資料３

経済産業省
Ministry of Economy, Trade and Industry

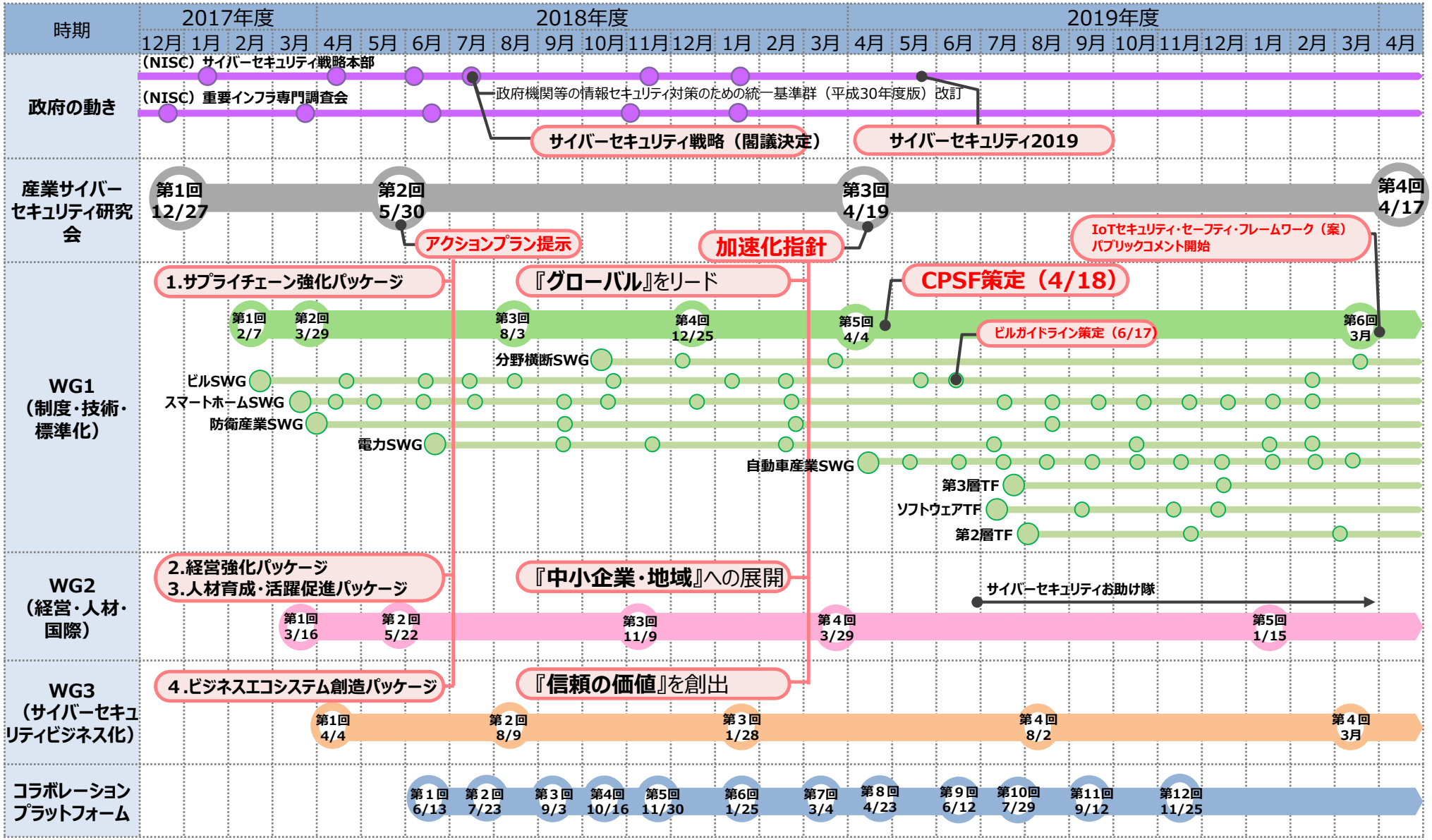
第５回　産業サイバーセキュリティ研究会
事務局説明資料
～アクションプランの持続的発展と、新領域へのチャレンジ～

令和２年６月３０日

経済産業省

商務情報政策局

産業サイバーセキュリティ研究会関連会議の活動状況



（復習）**アクションプランの4つの柱**

第2回研究会（2018年5月30日）において提示

1．サプライチェーンサイバーセキュリティ強化パッケージ

- グローバルサプライチェーンに対応した
  サプライチェーンサイバーセキュリティ強化パッケージ

2．サイバーセキュリティ経営強化パッケージ

- 経営・現場双方の課題に応えるサイバーセキュリティ経営強化パッケージ

3．サイバーセキュリティ人材育成・活躍促進パッケージ

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

4．セキュリティビジネスエコシステム創造パッケージ

- ニーズとシーズをマッチングしてビジネスにつなげる
  セキュリティビジネスエコシステム創造パッケージ

（復習）**３つの「加速化指針」**

第3回研究会（2019年4月19日）において提示

アクションプランを中心した取組を更に加速していくため、以下の3つの視点から重点施策を強化する。

１．『グローバル』をリードする

－G20等を視野に、サイバーセキュリティの取組をリードする

２．『信頼の価値』を創出する~Checked by Japan~

（Proven in Japan）

－「検証」を信頼につなげ、ビジネスにする

３．『中小企業・地域』まで展開する

－社会全体、中小企業・地域までサイバーセキュリティを浸透させる

（復習）産業界へのメッセージ①

第４回研究会（2020年4月17日）において提示

- 攻撃の痕跡を発見しにくいファイルレスマルウェアの利用など**攻撃の高度化**、海外事業所や取引先企業を通じた侵入経路の確立など**攻撃起点の変化・拡大**への対応が必要に。
- 直近、新型コロナウィルスの混乱に乗じて、**ランサムウェアや不正アプリ等の攻撃**も海外を中心に急増。
- 今般の事態を受け、今後、更にデジタル化を推進していくことの必要性が明らかになる中、改めてITシステムや制御システムの**セキュリティ対策の徹底と強化**をお願いしたい。

直近の状況に対応するために取り組んでいただきたいこと

- **新型コロナウィルスを騙る不正アプリや詐欺サイト、フィッシングメール/SMSに注意**すること。
- 上記の取組を効果的に進めるため、**NISCや、IPA、JPCERT等の専門機関からの注意喚起を定期的に確認**すること。
- 機器・システムに対して、**アップデート等の基本的な対策**をできるだけ実施すること（利用環境に依存することに留意）。
- 可能な環境であれば、ランサムウェアに感染した事態に備えて**システムやデータのバックアップと復旧手順を確認**すること。

（復習）**産業界へのメッセージ②**

第４回研究会（2020年4月17日）において提示

デジタル化を進めていく中で取組を進めていただきたいこと

1 事前対策の確認・強化

- **サプライチェーン全体を視野に入れたリスク管理**を行うこと。
- 稼働中の機器・システムに対して、**サポート切れのOSやアプリは使用せず**、**パッチ当て等の基本的に求められる対策**を実施することに加え、**振る舞い検知**など、既存の対策を**すり抜けた攻撃を防御・検知する仕組み**を導入すること。
- テレワークなど企業の管理策が及ばない起点や防御レベルが低い拠点からの侵入被害を限定するために、**情報資産やネットワークへのアクセスの継続監視と強化**、**システムの階層化**や、**子会社・海外拠点を含めた対応体制の整備**をすること。

2 事後対策の強化確認

- 攻撃されることを想定して、適切な**初動対応を行う体制と計画を整備**すること。
- インシデント発生時には、混乱した社員等の不適切な行動がセキュリティリスクを高めることも。平時の**“防災訓練”を徹底**して行うこと。

アクションプランの持続的発展と、新たな課題へのチャレンジへ

アクションプランの高度化　＜1～3年＞

- **デジタル化が急加速する中でのサイバー脅威の常態化**
  “Cyber New Normal (サイバー・ニュー・ノーマル)”
  - アクションプランの面的な拡大／質の高度化
  - 積極的サイバー防御を支える基盤の強化

For the future infrastructure　＜3～5年＞

- **重要インフラ産業の“基盤インフラ”も仮想化時代へ突入**
  - インフラの機能を支える“高信頼な基盤インフラ”の構築・保守能力の確保

アクションプランの持続的発展と、新たな課題へのチャレンジへ

アクションプランの高度化　＜1～3年＞

- **デジタル化が急加速する中でのサイバー脅威の常態化**
  “Cyber New Normal (サイバー・ニュー・ノーマル)”
  - アクションプランの面的な拡大／質の高度化
  - 積極的サイバー防御を支える基盤の強化

For the future infrastructure　＜3～5年＞

- **重要インフラ産業の“基盤インフラ”も仮想化時代へ突入**
  - インフラの機能を支える“高信頼な基盤インフラ”の構築・保守能力の確保

4つのアクションプランの進捗状況

- 4つのアクションプランは順調に進捗。

＜第3回研究会(2019年4月)以降に実現された取組及び今後の取組の方向＞

1 サプライチェーンサイバーセキュリティ強化パッケージ

- **ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン**第1版策定(2019年6月)
- インド太平洋地域向け**第二回日米サイバー演習**(2019年9月)
- 第3層TF、ソフトウェアTF、第2層TF開催(2019年8月-2020年3月)
- 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国際化の推進

1 サプライチェーンリスクマネジメント(SCRM)強化：サプライチェーン・サイバーセキュリティ・コンソーシアムの設立に向けて

2 フィジカル空間とサイバー空間のつながりの信頼性を確保するためのフレームワーク原案の提示（第2層TF)

2 サイバーセキュリティ経営強化パッケージ

- **経営ガイドライン可視化ツール**β版の策定（2020年3月）
- **サイバーセキュリティお助け隊**の8地域での実証事業完了（2020年3月）

3 サイバーセキュリティ人材育成・活躍促進パッケージ

- セキュリティ人材モデル（ITSS+更改版）の策定（2020年3月）
- 高専機構を中心とした産学官連携の推進
- 産業サイバーセキュリティセンター（ICSCoE)は3期生が卒業(2020年6月)
- **地方版コラボレーション・プラットフォームの開催**（青森、秋田、宮城、東京、岡山、広島）

3 ICSCoE 2025Visionの達成に向けて

4 セキュリティビジネスエコシステム創造パッケージ

- **ハイレベル検証**：機器のサイバーセキュリティ確保のための検証の手引き策定（2020年3月）
- セキュリティ製品の試行導入・実績公表の手引き策定（2020年3月）
- **情報セキュリティサービス審査登録制度登録数が192件**に(2020年6月)
- コラボレーション・プラットフォーム開催（全12回）

4 Trustを基盤とするセキュリティビジネス環境の構築

1 昨今のサイバー攻撃事案を踏まえた注意喚起と報告のお願い（報告の依頼）

- サイバー事案に対する社会的関心は非常に高く、これへの対応は、ステークホルダー等とのコミュニケーション等を間違えると会社の経営そのものに深刻な影響を与える可能性のある経営問題。
- 経営者の責任において、関係機関への報告や対外公表などを含めて、リスクの適切な管理のためのマネジメントの確立とその適切な実施に努めていくことが必要。
- 今年1月31日に「報告の依頼」を発出（報告〆切：2月14日）。

<「報告の依頼」内容>

■ 周知と点検

・機微情報を保有する企業に『サイバーセキュリティ経営ガイドライン Ver.2.0』などの周知徹底。

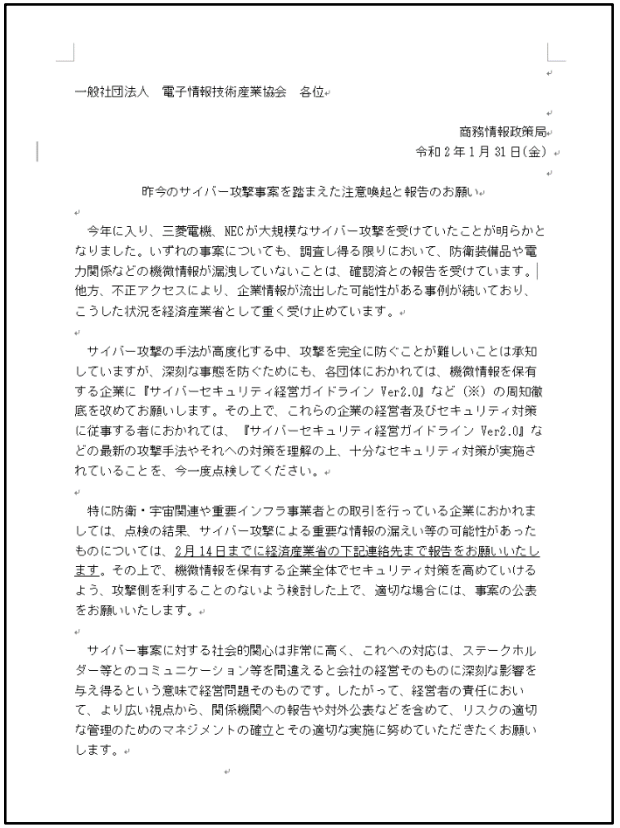
・最新の攻撃手法やそれへの対策を理解の上、『サイバーセキュリティ経営ガイドライン Ver.2.0』などを踏まえた十分なセキュリティ対策が実施されていることを、今一度点検。

■ 経済産業省への報告

・特に防衛・宇宙関連や重要インフラ事業者との取引を行っている企業に関しては、点検の結果、サイバー攻撃による重要な情報の漏えい等の可能性があったものについて、2月14日までに経済産業省へ報告を。

■ 事案の公表

・その上で、機微情報を保有する企業全体でセキュリティ対策を高めていけるよう、攻撃側を利することのないよう検討した上で、適切な場合には、事案を公表。



一般社団法人　電子情報技術産業協会　各位

商務情報政策局
令和２年１月31日(金)

昨今のサイバー攻撃事案を踏まえた注意喚起と報告のお願い

今年に入り、三菱電機、NECが大規模なサイバー攻撃を受けていたことが明らかとなりました。いずれの事案についても、調査し得る限りにおいて、防衛装備品や電力関係などの機微情報が漏洩していないことは、確認済との報告を受けています。他方、不正アクセスにより、企業情報が流出した可能性がある事例が続いており、こうした状況を経済産業省として重く受け止めています。

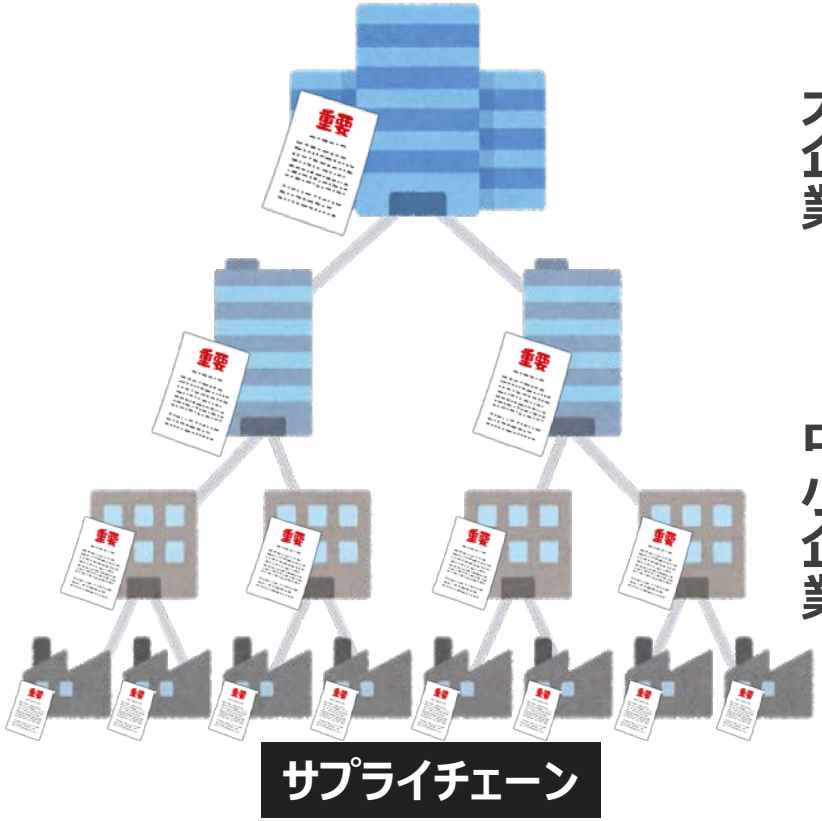
サイバー攻撃の手法が高度化する中、攻撃を完全に防ぐことが難しいことは承知していますが、深刻な事態を防ぐためにも、各団体におかれては、機微情報を保有する企業に『サイバーセキュリティ経営ガイドライン Ver2.0』など（※）の周知徹底を改めてお願いします。その上で、これらの企業の経営者及びセキュリティ対策に従事する者におかれては、『サイバーセキュリティ経営ガイドライン Ver2.0』などの最新の攻撃手法やそれへの対策を理解の上、十分なセキュリティ対策が実施されていることを、今一度点検してください。

特に防衛・宇宙関連や重要インフラ事業者との取引を行っている企業におかれましては、点検の結果、サイバー攻撃による重要な情報の漏えい等の可能性があったものについては、2月14日までに経済産業省の下記連絡先まで報告をお願いいたします。その上で、機微情報を保有する企業全体でセキュリティ対策を高めていけるよう、攻撃側を利することのないよう検討した上で、適切な場合には、事案の公表をお願いいたします。

サイバー事案に対する社会的関心は非常に高く、これへの対応は、ステークホルダー等とのコミュニケーション等を間違えると会社の経営そのものに深刻な影響を与え得るという意味で経営問題そのものです。したがって、経営者の責任において、より広い視点から、関係機関への報告や対外公表などを含めて、リスクの適切な管理のためのマネジメントの確立とその適切な実施に努めていただきたくお願いします。

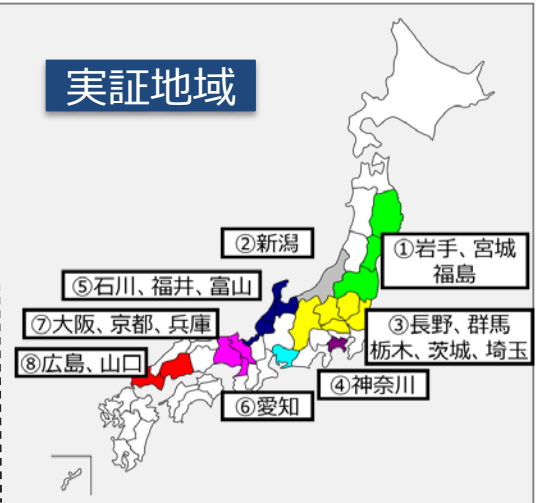
1 とりまとめの趣旨：サプライチェーン全体のサイバーセキュリティ対策が急務に

- **大企業から中小企業まで、サプライチェーンの弱点を狙ったサイバー攻撃が顕在化・高度化。**
  - 2020年1月以降、国内の複数の防衛関連の大企業が高度なサイバー攻撃の被害に遭っていたことが明らかに。
  - 「中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）」を通じて、中小企業に対するサイバー攻撃の実態も明らかに。
- 本報告では、サイバー攻撃の特徴や具体的事例を整理。
- 今後の取組の方向性をあわせて提示。産業界等の関係者等と調整しながら、サプライチェーン全体のサイバーセキュリティ対策を具体化していく方針。



- 2020年1月以降、三菱電機、NECなど、防衛省と取引関係にある企業が過去に高度なサイバー攻撃被害に遭っていたことが明らかに。防衛機微情報が狙われた可能性。

- サイバーセキュリティお助け隊を実施。
- 地域・企業規模に関わらず中小企業もサイバー攻撃の対象となっていることが判明。



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

1 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

- 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

1 （参考）令和元年度の取組：お助け隊 実証事業の結果

2020年6月12日公開資料

- 1,064社が参加した実証期間中に、全国８地域で**計910件のアラート**が発生。重大なインシデントの可能性ありと判断し、**対処を行った件数**は**128件**。対処を怠った場合の**被害想定額**が**5000万円**近くなる事案も。

＜駆け付け支援件数＞

対応種別	総数	内容	発生件数
インシデント対応	128件	**電話及びリモートによるインシデント対応※**	**110件**
		訪問によるインシデント対応	**18件**

※電話及びリモートによるインシデント対応には、訪問によるインシデント対応の一次対応を含む。

＜駆け付け支援の対象となった特徴的な対応事例＞

古いOSの使用

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

私物端末の利用

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

ホテルWi-Fiの利用

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

サプライチェーン攻撃

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

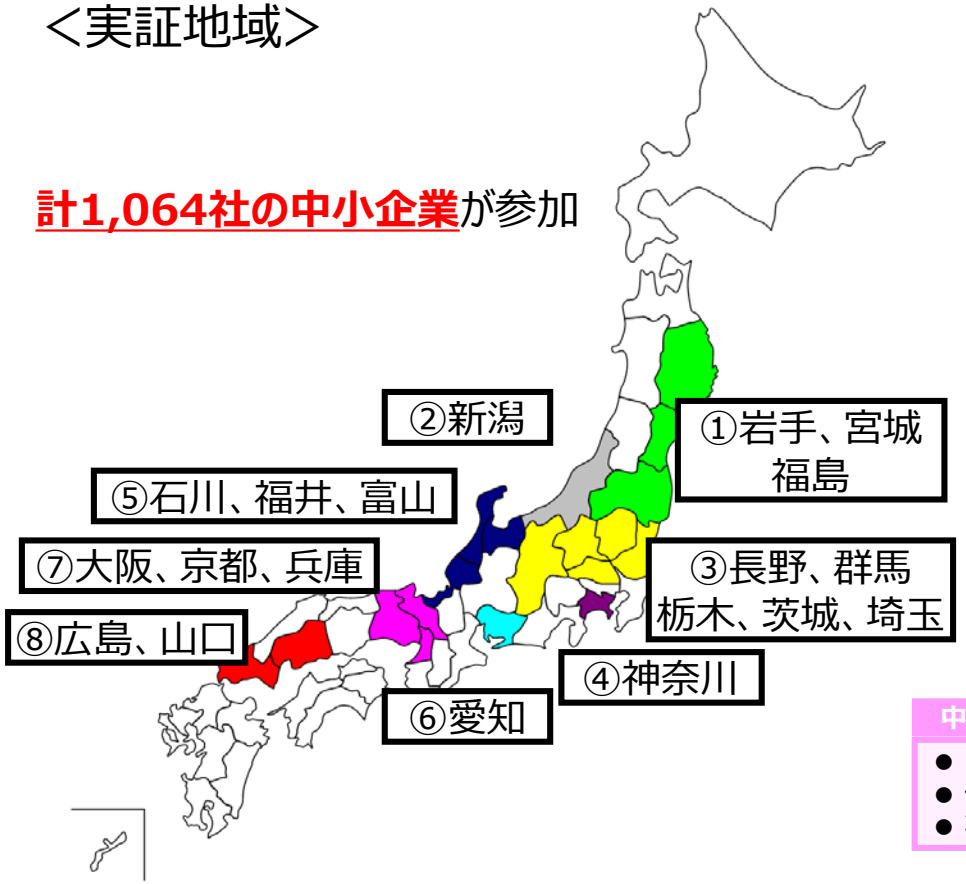
https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html

1 （参考）令和元年度の取組：サイバーセキュリティお助け隊実証事業

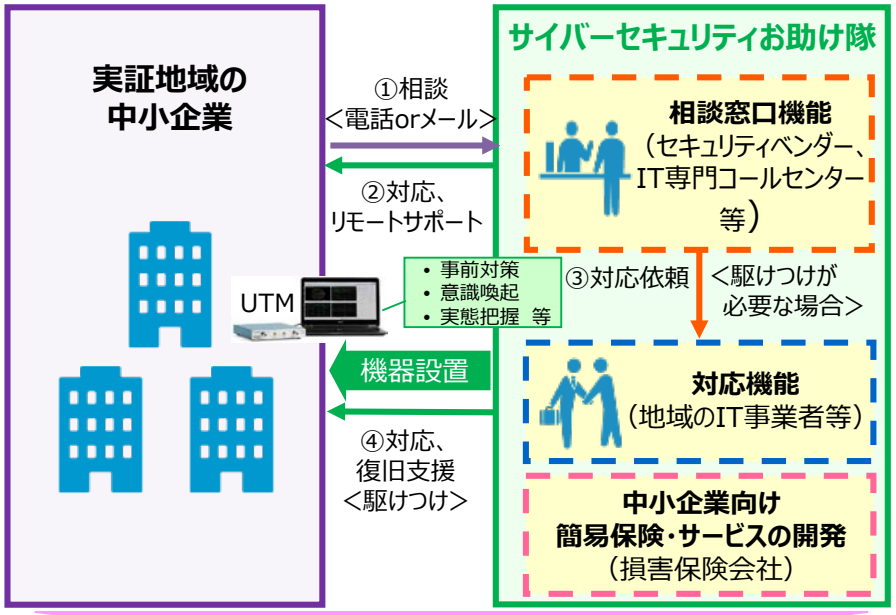
- 全国**8地域**において、地域の団体、セキュリティ企業、保険会社がコンソーシアムを組み、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした**実証事業**を実施。
- 本事業により、中小企業の事前対策の促進や意識喚起、攻撃実態や対策ニーズの把握を行い、**民間による中小企業向けのセキュリティ簡易保険サービスの実現を目指す**。

＜実証地域＞

計1,064社の中小企業が参加



＜実証のイメージ＞



実証結果

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

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

1 産業界を挙げたサプライチェーン全体のサイバーセキュリティ強化運動の展開へ

1．企業のリスクマネジメント強化のための基本行動指針の設定

共有（Share）	報告（Report）	公表 （Announcement）
①サプライチェーン共有主体間での高密度な情報共有 ☞ NDA関連情報が目安	②機微技術情報の流出懸念時の経産省への報告 ☞ 輸出管理対象技術が目安	③適切な場合の公表 ☞ 被害企業内での取締役会への報告事項(①の対象外のもの)が目安

2. 中小企業を含めたサプライチェーン・サイバーセキュリティ・コンソーシアムの立ち上げ

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。

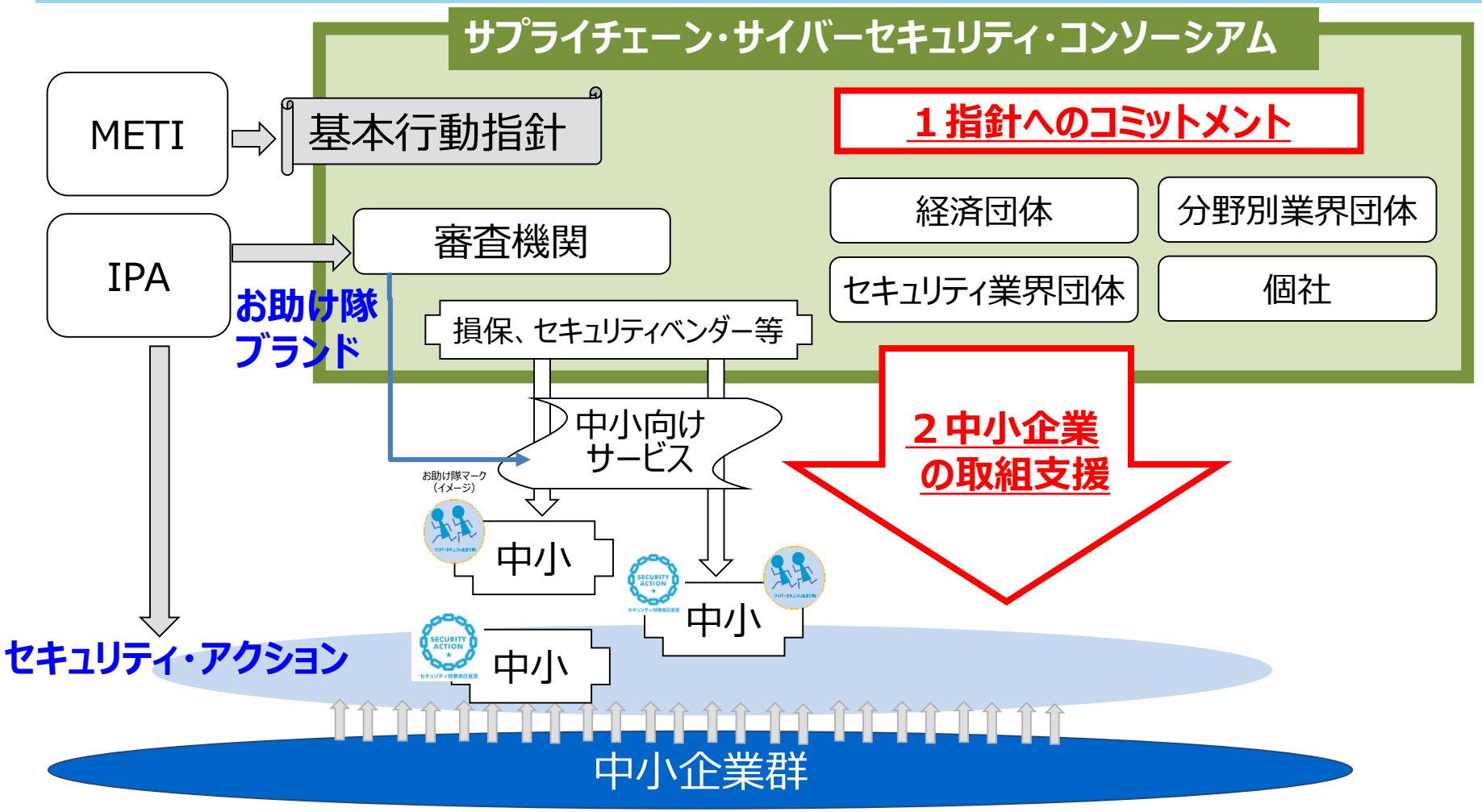
－サイバーセキュリティ対策の取組を可視化し、マークを持つモノとの取引を望むことを明確化

- 「お助け隊」のブランド化
- 「SECURITY ACTION」加速

1 サイバーセキュリティ強化運動の全体像（案）

- 立ち上げたコンソーシアムを活用し、
  – 基本行動指針の実践
  – 中小企業・地域を含めたサプライチェーンのサイバーセキュリティ対策

  を産業界全体の活動として展開。



2 分野別SWGにおけるサイバー・フィジカルセキュリティ対策フレームワーク（CPSF）の具体化 と テーマ別TFにおける検討

- **5つの産業分野別サブワーキンググループ(SWG)**を設置し、CPSFに基づくセキュリティ対策の具体化・実装を推進
- 分野横断の共通課題を検討するために、3つの**タスクフォース（TF）を設置**

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）

Industry by Industryで検討
（分野ごとに検討するためのSWGを設置）

- **ビルSWG**
  - ガイドライン第1版の策定
- **電力SWG**
  - 既存ガイドラインの強化
- **防衛産業SWG**
- **自動車産業SWG**
  - ガイドラインを公表
- **スマートホームSWG**
  - ガイドライン原案の作成
- ・・・

分野横断SWG

『第3層』TF：『サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
データマネジメントを俯瞰するモデルを提案し、データの信頼性確保に求められる要件を検討

ソフトウェアTF：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース

検討事項：OSSの管理手法に関するプラクティス集の策定等

『第2層』TF：『フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

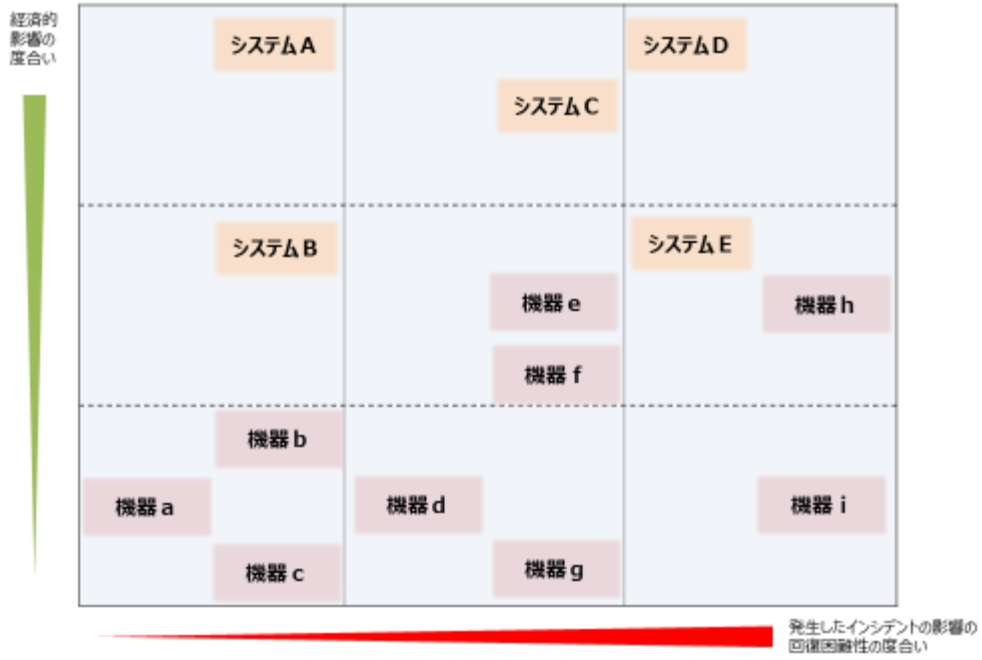
検討事項：
フィジカル空間とサイバー空間のつながりの信頼性の確保するための「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」のドラフト策定

詳細は次ページ

2 IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の案の策定

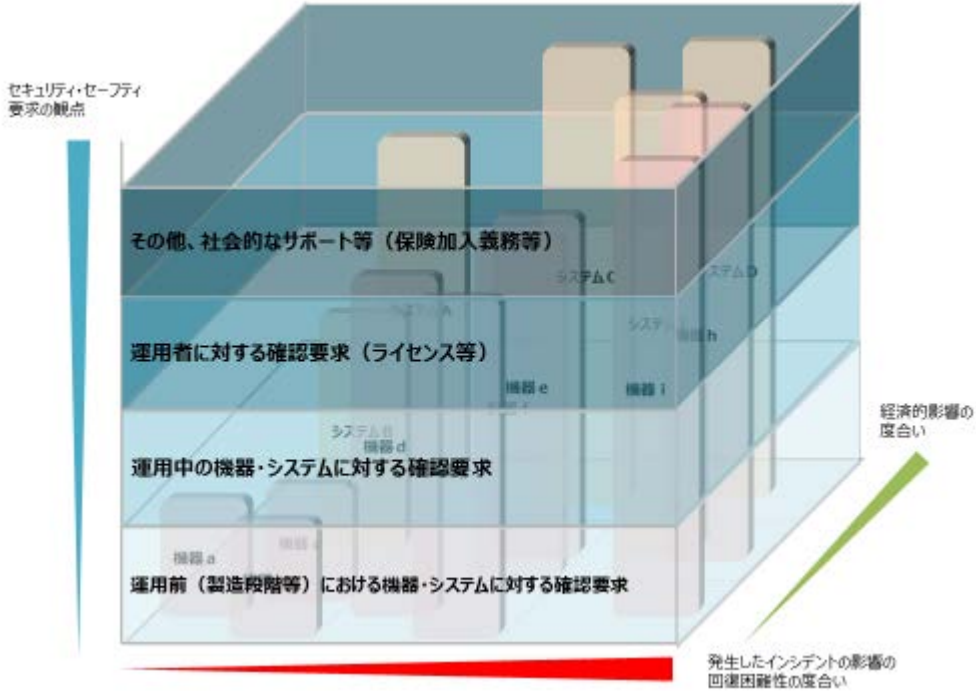
- IoT機器・システムの性質や利用環境によって課題が一様ではないことに着目し、IoT機器・システムをリスクに応じてカテゴライズした上で、それぞれに対するセキュリティ・セーフティ要求を検討することが重要。
- IoT機器・システムのカテゴライズやセキュリティ・セーフティ要求の検討に資するフレームワーク「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」の案を策定。世界中から幅広く意見を収集するため、日本語版・英語版のパブコメを実施（2020年3月31日～6月24日）。

フィジカル・サイバー間をつなげる
機器・システムのカテゴライズのイメージ



※ 同じ機器でも使用形態などによってマッピング先が異なり得る。
例えば、機器gと機器hが同じ機器で異なる使用形態である場合などがあり得る。）

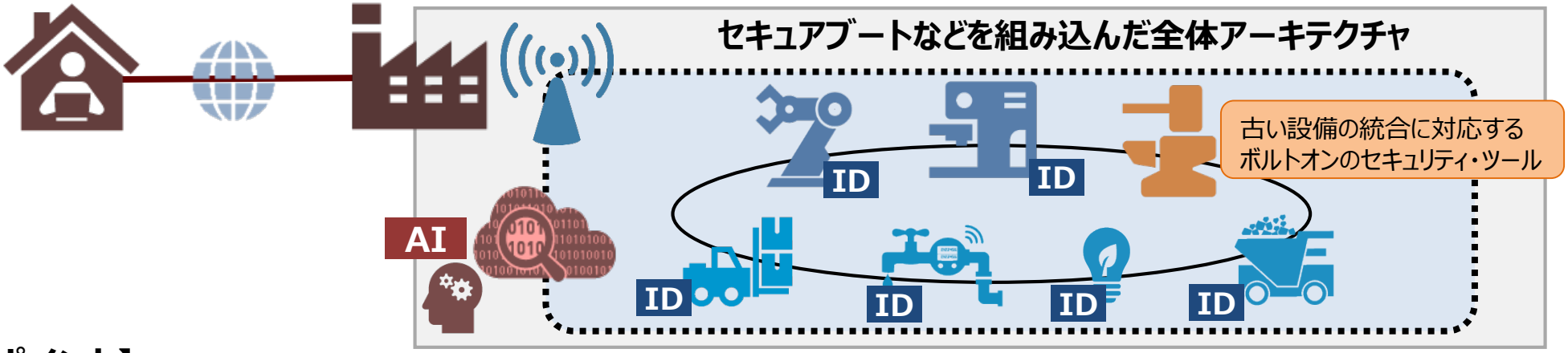
カテゴリに応じて求められる
セキュリティ・セーフティ要求の観点のイメージ



2 デジタル化の急拡大による新たなセキュリティ課題への対応（開発・実証）

- 今般の経験から、テレワークにとどまらず、IoTやAIを活用した製造現場や物流拠点・活動の無人化等の本格的なデジタル・トランスフォーメーション（DX）が急速に進展する見込み。
- 一方、新たなセキュリティ上の課題が深刻化する可能性があり、**IoT、制御系システム等のセキュリティ関連技術の開発やその効果の実証**を急ぐとともに、今後、こうした課題が増大することに**対応するための体制**について検討する必要がある。

例：産業IoTのセキュリティ・プロジェクト



【ポイント】

- CPSFをベースにしたリスク・マネジメント・モデルの整備
  →工作機械サプライヤー等を集めた「ファクトリー・オートメーションSWG」の設置等
- 個々の機器の信頼性確認や状況監視、後付け型のセキュリティ・ツールなどセキュリティ関連技術の開発
  →SIP事業におけるセキュア暗号ユニットの開発成果活用や、制御系に適した監視システム等の開発等
- それぞれのケースにおいて有効なセキュリティ・セーフティに関する技術・手法等の検証
  →様々なセキュリティの実践モデルやツールが機能するケースの検証による現場への導入支援等

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

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

事故調査の役割

幅広い分野のサイバー事故調査支援

世界に類を見ないユニークな機関

多様で実践的な研修プログラム

様々な分野の実環境の再現
外部機関の設備の活用

高い専門性・多様性

様々な分野・技術の専門家との
ネットワーク強化

最新情報の流通経路

OB会ネットワークの整備・組織化
OB人材活用

有能な人材輩出・知識のアップグレード

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

国際的な連携拠点

既存の国際交流活動の拡大・強化
JETRO・在外公館との連携強化

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

（参考）with/after COVID-19: オンライン化の推進

- 認証からオープンデータまでのユーザー体験を改善するため、**2017年から法人デジタルプラットフォーム構想を推進中。**
- 人との接触機会削減のための**テレワーク等を推進。**

法人デジタルプラットフォーム

認証
gBizID
- 法人・個人事業主向け行政手続の共通認証システム
- 手続きごとの本人確認書類提出が不要に
- 今年度から他省庁でも活用

行政手続
jGrants
- 補助金のオンライン申請
- 今年度から他省庁・自治体でも活用

データ連携
gBizConnect
- 行政・民間のシステム間を安全に接続
- 添付書類撤廃・ワンスオンリーを実現
- 今年度省内システムで実証

オープンデータ
gBizINFO
- 約190万件の法人活動情報を掲載
- EDINET等とAPI連携
- 2017年1月から運用

テレワーク等の推進

- これまで、テレワークを一度も検討したことのない中小企業や、テレワークのためのデジタル投資が不十分な中小企業にも、取り組んでいただくため、**すぐに実践できる取組例の紹介**や、**活用できる民間支援情報の集約・発信**、**ITツール導入のための補助金の拡充（補助率最大3/4）**、**相談体制の強化**等を行った。

- 4月22日、**ICSCoE技術研究室のハッカーが中心**となり、NTT東日本と連携して開発した、**中小企業でも安心してテレワーク環境を実現できる技術「シン・テレワークシステム」を無償開放。**
  - ▶ **既に地方企業でも導入報告**あり。 ユーザ数：**40,007人**(6/23時点)
    https://telework.cyber.ipa.go.jp/news/

4 信頼性 “Trust” を基盤とするセキュリティビジネス環境の構築

- 「サイバーセキュリティ戦略」（平成３０年７月２７日閣議決定）には、「**従来の受動的な対策だけでは対応しきれず、これまでよりも積極的な対策を行う必要がある**」とし、積極的サイバー防御の推進を掲げている。
- 積極的サイバー防御の実現に向けて、セキュリティビジネスのトラストを強固にし、セキュリティビジネスの役割を拡大する必要があるのではないか。

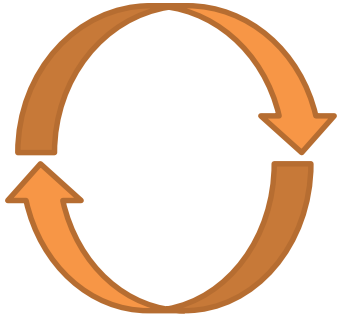
「サイバーセキュリティ戦略」における記載（平成３０年７月２７日閣議決定）

サイバー犯罪・サイバー攻撃は複雑化・巧妙化しており、攻撃の種類も多種多様となっていることから、**従来の受動的な対策だけでは対応しきれず、これまでよりも積極的な対策を行う必要**がある。
このような状況を踏まえ、サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じる「**積極的サイバー防御**」（サイバー攻撃に対して能動的に防御していく取組のこと）を推進する。具体的には、国は先行的防御を可能にするための脅威情報の共有・活用の促進、攻撃者の情報を集めるための攻撃誘引技術の活用、ボットネット対策等、サイバー犯罪・サイバー攻撃による被害を未然に防止できるような取組を推進する。

能力／信頼性と役割の拡大の好循環

セキュリティビジネスの高度化

- 信頼性の確認・可視化
- 能力の向上
  （人材育成・活用・技術開発）



**積極的サイバー防御における
ビジネスセクターの果たすべき役割の拡大**

求められる内容

- 脅威情報の把握
- 攻撃者情報の収集
- 脅威分析能力の強化

アクションプランの持続的発展と、新たな課題へのチャレンジへ

アクションプランの高度化　＜1～3年＞

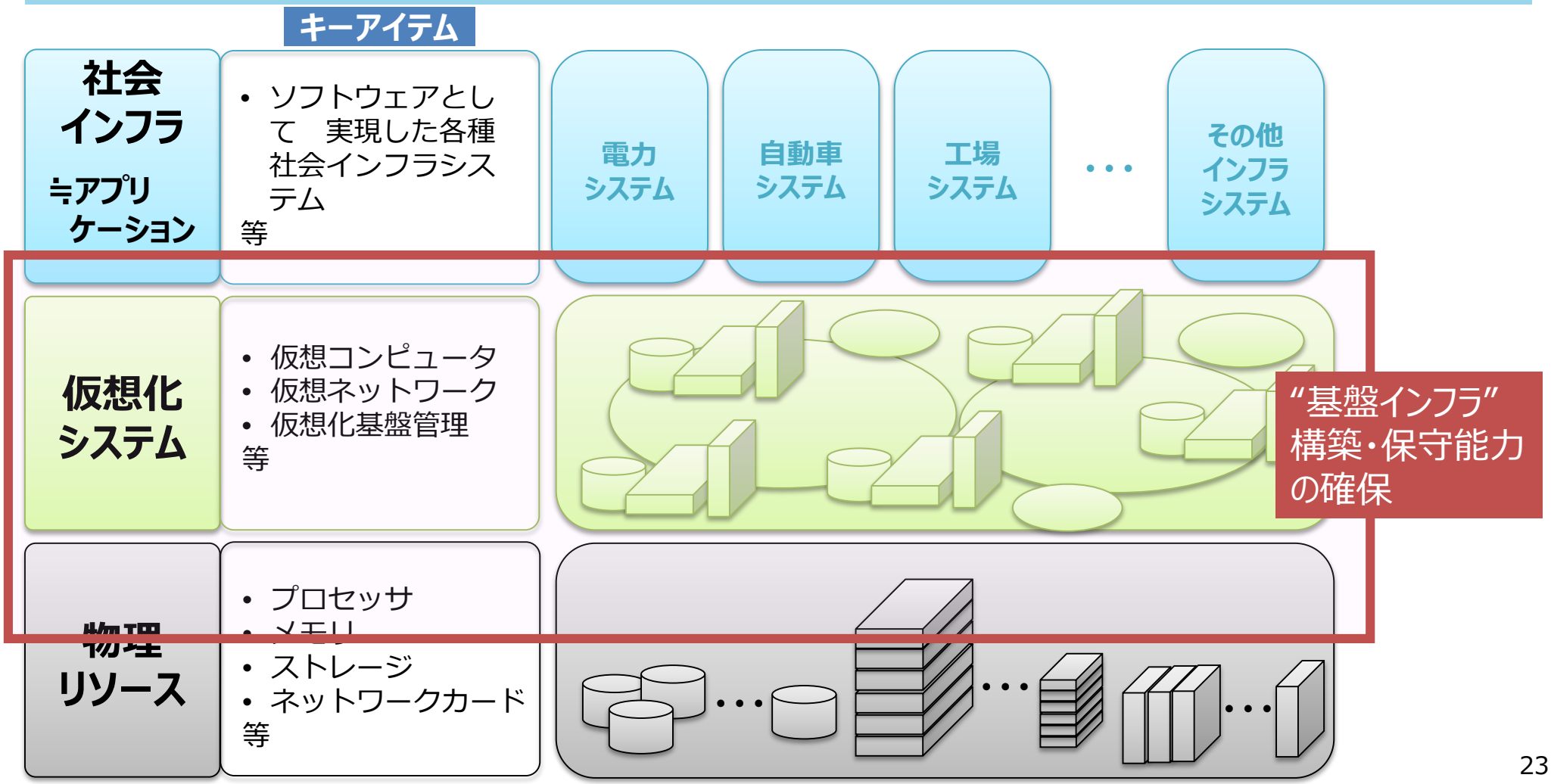
- デジタル化が急加速する中でのサイバー脅威の常態化
  “Cyber New Normal (サイバー･ニュー･ノーマル)”
  - アクションプランの面的な拡大／質の高度化
  - 積極的サイバー防御を支える基盤の強化

For the future infrastructure　＜3～5年＞

- **重要インフラ産業の“基盤インフラ”も仮想化時代へ突入**
  - インフラの機能を支える“高信頼な基盤インフラ”の構築・保守能力の確保

“基盤インフラ”の将来像

- 今後の社会インフラ（電力、工場等）は仮想化基盤の上のアプリケーション（ソフトウェア）として実現される可能性。
- 社会機能を維持していくために、その基盤（物理基盤、仮想化基盤）を構築、維持、運用・保守する能力の確保が必要。



基盤インフラのアーキテクチャ等の検討

- 基盤インフラが抱える課題について包括的に検討をし、我が国としての基盤インフラ構築、維持、運用能力の獲得に向けて、幅広い専門家からなる勉強会を開催
- 今後必要な施策に資する課題整理等を実施の予定

勉強会の体制

＜2020年2月時点＞

お名前	ご所属
浅井 大史	株式会社Preferred Networks リサーチャー
飯田 健一郎	NTT国際通信 代表取締役社長
上坂 利文	NECサービスプラットフォーム事業部 事業部長
江崎 浩	東京大学大学院情報理工学系研究科 教授
大江 将史	国立天文台情報セキュリティ室 助教／情報セキュリティ室 次長
太田 雅浩	富士通クラウドサービス事業本部 理事本部長
奥野 通貴	株式会社日立製作所エレクトロニクスイノベーションセンタコネクティビティ研究部 部長
榊原 彰	日本マイクロソフト株式会社 執行役員最高技術責任者
佐藤 剛	NTTコミュニケーションズクラウドサービス部 担当部長
澁澤 栄	東京農工大学卓越リーダー養成機構 教授
関谷 勇司	東大情報理工学教育研究センター 教授
田中 良夫	産業技術総合研究所情報技術研究部門
土井 裕介	株式会社Preferred Networks
冨安 寛	NTTデータシステム技術本部 本部長
成迫 剛志	デンソー
平井 真樹	NECサービスプラットフォーム事業部 部長代理
藤澤 克樹	九州大学マス・フォア・インダストリ研究所 フェロー
松浦 誠	NTTデータシステム技術本部
松本 修	富士通ファウンデーションビジネス事業部 事業部長
丸山 宏	株式会社Preferred Networks フェロー
宮田 裕章	慶應義塾大学医学部 教授

第1回勉強会で出てきた課題

①アプリケーション

- 次世代基盤インフラを必要とする**アプリケーションとは何か**
- どのような**特徴を有するアプリケーションを選定**すると、我が国において、次世代基盤インフラ技術を獲得することができるか

②次世代基盤インフラ技術

- 次世代基盤インフラを支える各種技術のうち、我が国において優先して**獲得するべき技術は何か**

③ルール・制度整備

- 次世代基盤インフラを用いたサービスを普及・促進する上で、**整備するべきルール**として考えられるものは何か

（参考資料）

4つのアクションプランの進捗状況

- 4つのアクションプランは順調に進捗。

＜第3回研究会(2019年4月)以降に実現された取組及び今後の取組の方向＞

1 サプライチェーンサイバーセキュリティ強化パッケージ

- **ビルシステムガイドライン**第1版策定(2019年6月)
- **スマートホームガイドライン**原案策定(2020年3月)
- **自動車ガイドライン**(2020年5月公開)
- 第3層TF、ソフトウェアTF、第2層TF開催(2019年8-2020年3月)
- 第3回**日イスラエル電力サイバーセキュリティ官民会合**(2019年11月)
- 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国際化の推進
- インド太平洋地域向け第二回**日米サイバー演習**(2019年9月)

2 サイバーセキュリティ経営強化パッケージ

- **「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)
- **経営ガイドライン可視化ツール**β版策定（2020年3月）

3 サイバーセキュリティ人材育成・活躍促進パッケージ

- セキュリティ人材モデル（**ITSS+更改版**）の策定（2020年3月）
- 産業サイバーセキュリティセンター（ICSCoE)は3期生が卒業(2020年6月)
- サイバーセキュリティ経営を進める**戦略マネジメント層の育成**
- **国立高専機構**と産・官との連携促進・具体化
- **各地域でのセキュリティコミュニティ形成**に向けた取組状況

4 セキュリティビジネスエコシステム創造パッケージ

- セキュリティ製品の**有効性検証・実環境における試行検証**
- ハイレベル検証：**機器のサイバーセキュリティ確保のための検証の手引き**策定（2020年3月）
- 中小企業向けセキュリティ製品・サービスの検証事業：**評価項目(案)**策定（2020年3月）
- **情報セキュリティサービス審査登録制度登録数が192件**に(2020年6月)

4つのアクションプランの進捗状況

- 4つのアクションプランは順調に進捗。

＜第3回研究会(2019年4月)以降に実現された取組及び今後の取組の方向＞

1 サプライチェーンサイバーセキュリティ強化パッケージ

- **ビルシステムガイドライン**第1版策定(2019年6月)
- **スマートホームガイドライン**原案策定(2020年3月)
- **自動車ガイドライン**(2020年5月公開)
- 第3層TF、ソフトウェアTF、第2層TF開催(2019年8-2020年3月)
- 第3回**日イスラエル電力サイバーセキュリティ官民会合**(2019年11月)
- 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国際化の推進
- インド太平洋地域向け第二回**日米サイバー演習**(2019年9月)

2 サイバーセキュリティ経営強化パッケージ

- **「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)
- **経営ガイドライン可視化ツール**β版策定（2020年3月）

3 サイバーセキュリティ人材育成・活躍促進パッケージ

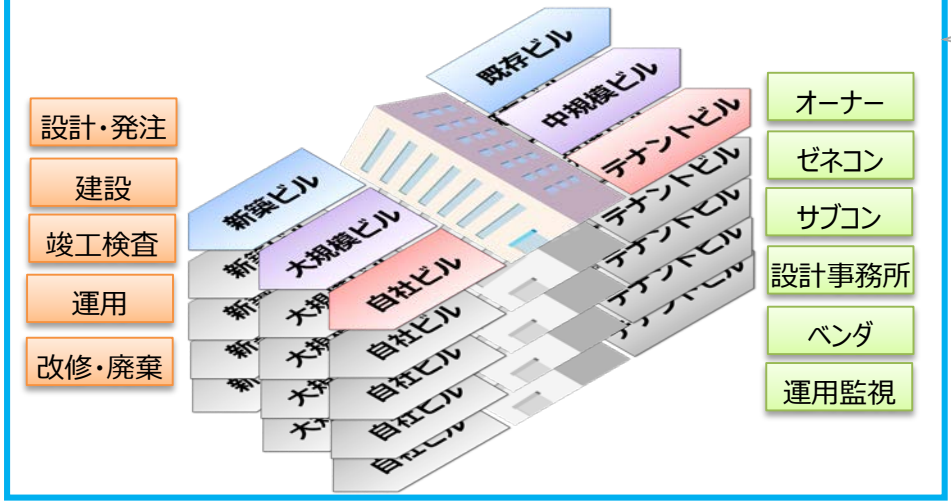
- セキュリティ人材モデル（**ITSS+更改版**）の策定（2020年3月）
- 産業サイバーセキュリティセンター（ICSCoE)は3期生が卒業(2020年6月)
- サイバーセキュリティ経営を進める**戦略マネジメント層の育成**
- **国立高専機構**と産・官との連携促進・具体化
- **各地域でのセキュリティコミュニティ形成**に向けた取組状況

4 セキュリティビジネスエコシステム創造パッケージ

- セキュリティ製品の**有効性検証・実環境における試行検証**
- ハイレベル検証：**機器のサイバーセキュリティ確保のための検証の手引き**策定（2020年3月）
- 中小企業向けセキュリティ製品・サービスの検証事業：**評価項目(案)**策定（2020年3月）
- **情報セキュリティサービス審査登録制度登録数が192件**に(2020年6月)

ビルSWG（座長：江崎 浩 東京大学 教授）

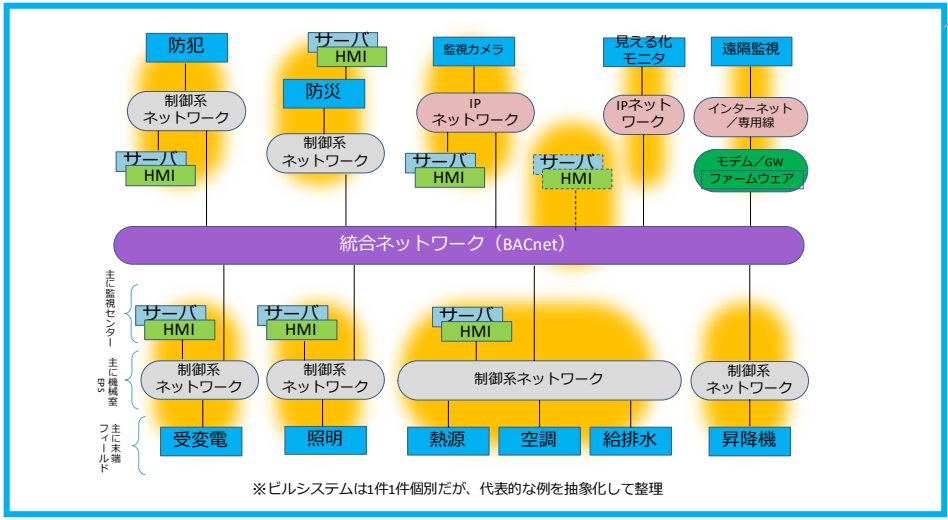
- ビルの管理・制御を行うビルシステムに係る各種**サイバー攻撃のリスクと、それに対するサイバーセキュリティ対策を整理**し、2019年6月17日付で**ガイドライン第1版を公開**。
- 記述充実化と**個別編(空調編)作成**を実施中。関係者間の**情報共有の在り方**についても検討中。



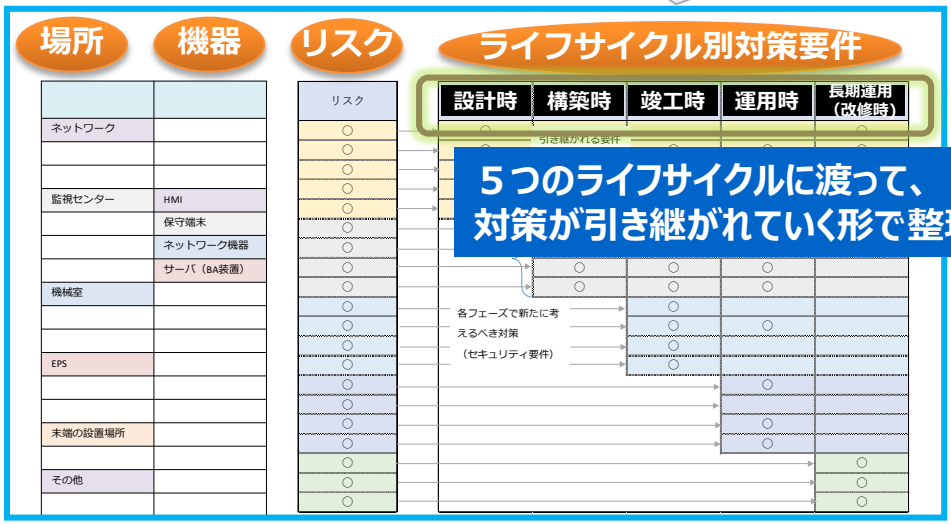
ビルシステムは、様々な種類のビルに、多種多数のステークホルダが関与し、多種の設備システムが稼働し、複数ステージからなる長期間のライフサイクルを持つ、という特徴を持つ。

モデル的なビルシステムを設定。

ビルシステムの置かれる場所、個々の機器等に応じたリスクに対し、ライフサイクルを意識した対策を整理。



※ビルシステムは1件1件個別だが、代表的な例を抽象化して整理



スマートホーム、自動車業界におけるCPSFをベースにしたガイドライン策定

- 策定・公表済みのビルガイドライン以外に、**CPSFをベースにした業界別ガイドラインの策定が進行**。
- 特に、**スマートホーム、自動車業界では、ガイドラインの公表に向けた準備が進捗**。

スマートホームSWG

ガイドライン原案を作成

目的

- スマートホームにおける安全で安心な生活の実現のため、**幅広いステークホルダに必要なセキュリティ対策の指針を示す**。

対象範囲

- IoT に対応した住宅設備・家電機器などがサービスと連携することで様々な便益が提供されるスマートホームにおける**多様なステークホルダーが対象**
  - スマートホーム向けの **IoT 機器関連事業者**
  - スマートホーム向けの**サービス事業者**
  - スマートホームの**管理者・住まい手**　　等

ポイント

- 知識やバックグラウンドが様々なステークホルダーに対応するため、ユースケースから想定されるインシデントを基に、**シンプルな対策ガイドから、具体的な対策要件や他の標準との対比まで、階層的に整理**。

今後の方針

- 公表を目指し、更なるブラッシュアップを進める。

自動車産業SWG

5/28 ガイドラインを公表

目的

- **業界全体のセキュリティのレベルアップ**
- 対策レベルの効率的な点検の推進

対象範囲

- 自動車業界の全ての企業の**エンタープライズ領域**
- OEMから小規模会社で最低限必要な必須項目を策定（ただし、強制するものではない）。

ポイント

- 部品やサービス/ソフトウェアのサプライチェーン対応
- **CPSFの対策要件をベースに、業界の実態に即した実施事項レベルや記載方法を検討**して作成。
- チェックリストを活用することにより、各社が自社**の取組状況をセルフチェックできる**。

今後の方針

- トライアルを行い自動車産業としての共通のセキュリティーガイドラインとして、本格運用を目指す。
- **今後、工場やコネクティッド等へ対象を拡大**する方針。

参考：http://www.jama.or.jp/it/cyb_sec/cyb_sec_guideline.html

第3回 日イスラエル電力サイバーセキュリティ官民会合（概要）

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

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

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

トピック

（先進的な取組の紹介）

①サプライチェーンセキュリティ対策

②サイバーセキュリティ体制（SOC、インシデント　対応）

③人材育成・トレーニング

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

マルチ・バイを通じた国際協調への取り組み

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

- **EUサイバーフォーラム（2019年4月@ベルギー・ブリュッセル）**
  - 欧州対外活動庁（EEAS）主催のフォーラムのIoTパネルにおいて、METIの取組、CPSFを紹介。
- **ICS-JWG2019（2019年4月@米・カンザスシティ）**
  - 米国土安全保障省（DHS）主催のフォーラムにおいて、当省の取組、 CPSFを紹介。
- **Consumers International Summit 2019 （2019年4月@ポルトガル・エストリル）**
  - 国際消費者保護団体主催のフォーラムのIoTパネルにおいて、 CPSFとIoTセキュリティTFを紹介。
- **プラハ５Gセキュリティ会議（2019年５月@チェコ・プラハ）**
  - チェコ政府主催の5Gに関する国際会議のテクノロジーWGにおいて、 CPSFを紹介。
- **第4回日EUサイバー対話（2019年6月@ベルギー・ブリュッセル）**
  - 日EU政府間のサイバーセキュリティ協議において、CPSFと３つのTFの立ち上げを紹介。
- **EIS年次総会・CPIC会合（2019年6月@米・ワシントンDC）**
  - EIS Council主催のEIS Summit、CPIC会合において、CPSF、各SWG、TFについて紹介。
- **第5回日仏サイバー協議（2019年7月@仏・レンヌ）**
  - 日仏政府間のサイバーセキュリティ協議において、 CPSF、各SWG、TFについて紹介。
- **サイバーテック・ミッドウェスト（2019年7月@米・インディアナポリス）**
  - イスラエル発の世界的なサイバーセキュリティ・カンファレンスにおいて、CPSFを紹介。
- **APEC第3回高級実務者会合（SOM3）（2019年8月@チリ・プエルトバラス）**
  - 米商務省主催のWSにおいて、CPSF、各TF、SWGでの活動、コラプラなどの取組を紹介。

- **インド太平洋地域向け日米サイバー演習（2019年9月@日本・東京）**
  - インド太平洋地域のCERT、官民の重要インフラ関係者に対し、CPSF、SWGでの活動を紹介。
- **IEEE-APL 5G Workshop、Global Cyber Dialogue（2019年10月@米・ワシントンDC）**
  - IEEE、米商工会議所主催の会議において、CPSF、各SWG、TFでの活動、日米サイバー演習を紹介。
- **第10回インターネットエコノミーに関する日米政策協力対話（IED）（2019年10月@日本・東京）**
  - 日米官民の協議において、 CPSF、各SWG、TFでの活動、日米サイバー演習を紹介。
- **第7回日米サイバー対話（2019年10月@日本・東京）**
  - 日米政府間のサイバーセキュリティ協議において、 CPSF、各SWG、TFでの活動、日米サイバー演習を紹介。
- **APEC TEL60（2019年10月@韓国・ソウル）**
  - 韓国主催のラウンドテーブルにおいて、ガバナンスイノベーションとCPSFの取組についてプレゼンを実施。
- **ETSI IoT Workshop（2019年10月@仏・ソフィアアンティポリス）**
  - ETSI主催のカンファレンスで、 CPSF、第2層TFでの活動について紹介。
- **第12回日アセアン政策会議（2019年10月@タイ・バンコク）**
  - 日ASEAN政府サイバー当局間の会議において、 CPSF、ビルSWG、 TFでの活動について紹介。
- **第2回OECD Global Forum on Digital Security for Prosperity（2019年11月@英・ロンドン）**
  - デジタルセキュリティ・イノベーションに係るパネルにおいて、CPSF、WG３の活動を紹介。
- **PJM会合（2019年12月@米・フィラデルフィア）**
  - 米国をはじめとする電力分野のセキュリティに関する国際会合において、CPSF、各SWG、TFでの活動を紹介。
- **Cybertech Tel Aviv 2020（2020年１月@イスラエル・テルアビブ）**
  - イスラエル最大のサイバーセキュリティに関する国際会合において、CPSF、第二層TFでの活動を紹介。
- **FIC 2020（2020年2月@仏・リール）**
  - ヨーロッパ最大級のサイバーセキュリティイベントにおいて、我が国の産業サイバーセキュリティ政策の概要を紹介。
- **ENISA – ETSI – CEN – CENELEC Conference（2020年2月@ベルギー・ブリュッセル）**
  - Cybersecurity Standardizationに関する会合で、CPSF、第二層TFでの活動を紹介。

インド太平洋地域向け日米サイバー演習

- 経済産業省及びIPA産業サイバーセキュリティセンター（ICSCoE）が、日米の専門家による制御システムのサイバーセキュリティに関する演習をインド太平洋地域（14の国・地域）向けに実施。
- 2020年度は、EUとの連携や、電力分野のセキュリティWSとの同時開催も検討中。

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

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

ICSCoE中核人材育成プログラム研修生　69名

■**来賓挨拶／講師：**

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

（日本）関芳弘経済産業副大臣、ICSCoE講師、日本企業

米国国務省挨拶


米国の専門家による講義


日本の専門家による講義

参加国・地域


ハンズオントレーニング


ワークショップ


サイバー攻撃のデモ

4つのアクションプランの進捗状況

- 4つのアクションプランは順調に進捗。

＜第3回研究会(2019年4月)以降に実現された取組及び今後の取組の方向＞

1 サプライチェーンサイバーセキュリティ強化パッケージ

- **ビルシステムガイドライン**第1版策定(2019年6月)
- **スマートホームガイドライン**原案策定(2020年3月)
- **自動車ガイドライン**(2020年5月公開)
- 第3層TF、ソフトウェアTF、第2層TF開催(2019年8-2020年3月)
- 第3回**日イスラエル電力サイバーセキュリティ官民会合**(2019年11月)
- 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国際化の推進
- インド太平洋地域向け第二回**日米サイバー演習**(2019年9月)

2 サイバーセキュリティ経営強化パッケージ

- **「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)
- **経営ガイドライン可視化ツール**β版策定（2020年3月）

3 サイバーセキュリティ人材育成・活躍促進パッケージ

- セキュリティ人材モデル（**ITSS+更改版**）の策定（2020年3月）
- 産業サイバーセキュリティセンター（ICSCoE)は3期生が卒業(2020年6月)
- サイバーセキュリティ経営を進める**戦略マネジメント層の育成**
- **国立高専機構**と産・官との連携促進・具体化
- **各地域でのセキュリティコミュニティ形成**に向けた取組状況

4 セキュリティビジネスエコシステム創造パッケージ

- セキュリティ製品の**有効性検証・実環境における試行検証**
- ハイレベル検証：**機器のサイバーセキュリティ確保のための検証の手引き**策定（2020年3月）
- 中小企業向けセキュリティ製品・サービスの検証事業：**評価項目(案)**策定（2020年3月）
- **情報セキュリティサービス審査登録制度登録数が192件**に(2020年6月)

段階的なサイバーセキュリティ経営の実現

- 以下の3Stepにより、サイバーセキュリティ経営の定着を目指す。

1st Step

サイバーセキュリティ経営の明確化

- サイバーセキュリティ経営ガイドラインの普及・定着

2nd Step

サイバーセキュリティ経営の実践

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

3rd Step

セキュリティの高い企業であることの可視化

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

サイバーセキュリティ経営ガイドライン

平成27年12月28日策定
平成28年12月8日改訂（Ver.1.1）
平成29年11月16日改訂（Ver2.0）

- 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。2015年12月に初版公開。
- 2017年11月公開のVer2.0は、ダウンロード数が毎月平均約2800件、累計８万件超と注目度の高い状況が続いている。

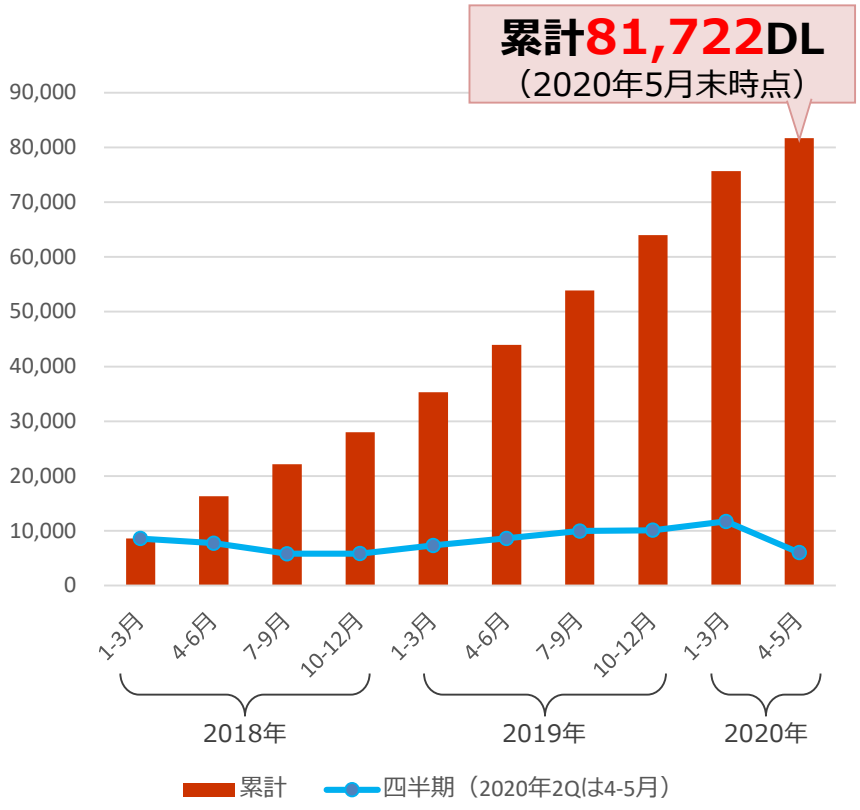
１．経営者が認識すべき３原則

（１）経営者が、**リーダーシップを取って対策**を進めることが必要
（２）自社のみならず、**ビジネスパートナーを含めた対策**が必要
（３）平時及び緊急時のいずれにおいても、**関係者との適切なコミュニケーション**が必要

２．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAサイクルの実施
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の対策及び状況把握
関係者とのコミュニケーション	**指示10** 情報共有活動への参加

サイバーセキュリティ経営ガイドラインV2.0のダウンロード数推移



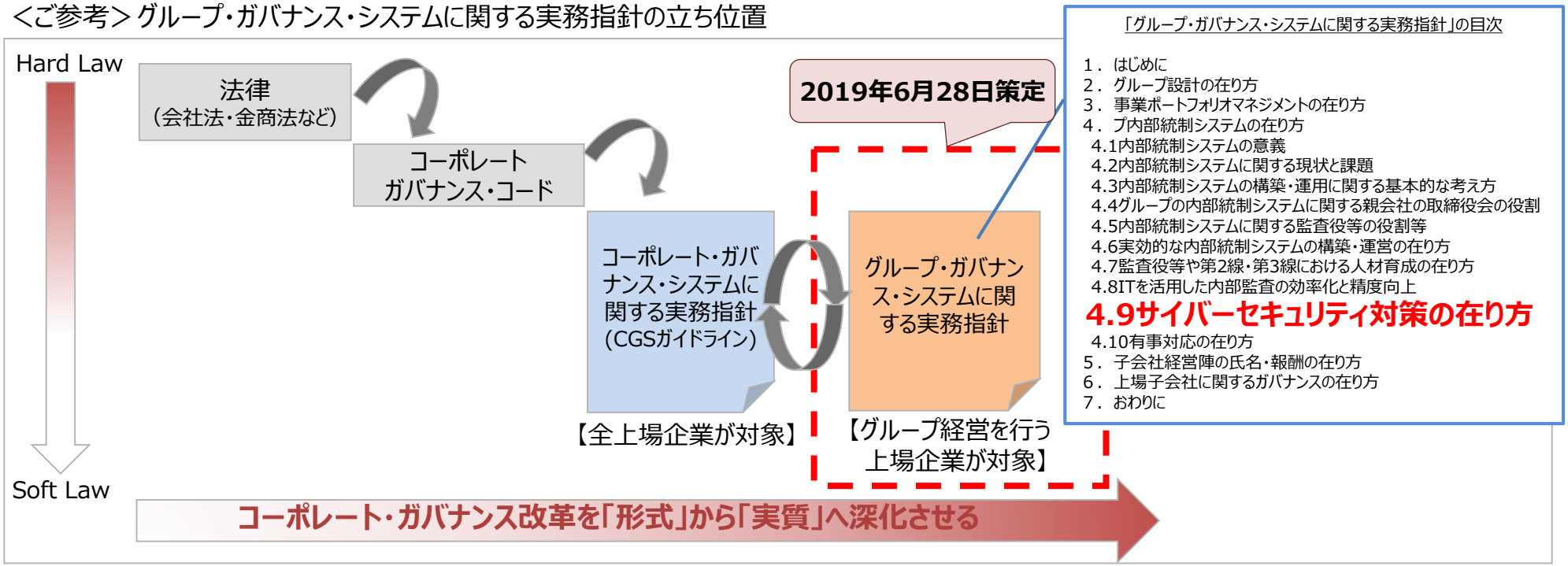
【参考】上場企業数　第一部　2,157社
第二部　488社
（日本取引所グループ公表 2019年12月17日時点）

2nd step

コーポレートガバナンスの一環として、サイバーセキュリティ経営を位置づけ

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

<ご参考> グループ・ガバナンス・システムに関する実務指針の立ち位置

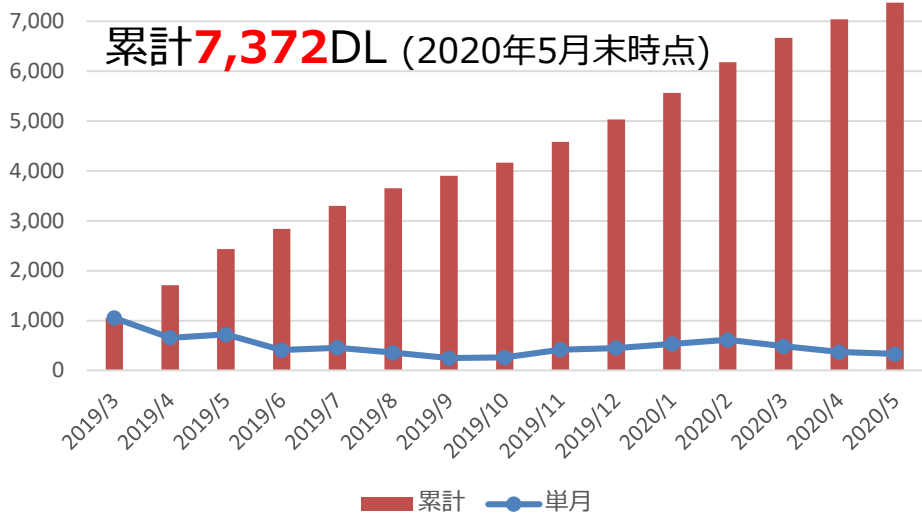


（出典）第13回CGS研究会資料より抜粋

『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』を策定

- 2019年3月、**「サイバーセキュリティ経営ガイドラインVer2.0実践のための経営プラクティス集」を公開**。経営ガイドラインの重要10項目の実践事例に加え、セキュリティ担当者の日常業務における悩みに対する具体的対応策を提示。
- 2019年度収集したプラクティスを反映した改定版を2020年6月3日に公表。

<プラクティス集のダウンロード数推移>



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

【参考】プラクティス集　目次

第一章：経営とサイバーセキュリティ

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

第二章：サイバーセキュリティ経営ガイドライン実践のプラクティス

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

第三章：サイバーセキュリティ対策を推進する担当者の悩みと解決のプラクティス

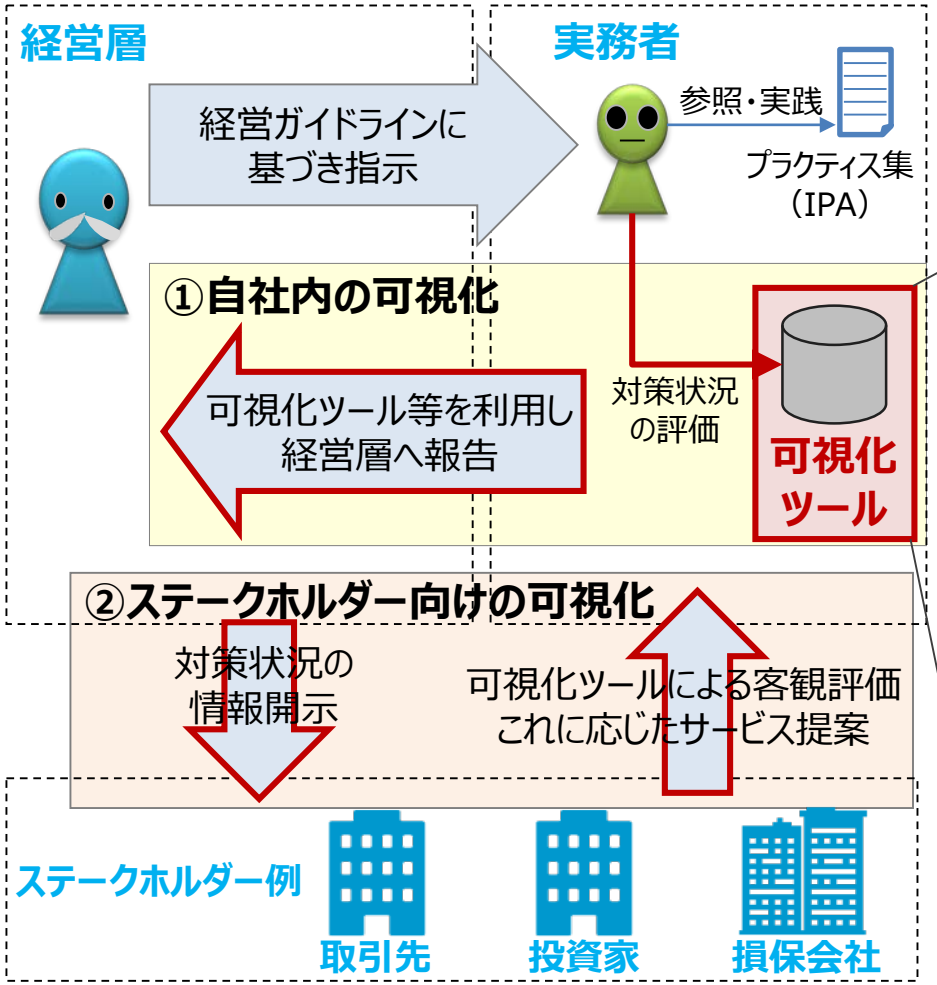
<セキュリティ担当者向け>
サイバーセキュリティ対策を実践する上での悩みに対する、企業の具体的な取組事例を紹介

<アップデートした指示項目>

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

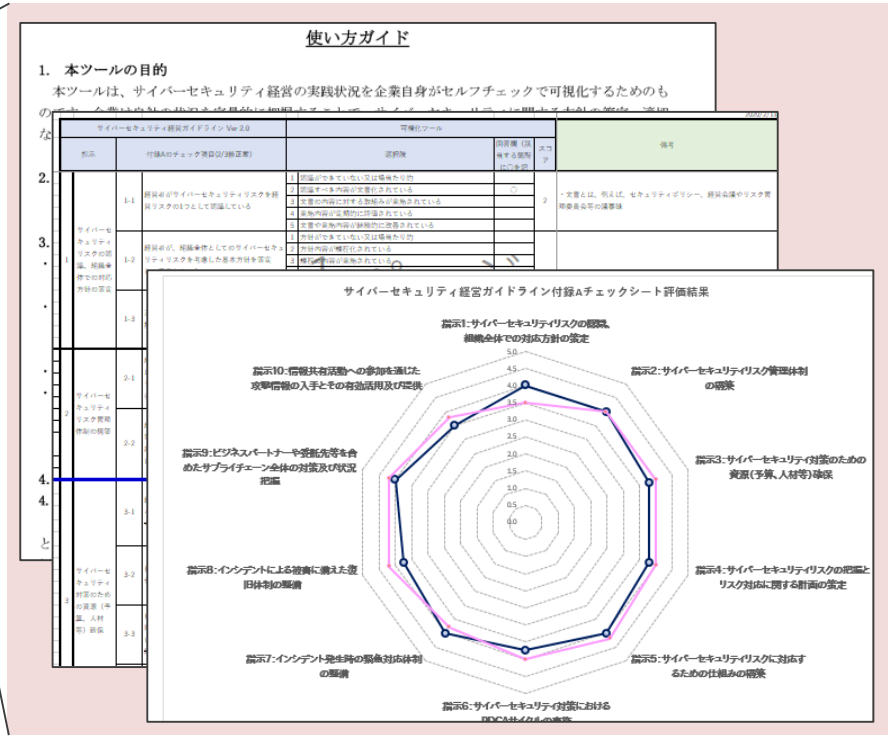
サイバーセキュリティ経営ガイドライン実践状況の可視化ツールβ版を公開

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



可視化ツールβ版の特徴：

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



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

4つのアクションプランの進捗状況

● 4つのアクションプランは順調に進捗。

＜第3回研究会(2019年4月)以降に実現された取組及び今後の取組の方向＞

1 サプライチェーンサイバーセキュリティ強化パッケージ

- **ビルシステムガイドライン**第1版策定(2019年6月)
- **スマートホームガイドライン**原案策定(2020年3月)
- **自動車ガイドライン**(2020年5月公開)
- 第3層TF、ソフトウェアTF、第2層TF開催(2019年8-2020年3月)
- 第3回**日イスラエル電力サイバーセキュリティ官民会合**(2019年11月)
- 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国際化の推進
- インド太平洋地域向け第二回**日米サイバー演習**(2019年9月)

2 サイバーセキュリティ経営強化パッケージ

- **「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)
- **経営ガイドライン可視化ツール**β版策定（2020年3月）

3 サイバーセキュリティ人材育成・活躍促進パッケージ

- セキュリティ人材モデル（**ITSS+更改版**）の策定（2020年3月）
- 産業サイバーセキュリティセンター（ICSCoE)は3期生が卒業(2020年6月)
- サイバーセキュリティ経営を進める**戦略マネジメント層の育成**
- **国立高専機構**と産・官との連携促進・具体化
- **各地域でのセキュリティコミュニティ形成**に向けた取組状況

4 セキュリティビジネスエコシステム創造パッケージ

- セキュリティ製品の**有効性検証・実環境における試行検証**
- ハイレベル検証：**機器のサイバーセキュリティ確保のための検証の手引き**策定（2020年3月）
- 中小企業向けセキュリティ製品・サービスの検証事業：**評価項目(案)**策定（2020年3月）
- **情報セキュリティサービス審査登録制度登録数が192件**に(2020年6月)

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

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

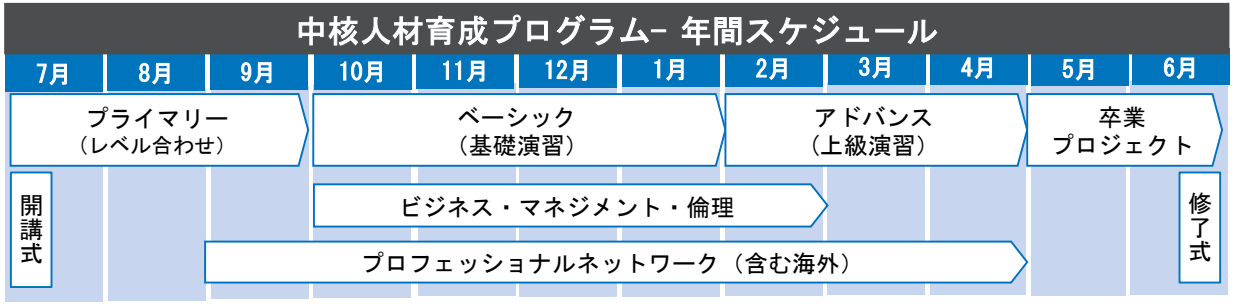
	経営層	戦略マネジメント層				実務者・技術者層			
						設計・開発・テスト		運用・保守	研究開発
ユーザ企業における組織の例	取締役会 執行役員会議	内部監査部門 （外部監査を含む）	管理部門 （総務、法務、広報、調達、人事 等）	セキュリティ統括室	経営企画部門 事業部門	デジタル部門／事業部門 （ベンダーへの外注を含む）			
セキュリティ関連タスクの例	• セキュリティ意識啓発 • 対策方針指示 • ポリシー・予算・実施事項承認	• システム監査 • セキュリティ監査	• BCP対応 • 官公庁等対応 • 法令等遵守対応 • 記者・広報対応 • 調達・契約・検収 • 施設管理・物理セキュリティ • 内部犯行対策	• リスクアセスメント • ポリシー・ガイドライン策定・管理 • セキュリティ教育 • 社内相談対応 • インシデントハンドリング	• 事業戦略立案 • システム企画 • 要件定義・仕様書作成 • プロジェクトマネジメント	• セキュアシステム要件定義 • セキュアアーキテクチャ設計 • セキュアソフトウェア方式設計 • テスト計画	• 基本・詳細設計 • セキュアプログラミング • テスト・品質保証 • パッチ開発 • 脆弱性診断	• 構成管理 • 運用設定 • 脆弱性対応 • セキュリティツールの導入・運用 • 監視・検知・対応 • インシデントレスポンス • ペネトレテスト	• 現場教育・管理 • 設備管理・保全 • 初動対応・原因究明・フォレンジック • マルウェア解析 • 脅威・脆弱性情報の収集・分析・活用	• セキュリティ理論研究 • セキュリティ技術開発
タスクに対応するセキュリティ関連分野 デジタル（IT／IoT／OT）	デジタル経営 （CIO／CDO）	システム監査			デジタル システム ストラテジー	システム アーキテクチャ	デジタル プロダクト 開発	デジタル プロダクト マネジメント		
セキュリティ	セキュリティ経営 （CISO）	セキュリティ 監査		セキュリティ統括		※クラウド、アジャイル、DevSecOps等により境界は曖昧化の傾向 ※チップ/IoT・組み込み/制御システム/OS/サーバ/NW/ソフト/Web等の取扱う技術の種類や事業分野によりタスクやスキルは大きく異なる				
その他	企業経営 （取締役）		経営リスク マネジメント 法務		事業ドメイン （戦略・企画・調達）			事業ドメイン （生産現場・事業所管理）		

産業サイバーセキュリティセンター（ICSCoE）

- 2017年4月、IPAに産業サイバーセキュリティセンターを設置。
- 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などを実施。

□　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）



- 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

サイバーセキュリティ経営を進める戦略マネジメント層の育成

- 経営層が示す戦略の下、事業継続と価値創出に係るリスクマネジメントを中心となって支える立場である「戦略マネジメント層」の育成が急務。
- このため、サイバーセキュリティ2019に基づき、IPA産業サイバーセキュリティセンターでは、2018年度に引き続き、2019年度も戦略マネジメント層向けのセミナーを実施。
- 東京工業大学CUMOTは「サイバーセキュリティ経営戦略コース」を新規開催。（IPAが後援）

産業サイバーセキュリティセンター「戦略マネジメント系セミナー」

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

東京工業大学ＣＵＭＯＴ「サイバーセキュリティ経営戦略コース」

- 令和２年１月～４月、６月～７月（予定）
- サイバーセキュリティ経営及びその戦略立案に求められる知識・能力を備え、企業・組織を先導する人材の育成を目的とする。
- 座学だけでなく、受講生同士による議論やワークショップによって理解を深める実践的なスタイルの講義を１回２時間、全14回を予定。

国立高専機構と産・官との連携促進・具体化

- METI、IPA、JPCERT及び業界団体が国立高専機構と連携し、高専生の専攻（セキュリティ、IT、その他（機械、電気等））に応じた教育コンテンツの提供や講師の派遣等、産学官連携の具体化を推進中。

使用できるインフラ
- 演習設備
- 同時中継
  （全国高専間で配信可）
- 仮想空間

国立高専卒業生 約1万人/年の内訳	コンテンツ開発・授業の提供（パワーポイント、ビデオ等）	セキュリティ合宿に関する協力
	パターン①：90分程度 ・高専教員がコンテンツを使って講義 又は 企業等の方が講義。（拠点校から全国各校に同時配信も可） **パターン②：15分程度** 授業冒頭や隙間時間でビデオ放映。	**高度セキュリティ合宿**（1泊2日） 年2回程度開催（インシデント対応演習等）参加者：35名程度 **KOSENセキュリティコンテスト**（1泊2日） 年1回程度開催（CTF）参加者：130名程度 ※開催期間中の一部の時間を利用して、一線で活躍するホワイトハッカーから講義を実施可能。
約1% トップガンの学生 → 主に**セキュリティ企業**に就職	※トップガンの学生は、全国各校、各学科に散らばっているため、通常の授業時間で集合する機会がない。  ゲーム形式教材のイメージ	• **JNSAが講師の派遣を検討中。** • **METIがセキュリティ専門官を高度セキュリティ合宿に講師として派遣。**  開催の様子@石川高専
約20% 情報系学科の学生 → 主に**IT企業**に就職	• **JNSAのゲーム形式教材を石川高専と連携してアプリ化。** ※JNSA：NPO日本ネットワークセキュリティ協会 • **四国地域企業のIPA ICSCoE終了生が講義を検討中。** • **日立製作所が一関高専生向けに出前授業、インターンシップを実施し、出前授業は全国各校に配信。**	• **JNSAとSECCONビギナーズを石川高専と苫小牧高専で開催。** • **JNSAがCTFビギナーズfor高専生@木更津高専に講師を派遣。** • **IPAが高度セキュリティ合宿に講師を派遣し、App Goat（脆弱性体験学習ツール）の講習会を開催。** • **METIがセキュリティ専門官を高知高専に派遣し、出前授業を実施。**
約80% 非情報系学科の学生 → 主に**ユーザー企業**に就職	• **CRICが佐世保高専と連携し、業界別（例．機械、電気、建築等）ビデオ教材（20分程度）を作成中。** ※CRIC：一般社団法人サイバーリスク情報センター	※セキュリティ合宿のような機会は特段なし。  AppGoat講習の様子
KOSEN 国立高等専門学校機構 国立高専教員	※授業実施側のため。	• **IPAが教員向けにAppGoat講習会を開催。** • **JPCERT/CCが情報担当教員向け研修に講師を派遣。** • **教員がIPAのセキュリティキャンプ全国大会を見学。** • **教師向け合宿で、METIがセキュリティ専門官の派遣を検討中。**

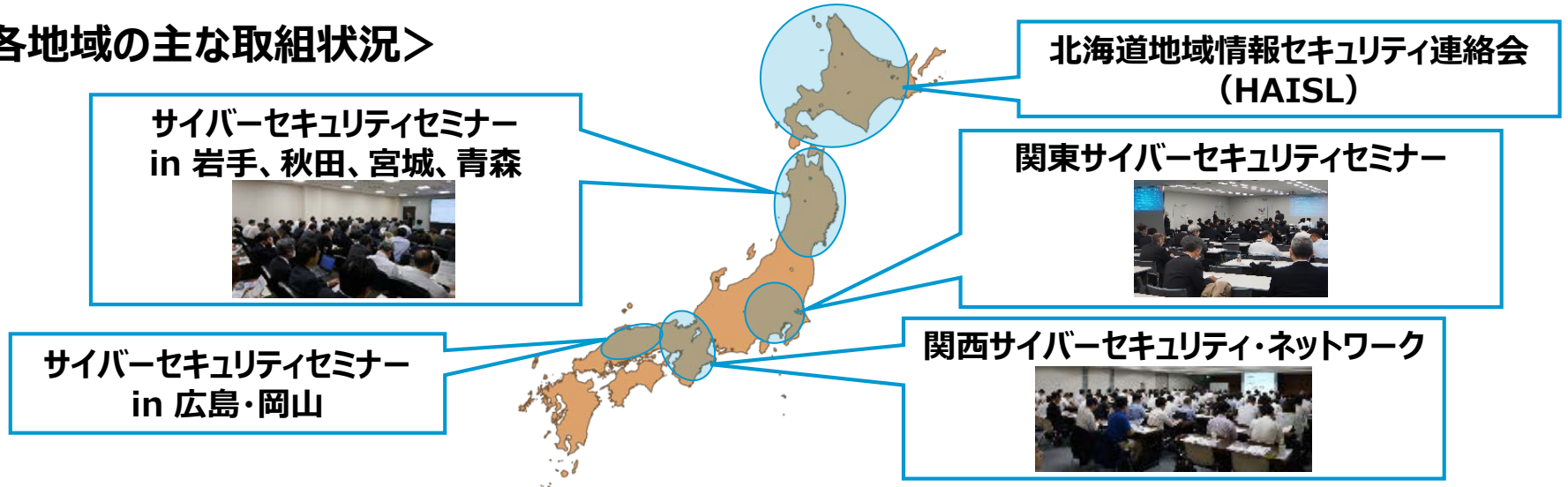
セキュリティスキルレベル

地域に根付いたセキュリティ・コミュニティ（地域SECUNITY）の形成促進

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

＜地域SECUNITYのコンセプト＞

＜各地域の主な取組状況＞



4つのアクションプランの進捗状況

- 4つのアクションプランは順調に進捗。

＜第3回研究会(2019年4月)以降に実現された取組及び今後の取組の方向＞

1 サプライチェーンサイバーセキュリティ強化パッケージ

- **ビルシステムガイドライン**第1版策定(2019年6月)
- **スマートホームガイドライン**原案策定(2020年3月)
- **自動車ガイドライン**(2020年5月公開)
- 第3層TF、ソフトウェアTF、第2層TF開催(2019年8-2020年3月)
- 第3回**日イスラエル電力サイバーセキュリティ官民会合**(2019年11月)
- 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国際化の推進
- インド太平洋地域向け第二回**日米サイバー演習**(2019年9月)

2 サイバーセキュリティ経営強化パッケージ

- **「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)
- **経営ガイドライン可視化ツール**β版策定（2020年3月）

3 サイバーセキュリティ人材育成・活躍促進パッケージ

- セキュリティ人材モデル（**ITSS+更改版**）の策定（2020年3月）
- 産業サイバーセキュリティセンター（ICSCoE)は3期生が卒業(2020年6月)
- サイバーセキュリティ経営を進める**戦略マネジメント層の育成**
- **国立高専機構**と産・官との連携促進・具体化
- **各地域でのセキュリティコミュニティ形成**に向けた取組状況

4 セキュリティビジネスエコシステム創造パッケージ

- セキュリティ製品の**有効性検証・実環境における試行検証**
- ハイレベル検証：**機器のサイバーセキュリティ確保のための検証の手引き**策定（2020年3月）
- 中小企業向けセキュリティ製品・サービスの検証事業：**評価項目(案)**策定（2020年3月）
- **情報セキュリティサービス審査登録制度登録数が192件**に(2020年6月)

包括的なサイバーセキュリティ検証基盤を構築し、『Proven in Japan』を促進

- 「Proven in Japan」では、2つの方向を追求し、**セキュリティビジネスの成長を促進**。

① 有効性確認等を通じ、日本発のサイバーセキュリティ製品のマーケット・インを促進

② IoT機器等の信頼性を高度に検証するハイレベル検証サービスの拡大

1．セキュリティ製品の有効性検証

2．実環境における試行検証

3．攻撃型を含めたハイレベルな検証サービス

信頼できる
セキュリティ製品・サービス

世界に貢献する
高水準・高信頼の検証サービス

信頼できるセキュリティ製品・サービスの創出
（セキュリティ製品の有効性検証・実環境における試行検証）

- ベンダー、ユーザ、有識者の協力を得て、製品の有効性検証と実環境における試行検証をそれぞれ実施。成果物として、製品のアピールポイント、導入事例公表の手引き(案)を整理し、2020年4月10日に重要分野マップとともに公表（IPA）。
- 日本発のサイバーセキュリティ製品の更なる創出とビジネス拡大を促進する。

2019年度検証内容

1. セキュリティ製品の有効性検証

yamory
- OSSに特化した脆弱性管理ツール
- ビジョナル・インキュベーション社製

2. 実環境における試行検証

AX-Network Visualization
- ネットワーク脅威可視化ツール
- アラクサラネットワークス社製

成果公表
（IPA、2020年4月10日）

① 2019年度版セキュリティ製品・サービス重要分野マップ
- 市場性、日本発の製品が強味を発揮可能か等の観点から作成

② セキュリティ製品の有効性検証の検証結果について
- 製品のストロングポイントの検証結果

③ 実環境における試行検証の検証結果について（手引き(案)）
- 導入事例を公開する際のポイント
  - ✓ 公開可否判断
  - ✓ 公表内容
  - ✓ 公表方法、公表対象 等

https://www.ipa.go.jp/security/economics/shikoukekka2019.html

日本発の製品創出

ビジネス拡大

『Proven in Japan』の促進

赤

Society5.0時代の信頼性確保のために必要となる 攻撃型手法を含むハイレベルな検証サービスの普及展開へ向けた実証

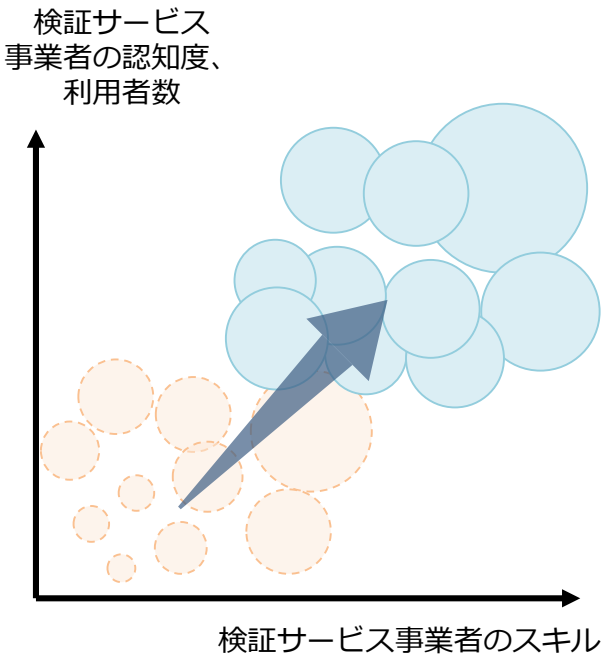
- 2019年度は、IoT機器等についてホワイトハッカー等を有する実力のある検証事業者による攻撃的手法を含むハイレベルな検証を通じて、信頼できる事業者を確認する仕組みや、事業者と利用者間のコミュニケーション、機器ごとの効果的な検証手法等の考え方を第一弾の**手引きとして整理**。
- 2020年度は、昨年度実施した機器とは異なる機器を対象として事業を実施するとともに、将来的に検証事業に活用でき得る技術に関する調査等を通じて、手引きの充実を図る。

検証事業者

検証

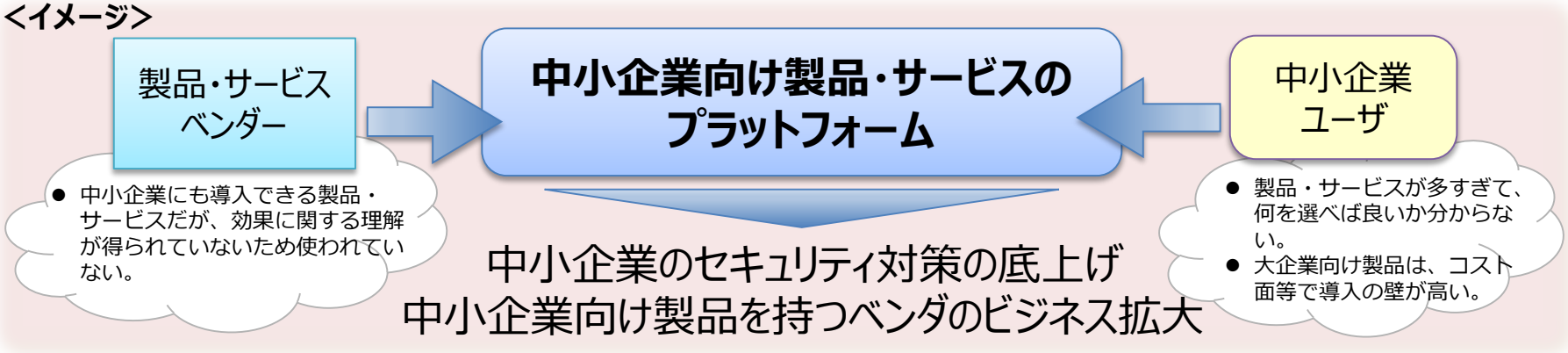
・IoT機器等
＜2019年度＞
ルータ、UTM、タブレット、スマートロック
＜2020年度＞
R1年度とは異なる機器

①様々な検証手法を用いた機器・システムごとの検証結果
→IoT機器等ごとに効果的な検証手法の考え方を整理
②検証事業者に求められる信頼性等の考え方の整理
→適切な情報管理を行う主体としての信頼性や、質の高い検証を行うことができる事業者としての信頼性について検討
③検証事業者と利用者間のコミュニケーション手法の整理
→検証サービスへの認知及び利用者の増加



中小企業向けセキュリティ製品・サービス検証基盤

- 中小企業向けセキュリティ製品・サービスが中小企業のニーズにマッチしているか検証することで、中小企業向け製品のビジネス確立と、中小企業のセキュリティ対策底上げを図る。
- 昨年度、ベンダー及びユーザ企業の協力を得て検証を実施し、中小企業向け製品・サービスの評価項目(案)と中小企業向け情報提供のあり方を整理。



協力ベンダー３社（公募）

ユーザ６社の実環境に導入・運用

- eGIS イージス株式会社 → A社：製造業、45名 / B社：製造業、15名
- NTT Communications Go the Distance. → C社：SI業、121名 / D社：ガス供給業、158名
- Blue Planet-works Safety for the Connected World → E社：NI業、18名 / F社：卸売業、14名

ヒアリング

昨年度検証結果

ユーザが特に重視する評価項目

- 導入及び運用のコスト
- 製品性能の客観的な根拠
- オールインワン　等

中小企業向けの情報提供のあり方

- ユーザ目線の解説情報
- 掲載情報の信頼性確保
- 自社のニーズにマッチした情報を検索可能 等

情報セキュリティサービス審査登録制度

- 2019年度は**制度の認知度向上と登録サービス数増加**を目指し、全国各地のセミナーでの制度紹介や個別ベンダへの働きかけ等を実施。現在の登録サービス件数は**192件**。

2019年度の取組

登録サービス数増加に向けた各種施策：

- 全国の**セミナーでの制度紹介**（50回程度）
- 業界団体や地方経産局等と連携して**個別ベンダへの周知実施**
- **制度紹介パンフレット**の作成・配布※
- 経産省**入札案件への引用**（ベンダーメリットの明確化）

制度の信頼性確保（2018年度から継続）

- リストに掲載されたサービスに対しての**サーベイランス実施**

※ユーザ向けパンフレット

＜参考＞登録ベンダーの所在地

- **情報セキュリティ監査**（54サービス）　**東京42**、神奈川5、埼玉2、兵庫2、京都1、大阪1、広島1
- **脆弱性診断**（76サービス）　**東京60**、神奈川6、大阪3、兵庫2、宮城1、新潟1、茨城1、大分1、沖縄1
- **デジタルフォレンジック**（26サービス）　**東京21**、神奈川3、兵庫1、熊本1
- **セキュリティ監視・運用**（36サービス）　**東京27**、神奈川6、大阪1、兵庫1、大分1

⇒ **登録サービスの約８割が東京に集中。本制度を地方にも普及・浸透させるため、地方に所在するベンダーの登録数を増やす取り組みも続ける。**（特に、ユーザ環境での作業が必要になる情報セキュリティ監査と脆弱性診断）


METI
Ministry of Economy, Trade and Industry