**サンプル・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 | 従業員が業務で利用するPCがランサムウエアに感染し、$800の身代金が要求されている在宅で勤務しており、会社とのVPN接続は行っていないオンラインストレージと同期をしているフォルダーがある |
| ⒝-2影響を受ける情報の種類深刻度：Critical ,Serious , Moderate Light, -可能性：occure, hIgh,medium,low, - | Ml 個人情報Sl クレジットカード情報などSl 顧客から預かった機密情報Sl 自社の機密情報 | Ll 公表済みの情報Sl 特定が困難（端末・メール等）Ll その他 |
| ⒝-3 システム停止の影響 | 業務用PC1台であるため、大きな影響はない |
| ⒝-4コンプライアンス | 現段階では、個人情報漏洩に影響する可能性は低い |
| ⒝-5社会的影響 | 身代金を支払ったことが公表された場合、一定の批判をあびる可能性がある |
| ⒝-6その他 | 特になし |
| **事業への影響** | ⒮-1対応レベルRACIで記載( - 対象外）Responsible, AccountableConsult, Inform | i 経営陣i 事業担当執行役員等- 広報 | RA 情シスRA CSIRTA CISO- 法務・知財 | - 人事- 社員全般 |
| ⒮-2 状況・概要 | 業務用PC1台であるため、大きな影響はないまた、在宅勤務であり、VPNを利用していないことから、イントラネットへの侵入した可能性は低い |
| ⒮-3 事業面の対応 | □ 事業の停止□ 事業の縮退（一部停止）■ 事業の継続 | ・背景・状況:原因はまだ確認できていない規定通りに、EDR、自動アップデートが有効であった |
| ⒮-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Ll 機密情報の漏洩 | -- 業務停止-- 脅迫行為-h なし | -- その他（不明） |
| ⒮-5 自社の被害深刻度：Critical ,Serious , Moderate Light, -可能性：occured, high,medium,low, - | Lo 金銭的な被害-- 詐欺行為などMl 機密情報の漏洩L- 業務停止 | Lo 脅迫行為（身代金）Ll 信用の失墜Ll 社会的責任-h なし（軽微） | -- その他（不明） |
| **顧客への影響** | ⒤-1 影響の概要 | 現段階では、顧客に関連する情報への影響はない |
| ⒤-2 影響を受けるデータ量・被害者数 | データ量：メール等に顧客に関する情報が含まれている可能性がある現段階では、当該PCの暗号化が行われているだけだが、漏洩についても懸念がある | 被害者数：不明 |
| ⒤-3 影響を受ける被害者の特徴 | 不明 |
| ⒤-4 想定される二次被害 | N/A |
| ⒞-1 被害の確認方法 | N/A |
| ⒞-2 被害者のワークアラウンド | N/A |
| ⒞-3 被害者が実施できる対策 | N/A |
| ⒭-5 外部の専門家RACINで記載( - 対象外）Responsible, AccountableConsult, Inform,Notification | - 公認会計士など- 弁護士- 安全保障貿易情報センター- 労働局 | - SIベンダー- セキュリティ企業- 損害保険窓口- その他： |
| **財務への影響** | f-(1)直接的な損害 | ■金銭損害身代金：$800（支払う場合）詐欺被害：現金の引き出し等： | ■利益損害直接的な機会損失：N/A間接的な機会損失：N/A |
| f-(2)費用・賠償・制裁金等 | ■費用損害事故原因調査：CSIRT１人日事故対応：上記に含む広告・宣伝：なしコールセンター：なし見舞金等：なし被害範囲等調査：事故原因調査に含む | ■損害賠償賠償費用、弁護士費用等：なし■行政損害個人情報保護法：なしGDPR/CCPAなど：なし |
| 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：N/A報告先：N/A時間的な制約：N/A | □ 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 | 担当者：N/A取引先名：N/A | □ 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：N/A | □ 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：N/A |
| **影響を受ける****システム** | ⒯-1 システムの名称・概要 | ■名称：社員ＡのＰＣ■責任者：本人・ビジネス面責任者：担当者：・技術面責任者：石田CISO, 矢野CIO担当者： | ■システム概要 |
| ⒯-3 情報流出の懸念 | 暗号化されたが、情報漏洩は確認されていない。しかし、近年のランサムウエアの手口を考えると、情報の流出も想定する必要がある |
| ⒯-4 システム停止の懸念 | PCは初期化または調査のため停止するが、代替えのＰＣを提供し、業務への影響は最小限にした |
| ⒯-5 システム侵害の懸念 | WFHでVPN接続を行っていないことから、イントラネット等への侵害は考えにくいファイルサーバーを利用しているため、ファイルサーバーに怪しいファイルがおかれていないか、至急確認する必要がある |
| ⒯-7事故の原因・要因 | EDRが稼働しており、シグネチャも最新に保たれている。OSの自動アップデートも実施されており、現段階での直接的な原因・要因は掴めていない |
| ⒯-8 再発防止策（具体的） | 原因・要因が分かり次第対策を検討する |

## 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

|  |  |  |
| --- | --- | --- |
| 対象事業 | ⒝-1 事業の概要 | **事業：**#2 JNSAアーキテクト GanGan~~#1JNSAアーキテクト事業全般~~**担当責任者：**#2 佐々木 EO~~#1石田CISO・矢野CIO~~**事業概要：**#2 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）~~#1PCオンラインゲーム開発及びサービス提供~~**売上：#2 年間で約20円**~~#1年間で約2.4億円（GanGanシステムの売上から）~~**顧客数：#2 約200万人の登録ユーザー、有償　約10万名**~~#1 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 システムが止まっている、身代金の支払いが求められている（約65.8万円/日）~~#1 従業員が業務で利用するPCがランサムウエアに感染し、$800の身代金が要求されている~~~~在宅で勤務しており、会社とのVPN接続は行っていない~~~~オンラインストレージと同期をしているフォルダーがある~~ |
| ⒝-2影響を受ける情報の種類深刻度：Critical ,Serious , Moderate Light, -可能性：occure, high,medium,low, - | ~~Ml~~Sm 個人情報~~Sl~~Ll クレジットカード情報など~~Sl~~Sm 顧客から預かった機密情報（プライベートチャットなど）~~Sl~~Cm 自社の機密情報 | ~~Ll~~Lm 公表済みの情報~~Sl~~Sm 特定が困難（端末・メール等）~~Ll~~Sm その他 |
| ⒝-3 システム停止の影響 | #2 システムが止まっている、身代金の支払いが求められている（約65.8万円/日）~~#1業務用PC1台であるため、大きな影響はない~~ |
| ⒝-4コンプライアンス | #2 最近のランサムウエアの攻撃を考えると、個人情報が漏えいしている可能性がある~~#1現段階では、個人情報漏洩に影響する可能性は低い~~ |
| ⒝-5社会的影響 | #2 システムの停止、ゲーム内通貨、身代金の支払い等について議論となる可能性がある~~#1 身代金を支払ったことが公表された場合、一定の批判をあびる可能性がある~~ |
| ⒝-6その他 | #2 #1 特になし |
| 事業への影響 | ⒮-1対応レベルRACIで記載( - 対象外）Responsible, AccountableConsult, Inform | **RA**~~i~~ 経営陣**RA**~~i~~ 事業担当執行役員等**A**~~-~~ 広報 | RA 情シスRA CSIRT**R**A CISO**RA**~~-~~ 法務・知財 | - 人事**I**- 社員全般 |
| ⒮-2 状況・概要 | #2 システムが止まっている、身代金の支払いが求められている（約65.8万円/日）最近のランサムウエアの攻撃を考えると、個人情報を含む機密情報が漏えいしている可能性がある~~#1 業務用PC1台であるため、大きな影響はない~~~~また、在宅勤務であり、VPNを利用していないことから、イントラネットへの侵入した可能性は低い~~ |
| ⒮-3 事業面の対応 | **■**~~□~~ 事業の停止□ 事業の縮退（一部停止）□~~■~~ 事業の継続 | ・背景・状況:#2 攻撃により既にシステムが停止している身代金を支払うことで、復旧できる可能性はあるが、いずれにしても、復旧に数日かかる~~#1原因はまだ確認できていない~~~~規定通りに、EDR、自動アップデートが有効であった~~ |
| ⒮-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Ll 機密情報の漏洩 | **MO**~~□~~ 業務停止(ゲームが出来ない)-- 脅迫行為--~~-h~~ なし | -- その他（不明） |
| ⒮-5 自社の被害深刻度：Critical ,Serious , Moderate Light, -可能性：occured, high,medium,low, | **So**~~Lo~~ 金銭的な被害-- 詐欺行為など**Sm**~~Ml~~ 機密情報の漏洩**Co**~~L-~~  業務停止 | **Ho**~~Lo~~ 脅迫行為（身代金）**So**~~Ll~~ 信用の失墜**Mm**~~Ll~~ 社会的責任**--**-h なし（軽微） | -- その他（不明） |
| 顧客への影響 | ⒤-1 影響の概要 | #2 システムが停止しているため、顧客はGanGanを利用できない近年のランサムウエアの傾向から、すでに情報を盗まれている可能性がある。~~#1 では、顧客に関連する情報への影響はない~~ |
| ⒤-2 影響を受けるデータ量・被害者数 | データ量：#2 GanGanユーザー~~#1 等に顧客に関する情報が含まれている可能性がある~~~~現段階では、当該PCの暗号化が行われているだけだが、漏洩についても懸念がある~~ | 被害者数：#2 約200万人~~#1 不明~~ |
| ⒤-3 影響を受ける被害者の特徴 | #2 GanGanユーザー~~#1 不明~~ |
| ⒤-4 想定される二次被害 | #2 万一、データが漏洩している場合は、詐欺などの2次被害が想定されるまた、ゲーム内でのチャット等も公表される懸念がある~~#1 N/A~~ |
| ⒞-1 被害の確認方法 | #2 現段階では不明~~#1 N/A~~ |
| ⒞-2 被害者のワークアラウンド | #2 現段階ではワークアラウンドはない~~#1 N/A~~ |
| ⒞-3 被害者が実施できる対策 | #2 現段階ではない~~#1 N/A~~ |
| ⒭-5 外部の専門家 | □ 公認会計士など**■**~~□~~  弁護士（法務からコンタクト）□ 安全保障貿A易情報センター□ 労働局 | □ SIベンダー**■**~~□~~  セキュリティ企業□ 保険会社　-> （保険適用範囲外）□~~■~~ 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：#2 約600万円~~#1 $800~~（支払う場合）詐欺被害：現金の引き出し等： | ■利益損害直接的な機会損失：#2 約67万円/日に相当 ~~#1N/A~~間接的な機会損失：#2 ユーザーの減少が予想される ~~#1N/A~~ N/A |
| f-(2)費用・賠償・制裁金等 | ■費用損害事故原因調査：#2 10名x10日と予想　　　　　　＋数百万円~~#1 CSIRT１人日~~事故対応：#2 不明、最低でも数百万円~~#1 上記に含む~~広告・宣伝：#2 要検討（広報 小屋EO）~~#1 なし~~コールセンター：#2 要検討（総務 中尾取締役）~~#1 なし~~見舞金等：#2 要検討（下村 CFO）被害範囲等調査：事故原因調査に含む | ■損害賠償賠償費用、弁護士費用等：#2 要検討（法務 下村CFO）■行政損害個人情報保護法：#2漏洩が確認された場合対応が必要　~~#1 なし~~GDPR/CCPAなど：#2海外展開をしていないため不要　~~#1 なし~~ |
| f-(3) 無形損害・その他 | ■無形損害ブランド棄損：#2 甚大 ~~#1 なし~~株価：#2 なし（未上場のため）~~#1 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：N/A報告先：N/A時間的な制約：N/A | **■**~~□~~  個人情報保護委員会 #2 堀口DPO□ GDPR #2（海外ユーザーはいるが海外を対象として展開していない）**■**~~□~~  監督官庁#2 経産省 佐々木EO、野間D**■**~~□~~  警察#2 要検討（法務 下村CFO）□~~■~~不要□ その他 |
| ⒭-2 取引先 | 担当者：#2佐々木 EO,井上D ~~#1 N/A~~取引先名：#2 別表に記載 ~~#1 N/A~~担当者：#2下村CFO ~~#1 N/A~~取引先名：#2 あけぼの銀行 ~~#1 N/A~~ | □ 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：#2佐々木 EO, 平山M広報（小屋EO） ~~#1 N/A~~ | **■**~~□~~  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：#2 広報（小屋EO）**■**~~□~~  メディア #2（システムが停止しているので、何らかの対応が必要）**■**~~□~~  ホームページ**■**~~□~~  SNS等□ その他□~~■~~ 不要 | 影響を受けない被害者：#2メディア、ホームページ、SNSなどを通じて周知~~#1 N/A~~ |
| 影響を受けるシステム | ⒯-1 システムの名称・概要 | ■名称：#2GanGanシステム~~#1 社員ＡのＰＣ~~■責任者：#1 本人・ビジネス面責任者：#2 佐々木EO担当者：・技術面責任者：#2 青島 D~~#1 石田CISO, 矢野CIO~~担当者：#2GanGan運用G（山口） | ■システム概要#2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）AWS上に構築 |
| ⒯-3 情報流出の懸念 | #2 懸念はより深刻になった#1 暗号化されたが、情報漏洩は確認されていない。しかし、近年のランサムウエアの手口を考えると、情報の流出も想定する必要がある |
| ⒯-4 システム停止の懸念 | #2 既にシステムが停止している~~#1 PCは初期化または調査のため停止するが、代替えのＰＣを提供し、業務への影響は最小限にした~~ |
| ⒯-5 システム侵害の懸念 | #2 最初に被害にあったPC内の情報を悪用して、GanGanシステムに侵入している。GanGanシステムは独立したアカウント管理を行っているため、他のシステムに波及する懸念は少ないが、GanGanシステムは完全に掌握されている~~#1 WFHでVPN接続を行っていないことから、イントラネット等への侵害は考えにくい~~~~ファイルサーバーを利用しているため、ファイルサーバーに怪しいファイルがおかれていないか、至急確認する必要がある~~ |
| ⒯-7事故の原因・要因 | #2 最初に被害にあったPCが、GanGanのシステム運用を担当していた。この認証情報などを悪用して、GanGanシステムに侵入し、特権を取得したものと考えられる。~~#1 EDRが稼働しており、シグネチャも最新に保たれている。OSの自動アップデートも実施されており、現段階での直接的な原因・要因は掴めていない~~ |
| ⒯-8 再発防止策（具体的） | #1 #2 原因・要因が分かり次第対策を検討する |

## 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** |  |  |  |

# 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 | 公表を実施する |
| 判断の理由・根拠 | システムが停止していることは周知であり、サポート窓口に多数の問い合わせがあることに加えて、SNSで誤った情報が流布され、炎上騒ぎになっている。 |
| **公表のタイミング** | 公表のタイミング | 出来るだけ早いタイミングで実施する（今日中に準備し、明日会見を行う） |
| 判断の理由・根拠 | クレジットカード番号の漏洩といった誤った情報が流布されているため、ユーザーの不安を解消するためにも早急な公表が望まれる。サービス再開の目途が立っていないが、この点についても現状に加えて、状況の更新予定などについて述べることにする |

## 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」かを記載した方がよい |  |
| 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 |  |