くらしの中に
総務省
MIC Ministry of Internal Affairs and Communications

サイバーセキュリティ戦略に基づく総務省の取組

令和3年12月15日

総務省サイバーセキュリティ統括官室

参事官補佐　広瀬　一朗

自己紹介

・平成21年（2009年）に総務省に入省後、米国留学などを経て、平成29年（2017年）から、高松市でスマートシティに向けた取組を推進。また、令和元年（2019年）からは、内閣官房IT総合戦略室（現在のデジタル庁）で個人情報保護制度の見直しを担当。
・令和3年（2021年）6月から現職。総務省のサイバーセキュリティ施策の全体調整、電気通信事業者における積極的対策の推進、クラウドやスマートシティの対策推進、地域でのセキュリティコミュニティ形成支援を担当。

「スマートシティたかまつ」プロジェクトの推進

ICT・データの活用と多様な主体との連携により、様々な地域課題を解決し、持続的に成長し続ける「スマートシティたかまつ」の実現

スマートシティたかまつ推進プラン（2019～2021）

2017年度～
防災分野
　水位センサー等の設置による対応迅速化
観光分野
　レンタサイクルを利用する観光客動態の把握

2018年度～
福祉分野
　ウェアラブル端末による高齢者見守り
交通安全分野
　交通事故ヒヤリ・ハット発生地点の特定

2019年度～
まちづくり分野
　商店街への通行量カメラの設置
人材育成
　データ利活用人材の育成
業務改革
　ビデオ会議システムを利用した
　お悔やみ手続ワンストップ窓口
デジタルデバイド対策
　地域住民を対象としたスマホ教室

2020年度以降
農業分野、健康分野、行政デジタル化・・・

他自治体への横展開

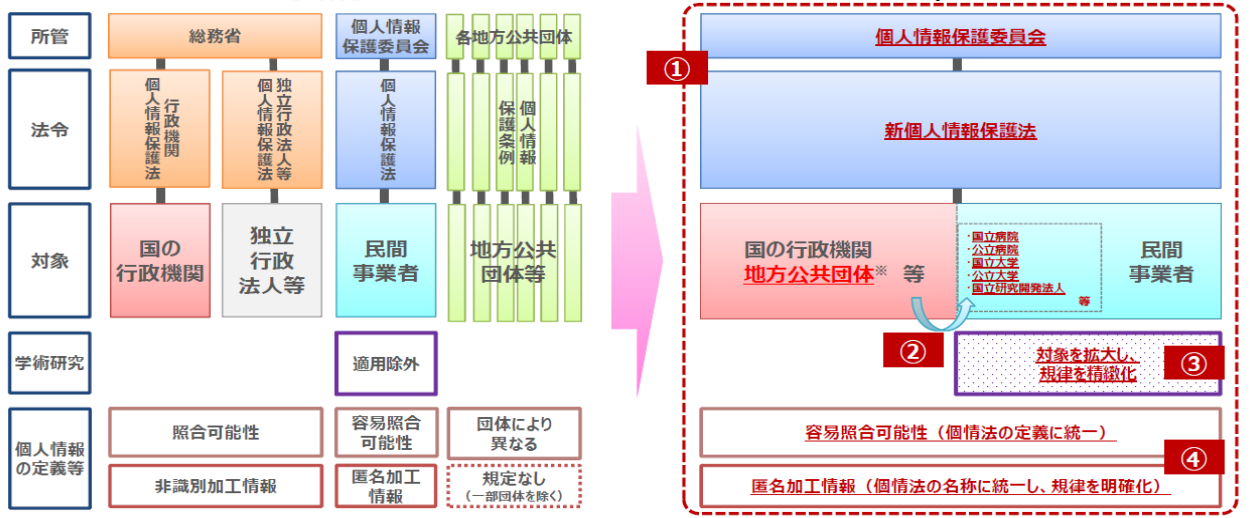
IoT共通プラットフォーム（FIWARE）【本番／実証環境／ODサイト】

産 学 スマートシティたかまつ推進協議会（会長：高松市長） 民 官

個人情報保護制度見直しの全体像

2

① 個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法の**3本の法律を1本の法律に統合**するとともに、**地方公共団体の個人情報保護制度**についても**統合後の法律において全国的な共通ルールを規定**し、**全体の所管を個人情報保護委員会に一元化**。
② 医療分野・学術分野の規制を統一するため、**国公立の病院、大学等には原則として民間の病院、大学等と同等の規律を適用**。
③ 学術研究分野を含めたGDPRの十分性認定への対応を目指し、**学術研究に係る適用除外規定**について、一律の適用除外ではなく、**義務ごとの例外規定として精緻化**。
④ **個人情報の定義等を国・民間・地方で統一**するとともに、行政機関等での**匿名加工情報の取扱いに関する規律を明確化**。



※ 条例による必要最小限の独自の保護措置を許容

１．サイバーセキュリティ戦略

２．総務省のサイバーセキュリティに関する取組

３．地域におけるセキュリティコミュニティ形成

政府全体のサイバーセキュリティ推進体制

- ✓ **「サイバーセキュリティ戦略本部」**（本部長：内閣官房長官）**が政府全体の司令塔**（「サイバーセキュリティ基本法」に基づき、平成27年に設置）。**総務大臣も、同戦略本部の構成員。**
- ✓ **「サイバーセキュリティ戦略」の策定・改定を始め、政府横断的にセキュリティ対策を推進することが役割。**

サイバーセキュリティ戦略本部（2015.1.9 サイバーセキュリティ基本法により設置）

本部長　内閣官房長官
副本部長　サイバーセキュリティ戦略本部事務を担当する国務大臣
本部員　国家公安委員会委員長
デジタル大臣
総務大臣
外務大臣
経済産業大臣
防衛大臣
東京オリンピック競技大会・パラリンピック競技大会担当大臣

本部有識構成員（８名）

遠藤　信博	日本電気株式会社代表取締役会長
後藤　厚宏	情報セキュリティ大学院大学学長
田中　孝司	KDDI株式会社代表取締役会長
中谷　和弘	東京大学大学院法学政治学研究科教授
野原佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英	日本大学大学院法務研究科教授
宮澤　栄一	株式会社デジタルハーツホールディングス取締役会長
村井　純	慶應義塾大学環境情報学部教授 大学院政策・メディア研究科委員長

デジタル庁

デジタル社会の形成に向けた司令塔としてデジタル改革を推進

緊密連携

緊密連携

国家安全保障会議（NSC）

我が国の安全保障に関する重要事項を審議

閣僚本部員6省庁

- 警察庁（サイバー犯罪・攻撃の取締り）
- デジタル庁（デジタル改革）
- **総務省**（通信・ネットワーク政策）
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
- 防衛省（国の防衛）

（事務局）

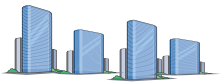
内閣官房　内閣サイバーセキュリティセンター（NISC）

協力

協力

重要インフラ（14分野）
情報通信、地方公共団体(=総務省所管)、金融機関、医療、水道、電力、ガス、化学、クレジット、石油、鉄道、航空、物流、空港

重要インフラ事業者等



政府機関（各府省庁）

企業

個人

サイバーセキュリティ戦略（2021年9月28日閣議決定）の課題と方向性

2020年代を迎えた日本を取り巻く時代認識　：　「ニューノーマル」とデジタル社会の到来

- デジタル経済の浸透、**デジタル改革**の推進
- **新型コロナウイルス**の影響・経験 テレワーク、オンライン教育等の進展
- 厳しさを増す **安全保障**環境
- **SDGｓ**への デジタル技術の貢献期待
- **東京オリンピック・パラリンピック**に向けて行ってきた取組

サイバー空間をとりまく課題認識　：　国民全体のサイバー空間への参画

- サイバー空間は、国民全体等**あらゆる主体が参画し公共空間化**
  サイバー・フィジカルの垣根を超えた各主体の相互連関・連鎖の深化
  攻撃者に狙われ得る弱点にも
- 地政学的緊張を反映 **国家間競争**の場に 安全保障上の課題にも
- 不適切な利用は 国家分断、人権の阻害へ
- 官民の取組の 活用

あらゆる主体にとってサイバーセキュリティの確保は自らの問題に
５つの基本原則※は堅持

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進

安全保障の観点からの取組強化

公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

「自由、公正かつ安全なサイバー空間」の確保

※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

経済社会の活力の向上及び持続的発展

課題認識と方向性　ーデジタルトランスフォーメーションとサイバーセキュリティの同時推進　ー

- 本年9月に「デジタル庁」が設置され、デジタル化が大きく推進される絶好の機会。
  そのためにも、サイバー空間への信頼を醸成し、参加・コミットメントを得ることが重要。
- また、業務、製品・サービス等のデジタル化が進む中、サイバーセキュリティは企業価値に直結する営為に。
  「セキュリティ・バイ・デザイン」の重要性は一層増し、デジタル投資とセキュリティ対策の一体性は高まる。

⇨ デジタル化の進展と併せて、サイバーセキュリティ確保に向けた取組を、あらゆる面で同時に推進。

主な具体的施策

① 経営層の意識改革

→デジタル経営に向けた行動指針の実践を通じ、サイバーセキュリティ経営のガイドラインに基づく取組の可視化・インセンティブ付けを行い、更なる取組を促進。

② 地域・中小企業におけるDX with Cybersecurityの推進

→地域のコミュニティの推進・発展、中小企業向けサービスの審査登録制度を通じ、デジタル化に当たって直面する知見や人材等の不足に対応。

③ 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

→Society5.0に対応したフレームワーク等も踏まえ、各種取組を推進。

- サプライチェーン：産業界主導のコンソーシアム
- データ流通　　：データマネジメントの定義、「トラストサービス」によるデータ信頼性確保
- セキュリティ製品・サービス：　第三者検証サービスの普及
- 先端技術　　：情報収集・蓄積・分析・提供等の共通基盤構築

④ 誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

→情報教育推進の中、「デジタル活用支援」と連携して、各種取組を推進。

国民が安全で安心して暮らせるデジタル社会

課題認識と方向性 ― 公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心確保 ―

- サイバー空間の**公共空間化、相互連関・連鎖の深化、サイバー攻撃の組織化・洗練化。**

  国は、様々な主体と連携しつつ、①自助・共助による**自律的なリスクマネジメントが講じられる環境づくり**と、②持ち得る手段の全てを活用した**包括的なサイバー防御の展開**等を通じて、**サイバー空間全体を俯瞰した自助・共助・公助による多層的なサイバー防御体制を構築**し、国全体のリスク低減、レジリエンス向上を図る。

主な具体的施策（１）国民・社会を守るためのサイバーセキュリティ環境の提供

① 安全・安心なサイバー空間の利用環境の構築

- サプライチェーン管理のためのガイドライン策定や産業界主導の取組、IoT、5G等の新技術実装に伴う安全確保
- 利用者保護の観点から安全かつ信頼性の高い通信ネットワークを確保するための方策の検討

② 新たなサイバーセキュリティの担い手との協調（クラウドサービスへの対応）

- 政府機関・重要インフラ事業者等向けにクラウド利用の際に考慮すべきセキュリティルール策定
- ISMAPの取組等の民間展開による一定のセキュリティが確保されたクラウド利用の促進
- 信頼性が高く、オープンかつ使いやすい高品質クラウドの整備の推進

③ サイバー犯罪への対策

- サイバー空間を悪用する犯罪者やトレーサビリティを阻害する犯罪インフラを提供する悪質な事業者等の摘発を推進し、実空間と変わらぬ安全・安心を確保
- 警察におけるサイバー事案対処体制の強化

④ 包括的なサイバー防御の展開

- サイバー攻撃対処から再発防止等の政策措置までの総合的調整を担うナショナルサート機能の強化（対処官庁のリソース結集と連携強化、サイバーセキュリティ協議会等の関係機関との連携による官民連携・国際連携強化）
- 包括的サイバー防御のための環境整備（脆弱性対策、技術検証、制御システムのインシデント原因究明機能の整備等）

⑤ サイバー空間の信頼性確保に向けた取組

- 個人情報や知的財産を保有する主体への支援
- 経済安保の視点を踏まえたITシステム・サービスの信頼性確保（政府調達、重要なインフラ、国際海底ケーブル等）

国民が安全で安心して暮らせるデジタル社会

主な具体的施策（２）デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

- デジタル庁が策定する国等の情報システム整備方針にサイバーセキュリティの基本的な方針も示し実装を推進。
- 情報と発信者の真正性等を保障する制度を企画立案し、普及を促進。ISMAP制度を運用し、民間利用の推奨。

主な具体的施策（３）経済社会基盤を支える各主体における取組

① 政府機関等

- 政府統一基準群に基づく対策の推進や監査・CSIRT訓練・GSOCによる監視等を通じた政府機関全体としてのセキュリティ水準の向上。
- クラウドサービスの利用拡大を見据えた政府統一基準群の改定・運用やクラウド監視に対応したGSOC機能の強化。

② 重要インフラ

- 「重要インフラの情報セキュリティ対策に係る第４次行動計画」を改定し、環境変化に対応した防護の強化や経営層のリーダーシップを推進。
- 地方公共団体情報システムの標準化や行政手続きのオンライン化等に対応したガイドラインの見直し等の諸制度整備。

③ 大学・教育研究機関等

- リスクマネジメント・事案対応に関する研修・訓練や、サプライチェーンリスク対策を含む、先端情報を保有する大学等への対策強化支援等。

主な具体的施策（４）多様な主体による情報共有・連携と大規模サイバー攻撃事態等への対処体制強化

- 東京大会での対処態勢や運用により得た知見やノウハウを広く全国の事業者等に対する支援として積極活用。
- 平素から大規模サイバー攻撃事態等へのエスカレーションを念頭に、国が一丸となったシームレスな対処態勢を強化。

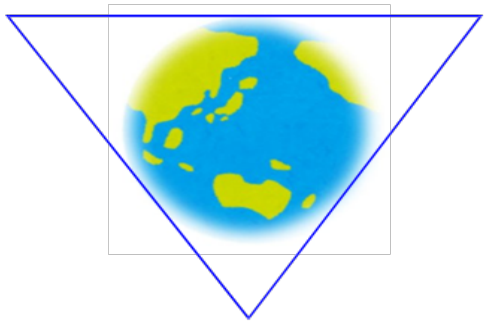
国際社会の平和・安定及び我が国の安全保障への寄与

課題認識と方向性　－ 安全保障の観点からの取組強化 －

- 我が国をとりまく安全保障環境は厳しさを増し、サイバー空間は、地政学的緊張も反映した国家間の競争の場となっている。中国・ロシア・北朝鮮は、サイバー能力の構築・増強を行い、情報窃取等を企図したサイバー攻撃を行っているとみられている。
- 一方、同盟国・同志国においても、サイバー脅威に対応するため、サイバー軍や対処能力の強化が進められており、サイバー事案やサイバー空間に関する国際ルール等をめぐる対立等に対して同盟国・同志国等が連携して対抗している。
- 加えて、安全保障の裾野が経済・技術分野にも一層拡大している中で、サイバー空間に関する技術基盤やデータをめぐる争いに対しても、同盟国・同志国が連携して対抗し、「自由、公正かつ安全なサイバー空間」を確保するため、我が国の基本的な理念に沿った国際ルールを形成していく必要がある。

⇨ サイバー空間の安全・安定の確保のため、外交・安全保障上のサイバー分野の優先度をこれまで以上に高めるとともに、以下を一層強化する。

「自由、公正かつ安全なサイバー空間」の確保



国際協力・連携

我が国の防御力・抑止力・状況把握力の向上

国際社会の平和・安定及び我が国の安全保障への寄与

主な具体的施策

① 自由・公正かつ安全なサイバー空間の確保

- サイバー空間における法の支配の推進（我が国の安全保障に資するルール形成）
  - 国際法の適用に関する議論・規範の実践の普及、サイバー犯罪に関する条約の普遍化等の推進
- サイバー空間におけるルール形成
  - 信頼性のある自由なデータ流通（Data Free Flow with Trust: DFFT）や5Gセキュリティ等国際的な取組の進展を踏まえた我が国の基本理念に沿う国際ルールの策定

② 我が国の防御力・抑止力・状況把握力の強化

- サイバー攻撃に対する防御力の向上
  - 防衛省・自衛隊におけるサイバー防衛能力の抜本的強化、自衛隊・米軍のインフラ防護の演習等の実施
  - 先端技術・防衛産業等のセキュリティ確保のための官民連携・情報共有等の強化
- サイバー攻撃に対する抑止力の向上
  - 相手方によるサイバー空間の利用を妨げる能力の活用や外交的手段・刑事訴追等を含めた対応の活用、日米同盟の維持・強化
- サイバー空間の状況把握力の強化
  - 全国的なネットワーク・技術部隊・人的情報を駆使したサイバー攻撃の更なる実態解明の推進

③ 国際協力・連携

- 知見の共有・政策調整
  - 米豪印やASEAN等同志国との府省庁横断的・各府省庁における国際連携の重層的な枠組みの強化
- サイバー事案等に係る国際連携の強化
  - 国際サイバー演習の主導等による国際的なプレゼンスの向上
- 能力構築支援
  - 「基本方針」*に基づく産学官連携や外交・安全保障を含めたASEANを含むインド太平洋地域における取組強化

*「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に係る基本方針」

サイバーセキュリティ戦略（横断的施策）

DXとサイバーセキュリティの同時推進

公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

安全保障の観点からの取組強化

● 上記の推進に向け、横断的・中長期的な視点で、研究開発や人材育成、普及啓発に取り組む。

１． 研究開発の推進

産学官エコシステム構築とともに、それを基盤とした実践的な研究開発推進。
中長期的な技術トレンドも視野に対応。

(2)実践的な研究開発の推進

①サプライチェーンリスクへの対応
②国内産業の育成・発展
③攻撃把握・分析・共有基盤
④暗号等の研究の推進

(3)中長期的な技術トレンドを視野に入れた対応

①AI技術の進展
AI for Security
Security for AI

②量子技術の進展
耐量子計算機暗号の検討
量子通信・暗号

(1)国際競争力の強化 産学官エコシステムの構築

・研究・産学官連携振興施策の活用
・研究環境の充実 等

２． 人材の確保、育成、活躍促進

「質」・「量」両面での官民の取組を一層継続・深化させつつ、環境変化に対応した取組の重点化。官民を行き来しキャリアを積める環境整備も。

(1)DX with Cybersecurity の推進

・「プラス・セキュリティ」知識を補充できる環境整備
・機能構築・人材流動に関するプラクティス普及 等
（xSIRT、副業・兼業等）

(2)巧妙化・複雑化する脅威への対処

・人材育成プログラムの強化
SecHack365 / CYDER / enPiT
ICSCoE中核人材育成プログラム 等
・人材育成共通基盤の構築
産学への開放
・資格制度活用に向けた取組 等

優秀な人材が民間、自治体、政府を行き来しながらキャリアを積める環境の整備

(3)政府機関における取組

外部高度人材活用の仕組み強化
「デジタル区分」合格者の積極採用、研修の充実・強化 等

３． 全員参加による協働、普及啓発

デジタル化推進を踏まえ、アクションプランの推進・改善、高齢者への対応を含め見直しの検討。

１．サイバーセキュリティ戦略

２．総務省のサイバーセキュリティに関する取組

３．地域におけるセキュリティコミュニティ形成

総務省のサイバーセキュリティに関する取組の大枠

情報通信分野におけるサイバーセキュリティの確保

＝ なりすましやサイバー攻撃による**情報・データの流出・改ざん・サービスの停止を防止**

⇒ 以下の施策を推進することで、**安全で信頼できる情報通信インフラ、機器・サービスを実現**

① 電気通信事業者による積極的セキュリティ対策

・フロー情報(※1)の分析によるC&Cサーバ(※2)の検知に向けた取組

② 5Gのセキュリティ

・5Gのサプライチェーンリスク対策を含むセキュリティ担保

③ テレワークのセキュリティ

・テレワークセキュリティガイドライン、中小企業等向けのチェックリストの作成

④ IoT(※3)のセキュリティ

・パスワード設定に不備のあるIoT機器の調査(NOTICE)

⑤ クラウドサービスのセキュリティ

・クラウドセキュリティガイドラインの策定

・ISMAP制度の推進

⑥ スマートシティのセキュリティ

・スマートシティセキュリティガイドラインの策定、普及促進

…

(※1) IPアドレスやポート番号、タイムスタンプ等の付随情報

(※2) 各感染端末(ボット)にサイバー攻撃の指示を出す管理サーバ

(※3)「Internet of Things」ネットに接続された監視カメラ等

⑦ 人材育成

・「ナショナルサイバートレーニングセンター」における取組 など

⑧ 「統合知的・人材育成基盤(CYNEX)」の構築

⑨ 国際連携

・米国との連携、ASEANとの連携(「日ASEANサイバーセキュリティ能力構築センター(AJCCBC)」) など

①電気通信事業者の積極的なサイバー攻撃対策の実現

➢ 大規模化・巧妙化・複雑化するサイバー攻撃・脅威に、電気通信事業者が積極的に対処できるようにするため、フロー情報（注１）の分析を通じて、サイバー攻撃の指令元であるC&Cサーバ（注２）を検知する技術の実証等を行う。

（１）通信の秘密に係る法的整理

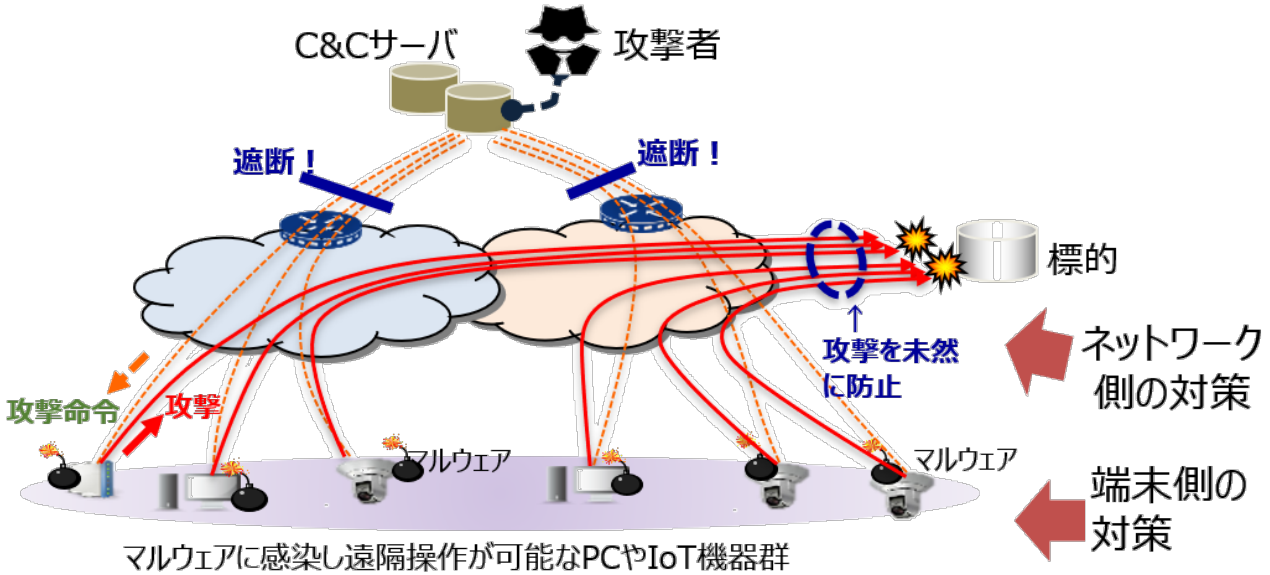
有識者による研究会において、電気通信事業者における、インターネット利用者のトラヒックのうち必要最小限の範囲で収集するフロー情報の統計的・相関的な分析によるC&Cサーバである可能性が高い機器の検知について、通信の秘密に係る法的整理を実施。

※「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」（座長：鎮目征樹学習院大学法学部教授）の第四次とりまとめ（令和３年11月24日公表）において、正当業務行為（通信の秘密の侵害に該当しない）として整理。

（２）実証事業（令和３年度補正予算案）

※「サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証」（18.0億円）

令和３年度補正予算案に、電気通信事業者におけるフロー情報分析によるC&Cサーバ検知技術の有効性の検証や、事業者間の共有に当たっての運用面の課題整理のための実証事業を盛り込んでいる。



注１　フロー情報
通信トラフィックに係るデータのうち、IPアドレス及びポート番号等のヘッダ情報並びにルータでヘッダ情報を抽出する際に付与されるタイムスタンプ等の情報（通信の内容は含まない）

注２　C&Cサーバ
Command and Controlサーバの略で、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者から指令を送り、制御を行うサーバコンピュータのこと

（参考）最近のサイバー攻撃の事例

１．国内の事例

2021年 4月　総務省や自治体から業務委託を受けるランドブレインがマルウェアに感染し、個人情報が流出した可能性。

5月　富士通のプロジェクト情報共有ツール「ProjectWEB」への不正アクセスにより、同ツールを利用していた内閣官房NISC、国交省、外務省等から利用する情報システム等の情報が流出したとの発表。

7月　国内大手製粉会社ニップンが大規模なサイバー攻撃を受け約9割のシステムに被害、決算報告にも影響。

9月　Fortinet製VPN機器から認証情報が流出、中小企業を中心に日本企業約1000社が含まれると報道。

10月　NTTドコモが同社を騙ったSMSによるフィッシング詐欺で、およそ1200人、１億円の被害が発生したと発表。

11月　徳島県の町立病院がランサムウェアによる攻撃を受け、電子カルテが暗号化。予約の受け入れなどを停止。

２．外国の事例

2020年12月　米国のソフトウェア企業であるSolarWinds（ソーラーウィンズ）社がハッキングされ、同社が提供するネットワーク管理ソフトウェア製品を導入している企業や政府機関の内部情報などが流出したことが判明。

2021年 5月　米国の石油パイプライン大手のColonial Pipeline（コロニアルパイプライン）社が、ランサムウェアによるサイバー攻撃を受けて操業を一時停止し、原油価格にも影響。

7月　米国のIT企業Kaseyaのリモート監視・管理製品がゼロデイ攻撃を受け、同製品を運用するMSP事業者を通して、MSPサービスを利用する多数の中小企業等でランサムウェアによる被害が発生。

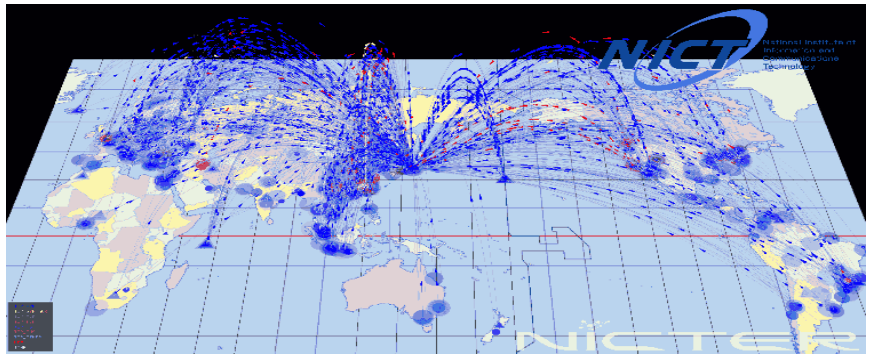
8月～9月　米・露・ニュージーランドなど世界各地でボットネット「Meris」によるものとみられるDDoS攻撃が発生。

10月　米国テレビ局運営大手Sinclairがランサムウェア攻撃を受け、傘下の複数のテレビ局で放送が停止。

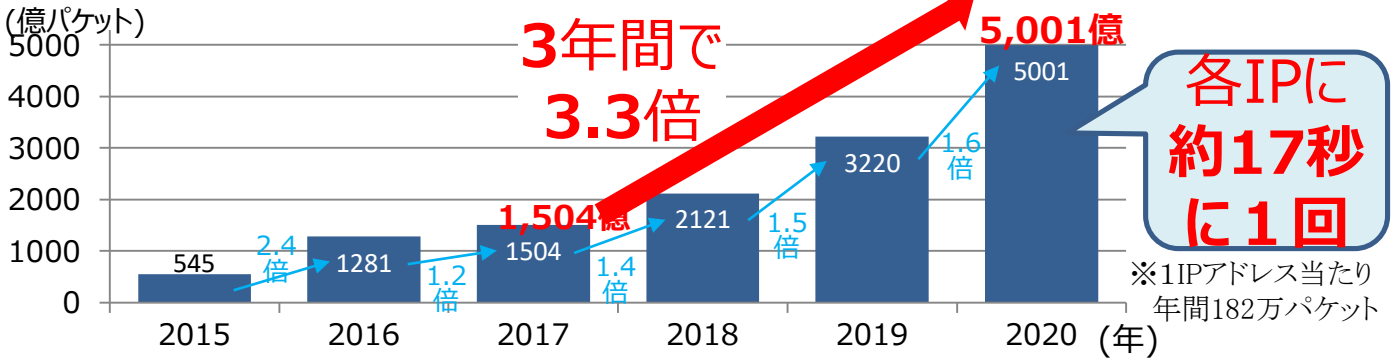
（参考）増加・多様化するサイバー攻撃

➢ 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

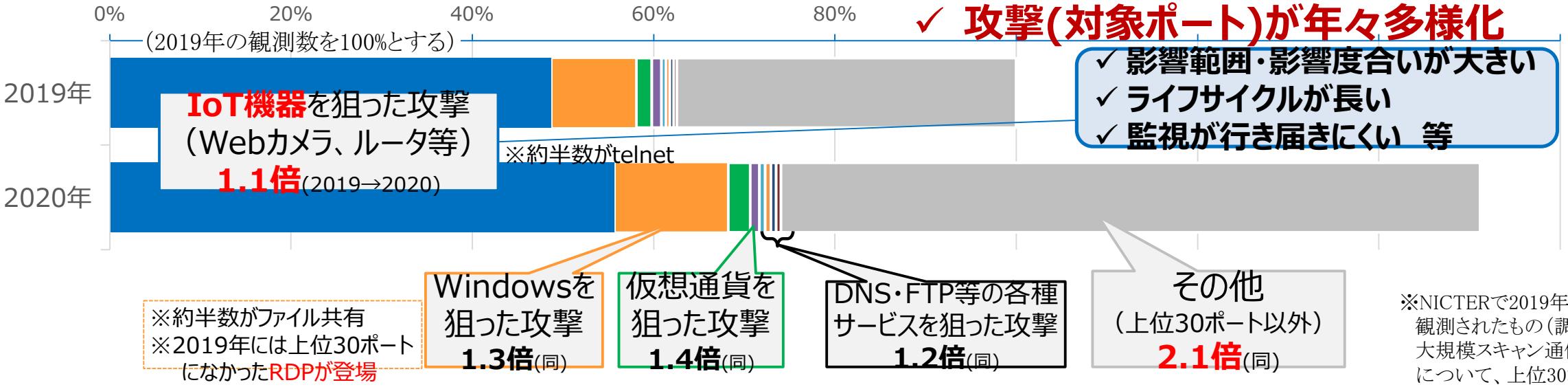


NICTERで１年間に観測されたサイバー攻撃関連の通信数



NICTERにより観測された通信の内容（上位30ポートの分析）

✓ **IoT機器を狙った攻撃が依然としてトップ**
✓ **攻撃(対象ポート)が年々多様化**



※NICTERで2019年・2020年に観測されたもの（調査目的の大規模スキャン通信を除く。）について、上位30ポートを分析。

②5Gの本格的な普及に向けたセキュリティ対策の強化

5Gのセキュリティについて、セキュリティ・バイ・デザインの観点から、総合的な対応を推進。

①脆弱性の検証手法や体制の確立		● ソフトウェア化が進む5Gネットワークの脆弱性を明らかにするための技術的検証や、通信ネットワークでも利用されるハードウェアの脆弱性（チップの脆弱性）を発見するための手法に関する技術的検証を実施。 ● 脆弱性検出技術の成果を活用（技術移転を含む）し、関連する脅威の分析の視点を踏まえた5Gシステムや利用者に対するインパクト分析を実施し、必要なセキュリティ対策に反映。 ● 上記の検証・分析の取組に関し、5Gの事業者・運用者やベンダー、研究機関等が協力して実施する体制を確立。
②脆弱性の情報共有の促進		● （一社）ICT-ISACの「5Gセキュリティ推進グループ」において、事業者・運用者間で5Gのリスク情報や脅威情報などの共有を推進。
③対策の促進	規制的措置	● サプライチェーンリスク対応を含む十分なサイバーセキュリティ対策を講じることを全国5Gの開設計画の認定及びローカル5Gの免許の条件とし、対策の実施状況について定期的にフォローアップ。
	振興的措置	● 全国5G及びローカル5Gの導入事業者に対する税制優遇措置等により、安全・安心な5Gシステムの普及を支援。

③テレワークセキュリティガイドラインの改定

- 総務省では従来から「**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**を示してきた。
  → テレワークを取り巻く環境やセキュリティ動向の変化に対応するため**2021年５月**に**全面的に改定**
- ガイドラインを補完するものとして、セキュリティの専任担当がいないような中小企業等においても、テレワークを実施する際に**最低限のセキュリティ**を**確実に確保**してもらうための**チェックリスト・設定解説**も策定・公表。

テレワークセキュリティガイドライン
（2021年５月　第５版）

2004年12月初版
2006年４月第２版
2013年３月第３版
2018年４月第４版

- ✓ テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針
- ✓ 中小企業を含む全企業を対象
- ✓ システム管理者のほか経営層や利用者(勤務者)を幅広く対象

ガイドラインに記載の内容について、理解や検討が難しい場合

中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)
（2021年５月　第２版）　2020年９月初版

中小企業等に向け**最低限のセキュリティを確実に確保**してもらうためのものに限定

【想定読者像】
- ✓ システム管理担当者向け
- ✓ 専任の担当・部門は存在しない
- ✓ 基本IT用語は聞いたことがあるレベル
- ✓ 設定作業は検索しながら実施可能

テレワークで活用される代表的なソフトについて、**設定解説資料**を作成し、具体的な設定を解説

【設定解説資料の対象】
CiscoWebexMeetings／Microsoft Teams／Zoom／Windows／Mac／iOS／Android／LanScope An／Exchange Online／Gmail／Teams_chat／LINE／OneDrive／Googleドライブ／Dropbox／YAMAHA VPN ルータ／CiscoASA／Windowsリモートデスクトップ接続／Chrome リモートデスクトップ／Microsoft Defender／ウイルスバスター ビジネスセキュリティサービス

テレワークセキュリティガイドラインの改定（2021年５月）

【テレワーク環境・セキュリティ動向の変化】

- ✓ テレワークは「一部の従業員」が利用するものから、Web会議を含め、一般的な業務・勤務形態に
- ✓ クラウドサービスの普及やスマートフォン等の活用が進むなど、システム構成や利用形態が多様化
- ✓ 標的型攻撃等の高度な攻撃が増え、従来型のセキュリティ対策では十分対応できない状況も発生

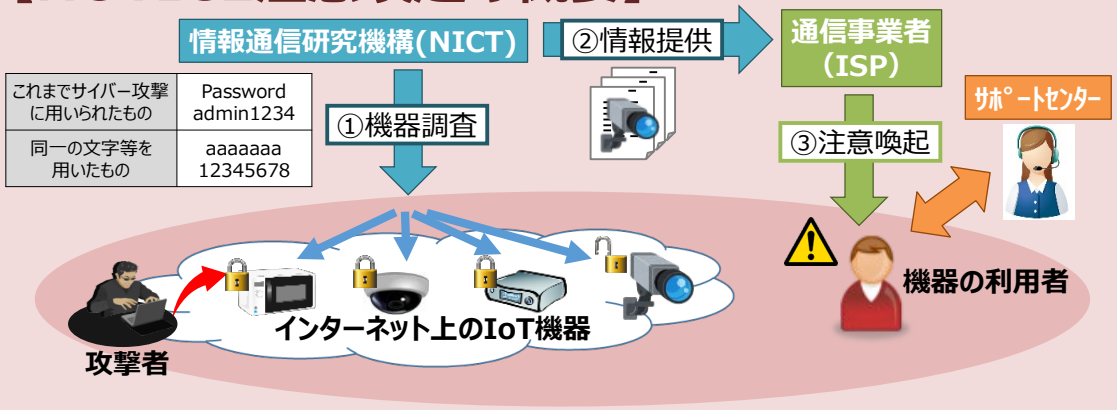
【ガイドライン改定の主要なポイント】

- ✓ テレワーク方式を再整理し、適した方式を選定するフローチャートや特性比較を掲載
- ✓ クラウドやゼロトラスト等のセキュリティ上のトピックについても記載
- ✓ 経営者・システム管理者・勤務者の立場それぞれにおける役割を明確化
- ✓ 実施すべきセキュリティ対策の分類や内容を全面的に見直し
- ✓ テレワークセキュリティに関連するトラブルについて、具体的事例を含め全面見直し
  （事例紹介のほか、セキュリティ上留意すべき点や、採るべき対策についても明示）

④IoT機器調査及び利用者への注意喚起

- 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。

【NOTICE注意喚起の概要】

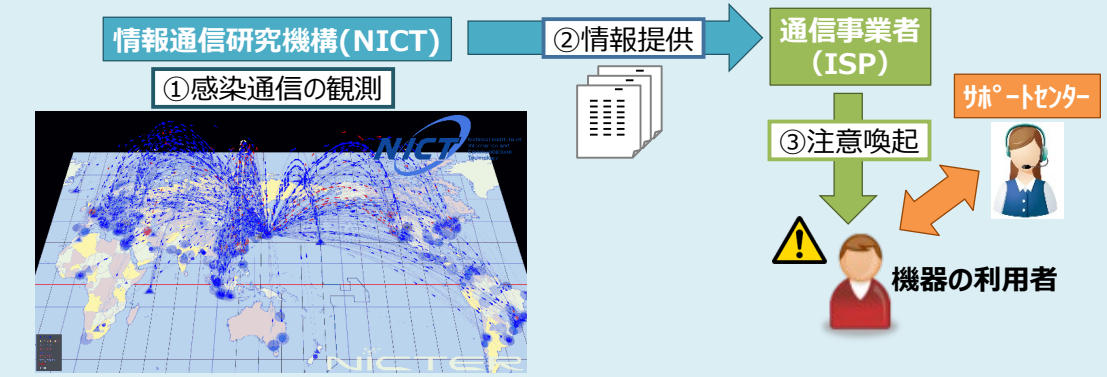


調査対象：パスワード設定等に不備があり、**サイバー攻撃に悪用されるおそれのある**IoT機器

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

⑤クラウドのセキュリティ

■総務省では、安全・安心なクラウドサービスの利活用推進のため、2014年に「クラウドサービス提供における情報セキュリティ対策ガイドライン」を策定し、2018年に改定（第2版）。

■今般、クラウドサービスを取り巻く環境の変化を踏まえ、クラウドサービスにおける責任分界のあり方や国際規格等との整合性の観点から、当ガイドラインの改定を検討し、2021年9月に「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」としてとりまとめた。

改定のポイント①

SaaS/PaaS/IaaSの特性や、クラウドサービス提供におけるクラウドサービス同士の相関性を踏まえた責任分界のあり方について追記

改定のポイント②

上述の責任分界に関する整理を踏まえ、

- ✓ SaaS/PaaS/IaaSを提供するクラウドサービス事業者で共通的に実施が求められる情報セキュリティ対策
- ✓ SaaSを提供するクラウドサービス事業者に実施が求められる情報セキュリティ対策
- ✓ PaaS/IaaSを提供するクラウドサービス事業者に実施が求められる情報セキュリティ対策

の3つのパターンに整理する形で当ガイドラインの章構成を見直し

改定のポイント③

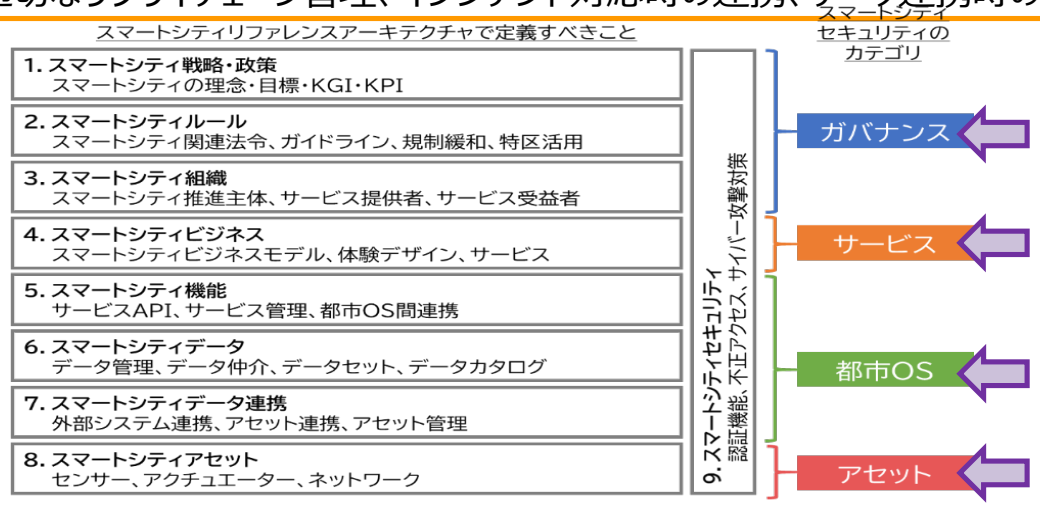
国際規格（ISO/IEC27017:2016）やNIST SP800-53 rev.5において記載されているセキュリティ対策と整合性をとる形で、当ガイドラインに記載されているセキュリティ対策の内容を見直し

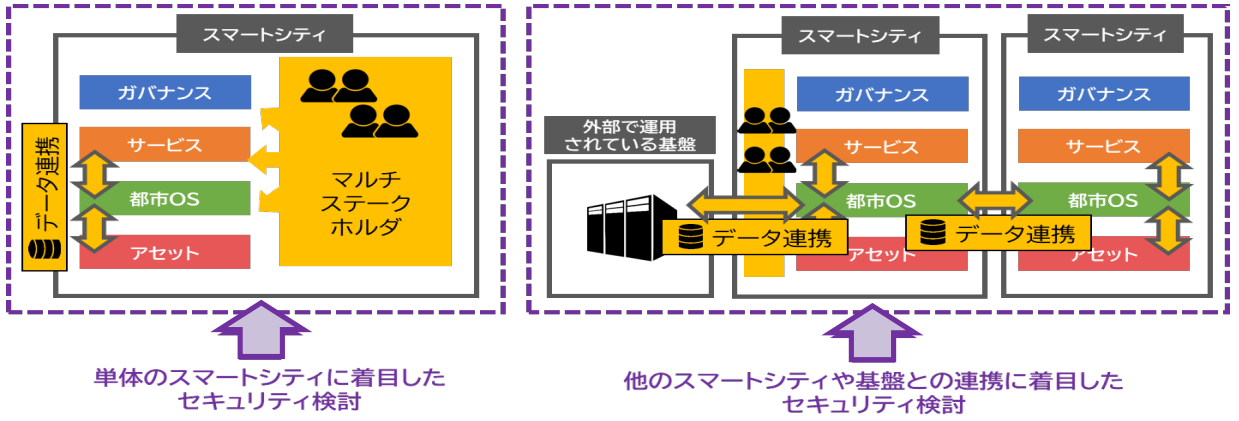
⑥スマートシティのセキュリティ

■「スマートシティセキュリティガイドライン」は、スマートシティの推進のための指針として、多様な関係主体が講じるべきセキュリティ対策や留意事項等を示したもの。令和２年10月に第1.0版を公表した後、内容のブラッシュアップを進め、令和３年６月に改定した第2.0版を公表。

■ガイドラインでは、スマートシティの構成要素(※)をセキュリティの観点から４つのカテゴリ（＝ガバナンス、サービス、都市OS、アセット）に分類し、　各カテゴリごとに想定されるセキュリティ上のリスクやセキュリティ対策を記載。（※:「スマートシティリファレンスアーキテクチャ」で定義されている各階層）

■また、「マルチステークホルダが複雑に関与」「多様なデータの連携」といったスマートシティの特徴を踏まえ、スマートシティ特有のセキュリティ対策を　３つに分類して（＝適切なサプライチェーン管理、インシデント対応時の連携、データ連携時のセキュリティ確保）、リスクや具体的な対策を記載。





上述の４つのカテゴリそれぞれにおけるリスクやセキュリティ対策を記載

ガバナンス
- ✓ セキュリティに関するポリシー策定
- ✓ マルチステークホルダへのポリシー浸透
- ✓ ガバナンス維持のための取組

サービス
- ✓ それぞれのサービスにおけるリスクアセスメント
- ✓ 外部からの攻撃等を防ぐセキュリティ対策
- ✓ インシデント発生防止のためのセキュリティ対策
- ✓ インシデント発生時に備えたセキュリティ対策

都市OS
- ✓ 外部からの攻撃等を防ぐセキュリティ対策
- ✓ インシデント発生防止のためのセキュリティ対策
- ✓ インシデント発生時に備えたセキュリティ対策
- ✓ 適切なクラウドサービスの利用

アセット
- ✓ アセットの監視・管理
- ✓ アセットそのものへのセキュリティ対策

スマートシティの特徴を踏まえ、スマートシティ特有のセキュリティ対策として
以下の３つに分類し、それぞれにおけるリスクやセキュリティ対策を記載

適切なサプライチェーン管理
- ✓ サプライチェーン全体のリスク・脆弱性情報の管理・把握
- ✓ 委託先のセキュリティ管理体制評価

インシデント対応時の連携
- ✓ インシデント対応体制の構築
- ✓ インシデント対応手順の整備
- ✓ インシデント対応訓練・演習の実施

データ連携時のセキュリティ
- ✓ データ連携元・連携先のセキュリティ管理体制評価
- ✓ 認証とアクセス制御の実施
- ✓ データ利用時の透明性、信頼性の担保、匿名化・秘匿化
- ✓ APIのセキュリティ確保

■　その他、補助コンテンツとしてスマートシティセキュリティ導入チェックシートやリスク一覧、セキュリティ対策一覧などを掲載

■　本ガイドラインをさらに読みやすくした「スマートシティセキュリティガイドブック」も本ガイドラインと同時に公表

⑦セキュリティ人材の育成

➢ 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（ＮＩＣＴ）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。

CYDER Cyber Defense Exercise with Recurrence（サイダー）

cyber colosseo（サイバーコロッセオ）

SecHack365（セックハック365）

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）
2017年度以降で、延べ**11,413名**が受講
2021年度から、オンライン受講コースを開設するとともに、準上級コースを開設

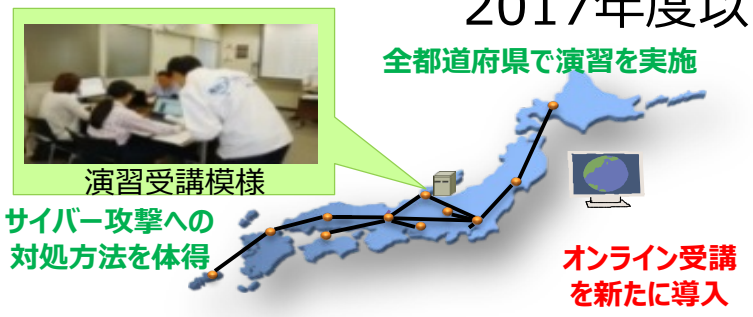
サイバーコロッセオのレガシーとして、準上級コースを制作

2020年東京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

⇒ 2017年度から開始し、2020年12月で事業完了
期間中に、**演習形式**で延べ**571**名、**講義形式**で延べ**1,717名**の人材を育成

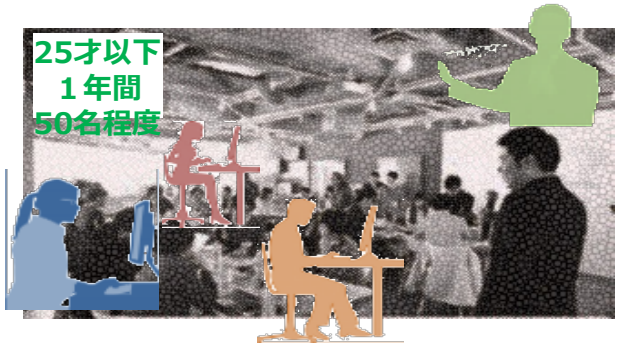
25歳以下の若手セキュリティイノベーターの育成

⇒ **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
2017年度以降で、計**171名が修了**



実事案に対処可能な人材育成
CYDER

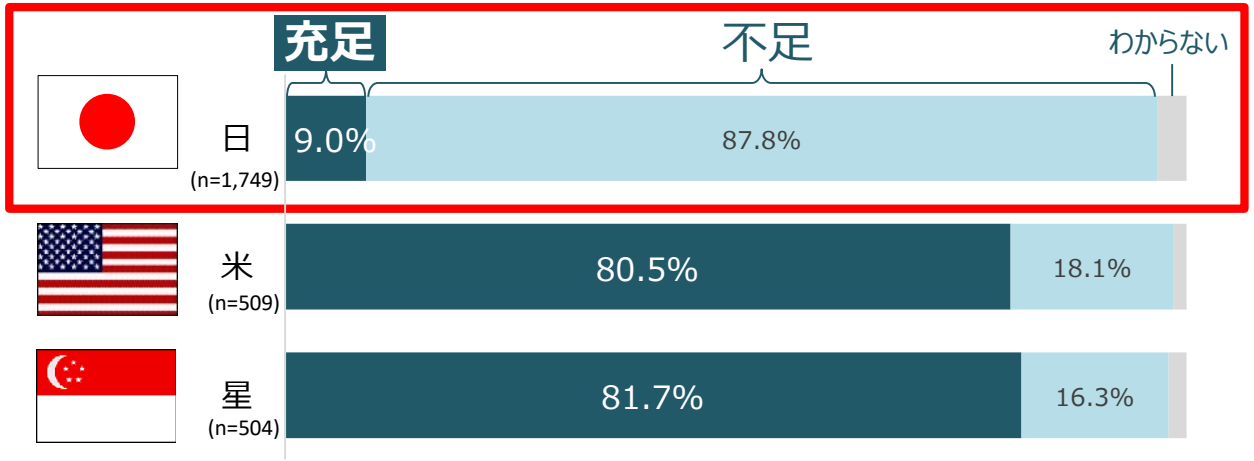
高度な攻撃に対処可能な人材育成
サイバーコロッセオ



ハイレベル層の人材育成
SecHack365

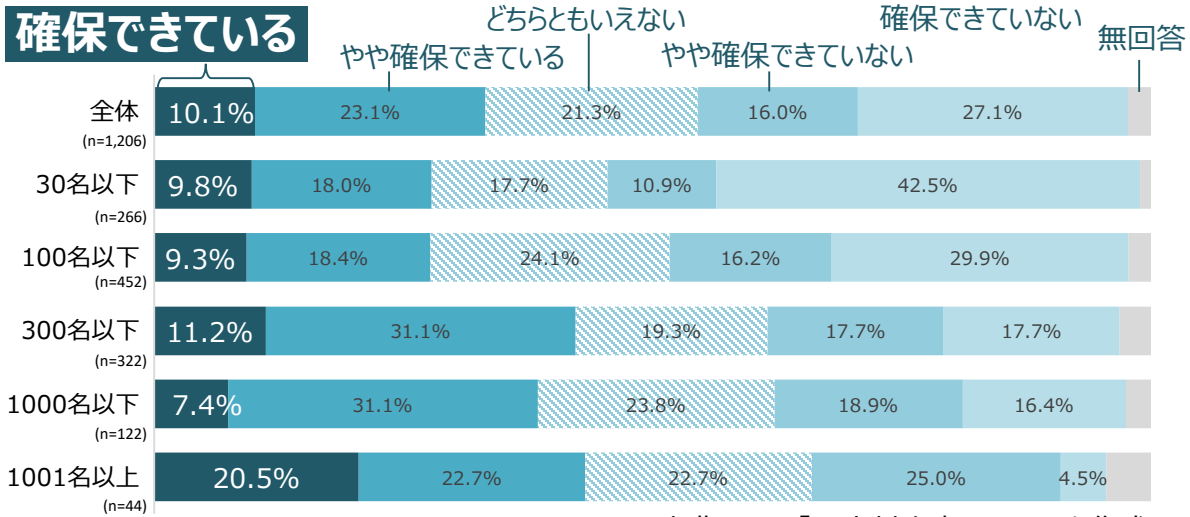
（参考）セキュリティ人材の不足

セキュリティ対策に従事する人材の充足状況



出典：NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2019」より作成

IT企業のセキュリティ専門技術者の確保状況



出典：IPA「IT人材白書2019」より作成

今後の投資を要するセキュリティ対策

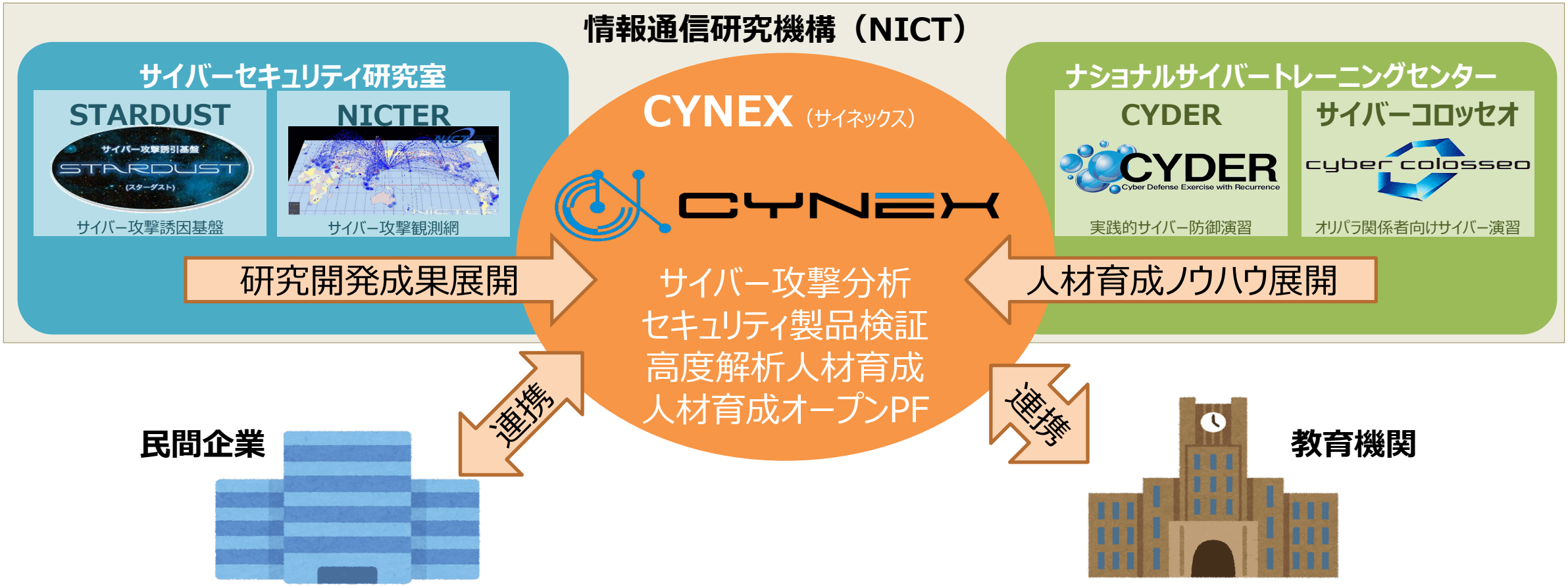
(n=313)

サイバーセキュリティ人材の育成	**56.2%**
セキュリティ監視の強化	52.1%
内部不正対策	50.5%
IoT／クラウド環境におけるセキュリティ対策	49.5%
インシデント対応体制（CSIRT）の強化	43.5%
モバイルデバイスの保護	43.1%
マルウェアやランサムウェア対策	40.6%
事業継続管理	39.3%
サイバーセキュリティ経営体制の構築	32.3%
脆弱性診断やペネトレーションテスト	30.0%
Webサイトやインターネット公開システムの保護	24.9%
外部委託先管理	24.6%
制御システム環境におけるセキュリティ対策	22.0%
プリバシー情報の保護	17.9%
ブロックチェーン／仮想通貨の利用環境におけるセキュリティ対策	4.5%
その他	1.9%
特にない	1.3%

出典：KPMGコンサルティング・EMCジャパンRSA「サイバーセキュリティサーベイ2019」より作成

⑧サイバーセキュリティに関する産学官の結節点『CYNEX』

- 情報通信研究機構（NICT）では、これまでも次のような取組を実施
  サイバーセキュリティ研究室・・・最先端のサイバーセキュリティ関連技術の研究開発を実施
  ナショナルサイバートレーニングセンター・・・実践的サイバー防御演習等による人材育成を実施
- これらの知見を活用し、サイバーセキュリティに関する産学官の巨大な結節点となる先端的基盤として
  ＣＹＮＥＸ（CYbersecurity NEXus：サイネックス） を構築



⑨サイバーセキュリティ分野における国際連携

①二国間・多国間連携

総務省のサイバーセキュリティ政策について、積極的な対外発信と連携強化を推進

○二国間連携
- インターネットエコノミーに関する日米政策協力対話
- 日EU・ICT政策対話・戦略ワークショップ
- その他、豪、中韓、英、仏を含む13か国等とのサイバー協議
- イスラエルの国家サイバー総局との間で協力覚書を締結　等

○多国間連携
- ITU-T SG17 等（標準化活動）

○官民連携
-Charter of Trust 等

石田総務大臣とベンアリ駐日イスラエル大使による覚書署名式（2018年11月）

②民間組織の国際連携の推進

○ ISP向け日ASEAN情報セキュリティワークショップ

日本とASEAN各国のISP事業者等との情報共有等の推進

○ 日米ISAC連携ワークショップ

日米の情報通信分野ISAC間における情報共有の推進。ICT-ISACと米国IT-ISACは、2019年11月に協力覚書を締結。

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

③能力構築支援

○ 日ASEANサイバーセキュリティ能力構築センター（AJCCBC）

AJCCBC ASEAN JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE Partnership by ASEAN and Japan

日・ASEAN統合基金（JAIF）を活用したASEAN域内のセキュリティ人材育成（４年間で700人程度を育成する目標）の拠点となるセンターで、2018年９月にタイで開所。ASEAN域内で高い評価を得ている。

■ 研修プログラムの概要

1. サイバーセキュリティ演習

政府機関や重要インフラ事業者等に対し、実践的サイバー防御演習（CYDER）等のプログラムを実施（年6回程度）

2. Cyber SEA Game

若手技術者・学生がサイバー攻撃対処能力を競う大会の開催（年１回）

■ 活動内容のオンライン化

新型コロナウイルス感染症拡大に伴う移動制限等を受け、上記研修プログラムのオンライン化を進めるとともに、①自己学習教材コース、②実践的解析演習コースのオンライン提供を開始。

■ 第三者との連携を通じた活動内容の拡充

欧米や国際機関等に対して、研修プログラムや講師の提供を募る予定。研修内容の拡充による日本とASESAN諸国との連携の深化に加え、日本と欧米等との連携の強化及び信頼醸成を図る。

1．サイバーセキュリティ戦略

2．総務省のサイバーセキュリティに関する取組

3．地域におけるセキュリティコミュニティ形成

地域セキュリティコミュニティの形成促進

■ 総務省、経済産業省が互いに連携しつつ、地域単位の事業者のセキュリティ対策の強化のため、地域に根付いたセキュリティコミュニティ（地域SECUNITY（セキュニティ））の形成の促進を図る。

● 全国規模で事業展開する企業に比べ、地域の企業や地方公共団体などについては、有効なサイバーセキュリティ対策をとるための人材育成・普及啓発の機会や情報共有の枠組みなどが不足しているおそれ。

➡

● 地域の企業や地方公共団体については、各者とも単独で有効なサイバーセキュリティ対策をとることは困難であり、地域レベルでのコミュニティを形成して情報共有等を強化する必要がある。

地域に根付いたセキュリティコミュニティ

セキュリティ関連の情報共有

定期的なセミナーや演習等の実施

セキュリティコミュニティの形成の促進

● ①当該地域における大手事業者、②業界団体（地方支部など）、③都道府県警、④サイバーセキュリティ関係事業者・機関、⑤地方公共団体、⑥有識者などによる地域のサイバーセキュリティ向上のための推進体制を構築する。なお、情報共有体制がすでに存在している地域においては、既存の体制を活用していくことが望ましい。

● 地域の企業等向けに①定期的なセミナーやインシデント演習の実施、②セキュリティ関連の情報共有の枠組みなどを構築。

（参考）地域の中小企業における課題

■ コロナ禍におけるテレワークやWeb会議の普及、デジタル化の進展に伴って、企業の所在や規模に関わらず、サイバーセキュリティに関するリスクが増大しており、約２割の企業が、直近半年以内にサイバー攻撃による被害を受けている（→図１）。

■ しかし、大都市圏を除く各地域に所在する中小企業では、大企業に比べて、サイバーセキュリティに関するリスクの増大を認識していない企業や、対策が不十分である企業が多い（→図２）。

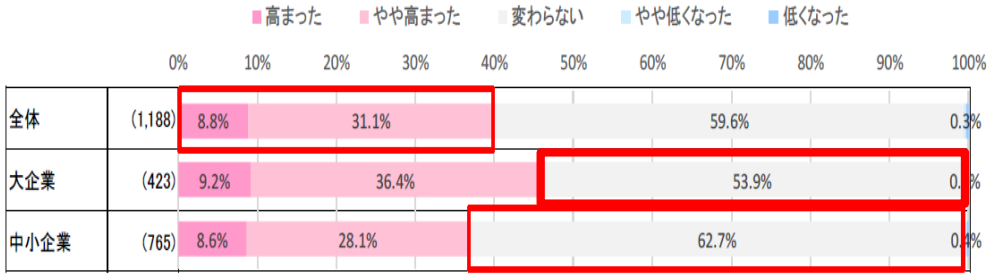
■ 対策が不十分にとどまっている理由としては、予算不足、人材不足、情報不足が挙げられている（→図３）。

（図１）直近でサイバー攻撃被害を受けた時期

	半年以内	１年以内	３年以内	５年以内
大企業	16.9%	13.5%	27.0%	13.5%
中小企業	19.8%	16.4%	22.4%	25.0%

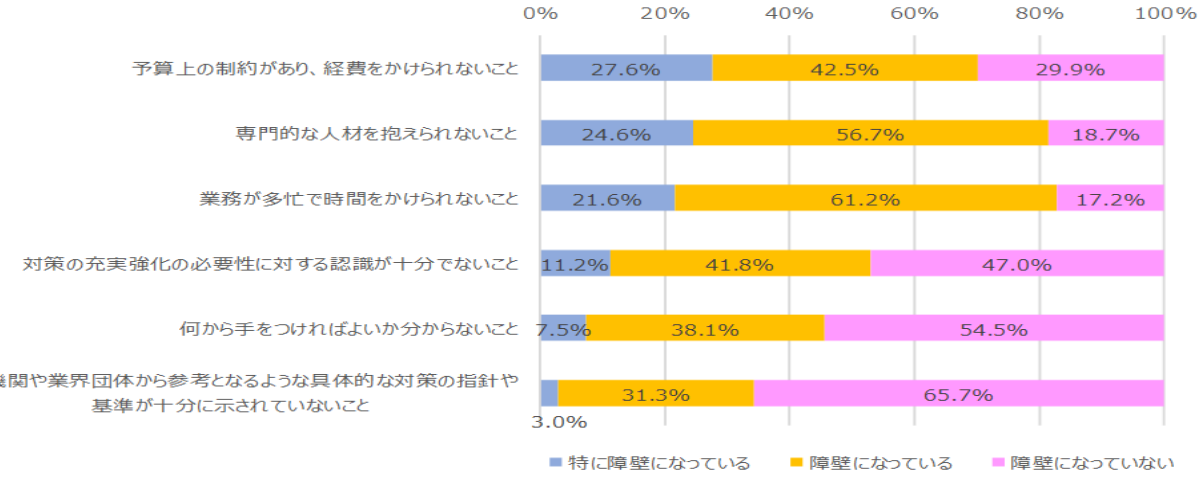
（出典）国内企業のサイバーリスク意識・対策実態調査2020（（一社）日本損害保険協会、2020年12月）

（図２）新型コロナ感染拡大以後のセキュリティリスク認識



（図３）セキュリティ対策を充実強化する際の障壁

（出典）令和2年度地域の放送事業者・電気通信事業者等を対象としたサイバーセキュリティ対策に関するアンケート調査結果（総務省委託調査、2021年2月）



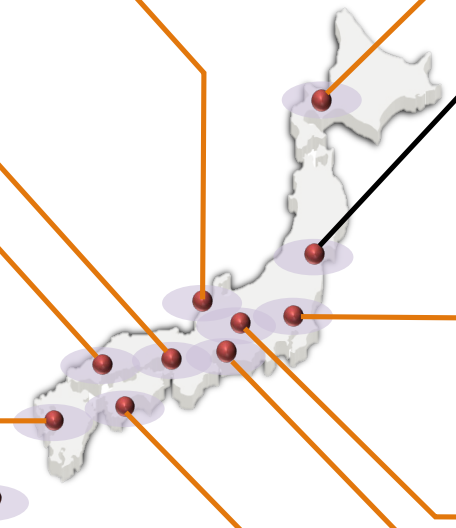
地域のセキュリティコミュニティの現状

関西サイバーセキュリティ・ネットワーク
【事務局】近畿総合通信局、近畿経済産業局、(一財)関西情報センター（2018年10月設立）

北陸サイバーセキュリティ連絡会
【事務局】北陸総合通信局（2020年3月設立）

北海道地域情報セキュリティ連絡会（HAISL）
【事務局】北海道総合通信局、北海道経済産業局、北海道警察本部（2014年9月 設立）

中国地域サイバーセキュリティ連絡会
【事務局】中国総合通信局、中国経済産業局（2020年10月設立）



東北地域サイバーセキュリティ連絡会
【事務局】東北総合通信局、東北経済産業局（2021年10月 設立）

関東サイバーセキュリティ連絡会
【事務局】関東総合通信局、関東経済産業局（2021年3月設立）

九州・沖縄地域情報セキュリティ推進連絡会議
【事務局】九州総合通信局、九州経済産業局（2012年5月設立）

信越地域のサイバーセキュリティコミュニティ（仮）
【事務局】信越総合通信局、関東経済産業局（2021年中 設立予定）

沖縄サイバーセキュリティネットワーク
【事務局】内閣府沖縄総合事務局、沖縄総合通信事務所、沖縄県警察本部（2015年3月設立）

サイバーセキュリティシンポジウム道後
【事務局】（一社）テレコムサービス協会四国支部、四国総合通信局（共催）、他複数団体が共催（2012年10月設立）

東海サイバーセキュリティ連絡会
【事務局】東海総合通信局、中部経済産業局（2020年8月設立）

（参考）各地域コミュニティの取組

全国共通

◇セミナー及びインシデント対応演習の開催

・全国各地において、サイバーセキュリティに関するセミナーやインシデント対応演習を開催し、普及啓発や意識向上を図っている。
・今年度は、全国あわせて25件開催予定。

北海道ブロック

◇若手人材育成

・学生や青年層向けに、サイバーセキュリティに関する知見や技術を教授し、将来のセキュリティリーダー、ホワイトハッカーになり得る人材の発掘と育成を目的としたプロジェクトとして、SC４Y（Security College for Youth）を公立千歳科学技術大学で開催。

北陸ブロック

◇CTF（Capture The Flag）の開催

・地域の若年層等を対象として、サイバーセキュリティに興味を持ち、セキュリティエンジニアになるためのスキルアップに向けた知識の習得等を目的として、楽しみながらサイバーセキュリティを学ぶ競技を中心とするイベントを開催。
（1/29（土）@鯖江）

近畿ブロック

◇地方都市におけるイベント

・地域の企業、団体等の方を対象にサイバー攻撃の現状や対策など「サイバーセキュリティ」に関するミニ講演と素朴な疑問や相談を気軽にできるよう“座談会”的な地域密着型のイベントを開催（奈良、豊岡）

ご清聴ありがとうございました。

i.hirose@soumu.go.jp

総務省
Ministry of Internal Affairs and Communications