別紙

「情報セキュリティ 10 大脅威 2015」の概要

各脅威の概要、対象、および順位変動は下記の通りです。なお、脅威の対象欄の上段は一次被害対象者、下段は被害が派生した場合の二次被害対象者を記載しています。

1 位：オンラインバンキングやクレジットカード情報の不正利用	脅威の対象	順位の変動
ウイルスやフィッシング詐欺により、オンラインバンキングの認証情報やクレジットカード情報が窃取され、本人になりすまして不正に利用や送金が行われた。また、2014 年は個人だけでなく法人口座からの不正送金被害が急増したことが特徴的だった。 [主な対策] ウイルス対策ソフトの導入、ソフトウェアの更新、ワンタイムパスワードの利用	 なし	UP 昨年：5 位
2 位：内部不正による情報漏えい	**脅威の対象**	**順位の変動**
企業の従業員が内部情報を窃取し、第三者に販売した事件が社会的な問題となった。内部の人間が悪意を持つと、正当な権限を用いて情報を窃取できるため、情報の重要度に応じたアクセス権限の設定や離職者のアクセス権の抹消等、厳重な管理と監視を継続的に行う必要がある。 [主な対策] セキュリティポリシー策定、啓蒙・教育、権限分離やアクセス制限、ログの監視	 	UP 昨年：11 位
3 位：標的型攻撃による諜報活動	**脅威の対象**	**順位の変動**
PC をウイルスに感染させ、外部から PC を遠隔操作して内部情報を窃取する、「標的型攻撃」と呼ばれる諜報活動を受ける政府機関や民間企業が後を絶たない。2014 年は、取引先や関連会社を踏み台にして最終的な標的組織を狙う等、手口の巧妙化が見られた。 [主な対策] 啓蒙・教育、ウイルス対策ソフトの導入、ソフトウェアの更新、権限分離やアクセス制限、ログの監視	 なし	DOWN 昨年：1 位
4 位：ウェブサービスへの不正ログイン	**脅威の対象**	**順位の変動**
脆弱なウェブサービスから窃取した ID とパスワードで別のウェブサービスに不正にログインし、利用される被害が多発した。原因の 1 つに利用者のパスワードの使い回しがある。多くのパスワードを覚えられないことがその理由で、適切なパスワード管理が求められている。 [主な対策] 推測されにくいパスワードの設定、サービスごとに異なるパスワードの設定	 なし	DOWN 昨年：2 位
5 位：ウェブサービスからの顧客情報の窃取	**脅威の対象**	**順位の変動**
ウェブサービスから氏名や住所などの顧客情報を窃取される事件が継続的に発生した。窃取された情報に ID とパスワードやクレジットカード情報が含まれる場合、影響が広範囲に及ぶだけでなく、金銭被害など深刻なものとなる。 [主な対策] ウイルス対策ソフトの導入、ソフトウェアの更新、脆弱性のないウェブサービスの開発、設定の確認（不要なサービスの無効化）	 	DOWN 昨年：4 位

6 位： ハッカー集団によるサイバーテロ	脅威の対象	順位の変動
在米の日系企業が執拗な攻撃を受け、詳細は不明だが情報漏えいやサービス停止などの被害に遭うサイバーテロが社会的な問題となった。また、2013 年には韓国でシステムを破壊され、業務停止により大きな損失を受ける事件も発生した。 [主な対策] ウイルス対策ソフトの導入、ソフトウェアの更新、権限分離やアクセス制限、ログの監視、バックアップ	 なし	UP 昨年：ランク外
7 位：ウェブサイトの改ざん	**脅威の対象**	**順位の変動**
企業・組織のウェブサイトが、閲覧するだけでウイルスに感染させるように改ざんされる事例が多く発生した。改ざんされたウェブサイトは一時停止による金銭的被害を余儀なくされるだけでなく、閲覧者に被害が及ぶこともある。 [主な対策] ウイルス対策ソフトの導入、ソフトウェアの更新、脆弱性のないウェブサービスの開発、設定の確認（不要なサービスの無効化）	 	DOWN 昨年：3 位
8 位：インターネット基盤技術の悪用	**脅威の対象**	**順位の変動**
DNS [*3] や電子証明書 [*4] などインターネットの基盤となる技術は、悪用されていないことを前提に成り立っている。これらの技術を悪用してウイルス感染サイトへ誘導するなどの攻撃が発生した。この攻撃は、利用者側では検知することが難しいため、インターネット提供側の対策が強く求められる。 [主な対策] 手続き申請の真偽の確認強化、サービスの監視強化、ウイルス対策ソフトの導入、ソフトウェアの更新	 	UP 昨年：ランク外
9 位：脆弱性公表に伴う攻撃の発生	**脅威の対象**	**順位の変動**
2014 年は Apache Struts、Open SSL、bash など、悪用される可能性が高いソフトウェアの脆弱性が相次ぎ、攻撃が発生した。システム管理者やユーザーは、製品の利用状況や攻撃発生の有無など脆弱性の影響度に応じて迅速に対策する必要がある。 [主な対策] ソフトウェアの更新、運用体制の強化	 なし	UP 昨年：ランク外
10 位：悪意のあるスマートフォンアプリ	**脅威の対象**	**順位の変動**
便利な機能があるように見せかけた悪意あるスマートフォンアプリにより、端末内の電話帳等の情報が知らない間に窃取されてしまう。窃取された情報がスパムメールや詐欺に悪用され、友人や知人にまで被害が及ぶ場合もある。 [主な対策] 信頼できるストアの利用、インストール時のアプリの権限確認、ウイルス対策ソフトの導入	 なし	DOWN 昨年：6 位

(*3) Domain Name System:インターネット上のドメイン名やホスト名と IP アドレスの対応を管理するシステム
(*4) ウェブサイトやソフトウェアが真正であることを示す電子的な証明書

【脅威の対象の凡例】

個人

家庭等でインターネットを利用するユーザー

企業・組織

企業および政府機関・公共団体などの組織全体、システム管理者、ユーザー