事務所ニュース News
2025.2
K-066
発行：税理士法人グッドパートナーズ

経営バイタルの強化書 KEIEI VITAL

長期休暇前後や日常的に行うべき情報セキュリティ対策について

年末年始における情報セキュリティに関する注意喚起

年末年始などの長期休暇の前後には、日常の利用とは異なる環境でのパソコン等の利用や長期間利用していない状態からの利用等情報セキュリティ対策上注意することがあります。
e-TaxやeLTAXの更新、税務会計システム等の更新等もありますので、必要な情報のバックアップを含め、情報セキュリティ対策を確認しておきましょう。

繁忙期の前に情報セキュリティ対策を確認しておきましょう。

1 年末年始における情報セキュリティに関する注意喚起

独立行政法人情報処理推進機構（IPA）は12月17日に「年末年始における情報セキュリティに関する注意喚起」を行い、IPAが公開している長期休暇における情報セキュリティ対策、日常における情報セキュリティ対策の案内を行いました※1。

長期休暇の時期は、システム管理者が長期間不在になる等、いつもとは違う状況になりがちです。

このような状況でセキュリティインシデントが発生した場合は、対応に遅れが生じたり、想定していなかった事象へと発展したりすることにより、思わぬ被害が発生したり、長期休暇後の業務継続に影響が及ぶ可能性があります。

また、資金提供や投資勧誘、不正送金、個人情報を聞き出す不審な電話等も増加しており、警視庁、金融庁、国民生活センター等からも注意喚起が行われています。

年末調整や所得税の確定申告等繁忙期に入る前に長期休暇における情報セキュリティ対策、日常における情報セキュリティ対策を再度確認し、円滑な業務運営に備えましょう。

2 長期休暇における情報セキュリティ対策

長期休暇前の対策には、企業・組織における**①緊急連絡体制の確認**、**②社内ネットワークへの機器接続ルールの確認と遵守**、**③使用しない機器の電源OFF**があり、利用者向けには、**①機器やデータの持ち出しルールの確認と遵守**、**②使用しない機器の電源OFF**があります。また、利用者向けには長期休暇中の対策として、持ち出した機器やデータの厳重な管理を行うことが求められます。

長期休暇明けの対策には、企業・組織における**①修正プログラムの適用**、**②定義ファイルの更新**、**③サーバ等における各種ログの確認**があり、利用者向けには、**①修正プログラムの適用**、**②定義ファイルの更新**、**③持ち出した機器等のウイルスチェック**、**④不審なメールに注意**が求められます。

①修正プログラムの適用は、長期休暇中にOS（オペレーティングシステム）や各種ソフトウェアの修正プログラムが公開されている場合があるため、修正プログラムの有無を確認し、必要な修正プログラムを適用することが求められます（年初には、e-TaxやeLTAXの更新等もあります）。

②定義ファイルの更新は、長期休暇中に電源を切っていたパソコンは、セキュリティソフトの定義ファイル（パターンファイル）が古い状態のままになっているため、電子メールの送受信やウェブサイトの閲覧等を行う前に定義ファイルを更新し、最新の状態にすることが求められます。

利用者向けには、さらに、長期休暇中に持ち出していたパソコンや、データを保存していたUSBメモリ等の外部記憶媒体にウイルスが混入していないか、組織内で利用する前にセキュリティソフトでウイルススキャンを行うこと（**③持ち出した機器等のウイルスチェック**）や長期休暇明けはメールが溜まっていることが想定されますので、特に注意してメールチェックを行うことが求められます（**④不審なメールに注意**）。

不審なメールを受信していた場合、「添付ファイルは開かず」、「本文中のURLにはアクセスせず」、各組織のシステム管理者に報告し、指示に従うことが必要となります。

また、ウェブサイトの閲覧中に、ウイルスに感染している、パソコンが壊れる等の偽の警告に遭遇する場合があります。表示されたメッセージに従って、操作したり、電話をかけて遠隔操作を許してしまったりすると、最終的に有償ソフトウェアの購

裏面へ続く→

入や有償サポート契約へ誘導されます。

利用しているセキュリティソフトによる警告ではない場合、特にインターネット利用中にブラウザ画面上に表示される警告は偽物である可能性が高いと考えられます。あらかじめ、利用しているセキュリティソフトのマニュアルやヘルプで、脅威が検知された場合の本物の警告画面を確認しておくことが必要です。

もし、偽の警告画面が表示された場合は、画面を閉じてください。画面が消せない場合は、ブラウザを強制終了するか、パソコンを再起動してください。

パソコンの動作が通常と異なる場合には、管理者に相談し、不審なメールや詐欺メール等が流行していないかを警察庁サイバー警察局の新着情報※2やIPAの重要なセキュリティ情報※3等を確認し、必要に応じて対応について相談を行うとよいでしょう。

3 日常における情報セキュリティ対策

長期休暇における対策は、日常的に行っている対策が行われていない場合の対策となりますが、情報セキュリティ対策は、日常的に行っていくことが最も重要です。情報セキュリティ対策を疎かにしてしまうと、ウイルスに感染してシステムに問題が発生したり、不正アクセスによって情報が流出したりといった被害が発生する可能性があります。年末調整や所得税確定申告等では、個人情報や特定個人情報、要配慮個人情報を多く扱うことになり、国税関係書類の提出における電子化やデータ連携が進んでいますので、繁忙期の前に、以下の対策を確認・実施しておくことが求められます。

日常的に行う情報セキュリティ対策は、企業・組織における**①修正プログラムの適用**、**②セキュリティソフトの導入および定義ファイルの最新化**、**③定期的なバックアップの実施**、**④パスワードの適切な設定と管理**、**⑤不要なサービスやアカウントの停止または削除**、**⑥情報持ち出しルールの徹底**、**⑦社内ネットワークへの機器接続ルールの徹底**が必要となり、利用者向けにはさらに、**⑧USBメモリ等の外部接続媒体の取り扱いの注意**、**⑨パソコン等の画面ロック機能の設定にも留意**することが必要です。

①修正プログラムの適用とは、管理するサーバやパソコン等のOS（オペレーティングシステム）、各種ソフトウェアに修正プログラムを適用して最新のバージョンに更新し、ルータやスイッチ等は最新のファームウェアに更新して維持することです。

②セキュリティソフトの導入および定義ファイルの最新化とは、管理するサーバやパソコン、スマートフォン等にセキュリティソフトを導入するとともに、セキュリティソフトの定義ファイル（パターンファイル）が常に最新の状態になるように設定し、最新の状態になっているか定期的に確認することです。

③定期的なバックアップの実施とは、システムの不具合やランサムウェア等のウイルスによるデータ破壊に備えて、定期的に外部記憶媒体等へバックアップを行うことです。重要なデータのバックアップは「321ルール」を適用するようにしてください。321ルールとは、データを3つ持ち（運用データ1つ、バックアップデータ2つ）、2種類の異なる媒体でバックアップし、そのうち1つは異なる場所（オフサイト）で保管する、という理想的なバックアップの方法とされています。

④パスワードの適切な設定と管理とは、システム管理等で使用するパスワードは可能な範囲で複雑な長い文字列を設定することで、大小英字、数字および記号を混在させて、最低でも10文字にすることが必要です。他のシステムやインターネットサービスで同じパスワードを使い回したり、デバイスやシステムのパスワードについて初期設定のまま利用することは避け、確実に初期パスワードを変更することが必要です。

退職者や新規雇用者のパスワード管理（退職者のパスワードをそのまま利用せず、新規雇用者には新たなパスワードを発行する等）についても留意してください。

⑤不要なサービスやアカウントの停止または削除とは、外部から接続できるサーバで稼働している不要なサービスや、管理する機器やシステムに存在する不要なユーザアカウントを停止または削除することです。不要なサービス等を適切に管理することで、外部からの攻撃に対するリスクを低減することができます。

⑥情報持ち出しルールの徹底とは、業務用パソコン等の機器やデータを組織外に持ち出す場合のルールを明確にし、関係者に周知徹底することです。設定したルールに則り適切に運用されているかについて定期に確認することも重要です。ルールの例としては、関係者に機器を貸し出しする際は、機器内に不必要なデータが保存されていないか事前に確認する、紛失した場合に備えて、持ち出す機器やUSBメモリ等の外部記憶媒体には適切な暗号化を施す、等があります。

⑦社内ネットワークへの機器接続ルールの徹底とは、ウイルス感染したパソコンや外部媒体等を社内ネットワークに接続することで、ウイルスをネットワーク内に拡散してしまうリスクを低減するために行うものです。普段は社内ネットワークに接続していないパソコン等の機器を社内ネットワークに接続する場合のルールを明確にし、関係者に周知徹底し、接続する機器の脆弱性対策やウイルスチェックなどが適切に実施されているかを確認してください。利用者は、USBメモリ等の外部接続媒体の取り扱いに十分注意すること（**⑧USBメモリ等の外部接続媒体の取り扱いの注意**）が求められます。また、外部でパソコン等を利用する場合には、第三者に見られたり、操作されたりしないようパソコンやスマートフォン等には画面ロックを設定し（**⑨パソコン等の画面ロック機能の設定にも留意**）、スマートフォンは放置しないように注意することが必要です。

INFORMATION SECURITY MEASURES

※1 2024年度 年末年始における情報セキュリティに関する注意喚起（IPA）（URL：https://www.ipa.go.jp/security/anshin/heads-up/alert20241217.html）
※2 サイバー警察局 新着情報（警察庁）（URL：https://www.npa.go.jp/bureau/cyber/index.html）
※3 重要なセキュリティ情報（IPA）（URL：https://www.ipa.go.jp/security/security-alert/index.html）