サイバー攻撃対策通信
（令和7年第4号）

令和7年４月22日

福岡県警察本部

大型連休における情報セキュリティ対策

大型連休期間は、連休中の隙を突いたセキュリティインシデント発生の懸念が高まるとともに、通常と異なる体制等により、対応に遅延が発生し、**ウイルス感染や不正アクセス等の被害が発生**する可能性が高くなります。

また、先日、Fortinet社が既知の脆弱性を悪用した新たな攻撃手法について公開しており、新たな脆弱性が公開されてから約５日後に悪用されていると注意喚起を行っております。

このような被害の発生を防止するためにも、**大型連休の前後に以下の対策を実施**しましょう。

連休前

■ **システム管理者・担当者**

- □ 不測の事態に備え、委託先企業を含めた緊急連絡体制、対応手順の確認
- □ メンテナンス等の予定がある場合、連休前に組織内ネットワークへの機器接続ルールを確認
- □ 連休中に使用しないサーバ等の機器は電源をＯＦＦ

■ **社員、職員など（組織内ユーザー）**

- □ ＰＣ等の機器や情報を持ち出す場合、持ち出しルールを確認
- □ 連休中に使用しない機器は電源をＯＦＦ

連休後

■ **システム管理者・担当者**

- □ 連休中に公開された修正プログラムの確認、適用
- □ ウイルス対策ソフトの定義ファイルの確認、更新
- □ サーバ等に対する不審なアクセスがないか、各種ログの確認、調査を実施

■ **社員、職員など（組織内ユーザー）**

- □ 連休中に公開された修正プログラムの確認
- □ システム管理者の指示を受け適用
- □ ウイルス対策ソフトの定義ファイルの確認、更新
- □ 組織内ネットワーク接続前に持ち出したＰＣ等のウイルスチェックを実施
- □ 心当たりのないメールの添付ファイルは開かず、本文のＵＲＬに接続しない
- □ 休暇中に受信したメールのチェックに注意

脆弱性情報

【概要】

- **攻撃者はFortiGateデバイスの既知の脆弱性を悪用**
  - **既知の脆弱性でシンボリックリンクを作成して読み取り専用アクセスを実装**
  - **脆弱性に対処したFortiOSバージョンに更新しても、このリンクファイルが残されている可能性があり、ファイルへの読み取り専用アクセスが維持される**

【対策】

- **最新バージョンへアップグレード（シンボリックリンクの検出を実装）**
- **パッチ適用まで「SSL-VPN機能」の無効可**

【最新FortiOSバージョン】

7.6.2、 7.4.7、 7.2.11、 7.0.17、 6.4.16

【参考】 **IPA** https://www.ipa.go.jp/security/anshin/heads-up/alert20250421.html
Fortinet https://www.Fortinet.com/blog/psirt-blogs/analysis-of-threat-actor-actibity

福岡県警察サイバー攻撃対策隊　　電話番号：092-641-4141（内線：5986）