経済産業省
Ministry of Economy, Trade and Industry

産業分野における
サイバーセキュリティ政策

経済産業省　商務情報政策局
サイバーセキュリティ課
鴨　田　浩　明

１．サイバー攻撃の動向

２．欧米の標準化動向

３．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

４．WG1：「Society5.0」において必要なセキュリティ対策
～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策定

５．WG2：サイバーセキュリティ対策の基盤整備
～経営、人材育成、中小企業

６．WG3：サイバーセキュリティビジネスの創出
～エコシステムの構築

(独)情報処理推進機構：情報セキュリティ10大脅威 2020

昨年順位	個　人	順　位	組　織	昨年順位
↗ ランク外	スマホ決済の不正利用 NEW	1位	標的型攻撃による情報流出	1位 →
→ 2位	フィッシングによる個人情報の詐取	2位	内部不正による情報漏えい	5位 ↗
↘ 1位	クレジットカード情報の不正利用	3位	ビジネスメール詐欺による金銭被害	2位 ↘
↗ 7位	インターネットバンキングの不正利用	4位	**サプライチェーンの弱点を悪用した攻撃**	4位 →
↘ 4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5位	ランサムウェアによる被害	3位 ↘
↘ 3位	不正アプリによるスマートフォン利用者への被害	6位	予期せぬIT基盤の障害に伴う業務停止	16位 ↗
↘ 5位	ネット上の誹謗・中傷・デマ	7位	不注意による情報漏えい（規則は遵守）	10位 ↗
→ 8位	インターネット上のサービスへの不正ログイン	8位	インターネット上のサービスからの個人情報の窃取	7位 ↘
↘ 6位	偽警告によるインターネット詐欺	9位	**IoT機器の不正利用**	8位 ↘
↘ 12位	インターネット上のサービスからの個人情報の窃取	10位	サービス妨害攻撃によるサービスの停止	6位 ↘

<出典：情報処理推進機構、2020.1.29.>

サイバー攻撃の脅威レベルの増大（制御系にまで影響が波及）
（情報システムを越えて制御システムに達する攻撃（垂直的脅威））

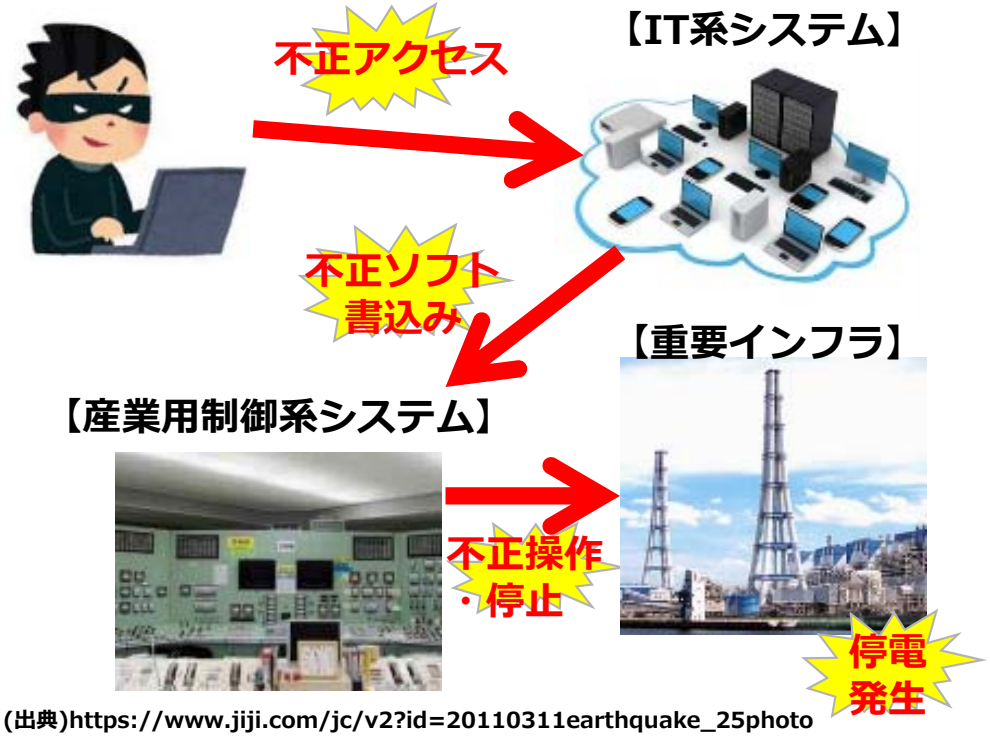
- 米国ICS-CERTの報告では、**重要インフラ事業者等において、制御系にも被害が生じている**。
- ウクライナでは、2015年と2016年にサイバー攻撃による停電が発生。**2016年の攻撃(CrashOverRide)**では、**サイバー攻撃のみで、停電が起こされた**。

米国の重要インフラへのサイバー攻撃の深さ

攻撃のうち約一割は、制御系までサイバー攻撃が到達

（出典）NCCIC/ICS-CERT Year in Review FY2015
Homeland Security より経済産業省作成

2016年に発生したウクライナの停電に係る攻撃（CrashOverRide(Industryoyer)）



(出典)https://www.jiji.com/jc/v2?id=20110311earthquake_25photo
(出典)www.chuden.co.jp/hekinan-pr/guide/facilities/thermalpower.html

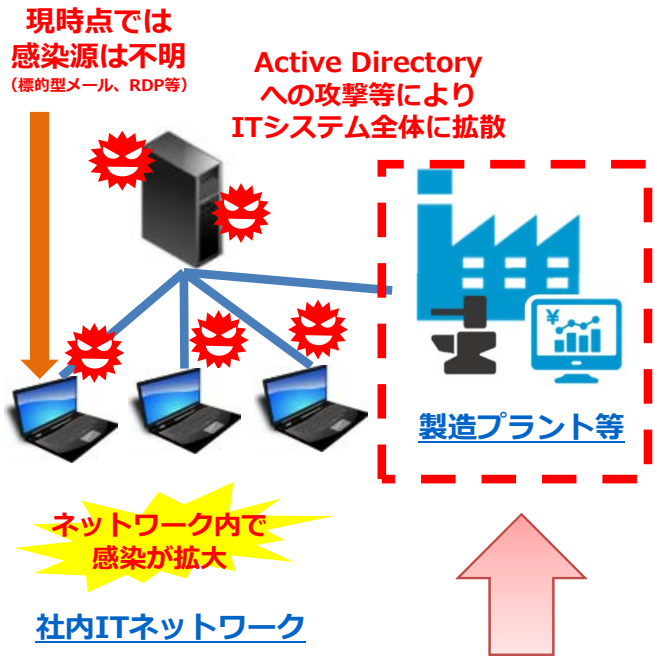
ランサムウェア(LockerGoga)によるノルウェーのアルミ精錬・加工企業への事業被害（情報システムを越えて制御システムに達する攻撃（垂直的脅威））

- 2019年3月、ノルスク・ハイドロ社（ノルウェーを拠点とする世界最大級のアルミニウム製錬・加工企業）が、ランサムウェア「LockerGoga」による被害を受けた。
- アルミニウム製造・発電プラントのITシステムからの切り離し及び手動操作への切り替え、プレス加工等の一時的な生産停止など、**感染確認から1週間で4000万ドルに相当する事業被害**。

本事案の詳細（原因・影響）

- 2019年3月19日、**ノルスク・ハイドロ社はランサムウェア「LockerGoga」への感染・大規模なシステム障害**を発表。
- 感染経路は不明（2019年３月時点）。
- ログオンシステム（ADサーバ）への攻撃を通じた感染拡大により、ほとんどの事業部門のITシステムが影響。
- **感染拡大・拡散防止のため、グローバルなITシステム全体を停止**。
- オフィス業務への影響の他、**プレス加工等の一時的な生産停止や、アルミニウム製造や発電プラントをITシステムから切り離して手動操作に切り替えるなどの影響**が生じた。
- 身代金の支払いには応じていないが、**感染の確認から1週間で4000万ドルに相当する事業への被害を確認**。

事案のイメージ



OSSライブラリに悪意のあるコードが仕込まれる：Copay

- 仮想通貨（暗号資産）のウォレットアプリ「Copay」にユーザーの仮想通貨を盗み出すバックドアが仕掛けられて公開されていた。
- 攻撃者はCopay本体ではなく、Copayが利用する外部ライブラリの一つ（event-stream）を正規の権限で編集し、悪意のあるコードが仕込まれた外部ライブラリ（flatmap-stream）に関連させることでバックドアを仕掛けた。
- 悪意あるコードを追加する工程を複雑にし、かつ隠蔽を行うことで発覚を遅らせようとした。

2017.10 ・開発者によるevent-streamの最終更新

⋮

2018.8末 ・攻撃者がevent-streamの開発者に**「メンテナンスを引き継ぎたい」と持ちかけメンテナンス権限を取得**

2018.9.9 ・攻撃者がevent-streamを更新 → event-streamがflatmap-streamと関連

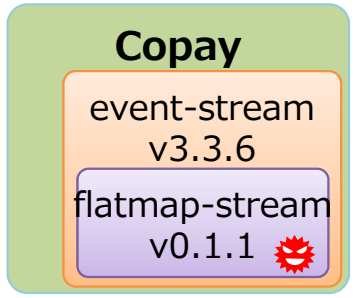
2018.10.5 ・攻撃者がflatmap-streamに**悪意のあるコードを追加**

2018.10.26 ・Copayが更新

→ Copayが悪意のあるコードが仕込まれたflatmap-stream に関連するようになり、攻撃者がバックドアを利用できるように

⋮

2018.11.26 ・ニュースになり、 flatmap-streamは削除された



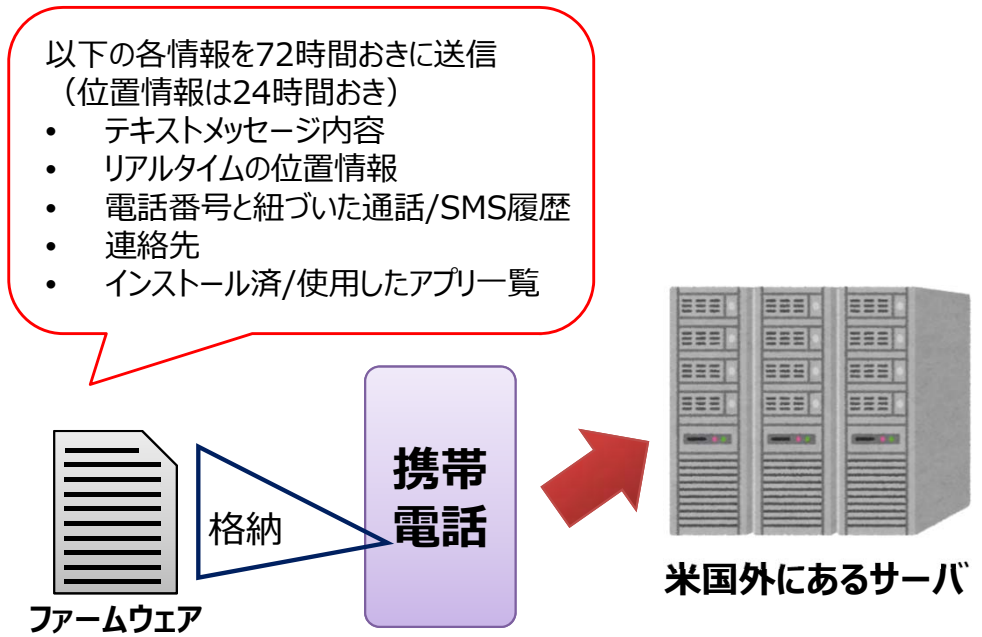
IoT機器のサプライチェーンリスク：信頼性の低い機器の販売による事業リスク

- 2016年11月、米国メーカーが販売していたスマートフォンのファームウェアが、消費者の同意を得ること無く、個人情報を海外サーバに送信していたことが判明。
- 米国連邦取引委員会（FTC）は、当該メーカーが開示する個人情報取扱方針に反する行為として提訴。当該メーカーが包括的なセキュリティプログラムを実装し、継続的な第三者評価を受けること等を条件に和解。

当該米国メーカーに対する命令

1. 個人情報のプライバシー、機密性、安全性、完全性の保護に関する誤認表示の禁止
2. 端末に関連するセキュリティリスクに対処し、個人情報を保護するための包括的なセキュリティプログラムの実装及び維持
3. 第三者による上記セキュリティプログラムの監査（2年毎に20年間）
4. 個人情報を収集し、他者に開示する際に、利用者に通知を行い、明確な同意を得る
5. コンプライアンス報告書の提出
6. 販売記録などの管理（20年間）

事案のイメージ



スマートスピーカーを悪用したフィッシング攻撃

- 2019年10月、ドイツのセキュリティ研究機関 SRLabs（Security Research Labs）が、スマートスピーカーの機能を悪用し、ユーザのパスワードの窃取や会話の盗聴が可能であることを公表。
- スマートスピーカーは、特定のフレーズを認識することでそれに対応した機能を実行するが、特定のフレーズに続く内容をテキスト化してサーバに送信する機能がある。
- スマートスピーカーのアプリストアに相当するAlexa SkillやGoogle Assistantの審査を、無害なアプリを装って通過した後に、メッセージを改変する手法によるフィッシングなど（※）、当該機能を利用してユーザの個人情報等を窃取するスマートスピーカーを通じた攻撃手法が実証された。

※攻撃プロセスの概要

●偽のメッセージでフィッシング

1．特定のフレーズ（e.g.「Start」）に続く内容をサーバに送信する、一見して無害なアプリを作成。
2．審査通過後、最初のメッセージをエラーメッセージのように改変（e.g.「現在この機能は利用できません。」）。
3．スピーカーにフィッシングメッセージを発声させる（e.g.「重要なアップデートがあります。Start updateに続いてパスワードを発声してください。」）。
4．「Start」の後にユーザが発声したパスワードがサーバに送信される。

●アプリの終了を誤認させて盗聴

1．一見して無害なアプリを作成。
2．審査通過後、アプリの終了時等に「Good Bye」と発声させた後、スピーカーが音声化できない文字列（e.g.“ . “）を繰り返すことで、アプリの動作を継続させるようアプリを改変。
3．２．の終了音やメッセージを聞いたユーザは、アプリが停止したと錯覚。
4．アプリが動作している間にユーザが特定のキーワードを発声した場合、それがサーバへ送信される。

https://srlabs.de/bites/smart-spies/

航空機の脆弱性に関するBlack Hat USA 2019での報告

- 2018年9月、大手航空機メーカーのサーバにおいて、航空機の**システム構成に関する情報がインターネット上に公開**されていることが発覚。IOActive社(I社)は、特定の脆弱性を用い、機内エンターテイメントシステム等から、**機器の操作に関わるネットワークに到達できることを発見**し、メーカーに報告。メーカーはI社に対して、報告されたのは**悪用可能な脆弱性ではなく、緩和策も実施済と回答するも、詳細は不開示**。
- これに失望したI社は2019年8月の**Black Hatで脆弱性の詳細を公開**。
- これを受けメーカーは、I社は航空機ネットワークの一部を評価しただけで、I社のシナリオでは**重要な航空機システムに影響を与えることはできず、発表は無責任だと失望を表明**。

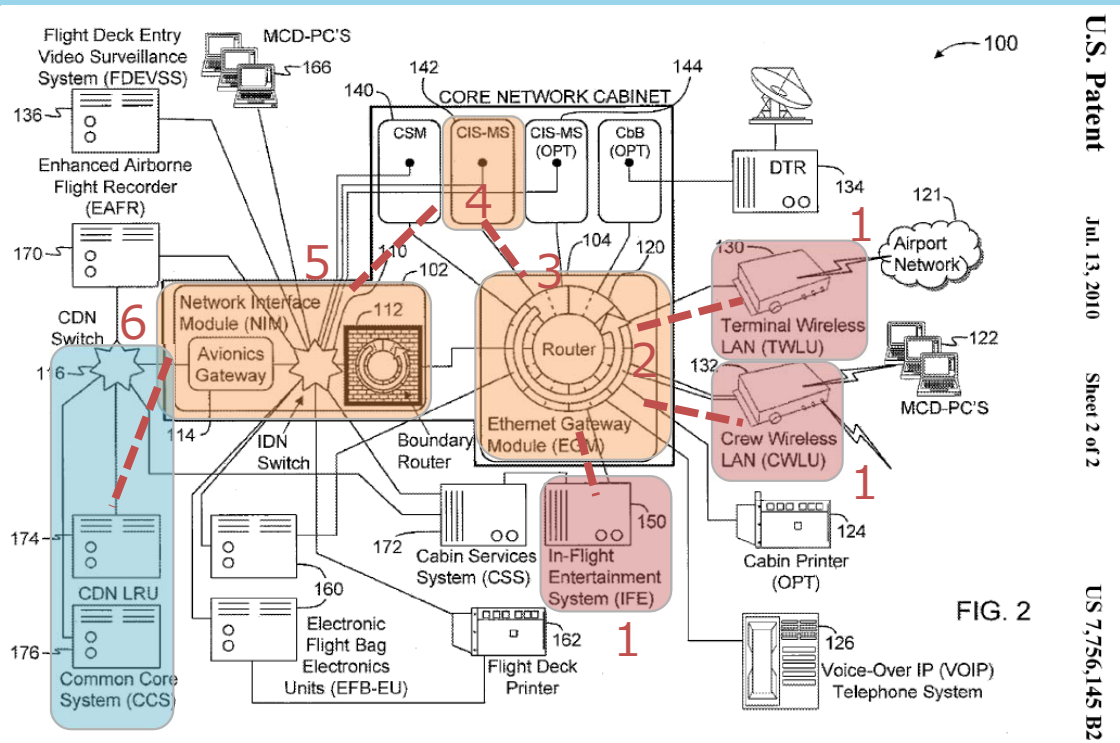


FIG. 2

U.S. Patent Jul. 13, 2010 Sheet 2 of 2 US 7,756,145 B2

●基本的な攻撃対象の解説図

1の機内エンターテイメントシステムや外部ネットワークから、6の機体の操作やナビゲーションに関連するとされるネットワークに到達できると解説されている。

https://ioactive.com/arm-ida-and-cross-check-reversing-the-787s-core-network/
https://www.wired.com/story/boeing-787-code-leak-security-flaws/

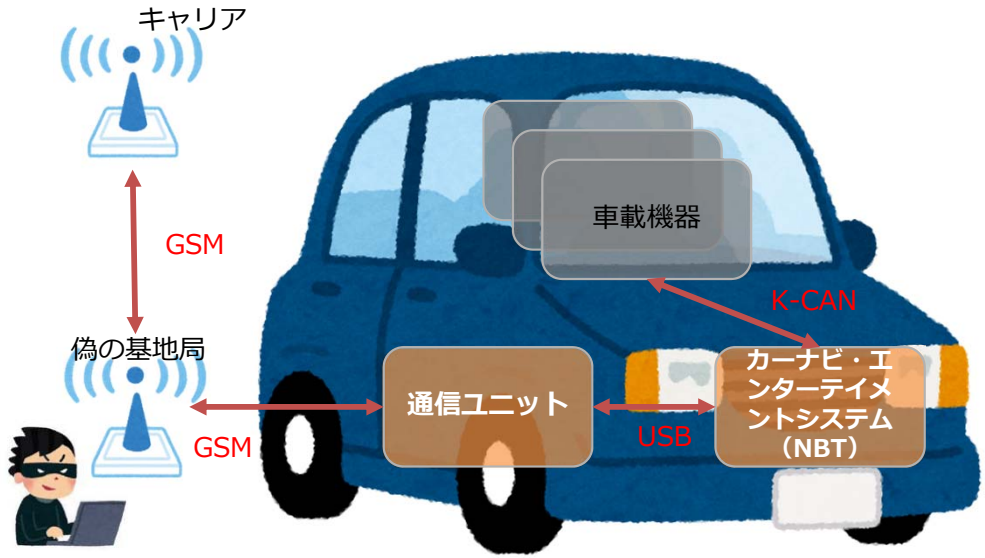
自動車の脆弱性に関するBlack Hat USA 2019での報告

- 2018年2月、中国Tencent社のKeen Security labは、大手自動車メーカーの自動車の脆弱性を検証してメーカーに通知。これを受け、メーカーは緩和策を実施。また、Keen labは、責任ある開示（Responsible Disclosure)方針に従い、2019年8月のBlack Hatにおいて、分析結果、検証内容及び対応策の詳細をメーカーと**共同発表**した。
- 報告では、カーナビやエンターテイメントシステムを提供する車載機器の脆弱性を用いて、偽の携帯電話ネットワークからSMSを送付する等の操作により、ドアの開錠や任意コード実行等の操作が行えたとしている。

＜開示プロセス＞

2017年2月～2018年2月	Keen labが自動車の脆弱性及び攻撃チェーンを検証し、メーカーに通知
2018年3月	メーカーは通知された脆弱性を確認し、緩和策を計画
2018年4月	脆弱性に関するCVE番号が予約
2018年5月	Keen labが概要レポートを一般公開
2018年夏	メーカーが必要な対策と緩和策を実施
2019年8月	Black Hatにおいて共同発表、詳細レポートを公開

＜偽GSM基地局を用いた遠隔攻撃イメージ＞



https://www.blackhat.com/us-19/briefings/schedule/#-days--mitigations-roadways-to-exploit-and-secure-connected-bmw-cars-15313

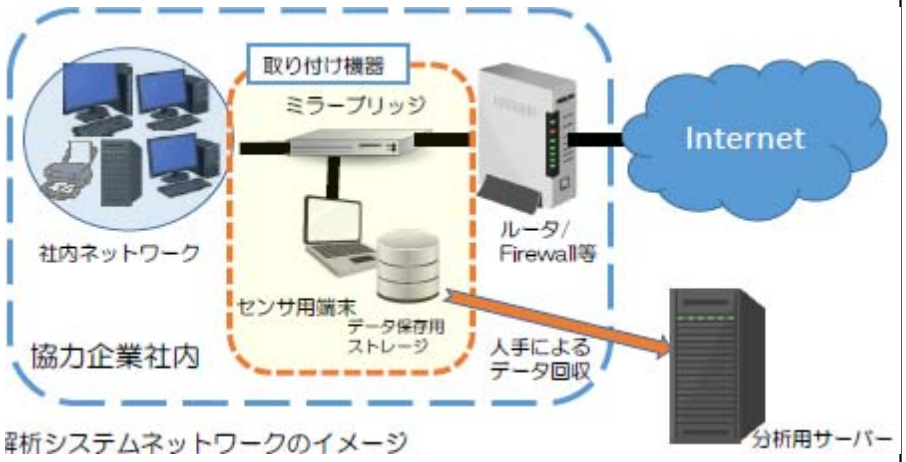
中小企業に対するサイバー攻撃の調査･分析結果（大阪商工会議所）

- 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（中間報告）

- 調査した**30社全てでサイバー攻撃**を受けていたことを示す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。

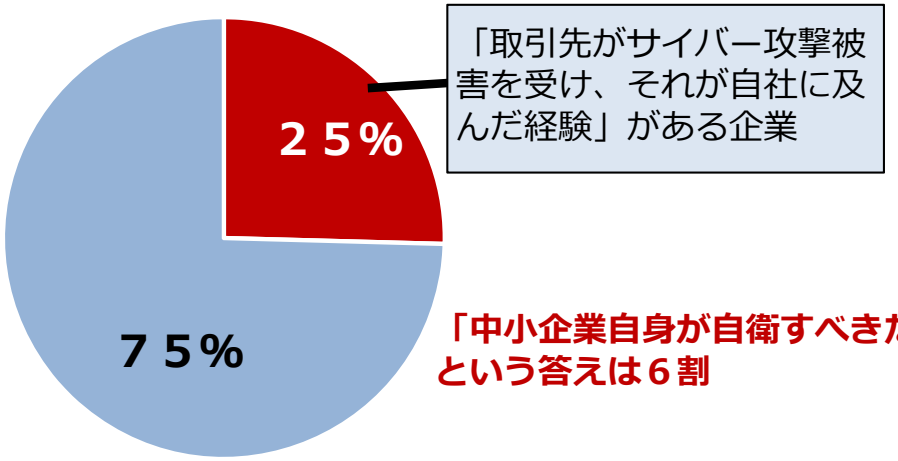
取引先経由の被害に関する調査

■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（中間報告）

- 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%）**



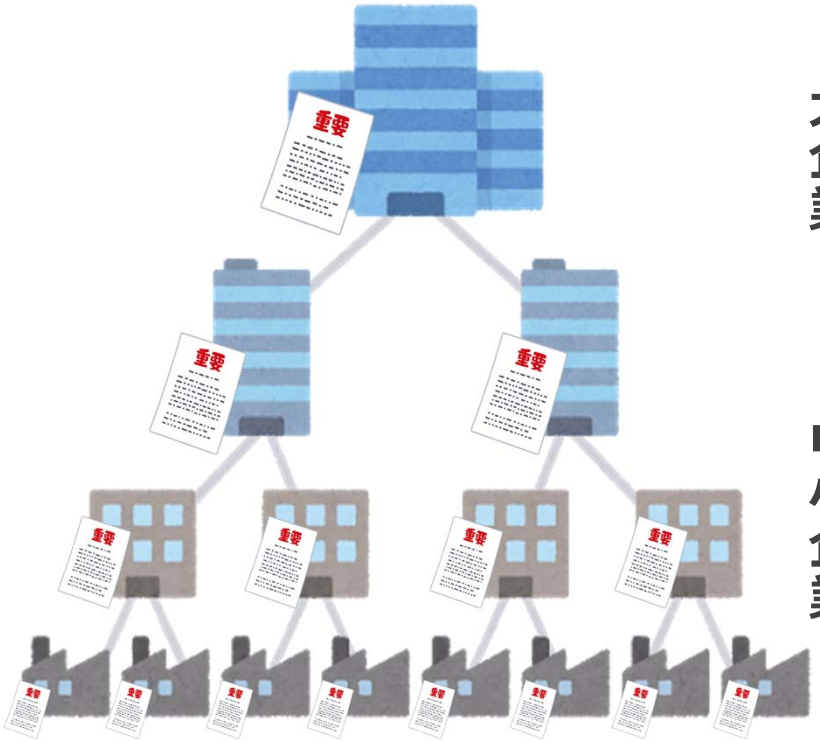
出典：大阪商工会議所「サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査」（2019年5月）

<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）>

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

2020年6月12日公開資料

- **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。

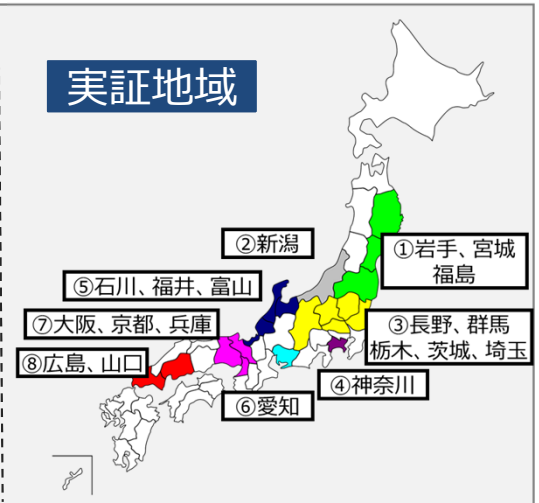


大企業

- 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。

中小企業

- 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

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

（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．サイバー攻撃の動向

２．欧米の標準化動向

３．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

４．WG1：「Society5.0」において必要なセキュリティ対策
～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策定

５．WG2：サイバーセキュリティ対策の基盤整備
～経営、人材育成、中小企業

６．WG3：サイバーセキュリティビジネスの創出
～エコシステムの構築

NISTIR 8228 – Consideration for Managing IoT Cybersecurity and Privacy Risks

- IoT機器の導入に伴い生じる、**サイバーセキュリティとプライバシーのリスクを軽減するための推奨事項**を整理。（2019年6月発行）
- IoT機器の機能の多様性を踏まえ、機器のセキュリティ、データのセキュリティ、個人のプライバシー情報という３つの観点からIoTデバイスにおいて生じうる懸念を列記し、NIST Cybersecurity Framework、SP 800-53 Rev.5（Draft）との対応関係を整理。

IT機器と比較して、IoT機器がサイバーセキュリティリスク、プライバシーリスクに影響を与えうる３つの懸念

物理世界とデバイスとの相互作用	IoT機器の多くは、従来のIT機器では通常行わない方法で物理世界とのやりとりを行う。
デバイスアクセス、管理、モニタリング機能	IoT機器の多くは、従来のIT機器と同じ方法でアクセス、管理、監視することができない。
サイバーセキュリティ機能、プライバシー機能の可用性、効率、有効性	IoT機器のためのサイバーセキュリティ機能、プライバイシー機能の可用性、効率、有効性は、従来のIT機器とは異なる。

IoT機器のサイバーセキュリティリスク、プライバシーリスクを軽減する対処領域

機器のセキュリティを守る	• アセットの管理、脆弱性管理、アクセス管理、機器のセキュリティインシデント検知
データのセキュリティを守る	• データ保護、データのセキュリティインシデント検知
個人のプライバシー情報を守る	• 情報フローの管理、特定個人情報の処理権限の管理、特定個人情報の提供に際する意思決定、データ管理との分離、プライバシー違反の検知

NISTIR 8259 – Foundational Cybersecurity Activities for IoT Device Manufacturers

- IoT機器を管理する組織向けの推奨事項をまとめたNISTIR 8228に対し、**IoT機器の製造者に推奨される6つのサイバーセキュリティに関連する活動**を整理(2020年5 月に最終版を公開)。なお、関連文書であるNISTIR 8259Aにて、**6つのサイバーセキュリティ機能**※1**をIoT機器が備えるべきベースラインと定義**した上で、当該機能を達成するために実装すべき共通の要素や、既存のIoTセキュリティガイダンスへの参照を記載。

※1 なお、NISTIR 8259Aではこれらのサイバーセキュリティの機能の実装を必須としていない。

製造者に推奨されるサイバーセキュリティ関連活動

販売前に影響する活動	活動1：予想される顧客特定、ユースケース定義 活動2：顧客が有するサイバーセキュリティのニーズ及び目的の調査 活動3：顧客のニーズ及び目的への対処方法の決定（NISTIR 8259Aにてベースラインとなるコアサイバーセキュリティ機能を定義） 活動4：顧客のニーズ及び目的の適切なサポートに向けた計画（ハードウェア、ソフトウェアの適切なプロビジョニング、ビジネスリソースの考慮）
販売後に影響する活動	活動5：顧客とのコミュニケーションアプローチ定義 活動6：顧客に伝える内容と伝達方法の決定（製造業者の設計・開発時のリスク関連の仮説、サポートと寿命、デバイス構成・機能、ソフトウェアの更新、デバイスの廃止オプション、技術的及び非技術的手段）

6つのコアサイバーセキュリティ機能（NISTIR 8259Aにて定義）

（1）**機器の識別**： IoT機器を論理的・物理的に一意に識別できる。	（4）**インターフェイスへの論理アクセス**： IoT機器のインターフェースへの論理アクセス、及びインターフェイスで利用されるプロトコルとサービスを正規のエンティティのみに制限できる。
（2）**デバイスの構成**： IoT機器のソフトウェアの構成変更を、正規のエンティティのみが行うことができる。	（5）**ソフトウェアの更新**： IoT機器のソフトウェアは、安全かつ設定可能なメカニズムを用いる正規のエンティティにみによってのみ更新できる。
（3）**データ保護**： IoT機器が保存・伝送するデータを不正アクセス及び改ざんから保護することができる。	（6）**サイバーセキュリティ状態認識**： IoT機器は自身のセキュリティに関する状態を報告し、その情報に対するアクセスを正規のエンティティのみに制限する。

欧州サイバーセキュリティ認証フレームワーク

- 「Cybersecurity Certification Framework」の創設を含む「Cybersecurity Act」は、2019年4月9日に欧州理事会で採択され、6月27日に発効。
- 「Cybersecurity Act」に基づき、ENISAが具体的な産業分野毎に「候補スキーム(Candidate Scheme)」を欧州委員会に提案し、順次、認証フレームワークが策定される予定。

欧州委員会、ENISAの動向

- 2019年4月、Cybersecurity Act が欧州理事会で採択、6月27日に発効。
- **2019年9月、ENISAがサイバーセキュリティ認証スキームの候補を準備するためのアドホックワーキンググループの設立を呼びかけ。候補スキームとしてCommon Criteria(ISO/IEC 15408)も考えられるとの記載もある。**
- 2020年2月、ENISAがIoT、クラウドインフラ及びクラウドサービス、電子医療記録、トラストサービス等の4分野について、欧州サイバーセキュリティ認証フレームワークの「候補スキーム(Candidate Scheme)」を提案するホワイトペーパーを公開。

Cybersecurity Actの概要

- 欧州委員会は、欧州サイバーセキュリティ認証スキームの対象となるICT製品、サービス、プロセス、カテゴリのリストを含む「Union rolling work programme」を発行。最初の「Union rolling work programme」は2020年6月28日までに発行される（Article 47）。
- 本スキームでは、ICT製品等について、インシデントの可能性と影響の観点を考慮し、「basic」、「substantial」または「high」のいずれかの保証レベルを1つ以上特定する（Article 52）。
- ICT製品等の製造者又は提供者は、保証レベル「basic」に対応する低リスクを示すICT製品等について、本スキームに示されている要件の充足が実証されていることを示すEU適合宣言をボランタリーに発行することができる（Article 53）。
- 本スキームには、評価に適用される国際規格、欧州規格又は国内規格への参照及び第三国との認証制度の相互承認のための条件等が含まれる（Article 54）。
- 欧州委員会は、サイバーセキュリティ認証スキームが義務づけられることによって、ICT製品等の適切なレベルのサイバーセキュリティを確保し、国内市場の機能を改善することに効果があるか定期的にアセスメントを行う。最初のアセスメントは2023年末までに行われ、その後は少なくとも2年ごとに行われる（Article 56）

消費者向けIoT製品のセキュリティに関する行動規範（英国）

- 英国デジタル・文化・メディア・スポーツ省（DCMS）が、消費者向けIoT製品の開発、製造及び販売の段階で安全が確保されるよう、**製造メーカー等が実践すべき対策を13項目のガイドライン**にまとめ、2018年10月に公表。
- 一部の項目の義務化法案について2019年5月～6月にかけてパブリックコメントを実施。コメントを踏まえた**ドラフト法案を2020年1月に公開。**

ベストプラクティス一覧（13項目）

1. デフォルトパスワードを使用しない
2. 脆弱性の情報公開ポリシを策定する
3. ソフトウェアを定期的に更新する
4. 認証情報とセキュリティ上重要な情報を安全に保存する
5. 安全に通信する
6. 攻撃対象になる場所を最小限に抑える
7. ソフトウェアの完全性を確保する
8. 個人データの保護を徹底する
9. ネットワーク停止・停電に対するシステムのレジリエンスを確保する
10. システムの遠隔データを監視する
11. 消費者が個人データを容易に削除できるようにする
12. デバイスの設置とメンテナンスを容易にできるようにする
13. 入力データを検証する

義務化項目の案（3項目）

① IoTデバイスのパスワードはユニークにする、かつ工場出荷時の共通設定にリセットできないようにする

② IoT製品メーカーは脆弱性開示ポリシーの一部として連絡先を提供する

③ IoT製品メーカーはデバイスに対するセキュリティアップデートを提供する最低期間を明示する

１．サイバー攻撃の動向

２．欧米の標準化動向

３．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

４．WG1：「Society5.0」において必要なセキュリティ対策
～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策定

５．WG2：サイバーセキュリティ対策の基盤整備
～経営、人材育成、中小企業

６．WG3：サイバーセキュリティビジネスの創出
～エコシステムの構築

産業サイバーセキュリティ研究会とWGの設置による検討体制

産業サイバーセキュリティ研究会

第１回：平成29年12月27日　開催
第２回：平成30年　5月30日　開催
　　アクションプラン（４つの柱）を提示
第３回：平成31年　4月19日　開催
　　アクションプランを加速化する３つの指針を提示
第４回：令和2年　　4月17日　開催（電話開催）
　　産業界へのメッセージを発信　※次ページ参照

構成員　※2020年4月開催時点

- **泉澤　清次**　三菱重工業株式会社取締役社長
- **遠藤　信博**　日本経済団体連合会サイバーセキュリティ委員長、日本電気株式会社取締役会長等
- **大林　剛郎**　日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、株式会社大林組代表取締役会長
- **櫻田　謙悟**　経済同友会代表幹事、ＳＯＭＰＯホールディングスグループＣＥＯ取締役　代表執行役社長
- **篠原　弘道**　日本電信電話株式会社取締役会長
- **中西　宏明**　株式会社日立製作所取締役会長
- **船橋　洋一**　アジア・パシフィック・イニシアティブ理事長
- **村井　純(座長)**慶應義塾大学教授
- **渡辺　佳英**　日本商工会議所特別顧問、大崎電気工業株式会社取締役会長

オブザーバー

NISC、警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省

WG１（制度･技術･標準化）

第１回　平成30年2月7日
第２回　平成30年3月29日
第３回　平成30年8月3日
第４回　平成30年12月25日
第５回　平成31年4月4日
第６回　令和２年3月（書面開催）

１．サプライチェーン強化パッケージ

WG２（経営･人材･国際）

第１回　平成30年3月16日
第２回　平成30年5月22日
第３回　平成30年11月9日
第４回　平成31年3月29日
第５回　令和　2年1月15日

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

WG３（サイバーセキュリティビジネス化）

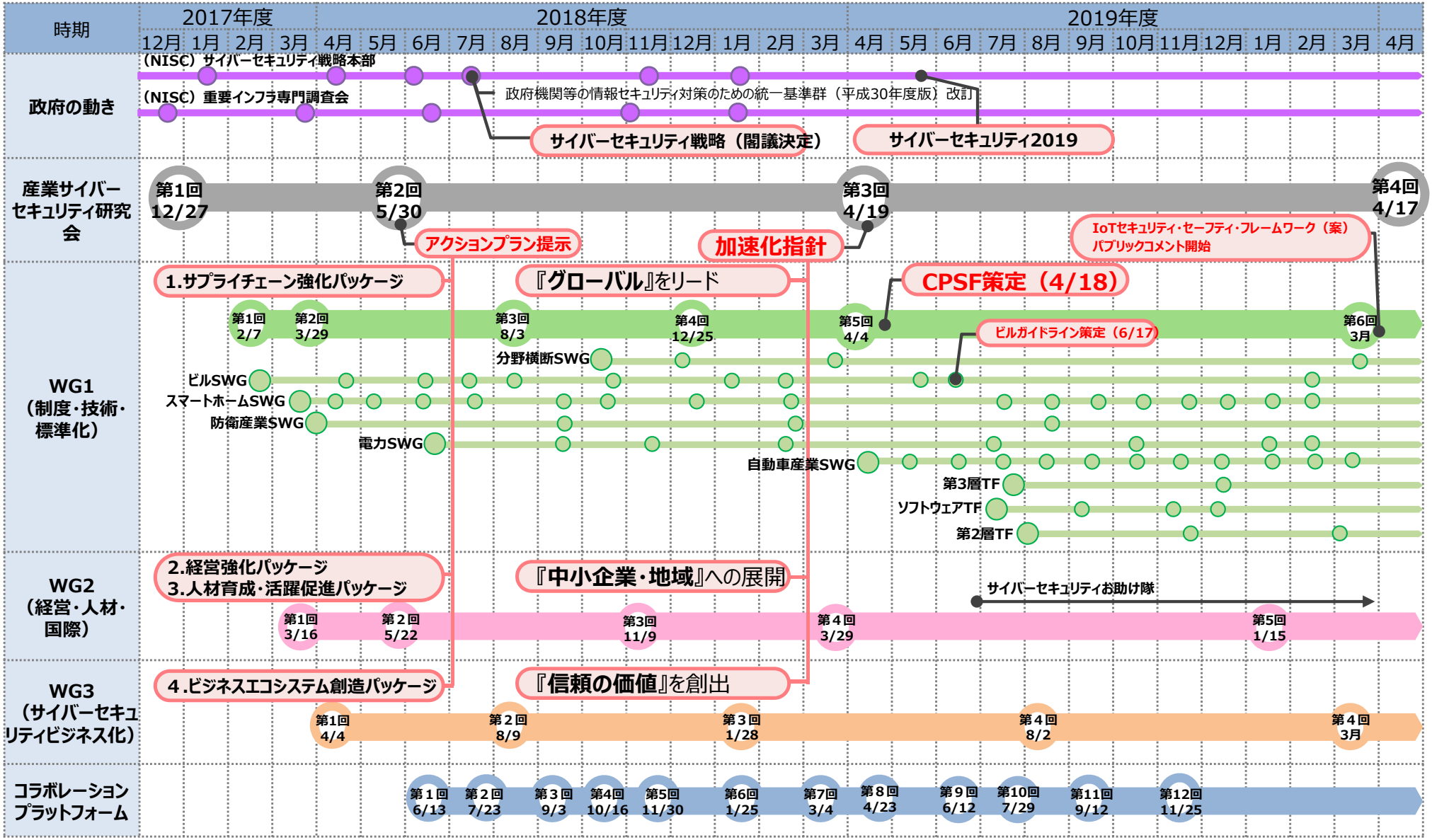
第１回　平成30年4月4日
第２回　平成30年8月9日
第３回　平成31年1月28日
第４回　令和元年8月2日
第５回　令和2年3月(書面開催)

４．ビジネスエコシステム創造パッケージ

産業サイバーセキュリティの加速化指針

１．『グローバル』をリードする
２．『信頼の価値』を創出する~Proven in Japan~
３．『中小企業・地域』まで展開する

産業サイバーセキュリティ研究会関連会議の活動状況



１．サイバー攻撃の動向

２．欧米の標準化動向

３．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

４．WG1：「Society5.0」において必要なセキュリティ対策
～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策定

５．WG2：サイバーセキュリティ対策の基盤整備
～経営、人材育成、中小企業

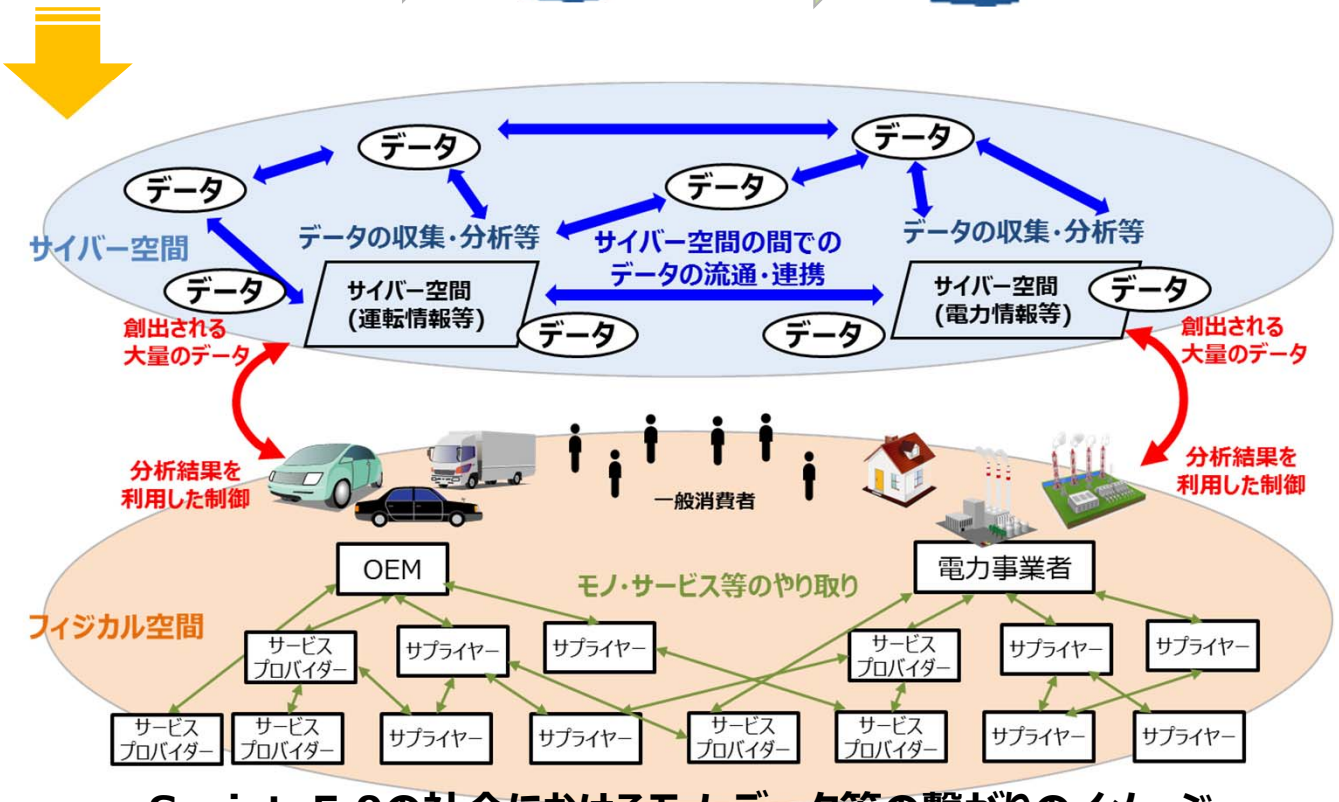
６．WG3：サイバーセキュリティビジネスの創出
～エコシステムの構築

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策定
＜サプライチェーン構造の変化＞

- 「Society5.0」では、データの流通・活用を含む、**より柔軟で動的なサプライチェーン**を構成することが可能となる。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要**となる。

「Society5.0」以前

個々の企業主体の定型的なつながりで価値を生み出す



Society5.0の社会におけるモノ・データ等の繋がりのイメージ

サイバー空間で大量のデータの流通・連携
⇒データの性質に応じた管理の重要性が増大

フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

＜三層構造と６つの構成要素＞
サイバー・フィジカル一体型社会のセキュリティのためにCPSFで提示した新たなモデル

- CPSFでは、産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するための新たなモデル（**三層構造**と**６つの構成要素**）を提示。

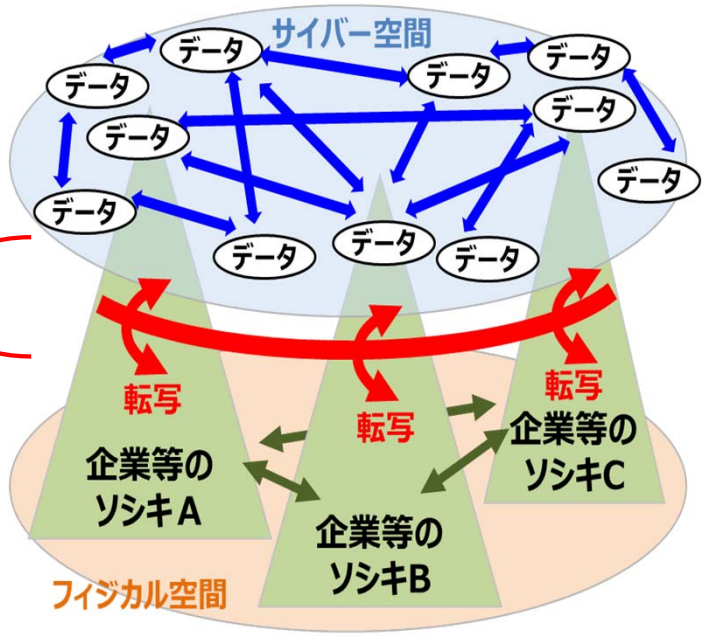
三層構造

「Society5.0」における**産業社会を３つの層に整理**し、セキュリティ確保のための信頼性の基点を明確化

サイバー空間におけるつながり
【第３層】
自由に流通し、加工・創造されるサービスを創造するための**データの信頼性**を確保

フィジカル空間とサイバー空間のつながり
【第２層】
フィジカル・サイバー間を正確に**“転写”する機能の信頼性**を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

企業間のつながり
【第１層】
適切な**マネジメントを基盤に各主体の信頼性**を確保



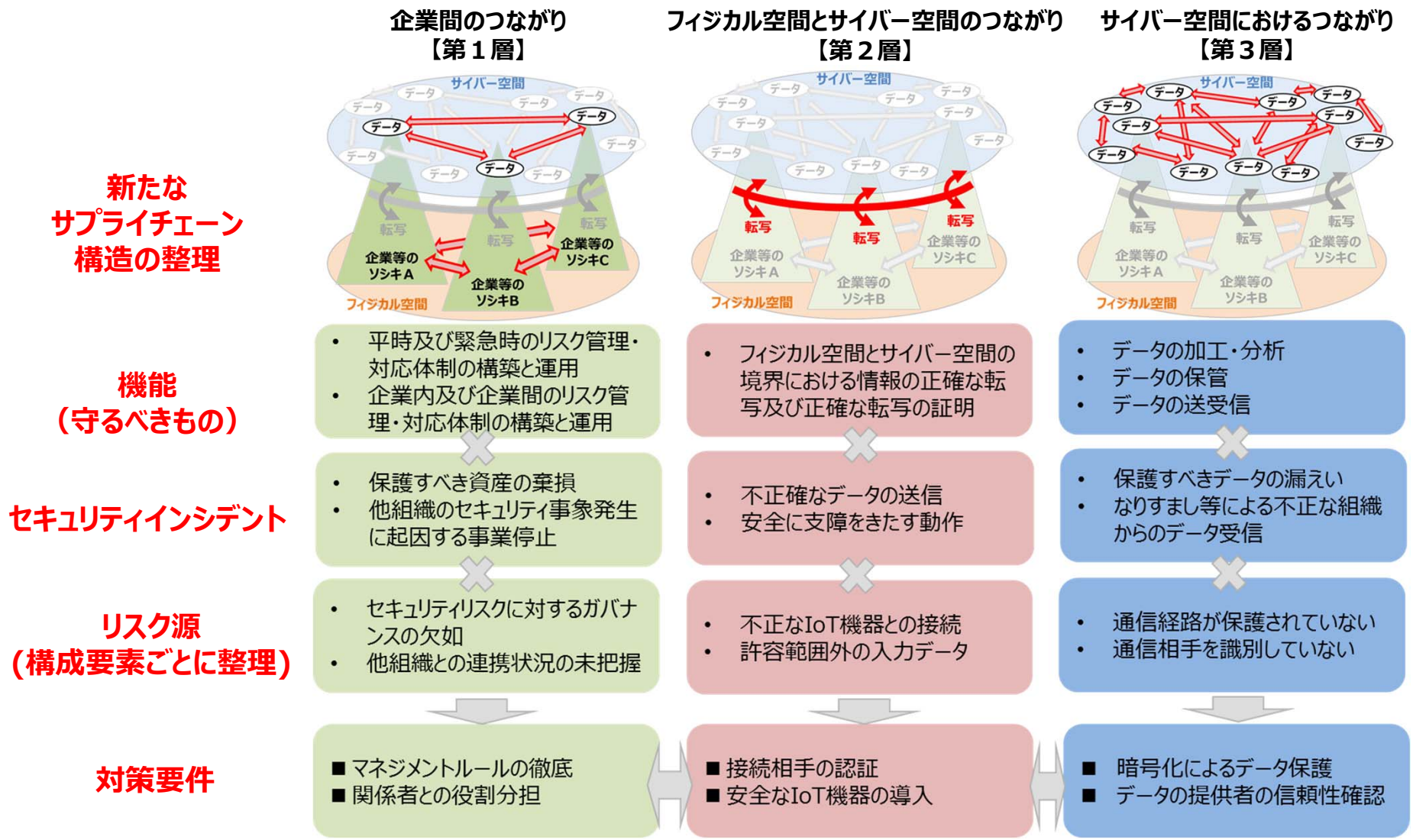
６つの構成要素

対策を講じるための単位として、**サプライチェーンを構成する要素を６つに整理**

構成要素	定義
ソシキ	• バリュークリエイションプロセスに参加する企業・団体・組織
ヒト	• ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	• ハードウェア、ソフトウェア及びそれらの部品 操作する機器を含む
データ	• フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	• 定義された目的を達成するための一連の活動の手続き
システム	• 目的を実現するためにモノで構成される仕組み・インフラ

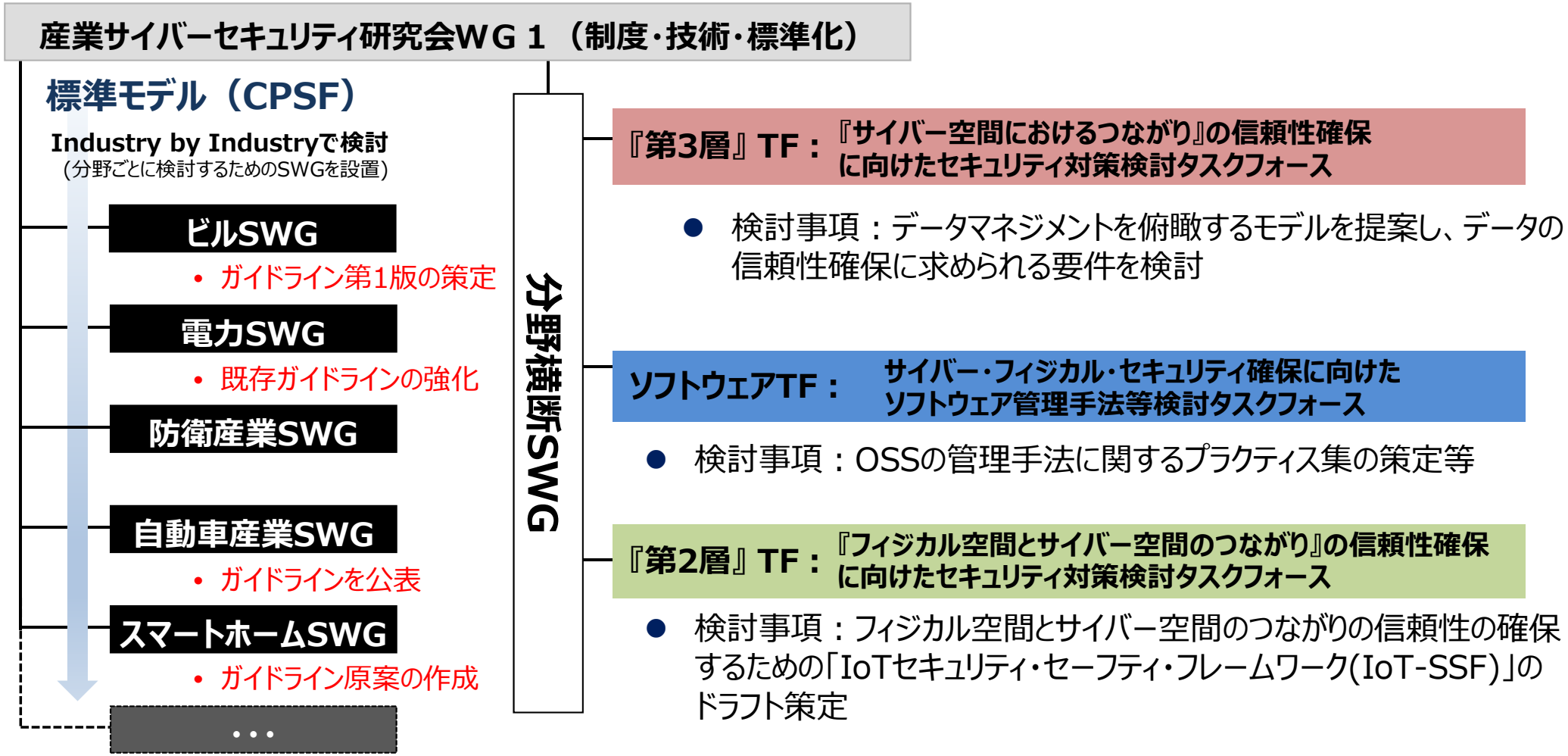
＜CPSFの全体概要＞
三層構造モデルに基づきリスク源、対応方針等を提示

- サプライチェーンの信頼性を確保する観点から、産業社会を３つの層から捉え、それぞれにおいて**守るべきもの、直面するリスク源、対応方針**等を整理。



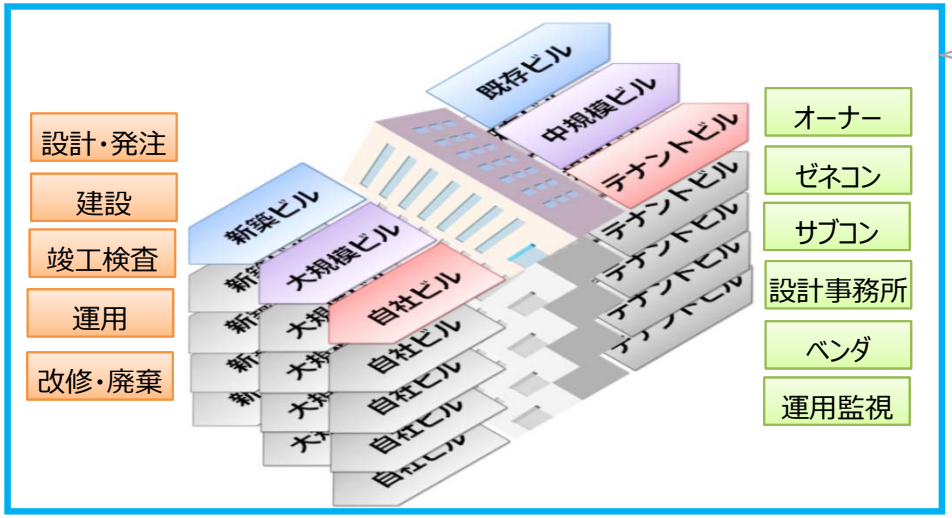
分野別SWGにおけるサイバー・フィジカルセキュリティ対策フレームワーク（CPSF）の具体化 と テーマ別TFにおける検討

- **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**



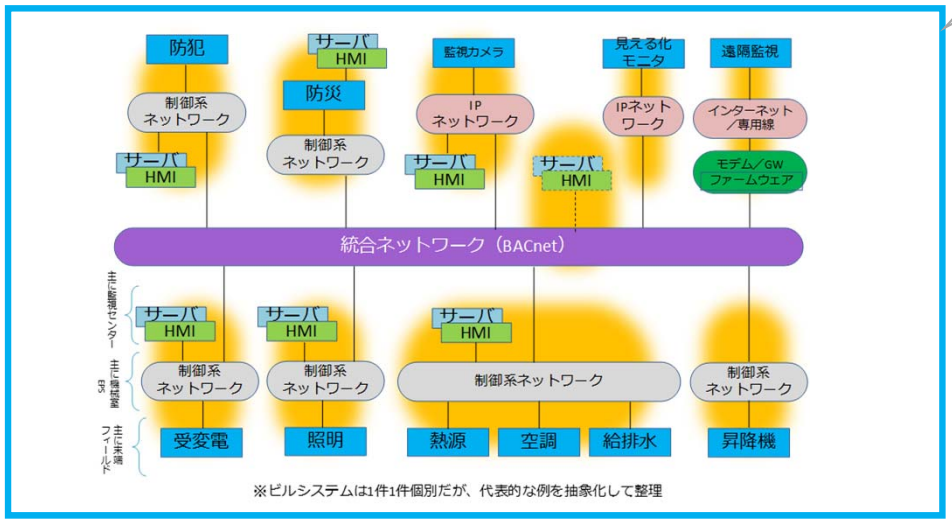
ビルSWG（座長：江崎 浩 東京大学 教授）

- 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。

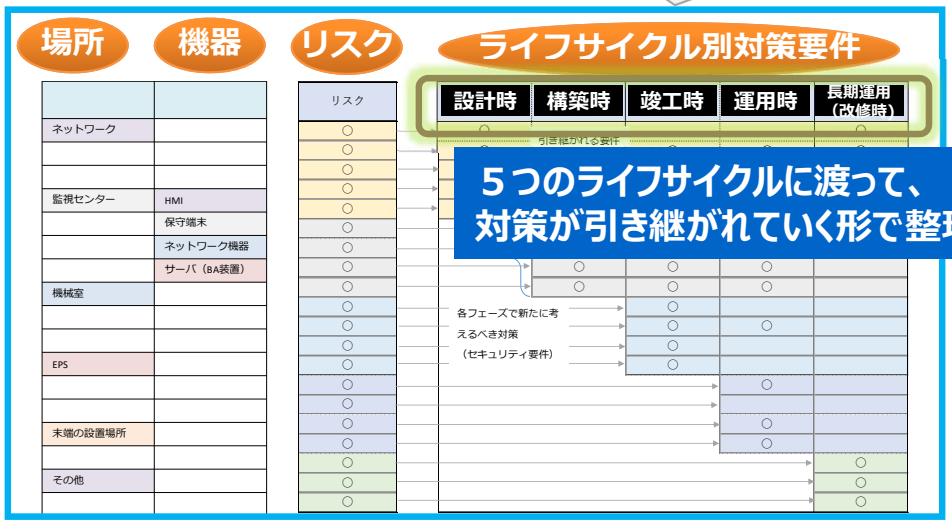


ビルシステムは、様々な種類のビルに、多種多数のステークホルダが関与し、多種の設備システムが稼働し、複数ステージからなる長期間のライフサイクルを持つ、という特徴を持つ。

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。



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

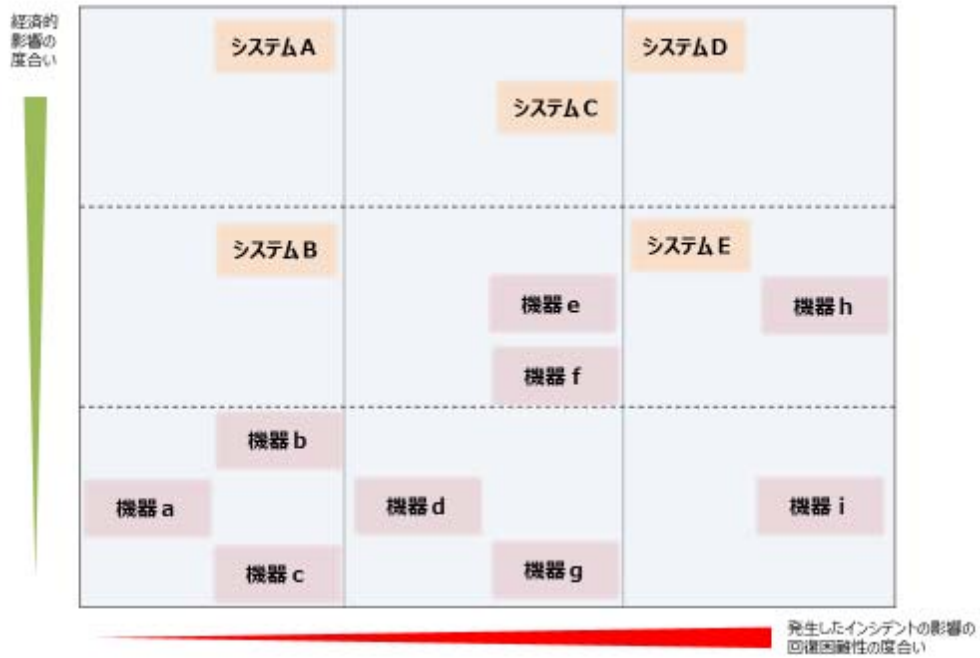
- トライアルを行い自動車産業としての共通のセキュリティーガイドラインとして、本格運用を目指す。
- **今後、工場やコネクティッド等へ対象を拡大**する方針。

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

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

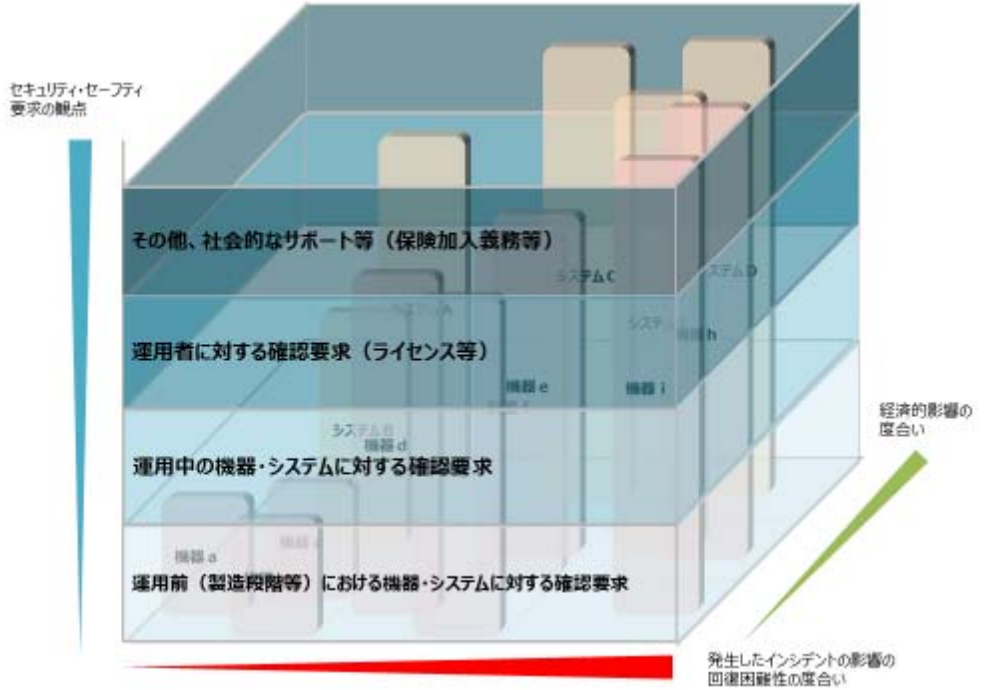
- IoT機器・システムの性質や利用環境によって課題が一様ではないことに着目し、IoT機器・システムをリスクに応じてカテゴライズした上で、それぞれに対するセキュリティ・セーフティ要求を検討することが重要。
- IoT機器・システムのカテゴライズやセキュリティ・セーフティ要求の検討に資するフレームワーク「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」の案を策定。世界中から幅広く意見を収集するため、日本語版・英語版のパブコメを実施（2020年3月31日～6月24日）。

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



１．サイバー攻撃の動向

２．欧米の標準化動向

３．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

４．WG1：「Society5.0」において必要なセキュリティ対策
～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策定

５．WG2：サイバーセキュリティ対策の基盤整備
～経営、人材育成、中小企業

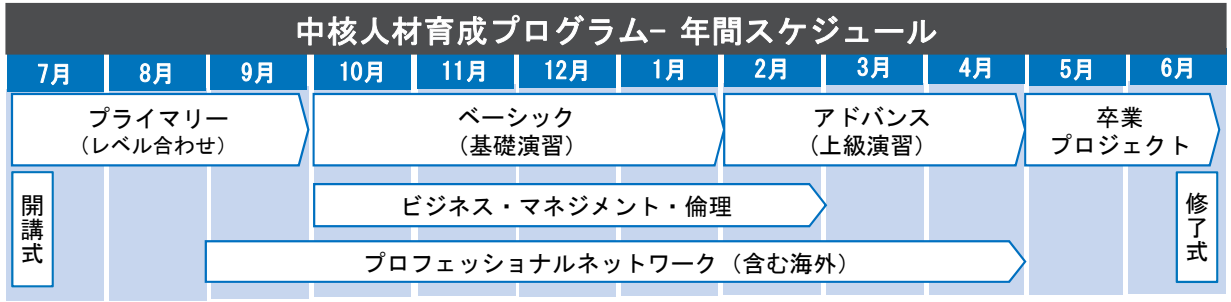
６．WG3：サイバーセキュリティビジネスの創出
～エコシステムの構築

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。

ロ　１年を通じた集中トレーニング

ロ　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

ロ　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

ICSCoEの施設（千石、秋葉原）

- 座学や基礎演習を行う千石と、各業界を想定した実機を使った模擬プラントを実際に攻撃して脆弱性を洗い出すなどの実践的なプログラムを行う秋葉原で活動を展開。

千石ー研修・演習施設

＜座学＞

＜基礎演習＞

秋葉原ー模擬プラント

＜実践的プログラム＞

攻撃

模擬プラントを攻撃

①発電模擬プラント

②機械製造模擬プラント

③鉄鋼圧延模擬プラント
④鉄道運行管理模擬プラント
⑤スマートグリッド模擬プラント
⑥施設管理模擬プラント

模擬プラント全景

対策を検討

脆弱性を発見

受講生

模擬プラント

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（セキュリティスキルレベル）	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。	• **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。**
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。
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。**


ゲーム形式教材のイメージ


開催の様子@石川高専


AppGoat講習の様子

１．サイバー攻撃の動向

２．欧米の標準化動向

３．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

４．WG1：「Society5.0」において必要なセキュリティ対策
～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策定

５．WG2：サイバーセキュリティ対策の基盤整備
～経営、人材育成、中小企業

６．WG3：サイバーセキュリティビジネスの創出
～エコシステムの構築

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

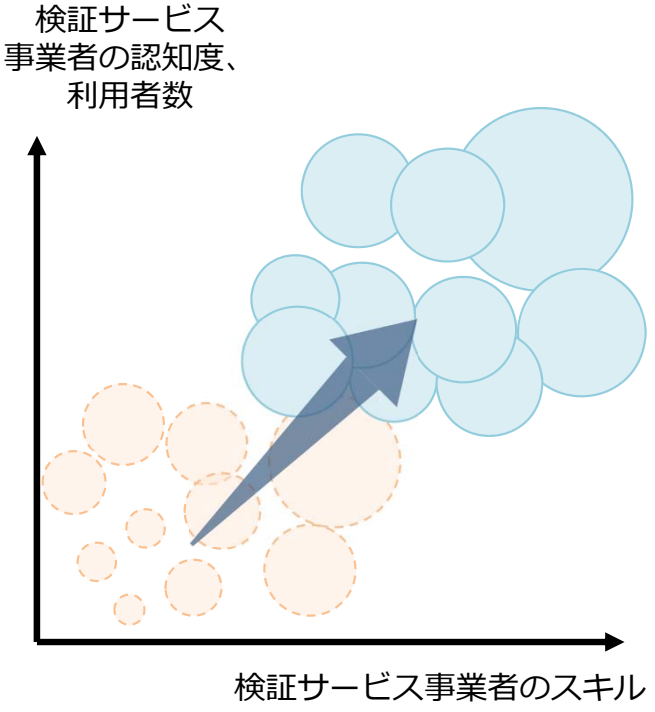
- 2019年度は、IoT機器等についてホワイトハッカー等を有する実力のある検証事業者による攻撃的手法を含むハイレベルな検証を通じて、信頼できる事業者を確認する仕組みや、事業者と利用者間のコミュニケーション、機器ごとの効果的な検証手法等の考え方を第一弾の**手引きとして整理**。
- 2020年度は、昨年度実施した機器とは異なる機器を対象として事業を実施するとともに、将来的に検証事業に活用でき得る技術に関する調査等を通じて、手引きの充実を図る。

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



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