モノづくりプリザーブ
Preservation for Industries in kyoto
モノプリ・ニュース！ 第25号

情報セキュリティ10大脅威 2017

組織編

1位 標的型攻撃による情報流出

企業や民間団体、官公庁等、特定の組織に対して、メールの添付ファイルやウェブサイトを利用してPCにウイルスを感染させ、そのPCを遠隔操作して、別のPCに感染を拡大し、最終的に個人情報や業務上の重要情報を窃取する標的型攻撃による被害が引き続き発生しています。（昨年順位：1位）

2位 ランサムウェアによる被害

ランサムウェアとは、PCやスマートフォンにあるファイルの暗号化や画面のロックを行い、復旧させることと引き替えに金銭を要求する手口に使われるウイルスのことです。（昨年順位：7位）

3位 ウェブサービスからの個人情報の窃取

ウェブサービスの脆弱性を悪用し、ウェブサービス内に登録されている住所や氏名、クレジットカード情報が窃取される事件が引き続き発生しています。数10万件の個人情報等の重要な情報が漏えいする事件も発生しており、ウェブサービスを運営・管理する組織は適切な対応が求められます。（昨年順位：3位）

4位 サービス妨害攻撃によるサービスの停止

攻撃者に乗っ取られたIT機器等から構成されたボットネットにより、企業や民間団体等、組織のウェブサイトや組織の利用しているDNSサーバに大量のアクセスを行うDDoS攻撃が急増しました。攻撃によりウェブサイトやDNSサーバが高負荷状態となり、利用者がアクセスできなくなる被害が発生し、ウェブサイト運営者が対応に追われました。（昨年順位：4位）

5位 内部不正による情報漏えいとそれに伴う業務停止

組織内部の職員や元職員による、情報の不正な持ち出し等の不正行為が起きています。不正に持ち出した情報の紛失により、情報漏えいにつながったケースもあります。（昨年順位：2位）

6位 ウェブサイトの改ざん

コンテンツ管理システム（CMS）等に存在する脆弱性を悪用し、ウェブサイトが改ざんされる事例が今年も発生しています。復旧までウェブサイトを停止することになり、特にオンラインショッピング等を運営している場合、事業上の被害が大きくなります。また、閲覧者がウイルスに感染するように改ざんされた場合、社会的信用を失うことにつながります。（昨年順位：5位）

7位 ウェブサービスへの不正ログイン

昨年確認されたウェブサービスへの不正ログインの多くが、パスワードリスト攻撃によって行われています。

ウェブサービスの利用者がパスワードを使い回している場合、不正ログインが行われる恐れがあります。ウェブサービスの提供者は、不正ログインされないように多要素認証等のセキュリティ機能をウェブサービスの利用者に提供する必要があります。（昨年順位：9位）

8位 IoT機器の脆弱性の顕在化

昨年、自動車や医療機器の脆弱性が一昨年に続いて公表されました。またIoT機器の脆弱性を悪用してボット化することで、インターネット上のサービスやサーバに対して大規模なDDoS攻撃が行われる等、IoT機器の脆弱性に関する脅威が顕在化しています。（昨年順位：ランク外）

9位 攻撃のビジネス化（アンダーグラウンドサービス）

犯罪に使用するためのサービスやツールがアンダーグラウンド市場で取り引きされ、これらを悪用した攻撃が行われています。攻撃に対する専門知識に詳しくない者でもサービスやツールを利用することで、容易に攻撃を行えるため、サービスやツールが公開されると被害が広がる恐れがあります。（昨年順位：ランク外）

10位 インターネットバンキングやクレジットカード情報の不正利用

ウイルス感染やフィッシング詐欺により、インターネットバンキングの認証情報が攻撃者に窃取され、正規の利用者になりすまし、不正送金や不正利用が行われました。（昨年順位：8位）

参考：ＩＰＡ「情報セキュリティ10大脅威2017」
https://www.ipa.go.jp/security/vuln/10threats2017.html

京都府警察本部モノづくりプリザーブ事務局　075-451-9111（内線 5821）