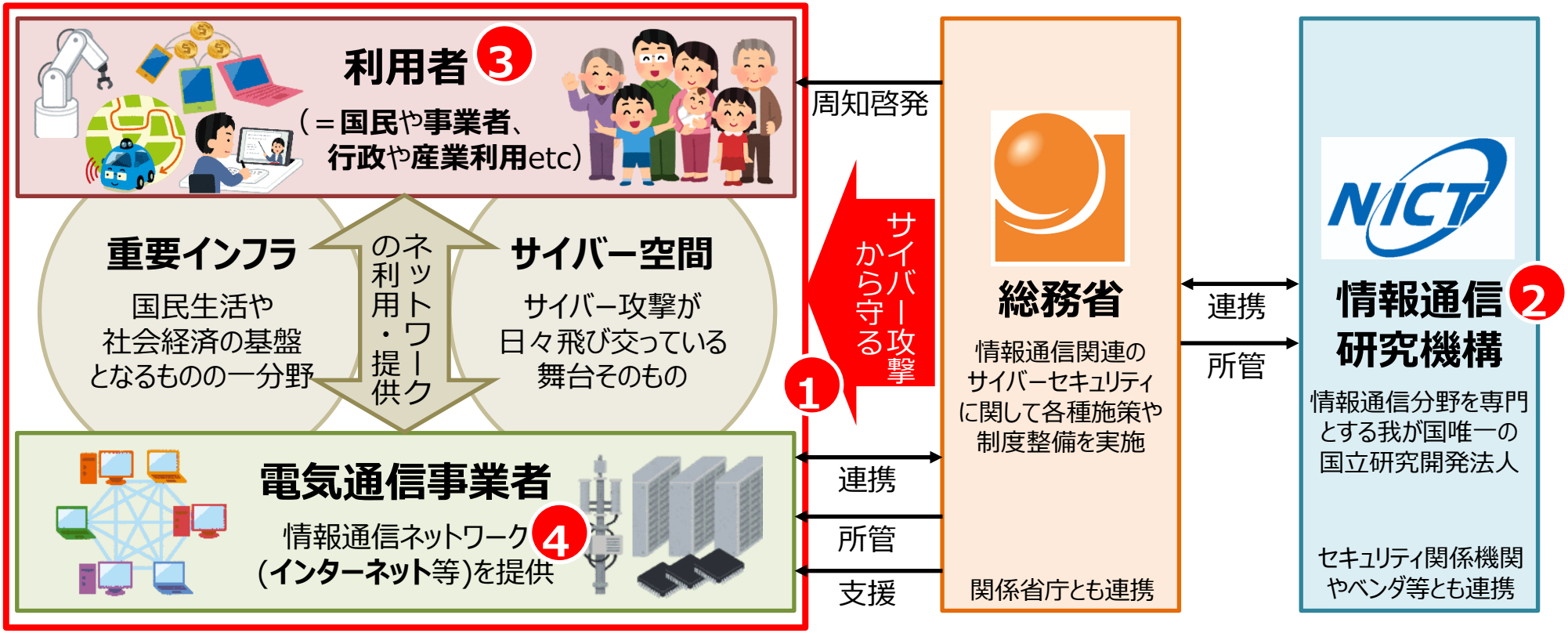
総務省におけるサイバーセキュリティ政策

２０２４年１１月

総務省　サイバーセキュリティ統括官室
総括補佐　梅城 崇師

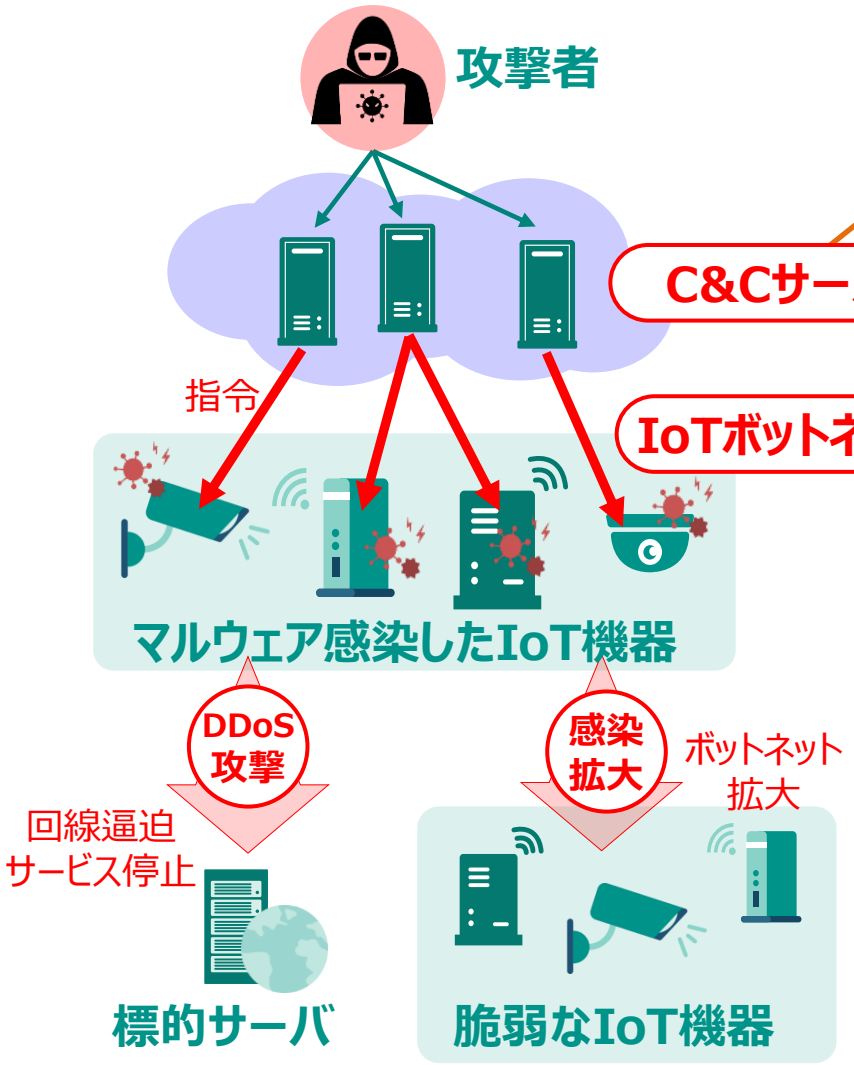
サイバーセキュリティと総務省の役割

- 総務省所管である**電気通信事業者＝情報通信ネットワーク**は、
  - 機能停止すれば国民生活や経済社会に甚大な影響が発生する**重要インフラ**（電力・金融等と同じく防護対象）
  - サイバー攻撃が飛び交う**サイバー空間そのもの**（サイバーセキュリティ確保のための重要な役割）
- **情報通信研究機構(NICT)**は、**サイバー攻撃**に関する**観測・分析**を長年行い、**高度な技術・人材**を保有
- **総務省**は電気通信事業者やNICTと連携し、**ネットワークや利用者**を**サイバー攻撃から守る**取組を実施
  （加えて、脅威情報・技術の国産化プロジェクトを推進し、我が国自らの力で脅威を検知し対抗できる基盤を構築）



❶ IoT機器を悪用したサイバー攻撃(DDoS攻撃等)への対策

- IoT機器の急増に伴い、**IoT機器を悪用**したサイバー攻撃（**DDoS攻撃**等）が増加
- DDoS攻撃は**ネットワークの速度低下**を引き起こすほか、**標的側での対応が難しい**
- **電気通信事業者と総務省が協力**して、**C&Cサーバ**と、攻撃役となる**脆弱なIoT機器**の両面から対策



IoTボットネットに対して指令通信を出すC&Cサーバへの対処

電気通信事業者がネットワークの管理のために利用する「**フロー情報**※」を**分析**することで、**C&Cサーバを検知**
→ 対策に活用するための**実証事業を実施中**

※IPアドレス、ポート番号、プロトコル、パケット数などに関する情報
ヘッダー情報のみでペイロード（データの本体部分）は含まない

マルウェアに感染した/感染する危険性が高い脆弱なIoT機器への対処

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、
（サイバーセキュリティに知見のあるNICTにおいて調査を実施）
電気通信事業者を通じ、**IoT機器の利用者に注意喚起**

＜調査＆注意喚起の対象＞
① 既にマルウェアに感染している機器
② ID・パスワードの設定に脆弱性がある機器
③ ファームウェアの脆弱性等がある機器

→「**NOTICE**」プロジェクト NOTiCE

❷ 研究開発・人材育成の産学官連携拠点『CYNEX』

- 国産セキュリティ技術の開発には、**サイバー攻撃データを大規模に収集・蓄積・活用する仕組み**が必要
- 情報通信研究機構（NICT）では、これまで次のような取組を実施
  サイバーセキュリティ研究所・・・最先端のサイバーセキュリティ関連技術の研究開発
  ナショナルサイバートレーニングセンター・・・実践的サイバー防御演習等による人材育成
- これらのデータ・知見を活用し、サイバーセキュリティに関する産学官の結節点となる先端的基盤として
  ＣＹＮＥＸ（CYbersecurity NEXus：サイネックス） を構築

❸ 無線LANセキュリティガイドライン

- 総務省では、**無線LAN(Wi-Fi)**の**セキュリティ対策**のため、2004年からガイドラインを継続的に作成
  ※2004年5月「安心して無線LANを利用するために」
- 新技術や最新のセキュリティ動向に対応するため、**2024年３月に最新の改定版を公表**

https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

自宅 Wi-Fi利用者 向け 簡易マニュアル

✓ 自宅にWi-Fiを設置・利用する方に向け、次のポイントをわかりやすく解説

① セキュリティ方式は **WPA2 または WPA3** に（WEPやTKIPは避ける）

② **パスワードは第三者に推測されにくい**ものに（管理用パスワードも要注意）

③ **ファームウェアを最新**に（自動更新設定を推奨）

公衆 Wi-Fi利用者 向け 簡易マニュアル

✓ 外出時に公衆Wi-Fiを利用する方に向け、次のポイントをわかりやすく解説

① 接続する**アクセスポイントをよく確認**（提供者やSSID名を確認；不審なものは使わない）

② **正しいURLでHTTPS通信**しているか確認（URL欄にエラーがない＆ドメインを確認）

公衆 Wi-Fi提供者 向け セキュリティ対策の手引き

✓ 公衆Wi-Fiを提供する方に向け、次のような点を確認するためのガイドを提示

・「公衆Wi-Fi」提供には**どのようなリスク**があるのか

・具体的に**どのような対策**をすればいいのか

❹ ISP等に対するネットワークセキュリティの確保

- インターネットは接続性と可用性を重視し、限られた信頼できる環境での使用が想定されていたため、仕様に脆弱な部分があり、**通信経路(BGP)**や**DNS**の**ハイジャック**、**なりすましメール**などが発生・懸念
- **電子認証技術を活用したセキュリティ向上策（RPKI／DNSSEC／DMARC）**が国際標準化
- 費用や導入インセンティブの面で国内ISPでの普及が進まないため、**ガイドライン策定**により導入を後押し

BGPハイジャック

Border Gateway Protocol
＝ネットワーク間で経路情報を交換するためのプロトコル

RPKI (Resource Public-Key Infrastructure)

IPアドレスとAS(ネットワークの集まり)番号の正当な所有者が、デジタル署名付きの情報を登録
受け取った経路情報が登録情報と一致するか確認することで、経路情報が正当かを確認
※登録情報をROA(Route Origin Authorization)、確認検証プロセスをROV(Route Origin Validation)という

→IPアドレスの分配を受けた者と、AS運用者の対策をガイドライン化

DNSハイジャック

Domaine Name System
＝ドメイン名をIPアドレス等に紐付けるための技術

DNSSEC (Domain Name System SECurity Extensions)

ドメインに関する正当な情報を保持するDNSサーバ(権威DNSサーバ)で、登録情報にデジタル署名を付与
DNS情報を読み取る側(フルリゾルバ)がデジタル署名を確認することで、DNS情報が正当かを確認

→ドメイン名登録者、権威DNSサーバ運用者、フルリゾルバ運用者の対策をガイドライン化

なりすましメール

DMARC (Domain-based Message Authentication, Reporting and Conformance)

ドメインの正当な所有者(メール送信側)が、処理方針をDNS上で宣言
受信側は、SPFやDKIMの検証を実施し、検証失敗時に送信側の処理方針に従って処理
※SPF：送信元IPアドレスを確認し、正当なドメインからのメールかを確認する仕組み
※DKIM：メールにデジタル署名を追加し、内容の改ざんを防ぐ仕組み
※処理方針：認証失敗時の処理方針として、何もしない(none)/隔離(quarantine)/拒絶(reject)を記載

→メール送信側、メール配信・再配信事業者、メール受信側の対策をガイドライン化