2020 年 11 月 16 日

大阪市中央区内平野町三丁目 1 番 3 号
株 式 会 社 カ プ コ ン
代表取締役社長 辻 本 春 弘
(コード番号：9697 東証第 1 部)

不正アクセスによる情報流出に関するお知らせとお詫び

株式会社カプコンは、第三者からのオーダーメイド型ランサムウェアによる不正アクセス攻撃を受け、当社グループが保有する個人情報流出の発生を確認いたしました。

また、この攻撃により、当社が保有している個人情報・企業情報が流出した可能性があることを確認しましたので、「2. 流出の可能性がある情報」にて併せてお知らせいたします。

なお、現時点ではコンテンツ開発や事業遂行において支障はございません。

お客様はじめ多くのご関係先にご迷惑とご心配をおかけしておりますことを、深くお詫び申しあげます。

現在も調査を続けており、今後新たな情報が判明する可能性がございますが、現時点で概ね確認できた事実関係（2020 年 11 月 16 日現在判明分）の概要は次の通りです。

1. 流出を確認した情報
   （1）個人情報 9 件
      ・元従業員の個人情報 5 件
      （氏名・サイン 2 件、氏名・住所 1 件、パスポート情報 2 件）
      ・従業員の個人情報 4 件
      （氏名・人事情報 3 件、氏名・サイン 1 件）
   （2）その他
      ・販売レポート
      ・財務情報

2. 流出の可能性がある情報
   （1）個人情報（お客様・お取引先等）最大約 35 万件
      ・国内　お客様相談室 家庭用ゲームサポート対応情報（約 13 万 4 千件）
      氏名、住所、電話番号、メールアドレス
      ・北米　Capcom Store 会員情報（約 1 万 4 千件）
      氏名、生年月日、メールアドレス
      ・北米　e スポーツ運営サイト会員情報（約 4 千件）
      氏名、メールアドレス、性別
      ・株主名簿情報（約 4 万件）
      氏名、住所、株主番号、所有株式数
      ・退職者およびご家族情報（約 2 万 8 千件）、採用応募者情報（約 12 万 5 千件）
      氏名、生年月日、住所、電話番号、メールアドレス、顔写真等
   （2）個人情報（社員およびご関係者）
      ・人事情報（約 1 万 4 千人）

（3）企業情報
・売上情報、取引先情報、営業資料、開発資料等

なお、当社はネット販売等における決済は全て外部委託しておりますので、クレジットカード情報を保有しておらず、クレジットカード情報の流出はございません。
また、流出した可能性のある情報の総数は、一部ログの喪失などから特定できないため、現時点で判明している最大数としてお示ししております。

3. 個人情報の流出が確認された方々およびその可能性がある方々への対応
（1）個人情報および企業情報の流出が確認された方々への対応
情報流出が確認された方々には、個別にご連絡を行い経緯・状況のご説明を始めています。

（2）個人情報の流出の可能性がある方々への対応
窃取、流出の可能性がある情報について、引き続き調査を行ってまいります。
また、流出可能性のある情報に関連する皆さまには、下記の通りご照会専用窓口を設置致しました。

日本：カプコン情報流出専用お問合わせ窓口
電話番号（フリーダイヤル）：ゲームユーザー問合わせ窓口　0120-400161
総合問合わせ窓口　0120-896680
受付時間：10:00～20:00
北米：カプコン USA カスタマーサポートページ
URL：https://www.capcom.com/support

4. 発覚と対応の経緯
（1）・11 月 2 日未明に社内システムへの接続障害を確認、システムを遮断し被害状況の把握に着手しました。
・今回の攻撃は、当社を標的としたランサムウェアを用いてサーバを破壊し暗号化するものであったことを確認しました。
・「Ragnar Locker」を名乗る集団からのメッセージを確認し、身代金要求が判明し大阪府警に通報しました。
・11 月 4 日に「不正アクセスによるシステム障害発生に関するお知らせ」を公表しました。
・11 月 12 日に 9 件の個人情報および一部の企業情報の流出を確認しました。
・流出が確認された情報 9 件に加え、流出可能性のある情報の範囲について調査を継続し、11 月 16 日に開示しました。（本リリース）
今回の不正アクセスは、サーバ保存情報の暗号化やアクセスログの抹消を伴うもので、不正アクセスの調査、解析等に時間を要しました。
（2）欧州 GDPR 監督官庁（ICO）、個人情報保護委員会（日本）にシステム障害の発生につき、報告しています。
（3）対策ソフトを投入、疑わしい通信を遮断しつつ、サーバの再構築を実施し、復旧したサーバを基に各部署が保存していた情報の確認作業を実施（継続中）しています。
（4）本件障害のシステム面における検証につきまして、外部のセキュリティ会社へ検証を委託ずみです。この検証結果については、別途公表する予定です。
（5）また、大手ソフトウェア企業、大手セキュリティ専門ベンダ、サイバーセキュリティに造詣の深い外部弁護士に状況を報告し、指導・アドバイスを得る体制といたしました。

情報の流出が確認された方、関係先にはご連絡を開始させていただくともに、その他窃取された可能性のある情報につき、引き続き調査を継続します。

この不正アクセスは、一部報道されておりますが、いわゆる「オーダーメイド型ランサムウェア」による「標的型攻撃」であり、当社を標的にして巧妙にサーバ保存情報の暗号化やアクセスログの抹消を伴うもので、不正アクセスの調査、解析等に時間を要しました。本日のご報告になりましたことをお詫び申しあげます。

皆様方宛にお心当たりのない郵送物が届く可能性や、不審な連絡が入る可能性がございますので、ご注意いただきますようお願い申しあげます。

5. 今後の対応

(1) 引き続き、日本・米国の警察当局との連携、関係各国の個人情報保護機関への適時報告を行いアドバイスを受ける体制を続けてまいります。
(2) 前述のとおり大手セキュリティベンダ等にも協力を依頼し、本件攻撃による障害の全容解明・再発防止に向け取り組んでまいります。
(3) すでに外部のセキュリティ専門家を交えた対策会議を開始しておりますが、今後外部専門家によるシステムセキュリティに関するアドバイザリー組織を新設し、再発防止に努めてまいります。

なお、当社ゲームをプレイするためのインターネット接続や当社ホームページ等へのアクセスにより、お客様や社外の皆様へ被害が拡大することはありません。

本件による当社グループの連結業績（2021 年 3 月期）への影響は現時点で軽微と考えておりますが、改めて開示が必要な場合には、別途速やかにお知らせいたします。

皆様には、多大なるご心配とご迷惑をおかけしておりますことを、あらためてお詫び申しあげます。

当社では、今回の事態を重く受け止め、デジタルコンテンツを扱う企業として、再びこのようなことがないよう、より一層の管理体制の強化に努めるとともに、不正アクセスなどの犯罪行為には厳正に対処してまいります。

何とぞご理解とご協力を賜りますようお願い申しあげます。

【本件に関するお問い合わせ先】

＜マスコミ・投資家様向けお問い合わせ先＞
総務部 広報 IR 室
TEL: 06-6920-3623／FAX: 06-6920-5108

＜個人のお客様のお問い合わせ先＞
カプコン情報流出専用お問合わせ窓口
ゲームユーザー問合わせ窓口　0120-400161
総合問合わせ窓口　0120-896680

＜お取引先様のお問い合わせ先＞
お取引先様の当社担当部門