

当社ファイルサーバーのランサムウェア感染による

情報流出の可能性についてお知らせとお詫び(第二報)※12/20更新

(2022年12月20日追記)

12月20日付で本件に関するお問い合わせ専用電話窓口の提供を終了しました。お電話でのお問い合わせは、「2. 本件に関するお問い合わせ窓口」に記載の代表電話までお問い合わせください。

株式会社UPDATER(所在地:東京都世田谷区、代表取締役:大石英司)が管理運用するファイルサーバーがランサムウェアに感染した事案につきまして、お客さま、お取引先さま、関係者の皆さまに多大なご心配とご迷惑をおかけしておりますことを、深くお詫び申し上げます。

外部の専門機関と連携して調査を継続しており、今後新たな情報が判明する可能性があります。9月22日にご案内した第一報※に続きまして、現時点で確認できている状況をお知らせします。

なお、本件による電力供給への影響はございません。

※9月22日公表 当社ファイルサーバーのランサムウェア感染による情報流出の可能性についてお知らせとお詫び(9/26 FAQ追記) <https://minden.co.jp/news/2022/09/22/7395>

1. 外部流出した可能性のある情報

第一報でお知らせしました情報の対象範囲、また新たに外部流出した可能性を確認した情報は以下のとおりです。

■対象範囲を確認した情報

(1) 個人顧客情報

対象期間: 2016年4月～2022年9月18日までに当社とご契約いただいた個人顧客

内 容:

- ・ 氏名、住所、電話番号、メールアドレス、契約内容
- ・ 「みんな電力」の電気料金を口座引き落としにてお支払いされている顧客の口座情報

※クレジットカード情報は当社にて保有しておりませんので、流出のおそれはありません。またマイページのパスワードにつきましても流出のおそれはありません。

(2) 法人顧客情報

対象期間: 2016年4月～2022年9月18日までに当社とご契約もしくはご契約を検討いただいた法人

内 容:

- ・ 法人名、担当者氏名、住所、電話番号、メールアドレス、契約内容、工事実施等に係る施設関連書類
- ・ 「みんな電力」の電気料金を口座引き落としにてお支払いされている顧客の口座情報

※クレジットカード情報は当社にて保有しておりませんので、流出のおそれはありません。また法人向けマイページのパスワードにつきましても流出のおそれはありません。

(3) 発電事業者および取引先情報

対象期間: 2015年1月～2022年9月18日までに当社とお取引した事業者

内 容: 法人名、担当者氏名、住所、電話番号、メールアドレス、契約・取引内容、口座情報

(4) 業務受託先の個人顧客情報・法人顧客情報

対象期間: 2017年4月～2022年9月18日に当社が業務受託した法人の顧客

内 容: 氏名・法人名、住所、電話番号、メールアドレス、口座情報、契約内容

(5) 株主情報

対象期間: 2011年5月～2022年9月18日に出資いただいた株主

内 容: 氏名、住所、電話番号、メールアドレス、保有株数、契約内容

(6) 退職者含む従業員情報

対象期間: 2011年5月～2022年9月18日に在籍した従業員

内 容: 氏名、住所、電話番号、メールアドレス、生年月日、経歴・資格関連情報、所属部署、給与データ、年金・社会保険関連データ、従業員持株会情報、社内レポート

■新たに外部流出の可能性を確認した情報

(7) 業務委託先の従業員個人情報

対象期間: 2019年12月～2022年9月18日に当社が業務委託をした方

内 容: 氏名、所属、社員番号、契約内容

(8) 当社主催イベント参加者

対象期間: 2018年4月～2022年9月18日開催したイベントの参加者

内 容: 氏名、所属、メールアドレス、電話番号

(9) 新卒採用応募者

対象期間: 2020年2月～2020年4月にエントリーいただいた新卒採用応募者

内 容: 履歴書、選考レポート

(10) キャンペーン応募・資料請求者の個人情報 ※10月17日 16:20追記

対象期間: 2019年12月～2022年9月18日にキャンペーン応募・資料請求をいただいた方

内 容: 氏名、住所、電話番号、メールアドレス

2. 本件に関するお問い合わせ窓口 (2022年12月20日更新)

<TEL> 03-6805-2228(代表) 受付時間: 平日11:00～15:00

<MAIL> privacy@minden.co.jp

3. 対象となる皆さまへのお願い

対象となるお客さま、お取引先さま、関係者の皆さまにおかれましては、以下のような不正利用にご注意くださいますようお願い申し上げます。

■想定される不正利用

- ・ メールアドレスを悪用したフィッシングメール詐欺(クレジットカード会社、金融機関、ECサイトなど実在する企業になりすまし、お客さまのカード情報を聞き出すなど)
- ・ 電話番号を悪用した勧誘電話や詐欺電話、フィッシングサイトに誘導するSMS
- ・ 個人情報悪用したなりすましによる第三者への詐欺

■ご注意いただきたいこと

- ・ 差出人や件名に心当たりのないメールを受信した際は開封や添付ファイル・URLのクリックはせず、直ちに削除をお願いいたします。
- ・ 登録していない知らない電話番号からの着信には出ないようお願いいたします。

<ご参考>

日本クレジット協会： フィッシング詐欺被害にあわないための注意事項

https://www.j-credit.or.jp/customer/attention/attention_02.html

個人情報保護委員会： なりすましメールによるウイルス感染被害への注意喚起

https://www.ppc.go.jp/news/careful_information/impersonation/

■不正利用による被害を受けた可能性がある場合

警察または消費者生活センターまでご相談ください。

- ・ 警察相談専用電話 TEL： #9110（地域を管轄する警察本部などの窓口につながります）
- ・ 消費生活センター消費者ホットライン TEL： 188

合わせて、当社での状況把握のため、2. に記載の当社窓口にもご連絡いただけますと幸いです。

4. 今後の当社対応

このたびのランサムウェア感染の原因や経路などにつきましては、外部専門機関の協力を得ながら引き続き調査を進め、詳細が分かり次第、すみやかにご報告します。また、当社はこのたびの事態を厳粛に受け止め、セキュリティー体制の厳格化や監視体制の強化を図り、再発防止に取り組んでいきます。

このたびはお客さま、お取引先さま、関係者の皆さまに多大なご心配とご迷惑をおかけしますことを、重ねて深くお詫び申し上げます。

以上