経済産業省

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．はじめに
～サイバー攻撃の脅威レベルの向上

２．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

３．サイバーセキュリティ支援施策
～地域、経営、人材

(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：(独)情報処理推進機構(IPA)、2020.1.29.>

新型コロナウイルスに乗じたサイバー攻撃の増加

- 海外において、新型コロナウイルス対策を行っている医療関連機関に対するサイバー攻撃が確認されており、混乱に乗じたフィッシングメールや偽アプリ、フェイクニュースなども増加。

WHOへのサイバー攻撃が倍増

- WHOへのサイバー攻撃が倍増。攻撃の一つは、**DarkHotelと呼ばれるAPT攻撃**。

スペインの病院で初のサイバー被害

- 3月上旬、スペインの病院が**ランサムウェア「NetWalker」**の攻撃を受けITインフラの一部が使用不能に。スペイン病院初のサイバー被害事例。

英ワクチン試験施設に攻撃

- 3月14日、COVID-19向けワクチンの試験施設が**ランサムウェア「Maze」**の攻撃を受け、個人情報窃取・同公開の被害。

フランスの医療機関に対するDDoS攻撃

- 3月22日、パリ周辺の大学病院等を統括するパリ公立病院連合（AP-HP)に**DDoS攻撃**。
- 攻撃は1時間続き、この間、外部との接続が遮断。

チェコの大学病院にサイバー攻撃

- 3月12-13日、チェコ内でコロナ対応を担っていたBrno大学の病院がサイバー攻撃を受け、全コンピュータ停止。
- 急患を受け入れられなくなり、近隣病院に患者が送られた。

米イリノイ州郡公衆衛生局HPがダウン

- 3月10日、イリノイ州Champaign-Urbana地区の公衆衛生局のHPが**ランサムウェア攻撃**を受けダウン。

米保健福祉省（HHS）にDDoS攻撃

- 3月15日、米保健福祉省に**DDoS攻撃**。
- 同省当局者は外国勢力が関与したとの見方を示している。

感染状況をトラッキングする**偽アプリ**

- ダウンロードするとスマートフォンがロックされ、「**ロック解除したければビットコインで100ドル払え**」とのメッセージが表示。

米JH大学を装った**悪性ウェブサイト**

- 新型コロナウイルスの感染状況をリアルタイムで確認できるジョンズ・ホプキンス大学HPを装った悪性ウェブサイトが多数出現。HPを閲覧しようとリンクをクリックするとマルウェアに感染し、個人情報が窃取される。

TV会議の招待を装う偽メッセージ

- 招待メールに見せかけたメール中のボタンを押すと、攻撃者Webサイトに誘導
- 「会議はすでに始まっています」「あなたの参加を待機しています」など、焦らせるような文章が記載。

米NSCが**フェイクメッセージ**を否定

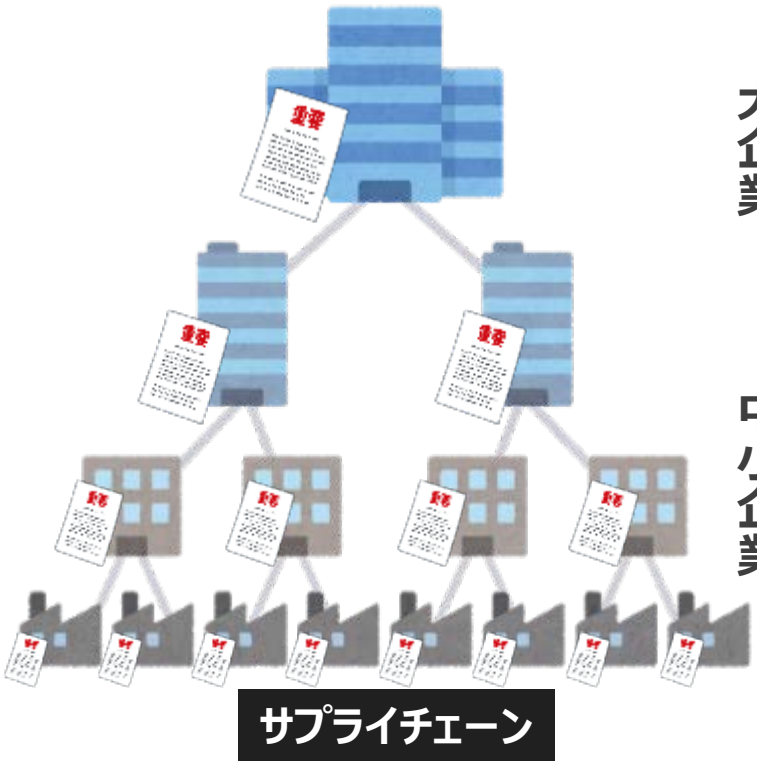
- 米軍所属の友人からの情報として「数日中にトランプ大統領が2週間の国家封鎖を実施する」とのテキストメッセージが急拡散。米NSCがツイッターでフェイクであると否定。

＜各種報道等に基づいて事務局作成＞

昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性についての報告書

2020年6月12日公開資料

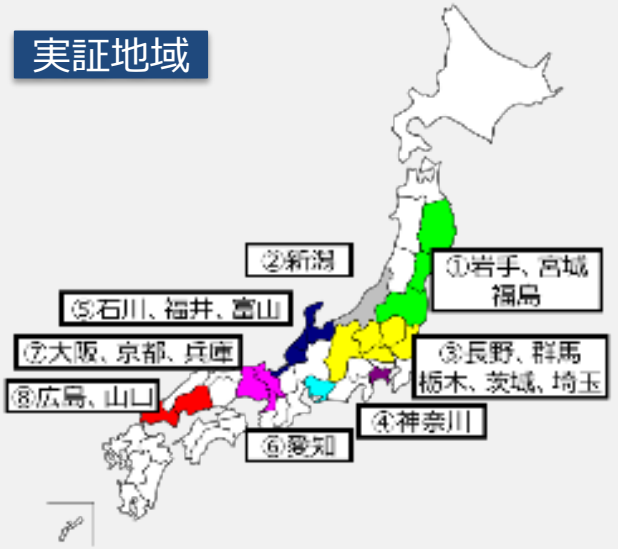
- **大企業から中小企業まで、サプライチェーンの弱点を狙ったサイバー攻撃が顕在化・高度化。**
  - 2020年1月以降、国内の複数の防衛関連の大企業が高度なサイバー攻撃の被害に遭っていたことが明らかに。
  - 「中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）」を通じて、中小企業に対するサイバー攻撃の実態も明らかに。
- 本報告では、サイバー攻撃の特徴や具体的事例を整理。



- 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。

実証地域



＜出典：経済産業省、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
公開資料を一部修正

- 2010年1月、経済産業省から企業に対して、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事案について報告いただくように、「報告の依頼」を発出。
- 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

- **間接攻撃から直接攻撃へ**
  - （従来）マルウェア添付メールの開封動作を通じた間接的感染。
  - （最近）**ネットワーク機器の脆弱性や設定ミスを利用したて直接的侵入。**
- **痕跡の秘匿・消去**
  - ウィルス対策ソフトに検知されないようなファイルを介さない攻撃。
  - 外部不正通信サーバとの通信の暗号化、痕跡の消去。

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。
- 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**。
- 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強化**が必要

＜出典：経済産業省、https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html＞

（参考）2020年4月14日：JPCERT/CCが注意喚起

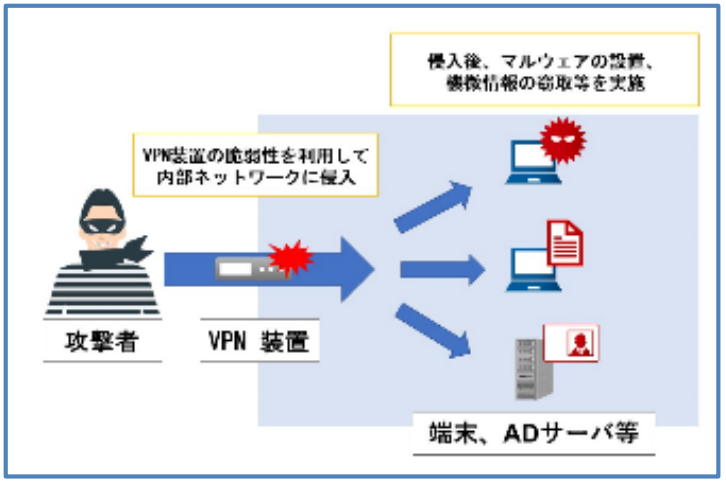
2020年4月17日公開
第4回産業サイバーセキュリティ研究会
資料を一部修正

- 2020年4月14日、JPCERT/CCは、ゴールデンウィークの長期休暇期間におけるコンピュータセキュリティインシデント発生の予防および緊急時の対応に関して、要点を公表。
- 新型コロナウイルス感染症(COVID-19)の拡大に伴うテレワークの増加により、テレワーク環境の脆弱性等を起因とした攻撃への注意が必要。

■テレワーク環境の脆弱性等を起因とした攻撃

- JPCERT/CC では、VPN 装置（主にテレワークなどに使用されるネットワーク機器）である Citrix Application Delivery Controller および Citrix Gateway の脆弱性 (CVE-2019-19781) などについて、日本国内で脆弱性を悪用したと思われる攻撃が行われていることを確認。**遠隔の第三者が任意のコードを実行する可能性**。

・複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起
https://www.jpcert.or.jp/at/2020/at200003.html
・Pulse Connect Secure の脆弱性を狙った攻撃事案
https://blogs.jpcert.or.jp/ja/2020/03/pulse-connect-secure.html



対策

■システム管理者・経営者における対策や対応

1. VPN 装置やファイアウォールを含めた自組織システムについて、アップデートの必要有無を確認する
2. 社内システムへのアクセス制御や認証方法を確認する
3. 利用サービスの攻撃事例やアップデート状況を確認し、利用継続を検討する

■個人・従業員における対策や対応

1. OSやウイルス対策ソフトを最新の状態に保つ
2. テレワーク用クライアントアプリ（テレビ会議、VPNアプリ）は正規のものをダウンロードする

出典：https://www.jpcert.or.jp/newsflash/2020041401.html
CyberNewsFlash：https://www.jpcert.or.jp/newsflash/

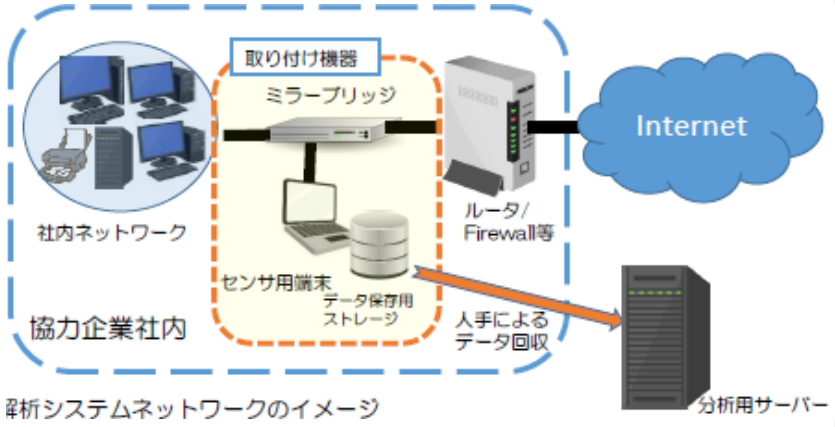
中小企業に対するサイバー攻撃の調査・分析結果（大阪商工会議所）

- 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。

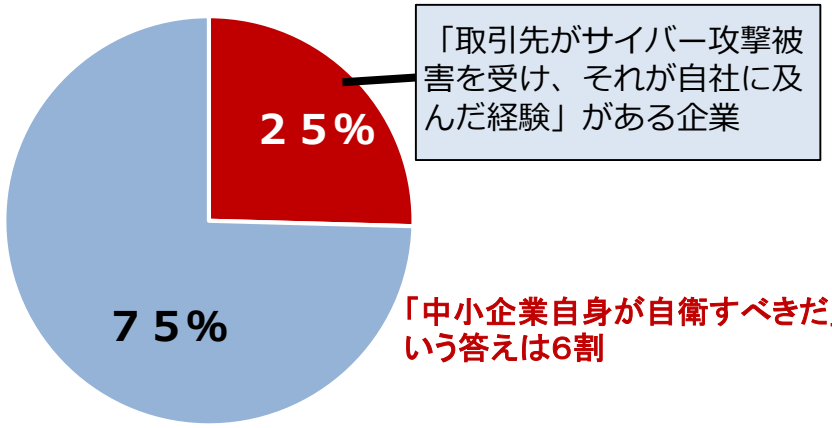
取引先経由の被害に関する調査

■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）>

令和元年度の取組：お助け隊 実証事業の結果

2020年6月30日
産業CS研究会 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**5,000万円**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としか接続できないプリンタを使用するために、**マルウェア対策ソフト未導入のWindows XP端末を使用**し感染。

・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**される。

・私物iPhoneにインストールされたアプリが、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**。

・感染により連絡先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

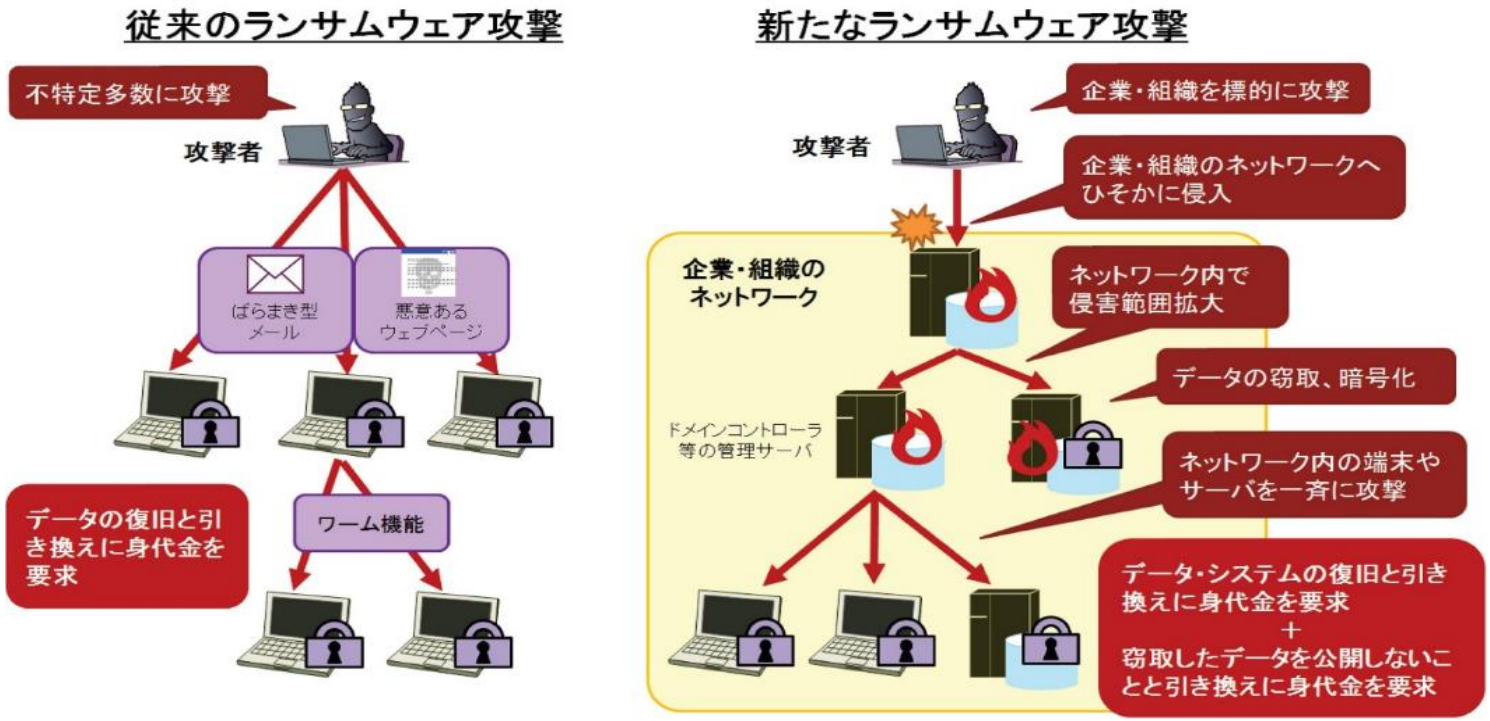
・**取引先のメールサーバーがハックされてメールアドレスが漏えい**し、それらのアドレスからマルウェア添付メールが送付されていた。

・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

ランサムウェア（Ransomware）とその手口の変化

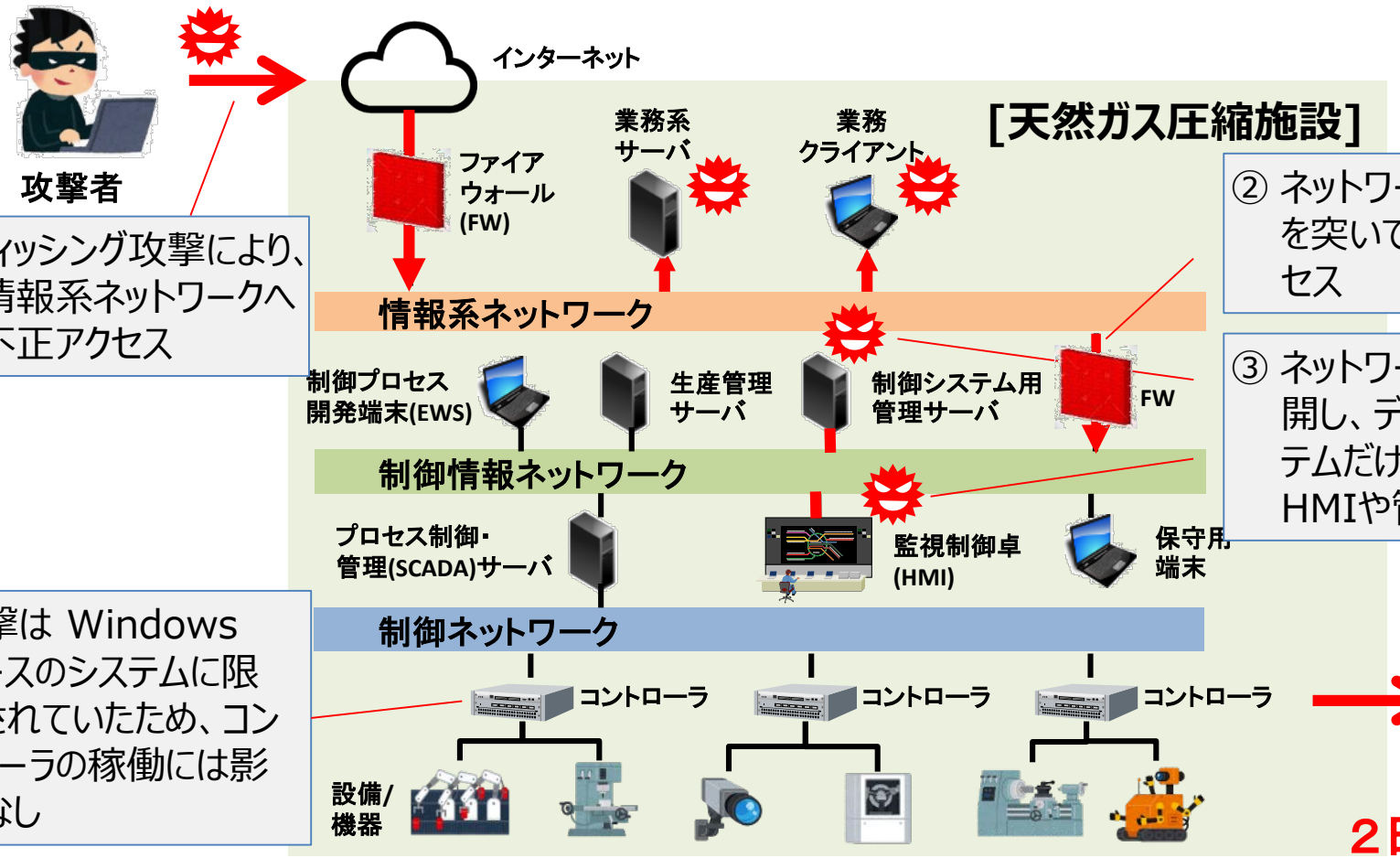
- **ランサムウェアとは**
  - 「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。
  - 感染したパソコンに特定の制限（データの暗号化など）をかけ、その制限の解除と引き換えに**金銭を要求**する挙動から、このような不正プログラムをランサムウェアと呼ぶ。
- **新たな（標的型）ランサムウェア攻撃とは**
  - 身代金として金銭を得ることを目的に、企業・組織内のネットワークへ侵入し、パソコン等の端末やサーバ上のデータを一斉に暗号化して使用できなくしたり、データを窃取して**公開すると脅迫**したりするサイバー攻撃。
  - 「ランサムウェア」と呼ばれるウイルスを用いた従来の攻撃に「人手によるランサムウェア攻撃」と「二重の脅迫」の新たな手口が加わったもの。



出典：(独)情報処理推進機構(IPA)

ランサムウェアによる制御システムへの被害

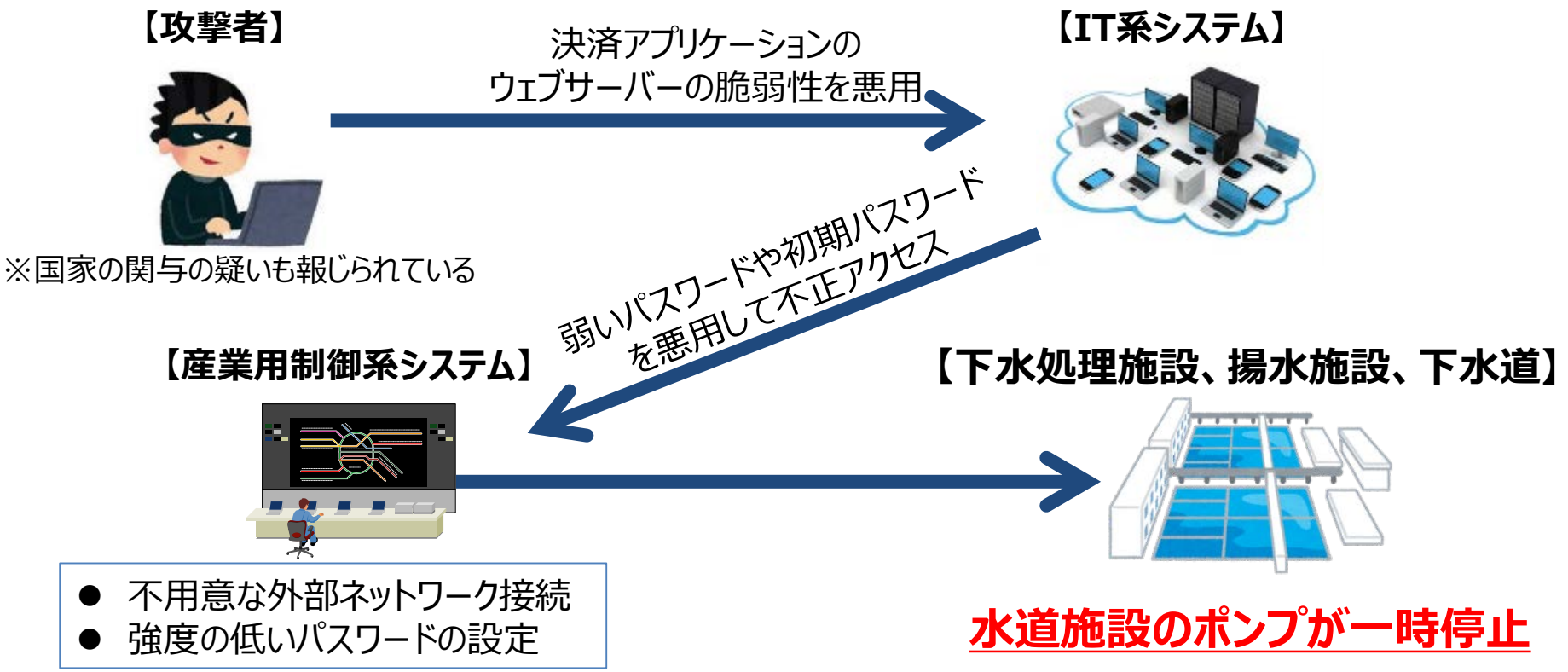
- 米国サイバーセキュリティ・インフラセキュリティ局(CISA)は、今年2月に同国の**天然ガス圧縮施設がランサムウェアを使った攻撃を受け、2日間の操業停止に追い込まれた**と報告している。



（出典）CISA "Alert (AA20-049A) Ransomware Impacting Pipeline Operations"

（参考）イスラエル水道システムへの組織的サイバー攻撃

- 2020年4月、イスラエル政府は、**廃水処理場、ポンプ場、下水施設の監視制御・データ収集(SCADA)システムを狙った組織的な攻撃**があったとの報告を受けたと発表。
- 同国政府から、事前に制御システムや塩素制御装置のパスワードを変更するよう指示が出ていたが、**適切な対策が取られていなかった水道施設のポンプが一時停止**。攻撃の最終目的は、同国の家庭用水道水に入る塩素量の増加だった、との見方が一部メディアで紹介されている。



（出典）各種公開情報に基づき経済産業省作成

１．はじめに
～サイバー攻撃の脅威レベルの向上

２．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

３．サイバーセキュリティ支援施策
～地域、経営、人材

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
第５回：令和2年　　6月30日　開催
　サイバーセキュリティ強化運動の展開

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
第６回　令和　2年8月25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）

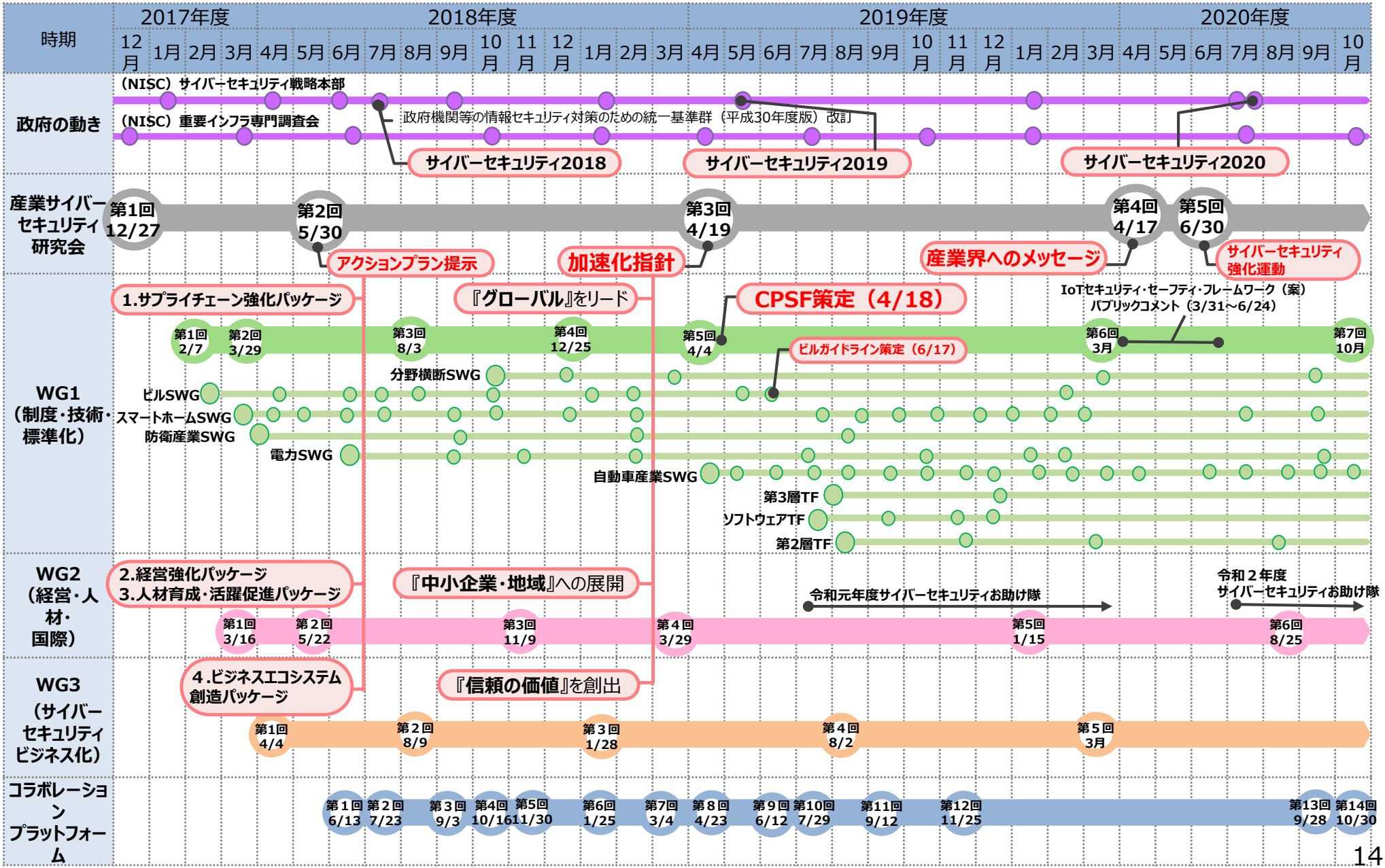
第１回　平成30年4月4日
第２回　平成30年8月9日
第３回　平成31年1月28日
第４回　令和元年8月2日
第５回　令和2年3月(書面開催)

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



産業サイバーセキュリティ研究会からの「産業界へのメッセージ」（4月17日）

- 令和２年４月17日に、**産業サイバーセキュリティ研究会（電話会議）**を開催。
- 最近の**サイバー攻撃の高度化・攻撃起点の多様化**に加え、**新型コロナウィルスによる混乱等に乗じたサイバー攻撃**が欧米を中心に増加していることから、各企業に対し、**直近の状況及び今後のデジタル化の急加速に対応するためのサイバーセキュリティの取組を促すメッセージ**を発出。

＜「産業界へのメッセージ」のポイント＞

① 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フィッシングメール/SMS等に注意**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。 等

② 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。
- **パッチ当て等の基本的対策**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。等

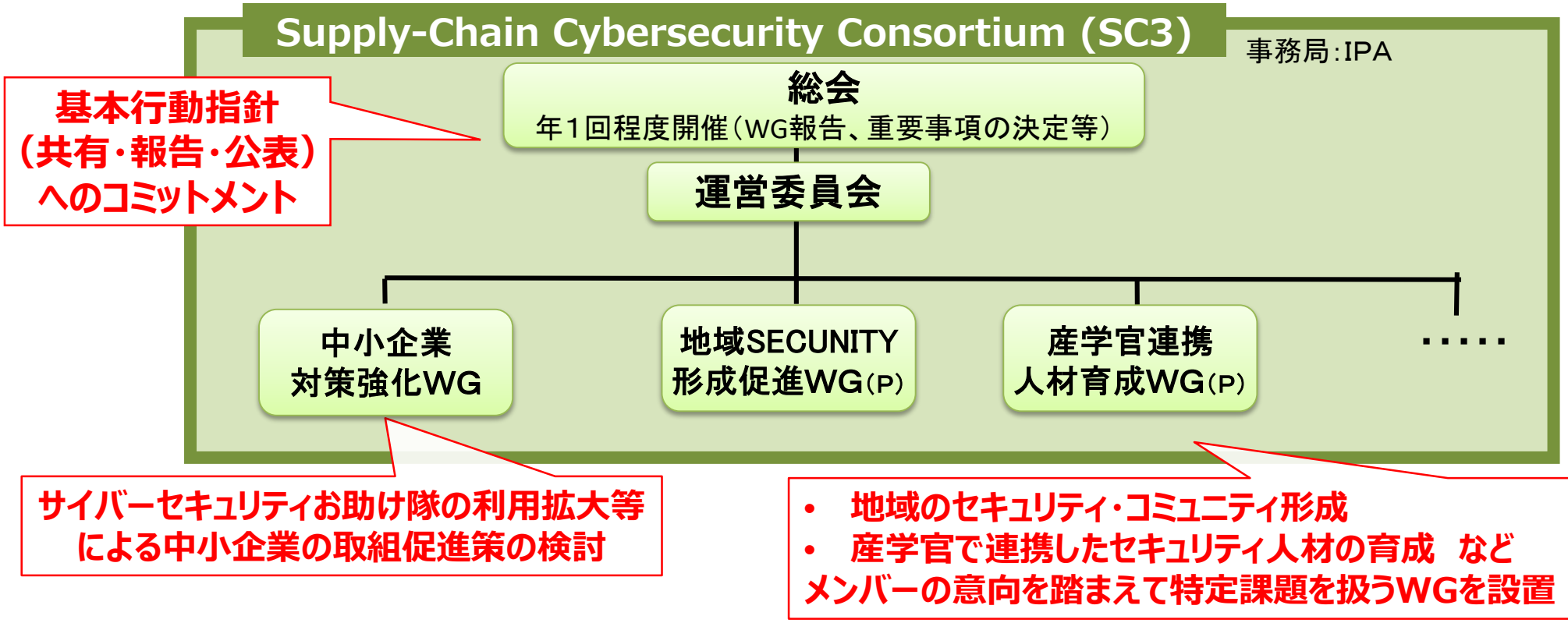
2　事後対策の強化確認

- 適切な**初動対応を行う体制と計画を整備**すること。
- 平時の**“防災訓練”を徹底**して行うこと。

（産業界へのメッセージ）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20200417.pdf

サイバーセキュリティ強化運動の全体像（コンソーシアムのイメージ）

- **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（経団連、日本商工会議所、経済同友会）、業種別業界団体　等
- **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。



１．はじめに
～サイバー攻撃の脅威レベルの向上

２．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

３．サイバーセキュリティ支援施策
～地域、経営、人材

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

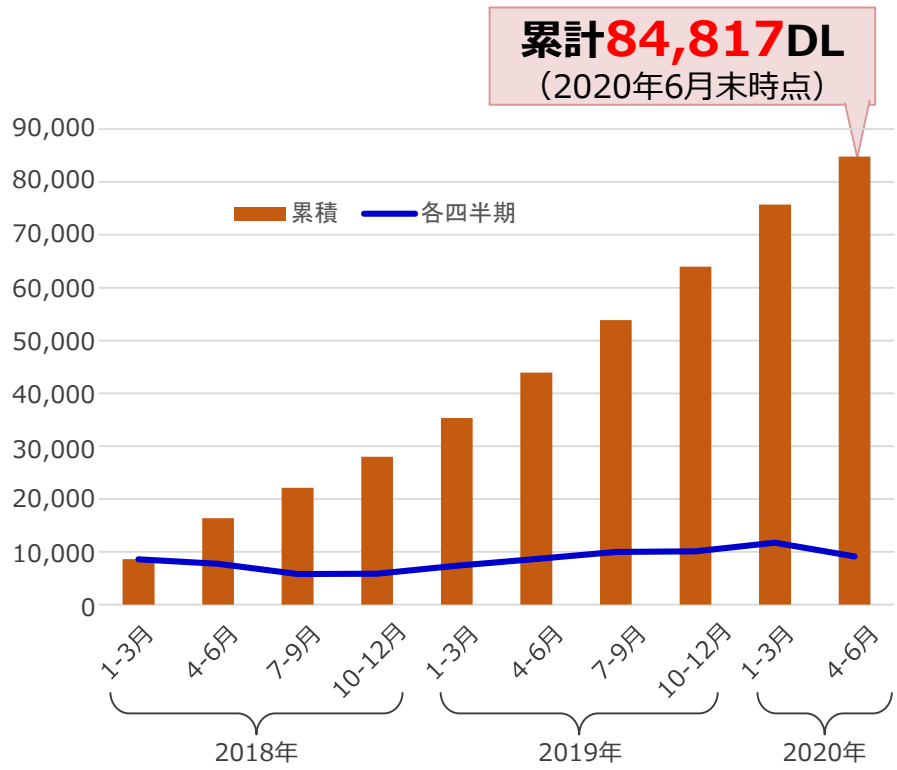
１．経営者が認識すべき３原則

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

２．経営者がCISO等に指示すべき１０の重要事項

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

サイバーセキュリティ経営ガイドラインV2.0のダウンロード数推移



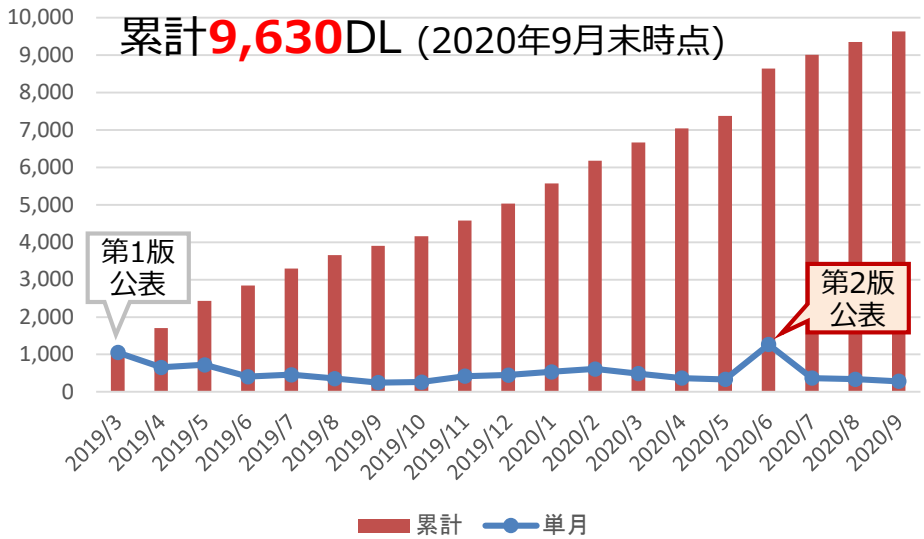
【参考】上場企業数　第一部　2,157社
　　第二部　488社

日本取引所グループ公表
2019年12月17日時点

『サイバーセキュリティ経営ガイドラインVer2.0実践のための経営プラクティス集』第2版を公表

- 2019年3月、**「サイバーセキュリティ経営ガイドラインVer2.0実践のための経営プラクティス集」を公開**。経営ガイドラインの重要10項目の実践事例に加え、セキュリティ担当者の日常業務における悩みに対する具体的対応策を提示。
- 2019年度収集したプラクティスを反映した**第2版を2020年6月3日に公表**。

<プラクティス集のダウンロード数推移>



【参考】上場企業数　第一部　2,157社
　　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）

（参考）実際の活用事例（ユーザ企業へのヒアリングより）

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

（参考）中小企業の情報セキュリティ対策ガイドライン

- これからセキュリティ対策に取り組む企業向けの対策や、ある程度対策の進んでいる企業向けの対策の提示など、企業のレベルに合わせてステップアップできるように構成。

ガイドライン本体

経営者向けの解説

サイバーセキュリティ経営ガイドラインの内容を中小企業向けに整理し、**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

実践者が具体的にセキュリティ対策を実施していくための方法を、**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

Step1 まず始める

最低限実施すべき
セキュリティ対策の5か条

Step2 現状を知り改善する

簡易的な
セキュリティ対策の25項目

Step3 本格的に取り組む


セキュリティポリシーを策定し、
組織的な対策の取り組み

Step4 改善を続ける

第三者認証(ISMS)の取得を
目指した取り組み

こちらより無料ダウンロード可能です
https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

（参考）セキュリティ対策自己宣言「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（IPA）。
- IT導入補助金の申請において、「SECURITY ACTION」の宣言を必須要件化。
- **１０万社を超える中小企業が宣言**（2020年7月時点）。

★ 一つ星

SECURITY ACTION ★
セキュリティ対策自己宣言

情報セキュリティ5か条に取り組む企業

① OS・ソフトウェアの最新化
（パッチ適用、バージョンアップ）
② ウイルス対策ソフトの導入
③ 強固なパスワード設定
④ データ等は必要最低限の人のみに共有
⑤ 攻撃の手口の把握

★★ 二つ星

SECURITY ACTION ★★
セキュリティ対策自己宣言

情報セキュリティ自社診断により自社の状況を把握し、セキュリティポリシーを策定する企業

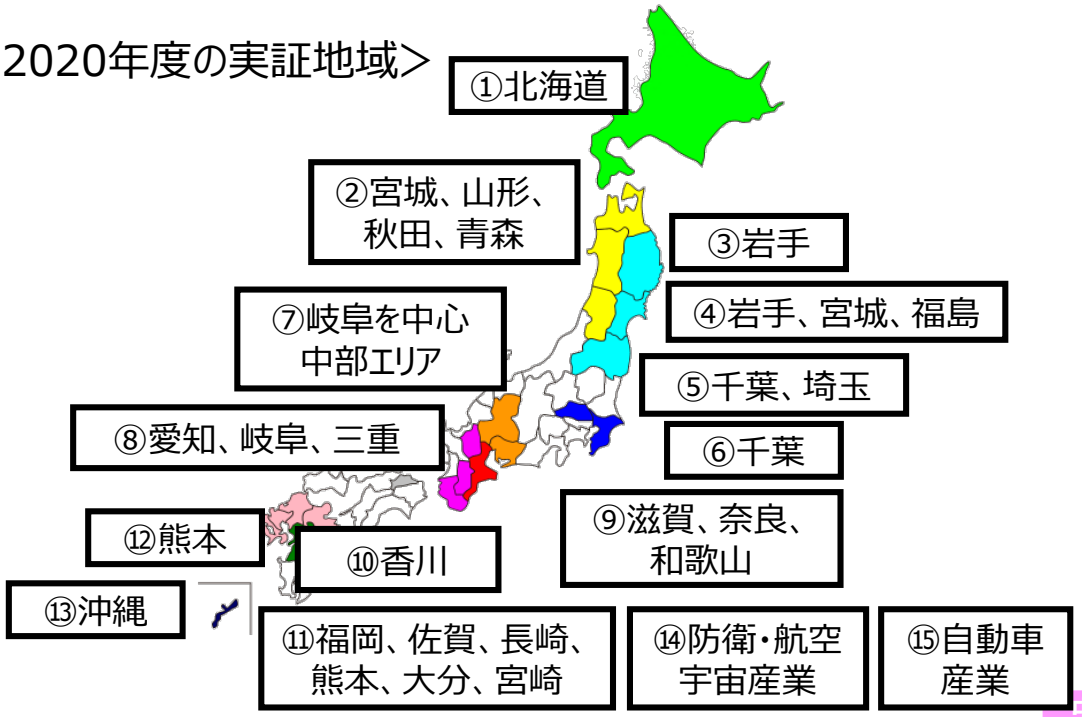
25の診断項目により
自社の対策状況を把握

セキュリティポリシー
策定のためのひな形も提供

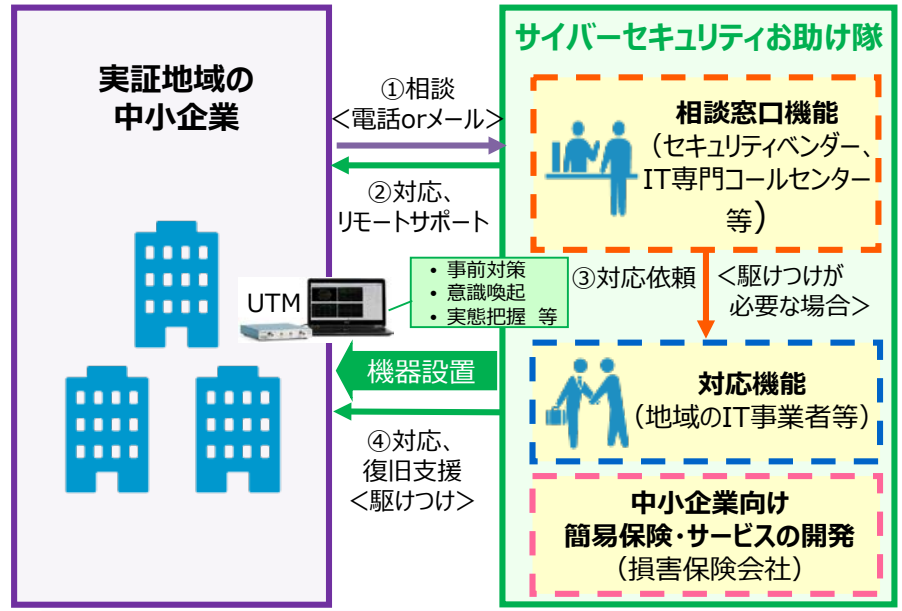
サイバーセキュリティお助け隊実証事業(2020年度)

- 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（全国で15件実施）。
- 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**。

<2020年度の実証地域>



<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

※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

（参考）サイバーセキュリティお助け隊チームリスト（2020年度）

	対象 （地域／産業分野）	実施体制 ●：実施主体）
①	北海道	●東日本電信電話株式会社 ・東京海上日動火災保険株式会社
②	宮城県、山形県、 秋田県、青森県	●東北インフォメーション・システムズ株式会社 ・ハイテックシステム株式会社 ・秋田システムマネージメント株式会社 ・あいおいニッセイ同和損害保険株式会社
③	岩手県	●富士ソフト株式会社 ・東京海上日動火災保険株式会社
④	岩手県、宮城県、 福島県	●株式会社デジタルハーツ ・損害保険ジャパン株式会社
⑤	千葉県、埼玉県	●富士ゼロックス株式会社 ・東京海上日動火災保険株式会社
⑥	千葉県	●SOMPOリスクマネジメント株式会社 ・ちばぎんコンピューターサービス株式会社 ・株式会社千葉銀行　・株式会社ラック ・損害保険ジャパン株式会社
⑦	岐阜県を中心とする 中部エリア	●MS&ADインターリスク総研株式会社 ・中部電力株式会社　・中部電力ミライズ株式会社 ・株式会社中電シーティーアイ ・三井住友海上火災保険株式会社 ・あいおいニッセイ同和損害保険株式会社
⑧	愛知県、岐阜県、 三重県	●名古屋商工会議所 ・株式会社日立システムズ ・西日本電信電話株式会社 ・東京海上日動火災保険株式会社 ・損害保険ジャパン株式会社
⑨	滋賀県、奈良県、 和歌山県	●大阪商工会議所 ・日本電気株式会社 ・東京海上日動火災保険株式会社 ・キューアンドエー株式会社

	対象 （地域／産業分野）	実施体制 ●：実施主体
⑩	香川県	●高松商工会議所 ・株式会社STNet ・西日本電信電話株式会社 ・キャノンマーケティングジャパン株式会社 ・損害保険ジャパン株式会社 ・東京海上日動火災保険株式会社
⑪	福岡県を中心とした 九州６県	●株式会社BCC ・日本電気株式会社 ・東京海上日動火災保険株式会社 ・NECフィールディング株式会社
⑫	熊本県	●西日本電信電話株式会社　熊本支店 ・株式会社くまなんピーシーネット ・東京海上日動火災保険株式会社 ・一般社団法人熊本県サイバーセキュリティ推進協議会
⑬	沖縄県	●沖電グローバルシステムズ株式会社 ・株式会社セキュアイノベーション ・ファーストライディングテクノロジー株式会社 ・那覇商工会議所 ・沖縄電力株式会社 ・損害保険ジャパン株式会社
⑭	防衛・航空宇宙 産業	●株式会社PFU ・株式会社エヴァアビエーション ・富士通株式会社 ・ウェブルート株式会社 ・損害保険ジャパン株式会社
⑮	自動車産業	●東京海上日動リスクコンサルティング株式会社 ・東京海上日動火災保険株式会社 ・エヌ・ティ・ティ・コミュニケーションズ株式会社 ・NTTコム ソリューションズ株式会社 ・NTTセキュリティ・ジャパン株式会社 ・ジェイズ・コミュニケーション株式会社

実証事業から民間サービスへの移行状況と普及促進のための支援策

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

実証事業から民間サービスへの移行状況

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

（大阪商工会議所）

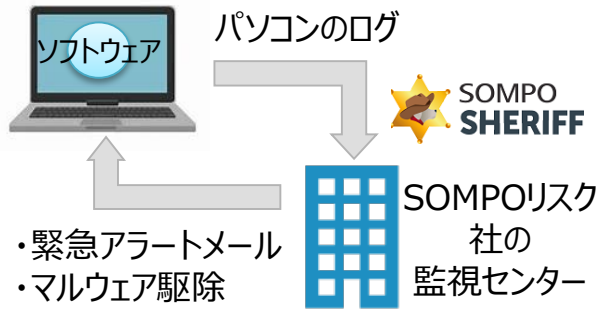
実証を通じて中小企業にとって必要な機能・サービスを精査することで、安価なサービスを実現。

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

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

（SOMPOリスクマネジメント）

<サービスのイメージ>



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

（NTT東日本）

(参考)同社の提供する「おまかせサイバーみまもり」

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

お助け隊サービスのブランド化・審査体制構築へ

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

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＞

地域にセキュリティについて相談できる相手がいない

地域にセキュリティを学ぶ機会が少ない

地域のベンダーを知らない

?

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

大学・高専
地元企業
県警
地元ベンダー
地域のセキュリティ関係者のつながり
自治体
民間団体
国

将来目指す姿

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

!!

地域のニーズとシーズのマッチング

- **地域の課題解決**
- **価値創出**

地域SECUNITYがない状態

地域SECUNITY形成

コラボレーション・プラットフォームを全国に展開

令和２年度の取組状況

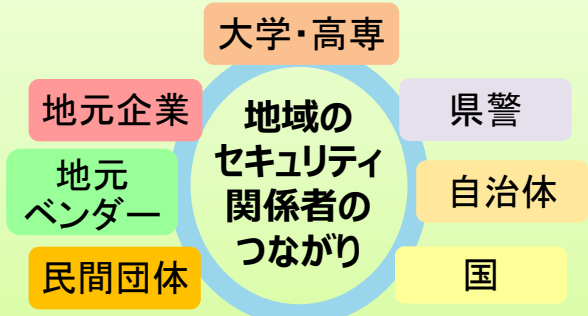
● 業界団体や専門家、各地方経産局等と連携し、各地域におけるセキュリティ関係者間での意見交換・情報共有等を実施。コミュニティ形成に向けた取組を全国で推進する。

＜各地域のコミュニティ形成の促進に向けた支援例＞

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

＜目指す姿＞

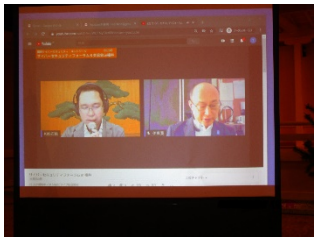
継続的に活動できるセキュリティコミュニティの形成を促進



先行事例：

＜福井県：サイバーセキュリティフォーラム　in　福井（8/3）＞

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





(※)YouTubeのユニーク視聴者数。

コミュニティ形成に必要な取組

● 全国各地で地域に根差したセキュリティコミュニティの形成を推進するために、以下の取組を開始する。

①セキュリティコミュニティを形成するための**モデル及びプラクティスの共有**

- 新たにコミュニティを形成する際にアプローチ先として想定される関係機関（自治体、商工団体、県警、大学 等）をリスト化。
- 他地域でのコミュニティの取組を参考にできるよう、各コミュニティのプラクティスを共通のフォーマットでとりまとめ、横展開。
- 課題なども共有することで、ソリューションを有するプレイヤーとの更なる連携を促進。

＜イメージ＞

②各地域に駆けつけ可能な専門家や、専門家派遣制度等の**情報・問合せ先リストの作成・共有**

- 連携できる可能性のある専門家やイベント（例．JNSA全国横断セミナー）、活用可能な制度（例．IPAセキュリティプレゼンター制度）等の情報・問合せ先リストを作成・共有。

＜イメージ＞

活用可能な制度

組織名	担当部署	連絡先
IPA セキュリティプレゼンター	××課	XX-XXXX
IPA 講師派遣制度	○○課	XX-XXXX

セキュリティ専門家

組織名	氏名	連絡先	専門等
JUAS	○○	XX-XXXX	経営層向け
JPCERT	△△	XX-XXXX	最新攻撃事例

国立高専機構と産・官との連携促進・具体化

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

（赤字＝前回WGからのアップデート）

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

国立高専卒業生 約1万人/年の内訳	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
セキュリティスキルレベル	**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。	• **高専機構がJNSAに講師派遣を依頼できる体制を構築。** • **METIがセキュリティ専門官を高度セキュリティ合宿に講師として派遣。**
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 • **JNSAがオンライン授業環境を利用した現場第一線講師による最新事例授業の開催検討中** ※一度に数十校を対象に同時開催可能。JNSAで実施中の岡山理科大学遠隔授業内容を最新事例中心に発展・展開。 • **高専機構が四国地域企業のIPA ICSCoE修了生に講師派遣を依頼できる体制を構築。** • **日立製作所が一関高専生向けに出前授業、インターンシップを実施し、出前授業は全国各校に配信。**	• **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が高専機構と連携し、業界別（例．機械、電気、建築等）ビデオ教材（20分程度）を作成。** ※CRIC：一般社団法人サイバーリスク情報センター	※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	**・JNSAが教員向けのセキュリティ基礎講座の実施を検討中。** ※神奈川県での高校教員向けセキュリティ基礎講座の実績を展開。	• **IPAが教員向けにAppGoat講習会を開催。** • **JPCERT/CCが情報担当教員向け研修に講師を派遣。** • **教員がIPAのセキュリティキャンプ全国大会を見学。** • **高専機構が、教師向け合宿の機会に、METIにセキュリティ専門官の講師派遣を依頼できる体制を構築。**


ゲーム形式教材のイメージ


開催の様子@石川高専

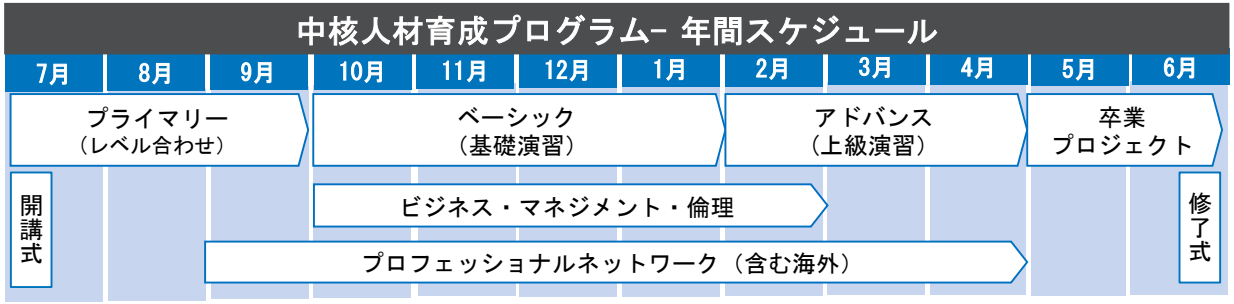

AppGoat講習の様子

産業サイバーセキュリティセンター（ICSCoE）（2017年4月設置）

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

ロ　１年を通じた集中トレーニング

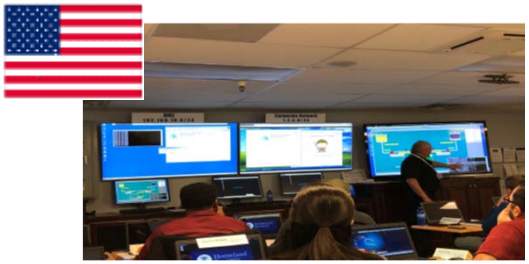
ロ　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：47人）



- 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

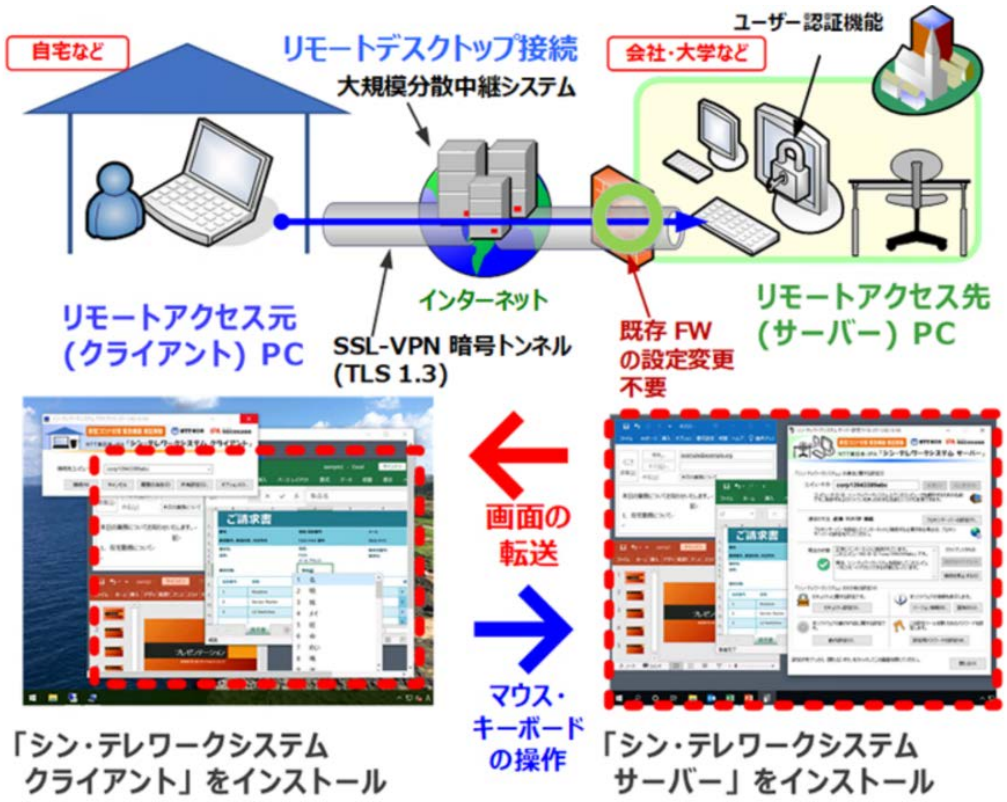
➢ 政府機関、自動車業界、スタートアップ企業の代表者等からの講義や意見交換を実施

➢ 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

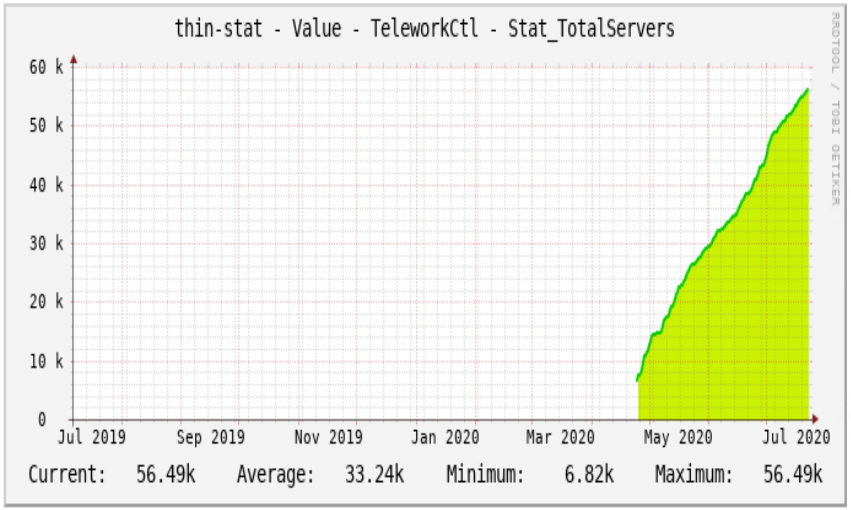
など

（参考）シン・テレワークシステム

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



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



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