重　要

サイバー攻撃関する内容

緊急報告書

IEAS 管制センター統括グループ

グループ統括：白原　信吾

世界を震撼させたソニーへのサイバー攻撃だが、他人事と考えていたら間違いなのだ。次の被害者になるのは、あなたの会社や、あなた自身かもしれない。攻撃したとされる「アノニマス」（匿名の意味）というハッカー集団の名が知れ渡ったが、まさに、名もない個人がテロリストになることができる時代になった。従来のサイバー攻撃は不特定多数に向けた愉快犯的なものが多かったが、今や特定の企業や個人を「標的」にして攻撃することが当たり前になっている。ウイルスソフトをパソコンに入れれば大丈夫という時代ではなく、組織を挙げてサイバー攻撃に取り組まなければならない。さらには、サイバー攻撃はテロからWar（戦争）へ、という様相を呈している。国防という観点から、国に求められる役割もこれまで以上に大きい。「アルカイダなんてもう古いという時代がくる」―。ある情報セキュリティ会社の幹部は言う。サイバー空間への窓口であるパソコンはタダ同然で手に入るようになり、サイバー空間の交通網は、この十数年で田舎のあぜ道が高速道路になったほど整備された。そこでは、コンピュータについて特別な知識がなくても、あるサイトの存在を知っていれば誰でも簡単にサイバーテロを依頼することができる。それが「サイバー攻撃代行サイト」だ。「ライバル企業に営業妨害を加えたい」、そう思った企業や個人が手数料を支払うことで、代行業者が相手のウェブサイトなどをダウンさせ、サービスを停止に追い込んでくれる時代も遠くないのである。代行サイトのほとんどはロシア語か中国語ある。サイバーディフェンス研究所（東京都中央区）による報告では、サイバー攻撃代行サイトの実体は次のようになる。業者に依頼する前に準備するものが 3 つ。(1) インターネットを通じてリアルタイムに業者と連絡を取り合うためのアプリケーションソフト、(2) インターネット決済サービスのアカウント、(3) 彼らと意思疎通するための英語力。代行サイトを見つけることさえできれば、手順はいたってシンプル。(1) を介して業者に攻撃相手を伝えたうえで、攻撃方法、攻撃期間などを交渉し、(2) を通じて手数料を支払えば、依頼は完了。あるロシア語サイトの価格は 1 時間あたり 5～6 ドル。500 円玉 1 つで、攻撃できるのだ。業者は依頼主の希望に応じてオーダーメードで相手にサイバー攻撃を加えてくれる。攻撃終了後にはその結果を報告までしてくれる。お隣の韓国でもサイバー攻撃が浸透。2009 年にはライバル企業の営業妨害の依頼などを受け、60 あまりのサイトをダウンさせたサイバー攻撃代行業者が摘発された報告がある。

「標的型」という新手の攻撃法

容易にサイバー攻撃を仕掛けられる環境になると同時に、攻撃の質も進化している。情報窃取を目的として特定の個人や組織を狙った「標的型サイバー攻撃」がある。経済産業省によると、07 年から 11 年までの 4 年間で、標的型攻撃が 6 倍にも増加した報告がある。IEAS 調査・分析グループは「サイバー攻撃の性質が変わった」と指摘する。面白半分に不特定多数のウェブサイトなどを狙ったものから、ある目的を実現するために意図的に特定の重要なシステムや情報などを狙うようになった。しかも、技術力が相当高いことが分析で分かる。不特定多数の攻撃のときは、風邪のようなものだからマスクや手洗いで予防するようにパソコンにウイルスソフトを入れるレベルで良かったが、標的型となると、特定の個人にだけ感染する、新型インフルエンザの進化版のようなもので付けているマスクの材質まで調べあげてそれを通り抜けるウイルスだと思って頂きたい。進化の背景には、通信回線が広がり大量のデータを送受信出来るよ

うになった環境的側面もあるが、「情報システムが社会全体に、より大きな影響を与えるようになり、攻撃対象としての価値が上がってきた」ことも要因として挙げられる。標的型攻撃の一例はこうだ。まず社外で配布された資料やウェブサイト上で公開している情報から、役員や総務部署のメールアドレスを手に入れる。このアドレスに悪意を持った者が不正プログラムを組み込んだファイルを添付してメールを送りつける。以前流行した「I Love you メール」のような怪しいメールであれば添付ファイルを開くこともないだろうが、送信者は本物のメールであるかのように装う。例えば送信元のメールアドレスに「go.jp」や「dpj.or.jp」を利用して、日本政府や民主党からのメールのように詐称する。表題や本文も東日本大震災や福島原発事故など興味を誘う時事ネタであったり、受信者の組織や業務に関係するテーマであったりする。情報処理推進機構（IPA）の『情報セキュリティ白書 2011』によると、標的型攻撃の送信元メールアドレスの約 5 割が「go.jp」、約 1 割が政党や団体、またメールテーマも 5 割が国際会議や法令改正、役員人事異動などのイベント、3 割が国際情勢や製品事故などニュース・注意喚起、2 割が政府部局内などの報告がある。

実際に送信された標的型サイバー攻撃メール。上は民主党から、下は内閣府から送信されたように装っている。

上の写真は実際に送信された標的型サイバー攻撃メールだ。あくまで推測だが、悪意を持った送信者は、民主党の政策調査会関係者や浜岡原発停止に関連する情報を必要とする人が、思わず開いてしまうような内容のメール本文を作成のうえ、不正プログラムが組み込まれたファイルを添付して送信したと思われます。添付の文書が「総理に出した紙」や「浜岡原子力発電所停止及び中部地域電力需給対策について」とあれば関係者は開かずにはいられないだろう。その裏側で自分のパソコンが不正プログラムに感染したこ

となど気づかないのです。このプログラムは、外部から感染したパソコンに不正に侵入することを容易にし、やがて管理者権限が奪われて、内部情報が外部に送信される。また不正プログラムが遠隔操作を可能にするものであれば、オフにしていたはずのカメラやマイクを知らないうちにオンにし、盗撮や盗聴することも可能なのだ。実際に 09 年にはダライ・ラマの亡命政府事務所のパソコンが感染し、事務所内の会話が外部に漏れるという盗聴事件が起きた。ここまでくると従来のウイルスメールとは全く違うことが理解できる。武器を購入し、お金をかけて多数のテロリストを養成しなくても、サイバー攻撃で標的に甚大な被害を与えることができる。冒頭の「アルカイダは古い」の意味はここにある。サイバー攻撃を仕掛ける者を一般的に「ハッカー」と呼ぶことが多いが、IEAS 情報セキュリティグループは次の 5 つに分類する。（1）システムの脆弱性を見つけ内部に侵入することで高い技術力を見せつけるパイオニア、（2）脆弱性をつく攻撃が誰でもできるようにするツールの開発者、（3）インターネットを通じて特定の主張を実現しようとするネット市民運動家、（4）金銭目的で個人情報や産業情報を窃取する犯罪組織、（5）各国のサイバー戦部隊など職業人ハッカー。正体不明のハッカー集団企業もこれまでの対策は通用しない。11 年 4 月に発生したソニーグループ全体で 1 億件にものぼる一連の個人情報流出事件がそうだ。きっかけは、不特定多数のメンバーで構成される謎の国際ハッカー集団「アノニマス」（匿名の意味）によるサイバー攻撃である。彼らを「ネット上での表現の自由を守る」ことを主な目的とした（3）に分類されるハッカーで、それまでも政府や企業を徹底的に攻撃してきたデータもある。ハッカーたちを怒らせたのは、ソニーのゲーム機プレイステーション 3 の改造プログラムをウェブサイトで公開した米国人ハッカーを提訴し、さらに同サイトにアクセスしたユーザー情報の開示まで裁判所に請求するなどソニーが強硬な手段をとった事が要因である。ネット上の自由が侵害されるととらえたアノニマスは、11 年 4 月 3 日にブログ上で「オペレーション・ソニー」（ソニー作戦）と称して、ソニーに対してサイバー攻撃をしかけると宣戦布告した。ソニーが運営するウェブサイトは接続不能となり、その後登場するのが（4）のタイプに分類される別のハッカー集団「ラルズセック」。ソニーのネットワークシステムの脆弱性をついて不正にデータベースにアクセスし、大量の個人情報を盗み取ったとみられる。彼らはその後も任天堂、米連邦捜査局（FBI）、米中央情報局（CIA）などにもサイバー攻撃を加え、6 月 26 日、同集団のウェブサイトで 50 日間におよぶ一連のサイバー攻撃の終了と組織の解散が宣言された。ソニーは、この事件に関して 11 年度だけで 140 億円の費用を計上した。サイバー攻撃の標的になって個人情報が流出すれば、賠償や対策のため多額の出費を余儀なくされるだけでなく、企業イメージが低下するなど、その損害は甚大なものとなるからである。一部にはソニー側の脆弱性を問題視する声もあるが、どの企業でも「第 2 のソニー」になる可能があることを強く認識する必要がある。

イラン政府を震え上がらせた攻撃

サイバー攻撃の標的は企業だけにとどまらないのが現実なのだ。まるで SF 小説さながらに国家を狙ったと思われるサイバー攻撃が、すでにイランの核関連施設で起きている。これは「Stuxnet（スタックスネット）」と呼ばれる不正プログラムがウラン濃縮施設のコンピュータを攻撃し、遠心分離機をコントロール

する制御システムのプログラムを書き換え、回転数を意図的に変えるというものだった。核兵器に利用する濃縮ウランを製造できなくなり、実際に「イランの核開発を数年遅らせた」（クリントン米国務長官）と米ニューヨーク・タイムズ紙は報じている。このスタックスネットは、これまでのサイバー攻撃の常識を覆した。通常、核関連施設や重要インフラなどは外部と遮断された閉鎖的なネットワークで構築されている。しかし、今回は USB を媒体として巧みに何人もの人間を介して感染が拡大した。最終的には核関連施設内のコンピュータにまで侵入していった。またこの不正プログラムは、独シーメンス社製のある周波数変換器が特定の周波数で遠心分離機を制御するときのみに作動するように作成されていた。発見当初からスタックスネットの解析をしてきたセキュリティソフト会社シマンテックの濵田譲治シニアセキュリティレスポンスマネージャは「開発には数千万円のコストと 10 人ほどの高度な技術者が半年以上の期間をかけなければ不可能と思われる」と報告している。作成したのは、米国やイスラエルなどではないかと報道されているが、詳細は不明である。「風邪」レベルだったコンピュータウイルスは、新型インフルエンザを経て生物兵器にまで進化している。攻撃手段の質が高くなっている上に、それを簡単に手に入れることができてしまう時代に入っており、量的にも拡大している。「今まで狙われなかったから大丈夫」「狙われるような情報はない」という過信はもはや幻想なのだ。