2022 年 3 月 7 日

（お知らせ）

NTT ビジネスソリューションズ株式会社

マルウェア感染による情報流出に関するお詫び、
ならびに本件に伴い流出したデータを用いた不審メールに関する注意喚起について

この度、NTT 西日本が愛知県公立大学法人様から受託している業務に使用しているパソコンがマルウェア（Emotet）に感染し、過去のメール送受信情報として保存されていた当社社員、愛知県公立大学法人教職員様、及び本受託業務に関するお取引先様等のメールアドレス等が流出し、これらを装った第三者からの不審なメールが発信されている事実を確認いたしました。

業務委託元である愛知県公立大学法人様、及びお取引先様等、また、上記の不審なメールを受信された皆様には、大変なご迷惑、ご心配をおかけしていることを深くお詫び致します。

現在、上記以外の影響の有無について引き続き調査するとともに、二次的被害や拡散の防止に努めております。

メールに記載された送信者をご存じであっても、不審なメールを受信された場合は、添付されたファイルやメール文中に記載の URL は開かずに、そのまま削除していただきますよう、宜しくお願い致します。

なお、当社サービス等への影響は発生しておりません。

【注意喚起】　当社にて確認した不審なメールの一例

下記以外にも類似したパターンで発信されている可能性があり、十分にご注意ください。

差出人：当社社員名、または本受託業務に関係される方々の氏名
（ただしメールアドレスは攻撃者のメールアドレス）

件名　：　RE:　当社社員名、または本受託業務に関係される方々の氏名

添付ファイル：　xxxxxxxxxx.xlsm（Excel ファイルが圧縮され zip ファイルとして添付されているケースも確認されています）

メール本文の一例：

- ・当社社員名、または本受託業務に関係される方々の氏名が入っている
- ・　「ご確認をおねがいします」、「宜しく御願い致します」といった文章が記載されている

１．これまでの経緯と対応

３月１日（火）　本受託業務に従事する担当者が、不審メールに添付されたファイルのマクロを実行

※この時点で当該パソコン端末がマルウェア（Emotet）に感染したと考えられる

３月２日（水）
- 当社社員等を装った不審なメールが、本受託業務に関わりのある複数の方へ発信されていることを確認
- 当該パソコンをネットワークから切り離しのうえ、二次的被害防止策を実行
- メールアドレスが流出した可能性のある方々に、お詫びと不審なメールに対する注意喚起のメール送付等を実施
- パソコン端末の解析、ネットワーク機器のログ確認等を実施

※3 月 3 日以降も以上の対応を継続して実施中

２．流出したと考えられる情報

当該パソコンにて、本受託業務に関連して過去のメール送受信情報として保存されていた方々のメールアドレス等（件数については確認中です）

現在、上記以外のデータについても引き続き調査中です。

３．二次的被害拡大防止に向けた取り組み

業務委託元のネットワークシステムへの技術的な対応及びメールアドレスが流出した可能性のある方々に、お詫びと不審なメールに対する注意喚起のメール送付等を実施

４．再発防止策

今後同様の事象が発生しないよう、引き続き基本動作の徹底を図り、情報セキュリティに関する教育の再徹底等を図ってまいります。

以　上