【参考出展】メディカルショージャパン＆ビジネスエキスポ2018

脅威可視化ソリューション

In-Line Security Monitor HAT

「つながる」からこそ高まる「稼動停止」リスク、対策は充分ですか？

昨今、チーム医療が推進される中で、医療機器のネットワーク化は確実な伝達による患者の安全管理や業務効率改善、発生する情報の安全管理など、非常に重要で欠かせないものとなっています。しかし、その一方でそれに比例して拡大しているのが、サイバー攻撃や偶発的なウィルス感染などによる病院システムの稼動停止リスクです。これは医療安全面においても病院ビジネスにおいても大きな脅威となります。

事例報告１

画像撮影診断システム

診断画像や3D化処理した画像を研究などの目的で活用する際、汚染されたUSBメモリを使いウイルス感染。コンソール、ワークステーションから周辺のコンピューターへネットワークを通じて拡散。

侵入経路：医療者

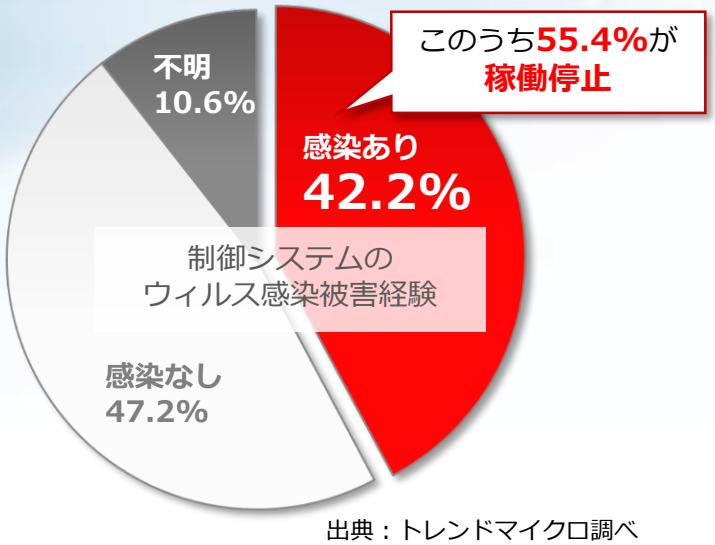
事例報告２

臨床検査システム

システムの保守作業で持ち込んだ作業端末、USBメモリを経由してWindowsベースで動作するコンソールが感染。

侵入経路：保守業者

日本の工場等における制御システムの被害実態（図1）



出典：トレンドマイクロ調べ

医療機器の稼働は止められず、プログラム更新にも慎重なバリデーションを求められるため脆弱性は残りやすくなります

病院ではネットワーク内部のサイバーリスクを前提として考慮していません

＋

医療分野においても
IoT技術を活用した医療機器など
ネットワーク接続は今後増えていきます

工場向け・病院向け セキュリティ対策のPoint

① **入口対策**
— **「情報系側に残る 脆弱性」**への対策

② **出口対策**
— **「医療情報の漏えい」**への対策

③ **内部対策**（コントロール～フィールド）
— **「内部不正の早期通知→保全」**対応

『 In-Line Security Monitor HAT』
3社共同開発！

TREND MICRO

内部対策

AlaxalA — HACHIWARA

In-Line Security Monitor HAT　システム構成

1 ホワイトリスト機能搭載スイッチ

- ■登録済端末の通信を許可し、未登録端末の通信を遮断
- ■ホワイトリストの自動学習可能

通信遮断

既存のL2スイッチと入れ替えるだけ
ホワイトリスト型セキュリティスイッチ

AlaxalA ホワイトリスト機能搭載スイッチ

2 ネットワークセンシング技術

- ■通信の振舞いを監視し、怪しい通信を発見・通知
- ■ホワイトリストで許可された端末のウイルス感染を発見

検知分析

工場(病院)ネットワーク内部のサイバーリスク可視化を実現する高度化検知センサーソリューション

TREND MICRO ネットワークセンシング技術

萩原テクノ製
HPU A100ECシリーズ

3 セキュリティ情報可視化

- ■以下の情報を現場保全員が理解可能な情報として表示
  - Ⅰ. ホワイトリスト機能搭載スイッチで検知された不正通信
  - Ⅱ. ネットワークセンシング技術で検知された脅威

可視化

脅威検知の結果を現場担当者が理解できる情報として表示する見える化ソリューション

HAGIWARA セキュリティ情報可視化

萩原テクノ製
HPU A100ECシリーズ

本ソリューションはIT化が進む製造業のFAシステム環境を主な対象として開発された製品ですが、
運用環境に共通点の多い医療機関、医療機器の分野においても応用可能なソリューションとなっています。

オプション

ウイルス発見時のウイルスチェックツール

調査保全

スタンドアロン／クローズド環境向け
ウイルス検索・駆除ツール

TREND MICRO Trend Micro Portable Security 2™

※仕様は予告なく 変更される可能性があります。

■お問い合わせ先
萩原テクノソリューションズ株式会社
システムインテグレーション事業部　IoTソリューション部
〒461-0001 名古屋市東区泉2丁目28番23号 高岳KANAMEビル
TEL ： 052-931-3624
Mail ： si-iots@hagiwara.co.jp