資料３

経済産業省

事務局説明資料

令和４年３月２３日

経済産業省　商務情報政策局

サイバーセキュリティ課

０．全体像

１．経営

２．中小企業

３．人材

４．地域

５．国際

６．本日議論いただきたい論点

０．全体像

１．経営

２．中小企業

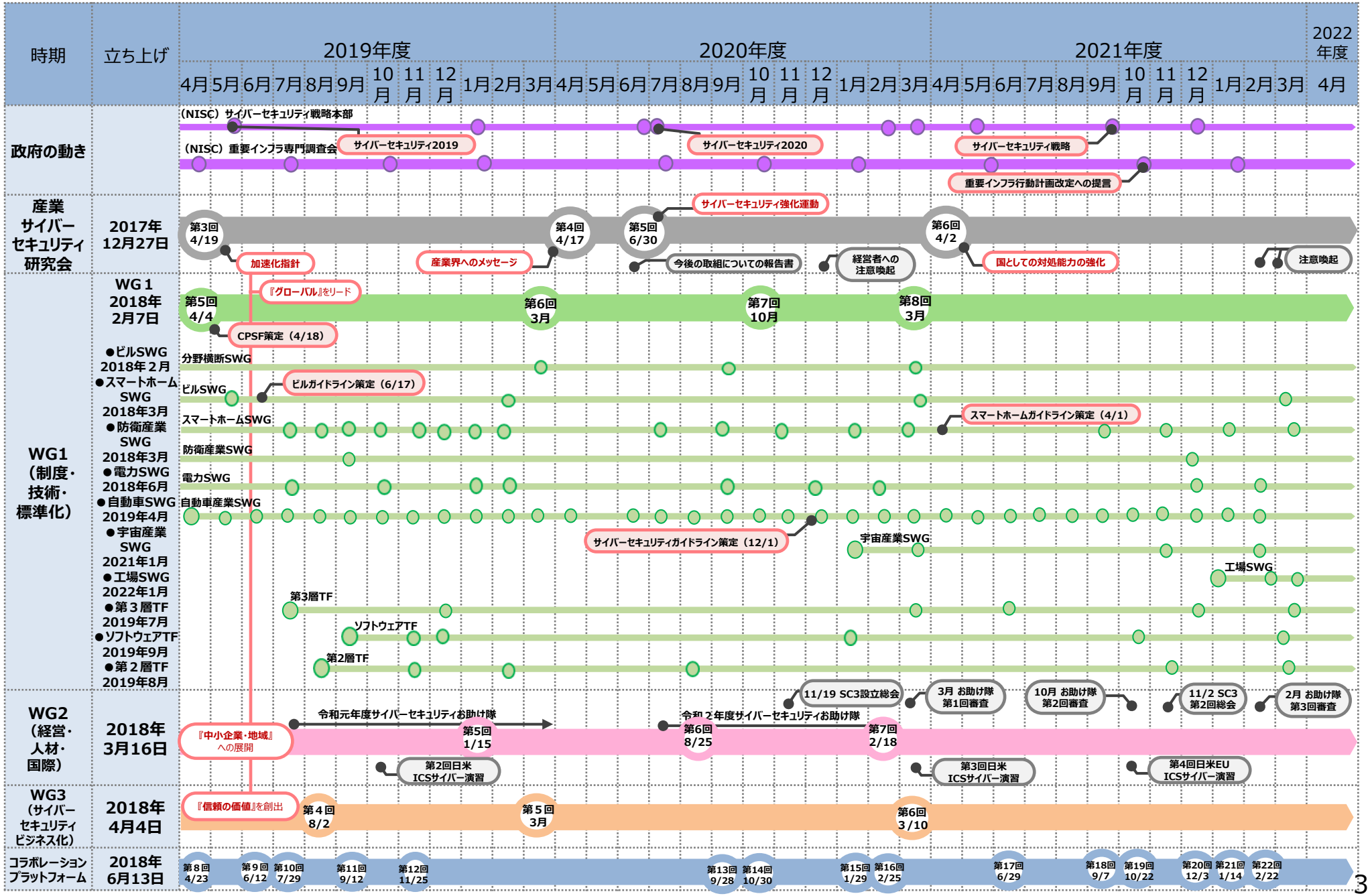
３．人材

４．地域

５．国際

６．本日議論いただきたい論点

産業サイバーセキュリティ研究会関連会議の実績



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＞

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:**「基本行動指針（インシデント発生時の共有・報告・公表）」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。
- **参加者:** 経済団体、業種別業界団体　等（2022年2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）

Supply-Chain Cybersecurity Consortium (SC3)

事務局：ＩＰＡ

総会
年１回程度開催（WG報告、重要事項の決定等）

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

2021年11月
第2回総会

運営委員会

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

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に向けた課題や取組の検討・推進

産学官連携WG
産学官連携によるセキュリティ関連の人材育成・活躍推進等について検討・推進

・・・・・

攻撃動向分析・対策WG
経営層が認識すべきサイバー攻撃関連動向や対策のポイントを産業横断で発信

地域SECUNITY形成促進WG
地域SECUNITYの取組を推進するための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

コンソーシアムの構成員

- 経済三団体（経団連、日本商工会議所、経済同友会）から役員が出ているほか、幅広い業界団体・個社が参加。（2022年2月末時点、96団体含む175会員）

役員
- 会　長　：一般社団法人 日本経済団体連合会　サイバーセキュリティ委員長　遠藤信博氏
- 副会長：日本商工会議所　特別顧問　金子眞吾氏　、　公益社団法人経済同友会　副代表幹事　間下直晃氏

団体会員リスト

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
一般社団法人 コンピュータソフトウェア協会
一般社団法人 日本金型工業会
鋳型ロール会
一般社団法人 日本陸用内燃機関協会
一般社団法人 日本機械工業連合会
石油連盟
特定非営利活動法人 ITコーディネータ協会
一般社団法人 日本電子回路工業会
一般社団法人 全国地方銀行協会
一般社団法人 日本自動車工業会
日本商工会議所
一般社団法人 中小企業診断協会
一般財団法人 日本自動車査定協会
一般社団法人 日本鋳鍛鋼会
日本筆記具工業会
一般社団法人 日本ボディファッション協会
日本化学繊維協会
一般社団法人 日本金属熱処理工業会
静岡県ソフトウェア事業協同組合
一般社団法人 日本化学工業協会
一般社団法人 情報サービス産業協会
一般社団法人 全日本文具協会
一般社団法人 日本ガス協会
特定非営利活動法人 映像産業振興機構
全国商工会連合会
全国社会保険労務士会連合会
日本ドキュメントサービス協同組合連合会
一般社団法人 日本風力発電協会
日本小売業協会
電気事業連合会
一般社団法人 日本医療機器産業連合会
一般社団法人 日本航空宇宙工業会
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
独立行政法人 中小企業基盤整備機構
一般社団法人 日本広告業協会
一般社団法人 情報処理安全確保支援士会
一般社団法人 日本電機工業会
一般社団法人 日本印刷産業連合会
一般社団法人 日本自動車部品工業会
一般社団法人 日本鉄鋼連盟
一般社団法人 ビジネス機会・情報システム産業協会
一般社団法人 太陽光発電協会
一般社団法人 日本中古自動車販売協会連合会
特定非営利活動法人 日本セキュリティ監査協会
一般社団法人 電子情報技術産業協会
一般社団法人 日本情報システム・ユーザー協会
一般社団法人 鹿児島県サイバーセキュリティ協議会
一般社団法人 日本工業炉協会
一般社団法人 日本経済団体連合会
一般社団法人 沖縄県情報産業協会
全日本フレキソ製版工業組合
一般社団法人 九州経済連合会
一般社団法人 日本金属プレス工業協会
産業横断サイバーセキュリティ検討会
一般財団法人 関西情報センター
一般社団法人 日本防衛装備工業会
四国ＩＴ協同組合
特定非営利活動法人 山梨ＩＣＴ＆コンタクト支援センター
一般社団法人 保健医療福祉情報システム工業会
せんい強化セメント板協会
一般社団法人 日本自動車機械器具工業会
一般社団法人 全国信用金庫協会
全国カレンダー出版協同組合連合会
一般社団法人 第二地方銀行協会
一般社団法人 日本損害保険協会
一般財団法人 デジタルコンテンツ協会
宮城県サイバーセキュリティ協議会
一般社団法人 中国経済連合会
一般社団法人 日本スポーツ用品工業協会
一般社団法人 日本オンラインゲーム協会
一般社団法人 長崎県情報産業協会
一般社団法人 日本レコード協会
一般社団法人 情報通信ネットワーク産業協会(CIAJ)
公益社団法人 経済同友会
一般社団法人 日本ボランタリーチェーン協会
公益社団法人 日本訪問販売協会
公益社団法人 日本マーケティング協会
一般財団法人 沖縄ITイノベーション戦略センター
公益社団法人 福岡貿易会
大阪商工会議所
公益財団法人 ハイパーネットワーク社会研究所
公益社団法人 関西経済連合会
一般社団法人 組込みシステム技術協会
一般社団法人 オープンガバメント・コンソーシアム
特定非営利活動法人 日本情報技術取引所
全国中小企業団体中央会
日本税理士会連合会
東部大阪経営者協会
一般社団法人 日本医療機器ネットワーク協会
独立行政法人　国立高等専門学校機構
一般社団法人　日本スマートフォンセキュリティ協会
一般社団法人　日本建設機械工業会
ICSCoE叶会
モバイルコンピューティング推進コンソーシアム
一般財団法人草の根サイバーセキュリティ運動全国連絡会

０．全体像

１．経営

２．中小企業

３．人材

４．地域

５．国際

６．本日議論いただきたい論点

段階的なサイバーセキュリティ経営の実現（全体像）

- 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、状況変化を踏まえた改訂

2nd Step

サイバーセキュリティ経営の実践

- DXの進展を踏まえ、サイバーセキュリティリスク対応の重要性に対する意識啓発を推進
- 投資家等ステークホルダーを通じたサイバーセキュリティの重要性の啓発
- GGS(グループ・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
- プラクティス集、人材の手引きの整備により、サイバーセキュリティ経営を現場レベルで推進

3rd Step

セキュリティの高い企業であることの可視化

- 可視化ツールの普及によるサイバーセキュリティ経営の可視化の推進
- 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の改訂

1st step

- 前回改訂時（平成29年11月）以降のサイバーセキュリティ経営を取り巻く情勢の変化等を踏まえ、**サイバーセキュリティ経営ガイドラインについて、2022年度中に改訂を実施予定。サイバー・フィジカル・セキュリティ対策フレームワーク(CPSF)のコンセプトの反映やサプライチェーンの再整理**など、所要の改訂を行う予定。

課題

- ◆ 現行のガイドラインの普及により経営層の意識は高まりつつあるものの、サイバーセキュリティ対策が事業継続や新たな価値創出のために不可欠な「投資」と捉える意識改革が引き続き重要。
- ◆ 他方、前回の改訂以降、サイバーセキュリティ経営を取り巻く情勢の変化（サプライチェーンの複雑化、ステークホルダーの広がり等）や、関連ガイドライン・ツールの策定・更新等（2019年サイバー・フィジカル・セキュリティ対策フレームワークの公表等）も生じているところ。

対応

- ◆ セキュリティはコストではなく投資であるとの位置づけや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す現行ガイドラインの基本的な方向性は維持。認識の促進を継続。
- ◆ 他方、新たな概念等も盛り込む形でアップデートを図り、より適確な形でサイバーセキュリティ経営の必要性を伝達。

<サイバーセキュリティ経営ガイドラインの改訂に向けた検討項目案>

- CPSF等新たなガイドラインのコンセプトの反映
- サプライチェーンの再整理
- 経営者がコミュニケーションを行うべき関係者の再定義
- クラウド等最新技術と留意点の盛り込み
- 制御系を含むインシデント演習の必要性の加筆　等

『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』

2nd step

- 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。その後第2版を2020年6月3日に公表。
- １万件超のダウンロードがあるなど一定の評価を得ているが、更なる改善のために、2020年度は**プラクティス利用の実態把握や企業が使いやすいプラクティスの在り方を明確にするための調査**を実施し、2021年4月にIPAより調査結果を公表。本調査結果等も踏まえた上で、プラクティスの追加等を行った**第３版を2022年３月に公表予定**。

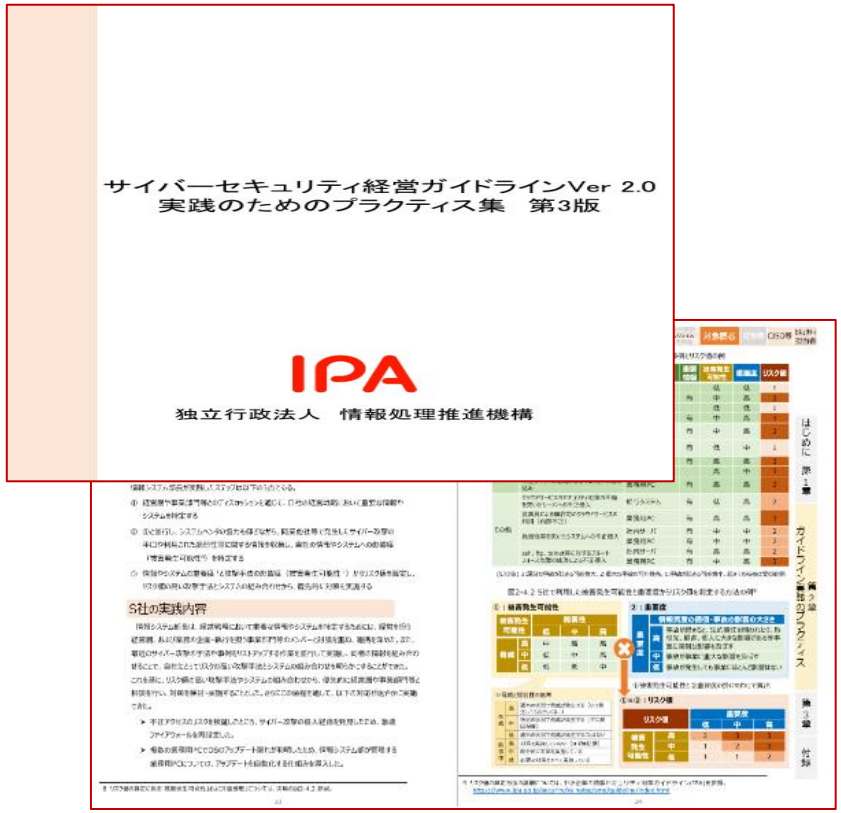
第２版までの累計17,552ダウンロード
（2022年1月末）

＜主な改訂内容＞

2020年度調査の結果を踏まえ、主に第2章と第3章の内容を充実させる形で改訂

◆第2章
　経営ガイドラインの付録A「チェックシート」より、「指示１」、「指示５」、「指示6」、「指示7」のチェック項目に関するプラクティスを追加

◆第3章
　情報セキュリティ10大脅威2022の「組織」向け脅威より、１位「ランサムウェアによる被害」、３位「テレワーク等のニューノーマルな働き方を狙った攻撃」、４位「サプライチェーンの弱点を悪用した攻撃」、５位「内部不正による情報漏えい」に関するセキュリティ担当者の悩みについてのプラクティスを追加



https://www.ipa.go.jp/security/fy2020/reports/practice/index.html

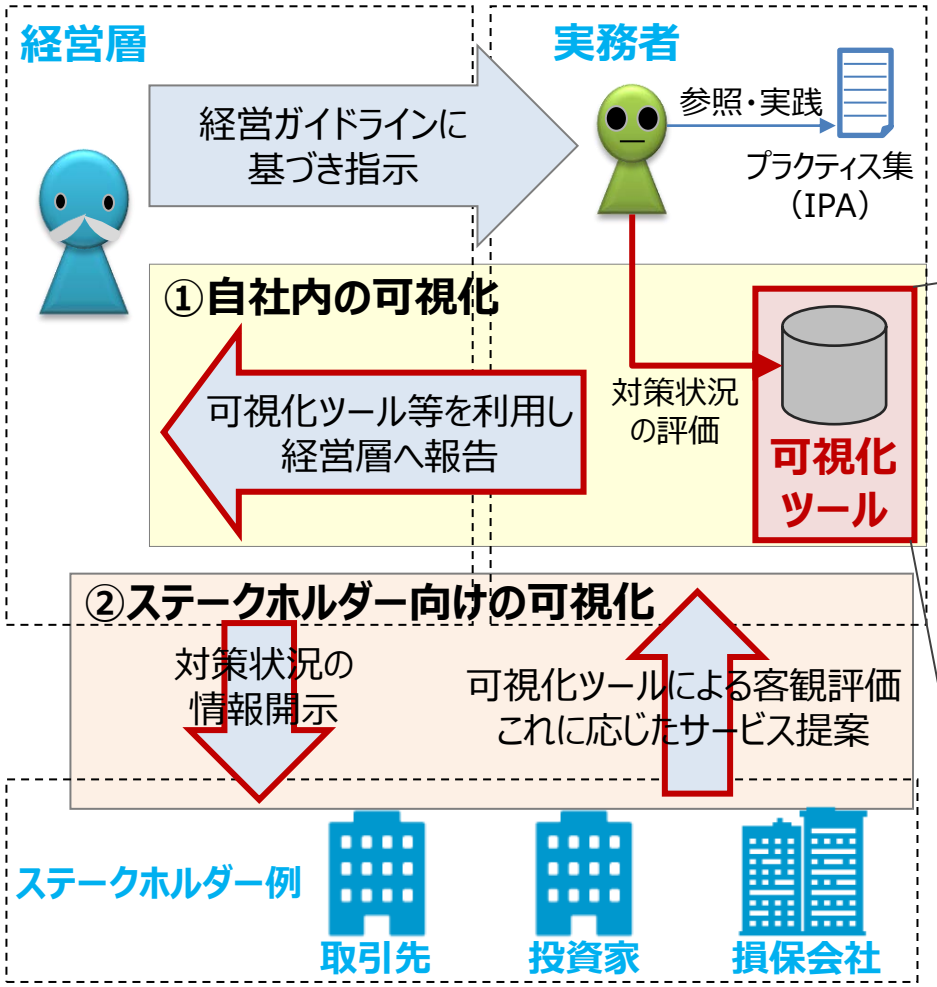
サイバーセキュリティ経営可視化ツールWeb版を公開（2021年8月17日）

2nd ～ 3rd step

- 2020年3月25日、可視化ツールβ版（Excel）をIPAから公開。
- 2020年度はユーザ企業、投資家等ステークホルダー向けにそれぞれβ版でテストを行い、ブラッシュアップを実施。**2021年8月17日、Ver1.0（Web版）公開！**

累計6,501ダウンロード（2021年8月末時点）

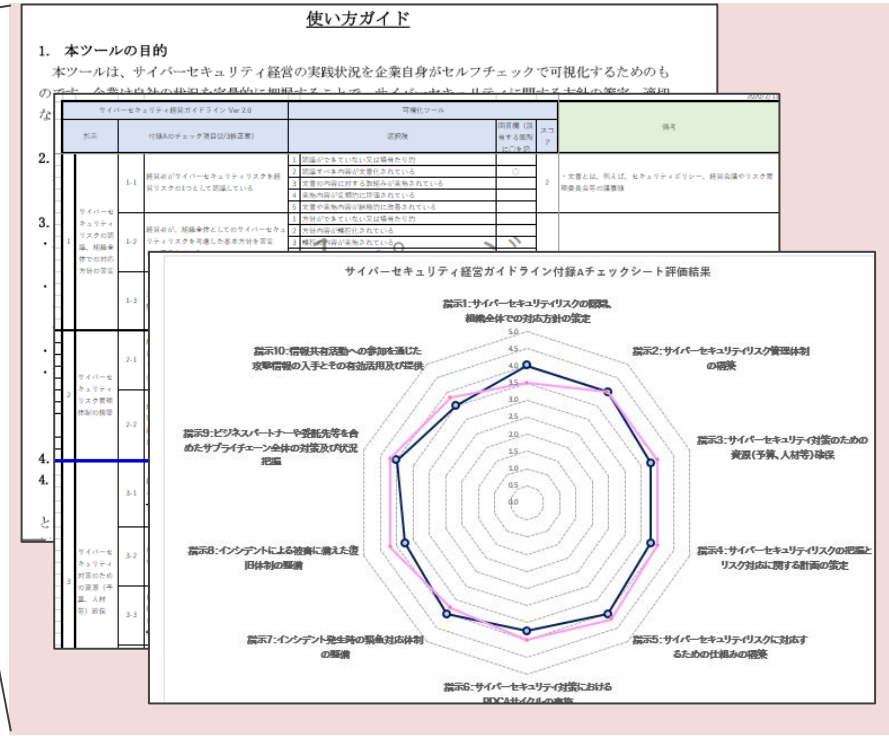
累計1046ダウンロード（2022年1月末）



特徴

- 39個の質問に回答⇒実践状況をレーダーチャート表示
- 過去の診断結果とも比較（経年変化）可能※
- 各業種の平均値とも比較可能※
- 「サイバーセキュリティ経営ガイドラインVer.2.0実践のためのプラクティス集」の実践事例も表示可能※

（※β版からの改良点）



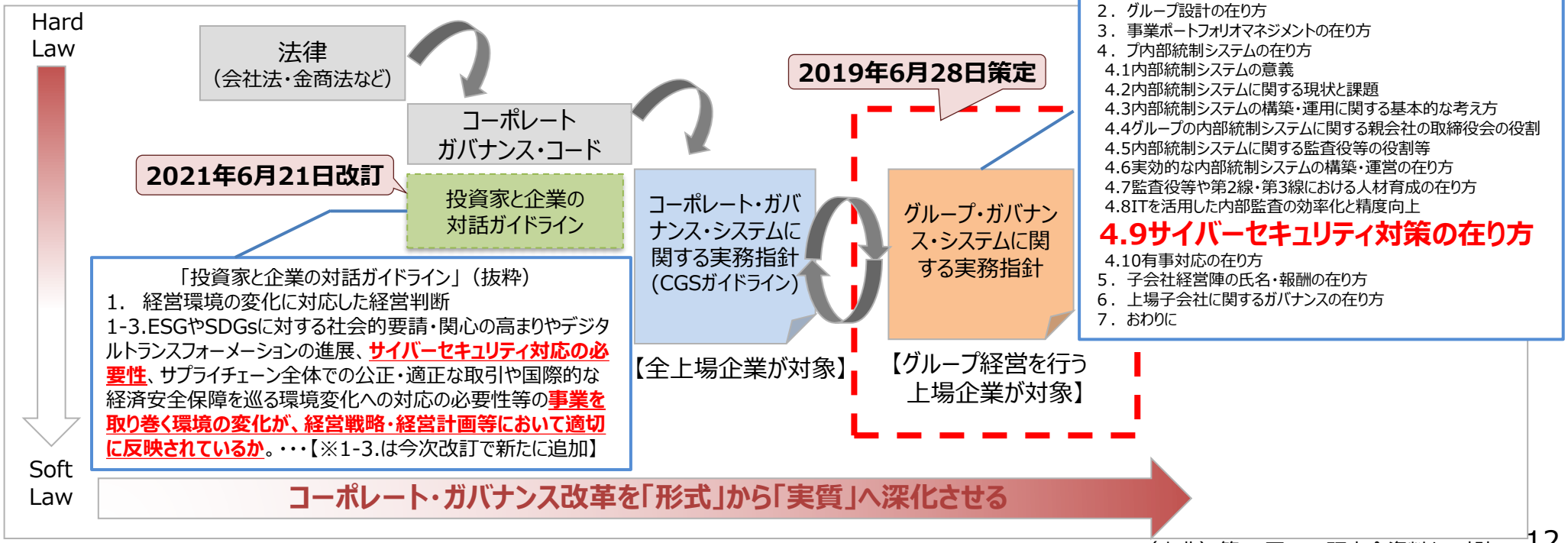
https://www.ipa.go.jp/security/economics/checktool/index.html

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

2nd step

- **「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。
- また、**「スチュワードシップ・コード」及び「コーポレートガバナンス・コード」の付属文書である「投資家と企業の対話ガイドライン」**（金融庁、2021年6月改訂）においても、新たにサイバーセキュリティ対策の必要性等を含む事業環境変化の経営戦略・経営計画等への反映が盛り込まれた。
- このほか、DXを進める企業におけるステークホルダーとの対話の在り方を示す**「デジタルガバナンスコード」**(2020年11月公表)においても、経営者がサイバーセキュリティリスク等に対して適切に対応を行うべき旨を記載。

<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研究会資料を一部加工

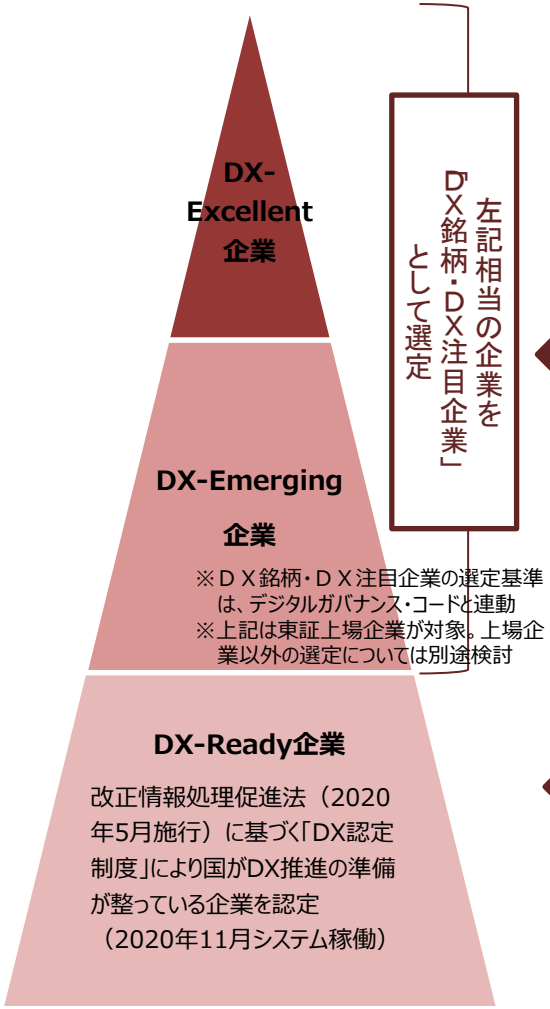
DX with Cybersecurity経営の推進：経営層によるリスク把握・企業情報開示

2nd ～ 3rd step

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

DX経営の推進

◆DX企業の体系



※ＤＸ銘柄・ＤＸ注目企業の選定基準は、デジタルガバナンス・コードと連動
※上記は東証上場企業が対象。上場企業以外の選定については別途検討

改正情報処理促進法（2020年5月施行）に基づく「DX認定制度」により国がDX推進の準備が整っている企業を認定（2020年11月システム稼働）

※「DX認定」は、「DX投資促進税制」の要件の一つとなっている。

◆デジタルガバナンス・コード(2020年11月策定)

経営者が企業価値向上に向け実践すべき事項

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

望ましい方向性に係る取組例より：

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

○情報処理安全確保支援士（登録セキスペ）の取得を会社として奨励。

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

認定基準：

○戦略の実施の前提となるサイバーセキュリティ対策を推進していること。

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

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

サイバーセキュリティ経営の推進

1st Step サイバーセキュリティ経営の明確化

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

2nd Step サイバーセキュリティ経営の定着

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

3rd Step セキュリティの高い企業であることの可視化

➢「可視化ツール」の普及によるサイバーセキュリティ経営の可視化の推進

活用推奨

活用推奨

◆Web版「可視化ツール」※

※経営ガイドライン実践状況の可視化ツールV1.0
→①経営層による自社リスクの可視化/把握
②ステークホルダー（取引先、投資家、損保会社）とのコミュニケーションに活用

機関投資家ヒアリング調査の概要（中間報告）

2nd ～ 3rd step

- 本年度の委託事業において、企業経営層の意思決定に影響を持つステークホルダー（機関投資家、M&A関連デューデリジェンスサービス事業者等）に対し、企業評価におけるニーズ・課題の把握や経営ガイドライン・可視化ツール等の普及を目的とした調査を実施。
- 企業評価の過程でセキュリティに関しては、**被害が生じた際の緊急対応体制や復旧体制の整備をより重視する傾向**が存在。また、業種、業態別にサイバーセキュリティの軽重が異なることも判明。

これまでにいただいた回答の例

機関投資家による投資先企業のサイバーセキュリティ対策状況の確認について

- **セキュリティ体制は機能していることが重要**。**現場と経営陣が円滑につながっているか**を確認したい。
- 扱う情報が多い業種・業態のリスクは高いと考える。**データの流出が企業の存続に関わるようなケースでは詳細に確認する**。
- 開示情報のエビデンスは重視していない。エビデンスがあってもリスクはゼロにならない。プライバシーマークやISO認証などは若干の安心材料だが、**体制や想定リスクに関する質問に対し、クリアな情報が提示されることが重要**。
- **事故発生の可能性はゼロにならないので、リカバリーの体制が取られているのかを含めた開示を期待**。
- サイバーセキュリティの世界は、人権デューデリジェンスに近い捕捉の難しさがあると感じている。**PDCAを通じたレベルアップを前提に、基準や取組事項をまとめた行動計画を普及させるべきではないか**。

M&Aにおけるデューデリジェンスでのサイバーセキュリティ対策状況の確認について

- M&AにおけるIT関連のデューデリジェンスはほとんどの企業を対象に実施。**サイバーセキュリティを対象とすることはまだ少ないが、以前に比べると増えている**。
- **買収対象企業のIT管理体制、委託関係、運用・監査等の規定整備状況等を確認**する。この中にサイバーセキュリティ対策状況も含まれる。場合により、**サイバーセキュリティの重点的な確認を依頼されることもある**。
- サイバーセキュリティ対策状況を評価する際に、**かけている費用よりは、構築している体制や管理状況を主に評価**する。買収先の社内環境をそのまま繋げて問題ないかどうかの視点で見る。

機関投資家ヒアリング調査結果を踏まえた情報開示の在り方の検討

2nd ～ 3rd step

- **経営ガイドラインはM&Aデューデリジェンスなどで活用されているが、可視化ツールは認知度の向上が課題**。気候変動に関する情報開示のプロトタイプなどを参考にすることも有用ではとの提案があった。

企業をサイバーセキュリティの観点で評価する際に参考にしているガイドライン等

- **企業のサイバーセキュリティ対策の評価には、経営ガイドラインを利用。**網羅的にまとまっていることを評価。経済産業省が作成したという点でも通りが良い。**可視化ツールについては認知はしていたが使ったことはなかった**（M&A関係者）。
- DXを進めていく上での落とし穴などは経済産業省などで手引きとして示してもらえるとよい（機関投資家）。
- **ステークホルダー保護の観点から、公的機関から最低限やるべきレベルを示してもらえるとよい**（M&A関係者）。

今後参考となりそうなポイント（機関投資家等によるDXやリスク管理等に関する評価方法について）

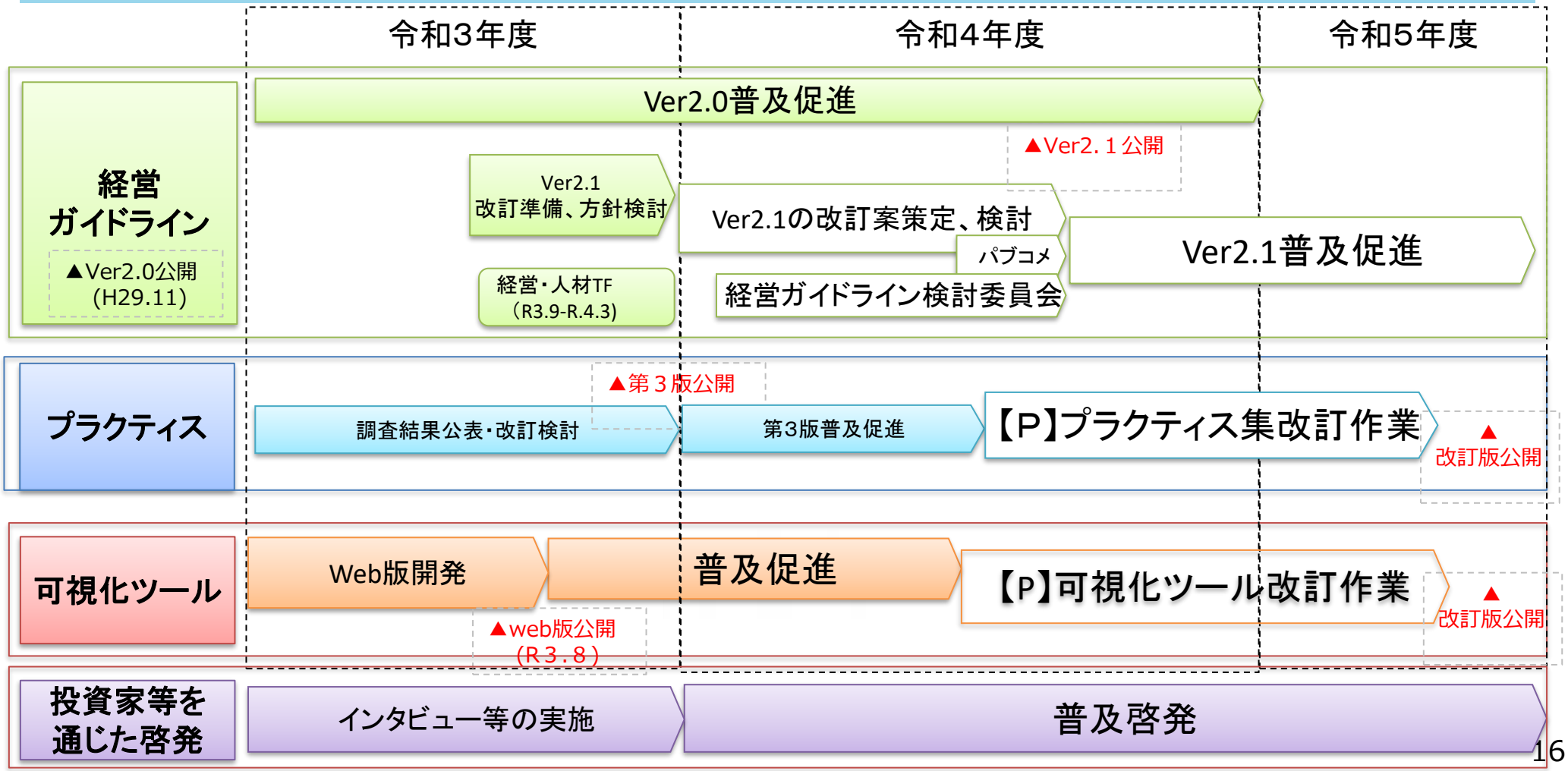
- 「気候関連財務情報開示タスクフォース（TCFD）」が「ガバナンス」、「戦略」、「リスク管理」、「指標と目標」の４つの柱に関して開示のプロトタイプを示している。投資家はこうした動きになじみはじめており、**他のリスクに関しても開示のプロトタイプとして、わかりやすい開示を求める動きが出てくる可能性**がある。
- 法律で開示が求められている情報の内容は各社とも似通っており、あまり読むことはない。**自社にとって致命的なリスクをメリハリをもって示すことが重要**。
- 企業としての社会的責任に関する対応状況については、ISO26000（組織の社会的責任）を活用している。

経済産業省による機関投資家への普及啓発の方法

- 証券会社が開催するセミナーには多くの投資関係者が参加するため、そこで施策紹介すれば認知度が高まるのではないか。
- GPIF（年金積立金管理運用独立行政法人）の取組を機関投資家が取り入れることが多いので、GPIFにアピールしてはどうか。

今後のスケジュール

- **サイバーセキュリティ経営ガイドラインVer2.1 の策定、プラクティス普及により、サイバーセキュリティ経営の明確化と実践を促進。**
- 可視化ツールの更なる普及促進を図り、取組状況を客観的な指標により評価可能とし、**自社の取組状況の確認やステークホルダーによる評価に結びつける。**



経営層・セキュリティ推進管理者向け情報発信コンテンツの整備

- SC3攻撃動向分析・対策WGを立ち上げ、**設立記念ウェビナーの開催、経営層向け情報発進コンテンツ（経営者インタビュー・専門家による情報コラム等）を整備。**
- 経営層への情報提供媒体・手法を協議の上、コンテンツ発信を試行し、**経営層が求めるコンテンツ類・効果的な情報提供手法の実践**を目指す。

攻撃動向分析・対策WG 設立記念ウェビナー (2021/11/15)
『ビジネス・経営の観点から認識・留意すべきサイバーセキュリティ関連動向と対策事例』
・講演：ランサムウェア攻撃 ～被害をどのように防ぎ・対応すべきか～
・ﾊﾟﾈﾙﾃﾞｨｽｶｯｼｮﾝ：今からできるセキュリティ対策～企業としての取り組み事例～
企業幹部・管理者中心に450名が聴講申込

[アンケートによる実態把握]
・セキュリティ運用体制・危機管理手順の状況
・危機管理情報の収集方法・対象
・経営層へのセキュリティ関連の報告手段・内容
・経営者が必要としている情報と提供形態

コンテンツ内容の設定　**提供手法の設定**

経営者インタビュー

■**対象**
・大手３者/中小２者
・ﾘﾌｧﾚﾝｽとなり得る企業
・ｲﾝｼﾃﾞﾝﾄ対応した企業

■**インタビュー内容**
・セキュリティ対策への取組
・ビジネス観点での効果
・人材/予算確保のﾎﾟｲﾝﾄ
・情報開示への取組み
・事業リスク対策の考え方

経営者に役立つ情報コラム

■**ｾｷｭﾘﾃｨ専門家による解説**
・グローバルセキュリティガバナンスの課題と対応
・クラウド/OSSセキュリティ動向
・ビジネスにおけるリスク・コミュニケーションの必要性
・セキュリティ経営に向けて考慮すべきチェックポイント
・システムにおけるセキュア設定の必要性

ウェビナーコンテンツ

■**ﾊﾟﾈﾙﾃﾞｨｽｶｯｼｮﾝﾃｰﾏ**
・今からできるセキュリティ対策（企業の取組事例）

■ **ﾓﾃﾞﾚｰﾀ/ﾊﾟﾈﾘｽﾄ**
・攻撃動向分析WGメンバ（民間企業５者）

■ **内容**
・自社における取組紹介（DX連携/見える化等）
・セキュリティ運用のﾎﾟｲﾝﾄ
・経営層とのｺﾐｭﾆｹｰｼｮﾝ

経営層の実態を踏まえた情報提供コンテンツ媒体・実施方法

情報発信効果の把握

周知・プロモーション計画

本日ご議論いただきたいポイント（経営）

- サイバーセキュリティ経営の促進に向け、主に以下の点について、ご意見等いただきたく存じます。

経営

- 経営ガイドラインの改訂において、考慮すべき状況変化等
- サイバーセキュリティ経営の促進のために経営者に発信していくべき情報や、投資家等ステークホルダーを通じた対策促進の方法
  （例：どのような施策・文書等と紐付けていくべきか）

０．全体像

１．経営

２．中小企業

３．人材

４．地域

５．国際

６．本日議論いただきたい論点

中小企業のサイバーセキュリティ対策促進の全体像

- 今年度は、各施策ツールの普及啓発に加え、中小企業やサプライチェーンのセキュリティ対策実態・施策ツール認知度等を調査。これらの結果や新たな課題を踏まえ、今後もさらなる対策促進を図る。

取組の全体像

ツール
- 中小企業向けガイドライン
- SECURITY ACTION
- サイバーセキュリティお助け隊

実態把握
- 中小企業の実態調査（IPA）
- 業界団体等へのヒアリング調査（IPA）
- 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（経済産業省）

地域における普及啓発
- 地域金融機関を通じた普及啓発
- 地域SECUNITY形成促進

【参考】各種インセンティブ施策との連携

サプライチェーンを通じた取組促進
- SC3中小企業対策強化WG
- 業界団体や各企業における取組の横展開

【参考】自動車業界における取組

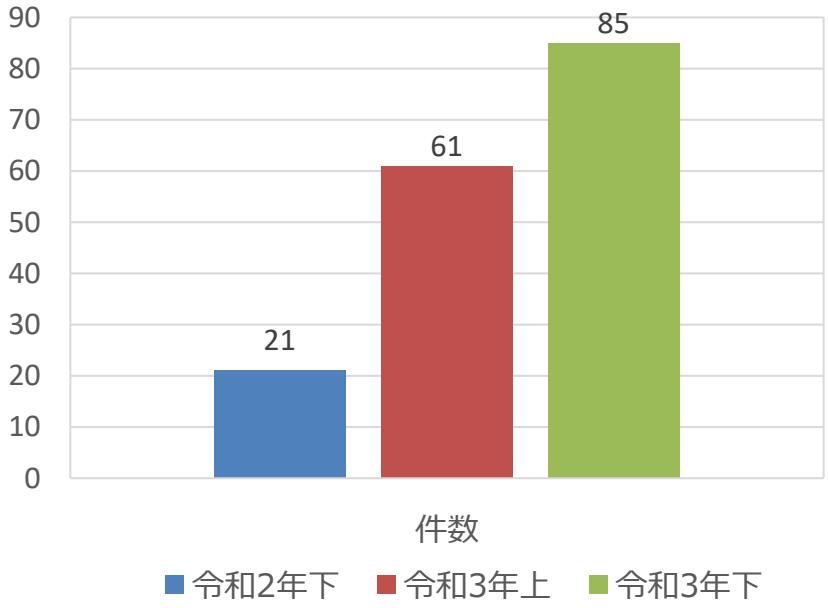
今後の取組
- 経済安全保障上重要となるサプライチェーン上の中小企業の対策強化
- 医療機関のサイバーセキュリティ対策強化
- ECサイトのセキュリティ強化

本パートの構成

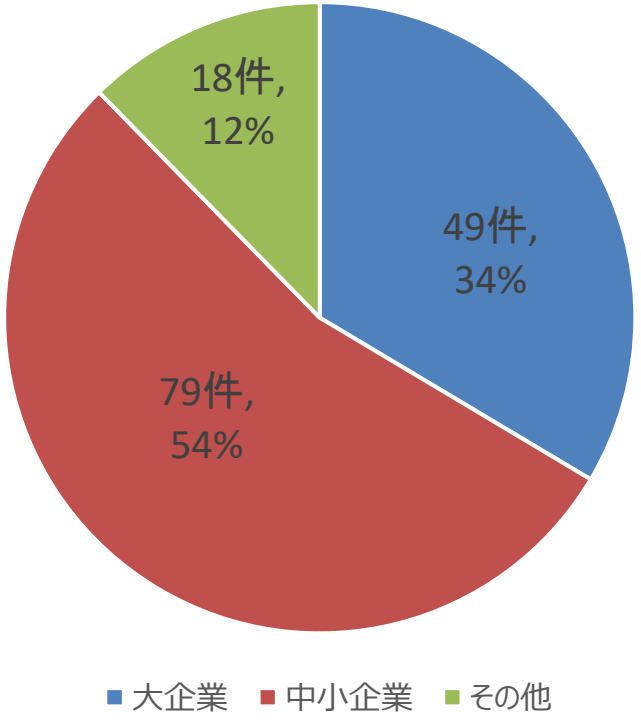
①中小企業におけるサイバー攻撃被害状況
②中小企業における対策状況、大企業・中堅企業等からの要請状況
③既存の政策ツールとその認知度
④各企業における取組にあたっての課題
⑤業界団体や企業における支援事例（プラクティス）
⑥今後の取組の方向性
（参考）諸外国における中小企業サイバーセキュリティ関連政策例

中小企業のランサムウェア被害の増加

- 企業・団体等におけるランサムウェア被害として、令和3年に全国の都道府県警察から警察庁に報告があった件数は146件であり、前年と比較可能な**７～12月だけで４倍と大幅に増加**。
- 被害件数(146件)の内訳は、大企業が49件（34%）に対して、**中小企業は79件（54%）と過半数超**。



企業・団体等におけるランサムウェア被害の報告件数の推移



ランサムウェア被害の被害企業・団体等の規模別報告件数（令和３年）

警察庁「令和３年におけるサイバー空間をめぐる脅威の情勢等について（令和4年2月10日）」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf

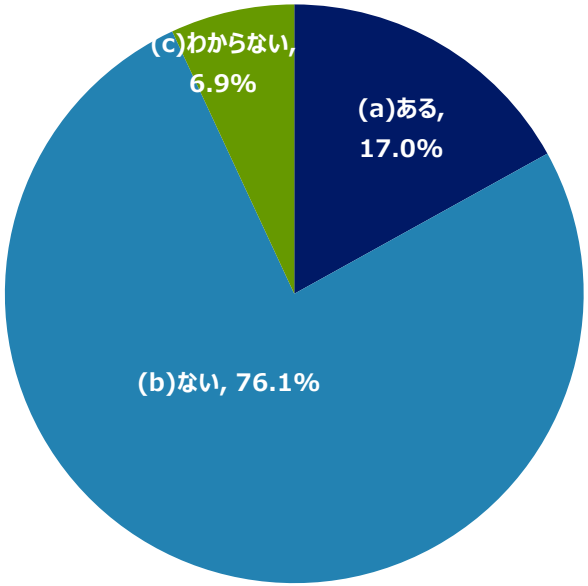
取引先等を経由した大企業・中堅企業のサイバー攻撃被害

- **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調査（※）。
- 結果、**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

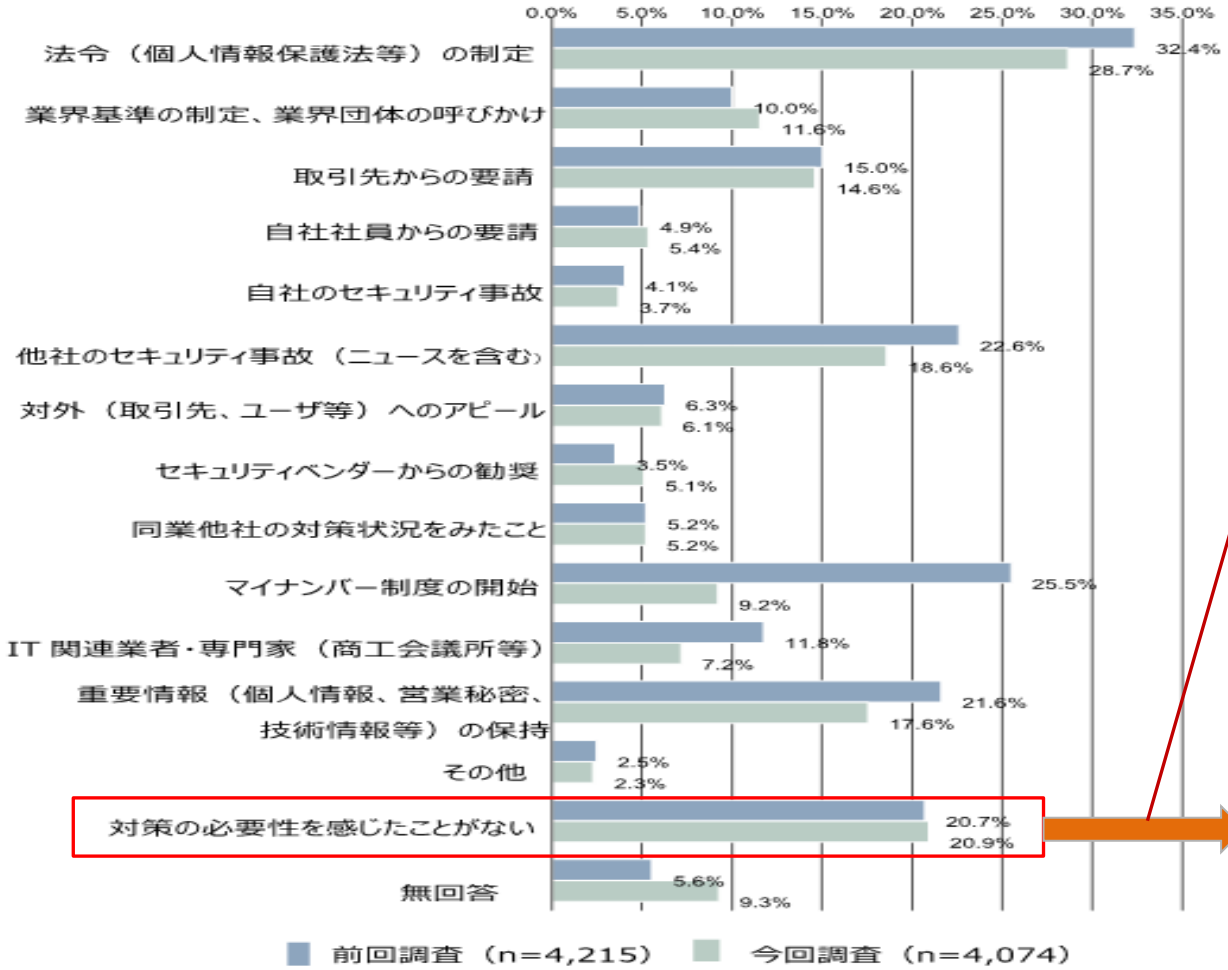
Emotet	● 取引先等がEmotetに感染し、不正なメールを受信
ランサムウェア	● 取引先等がランサムウェアに感染し、自社関連情報が暗号化／外部漏洩 ● 取引先等がランサムウェアに感染、業務停止し、自社業務に影響
不正アクセス	● 取引先等のシステムが不正アクセスをうけ、自社関連の情報が漏洩 ● グループ会社がVPNの脆弱性をついた不正アクセスによりネットワーク侵害をうけ情報が漏洩
ビジネスメール詐欺	● 取引先等がマルウェアに感染し、取引先を装い金銭を要求する詐欺メールを受信
DDoS攻撃	● 委託先のシステムや利用するクラウドサービスがDDoS攻撃を受け、自社業務に影響
その他	● 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）

中小企業のセキュリティ対策意識

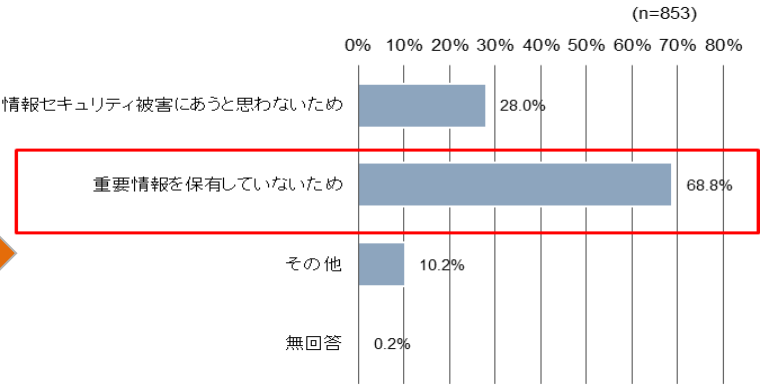
- IPAにおいて、全国の中小企業を対象とし、WEBアンケートを実施。有効回答数4,074（※）。
- 情報セキュリティ対策について、**「対策の必要性を感じていない」**企業が約２割(853社)で**2016年度の前回調査から変化がない。**また、その必要性を感じていない理由が**「重要情報を保持していないため」**と回答した企業が68.8%と多数。**中小企業のセキュリティ対策意識は依然として低い。**

情報セキュリティ対策の必要性を感じたきっかけについて教えてください(複数回答可)



「対策の必要性を感じたことがない」（20.9%）

情報セキュリティ対策の必要性を感じない理由について教えてください（複数回答可）【2021年度調査】



（※）独立行政法人情報処理推進機構（IPA）「2021年度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」

中小企業のセキュリティ対策状況

- 被害防止のための組織面・運用面におけるセキュリティ対策の取組状況の設問に対し、実施しているセキュリティ対策として、一番多いのは、「**重要なシステム・データのバックアップ**」である。次いで、「**セキュリティ対策を特に実施していない**」が**3割（1,224社）**にも上る。
- **中小企業のセキュリティ対策の取組をどのように促進するか課題。**

情報セキュリティ関連の被害を防止するためにどのような組織面・運用面の対策を実施していますか（複数回答可）

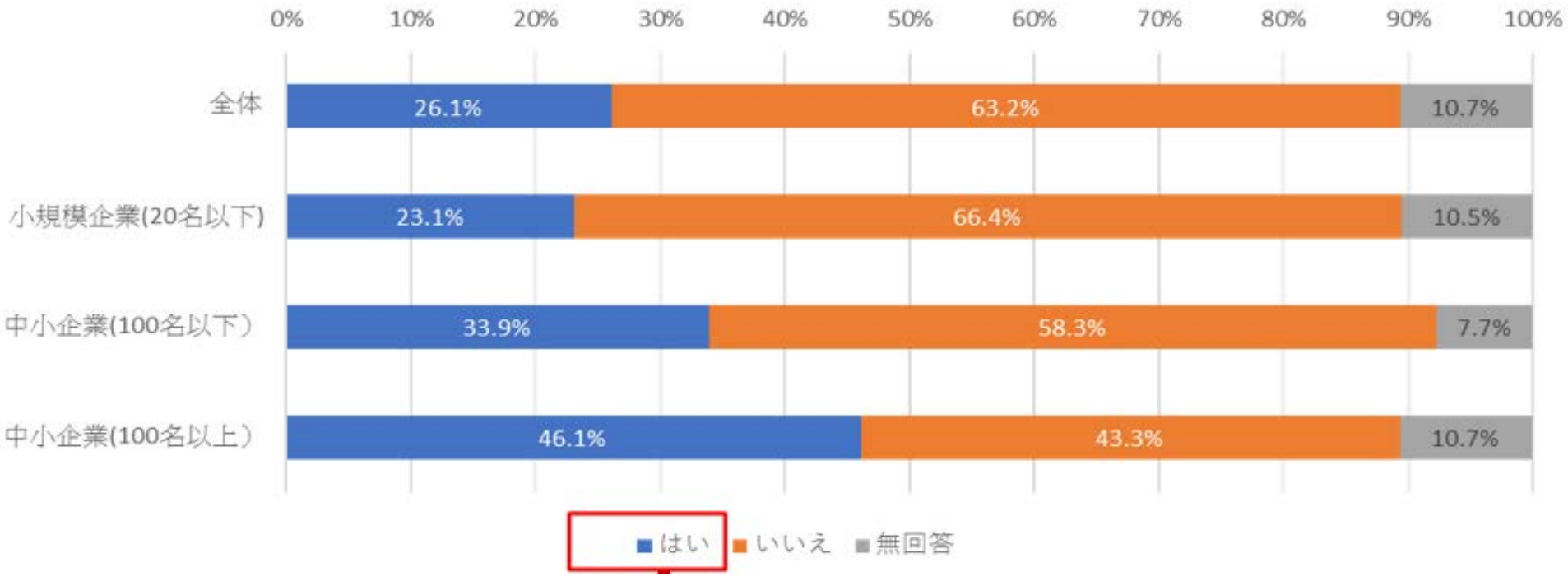
対策順	割合	前回調査（2016年度） n=4,215	今回調査（2021年度） n=4,074	割合	対策順
1	38.2%	重要なシステム・データのバックアップ	重要なシステム・データのバックアップ	37.5%	1
2	34.6%	セキュリティ対策を特に実施していない	セキュリティ対策を特に実施していない	30.0%	2
3	24.1%	情報（書類などの紙媒体）の施錠管理	一般ユーザーアカウントの管理ルールの策定（パスワード設定等）	28.2%	3
4	21.9%	ハードディスク等廃棄時の破砕/溶解	ハードディスク等廃棄時の破砕/溶解	27.2%	4
5	21.7%	一般ユーザーアカウントの管理ルールの策定（パスワード設定等）	情報（書類などの紙媒体）の施錠管理	25.7%	5

独立行政法人情報処理推進機構（IPA）「2021年度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」

中小企業におけるセキュリティ対策要請状況

- 発注元企業から何らかの情報セキュリティ対策を要請されている中小企業は、全体で２割強であったが、**企業規模が大きい企業ほど発注元企業から要請を受けていた**(100名以上の中小企業は4割強）。
- 要請された情報セキュリティ対策の上位は、**秘密保持(93.8%)、契約終了時の情報破棄(36.3%)、違反した場合の措置(32.4%)**であった。
- **セキュリティ対策費用**は、発注元企業が一部または全額費用負担しているケースは**5.1%**であり、**45.0%は中業企業の全額自己負担**であった。
- **<u>発注元企業から中小企業に求めるセキュリティ対策レベルの整理が必要。</u>**

発注元企業、仕入先からの情報セキュリティに関する条項・取引上の義務・要請はありますか



独立行政法人情報処理推進機構（IPA）「2021年度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」

大企業・中堅企業が取引先等に要請するセキュリティ対策の現状

②対策状況

- 仕入・外注・委託先等の取引先に対する要求事項としては、**プライバシーマークやISMSなどの認証取得**、**報告や損害賠償などに関する契約での取決め**などの事例が見られた。また、**サイバーセキュリティお助け隊の利用推奨**や、**第三者が提供するアセスメントサービス**を利用し取引先のセキュリティリスク評価を行う事例なども見られた。
- 他方で、グループ会社へのセキュリティ要求・取決めについては、**グループ会社での共通ポリシーの適用**のほか、**教育サービスのグループ会社への提供**、**自社のIT基盤のグループ会社への展開**などの事例が見られた。

セキュリティの要求/取決めの内容（取組事例）

①仕入・外注・委託先等の取引先

分類	内容
セキュリティに関する既存の基準への適合や認証取得等	● 自社で定めるセキュリティ基準・チェックシート ● Pマーク、ISMS ● クラウドサービスセキュリティ管理策 ● SOC2/SOC3（監査法人によるセキュリティ等の内部統制に係る保証報告書）
インシデントが発生した場合の対応	● 契約にもとづき、報告、原因調査、再発防止を要請 ● 損害賠償について契約書等で規定
推奨セキュリティ設定の実施	● 以下の各種対策 ✓ ウイルス対策ソフトの導入/適時の更新、セキュリティパッチの適用、アクセス管理、端末画面のロック、暗号化通信、パスワードの定期的な再設定、記憶媒体の使用や持ち出しの制限 等 ● リスクに応じ、PCやVDI環境の貸与
特定のITシステムやセキュリティサービス利用	● 以下の各種対策 ✓ ウイルス対策ソフト、ファイル転送サービス、Web会議システム、クライアント運用管理ソフト 等 ● サイバーセキュリティお助け隊の利用勧奨
その他	● 第三者が提供するアセスメントサービスを利用し、取引先のセキュリティリスクを評価。

②グループ会社

分類	内容
セキュリティに関する既存の基準への適合や認証取得等	左記に加え、以下のような事例があった。 ● グループ共通のセキュリティガイドラインへの準拠 ● 米国NISTのセキュリティフレームワークへの準拠
インシデントが発生した場合の対応	● グループのインシデント対応規定等にもとづき、報告、原因調査、再発防止を要請
推奨セキュリティ設定の実施	左記に加え、以下のような事例があった。 ● Webフィルタリング ● グループ会社共有のポリシーの適用
特定のITシステムやセキュリティサービス利用	● 自社の情報教育サービスのグループ会社への提供
その他	● 自社の規程、基準、IT基盤、運用をグループ会社に展開

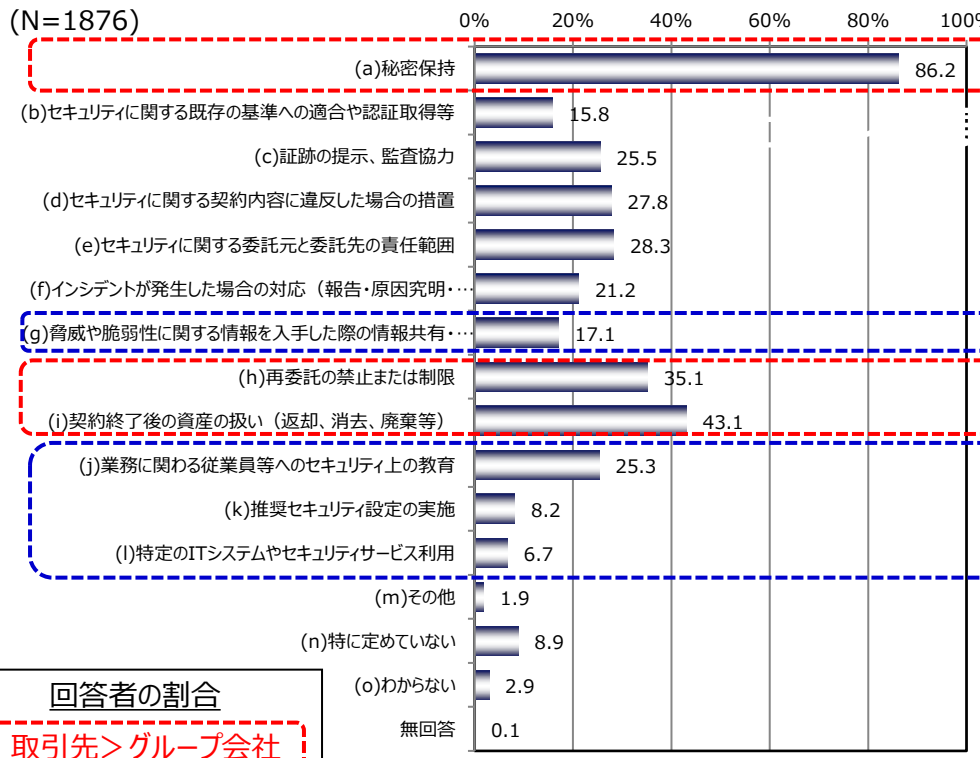
大企業・中堅企業が取引先等に要請するセキュリティ対策の現状

- 仕入・外注・委託先等の取引先に対する要求事項としては、**「秘密保持」、「契約終了後の資産の扱い」、「再委託の禁止または制限」**など**契約上の規定**に関する回答が多くあり、対グループ会社の回答割合と比べても大きい。
- 他方で、グループ会社へのセキュリティ要求・取り決めについては、「秘密保持」に次いで、**「業務に関わる従業員等へのセキュリティ上の教育」**との回答が多く見られたほか、**「脅威情報等の共有」、「推奨セキュリティ設定の実施」、「特定のITシステムやセキュリティサービス利用」等、細かな要請・支援が行われていることが分かった。**

セキュリティの要求/取決めの内容 ※複数選択（回答者の割合）

①仕入・外注・委託先等の取引先

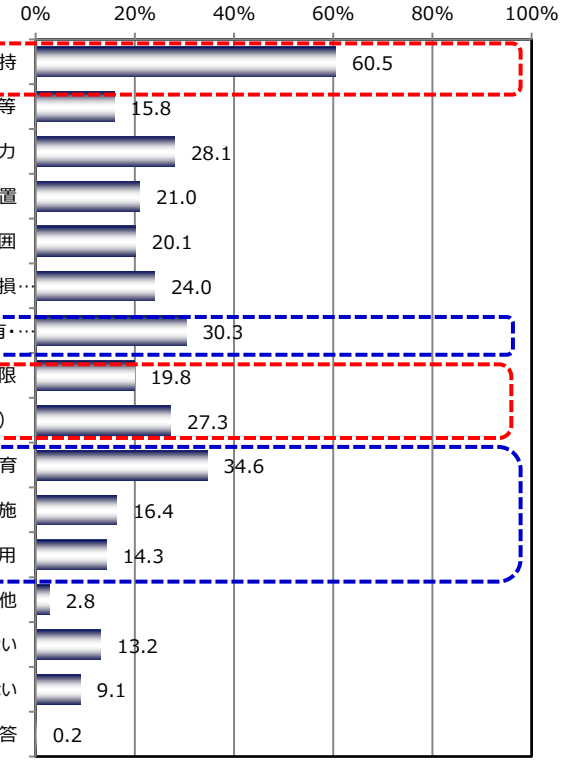
➢ 取引先等に対し、セキュリティに関してどのような要求事項または取決めを定めていますか※複数選択



※「仕入・外注・委託先等の取引先を有していない」回答先を除く

②グループ会社

➢ 取引先等に対し、セキュリティに関してどのような要求事項または取決めを定めていますか※複数選択



※「グループ会社を有していない」回答先を除く

回答者の割合
- 取引先＞グループ会社
- 取引先＜グループ会社

中小企業向けセキュリティ対策ツール

● 中小企業の情報セキュリティ対策ガイドライン（第3版 2019年3月）

–中小企業が情報セキュリティ対策に取り組む際の経営者が認識し実施すべき指針、社内において対策を実践する際の手順や手法をまとめたもの。

–第3版より、付録６として、クラウドサービスを安全に利用するための留意事項やチェック項目を記載した手引きを追加。

中小企業の情報セキュリティ対策ガイドライン

経営者向けの解説

経営者が認識すべき３原則と実施すべき重要７項目を解説

実践者向けの解説

企業のレベルに合わせて**段階的にステップアップ**できるような構成で解説

付録6:クラウドサービス安全利用の手引き

【クラウドサービス導入時の考慮ポイントの例】

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

● 「SECURITY　ACTION」

中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度。18万者を超える中小企業が宣言（2021年12月末）。

★一つ星

情報セキュリティ５か条に取り組む

★★二つ星

情報セキュリティ自社診断を実施し、基本方針を策定

● 「サイバーセキュリティお助け隊サービス」

相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など中小企業のサイバーセキュリティ対策に不可欠な各種サービス内容を要件としてまとめた基準を満たすワンパッケージサービス。（2022年３月時点で12サービス）

サイバーセキュリティ お助け隊

【参考】サイバーセキュリティお助け隊サービス

- 2019年度・2020年度実証事業で得られた知見に基づき、実証参加事業者がサービスを開発。
- サービス普及に向け、2021年度よりサービスブランドを設立。2022年３月時点で12サービスが登録。サービス審査登録制度の運営とともに、中小企業の意識啓発・サプライチェーンによる普及などの施策と一体となった普及施策の展開。

中小企業のサイバーセキュリティ対策に不可欠な各種サービス

- EDR・UTMによる異常監視
- 緊急時の対応支援・駆け付けサービス
- 相談窓口
- 簡易サイバー保険
- 簡単な導入・運用

中小企業でも導入・維持できる価格でワンパッケージで提供

サイバーセキュリティお助け隊サービスウェブページ（11/10公開）
＜https://www.ipa.go.jp/security/otasuketai-pr/＞

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

お助け隊サービスA
お助け隊サービスB
お助け隊サービスC

サービス提供

中小企業

自社の信頼性をアピール

取引先（大企業等）

お助け隊サービス利用の推奨等の中小企業の取組支援

サイバーセキュリティお助け隊

SC3(サプライチェーン・サイバーセキュリティ・コンソーシアム)

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

【参考】サイバーセキュリティお助け隊サービス　登録サービスリスト

③既存施策

- 全国各地域の中小企業にとって選択・利用可能な「サイバーセキュリティお助け隊サービス」登録サービスリスト
（第１回審査：5件、第２回審査：４件、第３回審査：３件）

【登録サービスリスト】

	サービス名	事業者名	対象地域
1	**商工会議所サイバーセキュリティお助け隊サービス**	大阪商工会議所	近畿（2府5県）全域、近畿に本社を置く中京圏都市部・福岡県北部の支社・工場、首都圏、長野県　等
2	**防検サイバー**	ＭＳ＆ＡＤインターリスク総研株式会社	全国
3	**PCセキュリティみまもりパック**	株式会社ＰＦＵ	全国
4	**EDR運用監視サービス「ミハルとマモル」**	株式会社デジタルハーツ	全国
5	**SOMPO SHERIFF（標準プラン）**	ＳＯＭＰＯリスクマネジメント株式会社	全国
6	**ランサムガード**	株式会社アイティフォー	関東地方、中部地方、関西地方、九州地方、沖縄県
7	**オフィスSOCおうちSOC**	富士ソフト株式会社	東北地方（岩手）を中心　※全国展開を計画中
8	**セキュリティ見守りサービス「＆セキュリティ＋」**	株式会社BCC	全国
9	**CBM ネットワーク監視サービス**	中部事務機株式会社	岐阜県（飛騨地方除く）・愛知県（三河地方除く）
10	**中部電力ミライズ サイバー対策支援サービス**	中部電力ミライズ株式会社	愛知県・岐阜県・三重県・長野県・静岡県（富士川以西）
11	**ＣＳＰサイバーガード**	セントラル警備保障株式会社	東京・神奈川・千葉・埼玉　※順次全国に拡大予定
12	**PCお助けパック　PC定期侵害調査プラン**	沖電グローバルシステムズ株式会社	沖縄県を中心　※全国展開を計画中

【参考】「サイバーセキュリティお助け隊サービス基準」の概要

- 【コンセプト】中小企業に対するサイバー攻撃への対処として**不可欠なサービス**を**効果的**かつ**安価**に、**確実**に提供する。
- 第1回審査(2021年3月)において出た論点を踏まえ、第2回中小企業対策強化WGにおいて、基準改定や基準解釈の目安となるガイドの作成等の方針を議論。**2021年７月に「v1.1版」として公開**した基準の概要は以下のとおり。

主な要件	概要
相談窓口	お助け隊サービスの導入・運用に関するユーザーからの各種**相談を受け付ける窓口を一元的に設置／案内**
異常の監視の仕組み	次のいずれかを含む異常監視サービスを提供すること ・ユーザーのネットワークを24時間見守り、攻撃を検知・通知する仕組み（UTM等のツールと異常監視サービスから構成）（**ネットワーク一括監視型**の場合） ・ユーザーの端末（PCやサーバ）を24時間見守り、攻撃を検知・通知する仕組み（EDR等のツールと異常監視サービスから構成）（**端末監視型**の場合）
緊急時の対応支援	ユーザーと合意したサービス規約等に基づき、ユーザーから要請された場合、ユーザーの指定する場所に**技術者を派遣することにより、緊急時の対応支援を行う**こと（リモートによる対応支援が可能な場合には、リモートによる対応支援も可とする。）
中小企業でも導入・運用できる簡単さ	IT・セキュリティの**専門知識のないユーザーでも導入・運用できるような工夫**が凝らされていること
簡易サイバー保険	インシデント対応時に突発的に発生する各種コストを補償する**サイバー保険が付帯**されていること なお、当該保険は初動対応（駆付け支援等）の費用を補償するものであること
上記機能のワンパッケージ提供	原則として、これら機能をユーザーが個別に契約することなく**一元的に契約可能**であること （例外的に個別契約とする場合にも、ユーザーにおいて手続上の煩雑さを伴わないよう工夫が凝らされていること）
中小企業でも導入・維持できる価格等	**・ネットワーク一括監視型**の場合：**月額１万円以下**（税抜き） **・端末監視型**の場合：**端末１台あたり月額2,000円以下**（税抜き） これらの仕組みを合わせて提供する場合には、この和（**月額１万円に端末１台あたり月額2,000円を加えた価格（税抜き））に相当する価格を超えない価格**であること。端末1台から契約可能であること。 ・最低契約年数は２年以内 **・初期費用、契約年数等の契約にかかる条件をサービス規約等に記載するとともに、口頭又は書面によりユーザに分かりやすく説明**すること
中小企業向けセキュリティ事業の実績	お助け隊実証事業に参加していたこと又は類似のサービスを**中小企業向けに提供・運用した実績**があること
情報共有	お助け隊サービス事業者間の**情報共有（少なくともアラートの統計情報の提供）**に応じること
事業継続性	要員の確保、品質管理等の社内プロセス整備、企業としての安定した財政基盤、経理処理能力等
更新	**２年毎に更新審査**を受けること

中小企業向けセキュリティ対策ツールの認知度

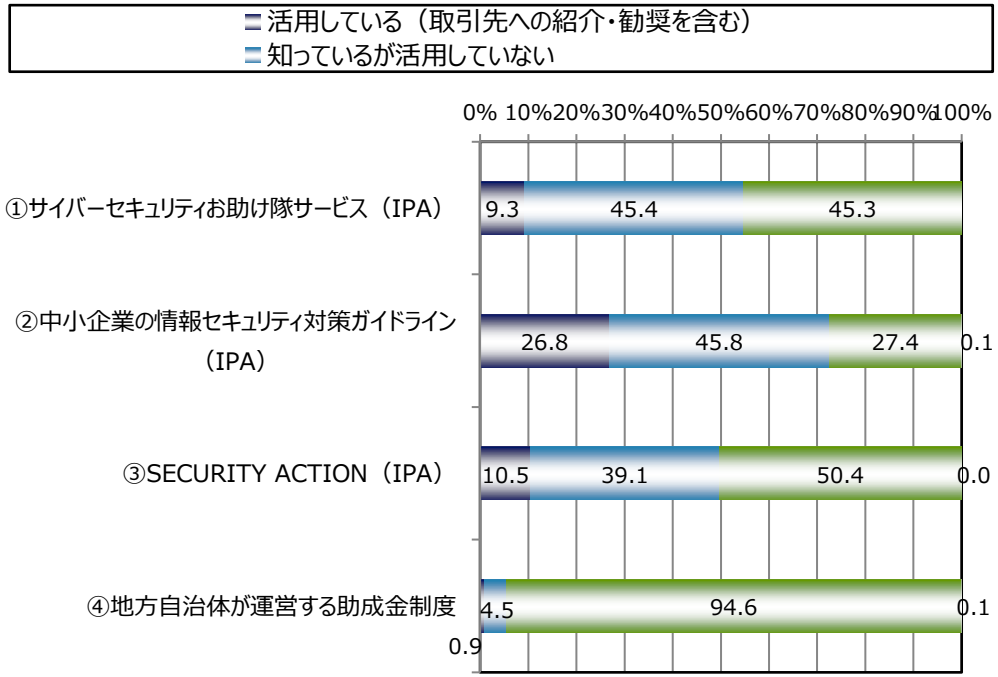
- 「SECURITY ACTION」を認識している中小企業は、全体の5.8%(235社）、「サイバーセキュリティお助け隊サービス」は、4.1%(165社）と**いずれも認知度は低く、「知っているものはない」が69.8%**（2,845社）であった。
- 発注元となる大企業・中堅企業では、「中小企業の情報セキュリティ対策ガイドライン（IPA）」の活用・認知は比較的進んでいる一方、**「SECURITY ACTION」「サイバーセキュリティお助け隊サービス」の活用・認知には課題**あり。

中小企業側

➢ IPAが実施する活動についてご存じのものをお答えください（複数回答可）

大企業・中堅企業側

➢ 下記①～④に挙げた国や自治体、関係機関による中小企業向けのサイバーセキュリティ対策支援活動の活用、認識状況について、あてはまるものをそれぞれお答えください



（左）独立行政法人情報処理推進機構（IPA）「2021年度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」
（右）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）

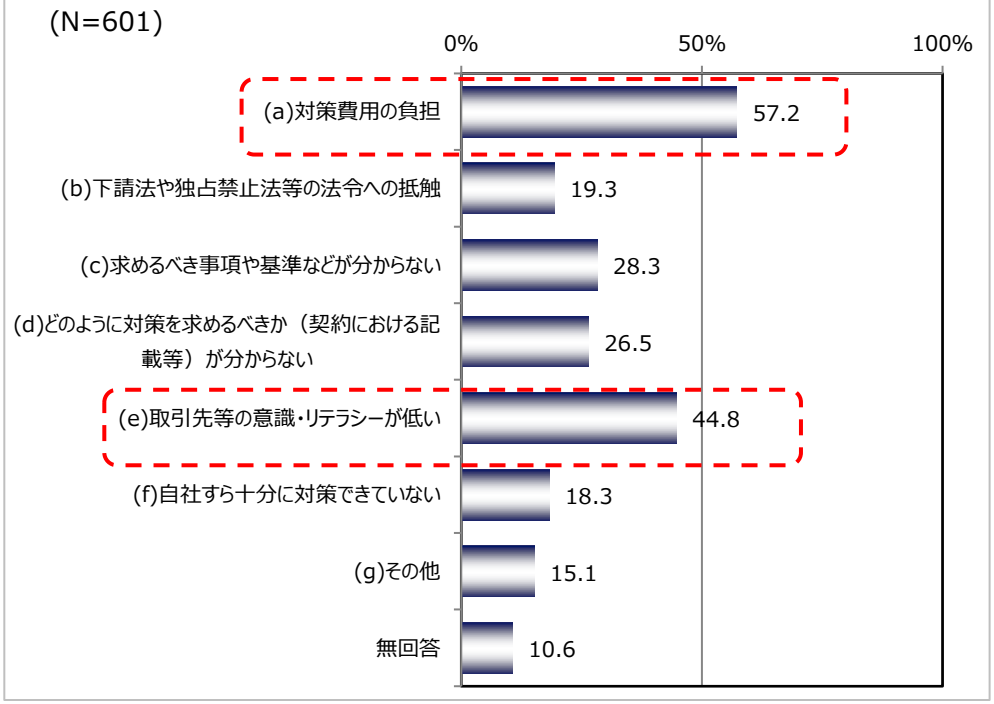
大企業・中堅企業から取引先等に対策を要請する際の課題

- 取引先等へ要請を行う上で**課題や足かせがあると回答した企業は約３割**にのぼった。
- 具体的な課題については、**対策費用の負担、取引先等の意識・リテラシーの低さ、求めるべき事項・基準や対策の求め方が不明であること、下請法や独占禁止法等の法令への抵触、自社すら対策できていないので要請できない**、等、いずれの選択肢についても一定数の企業が課題を有していた。また、取引先の業種や規模の違い、他社との関係性について課題と捉える企業もあった。

大企業等から取引先等へ要請を行ううえでの課題や足かせ

取引先等へ要請を行ううえでの課題や足かせの内容

➢ 取引先等に対して要請を行うにあたっての課題や足かせの内容として、当てはまるものを全てお選びください

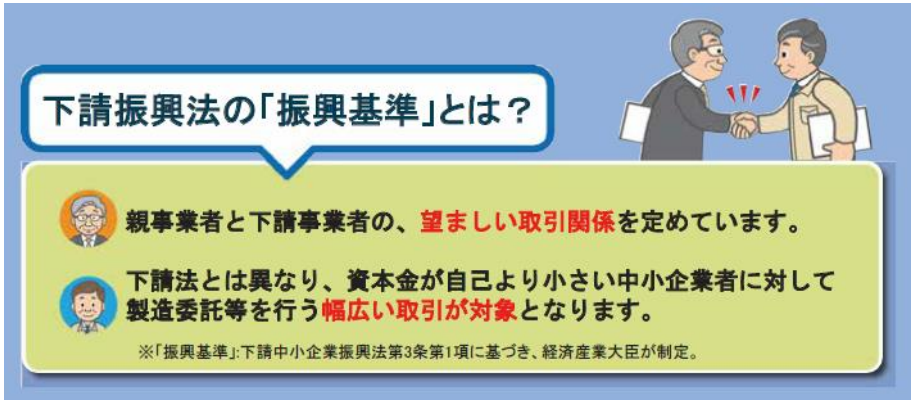


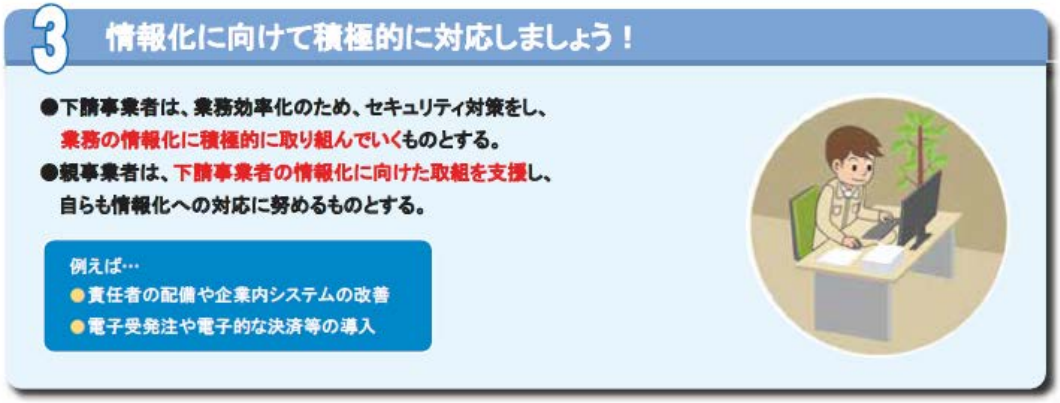
具体的な課題の内容

法令への抵触	● 下請法や独禁法（優越的地位の濫用）への抵触を懸念。（絶対にこれなら大丈夫というものでないと実施に踏み切れない。）
業種や規模の違い	● 業種が違う会社に要請に応えてもらうことが難しい ● 小規模事業者（個人事業主等）に高いレベルのセキュリティを要求しづらい ● 規模の小さい企業においては、PCスキルすら満足でないケースがあり依頼内容を理解してもらえない ● 重要性の高いシステムはペネトレーションテストを実施しているが少額の物品等の調達ではできない。企業の負担が大きいため何らかの認証制度が必要と考える。
他社との関係性	● 上下関係などにより、取引先相手への要請＋費用負担を要求しづらい（同業他社と比較して強い要請をすると、取引先が離れていくケースも懸念） ● 取引先ごとの関係性も各社様々で、取引先に対してどこまで求めることが出来るのかは簡単に判断できない ● 自社からの支援が他社など第三者の利益につながる可能性がある。

【参考】下請け中小企業振興法の振興基準

- 下請中小企業振興法の「振興基準」においても、 **下請事業者の要請に応じた、親事業者による下請事業者へのセキュリティ対策の助言・支援が推奨**されている。





【下請中小企業振興法　振興基準（令和３年７月）】

第３ 下請事業者の施設又は設備の導入、技術の向上及び事業の共同化に関する事項

５） 情報化への積極的対応

⑴ 下請事業者は、管理能力の向上、事務量軽減、事務の迅速化等の業務工程の見直しによる効率性の向上のため、必要なセキュリティ対策と併せて、次の事項に積極的に対応していくものとする。

① 情報化に係る責任者の配備及び企業内システムの改善（業務のデジタル化推進を含む）

② 中小企業共通ＥＤＩ（電子データ交換）などによる電子受発注

③ 電子的な決済等（インターネットバンキング、電子記録債権、全銀ＥＤＩシステムなどの活用）

⑵ 親事業者は、前号の下請事業者による取組の支援のため、下請事業者の要請に応じ、管理能力の向上についての指導、標準的なコンピュータやソフトウェア、データベースの提供、オペレータの研修、セキュリティ対策の助言・支援及び国・地方自治体による情報化支援策の情報提供等の協力を行うものとする。また、サプライチェーン全体の業務工程の見直しによる効率性向上を図る観点から、次号の配慮を行いつつ、電子受発注及び電子的な決済等の導入を積極的に働きかけていくとともに、自らも共通化された電子受発注又は電子的な決済等に係るシステムへの接続に努めるものとする。

https://www.chusho.meti.go.jp/keiei/torihiki/shinkoukijyun/zenbun.pdf

【参考】NISC「サイバーセキュリティ関係法令Q&Aハンドブックver1.0」(令和2年3月2日)におけるサプライチェーン・リスク対策に関する解説

- NISCのハンドブックでは、サプライチェーン・リスク対策を行う際の法律上の留意事項について以下のように解説している。

Q43 サプライチェーン・リスク対策

サプライチェーン・リスク対策を実施・推進するにあたり、ビジネスパートナーや委託先等 との関係において、どのような法律上の事項に留意すべきか。

１．概要

一定のサイバーセキュリティ対策を実施していることを取引の条件とすることや、一定 のサイバーセキュリティ対策を実施することを取引先に求めることは、社会全体のサイバーセキュリティ対策に資するものであり、原則として、我が国の何らかの法令に抵触するおそれはないが、優越的地位の濫用及び下請法に留意すべき場合もある。

（３）法律上の留意点について

不公正な取引方法（独占禁止法第 2 条第 9 項、第 19 条）のうち、①その 他の取引拒絶（一般指定42 項）、②拘束条件付取引（一般指定 12 項）、③優越的地位の濫用（独占禁止法第 2 条第 9 項第 5 号）、または④下請法に抵触しないかが問題となる。

ア その他の取引拒絶

検討：真にサプライチェーン・リスク対策を目的として、取引先に一定のサイバー セキュリティ対策を求め、当該対策ができない場合に取引を拒絶することは、独占禁止法上違法な行為の実効を確保するための手段として取引を拒絶しているとはいえず、また、「競争者を市場から排除する」といった目的を達成するためとはいえないことから、基本的には独占禁止法上問題となる場合は想定し難いといえる。

イ 拘束条件付取引

検討：取引先に一定のサイバーセキュリティ対策を求める場合、自社が当該対策を実施し得る代替的な取引先を容易に確保することができなくなる可能性はあっても、新規参入者や既存の競争者において代替的な取引先を容易に確保することができなくなることは想定し難いといえる。よって、取引先に一定のサイバーセキュリティ対策を求めることが不公正な取引方法に該当し、独占禁止法上問題となる場合は想定し難いといえる。

ウ 優越的地位の濫用

検討：自社が優越的な地位にある場合には、取引先に対して一定のサイバーセキュリティ対策を求めることが、正常な商慣習に照らして不当に、継続して取引する相手方に、自己の指定する事業者が供給する商品又は役務、つまり、当該取引に係る商品又は役務以外の商品又は役務を購入させること（独占禁止法第 2 条第 9 項第 5 号イ参照）に該当しないか、又は、一方的に、取引の条件を設定し、若しくは変更し、又は取引を実施する場合に、当該取引の相手方に正常な商慣習に照らして不当に不利益を与えること（同号ハ参照）に該当しないかという点に留意する必要があるといえる。

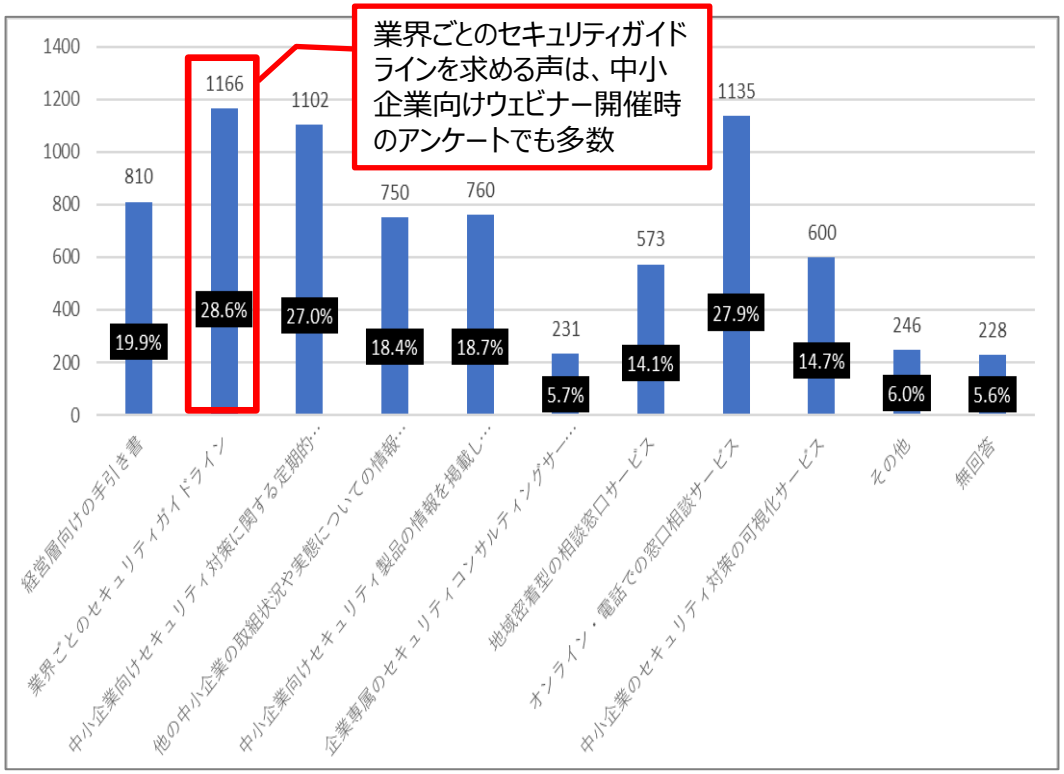
エ 下請法

検討：親事業者は、下請事業者に対して自己の指定するサイバーセキュリティ対策に関する物品の購入または役務の利用を強制する場合には、「下請事業者の給付の内容を均質にし、又はその改善を図るため」の必要があるか、またはその他正当な理由がないと、「購入・利用強制の禁止」（下請法第４条第 1 項第 6 号）に抵触し得るため、留意する必要があるといえる。

国等による取組・支援等に対する要望

- 中小企業に対するアンケートでは、どのようなセキュリティ対策に関するサービスがあれば活用したいかという問に対し、「**業界ごとのセキュリティガイドライン**」との回答が最も多く、**業界ガイドラインを活用することはセキュリティ対策を進める上で有効**であると考えられる。従業員100名以上の中小企業においては、「他の中小企業の取組状況や実態についての情報共有」を求める企業も多く、**他企業や他団体の取組状況や実態を情報共有することは参考となる可能性が高い。**
- 大企業・中堅企業に対するアンケートでも、**補助金の拡充やガイドラインの提供に関する要望**が多かった。

中小企業向け調査：どのようなセキュリティ対策に関するサービスがあれば活用したいですか(複数回答可)



大企業・中堅企業向け調査：サプライチェーンのセキュリティ向上のために国等に求める施策や取組

- **補助金の拡充**
- **ガイドラインの提供**
  - サプライチェーンのセキュリティ対策に関する企業規模別のガイドラインの官民での策定・遵守の仕組みの構築
    ※ 業界別ガイドラインは規模の小さい企業には向いていない、ガイドラインにより目標や投資の目安を明確化してほしいとの問題意識。
  - 非IT系中小企業向けのセキュリティガイドライン
  - テレワーク実施時におけるセキュリティ確保における企業・個人の費用負担についてのガイドライン
- **下請法・独禁法等の抵触が問題とならない要請方法に関する具体的な事例の提示**
- **強制力を伴う制度や政府調達への組入れ**
  （監査・報告、公共事業の入札での必須要件化等）
- **相談窓口・情報提供等の窓口の一元化**
- **ベースラインの達成を確認できる認証・監査制度**
- **セキュリティサービスを安価に利用可能とする仕組み等**

（左）独立行政法人情報処理推進機構（IPA）「2021年度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」
（右）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）

大企業・中堅企業における取引先等に対する支援事例

- 資本関係のない仕入・外注・委託先等に対しては、**「費用・備品の一部負担」、「教育の実施」**のほか、監査、アンケートを通じた**「対応状況確認」**が行われている。なお、グループ会社に対しては、上記に加え「稼働提供」や「設備の提供」といった支援が行われていることも明らかとなった。

取引先等に対するセキュリティの対策支援事例

分類	取引先への支援例	（参考）グループ会社への支援例
費用・備品の一部負担	● セキュリティ強化を目的としたIT環境の**整備費用の一部を負担** ● **協力会社同士で費用を分担** ● セキュリティ強化のための**備品を貸与** ● 脆弱性診断の費用と対応策の共有	● IT環境の整備費用の一部を負担 ● セキュリティ製品の**運用費用（SOC対応含め）について、本社での負担**
教育の実施	● セキュリティ教育 ● 着任時教育（e-Learning）	● セキュリティ教育資料の展開 ● グループ会社も対象にしたセキュリティ教育の本社主体での定期的な実施
脅威、脆弱性情報の共有		● 脅威、脆弱性情報の共有 ● 従業員等のセキュリティに関する注意喚起
稼働提供		● 共通で利用しているクラウドサービスにおける、必須・推奨に分けた設定の提示とサポートの実施 ● 新規案件に関する、本社からの情報セキュリティチェックの実施
設備の提供		● 従来から**本社が構築した環境を利用**させており、個社インフラは無い ● インフラ、セキュリティ環境の提供
対応状況の確認	● セキュリティ強化目的での**現地監査** ● **定期的なアンケート**調査 ● セキュリティ水準を確認するための当社**チェックシートによる実態調査**	

業界団体等におけるセキュリティ対策の取組事例

- **中小企業を含むサプライチェーンを構成する各業界団体(発注元となる大手企業）**において、**どのような情報セキュリティ対策・取組が採られており、どのような課題に直面しているのか、**IPAにおいてSC3中小企業対策強化WGと連携してヒアリング調査（※）を今年度実施（11業界団体）
- 下表のとおり、**業界団体におけるセキュリティ対策の取組の優良事例が**見られた。これらの中から、課題の解決につながる取組は、**業界団体のベストプラクティスとして業界横断で発信**することが考えられる。

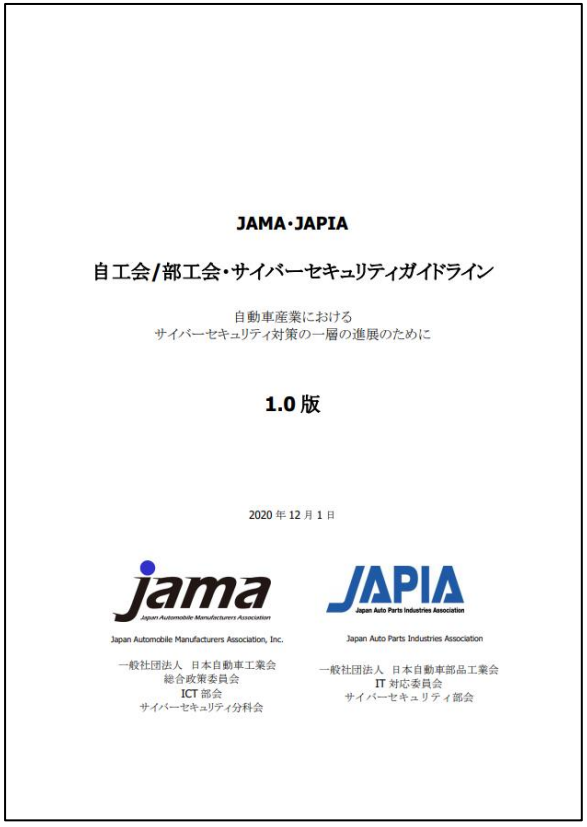
各業界におけるセキュリティ対策強化の取組

取組
業界でガイドラインを策定し、サプライチェーンを構成する取引先のセキュリティ対策状況のセルフチェックに活用。取引先からセルフチェック結果を回収し、結果を集計。
業界団体の中でWGを立ち上げ、**各種ガイドラインや対策推進に資するコンテンツ等を作成し、会員内で共有**。
情報セキュリティに関する勉強会や情報共有を実施
セキュリティ対策強化に向けた**訓練の場を提供**。例えば、インシデント発生時の報告訓練は中小規模の事業者も含めて実施。実践的な訓練としてはCSSCの演習に参加。
インシデントが発生した企業が対応に困っていればサポートをしたり、質問があれば対応したりする共助の取組もある。
業界団体として、**インシデント対応に関する統一的なガイドライン**を出している。
情報共有の際には、TLPを定めており、インシデント情報は企業名が特定できるような情報は伏せて共有している

（※）独立行政法人情報処理推進機構（IPA）「中小企業を含むサプライチェーンにおける情報セキュリティ対策状況等の調査」

【参考】自動車業界における取組

- 日本自動車工業会及び日本自動車部品工業会では、**自動車メーカーやサプライチェーンを構成する各社に求められる自動車産業固有のサイバーセキュリティリスクを考慮した対策フレームワークや業界共通の自己評価基準を明示**することで、自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進することを目的として、共同でセキュリティガイドライン(対策項目、基準)を策定。
- 自社のセキュリティ対策の取り組み状況をセルフ評価し、**対策レベルの効率的な点検を行うためのチェックシート**も作成。**これをサプライチェーンに展開し約2,300社の適正状況を集約**するとともに、**自社の取組状況を業界平均と比較し取組の優先順位付けに活用可能なツールを作成**して集計結果と共にフィードバックするなど、**業界全体でサプライヤーまで含めた対策の強化**を図っている。


JAMA・JAPIA

自工会/部工会・サイバーセキュリティガイドライン

自動車産業における
サイバーセキュリティ対策の一層の進展のために

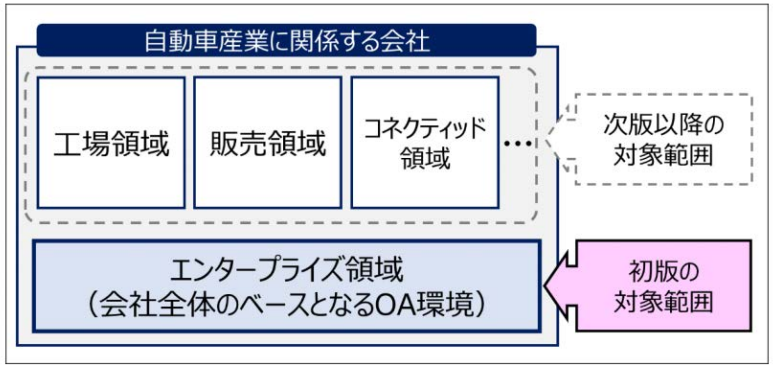
1.0 版

2020 年 12 月 1 日

jama
Japan Automobile Manufacturers Association, Inc.
一般社団法人 日本自動車工業会
総合政策委員会
ICT 部会
サイバーセキュリティ分科会

JAPIA
Japan Auto Parts Industries Association
一般社団法人 日本自動車部品工業会
IT 対応委員会
サイバーセキュリティ部会

【ガイドラインの概要】
- 2020年3月にv0.9を公表。その後のトライアルを踏まえ、2020年12月にv1.0を公表。
- 「経済産業省 サイバー・フィジカル・セキュリティ対策フレー ムワーク」を中核に、「NIST Cybersecurity Framework v1.1」、「ISO 27001」、「AIAG Cyber Security 3rd Party Information Security 1st Edition」、「IPA 中小企業の 情報セキュリティ対策ガイドライン」をベンチマークし作成。



＜図：自動車産業 CS ガイドライン初版の対象領域＞

https://www.jama.or.jp/it/cyb_sec/cyb_sec_guideline.html

調査を踏まえた現状の課題と今後の方向性

- 中小企業におけるセキュリティ対策を推進するために、中小企業の**ターゲットごとに既存制度を活用したアプローチ、SC3参加団体や業界の取組に沿った制度普及**を図る。
- いくつかの業界において既に策定されているガイドライン等を元に、共通的に求められる項目を抽出し、**業界ガイドラインの共通項としてとりまとめ、発信**するとともに、**業界横断でベストプラクティスの情報発信**を行う。

主な課題	
共通	SECURITY　ACTION制度、サイバーセキュリティお助け隊サービス等の**中小企業向けセキュリティ対策の認知度が低い**
中小企業	**セキュリティ対策を実施する意義**を感じていない
	セキュリティ対策に際し必要なサービスとして**「業界ごとのセキュリティガイドライン」がない**
発注元企業	**取引先にどこまでセキュリティを求めるか**、要件をどこまで契約書に盛り込むことが可能かわからない
業界団体	取引先にセキュリティ対策を要請する際、参考とすべきガイドラインが複数あり、**業界としてどれを参考にすべきかわからない**
	ガイドラインは策定しているものの、**ガイドラインをどのように業界内に普及、浸透**させていくかは課題
	取引先の立場としては、**似て非なる要求を受けるのが実態**であり、**業界としてのセキュリティ対策を推進**することが望ましい
	インシデントに関する情報共有の枠組みはありながらも、共有情報が機密情報にあたる場合もあり、**共有内容やそのタイミング、方法が悩ましい**
	他業界におけるセキュリティ対策の取組内容などについてわからないところも多いので参考にしたい

中小企業セキュリティ意識啓発、制度の普及・認知度向上

・マーケティングのターゲット(規模・セキュリティに対する意識など）を明確にし、既存の制度を活用した活動
・SC3参加団体、業界取組、業界ガイドラインとの連動(商流に沿った展開など)
・各種インセンティブ施策との紐付け
・地域金融機関を通じた普及

業界ガイドラインの共通項の抽出、発信

業界ガイドライン等の「共通項」を抽出、発信することで、ガイドライン未整備の業界における参考・業界横断的な共通水準（ベース）として活用

業界横断的な情報発信

参考となる各業界における取組（プラクティス）を業界横断的に共有

SC3中小企業対策強化WGでのこれまでの取組

- **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**
- 取組内容：
  - 中小企業におけるセキュリティ対策の促進
  - サイバーセキュリティお助け隊サービス制度（お助け隊サービス基準、審査登録機関基準）
  - 中小企業が直面する悩み・課題・解決策・プラクティスの共有
  - 業界ごとのサプライチェーンサイバーセキュリティ対策取組の共有　など

中小企業対策強化WGの活動経緯

2020年12月9日　第１回中小企業対策強化WG
- WGで取り扱うべき議題や中小企業のサイバーセキュリティ対策の強化に不可欠な各種サービスを**ワンパッケージ**で**安価**に提供することをコンセプトとした「**サイバーセキュリティお助け隊サービス**」の方針について議論

2021年4月28日　第２回中小企業対策強化WG
- 第１回審査で判明した課題等を踏まえ、**サイバーセキュリティお助け隊サービス基準の見直し検討**、今年度取り組むべき課題等について議論（**議論加速化のためにWG内にタスクフォースの設置**を決定）

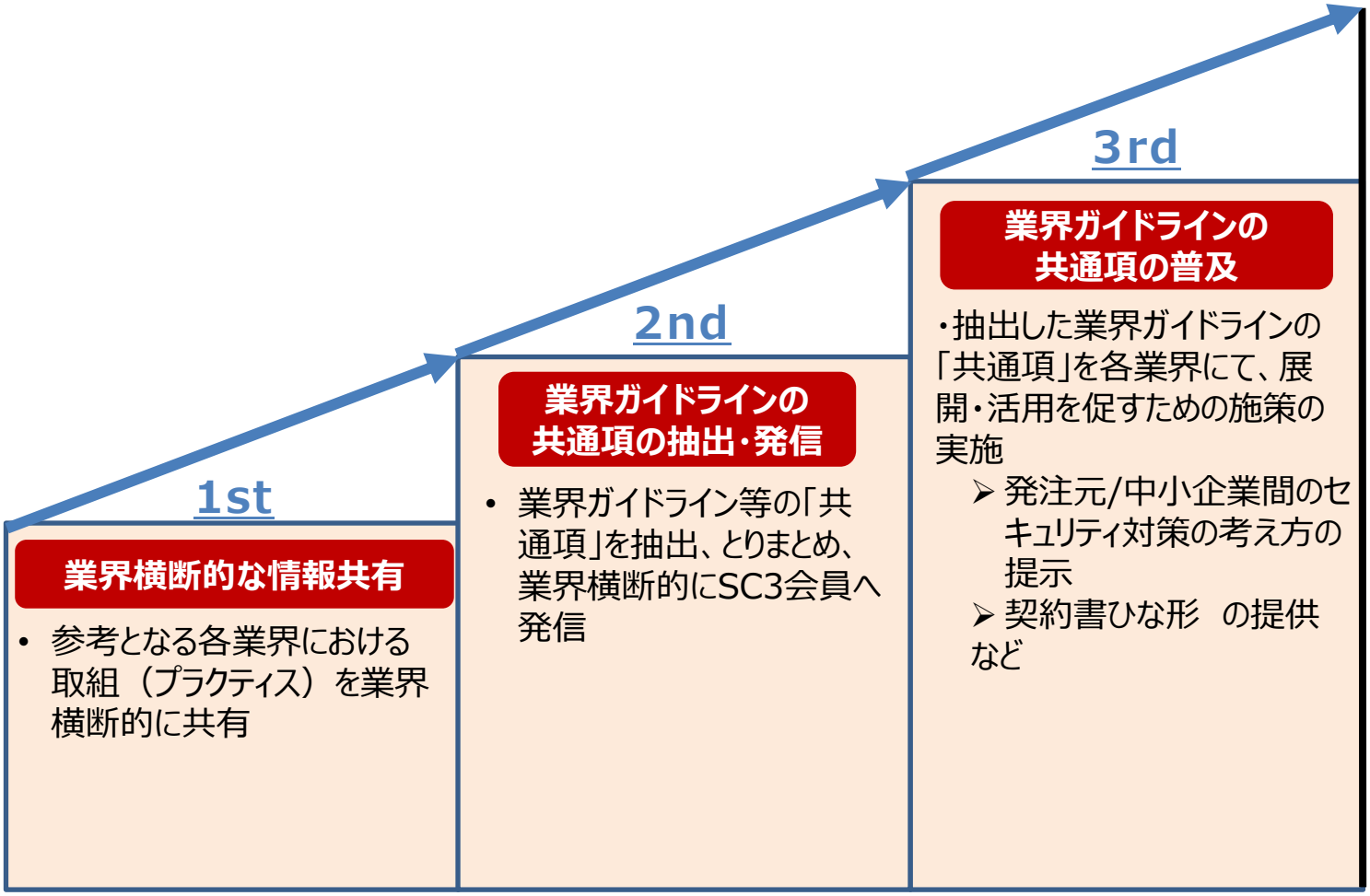
2021年6月30日　第３回中小企業対策強化WG(ウェビナー)
- **「中小企業のDX推進に伴うサイバーセキュリティ対策とお助け隊サービスの取組紹介」**ウェビナー開催

2021年10月19日　第４回中小企業対策強化WG
- **サイバーセキュリティお助け隊サービス基準**に関する諸論点の整理
- **令和3年度取組課題**等についてTFにおける検討結果を踏まえ議論

タスクフォース（TF）
メールベース・オンラインで継続議論

2022年３月１日　　第５回中小企業対策強化WG
- 中小企業のセキュリティ対策普及のため、**調査結果を踏まえた令和4年度取組**を議論

SC3における中小企業セキュリティ対策向上の今後の取組



制度の普及

- SC3参加団体、業界取組、業界ガイドラインとの連動(商流に沿った展開など)
- SC3でお助け隊サービスと合わせた普及

中小企業セキュリティ意識啓発、制度の認知度向上

- マーケティングのターゲット(規模・セキュリティに対する意識など）を明確にし、既存の基準、制度を活用した活動
- 関連制度の導入利点や問題点の整理し、それに基づいた認知向上策
- 補助金以外のインセンティブの提示

必要があれば調査を実施

地域金融機関を通じた中小企業サイバーセキュリティ対策普及

- 中小企業にとって身近な相談相手でもある**地域金融機関（地方銀行、第二地方銀行、信用金庫等）を通じて中小企業のサイバーセキュリティ対策を広める**ことにより、中小企業におけるサイバーセキュリティ対策の必要性にかかる認識を普及させ、ひいては中小企業を含むサプライチェーン全体のサイバーセキュリティ対策の底上げを図ることが期待される。
- よって、地域金融機関による中小企業向けサイバーセキュリティ対策の普及や必要な仕組みの検討材料とする目的のもと、**地域金融機関によって現状行われている関連取組、及び中小企業向けセキュリティ対策支援のニーズ等に関する調査を実施。**
- 同時に、**DX、サイバーセキュリティ対策にかかる中小企業向け施策のパンフレット、チラシ**を作成し、地域金融機関の協会会員行・信用金庫、商工会議所、商工会等にIPAから**一斉に送付（プッシュ型施策）。**

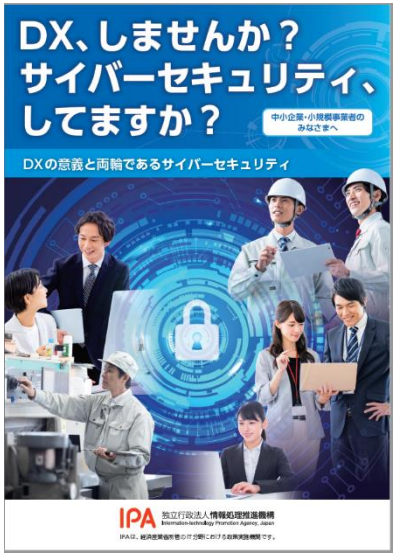
調査

- 地域金融機関による中小企業のリスクマネジメントやサイバーセキュリティ対策に関する既存の取組とその課題
- BCPの確保やDXの推進を含め地域金融機関が中小企業向けに取り組んでいる事業・施策、又は今後取組を進める予定の施策
- 地域金融機関によって現状行われている関連取組、及びそのニーズを含む必要性

中小企業向け施策パンフレット、チラシの作成、配布

中小企業向け施策（※）を記載したパンレット、チラシを作成し、地域金融機関団体の会員銀行、会員信用金庫へ発送。

（※）DX、サイバーセキュリティ、セキュリティ対策のための制度・ツール（サイバーセキュリティお助け隊サービス、SECURITY ACTION、中小企業の情報セキュリティ対策ガイドライン）、IT導入補助金等



【参考】各種インセンティブ施策との連携

- 各種補助金や税制措置等の施策とセキュリティ施策の連動により、幅広い層へのセキュリティ対策の普及を図る。

＜各種施策との連携例＞

IT導入補助金2022

- インボイス制度導入への対応も見据え会計ソフト、受発注システム、決済ソフト、ECソフト等のITツールの導入を補助。
- これまでに続き、**SECURITY ACTION一つ星または二つ星のいずれかの宣言を申請要件**に。
- メインツールとの組み合わせで補助対象となる「オプション」として「セキュリティ」も位置づけ。

ものづくり・商業・サービス補助金(デジタル枠)

- DXに資する革新的な製品・サービスの開発や、デジタル技術を活用した生産プロセス・サービス提供方法の改善等を行う事業者の設備投資等を支援する新たな申請類型。
- **SECURITY ACTION一つ星または二つ星のいずれかの宣言を申請要件**に。

事業継続力強化計画認定制度

- 中小企業が策定した防災・減災の事前対策に関する計画を、経済産業大臣が「事業継続力強化計画」として認定する制度。
- 認定を受けた中小企業は、税制措置、金融支援、補助金の加点などの支援策を受けられる。
- 自然災害リスクのほか、**サイバー攻撃**、感染症その他自然災害以外のリスクも支援対象に。

経済安全保障上重要なサプライチェーン上の中小企業、医療機関等のサイバーセキュリティ対策

- 経済安全保障の重要性の高まりや医療機関におけるサイバー攻撃被害を踏まえ、**経済安全保障上重要となるサプライチェーン上の中小企業、サイバーセキュリティ基本法上の重要インフラである中小医療機関等における対策強化が急務**。
- ノウハウがない中小企業でも攻撃の検知・防御の仕組みを安価かつ効果的に導入できる**「サイバーセキュリティお助け隊」が、これらのセクターの対策強化にも貢献する可能性**は高い。攻撃実態調査の活用や厚生労働省における調査事業との連携などにより、これらのセクターで取るべき対策を精査するとともに、お助け隊等の既存ツールの活用可能性などを検討していく。

経済安保上重要なサプライチェーン上の中小企業

経済安全保障上重要となるサプライチェーン上の中小企業については、高いセキュリティレベルが求められることや、高度な攻撃にさらされている可能性があることなどを踏まえ、令和４年度の調査事業において、これら企業への攻撃実態調査を実施。特定の企業におけるネットワーク・端末を監視することで、

- ✓ サイバー攻撃の数
- ✓ 攻撃手法（侵入深度・経路分析）
- ✓ 被害想定額
- ✓ どの時点で、どのツール・手法で攻撃を検知・防御できるか（お助け隊活用・オプションの検討）

などを調査する。

判明した攻撃実態を踏まえ、**これらのセクターで取るべき対策を精査するとともに、お助け隊や既存のガイドライン等の活用可能性や、追加すべきオプションや対策事項について検討**していく。

医療機関等のサイバーセキュリティ対策

厚生労働省において、医療機関における外部ネットワーク接続の拡大や、国内の医療機関を標的にしたサイバー攻撃の増加を踏まえ、医療機関等におけるサイバーセキュリティ対策のあり方に関する調査研究を実施。

本調査研究事業では、

- ✓ 国内外における医療情報セキュリティ動向調査
- ✓ 医療情報システムのクラウド化における現状調査
- ✓ よりわかりやすいチェックリストの提案
- ✓ 有効なモデルセキュリティポリシー案の策定
- ✓ **医療機関における「サイバーセキュリティお助け隊」の活用可能性・追加すべきオプション等の検討**

を実施予定。

医療機関の規模やネットワーク構成等により、お助け隊をそのまま活用できるもの、特殊事情に合わせたオプションを必要とするものなどが存在する可能性。これらを**厚生労働省と連携し精査・検討していく**。

ECサイトのセキュリティ脆弱性調査（令和3年度補正事業）

- **コロナ禍でECサイトの利活用が急増**しているが、脆弱性に気づかないまま運営されているECサイトにおいて、**サイトの改ざん**、**個人情報やクレジットカード番号等の流出などの被害が急増**。被害後は、**ECサイトの停止**に追い込まれ、さらには、一般消費者保護の観点からも対策が急務。

調査概要

- 既に被害に遭っている企業に対し、被害原因や被害後の対応をヒアリング調査を行い、特に留意すべき点を整理。
- また、中小企業のECサイト運営事業者に対し、ECサイトの管理状況（例：アップデート、脆弱性対応、アクセス管理の実施状況、ECサイト構築・保守ベンダーとの契約状況等）のセルフチェック及び専門家によるヒアリングを実施。
- 更に、被害企業へのヒアリングでは今後サイバー攻撃に悪用されるおそれのある潜在的な脆弱性の存在を明らかにするには不十分であることから、専門事業者による脆弱性診断（Webアプリケーション診断、ネットワーク診断）を実施することで、潜在的な脆弱性とその対応状況の傾向を分析し、見落とされがちなポイントや必要な対策を明らかにする。

成果イメージ

- 契約の実態を把握し、ECサイトの運営者となる中小企業に対し、ベンダーと契約する際の留意事項を示し、適切な関係が図られるようにする。
- ECサイトのネットワーク、WEBアプリケーションについて、どういったところに脆弱性があるか傾向を把握することで、確認のポイントや実施すべき対策を整理し、サイト構築時及び運営時における中小企業（運営者）及びベンダー（構築者）が留意すべき事項をまとめたガイドラインを策定する。

【参考】諸外国における中小企業向けサイバーセキュリティ政策の例(1/2)

- 中小企業向けのガイドライン等は数多く策定されている。自己診断を中心とした認証制度や、中小企業を支援するプロジェクトへの助成などが行われている国もある。

米国			
ガイドライン	CYBER ESSENTIALS	DHS/CISA	中小企業や地方自治体機関のリーダーが、組織のサイバーセキュリティの実践をどこから始めればよいのかなどの理解を深めるためのガイド。NIST Cybersecurity Frameworkやその他基準との整合性も確保されている。
ガイドライン	Cybersecurity Resources Road Map（A Guide for Critical Infrastructure Small and Midsize Businesses)	DHS/CISA	4つの階層と各階層における2つの質問で構成され、重要インフラの中堅・中小企業が、自社のニーズに合った有用なサイバーセキュリティ・リソースを特定できるように設計されたロードマップ。
ガイドライン	10 Cyber Security Tips for Small Business	FCC	中小企業を保護するためのサイバーセキュリティに関する10の重要なヒントの解説。
ポータルサイト	SMALL BUSINESS CYBERSECURITY CORNER	NIST	スモールビジネス向けのサイバーセキュリティ情報提供ポータル。啓発動画などもあり。また、NIST CSFのクイック・スタート・ガイドも公表（2021年4月）。
助成	Cybersecurity for Small Business Pilot Program	SBA（中小企業庁）	州政府が多様な産業の新興小規模企業に対するトレーニング、カウンセリング、レメディエーション、その他小規模事業者向けのサイバーセキュリティサービスを提供するプロジェクトに最大100万ドル助成を行うことを発表(2022年1月)。
EU			
ガイドライン	Cybersecurity guide for SMEs - 12 steps to securing your business	ENISA	中小企業が自社のシステムとビジネスの安全性を高めるための、12の実践的なステップを紹介したガイド（2021年6月）。
ガイドライン	ETSI TR 103 787-1 Cybersecurity Standardization Essentials	ETSI	中小企業が規格やフレームワークを導入してサイバーセキュリティを確立するために、何から手をつければよいのか、必要な情報を提供するために、主要な5つのフレームワークを分析し、5つのステップに展開したガイド（2021年5月）。
認証制度	Cybersecurity Label	cyberwatching.eu	EUのHorizon2020から助成を受けたプロジェクト。ISO27001や22301の一部を参照したチェックリストを仕様した簡単なオンライン自己診断により、中小企業のサイバーセキュリティ対策レベルを評価。70%をクリアすると、認定ラベルが取得できる。EU Cybersecurity Act対応へ向けた理解も助ける。

【参考】諸外国における中小企業向けサイバーセキュリティ政策の例(2/2)

英国			
ガイドライン	Small Business Guide: Cyber Security	NCSC	中小企業向けのサイバー対策の5つポイント（バックアップ対策、マルウェア対策、スマートフォン対策、パスワード管理対策、フィッシング対策）を紹介したガイド（2018年公表、2020年10月改訂）。
認証制度	Cyber Essentials	NCSC	オンラインで質問に回答し監査を受けることで、最も一般的なサイバー攻撃からの幅広い保護レベルを証明する認証制度（有料）。脆弱性スキャンなどを含むCyber Essentials Plusもある。政府調達でのセキュリティ要件の適合証明に利用する事業者が多数。
豪州			
ガイドライン	Small Business Cyber Security Guide	ACSC	一般的なサイバーセキュリティの事故を防ぐために、中小企業でも導入できる簡単な対策について解説したガイド（最新版:2021年10月）。補助的な資料として、「Step-by-step guides」（PCの起動、特定アプリの起動や認証、マルウェア防御等の29の特定のテーマについて、具体的な設定方法等を示した初心者向けマニュアル）や「Quick wins guides」（サイバーセキュリティに影響を与える技術的な問題について、その概要をユーザーに伝えるためのガイド）が紹介されている。
ガイドライン	Essential Eight	ACSC	サイバーセキュリティリスクと脅威緩和のための８つの基本的な対策を示したもの。企業はそれぞれの状況に応じて各項目の目標成熟度を設定し、対策を実施する。
診断ツール	Cyber Security Assessment Tool	Department of Industry, Science, Energy and Resources	オンライン上で質問に答えることにより、自社のサイバーセキュリティの成熟度を知ることができる自己診断ツール。
助成	Cyber Security Business Connect and Protect	同上	中小企業へのサイバーリスクの啓発や対策促進を支援するプロジェクトに対し、10～75万ドルの助成を行うもの。14件採択。（2021年）

【参考URL】
https://www.cisa.gov/cyber-essentials
https://www.cisa.gov/uscert/sites/default/files/c3vp/smb/DHS-SMB-Road-Map.pdf
https://www.fcc.gov/general/cybersecurity-small-business
https://www.nist.gov/itl/smallbusinesscyber
https://www.sba.gov/article/2022/jan/21/sba-administrator-guzman-announces-new-pilot-program-bolster-cybersecurity-infrastructure-emerging
https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes
https://www.etsi.org/deliver/etsi_tr/103700_103799/10378701/01.01.01_60/tr_10378701v010101p.pdf
https://label.cyberwatching.eu/Pages/Home.aspx
https://www.ncsc.gov.uk/collection/small-business-guide
https://www.ncsc.gov.uk/cyberessentials/overview
https://www.cyber.gov.au/acsc/view-all-content/publications/small-business-cyber-security-guide
https://www.cyber.gov.au/acsc/small-and-medium-businesses/cyber-security-assessment-tool
https://www.cyber.gov.au/acsc/view-all-content/essential-eight
https://www.grants.gov.au/Go/Show?GoUuid=2df49851-bc3b-beba-9601-4705b005e1e0

本日ご議論いただきたいポイント（中小）

- 中小企業のサイバーセキュリティ対策の促進に向け、主に以下の点について、ご意見等いただきたく存じます。

中小

- これまでのサプライチェーン・地域ベースの取組や実態調査結果踏まえた、今後取り組むべき中小企業関連政策の方向性
  - 取引関係における対策要請・支援の在り方
  - 地域金融機関等を通じた普及啓発の在り方
- 中小医療機関や経済安全保障上重要なサプライチェーン上の中小企業のサイバーセキュリティ等に対する取組の方向性

０．全体像

１．経営

２．中小企業

３．人材

４．地域

５．国際

６．本日議論いただきたい論点

人材施策の全体像

- 今年度は、「セキュリティ体制構築・人材確保の手引き」の改訂を行うとともに、セキュリティ人材育成の既存施策を進めつつ、特に、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。

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（案）

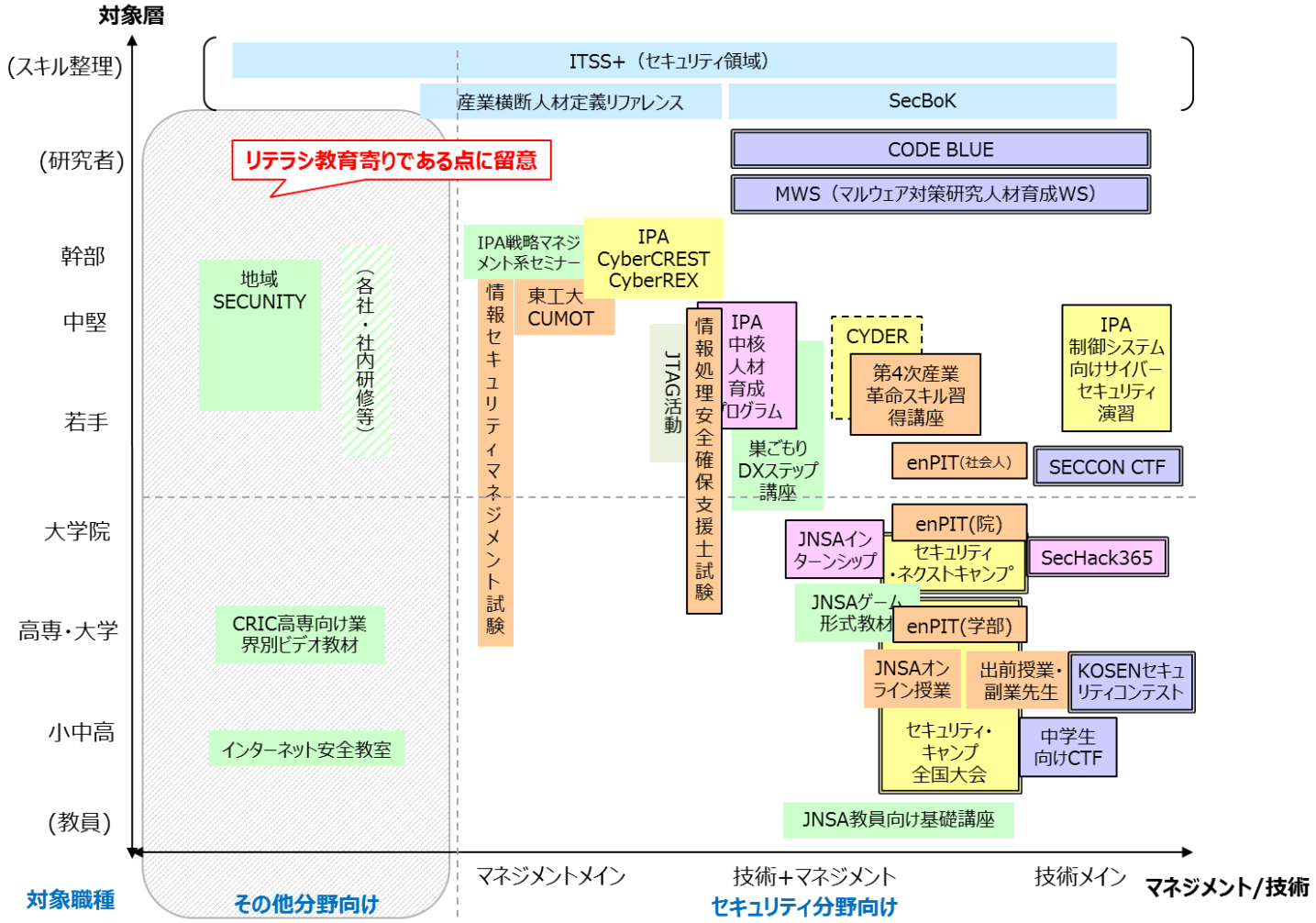
- 手引きの普及による各企業での体制構築の促進と各種セキュリティ人材育成施策を引き続き実施するとともに、プラス・セキュリティの取組を普及させるため、SC3産学官連携WG、デジタル人材育成プラットフォーム、各地域における産学官連携の取組（地域SECUNITY）との連携による取組の具体化・拡大を進めていく。

【参考】既存人材育成プログラムと対象のマッピングイメージ

- SC3産学官連携WGにおいて、国・関連機関による既存の取組を中心に位置づけを整理。今後、産業界のニーズとのギャップを明らかにしていく。

※国・団体による取組を中心に記載した暫定的なイメージ

※必ずしも上に向かうにつれレベルが上がるわけではないことに注意。



＜取組の種類＞
1.スキル整理
2.短期座学・教材
3.短期演習
4.講義・講座・資格
5.長期プログラム・インターン
6.コンテスト・専門家交流
7.その他

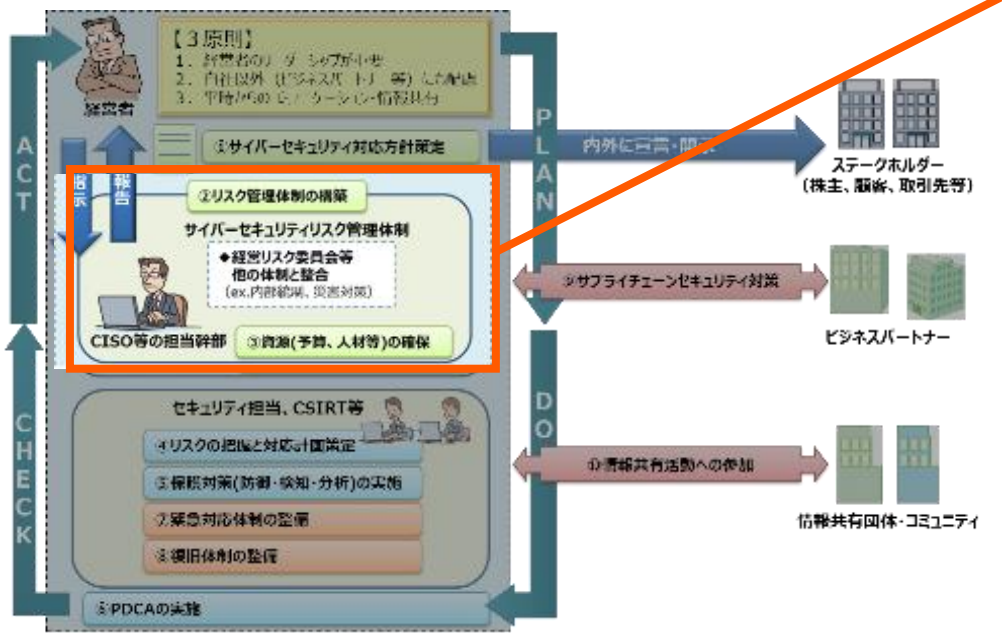
＜難易度(前提知識)＞
セキュリティ知識必要
IT基礎知識あると良し

サイバーセキュリティ体制構築・人材確保の手引きの改訂

累計25,159DL
※第1.0版、第1.1版の合計
（2021年11月末時点）

- 「サイバーセキュリティ経営ガイドライン」の付録Fとして2020年に公表した「サイバーセキュリティ体制構築・人材確保の手引きは、経営ガイドラインの指示２（リスク管理体制の構築）及び３（資源の確保）を具体的に行う際の参考文書として、**セキュリティ統括機能の構築方法、ITSS+（セキュリティ領域）の活用方法、「プラス・セキュリティ」等を解説。**
- 2021年度は、この手引きをより幅広い層にご利用いただくため、内容を簡素化し手引きの活用例を新たに追加。また、制御システム（OT）分野の体制構築等の内容を拡充。

サイバーセキュリティ経営ガイドライン（10の指示）



手引きの構成（指示2、3の深掘り）

指示２ サイバーセキュリティリスク管理体制の構築

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

指示３ サイバーセキュリティ対策のための資源確保

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

産業サイバーセキュリティセンター（ICSCoE）（2017年4月設置）

- 中核人材育成プログラムでは、電力、石油、ガス、化学、自動車、鉄道分野等の企業から受講者を受け入れ、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５期（2021年7月開講）には、48名が参加。修了者は産業サイバーセキュリティエキスパートとして業界内外のサイバーセキュリティの取組に貢献。
- また、短期プログラムとして、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向けのセミナーを実施。

中核人材育成プログラム

- 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

卒業プロジェクト（一例）

- **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、システムへの導入検証を実施。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。

- **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10事例を紹介。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」

- 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。

修了者の地域での活躍

- 修了者が卒業プロジェクトの延長としてフレームワーク推進活動を実施。地銀と連携し、中小企業を含めたサプライチェーンのセキュリティ強化に貢献。
- また、商工会議所の会報に地域・中小企業を対象としたセキュリティの取組促進の啓発記事（インシデント事例、SECURITY ACTION制度の紹介等）を執筆（札幌、名古屋、大阪）。地域での繋がりを持たせ、情報発信の場の支援を行う。

戦略マネジメント系セミナー（2018年～）

- 経営層を補佐し、実務者層・技術者層を指揮することでセキュリティ対策を進める戦略マネジメント層向けのセミナー。
- 組織全体のセキュリティレベル向上を目指し、セキュリティ対策を組織横断的に統括する体制及びその責任者の役割について理解を目指す。
- 2021年度は１～２月に対面・オンライン（ハイブリッド形式）で開講。講演・講義・グループディスカッションにより、先進事例・課題や解決策・ノウハウなどを体系的に学ぶプログラムを提供。

情報処理安全確保支援士（登録セキスペ）制度

- サイバーセキュリティの確保を支援するため、セキュリティに係る最新の知識・技能を備えた専門人材の国家資格として、「情報処理安全確保支援士」（通称：登録セキスペ）制度を平成２８年に創設。
- 令和３年１０月1日時点の登録者数は１９，４５０人。
- 令和２年５月より、**登録に３年間の有効期限**を設け、**更新が行われない場合**には、**登録が失効**する**更新制を導入**。

◆ 政府機関や企業等のサイバーセキュリティ対策を強化するため、専門人材を見える化し、活用できる環境を整備することが必要。

➡ **情報処理安全支援士の名称を有資格者に独占的に使用させることとし、さらに民間企業等が人材を活用できるよう登録簿を整備。**

◆ 技術進歩等が早いサイバーセキュリティ分野においては、知識等が陳腐化するおそれ。

➡ **有資格者の継続的な知識・技能の向上を図るため、講習の受講を義務化。**
※登録の更新制導入により、義務講習を受講したもののみ登録を更新。

◆ 民間企業等が安心して人材を活用できるようにするには、専門人材に厳格な秘密保持が確保されていることが必要。

➡ **業務上知り得た秘密の保持義務を措置。**

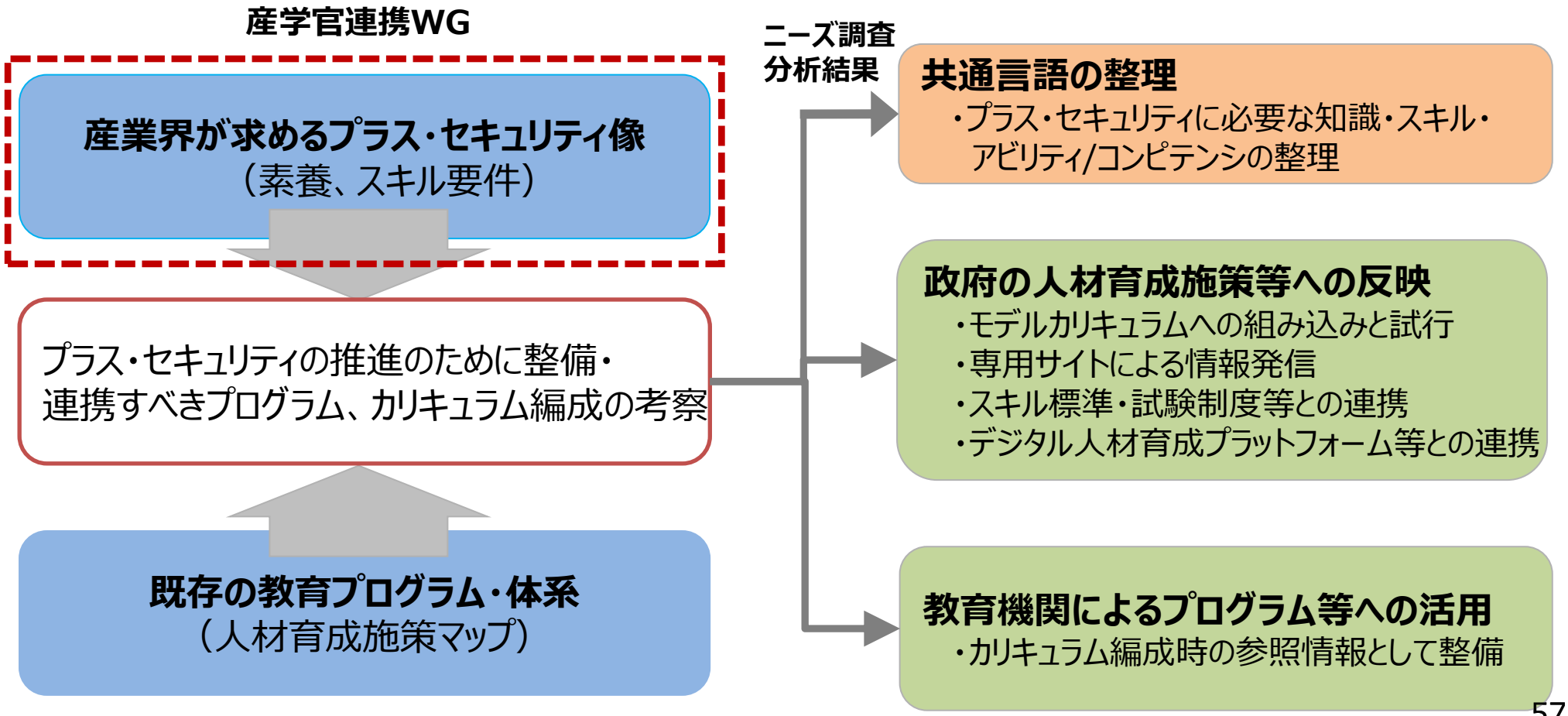
セキュリティ・キャンプの概要

- 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・生徒を対象として育成合宿（**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年の開始**からこれまでに、累計で**989名**（全国大会のみ）が修了。
- 昨年度に引き続き、今年度も**新型コロナウィルスの影響により**、従来の合宿形式に替え**オンライン形式**で実施。短期集中型の合宿形式に比べ、時間と場所の制約が少ないため、自分のペースで受講しやすいなど、利点も多い。

プラス・セキュリティの普及促進

- **プラス・セキュリティ＝（セキュリティが本務ではないが）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こと、あるいは身につけている状態のこと。**
- プラス・セキュリティの取組普及のため、SC3産学官連携WGにおいて必要なスキルの整理等が行われているほか、NISCにおいても「プラス・セキュリティ」のモデルカリキュラムの策定や官民のコンテンツのポータルサイトへの掲載などを実施中。デジタル人材育成プラットフォーム事業等の関連施策とも連携し、取組を普及させていく。

SC3産学官連携WGにおける「プラス・セキュリティ」の具体化



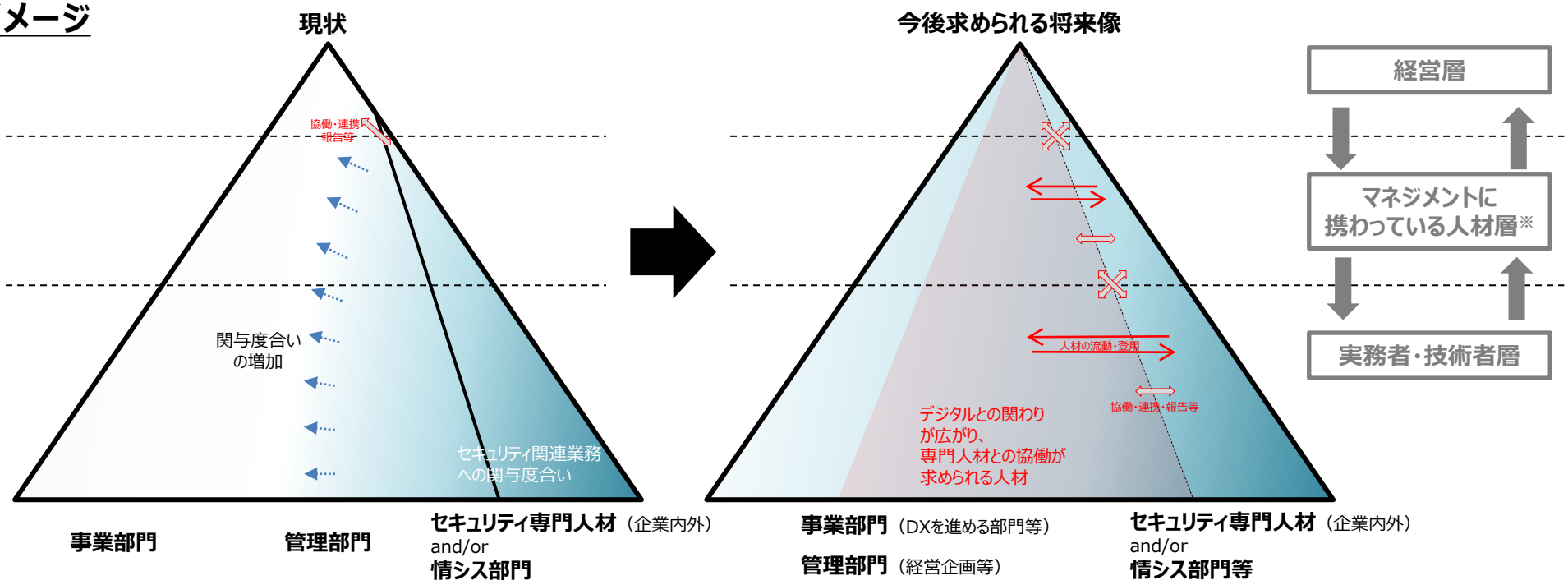
【参考】サイバーセキュリティ戦略におけるプラス・セキュリティの位置づけ

プラス・セキュリティ

- 経営層や、特に企業・組織内でDXを推進するマネジメントに関わる人材層をはじめとして、**ITやセキュリティに関する専門知識や業務経験を必ずしも有していない様々な人材に対して「プラス・セキュリティ」知識が補充され、内外のセキュリティ専門人材との協働等が円滑に行われることが、社会全体で「DX with Cybersecurity」を推進していく上で非常に重要**である。
- 需要に係る観点からは、「DX with Cybersecurity」に取り組む様々な企業・組織内において、これまで専門知識や業務経験を必ずしも有していない人材（経営層を含む）が、今後デジタル化に様々に関わるためにITリテラシーや**「プラス・セキュリティ」知識を補充しなければならない必要性は増しており**、潜在的な大きな需要が存在すると考えられる。

【サイバーセキュリティ戦略本文（令和3年9月28日閣議決定）より抜粋】

イメージ



- DX進展の中で、特にDXを進めている事業部門や経営企画部門等において、セキュリティ関連業務との関与が増加していく。
- 様々な人材層・部門において、専門人材との協働が求められる。（協働のためには、互いの領域への相互理解が前提となる。）

※ 経営戦略、事業戦略におけるサイバーセキュリティに関わるリスクを認識し、経営層の方針を踏まえた対策を立案し、実務者・技術者を指導できる人材を戦略マネジメント層と定義 「サイバーセキュリティ戦略」(2018年7月27日閣議決定より)

企業におけるプラス・セキュリティの実態調査

- セキュリティ運営の強化に取り組んでいる金融・サービス業、人材派遣業のIT/セキュリティ統括部門に、社内事業部門におけるプラス・セキュリティの位置づけと育成に向けた取組状況を調査。
- デジタル人材育成への組み込みやスキル・教育コンテンツの整備・体系化等のニーズを確認。

セキュリティ運営の強化に取り組んでいる企業のIT/セキュリティ統括部門へのヒアリング結果

分類	プラス・セキュリティの取組が比較的進んでいる企業	プラス・セキュリティはこれからの企業	現状・ニーズ（仮説）
必要性の認識	• **経営層と連携**して個人情報/内部情報取り扱い部門を中心に企画・試行段階	概念的に理解しているが、具体的な活動には至っていない	• 特定業種の経営層に必要性は理解されているものの、 • **認知度は低く、事業部門の理解・認識は低い**
スキル要件・知識の定義	• **特定部門向けセキュリティスキル底上げ**と、**全社員向けリテラシー教育**から着手 • ｴﾝｼﾞﾆｱ向けセキュリティバイデザイン教育		• 全社的なスキル要件の体系化・整備は行われていない • 取組が進む企業は、自社活用できる**外部コンテンツがなく、独自に教育プログラム・コンテンツを開発している**
教育プログラムの整備状況	• 全社推進者を外部専門会社から採用し、独自の実施計画を策定 • **DX関連部門のセキュリティ担当向け**演習を実施	プラス・セキュリティに特化したプログラムは未整備で実施していない	• **デジタル人材の育成とセットで、自社コンテンツを独自に開発している**が、特定部門での利用に留まる • **異動による人材流動化/ｷｬﾘｱﾊﾟｽ、人事評価は整理されていない** • セキュリティ人材をデジタル人材に配置転換する事例もある
人材確保・育成状況	• **社内人材のリスキル**が中心 • **IT/セキュリティ統括部門からの人事異動は行わず**、**DX関連等、特定部門**にて試験的に人材育成に着手	セキュリティ専門人材の育成に注力している	• 参考となる**先行企業が国内に見当たらず**、目安となる適切な要員数・スキル要件は定義されていない • 外部雇用・人事異動による補充はなく、**社員リスキルが中心となっている**
取組を進めるにあたり必要な施策（意見）	• 具体的なコンテンツ整備・育成計画を整備するための、**業界・企業規模に応じた目安となる指標の提示（スキル要件等）** • 組織・個人の役割・責任定義等、人事制度設計のための、**ガイドラインの整備** • 自社利用できる**業務内容に沿った教育コンテンツの整備・公開（DX、リスクマネジメントとの連動）** • **資格・試験制度**等との連携		

デジタル人材育成プラットフォームにおけるセキュリティの位置づけ

共通

- DXのために全てのビジネスパーソンが習得すべきリテラシーの中でセキュリティも位置づけ。また、DXを推進する立場の人材に必要な専門的なデジタル知識・能力の中でも、必要なセキュリティ知識・能力を位置づけることにより、プラス・セキュリティの取組を促進していく。

全てのビジネスパーソン

小・中・高等学校における**情報教育の内容**に加え、**ビジネスの現場でのデジタル技術の使い方の基礎**を学んだ人材

DX推進人材

DX推進のための組織変革に関する**マインドセットの理解・体得**が必要。

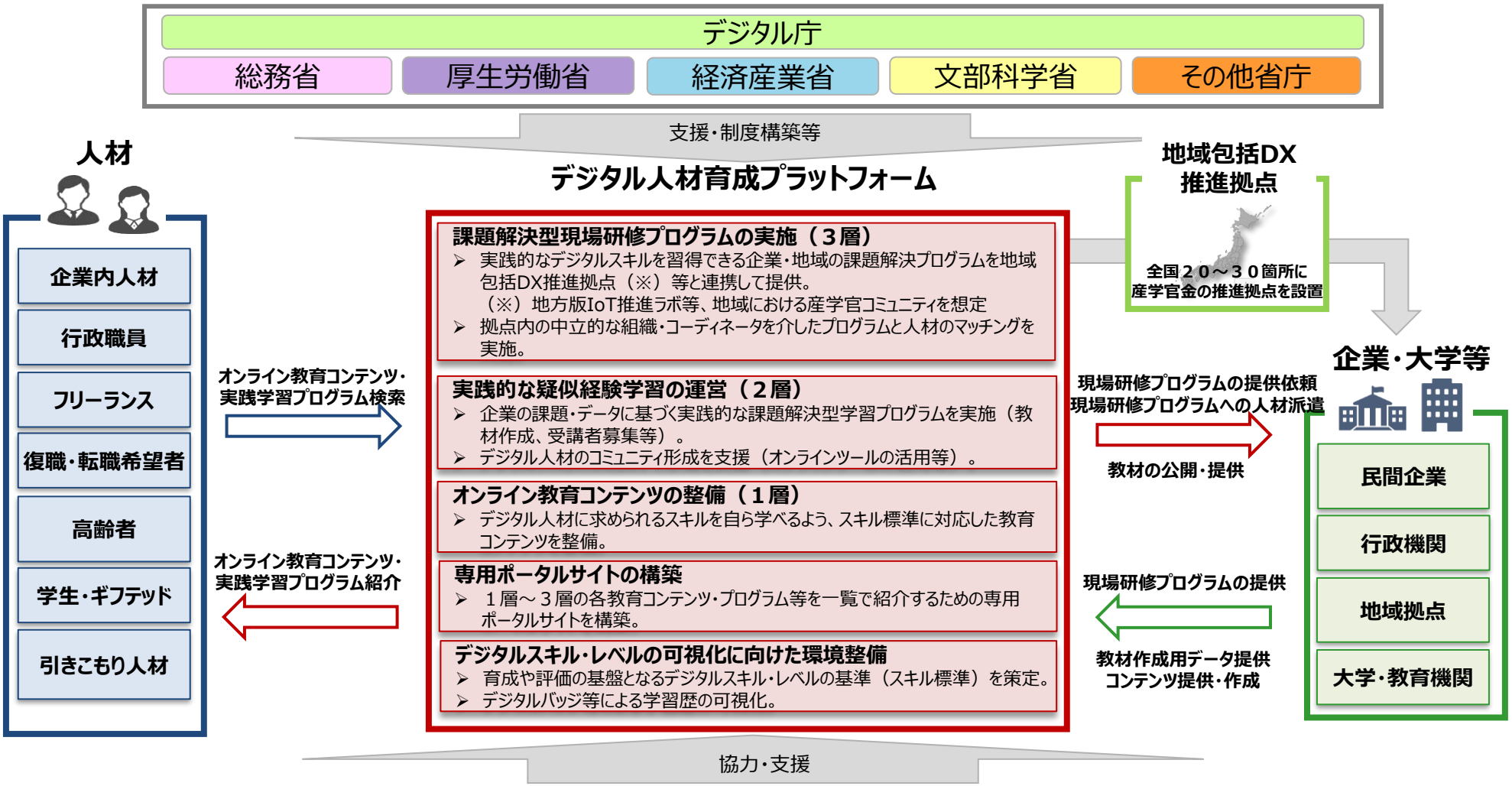
ビジネスアーキテクト	データサイエンティスト	エンジニア・オペレータ	サイバーセキュリティスペシャリスト	UI/UXデザイナー
デジタル技術を理解して、**ビジネスの現場においてデジタル技術の導入を行う全体設計**ができる人材	統計等の知識を元に、**AIを活用**して**ビッグデータから新たな知見を引き出し**、価値を創造する人材	クラウド等のデジタル技術を理解し、業務ニーズに合わせて必要な**ITシステムの実装やそれを支える基盤の安定稼働**を実現できる人材	業務プロセスを支える**ITシステムをサイバー攻撃の脅威から守る**セキュリティ専門人材	顧客との接点に**必要な機能とデザイン**を検討し、システムの**ユーザー向け設計**を担う人材

出典（図）：デジタル時代の人材政策に関する検討会 実践的な学びの場WG（第２回）資料

デジタル人材育成プラットフォーム 概要イメージ

共通

- プラットフォームでは、全てのビジネスパーソンに求められるデジタルリテラシーと専門的なデジタル知識の学習機会の提供と共に、組織においてＤＸの活動を牽引し、新たな付加価値の創造/業務効率化を実現できる実践的なＤＸ推進人材の育成手法を確立する。
- デジタル人材の不足に対応し、地域の企業・産業のDXを加速させることで、デジタル田園都市国家構想を実現するためのプラットフォームを構築する。



出典：デジタル時代の人材政策に関する検討会
実践的な学びの場WG（第２回資料）

大学・高専と連携した地域人材育成の取組

共通

- 産業界全体のサイバーセキュリティを強化するためには、**産学官の連携による取組基盤の整備**を行うとともに、各地域において、**地域の大学・高専との連携によって地域企業のセキュリティ強化につながる人材育成の実装を行い**、**継続的な人材循環に繋げていく必要がある**。

取組の全体像（イメージ）

＜地域での実装＞地域SECUNITY
[地場の特色を生かしたセミナー・人材育成の場]

学のリソース（情報・設備等）を使った地域企業におけるリカレント教育
- ◆ 経営層向けのセミナー・演習
- ◆ 実務者向けの演習・実習　等

官から地域企業へのコンテンツ・情報提供
◆ 全国各地でのセミナー・演習　◆地域企業向け情報発信

地域企業と学生の交流
◆ インターンシップ・イベント・キャリア教育等
→ 地域企業におけるセキュリティ人材やプラス・セキュリティを備えた人材の確保

地域SECUNITYの活性化による地域の人材育成と継続的な人材循環

＜地域間の連携＞SC3地域SECUNITY形成促進WG
[SECUNITY間での情報共有・連携促進]

各地域の優良事例の横展開
◆ SECUNITYの持続的な運営、地域のプレイヤーの巻き込み等に関する情報交換を通じた、優良事例の横展開

地域間連携によるリソースの共有
◆ 異なる強みを持つ地域の間でのセミナー受講者の相互受け入れ
◆ イベント共同開催
◆ 地域特性・異なるターゲットを踏まえたコンテンツ等の共有

＜取組の基盤整備＞SC3産学官連携WG等　[人材育成・活躍のために産学官で実施すべき事項の議論・検討]

産学官での共通言語（知識・スキル要件等）の策定
→ 学のカリキュラムへの反映
→ 産業界での採用/人事制度への反映

産業界・官から学へのコンテンツ/知見提供
◆ 副業先生等によるタイムリー・実践的な教育
◆ 分野別ビデオ教材（プラス・セキュリティ）
→ 企業人材の多様なキャリアパス形成/学への質の高い教育の提供

本日ご議論いただきたいポイント（人材）

- サイバーセキュリティ人材の育成や、プラス・セキュリティの普及に向け、主に以下の点について、ご意見等いただきたく存じます。

人材

- プラス・セキュリティの取組の普及のための施策の在り方
- 地域SECUNITY等を通じた、地域における産学官連携の加速化

0．全体像

1．経営

2．中小企業

3．人材

４．地域

5．国際

6．本日議論いただきたい論点

地域SECUNITY形成促進の全体像

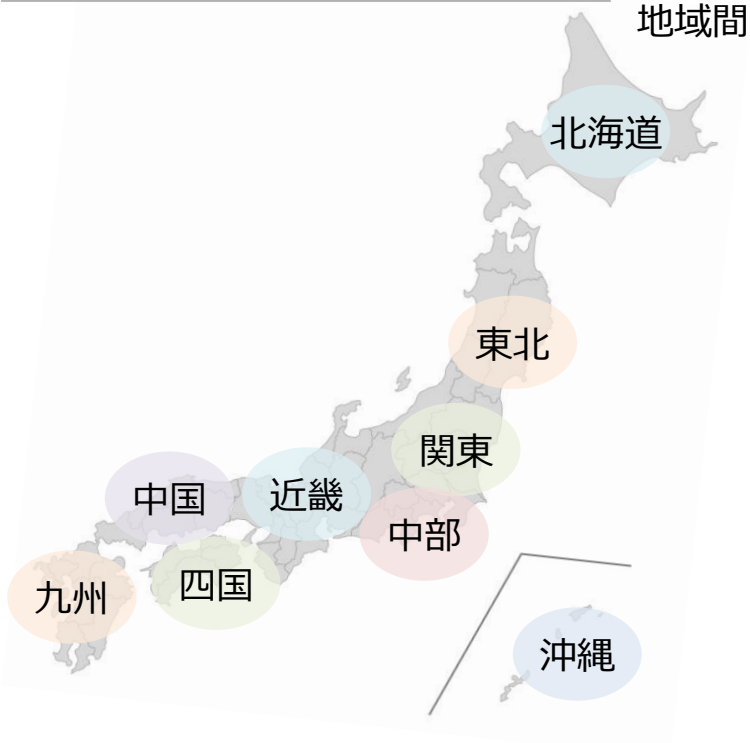
- 地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ（「地域SECUNITY」）の形成を全国において推進。
- 各地の取組をさらに促進するため、地域間の情報共有や、共通課題の解決に向けた取組の検討／推進を行うため、**SC3において地域SECUNITY形成促進WGが設立。**

①各地域での活動

各地域においてSECUNITYの活動を推進

他地域への事例共有

WSで得た知見の活用
地域間の連携創出



②活動の横展開

- **SC3地域SECUNITY形成促進WGワークショップ（WS）の開催**
- **地域SECUNITY形成・運営のためのプラクティス集の拡充**
- **地域SECUINITYリストの作成**

【活動の中で出てきた課題の例】

SECUNITYとしての地域の人材不足にどう対応するか。

活動の継続性をどう確保するか。
活動の裾野をどのように広げるか。

他のSECUNITYと連携しつつ、地域の特性にあったコミュニティの形成を目指すには

?

令和3年度地域SECUNITY形成促進の取組（北海道）

- 2014年9月、**総合通信局、経済産業局、道警察の3機関が連携し、全国に先駆けて「北海道地域情報セキュリティ連絡会（HAISL）」を発足。**道内の情報セキュリティ推進機関として、普及啓発や人材育成等を実施。

2021年度　HAISLの主な取組

サイバーセキュリティに対する理解促進に向けたセミナーを開催したほか、大学・高専等と連携した人材育成プロジェクト「SC4Y」による次世代のセキュリティ人材を育成する取組を実施。

人材育成

Security College for Youth(SC4Y)2021

・複数の道内教育機関等と連携し、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）
・ゲーム感覚でサイバー攻撃への対処能力を磨くことができる研修プログラム「**Micro Hardening for Youth**」を実施。（2021年10月）

定期的な勉強会の実施
（段階的に知識を身につける）

競技会への参加
（研鑽した力を試す）

HAISLサイバーセキュリティセミナー

・次世代育成事業「SC4Y」の一環として、セキュリティに興味のある学生を含む一般の方を対象にデジタル社会におけるサイバー脅威への対応等に関するセミナーを開催。(2022年2月)

普及啓発

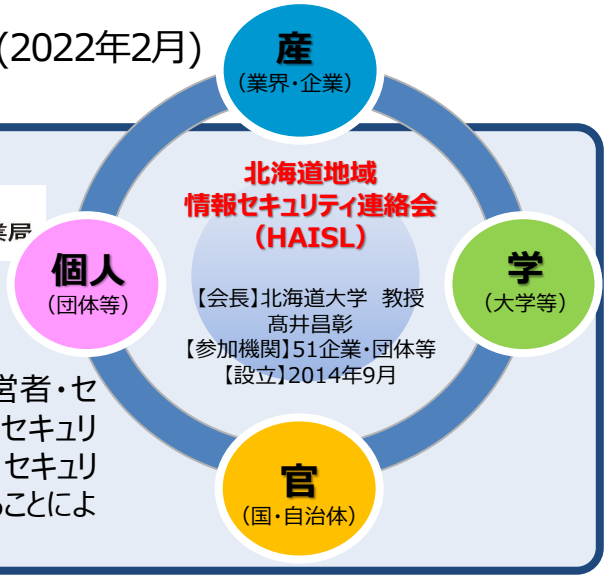
サイバーセキュリティオンライン・カンファレンス in NoMaps

中小企業を標的としたサイバー攻撃の現状や被害の実態、現実的なサイバーセキュリティ対策の進め方を紹介。

デジタル化により事業環境が変化していくなかで、必要なセキュリティ対策について専門家によるディスカッションを実施。(2021年10月)

【HAISL事務局】

総務省 MIC 北海道総合通信局　／　経済産業省 北海道経済産業局
Hokkaido Prefectural Police 北海道警察



産学官による地域コミュニティとして、企業経営者・セキュリティ担当者、支援機関等を対象とした情報セキュリティに関する意識の喚起や、情報セキュリティ技術・セキュリティマネジメント能力向上に向けた機会を提供することにより、セキュリティ意識の向上や人材育成を実施。

令和3年度地域SECUNITY形成促進の取組（東北）

- **デジタル化によるリスクに対応しつつ、その恩恵を享受**するためには、**サイバーセキュリティ対策の強化が急務。**
- このような状況の中、令和３年１０月、**東北総合通信局と共同**で、東北地域におけるサイバーセキュリティに対する意識向上・人材育成等に向けた取組を、産学官が連携して行うことを目的として**「東北地域サイバーセキュリティ連絡会」を設立。**
- セキュリティセミナーの開催等を通じ、**サイバーセキュリティの最新の脅威動向や、中小企業等が実施すべき対策等について理解を促進。**

＜東北地域サイバーセキュリティ連絡会＞

【概要】
東北地域におけるサイバーセキュリティに対する意識向上・人材育成等に向けた取組を、産学官が連携して行うことを目的として「東北地域サイバーセキュリティ連絡会」を設立。

【活動内容】
・サイバーセキュリティに関する最新情報等の提供
・セミナー開催、インシデント演習の実施
・構成員相互間の情報共有

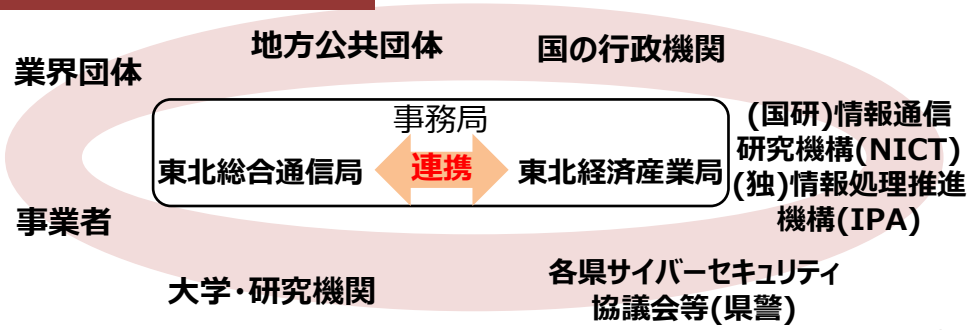
【構成員】
国の機関：東北財務局、東北農政局
地方公共団体：東北6県、仙台市
業界団体：(一社)東北経済連合会、各県情報産業協会等
事業者：(株)アキタシステムマネジメント、(株)ハイテックシステム、(株)デジタルハーツ、東北インフォメーション・システムズ(株)、富士ソフト(株)、三井住友海上火災保険(株)東北本部等
研究機関等：(独)情報処理推進機構、会津大学、東北大学等
連携団体：宮城県サイバーセキュリティ協議会、各県防犯連絡協議会等
事務局：東北経済産業局、東北総合通信局

○主な取組

【サイバーセキュリティセミナー】（主催：東北経済産業局）
【日程】2022年1月20日（木）
【参加者】中小企業経営者・担当者
【プログラム】
＊講演
①宮城県警察本部　サイバー犯罪対策課
「社会のデジタル化とサイバーセキュリティ」
②IPAセキュリティセンター
「中小企業における情報セキュリティの最新動向と対策」

【サイバーインシデント演習】（主催：東北総合通信局）
【日程】2022年2月22日（火）
【参加者】経営層・マネジメント層
【プログラム】
＊講義「事業経営の観点からみるサイバーセキュリティリスクの特定と対応戦略」
＊演習「セキュリティインシデント発生時の効果的な対応について」

連絡会の構成イメージ



令和３年度地域SECUNITY形成促進の取組（関東）

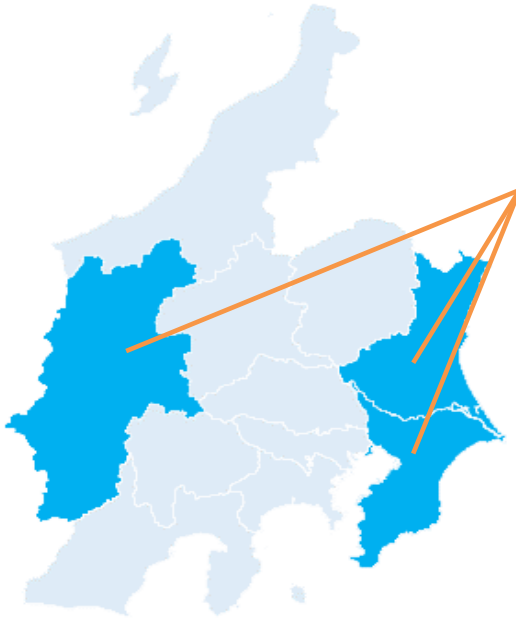
- 関東局管内における地域コミュニティの形成に向けて、茨城県、千葉県、長野県をモデル地域として、地域の関係機関と連携し、コミュニティ形成に取り組む。
- ３地域合同での普及啓発セミナーや各地域で個別企業の課題解決支援などを実施。

■　普及啓発のためのイベント実施

●普及啓発セミナー
最新の被害事例などを紹介し、事業継続のために求められる中小企業向けの対策を紹介

●千葉県ワークショップ
自社の課題を整理して、「SECURITY　ACTION」二つ星の宣言を目指すワークショップを開催

■　３地域でコミュニティ形成　事務局：特定非営利法人ITコーディネータ協会



●3地域で連絡会を定期的に開催
【連絡会の内容】
・各支援機関の取組内容を共有
　茨城県：13団体が参画　千葉県：8団体が参画
　長野県：13団体が参画
　（関東総合通信局、信越総合通信局もオブザーブ参加）
・普及啓発セミナーの企画と周知への協力
・個別企業の伴走支援先候補の検討、推薦

■　個別企業への伴奏支援、事例のとりまとめ

各地域コミュニティにて、セキュリティ対策等に課題をもつ企業を対象に、伴走支援を実施。支援事例はとりまとめの上、公表予定

訪問（Web会議）の目的		主な成果物（企業向け）
1回目	経営者から課題等をヒアリングし対策方針を決定	・支援計画書
2回目	情報セキュリティ対策の現状評価と課題の整理	・現状評価 ・取り組み方針
3回目	情報セキュリティ対策の改善に向けた要件整理	・改善対策/追加対策要件のまとめ
4回目	改善計画の作成と合意	・改善実施計画書

他自治体やIoT推進ラボ等に取組を共有し、管内各地域に普及させていく

令和３年度地域SECUNITY形成促進の取組（中部）

● 中部経済産業局では、東海と北陸地域の２拠点で活動。
①東海サイバーセキュリティ連絡会を２回開催。サイバー攻撃事例の共有、中小企業への普及促進について議論したほか、地域SECUNITY間の交流を促進。また、構成員が取り組むイベントについて、広く周知。
②北陸サイバーセキュリティ連絡会の活動では、北陸総合通信局との共催により、サイバーセキュリティデイズ2022としてセミナーや演習を開催。
③当局主催のDX推進セミナー及びワークショップを開催。デジタル技術の活用とともにその裏にあるサイバーリスクを認識し、中小企業のDXとセキュリティ対策を両輪としたデジタル企業への変革を促進する内容を実施。

1.東海サイバーセキュリティ連絡会

連絡会の開催(７月・２月)

- 構成員間の情報共有・事例研究
- 中小企業への普及啓蒙
  - ・サプライチェーン等面的支援
  - ・DXやBCP観点からのアプローチ
- シーサート協議会中部地区との交流、関西情報センターとの意見交換

モデル事例分析

中小企業取組事例
太田油脂(老舗食油製造)
自社のセキュリティの取組が発展し、三河地域でセキュリティサービスを展開する新会社設立へ
※東海総合通信局セミナーと連携し、事例紹介

構成員の主な活動

【愛知県警】サイバーセキュリティ防犯診断（中小企業のサイバー防犯診断を実施）
【シーサート協議会】シーサート協議会中部地区WS開催（連絡会など地域SECUNTY連携を議論）

2.北陸サイバーセキュリティ連絡会

「ビジネス」を護る
サイバーセキュリティデイズ2022

主催：北陸総合通信局、中部経済産業局、情報通信研究機構、北陸経済連合会、北陸情報通信協議会

- **Seminar Day　セキュリティ対策セミナー**
  経営者層が把握・理解すべきリスクと護るべきポイント
- **Practice Day 実践的演習**
  ECサイトに対するサイバー攻撃に対処する演習(講師：川口設計等)

3.DX推進セミナー・ワークショップ

中小企業におけるデジタル化とサイバーセキュリティを両輪で推進

サイバーセキュリティ講演

	回答数	構成比
1.大変参考になった	28	34.6%
2.参考になった	50	61.7%
3.あまり参考にならなかった	2	2.5%
4.参考にならなかった		
無回答		
計	81	100.0%

97%が参考になったと回答

デジタル化・DXの推進によりデータの重要性の理解

データを守るという観点からサイバーセキュリティ対策の必要性認識へ

令和３年度地域SECUNITY形成促進の取組（近畿）

- 「関西サイバーセキュリティ・ネットワーク（関西SEC-net）」の協力機関とともに、人材育成講座、地域別セミナー、セキュリティ専門家派遣、相談窓口や地域セキュリティコミュニティの見える化に取り組む。

【協力機関】 **取組を実施する主体の相互協力の促進**

産（業界・企業） **学（大学等）** **官（国・自治体）** **個（コミュニティ）**

関西サイバーセキュリティ・ネットワーク（令和４年３月現在７１機関）
共同事務局（近畿経済産業局、近畿総合通信局、KIIS）

サイバーセキュリティ人材の発掘・育成及び裾野拡大、交流の促進

【困り事、悩みの相談】相談窓口、地域セキュリティコミュニティの情報発信

- サイバーセキュリティ分野のお困りごとや技術的な相談、サイバー被害に遭われた場合など、中小企業等が相談できる窓口の一覧を発信
- 地域で活動をしているセキュリティコミュニティの一覧を発信

【人材育成連続講座】サイバーセキュリティ・リレー講座

- 関西を代表するセキュリティ研究者８名による集中講座
- 全国から約300名の申し込みがあった人気コンテンツ

【地域の関係者のつながりづくり】サイバーセキュリティ地域別セミナー

- 関西の２府５県で計７回開催
- 製品、ソリューションの目利き力向上
- 地域のセキュリティ関係者が一堂に会し、ネットワーク形成

【普及啓発、裾野拡大】サイバーセキュリティ専門家派遣

- 自治体、業界団体等のセキュリティセミナーに講師としてセキュリティ専門家を派遣し、講演やワークショップを実施
- セキュリティ意識の薄い企業に対し、【ゼロ→イチ】の普及啓発

令和３年度地域SECUNITY形成促進の取組（中国）

- 令和2年10月、中国地域におけるセキュリティ対策の充実を図るため「中国地域サイバーセキュリティ連絡会」を設立。情報共有や演習・セミナー等の開催、構成員間の交流促進によりセキュリティ意識向上や対応促進に取り組んでいる。
- セキュリティ人材の育成・確保が最大の課題。中国経済連合会、岡山大学、広島市立大学と連携し、中小企業等の実務者向けに実践的なオンライン演習等を実施。

中国地域サイバーセキュリティ連絡会

【設　立】令和２年10月
【事務局】中国経済産業局、中国総合通信局
【構成員】
参加機関（中国地域５県、２政令市、通信・放送事業者、金融機関、業界団体、産業支援機関、大学等）90機関
連携機関（国の出先機関、NICT、IPA等）15機関
※ 各県サイバーセキュリティ協議会（県警）と連携
【主な活動】

- 情報共有（セキュリティ対策、インシデント情報等）
- セミナーや演習等の開催/共催
- 構成員間の交流

Raspberry Pi 等の教材を使ったマルウェア対策実践演習（オンライン）の様子

令和３年度地域SECUNITY形成促進の取組（四国）

- 四国総合通信局、高専等の産学官関係者をセキュリティ関連関係者会議委員に選定し、ヒアリングを実施。
- 県警及びIPAを講師に中小企業向けサイバーセキュリティセミナーを開催。
- 同時に、事前予約制の中小企業向けセキュリティ相談会を実施。

令和３年度地域SECUNITY形成促進の取組（九州①）

- 業種ごとの特徴を踏まえたセキュリティ対策やビジネスリスク対応が出来るよう、地域企業からの体験（事例）紹介やサイバー保険など経営者が必要とする情報中心にプログラム構成し、**「業種別」に合計６回のセミナーを実施**。
- 地域企業への周知は、コミュニティ形成の核となる地域企業自身がインフルエンサーとなり商流を通じて幅広く案内。セキュリティベンダーや保険会社等も含め、**延べ計５９９名が参加**。
- 地域SECUNITYの核となるセキュリティ関連事業者、**地域企業等の発掘、連携強化を推進中**。
  【※地域企業：創ネット(株)、(株)ミズ、(株)オーイーシーなど】

【セミナー開催実績】

地域	第1回 福岡地域①	第2回 福岡地域②	第3回 大分地域	第4回 佐賀地域	第5回 熊本地域	第6回 宮崎地域
テーマ	製造業	海外ビジネス	宇宙産業	医療・薬局	農業	林業
チラシデザイン						
プログラムの特徴	・中小企業向けセキュリティ対策とサイバー保険 ・中小企業経営者によるサイバー被害事例	・サイバーセキュリティの各国法規制 ・中国子会社を含めたテレワークとセキュリティ運用	・宇宙産業の概観と大分の取り組み ・IoTとセキュリティ	・サイバーセキュリティ・インシデント対応机上演習の紹介 ・コロナ禍の医療機器メーカー・セキュリティチームの挑戦	・女性農家による講演「地震雷火事親父っより怖い『鬼嫁イノシシ雨サイバー』」	・林業サプライチェーンとサイバーセキュリティ ・ECサイトのセキュリティ
参加者数	141名	90名	79名	134名	80名	75名

令和３年度地域SECUNITY形成促進の取組（九州②）

- **<u>九州大学</u>**が取り組む**<u>社会人リカレント教育プログラム（SECKUN）との連携で、特別無料視聴参加プログラムを提供</u>**。
  中小企業の経営者やセキュリティ担当者等の人材育成として、実践的教育の機会を提供。
- SECKUN“サイバーセキュリティインシデント対応机上演習”では、事業継続のための組織のあり方を検討するため「医療調剤用TTXシナリオ」を策定。調剤薬局経営者のほか医師・薬剤師も含め地域SECUNITYメンバーから計６名が参加。
- **<u>参加した(株)ミズ　溝上代表取締役は「危機への備えが人の命を守ることに繋がると実感した」</u>**とコメント。

九州大学
KYUSHU UNIVERSITY

SECKUN
「サイバーセキュリティインシデント対応机上演習」
実施イメージ

SECKUN「ビジネスイノベーションコース」では、
地域SECUNITYメンバーから延べ１２名が参加。

日程	講師名/コース名	地域SECUNITYからの参加者数
10/17（日）	**講師：福田峰之先生** （多摩大学大学院客員教授、元ITC副大臣） **「安全保障経済政策からのサイバーセキュリティ基本法」**	５名
10/24（日）	**講師：乗口雅充先生** （株式会社セキュアスカイテクノロジー会長） **「スキュータムを題材としたセキュリティビジネスの戦略」**	４名
10/24（日）	**講師：田中先生** （株式会社NTTぷらら） **「VRスポーツHADOにおけるバイラルマーケティングの戦略」**	３名

令和３年度地域SECUNITY形成促進の取組（沖縄）

- 沖縄サイバーセキュリティネットワーク（2015年3月発足）など既存の産学官のセキュリティ関連ネットワークを有機的に連携。
- 沖縄地域の自治体、事業者に対し、実態把握のためのアンケート調査を実施し、これを踏まえたセキュリティに関するセミナー開催、相談窓口設置などセキュリティ対策を検討。

【実施団体】沖縄ITイノベーション戦略センター（ISCO）
・SECUNITY事業では、リテラシー向上のためのセミナーの実施やメールマガジンによる情報提供等を行い、総務省、沖縄県事業と連携した取組を展開。
・若手人材の育成のため情報セキュリティマネージメント等の資格者取得支援を実施。
・ビジネスマッチングサイト「インダストリンク」内にサイバーセキュリティ関連コンテンツを作成。

※セキュリティセミナーはコロナ感染対策を考慮してすべてオンライン開催するとともに、動画コンテンツとして提供。

SC3　地域SECUNITY形成促進WGの設置

- **目的：**各地域で形成が進みつつある地域のセキュリティ・コミュニティ（地域SECUNITY）の取組をさらに推進するため、地域間の情報共有や、共通課題の解決に向けた取組を検討・推進することを目的に2021年6月SC3第３回運営委員会で設置決定。
- **活動内容：**各地域SECUNITYの担当者等を対象として、**各地域における活動にあたって必要となる情報の共有、ベストプラクティスの展開、共通課題に対する解決策の検討**などを目的としたワークショップやセミナー等を企画・開催する。また、共通課題に対する解決策の検討にあたっては、必要に応じて支援機関、業界・経済団体等を募り、有効な取組の検討等を行う。

●メンバー

（敬称略）

	氏名	役職等
座長	梶浦 敏範	一般社団法人 日本経済団体連合会 サイバーセキュリティ委員会 サイバーセキュリティ強化WG主査
アドバイザー	川口　洋	株式会社 川口設計　代表取締役
	持田　啓司	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 情報セキュリティ教育事業者連絡会 代表
	吉岡　良平	一般財団法人 草の根サイバーセキュリティ運動全国連絡会　常務理事

他のWSの参加者

- 地域SECUNITYの事務局、専門家、地域のコミュニティのキーパーソン　地域SECUNITY参加団体 等
  その他 地域のSECUNITYにおける活動内容に関心を有する者

SC3　地域SECUNITY形成促進WG　WS開催

- 今年度、各地のセキュリティ・コミュニティの担当者等を集めたワークショップを２回開催。今後も**各地のプラクティスや課題に関する共有・議論**を行う予定。

日時	項目	内容
第１回 10月27日(水) 10:00～12:00 ※オンライン開催 ※参加者84名 （オブザーブ含む）	**<パート①>** 有識者による講演 **<パート②>** 地域の取組共有セッション **<パート③>** 少人数での意見交換	「地域コミュニティに対する期待」 川口　洋氏　（株式会社 川口設計　代表取締役） 取組が先行しているSECUNITYによるベストプラクティスの共有 ・【北海道】北海道地域情報セキュリティ連絡会（HAISL） ・【近畿】一般財団法人関西情報センター（KIIS） ・【九州】三井物産セキュアディレクション株式会社 有識者主導で、参加者の自己紹介・意見交換を実施（７グループ）
第２回 3月４日（金） 14:00～17:00 ※オンライン開催 ※参加者80名 （オブザーブ含む）	**<パート①>** 有識者による講演 **<パート②>** 地域の取組共有セッション **<パート③>** 少人数での意見交換 **<パート④>** 分科会での内容を共有	「利用者視点・地域視点で取り組む情報セキュリティ啓発」 吉岡　良平氏　（一般財団法人 草の根サイバーセキュリティ運動全国連絡会　常務理事） 具体的な取組について地域SECUNITY、企業様からの事例紹介 ・特定非営利活動法人ＩＴＣちば経営応援隊　様 ・株式会社ミズ　様 以下のテーマごとの分科会にて意見交換（３テーマ：６グループ） ①「地域SECUNITYの持続的な運営体制構築のための工夫・支援」 ②「地域SECUNITY形成におけるポイント・課題（関係機関、団体、企業の巻き込み方等）」 ③「地域における情報セキュリティビジネスの展開」 分科会での意見交換内容・課題等を発表

参加者の声

- 事例紹介は、まさに経営者自らがセキュリティ対策を実践していかないといけないとの思いが伝わった。
- 全国で同様の活動をしている人たちと横のつながりができて、大変ありがたい。
- SECUNITY形成を進める中で、色々なヒントをいただくことができた。３か月または半年に１回の開催であれば、タイムリーな情報交換ができると思う。
- DX化に伴い様々な業種から参画があっていいと思う。各地域SECUNITY形成促進の為に縦割りではなく横断的な参画が出来るようになればいい。
- 次の行動につながる活動をお願いしたい。例えば、事前に困りごとと解決策を持っている人たちをコーディネートする仕組みなどがあると良いのではないか。

地域SECUNITY形成のためのプラクティス集拡充

- 「地域セキュリティコミュニティ【地域SECUNITY】形成・運営のためのプラクティス集」について、当プラクティス集の更なる拡充に向けて現在活動中の地域のサイバーセキュリティコミュニティ等へヒアリング調査を実施し、**プラクティス集第２版を作成予定。**
- 合わせてコミュニティ形成に関連するセキュリティセミナー等への対応が可能な**講師派遣制度のリストも拡充**して公開する。

＜プラクティス集第１版概要＞

対象コミュニティ

- 北海道地域情報セキュリティ連絡会
- 北海道中小企業サイバーセキュリティ支援ネットワーク
- サイバーセキュリティセミナ in 岩手
- 宮城県サイバーセキュリティ協議会
- みちのく情報セキュリティ推進機構　みちのく情報セキュリティ推進センター
- 関西サイバーセキュリティ・ネットワーク
- 総関西サイバーセキュリティLT大会
- 九州経済連合会　サイバーセキュリティ推進WG
- 熊本県サイバーセキュリティ推進協議会
- 鹿児島県サイバーセキュリティ協議会

項目

1．コミュニティ設立の経緯・狙い
2．取組方針
3．協力機関・団体等との関係性
4．取組・イベント開催概要
5．実践からのプラクティス

活動中の地域コミュニティ、形成途上のサイバーセキュリティコミュニティをヒアリングを実施し、プラクティス集第２版のコンテンツとして、以下についての図表入り原稿を作成予定。

① コミュニティ単位での整理

第１版と同様、サイバーセキュリティコミュニティの単位で、コミュニティの特徴や属性、各コミュニティにおける実践から得られたプラクティスの内容等をまとめる。

② 条件別ポイントの整理

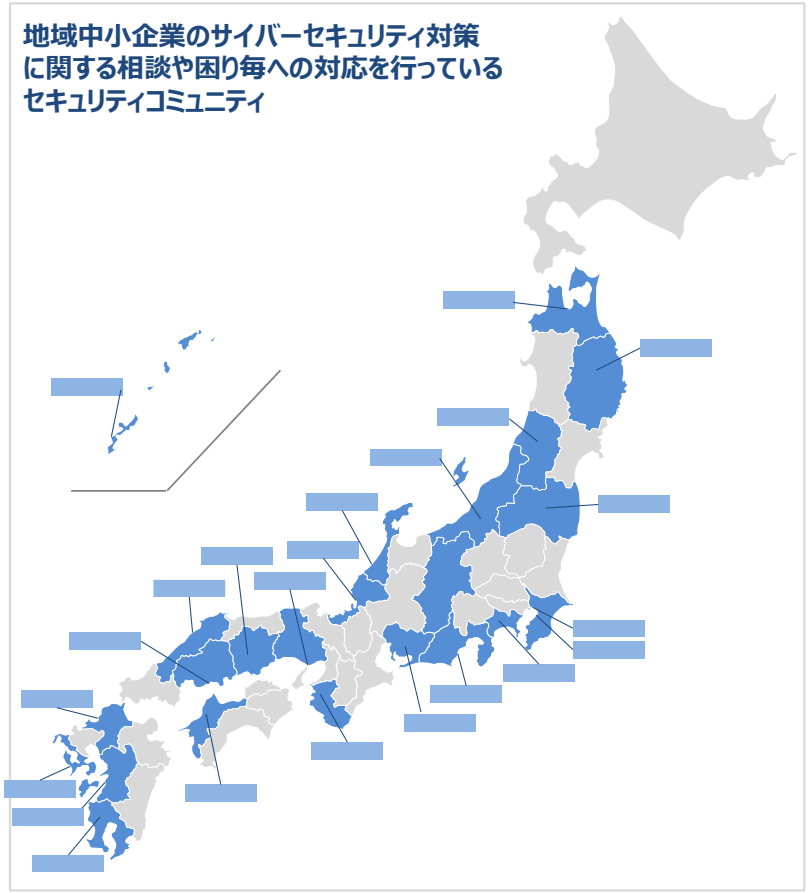
プラクティス集読者の利便性向上の観点から、以下に例示するようなコミュニティ形成に関わる諸条件に応じて考慮すべきポイントを整理する。

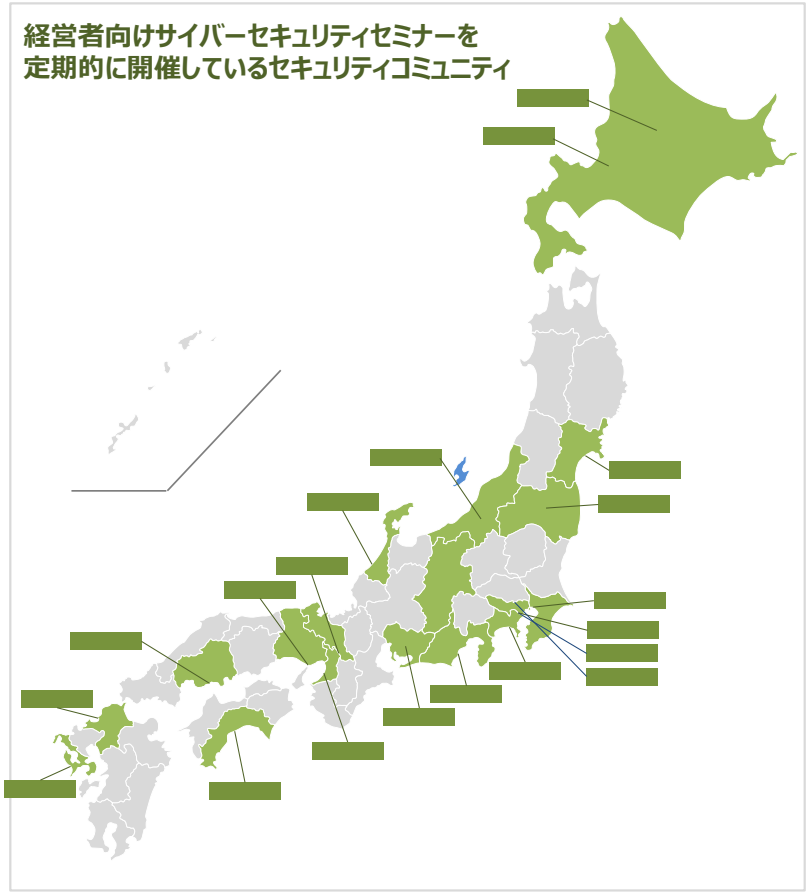
- コミュニティの実施主体に応じた構築や活動におけるポイント
- 関係機関・団体の効果的な関与を得るためのポイント
- 地域企業等によるコミュニティへの参加をしやすくするためのポイント
- 実施主体の運営負荷を軽減するためのポイント

各地域におけるセキュリティコミュニティリストの作成（新設）

- コミュニティリストの作成と併せて、同リストの利用者にとってより効果的に活用できるようにするため、**地域毎のコミュニティの存在を視覚的にわかりやすく伝えるため**地図上にマッピングし、経済産業省HPにて公開予定。マッピングのイメージは次のとおり。

コミュニティの活動地域に関する地図上へのマッピングのイメージ





（注）本図はいずれもマッピングのイメージであり、実在するコミュニティに対応するものではない。

０．全体像

１．経営

２．中小企業

３．人材

４．地域

５．国際

６．本日議論いただきたい論点

国際連携の全体像

- サイバーセキュリティ政策については、国際的な動向も踏まえつつ、関係国と連携して検討・推進することが重要。引き続き、関係国の官民と連携した情報収集・政策検討や、日本企業の多くが事業を展開するインド太平洋地域におけるキャパビルなどの国際貢献を実施していく。

取組の全体像

①インド太平洋向け演習

- 日米EU産業制御システムサイバーセキュリティウィーク
- JICA課題別研修
  （産業制御システムサイバーセキュリティ演習）
- [参考]「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」

情報収集　施策連携　施策周知　国際連携

②海外施策や国際標準等の動向

- 海外政府の施策動向調査
- 国際標準の動向

情報収集

③国際会議への出席

- 国際会議への出席状況

情報収集　施策連携　施策周知

④関係国の官民との連携

- 関係国の官民との意見交換実績

情報収集　施策連携

①インド太平洋向け演習
インド太平洋地域向け日米ICSサイバーセキュリティ演習（第3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は、米国政府（国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁、国務省、エネルギー省、アイダホ国立研究所）と連携し、**インド太平洋地域向け産業制御システム・サイバーセキュリティ演習（第3回）**を実施。
- 演習の一部分として、日米にEUも加わる形で、**初めて日米欧サイバーセキュリティセミナーを開催**。

■ **日時・場所：**2021年3月8日（月）～12日（金）（オンライン開催）

■ **参加者：**・ASEAN加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾の電力・石油会社、National CERT、エネルギー及びサイバーセキュリティ関係政府機関から40名を招聘。
・IPA産業サイバーセキュリティセンター（ICSCoE）の中核人材育成プログラム受講生も参加。

■ **開催概要：**リモートでのハンズオン演習や、日米欧の専門家によるエネルギー分野特有の問題も含む様々なサイバーセキュリティ関連のワークショップの受講、参加者間での知見の共有など、参加者に対してユニークかつ貴重な機会を提供。

長坂 経済産業副大臣挨拶

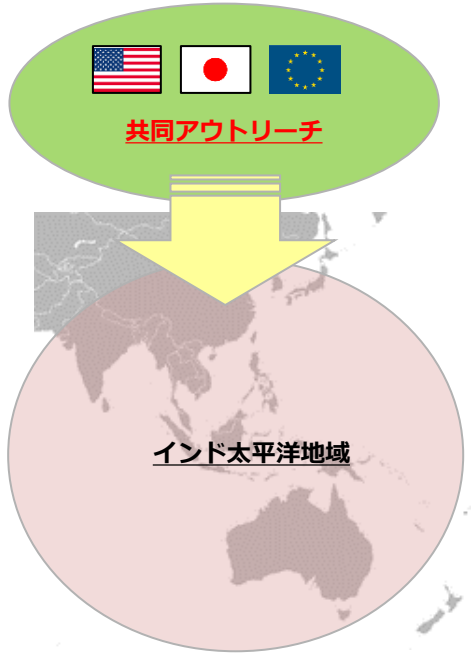
ウェールズ　米国DHS/CISA 長官代行挨拶


リモートハンズオン演習の様子


ロウハナ 欧州通信総局次長挨拶


ヤング 在日米国大使館　臨時代理大使挨拶


リモートハンズオン演習の様子



インド太平洋地域向け日米EU　ICSサイバーセキュリティ演習（第４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は、米国政府（国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁、国務省、エネルギー省、アイダホ国立研究所）、欧州連合（通信総局）と連携し、**インド太平洋地域向け産業制御システム・サイバーセキュリティ演習（第４回）**を実施。
- 主催者として、日米にEUも加わる形で、**初めて日米欧サイバーセキュリティセミナーを開催**。

■ **日時・場所：**2021年10月25日（月）～29日（金）（オンライン開催）

■ **参加者：**ASEAN加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾の電力・石油会社、National CERT、エネルギー及びサイバーセキュリティ関係政府機関から40名を招聘。一部セミナーにはオブザーバー参加も受入れ。IPA産業サイバーセキュリティセンター（ICSCoE）の中核人材育成プログラム受講生も参加。

■ **開催概要：**リモートでのハンズオン演習や、日米欧の専門家によるエネルギー分野特有の問題も含む様々なサイバーセキュリティ関連のワークショップの受講、参加者間での知見の共有など、参加者に対してユニークかつ貴重な機会を提供。

演習の様子

細田 経済産業副大臣挨拶

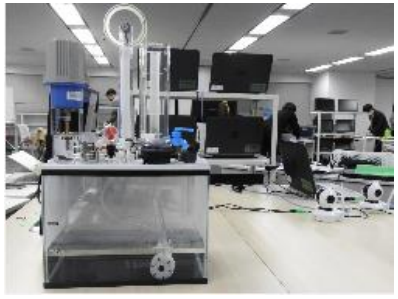
ゴールドスタイン　米国DHS/CISA 長官代行挨拶

リモートハンズオン演習の様子①

アロンソ 欧州通信総局デジタル社会・トラスト・サイバーセキュリティ局長挨拶

グリーン在日米国大使館　臨時代理大使挨拶

リモートハンズオン演習の様子②



インド太平洋地域向け 日米EU　ICSサイバーセキュリティウィーク（第4回）構成

(1) セレモニー

- 開会挨拶
  - ・細田経済産業副大臣
  - ・Goldstein米国国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁長官補
  - ・Greene駐日米国臨時代理大使
  - ・Alonso欧州委員会・通信ネットワーク・コンテンツ・技術総局 デジタル社会・トラスト・サイバーセキュリティ局長
- キーノートスピーチ（米Dragos社 Founder & CEO Robert M. Lee氏）
- 閉会挨拶 (遠藤IPA産業サイバーセキュリティセンター長、Tudorアイダホ国立研究所国家・国土安全保障セキュリティ理事、Lepassaar ENISA長官)

(2) 日米合同産業制御サイバーセキュリティトレーニング

- ICSCoEによるハンズオントレーニング（開会前に２日間かけて実施）
- アイダホ国立研究所(INL)・ICSCoEによるリスクアセスメントワークショップ
- INL・ICSCoEによる人材育成ワークショップ

(3) 産業制御システムサイバーセキュリティセミナー

- 電力セクターセミナー１：発電・送電・配電（従来型発電ビジネス）
- 電力セクターセミナー２：エネルギー・ソース・アグリゲーション・ビジネス、再生可能エネルギー
- プロセスオートメーションセクターセミナー
- サプライチェーン・リスクマネジメント セミナー
- 政策・標準化セミナー

JICA課題別研修：「産業制御システムのサイバーセキュリティに係るインド太平洋地域向け演習」

- IPA産業サイバーセキュリティセンターは、JICA課題別研修として、インド太平洋地域から招聘した研修生に対して、模擬プラントを用いたハンズオン演習及びグループディスカッションによる演習を実施。

■ **日時・場所：**2022年2月７日（月）～9日（水）（オンライン開催）

■ **参加者：**インドネシア、マレーシア、モンゴル、ベトナムから9名の研修生がリモート参加

■ **開催概要：**模擬プラントを用いたリモートでのハンズオン演習プログラムを提供し、研修生が抱えるセキュリティの課題や必要となるセキュリティ対策などについて講師陣と話し合うグループディスカッションを交えた演習を実施。

経済産業省からも、人材育成、CPSF等のガイドライン、J-CSIP及びSC3による情報共有スキームなど、サイバーセキュリティ政策に関する取組を紹介。

演習の様子

ハンズオン演習講師
満永拓法　東洋大学情報連携学研究科准教授
IPA ICSCoE　講師

遠隔で模擬プラントを不正操作するハンズオン演習

【参考】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

【参考】サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針

- 2021年12月13日、サイバーセキュリティ戦略本部にて「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」が決定された。
- これまで、ASEAN地域を中心として行ってきた能力構築支援をインド太平洋地域を中心に支援対象を拡大することなどが盛り込まれた。

支援の重要性

①我が国を含む世界全体へのセキュリティリスクの低減

②対象国の重要インフラ等に依存する邦人や日本企業の活動の安定の確保

③情報の自由な流通や法の支配を基本原則とする我が国の立場への理解の浸透

④我が国の産業等の現地展開を進める基盤の形成

⑤自由で開かれたインド太平洋等の政府方針の強化への寄与

具体的取組

①重要インフラ防護等を通したサイバーハイジーンの確保支援

- 支援ニーズが高まりつつある**重要インフラ向けの支援を官民連携により強化**
- ASEAN地域における成果と経験を基に、**インド太平洋地域を中心に支援対象を拡大し、多様なニーズに応じた国別支援を強化**

②サイバー犯罪対策支援

- サイバー関連法制度等に関する研修、条約締約国による関連会合等の枠組みの活用

③サイバー空間の利用に関する国際的ルール作り及び信頼醸成措置に関する理解・認識の共有

- サイバー空間における**国際法の適用や国家の行動規範について、各国の能力構築を支援**
- 民間企業、学術界、技術コミュニティ等を含むマルチステークホルダーによる取組の推進

④人材育成等横断的な領域

- 重要インフラ等分野のニーズ拡大にあたり、関係省庁間におけるより一層の緊密な連携
- 海外における**我が国事業者の活動を中長期的に支える人材の育成**

②海外施策や国際標準等の動向

【米国】国家のサイバーセキュリティの改善に係る米国大統領令の署名

- 2021年5月12日、バイデン大統領は、連邦政府機関におけるサイバーセキュリティ改善に係る大統領令に署名。
- **官民での脅威情報の共有**、**ソフトウェアサプライチェーンセキュリティ対策**の強化、**ゼロトラストアーキテクチャ**への移行等を通じて、連邦政府機関のサイバーセキュリティ対応能力の向上を図っている。

本大統領令における主な指示事項

1 **官民の脅威情報共有における障害の除去** (Section 2)	● ITサービスプロバイダーが連邦政府と確実に脅威情報を共有できるようにしたうえで、特定のインシデント情報の共有を義務づける。
2 **連邦政府におけるより強力な標準の近代化と導入** (Section 3)	● FedRAMP改定等を通じて、**連邦政府が安全なクラウド及びゼロトラストアーキテクチャに移行することを支援**し、多要素認証と暗号化の導入を義務づける。
3 **ソフトウェア・サプライチェーンのセキュリティ向上** (Section 4)	● NISTを通じて**政府が調達するソフトウェアの開発に関するセキュリティ基準(安全な開発環境の確保や構成要素に関する詳細（SBOM）の開示等を含む)を確立**し、特に**重要なソフトウェアに対して一定の対策を義務づけ**る。 ● 商務省は、既存のラベル表示などを参考にして、消費者向けの情報提供に関するパイロット制度を開始する。
4 **サイバー安全審査委員会の創設** (Section 5)	● 国土安全保障省は、**重大なインシデントが生じた際に政府と民間事業者が共同議長を務める「サイバー安全審査委員会」を設置**し、サイバーセキュリティ向上に向けた具体的な提言を行う権限を与える。
5 **インシデント対応のための標準プレイブックの策定** (Section 6, 7)	● 国土安全保障省は、連邦政府機関によるインシデント対応のためのプレイブックを策定する。 ● 連邦政府機関は、エンドポイント検知・対応(EDR)イニシアチブを展開し、インシデントの検知、積極的なサイバーハンティング、有事対応をサポートする。
6 **調査及び修復能力の向上** (Section 8)	● 連邦政府機関に対してセキュリティイベントログの要件を設け、侵入を検知し、対処する組織能力の向上を支援する。

（出典）各種公開情報より作成

【米国】大統領令におけるソフトウェア・サプライチェーンに関するタイムライン

- 大統領令では、**ソフトウェア・サプライチェーンの確保に向け、NISTが中心となりガイドラインを策定する**旨を指示しており、この**ガイドラインには製品購入者に対するSBOM提供に関する項目も含まれる**。
- また、NISTに対して、NTIAと連携して**SBOMの最小要素を公表すること**を指示している。
- 将来的には、公開されたソフトウェア・サプライチェーンに関するガイダンスの要求事項に基づき、**連邦政府のソフトウェア調達に関するFAR（連邦調達規則）が改正される予定**である。

2021.5.12	大統領令の署名
2021.6.25	「重要なソフトウェア」の定義の公表 NIST DoD DHS OMB
2021.7.9	「重要なソフトウェア」のセキュリティ対策に係るガイダンスの公開 NIST DHS OMB
	ソフトウェア検証の最低基準に関するガイドラインの公表 NIST DHS
2021.7.12	SBOMの最小要素の公表 NIST NTIA
2021.7.25まで	「重要なソフトウェア」の定義を満たすソフトウェア製品のカテゴリを特定し、政府機関に通知 DHS NIST
2021.8.10	NISTが公開した重要なソフトウェアのセキュリティ対策に関するガイダンスを、各省庁が遵守することを求めるための措置を講じる OMB
2021.10.28	ソフトウェアサプライチェーンのセキュリティを強化するための予備的なガイドラインの公表 NIST
2022.2.4	ソフトウェアサプライチェーンのセキュリティを強化するための指針を示すガイダンスの公表 NIST
2022.3.8まで	大統領令以降に調達されたソフトウェアに関して、各省庁がNISTによる指針を遵守するための適切な措置を講じる OMB
2022.5.8まで	「予備的なガイダンス」の定期的な見直し・更新のための手順を含む追加のガイドラインの公表 NIST
2022.5.12まで	FAR審議会に対し、各省庁が購入可能なソフトウェアサプライヤーに対する上記ガイダンスに基づく要求事項の遵守と、遵守の証明を義務付ける契約文言を勧告 DHS
(現状、期限の指定なし)	⇒ DHSによる勧告の検討、FARの改正 FAR審議会
	FAR改正に伴い、FARの要件を満たさないソフトウェア製品を調達契約から削除 各省庁

出所）White House, “Executive Order on Improving the Nation’s Cybersecurity” https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ , NIST, “Executive Order” https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/executive-order

【欧州】NIS指令の改正

- 2020年12月、欧州委員会は、域内の重要インフラ事業者等のサイバーセキュリティ対策について規定するNIS指令(Directive (EU) 2016/1148)の改訂案を公表。
- 現行指令から、適用業種が大きく拡大しており、事業者に課すセキュリティ要件や罰則等においても規定が強化されている。

変更項目	現行NIS(2016年制定)の規定	主な改正事項（検討中のもの）
適用範囲	● **基幹サービス運営者** ①エネルギー(電力、石油、ガス)、②輸送、③銀行、④金融市場インフラ、⑤医療、⑥上水道、⑦デジタルインフラ ● **デジタルサービス提供者** ①オンラインマーケット、②オンライン検索エンジン、③クラウドコンピューティングサービス	● 基幹サービス運営者・デジタルサービス提供者という分類を、重大エンティティ(essential entity)と重要エンティティ(important entity)に変更。 ● 重大エンティティは、基幹サービス運営者７分野に**「下水道」、「行政」、「宇宙」の３分野を追加**した10分野。 ● 重要エンティティには、デジタルサービス提供者以外に、「郵便・配送」、「廃棄物処理」、「化学品」、「食品」、**「製造(医療機器、コンピューター及び電気電子製品、電気設備、機械設備、自動車、その他の輸送機器)」が追加。**
適用範囲の事業者に関連する規律	● 適用範囲の事業者が適切かつ均衡の取れた技術的及び組織的措置を講じる。 ● サービスの継続性に重大な影響を及ぼすインシデントの、管轄官庁又はCSIRTへの届出。	● 重点的な対策（サイバーセキュリティテスト、暗号化の利用等）をリストアップし、**セキュリティ要件を強化。** ● **ICTサプライチェーンにおけるセキュリティへの対応を明記。** ● インシデント報告に関して、**プロセス、内容、およびタイムラインに関するより正確な規定を設定。**
罰則	● 罰則を設けることのみ規定。	● **罰則の程度を指定**（1000万ユーロまたは全世界の年間売上高の2%を上限とする罰金）。

改正指令については、欧州委員会HP内の「Proposal for directive on measures for high common level of cybersecurity across the Union」掲載の資料を参照

IoT機器・システムのセキュリティに係る日米欧の制度化動向

- 民間部門を対象としたものとしては、米国では、「国家サイバーセキュリティの向上に関する大統領令」に基づく**消費者向けIoT製品のラベリングプログラムの開発**、欧州では、サイバーセキュリティ法に基づく**認証制度の策定及びNLF関連指令/規則による対策の規制化**が進められている。

	 **米国における検討状況** **(連邦政府で議論されているもの)**	 **EUにおける検討状況** **(EU単位で議論されているもの)**	 **日本政府の検討状況** **(主にIoT機器・システムの認定に係るもの)**
主な法令等	**国家サイバーセキュリティの向上に関する大統領令** (Executive Order 14028)	**サイバーセキュリティ法(CSA)** **NLF関連指令/規則** (例：機械規則案)	**電気通信事業法** 上記のほか、IT関連製品を対象にした認証制度として、ITセキュリティ評価及び認証制度(JISEC)等が存在する。
適用対象	**消費者向けのIoT製品** IoT製品には、IoT機器に加え、機器の利用に必要な製品コンポーネント(ネットワーク機器、モバイルアプリ等)を含み得る。	**製品分野等により異なる** 機械規則や無線指令等の各NLF関連指令/規則に規定が設けられており、現状は垂直的な規制が議論されている。	**インターネット等に接続する端末機器** ルータ、ウェブカメラ等が該当し、IPを使用しない機器やインターネット等に直接接続しない機器は含まれない。
セキュリティ基準	**消費者向けIoT製品のサイバーセキュリティ・ラベリングのための推奨基準** 現行案はNISTIR 8259シリーズをベースに策定されている。	**製品分野等により異なる** 機械規則や無線指令等の各NLF関連指令/規則に規定が設けられており、現状は垂直的な規制が議論されている。	**端末設備等規則** 必ずしも機器・システム等の認定に関わらないものとしては、IoTセキュリティガイドライン、CPSF/IoT-SSF等が存在する。
事業者の義務等	**現状では必ずしも議論されていない** NISTは、政府主導の認証・ラベリング制度ではなく、今後制度を開発する主体が参照するものを志向している。	**NLF関連指令/規則を通じて義務化される見込み**	**技術基準適合認定が求められる場合等を除けば、必ずしも対策は義務とされていない。**
今後の予定	• 2022年5月12日までに、NISTは、上記検討に関する総括報告書を発行する予定。 • 上記報告書の公開後、基準に基づく認証制度の検討が推進される見込み。	• EUCC等、CSAに基づく認証制度の具体化が進む見込み。 • 草案が公開されているNLF関連指令/規則は、順次欧州議会等で議論が進められる。 • 2022年下期に、水平的なセキュリティ基準の確立を志向する「サイバーレジリエンス法」公表を予定。	• IoTを対象にした具体的な認証・ラベリング等の議論はなされていない。

セキュリティ・マネジメントに係る米国や国際標準の動向

- 昨今の情勢変化を踏まえ、米国において、NISTサイバーセキュリティフレームワークの改定や、サプライチェーンにおけるサイバーセキュリティ向上のためのイニシアチブの立ち上げが検討されているほか、ISO/IEC27000シリーズについても、新たな脅威への対応やサプライチェーン対策の必要性の高まりを踏まえた改定作業が行われている。

【米国】NIST-CSFの改定

- NISTは、**サイバーセキュリティフレームワーク(NIST-CSF)（2014年にv1.0、2018年4月にv1.1公表）について、**サイバーセキュリティのリスク、技術、リソースの変化を考慮し、**改定に向けた検討を開始**。
- 加えて、サプライチェーンにおけるサイバーセキュリティリスクに対処するため、官民のパートナーシップによる**「サプライチェーンにおけるサイバーセキュリティ向上のための国家イニシアチブ（NIICS）」を立ち上げ**ることを発表。
- NIST-CSFの改定及びNIICSの方向性の検討に向け、2/22-4/25でRequest For Information (RFI)を実施中。

＜RFIの内容＞

- NIST-CSFv1.1の利用方法、利用メリット、課題、改善すべき点、改定のインパクト等の情報
- 他のリスクマネジメントリソース（NIST-IR8286、ソフトウェア・IoT・制御システムに関する文書、NICEフレームワーク等）との整合性や統合性を向上させるための提案
- NIICSで取り組むべき課題、サプライチェーンにおけるサイバーセキュリティ関連のリスクを管理するために必要なアプローチ・ツールに関する情報

【国際標準】ISO/IEC 27000シリーズ関係

- 情報セキュリティ管理策の実践のための規範である**ISO/IEC27002**について、構成の再編や、**新しい脅威や技術動向に合わせた新規管理策（脅威インテリジェンス、クラウドサービス利用のための情報セキュリティ等）の追加**を行う改定作業が進行中。改定後速やかに、ISO/IEC 27001 Annex Aも改定される見込み。

- ISO/IEC 27001や27002におけるサプライチェーンのセキュリティ対策を詳細化した国際標準である**ISO/IEC 27036シリーズ**についても整備が行われており、要求事項や**ハードウェア・ソフトウェア・サービスのサプライチェーン・セキュリティの改定作業（SBoM関連の追記等の検討）**が進行中。

③国際会議への出席

- 「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）」の紹介や日米EUサイバー演習の結果共有により、関係国とのサイバー・フィジカル・セキュリティに関する共通認識を醸成し、インド太平洋地域での能力構築の重要性の理解を深めた。

- **Cybertech Dubai 2021（2021年4月@オンライン）**
  - イスラエル発の国際的フォーラムにおいて、CPSF、IoT SSF、SC３、「サイバーセキュリティお助け隊」の取組を紹介。
- **第11回日EU　ICT戦略WS（2021年4月@オンライン）**
  - EUとの政府間WSの場で、CPSF、IoT SSF、SC３、「サイバーセキュリティお助け隊」、日米EUサイバー演習の取組を紹介。
- **第8回日米サイバー対話課長級会合（2021年5月@オンライン）**
  - 米国との協議の場で、CPSF、SC3、「サイバーセキュリティお助け隊」、日米EUサイバー演習の取組を紹介。
- **第2回日独サイバー協議（2021年5月@オンライン）**
  - 独との協議の場で、日米EUサイバー演習の取組を紹介。
- **第6回日英サイバー協議（2021年6月@オンライン）**
  - 英国との協議の場で、CPSF、OSSガイドライン、「サイバーセキュリティお助け隊」、SC3、日米EUサイバー演習の取組を紹介。
- **第１４回 日･ASEAN サイバーセキュリティ政策会議（2021年10月@オンライン）**
  - ASEAN加盟諸国との協議において、日米EUサイバー演習の取組を紹介。
- **第12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（2021年11月@オンライン）**
  - 米国との政府間局長級対話において、日米EUサイバー演習の取組を紹介。
- **第4回日エストニア･サイバー協議（2021年12月@オンライン）**
  - エストニアとの協議の場で、能力構築の事例として、日米EUサイバー演習の取組を紹介。
- **Cybertech Tokyo 2022（2022年2月@オンライン）**
  - イスラエル発の国際的フォーラムにおいて、CPSF等の取組及び日イスラエル協力の重要性について言及。

※　2021年9月の日米豪印首脳会議において、日米豪印サイバー上級グループを立ち上げることに合意。

④関係国の官民との連携

- 公式な国際会議や、インド太平洋を中心とした能力構築支援の他、関係各国の政府機関・関連組織との連携強化を推進している。

関係機関との連携例

＜米国＞
- 国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁（DHS/CISA）、国務省（DOS）、エネルギー省（DOE）との間で、日米EU産業制御システムサイバーセキュリティ演習の開催等に向けて日々連携しているほか、DHS/CISAとの間ではハイレベルも含めて意見交換を実施。昨年12月には、DHS/CISAが主催するSBOMのイベント（SBOM-a-rama）にも登壇し、経済産業省の取組を紹介。
- また、現地の業界団体・シンクタンク・コンサルティング会社等との間でも、米国大統領令を踏まえた対応状況等をはじめとしたテーマについて意見交換を実施。

＜イスラエル＞
- イスラエル国家サイバー総局（INCD）との間で、中小企業向けのサイバーセキュリティに関する支援施策等について数次にわたり意見交換を実施。

＜EU＞
- 通信総局（DG CONNECT）等との間で、日米EU産業制御システムサイバーセキュリティ演習の開催等に向けて日々連携。
- また、現地のシンクタンクとの間でも、経済産業省の取組の紹介や、日EU連携などに関する意見交換を実施。

＜英国＞
- 英デジタル・文化・メディア・スポーツ省（DCMS）及び英国家サイバーセキュリティセンター（NCSC）との意見交換を行い、CPSF、IoT-SSF、人材育成スキームについて紹介し、英国の取組について聴取。
- 英国財務報告評議会（FRC）との間で、サイバーセキュリティにかかる情報開示に関する意見交換を実施。

＜国際組織＞
- EIS Council※との間で、サプライチェーンリスク管理の強化を目的としたCPIC（Cyber Product International Certification）に関する意見交換を実施した他、関連イベント等に登壇。

※Electric Infrastructure Security Council －重要インフラに対するサイバー攻撃等の脅威に対処するための国際組織

本日ご議論いただきたいポイント（国際）

- サイバーセキュリティ分野の国際協力・制度調和の推進に向け、主に以下の点について、ご意見等いただきたく存じます。

国際

- 今後の経済産業省の施策推進や、国際協力・制度調和などに向け、特にフォローすべき海外の動向、連携すべき海外の機関等
  - ソフトウェア、IoT、セキュリティマネジメント等
- ICSCoEの国際的な中核拠点としての位置づけ・方向性

０．全体像

１．経営

２．中小企業

３．人材

４．地域

５．国際

６．本日議論いただきたい論点

本日ご議論いただきたいポイント

- 主に以下の点について、ご意見等いただきたく存じます。

各分野における論点の例

経営

- 経営ガイドラインの改訂において、考慮すべき状況変化等
- サイバーセキュリティ経営の促進のために経営者に発信していくべき情報や、投資家等ステークホルダーを通じた対策促進の方法（例:どのような施策・文書等と紐付けていくべきか）

中小

- これまでのサプライチェーン・地域ベースの取組や実態調査結果踏まえた、今後取り組むべき中小企業関連政策の方向性
  - 取引関係における対策要請・支援の在り方
  - 地域金融機関等を通じた普及啓発の在り方
- 中小医療機関や経済安全保障上重要なサプライチェーン上の中小企業のサイバーセキュリティ等に対する取組の方向性

人材

- プラス・セキュリティの取組の普及のための施策の在り方
- 地域SECUNITY等を通じた、地域における産学官連携の加速化

国際

- 今後の経済産業省の施策推進や、国際協力・制度調和などに向け、特にフォローすべき海外の動向、連携すべき海外の機関等
  - ソフトウェア、IoT、組織、規制等
- ICSCoEの国際的な中核拠点としての位置づけ・方向性