SQAT® Security Report

2016 年上半期（1 月～6 月）

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

今や私たちの生活に欠かせないものとなったサイバー空間は、ここ数年でさらに激しく変化を続けています。競争環境がグローバルに変化する中で勝ち抜いていくためには、IT を有効活用したビジネスの革新が重要となっています。

一方で、サイバー攻撃も増加の一途をたどっています。例えば、不十分なセキュリティ対策が原因で、個人情報や取引先から預かった機密情報等を流出させてしまった場合、あるいは自組織のサーバやパソコンが踏み台とされ、意図せず不正アクセスや迷惑メール等の加害者側となってしまった場合、自組織の機密漏洩や取引先からの損害賠償請求によるダメージのみならず、ステークホルダーから管理責任を問われるおそれも出てきます。なにより、これらに伴う信用の失墜は計り知れません。組織の存続とビジネスの発展のために、サイバーセキュリティ対策は必要不可欠となっています。

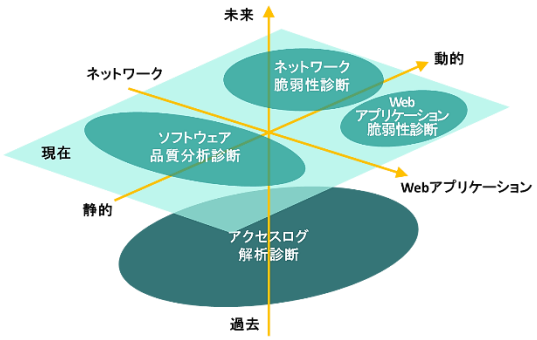
政府も、先の日本年金機構における情報漏洩のような深刻なインシデントの発生に危機感をつのらせており、2015 年施行のサイバーセキュリティ基本法が、早くもその 1 年後に改正法の成立に至るなど、サイバーセキュリティに対する取り組みは、これまでの官公庁に例のないほどの速さで進んでいます。また、今年 8 月 2 日に内閣官房 内閣サイバーセキュリティセンターが発表した「企業経営のためのサイバーセキュリティの考え方の策定について」においては、サイバーセキュリティへの取り組みが企業の社会的責任として要請される等、B to C・B to B 問わず、あらゆる組織が具体的実装を伴う変革を迫られています。常にこうした動向を調査し、自組織にフィードバックする仕組みの構築も求められることでしょう。

本書は、株式会社ブロードバンドセキュリティ（以下「当社」）の「SQAT®」が 2016 年 1 月～6 月の半年間に実施し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状や脅威の傾向について分析したレポートです。

本書が、これをご覧になった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

近年の情報セキュリティの脅威

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

直近 1 年間に国内企業の 3 割がセキュリティ侵害を経験し、データロスによる平均損失額は 1.4 億円を超えるとの調査が EMC から発表されました。[1]

セキュリティ侵害の原因は様々で、法人を標的としたランサムウェアの攻勢はとどまるところを知らず、また、Web サイトの脆弱性を突かれた大規模な情報漏洩が、ニュースで報道されるのを目にする機会が幾度もあったかと思います。ごく最近では、スマホアプリ「Pokémon GO」の人気を利用して、不正ツールを仕込んだ偽アプリをダウンロード/インストールさせる手口で、スマートフォンが狙われる脅威が目立ちました。

[1]Dell EMC「EMC Global Data Protection Index 2016」より

ランサムウェアによる脅威

「身代金」を要求する脅迫型マルウェアであるランサムウェアが、短期間のうちにこれほどまでの脅威に成長した背景としては、攻撃者にとって、手軽で採算の取れるビジネスモデルであったことが考えられます。感染させた被害者へ直接アプローチして「鍵」を売買するだけで、重要情報を盗み出す必要がないこと。さらには、多くの企業において「自組織は狙われるほど有名ではない」との認識から、具体的な対策がとられていないことが、攻撃を助長する結果につながっています。

ここで私たちは、ランサムウェアを用いた攻撃が「標的型攻撃」でのみ発生するという誤解を懸念しています。「標的型攻撃」は、主に重要情報の窃取を目的とした、特定の組織・個人を狙う攻撃です。狙いをつけた対象の関係者・SNS などから情報を収集、専用のマルウェアを作成するなどの時間と手間を惜しまない徹底した攻撃が行われる特徴があります。これに対し「ばらまき型攻撃」は、言葉のとおり、対象は誰でもよく、主に金銭の窃取を目的とした攻撃が行われる傾向にあります。例えば、○○国の▲▲業界を対象に、汎用的な文面のランサムウェア付メールを配布する攻撃は、ある程度の絞込みが行われているものの、「ばらまき型攻撃」であって、「標的型攻撃」ではありません。**ランサムウェアは組織の知名度に関わらず、いつでもあなたのもとに届く可能性がある**わけです。

主な対策として、定期的なバックアップをとることが挙げられていますが、「バックアップ時のみ接続すること」、「バックアップは複数種類のメディアに保存すること」、「バックアップを複数とること」といった運用が徹底されていないのが実情です。初期のランサムウェアの被害は、対象 PC のデータを暗号化するところまでであったため、ファイルサーバへのバックアップも対策として有効でしたが、最近ではサーバの既知の脆弱性を利用し LAN 接続されたファイルサーバのファイルが被害にあう事例もあり、LAN 内での拡散を防ぐための運用面の対策が重要となっています。もちろん、OS・ソフトウェアの最新化とセキュリティソフトの定義ファイルを最新化することも必要です。

組織の規模や知名度といった考え方のフィルタを外し、誰もが攻撃を受ける可能性を考え、攻撃を受けた場合に被害の拡大を最小限にするための迅速な対応が、今求められています。

Web アプリケーションの脆弱性を突く攻撃

Web サイトの脆弱性では、「日本テレビ」、「J-WAVE」、「Avex 所属アーティストの公式サイト」、「栄光ゼミナール」で、OS コマンドインジェクションによって、大量の個人情報漏洩が発生しました。とくに、後の 3 件については、採用していた特定の CMS プラグイン（ケータイキット for Movable Type）に存在する脆弱性を悪用されたものでした。一見、「皆が使っている・有名なプラグイン・ソフトウェア」は、安全に思えますが、実際はどうでしょう。とあるセキュリティ・エバンジェリストの言葉を借りれば、「The sky is blue, water is wet, and software has bugs.」とのことです。

OS コマンドインジェクションは、外部からデータの入力/操作を受け付ける Web アプリケーションプログラムにおいて、OS に対する命令文を紛れ込ませた文字列を送り込み、対象システムを不正に操作する攻撃です。攻撃を受けたプロセスの特権によっては、非常に深刻な被害が発生する可能性があります。対象プラグインのソースコードを、弊社でも検査ツールにかけてみたところ、OS コマンドインジェクション脆弱性が検出されました。

脆弱性が既知のものになると、攻撃ツールがインターネットで公開され、攻撃が流行化します。当然タイムリーに対応されるべき事象ですが、当社で実施した診断では、既知の脆弱性が解消されないままのシステムに遭遇することが多々あります。**開発部門では脆弱性を認識していたものの、ユーザ部門に情報が連携されておらず、結果として脆弱性が放置されたまま**というシステムも少なくありません。（参考：本書 8 ページ「診断結果にみる情報セキュリティの現状」）

既知の脆弱性を解消するには、「セキュリティパッチの適用」、「最新バージョンへの更新」などの対策が必要となりますが、今日の複雑化したシステムでは、変更による他システムへの影響や、人的リソースの問題により対策が進まないことがあります。システムの導入/リリース時の評価にどのように取り組んでいくのか、便利さ・スピードが求められる中であっても、大きな落とし穴に気付かない/放置しないための施策が必要とされています。

スマートフォンに対する脅威

おそらく世界一有名なゲームとなった「Pokémon GO」は、世界各国で配信スケジュールが異なったことから、早くに手に入れたいユーザが、非正規サイトから APK をダウンロード/インストールしてしまう現象が発生しました。非正規サイトから提供されたアプリには、遠隔操作ツールを含んだ「Pokémon GO」も確認されており、このバックドアつき「Pokémon GO」は、正規のものと画面がまったく変わらないため、通信/挙動を解析しないかぎり、正規アプリ等との区別がつかないものでした。自分自身で自分の端末にバックドアをインストールし、いまでもこの悪意あるアプリを使い続けているユーザが居ないとも限りません。先日閉会式を終えたリオオリンピックのセキュリティ監視でもアラートがあがったとか、虚実相半ばした話が漏れ聞こえてくるほどです。

正規サイト以外からのアプリのダウンロード/インストールは、決して行わないことを推奨します。非正規マーケットには、「お得」、「便利」、「自己責任」を謳い文句に、本来有料のアプリを無料で配布するものや、正規アプリの広告を改竄しリパッケージしたものなど、有象無象のアプリが存在します。インターネット上のまとめサイトで、お勧めアプリとして紹介されているからといって、信用するべきではありません。私物デバイスの業務活用（BYOD：Bring Your Own Device）が許可されている場合、企業のネットワークに接続されたリソースまでもリスクにさらされることになります。**万が一の場合には、「自己責任」では済まない**ことを認識しておくべきです。

情報セキュリティの脅威は、古くから認識されている脅威もあれば、新たに発見された脅威、未知の脅威まで多種多様であり、今後さらに分化し、対策が複雑化することが懸念されます。しかし、攻撃する側にもリスクが存在します。サイバー攻撃の流行やトレンド、その背景を分析し続け、攻撃者にとって「割に合わない」と認識させるよう、諦めずに対策し続けることが肝要です。

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

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

サイバー攻撃がはびこる昨今、組織の多くは自身が保有または管理する情報資産を守るべく日々奮闘している。しかし残念ながら、当社が実施したセキュリティ診断の結果*、攻撃に対して十分な対策が実施されていないシステムが診断対象システム全体の半数以上に上ることが明らかとなっている。

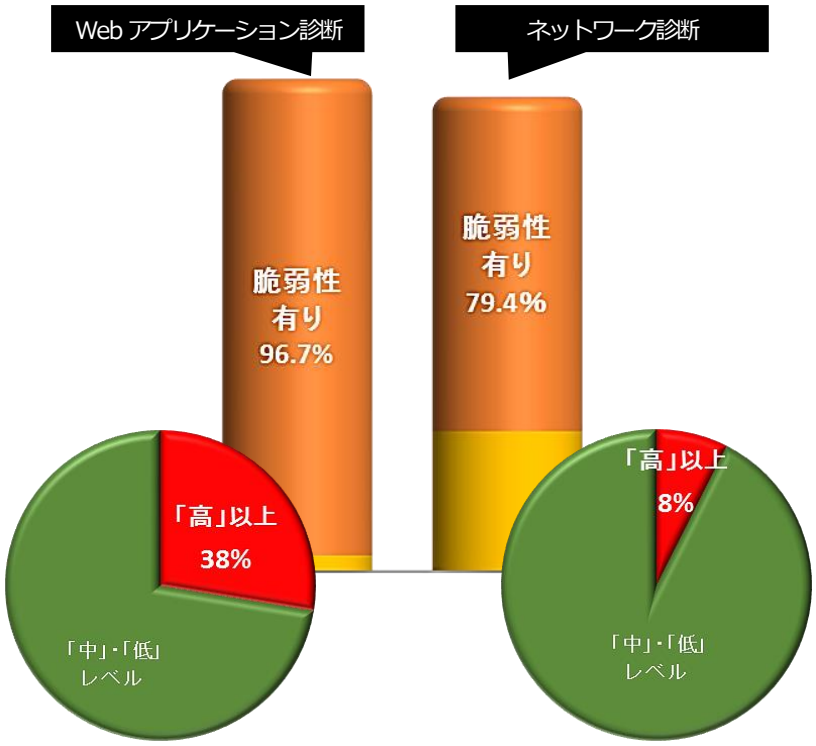
***セキュリティ診断結果：**
本書は、当社が 2016 年 1 月 1 日から 2016 年 6 月 30 日までの半年間に、13 業種、延べ 377 の企業・団体、1226 システムに対して実施したセキュリティ診断の結果。

当社では、セキュリティ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、レベル付けを行っている。当社で採用しているリスクレベルは以下のとおり。

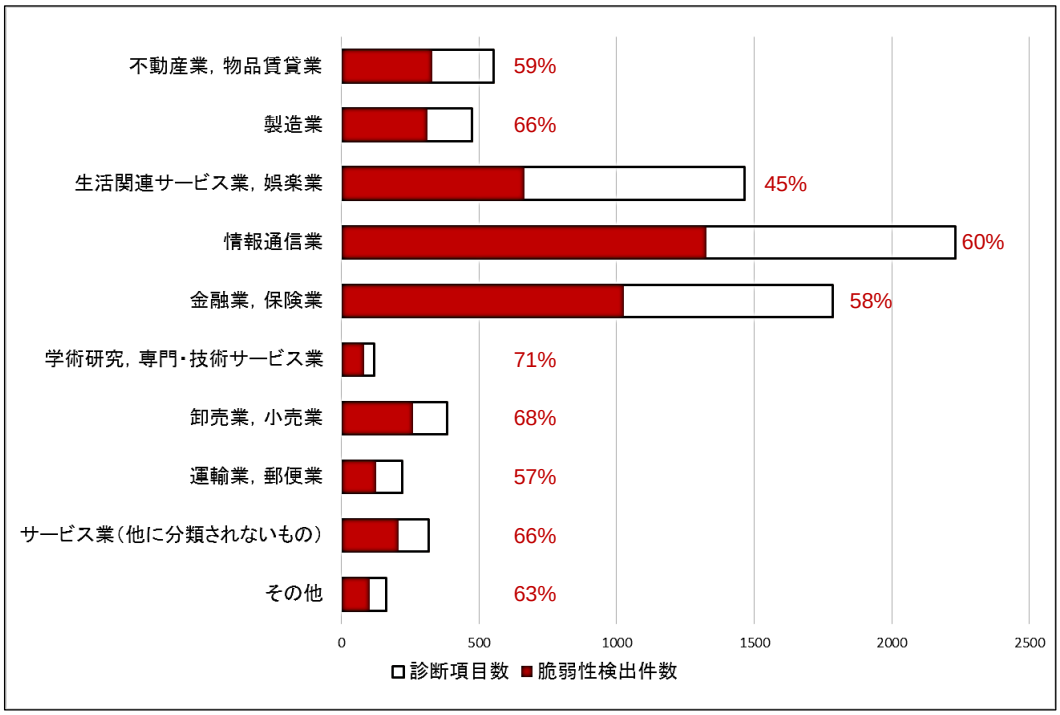
リスクレベル	説明
レベル５：緊急	攻撃された場合の影響が甚大、または容易に攻撃が実行可能
レベル４：重大	攻撃された場合の影響が大きい、またはある程度の知識や技術があれば攻撃が可能
レベル３：高	攻撃された場合の影響が限定的、または攻撃を実行するために特定の知識や技術が必要
レベル２：中	攻撃された場合の影響が限定的、間接的、または攻撃実行の難易度が比較的高い
レベル１：低	攻撃された場合の影響が軽微、または攻撃を実行するための条件が複数必要など、実現が困難

当社の診断の結果、Web アプリケーション診断においては、診断対象システム全体の 96.7%、ネットワーク診断においては診断対象システム全体の 79.4%において、なんらかの脆弱性が検出された。検出された脆弱性のうち、早々の対応を必要とする「緊急」「重大」「高」リスク（高レベル以上）の検出率は、Web アプリケーション診断においては約 38%、ネットワーク診断においては約 8%であった。

【全システム診断における脆弱性検出割合】



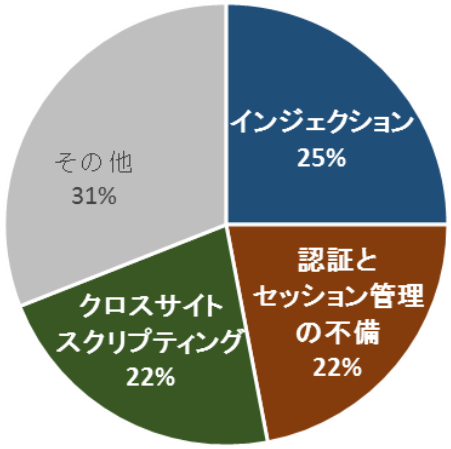
【セキュリティ診断実施　業種別件数と脆弱性検出割合】



※その他：電気・ガス・熱供給・水道業 / 宿泊業,飲食サービス業 / 建設業 / 教育,学習支援業
（業種分類は日本標準産業分類に基づく）

Web アプリケーション診断において検出された高レベル以上の脆弱性は全て「OWASP TOP 10 2013」に挙げられているカテゴリのいずれかに該当する。

【当社Webアプリケーション診断で検出された「高」レベル脆弱性の内訳】



【OWASP TOP 10】

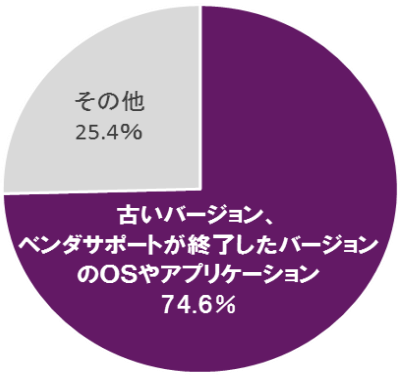
- インジェクション
- 認証とセッション管理の不備
- クロスサイトスクリプティング（XSS）
- 安全でないオブジェクト直接参照
- セキュリティ設定のミス
- 機密データの露出
- 機能レベルアクセス制御の欠落
- クロスサイトリクエストフォージェリ（CSRF）
- 既知の脆弱性を持つコンポーネントの使用
- 未検証のリダイレクトとフォワード

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

中でも、TOP 3 のカテゴリ（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（XSS）」）に該当するものは、約 70%を占めている。OWASP TOP 10 プロジェクトの目標は「組織が直面している最も重要なリスクのいくつかを説明すること」とされているが、当社での診断結果もまさに昨今の情報セキュリティ事情を表していることが明らかになった。

他方、ネットワーク診断では、古いバージョン、もしくはベンダ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を稼動しているシステムが多々検出された。「高」リスクレベル以上の脆弱性の約 75%がそれにあたる。また、そのうち 20%がサポート切れの OS またはアプリケーションであることが分かった。今日の攻撃で最も狙われやすいのが OS やアプリケーションにおける脆弱性である。こうした脆弱性を突くためのエクスプロイト（攻撃プログラム）はインターネット上に公開されており、誰でも入手することができる。その数も日々更新され、有名どころのデータベースには 35,000～80,000 件登録されており、エクスプロイトを利用した攻撃は全体の 6 割から多いときには 9 割も占めるとされている。

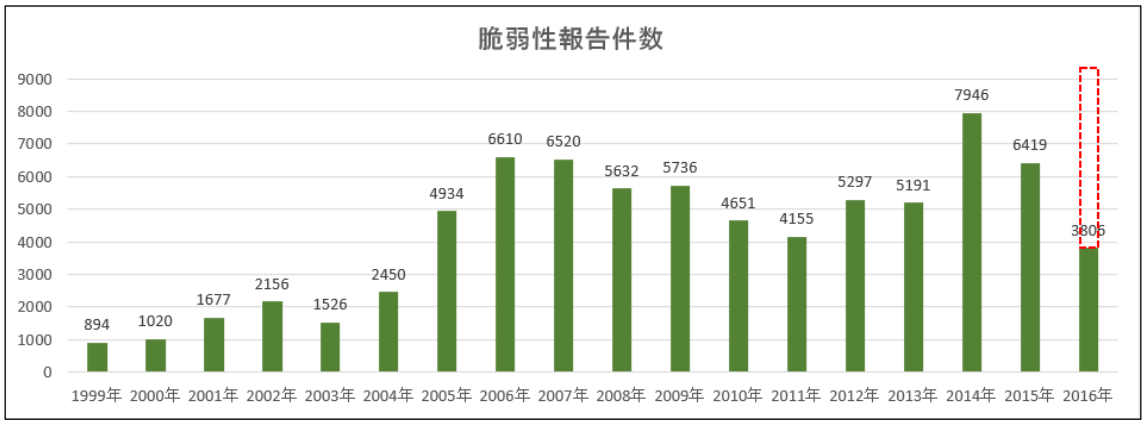
【当社ネットワーク診断で検出された「高」レベル脆弱性の内訳】



ご存知のとおり、昨今のサイバー攻撃は、ルータ、スイッチ、ファイアウォール、IDS などのネットワーク機器や、Web、DNS、メール、DB などの各種サーバ、Web アプリケーション、IoT（インターネットに接続しているモノ）というように、ありとあらゆるものをターゲットとする。

攻撃者は、これらに存在する「脆弱性」を突いて、システムに侵入したり、情報を奪取したりするのだ。こうした脆弱性は、CVE 番号が割り当てられているものだけでも既に 80,000 件近く報告されており、その数は日々増加している。

※ CVE : Common Vulnerabilities and Exposures（共通脆弱性識別子）の略称。CVE 番号は、米非営利団体 MITRE 社が管理運営を行う、一般公表された脆弱性情報を集約したデータベースに登録されている脆弱性に付与される番号。



出典：MITRE 社の CVE データベース脆弱性報告件数（http://www.cvedetails.com/browse-by-date.php）より当社作成
※ 2016 年の赤い点線部は当社予測

ところで、サイバー攻撃者はどのような基準でターゲットを選定しているのだろうか。

単純に、銀行や金融機関など「お金」に関連する業種、もしくはクレジットカードを大量に取り扱う企業。あるいは、知名度が高い大手企業を狙えば、リターンも高いだろう。また、エンドユーザ個人をターゲットにする場合は、企業役員、富裕層、著名人、あるいは複数のシステムにアクセスできる IT 管理者などが、狙われやすいと考えられる。

しかし、こうした考えは必ずしも正しいとはいえない。なぜなら、サイバー攻撃者の大半は、ターゲットを選定する上で、さほど「選り好み」をしないものだからだ。もちろん、前述のようなターゲットは、攻撃が成功した場合には得るものが大きいだろう。だが、実際に攻撃が成功する確率は低いのではないだろうか。であれば、よりセキュリティが甘いと思われる小さな組織等のほう

が、得られる利益が少ないとしても、攻撃が成功する確率が高い分、良いターゲットといえるかもしれない。

実際、攻撃者の多くが狙うのは「簡単に攻撃できそうな相手」、つまり情報セキュリティ対策が磐石でない組織や、セキュリティに関する意識または知識の低い層である。こうしたターゲットは「Low Hanging Fruit（低い位置になっている実：手を伸ばすだけで容易につかみ取ることができる簡単なターゲットという意）」と呼ばれ、攻撃者にとって、少ない労力で攻撃を成功させることができる格好の“獲物”なのだ。

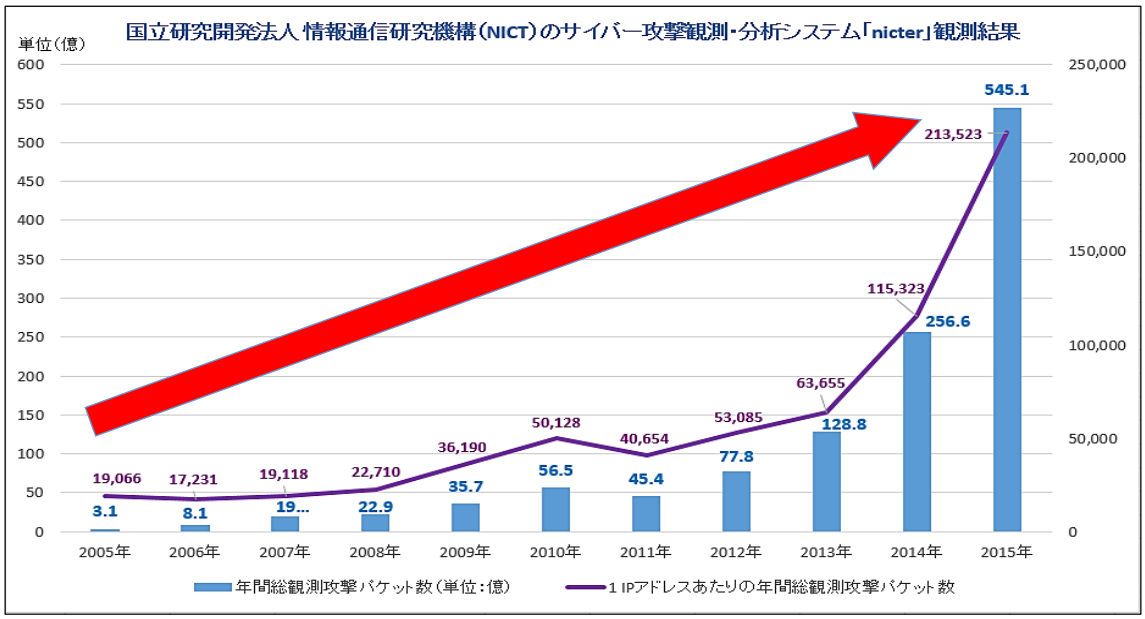
サイバー攻撃において、ターゲットの選定方法や理由は様々あるだろう。特定の企業やユーザを執拗に狙う攻撃者もいるし、その日の気分で、例えばサイコロを振ってターゲットを決める攻撃者もいる。しかし、一ついえることは、「**誰であろうと、どんな組織であろうとサイバー攻撃のターゲットになり得る**」ということだ。まず自分自身、そして自組織がサイバー攻撃にあう可能性があるということをきちんと認識することが必要である。

かつて日本は、「言語の壁」に守られてきたおかげで、海外諸国に比べサイバー攻撃の被害は限定的だった。しかし、近年は日本語のスパムメールやフィッシング詐欺サイトが検出されるなど、明らかに日本を標的とした攻撃が多数確認されている。また、国内でもサイバー犯罪が次々と検挙されている。

経済産業省から発表された資料においても、「個人から重要インフラまで、あらゆる分野に対しての攻撃が増加していることが明らかとなっている[2]。今後、早急に対処しないと、被害が連鎖的に拡大し、我が国の産業基盤や個人の生活基盤が著しく損なわれるおそれ」という注意喚起が記されている。

現代において 100%安全が保証されたシステムは存在しない。しかし、脆弱性、特に外部の第三者から悪用されうる脆弱性を放置したままシステムを運用し続けることは、情報漏洩や不正侵入などを誘発する恐れがあるため、危険であるし、社会的にも決して推奨されない。システムのユーザビリティを考慮して、リスクを許容することも選択肢の一つではあるが、その際にはリスクが顕在化した場合の対応策がきちんと整備されていることが重要である。

[2] 経済産業省「セキュリティ人材の能力評価を巡る 現状と課題」、「我が国のサイバーセキュリティ戦略」



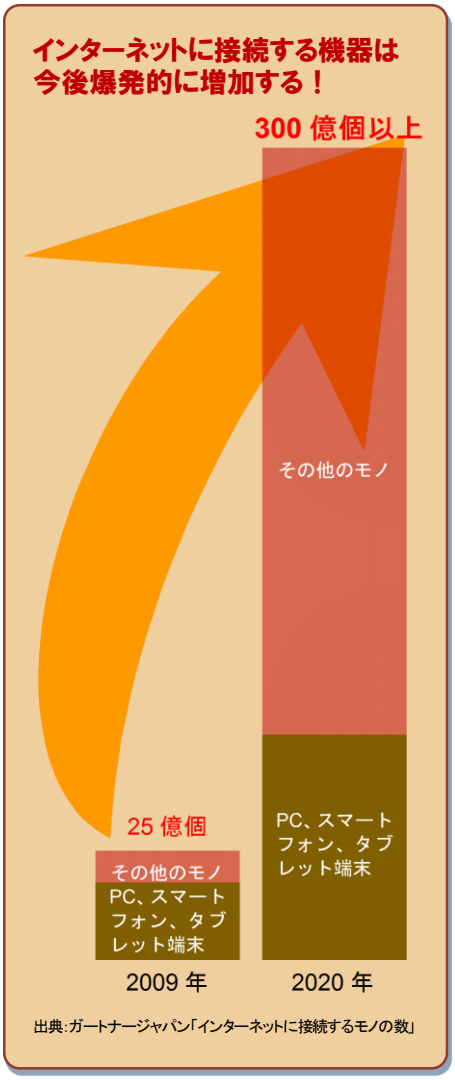
出典：国立研究開発法人情報通信研究機構（NICT）のインシデント分析センター「nicter」が観測したサイバー攻撃情報（http://www.nicter.jp/）より当社作成

近年におけるサイバー攻撃は実に多種多様である。また、攻撃手法やテクニックは常に進化し続けている。そして今後も、攻撃はますます巧妙化し、ステルス性もどんどん増してゆくことだろう。

歩きスマホと転ばぬ先のセキュリティ

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

「電話番号さえわかれば基本的には世界のどこからでもそのスマホの位置の特定、通話の盗聴、中断、割り込み、SMS の内容の盗み見、SNS の乗っ取りが可能」と聞いたら、皆さんどう思うだろうか。Internet of Things（IoT）の呼称が出て来て久しいが、「何でもインターネットに乗せてしまおう」というこの動きをセキュリティの側面から見ると、現状では 2 つの顕著な現象が起きているように見える。ひとつは「既にインターネットに接続されている機器のお粗末なセキュリティの露呈」、もうひとつは「インターネットに乗せたことでこれまで攻撃者の手が届かなかったプロトコルに攻撃が及ぶ」という現象だ。

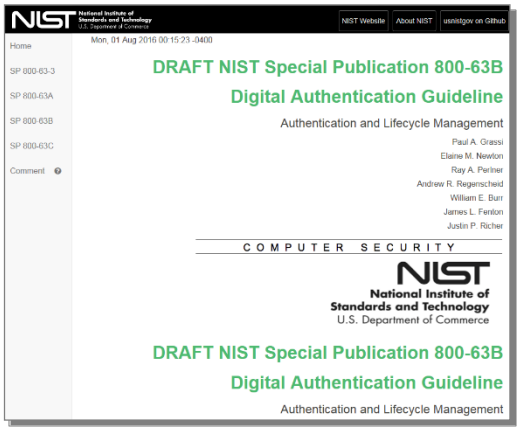


前者の例としてはプリンタ、モバイルルータ、監視カメラ等の脆弱性を持った機器が挙げられる。実際、インターネットに接続された脆弱性を持った機器がウイルス感染し、他所への攻撃の踏み台として使われていた等の報道は後を絶たない。これは製造側もユーザもリスクをよく考えずに「とりあえずインターネットに繋げて機器を使えるようした」結果と見ることができる。「安全に使える」という要件を考えると、脆弱性が見つかった際に「遠隔アップデート」ができるとか、強固な認証でなりすましを防ぐとか、操作内容を漏らさないために経路暗号化をするなどの必要な施策が整っていなかったのだ。これから IoT を考える際にはそれらの施策は必須となる。本当に安全に使おうとするなら PC の OS やアプリケーションと同じようにアップデートもできなければいけない。しかも遠隔操作で。

後者の例としては、1970 年代に作られた System Signal7（SS7）という、もともとは電話交換機間の通話制御のためのプロトコルが挙げられる。Voice over IP（VoIP）という流れに乗っ

て SS7 も SCTP/IP というプロトコル（UDP/IP や TCP/IP と同じトランスポート層のプロトコル）を使って IP ネットワーク上でやり取りされるようになっている。ちょっと知識のある方であれば、電話網（PSTN）と IP 網を結ぶ機器（IP-PBX）という存在が思い浮かぶだろう。冒頭に挙げた事象はこの SS7 を用いた攻撃例と考えられる。ネット上には SS7 を利用して SNS のアカウントを乗っ取る実演動画も掲載されている（「Hackers Can Steal Your Facebook Account With Just A Phone Number」）[3]。この攻撃に必要なものは基本的に交換機の代わりに SS7 プロトコルを送受信できる機器だ。多くのキャリアで通話の通信のベースが IP 化されているため、攻撃に用いる機器も従来と比較すると安価で済み、その最低費用は現在 15 万ドルほどと言われている。SS7 を用いて盗聴するサービスも各国のスパイに対して 2,000 万ドルで販売されているという報道もある（「SS7 Attack | Hacking Facebook Logins | June 2016」）[4]。意思とお金があれば悪用できる状況にある。

この事態を SS7 の側から見ると、コモディティ化した IP 機器で通信基盤をまかなった結果、攻撃側も容易に機器を入手できるようになり攻撃のコストが下がり、さらに交換機網自体に攻撃を受けやすい側面が形成されてしまったということになる。



出典：NIST「DRAFT NIST Special Publication 800-63-3　Digital Authentication Guideline」

最近 Public preview になった米国政府標準 NIST SP800-63-3（63B）の草稿[5]には「SMS は認証に用いるべきではない」という一文が見られる。VoIP という文字列も見えるが、その裏には「SMS は SS7 を使って送られる」という事実がある。盗聴されかねないのだ。

以前から『スマホをベッドルームに持ち込んではいけない』とは言われてきたが、その理由は不眠を防ぐこととされていた。だが SS7 の脆弱性とその悪用の可能性を目の前に見せられてしまうとその理由は大きく変わりそうだ。この悪用を防ぐにはキャリアの持つ数多くの交換機で不要な signal をフィルタする等の悪用対策が必要になる。全世界の新旧取り混ぜた交換機でそれを実施するのは困難だろうが、少なくともこれから導入されるものに関しては悪用防止の機能を入れないわけにはいかないだろう。もちろん UDP

[3] http://www.forbes.com/sites/thomasbrewster/2016/06/15/hackers-steal-facebook-account-ss7/#659fb5768fa7
[4] https://www.youtube.com/watch?v=XZuHuWWA9Yo
[5] https://pages.nist.gov/800-63-3/sp800-63b.html

と同様に SCTP の DTLS（経路暗号）化も考えるべきである。

これらの問題はまだまだ認知度が足りず、下手をすると携帯キャリアの関係者でさえほんの一握りしかその内容を知らないかもしれない。この脆弱性が指摘され始めたのは 2014 年 12 月ドイツでの学会発表であるが、本日現在 SS7 を使った abuse についての対策をネット上で明らかにしている国内キャリアは存在しないようだ。1970 年代に設計された SS7 にはユーザ認証の仕組みすらない。同じように「従来からあるものをとりあえずインターネットに接続」した結果、攻撃が可能になった例には「自動車」がある。こちらも元 NSA 職員によって全てのコントロール（アクセル/ギア/ブレーキ/ステアリング等）を奪われる実演動画（「Hacking a Car with an Ex-NSA Hacker: CYBERWAR (Clip)」）[6]がネット上に公開されている状況だ。こちらは制御用のプロトコル自体が IP ネットワーク上に乗った訳ではないが、クルマの制御に使われている CAN という閉じたパケット交換網に繋がっているコンピュータが、インターネットと接続したことで脆弱性を突かれて乗っ取られ、結果的にインターネット側からの操作で CAN に制御パケットを送れるようになったことが原因と考えられる。

これらの事象からわかることは、例えば従来からある機器をインターネットに繋ぐ際、あるいは、従来からある通信プロトコルを IP（インターネットプロトコル）上に乗せる際には「インターネットに繋ぐことを前提にセキュリティを最初から設計し直す」という覚悟が必要になるという事実だ。それは簡単なことではないし、場合によっては許容できないレベルでコスト上昇を招くかも知れない。だが、そこで手を抜くと文字通り致命的な結果になりかねないことも知っておかなければならない。

世界の電子メールのサーバ間送受信の経路暗号化率がここ数年でほぼ 0 からあっという間に 8 割を超えたり、その経路暗号化のための鍵交換プロトコルが「Perfect forward secrecy」（後から経路暗号化用の共有鍵が漏れても暗号化された通信を復号できないという要件）を意識したものに急激に変化したのと同じで、一般のユーザが知っていようがいまいが一気に変化や対策は進む。ただし、それは一般ユーザが変化や対策が必要になった理由を知らなくて良いということではない。悪用の実態やどんな対策が必要なのかは全ユーザに共有されるべき知識である。せっかく対策がしてあっても、ユーザがその対策を使う意味をわかっていないとセキュリティの根幹を揺るがしかねない。いつも持ち歩くスマホひとつ取ってもまだ問題は残っている。その上 IoT を進めるということは、身近なところまで IoT 機器が入り込むために、ユーザがしっかりとそれらのセキュリティを認識しなければならなくなる、ということを意味する。やられる可

[6] https://www.youtube.com/watch?v=MeXfCNwMG64

出典：NISC「内閣サイバーセキュリティセンターから ポケモントレーナーのみんなへのおねがい♪」

能性があるということを認識しておくだけでも結果は違って来る。

これを書いている間に世間では Pokémon GO がリリースされたようだ。スマホを覗き込みながら歩く人たちが街に溢れている。内閣サイバーセキュリティセンター（NISC）がこのゲームのリリース前から注意喚起リーフレットを公開したのには少々びっくりしたが（左図）、文字通りの『転ばぬ先の杖』こそセキュリティの目指す究極の目標のひとつである。

安藤 一憲

学生時代からネットワーク/サーバ管理に 20 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の講師を勤める。
sendmail（MTA）のエキスパートとしてのみならず、EXOCET においても高い評価を受けている。

- M3AAWG メンバー
- WIDE プロジェクト研究員

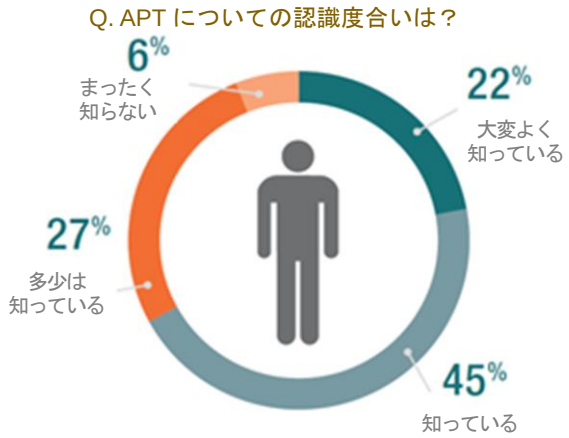
標的型攻撃に活用されるマルウェアの動向

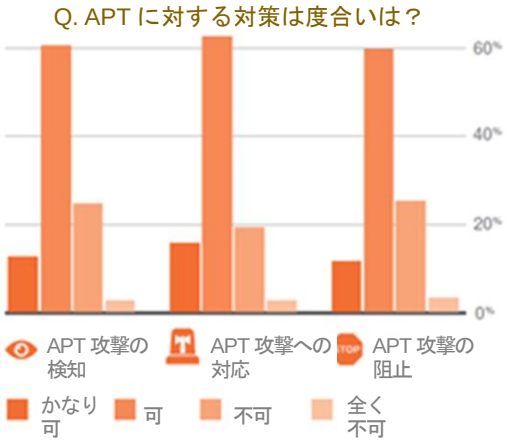
株式会社ブロードバンドセキュリティ 高度情報セキュリティサービス本部 本部長 大沼 千秋

ランサムウェアの脅威から始まった 2016 年も折り返すところまできた。依然としてランサムウェア脅威は収まることを知らず、ブラックマーケットにおいても RaaS[7]という言葉の登場に示されるように、ランサムウェアを媒介とした一大市場として確立しつつある。また、昨年発生した年金機構の標的型攻撃に代表される APT（高度で持続的なサイバー攻撃）は、以降水面下で主だった報道はなされていないが、攻撃は依然として継続しており、6 月に国内企業での大規模な情報漏洩という事故が発生したことは記憶に新しいところだ。

これらの攻撃でしばしば活用されるものが、悪意のあるプログラム「マルウェア」である。マルウェアは、いわゆる攻撃ツールで自動的に生成し、配布することが一般的であり、例えば 2015 年から 2016 年 6 月は、AnglerExploitKit という攻撃ツールがはびこっていた。この攻撃ツールを使用するとマルウェアの「亜種」は容易に生成することができる。こういった背景もあり、従来まで主流であったパターンマッチング型のウイルス（マルウェア）対策ソフトウェアではもはや追いつかなくなってきていると、一昨年前から言われ続けている。攻撃ツールにもトレンドがあり、前述の AnglerExploitKit はロシア国内の開発団体が摘発され、今後姿を消す見込みだ。ロシア当局では、国内のサイバー攻撃グループのテイクダウン作戦を推進しており、攻撃グループの主流もロシアからブラジルへ推移している傾向が見られる。一方で、ブラジ

◆ APT（標的型攻撃）に対する世界の企業の認識





出典:ISACA「2015 Advanced Persistent Threat Awareness - Third Annual」

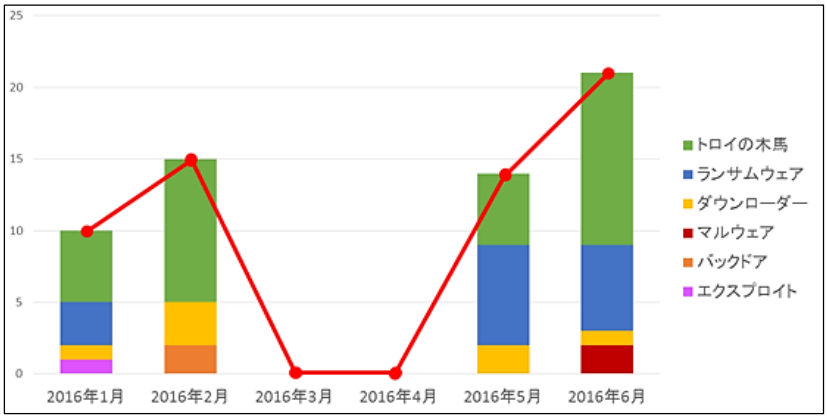
[7] Ransomware as a Service

ル発の攻撃グループから Rig、Neutrino といった新手の攻撃ツールが台頭してくるものと考えられる。

マルウェアは、感染する際にオペレーションシステム（OS）や、ソフトウェアの脆弱性を悪用することがほとんどである。代表的な攻撃手段が、ドライブバイダウンロード攻撃（Drive By Download）である。この攻撃は、Web サイトをブラウザで閲覧しただけで感染してしまうものであり、ほぼ確実に何らかの脆弱性を悪用しているといえる。したがって、脆弱性が存在する OS、アプリケーションを使用していると、常にマルウェアの脅威にさらされ続けていることになる、と言っても過言ではない。

◆ 2016 年上半期　マルウェア動向の例

下グラフは、ある組織に対して送信されたマルウェアの数と種類を分類したものである。トロイの木馬、ランサムウェアが目立つことや、時期をおいて活動が再び活発になる傾向があることがわかる。

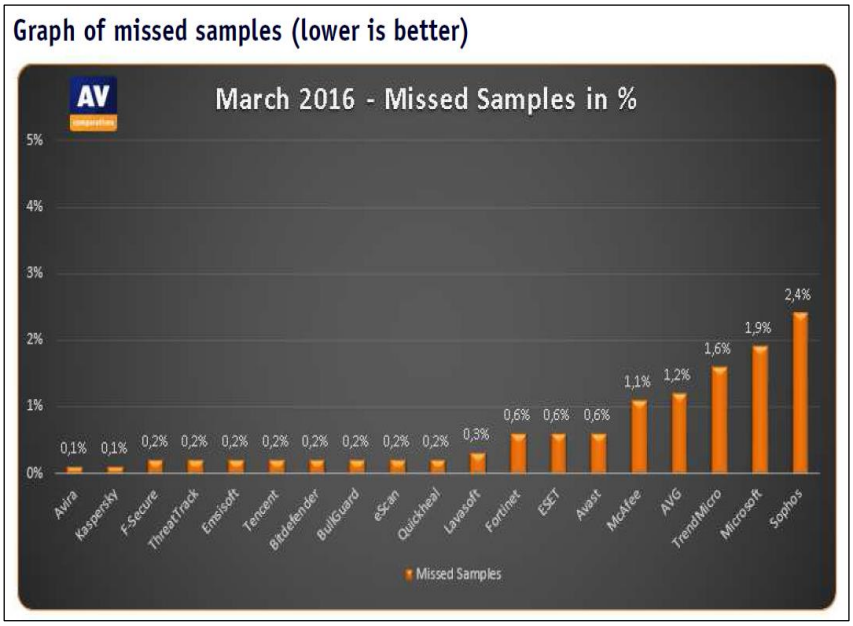


当社セキュリティオペレーションセンター調べ

また、ランサムウェアにも一つの傾向が見受けられる。ランサムウェアには一定期間大量にメール添付等で配信され、その後一定期間の収束期を経てまた増加するというパターンが見られる。これは、攻撃者がランサムウェアを配信するための情報としてメールアドレスを収集している期間が存在し、インターネット上のボットネットがアドレス収集を優先して実施する期間があるためと推測される。

◆ パターンマッチング型のマルウェア検出における漏れ率

マルウェアが検出できなかった割合を製品別に表したグラフ（棒グラフが低いほど検出漏れが少ない）。
検出漏れは、最多でも 2.4%にすぎないため、最低限、既知の脆弱性に対する対策は有効であることがうかがえる。



出典：AV-Comparatives GmbH「Anti-Virus Comparative - File Detection Test - March 2016」

品は多々存在する。もちろん、それらを有効活用することはセキュリティ強化に必要なことと言える。その一方で、ランサムウェア、標的型攻撃のためのマルウェアが狙う脆弱性は、エンドポイント、システム構成機器に存在するものであり、本質的な対策の一つとして脆弱性対策を常に念頭に置かなければならない。もちろん、0 Day 脆弱性のように未知の脆弱性については対策に限度があるものの、それ以上に、実際に発生している被害の実情は、既知の脆弱性を悪用されたケースが多いといえる。

したがって、自社のシステムの脆弱性の可視化、システムコンポーネントにおける堅牢化（ハードニング）を実施することが肝要である。

大沼 千秋

顧客向けアプリケーション開発、ISP 向けのネットワーク構築・運用管理の実績多数。当社脆弱性診断サービス立ち上げ時の主要メンバーとして、サービスの確立に貢献。豊富な実績を生かし、セキュリティコンサルタント、セミナー講師としても精力的に活動している。

- CISSP（Certified Information Systems Security Professional）取得
- PCI SSC 認定オンサイト評価人（QSA）
- テクニカルエンジニア（NW）
- JCDSC QSA 部会メンバー

◆ 日本でもこんなに多くの情報セキュリティ攻撃が！

2015 年下半期だけでこれだけの事件が発生。しかもこのように報道された事件は、**氷山の一角にすぎない**といわれている。もはや対岸の火事ではない。

組織名	日	インシデント
日本年金機構	6/1	標的型メールによるウイルス感染により、年金情報 125 万件が流出
富山大学	6/7	サーバが不正アクセスを受け海外の攻撃への踏み台に
石油連盟	6/9	標的型メール攻撃による情報流出
国立情報学研究所	6/9	サーバが不正アクセスを受け海外の攻撃への踏み台に
東京商工会議所	6/10	標的型メール攻撃による個人情報流出
健康保険組合連合会等	6/13	PC がウイルス感染。情報流出は確認されず
独立行政法人国際協力機構	6/16	標的型メールによるウイルス感染。情報流出は確認されず
一般財団法人海外産業人材育成協会	6/17	標的型攻撃によりウイルス感染
中間貯蔵・環境安全事業株式会社	6/17	サーバに不正なアクセス。情報流出は確認されず
全国健康保険協会	6/18	PC が不審な通信。情報流出は確認されず
香川県	6/18	不正アクセスでメールマガジン登録者 3,250 名が削除
新潟県	6/19	水飲み場型でのウイルス感染。情報流出は確認されず
香川大学付属病院など	6/19	PC がウイルス感染。情報流出は確認されず
五島市	6/21	Web サイトが改ざんされ、一時閉鎖
早稲田大学	6/22	標的型メール攻撃により個人情報 3,300 人分が流出
徳島大学	6/23	電子会議システムが不正アクセスされ、踏み台に利用
法務省	6/26	PC が不審な通信、ウイルスに感染した疑い
阪神高速道路株式会社	7/4	Web サイトに不正アクセスを確認し公開を一時中止
ホテルグランドヒル市ヶ谷	7/7	PC がウイルス感染。情報流出をしたおそれ
環境省	7/11	PC がウイルス感染。情報流出は確認されず
セブン銀行	7/14	DDoS 攻撃によりインターネットバンキングが利用不可
愛媛大・福岡大など	7/14	攻撃によりメールマガジンの管理アカウント等が流出
東京大学	7/16	標的型メール攻撃により氏名等 3,6 万件が流出
厚生労働省（ハローワーク）	7/18	事務用 PC がウイルス感染。情報流出は確認されず
東京都	7/21	水飲み場攻撃によりウイルス感染。流出は確認されず
内閣府	8/4	メールの管理アカウントが乗っ取られ 2 万件を送信
科学技術振興機構	8/8	PC がウイルス感染。情報流出のおそれ
国土交通省（琵琶湖河川事務所）	8/11	Web サイトに脆弱性が見つかり、サイトを一時閉鎖
関西広域連合	8/18	Web サイトが改ざん。情報流出は確認されず
日本政府観光局、成田国際空港など	10/10	DDoS 攻撃により Web サイトが閲覧できない状態
毎日新聞社	11/4	DDoS 攻撃により Web サイトが閲覧しにくい状態
東京オリンピック・パラリンピック組織委員会	11/6	DDoS 攻撃により Web サイトが閲覧できない状態
日本経済新聞社	11/12	DDoS 攻撃により Web サイトが閲覧しにくい状態
東京ガス オートサービス	11/14	不正アクセスにより、顧客情報 4,400 人分が流出のおそれ
厚生労働省	11/24	DDoS 攻撃により Web サイトが閲覧できない状態
町田市	12/8	PC がランサムウェアに感染。他への影響はなし
安倍首相個人 HP	12/10	Web サイトが閲覧しにくい状態
堺市	12/14	職員が全有権者 68 万人分の個人情報を民間レンタルサーバに公開状態で掲載し、外部にデータが流出していた
太地町	12/18	DDoS 攻撃により Web サイトが閲覧しにくい状態
日本郵政	12/19	日本郵政を名乗る不審メールが出回っていると発表

出典：NISC「2015 年下半期情報セキュリティ事件（報道ベース）」より抜粋

カテゴリ別の脆弱性検出状況

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　診断サービス部

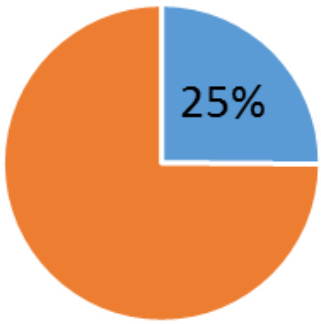
当社では、検出された脆弱性を対象システムに応じて以下のカテゴリに分類している。

	カテゴリ
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
ネットワーク診断	通信の安全性に関する問題
	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
	不適切な設定に関する問題

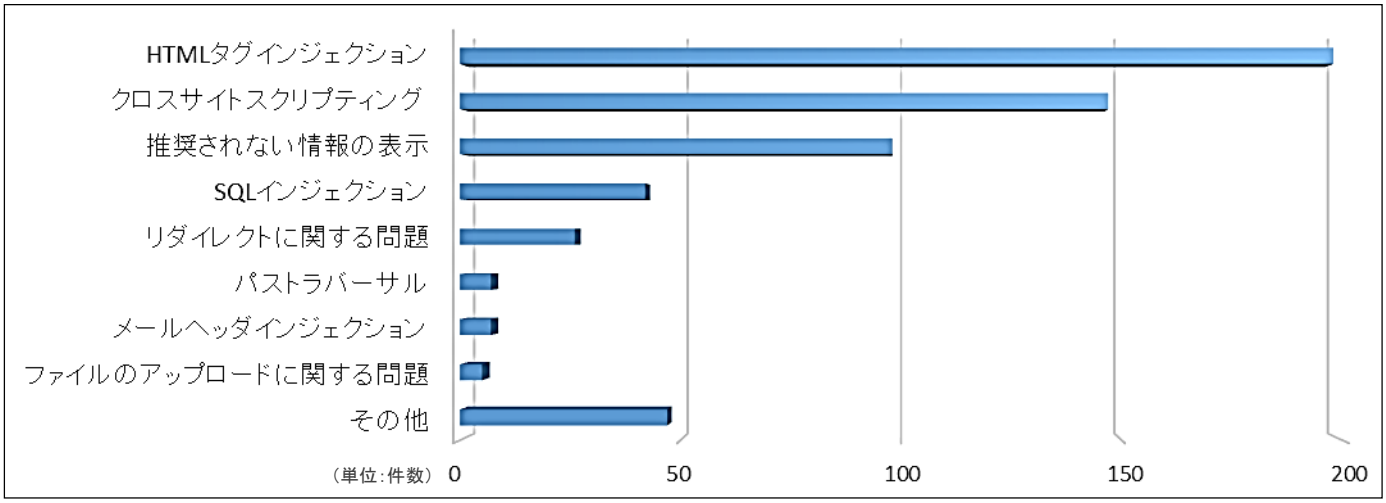
【Webアプリケーション診断】
入出力制御に関する問題

システムに対してユーザが何らかのデータを入出力する場合、そこで悪意のあるデータの入出力を行うことによってシステムに不正な動作を起こさせることが可能となる。当社の診断ではこのような入出力制御に関する脆弱性は全体の 25%のシステムにおいて見られた。

【入出力制御に関する問題の検出割合】



【入出力制御に関する問題の検出項目】



当社の診断では主に上記のような問題が検出されている。特に注目すべきは次の項目である。

- **SQL インジェクション**
- **クロスサイトスクリプティング（XSS）**
- **HTML タグインジェクション**
- **OS コマンドインジェクション**

脆弱性項目別に見ると、「インジェクション攻撃」、中でも「HTML タグインジェクション」と「クロスサイトスクリプティング」だけで、入出力制御に関する問題の過半数（58%）を占めている。いずれの脆弱性も、ユーザから入力された値に対して適切な検証や処理を行わずそのまま出力しているサイトで見られ、これらを悪用されると表示ページの改竄、Cookie や認証情報、その他機密情報の窃取、悪意のあるサイトへの転送、悪質なプログラムの実行といった被害につながる危険性がある。また、セッションハイジャックやマルウェア感染（ドライブ・バイ・ダウンロード攻撃）、フィッシング詐欺など、様々な二次被害に発展する恐れもある。

SQL インジェクションは、OWASP Top 10 における「インジェクション攻撃」の代表的な攻撃手法であるが、当社の診断結果においては、当該脆弱性が検出された割合は入出力制御に関する問題全体の 7%であった。検出割合は比較的少ないが、攻撃を受けた際の影響として認証の回避、Web サーバと連動するデータベース内の情報の奪取・改竄、バックドアの作成など、深刻な被害につながる恐れがあるため、当該脆弱性が検出された場合には速やかに対処し、問題を解消するよう強く推奨している。

なお、グラフでは「その他」に分類されているが、インジェクション攻撃としては「OS コマンドインジェクション」も忘れてはならない。OS に対する任意の命令文を実行可能にするこの脆弱性が検出されることは流石にまれだが、ゼロではない。ちなみに OS コマンドインジェクションが検出されたシステムは、ご想像のとおり脆弱性のデパートのようで、必要なセキュリティ対策がほぼ実装されていないに等しかった。まるで「攻撃してほしい」といっているようなものだ。

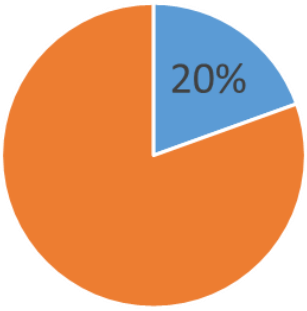
近頃では、自称ホワイトハッカー（Ethical Hacker）を名乗るグループが、セキュリティの低い Web サイトの情報をまとめたデータベースやブログなどを、インターネット上に数多く公開している。例えば、中国の「WooYun.org」などは記憶に新しい。既にこのサイトは閉鎖されているが、2016 年 2 月頃から日本の Web サイトも多く掲載されるようになっていた。中には、日本人なら誰でも知っているような企業の Web サイトに SQL インジェクションの脆弱性が存在する、といった情報もあり、掲載された企業にとっては迷惑を超えて大きな脅威である。

Web アプリケーションのセキュリティ強化において、外部入力値の検証および出力時の適切な処理（無害化）は基本中の基本であり、かつ必須であるといえる。

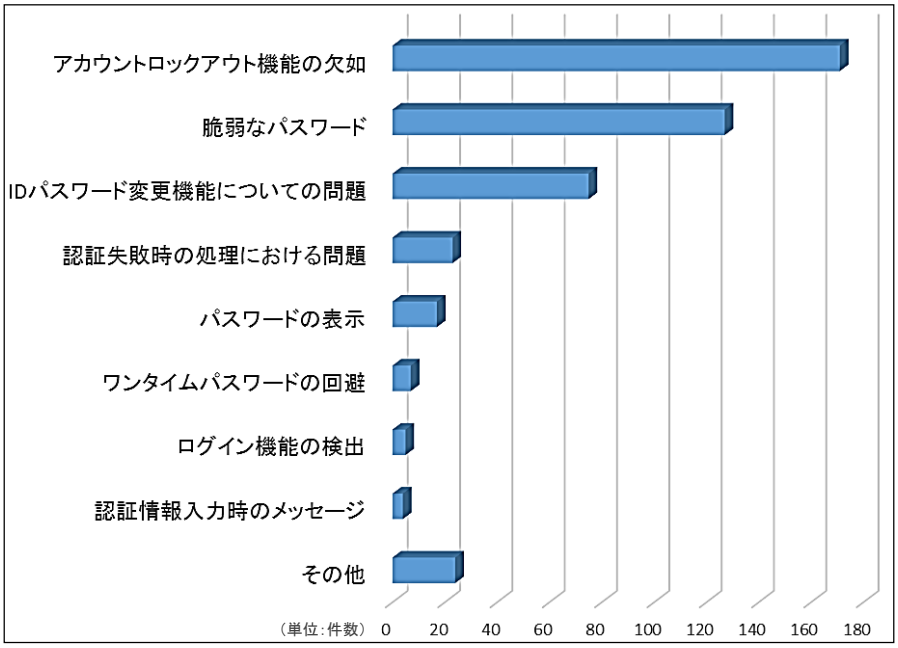
【Webアプリケーション診断】認証に関する問題

認証機構にセキュリティ上の問題が存在すると、攻撃者に悪用された場合に大きな被害につながることがある。特に、管理者権限を奪取されて不正アクセスが行われると、その影響は甚大なものになる。当社が実施した診断では、対象システム全体の約 20%において認証に関する問題が検出された。

【認証に関する問題の検出割合】



【認証に関する問題の検出項目】



認証に関して、特筆すべきはパスワードの強度に関する問題である。認証情報、特にパスワードは、機密エリアに入るためのいわば「鍵」であり、本来入ることが許可されていない者の手にこの鍵が渡ってしまうと、守りたい情報が守れなくなってしまうのは言うまでもないだろう。

それでは、実際の状況はどうか。当社 Web アプリケーション診断では、対象システムのうち約23%において、情報セキュリティ上「弱い」とされるパスワードの使用が許容されていた。中には、最小構成文字数 1 文字、最小構成文字種 1 種類（例：1 や a）といった極めて脆弱なパスワードが設定可能なシステムも確認された。1 文字、1 種類のパスワードはもはや論外だが、例えば「1234567」のような数字のみで構成されたパスワードでも一瞬でクラックされてしまう。

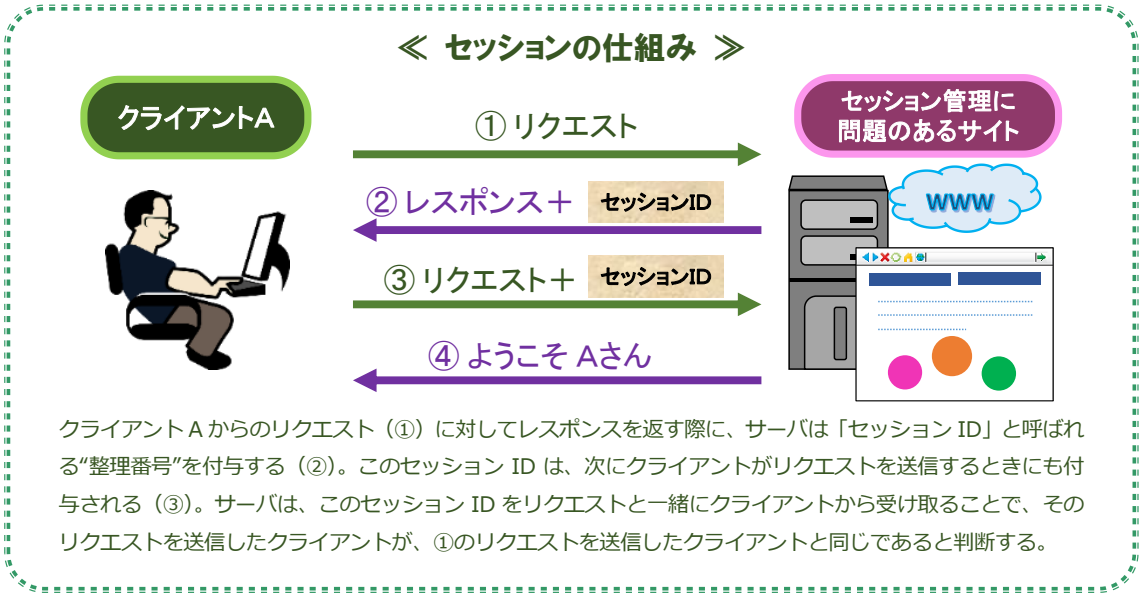
当社では、最小構成文字数 8 文字、最小構成文字種 3 種類から成るパスワードの利用を推奨しているが、近頃情報セキュリティ専門家の間では、14 文字、4 種類から成るパスワードを推奨する動きもある。ただし、複雑だから良いというわけでもない。というのも、あまり複雑なパスワードを設定すると、メモに書き残すなどして、かえって漏洩の危険性を高めるという結果を招きかねないからだ。守るべき情報の機密レベルにあった適切なパスワードを使用することが重要だといえる。

パスワードの強度が十分か、またそのパスワードをクラックするにはどれくらいの時間がかかるかを測定するツールは無料で数多く公開されているため、一度確認してみるのもよいだろう（ただし、確認に使用したパスワードを実際に設定することは避け、別の文字に置き換えることを推奨する）。例えば、米企業 BetterBuys が公開しているパスワード強度確認ツールは、現時点での強度から、2020 年における強度予想まで計算することが可能だ。

また、その他認証に関する問題として、一定回数認証に失敗した場合にアカウントを利用できないようにする「アカウントロックアウト」機能を実装していないケースが、診断対象システムの約 31%で検出された。ロックアウトがかからないと、繰り返し無限にログインを試せるため、パスワード解析ツール等で総当り的にログインを実行された場合、攻撃者が正しいパスワードを引き当ててしまう危険性がある。よって、ユーザビリティを考慮して敢えてロックアウト機能を実装していないシステムもあったが、情報セキュリティの観点からは推奨されない。

【Webアプリケーション診断】セッション管理に関する問題

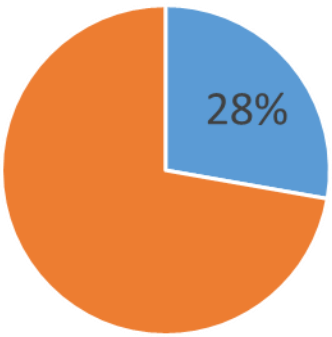
HTTP では、Web ブラウザと Web サーバは下図のようにして通信を行う。クライアントからのリクエストに対してサーバがレスポンスを返して通信を行い、最後に接続を切断するまでの一連の流れをセッションという。



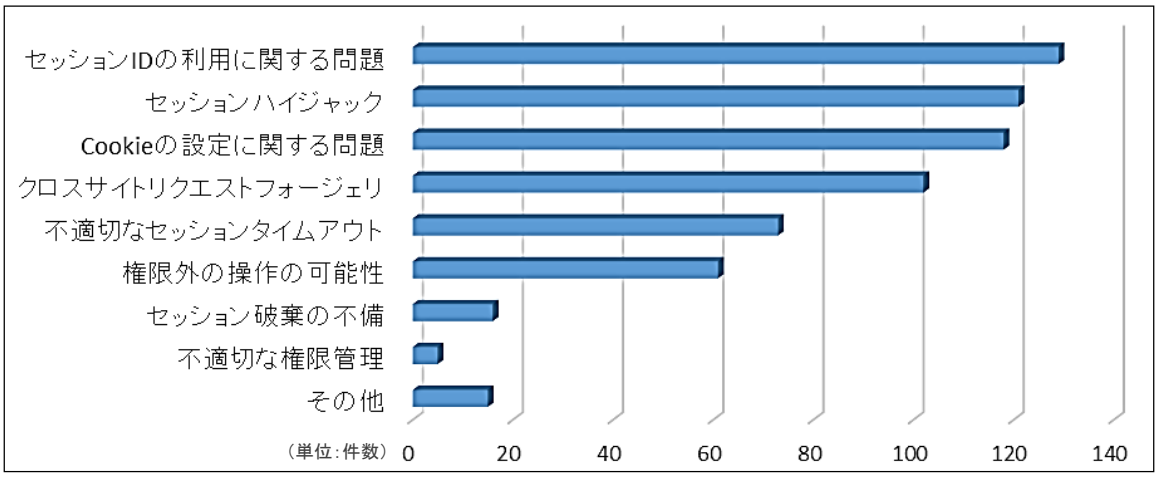
クライアント A からのリクエスト（①）に対してレスポンスを返す際に、サーバは「セッション ID」と呼ばれる"整理番号"を付与する（②）。このセッション ID は、次にクライアントがリクエストを送信するときにも付与される（③）。サーバは、このセッション ID をリクエストと一緒にクライアントから受け取ることで、そのリクエストを送信したクライアントが、①のリクエストを送信したクライアントと同じであると判断する。

セッション管理が適切に実装されていないことにより、第三者にセッションを乗っ取られる被害が発生する可能性がある。当社による診断の結果、セッション管理に関する問題は、対象システム全体の約 28%において検出された。

【セッション管理に関する問題の検出割合】



【セッション管理に関する問題の検出項目】



脆弱性項目別に見ると、上記グラフに示されるように、セッション ID の利用に関する問題が最も多く検出されている（全体の 20%）。セッション ID の管理に不備がある場合、セッションハイジャック（後述）の危険性が高まり、なりすましなどの被害につながる恐れがあるので早急に対策をとることが推奨される。

セッション管理に関する脆弱性の中で、危険性が高いものの代表が「セッションハイジャック」と「クロスサイトリクエストフォージェリ（CSRF）」である。当社が実施した診断ではセッションハイジャックは全体の約 18%、クロスサイトリクエストフォージェリは全体の約 16%で検出されている。

セッションハイジャックとは、正規ユーザが第三者にログイン済みのセッションをのっとられる攻撃である。攻撃が成功した場合、個人情報の漏洩やユーザ権限での処理の実行など重大な被害につながる可能性が高い。

クロスサイトリクエストフォージェリとは、ユーザが正規サイトから悪意のあるサイトへアクセスして操作を実行した結果、正規サイトにおいて意図しない処理を実行させられる攻撃である。この攻撃が成功した場合、不正サイトへの誘導や不正な処理を大量に行うことによる DDoS 攻撃などの被害につながる可能性がある。対策としては、送信されたリクエストが正しい画面遷移によるものであることを確認し、不正な場合には処理を実行しない仕組みを実装することを推奨している。

なお、検出率は比較的低いが重大なものとして、権限管理に関する問題がある。これは読んで字のごとく、ユーザが本来許可された権限を超えて操作が実行可能になるという脆弱性である。例えば、特定のページやコンテンツの閲覧権限のみを持つユーザが、本来自分には許可されていない情報の登録や編集ができてしまう問題がそれにあたる。ユーザのロール（役割）にあわせて「できること」を制限しているつもりが、この脆弱性があることで全く無意味になってしまう。

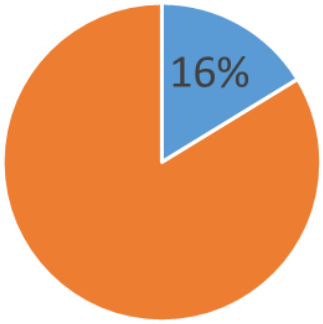
また、一般ユーザがシステム管理者ユーザになれる等、特権昇格が可能な問題が存在する場合、さらに危険性は増す。機密性や完全性が確保できなくなってしまうからだ。システムの設定を変更されたり、機密情報を根こそぎ奪取されたりする等、その被害範囲は計り知れない。

Web サイトが改竄被害に遭ったケースの多くは、最終的に管理者権限が乗っ取られるという被害につながっている。これにより、攻撃者は Web サイトをマルウェアに感染させたり、別の悪質なサイトへユーザを誘導する不正リンクを埋め込んだりと、被害を受けたサイトだけでなく、そのサイトにアクセスしたユーザにも深刻な影響が及ぶ。さらに、操作の痕跡を消すこともできる可能性があるため、サイト管理者は自身のサイトが攻撃被害を受けていることすら気付けない場合もある。よくニュースなどで、大量の個人情報やクレジットカード情報などが漏洩した事件が取り上げられ、最初に攻撃を受けてから発覚するまでに何年も経過していた、という話を耳にするが、上述のようなことが原因の一つとなっている。

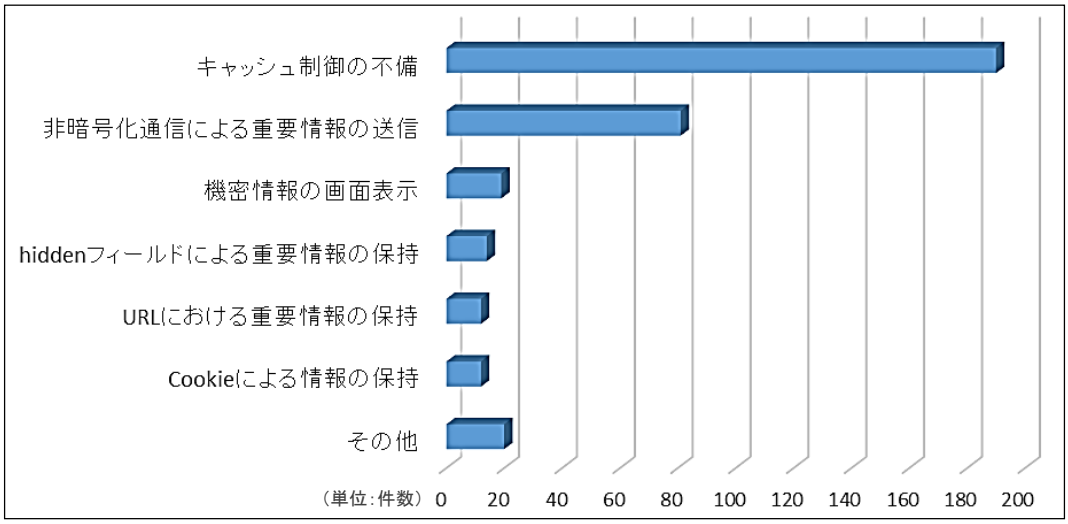
【Webアプリケーション診断】重要情報の取り扱いに関する問題

ユーザ ID 等の認証情報、住所やクレジットカード番号等の個人情報といった重要情報の取り扱い方法に問題があると、情報漏洩により組織の信用を失う深刻な事態に陥る可能性がある。当社診断では、このような問題は全体の 16%に検出された。

【重要情報の取り扱いに関する問題の検出割合】



【重要情報の取り扱いに関する問題の検出項目】



重要情報の取り扱いに関する問題における検出状況は、「キャッシュ制御の不備」が 53.5%、次いで「非暗号化通信による重要情報の送信」（21.4%）で、この両者でほぼ 7 割を占める。そのほかには、「機密情報の画面表示」（5%）、「hidden フィールドによる重要情報の保持」（4%）、「URL における重要情報の保持」（3.4%）といった問題が検出されており、多くの企業においてキャッシュ制御や通信の暗号化に対する意識が不足している状況が浮き彫りになった。

「非暗号化通信による重要情報の送信」が検出されたサイトで比較的多いのが、「サイト全体は暗号通信であるにもかかわらず、認証画面とその後の遷移において非暗号化通信（http）でのアクセスが可能」なケースである。非暗号化通信でアクセスした場合、通信の盗聴などにより、個人情報や認証情報といった重要情報を第三者に取得される可能性があるため、必要なフォームを暗号化通信としただけで安心せず、認証前後のアクセス検証（非暗号化通信でアクセスする経路は排除されているか否か）を実施することが肝要だ。

重要情報が漏洩するそもそもの原因は、情報の取り扱いにおける問題だ。「URL における重要情報の保持」もその一つである。例えば、URL 内にセッション ID を保持している場合、ユーザがその URL を第三者に不用意に開示してしまうと、セッション ID が容易に取得され、セッションハイジャックの危険にさらされることになる。より深刻なケースでは、URL に認証情報（ユーザ ID とパスワード）を保持している、という脆弱な実装も存在する。これは、言わずもがな不正アクセスを誘発する原因となる。

なお、機密情報の画面表示といった問題も情報漏洩の原因となる。代表的なものは「ショルダーハッキング」という攻撃手法による漏洩。ショルダーハッキングとは、重要情報を閲覧もしくは入力しているユーザの肩越しから、盗み見みによって情報を奪取する攻撃のことである。ちなみに情報を盗み見られるのは、PC からだけではない。昨今におけるスマートフォンやタブレット端末の普及は著しく（右図参照）、どこへ行っても誰かしら画面を開いている状況に遭遇するだろう。そうした端末に対応した Web サイトも増加の一途を辿っており、わざわざ PC を起動しなくても様々な操作や処理が実行できる。

【普段、私的な用途のために利用している端末】

（単位：%）

	スマートフォン	フィーチャーフォン	タブレット
[日本]			
全体加重平均	60.2	41.9	19.5
20代(N=200)	87.0	20.0	19.5
30代(N=200)	73.0	31.0	25.0
40代(N=200)	60.0	42.5	21.0
50代(N=200)	54.0	47.5	18.5
60代(N=200)	35.0	62.0	14.0
[米国]			
全体加重平均	78.6	18.4	57.2
20代(N=200)	92.5	8.5	67.0
30代(N=200)	94.5	11.5	76.5
40代(N=200)	83.0	17.0	57.0
50代(N=200)	61.5	23.0	45.5
60代(N=200)	58.5	35.0	37.0
[英国]			
全体加重平均	82.3	13.9	55.6
20代(N=200)	95.5	4.5	61.5
30代(N=200)	92.5	7.5	66.0
40代(N=200)	85.0	12.0	52.5
50代(N=200)	71.0	21.5	46.0
60代(N=200)	64.5	26.0	51.5
[ドイツ]			
全体加重平均	82.3	20.2	45.8
20代(N=200)	97.5	9.5	52.0
30代(N=200)	94.0	9.0	56.5
40代(N=200)	85.5	15.5	46.0
50代(N=200)	74.0	30.0	44.5
60代(N=200)	62.0	35.5	29.5
[韓国]			
全体加重平均	96.6	7.8	34.1
20代(N=200)	100.0	3.5	31.0
30代(N=200)	97.0	7.5	43.5
40代(N=200)	96.0	9.5	37.5
50代(N=200)	97.0	7.0	30.0
60代(N=200)	91.5	12.5	24.5
[中国]			
全体加重平均	98.3	5.0	47.3
20代(N=200)	98.5	3.0	49.5
30代(N=200)	100.0	2.5	57.5
40代(N=200)	98.0	6.0	46.0
50代(N=213)	97.7	5.6	44.1
60代(N=187)	96.8	9.6	34.8

出典：総務省「IoT 時代における新たな ICT への各国ユーザーの意識の分析等に関する調査研究」（平成 28 年）

通勤時の満員電車を想像してほしい。モバイル端末の利用者全員が高いセキュリティ意識を持っている、というなら問題にはならないが、残念ながらそうではない。満員電車で周り、しかもごく至近距離に他人が大勢いる中で、平気で送金処理やネットショッピングを行う人々もいる。そ

んな状況の中、クレジットカード情報やパスワードなどがマスクされずに画面上に表示されていたら簡単に取得されてしまう。記憶力の良い人間なら、14 桁～16 桁のクレジットカード番号と有効期限をその場で覚えることはさほど困難ではない。パスワードや個人情報も同様に、容易に取得される可能性がある。近頃、いわゆるシニア世代をターゲットとしたスマートフォンが次々と販売されているが、画面や文字が大きくなれば、さぞそうした情報は盗み見やすくなるだろう。

また、特定個人情報（マイナンバー）についてはどうだろうか。当社でも、昨年末あたりからマイナンバーを取り扱うシステムの診断が増えてきているが、脆弱性が検出されたシステムは少なくない。マイナンバーが漏洩した事件は相次いで発生しており、漏洩を起こした企業には罰則が科せられるだけでなく、社会的信用を失うというリスクもついてくる。当社が診断したあるサイトでは、マイナンバーと個人情報（氏名、住所等）の一覧が不正に取得できる状態にあった。前述のショルダーハッキングの観点からも、そうした一覧が画面上に表示されている場合、スマートフォンなどで撮影されることで漏洩する危険性もある。個人情報保護委員会が策定した「特定個人情報の適正な取扱いに関するガイドライン（事業者編）（本文及び（別添）特定個人情報に関する安全管理措置）」によれば、情報システムを使用して個人番号関係事務又は個人番号利用事務を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行わなければならないとされている。上記ショルダーハッキングを防止するための物理的な安全区画の設定はもちろんのこと、情報漏洩に関しては、データの暗号化、パスワードによる保護が要求されている。

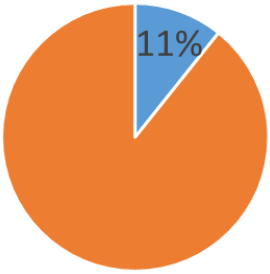
また、2017 年に全面施行となる改正個人情報保護法では、匿名加工情報取り扱い業者に対する義務、要配慮個人情報に対する義務も法制化されている。来年の全面施行にあわせ、今秋から年末にかけて、次々とガイドラインが策定される予定である。

現行のサイト構成で改正法に十分対応できているだろうか。システム構築には技術的な検討はもちろん、コンプライアンスや事業継続について十分検討する必要があることを忘れてはならない。

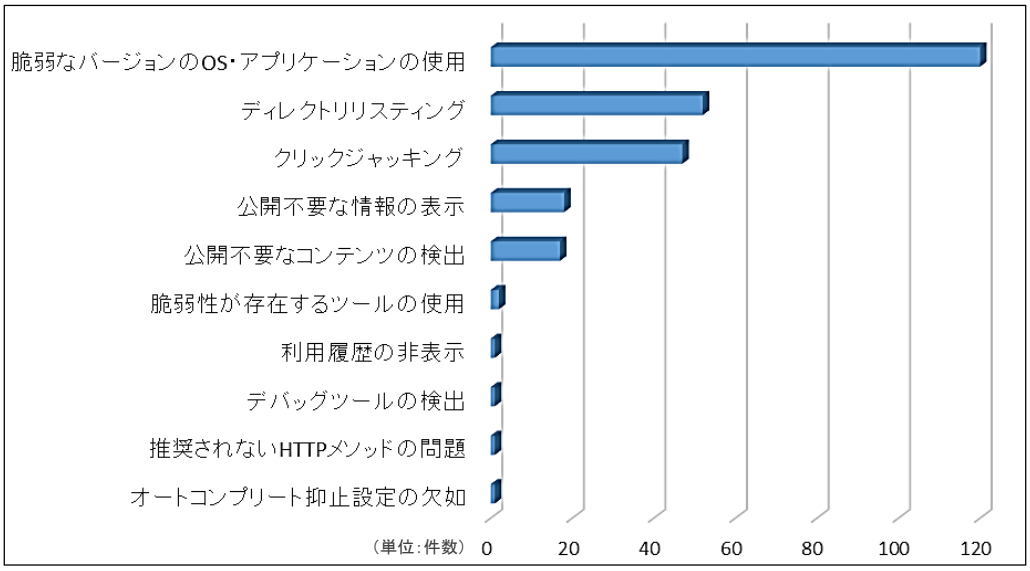
【Webアプリケーション診断】
システム情報・ポリシーに関する問題

サイバー攻撃を受けやすい状況に陥らないためには、不用意にシステム情報が外部にさらされていないか注意を払い、システムポリシーを策定して徹底することが大切である。当社の診断では、システム情報やポリシーに関する問題は全体の 11%を占めた。

【システム情報・ポリシーに関する問題の検出割合】



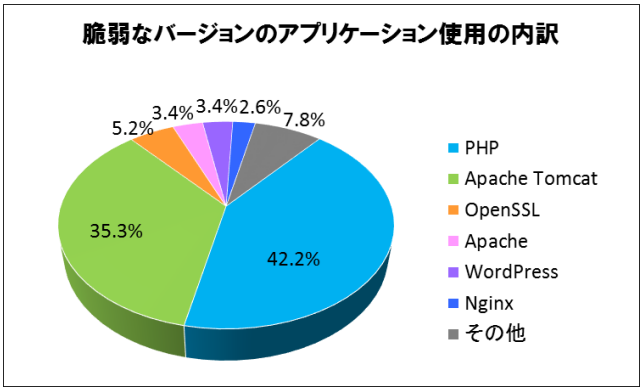
【システム情報・ポリシーに関する問題の検出項目】



システム情報・ポリシーに関しては、以下のような問題があるといえる。

- **脆弱なバージョンの OS・アプリケーションの使用**
- **公開不要な情報やコンテンツの開示**
- **ポリシーの不存在もしくは不徹底**

脆弱なバージョンの OS・アプリケーションの使用



当社診断では、既知の脆弱性がある、あるいはベンダサポートが終了しているバージョンの OS･アプリケーションを使用している問題は、検出件数全体の半分近くにのぼる。アプリケーションについてみると、特に目立つのが「PHP」と「Apache Tomcat」であり、両者を合わせると 80%近くを占める。

また、近年、ホームページの作成ツールとして組織・個人問わず非常に人気を集めている「WordPress」も、脆弱なバージョンのまま使用されることの多いアプリケーションの 1 つである。2016 年に入ってからも、WordPress の脆弱性を突かれて Web サイトが DDoS 攻撃の加害者側にされたり、プロバイダが管理者アカウントを狙った総当り（Brute-Force）攻撃を受けたり、といったサイバー攻撃が国内外で後を絶たない。「パナマ文書」で世界中の注目を集めた法律事務所「モサック・フォンセカ」の情報流出も、WordPress で使用していたプラグインの脆弱性により引き起こされた可能性があるという[8]。WordPress の特長は、単なる HTML 作成ツールではなく、データベースと連携して動作する CMS（コンテンツマネジメントシステム）を安価かつ容易に構築できる点だ。攻撃者にとって、機密情報を保持している可能性がある CMS は魅力的な攻撃対象であるし、WordPress のようなオープンソースのアプリケーションは脆弱性の有無について検証しやすいといえる。

このように、いずれのアプリケーションも、そのバージョンによっては複数の脆弱性が存在する場合があり、これらの脆弱性が悪用された場合、サービス運用妨害（DoS）、重要情報の窃取、任意のコード実行、バッファオーバーフロー等、様々な被害を受ける可能性がある。特にベンダサポートが終了したバージョンにおいては、新たに発見された脆弱性への対策が困難である。そのため、危殆化に対する対応策がなくなること、並びにそれを標的としたエクスプロイト（攻撃プログラム）が公開されることにより、攻撃者に対して無防備となる可能性がある。このため、当社では使用バージョン、および使用されているシステムの状況によっては、リスクレベルを「重大」、「高」と判断している。

各アプリケーション提供側も、脆弱性発覚の際にはすばやく反応し、脆弱性を修正したアップグレード版を発行しているので、使用しているアプリケーションのバージョン情報を常に管理し、最新バージョンへのこまめなアップデートを行うことが推奨される。

[8] https://www.wordfence.com/blog/2016/04/mossack-fonseca-breach-vulnerable-slider-revolution/

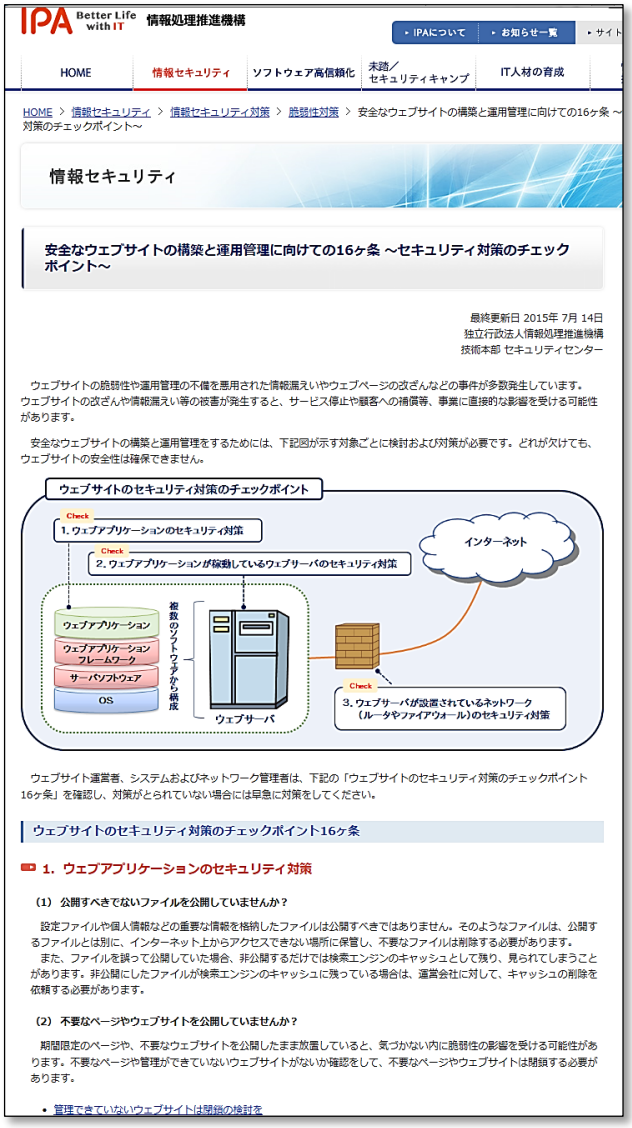
公開不要な情報やコンテンツの開示

システムに関する情報やファイルが不用意に表示されている問題である。例えば、システム内の特定のディレクトリやファイルが表示可能となっている「ディレクトリリスティング」のほか、各種アプリケーションの初期画面/管理者画面やシステム情報が表示されているケースがここに該当する。割合としては、以下の順に多く検出されている。

ディレクトリリスティング：20.0%
公開不要な情報の表示：6.9%
公開不要なコンテンツの検出：6.5%
デバッグツールの検出：0.4%

本来アクセスが制御されるべきシステム内部のファイル名、ディレクトリ構成等が表示されることや、システムに関する情報が表示されることは、攻撃者に対して有益な情報を与えることになる。万が一、他の脆弱性の存在によってシステムへ侵入された場合、さらに被害が拡大する可能性もある。

当社では、公開不要と推測させるファイルが表示されている場合、リスク「高」と判断することがある。例えば、Web サーバの挙動をコントロールする設定を記述した「.htaccess」ファイルが公開されている場合だ。数年前より、外部の攻撃者に.htaccess ファイルを改竄されて、マルウェア配布サイトやウイルス感染を引き起こすサイトへ強制的にリダイレクトさせられることで踏み台として利用される、といった被害がよく知られているためである。IPA（情報処理推進課機構）が発表している「安全なウェブサイトの構築と運用


IPA Better Life with IT 情報処理推進機構

IPAについて　お知らせ一覧

HOME　情報セキュリティ　ソフトウェア高信頼化　未踏／セキュリティキャンプ　IT人材の育成

HOME ＞ 情報セキュリティ ＞ 情報セキュリティ対策 ＞ 脆弱性対策 ＞ 安全なウェブサイトの構築と運用管理に向けての16ヶ条 ～対策のチェックポイント～

情報セキュリティ

安全なウェブサイトの構築と運用管理に向けての16ヶ条 ～セキュリティ対策のチェックポイント～

最終更新日 2015年 7月 14日
独立行政法人情報処理推進機構
技術本部 セキュリティセンター

ウェブサイトの脆弱性や運用管理の不備を悪用された情報漏えいやウェブページの改ざんなどの事件が多数発生しています。ウェブサイトの改ざんや情報漏えい等の被害が発生すると、サービス停止や顧客への補償等、事業に直接的な影響を受ける可能性があります。

安全なウェブサイトの構築と運用管理をするためには、下記図が示す対象ごとに検討および対策が必要です。どれが欠けても、ウェブサイトの安全性は確保できません。

ウェブサイト運営者、システムおよびネットワーク管理者は、下記の「ウェブサイトのセキュリティ対策のチェックポイント16ヶ条」を確認し、対策がとられていない場合には早急に対策をしてください。

ウェブサイトのセキュリティ対策のチェックポイント16ヶ条

1. ウェブアプリケーションのセキュリティ対策

(1) 公開すべきでないファイルを公開していませんか？

設定ファイルや個人情報などの重要な情報を格納したファイルは公開すべきではありません。そのようなファイルは、公開するファイルとは別に、インターネット上からアクセスできない場所に保管し、不要なファイルは削除する必要があります。
また、ファイルを誤って公開していた場合、非公開するだけでは検索エンジンのキャッシュとして残り、見られてしまうことがあります。非公開にしたファイルが検索エンジンのキャッシュに残っている場合は、運営会社に対して、キャッシュの削除を依頼する必要があります。

(2) 不要なページやウェブサイトを公開していませんか？

期間限定のページや、不要なウェブサイトを公開したまま放置していると、気づかない内に脆弱性の影響を受ける可能性があります。不要なページや管理ができていないウェブサイトがないか確認をして、不要なページやウェブサイトは閉鎖する必要があります。

- 管理できていないウェブサイトは閉鎖の検討を

出典：IPA「安全なウェブサイトの構築と運用管理に向けての16ヶ条」

管理に向けての 16 ヶ条」[9]においても、まず最初に「公開すべきでないファイルを公開していませんか？」と注意喚起している。

不用意に情報を表示して攻撃者に悪用されることがないよう、以下の対策をとることが推奨される。

- 公開不要なファイルは適切な場所に格納し、適切なアクセス制御を行う
- 不要なディレクトリやファイルは削除する

ポリシーの不存在もしくは不徹底

そもそもセキュリティポリシーが策定されていない、もしくは策定されていたとしても徹底されていないことにより、脆弱な状態になっている例がみられる。例えば、X-Frame-Options が設定されていないために、Web ページの透過表示機能を利用した「クリックジャッキング」攻撃を受ける可能性がある状態になっていたり、ブラウザの「オートコンプリート」機能が設定されたままになっていて、ログイン ID やパスワードが取得されかねない状態になっていたりするシステムが散見される。

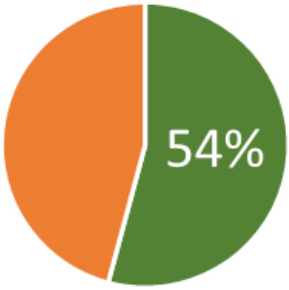
クリックジャッキング攻撃では、裏に隠されたボタンをクリックすることで、ユーザが意図しない悪意あるページに誘導され、個人情報を抜き取られたり、SNS に意図しない投稿を強いられたりする等、深刻な被害に発展する可能性がある。自組織が被害者にも加害者にもならぬように気をつけたい。

[9] http://www.ipa.go.jp/security/vuln/websitecheck.html

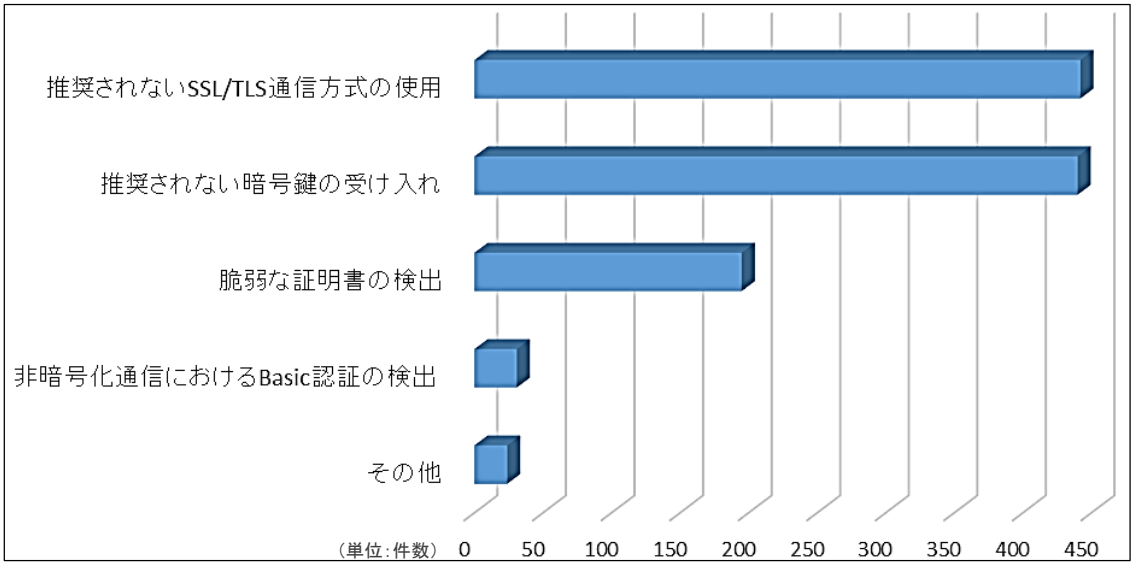
【ネットワーク診断】
通信の安全性に関する問題

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いても強度の低い暗号鍵が使用可能である等、通信の安全性に関する問題は、対象システム全体の半分以上（約 54%）で検出された。

【通信の安全性に関する問題の検出割合】



【通信の安全性に関する問題の検出項目】



「推奨されない SSL/TLS 通信方式の使用」では、その安全性が疑問視されるようになってから既に 10 年以上が経過している SSL 2.0 のほか、SSL 3.0 や TLS 1.0 といった「安全性が低い」と見做されているプロトコルの使用を許容しているシステムが多数確認された。SSL 3.0 や TLS 1.0 にはブロック暗号の CBC モードの取り扱いに関する脆弱性が存在し、「POODLE（Padding Oracle On Downgraded Legacy Encryption）」や「BEAST（Browser Exploit Against

SSL/TLS)」といった攻撃に対して脆弱である。攻撃が実際に成立するには一定の条件が必要であり簡単に実行できるものではないが、こうした状況を受け、サーバ/クライアントの主要ベンダの多くが対応を進めており、かつ、情報セキュリティのベストプラクティス（最善策）としても今後の継続利用は推奨されていないことから、これらのプロトコルは無効にすべきといえる。

また、「推奨されない暗号鍵の受け入れ」、「脆弱な証明書の検出」の問題では、悪意のある第三者に通信内容を取得、解析され、情報漏洩につながる危険性がある。なお、国内には、暗号技術の専門家が参画する CRYPTREC（Cryptography Research and Evaluation Committees）と呼ばれる、暗号の安全性を評価・監視し、暗号技術の適切な実装法や運用法を調査・検討するプロジェクト[10]があり、推奨される暗号技術の一覧を公開している。最新のリスト（「CRYPTREC 暗号リスト（平成 28 年 3 月 29 日版）」）では、ハッシュ関数 SHA-512/256、SHA3-256、SHA3-384、SHA3-512、SHAKE256 が新たに追加されている。この一覧に挙げられている推奨暗号技術は、市場における利用実績と安全性を確認したものであり、日本における「標準暗号」といってよい。自組織で使用している暗号技術と一覧を照らし合わせ、非推奨の暗号技術を使用していないか確認することを推奨する。また、CRYPTREC では「CRYPTREC Report」を毎年発表しているほか、暗号設定ガイドライン等を公表している。これらを参考に、通信の安全性確保につとめたい。

【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。

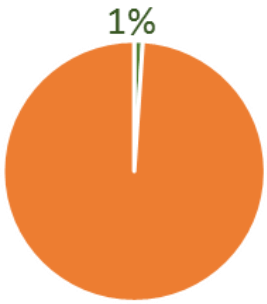
出典：CRYPTREC「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」

[10] http://www.cryptrec.go.jp/index.html

【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があったシステムは、全体の 1%だった。

【重要情報の取り扱いに関する問題の検出割合】



診断では、以下のような内容が検出された。

- システムに関する機密情報の開示：92.9%
- 公開の必要がないと推測されるファイルの検出：7.1%

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と、攻撃者にシステムの設定やネットワーク構成などを推測されてしまう原因となる。攻撃者はより的を絞った攻撃が可能となり、攻撃が成功する危険性を高めてしまう。例えば、バナーやエラー情報等に、システムで稼動しているデバイスやアプリケーションの情報が含まれていたとしよう。特に使用アプリケーションのバージョンが明らかになれば、攻撃者はそのアプリケーションに特化したエクスプロイト（攻撃プログラム）を試すことで、攻撃をより効率的に実行できることになる。詳細なエラー情報も、攻撃に有用な情報を多く与える一助となってしまう。場合によっては、システムの設定や動作もわかってしまうため、攻撃を組み立てやすくなるのだ。

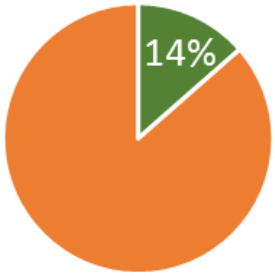
本来ならアクセス制限によって保護すべきファイルや情報が開示されてしまっている場合も同様である。当社の診断では、ミドルウェアのデフォルトファイル、場合によっては制御ファイルが、リモートからアクセス可能な状態にあるシステムが見られることがある。インストール時のデフォルト設定には脆弱性が含まれているケースが多く、そうした脆弱性を攻撃者に悪用される可能性があるのだ。制御ファイルや管理ファイルについては、実際に利用されているファイル名称が攻撃者に知られる原因となるため、攻撃をより容易にする有用な情報となりえる。

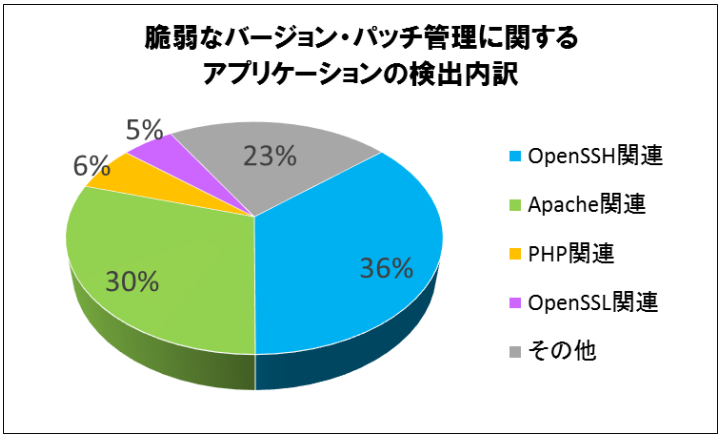
対策としては、システムの運用や業務に不要なファイルを全て削除することが推奨される。特定のユーザに対してのみ開示することを意図しているファイルやディレクトリについては、ミドルウェアのアクセス制御設定、もしくはパケットフィルタリング等の強固なアクセス制限により、限定されたユーザおよび特定の場所からのみ接続可能とすべきである。

【ネットワーク診断】
バージョン・パッチ管理に関する問題

ここ数年のサイバーセキュリティに対する意識の高まりにより、バージョンアップやパッチ適用を適宜実施している組織は増加しているものと思われる。しかし、診断結果では、ベンダサポートが終了したバージョンや既知の脆弱性が存在するバージョンの OS やアプリケーションを使っているシステム、重要なセキュリティパッチを適用していないシステムが、未だ 14%検出されている。

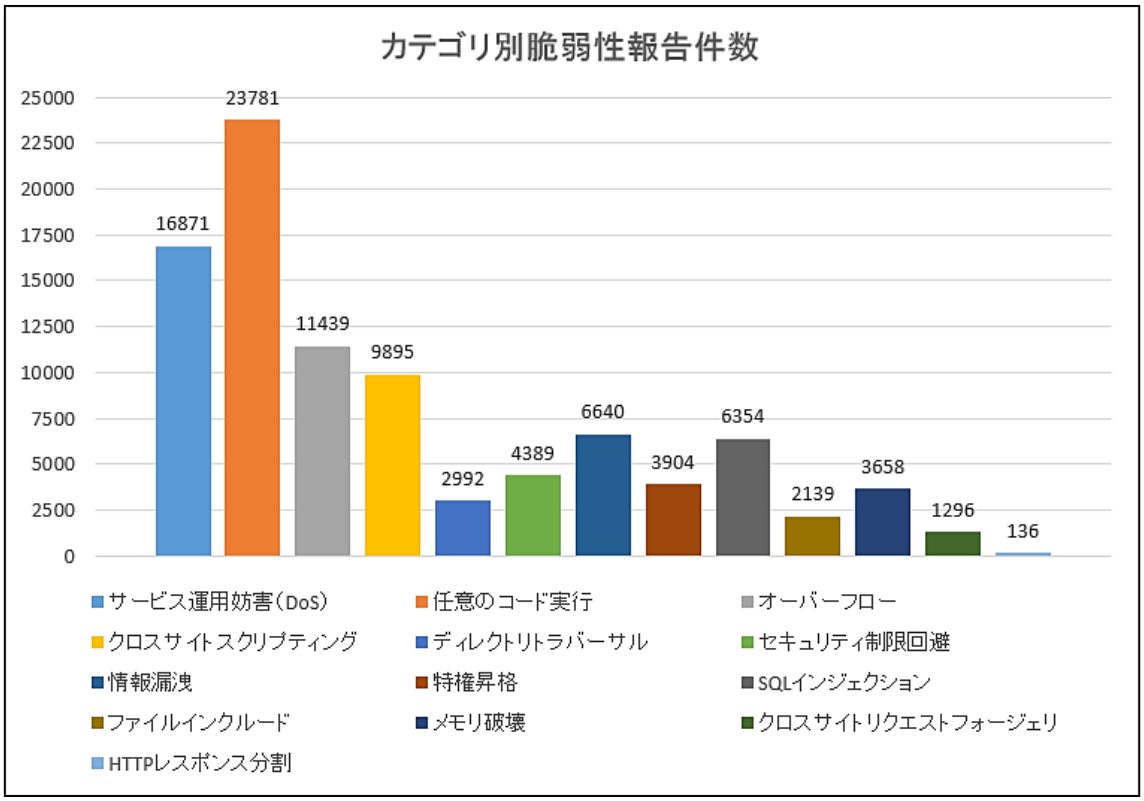
【バージョン・パッチ管理に関する問題の検出割合】





アプリケーション別で見ると、OpenSSH、Apache、PHP、OpenSSL に関する問題が多い。ただし、これはバージョン情報が表示されていることを前提とした診断結果であるため、実際にはより多数の、脆弱なバージョンのまま使用されているアプリケーションが存在する可能性があるといえる。

実際、共通脆弱性識別子 CVE（Common Vulnerabilities and Exposures）番号が割り当てられている脆弱性の累計数を比較しても、これらのアプリケーションが名を連ねており、2016 年 9 月時点で OpenSSH は 83 件、Apache HTTP Server は 193 件、PHP は 500 件、OpenSSL は 161 件となっている。なお、脆弱性のカテゴリ別報告件数は次ページのようになる。



出典:MITRE 社「カテゴリ別脆弱性報告件数」より当社作成

サイバー攻撃において、不正侵入や情報漏洩の被害を受けたケースの多くは、アプリケーションや OS における既知の脆弱性が悪用されたことによる。また、前述の「WooYun.org」(23 ページ参照)のように、脆弱なバージョンのアプリケーションを使用しているシステムを IP アドレス単位で公開している Web サイトも存在する。中でも有名なのが「Shodan[11]」だ。このサイトには、世界各国のシステムに関する情報が登録されており、日本も例外ではない。サイトの運営者はセキュリティ啓蒙活動の一環として公開していると主張するが、攻撃者にとってはとてつもない「お宝サイト」でもあることから、物議を醸している。

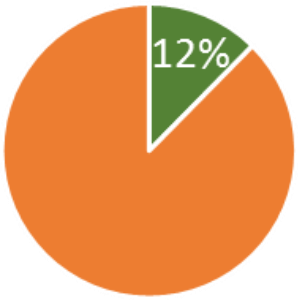
報告された脆弱性に対しては、それを修正するためのセキュリティパッチや更新バージョンなどが各ベンダより提供されている。対応が実施されないまま運用されているシステムは、脆弱性を悪用されて、サービス運用妨害(DoS)や不正な権限昇格、重要情報の奪取等、様々な被害を受ける可能性がある。当社でもその影響を考慮し、リスクレベル「重大」「高」として報告することも多い項目だ。OS・アプリケーションが最新の状態か、常に確認・管理を行うことが必要である。

[11] https://www.shodan.io/

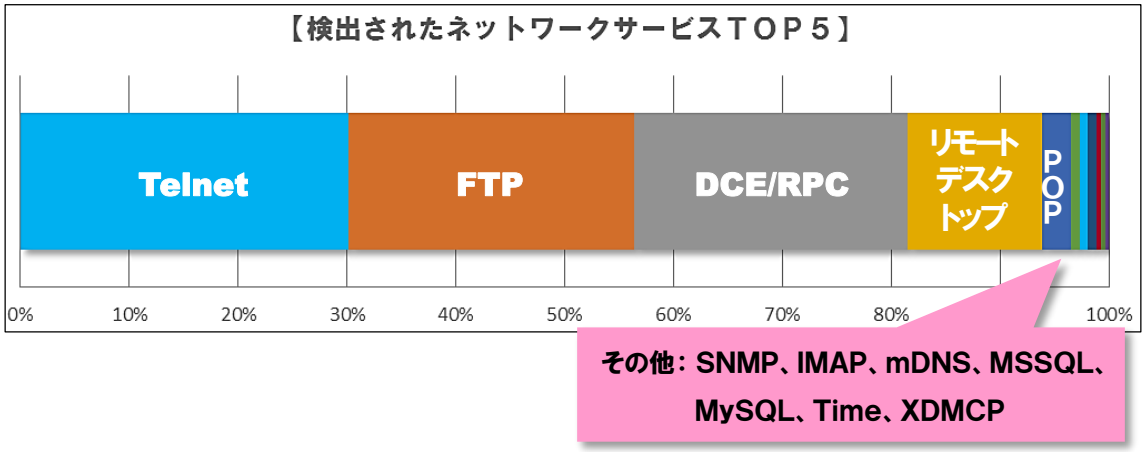
【ネットワーク診断】ネットワークサービスに関する問題

安全でないネットワークサービスが使用されていると、盗聴や情報漏洩の原因になる。このような問題は全体の 12%検出された。

【ネットワークサービスに関する問題の検出割合】



【ネットワークサービスに関する問題の検出項目】



古くからネットワークの運用管理に使用されてきたTelnet、ファイル転送に使用されてきたFTPは、いずれも暗号化されないまま通信が行われるネットワークサービスである。アカウント情報および認証後の通信もすべて平文で流れるため、盗聴されると情報漏洩につながる。また、パスワード不要の Anonymous（匿名）アカウントやゲストが設定されているとなおさら危険である。リモートデスクトップサービスにも同様の危険性がある。

当社の診断の結果、安全でないネットワークサービスは、Telnet サービス（30%）、FTP サービス（26.3%）、DCE/RPC サービス（25.1%）、リモートデスクトップサービス（12.4%）、POP3 サービス（2.7%）の順に多く検出されている。

TOP 5 に入っていないネットワークサービスの中に、POP と同じくメールプロトコルである IMAP がある。メールをダウンロードせずに直接サーバ上で読めるという利便性から、外出先や複数の場所からメールを読む必要がある場合や、Web メールサービス等で重宝されている。しかし、IMAP にも通信が暗号化されないという問題があるので、ご注意いただきたい。

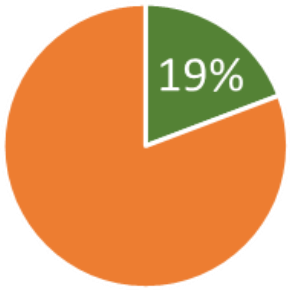
通信内容の盗聴による情報漏洩を防ぐためには、これらのネットワークサービスの使用をやめるか、インターネットなどの保護されていないネットワーク接続経由では使用できないようにするのが最も安全である。しかし、例えば、リモートデスクトップサービスは外出先から PC を使用できるというメリットが大きいため、業務に不可欠となっていることが多いだろう。このサービスを安全に使用するためには、セキュリティ設定を検討すればよい。VPN 接続、ポートスキャンされにくいポート番号への変更、サービスのアップグレードやファイアウォール設定による接続 IP アドレスのアクセス制御等、推奨される対策は複数存在する。前述の IMAP も、IMAPS を使用することで、暗号化された経路で通信することができる。

自組織のシステム上で実行されているネットワークサービスが業務上必要なものか、また、安全性に問題のない状態になっているか。セキュリティポリシーに沿って確認する習慣を定着させる工夫が必要だろう。

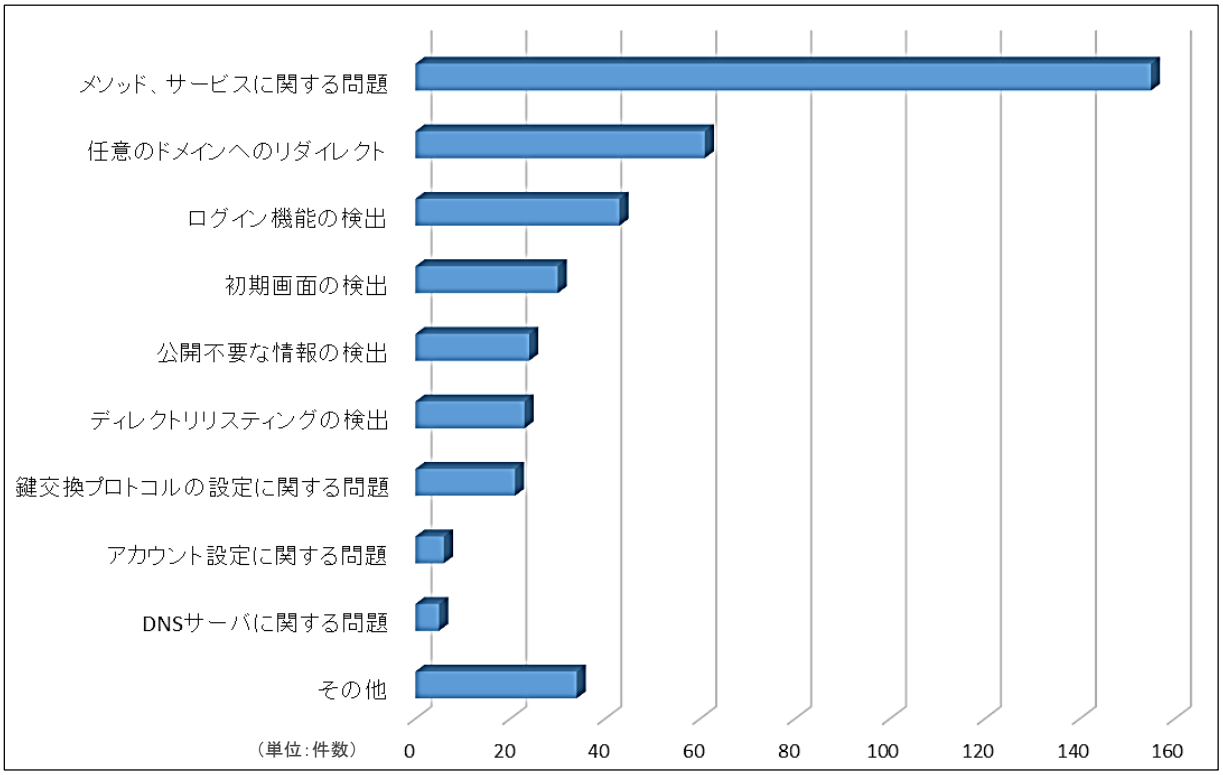
【ネットワーク診断】
不適切な設定に関する問題

ベンダ設定のまま、安全でないデフォルト値を使用し続けている場合、その部分に脆弱性が存在する可能性がある。その脆弱性が悪用されることで、様々な情報セキュリティ上の被害が生じかねない。当社診断では、不適切な設定に起因する問題の検出割合は 19%であった。

【不適切な設定に起因する問題の検出割合】



【不適切な設定に起因する問題の検出項目】



「不適切な設定」には、以下のような問題が含まれる。

- **メソッド、サービスの設定に関する問題**
- **任意のドメインへのリダイレクト**
- **ログイン画面のアクセス制限設定の問題**
- **デフォルト設定の初期画面**
- **脆弱なアプリケーションの問題**

こうした「不適切な設定」の問題の中で当社の診断で最も多く見られたのが、メソッド、サービスに関する問題である。例としては、HTTP メソッドにおける PUT や DELETE などのメソッドの使用や、SMTP サービスの送信元の検証不備などが挙げられる。HTTP メソッドが悪用された場合は、任意のファイルのアップロードを行われる恐れが生じる。SMTP サービスの送信元の検証に不備がある場合は、内部ドメインを詐称した送信元から、内部ドメイン宛のメールを送信可能になるリスクが生じる。これにより、なりすましによる標的型攻撃を受ける可能性が高まり、非常に危険である。

次に多かったのがリダイレクト機能に関する脆弱性だった（15.2%）。これは、パラメータに他ドメインの URL を設定することで、リダイレクト先に任意のサイトを指定することが可能になるという脆弱性であり、利用者が意図しないページにアクセスさせられるリスクが生じる。このため、フィッシング詐欺やマルウェア感染といった被害を受ける恐れがある。

また、ログイン画面に適切なアクセス設定がされていないシステムも多く見られた。これにより、総当り（Brute-Force）攻撃によってアカウント情報が奪取されたり、多数のログイン試行によりシステム負荷の過多に陥る可能性がある。

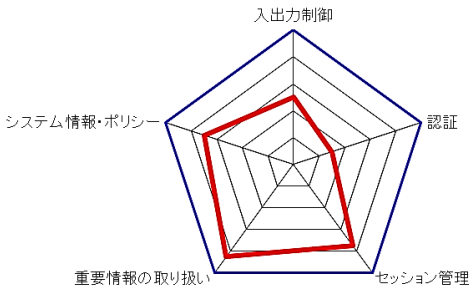
この他にも、ベンダ設定のまま、安全でないデフォルト値を使用し続けることで、セキュリティ対策を十分に行っていない企業であるという認識を攻撃者に与えることが予想される。そうした状態を放置することで、対策のされていない DNS サーバを踏み台にする DNS Amp などの攻撃の踏み台として狙われるなど、攻撃行為を助長することにつながりかねない。

参考情報

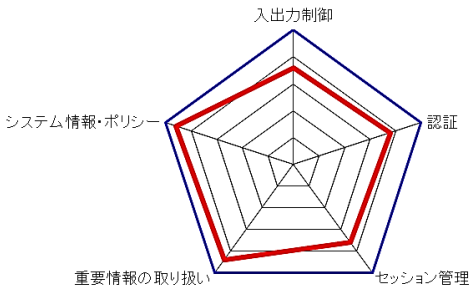
◆ 業種別　Web アプリケーション診断結果レーダーチャート

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、業界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」「認証の取り扱いに関する問題」について、対策強化の必要がある業界が多く見受けられる。

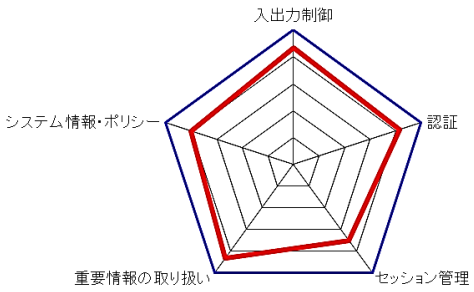
【建設業】



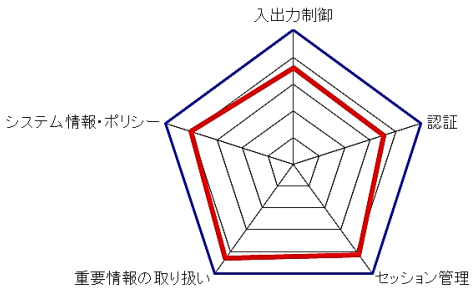
【製造業】



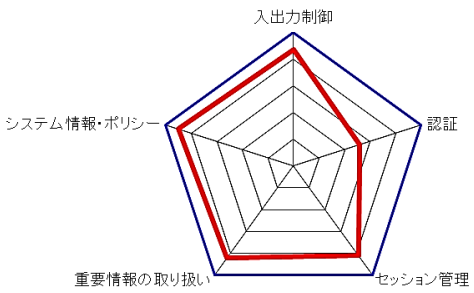
【電気・ガス・熱供給・水道業 】



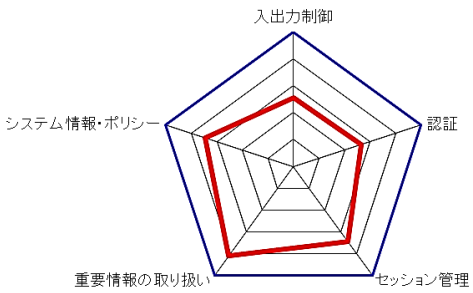
【情報通信業】



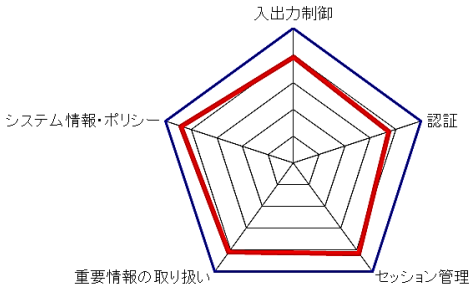
【運輸業，郵便業】



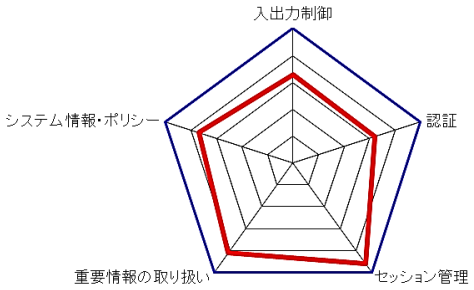
【卸売業，小売業】



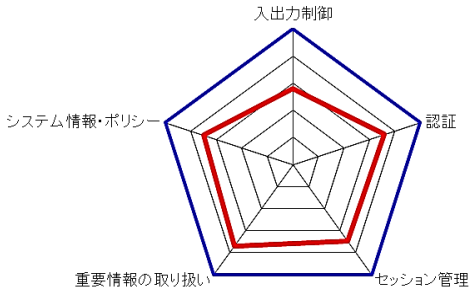
【金融業，保険業】



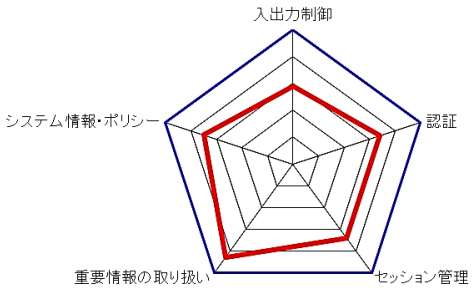
【不動産業，物品賃貸業】



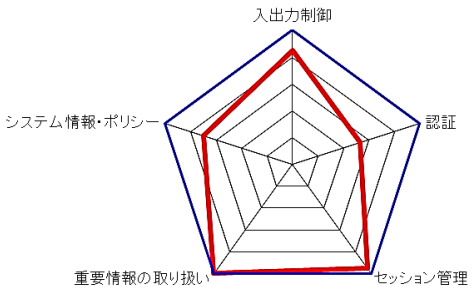
【学術研究，専門・技術サービス業】



【生活関連サービス業，娯楽業】



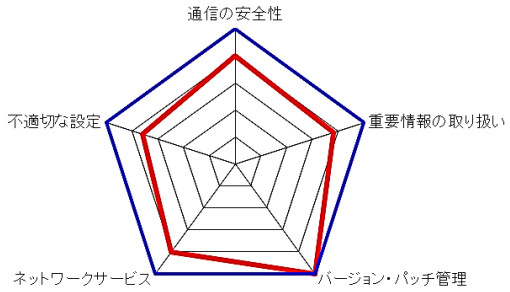
【サービス業（他に分類されないもの）】



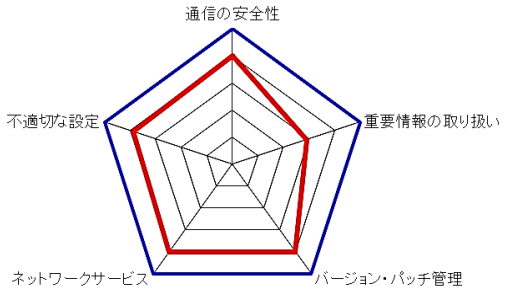
◆ 業種別　ネットワーク診断結果レーダーチャート

ネットワーク診断の結果より、各カテゴリに対す対策の度合いについて、業界別平均値をレーダーチャートで表した図である。業界ごとに対策を強化するべきカテゴリの特徴が異なるが、「通信の安全性」「不適切な設定」「ネットワークサービス」については、いずれの業界も等しくあと一歩というところであることがわかる。

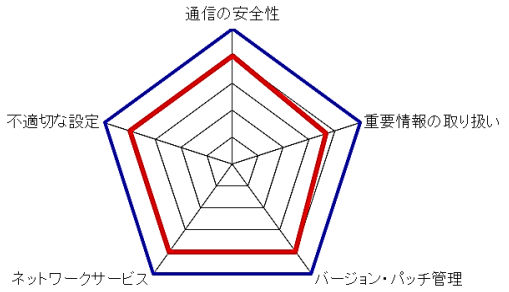
【建設業】



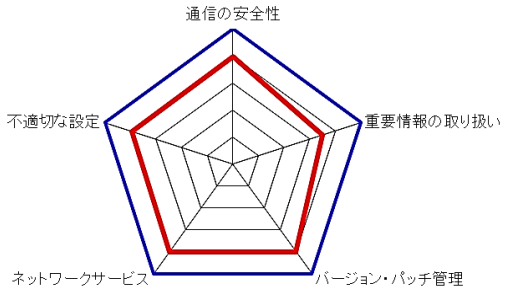
【製造業】



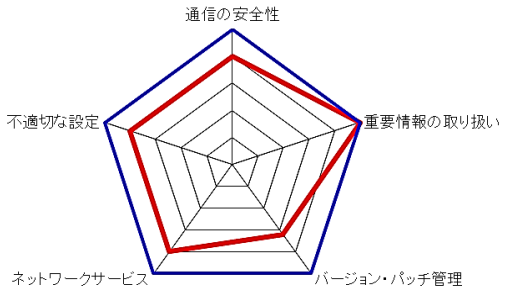
【電気・ガス・熱供給・水道業】



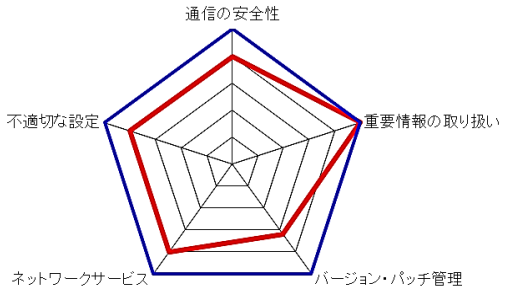
【情報通信業】



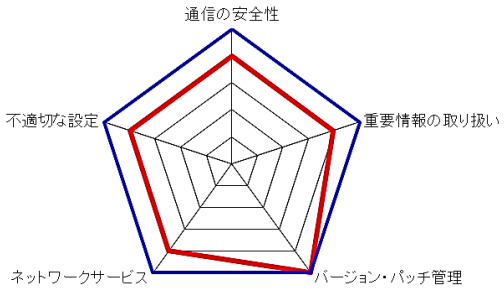
【運輸業，郵便業】



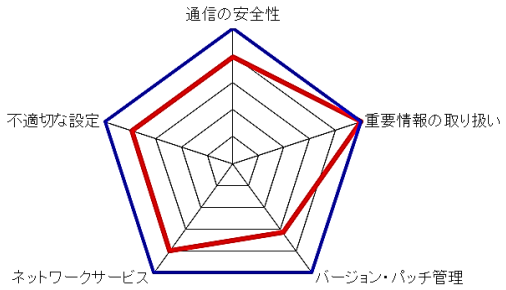
【卸売業，小売業】



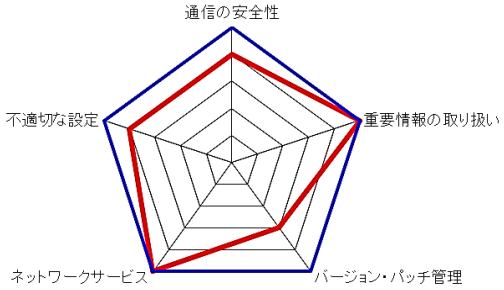
【金融業，保険業】



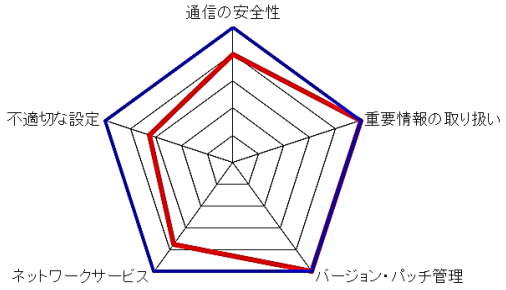
【不動産業，物品賃貸業】



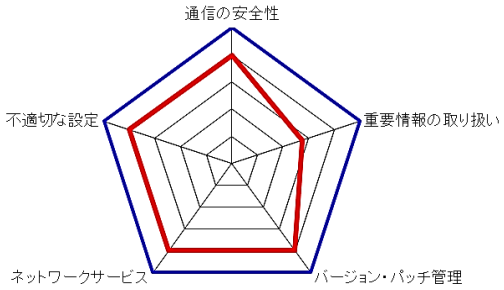
【学術研究，専門・技術サービス業 】



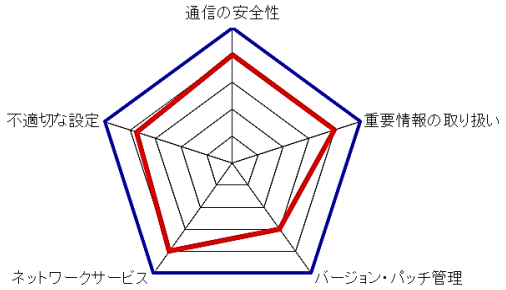
【宿泊業，飲食サービス業】



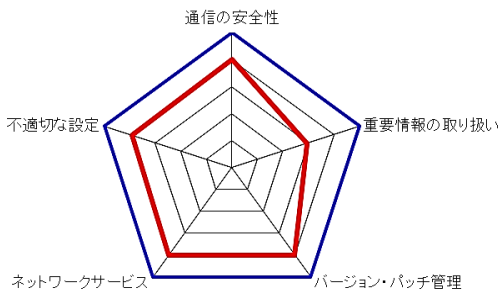
【生活関連サービス業，娯楽業】



【教育，学習支援業】



【サービス業（他に分類されないもの）】



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

SQAT® Security Report　2016 年上半期（1 月～6 月）
2016 年 9 月 15 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 4 階
TEL：03-5338-7417　　FAX：03-5338-7435
https://www.bbsec.co.jp/


BBSec