2022年6月13日
JPNIC総会座談会

インターネットを守るための技術普及を官民で考える

総務省
サイバーセキュリティ統括官室
佐々木将宣

日本政府のサイバーセキュリティ戦略

- **サイバーセキュリティ戦略：**2015年、2018年、2021年
- **一貫した目標：**自由、公正かつ安全なサイバー空間の確保
- **一貫した原則：**
  - 情報の自由な流通
  - 法の支配
  - 開放性
  - 自律性
  - 多様な主体の連携

日本政府のサイバーセキュリティ戦略

- **とある単語の出現回数：**
  - 2015年: 2回
  - 2018年: 6回
  - 2021年: 47回

答え：「信頼性」

何でサイバー空間の信頼性が
こんなに着目されているのか

- サイバー空間の根幹をなすインターネットは「脆弱だけど強靭」な性質を持つネットワーク
- サイバー空間と現実空間の一体化が進展したことによって、そのバランスが大きく変化…

  例）
  - 権威主義的国家の影響力の増大
  - サイバー攻撃による産業活動の停止
  - 戦争とサイバー攻撃
  - Disinformation　　etc.

解決策？

- 分断したり…？　規制したり…？
- 新技術で”インターネット”を変える?

最近の通信当局の国際的なうごき

- Declaration for the Future of the Internet
- G7 Digital Ministerial（Cyber Resilience）
- OECD
  - 通信ネットワークのセキュリティ
  - Domain Name Systemのセキュリティ
  - Routingのセキュリティ

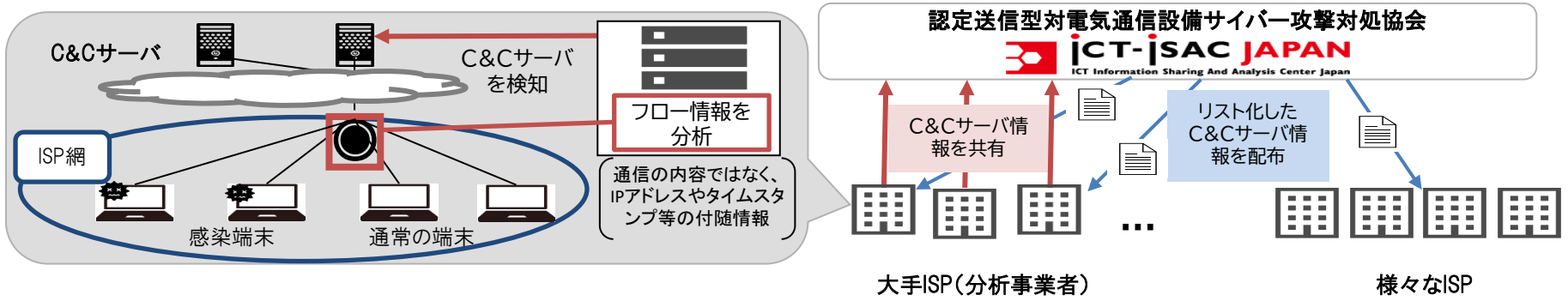
【参考】サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証

■ **大規模化・巧妙化・複雑化するサイバー攻撃・脅威に、電気通信事業者が技術的手法を活用して効率的・積極的に対処できるようにするため、**①フロー情報分析によるC&Cサーバ検知技術の実証、②悪性Webサイトの検知技術・共有手法の実証、**③ネットワークセキュリティ技術の円滑な導入のための実証を実施**。

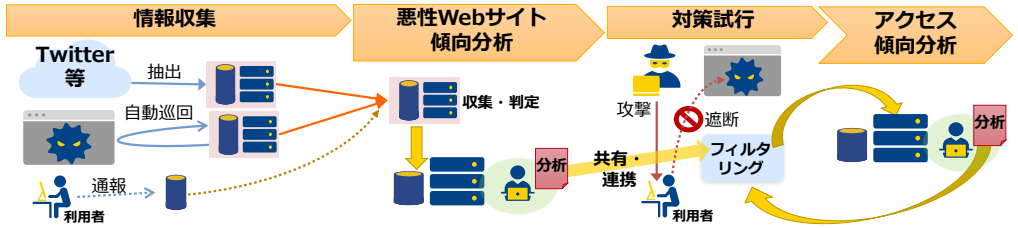
R3年度補正予算：18.0億円の内数

①フロー情報分析によるC&Cサーバ検知技術の実証

※C&C(Command and Control)サーバ：各感染端末（ボット）にサイバー攻撃の指示を出す管理サーバ

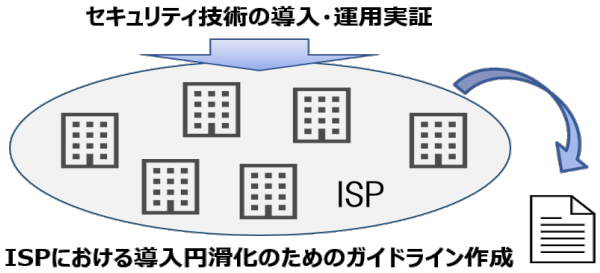


② 悪性Webサイトの検知技術・共有手法の実証



※悪性Webサイト：IDやパスワードなど個人情報の窃取に使用される、正規の金融機関等に偽装したWebサイト（フィッシングサイト） など

③ ネットワークセキュリティ技術の導入実証



※ ネットワークセキュリティ技術：BGPハイジャックに対するRPKI、DNSハイジャックに対するDNSSEC、なりすましメールに対するDMARC 等

ネットワークが出来ること

- インターネットの脆弱な仕様を改善可能な標準化されたネットワークセキュリティ技術：
  - 経路のセキュリティ対策（RPKI etc.）
  - フィッシングサイト対策（DNSSEC etc.）
  - フィッシングメール対策（DMARC etc.）

ネットワークセキュリティ技術の導入実証等

■ 既存のインターネットの一部の脆弱な仕様を悪用するサイバー攻撃には、国際標準化もされている電子認証技術を活用したネットワークセキュリティ技術により、通信ネットワーク側である程度抑え込むことが可能。

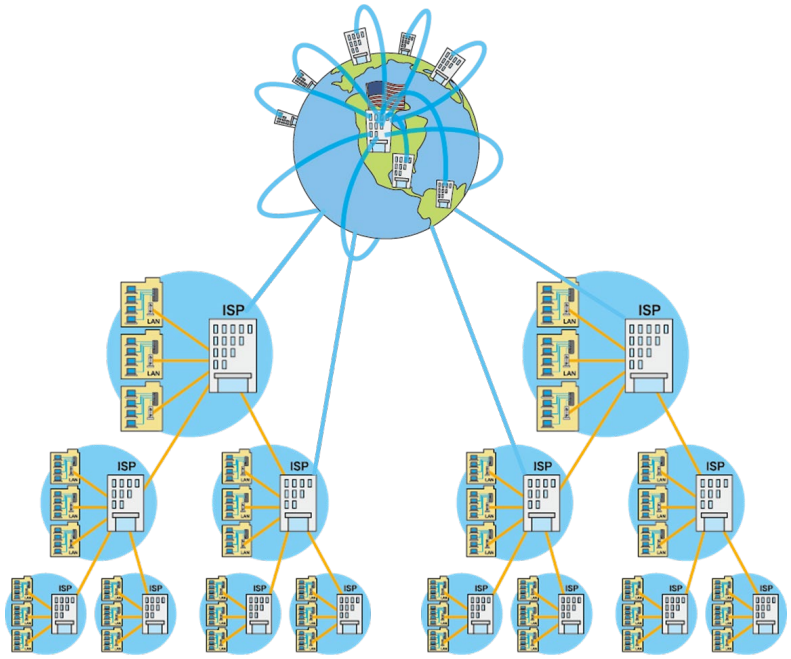
*例: BGPハイジャックに対するRPKI、DNSハイジャックに対するDNSSEC、なりすましメールに対するDMARC等がIETFでRFC化されている。

■ これらの実装には、各ISP等が管理する通信ネットワークに、対応ソフトウェア・ハードウェアを組み込み、継続運用していく必要があるところ、国内においては以下のような事情もあり、いまだ普及率が上がらないのが実情。

- ✓ 通信ネットワークの再構築を要するとともに、導入後は電子認証技術の運用に関する知見や能力が求められる。
- ✓ ユーザが、各ISPを選定する際、対策状況が分からない・判断が難しいなど、ISPが苦労して導入・運用しても競争優位に繋がるか不透明。
- ✓ ネットワークセキュリティ技術の実装に関する特段の規制も存在しない。

■ 本事業では、実際の通信ネットワークなどを実証環境として、ネットワークセキュリティ技術の導入実証を実施。

R3年度補正予算：18.0億円の内数



我が国の様々な通信ネットワークインターネットを構成する

- ネットワークセキュリティ技術の導入実証（想定される対象技術: RPKI, DNSSEC, DMARC等）
- 実証結果に基づき:
  - ISP等における導入円滑化のためのガイドライン作成
  - セキュアな通信ネットワーク・ISP等がユーザから評価される仕組みの在り方検討 等

- インターネットの一部の脆弱な仕様を悪用するサイバー攻撃に対する、通信ネットワーク側での積極的対処を推進
- 自律・分散・協調のもと、我が国サイバー空間の安全性と信頼性の強化とユーザの保護を実現