2025年2月 25 日
SOMPO企業保険金サポート株式会社

業務委託先鑑定会社におけるランサムウェア被害に伴う情報漏えいのおそれについて

当社が損害調査業務の委託契約を締結している東京損保鑑定株式会社(以下、「東京損保鑑定」)において、昨年 8 月に第三者からの不正アクセスによるランサムウェア被害が発生し(詳細は、3～4頁記載の ご参考 をご参照ください)、その後、東京損保鑑定から調査完了の報告を受け、当社お取引先さまのお客さま情報の漏えいのおそれがあることが判明しましたので、以下をお知らせいたします。

お客さまにはご迷惑とご心配をおかけすることになり深くお詫び申し上げます。

また、現時点で、お客さま情報が漏えいした事実および不正使用された事実は確認されておりません。

東京損保鑑定社に対し、調査結果を踏まえた再発防止策の徹底を求めていくとともに、当社においても、より一層の管理体制の強化に努めてまいります。

1. 漏えいのおそれがあるお客さま情報

(1)対象のお客さま

当社が、東京損保鑑定社へ損害調査業務として鑑定業務を委託したお客さま334 件

(2)漏えいのおそれのあるお客さま情報の項目

氏名、電話番号、物件所在地、事故日、事故内容、口座情報および損害調査のために提出された写真、修理見積書など

(3)二次被害又はそのおそれの有無及び内容

現時点でお客さま情報が外部に流出した事実および不正使用された事実は確認されておりません(※)。

(※)東京損保鑑定社が委託する調査会社を通じて、ダークウェブサイトの確認を行っていますが、2025 年1月24 日時点で流出した情報の掲載はないとの報告を受けています。

2. 今後の対応

情報漏えいのおそれがあるお客さまのうち、ご連絡先等が特定できた方に対し、損害調査業務の委託元の当社取引先様と連携し、順次お知らせいたします。なお、特定できなかった場合は、本公表をもって通知と代えさせていただきます。

本件に関しまして、ご不安な点やご不明な点がございましたら、以下のお問い合わせ窓口までご連絡いただきますようお願い申し上げます。

＜不正アクセスに関するお問い合わせ先（東京損保鑑定）＞
電話番号：0120-853-851
受付時間：月曜～金曜 9:00～17:00（土日・祝日を除く）

【東京損保鑑定ニュースリリース】
2024 年 10 月　7 日：https://www.to-son.co.jp/news/25858
2024 年 12 月 25 日：https://www.to-son.co.jp/news/27875

＜上記以外の全般的なお問い合わせ先（SOMPO企業保険金サポート）＞
電話番号：0120-336-215
受付時間：月曜～金曜 9:00～17:00（土日・祝日を除く）

関係者の皆様にご迷惑、および、ご心配をおかけする事態となりましたこと、改めて深くお詫び申し上げます。

以上

ご参考

東京損保鑑定社で発生したランサムウェア被害について

1. 概要

2024 年 8 月 29 日、東京損保鑑定社において、社内サーバーにアクセスできない状態であることが判明し、サーバー保守業者にサーバーの確認を依頼したところ、暗号化されていることが確認されました。

そのため、東京損保鑑定社はサーバー保守業者とセキュリティ専門会社に調査を依頼し、被害拡大防止措置、原因調査及び復旧対応に着手いたしました。

その後の調査により、9 月2日、サーバーに、要求に応じなければダークウェブ(※)に情報を公開する旨の攻撃者のメッセージが記載されたファイルが置かれていたことを発見いたしました。

もっとも、現在に至るまで、情報の公開や新たな攻撃活動等の被害は生じておりません。また、東京損保鑑定社は、不正アクセスの攻撃者とは一切接触しておりません。

2. 原因

セキュリティ専門会社の調査によると、本件の原因は、UTM機器(※)へのブルートフォース攻撃(※)後に、東京損保鑑定社内のサーバーにRDP 接続(※)によって侵入され、ランサムウェア(※)の実行によりファイルの暗号化及びドライブの暗号化が施されたことによるものと考えられます。

本件調査により、攻撃者によるファイル転送ツールによる情報の送出や東京損保鑑定社のクラウドストレージへのアクセスは確認できませんが、同社サーバーの複数のローカルフォルダへの不正なアクセスが確認されたことや、本件事象のあった時間帯に係るログが削除された可能性があることから、本件事象のあった時間帯において、攻撃者が情報を外部へ送出した可能性を完全に否定することはできないものと考えております。

3. 対策および再発防止策

使用していたパソコンやシステム、ネットワーク環境の入れ替えを行いました。UTM は多要素認証(※)を導入したうえでアクセス制限を設けました。EDR(※)やクラウドのセキュリティ対策の導入、不正通信対策など、セキュリティ専門業者のアドバイスを受けてセキュリティ強化策を講じており、あわせて、個人情報の管理体制の見直しを進めています。

また、東京損保鑑定社では警察のサイバー犯罪相談窓口に被害相談を行うとともに、被害届を提出しております。

(※)用語の解説

用語	解説
ダークウェブ	個人情報やソフトウェアの脆弱性が取引されるサイト
UTM機器	複数のセキュリティ機能を一つの機器で運用管理し、包括的に社内ネットワークを保護する製品
ブルートフォース攻撃	パスワードを破るためのサイバー攻撃手法。 パスワードに使われると推測される数字や文字列をすべて試し、正解を割り出します
RDP 接続	画面の表示内容を遠隔のコンピュータに転送するリモートデスクトップを実現するための通信規約
ランサムウェア	データを不正に暗号化し、復元と引き換えに身代金を要求する悪質なマルウェア
多要素認証	認証の 3 要素である「知識情報」、「所持情報」、「生体情報」のうち、2 つ以上を組み合わせて認証することを指します
EDR	ユーザーが利用する PC やサーバー(エンドポイント)への脅威に対応するセキュリティソリューション