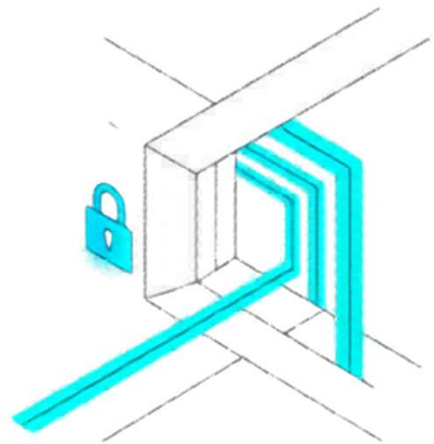
古い医療・産業機器をゼロトラスト化するSA1の不可視化テクノロジー

工場・病院におけるレガシー機器の延命とゼロトラスト化・真のDX化推進

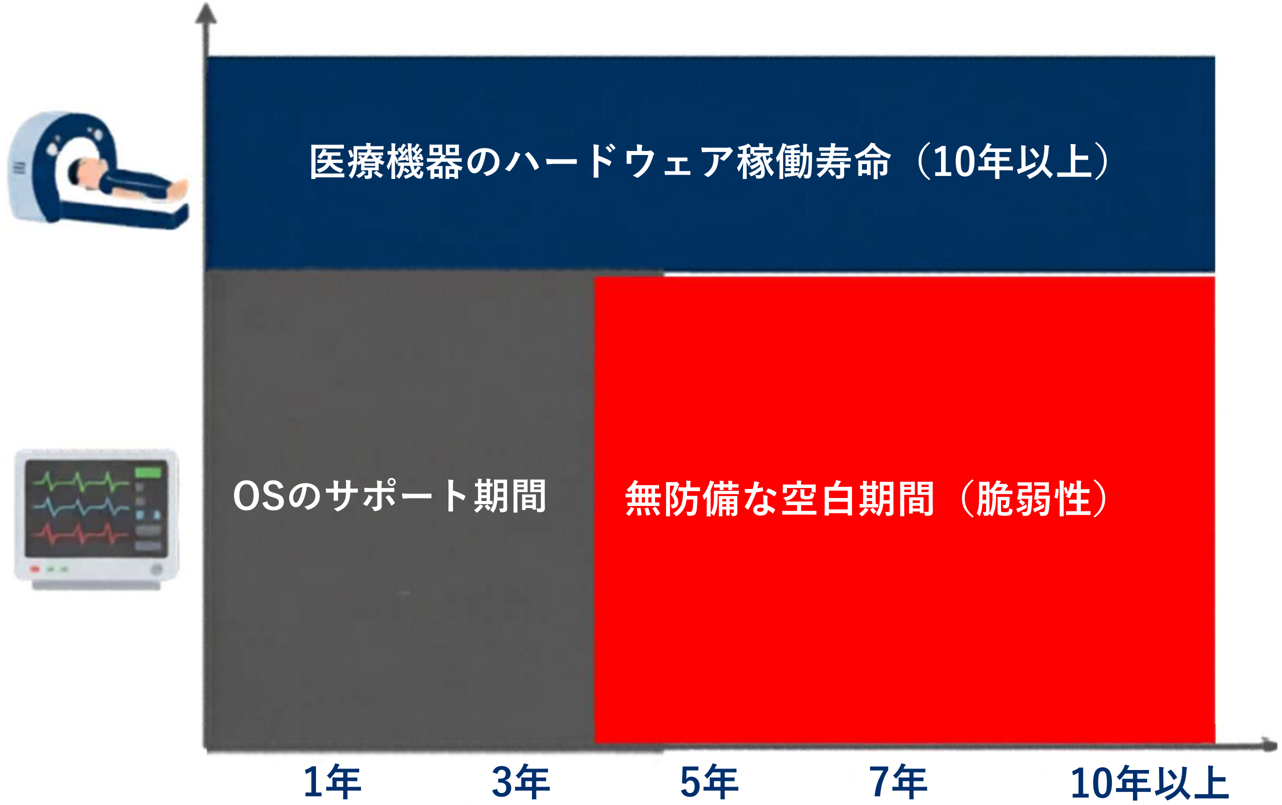


ベリフィケーションテクノロジー株式会社

工場・病院が直面するDXのジレンマと「最大の死角」

産業・医療機器は10年以上の長期稼働が前提。数年でOSのサポート切れ(EOL)を迎え、アップデートが不可能な「レガシー機器」化。

この公知の脆弱性を抱えた機器が、DX推進(遠隔医療・グローバルデータ連携)の足枷となり、ランサムウェア侵入の巨大なゲートウェイとなっている。



既存のソフトウェア対策（EDP・EDR）が抱える構造的限界

EPPの限界

パターンマッチングの死角

・古いOSにはインストール自体が不可能。
・また、内部ネットワークで正当な機器を装った「なりすましパット（偽装攻撃）」をブロックできない。

EDRの限界

過検知リスクと事後対応の代償

・EDRは脅威の「事後検知」が主であり、ランサムウェアによる暗号化が始まってから検知することも多く、レガシー機器を守るには遅すぎる。

・さらに、過検知（フォールスポジティブ）により、生産ラインや医療システムを強制シャットダウンさせるリスクがあり、費用対効果（コスト）に見合わない。

結論：ソフトウェア的手法では、
レガシー機器を安全にゼロトラスト化できない

物理レイヤーからサイバー攻撃を防御　「SA1」の特長

OS非依存・買い替え不要

端末にインストール不要。古いOSのままで最新のセキュリティを付与。

プラグ＆プレイ

LANポートに「挿すだけ」で強固な暗号化通信を確立。

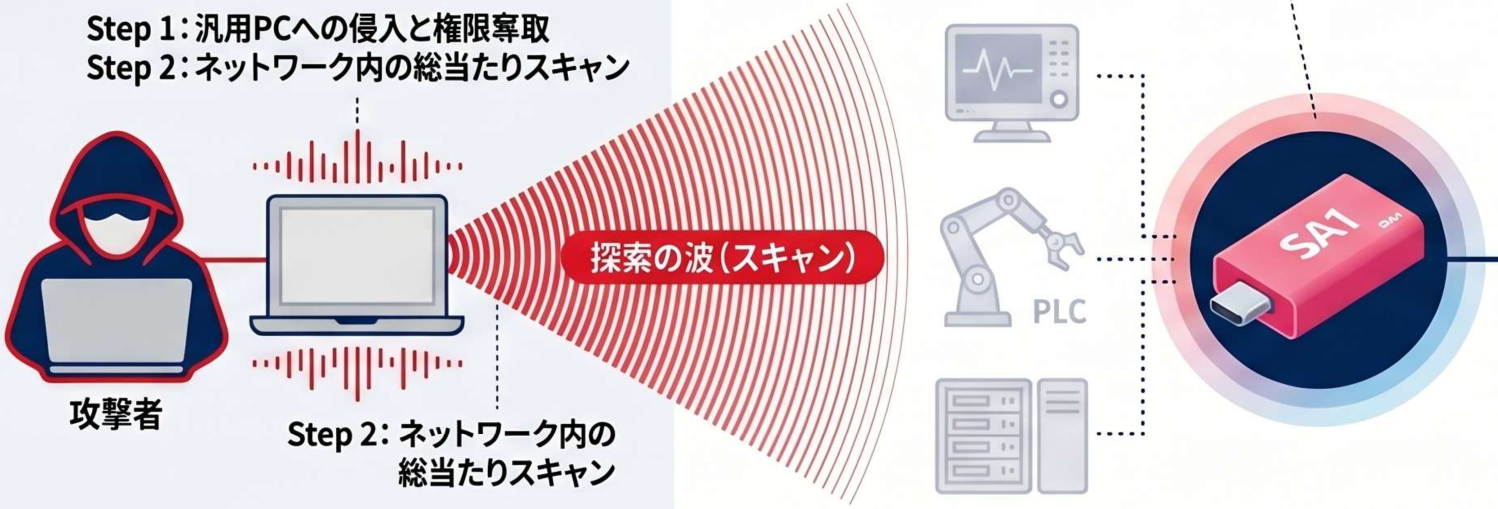
莫大なコスト削減

既存のレガシー機器の製品寿命まで安全な継続利用が可能になり、数千万円単位の機器買い替え費用を削減。ランサムウェアの横展開を物理レベルで阻止。

SA1の「完全隠蔽」：サイバー攻撃の横展開（ラテラルムーブメント）を無効化するステルス防御

侵入後の脅威「ラテラルムーブメント」

Step 1：汎用PCへの侵入と権限奪取
Step 2：ネットワーク内の総当たりスキャン



ランサムウェア等が境界防御を突破し、
社内・院内の汎用PCに感染。
攻撃者はこのPCを「踏み台」として制御権を得ます。

SA1による「完全隠蔽」のメカニズム

- **ネットワークからの完全隠蔽（ステルス機能）：**
  SA1を装着した機器は、事前設定された許可端末以外からのアクセスを物理・論理的に遮断し、スキャンに対して応答を返しません。

「見えない」＝「攻撃対象にならない」

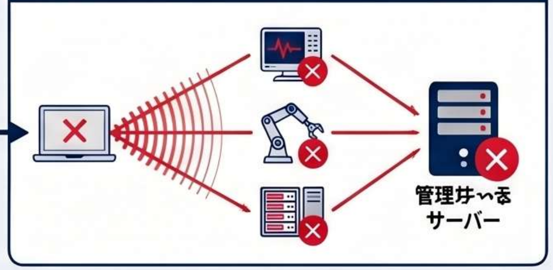
攻撃者の探索ツールにはSA1装着機器が表示されないため、
攻撃の足がかりとなるターゲットリストから完全に除外されます。

レガシー機器の延命と保護

OSのアップデートができない旧式の産業機器や医療機器でも、
SA1を「挿すだけ」で最新のゼロトラスト環境へ移行できます。

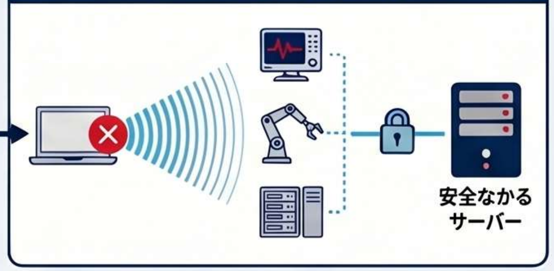
防御のプロセス：攻撃遮断の比較

未導入環境：感染の拡大



- 全ての機器が物理的に通信可能なため、踏み台PCから脆弱な機器へ次々と感染が広がり、最終的に管理サーバーが乗っ取られます。

SA1導入環境：攻撃の局所化

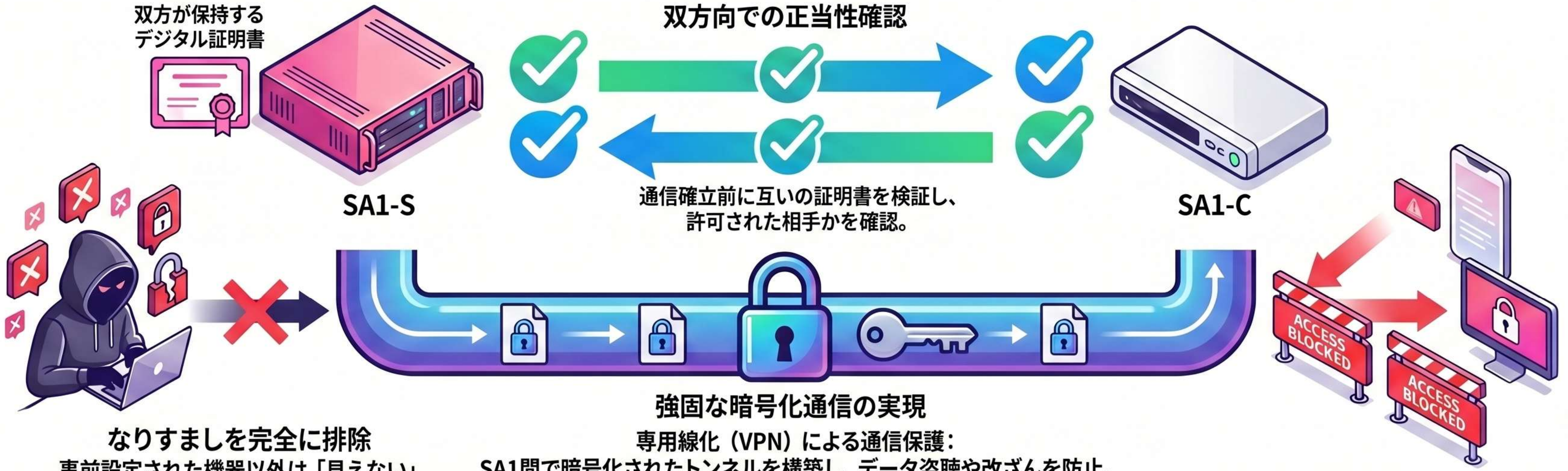


- 攻撃者のPath（経路）は遮断され、SA1装着機器は「存在しない」ものとして扱われるため、感染拡大は踏み台PCのみで停止します。
- 相互認証と暗号化（VPN）：正当な通信相手（サーバー）との間には強固な暗号化トンネルを構築し、なりすましやデータ盗聴も同時に防止します。

NotebookLM

SA1：相互認証による「なりすまし」完全排除の仕組み

サーバー（SA1-S）とクライアント（SA1-C）が互いに正当性を確認し合う「相互認証」の仕組みを視覚化し、なりすましを防ぐ強固なセキュリティを伝える。



なりすましを完全に排除
事前設定された機器以外は「見えない」状態となり、攻撃を物理的に遮断。

強固な暗号化通信の実現
専用線化（VPN）による通信保護：
SA1間で暗号化されたトンネルを構築し、データ盗聴や改ざんを防止。

最新のTLS 1.3規格に準拠した強固な暗号化通信

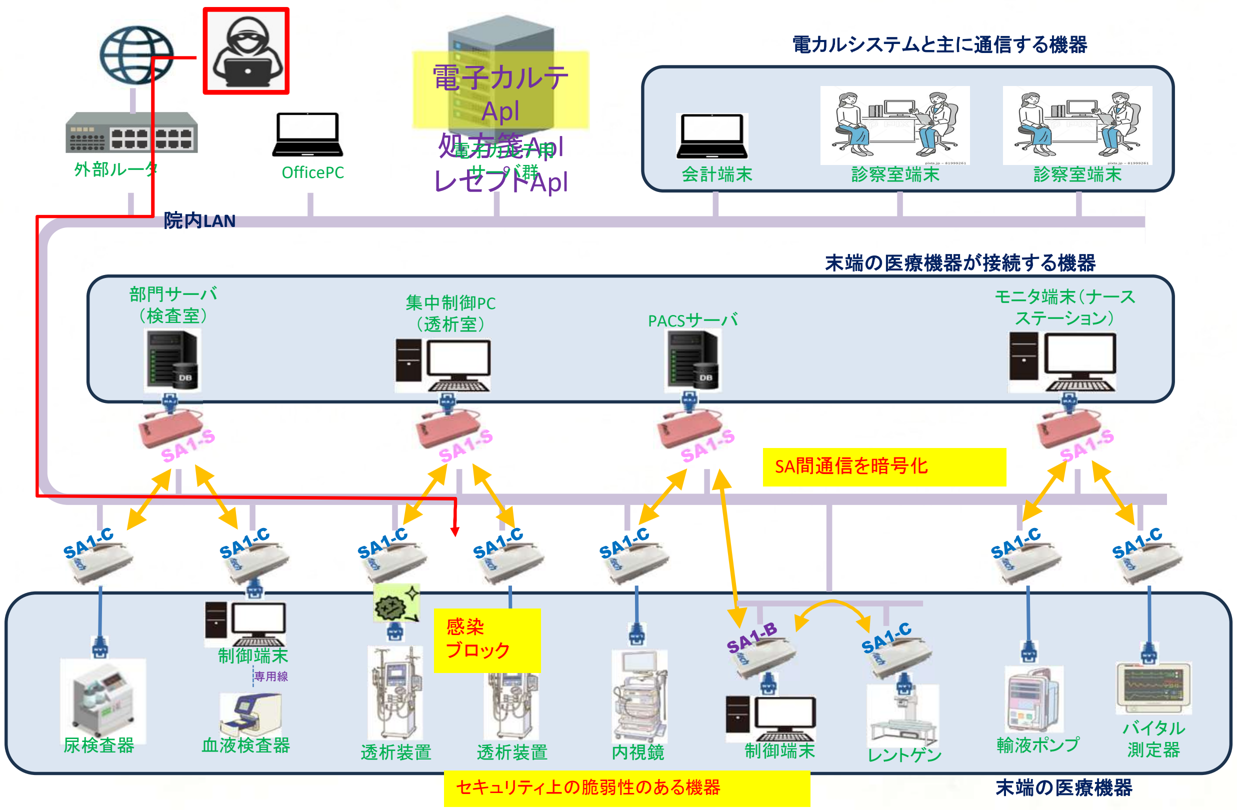
ゼロトラスト環境の実現
既存のネットワーク環境を変更せず、挿すだけで高度な防御を完了。

比較マトリクス：多層防御におけるSA1の明確な役割

機能軸	EPP	EDR	SA1
防御フェーズ	侵入前 （既知の脅威のみ）	侵入後 （事後・挙動監視）	侵入前 （アクセスの完全遮断）
対応対象OS	最新OS中心	最新OS中心	最新からレガシーOSまで全て （OS非依存）
導入アプローチ	ソフトウェア層	ソフトウェア層	ハードウェア・ ネットワーク層
運用リスク	未知の攻撃の すり抜け	過検知による システムダウン	ゼロインパクト （既存システムへの影響なし）

SA1は、ソフトウェア層で防ぎきれない「レガシー機器の接続層」を物理的に塞ぐ、従来とは異なるセキュリティ手法です

SA1運用構成例：総合病院の場合



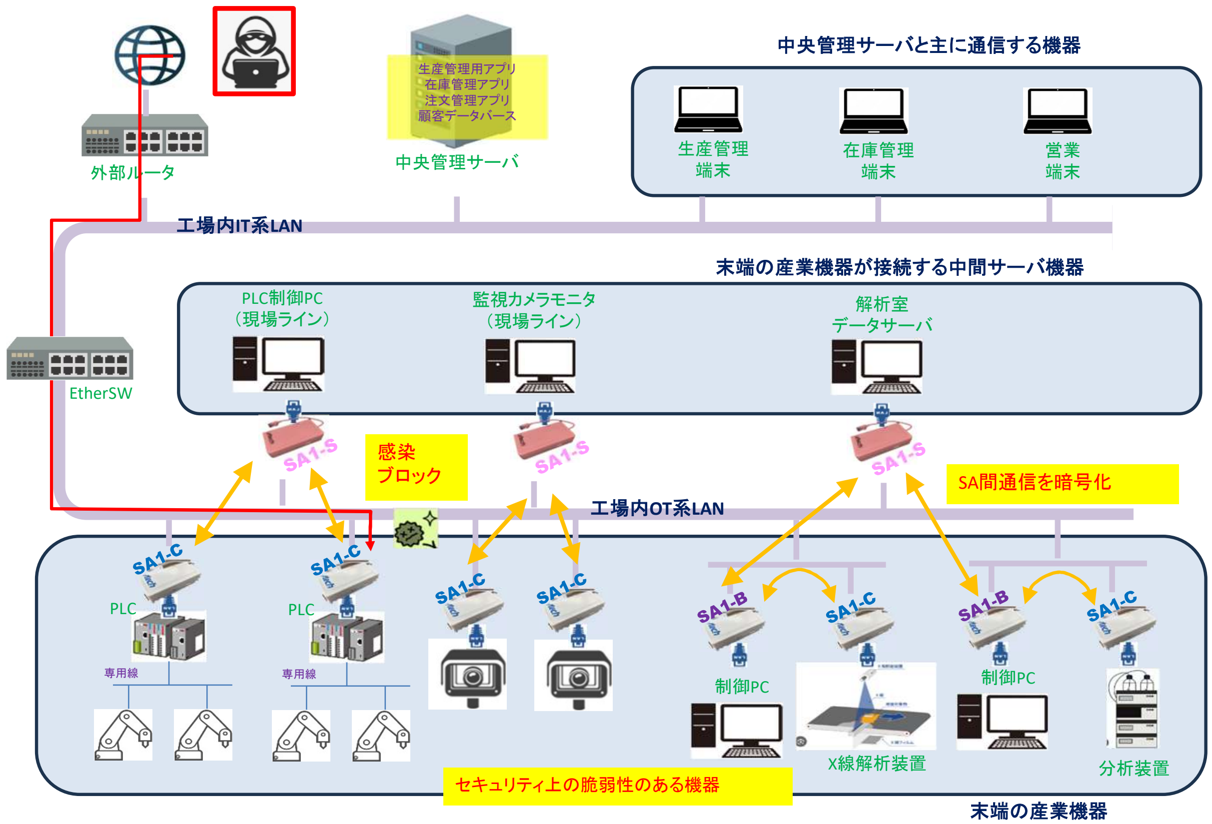
ネットワーク構造の変更は不要

論理的な接続が必須な機器のみを厳選してつなぐ究極のマイクロセグメント化を実現

[

末端機器にSA1-C（白）を取り付け、サーバ側にSA1-S（ピンク）を配置し、これらを結ぶだけの極めてシンプルな構成です。
これにより、既存のネットワークに手を入れることなく、強固な暗号化通信を確立します。

SA1運用構成例：メーカー工場の場合



病院同様にネットワーク構造の変更は不要

監視カメラ等最も狙われやすい工場内機器を効率よくゼロトラスト化

[
末端機器にSA1-C（白）を取り付け、サーバ側にSA1-S（ピンク）を配置し、これらを結ぶだけの極めてシンプルな構成です。
これにより、既存のネットワークに手を入れることなく、強固な暗号化通信を確立します。

DX推進の実現１：スマートファクトリーのグローバル連携

レガシー設備の安全なネットワーク参加

独立して稼働していた古いPLCや検査装置を、安全に工場OTネットワークへ統合。

リアルタイム生産管理

生産ラインネットワークを統合

工場内のIT系LANに潜むランサムウェアの脅威から生産ラインを完全に隔離しながら、稼働データを収集。

グローバルDXの加速

海外工場を含む一元管理

海外工場を含む全拠点での生産データ同期・一元管理を、セキュリティリスクゼロで実現。

DX推進の実現 2：次世代型スマートホスピタルの基盤

医療機構（IoMT）の完全保護

独自のOSで動く高額な医療機構（モダリティ）を、院内汎用PCからのマルウェア感染（踏み台攻撃）から防御。

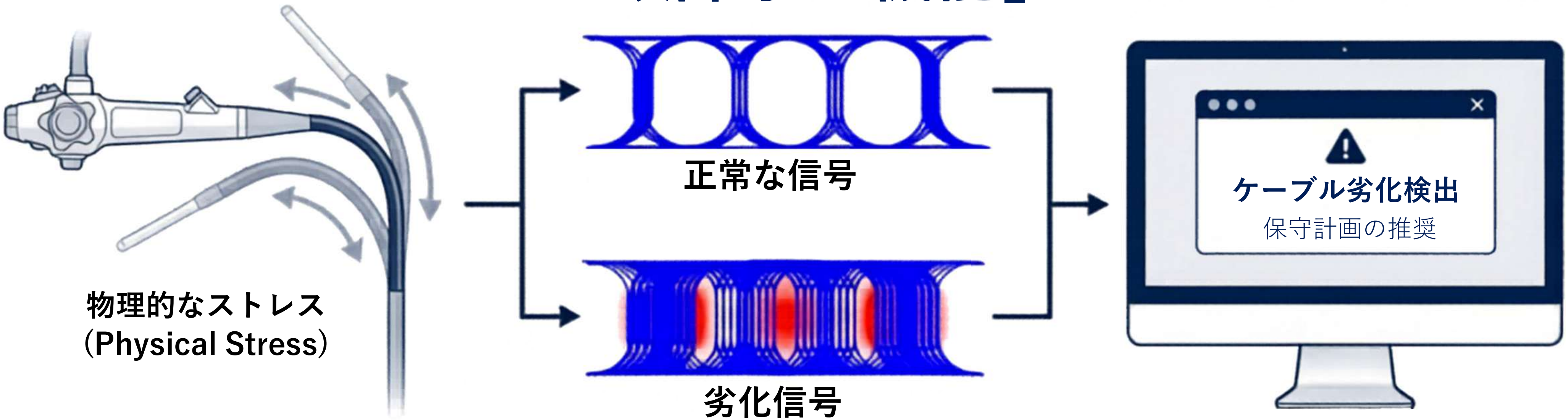
電子カルテ（EMR）との安全な統合

検査データを安全かつシームレスに電子カルテシステムへ自動転送。

遠隔医療（Telemedicine）の推進

患者の機微な医療データを外部へ安全に送信できる基盤を構築し、高度な遠隔診断や地域医療連携のDXを力強く後押し。

半導体設計企業ならではの付加価値
「故障予知機能」



物理レイヤーの監視

SA1は通信プロトコル（8B10B等）の最下層であるPhy部でのエラーを監視。

物理的な劣化を未然に防ぐ

内視鏡のケーブルや工場の可動部など、繰り返しの曲げ伸ばしによる通信ケーブルの物理的な劣化を信号波形（アイパターン）の異常から検知。

システムダウンの完全回避

通信が完全に途絶してシステムが停止する前に「ケーブル劣化検出」を通知。計画的なメンテナンスを可能にし、運用停止リスクを根絶。

結論：レガシーを守り、DXを加速する

【防衛】限界の突破

EPP/EDRでは守りきれない古いOS環境を、SA1の「完全隠蔽」と「相互認証」により、ネットワーク層から絶対防御。

【投資】莫大なコスト削減

高額な機器の買い替えを回避し、既存設備のまま製品寿命まで安全に継続利用。さらに「故障予知」で物理的ダウンタイムも排除。

【未来】DXの真の実現

ランサムウェアの脅威に怯えることなく、工場のグローバルデータ連携や病院の遠隔医療など、攻めのデジタル変革を推進。

既存のインフラに「挿すだけ」で、見えないセキュリティ基盤が完成します。