不正アクセスに関する調査結果のご報告

2023 年 3 月 27 日

三和倉庫株式会社
情報セキュリティ委員会

目次

１．はじめに

三和倉庫株式会社は、第三者による不正アクセス攻撃を受け、当社の保有する個人情報が流出した可能性があること（以下、「本インシデント」）を、第一報として 2022 年 8 月 1 日（月）に、第四報として 9 月 22 日（木）にホームページにて公表して参りました。

この度、外部専門企業による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等につきまして、ご報告申し上げます。なお、現時点で、当社システムはほぼ復旧しておりますが、今後もセキュリティおよび個人情報保護の強化を継続的に図って参ります。

お客様はじめ多くのご関係先の皆様へ、多大なご迷惑とご心配をお掛けいたしましたこと、深くお詫び申し上げます。今後とも変わらぬお引き立ての程、何卒よろしくお願い申し上げます。

２．事故概要

2022 年 7 月 29 日（金)、ランサムウエアの攻撃を受け、突然当社サーバが停止しました。この攻撃では、VPN機器の脆弱性を突かれ、社内ネットワークへの不正侵入を許してしまいました。同時に身代金要求の脅迫を受けましたが、関係機関と相談の上、要求には応じませんでした。

その後の調査において、ファイルサーバを含むエリアへの侵入の形跡が確認されたことにより、当社が保有する個人情報の流出の可能性が判明いたしました。

システムの停止期間中は、全社一丸となって業務に取り組みましたが、お客様はじめ関係各位からの多大なるご支援に支えられ、事業継続を堅持することが出来ました。システム復旧まで約 2 ケ月を要し、10 月 3 日（月）より業務を再開しました。

３．被害状況と影響範囲

外部情報セキュリティ専門企業と不正アクセス攻撃を受けた機器並びに通信ログ等の調査を行って参りましたが、本インシデントの原因およびその影響範囲等は、以下の通りです。

2022 年 7 月 29 日（金)、当社 VPN 機器の脆弱性を突いた攻撃を受け、社内ネットワークへ不正侵入（14 時 33 分～17 時 19 分)、その間に共有フォルダ内の一部ファイルが暗号化されました。しばらくファイルサーバへアクセスしにくい状態が続き、その後サーバが非常停止しました。障害発生後、更なる感染、被害等拡大防止の為、全てのサーバ等を物理的にもネットワークから切り離す処置を行い、システムの稼働を停止しました。停止期間中は、ＥＤＩの受送信、入出庫報告、在庫報告等を行うことが出来ませんでした。

停止期間 2022 年 7 月 29 日（金）17 時 20 分　～　2022 年 9 月 15 日（木）17 時 55 分

2022 年 9 月 16 日（金）よりシステムは復旧し、データ入力を開始しました。

本インシデントにおいて、ログ等を調査した結果、海外から接続された VPN 経由で当社ファイルサーバからデータが外部に持ち出された可能性があり、そのデータには、保険契約に関する個人情報が含まれていた可能性があることが判明しました。現在、個人情報流出の可能性のある方々には、個別のご連絡および経緯・状況等、継続的に対応させて頂いております。なお、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、現時点で確認されておりません。

4. 経緯

2022年7月29日（金）	社内システムへの接続障害を確認。システムを遮断し、現況確認、被害状況の把握に着手
2022年7月31日（日）	本社に非常対策本部を設置
2022年8月 1日（月）	障害の原因が、ランサムウエ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 捜査当局及び個人情報保護当局を含む関係機関へ連絡 ホームページにシステム障害報告の掲載　「【緊急】 当社サーバー障害のお知らせ（第１報）」
2022年8月 2日（火）	ホームページに不正アクセスであることを掲載　「【緊急】 当社サーバー障害のお知らせ（第２報）」
2022年8月 8日（月）	ホームページに情報漏えいの可能性があることを掲載　「【緊急】 当社サーバー障害のお知らせ（第３報）」 データ復旧専門事業者へサーバ復旧に向けての調査依頼
2022年8月 9日（火）	情報セキュリティ専門事業者へ原因究明調査を依頼
2022年8月23日（火）	インシデント調査レポート　第1報受領
2022年8月24日（水）	別の情報セキュリティ専門事業者とセキュリティ対策等打合せ
2022年8月29日（月）	データ復旧専門事業者によるサーバデータ復旧
2022年8月31日（水）	保険会社へインシデント概要説明 データ復旧専門事業者、別のサーバの復旧着手
2022年9月 4日（日）	インシデント調査レポート　第2報受領
2022年9月 6日（火）	データ復旧専門事業者による別のサーバ復旧成功
2022年9月16日（金）	システム復旧　データ入力開始
2022年9月22日（木）	ホームページに個人情報流出の可能性があることを掲載 「【緊急】 不正アクセスによる個人情報流出の可能性のお知らせとお詫び（第４報）」
2022年9月30日（金）	9月度データ入力完了
2022年10月3日（月）	業務再開
2022年11月10日（木）	「システム障害からの復旧と再発防止策に関するお知らせ（第５報）」

5. インシデント対応（データ復旧等）のための外部委託概要

本インシデント対応としては、外部専門企業に業務委託し、フォレンジック調査を通じて、ランサムウエア被害の実態の把握、攻撃者の動きやインシデント発生原因の究明、システム復旧のための暫定的並び恒久的な対策を検討いたしました。その間、システムの早期再開のため、データの復旧を図りました。

これまで行ってきた外部委託概要は次の通りです。

当該インシデント調査を通じて、次のことが明らかになりました。

【フォレンジック調査】

調査内容	フォレンジック調査
調査期間	2022年8月9日～2022年10月24日
調査機関	情報セキュリティ専門事業者
調査内容	サイバー攻撃による被害の早急な究明
	ランサムウエア感染拡大の有無
	情報流出の有無、その経路、内容等
	セキュリティホールの特定と再発防止策の立案

・ランサムウエアによる被害状況と範囲

・ランサムウエア感染拡大の防止対策

・情報流出の可能性、経路、持ち出し方法、流出量

・セキュリティホールの特定と暫定的な再発防止対策

・ネットワーク構成の見直し、新規セキュリティ製品等の導入等、恒久的な再発防止対策

【サーバ等復旧】

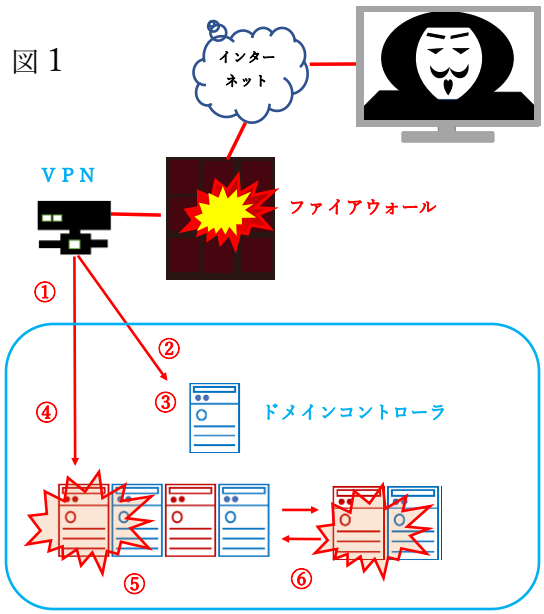
作業内容	サーバ等復旧作業
作業期間	2022年8月8日～2022年9月8日
作業機関	データ復旧専門事業者
作業内容	バックアップサーバのデータからRAID構築～診断作業
	サーバ等復旧

・サーバ等の復旧に成功

6. 事故原因

当該インシデントの発生は、「攻撃者からの遠隔操作による当社 VPN 機器の脆弱性を突いた攻撃により、ネットワーク内部に侵入され、ドメインコントローラーが攻撃を受け、重要な認証情報が盗まれた」ことに起因し、「サーバ上でランサムウエアが実行され、複数のサーバ上のファイルが暗号化、もしくは破壊」されました。詳細は以下の通り（図 1 ご参照下さい）。

図 1



①海外の IP アドレスからの不正接続

VPN 機器のログを分析した結果、VPN 機器の脆弱性を突いた攻撃が行われ、ロシアの IP アドレスからの接続が成功し、その後の約 3 時間に以下の不正アクセスが行われたことが判明した。

②内部ネットワークへの侵入

VPN 機器への接続後、複数サーバに対する大量の不正ログオンが試行された。大半のアクセスは失敗に終わるが、その数分後、ドメインコントローラーに対する不正ログオンが成功。

③ネットワーク管理サーバの管理者権限奪取

ドメインコントローラーの既知の脆弱性を突いた攻撃により、管理者権限を奪われる。

④複数のサーバへの接続

複数のサーバで遠隔操作（リモートデスクトップ）[※1] による不正ログオンが発生。この中には個人情報等の機密情報を保存したファイルサーバが含まれていた。

⑤ランサムウエアの実行

複数のサーバでランサムウエアを実行される。その実行前にアンチウイルスソフトの機能を停止させるツールがインストールされ、実行された痕跡が確認された。

⑥共有フォルダ等の暗号化

ランサムウエア実行の影響で、直接ランサムウエアを実行されたサーバを経由し、ネットワークアクセスが可能な別サーバの共有フォルダ等が暗号化された

※1：リモートデスクトップ（RDP ：Remote Desktop Protocol）

リモートデスクトップとは、あるコンピューターのデスクトップ画面をネットワーク経由で他のコンピューターに転送し、遠隔（リモート）で離れた場所にあるコンピューターの操作を可能とする仕組みのこと

7. 現在までの対応

暗号化されたデータの復旧、インシデント調査、業務復旧につきましては、前述しましたが、業務再開に向けてのシステムの真正性を評価いたしました。

（1）データベースの真正性評価

①インシデント発生後に復旧したデータベースを基に 2022 年 4 月～6 月の管理資料を作成。

②インシデント発生前に作成した 2022 年 4 月～6 月の管理資料と比較、検証。

③全ての数値等が一致していたことを確認。

④結果、復旧したデータベースの真正性は証明されました。

（2）システムの真正性評価

①インシデント発生後のシステムの真正性を評価するため、システム復旧後に作成した入出庫伝票等を検証。

②入力したデータと出力された伝票等帳票類の数値等を比較、確認。

③全ての数値等が一致していたことを確認。

④結果、復旧後のシステムの真正性は証明されました。

8. 再発防止策

本インシデントを踏まえ、本調査にて確認された攻撃者の動きやインシデント原因等の情報から再発防止のための対策を講じております。報告書作成時において対策済みおよび今後の対策予定の事項についてご説明いたします。

（1）主な再発防止策（対応済み）

直接原因となった VPN 機器への対策として、脆弱性への対応及びアカウントの棚卸しを実施し、多要素認証の徹底を図りました。

①外部への通信を必要最低限のもののみ許可し、ホワイトリスト方式にてネットワーク通信の制限を設けました。また、ホワイトリスト形式によって拒否された通信の発生元の確認を行える体制を整備しました。

②攻撃者からシステム内の認証情報を盗まれた可能性が高いため、ドメインユーザー並びにローカルユーザー共、アカウント、パスワード等の見直しを行いました。これにより攻撃者からの更なる悪用を防止します。

（2）恒久的なセキュリティ強化策（構築予定）

①ネットワークセグメントの構成を見直し、仮に侵入者がネットワーク内に侵入しても被害程度を最小限に抑えられるよう内部ファイアウォールの設置等、セキュリティ効果の高い構成

を構築いたします。

②リモートデスクトップ接続の接続元を限定し、使用制限することで、攻撃者が容易に遠隔にて操作を行えないようにします。

③セキュリティ監視ソフトの記録設置等を見直し、「重要情報」を特定し、その情報を保存しているファイルサーバへのアクセス記録を残す設定に変更いたします。

④システム内で悪意のある活動が行われた場合、不審な挙動を検知し、ログに記録を残すEDR(Endpoint Detection and Response)の導入を検討いたします。

⑤サーバ等の内部リソースから外部に対する不審なWEB通信が発生した際、検知、確認およびWEB通信のブロックが行えるURLフィルタリングの導入を検討いたします。

⑥上記記載のセキュリティ機器に対して、SOC(Security Operation Center)等の監視サービスを導入し、不審な挙動が発生した場合、迅速な検知、対応が行える監視体制を構築いたします。

（3）組織的対策

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専門事業者から最新動向に基づく提言を継続的に得ると共に、ノウハウの早期蓄積に向け「情報セキュリティ委員会」を2022年10月に発足しました。委員会は、サイバーセキュリティ専門事業者から2名、親会社である日本曹達株式会社から1名、ソフトウェア事業者から1名、社内からは取締役3名、IT推進部から2名で構成されます。

②「情報セキュリティ委員会」にて再発防止策案について協議し、対応策等を決定いたします。

③「情報セキュリティ委員会」では、再発防止策実行後の体制、対応策の検証、継続性の評価等を行い、セキュリティ強化対策の実効性を監視して参ります。

④従業員等に対し、セキュリティ・個人情報管理等の教育・啓発体制の構築を推進いたします。

9. 個人情報流出について

流出した可能性のあるデータには、保険の契約に関する個人情報が含まれていた可能性があり、該当者の方々には個別のご連絡および経緯・状況等のご説明を行っておりますが、流出した情報が実際に悪用されたことによる被害等、現時点では確認されておりません。

なお、これまでのご照会件数は、総務・人事部宛　0件、保険営業部宛16件です。

お客様への対応：当社ホームページ掲載の連絡先にて対応いたします。

当社といたしましては、引き続きネット上での情報収集を継続して参ります。何らかの被害等ございましたら、ご連絡頂きたく存じます。お手数をお掛けいたしますが、何卒よろしくお願い申し上げます。この度は、お客様並びに関係先の皆様へ多大なご迷惑とご心配をお掛けいたしますこと、重ねてお詫び申し上げます。

以　上