**アウトプット**

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 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

# セッション1: イベント対応

## 1-2ステータスレポート

|  |  |  |
| --- | --- | --- |
| **対象事業** | ⒝-1 事業の概要 | **事業：**JNSAアーキテクト事業全般**担当責任者：**石田CISO・矢野CIO**事業概要：**PCオンラインゲーム開発及びサービス提供**売上：**年間で約2.4億円（GanGanシステムの売上から）**顧客数：**約200万人の登録ユーザー、有償　約10万名（GanGanシステムから） |
| ⒝-1.5 事件・事故の概要 |  |
| ⒝-2影響を受ける情報の種類 | □ 個人情報□ クレジットカード情報など□顧客から預かった機密情報□自社の機密情報 | □ 公表済みの情報□ 特定が困難（端末・メール等）□ その他□ 不明：影響する可能性は低いと想定 |
| ⒝-3 システム停止の影響当該システムが停止した場合の事業への影響について記載 |  |
| ⒝-4コンプライアンス法律やガイドラインで義務付けられている対応について記載 |  |
| ⒝-5社会的影響人命,金銭的な被害,人権や公平性,SDG,倫理面の懸念を記載 |  |
| ⒝-6その他 |  |
| **事業への影響** | ⒮-1対応レベルRACIで記載( - 対象外）Responsible, AccountableConsult, Inform | RACI- 経営陣RACI- 事業担当執行役員等RACI- 広報 | RACI- 情シスRACI- CSIRTRACI- CISORACI- 法務・知財 | RACI- 人事RACI- 社員全般 |
| ⒮-2 状況・概要イベント・インシデントが事業に与える状況の概要を記載 |  |
| ⒮-3 事業面の対応事業の停止・縮退などの懸念を記載 | □ 事業の停止□ 事業の縮退（一部停止）□ 事業の継続 | ・背景・補足: |
| ⒮-4 顧客・取引先の被害深刻度：Critical ,Serious , Moderate Light, -可能性：occure, hIgh,medium,low, - | □□ 金銭的な被害□□ 詐欺行為など□□ 機密情報の漏洩 | □□ 業務停止□□ 脅迫行為□□ なし | □□ その他（不明） |
| ⒮-5 自社の被害深刻度：Critical ,Serious , Moderate Light, -可能性：occure, hIgh,medium,low, - | □□ 金銭的な被害□□ 詐欺行為など□□ 機密情報の漏洩□□ 業務停止 | □□ 脅迫行為（身代金）□□ 信用の失墜□□ 社会的責任□□ なし | □□ その他（不明） |
| **顧客への影響** | ⒤-1 影響の概要影響を受ける情報・データがある場合、その概要を記載 |  |
| ⒤-2 影響を受けるデータ量・被害者数 | データ量（件数、データサイズなど）： | 被害者数（影響を受ける被害者数など）： |
| ⒤-3 影響を受ける被害者の特徴影響を受ける被害者を特定するために必要な特徴を記載 |  |
| ⒤-4 想定される二次被害情報が流出した際に、その情報の悪用により懸念される二次被害について記載 |  |
| ⒞-1 被害の確認方法顧客などが事件・事故の影響を確認する方法を記載 |  |
| ⒞-2 被害者のワークアラウンド被害者がすぐに実施できる回避策、軽減策を記載 |  |
| ⒞-3 被害者が実施できる対策被害を防ぐか軽減するために被害者が実施できる対策を記載 |  |
| ⒭-5 外部の専門家RACINで記載( - 対象外）Responsible, AccountableConsult, Inform,Notification | RACIN 公認会計士などRACIN 弁護士RACIN 安全保障貿A易情報センターRACIN 労働局 | RACIN SIベンダーRACIN セキュリティ企業RACIN 損害保険窓口RACIN 特に必要はない |
| **財務への影響** | f-(1)直接的な損害 | □金銭損害身代金：詐欺被害：現金の引き出し等： | □利益損害直接的な機会損失：間接的な機会損失： |
| f-(2)費用・賠償・制裁金等 | □費用損害事故原因調査：事故対応：広告・宣伝：コールセンター：見舞金等：被害範囲等調査： | □損害賠償賠償費用、弁護士費用等：□行政損害個人情報保護法：GDPR/CCPAなど： |
| f-(3) 無形損害・その他 | □無形損害ブランド棄損：なし株価：なし | □その他 |
| **外部への****連絡・報告** | ⒭-1 必須の連絡先（監督官庁など） | 担当者：報告先：時間的な制約： | □ 個人情報保護委員会□ GDPR□ 監督官庁□ 警察□ 不要□ その他 |
| ⒭-2 取引先 | 取引先名1（担当者1）：取引先名2（担当者2）：取引先名3（担当者3）： | □ 第一報を即時入れる□ ある程度事実関係が分かった段階で報告□ 確実な状況が把握できるまで連絡しない□ 報告の必要はない |
| ⒭-3 影響を受ける被害者 | 担当者： | □ 第一報を即時入れる□ ある程度事実関係が分かった段階で報告□ 確実な状況が把握できるまで連絡しない□ 外部の被害者はいない |
| ⒭-4 メディア等の公知 | 担当者：□ メディア□ ホームページ□ SNS等□ その他□ 不要 | 影響を受けない被害者への対応： |
| **影響を受ける****システム** | ⒯-1 システムの名称・概要 | ■名称：■責任者：・ビジネス面責任者：担当者：・技術面責任者：担当者： | ■システム概要 |
| ⒯-3 情報流出の懸念情報流出の懸念について記載 |  |
| ⒯-4 システム停止の懸念システム停止の懸念、必要性について記載 |  |
| ⒯-5 システム侵害の懸念システムが侵害を受け、攻撃が継続、拡大する懸念を記載 |  |
| ⒯-7事故の原因・要因事件・事故の原因・要因を記載 |  |
| ⒯-8 再発防止策（具体的）具体的な再発防止策を記載。 |  |

## 1-4 経営者への報告

|  |  |
| --- | --- |
| **対応責任者** |  |
| **事件・事故の概要** |  |
| **影響を受ける事業** | 事業・インフラなど |  |
| **顧客や取引先への影響** | 影響の概要 |  |
| 影響を受ける被害者数と特徴 |  |
| 想定される２次被害 |  |
| ワークアラウンド |  |
| 被害者への補償 |  |
| **事業への影響** | 事業の停止・再開の予定と根拠 |  |
|  | 事業レベルの対応（営業停止、継続、縮退など） |  |
| **財務への影響** | 金銭損害、利益損害 |  |
| 費用・賠償・制裁金など |  |
| 無形損害・その他 |  |
| **事件・事故の経緯** | 事件・事故の原因・要因（なぜ防げなかったのか） |  |
| 実施した対処 |  |
| 対応のタイムライン |  |
| 再発防止策 |  |
| **責任関係** | 関係者の処分など |  |
| **対応の評価** |  |

# セッション2：イベント対応

## 2-1ステータスレポート

1-2 ステータスレポートを、コピーし変更記録を付けて更新してください

## 2-3 原因・要因・背景・課題・再発防止策

|  |  |  |  |
| --- | --- | --- | --- |
| **原因** |  |  |  |
| **要因** |  |  |  |
| **背景** |  |  |  |
| **課題** |  |  |  |
| **再発防止策** |  |  |  |

# セッション3: 模擬記者会見

## 3-1 公表の判断

|  |  |  |
| --- | --- | --- |
| **公表実施の判断** | 実施の有無 |  |
| 判断の理由・根拠 |  |
| **公表のタイミング** | 公表のタイミング |  |
| 判断の理由・根拠 |  |

## 3-2 ポジションペーパー

|  |  |
| --- | --- |
| 項目 | 内容 |
| **影響を受ける事業** | 事業の概要 |  |
| **顧客や取引先への影響** | 影響や被害の概要 |  |
| 影響を受ける被害者数と特徴 |  |
| 想定される２次被害 |  |
| ワークアラウンド（被害の軽減策） |  |
| 被害者への補償 |  |
| **事業への影響** | 事業の停止・再開の予定と根拠 |  |
| 事業レベルの対応（営業停止、継続、縮退など） |  |
| **事件・事故の経緯** | 事件・事故の原因・要因（なぜ防げなかったのか） |  |
| 対応のタイムライン（経営者が認識したタイミングを含む） |  |
| **再発防止策** | 再発防止策の内容と実施時期 |  |
| **責任関係** | 関係者の処分など |  |

## 3-3 ステートメント

|  |  |  |
| --- | --- | --- |
| 項目 | 留意点 | 内容 |
| **事実・内容****（事故、事件）** | 誰が、いつ、どこで、なにをしたのかを５W1Hの形で簡潔に記載 |  |
| **経過** | 発生から現在に至るまでの経過を日時、時間単位で箇条書きにする経過の結果、現在の状況説明を加える |  |
| **原因** | 憶測事項は書かない |  |
| **対策** | 対策が策定できていない場合は、「いつまでに対策を発表する」か記載した方がよい |  |
| **見解（結論）** | 事件・事故について会社としてどう思うかどのように結論付けるのかどう責任を取るのか |  |

## 3-4 模擬記者会見のロール

|  |  |  |
| --- | --- | --- |
| ロール | 適切な役職、立場 | 担当者 |
| **スポークスパーソン** | 経営者、事業責任者 |  |
| **司会役** | 広報担当者等 |  |
| **記者役** | 記者、ITを担当しない方複数のグループがある場合は、他のグループ１グループの場合は、上記以外のメンバー |  |

# セッション4：ラップアップ

|  |  |
| --- | --- |
| 検討項目 | 参加者からのコメントなど |
| 学んだ点、参考になった点はありますか |  |
| JNSA Architectが事前に準備すべきだった点は、ありますか（やっておけばよかったこと） |  |
| ワークショップで改善すべき点を挙げてください |  |
| 自社にフィードバックしたい点を挙げてください |  |