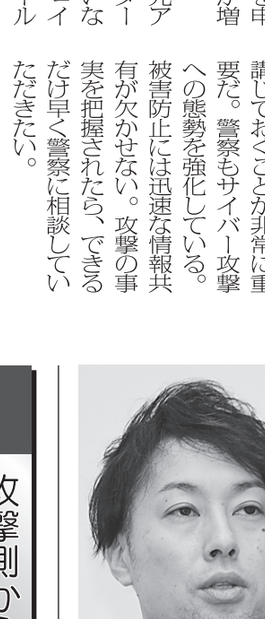
NIKKEI BUSINESS DAILY FORUM
日経産業新聞
フォーラム2015

サイバー攻撃 標的型にどう立ち向かうか

企業や団体から機密情報を盗みだす標的型サイバー攻撃が猛威を振るっている。無害の質問者を装い、メールの開封を促す「やり取り型」など、その手口は巧妙化するばかりだ。折しもサイバーセキュリティ基本法が成立、政府は「サイバーセキュリティ戦略本部」を発足させる。安全なネット社会を築くために、企業や行政の対策はどうあるべきか。日経産業新聞フォーラム2015「サイバー攻撃最前線」の模様をリポートする。

基調講演
サイバー・エスピオナージの情勢と警察の対応

警察庁警備局警備企画課 サイバー攻撃対策官　河原 淳平氏



迅速な情報共有が必要
標的型の手口は巧妙化

インターネットの普及に伴い、サイバー犯罪が多発している。政府機関や企業から機密情報を盗み取るサイバー・エスピオナージ「電子的諜報（ちょうほう）活動」、そして政府機関や重要インフラ事業者らの基幹システムを機能不全に陥れ、社会の機能をまひさせてしまうサイバーテロが世界的規模で頻発している。

その中でも、標的型メール攻撃が数多く報告されている。職員の知り合いや仕事上の関係者を装って、市販のウイルス対策ソフトでは検知できない不正プログラムを添付した電子メールを送付。ウイルスに感染させた当該職員の端末の情報を足がかりにして本丸部分に踏み込み、機密性の高い情報を盗み取っていくという手口だ。

最近は多数の宛先に同一内容のメールを送付する「ばらまき型」が減少し、攻撃対象を絞り込む傾向が強くなってきた。2014年度上半期では、就職活動を装ったメールや苦情を申し立てる内容のメールが増えている。

標的型メールの送信先アドレスの7割は、インターネット上で公開されていないものだ。攻撃者はフェイスブックやグループメールを利用して、ターゲットとする組織や職員個人の情報を事前に深く調査し、入念な準備を行った上で、犯罪を敢行している。

その手口は巧妙かつ多様化している。標的にした組織が頻繁に閲覧するウェブサイトを改ざんし、特定のアドレスからアクセスした場合にのみ、不正プログラムに感染するように細工した「水飲み場型攻撃」や、スマートフォンのセキュリティー対策情報を装ったメール攻撃などが確認されている。

企業は自社の情報が狙われているという危機感を持ち、被害が発生したときにどう軽減させることができるか、事前措置を普段から講じておくことが非常に重要だ。警察もサイバー攻撃への態勢を強化している。被害防止には迅速な情報共有が欠かせない。攻撃の事実を把握されたら、できるだけ早く警察に相談していただきたい。

基調講演
サイバーセキュリティ基本法と政府の取り組み強化について

内閣サイバーセキュリティセンター 内閣参事官　藤田 清太郎氏

戦略本部など対策指揮
基本法成立で体制整う

この数年で政府機関や重要インフラへの脅威件数は急増している。各府省庁などに置かれたセンサーが検知した2013年度の不正アクセスは508万件にも上る。

20年に東京五輪の開催が予定されるが、ロンドン五輪では2週間の開催期間中に2億回以上のサイバー攻撃があった。サイバー空間は世界中から多様な主体による攻撃にさらされている。警察庁によると、不正プログラムの接続先は97%は海外だという。

このような現状に対し国として組織横断的な取り組みを総合的に推進していくために制定されたのが、14年11月に成立したサイバーセキュリティ基本法である。

これまで国の情報セキュリティー施策は、情報セキュリティ政策会議とその事務局である内閣官房情報セキュリティセンター（NISC）が中心となって担ってきたが、明確な法的権限を持っていなかった。今回の基本法成立によって、司令塔としての機能が大幅に強化された。

具体的には各府省などに対する外部監査や、原因究明の調査を含む施策の評価、勧告などである。新たに設置されたサイバーセキュリティ戦略本部と内閣サイバーセキュリティセンター（NISC＝英語略称は変わらず）は、IT総合戦略本部や国家安全保障会議などと連携し、国の行政機関や独立行政法人のセキュリティー対策を指揮することになる。

加えて、NISCはGSOC（政府機関・情報セキュリティ横断監視・即応調整チーム）の機能強化や、国際連携の強化、さらに人材の育成と登用などに取り組んでいく。

全国には約26万人の情報セキュリティー従事者がいるが、そのうち質的にみて16万人が不足し、量的にも8万人ほど足りないという調査結果もある。人材育成は今後の大きな課題だ。

欧米諸国では、サイバーセキュリティーに関する国家戦略の策定や体制強化が進み、人員も増強されている。我が国も後れを取ることなく、スタンスを明確にした戦略と組織を構築していかなければならない。

講演
企業マイナンバー制度に伴うリスクと次世代セキュリティー対策

ディメンションデータジャパン シニアセキュリティースペシャリスト　**長高 史郎氏**
ブルーコートシステムズ ソリューションセールスディレクター　**皆川 文哉氏**

長高氏

皆川氏

社会保障と税の一体改革によって、2015年10月からマイナンバー制度がスタートする。行政を効率化し、国民の利便性を高め、さらに公平で公正な社会を実現する社会基盤となる。大きな経済効果も期待されている。

その一方で、社員のマイナンバーの保管責任を負う企業のリスクは高まる。データを暗号化したとしても、行政へ提出する場合などでは、暗号化されていない平文になり、脆弱な運用過程が存在するからだ。さらに、内部犯行で情報を外に持ち出すリスクにも対応しなければならない。

マイナンバー制度の中枢システムに関わるNTTグループの一員として、ディメンションデータジャパンはテクノロジーパートナーのブルーコートシステムズとともに、セキュリティー対策を担いたいと考えている。

マイナンバーを含む情報の漏洩を水際でブロックする仕組みや、クラウド上に特定個人情報を移管して、未知の転送が起こった場合にブロックするサービスなどを提供していくつもりだ。

企業情報の多くは暗号化されているが、その中にもすでに脅威が入り込んでいる可能性もある。情報セキュリティーでは、内部で何が起きているのかを素早く見つけ、なぜ起きたのかを解析して、次のステップにつなげることが大事だ。

それを可能にするのが今回提供するフォレンジックで、今、世界的に見直されている。マイナンバー制度でも、隠された足元のデータの動きを見ることが重要なポイントだと考える。

マイナンバーにリスク 企業の保管責任高まる

講演
標的型攻撃に対抗するための未知脅威対策

FFRI 執行役員事業推進本部長　川原 一郎氏

標的型攻撃は、単純なウイルス攻撃ではない。ソーシャルエンジニアリングや脆弱性攻撃など、高度なテクニックを組み合わせて特定の標的を狙うハッキング行為であり、従来型のセキュリティー対策では守りきれない。このような攻撃に対しては、パターンマッチングに頼らず、エンドポイントで振る舞いを検知することで未知の脅威を防御する対策が求められる。「FFR yarai」は標的型攻撃に特化した振る舞い検知で、未知のマルウエアや脆弱性攻撃を防御する当社のセキュリティー製品である。

最新バージョンから新たに「機械学習エンジン」を搭載し、未知のマルウエアへの対応を強化した。標的型攻撃に対抗するためには、既知・未知の脅威をエンドポイントで多層防御することが重要だと考える。

もう1つの課題は、不審なファイルが見つかった後の対応である。適切な事後対応ができなければ、情報の流出先や感染端末が分からない。かといって外部に解析を依頼すると時間がかかってしまう。

「FFR yarai analyzer」は、高度な知識と技術が必要とされるマルウエアの解析を自動で行うシステムだ。マルウエアの通信先や感染端末を特定できる情報などのリポートを日本語で出力する。

不審ファイルを発見したら、自社内で解析し、タイムリーな初動対応をすることで、被害拡大防止に役立てていただきたい。

高度化する標的型攻撃 エンドポイントで防御

講演
攻撃側から見た、広がり続ける防御側の（広義としての）脆弱性

ファイア・アイ 最高技術責任者　名和 利男氏

インターネットは、1967年に米国防総省が開発したARPAnetが起源だ。その基礎技術は今もあまり変わっておらず、基本的な仕様にセキュリティーの文言がない。50年近く前の非常に脆弱なネットワークシステムに、セキュリティーを後付けしているだけなので、穴は必ずある。

しかも今は、ネット上の相互接続・相互運用が拡大し、侵入可能な入り口が格段に増えた。攻撃者はセキュリティー対策が甘いと思われる2次請け、3次請けの関係者を狙って、あっさりと入り込んでくる。CMS（コンテンツ・マネジメント・サービス）に価値あるデータが集中していることも、脆弱性の内在化を高めている。

サイバー攻撃対策の意思決定者の中には、「インターネットにつながっていないから安全だ」と思っている人がまだいる。パソコンがインターネットにつながっていなくても、委託業者がネットワークにつながったPC上で作成した文書ファイルが1つでもあれば、マルウエアに感染している可能性を疑う必要がある。また、2つ目は既存セキュリティー対策の活用と統合。例えば、既存環境にサンドボックスを追加することで未知の脅威への対策が強化できるとともに、既存の当社のセキュリティー製品と連携し、脅威情報がフィードバックされることで既存システムそのものも強化される。

攻撃者は弱点見逃さず 防御側は態勢再構築を

講演
Next Generation『次』に求められる標的型攻撃対策

トレンドマイクロ プロダクトマーケティングマネージャー　横川 典子氏

標的型攻撃あるいはサイバー攻撃を考えるとき、もちろん防御も大事だが、最終的にカギを握るのは、問題が発生したときにどう対処するかである。攻撃の兆候に早く気づき、被害範囲を見極めた上で、ビジネスを元通りに戻す。ここまでの一連の作業こそが、新たに求められているソリューションとなる。

そこで、トレンドマイクロが考える次世代の標的型攻撃対策を4つにまとめてみた。1つはあらゆる情報を活用した被害範囲の特定である。クラウド上に蓄積された脅威情報とローカルログの分析により、過去に遡って影響度と根本原因を探っていく。

問題発生時の対処カギ 範囲見極め、復旧対応

3つ目は脅威知識に基づく復旧作業。復旧の工程は複雑で難しく、セキュリティー担当者には、不正プログラムの解析や脆弱性分析など様々な知識が要求される。そのため専門家の手を借りる手段もある。当社ではインシデントレスポンスのサービスも提供しており、ヒト、モノ両方の側面から問題発生後の対応を総合的にサポートしている。

最後はSDNなどの仮想化技術と連携した次世代セキュリティーアーキテクチャー。当社はこの新たなネットワークに対しても、親和性の高いセキュリティーを実装していくつもりだ。
