今月の特集

中小企業のセキュリティ対策

ネットワーク乗っ取り対策を

（独立行政法人情報処理推進機構・江島将和）

機器の不具合悪用攻撃の中継拠点に

近年、家庭用ルーターやIoTルーターなどのネットワーク機器について深刻な不具合や設定不備が多数報告されている。

これらの不具合や設定不備が悪用されると、ネットワーク内への侵入に加え、機器が攻撃者に乗っ取られ、ORB（攻撃の中継拠点）として他者への攻撃の踏み台とされる恐れもあるので注意していただきたい。

ネットワーク機器の不具合や設定不備などを悪用したサイバー攻撃の被害として、以下のような影響が生じる恐れがある。

■ORB化と攻撃への加担

ORB化された機器が、通信元の偽装などを目的として、第三者への攻撃の中継点として利用されることにより、結果的に攻撃に加担する恐れがある。特に、ルーターなどの機器からなるボットネット（攻撃者に乗っ取られた複数の機器から構成されるネットワーク）がDDoS（分散型サービス妨害）攻撃に用いられていると注意喚起されている。

■長期潜伏

侵入拠点として保持され、内部偵察や継続的な攻撃の基盤となる恐れがある。有事の際にさらなる侵害が発生するリスクがあるとして欧米の政府機関から注意喚起されている。

■社会的・法的リスク

信用失墜、訴訟、取引停止など、重大な組織的損失につながる恐れがある。

パスワード設定や機器の更新で対処

ORB化に対する主な対策として、以下が考えられる。

ログイン情報が初期設定のままのIoT機器が狙われるイメージ

①推測されにくいパスワードの設定

初期設定のパスワードが推測されやすいものや取扱説明書に記載されているものだと不正侵入が容易になるため、購入時の初期設定は変更することが肝心である。設定方法が分からない場合はメーカーに確認し、セキュリティ設定ができない製品は設定可能な製品に買い替える。

②迅速なパッチ適用・機器の更新

最新のセキュリティ機能を適用するため、定期的なセキュリティ更新プログラムを含むファームウエアのアップデートを心掛けたい。また、メーカーのサポートが終了した製品は、サポートしている後継製品に乗り換えるか、同様の機能を持つ製品に買い替えていただきたい。

③公開設定の最小化

管理インターフェースがインターネット上に公開されていると、攻撃者が容易にアクセスできるため、セキュリティ侵害や脅威の原因となることがある。管理インターフェースは外部公開せず、不要なサービスやポートは停止する。

④定期的な再起動

昨今確認されているルーターへの攻撃は不正なプロセスをメモリーに常駐させるものが多く見られる。ルーター再起動でこれを停止できるので、1～3カ月程度を目安に定期的に再起動する。月初や月末など日にちを決めて確実に実行いただきたい。自宅のルーターが攻撃の入口となり、自分が被害を受けるだけでなく会社や社会インフラにまで害をなす可能性があることを踏まえ、対策の徹底が問われる。

独立行政法人情報処理推進機構（IPA）では、これまでもORB化についての注意喚起を公表している。過去の注意喚起も参考に、必要な対策を行っていただきたい。

また、ネットワーク機器への不正なアクセスを含め、不自然な兆候を認知した場合には、IPA「企業組織向けサイバーセキュリティ相談窓口」または「コンピュータウイルス・不正アクセスに関する届出窓口」にご連絡いただき、サイバー状況把握活動への協力をお願いしたい。

（会議所ニュース令和7年12月21日号（日本商工会議所発行）より転載）

「注意喚起」については
こちらを参照