



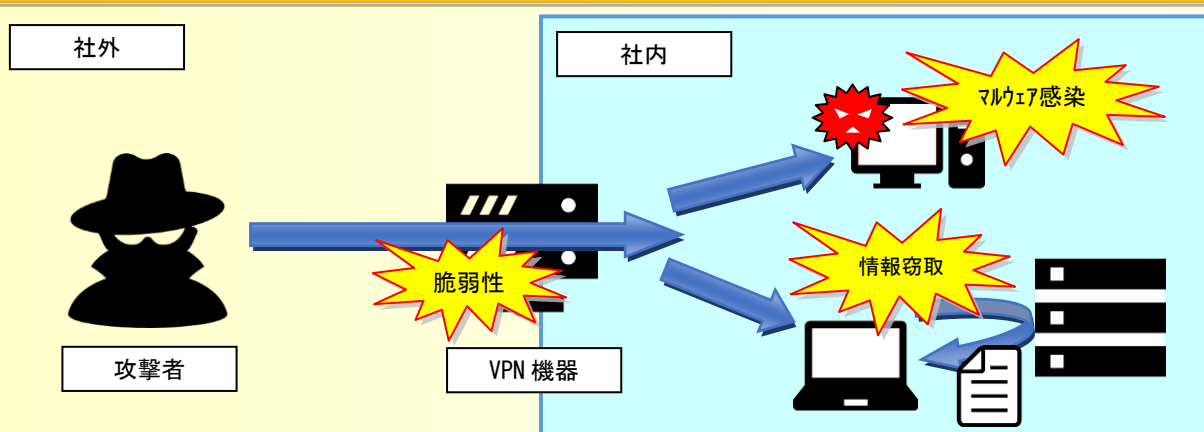
# サイバーセキュリティの置き薬

2020年  
第31号

## VPN機器を狙ったサイバー攻撃に注意!

昨今のテレワークの普及拡大に伴って、社外から社内ネットワークに接続するためにVPN環境の導入が拡大しています。

**VPN機器に脆弱性があると、社内ネットワークに不正侵入され、マルウェア感染や情報窃取の被害に遭う恐れがあります。**



複数のVPN機器メーカーで脆弱性が確認されています。  
脆弱性のあるVPN機器のIPアドレス等がリスト化され、インターネット上で公開されており、悪用されることが懸念されます。

自社で利用するVPN機器の脆弱性の有無を確認して、対処してください。

### 【確認されている脆弱性】

- 認証情報が漏えいする脆弱性
- ユーザーのパスワードが変更可能となる脆弱性
- 認証後に任意のコード実行が可能となる恐れのある脆弱性

### 【対策と対応】

- VPN製品を脆弱性に対応したバージョンに更新する。
- VPN接続のユーザアカウントのパスワードを変更する。
- VPN接続に多要素認証を導入する。
- ユーザアカウントやログに不審な点がないか確認する。

### 【参考】

- JPCERT/CC CyberNewsFlash「Fortinet社製FortiOSのSSL VPN機能の脆弱性(CVE-2018-13379)の影響を受けるホストに関する情報の公開について」(11月27日)
- LACテクニカルレポート「VPN機器を狙ったサイバー攻撃が継続中!セキュリティ事故を防ぐ3つのポイントとは」(9月8日)