2021 年 4 月 13 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）

不正アクセスに関する調査結果のご報告【第 4 報】

株式会社カプコンは、第三者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が流出しましたこと（以下「本インシデント」といいます。）を 2020 年 11 月 4 日から 2021 年 1 月 12 日にかけて公表いたしました（以下「既報」といいます。）。

この度、外部の専門企業の協力のもと進めてまいりました本インシデントに関する調査が完了し、報告書を受領しましたので、当該調査結果および再発防止に向けた取り組みにつきましてご報告申しあげます。なお、当社グループのシステムは現時点でほぼ復旧しており、新設の「セキュリティ監督委員会」と連携し、今後も継続的にセキュリティ、個人情報保護の強化を図ってまいります。

お客様はじめ多くのご関係先にご心配とご迷惑をおかけいたしましたことを、深くお詫び申しあげます。また、お客様はじめ関係各位のご支援に深く感謝申しあげます。

記

１．対応の経緯

2020 年 11 月 2 日	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
2020 年 11 月 2 日	障害の原因が、ランサムウェアの攻撃によるネットワーク上の機器に対するファイルの暗号化であることが判明。被害を受けた端末において「Ragnar Locker」を名乗る集団からの脅迫メッセージを発見し、大阪府警察に通報。外部企業に復旧支援を要請
2020 年 11 月 3 日	関係各国の捜査当局および個人情報保護当局を含む関係機関への連絡を順次開始
2020 年 11 月 4 日	「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」公表
2020 年 11 月 12 日	9 件の個人情報および一部の企業情報の流出を確認
2020 年 11 月 13 日	大手セキュリティ専門企業へ原因究明調査を打診
2020 年 11 月 16 日	「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」公表 情報の流出および流出可能性について調査を継続
2020 年 12 月 21 日	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として、 「セキュリティ監督委員会」の発足に向けた準備会を開催
2021 年 1 月 12 日	「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【第 3 報】」公表
2021 年 1 月 18 日	第 1 回セキュリティ監督委員会を開催
2021 年 2 月 25 日	第 2 回セキュリティ監督委員会を開催
2021 年 3 月 26 日	第 3 回セキュリティ監督委員会を開催
2021 年 3 月 31 日	大手セキュリティ専門企業より調査報告書を受領
2021 年 3 月 31 日	大手ソフトウェア企業より報告書を受領
2021 年 4 月 13 日	本ご報告「不正アクセスに関する調査結果のご報告【第 4 報】」公表

２．被害の原因および影響範囲

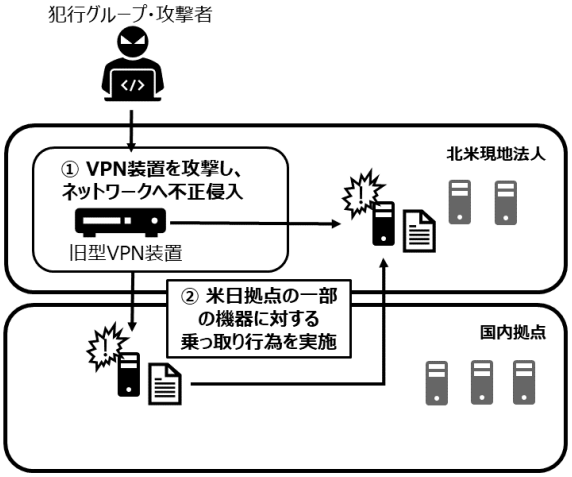
複数の大手セキュリティベンダなど大手 IT 専門企業と共に、不正アクセス攻撃を受けた機器および通信ログの調査を行いました結果、本インシデントの概要は以下の通りであることが判明しました。なお、既報の通り、国内外の警察等関係機関と連携すると共に、各国の個人情報保護当局に対しては、適時継続的に報告および対応を行っております。

2020 年 10 月、当社の北米現地法人（Capcom U.S.A., Inc.）が保有していた予備の旧型 VPN（Virtual Private Network）装置に対するサイバー攻撃を受け、社内ネットワークへ不正侵入されたものと調査により判断されています。当時、同現地法人を含め当社グループでは既に別型の新たな VPN 装置を導入済でしたが、同社所在地であるカリフォルニア州における新型コロナウイルス感染急拡大に起因するネットワーク負荷の増大に伴い、通信障害等が発生した際の緊急避難用として同現地法人においてのみ当該旧型 VPN 装置 1 台が残存しており、サイバー攻撃の対象となりました。なお、現時点で当該装置は既に廃棄済みです。

その後、かかる北米現地法人の当該旧型 VPN 装置を経由して米国および国内拠点における一部の機器に対する乗っ取り行為が実施され、情報が窃取されるに至ったと判断されています。従来より境界型※1 のセキュリティ対策は敷いており、また、後述する SOC※2 サービスや EDR※3 といった防御策の導入にも着手しておりましたところ、新型コロナウイルス感染拡大に伴いインフラ整備を優先せざるを得なかった結果、本件発生時は検証の途上（未済）でした。

これら一連の攻撃の後に、2020 年 11 月 1 日 23 時頃から米国および国内拠点における一部の機器がランサムウェアに感染させられ、各機器内のファイルを暗号化されました。同月 2 日未明より、当社グループシステムの一部でメールシステムやファイルサーバなどにアクセスしづらい障害が発生し、一部稼働を見合わせましたものの、早期に復旧を果たしております。本インシデントは、外部の専門企業によって上記の通り概ね解明されており、当社に向けた、防御が困難で多岐にわたる悪質な攻撃であったとの見解を受けております。

※1：外部ネットワークと社内ネットワークとの境界線にファイヤーウォールなどのセキュリティ措置をすること
※2：Security Operation Center の略。SOC サービスは、システムやネットワークを常時監視し、攻撃の検出・分析・対応などを支援する仕組みのこと
※3：Endpoint Detection and Response の略。ユーザが利用するパソコンやサーバなどの機器に不審な挙動を検知するソフトウェアを導入し、迅速な対応を支援する仕組みのこと



３．再発防止に向けたセキュリティ強化策

本インシデントを踏まえ、当社は従来の境界型セキュリティ対策に加え、外部との接続を常時監視する SOC サービスや機器の不正な挙動等を早期に検知する EDR の導入など、再発防止に向けた種々のセキュリティ強化策を講じております。本ご報告公表時点において対策済みの事項および今後の対策予定に分けてそれぞれご説明いたします。

（１）技術的対策

【対策済】（主要な事項）

① 大手ソフトウェア企業により、侵入の疑いのある機器全台をクリーニング済
② VPN 装置全台について改めて安全性等を確認し、対策が完了していることを確認済（北米現地法人の前記旧型 VPN 装置は廃棄済）
③ 外部との接続を常時監視するための SOC（Security Operation Center）サービスを導入済
④ 機器の不正な挙動およびコンピュータウイルス感染の早期検知を目的とした最新 EDR（Endpoint Detection and Response）を導入済
⑤ 業務用アカウントの見直しを実施済
⑥ VPN 装置および機器における、インシデント発生時の迅速な対処に向けたログの長期保存などの管理方法の更なる改善を実施済

【対策予定】

外部の専門企業およびセキュリティ監督委員会からは、上記①～⑥が現在のベストプラクティスに即しているとの回答を頂戴しているものの、今後も新たな脅威・攻撃の手口等が開発される可能性があり、そのような状況の進展に対応し、セキュリティ監督委員会のもと、様々な対策を継続的に講じてまいります。

（２）組織的対策

【対策済】

① サイバーセキュリティ（個人情報保護等のデータ保護を含む）の強化に関する外部チェックとノウハウの早期蓄積に向け、外部専門家から最新動向に基づく提言を継続的に得るため「セキュリティ監督委員会」を 2021 年 1 月下旬に発足。サイバーセキュリティの専門家である大学教授 2 名、サイバーセキュリティおよび個人情報保護法制の専門家である弁護士 1 名、システム監査専門家である公認会計士 1 名からなる外部専門家計 4 名※4 に加え、社内からは、取締役 1 名、セキュリティおよびネットワーク担当の技術職 3 名で構成。今後も保護水準の強化を目指して定期的に開催する予定です。
② 「セキュリティ監督委員会」の直下に、サイバーセキュリティに関する情報収集および防御についてのノウハウ集積、提案等を行う「セキュリティ対策室」を 2020 年 12 月に新設
③ 業務用アカウントの管理における、ツール導入を含む定期的な確認の仕組みを強化済
④ 当社グループ全体のセキュリティ・個人情報管理の更なる啓発体制を構築済

【対策予定】

PDCA サイクルに基づく更なるセキュリティ強化体制の構築および統制

※4：立命館大学 上原哲太郎 教授、英知法律事務所 岡村久道 弁護士、
大阪大学 猪俣敦夫 教授、PwC コンサルティング合同会社 丸山満彦 パートナー

４．流出およびその可能性を確認した情報

（１）流出を確認した個人情報
2021 年 1 月 12 日発表の情報から 766 人減少し、本事案発生からの累計は 15,649 人となりました。

（２）流出の可能性を確認した個人情報
2021 年 1 月 12 日発表の情報から更新はありません。

既報の通り、当社はネット販売等における決済は全て外部委託により別システムとなっておりますので（今回の攻撃対象外）、当社として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、当社ゲームをプレイいただくためのインターネット接続やダウンロードでのご購入につきましては、もともと今回攻撃を受けたシステムを用いておらず、外部委託あるいは外部サーバを別途利用しており（今回の攻撃対象外）、現在も同様です。このため、今回の本インシデントと関わりがなく、お客様に被害が及ぶことはございません。

なお、流出した可能性のある個人情報の総数は、ログの喪失などから一部特定できないため、侵害の可能性のあるサーバにおける保有数を最大数としてお示ししております。また、流出した情報が実際に悪用されたことによる被害等につきましては、現時点では確認されておりません（当社への身代金要求の件は、「６．身代金額に関する認知について」にて後述）。

５．情報の流出が確認された方々ならびに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は、個別のご連絡および経緯・状況のご説明を行っております。

（２）情報の流出に関連する皆様に向け、既報の通り以下のご照会専用窓口を設置しております。

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：Capcom U.S.A., Inc. カスタマーサポートページ
URL：https://www.capcom.com/support

ご照会の件数は減少傾向にあり、本ご報告公表前 1 ヵ月平均で 1 日あたり 0.2 件、1 週間平均で 1 日あたり 0.1 件程度となっております。

６．身代金額に関する認知について

ランサムウェアに感染した機器上には攻撃者からのメッセージファイルが残置されており、攻撃者との交渉に向けたコンタクトを要求されたことは事実ですが、同ファイルには身代金額の記載はありませんでした。既報の通り、当社は警察とも相談の上、攻撃者との交渉をしないこととといたしましたので、実際には、一切コンタクトも図っていないことから（2020 年 11 月 16 日発表のプレスリリース参照）、当社では金額を確知しておりません。

また、当社グループの連結業績（2021 年 3 月期）の見通しに変更はございませんが、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、今回の事態を真摯に受け止め、警察をはじめとする各国の関係当局からの要請および指示には適正に対応を行うとともに、デジタルコンテンツを扱う企業として、より一層の管理体制の強化に努め、犯罪行為に対しては関係機関との連携の下、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。

以　上

【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