

TBS アクト及び TBS テックスを退職した方々へのお知らせ

## 労働社会保険手続き業務委託先における、ランサムウェア感染についての報告

2023年7月7日

TBS アクト・コーポレート本部

この度、アクトが労働社会保険手続き業務を委託している「OURS 小磯社会保険労務士法人」（以下、「社労士法人」という）より、同社労士法人が利用しているクラウド型社会保険システム「社労夢」（以下、「本システム」という）のサービスを提供するベンダー（株式会社エムケイシステム）のサーバーがランサムウェアによる不正アクセスを受けた旨の連絡を受けました。

現時点で個人情報漏えいの事実は確認されていませんが、今後、漏えいの恐れがあることから、個人情報保護法第 26 条第 2 項に基づき、対象となる可能性のある皆様にご連絡させていただきます。皆様におかれましては、特に以下の「6. ご留意いただきたい事項」を確認いただき、念のため不審な連絡や訪問者等にご注意いただきますようお願い申し上げます。

皆様にご迷惑とご心配をおかけしますこと、お詫び申し上げます。

### 1. 概要

社会保険業務を委託している「社労士法人」より、同法人が利用している株式会社エムケイシステムのサーバーが、ランサムウェアによる不正アクセスを受けた旨、通知されました。問い合わせの結果、アクト業務の一部についても、「本システム」を利用していたことがわかりました。現時点で第三者への情報漏えいの事実は確認されていませんが、今後の漏えいの恐れは否定できない状況にあります。

### 2. 対象者

- ・ 2021年4月 TBS アクト発足時に TBS アクトに在籍していた方
- ・ 2021年4月～2023年5月に育児休業給付を受けた方
- ・ TBS テックスに在籍していた方

### 3. 漏えいする恐れのある個人情報の項目

労働・社会保険手続きに関する個人情報（氏名、生年月日、性別、住所、電話番号、メールアドレス、入退社年月日、給与額、基礎年金番号、雇用保険番号、各種社会保険の加入年月日、各種社会保険の喪失年月日、扶養家族の情報等）

#### 4. 漏えいの恐れが生じた原因

株式会社エムケイシステムのサーバーに対するランサムウェアによる第三者からの不正アクセス

#### 5. 二次被害の有無

現時点で情報漏えいの事実は確認されておりません。

#### 6. ご留意いただきたい事項

現時点においては、情報漏えいの事実は確認されていませんが、念のため、不審な連絡や訪問者等にはご注意ください。漏えいしていた場合に予想される二次被害としては「架空請求やセールス等の電話」「架空請求の郵便等の送付」等が考えられます。

以下の点に特にご留意いただきますようお願い申し上げます。

- ・不審なメールや電話が届いた場合は、開封や返信をせずに速やかに削除するか無視する。
- ・個人情報や口座情報などを求めるメールや電話には応じない。
- ・インターネットバンキングやクレジットカードなどの利用明細を定期的を確認し、異常があれば速やかに金融機関やカード会社に連絡する。

ご留意いただきたい事項に該当する事態が発生した際は、会社（問い合わせ窓口）までご一報ください。

#### 7. 問い合わせ窓口

コーポレート本部労政部 03-6230-8208

[ta-rousei@gr.tbsact.co.jp](mailto:ta-rousei@gr.tbsact.co.jp)

以上