強靭なセキュリティを築くために

コンピュータのOSやソフトウェアの脆弱性（製品に含まれるセキュリティ上の問題点）を狙う
巧妙なサイバー攻撃に対し、世界的なIT企業はどんな対策を講じているのか。
経済産業省とIPA（独立行政法人情報処理推進機構）が共催する「セキュリティ・キャンプ」を企画・指導する
サイバー大学の園田道夫教授に、情報セキュリティにおける問題と対策ついて話を伺いました。

セキュリティ事故を防ぐため、攻撃者の手法を学ぶ

――近年、大規模な顧客情報の流出など、セキュリティ事故が相次いで起こっていますね。

転機となったのは2007年頃です。ウイルスを作成できるツールが出現し、続いて実行者の身元を分からなくする遠隔操作ツールなども出てきました。その結果、犯罪者の技術的なハードルが下がり、サイバー攻撃が急増したのです。

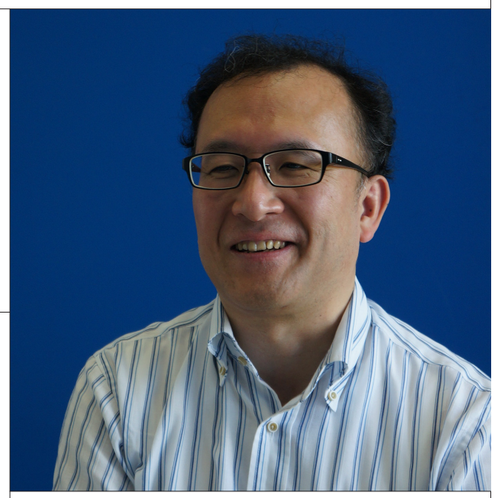
また最近では、「ゼロデイ攻撃」*のように、セキュリティ対策が講じられていない未知の脆弱性を突いてくるケースも増えています。

――ベンダー側も、提供するITサービスやソリューションから脆弱性を排除する努力が求められています。

例えばマイクロソフトは、開発プロセスに脆弱性検査を取り入れるなど大改革を行い、ここ十年ほどで自社製品のクオリティを劇的に向上させました。

――どんな施策が功を奏したのでしょうか。

外部のセキュリティ通報者（脆弱性を発見し指摘する善意の協力者）の声に耳を傾け、「攻撃者の手法」を徹底して学んだのです。これは海外のITベンダーでは、いまや当たり前のことになっています。ツイッターやグーグルなども、セキュリティの脆弱性を発見した通報者に賞金を支払う報奨金制度を拡充し、クラウドサービスの堅牢性向上に役立てています。



サイバー大学 IT総合学部 専任教授 **園田道夫氏**

独立行政法人情報処理推進機構（IPA）技術本部 セキュリティセンター 情報セキュリティ技術ラボラトリー 研究員。2008年に経済産業省商務情報政局長表彰を受賞。著書、訳書多数。

未知の脆弱性を摘み取る報償金制度

――優秀な人材を抱える企業が、なぜ外部の方からの通報を募集しているのでしょうか？

セキュリティ対策の90％までは、ツールの活用などで順調に進みます。しかし、残り10％の未知の脆弱性を摘み取るためには、膨大なコストと時間を費やさなければなりません。報奨金制度という形で、外部の優れた知見を取り入れていくことは、企業活動の経済性という観点からも理に適っています。

――海外では、複数のベンダーが合同で脆弱性発見コンテストを開くケースもありますね。

昨年はモバイルに関する世界的な脆弱性発見コンテストで、三井物産の子会社が率いる日本チームが優勝し賞金400万を獲得しました。

実は、脆弱性を扱う市場は2つあり、その1つは、初めにお話したウイルス作成ツールなどが流通するブラックマーケットです。新たな脆弱性を発見した場合、その情報はブラックマーケットに売ることもできますが、それに対して〝表の世界〟で対価を支払う仕組みが報奨金制度やコンテストになります。特にITベンダーの垣根を越えて行われる国際的なコンテストではブラックマーケットでの価格感を見て値付けをしています。これはブラックな市場に流出させないためにも重要なことです。

日本のIT企業の中で、先陣を切って報奨金制度を開始したサイボウズの「脆弱性報奨金制度」は高く評価しています。同様の取り組みが、より多くの国内ITベンダーやクラウド事業者に広がっていくことを期待しています。

セキュリティ・キャンプ

若年層の優秀な情報セキュリティ人材の育成を目的として、2004年に発足。現在は、経済産業省、IPA(情報処理推進機構)、産業界が一体となった大きな取り組みとなり、多くの優秀な人材を輩出している。サイボウズ・ラボ社も講師を派遣。

＊ソフトウェアの脆弱性が発見された際に、利用者が対策を実施する前の隙を突いて攻撃すること。

脆弱性を指摘してもらうことが品質を向上させる

サイボウズでは、2013年に国内商用クラウド初となる脆弱性発見コンテスト「cybozu.com Security Challenge」を実施しました。社内で脆弱性情報の対応を取りまとめているグローバル開発本部品質保証部の伊藤彰嗣に話を聞きました。

ベースとなる自社検証

サイボウズでは、サービスの公開前に自社で既定の脆弱性検証を行っています（図1）。サービスの内部仕様を理解して実施するこの自社検証が、全ての脆弱性対応のベースになります。

専門機関による外部監査

自社検証に加え、cybozu.comが提供している全サービスを対象として、外部機関による脆弱性の監査を年間1回以上実施しています。日々セキュリティ情報を収集・研究している専門機関に調査してもらうことで、より安全性を高めています。

国内外から報告が集まる脆弱性報奨金制度

この2つの検証・監査を前提として、さらに外部のセキュリティ専門家による視点や知見を取り入れる目的で実施しているのが「脆弱性報奨金制度」です。社内で検出されていない未知の脆弱性を発見した善意の協力者に、対価（報奨金）をお渡しするという制度です。

この制度の一環として、2014年8月には「cybozu.com バグハンター合宿」（写真）を開催しました。合宿では、国内トップクラスの見識者18名に参加いただき、合宿形式で集中的に脆弱性を検証してもらいました。そこでの発見がサービスの品質向上に役立てられています。また、協力者の攻撃手法を学び自社検証に生かしています。

品質へのこだわり

サービスに脆弱性が発見されたと聞くと、怖いと思われる方はいらっしゃると思います。けれども、本当に怖いのは、脆弱性に気付かずに攻撃を受けてしまうことです。

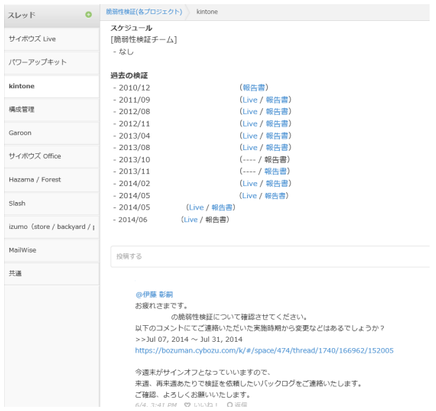
マイクロソフトのように真摯に対策されている企業でも、年間数百件の脆弱性が製品公開後に見つかり、修正プログラムを配布しています。昨日まで世界中が安全だと思って使っていた仕組みから突然脆弱性が発見されることもあります。

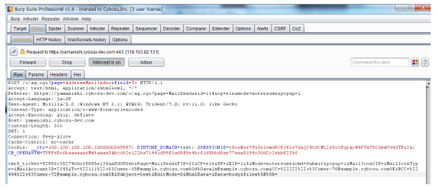
脆弱性の探求は、ある水準を超えると、回答のないパズルを解くような作業になってきます。そして世の中には、天才的にパズルを解くのが得意な人たちが存在します。

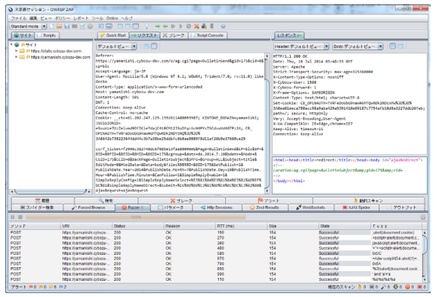
脆弱性報奨金制度を通じて彼らの力を借り、1件でも多くの脆弱性を発見することがお客様を守ることにつながります。攻撃者の先手を打って対処していくことが大事だからです。

これらの取り組みによって発見した脆弱性情報は、企業がどのように脆弱性を取り扱うべきかを定めた国際規格（ISO／IEC規格）に則って検証・改修・情報公開を行い、日々サービスの品質向上に努めています。

脆弱性に対してサイボウズ社で行う自社検証の様子／上はタスク管理と連絡に使っているkintoneの画面。中、下は脆弱性調査を行っている画面。綿密な検証を行います。







「バグハンター合宿」の様子／参加者が互いに技術知識を向上し合えるよう、セキュリティの知見を発表し、交流する時間帯も設けました。