挿すだけ簡単
セキュリティアダプタ – SA1

ランサムウェアを強固に防御

医療機器ライフを伸ばし病院収益を大きく改善

レガシー医療機器を守る重要性

- 医療機関には、長期間にわたって使用されている機器が多数あります。これらの機器には、脆弱性が判明している旧式のOSで動作する機器が残存しています。これらの機器を踏み台として、重要なデータを保管している管理サーバが攻撃される事例が発生しています。最新のウィルス対策ソフトウェアといえども、正当な通信相手からの通信に偽造した攻撃を検出することは、非常に困難です。
- このようなレガシー機器に対するサイバーセキュリティ対策は、医療機関自身での対応が必須です。
- SA1を装着することで、レガシー機器に対しても、強固なサイバーセキュリティ対策を簡便に実施できます。SA1は、サイバーセキュリティ対応での医療機器の買い替えを不要とし、医療機器の製品としての寿命まで、医療機器の継続利用が可能となります。

SA1で築く新世代セキュリティ

レガシー医療機器機器をサイバー攻撃から強固に守る

レガシー機器にSA1を取り付けるだけで、堅牢なEPPセキュリティを実現

医療機器ライフを長期化

最新ＯＳを搭載する新型機器への買い換えが不要

医療機器購入費用を大幅に削減

遠隔治療やＡＩ画像診断など最先端ＤＸ化を推進

SA1は、インターネット越しでも利用可能

サイバーセキュリティ上の不安なく、インターネット越しの医療サービスの利用の推進が可能

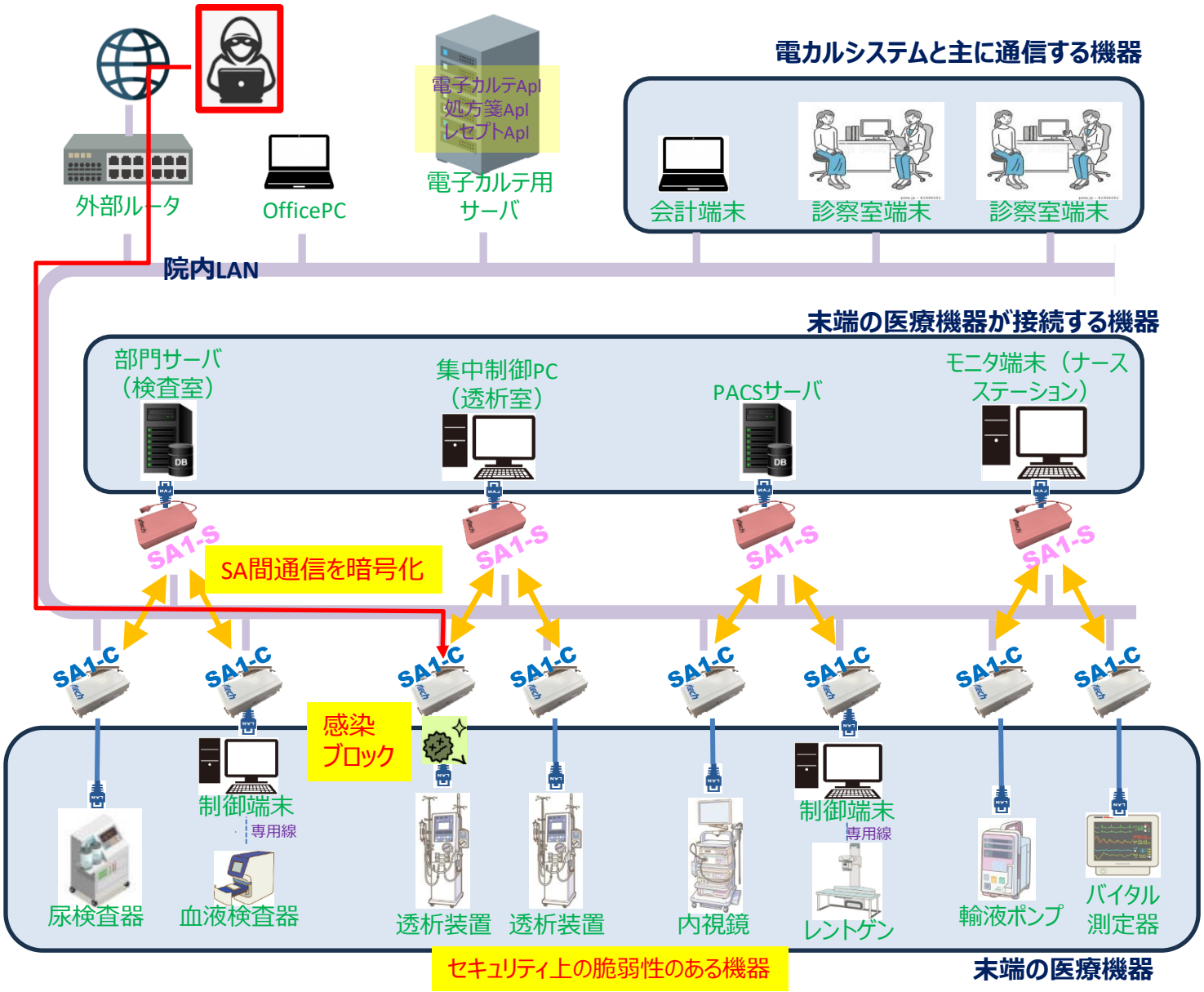
Contact Us

Verification Technology, Inc.
045-470-8310
https://vtech-inc.co.jp/

主ターゲットは末端の医療機器

末端機器とサーバ機器の通信を暗号化（VPN化）

ランサムウェアの拡大をブロック



SA1の主要なターゲットは末端の医療機器です。これらの機器は院内LANに接続しており、物理的には、医療機器間同士も通信も可能です。この特性を利用して、ランサムウェアは、院内ＬＡＮに接続している機器への侵入を繰り返し、患者情報との重要データを保持している電子カルテシステムへの侵入を行います。

しかし、末端の医療機器にとっては、医療機器の制御や取得したデータの保存やモニタを行う１つのサーバ側の機器とするだけで十分であることが一般的です。

SA1の運用では、末端の医療機器側にSA1-C（クライアントタイプ）、サーバ側にSA1-S（サーバタイプ）を接続します。これにより、SA1間の通信を暗号化し、また、本来の通信相手でない機器からのアクセスをブロックします。この機能により、機器数の多い末端の医療機器のサイバーセキュリティ感染を強力に防護できます。

Contact Us

Verification Technology, Inc.

045-470-8310

https://vtech-inc.co.jp/