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。

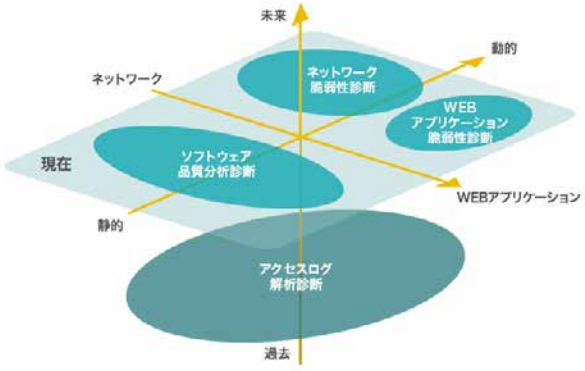
日本のカジノ運営についても、海外からの観光客増加に伴う経済の活性化・景気回復が期待されていますが、一方で懸念されていることもあり、サイバーセキュリティも懸念材料のひとつ。カジノ運営をしている国での情報漏洩などの事件も過去に何度も発生しています。サイバーセキュリティを強固なものにすることは、日本のカジノ運営においても必須といえるでしょう。今号では、日本のカジノ管理システムが守るべき法的要件と対応可能な設計に焦点を当てました。

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。