

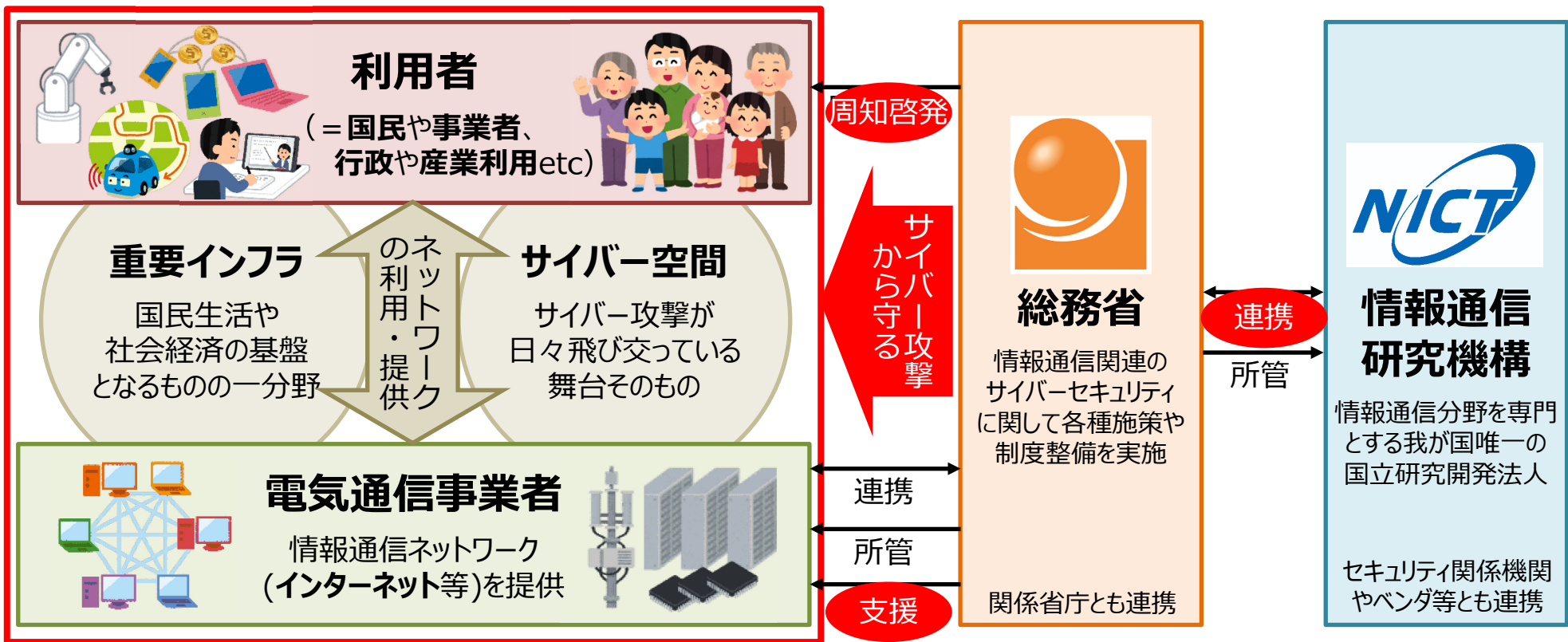
RPKI・DNSSEC・DMARCガイドラインが できた背景と現状

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

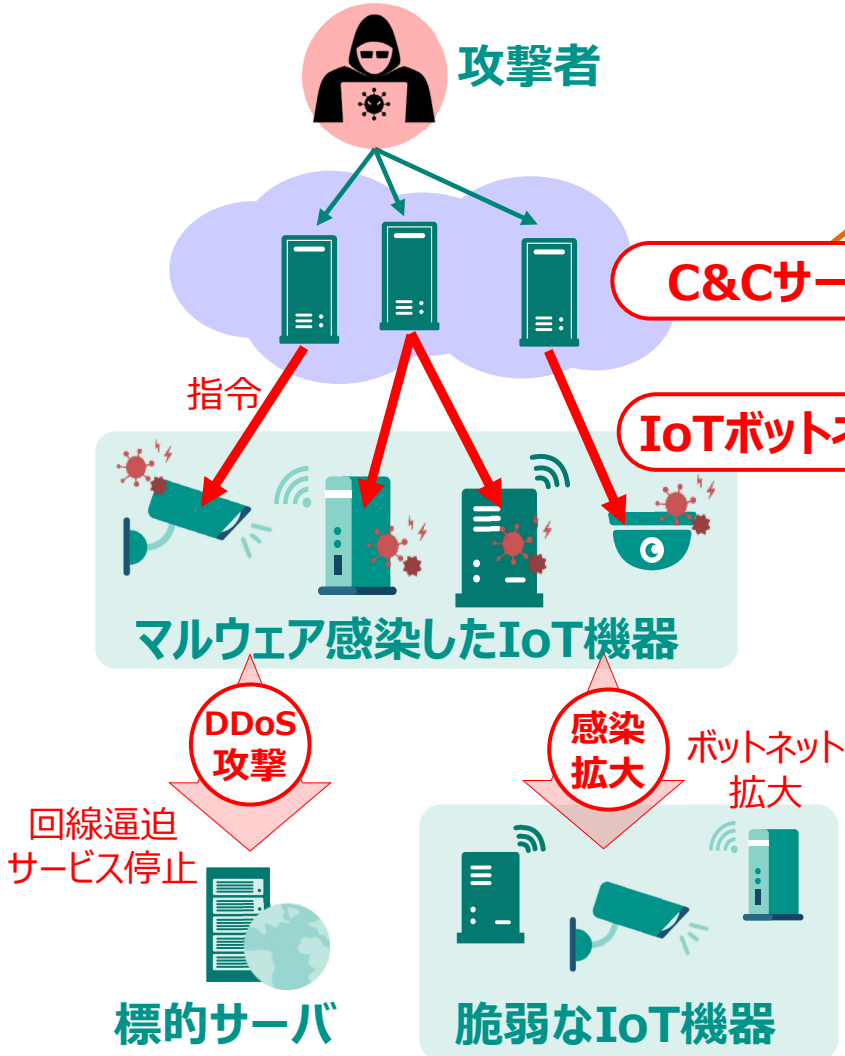
サイバーセキュリティと総務省の役割

- 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）



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機器を悪用した大規模なサイバー攻撃（DDoS攻撃等）が発生
- 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使用する「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



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室・・・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



テレワークのセキュリティ対策

- 総務省では、**テレワークのセキュリティ対策**のため、2004年からガイドラインを作成
- **コロナ禍による業務環境やセキュリティ動向の変化**に対応するため**2021年に全面改定**
- ガイドラインを補完するものとして、セキュリティ専任担当がいらないような中小企業等でも、**最低限のセキュリティを確実に確保**してもらうための**チェックリスト**や手引きを策定

https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/ →



テレワークセキュリティガイドライン (2021年5月 第5版)

2004年12月初版
2006年4月第2版
2013年3月第3版
2018年4月第4版



- ✓ テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針
- ✓ 中小企業を含む全企業を対象
- ✓ システム管理者のほか経営層や利用者(勤務者)を幅広く対象

ガイドラインに記載の内容について、**理解や検討が難しい場合**

中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト) (2022年5月 第3版)

2020年9月初版
2021年5月第2版



中小企業等に向け**最低限のセキュリティを確実に確保**してもらうためのものに限定

【想定読者像】

- ✓ システム管理担当者向け
- ✓ 専任の担当・部門は存在しない
- ✓ 基本IT用語は聞いたことがあるレベル
- ✓ 設定作業は検索しながら実施可能

5	1
4	2
3	3
2	4
1	5

Android/Chatwork/Chromeリモートデスクトップ/Cisco ASA/Cisco Webex Meetings/Dropbox/Exchange Online/Gmail/Google Meet/Googleドライブ/iOS/LANSCOPE エンドポイントマネージャー クラウド版/LINE/macOS/Microsoft Defender/Microsoft OneDrive/Microsoft Teams chat/Microsoft Teams Meeting/Windows/Windows リモートデスクトップ/YAMAHA VPNルーター/Zoom/ウイルスバスター ビジネスセキュリティサービス/たよれーるDMS

よく利用される製品・サービスの**具体的設定の解説資料も準備**

困ったときにやること

- 1 管理部門の担当者へ連絡
*メール: abcdef@xxxx.co.jp
電話: 000-0000-0000
- 2 パソコンをネットワークから切断する
- 3 パソコンの電源をオフ

従業員向けの事項を**携行可能なカード型で準備**

※テレワーク時には、本ハンドブックを携帯すること。

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

→**JPNICから公開(2024.11)** <https://www.nic.ad.jp/ja/rpki/guideline/>

DNSハイジャック

Domain 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

→**ガイドライン公開に向け検討・調整中**

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

→**迷惑メール対策推進協議会から公開(2024.6)** <https://www.dekyo.or.jp/soudan/aspc/report.html>