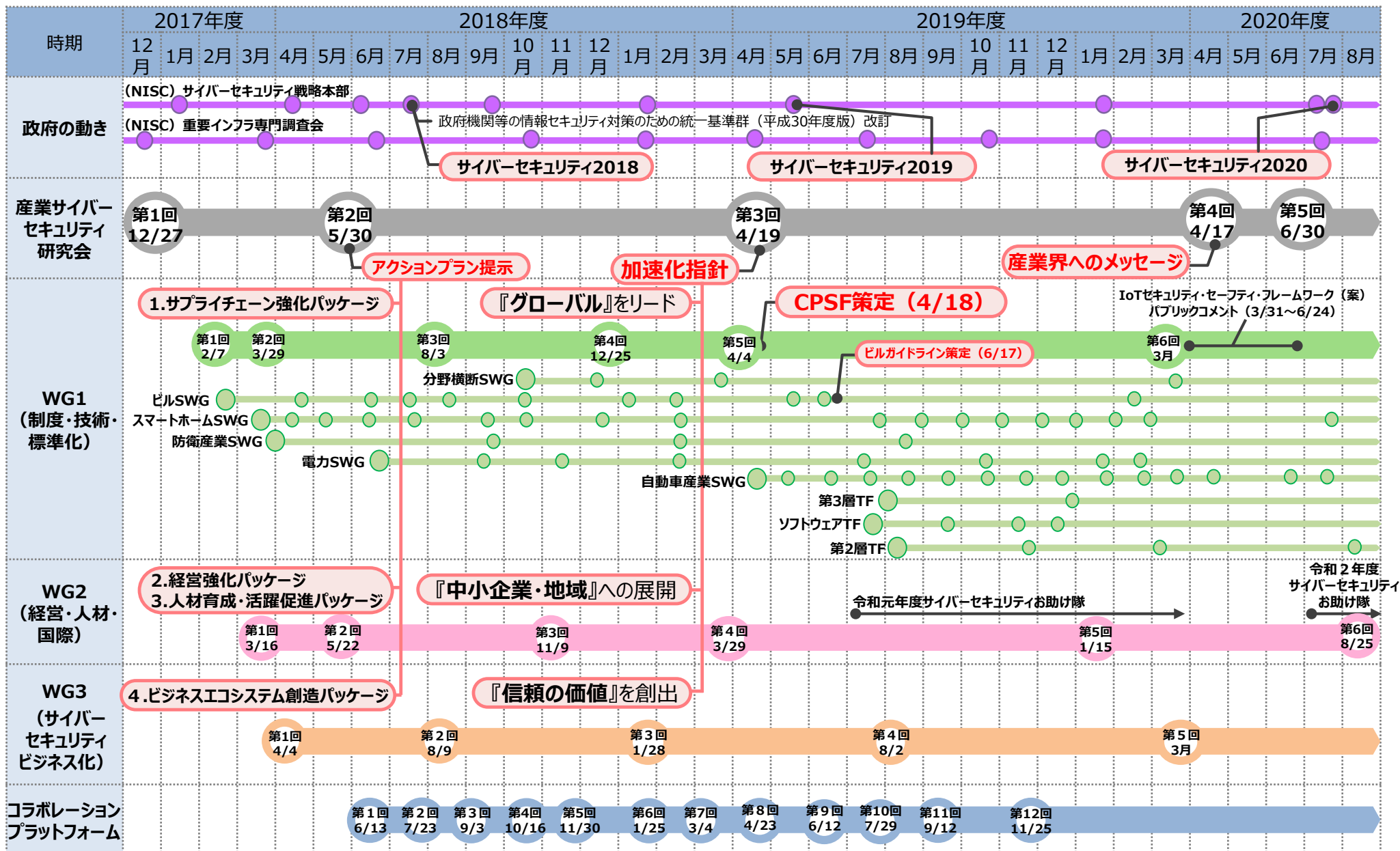


事務局説明資料

経済産業省
商務情報政策局
サイバーセキュリティ課

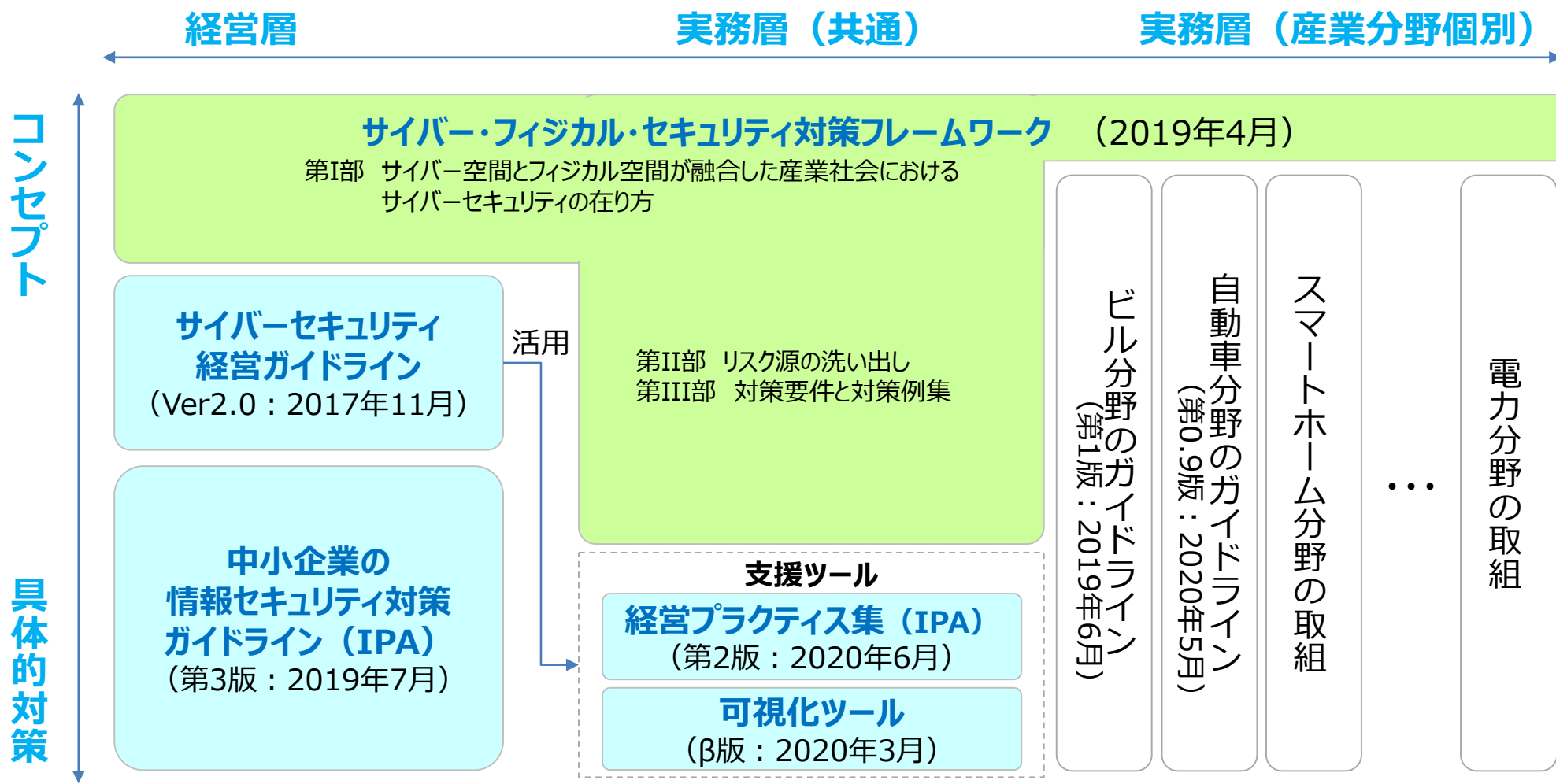
産業サイバーセキュリティ研究会関連会議の活動状況



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

**サプライチェーン・サイバーセキュリティ・
コンソーシアムの設立**

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

サイバーセキュリティ経営ガイドライン

平成27年12月28日策定
平成28年12月8日改訂 (Ver.1.1)
平成29年11月16日改訂 (Ver.2.0)

1st step

- セキュリティはコストではなく投資であると位置づけ、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要であることを示したガイドライン。
- 2017年11月公開のVer2.0は、ダウンロード数が毎月平均約2800件、累計 8 万件超と注目度の高い状況が続いている。

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

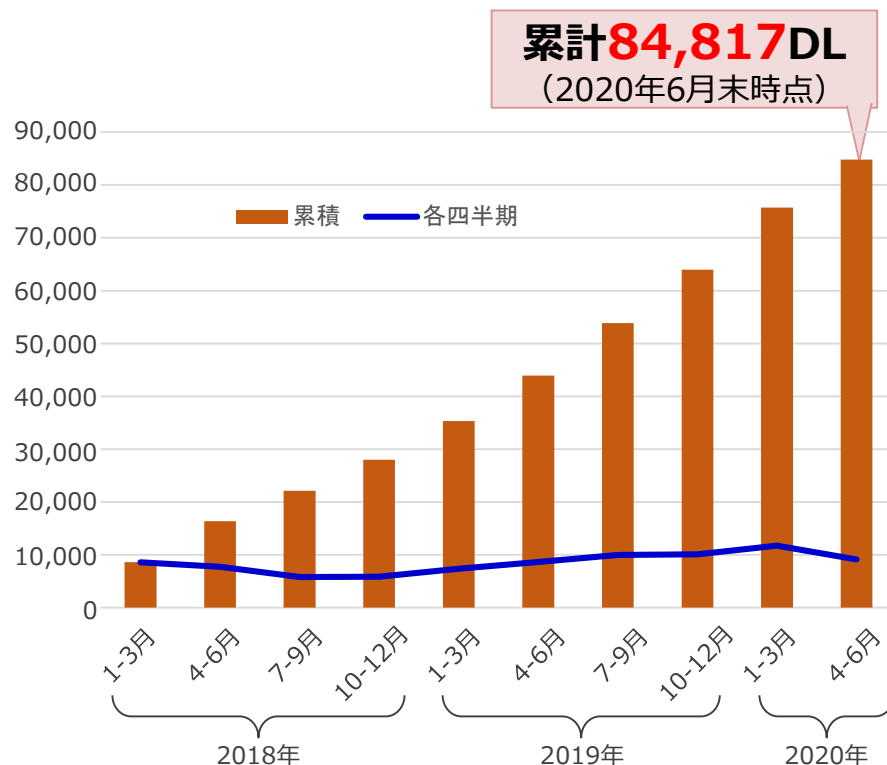
サプライチェーンセキュリティ

- 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

サイバーセキュリティ経営ガイドラインV2.0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

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

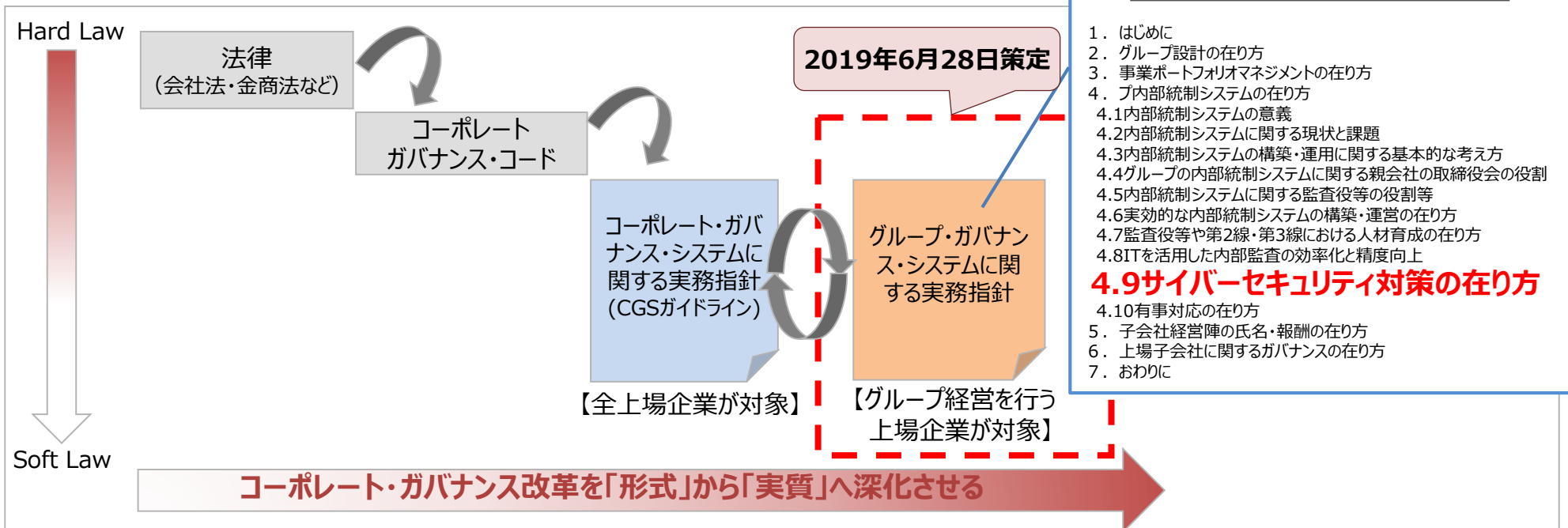
- セキュリティの高い企業であることを投資家が評価できるようにするための、サイバーセキュリティ経営に関する情報の開示の在り方の検討

(参考)

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



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

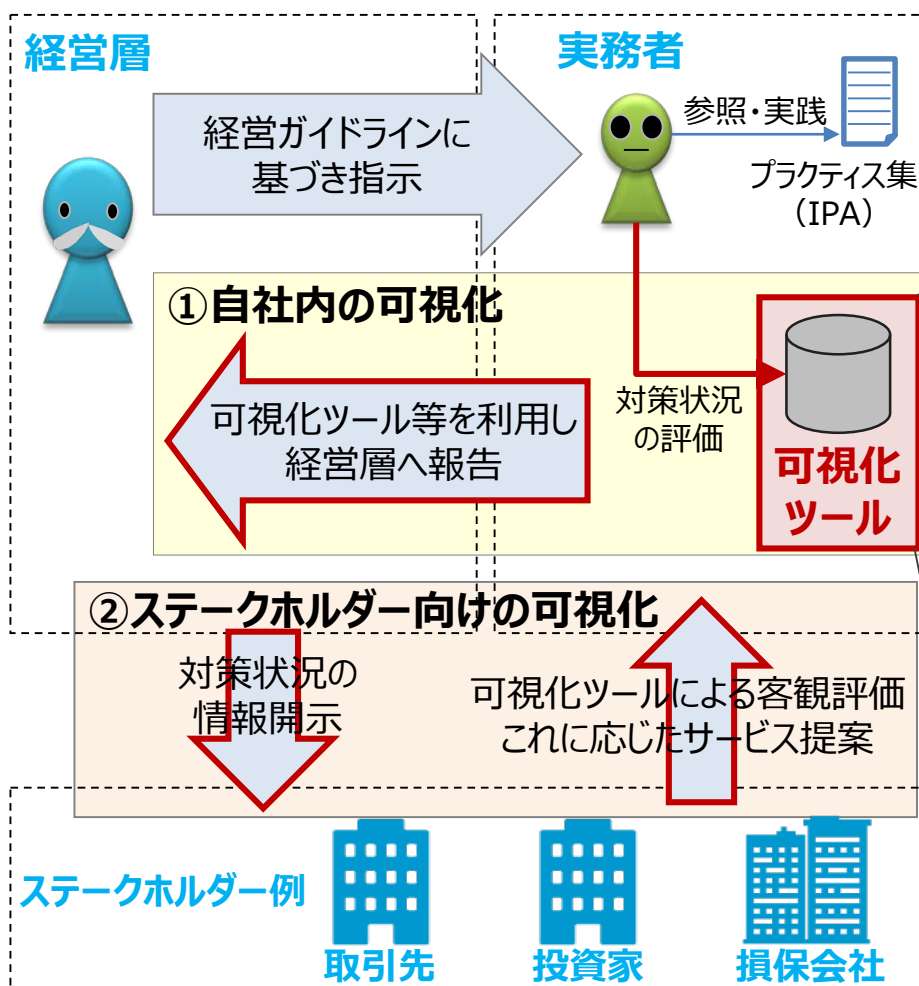
3rd Step

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

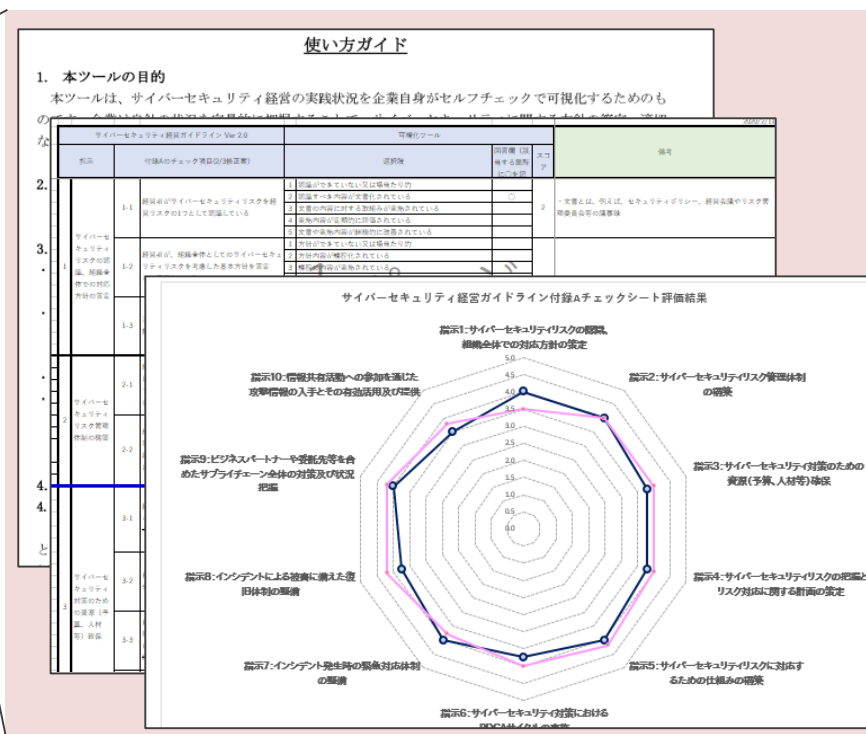
サイバーセキュリティ経営ガイドライン実践状況の可視化ツールβ版を公開

- 2020年3月25日、可視化ツールβ版（Excel）をIPAから公開。
- Ver1.0（Web版）公開に向けて、今年度はユーザ企業、投資家等のステークホルダー向けにそれぞれβ版テストを行い、ブラッシュアップを継続中。



可視化ツールβ版の特徴：

- 「使い方ガイド」「チェックリスト」「可視化結果」の3種類のシート
- 39個の質問にセルフチェックで回答
- 回答方式は5段階の選択式（成熟度モデル）
- グループ会社間等での比較も可能



今年度はβ版をベースにした調査とV1.0開発を推進

2nd ~ 3rd step

- ユーザ企業向け、ステークホルダー向けそれぞれヒアリング調査等を通じて用途と要件を明確化。今年度中にWeb化し、可視化ツールV1.0をリリースする。

2019年3月25日

可視化ツールβ版（Excel）を公開

累計**3,899**ダウンロード
(7月末時点)

2020年度

・ユーザ企業においてβ版をテスト

- 経営者⇔戦略マネジメント層⇔実務者・技術者層のコミュニケーションツールとしての利用を主たる用途と仮定し、β版の改良を進める。
- JUAS情報セキュリティWG参加企業へのヒアリングを実施中。

・投資家等ステークホルダーにおいてβ版をテスト

- 多様な立場のステークホルダーに対し、企業のサイバーセキュリティ対策に関してどのような情報を知りたいかを調査し、その用途に最適な可視化ツールを検討する。
- コンサルティングファーム、監査法人等へのヒアリングを実施中。

2020年度以降

可視化ツールV1.0リリースと本格展開

今年度スケジュール

4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
事前ヒアリング、類似ツール調査等			ユーザ企業ヒアリング			ヒアリング結果取りまとめ V1.0仕様策定			V1.0（Web版）開発		
			ステークホルダーヒアリング						V1.0リリース★		

投資家等ステークホルダー向けのβ版テストで得られた声

投資会社等計 6 社にヒアリング実施。サイバーセキュリティ対策状況の可視化・開示はステークホルダーとのコミュニケーションを促進し高い評価につながることに、そして、可視化ツールはその際の共通言語としての可能性があることが見えている。

投資会社

- 自社のサイバーセキュリティ対策状況を可視化・公表する企業とは具体的なコミュニケーションができるため、**投資家として高く評価する**。
- 可視化ツールは企業と投資家のコミュニケーションにおける**共通言語的な効果が期待**できる（質問ごとの重みづけ等、業種や企業ごとのカスタマイズも必要だが）。情報が集まり**DB化されたら、さらにコミュニケーションに役立つ**だろう。
- 自社のリスク情報は企業が積極的に開示したくないものであり、企業に開示を後押しする力も必要。
- 自己評価であっても、評価結果の透明性・客観性・継続性が担保されれば活用可能。

監査法人

- 自社のサイバーセキュリティ対策状況を開示する企業は増えているが、内容はまだ一般的なものが多く、項目も企業間でバラバラ。**共通の可視化ツールによる横並び比較ができると良い**。
- **DB化すれば、大きな方向性を示せる**。
- **業界横断の汎用の可視化ツールがあると良い**。
- 国内企業は一般にグループ管理が弱い。**共通言語として可視化ツールの活用**に期待。

損害保険会社

- サイバー保険加入時の申告書は保険会社毎で異なり統一されていない。質問数40問前後。保険業界特有の質問もあるので汎用的な可視化ツールをそのまま利用することは難しいが、ベースにすることはできると思う。
- 成熟度モデルは（Yes/No方式に比べ）レベル感を確認できるので良い。**自己評価でも参考情報としては有用**。
- マネジメント系だけでなく技術・プロセス系も網羅的に聞く。**過去のインシデントと再発防止策の状況も**。

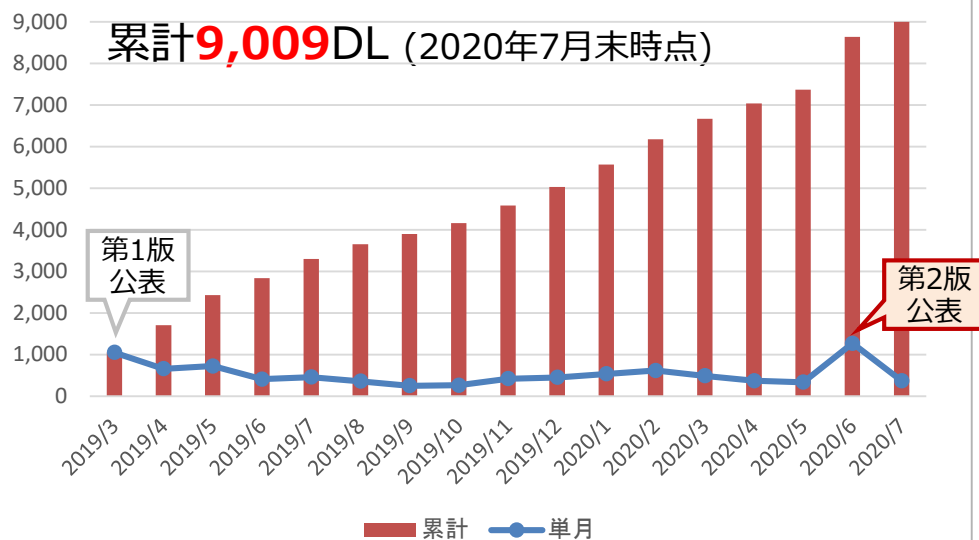
コンサルティングファーム

- **「投資家はサイバーセキュリティ対策状況も見る」というメッセージを出すことが重要**。
- 米国企業のサイバーに関する情報開示も一般的な内容が多く、投資家から不満の声が上がっている。
- M&Aのデューデリジェンスでは、サイバーセキュリティ対策状況の評価を松竹梅レベルで行う。**経営ガイドラインが共通言語として利用できるのではない**か。

『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』 第2版を公表

- 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。
- 2019年度収集したプラクティスを反映した**第2版を2020年6月3日に公表**。

＜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（日本取引所グループ公表
第二部 488社（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

＜アップデートした指示項目＞

- 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）

（参考）実際の活用事例（ユーザ企業へのヒアリングより）

- 経営陣への報告の際に、分かりやすく伝えるためにプラクティス集を参考に行っている。実践面で役立っている。

1. 経営

2. 中小・地域

3. 人材

4. 国際

サプライチェーン・サイバーセキュリティ・
コンソーシアムの設立

(1) サイバーセキュリティお助け隊

(2) 地域SECURITY

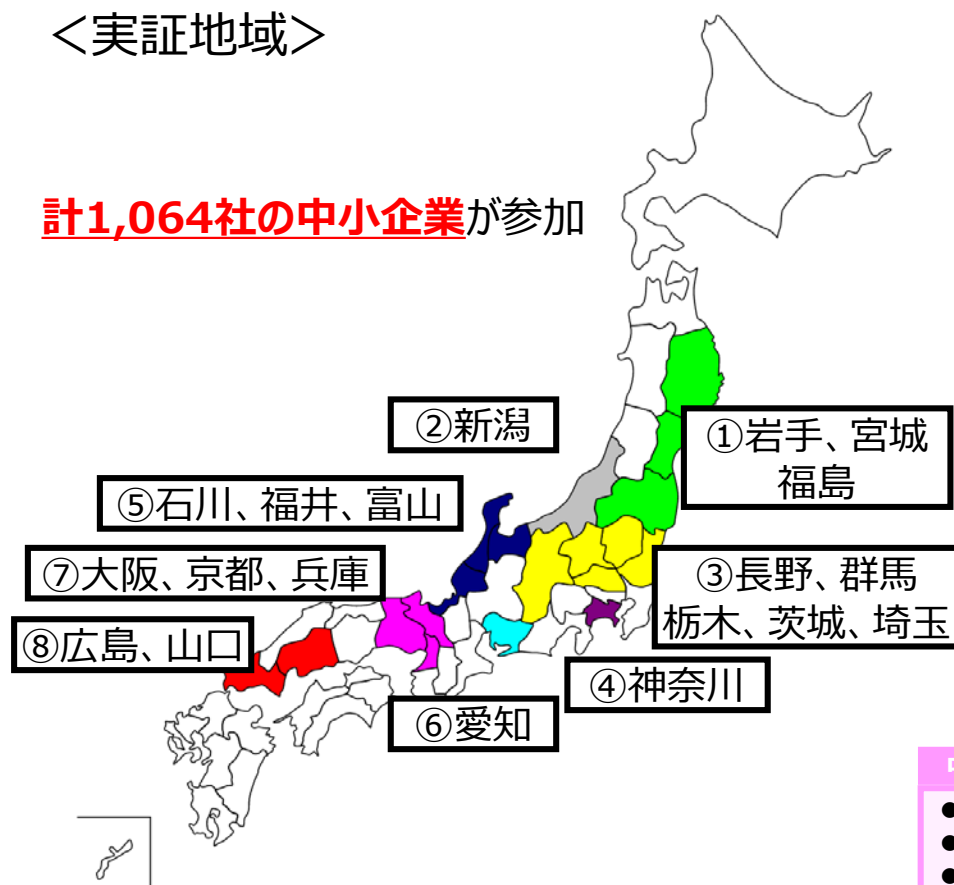
(旧称：地方版コラボレーション・プラットフォーム)

サイバーセキュリティお助け隊実証事業（2019年度の取組）

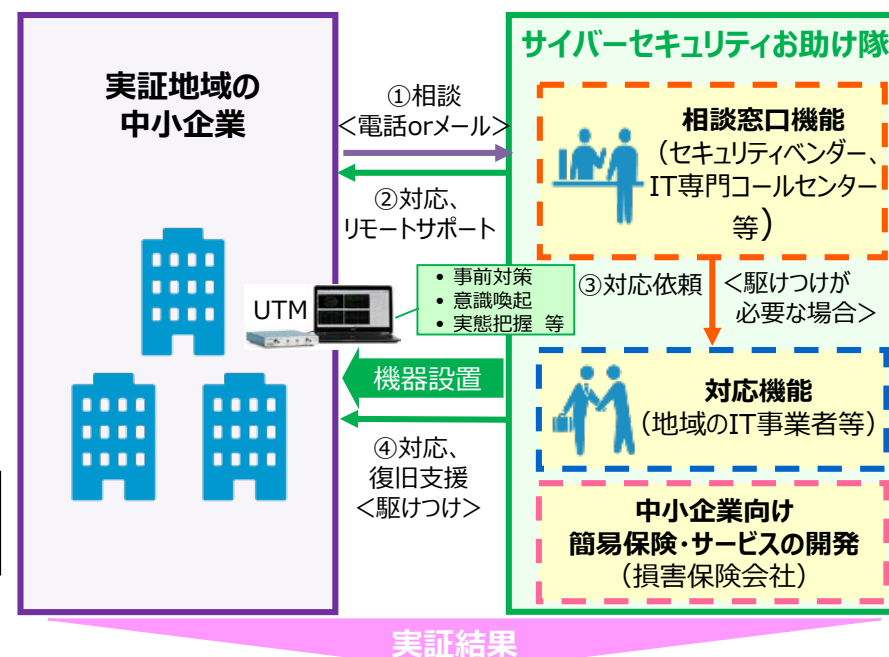
- 全国**8地域**において、中小企業のセキュリティ対策の促進や意識喚起、攻撃実態や対策ニーズの把握を行い、**民間による中小企業向けのセキュリティサービスの開発を目指し、実証事業を実施。**
- 2019年度の実施内容・成果について、IPAより報告書を公開。（2020年6月15日）

＜実証地域＞

計**1,064社**の中小企業が参加



＜実証のイメージ＞



(参考) サイバーセキュリティお助け隊チームリスト (2019年度)

対象地域	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ー株式会社 総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

2019年度サイバーセキュリティお助け隊実証事業の結果

- 1,064社が参加した実証期間中に、全国 8 地域で**計910件のアラート**が発生。重大なインシデントの可能性ありと判断し、**対処を行った件数は128件**。対処を怠った場合の**被害想定額が5000万円**近くなる事案も。
- 実証参加前後の中小企業の意識変化や、お助け隊サービスに求められる機能等が明らかになった。

<駆け付け支援の対象となった特徴的な対応事例>

古いOSの使用

- ・Windows XPでしか動作しないソフトウェア利用のために、**マルウェア対策ソフト未導入のWindows XP端末を使用**。
- ・社内プリンタ使用のために、社内LANに接続したことで、意図せずにインターネット接続状態になり、マルウェアに感染。
- ・検知・駆除できていなかった場合の**想定被害額は5,500万円**。

私物端末の利用

- ・社員の**私物iPhoneが会社のWi-Fiに無断で接続**されていたことが判明。
- ・私物iPhoneは、過去にマルウェアやランサムウェアの配布に利用されている攻撃者のサーバーと通信していた。
- ・検知・駆除できていなかった場合の**想定被害額は4,925万円**。

ホテルWi-Fiの利用

- ・社員が**出張先ホテルのWi-Fi環境**でなりすましメールを受信し、添付されたマルウェアを実行したことで**Emotetに感染**。
- ・感染により悪性PowerShellコマンドが実行され、アドレス情報が抜き取られた後、**当該企業になりすまして、取引先等のアドレス宛に悪性メールが送信**された。

サプライチェーン攻撃

- ・実証参加企業でマルウェア添付メールを集中検知。
- ・**取引先のメールサーバーがハックされてメールアドレスが漏えい**し、それらのアドレスからマルウェア添付メールが送付されていた。
- ・メールは賞与支払い、請求書支払い等を装うなりすましメールであり、**サプライチェーンを通じた標的型攻撃**であった。

<https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html>

<実証参加の成果（参加中小企業のアンケート結果より）>

- ・アラート通知が実際にあり、**他人事ではないとの意識につながった**。（大阪府・建設業）
- ・UTM導入時、当社に**専門知識が無いため、業者と話がかみ合わず、導入に手間取った**。（神奈川県・サービス業）
- ・参加することで、情報セキュリティ対策を実施していることを、**外向けにアピールできるのが良い**。（新潟県・電気通信工事業）
- ・総務担当がセキュリティを兼務していることもあり、**ワンパッケージでやってくれると非常に助かる**。（石川県・製造業）

実証事業から民間サービスへの移行状況と普及促進のための支援策

- 2019年度実証事業後に、民間サービスが開発されたり、実証終了後も継続的なサービス展開が図られたりと、お助け隊サービスの民間への移行が進みつつある。
- お助け隊サービスをブランド化し、審査体制を構築すること等により、民間でのサービス展開を支援していく。

実証事業から民間サービスへの移行状況

- 実証事業後の2020年4月、「サイバーセキュリティお助け隊サービス」を商用化。

(大阪商工会議所)



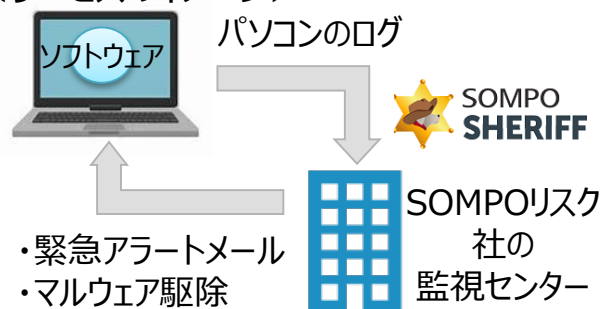
実証を通じて中小企業にとって必要な機能・サービスを精査することで、安価なサービスを実現。

【 商工会議所会員月6,600円（年79,200円）
非会員月8,250円（年99,000円） 】

- 実証事業での経験やノウハウを元に、2019年12月に新サービスを提供開始。

(SOMPOリスクマネジメント)

＜サービスのイメージ＞



- 参加中小企業148社の内、約4割の61社が有償サービスへ移行。※2020年2月17日時点

(NTT東日本)

(参考)同社の提供する「おまかせサイバーみまもり」



実証事業の取組（説明会や標的型メール攻撃の訓練、機器設置による脅威の可視化等）により、約4割の中小企業が民間サービスへの移行を希望。

お助け隊サービスのブランド化・審査体制構築へ

お助け隊サービス基準を策定し、一定の基準を満たすサービスに「サイバーセキュリティお助け隊」の商標を付与するスキームを構築することで、民間でのサービス展開を支援。

(1) サイバーセキュリティお助け隊

(2) 地域SECURITY

(旧称：地方版コラボレーション・プラットフォーム)

地域に根付いたセキュリティ・コミュニティ（地域SECURITY）の形成促進

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

<地域SECURITYのコンセプト>

地域にセキュリティについて
相談できる相手がいない

地域にセキュリティを学ぶ
機会が少ない

地域の
ベンダーを
知らない

- 地域の関係者間でのセキュリティに関する「共助」の関係を形成
- イベント等の継続開催による地域のセキュリティ意識向上・人材育成
- 国や専門家からの情報提供の場

大学・高専

地元企業

地元
ベンダー

民間団体

地域の
セキュリティ
関係者の
つながり

県警

自治体

国

将来目指す姿

- ニーズとシーズのビジネスマッチングや共同研究による地域発のセキュリティソリューションの開発
- 地域一体となった課題解決
- 地域を越えた連携



- 地域の課題解決
- 価値創出

地域SECURITY
がない状態

地域SECURITY
形成

コラボレーション・プラットフォーム
を全国に展開

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				セキュリティ専門家			
組織名	担当部署	連絡先		組織名	氏名	連絡先	専門等
IPA セキュリティプレゼンター	××課	XX-XXXX		JUAS	〇〇	XX-XXXX	経営層向け
IPA 講師派遣制度	〇〇課	XX-XXXX		JPCERT	△△	XX-XXXX	最新攻撃事例

地域SECURITYの全体スケジュール

- 令和2年度の地域SECURITYの取組の全体像としては以下の通り。
- 各地域での予算執行等を通じたコミュニティ形成の取組と並行して、コミュニティ形成のプラクティス集やセミナー等への専門家・講師派遣制度リストの作成・共有を実施する。2021年1月公表目標。

	2020年						2021年		
	7月	8月	9月	10月	11月	12月	1月	2月	3月
プラクティス集の共有	ヒアリング先の コミュニティの検討		ヒアリング項目の 有識者への意見照会		各コミュニティへの ヒアリング実施		プラクティス集の作成		
専門家・講師派遣制度 リストの作成・共有	有識者への意見照会 及び取りまとめ			リスト掲載機関との調整 (掲載の内容・可否等)			★ プラクティス集・リスト公表		
地域SECURITY事業	事業開始 ①セキュリティ・コミュニティ形成、②セミナー開催、③セキュリティの実態調査 等								

令和2年度の取組状況

- 業界団体や専門家、各地方経産局等と連携し、各地域におけるセキュリティ関係者間での意見交換・情報共有等を実施。コミュニティ形成に向けた取組を全国で推進する。

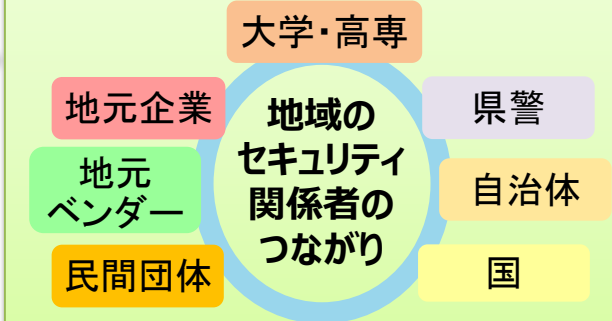
＜各地域のコミュニティ形成の促進に向けた支援例＞

- 地域のキーパーソン発掘支援
- 地域のセキュリティに関する活動調査
- 地域のセキュリティに関する意識調査
- セキュリティ関連のイベント・演習開催支援
- 講師・専門家派遣
- 他地域のプラクティス集の共有 等



＜目指す姿＞

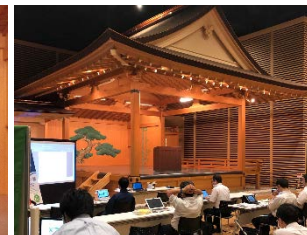
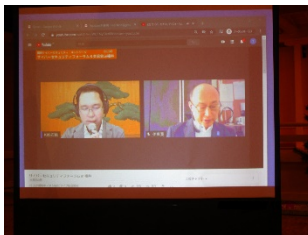
継続的に活動できるセキュリティコミュニティの形成を促進



先行事例：

＜福井県：サイバーセキュリティフォーラム in 福井（8/3）＞

- 福井県において、テレワーク時代にあった、サイバーセキュリティの取組機運向上及び域内関係者間のつながりを深めることを目的に実施。
- YouTubeLiveによるオンラインセミナーで148名(※)が参加し、地域の有識者による講演や、メディアが中心となった民間主体のセキュリティコミュニティ「メディアコンソーシアム」の立ち上げ等、県内の取組ピッチを実施。



(※)YouTubeの
ユニーク視聴者数。

1. 経営

2. 中小・地域

3. 人材

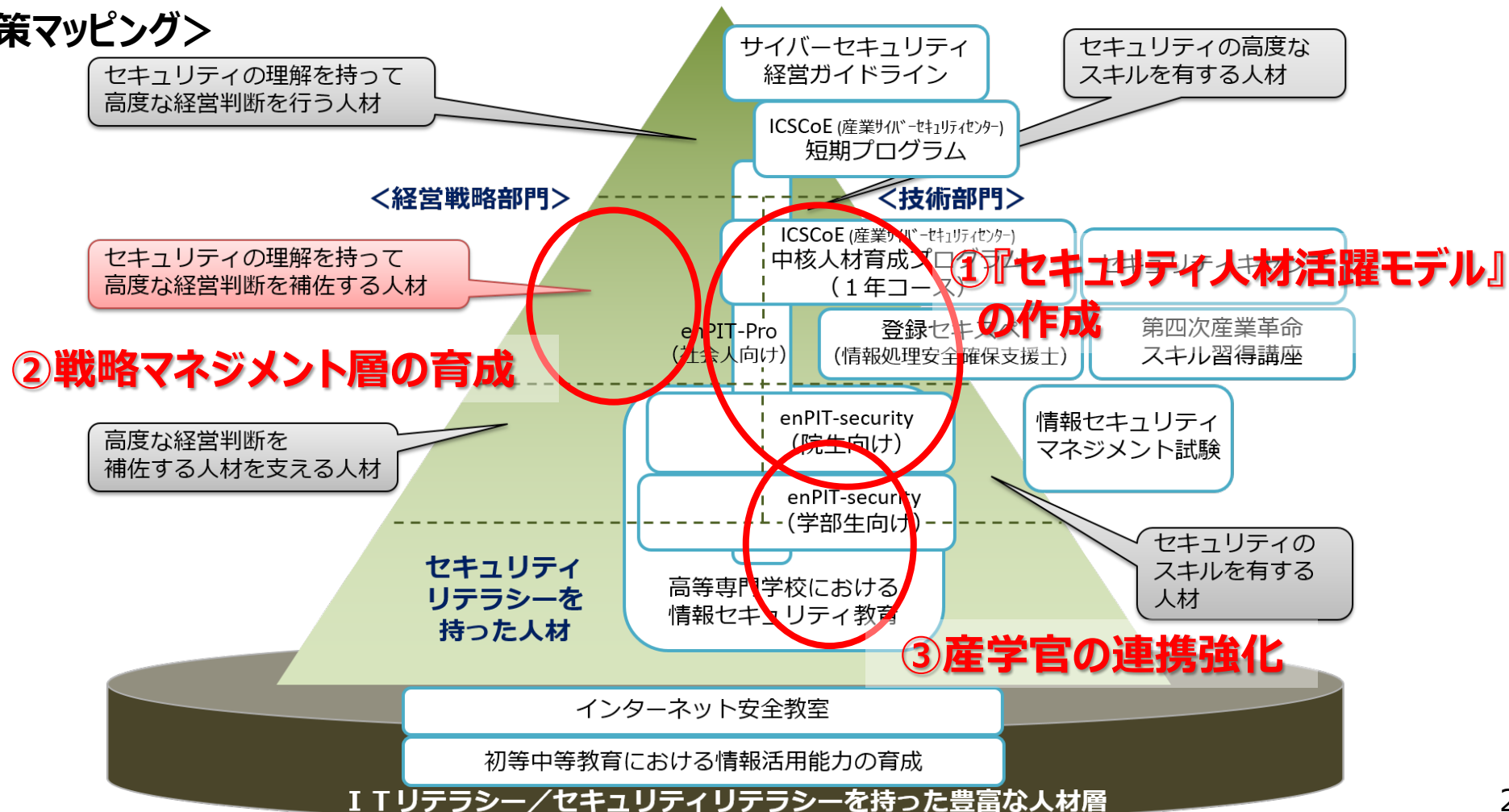
4. 国際

サプライチェーン・サイバーセキュリティ・
コンソーシアムの設立

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。

＜政策マッピング＞



(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

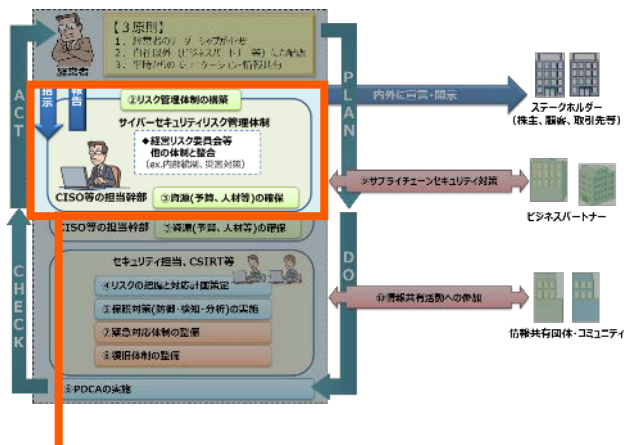
(3) 産学官の連携強化

(4) 産業サイバーセキュリティセンター

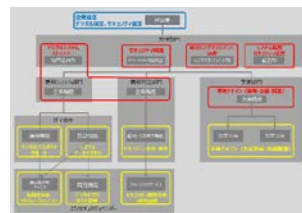
『セキュリティ体制構築・人材の確保の手引き』の開発

- サイバーセキュリティ経営ガイドラインの付録文書として新たに開発中。近日中に第1版を公表予定。

サイバーセキュリティ経営ガイドライン（10の指示）



手引きにおける共通言語としてのITSS+の活用の例



ユーザ企業・外注先における ITSS+のマッピングの例示

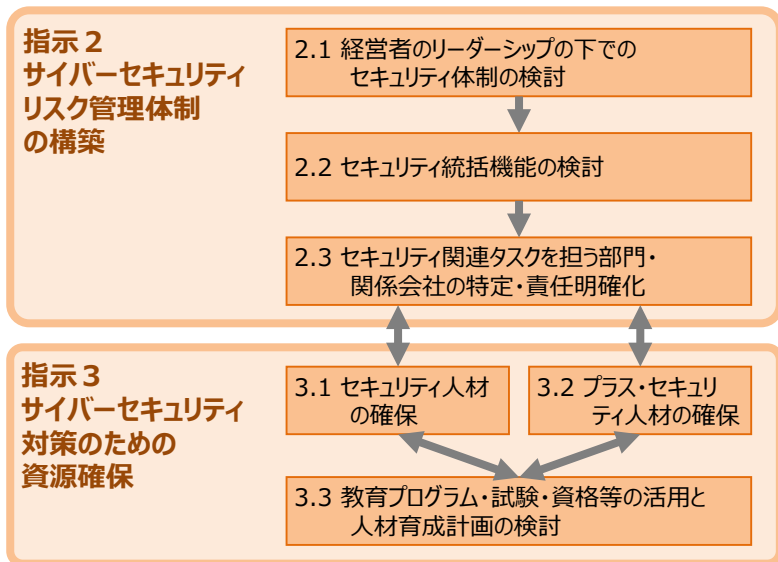


関連する試験・資格の例示



ITSS7段階での
保有スキル・キャリアの表現

手引きの構成（指示2、3の深掘り）



ITSS+（セキュリティ領域）改訂版を共通言語として活用

	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		
ユーザー企業における組織の例	取締役会 執行役員会議	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	<ul style="list-style-type: none">セキュリティ意識啓発対策方針指示ポリシー手続策定実施事項承認	<ul style="list-style-type: none">システム監査セキュリティ監査	<ul style="list-style-type: none">BOP対応官庁等対応法令遵守対応記者・広報対応調達・契約・検収施設管理・物理セキュリティ内部同行対策	<ul style="list-style-type: none">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外組織対応インシデントハンドリング	<ul style="list-style-type: none">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	<ul style="list-style-type: none">セキュリティシステム要件定義セキュリティアーキテクチャ設計セキュリティウェアハウス方式設計テスト計画	<ul style="list-style-type: none">基本・詳細設計セキュリティプログラミングテスト・品質保証パッチ開発脆弱性診断	<ul style="list-style-type: none">構成管理運用監視脆弱性対応セキュリティツールの導入・運用監査・検収・対応インシデントレスポンスペネテスト	<ul style="list-style-type: none">現場教育・管理設備管理・保全社庫持ち込み・開閉突発・フォレンジックマルウェア解析食糧・睡眠・情報線の収集・分析・活用	<ul style="list-style-type: none">セキュリティ理論研究セキュリティ技術開発
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	デジタル プロダクト サポート			
	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	※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/NN/IoT/Web等の 取扱い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						
						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)	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)			

情報処理安全確保支援士（登録セキスペ）の義務講習について

- 2020年5月の制度改正により、登録セキスペの義務講習の対象に、一定の条件を満たし、経済産業大臣が定めた民間事業者等が行う講習（特定講習）を追加。
- 特定講習は、登録セキスペが目指すキャリアパスなどに応じて、ITSS+（セキュリティ領域）の分野から受講したい分野を選択し、この分野に関連する知識・技能の実践的な活用力を習得することを目的とした講習。

登録セキスペの義務講習

登録セキスペには、①共通講習、②実践講習又は特定講習の2つの講習を受講することを義務付け。

①最新の知識・技能等を習得する講習

手法：オンライン 期間：年1回受講
実施機関：独立行政法人情報処理推進機構（IPA）

②知識・技能の実践的な活用力を習得する講習

手法：実習等の実践的な方法 期間：3年に1回受講

IPAの行う実践講習

又は

**民間事業者等が行う
特定講習**

特定講習

- 特定講習は、IPAが行う講習と同等以上の効果を有すると認められる講習。
- 登録セキスペが、ITSS+（セキュリティ領域）の分野から受講したい講習を選択できるようにする。

ITSS+（セキュリティ領域）のうち、特定講習対象分野

セキュリティ統括

セキュリティ監査

デジタルシステムストラテジー

デジタルシステムアーキテクチャ

デジタルプロダクト開発

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

デジタルシステム運用

(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

(4) 産業サイバーセキュリティセンター

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、サイバーセキュリティ2019に基づき、IPA産業サイバーセキュリティセンターでは、2018年度に引き続き、2019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。（IPAが後援）

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」



- 2020年2月実施（2018年度に続き2回目）
- サイバーセキュリティは経営課題であること及び経営層をはじめ関係者が認知すべきセキュリティ機能の重要性の理解を目指す。
- 体系だった知識の習得のため、「組織管理」と「実務管理」の座学2コースを実施（各2回、合計4回、1回あたり4時間）。延べ68名が参加。



東京工業大学CUMOT 「サイバーセキュリティ経営戦略コース」



- 2020年1月～実施中（当初終了予定は4月）
※新型コロナウイルス感染症対策で4月以降はオンライン講義で実施
- 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（1回2時間、4か月間）。



(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

(4) 産業サイバーセキュリティセンター

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。

（赤字＝前回WGからのアップデート）

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

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



国立高専教員

コンテンツ開発・授業の提供 （パワーポイント、ビデオ等）

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

※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。



- 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。
- 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

- 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。

セキュリティ合宿に関する協力

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。

- 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。



- 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。



※セキュリティ合宿のような機会は特段なし。

- 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。

(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

(4) 産業サイバーセキュリティセンター

産業サイバーセキュリティセンター（ICSCoE）（2017年4月設置）

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

□ 1年を通じた集中トレーニング

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

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

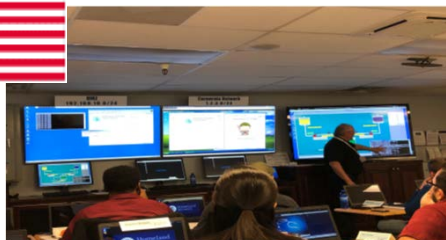
- IT系・制御系に精通した専門人材の育成
- 模擬プラントを用いた対策立案
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析



**現場を指揮・指導する
リーダーを育成**



□ 米・英・仏等の海外とも協調したトレーニングを実施



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



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



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

など

産業サイバーセキュリティセンター（ICSCoE）2025Visionの達成に向けて

- サイバー領域の脅威がフィジカル領域に大きな影響を与えるDXが進んだ産業社会のサイバーセキュリティ対応能力の開発・普及を行う中核機関を目指す。

事故調査の役割



幅広い分野のサイバー事故調査支援

世界に類を見ないユニークな機関



多様で実践的な研修プログラム



様々な分野の実環境の再現
外部機関の設備の活用

高い専門性・多様性



様々な分野・技術の専門家との
ネットワーク強化

最新情報の流通経路



OB会ネットワークの整備・組織化
OB人材活用

有能な人材輩出・知識のアップグレード



攻撃情報の分析・追究
カウンター能力とオープン・サイバーセ
キュリティ技術の開発

国際的な連携拠点

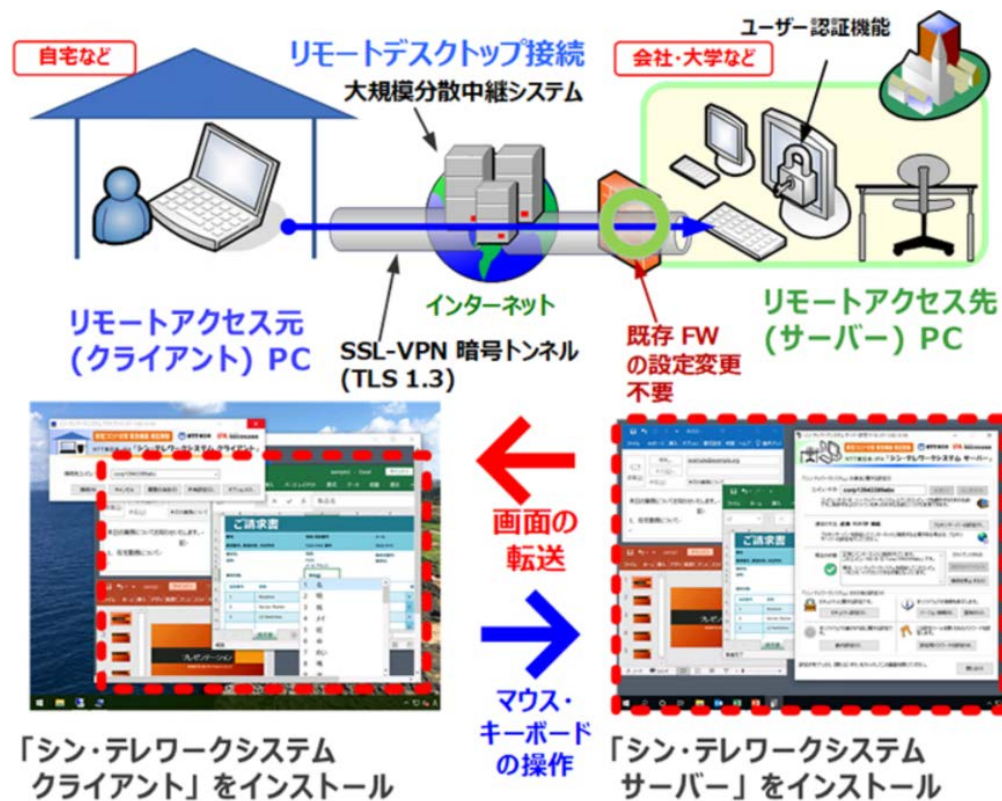


既存の国際交流活動の拡大・強化
JETRO・在外公館との連携強化

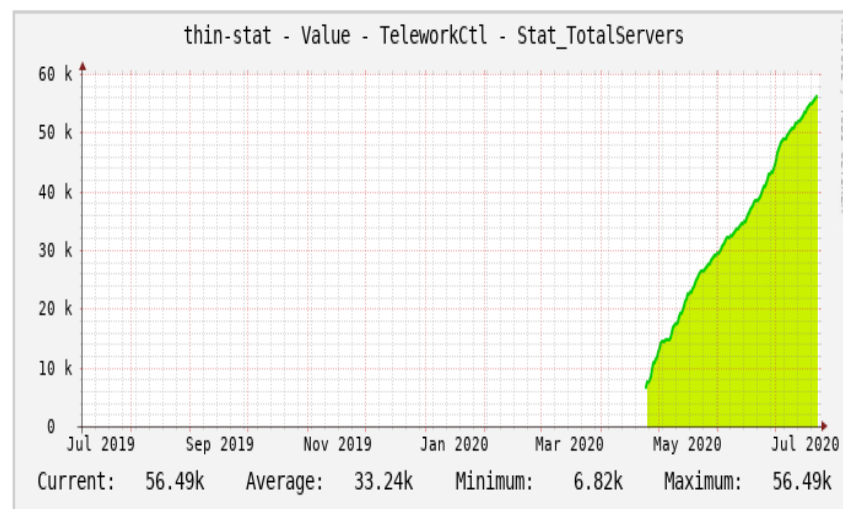
セキュアなテレワーク環境を実現する技術「シン・テレワークシステム」を
無償開放（次ページ参照）

(参考) シン・テレワークシステム

- 2020年4月21日、ICSCoEのサイバー技術研究室は、NTT東日本と連携し、緊急事態下においてテレワークを直ちに必要とされる方々のため、多くの方々が迅速かつ簡単に利用できるシンクライアント型SSL-VPNリモートデスクトップシステムを緊急構築し、無償提供。
- 公開3か月で5.5万ユーザーが利用。(2020/7/21時点)
- 現在もユーザーからの様々な要望を受けて機能強化を継続中。



NTT 東日本 - IPA「シン・テレワークシステム」
直近1年間のユーザー総数 (インストール・起動済の職場側 PC の台数) の推移



出典: <https://www.ipa.go.jp/about/press/20200421.html>
<https://telework.cyber.ipa.go.jp/stat/>

1. 経営

2. 中小・地域

3. 人材

4. 国際



**サプライチェーン・サイバーセキュリティ・
コンソーシアムの設立**


共有 (Share)

 **NDA関連情報が“目安”**

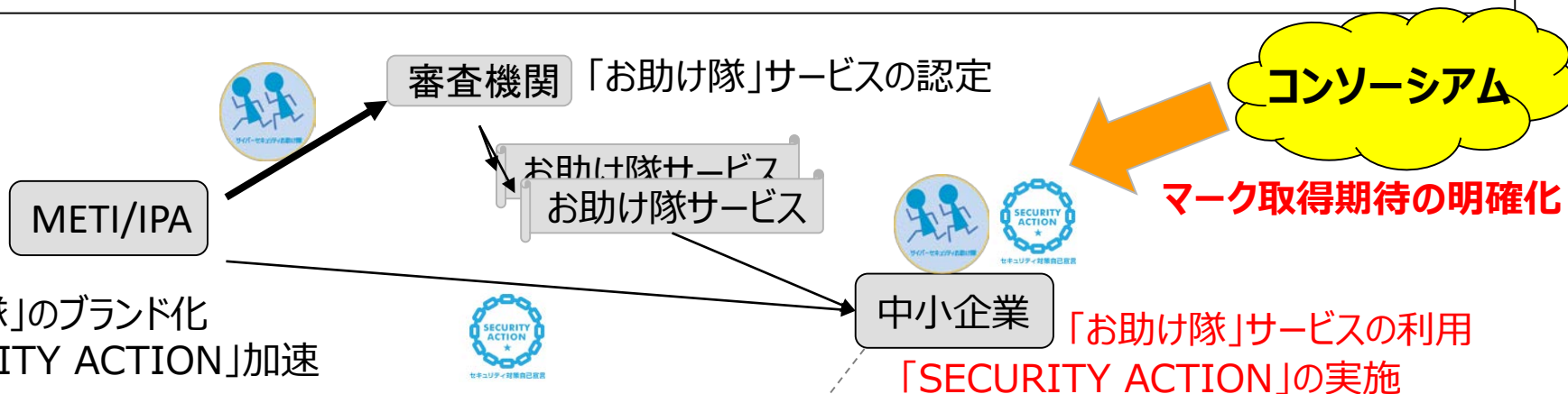
②機微技術情報の流出懸念時の経産省への報告

 **輸出管理対象技術が“目安**

③適切な場合の公表

 **被害企業内での取締役会へ
の報告事項(①の対象外の
もの)が目安**

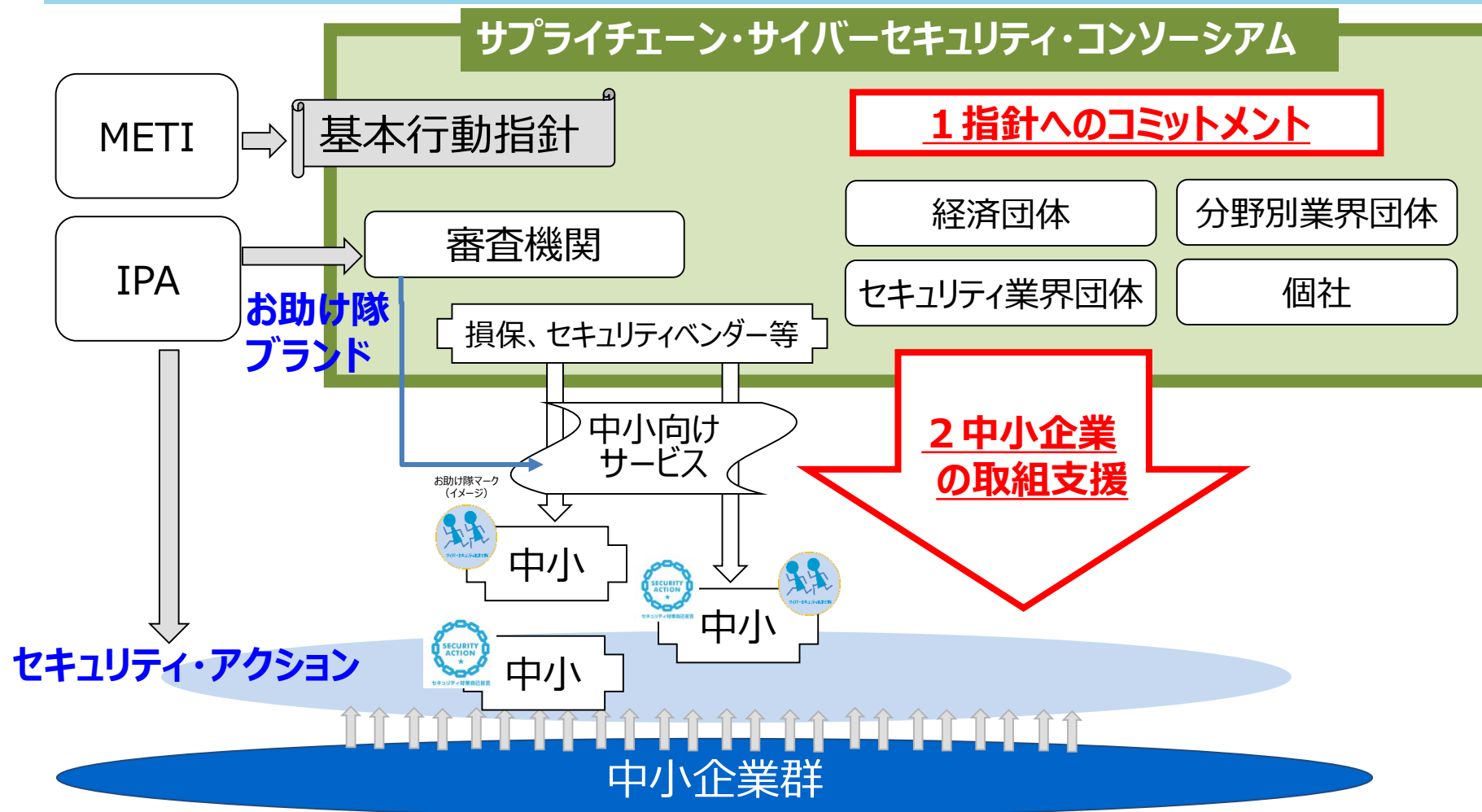
大企業と中小企業がともにサイバーセキュリティ対策を推進するためのコンソーシアムを立ち上げ。
 ーサイバーセキュリティ対策の取組を可視化し、マークを持つモノとの取引を望むことを明確化



特にサプライチェーン上重要な役割を担う者や多くの個人情報等を扱う者

サイバーセキュリティ強化運動の全体像（案）

- 立ち上げたコンソーシアムを活用し、
 - － 基本行動指針の実践
 - － 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。



サイバーセキュリティ強化運動の全体像（コンソーシアムのイメージ）

- 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。

参加資格：コンソーシアムの取組方針や経産省の「基本行動指針」に賛同いただき、規約に同意いただける個人・法人

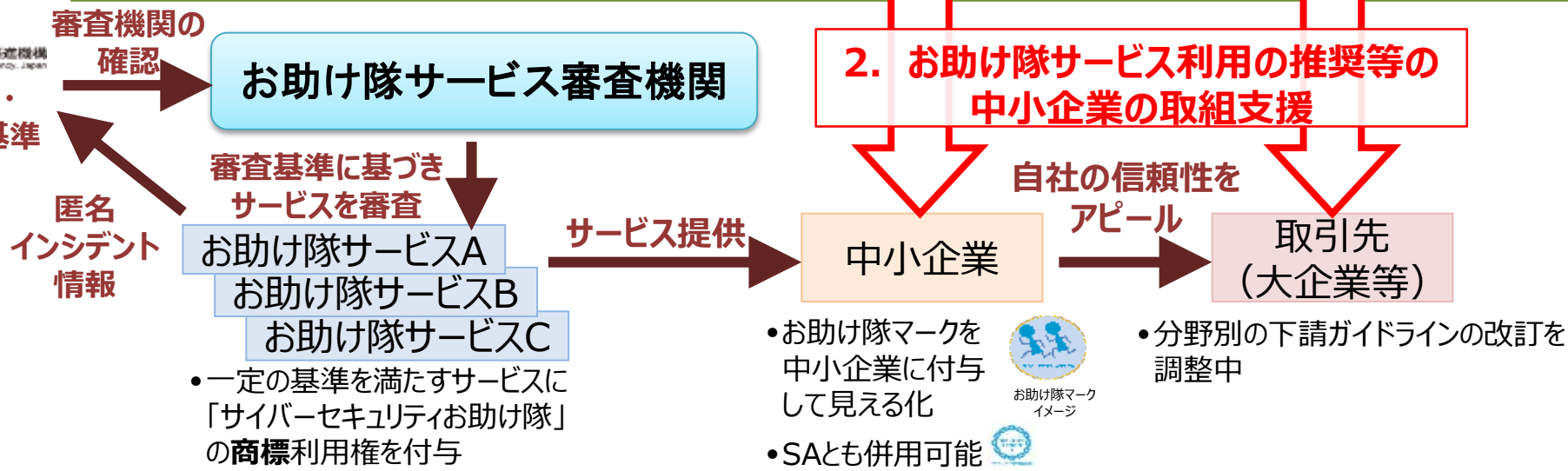
1. 基本行動指針へのコミットメント

Supply-Chain Cybersecurity Consortium (SC3)

事務局:IPA



2. お助け隊サービス利用の推奨等の中小企業への取組支援



コンソーシアム 各WGの議論内容（案）

中小企業対策強化WG

中小企業のサイバーセキュリティ対策強化のために、現状の課題や官民が取り組むべき施策や方向性について、幅広く検討。

地域SECURITY形成促進WG(P)

各地域におけるセキュリティ・コミュニティに関する取組について、プラクティスや課題を共有することにより、日本各地のサプライチェーンサイバーセキュリティ対策を底上げ・強化する。（原則オンライン開催）

産学官連携 人材育成促進WG(P)


産業界の求める人材像の共有、人材像を踏まえたカリキュラムの開発、各地域の高専等で生まれた産学官連携のプラクティスの共有を含む具体的な連携の促進などを通じ、サイバーセキュリティ分野における産学官連携での人材育成促進を図る。

1. 経営

2. 中小・地域

3. 人材

4. 国際



サプライチェーン・サイバーセキュリティ・
コンソーシアムの設立

インド太平洋地域向け日米サイバー演習2019の開催（第2回）



- 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（今年で2回目、以後毎年開催。）

■ **参加者**：ASEAN 9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



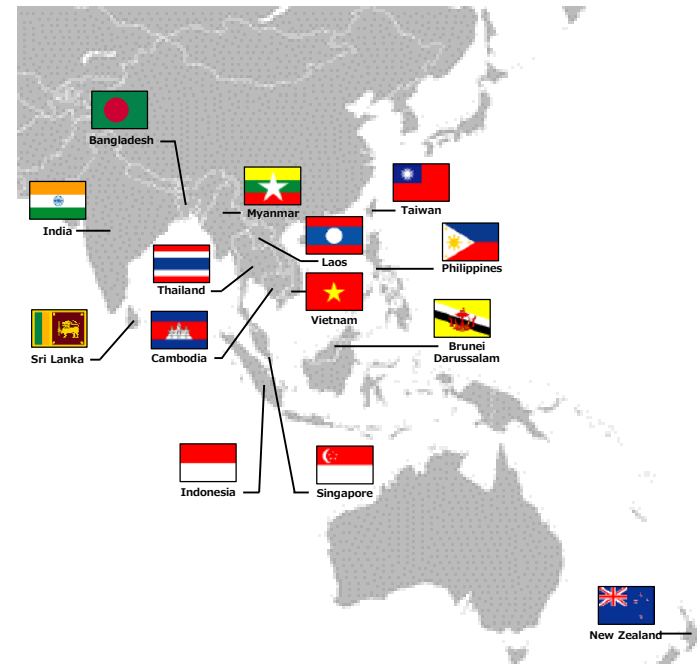
ハンズオントレーニング



ワークショップ



サイバー攻撃のデモ



参加国・地域

インド太平洋地域向け日米サイバー演習（第3回）の開催



- 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**インド太平洋地域向け産業制御システムに係るサイバーセキュリティ演習（第3回）**を実施予定。
- 過去2回の成果を踏まえ、**ユニークな国際イベントとして確立・発展。**

■ 日時・場所：2021年3月8日（月）～12日（金）@東京（予定）

■ 参加者：インド太平洋地域からの参加者、
ICSCoE中核人材育成プログラム研修生

■ 開催方針：

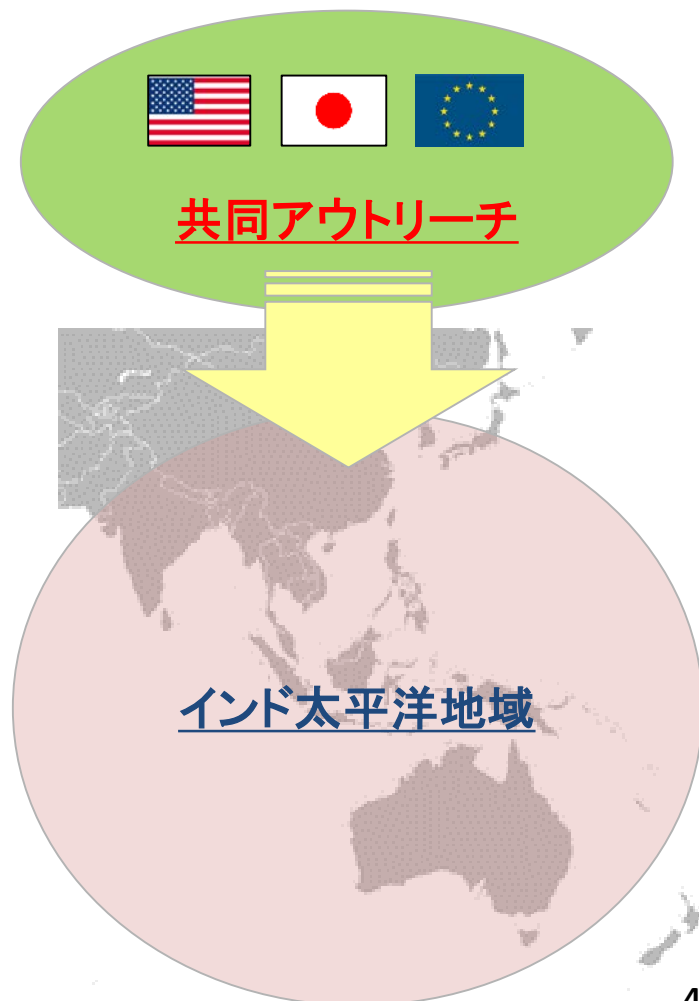
①電力、ガス等のエネルギー分野にフォーカス

⇒トレーニング、インタラクティブワークショップ等を通じ、エネルギー分野に特有の課題やソリューションについて情報共有、ネットワーキング、コラボレーションを促進。

⇒資工庁による日米電力サイバーセキュリティワークショップ等、既存の二国間での取組との連携により、二国間の協力強化、共同アウトリーチ効果の更なる向上を図る。

②日米に加え、EUからの専門家派遣

⇒インド太平洋地域の重要インフラ政策立案者、オペレーターに対して、日・米・EUが共同でアウトリーチを行うことで、「自由で開かれたインド太平洋」への取組を更に強化。



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。

- **日ウクライナサイバー協議（2020年1月@東京）**

- ウクライナ政府との協議において、CPSFと各TFでの議論、電力セキュリティ、人材育成の取組等を紹介。

- **サイバーテックテルアビブ（2020年1月@イスラエル・テルアビブ）**

- イスラエル発の国際的フォーラムにおいて、CPSFと第二層TFでの議論を紹介。

- **International Forum on Cybersecurity（2020年1月@仏・リール）**

- フランス発の欧州最大規模のフォーラムにおいて、CPSF、各TF、ビルガイドライン等の取組を広く紹介。

- **日英サイバー協議（2020年1月@東京）**

- 英国政府との協議において、CPSFと各TFでの議論、お助け隊、対ASEANキャパビルの取組等を紹介。

- **Cybersecurity Standardization Conference（2020年2月@ベルギー・ブリュッセル）**

- ENISA、ETSI主催フォーラムにおいて、CPSFと第二層TFでの議論を紹介。

- **APEC WS on IoT Security Best Practices（2020年2月@マレーシア・プトラジャヤ）**

- APECのマージンで米政府が主催したWSにおいて、CPSF、各SWG、各TF、特に第二層TFについて説明。

- **RSA Conference 2020（2020年2月@米・サンフランシスコ）**

- ITI主催のIoTセキュリティに関するラウンドテーブルにおいて、CPSF、第二層TFで検討中のフレームワークについて紹介。

- **NTIAとの意見交換（2020年7月@オンライン会議）**

- 米NTIAとの間で、SBOM（Software bill of materials）等、ソフトウェアのセキュリティに係る意見交換。

- **U.S. Chamber of Commerceとの意見交換（2020年7月@オンライン会議）**

- U.S. Chamber of Commerce主催のオンライン会議において、会員企業にCPSFと第二層TFでの議論、特にIoTセキュリティ・セーフティ・フレームワーク(案)を紹介。