

**ワークショップ用-仮想企業設定**

CISO-PRACTSIE　CISOのための逆算式セキュリティ実践ワークショップ

JNSA　CISO支援ワーキンググループ

|  |  |
| --- | --- |
| ドキュメント名 | 概要 |
| 01 ワークショップ進行用資料  | 当ワークショップ進行用の資料 |
| **02 ワークショップ用-仮想企業設定など** | **仮想企業、JNSAアーキテクトに関する情報** |
| 03 セッション２関係者の見解 | シナリオに対する関係者の見解 |
| 20 アウトプット | ワークショップのアウトプット |

© 2023 JNSA CISO支援ワーキンググループ

目次

[（株）JNSAアーキテクト　基本情報 3](#_Toc132696015)

[Pd ドキュメント・プロファイリング 5](#_Toc132696016)

[Pd1規定類・手順のプロファイル 5](#_Toc132696017)

[Pd1-a 一般的な規定類 5](#_Toc132696018)

[Pd1-b① コミュニケーション方法 5](#_Toc132696019)

[Pd1-b② コンタクト先一覧 6](#_Toc132696020)

[Pd1-c 通報・連絡を受ける窓口 7](#_Toc132696021)

[Pd2 システム・セキュリティ対策のプロファイリング 8](#_Toc132696022)

[Pd2-a. 技術資料・情報資産管理台帳など 8](#_Toc132696023)

[Pd2-b システム一覧、Pd2-cアカウント **エラー! ブックマークが定義されていません。**](#_Toc132696024)

[Pd2-cアカウント 13](#_Toc132696025)

[P2-d　委託先など 13](#_Toc132696026)

[Pd2-e セキュリティ対策状況 13](#_Toc132696027)

[Pr リスク・プロファイリング: 17](#_Toc132696028)

[Pr1 事業視点のリスク・プロファイリング 17](#_Toc132696029)

[Pr2 システムレベルのリスク・プロファイリング 20](#_Toc132696030)

# （株）JNSAアーキテクト　基本情報

表 1　JNSAアーキテクト　会社概要（未上場）

|  |
| --- |
| 社名 株式会社JNSAアーキテクト設立 2000年4月13日本社所在地 〒105-0003　東京都港区西新橋資本金 3億円従業員数 270名平均年齢 42歳事業内容 PCオンラインゲームの開発及びサービスの提供モバイルゲームの開発及びサービスの提供役員（2022年4月1日時点）  代表取締役会長（CEO） 田仲 太郎 代表取締役CFO 下村 雅彦 取締役 中尾 浩二 髙橋 正和 Tom Klaus 社外取締役 本川 祐司 林　 芳子 （監査等委員） 水木 次郎 |

表 2 組織構成

|  |  |  |
| --- | --- | --- |
| 組織 | 責任者 | 主要なメンバー |
| 財務・経理 | 下村 CFO | 黒川Ｄ |
| 法務（知財、輸出入管理を含む） | 下村 CFO | 稲葉D |
| 人事 | 下村 CFO | 三宅M、桜井M |
| 総務 | 中尾 取締役 | 川内M、元持M |
| 広報 | 小屋 執行役員(EO) | 唐澤Ｍ |
| ゲーム事業部 | 佐々木 執行役員(EO) | 中村D、福沢M |
| システム開発部 | 藤井 開発本部長 | GanGan開発Ｇ（後藤Ｍ）SokoSoko開発Ｇ（金子M） |
| システム運用部 | 青島D | GanGan運用G（山口）SokoSoko運用G(前田) |
| 情シス | 矢野 CIO | 佐藤M、鈴木M |
| セキュリティ | 石田 CISO | 辻井D、駒瀬M |
| CSIRT | 石田 CISO | 平山、大和、吉田 |
| GanGan事業部 | 佐々木 執行役員(EO) | 井上D、野間D、平山M |
| SokoSoko事業部 | 高橋 事業部長（取締役） | 森山D、前川M |
| データ保護管理責任者 | 堀口DPO |  |

# Pd ドキュメント・プロファイリング

JNSAアーキテクトの規定類、台帳類は以下の通りです。

## Pd1規定類・手順のプロファイル

### Pd1-a 一般的な規定類

JNSAが公表している、「情報セキュリティポリシーサンプル改版（1.0版）」をセキュリティポリシーとして採用（表 3）

表 3　情報セキュリティポリシー

|  |  |
| --- | --- |
| 01\_情報セキュリティ基本方針01\_情報セキュリティ方針02\_人的管理規程 03\_外部委託先管理規程04\_文書管理規程05\_監査規程.06\_物理的管理規程07\_リスク管理規程 | 08\_セキュリティインシデント報告・対応規程　09\_システム変更管理規程10\_システム開発規程11\_システム管理規程12\_ネットワーク管理規程13\_システム利用規程14\_スマートデバイス利用規程15\_SNS利用規程 |

出典：JNSA　情報セキュリティポリシーサンプル改版（1.0版）[[1]](#footnote-2)

### Pd1-b① コミュニケーション方法

緊急時の対応については、情報セキュリティポリシー「08\_セキュリティインシデント報告・対応規程　４．２ 事象の検知、報告と分析」で、以下のように定義しています。

ワークショップでは、事務局が適切な演習の実行責任者（CISO等）を決め、実行責任者の指示に基づいて演習を進めるようにしてください。

08\_セキュリティインシデント報告・対応規程　４．２ 事象の検知、報告と分析

|  |
| --- |
| セキュリティインシデント、あるいは発生が疑われる事象を検知したものは、情報セキュリティ委員会に遅滞なく報告しなければならない。 情報セキュリティ委員会は、報告されたセキュリティインシデントに応じ、策定した対応手順に従い、被害の特定、原因の分析を行う。 なお、策定した対応手順に該当しないセキュリティインシデントの場合、情報セキュリティ委員会は、そのための実行責任者を任命し、対応組織を始動し、被害の特定、原因の分析を行う。 検知したセキュリティインシデント情報、原因の分析状況について、実行責任者のもと、一元的に収集、管理する。 |

### Pd1-b② コンタクト先一覧

JNSAアーキテクツの関係者とコンタクト方法は以下の通りです（表 4）。

表 4コンタクト先とコンタクト方法

|  |  |  |  |
| --- | --- | --- | --- |
| コンタクト先 | 氏名 | 連絡方法 | （窓口） |
| 経営者 | 田中CEO | メール：tanaka@jnsa-architect.comビジネスチャット:@tanaka電話:090-xxx-xxxx | 緊急の場合を除き電話はNGアポイントは、原則秘書の木村さん経由で |
| 情報セキュリティ委員会 | 正：石田CISO | メール:ishida@jnsa-architect.comビジネスチャット:@ishida電話:090-xxx-xxxx |  |
| 副：中尾取締役 | メール:nakao@jnsa-architect.comビジネスチャット:@nakao電話:090-xxx-xxxx |  |
| プライバシー責任者 | 石田CISO | 情報セキュリティ委員会を参照 |  |
| 経営陣 | 下村CFO | メール：shimomura@jnsa-architect.comビジネスチャット:N/A電話:090-xxx-xxxx | アポイントは、原則秘書の佐々木さん経由で |
| 中尾取締役 | 情報セキュリティ委員会を参照 |  |
| 高橋事業部長 | メール：takahashi@jnsa-architect.comビジネスチャット:@takahashi電話:090-xxx-xxxx | メール見落としが多いので、チャットを使うこと。急ぎの場合は電話。 |
| 広報 | 小屋執行役員 | メール: terakoya@jnsa-architect.comビジネスチャット:@koryakoya電話: 090-xxx-xxxx |  |
| 唐澤M | メール: karasawa@jnsa-architect.comビジネスチャット:@karasawa電話: 090-xxx-xxxx |  |
| 法務 | 稲葉D | メール: inaba@jnsa-architect.comビジネスチャット:@inaba電話: 090-xxx-xxxx |  |
| 社外取締役 | 本川林  | メール: motokawa@example.comビジネスチャット:@motokawa電話: 090-xxx-xxxxメール: inaba@examplecomビジネスチャット:@hayashi電話: 090-xxx-xxxx |  |
| 外部専門家 | JNSA緊急対応サービス | メール: jnsa-ers@jnsa.jnsa-architect.comビジネスチャット:N/A電話090-xxx-xxxx | 平日: 9:00-17:00上記以外は別料金 |
| 監督官庁 | 個人情報保護委員会経済産業省 | ホームページ　漏洩などの対応から報告<https://www.ppc.go.jp/personalinfo/legal/leakAction/>佐々木執行役員 |  |

### Pd1-c 通報・連絡を受ける窓口

外部の窓口

|  |  |  |
| --- | --- | --- |
| 窓口名 | 窓口：担当者 | 電話 |
| 一般的な窓口 | 代表・大代表 | 総務：川内M | 電話：03-xxx-xxxxinfo@ jnsa-architect.com |
| 顧客窓口 | 総務：元持M | 電話：03-xxx-xxxxinfo@ jnsa-architect.com |
| サポート窓口 | 運用G：前田 | support@ jnsa-architect.com |
| 広報窓口 | 広報：唐澤Ｍ | 電話：03-xxx-xxxxpr@ jnsa-architect.com |
| 採用窓口 | 人事：桜井M | 電話：03-xxx-xxxxhr@ jnsa-architect.com |
| セキュリティ関係の窓口 | CSIRT | CSIRT: 平山 | security@ jnsa-architect.com |
| セキュリティ窓口 | CSIRT: 平山 | security@ jnsa-architect.com |
| 個人情報関係の窓口 | プライバシー窓口 | 法務：稲葉D | privacy@ jnsa-architect.com |
| データ保護責任者 | 堀口DPO | dpo@ jnsa-architect.com |
| EU代理人 | 堀口DPO | xxxx@example.com |

社内の窓口

|  |  |  |
| --- | --- | --- |
| 顧客担当 | ゲーム事業部：福沢M | 電話：090-xxxx-xxxxfukuzawa@ jnsa-architect.com |
| ヘルプデスク | 情シス：佐藤M | 電話：080-xxxx-xxxxsatoh@ jnsa-architect.com |
| 情シス | 情シス：鈴木M | 電話：080-xxxx-xxxxsuzuki@ jnsa-architect.com |
| CSIRT | CSIRT：平山 | 電話：090-xxxx-xxxxhirayama@ jnsa-architect.com |

## Pd2 システム・セキュリティ対策のプロファイリング

P2システム・セキュリティ対策のプロファイリングで収取する情報を以下にまとめます。

### Pd2-a. 技術資料・情報資産管理台帳など

JNSAアーキテクトの主要な技術資料の状況を表 5に記載します。

表 5 技術資料

|  |  |  |
| --- | --- | --- |
| 一般的な名称 | ドキュメント名 | 保存場所・アクセス方法 |
| 情報資産管理台帳 | なし | N/A |
| ネットワーク構成図 | 図 1に記載表 6にセグメント間の通信設定を記載 | 共有ドライブ: SecurityCommitteecに保存 |
| IPアドレス一覧 | 表 7に記載  | 共有ドライブ: SecurityCommitteeに保存 |

JNSAアーキテクツのネットワーク構成は図 1の通りです。



図 1　ネットワーク・システム構成図

イントラネットは、サーバーセグメント、オフィスセグメント、評価セグメント、ゲストセグメントの４セグメントで構成しています。

サーバーセグメントとオフィスセグメントは相互に通信が行えますが、評価セグメント、ゲストセグメントは、他のセグメントとは通信ができません。また、ゲストセグメントは、セグメント内のデバイス間の通信は出来ません（表 6）。

表 6　セグメント間の通信

|  |  |
| --- | --- |
|   | Destination Segment |
| S.サーバー | O.オフィス | E.評価 | G.ゲスト | I. Internet | V. VPN |
| Source Segment | S.サーバー | 〇 | 〇 | × | × | 〇 | N/A |
| O.オフィス | 〇 | 〇 | × | × | 〇 | N/A |
| E.評価 | × | × | 〇 | × | 〇 | N/A |
| G.ゲスト | × | × | × | × | 〇 | N/A |
| I. Internet | × | × | × | × | 〇 | N/A |
| V.VPN | 〇 | 〇 | 〇 | × | 〇 | N/A |

表 7　IPアドレス一覧

|  |  |  |
| --- | --- | --- |
| IPアドレス | 資産名 | 備考 |
| xxx.0.0.242xxx.0.0.243 | Internet GW(Router)VPN装置 |  |
| yyy.0.3.241yyy..0.1.31 | Home Page：[www.jnsa](http://www.jnsa)-architect.exampleGanGan サーバー：gangan.jnsa-architect.com |  |
| 172.32.0.0/22172.32.0.1172.32.0.2172.32.0.3172.32.0.8172.32.0.11172.32.0.12172.32.0.13172.32.0.14 172.32.0.21172.32.0.22172.32.0.23172.32.0.24172.32.0.101 | 管理セグメント Firewall (LAN側) IPS  Network SW DHCP Network SW1(サーバーセグメント)Network SW 2(オフィスセグメント)Network SW 3(評価セグメント)Network SW4（ゲストセグメント）WiFiAP-1(サーバーセグメント)WiFiAP-2(オフィスセグメント)WiFiAP-3(評価セグメント)WiFiAP-4（ゲストセグメント）VPN装置（サーバー、オフィス、評価セグメント） |  |
| 172.32.4.0/22 172.32.4.1 172.32.4.5172.32.4.10-29 | サーバーセグメント Network SW ログ集約DBプロジェクトが管理するサーバー類（固定IP） |  |
| 172.32.8.0/22 172.32.8.1 172.32.8.10-254 172.32.9.11 | オフィスセグメント Network SW DHCP に割り当て 複合機 |  |
| 172.32.12.0/22172.32.12.10-254172.32.13.20-39 | 評価セグメント　DHCPに割り当て 社員が管理するサーバーやデバイス固定IP） |  |
| 172.32.16.0/22172.32.16.10-254 | ゲストセグメント DHCPに割り当て |  |

### Pd2-b システム一覧、Pd2-cアカウント

主要なシステムを以下にまとめます（表 8）。

表 8主要システム一覧

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| カテゴリ | システム名 | 実装 | オーナー、担当者 | アカウント |
| 基本的なITインフラ | 認証システム | Azure AD | CIO　矢島、情シス | 特権：矢島CIO、佐藤M |
| メールシステム | O365 | CIO　矢島、情シス | 特権：佐藤M、鈴木M社員：全員へ付与社外：業務委託先などについて以下で管理「社外利用者アカウント管理台帳」 |
| ファイルサーバー | SharePoint | CIO　矢島、情シス |
| カレンダー | O365 | CIO　矢島、情シス |
| ビジネスチャット | Slack | CIO　矢島、情シス |
| 公開システム | ホームページ | www | AWS+Word Press | 小屋 広報部長　広報グループ（唐澤Ｍ）技術サポート：情シス（佐藤、鈴木） | Corporate Webのアカウント構成に記載 |
| コンシューマ向けシステム | gangansokosoko | AWSAWS | 佐々木 執行役員青島D、GanGan運用G（山口）高橋取締役青島D、SokoSoko運用G(前田) | 特権：青島D、山口他のアカウント：Ganganシステム管理台帳で管理特権：青島Ｄ，前田他のアカウントは：Sokosokoシステム管理台帳で管理 |
| SNS公式アカウント |  | @jnsa-architeccht | 小屋 広報部長　広報グループ（唐澤Ｍ） | 特権：なし小屋広報部長、唐沢Ｍ |
| 求人関係 |  | ホームページに記載 | 人事 三宅M | 特権：三宅Ｍアカウント：三宅Ｍ、桜井Ｍ、人事メンバー |
| 電子契約システム | N/A | 法務 稲葉D | 特権なし：アカウント：稲葉Ｄ、法務メンバー |
| その他 |  |  |  |
| 非公開システム | ERP、決済システム | kintone | 財務 黒川D | 特権：黒川Ｄアカウント：財務メンバー |
| 給与明細、源泉徴収 | OJY会計システム | 財務 桜井D | 特権：桜井Ｍアカウント：三宅Ｍ、桜井Ｍ。人事メンバー |
| システム開発環境 | GitHub | GitHub | 藤井 開発本部長 後藤M | 特権：後藤Ｍアカウント：全社員 |
| CI | GitHub Action | 藤井 開発本部長 金子M | 特権：後藤Ｍアカウント：CIアカウント管理台帳 |

### Pd2-cアカウント

Pd2-b システム一覧に記載しました。

### P2-d　委託先など

省略します。

### Pd2-e セキュリティ対策状況

P2-cセキュリティ対策状況を以下にまとめます。

#### インターネット境界

インターネット境界の構成は以下の通り（表 9）。公開サーバー等はクラウドを利用しているため、DMZは構成していない。

表 9　インターネット境界のセキュリティ対策

|  |  |  |
| --- | --- | --- |
| ネットワークデバイス | 設定 | ログなど |
| インターネットルーター | Outbound: All AllowInbound: All Deny | 認証log , Drop Log |
| ファイアウォール | Outbound:Inbound: All Deny | 認証log, Drop LogNet Flow |
| 侵入検知・遮断システム | チューニング済みのシグネチャ | IPS Event Log |
| VPN | 接続：２要素認証Source IP: 制限なし | 認証ログ（ID、IP、時刻、成否） |

#### デバイス

デバイスのセキュリティ対策は、MDMとEDRで構成している（表 10）。

表 10　デバイスのセキュリティ対策

|  |  |  |  |
| --- | --- | --- | --- |
| 対策 | 対象 | 設定 | 対処 |
| MDM | WindowsMaciOS, Android | デバイスの設定を強制 | ワイプ、ネットワーク遮断 |
| EDR | WindowsMac | Suspicious：Alert OnlyMalware: Isolationログ：ファイルアクセス、ネットワークアクセス、プロセス | 隔離・削除ネットワークからの隔離 |

#### クラウド

##### Corporate Web

アカウント管理は、以下のベストプラクティスに準じて実装（表 11）。

|  |
| --- |
| * IAM でのセキュリティのベストプラクティス – AWS Identity and Access Management (amazon.com)<https://docs>.aws.amazon.com/ja\_jp/IAM/latest/UserGuide/best-practices.html
* IAM のビジネスユースケース – AWS Identity and Access Management (amazon.com)<https://docs>.aws.amazon.com/ja\_jp/IAM/latest/UserGuide/IAM\_UseCases.html
 |

表 11　Corporate Webのアカウント構成

|  |  |  |
| --- | --- | --- |
| アカウント種別 | ID | 権限（グループ） |
| ルートユーザー(AWS Account) | 後藤M |  |
| IAM ユーザー | goto | Admins, AllUsers |
| kaneko | Developers, SysAdmins, Manager |
| yamaguchi | SysAdmins, Managers |
| yano | Managers |
| Ishida | Managers |
| Sato | SysAdmin |
| Suzuki | SysAdmin |
| WordPress ユーザー | Karasawa | 管理者 |
| Sato | 管理者 |
| Suzuki | 管理者 |
| Miyake | 編集者 |
| Aoshima | 編集者 |
| Kaneko | 編集者 |
| Goto | 編集者 |

システム構成は、以下の資料に準じて構築（図 2）

AWS:　「WordPressウェブサイトを構築する」に基づいて構築

|  |
| --- |
| * AWS(Amazon) AWS ソリューション構成例 - レンタルサーバーからの簡易 Web サイト移行 (<https://aws.amazon.com/jp/cdp/migrate-lightsail/>)
* AWS(Amazon) WordPressウェブサイトを構築する([https://aws.amazon.com/jp/getting-started/hands-on/build-wordpress-website)](https://aws.amazon.com/jp/getting-started/hands-on/build-wordpress-website%29/)
* AWS(Amazon) Amazon Lightsail でWordPress インスタンスを起動して設定する(<https://aws.amazon.com/jp/getting-started/hands-on/launch-a-wordpress-website/>)
 |

|  |  |
| --- | --- |
| AWS ソリューション構成例 - レンタルサーバーからの簡易 Web サイト移行 | WordPressは、Lightsail上に構築 |

図 2　Corporate Web システム構成

##### ゲームサイト

ゲームサイトは、以下の資料から、「オンラインゲームのためのクラウド構成と料金試算」に準じて構築（図 3）。

|  |
| --- |
| * AWS(amazon) 目的別クラウド構成と料金試算例(https://aws.amazon.com/jp/cdp/)
* AWS(amazon) オンラインゲームのためのクラウド構成と料金試算例(https://aws.amazon.com/jp/cdp/game/)
 |



図 3　ゲームサイトのシステム構成

# Pr リスク・プロファイリング:

## Pr1 事業視点のリスク・プロファイリング

JNSAアーキテクトのリスク・プロファイルを表 12として記載。

表 12　評価対象事業・システムのリスク・プロファイリング　 ホームページとオンラインゲームサイト

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | 確認する内容 | ホームページ | ゲームサイト |
| 事業概要 | 事業概要 | 事業概要、ユーザー特性、利用形態などを記載してください | 自社の情報発信の手段としてホームページを運用 | ビジュアルを強化したロールプレイングゲームユーザー間での共有や、SNSへの投稿が可能有償サービスあり（月額200円） |
| 事業責任者 | 役職と氏名を記載してください | 担当執行役員：下村CFO | 担当執行役員：唐澤事業部長 |
| 運用責任者・担当者 | 特に責任者は、役職と氏名を記載してください | 責任者：小屋 広報部長、担当：　広報グループ（唐澤Ｍ）技術サポート：情シス（佐藤、鈴木） | 青島D、GanGan運用グループ（山口）業務委託の計画あり |
| 開発責任者・担当者 | 特に責任者は役職と氏名を記載してください | 責任者：小屋 広報部長、システム構築：情シス（佐藤、鈴木） | 藤井 開発本部長GanGan開発グループ（後藤Ｍ） |
| ユーザー数（有償、無償） | システムを利用するユーザー数を記載してください | 月間 3000万ページビュー | 全体　約200万人の登録ユーザー有償　約10万名 |
| 売上高・見込み | 対象事業の売上高または、見込みを記載してください。 | N/A | 年間で約20億円月額会費：2.4億（10万名\*200円\*12カ月）有償アイテム販売など：9.6億円広告など：8億円 |
| ユーザーの居住地域サービス提供地域日本,EU, US, CH, KO,など | 海外対応の必要性を判断するため、ユーザーの主な居住地域を記載してください | 主に日本海外向け事業が始まった場合、海外向けの対応を行う | 主に日本、海外展開も検討中（EU,US） |
| 連絡窓口 | ユーザーサポート顧客担当会社代表インシデント・脆弱性 | インシデントが報告される可能性のある連絡窓口を記載してください | support@jnsa-architect.com | ask-gangan@jnsa-architect.com |
| 取り扱う情報 | 情報の種類 | 取り扱う情報の種類を記載してください。特に、機微性の高い情報に着目します。 | ■個人情報　□仮名個人情報　□金融関連情報　□その他の機微情報発表前の情報をステージングに掲載することはあるが、原則、公開情報のみを扱っている | ■個人情報　□仮名個人情報　■金融関連情報　□その他の機微情報決済はサービス代行業者が実施。原則として、決済情報はサービス内には持たない |
| 改竄された場合の影響（自社・顧客など） | 例えば、このような事例マルウエア拡散、金銭的な損害、社会インフラの停止、人命の影響、会計処理の問題、炎上 | マルウエア拡散など | マルウエア拡散、キャラクターの削除、盗難、不正な課金など |
| 業務停止の影響 | SLA | システム停止、金銭的な処理、責任の所在など | 特段のSLAは設けていない。意図しないシステムの停止は、１～２時間で解決したい | 利用規約の中で定義稼働率は保証しない旨を記載 |
| 自社への影響 | 業務の停止・遅延、決済の停止 | 技術力が疑われる可能性はあるが、重大な影響はない | ユーザーからのクレーム金銭的な保証の可能性海外展開後はGDPR等の影響 |
| 顧客などへの影響 | サプライチェーンの停止金銭的な損害 | 直接的な影響は考えにくい | 直接的に金銭的な損害をあたえる可能性は極めて低い |
| 直接的な機会損失（平均売上・利益） | １日当たり、１時間当たりの売上など | 直接的な機会損失は考えにくい | Ｎ／Ａ（金銭的な保証を除く）有償サービスとしては、550万円/日、約23万円/時に相当 |
| 遵守すべきコンプライアンス | 法的な義務ガイドライン | 個人情報保護、金融関係、医療関係、教育関係等の法令、ガイドライン | 個人情報の取り扱いを除き、特段のコンプライアンスはない | 個人情報保護法（海外展開後は、各国の規定など） |
| 制裁金・罰金・罰則など | GDPR　ｘｘ億円など | 現段階では想定していない | EU、 USで展開する可能性ありGDPR : €2000万（27億円）または、売上の4%以下（72時間以内の報告義務）CCPA: $2,500(約32万円), $7,500(約100万円) |
| 社会的な影響 | 人命・身体 | 自動運転、プラント、医療機器など | N/A | N/A |
| 環境汚染 | プラントなど | N/A | N/A |
| 倫理的バイアス | 分析、AI診断、 | N/A | N/A |
| 経済的損失（株価等） | 相場の乱高下、物価、 | N/A | N/A |
| その他 |  | N/A | N/A |

## Pr2 システムレベルのリスク・プロファイリング

JNSAアーキテクトの公開システムのリスク・プロファイルを表 13に記載します。

表 13　サイトのリスク・プロファイリング

|  |  |  |  |
| --- | --- | --- | --- |
| ENISA  | 具体的な確認項目 | ホームページ | ゲームサイト |
| O01: Geographic spread | O0100 複数のデータセンターの利用 | AWSを利用 | AWSを利用 |
| O02: Elasticity | O0200 柔軟なキャパシティを持つインフラ | AWSを利用 | AWSを利用 |
| O04: Physical security | O0400 信頼できるデータセンターを利用している | AWSを利用 | AWSを利用 |
| O05: Incident response around-the-clock | O0500 CSIRTが24x7で稼働している | 24x7では稼働していない。 | ゲームサイトに対するCSIRTは用意していない |
| O0510 インシデント対応窓口が用意されている | セキュリティ報告窓口を用意しているsecure@jnsa-architect.com | サポート窓口のみ公開している |
| O06: Software development　 | O0600 SDLが実装されている | プログラムは開発していないため、ＳＤＬは実装していない | 特段のSDLは実装していない |
| O0610 標準に基づいたセキュリティ検査を実施している | 実施していない | サービス開始前に、APIに対するセキュリティ検査を実施 |
| O07: Patching and updating | O0700 合理的なパッチ適用ポリシーがある | 実装していない | ネットワークレベルで十分な対策をしているため、ホストレベルのパッチについては特段定めていない |
| O08: Backups | O0810 特定の日時にリカバーできる | 30日間のバックアップがある | 30日間のバックアップがある |
| O09: Server-side storage | O0900 ボリュームレベルの暗号化 | 特段の暗号化は行っていない | S3をSSE、EBS、RDSをKMSで暗号化 |
| O10: Security-as-a-service and security add-ons | O1000 追加のセキュリティ機能を利用している | 特段の利用はない | 特段の利用はない |
| O11: Certification and compliance | O1100 何らかの認証を取得している | AWSは多数の認証を取得しているが、当Webサービスは認証を取得していない | AWSは多数の認証を取得しているが、当サービスでは特段の認証は取得していない |
| R01: Software security vulnerabilities | R0100 ホストレベルの要塞化を実施している | ＡＷＳのSecurity Hub CIS-Controlsで設定している | 必要なサービスのみインストールしている |
| R0120 ホストレベルのセキュリティ検査を実施 | 実施していない | ネットワークレベルの検査のみ実施 |
| R02: Network attacks | R0200 ネットワークレベルの要塞化をしている | ＡＷＳのSecurity Hub CIS-Controlsで設定している | ガイドラインに沿って、要塞化を実施している |
| R0210 ネットワークデバイスのパッチマネジメントを実施 | AWSの管理で実施されていると理解 | AWSの管理で実施されていると理解 |
| R0230 ネットワークレベルの検査を実施している | 実施していない | Security Hubを利用し、設定上の問題をモニタしている |
| R03: Social engineering attacks | R0300 ユーザーへのメールは署名している | 署名していない | 　 |
| R0302 ユーザーへのメールは、SPF, DKIM, DMARC等の対策を行っている | SPFのみ実施済み | SPFのみ実施 |
| R0310 ユーザーがMFAを利用 | N/A | 提供していない |
| R0320 IPアドレス制限を実施している | N/A | 実施していない |
| R04: Management GUI and API compromise | R0410 管理GUI/APIでMFAを利用 | 利用している | 利用している |
| R0420 IPアドレス制限を実施している | 制限をかけていない | 制限をかけていない |
| R06: Physical hazards | R0600 BCPプランを実装している | 現段階では準備をしていない | 現段階では準備をしていない |
| R07: Overloads | R0700 Overloads対応のインフラを利用 | Load Balancerを利用している | 特段の対策は行っていない |
| R10: Administrative or legal outages | R1000 予定停止 | N/A | 利用規約上、任意のタイミングで事業の停止が出来るようにしている |
| R11: Foreign jurisdiction issues | R1100 GDPR等の対応を行っている | 現段階では未実施。ただし、主要な内容については実施済み | 現段階では未実施。ただし、主要な内容については実施済み海外向けのサービスを予定 |

1. JNSA(2016)　 情報セキュリティポリシーサンプル改版（1.0版）(<https://www.jnsa.org/result/2016/policy/>) [↑](#footnote-ref-2)