

SQAT® SECURITY REPORT

2019年3月号

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

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/>



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
取締役 セキュリティサービス本部 本部長
田仲 克己

本誌は、株式会社ブロードバンドセキュリティ（以下、BBSec）の脆弱性診断サービス「SQAT®」における 2018 年下半期（7 月～ 12 月）の診断から得られた最新データをベースに、当社トップエンジニアらによるサイバーセキュリティの現状と展望について、さまざまな角度からお楽しみいただくことを目的としたレポートです。

色々なサイバーセキュリティの話題の中でも、昨年は仮想通貨のセキュリティについてのニュースに目を引かれました。仮想通貨取引所・コインチェックの盗難事件など、金銭的動機のネガティブな事案が見受けられましたが、過去には国の金融危機といった有事に仮想通貨が資産防衛策として機能した事例もあり、発展していく可能性は大いにありえます。そんな今後の動向が気になる仮想通貨を皮切りにして、有識者とともに関国のサイバーセキュリティの現状を考察しました。

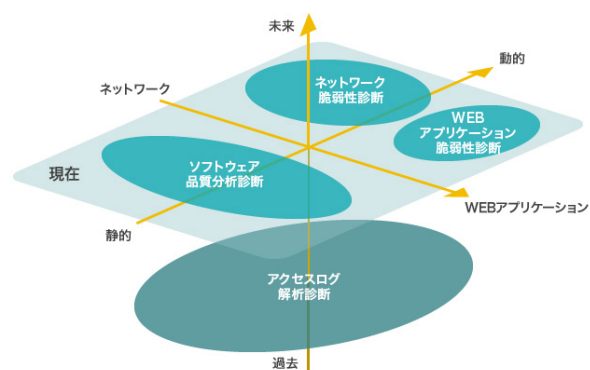
また、急速な普及を続けているクラウドサービスにも焦点をあてました。クラウドサービスは企業活動に欠かせないインフラの一部になってきている一方で、情報漏洩をはじめとしたセキュリティインシデントも増加しつつあります。そこで情報セキュリティの観点からいえるリスクなど、当社の見解を述べています。こういった移りゆく環境の中でセキュリティへの高い意識を持つことは大切です。しかしながら、万が一の事態というのは付き物。広報活動のプロの視点から、サイバーインシデント発生時の事後対応など想定しておくべきことも特集しています。さらには、物心がついた頃からインターネットやスマートフォンなどに慣れ親しみ、デジタルとの高い親和性を持つ若年層のサイバーセキュリティ意識も問うてみました。

当社は昨年開催された第 3 回国際銀行フォーラムに参加し、貴重な情報を得ることができました。所感はもちろんのこと、懇意にいただいているアゼルバイジャン中央銀行の国際決済システム開発部門長とのやりとりから見てきた、アゼルバイジャンの金融機関におけるデジタル化の展望を探り、さらには世界のキャッシュレス化に向けた動向にも迫ります。

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 3,940 組織、18,000 を超えるシステムで利用されています。



CONTENTS

- 01 はじめに
- 02 目次

巻頭特集

- 03 対談：サイバーセキュリティ最前線

特集

- 07 情報セキュリティ講義回想記
～社会へ旅立つ若者たちへ伝えたこと～
- 11 「クラウドファースト」な時代だから考えるべき
クラウドサービスの情報セキュリティリスク
- 15 アゼルバイジャン国際銀行フォーラム報告と
世界のキャッシュレス動向

注目テーマ

- 19 鈴木 孝徳 氏に聞く
パブリック・リレーションズと危機管理対応
～もしものときのコミュニケーション術～
- 23 診断の現場から
- 25 情報 Security Column

現状分析

- 27 診断結果にみる情報セキュリティの現状
- 27 2018 年下半期 診断結果分析
- 32 WordPress の普及とセキュリティ
- 35 2018 年下半期カテゴリ別脆弱性検出状況
Web アプリケーション／ネットワーク
- 37 業界別診断結果レーダーチャート

※ 本誌において記載されている会社名、商品名、サービス名は各社の商標または登録商標です。なお、本文中では商標または登録商標を表すマークを特に提示していない場合があります。



この冊子は、クリエイティブ・コモンズ表示 4.0 ライセンスの下に提供しております。
二次利用にあたっては、出典明示（出典：株式会社ブロードバンドセキュリティ発行『SQAT® Security Report 2019 年 3 月号』）をお願いします。
また、商用利用は許諾しておりません。

SQAT® は BBSec の登録商標です。登録商標第 5146108 号

サイバーセキュリティ最前線

合同会社エルプラス
代表社員
杉浦隆幸氏

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

日進月歩のサイバーセキュリティ。昨年「一般社団法人日本ハッカー協会」を設立し、サイバーセキュリティ、システム開発、IoT などさまざまな分野でハッカーに活躍の場を提供し、ハッカーの地位向上と活躍によるネット社会の安全や健全な発展を通じて日本のセキュリティの進歩に寄与する杉浦隆幸氏に、当社セキュリティサービス本部副本部長 齊藤義人が忌憚のない意見をぶつけました。

※当社は一般社団法人日本ハッカー協会の賛助会員です。

BBSec：まずはお二人に、昨年の総括と申しましょうか、2018年に起こったサイバー事案についてお伺いします。

杉浦：総括といいますか、2018年は仮想通貨まわりの事案が大きく動きまして、2018年1月にはCoincheck（コインチェック）^{*1}、9月にはZaif（ザイフ）^{*2}、Monappy（モナッピー）^{*3}の話題が世間をにぎわしましたね。被害額が通常では考えられないくらいの桁数が出ておりまして、500億とか、お金が絡んでハッカーが本気になるのと被害が大きくなるということが証明された感じです。

齊藤：金銭的な動機があった、ということが明確に現れてますね。2017年はランサムウェアとか小金を狙っていたのが、2018年では変化があった。インターネットで巨大な金額が動くとなれば、当然そ

ちらがターゲットになっていくわけですね。

杉浦：そうですね。ランサムウェアの場合も、小金と大金がありました。世界的な傾向として、データベースを狙うなど、金額が大きくなった感じですね。

齊藤：攻撃者の成功体験が、またその先の誰かの攻撃手法になっていくという。

杉浦：目立つ成功は真似されやすいですね。

齊藤：仮想通貨のお話はまさに杉浦さんのご専門ですが、先に話の出たZaifの事件は新聞にも掲載されて一般の方にも話題になるほどでした。元々OSINTコミュニティでMonacooinを追っている途中で、突然Zaifの話が出てきたという経緯があったため、有志の動

きがものすごく早かったと聞いています。いわゆるハッカーと呼ばれる人々が一気にビットコインのシステムのハッシュを集めて...という動きを、警察で実施するとおそらく膨大なコスト（人件費）がかかるので、同じようなスピードで対応するのは難しいのではないかと思います。こうしたハッカー有志が動けるというのは、言い方が正しいかどうかはともかく、経済効果がすごく見えてきたのではないかなと思っているんです。社会的な貢献要素というか。

杉浦：ただ実際に彼らが集まるのも、私が企画（「Zaif 犯人追跡ハッカソン」^{*4}）した以上は将来的にお金が見えている可能性があるのでは（笑）。そうでないとあんな優秀な人たちを使えないですから、実際は。そういう仕組みをしっかりと整えて、それを実証することによって、将来的に同様の事件があった

^{*1} 2018年1月26日、仮想通貨取引所「Coincheck」が5億2,300万仮想通貨ネム（XEM）の盗難を受けた。時価換算で620億円相当。

^{*2} 2018年9月20日、仮想通貨取引所「Zaif」が不正アクセスを受け、暗号通貨3種類（BTC、MONA、BCH）の入出金を停止。総被害額は約45億円相当。

^{*3} 高負荷時におけるギフトコード機能の不備を利用した悪意ある攻撃により、Monacooinウォレットサービス「Monappy」でホットウォレットに保管されていたすべてのMonacooinが不正に出金された。総額は93078.7316 mona（時価換算で1489万2597円相当）

場合に、速やかに対応をとれるような体制^{*5}を構築することが大事ですね。結構な費用がかかるんですが、(官は)前例がないことに費用はかけにくい。ですから前例を作ってしまうというのが狙いではありますよね。

齊藤:それが実際に功を奏した、と。

杉浦:まあ、そうですね。ただ、犯人はほぼ特定できたものの、実際の逮捕は警察次第。氏名が特定できても捕まるかどうかというのはまた別の問題なので。そこが難しいですね。

齊藤:それはどうしても民間では届かないところというか。役割の問題ですよ。FBI なんかですと、サイバーアタックの犯人リストがあったりしますが、日本ではそういった動きはまだないですね。企業の対応もどうしたらいいですかね。例えば、これからも仮想通貨サービスはどんどん増えていつかは法律で縛りがより強くなってくると思いますが。

杉浦:それがまさに問題ですね。実は LINE さんは仮想通貨の取引所をしていらっしゃるんですけど、知らないと思うんですよ、皆さん。というのも、サービスの提供で日本と米国は除外されているという、非常によくはない状況になってしまっていて。コインチェック事件があったことで、認可側のマンパワーが足りないために認可がとれない状況ですね。

齊藤:なるほど。そんなことで日本の経済スピードを落としてしまうという可能性も出てくる、と。

杉浦:そうです。実際、規制があまりにも厳しすぎて経済スピードは落ちています。まあ、事件起こしたところで、ちゃんと対策したところは、十分強くなっていますけど。

齊藤:確かに、反動がありますね。

杉浦:ええ。相場モノですので、戻しは必ずあります。1 回落ちたら必ず戻すっていうのが。

齊藤:「不正マイニング」の話なんかはどうですか。

杉浦:あれは微妙ですね。ちょうど裁判も大詰め^{*6}、どこが不正でどこがそうでないのか、といったところで、セキュリティにかかわる人たちが怯えながら仕事しなきゃいけないというのが現状ですね。

齊藤:たとえ、著名な方であっても、研究のための範囲だといっても関係ないですからね。



杉浦:(警察が)捕まえやすいかどうかという、あまりよろしくない状況ですね。実はセキュリティは法的なラインが低いんです。そのため、捕まるときは大量に捕まる^{*7}、という。

齊藤:それは足枷ですね。

杉浦:セキュリティ業界全体の足枷となっております、これは。

齊藤:やはり日本企業全体で、セキュリティというものがリスクをとりながら行っているものなんだという理解が進んでいかないと難しいですね。いわゆる「ホワイトハッカー」、彼らが研究しないことには・・・。

杉浦:実際に守る側というのは、攻撃するすべての手段を想定しなければならないから難しい。攻撃する側は一つでも当たれば OK なんですけども。ひとつ突破口があれば皆それをまねてしまう。(攻撃側に)1 人優秀な人が存在すればそれだけでリスクになる。

齊藤:日本国内ではセキュリティエンジニアが不足しているといいますが、例えばトップエンジニアとなるべき人をどう教育していくか、という課題がこれまでずっと何年も解決できていません。杉浦さんは昨年、日本ハッカー協会を設立されましたね。

杉浦:先にお話したような、攻撃者に対抗できるトップエンジニアになるには、相当高いスキルが必要です。ところが、セキュリティエンジニアの世界は特殊で、犯罪と紙一重ですから、一線越えたような人たちが業界には結構いる。そのおかげで進歩しているのに、「一線越えてしまったら帰ってこれない」では困ります。彼らの活躍の場が必要ですし、また罪に問われないように保護する仕組みが必要だと思ったわけです。日本では凶悪犯であればあるほど捕まりにくい、という面があります。小中学生とか、未熟なスキルの人ほど

^{*4} 杉浦氏が呼びかけ人となり、CTF (Capture The Flag: 情報セキュリティの技術を競う競技) の優秀者らで不正出金に対する調査方法を考案、実証した試み。

^{*5} 一般社団法人日本ハッカー協会。

^{*6} 自身の Web サイトに「Coinhive (コインハイブ)」と呼ばれるコインマイナー用のプログラムを設置し、他人の PC を使用して不正マイニングを実施したとして、警察に摘発され、「不正指令電磁的記録 (コンピュータウイルス) 取得・保管」の罪で横浜簡裁から罰金 10 万円の略式命令を受けた男性が、これを不服として正式裁判を請求した訴訟。2019 年 1 月 9 日の公判では産業技術総合研究所情報セキュリティ研究センター主任研究員の高木浩光氏が「刑法犯で処罰されるものではない」と証言したことで話題を集めた。2 月 18 日結審。判決は 3 月 27 日予定。

^{*7} Coinhive 事件では 16 人が摘発された。

つかまってしまう。法的な知識もありませんし。そうすると、そこで将来が閉ざされてしまう。それを何とかしないと。

齊藤：脆弱性が発見されることに対する考え方も問題ですね。お客様の現場から、「何でこんなに脆弱性が見つかるんだ！」と聞こえてくることがある。いや、見つかったよかったじゃないですか、という話なんですけども（笑）。

杉浦：悪用される前にね（笑）。

齊藤：そうなんですよ、悪用される前に見つかったじゃないですか（笑）。そのためにやっているのに、「何でこんなに脆弱性が見つかるんだ！」となってしまう。

杉浦：まあ、そういうものは出てきて当たり前、逆に早めに全部出してくれというマインドを持っていただくことが必要ですね。むしろ何で出てこないんだ、というくらい。何も出てこないシステムはよほどしっかりした作りか、逆に脆弱性診断が実にやりにくいサイトか（笑）。

BBSec：診断しにくいシステムですか。結構あるものでしょうか。

齊藤：ありますね、診断がしにくい。何でこんなことになっているんだ、と。

杉浦：IPSが入っていて、一部しかコマンド飛ばないとか。アプリケーション診断なら、そういうものを排除してから実施したいというのはありますね。脆弱性が確定してからIPS入れて、防御しましょう、となるべきなんですけど。

齊藤：本来はそういった「生」のものにアタックをかけて、さらに防衛されている防衛装置の上からでもいけますか、という二段階の診断をするのが望ましいですね。最近では、WAFとかIPSもある程

度負荷をかけた状態の時には抜けてしまうというようなこともありますから、防御装置を入れてあるから大丈夫、ではなくて、その外側からもちゃんと見ていく、ということも必要ですね。

杉浦：特にエンタープライズ系のセキュリティというのは、全体的な統制がとれていないとか、実際動いてない機械が半数ということも多いですし。

齊藤：そうですね、IPSはどこかにアラートをあげるような設定を初期に行っていたとしても、だんだんチューニングがおろそかになって行って、実態と乖離してることがある。

杉浦：やっぱり運用は難しいですからね。全部アウトソーシングしているところも多いですしね。社員1万人くらいの大きい会社さんでセキュリティをちゃんとマネジメントしようとする、全部で20名以上のセキュリティ要員が必要になるでしょうからね。SOC（Security Operation Center）を作ったり、新しく導入したシステムのテストをすとか、インシデントレスポンス対策など考えると、やはりそれだけの人数は必要になります。なかなか自前でそれだけの技術者を用意するのは難しい。ですからセキュリティ専門企業をうまく使いこなすのが日本のセキュリティマネジメントのキーファクターですね。

齊藤：そのとおりですね。SIEM（Security Information and Event Management）なんかは多くの企業で導入していますが、本当に必要なログを有効な方法で取得しているか、あとで確認できるものになっているか、というところはまだまだハテナをつけざるを得ない。特に企業側で運用を始めますと、工数のこと考え始めますから。余計なログはとりたくない、とか。そういう考えに陥ってしまう。そうい

う意味でいくと、セキュリティ専門でそこだけを見ているようなところに頼んでいただくと、運用工数ありきのセキュリティにはならないわけですね。



杉浦：またセキュリティのスペシャリストは専門性が高いですから、いろんな事例を知っていた方がお客様に対するフィードバックも厚くなる。そういうことを考えると、社外の、豊富な事例を知っている専門家に依頼する方が有効ですね。社内で脆弱性診断を抱える意味はまったくないです。よほどたくさんのサービスを持っているなら別でしょうけど。

BBSec：一人の優秀なエンジニアが突破口となって飛躍してしまう、とのことでしたが、そうした攻撃手法や脆弱性の検証に苦労したお話があれば伺いたいのですが。

杉浦：検証自体、結構苦労しますよね。脆弱性を見つけるだけならバージョンチェックで済むこともありますよ。いま年間1万件以上の脆弱性が発見されるじゃないですか。専門家であっても、その数を全部追いかけるのは難しいわけですよ。

齊藤：CVSSの登録をするのがセキュリティエンジニアのマスト要件か、ぐらいの感じで（笑）。再現性の問題ですが、IoT機器なんかは、製品は大きなものなのでひとつしかお貸し出しできません、となったりすると、トライできる回数が非常に限られてしまう。そういったことが、検証が難しい要因となりますね。

杉浦：理想を言えば、「壊すのでひとつください」ですよね。いろんな検査をして結果的に壊していいものと、正常な振る舞いを見るためのもの。このふたつをください、です。

齊藤：本当に 1 回しかトライできないとなると、例えば Black Hat の DEFCON で、爆弾処理のトレーニングがあるんですね。ちょうどその一人目がクリアする前の記録を見ると、342 人とありましたので「ああ、342 人死んだんだな」と。実際に防ぎなさいという場合はどう検証しようか (笑)。

杉浦：無理やり、液体窒素で冷やして、爆発しないようにして、爆発するときは爆発用に困った中とか、あるいは敢えて爆発させてみて検証するとか、色々あるんでしょうけども。訓練としては面白いですよ。作ってみましょうか。爆発したら花火が上がるとか・・・ (笑)。

先ごろ 4 年ぶりに改定された OWASP IoT Top 10 でもファームウェアのアップデートをちゃんとしなさい、と言っているんですが、当たり前なのがやっと書かれたくらいです。IoT 機器は使われる期間が長いし、ある程度ユーザが考えていかなきゃならない部分もあるんですよ。

BBSec：企業でも忘れられた機器が残っていることがありますね。

齊藤：繰り返しになりますが、システムの運用を維持する、というのは本当に大変なことなんですよ。

杉浦：セキュリティコストが高い、といわれる一番の原因は運用の問題でして。運用もやっぱり費用がかかるわけですから、そもそもの設計段階で、安全性を担保しながら費用を軽減できる方法を考えておかなければならない。それをしないと、セキュリティをまともにやろうとした段階ですごく高コストになるんですよ。大体機器の 2 倍から 5 倍かかるというのが一般的です。コストばかりかかって実効性がないセキュリティになってしまったりするんです。それは経営層がちゃんと考えておかなければならない。予算は有限ですからね。



齊藤：例えば、建物の縁の下がどれだけゴミだらけでも住んでる人は気にしない、みたいな感じですね。放置していたらそこから腐って行って土台が緩んだりすることもあるし、誰か入り込んでくる可能性だってある。その辺をセキュ

リティに置き換えたときにどのくらい想像できるかでしょうね。

杉浦：誰も見てない、録画してない監視カメラがやたらあるけど・・・みたいな (笑)。ある程度の防犯効果はあるだろうけど、いざというときに役に立っていない。

齊藤：そういった防犯効果だけを求めるのであれば、高額な機器を導入するのではなく、代替機器でどうにかする、という発想も必要ですね。本当に必要な機能を適正に選んでいく、というのが大事です。先ほどの家の話でいきますと、お風呂場で覗かれるのを防ぐために防犯カメラを導入するのかというと、そこまでは必要ない。むしろ、お風呂場の窓の下に砂利を敷き詰める方がコストもかからず効果も高い。

杉浦：そうです、音が鳴るだけでも十分効果が得られますから。

齊藤：ですから、そうした全体像をどこまで描けるか、が重要ですね。

BBSec：仮想通貨を巡る話題から、日本のセキュリティ業界のあり方やトップエンジニアの将来を守りたい、という強いお気持ちなど、「サイバーセキュリティ最前線」にふさわしいお話を伺うことができました。本日は長時間ありがとうございました。

杉浦 隆幸氏

合同会社エルプラス 代表社員。Winny の暗号の解読にはじめて成功、ゲームのコピープロテクトの企画開発をはじめ、企業や官公庁の情報漏洩事件の調査コンサルティングを行う。昨今では仮想通貨の安全性確保、Android アプリの解析や、電話帳情報を抜くアプリの撲滅、ドローンをハッキングで撃墜するデモや、自動車のハッキングなどを行う。テレビなどの出演多数。

齊藤 義人

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副本部長。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。数年にわたる長期かつ大規模システムのプロジェクトマネージャーとして活躍。

特集 1

情報セキュリティ講義回想記 ～社会へ旅立つ若者たちへ伝えたこと～

株式会社ブロードバンドセキュリティ
取締役 海外及び先端技術担当 安藤 一憲



2019年、私の仕事始めは某大学での講義であった。当社の各部署にいる技術陣が持ち回りで講師を務める体裁で、私は昨年末の初回講義と、本年初めの第3回講義を受け持った。当社の技術陣の中には、初めて学生たちに講義をする講師もいたようだが、私にとっては経験もあり、不慣れな仕事ではなかった。講義前日に現地入りすると、大学のあたりは初雪がそのまま積もって景色が白くなっていた。

講義の共通テーマは「セキュリティ」である。初回の講義は、セキュリティという仕事の目的を理解してもらう一端として各国の個人データ保護の動向について。第3回目では、メッセージングのセキュリティについての講義をおこなった。学生たちに私が伝えたこと、私自身が大学の講義をしながら考えていたことなどをここに記したいと思う。

個人データ保護についての講義

個人データの保護にはおおまかにふたつの源流がある。ひとつは1940年代後半頃から世界的に議論され、憲法21条にも規定される「通信の秘密」であり、もうひとつは1980年 OECD 理事会勧告 8 原則に端を発する「プライバシー保護」の考え方である。インターネットが普及して通信の重要性が増した現代においても、「通信の秘密」はメタデータを保護する上で重要な役割を担っており、他方、プライバシー保護の8原則は日本の「個人情報保護法」や各国の「データ保護」の法律に反映されている。しかしながら、後者は比較的新しい概念であるために、1980年を境にその保護感覚に大きなジェネレーションギャップがあると指摘されている。学生たちには「古い世代は必ずしもこの概念が理解されていないことがある」と説明するわけだが、実は私自身の世代がその境界線上にいるので、時にその大きなギャップを実感する機会がある。


学生たちに OECD の 8 原則から話し始め、さらに日本や米国、EUでの対応状況を説明した。これを明らかにすることで初めて、米国の GAFA¹ の個人データ収集の何がどう問題なのか、中国の HUAWEI² 製品がなぜ問題視されるのか、といった説明が可能になる。もちろん、セキュリティで守らなければならないものの一端が個人データであることは議論を待たない。さらにこの 10 年ほどで発生したエ

ドワード・スノーデンの事件³、スノーデンが使っていたメールサービス「Lavabit」で起きた事件⁴、「Keys under doormats 論文⁵」の発表などの話を絡ませながら、個人データ保護の実装である暗号技術とバックドアの問題、従来の RSA 鍵交換の限界と PFS (Perfect Forward Security) に対する意識の変化、TLS の急速な普及、TLS 1.0/1.1 の危殆化、それらの事案が TLS 1.3 の仕様はどう反映されているのか、ストーリー仕立ての講義をおこなった。この手の動向は「こういう原因でこういう動きになっ

た」という理解が肝心なのだが、忙しい大人ほど「こういう動きになった」という結果だけを追いがちになる。結果だけを追っても全体像が見えないことが多く、せめて学生たちには、原因と結果という因果関係を明確にして、物事の素直な把握の仕方を身につけてほしい、という隠しテーマがあった。こういった背景から、前述のようなストーリー仕立ての講義をするに至ったのである。

ここ数年の各国の個人データ保護施策はかなり大きな変化を見せて

講義で使われた実際の資料



Keys Under Doormats:
MANAGING UNCERTAINTY BY REDUCING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS

Harold Alford, Steve Anderson, Ramon N. Beresni, Jack Buehler, Matt Green, Michael Hilt, John Killian, Matthew Green, Russ Lounsbury, Peter G. Neumann, Ronald L. Rivest, Jeffrey S. Schalk, Steve Schriener, Michael Szymanski, Daniel C. Whalen

Abstract

July 7, 2015

米国と英国の15人の暗号技術専門家らが2015年7月7日に発表した論文。

超ざっくりした主旨:

「政府による暗号製品へのバックドアの要求は、そのバックドアが誰に使われるかわからず、我々の金産業を脆弱にする。」


つまり、

「危ないからバックドアもうやめようよ」

という提案…。

スノーデン事件の余波

- Pervasive Monitoringへの警戒
 - 欧州が顕著(特にドイツ)
 - 米国本拠のクラウドサービスへの拒否感
 - 「データを自国に置きたい」という強烈な要求
 - GDPRを盾に個人データ保護の強化
 - 最近米国とのセーフハーバー合意の無効判決
 - 通信の暗号化への強い要求
 - DNSSEC
 - DANE
 - TLS



Copyright (c) 2018 Broadband Security, Inc.

きた。もちろん代表格は欧州一般データ保護規則（GDPR）である。対して米国にはいまのところデータ保護の連邦法がない。米国・EU間のセーフハーバー協定にも違法判決が出てしまっている。この状況だと、世界企業は欧州に本社を置いた方が個人データを取り扱うのが楽になる。日本は改正個人情報保護法で欧州のデータ保護制度に近づき、EUの求めるデータ保護について十分性認定が合意された⁶。こうして OECD の 8 原則をベースに並べてみると、EU、米国、日本、この三者の中で個人データ保護の整備が遅れているのは、明らかに米国である。

学生たちの中には HUAWEI のスマートフォンを使っている方がいたので、「Windows も Android も HUAWEI のスマホも、初期設定の時に何かしらのユーザのデータをどこかに送るのは同じかもしれない。しかし、そのデータを送った先の国での個人データ保護は国によって全然違う。」という話をそれとなくしておいた。ただ、中国の国家情報法の話まではしなかった。データ保護の文脈で話せる法律ではないからだ。

メッセージングのセキュリティの講義

年明けの講義も、前回と同じように前日に現地入りして臨む。北海道出身の私からすれば大して寒くはないが吹雪いていた。講義のテーマは「メッセージングのセキュリティ」。学生たちぐらいの年代は、メールを日常的に使うより LINE あたりがメインだろうなと思ったので、メールと SMS と LINE の三者を比較しながら講義を進めた。メールでどのようにセキュリティ確保の施策が進展してきたのか、順を追って説明した。

OP25B（Outbound Port 25 Blocking）、その副次的な効果としての SMTP 認証の普及、送信ドメイン認証の導入、スパム対策とスパムの送信方式の変遷、通信の秘密とスパム対策、フィッシングやスミッシングの最前線、リスト型攻撃、アカウント乗っ取り対策、BEC/SCAM、SMTP-STTS に至るまで。最初「なりすまし対策」の話を目にしていた学生たちも、スミッシングのように、SMS がフィッシングに使われ始めた理由を説明するあたりから顔色が変わってきたように見えた。盗まれた ID/ パスワードが流通し、使い回され、乗っ取られたアカウントに別の所で調達したクレジットカード情報を登録して商品を買うことで発覚を遅らせ、調査を面倒にする手法にも言及した。アカウントの乗っ取りに至る攻撃では、メッセージングに限らず、あらゆる種類のオンラインアカウントが標的になることも説明した。そして、クレジットカードと紐づけられているアカウントが攻撃者の最終目的であることも。

アカウント乗っ取りはメールや LINE、SNS のアカウントに限ったことではなく、その対策も特定のサービス（例えばメッセージング）

だけでやれば済むという話でもない。ただし、最初の切り口がメッセージングによる誘導であることが多く、被害が発生すると複数のサービスとカード会社にまでまたがった対応が要求されるのが現実である。国を越え、通信事業者、ドメイン登録事業者、ホスティング事業者、クラウドサービス事業者、クレジットカード事業者など影響は多岐にわたり、リアルタイムな連携がないと止めるのが難しい攻撃も出てきている。こと日本において、これらの事業者は省庁縦割りの下に分断配置されており、必ずしも普段から分野横断な連携があるわけではない。これから必要になってくるのは、国も分野も横断した連携ということになる。と書くのは簡単だけれども、世界の国をまたがって調整のできる場となると、あまり多く用意されているわけではない。

ここまで話した上で、オンラインサービスのパスワードを全部同じにしておくと、被害は単一サービスでは済まなくなることを学生たちに説明した。また、フィッシングサイトに ID/ パスワードを詐取されてから金銭的な被害が出るまでわずか 1 秒以下というケースもあることも解説した。現状、日本



での普及が遅れている DMARC^{*7} (Domain-based Message Authentication, Reporting, and Conformance) を有効利用できれば、フィッシングメールの多くをとらえられることも話した。送信ドメイン認証はひとつひとつを見ると大した効果がないように見えるけれども、実際の被害事例から見ると「これがあればなあ ...」という技術に見えてくる。よって、「何を守る技術なのか」と、「防げる被害の実例」を多数詰め込んだ講義になった。

彼らは将来、メールサーバで送信ドメイン認証を実装することはないかもしれない。しかし、就職をしてビジネスの現場に出た時には、ほぼ確実にメールを使うことにな

る。仕事で使う以上、メッセージングは安全に使いこなせなければならない。メールと SMS と LINE を比較しながらの講義は、学生たちが就職して社会に参加していく過程をカバーしているつもりである。メールにある送信ドメイン認証の結果は目立たないヘッダに書かれているだけでまったく存在感がないが、BEC や SCAM といった攻撃の端緒をとらえられる可能性がある技術で、怪しいと思ったときに確認する価値はあるのだ。もちろん、攻撃側がアカウント乗っ取りを使った場合には無力かもしれないが、何も無いよりははるかによい。

説明をしながら、これらの講義のシチュエーションはハリーポッ

ターでいうところの「闇の魔術に対する防衛術」を教えるスネイプ先生の授業を連想させるものだった。マグルの世界ならばそれは「セキュリティ教育」という名を与えられる。私の講義によって、彼らが例えばフィッシングの被害から逃れることができるのであれば、お安いものである。



安藤 一憲

学生時代からネットワーク／サーバ管理に 25 年以上従事。

古くはメーリングリストサービスから多言語での携帯サイト構築、携帯向けメール配信、ディレクトリハーベスティング対策、サーバ負荷分散、独自の DDoS 対策などを考慮した規模の大きなサーバシステムなどを数多く設計構築。1999-2006 年まで 8 年間、InternetWeek のメール系チュートリアル講師を務める。古くは Sendmail (MTA) のエキスパートとして知られるが、現在は社外との共同研究や M3AAWG 等国際会議に参加しつつ先端技術と海外を担当する取締役を務めている。

<プロジェクト担当実績>

- 2005 年 メール ASP (AAMS) を企画設計構築し事業化
- 2009 年 CrackerDetect EXOCET を企画立ち上げ
- 2012 年 メールアカウントの乗っ取り検知を実装
- 2014 年 Dovecot Pro/Scalality の導入を主導
- 2015 年 Splunk SIEM 導入を主導
- 2018 年 AI 搭載自動脆弱性診断サービスの監修

<その他>

WIDE プロジェクト研究員、奈良先端科学技術大学院大学との共同研究の窓口、M3AAWG メンバー

*1 Google, Apple, Facebook, Amazon、以上 4 社のこと。

*2 ファーウェイ・テクノロジーズ。中華人民共和国深圳市に本社を置く通信機器メーカー。

*3 2013 年 6 月、米国家安全保障局 (NSA) による個人情報収集に、大手 IT 企業が協力していることを記載した機密文書が暴露された。米中央情報局 (CIA) 元職員のエドワード・スノーデン氏が関与を名乗り出た。

*4 2013 年 8 月 8 日に突如サービスを中止した件。理由は不明だが、米国政府からの情報公開および情報へのアクセス権付与の命令に従わずに運営中止したとされている。

*5 2015 年 7 月 7 日に発表された、バックドアについて反対の意を表明した論文。
<https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf>

*6 欧州委員会は 2019 年 1 月 23 日、EU と日本が個人データに関する保護レベルについて、相互に同等と認める決定を採択したことを歓迎すると発表した。欧州委は、EU 「一般データ保護規則 (GDPR)」の第 45 条に基づいて日本に対する十分性を認定し、日本の個人情報保護委員会も EU 側に同様の対応を行うことで合意した。
<https://www.jetro.go.jp/biznews/2019/01/61496577e90fd3e8.html>

*7 電子メールにおける送信ドメイン認証技術のひとつ。送信元メールサーバの IP アドレス等が正当かどうかの判別や、メール送信者と内容が改竄されていないかどうかの検証といった認証を補強する技術。

「クラウドファースト」な時代だから考えるべきクラウドサービスの情報セキュリティリスク

株式会社ブロードバンドセキュリティ
高度情報セキュリティサービス本部
セキュリティ戦略コンサルティング部 部長 山田 伸和

クラウドサービスは、ここ 15 年ほどで急速に普及してきています。総務省から発表された『平成 30 年版 情報通信白書』によると、クラウドサービスを利用している企業の割合が 50% を超える結果であり、もはや企業活動に必要不可欠なインフラの一部といえます。その一方で、クラウドサービスを利用することによる情報セキュリティリスクが存在することも事実であり、クラウドシフトが進む中、水面下でクラウドサービスを利用したことに起因する情報漏洩事故をはじめとしたセキュリティインシデントが増加しつつあります。

本稿では、クラウドサービスを導入、運用していく上で、どのような情報セキュリティリスクがあるのか、よりセキュアに利用していくためには何が必要なのかといったことを解説するために、クラウドサービス利用で懸念される 5 つの事項を中心に紐解いていきます。

クラウドサービス利用で懸念される 5 つの事項
1. 統制対象における管理主体の違い
2. ベンダーと利用企業間の役割分担や責任範囲
3. クラウドサービスベンダーからの情報開示の問題
4. サービスの継続性に関する問題
5. すでに実施している各種セキュリティ対策にかかわる問題

統制対象における管理主体の違い

クラウドサービスと従来型のオンプレミス型（自社内あるいはデータセンター内に機材を設置、構築するタイプ）の大きな違いは、取り扱う情報資産を自社がコントロールできる範囲下にあるかどうかです。クラウドサービスでは、各種情報資産はクラウドサービスベンダーに「預ける」こととなります。まさに、「所有」から「利用」への転換です。ここで考慮しなければならないのは、情報資産が物

理的に預けられている国、地域はどこになるのかということです。国、地域が異なれば遵守すべき法令が異なることとなります。もし、海外のデータセンターに収容されている場合は、当然現地法令の対応が必要です。昨今話題のひとつである、個人情報をはじめとしたプライバシー関連法令も同様であり、各国、各地域によって異なります。このことから、情報資産の移転、管理に加え、知的財産に関する統制等で制約を受ける恐れが出てきます。

また、クラウドサービス自体の管理は、クラウドサービスベンダーが主体となることから、システム設計や情報セキュリティを含む運用ルール、サービスレベルの維持といった各種活動もベンダーに委ねることになり、システム障害、情報漏洩などのインシデントといった問題発生時の情報連携が十分にできない、あるいは想像以上の時間を要するといった事態が考えられます。さらに、問題発生後の影響範囲、原因究明に関する利用企業の関与が制限、制約されることで、問題解決が不十分となり、問題が再発する恐れがあります。これらは、クラウドサービスベンダーを選定する段階で吟味しておくべき事項であり、要求するセキュリティレベルに応じ、適正に選択することが必要です。そして、クラウドサービスへ「預ける」情報資産を事前に把握しておくことが重要です。どのような情報を取り扱うのか、情報資産のデータ価値

は高いのか、万が一データが流出した場合の金銭、機会損失、信用・ブランドの損失、あるいはデータが失われたときの事業継続性といったことを吟味した上で、適正なクラウドサービスを選定してください。

ベンダーと利用企業間の役割分担や責任範囲

クラウドサービスを利用すれば、セキュリティ対策はすべてクラウドサービスベンダーが実施してくれているはずだという話を聞くことがあります。しかし、それは大きな間違いです。ほとんどのサービスモデルで、一部あるいは部分的なセキュリティ対策はベンダーによって提供されますが、それ以外は利用企業側が実施することが前提となっています。これらを解説するためには、クラウドサービスの形態を理解することが必要です。

クラウドサービスでは、大きく 3 つの提供形態 (SaaS/PaaS/IaaS) が存在します。これらの提供形態は、それぞれ責任分界点が異なり、セキュリティ対策もクラウドサービスベンダーが実施している範囲を認識しましょう。すなわち、責任範囲外は、すべて利用企業が実施する必要があるということです。

• SaaS (Software as a Service)

さまざまな機能を有するアプリケーションを提供している形態です。アプリケーションそのものの管理、サービス運行、運用は、クラウドサービスベンダーが提供し

ます。したがって、ログインアカウント、パスワードの管理、作成したコンテンツやデータに関するアクセス制御、権限管理といったことは、利用企業側でポリシーを策定、運用していくことが必要となります。

• PaaS (Platform as a Service)

アプリケーションを稼働させるための環境を提供する形態です。データベース等のミドルウェアまで提供されていることが一般的です。利用企業は、データ、コンテンツに加え、アプリケーション開発と運用を実施する中で、セキュア開発や各種運用管理、脆弱性診断と対策、マルウェア対策といったことを実施することが必要です。

• IaaS (Infrastructure as a Service)

Amazon の AWS が有名です。クラウドサービスベンダーが提供するものは、物理的なネットワーク、サーバ環境と仮想サーバ環境を管理するための機能です。したがって、オペレーティングシステムからアプリケーション、データ、コンテンツはすべて利用企業側が必要なセキュリティ対策を講じる必要があります。

下記表は、クラウドサービスベンダーがセキュリティ対策を担う範囲をまとめたものです。

これまで述べた以外に次の事項も合わせて利用企業側で担う必要があります。

• 通信の暗号化

SaaS 以外の形態では、各種通信の暗号化 (VPN、HTTPS) 等は、利用企業側で講じておく必要があります。特に、公開 Web サイト、管理機能へのアクセス、ファイル転送等のメンテナンスは、インターネットを通じた通信が必要となることから、通信の秘匿化による盗聴、改竄といったリスクを低減させることを考えなければなりません。そのためには、強固な暗号化通信による保護を実施します。HTTPS や SSL VPN では、正式な認証局の署名を受けたサーバ証明書を用いた暗号化を実施し、通信先の真正性を保証することで、よりリスクを低減させることができます。

• 管理機能へのユーザ認証とアクセス制御

クラウドサービスでは、インターネットを通じた通信から各機能のコントロールを実施することになります。したがって、クラウドサービスの管理機能や保守、メンテナンスといった運用上の行為において、不正アクセス、情報の閲覧、改竄といったリスクにさらされている状態といえます。特に管理者向けの機能については、クラウドサービスベンダーからユーザ認証機能が提供されていることがほとんどですが、サイバー攻撃では最優先に認証が狙われており、被害も多く発生している背景から、昨今は ID/ パスワード認証による保護だけでは十分とはいえません。ID/ パスワードに加え、クライアント証明書、あるいはワンタイムトークン等を用いた二要素認証、

クラウドサービスベンダーがセキュリティ対策を担う範囲

	SaaS	PaaS	IaaS	セキュリティ対策
データ、コンテンツ	—	—	—	アクセス制御、権限管理、暗号化
アプリケーション	クラウド	—	—	セキュア開発、脆弱性管理 (脆弱性診断、改修等)
DB 等のミドルウェア	クラウド	クラウド	—	アクセス制御、権限管理、セキュリティパッチ
オペレーティングシステム (OS)	クラウド	クラウド	—	アクセス制御、権限管理、セキュリティパッチ
ハードウェア、ネットワーク	クラウド	クラウド	クラウド	物理セキュリティ、アクセス制御、権限管理、セキュリティパッチ
サービス運行、運用	クラウド	クラウド	クラウド	物理セキュリティ、変更管理、構成管理、運用ルール等

あるいは二段階認証を用いることで効果的な対策となります。もちろん、パスワードの強度や設定する権限の範囲についても適正に設定しておくことは重要です。

クラウドサービスベンダーからの情報開示の問題

情報の開示は、クラウドサービスベンダーのセキュリティルール、方式に大きく依存します。特に情報漏洩をはじめとしたセキュリティインシデントが発生した場合に問題となることがあります。例えば、原因特定調査を実施するために必要な各種ログデータが開示されない、あるいは、専門的なデジタルフォレンジック調査を実施するために必要なハードディスク、メモリ等の記録装置、あるいは仮想環境イメージといった証拠の提供を拒否されるケースがあります。その場合、利害関係者に対する説明責任を果たせなくなる恐れがあるといえます。クラウドサービスベンダーから PCI DSS や ISO27017 をはじめとした、国際規格の認証取得による適合性証明や合理的保証に関するレポートを開示しているものはありますが、サービス契約時に合意できる適正な情報開示が含まれているかどうかを確認しておくことが重要です。

サービスの継続性に関する問題

クラウドサービスベンダーにおける事業戦略の転換、経営状況の悪化、最悪の場合は破綻などにより、サービスが終了される、あるいは大きく仕様が変更される、サポートを受けられなくなるといった事態が考えられます。その場合は、当然利用企業におけるサービス継続、ひいては事業継続の問題に発展するリスクがあるといえます。こういった事態も想定し、クラウドサービスの長時間にわたる中断、停止を考慮したサービス環境の冗長化、あるいは代替手段を予め考慮しておく必要があります。

すでに実施している各種セキュリティ対策にかかわる問題

最後は、クラウドサービス利用に限定されるものではありませんが、同時に考慮しておくべき事項です。クラウドサービス利用にかかわらず、企業のネットワーク、OA 環境といったインフラ環境では、さまざまなセキュリティ対策を講じていることと思います。ほとんどの企業ネットワークでは、インターネットからの境界にファイアウォールを設置し、攻撃検知のための IDS/IPS、公開システムは DMZ へ設置し、セキュアな Web 閲覧のための Web Proxy、マルウェア対策といった多層構造による境界セキュリティを実装しているでしょう。こういったすでに運用されている企業インフラにおいて、クラウドサービスを利用する場合、ファイアウォールのアクセスを許可する、Proxy のアクセス先をホワイトリストで許可するといったことが必要となることがほとんどです。つまりせっかく堅牢に構築した多層構造の城壁に穴を開けているわけです。これは、いままで安全だと思っていた社内のネットワーク領域のセキュリティレベルが低下していることに他なりません。例えば、クラウド環境で運用している公開サーバを、ホワイトリストや VPN 等で社内インフラからインターネット経由でのメンテナンスを実施している場合、クラウド環境のサーバが攻撃を受け、侵入を受ければ、多層防御をもの

ともせず社内のネットワーク環境へ攻撃が到達してしまうことになります。つまり、作ってしまった穴がセキュリティホールになっているということです。クラウドサービスを利用するために実施した変更点については、十二分に吟味し、弱点になっていないかを常に監視、評価することが必要です。

昨今は、ゼロトラストという考え方が主流になりつつあります。これは、たとえ会社の中からのアクセスであっても信頼しないという、性悪説に基づいた考え方です。日々進化し、より苛烈となっていくサイバー攻撃の事情を考慮するとどれだけ備えていても完全に守りきることは現実的ではありません。何らかの問題が発生しても早く気がつき、被害拡大を防止するといった事故前提に基づいたセキュリティ対策が必要であることを念頭におくことが肝要といえます。

クラウドサービスは利便性や拡張性が高く、一定の対策はクラウドサービスベンダーにまかせるといったことから、ますます普及が進んでいくものと思われます。本稿で述べてきたとおり、クラウドサービスの利用においてさまざまなリスクがあることを認識し、理解を深めておくことがスタートラインです。クラウドサービスの本質は、情報資産をサービスベンダーに預けることにあるといっても過言ではありません。つまり、信頼できるサービスベンダーを選定す



ることはもちろん、自社でどこまでの対応が必要かを認識し、現実的に運用できる範囲を検討し、総合的に情報セキュリティリスクを把握、判断することが重要です。2020年の東京オリンピック/パラリンピックを来年に控えた2019年は、サイバーセキュリティ対策を推進する、まさに過渡期といえるでしょう。新たにクラウドサービスを活用する機会、あるいはすでに利用されている場合は、ここまで述べてきたことを参考に現状を見直してみたいかがでしょうか。

本稿の総括と参考資料

クラウドサービスベンダーは、クラウドサービス利用者とは独立した組織であり、クラウドサービス

の提供にかかわる資産に対する脅威、脆弱性および事故の可能性の評価に関する何らかの情報をクラウドサービス利用者に開示するかどうかは、専らクラウドサービスベンダー自らの事業判断に委ねられています。したがって、クラウドサービス利用者がクラウドサービスを選定し利用するときには、クラウドサービス利用者自らが情報セキュリティ要求事項を確立し、クラウドサービスベンダーに対して、その要求事項を開示するように要請し、クラウドサービスベンダーとの責任分界点を明確にした上で利用を開始することが望ましいわけです。

企業の担当者が適正なクラウドサービスかどうかを判断するためにも、例えば、クラウドサービス

を選定している段階であれば、情報セキュリティ要求事項の確立のためにセキュリティコンサルティングサービスを利用するか、すでにクラウドサービスを利用している段階であれば、定期的にクラウドサービスの脆弱性診断を行い、クラウドサービスベンダーに対する監査やモニタリングを実効的に実施することなども視野に入れて検討されることをおすすめします。

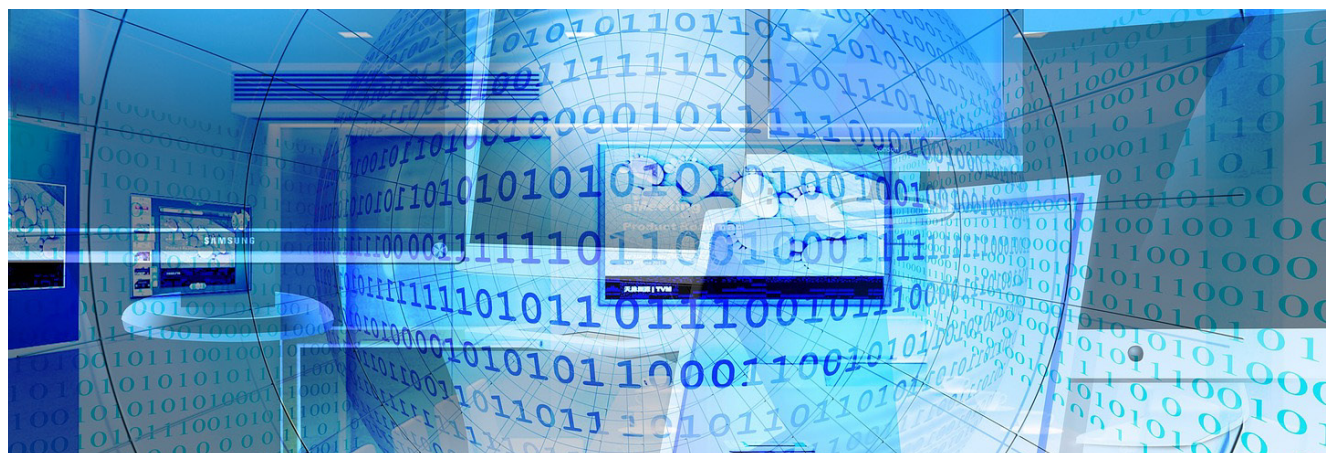
最後に、クラウドサービスの情報セキュリティ動向を踏まえて、その情報セキュリティリスクを検討し、情報セキュリティ要求事項を確立する上で規範となるセキュリティスタンダードやガイドラインを以下に紹介します。

セキュリティスタンダード・ガイドライン

- JIS Q 27017:2016 (ISO/IEC 27017:2015) 情報技術—セキュリティ技術—JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範
- 経済産業省 クラウドサービス利用のための情報セキュリティマネジメントガイドライン
- ENISA (欧州ネットワーク情報セキュリティ庁) Cloud Computing: Information Assurance Framework 【クラウドコンピューティング：情報セキュリティ確保のためのフレームワーク】
- ENISA (欧州ネットワーク情報セキュリティ庁) Cloud Computing: Benefits, risks and recommendations for information security 【クラウドコンピューティング：情報セキュリティに関わる利点、リスクおよび推奨事項】
- FISC (公益財団法人 金融情報システムセンター) 金融機関等コンピュータシステムの安全対策基準・解説書 (第9版)

山田 伸和

当社セキュリティ戦略コンサルティング部立ち上げの主要メンバーとして、情報セキュリティ全般に係る各種コンサルティングサービスの確立に貢献し、活躍している。金融業、製造業、流通業、IT 関連企業、独立行政法人等、幅広い分野の顧客向けに情報セキュリティリスクアセスメント、FISC 安全対策基準ベースの第三者評価、CSIRT 構築支援、情報セキュリティ文書策定、情報セキュリティ教育等のコンサルティング実績多数。



アゼルバイジャン 国際銀行フォーラム報告と 世界のキャッシュレス動向



株式会社ブロードバンドセキュリティ
セキュリティコンサルティングサービス本部
取締役本部長 雲野 康成 海外案件推進特命部長 増田 健

第2のドバイとも言われ、目覚ましい発展を遂げたアゼルバイジャン。炎をイメージして建てられた「フレイムタワー」が有名なこの国は今、金融インフラ構築が急速に進んでいる。昨年、同国で3回目となる国際銀行フォーラムが開催され、当社海外案件担当が招待された。本稿では、同フォーラムと世界のキャッシュレス動向について紹介する。

当社は PCI SSC (Payment Card Industry Security Standards Council) * の公認オンサイト評価企業 (Qualified Security Assessor Company、以下 QSAC) である。QSAC は、評価を行うにあたり、PCI SSC に活動可能な拠点 (リージョン) を登録する。

当社は、西欧、東南アジアおよびオセアニア、そして米国 (19 年 5 月時点以後の登録) を活動リージョンとしている。活動リージョンが固定であると、自社活動域外のリージョンとは関わり合いが少ないと思われるがちだが、実際そうではない。PCI SSC 自体や国際ブランド等は、世界各国で会議を開催しており、それらに参加または招待される機会もあるからだ。

例えば、国際ブランドが APAC で開催する国際会議への参加機会を通じて、CEMEA (中央ヨーロッパ、中東、およびアフリカ地域) リージョン各国の要人と知り合いになることも少なくない。昨夏、当該リージョンに区分されるアゼルバイジャンの中央銀行国際決済システム開発部門長 Ramil Mahmudov 氏と懇意になる機会を得、同国開催の国際銀行フォーラムに招待された。

* PCISSC : 5 社の国際ブランド (VISA・MasterCard・JCB・American Express・Discover) により設立され、クレジットカードに関連する世界基準を管理・運用する機関



2018 年当社韓国支店が VISA サービスプロバイダ部門のアワード受賞 (左) 筆者: 雲野 (右) 朴韓国支店長

アゼルバイジャン共和国 (Republic of Azerbaijan) とは

国名は、アゼルバイジャン語で「火の保護者」の意味を持つ。首都はバクー (BAKU)。公用語はアゼルバイジャン語。面積は日本の約 4 分の 1 で、人口 990 万人、IMF による GDP の世界順位は 89 位。

同国は、2014 年の世界的な石油相場下落により、経済的に深刻な影響を受けた。そこで政府は、脱石油、経済の復興、活性化を図るため 2016 年後半「アゼルバイジャン共和国の経済見通しに関する戦略的ロードマップ」を掲げた。このロードマップをもとに、経済発展を持続的で確実にするためのモデルが徹底的に調査され、実行されている。外貨獲得に資する自動車レース招致や万博の誘致活動もそのひとつ。

先端的分野を中心に、民間中心の高付加価値事業を発展させ、経済環境を改善する施策が推進中であり、これらを支援するための金融政策、金融インフラ強化政策も掲げられている。2015 年~ 23 年の予想成長率は 150% を超える。



出典: 外務省ホームページ
アゼルバイジャン共和国

第3回国際銀行フォーラム

国際銀行フォーラムは、アゼルバイジャンの国家新・戦略リリースの時期と重なるように 2016 年 11 月に第 1 回が開催され、今回は第 3 回である。フォーラムの目的は、金融インフラ発展のために世界各国、自国の動向をモニタリングし、討議すべきプラットフォームを関係者に提供し、成長に資する解決策の発見を支援、後押しすることである。

2018 年第 3 回国際銀行フォーラム	
主催者	アゼルバイジャン共和国中央銀行、金融市場監督庁、経済改革分析センター、アゼルバイジャン銀行協会
テーマ	キャッシュレス経済：伝統的な銀行業務からデジタル銀行業務への転換
参加者	米国、日本、ヨーロッパ、中国、CIS（旧ソビエト連邦構成国）諸国などの 100 以上の国際機関や企業から 600 名が参加
その他	・ 昨年設立、今年サイバーセキュリティ法を起案した運輸通信先端技術省も講演 ・ ロシア、モンゴルも出席

同フォーラムでは、2 日間で三つのパネルディスカッションが用意されており、取り扱うトピックスは 30 を超える。講演やパネルディスカッションには、MasterCard や Discover といった国際ブランド、またシティバンクやコメルツバンク AG、ライフアイゼンバンクインターナショナル AG、スタンダードチャータードバンクなどの巨大銀行、さらには個人信用情報機関、技術企業、監査法人などから、一見さまざまな分野に見えるが共通の目的や意志（金融インフラ発展）をもつ有識者 45 名が登壇した。当社は東アジア諸国の中で唯一のセキュリティベンダーとして招待された。

オープニングスピーチを務めたアゼルバイジャン銀行協会会長 Zakir Nuriyev 氏によれば、デジタル化がアゼルバイジャンの銀行システムをけん引する鍵になるという。同氏によれば、2012 年から 2017 年にかけて、銀行が金融テクノロジーを導入するためにかけた費用は約 3 億 1,000 万マナト（日本円にして約 19 億 8,400 万円）。この投資により銀行は、中期的に大きな収入を得ると考えられ、実際、インターバンクでの取引高は 2017 年で 2,100 億マナト。2018 年末までに 2,550 億マナトにも上る見通しと述べた。一方、アゼルバイジャン中央銀行第一副総裁 Alim Guliyev 氏によれば、アゼルバイジャンの現金支払いの割合は最終的に 74%から 40%にまで減少するとの見通しだ。年 7%の割合で現金以外の支払いが増加している。ただし、それには経済のデジタル化が重要課題である。

初日のパネル「銀行の変革」は、午前と午後大きく分けて行われ、20 以上のトピックスが議論された。

午前は、決済技術の未来や将来の課題のほか、デジタル銀行の鍵としてのオムニチャネル戦略、QR キャッシュレス社会、イノベーションの組み込み、ロシア企業が進める迅速な決済システム、スマートバンキングなどが討議された。また、日本でもカード会社の外部委託先として進出している Total System Services 社（米国のクレジットカード処理会社）の決済処理ソリューション、遠隔銀行口座開設プロセス等の紹介が行われた。

午後には、前述の Ramil Mahmudov 氏がパネルの司会役となり、さらにトルコ・イスタンブールとアンカラに拠点を置く Biznet Bilisim 社の Sefa Karabulut 氏がパネリストの要として登壇した。トルコの銀行数行がアゼルバイジャンに進出し、経済に貢献していることもあって、セキュリティ企業である Biznet Bilisim 社はアワードも受賞。トルコにおける「PCI DSS」の準拠状況について語った。



(左) Ramil Mahmudov 氏
(右) Sefa Karabulut 氏

フォーラムの 2 日目は、昼食を挟んでの 2 部構成。第 1 部は「金融機関の顧客確認 (KYC) およびアンチマネーロンダリング (AML) プロセス統制の自動化」がテーマとなり、KYC レジストリや制裁審査、禁輸政策、GDPR 等のトピックスが取り上げられた。第 2 部では「デジタルバンキングおよび司法リスクの司法規則」をパネルのテーマに、金融システムのデジタル未来、財政のデジタル未来、デジタル（電子）取引の司法的根拠、電子署名、FATCA および CRS、電子廷吏システムなどのトピックスに関するプレゼンテーションが開催された。

日本がバブル崩壊後、真摯に取り組み始めた①Swift 等の金融インフラプロセスの進展②IT技術の進化とともに普及したインターネット取引と同時に対峙しなければいけない不正利用、マネーロンダリングの回避③そして昨今のキャッシュレス社会の到来が、同時期

にこの国に到来、押し寄せた感覚を強く覚えずにはいられない。また、この強烈な動向に対して、果敢に中央銀行が（それも決済システム部長が他国の信頼できるパートナーを自らの足で探しつつ）オープンマインドで自ら動きソリューションの決着に動こうとしていることに感銘を隠さずにはいられなかった。

フォーラムを終えて

フォーラム終了後、筆者（増田）のもとには Ramil Mahmudov 氏からさまざまな問い合わせや依頼が来るようになった。多くは Cashless Azerbaijan 2020 の構築に関する問い合わせであり、官民学連携による当該プロジェクトに対し助言が求められている。すでにプロトタイプでは、銀行 30 行が名を連ねており、中央銀行主導で政府ペイメントポータルの開発を進めている。さらにアゼルバイジャンでは、金融政策について「アゼルバイジャン共和国における金融サービスの開発に関する戦略的ロードマップ」を発表しており、同ロードマップに沿ってデジタルバンキングサービスにおける銀行専門家の知識とスキルの向上を図っている。「2018 年から 2020 年までのアゼルバイジャン共和国におけるデジタル支払いの拡大に関する国家プログラム」も策定されており、今後も着々と金融デジタル化が進められることだろう。現状を鑑みても、アゼルバイジャン国内では銀行 ATM の利用率が極端に低く、キャッシュレス化は急速に進展すると考えられる。また、電子政府構築ではエストニアが協力するなど、国家群も関与しており、同国の金融インフラ等は飛躍的な進展を遂げると予想される。

アルファベットの表記が N で国名が終わる国は 26 カ国あるが、その中で J が付く国は Azerbaijan、Japan、Jordan、Tajikistan の 4 カ国のみであり、筆者らは西アジアに位置する Azerbaijan に親近感を覚えたのであった。

世界のキャッシュレス化動向

最後に、現在、筆者らがまとめた世界のキャッシュレス化動向について記載する。

現金決済システムの 問題点	<ul style="list-style-type: none"> ATM 維持管理・現金輸送・新札発行などコストがかかるシステムである。 GDP 比: 日本 (1.4%)、シンガポール (0.52%)、インド (3.2%)。あらゆる決済手段を利用できる環境が経済好循環を生むと考えない環境。
電子決済システムの 問題点	<ul style="list-style-type: none"> 銀行口座保有率が 50% 未満の国があり、銀行口座に紐付いたシステムが展開困難。 クレジットカード加盟店への手数料が高く、カード利用者に転嫁できない。 連合ロイヤリティの展開が主流となる中、排他的なポイント還元サービスの残留が目立つ。

出口戦略

キャッシュレス化の進捗を評価する上で、現金流通量残高 /GDP は目安になるが、中央銀行の動向・銀行口座保有率・ATM 設置台数・高額紙幣発行枚数などから、各国が選択する出口戦略は一意的に決定しやすい傾向にある。

各国の状況（代表例）

スウェーデン	中央銀行のもと、大手銀行 12 行が共同開発した Swish が国民の 60% に普及。Mobile Bank 認証の信頼性が向上したことで浸透。スウェーデンの個人識別番号制度の歴史は古く、1947 年にさかのぼる。
中国	ATM が少なく、与信管理ができないことから QR コード決済が進み、他国にシステムを輸出。
インド	高額紙幣廃止でキャッシュレス化が進む。また、銀行口座保有率が低いため QR コード決済が進む。
フィリピン・インドネシア	銀行口座保有率が低く、華僑進出により QR コード決済が普及。フィリピンの Coins.ph はブロックチェーンを利用した金融システムであるが、東南アジアでは、シンガポールを除き、フィリピンにのみブロックチェーン企業がある。
韓国	政府推奨によりクレジットカード決済が普及。年間利用額の 20% が所得控除の対象となる。
エストニア	中央銀行が X-Road を展開。900 以上もの組織や企業と連携し、1,600 ものサービスを提供。電子決済はそのひとつ。また、X-Road をフィンランド、アゼルバイジャン、ナミビア、フェロー諸島にも輸出。
タイ	PromptPay が 2017 年に導入。現在、KBank が 1 位、SCB が 2 位の実績を誇る。

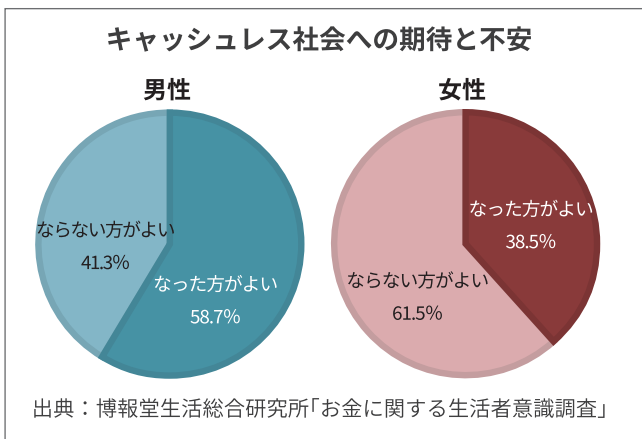


日本の状況

日本におけるキャッシュレス化は、他の先進国と比較しても低い水準にあるといえる。キャッシュレス決済比率は 2 割程度とされており、韓国では約 9 割、米国や中国でも 5 割前後であることを考えると（右：棒グラフ）、その低さが分かるだろう。経済産業省が平成 30 年 4 月に公開した「キャッシュレス・ビジョン」によれば、日本でキャッシュレスがなかなか普及しないのは、主に以下が原因であるという。

- (1) 盗難の少なさや、現金を落としても返ってくると言われる「治安の良さ」
- (2) きれいな紙幣と偽札の流通が少なく、「現金に対する高い信頼」
- (3) 店舗等の「POS（レジ）の処理が高速かつ正確」であり、店頭での現金取り扱いの煩雑さが少ない
- (4) ATM の利便性が高く「現金の入手が容易」

現金決済を好む国民性がキャッシュレス化を遅らせているといっても過言ではない。博報堂生活総合研究所が、キャッシュレス社会に「なった方がよい」または「ならない方がよい」の調査を実施したところ、次のような結果となった。



雲野 康成

日興証券株式会社（現 SMBC 日興証券株式会社）入社、株式会社インターネット総合研究所 経営企画室長を歴任後、株式会社ブロードバンドセキュリティ入社。日本における PCI DSS 黎明期から準拠支援ビジネスを立ち上げ、韓国支店では、韓国 QSA 案件シェア No.1 の礎を作った。その後 APAC 地域の PCI DSS 準拠支援ビジネスを立ち上げ現在に至る。

- PCI SSC 認定オンサイト評価人（QSA）
- ISACA 公認情報システム監査人（CISA）
- ISACA 公認情報セキュリティマネージャー（CISM）
- 情報セキュリティプロフェッショナル（CISSP）
- JCDSC（日本クレジットカード協議会）QSA 部会創生期からのメンバー

増田 健

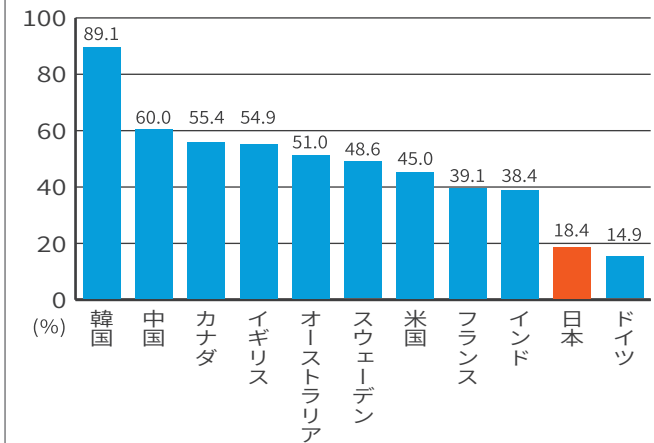
ロンドン育ち。大手メーカー海外駐在、外資大手イベント会社、経済産業省所管研究機関を経て現職。世界を目指す。

一言)「海外案件のご紹介をお待ちしております。」



(左) 雲野
(右) 増田

各国のキャッシュレス決済比率の状況（2015 年）



出典：経済産業省「キャッシュレス・ビジョン」

左下のグラフのように、女性は 6 割以上がキャッシュレス化に消極的であることが分かる。さらに興味深いのは、この調査で 40 代、50 代よりも、20 代、30 代の方が「ならない方がよい」と回答した割合が多いことが明らかになった点だ。柔軟性および多様性を持つ若年層にもキャッシュレス化への不安があることが伺える。

キャッシュレス化は、訪日外国人対応においても非常に重要な鍵となる。VISA 社の委託調査によれば、現金以外使えないことに不満を持つ外国人観光客は 4 割存在するとされている。さらに VISA 社は、現状のカード払いのインフラを改善しないと、2020 年に訪日外国人旅行者が 4,000 万人となった場合、109 億米ドル（日本円にして約 1.2 兆円）の機会損失が発生すると試算している。

政府は 2025 年に開催される大阪・関西万博に向けて、キャッシュレス決済の比率を 4 割へと 2 倍に引き上げる目標を掲げている。それでも、米国・中国に及ばないが、最近ではキャッシュレス化に関するテレビ CM も目にする機会が増え、今後どこまで普及するのかが期待される。



鈴木 孝徳 氏に聞く

パブリック・リレーションズ と危機管理対応

～もしものときのコミュニケーション術～

サイバーセキュリティの世界では、近年、事故前提社会の考え方が主流となり、CSIRT（Computer Security Incident Response Team）を構築する企業も少なくありません。しかし、こうした CSIRT も技術部門を中心に組織構築されているのが現状ではないでしょうか。一度、インシデントが発生すると、外部への公表が必要になりますが、外部に向けた対応を誤ることで、企業の評価を著しく損ない、いわゆる「炎上」が起こることも珍しくありません。本稿では、サイバーインシデント発生時の広報活動について、公益社団法人日本パブリックリレーションズ協会理事で株式会社井之上パブリックリレーションズ代表取締役社長兼 COO の鈴木孝徳氏にお話を伺いました。

パブリック・リレーションズとはあまり耳慣れない言葉ですが、これがサイバーインシデント対策とどう関係するのでしょうか。

鈴木：まずは、「パブリック・リレーションズ」という考え方からお話させていただきたいと思います。パブリックというと「公共」を思い浮かべると思うのですが、ここでいう「パブリック」は、「すべてのステークホルダー」「一般社会」を指します。つまり、マルチステークホルダーとのリレーションシップ・マネジメントが「パブリック・リレーションズ」なんですね。

現在、我々を取り巻く環境変化は驚くべきスピードで起こっています。また、情報の発信形態も大きく変化しています。情報を発信する企業や組織体、そして PR 企業、情報の受け手であるメディアがあ

ります。そうした中で、いかに正しい情報をマルチステークホルダーに届けるか、それによって例えば一度失われた企業の信頼をどう再構築するかといったメディア・リレーションズが重要であり、それはサイバーインシデントであっても変わらないと思っています。

セキュリティインシデント対応に関しては、CSIRT を構築されている場合が多いと思いますが、どうしても技術者が中心となりがちです。

鈴木：内容が内容ですので、やはり技術者中心に組織を作られるかと思うのですが、実際にインシデントが発生したときに、情報を伝える先が非技術者だということを考えなければなりません。取材される方、その記事をご覧になる方は、そこまでサイバーセキュリティ

に詳しくないと思った方がいいですね。一生懸命に情報を伝えても、正しく伝わるとは限らないわけです。そうした知識のギャップ、これにどう対応していくかが、実は大きな鍵といえるかもしれません。CSIRT における広報の役割というものこのあたりにあるといっても過言ではありません。ステークホルダーに納得していただけるような情報管理、といったことを考えていく必要があります。例えば、今、日本では残念ながら、ここ 3 年くらいに、日本を支えてきたような企業での不祥事が起きています。それが SNS を通じて拡散し、コントロールが難しくなってきました。

SNS が絡んでくると「炎上」の問題がありますよね。「炎上」してしまうと防ぐのは難しいでしょうか。

鈴木：炎上するのは、いくつかパターンがあって、「最初に出た情報が間違っていた」ケース、「最初に出た情報に不足があった」ケース、「情報自体が受け入れられない」ケースがあるようです。これを防ぐには、やはり初動が肝心ですね。メディアに情報が流れてしまったあとに緊急謝罪会見を開かなければならないような状況ですと、ある程度世間のイメージが出来上がってしまっています。それとは逆に、内部から出てきた不都合なことも含めて、積極的に情報を出していこうとする場合、これは大分違ってきます。

例えば、内部告発によって不正が発覚した場合、先手をとって発表してしまう、という方法もあります。「今後、こういう対策をとります」ではなく、「従来こういったことが行われていたことが内部調査の結果明らかになった、そのためこの部分を改善した」という情報発信の仕方ですね。反発する方もいるかもしれませんが、自浄作用が働いている企業だと印象付けることができます。

私が PR の仕事を始めた2000年頃は、インシデントの報告は新聞や雑誌というメディアを通じて広がるわけですから、風評被害の拡散には、1 週間から 2 週間かかったわけです。それがテレビになって、数日で広がるようになった。それがオンラインメディアからさらに SNS に変わって数分ですからね。この20年で3週間が3分になった、という感じですね。極端な言い方かもしれませんが、インシデントが発生してから 30 分以内に会見が行えるよう準備するよう心構えと準備をしておくのが大事だと思っています。

セキュリティインシデントですと、まず監督官庁に連絡しなければならない、ということもあるかと思いますが、そうしている間に世間の反応が進んでしまう、「隠してい

たのではないか」など憶測を呼ぶこともあるかと思いますが、このあたりのポイントはなにかありますか。

鈴木：これはサイバーに限ったことではなく、消防や警察への届出を優先しなければならない場合なども同じような悩みがあります。会見がずれ込んだ場合は、その背景をきちんと説明することが大事です。外資系企業の事例ですが、本社の了承を得ないと発表できないため、日本語の会見原稿を英訳して、本国で検討して、回答を日本語に再翻訳する、というプロセスが必要でした。すると日本国内で完結する企業と比較した場合、どうしてもおくれをとってしまいます。

こういった大きな案件では弁護士がかかわることも多いのですが、弁護士と我々の視点は必ずしも一致するとは限りません。弁護士は法律のプロですがコミュニケーションのプロではありません。我々は信頼関係をどう再構築するかに重点を置くので、情報の開示ラインが異なることもあるわけです。法律的に問題がない場合は、それを前面に出すべきです。また実害がないのであればそれも強調する。その上で、できるだけ早めに会見を開くことです。状況を見ているうちに、いつの間にか世論が盛り上がり過ぎてしまってタイミングを逃すと、隠れていたのだ、証拠隠滅だのと憶測を呼んでしまうことがあります。それとどのレベルの人間が会見で話すかの判断も重要です。社長が説明すべきなのか、担当部長・広報部長レベルの話なのか。その内容もさることながら態度も重要です。ご記憶かもしれませんが、昨年ある製造業での不正検査の謝罪会見で謝罪なのか何なのか分からない会見がありました。このときはメディアの反発を買ってしまい、それが視聴者に伝わって世論が形成され、結果、株価がガクッと下がってしまいました。

日本は意外とコミュニケーションをとるのが難しい社会なんですね。ハイコンテクスト型の社会、つまり「あうん」の呼吸とでもいいでしょうか、「俺の目を見る」で通じさせる文化でした。しかし、今はダイバーシティということで、多様な人種・文化・宗教観が混在してきています。ですから、俺の目を見ても通じないんです。この辺を理解する必要があります。

専門家がいくら擁護しても世間には響かない場合は、インフルエンサーを使うということも有効です。その業界の著名な方を介して情報を発信するのです。それから、ガバメントリレーションズを通じ、規制緩和が必要な場合もあります。米国の場合はロビイ活動が盛んですが、日本の場合はメディアをコミュニケーションチャンネルに、世論を形成する方法もあります。こういったさまざまなパブリック・リレーションの手法を駆使することが重要です。

例えば、近年ワンオペで炎上した外食産業の問題でも、ワンオペ問題が浮上した当初から改善目標が明確にありました。関与した弁護士の主導でゴールがはっきり示されていました。社内で決めた条件を満たさない店舗を閉鎖する、改善期間は 1 年間、ということで動いていたからこそ、フェイクニュースなどに対してもスピーディーに対策でき、世論も味方にできました。

先に伺ったように、できるだけ正確な情報を提供するとすると、ついエンジニアが頑張って説明しがちですが、ユーザの方には却って伝わりにくい。そのあたりのコミュニケーションポイントは何でしょうか。

鈴木：例えば説明資料としてプレスキットを活用すると思います。技術者の話を、メディア向けに、分かりやすい言葉と図解を



ら 2 ページ。ここに
 図表を入れる感じで
 すね。専門用語を使
 用する場合は、必ず
 用語解説を入れる。
 サイバーセキュリ
 ティ関係は日本語の
 訳が定まっていない
 もの、日本語に訳す
 と逆に分かりにくい
 用語もあるかと思
 います。それは無理に

そうもいかない。そこでメディア
 を通じて伝えるわけですが、メディ
 アに一番接しているのが広報です
 からね。例えば、投資家向けには
 インベスターズ・リレーションズ
 (IR 活動) をしますよね。お客
 さん向けにはカスタマー・リレー
 ションズを、このようなさまざま
 なリレーションズ活動を最終的に
 はメディア・リレーションズとい
 う形に落とし込んでいく必要があ
 ります。一度記事として出ると、
 投資家も従業員も、家族の方も
 ご覧になる。その伝わる範囲の
 大きさが非常に違いますので、
 すべての活動をメディア・リレー
 ションズに落とし込むことが大
 事です。

用いた資料を作っておきます。メ
 ディアの皆さんはセキュリティの
 専門家ではないわけで、こちらの
 伝えたいことと記事の間に齟齬
 が生じかねない場合があります。
 インシデントの記者会見で大事
 なのは、最終的に被害を受ける方
 が分かるように伝えるということ
 ですね。今話している内容でタ
 ーゲットに正しく伝わるのかど
 うか、その視点が大事です。そ
 のために、メディアの方が理解
 できるようなプレスキットを
 用意しておく。日頃から、社
 内でできるだけ分かりやすい
 表現に揉んでおくことです。

日本語にしなくてもいい。ただ
 最低限、読み仮名をつけたり、
 カタカナ表記などをつけておく
 ですね。

ちょっと手前味噌になりますが、
 弊社では品質管理という部署が
 あり、いまお聞きしたようなこ
 とをセキュリティ診断報告書に
 対して実施しております。技術
 者の報告を管理層や経営層に
 分かりやすく伝えるための作
 業をする部署ですが、ある意
 味、プレスキットの作成に似
 ているような気がします。

さらにいえば、いま、ソシヤ
 ルで炎上したものを、新聞なり
 テレビなりのトラディショナ
 ルなメディアが後追いつる流れ
 も出てきています。このような
 新しい情報流通の特性を理解
 することも重要です。

サイバーセキュリティというの
 は最先端の技術もあり、技術
 者でなければ分かりにくいも
 のもありますからね。そうい
 ったときにプレスキットがあ
 ると助かりますね。

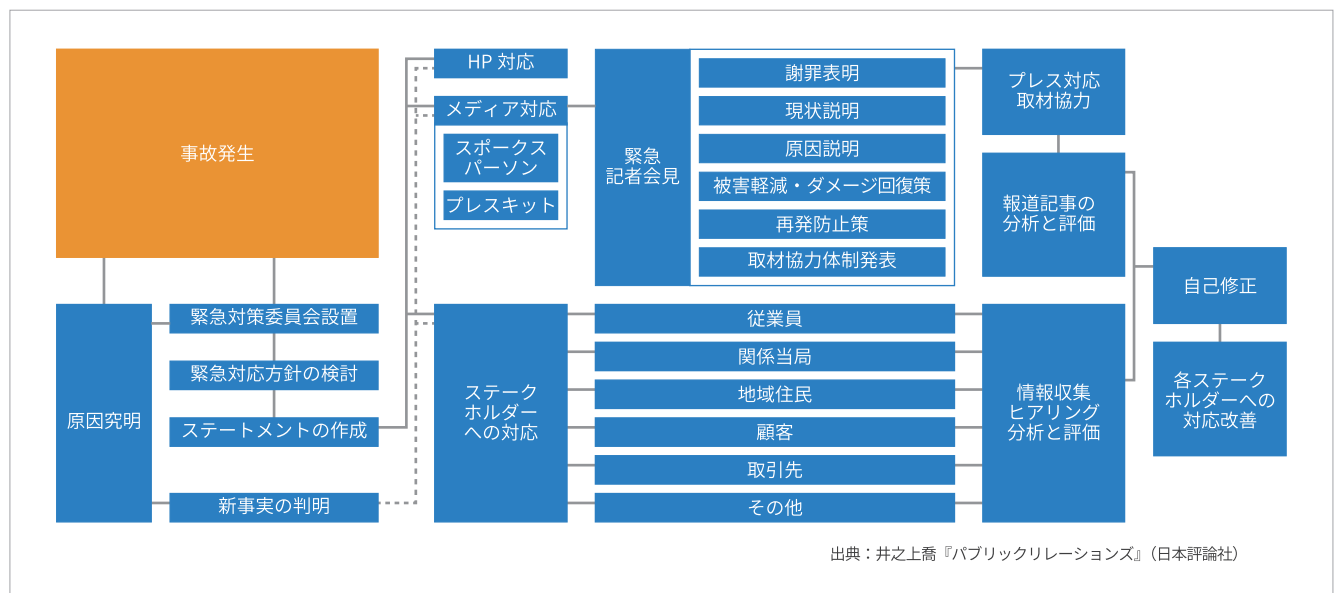
鈴木：それはいいですね。何
 のために作るのか、というこ
 とを考えればそうなると思い
 ます。同じように、インシデ
 ントの報告も広報の目を通す
 ことで、ユーザの側に立った
 資料を作ることができます。
 直接ユーザと話すという方
 法もあるでしょうが、なか

セキュリティインシデントの
 大きな特徴といえば、越境問
 題があります。データ漏洩が
 起きたとき、その対象が必ず
 しも日本国内であるとは限
 らない、そのあたりの勘所
 はありますか。

鈴木：長くても A4 で 1 ペ
 ージか

鈴木：海外に発信する場合、
 まず、言葉の問題があります
 ね。それが

クライシス・コミュニケーション時の緊急記者会見ガイドライン



出典：井之上喬『パブリックリレーションズ』（日本評論社）

ら関係する国の法律。個人情報を取ると、EU であれば GDPR、米国は各州で法律が違うので注意が必要です。中国の法令も注意が必要です。あとはスピード感も大事です。

先日もマリオットホテルで起きた情報漏洩事件に対して、アクションが遅いと集団訴訟が起きましたね。

鈴木：日本はグローバルスタンダードへの対応が後手後手にまわがちですね。もしもの場合の対応を事前に決めておかないと現地のスピード感についていけないことになります。今はネット社会ですので、余計にスピード感には注意を払っておく必要がありますね。

そのためにも、各国のレギュレーションへの対応を見える化しておく必要があります。そうはいつても、ガイドラインを読み込んで自社に対応できるまで落とし込むのはなかなか難しいことです。

一般の企業ですと、メディアとのつながりが薄いところもあります。そういった企業で、事前の取り組みはどのようにしたらいいでしょうか。

鈴木：例えば、CSIRT 構築時に PR 会社にコンサルを依頼するという方法もあります。日頃から関係をもっていると、いざというときの要点も分かります。何かあったと

きに相談できる先がある、というのも安心感につながります。

また、危機管理向けのメディアトレーニングも大切です。トレーニング参加者を 2 グループに分け、発表する会社側と質問する記者側とに分けてシミュレーションします。こういったシミュレーション計画もプラン段階で策定・実施するのが望ましいですね。

危機管理対応は広報だけでなく、全社で取り組まなければなりません。セキュリティインシデントであろうがなんであろうが、こうした視点でとらえておかなければ、いざというときに企業のイメージを守ることはできません。

誰に、何を伝えたいのか、という視点を持つことは技術者にとっても大事です。難解な専門用語、業界用語をいかにわかりやすく最終ターゲットに伝えるのか、PR の視点を持った技術者の方が一人でも多く増えることを願っています。

なるほど。CSIRT における広報の立ち位置とその重要性が理解できました。どうしても技術中心になりがちな組織にあって、こうした部門と連携する大切さを、技術部門の方に知っていただくことも必要ですね。本日はどうもありがとうございました。



鈴木 孝徳 氏

株式会社井之上パブリックリレーションズ代表取締役社長兼 COO
公益社団法人日本パブリックリレーションズ協会理事、教育委員会副委員長

これまでに世界トップの半導体製造装置メーカー、大手半導体メーカーなど半導体関連企業、通信インフラ大手、インターネットセキュリティ大手、ビッグデータ解析大手、CDN 大手などクラウドサービス関連企業、CES、CEATEC Japan、SEMICON Japan など国内外の展示会、国内外企業の社会貢献活動 (CSR) のコンサル、危機管理に関するコンサルなど幅広い PR 関連業務を実践している。

診断の現場から

Vulnerability Assessment

セキュリティサービス本部 診断サービス部

下地 菜月
浅見 まゆ

未経験から診断員へ

編集部員：こういった経緯で診断エンジニアになったのか聞かせてください。

下地：私はエンジニアになるつもりはなくて、元々美術の勉強をしていて、でも PC 触るのは好きだったから……という縁で BBSec に入りました。クローリング^{*1}の作業員として入って、そのときは診断までとは思っていなかったのですが、あるとき当時の上司から、診断もやってみないかって言われて。

浅見：私もリケジョではなく、文系でした。元々は横文字かっこいいくらいの気持ちでプログラマに。その後、派遣会社に入って Web 系の仕事をしたいと思っていたら BBSec を勧められて。「診断だったら Web にかかわれるよ」って言われたんです。で、「やりまーす」って、そんな感じで BBSec に入社しました。その後は私も下地さんと同じで、最初クローリング作業から入って、次は再診断^{*2}、その次は診断ってステップアップしてきました。

編集部員：お二人とも理系ではなかったんですね。

下地：私は全部 BBSec に入ってから知識を身につけました。とにかく業務をどんどんやっていたら結果的に知識が追いついていった形。

浅見：BBSec は OJT メインで、手を動かして実務を覚えるスタイルですね。そういうやり方が苦手じゃなければ、入社前に知識がなくても問題ないです。

診断という仕事

編集部員：仕事で気をつけていることや、大変だと思うことはありますか。

浅見：案件ごとに担当が決まっているのですが、体調を崩した人のフォローにいつでも入れるように、体調管理には

気をつけるようにしています。大変なのはシステムの構造が原因で診断速度が遅いとき、後ろ工程に影響が出ないように調整しないといけないところですかね。

下地：でも明確にゴールが決まっているから、自分のペースでやりやすいのはメリットかな。そこでイレギュラーなことが起きると、ペースが崩れちゃうのも確かで、それがデメリット。

編集部員：案件を担当することにプレッシャーを感じることはありませんか？

浅見：それほどプレッシャーじゃないです。やっぱり自分のペースでできるっていいですよね。ゴールを目指してこつこつやって。

下地：そもそも規模の大きい案件は複数人で分担することになっているので。そういうときにはチームワークですね。

編集部員：勤務時間はどうですか。残業は多くありませんか。

下地：そうでもないかな。深夜残業もありませんし。昔は今ほど人数がいなくて大変でしたけど。

浅見：私が入ったときにはもう深夜残業はなくて、下地さんのときが一番大変だったかもしれない。

下地：今は逆にあんまり残業すると怒られる（笑）。

編集部員：診断の現場は女性が活躍できる場だと思いますか。

浅見：BBSec は子育て中で時短勤務をしている人や、特定の曜日のみ出社という人もいるので、そういう意味では、女性が活躍できるかなと思ってますね。能力さえあれば、働く時間は調整しますよってスタンスがあるところが、うちの会社っていいなあって思います。

下地：比率として男性が多いってだけで、性別で活躍でき

*1 診断の前段階として行われる工程。対象システムの特性について把握するための重要な作業。

*2 診断で検出された脆弱性に対して、お客様側でのご対応後、ご希望いただいた項目について再度診断を行うサービス。

*3 情報処理安全確保支援士のこと。情報セキュリティ分野の国家資格のひとつ。

*4 Approved Scanning Vendor の略。クレジットカードのセキュリティ基準の管理や運用を担う団体である PCI SSC によって認定された脆弱性スキャンベンダー。

下地 菜月

セキュリティサービス本部 診断サービス部 診断2課

美術系の大学を卒業したのちに、IT系人材派遣会社を経て、当社に入社という経歴を持つ女性診断員。趣味はもちろん美術。顧客のシステム特性を考慮した診断を行うことのできる精度の高いスキルを持ち、また、診断結果をまとめた診断結果報告書の作成においては、丁寧な仕事ぶりで模範とされることも多い。

浅見 まゆ

セキュリティサービス本部 診断サービス部 診断3課

文系ながらもプログラマーとなり、IT系人材派遣会社を経て、Webにかかわる仕事がしたいと当社に入社した女性診断員。

趣味は音楽鑑賞。

入社後、持ち前の向上心を発揮して短期間で多くの診断実績を積み上げ、のみならず、さまざまな業務改善案を提案するなど、多岐にわたって貢献している。

るチャンスに差があるわけじゃない。女だから不利ってこともないし、体力勝負でもない。スキルがあれば、男だから、女だからってことがあるわけじゃない。性差というよりはそれぞれの個性。だから女だから得したってこともないけど、損したこともない。そんな感じです。

編集部員：職場環境においてメリットと感じていることを聞かせてください。

浅見：自分でスケジュール管理して休みを取りやすいことですかね。休みたいときに休めるのは助かります。女性に限らずですけど、例えばお子さんのいる人とか、子供の行事に行きたいじゃないですか、授業参観とか。そういうのに行きやすいかな。

下地：「美術は趣味でいい」と決めたんですけど、普通に仕事と趣味の両立ができてる。一昔前のIT関係だと家庭を犠牲に……というイメージがあったけど、BBSecの場合、男性も結構子供のことで休みをとってるかな。

浅見：それを堂々と言えますよね。「子供の行事だから」って。

下地：男性でも家庭のことをちゃんと両立できてる感じがある。

浅見：で、特に家庭のない人は趣味を続けられる。

下地：そうそう。

浅見：趣味のない人はどうするって言われたら困るけど、「……じゃあ仕事するう」っていう（笑）。

女性診断員のこれから

編集部員：これからの目標について聞かせてください。

浅見：登録セキスペ³を取るのが目標です。私たちはまだですけど、ASV⁴を取る人たちは、業務中に資格取得のための時間をとってますね。

下地：資格の勉強をするときに、外部の講師が教えてくれることもありますし。

浅見：(会社が)キャリアプランを考えやすくしてくれてるって感じですね。外部のセミナーもどんどん行くように推奨されます。

下地：プランがなくても、うちの会社にいると何か見えてくる……かな。

浅見：かな？ キャリアアップしたい人はすればいいし、趣味と仕事を両立したい人もいるし。みんながみんな、「そうしろ」ってところがない。

下地：私は偉くなりたいっていうのはないけど、部長も課長も、本部長にも女性がいるから、女性でもキャリアアップできるし。

浅見：女性だから課長になれない、部長になれないってことは全然ない。気持ちがあれば、というか。スキルと気持ちがあれば女性も活躍できる。

編集部員：では最後に。セキュリティエンジニアの中で、女性の割合は全体の10%以下なのだそうですけど、これについて何かありますか？

下地：単なるイメージの問題だけだと思います。

浅見：さっきの「生活を犠牲にして仕事をしなきゃいけない」感じが影響してるんじゃないですかね。

下地：他は知らないけど、少なくともうちの会社にはそういうのはない。そう考えると、女性エンジニアがこれから増えてもおかしくないかな？

浅見：業界としても色々女性エンジニアを増やそうって動きがありますし、きっとこれから女性のセキュリティエンジニアは、どんどん増えていくと思いますよ。





WordPress が WordPress を攻撃する？

WordPress (以下 WP) サイトが Bot 化し、その Bot 化した WP サイトが他の WP サイトに対して総当り (Brute-Force) 攻撃を行う事象が確認された。Bot 化した WP サイトは 2 万を超えており、現在も攻撃が続いている。

攻撃の概要

- C2 サーバおよび Bot 化した WP サイトから行われる攻撃は、WP の /xmlrpc.php に対して行われる。
 - 2016 年に猛威を振ったマルチコール攻撃と同じ仕組みだが、今回は総当り攻撃で認証を突破し、/xmlrpc.php に攻撃スクリプトを送り込む点に違いがある。
 - WP 4.4 以降のバージョンを使用している場合には、マルチコール攻撃対策が行われているため、影響は限定的と見られる。
 - WP 4.3 以前のバージョンを使用している場合には大量のログイン試行をフィルタすることができず、大きな影

- 響を受けるものと見られる。
- C2 サーバはロシア、ルーマニア、オランダにある Bulletproof ホスティングサービスにあることが確認されている。
- Bot 化した C2 サーバからは、攻撃スクリプトと同時に、総当り攻撃を Dictionary ベースで行うためのユーザ名とパスワードのリストをダウンロードし、総当り攻撃を実行する。
- ロシアにある Best-Proxies.ru を介して、C2 サーバの匿名化を行っている。

対策

- まずは、総当り攻撃対策として、アクセスログからログインの失敗を繰り返す IP アドレスを特定し、ブロックやアクセスの制限を行うことが求められる。ただし、Bot 化した WP サイトが 20,000 以上と多いため、いちごっこになる可能性も。
- WP 4.3 以前を使用している場合は、最新バージョンへアップデートすることも重要。

- また、自社の WP サイトが Bot 化していないか、ログイン試行の送受信や C2 サーバとの通信といった不審な通信の有無、総当り攻撃の実行の有無などから確認することが求められる。
- Bot 化している場合はクリーンアップが必要となるケースも考えられる。

参考情報
<https://www.wordfence.com/blog/2018/12/wordpress-botnet-attacking-wordpress/>



出典：<https://www.wordfence.com/blog/2018/12/wordpress-botnet-attacking-wordpress/>

●2018 年 12 月のトピックス



USB-Type-C™「認証プロトコル」導入

2019 年 1 月、USB-IF は、2016 年に定義されていた USB Type-C™認証プロトコルの導入を発表した。

認証プロトコルの導入で期待される効果

- 認証された製品同士のみ接続が確立
 - 接続時認証で、規格外製品から機器を保護できる。
 - USB 接続が悪用されるリスクを軽減できる。

従来の問題点

- 不審な USB との接続そのものは防げない
 - 規格に準拠した製品であっても、USB 経由のマルウェア感染を防げない。
 - 米ハネウェル社によると、自社顧客からサンプリングした調査対象の 44% で、マルウェアが入った USB が発見されている。
- 規格に未準拠の製品が多い
 - 未準拠の製品が市場に多く出回り、機器を破損する可能性も指摘されている。

<USB-C™ 認証ソリューションの概要>

- 1 USB 電源 / デバイス / ケーブル等に対する標準化プロトコルの採用
- 2 USB データバス / パワーデリバリの通信チャネルを使用
- 3 共通のセキュリティポリシーが適用される
- 4 あらゆる 128bit 暗号化方式への依拠
- 5 国際的に受け入れられている既存の暗号化手法を参照

USB 経由のマルウェア感染による被害は、制御システムを中心に世界中で数多くみられることから、認証制度の普及によるマルウェア感染の抑制が期待される。

●2019 年 1 月のトピックス

参考情報
https://www.usb.org/sites/default/files/2019-01/USB-IF_USB%20Type-C%20Authentication%20Program%20Press%20Release_FINAL_20181227.pdf
https://usb.org/sites/default/files/article_files/USB_Type-C_Authentication_PR_FINAL.pdf
https://www.automation.com/pdf_articles/honeywellps/Honeywell-USB-Threat-Report.pdf



パキスタンのほぼすべての主要銀行から顧客データが漏洩

2018年11月、パキスタン連邦捜査局(FIA)と米国の中央情報局(CIA)により、「パキスタンのほぼすべての主要銀行」から顧客データが漏洩し、ダークウェブ上で売り出されていたことが発表された。パキスタンの主要な22銀行から、約2万件のカード情報が盗み出されており、銀行システムに打撃を与えた。

データ侵害はすでに発生していたとみられ、漏洩したデータの一部はサイバー犯罪集団によって国際取引やATM、POSを介して米国やロシアを含む国々で現金化され、残りのカード情報が売り出されたものと思われる。パキスタンでは11月最初の週末までに少なくとも6つの銀行が

デビットカードを停止し、カード上で行われた国際取引のすべてをブロック。最初にサイバー攻撃の報告があったBank Islamiは、不審なトランザクションを停止し、パキスタン国内の生体認証を使用したATMカードのみ許可する対応を行った。

この件を受け、パキスタン国立銀行は、すべての銀行の代表に対して、情報技術システムおよび関連するカードの取り扱いのセキュリティ対策を改善するよう発令。ダークウェブ上で「PAKISTANWORLD-EUMIX-01」というタイトルのデータに、パキスタン国民のデビットカード情報が含まれていた。データには100~160ドルの値がつけられており、Citibankの

World Elite cardのような、より限度額の高いカード情報が1~35ドルの範囲で値がつけられているのとは比べ、高額である。

PakCERT社はこのことから、たとえ最初にデータを盗み出した(デジタルな侵入ではなくスキミング等の物理的な手段も想定される)のが国内グループの犯行であったとしても、その影にパキスタン国外の犯行グループの存在があると推測している。

一国の主要な銀行のほぼすべてでデータ漏洩が発生したことから、アジアのサイバーセキュリティ対策は欧米に比べて遅れているといわれている現状が浮き彫りになった。

No.	Bank Name	Type of Cards in the Darknet Dump	Number of Cards
1.	Bank Alfalah, Ltd	VISA (Prepaid, Classic, Platinum)	28
2.	BankIslami Pakistan, Ltd	VISA (Classic, Gold)	508
3.	Faysal Bank, Ltd	VISA (Classic, Gold, Platinum)	120
4.	Habib Bank, Ltd	VISA (Classic) Mastercard (Standard, Titanium, World)	6170
5.	Js Bank, Ltd	VISA (Classic, Gold)	355
6.	Samba Bank	Mastercard (Standard)	16
7.	Soneri Bank, Ltd	Mastercard (Standard, Gold)	333
8.	Standard Chartered Bank	VISA (Classic)	586
9.	The Bank of Punjab	Mastercard (Prepaid, Standard, Gold, Platinum)	748
TOTAL			8864

ダークウェブ上に売り出されていたカード情報の件数 (一部抜粋)

Thousands of debit cards of several other banks in Pakistan.

BIN	Credit/?	Level	TR1+2/TR2	Issuer	Country	SCode	Price
536619	Debit	Standard	TR2	Habib Bank, Ltd	Pakistan		\$100
462863	Debit	Gold	TR2	BankIslami Pakistan, Ltd	Pakistan		\$135
437460	Debit	Gold	TR2	Js Bank, Ltd	Pakistan		\$125
490471	Debit	Classic	TR2	Habib Bank, Ltd	Pakistan		\$100
421500	Debit	Classic	TR2	Standard Chartered Bank	Pakistan		\$100
536619	Debit	Standard	TR2	Habib Bank, Ltd	Pakistan		\$100
538967	Debit	Prepaid	TR2	The Bank of Punjab	Pakistan		\$110
454535	Debit	Platinum	TR2	Faysal Bank, Ltd	Pakistan		\$125

454535 thousands cards was posted on Darknet comprising of 2000 cards from Pakistan banks.

BIN	Credit/?	Level	TR1+2/TR2	Issuer	Country	SCode	Price
464578	Debit	Platinum	TR1+2	Standard Chartered Bank	Pakistan		\$125
428273	Debit	Classic	TR1+2	Dubai Islamic Bank	Pakistan		\$110
524521	Debit	Titanium	TR1+2	Meezan bank, Ltd	Pakistan		\$125
450086	Debit	Gold	TR1+2	United Bank, Ltd	Pakistan		\$135
420251	Debit	Signature	TR1+2	Bank Alfalah, Ltd	Pakistan		\$160
536619	Debit	Standard	TR1+2	Habib Bank, Ltd	Pakistan		\$100
428667	Debit	Classic	TR1+2	MCB Bank, Ltd	Pakistan		\$100
476215	Debit	Classic	TR1+2	Allied Bank, Ltd	Pakistan		\$110
517420	Debit	World	TR1+2	Habib Bank, Ltd	Pakistan		\$150

Screenshot of second dump from Darknet

ダークウェブ上に売り出されていたカード情報と値段

出典: <http://www.pakcert.org/img/PakCERT%20Threat%20Intelligence%20Report%20-%20web.pdf>

●2018年12月のトピックス



NSAが独自開発のリバースエンジニアリングツール「GHIDRA」を公開予定

米国国防総省の諜報機関である米国国家安全保障局(NSA)は、3月にサンフランシスコで開催されるセキュリティカンファレンス、RSA Conferenceで、独自開発したリバースエンジニアリングツール「GHIDRA」を披露すると発表した。その後、同ツールはオープンソースソフトウェアとして公開予定だという。

GHIDRAは実行ファイルからアセンブリ言語を生成して、人間による解析を手助けするGUIベースの逆アセンブラで、NSAによって2000年代初期に開発され

た。そして数年前から、さまざまなマルウェアや、疑わしいソフトウェア内部の仕組みを調べるサイバーチームを擁するほかの米政府機関と共有されていた。

GHIDRAが公開されれば、これを利用して新たにBug Bountyの賞金獲得を目指すユーザが現れるなどして、未知の脆弱性の発見と、その早急な改善に寄与する可能性がある。一方でGHIDRAを用いた悪意のある第三者による解析をもとに、攻撃が発生する危険もはらんでいる。

GHIDRAの概要

Javaベースのツール

動作OS: Windows, Mac, Linux

Windows, Mac, Linux, Android, iOS上のアプリの解析が可能

ハイエンドの市販ツールと同レベルの機能 + NSA独自開発機能を実装

無償のオープンソース

参考情報 <https://www.rsaconference.com/events/us19/agenda/sessions/16608-come-get-your-free-nsa-reverse-engineering-tool>

●2019年1月のトピックス

診断結果にみる 情報セキュリティの現状

～ 2018 年下半期 診断結果分析 ～

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

昨年からサイバー攻撃は新たな局面に入ってきたといわれる。技術的にはさほど高度でないものの、過去に流出した情報と組み合わせて膨大な金額を搾取する攻撃が増加し、まさにサイバー攻撃はビジネスとして成り立つ時代になった。各企業・組織は攻撃に対処するだけでなく、保有している情報資産等の管理・運用にも、これまで以上に注意を払わなければならない。あらゆる企業・組織にとって情報セキュリティ対策は喫緊の課題といえる。

その対策に欠かせない要素のひとつが、システム脆弱性診断である。当社では、技術者による高精度の手動診断と独自開発のツールによる効率的な自動診断とを組み合わせ、お客様のシステムにおける脆弱性を検出してリスクレベルを評価し、個別具体的な解決策を提供している。検出された脆弱性に対するリスク評価については、下表のとおりレベル付けを行っている。

2018 年下半期診断結果

当社では、2018 年 7 月から 12 月までの 6 ヶ月間に、14 業種延べ 441 企業・団体、3,790 システムに対してシステム脆弱性診断を行った。情報セキュリティ対策に重きを置く企業側の姿勢もあり、診断案件数は年々増加している。脆弱性のカテゴリ別、業界別検出率については P35 以降で触れているので、ご参照いただきたい。

診断の結果、Web アプリケーション診断では、脆弱性が検出されたシステムが全体の 84.9% と、前年同期（2017 年下半期）の 87.5% に比べ減少しているが、依然として高い割合である。ネットワーク診断においては、脆弱性が検出されたのはシステム全体の 61.7% と、前年同期（2017 年下半期）の 67.5% と比較して減少している。

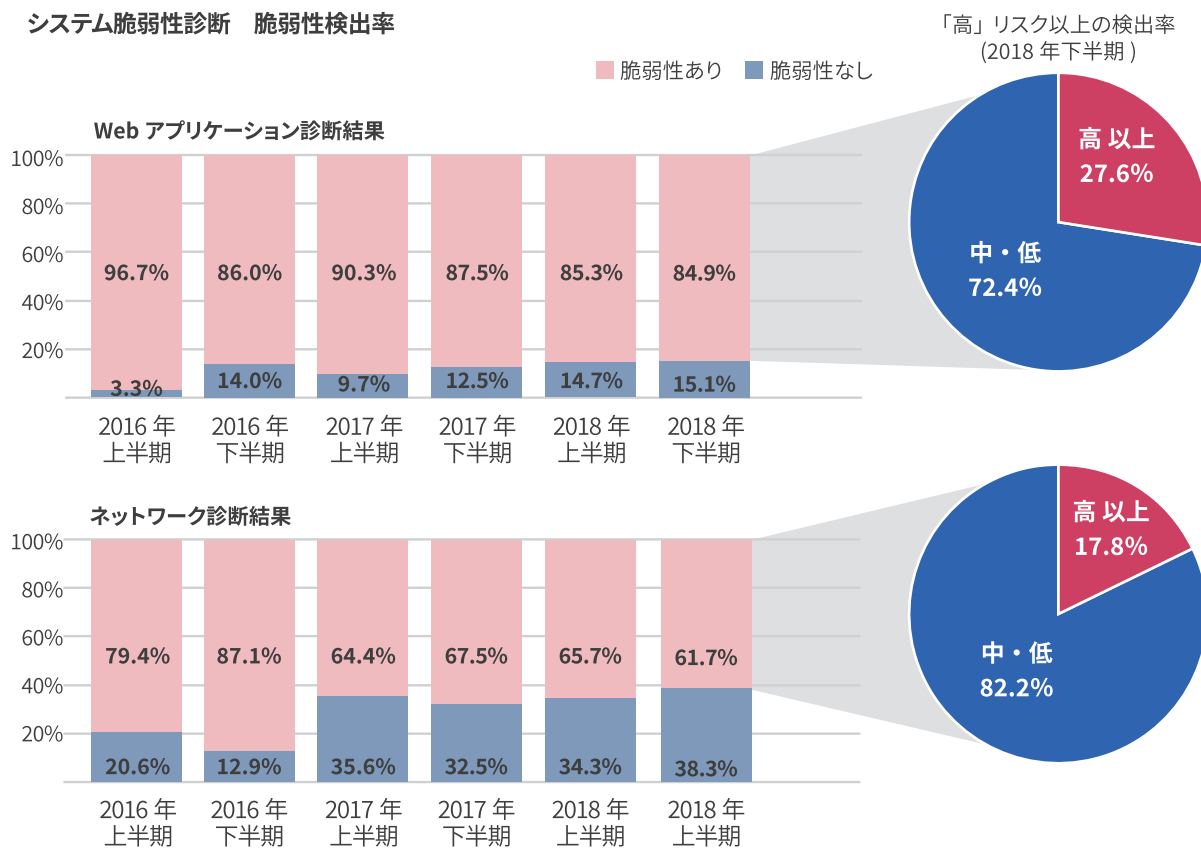
検出された脆弱性のうち、早急な対処が必要な「高」レベル以上のリスクと評価された脆弱性の比率は、Web アプリケーションでは 27.6%、ネットワーク診断においては 17.8%。2018 年上半期と比較して、脆弱性の検出率そのものはほぼ横ばいであるのに対し、高レベルの検出比率は、Web アプリケーションで 10.4% 増、ネットワークでは 8.2% 増とリスクレベルの高い脆弱性が増加傾向にある。

次のページより、診断カテゴリごとに 2018 年下半期の診断結果を解説していく。

システム脆弱性診断で用いるリスクレベル基準

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 脆弱性検出率



Web アプリケーション診断結果

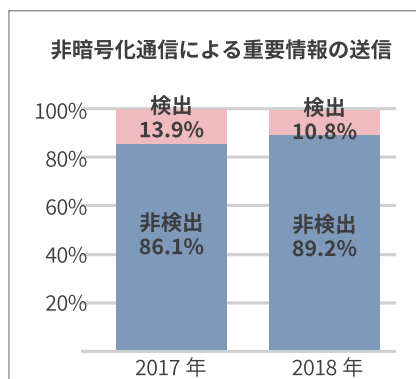
本稿では、昨今のセキュリティ動向を踏まえ、2018年下半期の当社診断結果において特に着目したい脆弱性について解説する。

重要情報の送信 一急がれる「常時SSL化」への対応

「常時SSL化」とは、Webサイト全体をhttpsで運用することだ。通信を暗号化しないhttpでは通信内容は平文のままやり取りされるため、万一データが不正に取得されてしまった場合、そのまま情報漏洩につながるリスクがある。それに対し、常時SSL化を行い、通信に堅牢な暗号化方式 / プロトコルを使用することでそうしたリスクを軽減できるのである。

現在、ECサイトのみならず、あらゆる公開Webサイトにおいてこの常時SSL化への対応が、急速に進んでいる。

Webアプリケーション脆弱性診断では、こうした常時SSL化の動きが活発化する以前より、平文で重要情報が送信されている状態に対し、「重要情報の取り扱い」というカテゴリにて脆弱性を指摘し、注意喚起を行ってきた。代表的な項目には、「非暗号化通信による重要情報の送信」（重要情報が暗号化されずに送信されている）がある。グラフに示すように、同項目の検出割合は減少傾向を見せているが（下記グラフ）、これは「常時SSL化」の流れが背景にあるものと考えられる。



常時SSL化への急速な対応の背景には、攻撃の高度化・巧妙化や、個人情報保護を求める法規制の強化といった要因も存在すると考えられるが、この半年で何よりも大きかったのはWebブラウザの提供元の動きだろう。

例えばGoogle Chromeの場合、2018年7月にリリースされたChrome 68から、httpで運用されているWebサイトには「Not Secure（保護されていない通信）」という警告が表示されるようになり、その後のリリースではこの表示がさらに強調されている。その他のブラウザでも同様に、httpのWebサイトに対しては警告が表示されるようになっている。

つまり、現在では、Webサイトが常時SSL化に非対応である場合、「警告」というユーザの不安をあおるラベルでそれがあらわになってしまうのだ。これにより、Webサイトに対するユーザの心証は損な



われ、企業の信頼性にマイナスの影響をもたらす。Web ブラウザの提供元が http への警告表示に踏み切ったことは、企業イメージへの影響を案じる事業者にとって何よりも強力な推進要因なのだろう。

Web ブラウザへの警告表示の実装は、ユーザ側の意識を否応なしに高める。今後、Web サイトの提供側は可能な限り「常時 SSL 化」への対応を進め、もし何らかの事情で当面 http にて運用せざるを得ない場合でも、その説明責任が確保できるような体制を整えておかなばならない。

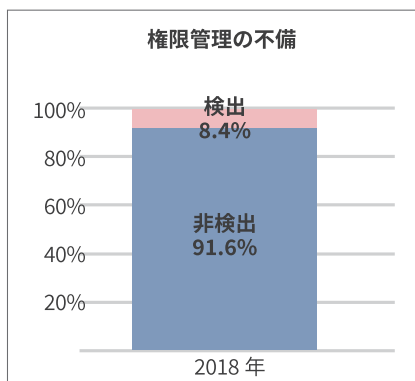
権限管理の不備 —自動診断では拾えない 設計ロジックの問題

もう1つ注目したいのは、「権限管理の不備」だ。当社診断における当該脆弱性の検出割合は、診断対象システム全体の 8.4% (右グラフ)。また、Web アプリケーションセキュリティに関する業界標準のガイドライン OWASP Top 10 の最新ランキングでは第 5 位のリスク (右リスト内の「アクセス制御の不備」) に相当する。

本稿では、当該脆弱性ならではの注意すべき側面—実際に攻撃が成功した場合のインパクト、インジェクションとは異なる脆弱性の特質、今後の拡大の可能性等—に着目し、この脆弱性を取り上げることとしたい。

まず、本脆弱性を一言で説明すると、「攻撃者が権限のあるアカウントのみに許可された特定の操作を実施することが可能となる問題」だ。管理者権限が奪取された場合にはあらゆる操作を不正に実行され得ることになり、その影響は甚大といえる。

さらに、この脆弱性には、自動スキャン等による機械的な診断では検出が難しいという特質がある。インジェクション等の脆弱性が、リクエストに対するレスポンスで機械的に評価できる問題であるのに対し、権限管理の不備は、アプリケーションの論理的欠陥 (権限管理の設計ロジックの問題等) に起因するものだ。どんな根拠でそのロジックを組んだのか、Web サイトの権限 / アクセス制御の機構を考察した上でないと不備を特定できない。



**OWASP Top 10
アプリケーションセキュリティリスク
- 2017**

- 1 インジェクション
- 2 認証の不備
- 3 機微な情報の露出
- 4 XML 外部エンティティ参照 (XXE)
- 5 アクセス制御の不備
- 6 不適切なセキュリティ設定
- 7 クロスサイトスクリプティング (XSS)
- 8 安全でないデシリアライゼーション
- 9 既知の脆弱性のあるコンポーネントの使用
- 10 不十分なロギングとモニタリング

OWASP Top10 - 2017 より当社作成

加えて、「権限管理の不備」が今後減る可能性は低い。Web ブラウザの画面遷移を設計して実現する従来のサービスに加え、API 通信を利用したスマホアプリでのサービスがますます普及すると見られるからだ。スマホアプリでは、Web サーバとの API 通信によってサービスを実現する。API は部品化されているため内部のロジックを把握せずともサービスが実現できてしまうという点が新たな脆弱性の温床となる。例えば、スマホアプリの実行動作上での制御機構のみに依拠し、API 通信のリクエストに対してアクセス制御の不備を検証する仕組みを実装しない。その結果、Web サーバのサービスには、「権限管理の不備」が潜在することになる。

「権限管理の不備」のような論理的な脆弱性には、自動診断ツールで検出が可能な技術的脆弱性とは異なる対応が必要だが、この点が往々にして看過されやすい。また、「スマホアプリに対応するということは新たな信頼境界に対応することを意味する」という点も見逃されがちだ。

対策としては、まず、アカウントの正当性および権限の確認チェックを実施し、Web サーバ環境内で包括的な権限管理を実装することが重要なポイントである。断片的な制御管理は徹底して排除することが必要だ。合わせて、設計の段階から権限管理に対するセキュリティ対策を組み込むことが推奨される。



ネットワーク診断結果

管理運用目的の プロトコルの検出状況

本稿では、ネットワーク診断での検出項目のうち、管理運用目的のプロトコルの検出傾向を振り返り、昨今の関連インシデントや攻撃の状況などと合わせて解説する。

取り上げるプロトコルの選定では、NICT（情報通信研究機構）が毎年公開しているサイバー攻撃関連通信の分析報告書『NICTER 観測レポート』の2018年度版を参照した。攻撃対象となっているポート番号の分布を確認すると（図1）、探索されているプロトコルのTop3はtelnet（23/TCP）、WindowsサービスのSMB（445/TCP）、そしてHTTP（80/TCP、81/TCP、8080/TCP）であった。

以降の解説では、上記3つのプロトコルに加え、当社診断で特に検出数の多いWindowsサービスのRDP（リモートデスクトップ、3389/TCP）を取り上げる。

図1
2018年の宛先ポート別パケット数分布
(NICTER 観測レポート2018より)^{*1}

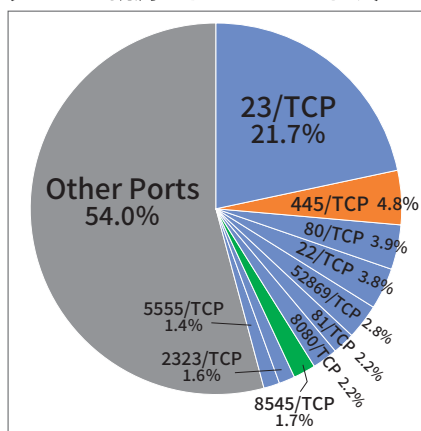


表1 当社診断結果における、管理運用目的のプロトコルの検出状況
(2018年7～12月)

	telnet	HTTP	SMBv1	RDP
オンサイト診断	149	61	427	392
リモート診断	1	25	1	4
計	150	86	428	396

なお、2018年下半期の当社ネットワーク診断の検出状況は、下表の通りである。

高いリスクをはらむ 非暗号化プロトコル telnet、HTTP

telnet、HTTPといったプロトコルでは通信が暗号化されず平文のまま送られるため、通信内容を盗聴される可能性がある。近年の傾向では、こうした非暗号化プロトコルの利用は全体的には減少してきており、外部からの非暗号化プロトコルの着信を許容しているケースは現在ではごくわずかに見られるのみとなった（表1「リモート診断」行）。しかしながら、組織の内部では未だに使われているケースが散見される（同「オンサイト診断」行）。

telnetについては、旧来からのバッチ処理に組み込まれていたり、古いアプリケーションやミドルウェアによる利用があったり、と一様に置き換えが進まない事情がある可能性が推察される。

HTTPについては、アプリケーションやミドルウェアにおいて、Web UIのログイン画面がHTTPとなっているシステムが検出されるケースが多い。おそらくHTTPからの移行が何らかの理由で困難であるため、やむを得ず利用しているものと思われる。

推奨される対策は、まずアクセス制限の実施だ。外部からの接続を

拒否し、特定のクライアントからのみの接続を許容するように設定を行う。加えて、HTTPはHTTPSへ、telnetはSSHへの移行を行うことが推奨される。

なお、telnet、HTTP以外の非暗号化プロトコルとして、FTPにも触れておきたい。FTPが許容されているシステムでは、やはり、バッチ処理や古いアプリケーション / ミドルウェアによる影響があるものと推測される。telnet、HTTP同様に、アクセス制限を実施した上で、暗号化プロトコル（SFTPやFTPS）への移行を進めていただきたい。

非暗号化プロトコルは、従来型の攻撃手法が通用するという点で容易に標的にされやすい。また、何らかの形で不正侵入に成功した攻撃者に攻撃の足場として悪用されやすいという面もあり、対策を取らずに放置しておくことは非常に危険だ。さまざまな事情で無効化や移行が難しいという場合も、そのままの状態に甘んじるのではなく、まずその利用を制限し、次いで、段階的にでも暗号化プロトコルへの移行検討を進めていく必要がある。

狙われやすい Windowsプロトコルの代表格 SMB、RDP

Windowsサービス関連で特に注意を喚起したいプロトコルがSMBとRDPだ。

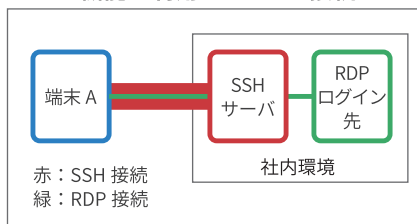
SMBのうちSMBv1は、2017年に全世界で大きな猛威を奮ったランサムウェア「WannaCry」で足がかりにされたプロトコルだ。すでに流行からずいぶんたつが、今も被害が報告されている。昨年秋には、パッチ未適用であった台湾の大手メーカーが攻撃を受け、製造

ラインが停止。莫大な損害が生じた^{*2}。また、「WannaCry」と同じ攻撃ツールを用いた「NRSMiner」というクリプトマイナーが現在アジア地域で猛威を振るっており、SMBv1 関連の攻撃はまだ収束したとはいえない状況だ。

SMBv1 への攻撃を防ぐには、Microsoft から供給されているアップデートを適用し、SMBv1 を無効化することが必須条件である。なお、この対策は、社内や外部から接続するクライアント・サーバ全体にわたって一律に実行する必要がある点に注意してほしい。

一方の RDP は、「SamSam」などのランサムウェアで足がかりにされるケースが多い^{*3}。総当たり (Brute-Force) 攻撃のほか、「ダークウェブで RDP の認証情報を購入してログイン試行する」という攻撃も確認されている。また、RDP には、「SSH ポートフォワーディングの機能を利用して接続を行う」という、一般的にセキュアと認識されている手法があるのだが (図 2)、それを悪用し、「ダークウェブ

図 2 SSH ポートフォワーディング機能を利用した RDP 接続



で SSH の秘密鍵を購入し、同機能を使って RDP をランサムウェアの踏み台にする」という攻撃も報告されている^{*4}。

以上より、RDP の場合は、SSH も含めた対策が求められるケースがある。まず、基本的な対策としては「環境内にあるクライアント・サーバで RDP を必要としない機器の RDP を無効化する」、「不審な RDP 接続がないか監視を行う」、「外部からの RDP 接続を許容しない」といったことが求められる。これに加えて、「サーバの中で、SSH を外部から着信可能にしており、内部で RDP を許容しているものがないか」という点を確認することが必要だ。該当する場合は、右のリストのような対応が必要となる。

まとめ

攻撃者に狙われやすいポイントの多くは、設定が管理されていない環境や古い環境、古い業務ルーチンに存在する。対策にあたっては、クライアントを含めたシステム全体で設定管理を見直し、古い環境・業務ルーチンを刷新していくための取り組みが求められる。

「事業継続性が最重要であるため、既存の仕組みを変更することは難しい」とはよく聞く声であるが、ひとたびセキュリティインシデントが発生した場合には、事業の継続に致命的な影響が及ぶかもしれない。こうしたリスクを回避するためには、仕方なしと現状に甘んじるのではなく、変更に向けた取り組みを、できることから、着実に進めていくことが肝要だ。

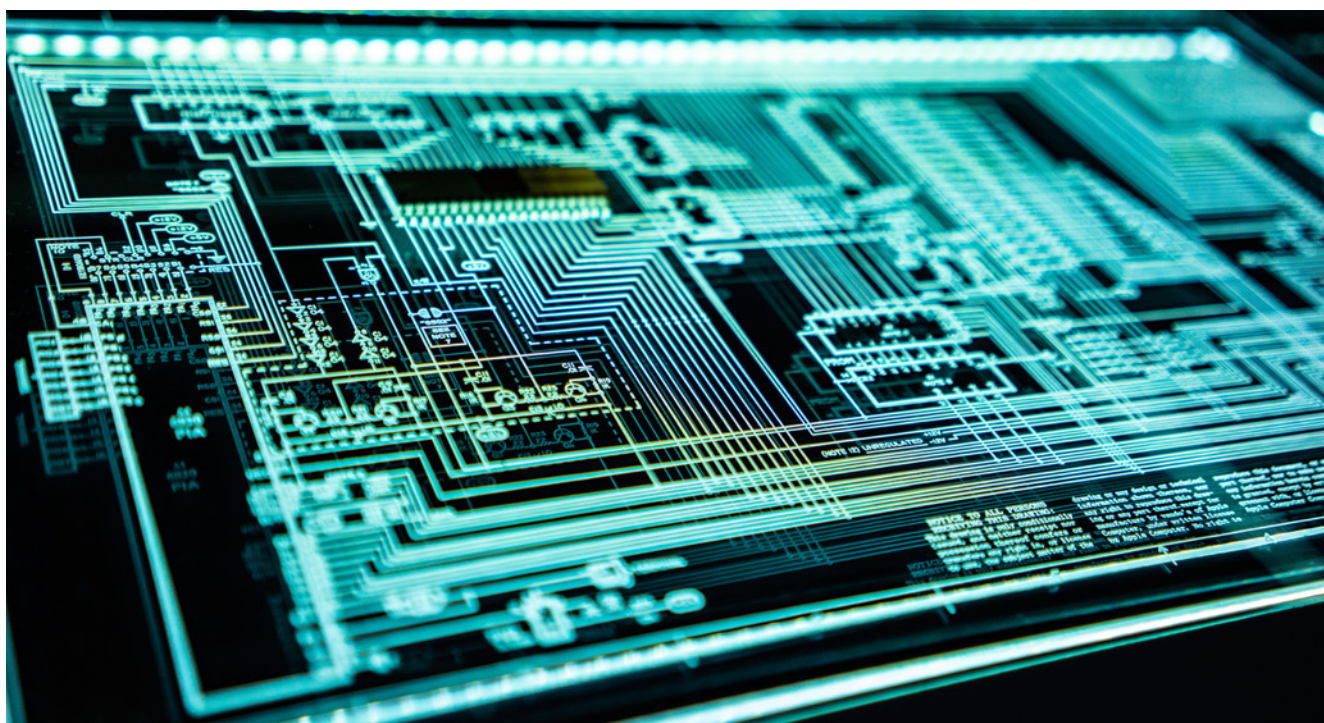
- IPS/IDS による SSH 経由での RDP 実行の検出
- RDP へのローカルユーザのログインの禁止
- SSH 側でのログイン監視

*1 https://www.nict.go.jp/cyber/report/NICTER_report_2018.pdf

*2 <http://www.taipetimes.com/News/biz/archives/2018/11/16/2003704292>

*3 <https://www.us-cert.gov/ncas/alerts/AA18-337A>

*4 <https://www.fireeye.com/blog/threat-research/2019/01/bypassing-network-restrictions-through-rdp-tunneling.html>



WordPress の普及とセキュリティ

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

CMS のデファクトスタンダード

今日、企業の事業活動には、迅速かつタイムリーにコンテンツを配信して効果的に製品・サービスを訴求できる Web サイトが欠かせない。そうした Web サイトの開発工数を大幅に削減できるテクノロジーとして注目を集めているのが CMS (Content Management System) だ。低コスト化・高効率化を求める多くの事業者を導入されている。

WordPress はその中でも群を抜く存在だ。現在、CMS の使用率は全 Web サイトの 55% ほどだが、WordPress のみで 33% を占める。CMS のみに限定して内訳を見ると、Joomla や Drupal といった 2 位以降の CRM 製品を大きく引き離すシェアを持っている (下左グラフ)。日本語サイトのみに限るとシェアはさらに増え、8 割を超える (下右グラフ)。CMS のデファ

クトスタンダードとして揺るぎない地位を確立しているといえるだろう。

WordPress の魅力は、何よりも無料であること、そして、柔軟性と拡張性に優れていることだ。操作性が高く直感的な編集が可能なのに加え、さまざまなデザインのテーマプレートや多彩なプラグインが提供されており、SEO 対策、ショッピングカート仕様の導入、動画埋め込みなど、Web サイトに求められるありとあらゆる機能を実践できる。そのため、Web サイト構築の専門知識を持たないビジネスユーザや個人ユーザにも人気で、幅広い支持を獲得している状況だ。

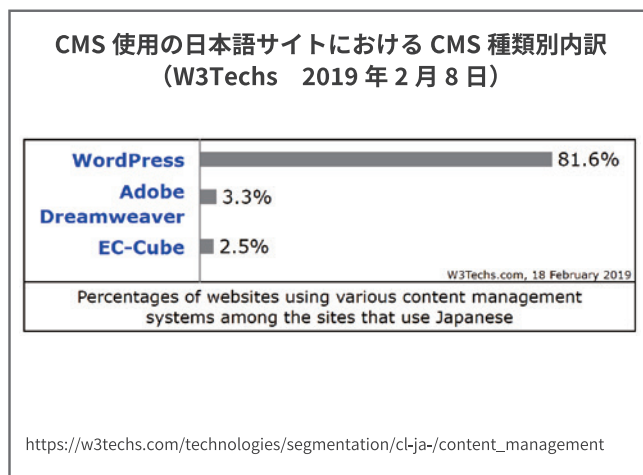
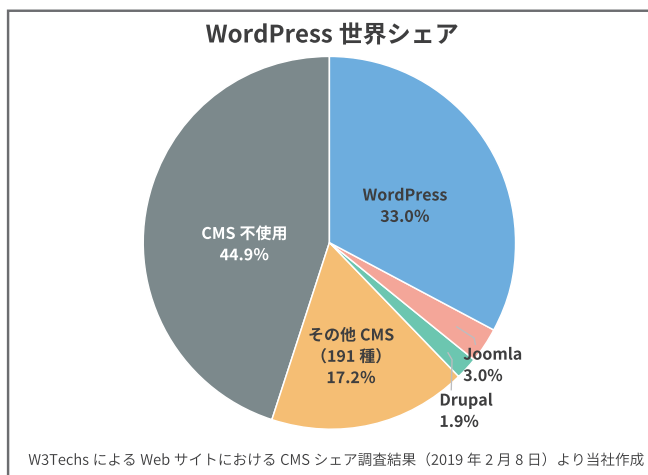
人気の裏で脆弱性も増加

圧倒的なシェアを誇る WordPress だが、実は、この CMS は、脆弱性という点においても近年著しい伸

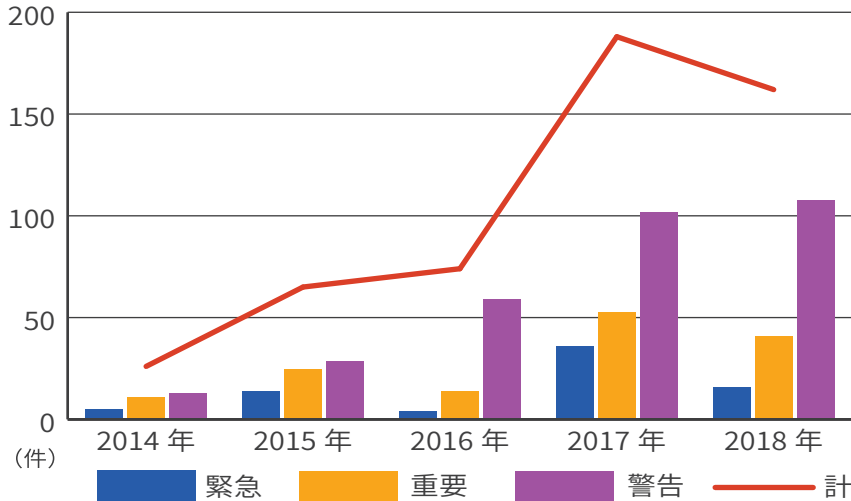
びを見せている。JPCERT/CC と情報処理推進機構 (IPA) が共同で管理している脆弱性対策情報データベース「JVN iPedia」の集計を見ても、その傾向は明らかだ (次ページグラフ)。

同様に、「JPCERT/CC インシデント報告対応レポート (2018 年 10 月 1 日 ~ 12 月 31 日)」でも、Web サイトの改竄が増加傾向にある中、WordPress を使用した攻撃事例が複数確認された旨が言及されている。加えて、ここ数ヶ月のニュースを見ても、WordPress の GDPR 対応プラグインに含まれる脆弱性を利用した Web サイト乗っ取り、大手ホスティングサービスに対する WordPress の ID を踏み台にした不正アクセスなど、大きな被害が立て続けに報じられている。

これだけシェアが大きいと、その人気の裏返しとして、必然的に幅



JVN iPedia に登録された WordPress の脆弱性



JVN iPedia データより当社作成

広い層を狙ったサイバー攻撃のターゲットになりやすい。しかしながら、何よりも大きな要因として考えられるのは、このソフトウェアがオープンソースであるという点だ。仕様が公開され、誰でも中身を解析・使用できるということは、利便性が高い反面、セキュリティ上の弱点になり得る。良く言えば不備の検証、悪く言えば脆弱性のあら探し、容易に行えてしまうからだ。オープンであるということは、攻撃者にとっても利用しやすいということの意味する。

さらにいえば、膨大な数が提供されている WordPress のプラグインにも注意が必要だ。プラグインの作成者はセキュリティ上の義務を負わない。提供形態がコミュニティベースでオープンなやりとりが可能である反面、オフィシャルな評価基準が確立されていない。そのため、プラグインを利用するユーザの側で、セキュリティの観点から品質を慎重に見極める必要がある。

インジェクション系の脆弱性
SQL インジェクション クロスサイトスクリプティング OS コマンドインジェクション 等
アクセス制御や運用上の不備
WordPress の設定情報奪取 WordPress の管理者権限奪取

では、WordPress では具体的にどのような脅威が報告されているのだろうか。主なものは左下のリストのとおりで、大別すると「インジェクション系の脆弱性」、「アクセス制御や運用上の不備」となる。いずれも深刻なリスクをもたらす可能性があるもので、Web サイトの改竄、重要情報の漏洩、DoS 攻撃、WordPress 自体の乗っ取り等の被害につながる懸念される。

なお、当社の Web アプリケーション診断結果においても、検出件数自体は多くはないが、傾向的には WordPress 関連の脆弱性は増加している（下表参照）。

対策の鍵は「DevSecOps」

Web サイトの構築・運用ではスピードと頻繁な更新を求められるケースが多く、一般には、開発担当（Development）と運用担当（Operation）が連携してシステム

当社診断結果における「脆弱性が存在するバージョンの WordPress」検出推移

年	比率
2016年	1.6%
2017年	2.3%
2018年	2.4%

※比率＝検出件数／診断システム数 × 100

開発を進める「DevOps」の手法がとられることが多い。しかし、WordPress のようなオープンソースの CMS を使用している場合、それだけでは不十分だ。そこで強く推奨したいのは、DevOps の取り組みにセキュリティ（Security）を連携させる「DevSecOps」である。

DevSecOps を実現するには、従来の開発体制を、「工数確保」、「体制構築」、「環境整備」といった観点から改めて見直し、セキュリティ対策に関する実施項目を組み込むようにする必要がある。中でも決定的に重要なのは「アップデート」と「アクセス制御」に関する対策と実施項目である。以下、具体的にしていこう。

頻繁なアップデートに対し万全の体制を組む

WordPress に限ったことではないが、まず基本となる対策は、「常に最新バージョンを適用する」ことだ。具体的な実施項目は以下のとおり。

- アップデート情報を定期的に確認する
- データベースを定期的にバックアップする
- 開発・ステージング環境にアップデートを適用し動作チェックを実行する
- 本番環境にアップデートを適用する

WordPress の場合、アップデートはかなりの頻度で行われているため、利用側も相応の工数を確保することが必要だ。頻繁なアップデートに持続的に対応できる体制を整えていくことが求められる。

もう 1 つ 注 意 し た い の は、WordPress のコア（本体）だけでなく、プラグインについても同様

の対応が必要になるという点だ。新たにプラグインを導入する場合は、Web サイトのコンテンツに対して過不足のない機能であるかどうかを評価する、事前にセキュリティの観点からソースコードレビューを実施する等、慎重な対応が求められる。特に、リリースから 1 年以上経過したプラグインでは、十分な検討を行いたい。

アクセス制御を強化する

アクセス制御も重要だ。ここでは、以下のような実施項目が想定される。

- 管理ユーザを特定／不必要なユーザを削除／ログイン ID を秘匿
- アクセスログを定期的にチェック
- Basic 認証を設定（アクセスは https に限定する）
- アクセス元 IP アドレスを制限
(対象：wp-login.php、admin-ajax.php 以外の wp-admin ディレクトリ)

(なお、アクセス制限については、管理画面以外に、xmlrpc.php や wp-config.php の設定も推奨される。)

脆弱性診断、改竄検知を定期的に実施する

そのほか、WordPress（コア、プラグインの双方）の重要情報を推測する手がかりになる情報や重要情報そのものが外部から見える状態になっていないか、脆弱性が指摘されている機能が不要なまま放置されていないか、Web サイト自体に脆弱性が内在していないか、等を定期的に確認することも必要になる。こうした実施項目については、システム脆弱性診断の実施が有効だ。診断の結果にもとづき、どのようなリスクの脆弱性が潜んでいるのを把握できれば、対策の優先度を判断したり、対策実装のために必要な期間や予算を適切に見積もることが可能になる。

さらに、コンテンツ改竄検知サービスの利用も検討に値する。とい

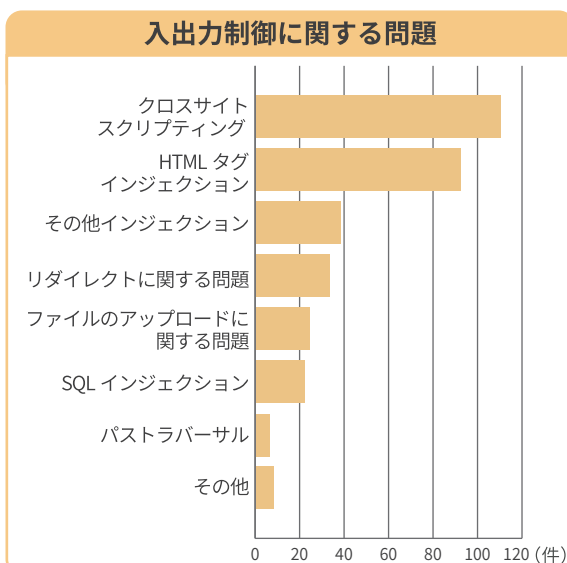
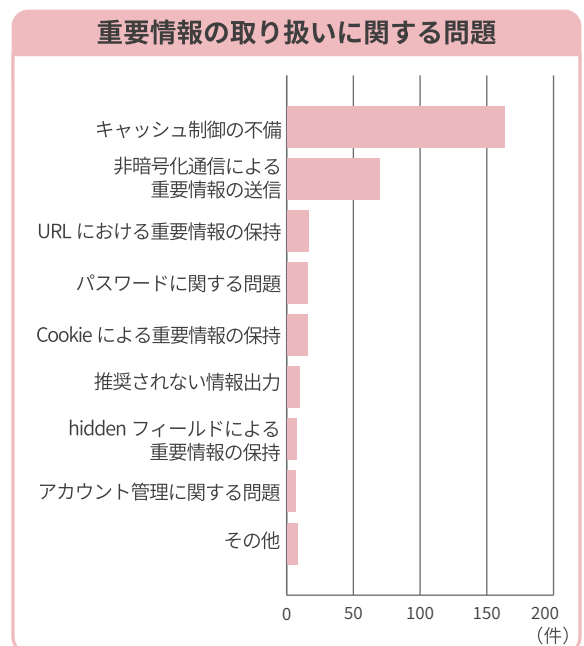
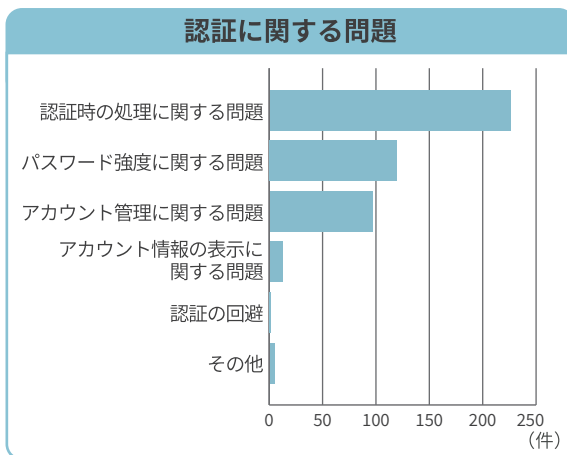
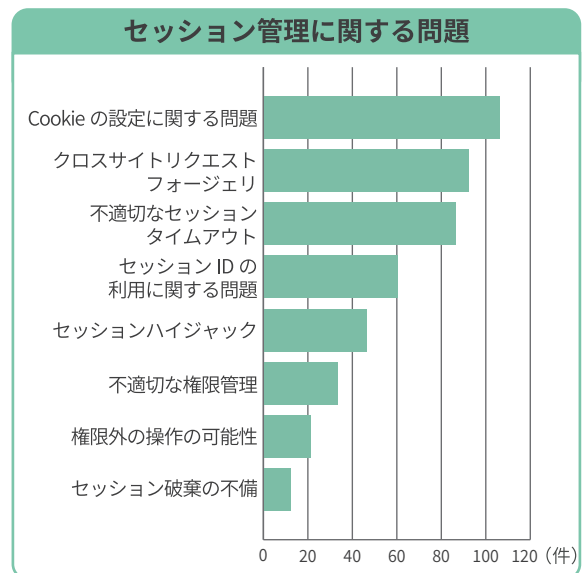
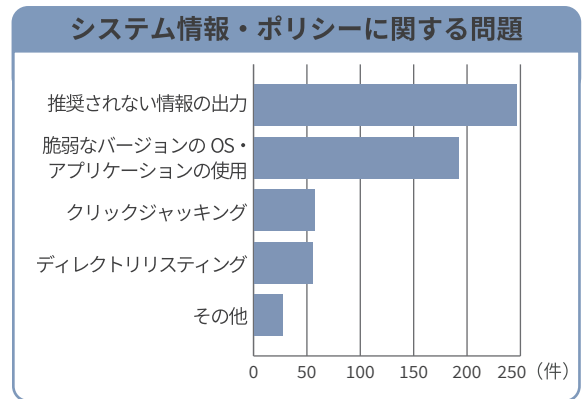
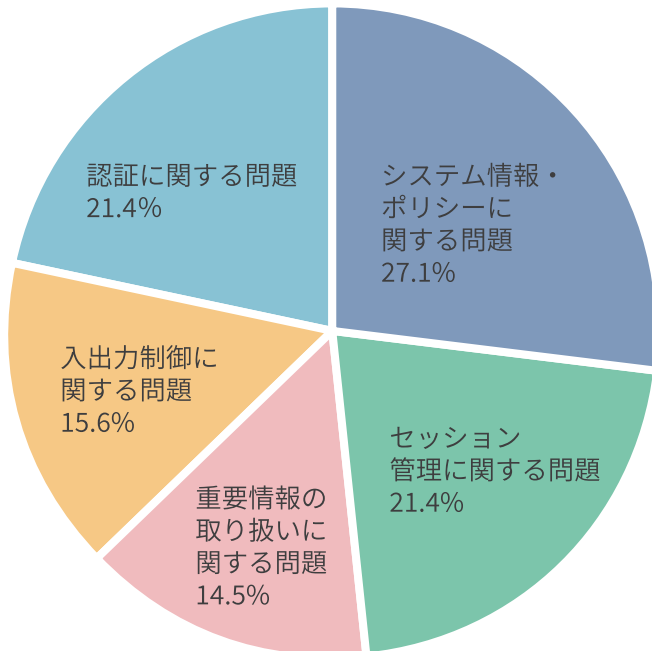
うのも、システム脆弱性診断は、脆弱性のある旧バージョンやセキュリティ上問題のある設定などを検出するための手法であり、「すでにアカウントが乗っ取られ自社の Web サイトが密かに改竄されている」といった事態には十分に対応できない可能性があるからだ。定期的にコンテンツ改竄の有無をチェックすることは、こうした改竄のリスクを早期に発見する上で有効な対策となる。

今後も、その導入のしやすさ、使い勝手の良さ等を理由に WordPress を導入する企業は増えていくだろう。一方で、同じ理由から、攻撃者にとっての人気も当面は衰えず、WordPress を狙った攻撃の勢いは続くものと思われる。企業の Web サービス開発を支援する CMS。そのメリットを享受し続けるには、次々に発見される脆弱性に対し、隙なく、持続的に対応できる体制の構築が必須だ。

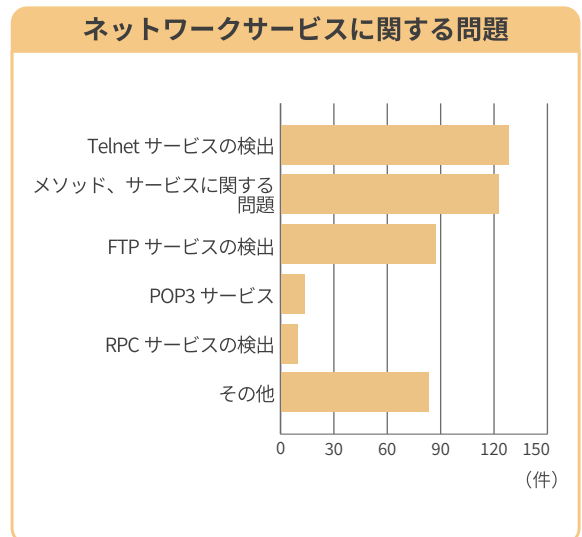
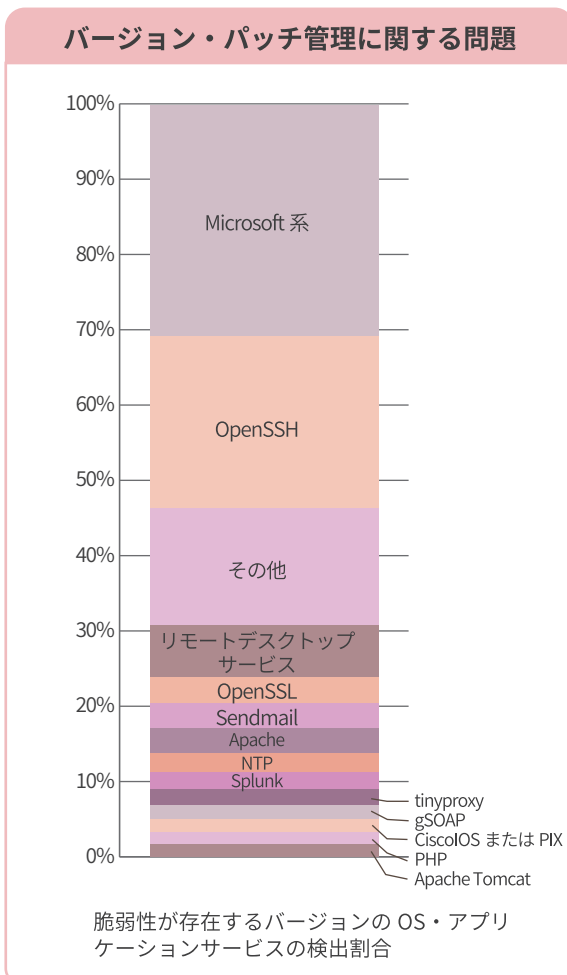
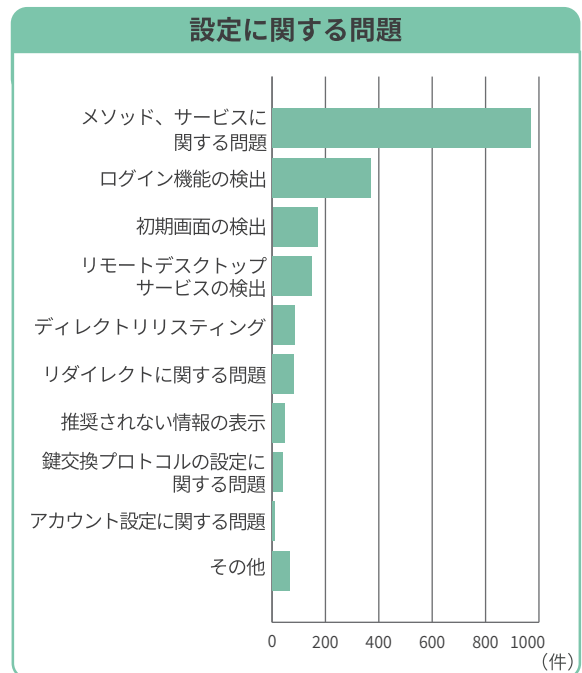
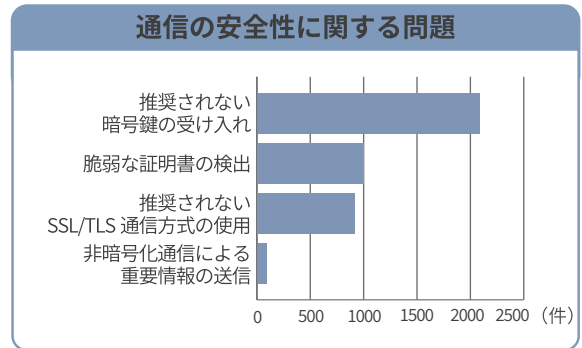
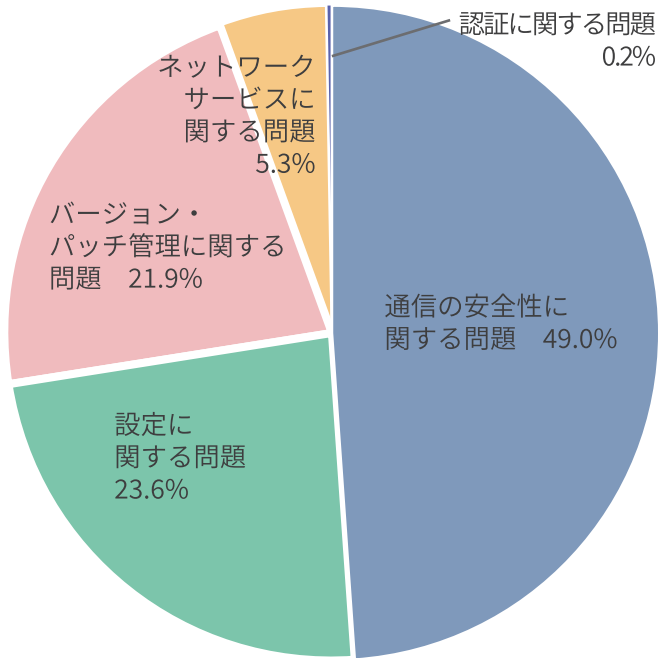


2018 年下半期 カテゴリ別脆弱性検出状況

Web アプリケーション診断結果



ネットワーク診断結果



業界別診断結果レーダーチャート

2018 年下半期 Web アプリケーション診断

診断対象を業界別に分類し、当社報告書内で使用している、入出力制御、認証、セッション管理、重要情報の取り扱い、システム情報・ポリシーといったカテゴリごとに、検出された脆弱性をリスクの重大性で評価してレーダーチャート化した。なお今号からレーダーチャートの算出方法を改め、集計期間に検出された脆弱性の平均値から、システムごとに判定した結果の平均値に切り替えた。これは、当社の診断結果と、システムが所属する業界のレーダーチャートとの比較をしやすくするためである。

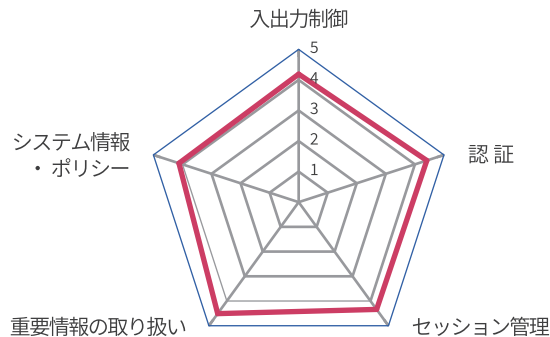
今回は「卸売業、小売業」「不動産業、物品賃貸業」の2業種をピックアップし、それぞれの傾向を分析した。

「高」リスク以上の脆弱性が検出されたシステムであっても、正しい対処を施せば影響は最小化できる。また、事故を未然に防ぐための方法を、官公庁などがガイドラインや対策提言などとして発表しているので、これらも参考にしていきたい。

Web アプリケーション診断実績（業界別割合）

業界	割合
情報通信業	42.4%
生活関連サービス業、娯楽業	22.3%
金融業、保険業	15.6%
製造業	8.6%
サービス業（他に分類されないもの）	2.1%
電気・ガス・熱供給・水道業	2.1%
卸売業、小売業	1.8%
医療、福祉	1.5%
建設業	1.2%
学術研究、専門・技術サービス業	0.9%
不動産業、物品賃貸業	0.6%
運輸業、郵便業	0.3%
教育、学習支援業	0.3%
宿泊業、飲食サービス業	0.3%

レーダーチャートの見方



5つのカテゴリ別に、リスクの重大性によって、「緊急：1」「重大：2」「高：3」「中・低：4」とレベル分けし、それ以外を「情報：5」として、各段階に応じた数値を定め平均点化したものを赤線で示す。数値が高いほど安全度が高く、数値が低いほど緊急の対応が必要となる。

●業界分類方法●

「日本標準産業分類」（総務省）の「大分類」をもとに当社にて選定

不動産業、物品賃貸業

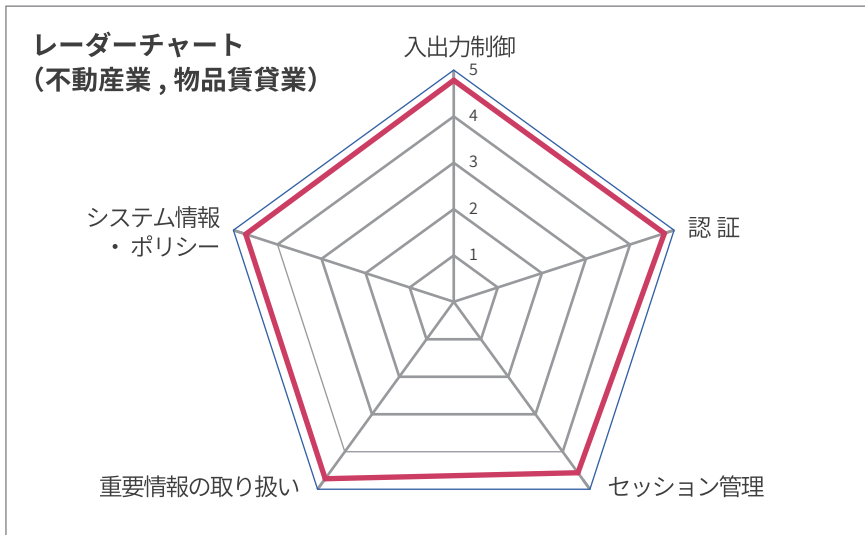
当社で診断を実施した不動産業の Web システムの状況は、次ページのレーダーチャートに示すとおりである。診断したシステムにおいて、ほぼ脆弱性が検出されなかったか、あるいは軽微な項目であることが見て取れる。取り扱い商材が高価格であること、取得するデータが家族構成、年収などの財産情報を含むセンシティブな個人情報であることから、不動産業界における個人情報については、監督官庁（国土交通省）

がガイドラインや「個人情報保護法の適用の考え方」で指導を強化しているだけでなく、各事業者が所属する団体においても個別のガイドラインが策定されている。不動産業界、特に大手企業においては一定のセキュリティ対策はなされていると推測される。

しかしながら、過去2年間で不動産業界で発生したセキュリティインシデントにおいては、不正アクセスや

公開されていないファイルの閲覧なども発生しているため、注意が必要だ。（次ページ表参照）

インターネットでの取引という観点からすると、不動産業は、他の業界とは異なる性質を有する。インターネットの利用率が高く、情報検索においては9割以上の消費者がインターネットを利用している。また、消費者の利用端末がPCからスマートフォンへ移行していること、さら



に他業界に比べ SNS の利用率の高いことが特徴である。一般社団法人不動産流通経営協会の「不動産流通業に関する消費者動向調査<第 23 回 (2018 年度)>」によれば、インターネットによる不動産情報の収集経験は 92.1%。利用したインターネット端末は、「スマートフォン」が 80.4%、「パソコン」が 79.9%と

なっており、不動産情報に Web サイトは欠かせない情報源であることが見て取れる。取り扱う商材が大きいこと、商材の移動ができず、利用者自身が足を運ばなければならないことが逆にネット検索の利用を促進していると考えられる。一方、インターネットによる商取引は法律 (宅地建物取引業法) の規制のため、こ

不動産業界ガイドライン

国土交通省

- ・不動産における個人情報保護法に関するガイドライン
- ・不動産流通業における個人情報保護法の適用の考え方
- ・賃貸取引に係る IT を活用した重要事項説明実施マニュアル (平成 29 年 9 月)
- ・宅地建物取引業法の解釈・運用の考え方 (平成 13 年国総動第 3 号)

一般社団法人 不動産流通経営協会

- ・個人情報の保護に関する法律についての不動産流通業に関するガイドライン

公益社団法人日本不動産鑑定士協会連合会

- ・不動産の鑑定評価等業務に係る個人情報保護に関する業務指針

一般社団法人 不動産協会

- ・不動産分譲事業における個人情報保護に関する留意事項 (ガイドライン)

公益社団法人 全日本不動産協会

- ・不動産業の個人情報保護法に関するガイドライン改訂版

住宅生産団体連合会

- ・個人情報保護法対策ガイドライン

不動産情報を調べる際に利用したもの (複数回答)

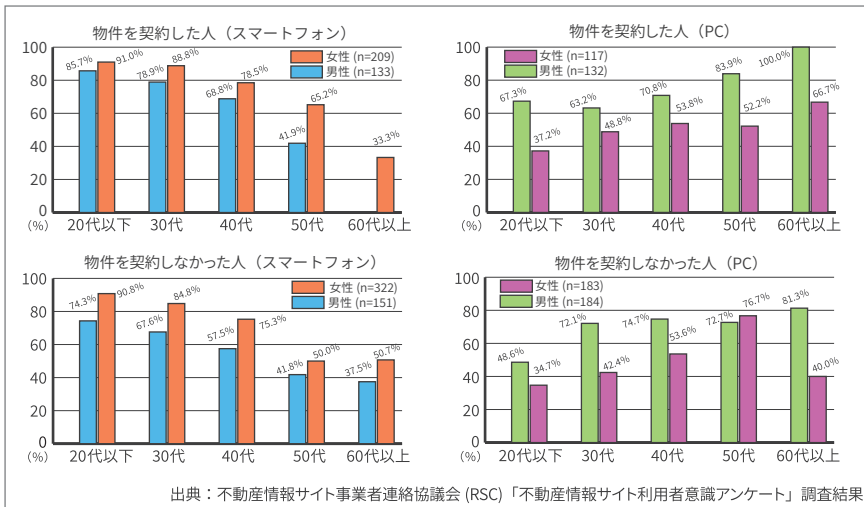


表 過去 2 年間の不動産業界のセキュリティインシデント

発生年月	概要
2017/6	国交省関連サイトへの不正アクセス、個人情報流出はなし
2017/7	SNS サイトでメール誤送信、会員メールアドレス 446 件流出
2017/8	取引仲介事業者の登録システムにおいて、非公開の登録情報が閲覧可能
2017/12	新規物件情報メールを誤送信、顧客 12 名のメールアドレス漏洩
2018/2	顧客情報など約 2.6 万件を従業員が持ち出し、ネット上に保存
2018/2	日本不動産鑑定士協会連合会のサーバに不正アクセス、ランサムウェアは回避
2018/9	顧客情報数十人分を保存した PC を含む鞆の盗難
2019/1	SNS サイトで当選者 30 人分の会員情報が閲覧可能

れまで普及が進まなかった。「重要事項の説明は対面で行うこと」という対面原則が、不動産業界の電子商取引の足枷となっていた。しかし IT 化推進のため、宅地建物取引法 35 条の解釈が改められ、法人取引に関しては、登録事業者に対して平成 29 年 10 月より本格運用が開始された。対消費者取引においても、一定の条件を満たす場合、IT を利用した賃貸取引が認められることとなった。

ただし、消費者側の環境についてもガイドラインに沿ったものであること、取引内容の録音を 6 ヶ月保存することが義務付けられているなど、普及にはまだ時間がかかりそうだ。しかしながら、同時に Skype や LINE といったインスタントメッセージャーでの取引についても検討されており、今後の展開が見込まれる。

卸売業，小売業

レーダーチャートからは、卸売業・小売業は多くのカテゴリで推奨値をかなり下回っていることが読み取れる。また、下段のグラフは脆弱性検出割合の半期ごとの推移を示すものであり、棒グラフはシステムに脆弱性が存在していたかどうかの割合を、折れ線グラフはシステムに存在する最も脅威度の高い脆弱性を基準にシステムの安全性を、「緊急」レベルを最底として目視化した結果の平均値を表している。棒グラフを見ると卸売業・小売業は、システムに脆弱性が潜んでいた割合が 2 期連続で 100%となっている。そして、折れ線グラフからは徐々に業界平均のリスクレベル傾向が「高」から「重大」へと悪化しつつあることも伺える。

データを見る限り、卸売業・小売業は重要情報の取り扱いに関しては傑

出して評価が高く、それ以外の部分では全業種中でも有数の低さである。以上から、セキュリティの観点から見ると、卸売業・小売業の対策はバランスを欠いたものといえるだろう。

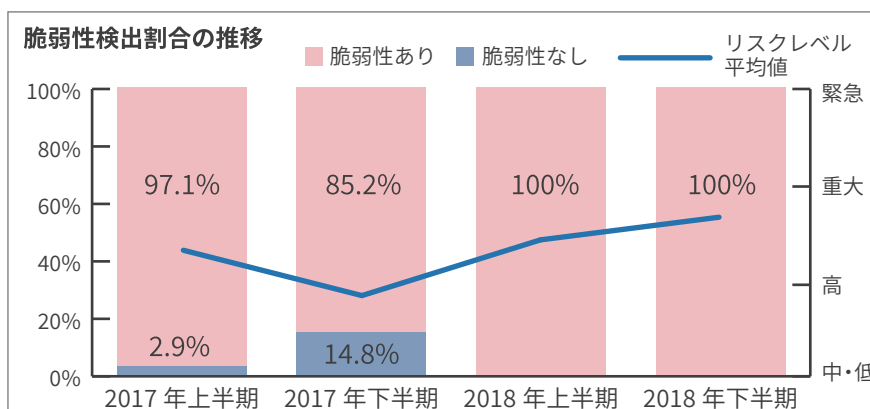
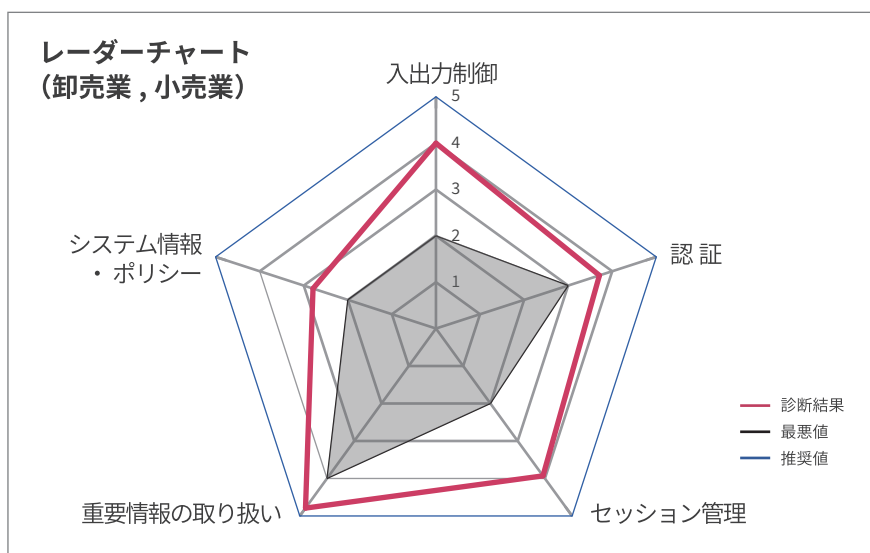
レーダーチャートの内側にあるチャートは、検出されたものの中で最もリスクレベルが高いケースのデータだ。見てのとおり、入出力制御やシステム情報・ポリシー、セッション管理に関して「重大」レベルの脆弱性が検出されており、ついで認証に関する問題では「高」レベルが検出されている。

「重大」レベルの脆弱性に目を向けると、全業界の中で最低の結果となったシステム情報・ポリシーに関する問題では、サポートが終了した

Apache 2.2 系の他、既知の脆弱性が存在するミドルウェアの検出が目立つ。これらの脆弱性が悪用されると、任意のコード実行やセキュリティ制限の回避、重要情報の漏洩、改竄、サービス運用妨害 (DoS) など、さまざまな被害を受ける可能性がある。報告されている脆弱性の中には、それらを悪用するエクスプロイト (攻撃プログラム) が公開されているものもあり、さらに危険性を高めている。入出力制御に関しては、クロスサイトスクリプティングをはじめとする早急に対応が必要な脆弱性が多く検出されており、対策を怠ると任意のプログラム実行や悪質なページへの誘導、コンテンツの改竄等につながる可能性がある。セッション管理に関しては、権限管理の問題が検出され、不正操作や情報漏洩につながる恐れがある。また、「高」レベルでは、セッションハイジャックやパスワードに関する脆弱性など、悪用された場合に、なりすましや情報漏洩に直接つながりうる問題が検出された。

一方、重要情報の取り扱いに関する項目は、おおむね「高」リスクレベル以上の脆弱性に対して対応がなされており、当社で診断した業界の中でもトップクラスを誇っている。これは、クレジットカード情報や個人情報情報といった重要情報を取り扱う業界であることや、クレジットカード情報非保持化の導入といった要因が影響しているであろう。

業界動向としては、昨年 6 月に施行された改正割賦販売法において、クレジットカード番号等の適切な管理や加盟店管理を強化する方針が打ち出された。加盟店との間でクレジットカード番号等の取り扱いを認める契約を締結する事業者 (クレジットカード番号等取扱契約締結事業者) に、登録を義務付ける制度が始まり、本年 2019 年にはこうした



事業者による加盟店への調査等が開始される。

加盟店は 2018 年 6 月 1 日までに「PCI DSS の準拠」か「非保持化」、つまり決済代行業者に決済業務を完全遷移することで、自社で保有す

る機器・ネットワークにおいて「カード情報」を『保存』、『処理』、『通過』させないことの、いずれかが求められた。この非保持化を実施して安心した事業者もいるであろうが、そのことがセキュリティ対策をおろそかにしていい理由にはならない。今回

の結果からも推察できるとおり、セキュリティ対策に偏りがあると、弱点を突かれ、重大なインシデントにつながる恐れがある。事実、決済代行業者の決済画面への遷移直前でフィッシングサイトへと遷移するようにサイトを改竄され、情報漏洩に

つながるインシデントが立て続けに起きている。セキュリティに絶対はない。卸売業・小売業は重要な個人情報を取り扱う業界である。以下にあげたガイドラインなどを参考に、攻撃に対して堅牢なシステムを構築・維持するよう努めていただきたい。

図 1 クレジットカード不正利用被害額の内訳

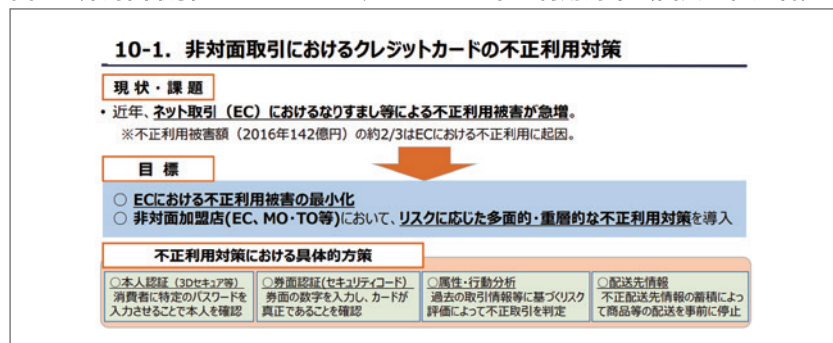
(出典：一般社団法人日本クレジット協会「クレジットカード不正利用被害の集計結果について」)

期 間	クレジットカード不正 使用被害額	クレジットカード不正使用被害額の内訳						
		偽造カード被害額		番号盗用被害額		その他不正使用被害額		
		被害額	構成比	被害額	構成比	被害額	構成比	
平成 26 年 (1月~12月)	114.5	19.5	17.0%	67.3	58.8%	27.7	24.2%	
平成 27 年 (1月~12月)	120.9	23.1	19.1%	72.2	59.7%	25.6	21.2%	
平成 28 年 (1月~12月)	142.0	30.6	21.6%	88.9	62.6%	22.5	15.8%	
平成 28 年	(1月~3月)	37.3	9.1	24.4%	22.8	61.1%	5.4	14.5%
	(4月~6月)	35.9	7.3	20.3%	23.1	64.4%	5.5	15.3%
	(7月~9月)	34.3	6.4	18.7%	21.9	63.8%	6.0	17.5%
	(10月~12月)	34.5	7.8	22.6%	21.1	61.2%	5.6	16.2%
平成 29 年 (1月~12月)	236.4	31.7	13.4%	176.7	74.8%	28.0	11.8%	
平成 29 年	(1月~3月)	57.2	10.6	18.5%	40.3	70.5%	6.3	11.0%
	(4月~6月)	62.4	9.6	15.4%	46.1	73.9%	6.7	10.7%
	(7月~9月)	57.2	5.6	9.8%	43.9	76.7%	7.7	13.5%
	(10月~12月)	59.6	5.9	9.9%	46.4	77.9%	7.3	12.2%

表 1 改竄による偽の決済画面へ誘導する手口を用いたインシデントリスト (例)

発生年月	業態	概要
2018/5	衣料品 販売会社	偽のカード入力画面へ遷移するように改竄され、カード情報が窃取された。偽のカード入力画面での情報入力後に、正規の入力画面へと遷移するように仕掛けられており、発覚までに時間を要した。流出したデータは 2,145 人分にも及んだ。
2018/7	書籍 販売会社	偽のカード入力画面へ遷移するように改竄され、カード情報が窃取された。偽のカード入力画面での情報入力後にエラー発生画面が表示され、その後に再び正規の入力画面へと遷移するように仕掛けられていた。流出したデータは 2,481 人分に及んだ。
2018/9	洋菓子製造 販売会社	偽のカード入力画面へ遷移するように改竄され、カード情報入力後にエラー発生画面を表示、その後に正規の入力画面へと遷移するように仕掛けられていた。偽サイトはドメイン名まで正規サイトに似せていた。流出したデータは 668 人分であった。
2018/10	デジタル コンテンツ ダウンロード 販売会社	偽のカード入力画面へ遷移するように改竄され、カード情報入力後にエラー発生画面を表示、その後に正規の入力画面へと遷移するように仕掛けられていた。カード情報が流出した可能性があるとして判断された件数は最大 7,741 件。決済は成立していないものの、偽のカード入力画面に誘導された可能性があるのは最大 903 件。

図 2 非対面取引におけるクレジットカードの不正利用対策 (出典：経産省)

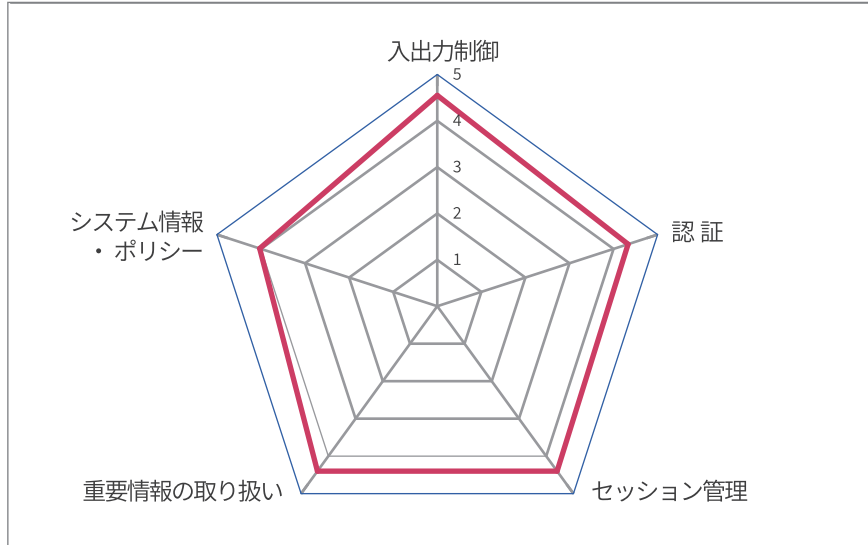


卸売業、小売業におけるセキュリティガイドライン (例)

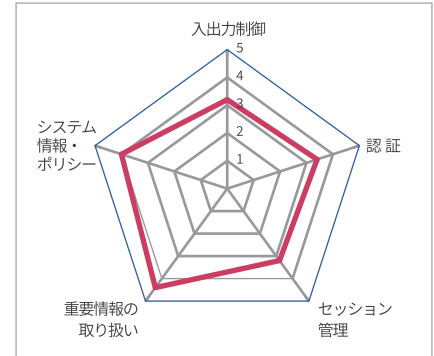
- 経済産業省**
 - 改正割賦販売法
 - クレジットカード加盟店契約に関するガイドライン
 - クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画 -2018-
- Payment Card Industry Security Standards Council**
 - Payment Card Industry Data Security Standard (PCI DSS) ver. 3.2.1
- 一般社団法人日本クレジット協会**
 - 対面加盟店における非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術要件について
 - 非保持化実現加盟店における過去のカード情報保護対策について
 - スマートフォン決済セキュリティガイドライン
- 日本クレジットカード協会 (JCCA)**
 - スマートフォン決済の安全基準等に関する基本的な考え方
 - インターネット上での取引時における本人なりすましによる不正使用防止のためのガイドライン
- 一般社団法人重要生活機器連携セキュリティ協議会 (CCDS)**
 - 製品分野別セキュリティガイドライン オープン POS 編 Ver. 2.0

その他の業種

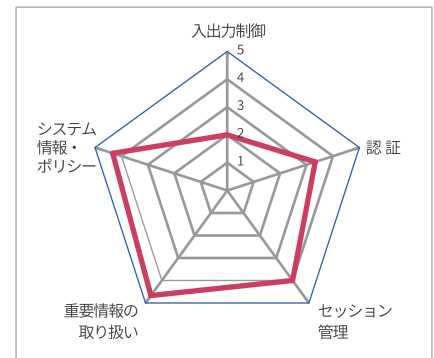
金融業，保険業



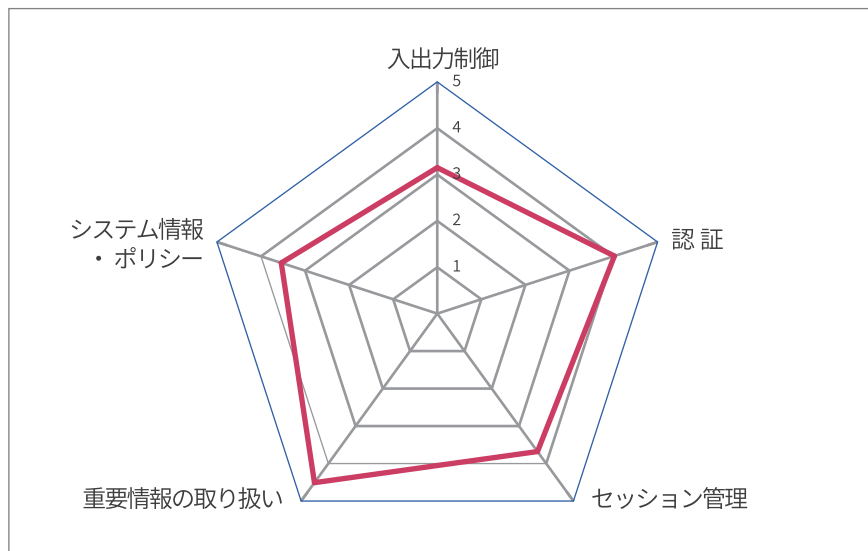
医療，福祉



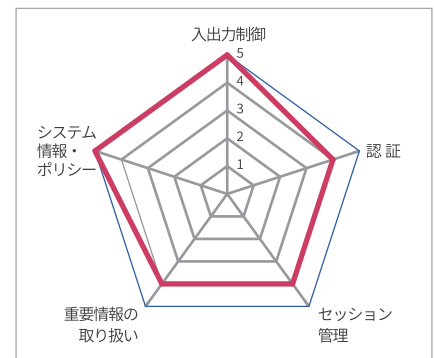
学術研究，専門・技術サービス業



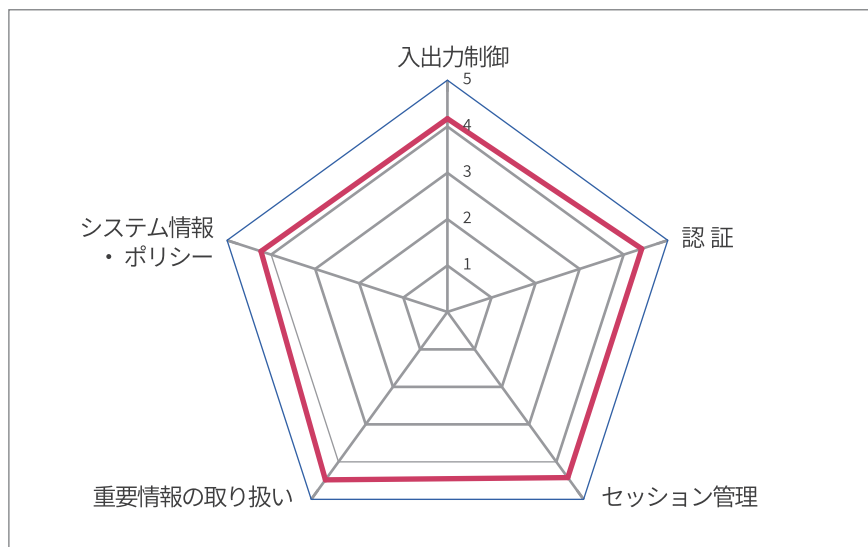
製造業



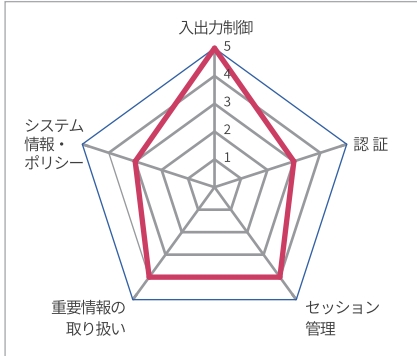
教育，学習支援業



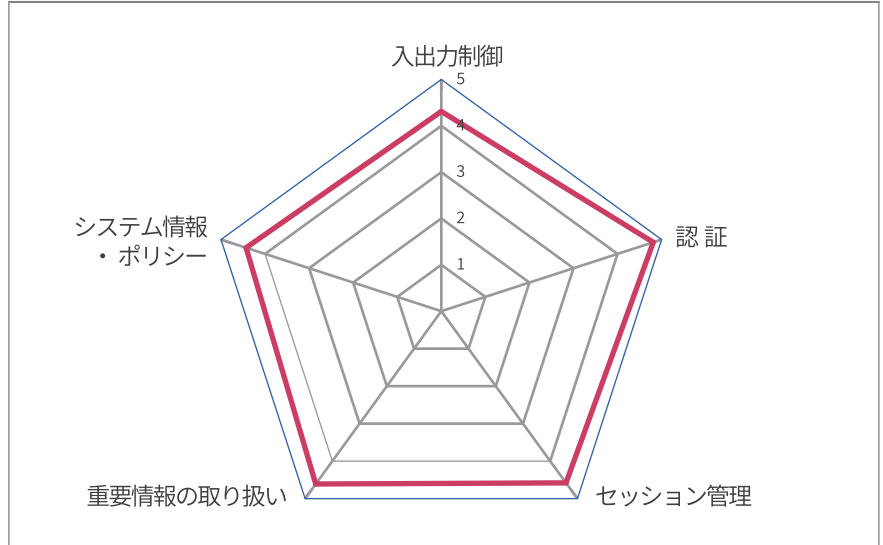
情報通信業



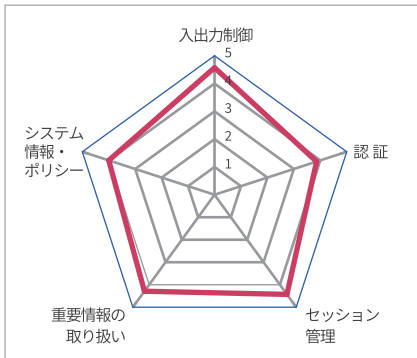
運輸業，郵便業



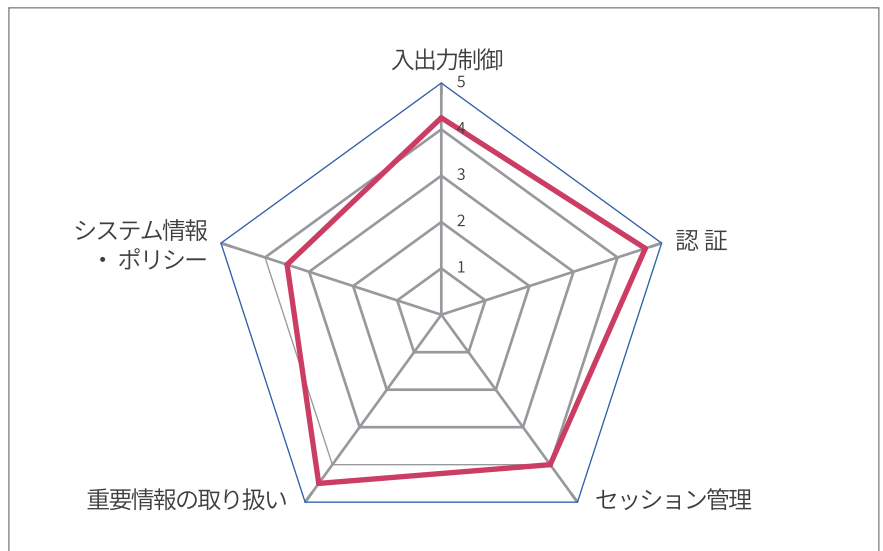
生活関連サービス業，娯楽業



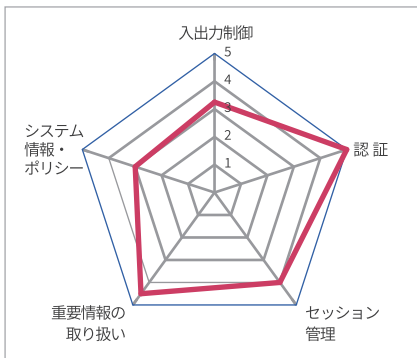
建設業



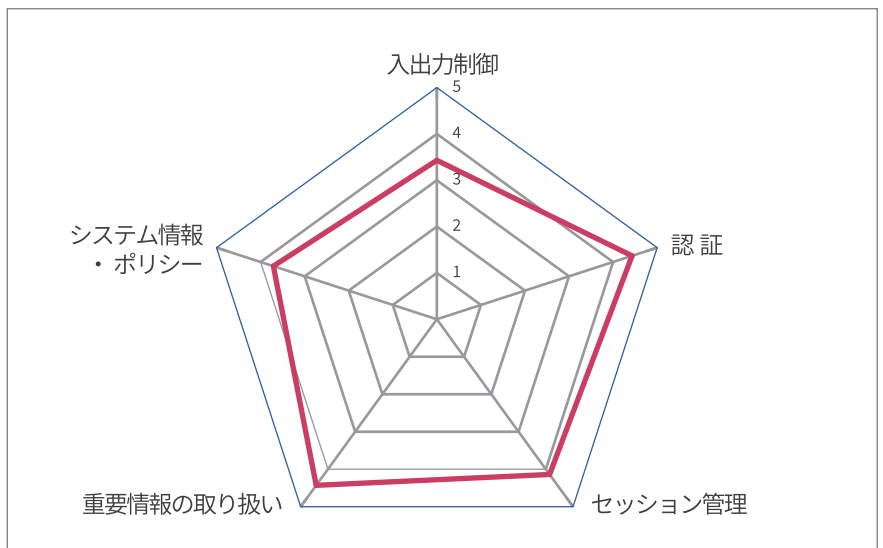
サービス業（他に分類されないもの）



宿泊業，飲食サービス業



電気・ガス・熱供給・水道業



※ レーダーチャートの中心点は、その項目において脆弱性の検出がないことを示します。
 なお、レーダーチャートの大小は年間診断の案件数によります。

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、さまざま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 (「AntiAbuse 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。

<事業拠点>

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

天王洲オフィス

〒140-0002
東京都品川区東品川 2-5-8
天王洲パークサイドビル 3F
TEL : 03-6433-3116

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

韓国支店

15F, Samsung Life Seocho Tower
4 Seocho-daero 74-gil, Seocho-gu
Seoul 06620, Korea
TEL : +82-2-6011-4640

名古屋支店

〒460-0003
愛知県名古屋市中区錦 1-6-18
J・伊藤ビル 6F
TEL : 052-265-7591