SQAT® SECURITY REPORT

2018年10月号

株式会社ブロードバンドセキュリティ
セキュリティサービス本部
東京都新宿区西新宿 8-5-1 野村不動産西新宿共同ビル 4F
TEL：03-5338-7417　FAX：03-5338-7435
https://www.bbsec.co.jp/

はじめに

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

本誌は、株式会社ブロードバンドセキュリティ（以下、BBSec）の脆弱性診断サービス「SQAT®」* における 2018 年上半期（1 月～ 6 月）の診断から得られた最新データをベースに、当社トップエンジニアらによるサイバーセキュリティの現状と展望について、様々な角度からお楽しみいただくことを目的としたレポートです。

情報セキュリティの考え方はこの数年で大きく変わってきました。いまや事故前提の考え方で、サイバーセキュリティ対応体制を構築することが主流となっています。とはいえ、サイバーセキュリティ対応とは名ばかりの、「ただ作ってみました」といわんばかりのシステムも残念ながら少なくありません。巻頭では、こうした体制について、本当に使える体制とは何か、備えておかなければならないログとは何か、について実例を交えて解説いたしました。

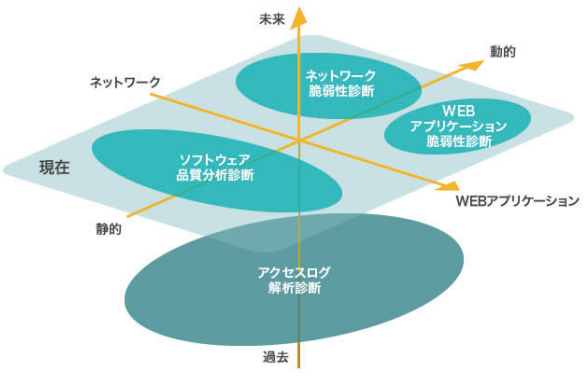
また、注目テーマとして、DevSecOps の考え方とソースコード診断について取り上げて解説しております。本年 5 月に起きた世界的なセキュリティインシデントはソースコード診断によって防げたかもしれない事例ですが、こうした事例を取り上げつつ、ソースコード診断のメリットと特徴を探っていきます。

さらに、今期忘れてならないのが、個人情報に関する世界的な潮流です。EU 一般データ保護規則（GDPR）は既に対応されている企業も多いと思われますが、2018 年上半期は米国においても各州がそれぞれ独自の規制法案を打ち出すなど、個人情報に関する流れは怒涛の勢いで変化しております。また、個人データに関しては、コンテンツデータに留まらず、メタデータにまで規制がかかろうとしています。EU において GDPR を補完する形で審議中の e- プライバシー規則案について、2018 年 9 月末までの時点で公表されている審議案を元に、今後の動向と対策のポイントを提示しておりますので、ぜひご一読ください。

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

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

「SQAT® 」は、BBSec がご提供する脆弱性診断サービスです。エンジニア、コンサルタント、ホワイトハッカー等から編成された精鋭チームが、あらゆる側面から網羅的な診断を実施。スペシャリストのノウハウを結集して組織の情報システム強化をお手伝いします。お客様は金融機関・インターネット事業者などの民間企業から、官公庁をはじめとする公共機関まで幅広く、これまでに延べ 3,500 組織、12,000 を超えるシステムで利用されています。



CONTENTS

ログ分析の現場からみるサイバーセキュリティ

株式会社ブロードバンドセキュリティ
高度情報セキュリティサービス本部
セキュリティ基盤開発部
セキュリティ基盤導入課　課長

宮城　和音

日進月歩で進化するマルウェアをはじめとしたサイバー脅威に立ち向かっていくためには、もはや事故前提の考え方が主流である。近年は、この考え方を元にした CSIRT をはじめとした体制構築が進みつつある。そして、サイバーセキュリティ対応態勢を構築、維持していく上で「適正なログ管理」がされていることは不可欠な要素といえる。なぜならば、ログは「発生したインシデントに関する原因究明・影響範囲の特定」のための信頼できるリソースであり、迅速なインシデント対応の上で重要な役割を果たすからだ。また、ログを「攻撃や不正の証拠として利用」できる場合もある。さらには、ログを分析することで「攻撃の兆候や潜在的なリスク、防御できなかった攻撃の早期発見」につなげることも可能だ。

一方で、実際にログが適切に管理された環境を実現するために「どういうことをすればよいのか？」「何から手をつけるべきなのか？」といった点でエンジニアの方が困っている話はよく聞く。あるいは、既にログの収集・管理を行っている組織においても「集めたログで何ができるのか」「具体的にどのように活用すればよいのか」といった点で悩んでいる声を聞くことも多い。

本稿では、まずセキュリティにおけるログの重要性およびログ管理の基本的な考え方について解説する。その上で、ログを収集していく上での課題や注意点について様々な事例を踏まえて解説する。最後に、実際に収集したログを分析することで、どのようなことが明らかになるのかについて、ログ分析の現場での事例を紹介する。

1. セキュリティとログ管理

ログはどのように役に立つか

ログは組織のシステムやネットワーク内で発生するイベントの記録である。その多くにコンピュータのセキュリティに関する記録を含んでいるため、セキュリティに関する様々な側面でログを活用することができる。

ログはどのような場面で役に立つのだろうか。まず挙げられるのは、発生したセキュリティインシデントに対する初動対応での活用である。ログからイベントの詳細を把握することで、本当に重大なインシデントであるかの切り分けを行うことができる。そして、インシデントの初動対応の肝となる、攻撃を受けた機器の特定、被害拡大防止のための封じ込め対応など、迅速な情報収集に役立つ。セキュリティインシデントではいかに迅速な初動対応を講じることができるかによって、被害の規模が大きくかわるため、適切なログをすぐに調べられるような体制を準備しておくことを推奨したい。

また、発生したセキュリティインシデントにおいて、原因究明や影響範囲特定のための信頼のおけるリソースとしても活用できる。例えば攻撃によって 1 万件の個人情報を持つシステムから情報流出が発覚した場合を考えよう。適切なログがあれば、流出したのは特定のユーザ数名に関する情報であるという正確な情報が明らかになるかもしれない。一方、調査するためのログが不十分な場合には、最大 1 万件の個人情報が流出した可能性があるというように、生じうる最大の被害を報告する事態に発展しかねない。したがって、過去に記録されたログを調べることができるよう、ログを適切な期間・適切な方法で保管しておくことが重要だ。

さらに、ログを定期的にレビュー・分析することは、様々なセキュリティ上の問題の発見につながる。例えば、不審な通信からサイバー攻撃の兆候が明らかになることもあれば、従業員のポリシー違反・不正行為などがみつかることもある。システムの異常を早期に発見することは、重要システムの可用性の維持のみならず、より安全なシステム環境を実現、運用していくための機密性、完全性といった面においても重要な要素といえよう。そのため、クレジットカード業界のデータセキュリティ基準 PCI DSS では、ログの定常的な確認が義務付けられているケースもある。

ログの活用例

- セキュリティインシデントにおける初動対応での活用
- セキュリティインシデントの原因究明や影響範囲の特定に活用
- 様々なセキュリティ上の問題発見に活用

ログ管理とは

前述のように、様々な場面で役に立つログであるが、ログの種類や量は膨大かつ多種多様である。そのため、ログを適切な期間、適切な内容を有した状態で保存するために必要になってくるのがログ管理という考え方だ。

アメリカ国立標準技術研究所（NIST）は、ログ管理とはログデータの生成、通信、格納、分析、廃棄を行うプロセスと定義している。[*1]

- 何をログとして記録するか
- 記録したログをどのように保管するか
- ログをどう活用するか

これらの方針を決定し、それを実現するための仕組みを作り、運用していくことがログ管理であるといえる。考え方の詳細は前述のNISTの資料に詳しく記載されているのでご一読いただくと参考になるだろう。本稿ではより現場寄りのログ管理における課題を解説していく。

2. ログ収集の落とし穴 ～現場でよく発見される問題点～

「ログ分析をして欲しい」との要望を受けて話を進めていると、分析したいイベント種別のログが収集できていないことが明らかになるケースがある。そんな時はログの取り方や、分析対象の期間変更などの見直しが必要となる。しかし、これがセキュリティインシデント発生時で、調査に必要なログがないと発覚した場合だったらどうだろうか。初動対応に支障がでて被害が拡大することや、影響範囲が特定できないことを考えるとゾッとする。

なぜ、このような事態になるのか。根本的には、ログ管理に関して「何をログとして記録するか」「記録したログをどのように保管するか」などの基本的な方針が定められていないことが問題となる。方針が定まっていなければ、管理に支障がでるのは当然だ。とはいえ、ログ管理において具体的にどのような課題があるのかを知らなければ、具体的な方針を考えることは難しい。そこで今回は、ログに関して現場でよく発見される問題を挙げながら、適切なログ収集について解説する。

ログが生成されていない

ログを生成するシステムの種類や数は膨大であり、内容も多種多様である。ところが、特別な設定をしないと生成されないログがある。これは、初期設定（デフォルト値）状態では、記録するイベントを限定することで、ログの量が無尽蔵に増加するのを抑えている面もあり、致し方のない部分もある。しかし注意しなければいけないのは、セキュリティにおいて重要な種類のイベントであるにも関わらず、ログの生成が無効になっているものがあることだ。

よく見かけるのが、Windows OSの監査ログにおいて、セキュリティの観点で重要なイベント種別がログとして記録されていないケースである。Microsoft社による「Windowsにおける OS の監査ログの推奨設定[2]」などをみると、推奨値と初期設定（デフォルト）値に大きな差異があることが分かるだろう。Windows OS 以外のシステムについても、どのイベント種別が必要かを丁寧に検討していくのは根気のいる作業である。各システムについて推奨設定を調べて、まずはそれが適用されているかどうか確認することを推奨したい。

ログに記録された情報が足りない

ログに記録するイベントを選定し、そのログが生成されるように設定した場合であっても、ログに保存された情報に不足があるケースもある。具体例をみてみよう。Webサイトへのアクセス分析において、不審な通信の発見に活用できる情報として、利用ブラウザなどを示す「ユーザエージェント」、直前に経由した Web ページを示す「リファラ」などがある。しかし、広く使われているソフトウェア「Apache HTTP Server」を初期設定（デフォルト）値で運用した場合、暗号化された HTTPS 通信において、上述の情報はログに出力されない。このように、ログのフォーマットが不適切な場合、ログから得られる情報が不十分になることがある。

上記は、特定のミドルウェアの例だが、どのようなシステムのログにおいても、最低限抑えておきたい項目が 2 つある。ひとつめは時刻情報だ。ログの生成や保存を行う各システムを標準時刻に同期することで、複数システムのログを照らしあわせることが可能になる。もうひとつが、そのイベントを他のイベントと結びつけるための識別情報である。例えば、認証システムであれば「アカウント名」、ネットワーク機器であれば「IP アドレス」、Web アプリケーションであれば「セッション ID」などである。特に独自開発したアプリケーションなどでは、ログの出力も独自仕様になることが多いため、特定のイベントを他のイベントと結びつけるための識別情報をログへ記録するようにアプリケーション開発の段階から注意が必要だ。

*1 NIST「SP 800-92, Guide to Computer Security Log Management」（2006）、（翻訳版）IPA「コンピュータセキュリティログ管理ガイド」
*2 Audit Policy Recommendations（https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations）

ログの保存期間が短い

ログは多くの場合、まずそのシステムのローカル環境に保存される。しかしそのストレージ容量に制限があるため、一定時間が経過すると古いログは次々と消えていく。そのため、適切なログが生成される設定になっていても、ログの保存期間が短いために、必要な期間のログが参照できないことがある。

例えば、Linux 系サーバの設定を確認した際に以下のような事例があった。とあるログに関して、設定ファイル上は出力項目も適切に設定され、保存期間も長期間に設定されているようにみえた。しかし、実際には数日分のログしか保存ができていなかったのである。ログ量が多いため、ログのデータサイズに関する設定が影響して、ログが数日分で自動的に削除、ローテーションされていたのだ。

また別の例では、ファイアウォールのトラフィックログのうち、Permit ログが短期間分しか残っていなかったことがある。ファイアウォールによって通信を遮断されたトラフィックに関する Deny ログは外部ストレージへ転送し、長期間適切に保存されていたのだが、ファイアウォールを通過したトラフィックに関する Permit ログは、ログ量が膨大になるためローカル環境のみに保存される運用であった。これは、Permit ログは短期間しか保存できていなくても仕方ないという認識の上での設定であったが、ファイアウォールにおいては Permit ログこそ重要といえる。なぜならば、ファイアウォールで遮断されずに、通り抜けてしまった不正アクセスやマルウェア感染などの悪性通信は、Permit ログに記録されるからだ。

どのログを保存すべきかを考える際には、どのくらいの保存期間が必要かについても検討し、その保存期間を確保できるような仕組みを考える必要がある。特に重要なログは最低でも 3 ヶ月、可能であれば 1 年間は保存することを推奨する。

ログの保存先とセキュリティ

ログに関する課題のひとつにログの保存先がある。

多くのログはまずシステムのローカル環境に保存されるが、ローカルシステムにのみログを保存している場合、様々な問題が生じうる。その筆頭がログ自体のセキュリティの問題である。ログはインシデント対応で活用できる重要なリソースであるため、攻撃者が自らの痕跡を消すためにログを消去・改竄しようと試みることも多い。これを防ぐためには、ログサーバや後述する SIEM を準備し、ログを外部環境へ転送し、集約することによるログの保全が不可欠だ。ログの分析においては様々なログを並行して閲覧する必要があるため、ログを集約することはセキュリティインシデントにおける迅速かつ効率的な初動対応においても大きな利点となる。

ログサーバなどを用いる場合も、ログ自体のセキュリティへの配慮は必要だ。ログには意図せずに混入したパスワードなど、セキュリティに関する記録やプライバシーに関わる記録が含まれることがある。そのため閲覧できる人を制限できるように機密性を確保する必要がある。また、ログが転送・保存の過程で改変や破損により完全性が損なわれると、インシデント対応のためのリソースとしての信頼性が損なわれる。そのため、ログの完全性についても配慮が必要だ。この観点は、特にログを何らかの証拠として用いる場合に重要である。

3. ログは集めて終わりではない

ログを適切に収集できれば、ログ管理は十分といえるだろうか。そんなことはない。集めたログは分析することでその真価を発揮する。特に定期的な分析を行うことは、セキュリティインシデントの発見につながるだけでなく、普段からログに親しんでおくことが、インシデント対応時の効率的な調査にもつながるだろう。

ログは分析を考慮した環境に集めることが重要である

集めたログを分析するためには、そのための基盤環境も必要になってくる。特に、インシデント対応などを考えると、現場の人間がその場ですぐに分析できることが好ましい。また、自動で特定の条件にあうログを拾い上げアラーティングするような仕組みがなければ、膨大なログの中から有用な情報を拾い出すのは難しい。そこで、近年はログを集約・分析するための基盤として SIEM（Security Information and Event Management）が普及してきている。SIEM が優れている点は、収集した複数のログの内容を横断的に分析し、異なるログにまたがる「相関分析」を行える点だ。SIEM 製品は複数あるが、多くの場合、先に述べたログ自身のセキュリティ関する配慮も備わっている。適正なログ管理のために、ぜひとも導入を検討いただきたい仕組みのひとつである。

ログ分析の事例

ログを分析するための環境が整ったあと、実際にどのように分析を行えばよいのか、あるいは、分析により何が分かるのだろうかというイメージがつかない方も多いだろう。そこで、Web プロキシサーバのアクセスログを例に、定期的なログ分析での事例を 2 件紹介したい。

分析事例１：外部への不審な通信

Web プロキシサーバのアクセスログからは、マルウェアなどに起因する、外部への不審な通信の発生有無を調査可能だ。

そのための、具体的な分析手法のひとつは、悪性の通信先であると知られている IP アドレスや URL のリストとのマッチングを行うものである。この手法では悪性通信先の情報をいかに入手するかが分析の肝となる。有償のデータベースを利用するだけでなく、様々なセキュリティ関連組織から提供されるマルウェアの分析情報の中に、C&C サーバのアドレスなどが公開されていることも多い。

別の分析手法として、「一定間隔で発生する通信」「夜間に発生する通信」など、ユーザによる正規の操作とは考えにくい通信パターンを探す方法がある。なお、正規のプログラムが上記のような通信を行うこともあるため、本当に不審な通信を絞り込んでいくためには、正常な通信を除外していく手順が必要になる。そのため、通常時にどのような通信が発生するかを定常的に確認しておくことが、効率的な分析につながっていく。

実際にこうした手法を用いてログの分析を行った場合、マルウェアの感染までは至らずとも、アドウェア（広告ツールの一種）などの潜在的に危険なソフトウェア起因の通信が発見されることは多い。アドウェアは、別名リスクウェアとも呼称されているツールの一種だ。このようなソフトウェアは、直ちにコンピュータに害があるわけではないが、不適切な機能や意図しない情報収集がなされるケースがあり、将来的なリスクとなりうるので注意が必要だ。（図１）

分析事例２：情報流出の経路となりうる WEB サービスの利用

セキュリティインシデントでは、外部の攻撃者に起因するもののみならず、内部犯による情報流出が問題となることも多い。Web プロ

図１：アドウェア由来と推測される通信詳細例

日時	（火）～ 日（金） 土・日・祝以外の毎日（ 日間）、9:00-21:00 の時間帯 関連イベント初出時刻：16:00:34 関連イベント最終時刻：18:43:00
接続端末情報	認証ユーザ名：
通信先	

分類	ホスト名	ポート	回数	プロキシのアクション
A	.com	80	94	allow
	.com	443	5,772	allow
	.com	443	5,668	allow
B	.com	443	5,743	allow
		4658	310	error
C	.co	443	246	allow
			4	eroor

事象	上記の通信先に対して、勤務時間帯に複数回の通信が確認されました。これらの通信先は、通信内容や通信量、公開情報などの調査から、ユーザがアクセスしたサイトの URL などの収集に利用されるものであり、直接的な危険は低いと判断できます。 下記への通信に関しましては、ほぼ一定の時間間隔で通信を行っていたことを確認しています。 「.com」「.com」「.com」 下記への通信に関しましては、朝 9 時台の通信が大半を占めたことから、コンピュータの起動や、ブラウザの起動のタイミングで通信を行っていたと推測できます。 「.com」

キシサーバのアクセスログからは、情報流出の経路となりうる Web サービスへのアクセスの実態を調査できる。このような分析を行うと、オンラインストレージや Web メールの利用を、システム面で制御、禁止している場合であっても、意外な実態が明らかになることがある。

とある組織では、WEB プロキシサーバの URL フィルタリング機能を用いてオンラインストレージにアクセスができないようになっていた。しかしながら、ログ分析をしてみると、複数種類のオンラインストレージに対してアクセスが成功していることが判明したことがある。しかも、ユーザの制限なくアクセスが可能である状態であった。業務上必要なデータの授受のために、特定のオンラインストレージの利用を例外として許可したものの、その際に通信元の IP アドレスやアカウントによる制限をかけていなかったため、ユーザを問わずに利用できる状態になっていたのである。しかも、アクセスを許可したオンラインストレージの棚卸しが行われていなかったことから、このアクセス制御ルールは有効な状態で長期間運用され、その結果、多様なオンラインストレージへのアクセスが行われた状態になっていたのである。（図 2）

No.	サービス	通信先ドメイン	通信元 IP アドレス数	通信回数
1	[redacted]	[redacted]	246	992
2	[redacted]	[redacted] 他（計 38 ドメイン）	287	69, 081
3	[redacted]	[redacted]	3	51
4	[redacted]	[redacted]	2	211
5	[redacted]	[redacted]	4	137
6	[redacted]	[redacted] 他（計 6 ドメイン）	49	6, 172
7	[redacted]	[redacted] 他（計 22 ドメイン）	22	1, 744
8	[redacted]	[redacted] 他（計 17 ドメイン）	9	623
9	[redacted]	[redacted]	28	652
10	[redacted]	[redacted]		
11	[redacted]	[redacted] 他（計 586 ドメイン）	1, 226	155, 316
12	[redacted]	[redacted] 他（計 4 ドメイン）	3	89

図 2：オンラインストレージサービスへの成立した通信例

その他の分析事例

上記以外にも多様なセキュリティ上の問題点がログ分析により明らかになることは多い。ログ分析の手法を紹介した資料としては、JPCERT/CC「ログを活用した Active Directory に対する攻撃の検知と対策」「高度サイバー攻撃への対処におけるログの活用と分析方法」などがある。興味のある方はそちらも参照いただきたい。

おわりに

ここまで、ログ管理の重要性とそれを実現するにあたってのポイントを紹介してきた。事例を含め紹介してきたが、ログ管理に関する具体的なイメージ形成の助けになったであろうか。

繰り返しになるが、適切なログ管理は、インシデント発見のみならず発生時の被害拡大防止を迅速に実現するために不可欠だ。そして、ログは情報システムが記録する唯一の監査証跡といっても過言ではない。いざセキュリティインシデントにより情報流出事故が発生した際に、企業としての説明責任を果たすためにも、これらは重要な経営課題のひとつといえるだろう。

今後、2020 年の東京オリンピックを控え、より苛烈になっていくことが予想されるサイバー攻撃から自組織を守るためにも、ログ管理が適正に実施できているか、今一度検討してみてはいかがだろうか。本稿が少しでもご参考になれば幸いである。

宮城　和音

当社脆弱性情報提供サービス立ち上げの主要メンバーとしてサービスの確立に貢献。
顧客向け統合ログ管理基盤（SIEM）構築の実績多数。
収集から分析まで、ログに関わる幅広いサービスで活躍している。

＜保有資格＞　Splunk Certified Knowledge Manager

注目テーマ

堅牢なシステムを構築するために

ソースコード診断のすすめ

人が受ける健康診断には身長体重測定、血液検査、血圧測定、触診など、身体の部位や状態、患者の体質などによって多種多様な検査方法がある。Web アプリケーションの診断にもさまざまな検査方法があり、検出できる問題はそれぞれ異なる。

本稿では、システムの開発段階から問題部位を見つけ出すソースコード解析による診断の有用性をお伝えする。

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／開発部

ソースコード診断とは

Web アプリケーションへのサイバー攻撃は増加の一途をたどっている。インターネットの普及、ITインフラの複雑化や攻撃の多様化などから、企業における情報セキュリティもより一層の強化が迫られている。そのような中、対策の一環としてソースコード診断を採用する企業が増加してきている。

ソースコード診断とは、システムの設計後、テストや運用前の開発段階でコーディングの問題部位を特定し、そのリスクと対応例を提示する検査手法である。一般的な外部からのセキュリティ診断では探しにくい脆弱性を開発段階から検出できる。（図 1）

Web アプリケーションに内在する不具合や脆弱性は不適切なコーディングや設定ミスによるものもあり、攻撃者に有用な情報を露呈してしまう可能性があることはもちろん、攻撃に直接利用される恐れもある。もしもこういった問題が発生すれば、重要な企業資産（顧客情報や社員の個人情報、機密情報など）が危険にさらされてしまう。攻撃に対して堅牢なシステムを構築するためには、開発段階からソースコードのレビューを行い不適切な部位を修正しておくことが理想。社内でコーディング規約に基づいた検討をしたり、ツールを使用したりする方法や、外部の専門家によるソースコード診断を取り入れてみる方法もある。

図 2　未解放のリソース（例）

JavaSource/com/sample/lessons/Challenge2Screen.java　429 行目

```
JavaSource/com/sample/lessons/Challenge2Screen.java

429         FileWriter fw = new FileWriter(usersFile);
430         fw.write(getFileText(new BufferedReader(new FileReader(masterFilePath)), false));
431         fw.close();
・・・
434         }
435         catch (Exception e)
436         {
437                     e.printStackTrace();
438         }
```

429 行目で作成している FileWriter は 431 行目で閉じる処理を行っているが、430 行目で例外が発生した場合は閉じる処理が行われずにスコープを抜けてしまう。

OWASP Top 10 とソースコード診断

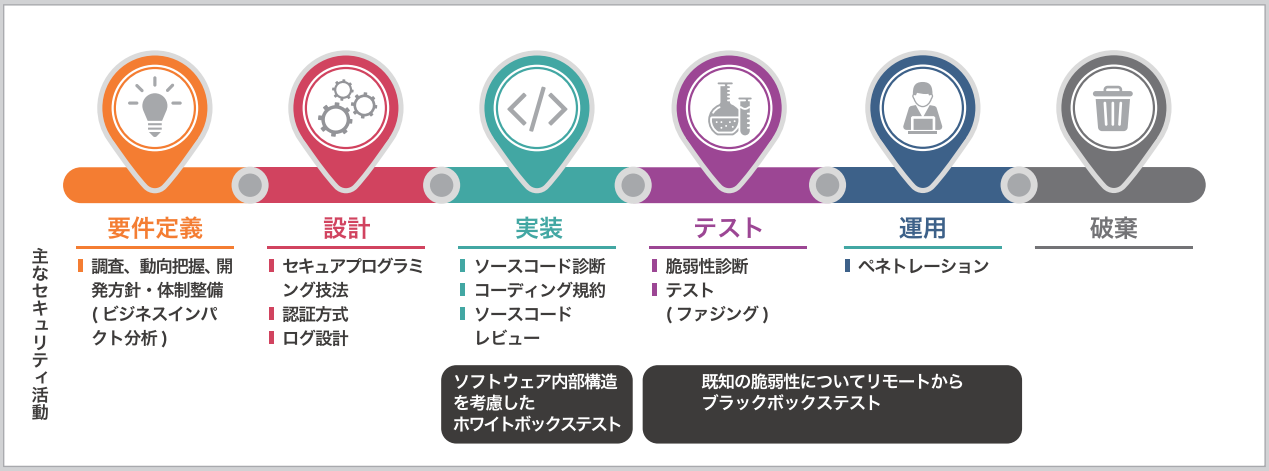
次に、Web アプリケーションセキュリティの課題解決に取り組む専門家らから成るグローバルなコミュニティ、OWASP（Open Web Application Security Project）が定期的に発表している脆弱性ランキング、OWASP Top 10 とソースコード診断の関係について説明する。（次ページ表 1）

検査方法によって観点が違うので、外部からのセキュリティ診断と、ソースコード診断では、検出される脆弱性がやや異なる。ユーザに見えている範囲で危険性を検査したい場合は外部からのセキュリティ診断、ユーザからは見えない、プログラム内部の危険性を検査したい場合はソースコード診断が有効だ。

例えば、OWASP Top 10 の＜1. インジェクション＞や＜2. 認証の不備＞が、外部からのセキュリティ診断で検出されなくても、ソースコード診断で内部を見てみたら問題点が見つかるというケースもある。＜3. 機微な情報の露出＞は外部からでも見つけられる脆弱性ではあるが、ソースコード内に平文でパスワードを保存している、あるいは脆弱なハッシュ関数でハッシュ化したパスワードを保存して

図 1　ソースコード診断の特徴

・リモート診断では探しにくい潜在的な脆弱性を実装工程で検出
・開発者担当者のスキルに依存しない、脆弱性を作り込まない対策を講じることが可能
・作りこんだ脆弱性をシステムライフサイクルの早い工程で摘出する



いないか、保持するべきではない情報（カード情報など）を保持していないかなどは、ソースコード診断でないとわからない。ほかにも、<9. 既知の脆弱性のあるコンポーネントの使用>について、一言に<コンポーネント>といっても幅が広い。OS やミドルウェア等ならば外部から見つかる可能性があるが、ライブラリなどソースコードの中で使っている場合も考えられるため、外部からだけではわからないだろう。

ソースコード診断の方が見つけやすい脆弱性

ここでシステムの内部構造に着目して行われるソースコード診断の方が見つけやすい脆弱性を述べる。パスワードなどの機密情報がソースコード内に記述されていて、開発担当者などが目にすることで情報漏洩につながる可能性がある状態（表 2<ハードコーディングされたパスワード>）や、リクエストから取得した値を使用してログに出力する機能において、攻撃者がパラメータを直接指定してきた場合に内容が保障されなくなる現象などは、ソースコード診断で見つけられる可能性が高い。

例えば、悪意のあるユーザは、パラメータに改行コードを含め、2 行目以降に細工を施した文字列を挿入することによって、ログの信頼性や可読性をそこなわせることができる。こういった脆弱性は、外部から見える機能を検証するプログラムの検査方法では検出が難しい。ほか、<不適切な例外処理>、(図 2<未解放のリソース>)、<未使用のコード>、<エラーメッセージによる情報の露出>といった脆弱性もソースコード診断で検知しやすい。(表 2)

ソースコード診断で防げたかもしれない事例

過去に公表された情報セキュリティ関連のインシデントのうち、ソースコード診断がなされて事前の対処をしていれば未然に防げたかもしれない事例をピックアップし、当社の見解を述べる。

2018 年 5 月の米・Twitter がユーザにパスワード変更を求めた事例[*1]について紹介する。同社はユーザのパスワードが社内システムに露出していたと発表し、すべてのユーザに向けてアカウントのパスワード変更を呼びかけた。影響規模は公表しなかったが、一部のユーザのパスワードが社内のシステムに通常のテキストで保存される不具合があり、この不具合を修正したと説明。社内調査では内部関係者がパスワードを盗んだり、悪用したりした兆候は発見されなかったが、念のためパスワード変更を検討してほしいと伝えた。

同社のブログによると、発見された不具合は、アカウントのパスワードがマスキングとハッシュ化を終える前に内部ログに書き込まれてしまうバグだったという。発表された一連の流れから察すると、ソースコード診断で検知しやすい脆弱性のうち、<プライバシー違反>に相当するものと考えられる。ソースコード診断やソースコードのレビューが実施されていれば検知可能な脆弱性だったと思われるため、未然に防げた可能性は高かったケースと言えよう。外部からログファイルを確認することはできないが、システムの運用をしている側からはログファイルを参照することができる。システム運用者がログに出力されたパスワードを見ていた可能性はあるので、それを悪用する場合も考えられた。パスワードの変更を呼びかけた事後処置は適切だったといえる。

こういったケースで万が一発見が遅れた場合に起こり得る二次被害も想定してみる。例えば悪意のあ

表 1　OWASP Top 10 アプリケーションセキュリティリスク – 2017

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

OWASP Top10 - 2017 より当社作成

表 2　検知可能な脆弱性の例

- SQL インジェクション
- セッション固定
- クロスサイトスクリプティング
- セッションの改竄
- コードインジェクション
- DoS 攻撃
- バッファオーバーフロー
- パラメータの改竄
- 未検証の入力
- クロスサイトリクエストフォージェリ (CSRF)
- 安全ではない URL リダイレクト
- HTTP レスポンス分割
- 未検証のファイルのアップロード
- 不適切な例外処理 ＊
- 未解放のリソース ＊
- ログの改竄 ＊
- ハードコーディングされたパスワード ＊
- 未使用のコード ＊
- ログファイルによる情報の露出 ＊
- エラーメッセージによる情報の露出 ＊
- プライバシー違反 ＊
- 既知の脆弱性が存在する、または安全性の低い暗号アルゴリズムの使用 ＊

※ 記載の脆弱性は一例
※ ＊はブラックボックステストでは検出されにくい脆弱性

る運用者が見ていた場合、パスワードなどの情報を流してしまったり、アカウントを乗っとったり、なりすましの投稿をするといったことが考えられる。また、ユーザが同じパスワードで他のサービスを利用していると、そのサービスでもログインされて被害を受ける恐れもある（リストアタック）。本件に関しては正確に言うとパスワードは流出していないが、別のケースでは顧客情報が流出してしまったこともある。OWASP が、<プライバシー違反>による情報流出のケースとして、2003 年 4 月～2004 年 4 月、米・AOL の元従業員が顧客名とメールアドレスをデータベースから盗み売却した事件を挙げている[2]。犯人が企業に支払うことになった損害賠償金は膨大であり、顧客対応にかかった費用は相当なものだったと考えられる。

情報セキュリティ関連の事件は海外に限ったことではなく、国内でも後を絶たない。脆弱性に対する認識やセキュリティ対策不足が原因で起きるケースも多く、外部からのセキュリティ診断やソースコード診断で未然に防止できた可能性があったと推測される事例もある。海外でのケース同様に顧客対応に要した時間や費用は計り知れないことはもちろん、社会的な信用を失ったことはいうまでもない。

ソースコード診断と外部からのセキュリティ診断を自動車に例えるなら

Web アプリケーションについては、開発段階からシステムの内部構造を考慮したホワイトボックステスト（＝ソースコード診断など）を実施し、さらに運用段階で既知の脆弱性について外部からのブラックボックステスト（＝Web セキュリティ診断）も行うことが理想といえる。自動車に例えるならば、ホワイトボックステストは車を解体して、または設計書などをもとに部品や仕組み、連結方法、電気の流れる経路等を調べる検査で、ブラックボックステストは車検のように車を解体せずに外側から行う動作確認を含めた検査といったところだろう。（図 3）

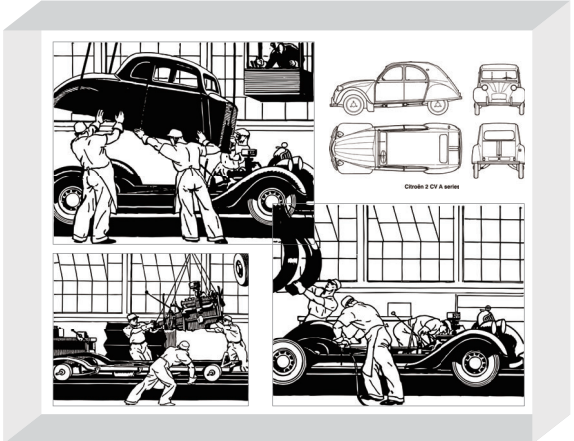
車を設計して、工場で作っているうちならいくらでも修正はできるが、出荷されて問題が発覚してしまったら、解体して洗いざらい調べなくてはならなくなる。出荷後の不具合への対応は、リコール、顧客対応、修正にとどまらない。修正したとしても一部分を直せば影響が別の部分に出ることも考えられる。費用のことを考えても、断然設計段階での修正の方が安く済むだろう。

Web アプリケーションに関しても同様で、例えば「ソースコードの○行目に問題がある」（次ページ図 5）など、ピンポイントで修正すべき箇所や原因が早期にわかり、前述の事例のような手遅れの状態になってしまう前に適切な処置を施すことができる。これはシステム開発のライフサイクルにおいて、セキュリティを考慮する段階を早めようとする概念 “シフトレフト” に相当する。上流工程でセキュリティ対策をした場合と、運用後に対策をしなければならなくなった場合を比較すると、運用後のコストは上流工程での対策の 60～100 倍ほど掛かると言われている。（次ページ図 4）

なお、ホワイトボックス、ブラックボックスの両面から診断を実施することで、より柔軟なセキュリティ対策を実現できる。例えば、古いシステムの改修に関する意思決定では、ソースコード診断を通じて、未使用のコードや廃止された関数が使われてはいるが相対的

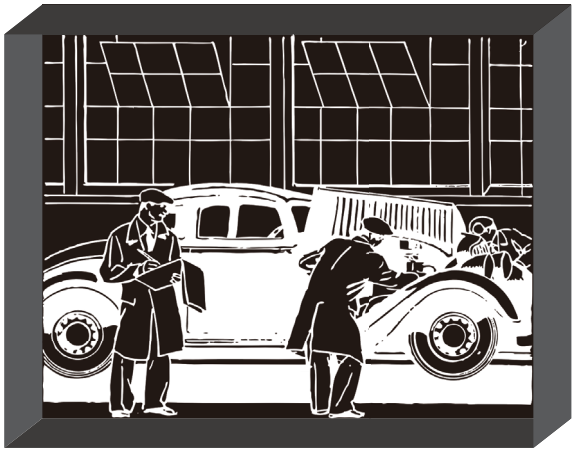
図 3　Web アプリケーション診断を車の検査に例えるなら…

ホワイトボックステスト



解体したり、設計図を見たりして、車を構成する個々の部品や部品同士の連携、仕組みを等を検査

ブラックボックステスト



解体せずに、車内外の見えている部分や想定される動作等に関する検査

図４　シフトレフトとは？

・システム開発のライフサイクルにおいて、セキュリティを考慮するフェーズを 早めようとする概念

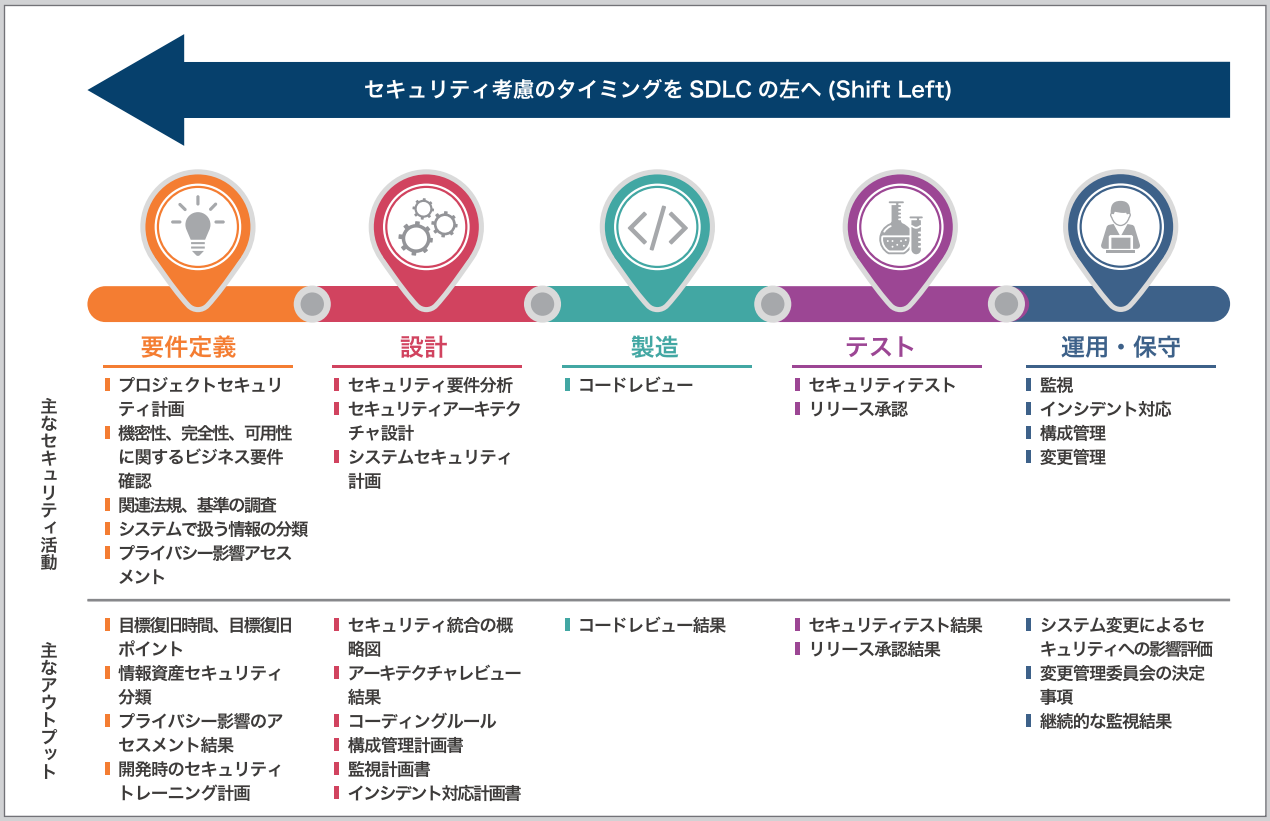


図５　ソースコードの問題箇所の例

```
3       $pass = $_GET['passowrd'];
4     ?>
5
6       ログイン ID:<?= $id ?>が登録されました。
7     <?
8       error_log($pass);
9     ?>
```

ソースコード診断の結果、ピンポイントで８行目の赤文字部分に問題があることを特定することができる。

に問題点は少ないと考えられる場合は直して使う、システムがつぎはぎのようなプログラミングで作られていたり開発者の考えたロジックを読み取れなかったり等で問題点が多すぎると考えられる場合は全てを作り変える、といった判断材料を得、並行してブラックボックステストを実施する。両面から評価を行うことで、コストや時間を最適化しながらシステムの堅牢性を高めるための取り組みが促進されるといえよう。

ガイドラインや法規制の基準を満たすためにも

ガイドラインや法規制には IT セキュリティの観点で推奨している検査があり、外部からのセキュリティ診断とソースコード診断をしておけば基準を満たすこともできる。国土交通省が策定している重要インフラにおける情報セキュリティ確保に係るガイドライン[3] のうちの“鉄道分野における情報セキュリティ確保に係る安全ガイドライン第３版”[*4] を例に挙げると、SQL インジェクション、OS コマンドインジェクションなどといった脆弱性も含め、Web 導入時にセキュリティ対策を講ずることが望ましいとしている。この中には「レースコンディション脆弱性」といった外部からの診断で検知することが難しい項目もある。ソースコード診断と外部からのセキュリティ診断で網羅されることになるので、どちらの診断もしておくことに越したことはないだろう。

また、クレジットカードの加盟店やサービスプロバイダにおいて、クレジットカード会員データを安全に取り扱うことを目的として策定されたクレジットカード情報保護の世界基準・PCI DSS (Payment Card Industry Data Security Standard)[*5] を遵守するためにも、内部と外部からの診断は有効だ。ソースコードのレビューや、社外に依頼するソースコード診断に焦点を当てると、要件 6：Develop and maintain secure systems and applications（安全性の高いシステムとアプリケーションを開発し、保守する）に、コー

ディングの脆弱性がないことを確認するためのリリース前のコードレビューを推奨する記載がある。コードのセキュリティに問題があると、悪意のある者によってネットワークにアクセスされ、カード会員データを侵害するために悪用されるため、コードレビューの知識と経験がある者がレビューに関与する必要がある、と述べられている。

さらに法規制絡みの話題では、欧州連合（EU）により 2018 年 5 月から施行された “一般データ保護規則（GDPR）”、その特別法として位置づけられる “e プライバシー規則（ePrivacy Regulation）” による影響は、もちろん日本企業にも及ぶ。違反した場合は日本円にして 26 億円以上もの巨額の制裁金が科される場合もある（* 詳しくは P.15 ～最新動向を参照。）のだが、適切な対策をしているのとしていないのとでは、その制裁リスクに雲泥の差が出る。というのも、罰則規定では企業としてどれほどのリスク対策をしているかどうかが基準になり、対策をしていたがどうしても防ぎようがなかったものに関しての責任は問われない。例えば、ソースコード診断や外部からのセキュリティ診断を実施していて、そのことが証明できれば、万が一事故が起きたとしても必ずしも巨額の制裁金を支払うことにはならないのだ。

Web アプリケーションのセキュリティ診断には複数の方法がある。それぞれの特徴を知り、それらを効果的に組み合わせて使用できれば、コストを抑制しながらシステムの安全性をより一層強化できるであろう。いくつかのセキュリティ対策を検討し、自社システムにとっての最善策がソースコード診断だと感じるならば一考してみてはいかがだろうか。

出典：

[1] https://blog.twitter.com/official/ja_jp/topics/company/2018/account_secure.html
[2] https://www.owasp.org/index.php/Privacy_Violation
[3] http://www.mlit.go.jp/sogoseisaku/jouhouka/sosei_jouhouka9999.html
[4] http://www.mlit.go.jp/common/001127563.pdf
[5] http://www.jcdsc.org/pci_dss.php
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

GDPR に続く e プライバシー規則

個人データの“セキュリティ正常化”を目指すグローバルスタンダードとは

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

2018 年 5 月 25 日、欧州連合（EU）により一般データ保護規則（GDPR：General Data Protection Regulation）が施行されたのは既にご存知のことだろう。国内では GDPR への対応に困惑している企業も少なくない。

これに加えて、もう一つの個人データ保護規則として EU が提案している e プライバシー規則（Regulation on Privacy and Electronic Communications）、略称「ePrivacy Regulation」がある。eプライバシー規則は、2017 年 1 月に EU が公表し、GDPR と同タイミングでの施行を目指していたが、様々な方面から反対の声があがり、本稿執筆時点では未だ審議中だ。ソーシャルネットワーキングサービス（SNS）やダイレクトマーケティングにおける個人データの収集や利用についてプライバシー保護に関する議論が活発化する中、同規則の成立に向け、EU 理事会（Council of the European Union）で審議が続けられている。

はじめに

現在、国内のデジタルマーケティング市場は 300 億円超といわれている。[*1] デジタルマーケティングは、しばしば Web マーケティングと同様の意味に捉えられがちだが、両者の違いはその対象範囲にある。Web マーケティングの対象範囲は Web サイトに限定されるが、デジタルマーケティングは Web サイトだけでなくデジタルで得られるあらゆるデータや接点を対象とする。個人消費者は企業の Web サイト以外でも、様々なチャネルを保有し、時には自ら情報を発信するなど、消費行動が大きく変化している。例えば、ある商品を購入するために、SNS や口コミサイト、個人の動画から情報収集や価格比較を行い、商品の販売元以外のオンラインストアで購入、後日その商品について自らがインターネット上で紹介する、といった一連の流れは今や珍しいものではない。

また、デジタルマーケティング市場が急速に成長しているのには、スマートデバイスの普及が背景にある。こうした背景により、サービス販売網は国内に留まらずグローバルに伸展している。B to C サービスモデルにおいて、デジタルマーケティングの行動分析は重要な役割を果たしており、2022 年には 639 億円に達するほどの成長が期待されるのも頷ける。

しかし、こうした多様化が進む反面、収集された個人データは様々な用途で、時には好き勝手に利用されてきた。個人に何の断りもなく二次、三次利用されることも多く、売買の対象にもなっていることから、プライバシー保護の観点で幾度となく問題視されてきた。e プライバシー規則は、無法地帯となりつつある現状を“正常化”するための施策の一つだといえる。同規則が施行されると、これまでデータ主導型広告の収益に依存し

[*1] 矢野経済研究所「2017 年版 DMP/MA 市場～デジタルマーケティング市場の現状とビジネス展望」

てきたサービスは個人の同意なく自由にデータを利用できなくなるため、サービス提供に大きな支障が出る可能性がある。企業によっては、サービスの提供プロセスの再設計を迫られることになるかもしれない。

導入の背景

そもそも、GDPR やｅプライバシー規則など、個人情報を保護する法令がなぜ次々と成立していくのだろうか。EU が根幹とする人権の普遍的価値観は、1948 年に採択された世界人権宣言にある。「すべての人間は生まれながらに基本的人権を持つ」という考えのもと、世界人権宣言は 1976 年発効の国際人権規約で法的拘束力を持つことになった。欧州で最初のプライバシーに関する法令は、1953 年に発効された「欧州人権条約」の第８条だ。同条約は、世界人権宣言、国際人権規約と並び、EU のプライバシーの考え方の基礎となっている。世界人権宣言からｅプライバシー規則が提案されるまでの経緯をまとめた年表は表１のとおり。

リスボン条約により法的拘束力を持つこととなった「EU 基本権憲章」は、欧州人権条約に規定された基本的な権利に加えて、「個人データの保護権利」等、時代の変化に応じて保護が必要となっている新たな項目が含まれている。同憲章第８条１項では、「すべて人は、自己に関する個人データの保護に対する権利を有する」と規定されており、欧州では、プライバシーは、すべての人が持つべき基本的人権として捉えられている。

GDPR は、この８条を守るために施行され、現在審議中のｅプライバシー規則は同７条「すべて人は、私的ならびに家族の、生活、住居および通信を尊重される権利を持つ」を守り、基本的人権として個人データを保護するという考えに基づいている。

GDPR とｅプライバシー規則

GDPR とは、欧州経済領域（EEA）域内に所在する個人のデータ保護を目的として、事業者に対し、そのデータの「処理」と「移転」に関するルールを定めた規則である。これまでのデータ保護指令（Directive 95/46/EC）では、指令に基づき各国が具体的な内容を定めており差異が生じていたが、GDPR は EEA 域内共通の法規制となる。GDPR の特徴は以下のとおり。

- 保護される個人情報の定義が極めて広く、個人の人種・民族・宗教・思想や医療情報などの特定の情報の取り扱いについて、極めて厳しい制約がある
- EEA 域内の個人に対して次ページ図１のような活動を行っている場合、法人の所在地にかかわらず、GDPR への対策の必要がある
- 個人情報の取り扱いについて、訂正の権利、削除権（忘れられる権利）、制限権、データポータビリティの権利、異議権といった権利が付与されている
- GDPR の規定を遵守せずにいた場合、最大で 2000 万ユーロまたは全世界年間売上高の 4% 以下のいずれか高い方を基準として制裁金を科される可能性がある

保護される個人情報の広い定義、厳

表１　世界人権宣言からｅプライバシー規則が提案されるまでの経緯

年月	条約、指令、規則等
1948 年 12 月	世界人権宣言採択
1953 年９月	欧州人権条約発効
1976 年１月、３月	国際人権規約発効（1 月：A 規約、３月：B 規約）
1980 年９月	OECD（経済協力開発機構）プライバシーガイドライン採択（理事会勧告 8 原則）
1980 年９月	欧州評議会、個人データの自動処理に係る個人の保護に関する条約（条約 108 号）採択
1993 年１月	「人、資本、サービス」の自由な移動および共通市場の形成実現を目指す「単一市場」の発足
1995 年 10 月	GDPR の前身にあたるデータ保護指令（Directive 95/46/EC）採択
2000 年 12 月	EU 基本権憲章公布
2000 年７月	ｅプライバシー指令（2002/58/EC）制定
2009 年 12 月	リスボン条約発効 (EU 基本権憲章に法的拘束力を付与)
2011 年４月	「デジタル単一市場（DSM）戦略」の主要分野を発表
2015 年５月	「欧州デジタル単一市場戦略」公表
2016 年４月	一般データ保護規則（GDPR）採択
2017 年１月	欧州委員会、ｅプライバシー規則案を公表
2017 年 10 月	欧州議会、修正したｅプライバシー規則案を承認
2017 年 12 月	EU 理事会、ｅプライバシー規則の修正案を公表
2018 年５月	一般データ保護規則（GDPR）施行
2018 年７月	EU 理事会、ｅプライバシー規則の修正案を公表

しい規制、巨額の制裁金等が原因で、施行後には制裁回避で欧州から撤退する企業や、EEA からのアクセスを遮断するWebサイトが出るなど、世界各地で準拠をめぐる混乱が生じており、GDPR に企業がどう対応するかの判断には、暫くの時間がかかるものと見られている。

GDPR が個人データ全般に対する規制なのに対して、eプライバシー規則は電子通信データを対象としている。位置付けとしては、GDPR を補完するための規則であり、GDPR の特別法（lex specialis）とされている。電子通信データの定義には、「電子通信コンテンツ」だけでなく「電子通信メタデータ」も含まれる。「電子通信コンテンツ」とは、電子通信サービスでやり取りされるテキスト・音声・画像・動画等のデータであり、「電子通信メタデータ」とは、「電子通信コンテンツ」をやり取りする目的で処理されるデータで、通信の日付・時間・期間・場所・種類や通信元や通信先を識別・追跡するため使用されるデータを含む。その代表的な例が Cookie で、e プライバシー規則は Cookie の使用の規制に重点を置いていることから、通称「Cookie 法」とも呼ばれている。

eプライバシー規則の概要

e プライバシー規則が適用される対象は表 2 のとおりで、この適用対象に企業や業界団体が懸念を表明している。

前身の e プライバシー指令では、電話、ファックス、IP 電話など従来の電子通信サービスを対象としていたが、e プライバシー規則ではそれに加えて、VoIP、メッセージングサービス、Web メール等の OTT（Over the Top）サービス（例：YouTube、Facebook、Twitter、Line、Messenger、Hulu、Netflix、Amazon）も対象となっている。また、適用対象はさらに拡大される可能性があり、M2M 通信（機器間の通信）にも、特に通信の秘密に関する要件が適用されるべきとしている。

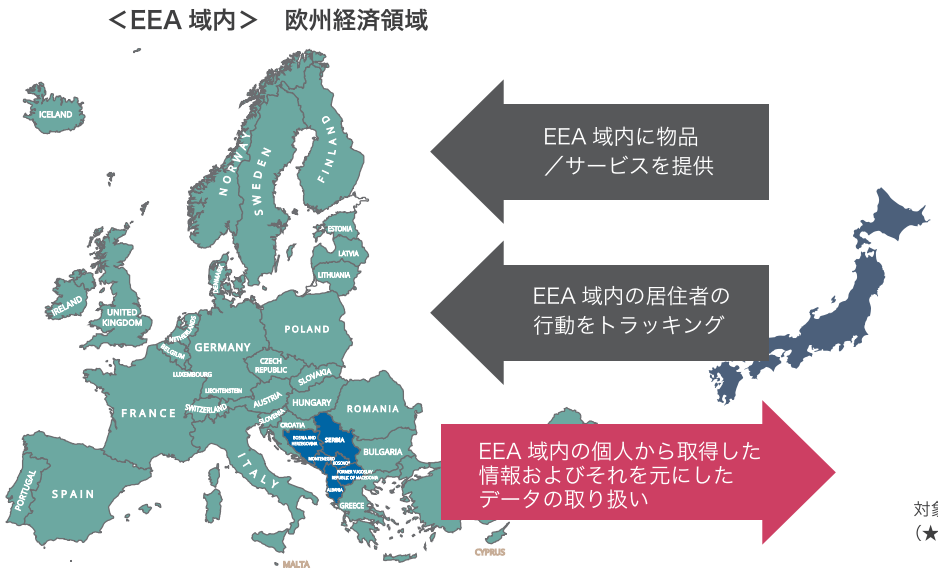
e プライバシー規則は企業活動に大きな影響を与える。主なポイントは図２のとおり。

通信の秘密との関連性

従来、「通信の秘密」は、ISP や通信事業者等が適用対象であり、電子通信データの秘密および保護は加盟国の国内法において確保することが定められていた。「通信の秘密」とは、利用者本人以外の者に対し、当該データを傍受、監視、あるいは取り扱うことを原則禁止するものである（犯罪の捜査や防止を目的とした所轄官庁による活動、特定の利用者のみが使用する社内ネットワーク等は適用対象外）。本稿では、禁止の例外となる場合について詳しく言及しないが、「サービス提供・契約履行に必要な場合」、「セキュリティ維持や復元、技術的障害やエラー、攻撃の発見に必要な場合」、また「エンドユーザの同意がある場合」等は取り扱いが可能となる。

e プライバシー規則では、適用対象の拡大に伴い、これまで対象ではなかった OTT サービスや IoT 機器にも、この「通信の秘密」が適用される。なお、これらの電子通信におけるデータ処理が EU 域外で行われていたとしても、EU 域内で電子通信サービスの利用者への提供や電気通信サービスの利用があった場合には適用範囲に含まれることに注意が必要だ。サービスの提供者が EU 域外の企業の場合、EU 域内に代理人を設置することが義務付けられる。この代理人は代表権を持ち、所轄官庁や裁判所、利用者へ情報提供を行う

図 1　GDPR の施行は日本の企業活動にも影響する



＜EEA 域外＞　日本

アイルランド	スロバキア
ベルギー	イタリア
スロベニア	ポーランド
英国	チェコ
ポルトガル	エストニア
アイスランド★	マルタ
オーストリア	リヒテンシュタイン★
ラトビア	オランダ
デンマーク	リトアニア
キプロス	ドイツ
ルーマニア	ギリシャ
ハンガリー	ルクセンブルク
クロアチア	フィンランド
ノルウェー★	スウェーデン
フランス	スペイン
ブルガリア	

対象となる国・地域、および対象となる活動
（★は BJ 非加盟国で EEA 加盟国）

出典：European Environment Agency　https://www.eea.europa.eu/about-us/countries-and-eionet

機能を有していなければならない、としている。（次ページ図３）

e プライバシー規則が施行されると、M2M 通信も「通信の秘密」の適用対象となる可能性がある。M2M（Machine to Machine）通信とは、機器間の通信を意味し、機器同士が人間の介在なしに情報の交換を行い稼動するシステムのことである。例として車の自動運転システムや無人の警備システム、ゲームアプリ等があげられる。端末機器から送信される情報の取得や処理は原則禁止され、ユーザの同意がある場合や、電子通信上必要な場合等のみ、例外的に可能とされる。

加えて、端末機器に保存されている情報の取得や処理も原則禁止となり、以下のような対策が求められる。

1. 事業者による、端末機器からの情報取得をしないような体制構築
2. 端末機器製造者による、本規則案に合致した機器の製造および既製品の改良
3. アプリケーション作成者による同様に本規則案に準拠した製品の作成
4. ２～３とも、端末機器・アプリケーションを使用するエンドユーザが使用時に本規則案に違反することのないよう注意

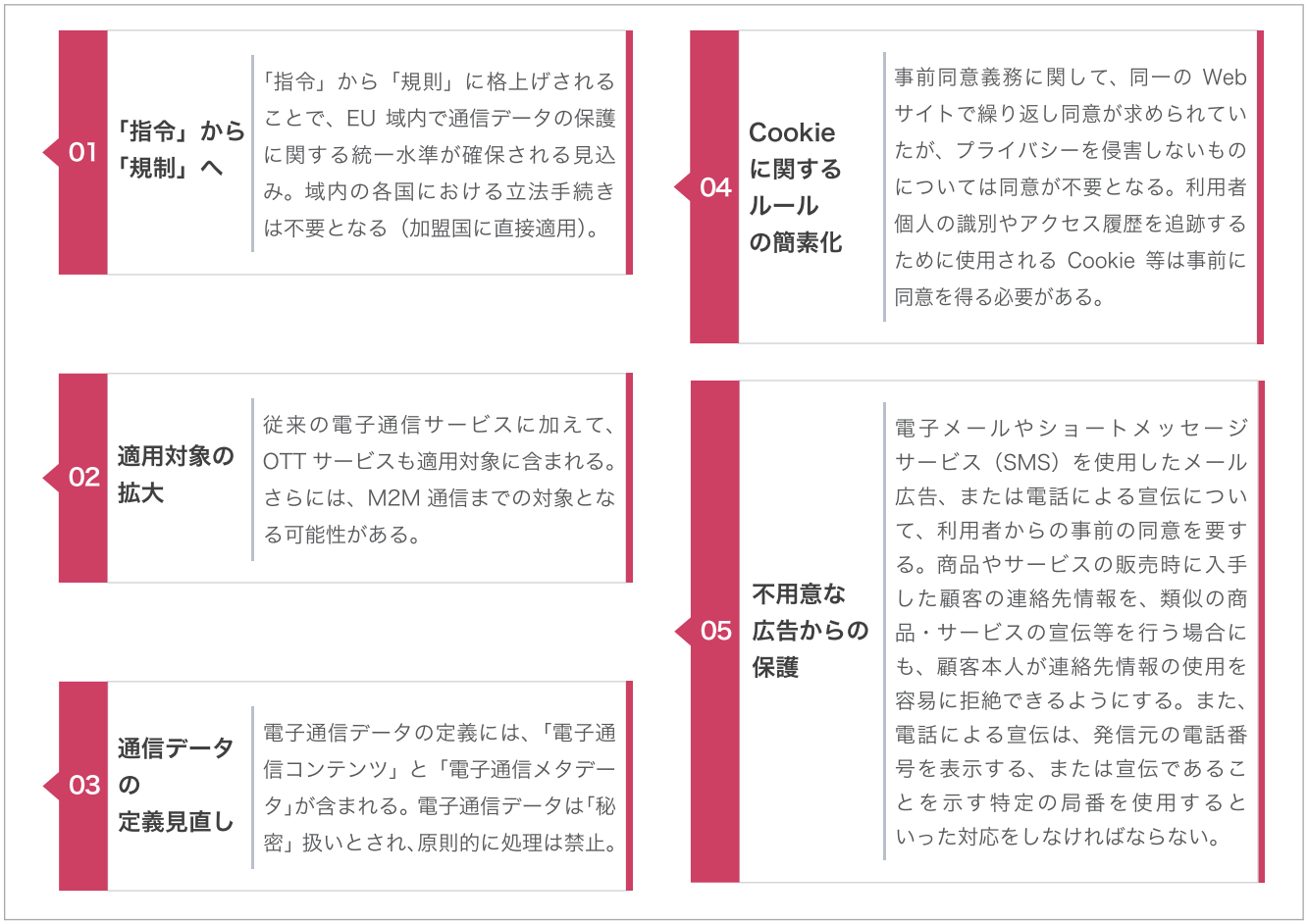
表２　適用対象

- ☑ 電子通信サービスの提供・使用に関連して送信される電子通信コンテンツの処理、および、同サービスの提供・使用に関連して実行されるメタデータの処理
- ☑ エンドユーザが所有する端末機器で処理、送信、保存される情報
- ☑ 電子通信が可能なソフトウェアの販売
- ☑ 電子通信サービスのエンドユーザに関する公開ディレクトリの提供
- ☑ ダイレクトマーケティングに関わる情報の送信、表示

【適用外】刑事司法活動や、社員のみが使用する非公開の電子通信サービスは適用の対象外。

電子通信データの取り扱いについて、e プライバシー規則では、保存や消去に関しても定めがある。まず、電子通信データの取り扱いは、基本必要な期間に限り使用が認められていること。また、電子通信コンテンツは、通信先が受信した後は消去または匿名化する必要があり、電子通信メタデータについても送信が不要となった時点で消去または匿名化しなければならない。匿名化されたデータではサービス提供が行えない場合等には、事前にエンドユーザから同意を得る必要がある。ただし、エンドユーザから委託を受けた第三者は、（GDPR に従い）電子通信コンテンツやメタデータの記録や保存を行うことが可能とされている。

図２　e プライバシー規則の主なポイント



ダイレクトマーケティングにおける Cookie の利用

企業のサービスサイトにおいて、Cookie に含まれる個人データの利用目的は、大きく分けて二つある。一つは、ユーザの利便性向上であり、Web サイトでユーザ情報を保存することで、例えば次回訪問の際も以前の情報を閲覧できる。

もう一つは、広告配信への活用だ。ユーザの閲覧情報を Cookie に保存しておき、ユーザの個人情報を Cookie から推測して表示するターゲット広告や、別のサイトと連携している場合に、そのサイトの訪問時に過去に閲覧した商品を表示するリターゲティング広告等がある。これら方法はデジタルマーケティングの主流であるダイレクトマーケティングとして現在広く使われている。

しかし、e プライバシー規則では、ユーザの同意がない限り、自然人であるエンドユーザに直接的なマーケティングコミュニケーションを送る目的での電子通信サービスを禁止している。広告配信におけるユーザの興味や行動を収集・追跡するサードパーティ Cookie などは規制され、事前の同意を得ない限り使うことはできない「オプトイン方式」が必要とされている。また、簡単かつ効果的に Cookie の取得を拒否できる手段を提供しなければならない。

つまり、ポップアップ等で Cookie に同意するかどうかの表示を出しチェック欄を設けるなど、ユーザの積極的で明示的な同意が必要とされる。なお、利用に同意を得られなくとも、同意を得た場合と同様の Web サービス提供が必要（トラッキングウォールの禁止）となる。

事業者は、同意に先立ち Cookie による個人データ取得の目的や期間・リスク等について明らかにする必要がある。事業者によって個別具体的対策が異なるであろうが主なものとして、以下があげられる。

1. 「オプトイン方式」のインターフェースに変更すること。
2. Cookie の利用方法等についての情報提供の整備
3. 1. と 2. は可能な限りユーザフレンドリーである必要。ブラウザや他のアプリケーションを使用することで同意できる形にするようにすべきであり、その同意があらゆる第三者を拘束し、かつ適用できるものにシステムを構築する必要がある。
4. 事業者には同意の証明責任がある。つまり事業者が、同意があったことを記録に残しておらず証明できない場合、争いが生じた際、責任は事業者が負うこととなるため、記録を管理・保存するシステム構築が必要。
5. ユーザには、同意の撤回権があるため、権利行使された場合ただちに削除等、処理できる体制も必要。

Google を例にあげると、同社は Cookie の使用制限に対応した「非パーソナライズド広告（nonpersonalized ads）」という個人情報を使わないターゲット広告を導入する計画を明らかにしている。海外の広告業界では共通の同意型プラットフォームを設置するなど対応に追われている。複数の日本企業においても、個人情報を収集せずにターゲット広告を作成できる技術を開発するなど、対応を模索している最中だ。

制裁金について

e プライバシー規則に違反した場合、GDPR と同じく最大で日本円にして約 26 億円か世界の売上高 4％の高い方という制裁金が科される可能性がある。

制裁金は巨額となることが予想されており、企業にとっては非常な脅威である。さらに制裁金を支払ったことによるレピュテーションリ

図 3　サービスの提供者が域外の場合、EU 域内に代理人を設置することが必要

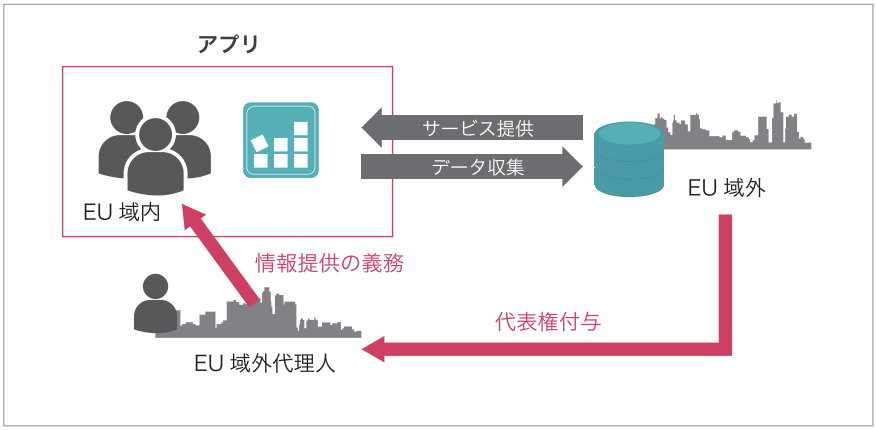
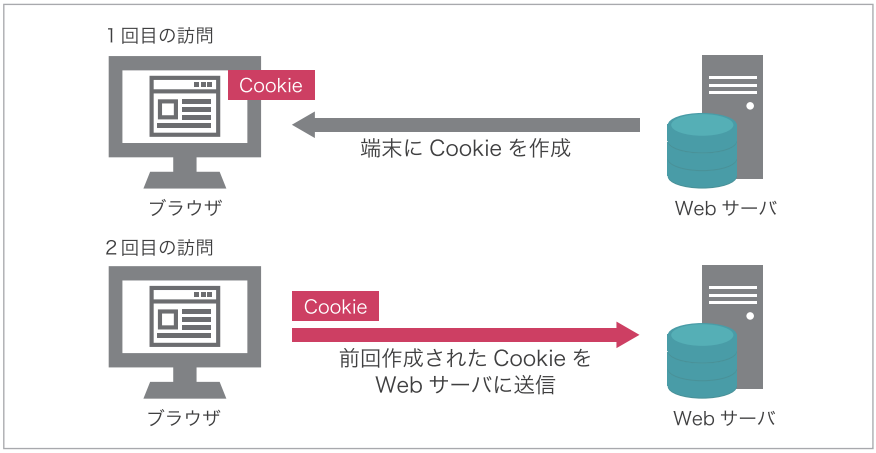


図 4　Cookie の仕組み



スクも深刻だ。プライバシー保護強化への流れが変わらない以上、もっとも厳しい法令にあわせた水準での社内体制構築が、事業活動の継続には欠かせないだろう。

事前の対応が急がれる

既に述べてきたように、eプライバシー規則は大きなビジネスインパクトを与えるだろうことが容易に予測できる。企業は、まず自社で取り扱う電子通信データについて正しく把握しておくことが必要だ。例えば、アプリケーションの動作が本規則に準拠しているか、Webサイトが EEA 域内のエンドユーザから情報を取得していないか、ダイレクトマーケティングが EEA 域内に及んでいないか、GDPR に基づいた製品やサービスの販売コンテクスト以外の方法で取得した電子メール等の個人データを利用していないか、などである。

自社の現状分析を行った後は、eプライバシー規則に抵触するリスクがあるものについて、早期対応を検討することが重要だろう。システムの改修、電子通信データの管理体制構築、ユーザからの問い合わせに対応できるシステム構築など様々な面での検討が必要となるかもしれない。

e プライバシー規則において、仮にインシデントが発生しても、制裁金を抑えるポイントは、適切な対策をしているかどうかである。

表 3　違反した場合の課徴金

違反項目	課徴金
- 電子通信データの処理に係る違反 - ソフトウェアプロバイダーの義務違反 - 公開ディレクトリに関する違反 - 電子通信サービスの利用に係る違反	1,000 万ユーロまたは 前会計年度全世界年間売上高の 2% のいずれか高い方
- 通信の秘密の侵害 - 通信の秘密の例外の濫用 - 電子通信データにおいて必要な消去を行わなかった場合	2,000 万ユーロまたは 前会計年度全世界年間売上高の 4% のいずれか高い方

しかし対策には、相応のコスト・時間がかかり、各部門個別では対応しきれないだろう。リーダーシップを取ることができる組織を中心に、企業全体で対応していくことが重要である。

おわりに

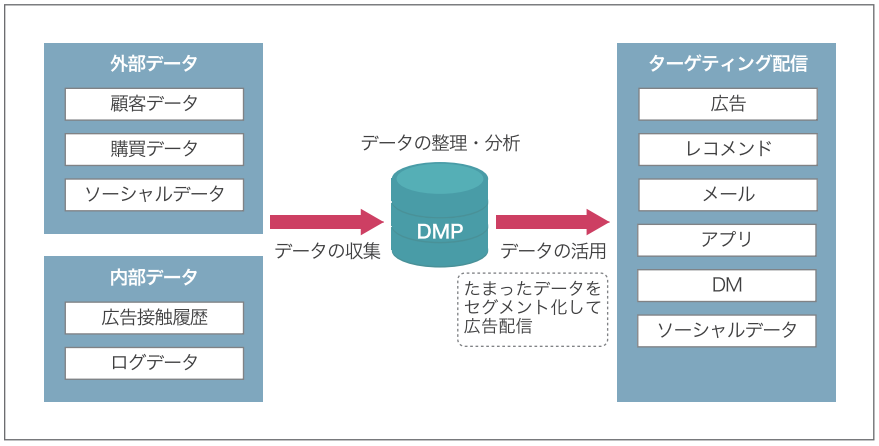
プライバシーに関する考え方は各国で隔たりがあることに加え、eプライバシー規則に対する反対意見も多くの企業や組織から発せられているが、EU 発のプライバシー保護の流れは、今後グローバルスタンダードとなっていくだろう。

冒頭でも述べたとおり、EU は個人データを普遍的価値観である基本的人権として、プライバシー保護の先駆者として本来あるべき形に戻そう、つまり正常化しようとしている。EU 圏外においても、追随するように個人データの取り扱いに関する法案が次々と提出されている。個人データの無法地帯であったデジタル世界に終止符を打つ時が来たようだ。

ソフトウェア開発においては、電子通信および Web ブラウザを許可するすべてのソフトウェア（アプリケーション）は、インストール時に、第三者による情報の保存を防止するオプションを含むプライバシー設定についてユーザに情報提供しなければならない、といった「Design by Privacy」コンセプトが提唱されている。これは、保護対策を後付けで行うのではなく、最初から組み込む考えだ。

事業でインターネットを活用する企業に今後求められるのは、エンドユーザのプライバシーが守られることを保証する、信頼度の高いサービスである。安定した事業継続のためには、IT システムで電子通信におけるプライバシー保護を実現すると同時に、経営課題としてプライバシー保護に対する認識を企業全体に徹底させていかなければならない。経営層が率先して取り組むのはもちろんのこと、eプライバシー規則に精通したコンサルタントや弁護士などの外部人材を確保しておくことも必要になってくるだろう。eプライバシー規則の今後の行方について注意深く追うとともに、時代の流れに取り残されないよう、今できることから進められてはいかがだろうか。

図 5　DMP（デジタル・マーケティング・プラットフォーム）のしくみ



音に対するハッキング

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

声で操作できるIT製品がいつのまにか身近な存在となりました。
「OK Gxxxle 洗濯物取り込んでおいて」で、誰かが席を立たなくても済むような世界が近い将来実現されるのでしょうか。
今回は音の利用をテーマとしたセキュリティについて書いてみます。

最近のセキュリティ事情について

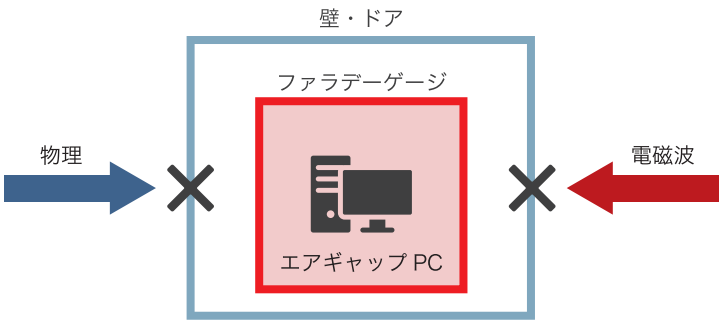
先日、引っ越ししたばかりの友人宅に呼ばれたのですが、夜中2時過ぎでしょうか。友人が近くのコンビニまで買い物に出かけるというので、その間ひとりで過ごしていたところ、ふと首筋に冷たい風があたるんですね。振り向いても誰もいないんです。こんなことが何回か続くので、おかしいなーおかしいなー、怖いなー怖いなーと思って、戻ってきた友人に訪ねてみました。熱源感知するエアコンだそうで、ひとりになったので、ピンポイントに冷風で狙われていたというオチです。スマート家電すごい！と感じた、とある夏の1日の出来事でした。

熱や音を感知するセンシング技術は私たちにとって身近な存在となり、様々なデバイスに活用されています。これらが組み込まれたスマート家電は、個人の生活情報を把握（監視）し、より豊かで便利な生活を提供していくものなのでしょう。

「音」に関するセキュリティ〜エアギャップを超えて〜

今回は前述のセンシング技術に関連し、最近の情報セキュリティ周りでも話題となった「音」に関係する事柄について書きたいと思います。

2018年3月、イスラエルのベン・グリオン大学の研究チームによって、超音波を使って秘密裏にデータを転送する「MOSQUITO」という手法が公開されました。この手法の特筆すべき点は、エアギャップされたPC間であっても超音波を使うことでデータ転送が可能であることを実証したことにあります。エアギャップとは（図1）のように、システムをインターネッ



*1 ファラデーゲージ

過去にはNSA（アメリカ国家安全保障局）のスキャンダル告発者であるエドワード・スノーデン氏が、盗聴防止のため携帯電話を冷蔵庫に入れるよう指示したとの嘘か真かわからない話もあります。ハードボイルド小説の1シーンのようですが、これもファラデーゲージとしての期待があったのでしょう。なお、最近はファラデーケージのDIYキットが数千円〜数万円で手に入りますので、夏休みの自由研究などにオススメします。

僕の試した製品は50%くらい着電しましたので、まぁこんなものか・・・というものでしたが。

図1　エアギャップとは

トやローカルエリアネットワークから隔離し、ファラデーケージ[*1]で覆い、電磁波パルス（EMP）や太陽フレア等の影響を遮る処理のことです。

通常であれば、エアギャップされたシステムからデータ転送するには、USB などでメディアを用いるか、ケーブル接続をしてアクセスする必要があります。しかし「MOSQUITO」手法では、情報を盗りたい対象システムのデータを超音波に変換し、スピーカやヘッドフォンから発信させ、発信された超音波を受信したシステムは、超音波から元のデータを復元させます。これにより、通常想定している転送方法以外で外部への情報送信が可能となります。そして、もともとマイクとして機能するように設計されていないスピーカやヘッドホンを、マイクとして機能するように改変し受信させることに成功しています。

エアギャップされたシステムとなれば、当然に高セキュア環境で用いられるものと皆さんも想像されることでしょう。事実、重要情報の保管された端末・システムは、安全でないネットワーク（インターネット含む）と隔離し、外部ネットワークから不正にアクセスするサイバー攻撃から守ることが重要であり、セキュリティ対策をすすめている企業・団体では、インターネット分離ソリューションを採用するケースが非常に多く見られます。また、仮想通貨の漏洩・消失といった事件・事故でも、その対策としてコールドウォレット[*2]が必須とされています。「便利のための接続」よりも「守るべきものの隔離」をより明確にする対策へシフトしていることは疑いようもありません。2018 年 5 月 4 日にはアメリカのサイバー軍が統合軍に格上げされ、「サイバー戦争」が言葉だけでなく現実味を帯びてきました。より高度なセキュリティ対策が求められる環境では、強力な電磁パルス（EMP）を利用した攻撃も想定する必要があり、エアギャップの重要性は増しています。

このような高度なセキュリティ対策がなされたシステムであっても、例えば出荷時や設定時に悪意あるソフトウェアが仕込まれてしまった場合、直接アクセスできずとも、情報窃取できる可能性があることを「MOSQUITO」手法は示しています。いささか大仰な話からはじめてしまいましたが、これまで注力してきたネットワークからの攻撃への対策だけでなく、物理現象を利用した攻撃についても、情報を守る側はいち早く情報をキャッチし、潜在的な脅威とリスクを把握することが求められているのだと、改めて意識するきっかけになればと思っています。

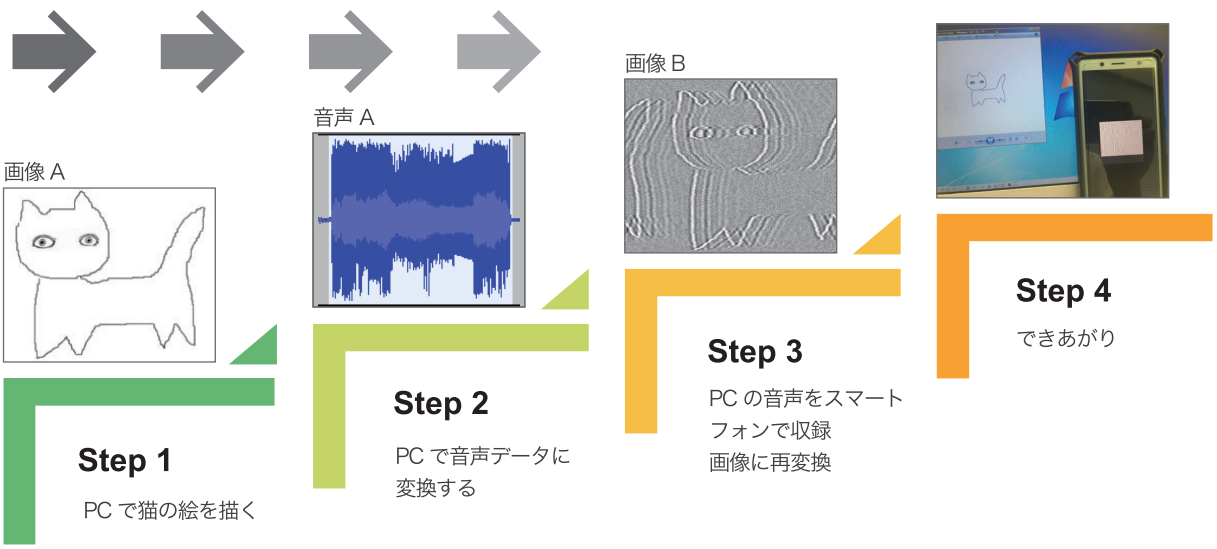
[*2] コールドウォレット

インターネットからの不正アクセスに対して仮想通貨を安全に保管するために、ネットワークから隔離しオフラインで管理するウォレットです。利便性は低下しますが、近年の仮想通貨への不正アクセスを鑑みると必須の対応といえます。

「音」に関するセキュリティ ～エアギャップを超えて：実験編～

前述の内容について、PC とスマートフォンで簡単な実験（図 2）をしてみます。まず、PC で（画像 A）のような絵を用意します。ねこです。次に、画像を音声に変換するプログラムを書き、先ほどのねこの画像を（音声 A）に変換します。PC で音声 A をスピーカから鳴らし、スマートフォンで録音します。スマートフォンで録音した音声 B を、音声から画像に変換するプログラムで変換した結果が（画像 B）です。結果、ノイズが多く上手くいったとは言えませんが、ねこがいます。おわかりいただけただろうか？

図 2　物理現象を利用した攻撃の実験



ノイズのフィルタリングなどをせず、可聴域の音声で実験したため、このような結果となりましたが、超音波帯の利用を限定することで、ノイズの影響などを極力受けずに転送することが可能と思われます。今回の実験では、音声を用いたデータ転送が想像よりもずっと容易であることが判りました。

重要情報を取り扱う環境への携帯電話・スマートフォンの持ち込みを禁止することは、セキュリティ対策上とても大事なことです。しかし、携帯電話・スマートフォンがこれだけ重要な連絡手段として確立された現代においては、持ち込み禁止を徹底することが困難な状況があるかと思います。このため、重要情報を取り扱う環境へ、たとえ携帯電話・スマートフォンが持ち込み可能であっても、カメラが利用できないように、カメラのレンズ部分にシールを張る対策がとられている場合や、画面をカメラで写すといった動き（明らかに挙動不審ですね）を、監視によって防止する取り組みが行われています。

しかし、今回のように音声でデータ転送されることへの対策が行われている環境は稀ではないでしょうか。音声（超音波）を録音する設定にした携帯電話・スマートフォンの検出は、カバンやポケットに入れられてしまうと難しそうです。

[*3] チェックポイント 3

「マイ QR コード」画面の Bluetooth マークの右隣にある「波マーク」がソレです。先日調べたときは、Android に実装されているのを確認しましたが、iOS 版には見当たりませんでした。経緯・状況をご存知の方がおられましたら教えてくださいますと嬉しいです。

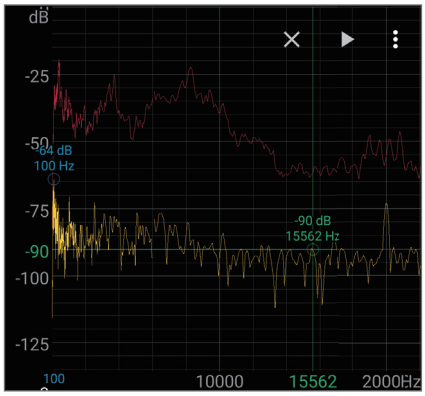
また、（エアギャップを超え）ドアの向こうにあるデバイスまで管理するとなると、なかなかに骨の折れる仕事となりそうです。ですが、今後考える対象から外すことは推奨いたしません。

ドキュメントを画像・音声ファイルに偽装する、情報を画像・音声ファイルに埋め込むなどで、機密情報を持ち出す手法自体は古くから存在し、その手のツールはインターネット上に溢れています。例えば、USB メモリなどで情報を持ち出す際、確認された場合でもバレないよう偽装しておく･･･といった悪巧みの背景が容易に想像できます。今回は、USB 接続やケーブル接続が出来ない対象であってもデータ転送が可能であり、外部への情報漏洩が起こりうることを検証しました。そして、ここで忘れてはならないのが、PC のマイク機能を使い「データを送り込むことも可能」なことです。USB ポートも塞いだ、ネットワークからも隔絶した、なのに、いつの間にかマルウェアに感染していた・・・といったことが起こるのも遠くない未来の話かもしれません。信じるか信じないかは・・・。

「音」に関するセキュリティ ～身近なケース～

「音（超音波）」の利用について、身近なケースで考えてみましょう。超音波は 20kHz 以上の音波であって、人間の耳では聞こえませんが、コウモリやイルカは通常の生活に利用しています。コウモリは超音波を発して、その反響をもとに物体（自分や相手）の位置を把握しており、イルカは位置情報の把握のほか、仲間との会話にも利用しているとされています。また特性上、高解像度な探知に向いているとされ、距離の計測や医療現場での検査機器にも広く活用されています・・・と、まだまだ身近なケースではありませんね。皆さんは LINE アプリをご利用されています

図 3　スペクトラムアナライザの結果



でしょうか？国内では 7,300 万人以上が利用し、世界的には 2 億人以上のユーザがいるそうです。この LINE アプリでは友だちを追加する際に、ID 検索や QR コードなどが使用できますが、2015 年から超音波での友だち追加機能 [*3] も実装されています。

「マイ QR コード」画面を開いている間、自身の ID を通知する「超音波」を発信しており、受信側は QR コードリーダーを開いて「超音波」を受信し、友だち追加ができる仕組みとなっています。発信されている音をスペクトラムアナライザで確認（図 3）したところ、20kHz あたりにピークが検出されており、まさに「超音波」であることが判ります。

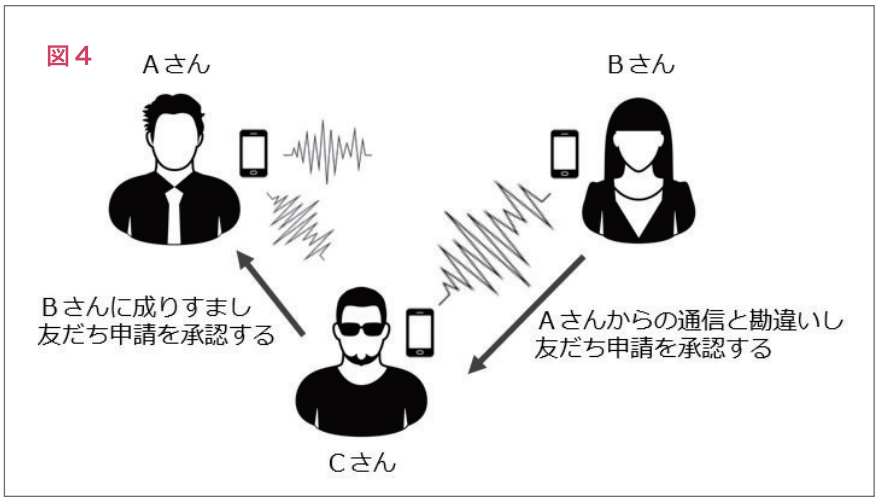
では、ここからセキュリティの観点（注：あくまで想像の範囲ですが）で話を進めてみたいと思います。「超音波」を利用して友だち追加をする際に、より高出力の「超音波」が邪魔をするとどうなるでしょうか。A さんが B さんへ ID を通知するには、A さん（「超音波」発信）ーB さん（「超音波」受信）となるわけですが、C さん（「超音波」高出力発信）がいると、B さんは A さんだと勘違いして C さんを友だち追加してしまうことが考えられます。また、C さんは A さんの発信した「超音波」を受信して友だちになります。すると、A さんは B さんだと勘違いして C さんを友だち追加してしまうことになります。この結果、C さんは、A さん

と B さんのメッセージのやりとりに対して中間者として存在することになります。（図 4）

実際に超音波の届く狭い範囲でこのような行為が可能かどうかでいうと、現実的ではありません。しかし、2018 年 4 月にサンフランシスコで行われた RSA カンファレンス "The Good, the Bad and the Ugly of the Ultrasonic Communications Ecosystem" で述べられたとおり、超音波による通信技術は現時点で明確な標準が存在せず、利用方法のコントロールが困難な状況にあります。現在の状況はもちろんのこと、今後の利用傾向についても私たちは注意を払っていかなければならないと思います。

「音」に関するセキュリティ ～まとめ～

音を使ったサイバー攻撃については、これまでにもさまざまな手法が報告されています。2018 年 5 月には、近くで大音量（100db 以上）を鳴らすことで、対象 PC をクラッシュさせることのできる「ブルーノート」攻撃が報告されました。これは、ハードディスクに実装されている衝撃センサーに誤作動を引き起こすことができるということで、数秒から百数秒と時間こそ幅があるものの、ハードディスクの搭載されている機器であれば PC だけでなく、監視カメラなども対象となるとの報告が上がっています。



なお、SSD（Solid State Drive）には影響しないとのことです。2008 年にはサン・マイクロシステムズの技術者が、稼働中のシステムに向かって大声を出して、ディスクに負荷をかけ、ディスク I/O にレイテンシを発生させた様子を公開しており、10 年以上前から「音」への耐性の懸念は身近な存在であったといえるでしょう。また、2017 年 8 月には、音声アシスタントで扱えるデバイス（Amazon Echo や Google Home、Apple Siri など）を、超音波を使って不正操作することが可能な「Dolphin-Attack」が公表されました。これらのデバイスは、基本的に人間の声にのみ反応するように作られていますが、超音波の共鳴によって生み出される倍音でも反応することが確認されたというものです。人の耳には聞こえない超音波によって、人の声に代わってデバイスへ指示を与えることが可能のため、現状は不正操作の検知が難しい領域にあるかと思います。このほか、2017 年 5 月にはインドの広告マーケティング会社が、TV コマーシャルで発せられる超音波のビーコンをアプリで受信し情報収集を行っているとの疑いがあり、調査レポートが発表されました。

音声・超音波技術を使った情報漏洩、破壊、スパイ活動など、調べはじめたらもう、最後まで興味は醒めることを知らず、今回は記事をまとめるのに苦労しました。「技術に対する悪巧み」の話は、私たち情報セキュリティに携わる者にうってつけの話で、もはや古典の風格すら感じられます。とにかく、拡げればどこまでも拡がっていきそうな話でありながら、それでいて持ち運び可能なサイズの本質を持っています。いつでも（帰りの電車の中でも、お風呂に入っているときでも）、あの技術をあーしてこーしてと、様々に思い浮かべてみることができるのは、わりと幸せなことなのでは？と思うのです。

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の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。

＜保有資格＞
CISSP、情報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、
情報セキュリティ監査人補

診断の現場から

セキュリティサービス本部 開発部 システム運用課
冨田　淳

<略歴>
異なる業種での経験を経て当社に入社。入社当時は情報セキュリティについては素人同然だったが、持ち前の向上心と溢れる好奇心、勉強意欲で現在はツール診断サービスの運用から管理、保守、契約顧客システムの診断、診断結果のチェック、検査シグネチャの開発や導入、脆弱性 DB 管理まで全般的に任せられるセキュリティエンジニアに成長。趣味は読書に音楽、昔はバンド活動も行っていたという。最近ではセキュリティも趣味の一つとなっている。また、休日には奥様と買い物に行ったり、先輩のご家族と家族ぐるみの付き合いをしたりと、人間関係を大事にする姿勢は仕事にも現れており、同僚や顧客からの信頼も厚い。

CPE　お客様に寄り添う診断

編集部員：装いも新たにリニューアルしました「診断の現場から」。今回はセキュリティサービス本部 開発部システム運用課の冨田淳さんにお話を聞きたいと思います。

冨田：よろしくお願いします。

編集部員：早速ですが、お仕事の内容についてお聞かせください。

冨田：主な仕事は、Cracker Probing-Eyes、略して CPE の運用となります。CPE は Web アプリケーション診断とプラットフォーム診断を、自動化されたツールで診断からレポート作成まで行うサービスです。CPE では、契約されたお客様に対して、指定された時間および周期で診断を行っています。その運用管理と診断結果チェックが基本的な仕事になります。また、数百社のお客様を日々診断していますが、そうしたなかで発生したさまざまな要望に応えるのも、重要な仕事の一つです。いわゆる一般的な“ツール診断”だと対象に通り一遍の診断をかけて終わりということが多いのですが、CPE では Web サイトに合わせて一つ一つ診断設定をカスタマイズするといったこともしています。

編集部員：自動化されたツール診断とはいえ、お客様との距離は近いということですね。

冨田：はい、そのとおりです。私の仕事は、日常的にお客様に寄り添う形になります。手動での診断に比べて制限等はありますが、可能な限り一番いい形でのサービスをご提供できるよう、お客様のご要望をツールの開発側に伝えたりであるとか、日々そのための診断手法のアップデートなども行っています。業務の範囲が多岐にわたるため、CPE の運用は、幅広い知識が必要になってくる仕事です。

趣味はセキュリティ

編集部員：そうした幅広い知識はどこで得ているのでしょうか。趣味の一つがセキュリティだとお聞きしましたが、それも関係あるのでしょうか。

冨田：趣味というか、アンテナを立てていると、新しい情報がいろいろ入ってくるじゃないですか。そういうのを調べたりするのが好きなんです。お昼休みもお弁当を食べながらセキュリティ系ニュースサイトを追いかけています。誰にも邪魔されたくない、私が一番大事にしている時間ですね（笑）。あとは、自分でも脆弱性を確認してみたくなり必要のない IoT 製品を買って妻に怒られたり、脆弱性関連の本を買い過ぎてまた妻に怒られたり、休日に家で脆弱性の検証していたところ、夢中で集中していたあまり、妻との約束をすっぽかしてしまい激怒されたこともあります。

編集部員：それはもう、趣味というよりマニアの域に達していますね（笑）。ちなみにそうして得られた知識は、社内で共有しているのでしょうか。

冨田：そうですね。社内で開かれる会議などで情報を発信して共有を図っています。情報は共有してチームで連携していくことでより価値が生まれてくると思っています。私は開発部の一員なので、最新技術を既存のシステムにどう組み込むか、そういった視点も重要です。今も CPE をさまざまな形で連携させていこうと工夫しているところです。

セキュリティは面白い

編集部員：セキュリティを趣味にしてしまうほどの冨田さんですが、以前は違う仕事に就いていたんですよね？

冨田：はい。もともとは広告代理店の営業でした。

編集部員：営業だったんですか！

冨田：はい。入社当初は、セキュリティに関する知識はゼロに近い状態でした。IT にもそこまで詳しくなかったですし、最初 BBSec を「他の人のサイトを攻撃する会社」だと思っていたくらいです（笑）。ただ、今思うと、他業種での経験は逆に自分の強みにもなっています。セキュリティって技術だけでは駄目なんです。お客様に正しく分かりやすく物事を伝えるのが大事なので。今でもお客様からのお問い合わせ対応などで以前の経験が生きているなぁと実感しています。

編集部員：そのような状態から、どうやってセキュリティの知識やスキルを身に付けたのですか。はじめはやはり苦労しました？

大丈夫だと思ったのに

© 槻木こうすけ

冨田：入社してすぐは、クローリングという診断の前段階の仕事を担当していました。診断をする上で対象のシステムを知るための非常に重要な過程ではあるのですが、何しろ単調で孤独な作業なんですよ（笑）。それほど飽きっぽい性格でもないのですが、隣で先輩たちが診断結果について「あーでもない、こーでもない」と議論していたり、「この方法は？」「いや、それよりこっちが…」なんて意見交換をしていたりするのを目の当たりにすると、それに刺激されて、自分もその輪に入りたくなったんです。

編集部員：そこから先輩に追い着こうと？

冨田：まずは、試しにクローリングを早く終わらせることに挑戦してみたんです。そして空いた時間でセキュリティについて勉強したり、「自分、手空いてます。手伝えます！」とアピールをしてみたり。そのうちに「じゃあ、これも」、「こっちもやってみる？」といろいろ任されるようになって、セキュリティの世界がどんどん広がっていきました。これがすごく面白くて、はまってしまいました。

編集部員：どこに面白さを感じたのですか？

冨田：セキュリティと一言で言っても幅広いジャンルがあるのが魅力的ですよね。掘れば掘るほど新しい情報が出てきて、分からないことを勉強して身に付けていくのが本当に楽しいです。社内外のさまざまなジャンルのスペシャリストたちと交流するのも刺激的です。セキュリティ業界って、いろんなスペシャリストが知恵を出し合っているんですよ。そういう人たちの輪に入って話していると、どんどん分からないことが出てくるんです。でも、それをその人に聞いたり、他の人に聞いたり、自分で調べたりして理解を深めていくのが楽しいです。社内にもたくさんのスペシャリストがいますが、雑食的に知識を吸収してオールマイティに力を発揮できる部分が、自分の強みだと思っています。

編集部員：面白さが知識やスキルに対する貪欲さにつながっていったのですね。

冨田：今は新人の教育もやっているので、私が感じたそうしたセキュリティの面白さや魅力についても、伝えていきたいと思っています。これはお客様に対しても同じで、最初はセキュリティに興味を持ってもらうところからはじめて、それをきっかけにゆくゆくはセキュリティ意識を高めてもらう、その手伝いをしたいと思っています。そうやって自分自身と周囲、お客様、みんながセキュリティに対して知識を深めていけたらいいなと考えています。

ICT 製品セキュリティ関連法令

EU 域内共通の認定制度整備へ

現在 EU では、この 5 月に施行された GDPR に引き続き、グローバルに影響が及ぶ新たなセキュリティ関連法令・制度の審議が進んでいる。

2018 年 7 月 10 日、欧州議会の常任委員会 ITRE（産業・研究・エネルギー委員会）が承認したサイバーセキュリティ認定制度（Cybersecurity Certification Framework）だ。

これは、2016 年に発効した「NIS 指令」* を補完すべく 2017 年 11 月に発表されたサイバーセキュリティ法（Cyber-security Act）の柱となるもので、対象は ICT 製品全般。コンピュータ機器のほか、自動車や医療機器等、IoT を構成するコネクテッドデバイスも広く含まれる。

背景には、昨年欧州各国に多大な被害をもたらした Wannacry、NotPetya など、IoT の普及と相まって強大化するセキュリティ脅威への懸念の高まりがあり、域内共通の制度を策定することで認定取得に取り組む企業の負荷を軽減し、IoT 機器のセキュリティ強化を加速させることを狙う。

認定の取得は任意だが、EU 加盟国のいずれかで認定を取得すれば、その他すべての加盟国で製品・サービスを販売できるため、企業にとってのメリットは大きいといえるだろう。

* NIS 指令
（The Directive on security of Network and Information Systems）：

重要インフラのセキュリティに関する指令。欧州委員会が2016年7月に採択し、同年 8 月に発効した。EU 加盟国による法制度化の期限は 2018 年 5 月 9 日、重要インフラ事業者の対応期限は 2018 年 11 月 9 日となっている。英国では 2018 年 1 月に法制度化され、違反した場合には最大 1700 万ポンド（26 億円）の制裁金が科される。

参考情報
http://www.europarl.europa.eu/news/en/press-room/20180710IPR07605/cybersecurity-act-build-trust-in-digital-technologies
http://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf

Wi-Fi セキュリティの新規格 WPA2 から WPA3 へ

この 6 月、Wi-Fi Alliance は、無線 LAN のセキュリティプロトコルとして広く知られている認証プログラム「WPA（Wi-Fi Protected Access）」の新規格「WPA3」を発表した。2017 年に「WPA2」で発見された「KRACK（Key Reinstallation AttaCK）」に対する脆弱性を根本から解決するものでもあり、2004 年の WPA2 の策定から実に 14 年ぶりとなる。

WPA3 では WPS2 との相互運用性を維持しながらの管理フレーム保護が必要である。

完全に WPA3 に移行するまでは WPA2 も引き続き移行モードで運用されるが、いずれすべての機器で WPA3 の Wi-Fi セキュリティが必要となる。

最新セキュリティ技術を導入し、時代遅れのプロトコルを排除。より強固なセキュリティが提供される。なお、法人向けの「WPA3-Enterprise」と個人・家庭向けの「WPA3-Personal」と 2 つのモードがあり、それぞれの特徴は表のようになる。

WPA3-Enterprise 政府や金融機関等、センシティブなデータネットワークに対するセキュリティ	WPA3-Personal パスワードベースの堅牢な認証
・暗号強度を強化（128 ビット⇒192 ビット） ・認証付き暗号方式（AES-GCM 等）をサポート ・堅牢な管理フレーム保護 ・192 ビットセキュリティの WPA3 ネットワーク展開	・WPA2 では脅威だった辞書攻撃への耐性 ・強度の低いパスワードでも認証の安全性を強化 ・パスワードが漏洩した場合でもデータトラフィックを保護 ・これまでの WPA2 と同様の接続方法で利用可能

参考情報
https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security
https://www.wi-fi.org/discover-wi-fi/security

総務省「IoT セキュアゲートウェイ実証実験」

IoT 機器へのサイバー攻撃は年々増加しており、その対策は急を要する。しかし、脆弱性を有する機器の完全排除は困難であり、また、機器に精通していない利用者保護も考慮しなければならない。そのため、ネットワーク側で一元的にセキュリティ対策を講ずる仕組みの確立が必要である。そのような背景を踏まえ、総務省は、セキュリティ脅威に対して、認証・検知・対処といった対策ができるかの実証実験を行った。

概要は以下のとおり。
- 接続しようとする IoT 機器が正当なものか、IoT セキュアゲートウェイ [*1] において認証
- 通信状況を基に、不正アクセス・異常通信を検知
- 不正な IoT 機器からの通信遮断や脆弱性を有する IoT 機器のソフトウェア強制アップデート

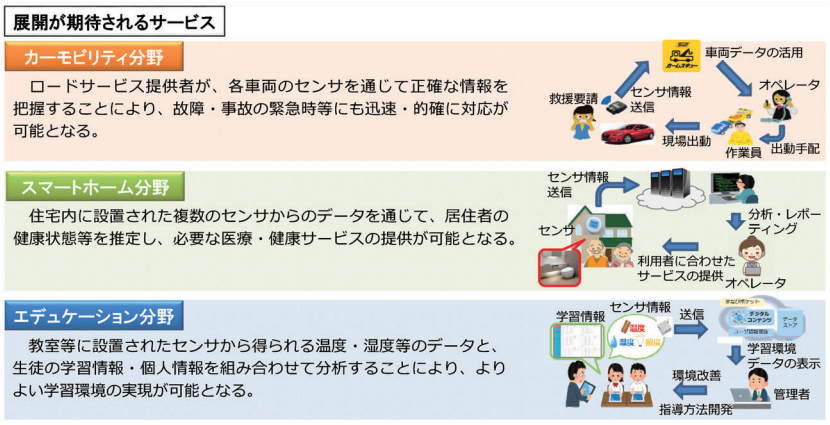
実証実験を実施したのは、カーモビリティ、スマートホーム、エデュケーションの 3 分野で、不正アクセス・なりすまし・乗っ取り・盗聴・盗難といった事例を想定し、リスク対処が可能かを検証した。

■実証実験の結果

通信の遅延や IoT サービス停止等は発生せず、認証・検知・対処といった機能も十分提供でき、堅牢なシステムであることも確認された。一方で、IoT 機器搭載の車両が電波の届かない場所で通信が途絶えた際、盗難に遭ったと誤検知が発生。また、通信が再開した際、一気にデータ受信したことから、乗っ取りにあったと誤検知する問題も生じた。

■今後の取組み

検知機能の向上・改善が必要。その上で、普及に向け、
①サービス提供者が、迅速かつ適切な行動をとれるよう、詳細情報等を提示する
②各種 IoT サービスに応じた多様な検知条件設定画面の作成する
③SOC[*2] との連携等、効率的なシステム運用環境の構築する
といった、実用的なサービスモデル提示の取組みが必要となってくる。



出典：総務省　「IoT セキュリティ基盤を活用した安心安全な社会の実現に向けた実証実験」の結果の公表

[*1] IoT セキュアゲートウェイ：IoT 機器とインターネットの境界に設置され、認証・検知・対処といった一連のセキュリティ対策を行う仕組み
[*2] SOC：Security Operation Center
参考情報　http://www.soumu.go.jp/main_content/000560886.pdf

標的型攻撃メールでウイルス感染 過去 1 年間で国内およそ 140 社

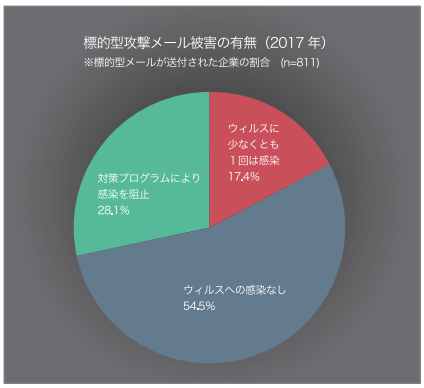
総務省が全国の企業と世帯を対象に通信利用動向調査を行い、2018 年 5 月に結果を発表した。調査は 2017 年 11 ～ 12 月にかけて行われ、2017 年 9 月末における情報通信サービスの利用状況等について、1 万 6117 世帯と 2592 社より回答を得た。

このうち、企業向けの情報セキュリティに関する項目では、50.9% もの企業が過去 1 年間に何らかのセキュリティ関連の被害を受けたと答えている。

何らかの被害を受けた企業の被害内容は、「ウイルスを発見または感染」が 44.1%、「標的型攻撃メールが送付された」が 28.8% あった。

「ウイルスを発見または感染」と回答した企業のうちの約 4 分の 1 が、実際にウイルス感染をしたという結果が出た。

標的型攻撃メールを送付された企業 811 社のうち、「ウイルスへの感染はなかった」と回答したのが 54.5%。対して、「ウイルスに少なくとも 1 回は感染」が 17.4%、「端末に到達する前にウイルス対策プログラム



出典：総務省　平成 29 年通信利用動向調査の結果

で阻止した」が 28.1% あった。

つまり、標的型攻撃メールを受信したうえ、さらにウイルスに感染した企業は、国内でおよそ 140 社に及ぶことになる。

参考情報
http://www.soumu.go.jp/johotsusintokei/statistics/data/180525_1.pdf

診断結果にみる情報セキュリティの現状

～　2018 年上半期　診断結果分析　～

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

BBSec の診断について

今年に入りサイバー攻撃は、ますます巧妙・複雑化し、ターゲットも多種多様にわたっている。これに伴い、情報漏洩に対する社会の目も厳しくなっている。各企業・組織は攻撃に対処するだけではなく、保有している情報資産等の管理・運用にも、これまで以上に注意を払わなければならない。あらゆる企業・組織にとって情報セキュリティ対策は喫緊の課題といえる。

その対策に欠かせない要素の一つが、システム脆弱性診断である。当社では、技術者による高精度の手動診断と独自開発のツールによる効率的な自動診断とを組み合わせ、お客様のシステムにおける脆弱性を検出してリスクレベルを評価し、個別具体的な解決策を提供している。また、検出された脆弱性に対するリスク評価について、下表 のとおりレベル付けを行っている。

当社では、2018 年 1 月から 6 月までの 6 ヶ月間に、15 業種延べ 348 企業・団体、3,110 システムに対してシステム脆弱性診断を行った。情報セキュリティ対策に重きを置く企業側の姿勢もあり、診断案件数は年々増加している。業種別の診断分析については、P39 から触れているので、ご参照いただきたい。

Web アプリケーション診断では、脆弱性が検出されたシステムが全体の 85.3% と、前年同期（2017 年上半期）の 90.3% に比べ微減しているが、依然として高い割合である。ネットワーク診断においては、システム全体の 65.7% と、前年同期（2017 年上半期）の 64.4% と比較して微増している。検出された脆弱性のうち、早急な対処が必要な「高」レベル以上のリスクと評価された脆弱性は、Web アプリケーションでは 17.2%、ネットワーク診断においては 9.6% 検出されている。ネットワーク診断では、「高」レベル以上の割合は減少しているものの、「中～低」レベルの検出件数は増加が見られる。

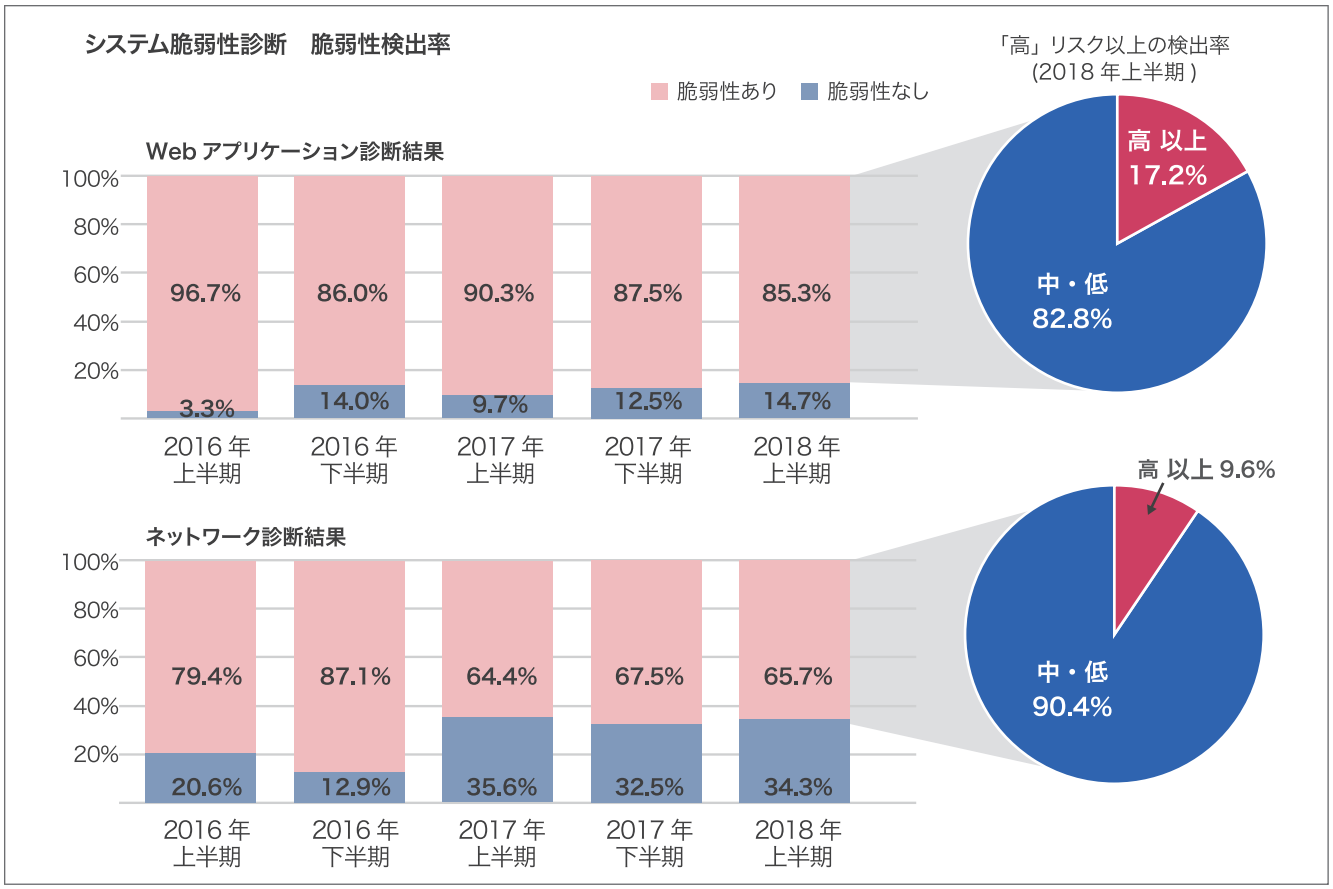
以下、診断カテゴリごとに 2018 年上半期の診断結果を解説していく。

Web アプリケーション診断結果

当社 Web アプリケーション診断の結果、システムに使用されているプログラミング言語やミドルウェア、CMS などの製品（以下『コンポーネント』と称する）について、バージョン・パッチ管理が徹底されていない問題が、対象システム中、約 2 割検出された。このうち、PHP、Apache、Apache Tomcat

システム脆弱性診断で用いるリスクレベル基準

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



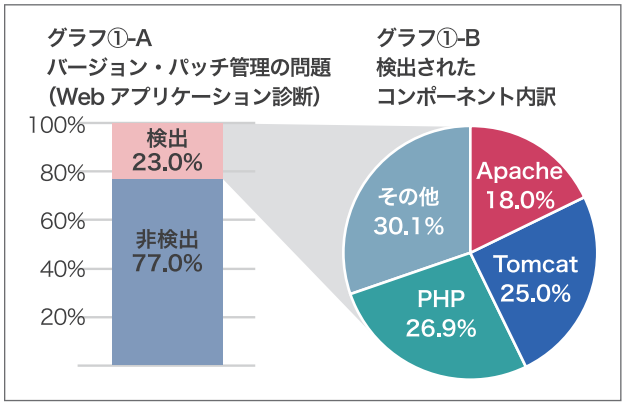
の３つが約 7 割を占めた。(グラフ①-A,B)

さらに、サポート終了もしくは終了間近のコンポーネントを使用しているシステムが、約５割存在する。例えば PHP の 5.6 系は、2018 年 10 月現在サポートが継続されているが、2018 年末にサポートが終了する予定である。(サポート状況 一覧表)

サポートが終了しているコンポーネントを使用し続けた場合、新たに発見された脆弱性への対策が困難になることはもちろん、製品のバージョンによっては既知の脆弱性を悪用するプログラムが公開されている場合もあり、攻撃者に対して無防備な状態となる可能性がある。さらに、攻撃を受けた場合は被害者になるだけで済むとは限らない。脆弱性のある製品を使用しているシステムを踏み台とした攻撃が実行され、意図せずサイバー攻撃の加害者となってしまうこともあるからだ。

また、サポート終了間近の PHP を使用していることに12月に入ってから気づいた場合、バージョンアップを試みようとしても、システム上、運用上、または経営上の制約などにより、サポート終了日までにバージョンアップを完了できるとは限らない。そのため、特にサイバー攻撃が増える傾向にあると見られる「年末年始」の時期に、前述したような不安・リスクを抱えながらサービス運用せざるを得ない状況となる可能性があるのだ。実際、数十万件という規模の個人情報が漏洩した事件も発生している。このような事件を発生させると、顧客に直接迷惑をかけるだけにとどまらず、社会的なイメージ低下、信用失墜にも繋がる大きなダメージとなりかねない。

セキュリティを強化するために CMS を導入するという方法もあ



サポート状況一覧表

	PHP	Apache Tomcat	Apache
現行バージョン	7.1 系以上	7.0 系、8.5 系、9.0 系	2.4
サポート終了	7.0 系以前*	6.0 系以前、8.0 系	2.2 以前

* 5.6 系と 7.0 系については、既にアクティブサポートが終了。
セキュリティサポートは継続中であるが、下記日程で終了予定。
・5.6 系：2018/12/31　セキュリティサポート終了予定
・7.0 系：2018/12/03　セキュリティサポート終了予定

る。当社 Web アプリケーション診断では、高いシェアを占める WordPress や Drupal といった CMS のバージョンに問題のあるシステムは、対象システム全体の約 1.3% に留まった。CMS の場合、ロジック基盤の部分などのテンプレート・パッケージとして提供されていることから、バージョンアップが比較的容易であるためと推測できる。ただし、CMS は汎用的なロジックが公開されていることから、攻撃対象としても人気がある。その理由として、攻撃コードが公開されるなど、攻撃するための難易度が低いことがあげられる。実際に、Web サイトの改竄など、多くの攻撃事例もあるため、注意が必要だ。

バージョン・パッチに関する問題の対策として、まずはシステムで使用しているコンポーネントに何があるかを把握する必要がある。それらのバージョンの有効期限を定期的にベンダのホームページなどで確認し、常に最新のバージョンに更新することが、システムを守るために大変重要だ。

とはいえ、完璧な情報セキュリティ対策は、バージョンアップを実施するためにシステムの大幅な改善開発を必要とするなど、様々な要因により困難である場合が多い。それゆえ、最新のバージョンに更新されないまま放置されるケースが存在すると考えられる。しかし、たとえバージョンアップが難しい状況にあるとしても、必要なセキュリティパッチを適用したり、ベンダやセキュリティ機関が発表するワークアラウンドを適用するなど、できる限りの対応が推奨される。せめて使用コンポーネントおよびそのバージョンについては把握しておき、どのようなリスクを許容した状態で運用されているシステムであるか、管理しておくべきである。

重ねて述べるが、脆弱性を内包するコンポーネントが放置された状態は、攻撃者にとって格好の標的となり得る。本来は、より早い検知と対策を行うためにも、バージョンアップの影響が出ないようなシステム構築をすることが有効と言えるだろう。

ネットワーク診断結果

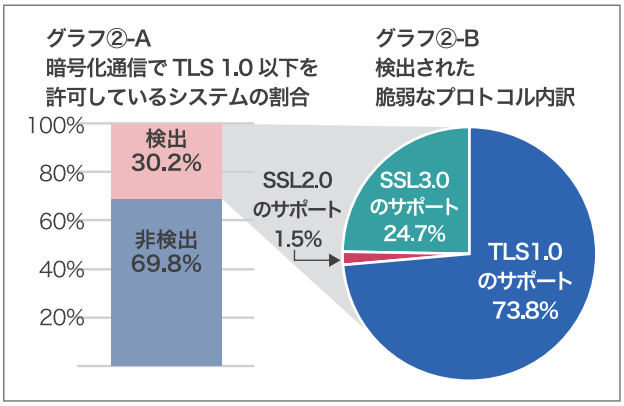
ネットワーク診断結果における問題として、検出数の多さに着目するよりも、注目すべき脆弱性、すなわち放置されているとその影響が著しいと思われるものについて述べる。

SSL/TLS について

まず、通信の安全性に関わる SSL/TLS プロトコルについて見ていきたい。当社の診断結果では、TLS 1.0 以下のバージョンのプロトコルによる暗号化通信を許可しているシステムが右のグラフ（グラフ②-A,B）のとおり検出された。

TLS 1.0 以下のままにしておくと、DROWN、POODLE、BEAST など、複数の既知の脆弱性により、暗号化された通信が解読され、情報漏洩などの被害を受ける危険性がある。様々な対策方法は存在するものの、これらの脆弱性はプロトコル自体に存在するものであるため、根本的な解決策は TLS 1.0 以下のサポートを停止することが最善である。まずこれらのバージョンをサポートしていないか、確認する必要がある。

世間では常時 SSL 化の流れがある。既に、常時 SSL 化していないと「保護されていない通信」と警告表示されてしまうブラウザも存在するため、対策の緊急性は高いと考えられる。その際、前述の旧バージョンのサポートを止めることも忘れずに対応したい。



2018 年 8 月には最新の TLS 1.3 が正式リリースされた。Google Chrome、Firefox など主要ブラウザにおいても対応が進められている。TLS 1.3 に対応することで、サービス提供者として信頼性の向上にも繋がる。TLS 1.3 が広く認知されるまでには一定の時間を要すると考えられるものの、既に TLS 1.3 の使用をルール化する動きはある。たとえばクレジットカード業界では、PCI DSS のマイナーリビジョン ver.3.2.1 がリリースされ、2018 年 7 月以降、脆弱な暗号化方式（初期 TLS/SSL）の廃止がベストプラクティスの位置づけから要件へと変更された。このような動向は、加速していくと推測される。

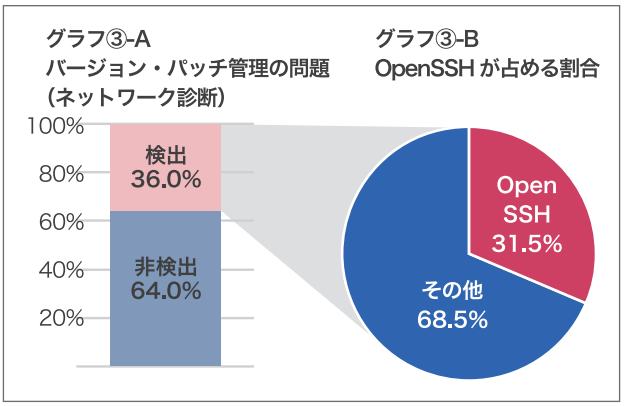
OpenSSH について

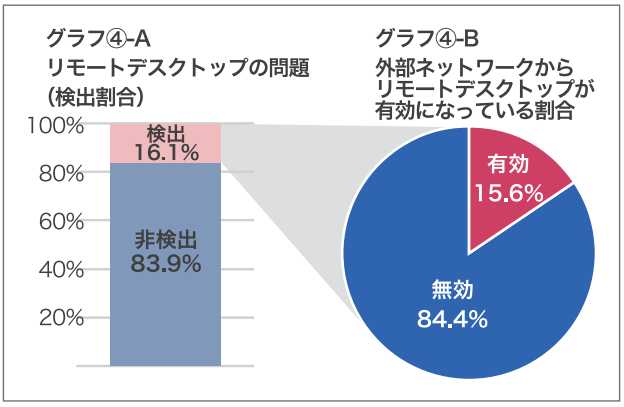
Web アプリケーション診断同様、ネットワーク診断においても、システムに使用されているコンポーネントについて、バージョン・パッチ管理が徹底されていない問題が顕著に出ている。診断対象のシステム中、36%で検出されており、その内の約 3 割を OpenSSH が占めている。（グラフ③-A,B）

OpenSSH は、ベンダからサポートの終了が明示的に公開されないという特徴があるため、新しいバージョンがリリースされた場合、実質的に、それ以前のバージョンはサポートが終了したと見なして差し支えないだろう。

旧バージョンの OpenSSH を使用し続けることは、脆弱性やバグが多数蓄積されたシステムを長期間放置していることになる。これらの脆弱性を悪用された場合、サービス運用妨害（DoS）や重要情報の奪取、セキュリティ制限の回避など様々な影響や被害を受ける可能性がある。そのため、システムの状況を常に把握し、最新のバージョンに保つことが推奨される。

また、「脆弱性が存在するリモートデスクトップ」や、「保護レベルの低いリモートデスクトップ」を使用しているシステムが、対象システム中、２割弱検出された。（グラフ④-A）リモートデスクトップ機能は遠隔から PC を操作できる便利な機能である反面、任意の場所から接続が可能な場合、総当り（Brute-Force）攻撃によりアカウント情報を奪取される危険性がある。検出された中で、外部ネットワークからリモートデスクトップ機能が有効になっているシステムも存在した。（グラフ④-B）アカウントを奪取された場合、高い権限での処理が実行されてしまう可能性があるため、早急な確認および対応が推奨される。





オリンピックや、サッカーワールドカップなど、世界規模のイベントのたびにサイバー攻撃の話題が取り上げられ、実際に攻撃による被害を受けたことが報道されていることからも明らかなとおり、コンポーネントなどのシステムの脆弱性を狙うマルウェアやサイバー攻撃は、国内外で後を絶たない。サイバー攻撃への対策は待ったなしの状況下で、古いバージョンのコンポーネントを使用し続け、脆弱性を積み重ねていくと、システム自体の経年劣化を早めることになる。日々、危険な状態のまま運用を継続した結果、事業継続自体が脅かされることがないよう、今一度、システムの状況を把握し、時代の流れをキャッチアップした積極的なセキュリティ対策を施す必要がある。その際、時代遅れになってしまったものは使用せずに排除するという決断をしていくことが肝要だろう。

スマホアプリ診断結果

BBSec では、スマホアプリを対象とした診断サービスも実施している。スマホの普及と相まって同アプリのセキュリティの重要性は今後も継続的に高まるものと見込まれる。

スマホはユーザが常に携帯しているため、生活を共にする「パートナー」である。アドレス帳、写真、スケジュール、訪れた場所の位置情報など、個人の生活に関わる全ての情報が格納・集約されているデバイスであり、まさに、「プライベート情報の宝庫」である。さらに、スマホは本人確認のための「認証の３要素」（右記）を保持している。もはや本人自身の一部といっても過言ではない。

「ネット世界」と「リアル世界」をつなぐ架け橋であるスマホが我々にもたらしている恩恵は、はかりしれない。我々は、決済、カーナビ、定期券、リモコンなど、様々なスマホアプリにより、日々の生活を支える様々な活動を「いつでも、どこでも」便利に実現できる。しかし、ネット世界につながっているがゆえに、第三者に「プライベート情報の宝庫」へアクセスされる

認証の３要素

- 記憶情報
  本人だけが知っていること
- 所有情報
  本人だけが所有しているもの
- 生態情報
  本人自身の特性（指紋、顔認識、声紋など）

危険性をはらんでいる。したがって、スマホアプリの安全性を確認する重要性はさらに高まっている。

では、2018 年上半期の当社スマホアプリ診断結果において、注目すべき項目を取り上げる。

「OWASP Mobile Top 10 2016」（右記）で 2 番目にランクインしている、「安全でないデータ保存」に関連する脆弱性項目の検出は、全体の約 2 割を占めた（グラフ⑤ ）。

「安全でないデータ保存」に関連する脆弱性は、アプリが処理する情報資産に対するリスクであり、主に次の 2 つの項目が挙げられる。

バックアップ可能な領域に重要情報が保存されている問題

1 つ目は「バックアップ可能な領域に重要情報が保存されている問題」である。スマホのローカル環境内において、信頼境界を意識しない領域に重要情報を保存していると、悪意のあるアプリに侵食されて、情報が漏洩してしまうリスクがある。これは、単に悪意のあるアプリをインストールしなければ良いというものではない。なぜなら、近年の、ネットワークおよびクラウド環境の劇的な進歩により、フルバックアップやアプリの保存データがクラウド環境に転送されているという実情があるからだ。このため、ユーザの知らない間に、意図せず情報が流出している可能性がある。転送されたデータを格納しているクラウド環境やサーバ環境に脆弱性が存在した場合、情報が漏洩する危険性があるのだ。

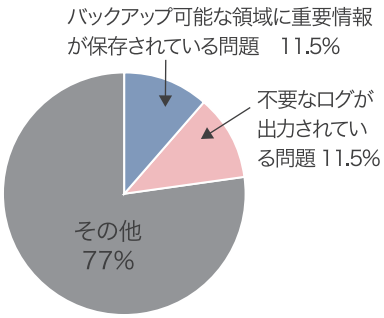
不要なログが出力されている問題

2 つ目は、「不要なログが出力されている問題」である。特に目立つのは、スマホが外部と通信した際のアクセスログ情報であり、API 認証に伴うトークン制御や暗号化に関わるキー情報などを含む。また、デバッグモードのまま利用された場合に認証情報などの機微な情報が露出することは、セキュリティの観点から推奨されない。さらに、最近は個人情報やプライバシー情報の保護について、世界的に法規制が定義されつつあるという動向もある。例えば、よく活用されているスマホアプリの機能の 1 つである「位置情報を活用したサービス」（ナビゲーション、お店検索など）は、アプリ提供側では、位置情報を収集する機能を開発して、ログに格納することも可能であるため、今後は位置情報などのプライバシー情報は、ユーザの同意を取得していないと規則違反となり、懲罰の対象となる可能性がある。

現在の風潮としては、ユーザの知らないところで、そのプライバシー情報を活用することは許されないのだ。最近のインシデントとして、QR コードのアプリにおいてユーザの同意なしに位置情報を活用していたために、サービス停止となった事例がある。

世の中の動向からわかるとおり、スマホアプリは、アプリ内部および外部へのアクセスの両面において、技術的な観点からセキュリティを強化することはもとより、スマホアプリおよびサービスを提供するためには個人情報の保護が必須であるという、社会的な観点からもセキュリティ対策を整備することも不可欠である。

グラフ⑤
「安全でないデータ保存」に関連する脆弱性項目



OWASP Mobile Top 10

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

OWASP Mobile Top10 2016 - Top10 より当社作成

スマホアプリの数は増える一方であり、乱立状態といえる。そして、スマホ普及率とデバイス自体の機能向上により、スマホを利用したサービスは我々の生活とは切っても切り離せない存在になり、ユーザの依存度も高まり続けるものと予想される。堅牢なスマホアプリの構築、および技術環境の変化に伴うセキュリティレベルの向上・維持は必須といえよう。

「重要情報の漏洩」に関する問題について

～　重大インシデントの【火種】となるかも？

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

2018 年上半期に当社で診断した対象システムのうち、「重要情報の漏洩に関する問題」が検出されたシステムは、全体の 7.1%である。（グラフ①-A）

決して大きい数字ではないが、検出されているという時点で見過ごすことはできない。

認証情報や個人情報といった重要情報の漏洩については、事故として報道される大規模なインシデントは氷山の一角にすぎない。水面下では、情報奪取を目的とした攻撃を行うため、認証情報リストやワーストパスワードリストなどが活発に収集されている実態があり、コミュニティサイトから漏洩した認証情報を元にインターネットバンキングでなりすましの被害に遭う可能性もある。

重要情報の取扱いに関しては、近年、各業界のガイドラインや法制度により世界標準として定義され、注意喚起がなされている。最近の主な動向で関連する基準には、OWASP Top10（A3:2017 機 微な情報の露出）、改正個人情報保護法、GDPR（General Data Protection Regulation）、e プライバシー規則（ePrivacy Regulation）[審議中]、PCI DSS v3.2.1 などが挙げられる。

こうした動向の背景には、人権を保障するための「個人情報の保護」や「通信の秘密」などがあり、事業活動として Web システムを運営する組織は、重要情報の露出やプライバシー情報の漏洩によって、利用者の利益価値の侵害や名誉毀損などを引き起こさないようにする必要がある。運営するサービスそのものにおける被害がなくても、あるサイバー攻撃のきっかけとなった「火元」は自社サイトから密かに漏洩した情報である場合もあるのだ。法的な懲罰を科せられる可能性があることからも、「対岸の火事」では済まされない。

機微な情報の露出

2018 年上半期に当社で診断した対象システムのうち、「重要情報の漏洩に関する問題」の検出分析は下のグラフ（グラフ①-B）のとおり。

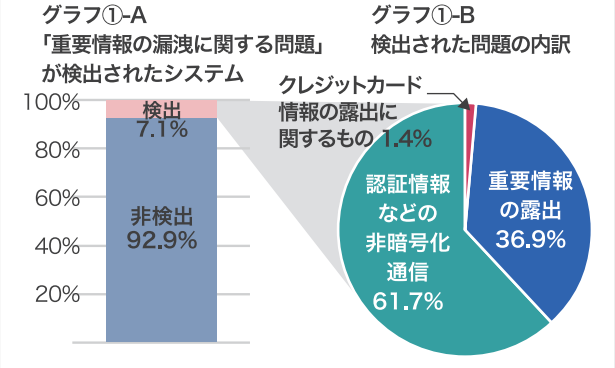
OWASP Top 10 のガイドラインによると、重要情報は 2 つの観点で考慮される。

１つ目は、『A3:2017 機微な情報の露出』に記載されている「機微な情報」（下記参照）である。

これらは、当社検出結果における、「認証情報」および「クレジットカード情報」に関連する問題に該当する。いずれの重要情報も、不用意に出力することは推奨されない。

また、重要情報には次ページ [重要情報とそのリスク] のように大枠を「一次重要情報」「二次重要情報」の２つにレベル分けできる。

「認証情報」について、ID・パスワードが不必要な場面で出力されていたり、認証関連のセッション管理情報が第三者に露呈したりしてい



機微な情報

- ◆ 認証情報
  - ・パスワード
- ◆ PCI DSS など金融の情報保護
  - ・クレジットカード　・仮想通貨 (暗号通貨)
- ◆ EU の一般データ保護規則（GDPR）
  - ・財務情報　・健康情報　・個人情報

重要情報とそのリスク

る状態があると、攻撃者がユーザになりすまして操作利用することが可能になってしまう。「クレジットカード番号」および「セキュリティコード」も同様であり、第三者に情報が露呈することで、カード不正使用など、ユーザに直接的な経済損失を負わせることが可能になる。

また、これら機微な情報は、リスト型攻撃向けのワーストパスワードリストやクレジットカード番号の流出などが闇市場で「名寄せ」されて膨大な量の名簿が作成され、それが取引されることにより、情報流出元とは全く関係のないサイトやサービスなどに二次的に被害が拡大する恐れがある。

いずれにしても、診断で検出された数値だけを見ると、少ない印象を受けるかもしれないが、当該問題を抱えたまま放置されているシステムが存在していること自体に注目したい。これらの重要情報が露呈していることを見逃していることや取扱いに注意していない状態のまま事業活動を継続することは、非常に危険である。

脆弱なパスワードの存在

OWASP Top 10 のガイドラインにおける重要情報の 2 つ目は、『A2:2017 認証の不備』で記載されている、認証情報＝パスワードの方針である。当社診断において、「脆弱なパスワードに関する問題」の検出結果を確認すると、脆弱なパスワード、単純なパスワードを許可しているサイトが少なくない。ユーザビリティのために、脆弱なパスワード設定を許容する傾向もあると見られるが、以下の観点からも見直すことが推奨されている。

最近のパスワードの方針

2017 年の NIST SP 800-63B 改訂により、従来の文字数・複雑性・定期変更によるパスワード強度の確保から、定期変更や複雑性への要件が削除されたことが、セキュリティ関係者の間で話題を呼んだ。これを受けて、各種標準においてもパスワードに対する推奨内容に変化が起きている（一覧表）。この中で、「よくあるパスワードの排除」が、多くの情報セキュリティ標準において推奨されるようになっている。

よくあるパスワードの 3 類型

使いまわされたパスワード
他のシステムで利用されていることが確認できるパスワードや、過去の漏洩で流出しているパスワード

推測可能なパスワード
ワーストパスワードリストに掲載されているパスワードや、システム名･ユーザ名を含むパスワード

あまりにも単純なパスワード
繰り返し（11111111 など）や連続文字（abcd1234）といったパスワード

現時点において特に注目すべきは、この「よくあるパスワード」についてである。具体的には次のようなパスワードが設定されないような機構を、Web システム側で許容させないようにすることが肝要だ。

「よくあるパスワードの 3 類型」を参考に、Web システム提供側としては、パスワード設定に対する意識レベルを高め、第三者に容易に推測されない、複雑なパスワードのみを許容する仕組みが求められている。

パスワード推奨事項の一覧表

	NIST SP 800-63B	OWASP TOP10	PCI-DSS	総務省の推奨
文字数	8 文字以上	NIST SP 800-63B 準拠	7 文字以上（8.2.3）	10 文字以上
文字種	-		2 種（8.2.3）	明記なし
複雑性	配慮しない		-	推奨
定期変更	なし		90 日ごと（8.2.4）	不要
多要素認証	レベルによるが基本推奨	推奨	-	推奨
よくあるパスワードの排除	推奨	推奨	推奨	推奨

情報漏洩は、『対岸の火事』ではない

重要情報の取扱いに対して問題がある状況で起こりうるリスクを考慮した場合に、次のようなインシデントが発生する可能性が高まると見られる。それは、ターゲットを特定した情報奪取を目的とするハッキングだ。

重要情報が第三者に漏洩した結果、被害範囲は想定以上に拡大する恐れがある。プライバシー情報をヒントに認証情報を見つけることや、関連する行動パターンを分析して他の重要サイトへの認証を突破するヒントとすることができるからだ。

ブラックハッカーが登場する映画やドラマで特定の個人の認証情報を奪って本人になりすます場面にあるように、趣味の A 社コミュニティサイトから漏洩した認証情報を利用してリスト型攻撃を実行し、その人物が銀行口座を保持する B 銀行のネットバンキングサイトのアカウントを乗っ取ることも実際に可能なのである。そんな災いが自分の身に降りかかることを想像したら……なんとも恐ろしい話である。世間を騒がせる大規模なインシデントは、もはや対岸の火事ではない。(図)

はるか昔の Web システム開発では、実現したい機能や利便性を追求することに主眼が置かれ、作り手においても、作り手に発注する側においても、また利用者の方も、セキュリティ意識は二の次だっただろう。しかし、時代の潮流は、機微な情報・個人情報を保護することについてシビアな方向に向かっていることが、法制度・規則、ガイドラインの整備状況からも顕著になっている。

法規制の動向

2018 年は、情報保護について、世界的に大きく動き出したターニング・ポイントにあたると考えられる。

OWASP Top 10 による Web システムのガイドラインで『A2:2017 認証の不備』と『A3:2017 機微な情報の露出』が上位にあるとおり、情報保護は重要なポイントである。

法制度においても、ヨーロッパの「GDPR」、「e-プライバシー規則 [審議中]」に見られるように、個人情報保護や電子通信データ保護が規則として続々と制定されていく傾向にある。日本国内においては、改正個人情報保護法があり、また日本国憲法における『通信の秘密』も該当する。また、クレジットカード情報などの保護を目的している PCI DSS では、2018 年 7 月より、脆弱な暗号化方式(初期 TLS/SSL)の廃止がベストプラクティスから要件となった。それぞれの観点や内容に差異はあれど、世界的に「基本的な人権の保護」を目的としている点においては同じである。

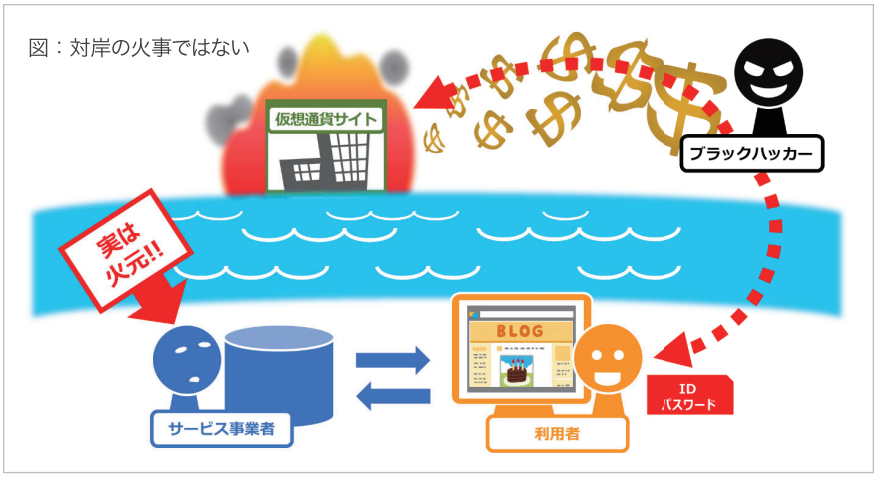


図:対岸の火事ではない

電子通信データを保護する時代で、求められること

機微な情報の露出に対してシビアな時代において、利用者に対して、以下の 3 つがポイントである。

- 利用者の金銭的価値の損失:【価値の保護】
- 利用者の機微な (個人) 情報の保護:【人権の保護】
- 利用者のプライバシーの保護:【行動・特性の保護】

サービス提供側として、機微な情報の保護を怠り、利用者の利益・価値を損失する事態を招くことがあってはならない。

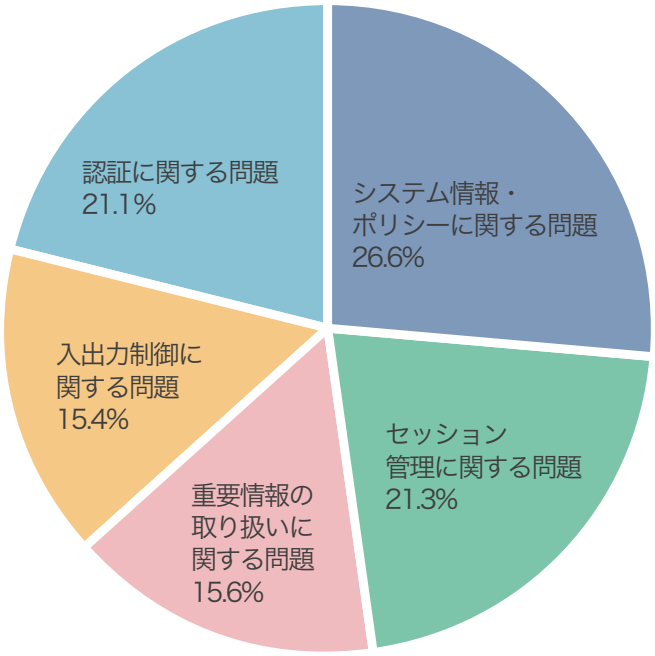
このとき、保護の対象として、認証情報や金融情報にとどまらず、事業活動を行う上で、基本的な人権に関わる個人情報の保護を徹底することは必須である。
また、プライバシーに関する情報も含める必要があることを忘れてはならない。利用者の行動や特性などの二次的な情報も取扱いを注意することが要求されている。

実際、法規制の面でも、コンプライアンス違反やリスク管理体制が甘いと、多大なる懲罰を科せられる状況になっている。

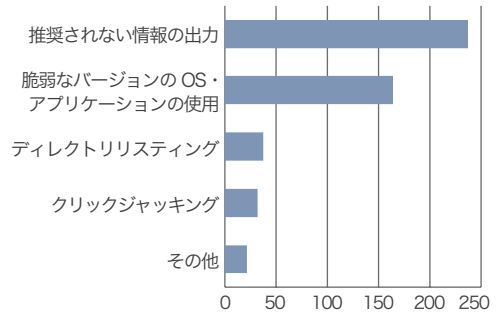
このような状況下において、Web システムによるサービス提供者は、「重要情報の取扱い」について見直し・再確認をすることが大切である。GDPR などの法制度においても推奨しているとおり、Web システムの脆弱性を診断することが重要だ。外部へ情報を漏洩させない適正な実装となっているか、定期的に確認を行っていただきたい。

2018 年上半期 カテゴリ別脆弱性検出状況

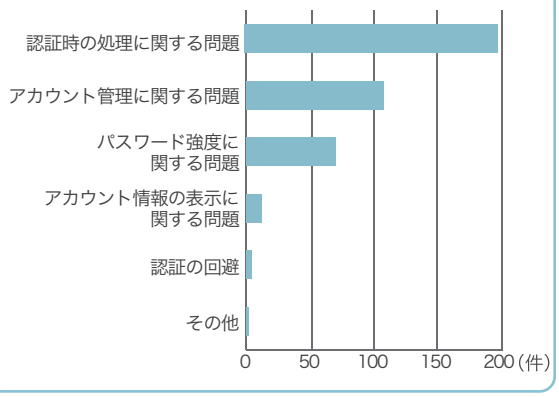
Web アプリケーション診断結果



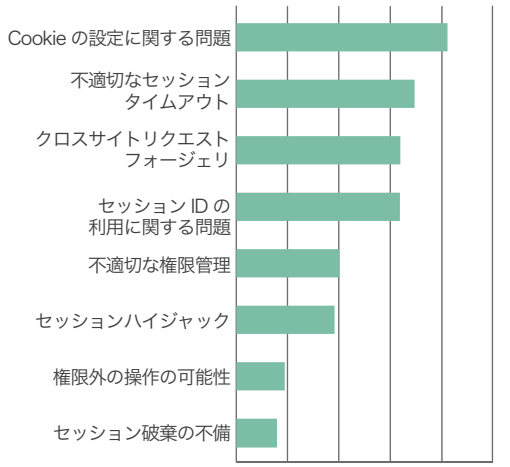
システム情報・ポリシーに関する問題



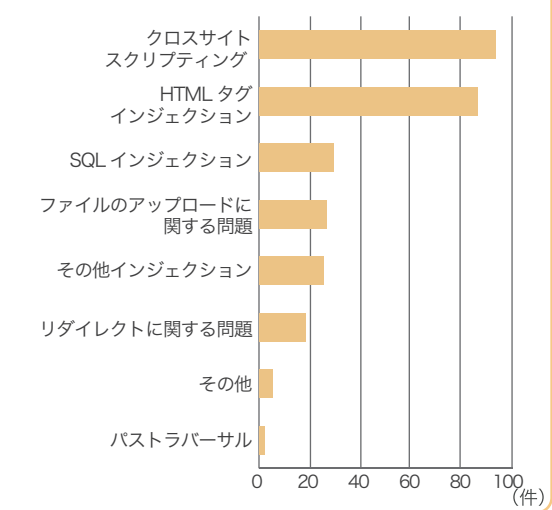
認証に関する問題



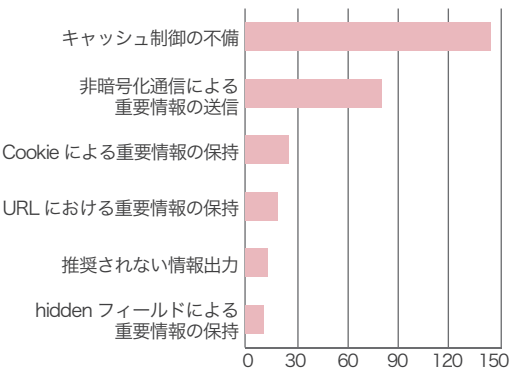
セッション管理に関する問題



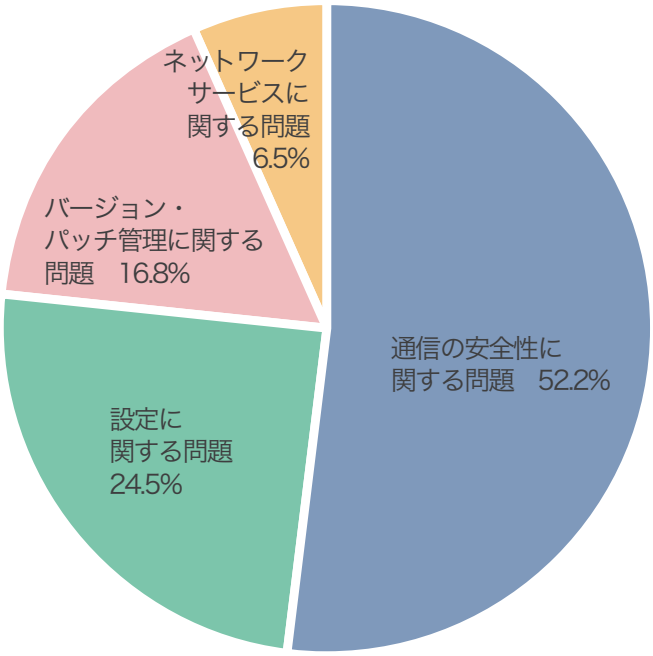
入出力制御に関する問題



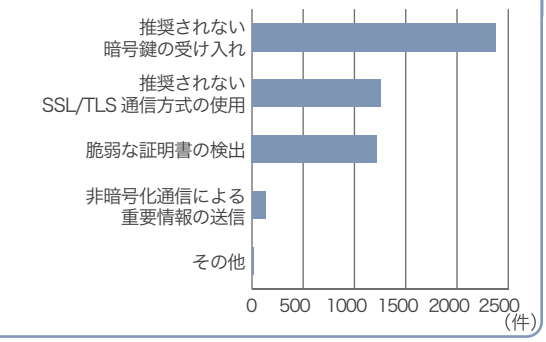
重要情報の取り扱いに関する問題



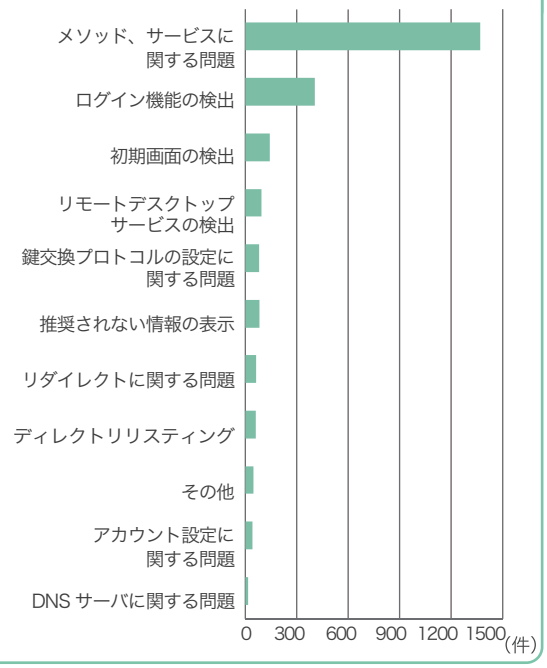
ネットワーク診断結果



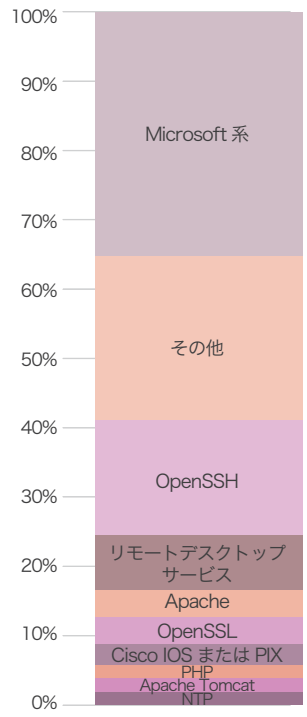
通信の安全性に関する問題



設定に関する問題

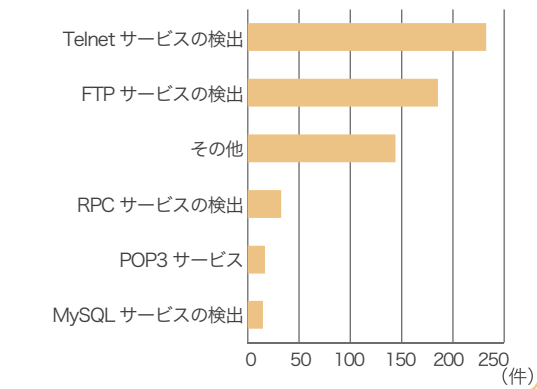


バージョン・パッチ管理に関する問題



脆弱性が存在するバージョンの OS・アプリケーションサービスの検出割合

ネットワークサービスに関する問題



業界別診断結果レーダーチャート

2018 年上半期 Web アプリケーション診断

診断対象を業界別に分類し、当社報告書内で示している、入出力制御、認証、セッション管理、重要情報の取り扱い、システム情報・ポリシーといった項目毎に、検出された脆弱性をリスクの重大性で評価してレーダーチャート化した。さらにここでは、「金融・保険業」「製造業」の 2 業種をピックアップし、それぞれの業種の傾向を分析したのでご覧いただきたい。

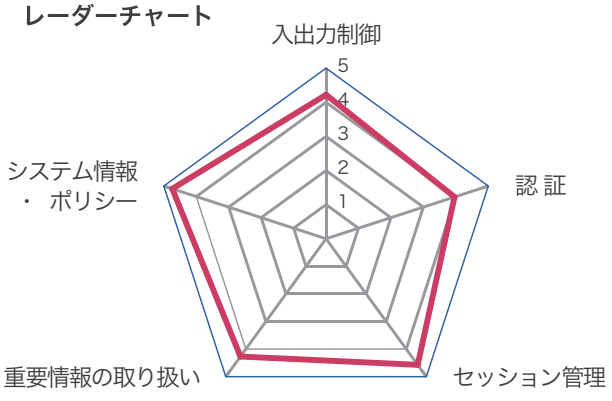
前段の現状分析コーナーでも述べたとおり、早急な対策の実施が求められる「高」リスク以上の脆弱性の検出割合は依然として高い。しかし、やみくもに不安がる必要はない。正しい対処を施せば影響は抑えることができる。その手助けを当社では行っており、また、事故を未然に防ぐための方法を、官公庁などがガイドラインや対策提言などとして発表している。これらを参考にすることで脆弱性への対応は可能である。

診断実績（業界別割合）

業界	割合
情報通信業	32.7%
生活関連サービス業，娯楽業	18.3%
金融・保険業	15.1%
不動産業，物品賃貸業	12.3%
製造業	5.5%
電気・ガス・熱供給・水道業	5.3%
サービス業（他に分類されないもの）	5.0%

業界	割合
医療，福祉	1.3%
学術研究，専門・技術サービス業	1.3%
教育，学習支援業	1.3%
卸売業，小売業	1.0%
運輸業，郵便業	0.3%
公務（他に分類されるものを除く）	0.3%
宿泊業，飲食サービス業	0.3%

レーダーチャート

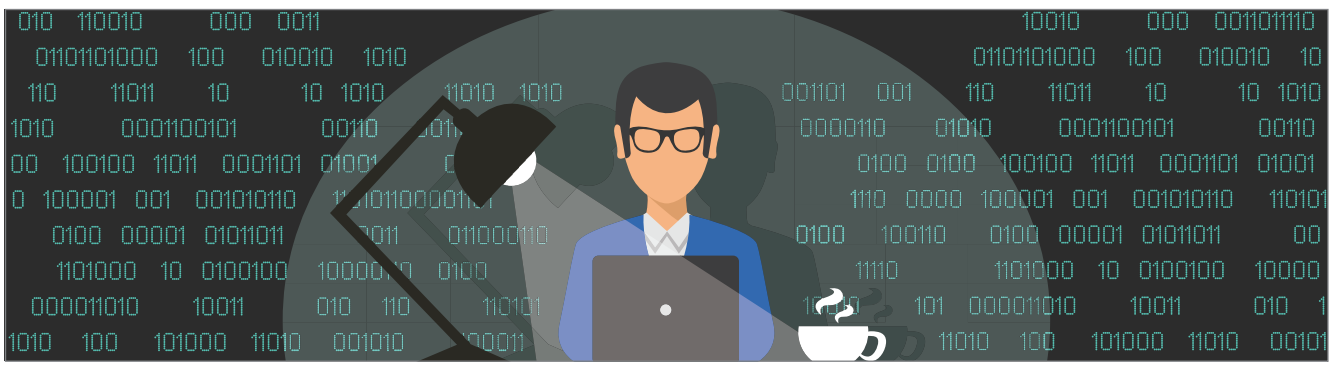


●レーダーチャートの見方●

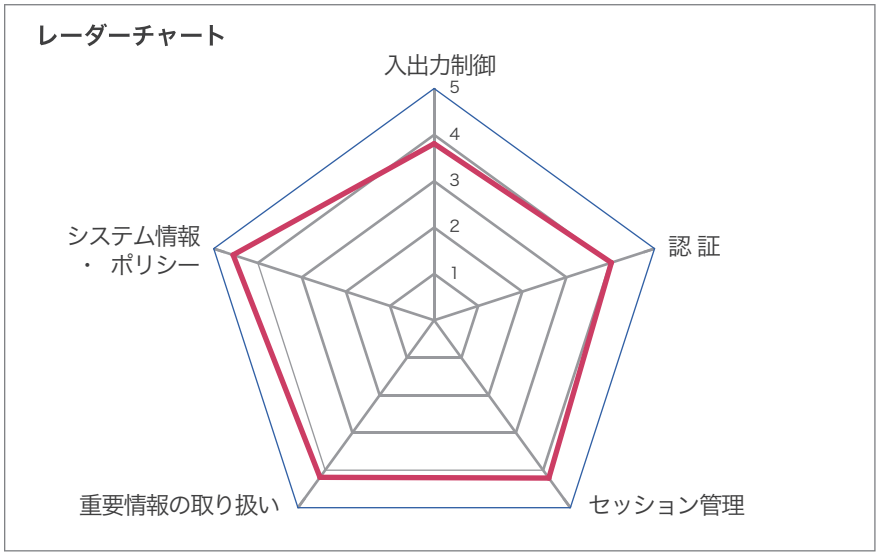
リスクの重大性によって「緊急」「重大」「高」「中」「低」「情報」というレベル分けを行い、各段階に応じた数値を定め平均点化したものを赤線で示す。数値が高いほど安全度が高く、数値が低いほど緊急の対応が必要となる。

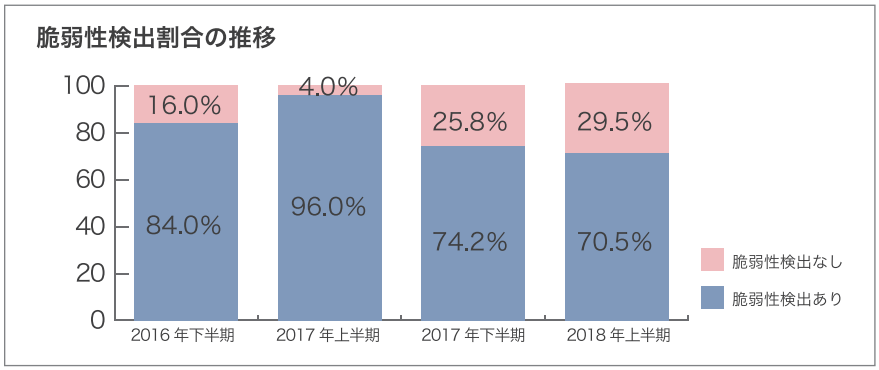
●業界分類方法●

「日本標準産業分類」（総務省）の「大分類」を基に当社にて選定



金融・保険業





金融・保険業に関しては、当社診断結果から、特定のシステムを除き、セキュリティレベルが比較的高い傾向が見られた。例えば、入出力制御に関する項目は、総体的に見て、早急に対応が望まれる「高」リスクレベル以上の脆弱性が多く検出される中、金融・保険業においては概ね対応がなされている。しかし、比較的堅牢といえる金融・保険業のシステムであっても、毎回 100 点の診断結果が得られるわけではない。悪用された場合にサービス運用妨害（DoS）や情報漏洩、アクセス制限回避等の被害につながる脆弱性が検出されることもある。ただそうした場合でも、多くの組織は早い対応を行い、再診断を行う際には少なくとも「中」リスクレベル以上の脆弱性への対処が完了しているのが同業種の特長である。

これは、金融庁の安全対策基準やクレジット業界におけるグローバルセキュリティ基準「PCI DSS」等に準拠している、または準拠しようとしているシステムが多いことが理由の一つにある。こうした基準に準拠していない場合、サービスの運用・継続自体ができなったり、万が一インシデントが発生した際の責任や罰が重くなったりする可能性があるため、コンプライアンス面を最重要視して取り組む組織も少なくない。

外部からの攻撃を想定して Web アプリケーションファイアウォール（WAF）などの境界セキュリティソリューションを導入しているシステムも多い。しかしその一方で、WAF を無効化した診断で多くの脆弱性が検出される場合がある。WAF はセキュリティ対策として確かに有効ではあるが万全ではない。ひとたび破られれば重大なインシデントにつながる恐れがあるため、根本的なセキュリティ対策が求められる。

システム毎の脆弱性検出割合について見ると、2017 年上半期に全システムの 96%で何らかの脆弱性が検出されていたが、2017 年下半期にはその割合が 74.2% に減少し、さらに今期は 71.5% へと継続して減少している。業種内でのセキュリティ意識が高まっている表れであろう。金融・保険業は、セキュリティ事故が起きた場合、影響力・影響範囲が非常に大きい業種であるため、以下にあげたガイドラインなどを参考に、より一層、攻撃に対して堅牢なシステムを構築・維持することが求められる。

金融業におけるセキュリティガイドライン (例)

経済産業省：
- 情報セキュリティ管理基準（平成 28 年改正版）

金融庁：
- 金融検査マニュアル・預金等受入金融機関に係る検査マニュアル
- 金融検査マニュアル・保険会社に係る検査マニュアル
- 金融検査マニュアル・システム統合リスク管理態勢の確認用チェックリスト
- 金融分野における個人情報に関するガイドラインの安全管理措置等についての実務指針

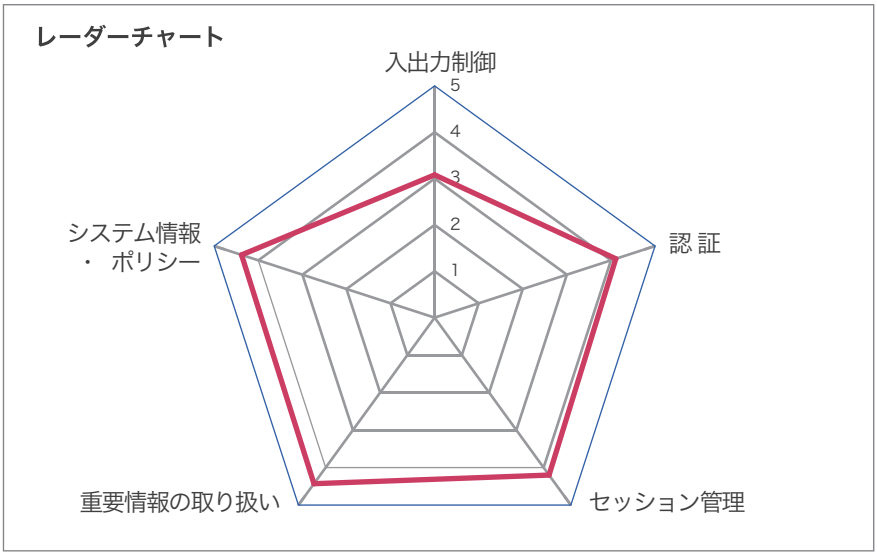
証券取引等監視委員会：
- 金融検査マニュアル・金融商品取引業者等検査マニュアル

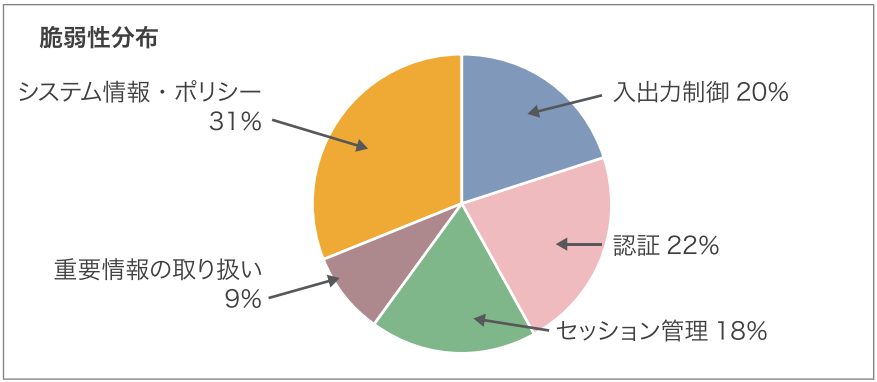
公益財団法人 金融情報システムセンター：
- 金融機関等コンピュータシステムの安全対策基準・解説書 (第 9 版)
- 金融機関等のシステム監査指針 (改訂第 3 版 , 改訂第 3 版追補)
- 金融機関等におけるコンティンジェンシープラン策定のための手引書（第 3 版追補 3）
- 金融機関等におけるセキュリティポリシー策定のための手引書 (第 2 版)

Payment Card Industry Security Standards Council：
- Payment Card Industry Data Security Standard（PCI DSS）ver. 3.2.1

※ 金融検査マニュアルは、平成 31 年 4 月 1 日以降廃止予定

製造業





製造業においては、入出力制御に関する項目のレーダーチャート値が、全業種の平均値より低い結果となった。これは、早急な対応が望まれる「高」リスク以上の脆弱性の検出割合が多いためで、特に、当社で定めるリスクレベルとしては深刻度で上から 2 番目、「重大」レベルの脆弱性が多く検出されており、その割合は実に、入出力制御における脆弱性の 75% を占める。

例えば、クロスサイトスクリプティングや HTML タグインジェクションといった脆弱性は、悪用された場合に任意のプログラム実行や悪質なページへの誘導、コンテンツの改竄といった影響を受ける可能性があるため、適切な対応が求められる。

また、システム情報・ポリシーに関する項目も検出数の割合が多く、サポートが終了した、あるいは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などの使用（使用の可能性も含む）が検出されている（円グラフ参照）。これらを放置していると、攻撃に対して脆弱な状態となってしまうため、最新バージョンへのアップデートや、セキュリティパッチの適用が求められる。

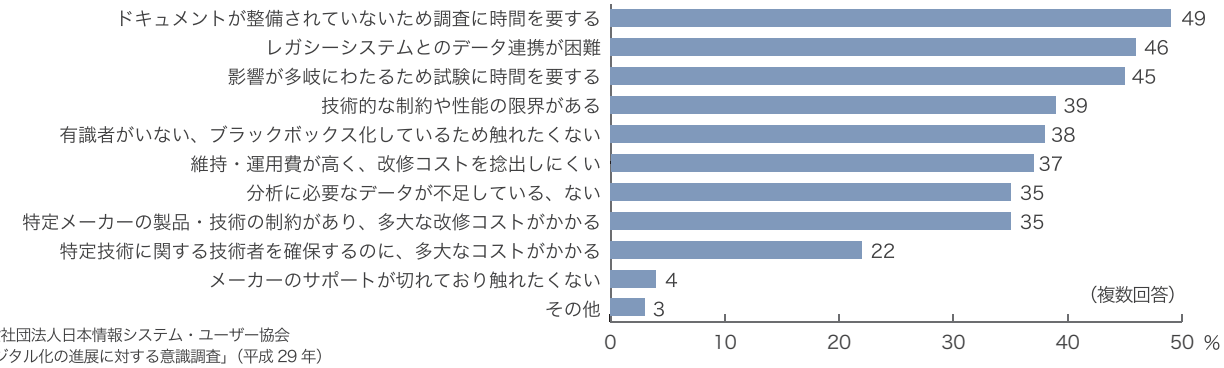
従来、製造業の制御系システムはインターネットに接続されていない独立系システム、いわゆる閉鎖系システムであるために安全、とされてきた。しかし最近では制御系システム機器に汎用 OS を使用する、通信プロトコルに標準プロトコルを採用するなど、攻撃を受けやすい環境に変わりつつある。その反面、前述のような経緯から、セキュリティの要素のうち、可用性に重きを置く傾向があること、パッチを当てるにしても操業を計画的に停止する必要があることなどから、なかなか OS の更新・パッチ適用がしにくいという特徴がある。（棒グラフ参照）

この 1 年ほどに国内で起きたセキュリティインシデントの中から、製造業に関連する事案をまとめた。インシデントが発生した要因として、必要なセキュリティパッチの適用の遅れや、Web サーバの脆弱性を突かれたりして、顧客情報の流出や、工場の生産停止にまで追い込まれている案件がある。特に製造業においては、生産に直接関係のあるシステムが停止した場合、多大な損害につながる危険性がある。大規模な工場では損害が数億、数十億単位になるかもしれない。海外ではすでにデータ消去、石油プラントの操業停止などの被害が起こっている。

また、情報漏洩に関しては、顧客情報だけでなく営業秘密にも留意する必要があるだろう。例えば、新しく開発される商品に関する情報などがそれに含まれる。そうした情報がライバル企業に漏れ、先に開発・販売されてしまった場合、市場における優位性や競争力が損なわれる可能性がある。製造業のサプライチェーンは国外に広く開放されている場合がしばしばあり、海外の製造拠点を感染源とし、被害が数カ国にまたがるというのは決して珍しいことではない。

「明日は我が身」と真摯に受け止め、被害を未然に防ぐ対策を施すことが重要である。国も製造業のセキュリティの取り組みを後押しする「コネクテッド・インダストリーズ税制（IoT 税制）」の制度を創設した。（図 1）制度利用の申請にあたっては、必要なセキュリティ対策が実施されていることを、情報処理安全確保支援士（登録セキスペ）等のセキュリティ専門家が担保する必要がある。ぜひご相談されたい。

レガシーシステムが足かせと感じる理由



出典：一般社団法人日本情報システム・ユーザー協会
「デジタル化の進展に対する意識調査」（平成 29 年）

表 1　2017-2018 重大インシデント（抜粋）

発生年月	業種	概要
2017/6	自動車製造会社	サイバー攻撃を受け工場の PC が「WannaCry」に感染。ウイルスの感染は確認されたが、金銭を要求するメッセージは表示されなかった。しかし、この影響から一時、工場の生産が停止に。
2017/10	半導体製造会社	地方工場でランサムウェアによる被害が発生。親会社のコンピュータがウイルスに感染し、当該工場にまで拡大。生産にも影響が出た。
2018/5	食料品製造販売会社	運営する通販サイトが不正アクセスを受け、顧客情報が流出した可能性。クレジットカード会社から連絡を受けクレジットカード決済を停止。流出が懸念される情報は約93,000人分に及ぶ。同社は、対象顧客に対してメールと書簡で状況を報告し、カード番号の変更を希望する場合は再発行の手数料を負担するとしている。
2018/6	洋菓子製造販売会社	運営する通販サイトが不正アクセスを受け、登録した顧客 34,149 件のメールアドレスとパスワードが、海外の Web サイトに掲載されてしまった。
	産業機器システム会社	ホームページが外部から不正アクセスを受け、顧客が登録した会員情報が社外へ流出した恐れ。同社は対象となる顧客へメールを送信し、パスワードの変更を要請するなど、注意喚起を行った。

図 1　IoT 税制の仕組み（出典：経済産業省）

【計画認定の要件】

① データ連携・利活用の内容
- 社外データやこれまで取得したことのないデータを社内データと連携
- 企業の競争力上重要なデータをグループ企業間や事業所間で連携

② セキュリティ面
必要なセキュリティ対策が講じられていることをセキュリティの専門家（登録セキスペ等）が担保

③ 生産性向上目標
投資年度から一定期間において、以下のいずれも達成見込みがあること
- 労働生産性：年平均伸率 2%以上
- 投資利益率：年平均 15%以上

課税の特例の内容

設定された事業計画に基づいて行う設備投資について、以下の措置を講じる。

対象設備	特別償却	税額控除
ソフトウェア 器具設備 機械装置	30%	3％ (法人税率の 15%を限度) 5%* (法人税率の 20%を限度)

【対象設備の例】
データ収集機器（センサー等）、データ分析により自動化するロボット・工作機械、データ連携・分析に必要なシステム（サーバ、AI、ソフトウェア等）、サイバーセキュリティ対策製品　等

最低投資合計額：5,000 万円

＊ 計画の認定に加え、継続雇用者給与等支給額の対前年比増加率 ≧3%を満たした場合。

製造業におけるセキュリティガイドライン (例)

独立行政法人 情報処理推進機構：
- 中小企業の情報セキュリティ対策ガイドライン

石油化学工業協会：
- 石油化学分野における情報セキュリティ確保に係る安全基準

一般社団法人 日本ガス協会：
- 製造・供給に係る制御系システムのセキュリティ対策ガイドライン

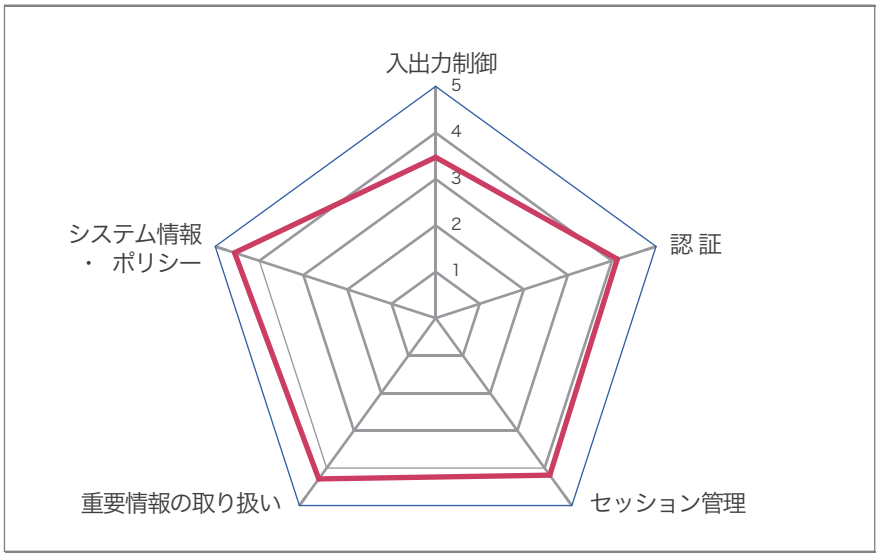
厚生労働省：
- 水道分野における情報セキュリティガイドライン

国際電気標準会議（IEC）：
- IEC 62443-1 シリーズ
- IEC 62443-2 シリーズ
- IEC 62443-3 シリーズ
- IEC 62443-4 シリーズ

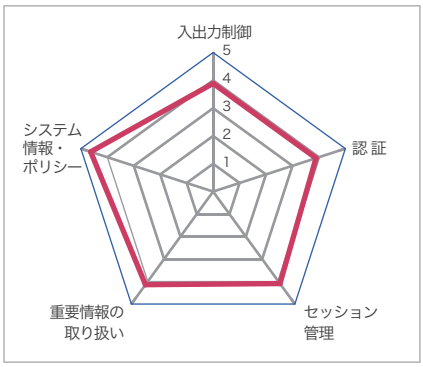
一般財団法人 日本情報経済社会推進協会：
- CSMS ユーザーズガイド

その他の業種

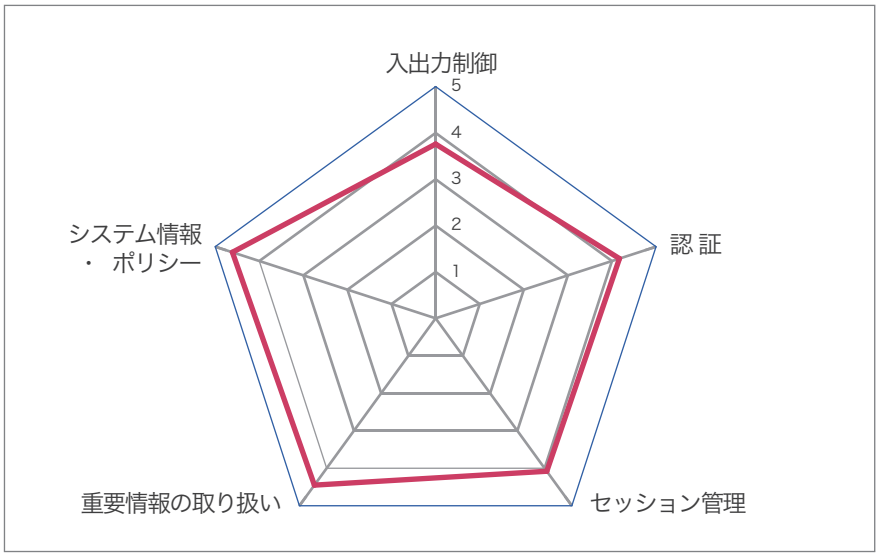
情報通信業



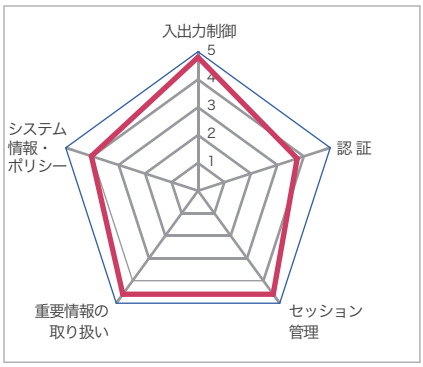
医療，福祉



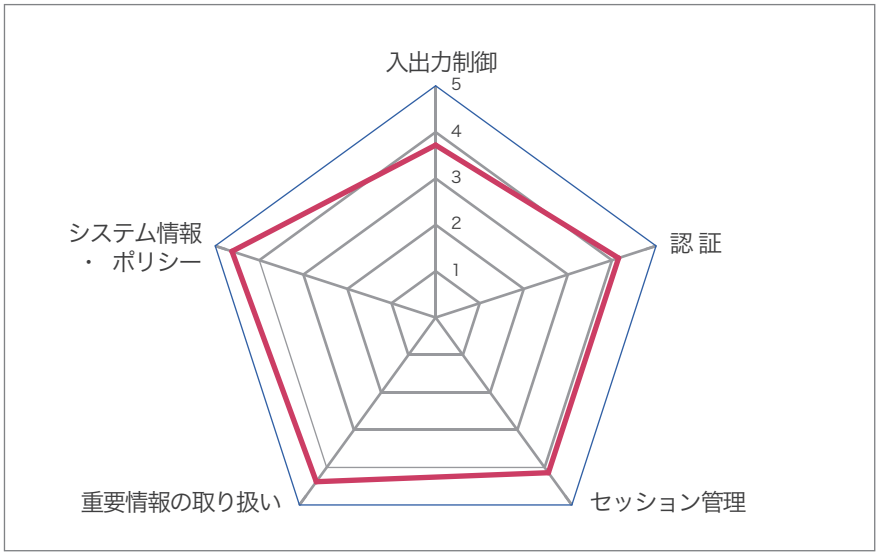
生活関連サービス業，娯楽業



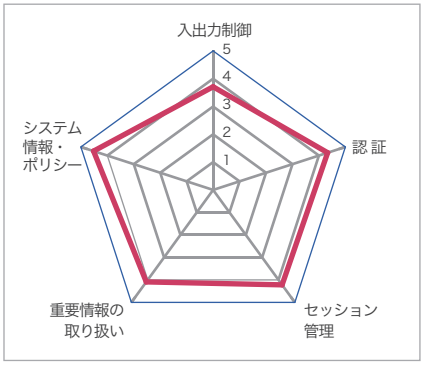
学術研究，専門・技術サービス業



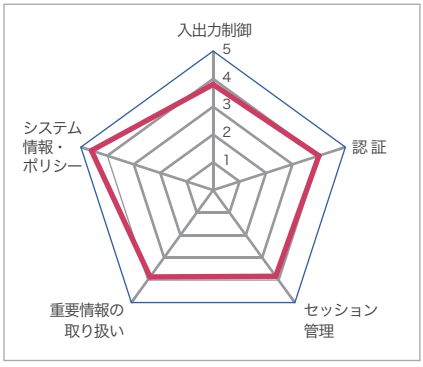
不動産業，物品賃貸業



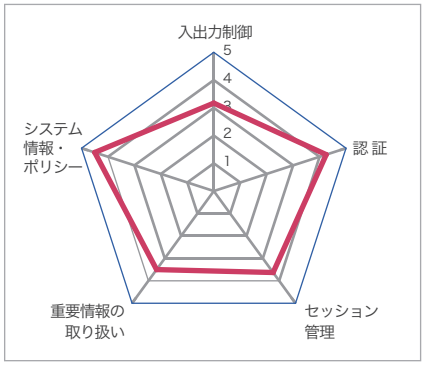
教育，学習支援業



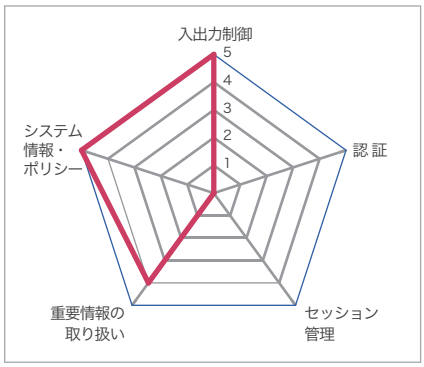
卸売業，小売業



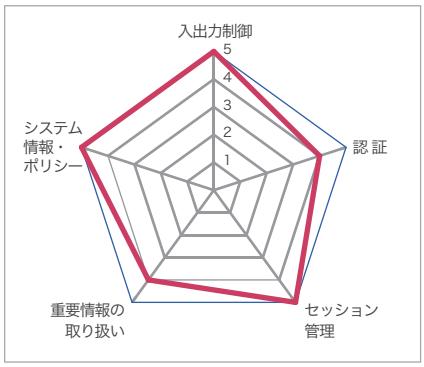
運輸業，郵便業



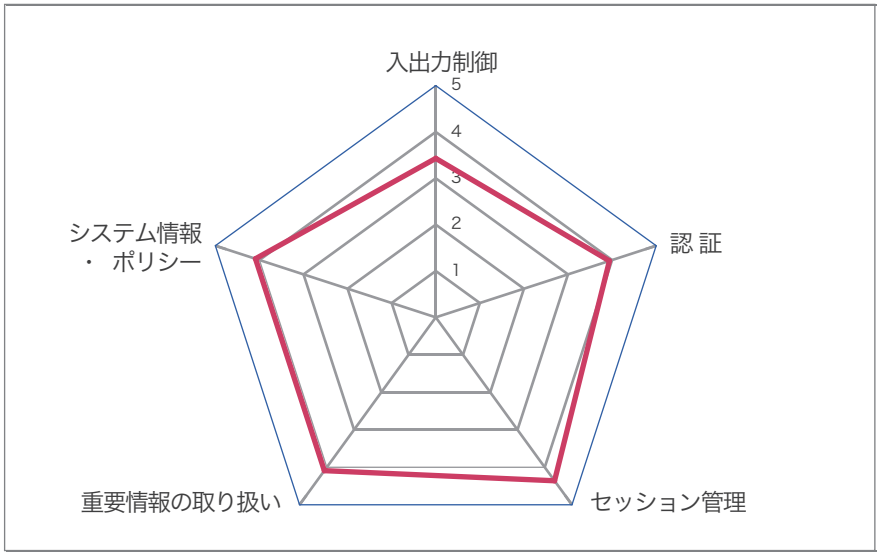
公務（他に分類されるものを除く）



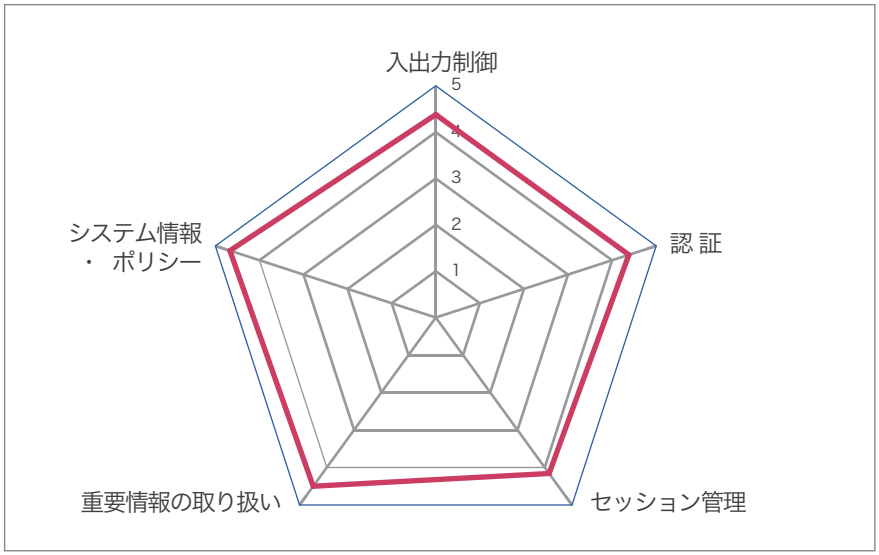
宿泊業，飲食サービス業



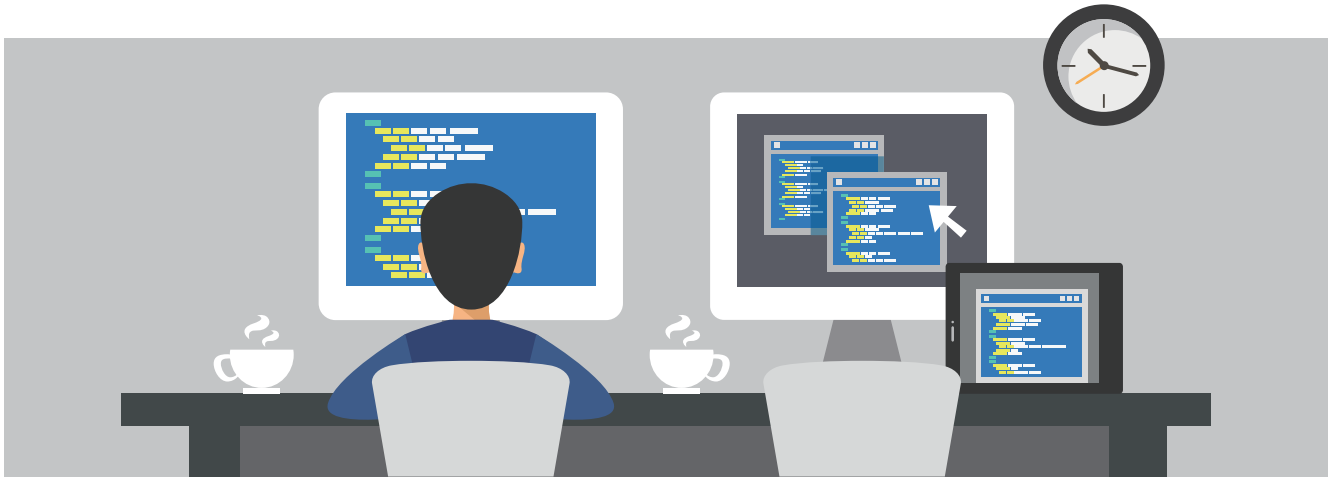
サービス業（他に分類されないもの）



電気・ガス・熱供給・水道業



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



BBSec の CSIRT 構築・運用支援

平時 / 有事それぞれで CSIRT の運営を側面支援してまいります。

セキュリティ・アドバイザリ
（セキュリティよろず相談）

リスクアセスメント
（網羅的弱点調査）

Security Emergency Response Service
（有事の緊急対応）

ログ取得環境整備 /SIEM 構築支援
（プロアクティブモニタリング及び訴求調査の証跡確保）

ログ分析 / パケット分析
（不正通信 / コンプラ違反可視化）

Secure Net Alert Mail Service
（脆弱性情報提供）

CSIRT 構築支援
（名ばかり CSIRT にしないための体制構築）

セキュリティ関連文書整備支援

BISC（インターネット分離クラウドサービス）

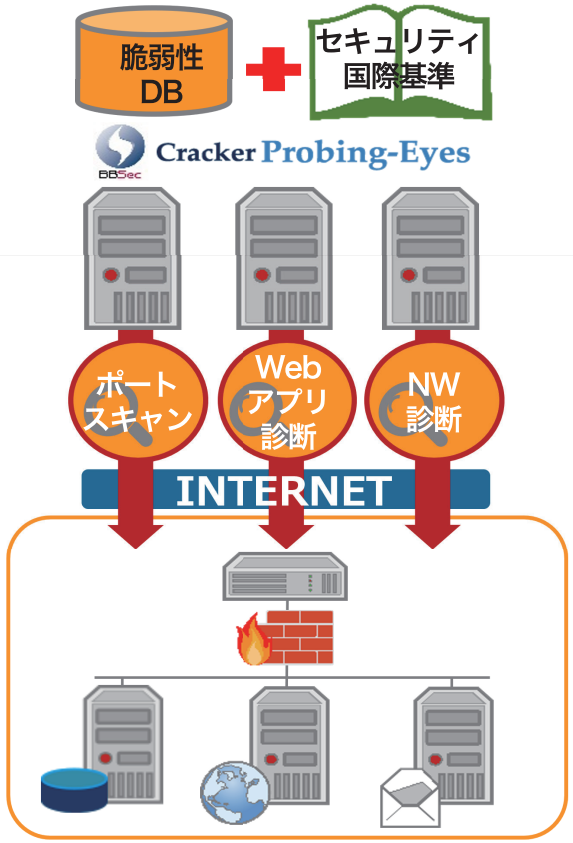
白：平時　黄：有事

今すぐできるホームページセキュリティ

Cracker Probing-Eyes®
（ASP 型外部脆弱性診断サービス）

AI 搭載

毎日診断するので、新たな脆弱性を
いち早く発見します。

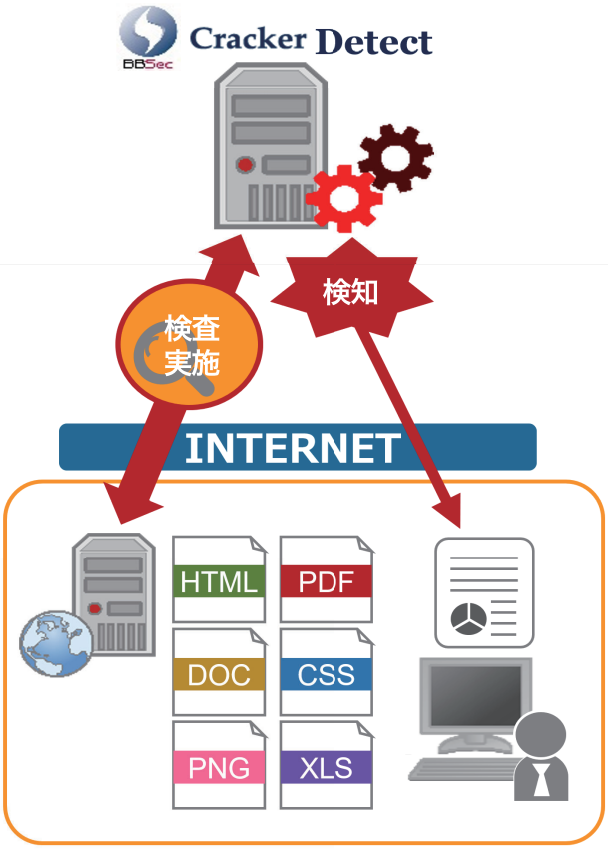


診断結果を Web 上で
いつでも確認可能

Cracker Detect
（Web サイト改竄検知サービス）

予防 ✖ 検知

Web サイトの改竄やウイルスの
埋め込みを高い精度で発見します。



設定／結果確認が
カンタン・便利

設備追加・
システム変更不要！

サービス特長

- ✔ お客様のニーズに合わせた検査周期を自由に設定可能
- ✔ 安心のレポートメール
- ✔ 優れたユーザインターフェース

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

＜事業拠点＞

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

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

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

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