

「医療情報システムの安全管理に関するガイドライン」に準拠していますか？

お使いのEM-Lines環境下において

ウィルス感染

や

不正侵入

などのリスクを

ホワイトリスト

の追加により軽減することができます。

ホワイトリストとは？

事前に「安全な対象・サイト」を定義したものとあり、EM-Linesでは、この「ホワイトリスト」へのアクセスのみ許可とすることで、対象外となるアプリケーションやプログラムの実行、サイトへの訪問を許可せず、外部からのサイバー攻撃を防ぐことができます。また、医療情報を扱うシステムとして、厚生労働省「医療情報システムの安全管理に関するガイドライン」で規定されるセキュリティ・ポリシーに準拠した形となります。

※ウィルス対策ソフトとの違いは、裏面を参照ください。

厚労省が公開するガイドラインでは、「医療情報システムを、内部ネットワークを通じて外部ネットワークに接続する際には、なりすまし、盗聴、改ざん、侵入及び妨害等の脅威に留意したうえで、ネットワーク、機器、サービス等を適切に選定し、監視を行うこと。（一部抜粋）※」とされています。この「セキュアな環境」で運用できていない場合には、問題発生時にガイドライン非準拠とされてしまう恐れがあります。ホワイトリストは、安全なサイトのリストのみアクセスを許可する仕組みであり、適用することで「セキュアな環境」を担保することができます。

※参考：厚生労働省「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」システム運用編 13.ネットワークに関する安全管理措置の遵守事項②より一部抜粋

リスク例

1

ウイルス感染



突然動かない



データが消える



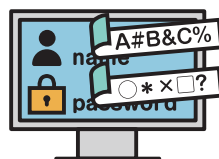
データ抜き取り

日常的に新たなマルウェアが世の中に出てきており、「ウィルス対策ソフト」を利用中の端末へ導入してもウィルスへ感染するリスクは多いにあります。EM-Linesでは、できるだけ安全にレセプトコンピューターをご利用いただくためにもホワイトリストによる対策を推奨しています。

リスク例

2

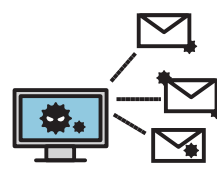
不正侵入



データ改ざん



情報漏えい



外部への自動メール
ウィルスの配布など

コロナ禍で、世の中がますますオンライン化していく中で、多数の不正アクセスが世界中で報告されており、医療機関・薬局も例外ではありません。2023年には国内の複数の病院で不正侵入による攻撃に遭い、被害を受けています。事前の対策が重要となります。

「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」に関するQ&A よりポイントを抜粋

- IPsecやTLSによる接続は、「適切な経路設定」を行うことで、セッション間の回り込み回避が可能である。
- 一般社団法人保険医療福祉情報安全管理適合性評価協会(HISPRO)公開の「レセプト・オンライン請求用チェックシート項目集」が参考となる。

<HISPRO「レセプト・オンライン請求用チェックシート項目集」より抜粋>

2.2.1 サービス拠点内のネットワークの構成

サービス拠点内においてサービス提供のためのネットワークとその他のネットワークについて分離していること

2.2.4 サービス拠点内のHigh Secure Areaを起点とした外部への接続

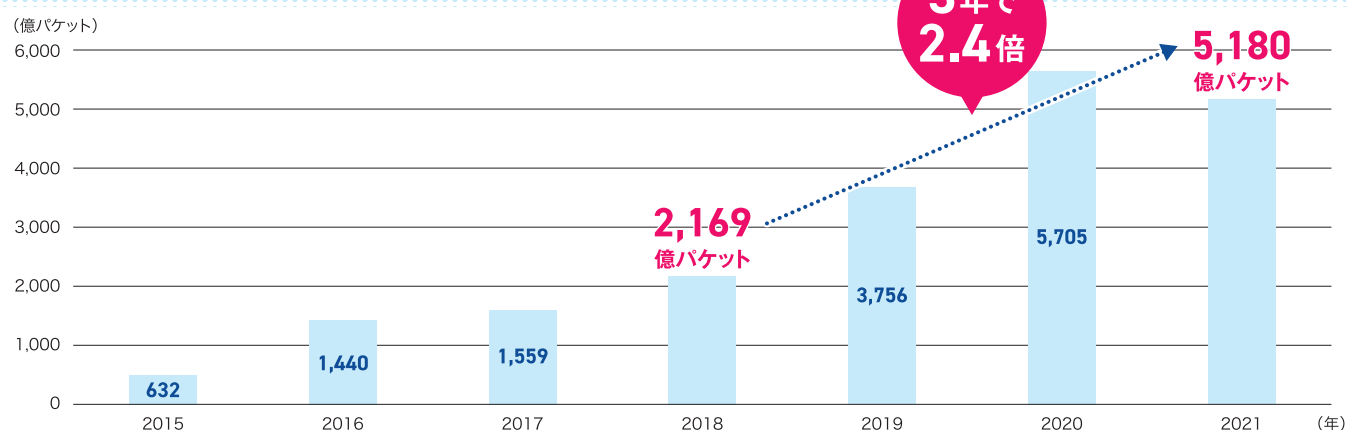
High Secure Areaからの外部に対する通信を原則禁止すること
やむを得ず通信を行う場合は、改ざんや侵入から守るため、外部への接続に対してセキュリティ機能を整備し、対策を実施すること
また、内部プロキシ等の機能を用い、アクセス元／先並びに通信内容について特定可能にしてあること

※参考：厚生労働省「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」に関するQ&A (<https://www.mhlw.go.jp/content/10808000/001102588.pdf>)

身近な環境で サイバー攻撃 が急増しています。

2021年時点でのサイバー攻撃関連通信数は、2018年と比較すると、なんと2.4倍も増加しており、今後対策を取ったとしても増加していく傾向が高いと考えられます。また、サイバー攻撃の対象としては、企業だけでなく、医療機関や薬局もターゲットとされる可能性があり、厚生省でも「医療情報システムの安全管理に関するガイドライン」の見直しが行われました。

サイバー攻撃関連の通信数の推移



※参考:総務省「令和4年度 情報通信白書」より

「ホワイトリスト」・「ブラックリスト」方式の違い

弊社では、「ホワイトリスト」・「ブラックリスト」方式を併用した環境を推奨しております。

対策方式	「ホワイトリスト」方式	「ブラックリスト」方式
概要	「安全な対象・サイトなど」(＝ホワイトリスト)のみアクセス許可する	「危険な対象・サイトなど」(＝ブラックリスト)のみアクセスNGする
メリット	新しく発生したマルウェア※などの脅威を防げる	ネットワーク上の制限は少なく、利用しやすい
デメリット	日常での運用上は制限が強い。 (検索サイト、オンラインショップ等は制限される可能性がある。)	登録しているブラックリストに無い、新しいマルウェアなどはリスクが生じる。
参考例	ホワイトリスト	一般的に利用されている「ウィルス対策ソフト」など

※マルウェア:不正・有害に動作させる意図で作成されたウィルスやワームなどの悪意のあるソフトウェアや悪質なコードのこと。

「ホワイトリスト」の適用基準

「ホワイトリスト」は、以下の項目に該当する企業、団体、機関等が運営するWebサイトのみに適応します。

- 1 病院、医師や歯科医師が常勤する医療法人、その他医療社団、医療財団。また、医療法人に情報や医療を提供する企業、薬局、社会保険、国民健康保険、製薬所、研究所といった各機関。
- 2 WindowsUpdate及びウィルス定義ファイルのDownloadといった、レセコン端末のセキュリティレベルを一定水準で維持するための情報、データを開示提供する各企業。

※業務上、接続する必要があるWebサイト等が「ホワイトリスト」に登録されていない場合には、追加での申込が可能です。ただし、審査基準により許可されない場合があります。

お求め・ご相談は信頼とサービスの行き届いた当社へ

株式会社 EMシステムズ

本社 〒532-0003 大阪府大阪市淀川区宮原 1-6-1 新大阪ブリックビル
TEL.06-6397-1888(代) FAX.06-6397-1890

東京本社 〒105-0012 東京都港区芝大門 2-10-12 KDX 芝大門ビル
TEL.03-3432-5144(代) FAX.03-3432-5145

<https://emsystems.co.jp>

TX | Thanks Transformation

医療・介護を「#ありがとう」に変えていく

●製品改良のため、仕様の一部を予告なく変更することがあります。
●会社名、商品名は各社の商標または登録商標です。



安全に関するご注意

正しく安全にお使いいただくために、ご使用前に必ず取扱説明書(マニュアル、手引書等を含む)をよくお読みください。