令和４年８月８日
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

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）

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、関係府省庁の連名にて「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）」等の注意喚起を発出しましたが、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。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。

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。

こうした長期休暇がサイバーセキュリティに与えるリスクを考慮し、別紙の対策を参考に、適切な管理策によるサイバーセキュリティの確保についてご検討をお願いいたします。

あわせて、不審な動き等を検知した場合は、早期対処のために速やかに所管省庁、セキュリティ関係機関に対してご連絡いただくとともに、警察にもご相談ください。

【参考】

＜これまでの注意喚起＞

○４月 25 日　経済産業省、総務省、警察庁、NISC「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）」

https://www.nisc.go.jp/pdf/press/20220425NISC_press.pdf

〇６月 15 日　NISC「我が国の公的機関や企業等の偽サイトにご注意ください（注意喚起）」
https://www.nisc.go.jp/pdf/press/20220615NISC_press.pdf

〇８月３日　IPA「夏休みにおける情報セキュリティに関する注意喚起」
https://www.ipa.go.jp/security/topics/alert20220803.html?s=09

＜ランサムウェア対策＞
〇ストップ！ ランサムウェア　ランサムウェア特設ページ　STOP! RANSOMWARE
https://security-portal.nisc.go.jp/stopransomware/

〇ランサムウェア対策特設ページ（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html

〇侵入型ランサムウェア攻撃を受けたら読む FAQ（一般社団法人 JPCERT コーディネーションセンター）
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

〇ランサムウエア対策特設サイト（一般社団法人 JPCERT コーディネーションセンター）
https://www.jpcert.or.jp/magazine/security/nomore-ransom.html

〇ランサムウェア被害防止対策（警察庁サイバー犯罪対策プロジェクト）
https://www.npa.go.jp/cyber/ransom/index.html

＜エモテット＞
〇「Emotet の解析結果について」（警察庁@police）
https://www.npa.go.jp/cyberpolice/important/2020/202012111.html

〇「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/announce/20191202.html

〇マルウェア Emotet の感染再拡大に関する注意喚起（一般社団法人 JPCERT コーディネーションセンター）
https://www.jpcert.or.jp/at/2022/at220006.html

（別紙）

長期休暇期間に向けて実施いただきたい対策について（注意喚起）

セキュリティ対策の実施に関する責任者及び情報システムを利用する職員等に実施いただきたい対策を下記のとおりまとめました。

記

＜セキュリティ対策の実施に関する責任者における実施事項＞

１．長期休暇期間前の対策

【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る。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すること。

□　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）の内容を再度確認すること。

□　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すること。

□　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。）等を確認すること。

□　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すること。

【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すること。また、長期休暇期間中に使用しない機器の電源を落とすこと。また、機器に自動起動機能を設定している場合は、長期休暇期間中の設定の要否を検討すること。

□　この機に使用しない外部サービスの無効化の要否を検討すること。

【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ずること。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、対応の検討が行われる体制としておくこと。

□　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すること。

【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すること。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すること。

【アクセス制御に関する対策】

□　この機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ること。

□　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すること。

【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、注意喚起を実施すること。

２．長期休暇期間明けの対策

【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すること。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うこと。

【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ずること。

【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うこと。

【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、利用を開始すること。

＜情報システムを利用する職員等における実施事項＞

１．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。

２．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。

以　上