

サイバーセキュリティ戦略(2018年)・サイバーセキュリティ2020(2020年7月21日サイバーセキュリティ戦略本部決定)の概要

- ◆ サイバーセキュリティ戦略(2018年7月)は、サイバーセキュリティ基本法に基づく2回目の「サイバーセキュリティに関する基本的な計画」。2020年以降の目指す姿も念頭に、我が国の基本的な立場等と今後3年間(2018年~2021年)の諸施策の目標及び実施方針を国内外に示すもの
- ◆ サイバーセキュリティ2020は、同戦略に基づく2019年度年次報告・2020年度年次計画として策定されたもの。各府省庁はこれに基づき、施策を着実に実施

＜新戦略(2018年戦略) (平成30年7月27日閣議決定)の全体構成＞

1 策定の趣旨・背景

- ・ サイバー空間がもたらす人類が経験したことのないパラダイムシフト(Society5.0)
- ・ サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会を見据えた新たな戦略の必要性

2 サイバー空間に係る認識

- ・ 人工知能(AI)、IoTなど科学的知見・技術革新やサービス利用が社会に定着し、人々に豊かさをもたらしている。
- ・ 技術・サービスを制御できなくなるおそれは常に内在。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的損失が生ずる可能性は指数関数的に拡大

3 本戦略の目的

- ・ 基本的な立場の堅持(基本法の目的、基本的な理念(自由、公正かつ安全なサイバー空間)及び基本原則)
- ・ 目指すサイバーセキュリティの基本的な在り方: 持続的な発展のためのサイバーセキュリティ(サイバーセキュリティエコシステム)の推進。3つの観点(①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働)からの取組を推進

4 目的達成のための施策

経済社会の活力の向上 及び持続的発展

～新たな価値創出を支える
サイバーセキュリティの推進～

- 新たな価値創出を支えるサイバーセキュリティの推進
- 多様なつながりから価値を生み出すサプライチェーンの実現
- 安全なIoTシステムの構築

国民が安全で安心して 暮らせる社会の実現

～「積極的サイバー防御」の推進による任務保証～

- 国民・社会を守るための取組
- 官民一体となった重要インフラの防護
- 政府機関等におけるセキュリティ強化・充実
- 大学等における安全・安心な教育・研究環境の確保
- 2020年東京大会とその後を見据えた取組
- 従来の枠を超えた情報共有・連携体制の構築
- 大規模サイバー攻撃事態等への対処態勢の強化

国際社会の平和・安定及び 我が国の安全保障への寄与

～自由、公正かつ安全なサイバー空間の堅持～

- 自由、公正かつ安全なサイバー空間の堅持
- 我が国の防御力・抑止力・状況把握力の強化
- 国際協力・連携

横断的施策

■ 人材育成・確保

■ 研究開発の推進

■ 全員参加による協働

5 推進体制

内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化を図るとともに、同センターが調整・連携の主導的役割を担う。

サイバーセキュリティ2020（1部 サイバーセキュリティを巡る動向）の概要

- 新型コロナウイルス感染症への対応をはじめ、直近のサイバーセキュリティを取り巻く環境の概観や基本的な考え方について解説
- また、2019年度に、政府機関、事業者、国民一般等において確認された国内外の主なサイバーセキュリティ事案等を整理
- さらに、諸外国の政策や、サイバー空間における国際法の適用に関する議論など、サイバー空間に係る国際的な動向を整理

【サイバーセキュリティを取り巻く環境】

○新型コロナウイルス感染症への対応

※1 令和2年3月28日（令和2年4月7日改正版）新型コロナウイルス感染症対策本部決定

・「新型コロナウイルス感染症対策の基本的対処方針」※1にて、事業者においては、テレワークなどを活用することで、さらに接触の機会を減らすことを協力して行っていく必要があるとされた。

・こういった状況注視しつつ、基本的な対策方法などについて効果的に周知活動を進めていくことが重要

＜これまでの主な政府の動き＞

NISC	総務省	経産省
一般・政府機関等・重厚事業者等に向けた「テレワークを実施する際にセキュリティ上留意すべき点について」を公開	対策の考え方や対策例を示す「テレワークセキュリティガイドライン（第4版）」について改めて周知	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取組を促す「産業界へのメッセージ」を発出

○新しいデジタル技術の活用とリスクマネジメント ～DX with Cybersecurity～

・企業が新たなデジタル技術を活用する効果を最大限に享受するためには、デジタル技術を使って何を実現したいのかを明らかにするとともに、事業に致命的な影響を与えるリスクの洗い出しを行うことが重要。
そのリスクの1つとしてデジタル技術の活用に対応するサイバーセキュリティへの対応は最も重要な柱

・また、新たなデジタル技術へのアクセシビリティは、攻撃者が排除されるものではないことも踏まえ、サイバー攻撃に対して、防御側におけるセキュリティ対応能力の効果・効率を向上させるDXを推進することも重要

○情報共有の推進と共助の取組

サイバー攻撃の複雑・巧妙化が進む現状において、被害を受けた組織等からの迅速な情報共有の重要性は増している。サイバー攻撃等の情報を一定のコミュニティに共有する動きが一層活発化している中、
運用の充実化や多様な枠組みの役割分担等によって、効果的、効率的に情報共有を進めることが重要

【政府機関等に対する攻撃の高度化・巧妙化】

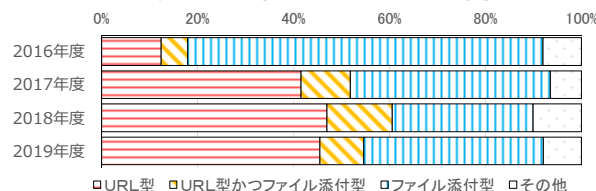
2019年度の政府機関に対する不審な通信の検知数は2018年度から減少したものの（図表1）、政府機関等に対する実質的な脅威度は引き続き高い状況にある。標的型攻撃については、より巧妙化されたメールも確認されている。また、2017年度を境として、ファイル添付型（不審なファイルを添付）に代わってURL型（不審なURLを記載）の不審メールの比率が増加（図表2）。

図表1 政府機関におけるマルウェア感染の疑いや標的型攻撃等の検知件数※2

年度	2017年度	2018年度	2019年度
マルウェア感染の疑い	169	111	55
標的型攻撃	57	66	30
その他※3	0	5	5

※2 既に攻撃手法に対応済みであるため攻撃としては失敗した通信、攻撃の前段階で行われる調査のための行為にとどまり明らかに対応不要と判断できる通信等を分析しノイズとして除去した上で、引き続き警戒を要するイベントについて集計
※3 調査行為とみられる通信やタイポスクワッシングの疑いのある通信。

図表2 政府機関等に対する不審メールの傾向



【2019年度の主なサイバーセキュリティ事案】

業務・機能・サービス障害

- ・**新型コロナウイルス感染症に**乗じ、国外において、医療関連機関などに対するサイバー攻撃が発生。ITインフラが停止するなどの影響
- ・米国の自治体においてランサムウェア被害が数多く発生。行政業務に支障を来すなどの影響

情報の毀損及び漏えい

- ・**Emotet**の再流行が広がり、多くの組織で情報流出等の被害を公表
- ・大手電機会社が、自社のネットワークに不正アクセスを受け、個人情報と企業秘密が流出した可能性があることを公表
- ・情報機器の処分等を営む企業において、従業員が**行政文書が蓄積されたHDDを盗み出し、転売**をしていたことが発覚

金銭の窃取・詐取等

- ・2019年7月にサービスを開始したキャッシュレス決済（コード決済）サービスが不正アクセスを受け、**約3800万円**の被害
- ・インターネットバンキングに係る不正送金事犯について、2019年9月から被害が急増し、発生件数**1872件**、被害額**約25億2100万円**

【国外の動き】

○諸外国の政策

- 米国**  ・新たな国家サイバー戦略（2018/9）
・サイバーセキュリティ人材の強化を目的とした大統領令（2019/5）
・情報通信技術等のサプライチェーンの保護に関する大統領令（2019/5）
- EU**  ・一般データ保護規則（GDPR）成立（2018/5 施行）
・欧州サイバーセキュリティ法成立（2019/6 施行）
・5Gネットワークのサイバーセキュリティに関するツールボックス（2020/1）
- 中国**  ・サイバーセキュリティ法の施行及び同法に基づく関連規制を制定（2017/6）
- ロシア**  ・情報安全保障ドクトリン公表。サイバー空間における安全保障を目的としたサイバーセキュリティ政策の方向性を明示（2016/12）

○サイバー空間における国際法の適用に関する議論

2019年12月、第6会期国連政府専門家会合（GGE）が立ち上がり議論を深化

(参考) 新型コロナウイルス感染症への対応と今後の取組

- 新型コロナウイルス感染症への対応として、様々な場面でインターネットの利用や新たなデジタル技術の活用が増加することが想定される。
- 今後は、新しい生活様式の定着に向けて、テレワークの導入や活用だけではなく、サービスの提供自体などにも新たなデジタル技術を活用することも想定され、このような状況を注視してサイバーセキュリティ対策を進めていくことが重要。

これまでの主な政府の動き

※ 令和2年3月28日（令和2年4月7日改正版）新型コロナウイルス感染症対策本部決定

「新型コロナウイルス感染症対策の基本的対処方針」※において、事業者においては、テレワークなどを活用することで、さらに接触の機会を減らすことを協力して行っていく必要があるとされた。こういった状況を注視しつつ、基本的な対策方法などについて効果的に周知活動を進めていくことが重要

NISC

- 国民一般に向けて、注意すべき基本的なポイントを周知（3/27）
- 政府機関等・重要インフラ事業者等に向けて、テレワークを導入する際のセキュリティ上留意すべき点について注意喚起（4/7及び4/9）
（「テレワークを実施する際にセキュリティ上留意すべき点について」をHPに公開（4/14））
- 新しい生活様式の実践に向けて、「テレワーク等への継続的な取組に際してセキュリティ上留意すべき点について」をHPに公開（6/11）

総務省

- テレワークの積極的な活用について周知するとともに、テレワーク関連支援情報やセキュリティ確保に関する情報をHPに公開（2/25）
- テレワークの導入に当たってのセキュリティ対策の考え方や対策例を示す「テレワークセキュリティガイドライン（第4版）」について改めて周知
- より具体的で分かりやすく実践的な内容のチェックリストを策定中であり、また、セキュリティの専門的な相談に対応できる窓口を設置しており、これらについても幅広く周知

経産省

- 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「産業界へのメッセージ」を公表（4/17）
 - ① 新型コロナウイ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
 - ② 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
 - ③ アップデート等の基本的な対策を実施すること
 - ④ 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

新しい生活様式の定着に向けた今後の取組

新しい生活様式の定着に向けて、更にデジタル化を推進していく必要性が明らかとなる状況を踏まえ、サイバーセキュリティ対策を進めていくことが重要

<主な具体的取組>

- ✓ 政府機関等においては、機関外での業務実施機会や複数の政府機関等が外部サービスを利用して連携する機会が増えたことを踏まえ、かかる環境下での情報セキュリティに対する特有の留意点や考え方を示していくことが有用であり、統一基準への追記を始め、必要な発信を行っていく。（NISC）
- ✓ 中小企業等に向けては、これまで未導入だった企業等においてもテレワークの導入が広まる中で、より具体的で分かりやすく、実践的な内容のガイドラインの策定を実施。また、セキュリティ対策に関する専門的な相談に対応できる窓口を設置する。（総務省）
- ✓ テレワークの推進に当たり、デジタルで様々なやり取りを完結できる環境の構築に向けて、電子データの信頼性を確保するトラストサービスを推進する。（総務省）
- ✓ IoT機器等を活用して制御系システムを含めた拠点の無人化等の推進が見込まれる中、フィジカル・サイバー間をつなげる機器・システムにおけるセキュリティ・セーフティ要求の検討等に資する「IoTセキュリティ・セーフティ・フレームワーク」を策定する。（経産省）

サイバーセキュリティ2020（2部3章 現状の認識を踏まえた加速・強化すべき取組）の概要

- 新たな情報通信サービスの普及、新型コロナ感染症対策としてのテレワークなどの積極的活用、急速な状況変化を逃さないサイバー攻撃の発生といった状況に着目し、自助・共助・公助の観点から、現在の戦略の実行に当たり特に加速・強化すべき取組をまとめ、今後の次期戦略につなげるものとして整理。

1 現状から見てきたこと

1.1 新型コロナウイルス感染症対応を踏まえたDXの推進とサイバーセキュリティ対策(DX with Cybersecurity)

1.2 クラウドサービスの利用拡大に伴う
防御範囲・手法の転換

1.3 5Gの商用サービス開始とそれに
伴うデータ活用の高度化

1.4 サプライチェーン・リスクの拡大と
予見性の確保

1.5 国際的な議論の高まりと統一的な
国際ルールへの期待

2 今後の検討に当たっての視点

2.1 リスクマネジメントの実施と戦略的行動

セキュリティを、DXを成功させる上での重要な機能と位置付けた上で、リソースの制約を意識しつつ、リスクマネジメントを進めることが重要

2.2 情報共有体制の積極的活用による共助の強化

情報共有体制の運用の充実化や多様な枠組みが存在し、それらの役割分担によって、効果的、効率的に情報共有を進めることが重要

2.3 政府に期待される役割

自助や共助の取組を過不足なくサポートするという役割を意識し、インセンティブ構造を明確にすることで仕組みをデザインして社会全体として効果を最大化。また、国際場裡においては、有志国等との連携協力を質・量とも高めていくことなどが重要

3 今後加速・強化して取り組むことが重要な事項

3.1(1) サプライチェーン全体のサイバーセキュリティ
対策の強化

3.2(1) 重要インフラ対策の推進

3.2(2) 政府機関対策の推進

3.2(3) 東京2020大会を踏まえた未来につながる
成果の継承

3.3(1) 情報共有と重層的な国際連携の枠組み

3.3(2) 海外支援戦略

3.4(1) DX with Cybersecurityの実現に向けた人材育成

3.4(3) 研究開発の推進

3.4(2) 政府機関等のサイバーセキュリティを支える人材の確保・育成

3.4(4) 普及啓発の推進

参考資料

（ 2 部 2 章（主な昨年度の取組実績、評価及び今年度の取組） 、
別添 1（2020年度のサイバーセキュリティ関連施策の抜粋） ）

2部2章（主な昨年度の取組実績、評価及び今年度の取組）

1. 経済社会の活力の向上及び持続的発展

昨年度の実績

- 経営層の意識改革等を目的に、企業のサイバーセキュリティ対策実施状況の可視化ツールや「サイバーセキュリティ関係法令Q&Aハンドブック」等を公開
- サプライチェーン全体の対策強化に向け、CPSF※の社会実装の推進や、中小企業向けにセキュリティ対策支援に関する実証事業等を実施
※サイバー・フィジカル・セキュリティ対策フレームワーク（経産省）
- 安全なIoTシステムの構築に向け、パスワード設定等に不備のあるIoT機器を調査及び注意喚起する取組「NOTICE」や、IoT機器の特性や利用方法等を踏まえて整理したセキュリティ要件を満たす機器の利用を推奨する施策等を実施

サイバーセキュリティお助け隊実証事業
＜実証地域＞



NOTICEの広報ポスター



評価

経営層の意識改革やサイバーセキュリティに対する投資の促進等については、引き続き、事業継続を確固なものとしつつ新たな価値を創出していくためにはサイバーセキュリティが必要であるとの認識を広げる取組を促進していくことが重要。また、中小企業をはじめサプライチェーン全体の対策強化の取組が着実に進展している中、取組の一層の強化に向けて、既存の制度の周知強化も含め、関係省庁が連携して各種取組を推進していくことが重要。安全なIoTシステムの構築については計画どおりに進捗しているものの、例えば、NOTICEにおける注意喚起後に改善が見られない利用者への有効な注意喚起手法の検討など、今後、整備した枠組み等が円滑に実施されるようフォローしていくことが求められる。

今年度の取組

- 経営層の意識改革等に向けては、これまでに整備したツールの改善や活用の促進を進める。
- サプライチェーン全体の対策強化に向けては、技術検証体制の整備等サプライチェーン・リスクに対応するための取組や、中小企業のサイバーセキュリティへの意識向上を図るとともに実態やニーズをよりきめ細かく把握する取組などを進める。
- 安全なIoTシステムに構築に向けて、産官学民及び民間企業相互間の連携により、脆弱なIoT機器の対策を進める。

2部2章（主な昨年度の取組実績、評価及び今年度の取組）

2. 国民が安全で安心して暮らせる社会の実現

昨年度の実績

- 重要インフラの安全性・持続性確保の観点から、指針※を改定したほか、官民の枠を超えた訓練・演習の実施等、第4次行動計画に基づく各施策を実施
※重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）（NISC）
- 政府機関等全体のセキュリティ対策強化に向け、次期統一基準群の改定に向けた検討を行ったほか、適切な水準が確保されたクラウド利用のため、「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組み」を決定。また、サイバーセキュリティに関する技術・能力を競う競技会を実施
- 東京2020大会に向け、重要サービス事業者等に対するリスクアセスメントの促進及びサイバーセキュリティ対処調整センターにて情報提供を実施
- 従来を枠を超えた情報共有・連携体制の構築として、サイバーセキュリティ協議会においては、協議会構成員の募集を3回行い、協議会構成員は漸次拡大するとともに、協議会の特性を活かした迅速な情報共有を行ったほか、運用ルールの見直しを実施

評価

重要インフラ防護、政府機関等の対策強化、東京2020大会のセキュリティ確保、従来を枠を超えた情報共有・連携体制の構築等、各種取組は着実に進展。今後、第4次行動計画、統一基準群については、それぞれ、昨今の環境変化や対策状況を踏まえて、次の改定に向けた検討が求められる。また、対処調整センターや協議会等、昨年度取組を開始したものについては、実際の運用の経験等を踏まえ、充実・強化していくことが重要である。

今年度の取組

- 重要インフラ防護、政府機関等の対策強化、東京2020大会のセキュリティ確保、従来を枠を超えた情報共有・連携体制の構築等について、既存の枠組みに基づく取組を着実に進めていくとともに、2019年度に発生又は明らかになった事案や運用の状況等も踏まえて、運用の充実・強化や枠組みの見直しなどを進めていく。

2部2章（主な昨年度の取組実績、評価及び今年度の取組）

3. 国際社会の平和・安定及び我が国の安全保障への寄与

昨年度の実績

- G20大阪サミット等における共同声明や意見交換を通じて、サイバー面での協力を強化していくことを確認。また、サイバー空間における法の支配の推進に寄与することを目指し、今期国連政府専門家会合に参画し、国連におけるサイバーセキュリティに関する議論に積極的に貢献
- サイバー空間を悪用したテロ組織の活動等に係る情報の収集・分析の強化や、ARF※の枠組等を通じ、今後取り組むべき信頼醸成について議論を実施
※ASEAN Regional Forum
- 13の国と地域の間で二国間協議を開催するとともに、多国間対話等を通じ、国際協調・協力を推進。また、事故対応等に係る国際連携の強化に向けた演習や能力構築支援を実施

日・ASEANサイバーセキュリティ政策会議



評価

サイバー空間における法の支配の推進や国際協力・連携の深化が着実に進展。今後は、継続的に関係国と連携しつつ、今期国連政府専門家会合への関与等を通じて、更なる議論の深化を図るとともに、既に合意された規範について国際社会が実施するよう促していく必要がある。

今年度の取組

- 法の支配の推進については、国連政府専門家会合における議論が報告書の作成に向けて加速することから、規範の形成・普遍化についての議論を深化させ、責任ある国家の行動規範及び国家実行を積み重ねていく。
- また、引き続き、サイバー攻撃に対する国家の強靭性を確保するとともに、積極的に能力構築支援等を行うなど国際協力・連携の深化に取り組む。

2部2章（主な昨年度の取組実績、評価及び今年度の取組）

4. 横断的施策

昨年度の実績

- サイバーセキュリティ人材の育成・確保を強化すべく、人材育成に関する産学官の多様な取組について、関係機関の間で情報共有を行うとともに、施策間の連携を促進。また、人材育成や普及啓発に関する官民の様々な取組を集約するポータルサイトを構築し、仮運用を開始
- 研究・技術開発の推進のため、「我が国におけるサイバーセキュリティ研究・技術開発の取組方針」を策定するとともに、方針に基づいて取組を実施
- 普及啓発の観点では、「サイバーセキュリティ意識・行動強化プログラム」に沿って具体的な取組を実施。また、「サイバーセキュリティ月間」において、認知度の高いコンテンツとのタイアップ
（ソードアート・オンライン-アリスゼーション-War of Underworld）を行い、若年層に重点を置いたキャンペーン等を実施

TVアニメ『ソードアート・オンライン-アリスゼーション
War of Underworld』とタイアップ



評価

戦略マネジメント層及び実務者層・技術者層の育成等の取組は着実に進展しているが、人材の育成・確保は継続して進めていく必要がある。研究開発については、研究・技術開発の取組方針に基づき、引き続き、取組を推進していくことが求められる。普及啓発の取組は、サイバーセキュリティ月間において、インフルエンサーの発信※によって、若年層でもよりリーチしにくい層に対しての普及啓発を図ることができたこと等も踏まえ、今後の検討を進めていくことが重要である。

※本年はInstagramやTwitterなどで多くのフォロワーを持つ、いわゆるインフルエンサーにサイバーセキュリティに関する普及啓発の投稿を依頼

今年度の取組

- 人材育成については、サイバーセキュリティ人材育成取組方針に基づき、関係施策を推進していく。
- 研究開発の推進に向けては、サプライチェーン・リスクに対応するためのオールジャパンの技術検証体制の整備、国内産業の育成・発展に向けた支援策、攻撃把握・分析・共有基盤の強化や暗号等の基礎研究の促進の取組等を推進するとともに、産学官連携の研究振興策について議論を進める。
- また、普及啓発については、普及啓発全体を表す代表的な指標をモニタリングし、PDCAサイクルを着実に推進していくほか、GIGAスクール構想における学校現場に一人一台の端末を配布するタイミングをきっかけとして、児童生徒がインターネットやセキュリティについて学ぶための資料の作成等を実施するなどにより、理解を深める。

2部2章（主な昨年度の取組実績、評価及び今年度の取組）

5. 推進体制

昨年度の実績

- 内閣サイバーセキュリティセンターを中心に、関係機関とのパートナーシップに基づく国内外のインシデント及びサイバー攻撃に関する情報の共有を行うとともに、国際担当者間の会合やIWWNでの分析レポートの情報発信により、総合的分析機能の強化を推進
- 戦略の趣旨を国内外の関係者に向け効果的に発信することを目的に、サイバーセキュリティ2019の冊子を制作。内閣官房及び関係府省庁において、戦略のカラー冊子やサイバーセキュリティ2019の冊子を活用するなどして、各種セミナーでの説明等を通じて、戦略等の発信を実施

サイバーセキュリティ戦略



サイバーセキュリティ2019



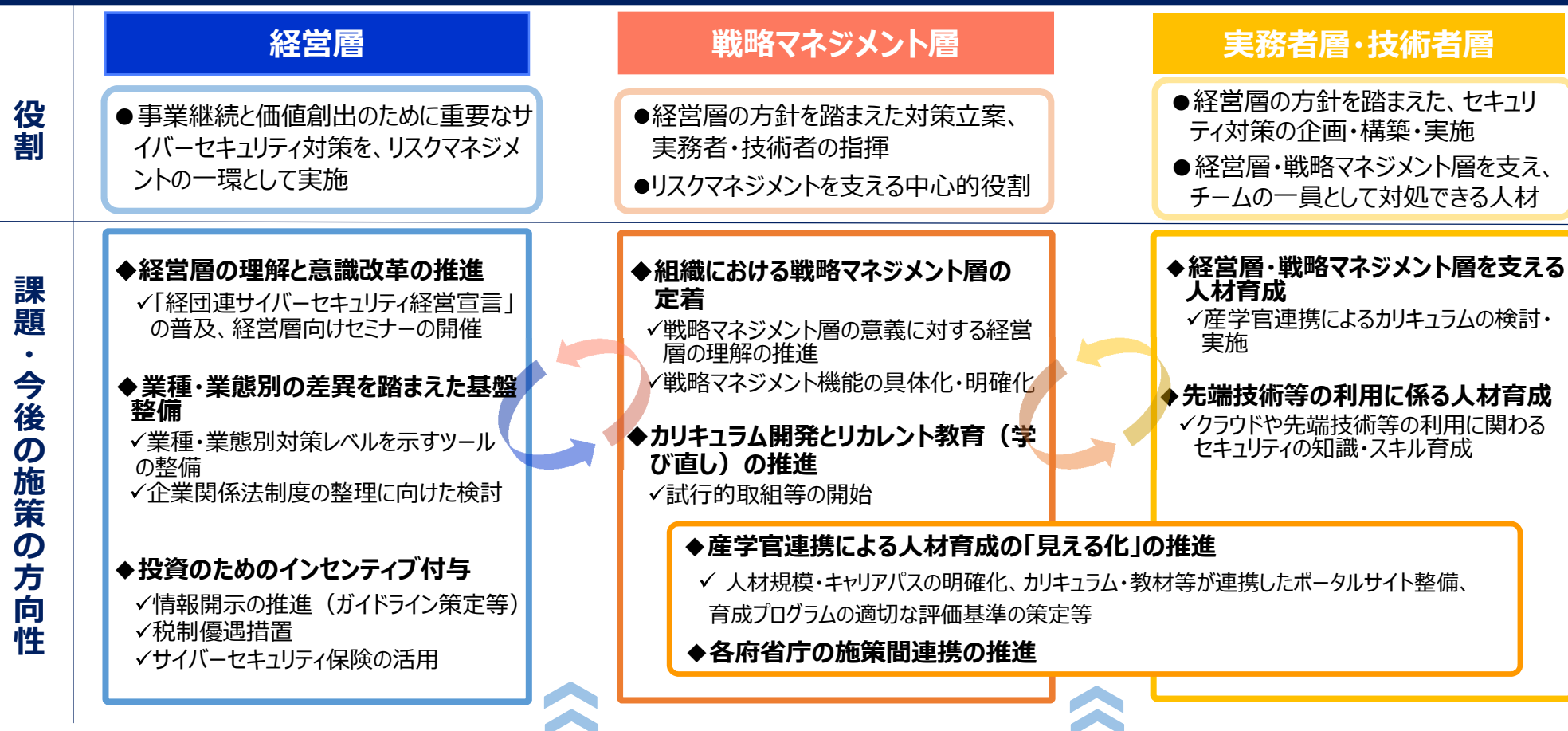
評価

戦略の国内外の関係者への更なる浸透を図るため、引き続き、取り組むことが重要。戦略で掲げたサイバーセキュリティエコシステムの実現には、あらゆる主体がセキュリティに取り組むインセンティブを生み出すことが重要であり、全体として統一感を持って、考え方を浸透させていくために、戦略の基本的な考えを示しつつ、官民の個別の取組に反映しやすいように説明を行うなど、国内外の関係者との一層の連携の強化を図り、戦略の発信等に取り組むことが求められる。

今年度の取組

- 関係機関の一層の能力強化に向けては、既に構築している仕組みの機能向上を図るとともに、連携体制についても逐次見直しを実施する。
- また、全ての主体に関する自律的な取組を促進するため、引き続き、国内外の関係者へ戦略及びこれに基づく年次計画等の発信を行う。加えて、関係者との意見交換を行って、サイバー攻撃による被害の実態を含むサイバー空間に係る動向の把握に努め、東京2020大会後を見据えた検討を進めていく。

- 「サイバーセキュリティ人材育成プログラム」(平成29年4月決定)等を踏まえ、①経営層によるリスクマネジメントの一環としてのサイバーセキュリティ対策の推進、②戦略マネジメント層の人材像やモデルカリキュラムについて、専門調査会における検討を踏まえ、本取組方針を策定。
- 本取組方針の内容については、新たな「サイバーセキュリティ戦略」(平成30年7月閣議決定)に反映。今後、具体的な取組を推進。



若年層教育の充実

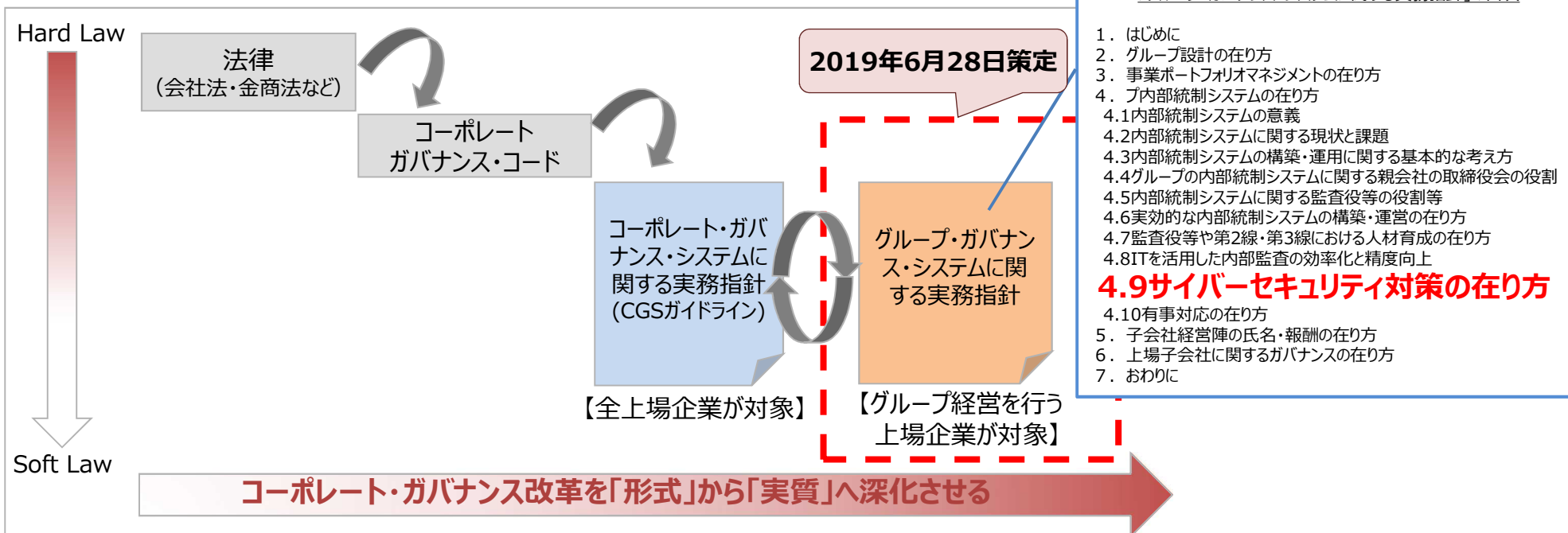
- ＜課題＞ ICTの基本的な原理・仕組みを理解し、論理的思考力を育成。情報モラル教育も重視
- ＜施策＞ 初等中等教育段階での教育課程内の取組に加え、地域や企業等で、自由に機器・ツールを用いて学べる機会を創出

中小企業関連の取組

- ＜課題＞ 知識・スキルが十分ではなく、セキュリティ対策への投資が困難。踏み台となった場合、社会への影響が大きい。
- ＜施策＞ クラウド活用等と一体の対策集の策定・普及、インセンティブの仕組(税制優遇等)の検討

- 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



- 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

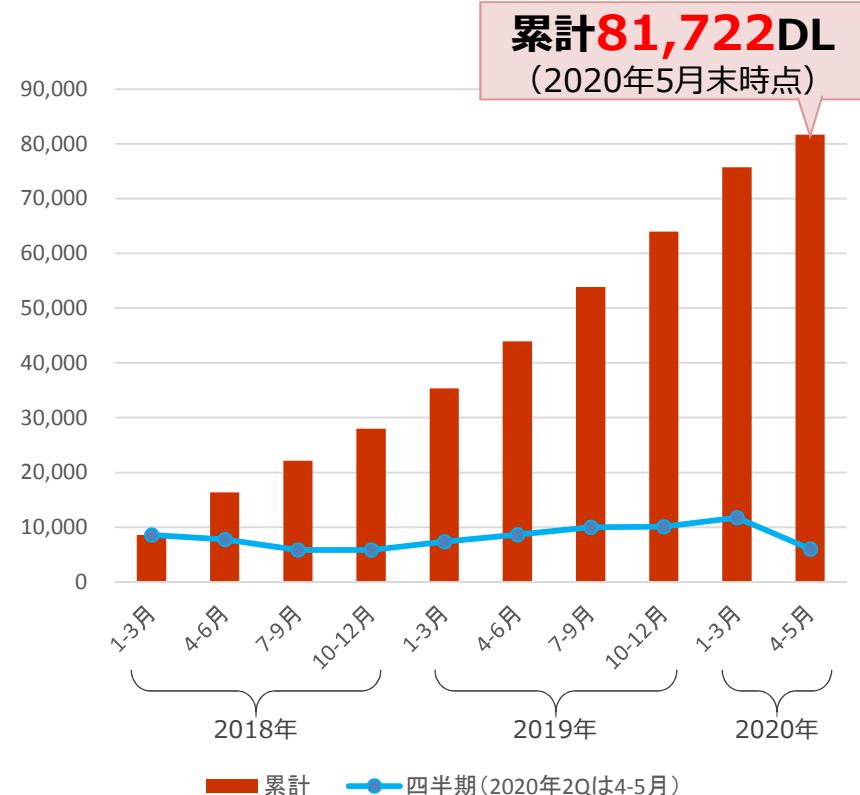
サプライチェーンセキュリティ

- 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

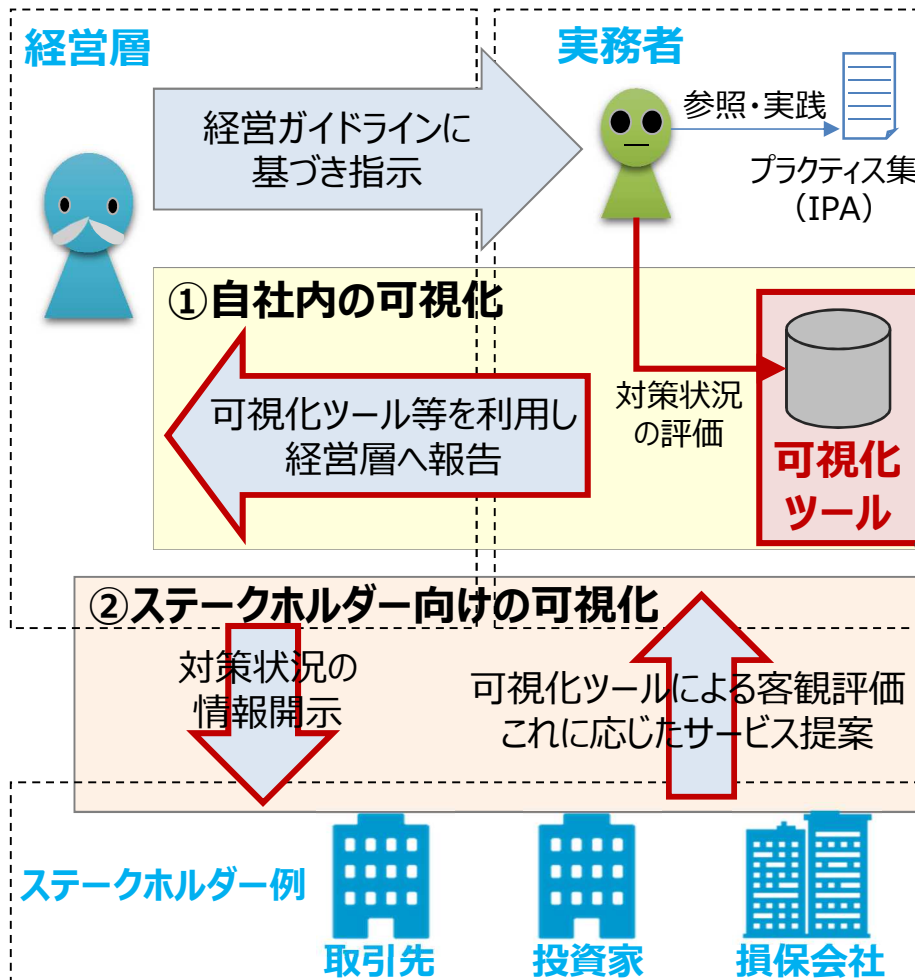
- 指示10** 情報共有活動への参加

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



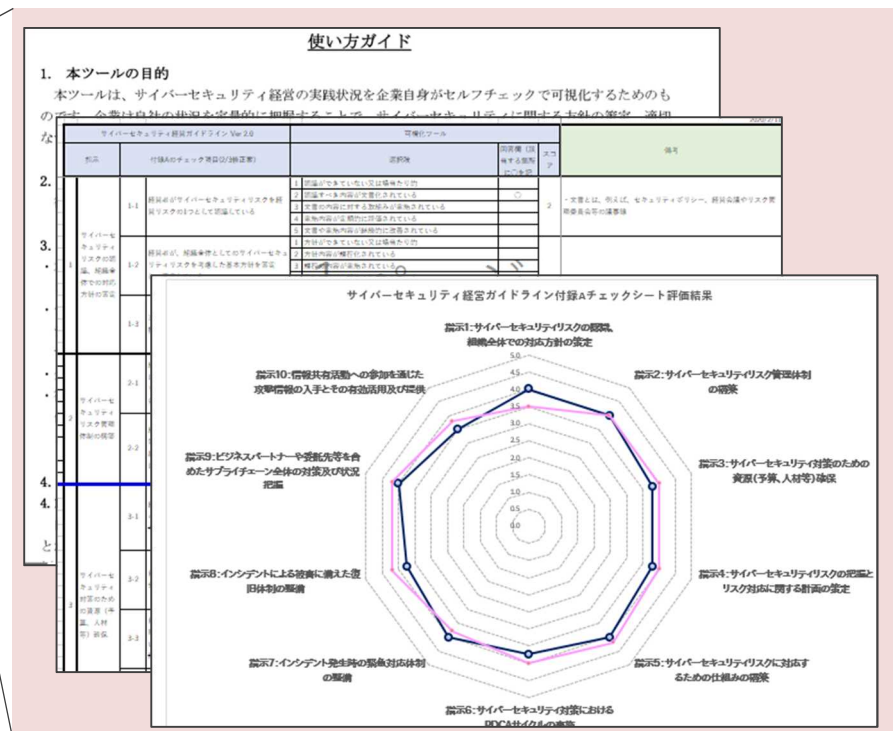
【参考】上場企業数 第一部 2,157社 第二部 488社
日本取引所グループ公表 2019年12月17日時点

- 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。



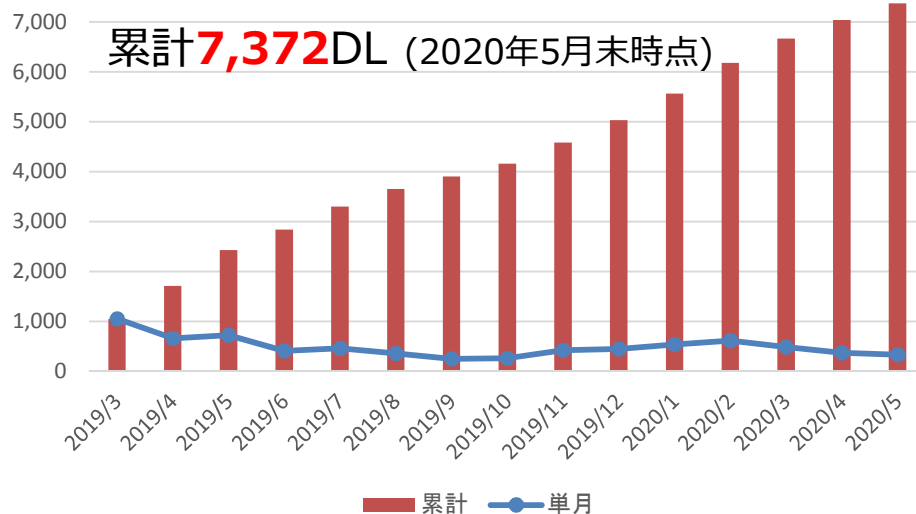
可視化ツールβ版の特徴：

- 「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



- 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＞

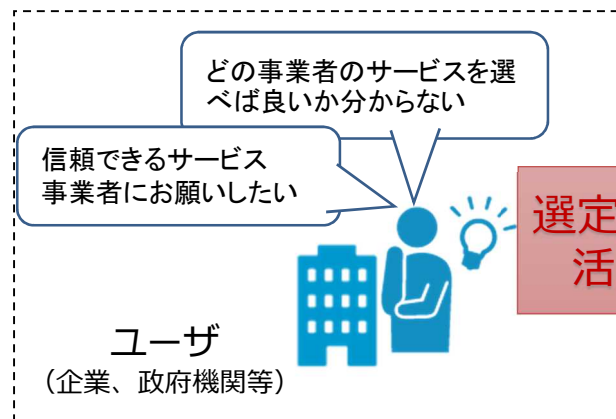
サイバーセキュリティ対策を実践する上での悩みに対する、企業の具体的な取組事例を紹介

＜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）

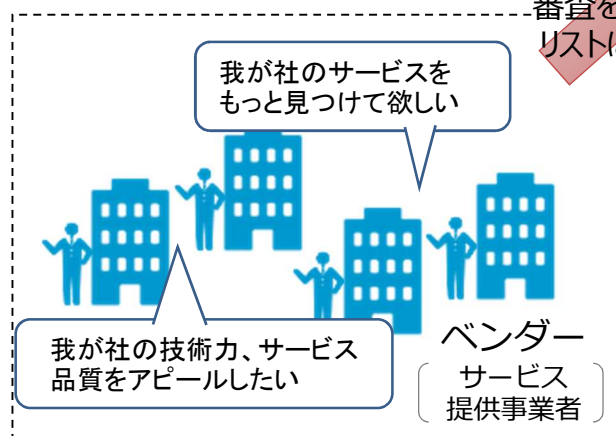
- 一定の技術・品質管理要件を定めた「情報セキュリティサービス基準」を策定し、基準に適合するサービスのリストを2018年6月よりIPAが公開。

＜情報セキュリティサービスにおける課題＞



選定時に活用

審査を受けてリストに掲載



○情報セキュリティサービス基準適合サービスリスト (IPA)

審査登録機関による審査で基準を満たすと認められたサービスをリストとして公開

サービス名称	事業者	登録年月	サービス内容	審査機関
情報セキュリティ監査	株式会社 情報セキュリティ監査	2018年7月	情報セキュリティ監査	IPA
脆弱性診断	株式会社 脆弱性診断	2018年7月	脆弱性診断	IPA
デジタルフォレンジック	株式会社 デジタルフォレンジック	2018年7月	デジタルフォレンジック	IPA
セキュリティ監視・運用	株式会社 セキュリティ監視・運用	2018年7月	セキュリティ監視・運用	IPA

基準を満たした **192** サービスが掲載

- 情報セキュリティ監査（54サービス）
 - 脆弱性診断（76サービス）
 - デジタルフォレンジック（26サービス）
 - セキュリティ監視・運用（36サービス）
- 2020年6月現在

情報セキュリティサービス基準

○情報セキュリティサービス基準 (METI)

技術

品質

上記4サービスに関して
技術要件・品質管理要件
を定めた基準

本制度を通じて
目指す社会

専門的知識を持たない
ユーザでも、自社に
最適かつ品質を備えた
サービスを選択できる

技術と品質を備えた
情報セキュリティサービスの
普及・発展

制度の普及・浸透

- ・セキュリティ製品等の選定の決め手の一つは、実環境への導入実績。
- ・実環境への試行導入・実績公表を行う企業向けの手引きを作成するとともに、試行導入に関心があるユーザーとベンダーをマッチングし、我が国発のセキュリティ製品の試行導入・実績公表を促進。

＜ベンダー側の課題＞

- ・良い製品を作っても、実績が示せず、利用者が試さない。

＜重要分野のセキュリティ製品評価のイメージ＞

- ・重要となる分野の予測をIPAが公開。
- ・当該分野に関連するセキュリティ技術・製品について、有識者による率直な評価を頂き、その内容を公表。

支援

ベンダー企業

＜ユーザー側の不安＞

- ・セキュリティ製品の導入が既存システムへ影響を与えないか。
- ・導入事例を公表することでリスクが高まらないか。

＜試行導入・導入事例公表の手引きのイメージ＞

- ・どのようなプロセスでセキュリティ製品の導入対象システムを選定したのか、事例公表に踏み切ったのか。

支援

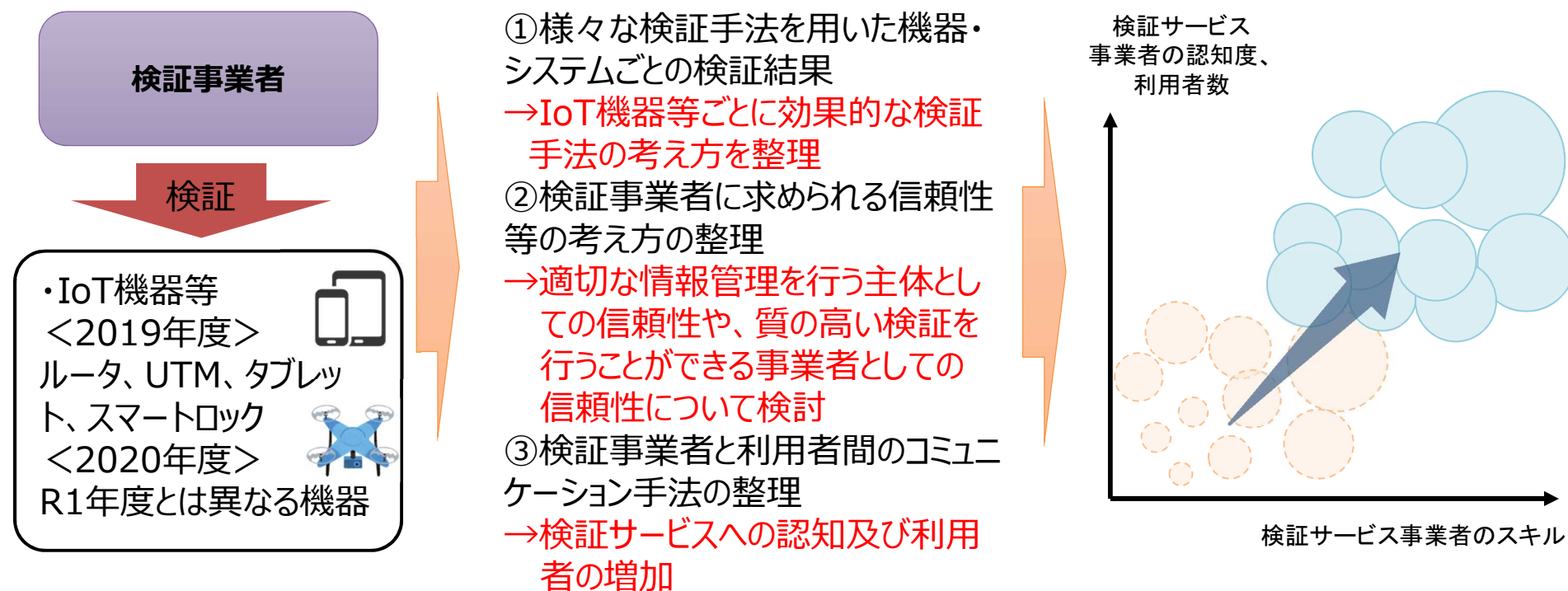
ユーザー企業

マッチングの機会を創出

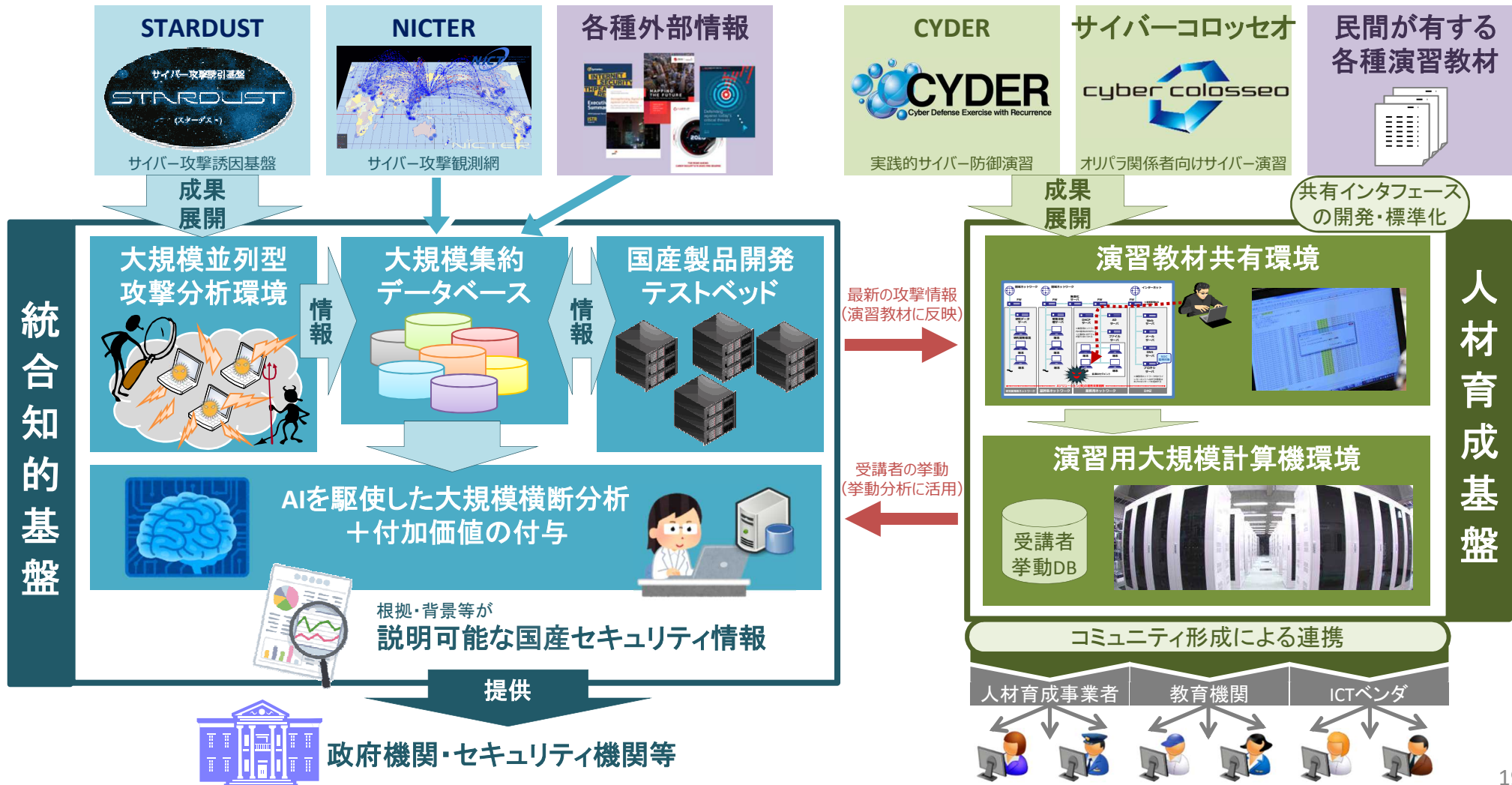
コラボレーション・
プラットフォーム

セキュリティ製品の実環境への試行導入と実績公表

- 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。



- サイバーセキュリティ情報を国内で収集・蓄積(生成)・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し、産学に開放し、結節点とすることで、サイバーセキュリティ対処能力の向上を図る。



- 民間企業のサイバーセキュリティ対策の情報開示の促進のため、民間企業にとって参考となり得る情報開示の事例等をまとめた手引きを策定し、令和元年6月に公表。

背景

- ✓ サイバー攻撃が深刻化する中、民間企業においてサイバーセキュリティ対策は重要な経営課題となっているが、企業としての社会的責任を果たしステークホルダーからの信頼を得るためには、**サイバーセキュリティ対策の実施のみならず、その内容について適切な情報開示が重要。**

目的

- ✓ 民間企業による**サイバーセキュリティ対策**やその対策の**情報開示の重要性**の認識を促進。
- ✓ 民間企業にとって参考になり得るような**既存の情報開示の実例**を**事例集として**示す。

活用主体

- ✓ **サイバーセキュリティ対策の情報開示**に一定の関心のある民間企業の開示の実務担当者等を想定。

対象とする情報開示

- ✓ **開示書類**を通じた情報開示を取り扱う。
- ✓ 開示書類の読み手は、**投資家、融資元、顧客・契約者・取引先、従業員、競合他社等を含む、社会全体の広範なステークホルダー**を想定。

本編 サイバーセキュリティ対策情報開示の手引き

1. 本手引きの趣旨・目的

- 【内容】
- ✓ サイバーセキュリティリスクの増大と対策の必要性
 - ✓ サイバーセキュリティ対策の情報開示の意義
 - ✓ 本手引きの目的、想定参照主体、及び内容・構成等

2. 情報開示の手段

- 【内容】
- ✓ 代表的な開示書類の紹介

3. 企業における情報開示の在り方

- 【内容】
- ✓ 企業において実施されるのが望ましいサイバーセキュリティ対策
 - ✓ 開示にあたってのポイントと記載例

4. 今後の方向性について

- 【内容】
- ✓ 手引きの改定の在り方等の今後の方向性

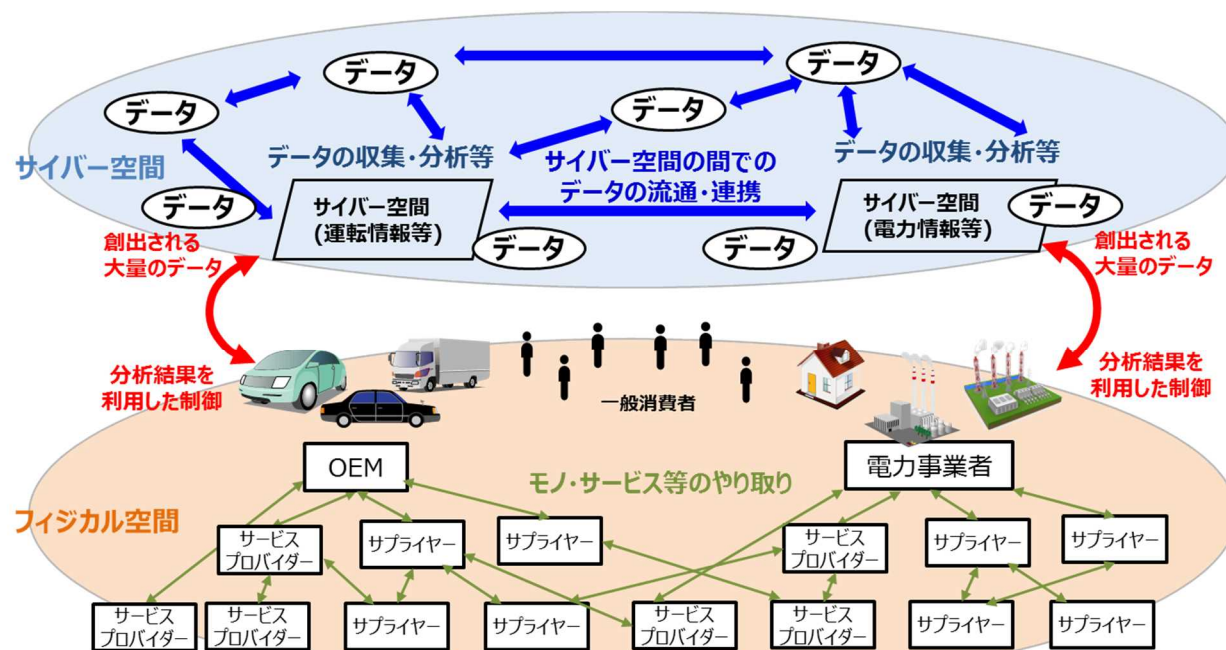
参考資料① 関連施策等の紹介

- 【内容】
- ✓ 本手引きに関連した様々な施策やガイドライン等について紹介

参考資料② 開示書類の事例集

- 【内容】
- ✓ サイバーセキュリティ対策の情報開示にかかる実際の開示書類の例について紹介

- 「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。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。
- 経済産業省では、「Society5.0」におけるセキュリティ対策の全体像を整理し、産業界が自らの対策に活用できるセキュリティ対策例をまとめた、『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）』を平成31年4月に策定。



Society5.0の社会におけるモノ・データ等のつながりのイメージ

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

- 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

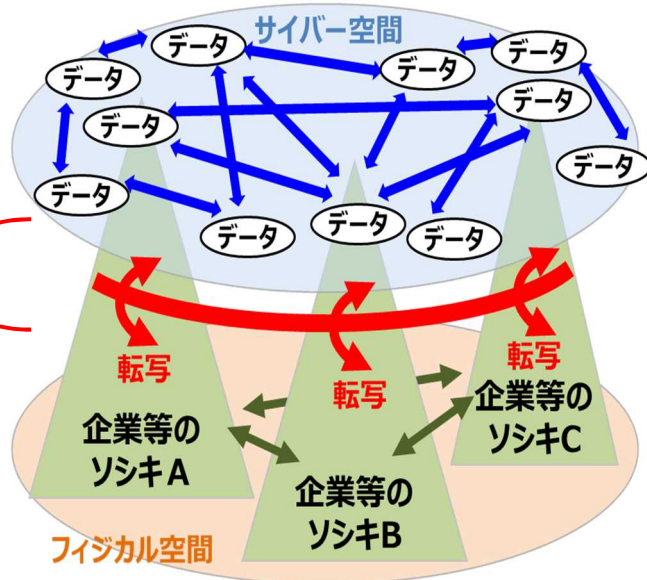
【第2層】

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	バリューチェー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、及びバリューチェー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

- 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WG 1（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

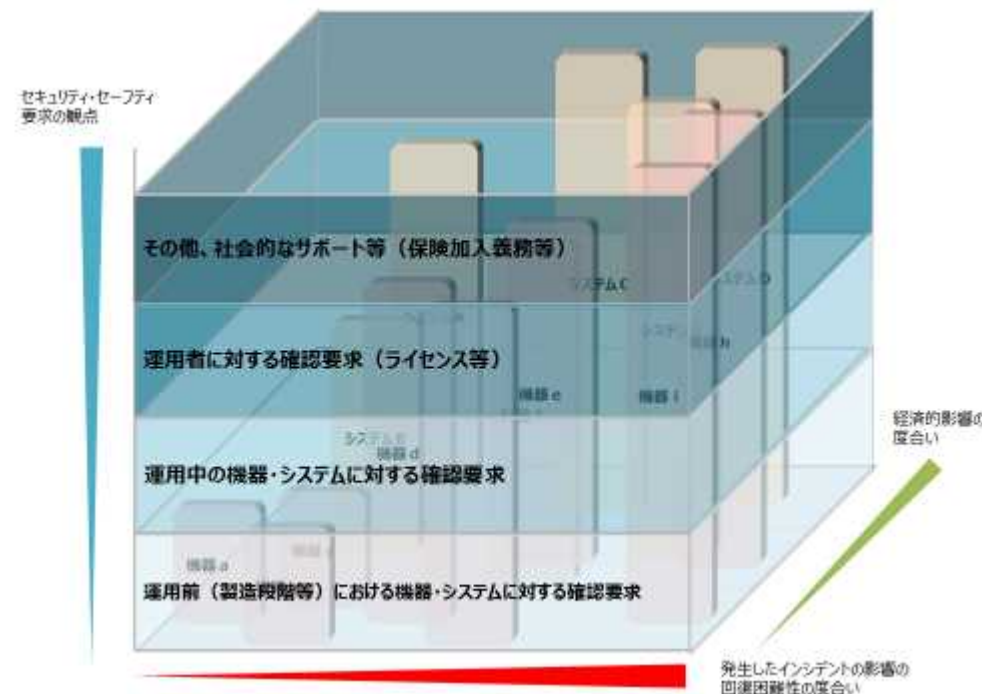
検討事項：
フィジカル空間とサイバー空間のつながりの信頼性の確保するための
「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」のドラフト策定

- IoT機器・システムの性質や利用環境によって課題が一樣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リ化した上で、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・システムのカテゴリ化やセキュリティ・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・システムのカテゴリ化のイメージ



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

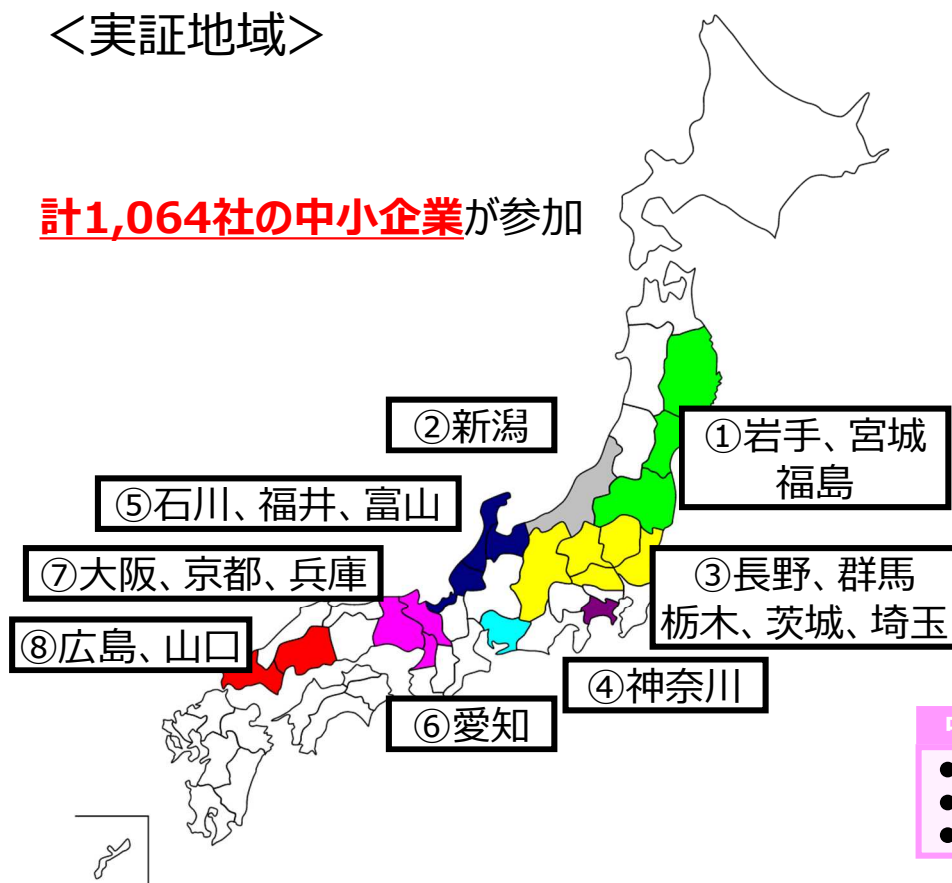


※ 同じ機器でも使用形態などによってマッピング先が異なり得る。
例えば、機器gと機器hが同じ機器で異なる使用形態である場合などがあり得る。）

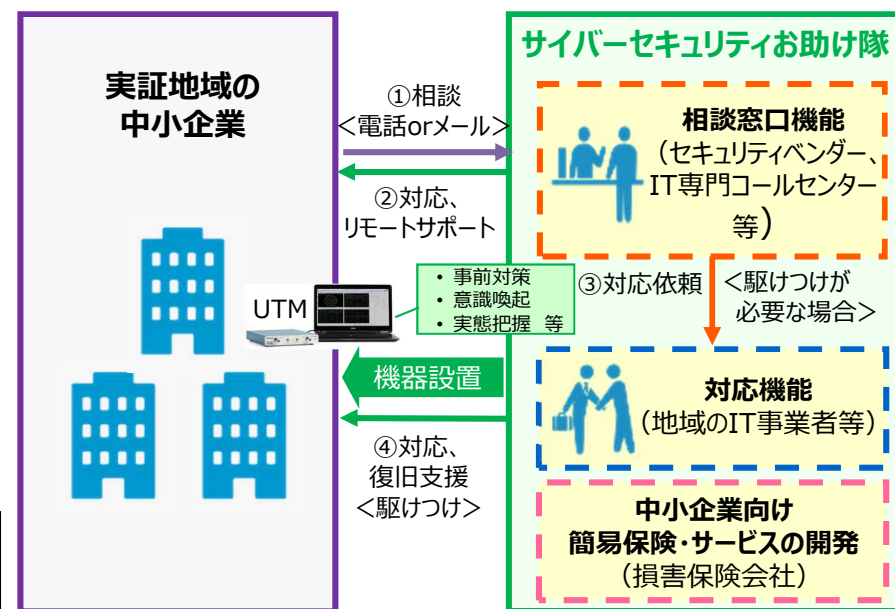
- 全国**8地域**において、地域の団体、セキュリティ企業、保険会社がコンソーシアムを組み、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした**実証事業**を実施。
- 本事業により、中小企業の事前対策の促進や意識喚起、攻撃実態や対策ニーズの把握を行い、**民間による中小企業向けのセキュリティ簡易保険サービスの実現を目指す。**

＜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

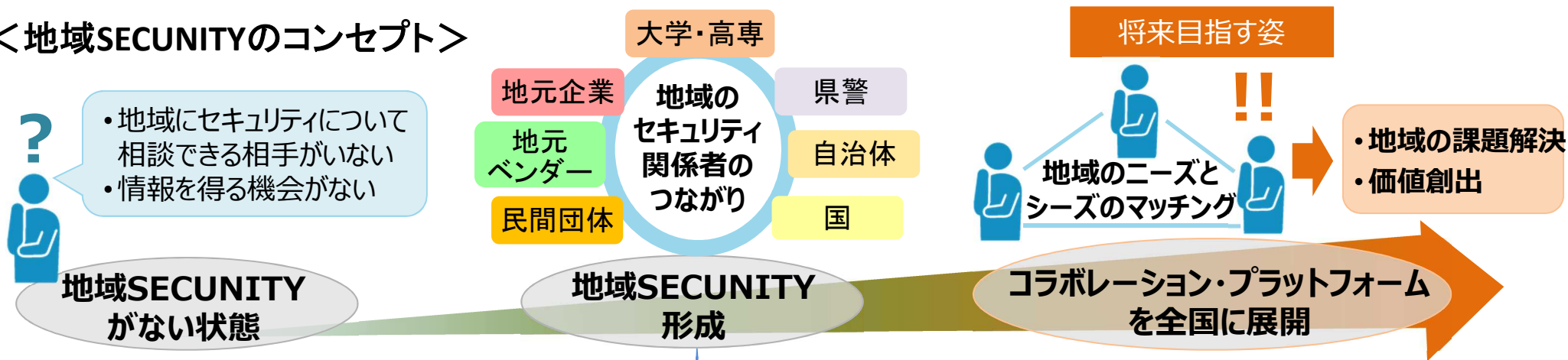
- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上 等

保険会社、セキュリティベンダー 側

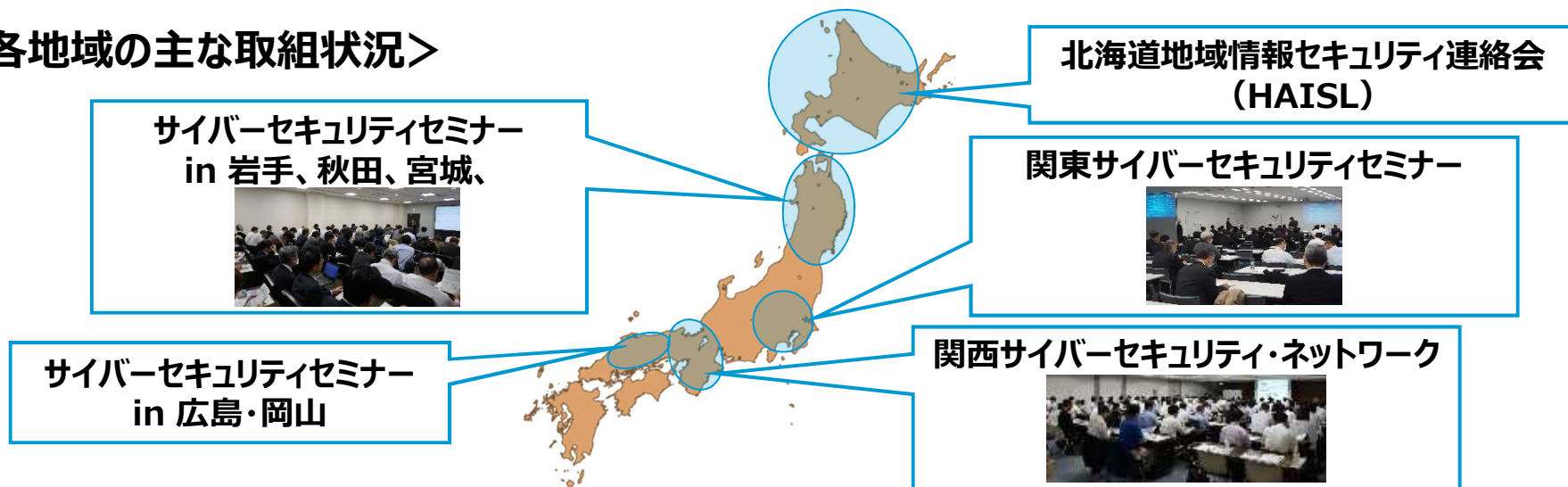
- 中小企業のセキュリティ対策状況の把握
- 中小企業の被害実態の把握
- 中小企業が求めるサービスの把握 等

- 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SECURITY」と命名。
- まずは各地域で地域SECURITY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SECURITYのコンセプト>



<各地域の主な取組状況>



- 中小企業の経営者やIT担当者に向け、情報を安全に管理するための具体的な手順等を示した**中小企業ガイドラインを改訂（第3版）し、2019年3月に公開。**



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

<主な改訂ポイント>

- サイバーセキュリティ経営ガイドラインVer2.0との整合性の改善
（「検知」、「復旧」の観点について、中小企業の実態に即した対応策を提示）
- 中小企業向けに、わかりやすい表現や記述に見直し（第1部 経営者編）
- 組織的な対策の実施体制を、段階的に進めていけるよう構成の見直し（第2部 実践編）
- 「中小企業のためのクラウドサービス安全利用の手引き」を新規追加（付録）

- ・ 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。
- ・ **9万者を超える中小企業が宣言** (2020年2月末時点)。



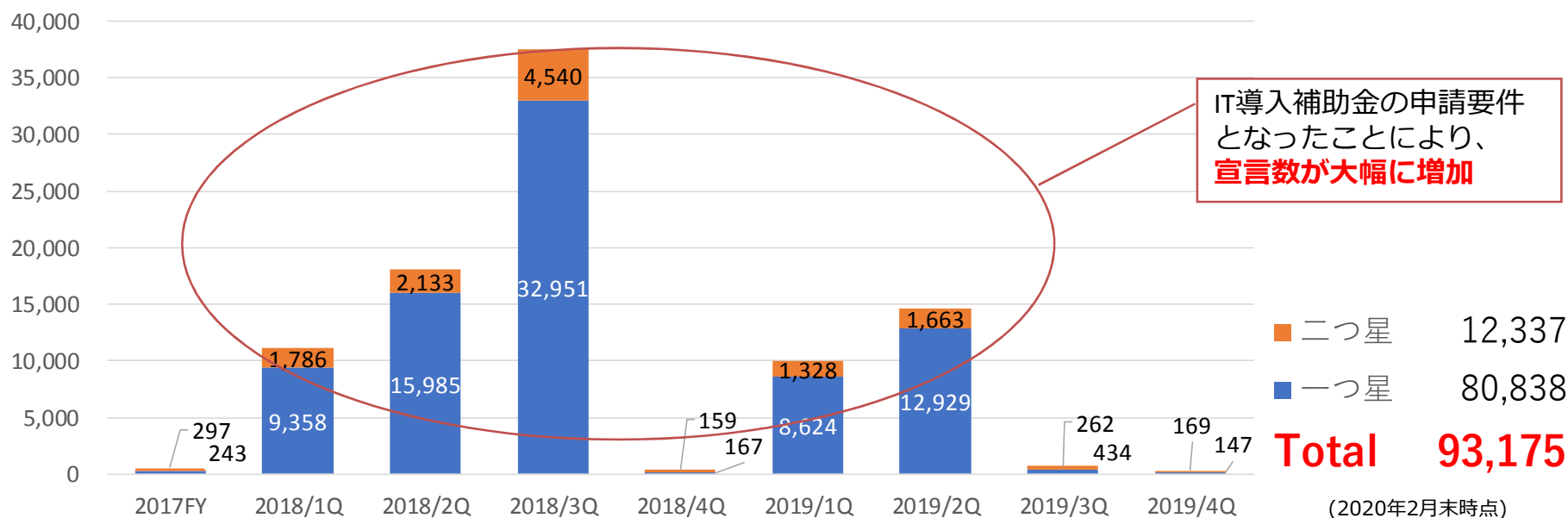
情報セキュリティ5か条に 取り組む企業



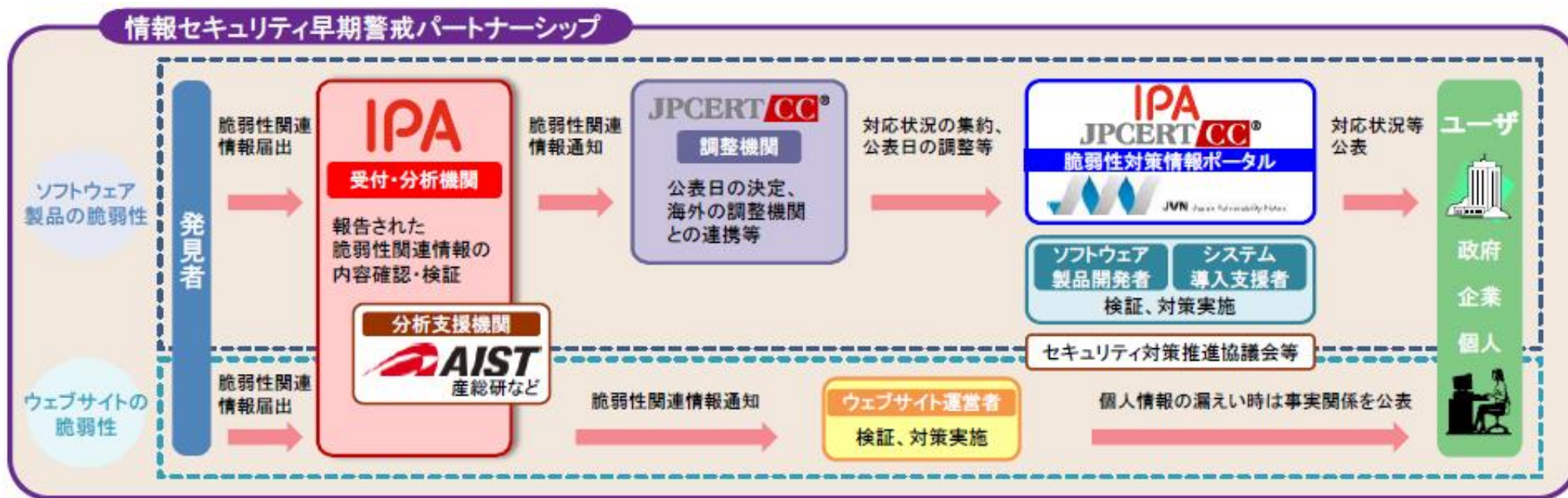
情報セキュリティ自社診断の実施及び セキュリティポリシーを策定する企業



※IPAにて、一般社団法人中小企業診断士協会、全国社会保険労務士会連合会、全国商工会連合会、全国中小企業団体中央会、特定非営利活動法人日本ネットワークセキュリティ協会、特定非営利活動法人ITコーディネータ協会、独立行政法人中小企業基盤整備機構、日本商工会議所、日本税理士会連合会と連携した普及促進活動を実施



- 「ソフトウェア製品等の脆弱性関連情報に関する取扱規程」（経済産業省告示（2017年改訂））に基づく脆弱性関連情報等の届出受付を実施。（2004年～）
- コンピュータウイルス、コンピュータ不正アクセス等による被害を抑制するため、関係機関との連携の下、脆弱性関連情報の適切な流通を実現するための取組みを実施。
- 脆弱性対策情報ポータルサイト（JVN）における対策情報等の公表、対策ツールの提供などを通じ、脆弱性対策を推進。



※IPA：独立行政法人情報処理推進機構、JPCERT/CC：一般社団法人 JPCERTコーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

- 今後製品化されるIoT機器がパスワード設定の不備等により悪用されないようにする対策として、IoT機器の技術基準※¹にセキュリティ対策のための技術基準を追加、導入※²。

※¹ 電気通信事業法では、電気通信事業者のネットワークに接続して使用する端末設備は、総務省令(端末設備等規則)で定める技術基準に適合しなければならないこととされている。

※² 情報通信審議会等からの答申を踏まえ、総務省令(端末設備等規則)を改正・施行。

【セキュリティ技術基準の概要】

- インターネットプロトコルを使用し、電気通信回線設備を介して接続することにより、電気通信の送受信に係る 機能进行操作することが可能な端末設備について、最低限のセキュリティ対策として、以下の機能を具備することを技術基準(端末設備等規則)に追加する。

① アクセス制御機能※¹(例えばアクセス制限をかけてパスワード入力を求め、正しいパスワードの入力時のみ制限を解除する機能のこと)

② 初期設定のパスワードの変更を促す等の機能

③ ソフトウェアの更新機能※¹

又は ①～③と同等以上の機能※²

※¹ ①と③の機能は、端末が電源オフになった後、再び電源オンに戻った際に、出荷時の初期状態に戻らず電源オフになる直前の状態を維持できることが必要。

※² 同等以上の機能を持つものとしては、国際標準ISO/IEC15408に基づくセキュリティ認証(CC認証)を受けた複合機等が含まれる。

- PCやスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能な機器については本セキュリティ対策の対象外とする。

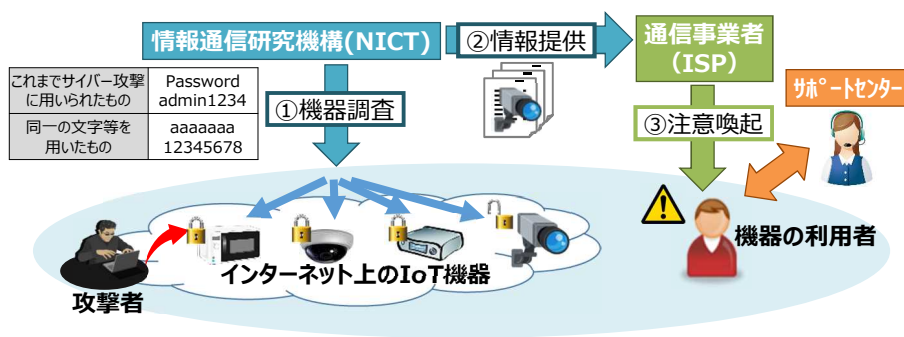
【技術基準運用の経緯】

- 2019年3月1日に端末設備等規則を改正、本年4月1日に施行。
- 改正省令の運用方法や解釈等を定めるガイドラインを2019年4月に公表。

- 情報通信研究機構(NICT)がサイバー攻撃に悪用されるおそれのあるIoT機器を調査し、インターネット・サービス・プロバイダ(ISP)を通じた利用者への注意喚起を行う取組「NOTICE」を2019年2月より実施。
- NOTICEの取組に加え、マルウェアに感染しているIoT機器をNICTの「NICTER」プロジェクト※で得られた情報を基に特定し、ISPから利用者へ注意喚起を行う取組を2019年6月より開始。

※NICTが、インターネット上で起こる大規模攻撃への迅速な対応を目指したサイバー攻撃観測・分析・対策システムを用いて、ダークネットや各種ハニーポットによるサイバー攻撃の大規模観測及びその原因（マルウェア）等の分析を実施。

【NOTICE注意喚起の概要】

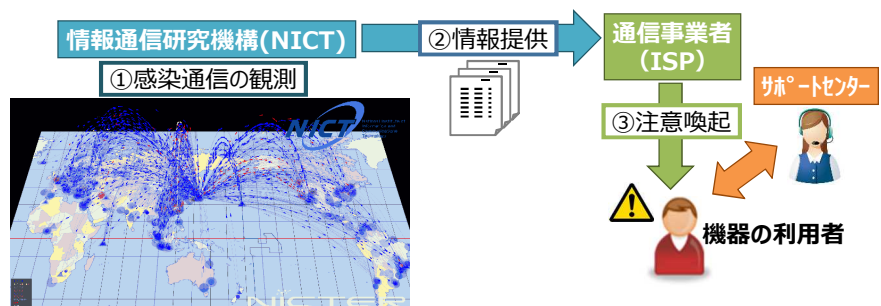


調査対象：パスワード設定等に不備があり、サイバー攻撃に悪用されるおそれのあるIoT機器

- ① NICTがインターネット上のIoT機器に、容易に推測されるパスワードを入力するなどして、サイバー攻撃に悪用されるおそれのある機器を特定。
- ② 当該機器の情報をISPに通知。
- ③ ISPが当該機器の利用者を特定し、注意喚起を実施。

【NICTER注意喚起※の概要】

※マルウェアに感染しているIoT機器の利用者への注意喚起

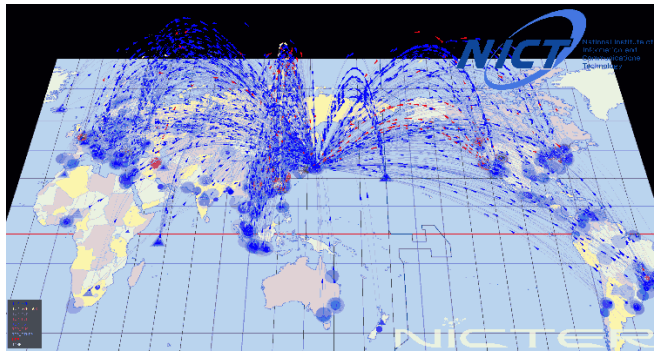


調査対象：既にMirai等のマルウェアに感染しているIoT機器

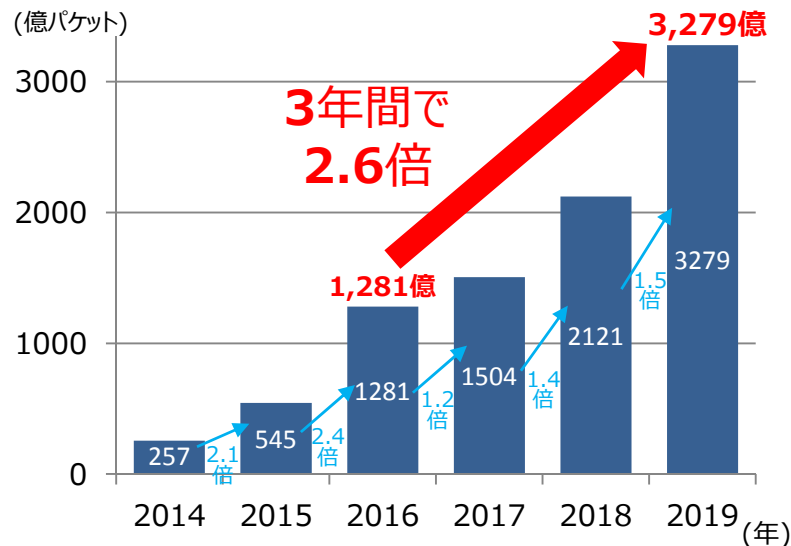
- ① NICTが「NICTER」プロジェクトにおけるダークネット※に向けて送信された通信を分析することでマルウェアに感染したIoT機器を特定。
※NICTがサイバー攻撃の大規模観測に利用しているIPアドレス群
- ② 当該機器の情報をISPに通知。
- ③ ISPが当該機器の利用者を特定し、注意喚起を実施

- 国立研究開発法人情報通信研究機構（NICT）では、大規模サイバー攻撃観測網であるNICTERにおいて、未使用のIPアドレス30万個（ダークネット）を活用し、グローバルにサイバー攻撃の状況を観測。

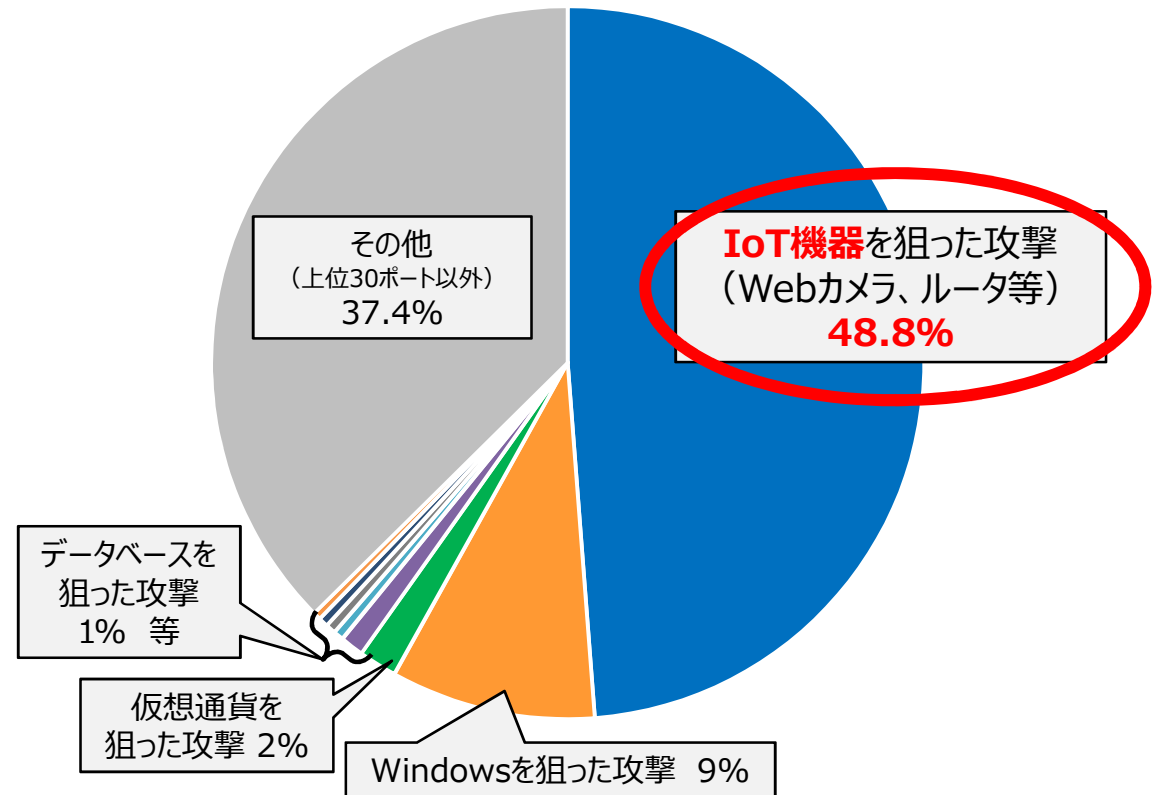
NICTERにより観測されるサイバー攻撃の様子



NICTERで1年間に観測されたサイバー攻撃関連パケット



約半数がIoT機器を狙った攻撃



※ NICTERで2019年に観測されたパケットのうち、調査目的パケット以外についてサービス種類（ポート番号）ごとに上位30ポートまでを分析したもの。

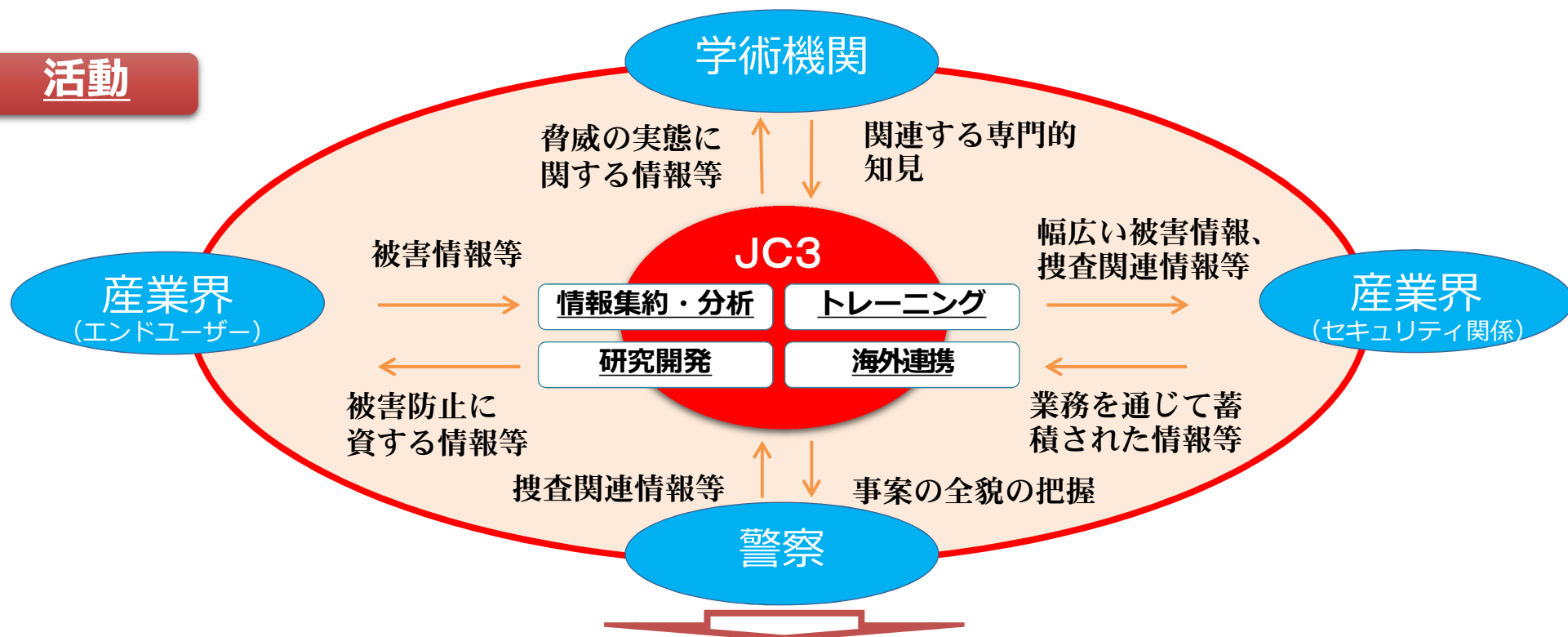
※ IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

一般財団法人日本サイバー犯罪対策センター (Japan Cybercrime Control Center: 略称JC3)

概要

産学官（法執行機関）それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を共有することにより、サイバー空間全体を俯瞰した上で、サイバー空間の脅威の大本を特定、軽減及び無効化し、以後の事案発生防止に資するための活動を行うための枠組み。

活動



サイバー空間の脅威に関する事象の全貌を把握し、その大本に対処することが可能に

情報セキュリティ安心相談窓口

独立行政法人情報処理推進機構(IPA)が国民に向けて開設している、一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する技術的な相談に対してアドバイスを提供する窓口

相談者

ウイルスに感染していると表示されたけど本当？



偽の不在通知だと気づかずリンクをタップしてしまった…



ファイルが暗号化されてしまって開けない…



アダルトサイトの請求画面が消えない…



情報セキュリティ安心相談窓口

メール、電話
で相談対応を実施



注意喚起、情報発信

安心相談窓口だより

宅配便業者をかたる偽ショートメッセージに引き続き注意！

IPAでは、安心相談窓口により、宅配便業者をかたる偽ショートメッセージ（以下SMS）の手法（図1）について取り上げてきました⁽¹⁾。本件に関する相談は継続して寄せられています（図2）。

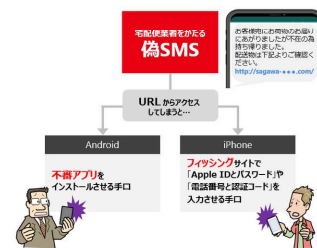
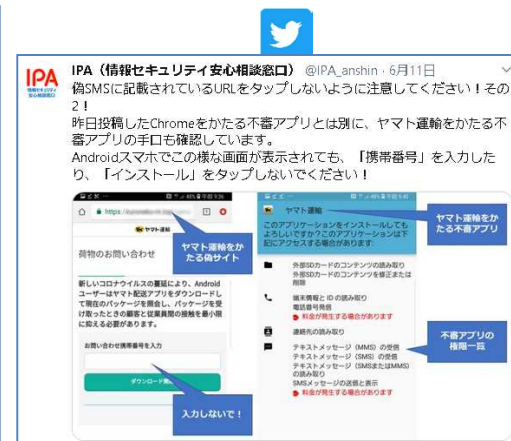


図1：アクセスする端末種類別の手口分類



自主規制団体（日本暗号資産取引業協会）の認定

- ✓ 2018年3月29日、一般社団法人 日本仮想通貨交換業協会設立
- ✓ 2018年10月24日、自主規制規則・体制の整備状況等について厳格に審査した結果、資金決済法上の自主規制団体に認定
- ✓ 2020年5月1日、金商法・資金決済法改正により、以下を実施
 - ・ 暗号資産デリバティブ取引が規制対象となったため、暗号資産デリバティブ取引に関する自主規制機関に認定（2020年4月30日）
※暗号資産デリバティブ取引を行っている会員が多数いるため、認定申請があったもの
 - ・ 仮想通貨の呼称が暗号資産に変更されたことから、「日本暗号資産取引業協会」に改称（2020年5月1日）

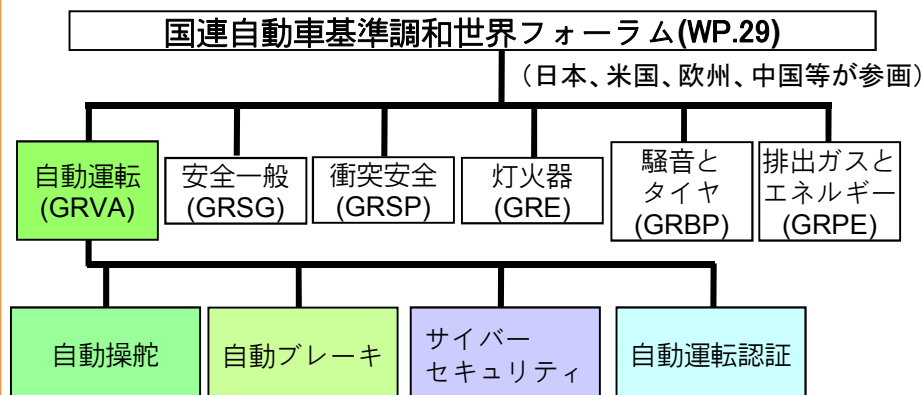
自主規制団体の主な役割

- ✓ 自主規制規則の制定（システムリスク管理、マネロン対策、不公正取引対応、勧誘・広告など）
- ✓ 会員のモニタリング（法令・自主規制規則等の遵守状況調査・検査）
- ✓ 会員の処分（法令等の遵守又は利用者保護を図るための会員への指導・勧告）
- ✓ 外部機関（FINMAC・国民生活センターなど）と連携、苦情対応 など

自動運転に関する課題と我が国の国際的な取組み

- 自動運転の早期実現に向けては産学官が密接に連携した取組みを推進しており、国土交通省としては、自動運転戦略本部（本部長：国土交通大臣）の下、車両の安全確保等に関するルール整備を着実に実施。
- 一方、自動運転に関する課題は世界共通であり、国際的な安全基準の策定には国際的な相互協力が不可欠。
- 国連WP.29（自動車基準調和世界フォーラム）において、我が国は、自動運転に係る基準等について、共同議長又は副議長として議論を主導。
- 引き続き各国と協力し、自動ハンドル、サイバーセキュリティ対策等の自動運転に係る国際基準の策定に向けて検討。

自動運転技術に係る国際基準検討体制及び検討項目



<これまでに策定された基準>

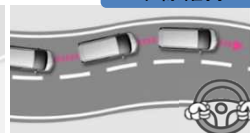
【レベル2】

- ・自動駐車（リモコン駐車）
- ・手を添えた自動ハンドル（車線維持／車線変更）

* 本田技研工業（株）HP

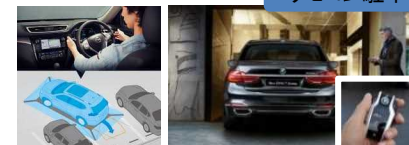


車線維持



* LEXUS HP

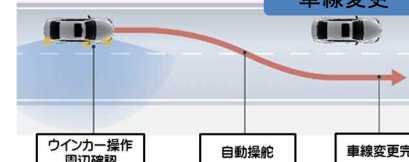
リモコン駐車



* 日産自動車（株）HP

* BMW HP

車線変更



ウインカー操作
周辺確認

自動操舵

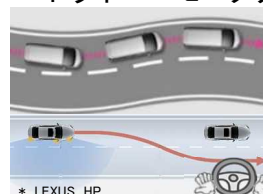
車線変更完了

* LEXUS HP

<検討中の基準>

【レベル3】

- ・自動ハンドル（車線維持／変更）
- ・ドライバーモニタリング



* LEXUS HP



* 日野自動車（株）HP

【全てのレベルに共通】

- ・サイバーセキュリティ



自動運転技術に係る主な会議体	日本の役職
自動運転専門分科会	副議長
自動操舵専門家会議	議長(独と共同)
自動ブレーキ専門家会議	議長(ECと共同)
サイバーセキュリティタスクフォース	議長(英と共同)
自動運転認証専門家会議	議長(蘭と共同)

1. 本行動計画のポイント

- ◆ 重要インフラサービスを、安全かつ持続的に提供できるよう、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らし、迅速な復旧が可能となるよう、経営層の積極的な関与の下、情報セキュリティ対策に関する取組を推進。（機能保証の考え方）
- ◆ また、取組を通じ、オリパラ大会に係る重要なサービスの安全かつ持続的な提供も図る。

2. 重要インフラの情報セキュリティ対策の現状と課題

- ◆ 第3次行動計画に基づく施策群により、自主的な取組が浸透しつつあるが、P D C AのうちC Aに課題。一部で先導的な取組も進展。
- ◆ 機能保証のため、情報系（I T）に限らず、制御系（O T）を含めた情報共有の質・量の改善や、重要インフラサービス障害に備えた対処態勢の整備が必要。
- ◆ 国内外の多様な主体との連携、情報収集・分析に基づく国民への適切な発信の継続・改善が必要。

3. 本行動計画の3つの重点

次の3つを重点として、第3次行動計画の5つの施策群の補強・改善を図る。

① 先導的取組の推進(クラス分け)

- 他分野からの依存度が高く、比較的短時間のサービス障害でも影響が拡大するおそれがある分野（例：電力、通信、金融）において、一部事業者における先導的な取組（I S A C※の設置やリスクマネジメントの確立等）を強化・推進

※所属事業者間で秘密保持契約を締結するなど、より機密性の高い情報の共有等を目的とした組織

- 上記先導的な取組みの、当該重要インフラ分野内の他の事業者等及び他の重要インフラ分野への展開による我が国全体の防護能力の強化

② オリパラ大会も見据えた情報共有体制の強化

- サービス障害の深刻度判断基準の導入に向けた検討
- 連絡形態の多様化（連絡元の匿名化、セプター※事務局・情報セキュリティ関係機関経由）による情報共有の障壁の排除。分野横断的な情報を内閣官房に集約する仕組みの検討
※重要インフラ事業者等の情報共有を担う組織
- ホットライン構築も可能な情報共有システムの整備（自動化、省力化、迅速化、確実化）
- 情報連絡・情報提供の範囲にO T、I o T等を含むことを明確化（I T障害→重要インフラサービス障害）
- 演習の改善、演習成果の浸透による防護能力の維持・向上
- サプライチェーンを含む「面としての防護」に向け範囲の拡大

③ リスクマネジメントを踏まえた対処態勢整備の推進

- 「機能保証に向けたリスクアセスメントガイドライン」の提供及び説明会の実施等によるリスクアセスメントの浸透
- 事業継続計画及び緊急時対応計画（コンティンジェンシープラン）の策定等による重要インフラ事業者等の対処態勢の整備
- 事業者等における内部監査等の取組において、リスクマネジメント及び対処態勢における監査の観点の提供等による「モニタリング及びレビュー」を強化

4. 本行動計画の期間

- 第4次行動計画はオリパラ大会開催までを視野に入れ、大会終了後に見直しを実施。その間であっても、必要に応じて見直す。

高度標的型サイバー攻撃を受けた組織への初動対応支援（経済産業省資料）

- 平成26年7月、IPAに、個々の組織の能力では対処困難な、高度標的型サイバー攻撃を受けた組織に対する初動対応を行う「サイバーレスキュー隊（J-CRAT）」を立ち上げ。
- 最初の標的となり、対応遅延が社会や産業に重大な影響を及ぼすと判断される組織（主として、重要インフラ事業者、業界団体・独法等）に対して、初動対応支援を実施。

【サイバーレスキュー隊の活動】



重要インフラ、
業界団体等



経済社会に被害が拡大するお
それが強く、一組織で対処が困
難な深刻なサイバー攻撃の発生

- ・初動時の緊急処置の助言
- ・被害状況の理解促進
- ・対応体制の早急な立ち上げの支援

IPA 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan



サイバーレスキュー隊

- 一般社団法人 JPCERT/CC（ジェイピーサートコーディネーションセンター）は、サイバー攻撃対処のための国際連携窓口業務を実施。
- 世界100カ国以上のCSIRT（コンピューターセキュリティ事案対処チーム）と連携し、民間企業がサイバー攻撃にあった際に、各国との情報共有や、海外の攻撃元サーバの停止等を海外の窓口と調整。
- 途上国からの攻撃に対応するため、アジア・アフリカ諸国のCSIRT新設や運用も支援
- サイバー攻撃の分析結果や脆弱性情報を共有し、グローバルなサイバー空間のセキュリティ向上に貢献。

＜JPCERT/CCについて＞

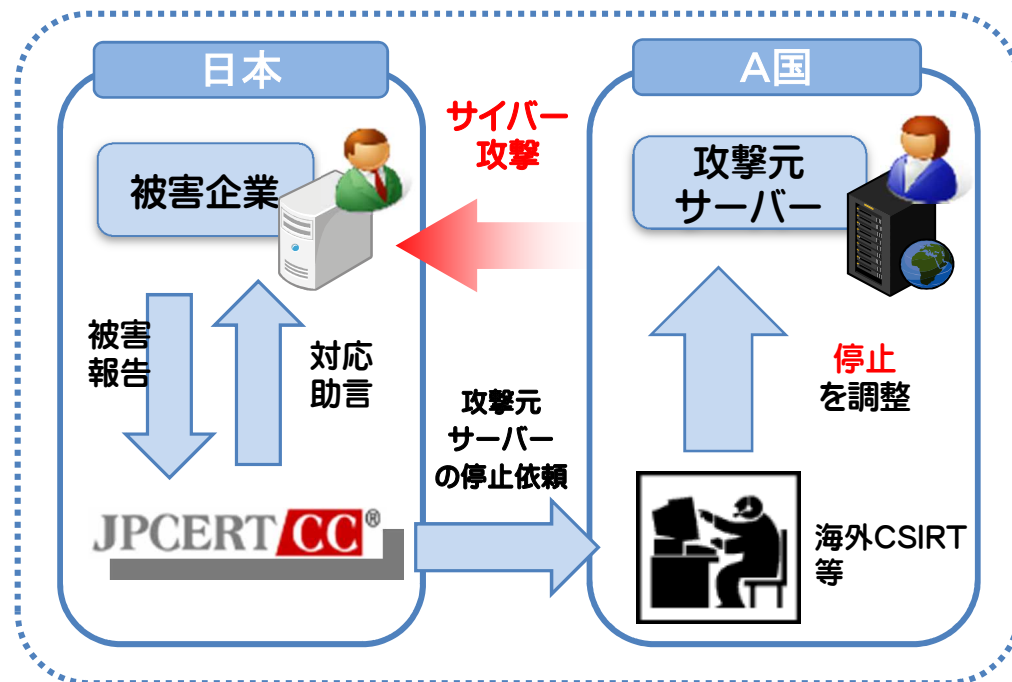
- 1996年に「コンピュータ緊急対応センター」として発足。2003年にJPCERT/CCとして登記。
- 民間の非営利団体として、政府機関や企業からは独立し、中立的組織として活動。

＜職員数＞ 約70名

＜予算＞ 経産省からJPCERT/CCに対して委託を行い、上記取組を実施。

平成27年度：12.0億円
 平成28年度：12.0億円
 平成29年度：12.6億円
 平成30年度：13.0億円

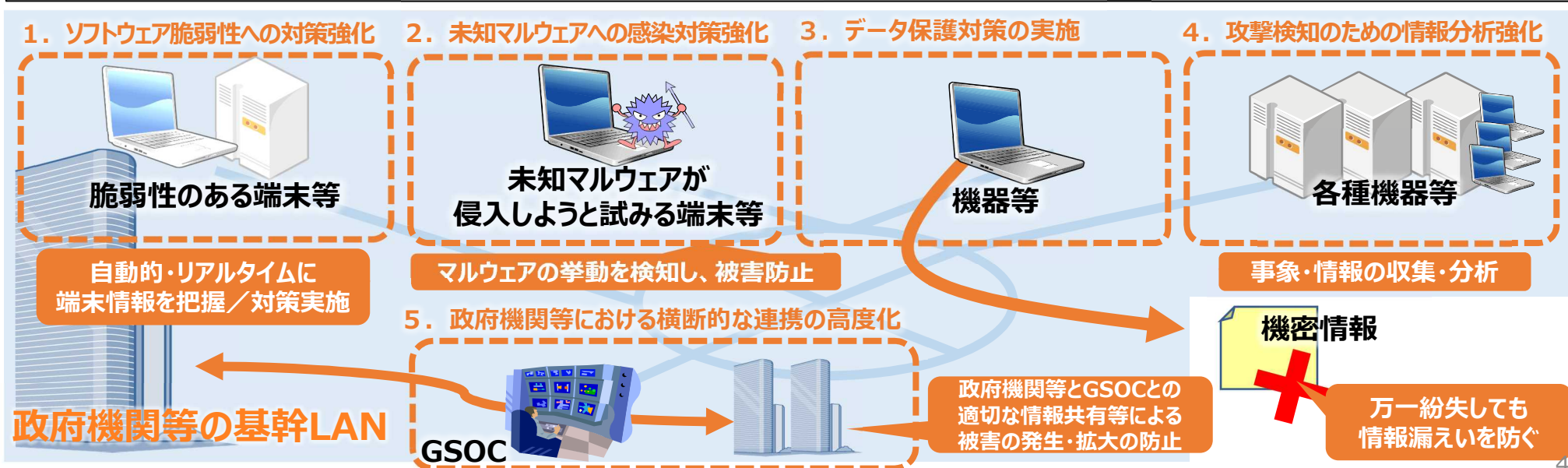
＜国際連携によるサーバの停止等の対応＞



情報システムの状態のリアルタイム管理をはじめとした、セキュリティ対策の強化（NISC資料）

攻撃側優位の状況を改善するため、将来像を見据えたサイバーセキュリティ対策を体系的に構築する

1. **【ソフトウェア脆弱性への対策強化】** これまで直接人手による作業によるものであったが、IT資産管理の自動化により、情報システムの状態をリアルタイムに把握し、迅速な対応が可能となる
2. **【未知マルウェアへの感染対策強化】** これまで被害発生後の対応にならざるを得なかった未知のマルウェアについて、エンドポイント（端末等）における挙動等によって検知し、被害の未然防止及び拡大防止を図る
3. **【データ保護対策の実施】** デジタル著作権管理等の技術を用いて、万一事案が発生した場合であっても情報を漏えいさせない取組を図る
4. **【攻撃検知のための情報分析強化】** 様々な機器で発生する事象や情報を収集し、脅威分析を行うことにより、これまで検知困難とされた攻撃であっても発見する対策について検討を行う
5. **【政府機関等における横断的な連携の高度化】** 政府機関等のセキュリティ強化策の今後の導入状況等を踏まえつつ、政府機関等とGSOCによる効果的かつ効率的な横断的な連携を推進する。



政府情報システムのためのセキュリティ評価制度（ISMAP）の取組状況について（NISC資料）

政府情報システムのためのセキュリティ評価制度（ISMAP）に関する主な背景

サイバーセキュリティ戦略（平成30年7月27日 閣議決定）

4.2.3 政府機関等におけるセキュリティ強化・充実

（２）クラウド化の推進等による効果的なセキュリティ対策

クラウド化の推進に当たっては、安全性評価など、適切なセキュリティ水準が確保された信頼できるクラウドの利用を促進する方策について検討し、対策を進める。

デジタル・ガバメント実行計画（令和元年12月20日 閣議決定）

3.3 行政機関におけるクラウドサービス利用の徹底

（１）クラウド・バイ・デフォルト原則を踏まえた政府情報システムの整備

各府省は、引き続き、クラウドサービス利用方針に基づき、政府情報システムを整備する際には、対象となる行政サービス・業務、取り扱う情報等を明確化した上で、メリット、整備の規模、費用等を基に、各種クラウドサービスの利用を原則として検討する。

（２）クラウドサービスの安全性評価

安全性評価基準及び安全性評価の監査の仕組みを活用して安全性が評価されたクラウドサービスの利用を開始できるよう、引き続き、環境整備等について検討を進める。

政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて（令和2年1月30日 サイバーセキュリティ戦略本部決定）

サイバーセキュリティ戦略本部第23回会合において、①本制度の基本的な枠組み、②各政府機関等における本制度の利用の考え方、③本制度の所管と運用体制を決定。あわせて、事務局は、本制度の運用状況について、サイバーセキュリティ戦略本部に報告を行うこととされた。

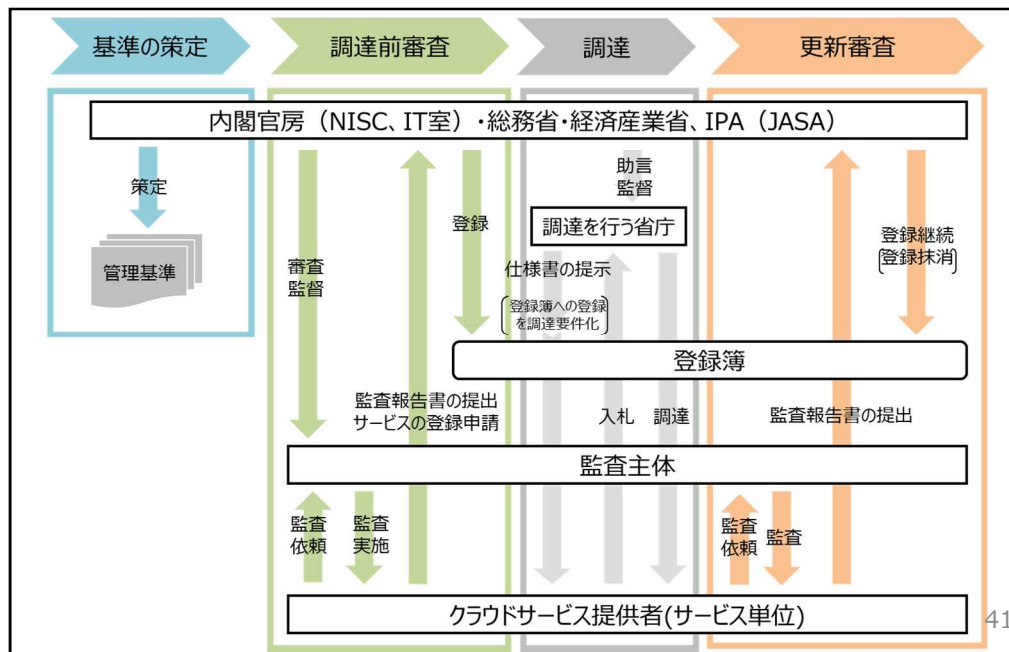
取組状況（令和2年7月現在）

○「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」（令和2年1月30日 サイバーセキュリティ戦略本部決定。以下「基本的枠組み」という。）において、本制度の最高意思決定機関として設置するとしていた、有識者と所管省庁（内閣官房（内閣サイバーセキュリティセンター・情報通信技術（IT）総合戦略室）・総務省・経済産業省）を構成員とした制度運営委員会（以下「ISMAP運営委員会」という。）を令和2年5月に設置するとともに、第1回ISMAP運営委員会を開催し、同委員会において制度に関する各種規程等が決定され、本制度の運用を開始。

○ 基本的枠組みに基づき、サイバーセキュリティ対策推進会議、各府省情報化統括責任者（CIO）連絡会議において詳細を定めるとしていた、原則利用や暫定措置の在り方のほか、各政府機関等とISMAP運営委員会との連携や令和3年度以降の制度運用に必要な経費の分担の考え方について、令和2年6月に開催された両会議の合同会議において決定。

○ 2020年度（令和2年度）内に、統一的なセキュリティ要求基準や監査の仕組みを活用してセキュリティ対策が評価されたクラウドサービスリストの公表を行うべく、監査機関の審査・登録、クラウドサービス事業者への監査・審査を進めていく。

セキュリティ評価制度の基本的流れ



IT調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ等について（NISC資料）

■ サプライチェーン・リスクとは

- 情報通信機器等の開発や製造過程において、情報の窃取・破壊や、情報システムの停止等の悪意のある機能が組み込まれる懸念。
- さらに、納入後においても、情報システムの特徴として、事後的な運用・保守作業により、製造業者等が修正プログラムを適用する等、調達機関が意図しない、不正な変更が行われる可能性。



■ サプライチェーン・リスク対策の重要性

- 「サイバーセキュリティ戦略」において、サプライチェーン・リスク対策の重要性について言及。
- 「政府統一基準群」において、サプライチェーン・リスク対策に係る考え方を記載。

～ 政府機関等の対策基準策定のためのガイドラインの解説（遵守事項5.1.2(1)(a)“「不正な変更が加えられない」について”に係る解説）から抜粋 ～
 「開発・製造過程において悪意ある機能が組み込まれる懸念が払拭できない機器等、及びサプライチェーン・リスクに係る懸念が払拭できない企業の機器等を調達しないことが求められる。」

■ 「サプライチェーン・リスク対策」のより具体的な方策として全省庁による「申合せ」を決定。

（平成30年12月10日 サイバーセキュリティ対策推進会議（第16回）各府省情報化統括責任者連絡会議（第81回）合同会議）

1. 適用対象：重要性の観点から5類型を提示。
2. 適用時期：平成31年度予算に基づき平成31年4月1日以降に調達手続（公告等）が開始されるもの。
3. 対象機関：国の行政機関、独立行政法人、サイバーセキュリティ基本法に定める指定法人
4. 調達手続の流れ：（令和2年度追加）
 - 「総合評価落札方式」や「企画競争」等を用い、RFIやRFPといった事前の情報取得や、審査の過程において、必要な情報を入手し評価することにより、サプライチェーン・リスク対策を実施。
 - 必要に応じて、情報通信技術（IT）総合戦略室及び内閣サイバーセキュリティセンターから、講ずべき必要な措置について助言を実施。

- ① 国家安全保障及び治安関係の業務を行うシステム
- ② 機密性の高い情報を取り扱うシステム並びに情報の漏洩及び情報の改ざんによる社会的・経済的混乱を招くおそれのある情報を取り扱うシステム
- ③ 番号制度関係の業務を行うシステム等、個人情報を含めて大量に取り扱う業務を行うシステム
- ④ 機能停止等の場合、各省庁における業務遂行に著しい影響を及ぼす基幹業務システム、LAN等の基盤システム
- ⑤ 運営経費が極めて大きいシステム

安全な政府調達のためのさらなる推進【情報セキュリティの第三者認証】

■ 情報セキュリティ評価及び認証制度(JISEC)とは

- セキュリティ評価の国際標準ISO/IEC 15408（[Common Criteria](#)）に基づき、第三者がIT製品のセキュリティ機能の妥当性・正確性を評価・認証する制度。[政府の一般市販製品調達におけるセキュリティの確保を目的とする。](#)

■ 国際標準と国際連携

- 認証結果の国際的な相互承認を実現。現在31カ国が加盟。
- 加盟各国で共通の政府調達要件（プロテクションプロファイル）を策定。

■ 日本における活用

- 「政府機関等の情報セキュリティのための統一基準」における調達セキュリティ要件を満たすため、省庁や自治体が認証製品を調達。
- 省庁がCCに基づき製品の調達セキュリティ要件を作成し調達を実施。



申請者	PPの名称	認証日
独立行政法人情報処理推進機構	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015	H29.5.29
外務省領事局旅券課	旅券冊子用ICのためのプロテクションプロファイル - SAC対応（BAC+PACE）及び能動認証対応 - 第1.00版	H28.3.22
外務省領事局旅券課	旅券冊子用ICのためのプロテクションプロファイル - SAC対応（PACE）及び能動認証対応 - 第1.00版	H28.3.22
地方公共団体情報システム機構	個人番号カードプロテクションプロファイル 第1.00版	H26.5.15

■ 2020年度の取組み

- 政府調達製品の多様化に対応し、IoT機器を含む特定用途機器（ネットワークカメラ、入退管理システム等）のセキュリティ要件を調査。
- ネットワークカメラの調達要件（プロテクションプロファイル）を策定し、試行評価を実施。

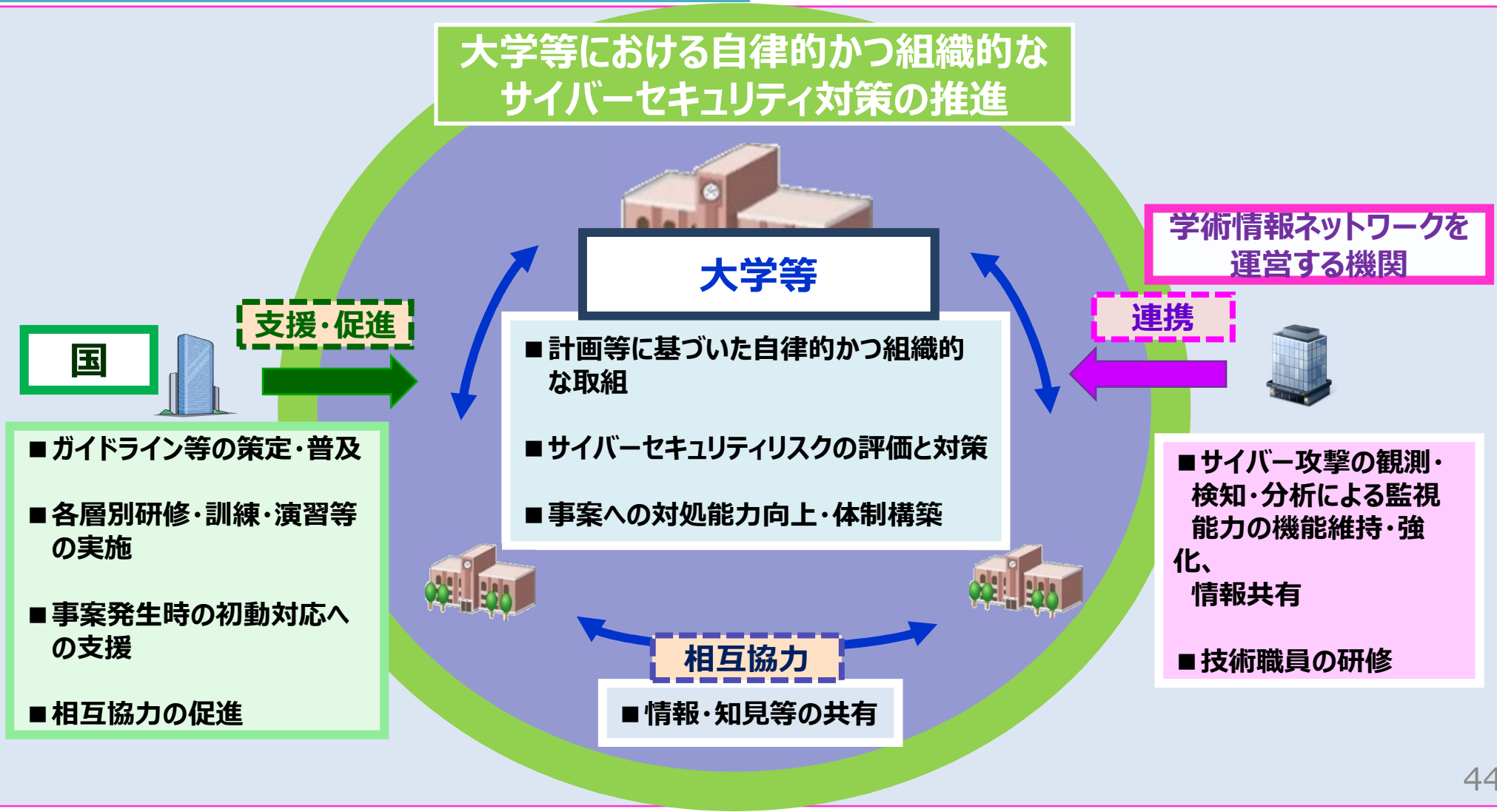


大学等の多様性を踏まえた対策の推進・大学等の連携協力による取組の推進（文部科学省資料）

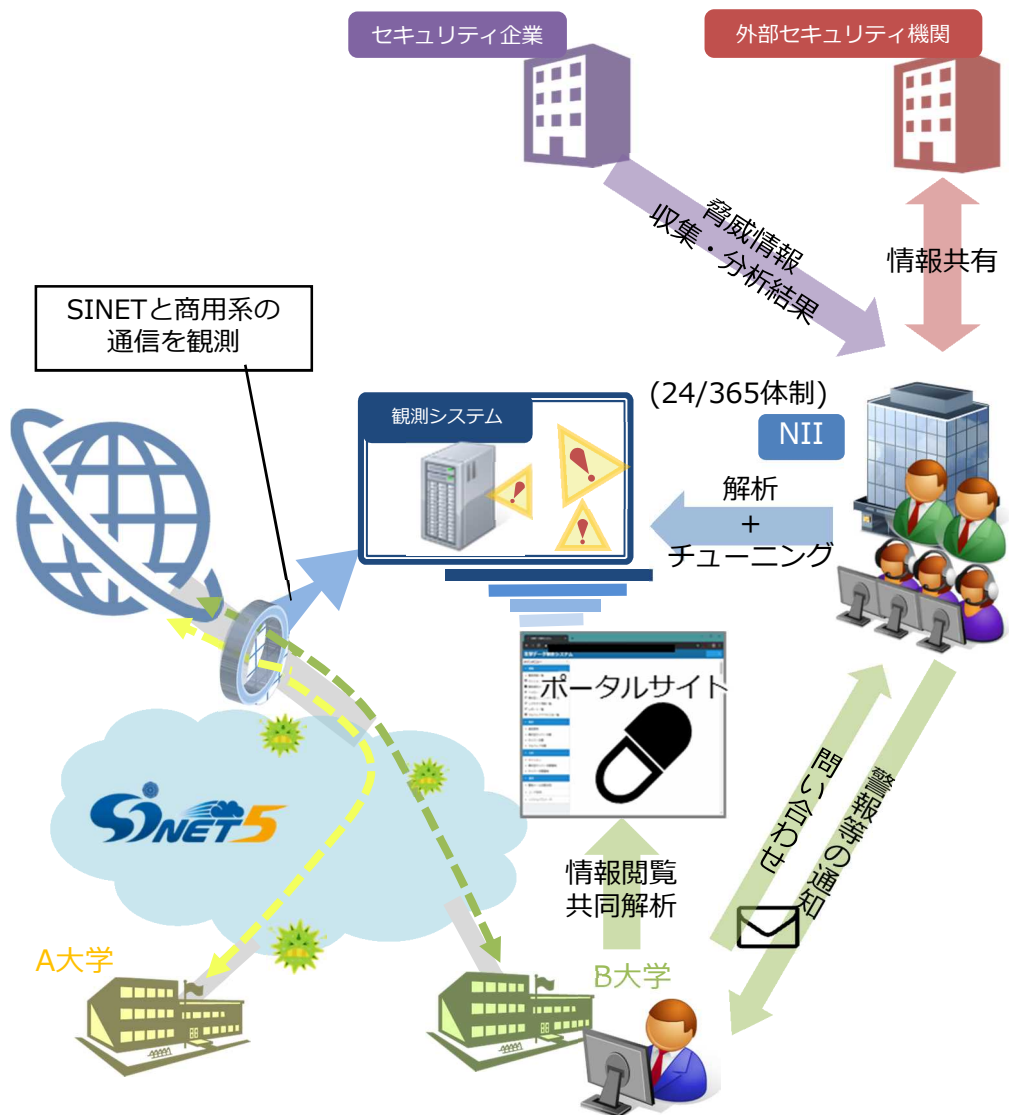
1. 大学等における自律的かつ組織的なサイバーセキュリティ対策の推進
2. 大学等の連携協力によるサイバー攻撃への対応体制の構築や情報共有等

大学等における安全・安心な教育・研究環境の確保

イメージ図



大学間連携に基づく情報セキュリティ体制の基盤構築（NII-SOCS）（NII資料）



– 3種類の観測システム

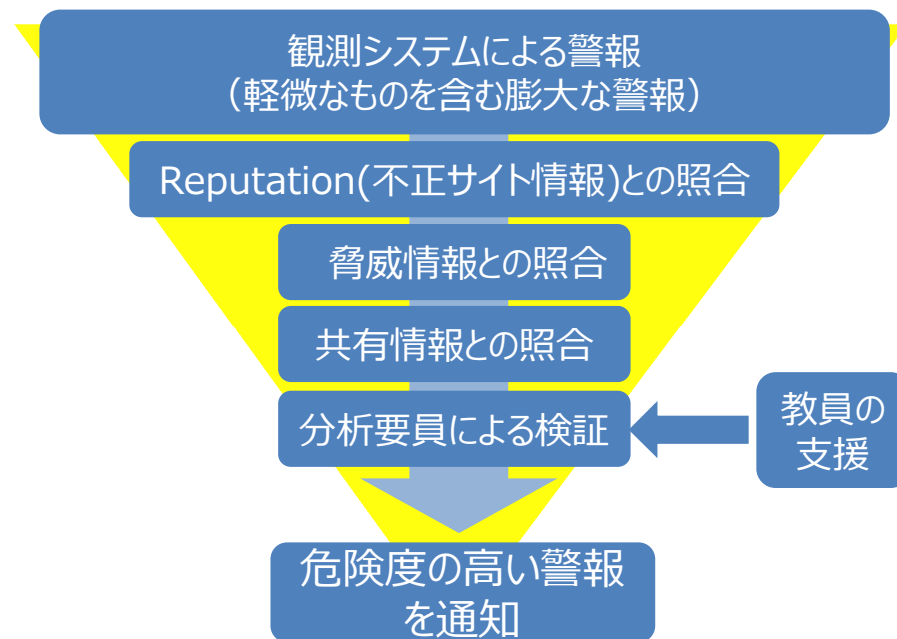
- Sandbox搭載侵入検知
- シグネチャベース侵入検知
- Reputation情報(不正サイト情報)

– 脅威情報サービスの利用

- サイバー攻撃の背景や危険度の把握

– 簡易解析システム + Webポータル

- 膨大な警報に緊急度・危険度の割付
- 危険度の高い警報のみ大学へ通知



– 外部セキュリティ機関との情報共有

サイバーセキュリティ基本法に基づく「サイバーセキュリティ戦略」に基づき、大会の運営に大きな影響を及ぼし得る重要サービス事業者等を対象とした**リスクマネジメントの促進**や、関係府省庁、大会組織委員会、東京都等を含めた関係組織と、サイバーセキュリティに係る脅威・事案情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターの運用等、**対処態勢の整備**を推進中。これらの仕組み、運用経験及びノウハウは、東京大会のみならず、我が国の持続的なサイバーセキュリティの強化のために活用。

さらに、新型コロナウイルスの感染拡大及び大会の延期に伴い生じる環境変化や新たな事象・リスク等を踏まえ、**必要な見直しを実施**。

リスクマネジメントの促進

○ 取組状況

手順書を作成するとともに、東京大会において開催・運営に影響を与える重要サービス事業者等を選定し、リスクの低減と最新のリスクへの対応のため、2016年度から**リスクアセスメント**の実施を依頼。実施結果について横断的に分析し各事業者等にフィードバック。2019年9月から12月末にかけて第5回目の取組を実施。

また、競技会場に提供されるサービスの重要度に応じて対象事業者等を選定の上、サイバーセキュリティ対策の実施状況をNISCが検証する**横断的リスク評価**を2020年3月末までに計3回実施。2019年度においては、第2回目及び第3回目を実施。

○ 今後の取組

リスクアセスメントの取組については、2021年3月末までに第6回目の取組を実施し、引き続き、重要サービス事業者等のリスクアセスメントにおいて、情報資産、リスクの洗い出しの網羅性及び要対応リスクに対する対策の網羅的な検討を促進するとともに、**環境変化を踏まえたリスクの見直し**、残存リスクが顕在化した場合の対応体制の強化を促進。

横断的リスク評価の取組については、第2回目及び第3回目の取組の対象であった重要サービス事業者等（会場（レガシー部分）を含む。）及び東京大会組織委員会に対するフォローアップを実施するとともに、**病院分野及び会場の変更がある場合には新規会場を対象として検証を実施**。

対処態勢の整備（サイバーセキュリティ対処調整センターの運用等）

○ 取組状況

情報共有システムを構築し、2019年4月に設置した**サイバーセキュリティ対処調整センター**から**情報共有システム**を使用した恒常的な関係組織・機関への迅速な情報提供を実施するとともに、情報共有及びインシデント発生時の対処に係る**訓練・演習**を重ねている。情報セキュリティ関係機関等の協力により観測活動を実施するとともに、サイバー脅威情報の提供について5社から協力を受けている。

また、2019年度は、大会までの大規模イベント（G20大阪サミット等関係閣僚会合、ラグビーワールドカップ等）において運用を実施し多くの教訓を得た。その結果を踏まえ、情報共有及びインシデント発生時の態勢について関係府省庁、大会組織委員会、東京都等と協議して決定した**対応手順等**について改善を実施した。

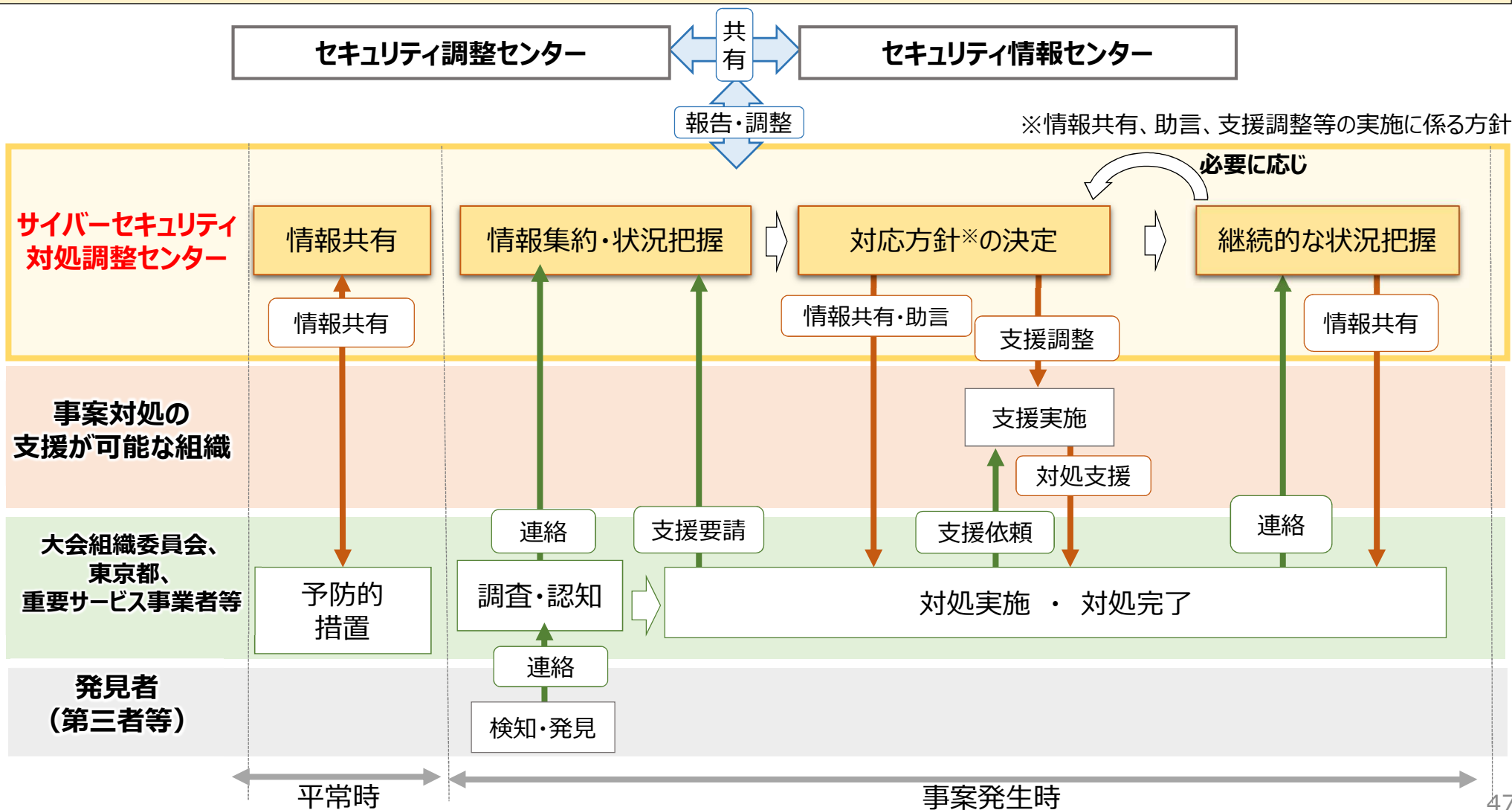
○ 今後の取組

新型コロナウイルスの感染拡大に伴う情勢の変化（テレワークの普及・大会運営の変更等）及び**大会が1年延期となったことで新たに発生・判明する事象等**を踏まえた関係組織・機関への**情報提供**の継続と**訓練・演習**の積み重ねにより、大会関係組織間の緊密な連絡調整を図るための態勢を強化するとともにインシデント対処能力を向上する。

これにより、大会に向けて万全の対処態勢を目指す。

サイバーセキュリティ対処調整センターについて（NISC資料）

- 東京2020大会のサイバーセキュリティに係る脅威・インシデント情報を収集し、これら情報を大会組織委員会を始めとした関係機関等に提供、必要があるときには関係機関等のインシデント対処に対する**対処支援調整**を実施



●リスクアセスメントの取組

サイバー攻撃等による東京2020大会の準備・運営への影響の未然防止や軽減等のため、大会を支える周辺サービスを提供する事業者等によるリスクマネジメントの強化を通じ、想定されるサイバーセキュリティ上のリスクへの対策を促進。

第6回の取組では、大会延期や新型コロナウイルスの感染拡大に伴う環境変化を踏まえたリスクの見直しに加え、要対応リスクに対する対策の網羅的な検討及び残留リスクが顕在化した場合の対応体制の強化を促進していく。

- リスクマネジメントの促進のため、サイバーセキュリティリスクを特定・分析・評価する手順をNISCで作成

- 大会の準備・運営に影響に与える重要サービス分野から、重要サービス事業者等を関連する所管省庁と調整の上で選定

重要サービス分野 + 会場（競技会場及び非競技会場）

通信、放送、金融、航空、鉄道、電力、ガス、上水道、物流、クレジット、行政サービス（地方公共団体）、下水道、空港、道路・海上・航空交通規制、緊急通報、気象・災害情報、出入国管理、高速道路、熱供給、バス、警備、旅行、病院、会場

2016年度	2017年度	2018年度	2019年度	2020年度
第1回 対象：東京23区 エリア 19分野	第2回 東京圏 (1都3県) 20分野	第3回 全競技会場周辺 (1都1道7県) 20分野+会場	第4回 全競技会場周辺 (1都1道8県) 22分野+会場	第5回 全競技会場周辺 (1都1道8県) 23分野+会場

- NISCが想定する『事業・重要サービス・経営資源（情報資産）』のモデルケース（重要サービス分野ごと）』『業務の阻害につながる事象の結果、結果を生じ得る事象（脅威）及びリスク源』を作成、各事業者等へ経営資源、リスク源等の洗い出しの漏れの可能性をフィードバックすることによって、より網羅的なリスクアセスメントの実施を促進

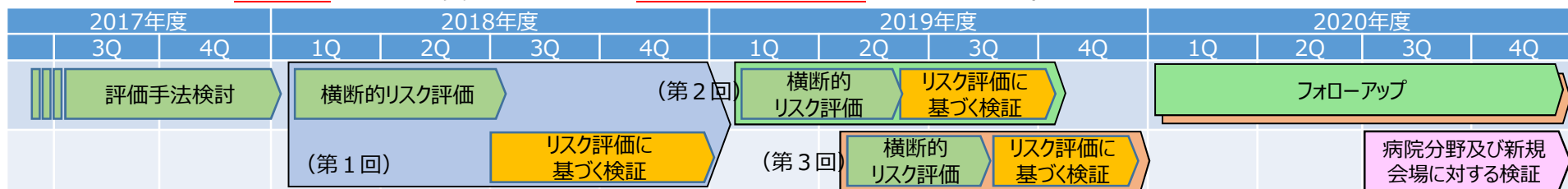
- サイバーセキュリティ対策の運用状況について、NISCからフィードバックを実施し、必要に応じて助言を実施

●横断的リスク評価の取組

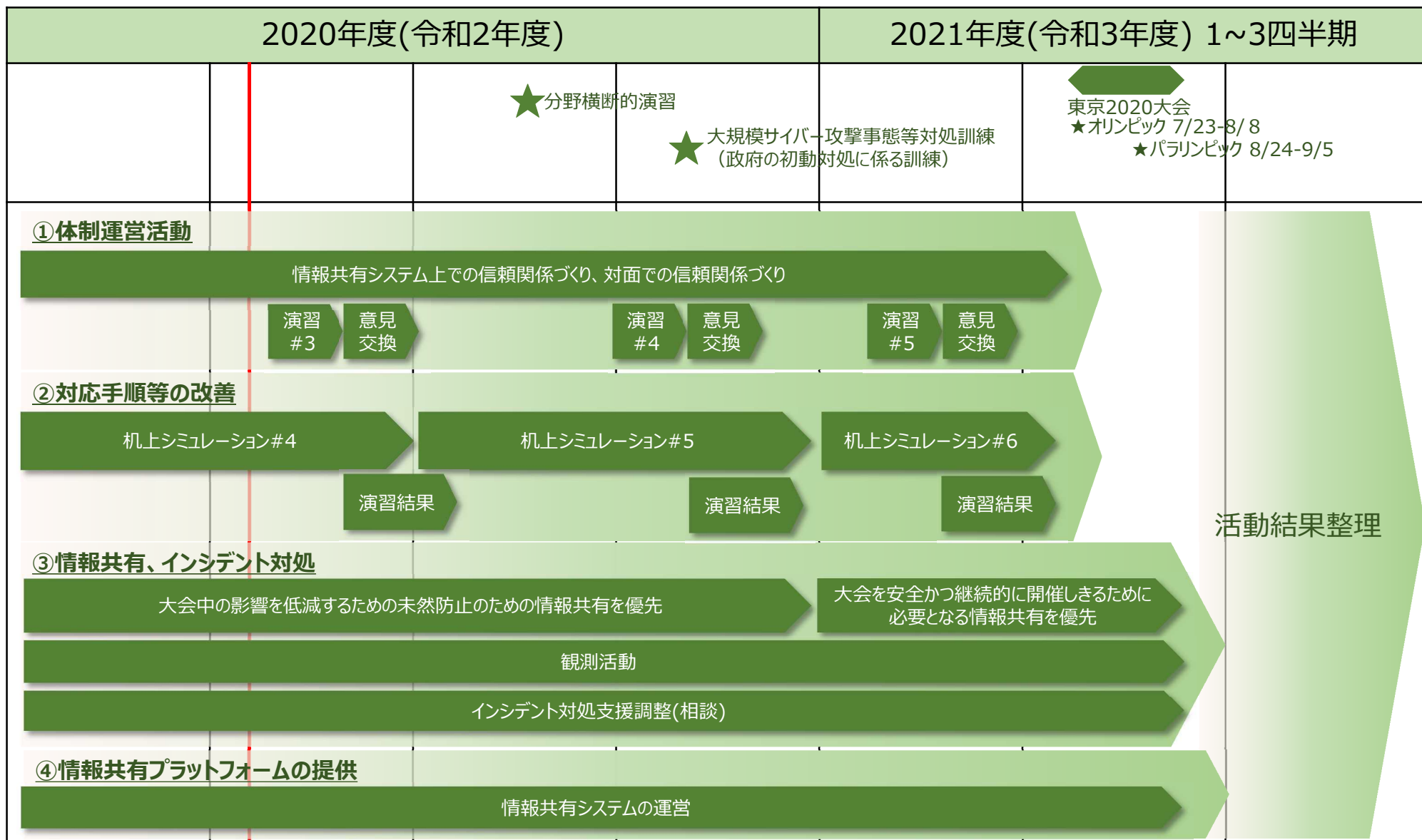
重要サービス事業者等において想定されるサイバーセキュリティリスクに基づき、サイバーセキュリティ対策の実施状況をNISCが検証する。

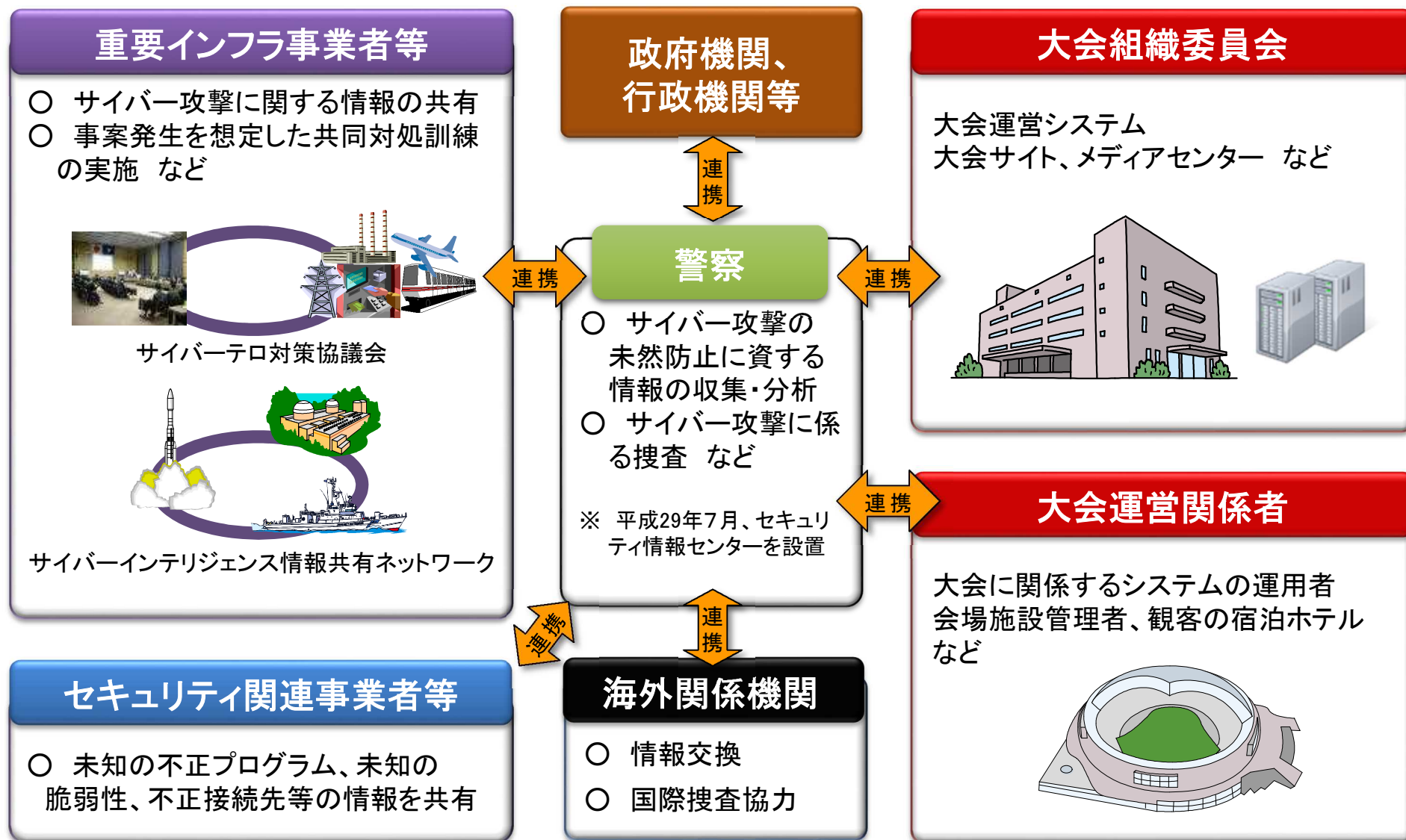
これにより、大会の成功にとって重要な機能が継続して提供されることを確認するとともに、不備があった場合は、重要サービス事業者等へフィードバックすることにより、当該重要な機能が継続して提供されることの確かさを向上させる。

- 大会に関わるリスクが顕在化するシナリオをリスクシナリオとして策定・活用し、重要サービス事業者等が設定したルールの妥当性や実効性について検証
- 第1回の取組においては、電力、通信、水道、鉄道、放送等 5者程度を対象に実地検証。全重要サービス分野から20者程度を対象に書面検証
- 第2回及び第3回の取組においては、重要サービス事業者等（会場（レガシー部分）を含む。）を対象に検証（実地又は書面）
なお、会場のオーバーレイ部分の対策の整備状況及び監督状況については、組織委を対象に実地検証
- 2020年度においては、病院分野及び会場の変更がある場合には新規会場を対象に検証（実地又は書面）



2021年度の東京2020大会に向けて、「体制運営活動」「対応手順等の改善」「情報共有・インシデント対処」「情報共有プラットフォームの提供」を継続及び改善し、大会の対処態勢を万全なものとしていく。





2020年東京オリンピック競技大会・東京パラリンピック競技大会に向けた実践的サイバー演習(サイバーコロッセオ)(総務省資料)

- 近年さらに高度化・多様化するサイバー攻撃に備え、東京2020大会の適切な運営を確保することを目的として、**大会関連組織のセキュリティ担当者等を対象とした、高度な攻撃に対処可能な人材の育成**を行う実践的サイバー演習「**サイバーコロッセオ**」を平成30年2月から本格的に実施。
- **実機演習を伴うコロッセオ演習**を補完する形で、演習時以外にも学習可能な学習コンテンツを提供するとともに、平成30年度からは**講義演習形式**によりセキュリティ関係の知識や技能を学ぶ**コロッセオカレッジ**を開設。
 ※コロッセオ演習・・・平成29年度：年間2回・74名受講／平成30年度：年間6回・137名受講／令和元年度：年間15回・193名受講
 ※コロッセオカレッジ・・・平成30年度：年間16回・347名受講／令和元年度：年間59回・992名受講
- 令和2年度については、大会実施延期やCOVID-19の状況を鑑み、組織委と連携しながら計画を策定中。

サイバーコロッセオ概要



コロッセオ演習

実機演習を伴ったの演習
(攻防型演習を含む)



- 大規模演習環境を用いて、東京2020大会の公式サイト、大会運営システム等ネットワーク環境を再現した、演習舞台（仮想ネットワーク環境）を構築。
- 東京2020大会時に想定されるサイバー攻撃を擬似的に発生させることができるようにし、本格的な攻防型演習等を繰り返し実施。

「攻防型演習」とは・・・

受講者が複数チームに分かれ、自組織のネットワークの守備と他チームのネットワークへの攻撃を両方体験することで、攻撃者側の視点をも踏まえたハイレベルな防御手法の検証及び訓練を行う演習

学習コンテンツ

コロッセオ演習当日
以外でも学習可能な
コンテンツを提供

コロッセオカレッジ

講義演習形式により
セキュリティ関係の
知識や技能を学習



リスク評価及び制御システムのセキュリティリスク分析ガイドについて（経済産業省資料）

リスク評価の徹底について

- サイバーセキュリティ戦略本部では、2018年度までに重要インフラ分野全てでリスク評価を実施する方針。
※東京2020大会に関する重要サービス事業者を中心に実施。
- 経済産業省は、2016年度、他省庁所管分野も含む重要インフラ4分野、2017年度、2分野で実施、2018年度は、1分野で実施。

制御システムのセキュリティリスク分析ガイドについて

- 平成29年10月にIPAにおいて、制御システムのセキュリティリスク分析のガイドを策定・公表。
- システムやサービスのセキュリティの実態とリスクを把握するリスク分析について2通りの手法を解説。

制御システムのセキュリティリスク分析ガイド

【ガイド本編】



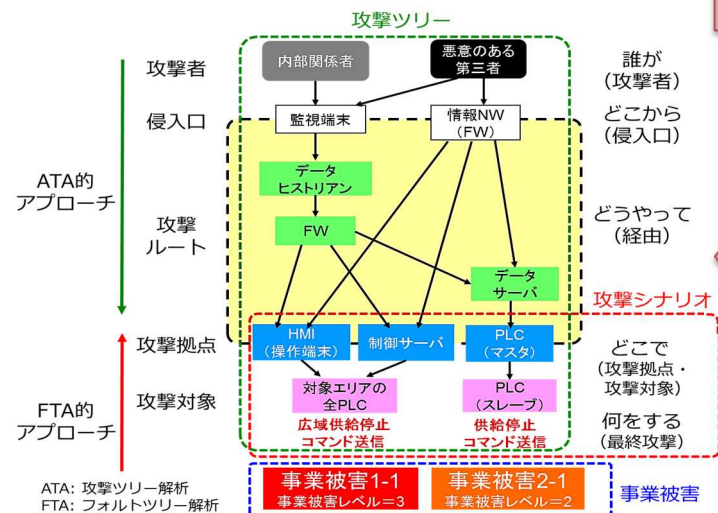
【別冊】



- リスク分析の全体像の理解向上と取組促進
- リスク分析を具体的に実施するための手順や手引きの提示

詳細リスク分析の手法

- 資産ベースのリスク分析
- 事業被害ベースのリスク分析**

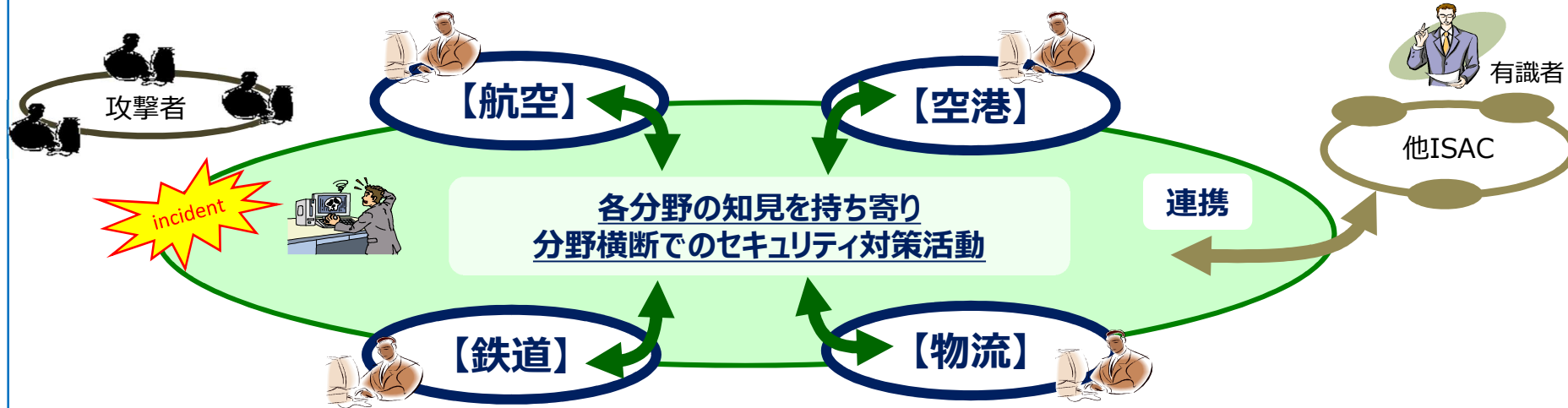


【事業被害、攻撃シナリオ、攻撃ツリーの関係】

所管する重要インフラ事業者（航空、空港、鉄道、物流）が情報の共有・分析や対策を連携して行う体制「交通ISAC」^(注)の2020年度の創設に向けた検討を支援する

(注) Information Sharing and Analysis Centerの略。

交通ISACのイメージ



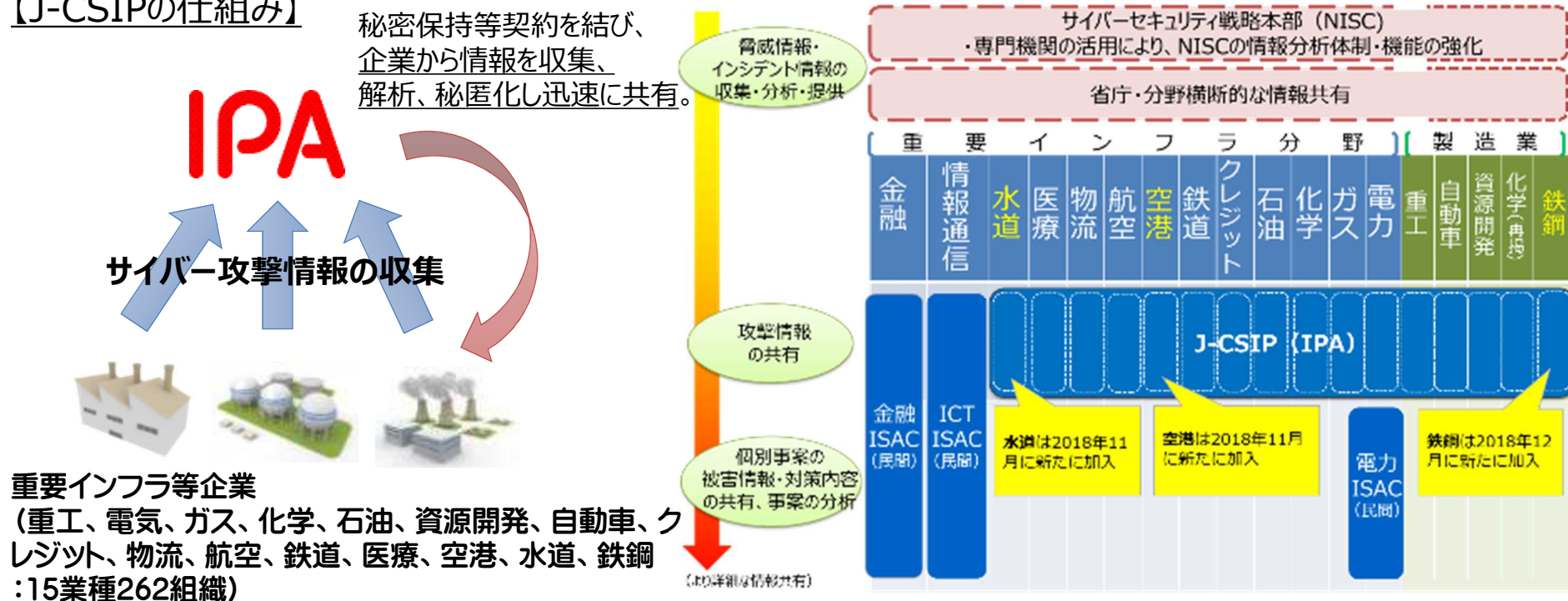
ISACの本格運用までのロードマップ

	2017年度	2018年度	2019年度	2020年度
ISACの創設に係る 検討会	検討会の立上げと運営	ISACの組織・体制等の検討 ISAC活動の検証		
ISACの 活動	検討開始	仮運用開始		本格運用
		WG活動及び情報共有活動		

インシデント情報の収集・共有によるサイバーセキュリティ対策の強化（経済産業省資料）

- IPAは、重要インフラ事業者に対する**サイバー攻撃情報共有体制（J-CSIP（ジェイシップ）：Initiative for Cyber Security Information sharing Partnership of Japan、15業種、262組織が参加）**を構築。
- 公的機関としての信頼性を基に、秘密保持等契約を結び、企業から情報を収集、解析、秘匿化し、迅速に共有することにより被害拡大を防止。
- IPAは、分野ごとの情報共有体制を強化（J-CSIPの対象拡大）していく方針。

【J-CSIPの仕組み】



概要

- ・サイバーセキュリティ基本法の一部を改正する法律に基づき、平成31年4月にサイバーセキュリティ協議会が組織され、同年5月下旬から情報共有活動が開始されている。
- ・本協議会は、国の行政機関、重要社会基盤事業者、サイバー関連事業者等、官民の多様な主体が相互に連携し、より早期の段階で、サイバーセキュリティの確保に資する情報を迅速に共有することにより、サイバー攻撃による被害を予防し、また、被害の拡大を防ぐことなどを目的としている。

サイバーセキュリティ協議会

事務局（NISC・政令指定法人JPCERT/CC）

✓積極的な情報提供に能力と意欲を有する者を**タスクフォース**としてグループ化タスクフォースにおいて作出された**対策情報等を迅速に共有**

国の行政機関

対策実施

地方公共団体

対策実施

重要インフラ事業者

対策実施

サイバー関連事業者
(セキュリティ事業者・システム関連事業者等)

対策実施

教育研究機関

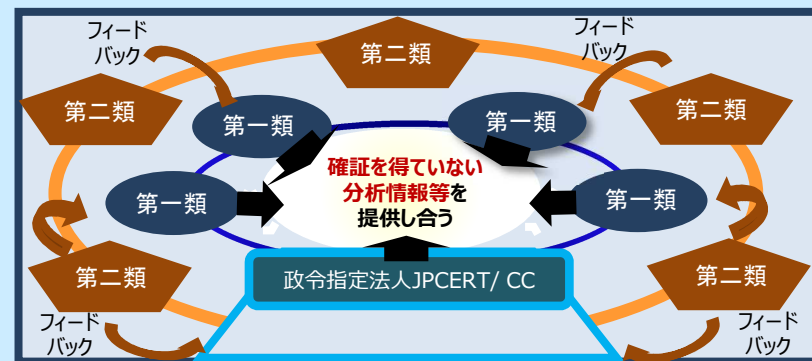
対策実施

サイバーセキュリティの確保の促進

国民の安心・安全の確保、経済社会の活力向上等に寄与

タスクフォース（第一類構成員・第二類構成員）

- ✓未確定の情報を相互にフィードバックを行い、速やかに対策情報等を作成
- ✓活動の中核となる第一類構成員は、主に専門機関・セキュリティベンダ等から構成
- ✓第二類構成員は第一類構成員に対して主にフィードバックを積極的に行う



協議会の取組状況

- 平成31年
 - 4月1日：サイバーセキュリティ協議会を組織（平成30年12月改正サイバーセキュリティ基本法施行）
- 令和元年
 - 5月17日：第一期の構成員を決定（全91者）
 - 5月下旬：協議会における情報共有活動を開始
 - 協議会の特性を活かした迅速な情報共有を実施するなど、**一定の成果**が出始めている。
 - 10月24日：第二期の構成員を決定→第一期構成員を含め全155者
- 令和2年
 - 3月10日：第三期構成員の入会申込受付開始（3月10日～27日まで）
 - 6月5日：第三期の構成員を決定→第一期及び第二期構成員を含め**全225者**
 - （今後の予定）
 - 令和2年内：第四期構成員の入会申込受付開始（予定）
 - ※具体的な時期については、新型コロナウイルスの収束動向等を踏まえ、決定する予定

都道府県ごとに設置したサイバーテロ対策協議会の枠組み等を通じて個別訪問、共同対処訓練等を実施

【重要インフラ】

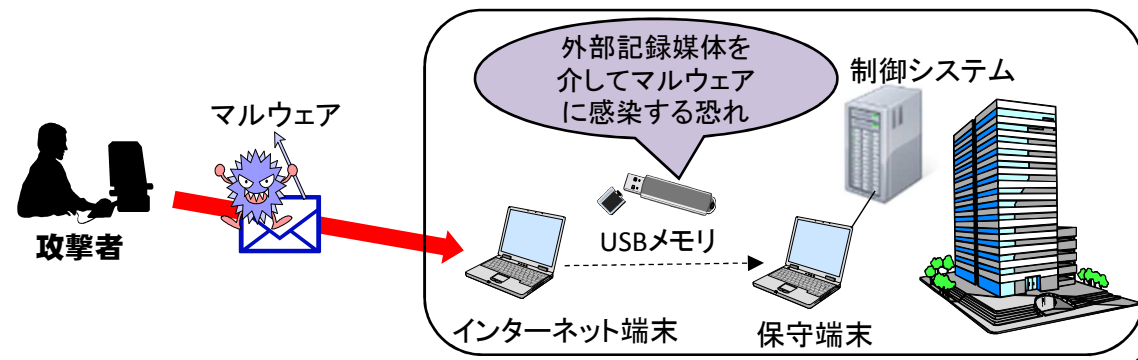


情報通信、金融、航空、空港、鉄道、電力、ガス、
政府・行政サービス、医療、水道、物流、化学、
クレジット、石油

個別訪問

- 警察職員が重要インフラ事業者等へ個別訪問し、最新の情勢やセキュリティ対策の実施状況等について情報共有

【例】マルウェア感染の手口



共同対処訓練

- 警察と重要インフラ事業者等が共同でサイバー攻撃の発生を想定した共同対処訓練を実施

【例】平成30年10月、警察庁及び警視庁では、大会組織委員会、重要インフラ事業者等と、東京2020大会の開催期間中におけるサイバー攻撃の発生を想定した訓練を実施。



「国際社会の平和・安定及び我が国の安全保障への寄与」に係る 取組状況について（NISC資料）

■ サイバーセキュリティ戦略（2018年7月27日 閣議決定）

- 政策目的：自由、公正かつ安全なサイバー空間を創出・発展させ、もって①経済社会の活力の向上及び持続的発展、②国民が安全で安心して暮らせる社会の実現、③国際社会の平和・安定及び我が国の安全保障に寄与すること
- 国際社会の平和・安定及び我が国の安全保障への寄与を達成するための施策：①自由、公正かつ安全なサイバー空間の堅持、②我が国の防御力・抑止力・状況把握力の強化、③国際協力・連携によって、達成していくことを宣言

■ サイバーセキュリティ分野における開発途上国に対する能力構築支援（基本方針）（2016年10月 関係省庁合意）

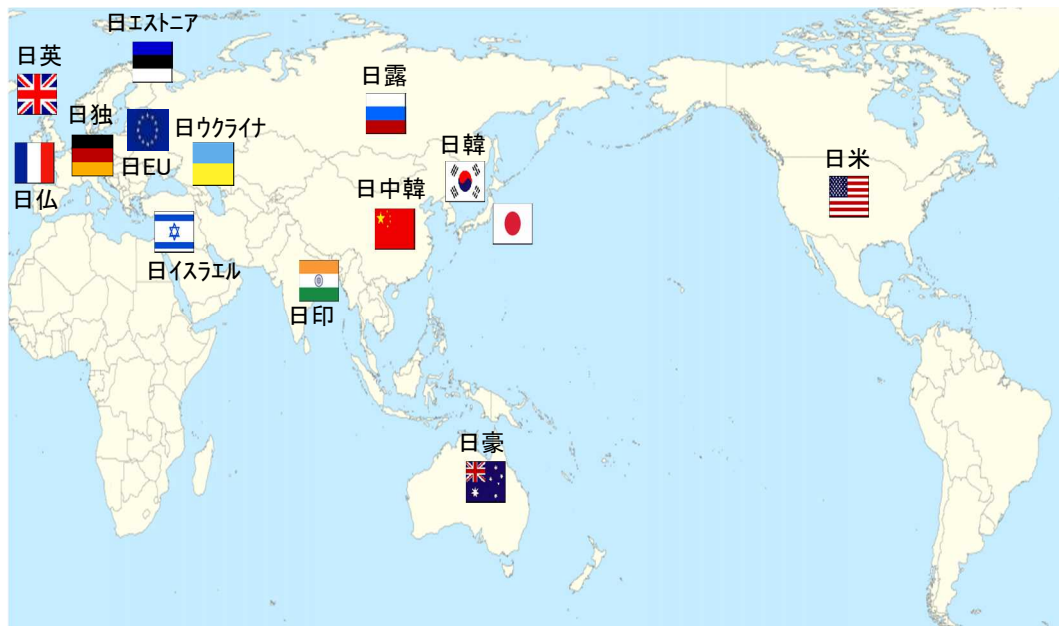
- ①インシデント・レスポンス等の能力の向上支援、②サイバー犯罪対策支援、③サイバー空間の利用に関する国際的ルール作り及び信頼醸成措置に関する理解・認識の共有の分野で、内閣官房を中心に、関係省庁間の緊密な連携の下、様々な政策手段を活用し、サイバーセキュリティ分野における開発途上国に対する能力構築支援を積極的に実施

■ 取組実績（2020年3月現在）

- 首脳・閣僚のハイレベル協議や国連政府専門家会合、G7、GCSC、IGF等各種国際会議への参加、法執行機関間の連携強化により、サイバー空間における法の支配の推進、自由、公正かつ安全なサイバー空間の堅持に積極的に寄与。2019年に第6会期GGEにおいては、我が国から専門家委員を参画させ、国連におけるサイバーセキュリティに関する議論に貢献。
- 二国間協議（2020年3月現在13か国・地域との間でサイバー協議等を実施）や多国間会議を通じ、我が国のサイバーセキュリティ関係施策や考え方等の積極的な発信、連携の具体化や信頼醸成を推進。2017年に立ち上げられた「サイバーセキュリティに関するARF会期間会合」は2020年1月に第5回目を開催。
- National CERTのコミュニティ（Meridian、IWWN、日ASEANサイバーセキュリティ政策会議、FIRST等）への参加を通じ、ベストプラクティスの共有や平時からの脅威情報共有などの活動を促進。特に事故対等にかかる国際連携の強化に向け、ASEAN諸国とのサイバー演習及び机上演習を継続的に実施したほか、有志国を我が国の分野横断的演習に招へいしてワークショップを開催する等連携体制の強化を実施。
- NISC及び関係省庁で主にASEANを対象とした能力構築支援を実施。サイバーセキュリティ政策能力向上等をテーマとした短期研修コースを提供したほか、2018年にタイに設立した日ASEANサイバーセキュリティ能力構築センター（AJCCBC）においてサイバー防御演習等を実施。また、産業サイバーセキュリティセンター（ICSCoE）が東京で制御システムに係るASEAN等向け日米サイバー共同演習を実施。

● 二国間サイバー協議

各国との知見の共有・政策調整を目的として、英国、インド、米国、EU、中韓、イスラエル、仏、エストニア、豪州、ロシア、独、韓及びウクライナとの間でサイバー協議を実施。各国との間でサイバー空間に関する政府横断的な政策協議を継続的に実施。我が国のサイバーセキュリティ政策を紹介しつつ、具体的トピックを議論。



各年別二国間サイバー協議等の開催実績

2013年	米
2014年	米、EU、中・韓、イスラエル、エストニア、仏、英
2015年	豪、露、米、中・韓、エストニア
2016年	仏、イスラエル、米、豪、独、英、韓、露、ウクライナ
2017年	仏、EU、エストニア、中・韓、米、印、イスラエル、豪
2018年	EU、英、仏、米、イスラエル
2019年	豪、印、EU、仏、米、中・韓、露
2020年	ウクライナ、英

注1: 米国とは上記以外にもサイバー空間に関する経済面や安全保障面についての協議を開催

注2: 中国及び韓国とは三カ国協議を開催

● 二国間協議の取組状況（2019年4月～2020年3月）

■ 第4回日仏サイバー対話（2019年6月、ブリュッセル）

両国における戦略、政策、法令に関連する進展について紹介し、デジタル経済・社会における信頼を強化するため、サイバーセキュリティの強化について引き続き協力していくことを確認するとともに、デジタル分野の発展が供与する機会を実現するためにも、安定し、安全なサイバー空間が必要であることを強調。悪意を持って ICTを乱用するいかなる行為も非難し、サイバー空間における国際紛争の解決に平和的手段をもって取り組むことを確認。サイバー空間において責任ある行動を促進するため、同空間において悪意ある活動を行う者を捕捉し、悪意あるサイバー活動を抑止し対応するために引き続き協力を強化する目的で協働することの重要性を強調。国連における政府専門家会合（GGE）及びオープンエンド作業会合の文脈において引き続き協力していくことを確認。

また、サイバー空間における脅威を防止及び緩和し、サイバー犯罪者を捜査及び訴追するためのグローバルな能力を強化するため、国際的な協力が必要であることを強調。サイバー犯罪に立ち向かうための国内法令及び国際協力のための強固な基盤であるサイバー犯罪におけるブダペスト条約の重要性に留意し、グローバルな能力を強化し、ベストプラクティスを交換していくことを確認。

■ 第5回日仏サイバー協議（2019年7月、レンヌ）

両国における脅威認識を示すとともに、それぞれのサイバーセキュリティ政策の直近の進展を共有。国連を始めとする、サイバー空間における平和と安全に関する多国間のフォーラムにおける議論とイニシアチブ、データ・フロー、5Gを含むICTのサプライチェーンリスク及びIoTに関するサイバーセキュリティの強化並びにデジタル製品・サービス・プロセスのライフサイクル・バリューチェーンを通じたセキュリティの強化への対応についても議論。特にオリンピック・パラリンピック大会のような大規模なイベントにおけるサイバーセキュリティ、重要インフラの防護、サイバーセキュリティにおける民間部門の役割、能力構築、第三者との二国間協議及び地域と多国間の文脈におけるサイバーセキュリティ協力についても議論。

サイバー空間における信頼性と安全性のためのパリ・コール、G7ディナール外相会合で発出された「サイバー規範イニシアティブに関するディナール宣言」、G20大阪サミットで共有された「信頼性のある自由なデータ流通（Data free flow with trust）」の考え方や「大阪トラック」の立ち上げ等に留意しつつ、開かれた、自由、公正かつ安全なサイバー空間へのコミットメントを再表明し、サイバー空間への既存の国際法の適用を強調することの重要性を再確認。また、国連における政府専門家会合（GGE）及びオープンエンド作業部会が、過去のGGEにおける成果を前提に、コンセンサスにより、相互補完的にかつ効果的に実施されるよう協力する意思を再確認。また、関係する国内法及び既存の国際法に沿った適切な枠組みを通じた、悪意あるサイバー活動を抑止し、軽減し、原因を特定するための情報共有等の協力を強化する意思を再表明。2020年東京オリンピック競技大会・東京パラリンピック競技大会及び2024年パリオリンピック・パラリンピック競技大会が近づく中、サイバーセキュリティに関する協力を発展させることに合意。

■ 第7回日米サイバー対話（2019年7月、東京）

情勢認識、両国におけるサイバー政策、国際場裡における協力及び能力構築支援等、サイバーに関する日米協力について議論。

■ 第3回日露サイバー協議（2019年11月、東京）

サイバー空間の現状、最新の戦略・政策について意見交換を行うとともに、多国間及び地域的な文脈におけるサイバーセキュリティや重要通信インフラのセキュリティの確保等に関して協議。

■ 第4回日中韓サイバー協議（2019年11月、北京）

最近のサイバー環境やサイバー分野における各国の施策等について意見交換を行うとともに、国連サイバー政府専門家会合（GGE）やオープンエンド作業部会を始めとする国際的なプロセス、サイバー問題等に関する日中韓協力の在り方等について議論。

■ 第2回日ウクライナサイバー協議（2020年1月、東京）

サイバー分野における両国の戦略や体制を紹介しつつ、情勢認識や具体的な取組について意見交換を実施。

■ 第5回日英サイバー協議（2020年1月、東京）

サイバー分野における最新の両国の戦略や取組について意見交換を行ったほか、能力構築支援、国連を含む国際場裡における協力等について議論。

● 国連サイバー政府専門家会合（UNGGE）への参加

- サイバー空間における国際法の適用、規範の形成に積極的に関与
- 2013年9月には、サイバー空間においても既存の国際法が適用されるとする報告書（第3会期）が提出された。
- 2015年9月の報告書（第4会期）では、2013年の報告書の内容を踏まえつつ、国家の責任ある行動規範に係る章において具体的なルールに係る勧告が盛り込まれているほか、ICTの使用に対する国際法の適用に係る章において、「国家が国際法に従って、かつ、国連憲章で認められた形でとり得る固有の権利に留意する」ことが明記された。しかし、2016年～2017年の第5会期では、国際法の適用のあり方等についてコンセンサスを得られなかった。
- 2018年国連総会決議に基づき、2019年12月に第6会期が立ち上がり、2021年央を目途に国連事務総長に報告書を提出することが求められている。

● サイバーに関する新たなG7作業部会（G7伊勢志摩サイバーグループ）の立ち上げ等

- サイバーセキュリティ環境及びG7各国のサイバーセキュリティ関連政策に係る情報共有並びにG7の政策調整に関する議論とサイバー空間における法の支配を促進するための国際的議論の加速を目的として設置。
- 2016年5月G7伊勢志摩サミットの首脳宣言及び附属文書において、以下を確認。
 - ・国連憲章をはじめとする既存の国際法のサイバー空間への適用を確認するとともに、サイバー空間を通じた武力攻撃に対し、国連憲章第51条で認められた個別的又は集団的自衛権が行使可能である。
- 2017年4月G7ルッカ外相会合の外相共同コミュニケ及び「サイバー空間における責任ある国家の行動に関するG7（ルッカ）宣言」において、以下を確認。
 - ・国際違法行為を行った国家に対して均衡性のある対抗措置をとり得る。
 - ・事実を評価し、他の国家にサイバー行為を帰属させることについて国際法に従って独自の決定を自由に行うことができる。
- 2018年4月G7トロント外相会合の外相共同コミュニケ及び「G7伊勢志摩サイバーグループ会合議長報告書」において、以下を確認。
 - ・悪意のあるサイバー行為を阻止し、抑止し、妨げ、対抗するための措置を展開するために協働し、適時にコストを課すことで、悪意のあるサイバー行為を行う者を抑止する。
- 2019年4月G7ディナール外相会合の外相共同コミュニケにおいて以下を確認し、「サイバー規範イニシアチブに関するディナール宣言」を発出。
 - ・悪意のあるサイバー行為を非難し、そのような行為を防止することを目的とした措置を発展させるよう協力を強化すべき。
- 2019年6月G20大阪サミットにおいて、データフリーフローウィズトラスト（信頼性のある自由なデータ流通）の重要性を確認。

● サイバー犯罪条約の締約国の拡大・推進

- 迅速かつ効果的な捜査共助等の法執行機関間における国際連携の強化。国境を越えるサイバー犯罪者の検挙に向けた国際協力の推進。

● その他、GCSC、GCCS等、各種国際会議への参加

- NISC及び関係省庁は、主にASEAN諸国向けに各種の能力構築支援プロジェクトを主催または支援。昨年度の主な取り組みは以下の通り。

分類	名称	実施時期	実施組織
日ASEAN 政策会議	情報連絡演習	6月	NISC
	机上演習	7月	NISC
	CIIPワークショップ	7月	NISC
短期研修	サイバーセキュリティ対策強化のための国際法・政策能力向上	2月	JICA
	サイバー攻撃防御演習	翌年に延期	JICA
	日ASEAN・サイバーセキュリティ能力構築センター(AJCCBC)	通年	総務省・ETDA(タイ)
	制御システムに係る日米サイバーセキュリティ演習	9月	経産省
	日・ASEAN ISP向け情報セキュリティワークショップ	12月	総務省
	APTサイバーセキュリティ技術研修	2月	APT
	日越サイバーセキュリティセミナー	1月	防衛省
共有情報	DAEDALUS：サイバー攻撃アラートシステム	通年	総務省
	TSUBAME：インターネット定点観測システム	通年	JPCERT/CC

- 安倍総理席上発言：「サイバーセキュリティの確保のため、能力構築支援の方針を策定し、引き続きオールジャパンでASEANを支援していく」
- 議長声明：「ASEAN諸国のサイバーセキュリティ確保の取り組みに対する日本の積極的な支援の決意を歓迎」

■ 日・ASEAN首脳会議（2019年11月22日）

- 議長声明：「サイバーセキュリティを含む非伝統的安全保障上の課題及び伝統的犯罪に対処すべく、引き続き協力強化を決意。日ASEAN政策会議、日ASEANサイバーセキュリティ能力構築支援センター等を通じて一層の協力の強化を期待。また、産業制御システムに係る日米共同サイバーセキュリティ演習を東京で実施したことに関し、日本の産業サイバーセキュリティセンター（ICSCoE）を称賛。」

国際連携（警察庁資料）

外国捜査機関・国際機関との連携

- 捜査協力・・・国際捜査共助（外交、刑事共助条約、サイバー犯罪条約）、ICPO、G7・24時間コンタクトポイント
- 国際機関等への職員派遣・・・IGCI（在シンガポール）、米国研究機関等



IGCI

能力構築支援（キャパシティ・ビルディング）

- JICA課題別研修・・・サイバー犯罪対処能力の向上を目指した研修
- ベトナム公安省への支援・・・ベトナム公安省を対象にサイバーセキュリティ及びサイバー犯罪対処能力強化を目指した研修



ベトナム公安省への研修

国際会議への参画等

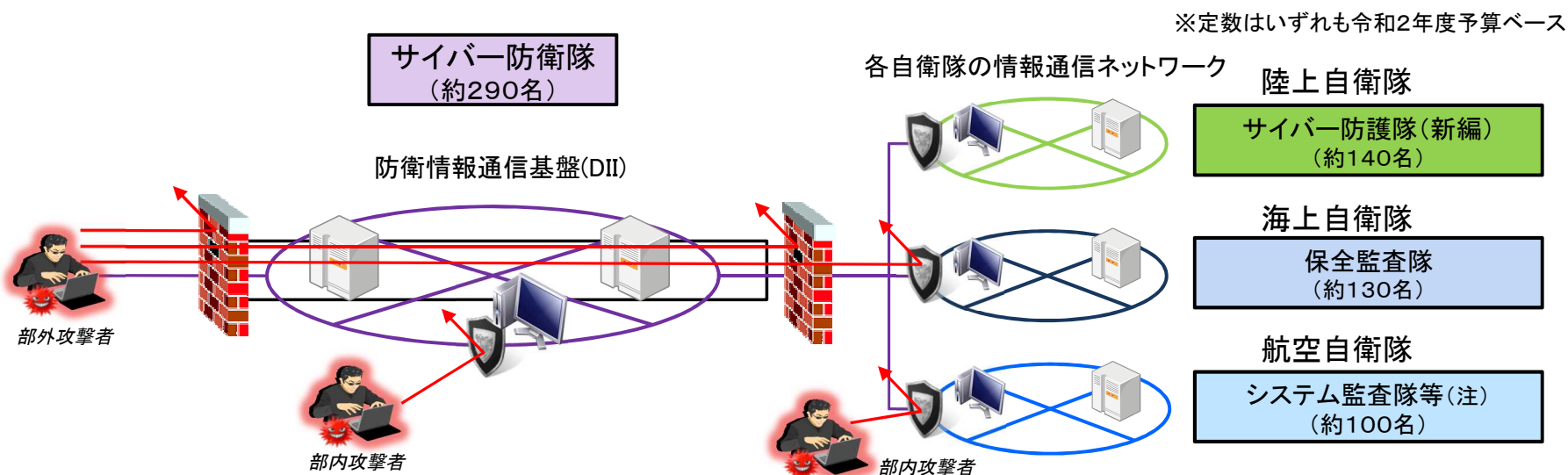
- 二国間協議（サイバー対話・協議）・・・主に欧米、アジア、中東
- 多国間会合・・・G7ローマ/リヨン・グループ（ハイテク犯罪サブ・グループ）
欧州評議会サイバー犯罪条約締約国委員会



G7ローマ/リヨン・グループ

- サイバー防衛隊はDIIを、陸海空のサイバー関連部隊等(陸:システム防護隊、海:保全監査隊、空:システム監査隊等)はそれぞれが管理するシステム・ネットワークを24時間態勢で監視し、サイバー攻撃に対処。
- サイバー防衛隊及び陸海空のサイバー関連部隊等の規模は、以下のとおり。
平成30年度末時点:合計約430名(うち、サイバー防衛隊は約150名)
令和元年度予算:合計約580名(うち、サイバー防衛隊は約220名)
⇒ 令和2年度予算:合計約660名(うち、サイバー防衛隊は約290名)

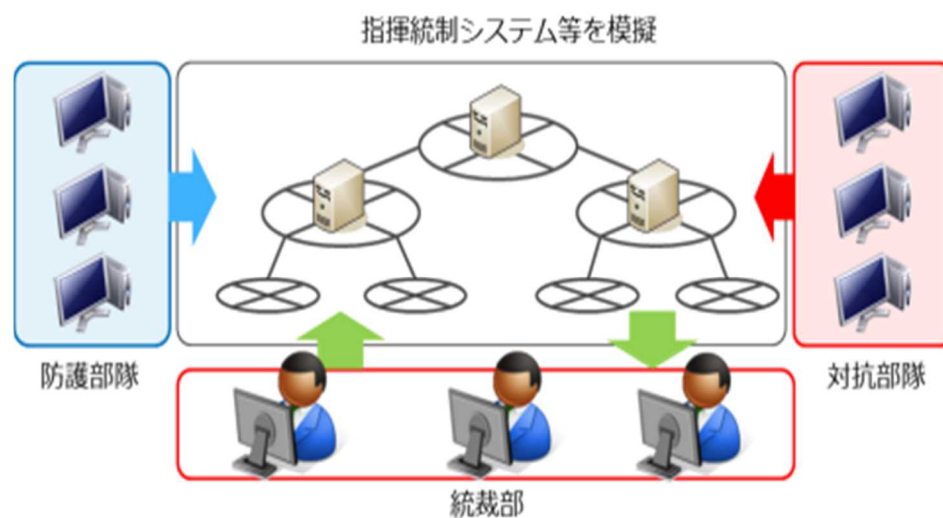
セキュリティ機材等に加え、複数の部隊による重層的な防護態勢を構築



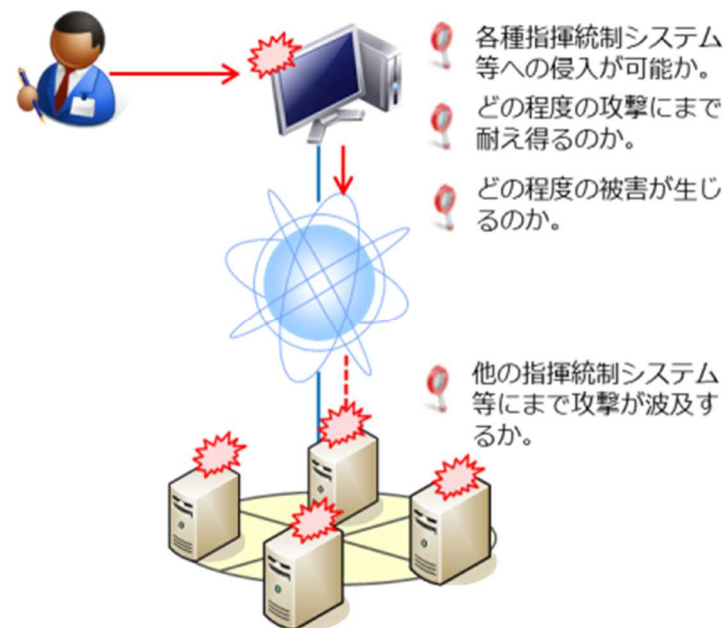
(注)システム監査隊のほか、空自の作戦システム等に係るサイバー防護のための要員

防衛省・自衛隊においては、武力攻撃事態等において相手方のサイバー空間の利用を妨げることが必要となる可能性(注)を想定しつつ、自衛隊の指揮統制システム等を模擬した実戦的なサイバー演習環境の整備、実際のサイバー攻撃と同じ手法を用いた自衛隊の指揮統制システム等の脆弱性の検査(ペネトレーションテスト)等を実施する。

(注)平成31年度以降に係る防衛計画の大綱においては、「有事において、我が国への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力等、サイバー防衛能力の抜本的強化を図る」とこととしている。



実戦的なサイバー演習(イメージ)



ペネトレーションテスト(イメージ)

防衛省・自衛隊主催により、一般の人々を対象としたセキュリティコンテスト(CTF※形式)を開催し、参加する高度サイバー技術者の知見・技能を把握するとともに、当該知見等の防衛省・自衛隊にとっての有用性(契約等により当該技術者の知見等を活用し得る可能性)を調査する。

(※)CTFとは、Capture The Flagの略で、コンピュータのハッキング技術を競うコンテストなどで採用される競技のこと。コンピュータセキュリティに関する攻撃・防御の両方の立場から、暗号、ネットワーク技術、プログラミングなど様々な問題を解くことで技量や知識を競う。



サイバーコンテストのイメージ

国際連携(防衛省資料)

- 近年、サイバー攻撃の態様は、より一層複雑化・巧妙化・高度化。また、国境を越えるサイバー空間の脅威に対しては、国際的に連携して対処していく必要。
- サイバー攻撃は、自衛隊や米軍の任務遂行の場面において大きな阻害要因等となり得ることから、今後日米防衛協力を一層推進していく上で、サイバー空間の安定的かつ効果的な利用の確保は重要。

日米サイバー協力の主要枠組み

日米サイバー対話

(政府間の包括的な協議)

日米サイバー防衛政策
ワーキンググループ

(防衛当局間の政策協議)

日米ITフォーラム

(防衛当局間の情報通信分野に関する協議)

日米情報保証
実務者定期協議

(統幕、在日米軍間の協議)

日米サイバー防衛協力の主要成果

日米防衛協力のための指針(平成27年4月)

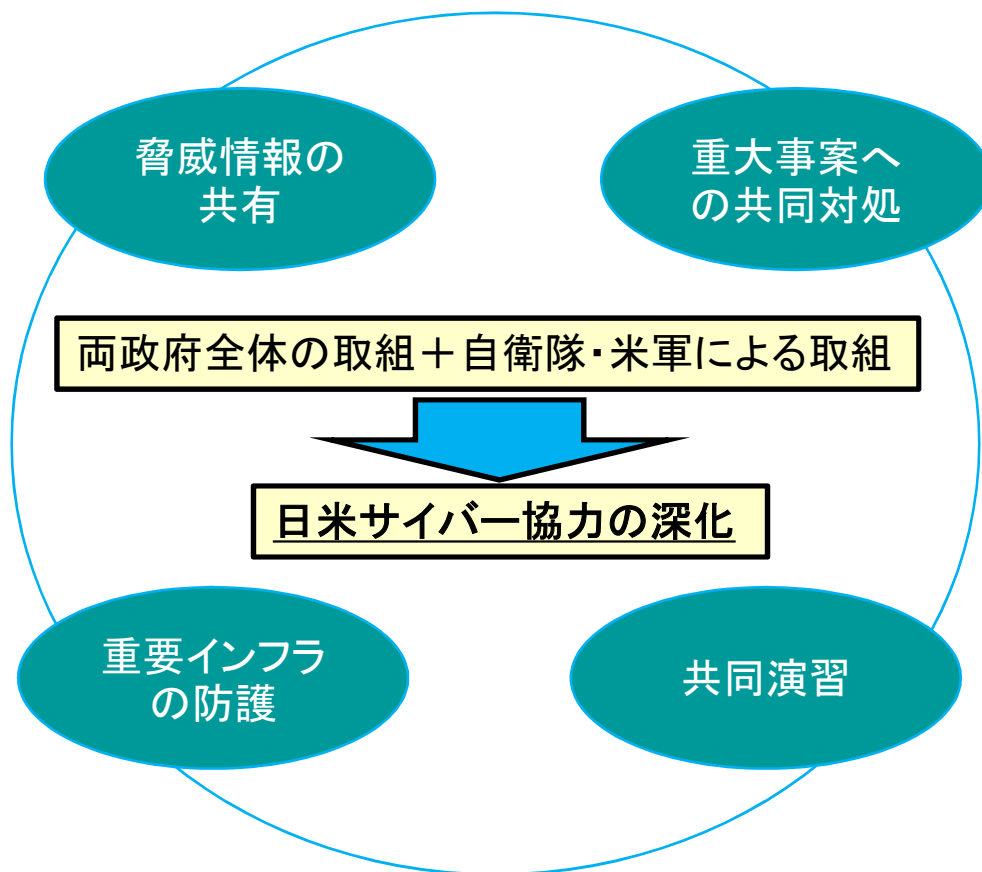
- サイバー空間に関する協力の項を新たに設け、情報共有等、今後の日米のサイバー協力に関する方向性を記述

日米サイバー防衛政策ワーキンググループ共同声明(平成27年5月)

- サイバーに係る脅威認識を共有した上で、重大なサイバー事案への対処、役割・任務、情報共有、重要インフラ防護等、防衛省＝国防省間における具体的な協力分野を記述。

日米「2+2」共同発表(平成31年4月)

- サイバー分野における協力を強化していくことで一致し、国際法がサイバー空間に適用されるとともに、一定の場合には、サイバー攻撃が日米安全保障条約第5条にいう武力攻撃に当たり得ることを確認。



この他、シンガポール、ベトナム、インドネシアとの防衛当局間でITフォーラムを実施するとともに、英国、豪、NATO等との間で、防衛当局間によるサイバー協議を設け、脅威認識やそれぞれの取組に関する意見交換を実施。

防衛産業に適用される調達に関する情報セキュリティ基準の整備（防衛省資料）

取組の背景・経緯

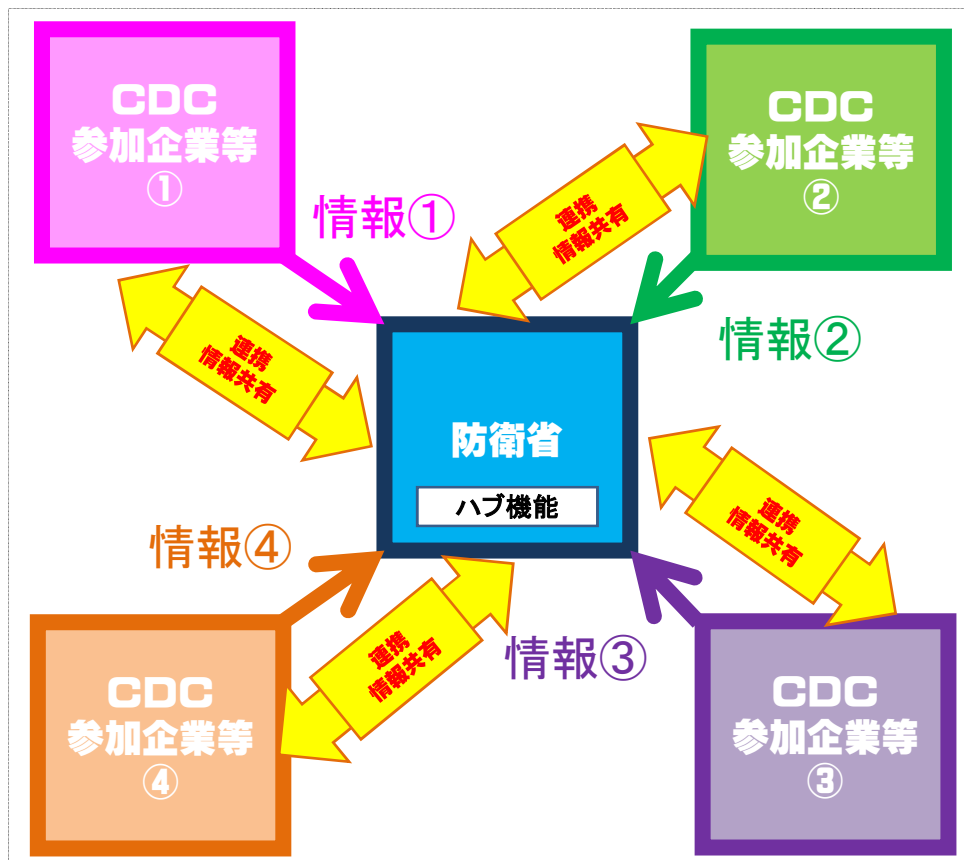
- 現在、防衛省においては、「保護すべき情報」（注意・部内限り）を取り扱う契約企業に対し、特約条項に基づき、防衛省の情報セキュリティ基準（ISO（国際標準化機構）の情報セキュリティ基準（ISMS）がベース）の遵守を義務付け
- 他方、サイバー攻撃の脅威が増大する中、米国の国防調達においては、保全が必要な情報（CUI※）を取り扱う全ての調達先企業（下請企業を含む）に対し、**2017年末までにNIST SP800-171（ISMSより強化された米国の情報セキュリティ基準）の要求事項を満たすことを義務化**
（※ Controlled Unclassified Information：保護すべき非秘密情報）
- NIST SP800-171を満たすことが、今後の米国等との**国際共同研究・開発への参加を継続する最低条件となる可能性**

- 
- 平成29年に主要な防衛関連企業等との間で「官民検討会」を設置し、**我が国の防衛調達における情報セキュリティ強化の方策について検討を実施**
 - その結果を踏まえ、契約企業が「保護すべき情報」を取り扱う際に適用する**防衛省の情報セキュリティ基準について、出来るだけ早い段階で、NIST SP800-171と同程度まで強化する改正を行うことを検討**（改正後、所要の準備期間を経て、令和3年度を念頭に施行することを検討）

目的：防衛省・自衛隊及び防衛産業双方のサイバー攻撃対処能力の向上

設立：平成25年7月

メンバー：サイバーセキュリティに関心の深い防衛産業(10社程度)



○ 主な取組

■ 防衛省がハブとなり、防衛産業間において情報共有を実施

(防衛産業側のメリット)

- ・サイバー攻撃に関する情報の早期入手
- ・企業間におけるベストプラクティスの共有

(防衛省側のメリット)

- ・防衛産業の状況及びニーズの把握

(双方のメリット)

- ・断片情報の集約によるサイバー攻撃の全体像把握

■ CDCでは、毎年1回、防衛省・自衛隊及び防衛産業にサイバー攻撃が発生した事態等を想定した共同訓練等を実施している。

■ASEAN各国との連携

日ASEANサイバーセキュリティ能力構築センター等を活用し、ASEAN加盟国の政府職員、重要インフラ事業者等を対象とした実践的サイバー防御演習及び若手エンジニア向けサイバーセキュリティ競技等を継続的に実施し、域内のサイバーセキュリティ人材の育成支援を推進。また、ISPを対象としたワークショップの開催等を通じて、我が国とASEAN加盟国のネットワークオペレータによって培われた知見や経験の相互共有を促進。



実践的サイバー防御演習の様子

■国際的なISAC間連携

2019年11月に一般社団法人ICT-ISACと米国のIT-ISACとの間でサイバーセキュリティ上の脅威に対する情報共有体制の一層の強化を目的として締結された覚書に基づき、国際連携ワークショップの開催等を通じて、ICT-ISACと米国のICT分野のISACとの連携を強化し、通信事業者、放送事業者、IoT機器ベンダー、セキュリティベンダー等が、脅威情報やインシデント情報等を自動的に共有し、サイバーセキュリティ対策に活用することを促進。



若手エンジニア向けサイバーセキュリティ競技大会(Cyber SEA Game)の様子

■国際標準化の推進

ISO/IEC(国際標準化機構/国際電気標準会議)及びITU-T(国際電気通信連合電気通信標準化部門)における、IoTシステムのセキュリティに係る国際標準化に関する活動に積極的に貢献。

■サイバー空間における国際ルールを巡る議論への積極的参画

様々なチャネルを通じて進められている、サイバー空間における国際ルール等に関する議論へ積極的に参画。



ICT-ISACと米国IT-ISACによる
覚書署名式の様子(2019年11月)

1. インド太平洋地域向け日米サイバー演習

- 2018、2019年度、制御システムのサイバーセキュリティに関する日米専門家による講義・演習を実施。
- 多国間連携のシンボル事業として、2020年度も開催に向けて準備中。
- EUからも専門家派遣の提案があり、日・米・EU三極での共同アウトリーチの実施を目指す。

<昨年度の例>



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



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

<2020年度のイメージ>



2. ASEAN諸国サイバーエコシステム健全性分析調査

- 東アジア・ASEAN経済研究センター（ERIA）が中心となり、米国のNPOとも連携し、ASEAN各国のネットワークやサーバー等のインターネットインフラの健全性やセキュリティ状況に関する分析レポートを作成。

現状と課題

- 脅威は更に深刻化、これまでの人材育成の取組は一定の成果を得つつも専門性を高める取組等一層の充実が必要。
- ITの利活用により、新しい価値を創造するビジネスイノベーションと一体となったサイバーセキュリティへの取組が必要。
→ビジネスにおけるそれぞれの役割の中で、サイバーセキュリティ全体を俯瞰でき、関連するサイバーセキュリティを実践できる人材の育成が必要。
- 高度サイバーセキュリティ人材に関しては、ビジネスイノベーションを生み出せる人材の育成が必要。また、将来的な社会変化に対応するため、セキュリティに対する意識を若年層から高めることが必要。

今後の取組方針

【基本方針】

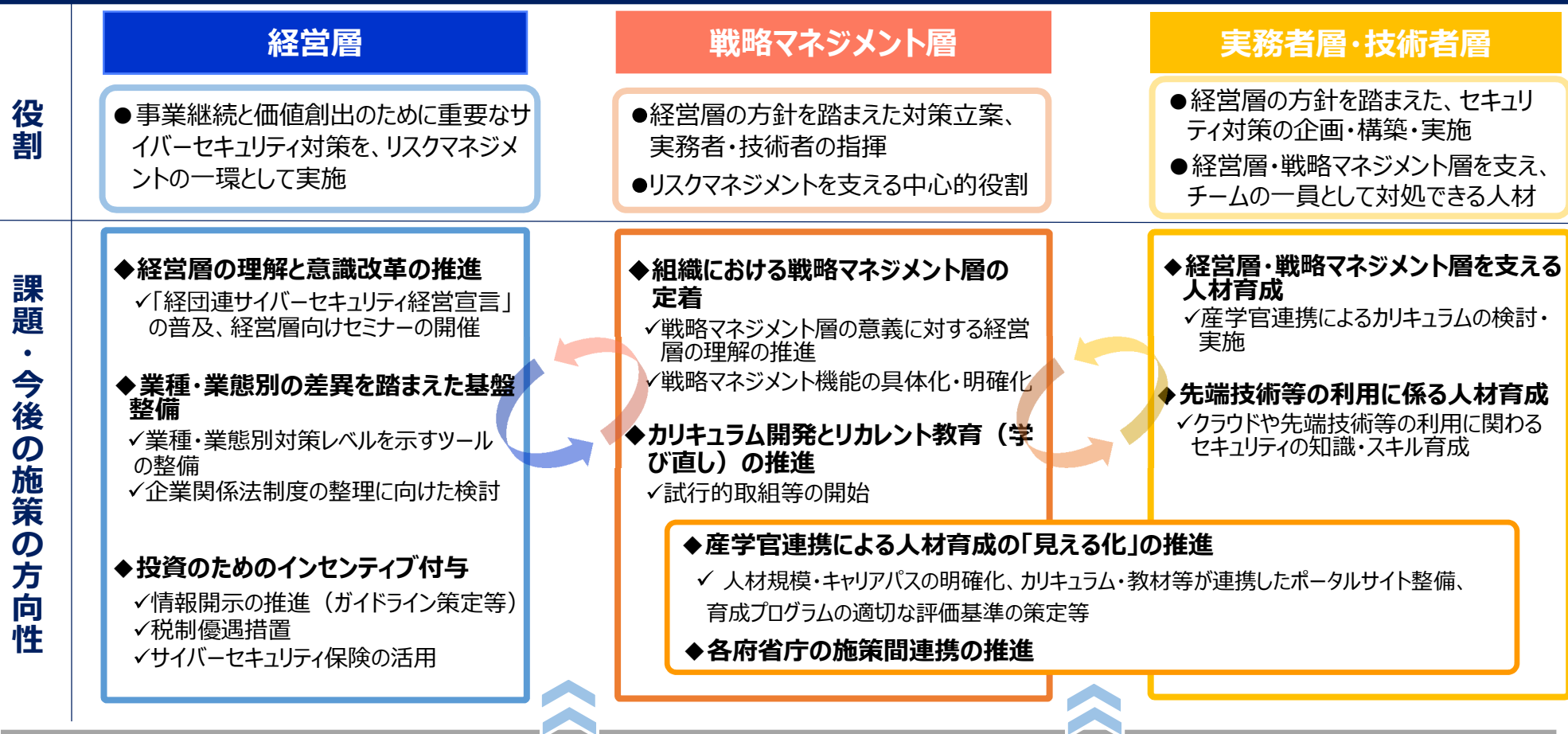
需要(雇用)と供給(教育)の好循環の形成

- これまでの取組に加え、ITの利活用により新たな価値を創造するためのサイバーセキュリティ人材育成が必要。
 - ・経営層:サイバーセキュリティを実務者層だけの問題ではなく経営問題として捉えるとともに、新たな価値の創造という「挑戦」に付随する「責任」としてサイバーセキュリティに取り組むという意識改革を図る。
 - ・橋渡し人材層:経営層・実務者層のコーディネーターにとどまらず、ビジネス戦略と一体となってサイバーセキュリティの企画・立案を行い、実務者層を指揮できる橋渡し人材層の育成に取り組む。
 - ・実務者層:情報セキュリティ技術に関する知識・能力の向上だけでなく、チームとなってサイバーセキュリティを推進するための人材育成に取り組む。
 - ・高度人材(高等教育段階を含む):高度なセキュリティ技術の専門性を持ちつつ、ビジネスイノベーションを創出する高度人材の育成に取り組む。
 - ・初等中等教育段階:児童生徒の情報活用能力(プログラミング的思考や情報セキュリティ、情報モラルを含む)を培う。
- これまでの取組と新たな取組の質的向上を図るため、施策間連携の場をつくり、具体化(例:モデルとなるカリキュラムの策定)を図る。

まとめ

産学官の取組状況や施策間連携の検討状況、サイバーセキュリティ人材を取り巻く課題について、フォローアップを行い、必要に応じて本プログラムの見直しを検討。

- 「サイバーセキュリティ人材育成プログラム」（平成29年4月決定）等を踏まえ、①経営層によるリスクマネジメントの一環としてのサイバーセキュリティ対策の推進、②戦略マネジメント層の人材像やモデルカリキュラムについて、専門調査会における検討を踏まえ、本取組方針を策定。
- 本取組方針の内容については、新たな「サイバーセキュリティ戦略」（平成30年7月閣議決定）に反映。今後、具体的な取組を推進。



若年層教育の充実

＜課題＞ ICTの基本的な原理・仕組みを理解し、論理的思考力を育成。情報モラル教育も重視

＜施策＞ 初等中等教育段階での教育課程内の取組に加え、地域や企業等で、自由に機器・ツールを用いて学べる機会を創出

中小企業関連の取組

＜課題＞ 知識・スキルが十分ではなく、セキュリティ対策への投資が困難。踏み台となった場合、社会への影響が大きい。

＜施策＞ クラウド活用等と一体の対策集の策定・普及、インセンティブの仕組（税制優遇等）の検討

背景

- サイバーセキュリティ、IoT、ビッグデータ、人工知能、組込みシステムなど、情報技術を高度に活用して、社会の具体的な課題を解決することのできる人材の育成は急務であり、我が国の極めて重要な課題
- 今後のIT需要の拡大にもかかわらず、労働人口の減少から、IT人材不足が今後一層深刻化する可能性が高い

例えば、2020年東京オリンピック競技大会・東京パラリンピック競技大会を成功に導くためにもセキュリティ技術者等の高度のIT技術者の育成は不可欠
Society 5.0を実現するためには、ビッグデータ、人工知能等の情報技術の利活用が重要な鍵を握る
また、長期的視点からも、学部教育でのアクティブラーニングの推進や、大学における社会人学び直し機能の強化は喫緊の課題

高等教育機関の役割

- 学生に対する実践的教育の推進**：大学教育改革により、質の高い情報技術人材を多く輩出すること
- 社会人学び直しの推進**：個々の情報技術人材の生産性を高めるための学び直しに貢献すること

改革の
好循環

<産業界に期待する役割(例)>

- ✓ 産業の魅力向上(処遇・キャリア)
- ✓ 流動性向上により高付加価値領域への人材配置
- ✓ 高い競争力の実現→企業収益の確保→優秀な情報技術者に対する高い処遇という好循環の実現

第四次産業革命や
働き方改革に貢献

enPiTの概要

Education Network for Practical Information Technologies (エンピット)

産学連携による課題解決型学習(PBL)等の実践的な教育の推進により、大学における情報技術人材の育成機能強化を目指す取組

① 学生に対する実践的教育の推進

大学院生に対する第1期enPiT

平成24～28年度(5年間)
15大学連携による取組

学部生に対する第2期enPiT

平成28～令和2年度(5年間)
34大学+αの連携による取組

連携協力

- 大学間連携により、PBL中心の実践的な情報教育を行う
- 教育ネットワークを構築し、開発した教育方法や知見を広く全国に普及させる
- 産業界と強力な連携体制を構築する

② 社会人学び直しの推進

社会で活躍するIT技術者の学び直しを推進するenPiT-Pro

複数大学協働(36大学)+産業界(平成29～令和3年度[5年間])



- 大学が有する最新の研究の知見に基づき、情報科学分野を中心とする高度な教育(演習・理論等)を提供する
- 拠点大学を中心とした産学教育ネットワーク構築し、**短期の実践的な学び直しプログラムを開発・実施**する

- 巧妙化・複雑化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、平成29年4月より、情報通信研究機構（N I C T）の「ナショナルサイバートレーニングセンター」において演習等を実施。



国・地方公共団体・独法・重要インフラ事業者等を対象とした実践的サイバー防御演習

⇒ 年間100回、計3,000名規模で実施（1日コース&全都道府県で開催）

2019年度は延べ3,090名が受講（2017年度は延べ3,009名、2018年度は延べ2,666名が受講）

※2021年からオンライン受講を新設予定



東京2020大会関連組織のセキュリティ担当者等を対象とした実践的サイバー演習

⇒ 東京2020大会まで実施予定

2019年度は延べ193名が受講（2017年度は延べ74名、2018年度は延べ137名が受講）



25歳以下の若手セキュリティイノベーターの育成

⇒ 年間50名程度の受講者を選定し、1年間のトレーニングコースを実施

2019年度は45名が修了（2017年度は39名、2018年度は46名が修了）

新たな手法のサイバー攻撃にも対応できる演習プログラム・教育コンテンツを開発



実事案に対処可能な人材育成
CYDER



高度な攻撃に対処可能な人材育成
サイバーコロッセオ



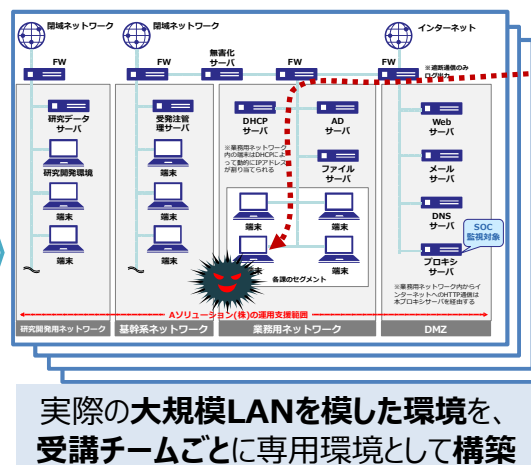
ハイレベル層の人材育成
SecHack365

実践的サイバー防御演習(CYDER)(総務省資料)

- 総務省は、情報通信研究機構(NICT)を通じ、国の機関、指定法人、独立行政法人、地方公共団体及び重要インフラ事業者等の情報システム担当者等を対象とした体験型の実践的サイバー防御演習(CYDER)を実施。
- **全都道府県**において、年間**100回・計3,000名規模**で実施。
※平成29年度：年間100回・3,009名受講／平成30年度：年間107回・2,666名受講／令和元年度：年間105回・3,090名受講
- 2021年1月頃から、未受講の地方公共団体の受講促進等のため、オンライン演習形式を導入予定。

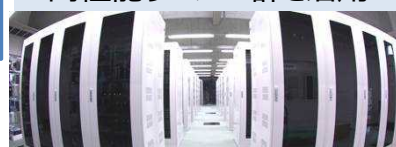
演習のイメージ

NICTの有する技術的知見を活用し、サイバー攻撃に係る我が国固有の傾向等を徹底分析し、現実のサイバー攻撃事例を再現した**最新の演習シナリオ**をコースごとに用意。



擬似攻撃者

NICT北陸StarBED技術センターに設置された大規模高性能サーバー群を活用



演習実施模様
専門の指導員による補助



機材・データを使用して
本番同様の作業を実施



インシデント(事案)
対処能力の向上

令和2年度の実施計画(予定)

※このほか、令和3年1月頃から未受講の地方公共団体を対象としたオンライン演習を導入予定

コース	受講対象組織	対象者	開催地	開催回数	実施時期
Aコース(初級)	全組織共通	システムの運用担当者 (システムの利用者レベルを含む)	47都道府県	65回	8月～翌年2月
B-1コース(中級)	地方公共団体	セキュリティ管理業務を 主導する立場の者	全国11地域	20回	10月～翌年2月
B-2コース(中級)	国の機関等、 重要インフラ事業者等		東京・大阪・ 名古屋・福岡	15回	1月～翌年2月

- 日本国内に居住する**25歳以下の若手ICT人材を対象**として、既存ツールを単に「ユーザー」として利用するだけでなく、**自ら手を動かしセキュリティに関わる新たなモノづくりができる人材（セキュリティイノベーター）**を育成。
- NICTの持つサイバーセキュリティの研究資産を活用し、実際のサイバー攻撃関連データに基づいたセキュリティ技術の研究・開発を、**第一線で活躍する研究者・技術者が1年かけて継続的かつ本格的に指導**。
(2017年度:39名、2018年度:46名、2019年度:45名が修了)
- 受講者は、NICTの有する遠隔開発環境※を活用し、**年中どこからでも遠隔開発実習が可能**。また、集合イベントとして、**座学講座（研究倫理）やハッカソン等**を実施。

※ NONSTOP(NICTER Open Network Security Test-out Platform)では、NICTの長年にわたるサイバーセキュリティ研究によって得られた膨大なセキュリティ関連データを活用することができ、NONSTOP内に整備された様々な研究開発・解析用ツール類と、他では触れることのできない貴重なデータを用いて研究・開発に取り組むことが可能。

若手セキュリティ
イノベーターの育成

ハイ
レベル層



通常のシステム開発者層



座学講座



ハッカソン

通年の遠隔開発実習 + 年6回の集合研修（座学講座・ハッカソン等）の組合せによる総合的な人材育成プログラム

- SECCON (SECurity CONtest) とは、2012年度から開催されている、実験ネットワーク内で行う疑似的な攻防戦などを通じてセキュリティ技術を競うコンテスト。
- 2011年度に経済産業省でセキュリティコンテストの実証事業を行い、同事業の成果を引継ぎ、2012年度からJNSA (NPO法人日本ネットワークセキュリティ協会) が実施している。2019年度で8回目。
- 2019年には世界64カ国、2,347人が予選参加する日本最大の国際競技大会に成長。



■ SECCON2018 国際競技大会

- 1位 TSG (日本)
- 2位 NaruseJun (日本)
- 3位 urandom (日本)
- 4位 CodeRed (韓国)
- 5位 217 (台湾)

■ SECCON2019 国際競技大会

- 1位 NaruseJun (日本)
- 2位 CodeRed (韓国)
- 3位 Blue-Lotus (中国)
- 4位 LC4BC (ロシア)
- 5位 noraneco (日本)



- サイバーセキュリティの確保を支援するため、セキュリティに係る最新の知識・技能を備えた専門人材の国家資格として、「情報処理安全確保支援士」（通称：登録セキスペ）制度を平成28年に創設。
- 令和2年4月1日時点の登録者数は20,413人。
- 令和2年5月より、**登録に3年間の有効期限**を設け、**更新が行われない場合**には、**登録が失効する更新制を導入**。

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

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

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

➡ 有資格者の継続的な知識・技能の向上を図るため、講習の受講を義務化。

※登録の更新制導入により、義務講習を受講したもののみ登録を更新。

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

➡ 業務上知り得た秘密の保持義務を措置。

- 複雑かつ高度化しているサイバー攻撃に適切に対応するため、**若年層のセキュリティ人材発掘の裾野を拡大し、世界に通用するトップクラス人材を創出**することが必要。
- 民間企業と一丸となって、若年層(22歳以下)セキュリティ人材の育成合宿を開催し、**倫理面も含めたセキュリティ技術と、最新ノウハウを、第一線の技術者から伝授する場を創出**。これまでの**セキュリティ・キャンプ全国大会(2004年より開始,計15回開催)**については累計で**748名**が受講。
- 更に、地方における**セキュリティ・キャンプ地方大会(2013年より開始)**も併せて実施することにより、セキュリティ人材の裾野と輪を広げている。



セキュリティ・キャンプ卒業生の例



清水郁実さん
2015年修了（当時15歳）

毎年夏に、米国ラスベガスで開催される世界最大のハッカーの祭典「DEFCON(デフコン)」その目玉イベントのハッカー大会において、3位入賞を果たした。プログラミングや暗号解読をはじめとしたサイバーセキュリティ分野の技術力と知識を武器に、大人達に交じって勝ち抜き、セキュリティ・キャンプ修了生が有する高い技術力を発揮した。

- ・ I T・データを中心とした将来の成長が強く見込まれ、雇用創出に貢献する分野において、社会人が高度な専門性を身に付けキャリアアップを図る、専門的・実践的な教育訓練講座を経済産業大臣が認定する。

※ 厚生労働省が定める一定の要件を満たし、厚生労働大臣の指定を受けた講座は「専門実践教育訓練給付」の対象となる。

■ 講座の要件

- ✓ 育成する職業、能力・スキル、訓練の内容を公表
- ✓ 必要な実務知識、技術、技能を公表
- ✓ 実習、実技、演習又は発表などが含まれる実践的な講座がカリキュラムの半分以上
- ✓ 審査、試験等により訓練の成果を評価
- ✓ 社会人が受けやすい工夫（e-ラーニング等）
- ✓ 事後評価の仕組みを構築 等

■ 実施機関の要件

- ✓ 継続的・安定的に遂行できること（講座の実績・財務状況等）
- ✓ 組織体制や設備、講師等を有すること
- ✓ 欠格要件等に該当しないこと 等

■ 認定の期間

- ✓ 適用の日から3年間

■ 対象分野・目標

※IT技術の基礎・初級は対象としない。

（目標）

(1)
IT
(IT業界)

新技術・
システム

高度技術

①

クラウド、I o T、
A I、データサイエンス 等

開発手法

デジタルビジネス開発（デザイン思考、サービス企画、データ分析、アジャイル等）との組み合わせも想定

②

ネットワーク、セキュリティ 等

(2) 産業界の
I T利活用

自動車（モデルベース開発） 等

I T S S
レベル4相当
を目指す

※ I P A等からの専門的な助言を踏まえ、外部専門家による審査を経て認定を行う

- 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し、IT系・制御系に精通した専門人材の育成を開始。
- 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を実施。

1年を通じた
集中トレーニング

中核人材育成プログラムー 年間スケジュール											
7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月
プライマリー (レベル合わせ)			ベーシック (基礎演習)			アドバンス (上級演習)			卒業 プロジェクト		
開 講 式			ビジネス・マネジメント・倫理								修 了 式
			プロフェッショナルネットワーク（含む海外）								

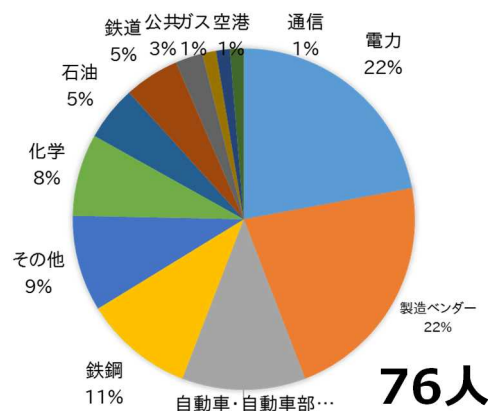


◀ 模擬プラント
全景

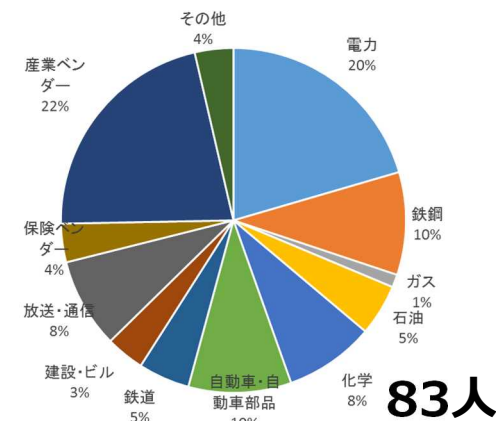
- IT系・制御系に精通した専門人材の育成
- 模擬プラントを用いた対策立案
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析

現場を指揮・指導するリーダーを育成

第1期受講生
(平成29年7月～平成30年6月)
業界別構成



第2期受講生
(平成30年7月～令和元年6月)
業界別構成



- 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。



- 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

約1%

トップガンの学生
→ 主にセキュリティ企業
に就職

約20%

情報系学科の学生
→ 主にIT企業に就職

約80%

非情報系学科の学生
→ 主にユーザー企業に就職



国立高専教員

コンテンツ開発・授業の提供
(パワーポイント、ビデオ等)

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。



ゲーム形式教材のイメージ

※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。

・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

※授業実施側のため。

セキュリティ合宿に関する協力

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。

・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

・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。

※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

・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。

- 平成28年3月に「**サイバーセキュリティ人材育成総合強化方針**」を策定・公表し、同方針に沿った取組を推進。
- 各府省庁は、平成28年度から「**サイバーセキュリティ・情報化審議官**」等を設置し、司令塔機能を抜本的に強化。

主な施策

1. 人材確保・育成計画の作成 【計画的な取組】

- ✓ 各府省庁は、サイバーセキュリティ・情報化審議官等の主導の下、採用・人材育成等にわたる具体的な取組方策を定めた「**セキュリティ・IT人材確保・育成計画**」を作成。
- ✓ 毎年度、見直しを実施。

2. 体制の整備 【人員の確保】

- ✓ 各府省庁は、統括部局・システム所管部局等の体制整備を図るため、政府全体の方針に従って、**機構・定員を要求**。
- ✓ これまで、政府全体で**計約190のポスト増**を実現（29年度：約80ポスト、30年度：約50ポスト、31年度：約60ポストの増加）

3. 研修の実施 【質の維持・向上】

- ✓ 役職段階別（補佐、係長、係員）のスキルレベルのモデルを設定。これに応じた**研修**（総務省の「情報システム統一研修」）の受講を、**原則必須化**。
- ✓ これまで、政府全体でのべ**約28100人の職員が修了**（28年度：のべ約3600人、29年度：のべ約6200人、30年度：のべ約9300人、元年度：のべ約9000人）

4. スキル認定の推進 【能力の評価】

- ✓ 一定の実務経験と研修修了を要件とする、橋渡し人材のスキル認定を行うための**全府省庁共通の基準を策定**（平成30年1月）。
- ✓ 同基準に基づき、各府省庁は、手続規程を整備し、**対象職員の認定を推進**。

5. 適切な処遇の確保 【俸給の調整額】

- ✓ スキル認定された人材を専門性・特殊性の高い業務に充てる場合に、適切な処遇を確保するため、「**俸給の調整額**」を支給。
- ✓ NISCのGSOC業務従事者をモデルとして、これまで、政府全体で**計約90のポストへの適用**が実現（30年度：約50ポスト、31年度：約40ポストへの適用）。

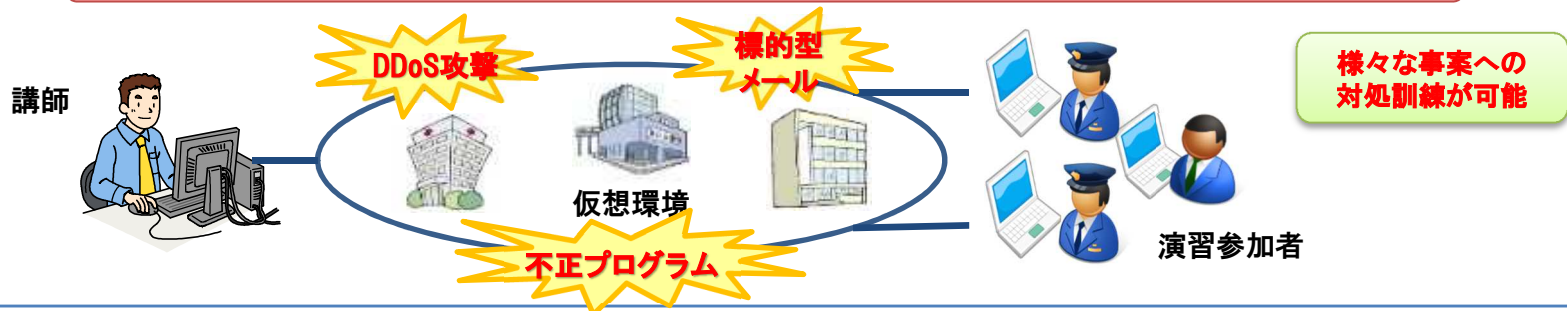
これらの取組により、政府機関におけるセキュリティ・IT人材を着実に確保・育成

- 深刻化するサイバー空間の脅威に対応するためには、**捜査に関する知識と情報通信技術に関する知識の両方を持った人材を組織的かつ体系的に育成することが重要**

警察庁サイバー人材確保・育成計画



人材育成基盤装置を活用した実践的演習



サイバー捜査に必要な
となるログ解析等の訓練

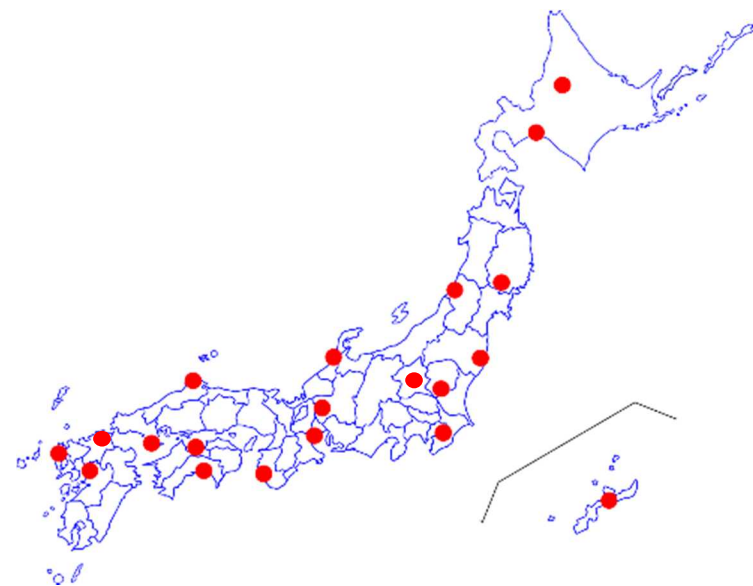
事案対処に必要な
ネットワーク分析訓練

リアルタイム対処訓練

最新事例を
題材とした訓練

カスタマイズ可能な
仮想環境による訓練

- 警察庁では、(独)国立高等専門学校機構と連携し、高等専門学校を対象として、サイバーセキュリティに関する講義を実施。
⇒ 学生のサイバーセキュリティ分野に対する興味・理解を促進し、人材育成とそれに伴う社会全体の対処能力向上を図る。



- (独)国立高等専門学校機構の情報セキュリティ人材育成プログラムに参加する高等専門学校が対象。



不正プログラムに関するデモ



基調講演



捜査支援を模擬した実習

「サイバーセキュリティ戦略」（平成30年（2018年）7月閣議決定）に基づき、戦略期間中の実践的な研究・技術開発に関する取組の具体化を図るという目的のもと、研究開発戦略専門調査会において「サイバーセキュリティ研究・技術開発取組方針」を策定。

取り組むべき課題

- (1) サプライチェーンリスクの増大
- (2) サイバーセキュリティ自給率の低迷
- (3) 研究・技術開発に資するデータの活用
- (4) 先端技術開発に伴う新たなリスクの出現
- (5) 産学官連携強化の必要
- (6) 国際標準化の必要

（参考）セキュリティ関連製品の地域別市場シェア（2016年）



（出典）拡大するサイバーセキュリティ市場（JETRO）
<https://www.jetro.go.jp/biz/areareports/2018/1fb2ecd606c590e5.html>

今後の取組強化の方向性

① サプライチェーンリスクへ対応するためのオールジャパンの技術検証体制の整備

- ICT機器・サービスの信頼性・有効性を検証するためのオールジャパンの体制整備
- ハードウェア・ソフトウェア両面の検証技術の研究開発・実用化（5Gセキュリティ、チップ脆弱性検知、エッジからクラウドに至るまでのハードウェアセキュリティ）

② 国内産業の育成・発展に向けた支援策の推進

- 「Proven in Japan」の推進に向けた、日本発のサイバーセキュリティ製品・サービスの創出・活用及び信頼性を検証するための包括的検証基盤の構築
- 中小企業のニーズに対応したビジネス創出のための支援（サイバーセキュリティお助け隊、コラボレーション・プラットフォーム）

③ 攻撃把握・分析・共有基盤の強化

- サイバー攻撃を迅速に把握するための観測技術の高度化や、AI等の活用による分析・解析技術の効率化・自動化（NICTER、STARDUST等）
- サイバー攻撃の把握・分析データを共有する基盤（CURE）構築

④ 暗号等の基礎研究の促進

- 耐量子計算機暗号や量子暗号等の安全なセキュリティ技術、IoTデバイスにて活用可能な暗号技術の研究・開発
- 暗号技術、暗号・セキュリティ製品やモジュール認証等の国際標準化促進

⑤ 産学官連携の研究・技術開発のコミュニティ形成

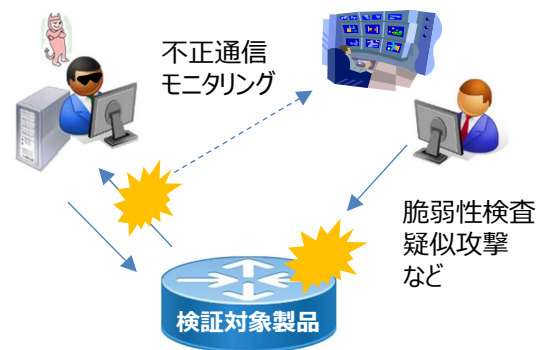
- 産学官によるコミュニティの形成及び諸外国との連携に向けた検討

- 上記の取組強化の方向性に沿って、関係省庁が連携して、具体的・実践的な研究開発を推進
- 個別の研究・技術開発の成果の創出に留まらず、**社会実装までのプロセスを念頭に置きつつ推進**するとともに、**国民社会におけるサイバーセキュリティに関する意識向上**に向けた取組も併せて実施
- 研究開発戦略専門調査会において**定期的に評価**を行い、**必要に応じて方針の見直しを実施**

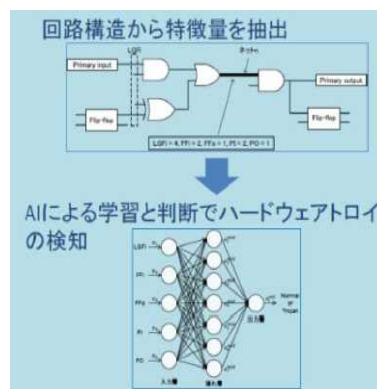
- Society5.0の進展、サイバー攻撃の複雑化・巧妙化に伴い、サプライチェーンリスクの問題が顕在化。諸外国においても、対応強化のための取組が進められている。
- 我が国においても、ICT機器の信頼性を検証するための技術開発と推進体制の構築を進め、サプライチェーンリスクに対応するための技術検証体制の整備を推進することが必要。

(1) 検証技術の開発

脆弱性、不正機能のチェック

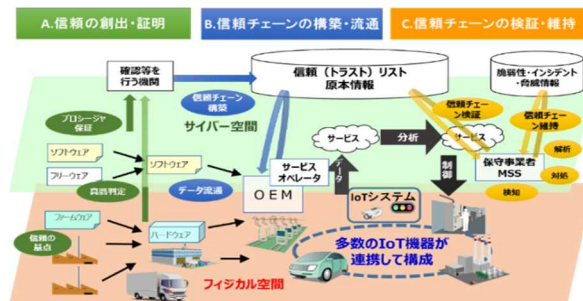


ハードウェアトロイの検出



信頼性・安全性確保のための基盤構築

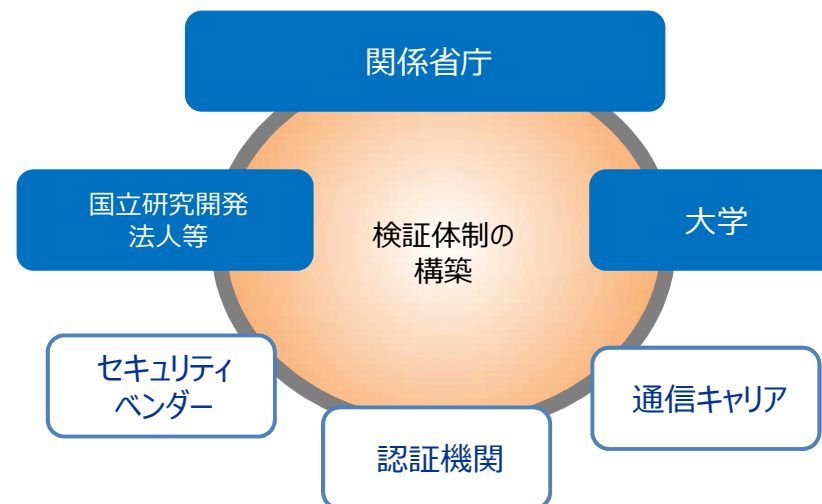
サプライチェーン全体を守るための『サイバー・フィジカル・セキュリティ対策基盤』の開発



(2) 推進体制の整備

推進体制の整備

オールジャパンの官民連携体制の構築



検証結果の活用方策の推進

政府機関や重要インフラ事業者等のシステムで活用するための措置を推進

- 総合科学技術・イノベーション会議の**戦略的イノベーション創造プログラム（SIP）**を活用した研究開発を着実に実施すると共に、研究開発事業を拡充。
- 産業技術総合研究所にサイバー・フィジカル・セキュリティの中核的な研究開発拠点を開設。研究成果の実装のための**認定・認証体制の強化**を推進。

SIP第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」
プログラムディレクター：後藤 厚宏 情報セキュリティ大学院大学 学長



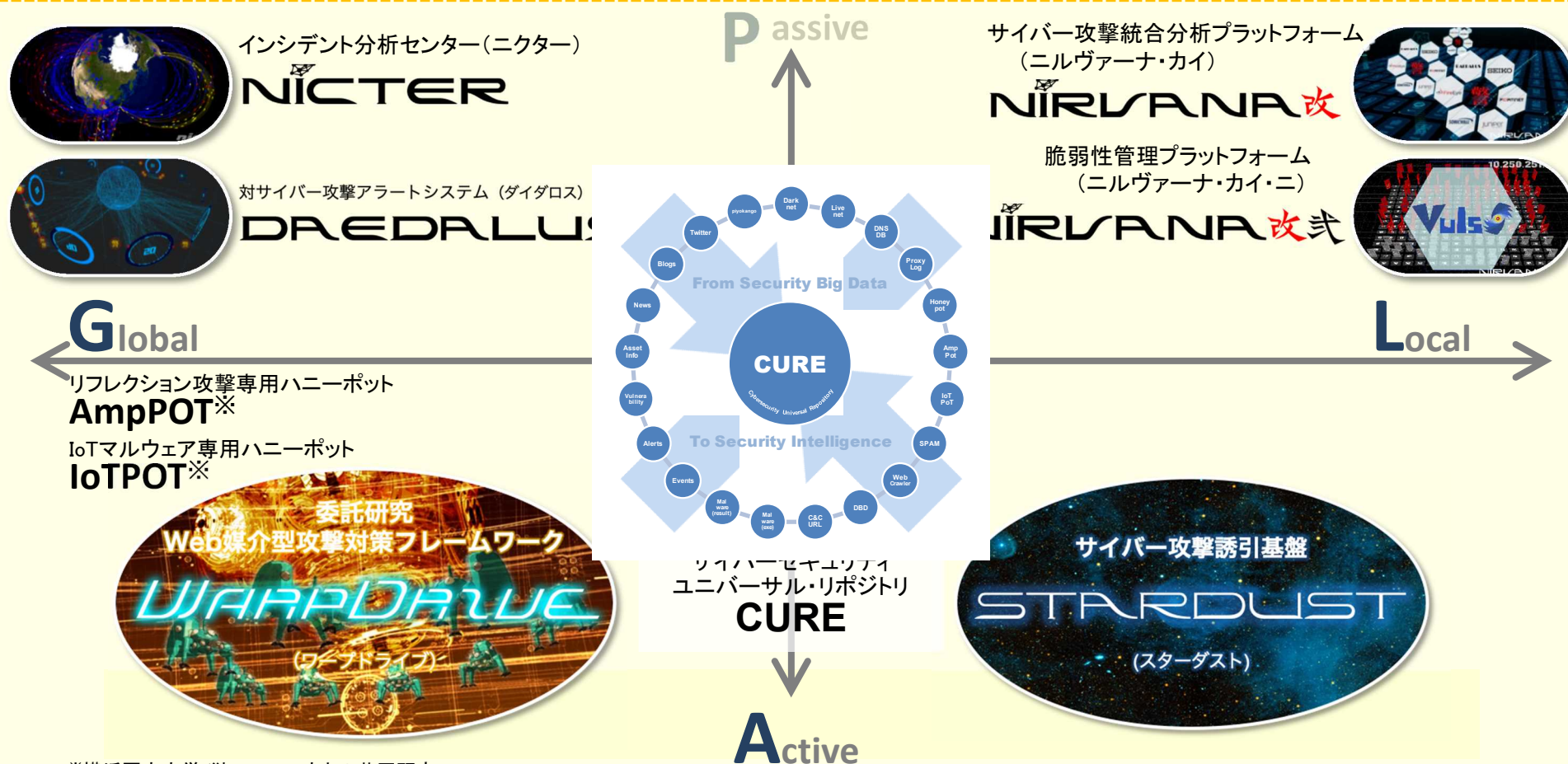
- セキュアな「Society5.0」実現に向けて、サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の社会実装に求められる、IoTシステム・サービス及び大規模サプライチェーン全体を守る対策基盤の開発・実証。

産総研 サイバーフィジカルセキュリティ研究センター（2018年11月設立）
研究センター長：松本 勉 横浜国立大学 教授



- バリューチェーンにおけるセキュリティで必要となる「研究開発」～「評価制度」まで技術面からサポート。
- セキュリティを測定可能とする研究、継続的な最新技術／知見の蓄積。

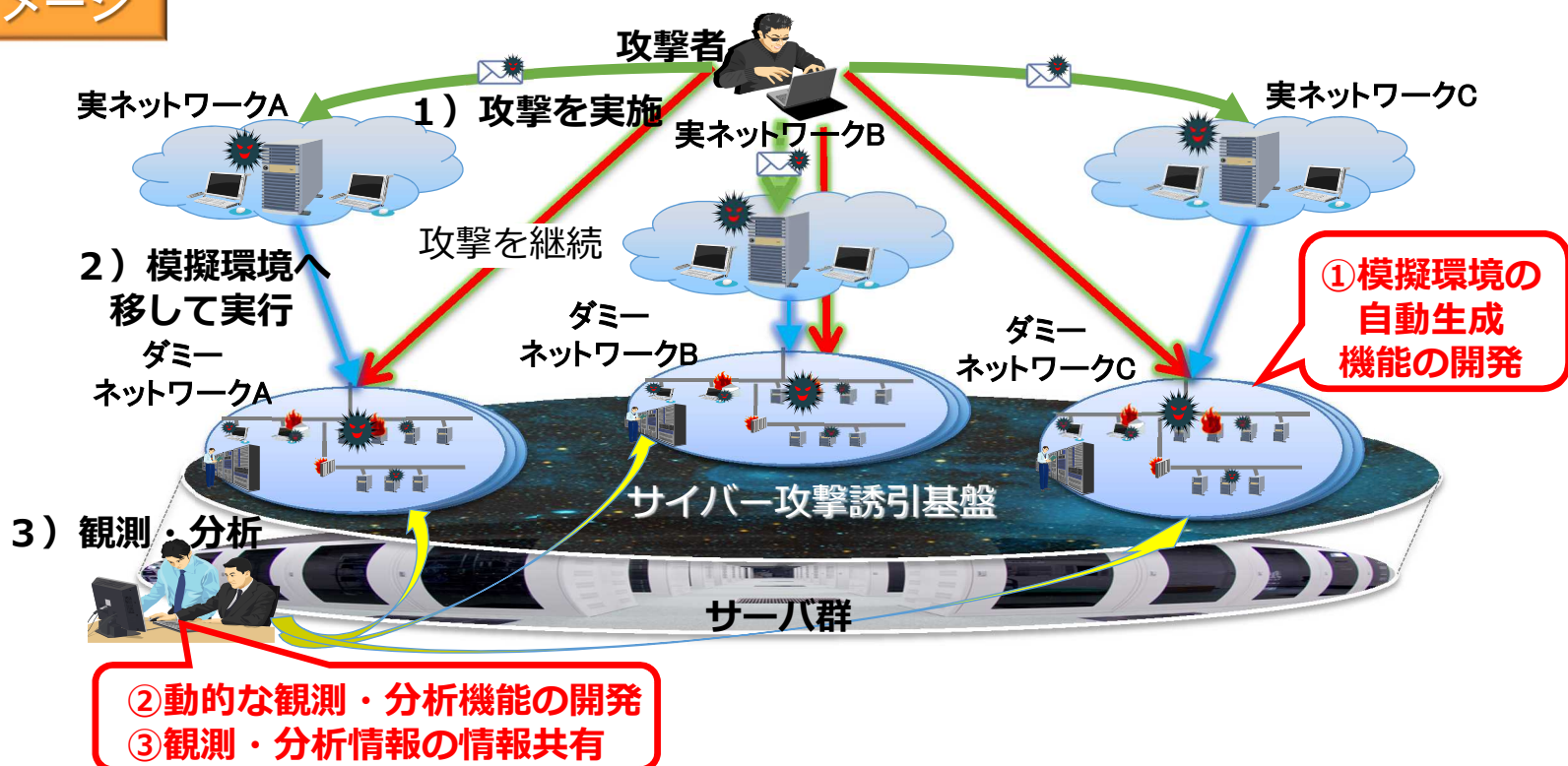
- 急増するサイバー攻撃から社会システム等を守るサイバーセキュリティ分野の技術の高度化が不可欠となっていることを踏まえ、受動的/積極的な観測技術、標的型攻撃対策 (Local)、無差別攻撃対策 (Global) など、技術の種類を問わず、NICTにおいて研究開発を推進。
- 更なる高度化を図るため、各研究分野においてAIを積極的に活用。



※横浜国立大学/独Saarland大との共同研究

- 高度かつ複雑なサイバー攻撃に対処するため、政府や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することが可能な、高度なサイバー攻撃誘引基盤を構築。
- 攻撃活動の早期収集や未知の標的型攻撃等を迅速に検知する技術等の実証を行うための研究開発環境を、情報通信研究機構（NICT）に整備。分析結果は、セキュリティ対策機関等と連携して情報共有を図り、安全なサイバー空間を実現。

システムイメージ



背景・課題

- ✓ 量子技術は、**将来の経済・社会に大きな変革をもたらす源泉・革新技術**。そのため、米国、欧州、中国等を中心に、**諸外国においては「量子技術」を戦略的な重要技術として明確に設定し投資が大幅に拡大**。
- ✓ このままでは、我が国は、量子技術の発展において諸外国に大きな後れを取り、**将来の国の成長や国民の安全・安心の基盤が脅かされかねない状況**。
- ✓ 日本の優れた**量子技術をいち早くイノベーションにつなげることが必要**。

事業概要

事業の目的

- ✓ Q-LEAPは、経済・社会的な重要課題に対し、光・量子技術を駆使して、非連続的な解決 (Quantum leap)を目指す研究開発プログラム

技術領域 1 量子情報処理 (主に量子シミュレータ・量子コンピュータ)

◆ Flagshipプロジェクト※1

- ・ **汎用量子コンピュータ等のプロトタイプを開発**し、クラウドサービスによる提供等

◆ 基礎基盤研究※2

- ・ 量子シミュレータ、量子ソフトウェア等の研究



超伝導量子ビット

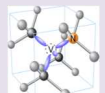
技術領域 2 量子計測・センシング

◆ Flagshipプロジェクト

- ・ **ダイヤモンドNVセンタを用いて脳磁等の計測システムを開発**し、室温で磁場等の高感度計測

◆ 基礎基盤研究

- ・ 量子もつれ光センサ、量子原子磁力計、量子慣性センサ等の研究



ダイヤモンドNVセンタ

技術領域 3 次世代レーザー

◆ Flagshipプロジェクト

- ・ ①**アト(10^{-18})秒スケールの極短パルスレーザー光源等の開発**及び
②**CPS※3型レーザー加工にむけた加工学理等を活用したシミュレータの開発**

◆ 基礎基盤研究

- ・ 強相関量子物質のアト秒ダイナミクス解明、先端ビームオペランド計測等の研究



アト秒パルスによる電子状態の観測

CPS型次世代レーザー加工

事業スキーム

- ✓ 事業規模：7～19億円程度／技術領域・年
- ✓ 事業期間：**最大10年間**、ステージゲート評価を踏まえ研究開発を変更又は中止

1 量子情報処理 (主に量子シミュレータ・量子コンピュータ)

◆ 新規Flagship (量子AI)

- ・ 大規模データの複雑な解析を高速に行い、機械学習する**量子アルゴリズム等を開発**し、画像診断、材料開発、創薬等に应用可能な**量子AI技術**を実現

◆ 既存Flagshipの拡充

- ・ 新たに、クラウドサービスを踏まえて、**実装の検証をするためのシステムを構築**

2 量子計測・センシング

◆ 新規Flagship (量子生命)

- ・ MRIイメージングの超高感度化を実現する**超偏極技術等を開発**し、代謝のリアルタイムイメージングやMRI検査の短縮化が可能な**量子生命技術**を実現

◆ 既存Flagshipの拡充

- ・ 新たに、**電力システムなどのインフラを非侵襲・非接触で安全に故障の予兆をとらえる計測技術を開発**

3 新規人材育成プログラムの開発

- ・ 新たに、我が国の量子技術の次世代を担う人材の育成を強化するため、**量子技術に関する共通的な教育プログラムの開発**を実施



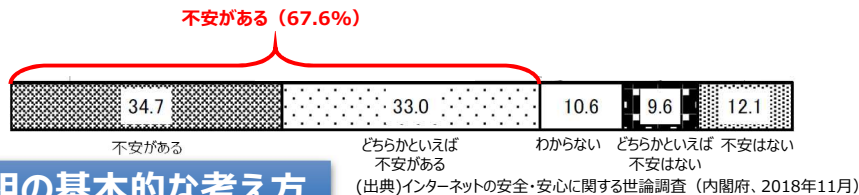
1 はじめに

「サイバーセキュリティ戦略」(2018年7月閣議決定)に基づき、普及啓発について、2020年東京オリンピック競技大会・東京パラリンピック競技大会を見据えつつ、産学官民の関係者が円滑かつ効果的に活動し、有機的に連携できるよう、本プログラムを策定。

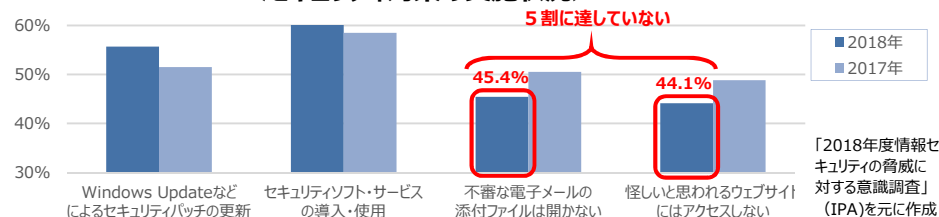
2 現状

- ①個人：**AIやIoTの「生活」への浸透**に伴い、インターネット利用への**不安感が拡大**。一方、**具体的な対策の実施に十分に結びついていない**。
- ②企業：**中小企業では、特に規模の小さい企業ほど**担当者が置けない場合も多いなど、**取組が遅れている**。

＜インターネットの利用に関連するトラブルへの不安感＞



＜セキュリティ対策の実施状況＞



3 今後の取組の基本的な考え方

- ・対策に関する情報が国民一人一人や中小企業に必ずしも行き届いていない、いわば「**サイバーセキュリティのラストワンマイル**」の状況。
- ・「3つの視点」から取組を推進：**①継続的な実施、②対象に合わせた適切なツール・コンテンツの提供、③関係者間の連携の促進**

4 具体的取組の推進

(1) 基本的な対策の徹底

- ・個人や企業が**取組の必要性を自覚し、当たり前のこととして取組を講じる状態**を目指し、**必要な対策を継続的に伝える**

(取組の一例)

「インターネットを安全に利用するための情報セキュリティ対策9か条」(2015年2月 NISC・IPA)の各種取組への浸透



(2) 重点的な対象とその内容

- ・様々な対象に幅広く実施することを前提としつつ、以下の対象について、**重点的に取組を実施**

- ①**中小企業** 中小企業のトラブル対応を支援する「サイバーセキュリティお助け隊」の地域実証、「SECURITY ACTION」活用の促進、中小企業支援ネットワークによる啓発等
- ②**若年層** 無自覚なまま加害者になることを防ぐためのリテラシー向上の取組、先端的人材育成施策の推進
- ③**地域における取組の支援** 産学官連携型の取組の活性化、高専学生によるボランティア活動等



高専学生によるボランティア活動(提供:警察庁)

(3) 情報発信・相談窓口の充実

- ・最新の脅威の情報・対策の適時かつ**迅速な発信**や相談できる窓口の確保等、自ら取り組むための環境を整備

(取組の一例) NISCにおけるSNSによる情報発信



5 連携体制の強化

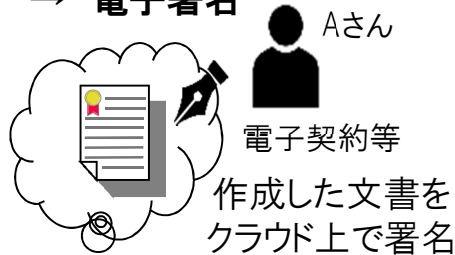
- ・**NISCをはじめとした関係機関が連携し、ラストワンマイルに情報が行き着くよう配慮しつつ取組を推進**
- ①ポータルサイトによる取組の見える化・連携推進 ②ツール・コンテンツの共有 ③サイバーセキュリティ月間の推進 ④国際的連携の強化、⑤P D C Aによる継続的改善
- ・**官民の様々な取組を集約するポータルサイトを構築し、対象となる層や伝達手法の見える化及び連携を推進**
- ・個別施策の実施状況に加え、**個人や企業の対策の実施状況等**を分析し、本プログラムの**内容・効果の定期的な評価、見直しを実施**

「トラストサービス」とは(総務省資料)

- データの自由な流通 (Data Free Flow with Trust) は、これからの成長のエンジン。
- Society5.0の実現に向けて、サイバー空間と実空間の一体化が進展し、社会全体のデジタル化を進める中、その有効性を担保する基盤として、ネット利用者の本人確認やデータの改ざん防止等の仕組みである**トラストサービス**が必要。

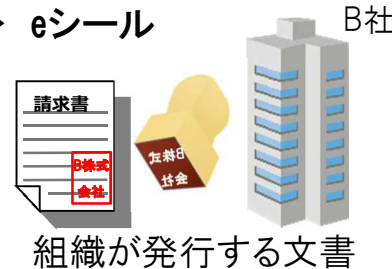
国の制度(電子署名法)有り

- ①人の正当性を確認
→ 電子署名



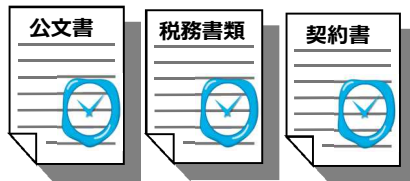
制度無し

- ②組織の正当性を確認
→ eシール



民間の認定スキーム有り

- ④データの存在証明・
非改ざんの保証
→ タイムスタンプ



制度無し

- ③データの送信元(モノ)
の正当性を確認



制度無し

- ⑤データの送達等の保証(①～④の組合せによるサービス)

トラストサービスにより期待される効果の例

- ① 電子署名のクラウド利用への適用(リモート署名※)により、ICカード携行が不要となり、テレワークや出張の際でも、速やかに電子契約が締結可能となることで、ビジネスの迅速化に寄与

※ 利用者がサーバにリモートでログインし、サーバ上で行う電子署名のこと

- ② 組織の正当性を簡便に確認できることにより、企業の文書等の電子化を推進し、社内業務や企業間取引を効率化
- ③ ビッグデータの発信元であるIoT機器等からのデータの真正性を確保し、なりすましを防止
- ④ いつ作成された電子データであるか保証されることで、電子データのみで長期保存が可能となり文書の保存コストが低減
- ⑤ トラストサービスを活用した新たなサービスの創出
(例: "書留"の電子版)

- 2010年より、毎年**2月1日から3月18日**を「**サイバーセキュリティ月間**」に設定。各種啓発主体と連携し、**インターネットを介してサイバーセキュリティに関する普及啓発活動**を集中的に実施。
- 2020年は**新型コロナウイルス感染症の影響**により、各団体の関連行事やNISC主催のイベントなど一部が開催中止となった。
- 一方で、オンライン開催への変更などにより、各種活動は進められ、総じてサイバーセキュリティに関する普及啓発活動を進めることができた。

認知度の高いコンテンツとのタイアップ

- ・『ソードアート・オンライン-アリシゼーション-War of Underworld』とタイアップし、特設サイトを開設した。若年層やサイバーセキュリティに関心の薄い層等を含む幅広い層にサイバーセキュリティに対する関心を高めてもらえるよう、キャラクター同士が会話する形でサイバーセキュリティについて学べるような特別コンテンツも掲載し、**特設サイト全体で累計約160万PVを達成した**。
- ・より多くの国民にサイバーセキュリティ月間を知ってもらえるよう、登場人物を用いたポスターを作成し、**全国の約300機関に約4,200枚を配布した**。

情報発信の強化

- ・サイバーセキュリティ月間の開始にあわせて、2月3日（月）に**菅官房長官によるトップメッセージ**を発信した。
- ・NISCや関係機関のSNSアカウント等において「**#サイバーセキュリティは全員参加**」をつけた情報発信を実施した。
- ・NISCのWebサイトで、7名の有識者による週替わりコラム「**サイバーセキュリティ ひとこと言いたい！**」を発信した。
- ・各種啓発主体の実施する行事を**サイバーセキュリティ月間関連行事**と位置付けて募集し、160件の登録を得た。NISCのWebサイトやSNSで案内を行った（うち、中止等連絡のあったものは26件）。
- ・SNSで**10代を中心に多くのフォロワーを抱えるインフルエンサー**を6名起用し、InstagramやTwitterにおいてサイバーセキュリティを啓発する投稿を行うことで、サイバーセキュリティに関心の薄い層にもサイバーセキュリティに対する関心を高めていただいた。

イベント・行事の開催

- ・ **NISC-CTF**〔CTF：Capture The Flag、セキュリティ技術の競技〕
2月19日に各府省庁・独法等の職員の参加による、サイバーセキュリティに関する幅広い技術・能力を競う競技会を開催。
- ・ **NISC主催 特別イベント「たちあがれ！この世界（インターネット）を守るために。」の動画収録及び配信**
NISC主催の秋葉原での集客イベントは新型コロナウイルス感染症の影響により中止とし、オンライン開催へ変更。イベント内容を動画収録し、YouTubeにて配信した。**閲覧数は約2,600回**となり、所期の普及啓発上の訴求を実施できた。

- ・ タイアップコンテンツの起用や特別イベントの取組について、効果の分析を実施し、次回以降の取組に反映する。
- ・ 特に、今回は緊急的に実施したインターネットを介したイベントの配信について、より効果的に実施できるよう検討を進める。



配布したポスター



官房長官トップメッセージ



NISC-CTFの様子



NISC主催 特別イベントの収録の様子 95

内閣サイバーセキュリティセンター（NISC）における情報発信ツール -インターネットの安全・安心ハンドブック-

NISCでは、身近な話題からサイバーセキュリティに関する基本的な知識を紹介し、学んでいただくことを目的として、**インターネットの安全・安心ハンドブック**（旧 情報セキュリティハンドブック）を作成し、Webサイトにて公開、国内複数の電子書店、公式アプリにて**無料配信**を行っています。



目次

プロローグ サイバー攻撃ってなに？

第1章 基本のセキュリティ

～ステップバイステップでセキュリティを固めよう～

第2章 サイバー攻撃にあつどうなるの？最新の攻撃の手口を知ろう

第3章 パスワード・Wi-Fi・ウェブ・メールのセキュリティを理解して、インターネットを安全に使う

第4章 スマホ・パソコンのより進んだ使い方やトラブルの対処の仕方を知ろう

第5章 SNSやインターネット関連の犯罪やトラブルから、自分や家族を守ろう。

災害に備えよう

エピローグ 来たるべき新世界へ

<入手方法>

■ webサイト

pdfファイルにて公開

「みんなでしっかりサイバーセキュリティ」

<https://www.nisc.go.jp/security-site/handbook/index.html>

■ 国内複数の電子書店

■ スマートフォン・タブレット端末用アプリ

iOS 9.0以降、Android OS 6 以降

レイアウト自動調整（リフロー）形式に対応



★ハンドブックは、内容に改変を加えないことを条件に、多様なかたちで御活用いただけます。

※著作権はNISCに留保されます。

- ・PDF、コピー、印刷所製本での無料配布。実費での販売。
- ・ページ、イラスト単位での使用
- ・自団体のセキュリティ資料と合体して配布
- ・分割、抜粋配布
- ・使用団体名を表紙に記入して使用
- ・HPにダウンロードリンク設置

内閣サイバーセキュリティセンター（NISC）における情報発信ツール -SNS、webサイト-

NISCでは、サイバー攻撃の被害に遭う前に対策をとってもらえるよう、国民向けに、緊急時における注意・警戒情報を含めた情報発信を行っています。

注意・警戒情報発信



Twitter「内閣サイバー（注意・警戒情報）」

プログラムの更新情報やマルウェアの注意喚起情報を発信

https://twitter.com/nisc_forecast



NISCの取組、サイバーセキュリティ関連情報発信



Twitter「NISC内閣サイバーセキュリティセンター」

NISCの取組やサイバーセキュリティに関連する情報を発信

https://twitter.com/cas_nisc



Facebook「内閣サイバーセキュリティセンターNISC」

NISCの取組やサイバーセキュリティに関連する情報、読み物（1日1回）を発信

<https://www.facebook.com/nisc.jp>



LINE「内閣サイバーセキュリティセンターNISC」

NISCの取組やサイバーセキュリティに関連する情報、読み物（1日1回）を発信

ID: @nisc-forecast

Webサイト「みんなでしっかりサイバーセキュリティ」

サイバーセキュリティに関する基礎知識の紹介、情報発信

<http://www.nisc.go.jp/security-site/index.html>

※NISCのHP（<http://www.nisc.go.jp/>）から移動可能



- 総務省では「**テレワークセキュリティガイドライン**」を策定し、**セキュリティ対策の考え方**を示している。
- 新型コロナウイルスの影響により、これまで未導入だった中小企業等においてもテレワークの導入が広まる中で、より**具体的で分かりやすく、実践的な内容のチェックリスト**が求められており、**策定に向けた検討を開始予定**。
- またチェックリスト策定と併せ、**セキュリティ対策**に関する**実態調査**と**専門的な相談対応**を実施予定。

チェックリストの策定

テレワークセキュリティガイドライン (平成30年4月総務省策定)



抽象度の高い一般的な記載
(例)

「ファイアウォールを設置し不必要なアクセスを遮断する」

考え方・方針について記載
(例)

「パスワードは一定以上の長さで推測されにくいものを用いる」

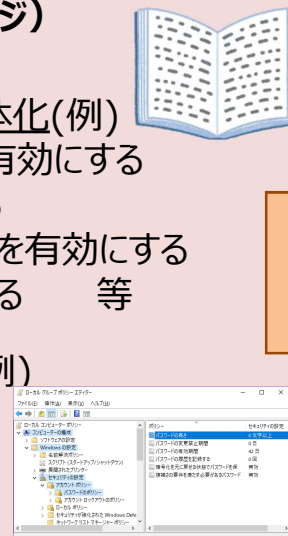
チェックリスト (策定イメージ)

チェックリスト形式による具体化(例)

- ☐ ファイアウォール機能を有効にする
- ☐ NAT機能を有効にする
- ☐ DNSフィルタリング機能を有効にする
- ☐ UPnP機能を無効にする 等

具体的な設定例の解説(例)

Windowsに備わるLGPE機能を使用して一定のパスワード長の強制が可能



これからテレワークを導入する企業でのセキュリティ対策の参考となるだけでなく、テレワークを既に導入済の企業での自己チェックへの活用も可能

実態調査／専門相談対応

テレワーク導入企業が急拡大していると想定され、セキュリティ等の実態や抱えている課題について調査(結果はチェックリスト策定にもフィードバック)



テレワーク導入企業



テレワーク導入時及び導入後におけるセキュリティ対策の専門的な相談