IT Topics & News

コンピュータウイルス・不正アクセスの届出事例（2019年上半期）を公開【IPA】

8月28日、独立行政法人情報処理推進機構（略称＝IPA）は、2019年上半期（1月～6月）のコンピュータウイルス・不正アクセスの届出事例を公開した。主な事例として挙げられているものからいくつか概要を紹介する。

①外部組織からの連絡により、届出者（企業）が運用するウェブサイトからのクレジットカード情報の漏えいが発覚。ウェブサーバーを調査したところ、何者かによってECサイトの決済画面が書き換えられ、入力されたクレジットカード情報が第三者に送信される状態となっていた。管理者アカウントのパスワード強度、アクセス制限が脆弱であったことが原因と見られる。

②届出者（企業）の内部のネットワーク負荷が高くなり、調査したところ、300台を超えるパソコン及びサーバー類でウイルス感染を確認した。原因を調査した結果、一時的にグローバルIPアドレスが付与された外部持出し用パソコンが感染源となり、組織内ネットワークへウイルスが拡散したことが判明した。

③届出者（教育機関）のサーバー死活監視で異常が見つかり、状況を確認したところ、サーバーがランサムウェアに感染したことが発覚。組織内に提供しているメールサービスの一部機能が利用できなくなった。感染経路を確認すると、当該サーバーへのリモートデスクトップアクセスを許可していた業務委託先の作業パソコンを経由し、何者かが不正アクセスしていたことが判明した。

なお、届出にはこれらの事例だけでなく、メールアドレスやパスワードの漏えい、ウェブサイトの改ざん、管理者権限アカウントの不正利用、公開用ディレクトリのアクセス権限の変更、VPNサーバーへの不正ログイン、ウイルスの発見・感染、DoS攻撃、顧客情報やアカウント窃取等の情報も複数寄せられている。

被害の多くは、一部推測も含まれるが、修正プログラムの適用やアクセス制限などの基本的な対策を行っていれば防げた可能性が高いものであった。それでも、基本的な対策が行われず、一部被害まで生じている背景には、人手や時間がないといった運用面の不備によって対策の着手が遅れたり、放置されたりしてしまう状況があることが考えられる。

対策を着実に実行するためには、事業計画やシステム構築の検討段階から、セキュリティに関する運用面の設計や計画を行う必要がある。また、すでに運用中のシステムにおいて、事前の計画が十分でなかったとしても、万が一被害が発生した際の損害を想定し、必要な人員確保や運用の見直しが求められる。

古くから知られている、あるいは過去に流行した攻撃手口が世間で話題にならなくなったからと言って、必ずしも同様の攻撃が無くなっているわけではなく、攻撃者らは日々世界中のネットワークをスキャンして、悪用できる脆弱性を見つければ攻撃してくる。すでに知られた攻撃手口での被害は確実に防止すべく、基本的な対策はしっかりと行うべきであろう。