Ksisnetだより

発行:Ksisnet事務局
平成30年12月18日
Vol.58

重要連絡

年末年始休暇時の情報セキュリティ対策について

長期休暇の時期は、「システム管理者が長期不在になる」等いつもとは違う状況になりやすく、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れたり、SNS上での思わぬ風評被害が発生したり、場合によっては関係者に対して被害が及ぶ可能性があります。

このような事態とならないよう、以下の対策を実施してください。

システム管理者向け対策

【長期休暇前の対策】

1　緊急連絡体制の確認

不測の事態が発生した場合に備えて、委託先企業を含めた緊急連絡体制や対応手順等が明確になっているか確認してください。

- 連絡体制の確認（連絡フローが現在の組織体制に沿っているか等）
- 連絡先の確認（各担当者の電話番号が変わっていないか等）

2　使用しない機器の電源OFF

長期休暇中に使用しないサーバ等の電源をOFFにしてください。

電源OFF

【長期休暇明けの対策】

1　修正プログラムの適用

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ります。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してください。

2　定義ファイルの更新

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ます。利用者に使用させる前に定義ファイルを更新し最新の状態にしてください。

3　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、各種ログを確認してください。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ってください。

CAUTION **巧妙に細工したメールのやり取りにより企業の担当者を騙し、攻撃者（犯人）の用意した口座へ送金させる「ビジネスメール詐欺（BEC）」について、国内では継続して攻撃が確認されています。**

2018年の夏には「日本語のビジネスメール詐欺」が確認され、本物の代表の名前とメールアドレスが使われるという手の込んだものでした。今後「日本語のビジネスメール詐欺」の増加が予想されることから、社内での情報共有とチェック体制の再確認を徹底し、被害に遭わないようにしてください。

利用者向け対策

【長期休暇前の対策】

1　機器やデータの持ち出しルールの確認と遵守

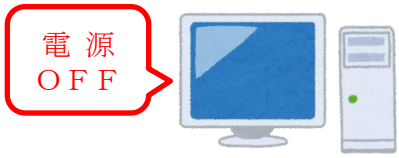
長期休暇に社外での対応が必要となるなどパソコン等の機器やデータ等の情報を持ち出す場合は、持ち出しルールを事前に確認し遵守してください。

2　社内ネットワークへの機器接続ルールの確認と遵守

ウイルス感染したパソコンや外部記憶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おそれがあります。長期休暇中にメンテナンス作業などで社内ネットワークへ機器を接続する予定がある場合は、社内の機器接続ルールを事前に確認し遵守してください。

3　使用しない機器の電源OFF

長期休暇中に使用しない機器は電源をOFFにしてください。



【長期休暇中の対策】

1　持ち出し機器やデータの厳重な管理

自宅等に持ち出したパソコン等の機器やデータは、ウイルス感染や紛失、盗難等によって情報漏えい等の被害が発生しないよう、厳重に管理してください。

【長期休暇明けの対策】

1　修正プログラムの適用

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ります。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してください。なお、修正プログラムの適用については、システム管理者の指示に従ってください。

2　定義ファイルの更新

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ます。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、最新の状態になっていることを確認してください。

3　持ち出し機器のウイルスチェック

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感染していないか、組織内で利用する前にセキュリティソフトでウイルスチェックを行ってください。

4　実在の企業などを騙ったばらまき型メールに注意

実在の企業などを騙った不審なメールに関する相談が多く寄せられています。こういったメールの添付ファイルを開いたり、本文中のＵＲＬにアクセスしてダウンロードしたファイルを開いたりすることでウイルスに感染してしまう可能性があります。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、誤って不審なメールの添付ファイルを開いたり、本文中のＵＲＬにアクセスしたりしないように注意してください。不審なメールを受信していた場合は各組織のシステム管理者に報告し、指示に従ってください。

参考　ＩＰＡ（情報処理推進機構）