令和４年４月２５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

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）

昨今においてはサイバー攻撃被害のリスクが高まっており、こうした情勢を踏まえ、今年３月には、関係府省庁の連名にて「現下の情勢を踏まえたサイバーセキュリティ対策の強化について（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うなどにより知り合いからのメールであると信じ込ませたり、本文が業務上開封してしまいそうな正規のメールの返信を装うなど巧妙化が進み、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。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、増加傾向にあります。

このように依然として厳しい情勢の下での春の大型連休においては、連休の間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、連休明け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、大型連休中は、通常と異なる体制等により、予期しない事象が生じることが懸念されます。

こうした春の大型連休における長期休暇期間がサイバーセキュリティに与えるリスクに鑑み、政府機関や重要インフラ事業者をはじめとする各企業・団体等は、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、別紙の対策を講じるようお願いいたします。

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連絡していただくとともに、警察にもご相談ください。

【参考】

＜これまでの注意喚起＞

〇２月 23 日　経済産業省「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）」

https://www.meti.go.jp/press/2021/02/20220221003/20220221003-1.pdf

〇３月１日　経済産業省、金融庁、総務省、厚生労働省、国土交通省、警察庁、ＮＩＳＣ「サイバーセキュリティ対策の強化について（注意喚起）」
https://www.nisc.go.jp/pdf/press/20220301NISC_press.pdf

〇3 月 24 日　経済産業省、総務省、警察庁、NISC「現下の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）」
https://www.nisc.go.jp/pdf/press/20220324NISC_press.pdf

＜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

＜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

＜外国の動向＞

○４月 20 日　米・豪・加・新・英のサイバーセキュリティ機関による共同アドバイザリ「基幹インフラに対するロシア政府のサイバー脅威に関するアドバイザリ」等（英文）

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

<https://www.cisa.gov/uscert/ncas/current-activity/2022/04/20/russian-state-sponsored-and-criminal-cyber-threats-critical>

<https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf>

（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を認知した際の対処手順及び連絡体制の確認】

□　セキュリティインシデントに即応できるよう、システムアラート、各種ログ等を監視する体制を確認し、必要に応じ、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（サーバ装置、端末、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。

□　長期休暇期間中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。

【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を確認し、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。

【アクセス制御に関する対策】

□　パスワードが単純でないかの確認、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)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（VPN、ファイアーウォール、監視装置等）に対する不審なアクセスが発生していないか、発生したアラートや各種ログを確認すること。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、セキュリティソフト等でウイルススキャンを行うこと。

【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