



春の大型連休に向けたセキュリティ対策について



連休の間隙を突いて攻撃を仕掛けてくる可能性が非常に高いです
しっかりと各種対策をしましょう

連休前の対策

利用機器の状態や万が一の備えについて確認



最新状態に更新

利用機器のファームウェア等を
最新の状態に更新しましょう



脆弱性情報の確認

脆弱性情報を確認して、**必要があれば**
修正パッチ等の適用をしましょう



バックアップファイルの作成

万が一に備えて**バックアップ**
ファイルを作成しましょう

連休期間中にサイバー攻撃等が発生した場合の対処手順や連絡体制の確認



対処手順の確認



連絡体制の確認

確実な対処が被害拡大防止に有効です

連休明けの対策

サーバ等における各種ログの確認



サーバ等の機器に**不審な通信等のログ**が記録されていないか確認をしましょう
不審なログが記録されていた場合は、
早急に対処してください

マルウェア感染の確認



機器を使用する前に**マルウェア等**に感染していないかを確認しましょう

※連休明けも利用機器のファームウェア等が最新状態になっているかを確認しましょう



受信メールを確認するときは、いつも以上に慎重に

連休明けには、未開封のメールがたくさんあることが想定されます

たくさんあるからといって確認作業を怠ってしまうと、マルウェア感染などのリスクが高まります

マルウェア「Emotet」で新しい手口が確認されました



これまでは、Word・Excel・PDFファイルのマクロ機能を実行することで感染していました
「ショートカットファイル (lnkファイル)」を実行することで感染する手口が確認されました
※パスワード付きZIPファイルの中にショートカットファイルが含まれていることもあります



これまで



新しい手口

Word・Excel・PDFファイルだけでなく、
ショートカットファイルにも注意しましょう