モノづくりプリザーブ
Preservation for Industries in kyoto
モノプリ・ニュース！ 第30号

情報セキュリティ10大脅威 2018

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、特定の組織を狙う、標的型攻撃による攻撃が引き続き発生しています。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られると、別のPCに感染を拡大され、最終的に個人情報や業務上の重要情報が窃取されます。（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。OSの脆弱性を悪用し、感染した端末が接続しているネットワークを経路として感染を拡大させるタイプも登場しています。（昨年順位：2位）

3位 ビジネスメール詐欺

「ビジネスメール詐欺」（Business E-mail Compromise：BEC）は、巧妙に細工したメールのやりとりによって企業の担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口です。詐欺行為の準備としてウイルス等を悪用し、企業内の従業員の情報が窃取されることもあります。これまでは主に海外の組織が被害に遭ってきましたが、近年では海外取引をしている国内企業でも被害が確認されています。（昨年順位：ランク外）

4位 脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加

脆弱性対策情報の公開は、脆弱性の脅威や対策情報を広く呼びかけられるメリットがある一方で、その情報を攻撃者に悪用され、対策前のシステムを狙う攻撃が行われています。また、近年では脆弱性情報の公開後、その脆弱性を悪用した攻撃が本格化するまでの時間が短くなっている傾向があります。（昨年順位：ランク外）

5位 セキュリティ人材の不足

セキュリティ上の脅威は今後さらに増大するだけでなく、新たな脅威も発生し続けていくことが予想されます。これらの脅威に対応するためには、セキュリティの知識や技術を有するセキュリティ人材が欠かせませんが、圧倒的に不足しており、問題視されています。（昨年順位：ランク外）

6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が悪用され、ウェブサービス内に登録されている個人情報やクレジットカード情報等の重要な情報を窃取される被害が引き続き発生しています。（昨年順位：3位）

7位 IoT機器の脆弱性の顕在化

IoT機器の脆弱性を悪用しウイルスに感染させることで、インターネット上のサービスやサーバに対して、大規模な分散型サービス妨害（DDoS）攻撃が行われる等の被害が確認されています。また、国内で発売されているIoT製品において脆弱性が発見されており、機器を乗っ取られる、または撮影機能等を悪用して個人情報を窃取されるといった危険性があることが公表されています。（昨年順位：8位）

8位 内部不正による情報漏えい

組織内部の職員や元職員により、私怨や金銭目的等の個人的な利益享受のため組織の情報が不正に持ち出されています。また、組織の情報持ち出しのルールを守らずに不正に情報を持ち出し、さらにその情報を紛失し、情報漏えいにつながったケースもあります。（昨年順位：5位）

9位 サービス妨害攻撃によるサービスの停止

ウイルスに感染し、ボットネット化した機器からDDoS攻撃が行われ、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確認されています。（昨年順位：4位）

10位 犯罪のビジネス化（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：9位）

出典：ＩＰＡ（独立行政法人情報処理推進機構）「情報セキュリティ10大脅威2018」
https://www.ipa.go.jp/security/vuln/10threats2018.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）