

2022年2月2日

各位

東京コンピュータサービス株式会社

## サイバー攻撃による被害と復旧状況について(第二報)

2021年12月31日未明に弊社システムがサイバー攻撃を受け、ランサムウェアに感染し、本年1月4日付け「サイバー攻撃による被害と復旧状況について(第一報)」で公表しました件につき、お客様はじめ関係する皆様に、多大なるご心配をおかけしますことを深くお詫び申し上げます。

第一報でご報告しましたとおり、感染発覚後、社内ネットワークの再構築を進めてまいりましたが、一部業務を再開できていなかった部門を含め、代替システムの構築等により、業務再開の目途が立ちました。また、納期遅延等が発生しているお客様には、順次、お詫びと対応策をご提案・ご相談いたしております。

弊社は、本件発覚後、速やかにサイバーセキュリティ緊急対策本部を立ち上げ、専門会社の協力を得て、侵害調査や被害の実態解明等を実施しております。

下記にこれまでに判明した事実についてお知らせいたします。

### ■判明した事実

- ・今回、弊社システムに対する攻撃は、「Night Sky」と呼ばれるランサムウェアグループによるものと判断しており、侵入された弊社サーバおよびPCに格納されたファイルが暗号化された上、拡張子が nightsky に変更され、開くことができない状態となりました。
- ・また、暗号化されたファイルが存在するフォルダに、攻撃者へのアクセス方法等が記載されたファイルが残されており、弊社システム内の情報を窃取した旨と弊社システム内のデータを公開されたくなければ、攻撃者側に連絡するようとのメッセージが残されておりました。
- ・攻撃者が窃取したとする情報の画像ファイルが特殊サイトに公開されていることを調査の過程で確認しましたが、公開された情報はいずれも社内管理情報であり、弊社が取り扱うお客様取引情報等のデータは確認されませんでした。また、現在のところ、上記画像ファイルの他に、追加情報が公開されたとは確認されておりません。
- ・弊社内のサーバやパソコンには、すべてウイルス対策ソフトウェアを導入し、最新の状態に保っていましたが、12月31日時点において、この新種のランサムウェアには対応していませんでした。
- ・既に第一報にも記載したとおり、弊社は事件発生直後に所轄警察署に被害申告を行いました。また、情報処理推進機構 (IPA)、日本サイバー犯罪対策センター (JC3)、経済産業省等、各種機関への報告を行っております。その結果、弊社以外にも、同時期に同種の被害が発生していることを確認しております。

- ・現在、サイバーセキュリティ専門会社に依頼し詳細調査を行っておりますが、本日時点で判明したこととして、攻撃者が社員向けAD情報の管理システムに不正侵入し、ランサムウェアを組み込んだことがわかってきております。更に全容を掴むべく、調査を継続しております。

上記のとおり、画像ファイルから確認できる漏洩情報に、取引情報や個人情報等のデータは確認されていないことから、今回の件により、弊社が取り扱うお客様取引情報等のデータが流出したとは想定しにくいと考えておりますが、未だその可能性がゼロであるとは言い切れない状況であります。もし、そのような事象が発見された場合には、漏洩情報の内容に応じ、誠実に対処させていただきます。

お客様はじめ関係する皆様に多大なるご迷惑をおかけしておりますこと、改めて心からお詫び申し上げます。可及的速やかに今回の事態を解明、分析し、再発防止に向けて、全社あげて取り組んでまいりますので、何卒よろしくお願い申し上げます。

(お問い合わせ先)

東京コンピュータサービス株式会社 本社機構 業務推進室  
03-3815-7911