資料　29－2

電気通信事業者のネットワークの安全・信頼性の確保に向けた取組について

サイバーセキュリティタスクフォース事務局

令和３年３月９日

ネットワークの安全・信頼性確保のためのセキュリティ対策①

【電気通信事業者のネットワークへのサイバー攻撃のリスクの高まり】

- ネットワーク技術の進展により、ソフトウェア化（SDN、仮想技術）等が進むことにより、電気通信事業者のネットワークの柔軟で効率的な運用が可能になる一方で、技術的な脆弱性のリスクも増加。
- また、電気通信事業者は、例えば、５Ｇ構築のための知見などの技術優位性を保持するための技術情報や営業秘密などの経営上の機微情報など、電気通信事業者が有する情報・ノウハウが、安全保障上または経営戦略上の理由から狙われやすい傾向にある。
- さらに、ネットワーク機器の生産・流通プロセスのグローバル化やオープン化に伴う関係者の多様化の進展に伴い、ネットワーク機器内に脆弱性が存在するなどのサプライチェーンリスクも高まりつつある。
- このほか、近年増加しつつある多数のマルウェア感染させたIoT端末（監視カメラ等）を踏み台にして特定のサーバ等に大規模なDDoS攻撃を仕掛ける事例などについて、これまでは端末機器側（ユーザ側）での対策を中心として措置を講じてきたところ（例：NOTICE）。
- しかしながら、今後5Gの進展によりIoT機器の増加が予想される中、現状の端末機器側での対応だけでは難しくなっていくことが予想される。
- したがって、今後は端末機器（IoT機器）側とネットワーク側の両面での対策により、こうしたサイバー攻撃のリスクを低減させることが必要になっていく。

ネットワークの安全・信頼性確保のためのセキュリティ対策②

【電気通信事業者のネットワークの適切かつ積極的なセキュリティ対策の実施の必要性の高まり】

- 国民の生活や経済活動に必要な多くのやりとりが、電気通信事業者が設置しているネットワークを通じて行われるなど、社会全体のデジタル化が進展する中で、サイバー攻撃も複雑化・巧妙化。
- 電気通信事業者のネットワークに対して大規模なサイバー攻撃が発生すれば、大きな被害や社会的な影響を及ぼすリスクが高まっている。実際、電気通信事業者のネットワークがサイバー攻撃の標的となるインシデント事案も発生しているところ。（例：昨年のNTTコム事案など）

➢ **電気通信事業者のネットワークへのサイバー攻撃のリスクや脆弱性に対して適切かつ積極的な対策を講じること**により、**ネットワークの安全・信頼性を確保**し、ユーザが安心してICTを利用できる環境を確保することが必要ではないか。

ネットワークの安全・信頼性確保のためのセキュリティ対策③

【電気通信事業者によるセキュリティ対策の取組の現状把握と検証】

- 電気通信事業者のネットワークへのサイバー攻撃のリスクの高まりに対して、各電気通信事業者がどのような対策を講じているのかやサイバー攻撃による通信障害等のインシデントを十分には把握できていないことから、各事業者の取組が適切であるか否かの検証も困難であるのが現状。

➢ 電気通信事業者のネットワークへのサイバー攻撃のリスクや脆弱性に対して、まずは電気通信事業者によるセキュリティ対策の**取組状況の現状を把握することが必要**ではないか。なお、サイバー攻撃等による電気通信事故の報告制度等との連携強化を図ることも必要ではないか。

- 具体的には、複雑化・巧妙化するサイバー攻撃手法を念頭に、以下のような事項を把握する必要があるのではないか。
  - ✓ **体制面における対策**（社内組織体制、ポリシー等の策定・公開状況、関係機関への報告や情報共有 等）
  - ✓ **業務系設備における対策**（社員等の認証、監視サーバの運用、未使用(運用停止)中の設備の切り離し 等）
  - ✓ **サービス系設備における対策**（加入者の認証、業務系へのアクセス制御 等）

➢ その上で、各電気通信事業者による取組が、高まりつつある**サイバー攻撃リスク対策として適切であるか否かを検証することが必要**ではないか。

ネットワークの安全・信頼性確保のためのセキュリティ対策④

【サプライチェーンリスクの高まり】

- ネットワーク機器の生産・流通プロセスのグローバル化やオープン化に伴う関係者の多様化の進展に伴ってサプライチェーンリスクも高まりつつある。

➢ ネットワーク機器のハード面・ソフト面の脆弱性の技術的な検証手法や検証体制の確立を始めとして、**広く電気通信事業者のネットワークに対するサプライチェーンリスク対策の在り方について検討することが必要**ではないか。

【電気通信事業者による積極的なセキュリティ対策の実施の必要性】

- 電気通信事業者のネットワークへのサイバー攻撃が発生した場合には、多くの被害と多大な影響を及ぼすことになることにかんがみて、これまでの端末機器側における対応に加えて、電気通信事業者においてネットワークにおけるトラフィックの流れ（フロー情報）を把握・分析して、C＆Cサーバ（＝マルウェア感染させたIoT端末に対して、標的とするサーバ等に攻撃通信を送るなどの不正な指令を送るサーバ）を検知できるようにするなど、サイバー攻撃の予兆を捉えて早期に対処できるようにする必要性が高まりつつある。

➢ 電気通信事業者がフロー情報分析を行いC&Cサーバを検知することについて、通信の秘密の規定との関係などの**法的課題や技術的課題を整理・検討することが必要**ではないか。