「巧妙化・複雑化するサイバー攻撃への対策の在り方に関する検討会」
中間論点整理

令和８年７月
事　　務　　局

１．検討の背景等

1． 検討の背景等

情報通信ネットワークとサイバーセキュリティの確保

- 情報通信ネットワークは、国民生活や経済社会に不可欠な重要インフラであると同時に、サイバー攻撃が飛び交うサイバー空間のインフラそのものである。
- サイバー空間のインフラを担う電気通信事業者は、サイバーセキュリティの確保のために果たすべき役割は大きい。

サイバー脅威の現状・課題

- ランサムウェア攻撃の被害や、家庭用IoT機器を悪用した攻撃の被害が顕在化するなど、サイバー攻撃の巧妙化と複雑化が進展。サイバー攻撃関連通信数は年々増加。
- 脅威の質と量の両面での深刻化が、重要インフラ事業者をはじめとする情報通信ネットワークの利用者に大きな影響を及ぼしている。
- こうした脅威に対し、一層実効的な対策を講じていくことが安全・安心なサイバー空間の実現に当たって重要な課題となっている。

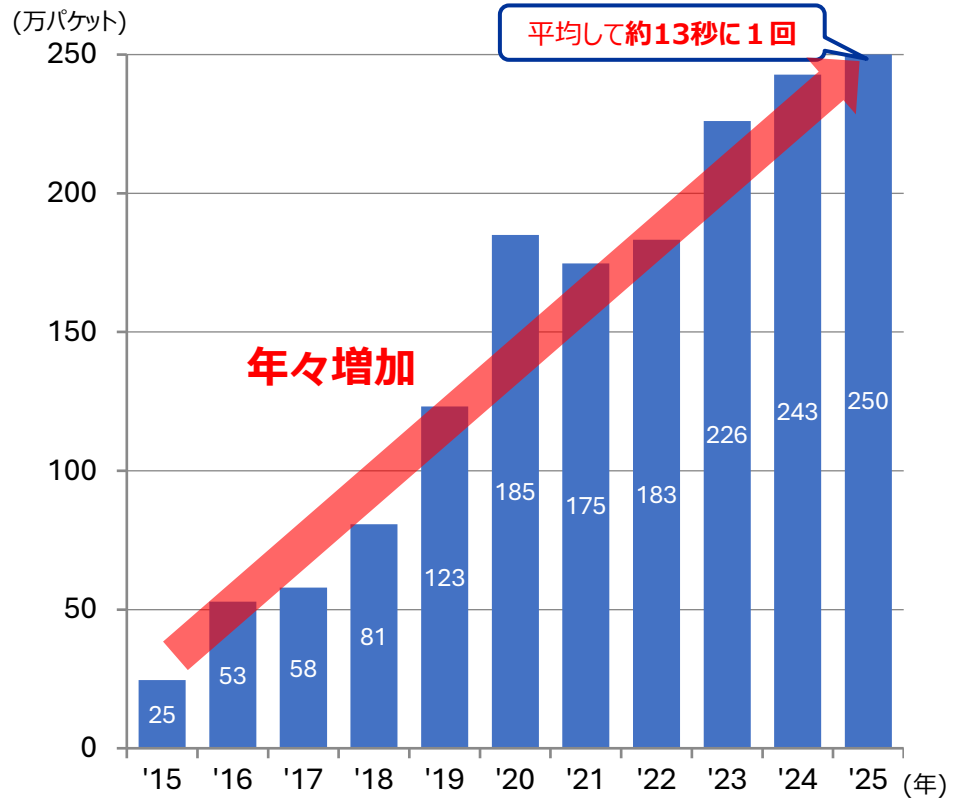
電気通信事業者をはじめとした関係主体が、サイバーセキュリティの確保のために講じる対策の在り方について検討することが必要である。

1．検討の背景等（サイバー脅威の現状）

- サイバー攻撃は巧妙化・高度化するとともに、サイバー攻撃関連通信数は増加傾向にあり、**質・量両面でサイバー攻撃の脅威は深刻化**
- 令和７年中に観測された**サイバー攻撃関連の通信の99%以上※が海外から発信**
  ※警察庁資料。令和７年中に警察庁が観測したサイバー攻撃関連の通信（ダークネット向けの攻撃通信を含むパケット）の99.4%が海外のIPアドレスを発信元とするもの
- 近年、従来は人手による発見が困難であった**脆弱性を、短時間で大量に検出し得るAIが登場**

サイバー攻撃関連通信の量

NICTが観測したサイバー攻撃関連通信数の推移
（1つのIPアドレスで１年間に観測されるパケット数）



出典：国立研究開発法人情報通信研究機構「NICTER観測レポート2025」等に基づき事務局にて作成

サイバー攻撃の巧妙化・深刻化

システムの侵害
（暗号化・システム障害、身代金要求）
（例：令和３年 米コロニアルパイプライン、令和４年 大阪急性期・総合医療センター、令和５年 名古屋港、令和７年 大手飲料メーカー等の業務停止）

有事に備えた重要インフラ等への侵入
（高度な侵入・潜伏能力）
（例：令和３年 ウクライナ侵略、令和５年 VoltTyphoonによるグアム等にある米軍施設や政府機関、重要インフラへの侵害、令和６年 SaltTyphoonによる各国の政府機関や通信事業者の情報システム・ネットワークへの侵入）

機微情報の窃取
（アクセス権限の獲得）
（例：令和３～７年 JAXAからの情報窃取、令和５年 NISCのメール窃取）

新たなサイバー脅威の登場

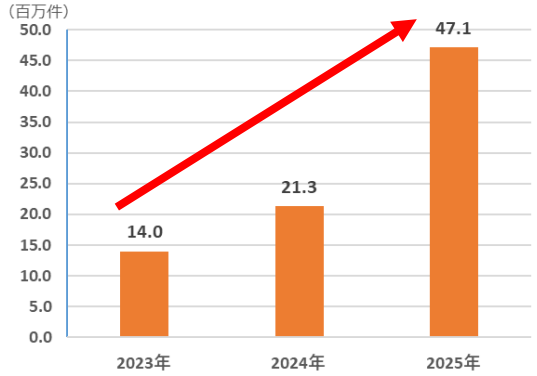
令和８年４月７日、アンソロピック社が高度な脆弱性発見能力を持つ、Claude Mythos Previewを発表。Mythosは数週間で、数十年間未発見だったものを含む脆弱性を数千件発見。

出典：Anthropic社"Project Glasswing"

1．検討の背景等（サイバー攻撃の被害状況）

DDoS攻撃の被害状況

発生件数



- 大手クラウド事業者の調査によると、2025年のDDoS攻撃の件数は、2023年から約236%増加。
- 同調査によると、最大31.4Tbpsの攻撃も観測。

出典：Cloudflare「2025年第4四半期DDoS脅威レポート」に基づき事務局にて作成

日本国内における近年のDDoS攻撃の事例

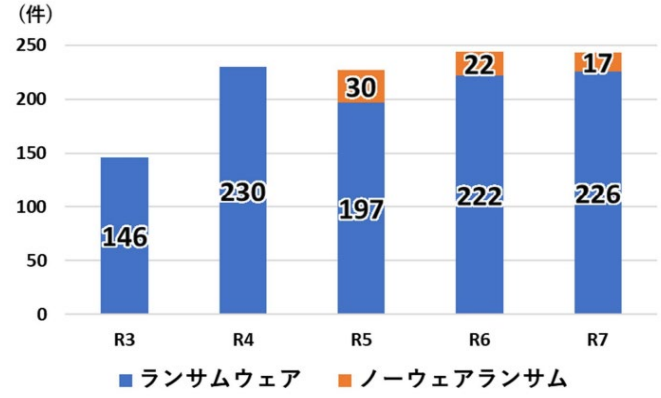
（令和6年12月～令和7年1月）

被害企業・組織	被害概要
航空事業者	社内外をつなぐシステムに障害が発生し、航空便の遅延や航空券の販売停止等に波及。
金融機関	複数の銀行・カード事業者で、ネットバンキングや会員向けサービスのログイン障害等が発生。
通信事業者	一部サービスにおいてウェブサイトにアクセスしづらい事象が発生。
天気予報メディア	天気予報サイト・アプリが利用しづらい事象が発生。

出典：報道資料等に基づき事務局にて作成

ランサムウェアの被害状況

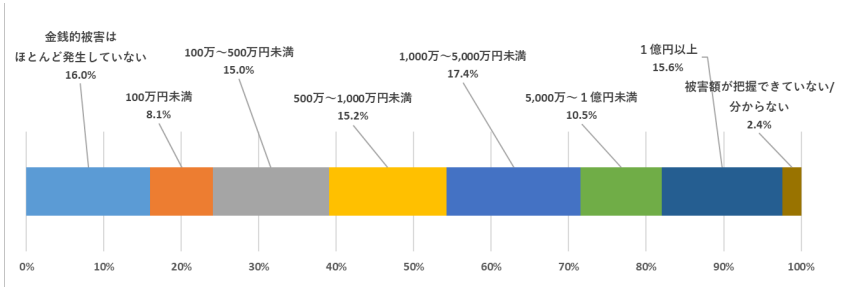
被害報告件数の推移



※ノーウェアランサム（令和5年上半期から集計）：暗号化を行わずに情報を窃取。情報を暴露すると恐喝し、身代金を要求するもの。

- ランサムウェアの被害報告件数は、増加傾向にあり、年間約200件以上に高止まり。（左のグラフ）
  出典：警察庁「令和７年におけるサイバー空間をめぐる脅威の情勢等について」
- また、過去、ランサムウェアへの感染を経験した企業は45.8%に上る。
  出典：JIPDEC「企業IT利活用動向調査2026」

被害額



- ランサムウェアの被害額※は、100～5000万円の範囲で半数近くとなっている。１億円以上の被害も約15%存在。

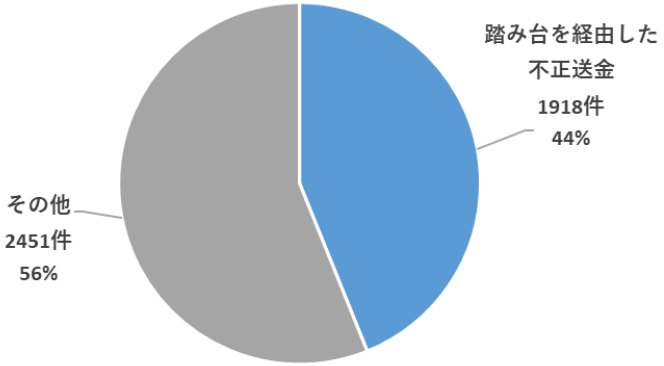
※「被害額」には、事故調査、被害範囲調査、身代金支払い額、データやシステムの復旧・再構築、再発防止のためのセキュリティ対策費用を含む。

出典：JIPDEC「企業IT利活用動向調査2026」に基づき事務局にて作成

1．検討の背景等（IoT機器に係る新たな脅威）

家庭用IoT機器を悪用したサイバー攻撃

IoT機器を踏み台とした攻撃



- 昨今、家庭用IoT機器を悪用したサイバー攻撃による被害が確認。これらは、**無料で国内外のテレビ番組が視聴できると謳う「動画ストリーミングデバイス」等**の様々な形で存在。利用者が気付くことなく、サイバー攻撃に悪用。
- 攻撃者グループは、当該機器を経由し**通信元を一般家庭と偽る**ことで、サイバー攻撃の検知を困難なものとしている。
- また、こうした機器は**家庭等のLAN内に潜伏**することで、**NOTICEプロジェクトによる検知が困難**なものとなっている。

出典：警察庁「令和７年におけるサイバー空間をめぐる脅威の情勢等について」

サイバー攻撃に悪用される家庭用IoT機器

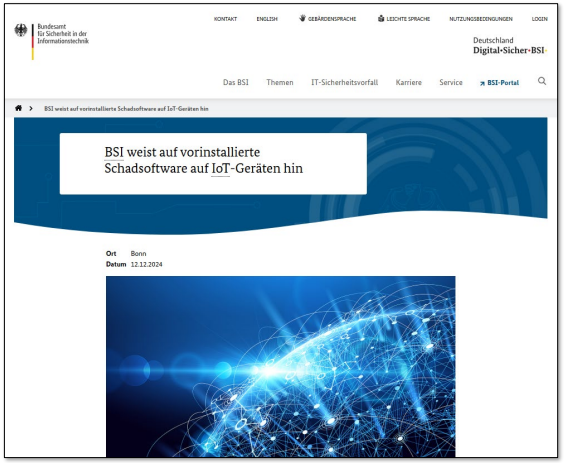
- 国内に数万台規模で存在と推定

動画ストリーミングデバイスのイメージ（生成AIで作成）

- ネットバンキング不正送金事案の被害額が令和６年中で約30億円との試算（※）のほか、証券会社不正アクセス等での悪用も報告

（※）出典：警察庁「令和７年におけるサイバー空間をめぐる脅威の情勢等について」

海外における官民での対処事例



独ドイツ連邦情報保安局（BSI）は、インターネットサービスプロバイダに対し、「Badbox」マルウェアに感染したデバイスを所有するユーザへの通知を要請

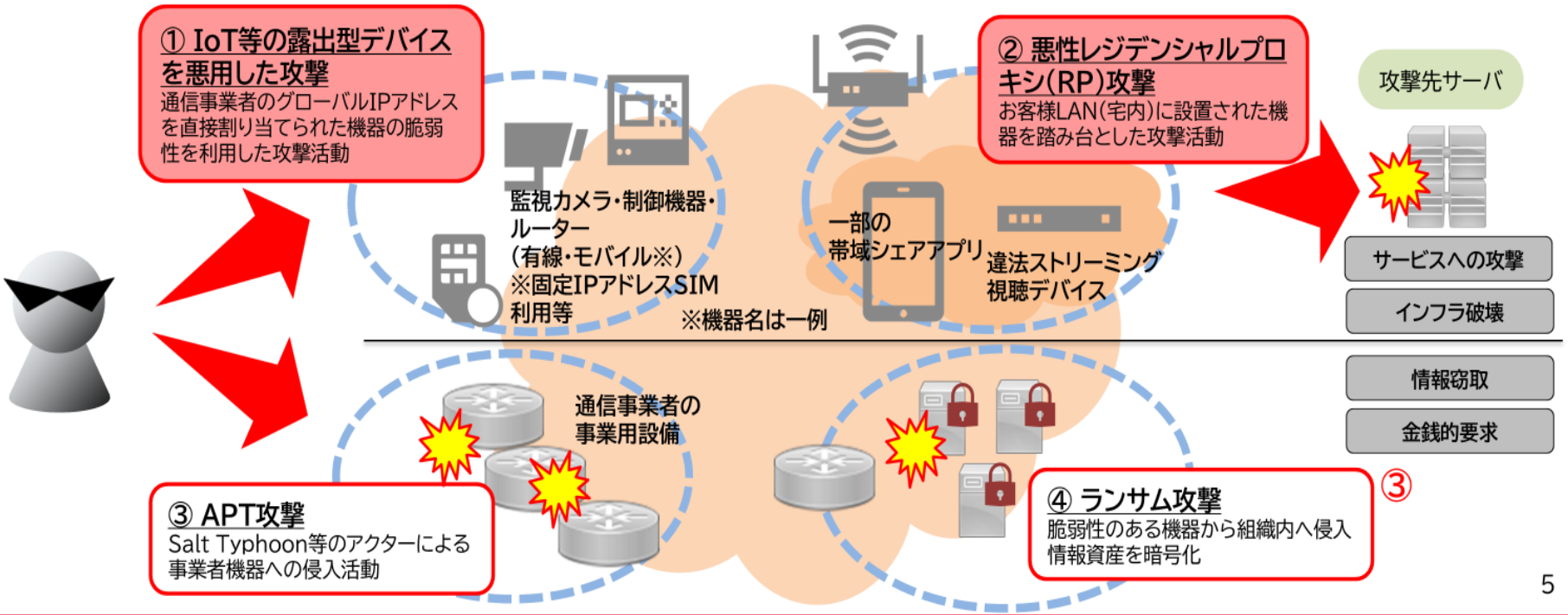
出典：BSIウェブサイト（令和６年12月12日）

米Googleは、一般人のスマートフォンやテレビ受信機を「踏み台」にしたサイバー攻撃に使われる世界最大規模のネットワークを無効化したと発表

出典：日本経済新聞（令和８年１月30日）

3. 通信分野を取り巻く最近の脅威動向

- IoT機器等を踏み台にした第三者への攻撃
  - ① IoT等の露出型デバイスを悪用した攻撃　IoT機器等の既知脆弱性や設定不備をを利用した攻撃（NOTICEで対策実施）
  - ② 悪性レジデンシャルプロキシ(RP)攻撃　宅内に設置した機器(違法ストリーミングデバイス・一部の帯域シェアアプリ)を利用した攻撃
- 通信先の組織自体を狙う攻撃
  - ③ APT攻撃(国家アクター等による攻撃)　特定組織に長期間潜伏、事業者に気づかれないまま内部情報・通信情報を窃取
  - ④ 情報資産を交渉材料にしたランサム攻撃　脆弱なVPN機器・リモートアクセス可能なホストから組織侵入、情報資産を暗号化し身代金交渉



２．検討の視座

2．検討の視座

- ２～６ページで述べたような現状や課題を踏まえ、これまでの巧妙化・複雑化するサイバー攻撃への対策の在り方に関する検討会においては、以下の観点から、電気通信事業者をはじめとした関係主体がサイバーセキュリティの確保のために講じる対策の在り方について、御議論いただいたところ。

検討の視座

① 近年のサイバー攻撃による被害等の現状を踏まえ、電気通信事業者は、サイバー空間のインフラそのものを担う立場から、サイバーセキュリティの確保においてどのような役割を果たすことができるか。

② 電気通信事業者をはじめとした関係主体が、サイバーセキュリティの確保においてどのような連携を進めることで、それぞれの強みを生かすことができるか。

③ 上記①・②も踏まえ、情報通信ネットワークの利用者は、サイバーセキュリティの確保のために、どのように取り組むことが考えられるか。

３．検討に当たっての主なポイント等

検討の視座①関連

検討の視座①

近年のサイバー攻撃による被害等の現状を踏まえ、電気通信事業者は、サイバー空間のインフラそのものを担う立場から、サイバーセキュリティの確保においてどのような役割を果たすことができるか。

【ヒアリングで述べられた主な意見】

- 電気通信事業者は、攻撃通信を観測して異常を検知して通信設備への影響を抑えることができる、利用者との接点があるといった強みがある。
- 電気通信事業者の事業用設備に対しても不正アクセス等の攻撃の試行が増加している。また、社会インフラを守る電気通信事業者として、重要なインフラ企業なども含め、利用者をしっかりと守りたい。場面に応じてできることが明確だとありがたい。
- 電気通信事業者の対応の高度化に当たっては、電気通信事業者を単にデータを運搬するものと捉えるか、社会のデジタルインフラを支えるものと捉えるかで、整理の方向が変わって来るのではないか。後者の場合、電気通信の安定的なサービスの提供から更に踏み込み、観測だけでなく予兆に踏み込んだり、自社だけでなく社会全体を守る取組ができないか、ということになるのではないか。
- 高度な対策環境を企業、産業界が作ることは難しい場合もあるため、セキュリティ機能を備えたネットワークサービスを展開している。また、セキュリティ対策ができていないIoT機器が存在し、利用者がそれに気付けていない場合も、こうしたサービスは利用者をサポートできると考えている。利用者の設備をしっかり保護していくことが重要である。
- 総務省の実証実験を通じ、自社の設備保護を目的にフロー情報分析を実施している。得られるC2サーバリストを自社設備の保護だけでなく、セキュリティ機能を備えたネットワークサービスで活用したり、連携先としてセキュリティベンダ等に提供したりすることで、利用者の保護、ひいては我が国のセキュリティ向上にも寄与できると考える。様々な対策ができれば、海外プレーヤーとの協力にも繋がる。
- AIが劇的に進化する中にあって、対策の本質は基本の徹底と対応の超高速化である。この観点からは、攻撃が届く前の対処など、いかに早くBotに対処できるかが重要であり、フロー情報分析によるC2サーバ検知の実証事業等の知見や、それを用いたネットワーク側での対処が有用ではないか。
- エンドポイント側での対策費用はエンドポイントのサービスの利用料に反映されていくように、電気通信事業者が講じる対策の費用は、当該事業者のサービスの提供に当たって考慮されていくものと考えている。

検討の視座①関連

【構成員からの主な意見】

- 電気通信事業者によるサイバーセキュリティ対策は、その実施がただのコストになるのではなく、利益も得て、人材育成、サービスの高度化につなげられるような、安心して取り組むことができるインセンティブの仕組みが重要ではないか。
- インターネットのアーキテクチャとして、電気通信事業者と利用者の責任分界点の向こう側である利用者の領域は、基本的に利用者が自分で管理するものであり、それに準じて制度設計もされているが、利用者にやってもらうしかないという点に、限界が見えつつあるのではないか。利用者と電気通信事業者の二者間の問題だけでなく、踏み台にされることで更なる被害が拡大していく可能性もある。こうした問題意識を踏まえ、引き続き検討していくべきではないか。
- 電気通信事業者の役割は、重要な社会インフラである通信サービスを止めないことが中心であるが、サイバー空間を支える立場から、サイバー空間の利用者の保護も役割の一環と捉え得るのではないか。
- 電気通信事業者による利用者の保護には制度上の制約があるところだと思う。利用者の保護について検討の俎上に載せるべきではないか。

【検討に当たっての主なポイント】

- 電気通信事業者が、サイバー空間を観測でき、利用者との接点を有するという立場を生かして、利用者のサイバーセキュリティの確保のための措置や、利用者が踏み台とされてサイバー攻撃に加担させられないようにするための措置を、安心して講じていけるようにすることが重要ではないか。
- その際、利用者側の責任範囲におけるサイバーセキュリティの確保が利用者の責任となっていることや、電気通信事業者が利用者の保護のために講じる対策の法的な位置づけも踏まえて、検討を深めていくことが考えられるのではないか。
- AIが劇的に進化する中にあって、攻撃発生前に攻撃インフラのネットワーク（C2サーバ及びBotのネットワーク）を把握し、攻撃に備えた対処を行っていくことが一層重要となるのではないか。その具体的な方策の一つとして、総務省が実証事業を行ってきた電気通信事業者によるフロー情報分析技術が位置づけられるのではないか。
- 電気通信事業者によるサイバーセキュリティ対策は、ただのコストになるのではなく、利益も得て、人材育成やサービスの高度化にも繋げられるようなインセンティブのある仕組みとして促進されることが重要ではないか。

検討の視座②関連

検討の視座②

電気通信事業者をはじめとした関係主体が、サイバーセキュリティの確保においてどのような連携を進めることで、それぞれの強みを生かすことができるか。

【ヒアリングで述べられた主な意見】

- 電気通信事業者の事業用設備に対しても不正アクセス等の攻撃の試行が増加している。社会インフラを守る電気通信事業者として、重要なインフラ企業なども含め、利用者をしっかりと守りたい。場面に応じてできることが明確だとありがたい。（再掲）
- 総務省の実証実験を通じ、自社の設備保護を目的にフロー情報分析を実施している。得られるC2サーバリストを自社設備の保護だけでなく、セキュリティ機能を備えたネットワークサービスで活用したり、連携先としてセキュリティベンダ等に提供したりすることで、利用者の保護、ひいては我が国のセキュリティ向上にも寄与できると考える。様々な対策ができれば、海外プレーヤーとの協力にも繋がる。（再掲）
- 高度化するサイバー攻撃に対応するためには、AIも活用しながら攻撃を早く正確に検知し、対応につなげることが必要。そのためにも、外部からの情報も含め、情報の質と量を上げていく必要がある。
- SOC事業者ではインターネット全体における広範な脅威動向については把握が限定的であり、通信レイヤーで観測される情報を一定程度活用できる場合、利用者に対する注意喚起や監視強化など、限定的ではあるが予防的な対応の高度化につながる可能性がある。ただし、現状では、どの範囲・粒度の情報が活用可能であり、実際の対策に寄与するかについては、費用対効果も含め、必ずしも明確ではないため、実務的な観点から、情報連携の在り方や活用の可能性について検討していくことは一定の意義がある。
- AIの劇的な進歩もある中で、エンドポイントとネットワークが素早く連携できると有用と考えられるが、制度面やビジネス面での課題がある。例えば、フロー情報から抽出された脅威情報を利用者のシステムと連携したり、エンドポイント側で得られる脅威情報をネットワーク側と連携させることが考えられる。また、こうした情報が集約できれば研究開発にも有用であり、そのためには、電気通信事業者、セキュリティベンダ、公的機関のほか、利用者側の協力も必要である。国内である程度強力なセキュリティ対策手段を持っておくことが、海外との交渉においても重要である。
- C2サーバに関する情報やフィッシングドメイン等の脅威情報の官民・業界横断での共有が有用ではないか。
- 高度化するサイバー攻撃への対応について、生じるコストの適正負担も考慮の上で、官民・民民の連携を更に進めることが必要。

検討の視座②関連

【ヒアリングで述べられた主な意見】（承前）

- 家庭内に設置された一部のストリーミングデバイスや帯域シェアアプリを利用したレジデンシャルプロキシ攻撃は、海外からのアクセスを国内IPアドレスで中継するため、被害側では正常通信と見分けることが困難である。また、LAN内にあるため、NOTICEの取組での検知も困難である。利用者自身は悪性通信を中継しているとは認識していないことが通常である。対策には、官民の様々な主体による協力・協働が不可欠である。具体的には、利用者の行動変容を促す社会的な啓発や効果的な警告を行う、流通経路の対策を講じる、C2サーバとレジデンシャルプロキシ間の通信をフィルタリングすることの効果を検証するといったことが考えられる。
- IoT機器の製造はサプライチェーンが多層的であり、その過程で、脆弱性の対応ができない又は追い付かないところが狙われると踏み台化する。対策としては、更新提供されない製品への対応や、感染端末の検知・利用者への通知などが考えられる。

【構成員からの主な意見】

- IoT機器のセキュリティ対策について、利用者に対しては、キャンペーンや診断ツールの認知拡大等により、自身がサイバー攻撃の加害者になり得るということも含め、意識を高め、行動変容を促していくことが重要ではないか。また、機器に関わる対策や流通に係る対応など、様々な関係主体によるトータルな対策が必要ではないか。電気通信事業者は、利用者との接点を有する立場から果たせる役割があるのではないか。
- ネットワークの観測により得られる情報は、技術の観点で言えば、共有して色々な対策へ活用した方が良い。また、AIを対策に活用することで、攻撃通信や脆弱性、公開情報の分析の自動化・効率化が可能になっている。
- ヒアリングにおいてネットワークからの脅威情報とエンドポイントから得られる脅威情報を収集・集約できれば有用との説明があったとおり、ネットワークで取得・収集可能な脅威情報が、適正かつトラストある形で共有されることは、具体的な対策として重要である。ここでいう適正とは関連法規の法解釈として矛盾なく成立すること、またトラストある形とは実際の運用に一定の制約を課すこと（例えば共有できる対象の特定とその理由、また廃棄やデータ加工を含めたデータ管理方法の規範の確立、対処の結果に関する透明性の一定程度の確保等）を意味する。こうした観点から検討を更に深めていただきたい。
- 利用者が安全なネットワーク環境を求めることは自然な期待であり、そのために電気通信事業者が果たせる役割は大きい。制度やガイドラインを含め、電気通信事業者が安心してサイバー防御や脅威情報の共有に取り組める環境を整備していくことが重要ではないか。ネットワーク側が講じる対処の責任に関して、利用者において事前に、誤ってフィルタリングされる等のリスクの一部を引き受ける旨の意思表示や、対処の優先度の設定を行わなければ、迅速な対処は難しいのではないか。費用負担に関して、善意に支えられた仕組みは規模が大きくなるほど続かないのではないか。

検討の視座②関連

【検討に当たっての主なポイント】

- 利用者のサイバーセキュリティの確保を含むネットワークの安全性確保のため、また、利用者が踏み台とされてサイバー攻撃に加担させられないようにするため、電気通信事業者、セキュリティベンダ、公的機関、研究機関等の官民の関係者間で、それぞれの強みを生かして脅威情報の共有その他の連携を深めていくことが重要であり、そのための具体的方策を検討していくことが考えられるのではないか。
- 一部の電気通信事業者は、サイバー空間を観測できるという立場を生かし、総務省の実証事業により、フロー情報分析によってC2サーバを特定する取組を実施している。このようなネットワークで観測・生成される脅威情報が、利用者のサイバーセキュリティの確保のためにも、サイバー攻撃対策に取り組む様々な関係者間で共有されていくことが具体的方策の一つとして重要なのではないか。そのためには、関係者が安心して取り組むための制度的な対応や、運用に当たっての適切な規律が求められるのではないか。規律としては、例えば、共有できる情報や共有先の範囲、共有する情報の適切な取扱い、共有に係る透明性の担保措置などが考えられるのではないか。
- 連携を促進するに当たっては、各関係者の取組が、ただのコストになるのではなく、インセンティブをもって進められるようにする観点も重要ではないか。
- レジデンシャルプロキシと呼ばれる家庭用IoT機器が巧妙な手段によって利用者に導入され、サイバー攻撃の踏み台とされているという喫緊の問題への対応については、電気通信事業者をはじめとする関係主体が連携し、実施可能な措置を速やかに講じていくことが必要ではないか。

検討の視座③関連

検討の視座③

検討の視座①・②も踏まえ、情報通信ネットワークの利用者は、サイバーセキュリティの確保のために、どのように取り組むことが考えられるか。

【ヒアリングで述べられた主な意見】

- 高度な対策環境を企業、産業界が作ることは難しい場合もあるため、セキュリティ機能を備えたネットワークサービスを展開している。また、セキュリティ対策ができていないIoT機器が存在し、利用者がそれに気付けていない場合も、こうしたサービスは利用者をサポートできると考えている。利用者の設備をしっかり保護していくことが重要である。（再掲）
- 脆弱なIoT機器は、踏み台になって利用者自身が被害を受けるかもしれず、電気通信事業者も何かしらの悪影響を受けるかもしれないが、利用者に「脆弱なIoT機器がありますよ」とお知らせしても、なかなか対応していただけないところがあり、どうすれば良いのか非常に難しい。
- 踏み台化する脆弱なIoT機器の観測・注意喚起を継続し、攻撃インフラそのものの母数を削減することは重要。

【構成員からの主な意見】

- IoT機器のセキュリティ対策について、利用者に対しては、キャンペーンや診断ツールの認知拡大等により、自身がサイバー攻撃の加害者になり得るということも含め、意識を高め、行動変容を促していくことが重要ではないか。また、機器に関わる対策や流通に係る対応など、様々な関係主体によるトータルな対策が必要ではないか。電気通信事業者は、利用者との接点を有する立場から果たせる役割があるのではないか。（再掲）
- 利用者が知らないうちにサイバー攻撃の加害者になってしまうことを防ぐためにも、セキュリティに関する知識が不足している利用者も守ってもらえるようなシステムを構築してほしい。また、利用者が知らないうちにサイバー攻撃に悪用され得る機器を購入・利用してしまうこともあり得るので、利用者がわかるように周知広報してほしい。
- レジデンシャルプロキシ等の広がりは、「国内のIPアドレスからの通信は受信を拒否しづらい」という点を逆手に取っていると思われる。こうした攻撃の巧妙化も踏まえ、利用者自身による重層的なセキュリティ対策も必要ではないか。

検討の視座③関連

【検討に当たっての主なポイント】

- 通信サービスの利用者自身においても、巧妙化するサイバー攻撃の実態も踏まえ、サイバー攻撃対策に取り組む官民の関係者とも連携しながら、リスクの度合いに応じて重層的なセキュリティ対策を講じる等、サイバー攻撃から自身を保護するための措置を講じることが重要ではないか。
- サイバー攻撃から自身を保護するためだけではなく、自身がサイバー攻撃に加担しないようにするため、利用者が脆弱性を有する等の悪性のIoT機器を導入しないようにすることが求められるのではないか。
- 電気通信事業者や、電気通信事業者と連携する関係者によって、多様なセキュリティサービスが提供され、利用者がニーズに応じてそれらのサービスを選択できるようになることは、利用者にとって有用ではないか。
- レジデンシャルプロキシへの対応については、電気通信事業者等の関係主体が連携し、実施可能な措置を速やかに講じていくことが必要ではないか。その際、利用者の行動変容を促すような効果的な注意喚起・啓発の観点も重要となるのではないか。

（参考）本検討会の概要

構成員及びオブザーバ（敬称略）

上沼 紫野	LM虎ノ門南法律事務所 弁護士	【オブザーバ】
木村 たま代	主婦連合会 常任幹事	一般社団法人ICT-ISAC
クロサカ タツヤ	株式会社企 代表取締役	一般社団法人テレコムサービス協会
宍戸 常寿	東京大学大学院法学政治学研究科 教授（座長代理）	一般社団法人電気通信事業者協会
鎮目 征樹	学習院大学法学部 教授（座長）	一般社団法人日本インターネットプロバイダー協会
篠田 佳奈	株式会社 BLUE 代表取締役	一般社団法人日本ケーブルテレビ連盟
蔦 大輔	森・濱田松本法律事務所外国法共同事業 パートナー弁護士	内閣官房国家サイバー統括室
中尾 康二	一般社団法人ICT-ISAC 顧問、 国立研究開発法人情報通信研究機構（NICT）サイバーセキュリティ研究所 主管研究員	
吉岡 克成	横浜国立大学大学院環境情報研究院／先端科学高等研究院 教授	

主な検討事項

（１）巧妙化・複雑化するサイバー攻撃への実効的な対策について
（２）サイバー攻撃対策における関係主体の連携について
（３）その他

これまでの検討状況

回　次	議　事　内　容
第１回 （R8.5.29）	✓ 開催要綱（案）について（事務局） ✓ 「巧妙化・複雑化するサイバー攻撃への対策の在り方に関する検討会」について（事務局） ✓ IoT機器調査及び利用者への注意喚起について（事務局） ✓ サイバー攻撃の最新動向と観測・分析・対策技術研究の現状（吉岡構成員） ✓ 自由討議
第２回 （R8.6.12）	✓ ヒアリング及び質疑応答（NTT、NTTドコモビジネス、KDDI、ラック、ソフトバンク） ✓ 自由討議
第３回 （R8.7.3）	✓ ヒアリング及び質疑応答（FFRIセキュリティ、SBIホールディングス、ICT-ISAC、デジタルライフ推進協会） ✓ 自由討議
第４回 （R8.7.17）	✓ 中間論点整理（案）について（事務局） ✓ 「家庭用IoT機器を悪用するレジデンシャルプロキシの対策について（提言）」（案）について（事務局）