SQAT® SECURITY REPORT

2020年 春夏号

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/
https://www.sqat.jp/

知る・守る
続ける

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

はじめに

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

本レポートは、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2019 年下半期（7 月～ 12 月）の膨大な診断結果からデータを抽出し、集約したものを、当社のエンジニアらの感性も交えてアウトプットしたレポートです。主にサイバーセキュリティのトレンドや展望についてお楽しみいただくことができる内容となっております。

2019 年のラグビーワールドカップ日本大会では興奮と感動に包まれ、さらには東京五輪開催も間近に迫り、色めき立つ日本。国際的イベントが日本で行われることで、世界中の人々との交流もあれば、インバウンド需要が増える機会もあります。しかしながら、浮かれてばかりいられないのが世の常というもの。世界平和を謳った祭典が行われ自国が大健闘した、会場付近の缶ビールの売上が跳ね上がった、などという報道の陰で、開催組織に対するサイバー攻撃が観測された、といった報道も多数見受けられます。

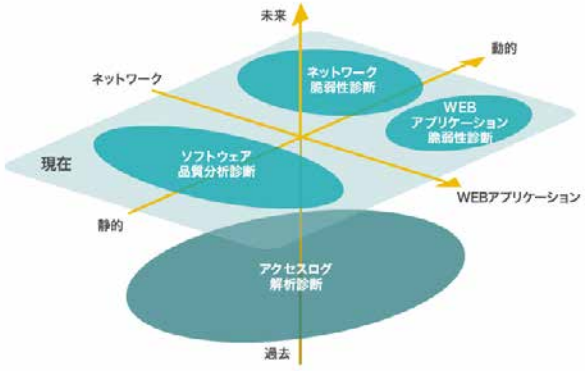
日本のカジノ運営についても、海外からの観光客増加に伴う経済の活性化・景気回復が期待されていますが、一方で懸念されていることもあり、サイバーセキュリティも懸念材料のひとつ。カジノ運営をしている国での情報漏洩などの事件も過去に何度も発生しています。サイバーセキュリティを強固なものにすることは、日本のカジノ運営においても必須といえるでしょう。今号では、日本のカジノ管理システムが守るべき法的要件と対応可能な設計に焦点を当てました。

また、当社エグゼクティブ・フェローが、「Frama-C のもたらすセキュリティ」と題し、クリティカルなソフトウェア、クラウドサービス、あるいは他システムの基盤となるソフトウェア等の安全性や品質が、ソースコード検証を通じてどのように担保されているのかを、実際の検証も交えて書きつづりました。いわば究極の「シフトレフト」を実現可能にする、Frama-C のような形式手法によるソースコード検証ツールは、「攻撃者に付け込む隙を与えない」ソフトウェア開発の解のひとつとなるでしょう。

本レポートが、読者の皆様のセキュリティ対策における有益な情報としてご活用いただけ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 の使命であると考えております。

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 4,800 組織、27,000 を超えるシステムで利用されています。



CONTENTS

巻頭特集

日本のカジノにおける カジノ管理システムの法的要件と設計

株式会社ブロードバンドセキュリティ
取締役（監査・コンサルビジネス・システム化推進管掌） 紫藤貴文

2016 年 12 月に「特定複合観光施設区域の整備の推進に関する法律」(IR 推進法) が成立し、日本でもカジノが解禁されることになった。2018 年 7 月に制定された「特定複合観光施設区域整備法」(以降、IR 整備法) では、具体的なカジノに関する規定が定められ、この法に基づき 2020 年 1 月 7 日にはカジノを監督する機関としてカジノ管理委員会が設置された。2022 年には IR が設置される自治体が 3 か所決定され、開業は 2025 年に予定されている。本稿では、日本のカジノにおけるシステムが遵守すべき法律および標準と、それに対応可能なシステムの設計について述べていく。

カジノ管理システム CMS

一般にカジノはカジノ管理システム (Casino Management System=CMS) と呼ばれるコンピュータプログラムで管理されている。
このシステムは主に

ア）顧客管理
・ハウスカード (残高やポイントを管理するカジノ内で使えるカード) の作成
・顧客の個人情報、残高、ポイントの管理
・プロモーション
・マネーロンダリングの検出など

イ）従業員管理
・シフト管理など

ウ）ゲーム機器管理
・ゲーム機の稼働状況の把握など

に利用されることとなる。

CMS はカジノを運営するうえで中心となるシステムであり、「IR 整備法」で要求されている要件の多くは、実際にはこの CMS で対応することとなる。

カジノに関する法的要件

日本のカジノは IR 整備法などの法規制により、諸外国のカジノとはかなり違ったものとなる見通しだ。後述する 1.1、1.2、および 2 の要件は諸外国でも類似の規制が行われているが、一方でそれ以外の要件は日本独自のものとなる。そのため外国で使われていた CMS をそのまま日本で利用することは現実的ではなく、日本の法規制に合うように変更し、かつ認証を取る必要があるのだ。

1　IR 整備法

1.1 型式検定
カジノで利用する電磁的な機器は、カジノ管理委員会が指定する検査機関の検定を受け合格する必要がある（第百五十一条、第百五十九条）。

CMS もこの対象となるが、具体的な検定方法は法律には記載されておらず、「カジノ管理委員会規則」に記載される予定である。国際的なカジノ関連機器の標準としては、GLI(Gaming Laboratories International) 標準があり、CMS は以下の GLI 標準に準拠する必要がある。

GLI-13	On-Line Monitoring and Control Systems
GLI-16	Cashless Systems in Casinos
GLI-18	Promotional Systems in Casinos
GLI-19	Interactive Gaming Systems

※GLI-13とGLI-19 は必須、GLI-16と GLI-18 は関連する機能がある場合には準拠する必要がある。

このことから日本のカジノ機器の標準も、GLI 標準に類似のものになると考えられる。

1.2 マネーロンダリング防止
第百三条、第百四条、第百五条には犯罪による収益の移転防止、いわゆるマネーロンダリング防止のための措置が定められている。
また、カジノ運営会社は「犯罪移転収益防止法」に基づいて、犯罪収益移転防止規程を定める必要がある (第五十六条)。カジノにおける取引を管理するのは CMS であるため、CMS はマネーロンダリングを検出できる機能を有する必要が

ある。マネーロンダリング・テロ資金対策の国際基準である FATF（Financial Action Task Force）勧告に対応するため、カジノの顧客の取引時確認、確認記録の作成・保存、疑わしい取引の届出等について、罰則を含む必要かつ厳格な措置を講ずることが、IR 推進法の附帯決議として謳われている。

1.3 本人確認

日本のカジノでは、入場者の本人確認を行う必要がある (第七十条)。本人確認には、日本人および日本居住者はマイナンバーカードを、外国からの訪問者はパスポートを用いることとなる。また、以下の記録を残す必要がある。加えて 1.4 で述べる入場回数制限に関する要件を満たすために、こうした情報は日本国内にあるすべてのカジノで共有する必要がある。

一　当該確認をした日時及び当該入場者の本人特定事項（写真を除く）
二　当該入場者が入場禁止対象者に該当するかどうかについての当該確認の結果
三　当該入場者がカジノ行為区画に入場したときは、その入場した日時及び当該カジノ行為区画から退場した日時
四　前三号に掲げるもののほか、カジノ管理委員会規則で定める事項
(第七十条より)

1.4 入場規制

以下に該当する者はカジノに入場することができない (第六十九条)。

一　二十歳未満の者
二　暴力団員又は暴力団員でなくなった日から起算して五年を経過しない者
三　入場料を支払わないもの
四　日本人および日本に居住する外国人で、過去 7 日間に 3 回カジノに入場した者
五　日本人および日本に居住する外国人で、過去 28 日間に 10 回カジノに入場した者
(第六十九条要約)

ここに挙げられている入場回数制限は、個々のカジノだけではなく、日本に存在するすべてのカジノが対象となる。例えば、一週間の間に大阪で 2 回、横浜で 2 回カジノに行くことはできない。また、依存症患者の入場を制限する措置も必要となる (第六十八条)。

1.5 入場料徴収

日本人および日本に居住する外国人は、入場料 3,000 円と認定都道府県等入場料 3,000 円が徴収される (第百七十六条、第百七十七条)。また、カジノ運営会社は入場料と認定都道府県等入場料を、月ごとに国に納付しなければならない。

1.6 クレジットカードの利用

訪日外国人は、クレジットカードを用いてチップを購入することができる (第七十三条)。

当然、クレジットカードを取り扱う場合は、割賦販売法に則ってクレジットカード情報のセキュリティ措置を講じる必要があり、具体的には PCI DSS（Payment Card Industry Data Security Standard）への準拠が求められることとなる。

2 マイナンバー法および個人情報保護法

マイナンバーを扱うため、その取り扱いを「行政手続における特定の個人を識別するための番号の利用等に関する法律」(マイナンバー法) に則って行う必要があり、加えて、個人情報を取り扱うこととなるため、「個人情報保護法」に準拠する必要がある。また、カジノ運営会社がヨーロッパに子会社や支店を有する場合は、GDPR に準拠する必要が生じることとなる。なお、ヨーロッパに子会社がない場合も適用される可能性がある。

3　割賦販売法

PCI DSS に準拠して、クレジットカード情報の機密性を担保する必要がある。

4　犯罪収益移転防止法

マネーロンダリングの防止に関する法律であり、カジノ運営会社はこの法律に従って、マネーロンダリング防止策を策定する必要がある。

5　課税

カジノで得た利益は課税対象となる（訪日外国人の場合は、源泉徴収をすることが検討されている）。このため、利用客がカジノで使うチップの購入額や、勝ち負けを記録するよう事業者に義務付けることも検討されている。

日本における CMS の設計案

このような法的要件を満たすために、日本における CMS は次のような形態になると考えられる。

概要
図 1 に、日本における CMS の概略図を示した。

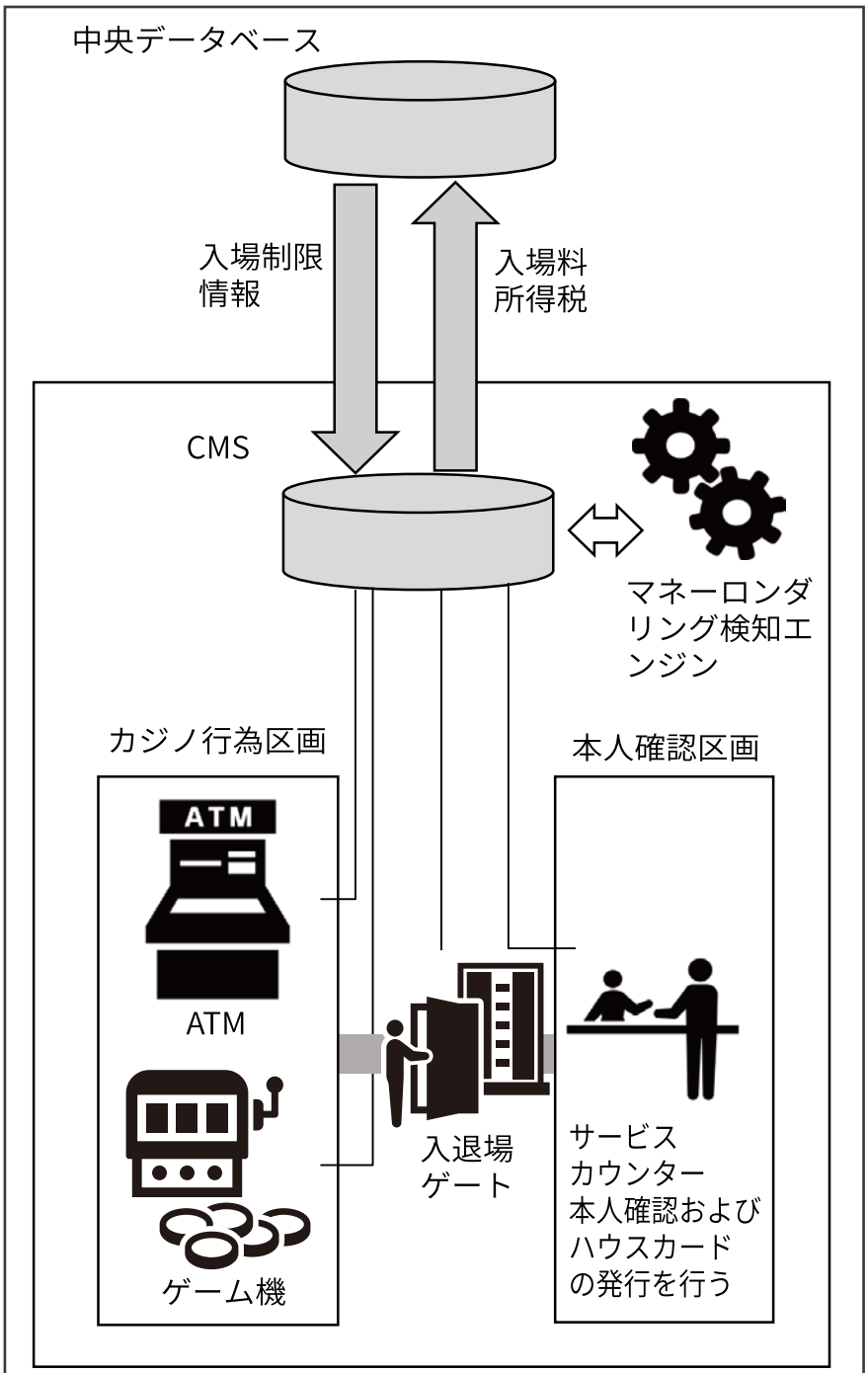
入場規制や入場料・所得税の徴収のために、入退場ゲートや、カジノ管理委員会が管理する中央データベースの設置が必要となる。また、税金の徴収やマネーロンダリングを防止する観点から、個々のゲーム結果を顧客にひもづけて保持する必要があるため、ゲーム機に直接現金を投入することを禁止し、ハウスカードにチャージをしてゲームを行う仕組みにしなければならない。

入退場ゲート
外国の多くのカジノでは入場ゲートを設けていないが、日本の場合、本人確認と入場規制を行う必要があるため、入場ゲートが設けられることとなる。入場ゲートでは、マイナンバーカードやパスポートによる本人確認、入場禁止者かどうかの確認、入場料の徴収が行われ、入場時間が記録される。また必要に応じてハウスカードの作成も行われることとなる。退場ゲートでは、税金の徴収、払い戻しが行われ、退場時間が記録される。
入退場ゲートでは、処理により渋滞が起きることが予想されるため、効率的な処理方法を考案する必要があるだろう。

中央データベースの設置
カジノ利用頻度が高い、反社会的勢力、ギャンブル依存症患者といった人たちの入場制限を実施するために、各 CMS から参照可能な中央データベースの設置が必須となる。また、中央データベースは税金や入場料の徴収機能も有しているほか、精度の高いマネーロンダリング検知の活用にも期待ができる。この中央データベースは、カジノ管理委員会が管理することとなる。

キャッシュレスなゲーム機器
各利用者の収支を把握するために、ゲーム機器やテーブルで現金の取り扱いは禁止され、必ずハウスカードにチャージしてからゲームを行うようになる。ハウスカード番号にひもづいたゲーム結果をデータベースに保存することによって、顧客ごとの収支を把握することが可能である。ハウスカードについては貸し借りができないように、生体認証を用いることも検討されている。

図 1　日本の法律を遵守した CMS



CMS: 顧客ごとに入退場記録、ゲーム結果、残高を管理する。そのため、ゲーム機、ATM、入退場ゲート、サービスカウンターと接続している。また、マネーロンダリングを検出するためのエンジンを有する。中央データベースはカジノ管理委員会が管理する。

チャージ機

日本のカジノは現金でのゲームができないため、現金やクレジットカードからハウスカードにチャージをする ATM が設置されることとなる。もちろん、この ATM はハウスカードにある金額を、現金として引き出すことが可能なものだ。ATM はクレジットカードを扱うこととなるので、割賦販売法に則ったセキュリティ措置が必要となる。また、ギャンブル依存症などへの懸念を受けた対策として、日本人がクレジットカードを利用できないようにしなければならない。

CMSおよび顧客データベース

個人情報保護法、マイナンバー法、PCI DSSおよびGDPRに則って運用する必要がある。具体的には以下のセキュリティ措置をとる必要だ。

- ネットワークや機器の堅牢化
- 個人情報、マイナンバー、クレジットカードデータの暗号化
- ユーザ管理とアクセス制御
- 物理セキュリティ
- 定期的なセキュリティ診断
- 忘れられる権利など GDPR で謳われている権利の実装

また、CMS は不正検知エンジンと連携し、マネーロンダリングを検出できる必要がある。

まとめ

日本のカジノは IR 整備法その他の法律に遵守しなければならないため、既存の CMS を日本でそのまま使用することはできない。日本の法規制に合致するようにカスタマイズし、カジノ管理委員会が指定する検査機関の検定を受ける必要がある。

CMS に対する具体的な要件はまだ公表されていないが、GLI 標準に類似のものになると考えられる。今後、さまざまな事柄が具体的に決定されていくことであろう。

文献

特定複合観光施設区域の整備の推進に関する法律 (IR 推進法)
https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=428AC1000000115

特定複合観光施設区域の整備の推進に関する法律案に対する附帯決議
http://www.shugiin.go.jp/internet/itdb_rchome.nsf/html/rchome/Futai/naikaku1063EFFDA0F22F394925807D00266E7F.htm

特定複合観光施設区域整備法 (IR 整備法)
https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=430AC0000000080_20210726_000000000000000&openerCode=1#613

GLI 標準
https://gaminglabs.com/gli-standards/

割賦販売法
https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=336AC0000000159

行政手続における特定の個人を識別するための番号の利用等に関する法律 (マイナンバー法)
https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=425AC0000000027

個人情報保護法
https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=415AC0000000057

GDPR
https://eur-lex.europa.eu/eli/reg/2016/679/oj

犯罪収益移転防止法
https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=419AC0000000022

PCI DSS
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

FATF 勧告
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

紫藤貴文

取締役 (監査・コンサルビジネス・システム化推進管掌)
山梨大学非常勤講師

長期に渡り、国立大学にて物理化学の研究に従事し、当時より計算機を多用した研究を行う。退職後はフリーエンジニアとして活動し、その後、BBSec に入社。入社後は PCI DSS 案件、P2PE 案件、海外案件、英語が必要な案件などに従事する。プログラミング言語 Python に関する著書あり。

＜プロジェクト担当実績＞
- 決済代行業者、クラウドサービス、データセンターの PCI DSS 準拠支援コンサルタントおよび オンサイト評価
- P2PE 準拠支援コンサルタント
- 大手医療機器メーカーの海外拠点のセキュリティ監査
- 多国籍企業の英語版セキュリティポリシの作成 他多数

＜保有スキルと専門分野＞
- PCI DSS ならびに P2PE コンサルティング
- セキュアプログラミング、ネットワーク、データベース、暗号

＜保有資格＞
- PCI SSC 認定オンサイト評価人 (QSA)
- PCI SSC 認定 P2PE 評価人 (QSA(P2PE))
- CISSP (Certified Information Systems Security Professional)
- テクニカルエンジニア (情報セキュリティ)
- 理学博士

注目テーマ

Frama-C のもたらすセキュリティ

株式会社ブロードバンドセキュリティ
エグゼクティブ・フェロー　安藤 一憲

本稿はC言語のわからない方も、ゆくゆくは一般に「プログラミング言語」に適用できそうな話だと思って読んでいただきたい。ソフトウェアのバグで航空機が飛べなくなり、航空機メーカーの業績にも影響する昨今、ソフトウェアの品質管理はどの会社にとっても重要な課題である。すでにソースコード診断でセキュリティや品質を担保しているお客様も多い中、本稿ではエアバス社等で使用されているソースコードの検証ツールを紹介する。

C言語のソースコード解析ツール Frama-C

「ソフトウェアはソースコードに書いた通りに動作するのか?」という命題にはさまざまな答えがあろう。コンパイルエラーが出るもの、実行時にエラーで止まるものもある。ソースコードの脆弱性をチェックするツールはすでに弊社診断サービスにも使われているが、さらに精度を上げて厳密にやろうとすると、定理証明支援系と呼ばれるツールが存在する。

数理論理学では、正しい定理から演繹的に推論を積み重ねて得られる定理は正しいといえる。定理とは証明の与えられた命題である。したがって、ソースコードにおいて、命題に相当する「型」と証明に相当する「プログラム」が与えられていれば、そこから演繹的に積み上げていった型とプログラムは正しいセット、すなわち正しいソースコードといえることとなる。こうしたツールで最も有名なのはたぶんフランスの INRIA [*1] で開発された Coq であろう。Coq は OCaml という言語で書かれており、「命題の証明」を積み上げていって、証明できたものに関しては OCaml 言語でプログラムが抽出できる。しかしながら、我々の目の前にあるのは例えば C 言語などのソースコードであり、プログラマは必ずしも抽象化された命題の証明を書きたいわけではない。数理論理学の言うように、命題が「型」であり証明が「プログラム」に対応するのであれば、C 言語などのソースコードはそもそも証明の一部を成すはずであり、それが論理的に正しい（ソースコードの記述に不具合がない）かどうかをチェックできればことは足りる。つまりバグがないことを数学的に証明できればよい。

そこで登場するのが、同じフランスの原子力・代替エネルギー庁の CEA-LIST [*2] で開発された、Frama-C である。Frama-C は Coq と同様に OCaml で書かれているが、Coq とは違って「C 言語のソースコード解析ツール」であり、C言語（C99）のソースコード解析のためのプラグインの集成という体裁が取られている。ソースコードのチェックツールではあるが、そのプログラムを実行せずに実行エラーを検知したり、変数の取り得る値をチェックしたりできる。

簡単な使い方としては、C 言語のソースコードをそのまま Eva プラグインでチェックすることで、実行時エラーがないことを確認できる。これだけでも脆弱性を大幅に減らすことができるだろう。Frama-C のサンプルサイトには、わざと問題がある gzip-1.2.4 などのソースコードがサンプルで集められているが、Eva プラグインに食わせてみると、ソースコードに問題がある部分がオレンジ色のバルーンで示される。カバーできなかったコードは赤で表示される。動作するようになったプログラムを、これでチェックしてみるだけでも十二分に価値がある。

さらに、論理的あるいは数学的な検証を動作させるのに必要なのは、C 言語のソースコード自体と、ソースコード中にコメントの形で追加する ACSL（The ANSI/ISO C Specification Language）で記述された関数やループ構造の動作前提条件や仕様である。検証を受け持つのは Wp プラグインである。この「Wp」という名称は 1967～69 年にロバート・フロイド、エドガー・ダイクストラ、アントニー・ホーアらが提唱しその後改良が重ねられて来た「Weakest Preconditions calculus（最弱事前条件計算）」にちなんで名付けられている。Wp プラグインの下には、推論的プログラム検証プラットフォーム Why3 を介して、前述の Coq や SMT ソルバー [*3]（prover）を複数配置することができる。

ちまたでは AI がバズワードになっているけれども、SMT ソルバーはなかなか表には出て来ないものの、人工知能分野の成果物のひとつである。Frama-C でデフォルト利用される prover は Alt-Ergo であるが、前述の Coq や

マイクロソフトリサーチ製の Z3 や、スタンフォード大学とアイオワ大学等の共同プロジェクトで Google、Amazon Web Service、DARPA、Intel、NASA等のサポートを受ける CVC4 など、著名な SMT ソルバーを外部 proverとして並列に利用することができる。Wpプラグインのマニュアルにも「Coq、Gappa、Z3、CVC3、CVC4、PVS その他の多くのproverがWhy3を介してアクセス可能」と書いてある。まだまだいろいろなものが使えるようだ。すべての prover が Why3 の下に配置されたのは最新バージョン（20.0 Calcium）からのようで、ネット上で検索にかかる古いバージョンの説明文書は役に立たないが、Alt-Ergo や Coq や Z3 や CVC4 を直接知らなくても、それらを動作させて検証結果を得ることができる。動作させたいSMTソルバーはコマンドラインオプションで選択指定が可能だ。Frama-CはGUIを備えているがコマンドラインでも使える。実際に動く簡単なプログラムを書いて検証してみた。

```
#include <stdio.h>

void swap(int *a, int *b){
   int tmp = *a;
   *a= *b;
   *b=tmp;
   return;
}

int main(void){
   int a = 11;
   int b = 23;
   int c = 37;
   int d = 0;
   const char *fmt = "d: a/b/c = %02d: %02d/%02d/%2d\n";

   while (d < 17){
      swap(&a,&b);
      swap(&b,&c);
      printf(fmt,d,a,b,c);
      d++;
   }

   return 0;
}
```

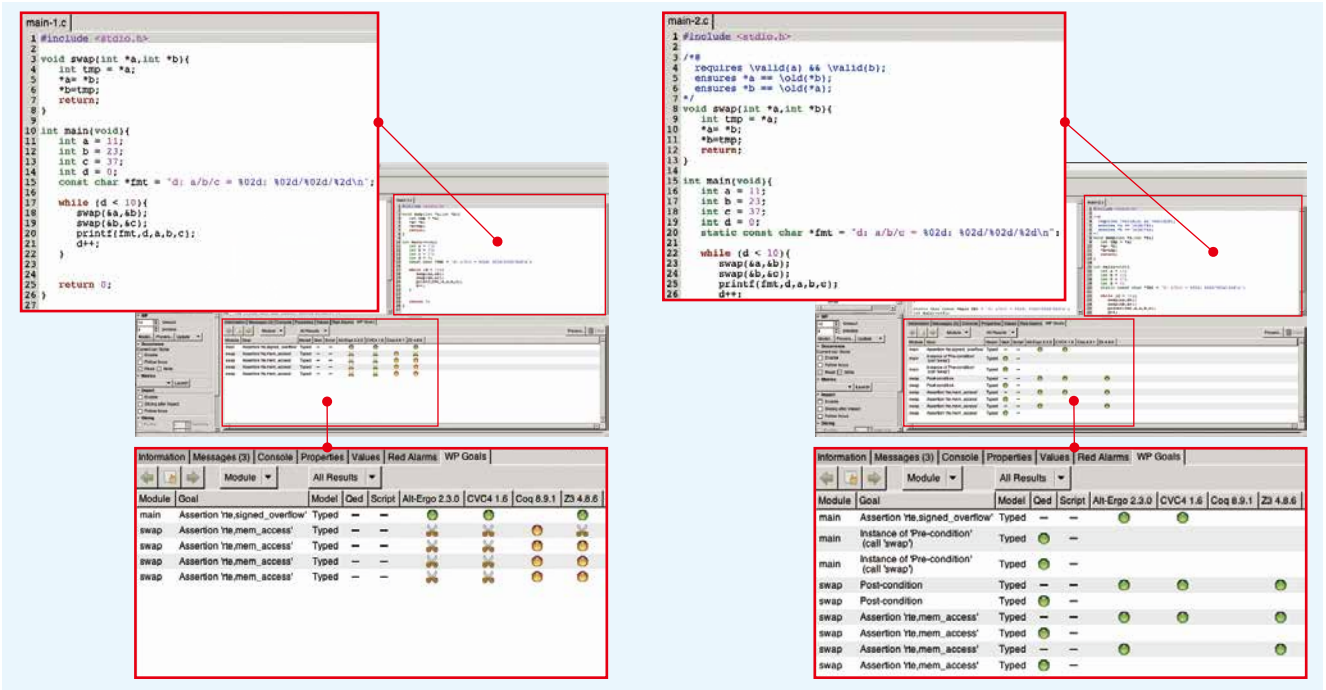
試しに ACSLで書くべき前提条件や仕様をまったく書かずに、これを Frama-C の Wpプラグインに食わせてみると、5 件の固有性の検証（goal）が走り、そのうち 1 件しか正当（valid）と判定されなかった。検証されると緑のバルーン、検証失敗だとオレンジのバルーン、prover がタイムアウトするとハサミのアイコンが表示される。さすがにソースコードだけでは論理的な検証をするには情報不足のようだ。どの部分がどのような検証に失敗したのかは、GUIからドリルダウンできるようになっている（左下図）。

GUI の表示を見ると swap() という関数が検証できていないようなので、その関数の直前に ACSL で動作前提条件を加えて、もう一度 Frama-C の Wpプラグインで検証してみる。加えたのは以下 3 行の ACSL 記述である。

```
/*@
    requires \valid(a) && \valid(b);①
    ensures *a == \old(*b);②
    ensures *b == \old(*a);③
*/
void swap(int *a, int *b){
…
```

①: a と b の入力値は有効な範囲にあり
②: 実行結果の *a は入力値の *b と同じ
③: 実行結果の *b は入力値の *a と同じ

すると、9 件の固有性の検証が走りすべてが正当と判定された。Wp プラグインのマニュアル例をもとに、実際に動くように書いたプログラムではどう検証されるのかを確かめるために用意したショボいプログラムではあるが、たった 3 行の ACSL 記述を加えただけで、人工知能分野の成果物である複数のSMTソルバーが動員されて「正当」という判定結果が出てしまった（右下図）。ちなみに Frama-C のサイトにある ACSL-1.14 のマニュアルは 118 ページしかない薄い本である。論理演算子なんかはすべて C 言語と同じ。おかげで関数の仕様を書いたコメ



ントだと思って読めば前提知識がなくてもなんとなく読めてしまう。ただし、まだ泣き所もあって strlen や strcpy など文字列操作関数を記述するための ACSL 側の道具立てが弱い。まぁ今後何らかの改善がされてくるだろうけれども、この Wp プラグインでの検証は、Eva プラグインでの検証と違ってプログラムが実行できなくても、関数単位で実施できるのが味噌である。

このように論理的にソースコードをチェックする手法は Formal Method（形式手法）、あるいは Light-Weight Formal Method（軽量形式手法）と呼ばれる。Frama-C は CEA-LIST 製のオープンソースツールで、ライセンスはほぼ LGPLv2 互換であり、商用ライセンスも用意されている。作っているのは重要インフラのど真ん中にいる人たちということになる。原子炉の制御プログラムが脆弱性だらけとかいう事態だけは勘弁願いたいという思いは世界共通であろう。実は 2000 年に策定された ISO/IEC 61508 は電気・電子分野における「機能安全」と呼ばれる国際規格だが、この中で安全度基準（SIL）が 4 段階規定され、レベル2以上でこの「形式手法」の利用が推奨されている。ISO/IEC 15408 は IT 製品のセキュリティに関する国際標準で、Common Criteria と言った方が知っている方は多いかもしれない。情報セキュリティの実現度は評価保証レベル（EAL）で7段階規定され、EAL5 以上で軽量形式的な設計記述が要求され、EAL6 で軽量形式手法による検証、EAL7 で形式手法による検証が要求される。EAL5 以上は「軍用や特殊用途向け」と言われていて、一般になじみがないのはそのせいかもしれないが、これら形式手法のツールが原子力関連や航空機関連で使われているのは、規格上の必然でもある。[*4]

Frama-C 自体は macOS 上で開発されているようで、Homebrew と OCaml 系ソフトウェアのパッケージ管理ツールopamを使うと、あっさり最新版（20.0 Calcium）がインストールできる。Ubuntu などでもパッケージでインストールすることもできるが、Frama-C 自体のバージョンが古く、最新の機能が使えず、プラグインの構成も異なるため、この記事を書くにあたっては macOS 上で動作する最新バージョンで動作確認している。

ソフトウェア信頼性向上とセキュリティ

Formal Method の歴史は古いこともあって、Frama-C 以外のチェックツールもいくつも存在している。マイクロソフトは、Windows のデバイスドライバをマイクロソフトリサーチ製の SLAMというチェックツールで検証しており、そうすることで Windows のセキュリティ向上に貢献しているという記述も見つかる。さらに検索してみると案の定、SLAM の精度とパフォーマンスを上げるために Z3 を使っているという情報も見つかる。[*5]
プログラムだけではなく、TLS 1.3 のプロトコル安全性の検証にも Formal Method なチェックツール ProVerif や Coqが併用されたことはよく知られている。

さらに、Amazon Web Service は、Leslie Lamport 先生（LaTeX の原著者で現在マイクロソフトリサーチ所属）作の TLA+ という形式手法を実現する言語で、サービスに使用するプログラムをチェックしている。たまに「似たような機能を実現しているプログラムなのに AWS で使用しているプログラムにだけ脆弱性がない」という事象を目にすることがあるが、その理由のひとつはこの TLA+ を含む検証の成果であろう。代表的なところで Amazon S3 はこのツールによる検証を経て作られている。[*6]

クラウドベンダーのソフトウェア信頼性向上にこれらの Formal Method な検証ツールが使われていることは一般には意外と知られていないが、航空機の安全性だったり、OS の安全性だったり、暗号化プロトコルの安全性だったり、クラウドサービスの安全性だったり、クリティカルなソフトウェアの安全性を向上させるために実際に利用されている。20 年以上の歴史があるのに、これらが表にはなかなか出て来ないのは、これらのツールの多くが、プログラマから見ると飛びつきにくい代物にしか見えないことに起因していると思われる。しかし、世の中には C 言語プログラマに優しい Frama-C のようなツールがあり、使う気になればいつでも使えるということは知っておいた方が良い。TLA+ の仕様などを含めて、筆者の頭の中にあった「形式手法による検証はひたすら面倒くさい」という先入観は、Frama-C であっさりと打ち砕かれた。実際エアバス社では、航空機を飛ばすためのプログラムを、すべて Frama-C でチェックしていると聞く。これは作りたての実験的なものではなく、実戦で使われて何年もかけてアップデートされているツールである。検査の実現レベルは軍か特殊用途向けとされる EAL5 に相当するけれども、ツール自体はなんとオープンソースである。

ソフトウェアの信頼性が、セキュリティと何の関係があるのかと思う方もおられるかもしれない。マルウェアがソフトウェアのバグや脆弱性を突いて感染を拡大することを見ればわかるように、ソフトウェアの信頼性を向上させバグの混入を防ぐことは、セキュリティの言葉に翻訳すると「攻撃者に付け込む隙を与えない」ことを意味する。理屈としては攻撃者だけではなく、ペンテスターに対しても付け込む隙がなくなる。攻撃者／ペンテスターが「脆弱性の1本釣り」であるならば、Formal Method によるソフトウェア検証は「脆弱性の底引き網」に相当する。

現状を見てみると、せっかく Formal Method でチェックされたコードで作られたサービスを利用していても、その上で自前の未チェックコードを動作させることで、セ

キュリティ上の問題が発生することは多々あるようだ。チェック済みのコードで構成されたクラウドサービス上で、自前のソフトウェアを併用して同レベルの安全性を確保しようと思う場合には、Formal Method なチェックツールの利用は解のひとつになり得る。もちろん開発の初期段階から利用することで、最初から不用意なバグの混入を防ぐ使い方が推奨される。この手のツールはいわば究極の「シフトレフト」を実現するツールである。なお、本稿に登場させた SMT ソルバーの調査過程で、Java、C++、Python など、各言語のプログラムのチェックに利用できるツールの存在もいくつか目に入った。これは各言語でプログラムの信頼性を高めようと努力している人たちがいるという証左である。Formal Method を使ってプログラムの信頼性を確保しようという試みは C 言語と Frama-C だけに限った話ではない。Formal Method のチェックツールの裏で、SMT ソルバーを使うこと自体がトレンドになっているようだ。それらも含めて今後の動きに注目したい。ただ、Frama-C はそれらのチェックツールの中でも抜群にかっちょいい。

おわりに

実は本稿を書くにあたって与えられたお題は、「クラウドのセキュリティ」だった。多くの記事がそれを題材にしながら、Amazon Web Service や Microsoft や Google が地道にやっているソースコードレベルでのセキュリティ対策を取り上げてこなかった。大声で「シフトレフト」を叫んでいる方面からも、「形式手法」という声は聞こえて来ない。クラウドのセキュリティは、実は「軍や特殊用途向け」として一般には目が向けられてこなかった方法で担保されているのである。それを記事にするかどうかでも悩んだ。検索しても日本語で出て来るのはせいぜい国立情報学研究所の先生の研究プロジェクトくらいだ。しかも、クラウドベンダーの使っているツールを見ると、お世辞にもプログラマとの親和性が高いとは言い難い。多くは論理記号を使ってプログラムとは別に仕様を書き下すタイプのものだ。それらの取り組みを紹介するだけでは、開発の現場に対してあまり現実味がない。どうしたものかと思案しているところにレジリエンスな研究室の門林先生から Frama-C の紹介があって、この記事になった。聞くと笑顔で作者が知り合いなのだと言う。さすがの知見の広さとタイミングの良さに感謝したい。クラウドに限らず、ツールが進化することでこういった技術が身近になり、形式手法であらかた脆弱性がつぶしてあるルータや IoT 機器等の製品が増えてくることに期待したい。

安藤 一憲
エグゼクティブ・フェロー

学生時代からネットワーク／サーバ管理に 30 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。古くは Sendmail（MTA）のエキスパートとして知られるが、現在は社外との共同研究や M3AAWG 等国際会議に参加しつつ海外動向と先端技術担当を勤めている。

＜プロジェクト担当実績 (BBSec のみ)＞
- 2005 年 メール ASP（AAMS）を企画設計構築し事業化
- 2009 年 Cracker Detect EXOCET（Web コンテンツ改竄防止ソリューション）を企画立ち上げ
- 2012 年 メール ASP にアカウントの乗っ取り検知実装を主導
- 2014 年 Dovecot Pro/Scality の導入を主導
- 2015 年 Splunk SIEM 導入を主導
- 2018 年 AI 搭載自動脆弱性診断サービスの監修

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

*1 国立情報学自動制御研究所
*2 システム統合技術応用研究所
*3 一階の述語論理式の充足可能性を判定するためのツール
*4 https://www.ipa.go.jp/security/jisec/forusers/abouteal.html
https://frama-c.com/index.html
https://www.ipa.go.jp/files/000066608.pdf
*5 https://www.nii.ac.jp/TechReports/public_html/07-007J.pdf
*6 http://lamport.azurewebsites.net/tla/amazon-excerpt.html
https://cacm.acm.org/magazines/2015/4/184701-how-amazon-web-services-uses-formal-methods/abstract

診断の現場から

セキュリティサービス本部 診断サービス部

アンドリュー クロフト

金（キム） 泰熙（テヒ）

日本、そして情報セキュリティとの出合い

編集部：BBSec には外国籍の社員も在籍していますが、本日は、セキュリティサービス本部 診断サービス部で活躍しているクロフトさんと金さんに、お話を伺いたいと思います。ではまず、おふたりが来日した経緯を教えてください。

クロフト：私はオンラインゲームやアニメが好きで、そこで日本語に触れるうちにマスターしたいと思うようになりました。日本の大学に留学して勉強した後、せっかく学んだので、日本で日本語を使う仕事をしたいと考えました。

金：私はもともと、外国で人生を開拓してみたいと思っていました。交換留学で京都に来てから、日韓の文化の研究に興味を持ち、兵役や大学の日本語アカデミーで学びました。韓国では、日本の IT 業界で働きたいと考えている若者が多く、私もそのひとりでしたので、希望が叶って嬉しいです。

編集部：情報セキュリティに興味を持つようになったきっかけは？

クロフト：イギリスにいた 16 歳のころ、ハッキングを勉強している友達がいて、「おお！ それカッコイイ！」と飛びつきました。掲示板や Web サイトで仕組みを調べ、簡単なツールを使ってハニーポットでクロスサイトスクリプティング[*1]を発生させて遊んでました。そのころは今ほど高度な知識はなかったですね。

金：私はまず、プログラミングなど IT の基礎的なことを韓国で勉強しました。いずれはその知識を仕事に活かしたいと考え、そこからセキュリティに関して意識するようになりました。

編集部：日本と母国で情報セキュリティの違いはありますか？

金：韓国では、セキュリティソフトウェアについて、日本より義務的に導入が課せられていると感じます。例えば、ある銀行のサイトを利用するときは、セキュリティソフトウェアモジュールの設定が義務化されています。

クロフト：イギリスはブレグジット（EU からの離脱）しましたが、情報セキュリティ面では引き続き連携する必要がありますね。GDPR に準拠するため、プライバシー管理については日本より厳しいと感じます。

金：でも昨今の日本は、政府主導でソーシャルエンジニアリングに対する防御対策するなど、意識が高まってきているんじゃないかと感じてます。

編集部：韓国やイギリスにも「オレオレ詐欺」のようなものはありますか？

金：もちろんありますね（笑）。

クロフト：そうですね。「ナイジェリアの王子様がメッチャお金くれるよ。」というのもありますし（笑）。あと、クレジットカードスキマーも多くて、よく報道されているので、使う前に機械を調べますね。でもやっぱり高齢者は被害に遭いやすいので、今後も啓発が必要だと感じます。

編集部：情報セキュリティの仕事をする前からセキュリティに対する意識を持っていましたか？

金：IT の勉強を始めたころセキュリティに対する意識が深まりましたが、セキュリティに対する意識は、企業によってまちまちだと思います。トレーニングが必要なのではないかと感じるケースも時々あります。

クロフト：以前から意識してましたが、セキュリティの仕事をするようになり、より過剰に意識するようになったと思います。大きな企業だったら充分に徹底しているだろうと思っていたけど、そうではないところもあると分かり、情報セキュリティの現状は、思っていたよりもろい、ということに気付いてしまいました。

編集部：普段はどのような勉強をしていますか？

クロフト：私にとって「人生はハッキング！」です。それぐらいやりがいを感じているので、毎日ずっと、常に勉強しています。通勤中はもちろん情報を調べていますし、家に帰ったら Black Hat[*2] などのハッキング動画を見たり、もっと効率化できる方法や、普段検証しないような新しい脆弱性や高度な知識が必要な脆弱性について調べたりしています。

金：私は、脆弱性や診断方法などについて、同僚のみなさんに毎日教えてもらっていて、仕事をしているというより、日々勉強させてもらっているという感覚で働いています。

情報セキュリティは楽しい

編集部：これから情報セキュリティ業界に就職・転職しようと考えている人に、仕事の面白さを教えてください。

クロフト：とにかく毎日が新しいです。脆弱性自体はそれほど大きく変化しませんが、発生の仕方がそれぞれのシステムによって違うので、推測して攻撃コードを試すとか、パズルを解くような仕事で面白いです。問題は必ずどこかにある、という前提でシステムの構造を調べ、論理的に考えて答えを導き出す。脆弱性が存在していること自体は悪いことなんですが、見つけることができた、という達成感がありますね！

編集部：どういう人が診断エンジニアに向いていると思いますか？

クロフト：好奇心があって勉強に熱心な人ですね。セキュリティ診断手法自体は世間に広く知られていないので、ゼロから始める人が多いと思います。基礎から積極的に自分で勉強し、常に最新の情報を把握して活用するという熱心さも必要ですね。

金：どんな仕事でもそうですが、自分の仕事に責任を持てない人は難しいんじゃないかと思います。

編集部：普段の業務に関してお聞きします。診断しているシステムで、脆弱性がいっぱい出てしまった場合、診断員として、どのような感情が起こりますか？

クロフト：たくさん出るとワクワクしちゃいますね（笑）。報告書としてまとめるのは大変だけど、知恵を振り絞って試行錯誤して、見つけにくい脆弱性を発見できたときには達成感があります。逆に、単純な脆弱性がたくさん出てきてしまうと、なんでこんな作りにしてるんだろう…と、怒りではないけれど、ガッカリな気持ちになってしまいます。

金：私はいま再診断 *3 を担当していますが、本診断 *3 で見つかった重大レベルなどの脆弱性が修正されてくると嬉しいですが、修正されていないと…お客様の事情もあるので仕方ないのですが、残念な気持ちになります。これから本診断を担当して、私も脆弱性を見つける喜びを早く味わいたいです！

編集部：仕事上の悩みや困ることってありますか？

クロフト：怪しいと思われる部分があって、本当はもっと複雑なパターンを試してみたいんだけど、診断範囲外や、契約上の制約などでできない、というのはエンジニアとしてメチャメチャもどかしさを感じます。

編集部：エンジニアって、ひとりで黙々と作業する…と思われがちですが、実際はコミュニケーション能力も重要ですよね？

クロフト：お客様にお問い合わせする際、分かりやすく伝えられなければ効率的に仕事を進められません。私はまだ報告会に行ったことはありませんが、脆弱性の再現方法や対策など、お客様が求める情報を分かりやすく伝える必要がありますね。

金:アメリカのシリコンバレーの話ですが、分かりにくいコーディングをする人は解雇対象になる、という逸話を聞いたことがあります。どのような複雑な内容でも、相手の立場や状況を考え、可読性といいますか、理解可能な説明をすることが重要だと思います。

クロフト：情報セキュリティに関することで、これは常識、と思っていることを、例えば IT に詳しくない相手に伝えるとき、どんな風に説明すれば理解してもらえるか。ちょっと苦労するときはありますね。

編集部：そういった説明をするときに、母国語の方が楽なんじゃないですか？

金：母国語だったらより詳細に、という部分はあると思いますが、言語問わず、相手が理解できるように伝える、ということが一番かなと思います。

クロフト：論理的に説明するということを意識しているので、特に極端な感情が交じらない分、普通に説明すれば通じるので、英語が楽、日本語が楽、というのはないですね。

編集部：ところで、おふたりとも日本語がとても上手ですが、敬語などで困ることありませんか？

クロフト：大学の日本語の授業で敬語や手紙の書き方を教わりました。さらに、前職は営業職でテレアポもしてましたので、丁寧な言葉遣いや敬語を早くからたたき込まれたと思います。逆に、英語のビジネスメールは自信ないです（笑）。

金：私も韓国のビジネス日本語教室で敬語の使い方を集中して勉強しました。おかげで丁寧な言葉遣いが身についたと感じています。

編集部：なるほど、まず敬語を勉強するから違和感なく使えるんですね。我々日本人の方がちゃんと敬語を使えるか…怪しい部分がありますよ（笑）。それでは最後に、今後の目標を聞かせてください。

クロフト：日々努力して勉強して、一流のハッカーになりたいです。多くのシステムを診断して、たくさん脆弱性を見つけたいですね。スキルを磨いて、ハッキング大会で声をかけてもらえるような、世界有数のハッカーになりたいです。さらには、論文を書いたり講演をしたりしてみたいですね。

金：まずは本診断の業務を早く覚えて、重要な役割を多く担えるようになりたいです。そして、「情報処理安全確保支援士」や、「CISSP 認定資格」*4 などの資格を取りたいです。

*1 外部から入力された値を出力する際に適切な処理が行われていないため、ブラウザ上で表示内容の改竄やプログラム実行などが可能となる問題。
*2 世界最大規模のサイバーセキュリティの国際カンファレンス。世界中の研究者が日々の研究成果を発表する場となっている。
*3 当社では診断後 3 カ月以内であれば希望するお客様のシステムを再診断しています。本ページでは通常の診断を再診断と区別するため、本診断と表記します。
*4 $(ISC)^2$ (International Information Systems Security Certification Consortium) が認定を行っている国際的に認められた情報セキュリティ・プロフェッショナル認証資格。

アンドリュー クロフト
イギリス・リバプール出身。好きなサッカーチームはもちろんリバプール FC。スコッチウイスキーが大好き。

金 泰熙
韓国・ソウル出身。趣味は日本文化の研究。帰省したら絶対に行く飲食店がある。サムゲタンが絶品で超オススメらしい。

診断結果にみる情報セキュリティの現状

～　2019 年下半期　診断結果分析　～

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

BBSec の診断について

当社では、Web アプリケーション、ネットワーク（プラットフォーム）、スマホアプリ、IoT、パブリッククラウド、ソースコード、標的型攻撃に対するリスク可視化等、様々な局面における診断サービスを提供することで、お客様のニーズにお応えしている。

当社の脆弱性診断サービスは、専門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、検出された脆弱性に対するリスク評価について、右表のとおりレベル付けしている。お客様のシステム特性に応じた脆弱性の検出、リスクレベルの評価、個別具体的な解決策の提供が適切に行えるよう、高い頻度で診断パターンを更新し、診断品質の維持と向上に努めている。

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

2019 年下半期診断結果

当社では、2019 年 7 月から 12 月までの 6 カ月間に、14 業種延べ 537 企業・団体、4808 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・組織側の姿勢もあり、診断案件数は年々増加している。脆弱性の検出率は次ページのとおりである。

診断の結果、Web アプリケーション診断では、脆弱性が検出されたシステムが全体の 81.5% と、前年同期（2018 年下半期）の 84.9% に比べて微減しているものの、依然として高い割合である。ネットワーク診断においては、脆弱性検出率はシステム全体の 47.8% であり、2017 年下半期以降、減少傾向にあるが、およそ半数のシステムに何らかの脆弱性が検出されている。

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 26.9%、ネットワーク診断では 30.4% 検出されている。前年同期比（2018 年下半期「高」レベル検出率：Web アプリケーション 27.6％／ネットワーク診断 17.8%）でいうと、Web アプリケーションはほぼ横ばいだったが、ネットワークは 12.6 ポイント増えておりリスクレベルの高い脆弱性が増加傾向にある。

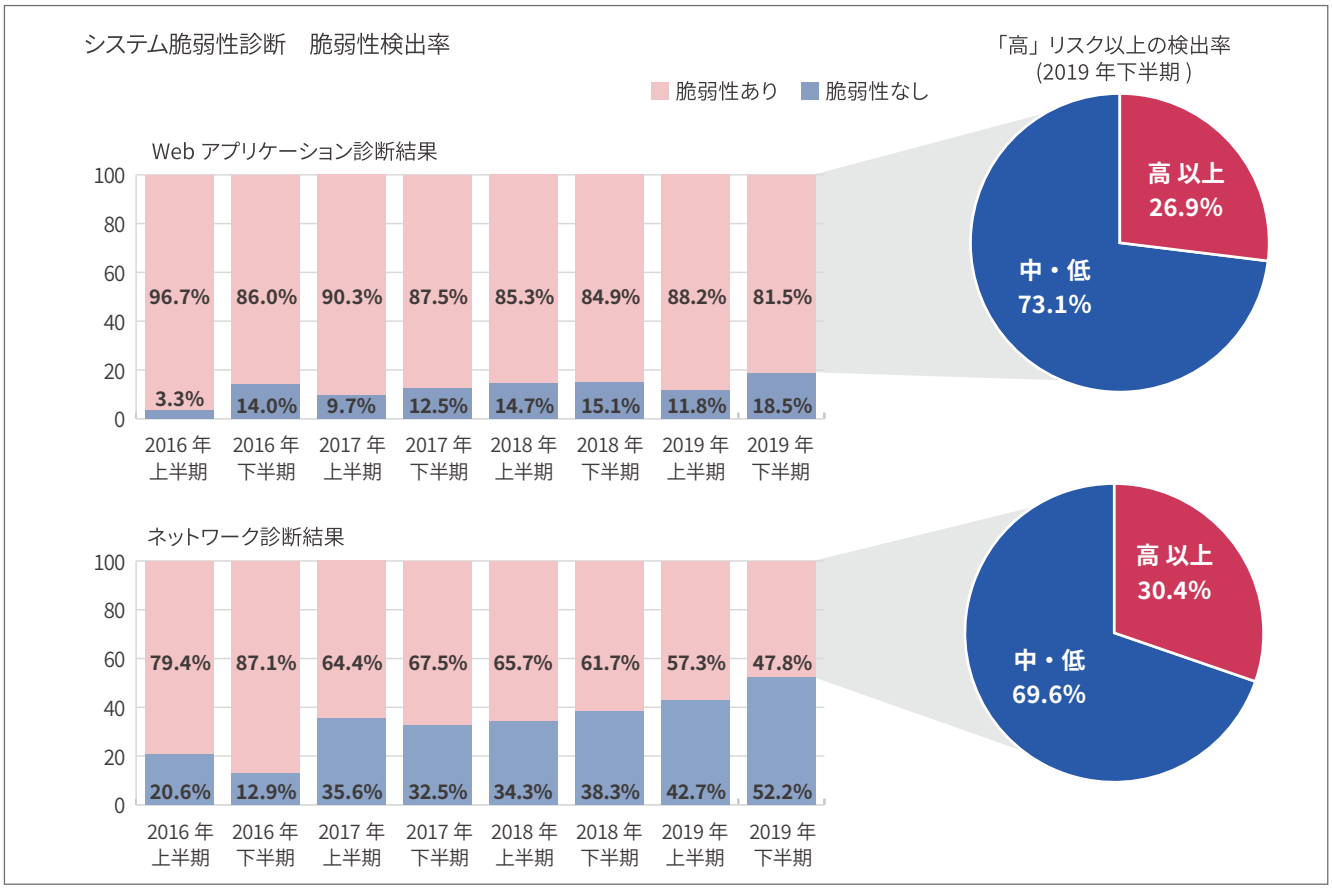
本誌 19 ～ 20 ページで、「2019 年下半期カテゴリ別脆弱性検出状況」とし、当社診断で検出された脆弱性を各性質に応じてカテゴライズし、評価・分析をした結果をまとめた。以降、診断カテゴリごとに検出数が多かったものの中から、特筆すべきことに焦点を当ててリスクや対策を述べる。

Web アプリケーション診断結果

※P.19 データ参照

Web カテゴリ結果の 31.4% を占める「システム情報・ポリシーに関する問題」のうち、最も検出数が多かったのは、「脆弱なバージョンの OS・アプリケーションの使用」である。脆弱なバージョンの OS、アプリケーションを使用している場合、既知の脆弱性の影響を受ける可能性がある。最新バージョンへのアップデートが望ましいが、システム環境における制約等の理由でバージョンアップができないのであれば、必要なセキュリティパッチがすべて適用されていることを確認すべきである。

次に Web カテゴリ結果の検出割合



が多かったのは、19.7% を占める「セッション管理に関する問題」。最も検出されたのは、「不適切なセッションタイムアウト」であった。ログインセッションのタイムアウト値が適切に設定されていないと、長時間操作を行わずアイドル状態のままでもセッションが維持されることから、セッションハイジャック等の攻撃が成功する確率が高まるほか、サービス運用妨害（DoS）攻撃につながる可能性もある。セッションタイムアウトは、Web アプリケーションのデフォルト設定として一般的に採用されている 30 分が望ましいが、ユーザビリティを考慮してタイムアウト値を長くする場合は、追加のリスク緩和策を講じることが推奨される。

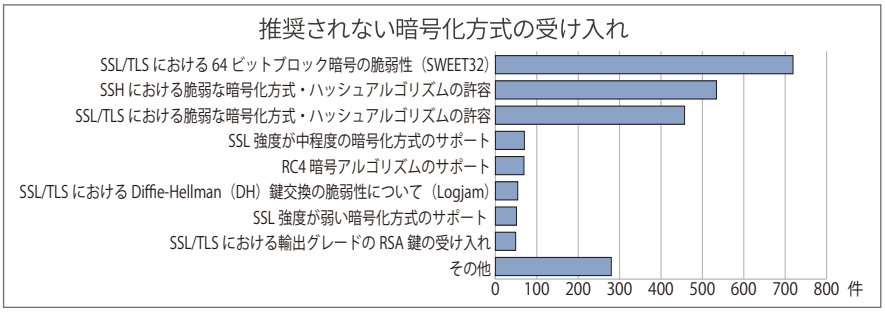
ネットワーク診断結果

※P.20 データ参照

NW カテゴリ結果の 52.3% が「通信の安全性に関する問題」であった。なかでも、「推奨されない暗号化方式の受け入れ」（検出割合は右表を参照）の検出数がトップであり、第 2 位の「推奨されない SSL/TLS 通信方式の使用」と比べて 2 倍以上の差がある。

サーバがブロック長 64 ビットのブロック暗号をサポートしている場合、誕生日攻撃（birthday attack）を介して長い期間暗号化されたセッションを復号・解読される「SWEET32」と呼ばれる攻撃の影響を受ける可能性がある。「NVD（National Vulnerability Database）」などに本脆弱性の影響を受ける製品は公表されており、ベンダからも正式な対策が公開されていて、ベンダ情報を参照のうえ対策することが望ましい。

SSL/TLS 通信において、強度の低い暗号化方式（RC4、3DES など）が許容されていると、既知の脆弱性を悪用した攻撃（平文回復攻撃など）により、攻撃者に暗号化されたデータが解読される危険性がある。また、強度が低いハッシュアルゴリズム（SHA-1 など）が許容されていると、衝突攻撃に弱くなり証明書の偽造等が可能となる恐れがある。鍵長が 128 ビット未満の暗号方式については、総当り（Brute-Force）攻撃への耐性が低く、中間者（Man-in-the-Middle）攻撃などの標的になりうる。強度の低い暗号化方式やハッシュアルゴリズムは使用を停止し、SSL/TLS による通信の保護には鍵長が 128 ビット以上の暗号化方式を実装するべきである。SSH プロトコルにおいても、攻撃者に暗号文を解読される恐れがあるため、脆弱な暗号化方式およびハッシュアルゴリズムを許容しないことが望まれる。



SQAT® Security Report 編集部が選ぶ 2020 年 5 大セキュリティ脅威

サイバーセキュリティにおける最大の懸念は「データ侵害」である。データ侵害とは、情報資産に対する偶発的または違法な破壊、滅失、変更、許可されていない開示やアクセスをもたらすセキュリティ脅威のことを指す。企業は自社のデータをこうした侵害から守るために様々なセキュリティ対策を講じているわけだが、益々複雑化、巧妙化するサイバー攻撃の被害が後を絶たない。常日頃からサイバー攻撃やセキュリティ脅威に関する情報を国内外から収集し、また世の中のトレンドや当社への相談・依頼内容と比較、分析した結果から当編集部が選んだ 2020 年における 5 大セキュリティ脅威は次のとおりである。

1. クラウドセキュリティ設定ミス

「クラウド・バイ・デフォルト」が定着しつつある中、設定ミスによるセキュリティ事故が相次いで発生している。クラウドセキュリティ事故の 99%は利用者側に責任があり、また設定ミス等、管理不備の問題を抱える企業や組織の 90%が機密情報漏洩の危険性と常に隣り合わせにいる[*1]。当社の設定診断サービスでも診断を実施したシステムほぼすべてに設定ミスが確認されている。クラウド利用が時代の潮流となっている今、機密情報を狙う攻撃はさらに活発化することだろう。

2. 標的型攻撃

2020 年 1 月に IPA から公開された「情報セキュリティ 10 大脅威 2020[*2]」でも、標的型攻撃による機密情報の窃取は組織に対する脅威の第一位に挙げられている。近年では APT〇〇（〇〇には数字が入る）と呼ばれる組織的なグループによる攻撃が頻発し、その影響や被害は大規模かつ広範囲に及ぶ。日本に対しても標的型攻撃は断続的に行われており、特に 2020 年は東京でオリンピック・パラリンピックが開催されることからも格好の攻撃ターゲットである。

3. マルウェア感染

2019 年 5 月以降、毎月約 2,500 万件のマルウェア出現が観測されている[*3]。新種も次々と作成され、マルウェア対策サービスベンダでは 1 日に登録する新種のマルウェアは 35 万件にも上るという[*4]。2019 年末に流行した「Emotet」などは記憶に新しいことだろう。Emotet は亜種も多数かつ絶えず出現するため、従来のマルウェア対策ソフトで検知できない事態も起こっている。日本でも増加傾向にあるビジネスメール詐欺やフィッシング攻撃等に用いられた事例も少なくない。

4. 攻撃ターゲットの拡大

5G（第 5 世代移動通信システム）の商用サービス開始に伴い、多数同時接続や高速大容量通信が実現可能となり、IoT 化の加速、働き方改革でのリモートワーク推進等により、守るモノや環境に変化が訪れるのは必至であろう。しかし、そうした変化にユーザ側のセキュリティ対策が遅れを取っているのが現状で、攻撃者にとっては 5G 利用が浸透すればするほど、“仕事場”や“取引先”が拡大していくのである。5G が普及することでデータの生成および処理量が莫大に増え、個人情報や機密情報が危険に晒される機会が増大する。

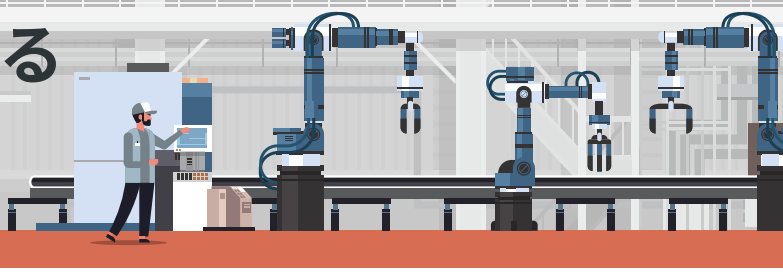
5. 内部不正

「この世で最も危険な脆弱性はヒトである」とは誰の言葉だったろうか。うっかりミスにより情報が漏洩した、設定ミスでシステムが停止した、などのニュースは残念ながら頻繁に目にする。さらに、攻撃ファクタが内部に存在し、明確な意図を持って行われる内部不正や攻撃は、企業にとって重大な懸念事項の一つである。これは大手企業やセキュリティベンダでさえ、例外ではない。内部犯行者は、外部の第三者に比べ、システムやフロー等に精通しており抜け穴を知り尽くしている可能性は高く、攻撃が企業に与えるダメージは甚大となりがちだ。

最後に、選出外ではあるが、サイバーセキュリティの大きな脅威としてセキュリティ人材の不足を挙げたい。最新の調査[*5]によると世界規模で 400 万人のセキュリティ人材が不足しているという。特に、アジア太平洋地域は深刻な状態で全体の 64%となる 260 万人の不足だ。技術の進化に応じて求められるセキュリティスキルが多様化しているのも一つの要因である。サイバー攻撃は待ってくれず、また多勢に無勢の戦況ではあるが、若い世代の積極的な参画に大いに期待したい。

*1 Gartner 社「Is the Cloud Secure?」：https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/
*2 IPA「情報セキュリティ 10 大脅威 2020」：https://www.ipa.go.jp/security/vuln/10threats2020.html
*3 Reason LABS Reason Cyber Stats & Insights：https://labs.reasonsecurity.com/insights
*4 AV-TEST Malware Statistics：https://www.av-test.org/en/statistics/malware/
*5 (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2019：
https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

産業制御システムセキュリティの いまとこれからを考える



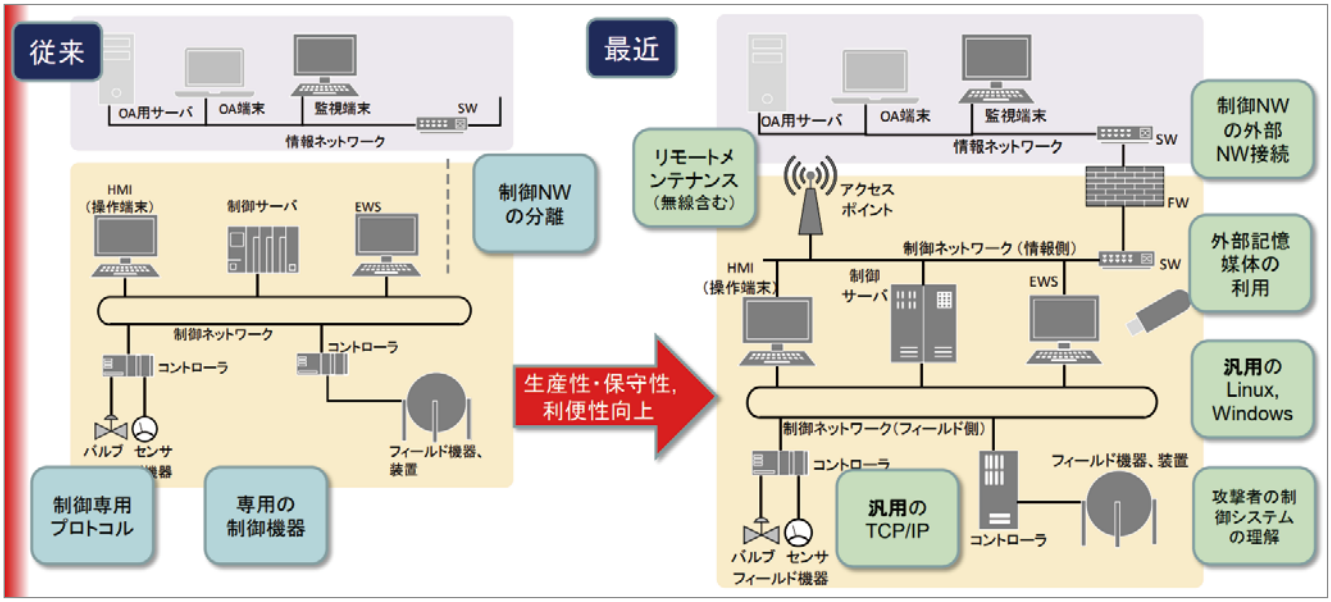
今やIoTシステムや制御系システムのセキュリティの問題は、経済的な損害だけでなく、社会的信用の失墜につながりうるものとの認識が一般的になりつつあります。特に、2020年はオリンピック・パラリンピックという国際的な大型イベントを控えており、大規模なサイバー攻撃が予想されます。こうしたイベント時に狙われる制御システムは、電気・ガス・水道や空港設備といったインフラ施設、石油化学プラントなどの制御システムなどがあげられます。

平成三十年４月にはサイバーセキュリティ戦略本部から「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」が公表されたものの、「サイバーセキュリティに係る保安規程・技術基準等」については未整備の業界も多く、省令の改正や国としてのガイドライン等の策定が急ピッチで進められています。こうした中、「IoTシステムや制御システムのセキュリティ」は、事業継続計画（BCP）において想定すべき主要なリスクの一つであり、経営責任が問われる課題として捉える必要があります。

産業制御システムのセキュリティとは？ その現状

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考えられてきましたが、近年状況が変化してきています。一般的に、OT（Operational Technology）のライフサイクルは10～20年と、ITに比べ長く、さらにシステムが停止することなく稼働し続けること（可用性）が最も重視されるため、装置自体の脆弱性が発見されたとしてもすぐに交換できません。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、ファームウェアやエンベデッドOS（産業用機械などに内蔵されるコンピュータシステムを制御するためのOS）のアップデートにUSBを使用するケースも少なくありません。しかし検疫体制が甘く、そこから感染してしまったという事例もあります。

図１　制御システムの進化とセキュリティ



（出典：IPA「情報システムのようにはいかない制御システムのセキュリティ」https://www.ipa.go.jp/files/000078215.pdf）

さらに最近、利便性を考え制御系システムでもエンベデッドOSとしてWindowsやLinuxを採用されることが増えてきましたが、それらの端末がインターネットに接続されていることから、標的型攻撃などの脅威にさらされる機会が増えるという皮肉な結果を生んでいます（図1参照）。

制御システムのセキュリティと一般的な企業の情報システムとは、その対象や優先度が大きく異なり、またセキュリティの基本であるCIA（機密性・完全性・可用性）の優先度も大きく違うため、単純にWebアプリケーションやネットワークのセキュリティ対策を当てはめるわけにはいきません。特に制御システムで優先されるリスク管理項目は「人命」「環境」であり、リアルタイム性も求められるのが大きな特徴です（表1参照）。

制御システムのインシデントでは2017年に起きたランサムウェア「WannaCry」が記憶に新しいでしょう。政府・病院・工場などのシステムに侵入し、コンピュータのストレージが暗号化されて身代金を要求された事件です。また、2019年にはランサムウェア「LockerGoga」により世界40ヶ国のコンピュータがサイバー攻撃を受け、ノルウェーのアルミ生産会社では、生産システムとオフィスITシステムが感染したため、手動生産に切り替えての操業を余儀なくされ、生産が大幅に減速されました。同じく、2019年の7月には南アフリカのヨハネスブルグで電力会社のプリペイド供給システムがサイバー攻撃により停止し、顧客が電力を購入できなくなる事態が発生しました。

産業制御システムのセキュリティフレームワーク

前述のように、OTはライフサイクルが長く、セキュリティよりも可用性が重視されるので、制御システムのアップデートもベンダが実施することが多いのですが、最新の脆弱性情報がOT担当者とIT担当者の間でスムーズに連携されず、結果として対策が不十分になっていることが散見されます。そもそも、IoTシステムや制御システムのセキュリティはフレームワークの違いもあり、専門家の知見によるリスクアセスメントが欠かせません。

汎用的な標準・基準として、ISMS（情報セキュリティマネジメントシステム）に対してCSMS（サイバーセキュリティマネジメントシステム）と呼ばれている制御システムセキュリティ基準IEC62443-2-1がありますが、当社では、近年のサイバー攻撃の動向や脅威を踏まえた上で、独自に開発したフレームワークを使用しています。IEC62443に加え、NIST（米国標準技術研究所）のセキュリティガイドラインであるNIST SP800-82および53、IPAのガイドラインなどをベースとしています。（図2、表2参照）

表1　産業制御システムと情報システムの違い

項目	産業制御システム	情報システム
セキュリティの対象	モノ（設備、製品）、サービス（連続稼働）	情報、データ
リスク管理	人命が優先、制御システムの停止、環境への影響も重視	データの機密性と保全が優先
セキュリティの優先順位	システムが継続して安全に稼働できることを重視 事業継続（BCP）に重きを置く	情報が適切に管理され、情報漏洩を防ぐことを重視 情報セキュリティに重きを置く
セキュリティのCIA	A（可用性）を重視、以下はI（完全性）、C（機密性）の順番	C（機密性）を重視、以下はI（完全性）、A（可用性）の順番
求められる可用性	24時間365日の連続運転、安定稼働（再起動は許容されない）	再起動と遅延は許容範囲
求められる耐障害性	冗長システム構成をとるが、冗長システム構成を取れないケースも多い	一般的にはシステムの二重化など冗長システム構成をとる
求められる性能要件	リアルタイム性能の要求は高い	リアルタイム性能の要求はそれほど高くない 処理能力は要求されることが多い
システム運用	専用のリアルタイムOSを使用するケースが多い 汎用のOSを使用する装置、機器も増えてきている	汎用的なOSを使用し、OSの更新、パッチ適用は容易
通信プロトコル	専用独自プロトコルと標準通信プロトコル（TCP/IP）	標準通信プロトコル（TCP/IP）
パッチ適用	計画停止ができず、パッチを適用しないケースが多い	定期的に計画的にパッチ適用を実施
技術のサポート期間	システムのライフサイクルも踏まえて、10～20年	システムのライフサイクルも踏まえて、3～5年
運用管理	現場技術部門、遠距離/無人の場所も多く遠隔監視が多い	情報システム部門、一般的にIDC等に設置し、アクセスが容易

図 2　産業制御システムのセキュリティフレームワーク

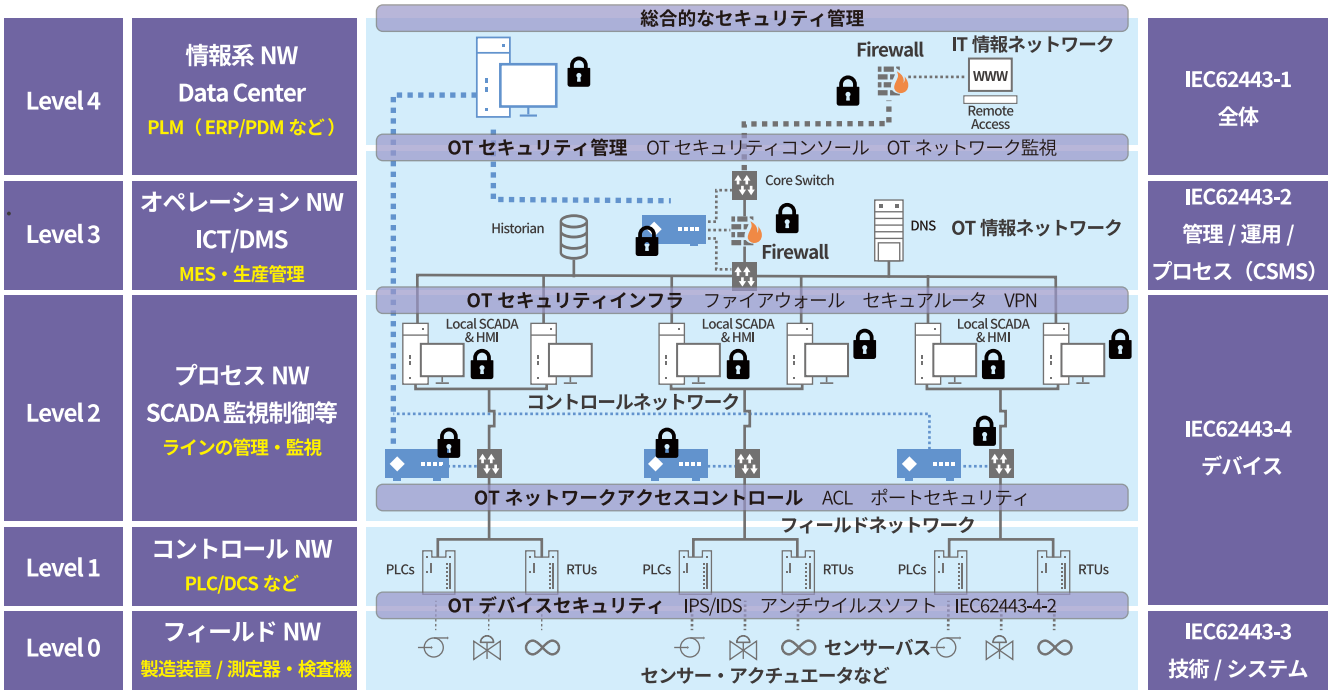


表 2　BBSec の産業制御システム向けリスク評価項目例

		区分	特徴
BBSecの制御システム向けリスク評価項目構成	ベースガイドライン	NIST Cybersecurity Framework v1.1 (2018/4)	現在効果が認められている基準、ガイドライン、プラクティスを集約することで、複数のアプローチを体系化する共通の構造を示している。重要インフラ分野のみならず、他の業界においても国際協力のもとで活用できる。
	セキュリティ管理策	NIST SP800-53 r.4 (2017.1)	連邦政府情報システム及び連邦組織のためのセキュリティ管理策。セキュリティマネジメント、リスクマネジメント、セキュリティ技術、セキュリティの対策状況を評価する指標、セキュリティ教育、インシデント対応など、セキュリティに関し、幅広く網羅している。
	ICS補足ガイダンス	NIST SP800-82 r.2 (2015/5)	2015 年 5 月に NIST により発効された。アメリカ政府機関に産業用制御システム（ICS）を納入する際に、納入業者が守るべきセキュリティポリシーを示した文書。
	参考セキュリティ要件	PCI-DSS v3.2.1 (2018/5)	クレジット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、クレジットカード業界の情報セキュリティ基準。
		CIS Critical Security Controls v7.0 (2018/3)	米国国家安全保障局（NSA）等の米国の公的機関や情報セキュリティ専門企業等が共同で研究し、米国のセキュリティ専門団体である SANS Institute が取りまとめた CSC（Critical Security Controls）をルーツとしている。

事業継続のためにできること

冒頭にあげた「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針(第 5 版)」において、定期的な情報セキュリティリスクアセスメントの実施、サイバー攻撃の特性を踏まえた対応計画の策定などが求められています。

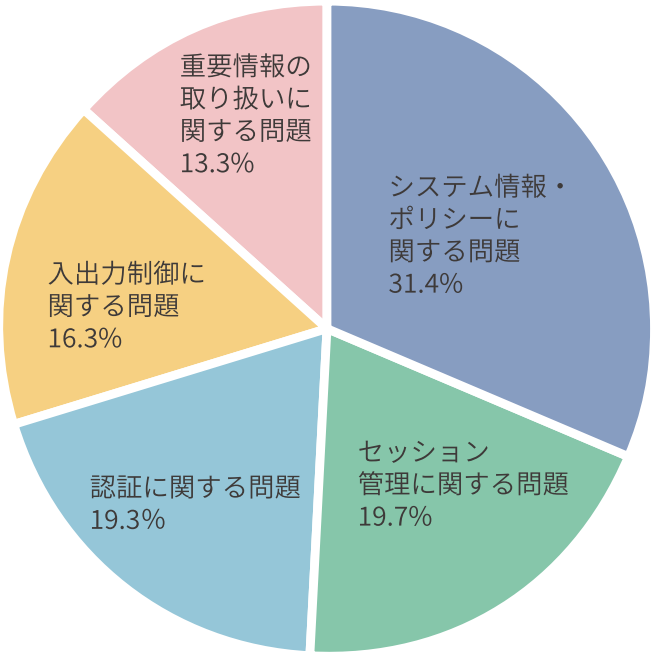
これらの重要インフラのシステムには先にみたように、一般的な情報システムのセキュリティ対策では対応できない部分も多くあります。まずはセキュリティリスクを可視化し、脆弱性があることを認識することが重要です。その上で脅威を最小化する方策を検討する必要があります。

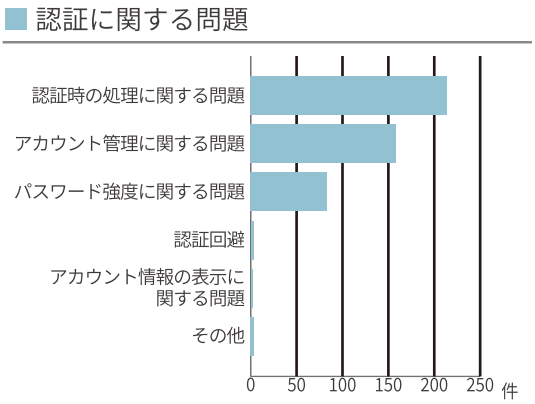
可用性と人命・環境への配慮という 2 つの命題を実現するためにも、OT 担当者と IT担当者が連携し、セキュリティの専門家を交えてセキュリティ体制を構築・運用していくことが欠かせません。当社では制御システムのリスクアセスメントをはじめ、CSIRT 構築、セキュリティオペレーションセンターによる監視、ケースによってはセンターからのオペレーションで防御するところまでお手伝いしています。対策についても一般的なセキュリティ対策の提案だけでなく、装置の交換やエンベデッド OSのバージョンアップが難しい場合のリスク低減策もご提案いたします。

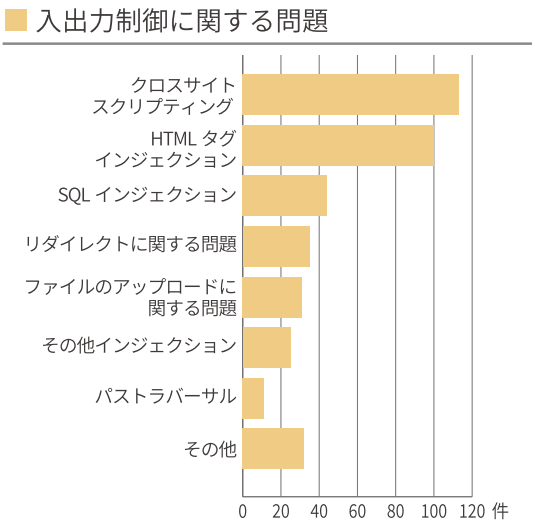
制御システムセキュリティのリスクアセスメントは、情報セキュリティ対策の第一歩である現状把握を行い、現状を踏まえた上で、セキュリティリスクに対する今後の対策を考えるためのファーストステップです。セキュリティ専門家の知見でこそできることがあります。事業継続のためにもまずはリスクアセスメントからはじめてはいかがでしょうか。

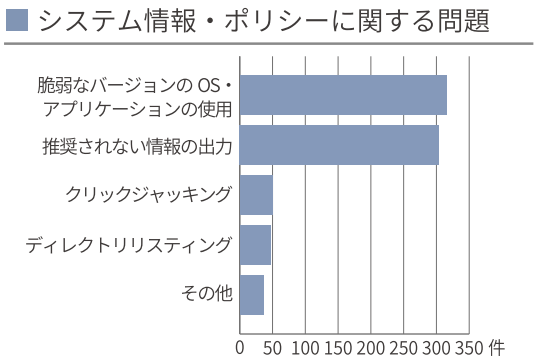
2019 年下半期 カテゴリ別脆弱性検出状況

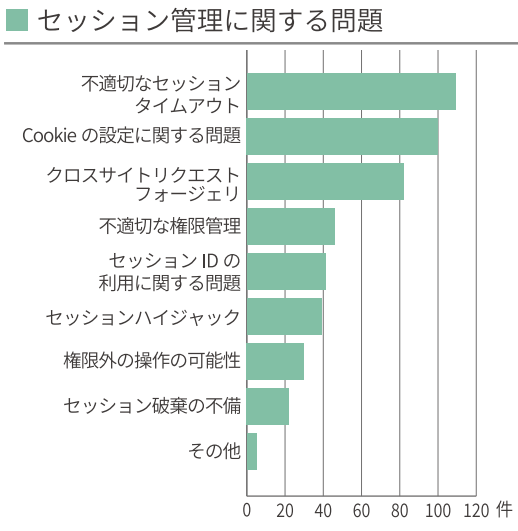
Web アプリケーション診断結果

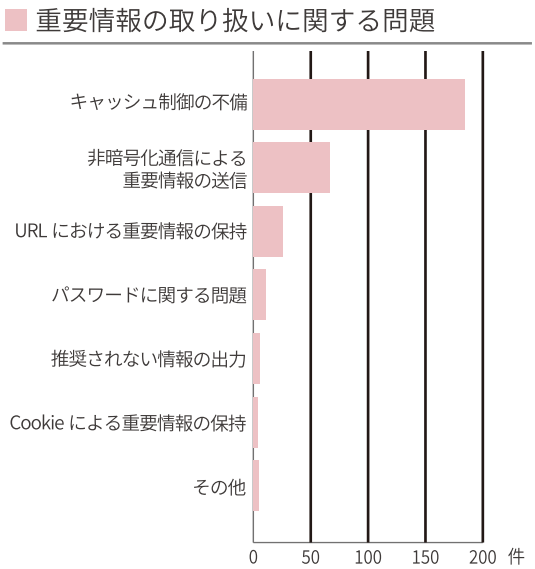




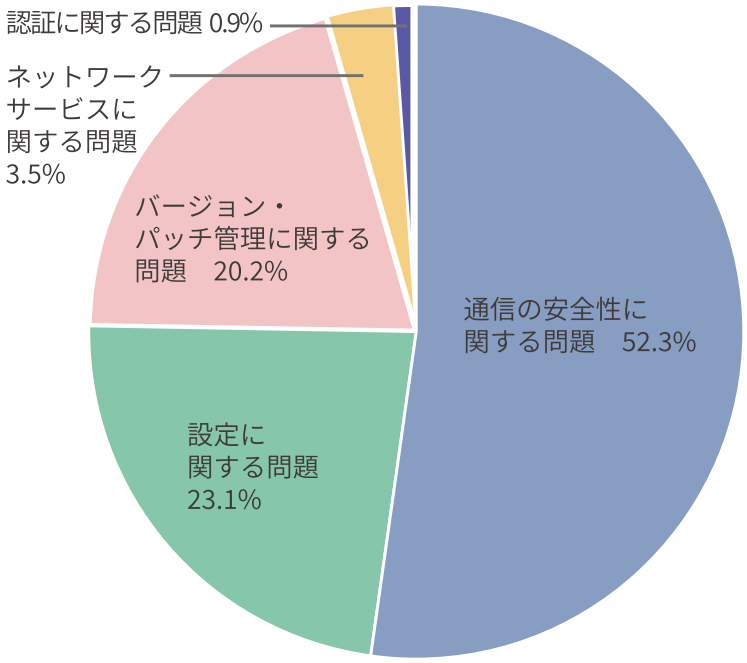


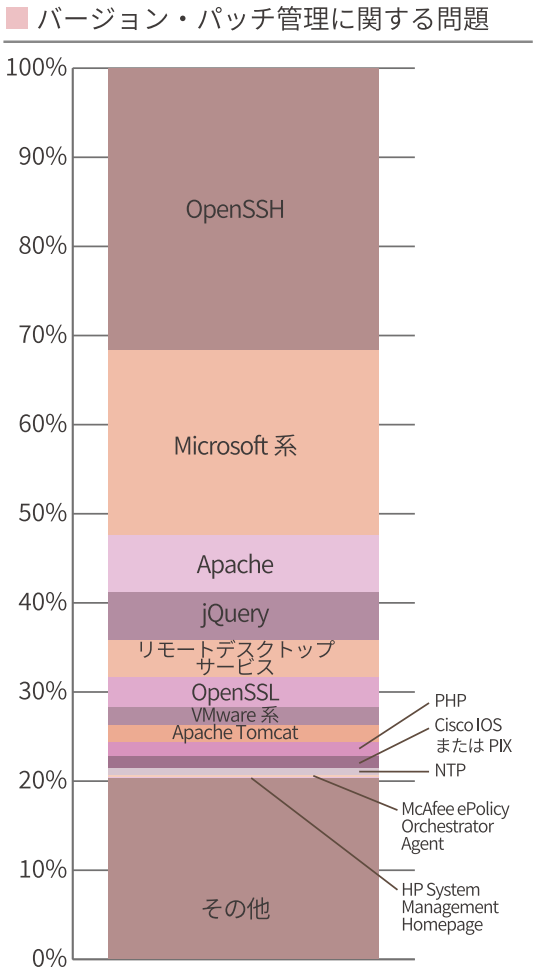




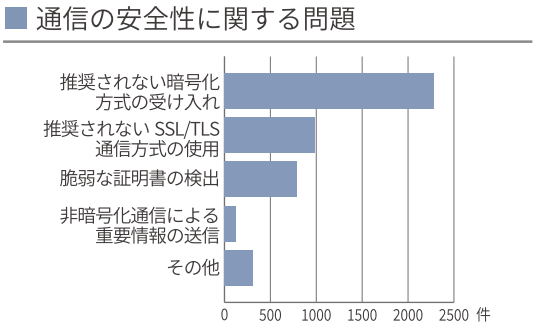


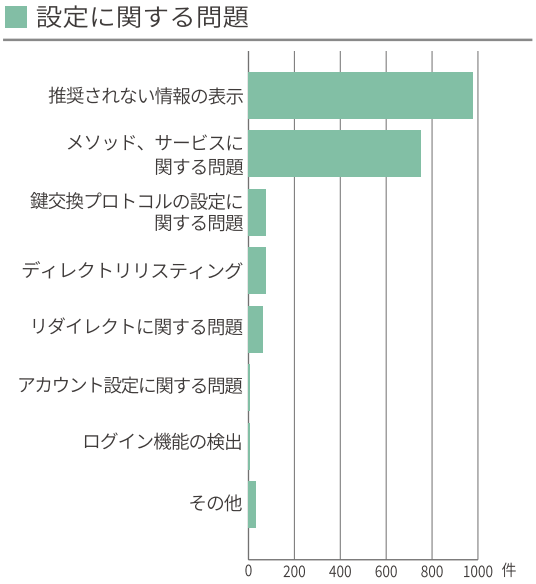
ネットワーク診断結果

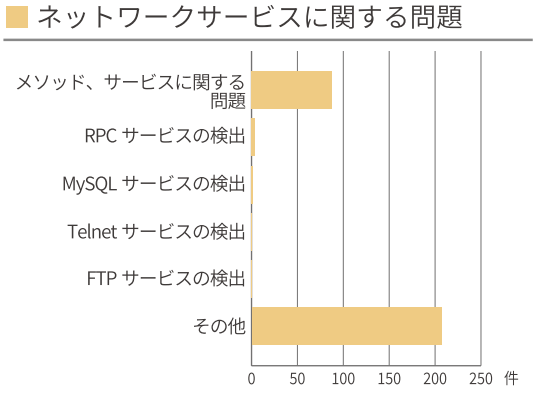




脆弱性が存在するバージョンの OS・アプリケーション・サービスの検出割合







業界別診断結果レーダーチャート

2019 年下半期 Web アプリケーション診断

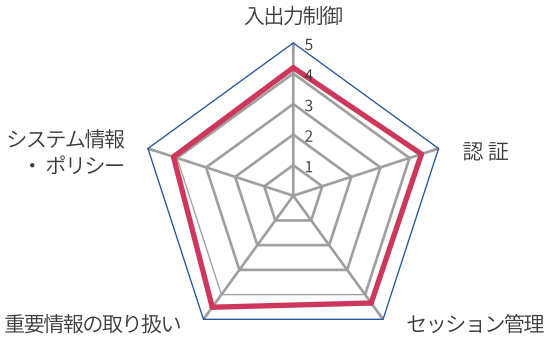
診断対象を業界別に分類し、当社報告書内で使用している、入出力制御、認証、セッション管理、重要情報の取り扱い、システム情報・ポリシーといったカテゴリごとに、検出された脆弱性をリスクの重大性で評価してレーダーチャート化した。レーダーチャートの算出方法は、集計期間に検出された脆弱性の平均値から、システムごとに判定した結果の平均値である。今回は、オリンピック・パラリンピックを目前に控え、新しい試みを続ける観光・宿泊・運輸（航空・旅客）業などの「ホスピタリティ」業界をピックアップし、分析した。

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

Web アプリケーション診断実績（業界別割合）

業界	割合
情報通信業	37.9%
金融業，保険業	19.9%
生活関連サービス業，娯楽業	15.0%
製造業	8.9%
サービス業（他に分類されないもの）	4.6%
電気・ガス・熱供給・水道業	4.0%
教育，学習支援業	2.5%
学術研究，専門・技術サービス業	1.9%
卸売業，小売業	1.6%
医療，福祉	1.2%
公務（他に分類されるものを除く）	1.1%
運輸業，郵便業	0.5%
建設業	0.5%
不動産業，物品賃貸業	0.4%

レーダーチャートの見方



5 つのカテゴリ別に、リスクの重大性によって、「緊急：1」「重大：2」「高：3」「中・低：4」とレベル分けし、それ以外を「情報：5」として、各段階に応じた数値を定め平均点化したものを赤線で示す。数値が高いほど安全度が高く、数値が低いほど緊急の対応が必要となる。なお、レーダーチャートの中心点は、その項目が診断対象外であることを示す。

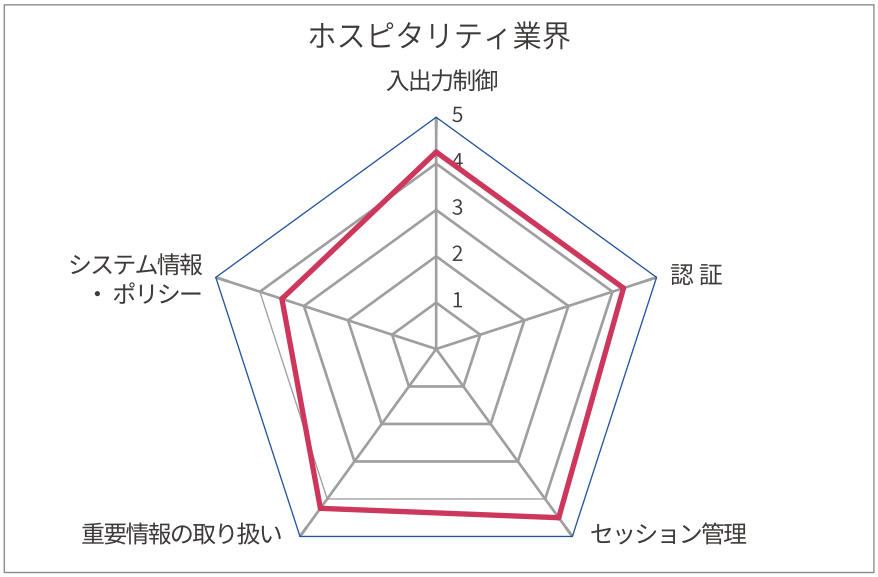
●業界分類方法●
「日本標準産業分類」（総務省）の「大分類」をもとに当社にて選定

ホスピタリティ業界

ホスピタリティ業界（観光・宿泊・運輸）分野のシステム脆弱性診断の平均値は図 1 のとおり。システム情報・ポリシーにおいてやや数値が低いものの、平均して大きな問題が検出されたシステムは少ない。

しかし注意を喚起したいのが、このレーダーチャートがあくまでも「平均」であることだ。殆どのシステムは平均値を上回る、あるいはほぼ平均値に近い値であったものの、大きく平均を下回るシステムも存在した。特に入出力制御とセッション管理においてその傾向が顕著であった。なお、システム情報・ポリシー

図 1　検出された脆弱性の平均値



は総じて平均に近い値であった。オリンピック・パラリンピックに向けて活況な業界の現状と課題について考えていく。

◆電子商取引（BtoC-EC）の活況と課題

2019 年 5 月に経済産業省が公表した「平成 30 年度 我が国におけるデータ駆動型社会に係る基盤整備」によれば、日本のBtoC-ECのサービス系分野において、最も市場規模が大きいのが旅行サービスである。2018年のBtoC-ECの市場規模は3兆7,186 億円にのぼり、全体の約56%を占める。ここでいう「旅行サービス」とは、旅行代理店への申し込み、航空機利用（国内便・国際便）、鉄道（新幹線・その他在来線）、バス利用、ホテル・旅館の宿泊費に関して、消費者の国内外を問わず日本の事業者に支払いが発生する市場を指す（ビジネスで利用する「出張」は除外）。牽引するのはインターネット専業の旅行代理店（通称：OTA：Online Travel Agency）で、国内のサイトをはじめ、エクスペディアやBooking.com といった外資系 OTA も目立っている。特にインバウンドにおいては外資系 OTA 抜きでは成り立たないといっても過言ではない。

旅行サービス業において BtoC-EC は、航空券やホテル予約における空席や空室といった「在庫」管理に直結している。例えば、客室数という確定サービス枠が存在し、空室を「在庫」として顧客に提示しインターネットを介して予約を受け付け、自動で在庫管理を行う形態は、「在庫数」が明確に定義できるサービスにとって非常に親和性の高い形態である。

しかし、市場が成長を続ける一方でセキュリティの甘さも課題として浮かんできた。

2018 年にセキュリティ企業の Trustwave が犯罪被害にあった世界 19 カ国の企業・団体など数千社を対象に行った調査結果では、宿泊業・旅行業を含む「ホスピタリティ産業」は、小売、金融に次いで 3 番目に被害が多く、全体の 10% を占めた。特にクレジットカード払いができるシステムが狙われている。またセキュリティ企業の Dashlane が 2018 年に実施した調査では、旅行関連サイト55社の89%でパスワードポリシーや認証機構に問題があったとの結果が報告されている。さらにシマンテックの研究者による調査では、54 カ国約 1,500 のホテルにおける 67%もの予約サイトがサードパーティサイトに予約参照コードを意図せず漏らしているリスクを内包しているという報告がなされている。同調査では、ホテルサイトの 4 分の 1 以上（29%）が、顧客への予約受領のメールに記載している予約管理システムへのリンクを暗号化していないとも述べている。実店舗を狙ったサイバー攻撃は減少傾向にあるものの、電子商取引ではむしろ増加傾向にあるといえるだろう。

OTA に関しては観光庁が 2015 年に「オンライン旅行取引の表示等に関するガイドライン」を策定し、旅行業のオンライン取引で表示すべき内容やその表示方法について細かく規定した。しかしセキュリティ対策については触れられておらず、各企業・団体によって対策状況はまちまちであった。2016 年、大手旅行会社・中堅運輸会社において情報流出事件が発生したのを受け、「観光庁・旅行業界情報共有会議」が発足された。「中間とりまとめ」において旅行業情報セキュリティ向上のため早急に講ずべき対策が提言され、2018 年には「旅行業者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」策定の予算が支出されたものの、2020年1月の段階では、公表されていなかった。ただし、社団法人日本旅行業協会／社団法人全国旅行業協会が 2014 年に「旅行のウェブ取引に関するガイドライン（改訂版）」を出しており、事実上これがスタンダードになっているともいえる。

一方、国土交通省ではサイバーセキュリティ戦略本部の「重要インフラ分野における情報セキュリティ確保に係る安全基準等策定指針」に依拠する形で、航空・物流・鉄道・空港の各分野に対し、個別に「情報セキュリティ確保に係る安全ガイドライン」を策定している。また、鉄道、バス・バスターミナル、タクシー、宿泊施設の各業種に対しては個別の「情報セキュリティ対策のチェックリスト」を公開して対策を促している。

2015年

オンライン旅行取引の表示等に関するガイドライン（OTA ガイドライン）

観光庁

2008年

インターネットを利用した旅行取引に関するガイドライン（2019 年改訂）

社団法人日本旅行業協会／社団法人全国旅行業協会

◆インバウンドサービスの動向

ホスピタリティ業界において今年開催のオリンピック・パラリンピックを目前に脚光を浴びているのが、訪日外国人観光客を対象とするインバウンドサービスである。日本が「観光立国」を打ち出したのは今から 17 年ほど以前に遡る。小泉首相（当時）による「観光立国懇談会」が平成 15 年（2003 年）に発足し、2006 年には「観光立国推進基本法」が成立した。2015 年以降、国際貿易収支上、観光業は「輸出産業」となっている。また、2019 年の世界経済フォーラムの観光競争力レポートで

は第4位と、2017 年より2 回連続で上位にランクインしている。日本の評価を押し上げた項目としては「安全・安 心」、「保 険・衛 生」、「ICT の普及」がある。

世界観光機関（UNWTO）によれば、今後のインバウンドサービスのカギとなるのはデジタル技術、特にバーチャル・アシスタントとリアルタイムデスティネーションであるとしている。国土交通省では令和元年度の施策として、主要観光地の多言語対応、全国 3 万カ所の主要観光地・防災拠点で無料 Wi-Fi 整備を進めるとともに、「キャッシュレス・消費者還元事業」として中小・小規模事業者のキャッシュレス決済の普及に力を注いでいる。観光庁も、2018 年には「外国人観光旅客利便増進措置に関する基準」、「公共交通機関における外国人観光旅客利便増進措置ガイドライン」を策定した。同ガイドラインでは「インターネットによる予約環境の整備」として「インターネット上でクレジットカード等による決済も可能であることが望ましい」としている一方で、セキュリティに関しては、「公衆無線 LAN 等を整備するにあたっては、以下を参照されたい」として、「Wi-Fi 提供者向けセキュリティ対策の手引き」（平成 28 年総務省）、「公衆無線 LAN セキュリティ分科会報告書」（平成 30 年 3 月総務省）を挙げているのみである。

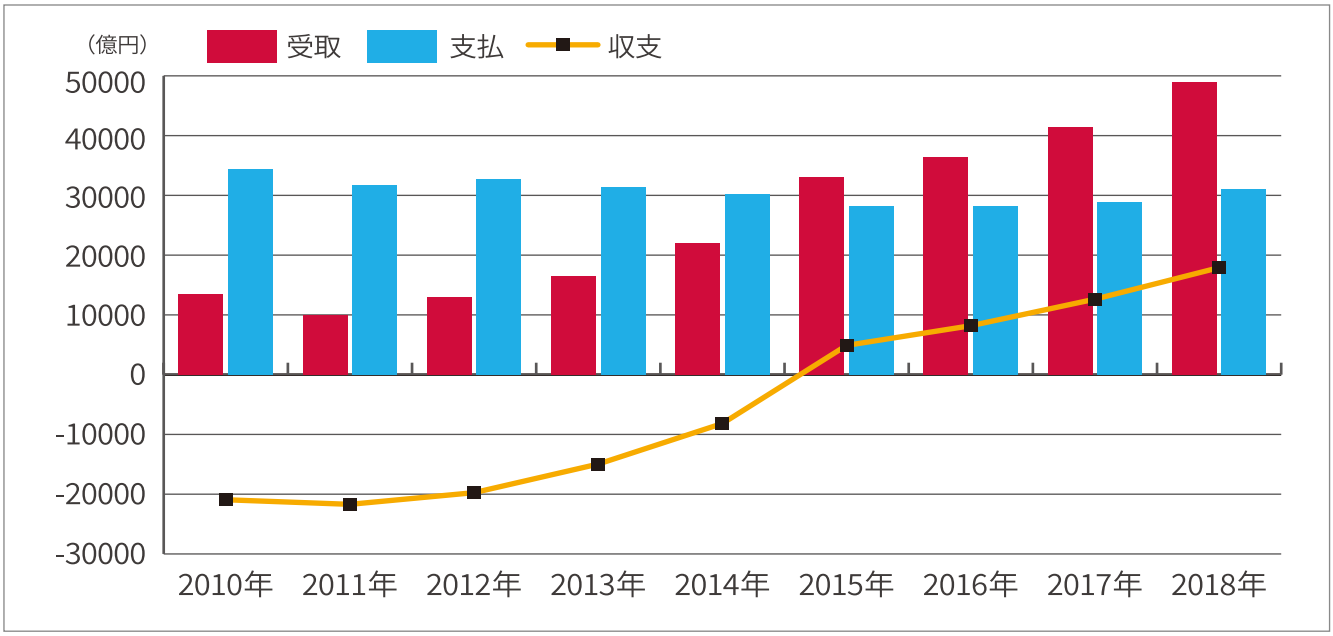
旅行者はパスポート、支払い情報、詳細な旅程など、データの宝庫を持ち歩く存在といえる。さらに旅行者は、旅行先では利便性を優先し、セキュリティ意識が通常より甘くなりがちであることから、攻撃者にとっては格好の「獲物」となりやすい。先の Trustwave のレポートによれば、調査対象のアメリカ人の 70% 以上が公共の Wi-Fi への接続や公共の USB ステーションでのデバイス充電、Wi-Fi への自動接続を有効化することで自分自身の情報をさらす行為をしていた。なお、個人旅行に比べビジネス旅行の方が、リスクの高い行動をとる人が多い。

◆新たな取り組み―VR/AR を活用した観光コンテンツ

こうした中、セキュリティ要件を組み込まないガイドラインを基に「VR/AR 等を活用した観光コンテンツ」が独り歩きしている現実もある。VR（Virtual Reality：仮想現実）が現実世界から得られる感覚情報を遮断して人工的に再現した感覚情報に置き換えるのと対照的に、AR（Augmented Reality：拡張現実）は現実空間を起点としデジタル情報を付加し、CG や動画を合成表示する。RPG を現実の空間と重ねるスマホゲームなどが AR の代表である。ARに固有のセキュリティやプライバシーを考慮する必要があると主張する研究者もいる。

2019 年にはサイバーセキュリティカンファレンス RECON において、VR のハッキングが紹介された。観光に関するVRコンテンツは観光庁・文化庁がそれぞれ個別にガイドラインを公表しているが、どちらもセキュリティ要件を含んでいない。また経済産業省の補助事業として、特定非営利活動法人映像産業振興機構（VIPO）が「VR 等のコンテンツ制作技術活用ガイドライン 2018」を公表しているが、やはりセキュリティについては触れられていない状況だ。データセキュリティのみならず、個人情報（位置情報）保護、プライベート空間権利（公的空間の境界）等の課題もある。これらに関して今春以降、矢継ぎ早にガイドラインが発行されることが予想されるが、現在設計・開発中の案件については、ガイドラインが発行されてからセ

図 2　国際観光収支の推移（観光庁資料より当社作成）　出典：https://www.mlit.go.jp/common/001186621.pdf



キュリティ要件を追加することになり、いびつな構造になってしまう。

まずは設計・開発の段階から「セキュリティ・バイ・デザイン」の思想を実践するとともに、ガイドラインに盛り込まれるであろう最低限のセキュリティ要件は予め組み込んでおくことが肝要だろう。どんな要件がガイドラインに組み込まれるか、あるいはガイドラインの最低基準以上の対策が必要なものは何かといった、専門家の知見が必要になる。これからインバウンド関連の事業を展開するのであれば、是非にも開発段階からのセキュリティ診断を実施することをお勧めする。

ガイドライン一覧

●観光・宿泊

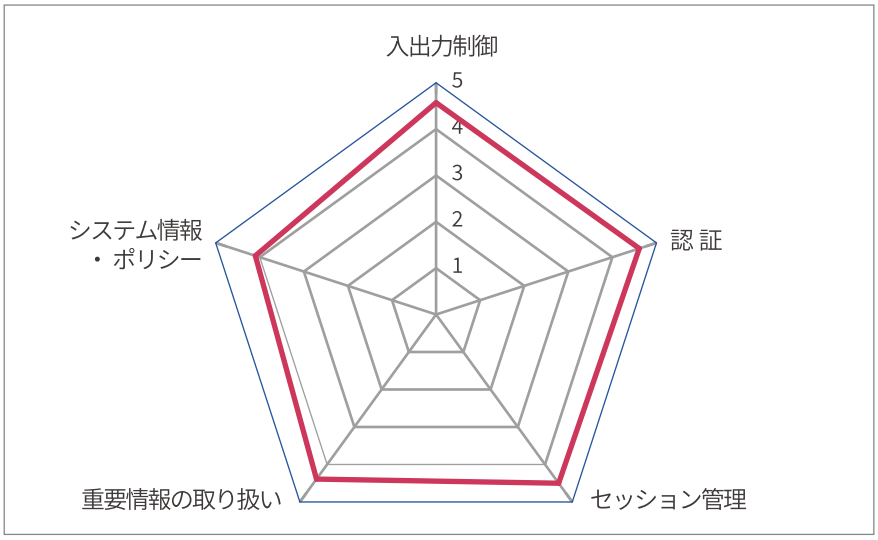
外国人観光旅客利便増進措置に関する基準	観光庁
公共交通機関における外国人観光旅客利便増進措置ガイドライン	観光庁
情報セキュリティ対策 チェックリスト（宿泊施設用）	国土交通省
ビルシステムにおける サイバー・フィジカル・セキュリティ対策ガイドライン	経済産業省

●インターネット・VR・AR 関係

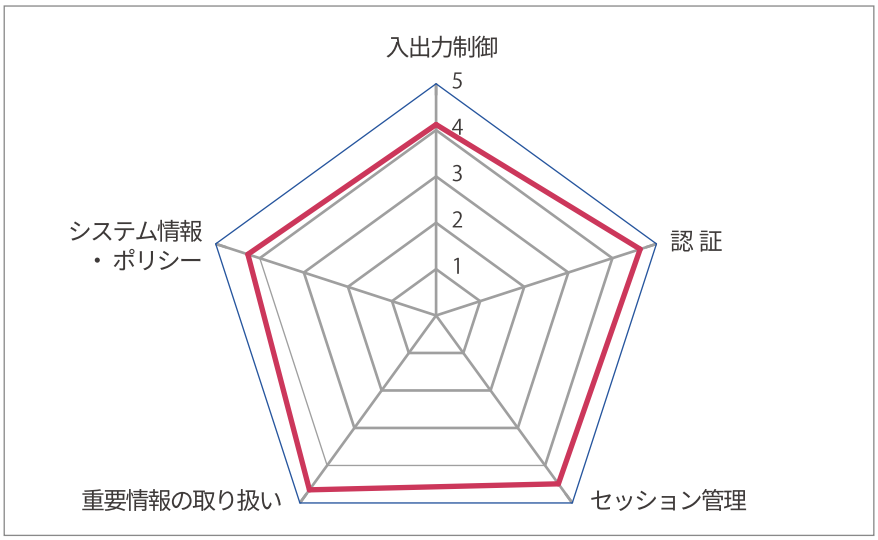
オンライン旅行取引の表示等に関するガイドライン（ＯＴＡガイドライン）	観光庁
インターネットを利用した 旅行取引に関するガイドライン	社団法人日本旅行業協会 社団法人全国旅行業協会
旅行のウェブ取引に関するガイドライン（改訂版）	社団法人日本旅行業協会 社団法人全国旅行業協会
Wi-Fi 提供者向け セキュリティ対策の手引き	総務省
スマートフォン決済セキュリティガイドライン	日本クレジットカード協会（JCCA）
スマートフォン決済の安全基準等に関する基本的な考え方	一般社団法人 日本クレジット協会
VR 等のコンテンツ制作技術活用ガイドライン 2018	特定非営利活動法人 映像産業振興機構
最先端 ICT（VR/AR 等）を活用した 観光コンテンツ活用に向けたナレッジ集	国土交通省 / 観光庁

その他の業種

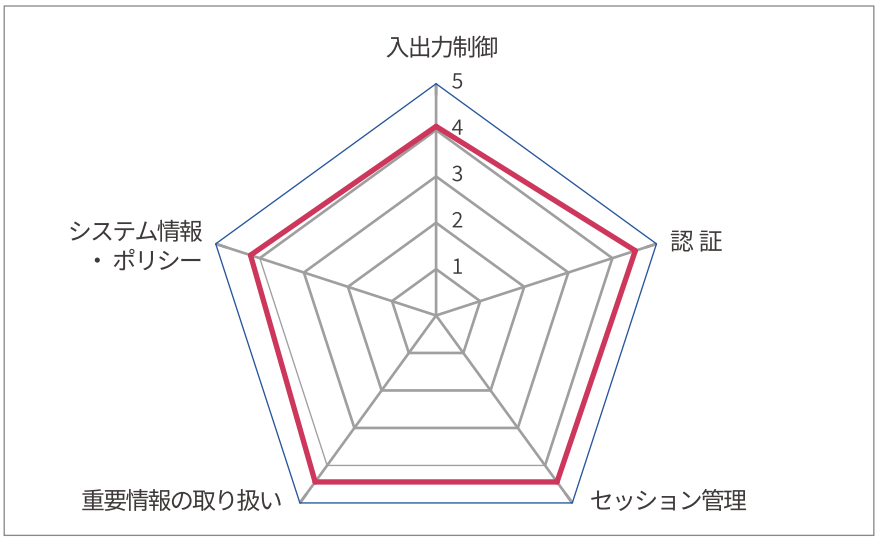
金融業・保険業



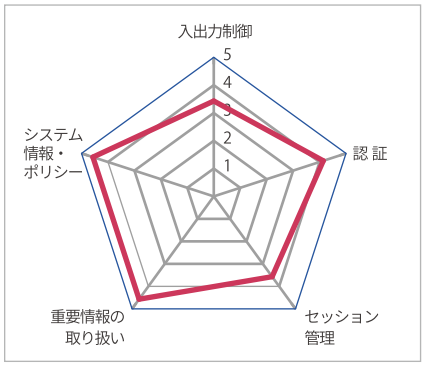
製造業



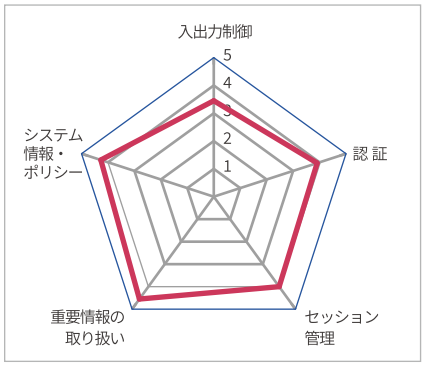
情報通信業



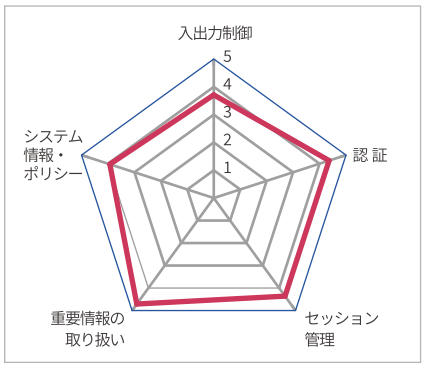
医療・福祉



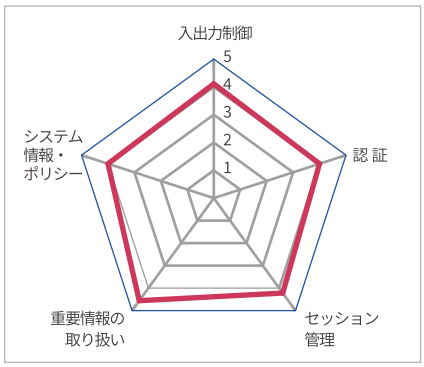
学術研究・専門 / 技術サービス業



教育・学習支援業

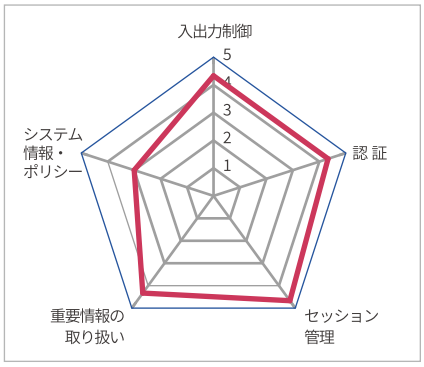


卸売業・小売業

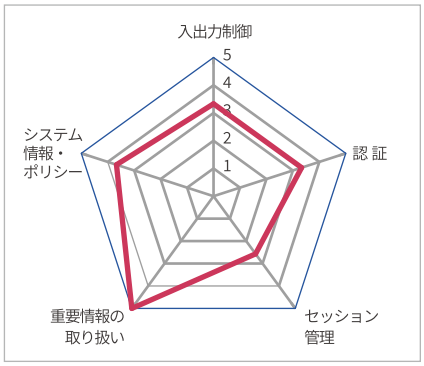


※ レーダーチャートの中心点は、その項目が対象外であることを示します。
なお、レーダーチャートの大小は年間診断の案件数によります。

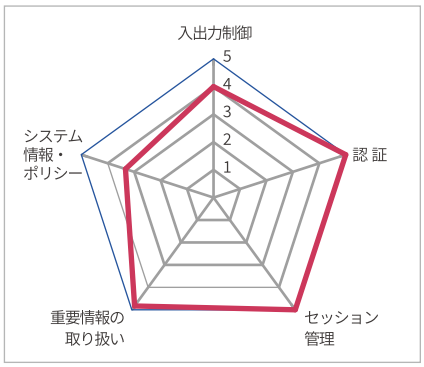
運輸業・郵便業



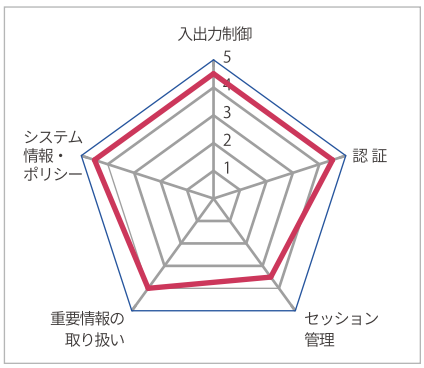
建設業



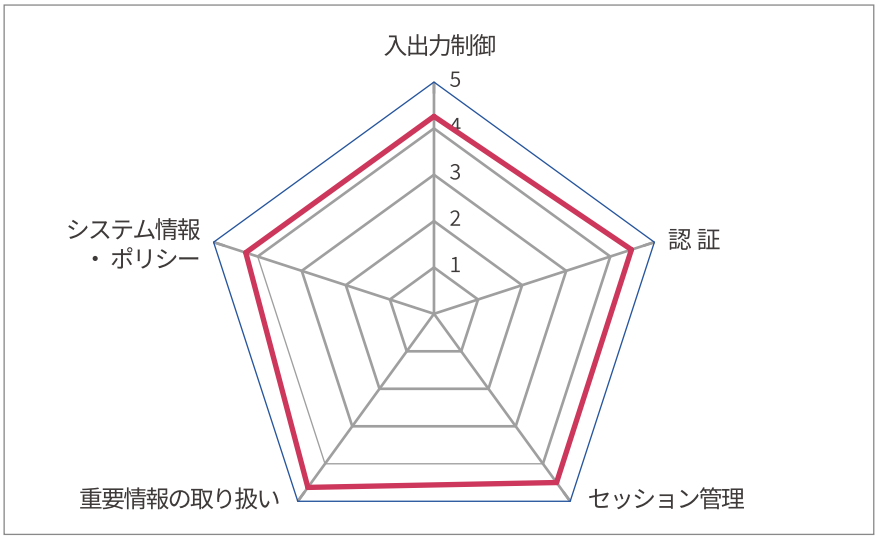
公務（他に分類されるものを除く）



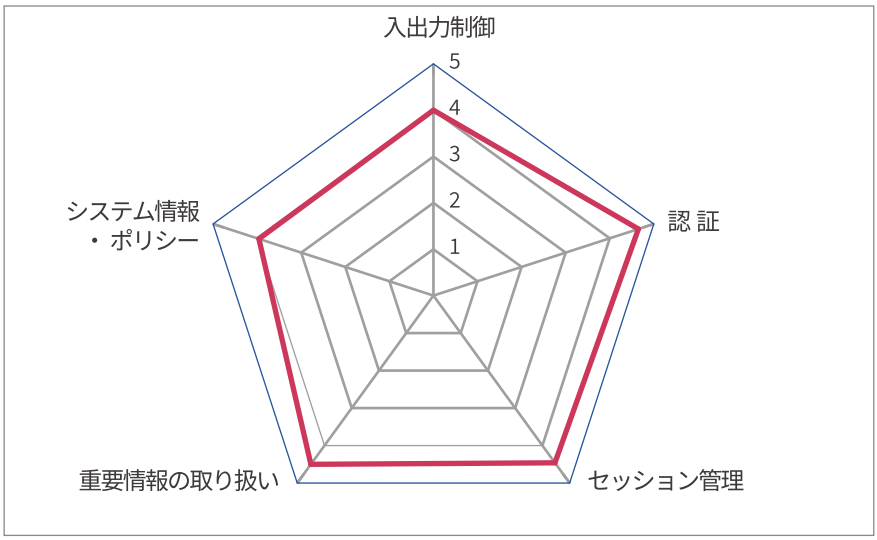
不動産業・物品賃貸業



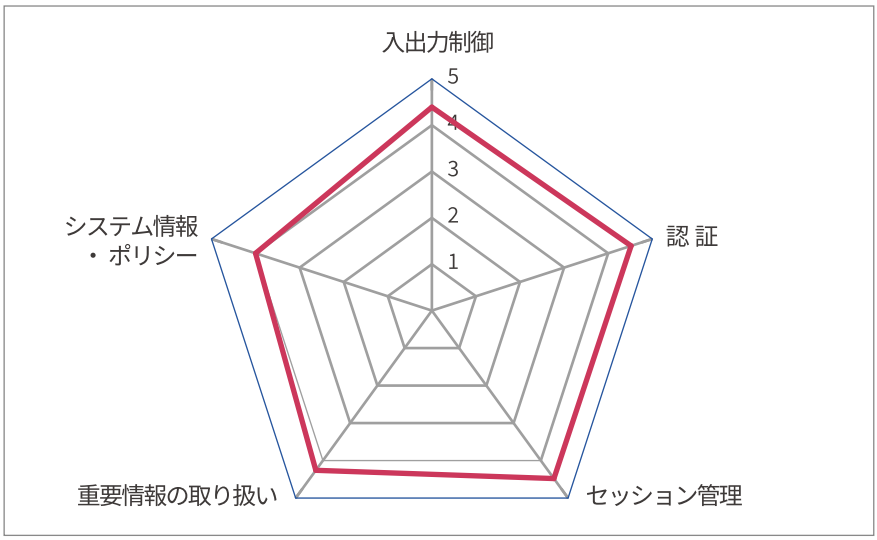
生活関連サービス業・娯楽業



サービス業（他に分類されないもの）



電気・ガス・熱供給・水道業



ブロードバンドセキュリティについて

株式会社ブロードバンドセキュリティ（BroadBand Security, Inc./BBSec）は、「企業の IT セキュリティ・ガーディアン（守役）として組織の健全経営に貢献する」というミッションを掲げ、2000 年の創業以来、様々なニーズに対応するセキュリティサービス事業を展開してまいりました。2004 年には、標的型攻撃に対応するクラウド型メールセキュリティサービスを国内で初めて提供（「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