資料25－3

「IoT・5Gセキュリティ総合対策2020（案）」の主要な検討課題

令和2年7月17日
サイバーセキュリティタスクフォース事務局

「IoT・5Gセキュリティ総合対策2020」の主要な検討課題

(1)COVID-19への対応を受けたセキュリティ対策の推進

① テレワークシステムのセキュリティに関するチェックリストの作成や相談・助言体制の構築など、特に中小企業を念頭においたテレワークセキュリティの確保のための実践的な対策を推進する。

② ネット上で業務・手続きを完結可能とするため、電子署名やeシールなどのトラストサービスの制度化や普及促進を図るとともに、制度・手続き・慣習の見直しを進める。

(2)5Gの本格開始に伴うセキュリティ対策の強化

① 5Gネットワークの脆弱性及び脅威の検証・分析のための手法や体制の確立

② 関係者間のリスク・脅威情報の共有

③ 規制・振興両面でのセキュリティ対策の実装の促進など

セキュリティ・バイ・デザインの観点で推進

(3)サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

巧妙化・多様化するサイバー攻撃に対処するため、電気通信事業者における積極的なサイバーセキュリティ対策（C&Cサーバの能動的な検知や攻撃指令通信の遮断等）を迅速かつ効果的に実施可能とするため、通信の秘密の保護を図りつつ、一層のサイバーセキュリティを確保する方策について検討を行う。

(4)我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

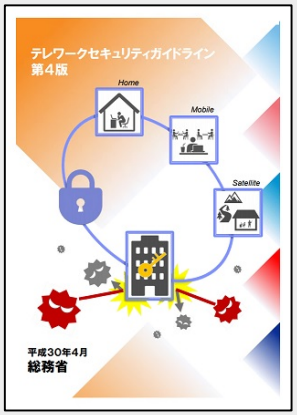
我が国におけるセキュリティ技術の海外依存や慢性的な人材不足から脱却するため、サイバーセキュリティ情報を国内で収集・蓄積(生成)・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し、産学官連携の結節点とするための体制の構築を図る。

（1）①COVID-19への対応を受けたセキュリティ対策の推進

企業及び地方自治体によるテレワークセキュリティの確保

- テレワークセキュリティに関するチェックリスト等の策定

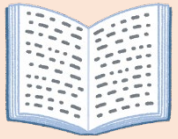
テレワークセキュリティガイドライン
（平成30年４月総務省策定）



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」

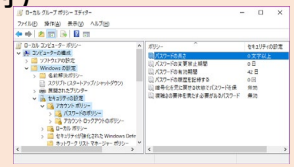
考え方・方針について記載
（例）
「パスワードは一定以上の長さ
で推測されにくものを用いる」

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

- テレワークセキュリティに関する実態調査、専門的相談の実施

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

（1）② COVID-19への対応を受けたセキュリティ対策の推進

「トラストサービス検討WG最終取りまとめ（令和２年２月）」において、具体的なニーズと課題が顕在化している①タイムスタンプ、②eシール及び③リモート署名、それぞれの取組の方向性を整理。

現状・課題	取組の方向性
①データの存在証明・非改ざんの保証の仕組み（タイムスタンプ） • 民間の認定スキームの下で、一部の分野を除き、利用が十分に広がっていない。 → 電子データと紙による保存を併存している実態があり、保存コストを要している。	• タイムスタンプ事業者に対する国としての認定制度を創設。 （2020年度中の創設を目指し、認定基準等の詳細を検討。） **具体的な認定スキームについて有識者会議で検討中。** 可能な限り前倒し
②組織の正当性を確認できる仕組み（eシール） • 請求書や領収書等について、企業が電子的に発行したことを簡便に保証する仕組みがない。 → 企業内の業務や企業間の取引における電子化が進まず、業務効率化の妨げとなっている。	• eシールの認証事業者に対する国の基準に基づく民間の認定制度を創設。 （2021年度中の創設を目指し、認定基準等の詳細を検討。） **具体的な認定スキームについて有識者会議で検討中。** 可能な限り前倒し
③人の正当性を確認できる仕組み（電子署名） • クラウドを活用したリモート署名など最新の技術に制度 が十分に対応しきれていない部分が存在。 → 電子署名の利用が伸びていない。 • リモート環境で本人だけが安全に署名できるための技術的な要件について民間団体で検討中。	• 電子署名法にリモート署名を位置づけて運用できるよう、省令改正に向けた検討を進める。 （2021年度中の運用開始を目指し、民間団体の技術的要件の検証等を実施。） 可能な限り前倒し

■ 上記に加え、**電子文書の送受信・保存**について規定している**法令との関係**で有効な手段として認められるトラストサービスの**要件を明示**するよう、所管省庁への働きかけを行う。

(2) 5Gの本格開始に伴う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

- 5Gのネットワークに関する脆弱性（ソフトウェア含む）を明らかにするための技術的検証を実施。また、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) サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

- インターネット接続機器が急激に増加し、脆弱でセキュリティ対策が困難な機器も増加する中、端末側とネットワーク側の双方から、総合的なセキュリティ対策を実施することが求められている。
- 端末側の対策としては、これまで電気通信事業法における端末設備等規則へのセキュリティ要件の追加や、脆弱な状態にある機器の利用者への注意喚起等の取組みを実施しているところ。
- これらに加えて、ネットワーク側の対策として、電気通信事業者が個々の感染端末に指示を出すC&Cサーバに直接対処するなど、より効率的にセキュリティ対策を実施することが求められており、電気通信事業者が自らC&Cサーバーを検知し、遮断等の対策を実施するために必要となる制度的検討や、技術的な課題の解決に向けた取組みを実施する必要がある。

（制度的課題とその対応）

① 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。

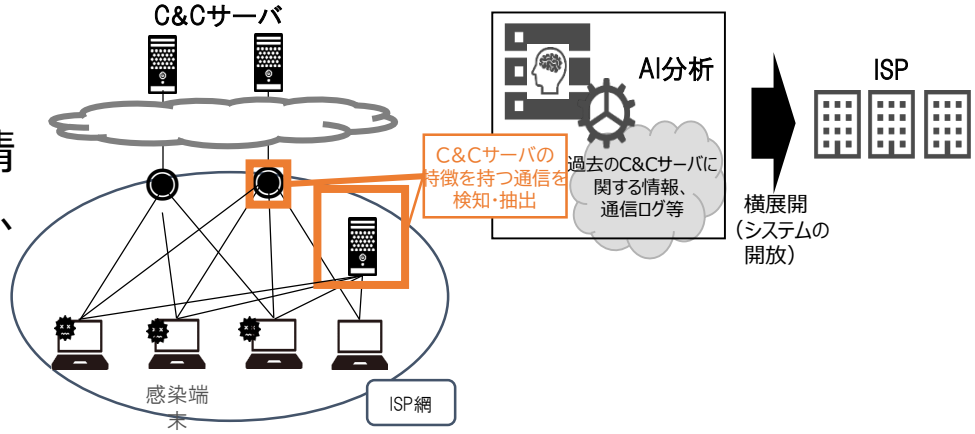
→ 電気通信事業者が通信の秘密に配慮した円滑な対応を行うことが求められるところ、制度的な観点から検討を行うことが重要。

※ 中長期的な対応として、サイバーセキュリティ対策と通信の秘密の保護の関係性について、新たな視点からの議論も行うことが必要。

（技術的課題とその対応）

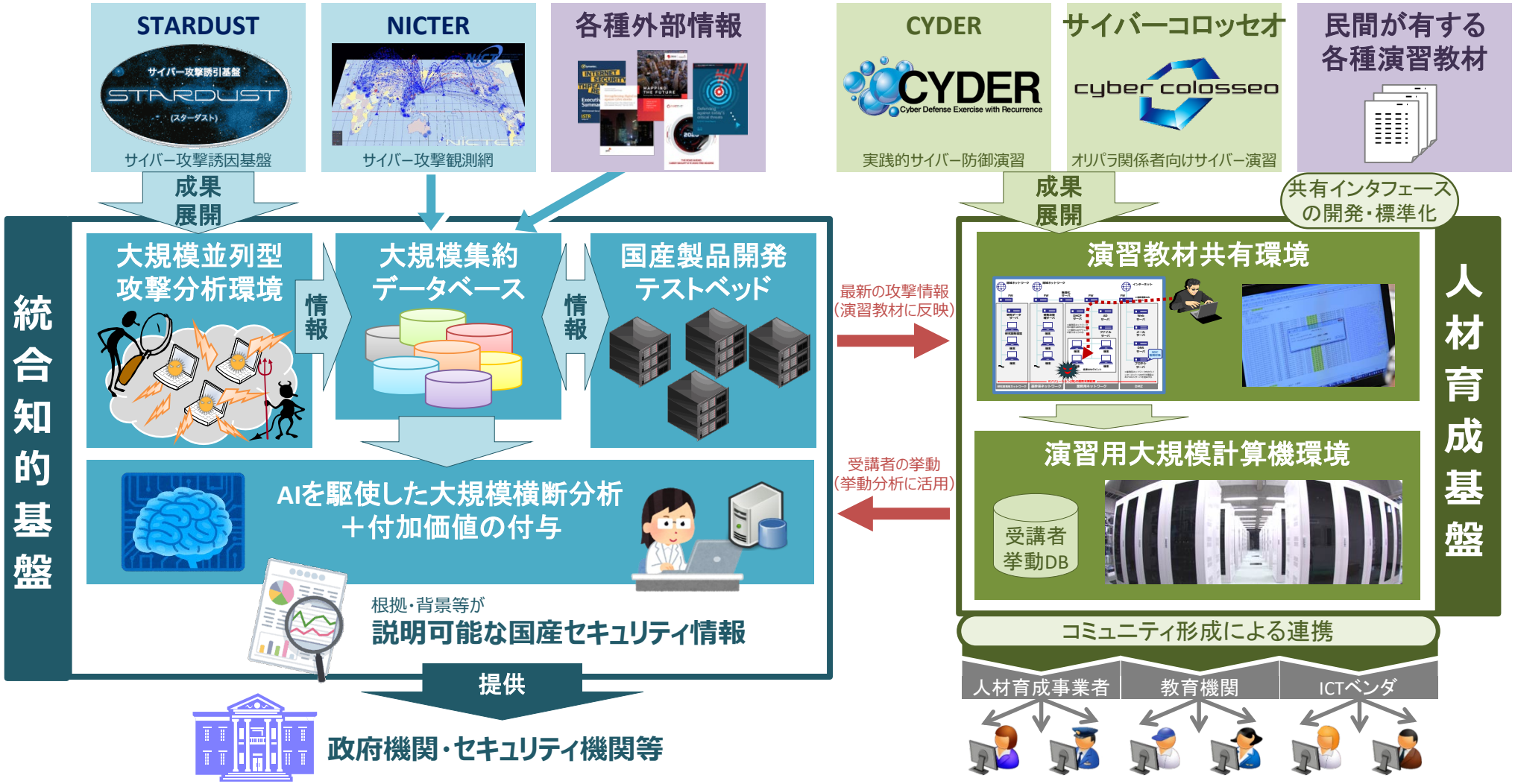
② 電気通信事業者が自ら、C&Cサーバを検知するには、過去のC&Cサーバに関する情報や、通信ログ情報等の膨大な情報を調査、処理する必要があるため、迅速な対応が難しい。

→ 通信の秘密に配慮しつつ、AIシステム等を用いC&Cサーバの検知手法の高度化を図る。



(4) 我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

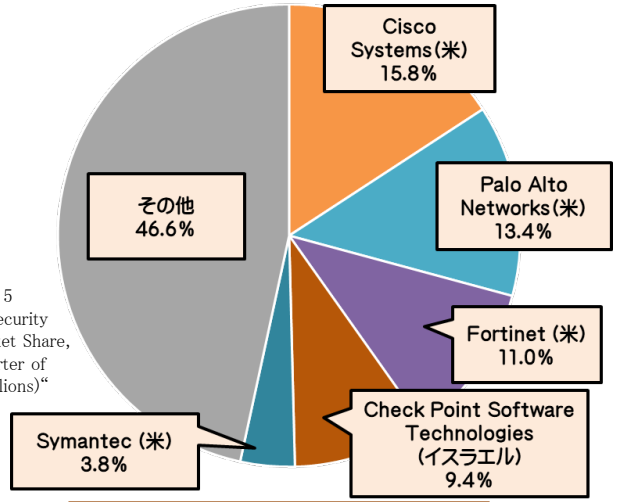
■ サイバーセキュリティ情報を国内で収集・蓄積(生成)・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し、産学に開放し、結節点とすることで、サイバーセキュリティ対処能力の向上を図る。



（参考）情報集約・分析及び人材育成における課題認識

■ 我が国におけるセキュリティ製品は海外に大きく依存しており、製品開発に必要なノウハウや知見の蓄積が困難。また、開発・利用者側の双方においてセキュリティ人材が不足。

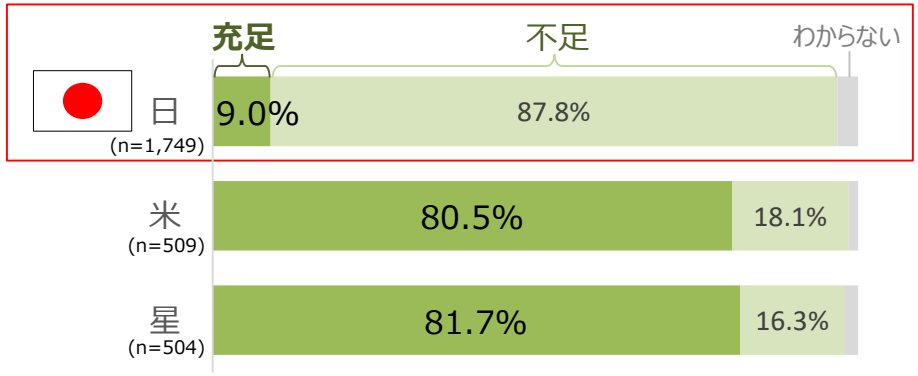
世界セキュリティアプライアンス製品市場ベンダー別シェア（売上額）（2019年（令和元年）第４四半期））



IDC プレスリリース〝Top 5 Companies, Worldwide Security Appliance Revenue, Market Share, and Growth, Fourth Quarter of 2019 (revenue in US$ millions)〟より作成。

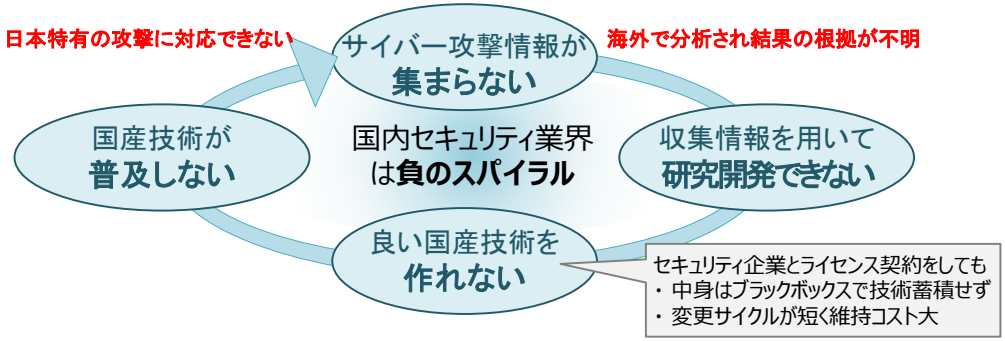
国内のセキュリティ情報の多くが海外に流出

セキュリティ対策に従事する人材の充足状況



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

育成ニーズはあるが育成の仕組みが不十分



- 演習の実施には、**高度な技術**力と**計算機環境**が必要
- **海外教材**に依存し、**日本**特有の**事例**が**反映**できない

本来防げるはずの**攻撃が防げない**

- セキュリティ**対策を先導**できる人材**不足**
- **技術者・開発者**のセキュリティ**知識不足**

国内でのサイバーセキュリティ情報の生成や、人材育成を加速するエコシステムの構築が必要