

**セッション２：関係者の見解**

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

* CSIRT
  + 侵入経路
    - 最初に感染したPCからPC所有者のGanGanシステム管理者としてのSSHの認証鍵を含めた、認証情報を使って侵入が行われた。
    - このアカウントから横展開をして、GanGanシステムの管理者権限を取得した模様
    - 現在は、侵入を受けたPCは、初期化しており、このPCから更なる侵害の懸念はないと判断している
  + 脆弱性などの悪用：脆弱性の悪用については、わかっていない
  + データ漏洩：データ漏洩の懸念は拭えない
* 運用チーム
  + 状況
    - 基本的に、GanGanシステム全体が侵害されていて、データもほぼすべて暗号化されている
    - GanGanシステムは、完全にCondorの配下にあり、業務継続は出来ない状況
    - バックアップは、一週間前のバックアップが利用できるが、リストアを実施したことはない
    - GanGanは、他のシステムとは独立したシステム・アカウントで構成をしているため、GanGanを起点に侵害が広がる懸念は少ない
    - 全てのサーバーは、国内のリージョンを使用している。
    - 顧客には海外の方も含まれるが、国内向けのサービスであり、特に国外向けの事業は行っていない。
  + システム（プログラム）の１か月前のスナップショット（バックアップ）がある
    - 決済代行を使っており、この情報からアカウントの復旧が可能（決済のステータスレポートなど、ただし、パスワードは戻らない）
    - 支払いの記録などは、決済代行事業者に記録されている
  + アカウント情報はバックアップがある
* 開発部の回答
  + ソースコードは復旧が可能
  + ゲームのデータセットは、バックアップがない（キャラクター、画像、ゲームの設定、その他）
  + スクラッチ（＝新しいクラウドアカウント）からシステムを構築すると１か月（20人月）かかる
    - 加えて、動作検証にも１か月程度、セキュリティ検証に2週間は必要。
    - この対応を行った場合、現在進めている６カ月後にリリース予定の新規開発ゲームのリリースが遅れる（２~３カ月）。
  + ユーザーが保有しているゲーム内ポイントの総額は、前月末で３千万円相当。
* 法務の回答
  + 身代金を支払うことは推奨できない
  + 警察への届出をしておくことが望ましい。直接、事件が漏れることはないはず。
* 広報
  + メディアに公表する必要がありそう
  + 停止直後から、SNS等で話題になっている
* 事業責任者
  + 一刻も早く復旧をしてほしい
* サポート窓口
  + 苦情がたくさん上がっていて、電話回線がパンクしている
  + メールでの対応も追いつかない、何とかしてほしい。
  + 個人情報が大規模に漏洩したとの問い合わせが多数
  + クレジットカード情報が漏えいしたとの問い合わせも多数。
* 犯人
  + 身代金を払えば、復旧するための情報を確実に提供する犯行グループとの評判
  + 被害者が独自に復旧を試みた場合、復号鍵を使っても復号できない場合があると主張