

各都道府県衛生主管部（局） 御中

厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室
厚生労働省政策統括官付サイバーセキュリティ担当参事官室

FortiOS に関する脆弱性情報への対応について（注意喚起）

昨今、医療機関において、ランサムウェアによるサイバー攻撃事案が発生し、電子カルテの閲覧・利用ができなくなる等により、地域の医療提供体制に影響が出る事案が複数発生しているところです。これらの事案に共通する攻撃者の侵入経路として、医療機関と外部機関（主にベンダーや取引事業者等）を接続する通信機器とそのソフトウェア（以下「ゲートウェイ装置」という。）の脆弱性を通じて行われていることが指摘されています。

特に、FortiOS については、本年 10 月に続き、12 月にも脆弱性が発見されておりますので、下記を参考にセプター等を通じて情報提供した「Fortinet 製品の深刻な脆弱性について（注意喚起）」（参考1）等へ速やかに対応するよう周知をお願いします。

記

1 ゲートウェイ装置の使用状況の確認

各医療機関のシステムを管理するベンダーに対し、セプター等から提供された脆弱性情報の対象となるソフトウェアが使用されているか、及びサポート期限が切れていないかを確認するよう依頼すること。

2 脆弱性への対応及び緩和策の実施

上記1の確認の結果、対象ソフトウェアを使用している場合には、事前にログ等を保全した上で速やかに最新のソフトウェアにバージョンアップする等の必要な対応を実施すること。

3 侵害の兆候の確認

「Fortinet 製品の深刻な脆弱性について（注意喚起）」のように、攻撃を受けた場合に記録されるログ、悪性 IP アドレス、ネットワーク機器のファイルシステム上に作成されるファイル名が示されている場合、ログ等を確認し攻撃の兆候がないか確認するこ

と。

なお、自組織内またはベンダーが確認した結果、攻撃の兆候が認められた場合は、医政局特定医薬品開発支援・医療情報担当参事官室もしくは医療機関向けセキュリティ教育支援ポータルサイト上の「インシデントかも？」を通じて報告すること。

※医療機関向けセキュリティ教育支援ポータルサイトはこちら

<https://mhlw-training.saj.or.jp/>

4 その他

その他令和4年11月10日付け事務連絡「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」（参考2）等も踏まえ、適確なサイバーセキュリティ対策を講じること。

以上

2022 年 12 月 14 日

内閣官房 内閣サイバーセキュリティセンター
重要インフラグループ**Fortinet 製品の深刻な脆弱性について（注意喚起）（第 2 報）**

2022 年 12 月 13 日（火）（日本時間）、Fortinet はアドバイザリを更新し、本脆弱性の影響を受ける対象バージョンとして、FortiOS 5 系及び 6.0 系を追加しました。また、本脆弱性の回避策として、SSL-VPN の無効化を追加しました。本第 2 報は第 1 報（2022 年 12 月 13 日付け Fortinet 製品の深刻な脆弱性について（注意喚起））の内容を含むものとなっています。

NISC において、当該製品のようなネットワーク機器の脆弱性を突く攻撃の発生を確認しています。この脆弱性が悪用され、組織内ネットワークが侵害された場合、ランサムウェア等により被害が甚大になる恐れがあるため、即時のバージョンアップを強く推奨します。また、サプライチェーン攻撃等、自組織以外の接続先から侵害を受ける可能性もあるため、この点についても、十分以上に留意してください。

1. 対象ソフトウェア

- ・ FortiOS 5.0.0 から 5.0.14、5.2.0 から 5.2.15、5.4.0 から 5.4.13、5.6.0 から 5.6.14、6.0.0 から 6.0.15、6.2.0 から 6.2.11、6.4.0 から 6.4.10、7.0.0 から 7.0.8、7.2.0 から 7.2.2
*ハードウェアサポートが継続している一部製品の場合を除き、5 系及び 6.0 系はサポート対象外のため、直ちにバージョンアップをしてください。
- ・ FortiOS-6K7K 6.0.0 から 6.0.14、6.2.0 から 6.2.11、6.4.0 から 6.4.9、7.0.0 から 7.0.7

2. 脆弱性悪用による影響等

対象ソフトウェアを使用しているネットワーク機器に対して、攻撃者による任意のコード実行等の恐れがあります。

3. 深刻度

ソフトウェアの開発元が深刻度「Critical」（5 段階中、最高）に分類する脆弱性が含まれます。

4. 悪用

開発元により脆弱性を悪用した攻撃が確認されています。

5. 対応

対象ソフトウェアを最新のバージョンに更新してください。

TLP: CLEAR 【全分野】

加えて、侵害の兆候がないか確認するとともに、監視の強化（本項目参照）等についても検討してください。

開発元が公開している侵害の兆候を以下に示します。

(1) ログ

攻撃を受けた際、次の特徴的なログが記録されます。

```
Logdesc="Application crashed" and msg="[...] application:sslvpnd, [...],  
Signal 11 received, Backtrace: [...]"
```

(2) 悪性 IP アドレス

現在のところ、ネットワーク機器から次の疑わしい IP アドレス宛での通信が確認されています。

188.34.130.40:444

103.131.189.143:30080, 30081, 30443, 20443

192.36.119.61:8443, 444

172.247.168.153:8033

(3) ファイル

現在のところ、攻撃を受けた際、対象ソフトウェアを使用しているネットワーク機器のファイルシステム上に次のファイルが作成されます。

/data/lib/libips.bak

/data/lib/libgif.so

/data/lib/libiptcp.so

/data/lib/libipudp.so

/data/lib/libjpeg.so

/var/.sslvpnconfigbk

/data/etc/wxd.conf

/flash

6. その他

SSL-VPN を無効化することで本脆弱性の影響を回避できますが、直ちにバージョンアップを行うことを強く推奨します。

参考 URL

- FortiOS – Heap-based buffer overflow in sslvpnd (Fortinet)

<https://www.fortiguard.com/psirt/FG-IR-22-398>

- FortiOS のヒープベースのバッファオーバーフローの脆弱性 (CVE-2022-42475) に関する注意喚起 (JPCERT/CC)

<https://www.jpcert.or.jp/at/2022/at220032.html>

- FortiOS SSL-VPN の脆弱性対策について (CVE-2022-42475) (IPA)

<https://www.ipa.go.jp/security/ciadr/vul/alert20221213.html>

事務連絡
令和4年11月10日

各都道府県衛生主管部（局） 御中

厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室
厚生労働省政策統括官付サイバーセキュリティ担当参事官室

医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）

今般、大阪急性期・総合医療センター（以下「センター」という。）において、ランサムウェアによるサイバー攻撃事案が発生し、電子カルテの閲覧・利用ができなくなる等により、地域の医療提供体制に影響が出ているところです。医療機関を攻撃対象とする同種攻撃は近年増加傾向にあり、その脅威は日増しに高まっています。

厚生労働省では、センターに専門家チームを派遣して、原因の調査と復旧支援を行っていますが、攻撃の侵入経路は、医療機関自身のシステムではなく、院外の調理を委託していた事業者のシステムを経由したものである可能性が高いことが判っています。

医療機関においては、保有する医療情報の安全を確保するため、「医療情報システムの安全管理に関するガイドライン」（以下「ガイドライン」という。）等に基づき、必要な対策を講じていただいているところですが、今般のセンターにおける事案も踏まえると、医療機関自身のシステムにおけるサイバーセキュリティ対策に加え、サプライチェーンとの接続状況や、取引先システムのサイバーセキュリティ対策等をも俯瞰しつつ、必要な対策を講じていくことが求められています。

こうした状況を踏まえ、管内、管下の医療機関に対し、同種のサイバー攻撃に備え、令和3年6月28日付事務連絡「医療機関を標的としたランサムウェアによるサイバー攻撃（注意喚起）」（参考）に加え、下記の対策が適切に講じられているか確認を要請するとともに、万が一、サイバー攻撃を受けた場合にも事業継続計画等により地域住民への医療提供体制に支障が出来ることのないよう注意喚起をお願いします。

また、内閣サイバーセキュリティセンターにおいて、ランサムウェア対策に関する特設サイトを作成しているのので、必要に応じてご活用下さい。

1 サプライチェーンリスク全体の確認

上記の通り、自組織のみならずサプライチェーン全体を俯瞰し、発生が予見されるリスクを医療機関等自身でコントロールできるようにする必要があることから、関係事業者のセキュリティ管理体制を確認した上で、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施する。

2 リスク低減のための措置

- パスワードを複雑なものに変更し、使い回しをしない。不要なアカウントを削除しアクセス権限を確認する。多要素認証を利用し本人認証を強化する。
- IoT 機器を含む情報資産の保有状況を把握する。
- VPN 装置を含むインターネットとの接続を制御するゲートウェイ装置の脆弱性は、攻撃に悪用される可能性があるため、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。
- 悪用が既に報告されている脆弱性については、ログの確認やパスワードの変更など、開発元が推奨する対策が全て行われていることを確認する。
- VPN 機器に対する管理インターフェースのインターネット上の適切なアクセス制限を実施する。
- メールの添付ファイルを不用意に開かない、URL を不用意にクリックしないこと。不審メールは、連絡・相談を迅速に行い組織内に周知する。

3 インシデントの早期検知

- サーバ等における各種ログを確認する。（例：大量のログイン失敗の形跡の有無）
- 通信の監視・分析やアクセスコントロールを再点検する。（例：不審なサイトへのアクセスの有無）

4 インシデント発生時の適切な対処・回復

- サイバー攻撃を受け、システムに重大な障害が発生したことを想定した事業継続計画が策定する。
- データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。
- インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、外部関係機関への連絡体制や組織内連絡体制等を準備する。
- インシデント発生時及びそのおそれがある場合には、速やかに厚生労働省等の関係機関に対し連絡する。

5 金銭の支払いに対する対応

厚生労働省としては、サイバー攻撃をしてきた者の要求に応じて金銭を支払うこ

とは、犯罪組織に対して支援を行うことと同義と認識しており、以下の観点により金銭の支払いは厳に慎むべきである。

- 金銭を支払ったからと言って、不正に抜き取られたデータの公開や販売を止めることができたり、暗号化されたデータが必ず復元されたりする保証がないこと。
- 一度、金銭を支払うと、再度、別の攻撃を受け、支払い要求を受ける可能性が増えること。

6 ランサムウェア特設ページ

<https://security-portal.nisc.go.jp/stopransomware/>

■医療機関等がサイバー攻撃を受けた場合等の厚生労働省連絡先
医政局特定医薬品開発支援・医療情報担当参事官室

TEL : 03-6812-7837

MAIL: igishitsu@mhlw.go.jp

※迷惑メール防止のため、メールアドレスの一部を変えています。

「×」を「@」に置き換えてください。