資料1－3－7

インターネットにおける最近のサイバー攻撃に関して

2017 年 10 月 26 日
横浜国立大学大学院環境情報研究院/横浜国立大学先端科学高等研究院
吉岡　克成

1. サイバー攻撃の多様化

インターネット上のサービスの発展や IoT の進展により、やり取りされる情報やサービスの価値が増大し、それを狙うサイバー攻撃が増加し、かつ、「多様化」している.

攻撃規模の観点では、1Tbpsを超えるような超大規模サービス妨害攻撃やランサムウェアの大流行など、多くの被害者をもたらす大規模な攻撃が発生する一方で、特定の組織、特定の個人を狙ったステルス性の高い高度な標的型攻撃が発生している. また、ばらまき型の攻撃から、攻撃対象の価値に応じて標的型攻撃に移行するようなハイブリッド型の攻撃も存在すると思われる.

攻撃対象機器の観点では、従来のPCやスマートフォンだけでなく、それらをつなぐネットワーク機器や、カメラ、家電といった IoT 機器が攻撃の新たな対象となっている. また、重要インフラや自動車の構成要素のように攻撃による影響が甚大となる重要機器も攻撃対象と成り得る状況である.

攻撃者の観点では、国家等の関与が暗示されるような高度かつ高コストな攻撃から、既存のマルウェア、ツール、サイバー攻撃サービスの組み合わせからなる技術レベルが低い攻撃が存在する.

攻撃手法の観点では、攻撃対象機器の脆弱性や設定不備を突く攻撃、利用者の人間の誤判断を誘導する攻撃、内部者による攻撃、サプライチェーンなど攻撃対象機器やシステムの製造や設置段階を狙う攻撃などがあり、その実現方法も、RAT など人間の攻撃者による定常的な操作を必要とする手動型、ボットネットのように自律的に動作しつつ、人間の攻撃者からの命令に従う半自動型、ワームのように自律的に活動を続ける自動型の攻撃があり、多くの攻撃がこれらの組み合わせで成り立っている. 今後、AI の悪用による攻撃の自動化・高度化も懸念される.

攻撃目的の観点では、ランサムウェア、サービス妨害攻撃による脅迫、ビットコインマイニング、迷惑メール送信、フィッシング、クリック詐欺など、直接的または間接的に利益を求めるものが多く見られる一方、政治的な主張、自己顕示や復讐など個人的な目的などによりサイバー攻撃が行われる場合がある.

サイバー攻撃対策を論じる際には、具体的な対象が定まらなければ有効な対策が検討できない. また、上記のように多様な攻撃の全てに対応することは困難であることから、まず高い優先度で対応すべき問題は何かを議論すべきと考える.

2. 電気通信事業者による対策について

電気通信事業者は、上記のような多様な攻撃に対して有効な対応手段を取り得る可能性のある主体である. 特に IoT が進展する現在、個々の機器のエンドポイントでのセキュリティを一律に向上することが困難となっていることから、ネットワークにおける対策は従来よりも重要となっている. 一方で、効果的な対策を実施するためには、通信内容の把握や利用者との結び付け、それに応じた通信制御を行う必要がある場合があり、これらを実施する能力の悪用は、ユーザプライバシの侵害等に繋がる. そのため、この能力を適切に利用するための技術的、法制度的、運用的な仕組みが必要と考える.