資料37－2－1

情報通信ネットワークの安全性・信頼性の確保に係るサイバーセキュリティ対策の現状と課題

令和4年4月

サイバーセキュリティタスクフォース事務局

①　電気通信事業者におけるサイバーセキュリティ対策の推進

①－１ 国内外の動向

①－２ 電気通信事業者によるサイバー攻撃対策

①－３ 電気通信事業法改正案

①－４ 5Gネットワークにおけるセキュリティの確保

②　IoTセキュリティの確保

②－１ NOTICEの現状/NICTERの現状、http（s）への拡大

②－２ 機器メーカとの関係

③　その他の取組

③－１ トラストサービス

③－２ クラウドサービスのサイバーセキュリティ確保

③－３ スマートシティのサイバーセキュリティ確保

③－４ 放送設備のサイバーセキュリティ確保

前々回タスクフォースの振り返り

総務省におけるこれまでの取組（前々回タスクフォース資料抜粋）

○電気通信事業者におけるサイバーセキュリティ対策

＜電気通信事業者間の情報共有＞

・2018年5月の改正電気通信事業法において、電気通信事業者が「送信型対電気通信設備サイバー攻撃」への対応を共同して行うため、攻撃の送信元情報の共有等の業務を行う第三者機関を総務大臣が認定する制度を創設（2019年1月に一般社団法人ICT-ISACを認定）。

＜サイバー攻撃が原因である電気通信事故の報告＞

・また、「送信型対電気通信設備サイバー攻撃」が原因である電気通信事故の発生状況の報告を求めることを内容として、電気通信事業報告規則（昭和63年郵政省令第46号）を改正。2019年度には8件、2020年度には13件の報告があった。

＜電気通信事業者による積極的な対策＞

・電気通信事業者によるC&Cサーバ（マルウェアに感染した端末に対して指令を与えるサーバ）検知・共有のためのフロー情報の分析について、制度面では、「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」において、2021年11月に「通信の秘密」との関係を整理した「第四次とりまとめ」を公表するとともに、技術面では、C&Cサーバの検知技術及び共有手法について、2022年度に実証事業を実施（令和3年度補正予算）。

・あわせて、悪性Webサイト（フィッシングサイト等）の検知技術・共有手法、ネットワークセキュリティ対策技術（RPKI等）についても2022年度に実証事業を実施（令和3年度補正予算）。

＜５Gのセキュリティ確保＞

・5Gのネットワークやその構成要素及びサービスについて、ソフトウェア・ハードウェアの両面から技術的検証を行うことを通じ、5Gのネットワークのセキュリティを確保する仕組みや体制を整備するための取組を実施し、その成果を「5Gネットワーク構築におけるセキュリティに関する対策等の留意点」として公表予定。

＜事業者のガバナンス確保＞

・2021年5月には「電気通信事業ガバナンス検討会」が設置され、電気通信事業におけるサイバーセキュリティ対策とデータの取扱い等に係るガバナンス確保の在り方についての検討を実施中。

前々回タスクフォースでお寄せいただいた意見（抜粋）

✓「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 第四次とりまとめ」によりC&Cサーバ のIPアドレス等の調査ができるようになったが、国内の端末を踏み台として海外に攻撃を行うケースにおける対処には悩んでいる。（小山構成員）

✓「重要インフラのサイバーセキュリティに係る行動計画」について、効果のレビューが待たれる。（篠田構成員）

①　電気通信事業者におけるサイバーセキュリティ対策の推進

①－１ 国内外の動向

①－２ 電気通信事業者によるサイバー攻撃対策

①－３ 電気通信事業法改正案

①－４ 5Gネットワークにおけるセキュリティの確保

②　IoTセキュリティの確保

②－１ NOTICEの現状/NICTERの現状、http(s)への拡大

②－２ 機器メーカとの関係

③　その他の取組

③－１ トラストサービス

③－２ クラウドサービスのサイバーセキュリティ確保

③－３ スマートシティのサイバーセキュリティ確保

③－４ 放送設備のサイバーセキュリティ確保

重要インフラ行動計画の改定

- サイバーセキュリティ基本法に基づき、重要インフラの14分野（総務省所管の情報通信（通信・放送）を含む。）及び重要インフラの安全基準等の整備・浸透、情報共有体制の強化等を内容とする「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」（平成29年4月サイバーセキュリティ戦略本部決定）が策定されている。
- 現在、サイバーセキュリティ戦略本部重要インフラ専門調査会では、同計画の改定に向けた検討を行っており、パブコメ（令和４年１～２月）を経て、３月22日の同調査会で討議が行われたところ。今後、サイバーセキュリティ戦略本部において審議される見通し。

改定案の概要

1．第４次行動計画における有効な取組は継続

2．サイバーセキュリティ基本法が公布・施行されたことを踏まえて対応

- ✓ 題名を「重要インフラのサイバーセキュリティに係る行動計画」へ
  - 「情報セキュリティ対策」から「サイバーセキュリティ」へ
- ✓ 行動計画はサイバーセキュリティ基本法に基づき策定することを明示
- ✓ 「サイバーセキュリティ」の定義を明確化
  - サイバーセキュリティ基本法第２条に規定する「サイバーセキュリティ」をいう電磁的方式による情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること
- ✓ 関係主体の責務を明確化
  - 「国」、「地方公共団体」、「重要インフラ事業者」、「サイバー関連事業者その他の事業者」

3．障害対応体制の強化の在り方を抜本的に見直し

- ✓ 現在の「経営層への働きかけ」から、組織統治にサイバーセキュリティを組み入れる方針を具体的に記載

4．将来の環境変化を先取り

- ✓ サプライチェーン等を含め包括的に対応

内閣サイバーセキュリティセンターホームページ「『重要インフラのサイバーセキュリティに係る行動計画（案）』に関する意見の募集について」より抜粋

（参考）重要インフラ行動計画の改定案 要点

1.「重要インフラ防護」の目的

重要インフラにおいて、任務保証の考え方を踏まえ、重要インフラサービスの継続的提供を不確かなものとする自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等をリスクとして捉え、リスクを許容範囲内に抑制すること、及び重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ることの両面から、強靭性を確保し、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現すること。

2. 関係主体の責務

- 関係主体の責務は、サイバーセキュリティ基本法(平成26年法律第104号)を基本とする。
- 国は、サイバーセキュリティに関する総合的な施策を策定し、及び実施する。
- 地方公共団体は、サイバーセキュリティに関する自主的な施策を策定し、及び実施する。
- 重要インフラ事業者は、サービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努める。

（重要インフラ事業者等を構成）

- サイバー関連事業者その他の事業者は、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努める。

3. 基本的な考え方

- 重要インフラを取り巻く情勢は、システム利用の高度化、複雑化、サイバー空間の脅威の急速な高まりを受け、重要インフラ事業者等においては、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応を一層促進する。特に、経営の重要事項としてサイバーセキュリティを取り込む方向で推進する。
- 自組織の特性を明確化し、経営層からシステム担当者までの各階層の視点を有機的に組み合わせたリスクマネジメントを活用し、自組織に最も適した防護対策を実施する。
- 重要インフラを取り巻く脅威の変化に適確に対応するため、サプライチェーン等を含め、将来の環境変化を先取りした包括的な対応を実施する。

4. 障害対応体制の強化に向けた取組

- リスクマネジメントによる事前対応と危機管理の組合せにより、障害対応体制を強化する。
- 組織におけるサイバーセキュリティに対する経営者と専門組織の関係を経営の重要事項としてサイバーセキュリティを取り込む。
- サイバーセキュリティの確保には、サイバーセキュリティ基本法第2条の定義を踏まえ、外部からの攻撃のみならず、システム調達、設計及び運用に関係する事象を含め対応できるよう障害対応体制を整備・運用する。

内閣サイバーセキュリティセンターホームページ「『重要インフラのサイバーセキュリティに係る行動計画（案）』に関する意見の募集について」より抜粋

（参考）重要インフラ行動計画の改定

改定案における施策群と補強・改善の方向性等

改定案における施策群	第4次行動計画の施策群との対応	第4次行動計画からの主な補強・改善の方向性
1.障害対応体制の強化	「4.リスクマネジメント及び対処態勢の整備」の一部と「5.防護基盤の強化」の一部を統合した上で整理	○ 重要インフラ防護を適切に行うためには、経営層、CISO、戦略マネジメント層、システム担当等組織全体及びサプライチェーン等に関わる事業者の取組の必要性が高まってきていることを踏まえ、組織統治の一部としての障害対応体制の強化を推進 ○ サイバーセキュリティを取り巻く環境が大きく変化することを背景としたサプライチェーン・リスク等の新たな脅威への先取りした対応の推進 ○ 重要インフラ事業者等の自組織のリスクに応じた最適な防護対策の推進 ○ 政府と重要インフラ事業者等の相互連携を密にした官民一体としての対応を検討 ○ 事前対応のリスクマネジメントと障害発生時の危機管理の一体的な対応の推進
2.安全基準等の整備及び浸透	「1.安全基準等の整備及び浸透」を基本的に踏襲	○ 障害対応体制の強化及びリスクマネジメントに資する安全基準等を整備することを明確化 ○ 重要インフラ事業者等の取組の継続的な改善を図ることができる調査手法の検討
3.情報共有体制の強化	「2.情報共有体制の強化」を「3.障害対応体制の強化」の一部と統合した上で整理	○ 重要インフラ事業者等の自主的な取組の活性化を前提とした共助の推進 ○ ISAC連携等による分野間・官民連携の枠組みの整備の検討 ○ ナショナルサートの枠組みの強化の検討との整合性保持
4.リスクマネジメントの活用	「4.リスクマネジメント及び対処態勢の整備」の一部を整理	○ 組織の特性を踏まえた経営層による組織のリスクの明確化 ○ 自組織に適した防護対策の実現を支援するため、既存の手引書の見直しに加え、既存の基準類をどのように自組織に活用するかを含めた新たなガイダンスの整備の方向性の明示 ○ 2020年東京オリンピック・パラリンピック競技大会開催に向けて官民が連携して行ってきた取組の活用を検討
5.防護基盤の強化	「5.防護基盤の強化」の一部を「3.障害対応体制の強化」の一部と統合した上で整理	○ 障害対応体制の有効性検証としての分野横断的演習の推進 ○ 警察による重要インフラ事業者等との協力等の必要な取組の支援 ○ デジタル庁と連携した地方公共団体及び重要インフラに関連する準公共部門におけるサイバーセキュリティの確保に向けた支援等の実施

内閣サイバーセキュリティセンターホームページ「『重要インフラのサイバーセキュリティに係る行動計画（案）』に関する意見の募集について」より抜粋

海外の政策動向

米国

- FCCは、3月11日、ネットワーク間でのインターネットトラフィックルーティングに利用されているBorder Gateway Protocol（BGP）の脆弱性に関する意見募集を開始した（5月10日まで）。
- BGPについて、インターネット上で個別に管理されるネットワークの数が少なく、ネットワーク間の信頼も高かった時代に生まれたものだとし、「BGPの初期設計は現在も広く使われているが、交換される情報の信頼性を確保するセキュリティ機能は用意されていない」と指摘。
- FCCはBGPの脆弱性がもたらすリスクとして、電子メールやウェブトラフィックの劣化、VoIP通話の着信障害、911などの公共安全業務の障害などを挙げており、今回の意見募集では、ネットワーク事業者がBGPの脆弱性対策を導入する上での課題、インターネットの通信速度等への悪影響、必要となるコスト等について意見を求めている。

英国

- 2021年11月に施行された電気通信（セキュリティ）法は、ネットワーク障害や機密データの盗難を引き起こす可能性のあるサイバー脅威からネットワークを守るため、公共通信事業者に強力な法的義務を課している。
- デジタル・文化・メディア・スポーツ省（DCMS）は3月1日、同法の下で電気通信事業者が法的義務を果たすために必要な具体的措置の概要を示した規則案と、事業者が規制を遵守する方法に関する実施規則案の公開諮問を開始した（5月10日まで、今年後半に施行される予定）。
- 規則案では、電気通信事業者に対して、「ネットワークやサービスに保存されているデータを保護し、それらを運用・管理するための重要な機能を保護すること」、「公共ネットワークを監視して潜在的に危険な活動を特定し、そのセキュリティリスクを深く理解し、定期的に社内取締役会に報告すること」などが法的に要求される。

豪州

- 豪州インフラ・運輸・地域開発・通信省は、2月25日、通信事業者等への新たなセキュリティ情報提供義務の設計案について意見募集を開始（3月29日まで）。通信事業者等には、重要インフラ資産の登録及びサイバーセキュリティインシデントの報告（重大なものは認知してから12時間以内、その他は72時間以内）義務が課せられる。

FMMC収集・提供情報などより抜粋

①　電気通信事業者におけるサイバーセキュリティ対策の推進

①－１ 国内外の動向

①－２ 電気通信事業者によるサイバー攻撃対策

①－３ 電気通信事業法改正案

①－４ 5Gネットワークにおけるセキュリティの確保

②　IoTセキュリティの確保

②－１ NOTICEの現状/NICTERの現状、http(s)への拡大

②－２ 機器メーカとの関係

③　その他の取組

③－１ トラストサービス

③－２ クラウドサービスのサイバーセキュリティ確保

③－３ スマートシティのサイバーセキュリティ確保

③－４ 放送設備のサイバーセキュリティ確保

電気通信事業者によるサイバー攻撃対策

➢ 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。

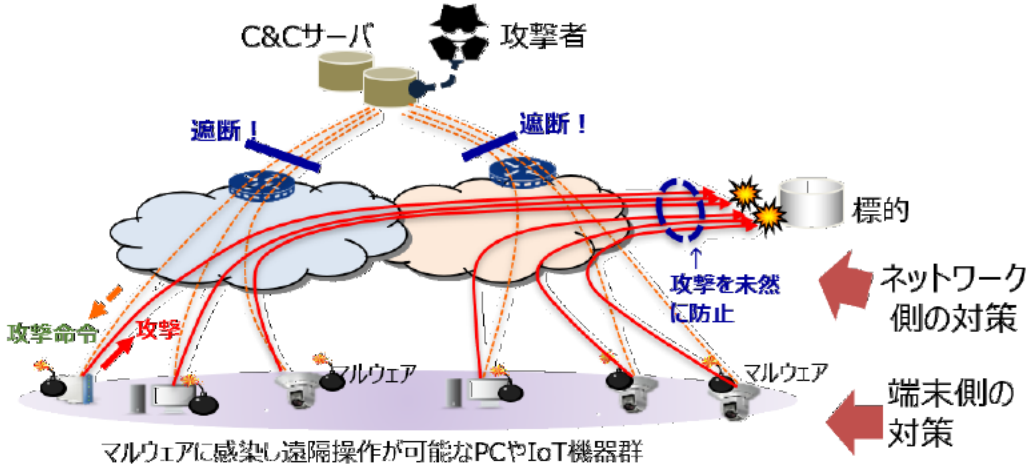
（１）通信の秘密に係る法的整理

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）※「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４年度に、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行う。事業の成果を踏まえ、令和５年度も継続的に実証事業を実施予定。



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）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

- サイバー攻撃が巧妙化・複雑化する中で、電気通信事業者が通信の秘密等に配慮しつつ、新たな対策や取組を講じていくことが可能となるよう、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ついて検討を行うことを目的として、「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」（総合通信基盤局長及びサイバーセキュリティ統括官による原則非公開の研究会）を開催している。
- 平成26年４月には「第一次とりまとめ」、平成27年９月には「第二次とりまとめ」、平成30年９月に「第三次とりまとめ」を公表。
- 今般、サイバー攻撃に予防的に対処するため、①ISPが、平時から自らのネットワーク内の通信トラフィックデータを把握・分析し、C&Cサーバである可能性が高い機器の検知等を行うこと、②検知したC&Cサーバである可能性が高い機器に関する情報を他の電気通信事業者と共有することについて、令和３年６月より通信の秘密との関係性の整理のための検討を行い、同年11月に「第四次とりまとめ」を公表。
- 第一次～第四次とりまとめについては、関係団体が作成する「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」に反映されている。

＜通信の秘密の保護について＞

原則：電気通信事業者の取扱中に係る通信の秘密は、侵してはならない（電気通信事業法第4条第1項）

例外①：通信当事者の有効な同意がある場合

※原則として、通信当事者が個別具体的かつ明確に同意した場合でなければ有効な同意があるとはいえない。

例外②：違法性阻却事由がある場合

・**法令行為**に該当する場合（他の法令の規定に基づき正当に行う行為）

・**正当業務行為**に該当する場合
（電気通信事業者として電気通信役務の提供等の業務を遂行するために必要であって、①目的の正当性、②行為の必要性、③手段の相当性の要件を満たす行為）

・**緊急避難、正当防衛**に該当する場合
（緊急避難の要件（①現在の危難の存在、②法益の権衡、③行為の補充性）、正当防衛の要件（①急迫不正の侵害、②自己又は他人の権利を防衛するため、③やむを得ずした行為）を満たす行為）

①　電気通信事業者におけるサイバーセキュリティ対策の推進

①－１ 国内外の動向

①－２ 電気通信事業者によるサイバー攻撃対策

①－３ 電気通信事業法改正案

①－４ 5Gネットワークにおけるセキュリティの確保

②　IoTセキュリティの確保

②－１ NOTICEの現状/NICTERの現状、http(s)への拡大

②－２ 機器メーカとの関係

③　その他の取組

③－１ トラストサービス

③－２ クラウドサービスのサイバーセキュリティ確保

③－３ スマートシティのサイバーセキュリティ確保

③－４ 放送設備のサイバーセキュリティ確保

電気通信事業法の一部を改正する法律案（概要）

➢ 電気通信事業を取り巻く環境変化を踏まえ、電気通信サービスの円滑な提供及びその利用者の利益の保護を図るため、以下の措置を講ずる（令和４年３月４日閣議決定、国会提出）。

情報通信インフラの提供確保

■ ブロードバンドサービスについては、契約数が年々伸び、「整備」に加え、「維持」の重要性も高まっている。

■ 新型コロナウイルス感染症対策を契機とした社会経済活動の変化により、テレワークや遠隔教育などのデジタル活用の場面が増加している。

※ デジタル田園都市国家構想の実現のためにも、ブロードバンドの全国整備・維持が重要。

■ 一定の**ブロードバンドサービスを基礎的電気通信役務（ユニバーサルサービス）に位置付け**、不採算地域におけるブロードバンドサービスの安定した提供を確保するための**交付金制度を創設**する。

■ 基礎的電気通信役務に該当するサービスには、**契約約款の作成・届出義務、業務区域での役務提供義務等**を課す。

②

①

安心・安全で信頼できる通信サービス・ネットワークの確保

■ 情報通信技術を活用したサービスの多様化やグローバル化に伴い、情報の漏えい・不適正な取扱い等のリスク※が高まる中、事業者が保有するデータの適正な取扱いが一層必要不可欠となっている。

※ 国外の委託先から日本の利用者に係るデータにアクセス可能であった事案などが挙げられる。

■ 大規模な事業者※ が取得する**利用者情報について適正な取扱い**を義務付ける。

■ 事業者が利用者に関する情報を第三者に送信させようとする場合、**利用者に確認の機会を付与**する。

※ 大規模な検索サービスまたはSNSを提供する事業についても規律の対象とする。

電気通信市場を巡る動向に応じた公正な競争環境の整備

■ 指定設備（携帯大手３社・NTT東・西の設備）を用いた卸役務が他事業者に広く提供される一方、卸料金に長年高止まりとの指摘がなされている。

■ ＮＴＴ東・西が提供する固定電話について、従来の電話交換機網からＩＰ網への移行を令和３年１月に開始、令和７年１月までの完了を予定している。

■ 携帯大手３社・NTT東・西の指定設備を用いた卸役務に係るMVNO等との協議の適正化を図るため、**卸役務の提供義務**及び**料金算定方法等の提示義務**を課す。

■ 加入者回線の占有率（50%）を算定する区域を都道府県から**各事業者の業務区域（例えばNTT東は東日本、NTT西は西日本）**へ見直す。

上記のほか、**認定送信型対電気通信設備サイバー攻撃対処協会（認定協会）の業務の追加、重大事故等のおそれのある事態の報告制度の整備**等を行う。

電気通信事業ガバナンス検討会　第18回会合（令和４年４月15日）参考資料18-２より抜粋・一部編集

（参考）電気通信事業ガバナンス検討会

1．背景・目的

- **「デジタル社会」の実現**のためには、その中枢基盤として、サイバー空間とフィジカル空間を繋ぐ神経網である**通信サービス・ ネットワークが安心・安全で信頼され、継続的・安定的かつ確実に提供されることが不可欠。**
- 最近、通信サービス・ネットワークを司る電気通信事業者において、利用者の個人情報や通信の秘密の漏えい事案が発生し、海外の委託先等を通じ、これらのデータにアクセス可能な状態にあることに関する**リスク等が顕在化。**
- 更に、電気通信事業者に対するサイバー攻撃により、通信サービスの提供の停止に至る事案や、通信設備に関するデータが外部に漏えいした恐れのある事案など、サイバー攻撃の**リスク等が深刻化。**
- デジタル時代における安心・安全で信頼できる通信サービス・ネットワークの確保を図るため、**電気通信事業者における**サイバーセキュリティ対策と**データの取扱い等に係るガバナンス確保の在り方を検証し、今後の対策を検討。**

2．主な検討事項

① 電気通信事業者におけるサイバーセキュリティ対策とデータの取扱い等に係るガバナンス確保の今後の在り方
② 上記①を踏まえた、政策的な対応の在り方
③ その他

3．体制

- データ、サイバーセキュリティ及びガバナンスに関する有識者から構成される検討会（座長：大橋教授）を設置。
- 構成員及びオブザーバーは右のとおり。

大橋　弘	東京大学公共政策大学院院長
相田　仁	東京大学大学院工学系研究科教授
石井　夏生利	中央大学国際情報学部教授
上沼　紫野	虎ノ門南法律事務所弁護士
後藤　厚宏	情報セキュリティ大学院大学学長
中尾　康二	（一社）ICT-ISAC顧問 （国研）NICTサイバーセキュリティ研究所主管研究員
中村　修	慶應義塾大学環境情報学部教授
古谷　由紀子	（公社）日本消費生活アドバイザー・コンサルタント・相談員協会監事
森　亮二	英知法律事務所弁護士
山本　龍彦	慶應義塾大学大学院法務研究科教授

※ 内閣官房国家安全保障局、デジタル庁、NISC、個人情報保護委員会事務局がオブザーバー参加

4．開催状況

- 令和3年5月12日に第1回会合を開催し、令和4年2月18日までに17回の会合を開催。
- パブコメ（1月15日～2月4日）を経て、2月18日に報告書を公表。

電気通信事業ガバナンス検討会　第17回会合（令和４年２月18日）　参考資料17-１より抜粋

①利用者に関する情報の適正な取扱いに係る制度整備

大量の情報を取得・管理等する電気通信事業者を中心に、諸外国における規制等との整合を図りつつ、利用者に関する情報の適正な取扱いを促進するための新たな規律を整備。

【 現状・課題 】

利用者情報の適正な取扱い

- **デジタル変革時代のイノベーションを促進するため安心・安全な電気通信サービスの確保**が不可欠
- **諸外国の法的環境の変化、サイバー攻撃の複雑化**により、利用者が安心して利用できる電気通信サービスの提供の確保が急務
- 特に、**大量の利用者情報を取り扱う事業者**には一層の高い信頼性の確保が必要

利用者の情報の外部送信

- 利用者がアプリやwebサイトを利用する際、タグ等により、**利用者の意思によらず第三者に自身の情報が送信**されている場合がある

【 規律の内容 】

1. 利用者の利益に及ぼす影響が大きい電気通信事業者(例:利用者数1000万人以上)に対する義務

利用者情報を守るための必要最小限の規律 → 効果

- ・利用者情報※の取扱いに関する**社内ルール**(取扱規程)**の策定**、利用者情報の**取扱方針の公表等**
  (記載事項例:安全管理の方法等)
  → **電気通信サービスの高い信頼性を保持**するとともに、**利用者自らが安心して利用できるサービスを選択**することが**可能となる**
- ・利用者情報の取扱いに関する**自己評価**、取扱規程・取扱方針への反映
  → **自ら PDCAを実施して、各事業者の実態を踏まえた情報の適正な取扱い体制を確保**
- ・利用者情報の**統括責任者**の選任等
  → **全体的観点からの適切な判断や、情報漏えい時の迅速な対応が可能となる**

※ 利用者に関する情報のうち、通信の秘密に該当する情報、役務契約を締結又はID等により利用登録をした利用者の情報を想定。

大規模な検索サービスまたはSNSを提供する事業についても規律の対象とする。

2. 電気通信事業者※に対する義務

- ・利用者に電気通信サービスを提供する際に、**情報を外部送信**する指令を与える電気通信を送信する場合、**確認の機会を付与**
  → 利用者が意図しない情報の外部送信がなくなり、**利用者が安心して電気通信サービスを利用することが可能となる**

※ 電気通信設備を用いて他人の通信を媒介する電気通信役務以外の電気通信役務を電気通信回線設備を設置することなく提供する電気通信事業(電気通信事業法第164条第1項第3号)を営む者を含む。利用の状況からみて利用者に与える影響が少なくない者に限る。

電気通信事業ガバナンス検討会 第18回会合(令和４年４月15日)資料18-２より抜粋・一部編集

②電気通信サービスの停止に関するリスクの対応に係る制度整備

事業者間連携によるサイバー攻撃対策や事故報告制度について、電気通信役務の安定的な提供の確保を目的とした規律を整備。

	【 現状・課題 】	【規律の内容 】	
事業者間連携によるサイバー攻撃対策	➢ サイバー攻撃では、指令元、攻撃元、攻撃先が複数のISPにまたがる場合が多く、ISP間の連携協力が必要	・これまではサイバー攻撃の発生後に限られていた**ISP間の情報共有や分析をサイバー攻撃の発生前にも実施できるようにするための環境を整備**	⇒ ISP間の連携が促進され、より機動的なサイバー攻撃対策が可能に
重大事故等のおそれのある事態の報告制度	➢ 電気通信サービスの事故原因が多様化※ ※ 設備の設定（通信経路等）の誤り、他者の提供する設備やサービスの不具合等 ➢ 電気通信サービスの停止が社会に及ぼす影響の増大	・これまでの重大事故等が生じた際の遅滞のない報告に加え、**重大事故等のおそれのある事態に関する報告制度を整備**	⇒ より精緻な実態把握や原因分析等が可能となり、重大な事故等の発生の未然防止や被害軽減に寄与

電気通信事業ガバナンス検討会 第18回会合（令和４年４月15日）資料18-２より抜粋・一部編集

①　電気通信事業者におけるサイバーセキュリティ対策の推進

①－１ 国内外の動向

①－２ 電気通信事業者によるサイバー攻撃対策

①－３ 電気通信事業法改正案

①－４ 5Gネットワークにおけるセキュリティの確保

②　IoTセキュリティの確保

②－１ NOTICEの現状/NICTERの現状、http(s)への拡大

②－２ 機器メーカとの関係

③　その他の取組

③－１ トラストサービス

③－２ クラウドサービスのサイバーセキュリティ確保

③－３ スマートシティのサイバーセキュリティ確保

③－４ 放送設備のサイバーセキュリティ確保

5Gネットワークにおけるセキュリティ確保に向けた調査・検討

- 国家が背景にあるとみられるサイバー攻撃も増加する中、情報通信ネットワークやICTサービス等の**サイバー空間を構成する様々な要素に関するサプライチェーンリスク問題が国際的に顕在化**
  - ⇨ **サイバーセキュリティ上のサプライチェーンリスクに対応するための我が国としての技術検証体制の整備が急務に**（次ページに参考資料）

- 一方、**重要インフラである通信ネットワークの5G化が進展**
  - ⇨ サプライチェーンリスクの発現を含め、**5Gのセキュリティが不十分となれば、我が国の社会経済活動や国民生活に甚大な被害が発生**するおそれ

- **総務省では、5Gネットワークに関するサプライチェーンリスク対策を含むサイバーセキュリティの確保のため**、5G向け周波数の割り当て等の制度面での対応や、安全で信頼できる5Gを対象とした投資促進税制等の取組を進めつつ、政府全体の技術検証体制の整備の一環として、**5Gネットワークのセキュリティについての技術的な検証の取組*を実施**
  （⇨資料37-2-2で報告）

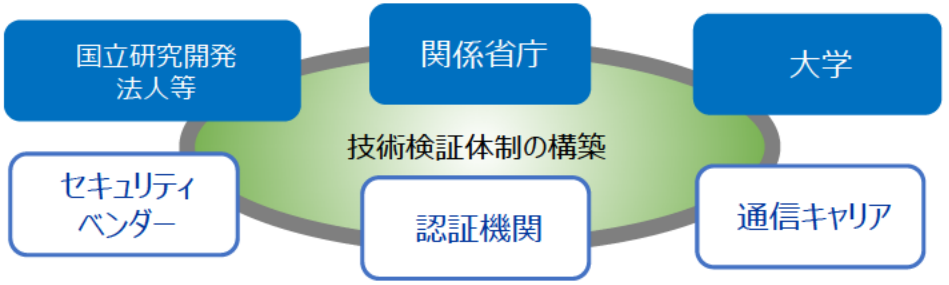
*令和元年度～3年度 総務省予算事業「5Gネットワークにおけるセキュリティ確保に向けた調査・検討等」

（参考）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

- 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、5Gネットワークのセキュリティ確保や、サイバーセキュリティの検証ビジネスの活性化などをはじめとして、ICT機器・サービスの信頼性を確保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。

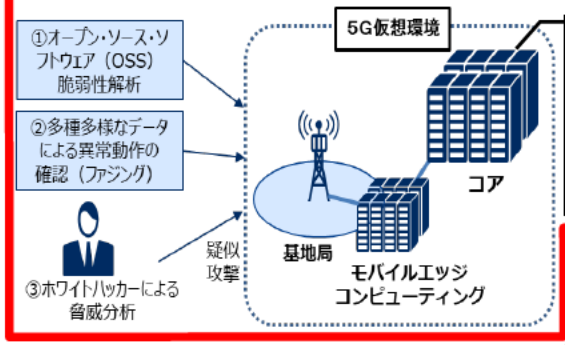
オールジャパンの官民連携体制の構築

○関係省庁に加え、公的研究機関や大学、民間のセキュリティーベンダーや通信キャリア等と連携し、 技術検証体制を構築（内閣官房）

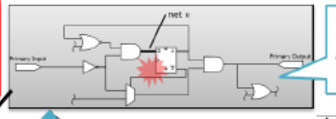


技術検証体制を支える施策の推進

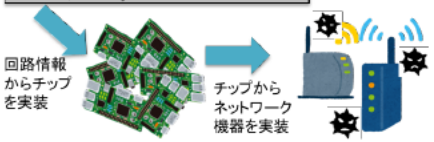
○５Gを含むシステム等に組み込まれた不正な機能や脆弱性を効率的に検出する技術開発・検証（総務省）



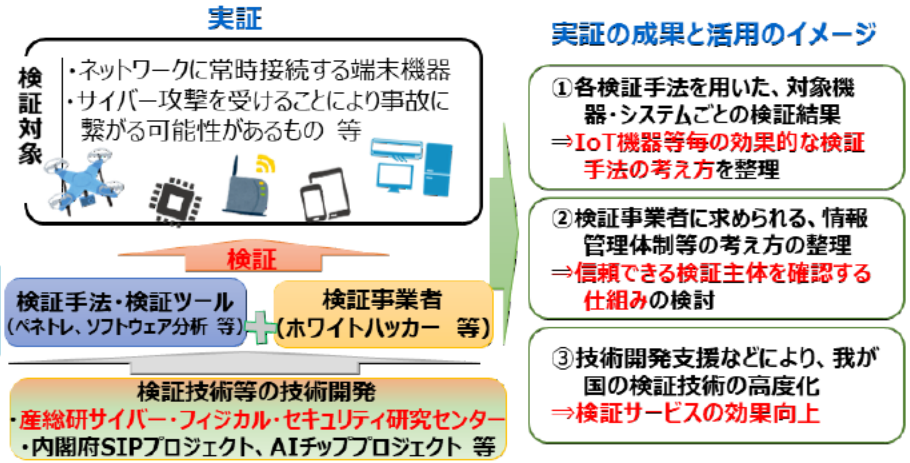
- 標準化動向の調査やリスク検討
- 5G仮想環境を構築、オープンソースソフトウェアの解析、ファジング、ホワイトハッカーによる脆弱性調査等を実施



- AIを活用して回路情報や電力波形等から不正回路を検知する技術の開発等を推進



○攻撃型手法を含むハイレベルな検証サービスの実証（経済産業省）



○IoT社会に対応したサイバー・フィジカル・セキュリティ（内閣府）

・IoTシステム・サービス及び中小企業を含む大規模サプライチェーン全体を守ることに活用できる「サイバー・フィジカル・セキュリティ対策基盤」の開発と実証

①　電気通信事業者におけるサイバーセキュリティ対策の推進

①－１ 国内外の動向

①－２ 電気通信事業者によるサイバー攻撃対策

①－３ 電気通信事業法改正案

①－４ 5Gネットワークにおけるセキュリティの確保

②　IoTセキュリティの確保

②－１ NOTICEの現状/NICTERの現状、http（s）への拡大

②－２ 機器メーカとの関係

③　その他の取組

③－１ トラストサービス

③－２ クラウドサービスのサイバーセキュリティ確保

③－３ スマートシティのサイバーセキュリティ確保

③－４ 放送設備のサイバーセキュリティ確保

前々回タスクフォースの振り返り

総務省におけるこれまでの取組（前々回タスクフォース資料抜粋、一部時点更新）

○IoTのセキュリティ

＜NOTICE＞

・2018年の国立研究開発法人情報通信研究機構法（平成11年法律第162号）の改正により、国立研究開発法人情報通信研究機構（NICT）の業務に、パスワード設定等に不備のあるIoT機器の調査等を5年間（2024年3月31日まで）の時限措置として追加。2019年2月より、NICTがIoT機器を調査し、電気通信事業者（ISP）を通じて利用者への注意喚起を行うプロジェクト「NOTICE」を実施。これまでに、約36,000件の（2022年3月時点）注意喚起対象をISPに通知。

＜NICTER＞

・2019年6月より、既に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を通じて利用者へ注意喚起を行う取組を実施。１日平均約200件の注意喚起対象をISPに通知。

＜端末設備等規則の改正等＞

・電気通信事業法の枠組みの中で、IoT機器を含む端末設備のセキュリティを確保するため、端末設備等規則（昭和60年郵政省令第31号）の一部改正を実施し、2020年4月に施行（あわせて、民間の任意の認証制度として、一般社団法人重要生活機器連携セキュリティ協議会（CCDS）において、IoT機器のセキュリティ要件を定め認証プログラムを実施）。

前々回タスクフォースでお寄せいただいた意見（抜粋）

- ✓ IoT機器等のセキュリティ強化においては、個人だけでなく組織に対しても、どのように情報提供のリーチャビリティを高め、今までの様々な施策を有効活用していくかという点が重要。（吉岡構成員）
- ✓ 保証期間を終えた機器や中古機器に加え、製造元が解散しておりパッチの提供ができず、注意喚起すらできないIoT機器への対処を検討いただきたい。（小山構成員）
- ✓ SSHやtelnetは開いておらず、http、httpsのみで管理ポートが開いている機器が攻撃者の隠れみのになり悪用され続ける問題が根深く残っている。NOTICEの調査対象ポートのhttp、httpsへの拡大について検討いただきたい。（辻構成員）
- ✓ 自らのインターネット利用が世界的に様々なところで迷惑をかけていても、自分自身は不利益を被らないというところがIoTの脆弱性対策が進まない1つの理由と思われる。NOTICEがもっと世間で話題にしてもらえるよう、国民的アニメとのコラボ等を検討してはどうか。（辻構成員）
- ✓ 大規模・広範囲に使用されるIoT機器の不具合につながるOSSの問題等は、総務省だけの取組ではなく、IoT社会の安全性という意味では非常に大きな課題だと認識している。（後藤座長）

①　電気通信事業者におけるサイバーセキュリティ対策の推進

①－１ 国内外の動向

①－２ 電気通信事業者によるサイバー攻撃対策

①－３ 電気通信事業法改正案

①－４ 5Gネットワークにおけるセキュリティの確保

②　IoTセキュリティの確保

②－１ NOTICEの現状/NICTERの現状、http(s)への拡大

②－２ 機器メーカとの関係

③　その他の取組

③－１ トラストサービス

③－２ クラウドサービスのサイバーセキュリティ確保

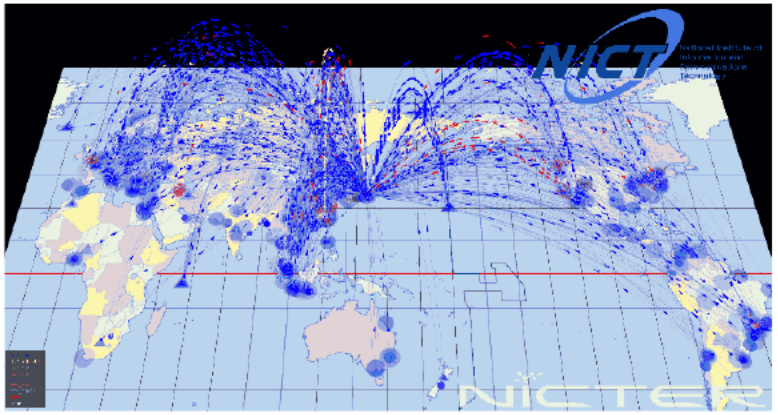
③－３ スマートシティのサイバーセキュリティ確保

③－４ 放送設備のサイバーセキュリティ確保

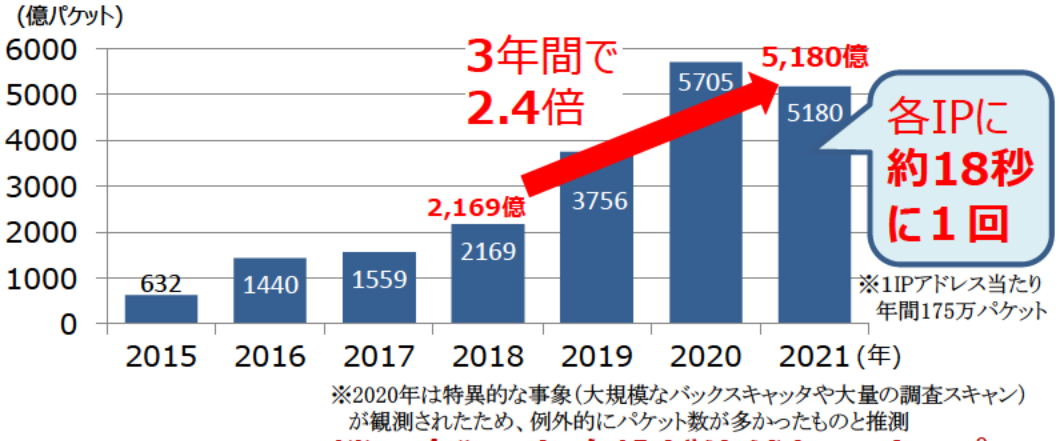
IoT機器を狙った攻撃の情勢（NICTERによる観測）

➢ 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



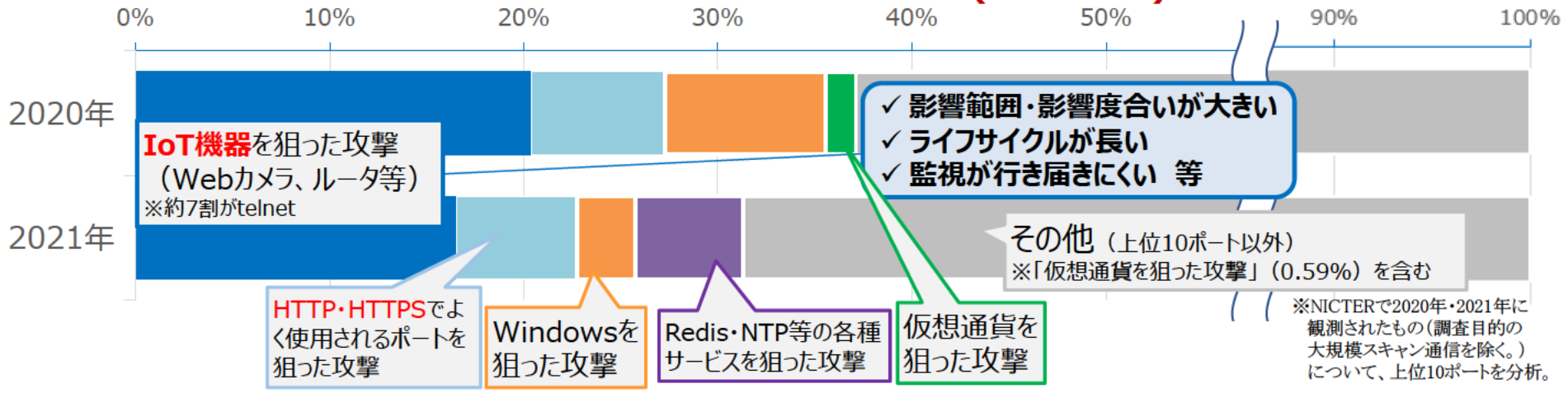
NICTERで１年間に観測されたサイバー攻撃関連の通信数



※2020年は特異的な事象（大規模なバックスキャッタや大量の調査スキャン）が観測されたため、例外的にパケット数が多かったものと推測

NICTERにより観測された通信の内容（上位10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)が多様化**



※NICTERで2020年・2021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10ポートを分析。

現在のNOTICEの実施状況（2022年3月度）

- 参加手続きが完了している**ISP**（インターネット・サービス・プロバイダ）は**69社。**
  当該ISPの**約1.12億IPアドレス**に対して調査を実施。
- **NOTICE**による注意喚起は、**１，６６４件の対象を検知**しISPへ通知。
- **NICTER**による注意喚起は、１日平均**１９３件の対象を検知**しISPへ通知。

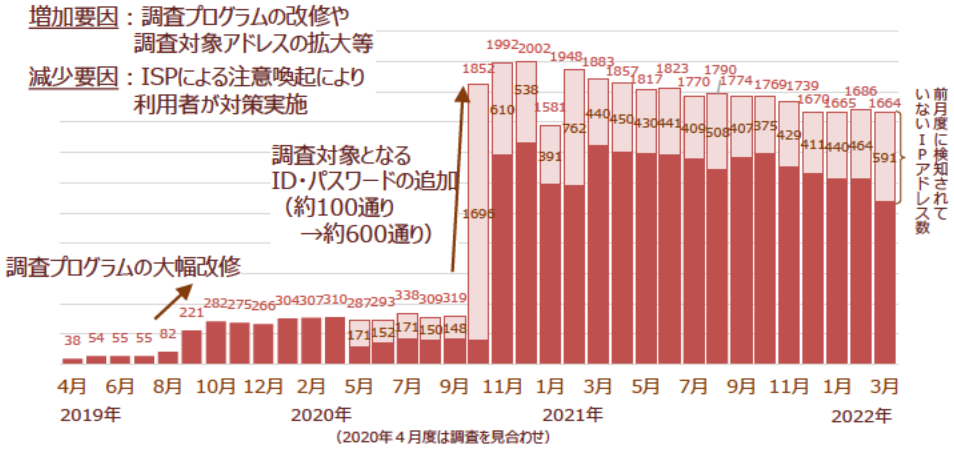
NOTICE注意喚起の取組結果

注意喚起対象としてISPへ通知したもの*

１，６６４件（2月度:1,686件）

（参考）2019年度からの累積件数：36,077件
ID・パスワードが入力可能だったもの：9.8万件

*) 特定のID・パスワードによりログインできるかという調査をおおむね月に1回実施し、ログインでき、注意喚起対象となったもの（ユニークIPアドレス数）



NICTER注意喚起※の取組結果

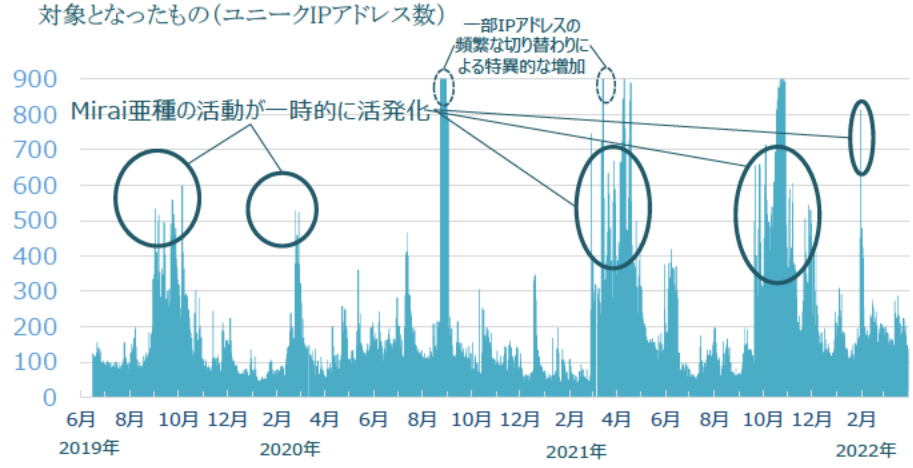
※マルウェアに感染しているIoT機器の利用者への注意喚起

注意喚起対象としてISPへ通知したもの**

１日平均１９３件（2月度:231件）

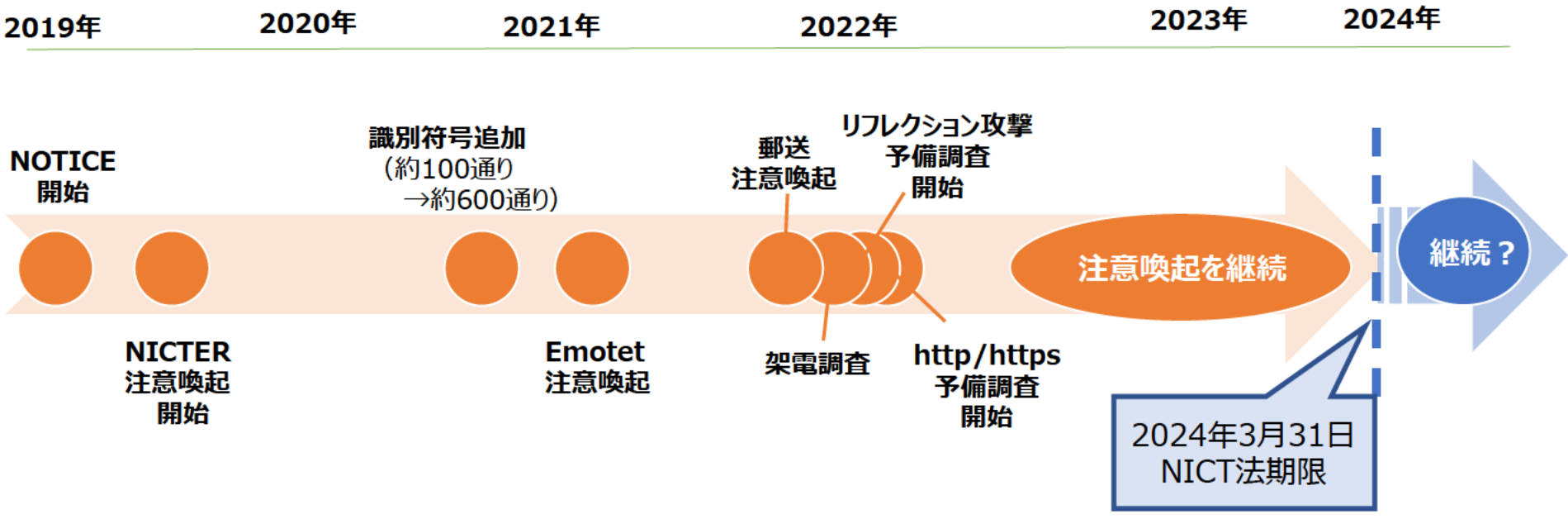
（参考）期間全体での値：１日平均219件
最小：40件(2021/2/10)／最大：3,227件(2020/8/24)

**) NICTERプロジェクトによりマルウェアに感染していることが検知され、注意喚起対象となったもの（ユニークIPアドレス数）



これまでのNOTICEの実施過程

- 2019年のNOTICE開始以降、取組内容の拡大や特異なインシデントへ対応しながら継続。
- 2021年度も様々な取組を実施してきた。
  - ✓ 希望するISPにおいて、**総務省のロゴ入り封筒による郵送の注意喚起**を実施
  - ✓ 注意喚起に対応してもらえていない一部の利用者（法人）に、**架電によるヒアリング**を実施
  - ✓ **リフレクション攻撃に悪用されるおそれのある機器への対処**※に向け、**予備調査を開始**
    ※リフレクション攻撃に用いられやすいリクエストを送信し、応答があった場合にISPへ情報提供することを想定
  - ✓ **http/https**について、ID/パスワードが脆弱な機器の特定・注意喚起の実施に向け、**予備調査**を開始



NOTICEに係る周知広報

- IoT機器のセキュリティ対策の必要性、NOTICEの取組の広報のため、**リーフレット**や**ポスター**を作成し、家電量販店やサイバーセキュリティ関係イベント（セミナー等）で配布。
- 加えて、**政府広報**や**新聞広告、サイネージ広告**等を通じてNOTICEの取組を周知。

リーフレット

セキュリティ関連イベント等で**リーフレット配布**

ポスター

各所での**ポスター掲示**を実施（2019年２月）

- 大手家電量販店（計約3000店舗）
  エディオン系列、ケーズデンキ系列、上新電機、ビックカメラ系列、ヤマダ電機系列
- 地方公共団体（約500団体）
- 東京メトロ駅構内（10駅）
- 電車中吊広告（東京メトロ全線、JR山手線等）

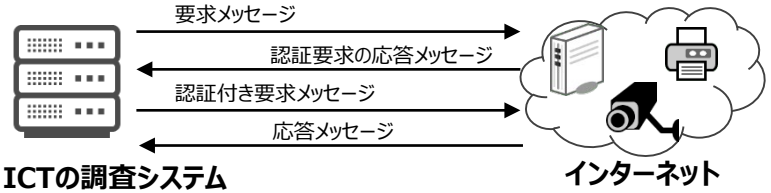
その他

- **政府広報**（ラジオ、全国（TOKYO FM系列） 2019年12月、2021年7月 ）
- **新聞広告**（全国日刊紙 2019年5月、2020年3月）
- **サイネージ公告**（全国主要39駅 2019年2月）
- 総務省広報誌（2019年5月、2020年3月）
- NOTICE HP（実施状況を月ごとに）
- 業界誌への寄稿 等

（参考）http/httpsへの注意喚起拡大について

- NOTICE調査において、これまではTelnet及びSSH(パスワード認証)のみを対象に調査を実施しているところであるが、http/httpsに対しても容易に推測可能なID/パスワードが設定されている機器に対する注意喚起に向けて、令和4年3月より予備調査を開始した。

調査方法（これまでから変更なし）



※IPアドレス、タイムスタンプ、ポート番号、応答メッセージを取得

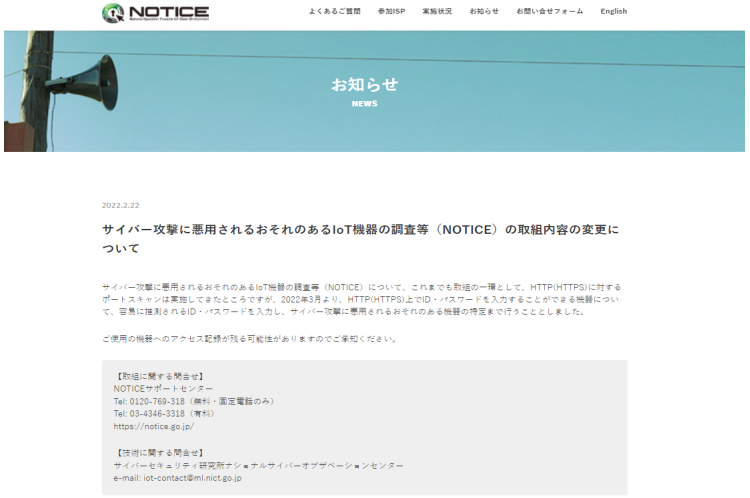
① http/httpsが稼働するポートに対してGETリクエストを送信
② Basic認証もしくはDigest認証を求めるレスポンスが観測された場合は、調査用のID/Passwordを用いて、認証情報を付加して再度リクエストを送信
③ 応答メッセージがエラーでなければ特定アクセス成功と判定

今後の進め方について

- ３月～５月は予備調査としてhttp/httpsの調査を実施
  - ✓ 予備調査の結果を踏まえつつ、実際の調査及び注意喚起に向けたマニュアル作成等の準備を進める。
- （想定） ６月から本調査としてhttp/httpsも調査実施
  - ✓ 注意喚起対象として各ISPへ通知を開始する。

（参考）NICT及びNOTICEのHPでも告知

（出典）https://www.nict.go.jp/publicity/topics/2022/02/22-1.html



（出典）https://notice.go.jp/news/topic/news20220121

①　電気通信事業者におけるサイバーセキュリティ対策の推進

①－１ 国内外の動向

①－２ 電気通信事業者によるサイバー攻撃対策

①－３ 電気通信事業法改正案

①－４ 5Gネットワークにおけるセキュリティの確保

②　IoTセキュリティの確保

②－１ NOTICEの現状/NICTERの現状、http(s)への拡大

②－２ 機器メーカとの関係

③　その他の取組

③－１ トラストサービス

③－２ クラウドサービスのサイバーセキュリティ確保

③－３ スマートシティのサイバーセキュリティ確保

③－４ 放送設備のサイバーセキュリティ確保

インターネット上に存在するIoT機器への対処と機器メーカーとの関係について

- 2019年に端末設備等規則を改正して、①アクセス制御機能、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を具備するよう技術基準に追加された。
- しかし、インターネット上には、脆弱性が放置されたままになっているIoT機器が存在しており、NICTERプロジェクトにおいてこれらがマルウェアへの再感染を繰り返していることが観測されるなど、潜在的な脅威として残存し続けている。
- 各機器メーカーにおいては、新たな脆弱性が発見されれば、ファームウェアのアップデートや使用の中止を促す周知広報を実施していただいている。
- 個別に機器利用者を特定し、注意喚起を行うことが効果的ではあるものの、各機器メーカーにおいては、実際の使用者に関する情報は持ち合わせない。この点、NOTICE/NICTER注意喚起の取組は、IoT機器の利用者を特定できることから、協力できないかと相談をしているところである。
- 一方で、個人情報等の情報共有のあり方や、費用負担の観点から多くの課題が存在している。

（参考）機器メーカー公式サイトにおける脆弱性のお知らせ事例

セキュリティ情報

セキュリティ情報

EL36-221
2021.01.26

無線LANルーターなどネットワーク製品の一部における脆弱性に関して

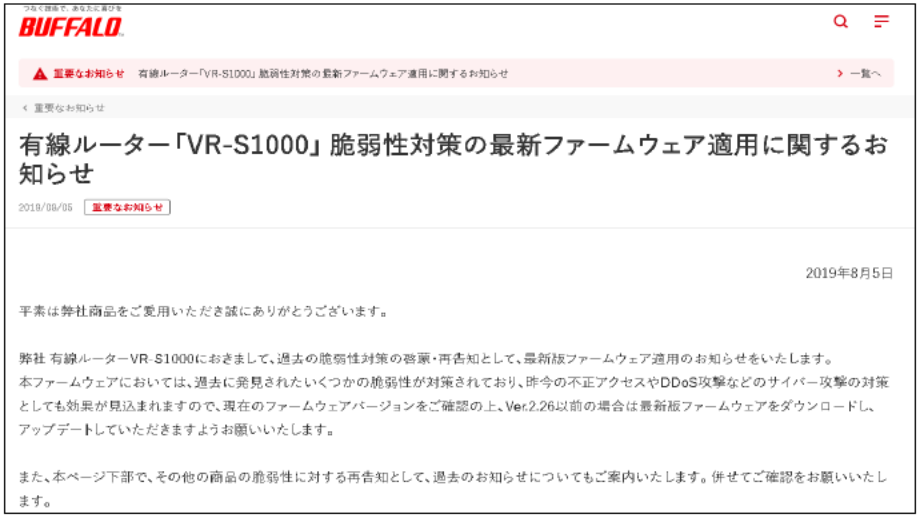
日頃は、当社製品をご愛顧いただきまして、誠にありがとうございます。当社製の一部の無線LANルーターなどネットワーク製品の一部におきまして、以下脆弱性が判明いたしました。

対象製品のアップデートサービスは終了しております。お客様が気づかない状態でも悪用される場合がありますのでセキュリティ保護のため対象製品のご利用を中止いただき、現行製品への切り替えをご検討いただけますようお願い申し上げます。
お客様に大変ご迷惑をおかけしますことを深くお詫び申し上げます。何卒ご理解とご協力を賜りますようお願い申し上げます。

対策方法

本製品の利用を中止する。
現在、弊社にクレームや被害のご報告はございません。
製品の不具合ではございませんが、発売後年数が経過している製品であり、今後も攻撃を受けるリスクがあるため利用中止をお願いしております。

（出典）：https://www.elecom.co.jp/news/security/20210126-01/



BUFFALO

重要なお知らせ　有線ルーター「VR-S1000」脆弱性対策の最新ファームウェア適用に関するお知らせ　一覧へ

重要なお知らせ

有線ルーター「VR-S1000」脆弱性対策の最新ファームウェア適用に関するお知らせ

2019/08/05　重要なお知らせ

2019年8月5日

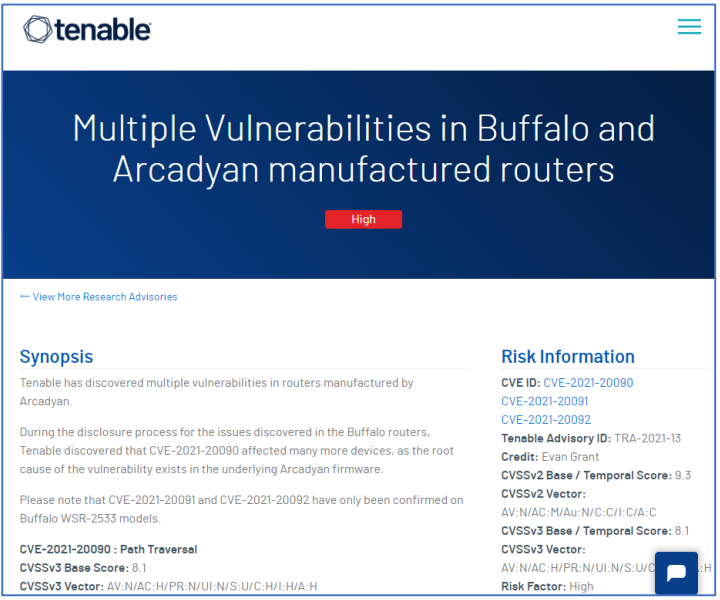
平素は弊社商品をご愛用いただき誠にありがとうございます。

弊社 有線ルーターVR-S1000におきまして、過去の脆弱性対策の蓄積・再告知として、最新版ファームウェア適用のお知らせをいたします。
本ファームウェアにおいては、過去に発見されたいくつかの脆弱性が対策されており、昨今の不正アクセスやDDoS攻撃などのサイバー攻撃の対策としても効果が見込まれますので、現在のファームウェアバージョンをご確認の上、Ver.2.26以前の場合は最新版ファームウェアをダウンロードし、アップデートしていただきますようお願いいたします。

また、本ページ下部で、その他の商品の脆弱性に対する再告知として、過去のお知らせについてもご案内いたします。併せてご確認をお願いいたします。

（出典）：https://www.buffalo.jp/news/detail/20190805-01.html

（参考）NICTERにおける国内感染機器の観測事例①（バッファロー製品）



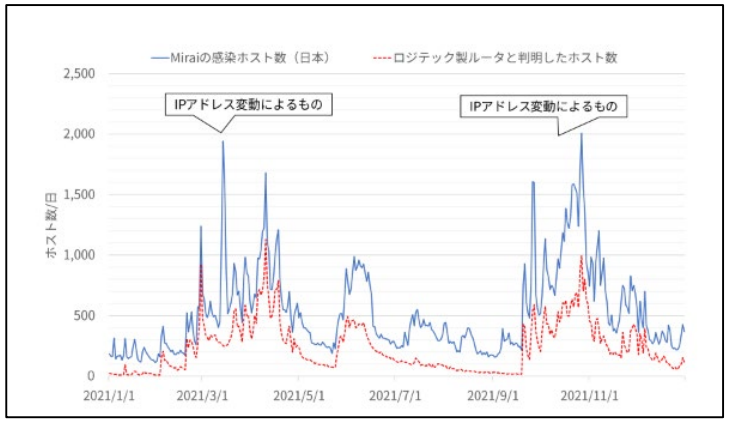
- tenableがArcadyan製のルータの複数の脆弱性（CVE-2021-20090、CVE-2021-20091、CVE-2021-20092）とそれに対するPoCを公開（2021年4月-8月）

- NICTERでは2021年8月以降、BUFFALO製の複数のブロードバンドルータからのパケットを観測
  - ✓ 50ホスト/日前後
  - ✓ APモードで動作し、前述の脆弱性が対策されていない場合、遠隔からのTelnetの有効化と機器へのログインが可能なことを実機で確認
  - ✓ Telnetが一度有効にされると再起動や自動アップデートで対策済のファームウェアにアップデートされてもTelnetは無効にならず、攻撃者によって悪用され続ける可能性がある
  - ✓ 機器に設定された管理画面のパスワードやWi-Fiの設定情報などを取得する攻撃も観測

Multiple Vulnerabilities in Buffalo and Arcadyan manufactured routers
（https://www.tenable.com/security/research/tra-2021-13）

（参考）NICTERにおける国内感染機器の観測事例②（ロジテック製品）

（出典）：JPCERT/CCウェブサイト
「Mirai 亜種の感染活動に関する注意喚起」
https://www.jpcert.or.jp/at/2017/at170049.html



（出典）：NICTERWEB「NICTER 観測レポート 2021」
図4: Mirai の感染ホスト数とロジテックと判明したホストの推移（日本）
https://www.nict.go.jp/cyber/report/NICTER_report_2021.pdf

- 既知の脆弱性（CVE-2014-8361）を持つロジテック製機器が脆弱性を悪用され、マルウェアへの感染を繰り返す実態が確認されている。当該脆弱性は、2015年に公開されたものであり、また2017年の段階で ICT-ISAC や JPCERT/CC、警察庁等からは注意喚起が出されている。
- NICTERでは、これらのロジテック製のブロードバンドルータからの感染と思われるパケットを継続して観測している。
- なお、2012年５月に発見された脆弱性（CVE-2012-1250）によりPPPoEのID/PWが窃取されることが判明し、所有者の洗い出しや、新聞広告によるアップデート依頼を行ったものの放置され続けた機種の残存（27万台中、数千台）も含まれる。

NICTERWEB「NICTER 観測レポート 2021」（抜粋）

URL:https://www.nict.go.jp/cyber/report/NICTER_report_2021.pdf

国内のMirai感染ホストの機器の割合は、昨年同様にロジテック社製の古いブロードバンドルータが一定数を占めていました（図4の赤点線）。該当機器は 52869/TCPで動作するサービスに脆弱性があり、この脆弱性を狙った攻撃は 2021年も継続して観測されました（図5）。9月以降はその件数は減少傾向にありますが、攻撃自体は継続しており、検体のダウンロードサーバ等の攻撃インフラや検体のハッシュ値が数日から数週間で変化する状況を確認しています。

①　電気通信事業者におけるサイバーセキュリティ対策の推進

①－１ 国内外の動向

①－２ 電気通信事業者によるサイバー攻撃対策

①－３ 電気通信事業法改正案

①－４ 5Gネットワークにおけるセキュリティの確保

②　IoTセキュリティの確保

②－１ NOTICEの現状/NICTERの現状、http(s)への拡大

②－２ 機器メーカとの関係

③　その他の取組

③－１ トラストサービス

③－２ クラウドサービスのサイバーセキュリティ確保

③－３ スマートシティのサイバーセキュリティ確保

③－４ 放送設備のサイバーセキュリティ確保

前々回タスクフォースの振り返り

総務省におけるこれまでの取組（前々回タスクフォース資料抜粋（一部更新））

○トラストサービスの普及

・タイムスタンプについて、2021年4月に「時刻認証業務の認定に関する規程（令和3年総務省告示第146号）」を公布し、国によるタイムスタンプの認定制度を整備。

・eシールについては、2021年6月に「eシールに係る指針」を公表し、今後、我が国のeシールにおける信頼の置けるサービス・事業者に求められる技術上・運用上の基準等について整理。

・電子署名については、2020年7月に「電子署名法2条1項に関するQ&A」を、同年9月には「電子署名法3条に関するQ&A」を公表する等、電子署名法上の電子署名の利便性を改善。

○クラウドサービスのセキュリティ

＜提供事業者ガイドラインの改定等＞

・2014年に策定したクラウドサービス提供事業者向けの「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」について、全体の構成見直しや責任共有モデルの考え方、管理策の見直しなどを行い、2021年10月に改定。引き続き、クラウドサービスにおける適切な設定を促す方策を検討中。

＜ISMAPの立ち上げ＞

・政府機関が利用するクラウドサービスの安全性評価の仕組みとして、内閣官房（NISC・IT室（現在のデジタル庁））、総務省及び経済産業省において、2020年6月に「政府情報システムのためのセキュリティ評価制度」（ISMAP）を立ち上げ、2022年3月末現在、35サービスを登録済み。

○スマートシティのセキュリティ

・2020年にスマートシティのセキュリティ対策の指針として策定した「スマートシティセキュリティガイドライン」について、多様な主体の関与、多様なデータの連携などのスマートシティの特徴を踏まえ、2021年6月に第2.0版として改定。国内における普及促進や海外との意見交換の取組を行っている。

○放送事業者におけるサイバーセキュリティ対策

・2019年2月の情報通信審議会答申を踏まえ、放送設備に関するサイバーセキュリティ対策の確保を技術基準に位置づけるとともに、放送設備に関する定期状況報告の際、サイバー事案に起因する事故報告を明記して報告を求めることを内容として、放送法施行規則（昭和25年電波監理委員会規則第10号）等を改正し、2020年3月に施行。これまでにサイバー事案に起因する事故の報告なし。

前々回タスクフォースでお寄せいただいた意見（抜粋）

✓ クラウドサービスの障害は、ユーザ側の設定ミスというよりは、仕様変更に関するユーザ側と事業者側とのコミュニケーション不整合に起因しているもの。情報通信全体に関して、仕様変更の際にはコミュニケーションをきちんと取ることによって、そうした不整合を解消していく必要があるのではないか。（岡村構成員）

✓ サイバー攻撃は今やネットワークに対する脆弱性を突いた行為だけではなく、人間の脳の脆弱性を突いた行為にも及んでいる。NATOが概念として示しているCognitive Warfare（認知戦）のように、計画的に人間に対して特定の情報を浴びせて認知を変化させることで、民主主義国家における考え方を二極化させる影響工作に対する検討や状況認識を進めていく必要がある。（名和構成員）

①　電気通信事業者におけるサイバーセキュリティ対策の推進

①－１ 国内外の動向

①－２ 電気通信事業者によるサイバー攻撃対策

①－３ 電気通信事業法改正案

①－４ 5Gネットワークにおけるセキュリティの確保

②　IoTセキュリティの確保

②－１ NOTICEの現状/NICTERの現状、http(s)への拡大

②－２ 機器メーカとの関係

③　その他の取組

③－１ トラストサービス

③－２ クラウドサービスのサイバーセキュリティ確保

③－３ スマートシティのサイバーセキュリティ確保

③－４ 放送設備のサイバーセキュリティ確保

eIDAS規則改正提案について

- 2014年7月23日、市民、企業、公的機関が、オンラインサービスへのアクセスや電子取引の管理を行う際に、eIDやトラストサービスを利用できるようにするため、eIDAS規則(Regulation (EU) No 910/2014)を制定した。
- 4年ごとに行われるeIDAS規則のレビューを踏まえ、2021年6月に欧州委員会から改正法の草案が示された。

eIDAS規則とは

欧州域内のデジタル単一市場の実現を目標に、

①加盟国が、他の加盟国の自然人及び法人のeIDを承認する条件
②トラストサービス(電子署名、eシール、タイムスタンプ、eデリバリー、ウェブサイト認証証明書)の定義や法的効果、各加盟国の監督機関による適格なトラストサービスやプロバイダの認定制度等を規定しているEU規則。

eIDAS規則改正提案のポイント

（1）EU Digital Identity Wallet(EUDIW)の枠組み整備

- EUの公的及び民間のデジタルサービスにおける本人確認に利用できるEUDIWについて、希望する全EU市民が利用できるような枠組み整備を加盟国に義務づける。
- EUDIWを用いることで、個人識別データの交換、適格電子署名、電子属性証明が可能とされている。

（2）トラストサービスの拡充

- 電子アーカイブ、電子台帳等の新しいトラストサービスについて定義・法的効果を規定する。

（3）下位規則の整備

- 技術基準を指定する下位規則の整備を欧州委員会に義務づける。

トラストを確保したDX推進サブワーキンググループ

- 令和3年11月より、デジタル庁の「データ戦略推進ワーキンググループ」の下に「トラストを確保したDX推進サブワーキンググループ」が発足。

トラストを確保したDX推進SWGでの検討項目（案）

官民での様々な手続・取引について、デジタル化のニーズや、必要なアシュアランスレベルを検討し、デジタル化の障壁を特定することで、官民でのDXを加速する。

1. トラストスコープの再整理
2. トラスト確保の実態調査
   - デジタル化できる手続・取引の見取り図やボリュームを把握
   - 手続・取引におけるデジタル化阻害要因の特定
3. ID及びトラストサービスに関するアシュアランスレベルの整理
4. 技術発展やトラストサービス利用者の利便性増大が可能となる枠組みの基本的考え方
5. トラスト確保に向けた国の関与の在り方

ユースケースを特定し検証

5

トラストを確保したDX推進サブワーキンググループ（第1回）資料より抜粋

eデリバリーについて

- eデリバリー（送受信者の識別とデータの送受信日時の正確性、送受信データの完全性を保証する仕組み）についてEUにおけるユースケースの調査を令和3年度に実施。
- 債権譲渡通知等で用いられる、配達証明付き内容証明郵便の電子化への利用可能性を含め、研究中。

eIDAS規則における定義

- eIDAS規則では以下２種類のeデリバリーを規定。

●eデリバリー

データ送受信の証拠等を提供し、送信されたデータを損失、破損や窃盗、損害、又は不正な変更のリスクから保護する手段。

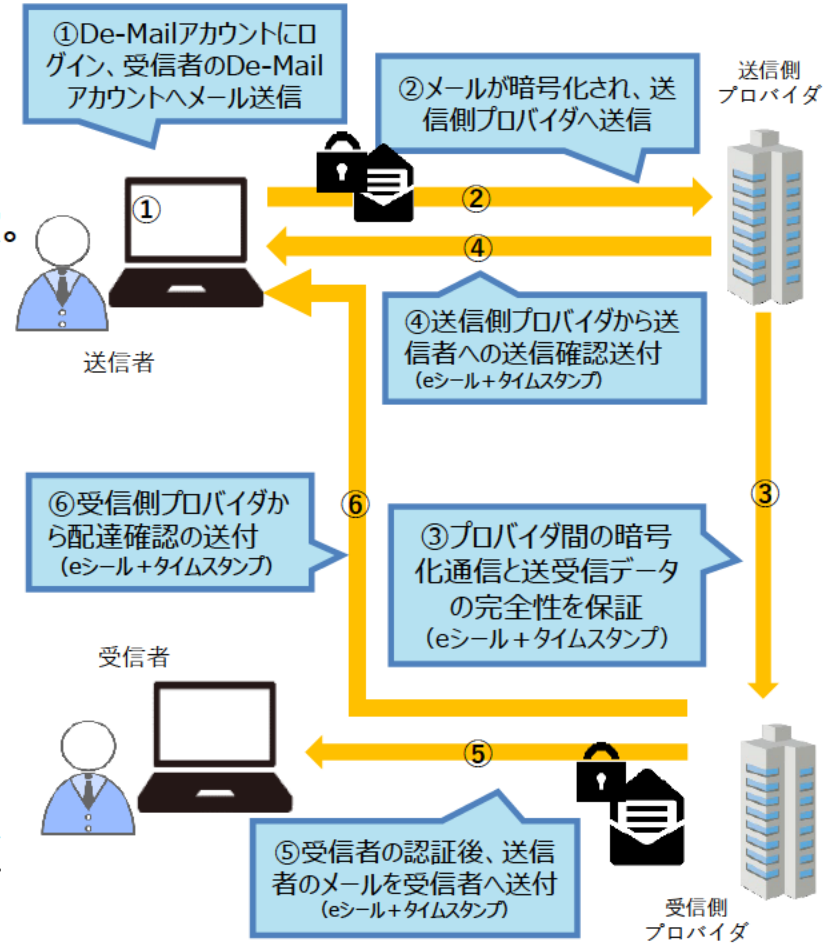
●適格eデリバリー

適格トラストサービスプロバイダー（QTSP）※による提供や、高レベルの信頼を持った送信者識別や宛先識別の保証、適格タイムスタンプの使用等が求められている。

※eIDAS規則で定められた各加盟国の適合性評価機関により認められた、１つ以上の適格トラストサービスを提供するトラストサービスプロバイダ（TSP）。TSPがQTSPの条件を満たしている場合、QTSPはEUのトラステッドリストに記載される。

どの場面でどの種類のeデリバリーが求められるかはeIDAS上に規定がないため、各国法令の整理に委ねられていると考えられるが、<u>法的効力及び法的手続における証拠としての許容性についてはいずれのeデリバリーにも認められる。</u>

eデリバリーの例（ドイツ De-Mailの仕組み）



欧州におけるeデリバリーの活用例

PEC（イタリア）

- 証明電子メール（Posta Elettronica Certificata）がデジタル行政法典で制度化されており、**証明電子メールによって行われる文書の電子送信は、郵送による通知と同等と規定されている。**
- 弁護士等の一定の専門家や公的な団体については、「デジタル住所」（特定の行為のために指定する特別なメールアドレス）の**登録が義務づけられている。**
  「デジタル住所」に対して行われた通信は、発送及び受領の時刻に関して、配達証明付き書留郵便と同等の法的効果を持つ。
- 認証電子メール事業者は受領証・配達証明証を発行し、認証電子メールの送信・受信の有効性の証明を可能にしている。

LRE（フランス）

- 登録電子郵便（La lettre recommandée électronique）が郵便・電子通信法典で制度化されており、eIDAS規則の適格eデリバリープロバイダによるサービスがLREとして定義されている。
  登録電子郵便は書留による送付と同等と規定されている。
- **受信者が送信者に対して、LREの受信に同意している旨を表明している場合にのみ利用できる。**
  （ただし弁護士等の専門家が受信者となる場合は、同意の表明が必須ではない）
- フランスの国内法において、
  ・従業員に対する懲戒処分の通知
  ・住居用賃貸契約の解除
  ・商業用賃貸契約の更新要求
  等でのLREの利用が法定されており、その他任意のユースケースについてもガイドラインで推奨されている。

→「送信先への到達」を確保するための制度的措置が用意されている。

①　電気通信事業者におけるサイバーセキュリティ対策の推進

①－１ 国内外の動向

①－２ 電気通信事業者によるサイバー攻撃対策

①－３ 電気通信事業法改正案

①－４ 5Gネットワークにおけるセキュリティの確保

②　IoTセキュリティの確保

②－１ NOTICEの現状/NICTERの現状、http(s)への拡大

②－２ 機器メーカとの関係

③　その他の取組

③－１ トラストサービス

③－２ クラウドサービスのサイバーセキュリティ確保

③－３ スマートシティのサイバーセキュリティ確保

③－４ 放送設備のサイバーセキュリティ確保

クラウドサービスのセキュリティ確保

- 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、クラウドサービス提供者を対象として、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）。
- 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、事業者への普及促進を図っている。

ガイドラインの構成

- **Ⅰ．序編**
- **Ⅱ．共通編**
  - 管理策＋サプライチェーン
  - ベストプラクティス
  - 評価項目(SLA)
- **Ⅲ．SaaS編**
  - 管理策＋サプライチェーン
  - ベストプラクティス
  - 評価項目(SLA)
- **Ⅳ．PaaS/IaaS編**
  - 管理策＋サプライチェーン
  - ベストプラクティス
  - 評価項目(SLA)
- **Ⅴ．IoTサービスリスクへの対応方針編**

第3版改定のポイント

○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

○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

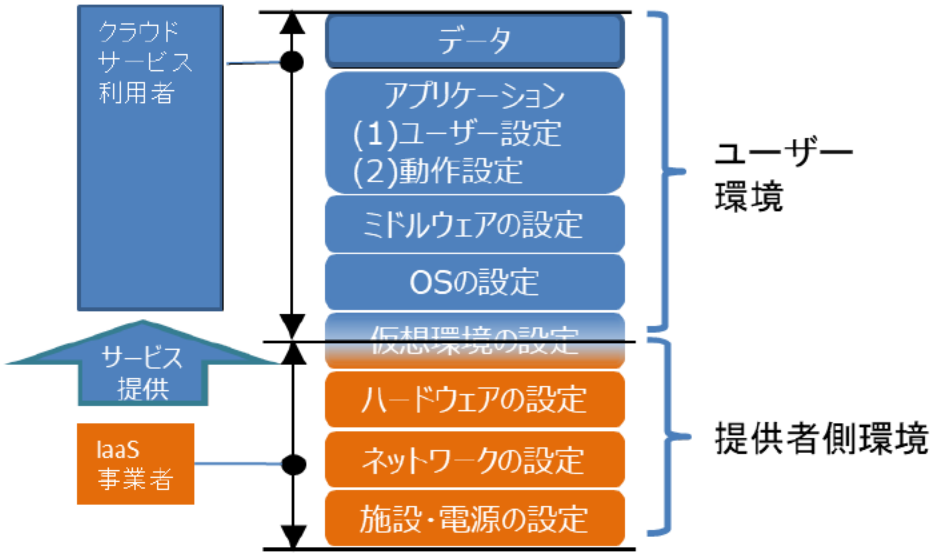
○国際規格（ISO/IEC27017:2016）やNIST SP800-53 rev.5において記載されているセキュリティ対策と整合性をとる形で、当ガイドラインに記載されているセキュリティ対策の内容を見直し

※その他、改定に伴い、読み手における読みやすさの観点で全体の構成を見直し

クラウドサービス利用・提供における適切な設定の促進

- 近年、クラウドサービスの利活用が急激に拡大する中で、クラウドサービス利用者がクラウドサービスを利用する際の設定ミスに起因する事故や、他事業者のクラウドサービスを調達・利用するクラウドサービス提供者における設定ミスに起因する情報漏えいや障害といった事故が多発している。
- このため、総務省において、有識者及び事業者を交えて、過去の情報漏えい等の事故の原因や、クラウドサービス利用者及び提供者において実施されている設定ミスを防止するための取組について調査・分析を行った上で、クラウドサービス利用者及び提供者において実施することが望ましい取組を整理・検討しているところ。
- 検討結果については、「クラウドサービス利用・提供における適切な設定のためのガイドライン（仮称）」として、広く意見募集を行った上で、2022年中に策定・公表する予定。

（例）IaaSの設定に関する責任共有モデル



（利用者に求められる取組例）

- クラウド利用における社内ガバナンスの確保
- セキュリティに係る設定項目の確認
- 支援ツールや外部診断サービス等の活用
- 設定に関する定期的なチェックや内部監査

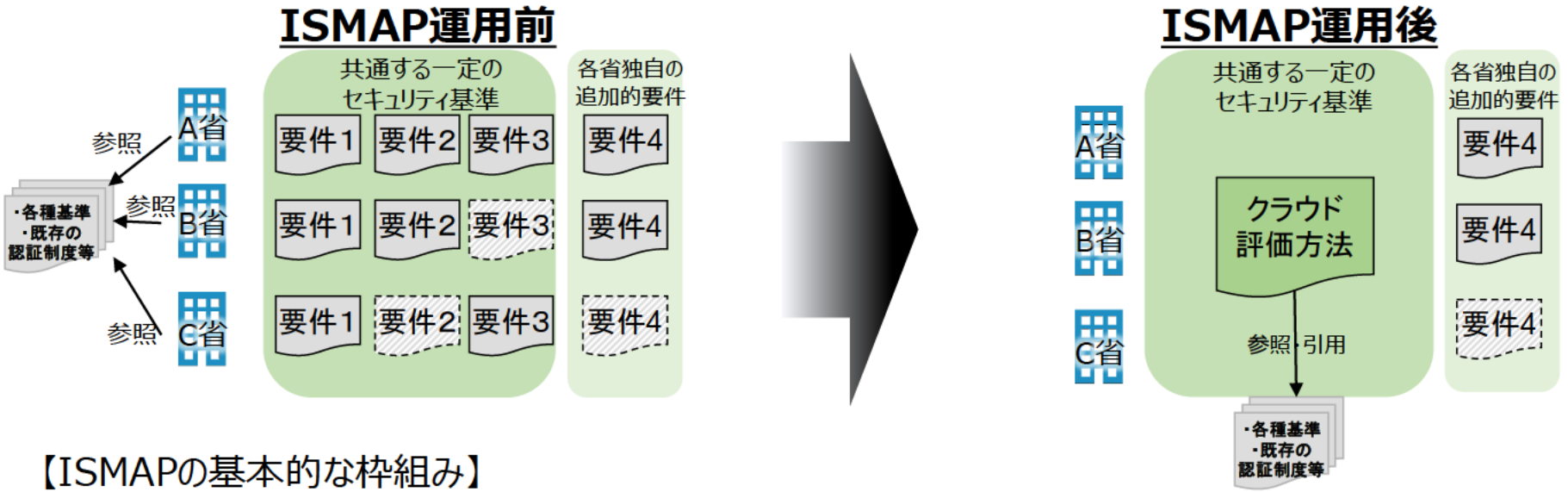
（提供者に求められる取組例）

- 正しく、十分で、わかりやすく、タイムリーな情報の提供
- 体系的な学習コンテンツの提供
- 設定項目管理ツールの提供
- デフォルト値の見直し

政府情報システムのためのセキュリティ評価制度（ISMAP）

➢ クラウドサービスの導入に係る様々な方針やガイドライン等が存在するが、同じクラウドサービスに対して各政府機関等が独自に、全てのセキュリティ要件を最初から確認することとなり、非効率。

⇒クラウドサービスについて、統一的なセキュリティ基準を明確化し、実効性・効率性のあるクラウドのセキュリティ評価制度である**「政府情報システムのためのセキュリティ評価制度」**（**ISMAP**：Information system Security Management and Assessment Program）を運用。



【ISMAPの基本的な枠組み】

- **国際標準等を踏まえて策定した基準に基づき、各基準が適切に実施されているか監査**するプロセスを経て、サービスを登録する制度（2020年6月に立ち上げ、2021年3月にクラウドサービスの登録・リストの公開が開始）として、制度所管４省庁（NISC・デジタル庁・総務省・経済産業省）が運用（IPAが支援）
- 各政府機関は、原則、安全性が評価され「登録簿」に掲載されたサービス（**35サービス（2022年３月末現在）**）から調達。2022年４月からは、独立行政法人及び指定法人による調達に対象を拡大。
- また、**セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組み**を2022年中に策定する予定。

①　電気通信事業者におけるサイバーセキュリティ対策の推進

①－１ 国内外の動向

①－２ 電気通信事業者によるサイバー攻撃対策

①－３ 電気通信事業法改正案

①－４ 5Gネットワークにおけるセキュリティの確保

②　IoTセキュリティの確保

②－１ NOTICEの現状/NICTERの現状、http(s)への拡大

②－２ 機器メーカとの関係

③　その他の取組

③－１ トラストサービス

③－２ クラウドサービスのサイバーセキュリティ確保

③－３ スマートシティのサイバーセキュリティ確保

③－４ 放送設備のサイバーセキュリティ確保

スマートシティのセキュリティ確保

- 総務省では、スマートシティのセキュリティ確保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記載した「スマートシティセキュリティガイドライン」を策定（令和２年10月に第1.0版を公表、令和３年６月に改定した第2.0版を公表）。ガイドラインを読みやすくした「スマートシティセキュリティガイドブック」も公表。
- ガイドラインでは、「スマートシティリファレンスアーキテクチャ」に基づき、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。
- 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。
- 政府のスマートシティ関連事業（現在公募中）では、ガイドラインに基づいて作成した「スマートシティセキュリティ導入チェックシート」を応募書類の一部として位置付け、セキュリティ対策の積極的な実施を促進。

○スマートシティセキュリティの４カテゴリ

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

○スマートシティ特有のセキュリティ対策

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

①　電気通信事業者におけるサイバーセキュリティ対策の推進

①－１ 国内外の動向

①－２ 電気通信事業者によるサイバー攻撃対策

①－３ 電気通信事業法改正案

①－４ 5Gネットワークにおけるセキュリティの確保

②　IoTセキュリティの確保

②－１ NOTICEの現状/NICTERの現状、http(s)への拡大

②－２ 機器メーカとの関係

③　その他の取組

③－１ トラストサービス

③－２ クラウドサービスのサイバーセキュリティ確保

③－３ スマートシティのサイバーセキュリティ確保

③－４ 放送設備のサイバーセキュリティ確保

放送設備のサイバーセキュリティ確保

- 総務省において、令和2年3月に放送設備のサイバーセキュリティ確保に関する省令改正等を実施。
- これまでに、国内ではサイバー攻撃に起因する放送停止事故は発生していないが、放送設備のIP化・クラウド化や海外の事例も踏まえ、更なるサイバーセキュリティ対策が重要。

- 放送法第121条等において、放送設備の技術基準への適合を義務付け。
- 技術基準は、その発生を未然に防止するための措置及び発生した際の復旧を目指した措置として、設備故障、自然災害、停電その他の措置事項を省令（放送法施行規則）で規定。
- 令和2年3月に、放送法施行規則にサイバーセキュリティの確保の規定を追加。

・予備機器等
・故障検出
・試験機器及び応急復旧機材の配備
・機能確認
・誘導対策（アンテナからの電磁誘導影響への対策）
・耐震対策
・耐雷対策
・防火対策
・屋外設備
・収容する建築物
・停電対策
・宇宙線対策
・サイバーセキュリティの確保【追加】

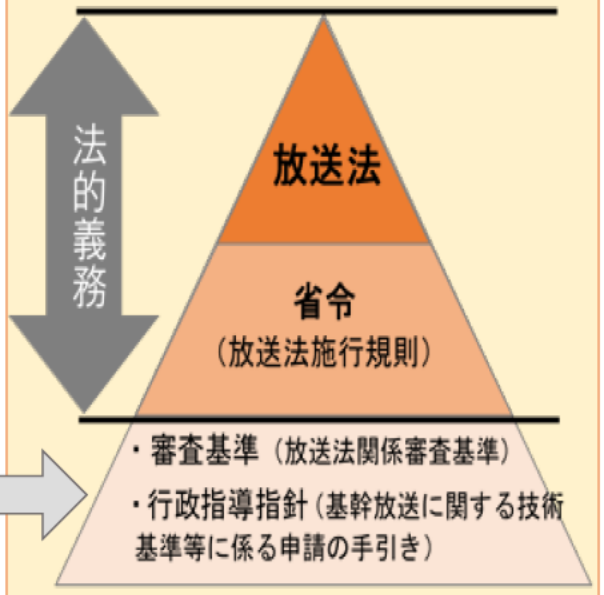
【放送法施行規則】

（サイバーセキュリティの確保）

第百十五条の二　放送設備及び当該放送設備を維持又は運用するために必要な設備は、当該放送設備によつて行われる放送の業務に著しい支障を及ぼすおそれがないよう、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。以下同じ。）の確保のために必要な措置が講じられていなければならない。

【サイバーセキュリティの確保に関する具体的措置事項（放送法関係審査基準）】

1　放送本線系入力となる番組送出設備について、外部ネットワークからの隔離
2　監視・制御及び保守回線について、外部ネットワークからの不正接続対策
3　設備の導入時及び運用・保守時においては、放送設備のネットワークからの分離・遮断の措置及び不正プログラムの感染防止の措置
4　放送設備に対する物理的なアクセス管理
5　サイバーセキュリティ対策に関する組織体制の構築及び業務の実施に係る規程類の整備



論点

電気通信事業者におけるサイバーセキュリティ対策

○ サプライチェーンリスク対応を含めたサイバーセキュリティの重要性の高まりや、今後サイバーセキュリティ戦略本部において重要インフラのサイバーセキュリティに係る行動計画が改定されること等を踏まえ、総務省としてどのような取組が必要か。

○ サイバー攻撃が巧妙化・複雑化する中で、電気通信事業者が通信の秘密等に配慮しつつ、新たな対策や取組を講じていくためには、どのような環境整備が必要か。

○ 海外における政策やサイバー攻撃の動向から留意すべきことはあるか。

IoTのセキュリティ

○ 最近のサイバー攻撃の動向や「サイバーセキュリティ戦略」に盛り込まれた積極的サイバー防御の議論を踏まえて、既存の事業者・利用者による対策に加えて、例えば以下の点も含めて、今後どのような更なる対策を講ずる必要があると考えられるか。

- ２年後に実施期限を迎えるNOTICEの在り方を含むIoT機器などの脆弱性調査・注意喚起等の対応
- 明らかに脆弱性があるメーカー保証期間を終えた機器や中古機器を使用しない（使用中止させる）方法

その他の取組

○ クラウドサービス等のセキュリティ確保に向けて、今後どのような取組が必要か。