特集　知っておきたい　金融サイバーセキュリティの基礎知識

①金融機関を狙うサイバー攻撃の現状と対策

サイバー攻撃の脅威が高まるなか、社会インフラである金融機関も標的になっており、二〇二四年には金融庁からガイドラインが公表されるなど、職員一人ひとりの高いリテラシーが求められている。本稿では、金融機関職員が知っておきたい基礎知識と関連用語を紹介する。

株式会社NTTデータ経営研究所
マネージングディレクター
金融政策コンサルティングユニット長
大野 博堂

1993年早稲田大学卒業後、NTTデータ通信に入社。デリバティブ取引管理システムなどの企画に従事。2000年、大蔵省大臣官房調査企画課、総合政策課にてマクロ経済分析に従事。2006年からNTTデータ経営研究所にて政府、金融機関への調査研究、コンサルティングを担当。著書多数。毎年70回程度各地で講演。

1 サイバー攻撃とは

(1) サイバー攻撃の概要と個人・企業への影響

サイバー攻撃とは、インターネットや通信回線などを通じて、個人や企業、団体が保有もしくは使用するIT機器やシステムを対象に行われる悪意のある外部からの攻撃を指します。

個人の場合は、SNSやメールを通じて特定のURLをクリックすることで、敵が立ち上げた偽のホームページに誘導され、自身のIDやパスワードが盗み取られ、インターネットバンキングなどから不正に送金や出金がなされるケースが後を絶ちません。また、クリックしただけでウイルスに感染し、自身が利用するIT機器が乗っ取られたり、IT機器に保存していた個人情報が窃取されるという手口も増加傾向をたどっています。

同様に、企業が狙われるケースも増加しています。企業自身が敵のターゲットとなり、対外接続系のシステムに不正侵入されたりするケースのほか、企業が連携する他社、例えば業務やシステムの委託先に攻撃が仕掛けられ、当該企業を経由して自社のシステム環境が攻撃されたり、障害を発生させられてしまうケースも増加しています。

また、最近は、外部からインターネットや通信回線を経由することなく、直接、内部者や外部からの指示を得て持ち込まれたUSBなどを使い、いわゆる**マルウェア**（九頁～「関連用語」※1参照）などを直接にIT機器やシステムに感染させる手法もみられます。

このように、これまでにな