

2020年8月

各位

情報科学センター長

連休期間中の情報セキュリティに関する注意喚起

長期連休を控え、以下の事項についてご参考にしていただき、休暇期間前後における情報セキュリティインシデント発生の防止等について、ご留意くださるようお願いいたします。

●情報セキュリティに関する情報提供サイト

独立行政法人情報処理推進機構 (IPA) の情報提供サイトです。長期休暇における情報セキュリティ対策について掲載されております。

IPA <https://www.ipa.go.jp/security/measures/vacation.html>

●休暇期間前の対応

1. 業務で使用するパソコン等の OS やソフトウェア等に最新のセキュリティ更新プログラムが適用されていることを確認願います。
2. 容易に推測できる文字列(名前、生年月日、電話番号及びアカウントと同一 の文字列)、安易な文字列(12345、asdfg 及び qwerty 等)をパスワードに設定していないことを確認願います。
3. 業務で使用する Web サービスで使用している ID やパスワードを他の Web サービスでも使い回していないか確認願います。使い回している場合にはパスワードを変更願います。
4. パソコン、USB メモリ等の外部記録媒体については、適正に管理をお願いします。
5. ウイルス対策ソフトに最新のパターンファイルを適用してフルスキャンを実施して、不正なプログラム等がインストールされていないか確認願います。
6. 休暇期間に使用しないパソコンやプリンタ、ネットワークストレージ等は 電源を落としてください。

●休暇期間後の対応

1. 休暇期間にセキュリティ更新プログラムが公開されていた場合は、更新プログラムを適用願います。
2. 出勤後直ちに、業務で使用するパソコンのウイルス対策ソフトを最新のパターンファイルに更新した後、フルスキャンを行ってください。
3. 休暇期間に持ち出したパソコン、USB メモリ等の外部記録媒体は、使用する前に必ずウイルス対策ソフトでフルスキャンを行った後に使用するとともに、不要なデータは速やかに削除してください。
4. 休暇期間に受信したメールに不審なメールが含まれている可能性があるため、添付ファイルは安易に開封しない、メール本文に記載された URL リンクも不用意にクリックしないようにしてください。
5. 万一、不審なメールの添付ファイルを開封、あるいは URL リンクをクリックしてしまった場合は、速やかにパソコンに接続されているネットワークケーブルを切り離してください。

以上