当社サーバーへの不正アクセスに関する
中間報告書

2018 年 3 月 26 日

株式会社マイネット

目次

用語定義

本報告書で使用する用語・略語について説明いたします。

用語	説明
VPN	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
スクリプト	簡易プログラム
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
フォレンジック	システムに残された証跡やログを解析し事実を明らかにする作業
AD	AD（Active Directory）の略。当社グループ内のネットワークの認証基盤

第１　報告書の概要

本報告書は、2018 年 3 月 1 日から 3 月 3 日にかけて、株式会社マイネットの事業会社（以下、「当社グループ」という。）が運営するゲームサービスの一部サーバーに対する断続的な不正アクセスが発生し、マイネットグループが運営する 13 タイトルに長時間メンテナンス等の影響が及び、一部タイトルについては未だにサービスが再開していない状況となった事象について（以下、「本事象」という。）、本事象の概要、原因、及び再発防止策について、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す。

なお、本報告書は、社内調査の結果、現時点で判明している事実を元に作成しており、今後の調査の結果によって、内容に変更がある旨、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。

第２　本事象の概要

3 月 1 日から 3 日にかけて、VPN（Virtual Private Network）経由で当社グループの株式会社マイティゲームスのネットワークに断続的に不正アクセスが行われ、サーバーが攻撃され一部データを削除されたことにより、サービスの提供ができない状態となりました。影響を受けた 13 タイトルのサービス再開を目指し、現在はサーバーのセキュリティを再構築し、セキュアな環境で順次再起動し、データベースなどへの影響を確認しております。また、サーバーの復旧作業、一部データの復元作業、サービスの再開作業と並行して、VPN 経由での不正アクセスされた原因の特定を図っております。

なお、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、ユーザー様のクレジットカード情報は所有していないため、本件によるクレジットカード情報の流出はございません。また、当社グループは、ブラウザタイトル版においてはユーザー様のメールアドレス情報は所有しておらず、また他タイトルにおきましても、ユーザー様のメールアドレス情報の流出は現時点では確認されておりません。

当社グループでは、本事象を当社グループへのダメージを企図した悪意ある攻撃であると考え、警察に被害の届出を行い必要な資料を提出しており、今後の捜査に全面的に協力していく方針です。

現時点で考えうる不正アクセスへの対処は完了しておりますが、未知の残存リスクの可能性は否定できないため、セキュリティの強化策は継続して実施しております。同時に当社グループでは今回の事態を厳粛に受け止め、外部の専門家のアドバイスを取り入れつつ、抜本的な情報セキュリティ強化対策を取るプロジェクトを立ち上げ、再発防止に着手しております。

第３　不正アクセス発生からこれまでの経緯

2018 年 3 月 1 日の不正アクセス発生からこれまでの経緯について、以下、時系列にて記載いたします。

日時	内容
2018 年 3 月 1 日 （木） 11 時 40 分	システム部門のメンバーが対象サーバーのアラートを検知し、同タイミングにて、複数のタイトルにて不具合を確認
同日 13 時 00 分頃	ユーザーへの影響を考慮し、対象タイトルを緊急メンテナンスへ順次移行を開始
同日 13 時 10 分頃	対象タイトルのサーバーが稼動している都内のデータセンターへエンジニアを派遣し、調査を開始
同日 14 時 00 分頃	都内のデータセンター内のサーバーの状態を確認し、異常が無いことを確認
同日 19 時 00 分頃	攻撃に利用されたと思われる、サーバーの特権 ID でサーバーのデータを削除するスクリプトを発見し、その攻撃を防いで安全性を担保する為、サーバーのログインパスワードの変更を実施
同日 19 時 30 分頃	サービスに影響のなかったタイトルから順次サービス再開
2018 年 3 月 3 日 （土） 17 時 40 分頃	タイトル担当メンバーがサーバーのデータベースが消失していることを確認し、複数のタイトルにて不具合を確認
同日 同時刻	調査の結果、同一 IP アドレスから複数アカウントで VPN へのアクセスおよびサーバーへのログインが確認されたため、対象の VPN アカウント及び VPN そのものを全て停止（現在も継続中）

同日 19 時 30 分頃	本事象については、不正アクセスの可能性が高いと判断し、不正アクセスされたサーバーと類似環境にて運営しているタイトルのサービス停止を決定
同日 同時刻	緊急対策チームの組成を行い、初動対応（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
2018 年 3 月 4 日 （日） 21 時 45 分	警察に通報
2018 年 3 月 7 日 （水） 以降	サービス再開に必要なセキュリティ対策、データ保全方法の強化、サービスの再開に向けて、サーバーの復旧、一部データの復元、などのサービスの再開作業を開始
2018 年 3 月 15 日 （木）15 時 00 分以降	サービスの再開基準（①ユーザーデータの保全強化策の完了、②現時点で考えうるセキュリティ作業の完了、③社外ステークホルダーの承諾※）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）

※サービス再開をするために社外ステークホルダーの承諾が必要である理由は、当社グループの運営タイトルにはプラットフォーマー様、運営権の配信元様、運営タイトルの著作権等の権利保有者様等の関係者が複数存在するビジネスモデルに起因しております

第４　社内調査の内容、結果（概要）

１　調査の概要

上記の通り、当社グループでは、異常の検知後、速やかに、緊急対策チームを組成し、サービスの再開作業と並行して、原因の究明を含む事実関係の調査を進めて

まいりました。

調査の内容としては、不正アクセスの原因特定の為、サービス業者からのログデータの提供、フォレンジック業者等によるログデータの解析、不正アクセスの痕跡調査等を実施いたしました。並行して、警察に被害の届出を行い必要な資料を提出しております。

２　調査の結果

社内調査の結果、本報告書の提出時点で判明している事実としては、当社グループのサーバーの一部に対して、3 月 1 日 11 時頃から 2 回にわたる攻撃がなされていたことが判明いたしました。

1 回目の攻撃については、3 月 1 日 11 時頃に、本事象発生以前に犯人が何らかの方法で入手した ID 及びパスワードを利用し、当社グループのネットワーク環境内に不正に侵入の上、事前に入手したサーバーの特権 ID を使い、サーバーにログインの上、サーバー上のデータを削除するプログラムを実行しました。それにより、複数タイトルにて不具合が発生し、結果、同日 12 時の時点で、13 タイトルのサービス停止を余儀なくされました。その後、3 月 2 日午前 1 時までに 7 タイトルを再開し、午前 3 時 30 分までに 2 タイトルを再開、残り 3 タイトルについては 3 日午前 0 時頃の再開となりました。なお、1 回目の攻撃となった不正アクセスは、VPN 経由での進入の可能性が高いものと考えておりますが、その ID 及びパスワードの入手方法については現時点では不明であります。

2 回目の攻撃については、3 月 3 日 17 時 30 分頃、VPN 経由で不正にアクセスし、サーバーにログインし、サーバーデータを削除するコマンドを打鍵されたことにより発生しております。それにより、同日 19 時頃より、複数タイトルのタイトルがダウンしていたことが判明しましたので、同日 19 時 30 分頃、13 タイトル全てのサービスの停止を決定し、順次作業を行いました。その後、12 日後に最初のタイトルを再開したものの、23 日経過した現在でも 6 タイトルが停止したままとなっております。

なお、サーバーの ID 及びパスワードは、不正にアクセスしたビジネスチャット

ツール上で窃取した可能性が高いものと考えておりますが、ビジネスチャットツールと VPN の ID 及びパスワードの入手方法は不明です。

また、調査の結果、不正アクセスが VPN 以外にも、当社グループ内の 5 アカウントのビジネスチャットツール、グループウェアアカウントへ行われていたことが判明しており、そこから攻撃に必要な情報を入手した可能性が高いものと考えております。

なお、不正に接続されたものの中に、個人情報等の情報は確認されておりません。また、本事象の発生以後、不正な接続は確認されておりません。

第５　不正アクセスの原因

上記調査の結果に記載の通り、不正アクセスの原因について、現時点では犯人が何らかの方法で当社グループ内の 5 アカウントのビジネスチャットツール、グループウェアアカウント、当社グループ内のネットワークの AD（Active Directory）、VPN の ID 及びパスワード情報を盗み、盗んだ ID 及びパスワード情報を使って犯行を行ったものと考えております。ID 及びパスワード情報の入手方法等については判明しておりません。引き続き、警察の協力の元、調査を進めてまいります。

第６　本事象によるユーザーへの影響

当社グループでは、全てのゲームデータのバックアップの完全性を担保する為、バックアップの見直しを実施いたしました。

なお、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、ユーザー様のクレジットカード情報は所有していないため、本件によるクレジットカード情報の流出はございません。また、当社グループは、ブラウザタイトル版においてはユーザー様のメールアドレス情報は所有しておらず、また他タイトルにおきましても、ユーザー様のメールアドレス情報の流出は現時点では確認されておりません。よって、個人情報の流出等は発生しておりません。

当社グループでは、ユーザーデータの保全強化策の完了、現時点で考えうるセキ

ュリティ作業の完了をしたタイトルから、順次サービスの再開を行う予定であり、準備が整うまでの間、ユーザー様にゲームサービスの提供が出来ない状況となっております。

第７　サービスの再開状況について

１　サービスの再開状況

現在当社グループは、現時点で考えうるセキュリティ対策及びデータの保全方法の強化が完了したタイトルから順次サービスを再開しております。

（3 月 15 日 15 時頃 再開）
・天下統一オンライン（Mobage 版）
・天下統一オンライン（GREE 版）
・タイトル（タイトル名非公開）＜海外地域＞

（3 月 16 日 12 時 30 分頃 再開）
・熱血硬派くにおバトル（Mobage 版）

（3 月 19 日 12 時頃再開）
・HUNTER×HUNTER バトルコレクション（Mobage 版）＜ForGroove 提供＞
・HUNTER×HUNTER アドバンスコレクション（Yahoo!モバゲー版）＜ForGroove 提供＞

（3 月 19 日 15 時頃再開）
・究極×進化!戦国ブレイク（Yahoo!モバゲー版）

（3 月 20 日 17 時頃再開）
・ラグナブレイク・サーガ（Yahoo!モバゲー版、DMM GAMES 版）

（3 月 20 日 19 時頃再開）

・アヴァロン Ω（Android 版、iOS 版）

（3 月 22 日 12 時頃再開）

・HUNTER×HUNTER トリプルスターコレクション（GREE 版）＜ForGroove 提供＞

（3 月 22 日 15 時頃再開）

・天下統一オンライン（d ゲーム版）

２　サービス停止中タイトル　（3 月 26 日 16 時 00 分時点）

・アヴァロンの騎士（d ゲーム版、GREE 版、Mobage 版）

・神魔×継承！ラグナブレイク（Ameba 版、d ゲーム版、GREE 版、mixi 版、Mobage 版）

・HUNTER×HUNTER バトルコレクション（Ameba 版、d ゲーム版）＜ForGroove 提供＞

・ファイナルファンタジー グランドマスターズ（Android 版、iOS 版）＜スクウェア・エニックス提供＞

・ミリオンアーサー エクスタシス（d ゲーム版、GREE 版、Mobage 版、コロプラ版）

・タイトル（タイトル名非公開）＜国内地域＞

３　今後のサービス再開の見通し

現在サービス利用ができないゲームタイトルにつきましては、引き続きサービス再開に向けた準備を進めており、今後順次再開していく予定です。ゲームタイトルごとのサービス再開時期は未定ですが、決定次第、当社ホームページ等にてご報告いたします。

第８　再発防止策、今後の対応について

当社グループでは、サービス再開に必要な不正アクセスへの対処は完了し、更に、考えうるセキュリティの強化策を完了しております。本事象に至った原因を当社グループに対する悪意の不正アクセスに端を発していると考えつつも、今回の事

態を厳粛に受け止め、抜本的な情報セキュリティ強化対策を取るプロジェクトを立ち上げ、再発防止に着手しております。今後、外部の専門アドバイザーを含め、セキュリティ強化と再発防止に取り組み、信頼の回復に努めてまいります。

なお、今後の対応については、サービス再開を最優先に進めてまいりますと共に、更なる調査が必要と判断した場合は、第三者による調査等も検討してまいります。

加えて、本事象による当社グループに対する損害についても判明次第、お知らせするとともに、損害の回復のための犯人の特定、民事及び刑事手続きによる責任追及を実施する方針でおります。

以　上