け支援状況>

対応種別	総数	アラート種別	発生件数
コールセンター対応	545件	実証参加に関する問い合わせ	125件
		セキュリティ機器設置等の問い合わせ	294件
		セキュリティ対応の相談	70件
		その他	56件
インシデント等対応	74件	**電話およびリモートによるインシデント対応**	**31件**
		訪問によるインシデント対応	**17件**
		機器設置等のトラブル対応	22件
		その他	4件

令和２年度事業概要

- 今年度事業で明らかになった中小企業の実態やニーズを踏まえつつ、次年度も「サイバーセキュリティお助け隊」の実証事業を各地で実施予定。

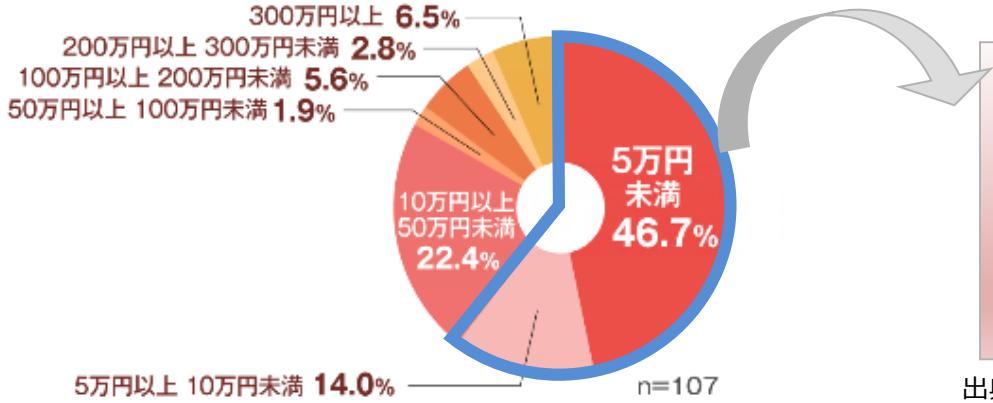
今年度事業で明らかになった課題等	次年度事業の方針
マーケティングには地域特性、産業特性等の考慮が必要	**地域特性や産業特性等を一定程度考慮した単位**での実証
無償の実証事業でも参加の必要性を感じない中小企業が多い	今年度事業で明らかになった各地域の攻撃実態等のデータ等を用い、参加募集説明会等を通じて**各地で普及啓発を実施**
実証事業に参加したくても、人手不足により、機器設置等に対応できない	セキュリティサービスの**導入・運用負荷を下げる**方法を検討
同規模サービスを有償提供する場合、年間10万円以下での提供は厳しい	**サービス内容のスリム化、事前サービス等とのセットによるリスク低減**方法を検討

（参考）中小企業の実態調査結果

- 中小企業の中でも比較的サイバーセキュリティ意識の高いSECURITYACTION宣言企業やお助け隊参加企業でも、セキュリティ対策にかける費用について非常にシビアであるのが実態。

<SECURITYACTION宣言企業へのアンケート調査>

Q13 情報セキュリティ対策費はどれくらいかかりましたか?
(ひとつだけお選びください)※貴社・貴団体の職員の人件費は含まず、セキュリティ対策ソフト等の導入や社外の専門家に支払った費用等



サイバーセキュリティの意識が高い中小企業でも年間10万円もかけられない。

- セキュリティアクション宣言企業の60.7%が、「セキュリティ対策に掛けた費用は10万円未満」と回答。

出典：2018年3月2日東洋経済新報社 SECURITY ACTION実態調査結果

<お助け隊説明会@大阪で実施したアンケート結果（n=69社）>

Q.サイバーセキュリティ対策に年間どれくらい経費をかけていますか？
（正社員情シス担当者の人件費除く）

5万円以内	31
6～10万円	10
11～15万円	7
16～20万円	2
21～50万円	5
51～100万円	2
101万円～	4

Q.お助け隊サービス（有償サービスとなった場合）に
年間いくらなら出せますか？※アンケート結果を月額から年額へ換算

1.2万円未満	3
2.4万円未満	7
3.6万円未満	11
4.8万円未満	5
6.0万円未満	24
7.2万円未満	4
8.4万円未満	0
8.4万円以上	3

（参考）中小企業向けサービスの開発状況

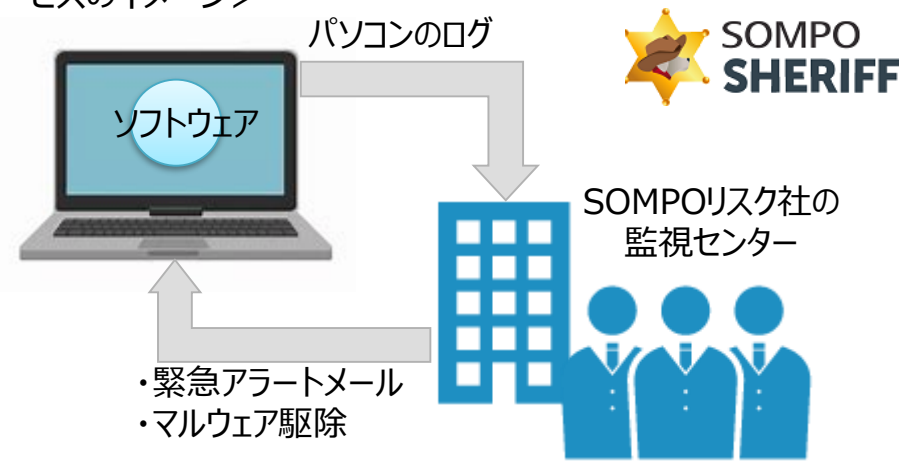
- お助け隊受託事業者の中から中小企業向けのサービスが開発され始めている。

例）SOMPOリスクマネジメント社の新サービス「SOMPO SHERIFF」

同社が神奈川県での実証事業で感じた中小企業の課題

通信機器を設置する作業において、中小企業では自社の社内ネットワークの状況が分かる人がいないことが多く、設置作業が難航。

<サービスのイメージ>



- 新サービス「SOMPO SHERIFF」では、顧客企業が保護したいパソコンに専用ソフトウエアをインストールするだけで利用できるようにした。
- パソコンのログを収集し、監視センターに送る仕組みのため、ソフトの動作設定など顧客側の負担になる作業はほぼ発生しない。

<サービスの特徴>

運用
監視センターから遠隔でマルウェアを検出、早期駆除

導入
ソフトウェアをインストールするだけ

コスト
初期費用35,000円、月額1台あたり1,800円(税抜)

保険
サイバー保険を自動付帯

出典：SOMPOリスクマネジメント株式会社の2019年11月21日ニュースリリースを基に経済産業省で作成

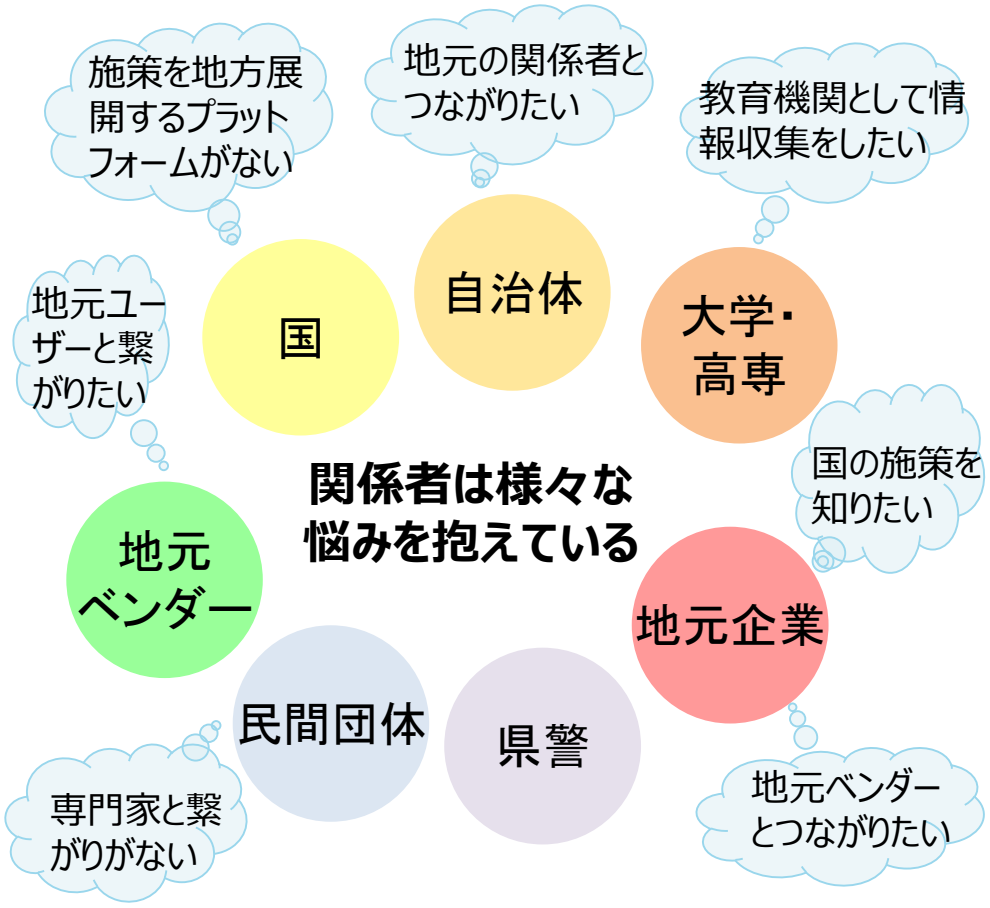
（１）サイバーセキュリティお助け隊

（２）地方版コラボレーション・プラットフォーム

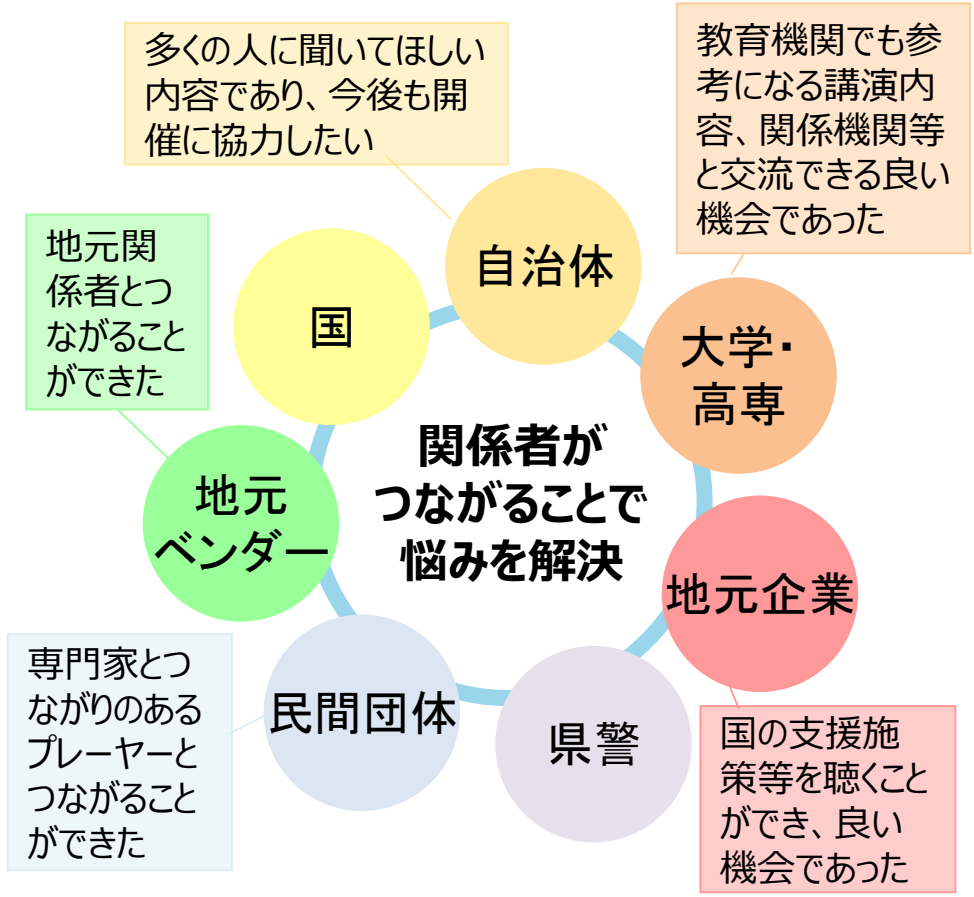
地方版コラボレーション・プラットフォームのコンセプト

- 各地域において、地方自治体、教育機関、地元企業、地元ベンダー、地元関係団体等による**セキュリティコミュニティの形成を促すことを目的に開催。**

【サイバーセキュリティセミナー in 岩手の例】



＜イベント開催後の声＞



（参考）各地域でのコミュニティ形成に向けた取組状況

- コミュニティ形成に向けた取組を実施している地域が増えてきているが、更に取組を広める必要がある。

＜各地域の主な取組状況＞

サイバーセキュリティセミナー in 秋田
（東北経産局、IPA、秋田県、
秋田デジタルイノベーション推進コンソーシアム）

令和元年12月に、秋田県が中心となり、地方版コラボレーション・プラットフォームの第2弾として開催

サイバーセキュリティセミナー in 宮城
（東北経産局、IPA、MISEC※1、TiSA※2）

令和元年12月に、地方版コラボレーション・プラットフォーム第3弾として開催し、セミナーと合わせ個別相談会を実施

北海道地域情報セキュリティ連絡会（HAISL）
（北海道経産局、北海道総通局、北海道警察）

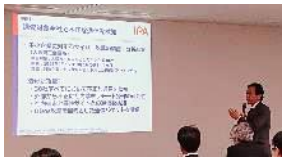
平成26年9月に発足し、年３回程度セミナー開催（計14回）

一般向けセミナー(令和元年9月)

会員向け勉強会の様子

サイバーセキュリティセミナー in 岩手
（東北経産局、IPA、岩手県、滝沢市、
いわて組込技術研究会）

令和元年10月に、地方版コラボレーション・プラットフォームの第1弾として開催



2/18 東京

3/18 大分

サイバーセキュリティセミナー広島・岡山
（中国経産局、中国総通局、広島県警、岡山県警）

平成31年2月に広島で、3月に岡山で初開催し、令和元年度も2月5日に岡山、6日に広島で開催予定

平成31年2月広島開催の様子

関西サイバーセキュリティ・ネットワーク
（近畿経産局、近畿総通局、KIIS※3）

平成30年10月に発足し、人材育成、機運醸成等に取り組む

サイバーセキュリティソリューション地域別講座(令和元年7月京都、大阪、神戸にて開催)

関西を代表する研究者8名によるリレー講義（令和元年8～9月 計8回）

※1 MISEC･･･特定非営利活動法人みちのく情報セキュリティ推進機構
※2 TiSA･･･東北地域情報サービス産業懇談会　※3 KIIS･･･一般財団法人関西情報センター

地方版コラボレーション・プラットフォームの開催形態

- セキュリティコミュニティの中心になり得る団体は、**地域によって様々なパターン**（都道府県警、地方経産局／総通局、自治体、民間団体、高専等）が考えられる。
- 地域特性、中心的団体、物理的距離等も考慮しつつ、関係省庁等とも連携し、**地域・都道府県単位でのセキュリティコミュニティの形成を目指したい**。

＜想定される中心的な団体＞

➢ 地域の特性や既存の取組によって、セキュリティコミュニティの中心になる組織としては例えば下記が考えられる。

自治体

県警

地方経産局

大学・高専

地元民間団体

商工会議所

＜コミュニティの継続性に必要な条件＞

① **中心的団体の活動エリア単位での実施**
⇒ 中心的団体の活動エリアは地域単位・都道府県単位が多い

② **物理的距離の近さ**
⇒ 地域単位での集客が難しい地域もある
（例：青森-仙台間　車で約4時間半）

③ **地域特性に応じた内容**
⇒ 実施単位が小さい方が、地域特性を考慮しやすい

地域・都道府県単位での
セキュリティコミュニティ形成を目指す

必要と考えられる取組

- 全国各地で地域に根差したセキュリティコミュニティの形成を推進するために、以下の取組を開始する。

<コミュニティ形成に必要な取組>

①セキュリティコミュニティを形成するためのモデル及びプラクティスの共有

- 新たにコミュニティを形成する際にアプローチ先として想定される関係機関（自治体、商工団体、県警、大学 等）をリスト化。
- 他地域でのコミュニティの取組を参考にできるよう、各コミュニティのプラクティスを共通のフォーマットでとりまとめ、横展開。
- 課題なども共有することで、ソリューションを有するプレイヤーとの更なる連携を促進。

<イメージ>

②各地域に駆けつけ可能な専門家や、専門家派遣制度等の情報・問合せ先リストの作成・共有

- 連携できる可能性のある専門家やイベント（例．JNSA全国横断セミナー）、活用可能な制度（例．IPAセキュリティプレゼンター制度）等の情報・問合せ先リストを作成・共有。

<イメージ>

活用可能な制度

組織名	担当部署	連絡先
IPA セキュリティプレゼンター	××課	XX-XXXX
IPA 講師派遣制度	○○課	XX-XXXX

セキュリティ専門家

組織名	氏名	連絡先	専門等
JUAS	○○	XX-XXXX	経営層向け
JPCERT	△△	XX-XXXX	最新攻撃事例

1．経営

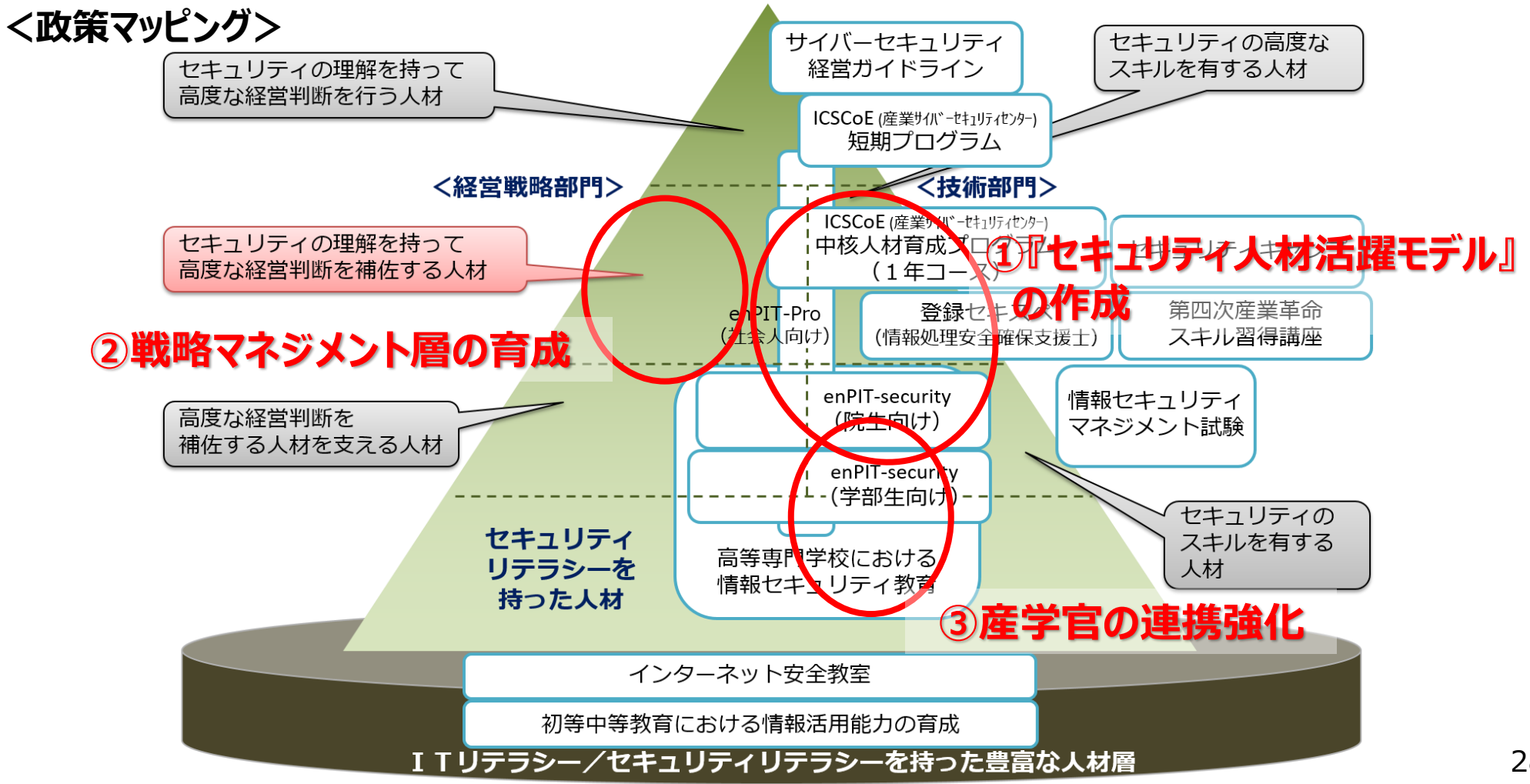
2．中小･地域

3．人材

4．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

- **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。**



（１）『セキュリティ人材活躍モデル』の構築

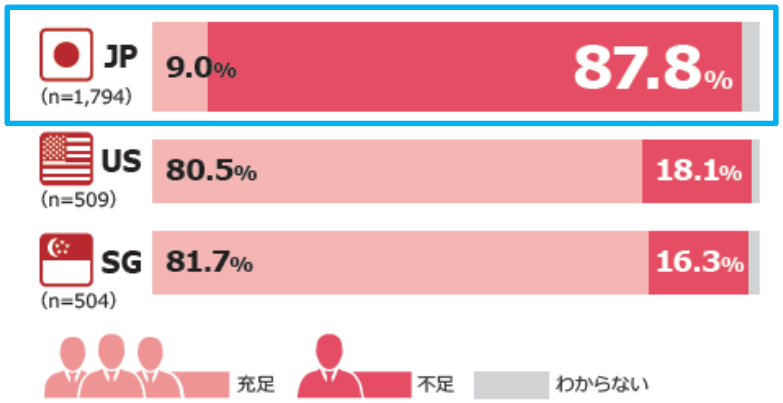
（２）戦略マネジメント層の育成

（３）産学官の連携強化

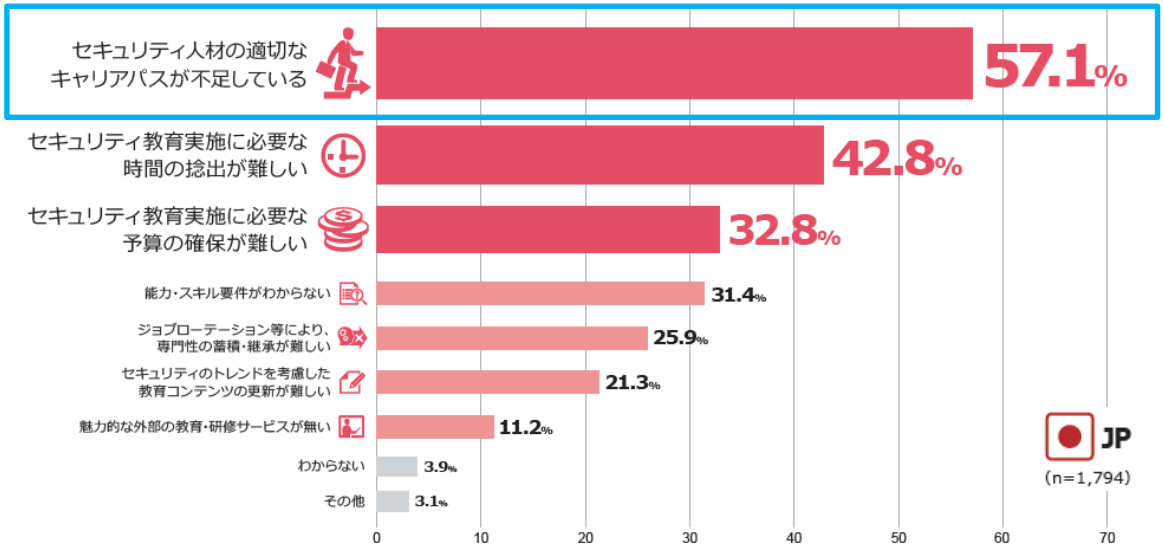
我が国企業におけるセキュリティ人材の不足感と育成に係る課題

- 米・星に比べ、日本ではセキュリティ人材の不足感が非常に高い。
- セキュリティ人材の教育・育成に当たっては、キャリアパス不足が第一課題として挙げられている。
- 約５割の企業では、業務に必要な能力・スキルを整理せずにセキュリティ教育を実施している。

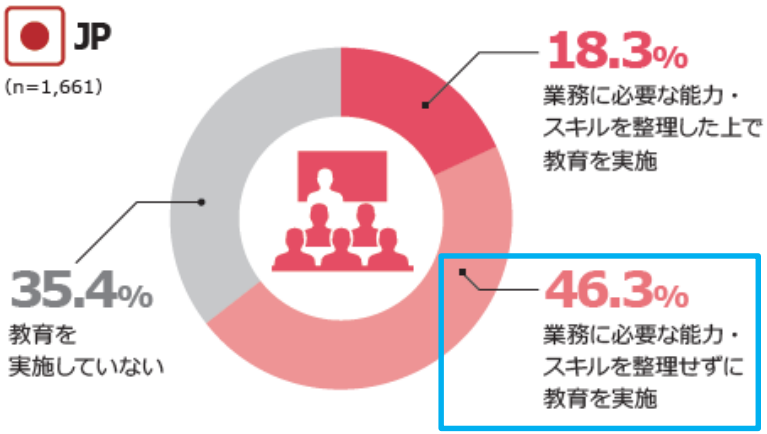
セキュリティ対策に従事する人材の充足状況



セキュリティ人材の育成・教育における課題



セキュリティ人材の育成・教育の実施状況



（出典）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2019
調査対象：日本、アメリカ、シンガポール企業の情報システム/情報セキュリティ担当者
回答企業：計2,807社（日本：1,794社、アメリカ：509社、シンガポール：504社）

セキュリティ人材の全体像の可視化や育成・活躍促進のためのモデルの構築

- ITSS＋(セキュリティ領域）改定により、各分野に紐づくセキュリティ関連タスク等を整理中。
- その後、各分野に関するキャリアパス事例集や、ユーザ企業における体制・人材確保のプラクティス集等を開発。

ユーザー企業　／　**IT・セキュリティベンダー**　／　**人材**

セキュリティ関連タスク

セキュリティ部門のみではなく、デジタル部門や管理部門にもタスクが存在

- ・セキュリティポリシー策定
- ・関連法令等順守対応
- ・システム／セキュリティ監査
- ・セキュアなシステムの調達
- ・インシデント対応　等

タスクを担う分野の整理

タスクに対応するセキュリティ関連分野

様々な団体から様々な定義が公開されているが、目的や用途の違いもあり共通言語化はされていない

ユーザ企業での対応が多い分野

- ・セキュリティ統括
- ・ITストラテジー
- ・ITサービスマネジメント
- ・セキュリティ監視・運用　等

発注 / 提供

ベンダーでの対応が多い分野

- ・システムアーキテクチャ
- ・システム／セキュリティ監査
- ・脆弱性対策・診断・テスト
- ・セキュリティ研究・開発・分析　等

分野とスキルの紐づけ

知識・技能（スキル）

- ・ITSS+(IPA)
- ・SecBoK(JNSA)
- ・統合セキュリティ人材モデル(CRIC)
- ・NICEフレームワーク(NIST)　等

スキルと資格等の紐づけ

資格・試験

- ・登録セキスペ
- ・民間資格　等

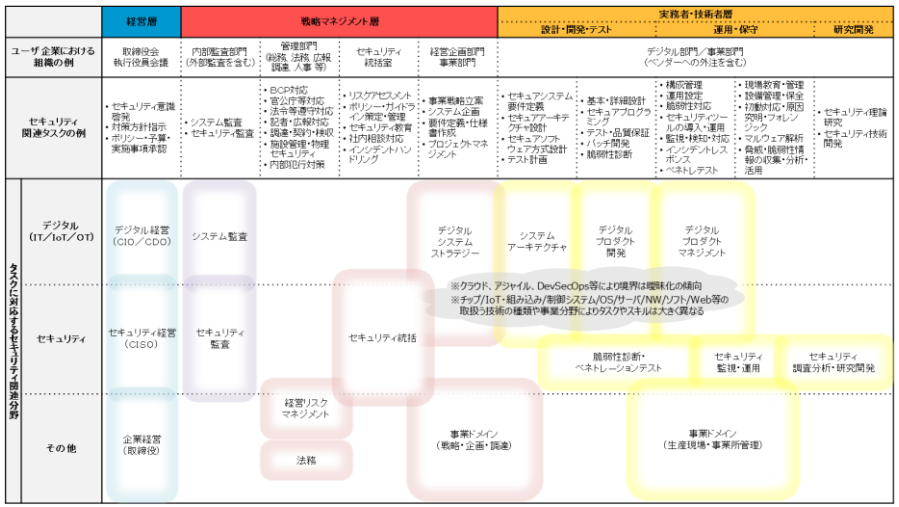
研修・訓練

- ・IPA ICSCoE
- ・民間研修・訓練　等

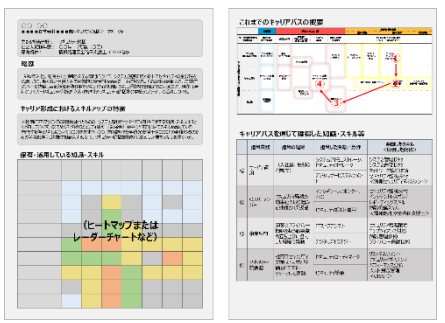
教育

- ・Enpit Security
- ・高専教育　等

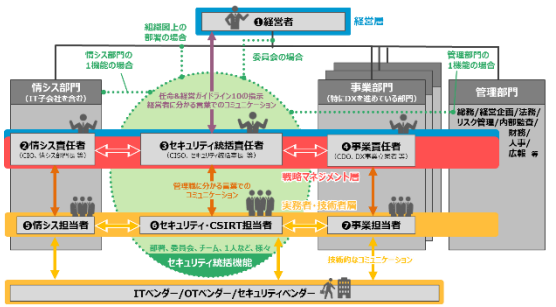
ITSS＋(セキュリティ領域）の改定により、セキュリティ関連分野と各分野に対応するタスク・スキルを整理中



その後、キャリアパス事例集やユーザー企業の体制・人材確保のプラクティス集の開発、セキュリティ成熟度と体制・人材との関係整理等により、企業における人材の育成・確保を促す



キャリアパス事例集



ユーザ企業のプラクティス集・セキュリティ成熟度との関係整理

改訂中のITSS＋（セキュリティ領域）におけるセキュリティ関連分野の概観（現状版）

- セキュリティ技術者のみではセキュリティは確保できない。IT/IoT/OT等のシステムの企画・設計・開発・運用・保守を行う人材や、管理部門等の人材にも、セキュリティ関連スキルは必須となってきている。
- こうした観点から、セキュリティ関連分野を以下の通り整理し、各分野に関連する主なタスク等を紐づけ中。

	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 • 法令等遵守対応 • 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 • インシデントハンドリング	• 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	• 基本・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 • 脆弱性診断	• 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 • ペネトレテスト	• 現場教育・管理 • 設備管理・保全 • 初動対応・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
タスクに対応するセキュリティ関連分野 デジタル（IT／IoT／OT）	デジタル経営 （CIO／CDO）	システム監査			デジタル システム ストラテジー	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 マネジメント		
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				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
その他	企業経営 （取締役）		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）			事業ドメイン （生産現場・事業所管理）		

※クラウド、アジャイル、DevSecOps等により境界は曖昧化の傾向
※チップ/IoT・組み込み/制御システム/OS/サーバ/NW/ソフト/Web等の取扱う技術の種類や事業分野によりタスクやスキルは大きく異なる

情報処理安全確保支援士（登録セキスペ）制度の見直し概要

- 「情報処理の促進に関する法律の一部を改正する法律」が第200回臨時国会で成立し、12月６日に公布。施行日は、公布の日から６ヶ月を超えない範囲内において政令で定める日。
- 改正法により、デジタル技術の急速な発展に伴うサイバーセキュリティ上のリスクに対応するため、登録セキスペの信頼性の向上等を目的とした制度の見直しを実施。
- これにより、**①登録の更新制導入、②一定の条件を満たした民間事業者等が行う講習を義務講習の対象とすることが可能**。

更新制の導入

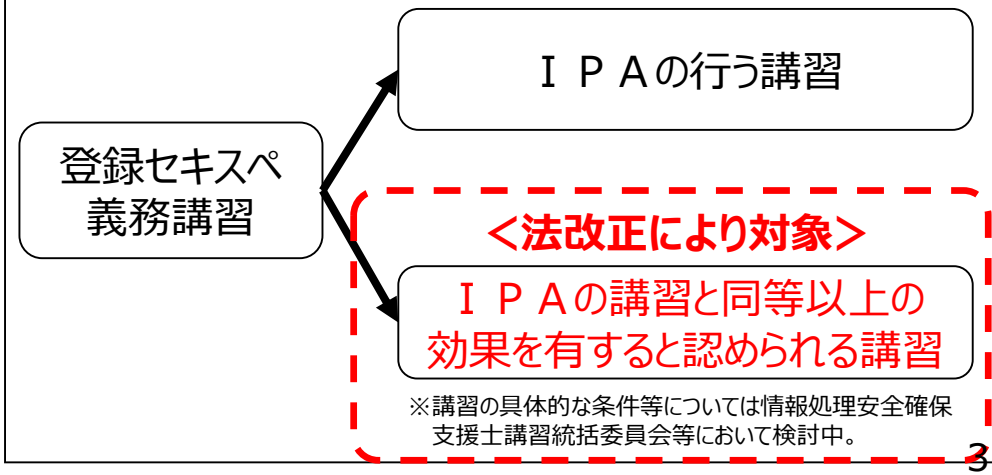
登録に**３年間の有効期限**を設け、義務講習を受講した者のみ更新を認め、**更新が行われない場合**には、**登録が失効**する制度を導入。

登録日	最初の更新日
2017年　4月1日	法律施行の日から６ヶ月を超えない範囲内で政令で定める日
2017年10月1日	2020年10月1日
2018年　4月1日	2021年　4月1日
2018年10月1日	2021年10月1日
2019年　4月1日	2022年　4月1日
2019年10月1日	2022年10月1日

※更新には申請手続きが必要。詳細は検討中

民間事業者等の講習追加

これまで、義務講習として認められる講習は、独立行政法人情報処理推進機構　（ＩＰＡ）が行うものに限られたが、**一定の条件を満たした民間事業者等が行う講習も対象**とすることが可能。



（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）産学官の連携強化

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。
- このため、IPA産業サイバーセキュリティセンターでは、昨年度に引き続き、今年度も戦略マネジメント層向けのセミナーを実施予定。
- また、東京工業大学CUMOTが開催する「サイバーセキュリティ経営戦略コース」についても支援予定。

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」

- 令和２年２月～３月（予定）
- 今年度は、「戦略マネジメント層のためのセキュリティ組織管理」と「戦略マネジメント層のためのセキュリティ運用管理」の２コースを用意（それぞれ２回、合計４回）。

（写真は昨年度の様子）

東京工業大学ＣＵＭＯＴ「サイバーセキュリティ経営戦略コース」

- 令和２年１月～４月（予定）
- 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回を予定。

（写真はCUMOTの別の講座の様子）

（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）産学官の連携強化

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。
- このため、国立高専機構がIPAや業界団体（CRIC CSF、JNSA）との協力内容を具体化していくための議論を継続的に実施。

＜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

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
	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。
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。  ゲーム形式教材のイメージ	• **JNSAが講師の派遣を検討中。** • **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。**  開催の様子@石川高専
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 • **四国地域企業のIPA ICSCoE終了生が講義を検討中。** • **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が佐世保高専と連携し、業界別（例．機械、電気、建築等）ビデオ教材（20分程度）を作成中。** ※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。  AppGoat講習の様子
KOSEN 国立高等専門学校機構 国立高専教員	※授業実施側のため。	• **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。** • **教師向け合宿で、METIがセキュリティ専門官の派遣を検討中。**

セキュリティスキルレベル

１．経営

２．中小･地域

３．人材

４．国際

インド太平洋地域向け日米サイバー演習

- 経済産業省及びIPA産業サイバーセキュリティセンター（ICSCoE）が、日米の専門家による制御システムのサイバーセキュリティに関する演習をインド太平洋地域（14の国・地域）向けに実施。

■**日時・場所：**2019年9月9日（月）～12日（木）@東京（今回で２回目。以後毎年開催。）

■**参加者：**ASEAN９カ国、スリランカ、バングラデシュ、インド、NZ、台湾　35名

ICSCoE中核人材育成プログラム研修生　69名

■**来賓挨拶／講師：**

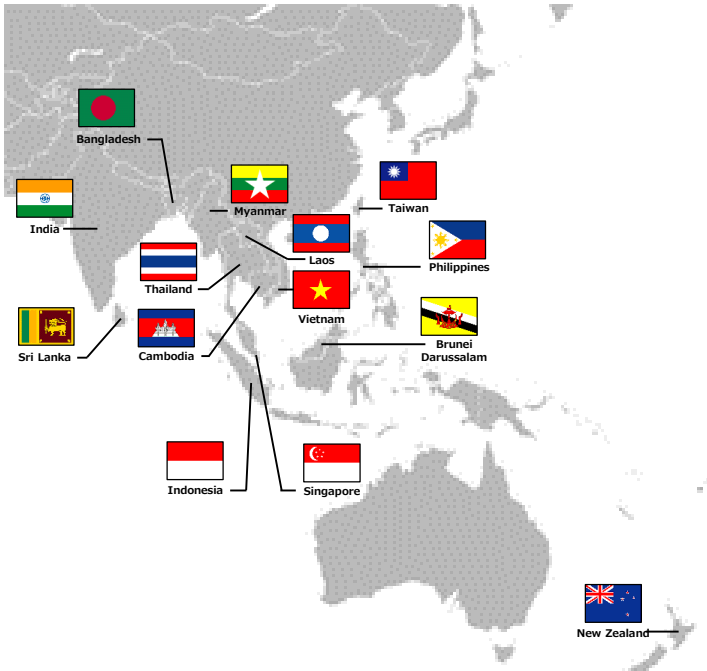
（米国）在日米国大使館首席公使代理、国務省東アジア・太平洋局首席次官補代理、エネルギー省、NIST、INL、ISA、米国企業

（日本）関芳弘経済産業副大臣、ICSCoE講師、日本企業

米国国務省挨拶


米国の専門家による講義


日本の専門家による講義



参加国・地域


ハンヅオントレーニング


ワークショップ


サイバー攻撃のデモ

第3回 日イスラエル電力サイバーセキュリティ官民会合（概要）

- **2019年11月25日、電力分野のセキュリティにかかる議論を更に深めることを目的とした官民WSを開催。**
- 参加者

  イスラエル側：**在京イスラエル大使館**、**イスラエル電力公社（IEC）**、**サイバージム**

  日本側：**経産省**、**電事連**、**10電力事業者**
- WS終了後、サイバージム東京支社を視察。

トピック

（先進的な取組の紹介・意見交換）

①サプライチェーンセキュリティ対策

②サイバーセキュリティ体制（SOC、インシデント　対応）

③人材育成・トレーニング

イスラエルの取組を参考に、電力分野における
サイバーセキュリティ対策の向上を図る。

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（CPSF）」**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。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。

- **EUサイバーフォーラム（2019年4月@ベルギー・ブリュッセル）**
  - 欧州対外活動庁（EEAS）主催のフォーラムのIoTパネルにおいて、METIの取組、CPSFを紹介。
- **ICS-JWG2019（2019年4月@米・カンザスシティ）**
  - 米国土安全保障省（DHS）主催のフォーラムにおいて、当省の取組、 CPSFを紹介。
- **Consumers International Summit 2019 （2019年4月@ポルトガル・エストリル）**
  - 国際消費者保護団体主催のフォーラムのIoTパネルにおいて、 CPSFとIoTセキュリティTFを紹介。
- **プラハ５Gセキュリティ会議（2019年５月@チェコ・プラハ）**
  - チェコ政府主催の5Gに関する国際会議のテクノロジーWGにおいて、 CPSFを紹介。
- **第4回日EUサイバー対話（2019年6月@ベルギー・ブリュッセル）**
  - 日EU政府間のサイバーセキュリティ協議において、CPSFと３つのTFの立ち上げを紹介。
- **EIS年次総会・CPIC会合（2019年6月@米・ワシントンDC）**
  - EIS Council主催のEIS Summit、CPIC会合において、CPSF、各SWG、TFについて紹介。
- **第5回日仏サイバー協議（2019年7月@仏・レンヌ）**
  - 日仏政府間のサイバーセキュリティ協議において、 CPSF、各SWG、TFについて紹介。
- **サイバーテック・ミッドウェスト（2019年7月@米・インディアナポリス）**
  - イスラエル発の世界的なサイバーセキュリティ・カンファレンスにおいて、CPSFを紹介。

- **APEC第3回高級実務者会合（SOM3）（2019年8月@チリ・プエルトバラス）**
  - 米商務省主催のWSにおいて、CPSF、各TF、SWGでの活動、コラプラなどの取組を紹介。
- **インド太平洋地域向け日米サイバー演習（2019年9月@日本・東京）**
  - インド太平洋地域のCERT、官民の重要インフラ関係者に対し、CPSF、SWGでの活動を紹介。
- **IEEE-APL 5G Workshop、Global Cyber Dialogue（2019年10月@米・ワシントンDC）**
  - IEEE、米商工会議所主催の会議において、CPSF、各SWG、TFでの活動、日米サイバー演習を紹介。
- **第10回インターネットエコノミーに関する日米政策協力対話（IED）（2019年10月@日本・東京）**
  - 日米官民の協議において、 CPSF、各SWG、TFでの活動、日米サイバー演習を紹介。
- **第7回日米サイバー対話（2019年10月@日本・東京）**
  - 日米政府間のサイバーセキュリティ協議において、 CPSF、各SWG、TFでの活動、日米サイバー演習を紹介。
- **APEC TEL60（2019年10月@韓国・ソウル）**
  - 韓国主催のラウンドテーブルにおいて、ガバナンスイノベーションとCPSFの取組についてプレゼンを実施。
- **ETSI IoT Workshop（2019年10月@仏・ソフィアアンティポリス）**
  - ETSI主催のカンファレンスで、 CPSF、第2層TFでの活動について紹介。
- **第12回日アセアン政策会議（2019年10月@タイ・バンコク）**
  - 日ASEAN政府サイバー当局間の会議において、 CPSF、ビルSWG、 TFでの活動について紹介。
- **第2回OECD Global Forum on Digital Security for Prosperity（2019年11月@英・ロンドン）**
  - デジタルセキュリティ・イノベーションに係るパネルにおいて、CPSF、WG３の活動を紹介。
- **PJM会合（2019年12月@米・フィラデルフィア）**
  - 米国をはじめとする電力分野のセキュリティに関する国際会合において、CPSF、各SWG、TFでの活動を紹介。