2022 年 2 月 8 日

葛飾区様

ランサムウェア攻撃に対する調査結果についての最終報告

株式会社オリエンタルコンサルタンツ

貴区益々ご清栄のこととお慶び申し上げます。
また、平素は格別のご高配を賜り、厚く御礼申し上げます。

さて、この度は弊社に対するランサムウェア攻撃により、葛飾区様をはじめとする関係者の皆様には、多大なるご迷惑・ご心配をおかけしておりますこと、深くお詫び申し上げます。

先般お知らせいたしました 2021 年 8 月 15 日及び同 19 日に生じた弊社社外データセンターのサーバーならびに社内のサーバー及び PC 端末に対するランサムウェアによる攻撃について調査（以下「本調査」といいます。）し、確認された結果につきましてご報告をさせていただきますのでご査収下さい。

１．今回のサイバー攻撃の概要

(1) 2021 年 8 月 15 日

・社外データセンターの AD サーバー、ファイルサーバーおよび社内のファイルサーバー、PC 端末に対して、ランサムウェアの攻撃を受けました。
・速やかに外部専門業者へ相談を行い、その助言に基づき、顧客からのデータ保護を優先するとともに、二次被害を防止するため、ファイルサーバーのシャットダウンを実施し、同日中に完了いたしました。

(2) 2021 年 8 月 19 日

・社外データセンターの業務サーバーに対して、ランサムウェアの攻撃を受けました。なお、当該攻撃は 8 月 15 日とは別の攻撃者による可能性が高いと考えられます。
・この攻撃による、顧客の業務関連データへの被害はございませんでした。
・同日中に、外部専門業者の助言に基づき、業務サーバーのシャットダウンを完了いたしました。

２．今回のサイバー攻撃に関する対応経緯

・令和3年8月15日（日曜日）　当社のADサーバ、ファイルサーバがランサムウェアの攻撃を受ける
・同年　8月17日（火曜日）　当社から区へ状況を報告
・同年　8月19日（木曜日）　当社の業務サーバに対してランサムウェアの攻撃を受ける
・同年　8月20日（金曜日）　当社ホームページにて外部公表
・同年　8月24日（火曜日）　区を訪問し、当社から状況を説明・報告
・同年　9月15日（水曜日）　当社から区へ経過状況を報告
・同年　10 月 1 日（金曜日）　当社から区へ中間報告および「メールファイル添付再開の承諾願い」を提出
・同年　10 月 7 日（木曜日）　当社から区へ中間報告（その２）を提出
・同年　10 月 13 日（水曜日）区から「事実調査及び再発方針策の報告等について（依頼）」及び質問書を受領
・同年　10 月 19 日（火曜日）当社から区へ質問回答書を提出
・同年　11 月 1 日（月曜日）　区 CIO 補佐官と当社で確認・協議を実施

３．区から受領した情報

(1)　民間施設の浸水対応型拠点建築物化検討に関する業務（都市計画課）

◇個人情報の取扱い：有り（中高層集合住宅建設に係る情報）

◇機密性情報の取扱い：無し

(2)　金町駅北口周辺地区基盤整備推進計画案策定支援に関する業務（金町街づくり担当課）

◇個人情報の取扱い：有り（金町駅北口周辺地区基盤整備に係る情報（土地・建物登記事項証明書））

◇機密性情報の取扱い：無し

(3)　葛飾区河川監視カメラ設置実施設計等に関する業務（危機管理課）

◇個人情報の取扱い：無し

◇機密性情報の取扱い：無し

(4)　葛飾区道路管理計画更新業務支援委託に関する業務（道路補修課）

◇個人情報の取扱い：無し

◇機密性情報の取扱い：無し

(1)～(3)は、㈱オリエンタルコンサルタンツの受注業務。(4)は、㈱エイテックの受注業務。

４．本調査の結果

(1) 本調査の目的と概要

本調査の目的は、攻撃手口の分析による原因究明、被害範囲の把握、データの窃取状況を明らかにすることとしております。

本調査では、ネットワーク装置やサーバー内に残されたログ(サーバーの利用状況やデータ通信などの履歴や情報を記録したもの)を解析することにより、サイバー攻撃の種類や経緯・経路などの原因究明を行い、データ窃取の痕跡の確認を行いました。

(2) 調査の結果

弊社グループの情報セキュリティ対策は、一般に必要とされるレベルでありましたが、外部からの不正アクセスにより攻撃されたことが確認されました。また、今回の攻撃により、サーバー内に保管されていた業務関連データの一部が不正に外部送信された可能性は否定できないことが判明いたしました。

ただし、具体的にどのデータが不正送信されたかについては確認することができませんでした。

５．現在のセキュリティ対策

（1）社内サーバー

サイバー攻撃を受け、シャットダウンしている社内サーバーは、**アクセスできない状態を継続**し、安全性を確保しながら調査を実施しているところであり、今後業務において当該サーバーを使用することはありません。

（2）Web サイトの安全性

一般的にランサムウェアの感染経路としてメール以外にWeb サイトが挙げられますが、**弊社のHP はネットワーク対策により、攻撃の影響はありません。**

（3）使用するパソコンの安全性

業務に従事する社員を含む社内で使用している全パソコンについては、アンチウイルスソフトによるフルスキャンを定期的に実施し、**パソコンがウイルスに感染していない**ことを確認した上

で使用しています。

（４）メール送受信の安全性

メールの送受信は、**安全性が確保されたメールサーバーを利用**しています。また、今回の攻撃の後、メールのパスワードを新たなルールによってすべて変更しており、**なりすましメールを防止**し、Web 会議などへの安全な参加ができると考えています。

さらに、今回のランサムウェア攻撃後、新たなセキュリティ機能を活用する契約としました。

上述の対策に加えて新たな契約により、弊社での受信メールについても安全性が高まり、弊社とのメール、ファイルを添付したメール通信についても安全性が高まり、安心してご利用いただけるものと考えております。

（５）業務執行時の社内環境の安全性

業務執行する際に使用するパソコンは（３）に示す安全性が確認されたパソコンとして、社内でのデータ格納、共有は、**社外のクラウドストレージサービス上**で実施しています。

また、大量のデータファイルなど共有が必要な場合には、指定された安全な配信サービスおよび安全性が確保されている社外のクラウドストレージサービスを利用します。

６．今後の対応

(1) 各当局への報告

弊社は、個人情報保護委員会、監督官庁を含む関係各局、警察等にも報告を実施済みであり、当局の指導に従い、本件への対応を適切かつ真摯に行って参ります。

(2) 情報漏洩の監視

外部専門業者の協力の下、インターネット上に窃取された情報の公開がなされていないか監視を行っております。現時点におきましては、葛飾区様の業務関連データがインターネット上に公開されるなどの具体的な情報漏洩の事実は確認されておりませんが、引き続き、情報漏洩の事実確認のため、外部専門業者の助言の下、調査・監視を継続して参ります。

具体的には、インターネット上の情報の公開の監視は、外部専門業者に依頼しており、弊社から窃取された情報の公開が確認されればすぐに報告されることになっています。

万が一、具体的な情報漏洩の事実が確認されました場合には、速やかに葛飾区様にお知らせいたします。

(3) 情報漏洩が確認された場合の対応

万が一、情報漏洩による被害が発生いたしました場合につきましては、葛飾区様とご相談の上、契約内容等も踏まえ、適切かつ真摯に対応させていただきます。

(4) 再発防止策

弊社は、今後、本調査の結果や外部専門業者による助言をもとに、セキュリティ対策を一層強化し、再発防止に取り組んでまいります。

弊社グループおよびグループ各社において、インターネット接続に関するセキュリティ強化、エンドポイントに関するセキュリティ強化を行い、今後のIT基盤の再構築整備を進めており、今後、定期的な評価・見直しを行ってまいります。

再発防止策の実施体制としては、弊社グループおよび弊社のサイバー対策本部でセキュリティ対策の再構築を実施し、弊社のＤＸ推進本部により監視・運用を致します。

以上