SQAT® Security Report

2017年9月号

株式会社ブロードバンドセキュリティ

BBSecは内閣サイバーセキュリティセンターの
「サイバーセキュリティ普及啓発」に賛同しています

はじめに

株式会社ブロードバンドセキュリティ
セキュリティサービス本部 取締役本部長
田仲 克己

2017年上半期は、深刻なサイバー事案が立て続けに発生した半年でした。2月にはオープンソースのCMSであるWordPressの脆弱性を悪用したホームページの改竄が頻発、3月には同じくオープンソースのWebアプリケーション開発フレームワークApache Struts 2の新たな脆弱性を突いた攻撃が発生しました。また5月にはランサムウェアWannaCryが世界規模で拡散し、各国に大きな被害をもたらしています。

国内を見ても、各種システムの脆弱性を悪用した攻撃の勢いは増す一方です。内閣サイバーセキュリティセンター（NISC）が7月に発表した『サイバーセキュリティ政策に係る年次報告』によると、2016年度の脅威件数は政府機関関連だけで711万件に達し、前年度から100万件増加しました。比率にすると約4.4秒に1回、脅威が認知されています。ここに民間企業への脅威も加えると、私たちはまさに「絶え間なく脅威に晒されている」と言えるでしょう。

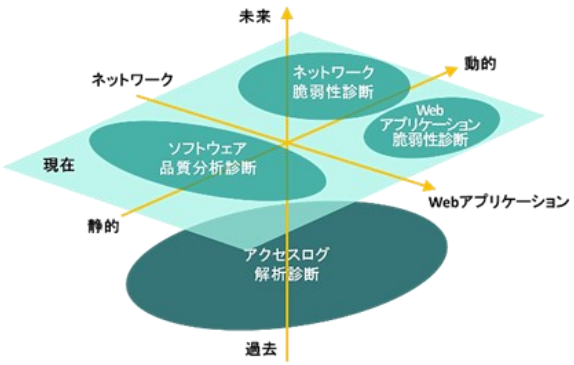
こうした状況に対処すべく、株式会社ブロードバンドセキュリティ（以下、「BBSec」)では、各種サービスのさらなる拡充を進めています。ホームページ改竄事案の増加にいち早く対応を図り、脆弱性診断サービスの「SQAT®」*にWebコンテンツ改竄検知を標準で組み込んだほか、Apache Struts 2、WannaCryをはじめとするサイバー事案の発生時には国内外のネットワークを駆使してリアルタイムに状況を把握し、すみやかに注意喚起を配信しました。今後も、進化する脅威に遅れを取ることなく対応し、お客様の組織のセキュリティリスク軽減を支援いたします。

本誌『SQAT® Security Report』も、以上のような取り組みの一環として刊行するものです。「SQAT®」での2017年上半期診断から得られた最新データに基づくレポート、トップエンジニアによる動向分析、分野の第一線で活躍する研究者との対談など、前号・前々号の読者からのご意見・ご要望を踏まえ、コンテンツのさらなる充実を図りました。

本誌が、これをご覧になった皆様の組織のセキュリティ向上に資し、セキュリティ対策を「投資」として役立てる一助となることを願ってやみません。それこそが「便利で安全なネットワーク社会を創造する」をモットーに掲げるBBSecの使命と考えております。

***SQAT®（Software Quality Analysis Team）とは**
～スペシャリスト集団が組織の脆弱性対策をトータルに支援～

「SQAT®」は、BBSecがご提供する脆弱性診断サービスです。エンジニア、コンサルタント、ホワイトハッカー等から編成された精鋭チームが、あらゆる側面から網羅的な診断を実施。スペシャリストのノウハウを結集して組織の情報システム強化をお手伝いします。お客様は金融機関・インターネット事業者などの民間企業から、官公庁をはじめとする公共機関まで幅広く、これまでに延べ3,000組織、1万を超えるシステムで利用されています。



目　次

巻頭特集

特別対談 ～レジリエンスからAI・IoTまで～

門林 雄基 氏 × 安藤 一憲

（奈良先端科学技術大学院大学 教授）（株式会社ブロードバンドセキュリティ 取締役）

本年4月、奈良先端科学技術大学院大学に「サイバーレジリエンス構成学研究室」が発足し、多方面から注目を集めている。「レジリエンス(resilience)」とは一般的に「回復力」と訳される用語だが、サイバーセキュリティの文脈では「事故・被害が生じた場合にすみやかにシステムや事業を回復させる力」を意味する。同研究室では、「事故・被害は発生するものである」という前提に立ち、官民のさまざまな組織と連携して、侵入の早期検知や被害軽減を図るための方策に取り組んでおり、BBSecも共同研究メンバーの一員である。
本特集では、同研究室を率いる門林教授と、当社取締役で海外・先端技術分野を統括する安藤が、これからのサイバーセキュリティを考える上で鍵となるコンセプト、テクノロジーを縦横に語り合う。

（2017年5月10日 於 株式会社ブロードバンドセキュリティ会議室）

「サイバーレジリエンス」とは何か

安藤：門林先生、早速ですが、奈良先端科学技術大学院大学にこの春新設された「サイバーレジリエンス構成学研究室」について伺いたいと思います。研究室発足のパーティーに、僕、出席させていただいたので、発足したのは知っています。ただ、「サイバーレジリエンス」とは耳慣れない言葉ですよね。どっちの方向に舵を切っていくのかなっていうのが、はっきりとはまだ僕には見えてない。その辺はどうでしょうね。

門林：実は今年度教授に就任するにあたって、学長からちょっと目立つことをやれと言われました。それで、じゃあ目立つことって何だろうとまず考えた時に、名前、というか言葉の選び方だろうと思ったわけです。「サイバーセキュリティ」って、今、割とホットなキーワードになっていて、新聞とか経営者の方とか、技術者の方とか、もう重要性は認識されるようになってきたと思うんです。

私もサイバーセキュリティの標準化に8年ぐらい関わっているんですけれども、ある程度社会的に認知されたというか、社会的にも技術的にもメインストリームなアジェンダになってきたな、と。ただ、その中で、サイバーセキュリティを横目に見ている技術者の方、例えばネットワークの技術の方などは、サイバーセキュリティの取り組み全体に対して少し不安感を持っている。なぜかというと、例えばBlack Hat[*1]などのサイバーセキュリティのカンファレンスに行くと、脆弱性をとにかくすごくショッキングに報道する。システムがハッキングされますとか、IoTのハッキングが問題だ、みたいに煽るような論調になりがちです。

一方で脆弱性が見つかったあとの本当に難しいところ、「それをどうやって現場で直していくのか」とか「実際にそれをどうやってお客様に伝えていくのか」といったことにはあまり触れない。問題はそこなんですよね。お客様に売ってしまったあとに本当の問題が見つかった時のフォローアップ、そこからどうやって直していくのか、現場で、そういう問題がある機器なんかを使いながら、どうやってダメージコントロールをしていくのかというところが大きな課題認識だったんです。で、それを一言で言い表すと、「サイバーレジリエンス」でないかと考えているわけですね。

一方、「サイバーレジリエンス」というものをどう作るのかっていうところは、これはまだわかってないんですよ。大学の研究室なので、わかってないことをテーマにしたほうがよくて。ここで「『サイバーセキュリティ』の研究室を作ります」と言っても、ある意味僕にとっては手垢のついた言葉です。10年ぐらい前からやっているわけですから。「サイバーセキュリティ」という単語は、その言葉が一般認知されるようになった段階で、学問的なフラッグシップの役割を終えたと思っているんですよ。で、次のキーワードを探した時に、これは「サイバーレジリンス」だろうと。

*1 世界最大規模の年次セキュリティカンファレンス。最新の知見や研究成果が多数発表される。

どうやって「やられる（攻撃される）」ことを前提に普及させていくのか。ダメージを最小化していくのか。あるいは、ダメージコントロールの前提になるようなリスクコミュニケーション、そういったいろんなことを若い人たちと一緒に考えたい。「サイバーレジリエンス構成学研究室」の「構成学」というのも同じで、どうサイバーレジリエンスを作るかっていうことも、僕らを含めてわかっていないんです。どんな技術を組み合わせるのか、クラウドでやるのがいいのか、あるいはIoTでやるのがいいのか、あるいは非常にデバイスを安くして問題を解決するのか、あるいはソフトウェアの作り方を変えればいいのか。そういうところもいろんな自由度があって。若い人の発想ってすごく柔軟じゃないですか。その発想を取り入れながらサイバーレジリエンスを作っていければなあと思ってこういう講座名にしました。

この「サイバーレジリエンス構成学研究室」を作る、という段階で、かなり大きな手応えがありました。民間の方も結構サイバーレジリエンスっていう言葉に鋭敏に反応されて、セミナーがあちこちで開かれたり、メディアにも取り上げられました。

「レスポンス」から「レジリエンス」へ

安藤：一言で言うと、「後手の先をどう取るか」っていう課題なんですよね、きっと。

門林：そうですね。

安藤：やられるのはやられるんだけど、そのあとの対応をどう取って被害を最小化するかっていう課題。難しいですよね。

門林：そうですね。旧来型な考え方で言うと、「やられました」＝「インシデントレスポンス」だったんですよ。けれども、僕はインシデントレスポンスに限らないと思っているんですね、サイバーレジリエンスっていうのは。

例えばDDoSなんかそうですけれど、あれもある意味防ぎようがないですよね。それこそ、「いっせーの」って感じのDDoSが来るわけで、それでやられるのはもう仕方ない、という時に、インシデントレスポンス的な考え方で言うと、「対処しなさい」ということになる。その対処も、例えばJPCERT/CCに連絡してとか、お客様に連絡してとか、それこそ広報してとか。それを一般に「インシデントレスポンス」と言ってます。だけど、サイバーレジリエンスの考え方でいくと、やはりインフラそのものも ― 例えば「DDoSが来るのを前提に設計も考えないといけない」というところも ― 入ってくると思うんですよ。最近だと「DevSecOps*2」なんて言葉もありますけれど、インフラを設計する段階、あるいは実際にソフトウェアを作る段階から「やられること」を前提に作っておくと、いわゆるインシデントレスポンスよりも自由度が高いと思うんですよね。「やられたらこのクラウドを使うことにしよう」とか、やられることを前提にシステムを二重化して日本とヨーロッパに置いとこうとか、いろんなことができるわけじゃないですか。

編集部：先生は普段から外国の学生たちと研究に取り組まれていると思いますが、国別で見ると、日本のレジリエンスに対する熱量はどれくらいなんでしょう。そういうことに対する危機感とか。

門林：日本は低かったんですよ、危機感は。ちなみに「サイバーレジリエンス」っていうのは、ヨーロッパでは政治的キーワードです。「サイバーセキュリティ」の次ぐらいのセキュリティキーワードです。私は2013年度から3年間、EUと日本の国際共同研究をしてたんですが、そのプロジェクトは、サイ

門林 雄基 奈良先端科学技術大学院大学 情報科学研究科教授。国内外でサイバーセキュリティの標準化に取り組む。日欧国際共同研究NECOMAプロジェクトの日本研究代表、WIDEプロジェクトボードメンバーなどを歴任。

*2 「Development」「Operations」「Security」を組み合わせた造語。開発担当、運用担当、セキュリティ担当が連携してシステム開発を進めるための手法。

バーレジリエンスのプロジェクトだったんです。いわゆるビッグデータの技術、Hadoopとかありますよね。ああいうビッグデータの技術をサイバーセキュリティ・サイバーインフラストラクチャに提供して、どうやってサイバーレジリエンスを向上させるかっていうプロジェクト、「NECOMA（Nippon-European Cyberdefense-Oriented Multilayer threat Analysis）」っていうのをやってたんです。これは、欧州委員会のサイバーレジリエンスの研究をしてくださいという公募だったんですよ。それぐらい政治的なキーワードなんですよね、サイバーレジリエンスっていうのは。

編集部：「サイバーレジリエンス」という言葉に対して民間企業からの反応も熱いというお話でしたが、どういった層で、どういった部門で、という特徴はありますか。やはり技術部門の方たちがまず立ち上がっているという状況なんでしょうか。

門林：いろんなところに仲間はいるんですが、マーケや営業の方面からも結構サポートいただいてますし、技術のトップ中のトップのような人も「サイバーレジリエンス、正しいと思いますよ」みたいな言い方をしてくれますね。

安藤 一憲　株式会社ブロードバンドセキュリティ 取締役。海外および先端技術担当として、国内外の業界団体に参与。WIDEプロジェクト研究員、M3AAWGメンバー。

編集部：普段はお互いに意見を戦わせることの少ない部門の方が、色々なところから集まってくる場になりつつある、という感じでしょうか。

門林：そうなるといいな、っていうところですね。これからそういうのは作っていかないといけないと思ってます。インターネットができて40、50年近くになるんですかね、1969年の発明なので。産業界と大学の距離がどんどん開いてるんですよ、端的に言うと。昔、インターネットっていうのは研究者中心でしたから、企業も大学にお願いしてつなぐ、という面もあって、すごく距離が近かったんですね。僕らも企業の研究開発部門の方を存じ上げていて、大学と企業の研究開発部門が一緒になって日本のインターネットを作ってきた。セキュリティも一緒にやってたんですね。だけど、今、セキュリティもネットワークもすごく産業化してるじゃないですか。だから大学なんかに何も聞かなくても作れちゃうんですよ。非常に距離は開いてますよね。ただ、セキュリティのように、どんどん変わる状況で正解がないもの、技術革新が激しいもの― それこそIoTセキュリティもそうですし、最近のプラントだとかSCADA[*3]のセキュリティもそうですけれど― 正解がないものに対しては、産業界と大学の間に距離があるのはすごく不幸なんですよね。研究でも、産業界でも、今、ものすごい勢いでイノベーションが進んでますから。

安藤：逆に僕から見ると、サイバーレジリエンスっていう言葉がウケた背景っていうのは、現場の、例えばISMSの枠組みであるとか、そういうもので構築したセキュリティを維持するための体制が必ずしもうまく回ってない、って認識があるからだと思いますね。「それ（うまく回ってない）はどうして？」っていうところから、みんなスタートしてるんだと思います。だから、CSIRTの次に来る概念だと僕は思っている。運用の話に落とそうとしているのがCSIRTですよ。セキュリティインシデントが発生した時にまさにインシデントレスポンスのPDCAサイクルを回すのがCSIRTだと考えるならば、そこにもうちょっと俯瞰的な目を入れて、「じゃあ仕組みをこういうふうにしていこうよ」っていうのを入れていこう、というのがレジリエンスだと思う。そう考えると、「現状がうまくいってない」と現場は感じているんだと思いますよ。だから食いつく。もしそういう状況がなかったら、「えっ？」って思うだけでしょう。でも、問題意識、課題意識を持ってるから、みんな食いつく。

*3 Supervisory Control And Data Acquisition。監視制御、データ取得を行う産業制御システム。

編集部：真剣に悩み始めているという。

安藤：そう。真剣にならなきゃならないところが出てきたっていうことが、時代の変化なのかもしれないですけど。

門林：そうですよね。だから、大変な状況ではありますけどある意味チャンスですよ。インターネットを最初に作った時って、どうやって作っていいかみんなわかってなかったんです。学術と産業界で割と力を合わせてみんなでやったんですね。で、それが安藤さんの世代とか、そのちょっと上の世代とかを作ったと思うし、それが今の日本のIT業界の財産になってると僕は思うんです。今、サイバーセキュリティでも、サイバーレジリエンスでもそうですが、この解のない状況の中、若い人がいっぱいいるじゃないですか。これはチャンスだと思うんですよ。それこそ若い、大学の人たちも目をキラキラしてやってくれてるし、企業の方もしゃかりきにお仕事をされてるので、これ、いいことかなと思っています。

「ニーズドリブン」で「分業」を超える

門林：インターネットが実用化されてもう20数年経つんですが、今、運用する人とか、火消しをする人とか、開発をする人の分業が進みすぎていて、そこの発想ができなくなってると思うんです。

僕も安藤さんもその頃から関わっているから感じるんだと思うんですけど、インシデントレスポンスの発想でいくと、「じゃあ、パソコンを取りあえずこうしましょう」とか、「ネットワークにSSLを設定しましょう」とか、すごく近視眼的な、小手先の対応、あるいは「お客様にコミュニケーションしましょう」となる。そうじゃないんじゃないかっていう問題意識が根底にあります。

安藤：分業化して、細分化して守ってるんで、その範囲でできること、対策っていうふうになると小手先になりがちだと。だけど本当は全部のシステムを上から俯瞰的に見て、こういう組み方をしたほうがいい、というような対策があるはずだということですね。そこに着目して、設計からそれこそ「レジリエンシーの高いもの」を作っていこうっていう考え方ですよね。わかりやすいんじゃないかな。

門林：僕はDevOpsの流れというのはすごく良いことだと思っていて、例えばブロードバンドセキュリティさんとか、ITサービスプロバイダの会社の方って、割とそういう意味で自然に、業務のニーズからして自然にDevOpsになっているケースが多いと思っています。と

いうのは、自社のシステム、例えばメールサービスがあったとして、「このサービスを何とか良くしていかないといけない」というところで全社的に力を合わせようと思うと、自然と、「運用部門と開発部門が一緒に仕事をしましょう」っていう形になるじゃないですか。これはすごくいいことで、従来の、「製造業・メーカーさんがいて、SIerさんがいて、ユーザさんがいる」っていう、ウォーターフォールモデルとは違うと思うんですよ。

従来の製品の提供販売のやり方が典型ですが、メーカーさんが「こういう製品が欲しいだろう」という想像で作って、SIerさんが「あるものを売ればいい」という姿勢で売る。エンドユーザさんは、「こういう製品ですから仕様に沿ってお使いください」と押しつけられて、そもそも自社の枠に合わないのにオペレーションで頑張るわけです。それに対して、DevOpsみたいにニーズドリブンで行くっていうのはすごく大事だと思います。

よくあるのが、教科書的な考え方。「JPCERTがあります」、「ISAC[*4]があります」、インシデントレスポンスに対して「ISO 27035があります」と、何か「既にきちんとしたものがあって、工夫したらちゃんとできるんだ」っていう、変な幻想があると思うんですけれど、現実そうではないんですよね。「DevOps」だって、後付けなんですよ。うまくいった会社さんが、例えばシリコンバレーだったり東京だったりで、いろいろ勉強会とかで話してる中で見出されてきた概念だと思うので、そこをニーズドリブンで行く。「CSIRT」とか「ISAC」とか「情報共有」とか「サイバーセキュリティ」もそうですけど、全部後付けでしかないっていうところですよね。そこに注意してやっていくのは大事かなと思います。

*4 Information Sharing and Analysis Center。セキュリティ関連の情報を共有し、組織の枠を超えた連携を促進するための機関。日本では「金融ISAC」「ICT-ISAC」等が発足している。

どんな人材が必要か

編集部：最近、「エンジニアよりも橋渡し人材が必要だ」といった議論が見られますが、どうお考えでしょう。

門林：そうですね。「橋渡し人材」っていう言葉が適切かどうか、ということはありますが、先ほどのニーズドリブンという話で言うと、「橋渡し人材」とは、恐らく、ゴールオリエンテッドに動ける人材のことだと思うんですよ。例えばそのゴールに向かっていくのに、ある時はCISOがいないといけない、ある時は社長を口説かないといけない、ある時は財務を口説かないといけない、ある時はカスタマーコミュニケーションをしないといけない、ある時は開発を口説かないといけないっていう場合に、セキュリティなりレジリエンスというものをビジネス目標にして、ゴールオリエンテッドに動ける人を「橋渡し人材」と言ってるんだと思うんです。決して、「技術の言葉と経営の言葉だけしゃべれれば橋渡し人材」というわけじゃないですね。

安藤：そうじゃないと説明もはずしちゃうんだと思いますね、ゴールが的確に認識されていないと。橋渡しの仕方を間違えることだってあるでしょうね。「本来はこうあるべきだからこういうふうに持っていくんだ」っていう話し方ができる人じゃないと橋渡しはできないよね。

門林：人材育成の議論で欠けてるな、と思うのは、「本気度」なんですよ。これは爆弾発言になっちゃうかもしれませんけど、本気でゴールに向かって目標を達成できる人っていうのを経営サイドは評価するじゃないですか。ビジネスの継続性が大事だ、顧客満足度が大事だ、そのために君は技術で何ができるんだ、あるいはどういうふうに技術チームを動かせるんだ、財務をどういうふうに口説けるんだ、…そういうところだと思うんですよ。本気度っていうのは。「最近就職に有利なんでセキュリティ頑張ります」みたいな感じだと、得られないわけですよね。「セキュリティで頑張って会社に潜り込みました」となっちゃって。それこそ、「人材育成プログラムで経営の言葉を覚えました」、「次は技術の言葉を覚えましょう」、「とりあえず流儀は覚えました」だと、「おまえ本気で仕事できるの？」って話になるじゃないですか。そこなんですよね、僕がすごく気にするのは。なので、本来的には教えなくてもできる人が欲しいんですよ。人材育成の話がすごく盛んなんですが、「教えなくても経営の言葉と技術の言葉を泣きながら勉強するやつ」が僕は欲しいんですよ。

安藤：必要で覚えた人のほうが使える、僕もそう思いますね。入社して3、4年でセキュリティのことだけやって、「人材育成されました」って言ってるけど、「それって本当？」っていう話ですよね。

僕なんかは多分化石人類扱いなんだろうけど、ずっと昔からやってる人っていうのは、技術的なことを全部一通りやっているんですよね。ネットワークもサーバも全部いじって。開発も運用も全部やって、自分でやって知ってますよ、と。泥くさいところも知ってます、という中でセキュリティを見ているっていうのと、分業化された中でセキュリティのところだけ ー 脆弱性はこういうのがあって、管理はこうやってやんなきゃいけないとか、そういうフレームワーク ー を覚えた人間とを比較すると、重さが違うよね。だから、人材育成で、「本当にそれでいいの？」っていう疑問は僕もずっと持ち続けていて。教えるのは否定はしないんだけど、それが役に立つのは何十年後なんだろう、っていう感想も同時に持ってる。泥くさいところなり、俯瞰的にものを見るだけの経験なりがないと、本当のところを判断できないんじゃない？って思うことが多い。「これはこれに優先させて社長止めてでも何とかしなきゃいけない」みたいなところができる人間じゃないと止められないことってあると思うので（笑）。そのレベルじゃないとできないことってありますよね、きっと。

門林：そうですね。人材育成っていうのは、僕らは生涯学習だと思っているんですけど。セキュリティってどんどん新しい攻撃が出てくるし、どんどん新しい製品とかサービスも出てくるし、クラウドとかIoTとか技術の革新もすさまじい勢いじゃないですか。日々勉強だと思うんですよね。で、日々勉強の中にたまたま、経営の単語も入っています、法律の単語も入ってます、営業の知識も入ってます。そういうことで僕はいいと思うんですよ。それでどのくらい場数を踏んだかだと思うんですよね。促成栽培で、「2年ぐらいのプログラムで人材育成できました」のような話ではなくて、継続的に、セキュリティ業界全体で、それこそい

ろんな会社さんの商売を任せられるシステムを、レジリエンスを高めることができる人を、どれぐらい育てていくか。社会の中にどれくらいそういう人が存在するのが望ましいかっていうことだと思うんですよね。「何百人作りました」のような、ワンショットで短期的に済む話ではないと思うんですよ。

編集部：若者の人材不足という点は、そこも含めて議論をしていく必要があるのでしょうか。

安藤：だって、もともと（人材が）少ないんじゃない？ないものねだりだと僕は思うよ。そういう経験ができる人って少ない。「大きなサーバを作りました」っていう人、どれだけいます？日本に。いないでしょ？あんまり。だからそういう人材はもともと不足してるんだと思うし、それをちゃんと拾って、セキュリティのわかる人に育てる機会も少ない。だから結果的に「少ない少ない」でずっと来てる。アプローチとしては、セキュリティの素養を大学の間にやっておいて、それがわーっと育っていって、ある程度の経験を積んだ時に、「こいつ、セキュリティもできるよ」っていう状態になってるのが理想像かもしれない。だから、今やってることは無駄ではないだろうと。効率は悪いけど（笑）。

門林：見ていて思うのは、業界全体が現状肯定から入ってると思うんですよ。こういうアプライアンスがあります、PCI DSSがあります、こういう仕組みがあります、こういう決め事があります、こういう組織論があります、これで何とかうまく回しましょう、で動いてると思うんですが、今のままやるとあまりにも大変じゃないかって思うんです、僕自身は。

例えば、フォレンジックするにしても、一千万円かかりますと。何でかっていうと、大変だからなんですよね。そこの大変さをなくすっていう努力を本当はしなきゃいけない、業界として。要するに、効率化ですよね。低廉化だったり生産性の改善、つまり、フォレンジックを1個5分でできるようにするにはどうするか、あるいはそれを5秒にするにはどうするかっていうところの技術開発だったりイノベーションが必要なんですけど、そこの問題意識がすごく欠けてると僕は思うんですよ。

編集部：現場が近視眼的な見え方しかできないというお話でしたが、そもそも、リーダーが舵取りできていないから現場が苦しむ、という面もあるのではないでしょうか。

安藤：システムの開発提案で、こういうサーバ置いてこういうアプリケーションを動かすんです、っていう提案だけが出てくるんですよ、放っとくと。「じゃあ、そのネットワークはどこに構築して、どこにその場所を置いて、誰がその実態の機器を管理するの？」って聞くと答えが返ってこない、というのは日常茶飯事ですよ。つまり、上で誰か勘案しなきゃいけないわけね。どっかで誰かが決めなきゃいけなくて、ちゃんと決めて持ってらっしゃいっていうことを言って返す。リーダーが舵取りできてないんですね。今回決められないなら、ちゃんと決めて持ってきてね、みたいなことってありますよ。「そこのラック、場所は空いてるけどもう電源はないよ」とか、平気であるわけですよ。誰がコントロールするんですかと、それを（笑）。近視眼的にしか見てないからだよね。交通整理する人もいなきゃだめなんですよね。あるいは、そのラックを管理してるのは「誰か」はそういうこと分かってるわけですけれど、その情報が会社の中でシェアされてない。

標準化の重要性

安藤：例えばね、同じ開発系であっても、自分たちのオフィスの中で必要なソフトウェアを開発しているのと組み込み系の開発とではまるで違うし、用語も違うしモチベーションも違うし、どういうソフトウェアを作るがいいのかっていう、その価値観も違うんです。

編集部：それぞれの専門の中でサイロ化が進んでいるということですか。

安藤：そう。だから、組み込みの中ではいかにサイズを小さくするかとか、いかに安いハードウェアで上げるかとか、そういうモチベーションがあるけど、オフィスのソフトウェアを作ってる時にはないよね、そういうのは。

門林：ただ、それはずっと意識して闘っていかなきゃいけない闘いなんですよ。つまり、お客様のほうを向いて、ビジネスプライオリティだけで仕事をしていると、どんどんサイロ化って進むんです。お客様のビジネス要件とかお客様が使う用語とか、いろんなものに左右されるんですね。それはもう本当サイロエフェクトの最たるもので、それをずっと続けていくと人材流動性も高まらないですし、やっぱり標準化ができてないっていうことになるんですよ。概念そのものが標準化しないと会話ができない、教科書が書けない、教科書が売れないってことになりますから。例えば、自動車業界なんかが最たるものですけど、系列で随分と違うんですよね。だから、「本当に、それがいいんですか？」っていうのをIT業界は考えなきゃいけない。業

界全体としてね。これはビジネスのコンテクストだけで数字を追いかけてると絶対出てこない話なんですけど、国際的にはすごく大事な話なんですよ。

僕は国際電気通信連合っていうところで単語の定義の標準化をやってるんですけど、例えば「サイバーセキュリティ」っていう単語の定義は、「X.1205」っていうリコメンデーションがスタンダードになっているんです。「サイバーセキュリティ」っていう単語は2004年に定義されたんですが、それが国際的な国連の議論だとかいろんなところの議論で使われる礎になってる。単語の定義がしっかりしている、お互いにちゃんと意思疎通ができるっていうことは、社会全体として技術を考える上ですごく大事なことです。ただ、ここで僕ら標準化をやってるんですけど、儲からないんですよね、全然ね。

「サイバーセキュリティ」という語は、ITU-T X.1205 勧告において定義された。
（https://www.itu.int/rec/T-REC-X.1205-200804-I）

安藤：（笑）

門林：当然、国の研究所でやってるんで問題ないんですけど、やっぱりそういうことをITとして考えないといけないんじゃないかなあと思いますね。例えばISO/IECに関しても、メーカーの方とか国の研究所とかが人を出し合って、やってるわけですよね。それが主たる業務の人は少ないです、実は。ISO/IECに「SC 27」っていう委員会があるんですが、皆さんご存じのISMS、いわゆるISO 27000シリーズの標準化をやってるんです。アメリカもヨーロッパも同じような感じなんですよ。その27000、皆さんバイブルみたいに大事に拝んで仕事されてると思いますけれど、あれは別に何のギャランティもないんですよね。「これでやったら事故は防げます」というものではなくて、「これでやったら訴えられません」ということでもなくて、そこは何もギャランティがないんです。なぜならば、片手間だからですよね。イギリスでやっていた「BS 7799[*5]」っていうのがあって、これがいいんじゃないかっていう話で、イギリスが持ってきて、アメリカもドイツも日本も、ほかにいい提案がないからこれ呑んで標準化するか、って。そういう話なわけですよ、結局ね。

国際標準って、皆さん何か「すごい人がすごいリソースかけて作ってる」と思ってるかもしれませんけど。もちろんコストはかかってますよ。すごい人が動いてますから。年に何回も世界中でミーティングしてますし。1回で1億かかるようなミーティングもあります。ただ、そこで作ってる標準っていうのは、ギャランティはないです。ある意味「欠陥が見つかったら直しましょうというスタンスでやっているから受け入れられている」というものですよね。

安藤：中身を細かく見ていくと、2013年で大きく変わった部分がいくつかありますけどね。パスワードの扱いとかはだいぶ記述が変わっているんで、そこはやっぱり、「まずい点が出てきて変わる」っていうプロセスが正常に動いているんですよ。アメリカの「SP 800-63[*6]」も、先日、リビジョン3ですか、出ましたよね。

門林：ええ。

安藤：そこでもパスワードの扱いは、連動して動いてるんですよね、実は。アメリカで使っている標準、日本で使っている標準があるけれど、みんな同じような議論を経て、それを反映した改訂がなされている。

門林：委員会には、パートタイムなんですが、それこそ10年選手、20年選手がたくさんいるんですよ。シニアメンバーは10年選手20年選手で、標準化をやってます。だけど、誰もそれが完全だとは思ってなくて、悪かったら直せばいいよ、悪いところがあったら言ってくれというスタンスなんですよね。そこが（日本には）伝わっていないんですよ。27000にしても、多分、皆さんいろいろ一家言お持ちだと思うんですけど、それを日本のSC 27の委員会に上げているかといったら上げていない。「現場でこういう問題があります」、「困ってます」という時に、「（委員会に問題を）上げてますか？」って聞くと、多分上がってないと思うんですよね。

安藤：SC 27には上がってないですね。議論の場は他にもあるので。そこで議論した内容が、例えばIETF経由で上がっていくか、ISOのまま、そのままいっちゃうか、みたいなパスで、いろんなところから上がってくる。

あともう1つはやっぱり論文ですよね、主要な認識を変えるような論文が出てきたのを反映しているっていう流れはあると思います。パスワード変更で、「定期的な変更を強制するとロクでもないことが起こる」っていうのが統計調査の結果だと言われてますよね。その

*5 英国規格協会（BSI）が策定したISMSの規格。
*6 米国国立標準技術研究所（NIST）が作成した電子認証に関するガイドライン。

ベースはFTC（米国連邦取引委員会）の人の研究論文なんですが、そこでは統計調査をやって、まともなパスワードがつけられなくなっていくというのをちゃんと示して、その結果、定期的変更は一番エンドのユーザには課さないほうがいいよっていう結論になっている。それが、ISO 27001の2013年の変更に反映されています。SP 800-63も同じですね。紐解いていくと、ああ、この論文だっていうのはあります、ちゃんと。

大体どのぐらいの時間感かっていうと、2013年の改訂、2013年にやってるじゃないですか。その新基準に沿ったパスワードの運用方法になってきたよ、っていう記事が、昨日（編集部注：2017年5月）に出ています。こういうパスワードの運用が新基準に沿った形になってきたよっていう記事が初めて出たなと思って僕は見てたんですけど。

門林：遅いですけど。そういうスタンスなんですよね。それはもう人対人で。

安藤：しょうがないよ、だってそれだけデカイんだもん（笑）。

門林：世界中のコンセンサス形成ですから。それこそ国で反対したり賛成したりしますので。

AIとセキュリティ ― 「AIは使える」か？

編集部：AIはセキュリティにとってどのようなインパクトを持つとお考えでしょうか。

安藤：AIの話って、多分一般の人たちが思っているよりもはるかに身近で、最初に応用されたのは何かっていうと、「スパムフィルター」なんだよね。うち（BBSec）のサービスを作ったのは2005年ですが、その時点でもうAIの応用が始まっていて、スパムフィルターの中にその要素が入っていて、というところからスタートしてます[*7]。今12年たって、情報をフィードバックするユーザの数が2ケタ億のオーダーに乗るところまで来ている。そうすると、学習させるスパムのネタは十分な数があります。使ってる技術はAIだけではないとは思いますが、精度は、99.9、その下の桁で各社がつばぜりあいをやっているところまでいってます。だから、応用例としてそこまでいってる例が1つあるんだっていうことは知っておいていいかな、と。

皆さんAIという括りなもんだからあまり認識してないけど、スパムフィルターって「分類器」で、メールと

いうコンテンツを入れた時に、「それはスパムである」、「スパムでない」って分類する機械、という話です。そういう認識は持っておいたほうがいいです。

まあ、言ってしまえば、今AIっていうのはブームになってる。とはいえ、ここ5年ぐらいのスパンで新しい技術として出てきたのって、ディープラーニングですよね。それが出てきてブームになって、AIっていう言葉が20年ぶりぐらいで復活しましたというところで、みんなAIだ、AIだって言ってるんですけど、多分、応用範囲を拡張する話なのね。スパムフィルター以外でもどんどん使っていきましょうっていう動きだと思うんですよ。

「そういう見方で、横目で見てるやつがいるよ」っていうところでどうですか（笑）。

門林：クラウドもそうだったんですけど、こういう「AI」のようなバズワードっていうか、ブームになる時っていうのはいくつかの技術的なシーズが成熟してるんですよね。例えばクラウドの時は仮想ネットワークとか、データセンターとか、いくつかの技術が成熟していた。AIも、先ほど安藤さんが言ったディープラーニングっていうのは1つの要素で、例えばGPUを使った並列処理であるとか、車の自動運転みたいなアプリケーションであったり、いろんなものが複合的に組み合わさってくる。あるいは、囲碁のように、コンピュータプレイヤーが人間のプレイヤーを打ち負かして社会的な現象として取り上げられるに至るイベントもいくつかあるし、技術的なことに加え、それをサポートする潮流もいくつかあるっていうことだと僕は思ってるんです。安藤さんが言われたように、いい技術っていうのは使われる時には一般人は気にしなくていいんですね。要するにスパムフィルターもいい技術だったので、これもAIの応用なんですけど、普通の人は気にしてないんですよ。いい技術って、見えないんですよね。

実は、今話題になってるディープラーニングって、セキュリティ用途に使うとからきし効き目がないんです

*7 詳細は安藤執筆の下記論文を参照：
『情報処理』Vol.46 No.7（特集「spamメールの現状と対策の動向」）
2. 技術的側面から見たspamメール対策／2.3 フィルタリング

よ。あれは画像みたいな、多次元の連続系の情報には効くんですけど。コンピュータのデータっていうのは連続系のデータじゃないんです。要するにパターン認識できるようなものではないので。細かく言うと、「連続系」に対して「離散系」って言うんですけど、離散系なので、従来の機械学習アルゴリズムのほうが精度が高いんですね。うちの研究室でもやってみて確認しているんですが、「ディープラーニングはあんまりよくないね」という話は出ていて、これは、理論的バックグラウンドからすると当然です。

ただ、一般の方から見ると、GPUだったり、それこそディープラーニングだったり、いろんな技術革新が組み合わさった瞬間に、化学反応が起きたように見える･･･というところで、少し違和感を持って捉えられている、警戒感を持って捉えられているのかなと思いますけれど。

安藤：AIって「人工知能」って訳されるから、怖いんですよね（笑）。

門林：今、一般的に自動運転とかメールのスパムフィルターとかでよく使われているAIと称されるものはほとんど認識器、分類器なんですよ。顔画像認証ってあるじゃないですか。「ドアの前でニコッってやるとドアが開く」ような。あれって結局顔認識じゃないですか。車の自動運転も基本そうなんです。車線の認識とか障害物の認識とか。メールだと「迷惑メールの認識」っていう認識問題なんですよ。なので、推論はしてないんです。「こうだったらこう」のようなタイプの推論、これはいわゆる90年代までのAIなんですけど、そっちは全然使っていなくて、いわゆる大人の知能・子どもの知能っていう話で言うと、「子どもの知能みたいなものの、性能が良くなりますよ」っていうのが今言っているディープラーニングとかの話なんですよね。それだけであって、それこそ、「人間の知能を超える何かができる」ような話じゃないので、僕ら「オーバーハイプ」って言いますけど、バズワードが拡大解釈されている傾向にあるのかなと思うんですが。

安藤：認識器の精度が上がった、あるいは画像を正確に「これはイヌの画像だ」って言えるようになったっていう進歩、それがここ5年の進歩です、と。だけど、推論エンジンとかって20年前と何にも進歩ないですよね？恐らく。

門林：そうです。

安藤：なので、そこが全く進歩してないと。

門林：セキュリティでインシデントレスポンスとか、セキュリティオペレーションの効率化をやろうとした

時に、本当に必要なのは大人の知能なんですよ。それこそ標的型攻撃をキャンペーンとして認識するには、点と点を結びつけなきゃいけない。「ここでこういう攻撃が使われました→別のところでこういう攻撃が使われました→同じ手口が使われている→したがって彼らは同じグループだ。同じタイムゾーンで仕事をしている」みたいな推論があるじゃないですか。そこで推論なんですよね。そういう推論をするには大人の知能が必要で、そこの理論的進歩は実は全然ないんですね。

編集部：じゃあ、「AIでたくさんの人が失業する」ことはない、と。

安藤：分類を正確にできるようになって失業する人って、多分それだけでもいる。例えばトラックドライバーって、安全対策も必要ですけど、「車線をこうやって保って運転してる」っていうのがメインの職業だよね、究極に言っちゃえば。そういうところっていうのは多分一番先に「人じゃなくてもできるんじゃない？」となって、職を失うことになる。だから、レジ打ちとトラックドライバーってよく言われますね、「ここ10年でなくなるんじゃないか？」というのは。

編集部：AIがバズワードになっている背景には、マーケティング自動化の動きがあるように思います。例えば、SNSで「このユーザの写真にバスケットコートが写っているから、関連商品を売ろう」とか、これまでと違うことができると売り込むキャンペーンが盛んですよね。

安藤：「こういう傾向が出てる」っていうのを自動認識するのはある程度できるかもしれないけど、そこから次の動きを推論する、「これはこうだからこうじゃないか」って考えるっていうことはまだできていない。ただし、キラキラして見せることはできる。

門林：できますよ、それは。それこそ、Splunk[*8]の何とかのエンジンで機械学習使ってます、とか、言おう

*8 様々なITシステムから生成されるマシンデータを処理するビッグデータ分析用ソフトウェア。

と思ったら言えるじゃないですか。要するに、そういうマーケティングだと、今AIとかディープラーニングって言うとお金がつくので、そうやって商売してる方が多いということだと思うんです。セキュリティも今、「機械学習を使ってサイバーセキュリティをやる」ってスタートアップがアメリカではたくさん出てきてますし、実際それでお金もついてます。

ただ、そこの（機械学習を使う）根底は何かっていうと、「どうでもいい認識を、コストの高いアナリストにやらせたくない」。今のセキュリティー業務ではSOCの監視とか、ログが延々あるじゃないですか、SIEM[*9]にしてもIDS[*10]にしても。それは人間が見てたりするわけですよね。「本当にそこは人間がやんなきゃいけない」っていうところはあるわけですよ。

ソースコード診断にしても、ソースコードは延々何十万行もあるわけじゃないですか。その中から脆弱性を見つけるという時、本当に「人間がやらなきゃいけない」のはどこなのか。全部人間がやってたらもたないぐらいのデータ量があったりするわけでしょ。ネットワークもどんどん速くなっているし。だから、機械を使ってある程度人間の作業を本質的なところに絞っていくっていうのは不可逆ですよね。もうこの流れは変えられない。

編集部：「AIが付加価値を創出する」ということではないんですね。

門林：そうですね。セキュリティはそもそも生産性が低い業界だと僕は思っていて。機械学習を使って、それこそDoSの検知とか、研究ではいろいろやっているんですけど。ボットネットの解析とか、そういうのはもう10年来、15年来ぐらいの課題なんですよ。いろんなところにそういう機械学習なりパターン認識なりっていう技術を取り入れて対策のコストを下げていく、あるいは解析の時間を短縮していく。これはもっと皆さんやればいいと僕は思ってるんです。オペレーションの方ってそのオペレーションを回すのが精一杯じゃないですか。そこで何か新しい技術を投入してオペレーションを自動化する、とはなっていないので、そこがちょっと見ていてもどかしいところではあるんですけど。

安藤：分類器だから、「これは本当に対応が必要なものかそうじゃないか」ぐらいの勢いで分類はできるわけですよ。人間はその対処が必要なほうだけ見ればいいっていう使い方ですよ。でも、最後の判断は人間ですよね？

門林：そうです。人間が持ってる嗅覚、すごいですよね。縮退した情報というか、膨大なログとかからの情報を少しずつオペレーターに見せても、おかしいって思った瞬間、気づくんですよね。人間のメタ認知能力はすごいなと思います。あと、そういう認識を機械に任せられると人間は本来すべきことに集中できるじゃないですか。例えば、コーディネーションなんかそうですね、お客様に電話してとか、現場行って対応してとか。そっちの調整であるとか、そのほかの業務との連絡とか、そういうところは本当に人間にしかできないので。

実は、セキュリティの現場って非常にクリエイティブでなければいけないと思っていて、これはロンドンオリンピックでCERTをしていた人たちの言葉なんですけど、彼らは「インシデントレスポンスはinventive（発明的）でなければいけない」と話していました。敵も人間じゃないですか。なので、いろいろ手を変え、品を変えやってくるわけですよね。その時に、次にこうきたらこの製品でやろうかとか、この製品の使い方を変えてやろうとか、このチームを配置転換してやろうとかっていう、いろんなinventiveな方法があると思うんですよ。

編集部：「やり方は柔軟に、トライ＆エラーも含めたいろんな判断を交えながら人間ならではの部分に英知を集結すればよい、プロセスとして自動化できるものは効率的にAIなりにやってもらおう」ということでしょうか。

門林：気が利いたITサービスプロバイダさんは、AIを何らかの形で使われてますよね。いろんな機械学習のアルゴリズムを使って、それこそログの解析を効率化したり、いろいろやってらっしゃいますよね。これはセキュリティサービスプロバイダとしては避けられない流れだと思いますね。

安藤：人がかかるところにどうやってうまく使って効率化していこうかっていう、その一環で始まるんですね。

編集部：例えばですが、一般企業の経営者や意思決定者がAIのサービスを売り込まれた場合、どういう点に気をつければいいのでしょうか。

安藤：ものすごい簡単な指標を1つ挙げるとすると、「そのAIの判定精度を聞いてみる」のがいいんじゃないかな。99%なのか、99.9%なのか、99.99%なのかのあたりで聞いてみることで、それがどのぐらい使える

*9 Security Information and Event Management。ソフトウェアが出力するイベント情報を一元的に収集して分析することにより、脅威や攻撃への対応を支援するシステム。
*10 Intrusion Detection System。ネットワーク上のパケットを監視し、不正侵入を検知するシステム。

かがわかるよね。スパムフィルターでは99.9をクリアするまではほとんど使い物にならないと思われてた。だけど、今の精度っていうのはちゃんとスパムがスパムフォルダに区分けされてて、メールが健全に使えるところまでいってますので、実用になってるわけですよね。だから、そこで完成度を聞くのがいいと思う。

編集部：小数点第3位レベルとか？

安藤：小数点第3位までいってるAIの応用って、残念ながら厳しすぎるので、昨今AIを使ってこういうふうなものを作りました、っていうところには98%ぐらいですかね（笑）。そのぐらいから始めたほうがいいと思いますけど。

編集部：それぐらいで「実用に耐え得る、しっかりした回答ができるデータがある」と評価できるわけですか。

安藤：必要なデータがあればね。開発する人は必ずそれを意識してやってるはずなので、どのぐらいの認識精度でその分類ができるんですか、と。「人の手を煩わせる作業をこうやって半分機械にやらせて」というケースでもある程度の精度は必要なので、そこから聞いてみるのがいいんじゃないかな。

門林：結局、分類とか認識作業じゃないですか。認識作業を機械で置き換えますっていうだけの話なんですよね、AIって言っても、突き詰めると。ただ、99.何%、いいところでそこまでなんですよね、ディープラーニングでやったとしても。「サポートベクターマシン」とかいろいろありますけど、95%以上は出る。その残りの1%なり5%なり取り逃したものを人間がハンドリングしないといけない。「それがどれぐらいのコストなんですか？」っていう話なんですよね。

安藤：AIだけでやろうとすると、学習モデルをどう拡張するんですかっていう話になります。だから、ただ「AI使いました」って言うだけだったら30年ぐらい前からあるベイジアンを持ってきて、使ったよ、って言えば使ったことにはなるんですよ。だけど、本格的な応用でどこまでいってるんだっていう話をする時には、認識率がどのぐらいで、もうちょっと言うと　ーフィルターの話と同じですけど ー 誤検知がこれだけ、過検知がこれだけ発生しますというところまで見て、初めて本物って話になる。

門林：結局、イヌの画像を見せて、「これはイヌです」って、人間が教えなきゃいけないわけです。だから、「クラスラベル」って言うんですけど、AIに教え込むための人間の工数はかかる。「これがスパムです」、「これはスパムではありません」というのを延々やらなきゃいけないわけじゃないですか。それがある程度母数がたまらないと精度も出ないし、スパムもどんどんパターンが変わりますから、そこの工数はすごくかかるんですよね。

編集部：例えば、いろんな種類のイヌがいる中で「これがイヌだ」という特徴を抽出して、抽象化しなければならないですよね。

安藤：ディープラーニングが勝手にやってくれるんで。

門林：ただ、オペレーターさんがいて、「これ、イヌ。これ、ネコ」ってやんなきゃいけないわけじゃないですか。延々やる人が必要なんですよね。

編集部：「相当なパターンを入れないと誤認識する」という。

門林：そうです。そういうデータがそもそもあるものだったらいいですけど、ないものだったら作らなきゃいけないですから。

安藤：確かGoogleでは、数十万枚の画像を認識させて、このぐらいの精度が出ますっていう論文が最初出たんですよね。だから、ディープラーニングでも、やっぱり最低でもそのぐらいは必要ですよという話ですよね。「イヌとそれ以外を取り混ぜて数十万枚画像を用意できますか？」という。

門林：AIの応用という時、大体最初に偉い学者先生を連れてきて、じゃあ、これやれって言ってやらせるじゃないですか。そこで最初に騒ぐのは「データがありません」って話なんですよ。要するに、ラベル付きデータがいるんです。「これがDDoSです」、「これはDDoSではありません」みたいなラベルを付けたものを提供しないと、彼らは分析精度も何も言えないんですよね。

編集部：ただデータがあればいいわけじゃない、ということですね。

門林：はい、そうです。

編集部：そのラベル付けは人間でないとできない。

門林：そこがコストなんです。

安藤：そういうところも考えると、スパムフィルターに応用したっていうのは大正解だね。とんでもない数が来ますし、人間が判断して、これスパムだったらレポートしてくれます、っていうところからスタートしたから。うまかったと思いますよ。

編集部：私たちユーザは、全く意識しないでメールを使っています。

安藤：皆さん、スパムフィルターの中にがんがんAIの

要素が入ってるなんて夢にも思ってない（笑）。

IoTとセキュリティ ― 脅威か？機会か？

編集部：IoTについては、どうお考えでしょう。

安藤：IoTっていうのは、実はデータをめちゃめちゃいっぱい生み出すフレームワークなんですよね。じゃあそれをどうやって処理していくんだ、っていうところからAIと結びついて発展が期待される分野になってる。技術のフレームワークとしてデータをそんなに大量に生み出した時に人間がそれを全部見ていられるか？　見ていられません、と（笑）。そこでAIの応用、っていうところで始まっているんだけど、「じゃあIoTの足回りってセキュリティどうなの」っていうのが心配なんじゃないですか。上のほうはAIで何とかすると考えておいていいかもしれないけど、でも、元のデータ化するところを嘘つかれたらどうするの？っていうところでセキュリティが必要になる。そこで、IoTのセキュリティも徐々に問題化してきている。

門林：IoT、そうですね。「IoTのセキュリティ」って、もちろん、IoTそのものの安全性に対する懸念っていうのもありますけど、IoTを使ったからこそできるセキュリティもあるんですね。両方あると思っているんですが、ほとんどの技術的な議論は前者なんですよ。「IoT、大丈夫なんですか」って皆さん聞かれる。クラウドの時もそうでした。「クラウド、これ、大丈夫なんですか、使って」って聞かれます。でも、実際にはクラウドを使うとサーバって1秒もたたないで作り直せるんですね。なので、やられたら作り直したらいいじゃない、っていう発想ができるようになったんですよ、クラウドのおかげで。

これはレジリエンスですよね。レジリエンスの1つの実現方法です。これがDockerとかのコンテナ技術を使ってできるようになった。これはすごいことなんですよ、実は。IoTでも恐らくそういうことが起きると思っています。IoTだからこそ、「何か1個落ちても大丈夫だよね」とかね。あるいは、部屋そのものが認証装置になっていて、この部屋の中に安藤さんがいることがわかっていて、かつ、安藤さんのMacがこれだってわかっていた場合、「この部屋に居るから、安藤さんは、この操作ができる」と言える。そういう、場所に紐付いたようなこと。例えば、「サーバルームに行かないとできない操作」とか「経理部門に居ないとできないような操作」とかあってもいいと思うんですけど、今の認証ってそうなってないんですよ。場所とか文脈の情報とかを全く考慮しないで、ID・パスワードで認証するじゃないですか。でも、本当は、ハイリスクな操作や会話をするっていうのは、それなりの場所なり文脈なり、周りの環境っていうのがあるはずで、そういうのを考慮したようなセキュリティっていうのが考えられるんですよね、将来的には。今、たまたまそれが2要素認証っていう形ですごく不便に実装されています。「あなたはこれを持っています、USBを挿します、あなたはパスワードを知っています、したがって、あなたは確実にあなたです」ーこういうのが2要素認証なんですけど、すごく不便ですよね、挿さなきゃいけないから。最終的には、部屋の中にいろいろ、それこそ、蛍光灯が何かがIDを出していたり、Bluetoothで壁に埋め込まれていたり、そういう情報を総合的に勘案して、「ここに居るのは安藤さんです」と言えるような形になると思うんですよ。要するに乗っ取りができにくくなる。

編集部：「IoTとセキュリティ」と聞くと、「乗っ取られたらどうしよう」とばかり考えていました。

安藤：多要素認証じゃなくて、「多人数ドメイン認証」があってもいい。「ここに座ってるのは安藤だよ」ってみんなわかってるから不思議に思わないわけで、怪しいやつが来て、ここで何か操作してるとなったら、みんな怪しいと思うわけだよね。そういう認証があったっていいわけですよ、仕組み的には。

門林：リアルなセキュリティとサイバーのセキュリティを紐付けることに成功してないんですよ。だから、どこかから入ってきて、ファイルをパクられるわけですよね。でも、リアルのセキュリティと紐付けることによって、それができにくくなるんじゃないかと。

安藤：この部屋のこの席にいて、PCをいじってる、このIDでログインしてる、顔認識したら安藤ってやつだ、合ってるからOK、みたいな。

編集部：一種のパラダイムシフトにも思えます。

安藤：でも、昔から、「じゃあツケといて」って顔でやってるわけでしょ。みんな分業化して、通信のところから何とかしようとか、デバイスから何とかしようとか考えてるけれど、そうじゃないですよ、と。例えば、監視カメラの画像から、振る舞いがおかしいって検知する仕組みは実用化されているよね。だから要素技術はできている。走ってるとか、転んだとかいうのが検知できる仕組みはもうあるわけです。それを銀行の現場に取りつけた時に、「こいつ、いつもと違うことやってる」というのはわかりますよ。

門林：ただね、ATMを作った時は横領できそうな機会を減らすとか、そういう意図があったわけじゃないですか。それでATMを作ったわけでしょ。でも、やっぱ

り、ATMごとフォークリフトで持って行ってしまうような、いろんな攻撃があるわけですよね。

とはいえ、それでも僕はIoTの可能性に注目するべきだと思っています。危険性ばかりが言われるんですけど、それだと全然、経済的インセンティブが働かないんですよ。誰も作り直そうと思わないし、結果として、「LinuxをRaspberry Piに入れて」とか、何か高校生の工作のような話でIoTとか言ってるのがほとんどですよね。それは経済的インセンティブが働かないからですよ。イノベーションすることによって、巨大なマーケットがあるんだ、っていうのをみんなが認識して、「これはもうOSからしっかり作り直そう」とか、「無線もいいことだからどんどん無線使おう」とか、ポジティブに考えていいと思うんですよね。

安藤：今は入退室管理って認証のシステムと全く結びついてないでしょ。Active Directory構築しましたって言っても、入退室管理とは全く結びついていない。部屋に居ない人がログインしても、おかしいと思わないんだよね、システムは。だから、それをもうちょっと拡張すると、自宅からログインしましたっていう、「この人の自宅だから」っていうことがわかるようになるとかね。そういう世界が来てもいいわけですよ。

編集部：それを阻んでいるのは何でしょうか。

安藤：分業。俯瞰して融合させようっていう動きが弱い。

門林：でも、僕は可能性があると思っていて、例えばモバイルOSってどんどん変わってるじゃないですか。それこそAndroidとかiOSとか、どんどんイノベーション進んでますよね。モバイルはお金、マーケットインセンティブがあるので、彼らはイノベーションをどんどん続けてますよね。2要素認証も結構積極的に導入してるし。モバイル系のプレイヤーが中心になってIoTのエコシステムでもイノベーションを起こすんじゃないかなと思ってます。皆さんご存じないかもしれませんけど、2要素認証のスタンダードを作っている「FIDOアライアンス」っていう団体があるんですが、そこの人たちは多分、次はこのUSBで挿すとかじゃなくって、無線とか、そういうのを考えてると思うんです。Appleもそうじゃないですか。iPhoneか何かを持っていくと自動的にロックがはずれるとかありますよね？

安藤：あります。電波をどうやって有効利用しようか、持ってるデバイスをどう有効利用しようかっていう話でいくわけですね。だけど、オフィスの中にこうやって入ってきて、認証、セキュリティにまで応用しようっていう発想には、彼らもまだなってないだろうと。残念ながら。

門林：そこら辺は割とスマートシティ的な話なので、どっちかっていうと日本のメーカーさんのほうが強いんじゃないかなと思いますけどね。

安藤：いや、でも、こうやって使おうとすると、こう悪用しようって考えるやつもいるわけで、例えば自動車のキーレスエントリー。キーを持ってると鍵開くよ、っていうやつ。あれ、破られたよね。たった20ドルのデバイスで。どうやったかっていうと、キーの電波を中継する装置を持って、1人がドライバーについて行って、中継して、鍵開けちゃう。車上狙い簡単にできるよ、っていうのがこの間明らかになってましたけど、今のIoTの認証も同じことができない？ 1人、そういうデバイス持ってる人について行って、中継して、悪いやつがここで何かやってる、みたいなことできちゃうでしょ。悪いやつは考えると思いますよ。

自動車のキーレスエントリーは、既に傍受手法が確立されている。

編集部：何歩か先を読み「こんな悪いやつが出てくるだろう」ということを想定する力、ということでしょうか。それはなかなか育成しづらいのではないかと思いますが。

門林：いや、でもそれは、見た場数だと思いますよ。だからそのためにBlack Hatなんかにお金を払って毎年行くべきだと思います。FIRST[*11]だったり、非公開の会議にもどんどん出て。

安藤：事例をどれだけ知ってるか。過去の事例でどれだけこういうのがあったかっていうのを詳しく知ってるかで想定力の幅が大幅に変わる。攻撃側も過去の事例は調べているはずで、多分同じ技量なんですよね。同じ技量だけども、攻撃側の上前をはねて想像ができて対応ができる、こんなこともあろうかと想定できるということですよ。

門林：サイバーセキュリティって、いまだに皆さん、「原理原則で何とかなる」と思ってる人もいるんです。PDCAだとか。

安藤：（笑）

門林：最近だと、「OODAループ[*12]で何とかなる」と

*11 Forum of Incident Response and Security Teams。セキュリティ対策の共有、連携を目的として1990年に設置された国際的なフォーラム。

*12 米海軍で開発された意思決定手法。観察（Observe）−情勢判断（Orient）−決定（Decide）−行動（Act）というループを繰り返すことによって迅速・的確な意思決定を促進する。

か言ってる人がいますけど、その原理原則だけ覚えて何とかなるものじゃなくて、これ、ボキャブラリーなんですね、「語彙」。どれぐらい場数を踏んだか、どれぐらいのケースを見て、詳細に分析したかだと思うんですよ。「ボキャブラリーが大事だね」っていうところがわかっていなくて、何か原理原則を吹聴して回る人が多いですよね。「OODAループで弊社もいきます」とか（笑）。

編集部：「ボキャブラリー」とは、具体的にはどういうことでしょう。

門林：例えば、東京を語ろうと思ったら、「新宿通りがあります。新宿通りも四谷のあたりは上智大学があってちょっと瀟洒な感じだけども、新宿まで行くとかなり雑然とした感じになります」と言える。今、IT業界そのものがすごく発達していて、何か路地とか通りみたいになってるんですよね、地図で言うと。それぞれに具体的なリスクもあるし、可能性もある。Pythonだったらこうとか、Javaだったらこうとか、Web系はこうとか、組み込み系はこうとか、各論がいろいろあるわけじゃないですか。それぞれの路地をどれぐらい歩いたかだと思うんです。「ボキャブラリー」というのは僕の例えですけど、それぞれ言葉が違うので「語彙」が要るんです。

テクニカルな、ごちゃごちゃとした違いを無視して、原理原則で語ろうとする人は必ずいて、頭がいい人って必ず還元論で語ろうとするんですけど、僕はサイバーの話っていうのは還元論で語れるところって本当に限られてると思うんですよね。

安藤：例外だらけなんで、そんな原理原則でやっただけじゃ抜け穴だらけなのができるだけです。

編集部：なるほど、耳の痛い話ですが、原理原則に固執していては今後ますます激しくなるサイバーの脅威に対応できない、ということですね。

― 原理主義に陥ることなく、色々な現場に飛び込んで分野横断的に語彙を身につけ、表層的な変化に惑わされず事の本質を見据える。これからのサイバーセキュリティを考えるヒントをいくつもいただけたように思います。本日は長時間有難うございました。

対談を終えて

サイバーセキュリティからAI、IoTまで縦横にディスカッションさせていただきましたが、これらの先端領域に共通することは「正解がない」ことと「技術の動作原理が分かっていないと、結局はどうにもならない」ということではないでしょうか。対談で言ったことも、イノベーションの結果として半年後に陳腐化している可能性すらあると思います。

最近の例で言えばビットコインがそうでしょう。貨幣経済の世界にもいよいよインターネット技術の襲来かと思われたビットコインですが、取引高の急拡大にともない分裂する事態を招いています。ビットコインがなぜ分裂に至ったのか、という点については技術の動作原理が分かっていないと理解することができません。

今後ますます技術の蓄積が進んで、技術の動作原理が分かっていないと社会現象の理解に苦しむケースが増えることでしょう。対談形式で、過渡的であっても、たとえ不完全であっても解説を試みることは、多くのステークホルダの皆様にとって有益なのではないかと今回あらためて感じました。業界全体でサイロ化が静かに進行する中で、「もともと一緒にやっていた人たち」のつながりを掘り起こして、今こそ大いに対談し、自由な発想をすべきではないかと思う次第です。

門林 雄基

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

技術が高度化して分業が進んで、一方で全体を俯瞰できる者がいないという状態は、技術的なデマや煽りに対して大変脆弱だと言えます。

その分野しか知らない人にはよその分野になると真偽を知る術がなく、簡単に騙される・付け込まれる要素が分業やサイロ化で構造的に作り込まれてしまっているように見えます。逆に言えば、動作原理からきっちり理解してる人がどれだけ組織の中にいるかが組織のレジリエンスを構成する鍵になっていくような気がします。「セキュリティは生涯学習だ」という言い方も多分そこらへんに絡んでいるのではないでしょうか。

安藤 一憲

TREND

情報セキュリティの脅威と動向

株式会社ブロードバンドセキュリティ セキュリティサービス本部 副本部長　齊藤 義人

2017年上半期、情報セキュリティに関する大きなニュースが立て続けに起きていたのは、皆さんご存知のところかと思います。次々とインパクトの大きな話が舞い込んでくるため、それ以前に起きた事件・事故が薄らいでしまう。当事者以外にとっては、そういうものでしょう。Aの対応が必要か否かを調査している最中にBが発生し、「Aより優先してBに対応せよ」との指示に現場はてんてこ舞い。こういった苦労も漏れ聞こえてきた半年でした。

「セキュリティ界隈が大騒ぎでした」以外の書き出しはないものかと、記事を書くたびに思います。それでも、いつか落ち着く時が来ることを信じて、気を取り直していきましょう。

Apache Struts 2 の脆弱性（S2-045、S2-046～S2-048）

まず挙げておきたいのは、Apache Struts 2の脆弱性が悪用された事件・事故です。3月8日、独立行政法人　情報処理推進機構（IPA）のWebサイトや、JPCERTコーディネーションセンター（JPCERT/CC）の早期警戒情報で、この脆弱性に対する注意喚起が発せられました。被害にあったサイトを以下に例示しますが、多様なサイトが影響を受けていることがわかります。

早くに対策に乗り出したサイト運営元もいましたが、残念なことに、攻撃は注意喚起以前から発生していたため、既にバックドアを設置されるなどの被害が起きていました。これは、「3月6日にApacheサイトでS2-045の情報が公開された翌日には、この情報を元にした攻撃コードが出回ってしまった」背景によるものです。

◇ 運輸・郵便会社　マイページサービス
◇ 独立行政法人統計センター「地図による小地域分析（jSTAT MAP）」
◇ 民間放送事業者　音声配信サービス★1
◇ 重要インフラ会社　情報公開サービス
◇ 娯楽サービス会社　ファンクラブ受付サイト
◇ 流通会社　オンラインショップ
◇ 東京都主税局「都税クレジットカードお支払サイト」
◇ 独立行政法人住宅金融支援機構「団信特約料クレジットカード払いサイト」
◇ 独立行政法人工業所有権情報・研修館「特許情報プラットフォーム（J-PlatPat）」
など

★1 こちらは再開せずサービス終了となりました。

セキュリティ情報の開示は、これまでにも幾度となく議論されてきた課題の1つです。脆弱性の情報を伏せてアップデートを提供し、一定期間後に情報開示する方法や、セキュリティ対策パッチやアップデートのリリースを事前に通

知し、ユーザへ準備を促す方法が、様々なベンダでとられつつあります。前者は、情報を伏せていたとしても、アップデートによる差分が分析されてしまえば、攻撃コードが作成される可能性が高まります。その点では後者がオススメといえます。

各サイトの対応について

また、被害にあった各サイトでのセキュリティ情報開示から調査・対策までの期間はまちまちで、情報開示から1～2週間後に対策したものの、それまでの間、情報漏洩し続けたケースが幾つもありました。中でも、総務省管轄の「地図による小地域分析（jSTAT MAP）」は、4月11日にサービス停止と、公表から1か月遅れての対策となっています。サービス継続は事業にとって最も重要なことの1つです。しかし、何れにせよセキュリティ対策をとるための時間や工数・費用が割り当てられない、優先度が低い、そもそも見込んでいない、という実態が変わらなければ、同じことが繰り返されることになるでしょう。過去にもApache Struts 2の脆弱性に起因する攻撃を受け、その際に対策を講じたにもかかわらず再び被害を被った組織も1つならず存在しました。担当者のリスクに対する意識は高かったと思われますが、担当者以外の社内ステークホルダーへの連携や事業継続計画については、発展途上だったのかもしれません。このほか、対策後に再開予定と発表していたものの、どういった対策をとったのか不明のまま再開されているサイトがあります。セキュリティリスクとなり得る情報について公表する必要はありませんが、調査結果（影響範囲・実施した対策・今後の方針）を開示できないのか、しないのか判らないサイトは、トップダウンの意思や指示が見えず、また同じことが繰り返されるのではと心配でなりません。

攻撃ターゲットの選定

ところで、攻撃者はどのようにターゲットを探り当てるのでしょうか？

Apache Struts 2で構築されているであろうサイトのURLは、拡張子に「.action」が用いられる特徴があります。Googleで「.co.jpドメインで、.action拡張子のサイトを探す」ことは簡単で、Googleの検索ウィンドウに「site:.co.jp filetype:action」と入力して検索するだけです。この応答結果で得られた各サイトに対して、機械的に攻撃リクエストを仕掛けるのは、ほんの数十行のプログラムで実行できてしまいます。実際は、すぐに攻撃を仕掛けるのではなく、脆弱性が存在するかどうかを調査するだけのリクエストから始まるのですが。このような、一般公開されて利用可能な情報源をもとにした諜報活動/情報収集のことは「OSINT[★2]」と呼ばれています。OSINT Search Tool（inteltechniques.com）などが有名なツールとして存在します。Googleなどを一括検索できるツールです。ぜひ試してみてください。得られた情報と分析結果を元に、正しく意思決定へ展開・活用するには、認知バイアスの排除など特有のトレーニングが必要な領域であるとは思いますが、有効活用できるに越したことはありません。OSINTについては、また別の機会に紹介できればと思っています。

[★2] open source intelligence

このように、情報を容易に収集できる状況は、守る側も攻撃する側も同じことです。そして、情報収集のスピードが速まるにつれ、セキュリティ対策の猶予期間が短くなっていることは、お分かりいただけるかと思います。以前（数年前～昨年かもしれません）に想定していたよりも安全側に倒してシステム構築・運用することを、頭と心の片隅に置いていただきたいと思います。今後のリスクアセスメントでは、多層防御ソリューションを検討することはもちろん、サービスの緊急停止ルールや、不安視されるシステム（例えばApache Struts 2）を使わない/切り替えるという選択が追加されても、まったくおかしなことではないのです。

世界に広がるランサムウェア/ワイパーウェア

5月14日、IPAの記者会見から「世界各地で発生している大規模なサイバー攻撃」を知った方は多いのではないでしょうか。ある種の大騒ぎとなったわけですが、セキュリティ/システム担当者は、報道を横目に粛々と対応している。そんな１日でした。

何が起きていたのか？

この日、世界規模の感染キャンペーンに用いられた「WannaCry」は、Windowsを標的としたワーム型ランサムウェアです。簡単に感染の流れを追うと、次のようになります。①ローカルネットワークのIPアドレスとランダムなIPアドレスをリストアップし感染のターゲットとします。②ターゲットとなったシステムへTCP 445番ポートで接続し、攻撃コードを含むServer Message Block（SMB）★3パケットを送りつけます。③「DoublePulsar★4」に感染している端末であれば、このバックドアを用いて「WannaCry」への感染を試みます。「DoublePulsar」に感染していない場合は、「MS17-010」の脆弱性を利用して「DoublePulsar」に感染させ、やはりバックドアを用いて「WannaCry」への感染を試みます。④「WannaCry」に感染した端末のローカルファイルやネットワーク共有ファイルを暗号化して使用不能にします。

★3 主にLAN内でのファイル/プリンタ共有などに使用される通信プロトコル。通常であれば、インターネット側へ公開する必要はありません。

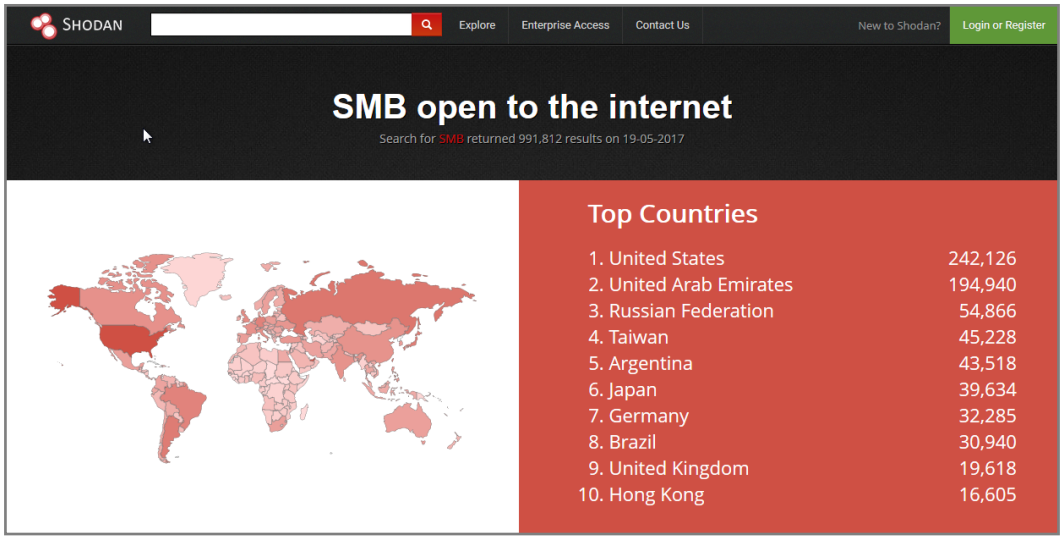
★4 「NSA（米国家安全保障局）」から流出した情報に含まれていたバックドアツールです。「NSA」つまりアメリカ政府が脆弱性を秘密にしていたことも大きな問題になっています。

当時、Microsoft提供の「MS17-010」対応パッチを当てることが対策として案内されましたが、周辺情報が不十分だった印象があります。例えば、既に「DoublePulsar」へ感染している端末は、パッチを適用した場合でも、③のとおり感染するわけですが、「感染状況をチェックすること」は表立って注意喚起されていませんでした。また、②のとおりTCP 445番ポートが空いていない場合は、「WannaCry」に侵入されません。つまり、不要（判断は難しいかもしれませんが）であれば445番ポートを閉じること、また、インターネット側に445番ポートを開放しない★5ことも効果的な防衛策でした。とくに本件では、メール経由の攻撃が確認されておらず★6、「まずは、侵入経路を塞ぎましょう」と、もっと早くに発せられるべきだったと思います。「ランサムウェア」という単語から、反射的にメール添付ファイルへの警戒を呼びかける誤解もあったようで、混乱が広がったように見えます。

その昔、世界中で広く用いられた暗号化方式「DES」には、必ず用いられるテーブルが存在しますが（ここにも「NSA」の関わりが！）、なぜソレなのか？について説明がなされないため、「アメリカ政府だけがこっそり解読するための仕掛けなのだ！」と《使用しない宣言》をする方がいました。信じるか信じないかは・・・

また、6月に発生した「Petya亜種」についても、情報が錯綜していました。当初、ランサムウェアとして報道されましたが、実態は解除キーの存在しない（身代金を払ってもデータ復旧できない）、破壊を目的としたワイパーウェアであることがわかっています。支払い後の連絡先として指定されていたメールアドレスも、すぐに利用不可になっていたため、初めから終わりまで「支払い損」な事件でした。

これらの件をうけて、まず「何が起きているのか」を正しく知る/伝えること★7が、セキュリティ界隈の



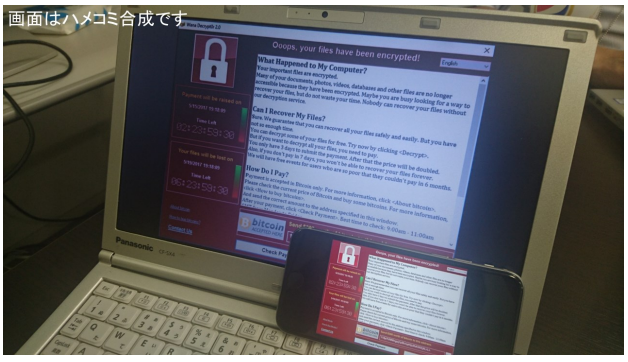
【インターネットへのSMB開放】

課題であると、改めて実感しています。とくに、警戒すべき脅威ベクタを見誤ることが無いようにすること、注意していきたいと思います。

★5 Web検索サービス「SHODAN」によると、５月時点の日本でも約４万の端末がインターネット側に445番ポートを開放しています。（上図参照）。

★6 メール添付された「WannaCry」を実行しても、（設定変更していなければ）ユーザー・アカウント制御（UAC）が起動するため悪用されにくい。

★7 感染後の画面が特徴的なこともあり、偽情報の画像が多く出回りました（下図参照）。



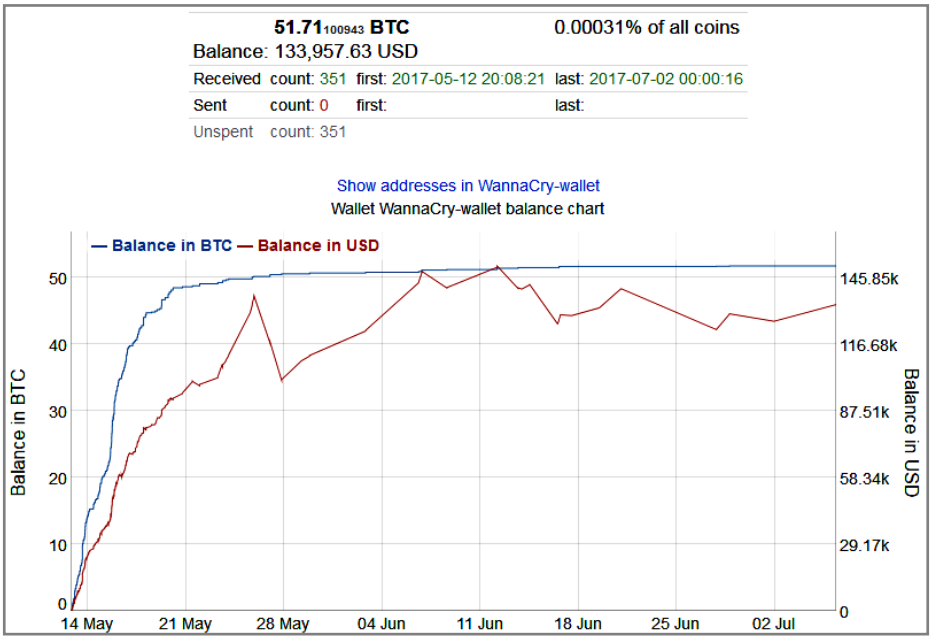
【感染後の画面イメージ】

サイバー犯罪はより容易に 対応はより困難に

さて、これらのランサムウェア/ワイパーウェアで、どれくらいの支払いが発生していたのか。皆さん気になりますね。過去、マルウェア作者は、感染させた端末の情報を得て、ブローカー（インターネット上にこの手のサイトが点在していました）に販売し金銭に換えるという動きをとっていました。しかし現在は、仮想通貨の一種であるビットコインを用いることで、より手軽にサイバー犯罪が起こりうる状況になっているといえます。「WannaCry」では３つのビットコインアドレスが指定されていました。この支払い状況をみてみますと、7月にも発生しており、51.71BTCに到達しています（次ページ図参照）。これは日本円で約1500万円に上るものです。

つい先日（8月）、WannaCryの拡大を阻止したハッカーが、過去にマルウェア作成に関与したとして逮捕されました。「DEFCON」帰路の出来事のため、後日「DEFCON」ですべきことに「FBIに起訴されること」を挙げるあたり逞しい。

ランサムウェアに感染した場合、要求通りに身代金を支払うべきか否かという論点があります。そもそも、支払ったものの、本当に暗号化が解除される保証もありません。過去に、病院で救急患者の情報がロックされてしまった際、身代金を支払った病院の対応に非難があがったことがありました。この身代金が、他の犯罪の資金となり、最終的により多くの犠牲を生むかもしれないからです。ただし、それでも、非難で終わるべきではないと、私は考えます。（セキュリティ対策が不十分とか、バックアップをとっておくべきだったとか、指摘すべき点はいくつもありますが）



【WannaCryのビットコイン】
（URL：https://bitinfocharts.com/bitcoin/wallet/WannaCry-wallet）

正しい指示のもと、正しく行動し、どれだけ正しく機能していても、インターネットの世界では、悪意との対峙は避けられません。悪意そのものというよりも、悪意や敵意、好奇心に影響された「うねり」のようなものかもしれません。そして、私たちは、ある日突然「うねり」に飲み込まれます。始まりは極々小さな一滴が水面を揺らす程度でしょう。この予測は困難で、被害が顕在化して初めて気付くのです。

資産の棚卸し、優先順位づけは、当然、皆様されていると思いますが、有事に何を「切り捨てる・犠牲にする」まで、議論・検討は進んでいますでしょうか。簡単に答えの出る問題ではありませんが、それでも、いつか答えを出さざるを得ない日に向けて、備えてゆきましょう。

もちろん、私たちブロードバンドセキュリティがサポートいたします。

齊藤 義人
Webアプリケーションを中心とした開発エンジニアを経て、官公庁および大手顧客向け脆弱性診断・ペネトレーションテストに従事。
数年に亘る長期かつ大規模システムのプロジェクトマネジャーとして活躍。
企業のセキュリティ担当者向けセミナーにおける講師経験も豊富で、解説のわかりやすさには定評がある。

- CISSP取得
- セキュリティスペシャリスト・システム監査技術者・ITストラテジスト・ネットワークスペシャリスト
- JASA 公認情報セキュリティ監査人補

TOPIC

韓国カードセキュリティ最前線

株式会社ブロードバンドセキュリティ 韓国支店 支店長　朴 宰範
同 セキュリティコンサルティング本部 取締役本部長　雲野 康成

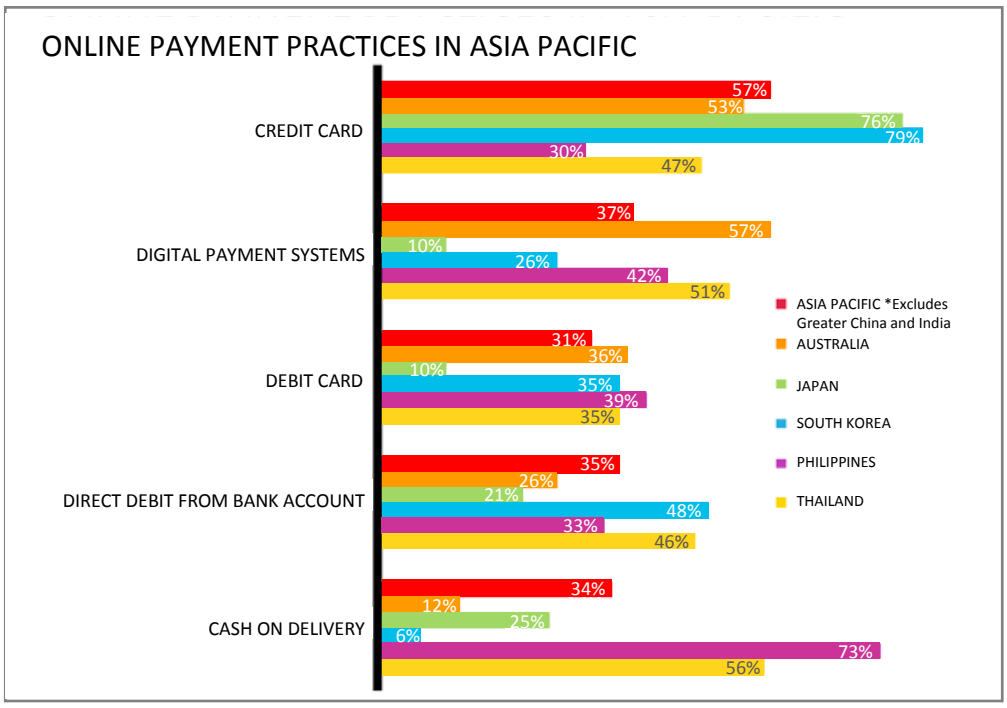
BBSecは2012年に韓国支店を設立した。現在、同支店が展開するPCI DSS事業は韓国市場の70%をカバーし、同国内のトッププロバイダーとして圧倒的な実績を上げている。本稿では、2018年平昌オリンピックを目前にした同国のセキュリティビジネスをめぐる動きを、当社の取り組みを交えて紹介したい。

「クレジットカード大国」韓国

韓国は、実は「世界有数のクレジットカード大国」である。クレジットカードの決済が租税公課の仕組みにも取り入れられ、コンビニでの買い物や平日のビジネスランチに至るまで、少額決済においてもクレジットカード決済が当たり前。普及率は90%を超える。そんな同国で2013年、当時世界第3位の規模と言われる漏洩事故が発生した。流出したのは1億件ものカード情報で、実に韓国人口の2倍の数に達する。社会を大きく揺るがす一大事件となった。

これをきっかけに、韓国では、それまで進展が見られなかったカードセキュリティ標準策定の動きがにわかに活発化した。そこでベンチマークとされたのが国際標準PCI DSSであり、世界的カードブランドのVISAが標準化の推進役として中心的な役割を果たしている。BBSecは、こうした動きと前後して、翌2014年に同国でPCI DSS準拠の支援・監査を行えるQSA資格を取得。業界に先駆けてPCI DSS認証取得サービスを開始した（現時点で、韓国全土には11名のQSA有資格者がいるが、うち4名がBBSec韓国支店の社員）。

そうした取り組みの最中、追い打ちをかけるようにまたもや大規模な漏洩事故が起こった。2016年7月、韓国を代表するチケット販売大手INTERPARKのシステムから、1千万件強に及ぶ個人情報が流出したのである。INTERPARKでは、平昌オリンピックのチケットも大々的に取り扱っている。カード事業者に対する信頼性が揺らぐ中、オリンピックの開催は待ったなしである。セキュリティ体制の構築はまさに喫緊の課題となった。



■ アジア太平洋地域におけるオンライン決済普及率
出典：Nielsen Company「Nielsen Global Connected Commerce Survey, Q4 2015」

複数のドライバーで標準化が加速

2013年の事故以降、次のような推進要因が相次いで登場し、標準化の動きはさらなる加速を見せている。

1) VISAのPCI DSS準拠推進

VISAは、VISA NET（VISAが運営するグローバルな決済ネットワークのこと）のセキュリティを確保するために、韓国内の決済事業者にPCI DSS認証取得を勧告した。カード会社、VAN（Value Added Network）事業者、PG（Payment Gateway）事業者は、VISAとのビジネスを維持継続するために、認証取得に動かねばならない。

2) 簡単決済事業者の承認基準

2014年、与信金融協会の簡単決済事業者の承認基準としてPCI DSS準拠認証が勧告された。PCI DSSは、簡単決済事業の構造に応じてセキュリティ脆弱性対策を補完するためのツールとして位置付けられている。

3) グローバルなビジネス展開

PCI DSSが、決済事業者が海外事業に進出する際の必須条件となった。同様に、韓国内に進出したグローバル企業が国内決済事業者を選定する際の基準としてもPCI DSSが使われるようになっている。

そして、2016年11月、韓国初のPCI DSS準拠企業がついに誕生した。サムスンカードである。2017年5月現在の状況は以下の通り。

	カード会社	VAN（推定）	PG（推定）
準拠認定済	1社（サムスンカード）	14 社	15 社
準拠推進中	7 社	-	3 社
準拠準備直前	2 社	-	5 社

カードセキュリティの標準化は官民挙げての取り組みではあるが、その牽引役となっているのは、名実ともにVISAだといえよう。そんな中、同社がグローバルに実施している年次イベント「VISA Security Summit」が、本年は韓国ソウルで開催され、BBSecもスポンサーとして、展示や講演等を行った。以下、そのハイライトをお伝えしたい。

VISA Security Summit 2017 in Seoul

VISAワールドワイド（以下、VISA）は、毎年5月、アジア太平洋各国で「VISA Security Summit」というイベントを開催している。一昨年はオーストラリア シドニー、昨年はタイ バンコク、そして今年は韓国 ソウルとなった。同地では折しも、VISAがスポンサーを務めるFIFA U-20ワールドカップが幕を開け、熱戦が繰り広げられていた。もちろん、VISAは平昌冬季オリンピックのスポンサーでもある。前売チケットの販売は既に始まっており、当然ながら、EC店舗はチケット販売に際して、VISAからPCI DSS準拠認定を要請されている。

（写真：当社雲野[左から2番目]が登壇したセッション）

サミットは3日間開催され、VISAと直接契約するカード会社（VISAでは「クライアント」と呼ぶ）も、アジア各国から多数参加した。セッションのトピックは多彩で、アジア各国の経済成長率を踏まえたキャッシュレス化の方向性の予測、南半球と日本をまたにかけて発生したATMからの同時現金不正搾取の実態、VISAセキュリティチームの日々のセキュリティ運用体制、等々、連日活発な議論が交わされた。

BBSecでは、アクワイアラ業務のリスクマネジメントに関するセッションに雲野がスピーカーとして参加し、登壇者との議論を深めると同時に会場からの質問に応えた。同テーマへの関心はきわめて高く、セッション後、当社ブースには多くの参加者が訪れ盛況となった。

なお、最終日の3日目には、アジア各地域の警察機関とカード会社を対象に、この1年で際立った活躍を見せた団体がVISAから表彰された。韓国ではサムスンカードが受賞したが、その理由は、先に触れたとおり、韓国VISAクライアントであるカード会社として同国で初めてPCI DSSに準拠したことである。同社

（図：VISA Security Summit 2017の参加状況）

（写真[左]：韓国支店の主要メンバー）

（写真[右]：当社がVISA Security Summitで配布したノベルティ。ミネラルウォーターのボトルに「The One Solution for You」のメッセージを刻んだ）

のプレゼンスの高まりが刺激となり、今後、さらに多くの企業が標準化の取り組みを加速させることが見込まれる。

平昌オリンピック、そしてその先へ

VISAは、現在、オリンピックでの決済サービスを独占的に担う唯一のカードブランドであり、加盟店にとって、平昌オリンピック開催までにPCI DSS準拠を達成することは至上命題と言える。先述のINTERPARKのほか、ロッテ、新世界フード、現代百貨店、江原道（カンウォンド）開発公社等、名だたる大企業が、サムスンカードの後を追い、準拠への取り組みを進めている。

実は、VISAは、2008年来、日本と韓国の双方において、VISAクライアントのPCI DSS準拠に熱心に対応してきた（担当者は日本人であり、その後日本に帰国したが、今も韓国のクライアントから絶大な信頼を寄せられている）。その結果、日本では2011年から2013年頃までに当該VISAクライアントのアクワイアリング業務について、PCI DSS準拠をほぼ果たし終えた（本誌前号参照）が、一方で韓国の状況は芳しくなかった。平昌オリンピックの開催を目前にして起きたカード会社の大規模漏洩事件によって、状況が一気に前進することになったのである。

以上のような動きを背景に、BBSec韓国支店でも、目下、一層のサービス体制強化を図っている。東南アジアにおいてもPCI DSS準拠の動きは活発であり、インドをはじめとしたQSA各社が大きな市場を見据えている。そんな中、国による商習慣の違いなどから、より実効性の高いPCI DSS準拠を求めて、日本や韓国のQSAに対する期待が高まっている。

BBSecには、他の韓国QSA事業者と一線を画する強みがある。PCI DSS準拠支援にとどまらず、常にコンサルティング的な目線から、システム全体のセキュリティ課題を踏まえてソリューションを提案し、認証要件を満たす以上に実効性のあるシステム構築・運用に寄与できる点である。今後、韓国ビジネスは、平昌オリンピックというグローバルな大事業を大過なく遂行するセキュリティ対応力を完全装備する必要がある。その一助となるべく、当社も奮闘していきたい。

平昌の2年後は、いよいよ東京オリンピックである。

朴　宰範（パク　ジェバム）
韓国情報セキュリティ企業AhnLab, Inc.を経て、2009年より当社。
BBSec本社にてSOC（Security Operation Center）企画従事後、2012年韓国支店立ち上げに伴い韓国支店勤務。
2016年支店長就任。セキュリティコンサル対応QSAを率いて、韓国クライアントの信頼を獲得している。

雲野　康成
日興証券株式会社（現 日興コーディアル証券株式会社）、株式会社インターネット総合研究所 経営企画室長を経て当社。
セキュリティコンサルタントとして数多くのお客様へ情報セキュリティ対策・改善に役立つソリューションを提供している。
公認情報システム監査人（CISA）、情報セキュリティプロフェッショナル(CISSP)、公認情報セキュリティマネージャー(CISM)、
PCI DSS評価認定員QSA

診断の現場から

株式会社ブロードバンドセキュリティ セキュリティサービス本部　某診断員

私はBBSecに転職して間もないシステムエンジニアです。

BBSecへの転職契機について

実は、私は以前勤務していた会社で、サイバー攻撃を受けたことがありました。攻撃自体については、保守担当からの伝聞ではあるのですが、攻撃を受けたサイトの構築担当だっただけに、悔しい思いをしまして、そのリベンジもあって当社へ転職してきました。

サイバー攻撃

自分が経験したサイバー攻撃では、ある日、サーバに大量にアクセスがあったのですが、通常のアクセスとはちょっと違った感じでした。負荷の監視をしていたのですが、普通にアクセスが多くなっただけですと、Webサーバに負荷がかかるけれども、他のサーバにはそれほど負荷がかかるわけではありません。しかし、その時は、データベースサーバの負荷だけが非常に高かった。そこでアラートがあがって、社内で原因調査をしたところ、リクエストの中に不正なものが仕込まれていた、と。リクエストを調べた後にレスポンスを調べましたところ、データを盗み出そうとしている動きが見られました。

盗み出されたのは個人情報でした。パスワードについては暗号化を行っていたため、大事には至りませんでした。そのため、インパクトはそれほど大きくなかったのですが、自分にとってはエポックメーキングでした。

自分がそのサイトを構築していた5年ほど前は、もちろんセキュリティについてある程度考慮して構築していましたが、外部機関への脆弱性の試験検証などは行っておらず、またテストもツールを使っていないため、網羅的なテストはできていませんでした。

その後、すぐにお客様への連絡など、社内CSIRTがあったおかげで、対処は迅速に行えたわけですが、自分としては忸怩たる思いがありました。

また、監視も当時は負荷監視のみ、ログの管理も甘く、設定もロードバランサのIPからのアクセスしか分からないような設定でした。そのため、攻撃元を特定することもできませんでした。攻撃を初期段階で発見できたのは、たまたま運がよかっただけだ、という気持ちもありました。

診断を通じて日々思うこと

自分が脆弱性診断を実施する側になってあらためて感じることは、「ソースコードに対してこれだけ防御策を講じたぞ」と思っていたとしても、「環境等の設定を正しく行えているか」を今一度確認する目を持つ必要がある、ということです。実は、診断において、攻撃できるかできないか／脆弱性が存在するかどうかを調べる上では、そうした設定情報は必要ありません。しかし、実際にインシデントが発生した場合、設定が正しく行われていないと調査ができない、もしくは対応に時間がかかってしまいます。もちろん、お客様が設定に関する情報も伝えてくだされば、コンサルテーションの段階で注意を促すことはできます。

自分も開発側だったからこそ分かるのですが、開発のスケジュールが押してくると、もう「作ること」に主眼を置きがちで、同時に実施すべきセキュリティ対策は「この程度しておけば・・・」という気持ちになりがちです。もちろん、必要最低限のセキュリティ対策は実施しているつもりですが、往々にして「つもり」にしかなっていないことも多いと思います。

ソースコード診断をしていると、「念のためにescape処理を入れておいたほうがよいのでは」と思われる箇所を見ることがあります。「なんとなく」「念のために」ではなく、「ここはコストをかけてでも処理をする」「ここは重要でないのでそこまでコストをかけなくても大丈夫」という切り分けをすることが大事ですが、「めんどくさい」というので省略してしまうことがしばしばあるように思います。確かにソースコードを書く手間はかかるのですが、事前にきちんと処理を検討しておくことで、インシデントの発生率を抑えられる。とはいえ、古いシステムを継承して使用していることも多いので、簡単ではないでしょうが、最低限、改修の際にはセキュリティ機能を見直すのが結局はコスト削減につながると感じています。

開発している会社と運用している会社が異なるために、セキュリティが継承されていない、という側面もあるかもしれません。ただ、自分が参加している開発者のためのセキュリティセミナーでも回を重ねるごとに参加者が増えているように見受けられ、開発側でもセキュリティ開発についての興味は俄然高まっていると感じています。

現在の業務について

現在の業務は主に当社のCracker Detectの開発・保守です。これはWebの改竄検知ツールですが、改竄検知というのは実は難しい技術です。Webはアクセスするたびにパラメータが変わる場合があり、過検知になることもしばしばです。精度を高めていくと、なんでもないものが検知されてしまい、アラートばかりになってしまいます。かといって、精度を甘めに設定すると、肝心なときに検知をすり抜けられてしまうかもしれない。その兼ね合いが難しい。また、Cracker Detectで未知のマルウェアの検知も実施していますが、「未知のマルウェア」というだけあって一筋縄ではいきません。外部のリソースも利用しながら、開発しています。今のチームは新しいツールを取り入れることに意欲的ですし、チャレンジさせてくれる組織なので嬉しいですね。

ANALYSIS

診断結果にみる情報セキュリティの現状

株式会社ブロードバンドセキュリティ セキュリティサービス本部 セキュリティ情報サービス部

BBSecの診断について

今日サイバー攻撃の手法はますます高度化・巧妙化し、被害を受けた場合、自社・自組織の事業継続に大きな影響が及ぶ可能性がこれまでになく高まっている。こうしたリスクの最小化は世界中の企業・組織が直面する喫緊の課題だが、その対策の1つが、システム上の脆弱性の有無について現状把握し、既知の脆弱性を解消することである。

当社が提供するシステム脆弱性診断サービスでは、ツールによる自動診断と精度の高い手動診断と組み合わせて脆弱性を検出し、解決策をご提案している。以下、2017年上半期の状況を総括し、そこから学ぶべき教訓を考察したい。なお、検出された脆弱性については、右記のようなリスクレベル基準を設け、その深刻度を評価している。

リスクレベル	説　明
レベル５：緊急	攻撃された場合の影響が甚大、または容易に攻撃が実行可能
レベル４：重大	攻撃された場合の影響が大きい、またはある程度の知識や技術があれば攻撃が可能
レベル３：高	攻撃された場合の影響が限定的、または攻撃を実行するために特定の知識や技術が必要
レベル２：中	攻撃された場合の影響が限定的、間接的、または攻撃実行の難易度が比較的高い
レベル１：低	攻撃された場合の影響が軽微、または攻撃を実行するための条件が複数必要など、実現が困難

■ システム脆弱性診断で用いるリスクレベル基準

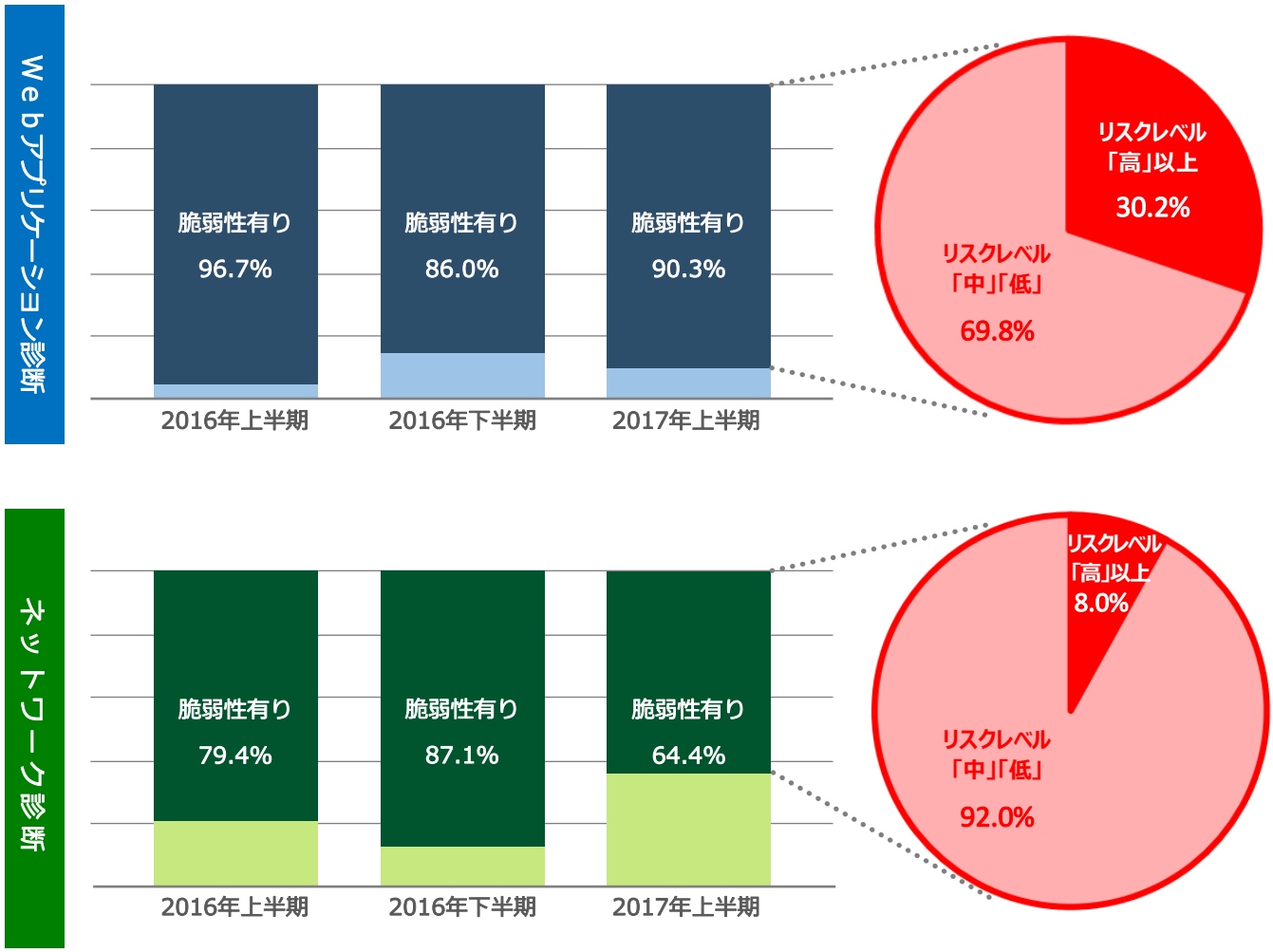
2017年上半期診断結果全体

BBSecでは、2017年1月から2017年6月までの6か月間に、15業種延べ493企業・団体、1879システムに対してシステム脆弱性診断を行った。

結果概要を次ページ上に示す。まず、Webアプリケーション診断においては、脆弱性が検出されたシステムが全体の90.3%と、何らかの対策を行うことが望ましいシステムが実に9割にのぼった。2016年下半期（86.0%）と比較してもやや増加している。ネットワーク診断においては、脆弱性が検出されたシステムの割合は64.4%であり、2016年度下半期（87.1%）と比較して顕著な減少がみられた。

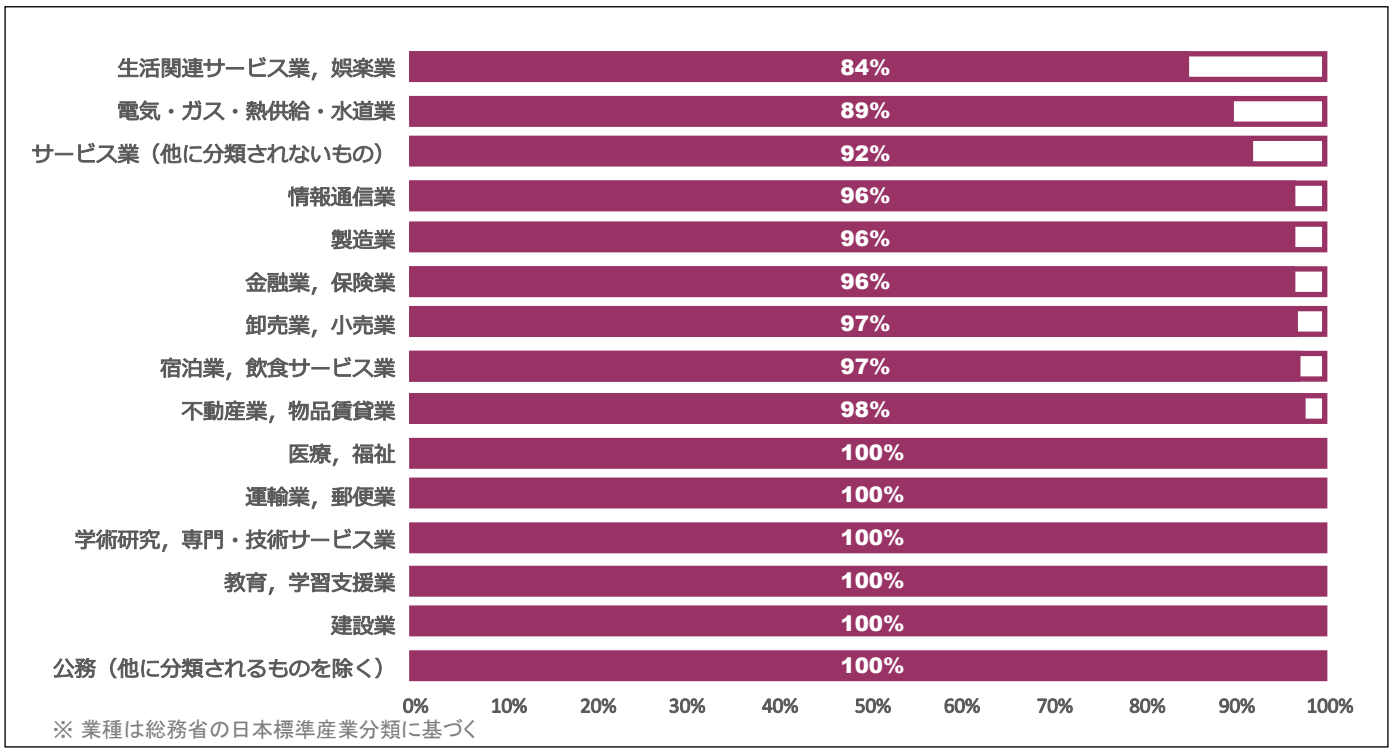
検出された脆弱性のうち、早急な対応を必要とする「高」レベル以上（上記リスクレベル表の「緊急」「重大」「高」）の脆弱性は、Webアプリケーションにおいて30.2%、ネットワーク診断においては8.0%検出された。リスクレベルの高い脆弱性を内包しているシステムが依然として存在する状況である。

業種別の検出割合は次ページ下のとおりである。すべての業種において、脆弱性の検出されなかったシステムは20%以下である。特に、内閣サイバーセキュリティセンター（NISC）の情報セキュリティ政策会議において決定された重要インフラグループ（「情報通信」「金融」「航空」「鉄道」「電力」「ガス」「政府・行政サービス（地方公共団体を含む）」「医療」「水道」「物流」「化学」「クレジット」「石油」）に属する業種については、脆弱性を悪用された場合の社会に与える影響度が大きいと想定されることから、今後の改善に期待したい。



■ システム脆弱性診断　脆弱性検出割合

■「高」リスクレベル以上の検出割合
（2017年上半期）



■ 業種別脆弱性検出割合

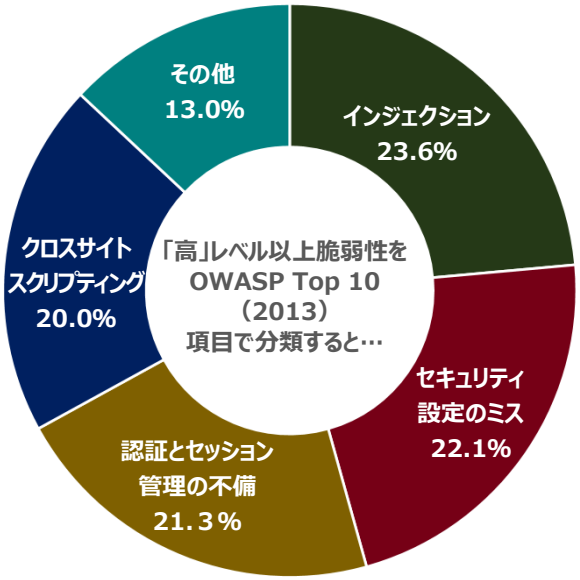
Webアプリケーション診断結果

Webアプリケーション診断で検出された脆弱性について、BBSecがリスク評価の判断基準の1つとしているのが、「OWASP Top 10」である。OWASP（Open Web Application Security Project）とは、Webアプリケーションセキュリティに関する課題解決のために、世界各国のスペシャリストが自主的に集まり活動している国際的なコミュニティである。成果物としてさまざまなガイドラインやツールを公開しており、「OWASP Top 10」は、Webアプリケーションにクリティカルな影響を与える脆弱性上位10種をリストアップしたものだ。現在、当社が基準としているのは「OWASP Top 10 - 2013」であり、4年ぶりの改訂となる「OWASP Top 10 - 2017」は2017年11月下旬に正式リリースされる予定である。参考までに、現時点での暫定版「OWASP Top 10 - 2017 RC1」と「OWASP Top 10 - 2013」の比較表を掲げておく。

OWASP Top 10 - 2013	OWASP Top 10 - 2017 RC1
A1 - インジェクション	A1 - インジェクション
A2 - 認証とセッション管理の不備	A2 - 認証とセッション管理の不備
A3 - クロスサイトスクリプティング(XSS)	A3 - クロスサイトスクリプティング(XSS)
A4 - 安全でないオブジェクト直接参照 A7と統合	A4 - アクセス制御の欠如 2003/2004版から復活
A5 - セキュリティ設定のミス	A5 - セキュリティ設定のミス
A6 - 機密データの露出	A6 - 機密データの露出
A7 - 機能レベルアクセス制御の欠落 A4と統合	A7 - 攻撃に対する保護不十分 新
A8 - クロスサイトリクエストフォージェリ(CSRF)	A8 - クロスサイトリクエストフォージェリ(CSRF)
A9 - 既知の脆弱性を持つコンポーネントの使用	A9 - 既知の脆弱性を持つコンポーネントの使用
A10 - 未検証のリダイレクトとフォワード	A10 - セキュリティ対策が不十分なAPIの使用 新

出典：OWASP（OWASP Top 10―2007 RC1は当社和訳）

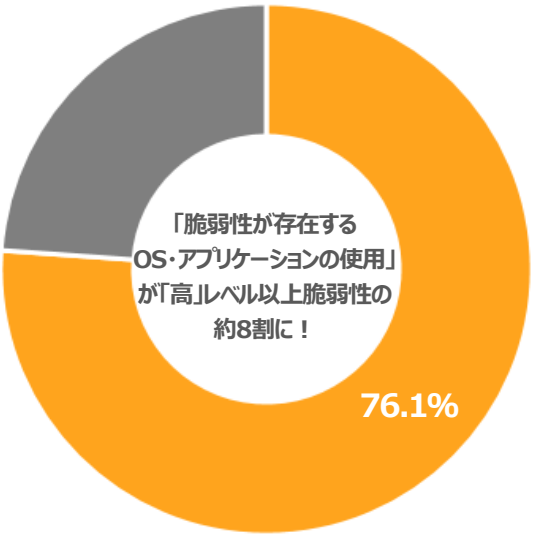
次の円グラフは、当社Webアプリケーション診断で「高」以上と評価された脆弱性を「OWASP Top 10 - 2013」に基づいて分類したものである。OWASP Top 10のTop 3である「インジェクション」「認証とセッション管理の不備」「クロスサイトスクリプティング」のいずれかに分類されるものが6割以上に達している。最も多かったのは「インジェクション」（23.6%）だ。内訳としては、HTMLタグインジェクション、SQLインジェクション、HTTPヘッダインジェクション、CSSインジェクション、メールヘッダインジェクション、OSコマンドインジェクションの順となっている。次に、「認証とセッション管理の不備」（21.3%）に分類される脆弱性としては、主に、Cookieの設定不備、セッションハイジャック、権限昇格、脆弱なパスワードの許容等が挙げられる。そして「クロスサイトスクリプティング」（20.0%）の検出も依然として少なくない（クロスサイトスクリプティングについては、Webアプリケーションの代表的な脆弱性として、本誌前号で解説しているので参照されたい）。また、「セキュリティ設定のミス」（22.1%）は、脆弱性が存在するアプリケーションの使用や不用意な情報の開示といった脆弱性を含んでおり、当社診断では「インジェクション」に次ぐ高い検出率を占めた。OWASP Top 10でも5番目にランクインしている。



なお、上記トップ3のランキングは本秋公開予定の「OWASP Top 10 - 2017」においても同様となる見通しである。開発ベンダはもちろん、発注側企業・組織に大きな影響を及ぼす指標となることは間違いない。引き続きランクインが想定される脆弱性については、すみやかに対策を講じる必要がある。OWASP Top 10に掲載されているような主要な脆弱性対策の実装を怠り、開発ベンダが発注企業から損害賠償を請求され、それが裁判で認められるというケースも実際に起きているのだ。

ネットワーク診断結果

他方、ネットワーク診断で検出されたリスクレベル「高」以上の脆弱性を見ると、「脆弱性が存在するOS・アプリケーションの使用」が圧倒的に多く、8割近くにのぼる（次ページのグラフ）。



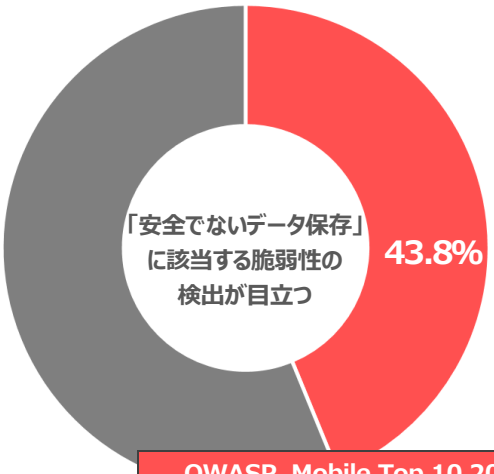
中でも憂慮されるのは、内訳の1/4強を占めた「サポートが終了したOS・アプリケーションの使用」である。サポートが終了してしまうと、新たに脆弱性が発覚した場合でも公式発表されないなど脆弱性の存在を知ることが難しくなり、かつ、セキュリティパッチが適用されない可能性も高いため、セキュリティリスクが増大する。

例えば、本年5月に世界中で猛威を奮った「WannaCry」は、Windows OSのファイル共有プロトコルSMB（Server Message Block）の脆弱性を狙ったランサムウェアであったが、「適時のWindows Update」というシンプルな対策すら講じられていないシステムが多かったことも、被害の拡大に拍車をかけたものと思われる。OSやアプリケーションに含まれる脆弱性には、任意のコード実行、DoS攻撃の誘発、機密情報の奪取等、深刻なものが多く、攻撃手法がネット上に公開されているケースすらある。既知の脆弱性を放置しておくことは自らサイバー攻撃を招くようなものである。常に最新バージョンへのアップデートやパッチの適用を行うこと、システムの仕様や環境上それが困難な場合にはワークアラウンドを検討することを、今一度肝に銘じたい。

【参考】スマホアプリ診断結果

BBSecでは、スマホアプリを対象とした診断サービスも実施している。診断数自体はまだ少ないものの、スマホの普及と相まって同アプリのセキュリティの重要性は今後急速に高まるものと見込まれる。以下、参考情報として、2017年上半期の診断結果における傾向を紹介する。

2017年上半期のスマホアプリ診断では、「OWASP Mobile Top 10 2016」でも2位に挙げられている「安全でないデータ保存」に該当する脆弱性の検出が、全体の43.8%を占めた（下グラフ）。その中でも特に目立ったのは「外部ストレージ（SDカード等）に重要情報が保存されている」ケースである。権限が与えられているアプリから外部ストレージに自由にアクセスすることが可能な場合、攻撃者のアプリに重要情報を取得される危険性が生じる。これを防ぐには、外部ストレージに重要情報を保存しないつくりにするなどの対策が必要だ。



OWASP Mobile Top 10 2016
M1 - 不適切なプラットフォームの利用
M2 - 安全でないデータ保存
M3 - 安全でない通信
M4 - 安全でない認証
M5 - 不十分な暗号化
M6 - 安全でない認可/制限制御
M7 - クライアントコードの品質
M8 - コードの改竄
M9 - リバースエンジニアリング
M10 - 本番運用に不要な機能や情報

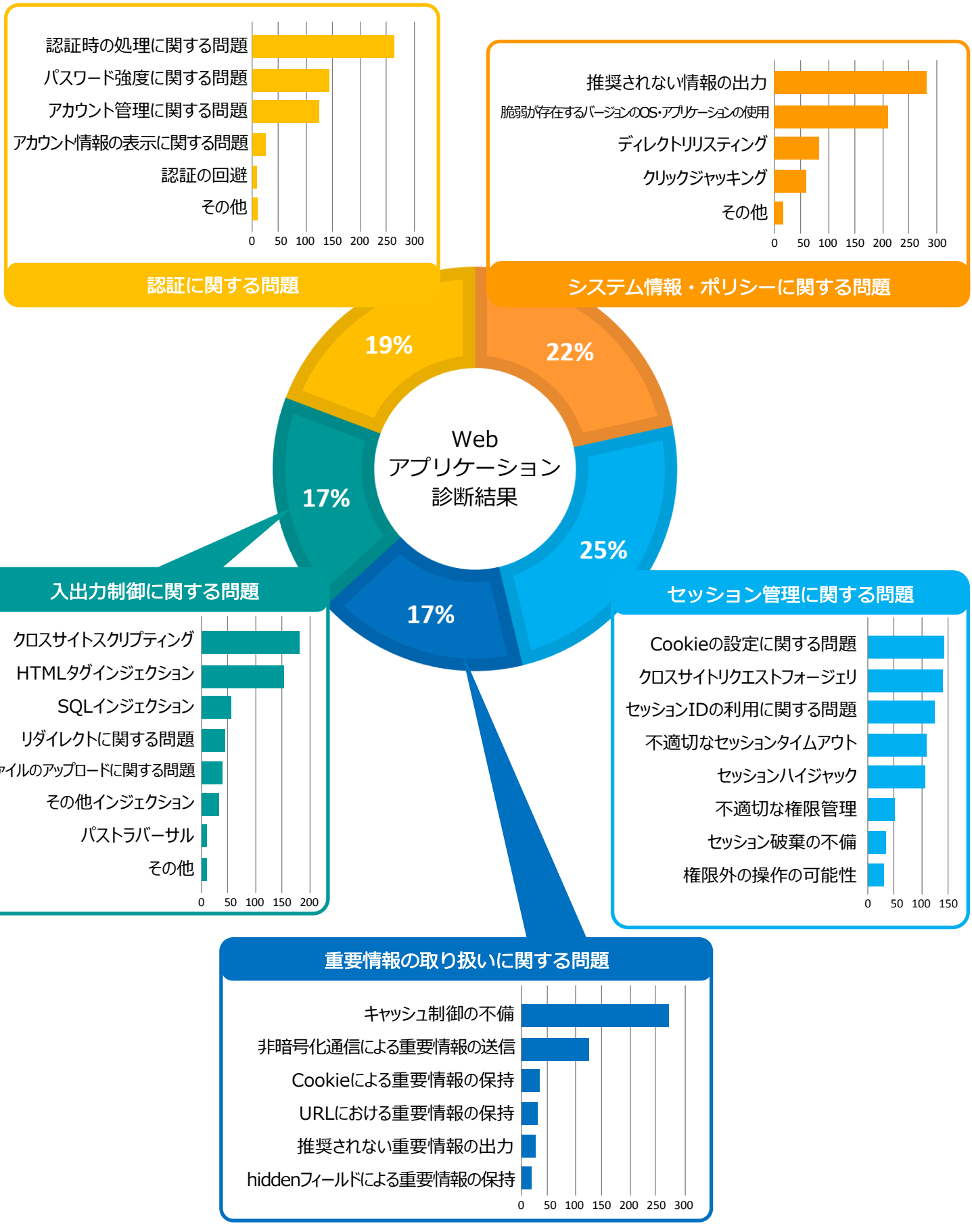
出典：OWASP

スマホの普及を背景に、スマホアプリの数は増える一方である。ツールの進化や関連書籍の充実が進み、開発のハードルが低くなりつつある反面、セキュリティ対策の課題は多く、企業や組織のセキュリティシステム全体を理解し、脆弱性、悪用の可能性など、いくつものハードルをクリアしなくてはならない。

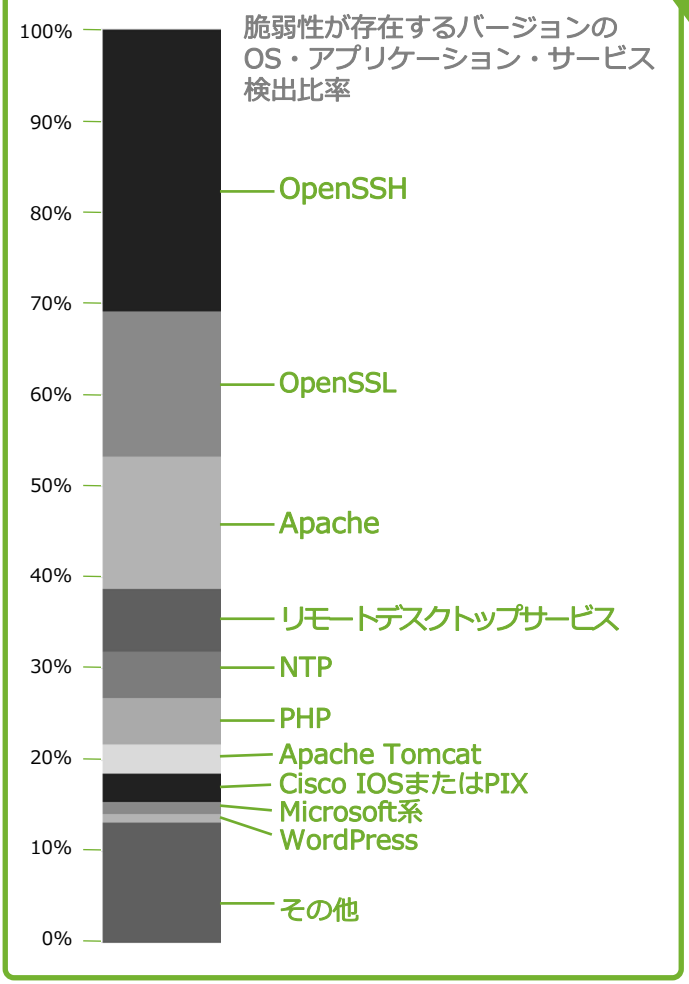
スマホのセキュリティ上の不備を狙ったサイバー攻撃は、近年増加の傾向にあり、攻撃手法も高度化している。特に、個人情報や機密情報を取り扱う場合、堅牢なスマホアプリの構築・維持は最重要課題といえよう。

2017年上半期 カテゴリ別脆弱性検出状況

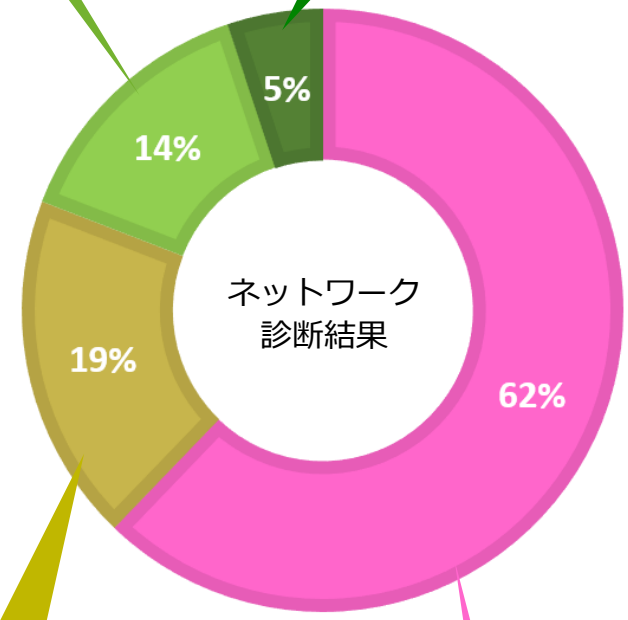
※当社カテゴリ分類にもとづく集計



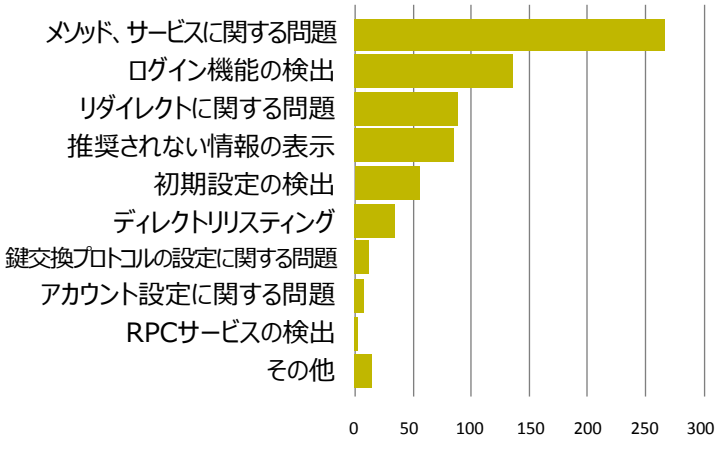
バージョン・パッチ管理に関する問題



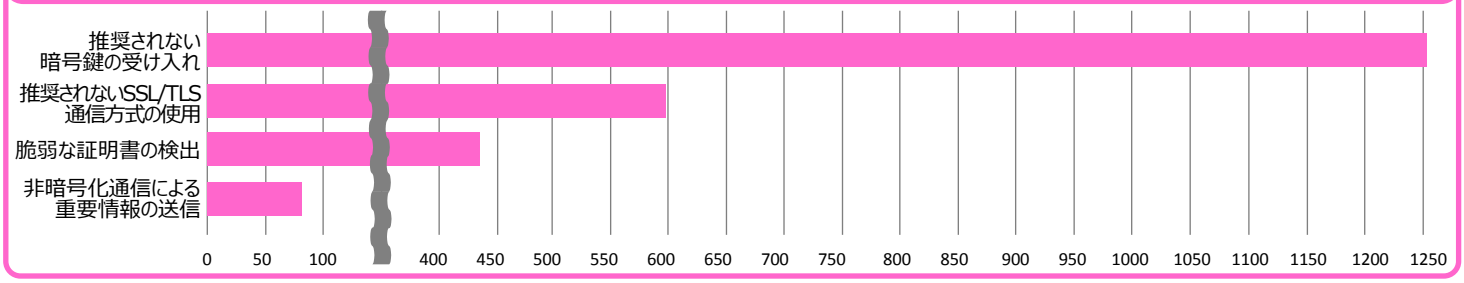
ネットワークサービスに関する問題



不適切な設定に関する問題



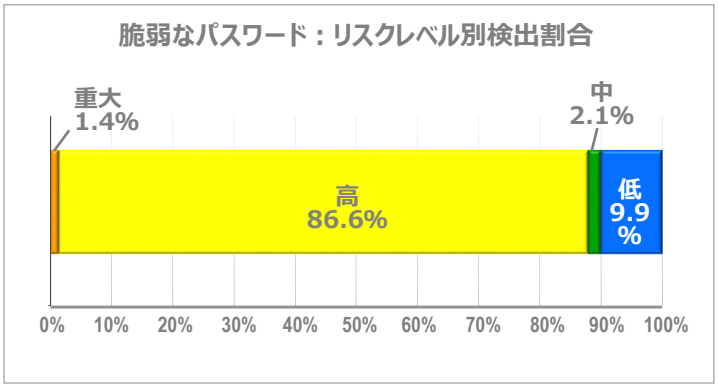
通信の安全性に関する問題



Webアプリケーション診断結果より
認証に関する問題：パスワード

パスワードの強度

2017年上半期に当社で診断した対象システムのうち、パスワードの強度について何らかの問題が検出されたシステムは全体の4.8%であった。内訳を見ると、リスクレベル「重大」に相当するものが1.4%、「高」が86.6%、「中」が2.1%、「低」が9.9%検出されている（右グラフ参照）。



なお、パスワード強度については、IPAをはじめとするさまざまな機関から文字数・文字種を基準としたガイドラインが出されているが、当社診断では文字数8文字・文字種3種以上を推奨している。

ただし、パスワード強度で求められる要件は、文字数・文字種のみではない。

次ページ上の表は、米国のセキュリティ企業Keeper Securityが、インターネット上で利用されている1,000万件以上のパスワードを調査してまとめた「最も利用率の高い」、脆弱なパスワードトップ25である。このリストに含まれるパスワードのうち、文字数・文字種の最大値は10文字・2種だ。パスワードクラックにかかる時間はRandomize（Random Password Generator：http://random-ize.com/how-long-to-hack-pass/）では14日21時間、Better Buy（Estimating password-Cracking Time：https://www.betterbuys.com/estimating-password-cracking-times/）では8年9か月3週間6日8時間50分57秒と予測されている。クラックされるまでにこれだけの時間を要するのであれば、通常は安全なパスワードだとみなされるだろう。だが、このようなリストに記載されてしまった場合は、もはや安全とは言えない。攻撃者は、リストを使った辞書攻撃を試みるため、総当り（Brute-Force）攻撃が始まった瞬間に破られてしまうのだ。

ちなみに、こうしたリストでは毎年ランキングは変わっている。次ページ下の表は同じく米国のセキュリティ企業SplashDataが2015年1月に発表した「最悪なパスワード」トップ25だが、Keeper Securityのリストとは重複しないものも多い。辞書攻撃を防御するには、システム側で、毎年複数のリストをブラックリストとして登録し、リスト上のパスワードは受け付けない、もしくはアラートを表示してユーザに変更を促すなどの仕組みを検討する必要がある。

「パスワード頼み」では守れない

パスワードは、これまで、認証の要となる手段とみなされてきた。しかしながら今、そうした考え方が根本から揺さぶられている。

さまざまな調査研究を通じて、従来有効とされてきたパスワードの定期更新が、むしろ「百害あって一利なし」と結論付けられたのだ。米国立標準技術研究所（NIST）で『電子認証に関するガイドライン』（NIST SP 800-63）の策定に携わったBill Burr氏も、自ら「パスワードの定期変更をガイドラインに盛り込んだのは失敗だった」と述べており、SP 800-63 Revision 5では定期更新は明記されない予定である（2017年9月現在、Revision 5はパブリックコメント募集中）。パスワードの定期更新に代わって有効とされているのは、覚えやすい「パスフレーズ」だ。

この勧告に従う場合、パスフレーズの文字数には最初から上限を設けないようにするか、上限を設ける場合は最低でも64文字にする必要がある。当社の診断で、パスワードの入力文字数に上限を設定しているケースを時折見かけるが、そうしたシステムで見直しが必要になる可能性がある。システムの変更に要するコスト

順位	パスワード	文字数	文字種類	Randomizeによるパスワードハックにかかる時間	Better Buyによるパスワードクラックにかかる時間
1	123456	7文字	1種類	1秒未満	0.25ミリ秒
2	123456789	9文字	1種類	1秒未満	0.25ミリ秒
3	qwerty	6文字	1種類	1秒未満	0.25ミリ秒
4	12345678	8文字	1種類	1秒未満	0.25ミリ秒
5	111111	7文字	1種類	1秒未満	0.25ミリ秒
6	1234567890	10文字	1種類	3秒	0.25ミリ秒
7	1234567	7文字	1種類	1秒未満	0.25ミリ秒
8	password	8文字	1種類	1秒未満	0.25ミリ秒
9	123123	6文字	1種類	1秒未満	0.25ミリ秒
10	987654321	9文字	1種類	1秒未満	0.25ミリ秒
11	qwertyuiop	10文字	1種類	13時間48分	4か月4日7時間11分46秒
12	mynoob	6文字	1種類	1秒未満	24秒
13	123321	7文字	1種類	1秒未満	0.25ミリ秒
14	666666	6文字	1種類	1秒未満	0.25ミリ秒
15	18atcskd2w	10文字	2種類	14日21時間	8年9か月3週間6日8時間50分57秒
16	7777777	7文字	1種類	1秒未満	0.25ミリ秒
17	1q2w3e4r	8文字	2種類	16分33秒	0.25ミリ秒
18	654321	6文字	1種類	1秒未満	0.25ミリ秒
19	555555	6文字	1種類	1秒未満	2分46秒
20	3rjs1la7qe	10文字	2種類	14日21時間	8年9か月3週間6日8時間50分57秒
21	google	6文字	1種類	1秒未満	0.25ミリ秒
22	1q2w3e4r5t	10文字	2種類	14日21時間	8年9か月3週間6日8時間50分57秒
23	123qwe	6文字	2種類	1秒未満	0.25ミリ秒
24	zxcvbnm	7文字	1種類	2秒	0.25ミリ秒
25	1q2w3e	6文字	1種類	1秒未満	0.25ミリ秒

Keeper Security「The Most Common Passwords of 2016」よりBBSecにて作成

順位	パスワード	順位	パスワード
1	123456	14	letmein
2	password	15	photoshop
3	12345678	16	1234
4	qwerty	17	monkey
5	abc123	18	shadow
6	123456789	19	sunshine
7	111111	20	12345
8	1234567	21	password1
9	iloveyou	22	princess
10	adobe123	23	azerty
11	123123	24	trustno1
12	Admin	25	000000
13	1234567890		

出典：「“123456” Maintains the Top Spot on SplashData’s Annual “Worst Passwords” List」
http://www.prweb.com/releases/2015/01/prweb12456779.htm

も無視できない。「パスワードの強度は敢えて最低限で許容し、複数認証をはじめとする他の手法を組み合わせて運用する」といったシナリオも考えられる。

いずれにせよ、パスワード頼みの認証ではもはや組織は守れない。総当り（Brute-Force）攻撃のリスクを緩和する「アカウントロックアウト」など、従来と変わらず効果を発揮する手段もあるが、効果的な防御体制を実現するには、今後も認証技術の最前線を注視していく必要があるだろう。

ネットワーク診断結果より
バージョン・パッチ管理に関する問題 ：サポートが終了したバージョンのミドルウェア・ソフトウェア

サポートが終了したバージョンのミドルウェア・ソフトウェアを使用することには大きな問題がある。何よりも、脆弱性に対応したバージョンのミドルウェア・ソフトウェアが開発元から提供されず、既知の脆弱性が含まれるミドルウェア・ソフトウェアを使用し続けることのリスクがきわめて高い。各種セキュリティ基準/標準でも、インフラを構成するミドルウェア・ソフトウェアやアプライアンスについては、最新バージョンまたは最新パッチが適用された状態で使用することが求められている。例えば、クレジットカード業界のセキュリティ基準であるPCI DSSでは、脆弱性に対応したパッチをリリース後1か月以内に適用する旨が要件6.2（Ver.3.2）に記載されている。

当社のツール診断・手動診断では、サポートが終了したバージョンのミドルウェア・ソフトウェアが使われているかどうかを、診断対象システムからのクエリによって特定する。システムがミドルウェア・ソフトウェアのバージョン情報をクエリの一部として出力した場合、自らの環境に関する情報を第三者に開示していることになるため、診断では「攻撃者への情報提供につながる恐れがある」とみなし、「情報」としてご報告している。本年上半期は、診断対象7200IPアドレスのおよそ7.6%にあたる550件で、ミドルウェア・ソフトウェアのバージョン情報の出力を確認したが、そのうち158件が、開発元からのサポートが既に終了しているバージョンであった。内訳は右表のとおりである。

ミドルウェア・ソフトウェア	検出数
PHP	61
.NET Framework	29
OpenSSL	27
Apache Tomcat	16
BMC BladeLogic Server Automation	9
IIS	4
BIND	2
JBoss	2
phpThumb	2
WordPress	2
Movable Type	1
phpMyAdmin	1
ProFTPD	1
合　計	157

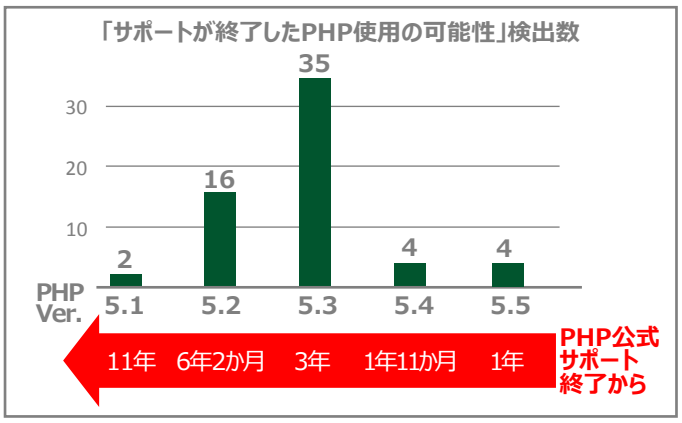
今回は、特に検出数の多かったPHP、および.NET Frameworkについて解説する。

PHP

2017年上半期診断で検出された「サポートが終了したバージョンのPHP」を、メジャーバージョン番号にもとづいて直近のものから並べてみた。結果は次ページのとおりで、圧倒的にPHP 5.3の検出数が多くなっている。

なお、診断で得られたクエリどおりにPHP 5.3が使用されているケースもあるが、「OSのパッケージとしてインストールしyumなどでレポジトリ管理をしているPHP 5.3にバックポートしているケース」も想定される。今回は、後者に該当する可能性が高いとみなせるPHP 5.3.3が23件ほど検出された。バックポートしているケースについては、OSのサポート期限を考慮のうえ、まずは最新のパッチを適用することを推奨したい。なお、バックポート対応は決して即時性があるものではない。並行して、より包括的な対策を検討することが求められるだろう。

なお、PHPに関しては、設定情報やEaster Egg情報が表示される脆弱性が2017年上半期で計63件検出されているが、そのうちの実に47件がサポートが終了したバージョン上のものであった。検出総数として多くはなかったが、サポートが終了したバージョンを使用し、かつ、システム内部の情報も露呈している場合、攻撃のリスクは格段に高まる。各組織におけるセキュ



リティ意識の向上により、今後の検出数がゼロになることを期待したい。

.NET Framework

.NET Frameworkはご存知のとおりWindows Serverシリーズにプリインストールされていることが多く、一般に、WindowsのWebプログラミング環境としては第一の選択肢となる。

バージョン別の検出数を見ると、2016年1月12日にサポートが終了した.NET 4.0/4.5/4.5.1のシリーズが大半を占める。おそらく、4.5.2へのインプレース更新を検討中の組織が多かったのではないかと推測される。.NET Frameworkのサポートについては、バージョン間の互換性なども含めて非常に複雑な対応が必要になる場合があるため、Microsoftからの情報[*1]等を参考に、現行のバージョンからの移行プランを策定することを推奨したい。

また、少数ながら、.NET 2.0/3.5 SP1以前/1.1 SP1以前といった、「OSを含めてサポートが終了しているバージョン」と推察されるケースも存在した。.NET FrameworkのバージョンはOSのバージョンと紐付けることが容易であり、.NET Frameworkのバージョンを出力することは、OSのバージョンを知らせることにつながる。対して、Windows OSを狙った攻撃は定常的に発生しており、直近ではWannaCryやPetyaが世界各地に大きな被害をもたらした。サポートが終了したバージョンのOS（Windows Server 2003以前）では、Microsoftからセキュリティパッチが提供されることはもはや期待できず、リスクがきわめて高い状態である。当該バージョンを使用している組織には早急な対応が求められる。

PHPおよび.NET Frameworkは、共にWebアプリケーションの開発・運用環境としてメジャーな選択肢であり、プログラミング言語のランキングでも長年トップ10に入る地位を保持している[*2]。その反面、いずれのプラットフォームも、Webアプリケーションの導入から安定運用までに多大な労力がかかり、苦労話は枚挙にいとまがない。それゆえ、本脆弱性検出の背景には、「現在安定運用しているものに手を加えることのデメリットを憂慮して対処が遅れる」というシナリオが多少ともあったものと想像できる。

もちろん、現場レベルでは、リスクの高い環境に対するリスク低減策を立案し、かつ、日々のオペレーションでインシデントが発生しないよう、細心の注意を払って運用が行われているものと思う。しかしながら、それでは本質的な対策とは言えない。リスクの高い環境を使い続けることにより発生しうるコスト（インシデントが発生した場合の対策、インシデント発生後の緊急的なプラットフォームの入れ替え等にかかる加算コスト）の算定や、ロードマップの策定は手付かずだ。マネジメント層が、ソフトウェアのみならずハードウェアを含めたプラットフォーム全体に対して、現場からのボトムアップにもとづいた的確な意思決定を下すことが必要である。昨今の脅威の高まりを受け、マネジメント層の積極的な関与がこれまでになく求められるといえるだろう。

---

*1
「.NET Frameworkサポート ライフサイクルポリシーについて(2015年10月)」
https://blogs.msdn.microsoft.com/visualstudio_jpn/2015/10/18/net-framework-201510/
「ライフサイクルに関する FAQ - .NET Framework」
https://support.microsoft.com/ja-jp/help/17455/lifecycle-faq-net-framework

*2 参考：TIOBE Index（https://www.tiobe.com/tiobe-index/）

ネットワーク診断結果より
ネットワークサービスに関する問題：攻撃の踏み台にされる可能性が高いプロトコル

本稿では、2017年度上半期診断で検出されたネットワークサービスに関する脆弱性のうち、攻撃の踏み台にされる可能性が高い「Well Knownポートを使用するプロトコル」[*1]を取り上げる。特に注意を喚起したいものとして、ファイル転送を目的としたプロトコル「FTP」、管理コンソールへのアクセスを目的としたプロトコル「Telnet」「SSH」、さらに、Windowsのファイル共有サービスの主要プロトコルである「SMB」について順に解説する。まず、下表にプロトコル別の検出数を示す。

■ 主要プロトコルサービスに関する脆弱性の検出状況

	FTP	Telnet	SSH	SMB
オンサイト診断	26	23	760	78
リモート診断	36	2	61	1
合　計	62	25	821	79

FTP、Telnet

Well Knownポートを使用するプロトコルの多くは、1980年代から1990年代前半にかけて実用化された。ご存知のとおり、1990年代後半以降ネットワークインフラの高速化が進み、ネットワーク経由で取り扱えるデータ量は飛躍的に増大した。データ量の増大と並行し、パフォーマンスやセキュリティに関する要件のハードルも高まっている。多くのプロトコルでは機能追加によって一連の課題に対応しているが、その一方で、プロトコル自体の仕様上の理由により機能追加が行われていないものもある。その代表格がFTPとTelnetだ。

いずれのプロトコルも認証は平文によるもののみで、通信も暗号化されない。このため、FTPについては、「FFTP」や「SFTP」などへの置き換えにより暗号化されたファイル転送を導入すること、Telnetについては、リモートからのアクセスを暗号化と秘密鍵/公開鍵による認証が可能なSSHに切り替えることが、それぞれ推奨されている。業務上の理由でそうした対応が困難な場合には、アクセス制御などの対策を行う必要がある。

翻って当社診断の結果を見ると、僅少ながら、そうした対策がとられていないシステムが依然として存在する。より危険性の高いリモートでの検出について見ると、FTPでは、36件のうち平文認証が用いられていることが確認されたシステムが8件、匿名FTPが有効であることが確認されたシステムが1件あった。リモートでのTelnet検出分2件と合わせ、これらは、攻撃に対してきわめて脆弱な状態のシステムといえる。

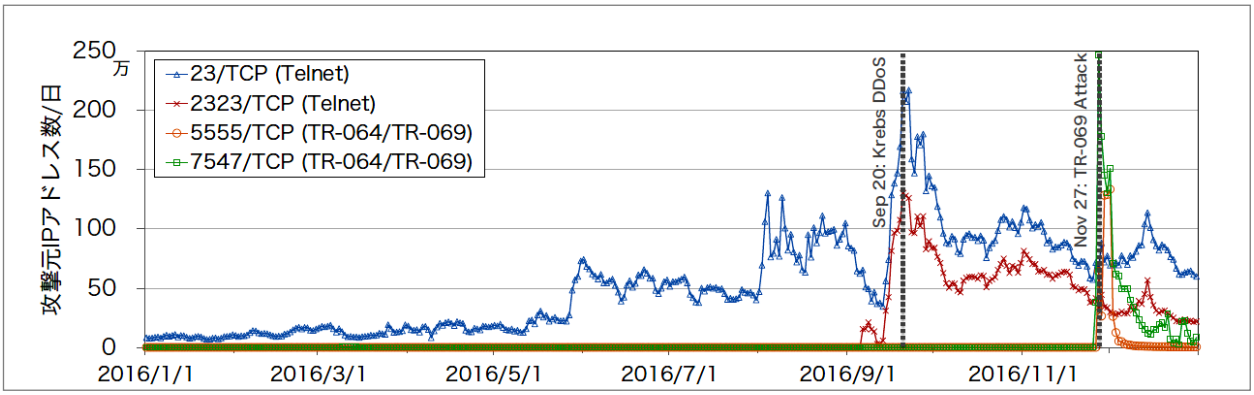
対策として、FTPについては、同サービスの必要性を再検討し、不要と判断された場合はサービスを無効にする。必要と判断された場合は、FTPサーバでやり取りするファイルの重要性にもとづき暗号化を含む適切な運用を実行する。なお、その際、IT部門の担当者だけでなく、FTPサービスを利用する他部門の担当者にも運用ルールの周知徹底が必要となる点に留意したい。

Telnetについての対策は、先に述べたとおりだが、参考までにTelnetポートを悪用した攻撃事案を挙げておこう。2016年秋に発生した「Mirai」ボットネットによる大規模なDDoS攻撃である。Miraiでは、コンシューマ向けのブロードバンドルータや監視カメラなどのIoT機器が踏み台にされたが、Telnetポートを外部に開放している機器がその中に含まれていたであろうことは想像に難くない。次ページに『NICTER 観測レポート2016』（http://nict.go.jp/cyber/report/NICTER_report_2016.pdf）のデータを紹介する。

上段は、攻撃元IPアドレス数を宛先ポート別に追跡したグラフである。Telnetのデフォルトポートであるtcp

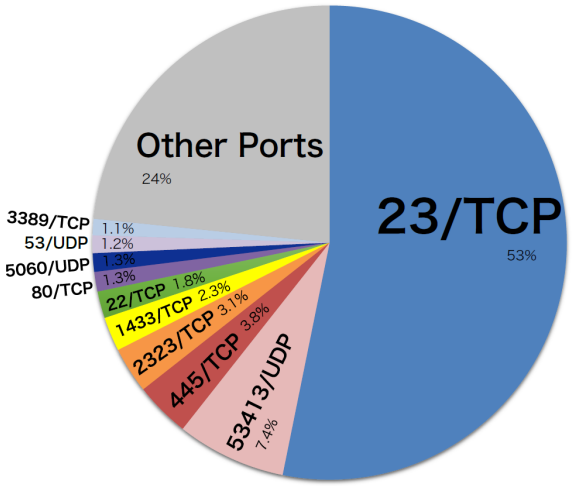
*1 一般的には、TCPおよびUDPのポート番号20・21番のFTP、22番のSSH、23番のTelnet、25番のSMTP、53番のDNS、80番のHTTP、110番のPOP3、123番のNTPなどを指す。

■ 2016年に急増した宛先ポート別の攻撃元IPアドレス数統計



出典：国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所サイバーセキュリティ研究室 『NICTER 観測レポート2016』

■ ダークネット観測における宛先ポート番号別の
2016年年間観測パケット数割合



出典：国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所サイバーセキュリティ研究室
『NICTER 観測レポート2016』

23番、次候補として使われやすいTCP 2323番が、Miraiの拡大に伴って跳ね上がっている。下段は、比率についてのグラフだが、TCP 23番のみで半数を超えていることがわかる。

Telnetは、前述のとおり仕様が古いままで非常に簡便な設計のプロトコルであるため、侵入経路としても手軽だ。不正なパケットの送信が恒常的に行われていると考えてよい。悪意のある第三者によってTelnet経由で社内システムへのアクセスがなされた場合、被害の影響は甚大となる可能性がきわめて高い。2017年下半期の診断報告では、リモートからのアクセスがゼロ検出となることをぜひとも期待したい。

SSH

当社診断では、ポートが開放されているケースのほか、プロトコルのバージョンが古い、脆弱な暗号化方式・ハッシュアルゴリズムが許容されているといった場合に指摘を行っている。Telnetに代わるプロトコルとして長年推奨されてきたSSHだが、つい最近、懸念すべき動きがあった。

2017年7月、SSH認証情報窃取のための2種のツール「BothanSpy」「Gyrfalcon」の取扱説明書がWikiLeaksにアップロードされた[*2]。しかも、両者は共にCIA（米中央情報局）が秘密裏に作成していたものだったといわれる。SSHのゼロデイ脆弱性は含まれていないが、実際にこういったツールが存在し、用いられていた可能性は認識しておきたい。あのWannaCryの経緯を彷彿とさせるものがあるからだ。WannaCryでは、NSA（米国家安全局）が使用していたハッキングツールが流出。ハッカー集団「Shadow Brokers」が同ツールを元にSMBの脆弱性を突くツールを新たに作成して公開し、大規模被害につながった。残念ながら、「今回はNSAではなくCIAだから、ハッキングツールまで流出するはずがない」という確証はなく、SSHについても改めての注意喚起が必要となった格好である。リモートからのSSH接続を許容している企業・組織においては

*2 https://wikileaks.org/vault7/#BothanSpy
BothanSpyはWindows向け、GyrfalconはLinux向けのツール。
BothanSpyではSSHに加えてtelnet、rloginの認証情報の取得も可能となっている。

特に注意が必要だ。該当しない場合も、この機会にぜひ、SSHのバージョン、暗号化方式やハッシュアルゴリズムの安全性、OSへのパッチの適用状況などを点検していただきたい[*3]。

SMB

診断結果では、リモート（外部向け）でポートが開いていたケースは1件のみであった。一方、オンサイトでは78件の脆弱性が検出され、そのうちWannaCryでも悪用されたSMB v1が使用されているケースが5件あった。WannaCryを含む複数のランサムウェアに対する脆弱性が発見されたケースは1件、任意のコード実行が可能な脆弱性が発見されたケースが1件となっている。残りの71件は、SMBセキュリティ署名が無効となっていたことにより検出されたものである。Windowsの初期設定では無効となっているため単に有効化のし忘れと想定されるケースのほか、パフォーマンス低下の可能性を懸念して有効化を行えていないケースがあったのではないかと推定される。

SMBについては、その脆弱性を狙ったWannaCryの亜種が今も出続けている。外部にポートを開くことは禁忌であるが、社内においてもセキュリティに配慮した運用が求められる。なお、SMB v3以降では、暗号化の一機能として署名がビルトインされており、SMB v2以前で懸案だった署名によるパフォーマンスの低下が解消されている[*4]。システムの要件と照らし合わせて十分な検証をした上で、可能なケースについてはSMB署名を有効にすることを推奨したい。

今回取り上げたプロトコルをはじめ、Well Knownポートを使用するプロトコルの多くは、システムにとって基本ともいえる機能を担っている。それゆえ、第三者によって悪用された場合の影響は甚大だ。パフォーマンス、利便性、システム構成上の要件とのバランス等々、業務にもとづくさまざまな制約が存在するとはいえ、最低でも、

① 不要なポートを外部に開放しない

② 利用しているプラットフォームの脆弱性・マルウェア・攻撃に関する最新情報を収集する

③ FTPやTelnetを外部向けに利用する必要がある場合は暗号化が可能な代替策への切り替えを行う

の3点は必須としたい。その上で、自組織における防御の最適解を見出していただきたい。

---

*3 以下の分析記事が参考になる。
https://www.ssh.com/ssh/cia-bothanspy-gyrfalcon

*4 https://blogs.msdn.microsoft.com/openspecification/2017/05/26/smb-2-and-smb-3-security-in-windows-10-the-anatomy-of-signing-and-cryptographic-keys/

ブロードバンドセキュリティについて

株式会社ブロードバンドセキュリティ（BroadBand Security, Inc./BBSec）は、「企業のITセキュリティ・ガーディアン（守役）として組織の健全経営に貢献する」というミッションを掲げ、2000年の創業以来、様々なニーズに対応するセキュリティサービス事業を展開してまいりました。

2004年には、標的型攻撃に対応するクラウド型メールセキュリティサービスを国内で初めて提供（「Anti-Abuse Mail Service」）。2008年には、国際的なクレジットカードセキュリティ基準PCI DSSの認証監査機関としての認定資格「QSAC」を国内で2番目に取得。有資格者によるセキュリティ認証取得・準拠支援サービスは、国内外の多くのお客様にご評価いただき、現在、韓国ではトップシェアを獲得しています。その後も、セキュリティ・コンサルティング、デジタル・フォレンジック、脆弱性診断、マネージドセキュリティサービスなど、対応分野を次々と拡大。ITセキュリティのエキスパートとして、豊富な知識と経験に裏打ちされた高品質のサービスをお届けしています。

株式会社ブロードバンドセキュリティ

https://www.bbsec.co.jp/

東京本社
〒160-0023
東京都新宿区西新宿8-5-1
野村不動産西新宿共同ビル4F
TEL：03-5338-7430

大阪支店
〒530-0001
大阪府大阪市北区梅田1-1-3
大阪駅前第3ビル30F
TEL：06-6345-3880

名古屋支店
〒450-0002
愛知県名古屋市中村区名駅2-45-14
東進名駅ビル4F
TEL：052-856-2055

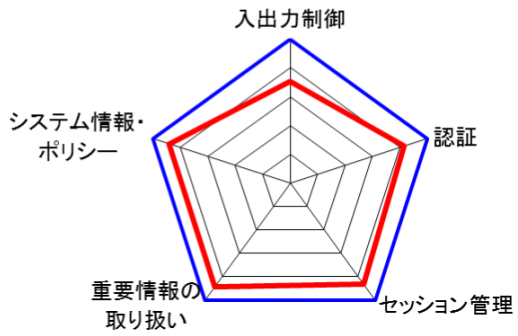
韓国支店（Korea Branch）
Level 41, Gangnam Finance Center, 152 Teheran-ro, Gangnam-gu, Seoul Korea 135-984
TEL：+82-2-2008-4640

業界別診断結果レーダーチャート

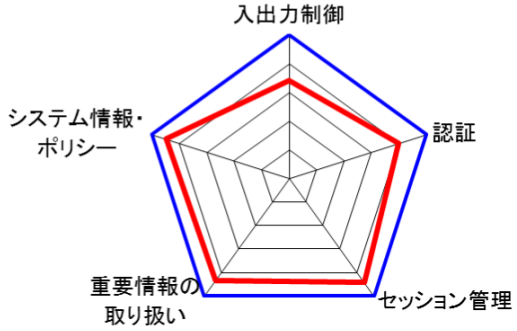
― 2017年上半期 Webアプリケーション診断 ―

Webアプリケーション診断結果より、各カテゴリに対する対策の度合いについて、業界別の平均値をレーダーチャートで示した。業種を問わず、「入出力制御」「認証」について、対策が十分でない傾向が強い。

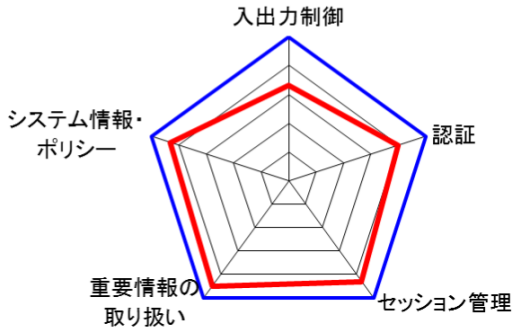
生活関連サービス業，娯楽業



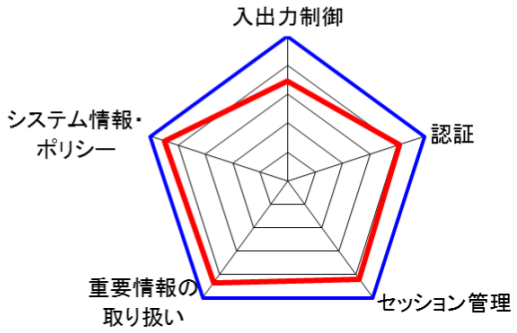
電気・ガス・熱供給・水道業



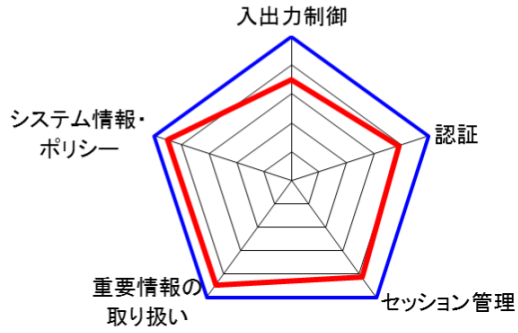
サービス業（他に分類されないもの）



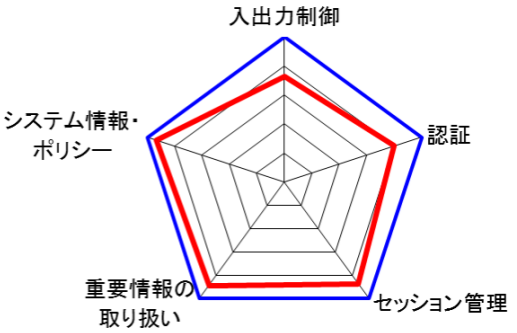
情報通信業



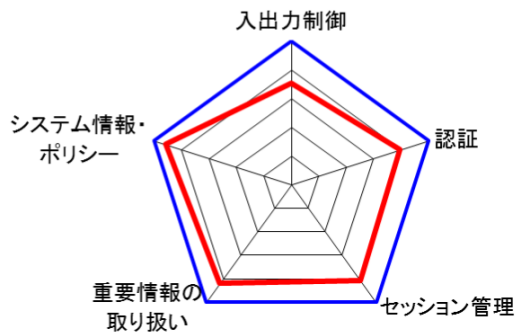
製造業



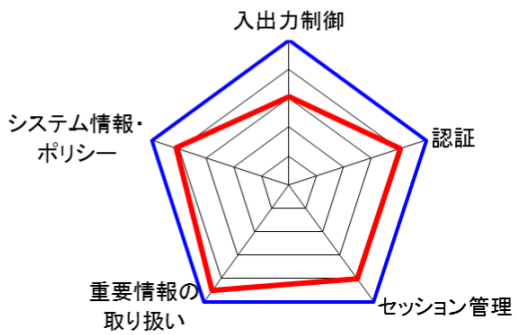
金融業，保険業



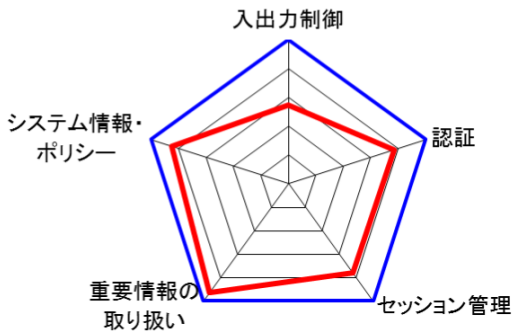
卸売業，小売業



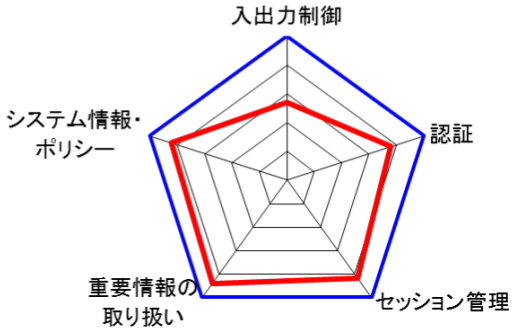
宿泊業，飲食サービス業



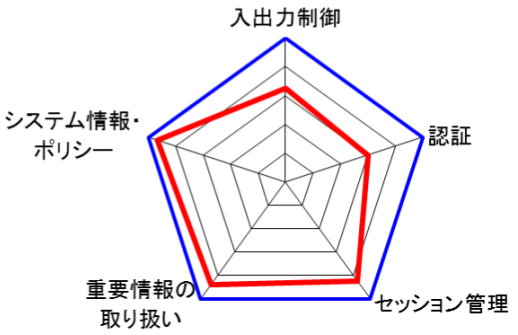
不動産業，物品賃貸業



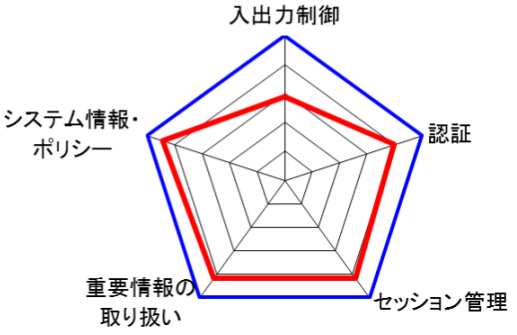
医療，福祉



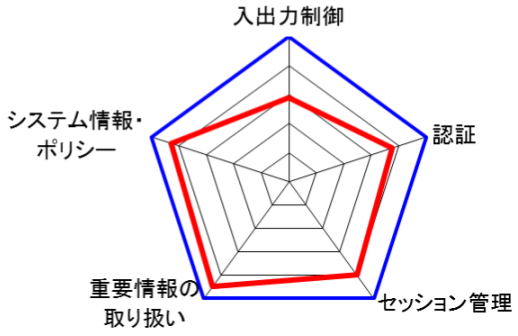
運輸業，郵便業



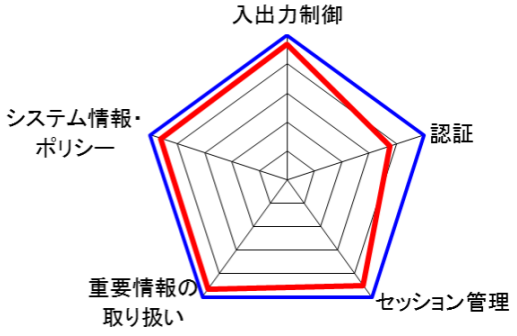
学術研究，専門・技術サービス業



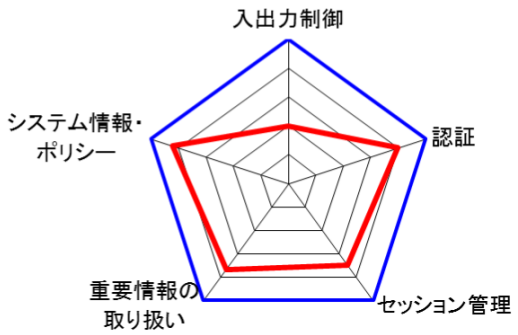
教育，学習支援業



建設業



公務（他に分類されるものを除く）



脆弱性診断

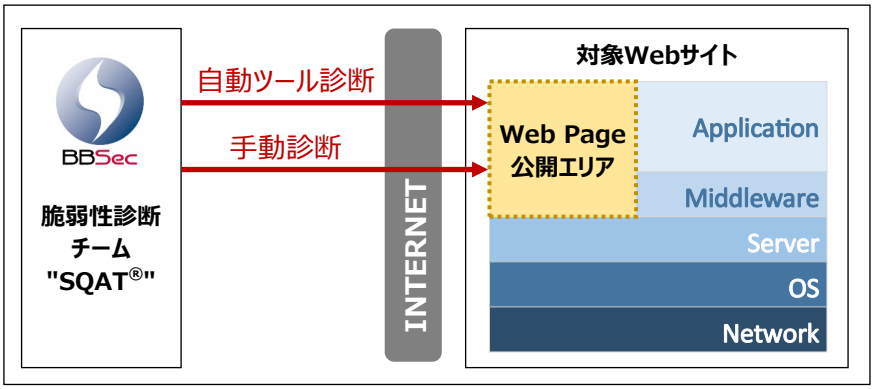
脆弱性診断は、悪意ある攻撃を受ける前に、自らを防御するための問題特定ツールです。BBSecでは、“セキュリティリスク最小化”にむけて、精度の高い手動診断と自動診断を組み合わせ、お客様システムの健全化を支援しています。

Webアプリケーション脆弱性診断

SQAT® for Web

インターネットを介して外部からWebアプリケーションの脆弱性を診断

悪意ある攻撃を想定した外部からの診断を最新のセキュリティ情報に基づき実施します。導入時の脆弱性診断だけでなく、既存システムの脆弱性対策の確認にも活用することができます。

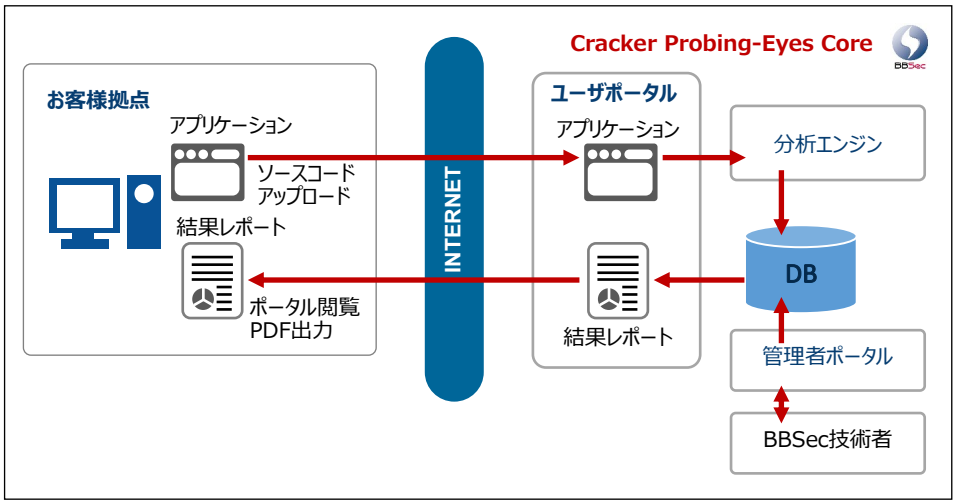


SaaS型ソフトウェア品質自動分析診断

Cracker Probing-Eyes Core

開発段階からの脆弱性チェックをオンデマンドで実現

アプリケーションのソースコードをそのまま圧縮／アップロードするだけで、ソースコードの脆弱性と品質の診断を行えるSaaS型品質分析自動ツールです。お客様のオフィスから、任意のタイミングで品質分析を行えるため、時間が切迫した開発現場での品質分析診断に大きなメリットをもたらします。

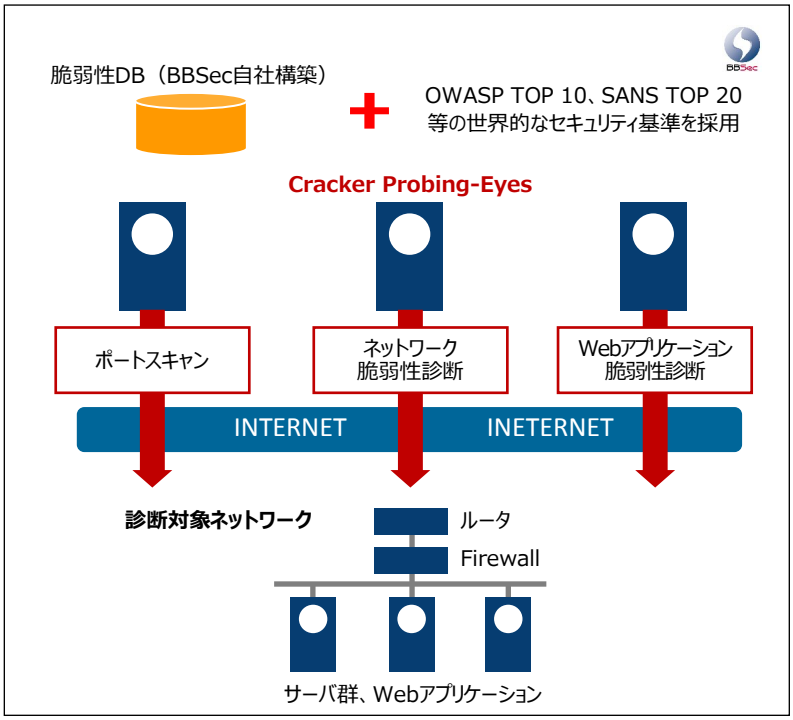


デイリー自動脆弱性診断

Cracker Probing-Eyes

不正アクセス防止用クラウド（ASP）型デイリー脆弱性診断サービス

デイリー自動脆弱性診断は、1日1回、インターネット越しにお客様サイトの脆弱性をチェックする自動診断サービスです。米国 国家安全保障局（NSA）、米コンピュータセキュリティ研究所（CSI）、米連邦捜査局（FBI）、およびSANSなど、世界トップクラスのセキュリティ組織により策定された規格や基準に準じた信頼性の高い診断プログラムは、お客様のシステムを健全に保つ上で、大きな効果を発揮します。



SQAT® Security Report　2017年9月号

2017年9月1日 発行

発行人：株式会社ブロードバンドセキュリティ セキュリティサービス本部

〒160-0023 東京都新宿区西新宿8-5-1　野村不動産西新宿共同ビル4F

TEL：03-5338-7417　　FAX：03-5338-7435

https://www.bbsec.co.jp/