

## 長期休暇に向けたサイバーセキュリティ対策の実施について

### 前略

株式会社テクノステートは、経済産業省・総務省・警察庁・内閣サイバーセキュリティセンターが掲載した、[「夏季の長期休暇において実施いただきたい対策について（注意喚起）」](#)（令和4年8月8日）を受け、Emotet ウイルス蔓延が収束しない現状に鑑み、サイバーセキュリティ対策を以下のとおりご報告します。

### 1 背景

上記、「夏季の長期休暇において実施いただきたい対策について（注意喚起）」（令和4年8月8日付 経済産業省・総務省・警察庁・内閣サイバーセキュリティセンター）のとおり、夏季休暇によって

- ・「休暇中の隙を突いたセキュリティインシデント発生の懸念」
- ・「長期休暇後に電子メールの確認の量が増えることで偽装のチェックなどがおろそかになるといった感染リスクの高まり」

上記のセキュリティ・リスクが懸念されます。

### 2 対応事項

#### （1）夏期休暇取得前

- ・ Windows OS の最新セキュリティパッチ適用
- ・ 常時接続を要しない従業員用 PC は、長期休暇取得前日に LAN ケーブルを抜く。

#### （2）連休明け後

- ・ 不審メール開封に注意し、当社が取り組んでいる、JPCERT/CC 提供「[Emocheck Ver.2.3.2](#)」による感染チェックおよびウイルス対策ソフトによるウイルススキャン後の業務実施の徹底。

#### （3）その他

セキュリティインシデント発生を認識した際の、情報セキュリティ担当への連絡および対応の実施。

以上、ご報告します。