資料１－２

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について

令和5年1月

事　務　局

１．情報通信ネットワークの機能に支障を及ぼし得るサイバー攻撃の状況

２．対策の方向性・現在の総務省の取組

３．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について

情報通信ネットワークの機能に支障を及ぼし得るサイバー攻撃の状況

➢ DDoS攻撃をはじめとする情報通信ネットワークの機能に支障を及ぼし得るサイバー攻撃の発生数や規模等は増大している。

攻撃の規模・数の増加

- 2022年第3四半期における**最大規模のDDoS攻撃は2.5Tbps**(※1)
  （参考）2016年10月当時、過去最大規模の攻撃とされたマルウェア「Mirai」による米国のDyn社のDNSサーバーに対する大規模DDoS攻撃の最大通信は1.2Tbps
- 2022年第3四半期のネットワーク層で発生したDDoS攻撃の数は、**前年比97%増**、金銭の支払いを要求するランサムDDoS攻撃の数は**前年比67%増**(※1)

攻撃対象の拡大

- 2022年第4四半期に攻撃を受けたユニークIP数は**過去5年間で最多**(※2)

攻撃継続時間の増加

- 2022年第2四半期のDDoS攻撃の平均継続時間は**前年比100倍の3000分に増加**(※3)

攻撃の潜在的脅威の増大

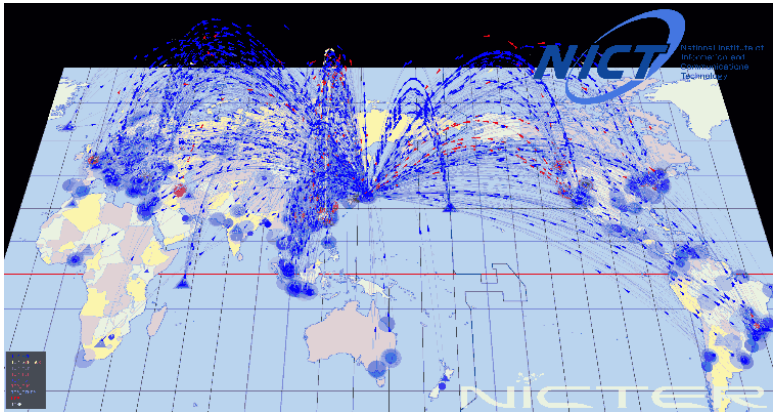
- 2021年下半期に観測した、DDoS攻撃に利用される可能性のあるコンピュータ、サーバ、IoT機器数はグローバルで1540万台となり、**2年間で3倍に増加**(※4)
- 2019年第3四半期から2020年第4四半期にかけて、IoT機器を対象とした**マルウェアの活動が3000%増加**(※5)

出典：
(※1)Cloudflare DDoS脅威レポート 2022年第3四半期 https://blog.cloudflare.com/ja-jp/cloudflare-ddos-threat-report-2022-q3-ja-jp/
(※2)Akamai：第 2 四半期にはサイバーテロリストによる DDoS 攻撃の標的となった被害者数が過去最多を記録 https://www.akamai.com/ja/blog/security/cyberterrorists-target-record-number-of-victims
(※3)Kaspersky：Crypto-collapse and rising smart attacks: Kaspersky reports on DDoS in Q2 (August 03, 2022) https://www.kaspersky.com/about/press-releases/2022_crypto-collapse-and-rising-smart-attacks-kaspersky-reports-on-ddos-in-q2
(※4)A10 DDoS脅威インテリジェンスレポート 2022年5月版 https://info.a10networks.com/2022-5-20-JP-CNT-DDoS-DDoSThreatIntelligenceReport-HD_LP-Registration-2.html
(※5)IBM Security X-Force https://www.ibm.com/reports/threat-intelligence/jp-ja/

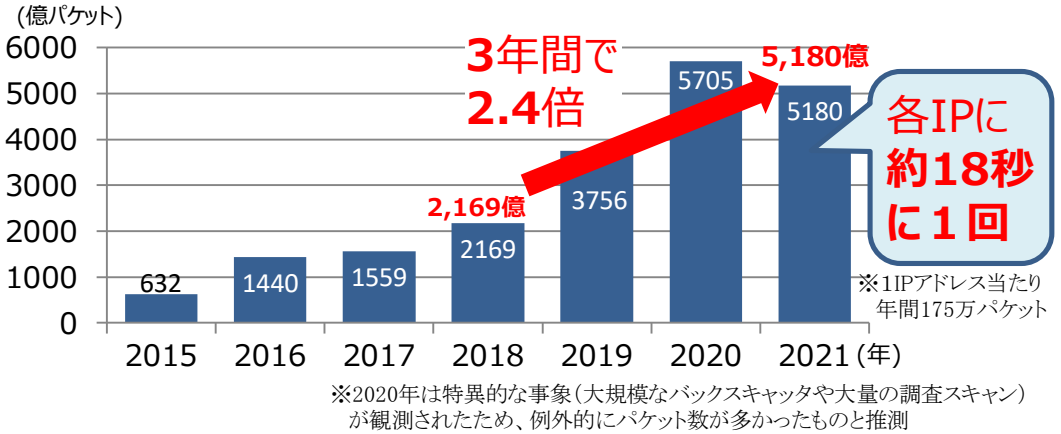
増加・多様化する無差別型サイバー攻撃　～NICTERによる観測～

➢ 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



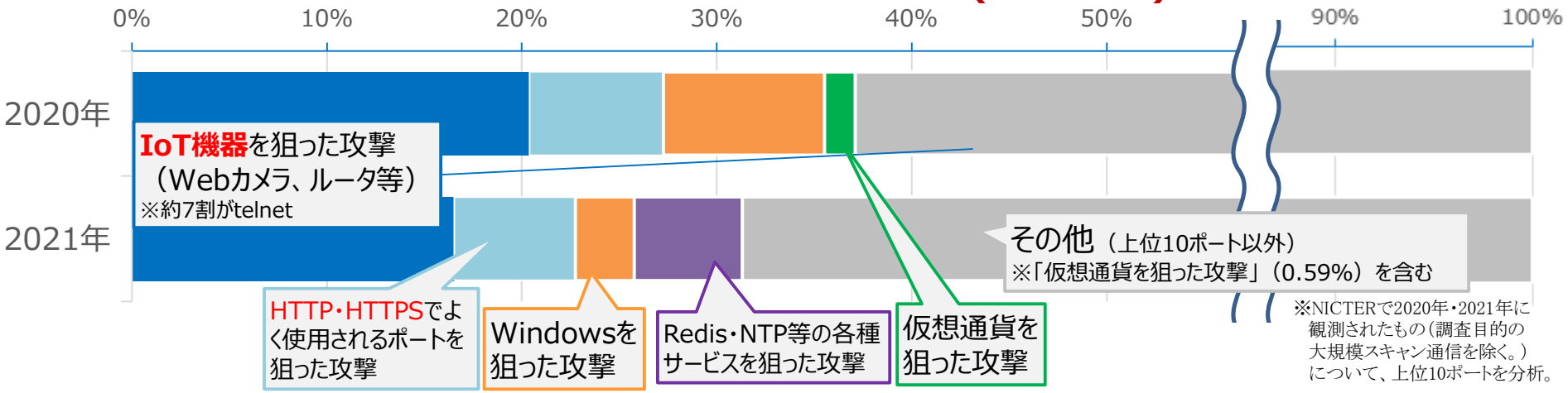
NICTERで１年間に観測されたサイバー攻撃関連の通信数



※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）

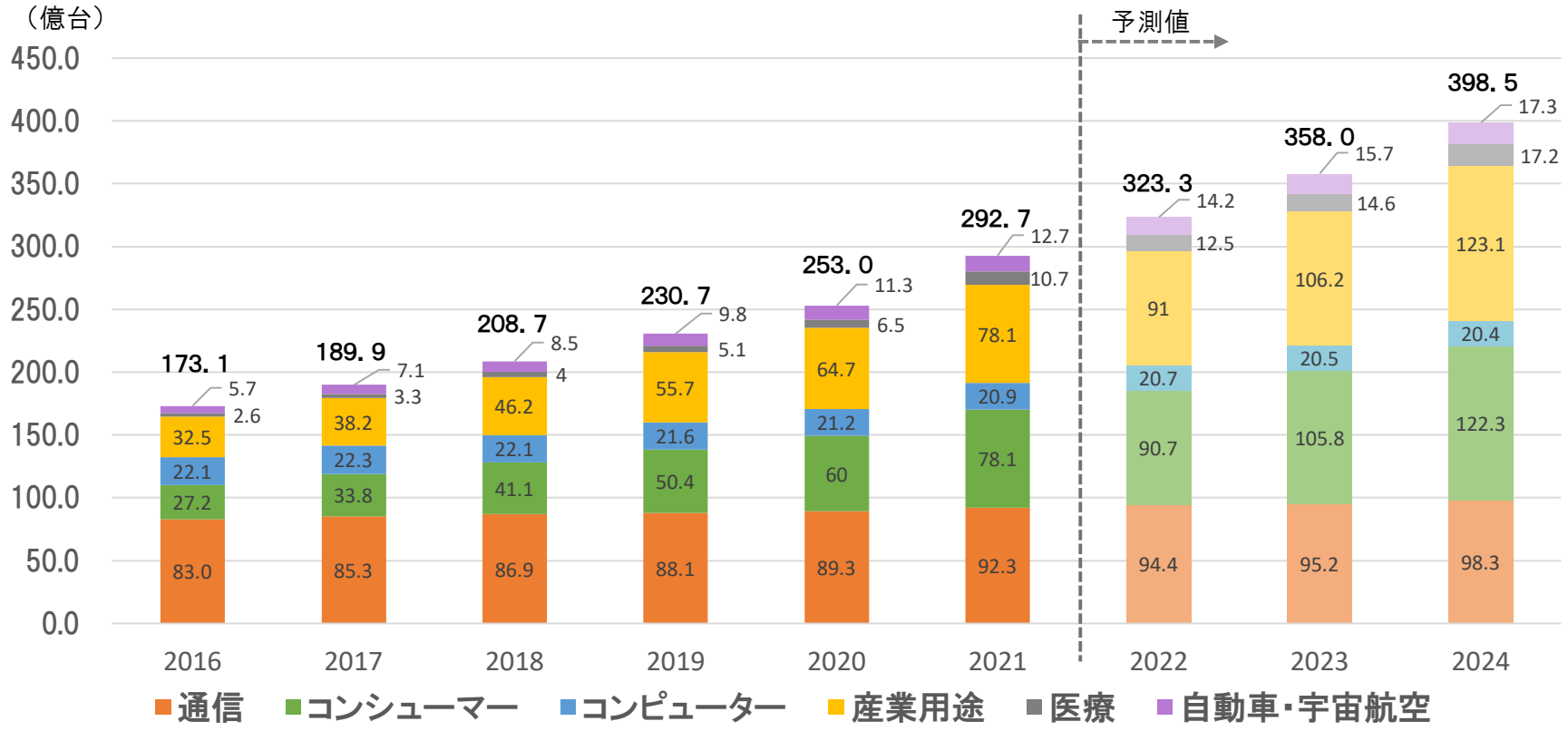
✓ **IoT機器を狙った攻撃が依然としてトップ**
✓ **攻撃(対象ポート)が多様化**



※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。

世界のIoT機器数の推移

➢ 社会全体のデジタル化等を背景として、世界のIoT機器の数は急速に増加。2021年の約293億台から、2024年には約400億台になると予測されており、今後も増加の一途を辿ることが見込まれている。



情報通信白書（R3年版、R4年版）を基に事務局作成

※図におけるIoTデバイスとは固有のIPアドレスを持ちインターネットに接続可能な機器及びセンサーネットワークの末端として使われる端末等を指す。
※各カテゴリの範囲は以下のとおり。
「通信」：固定通信インフラ・ネットワーク機器、2G・3G・4G各種バンドのセルラー通信及びWi-Fi・WiMAXなどの無線通信インフラ及び端末・
「コンシューマー」：家電（白物・デジタル）、プリンターなどのパソコン周辺機器、ポータブルオーディオ、スマートトイ、スポーツ・フィットネス、その他。
「コンピューター」：ノートパソコン、デスクトップパソコン、サーバー、ワークステーション、メインフレーム、スパコンなどのコンピューティング機器。
「産業用途」：オートメーション（IA/BA）、照明、エネルギー関連、セキュリティ、検査・計測機器などのオートメーション以外の工業・産業用途の機器。
「医療」：画像診断装置ほか医療向け機器、コンシューマーヘルスケア機器、その他検査機器（血統値計、心電計などのウェアラブル検査機器）。その他の検査機器は、2021年の数値から集計対象としている。
「自動車・宇宙航空」：自動車（乗用車、商用車）の制御系及び情報系においてインターネットに接続が可能な機器、軍事・宇宙・航空向け機器（例：軍用監視システム、航空機コックピット向け電装・計装機器、旅客システム用機器など）。

（参考）IoT機器がサイバー攻撃の対象として狙われやすい理由

➢ IoTの進展が企業活動や製品・サービスのイノベーションを加速する一方で、IoT特有の性質と想定されるリスクをもつことから、これらの性質とリスクを踏まえたセキュリティ対策を行うことが必要。

１）脅威の影響範囲・影響度合いが大きい

攻撃を受けると、ネットワークを介してシステム・サービス全体へその影響が波及（自動車・医療等における致命的影響等も存在）

２）IoT機器のライフサイクルが長い

工場の制御機器等をはじめ10年以上の長期にわたって使用され、構築・接続時に適用したセキュリティ対策が危殆化

３）IoT機器に対する監視が行き届きにくい

画面がなく問題の発生がわかりづらい上に、人目が行き届きにくく勝手なネットワーク接続をされかねない

４）IoT機器側とネットワーク側の環境や特性の相互理解が不十分である

IoT機器と接続ネットワークの双方でセキュリティ要件の整合をとらなければ、必要な安全性等をみたせない

５）IoT機器の機能・性能が限られている

適切な暗号等のセキュリティ対策を適用できない場合が存在

６）開発者が想定していなかった接続が行われる可能性がある

これまで外部につながっていなかったモノがネットワークに接続され、当初想定していなかった影響が発生

出典：IoT推進コンソーシアム・総務省・経済産業省「IoTセキュリティガイドラインver1.0」（平成28年7月）

１．情報通信ネットワークの機能に支障を及ぼし得るサイバー攻撃の状況

２．対策の方向性・現在の総務省の取組

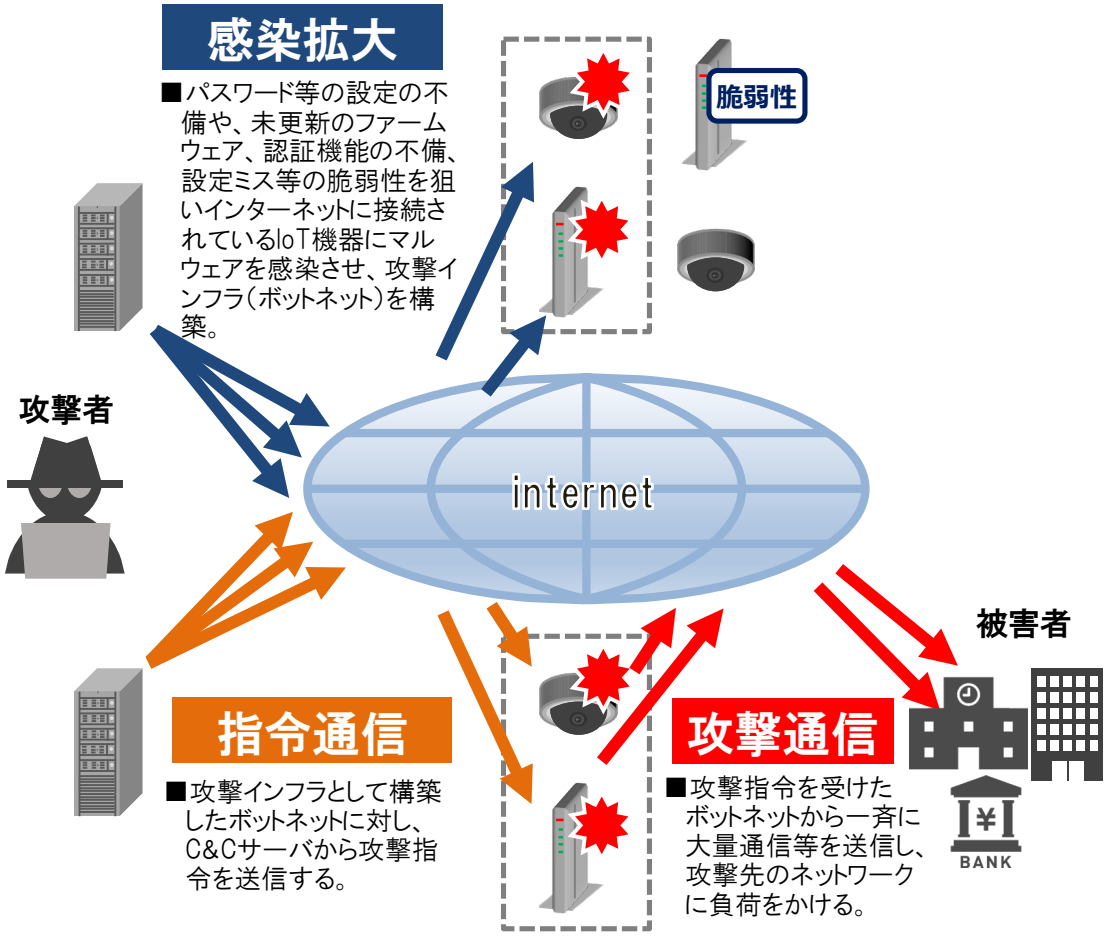
３．情報通信ネットワークにおけるサイバーセキュリティ対策分科会について

対策の方向性

- DDoS攻撃のように情報通信ネットワークの機能に支障を生じさせるようなサイバー攻撃には、①IoT機器にマルウェアを感染させる攻撃インフラの拡大と、②これらの攻撃インフラを利用するネットワークを通じた攻撃の実行の２つの段階が存在。
- このようなサイバー攻撃への対策として、現在の取組状況や課題を踏まえた上で、**端末側（IoT機器）、ネットワーク側の双方から総合的な対策を講じていくことが必要。**

①攻撃インフラの拡大

②攻撃実行



端末側（IoT機器）における対策

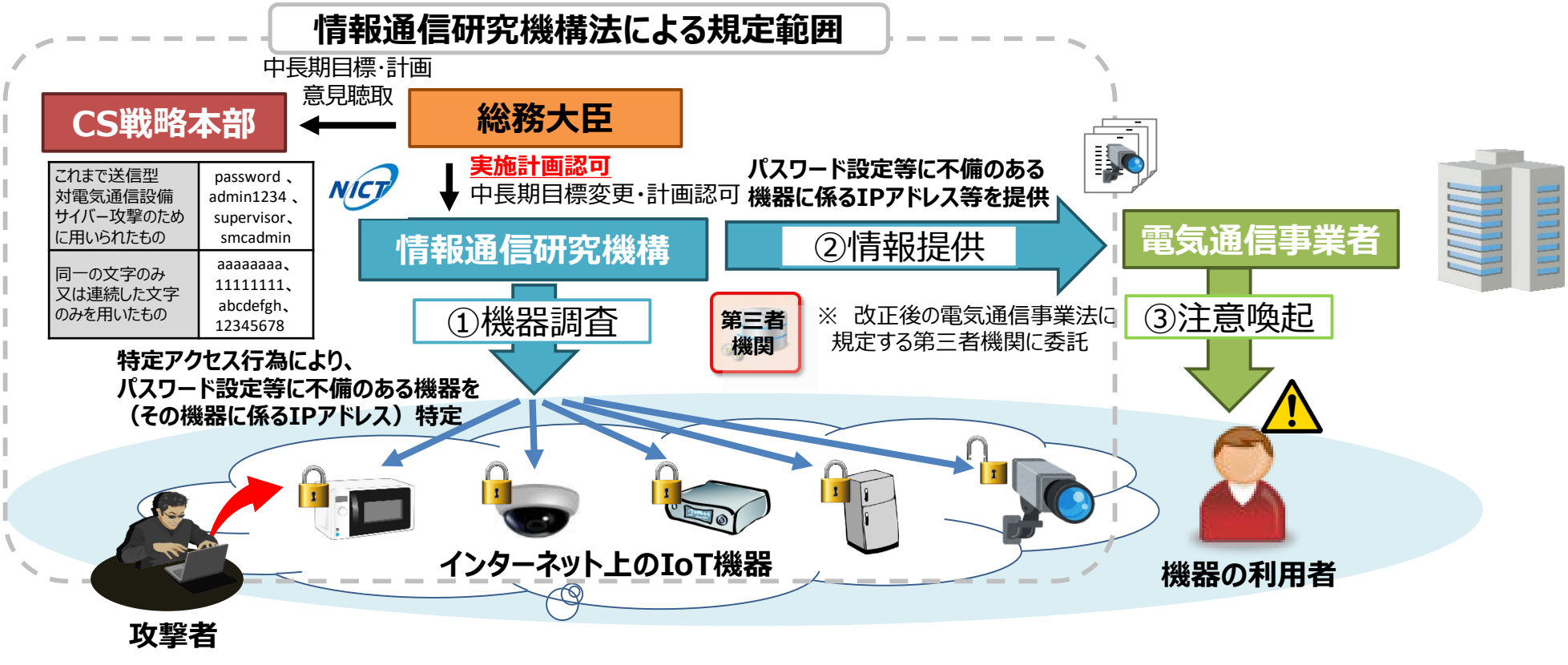
■ 攻撃インフラの拡大（ボットネット化）を防ぐため、既にマルウェアに感染しているIoT機器や、感染する蓋然性の高い脆弱性を有するIoT機器への対処が必要。

ネットワーク側における対策

■ サイバー攻撃による被害を抑止するため、ボットネットに対して攻撃の指令通信を出すC&Cサーバへの対処をはじめ、ネットワーク側の対策が必要。

国立研究開発法人情報通信研究機構法の改正（NOTICE）

- IoT機器（監視カメラ、センサ等）を悪用した**サイバー攻撃の深刻化**への対応として、**情報通信研究機構法（NICT法）を改正し、パスワード設定等に不備のあるIoT機器の調査**等の業務を追加（**2018年11月1日施行、2024年3月31日までの５年間の時限措置**）
- NICTが**サイバー攻撃に悪用されるおそれのあるIoT機器**にネットワーク上でアクセスし、ログインを試行。その結果、容易に推測できるパスワード設定のまま使用している利用者への注意喚起を行う「**NOTICE**」プロジェクトを2019年2月より実施。
- また、**感染通信を出している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、NOTICEの枠組みを活用して、利用者への注意喚起を行う取組を2019年６月より開始。



（参考）不正アクセス禁止法における手当て

➢ 平成30年５月に改正されたNICT法※において、不正アクセス禁止法で禁止されている不正アクセス行為から除外。※NICT法附則第８条第７項に規定

〇不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）

第二条（定義）

４　この法律において「**不正アクセス行為**」とは、次の各号のいずれかに該当する行為をいう。

一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）

（不正アクセス行為の禁止）

第三条　何人も、不正アクセス行為をしてはならない。

〇国立研究開発法人情報通信研究機構法（平成十一年法律第百六十二号）

附則第８条

２　機構は、第十四条及び前項に規定する業務のほか、**令和六年三月三十一日までの間、次に掲げる業務**を行う。

一　**特定アクセス行為を行い、通信履歴等の電磁的記録を作成**すること。

二　特定アクセス行為に係る電気通信の送信先の電気通信設備が次のイ又はロに掲げる者の電気通信設備であるときは、当該イ又はロに定める者に対し、**通信履歴等の電磁的記録を証拠として当該電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信先又は送信元とする送信型対電気通信設備サイバー攻撃のおそれへの対処を求める通知**を行うこと。

イ　電気通信事業者　当該電気通信事業者

ロ　電気通信事業者（電気通信事業法（昭和五十九年法律第八十六号）第百十六条の二第二項第一号イに該当するものに限る。第八項において同じ。）の利用者　当該電気通信事業者

三　前二号に掲げる業務に附帯する業務を行うこと。

７　第二項から第四項までの規定により機構の業務が行われる場合には、次の表の上欄に掲げる規定中同表の中欄に掲げる字句は、それぞれ同表の下欄に掲げる字句とする。

不正アクセス行為の禁止等に関する法律第二条第四項第一号	及び当該	、当該
	を除く	及び国立研究開発法人情報通信研究機構法（平成十一年法律第百六十二号）附則第九条の認可を受けた同条の計画に基づき同法附則第八条第二項第一号に掲げる業務に従事する者がする同条第四項第一号に規定する特定アクセス行為を除く

（参考）NOTICEの実施状況（2022年11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**74社**。
  当該ISPの**約1.12億IPアドレス**に対して調査を実施。
- **パスワード設定等の不備があるIoT機器**に対する注意喚起は、**４，４３０件**の**対象を検知**しISPへ通知。
- **感染通信を出しているIoT機器**に対する注意喚起は、１日平均**５６０件**の**対象を検知**しISPへ通知。

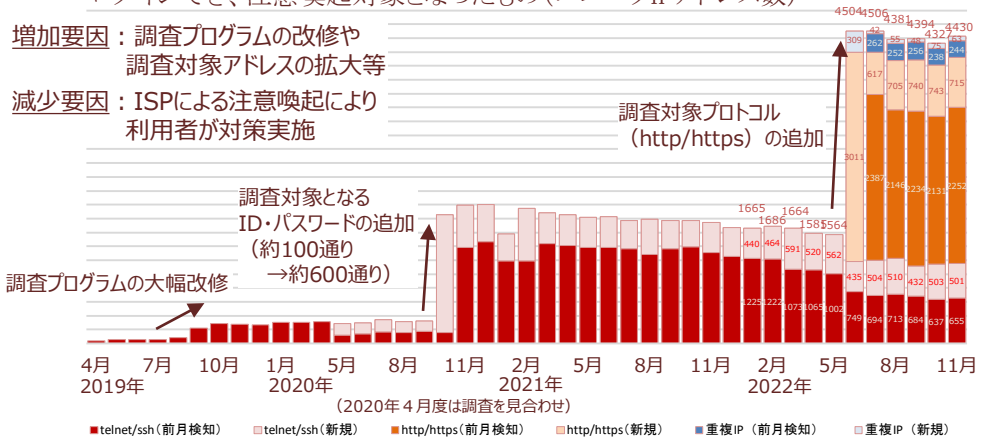
パスワード設定等に不備があるIoT機器に対する注意喚起の取組結果

注意喚起対象としてISPへ通知したもの*

４,４３０件（10月度:4,327件）

（参考） 2019年度からの累積件数：65,768件
ID・パスワードが入力可能だったもの：19.1万件

*) 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）



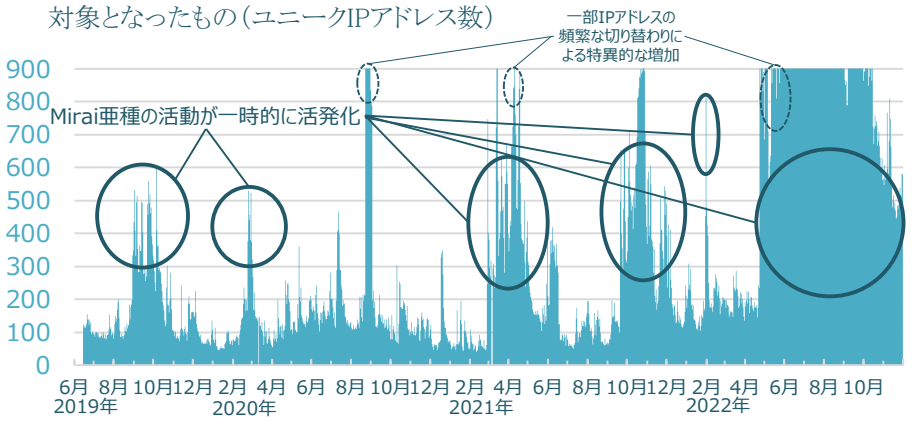
感染通信を出しているIoT機器に対する注意喚起の取組結果

注意喚起対象としてISPへ通知したもの**

１日平均５６０件（10月度:817件）

（参考） 期間全体での値： １日平均421件
最小：40件(2021/2/10)／最大：3,288件(2022/6/6)

**) 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）



✓ パスワード設定等に不備があるIoT機器に対する注意喚起における2022年6月以降の大幅な増加は、調査対象プロトコル（http/https）の追加によるものであり、急激にリスクが高まった訳ではありません。
✓ 感染通信を出しているIoT機器に対する注意喚起における2022年4月下旬以降の増加は、Mirai亜種の活動活発化を受け、国内の脆弱な機器(主にDVR/NVR)が感染したことによるものと考えています。

電気通信事業者による積極的セキュリティ対策

➢ 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）の分析を可能とする法的整理を行うとともに、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（令和３年11月）

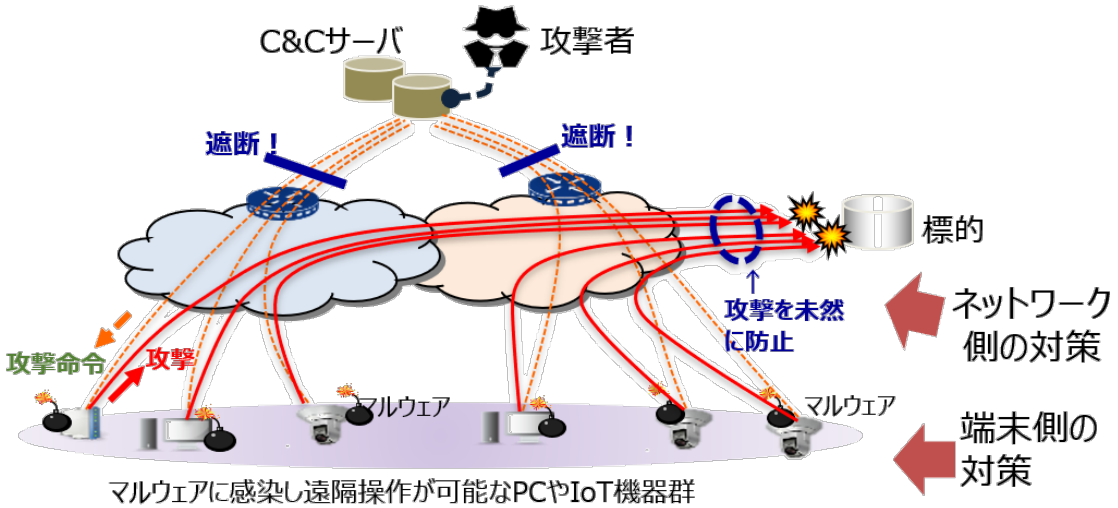
有識者による研究会において、電気通信事業者における、インターネット利用者のトラヒックのうち必要最小限の範囲で収集する**フロー情報の統計的・相関的な分析によるC&Cサーバである可能性が高い機器の検知**について、**通信の秘密に係る法的整理を実施済**。

※「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４～５年度）

※「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」

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**を実施中。



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

1. 情報通信ネットワークの機能に支障を及ぼし得るサイバー攻撃の状況

2. 対策の方向性・現在の総務省の取組

3. 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について

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

目的

- サイバー空間があらゆる主体が利用する公共空間となり、デジタル化を支える情報通信ネットワークは、今や国民生活や経済活動の重要かつ不可欠な基盤となっている中、サイバー攻撃により情報通信ネットワークの機能に支障が生じた場合には、社会・経済に多大な影響を及ぼすおそれがあり、その安全性・信頼性の確保は喫緊の課題。
- 本年８月にとりまとめられた「ICTサイバーセキュリティ総合対策2022」を踏まえ、依然としてIoT機器を狙ったサイバー攻撃が多く発生している状況等に対応するため、NOTICEや「電気通信事業者による積極的なサイバーセキュリティ対策に関する総合実証」等の取組みを含めた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について検討を行うことを目的として、「サイバーセキュリティタスクフォース」の下に分科会を設置。

主な検討事項

- IoTにおけるサイバーセキュリティの確保に向けた取組（NOTICE等）の現状と課題
- 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の現状と課題（総合実証の検討等）
- 上記課題の解決に向けた必要な方策

構成員

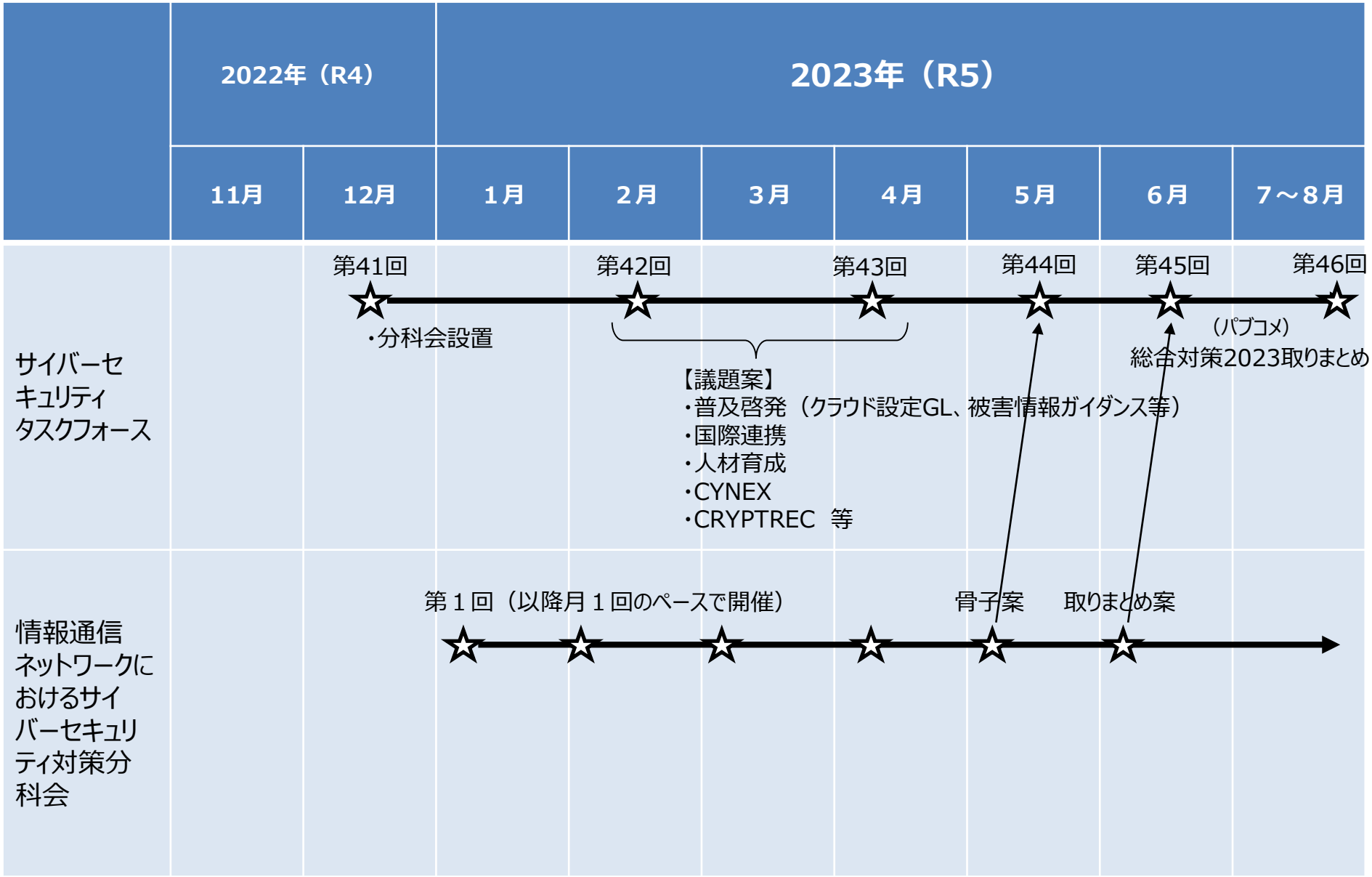
後藤　厚宏	情報セキュリティ大学院大学　学長	井上　大介	NICTサイバーセキュリティ研究所 サイバーセキュリティネクサス長
河村　真紀子	主婦連合会　会長	小塚　荘一郎	学習院大学法学部　教授
小山　覚	(一社)ICT-ISAC　ステアリング・コミッティ運営委員長 NTTコミュニケーションズ（株）　情報セキュリティ部長	齋藤　衛	(株)インターネットイニシアティブ　セキュリティ本部長
田中　暁	KDDI(株)　情報セキュリティ本部　セキュリティ管理部長	辻　伸弘	ＳＢテクノロジー(株)　プリンシパルセキュリティリサーチャー
藤本　正代	情報セキュリティ大学院大学　教授	吉岡　克成	横浜国立大学大学院環境情報研究院　准教授

（オブザーバ）ＮＩＳＣ、経産省

スケジュール

令和４年１２月	第41回サイバーセキュリティタスクフォース（分科会設置を決定）
５年　１月	第１回分科会（以降月１回程度のペースで開催）
令和５年夏	とりまとめ

今後のスケジュール（案）


2022年（R4）
2023年（R5）
11月
12月
1月
2月
3月
4月
5月
6月
7～8月
サイバーセキュリティタスクフォース
第41回
第42回
第43回
第44回
第45回
第46回
・分科会設置
【議題案】
・普及啓発（クラウド設定GL、被害情報ガイダンス等）
・国際連携
・人材育成
・CYNEX
・CRYPTREC　等
（パブコメ）
総合対策2023取りまとめ
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
第１回（以降月１回のペースで開催）
骨子案
取りまとめ案