

2021年12月06日

お客様各位

株式会社日立ソリューションズ  
Fortinet 製品ユーザサポート

## サイバーセキュリティ被害事例の続発に伴う脆弱性情報の確認と対策のお願い

拝啓、平素は Fortinet 製品サポートをご利用下さいまして誠にありがとうございます。

昨今、医療機関でのサイバーセキュリティ被害が続いていることから、厚生労働省より Fortinet 社に注意喚起の協力要請が出されています。お客様におかれましては、下記に示しましたお願い事項をご確認いただき、脆弱性対策を今一度お願いいたします。

敬具

### 記

#### 1. 定期的な脆弱性情報の確認とバージョンアップのお願い

Fortinet 製品の脆弱性情報は、Fortinet 社 FortiGuard Labs の PSIRT Advisory(\*1) で公開されています。脆弱性情報につきましては定期的にご参照頂くとともに、ご利用の環境が脆弱性を持つ場合は、必要に応じて設定見直し、また対策済みバージョンへのバージョンアップを実施頂きますようお願いいたします。

尚、同サイト記載内容以上の情報は開示されていません。記載内容の解釈また記載内容以上の情報については、弊社サポートではお答えいたしかねます。予めご了承ください。

#### 2. Fortinet 製品の設定および警告表示に関するお願い

Fortinet 製品をご利用の際は工場出荷時の設定のままとはせず、各種マニュアルをご確認いただくとともに、お客様環境の各種セキュリティルール、ガイドライン等を遵守した構成、設定でのご利用をお願いいたします。

また、設定時、利用時に警告が表示された場合は、適切な対応をお願いいたします。

Fortinet 製品の各種マニュアルは、Fortinet 社 Docs Library(\*2)で公開されていますので、こちらをご覧ください。

#### 3. OS ファイルの入手方法

バージョンアップは、対象機器がインターネットに接続している場合は、GUI で OS のダウンロード、及びバージョンアップを行うことができます。

OS ファイルがご入用の場合は、弊社サポートからご提供しております。対象機器のシリアル番号(S/N)と共に、現在のバージョン、バージョンアップ先のバージョンをご連絡下さい。

以上

---

(\*1) Fortinet 社 FortiGuard Labs PSIRT Advisory

<https://www.fortiguard.com/psirt>

(\*2) Fortinet 社 Docs Library

<https://docs.fortinet.com/>