2018年５月11日

各　位

会　社　名　株式会社マイネット
住　　所　東京都港区北青山二丁目11番３号
代表者名　代表取締役社長　上原　仁
（コード番号：3928）
問い合わせ先　取締役コーポレート本部長　村兼　躍
TEL. 03-6864-4261

当社サーバーへの不正アクセスに関する最終報告についてのお知らせ

2018年３月５日に開示しました「当社サーバーへの不正アクセスの発生と対応について」※１、３月23日に開示しました「当社サーバーへの不正アクセスに関する概要、経緯及びサービス再開状況」及び３月26日に開示しました「当社サーバーへの不正アクセスに関する中間報告書についてのお知らせ」のとおり、2018年３月１日12時頃からマイネットグループ※２が運営するゲームサービスの一部サーバーに対して不正アクセスが発生し、13タイトルに長時間メンテナンス等の影響が発生していた事象について、現在13タイトル全てのゲームが再開しております（神魔×継承！ラグナブレイクの一部プラットフォーム（Ameba版、dゲーム版、GREE版、mixi版）を除く）。

この度、社内調査の結果、判明している事実を元にインシデントの概要、原因、及び再発防止策について「当社サーバーへの不正アクセスに関する最終報告書」として取りまとめましたので下記のとおりお知らせいたします。

なお、１タイトルが一部プラットフォームにおいて再開していない状況ではありますが、本インシデントが発生した事実、発生当時の状況、サービス再開に向けて実施した作業及び社内調査の結果判明した内容についての確認は完了しており、インシデントが発生した原因に対する考察、それを踏まえての今後の当社グループとして取り組むべき再発防止策は明確となりましたので、このタイミングをもってお知らせいたします。

本インシデントにより多大なご迷惑をおかけしましたユーザーの皆様、お取引先の皆様をはじめとする関係先の皆様にご不便・ご迷惑をおかけしていることを深くお詫び申し上げます。

記

１．最終報告書の内容
添付資料の「当社サーバーへの不正アクセスに関する最終報告書」をご覧ください。

２．今後の見通し
本日開示いたしました「業績予想の修正に関するお知らせ」のとおりであります。

※１　同日に「（訂正）当社サーバーへの不正アクセスの発生と対応について」を訂正開示しております。

※２　「マイネットグループ」とは、持株会社である株式会社マイネット及びその100%子会社の総称を意味します。

以上

当社サーバーへの不正アクセスに関する最終報告書

2018年5月11日

株式会社マイネット

目次

1. はじめに

本報告書は、2018年3月1日から3月3日にかけて、当社グループが運営するゲームサービスの一部サーバーに対して断続的な不正アクセスが発生し、その結果、13タイトルに長時間メンテナンス等の影響が及んだインシデント（以下、「本インシデント」という）について、本インシデントが発生した事実、発生当時の状況、サービス再開に向けて実施した作業及び社内調査の結果判明した内容について記載し、インシデントが発生した原因に対する考察を加えた上で、今後、当社グループとして取り組む再発防止策を記したものであり、本インシデントについて当社グループのステークホルダーに説明するためのものであります。

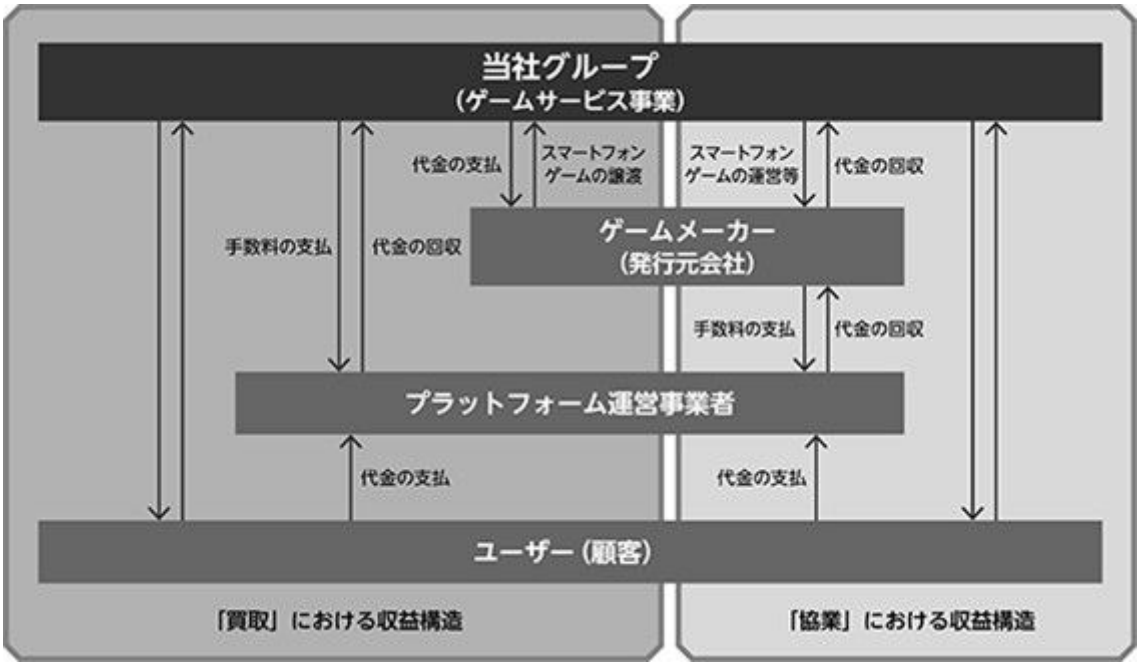
なお、本報告書は、社内調査の結果判明した事実を基に作成しており、3月4日に警察に通報し現在も捜査が継続していることから内容に変更が起こりえる旨、また、当社グループの機密情報、個人情報及びセキュリティ体制の開示に当たる情報や警察の捜査の妨げになる情報は公開していない旨、念のため申し添えます。

2. マイネットグループについて

当社グループは、「オンラインサービスの100年企業」を経営ビジョンに、社会のオンライン化の最先端で、人と人とを結び付けるサービスを提供し続けることを目指しております。現在最もオンライン化が進行している市場の一つである、スマートフォンゲームの領域で、ゲームメーカーから買取や協業で仕入れたゲームタイトルを再設計・バリューアップした後に長期サービス運営を行うゲームサービス事業を展開しております。

再設計・バリューアップの施策は大きくコストダウンの施策と売上高拡大の施策に分けられます。具体的には、運営に係る業務を分析・分解し、フローを見直すBPR（Business Process Re-engineering）やツールの開発・導入によって業務を自動化し、ゲームサービスの効率化を行っております。また同時に複数のタイトル運営で蓄積されるノウハウやユーザーの行動データを活用し、最適な施策を実施することで、売上高の拡大を図っております。運営コストの削減と売上高の拡大、その両面からのアプローチで、長く、ワクワク楽しめるゲームサービスをユーザーに提供しております。

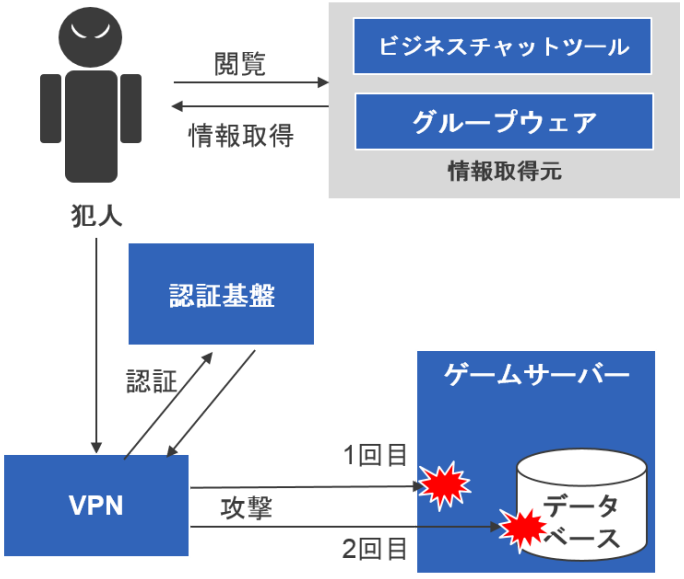
2018年5月現在、当社グループが提供しているスマートフォンゲームのタイトル数は37タイトルになります。



3. 本報告書の概要（要約）

（1）不正アクセスの概要

3月1日11時30分頃に悪意ある何者かが、何らかの方法で当社グループのネットワークに侵入し、サーバー上のデータを削除してサービス停止に至りました。また、3月3日15時頃にVPN経由で同ネットワークに侵入し、その後、一部のデータベースサーバーに対し、全てのデータベースを一括消去するコマンドを発行されたため、サービスが停止いたしました。



（2）不正アクセスによる影響とサービス再開状況

不正アクセスの結果、当社グループが運営している13タイトルのサービス提供が、一旦は再開したものの、3月3日18時頃よりメンテナンスに入り、長時間に渡るサービスの停止等の影響が及びました。

サービス再開に向けて、セキュリティ対策の実施、サービス提供環境の復旧、パブリッシャー・プラットフォームへの対応を行い、条件を満たしたタイトルからサービスを順次再開しています。5月9日時点における状況の概要は下表の通りです。

	再開状況	備考
9タイトル	再開	
2タイトル	再開	● 一部のプラットフォームについては直近のバックアップ時点に巻戻し

1タイトル	再開	● 一部のプラットフォームについては直近のバックアップ時点に巻戻し ● 一部のプラットフォームについては一部のデータが消失
1タイトル	一部プラットフォームで再開	● 残りのプラットフォームについては復旧作業継続中

（3）不正アクセス元についての特定

社内調査の結果、二度に及ぶ不正アクセスはその手口から同一の者である可能性が高いものと考えておりますが、不正アクセス元の特定には至らず、引き続き、警察による捜査の進捗を見守りたいと考えております。

（4）不正アクセスを受けた直接的な原因

本インシデントの直接的な原因は、悪意ある何者かによる当社グループのネットワークへの不正アクセスによるものですが、アカウント管理やアクセス制御にも一部不十分な面があったと考えております。当社グループ社内ネットワークへのアクセスに現在の在籍メンバーのアカウントが不正利用されていた形跡があり、当該メンバーのVPNアカウント情報（ID、パスワード）が窃取されているものと断定いたしました。また、別のグループウェアのアカウントを利用して本番環境のサーバーの共通アカウント情報が窃取されており、不正アクセス元は窃取したこの情報を使って、今回の攻撃に至ったと考えております。

（5）インシデントと当社グループのビジネスモデルとの関係

本インシデントの発生、影響が広範囲に及んだ背景には、当社グループのビジネスモデルの特徴が深く関係しております。

メーカーが開発・運営しているタイトルの環境を当社グループに移管するに際しては、移管前と同等の環境、同水準のセキュリティを維持することを基本としており、様々なサーバー環境やセキュリティ水準のものが混在している状態でありました。本インシデントが発生した13タイトルについては、同時に移管したものであり、それが当社グループが運営する他のタイトルには影響が及ばなかった理由であります。

また、今回の被害が発生した対象タイトルは全てブラウザ型のサービスとなっており、共通機能を使用していることから同一のサーバー環境下にありました。それも当社グループが運営する他のタイトルには影響が及ばなかった理由であります。なお、

一部のアプリ型タイトルについては本インシデントによる直接的な被害はありませんでしたが、安全性を重視しサービスを停止するという判断をいたしました。

様々なメーカーからタイトルを移管してくる当社のビジネスモデルでは、統一されたセキュリティポリシーの運用が困難な状況ではありましたが、本インシデントを受け、ゲームサービス事業者として対応すべきものであると考えております。

（6）不正アクセスによるインシデント発生の根本的な原因

情報システムの停止による損失や顧客情報の漏洩・喪失による信頼の失墜などの情報セキュリティ上のリスクは、ゲームサービス事業を生業とする当社グループの存在そのものに多大な影響をもたらすものであると認識しています。また、不正アクセス等は一般的に起こりうる事象であるとも認識しています。そのため、情報セキュリティに対するリスクマネジメントは最重要な経営課題の一つと位置付けておりましたが、当社グループの急成長、急拡大に情報セキュリティに対するリスクマネジメント体制が追いついていなかったことが、今回のインシデントの根本的な原因であると考えております。

（7）今後について

当社グループは情報セキュリティの抜本的な対策を求められていると認識しております。

今後、緊急対応では劣後させた課題への対処、被害を受けなかったタイトルの確認、仕入・移管時におけるセキュリティ対策に取り組むとともに、抜本的なセキュリティ対策として「セキュリティ対策の水準の向上とセキュリティガバナンス及びマネジメントシステムの構築」を目的とし、セキュリティ対策に係る全体ロードマップを策定して、専門家の支援を得つつ、経営の最重要課題として取り組んでまいります。

当社グループの役職員一同、本インシデントの発生を重く受け止め、再発防止策を実施してまいります。

4. 発生した事実

4.1. インシデントの発生からサービス再開までの経緯

2018年3月1日と3月3日に当社グループの一部のサーバーに対して、不正アクセスが行われ、本番環境のサーバーのOSのディレクトリの削除とデータベースのデータを削除されました。攻撃を受けたサーバーは、タイトルにて利用しているサーバーと共通利用のサーバー含めた全610台のうち115台に及び、長期間にわたるサービス停止が生じました。以下、時系列にて記載いたします。

日時	内容
3月1日（木） 11時40分頃	当社グループ会社である株式会社マイティゲームス（現株式会社マイネットゲームス）が運営する13タイトルを監視するサーバーより発報されたアラートを検知した当社メンバーが、データセンターで稼働している当該タイトルを提供する複数のサーバーに接続できない事象を確認。また、同タイミングにて、複数のタイトルでサービス提供に影響を及ぼす不具合が発生
同日 13時00分頃	当該13タイトルが同一環境下で運営されていることから、不具合が確認されていないサービスにも影響が及んでいる可能性を考慮し、当該13タイトルの緊急メンテナンスを実施
同日 13時10分頃	不具合の発生した対象タイトルがデータセンターで稼働していたため、データセンターへエンジニア社員3名を派遣し、調査を開始
同日 14時00分頃	データセンター内のサーバーの機器に物理障害がないかを確認し、障害がないことを確認
	データセンター内にてサーバーに直接コンソール接続し、不具合の発生した対象タイトルで、サーバーのOSのディレクトリが消失していることを確認
	サーバーのOSのディレクトリを削除する命令が書かれているスクリプトが、障害発生サーバー全てに存在していることを社員

	が確認（障害が発生しなかったサーバーには、本スクリプトは存在しなかった）
同日 19時00分頃	タイトル毎にサーバーの共通アカウント及び特権管理者アカウントのパスワード変更を実行
	限られたメンバーのみに変更後のパスワードを直接通知
同日 19時30分頃	外部からの攻撃に対するセキュリティ対応が完了し、サービス提供に影響のなかったタイトルから順次サービスを再開
3月3日（土） 17時40分頃	一部の開発サーバーのデータベースが消失していることを確認。また同タイミングで同一環境下にある13タイトルにてサービス提供に影響を及ぼす不具合を確認
同日 19時30分頃	本インシデントが3月1日に実施したインシデントへのセキュリティ対応で防げなかったことから、3月1日の攻撃とは異なり内部ネットワークを経由した不正アクセスの可能性が高いと判断し、VPNのアクセスログ調査を開始
	同一環境下にある13タイトルへの影響を考慮し、当該13タイトルの緊急メンテナンスを実施
	上原グループ代表を責任者とする緊急対応チームの組成を行い、分析及び封じ込め（①原因の調査、②ユーザーのゲームデータの保全、③開発環境の復旧、④サービス再開に必要なセキュリティ対策の実施、⑤他タイトルへの影響調査）に着手
同日 20時00分頃	同時刻にVPNにアクセスできない状況にいたメンバーのIDを利用したVPNアクセスを確認。また、そのVPNアクセス元のIPアドレスと同一IPアドレスから複数アカウントでVPNアクセス及びサーバーへのログインを確認したため、VPNを利用し内部ネットワークを経由した不正アクセスであると断定し、不正利用されている2名のVPNアカウントを停止
同日 21時00分頃	他のVPNアカウントも不正利用されている可能性を考慮し、VPNを全停止

3月4日（日） 21時45分	本インシデント内容を警視庁赤坂警察署に通報
3月5日（月）以降	不正アクセスの根絶及び復旧に着手。セキュリティ対策の実施、サービス提供環境の復旧、パブリッシャー・プラットフォームへの対応などのサービスの再開作業を開始
3月15日（木） 15時00分以降	サービスの再開条件（後述）を満たしたタイトルから、順次サービスを再開（現在に至る）

4.2. サービス再開の状況

3月15日から5月9日までにサービス再開条件を満たした全てのタイトルでサービスを再開しております。ただし、神魔×継承！ラグナブレイク（グリー版、dゲーム版、mixi版、アメーバ版）については、現時点でデータの復旧作業中であります。

また、ミリオンアーサーエクスタシス（dゲーム版、グリー版、モバゲー版、コロプラ版）、アヴァロンの騎士（dゲーム版）、HUNTER×HUNTER バトルコレクション（アメーバ版、dゲーム版）については、データが完全に復旧できなかったため、直近のバックアップ時点（それぞれ3月3日1時頃、2月28日16時頃、2月26日6時頃）に巻戻しての再開を余儀なくされました。アヴァロンの騎士（モバゲー版）ではゲームデータを完全に復旧させることが難しかったため、戦歴・履歴データの一部が消失した状態での再開となりました。

以下、サービスの再開状況について記載いたします。

3月15日15時頃	● 天下統一オンライン（モバゲー版、グリー版） ● 非公開タイトル　海外版（Android版、iOS版）
3月16日12時30分頃	● 熱血硬派くにおバトル（モバゲー版）
3月19日12時頃	● HUNTER×HUNTERバトルコレクション（モバゲー版） ● HUNTER×HUNTERアドバンスコレクション（Yahoo!モバゲー版）
3月19日15時頃	● 究極×進化!戦国ブレイク（Yahoo!モバゲー版）

3月20日17時頃	● ラグナブレイク・サーガ（Yahoo!モバゲー版、DMMゲームス版）
3月20日19時頃	● アヴァロンΩ（Android版、iOS版）
3月22日12時頃	● HUNTER×HUNTERトリプルスターコレクション（グリー版）
3月22日15時頃	● 天下統一オンライン（dゲーム版）
3月28日16時頃	● 非公開タイトル　国内版（Android版、iOS版）
4月17日15時頃	● 神魔×継承！ラグナブレイク（モバゲー版）
4月18日15時頃	● ミリオンアーサーエクスタシス（dゲーム版、グリー版、モバゲー版、コロプラ版）
4月20日12時頃	● ファイナルファンタジーグランドマスターズ（Android版、iOS版）
4月20日15時頃	● HUNTER×HUNTERバトルコレクション（アメーバ版、dゲーム版）
4月26日15時頃	● アヴァロンの騎士（dゲーム版、グリー版）
5月2日15時30分頃	● アヴァロンの騎士（モバゲー版）

4.3. 個人情報流出の有無

社内調査の結果、現時点において、本インシデントによる個人情報等の流出は確認されておりません。当社グループは、外部事業者に各種決済システムを委託しており、ユーザーのクレジットカード情報は所有しておりません。

また、その他の個人情報については、一部のタイトルにおいてユーザーのメールアドレス情報を保有しているものの、当該情報が流出した事実または形跡は確認されておりません。

5. サービス再開作業

5.1. サービス再開の条件

社内調査の結果、攻撃経路が当社グループの社内ネットワークであると特定できたため、サービス再開に必要な条件を定め、当該条件を満たしたタイトルから順次サービスの再開を行うことといたしました。

条件として、①セキュリティ対策が完了していること、②ユーザーデータのバックアップが物理的に取得されていること、③最新のソースコードが外部管理されていること、④タイトルの各種施策の更新作業が行え本番反映が出来る状態であること、⑤パブリッシャー・プラットフォームからの再開承諾が得られていること、を定めました。

サービス再開に向けて、セキュリティ対策の実施、サービス提供環境の復旧、パブリッシャー・プラットフォームへの対応を行い、条件を満たしたタイトルから順次サービスの再開を行いました。

5.2. セキュリティ対策の実施

5.2.1. 社内情報へアクセスできるアカウントへの対応

不正アクセス元にパスワードが窃取されていると判断し、認証基盤グループウェア、ビジネスチャットツール、クラウドサーバー、ネットワーク機材など、社内で利用する全アカウントのパスワードを変更いたしました。

また、ファイルサーバーのアクセス権限を適切に変更いたしました。

5.2.2. サーバーのセキュリティ対策

社内調査の結果、不正アクセス発生当時の環境では、社内ネットワークからであれば全てのサーバーにアクセス可能な状態であったため、適切なアクセス制限に変更いたしました。また、サーバーへのログインを検知する仕組みを導入いたしました。その他、必要な通信のみを許可するようにファイアウォールのポリシー変更を行いました。

5.2.3. サーバーのセキュリティ診断

サービスを再開するに際して、攻撃を受けたサーバーにマルウェア等の意図しない遠隔制御等の不正アクセスの要因となるプログラムの有無について確認するために、サーバーのセキュリティ診断を専門業者に依頼いたしました。診断の結果、疑わしいサービスは設定されておりませんでした。

なお、その他のセキュリティ上の課題が判明したため、今後対応方針を検討し、優先度をつけ対応を実施してまいります。

また、攻撃を受けたサーバーと同じネットワーク環境上で攻撃を受けていないサーバーに対しても同様の調査を行い、不正アクセスの原因となるようなプログラムの存在等は設定されていなかったことを確認いたしましたが、上記サーバーと同様にその他のセキュリティ上の課題が判明したため、今後対応方針を検討し、優先度をつけ対応を実施してまいります。

5.2.4. ネットワークのセキュリティ診断

サービス再開に際して、3月3日の攻撃に利用されたVPN機能を利用した経路以外にも侵入可能な経路がないことを確認するため、VPN機器に対するネットワーク脆弱性診断を専門業者に依頼いたしました。診断の結果、早急に対応が必要な脆弱性はないことが判明いたしましたが、緊急度は高くないもののセキュリティ上の懸念事項が指摘されたため、今後対応方針を検討し、優先度をつけ対応を実施してまいります。

5.2.5. クライアントPCのセキュリティ診断

サービス再開に際して、不正アクセスを受けた或いは、不正アクセスの試みを受けたアカウントの利用者のクライアントPCについて、攻撃のためのマルウェアやバックドアなどがないことを確認するために、専門業者によるセキュリティ診断を行いましたが、診断の結果、疑わしい設定はされていないことを確認いたしました。

5.3. サービス提供環境の復旧

5.3.1. サーバーの復旧

サービス再開に向けて、全ファイルを削除されたサーバーに関しては、同用途のサーバーの冗長化されたディスクの一部を流用して、復旧作業を行いました。一方、同用途のサーバーが存在しないサーバーに関しては新規に構築いたしました。

5.3.2. データの復旧とバックアップの設定

データベースサーバーへの攻撃を免れたタイトルについては、データの破損がなかったため、データを継続利用いたしましたが、再度の攻撃に備えてサービス再開前に、物理的に乖離された環境にバックアップを取得いたしました。

データベースサーバーが攻撃され、データが消失したサーバーについては、コールドバックアップからデータを復旧いたしました。コールドバックアップが保管されていたサーバーも攻撃され、全てのデータを消失したタイトルについては、コールドバックアップのデータサルベージを専門業者に依頼しデータ復旧をいたしました。

コールドバックアップのデータサルベージが成功したタイトルについては、データベースサーバーへデータ復旧をいたしました。データサルベージが失敗したタイトルについては、マスタデータベースサーバーやスレーブデータベースサーバーのデータサルベージを専門業者に依頼しデータ復旧をいたしました。

コールドバックアップからデータ復旧したタイトル

- ミリオンアーサー エクスタシス（dゲーム版、グリー版、モバゲー版、コロプラ版）

コールドバックアップのデータサルベージが成功したタイトル

- アヴァロンの騎士（グリー版、dゲーム版）
- HUNTER×HUNTERバトルコレクション（dゲーム版、アメーバ版）

データベースサーバーのデータサルベージが成功したタイトル

- アヴァロンの騎士（モバゲー版）

データベースサーバーのデータサルベージ中のタイトル

- 神魔×継承！ラグナブレイク（mixi版、dゲーム版、アメーバ版、グリー版）

5.3.3. 開発・運用環境の復旧

複数タイトルで共用していた開発サーバーについては、データを削除され起動できない状態であったため、タイトル毎に専用の開発サーバーを構築いたしました。

ソースコードを管理するバージョン管理サーバーについては、データを削除され起動できない状態であったため、タイトル毎に乖離された環境に構築いたしました。

画像キャッシュサーバーについても、データを削除され起動できない状態であったため、タイトル毎に乖離された環境に構築いたしました。

また、一部の監視サービスとして利用していたサーバーについては、データを削除され起動できない状態であったため、設定を変更の上、構築をいたしました。

5.4. パブリッシャー・プラットフォームへの対応

3月4日0時頃より、本件が悪意のある不正アクセスによるインシデントである旨を、影響を受けた13タイトルのパブリッシャー・プラットフォーム各社に第一報を報告しました。以後、適宜連携の上、被害の状況、サービス再開に向けての作業の進捗状況、講じているセキュリティ対策等の報告、今後の対応についての協議を行い、サービス再開に向けて対応を行ってまいりました。

タイトルによっては、パブリッシャーと協議の上、特別なセキュリティ対策を講じて、サービスの再開を行いました。

6. 原因究明調査

6.1. 調査方法

当社グループでは、2018年3月1日の不正アクセスの発生後、サービスの再開作業と並行して、機器及びサービスのログ調査、サーバーのフォレンジック調査や関係者へのヒアリング調査など原因の究明を含む事実関係の調査を実施いたしました。フォレンジック調査については、外部の専門業者に依頼いたしました。

6.2. ログ調査の結果

2018年3月3日に発生した二度目の不正アクセスに関連してVPNサーバーのログを調査したところ、当該不正アクセスが当該VPNサーバーを利用し内部ネットワークを経由したものであることが明らかになり、当該不正アクセスに利用されたVPNセッションの接続元のグローバルIPアドレスを特定いたしました。これらの情報を踏まえ、次の2点についてログを調査いたしました。

- VPNサーバーから攻撃を受けたサーバーへの経路上に位置する機器として下表に掲げるもの

経路上の機器	● VPNサーバー ● 認証基盤 ● ファイアウォール ● データセンター内のネットワーク

- 当社で利用していたクラウド等の社外サービスとして下表に掲げるものから、上記グローバルIPアドレスからのアクセスに関連するログ

利用される可能性を有していたサービス	● グループウェア ● ビジネスチャットツール ● 共有ウェブサービス

社内調査の結果、判明したログ調査の結果について、機器及びサービス別に以降に記載いたします。なお、当社グループ関係者5名をA,B,C,E,Fと表し、社内の共有グループウェアのアカウントをDと表します。

6.2.1. VPNサーバーのログ調査

2018年3月3日の二度目の不正アクセスについては、VPNサーバーに同一のグローバルIPアドレスから、A,B,Cのログイン IDを用いてログインを試みていた事実が判明いたしました。詳細といたしましては、11時08分34秒に1回、Aのユーザーアカウントを用いてログインを試みた上で成功し、最終ログアウトの時刻は15時13分40秒までであり ました。また、15時10分26秒、15時33分01秒、17時36分35秒にそれぞれ1回ずつ、Bのユーザーアカウントを用いてログインを試み、成功し、最後のログインから、最終ログアウトまでの時刻は17時36分35秒から、20時17分11秒までであり ました。さらに、14時59分44秒に1回、Cのユーザーアカウントを用いてログインを試み、失敗している事実が判明いたしました。

2018年3月1日の一度目の不正アクセスでのVPNの利用についての有無は、ログの保存期間を超えており、ログが見つからなかったため、判明いたしませんでした。

6.2.2. 認証基盤のログ調査

3月1日の一度目の不正アクセスにVPNが用いられたことを示すVPN機器からの認証要求の有無は、ログを集約するサーバーが攻撃を受け、ログが削除されたため、本調査では判明いたしませんでした。3月3日の二度目の不正アクセスに用いられたA及びBのユーザーアカウントに対するVPN機器からの認証要求については、認証許可がなされていることが判明いたしました。3月3日の二度目の不正アクセスに用いられたユーザーアカウントのパスワード入手経路については本調査では判明いたしませんでした。

6.2.3. ファイアウォールのログ調査

ファイアウォールのログ調査については、3月1日にログを集約するサーバーが攻撃を受け、ログが削除されていたため、本件に関係すると思われる履歴を確認することはできませんでした。

6.2.4. データセンター内のネットワークのログ調査

データセンター運営会社にログの提供を依頼いたしましたが、ログの提供については、機密情報の開示に当たるということでログの提供は得られず、履歴を確認するこ

とはできませんでした。今後の本インシデントの調査については、警察に相談の上、進めてまいります。

6.2.5. グループウェアのログ調査

2018年3月3日の二度目の不正アクセスに用いられたVPNのアクセス元グローバルIPアドレスから、1月9日にDでログインを試み、ログインに成功していた事実が判明いたしました。2018年3月3日の二度目の不正アクセスに用いられたVPNのアクセス元のグローバルIPアドレスから、2018年1月9日より、グループウェアアカウントであるDでログインを行い、グループウェアドライブ上のアイテムの閲覧及びダウンロードが実行されていた事実が判明いたしました。1月9日の初回ログイン直後にVPNの利用方法及び、VPNに用いるクライアントソフトウェアのインストーラーを閲覧・ダウンロードしている形跡が確認され、1月9日と1月24日に攻撃を受けたサーバーで利用されている共通アカウントのユーザー名とパスワードが暗号化されていない状態で記載されているアイテムを閲覧、1月9日に、マイネット名義で契約しているグループウェアのアカウントであれば誰でも閲覧或いはダウンロードが可能な権限設定となっているアイテムを閲覧・ダウンロードしている事実が判明いたしました。さらに、D及びEでログインを試み、失敗した履歴があり、Dへのログインについては、1月9日に3回、1月17日に3回試み、失敗している履歴が確認されました。閲覧或いはダウンロードされたアイテムの中には攻撃を受けたサーバーに関する環境構成情報を記載したものは認められませんでした。2018年3月3日の二度目の不正アクセス時に用いられたVPNのアクセス元グローバルIPアドレスから、2018年1月8日以前にグループウェアへのアクセスは認められませんでした。

6.2.6. ビジネスチャットツールのログ調査

2018年3月3日の二度目の不正アクセス時に用いられたVPNのアクセス元グローバルIPアドレスから、2018年1月7日より、ビジネスチャットツールアカウントにブラウザ版ビジネスチャットツールより不正にログインを試み、ログイン成功している履歴があり、ログアウトをした履歴はありませんでした。1月9日に2回、1月11日に1回、1月17日に2回、1月19日に1回、1月22日に1回、1月23日に1回、1月24日に1回、1月28日に1回、1月29日に2回、Dのアカウントで不正にログインを試み、成功しており、1月31日に1回、2月2日に1回、Bのビジネスチャットツールアカウントに不正にログインを試み、成功しており、2月2日に1回、Aのアカウントに不正にログインを試み、成功して

おり、2018年3月3日の攻撃時に用いられたVPNのアクセス元ではないグローバルIPアドレスから、2018年1月7日午前8時57分58秒に、Fのビジネスチャットツールアカウントにデスクトップアプリ版ビジネスチャットツールよりログインを試み、成功しており、今度は3月3日二度目の不正アクセス時に用いられたVPNのアクセス元グローバルIPアドレスから、一時間後の同日9時58分00秒にFのビジネスチャットツールアカウントにデスクトップアプリ版ビジネスチャットツールよりログインを試み、成功している事実が確認されました。2018年3月2日に、Aのダイレクチャット上で、3月1日に攻撃を受けた後に変更したサーバーのパスワードが暗号化されていない状態でやり取りされている投稿がありましたが、不正ログインされていたビジネスチャットツールアカウントのパスワード入手経路は本調査では判明いたしませんでした。2018年3月3日の攻撃時に用いられたVPNのアクセス元グローバルIPアドレスから、2018年1月8日以前にビジネスチャットツールへのアクセスがあった事実はありませんでした。

6.2.7. 共有ウェブサービスのログ調査

本件に関係すると思われる履歴は、本調査では発見できませんでした。

6.3. サーバーのフォレンジック調査結果

本インシデント発生の際に攻撃を受けた、または受ける可能性のあったサーバーについて専門業者によるフォレンジック調査を実施いたしました。調査の結果、2018年3月1日の一度目の不正アクセスを受けたサーバーに、攻撃用のスクリプトが作成され・実行された事実が判明いたしました。3月1日12時12分50秒に、攻撃を受けたサーバーの特定フォルダに攻撃用のスクリプトが作成され、同スクリプトが実行された事実が判明いたしました。3月1日12時13分00秒頃に、攻撃を受けたサーバーであるフォルダに攻撃用のスクリプトが作成され、実行された事実が判明いたしました。3月1日12時13分00秒頃に、攻撃を受けなかったサーバーであるフォルダに攻撃用のスクリプトが作成され、実行されなかった事実が判明いたしました。2018年3月3日に開発環境のサーバーフォルダにBのユーザーアカウントを用いてログインしたVPNサーバー経由でログインを試み、ログインに成功している事実が判明いたしました。更に2018年3月3日に攻撃を受けたサーバーのデータベース管理システムにおいて特権管理者アカウントを用いてデータベースを一括消去するコマンドを実行した事実が判明いたしました。

6.4. 関係者へのヒアリング調査結果

本インシデント発生当時の状況、社内のシステム環境及びセキュリティ状況について把握している社内のメンバー計3名からヒアリングを行いました。各人のヒアリング結果については、本報告書を作成する上で、各所の内容を補完するために用いており、内容については省略いたします。

6.5. 調査結果のまとめ

6.5.1. 2018年3月1日に発生したこと

社内調査の結果、一度目の不正アクセスは、2018年3月1日11時30分頃に、悪意ある何者かが、何らかの方法で社内ネットワークに侵入し、グループウェア上で窃取したID及びパスワードを利用して攻撃を受けたサーバーに侵入し、特権管理者権限へ昇格した後、ディレクトリを削除するスクリプトを用いてサーバー上のデータを削除し、サービス停止に至らしめたと判明いたしました。

6.5.2. 2018年3月3日に発生したこと

社内調査の結果、二度目の不正アクセスは、2018年3月3日15時頃に、悪意ある何者かが、VPN経由で社内ネットワークに侵入し、ビジネスチャットツールで窃取したID及びパスワードを利用してデータセンター内に設置されているサーバーに侵入いたしました。その後、データベースサーバーに対し、全てのデータベースを一括消去するコマンドを発行されたため、サービスを停止いたしました。

6.5.3. 不正アクセス元

社内調査の結果、不正アクセス元は、VPNを利用して社内ネットワークに侵入可能なことや、攻撃対象であるサーバーへの経路を含めたシステムの構成を把握しており、事前にVPNに用いるユーザーアカウントやビジネスチャットツールアカウントをログの残らない方法で窃取している事実については判明いたしましたが、不正アクセス元の特定には至りませんでした。

6.5.4. 直接的な原因

社内調査の結果、判明した本インシデント発生の直接的な原因は、悪意ある何者かによる当社グループのネットワークへの不正アクセスによるものですが、アカウント管理やアクセス制御にも一部が不十分な面があったと考えております。一部のタイトルで業務の効率性を重視し、共通アカウントと特権管理者アカウントを移管前からの状態で使用しており、アクセス制御として不十分な状況であったものと考えております。VPNサーバーに特定アカウントのID及びパスワードの管理はなされていたものの、不正アクセス元が何らかの方法で当社グループで利用しているグループウェア、ビジネスチャットツール、当社グループ内ネットワークの認証基盤、及びVPNサーバー内のアカウントのID及びパスワード情報を窃取・不正利用し攻撃を行った蓋然性が高いものと考えており、一部タイトルでのアカウント管理やアクセス制御が不十分であったとと考えております。

6.6. 残存リスクへの対応

社内調査及びサービス再開に向けた対応を進める過程で認識した本インシデントに直接的な関係はないものの、当社グループのセキュリティについて対処すべき課題が認められた項目については、後述の再発防止策に含めて今後対応することとしたいと考えております。

7. 考察

7.1. インシデントが起こった原因及び防止策

当社グループでは、本インシデントの直接的な原因は悪意ある何者かによる当社グループのネットワークへの不正アクセスによるものですが、アカウント管理やアクセス制御にも一部が不十分な面があったと考えております。社内調査の結果、社内ネットワークへ社外から不正アクセスされた履歴に社員のアカウントが利用されていた形跡があり、当該社員のVPNアカウント情報（ID、パスワード）が窃取されていると断定いたしました。また、当該アカウントを利用して本番環境の共通アカウント情報を窃取されており、不正アクセス元は窃取したVPNアカウント、本番環境の共通アカウントを利用し、今回の攻撃に至ったと考えております。

インシデント発生当時の環境では、当社グループ運営の他タイトルとは異なり、VPNアカウント、本番環境の共通アカウント、本番環境のサーバー構成、これら全てを知る事ができる環境にしないという本来のセキュリティ基準から乖離があり不十分なものでした。今後は本番環境のサーバーへのアクセス経路を限定し、多要素認証等の強固な認証方式を導入した環境とすることで、特定の人物が特定の経路でしか本番環境のサーバーにアクセスできなくなるようにすることで、インシデントの再発を防止できるものと考えております。

7.2. 二度目の攻撃が起こった原因及び防止策

本インシデントは二度の攻撃により生じております。本来であれば最初の攻撃の際に、アクセス経路の特定を行うべきでありましたが、一度目の攻撃の後、必要な情報を収集する術がなく、外部からの攻撃に対して考えうるセキュリティ対策を実施した上でサービス再開をしたものの、二度目の攻撃がVPNを利用した攻撃であったため防ぎきれませんでした。

今後は多要素認証等の強固な認証方式を導入した対策を講じるとともに、各アカウントの作り直しと権限の適正化を行ったことにより、防止できるものと考えております。

7.3. 復旧に時間がかかった原因及び防止策

本インシデント発生からサービス再開までに時間を要したのは、データが一部消失していたことから、サーバーのデータサルベージを行ったことが原因であると考えております。データが消失した理由としては、不正アクセスにより、バックアップサーバーを攻撃されたことによるものであります。バックアップデータを別の環境に保存することにより、防止できるものと考えております。

7.4. インシデントと当社グループのビジネスモデルとの関係

本インシデントの発生、影響が広範囲に及んだ背景には、当社グループのビジネスモデルの特徴が深く関係しております。

メーカーが開発・運営しているタイトルの環境を当社グループに移管するに際しては、移管前と同等の環境、同水準のセキュリティを維持することを基本としており、様々なサーバー環境やセキュリティ水準のものが混在している状態でありました。本インシデントが発生した13タイトルについては、同時に移管したものであり、それが当社グループが運営する他のタイトルには影響が及ばなかった理由であります。

また、今回の被害が発生した対象タイトルは全てブラウザ型のサービスとなっており、共通機能を使用していることから同一のサーバー環境下にありました。それも当社グループが運営する他のタイトルには影響が及ばなかった理由であります。なお、一部のアプリ型タイトルについては本インシデントによる直接的な被害はありませんでしたが、安全性を重視しサービスを停止するという判断をいたしました。

様々なメーカーからタイトルを移管してくる当社のビジネスモデルでは、統一されたセキュリティポリシーの運用が困難な状況ではありましたが、本インシデントを受け、ゲームサービス事業者として対応すべきものであると考えております。

7.5. 根本的な原因

情報システムの停止による損失や顧客情報の漏洩・喪失による信頼の失墜などの情報セキュリティ上のリスクは、ゲームサービス運営を生業とする当社グループの存在そのものに多大な影響をもたらします。また、不正アクセス等は一般的に起こりうる事象であるとも認識しております。そのため、情報セキュリティに対するリスクマネジメントは最重要な経営課題のひとつと位置付けておりましたが、当社グループの急

成長急拡大に情報セキュリティに対するリスクマネジメントが追いついていなかったことが、今回のインシデントの根本的な原因であると考えております。

8. 再発防止策

8.1. マネジメントの決意

当社グループは情報セキュリティの抜本的な対策を求められていると認識しております。本インシデントの発生を重く受け止め、今後、緊急対応では劣後させた課題への対処、本インシデントで被害を受けなかったタイトルの確認、仕入・移管時におけるセキュリティ対策に取り組むとともに、抜本的なセキュリティ対策を経営の最重要課題として取り組んでまいる所存です。

8.2. 抜本的なセキュリティ対策

抜本的なセキュリティ対策として「セキュリティ対策の水準の向上とセキュリティガバナンス及びマネジメントシステムの構築」を目的とし、セキュリティ対策に係る全体ロードマップを策定して、専門家の支援を得つつ、経営の最重要課題として取り組んでまいります。グループ代表直轄によるプロジェクトを立ち上げ、外部の専門家の支援の下、以下の施策を実施してまいります。

セキュリティ対策水準の向上	
脆弱性評価とリスクの特定	マイネットグループの事業内容、企業規模等を踏まえ、リスク項目の調査、ヒアリング、ディスカッションを行い、リスクを洗い出す
対処すべき課題と優先順位付け	洗い出したリスクに対する影響等を算定し、優先対応すべき重要リスクについて提案し、関連部署とともにこれを検討する
セキュリティ対策と費用の算出	優先対応すべきと判断されたリスクに対して、関連部署が対策を実施するために、費用感を含めた必要な実務作業を立案、計画する
その他	上記以外にも、リスクアセスメントについて必要な事項を実施し、他社事例等を活用しリスクアセスメント結果を纏める

セキュリティガバナンス及びマネジメントシステムの構築	
セキュリティポリシー、関連規程、ガイドライン等の整備	セキュリティポリシー等に定めるべき内容やレベルが、第三者から正当な評価を得られるよう、根拠として必要なセキュリティポリシーに関する他社事例や関連情報を収集し、セキュリティポリシー、関連規程、ガイドラインを策定する
セキュリティマネジメント体制の構築	情報セキュリティ管理者及び関係者を含めた全体の体制を立案し、必要な情報を記載したセキュリティマネジメント実施体制図を策定する
ユーザー教育の準備・実施	セキュリティポリシー、関連規程等に沿って、全グループメンバーがセキュリティに対する意識を維持できるトレーニングを実施する
危機管理体制の構築	危機管理に対する関係者を含めた全体体制を立案し、必要な情報を記載した危機管理実施体制図を策定する。また、インシデント対応組織に必要な手順書等を策定する

8.3. 緊急対応では劣後させた課題への対処

当社グループでは、再発防止策として、原因究明調査を進める中で判明した、本インシデントに直接的な関与はないが、対処すべき課題や、本件に係る暫定対応で運用している既知の課題などについては、優先度をつけ対応を実施してまいります。

8.4. 被害を受けなかったタイトルの確認

当社グループでは、再発防止策として、本インシデントでサービスを停止したタイトルに対して行った対策については、全ての環境で対応すべきものを峻別しリスト化を実施した上で、今回被害を受けなかったタイトルについても調査を行い、未対応の項目がある場合には、適宜対応を実施してまいります。

8.5. 仕入・移管時におけるセキュリティ対策

タイトルの仕入が恒常的に行われる当社グループにおいては、仕入元のセキュリティ環境に一定の依存はしつつも仕入・移管時に適切なセキュリティ対策は講じておりましたが、本インシデントを受け、再発防止策として、新たなタイトルを仕入れる際のデューデリジェンス時に、リスク対策費用などを予め見積もるとともに、セキュリティ対策のチェックリスト等を作成・運用し、移管後にグループ全体のガイドラインに沿ったタイトル運営を実施する体制を構築する等の対策を行い、より適切なリスクマネジメントを行ってまいります。

9. 最後に

このたびは、ユーザー様、お取引先様、株主・投資家の皆様をはじめ、関係各位には、ご心配とご迷惑をおかけいたしましたこと、改めて深くお詫び申し上げます。

ゲームサービス事業者としての責任を再認識し、再発防止に向けた取り組みについては、上記の対応に留まらず、広く検討を行い、実行していくことで信頼回復に努めてまいります。

以　上

用語集

用語	意味
クリーンインストール	OSやアプリケーションソフトを新規にインストールすること
グループウェア	組織内の複数人による情報共有や共同作業を支援するネットワークソフトウェア
グローバルIPアドレス	プロバイダー等から割り振られた一意のIPアドレス（パソコンやネットワーク機器などに個別に付けられた識別番号）
コールドバックアップ	データベースを停止した状態でバックアップを取得する方法
コマンド	コンピュータで、特定の処理の実行を指示する信号や命令
コンソール	ネットワークなどの制御やジョブ管理のためにサーバーに直接取り付けられた制御装置
スクリプト	簡易プログラム
スレーブデータベース	マスターデータベースに従うもの、複製されたもの、制御されるデータベース
ソースコード	コンピュータプログラミング言語で書かれたコンピュータプログラムである文字列（テキストないしテキストファイル）のこと
多要素認証	アクセス権を得るのに必要な本人確認のための要素（証拠）を複数、ユーザーに要求する認証方式
ディレクトリ	コンピュータで、補助記憶装置中のファイルを管理するための情報を記録した部分のこと
データサルベージ	記憶装置からのデータ復旧、つまり不具合などによって正常にデータの読み出しが行えなくなったストレージ機器からデータを取り出す作業

バックアップ	プログラムやデータの破壊に備え、予備の記憶装置にデータを複製しておくこと
ファイアウォール	企業などの内部ネットワークに対して、インターネットを通して侵入してくる不正なアクセスから守るための防護壁
ファイルサーバー	主に社内ネットワークにおいて、ユーザーが自由にファイルを保存し、共有できる仕組みに使用されるサーバーコンピュータのこと
フォレンジック	コンピュータの記憶媒体に保存されている文書ファイルやアクセスログなどから犯罪捜査に資する法的証拠を探し出すこと
マルウェア	不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアや悪質なコードの総称
OS	Operating systemの略。コンピュータで利用者とハードウェアの間にあって、利用者がコンピュータ・システムをできるだけ容易に使うことができるようにするための基本的なソフトウェア
VPN	Virtual Private Networkの略。仮想専用線を構築し、セキュリティを保った状態で、複数拠点間を接続する技術