令和４年 12 月 20 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

年末年始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、本年８月には、関係府省庁の連名にて「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）」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・団体等で続き、国民生活に影響が出る事例も発生しました。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、本年１１月に活動再開とその新たな手口（【参考】内※１，２，３を参照）を確認しており、感染や被害の拡大が懸念される状況にあります。

さらに、本年９月には、日本の政府機関や企業のホームページ等を標的としたDDoS攻撃と思われるサービス不能攻撃により、業務継続に影響のある事案も発生したほか、国家等が背景にあると考えられる攻撃者による暗号資産取引事業者等を狙ったサイバー攻撃や、一定の集団によるものとみられる学術関係者等を標的としたサイバー攻撃も明らかとなり、国民の誰もがサイバー攻撃の懸念に直面することとなっています。

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、サプライチェーンも含め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＞

〇８月８日　経済産業省、総務省、警察庁、NISC「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）」

https://www.nisc.go.jp/pdf/press/20220808NISC_press.pdf

〇10 月 14 日　金融庁、警察庁、NISC「北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）」
https://www.nisc.go.jp/pdf/press/20221014NISC_press.pdf

〇11 月 30 日　警察庁、NISC「学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）」
https://www.nisc.go.jp/pdf/press/20221130NISC_press.pdf

〇12 月 13 日　IPA「年末年始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/alert20221213.html

＜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「マルウェア Emotet の活動再開に関する注意喚起について」（警察庁）（※１）
https://www.npa.go.jp/cybersecurity/pdf/20221104press.pdf

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）（※２）

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）（※３）
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やサプライチェーン企業の営業状況、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。

【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へのアクセスは必要なものに限定し、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）及びプロトコルを不必要に開放していないことを確認すること。

【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。

【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。

【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

【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。

【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が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。

【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。

＜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

【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。

【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。

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

長期休暇に向けて、セキュリティ対策は万全ですか？

セキュリティ対策責任者・システム担当者向け

休暇前

対処手順・連絡体制

重要

- 長期休暇期間中の監視体制を確認する。
- 必要に応じ、システムアラート等の監視体制を強化する。
- セキュリティインシデントの対処手順を確認し、連絡体制を更新する。

長期休暇期間中に認知したインシデントの対応が休暇明けとなり、被害が拡大した事例も！

休暇前

バックアップ

重要

- 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。
- 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。

ランサムウェア攻撃により、大切なバックアップも暗号化されてしまう被害が出ています！

休暇前

アクセス制御

- 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。
- 利用者にパスワードが単純でないか確認させる。
- 外部ネットワークからアクセス可能な機器へのアクセスは必要なものに限定する。

休暇前

ソフトウェアの脆弱性対策

- 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。
- 長期休暇期間中に公表された重要な脆弱性情報に対応するための体制を整える。

休暇前

利用機器に関する対策

- 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にアップデートする。
- 長期休暇期間中に使用しない機器の電源を落とす。

休暇後

電源を落としていた機器に関する対応

- 長期休暇期間中に電源を落としていた機器は、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する。
- 最新の状態になっていない場合は、更新してから、利用を開始する。

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になっていないおそれがあります。

休暇後

ソフトウェアの脆弱性対策

- 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。
- 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る。

休暇後

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が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する。

休暇後

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。
- 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を行う。

情報システム利用職員向け

休暇前

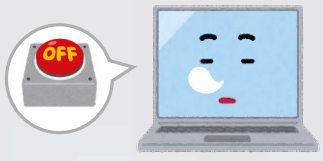
機器やデータの持ち出しルールの確認と遵守

- 端末や外部記録媒体等の持ち出しは、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。
- 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。

休暇前

利用機器に関する対策

- 不正アクセスを防止するため、長期休暇期間中に使用しない機器の電源を落とす。



休暇後

電子メール

- 電子メールを確認する前に、利用機器のOS・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。
- 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。
- 不審な点があれば、電子メールを開封する前に、電話等、別の手段で確認する。

実在組織や知人を騙ったメールのやり取りを通じ、正式の書類を装ったマルウエアをダウンロードさせ、情報を盗み取るサイバー攻撃が発生！

経済産業省 Ministry of Economy, Trade and Industry

総務省 Ministry of Internal Affairs and Communications

警察庁 National Police Agency

NISC

相談窓口

■警察庁サイバー警察局 都道府県警察本部のサイバー犯罪相談窓口
https://www.npa.go.jp/cyber/soudan.html
具体的な被害の相談については、最寄りの警察署又は都道府県警察本部のサイバー犯罪相談窓口にお問い合わせください。

■内閣サイバーセキュリティセンター
nisc_soudanmadoguchi@cyber.go.jp