



連休前後のセキュリティ対策はできていますか？

8月に入り、子供たちは夏休みに入って2週間ほどとなりましたが、もうすぐお盆ということで、長期休暇に入る職場も多いと思います。
長い休みに入る場合、セキュリティ上注意すべき点がいくつかあります。

<長期休暇前の対策>

○ 休暇中の対応手順の確認を

偽メールなど、担当者への連絡が取りにくい長期休暇を狙われる可能性があります。休暇中でも、インシデントが発生した場合に備え、それぞれの立場での対応手順を確認しておきましょう。

○ 定期的なバックアップ取得を

パソコンの盗難や紛失、故障、マルウェア感染などに伴うデータ消失に備えるため、日頃からバックアップを取り、職場で指定された場所に保管しておきましょう。

<長期休暇明けの対策>

○ OSやソフトを最新の状態に更新を

OSやソフトの開発元から更新プログラムが提供されたら、早期に適用しましょう。脆弱性を狙われてしまう可能性があります。休暇明けは、最初にOSやソフトの更新情報がないかチェックし、最新の状態にしておきましょう。
(職場によって更新プログラム適用のタイミングは異なりますので、職場のルールに従ってください)

○ メールのチェックは慎重に

情報システム部門の担当者や職場の責任者をかたって、更新を呼びかけたり、電話をかけさせたりするようなものは、偽物かもしれません。

また、長期休暇明けは、大量のメール処理を行わなければならないため、チェックがおろそかになる可能性があります。

メールの真偽が不明なまま、添付ファイルや記載されたリンクを開いてはいけません。



長崎県警察本部サイバー犯罪対策課
095-820-0110 (3451・3452)
メール e103107@police.pref.nagasaki.jp

サイバー犯罪対策課
公式LINEアカウントで
情報配信中！
友だち登録をお願いします！

@387ojopi

