**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

© 2023-2024 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

## E1-b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30億円  **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、約90万円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が、オンラインストレージと同期。 | | |
| ⒝-2影響を受ける情報の種類  深刻度：Critical ,Serious ,  Moderate Light, -  可能性：occur, high,  medium, unlikely, - | Mu 個人情報  Lu クレジットカード情報など  Mu 顧客から預かった機密情報  Lu 自社の機密情報 | Lu 公表済みの情報  Cu 認証情報  Su 特定が困難（端末・メール等）  Lu 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 | コンプライアンス上の問題はないと判断。 | | |
| ⒝-5社会的影響 | 社会的な影響はないと考えるが、身代金を支払らうことになった場合に、これが明らかになると、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, Accountable  Consult, Inform | i 経営陣  i 事業担当執行役員等  - 広報 | RA 情シス  RA CSIRT  A 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：occur, high,  medium, unlikely, - | -- 金銭的な被害  -- 詐欺行為など  Lu 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：occurred, high,  medium, unlikely, - | Lo 金銭的な被害  -- 詐欺行為など  Mu 機密情報の漏洩  L- 業務停止 | Lo 脅迫行為（身代金）  Lu 信用の失墜  Lu 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 | 被害者数：不明。  データ量：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あり。  当該社員のメールボックス等に顧客に関する情報が含まれている。 | | |
| ⒤-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, Accountable  Consult, 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：約90万円（支払う場合）  詐欺被害：N/A  現金の引き出し等：N/A | ■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 | 影響を受けない顧客など：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。 | | |

# セッション２

## E2-bステータスレポート

「31 サンプル・アウトプット - 更新例」に記載

## E2-c 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** | |  |

# 3 模擬記者会見

## 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。 |

## S1 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 |  |

## S2 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 |  |