資料23－４

取りまとめの方向性について

サイバーセキュリティタスクフォース事務局

令和元年４月１６日

これまでの議論について

■ 過去７回のサイバーセキュリティタスクフォースにおいて、「IoT・5Gセキュリティ総合対策」の策定・公表以降のサイバーセキュリティ政策の在り方について御検討いただいていたところ。

回　次	議　事　内　容
第16回 （R元.11.1）	✓ 今後の検討課題等 ✓ 昨今のサイバーセキュリティの現状等
第17回 （R元.11.22）	✓ 今後の検討課題とスケジュール ✓ IoTのセキュリティ対策 ✓ 人材育成の推進 ✓ 情報共有の促進
第18回 （R元.12.5）	✓ 前回までの御議論 ✓ Wi-Fiのセキュリティ対策 ✓ 総務省所管分野のサイバーセキュリティ対策
第19回 （R元.12.25）	✓ 前回までの御議論と今後の進め方等 ✓ 研究開発の推進
第20回 （R2.1.27）	**✓ 我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項[緊急提言]（案）** ✓ 研究開発の推進
第21回 （R2.2.20）	✓ 地域のセキュリティコミュニティの形成 ✓ スマートシティのセキュリティ ✓ 研究開発の推進
第22回 （R2.3.18）	**✓ IoT・5Gセキュリティ総合対策の進捗状況と今後の取組** ✓ 国際標準化の現状

短期的な検討課題についての検討結果を第20回（1/27）で御議論いただき、28日付で緊急提言として公表

短期的な検討課題

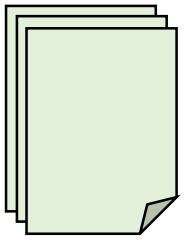
中長期的な検討課題

「IoT・5Gセキュリティ総合対策」の進捗状況と今後の取組を「プログレスレポート」としてまとめて公表予定。

取りまとめの方向性（案）

■ タスクフォースでの御議論や昨今のサイバーセキュリティの現状を踏まえ、2019年（令和元年）８月に公表した「IoT・5Gセキュリティ総合対策」を改定する方向性を検討。

IoT・5Gセキュリティ総合対策



【具体的に取り組むべき課題・施策の項目】

Ⅰ 背景
（１）ICT利活用の進展
（２）サイバーセキュリティリスクの増大や脅威の深刻化

Ⅱ 施策展開の枠組み

Ⅲ 情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策
（１）IoTのセキュリティ対策
（２）5Gのセキュリティ対策
（３）クラウドサービスのセキュリティ対策
（４）スマートシティのセキュリティ対策
（５）トラストサービスの在り方の検討
（６）公衆無線LANのセキュリティ対策
（７）重要インフラとしての情報通信分野のセキュリティ対策
（８）地域の情報通信サービスのセキュリティの確保

Ⅳ 横断的施策
（１）研究開発の推進
（２）人材育成・普及啓発の推進
（３）国際連携の推進
（４）情報共有・情報開示の促進

①「Ⅰ　背景」の部分で、これまでのタスクフォースでの御議論や昨今のサイバーセキュリティの現状を踏まえた**主要な課題認識と対応の方向性**をトピックとして特出しし、**それを踏まえて総合対策を改定**する方向性でどうか。

反映

②「Ⅲ　情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策」「Ⅳ　横断的施策」の部分では、柱立ての基本的な構造は維持しつつも、**①で示した主要な課題認識と対応の方向性**や、**１月に策定いただいた緊急提言**などを踏まえて**施策内容の現行化及び新たな取組を追加**してはどうか。

本日は①の主要な課題認識と対応の方向性について御議論をいただきたい。

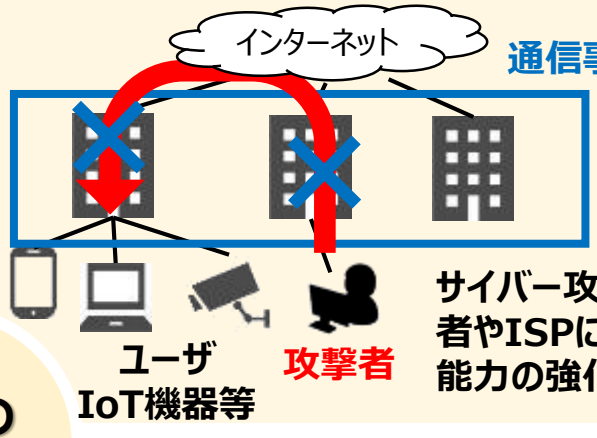
総合対策の改定に当たっての主要な課題認識と対応の方向性

■ 総合対策の改定に当たり、以下の主要な課題認識と対応の方向性を踏まえるべきではないか。

① 5Gセキュリティ対策の更なる強化

5G時代を見据え、多面的アプローチで対策を推進

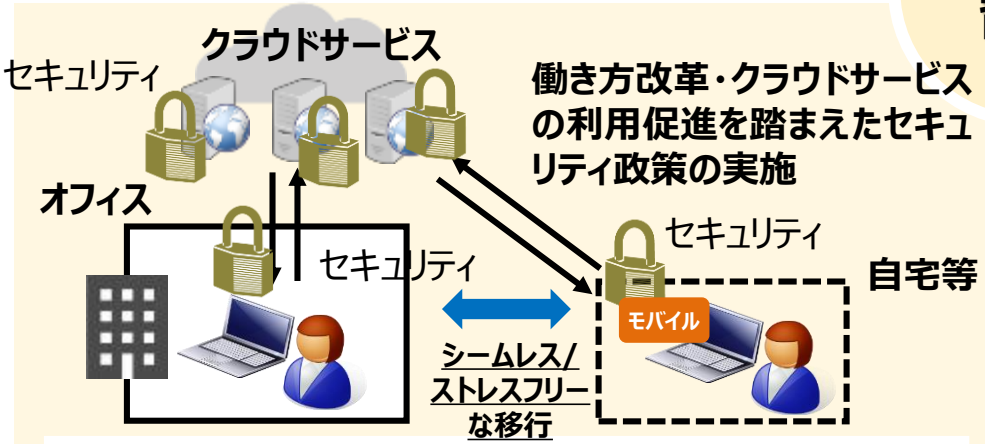
② Active Network Securityの実現



サイバー攻撃が経由する通信事業者やISPにおける分析能力/対処能力の強化を通じ、対策を促進

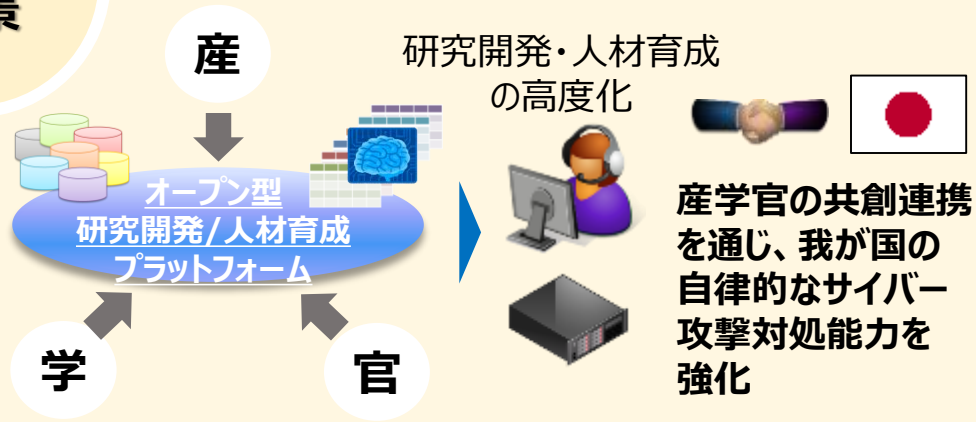
改定の背景

③ クラウド・リモート時代のセキュリティ確保



働き方改革・クラウドサービスの利用促進を踏まえたセキュリティ政策の実施

④ 共創的研究開発/人材育成基盤の構築



産学官の共創連携を通じ、我が国の自律的なサイバー攻撃対処能力を強化

① 5Gセキュリティ対策の更なる強化【背景】

■ 令和2年以降、5Gの運用が始まっていく中で、5Gのセキュリティ対策に関して官民で連携していくことが必要ではないか。

● 5Gをめぐる最近の動きについて

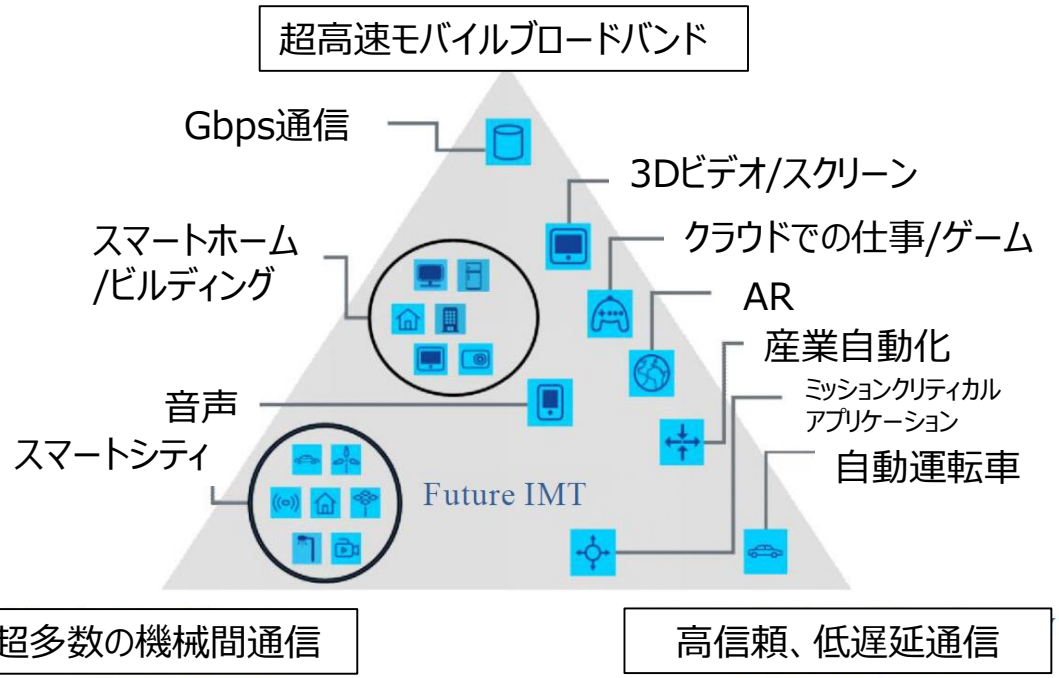
✓ 大手携帯電話事業者が一般向け5Gサービスを提供開始

✓ 令和2年１月には第1号のローカル5Gの予備免許が交付

✓ 多種多様な分野における5Gを利活用したサービスの実証実験・提供の開始

将来的には、社会における5G通信への依存性が、より拡大することが見込まれる

● 5Gのユースケースは将来的に様々な分野に拡大



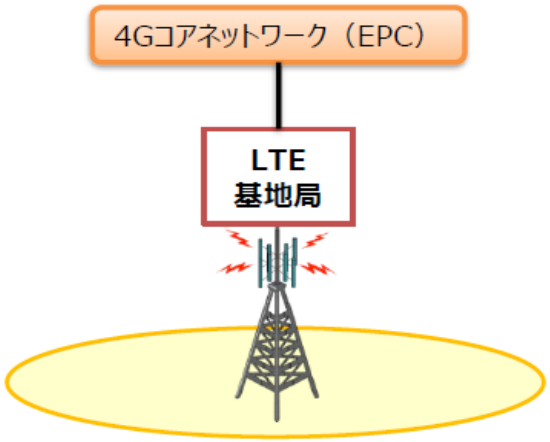
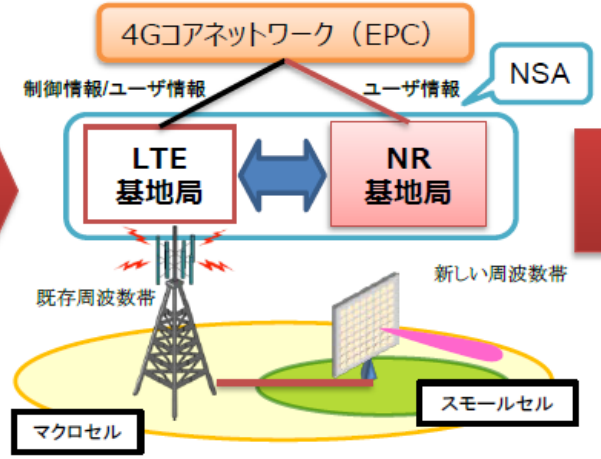
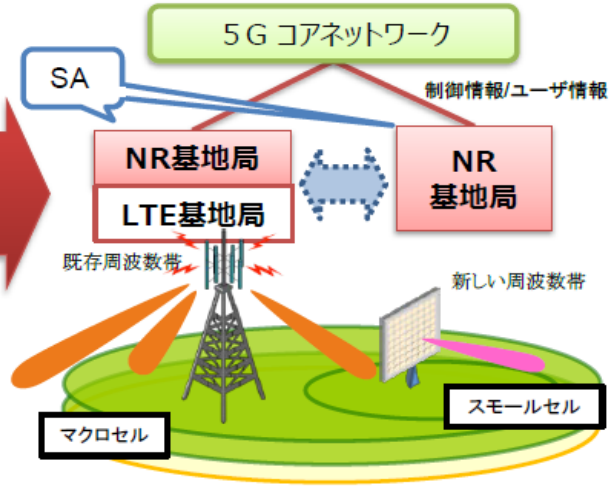
出典：IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond, Recommendation ITU-R M.2083-0

将来の社会基盤としての5Gの安全性や信頼性の確保のため、5G黎明期の現段階から、セキュリティ・バイ・デザインの観点で官民で連携して対策をとる必要がある。

① 5Gセキュリティ対策の更なる強化【背景】

- 我が国においては、5Gの導入の初期段階では4G対応のコアネットワークを活用したノンスタンドアロン5Gサービスの導入が予定されている。
- 他方、5Gの普及期に導入が想定されるスタンドアロン5Gについては、ネットワークそのもののリスクや脆弱性がこれまでと大きく変わる可能性もあることから、現段階でそのセキュリティの在り方についても検討を始めることが必要。

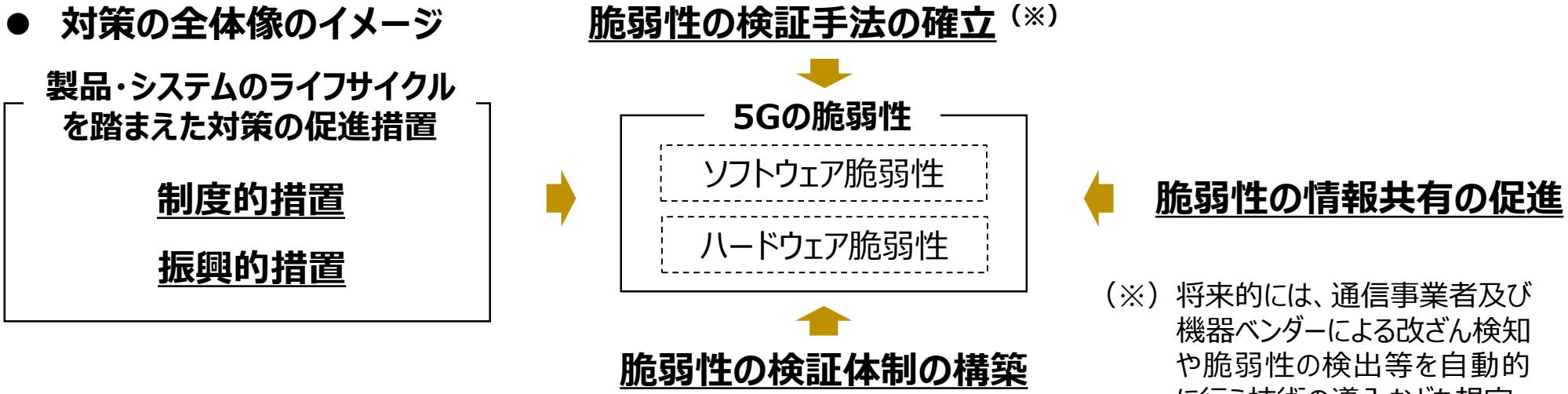
ノンスタンドアロン5G（NSA-5G）　**スタンドアロン5G（SA-5G）**

現在【LTEの面展開】	2020年【5G導入当初】	202X年【5G普及期】
		
● LTE、LTE-Advancedをベースとしたネットワーク構成であり、3GPPでの検討状況を踏まえ、上りCAの導入や256QAM導入などの高度化 ● 800MHz、2GHzなどの周波数帯を用いて、 スマートフォン向けサービスを念頭に、高いスループットを実現する面的なサービスエリアを展開 ● NB-IoTやeMTCなどのワイドエリア、省電力を特徴としたIoT技術を先行導入	● コストを抑えつつ、円滑な5G導入を実現するため、NR基地局とLTE基地局が連携したNSA構成のシステムが導入 ● 需要の高いエリア等を中心に、5G用周波数帯を用いた「超高速」サービスが提供され、eMTC/NB-IoT等によるIoTサービスが普及 ● 高い周波数帯の活用が進展するとともに、Massive MIMOなどの新たな技術の導入が加速	● 「超高速」、「多数同時接続」、「低遅延」の全ての要求条件に対応したサービスが提供 ● ネットワークスライシング等に対応した5Gコアネットワークが導入され、モバイル・エッジ・コンピューティング（MEC）の導入も進展 ● SA構成のNR基地局の導入が開始（NSA構成の基地局も併存）。既存周波数帯にもNR導入が進展 ● 広く普及しているLTEについては、継続的にサービスを提供 ● WRC-19で特定された周波数帯域も活用

① 5Gセキュリティ対策の更なる強化【方向性】

■ 5Gのセキュリティ確保については、脆弱性の検証や情報共有、それらを踏まえた対策の推進など、多面的な対策が必要ではないか。

● **対策の全体像のイメージ**



（※）将来的には、通信事業者及び機器ベンダーによる改ざん検知や脆弱性の検出等を自動的に行う技術の導入なども想定

（参考）過去の会合における構成員からの御意見

- ✓ ネットワーク機器等に安全保障上懸念されるバックドアが仕込まれていないかというのは民間企業の関心事項なので、IoT・5Gセキュリティ総合対策の観点から1つの軸として考えてみるべき。
- ✓ 5GやIoTのサプライチェーンにおいては、色々なモジュールがつながっていて、そこに発生するリスクとしてサプライチェーンリスクがあり、攻撃の機会が非常に広範囲になる。
- ✓ 脆弱性検知手法を開発したときに、いろいろなテストを実施すると思うので、是非そのテスト結果についての情報共有をお願いしたい。
- ✓ 5Gをきちんと普及させていく中で、安全性を担保していくにあたり、ある程度の規模感で解析を実施する必要がある。
- ✓ ソフトウェア化が着々と進んでいくという前提のうえで、一般の方々や企業、研究所の方々が使える検証ツールが日本ではまだまだ足りていない。

（参考）「Beyond 5G推進戦略」（令和2年4月14日～令和2年5月14日の間パブリックコメント中）におけるサイバーセキュリティの記述

研究開発戦略

● Beyond5G実現の鍵を握る**先端技術の早期開発を目指し、特に「つぼみ」の段階において国のリソースを集中的に投入**。

● あわせて、研究開発拠点の構築や大胆な電波開放等により**世界最高レベルの研究開発環境**を整備。

（具体的施策）

先端的な要素技術の研究開発

- Beyond5Gの中核技術となる先端的な要素技術の研究開発を、期間を限り、関係省庁と連携して集中的に推進。（→"参考１"）

Beyond 5G研究開発プラットフォームの構築

- エミュレーターや各種テストベッドの提供、共同研究の実施等により産官学が協働して研究開発を推進する場をNICT等に構築。（→米独で同様の取組）

研究開発促進税制の拡充

- 民間による研究開発促進のため、関係省庁との連携により拡充を実施。

電波の開放

- テラヘルツ波など高周波数帯域電波を一定期間、簡素な手続きにより原則として自由に使用できる仕組みを整備。
- 一定の条件を満たして行う実験等について実験等無線局免許の取得・変更手続きを大幅に緩和。

破壊的イノベーションの創出と人材育成

- 懸賞金など強力なインセンティブが付与される公募（「無線チャレンジ」）により、新奇なアイデアや人材を発掘・支援。

知財・標準化戦略

● 我が国が目指すBeyond5Gの実現と、**ゲームチェンジ**を目指し、知財取得と標準化活動の促進にコミット。

● 特に、**①オール光化、②オープン化、③最大限の仮想化、④上空・海上等への拡張、⑤セキュリティの抜本的強化**を重視。

（具体的施策）

戦略的な知財化・標準化の見極めとオープン化・デファクト化の推進

- 国による研究開発プロジェクトにおいて、我が国に強みがある技術のオープン・クローズド戦略を促進する仕組みを構築。
- オープン化・デファクト化に向けた機器開発に係る負担を軽減し、その促進を図るため、相互接続・相互運用テストベッドやエミュレータを国が整備。（→内外企業に開放）

戦略的パートナーとの連携体制の構築

- 研究開発の初期段階から国際共同研究を拡充し、国際標準化に向けた国際連携を強化。

標準化拠点の活用と戦略的な知財・標準化活動の促進

- 産官学の主要プレイヤーが参加し、戦略的に標準化等に取り組む場として「Beyond 5G知財・標準化戦略センター」を設置。
- 標準化と事業との間の紐づけの強化のため、研究開発プロジェクトの採択や新たな電波割当等において、オープン化規格の採用や国際標準化への貢献度・知財戦略を要件化。

展開戦略

● Beyond5Gの早期かつ円滑な展開のため、5Gがあらゆる分野や地域において浸透し、徹底的に使いこなされている**「Beyond5G ready」な環境の早期実現**を目指す。

● このため、5G基地局の面的拡大と5Gの産業・公的利用を強力に推進。

（具体的施策）

ネットワークの面的拡大

- 税制支援等により５G基地局の面的整備拡充とローカル５Gの導入を促進（2023年度末までに当初計画の３倍以上の基地局を整備し、全市町村でエリア展開）。
- ５Ｇ基地局の面的整備拡充のため、インフラシェアリングを促進。

サイバーセキュリティ常時確保機能の実現

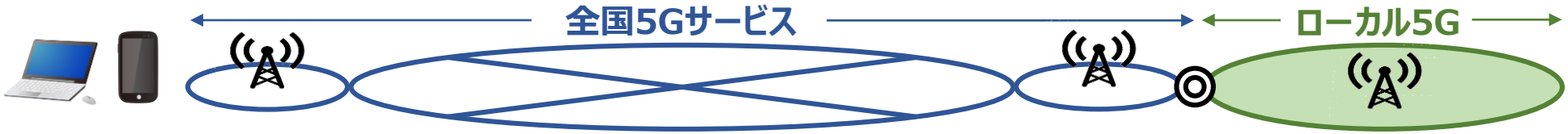
- セキュリティ・バイ・デザインに基づく規格策定、自動で改竄検知や脆弱性検出を行う技術の導入、量子暗号システムの社会実装等を推進。

課題解決に資するユースケースの構築・拡大

- 社会課題解決に向けた５Gソリューションを実証プロジェクトを通じて確立。特に、遠隔医療、遠隔教育、防災等のニーズの高い国と連携し、今後５年間での集中的な実証を実施。
- 地域の大学等を拠点に人材育成・開発、事業展開支援等を含めた体制を整備。
- スマートシティの各種機能等のソリューションモデルを、SaaSにより「５Ｇソリューションセンター」として提供。
- 一つの街を「リビング・テストベッド」として自由かつ柔軟な実証を実施できる環境を整備。（「スーパーシティ」構想など国家戦略特区を活用。）
- 緊急事態においてもICTにより国民生活や経済活動が円滑に維持される社会を実現するため、速やかに必要な制度見直し等を推進。

① 5Gセキュリティ対策の更なる強化【方向性】

- 今後の5Gのセキュリティ対策の全体像のイメージ



脆弱性の検証手法の確立

- 総務省において、将来の5Gのネットワーク（スタンドアロン5G）に関する脆弱性（ソフトウェアを含む）を明らかにするための技術的検証を実施
- 総務省において、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研究開発を実施

脆弱性の検証体制の構築

- 総務省において、関係省庁と連携し、5Gを含む情報通信分野で用いられる機器やサービスに関し、我が国独自の検証能力を獲得し、かつその能力を活用して検証活動を行うための体制を構築

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、5G（全国5G及びローカル5G）のリスク情報や脅威情報などを事業者間や運用者間で共有

対策の促進措置

制度的措置

- 総務省において、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
- なお、対策の実施に当たっては以下に留意

・「情報通信ネットワーク安全・信頼性基準」　・「政府機関等の情報セキュリティ対策のための統一基準群（平成三十年度版）」
・「ＩＴ調達に係る国の物品等又は役務の調達方針及び調達手続きに関する申合せ」（平成三十年十二月十日関係省庁申合せ）

開設計画の認定時の条件	免許交付時の条件

振興的措置

- 総務省・経済産業省（及びローカル5Gについては業所管省庁）において、法律上の認定スキームと連動した税制優遇措置により、セキュリティの確保された5G設備の早期導入を支援

（参考）特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律案の概要

■ **特定高度情報通信技術活用システム**（**全国及びローカル5G**、ドローン）の開発供給及び導入を促進するための措置を講ずることにより、サイバーセキュリティ等を確保しつつ特定高度情報通信技術活用システムの普及を図る。

【講ずる措置の全体像（イメージ）】

国/指針の策定

(総務省・経済産業省＋関係省庁)

【認定基準】

①安全性・信頼性
（セキュリティ、ベンダー企業の信頼性）

②供給安定性

③オープン性
（国際標準規格に準拠、グローバル連携）

システム導入事業者
（**通信キャリア**・製造事業者等）
（導入計画の作成）

申請 ⇒
⇐ 認定・支援

特定高度情報通信技術活用システム
①全国５G　②ローカル５G　③ドローン

開発供給事業者
（ベンダー）
（開発供給計画の作成）

申請 ⇒
⇐ 認定・支援

情報通信機器サプライチェーン
半導体　通信設備　ソフトウェア

事業所管大臣

■ 導入計画認定に基づく支援措置

- **５G投資促進税制**
（**税額控除15%、特別償却30%、固定資産税減免1/2(3年間)**※1）
- ツーステップローン※2
- 中小企業投資育成株式会社法特例
- 中小企業信用保険法特例

経産・総務大臣※3

■ 開発供給計画認定に基づく支援措置

- ツーステップローン※2
- 中小企業投資育成株式会社法特例
- 中小企業信用保険法特例

（参考）予算支援　※法律とは別途措置

・ポスト5G情報通信システム基盤強化研究開発事業
・地域課題解決型ローカル5G等の実現に向けた開発実証
・5Gの更なる高度化のための研究開発
・ドローン基盤技術開発事業　　等

※１：固定資産税については、ローカル５Gのみ
※２：ツーステップローンについては、５Gが対象
※３：ドローンについては、主務大臣は経産大臣

② Active Network Securityの実現【背景】

- IoTのセキュリティに関する対策は、これまでIoT機器の対策を中心にとられてきたところ。
- IoTを狙った攻撃は依然として多く、今後、様々な産業でIoT機器の利用が拡大することが予想される中、これまでの対策だけでは必ずしも十分ではないおそれがあるのではないか。

● IoT機器を狙った攻撃は依然として多い

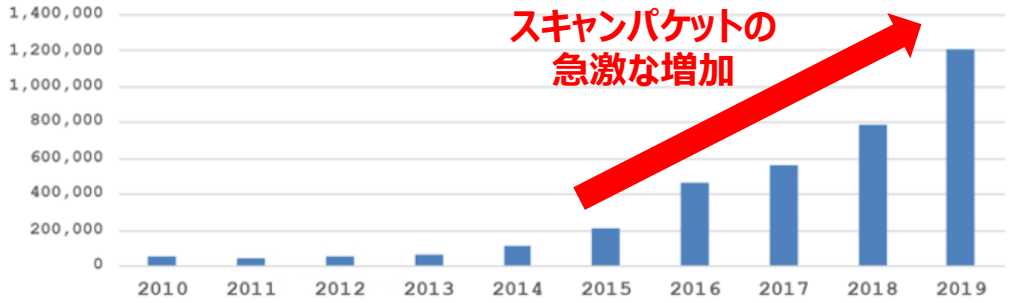
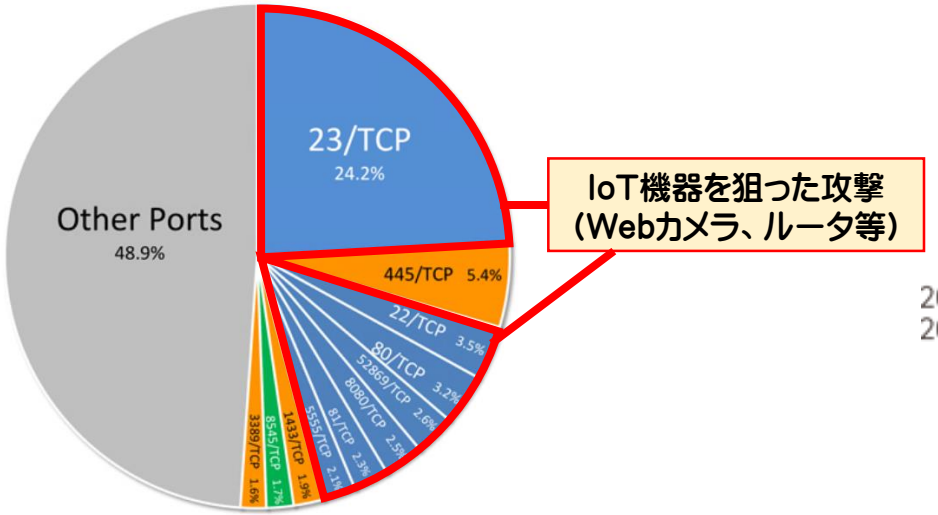
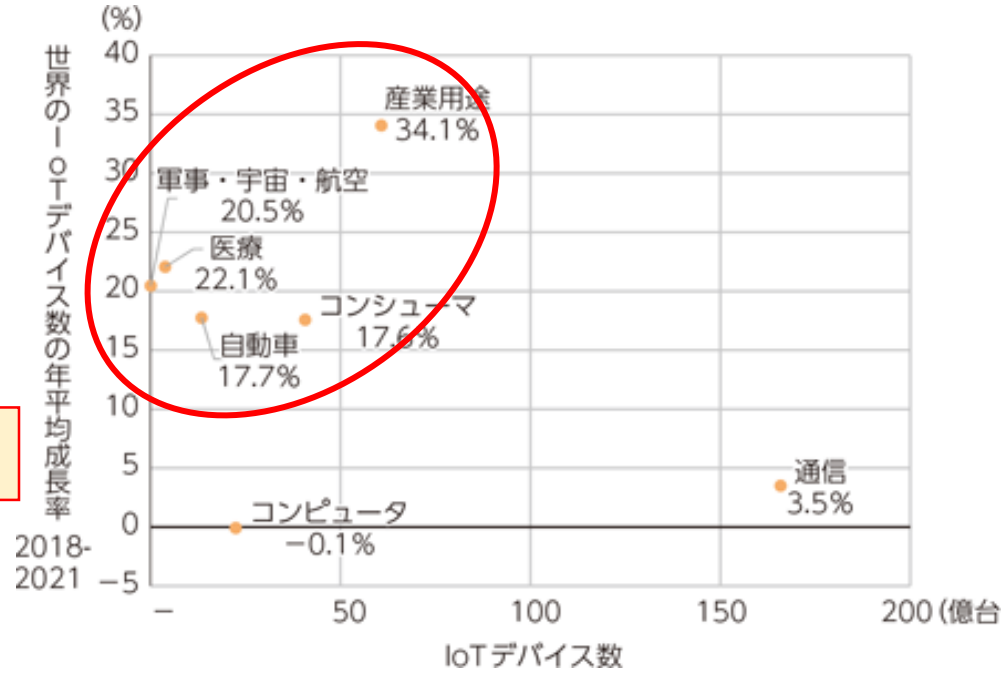


図2. 1 IPアドレス当たりの年間総観測パケット数（過去10年間）



（出典：NICTER観測レポート2019 - NICT）

● 通信分野でのIoT機器の利用は成熟しつつあり、直近3年間は産業用途等での利用が増加



（出典：IHS Technology）

② Active Network Securityの実現【背景】

- これまでのIoTのセキュリティ対策は、IoT機器の機能要件の設定や、パスワード等の設定に不備のあるIoT機器等の調査及び注意喚起の実施など、IoT機器に対する対策が中心。
- 一方で、IoTのセキュリティ対策をより実効的なものにするためには、サイバー攻撃が通過する通信ネットワーク側でより機動的な対処を行う環境整備が必要と考えられる。

● 現在取組がなされているIoTのセキュリティ対策

IoT機器の**設計・製造・販売**段階（**今後設置される**IoT機器）

IoT機器の**設置・運用・保守**段階（**既に設置された**IoT機器）

（１）IoT機器の技術基準

- 端末設備等規則を改正し、インターネットに直接接続されるIoT機器に関する基本的なセキュリティ要件を技術基準に位置づけ（本年4月施行）。
- 民間団体において上乗せの対策がなされた機器についての認証制度を立ち上げ。

（２）IoT機器の利用者への注意喚起

＜マルウェア**感染前**の機器への対処＞

- NICTがサイバー攻撃に悪用されるおそれのある機器を調査し、ISPを通じて利用者へ注意喚起を行うプロジェクト「NOTICE」を実施

＜マルウェア**感染後**の機器への対処＞

- NICTがマルウェアに感染している機器を「NICTER」プロジェクトにより特定し、ISPを通じて利用者へ注意喚起を行う取組を実施

（３）電気通信事業者間の情報共有

- 主にDDos攻撃等への共同対処を目的とする認定送信型対電気通信設備サイバー攻撃対処協会の取組を実施

これまではIoT機器に対する対策が中心

今後は通信ネットワーク側で攻撃そのものに対する対処をより機動的に行う環境整備が必要ではないか。

（※）上記のほか、IoT機器・システムに関する様々な基準・ガイドラインなどが存在

② Active Network Securityの実現【方向性】

■ IoTのセキュリティ対策を含め、様々な分野において、海外における動向（制度、実施状況等）も参考としながら、通信ネットワーク側で高度かつ機動的な対処を実現するための方策を検討することが必要ではないか。

例）電気通信事業者においてサイバーセキュリティ対策を円滑に実施するための法的課題について整理することが必要ではないか。

例）通信ネットワークにおけるサイバー攻撃対策について、新技術を活用して高度化を図ることが必要ではないか。例えば、Command & Control（C&C）サーバの検知についてAIなどを活用して高度化を図ることが必要ではないか。

（参考）過去の会合における構成員からの御意見

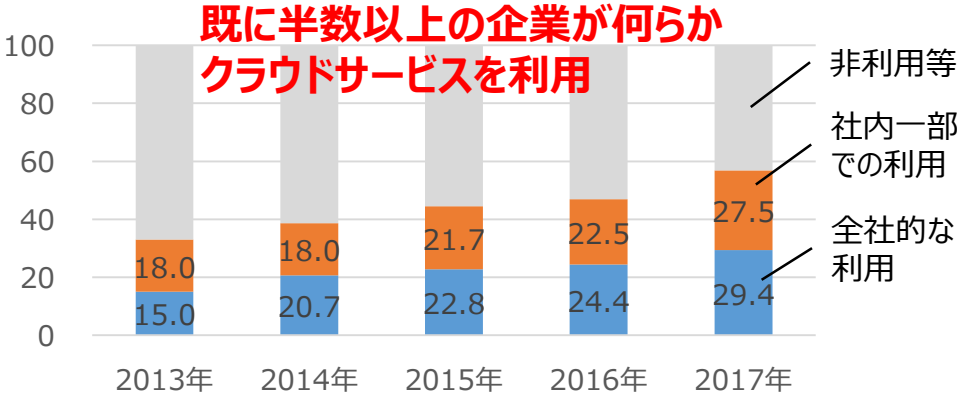
- ✓ サイバーセキュリティと通信の秘密の違法性阻却の考え方について議論が必要ではないか。
- ✓ 攻撃は相変わらず増えているという状況を見ていると、IoTを狙う攻撃の攻撃元はどこであるのか、それを止める、もしくは無くすために、本来取り組まなければならない対策は何であるのかという議論を行う必要があるのではないか。
- ✓ IoT機器に対する対策を今後どうしていくかということについて制度面も含めて考えていく必要がある。
- ✓ 個別のIoT機器そのもののクオリティについては短期的な改善は望めないので、即効性のある対策も必要なのではないかという印象を受ける。
- ✓ サービスが進展して振り返ってみたときに、通信の秘密に抵触していて、ビジネスに影響が出るということがあってはならないと思うので、そういうところを見越した対策を進めていくべき。

③ クラウド・リモート時代のセキュリティ確保【背景】

■ 昨今、クラウドサービスは重要な社会基盤となりつつあるが、セキュリティ不安やセキュリティ上の課題は依然として存在することから、着実なセキュリティ対策の実施が求められているところ。

■ また、クラウドサービスのセキュリティの確保に当たっては、サービスの提供者のみならず、サービスの利用者・調達者におけるリテラシーの向上も重要な課題。

クラウドサービスを利用している企業の割合



出典：平成30年版　情報通信白書

昨今のクラウドサービスに関する障害の例

例）大手クラウドサービスの障害（2019年8月）

- 大手クラウドサービスの東京リージョンの1つのアベイラビリティゾーン（AZ）において、空調設備の管理システムの障害が原因で長時間にわたってサービス障害が発生。

例）自治体専用IaaSサービスの障害（2019年12月）

- 自治体専用IaaSサービスにおいてストレージ障害やデータアクセス障害が発生し、大多数の仮想OSに影響が発生し、結果、多数の自治体の業務システムなどに長期間影響が出た。

クラウドサービスの社会経済上の重要性は増す一方、サービスに障害等が発生した際の影響が増大。

- クラウドサービスは昨今重要な社会基盤となっており、高い可用性を求められるユースケースも存在していることから、クラウドサービスの提供者において着実なセキュリティ対策が求められている。
- 一方、クラウドサービスのセキュリティは一般的に「責任共有モデル」が採用されており、クラウドサービス提供者と利用者/調達者の共通の認識の下、管理権限に応じた責任分担を行うものであるため、利用者等の意識向上も必要。

③ クラウド・リモート時代のセキュリティ確保【背景】

■ COVID-19への対応などの観点から、民間企業・自治体等においてはテレワーク・リモートワークシステムのニーズが増えており、そのセキュリティの確保も重要な課題。

安倍内閣総理大臣記者会見（令和2年4月7日）（抄）

（前略）・・・ゴールデンウイークが終わる５月６日までの１か月に限定して、**７割から８割削減を目指し、外出自粛をお願い**いたします。・・・（中略）・・・これまでもテレワークの実施などをお願いしてまいりましたが、社会機能を維持するために必要な職種を除き、**オフィスでの仕事は原則自宅で行うようにしていただきたい**と思います。・・・（後略）

- COVID-19への対応に当たり、多くの組織において在宅勤務が実施されているが、想定しないリスクに晒される可能性があることなどを踏まえ、各政府機関等において注意喚起が行われている。

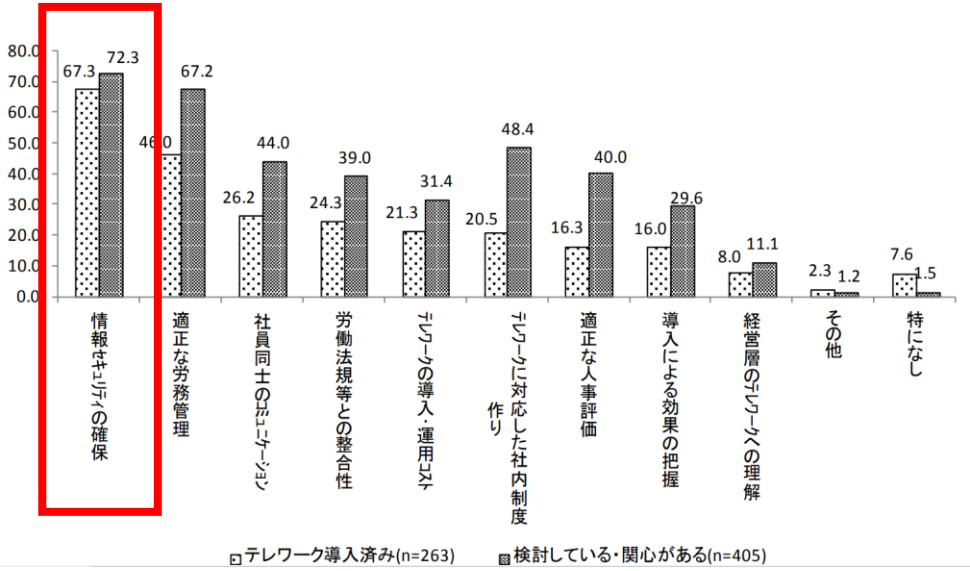
＜例①　警視庁の注意喚起（3月16日）＞

警視庁より、テレワークに関し、端末のOSやウイルス対策ソフトは常に最新の状態に更新し、定期的なウイルススキャンを実施するよう呼び掛け。

＜例②　NISCの注意喚起（3月27日）＞

内閣官房内閣サイバーセキュリティセンターより、パスワードの複雑化、多要素認証、アップデートの励行、通信の暗号化などテレワーク実施に当たっての注意喚起を実施。

- テレワークの導入において、約7割の企業が、情報セキュリティの確保が課題と考えている。



出典：地方創生と企業におけるICT利活用に関する調査研究（2015年３月 三菱UFJリサーチ&コンサルティング）

（参考）クラウド・リモート時代の新たなセキュリティモデル

■ クラウドサービスの利用の進展や、テレワーク・リモートワークの利用促進に伴う社内外のアクセスの増加など、ICT利活用の進展に合わせ、ネットワーク維持・管理の在り方と対応するセキュリティ対策の在り方も変化していくことが想定される中、新たなセキュリティモデルも考案されている。

● Zero Trust Archtecture

NIST による「Zero Trust」（＝全て信頼できない）モデル

SP 800-207

＜「Zero Trust」のネットワークインフラの前提＞

・企業のプライベートネットワークは信頼できない
・ネットワーク上のデバイスは企業によって所有又は設定可能でない可能性がある
・内在的に信頼されているデバイスは存在しない
・全ての企業のリソースが企業の所有するインフラストラクチャ上に存在するわけではない
・企業の遠隔ユーザはローカルのネットワーク接続を信頼できない

Zero Trust Archtectureが踏まえるべきコンセプトの例

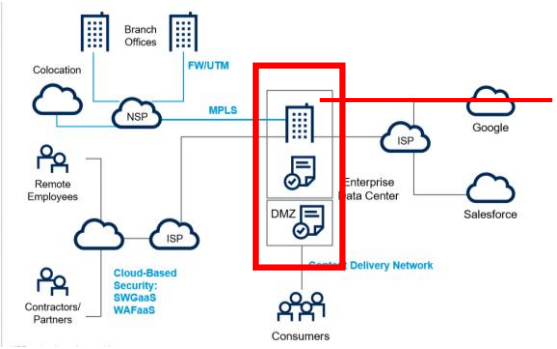
・あらゆる通信はネットワークの場所に関係なく保護される
・個々の企業のリソースへのアクセスは、接続単位で保証される
・ユーザ認証はアクセスが許可される前に動的かつ厳格に実施される

（出典）Draft (2nd) NIST Special Publication 800-207 より総務省作成

● Secure Access Service Edge

Gartner社の「Secure Access Service Edge」モデル

従来のデータセンター中心のセキュリティモデル



企業のデータセンターをネットワークセキュリティの中心に置く場合、トラフィック増大に伴うネットワーク遅延などが発生するおそれ。

ネットワーク機能とネットワークセキュリティ機能を1つのクラウドプラットフォームに統合し、各機能をサービスとしてエッジに提供するモデル（Secure Service Access Edge モデル）が提唱されている。

これにより、複雑性やコストの削減、遅延の改善などが期待。

（出典）「The Future of Network Security Is in the Cloud」（Gartner、2019）より総務省作成

③ クラウド・リモート時代のセキュリティ確保【方向性】

■ COVID-19への対応、クラウド＝バイ＝デフォルトや働き方改革などの流れを受けた、ネットワーク・システムの在り方の変化などを踏まえつつ、新たな時代に対応したセキュリティ対策を引き続き促進するべきではないか。

例）政府機関においてクラウドサービスを安全に活用できるよう、政府情報システムのためのセキュリティ評価制度（ISMAP）の着実な制度の立ち上げ、運営を図ることが必要ではないか。

例）クラウドサービスのセキュリティ確保のために求められる要件や留意事項等について、提供者と調達者・利用者双方への認知・普及が必要ではないか。

例）テレワークシステムに関する具体的なセキュリティ要件について、例えばシステム担当者が参照可能なチェックリスト等を作成し、普及させることが必要ではないか。

例）テレワークセキュリティに係る実態調査やテレワーク相談窓口のセキュリティ面での拡充など、実態把握・サポートを強化することが必要ではないか。

（参考）過去の会合における構成員からの御意見

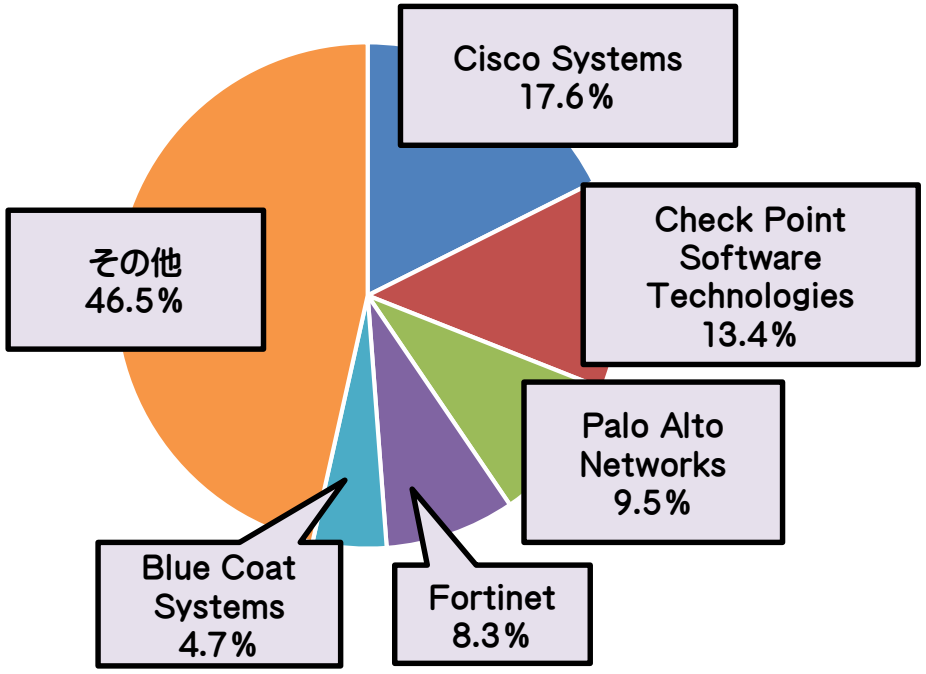
- ✓ サプライチェーンリスクの観点からの小規模企業のセキュリティ対策については、クラウドと掛け合わせる形で端末管理の方に集中できるようなアウトソーシングの仕組みづくりを外から持ってくるしかない。
- ✓ 今後の日本社会における大きなテーマとして、テレワーキングにおけるセキュリティの実装という観点についても、今後の課題として検討していただきたい。

④ 共創的研究開発/人材育成基盤の構築【背景】

■ わが国のサイバーセキュリティは、海外製品や海外由来の情報に依存してきており、「サイバーセキュリティ自給率」が低く、国産技術や情報の収集・分析の点で海外に後れを取っている状況。

● 世界のセキュリティ製品市場（2015年）

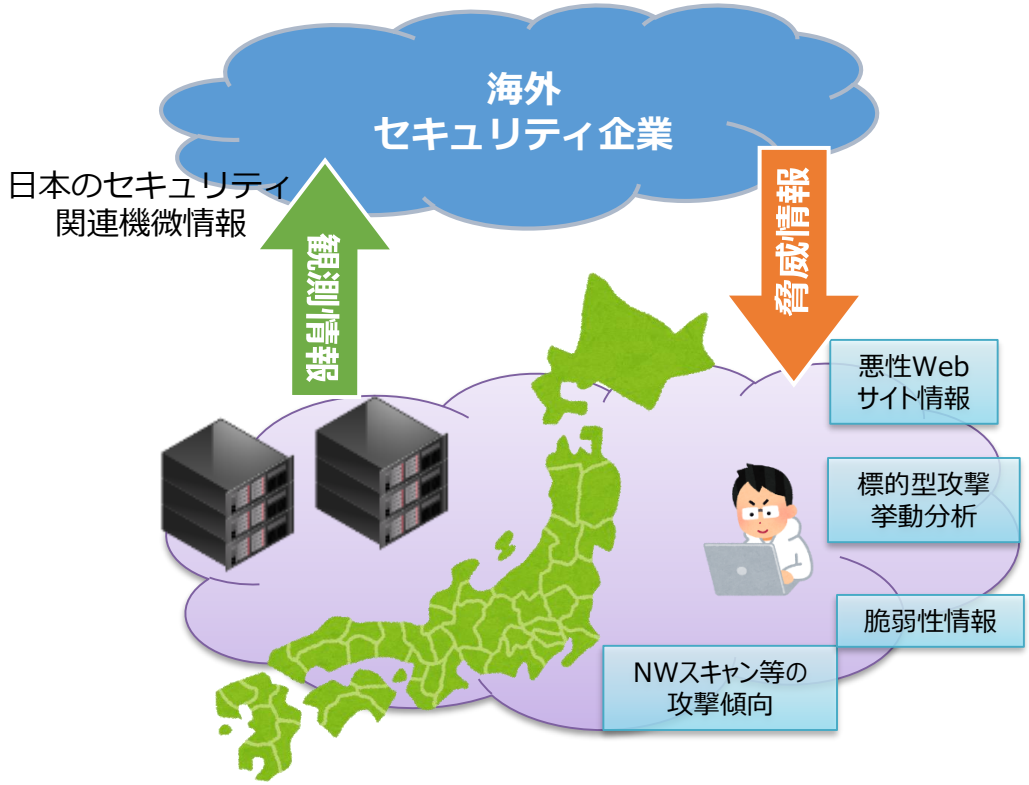
※F/W, VPN-GW, IDS/IPS 等のセキュリティ機能に特化した製品



上位5社が約半数のシェアを占める。日本のシェアは3.9%。

IDC Worldwide Quarterly Security Appliance Tracker, June 4, 2015
https://www.businesswire.com/news/home/20150608005363/en/Worldwide-Security-Appliance-Market-Continues-Grow-Quarter

● サイバーセキュリティ関連情報の海外依存



我が国のセキュリティ関連の機微情報が海外で分析される一方、ブラックボックス化した脅威情報を海外から購入せざるを得ない状況が継続。

④ 共創的研究開発/人材育成基盤の構築【背景】

■ 教育機関・産業界等からは、セキュリティ人材育成について、産学官の協力体制の構築やリソースの共有が必要との声が上がっている。

1. 新たな人材育成事業のニーズに関して (ターゲット人材層に関するご指摘)

- 「地方自治体においては、現場の対応要員に加えて、セキュリティ戦略を立ててシステムベンダと共働しつつ、組織のセキュリティ対策を先導できる人材が不足している」(by 地方自治体)
- 「IT システムを支える環境構築技術者、開発者層のセキュリティ知識の不足により、本来防げるはずのセキュリティインシデントが多発している」(by 民間の教育事業者)
- 「将来的には 5G や IoT 等の革新的技術の普及により、組織の末端に至るまでネットワークが張り巡らされる見込みだが、特に小規模組織におけるセキュリティ対応能力は人的にも予算的にも不足しており、早急になんらかの対策が必要」(by セキュリティ関連団体)

2. 人材育成基盤に関して (人材育成の仕組みに関するご指摘)

- 「慢性的に講師人材が不足している上に、同一の訓練であっても講師の能力にばらつきがあり、品質に差が生まれることがある」(by セキュリティ関連団体)
- 「演習用の環境構築やシナリオ開発には高度な知識や技術力が必要となるが、これらに単一組織だけで取り組むのは非常に効率が悪い」(by 民間の教育事業者)
- 「我が国はサイバーセキュリティ自給率が他国に比べて低く、サイバー演習においても海外製の演習環境やシナリオに依存しがち。日本特有の環境ゆえのインシデント事例等が活用されていないことが、安全保障の観点において大きな課題である」(by 教育機関)

3. 新たな人材育成事業のための基盤環境に関して (人材育成のベースに関するご指摘)

- 「演習事業の実施にあたっては、その基盤となる計算機環境や演習システムが必要となるが、その構築と維持には高い技術力が必要であり、単一組織での構築・長期的運用は困難」(by 教育機関)

④ 共創的研究開発/人材育成基盤の構築【方向性】

■ サイバー攻撃の多様化、巧妙化が進む中、オープン型の研究開発や人材育成の基盤を構築・運用して産業界等に開放し、産学官で連携して我が国のサイバー攻撃への自律的な対処能力を高めることが必要ではないか。

例）マルウェアの挙動情報等のサイバー攻撃関連情報を官民で集約・蓄積・分析し、その成果を踏まえて我が国のセキュリティ製品の検証・開発の支援などを行う、統合的研究開発プラットフォームを整備することが必要ではないか。

例）演習の実施に関する様々な要素（データセット、教材、演習用ミドルウェア、計算機リソースなど）を総合的にカバーする、オープン型の新たな人材育成プラットフォームや、産学官の連携による当該プラットフォームの活用コミュニティの構築が必要ではないか。

（参考）過去の会合における構成員からの御意見

- ✓ 攻撃者の視点がないといろいろと変遷する脅威に対して追随することができない。攻撃者側の視点を持った研究や活動が大事である。
- ✓ 集約した情報について、NICTとトラストリレーションシップを結んだ研究機関と連携して活用することは十分あり得る。
- ✓ 産業と一体になって進めていけるような分野は、参と官が一体となって共同研究開発を進めていくことができるとよい。
- ✓ 研究開発については、特にデータの利活用について、個々が頑張ってもうまくいかないので、国レベルでセキュリティ研究のためのデータプラットフォームを構築することが必要。