資料４－３

諸外国におけるサイバーセキュリティ対策の取組事例

令和5年4月

ISPによる取組事例

米国

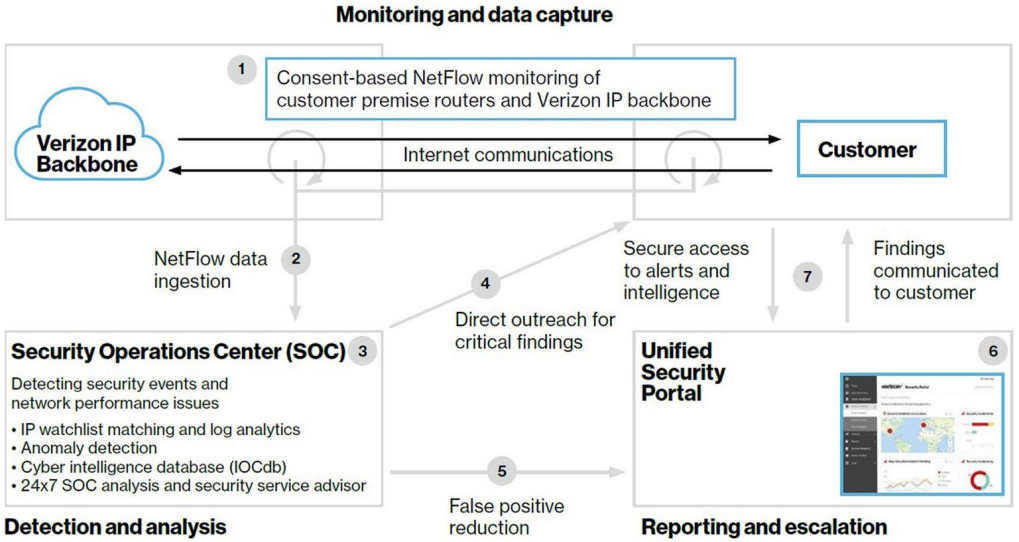
（個別のISPによる対策の実施）

■ 連邦取引委員会（ＦＴＣ）が米国の６大ＩＳＰ（ＡＴ＆Ｔ、ベライゾン、チャーター、コムキャスト、Ｔ-モバイル、グーグルファイバー）を対象に各社の顧客データの取り扱いにつき調査を行ったレポート（２０２１年１０月）には、事業者の慣行としてセキュリティ対策を行っている旨の記載がある。

“調査対象のISPの多くは、詐欺を防止し、ISPのネットワークに接続されている顧客のデバイスのセキュリティを確保するために、消費者の名前、電話番号、位置情報、デバイス情報、永続的識別子、モバイルブロードバンド利用情報などを使用している。例えば、いくつかのISPは、位置情報や消費者のネットワーク上のデバイス数に関する情報を利用して、ボットネットやその他の悪質な行為を検知・防止している。同様に、ISPが、ある顧客のIPアドレス経由で分散型サービス拒否（「DDoS」）攻撃を行っているとの報告を受けたり、検出したりした場合、ISPはその顧客の利用情報、主にその顧客が生成するトラフィック量について調べ、その量が DDoS攻撃の発生を示唆しているかどうかを判断することができる。その場合、ISPは顧客に通知し、または正当な理由があれば、これらの送信をブロックすることがある。”

■ また、ベライゾンやAT＆T等の大手通信事業者では、企業向けに通信のフロー情報を活用した脅威監視サービスを提供している。

- ベライゾンのNetwork Threat Advanced Analyticsでは、顧客構内のルータとベライゾンのIPバックボーンから同意ベースでNetFlowデータを抽出し、自動化された監視機能と、SOCでのアナリストによる分析を組み合わせて提供している。



（出典）ベライゾン社HP

政府機関・官民連携による取組事例

英国

（政府機関による脆弱性スキャン調査の実施）

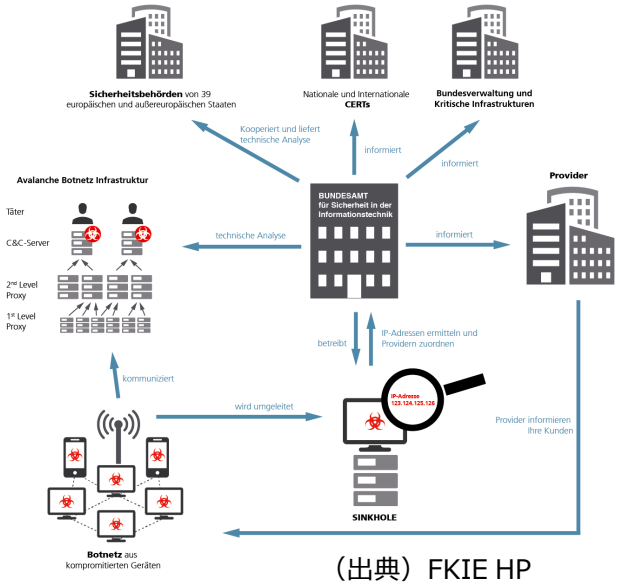
■ NCSC（国家サイバーセキュリティセンター）では、2022年11月から**インターネットに接続されたすべてのデバイスを対象としてアクティブスキャンによる脆弱性調査を実施**している。この活動は、サイバー攻撃に対する英国内の脆弱性・安全性を評価し、インターネットに接続されたシステム所有者が、日々のセキュリティに対する心構えを理解することなどを目的としている。NCSCは、共通する脆弱性、または影響が大きいために特に重要な脆弱性を対象とし、収集したデータを使って、脆弱性の公開後に英国が脆弱性にさらされている状況を概観し、その修復状況を長期的に追跡していくとしている。

ドイツ

（官民連携による感染被害者への通知の取組）

■ FKIE（フラウンホーファー通信・情報処理・人間工学研究所）は、BSI（情報セキュリティ庁）の委託を受けて、「ボットネットの体系的分析」等のプロジェクトを実施しており、**悪意のあるドメインをシンクホールでパッシブ検知し、ボットネットのトラヒックから検出した感染対象をISPに提供し、当該情報を得たISPは、対象ユーザに通知**することができる。

■ 上記について、その技術提供により貢献した、2016年の不正送金マルウェアのボットネット「Avalanche」の摘発に関する公表資料によれば、
－FKIEが開発したシンクホールソフトウェアにより、Avalancheを取り押さえた後も感染しているシステムからの接続要求をシンクホールサーバーに転送することで、被害者特定が可能
－FKIEが開発したプロバイダ情報システムを通じて、2014年以降、ドイツのプロバイダー（450万人以上）には、100万通の通知が届いていた
とされている。



（出典）FKIE HP

産学連携による取組事例

オランダ

（産学連携による効果的な通知手法の研究）

■ 2018年にデルフト大学・横浜国立大学・NICTが、オランダのISPであるKPNの協力を得て、実際の環境を用いてマルウェア（Mirai）に感染したルータやネットワークカメラ等の機器の利用者を特定し、対象者への通知の手法・内容と改善状況に関する実証実験を実施している。その中で、Walled Gardenと呼ばれる、マルウェアに感染した利用者がインターネットにアクセスしようとする際のランディングページに表示を行うなどインターネットアクセスに制限を加える方法で通知を行った場合、メールで通知を行った場合、通知を行わなかった場合で改善状況の比較を行った結果、Walled Gardenによる通知での改善率が最も高く、92%の利用者においてマルウェアが消滅するといった、極めて高い効果が判明した。