日本の防衛オピニオン　第10回　防衛問題特別取材班

拡大するサイバーテロの脅威に備えよ

官公庁や民間企業、そして個人まで、あらゆる対象がサイバー攻撃の標的となり、毎日のように被害が発生している。セキュリティーの強化が加速しているものの、国境を越えて襲う脅威に対策は後手となっているのが現状だ。サイバー攻撃をめぐっては、個人情報や技術などが盗まれるリスクが懸念されてきた。だが、これらに加えて近年、国家の安全保障を根幹から脅かし、人命に直結しかねないような「サイバーテロ」の危機も現実のものとなっている。手口の高度・複雑化が止まらない攻撃に打つ手はあるのか。

極小のコストで「壊滅的打撃」攻撃の拡大と深化が止まらない

「極小のコストで社会に大打撃を与えられる。例えば、小学生でも知識さえあれば大規模な『テロ』を実行できる」。

ハイテク犯罪に詳しい公安関係者は、サイバー攻撃の脅威についてこう説明する。

サイバーテロは、インターネット上に構築された情報インフラなどを攻撃することにより、大規模で深刻な影響を与えるーと定義される。過去には、特定のサイトにアクセスを集中させて負荷を加え、閲覧を不可能にする攻撃などが知られてきた。近年、社会機能に壊滅的な打撃を与えかねない、より危険で、悪質な攻撃が増加しつつある。

背景には、社会の根幹を支える重要インフラに、コンピューターを始めとする情報技術が深く根ざしつつある現状がある。昨年、米国のFCAUS（旧クライスラー）が車両140万台をリコール（回収・無償修理）すると発表した。理由は「ハッキング対策」。きっかけは、著名ハッカーが、ネットに接続されたクライスラー車を不正アクセスで乗っ取る実験を動画で公開したことだったという。実験では車に搭載されたコンピューターに侵入し、外部からエンジンを切ったり、ワイパーを動かしたりした。さらに遠隔操作でハンドルを動かし、スピードを意のままに操ることも可能とされた。

サイバーテロの疑いがある事件は、ほかにも世界各地で確認されている。ウクライナで昨年発生した大規模停電について、米国の情報当局は、サイバー攻撃で引き起こされたものと分析しているとされる。攻撃者は電力管理システムの基幹に不正アクセスして電力供給を遮断。バックアップシステムも使用できないようにしていたという。このニュースを報じた米紙は、情報当局が、クリミア併合などでウクライナと対立するロシア軍による関与を疑っていると伝えた。

「潜入」と「拡大」がポイント標的に関係なく手口の基本同じ

重要インフラがサイバー攻撃にさらされた例はほかにもある。イランの核開発施設の制御系システムがウイルス感染した事件はよく知られている。米国では鉄道の信号管理システムが制御不能となる事態が発生した。フランスの国営放送が攻撃されて放送不能に陥ったり、米国の医療機関のシステムがダウンして患者の治療ができなくなったりした事案も起きた。

攻撃者は高度な技術を駆使して攻撃を実行しているようにも思えるが、サイバーセキュリティー関係者は「標的の政治的・社会的位置づけにかかわらず、国内外で発生する攻撃の経緯や構図は、基本的に類似している」と指摘する。

《「貴社の端末が外部と接続し、不審な通信をしている。サイバー攻撃の恐れがあります」。ある日、ネット上を監視する政府関係機関から、A社に通報があった。確認すると、社内のパソコンがウイルスに感染。基幹サーバーに侵入された恐れがあり、間もなく、重要な顧客情報が大量流出したことが分かった》

これは実際に日本国内で発生した被害で、「標的型攻撃」と総称される攻撃の一例だ。サーバーは、ホームページ運用やデータ蓄積などに使うコンピューターやプログラムの全体を指し、インターネット上では不可欠な存在。攻撃者は標的となる組織の基幹システムを乗っ取ってコントロールし、情報の窃取などを狙う。被害者は攻撃に一切気付かず、ネット上の動向を監視する政府当局や警察当局の指摘を受けて初めて、事態を把握することがほとんどだ。被害のきっかけは一体、何だったのか。時間をさかのぼる。

《A社に勤務するBさん。出社すると最初の仕事は毎日届く大量のメールチェックだ。この日は共同事業を進める得意先からメールが届いていた。表題は『プロジェクトの進捗状況』。疑問を感じることもなく添付ファイルを開いた…》

Bさんが何気なく開いたファイルは、実は不正プログラムだった。この時点で端末はウイルスに感染し、外部からの遠隔操作が始まる。攻撃者は別の端末にも侵入してウイルスを拡散。基幹サーバーにも侵入して、社内の動向を監視した。パスワードを次々に盗み、幹部のみが閲覧可能な情報にアクセスし、同社が保有する個人情報などを難なく持ち出した。

写真＝自衛隊サイバー防衛隊が平成26年3月に編成され、防衛省のサイバーディフェンス態勢は強化されつつあるが、防衛産業だけでなく、個人を含めた民間側のサイバーセキュリティー対策が一層必要だ。

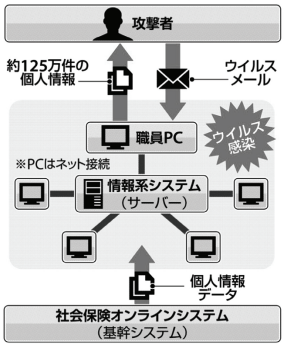
写真＝日本中に衝撃が走った日本年金機構の個人情報流出事件。職員の端末へウィルス・メールを送り、添付ファイルを開いたことにより125万件もの個人情報の流出を許した。

激化する〝入り口〟の攻防啓発進むも拡大する被害

標的型攻撃のポイントは、標的の内部にひそかに侵入し、長期間潜伏して、浸食範囲を拡大することだ。この〝入り口〟を切り開こうと、攻撃者は先に述べた「メールの送受信」など、日常業務で必要な作業を狙っている。

昨年、日本年金機構から125万件もの個人情報が流出した事件でも、職員の端末が標的型メール攻撃でウイルスに感染したことが被害のはじまりだった。機構側は不審なメールの受信や、外部との不審な通信を早期に把握していたが、連続した攻撃に十分な対応を取ることができず、大量の情報流出を許した。

日本年金機構の情報流出の構図



警察当局の統計では、2015年の一年間に標的型メールによる国内企業などへの攻撃は過去最多の3828件も把握された。13年は492件、14年は1723件で急増が続いている。警察関係者は「把握された攻撃は氷山の一角」と分析する。

メールを介した攻撃以外にも、業務で使用されるウェブサイトを改竄してウイルスに感染させる手口や、端末のセキュリティーを高めるソフトウエア更新サイトに罠を仕掛け、不正プログラムがダウンロードされる事態まで発生している。

サイバー攻撃の脅威が広く認識される中、ウイルス検知やネット接続の監視などは強化されている。それでも、被害が後を絶たない理由について、セキュリティー関係者はこう指摘する。

「メールの送受信やウェブサイトの閲覧は結局、人間が行う。人間である以上、すべてのリスクを回避しミスしないのは不可能だ」

巧妙化で続く「イタチごっこ」被害前提に〝致命傷、防衛策を

セキュリティー会社などの分析によると、攻撃者は研究を重ね、不正アクセスの監視をすり抜ける偽装や、ウイルスの高度化を進めている。国境を容易に飛び越えるネット上で、日本を狙った攻撃でも歓迎されない〝進化〟は加速している。

セキュリティー関係者によると、かつて標的型メールの文章は多くが雑で、いい加減な日本語だった。ところが、最近では表題や内容も正確で、標的をあらかじめ調査したような精巧なものが増えている。特定部署にいる政府の個人を狙い、関係のある実在の人物を装って標的型メールが送付された事例もある。

捜査当局による攻撃者の追跡も事実上不可能とされる。無数のサーバーが外部に乗っ取られていることが国内外で確認されている。攻撃者は支配した複数のサーバーを経由し、匿名性を保ちながら遠隔操作を実行。盗んだ情報の蓄積にも悪用している。仮にサーバーを特定しても、サーバーが所在する現地当局の協力が得られないケースが多いという。

それでは、被害を防ぐ手立てはないのか。セキュリティー関係者は「侵入を完全に防ぐのは極めて難しい。侵入を許したとしても、被害を可能な限り軽減するシステムの構築が有効だ」と指摘する。

例えば、攻撃の「入り口」を守るのは基本的な対策となる。日本年金機構をめぐる情報流出事件で、標的型メールに添付されたウイルスは「exe（エグゼ）」というファイル形式だった。このファイル形式は何らかのプログラムを実行するもので、メールで送受信する必要性は低く、ウイルスの可能性が高い。最近では、ファイル形式を文章ファイルなどに偽装する手口が増えており、形式の詳細を確認することはもちろん、ファイルを不用意に開かないことが重要だ。

外部と接続した脆弱性のある端末を、重要な機密などが含まれた基幹システムから遠ざけることも不可欠といえる。警察当局では、ネットに接続する端末と、捜査情報や個人情報などが含まれる業務用端末を完全に分け、ウイルス感染の恐れがあるUSBメモリなどの使用も制限している。

情報当局が関わった疑いがある高度なサイバー攻撃も発生している。サイバーテロの威力は、1990年の湾岸戦争に前後して認識され、各国の情報機関で技術体系が確立していったとされる。米当局は、サイバー攻撃によるスパイ行為に関与したとして、中国軍当局者らを起訴した。北朝鮮の朝鮮労働党委員長、金正恩の暗殺を描いたコメディー映画を製作した米企業は、北朝鮮が関与したとみられるサイバー攻撃を受けた。日本でも、ミサイルシステムなど防衛に関連する機関が不正アクセスを受け、情報が流出した可能性が指摘されている。

警察関係者は、「ネット上の技術は日進月歩で、攻撃者が圧倒的に有利だ。それでも情報技術は社会で欠かせないものになっており、セキュリティーをめぐる厳しい攻防が続くことになる」と話した。（敬称略）