経済産業省

サイバーセキュリティ経営の実現に向けた政策について

経済産業省　商務情報政策局
サイバーセキュリティ課 課長補佐
原田 典明

１．はじめに
～サイバー攻撃の脅威レベルの向上と海外の動き

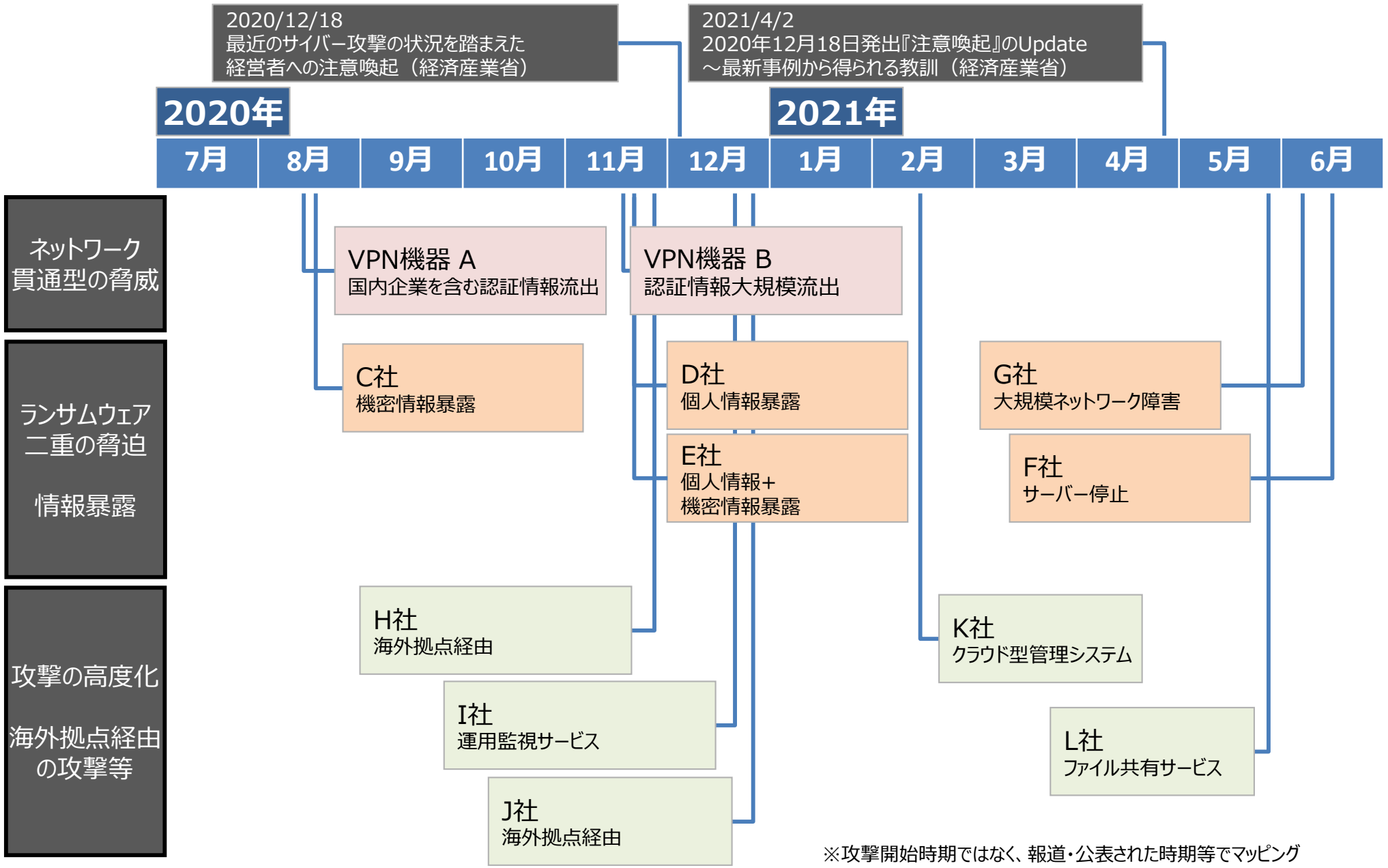
２．サイバーセキュリティ対策の基盤整備
～経営者の意識喚起、人材育成、情報共有、初動対応、重要インフラ支援

・サイバーセキュリティ経営ガイドライン
・経営プラクティス集
・サイバーセキュリティ体制構築・人材確保の手引き
・可視化ツール

３．中小企業のセキュリティ対策支援

・中小企業の情報セキュリティ対策ガイドライン
・サイバーセキュリティお助け隊実証事業（2019・2020年度）

2020～2021年の主なサイバー攻撃事案



※攻撃開始時期ではなく、報道・公表された時期等でマッピング

昨今のサイバーセキュリティに係る状況：日々高度化するサイバー攻撃への継続的な対応が肝要に

2020年6月12日公開資料

- 2月14日〆切の「報告の依頼」に基づく企業からの報告では、**サイバー攻撃によって重要な情報が漏えいしたとの報告はなかった**（ただし、〆切後に検知した事案で現在継続調査中の案件はあり。）。
- 一方、報告の内容や昨今のサイバー事案からは、**サイバー攻撃が日々高度化**していることが明らかになっており、**継続的にサイバーセキュリティ対策の状況を点検していくことがますます重要**に。

＜サイバー攻撃による昨今の被害の特徴＞

標的型攻撃の更なる高度化

- **マルウェア添付メール経由での感染等に加え、**ネットワーク機器の脆弱性や設定ミスを利用して侵入経路を確立するなど、メール開封等の**ユーザーの動作を介さずに直接組織内のシステムに侵入する手法等を確認**。
- 加えて、侵入後も、PowerShell等を用いたファイルレスの攻撃や、C&Cサーバとの通信の暗号化、痕跡の消去など、**攻撃の早期検知と手法の分析を困難にする攻撃手法**を確認。

サプライチェーンの弱点への攻撃

- 海外拠点や取引先など、**サプライチェーンの中で相対的にセキュリティが弱い組織が攻撃の起点**となり、そこを踏み台に侵入拡大が図られる事例が増加。
- 企業がグローバルにビジネス活動を拡大し、活動内容の統合レベルを上げていくほど、インシデント発生時の被害も大きくなるおそれ。影響範囲を限定するためのシステムの階層化など、**海外子会社等も含めた対応体制の整備が一層必要**に。

不正ログイン被害の継続的な発生

- ID・パスワードのみで利用可能な会員制サイトやクラウドメールアカウント等が、流出したID・パスワードのリストを利用した「**リスト型攻撃**」により**不正ログインされる事案が継続的に発生**。
- ログイン機能に二段階認証や二要素認証を導入することで**ウェブサイトへのアクセスに係るセキュリティを強化**したり、個人情報を機微度に応じて分割して管理し、各データへのアクセス権を別に設定するなどの**システム構造の見直し**が大切に。

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

「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」

2020年12月18日公開資料

●サイバー攻撃は規模や烈度の増大とともに多様化する傾向にあり、**実務者がこれまでの取組を継続するだけでは対応困難**になっている。

●アップデート等の基本的な対策の徹底とともに、**改めて経営者のリーダーシップが必要に**。

① 攻撃は格段に高度化し、被害の形態も様々な関係者を巻き込む複雑なものになり、技術的な対策だけではなく関係者との調整や事業継続等の判断が必要に。改めて経営者がリーダーシップを。

② ランサムウェア攻撃による被害への対応は企業の信頼に直結。経営者でなければ判断できない問題。

●「二重の脅迫※」によって、顧客等の情報を露出させることになるリスクに直面。日常的業務の見直しを含む事前対策から情報露出に対応する事後対応まで、経営者でなければ対応の判断が困難。

●金銭支払いは犯罪組織への資金提供とみなされ、制裁を受ける可能性のあるコンプライアンスの問題。

③ 海外拠点とのシステム統合を進める際、サイバーセキュリティを踏まえたグローバルガバナンスの確立を。

●国・地域によってインターネット環境やIT産業の状況、データ管理に係るルール等が異なっており、海外拠点とのシステム統合を通じてセキュリティ上の脆弱性を持ち込んでしまう可能性も。

●拠点のある国・地域の環境をしっかりと評価し、リスクに対応したセグメンテーション等を施したシステム・アーキテクチャの導入や拠点間の情報共有ルールの整備等、グローバルガバナンスの確立が必要。

④ 基本行動指針（高密度な情報共有、機微技術情報の流出懸念時の報告、適切な場合の公表）**の徹底を。**

※攻撃者が、被攻撃企業が保有するデータ等を暗号化して事業妨害をするだけではなく、暗号化する前にあらかじめデータを窃取しておいて支払いに応じない場合には当該データを公開することで、被攻撃企業を金銭の支払いに応じざるをえない状況に追い込む攻撃形態。

経済産業省「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起（2020年12月18日）」https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html

１．はじめに
～サイバー攻撃の脅威レベルの向上と海外の動き

２．サイバーセキュリティ対策の基盤整備
～経営者の意識喚起、人材育成、情報共有、初動対応、重要インフラ支援
- ・サイバーセキュリティ経営ガイドライン
- ・経営プラクティス集
- ・サイバーセキュリティ体制構築・人材確保の手引き
- ・可視化ツール

３．中小企業のセキュリティ対策支援
- ・中小企業の情報セキュリティ対策ガイドライン
- ・サイバーセキュリティお助け隊実証事業（2019・2020年度）

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＞

1st step

サイバーセキュリティ経営ガイドラインの概要

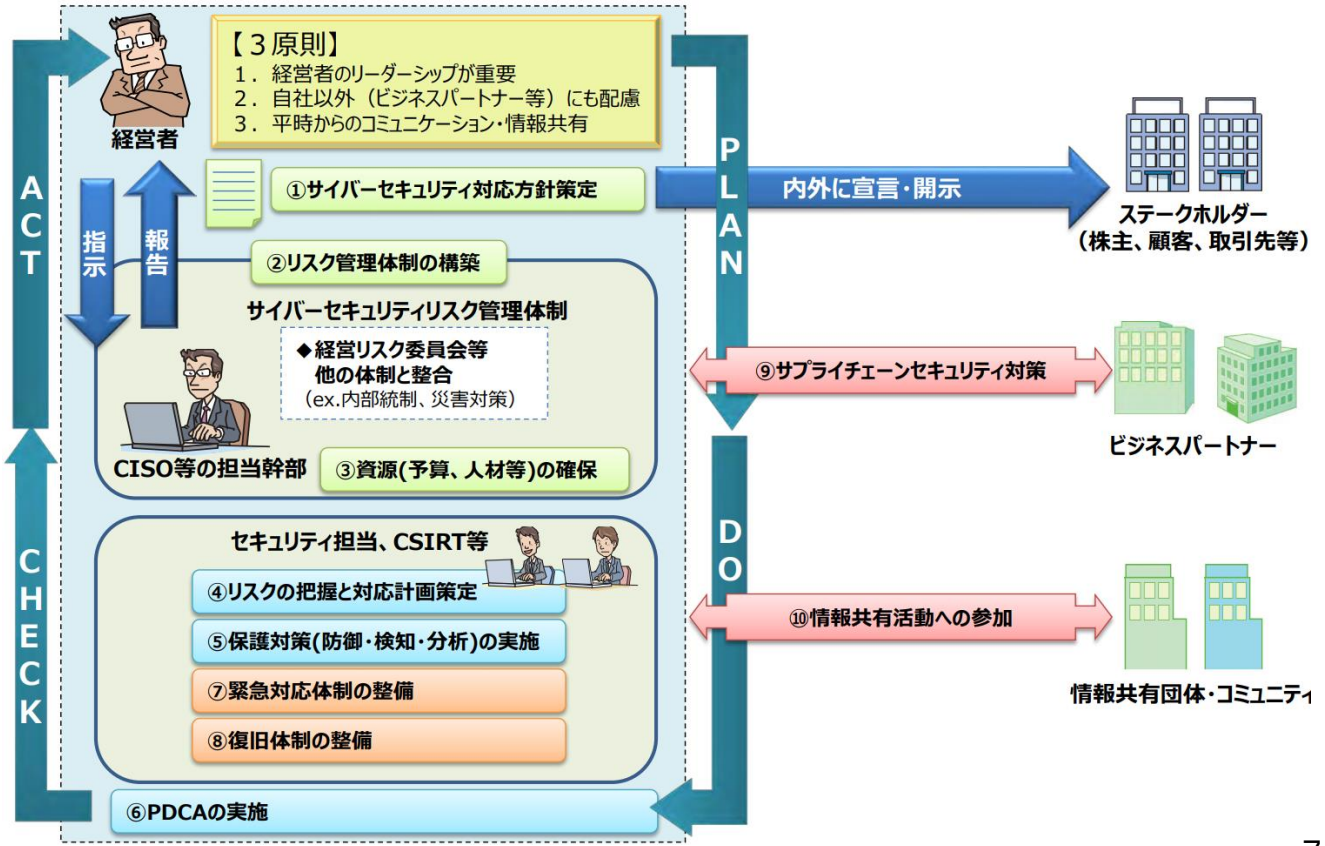
- セキュリティはコストではなく投資であると位置づけ、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要であることを示したガイドライン。
- 経営者が認識すべき３原則を維持しつつ、基本構成を見直し、経営者がCISOに指示すべき10の重要項目をその対策例とともに提示

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



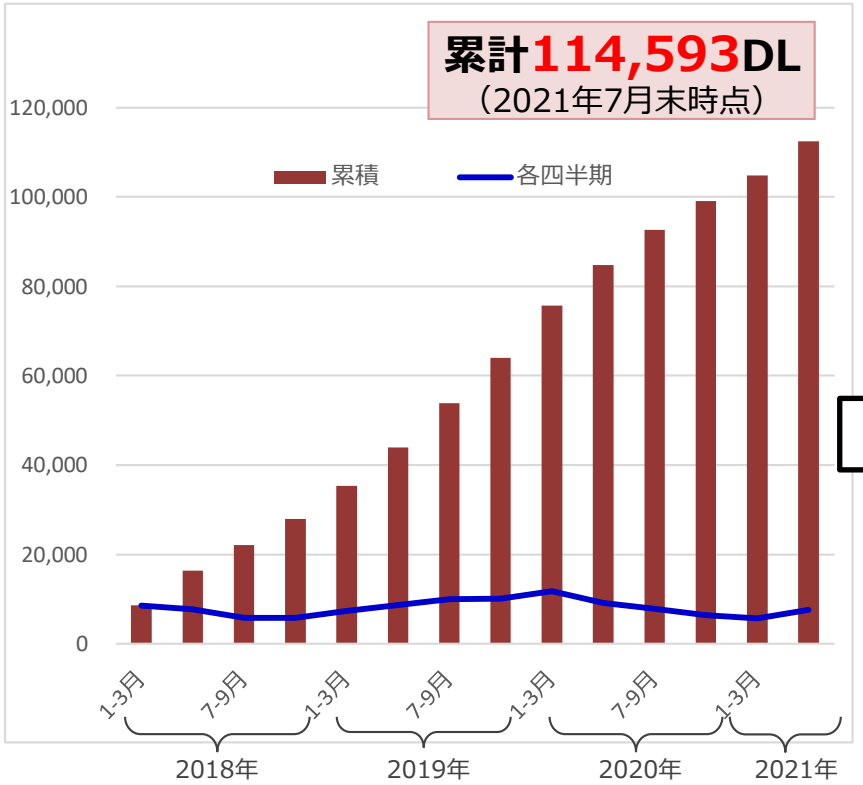
サイバーセキュリティ経営ガイドラインの利用状況

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（Ver2.0）

1st step

- 2017年11月公開のVer2.0は、ダウンロード数累計約１１万件と注目度の高い状況が続いている。
- 特に資本金100億円以上、総従業員数5,001人以上の企業において、約60%の企業が当該ガイドラインを活用。

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

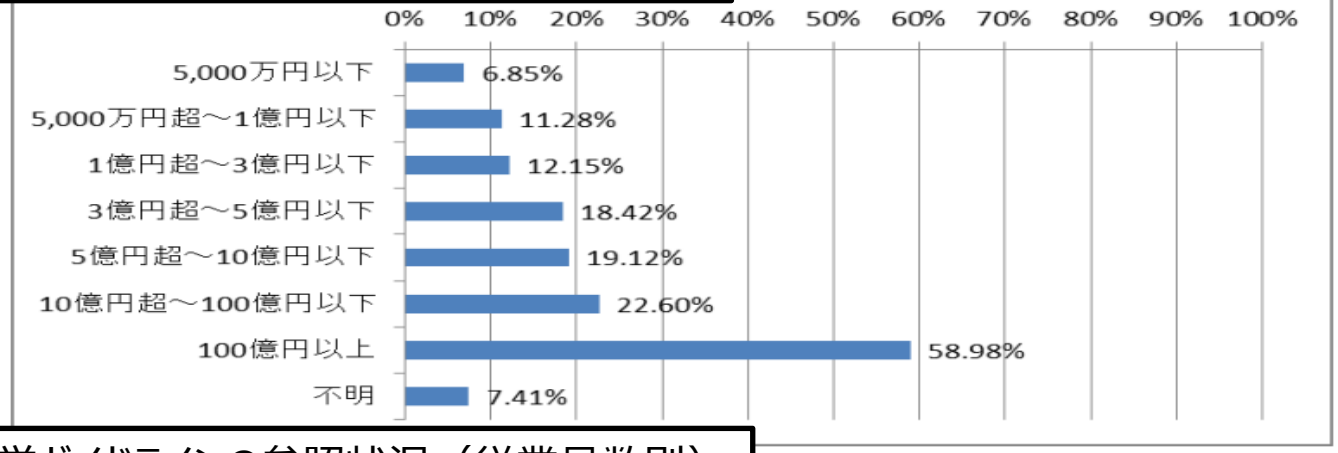


【参考】上場企業数　第一部　2,190社
　　第二部　474社

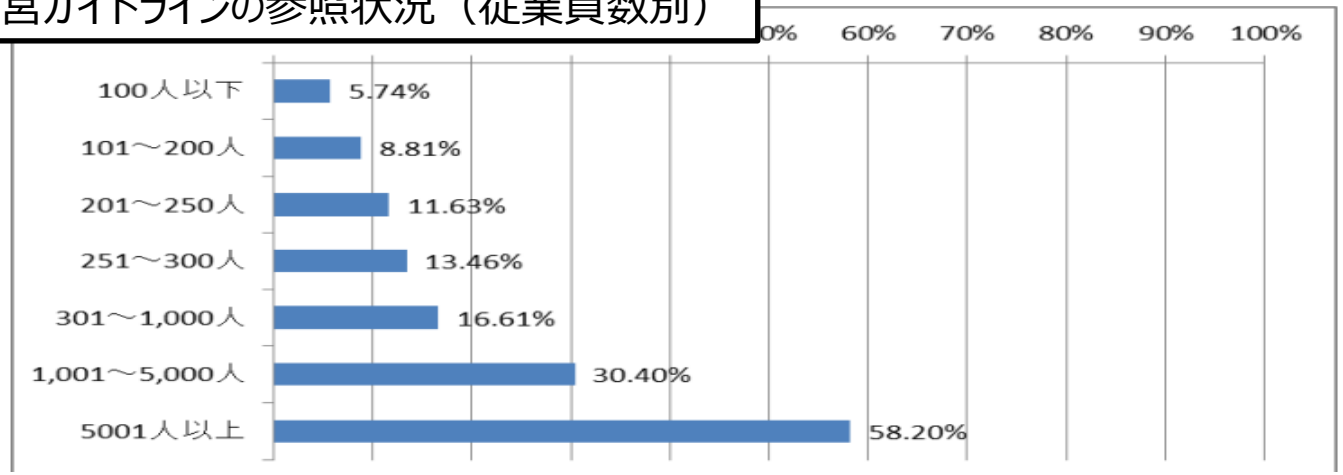
日本取引所グループ公表
2021年6月30日時点

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

経営ガイドラインの参照状況（資本金別）



経営ガイドラインの参照状況（従業員数別）



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

- 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
- 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

- 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

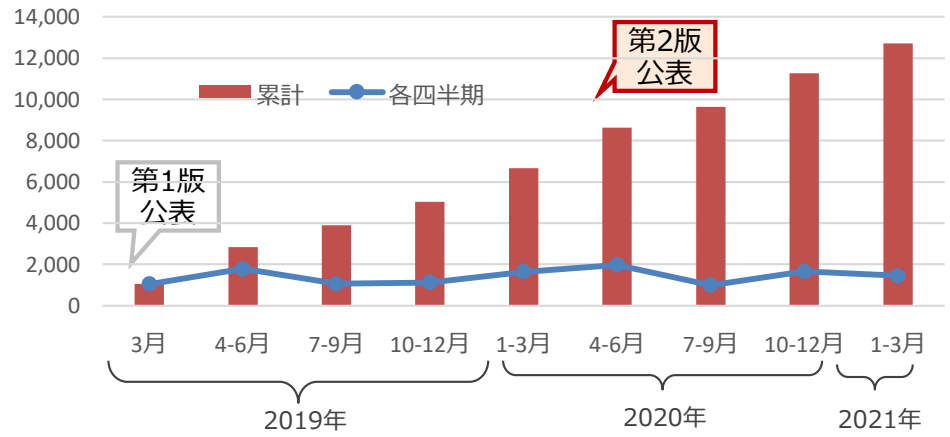
『サイバーセキュリティ経営ガイドラインVer2.0実践のためのプラクティス集』

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。プラクティスを追加した**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**を実施中。2021年4月にIPAより調査結果を公表。

<プラクティス集のダウンロード数推移>

累計**14,989**DL (2021年7月末時点)



【参考】上場企業数　第一部　2,192社
　　第二部　474
（日本取引所グループ公表 2021年５月31日時点）

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

<2020年度調査結果>

文献調査（6件）／アンケート調査（930社）／有識者インタビュー（3名）／企業インタビュー（5社）

◆文献調査
- 国内外のセキュリティ関連のプラクティスの多くは、**民間企業などがボランティアで作成・共有**している。

◆アンケート調査
- 企業ユーザのプラクティス集の**認知度は4割強**で、**インシデント発生時に備えた**セキュリティ強化を目的として活用されている。
- 半数以上の企業ユーザが**プラクティス集**のようなセキュリティ対策事例の**必要性**を感じており、**プラクティス集の作成に協力的**である。

◆有識者・企業インタビュー
- **「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」と連携**し、企業が本ツールを用いて自己診断を行った結果、対策レベルの低い項目について、プラクティスの事例を表示させることができると良い。
- 現在、企業が直面しているセキュリティの脅威に対して打てる**具体的な対策が示されている**と良い。

『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。プラクティスを追加した**第2版を2020年6月3日に公表**。

＜特徴＞

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

＜イメージ＞

累計14,989DL
（2021年7月末時点）

＜構成＞

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

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

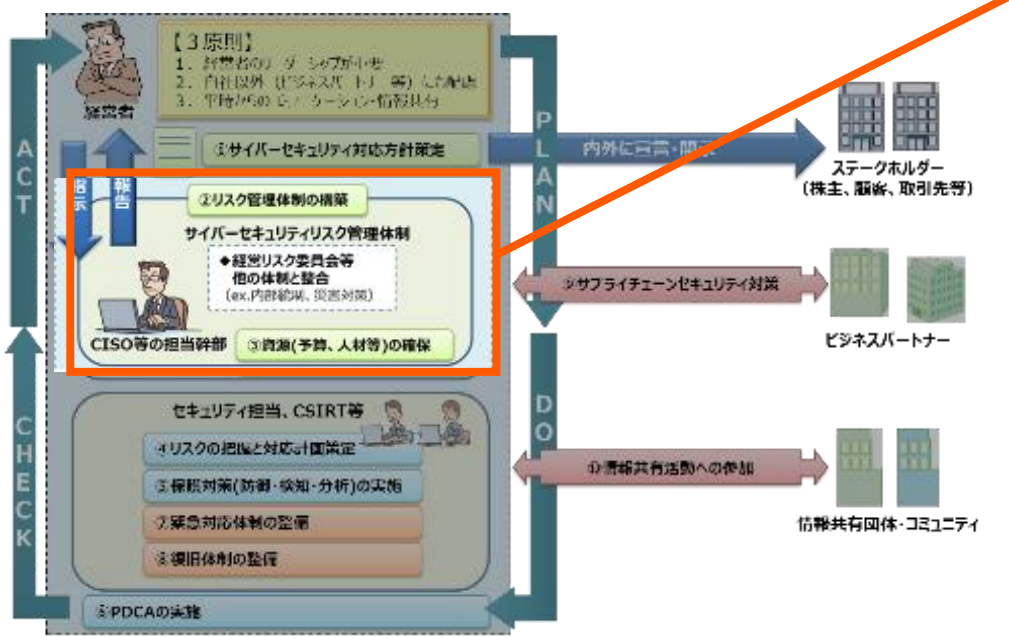
『セキュリティ体制構築・人材確保の手引き』の開発

累計6,925ダウンロード
（2021年6月末時点）

2nd step

- サイバーセキュリティ経営ガイドラインの付録Fとして**2020年9月30日に第１版を公表。**
  今後の課題としていた箇所を更新した**第1.1版を2021年4月15日に公表。**

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

第1.1版での更新ポイント（例）：

- サイバーセキュリティ対策に従事する人材の確保
- ユーザー企業で必要となるスキルの習得に活用可能な資格制度
- ユーザー企業でサイバーセキュリティ対策に従事する人材の育成パスのイメージ

https://www.meti.go.jp/press/2021/04/20210426002/20210426002.html

（参考）『セキュリティ体制構築・人材確保の手引き』で扱う主要な概念の解説

セキュリティ統括機能

- セキュリティ対策及びインシデント対応において、CISOや経営層を補佐してセキュリティ対策を組織横断的に統括することにより、企業におけるリスクマネジメント活動の一部を担う
- 「機能」であって「組織」として設置しなくてもよい（状況に応じて、最適な形態は異なる）
  - 独立した組織として設置
  - 管理部門の１機能として割当
  - 情シス部門の１機能として割当
  - 組織横断的な委員会形態で運用

ITSS+（セキュリティ領域）

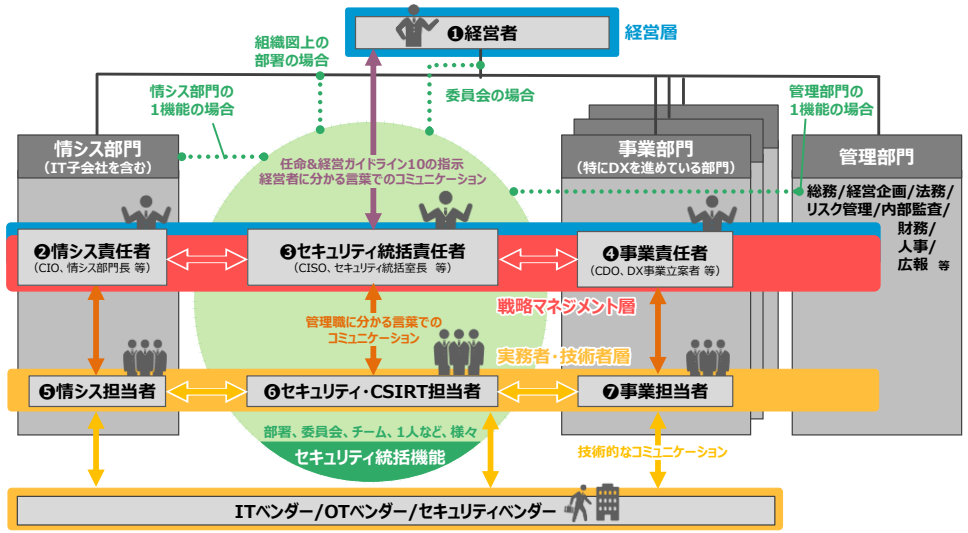
- 企業のセキュリティ対策に必要となる関連業務のまとまりを17分野に整理したもの
- セキュリティの専門性の高い分野だけでなく、経営層や法務部門、事業ドメインまで、サイバーセキュリティ対策に関わる幅広い領域を網羅
- DXの取り組みを通じたクラウド化、アジャイル開発、開発・セキュリティ対策・運用の一体化（DevSecOps）等の動きの中、ITSS＋で定める各分野の境界は曖昧化の傾向

プラス・セキュリティ

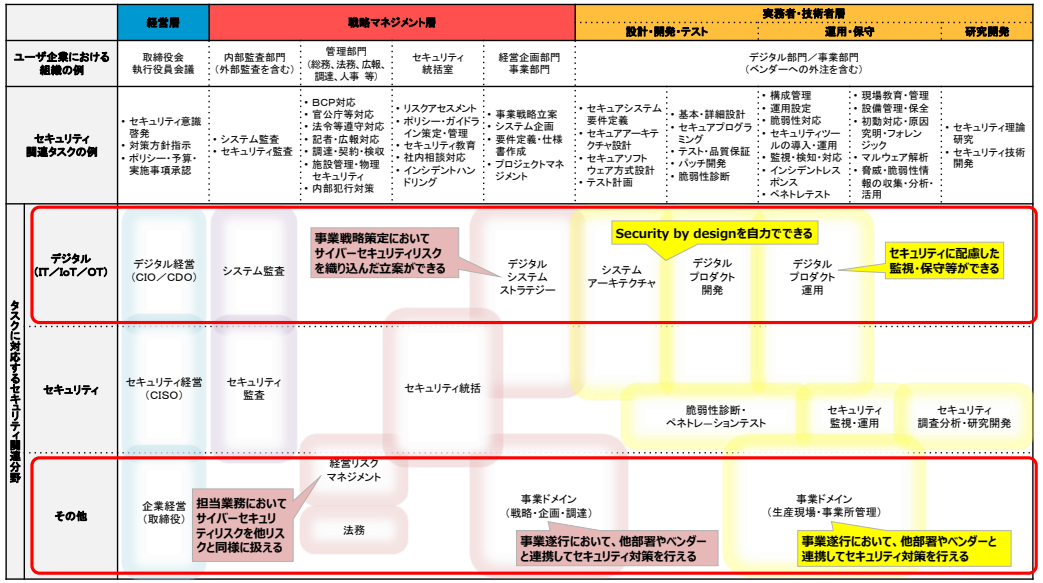
- セキュリティ対策を本務としないが、業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策の実践が求められる業務が「プラス・セキュリティ」の対象
- 「プラス・セキュリティ」人材が業務担当者と別に存在するわけではなく、これまでの業務担当者がサイバーセキュリティの知識・スキルを習得し、実践することを通じて対策を担う
- DXの取り組み有無に関わりなく、ITを活用するすべての企業において必要

セキュリティ統括機能のイメージ

企業の組織構造や事業内容に応じて下図の緑色部分の実現方法の検討が必要



ITSS＋（セキュリティ領域）（赤枠が「プラス・セキュリティ」の分野）

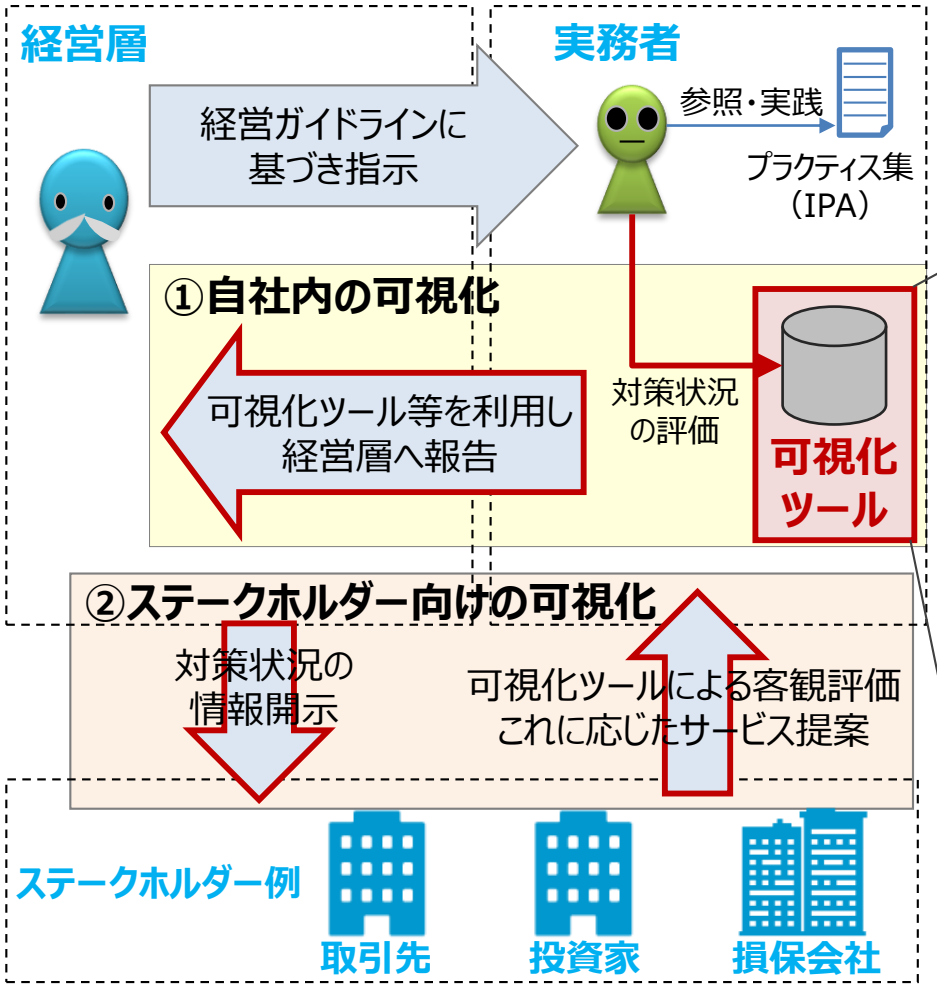


サイバーセキュリティ経営ガイドライン実践状況の可視化ツールを公開

2nd ～ 3rd step

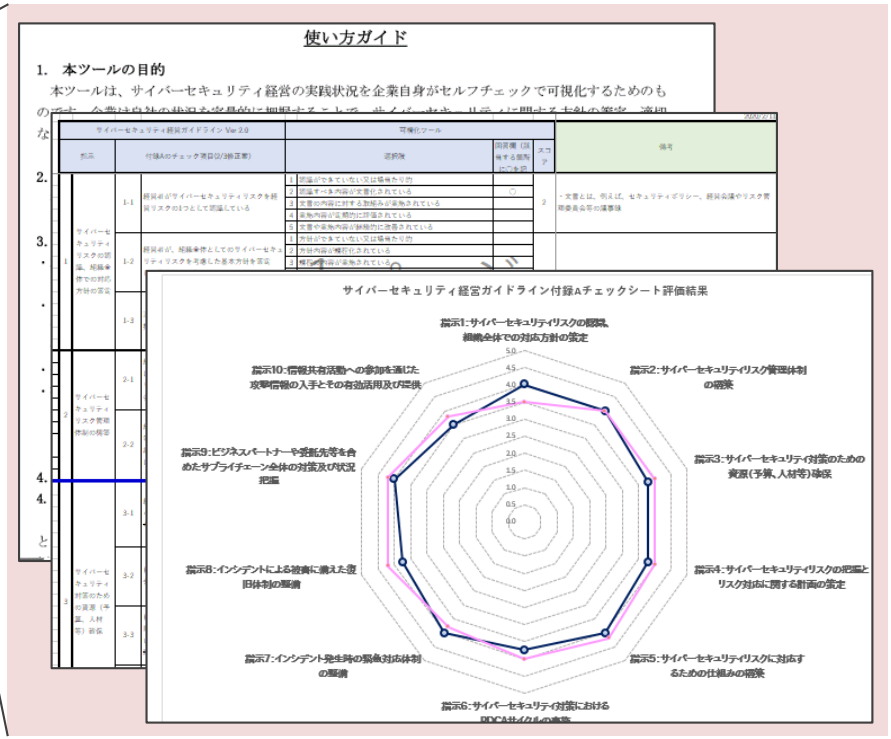
- 2020年3月25日、可視化ツールβ版（Excel）をIPAから公開。
- 2020年度はユーザ企業、投資家等ステークホルダーを対象にβ版評価を行い、**2021年８月16日にVer1.0（Web版）をリリース。** https://www.ipa.go.jp/security/economics/checktool/index.html

累計**6,387**ダウンロード
（2021年７月末時点）



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



１．はじめに
～サイバー攻撃の脅威レベルの向上と海外の動き

２．サイバーセキュリティ対策の基盤整備
～経営者の意識喚起、人材育成、情報共有、初動対応、重要インフラ支援
- ・サイバーセキュリティ経営ガイドライン
- ・経営プラクティス集
- ・サイバーセキュリティ体制構築・人材確保の手引き
- ・可視化ツール

３．中小企業のセキュリティ対策支援
- ・中小企業の情報セキュリティ対策ガイドライン
- ・サイバーセキュリティお助け隊実証事業（2019・2020年度）

中小企業のセキュリティ対策支援

● 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。15万者を超える中小企業が宣言（2021年6月末時点）。

★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

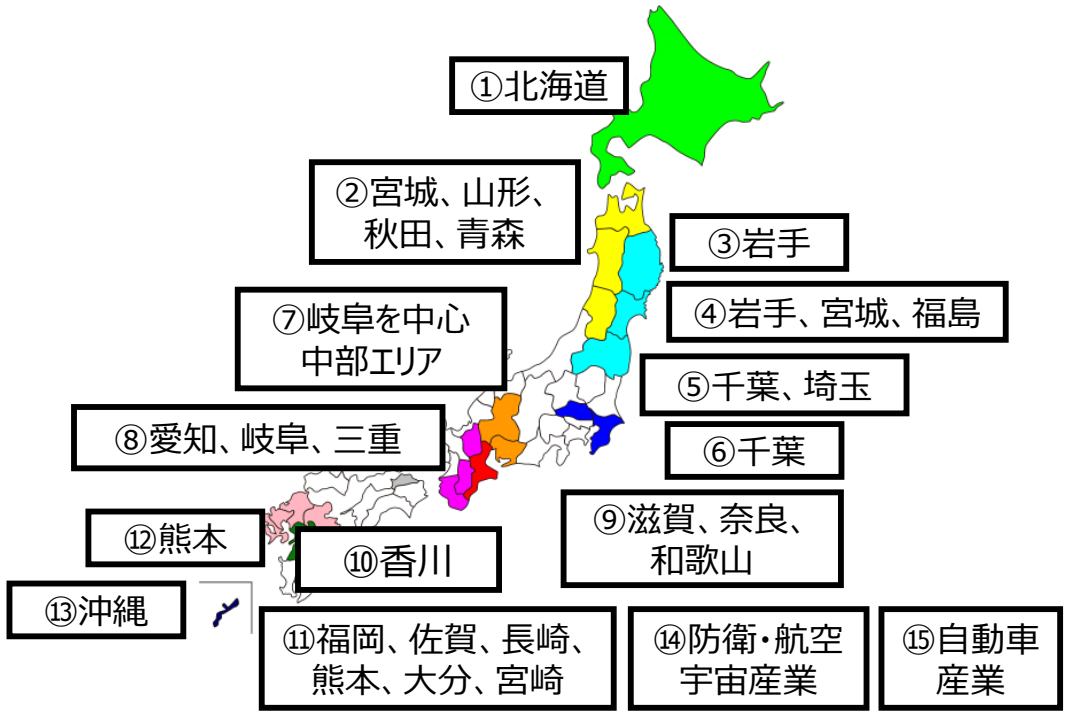
相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など中小企業のサイバーセキュリティ対策に不可欠な各種サービス内容を要件としてまとめた基準を満たすサービス。（2021年7月時点で5サービス）

サイバーセキュリティ
CSお助け隊

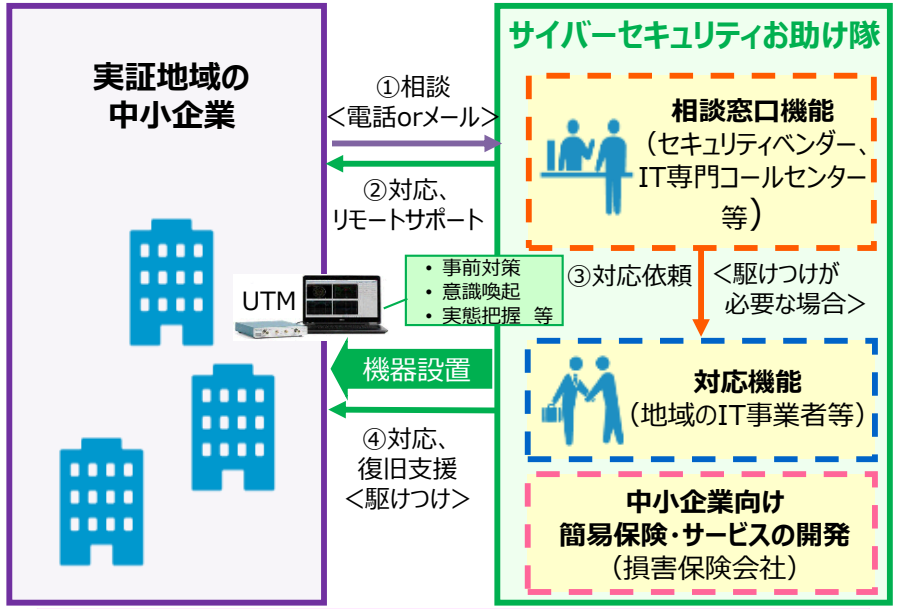
サイバーセキュリティお助け隊実証事業（2019･2020年度）

- 地域の団体、セキュリティ企業、保険会社がコンソーシアムを組み、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした実証事業を実施（2019年度：全国で8件、2020年度：全国で15件）。のべ2,181社の中小企業が参加。
- ２年間にわたる実証事業を通して、サイバーセキュリティに関する中小企業の実態を把握。2021年度より簡易サイバー保険を含むサイバーセキュリティお助け隊の民間自走化を促進すべく、お助け隊サービス基準を策定し、同基準を満たすサービスの審査登録制度の運営を開始。

＜2020年度の実証地域＞



＜実証のイメージ＞



中小企業　側
- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上　　等

保険会社、セキュリティベンダー　側
- 中小企業のセキュリティ対策状況の把握
- 中小企業の被害実態の把握
- 中小企業が求めるサービスの把握　　等

※2019年度実証地域（全8地域、1064社の中小企業が参加）：
①宮城、岩手、福島②新潟③長野、群馬、栃木、茨城、埼玉④神奈川⑤石川、富山、福井⑥愛知⑦大阪、京都、兵庫⑧広島、山口

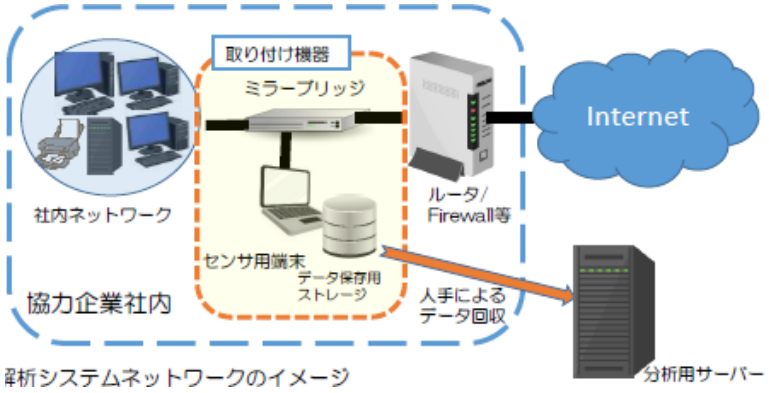
中小企業に対するサイバー攻撃の調査・分析結果（大阪商工会議所）

● 地域の中小企業も、例外なくサイバー攻撃の脅威にさらされている。

中小企業被害実態に関する調査

■調査内容

実証期間：平成30年9月～平成31年1月
実証内容：中小企業30社を対象に、ネットワーク上の通信データ等を一定期間収集。



解析システムネットワークのイメージ

■ 調査結果

- 調査した**30社全てでサイバー攻撃に繋がりうる不審な通信**が記録されていた。
- 少なくとも5社ではコンピューターウイルスに感染するなどして、**情報が外部に流出したおそれ**があることが分かった。

出典：大阪商工会議所「平成30年度中小企業に対するサイバー攻撃実情調査（報告）」共同研究実施者：神戸大学、東京海上日動火災保険（株）（2019年7月）

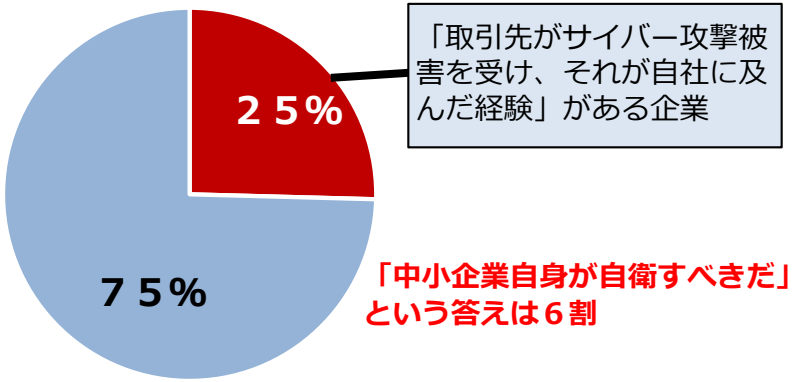
取引先経由の被害に関する調査

■調査内容

調査期間：平成31年2月～3月
調査内容：全国の従業員100人以上の企業を対象に、郵送、FAX、メール、Web、対面による依頼・回答

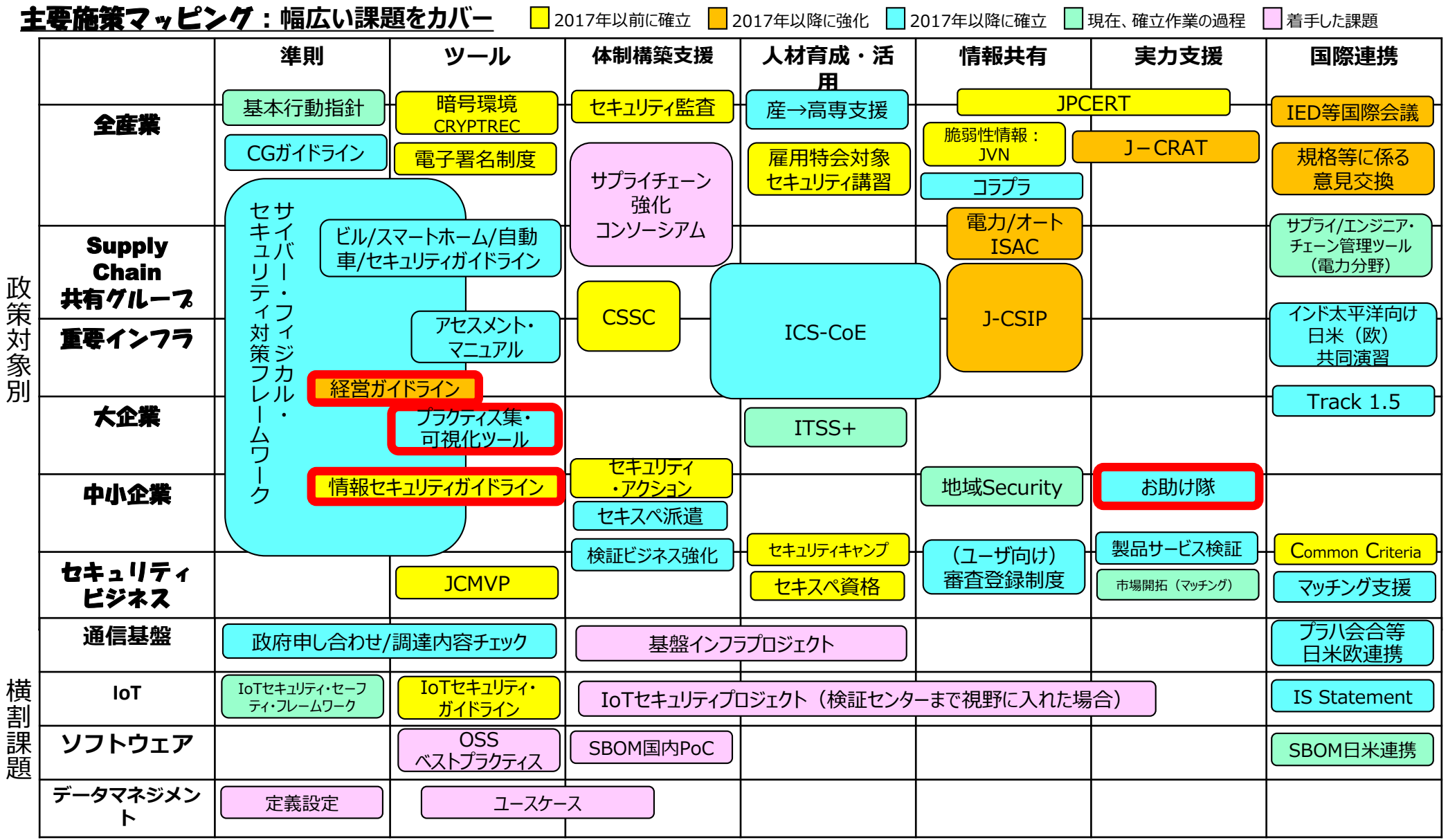
■調査結果

- 大企業・中堅企業118社に調査したところ、取引先がサイバー攻撃被害を受け、**影響が自社に及んだ経験**がある企業が30社あった（**25%**）



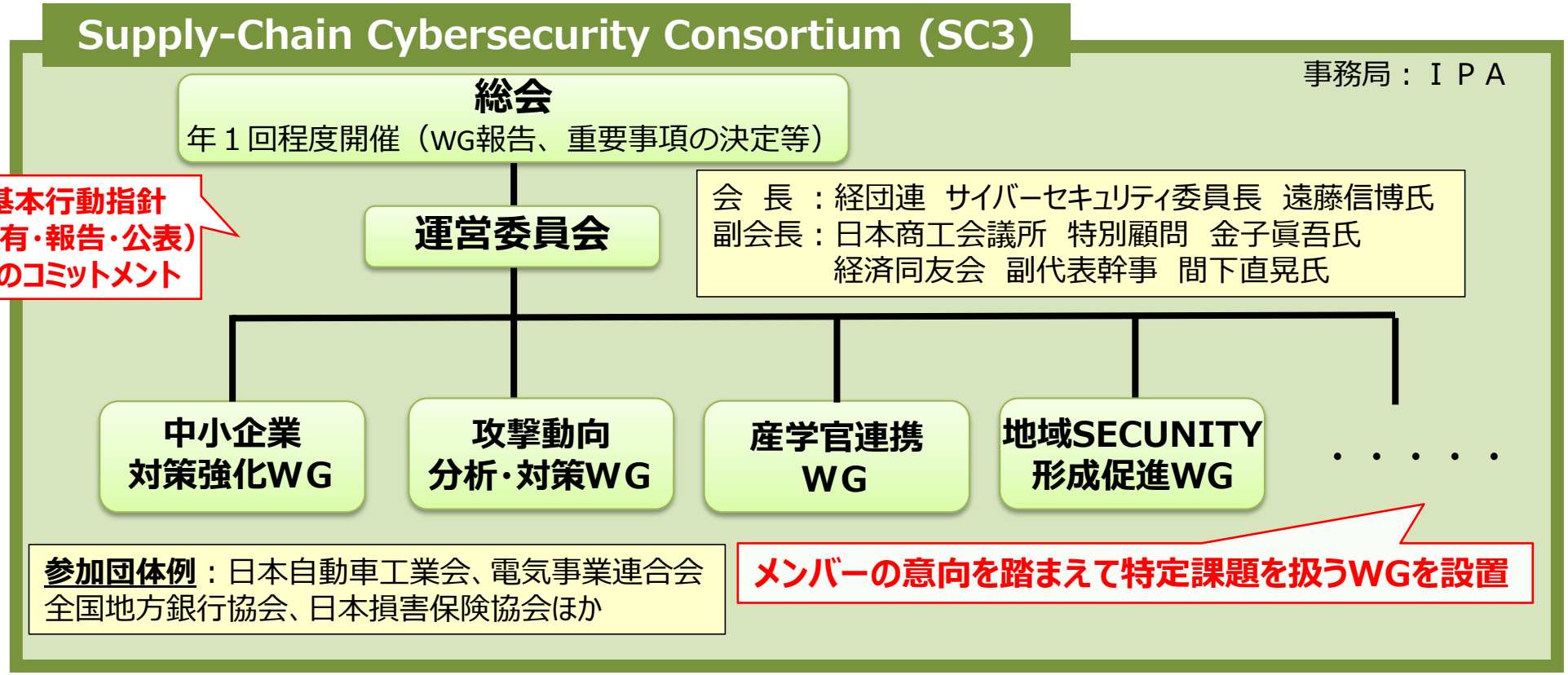
出典：大阪商工会議所「サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査」（2019年5月）

経済産業省における主要なサイバーセキュリティ政策のマッピング



サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）

- **趣　旨:** 大企業と中小企業がともにサイバーセキュリティ対策を推進するためのコンソーシアムを立ち上げ、「基本行動指針※」の実践と中小企業・地域を含めたサプライチェーンのサイバーセキュリティ対策を産業界全体の活動として展開していく。
  ※サイバー攻撃事案発生時における、「共有、報告、公表」によるリスクマネジメントの徹底。
- **参加者:** 経済団体、業種別業界団体　等（2021年７月末時点で171会員）
- **設立日:** 2020年11月1日（設立総会：2020年11月19日）
- **活　動:** 特定の課題についてWGを設置し、具体的アクションを展開。



SC3の全体像

- 産業界全体で取り組むべきサプライチェーンセキュリティ対策の議論・浸透のため、SC3に対し、産学官連携や経営層向けの注意喚起、地域・業界別の取組・課題共有等のプラットフォームとしての機能への期待の声が挙がったことを踏まえ、中小企業対策強化WGに加えて、新たに３つのWGを設置。

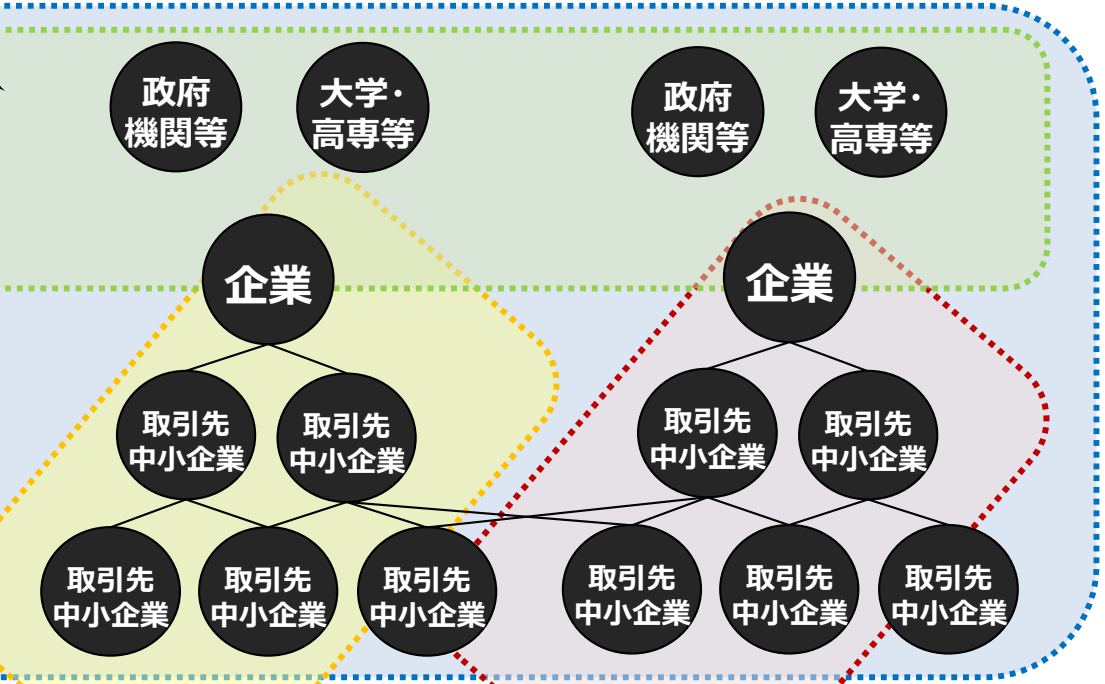
攻撃動向
分析・対策WG

産学官連携WG

- 産学官連携促進
- 人材育成
- 共同研究

地域SECUNITY
形成促進WG

- 地域SECUNITY形成促進
- 悩み・課題共有
- 解決策・プラクティス共有



中小企業
対策強化WG

- 中小企業対策促進
- サイバーセキュリティお助け隊の普及
- 悩み・課題・解決策・プラクティス共有

業別ごとの
サプライチェーン対策

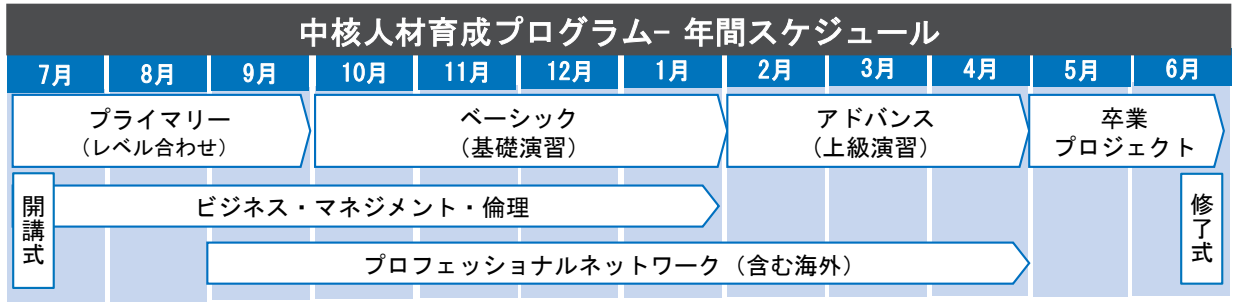
- 業界ごとのサプライチェーン対策取組共有（ビル、自動車、電力、防衛、スマートホーム、宇宙など）

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（2021年7月開講）には、48名が参加。

□ １年を通じた集中トレーニング

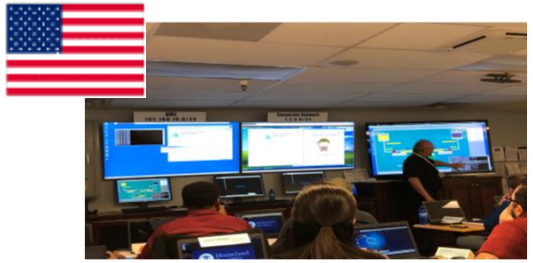
□ 電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人）



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

現場を指揮・指導するリーダーを育成

□ 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

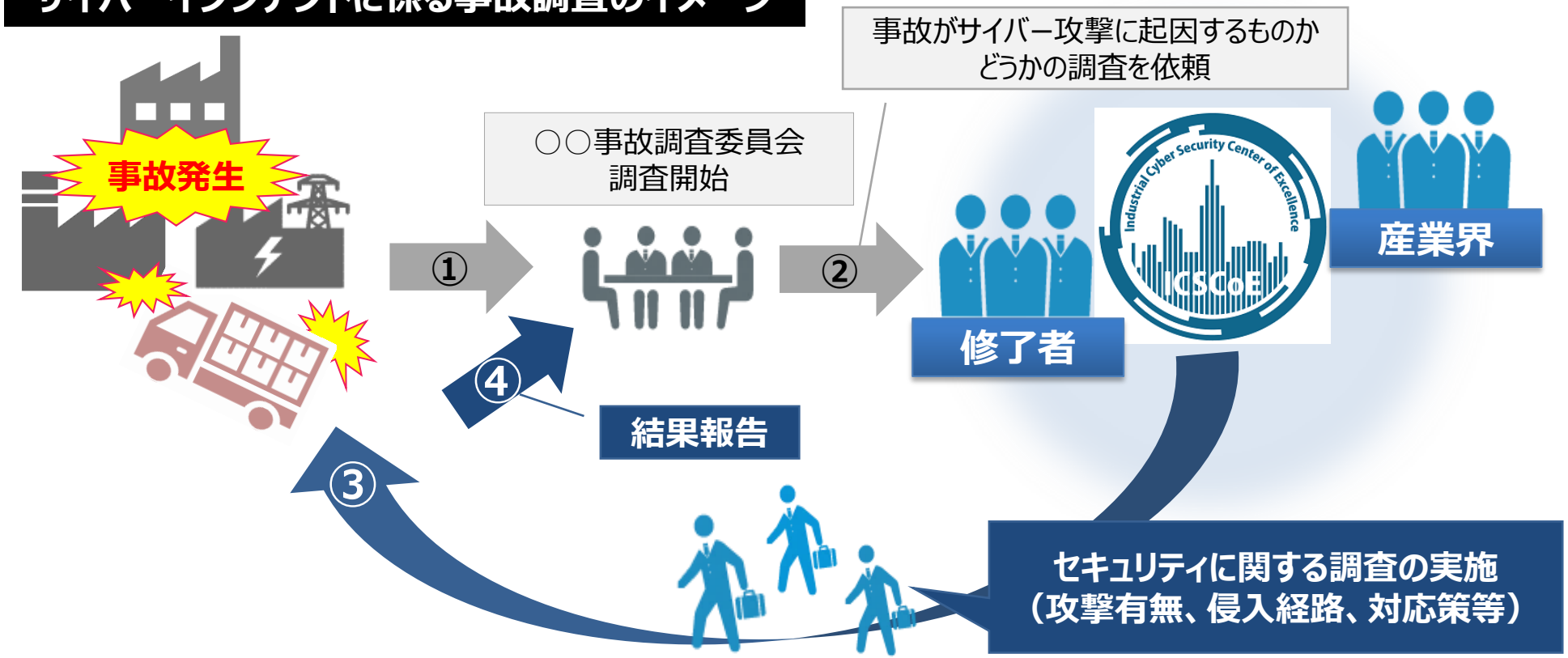
➢ 政府機関、産業界等のセキュリティ専門家との意見交換や研究機関の施設見学等を実施

など

国としての対処能力の強化
～サイバーインシデントに係る事故調査の体制整備に向けた検討の開始

- サイバー攻撃がフィジカル領域に大きな影響を及ぼすようになり、経済活動の基盤を守るためには、**プラント等の事故が発生した場合に、サイバーインシデントの観点からの原因究明可能な機能**を有することが必要に（いわゆる「サイバー事故調」）。
- 産業サイバーセキュリティセンター（ICSCoE）は、**2025年を目途にサイバーインシデントに係る「事故調」機能を整備**するため、事故調査に必要な能力、体制、人材等に係る議論を開始。

サイバーインシデントに係る事故調査のイメージ



国立高専機構と産・官との連携促進・具体化に向けて

- 国立高専におけるセキュリティ教育が産業界の求める人材像とも整合していくためには、産学官の継続的な協力関係が必要。
- これまで国立高専機構がIPAや業界団体（CRIC CSF、JNSA）等と進めてきた連携を効果的かつ継続的なものとするために、SC3の場の活用も含め、産学官連携を推進していく。

＜高専・産・官の対話の場（イメージ）＞

METI
Ministry of Economy, Trade and Industry

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