別添

【VPN 装置のセキュリティ対策に関する確認事項】

医療機関等の管理者は、自施設に設置されている VPN 装置について、以下の項目に基づき速やかに点検・対策を実施してください。

○保守管理体制及び責任分界の明確化

確認項目	解説・具体的な対応
委託先との責任分界を契約等で明確にしているか。	自院の VPN 装置等の外部接続機器に対してセキュリティアップデートを含む保守契約が結ばれているか再確認をお願いします。 医療機関側は事業者に保守されていると考えている一方で、事業者は保守対象でないと考えていること等が原因で VPN 装置等の管理・設定が適切に行われないことにより、サイバー攻撃被害に遭う事例が多発しています。 今一度、契約書や保守事業者への契約状況等を確認し、VPN 装置等の適切な管理・設定をお願いします。

○機器のサポート状況及び脆弱性対策の実施

確認項目	解説・具体的な対応
VPN 装置が EOS（サポート終了）製品となっていないか。	サポートが終了した製品（EOS: End of Support）は、新たな脆弱性が発見されても修正プログラムが提供されず、サイバー攻撃の温床となります。 速やかに現行製品への買い替え等を検討してください。 また、サポート終了直前の機器を購入したことがサイバー攻撃を受けた要因のひとつとなった事例も確認されています。 新規導入の際には EOS が迫っていないか確認をお願いします。

○アクセス制御の徹底

確認項目	解説・具体的な対応
不要なポートや SSH 等の管理機能がインターネット側に露出していないか。	管理画面や SSH ポートが外部からアクセス可能な状態は極めて危険です。設定を確認し、不要なポートは閉鎖（遮断）してください。
VPN 接続が「常時接続」のまま放置されていないか。	業務上必要な時以外は外部との接続を遮断してください。 不要な常時接続により、サイバー攻撃被害に遭った事例が確認されています。
多要素認証やアクセスコントロールが実施されているか。	記憶に頼った ID・パスワードのみの認証は使い回しや容易なパスワードが採用されるリスクが高く、サイバー攻撃の主要原因となっています。 多要素認証やクライアント証明書等によるアクセスコントロールの導入を検討してください。

（参考）

■医療機関に対するサイバーセキュリティ対策リーフレット（令和５年 10 月）

URL：https://www.mhlw.go.jp/content/10808000/001180153.pdf

■医療機関におけるサイバーセキュリティ対策チェックリスト（令和７年５月）

URL：https://www.mhlw.go.jp/content/10808000/001253950.pdf

■薬局におけるサイバーセキュリティ対策チェックリスト（令和７年５月）

URL：https://www.mhlw.go.jp/content/10808000/001490744.pdf

■医療機関等におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関等・事業者向け～（令和７年５月）

URL：https://www.mhlw.go.jp/content/10808000/001490741.pdf

■医療情報システムの安全管理に関するガイドライン　第 6.0 版（令和５年５月）

URL：https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

■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。

URL： https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html