資料12－2

総合対策策定後の状況変化と今後の方向性について

総務省　サイバーセキュリティ統括官室

IoTセキュリティ総合対策後の状況変化を踏まえて

- ✓ 2017年11月の「IoTセキュリティ総合対策」の策定・公表後、2018年７月には「IoTセキュリティ総合対策 プログレスレポート2018」を作成し、同総合対策の進捗状況や今後の取組についてフォローアップを行ってきたところ。

- ✓ 一方、同総合対策の策定・公表後を中心に様々な状況変化があったことも踏まえ、総務省としてサイバーセキュリティ政策に取り組んでいくためのビジョンや方向性について、改めて検討が必要。

＜状況変化の例＞

① 2019年目途の５Ｇサービスの提供開始

② サプライチェーンリスクへの対応の重要性

③ データ管理・流通の安全性・信頼性の確保

④ サイバーセキュリティ×AIの重要性の高まり

⑤ 2020東京大会に向けた対策の強化

状況変化の例① 2019年目途の5Gサービスの提供開始

■ 5Gが運輸・交通、医療、製造業など様々な産業に活用される基幹的な社会インフラとなるにしたがって、これまでとは全く異なるサイバーセキュリティへの対応の在り方が求められる可能性がある。

－ 5GはAI/IoT時代のICT基盤 －

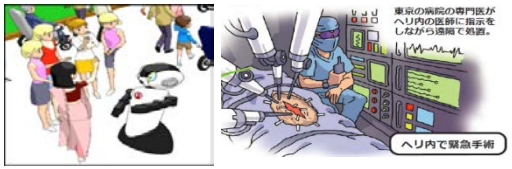
超高速

現在の移動通信システムより100倍速いブロードバンドサービスを提供

⇒ **２時間の映画を３秒でダウンロード**

超低遅延

利用者が遅延（タイムラグ）を意識することなく、リアルタイムに遠隔地のロボット等を操作・制御

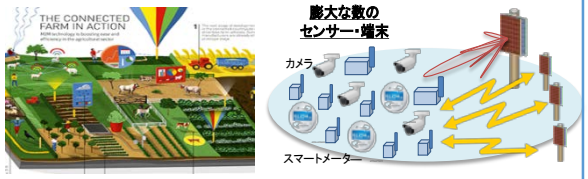


ロボットを遠隔制御

⇒ **ロボット等の精緻な操作をリアルタイム通信で実現**

多数同時接続

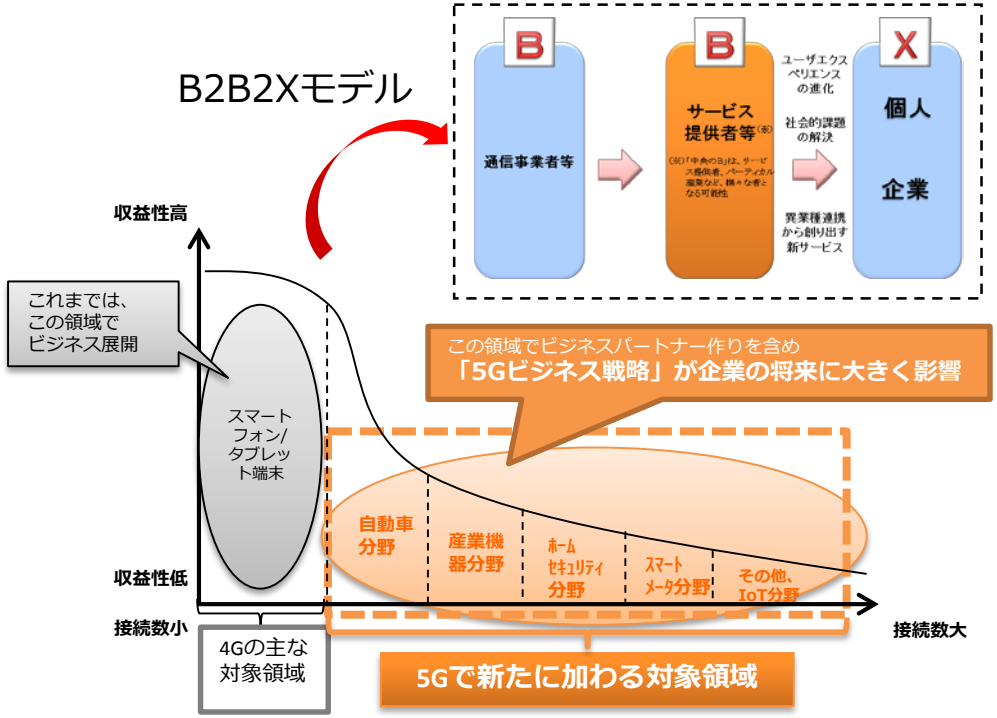
スマホ、PCをはじめ、身の回りのあらゆる機器がネットに接続



⇒ **自宅部屋内の約100個の端末・センサーがネットに接続**
（現行技術では、スマホ、PCなど数個）

社会的なインパクト大

－ 様々な産業との融合が期待される5G －



状況変化の例② サプライチェーンリスクへの対応の重要性

【サイバーセキュリティ戦略（平成３０年７月２７日閣議決定）】

4.1.2 (2)　サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築

サプライチェーン全体としてのサイバーセキュリティを確保するためには、製造される機器、生成されて流通するデータ、それらを利用したサービス等のサプライチェーンの構成要素における信頼の確保が不可欠である。このため、それぞれの構成要素がセキュリティ要件を満たした形で生成・流通されるよう、要件の明確化を図るとともに、その要件が満たされていることを確認等することにより信頼を創出する仕組みの構築が必要である。また、サプライチェーンにおける調達者が機器・サービス等の利用に際し、その信頼を確認できるよう、官民が連携して、信頼性が証明されている機器・サービス等のリストの作成と管理を行う仕組みの構築が必要である。さらに、これらがサプライチェーンのつながりにおいて、連続的な仕組みとなるよう、トレーサビリティを確認するための仕組みと、創出された信頼そのものに対する攻撃を検知・防御するための仕組みを検討する。

4.2.3　政府機関等におけるセキュリティ強化・充実

複雑化・巧妙化しているサイバー攻撃に対しては、引き続き攻撃を前提とした多層防御や、サプライチェーンリスクへの対応を強化するとともに、新たな技術を活用し、従来の攻撃側優位の状況を改善するための取組を進めることが求められる。

4.4.2 (1)　実践的な研究開発の推進

特に、サプライチェーンにおける価値創出のプロセスにおける信頼の創出や証明、トレーサビリティの確保とこれらに対する攻撃の検知・防御に関する研究開発を進めるほか、機器に組み込まれた不正なハードウェアやソフトウェアを効率的に検出する技術開発、プラットフォームにおいて利用者の意図しない動作を生じさせるおそれがあるときにもデータや情報の真正性・可用性・機密性を確保するための研究開発を行う。

状況変化の例② サプライチェーンリスクへの対応の重要性

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に関する申合せ （平成30年12月）

１．適用対象

各省庁等において下記に該当すると思われる情報システム等のうち、ＮＩＳＣ・ＩＴ室と協議のうえ、対象としたもの。

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、個人情報を極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

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．調達手続の流れ

「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。

４．ＮＩＳＣ・ＩＴ室の助言

調達する情報システム等の構成品候補について、「製造業者」「機種」等の情報を事前に受けることで、「サプライチェーン・リスクに係る懸念が払拭できない」か否か、助言を行う。

状況変化の例③ データ管理・流通の安全性・信頼性の確保

■ Society5.0を迎えるにあたり、各産業においてデータの重要性が急速に増大していることから、政府の様々な戦略にもデータ管理や流通の安全性・信頼性の確保に関する方向性が盛り込まれ始めているところ。

【サイバーセキュリティ戦略（平成３０年７月２７日閣議決定）】

4.2.2 (1)② 安全基準等の改善・浸透

データの管理の状況に関する調査や国際動向も踏まえた望ましいデータ管理や人的要因によるリスク軽減の在り方を含め、業務の内容、組織の規模、システムの使用期間、国際競争力への影響等を考慮して安全基準等を改善する取組を継続的に推進する。

4.2.3 (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。

状況変化の例③ データ管理・流通の安全性・信頼性の確保

【 デジタル時代の新たなＩＴ政策の方向性について（案）
～デジタル時代に対応した「新たな社会システム」への移行に向けて～
（平成３０年１２月高度情報通信ネットワーク社会推進戦略本部・
官民データ活用推進戦略会議決定）】

１．基本的な考え方

- また、ビジネスにおいては、人工知能（AI）、IoTなどの新たな技術の利活用が進むにつれて、大量に流通する**データがデジタル時代の「新たな資源」**として注目を集めている。例えば、センサーなどにより収集した情報をビッグデータ化し、AIを活用して分析することで、小売分野での需要予測、潜在需要を喚起する新商品・サービス開発、医療分野での予防医療やオーダーメイド治療、都市での犯罪・事故・災害抑制などの新たな価値の創造につなげることが可能となるためである。

２．新たなIT政策の方向性

（１）データの安全・安心・品質

- 一方、経済のグローバル化が進展する今日においては、国内のみならず国際的なデータ移転も大幅に増加しており、例えば、**日本企業の約40%、米国企業の約60%が越境データ移転を行っている**との調査もある。
- こうした現状を踏まえ、国内はもとより国際的なデータの移転についても、自由かつ公平なルールを基本としつつ、個人及び法人の権利利益や国の安全等が損なわれることのないよう、個人に関するデータや重要産業のオペレーションデータなどについて、透明性の高いルールの下、相互に個人情報の保護やセキュリティを確保しつつ、国際的なデータ流通環境を構築するために必要な措置を講ずる。

状況変化の例④ サイバーセキュリティ×AIの重要性の高まり

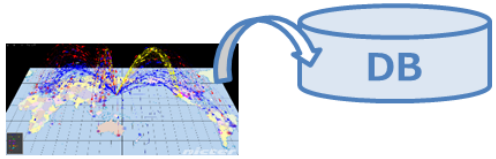
■ AIを活用したサイバーセキュリティ対策の高度化についてはこれまでも様々な事業者、関係機関で実施されてきたところであるが、サイバー攻撃の巧妙化、多様化が進む中で、AIを効果的にサイバーセキュリティ対策に活用することが求められている。

【NICTによる機械学習（AI技術）を活用したサイバーセキュリティの研究開発】

データセットの構築（例）

■ダークネット関連データ

未使用IPアドレスへの攻撃関連通信データ等

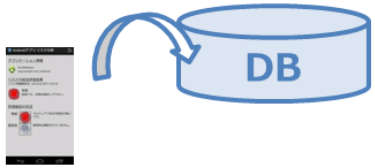


■マルウェア関連データ

マルウェア検体等、静的・動的解析結果等

■Android APK関連データ

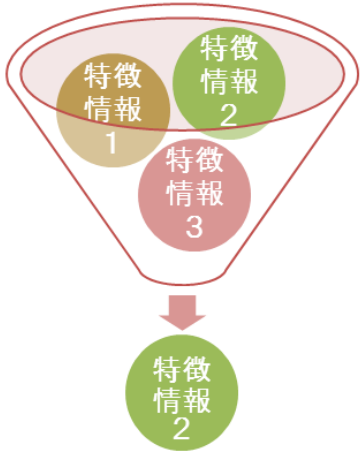
アプリのカテゴリ情報や説明文等



機械学習技術の活用（例）

■特徴選択

多様な特徴情報から最も影響力の高い特徴情報を特定



■SVM（サポートベクタマシン）

特徴情報に基づき、機械学習技術（SVM）を用いて、データを分類。

攻撃パターンの分析やマルウェアの動作・影響分析等を自動化

研究開発成果

（事例１）DDoS攻撃の発生検知

ダークネットトラフィックにおける特徴情報を効果的に特定することで、DDoS攻撃の発生を早期に検知。

（事例２）パッカーの特定

マルウェアがどのようなパッカー（難読化ツール（※））を利用しているかを特定。

（事例３）Androidアプリ分析

オンラインマーケットに配布されているアプリがマルウェアであるかどうかを判定。

状況変化の例⑤ 2020東京大会に向けた対策の強化

【検討体制】

オリパラ推進本部
（本部長：安倍総理）

オリパラ関係府省庁連絡会議
（議長：杉田副長官）

セキュリティ幹事会

座長	– 内閣危機管理監
座長代理	– 内閣官房オリパラ事務局長、内閣官房副長官補（内政）、内閣官房副長官補（事態、NISCセンター長）、警察庁次長（シニア・セキュリティ・コマンダー）
構成員	– 内閣官房（NSS、内政・オリパラ事務局・事態・内調・NISC）、内閣府（防災）、警察庁、金融庁、総務省、消防庁、法務省、公安調査庁、外務省、財務省、スポーツ庁、厚労省、農水省、経産省、国交省、観光庁、気象庁、海上保安庁、環境省、原子力規制庁、防衛省の局長級
オブザーバー	– 東京都、組織委、警視庁、東京消防庁の幹部
事務局	– 警察庁、総務省、外務省、経産省、国交省、防衛省の協力を得て内閣官房において処理

テロ等警備対策ＷＴ

座長	– 内閣審議官（事態、オリパラ事務局）
座長代理	– 内閣審議官（内政）、内閣府審議官（防災）、警察庁審議官
構成員	– 関係省庁の課長級
オブザーバー	– 関係機関の幹部
事務局	– 関係行政機関の協力を得て内閣官房において処理

サイバーセキュリティＷＴ

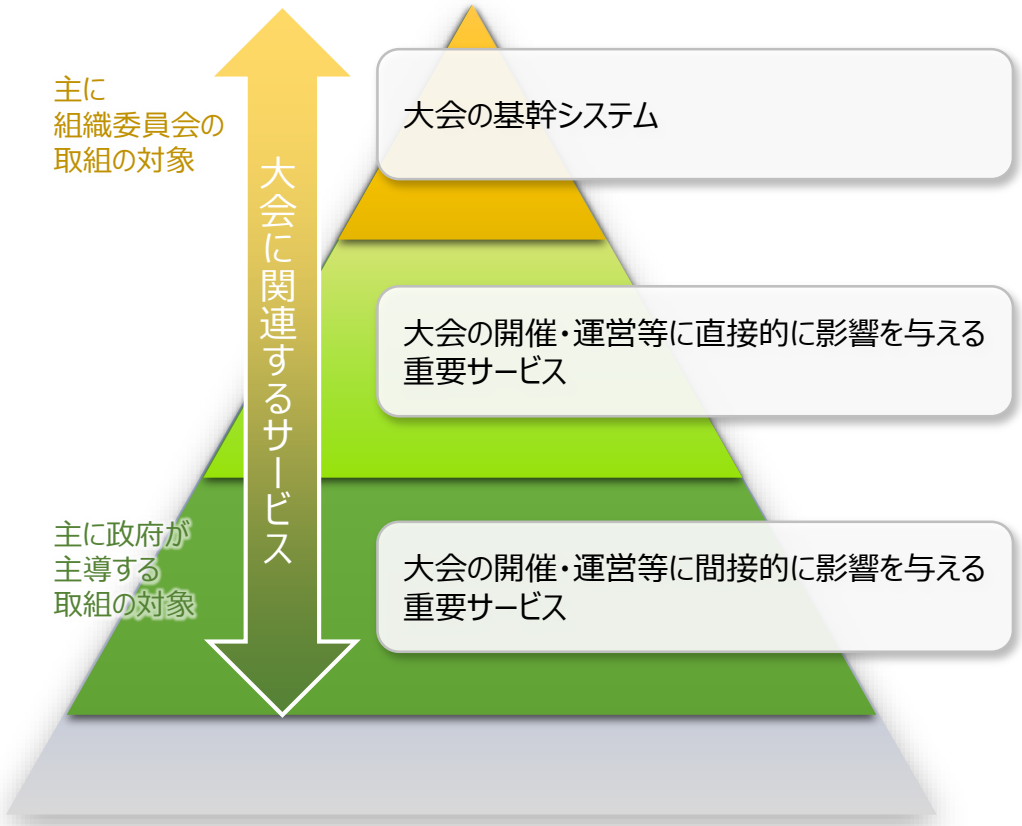
座長	– 内閣審議官（NISC副センター長）
座長代理	– 内閣審議官（オリパラ事務局）、警察庁審議官
構成員	– 関係省庁の課長級
オブザーバー	– 関係機関の幹部
事務局	– 警察庁、総務省、外務省、経産省、防衛省の協力を得て内閣官房において処理

2020年東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ体制に関する検討会

セキュリティ情報センター

- 平成29年7月24日、警察庁に設置
- 大会の安全に関する情報を集約
- 関係機関等と協力し、大会の安全に対する脅威及びリスクの分析、評価を行い、国の関係機関等に対し必要な情報を随時提供

【大会の開催・運営を支える重要サービスのイメージ】



（出典）NISC作成資料より抜粋

- ✓ 2020東京大会に向け、通信・放送を含む重要サービス事業者、重要インフラ事業者のセキュリティの確保が重要な政策課題となっている。
- ✓ 特に対策の遅れている地方の中小の事業者等については、サイバーセキュリティ対策に関する啓発、人材育成の機会の確保等を含めた政策的支援が必要。

IoTセキュリティ総合対策の改定の方向性(案)(１)

IoTセキュリティ総合対策

はじめに

Ⅰ 基本的考え方

Ⅱ 具体的施策

（１）脆弱性対策に係る体制の整備
（２）研究開発の推進
（３）民間企業等におけるセキュリティ対策の促進
（４）人材育成の強化
（５）国際連携の推進

Ⅲ 今後の進め方

（１）「Ⅰ 基本的考え方」について

✓ 総合対策では、IoTシステムのセキュリティについて、NISCの「安全なIoTシステムのためのセキュリティに関する一般的枠組」を踏まえつつ、レイヤーごとの課題抽出を行ったところ。

✓ 総合対策の改定に当たってはIoT機器・システムのサイバーセキュリティの重要性は認識しつつも、課題認識を**IoT機器・システム以外の分野まで広げて整理**するとともに、総務省として**目指すべき社会の在り方**などをコンセプトとして打ち出すことを想定。

IoTセキュリティ総合対策の改定の方向性（案）（２）

IoTセキュリティ総合対策

はじめに

Ⅰ 基本的考え方

Ⅱ 具体的施策

（１）脆弱性対策に係る体制の整備
（２）研究開発の推進
（３）民間企業等におけるセキュリティ対策の促進
（４）人材育成の強化
（５）国際連携の推進

Ⅲ 今後の進め方

（２）「Ⅱ 具体的施策」について

✓ 総合対策では、具体的施策について、（１）脆弱性対策に係る体制の整備、（２）研究開発の推進、（３）民間企業等におけるセキュリティ対策の促進、（４）人材育成の強化、（５）国際連携の推進、の５つの柱で整理。

✓ 総合対策の改定に当たっては、基本的には上記の**５つの柱は維持**しつつも、直近のサイバーセキュリティの状況やタスクフォースでの御議論等を踏まえ、適宜、**柱立ての変更も視野に入れつつ中身を検討**する。

IoTセキュリティ総合対策の改定の方向性（案）（３）

IoTセキュリティ総合対策

はじめに

Ⅰ 基本的考え方

Ⅱ 具体的施策

（１）脆弱性対策に係る体制の整備
（２）研究開発の推進
（３）民間企業等におけるセキュリティ対策の促進
（４）人材育成の強化
（５）国際連携の推進

Ⅲ 今後の進め方

（３）「Ⅲ 今後の進め方」について

✓ 総合対策では、半年に１度を目途としつつ、必要に応じて検証を行い、進捗状況を把握するとともに、本分野における技術革新や最新のサイバー攻撃の態様を踏まえ、必要に応じて（総合対策そのものも）随時見直しを行っていくとされていたところ。

✓ サイバーセキュリティ分野が変化や進歩が激しい分野であることに鑑み、**対策そのものの見直しの頻度や進捗状況の把握の在り方**なども本タスクフォースで御議論いただき、適切に反映。

今後のスケジュール

- タスクフォースにおいて、以下のスケジュールで総合対策の改定版（案）について御議論いただき、６月を目途に公表する。
- プログレスレポートについては、事務局にて原案を作成後、メール回付にて御議論、御承認いただく予定。

2019年３月	2019年４月	2019年５月	2019年６月

タスクフォース

第12回

- ✓ 総合対策の主な取組の進捗報告
- ✓ 検討課題の洗い出し

第13回

- ✓ 改定版（案）

第14回

- ✓ 改定版（案）

公表

プログレスレポート

事務局にて原案作成後、メール回付にて
御議論、御承認いただく

**「IoTセキュリティ総合対策
プログレスレポート2019」
公表**