

経営バイタル
の強化書 KEIEI VITAL

▶ 長期休暇前後のセキュリティ対策

長期休暇に向けてセキュリティの再確認を



既に夏季休暇を取得された方が多いと思いますが、これからシルバーウィークや年末年始、ゴールデンウィークなど1年を通して断続的に長期休暇があります。

このような長期休暇前後にはセキュリティ事故が発生する可能性が高くなります。有名企業や宅配便を装ったフィッシング詐欺も相変わらず増加しています。

経済産業省、総務省、警察庁、内閣官房内閣サイバーセキュリティセンターは令和4年8月8日に共同で注意喚起を行い、実施すべき対策のリストを公開しました。

長期休暇前後はセキュリティインシデントが発生しやすい時期。
ではどのような対策が有効か、具体的なセキュリティ対策をご紹介します。

1 長期休暇前後のセキュリティ対策の必要性

経済産業省、総務省、警察庁、内閣官房内閣サイバーセキュリティセンターは令和4年8月8日に共同で注意喚起を行い、実施すべき対策のリストを公開しました※1。

サイバー攻撃被害のリスクの高まりを踏まえ、今年4月には総務省、警察庁、内閣官房内閣サイバーセキュリティセンターの連名にて「春の大型連休に向けて実施いただきたい対策について（注意喚起）」等の注意喚起が行われましたが、その後も、ランサムウェアによるサイバー攻撃被害が国内外の様々な企業・団体等で続いています。また、エモテットと呼ばれるマルウェアへの感染を狙う攻撃メールについては、知り合いのメールアドレスをそのまま使い正規のメールであると信じ込ませたり、業務上の正規のメールの返信を装ったりするなど巧妙化が進み、国内の企業・団体等へ広く感染の被害が広がっていると考えられます。

都内の税理士事務所や日本税理士会連合会事務局を騙ったエモテットによる攻撃メールもありました。

今年6月には、ウェブブラウザに保存されたクレジットカード情報を窃取する機能も確認され、今後、攻撃の多様化、悪質化による被害の深刻化のおそれがあります。さらに、ブロードバンドルータ、無線LANルータ、監視カメラ用機器類、コピー機をはじめとするネットワークに接続された機器・装置類がマルウェアに感染したことに起因する攻撃通信が、引き続き増加傾向にあります。また、脆弱性が公表されてから悪用されるまでの時間が短くなっているとの報告もあります。

今年7月にフィッシング対策協議会に寄せられたフィッシング報告件数（海外含む）は、前月より19,698件増加し、107,948件と

なっています※2。

このように依然として厳しい情勢の下での長期休暇においては、休暇中の隙を突いたセキュリティインシデント発生への懸念が高まるとともに、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が予想されます。さらに、長期休暇中は、通常と異なる体制等により、対応に遅延が生じたり、予期しない事象が生じたりすることが懸念されます。

長期休暇前後のセキュリティ対策を再確認し、セキュリティ事故に備えましょう。

2 長期休暇期間前のセキュリティ対策

長期休暇に際しては、休暇前と休暇明けの対策を行うことが必要となります。長期休暇前には下記の対策を実施しましょう。

① 長期休暇期間中のセキュリティインシデント発生時の対処手順及び連絡体制の確認

- 長期休暇期間中ではセキュリティインシデントをリアルタイムで認知しづらく対応が遅れがちとなります。そのため、セキュリティインシデントに即応できるよう長期休暇期間中の監視体制を確認し、必要に応じ、システムアラート、各種ログ等の監視体制を強化しましょう。
- セキュリティインシデントを認知した際に迅速かつ円滑に対応することができるよう、セキュリティインシデントを認知した際の対処手順（事業継続計画等）の内容を再度確認しましょう。
- セキュリティインシデントを認知した際における連絡体制（情報セキュリティインシデントを認知した際における対応等の決定

権者及び担当者等の連絡先、連絡が取れなかった場合の予備の連絡先)が最新の情報に更新されていることを確認しましょう。

- システムベンダ(保守業者を含む)、回線業者、外部サービス提供者、データセンタ事業者等のサポート窓口の営業状況、連絡先(夜間・休日等の通常営業時間帯以外の連絡先を含む。)等を確認しましょう。
- 情報システムを利用する職員等に対して、セキュリティインシデントを認知した場合の報告窓口を周知しておきましょう。

② 利用機器・外部サービスに関する対策

- 外部からの不正アクセスを防止する観点から、機器(サーバ、パソコン等、通信回線装置、特定用途機器(防犯カメラなど)等)のファームウェアを最新のものにアップデートしましょう。また、長期休暇期間中に使用しない機器の電源は落としておき、機器に自動起動機能を設定している場合には、長期休暇期間中の設定の要否を検討しておきましょう。
- この機会に使用しない外部サービスの無効化の要否を検討しましょう。

③ ソフトウェアに関する脆弱性対策の実施

- 脆弱性対策の状況を確認し、必要に応じてセキュリティパッチの適用やソフトウェアのバージョンアップを行うとともに、直ちに実施することが困難な場合はリスク緩和策を講じておきましょう。
- 休暇期間中に公表された重要な脆弱性情報について遅滞なく確認し、対応の検討が行われる体制としておきましょう。
- セキュリティパッチの適用やソフトウェアのバージョンアップについて、やむを得ず長期休暇期間前に実施できない場合、長期休暇期間明け直後は業務システムへのアクセス集中が予想されることから、事前に実施時期のスケジュールを検討しておきましょう。

④ バックアップ対策の実施

- システムの不具合やランサムウェア等の不正プログラムによるデータ破壊に備えて、重要なデータや機器設定ファイルに対するバックアップ対策を実施するとともに、最新のバックアップが確実に取得されていること、バックアップデータから実際に復旧できることを確認しておきましょう。また、バックアップデータはネットワークから切り離し、変更不可とするなどの対策を検討しておきましょう。

⑤ アクセス制御に関する対策

- この機会にアクセス権限の確認、多要素認証の利用、不要なアカウントの削除等により、本人認証を強化するとともに、個々の利用者にパスワードが単純でないか確認させておきましょう。
- インターネット等外部ネットワークからアクセス可能な機器については、外部からの管理機能、ポート(例えば、ファイル共有サービス等によく利用される137(TCP/UDP)、138(UDP)、139(TCP)、445(TCP/UDP)、リモートデスクトップ等で利用される3389(TCP)など)、プロトコルを必要なものに限定するなど、不要なポートやプロトコルを外部に開放していないか確認しておきましょう。

⑥ 職員等への注意喚起の実施

- 情報システムを利用する職員等に対して、後述する〈情報システムを利用する職員等における実施事項〉を含む長期休暇期間に伴うサイバーセキュリティ確保の観点から留意すべき事項について、注意喚起を実施しましょう。

3 長期休暇期間明けのセキュリティ対策

長期休暇明けには下記の対策を実施しましょう。

① サーバ等における各種ログの確認

- サーバ等の機器に対する不審なアクセスが発生していないか、VPN、ファイアーウォール、監視装置等ログやアラートで確認しましょう。もし何らかの不審なログが記録されていた場合は、早急に詳細な調査等の対応を行いましょう。

② ソフトウェアに関する脆弱性対策の実施

- 長期休暇期間中における脆弱性情報を確認し、必要に応じてセキュリティパッチの適用やソフトウェアのバージョンアップを行うとともに、直ちに実施することが困難な場合はリスク緩和策を講じましょう。

③ 不正プログラム感染の確認

- 長期休暇期間中に持ち出しが行われていたパソコン等に、不正プログラムに感染していないか、不正プログラム対策ソフトウェア等で確認を行いましょう。

④ 長期休暇期間中に電源を落としていた機器に関する対策

- 長期休暇期間中に電源を落としていた機器は、不正プログラム対策ソフトウェア等の定義ファイルが最新の状態となっていないおそれがあることから、端末起動後、最初に不正プログラム対策ソフトウェア等の定義ファイルを確認し、最新の状態になっていない場合は更新作業を実施してから、利用を開始しましょう。

4 情報システムを利用する職員等における実施事項

長期休暇期間前の対策

【利用機器に関する対策】

- 外部からの不正アクセスを防止する観点から、長期休暇期間中に使用しない機器の電源を落とすこと。

【機器やデータの持ち出しルールの確認と遵守】

- 長期休暇期間中に端末や外部記録媒体等の持ち出し等が必要な場合には、組織内の安全基準等に則った適切な対応(持ち出し・持ち込みに関する内規の遵守等)を徹底すること。
- 許可を得て持ち出した機器の不正プログラム感染や、紛失、盗難による情報漏えい等の被害が発生しないように管理すること。

長期休暇期間明けの対策

- 電子メールの確認を行う前に、利用機器のOSおよびアプリケーションに対する修正プログラムの適用や不正プログラム対策ソフトウェア等の定義ファイルの更新等を実施すること。
- 電子メールの確認を行う際は、不審な添付ファイルを開いたり、リンク先にアクセスしたりしないこと。



※1 経産省「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)」(URL: <https://www.meti.go.jp/press/2022/08/20220808003/20220808003.html>)
 ※2 フィッシング対策協議会 月次報告書「2022/07 フィッシング報告状況」(URL: <https://www.antiphishing.jp/report/monthly/202207.html>)