



SQAT[®] Security Report

2016年下半期(7月~12月)



BBSec

株式会社ブロードバンドセキュリティ

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

いまや、Webサイトを利用しない企業はないと言ってもいいほどWebサイトの構築数は増えて
います。しかし、その一方で、Webサイト強化のための機能であるJavaScriptやCMS等の脆弱性を
突いた攻撃も増加しています。攻撃を受けた場合、ターゲットとなった脆弱性の修正には相応の期
間が必要となり、独立行政法人 情報処理推進機構（IPA）の調査によると、91日以上を要したとい
うケースが全体の1/3にも上っています。

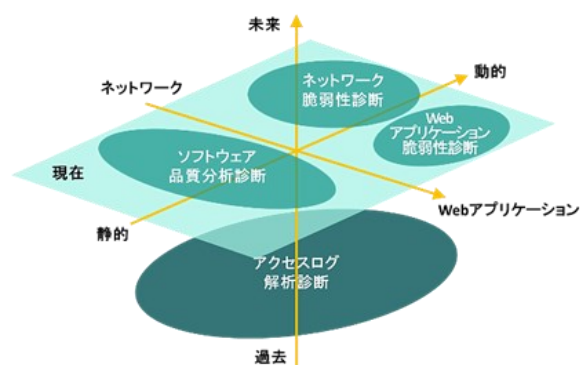
こうした情勢を踏まえ、経済産業省は、2016年12月8日に『サイバーセキュリティガイドライン
Ver1.1』を発行し、「サイバー攻撃が避けられないリスクとなっている現状において、経営戦略と
してのセキュリティ投資は必要不可欠かつ経営者としての責務である」と新たに決めました。企業
として、常に最新の情報セキュリティ状況を把握し、自組織の対策に反映することが必須になった
と言えるでしょう。

本誌は、株式会社ブロードバンドセキュリティ（以下「当社」）の「SQAT®」*において2016
年7月～12月の半年間に実施されたセキュリティ診断の結果をもとに、組織における情報セキュリ
ティ対策の実情や脅威動向を分析したレポートです。サイバーセキュリティ対策は「予見」「防
御」「対処」「発見」「啓蒙・育成」の5象限から構成されると言われています。それぞれの組織
の状況に応じて優先度を決め、対策をとるのが望ましく、その水先案内となるべく執筆いたしまし
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当社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、当社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2,900組織、1万を超えるシステムで利用されていま
す。



目次

はじめに	2
------------	---

巻頭特集

Neil Schwartzman氏来日インタビュー	4
--	----------

最新動向

情報セキュリティの脅威と動向.....	11
----------------------------	-----------

注目テーマ

PCI DSS準拠の現状と展望.....	14
-----------------------------	-----------

現状分析

診断結果にみる情報セキュリティの現状.....	18
--------------------------------	-----------

診断の現場から.....	23
---------------------	-----------

カテゴリ別の脆弱性検出状況.....	24
---------------------------	-----------

業種別診断結果レーダーチャート	34
------------------------------	-----------

ブロードバンドセキュリティについて	38
-------------------------	----

※ 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又は登録商標です。なお、本文中では商標又は登録商標を表すマークを特に提示していません。



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：SQAT® Security Report ～2016年下半期，株式会社ブロードバンドセキュリティ）をお願いします。また、商用利用は許諾しておりません。

SQAT®は当社の登録商標です。登録商標第5146108号

Neil Schwartzman氏 来日インタビュー

国際的ITコンサルタントとして精力的に活動されているNeil Schwartzman氏がカナダより来日！この度、日本各地での講演活動で多忙の同氏を当社にお招きし、インタビューする機会を得ました。氏ならではの知見に富んだ貴重なお話の数々を、ぜひお楽しみください。



Neil Schwartzman氏プロフィール

カナダ出身のITコンサルタント。
1995年よりスパム対策活動に尽力し、世界で現在最も厳格といわれるカナダスパム対策法（連邦法）（CASL: Canada's Anti-Spam Legislation）の制定に貢献。
迷惑メール対策における国際的な非営利団体「CAUCE」共同創業者・事務局長。
カナダ連邦スパム対策タスクフォースおよびアメリカ連邦通信委員会のCSRIC IIIにおけるNetwork Abuse Protectionワーキンググループのメンバーを務める。
現在、M3AAWG（Messaging Malware Mobile Anti-Abuse Working Group）の表彰選考委員会委員長。
このほか、民間企業でのITコンサルタントとして活躍。

聴き手

株式会社ブロードバンドセキュリティ
取締役 **安藤 一憲**

同 セキュリティコンサルティングサービス本部
APAC推進部 副部長 **紫藤 貴文**

同 高度情報セキュリティサービス本部
セキュリティ緊急対応部 **渡邊 寛昭**

同 セキュリティ情報サービス部
部長 **田澤 千絵**
情報管理課 **神保 冬和子**
品質管理課 **今野 麻希**

2016年11月29日
於 BBSec会議室

— ではまず、スパムについてうかがいます。ポットネットを介した違法なスパムが多く見られますが、どのような対策が考えられますか。

カナダスパム対策法（以下、CASL）は民事訴訟法なので、違反した企業に課徴金の支払い命令が出る。しかし、ポットネットによるスパムには、アフィリエイトによるものも多く見られるため、送信者が特定しづらいのが実情だ。例えば衛星放送サービスのDish Networkはホームセキュリティ事業も展開しているため、ポットネットに利用されがちである。結論として、CASLでは利益享受者とみなされる者、すなわち、スパム送信ドメインの登録名義人である個人または企業が責任を負う。Dish Networkはアメリカの巨大企業であり、ポットネット経由で同社名義のメールが送信されているので、これを根拠に同社を提訴でき、もし賠償金の支払いを拒んだ場合はカナダ連邦裁判所により課徴金の納付を命じるこ

とができるし、納付命令に応じなかった場合は民事から刑事扱いとなり、身柄を拘束することもできる。もちろん、このような法制度は果たしてパーフェクトだろうか、という声もある。確かにこの法律で取り締まれない人々は世界中に大勢いるが、とりあえずCASLのおかげで、Dish NetworkやFidelityに彼ら名義のスパム送信をやめるよう通達することができるところまでは来た。

エンジニアはスパムを技術的な問題と捉えがちだが、スパムを含めITセキュリティの問題は、法的問題や技術的問題である以前に、社会的問題であると私は捉えている。貧しい国でまともな仕事に就けない人々が窃盗を犯すのと同様に、スパム送信によりリソースを盗むのだ。それがスパムの実態である。もちろん、技術的な解決策は必要だ。しかし、私がインターネット史上初のスパムフィルターをリリースしてから20年以上経つというのに、未だに技術者達はその修正対処に追われ続けている

ということは、技術的なアプローチのみでは解決できないことを意味する。

法律に抑止力はないという考え方もあるが、少なくとも一定の効力はあるし、違反者に対して、善良な市民が正当に処罰を与える権利を得られるというメリットもある。こうした法的な解決策や取り締まりのほか、ベストプラクティス（最善策）を構築するなど、国をあげて取り組むレベルの問題だ。啓蒙や教育活動は、発展途上国と共に取り組むべきである。現在、深刻な問題を抱えているのは日本でもカナダでもG8でもなく、豊かでない国々だからだ。ベトナムには大勢の非合法的なハッカーがいる。優れた教育を受け、コンピュータに関する技術力があるにもかかわらず、まともな仕事に就ける環境が無いからだ。もし、ベトナムにシリコンバレーを設けてベンチャー企業を立ち上げれば、こうした子ども達が収入を得られる場所となるだろう。これまでにない新しいスマホが開発されるかもしれない。次世代のFacebookやiPhoneが世界のどこかで誕生するとしたら、ロシアか、ベトナム、ブラジル、インドかもしれない。サイバー攻撃でなく、正しく技術力を生かせる機会を提供すれば、問題は減るはずだ。

— DKIM (DomainKeys Identified Mail) のような電子署名技術がスパムを減少させる効果はあるでしょうか。

送信ドメイン認証システムは合法的な企業にとって大変良い仕組みだ。しかし、スパム送信者やフィッシング詐

欺師がメール認証を利用しているのも、私は見てきた。送信者認証の利点は、自分の身元を世界に公言できることだ。受信者側にとってこれは福音で、「今後、この送信元にはフィルタをかけよう」とか「スパムを送られたことがない送信元だから警戒レベルは低めにしておこう」といった具合に態度を決めることができる。送信ドメイン認証システムは、スパムをランク付けする目安になる。ただ、送信ドメイン認証システムを利用すればスパムやフィッシングを防止できると思われがちだが、そうではない。

— 悪意のある人々が、DKIMの認証署名をコピーしてコンテンツを改竄した上で、他の相手に送るような問題が起こっています。

メッセージがハッシュ化されていても、悪意のある人間がそれを回避してしまう。そして、その度に我々のような人間が脆弱性の修正を行う。私は何年もの間、スパムに関する多くの議論を重ねてきたが、その中で、スパマーを愚弄する発言があった。それに対する私の答えはこうだ。スパマーが愚かなら、なぜ我々は負け続けているのか。スパマーは、非常に熱心で働き者であり、ナメてかかると手ごわい相手だ。しかし、別に世界が終わるわけではない。回避されたからといって、DKIM標準がすべてダメということにはならない。

同様に、署名文化を無くすべきでもない。特に、トランザクションメッセージについては、ISPがメッセー

カナダスパム対策法 (CASL: Canada's Anti-Spam Legislation)

2014年7月1日施行。

欧州各国・アメリカ・オーストラリア・日本といった、主要国の迷惑メール対策関連法より10年ほど遅れての制定だが、世界一厳格な内容であることが知られている。



カナダ在住者に対するあらゆる商用電子メッセージ (CEM : commercial electronic message。テレックスからメール、SNSのメッセージまで全てを含む) を対象とする



CEM送信にあたっての要件

- 1) 「オプトイン方式」による受信者の明確な合意
- 2) 送信者の身元 (名称、所在、連絡先等) の明示
- 3) 受信者から「配信停止」を申し入れる仕組みの実装



違反すると1CEMにつき1千万カナダドルの課徴金

詳しくはこちら :

“CANADA'S LAW on SPAM and other ELECTRONIC THREATS”

<http://fightspam.gc.ca/eic/site/030.nsf/eng/home>



ジを受信し、要求されたアクションを実行できることが重要だ。消費者に対する宣伝メールを送信する企業側は、受信者側の気持ちを完全には理解していないだろう。送信側としては「ただ顧客リストに従って送っただけだ」というつもりだろうが、実際には、1.5秒くらいで300万人もの人々にメールが送信される状態なのだ。世の中で1日あたり20億、30億、40億のメールがいつせいに届く。そして、その300万通に対するISPの責任は、第一にユーザがinboxに入っていることを望むメールを取得できるようにすることであって、ユーザが望まないメールが届かないようにするのはその次だ。最近、Yahoo!が「適法なメールをブロックしてしまう方が問題なので、多少のスパムが届いてしまってもいたしかたない」と言った。もしあなたのアカウントが乗っ取られたとしても、それで直ちにメールがブロックされる心配はないということだ。時々、銀行の職員が「取引に関するメールを一体全体なぜブロックするんだ！」と、激昂してISPに連絡してくることがある。それは、単に彼らが初めてそのIP領域から送信したというだけのことで、あたかもフィッシングメールのように見える代物だったからだ。このようなトラブルは日常茶飯事であり、バランスが非常に難しい。

— CASLの特長を教えてください。

後発であることの利点を生かし、すでにスパム対策法を制定しているあらゆる国々（欧州各国、アメリカ、日本、オーストラリア、ニュージーランド等）の専門家と話し、各国それぞれの成果と問題点をヒアリングした。そうやって学び、得られた情報から、想定される課題をできるだけ解消した法律を策定することを目指した。法案通過から2年半を費やし、世界中の大量メール送信者を教育し、法律要件を満たす行動の理解に努めた。商用メッセージの送信にあたっては、「確実に同意を得ること」「送信者の身元を明らかにすること」「容易に配信停止を申し込める仕組みを実装すること」である。

— 欧州プライバシーポリシーを順守するには膨大な量の規則に従わなければなりません。CASLを順守する場合にも同様のことが起こりますか。



例えば、欧州におけるCookieの規則については、誰もが従わなければならない、日本にしようがカナダにしようがフランスにしようが関係ない。欧州のWebサイトを閲覧すると、「このサイトではCookieを使用しています」という表記を見かけるだろう。Cookieの使用を明示する責任があるためだ。欧州からアクセスされる可能性があるという理由で多くの企業がこの規則に従っている。同様に、日本の企業であっても、カナダに対してメールを送信するのならカナダの法律に従わなければならない。実際、複数のアメリカ企業がCASLに違反したかどで提訴されているし、そのほかの国の企業が提訴されるケースも今後出てくるだろう。自国内だけで運営されている会社なら、自国の法律にさえ従っていればよいかもしれないが、インターネット上で商業活動をする以上、そうはいかない。特に、ホンダや東芝、パナソニック、トヨタといった世界の有名ブランドであれば、カナダの法律と無縁ではいられない。

— もし、企業が顧客に自分の情報をメール送信先リストから外すよう要求された場合は、その顧客の情報をリストから削除するべきでしょうか。

そのような場合でも削除すべきでないというのが私の考えだ。企業としては、その顧客が「配信不要」であるという情報を登録して管理し続けるべきだ。顧客の記録は企業が身を守るためのデータでもある。例えば、顧客からクレームがあった場合でも、「お客様がこの日に登録してメール配信を希望したため、弊社のメールを受信しています。そして後日、配信不要のご希望をいただいた後、メール配信を停止しました」と明確に回答することができる。企業は顧客データを削除すべきでなく、防衛策やエビデンスとして保持するべきだ。なお、北米では、大企業が技術的対応や法的対応を行う部隊を自社内に抱えるのではなく、メールサービスプロバイダ（ESP）を利用するのが一般的だ。メールによるマーケティングキャンペーンを展開する場合、ESPにメール送信やリスト管理を委託する。

— 欧州プライバシー法では、ユーザが自身のプライバシー情報に関して企業に削除を求めた場合、企業はただちに削除しなければならないと既定していますが。

欧州の「忘れられる権利」は、主に検索エンジンやSNSを対象としたものだ。恐ろしい事件に巻き込まれ、そのことが検索エンジンに記録された個人がGoogleの検索エンジンから情報が削除されることを望んだ場合などは、合理的な要求であるように思える。すべてがアナログ

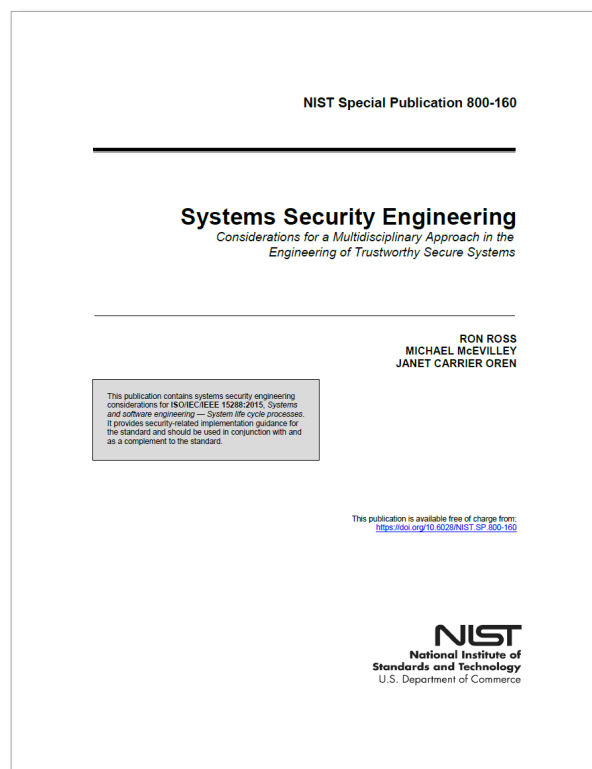
だった時代は、情報閲覧のためには市役所や裁判所に行き閲覧許可を得なければならなかった。しかし今では個人の情報を容易に取得できる。「若い頃、窃盗で逮捕されたことがある」などという情報が知られてしまう。若者達がFacebookに気軽に写真を載せるが、彼らはそれがインターネット上に永遠に残るということをわかっていない。18歳の時には愉快と感じたことが、30歳になってから厄介ごとになる。好成績で大学を出たのにどこにも就職できず、企業から「あなたがアップした写真を不適切と判断しますので、当社はあなたを採用しません」と宣告されるかもしれない。その時初めて、「ああ、あれは永遠に消えないのか」と気づく羽目になる。

一方、自動車メーカーの場合はどうだろう。欧州でホンダやメルセデスやBMWに電話して「私の情報を消してくれ」と連絡しても、メーカー側はその要望どおりにしない。自動車メーカーには、安全上の理由によるリコール発生時に備えて、ユーザに連絡するための情報を保持する権利があるからだ。ユーザが自社製品のせいで怪我をする危険性が完全に排除できるまで、メーカーが電話連絡やメッセージの送信をやめることはない。

一 自動車産業についてお訊きします。ADAS (Automatic Driving Assistance System : 自動運転支援システム) が導入された場合、どのようなセキュリティ上の影響があるのでしょうか。

社会保障上も、サイバーセキュリティ上も、影響があるだろう。まず前者について話そう。トラック運転手は、アメリカおよびカナダで高卒の中流階級出身者にとって最も高い収入が見込める仕事だ。年収8万ドルのおかげでマイホームを購入して、iPhoneを持ち、子どもに十分な教育を受けさせられる。しかし、ほんの一月半ほど前、北米で最初のロボットトラックがビールを配達する実験が成功した。自動運転技術がトラック全般に適用されたら、まずこの職業が失われ、200万人が失業を強いられるだろう。大量の失業により中間層の生活は崩壊し、深刻な社会不安に直面するだろう。

サイバーセキュリティ上の影響についてはどうだろう。最近のIoTにおけるDDoS攻撃について興味深い実態がある。通常、ボットネットでDDoS攻撃やその手の活動を行う場合、同じ手口を再利用できるように攻撃元を隠そうとするものだ。しかし、我々が目撃したケースでは、幾多もあるIP付きのCCTVカメラを通じて攻撃しているので、そのあまりの数の多さに、攻撃者は痕跡を隠す気などさらさら無かった。実に恐ろしいことだ。彼らは、いかに自分たちの力が強大かを誇示したがつている。



NIST 『Systems Security Engineering』
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf>

アメリカのNIST (National Institute for Standards and Technology : 国立標準技術研究所) が『Systems Security Engineering』という475ページにもおよぶドキュメントを作成した。これは、IoTに関する初のベストプラクティスを示したレポートである。IoTが我々の家や自動車や職場のデファクトスタンダードとなった世界における指針だ。製造一辺倒でセキュリティに無頓着な産業界に警鐘を鳴らしている。NISTはこのドキュメントに何年も費やし、10年遅れの発行となった。本来は、事前にこうした整備を行ってしかるべきだろう。しかし、我々人間というものは、何も発生しないうちは備えることをしない。悲劇が発生して初めて対策を講じ始めるのだ。RCMP (王立カナダ騎馬警察) の警察官に2005年にボットネットの話をしたら、鼻で笑われてまったく相手にされなかったが、今はどうだろう。我々は深刻な事態に直面している。

一 10年以上前からあった「IoT」の概念がここ数年で産業界から注目され、急速に進んでいます。ひたすら邁進する人々は楽観的に過ぎないでしょうか。

それこそ人間の本質だ。人間は何か悪いことが起こらない限り、ヤル気が起きないということだ。それに、IoT自体は素晴らしいことだ。しかし、私は1990年代から2000年代初頭にかけて、子どものいたずらで仕込まれ

た病院の救急救命室の扉を制御するマルウェアや、アメリカの核施設のコンピュータで検出されたマルウェアなどを見てきた。どうしてこのようなことが起こるのだろうか。最近では、テスラの自動車に対してスマホアプリを通じて動作させられるエクスプロイトコードがあることがわかった。製造側がセキュリティについて考慮していないから、製品にセキュリティ対策が施されない。セキュアでない製品の受け入れを拒否し、セキュアでない設計を規制する社会であるべきだ。アメリカでは、



Underwriters Laboratoriesという、製品の安全性を保証する会社により、北米で購入されるすべての電源コードにUL認証の小さな青いタグが巻きつけられている。テレビの機能に異常がある場合は、同社が市場に流通する前にそれを検知するのだ。当該製品のモデルチェンジやグレードアップが行われた際も、再度UL認証を受ける必要がある。

ルイス・ブラックというコメディアンが、「アプリがこんなに！いったいどこからやってきたんだ？空からか！」というジョークを言っていた。本当にそうだ。どこから来たとははっきり言い切れるだろうか。例えば、私のスマホで見ているFacebookアプリは本当にFacebookなのか。わからないし、突き止める方法もない。もしかしたら、私のスマホの画面に出ているのはすべて悪意あるアプリによって作られたコピーで、私はボットに向かって話しかけているのかもしれない。本物だと保証してくれるものは何もないし、保証する方法も私にはわからない。もちろんあなたにもわからない。なぜなら、これらのアプリはすべて空からやってきたのだから。

まさにマジックだ。実に素晴らしいマジックだと言える。我々はこのような奇跡の時代に生きている。しかし、その奇跡は、誰かに車や核施設を制御されてしまう危険と隣り合わせだ。現に、サンフランシスコ市営鉄道がランサムウェア攻撃に遭ったように。私が考える悪夢のシナリオは、今のところまだ現実にはなっていない。2003年のロンドンでのテロでは（皆さんもここ東京でテロ攻撃を経験しているが）、まだサイバー関連の要素はなかったということに驚いた。もし、日本で震災が発生したり、世界のどこかでテロ攻撃が発生したりした場合に、誰かが災害やテロの間1時間ほど緊急通話システムと病院を狙って回線を遮断したとしたらどうなるだろう。我々は、ロシアが砲撃と同時にサイバー攻撃でグル

ジアのインターネットを使用不能にしたサイバー戦争を目の当たりにした。そして、いよいよテロリストがIoTを利用したら何が起こるか考えると、その脅威は一目瞭然だ。悪意のある者達は、間違いなくサイバー世界を現実の世界に融合させようとしている。カナダのオンタリオでプライバシー・コミッショナーを務めるアン・カポーキアン氏は、何年もの間、「設計によるセキュリティ（Security by design）」という概念について語ってきた。必須の概念だが、まだ実現されていない。

— IoTに対するサイバー攻撃が物理的に人を害する恐怖に関しては、フィンランドでハッカー達がDDoSによりビルの暖房を止めたというニュースがありました。幸い、この事件での死者は出ませんでした。状況によっては大災害に発展してもおかしくありませんよね。

私はカナダのモントリオールに住んでいる。冬はマイナス30度にもなる極寒の地だ。もし、そんな攻撃が老人ホームで起こされたら大惨事となるだろう。何年か前の話だが、友人が勤務していたある政府系の建物は、彼の操作するコンピュータにより全館の照明が制御されていた。なんとそのシステムのパスワードは15年もの間、変更されていないのだ。このような実態が山ほどあるのが大変怖い。口に出すのも恐ろしいことだが、我々が本気で対策を講じる前に、サイバー攻撃で多くの人々が亡くなるだろう。

数年前、ITU（国際電気通信連合）のロバート・ショー氏とスパム問題の解決策について話し合った時、彼は「インターネット需要はタイタニック期にある」と言っていた。アマチュア無線を積んでいたタイタニックが沈没した際、救出作成において多くの死者を出してしまった理由の1つが、当時アマチュア無線に規制が無かったことだ。多くの人々がタイタニックの乗客を救おうと必死に無線通信を試みたが、互いの通信が妨害電波となって船の位置を特定することができなかったのだ。この事故をきっかけに、アマチュア無線に関する規制が設けられることとなった。同様に、もしインターネットのせいで人々が死に至る事態が発生すれば、政府による何らか





の規制が入ることになるだろう。「さあ、もう遊びは終わりだ」と言わなければならない。

そして、「インターネットを使いたいならライセンスを取得しろ」となり、インターネット上でIDが管理されることになる。これは恐ろしいことだ。インターネットの力はその匿名性にあり、独裁政権がインターネットによって転覆する様子も見てきたというのに、プライバシーや匿名性が失われてしまう可能性があるのだ。9.11のような事件で人々が死ねば、法律の規制が入り込んでくる。権力を満たすためのバカバカしい法律が。

— 5~10年後のセキュリティピックとしては、IoT以外に何が考えられますか。

国家間においてもビジネスにおいても、多くのサイバー攻撃がすでに行われている。何年か前に、あるカンファレンスで、とある中東の国の政府に雇用されているという2人組に会った。おそらくMicrosoft Officeではないかと思われるが、その手の有名なソフトウェアをハッキングするのがミッションで、その結果スパイウェアが作成されたそうだ。そのスパイウェアは、その国家が国内で市民を監視するために使用する目的だったそうだ。彼らが白熱電球や冷蔵庫に対して同様の仕掛けをしないと云えるだろうか。今のところ、世界各国の政府機関はまだDDoS攻撃を本格的に行える能力を保持していないと思われる。しかし、その内、実践するのは間違いない。銃や戦車や戦闘機による戦争はこれからも続くが、攻撃されようとした瞬間に、サイバー攻撃によりその戦闘機を墜落させられる能力を持つとしたら、どのように流れが変わるだろう。

我々の生命はネットワークという非常に信頼度の低いものに依存している。セキュアでないし、安定もしていない。このネットワークに基盤を置いているのが現状である。しかし、私は悲観的になることを好まない。ネガティブなことばかり語ってきたが、私にはモントリオールから5秒でつながる友人が日本にいるし、アフリカにも中国にも友人がいる。小作農地に暮らすチャット仲間の女性もいる。そういう自分にとって大切な人達を守りたいという思いで、私は闘い続けている。

— 自らがテロリストや大量殺人者のような異常心理の持ち主でなくても、サイバー攻撃の、しかもより洗練されたシナリオを、あれこれ考えてしまうことはあります。

私の友人で、ATMをハッキングする方法を知っている人間がいる。彼がその気になれば、ATMに20ドルと入力した上で、50ドル吐き出させることが可能だ。北米の銀行はATMを何年も変更していない。このため、同じ脆弱性が残存したままであり、私の友人はそんなATMのシステムに直接入り込めるキーコードを知っている。実際、そのような技術を持っている人間はそこらへんにゴロゴロいる。

わかりやすい例がクレジットカードのチップとPINだ。カナダと日本のクレジットカードにはPINがあるが、アメリカのクレジットカードにはチップしかなく、PINが無い。クレジットカード情報がすべて奪われる危険性があるというのに、未だにPINが導入されていないのは、アメリカのほとんどの支払いシステムのネットワークが未だに56Kダイヤルアップ接続で稼動しているからだ。PINによる認証を導入すると、重すぎて途中で通信が切れてしまう。かと言って、ブロードバンド接続の整備やカード認証機器の入れ替えに要する巨額な費用を誰も負担したくない。本来なら、PINが無いことによって発生する莫大な被害額の方をこそ想定するべきである。ところが、両者の費用を比べると、どうもシステムのアップグレード費用の方が高つくらしい。だからPINは導入せずに、56Kのままで行こう、と。これがセキュリティの現実だ。

— スマホのセキュリティについてどうお考えですか。

アプリは空からやってくるというジョークの話をしたが、実は怖いことである。ある日、ハッカーが自分のデバイスとデータ送信元の間にある複数の衛星間のデータフローを妨害できるようになるかもしれない。

しかし、スマホのセキュリティは非常にシンプルだ。オープンソースは死に、クローズドシステムに身を任せよう。もし私が、母親におススメのマシンは？と訊かれたら、世界中で99%のユーザが使用しているまさにこのデバイス (iPhone) と答える。これは美しいコンピュータだ。キーボードが内蔵されているし、ちゃんと人間が検査したアプリが入っている。空から巨大なAppleが見

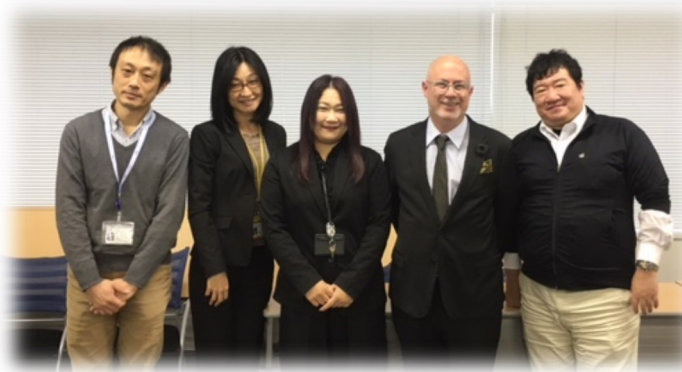


張ってくれていて、もし悪いアプリがあれば、ユーザ本人が削除する前に、目の前から消してしまう。これこそがセキュリティだ。ほとんどの人々はプログラミングもコーディングもしないのだから、ノートPCなど必要ない。Facebookして、YouTubeして、Netflixして、Skypeして、メールするだけだ。実のところ、私はAppleのシステムしか知らない。1986年以降Apple製品しか使っていないのだ。ノートPCにしる、タブレットにしる、携帯電話にしる、他のプラットフォームは使ったことがない。これからのOSは、吟味されたアプリと強固な組み込みセキュリティ、そしてプライバシー保護が完備されたものになっていくだろう。

一 最後に、日本のサイバー関連法について、どう思われますか。

私の見解では、日本における唯一の問題点は、3つか4つあるサイバー関連法の各ベストプラクティスが互いに利害衝突を起こし、整合性が取れていないことだと思う。日本政府がタスクフォースを招集し、これらの法律を刷新して実効性のあるものに統合することを提案する。CASL制定にあたって、我々は、マーケティング事業者、実業家、そして一般消費者の声を代弁する人々を巻き込み、1年かけて議論をした。互いの意見を聴き合うことは、怒りを感じると同時に幸せな気持ちにもなった。そうやって試行錯誤しながら、目標とする仕事を成し遂げた。

もし対処療法的な法律に走った場合、現在、DMARC (Domain-based Message Authentication, Reporting and Conformance) が陥っている状況のようになる。そもそもDMARCはなりすましを防ぐことでプライバシーを保護するためのものであるのに、法律自体のデキが悪く、DMARCの適用を許容していないかのような内容になっているのだ。法律の内容を修正する必要があり、そのためには政治的な主導者が結果を約束して物事を進める必



▼ 情報セキュリティに関連する主な法律

不正アクセス行為の禁止等に関する法律

不正アクセス行為や、不正アクセス行為につながる識別符号の不正取得・保管行為、不正アクセス行為を助長する行為等を禁止（平成11年公布）

電子署名及び認証業務に関する法律

一定の条件を満たす電子署名が手書き署名や押印と同等に通用することや、認証業務（電子署名を行った者を証明する業務）のうち一定の水準を満たす特定認証業務について、信頼性の判断目安として認定を与える制度などを規定（平成12年公布）

高度情報通信ネットワーク社会形成基本法（IT基本法）

インターネットその他の高度情報通信ネットワークを通じて自由かつ安全に多様な情報又は知識を世界的規模で入手し、共有し、又は発信することにより、あらゆる分野における創造的かつ活力ある発展が可能となる社会を目指して、国家のIT基本戦略を規定（平成12年公布）

サイバーセキュリティ基本法

サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念を定め、国の責務等を明らかにし、サイバーセキュリティ戦略の策定その他当該施策の基本となる事項等を規定（平成26年公布）

要がある。しかし、これに関しては、次の四半期までに成果をあげるのは難しそうだ。

まず、誰かが声をあげなければならない。でなければ、先に述べた「タイタニック期」がやってきて、規制を強化されるだけの展開になってしまうかもしれない。サイバー関連法の策定には、開かれたマインド、すなわち世界中の専門家達と意見交換ができる環境を作り出すことが必要だ。例えば自分よりその分野に詳しい人がイタリアにいるのなら、その人を呼び寄せて教を請わない手があるだろうか。もちろん日本には必要な頭脳がすでに揃っている。しかし、すべての知識を自分のコミュニティだけで賄いきれているわけではない。外の世界の誰かに教を請うことは難しく感じられるかもしれないが、カナダではそれを実行したことで、商業側にも消費者側にも配慮した素晴らしい法律を実現することができた。日本におけるサイバー関連法は、確かに自己矛盾を抱えている。しかし、そんなことは小さな問題にすぎない。臨機応変に対応し、修正していけばいいだけで、決して克服できない課題ではないのだから。



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

2016年12月、共通脆弱性識別子CVE(Common Vulnerabilities and Exposures)が、9999を超えて払い出されました。CVEは個別製品中の脆弱性を対象に、アメリカの非営利団体MITRE（マイター）社が採番している識別子です。当初「CVE-西暦年号-4桁の数字」の形で運用されてきましたが、脆弱性を含みうるシステム/製品の増加や、新たな脆弱性の出現への対応として、2014年に6桁の数字まで拡張されました。順当(?)に現実のものになったということです。

システム/製品は何が増えたのでしょうか？私たちがパッと思い浮かべるのは、スマートフォンや「IoT (Internet of Things)」という言葉ではないでしょうか。モノのインターネット「IoT」の対象は定義が曖昧ですが、これまでインターネットに繋がる必要のなかった「モノ」がインターネットに繋がることで、情報の取得・連携が行われ、生活が便利になる「モノ」といえるでしょう。

身の回りの例では、帰宅前にスマートフォンから家のお風呂を沸かす、エアコンをつけるといった指示をしたり、外出先から家のペットや子どもの様子をカメラで確認できたりと、確かに便利になっているようです。

■スマートフォンの脆弱性

2016年8月には、Apple iOSに3つのゼロデイ脆弱性「Trident」(CVE-2016-4655,CVE-2016-4656,CVE-2016-4657)が公表されました。「CVE-2016-4655」でメモリ上のデータから情報を収集し、「CVE-2016-4656」で利用者に気が付かれることなくJailBreakを実行、「CVE-2016-4657」で悪意あるサイトへ誘導することが可能でした。「Pegasus」というツールは、これらの脆弱性を悪用するスパイウェアでした。

また、2016年のAndroidの脆弱性の登録件数は、前年の4.5倍という報告があります。この背景のひとつには、2016年10月 Linuxカーネルの脆弱性「Dirty COW (CVE-2016-5195)」が公表されたことにあります。AndroidではLinuxが利用されているため、全てのバージョンに影響する可能性があり、多数の攻撃コードが公開されました。「Dirty COW」攻撃では、スマートフォン端末のほ

ぼすべてが制御可能となるため、スマートフォン内の情報の窃取、システム設定の変更が行われます。

これらの脆弱性は、実際の攻撃が確認されており、前述のCVEが9999を超えた要因のひとつといえます。スマートフォンは、音声通話、メール、カメラ、位置情報、アドレス帳、SNS (Facebook, LINE, ...) 情報など、私たちの生活に関わる情報が集約されています。個人や仕事で使用するスマートフォン端末がこれらの攻撃のターゲットとなってしまった場合、個人のプライバシーに関わる問題にとどまらず、深刻な被害に発展する可能性があることを、改めて申し上げておきたいと思います。

■IoTにおけるサイバー攻撃

IoTについては、IDDoS (IoT DDoS (Distributed Denial of Service) の略) が有名な攻撃の例としてあがるようになりました。2016年9月には、インターネットにつながった監視カメラを経由した、大規模なDDoS攻撃によって、サイトが利用不能になった事件がありました。このとき、600ギガビット/秒を超える攻撃が行われていたと報告されています。

IoT機器の不正な利用は、リモートアクセスに用いられるプロトコルの悪用や、OSコマンドインジェクションなどの脆弱性を利用して、マルウェアに感染させることを契機とすることが多くあります。今回は身近なIoT機器を用いて少しだけ検証をしてみましよう。

その1：小型Wi-Fiルータ/ストレージについて

2016年11月・12月に脆弱性の情報が公開され、ファームウェアのアップデートが実施/案内された「WFS-SR01」と「PTW-WMS1」を扱います。両製品とも「直接インターネットへ接続する使われ方を想定していなかった」という背景からくるセキュリティ上の問題がありました。

検証のため、機器をネットワークへ接続し、外部から接続可能なサービスの稼働状況を確認すると、「Telnet」

や「HTTP」などのサービスが立ち上がっていることが判りました。なかでも、リモートアクセスに用いられるプロトコルの代表「Telnet」で接続してみます。管理画面のアカウント「admin」でログインを試みると、パスワード：空 でログイン可能であることが確認されました。

続けて、システムのrootアカウントを獲りにいきます。詳細は割愛しますが、特段工夫もなくrootアカウントのパスワードが得られ、Telnetからrootでログイン可能なことも確認できました。ここでDoS攻撃を行うツールをインストールし、実行すれば、IDDoSの一端を担うIoT機器の出来上がりとなります。

```
Host is up (0.0054s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
81/tcp    open  hosts2-ns
5880/tcp  open  unknown
```

図1：サービスの稼動状況確認

```
Trying 18...
Connected to 18.
Escape character is '^'.
WFS-SR01 login: root
Password:
login: can't chdir to home directory '/root'

BusyBox v1.12.1 (2012-04-26 15:28:18 PHT) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# who
USER      TTY      IDLE     TIME     HOST
root     pts/15   00:00    Jan 26 00:14:41
```

図2：rootでのログイン結果

今回取り扱った「WFS-SR01」と「PTW-WMS1」は、別のメーカーの異なる製品ですが、どちらも同一のrootパスワードで使用されています。機器の所有者にとって、adminパスワードを変更する機会はあるかもしれませんが、rootパスワードの変更機会は無いものと思われます。従いまして、ファームウェアをアップデートしない限り、リスクのある状態で使い続けることになってしまいます。また、小型で機能が限定された機器では、ファームウェアの強制アップデートは望めません。ぜひ、これを機会に身の回りの製品のセキュリティ情報を一度チェックすることをオススメいたします。

その2：ネットワークカメラについて

先日、ネットワークカメラを購入してみました。とくに観察したいものもありませんが、売れ筋のものを選びました。2014年には、不用意なネットワークカメラの映像が、ロシアのサイト上で公開されていたことが大きくニュースに扱われたことがありましたが、最近では、カメラの映像にアクセスするための、セキュリティや安全性を考慮したサービスや機能が、様々な形態で提供されるようになっているようです。

今回購入したネットワークカメラは、利用者用スマートフォンアプリのダウンロード数が1万件を超えており、一定の利用者がいるものだといえるでしょう。カメラが撮影したデータをサービス提供者のクラウドへ接続して提供、利用者はスマートフォンアプリを用いて、サービスのクラウドへ接続することで、映像が閲覧できる仕組みとなっています。サービスのクラウドで自身の映像へアクセスするには、機器の背面に記載された個体識別番号とパスコード（4桁の数字）の入力が必要となります。個体識別番号は、ある程度の長さの英数文字列で構成されており、スマートフォンアプリ上での入力を簡略化するため、QRコードも用意されています。QRコードを撮影することで、スマートフォンアプリには、個体識別番号を手動入力せずに済むわけです。

また、個体識別番号は、アクセスを許可された人だけが知っていれば良い情報であって、不用意に開示されるべきものではありません。もし判明した場合には、パスワードの総当たり攻撃によって、不正にログインされる可能性が高まります。

さて、今回購入したネットワークカメラの商品名をインターネットで画像を検索すると、機器の裏面を写したものが見つかりました。製品の紹介記事や、個人の利用状況ブログなど様々です。個体識別番号の文字列はモザイク・マスク処理をしてあるものの、QRコードが未処理のため、個体識別番号が判別するもの。QRコードの一部をモザイク・マスクしているものの、十分ではなく、QRコードが復元可能なものがほとんどでした。また、デフォルトのパスコードは4桁の数値であるため、変更していないユーザは、個体識別番号が漏洩した場合に不正アクセスを受ける可能性が高いといえます。なお、初回アクセス時にパスワードの変更を促すメッセージがありますが、強制されるわけではありませんでした。

ここで、少しQRコードの復元について記載しておきます。

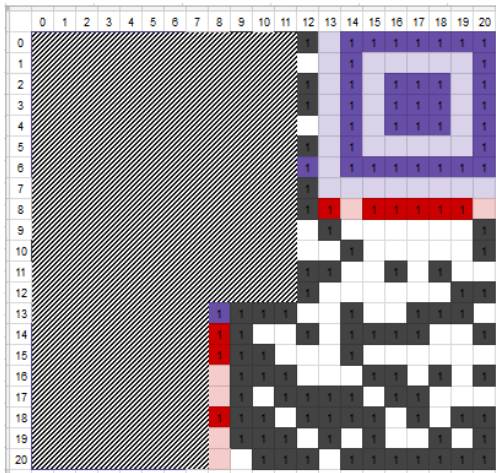


図3：QRコード（欠損あり）

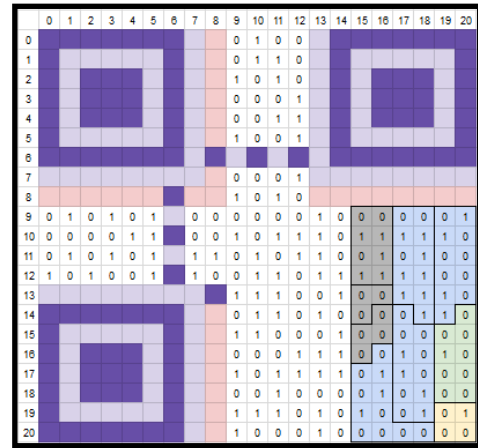


図5：青い背景の箇所が文字列に該当

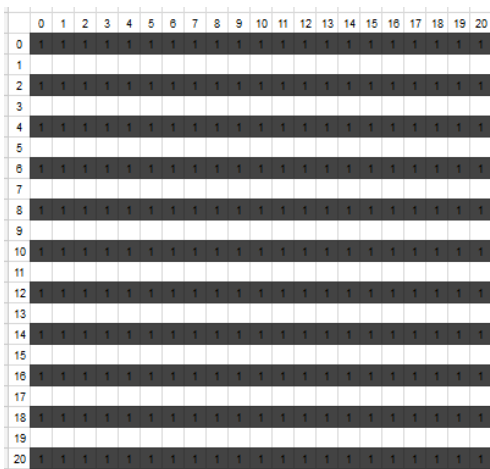


図4：マスクパターン

図3のような、一部が欠損したQRコードがあります。皆さんがお持ちのスマートフォンなどでQRコードの読み込みを行ってみてください。

QRコードには「値・文字列」以外に、「値・文字列」長さ・文字種、誤り補正、マスクパターン指定といった「情報」が含まれており、これらの部分的な情報をヒントに、元データを復元することが可能です。QRコードの仕様上、マスクパターンは8種類に限られますし、

「値・文字列」長さ・文字種が判明していれば、復元はより容易になります。なお、サンプルのQRコードの「値・文字列」は「SQAT2017」です。青い背景の箇所が「SQ」「AT」「20」「17」に該当し、欠損している箇所は「情報」に該当します。

■まとめ

IoTの普及やSNSの利用はより身近になっていますが、一部であっても情報の開示には、一定のリスクが内在されるのだということを改めて感じています。近い将来には、SNSへアップロードしているピースサインの画像から、指紋情報を取得され悪用されるといったことが、身近な出来事となる可能性があります。指紋認証については、高精細インクジェットプリンタで印刷した指紋で突破可能であることが、昨年発表のあったとおりです。

すぐそこにある危険ではないにせよ、子どもの写真はどうでしょうか？指紋は子どもから大人になっても変化しないということですので、将来子どもの写真から指紋が複製されてしまうことも、ゼロでは無いということです。と、心配の「おしり」にならないよう、少しSFめいた話で今回はおしまいです。

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ージャーとして活躍。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 (Certified Information Systems Security Professional) 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



PCI DSS 準拠の現状と展望

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本部 取締役本部長 雲野 康成

はじめに

今、筆者は九州「亀山社中」跡地の近くにいる。

「亀山社中」、のちの海援隊は、1867年5月26日（慶応3年4月23日）深夜、同隊が借り受けて長崎港から大坂に向かっていた「いろは丸」と、長崎港に向かっていた紀州藩軍艦「明光丸」が備中国（現在の岡山県）海上で衝突した「いろは丸事件」において、「いろは丸」側の当事者であった。この事件は、日本で最初の海洋国際法を取り扱った海難審判を経て、事件発生から1か月後、紀州藩が賠償金を支払うことで決着した。当事者として交渉役にあたったとされる坂本龍馬の数ある武勇伝の一つとして語られる機会も多いが、「長年培われてきた国内ルールをグローバルスタンダードが凌駕した」事件でもある。

これと同様のことが、近年、我が国のクレジットカード発行会社でも起こっている。すなわち、「グローバルなセキュリティ基準PCI DSS vs. 従来の国内セキュリティルール」という構図である。本稿では、PCI DSS上陸以降現在に至るまでの、クレジットカード発行企業をはじめとした国内の動きを振り返ってみたい。

■ PCI DSSとは

本稿にはPCI DSSが所定する用語を用いる。故にPCI DSSについてまず簡単に記しておきたい。

PCI DSSとは、「Payment Card Industry Data Security Standard」の略である。「Payment Card」には、クレジットカードのみならず、最近銀行や証券会社等が注力している「デビットカード」、若者向けに普及が進んでいる「プリペイドカード」なども含まれるが、本稿では総じて「カード」と表記する（「カード会社」、「カード情報」等）。

PCI DSSはカード情報を安全に取り扱うための基準であり、カード情報を、「伝送」、「保存」、「処理」するシステムや業務がその対象となる。「伝送」とは、ネットワークシステムのほか、物理的配送なども含む。「保存」は、紙、音声、画像データなど電子的な文字データ以外のカード情報も含む。「処理」は、システム的な処理に加え、音声通話、メモの記入、廃棄行為も含む。

PCI DSSの現在の最新バージョンは3.2であるが、その策定・管理を担うのが、2006年に設立されたPCI SSC（SSC：Security Standards Council）である。これは、クレジットカードブランド大手5社が共同で設立した協議会であり、PCI DSSの策定・管理のほか、カード会社や加盟店（定義は後述）等に対してPCI DSS準拠状況の訪問評価を行う認定評価人・評価企業（QSA：Qualified Security Assessors）の認定も行っている。当社は2008年5月、日本で2番目にQSA認定を取得しており、筆者もPCI DSSの日本における黎明期から今日までQSAとして業務を遂行してきた。

PCI DSSの準拠対象は、PCI DSSが所定する「アカウントデータ」（「アカウントデータ」には厳密な定義が存在するが、本稿では便宜上「カード情報」と表記する）を「保存」、「処理」、「伝送」する企業であり、カード会社そのもの。また、クレジットカード等による物品・サービス購入を可能にしている加盟店、その決済代行を行う決済代行企業等もPCI DSSへの準拠が必要とされている。

■ 上陸、そして黎明期

PCI DSSが日本に上陸したのは2000年代後半。VISA World Wide（以下「VISA」）等の国際カードブランドが保有する国際クレジットカード決済ネットワークに直接接続して事業を遂行していたメガバンク系のカード会社や決済代行会社が、国際カードブランドの要請（指示命令）により、2008年頃からPCI DSS準拠に舵を切った。

これら大手のカード会社は、カード会員の管理に係る「イシュー」業務（与信審査や債権管理業務、キャッシング等）と、カード会員がカード等を利用できる店舗やECサイト（以下「加盟店」）の管理に係る「アクワイアラ」業務（カード利用の承認、精算等）の2つを営んでいる。2008年からPCI DSS準拠に舵を切ったのは、そのうちのアクワイアラ事業である。これは国際ブランドの指示命令によるものであった。国際ブランドと直接契約を締結し、同ブランドのネットワークを利用する各社アクワイアラ事業のシステムには、自社発行以外のカード情報も含まれる。その事業システムへの不正侵入による漏えい規模は、膨大になる可能性があるからである。一方、この時点ではイシュー事業に対するPCI DSS準拠は

ほぼ実施されなかった。理由は、イシュー事業に係るシステムがメインフレーム等で構築され、その改修に膨大なコストと時間がかかること。システム改修プロジェクトに合わせてPCI DSS準拠を進めるほうが合理的であること等が国際カードブランドにも受け入れられることとなり、日本のカード会社においては、段階的なPCI DSS準拠（以下「段階的準拠」）が認められることになった。

なお、我が国では、大手カード会社のシステムを利用するFC（フランチャイズカード会社）が全国に400社ほどあり、多くはイシュー業務に重きを置いているが、アクワイアラ業務もその比率を問わなければ概ね存在する。一方、預貯金のキャッシュカード一体型のクレジットカードやデビットカードを発行する銀行本体は、イシュー業務のみに分類されている。故に、カード会社は2つの主管官庁の管理監督を受けている。イシュー業務については貸金業法の主管省庁である金融庁、アクワイアラ業務については改正割賦販売法の主管省庁である経済産業省である。

一部の大手Eコマースや大手インターネットサービスプロバイダ、外資系の流通企業は、国内の多くの事業者の反駁の声（「一私団体の私的セキュリティ基準である。法による強制もないし今は必要ない!」、「日本には日本の慣習・ルールがある。この基準に取り組んだら会社がつぶれる!」）に耳を傾けることもなく、早々と2010年前後に国内でPCI DSS準拠を達成した。一方、加盟店のPCI DSS準拠推進を国際カードブランドから委託されているプリンシパルカード会社の一部は、2010年から2012年頃にかけて大手対面流通業各社に対してPCI DSS準拠の啓蒙活動を推進したが、九割方で否定され、突き返される実態であった。

ここで、「日本には日本の慣習・ルールがある…」に関する事例を1つ記したい。

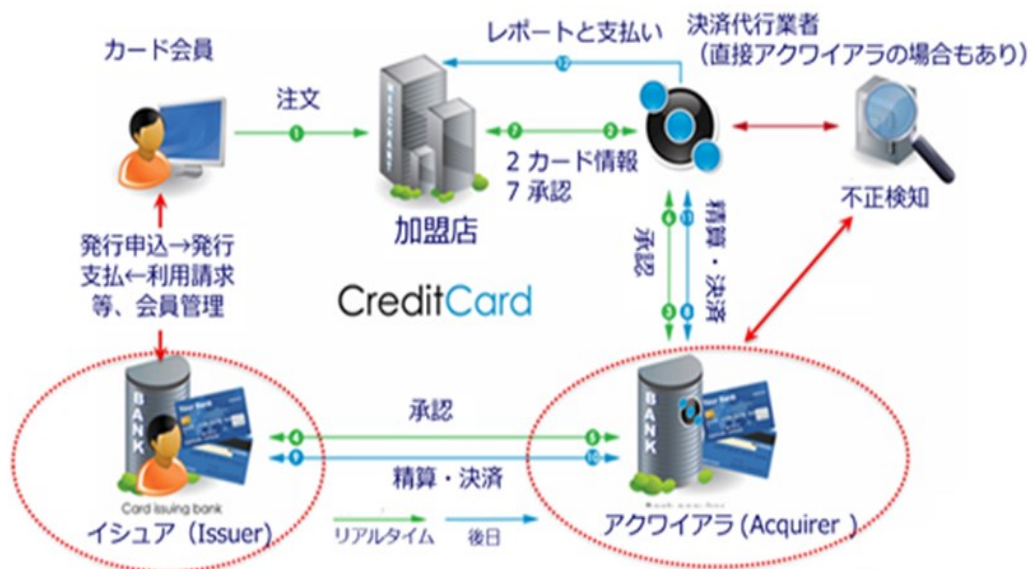
当時、日本クレジットカード協会（JCCA）には、「加盟店でクレジットカードを利用するカード会員に手渡す利用明細に対しては、カード番号のうち下3桁のみが*マークで消されていれば良い」というルールが存在し（マスキング）、多くの企業では、レシート等でしっかりとそのルールを遂行していた。

一方のPCI DSSでは、要件3.3の評価手順に「カード情報（Primary Account Number=PAN）の表示（画面、紙のレシートなど）を調べ、業務上の合法的な必要性によりPANの最初の6桁と最後の4桁よりも多い桁を見る必要がある場合を除き、カード会員データを表示する際にPANがマスクされることを確認する」とある。すなわち、上述のJCCA基準は、PCI DSSでは非準拠となる。しかし、この要件は、当時、多くの事業体に「一私団体の、面倒な外来基準」として受け止められていた。

現在、JCCAのホームページには、カード情報の流出防止対策として、PCI DSSへの準拠（全加盟店共通）、ならびに、カード情報の非保持化（非対面加盟店）の2項目が記載されている。

さて、以上のような国際カードブランドによる動きと並行し、日本の法整備でも展開があった。2009年、改正割賦販売法第35条においてクレジットカード会社が加盟店等に対してクレジットカード情報の保護を指導することが所定された。「どのように」、「どこまで」といった具体的な明示はなく、改正割賦販売法を管轄する経済産業省配下の団体がその役を担う旨の記載で法令は留まっていた。現在、その責務は社団法人日本クレジット協会（以下「JCA」）が担っている（改正割賦販売法は2016年改正された）。

2012年5月31日、JCAは「日本におけるクレジットカード情報管理強化に向けた実行計画」（以下「初版実行計画」）を発表し、カード情報に関して国際基準であるPCI DSSを前提にする、と記載した。同計画は、加盟店のレベルやカード取り扱い業務の内容に基づき2012年9月から2018年3月までの期間においてカード情報の保護対応を求めるものであったが、PCI DSSを「前提」とする、という、一部のイシュー企業への対応は範囲外と受



(<http://monlaudigitalmarketing.wikispaces.com/Online+payments>より引用、改変)

け取れる記載をしていたことにより、上述のとおり、一部のカード会社が加盟店にPCI DSS準拠推進を啓蒙したものの、黎明期を抜け出すには至らなかった。PCI DSS準拠済みの加盟店からは、「先行者メリット」ならぬ「先行損」という言葉も耳にした。筆者が属する部門も、この黎明期は地道な啓蒙活動に明け暮れる日々であった。

■普及期、そのきっかけ

その後2011年から2015年にかけては、スマートフォン決済を筆頭にカード決済の手段が多様化し、これら技術やサービスをコアコンピタンスにしたベンチャー企業が台頭した。カード会社はこうした企業と新規取引する際には、PCI DSS準拠を契約条件とした。その際にPCI DSSに関連して準拠すべきとされたガイドラインも存在する。2011年にはJCCAが、「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」にて、スマートフォン等を活用したクレジットカード決済について、カード番号をはじめとした各種情報が、安全かつ適切に取り扱われることを目的とした安全基準を刊行し、安全な鍵管理の手法の1つであるDerived Unique Key Per Transaction(DUKPT)が普及するきっかけにもなった。

普及期を迎えた国際カードブランドマークが付与されたプリペイドカードサービスについても、PCI DSSの準拠が必須となったことは記すまでもない。国際カードブランドネットワークにアクセスする必要があるため、新サービス開始のタイミングで準拠が求められる。

また、委託先としてのデータセンターが普及期を迎え、かつ、クラウドサービスが急速に浸透したことにより、国際カードブランドの対応も変化した。プリンシパルカード会社が新たにデータセンターを選択する際には、そのデータセンターが必ずPCI DSSに準拠していることを条件に課すようになったのである。欧米に拠点を持つクラウドサービス事業者も、PCI DSSが普及した欧米の企業のみならず、今後PCI DSSが日本、アジアで普及することを見据え、クラウドサービスとしてPCI DSS普及に舵を切り始めた。

更に、PCI DSSが欧米・アジアで通じる国際基準であること、具体的なデータ保護のための数値基準が設定されていること等の理由から、カード情報保護を各企業の重要情報に読み替えてグローバル情報統制を施行する本邦企業も登場した。これは、PCI DSSの内容が、企業の重要情報保護に有効であることを示す動きでもある。

金融庁の外郭団体であるFISC（金融情報システムセンター）の動きについても記しておこう。標的型メール攻撃等による企業へのサイバー攻撃が増加する中、FISC

は、2008年秋の機関誌で早々にPCI DSSが所定する数値基準に着目し、その有用性を説いていた。並行してFISCは、金融機関のシステムの可用性向上を主たる目的とした安全対策基準において、その改訂毎にPCI DSSの適用を検討していたが、金融機関がカード情報を原則取り扱わない（実際はキャッシュカードに付属したクレジットカード、デビットカードの発行やATMによるキャッシングでカード情報は扱っているが）ことから、その本格的な取り組みは見送られていた。2015年7月、第8版追補改訂の新設基準（運113：サイバー攻撃対応態勢を整備すること）に準拠するにあたり、第三者のセキュリティ評価にはPCI DSSを評価基準として用いることも有効である旨が、FAQにも記載されるに至ったのである。

これら動きに前後して、2020年の東京オリンピック・パラリンピック開催が決まった。まず動いたのは金融庁、そして東京に本拠地を置く都市銀行等である。従来、海外のクレジットカードでのキャッシングに対応する銀行ATMを設置しているのは一部銀行に限られていた。この機能を有効にするには、国際ブランドのネットワークを利用する必要がある。多くの大手都銀等は、金融庁の要請もあり、現在、ATMネットワークのPCI DSS準拠化を推進している最中である。

一方、経済産業省は、2014年7月11日に「クレジットカード決済の健全な発展に向けた研究会の中間報告書」を発表した。同報告書では、2020年の東京オリンピック・パラリンピック開催決定により海外からの旅行者等の増加が予想されることを踏まえ、「国内外のカード利用者への利便性・安心の提供」、「国内外からの不正利用を防止する安全性」の両面で世界最高水準のカード決済環境を整備することが重要な点として挙げられており、今後の方向性として明確に「PCI DSS準拠」という言葉が使われた。

そして2016年、PCI DSSは日本において普及期を迎える。

■「実行計画2016」

2016年2月23日、2020年の東京オリンピック・パラリンピック開催時までに国際水準のカード決済環境を整備することを目標に、経産省が関与するクレジット取引セキュリティ対策協議会（事務局：日本クレジット協会）は、実行計画改訂版（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－2016－【公表版】）をリリースした（以下「実行計画2016」）。

実行計画2016によれば、加盟店はカード情報を保持し

ないことを原則とし、やむを得ずカード情報を保持するのであればPCI DSS準拠を必須と定めている。準拠達成期限については、カード会社やEC（ネット通販）加盟店等は2018年3月末、デパートなどの対面加盟店は2020年3月末と明記された。計画の3本柱は以下のとおりであり、その中の一つであるIC対応は既に法制化されるに至っている。

- 1 カード情報の保護 (PCI DSS)
- 2 カード偽造防止対策 (IC対応<EMV>)
- 3 ECにおける不正利用対策

(クレジット取引セキュリティ対策協議会『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-2016-【公表版】より当社作成)

JCAでは、2016年6月14日から7月14日にかけて、札幌、仙台、東京、名古屋、大阪、広島、福岡、沖縄等の各拠点に全国のカード発行企業(イシュア)を招請して、実行計画2016の骨子を説明した。この動きに続いて、昨秋より、国際カードブランドとのネットワーク接続がある大手カード会社各社は、契約のあるフランチャイズカード会社を招請し、PCI DSS準拠の要請を行っている。

この時節から全国の地銀系、ノンバンク系カード会社でもPCI DSS準拠の検討がにわかに進行し、今日に至ることになる。なお、準拠に関しては、2018年3月に達成必須であれば少なくとも1年前から着手が必要であるが、実際オンサイト評価ができるQSAは日本全国に100名程度しか存在しない。こうした背景のもと、QSA囲い込みの動きが2017年になって突如起きている。

■デュアルスタンダード化の懸念

旧実行計画と比較すると、実行計画2016では、カード情報の定義がグローバルスタンダードであるPCI DSSに一步近づいた。たとえば、「クレジットカードの保持」という用語については、旧実行計画ではPCI DSSで定義する「保存 (Store)」と同義であり、故にPCI DSSでカード情報の保護対象とされている「処理」、「伝送」

については曖昧な状態であった。一方、実行計画2016では、PCI DSSが定義するカード情報の「保管」、「伝送」、「処理」が保護の対象となると定義された。更に、旧実行計画で、PCI DSSを「前提」にカード情報を保護する、と表記されていた箇所が、PCI DSS「準拠」によりカード情報を保護する、と変更された。

カード情報は、カード会社や加盟店等において、自社・委託先のネットワーク、サーバ機器、データベース、アプリケーション等で処理、伝送、保管されるにとどまらず、電話による音声、画像データ、帳票等の紙、作業事務行為等を通じて伝送、処理、保管される。その範囲は広く、業務やシステムネットワークが整備されていない状態でPCI DSS準拠対応を進めれば、準拠や準拠維持にかかる費用が莫大になる可能性もある。故に実行計画2016では加盟店に対してカード情報の非保持化を原則としたが、加盟店側からは、この「非保持化」について、「定義が分かりにくい」、「もっと明確に記載してほしい」等の声が上がっている。こうした指摘や要望を受け、現在、実行計画2017策定に向けた検討が進んでいる（おそらく、この冊子が刊行される頃にはリリースされているだろう）。

2017年2月17日の時点、実行計画2017の策定にあたる経済産業省と日本クレジット協会は、当事者となるカード事業者、対面流通、通販事業者、そしてQSA各社との会合の場を持って、この国家的プロジェクトを確実に進めるための意識合わせを進めている。昨年末から今日に至るまで、実行計画遂行においてはPCI DSSが所定する定義と異なる内容を記した文書も示された。実行計画2017は、それら未整理事項が、個別ケース毎に整理される予定であると伺っているが、その内容がPCI DSSの趣旨、定義とかけ離れないことを切に願いたい。PCI DSSは、クレジットカード等を扱う事業者が最低限遵守すべき国際セキュリティ基準である。この最低限遵守すべきベースラインから緩く逸脱しないことを願って止まない。

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、株式会社ブロードバンドセキュリティ入社。
現在は、同社にて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)
- 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)
- PCI DSS評価認定員 QSA



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

■ 当社の診断について

複雑化、多様化の一途をたどるサイバー攻撃が多発する現状、企業における情報セキュリティ対策も日々新たな対応を迫られている。その一環となる、システム脆弱性診断サービスを当社は継続して提供している。当社では、この診断により検出された脆弱性についてそれぞれのリスクを評価し、下記のとおりレベル付けを行っている。

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

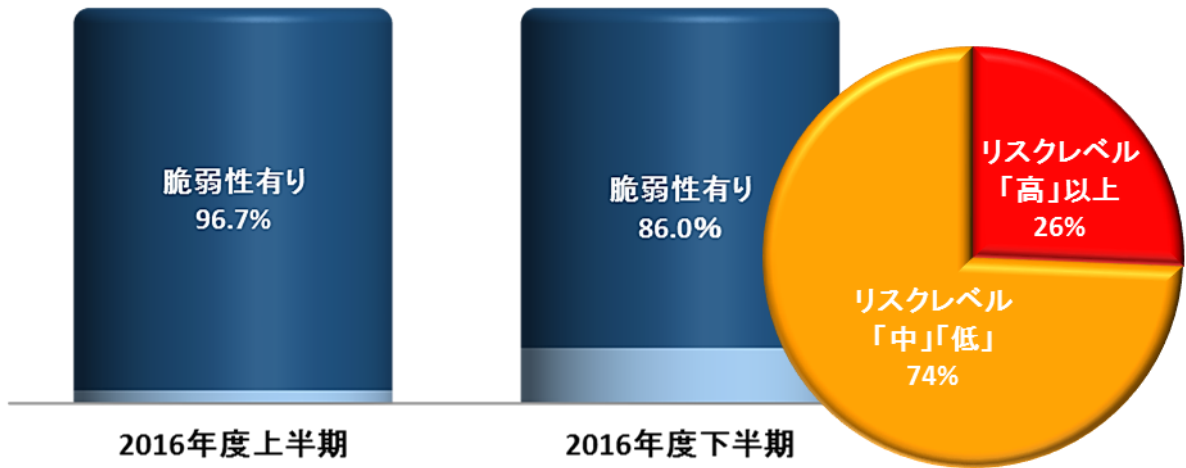
■ 2016年下半期診断結果

当社が2016年7月1日から2016年12月31日までの半年間に、13業種延べ444社の企業・団体、1060システムに対して実施したセキュリティ診断の結果について述べる。

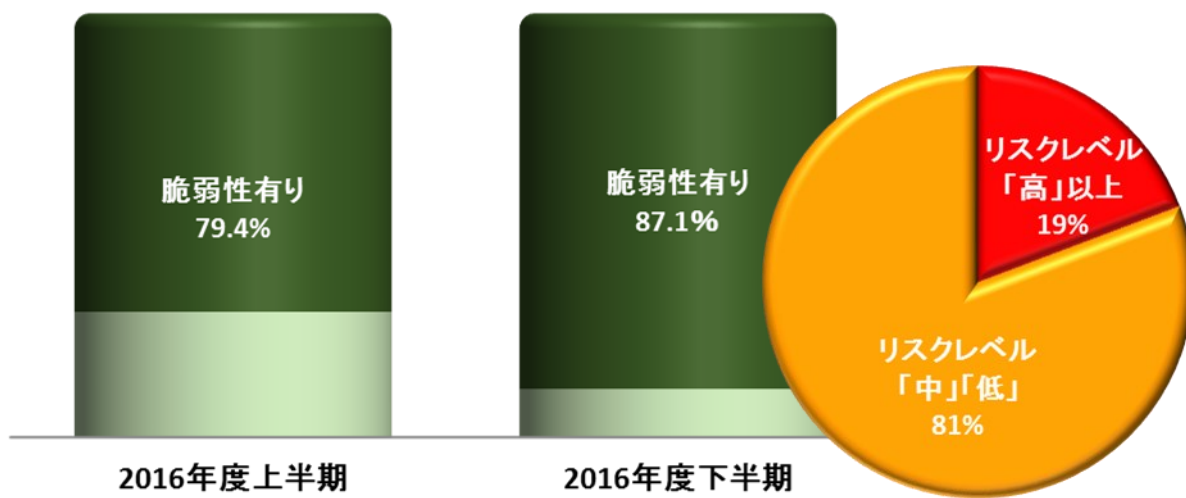
診断の結果Webアプリケーションの診断においては診断対象システム全体の86.0%の割合で何らかの脆弱性が検出された。2016年上半期の割合は

96.7%であったことから、Webアプリケーションシステムにおいては脆弱性対策が進んでいることが見て取れる。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87.1%であった。2016年度上半期は79.4%であり、ネットワークにおける脆弱性検出の割合は増加傾向にある。検出された脆弱性のうち、早々の対応を必要とする高レベル以上のリスクの脆弱性（「緊急」「重大」「高」）の検出率はWebアプリケーションにおいては26%、NW診断においては19%であった。

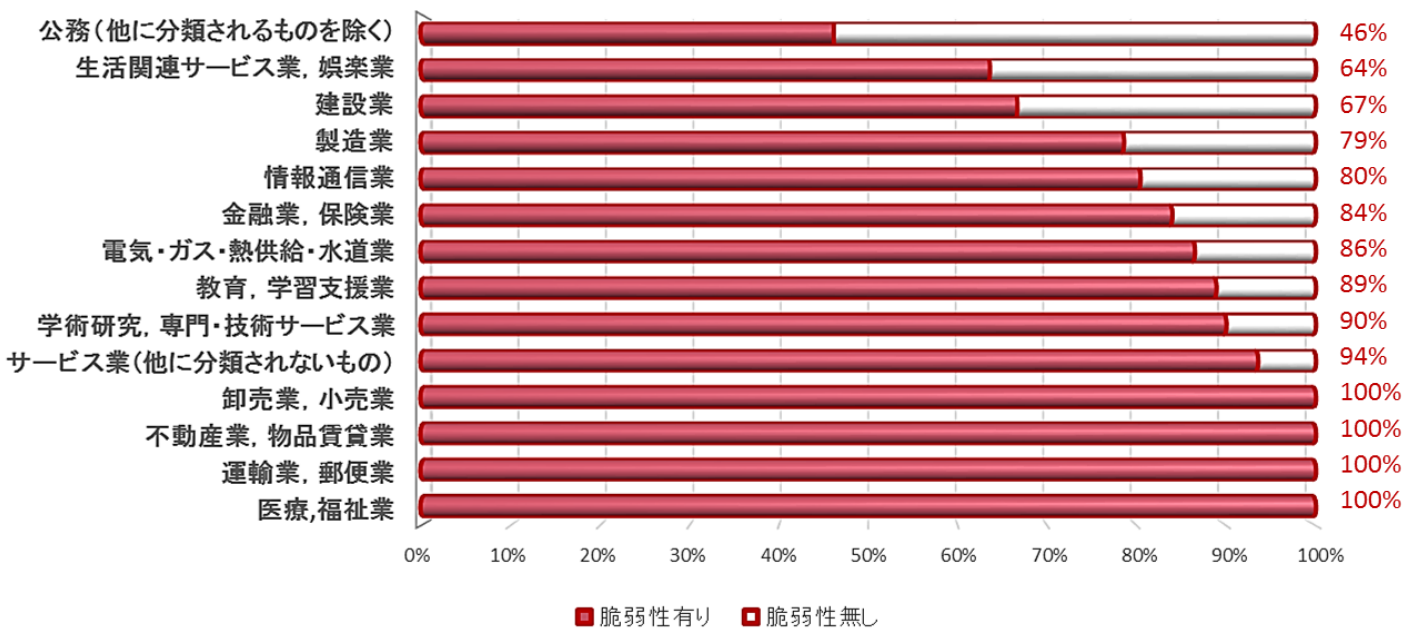
Webアプリケーション診断



ネットワーク診断



業種別脆弱性検出システムの割合



(業種分類は日本標準産業分類に基づく)

■ 2016年下半期Webアプリケーション診断結果

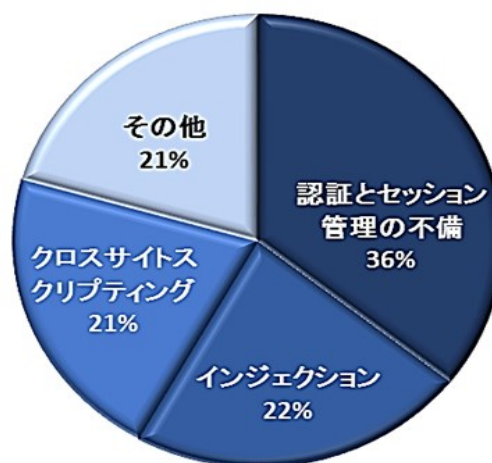
まずWebアプリケーション診断の結果から見ていこう。当社のWebアプリケーション診断では、検出された脆弱性に対するリスク評価において「OWASP Top 10」を一つの基準としている。2016年度下半期の結果に対しては、上半期同様2013年版を採用したが、当社診断にて検出された「高」リスクレベル以上の脆弱性は、その約80%がOWASP Top 10のTop 3（上から順に「インジェクション」、「認証とセッション管理の不備」、「クロスサイトスクリプティング」）のいずれかに該当する結果となった。これは2016年度上半期と同様の傾向である。ただし、上半期の当社結果はOWASP Top 10のTop 3の順位をそのまま反映していたところ、下半期では「認証とセッション管理の不備」の割合が増加したことで、「インジェクション」を上回ってトップの検出数となった。

なお、ご存知の方も多いと思われるが、OWASP Top 10は3年ごとを目処に更新されている。2016年度の診断結果には当時最新の2013年版を使用した。次に公開予定の恐らく2017年度版となるリストのほうが現状に即しているかもしれない。

OWASP Top 10は複数のアプリケーションセキュリティ専門企業によって提供される数百の組織、数千のアプリケーションのデータセットをもとにリストが決定される。OWASPによれば、Top 10の項目は「悪用難易度、検出難易度および影響についての世論的推計と普及度データに基づいて選択され、順位付けされている」とある。2017年度版用のデータセット提供期間は既に終了しており、OWASPのWebサイト上で公開されているが、それを見ると2013年版でクリティカルとされた脆弱性は変わらず候補としてあがっているようだ。普及度でダントツ

の脆弱性は「クロスサイトスクリプティング」となっており、悪用された場合の影響を考えると、Top 10に入るのは容易に推測できる。「認証とセッション管理の不備」についても普及度は4番目に高く、悪用された場合の影響も大きいためTop 10入りするだろう。「インジェクション」に関しては、普及度はこれら2つに比べると低い。こちらも影響は大きいため上位に位置付けされるのは必至だ。2017年版のTop 10がどのようになるのか楽しみである。

当社Webアプリケーション診断で検出された「高」レベル以上の脆弱性の内訳



▼ OWASP Top 10

- 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(XSS)
- 安全でないオブジェクト直接参照
- セキュリティ設定のミス
- 機密データの露出
- 機能レベルアクセス制御の欠落
- クロスサイトリクエストフォージェリ(CSRF)
- 既知の脆弱性を持つコンポーネントの使用
- 未検証のリダイレクトとフォワード

出典：OWASP「OWASP Top 10-2013: The Ten Most Critical Web Application Security Risks」(日本語版)

■2016年下半期ネットワーク診断結果

他方、ネットワーク診断では上半期と同様に「古いバージョンもしくはベンダーサポートが終了したバージョンのOSやアプリケーションの脆弱性」が、リスクレベル「高」以上では約73%に検出された。そのうち約14%がサポート切れのOSまたはアプリケーションである。サポートの終了したOSやアプリケーションはセキュリティパッチが適用されない場合があり、マルウェアに感染しやすくなるなどの様々な危険性がある。上半期のレポートでも述べたが、OSやアプリケーションにおける脆弱性は攻撃の入口として最も狙われやすい。自社に対する標的型攻撃やキャンペーンなどの無差別攻撃、さらには昨今被害がますます拡大している分散型サービス運用妨害（DDoS）攻撃のボット構築に悪用されるなど、既知の脆弱性を突いた攻撃の影響を受けないよう予防対策を講じておくことは重要である。特に近年は、固有の名前が付けられた脆弱性が世間を騒がせていることをご存知だろう。その代表例として有名なものは次のとおり。

- ・ Heartbleed
- ・ Badlock
- ・ HTTPoxy
- ・ SWEET32

なお、当然ながらこれらを悪用するExploit（攻撃プログラム）もアンダーグラウンドをはじめとする様々な場所で提供されている。それらは無償もしくは有償で入手可能であり、その価格は該当する脆弱性に対するパッチやアップデートが出ると途端に下落する傾向にある。つまり、脆弱性が発見されてから時間が経過すればするほど攻撃者にとっては「武器」が手に入りやすくなる、というわけだ。

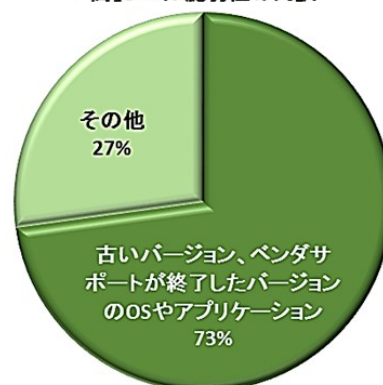
HeartbleedやSWEET32の攻撃プログラムはもはや無料で入手できることもある。その他に関しても、ピーク時の1/4から1/10まで価格が下がっていることを考えると、いかに早急な対応が重要であるかが分かるだろう。

▼ 攻撃プログラムの価格

脆弱性	発見時	現在
Heartbleed	\$25,000～\$100,000	\$0～\$5,000
Badlock	\$25,000～\$100,000	\$5,000～\$25,000
HTTPoxy	\$25,000～\$100,000	\$5,000～\$10,000
SWEET32	\$5,000～\$25,000	\$0～\$5,000

<https://vuldb.com/>より当社調べ

当社ネットワーク診断で検出された「高」レベル脆弱性の内訳



Badlock




SWEET32



■スマートフォンアプリ診断

当社の診断では、Webアプリケーションやネットワークに比べてまだまだ数は少ないが、スマートフォンアプリも対象としている。先にOWASP Top 10について述べたが、OWASPでも、スマートフォンの普及が世界的に増加、特に先進国においては普及率が非常に高いことから、モバイルセキュリティに関するプロジェクトが進んでいる。つい先日の2017年2月13日、OWASP Top 10 Mobile Risksの2016年版（リリース候補）が公開されたのはご存知だろうか。モバイルリスクのTop 10候補は下図に示すとおりである。

当社の診断でも、これらに該当する項目が検出されている。特に、「安全でないデータ保存」と「安全でない通信」は検出頻度が高い。

2016年はスマートフォン診断の需要が増加した年であり、今後もさらに増加する傾向が見られる。近頃では、スマートフォンの電話アイコン（)を見て「これって何をもとにしたマーク？」と固定電話の受話器を実際に見たことすらない世代がいるほど国内では普及が進んでおり、またスマートフォンのみで様々なことができるようになった今、取り扱う機密情報に対するセキュリティ強化や利用者へのセキュリティ教育などは大きな課題となっている。

M 1 : Improper Platform Usage (不適切なプラットフォームの利用)

M 2 : Insecure Data Storage (安全でないデータ保存)

M 3 : Insecure Communication (安全でない通信)

M 4 : Insecure Authentication (安全でない認証)

M 5 : Insufficient Cryptography (不十分な暗号化)

M 6 : Insecure Authorization (安全でない認可/権限制御)

M 7 : Client Code Quality (クライアントコードの品質)

M 8 : Code Tampering (コードの改竄)

M 9 : Reverse Engineering (リバースエンジニアリング)

M10 : Extraneous Functionality (本番運用に不要な機能や情報)

▲ OWASPによるモバイルリスクのTop10候補



診断の現場から

関口 真と申します。私は、当社において約4年間、脆弱性診断を担当しています。今回は、外部からは見えにくい脆弱性診断の現場における取り組みや、診断エンジニアとしての思いをお話しさせていただきます。

【当社の診断業務について】

まず、私たちが行っている脆弱性診断とはどのようなものであるかをお話します。「脆弱性診断」とは、一言で言えば、お客様のシステムに対してサイバーセキュリティ上のさまざまな攻撃が成立する可能性を検査する行為です。当社では、「A&P」と呼ばれる擬似アタックによる診断、「ソースコード診断」と呼ばれるソフトウェア品質の診断をサービスとして提供しています。現在私が担当しているのは、A&Pのほうで、Webアプリケーションやネットワークへ擬似アタックした結果を検証・分析しています。

当社の診断の特徴は、ツールによる診断とエンジニアによる手動診断という二重の診断体制です。診断はチーム制で実施します。診断担当者とは別の担当者が視点を変えて診断結果をチェックすることにより、ミスを防げると同時に、お互いの得意分野を活かしてフォローアップし合えます。また、診断結果を分析して報告書を作成する段階では、法的要件や業界標準への準拠状況などを踏まえた、より包括的な所見をまとめています。

診断対象は、非常に利用者の多い大規模企業のシステムから中小規模の企業のシステムまで、多岐にわたります。業種もさまざまです。自分が担当する年間の診断件数は数百件程度ですが、昨今のサイバーセキュリティへの関心の高まりを反映してか、私の入社当時と比較しても、依頼が急増していることを実感しています。

【診断業務における改善の取り組み】

お客様に満足いただける診断サービスを提供するために、現場のエンジニアも、日々工夫や改善を重ねています。最近の取り組みを1つ紹介させてください。診断の準備段階で診断対象システムのページ構成を調べる際に、結果一覧を自動生成できるツールを開発しまし

た。その結果、見積りの精度が向上し、スピードを格段にアップさせることができました。そもそものきっかけは、「結果一覧を技術者以外の担当者にもわかりやすい形で提示して欲しい」というお客様の声でしたが、完成したツールを用いることによりお客様とのやりとりがスムーズになり、効率的な業務の実施はもちろん、改善に対する姿勢を認められてお客様との信頼関係を深めることにも役立ちました。

診断エンジニアは、お客様のシステムに直接アクセスして業務を行います。その任務の重みを忘れずに、常にお客様との信頼関係を第一に考え、診断過程で生じたさまざまな課題に真摯に向き合いながら、今後も改善を重ねていければと思っています。

そのほか、継続的な取り組みとしては、最新のシグネチャを自社開発の診断ツールに追加するためのミーティングを定期的に行っています。サイバー攻撃は日々進化しており、現場ではそうした進化にいち早く対応する必要があります。当社では、開発部と協力して対応をスピードアップさせていますが、他部門との密なチームワークで課題に対処できたときの達成感は最高で、非常にやりがいを感じています。

【診断を通じて日々思うこと】

診断業務では、トークンが発行されるページ数の多いサイトを担当することがあります。診断を実施する側からすれば、トークンの発行が多いと、通常より作業時間がかかります。しかし、お客様にとっては、トークンはサイトのセキュリティを高めるために重要なものです。トークンの発行が多い案件を引き受けることになった場合、「これは大変だ!」と思うと同時に、お客様のセキュリティに対する意識の高まりを実感して手ごたえを感じます。診断担当者として、専門性の向上に努めなければと思わされる瞬間でもあります。

セキュリティ対策は、企業を影で支える裏方の仕事ですが、情報資産を扱うすべての会社にとって、健全な事業運営のために不可欠です。「コストではなく投資」として経営レベルでセキュリティ対策に取り組むために当社の診断サービスを役立ててほしい—そう思いながら、毎日、画面に向かっていきます。

診断サービス部 関口 真

「緊急性の高い脆弱性を発見し、お客様へいち早くご連絡することでインシデントを未然に防げたときは達成感もひとしおです。」



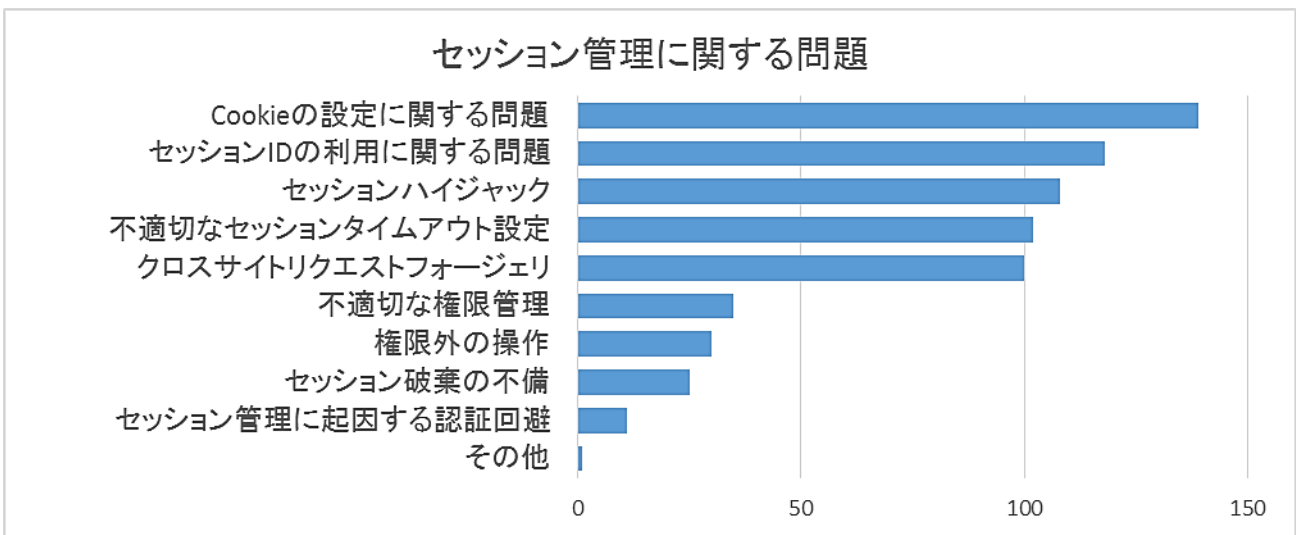
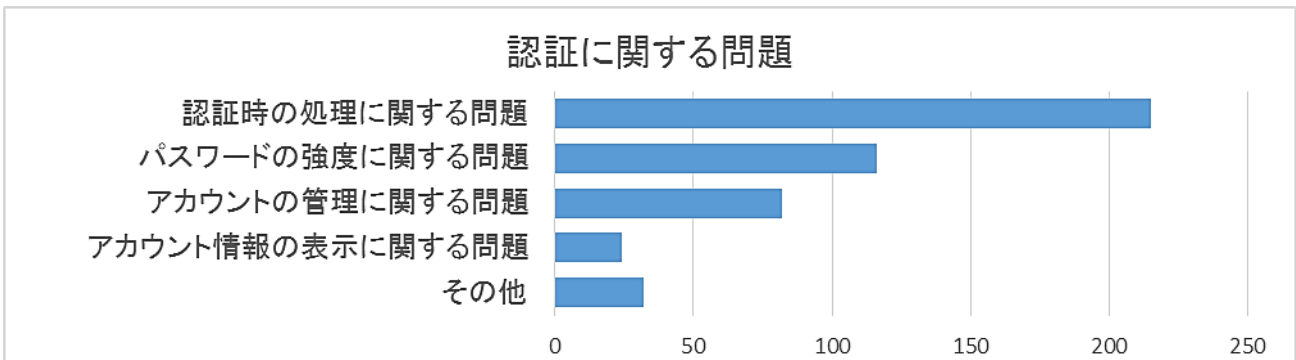
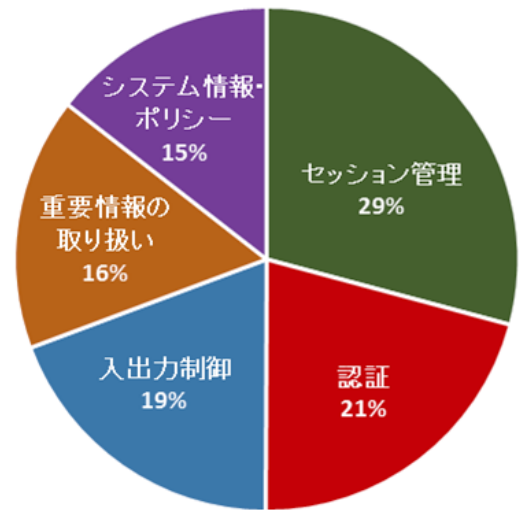
カテゴリ別の脆弱性検出状況 -Webアプリケーション診断-

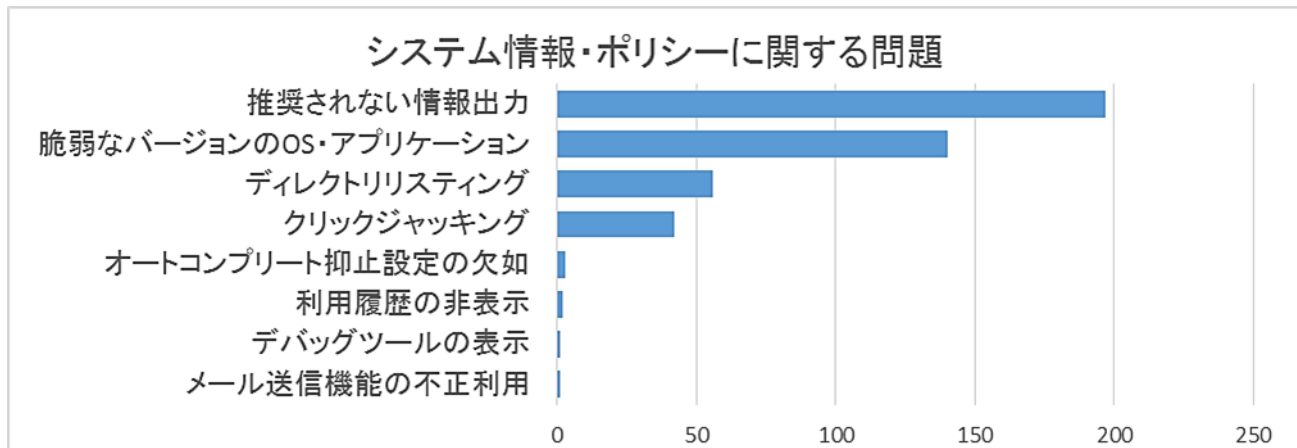
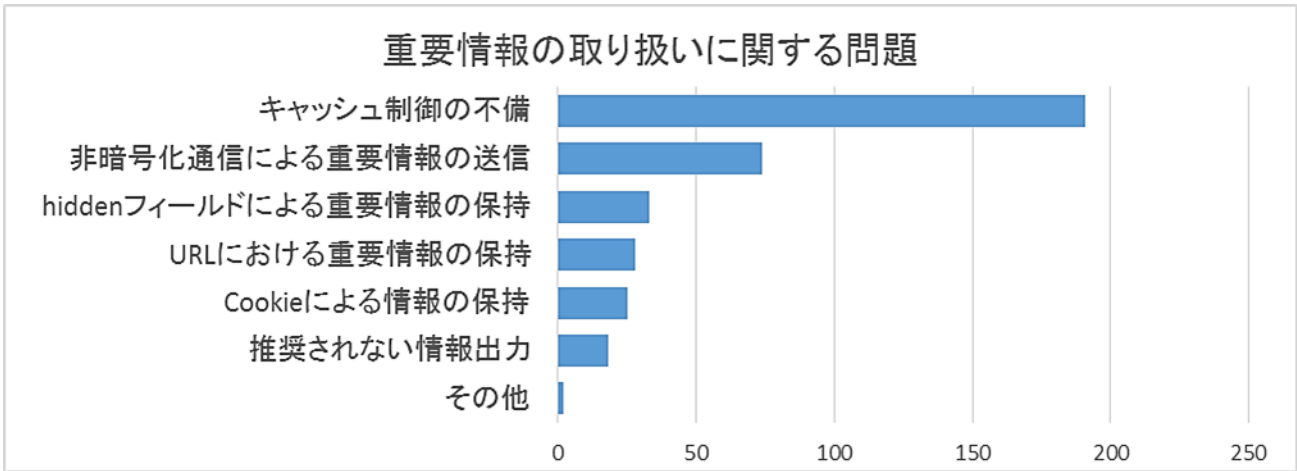
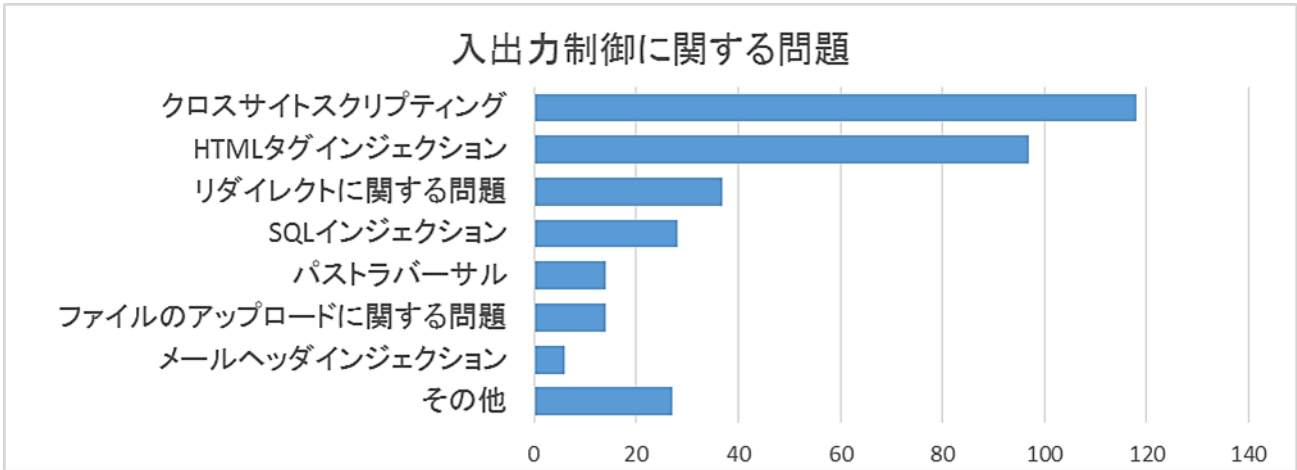
株式会社ブロードバンドセキュリティ セキュリティサービス本部

当社では、検出された脆弱性をカテゴリ分類している。

2016年7月～12月の半年間のWebアプリケーション診断における各カテゴリの検出結果は以下のとおりである。

Webアプリケーション診断	入出力制御に関する問題
	認証に関する問題
	セッション管理に関する問題
	重要情報の取り扱いに関する問題
	システム情報・ポリシーに関する問題





【Webアプリケーション診断】

入出力制御に関する問題

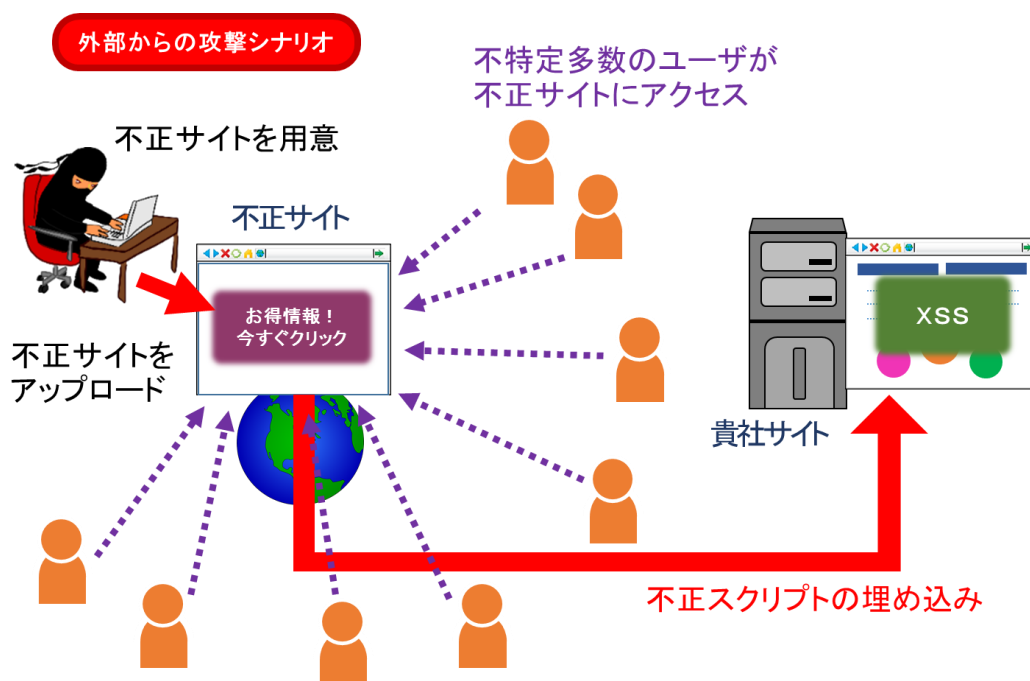
- 1 : クロスサイトスクリプティング
- 2 : HTMLタグインジェクション
- 3 : リダイレクトに関する問題
- 4 : SQLインジェクション
- 5 : パストラバーサル

入出力制御に関する問題は、Webアプリケーションにおける脆弱性の代表的な類型の一つである。ユーザ入力データおよびシステム出力データが的確に制御されていないために、攻撃者に悪意のあるスクリプトやデータを入力または出力される状態となっている問題だ。不正なプログラムを実行されたり、情報の漏洩や改竄を引き起こされたりする危険性がある。

このカテゴリにおける主な脆弱性を検出数順に挙げると、次のとおりである。検出された場合はお客様へ速報を発行し、いち早く対応をお願いしている、リスクレベル「緊急」「重大」に当たる脆弱性が多く含まれている。

このうち、インジェクション攻撃である「クロスサイトスクリプティング」、「HTMLタグインジェクション」、「SQLインジェクション」で、入出力制御に関する問題の70%以上を占めている（本誌25ページ参照）。

35%という最も高い割合で検出された「クロスサイトスクリプティング」は、新旧バージョン問わず、「OWASP TOP 10」に掲載され続けている、Webアプリケーションの代表的な脆弱性である。クロスサイトスクリプティングには、攻撃者によるスクリプトがレスポンス時に直ちに実行される「反射型」、



▲ クロスサイトスクリプティング：外部からの攻撃イメージ

Webサーバ内に格納された後で実行される「蓄積型」、そして、サーバを経由することなくブラウザ上で実行される「DOMベース」がある。IPAへのDOMベースクロスサイトスクリプティング届け出件数は、2012年の終盤を境に急増した。Ajaxの普及やHTML5の登場により増加しているものと思われる。HTML自体の機能強化により、その脆弱性を突かれる危険性もまた高まっているのだ。このため、対策として、特殊文字のエスケープ処理のほか、信用できるAjaxライブラリの使用、DOM操作のメソッドやプロパティの使用、JavaScriptライブラリの最新版の使用等、DOMベースクロスサイトスクリプティングを意識した漏れのない実装が必要である。クロスサイトスクリプティングが検出されたシステムは、外部から入力される文字列の検証、および出力時の適切な変換処理が実施されていないことから、次いで28%を占める「HTMLタグインジェクション」も同時に検出されることが多い。対策は併せてしっかり行っておきたい。

インジェクション攻撃の代表格である「SQLインジェクション」については、2014年に注目すべき判例がある。インテリアのオンラインショップにおいて7,000件以上のクレジットカード情報が漏洩した事例で、システム開発に必要な安全策を怠ったとしてベンダの賠償責任を認める判決が出されたのだ。これは、IPA発行の『安全なウェブサイトの作り方』にみられるような対策が、システム開発にあたって当然実装されるべきものとみなされることを意味している。安全なWebアプリケーション構築のためには、システム開発側ばかりでなく、発注側もまた、システムの安全性を疎かにした場合のリスクを肝に銘じ、開発期間や予算配分、セキュリティに配慮した技術力のある発注先の選定を検討すべきだろう。

しかし、現状はどうだろうか。本誌の前号で、中国の脆弱性情報ポータル「WooYun.org」（既に閉鎖されている）に2016年2月頃からSQLインジェクションの脆弱性が存在する日本のサイトが多く掲載されていることを紹介したが、その数は約400件にものぼっていたことがわかった。そして、脆弱性が存在するとされた248件のWebサイト運営者に対し、2017年1月、特例としてIPAが直接注意喚起する事態

にまで発展した。上場企業や公的機関のものも含まれていたため、IPAとしても、脆弱性を悪用された場合の影響を看過できなかったようだ。最近では、2016年に滋賀県の病院に対してSQLインジェクション攻撃を行っていた香川県の高中生らが逮捕された事件が記憶に新しい。この病院はセキュリティ対策が甘いことから6回にもわたる侵入を許していたと報道されている。病歴等、機密性の高い個人情報を取り扱っている組織においてもこのような状況が見受けられるのだ。バインド機構等の対策をとることで防げる問題であるにもかかわらず、今なお、多くの企業・組織に対して同様の攻撃が容易に実現できる状態である可能性が高い。

入出力制御に関する問題の検出量において5位の「パストラバーサル」は、件数こそ4%と少ないものの、リスクレベルが最も高い「緊急」と判定されることの多い脆弱性だ。リクエストパラメータを操作することで、本来制限された領域外のファイルやディレクトリにアクセスすることが可能となる攻撃である。この攻撃の実例として有名なのが、2003年のACCS（一般社団法人コンピュータソフトウェア著作権協会）のケースだ。同協会の相談受付サイトに入力された内容が外部にさらされていた。当該システムがパストラバーサル攻撃を受けたのは、脆弱性に配慮したCGIプログラミングが行われていなかったのが原因であった。3年間にわたりこの状態が放置されていたと判明したこともあって、当時センセーショナルに報じられた。パストラバーサルは、アクセスされたファイルによっては、サーバをまるごと乗っ取られてしまう危険性をはらむ場合もある。この脆弱性が検出された場合は喫緊の対策が必至だ。具体的には、ユーザがファイルパスを操作できないようにする、ホワイトリストに基づいた入力値検証を実施する等の方法がある。

【Webアプリケーション診断】

セッション管理に関する問題

HTTPにおいてクライアントからのリクエストに対してサーバがレスポンスを返して通信を行い、最後に接続を切断するまでの一連の流れをセッションという。セッションの管理に関して問題があった場合、攻撃者にセッションを乗っ取られて不正な処理を行われたり、不正な権限昇格を行われたりする危険性がある。

2016年下半年期において、当社の診断ではセッションの管理に関する問題はもっとも多く検出され、全体の29%を占めるにいたっている。

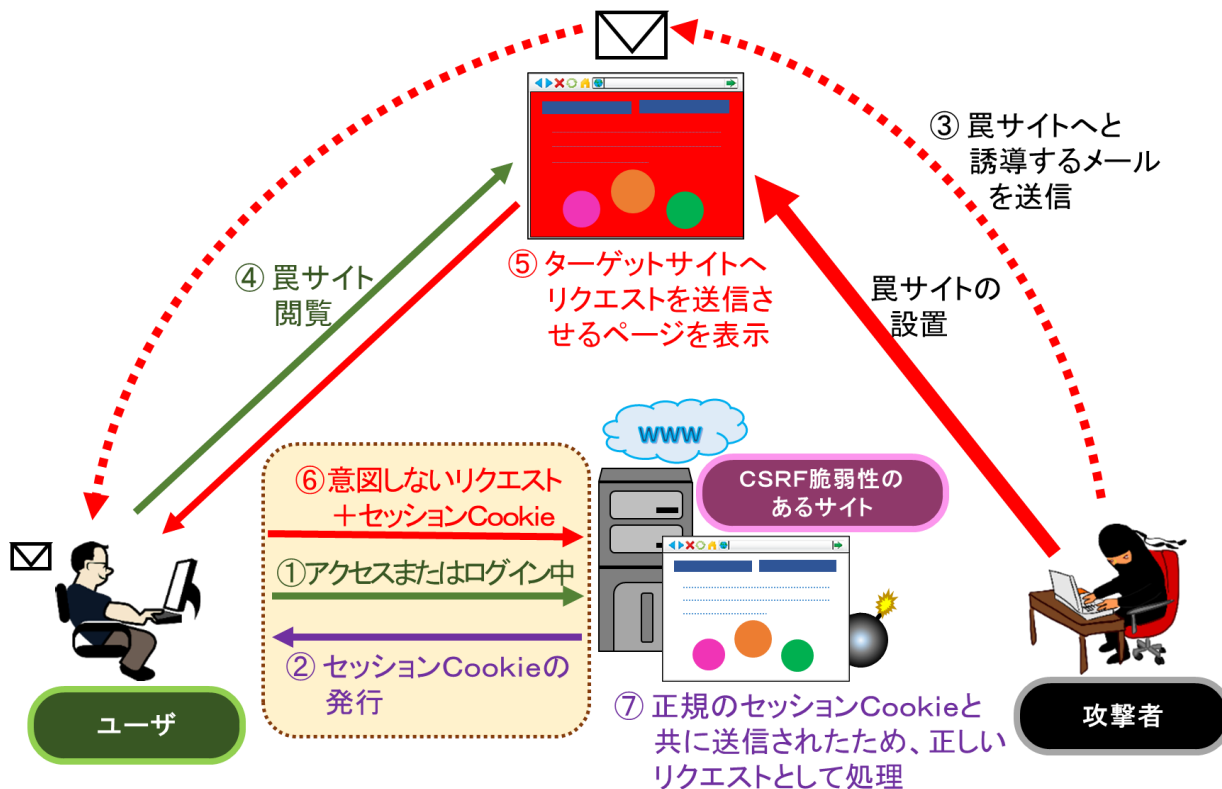
2016年に数多く検出された脆弱性のうち、セッションに関する代表的な脆弱性にセッションハイジャックがある。セッションハイジャックは攻撃者にセッションを乗っ取られる攻撃であり、成功するとログイン後の機能においてユーザ権限で様々な処理を行われたり、情報を閲覧されてしまう事態に発展する。

セッションハイジャックを可能にするためにはセッションIDを何らかの方法で奪取するか、あらかじめ攻

撃者が用意したセッションIDを使用させることが必要である。そのためセッションIDの漏洩の防止や適切な破棄がセッションを管理する上で重要である。2016年度下半期の当社の診断では実際にセッションIDの奪取が可能な、リスクレベル「高」以上のセッションハイジャックの脆弱性はセッションハイジャック全体の約30%みられた。

セッションIDを奪取する攻撃としてよく知られたものにクロスサイトスクリプティングがある。攻撃者はクロスサイトスクリプティングによってCookieを奪取し、そこに含まれるセッションIDを盗むことによりセッションハイジャックを可能にできる。すなわちあるシステムにおいてセッションハイジャックの脆弱性とクロスサイトスクリプティングによるセッションID奪取の可能性の両方が検出された場合は、単体で検出された場合に比べて危険性がさらに高まることになる。

クロスサイトスクリプティングによるセッションハイジャックの事例として2010年Apacheのバグトラッキングソフト「JIRA」の事例が挙げられる。「Apache Infrastructure Team」ブログによると、クロスサイトスクリプティングによる攻撃コードが仕込まれたURLを



▲ クロスサイトリクエストフォージェリ：攻撃イメージ

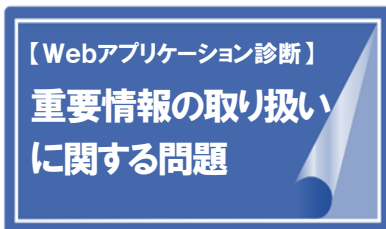
クリックしたJIRAの管理者がCookieを盗まれ、これによりセッションハイジャックを受けた可能性があるとのことであった。

この他にもセッションに関する脆弱性として有名なものにクロスサイトリクエストフォージェリがある。クロスサイトリクエストフォージェリは、正規のサイトに接続しているユーザが攻撃者の作成した罠サイトへアクセスして処理を実行することにより、正規のサイトへ意図しない処理を実行させられる攻撃である。

セッションに関する問題のうちこの2つの脆弱性が31%を占めている。これらの例に見られるようにクロスサイトスクリプティング対策をはじめとしたセッ

ションIDの漏洩防止や、リクエストが正しい画面遷移によるものであることの確認などを徹底して行い、セッションハイジャックやクロスサイトリクエストフォージェリなどへの堅牢なセキュリティ対策が必要であると言えるだろう。

また、比較的検出件数は少ないが、セッション管理に関する問題の中で極めて危険性が高いものに「セッション管理に起因する認証回避」がある。2016年度下半期の検出数は11件と少ないが、この脆弱性を悪用された場合、認証が必要な機能の操作を比較的簡単に実行できる可能性がある。したがってこれらの脆弱性が検出された場合は緊急で対応しなければならない。



しさが出るとはいえ、例えばマスキングによりマイナンバーと氏名が結びつかない仕組みを構築し、ショルダーハッキングなどが物理的に不可能となる対策を検討してはどうか。法で規制されているものはなるべくシステム側に寄せた対策を実施することを推奨する。

一方、URL内にIDやパスワードなどの重要情報を保持した作りのサイトもまだまだ存在する。一般の利用者が多いサイトの場合、どんな経路でそれら重要情報を含んだURLが公開されるかを考慮すべきである。口コミで販売機会の拡大を狙う商品なのか、メイン顧客の情報リテラシーはどうか、といった情報を考慮する必要がある。セキュリティ対策は脆弱性単体ではなく、そのサービスがどういった層を相手にしているのかを考慮しないと、実際のリスクは判定できない。

当社で診断に際して、「ヒアリングシート」として細かく対象システムの特徴をお客様に伺うのも、できる限りシステムに特化したリスク判定を目指すためである。より詳細なリスク判定を望む場合、ぜひともこの項目を活用していただきたい。

2017年1月にIPAから発表された、「情報セキュリティ10大脅威 2017」の3位に「ウェブサービスからの個人情報情報の窃取」がある。

こうした個人情報を含む重要情報の窃取には、大きく分けて二通りの原因がある。ひとつは、サイトの脆弱性を悪用した攻撃の結果、個人情報を窃取されるもの。もうひとつは、そもそも重要情報の取り扱いに問題があるために窃取されてしまうものだ。

当社が2016年下半期に診断した472システム中、「重要情報の取り扱いに関する問題」は、全検出項目の16%を占める。2016年度上半期とほとんど変わらない。

当社で「重要情報」と規定している情報は、個人情報、クレジットカード情報、営業秘密情報、認証情報などがある。個人情報や特定個人情報は法令で取り扱いが決まっており、セキュリティ上の脆弱性レベルは高くないものの、悪用された場合の影響度は決して小さくない。例えば、「マイナンバーの取り扱い」については、もちろん「万全の」体制を整えているだろう。しかし、それが正しく運用されているか、運用が継続されるかは別である。であれば、作業員にとって多少、操作のわずらわ



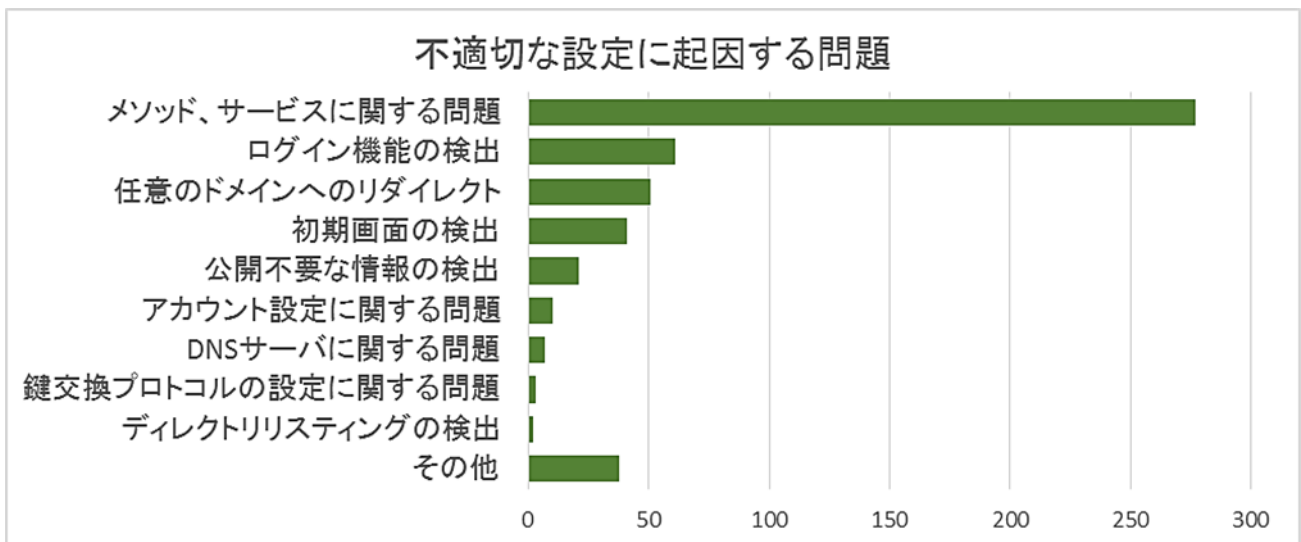
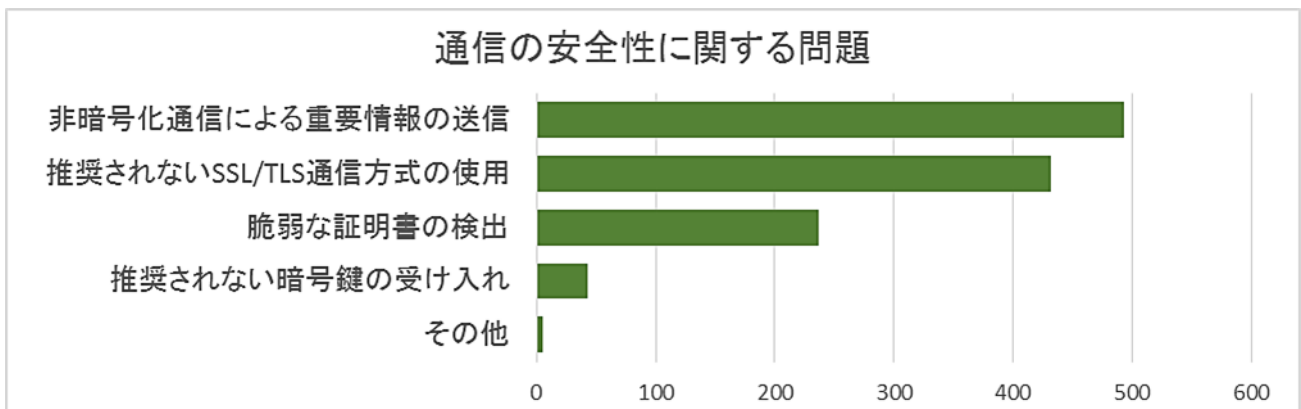
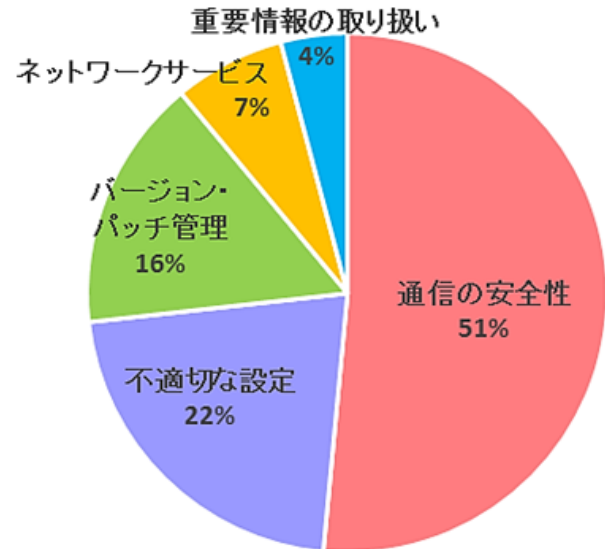


カテゴリ別の脆弱性検出状況 — ネットワーク診断 —

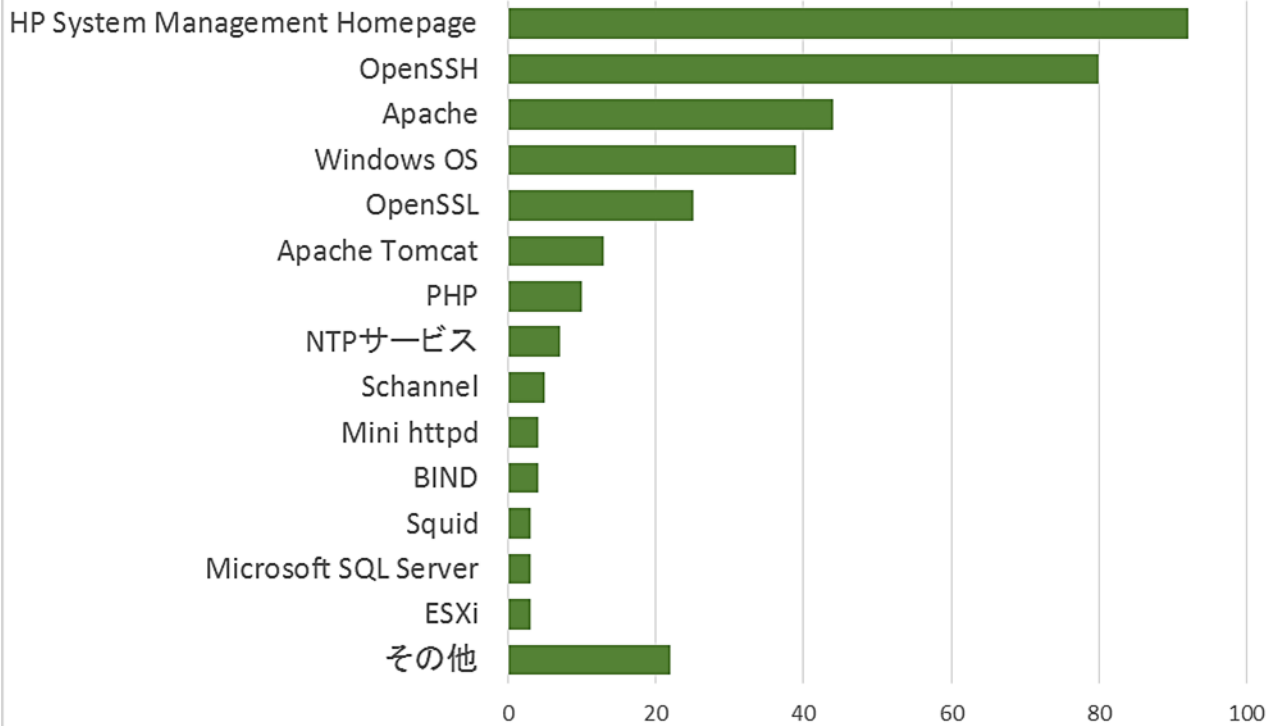
株式会社ブロードバンドセキュリティ セキュリティサービス本部

2016年7月～12月の半年間のネットワーク診断における各カテゴリの検出結果は以下のとおりである。

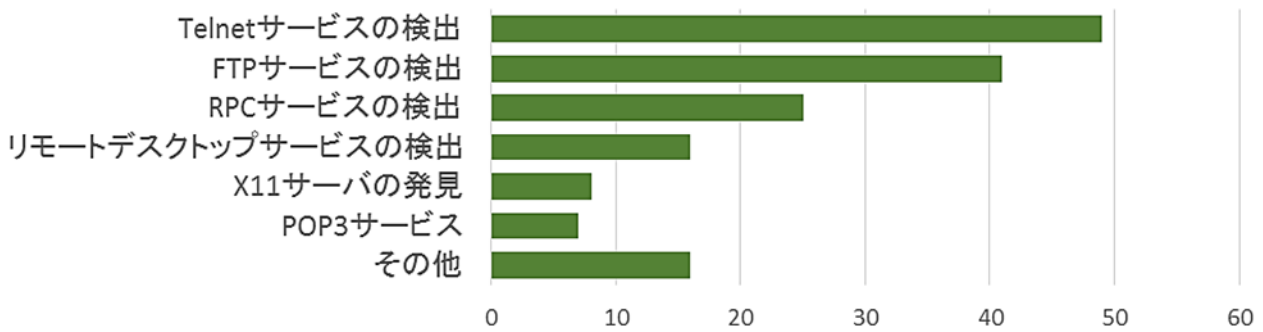
ネットワーク診断	通信の安全性に関する問題
	不適切な設定に起因する問題
	バージョン・パッチ管理に関する問題
	ネットワークサービスに関する問題
	重要情報の取り扱いに関する問題



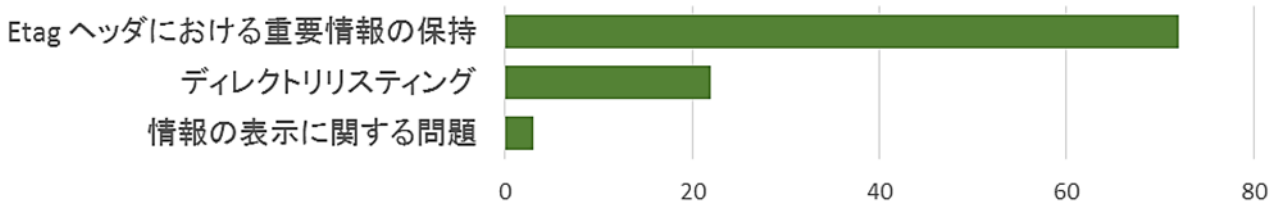
バージョン・パッチ管理に関する問題



ネットワークサービスに関する問題



重要情報の取り扱いに関する問題



【ネットワーク診断】

通信の安全性に関する問題

重要な情報の送信に暗号化通信を使用していない、または暗号化通信を使用しても強度の低い暗号鍵が使用可能であるなど、通信の安全性に関する問題は下半期も対象システムの半分（約51%）で検出された。

■ 通信プロトコルに関する問題

SSL 2.0、3.0及びTLS 1.0といったSSL/TLSの安全性に問題がある古いバージョンのプロトコルの使用は、検出数における比率は下がっているものの、依然として多くのシステムで許容されている。TLS 1.1及び1.2については近年リリースされているWebブラウザの多くでサポートされており、古いプロトコルを無効化するための障壁は低くなっている。このことから古いプロトコルを使わなければならない必然性は減っており、無効に設定することが推奨される。

また、数としては多くないものの、SSH 1.0及び互換設定が検出されたシステムも散見される。SSHについては後述する「バージョン・パッチ管理に関する問題」においても古いバージョンのアプリケーションの検出数が突出して多く、システム構築時の構成・設定が見直されていない可能性が考えられる。また、SSH自体、攻撃者にとっては極めて使いやすい踏み台であることから、その必要性を今一度見直し、設定及び構成を見直すことを推奨したい。

■ 暗号鍵、証明書に関する問題

脆弱な暗号化方式や推奨されない暗号鍵の使用など、「通信の暗号化に関する問題」は依然として多く検出されている。右記のCRYPTREC暗号リストなどを参考に、システムで使用する暗号技術の見直しを推奨したい。

証明書についてはオンサイト診断の場合、不明な認証局による証明書や自己署名による証明書が多く検出されている。実際に顧客や取引先などに公開しているシステムにおいて自己署名や不明な認証局による証明書を使用した場合、結果として顧客や取引先に被害が及ぶような攻撃

を受ける可能性も十分にあるため、信頼された認証局が発行する証明書を使用することが望まれる。

■ 非暗号化通信に関する問題

依然として非暗号化通信が許可されているシステムが検出されている。この中にはネットワーク機器やネットワークに接続されたOA機器の管理者ログイン画面が非暗号化通信で検出されるケースも含まれており、企業内におけるセキュリティ担当者だけではなくネットワーク担当者なども含めた横断的な対応が必要と考えられる。

【電子政府推奨暗号リスト】

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS ^(注1)
		RSASSA-PKCS1-v1_5 ^(注1)
	守秘	RSA-OAEP ^(注1)
鍵共有		DH
		ECDH
共通鍵暗号	64ビットブロック暗号 ^(注2)	3-key Triple DES ^(注3)
	128ビットブロック暗号	AES
		Camellia
ストリーム暗号	KCipher-2	
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
	GCM ^(注4)	
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

(注1) 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」（平成20年4月情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
 （平成25年3月1日現在）

(注2) より長いブロック長の暗号が利用できるのであれば、128ビットブロック暗号を選択することが望ましい。

(注3) 3-key Triple DESは、以下の条件を考慮し、当面の利用を認める。

1) NIST SP 800-67として規定されていること。
 2) デファクトスタンダードとしての位置を保っていること。

(注4) 初期化ベクトル長は96ビットを推奨する。

出典：CRYPTREC「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」

【ネットワーク診断】

重要情報の取り扱い に関する問題

システムや内部ネットワークに関する情報が不用意に開示されている問題は、ネットワーク診断の脆弱性全体の4%だった。上半期の1%に比べると全検出項目に占める割合は約4倍となり、検出数は前回のおよそ7倍となっている。

今回検出されたケースのうち74.2%が特定のアプリケーションの一部の設定により、攻撃者にとって有用な情報が開示されているものであった。

【ネットワーク診断】

バージョン・パッチ管理 に関する問題

ソフトウェアを最新バージョンにしていない、または、脆弱性のあるバージョンのソフトウェアに対して適切なパッチ・対応策をとっていない等、バージョン・パッチ管理に関する問題は、全検出項目の約16%で検出された。

システム管理上は全てのソフトウェアを最新の状態に保つことが理想であるが、ソフトウェアのアップデート時には常にその上で稼動しているアプリケーション群に影響がでる可能性が伴う。また、PC、スマートフォン等をインターネットを介し、複雑に連動させ業務を行うことが当たり前になってきた昨今、1システムをアップデートすることによる影響範囲はシステム管理者の想定を超える場合も多い。とあるシステムのアップデートが空港の業務に大きく影響し、フライトスケジュールが大幅に乱れた事故は記憶に新しい。

これを防ぐために、システム管理部門はバージョンアップ・パッチ管理には慎重にならざるを得ない部分がある。とくにOSに関するアップデート、よりデバイスに近い部分で動くプログラム部分のアップデートは、システム自体を支える土台になる部分のため、ひいてはネッ

このような設定による問題は、運用フェーズに入っているシステムではなかなか発見することが難しい。また、システム設計や構築全体のボリュームからすると非常に小さなほころびであり、設計・構築フェーズでも発見されないケースがあるものと思われる。今回は取り上げていないが、不適切な設定が行われていることで検出される脆弱性は他にも多数ある。こういったところで脆弱性診断を利用していただき、効率的なシステムの見直しやチェックを実施することを推奨したい。

トワーク経由で間接的にシステムとのデータのやり取りをしている末端ユーザにまで影響が及ぶ可能性があり、より慎重に行わざるを得ない。今回の結果をみても、やはり圧倒的にOS・デバイス関連のソフトウェア群のバージョン・パッチ管理の問題が多く検出されている。

■ OSに同梱され配布されるソフトウェアの問題

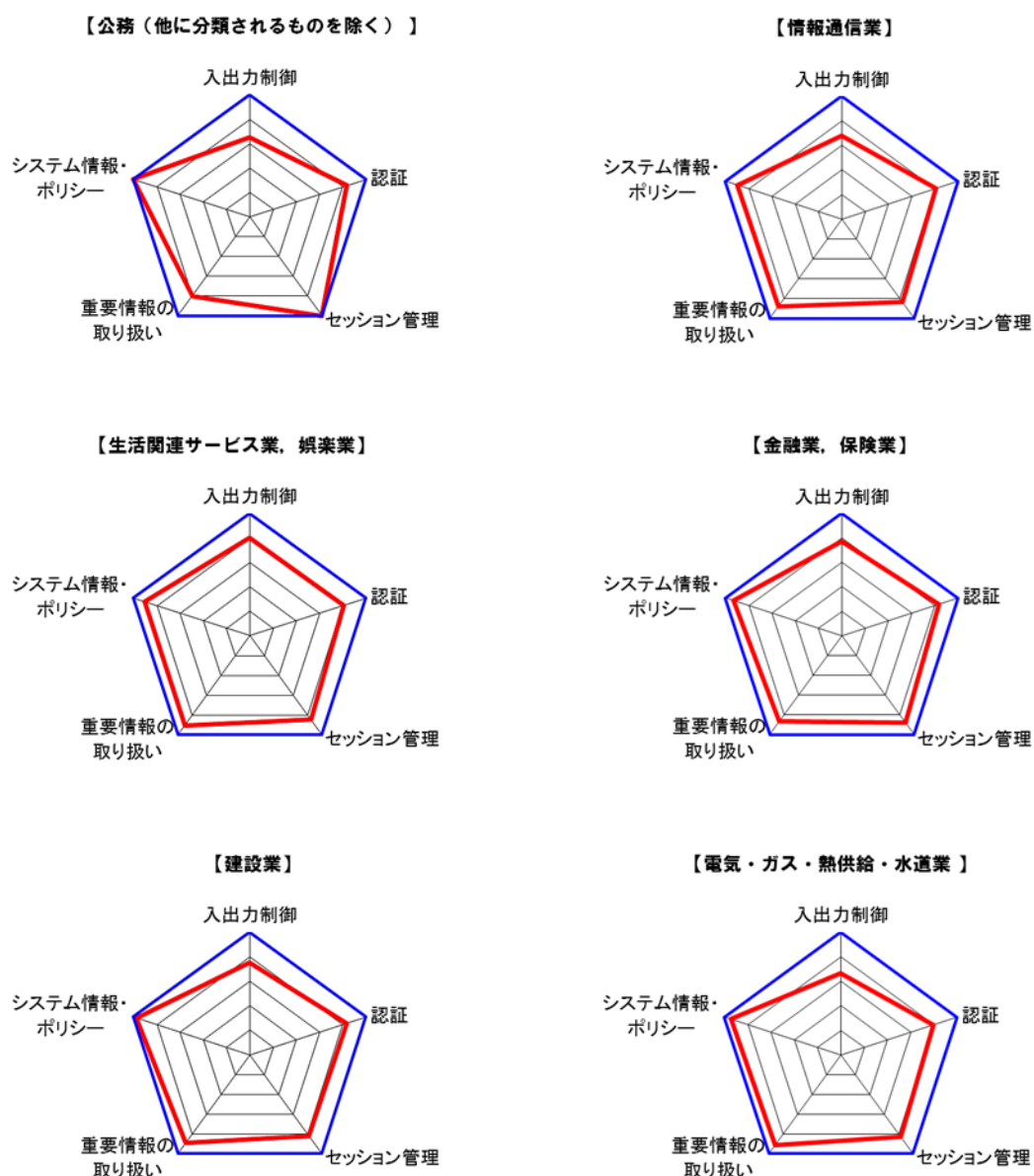
OpenSSHが適正なバージョンにアップグレードされていないことに起因する脆弱性が、バージョン・パッチ管理に関する問題のうちの21%を占めている。OpenSSHはUnix系のオペレーションシステムのパッケージの一部としてはじめから含まれており、通常はOSのセキュリティパッチを適用していれば、意識してOpenSSH単体でアップグレードする必要は無いのだが、上記のような理由でOSに関係するアップデートに含まれるがゆえに慎重になっている姿が見て取れる。

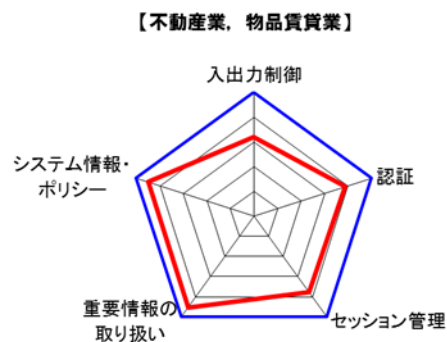
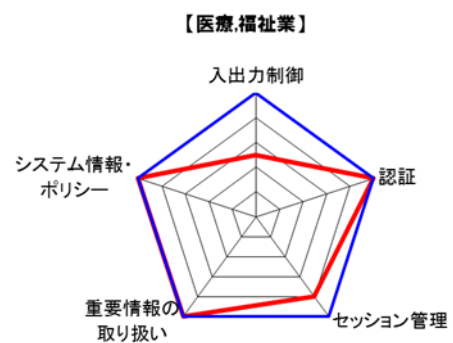
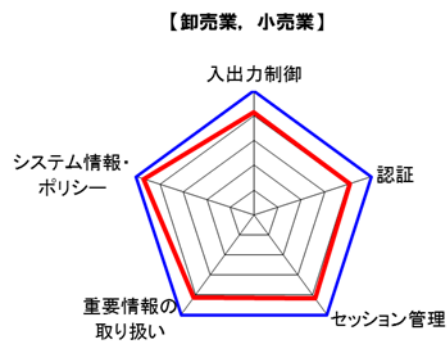
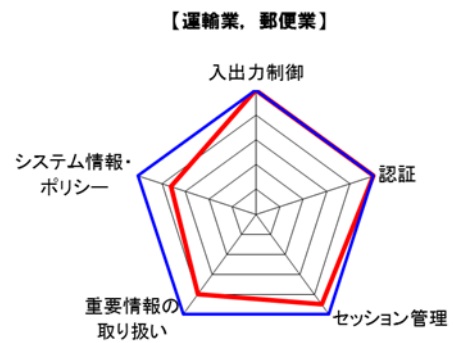
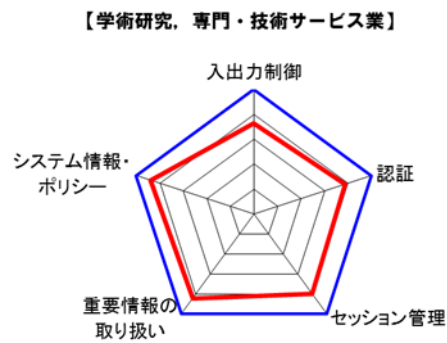
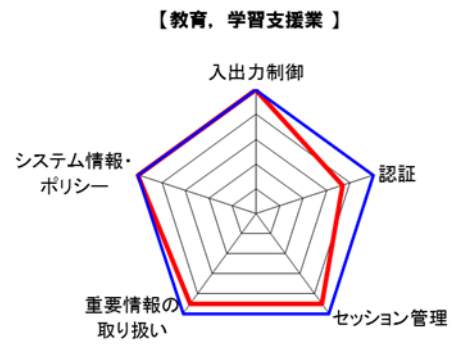
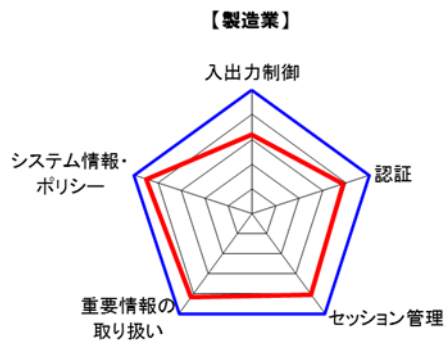
上記のような困難がともなうバージョン・パッチ管理の上で、リリース前動作確認テストの難易度は年々上がっている。システム管理者は最新のリリース情報に気を配るだけでなく、できるだけ広範囲にユーザを巻き込んで、長期管理計画の中に組み込んでいくプロジェクト管理能力が求められる所だ。

参考資料

◆業種別 Webアプリケーション診断結果レーダーチャート

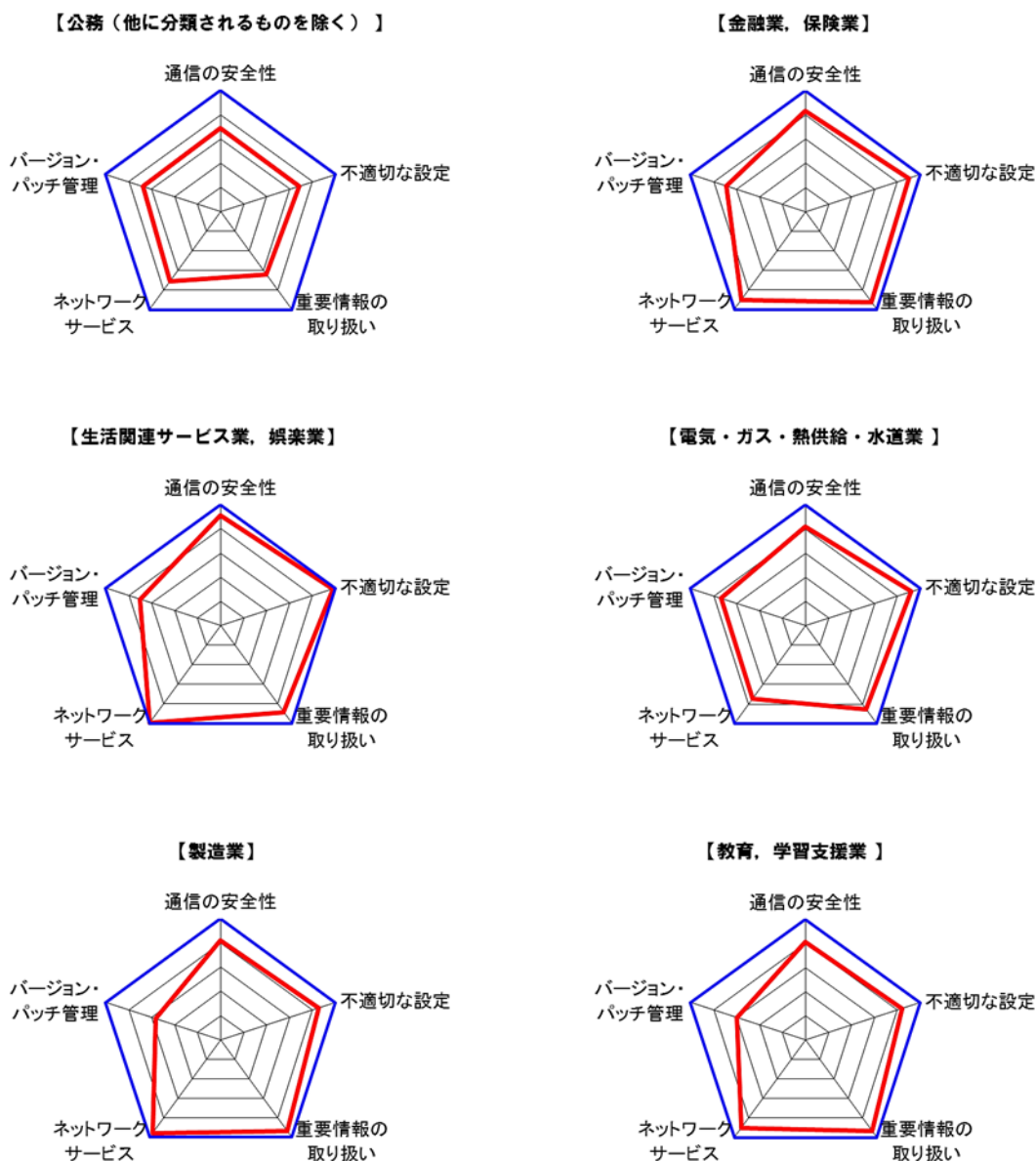
Webアプリケーション診断の結果より、各カテゴリに対する対策の度合いについて、業種別平均値をレーダーチャートで表した図である。特に「入出力制御に関する問題」について、早急な対策が求められる業種が多く見受けられる。





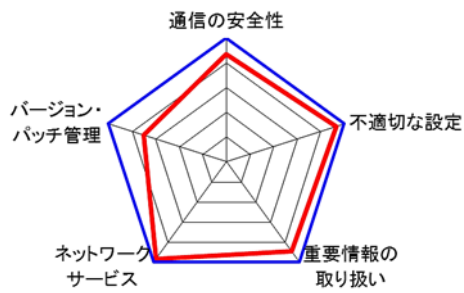
◆業種別 ネットワーク診断結果レーダーチャート

ネットワーク診断の結果より、各カテゴリに対する対策の度合いについて、業種別平均値をレーダーチャートで表した図である。業種ごとに対策を強化するべきカテゴリの特徴が異なるが、「バージョン・パッチ管理」が徹底されていない業種が多く見受けられる。

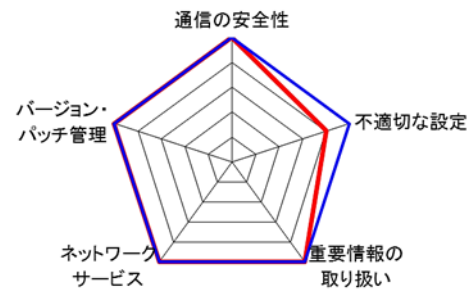




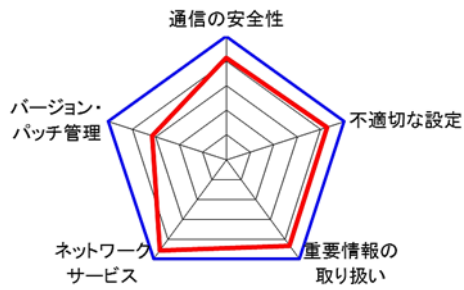
【情報通信業】



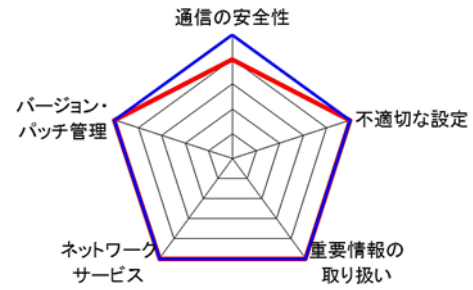
【学術研究、専門・技術サービス業】



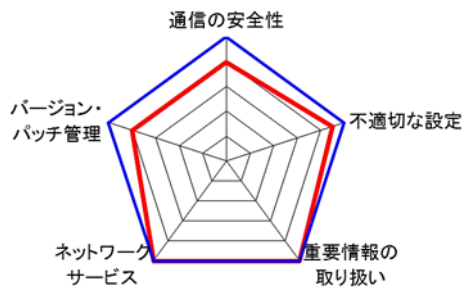
【サービス業（他に分類されないもの）】



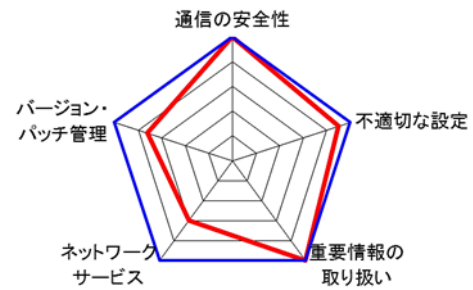
【不動産業、物品賃貸業】



【卸売業、小売業】



【運輸業、郵便業】



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)

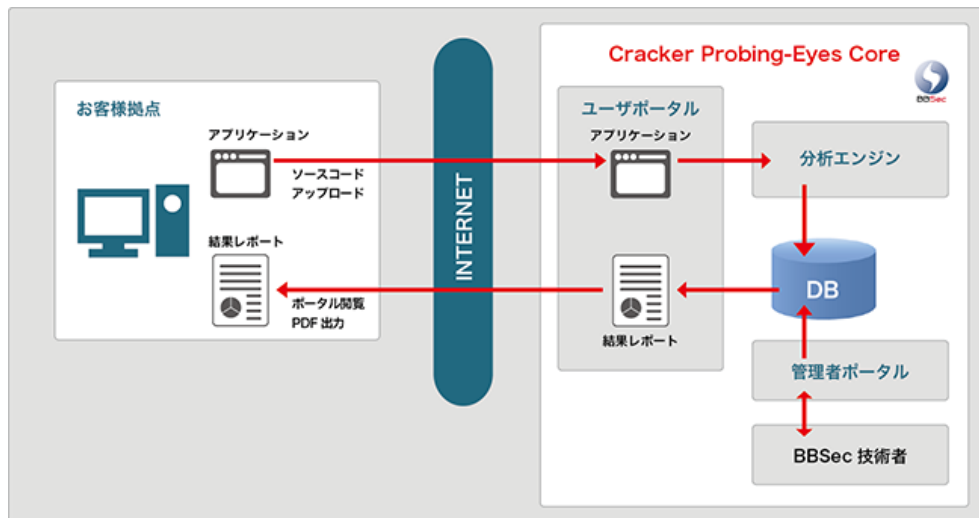
20/F Glass Tower, 534, Teheran-ro, Gangnam-gu, Seoul, 06181, Korea

TEL : +82-2-2008-4642

SaaS型ソフトウェア品質自動分析診断

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が行えるため、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。



サービス特徴

手間なくソフトウェアの品質と脆弱性を検査

開発ソフトウェアの品質と脆弱性を同時に検査することが可能です。またコンパイルすることなくWebブラウザ経由でソースコードをそのまま圧縮してアップロード／診断する利便性を提供しています。

幅広い診断対象

多様なプログラムに対応できるよう、様々な業界標準、各種プログラム言語に対応しています。

任意のタイミングに診断が可能

診断のタイミングを自由に設定できるだけでなく、短時間で結果を確認することができ、時間の切迫する開発現場が望む診断時間の短縮化に大きな効果を発揮します。

わかりやすい診断結果

ブラウザ上では、セキュリティリスクの結果だけでなく、そのリスクが発生する流れを確認することができます。

高い費用対効果

サービス範囲内であれば、いくらでもアップロード／解析／結果確認が可能のため、費用対効果にも優れています。

スピーディーかつ高品質の診断レポート

診断直後に受け取れるレポートは、BBSecのナレッジが集約された国内企業に最適化された内容です。

お電話でのお問い合わせ

03-5338-7430

受付時間 9:30～18:00(土・日・祝・年末年始を除く)



SQAT® Security Report 2016年下半年 (7月~12月)

2017年2月28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/>