滋賀県警察サイバーセキュリティ情報
サイバーコネクトSHIG@
R５年度 No.１４
今、注目のサイバーセキュリティに関する情報をお届けします。

年末年始のセキュリティ対策万全ですか？

年末年始などの長期休暇後は、インシデント事案の発生件数が増加する傾向にあります。
年末年始の社内体制については縮小される事業所が多い傾向にありますが、これは、情報システム関連部署やセキュリティ対策チームも同じです。通常時は、何か異常があってもすぐに対応して被害の拡大を防げますが、休暇期間中の体制では、特異なふるまいを検知しても対応が遅れたり、見過ごされてしまうため、インシデント事案が発生する可能性が高くなります。
そうした各企業のセキュリティ上の「隙」を突くために、サイバー攻撃者は、計画的に攻撃を実行していると考えられており、長期休暇期間中は、サイバー攻撃集団に狙われやすい時期と言えます。
長期休暇期間中に考えられるリスクを予測して事前に対策を打ち、自社のセキュリティを万全にして新年を迎えられるように準備をお願いします。

長期休暇前の対策（主なもの）

- ○　長期休暇期間中のシステム監視体制を確認する。
- ○　休暇中の緊急連絡体制や対処体制を確立する。
- ○　協力会社や子会社にも、長期休暇期間中におけるセキュリティ体制の強化を要請する。
- ○　重要なデータのバックアップ対策を実施する。
- ○　システムの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アプリのバージョンアップを実施する。
- ○　外部ネットワークからの不正アクセスを防止するため、長期休暇中に使用しない機器は、電源を落としたり、ネットワークから切り離しておく。
- ○　ＰＣや外部記録媒体の持ち出しは、各事業所の内規を遵守する。（一般利用者の遵守事項）

長期休暇明けの対策（主なもの）

- ○　不審なアクセスの有無を確認するため、ＶＰＮやファイアウォール、監視装置等のログを確認する。
- ○　長期休暇期間中に電源を落としていた機器やネットワークから切り離していた機器は、起動後、ウイルス対策ソフトを最新版にしてから運用する。
- ○　長期休暇期間中に持ち出されていたＰＣ等は、まず、ウイルス対策ソフト等でウイルスチェックを行う。
- ○　休暇中の持ち出し機器の紛失・盗難について確認しておく。
- ○　休暇中に届いた電子メールをチェックする際は、内容に注意を払い、不用意に添付ファイルを開いたり、ＵＲＬリンクをクリックしないようにする。（一般利用者の遵守事項）

長期休暇　サイバー攻撃　休みなし

長期休暇後にサイバーインシデント事案を認知された場合は、
当県警サイバー犯罪対策課へ御相談ください！

«CS情報SHIG@»　偽ショッピングサイトに注意！

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）　詳細は県警webページで　→