サイバーセキュリティ分野で進む新たな「ボーダレス化」

従来からサイバー攻撃に国境は存在しなかったが、現在、それだけではない様々な「境界」が曖昧になりつつある。この変化に対応するためには、権限を持ったCISOのリーダーシップが必要となる。

NRIセキュアテクノロジーズ（以降、NRIセキュア）では、自社の提供するセキュリティサービスを通じて得られたデータを分析し、2005年より毎年「サイバーセキュリティ傾向分析レポート」[1)]として発表している。14年目となる2018年のレポートから、「境界」というキーワードで、いくつかのトピックを取り上げてみたい。

「常時SSL化」が広がり50%を突破。クラウド利用もさらに拡大

これまでもパスワード入力等の重要な情報をやり取りする通信はHTTPS（通信の暗号化）によって保護されてきたが、それだけでなくウェブサイトとの間の全通信をHTTPSで保護する、いわゆる「常時SSL化」が広がっている。NRIセキュアが監視する、企業から外部ウェブサイトへのアクセスにおいても、2017年度、HTTPS通信の占める割合がついに50%を突破した。Chromeの最新バージョンではすでに、HTTPSではないウェブページに対して「保護されていない通信」と表示されるようになっており、常時SSL化への移行を促す動きは今後も継続すると考えられる。

他方で、企業におけるクラウドサービスの利用も拡大を続けている。NRIセキュアが監視するウェブアクセスから代表的なクラウドサービスの利用状況を調査したところ、82.6%の企業でOffice365[2)]、77.1%の企業でDropBox[3)]の利用が確認された。

これら2つの動きは独立したものであるが、ともに古典的な境界防御を困難にする、という共通点がある。古典的な境界防御は、企業内のネットワークと外部のネットワークを分け、境界線上の通信をファイアウォールやプロキシなどで監視・遮断するという手法を取るが、「常時SSL」化は、通信内容の監視のために経路上で行う復号処理のコストを増加させる。また、クラウドサービスの利用は守るべき情報を古典的な「境界」の外（すなわちクラウド上）へと出すことを意味する。

普及が広がるIoT機器

ホームルータやウェブカメラを代表とするIoT機器へのサイバー攻撃といえば、2016年に大規模な被害を引き起こしたマルウェア「Mirai」[4)]がまだ記憶に新しい。NRIセキュアが管理するネットワークにおいてファイアウォールによって遮断された通信を分析したところ、IoT機器がターゲットとみられるものは、前年度よりやや減少したものの、2017年度も依然として全体の約4割を占めていることがわかった。

一方、これらの通信の宛先ポート[5)]には変化がみられる。2016年度にはおよそ半分を占めていたtelnetポートへの攻撃割合が減少し、特定の機器をターゲットとしたポートに分散している。IoT機器の普及が進むなか、攻撃対象も多様化していることが見て取れる。世界中の家庭やオフィスにあり物理的にアクセス可能な、「ありふれた」機器が攻撃対象となり、あるいは乗っ取られて攻撃の起点となる。IoT機器の普及は、ネット上の世界とリアルな（物理的な）世界の境界をまたがったリスクの増加と、そのセキュリティ対策の必要性を示している。

仮想通貨の採掘につながる通信が急増

ユーザーがウェブページを閲覧すると、そのページ

NOTE

1) https://www.nri-secure.co.jp/report/2018/cstar2018.html
2) Microsoftの提供する、Officeアプリケーションを中心としたクラウドサービス。
3) 米DropBox, Inc.の提供する、データをクラウド上に保存し、ローカルの端末と同期させることのできるサービス。
4) IoT機器をターゲットにしたマルウェア。ウェブカメラなどのIoTデバイスを遠隔から乗っ取り、大規模なBotネット（マルウェアに感染し、遠隔から操作されるデバイス群）を構築し、攻撃対象のサービスにDDoS（分散サービス拒否攻撃：一斉に攻撃を仕掛けることにより、対象サービスのリソースを枯渇させ、サービス提供を継続できなくさせる攻撃）を仕掛けた。
5) インターネットの通信で利用されるプロトコルTCP/IPにおいては、アプリケーションごとに接続に利用するポートは慣例的に定まっている。例えば、単純な遠隔操作を暗号化しない平文で行うtelnetでは、通常23番ポートが利用される。
6) Endpoint Detection and Response。PCやスマートデバイスなどのエンドポイントで、サイバー攻撃をはじめとする不審な動作を監視・検出し、ネットワークの遮断や証跡の保全などを行うツール。
7) Cloud Access Security Broker。ユーザーからの（複数の）クラウドサービス利用を管理し、クラウド利用の可視化や、組織のポリシーに則ったアクセス制御、サイバー攻撃や重要情報漏洩からの防御を行うための製品・サービス。
8) https://www.nri-secure.co.jp/report/2018/analysis_global2018.html

に読み込まれたスクリプトがユーザーのブラウザ上で実行され、仮想通貨を採掘、スクリプトの設置者が採掘された仮想通貨を手にする。このようなスクリプト「CoinHive」が2017年9月に登場した。それ以降、CoinHiveや類似の仮想通貨採掘スクリプトへのアクセス件数は一気に跳ね上がり、同年10月には8月に比べ7倍となった。その中には、脆弱性を悪用され第三者によって外部から不正にスクリプトを「注入」されたサイトもあるし、サイトの管理者がウェブ広告に変わるマネタイズの手段として自らスクリプトを設置する例もある。UNICEFオーストラリア支部は、採掘スクリプトの実行を訪問者に確認した上で、採掘により得られた仮想通貨を寄付として取り扱っている。一方国内では、訪問者に明示せずCoinHiveを設置したサイト管理者が不正指令電磁的記録供用罪で逮捕されるという事例もある。

機密情報の窃取やランサムウェア等とは異なり、このような仮想通貨採掘スクリプトは企業活動に直接的な被害をもたらすものではない。しかし、業務に供する端末のリソースを消費するという意味では無害とも言えないだろう。なにを「有害」として遮断し、どこまでを「無害」として許容するか、CoinHiveは、その境界の曖昧さを再認識させる契機になったのではないだろうか。

曖昧になりつつある「境界」

これまでに挙げた変化はいずれも、サイバーセキュリティの様々な文脈における「境界」が複雑化し、曖昧さを増していると感じさせるものだ。単純な境界防御だけでは限界があることは、すでに2000年代初頭から様々な指摘がなされているが、今回の調査にはその裏付けとなる環境変化が明確に現れていると言えよう。さらに、直接データとしては現れていないが、「働き方改革」でも注目されるリモートワークの普及もまた、オフィスの「中」と「外」の境界を不明確にすることに繋がることが、今回のレポートで触れられている。

では、こうした変化にどのように対応すればよいだろうか。EDR[6]やCASB[7]といったツールは問題の一部の解決策にはなるだろうが、全てを解決する「銀の弾丸」はもちろん存在し得ない。様々な新しい技術を適切に使いこなすためにも、まずは、基本に立ち返ることが重要ではないだろうか。何を守り、何を守らないか、全体を俯瞰しリスクベースでポリシーを定め、それに従って方針を定める。さらに、定期的にそのポリシーを見直す仕組みを組織の中に作り込む。このようなセキュリティ対策の基本の実効的・継続的な実現、特にどこまでのリスクを受容するかの方針決定には、セキュリティ対策全体に責任をもつCISO（最高情報セキュリティ責任者）に相応の権限が必要となる。当社の別の調査（NRI Secure Insight 2018[8]）によると、経営層がCISOに就任している日本企業は、海外（米・英・豪・星）のおよそ半分の35%しかない。CISOがリーダーシップを発揮できる体制をどのように実現するかが、「セキュリティのボーダレス化」に対応するための鍵となるだろう。

（監修：NRIセキュアテクノロジーズ
サイバーセキュリティサービス開発部 原田 諭）

Writer's Profile

西谷 昌紀 Masaki Nishitani
NRIセキュアテクノロジーズ
上級セキュリティエンジニア
専門は認証・IDセキュリティ
focus@nri.co.jp