IoTの安心・安全かつ適正な利用環境の構築

補足説明資料

令和7年6月
サイバーセキュリティ統括官室

IoTサービスの普及とサイバー攻撃の現状

- IoT※1サービスの普及に伴い、**IoT機器を悪用にした世界規模のサイバー攻撃（DDoS攻撃※2）**が発生。
- 国内でもマルウェア※3感染機器は恒常的に観測されており、セキュリティ対策の強化が引き続き重要。

※1　IoT　：「**I**nternet **o**f **T**hings」の略。
インターネットに接続して使用するモノを「**IoT機器**」と呼ぶ。

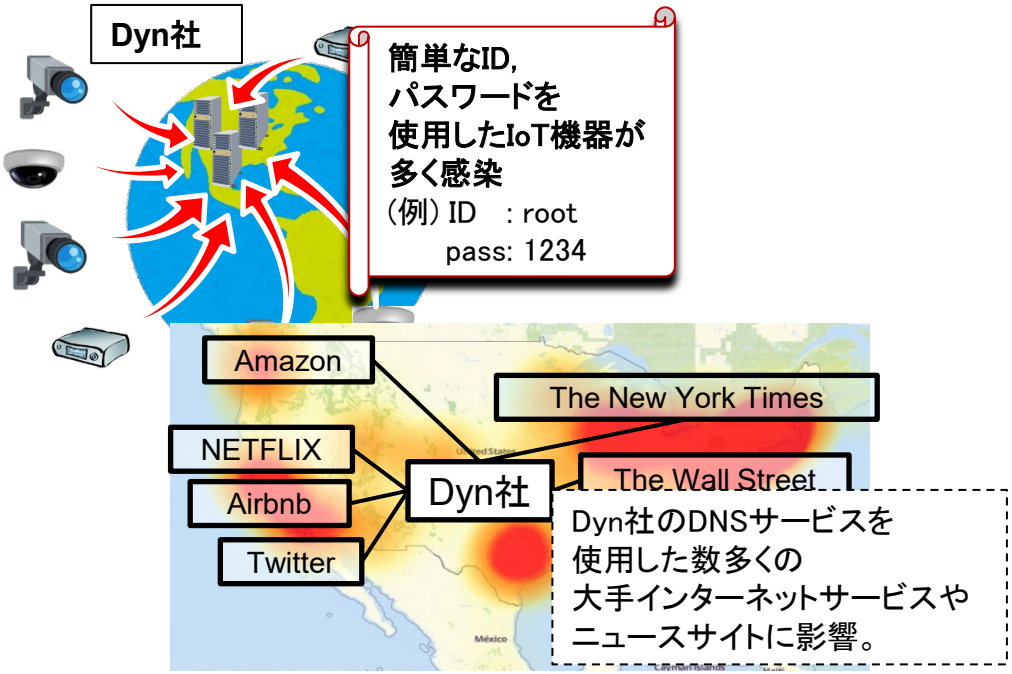
※2　DDoS攻撃：「**D**istributed **D**enial **o**f **S**ervice attack」の略。
多数の機器から一斉に攻撃通信を送る攻撃。

※3　マルウェア　：「**Mal**icious Soft**ware**」の略で、「悪意のあるソフトウェア」。
パソコンやIoT機器等に対し、遠隔操作や情報窃取等をする

IoT機器を踏み台とした大規模DDoS攻撃の事例

■ 米国DNS事業者への大規模攻撃事例

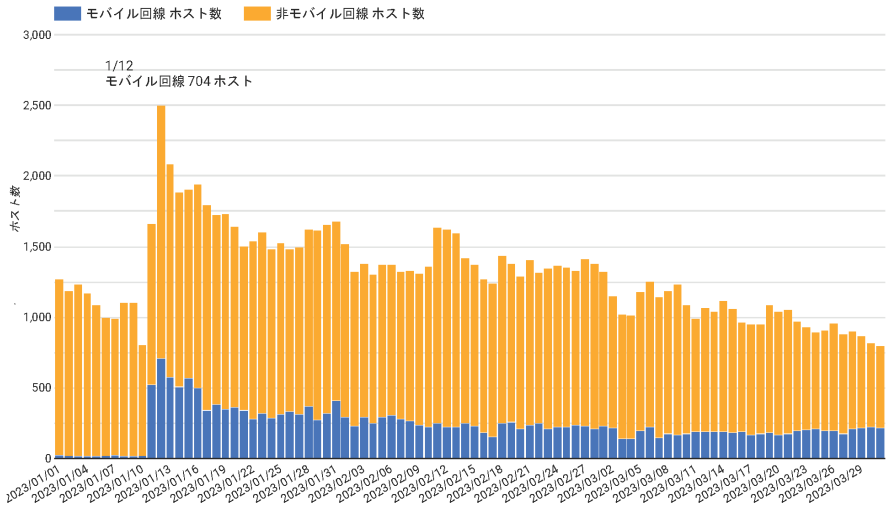
- 2016年10月21日、米国のDyn社のDNSサーバーに対し、大規模なDDoS攻撃が２回発生。その結果、多数の企業のサービスにアクセスしにくくなる等の障害が発生。
- 「Mirai」というマルウェアに感染した10万台を超えるIoT機器から、大量の通信（最大1.2Tbps)が発生したことが原因。



国内IoT機器が踏み台にされた事例

■ 国交省地方整備局の河川監視カメラ侵害事例

- 2023年1月、国土交通省　近畿地方整備局が管理する河川監視用のモバイルカメラ199台において、大量の通信を確認。中部・中国地方整備局等が管理するカメラも合わせ、不正アクセスの疑いのある337台のカメラの運用を休止。



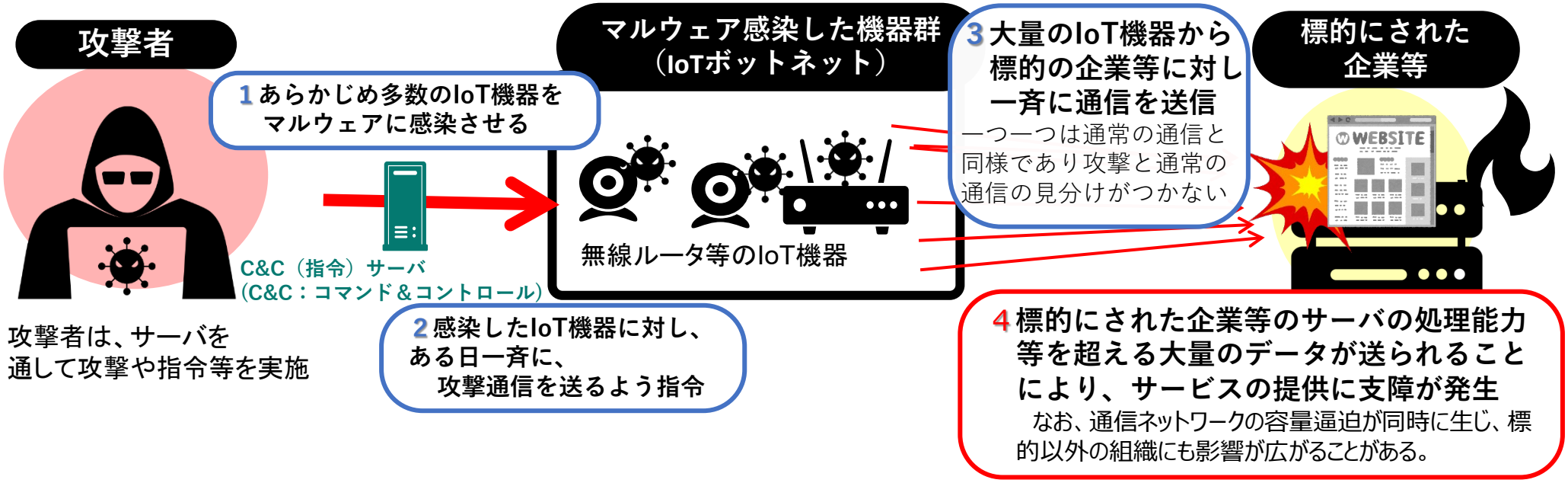
2023年１月からのモバイル機器の感染の急増（グラフ青）

IoT機器を悪用したサイバー攻撃（DDoS攻撃等） ～DDoS攻撃とは～

- 情報通信ネットワークに大きな影響を与えるDDoS攻撃は、**IoT機器に攻撃指令を出すC&Cサーバ**※1と、マルウェアに感染した**多数のIoT機器（ボット）**から構成される**IoTボットネット**※2によって引き起こされる。
- 攻撃者は、あらかじめ脆弱な無線ルータ等のIoT 機器にマルウェアを感染させ、多数のIoT機器をボット化しておく。そしてある日突然、それら大量のIoT機器から一斉に攻撃を行い、標的にされた企業等のサーバをダウンさせる等によりサービス提供不能な状態に追い込む。
  （ IoT機器から届く一つ一つの通信はサーバ側からは通常の通信と見分けがつかず、通常の通信だけを選別してサービスを継続することが難しい。）

※1　C&Cサーバ：「Command & Controlサーバ」の略。
　　マルウェア感染端末にサイバー攻撃に係る指示を送る指令元のサーバ。
※2　ボットネット：遠隔から操作出来ることから、ロボットとネットワークの造語。
　　IoT機器で構成されるものを「**IoTボットネット**」という。

DDoS攻撃の概略図

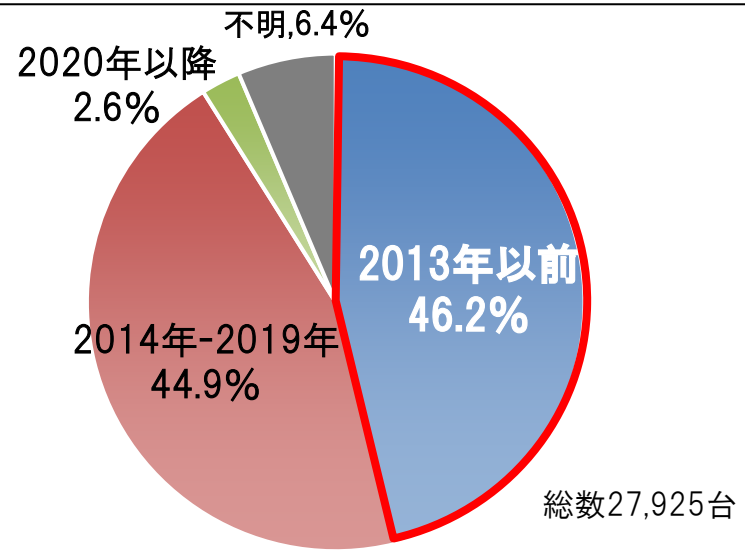


IoT機器のセキュリティ対策における課題

脆弱性等があるIoT機器やサイバー攻撃の脅威に関する課題

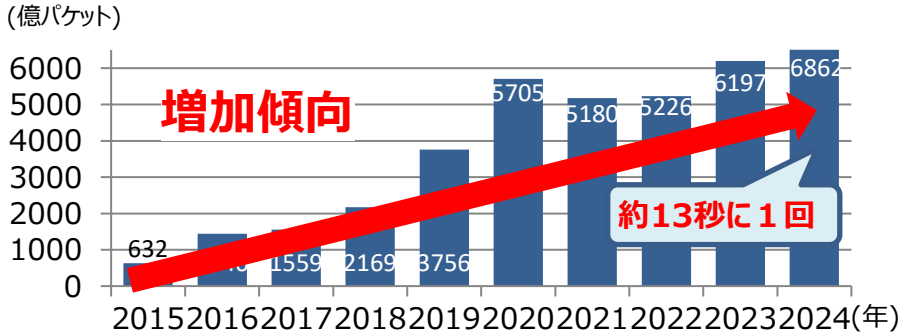
■ **ID・パスワードに脆弱性があるIoT機器**は、10年以上前の機種が４割強も存在するなど**古い機器を中心に残存。**

ID・パスワードに脆弱性がある機器の発売年別内訳
（2022年11月～2023年４月）



■ **サイバー攻撃の脅威は変化**しており、
①**新たなネットワーク経路**（通信プロトコル、ポート）を狙った攻撃
②**ID・パスワード以外の脆弱性**（ファームウェア等）を狙った攻撃
も発生。

■ **マルウェアの活動状況は依然として活発。サイバー攻撃関連通信数**も逓増。



利用者の意識に関する課題

■ IoT機器のセキュリティ対策に対する**利用者の意識が十分ではなく、対策方法も利用者にとって難しい**ものとなっている。

Wi-Fiルータ利用者向けのアンケート結果によれば、
- **57.8%**の利用者がWi-Fiルータのセキュリティを意識したことがない
- **81.7%**の利用者が自宅のWi-Fiルータがサイバー攻撃されると考えたことがない
- 購入時のパスワードをそのまま利用している利用者が**42.7%**

（出典）デジタルライフ推進協会（DLPA）Wi-Fiルーターセキュリティ対策ポイントを基に作成

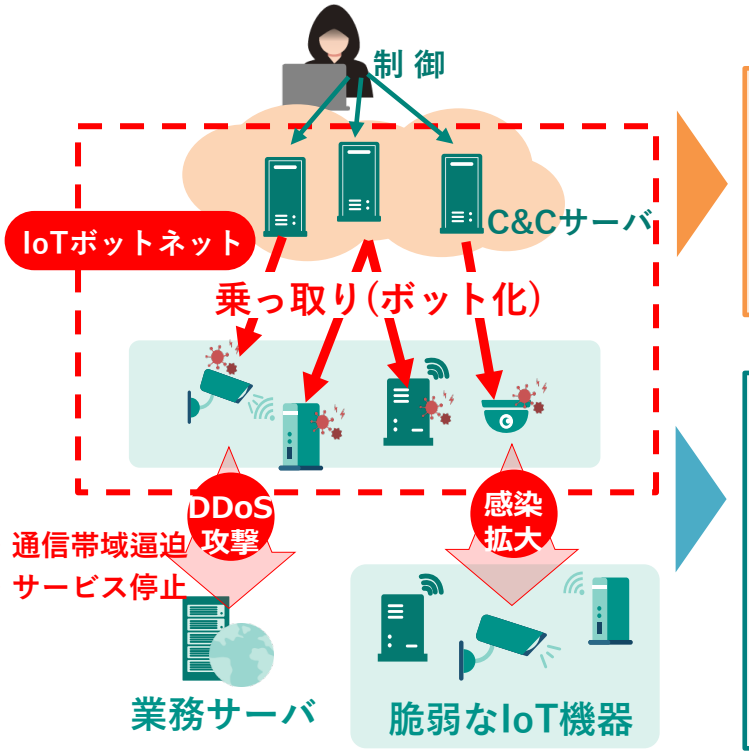
■ **法人利用者**については、管理責任の所在が曖昧など**適切な管理体制がない**ケースもある。

	所有者	設置者	管理者	使用者
一般利用者	購入者			（＋家族）
法人利用者	企業	設置委託業者	管理委託業者	社員、客

（出典）第３回情報通信ネットワークにおけるサイバーセキュリティ対策分科会ヤマハ発表資料を基に作成

IoTセキュリティ対策の強化に向けた対策（全体像）

- **IoT機器のセキュリティ対策**を進め、**IoT機器の安心・安全な利用環境を確保**するためには、(1) マルウェアに感染した、又は感染する危険性が高い**脆弱なIoT機器の検出と対処**と、(2) 指令を出す**C&Cサーバの検知と対処**を実施するとともに、(3) IoTの適正な利用環境構築に向けた**リテラシー向上活動**の展開が必要。



ネットワーク側

(2) ボットに対して指令通信を出す
C&Cサーバへの対処

■ ネットワーク上の情報の分析により**C&Cサーバを検知**し、その**情報を収集・分析・共有**

端末側

(1) マルウェアに**感染済**、感染する蓋然性の高い**脆弱性を有するIoT機器への対処**

■ 感染拡大通信等から**既にマルウェアに感染しているIoT機器を検知**し、対処

■ 攻撃インフラの拡大を防ぐため、感染する蓋然性の高い**脆弱性を有するIoT機器を検知**

■ 脆弱なIoT機器等の観測結果を踏まえたIoT機器の**利用者への注意喚起等**の実施

連携

周知啓発等

(3) IoTの適正な利用環境構築に向けた**リテラシー向上活動**

■ **ネットワークセキュリティに関するガイドライン**の作成・普及

■ **ホームページ・オンライン講座等**を通じた普及啓発活動

(1) マルウェアに感染したIoT機器への対処（端末側の対策）

NICTによる「サイバー攻撃に悪用されるおそれのあるIoT機器等」の観測を実施。 ※第５期NICT中長期計画（令和３年度～令和７年度）に基づき実施。

(2) 指令通信を出すC&Cサーバの検知・対処（ネットワーク側の対策）

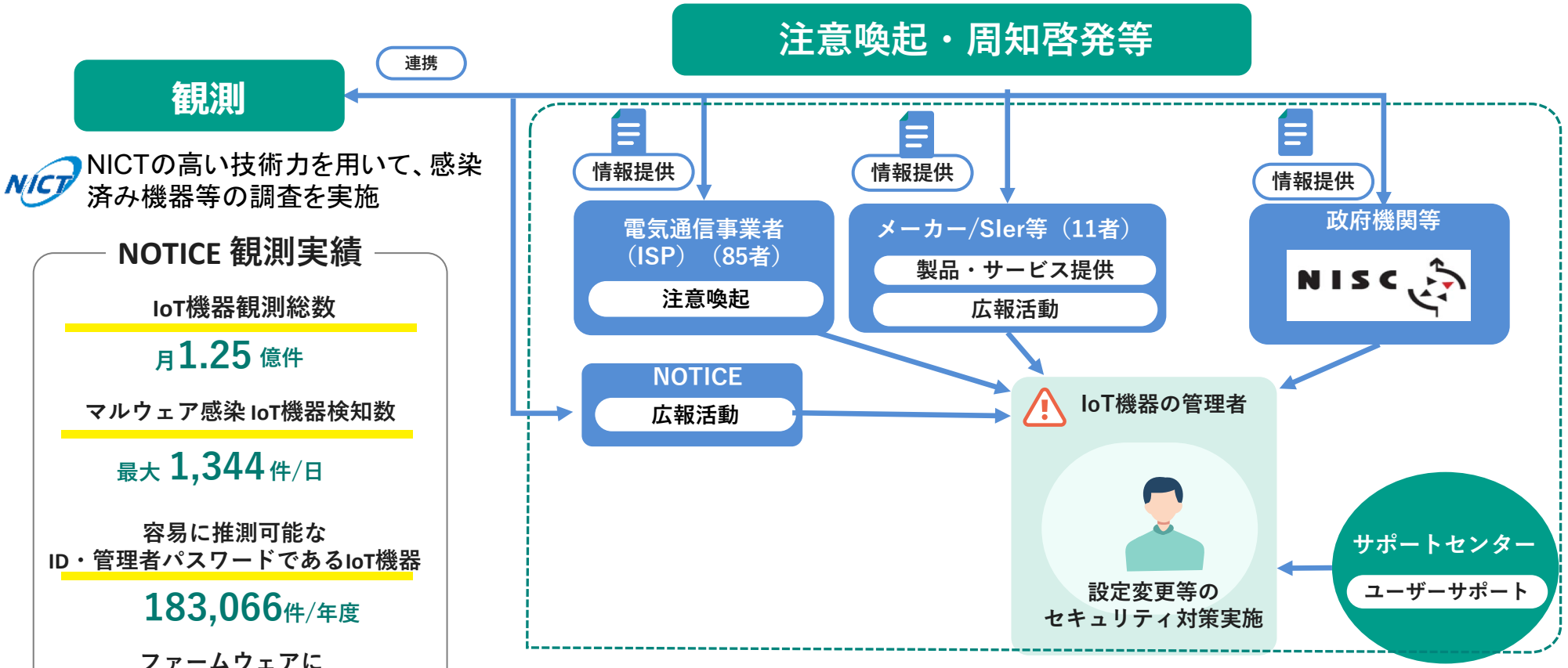
ネットワーク上の情報を活用した、ISP等によるサイバー攻撃インフラ（C&Cサーバ）の観測を実施。 ※令和６年度より本事業において実施。

(3) IoTの適正な利用環境構築に向けたリテラシー向上活動

無線LAN（Wi-Fi）をはじめとするIoT無線通信の利用者・提供者向けにセキュリティガイドラインを作成、周知啓発を実施。

（１）マルウェアに感染したIoT機器への対処（端末側の対策）

- マルウェアに感染したIoT機器は新たな機器に感染を広げ規模を拡大するため感染拡大通信を行う。この感染拡大通信等をNICTが観測・調査し、**既に感染しているIoT機器や、今後感染する危険性が高い脆弱なIoT機器を発見**する。**それらのIoT機器を使用している管理者**に対し、電気通信事業者と連携して**注意喚起・周知啓発等**を行うことで、IoTボットネットによる**サイバー攻撃（DDoS攻撃）の発生と被害を軽減**する。（NOTICE事業）



NOTICE 観測実績

IoT機器観測総数

月1.25 億件

マルウェア感染 IoT機器検知数

最大 1,344 件/日

容易に推測可能な
ID・管理者パスワードであるIoT機器

183,066件/年度

ファームウェアに
高リスク脆弱性を有するIoT機器

月 4,138 件

※2025年3月結果

※利用者からのサイバー攻撃の被害の申告を待つことなくプッシュ型による支援を実施

（１）マルウェアに感染したIoT機器への対処（端末側の対策）

- NICTでは、NICT法の改正に伴い、令和６年度より、サイバー攻撃に悪用されるおそれのあるIoT機器を調査し、電気通信事業者（ISP）や機器メーカー、機器の管理者等に必要な助言及び情報提供を行う「サイバーセキュリティ対策助言等業務」を法定業務として開始。

情報通信研究機構（NICT）法

中長期目標・計画に合わせ
5年サイクルで更新（現目標・計画は令和7年度まで）

総務大臣

中長期目標・計画に係る意見聴取 → **サイバーセキュリティ戦略本部**

特定アクセス行為等に係る実施計画認可

中長期目標策定・計画認可

情報通信研究機構（NICT）

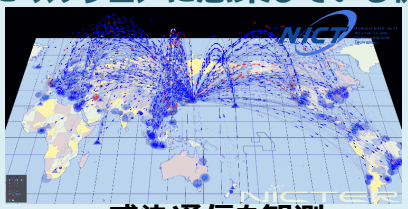
サイバーセキュリティ対策助言等業務

（サイバー攻撃に悪用されるおそれのあるIoT機器を調査し、機器の管理者等に必要な助言及び情報を提供）

ID・パスワードの設定に脆弱性を有する機器

ファームウェアの脆弱性等のID・パスワード以外の脆弱性を有する機器

既にマルウェアに感染している機器



感染通信を観測

令和６年度以降も継続して実施（特定アクセス等実施業務）

NICTの業務として新たに法的に位置づけ

IoT機器メーカー

電気通信事業者（ISP）

SIer

その他セキュリティ関係者

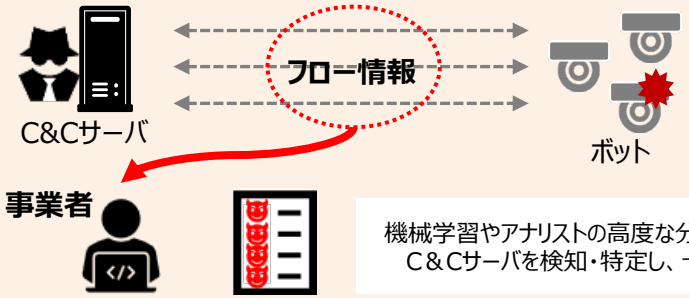
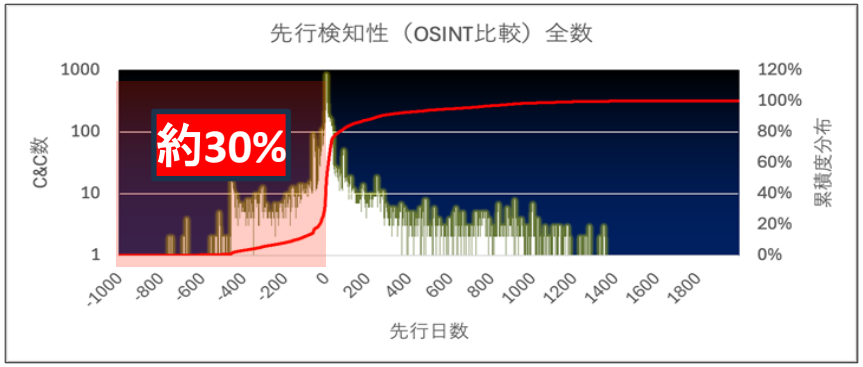
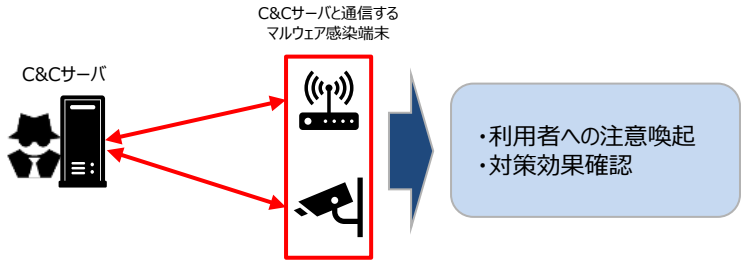
注意喚起

機器の利用者

（２）指令通信を出すC&Cサーバの検知・対処（ネットワーク側の対策）

- 電気通信事業者（ISP）が自社のネットワーク上を流れるフロー情報※を分析することで、IoTボットネットと通信をする**C&Cサーバを事前に検知**し、**対策に活用**するための実証事業を実施中。
- 実績については、検知したC&Cサーバの一部は**公開情報よりも早く検知**できたほか、検知したC&Cサーバのリストに基づき、**NOTICE事業と連携した注意喚起及び対策効果確認**を試行的に実施中。

※ 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）

	検知	対処
取組	フロー情報を分析することによりC&Cサーバを検知  機械学習やアナリストの高度な分析によりC&Cサーバを検知・特定し、一覧化	検知したC&Cサーバのリストに基づき注意喚起等の対処を実施  サイバー攻撃対処を実施
主な実績	 本実証で検知したC&Cサーバのうち、約30%の数は公開情報よりも早く検知。	C&Cサーバを活用したサイバーセキュリティ対策の試行例  NOTICE事業と連携した注意喚起を実施した上で、当該C&Cサーバとの通信が行われなくなったことを確認。

（３）IoTの適正な利用環境構築に向けたリテラシー向上活動

- 総務省では、無線LAN（Wi-Fi）をはじめとするIoT無線通信の利用者・提供者向けにセキュリティガイドラインを作成し、周知啓発に活用。
- 令和６年度は、無線LAN利用者・提供者への調査を実施するとともに、最新のセキュリティ動向に対応させるため、無線LAN利用者・提供者向けのセキュリティガイドライン等の改訂・公表や、無線LANセキュリティに関するオンライン講座の開講による、各種周知啓発活動に取り組み、セキュリティ対策・対策意識の浸透に貢献。

今後の方向性

- 本事業のそれぞれの取組の今後の方向性について、
  - ① **マルウェアに感染したIoT機器への対処**の取組について、サイバー攻撃の質的な変化（ファームウェア脆弱性の悪用）への対応に重点を移した取り組みを行う。また、IoT機器の直接の管理者だけでなく関係するステークホルダーを対象とした取り組み（メーカー/SIerとの連携等）を強化する。
  - ② **指令通信を出すC&Cサーバの検知・対処**の取組については、検知の部分ではC&Cサーバの早期検知に成功しており、対処の部分ではC&Cサーバ情報を利活用したISPにおいて自社網内の脆弱な端末を発見し注意喚起に繋げるなど、一定の実績を上げている。こうした実績を積み重ねることで、フロー分析が可能な事業者やC&Cサーバ情報を利活用し対策に取り組む事業者の増加を目指す。
  - ③ **IoTの適正な利用環境構築に向けたリテラシー向上活動**の取組については、サイバーセキュリティ全体の動向や、通信規格の高度化、利用・提供状況の変化等を踏まえ、必要に応じて無線通信に関するガイドライン等の改訂を行い、最新の状況を反映した形での周知啓発・リテラシー向上活動を継続実施する。
- サイバー攻撃の大規模化・複雑化・巧妙化を踏まえ、**国家安全保障戦略（令和４年12月16日閣議決定）**に基づき、本年５月に**サイバー対処能力強化法等**が成立。脆弱性の対処をはじめとする官民連携の観点で、**NICTが観測したIoT機器の脆弱性情報等の情報連携**や**IoT機器の利用者等に対する注意喚起業務に係る連携**が求められており、こうした政府全体のサイバー安全保障の取組とも連携しながら事業を推進する。

（参考）サイバー対処能力強化法等の国会審議

2024年4月24日 参議院内閣委員会

○河野義博君

次に、関係機関との連携について伺います。第七十一条二項におきまして、国の行政機関、情報処理推進機構、IPAですね、情報通信研究機構、NICT、相互に緊密に連絡、協力しなければならない旨規定をされております。例えば、NICTでは大規模なサイバー攻撃観測網を構築していますが、政府が独自で収集した情報に加えて、これらの組織の能力も活用していくことが必要ではないでしょうか。IPAやNICTといった関係機関と具体的にどのように協力をしていくことを想定しておられますでしょうか。

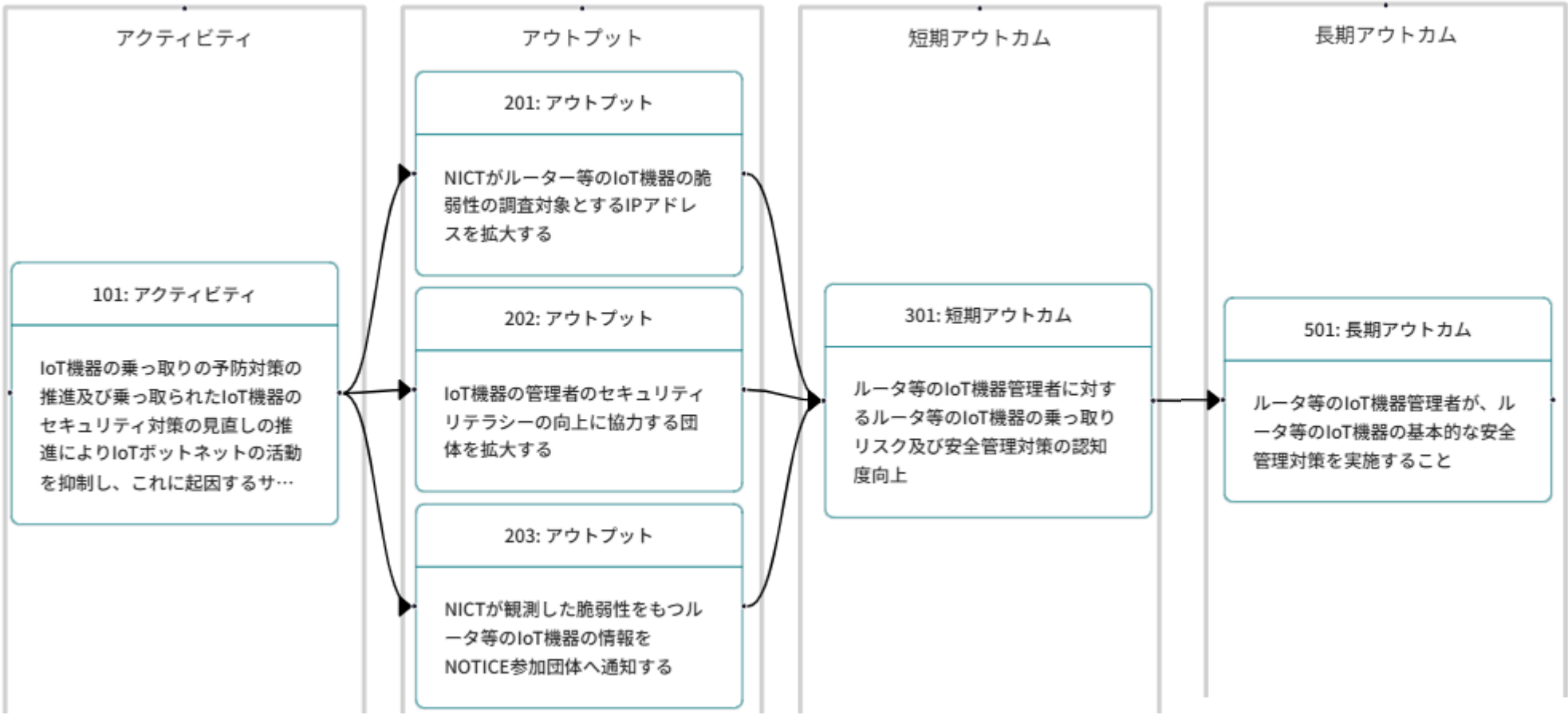
○政府参考人（門松貴君）

お答えいたします。御指摘のとおりでございまして、第七十一条において、国の行政機関のほか、情報処理推進機構と情報通信研究機構について相互に緊密に連携し、協力しなければならない旨規定をしているわけでございます。両独立行政法人、いずれもサイバーセキュリティーに係る高い専門性と情報収集能力を有しているわけでございまして、日頃からサイバー空間の観測や分析、脆弱性情報の管理、事業者への支援、注意喚起を行っているわけでございます。

本法案の中では、例えば第四十二条の部分ですが、脆弱性の対処について定められているところでございますが、これを例に取ると、両法人においては、例えばまずNICTさんの観測網との関係で、サイバー空間における脆弱性悪用情報を監視する内容を利用させていただいたり、IPAの早期警戒パートナーシップに基づく脆弱性情報の集約管理、さらにはNICT、IPA双方から電子計算機等のユーザーに対する周知、助言といったことを今取組を行っておられますので、こうした業務を連携させて実施していくということを想定をしております。いずれにせよ、高度化するサイバー攻撃に対しては、政府の司令塔機能の下で、御指摘の両独立行政法人を始め、関係行政機関や専門機関、一体となって対処するように万全を期してまいりたいと考えております。

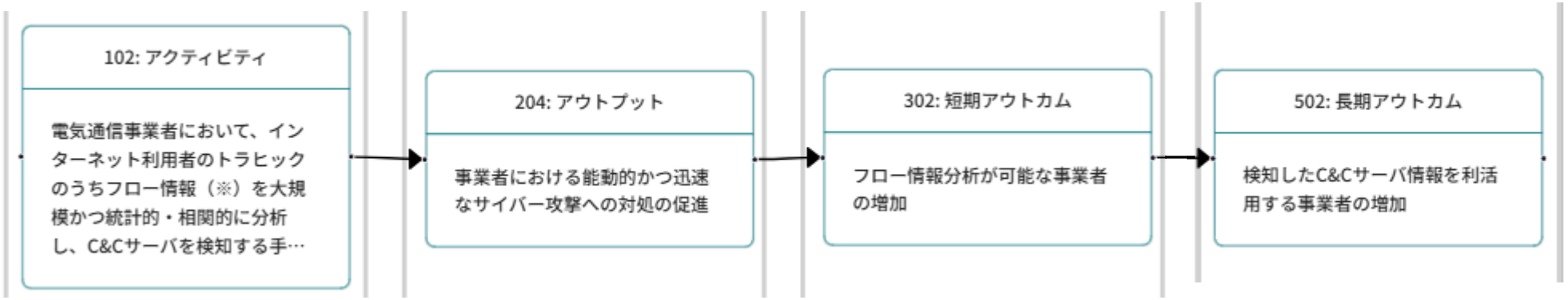
活動・成果目標　（１）

(1) マルウェアに感染したIoT機器への対処



活動・成果目標　（２）（３）

⑵ 指令通信を出すC&Cサーバの検知・対処



⑶ IoTの適正な利用環境構築に向けたリテラシー向上活動