医療機器向け見守りソリューション

ベリフィケーションテクノロジー株式会社
2024年8月28日

日本の病院の現状

医療DX

医療DXについて

■ 国としては、医療の効率化を目指して、医療DXを推進中
（医療DX推進体制整備加算による、補助を実施中）

電子カルテの浸透状況

電子カルテシステム	一般病院（※1）	病床規模別			一般診療所（※2）
		400床以上	200～399床	200床未満	
平成 20年	14.2 % (1,092／7,714)	38.8 % (279／720)	22.7 % (313／1,380)	8.9 % (500／5,614)	14.7 % (14,602／99,083)
平成 23年（※3）	21.9 % (1,620／7,410)	57.3 % (401／700)	33.4 % (440／1,317)	14.4 % (779／5,393)	21.2 % (20,797／98,004)
平成26年	34.2 % (2,542／7,426)	77.5 % (550／710)	50.9 % (682／1,340)	24.4 % (1,310／5,376)	35.0 % (35,178／100,461)
平成 29年	46.7 % (3,432／7,353)	85.4 % (603／706)	64.9 % (864／1,332)	37.0 % (1,965／5,315)	41.6 % (42,167／101,471)
令和 2年	**57.2** % (4,109／7,179)	**91.2** % (609／668)	**74.8** % (928／1,241)	**48.8** % (2,572／5,270)	**49.9** % (51,199／102,612)

- **電子カルテの導入が進んでいる。**
- **大規模病院だと、90%以上、小規模病院まで加えると、半分程度。**

医療DXの負の側面

医療機関は狙われやすい

- 病院などの医療機関は社会保障番号や病歴、患者の個人情報など、情報の転売や恐喝に悪用されやすいデータを多く保有していること
- 他の業界に比べてバックアップやOSのアップデート、セキュリティパッチの適用などのセキュリティ対策が進んでいないこと
- 医療行為を提供しなければならない社会的責任から、身代金の支払いに応じる可能性が高いと見られていること

サイバー攻撃の主な事例（日本の病院）

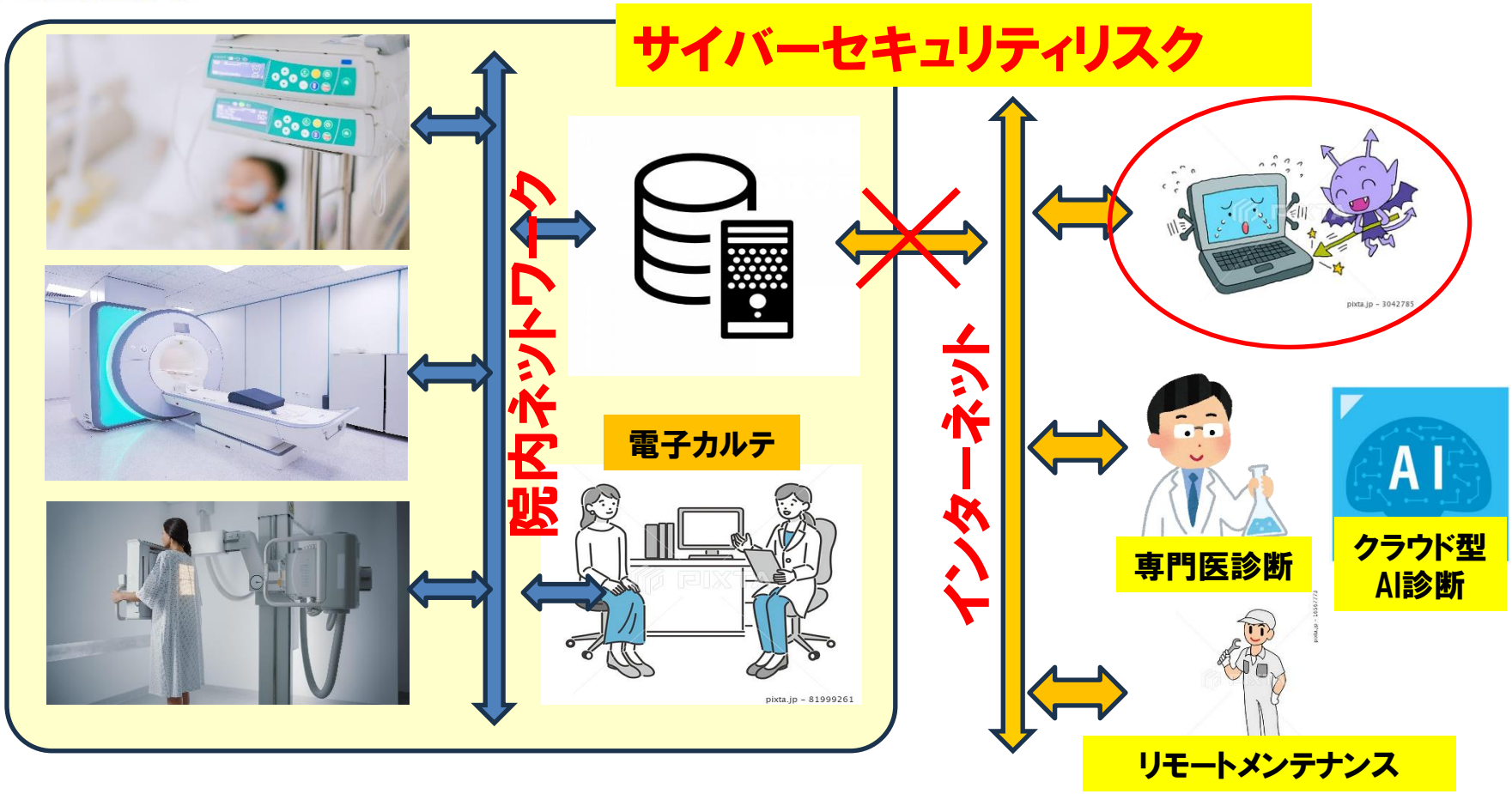
■2021年10月
徳島県の病院がランサムウェア「Lockbit 2.0」攻撃による被害。病院内の十数台のプリンタから英文の「犯行声明」が出力された。8万5千人分の電子カルテや院内LANが使用不能になり、会計システムで診察費の請求もできなくなったため、一部の診療科を除き新規患者の受け入れを中止。復旧に2か月を要した。

■2022年1月
東京都の病院で院内サーバーがコンピュータウイルスに感染。電子カルテが閲覧不能になり、会計システムも停止。診療を一部停止し、診療費を後日請求する事態に。

■2022年6月
徳島県の病院でランサムウェア「Lockbit 2.0」によるシステムへの侵入被害。電子カルテ、院内LANシステムが使用不能に。オフラインバックアップによって早期に復旧。

■2022年10月
大阪の医療センターでランサムウェア攻撃被害。電子カルテなどが暗号化され、外来診療や各種検査が停止し、復旧に2か月を要した。ランサムウェアの侵入口は給食委託事業者のVPN装置とされる。

日本の院内医療機器の現状と課題



病院内では、医療機器は院内ネットワークに接続している。
ただし、サイバーセキュリティリスクから、積極的にはインターネット接続していない。
この影響で、「外部の専門医やデータサイエンティストの活用が難しい」「機器のリモート診断＆メンテナンスが出来ない（故障による不稼働が発生）」といった状況になっている。

医療機器見守りソリューション

概略

Vtechでは、サイバーセキュリティ対応と故障予知のソリューション事業を提供中。
最初のターゲットとして、医療機器の故障予知とリモートメンテナンスの実現を図ることを模索。名称は、「医療機器見守りソリューション」。

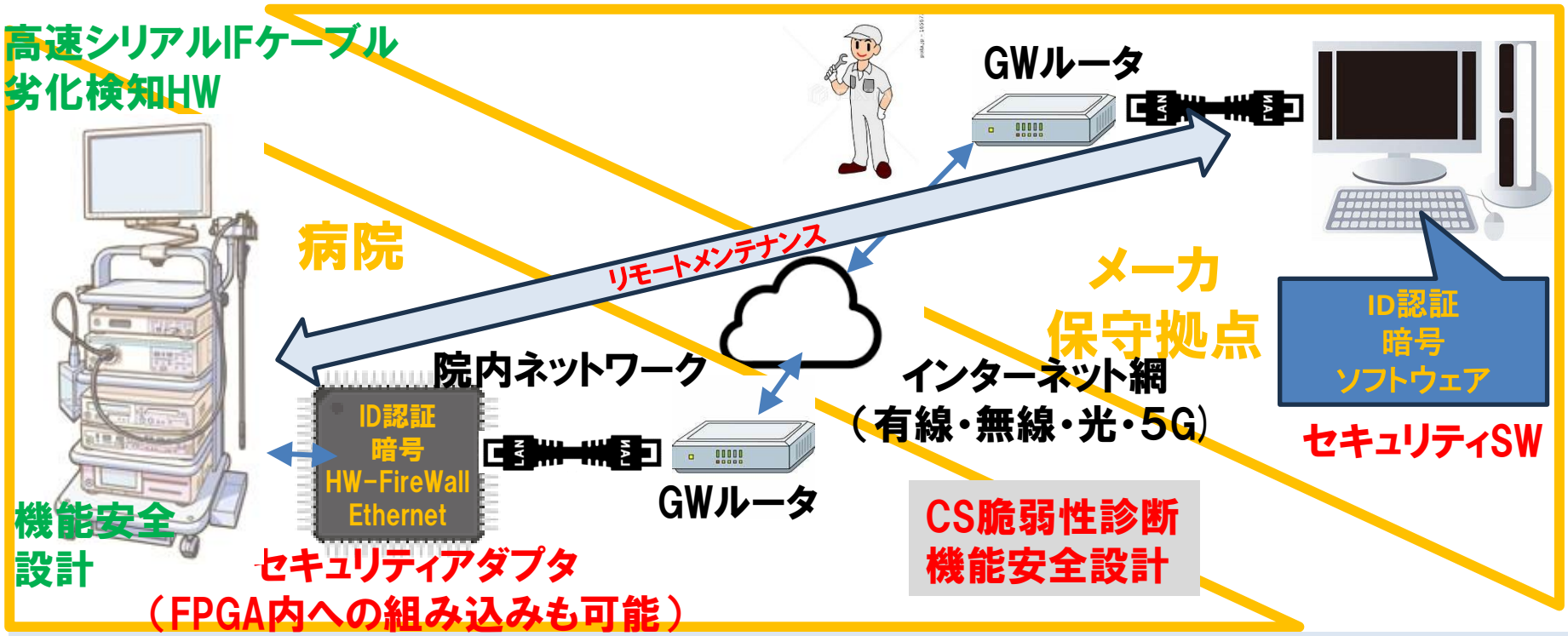
以下の要素技術やサービスを組み合わせたソリューションを提供可能。

- サービス
  - 脆弱性診断サービス（CS対策が必要な要素の洗い出し）
  - 機能安全設計サービス（SafetyMechanizmの実装＝故障検知）
- IP技術
  - セキュリティ
    - ✓ ID機器認証IP（機器側はHW、サーバ側はSW）
    - ✓ リアルタイム画像データ転送に対応可能な高性能暗号化IP
    - ✓ 組み込み型ファイアウォールIP
  - 故障検知
    - ✓ 高速IFケーブルの劣化検知IP（特許出願済）

内視鏡を題材に検討をしているが、検査機器にも適用可能と考えている。
長期的には、FA向けを含めた、IoT機器全体に適用範囲を広げることを想定。

ソリューションの導入イメージ

目的:リモートメンテナンスによる保守業務の軽減



- CS対策
  - 病院の医療機器とメーカ保守拠点のPC同士でID認証(他の機器からの接続をブロック)
  - 暗号化HWにて、通信データ自体を暗号化
    （共通暗号化キーは、公開鍵方式をつかって、暗号状態で交換）
  - 組み込み型ファイアウォールHWにて、他の機器への感染防止
- 故障診断
  - 機能安全機構の実装による故障検知
  - 高速シリアルIFケーブル劣化検知HWによる、故障予知

CRA（Cyber Resilience Act）対策

セキュリティ特性要件：付属書1

附属書Iの１「セキュリティ特性要件」

（１）リスクに基づいて適切なサイバーセキュリティを確保するよう設計・開発・生産されていること。
（２）悪用可能な脆弱性が含まれないこと。
（３）リスクベースアセスメントに基づいて、以下を満たすこと。
(a) 製品を元の状態にリセット可能である等、安全な構成となっていること。
(b) 適切な制御メカニズムにより不正アクセスからの保護が確保されていること。
(c) 最先端の暗号化などにより個人データ・その他のデータの機密性を保護すること。
(d) データやプログラムなどの完全性を許可されていない操作から保護し、破損についても報告すること。
(e) 必要なデータに限定して処理を行うこと。（データの最小化）
(f) DoS攻撃からの回復・緩和などの重要な可用性の機能を保護すること。
(g) 他の機器やネットワークからのサービスの可用性について自身への悪影響を最小化すること。
(h) 外部インターフェース等の攻撃対象領域を制限して設計・開発・製造されていること。
(i) インシデントの影響を軽減するように設計・開発・製造されているころ。
(j) アクセス、データ修正、サービス、機能などの内部活動を記録・監視し、セキュリティ情報を提供すること。
(k) 自動更新やユーザーへのアップデート通知などによりセキュリティアップデートによる脆弱性対応を確実に行えること。

附属書Iの２「脆弱性処理要件」　・・・製造業者が満たすべき要件

（１）製品に含まれる脆弱性とコンポーネントを特定し、文書化すること。そのために、機械読み取り可能な形式で一般的に使用されるSBOM作成（少なくとも最上位レベルの依存関係含む）を行うこと。
（２）セキュリティアップデートの提供など、遅滞なく脆弱性に対処・緩和すること。
（３）効果的かつ定期的なテストとレビューを行うこと。
（４）脆弱性情報の公開及び修正を行うこと。
（５）脆弱性開示ポリシーを導入し、実施すること。
（６）製品やサードパーティコンポーネントの潜在的な脆弱性に関する情報共有を行い、連絡先を提供すること。
（７）悪用可能な脆弱性が適時に修正・緩和されるように安全にアップデートを配布するメカニズムを提供すること。
（８）セキュリティパッチや更新プログラムが遅滞なく無料で配布され、ユーザーへの助言メッセージも添付すること。

CRAでは、現状、医療機器は対象外となっている（IEC81001-5-1に準拠：SW開発時のCS対応要件だけ）が、今後、CRA準拠の対応を求められる流れとなるのは必須。その際に、「SWの自動更新」の実装が求められる。この面でも、リモートメンテナンス機能の実装は重要。

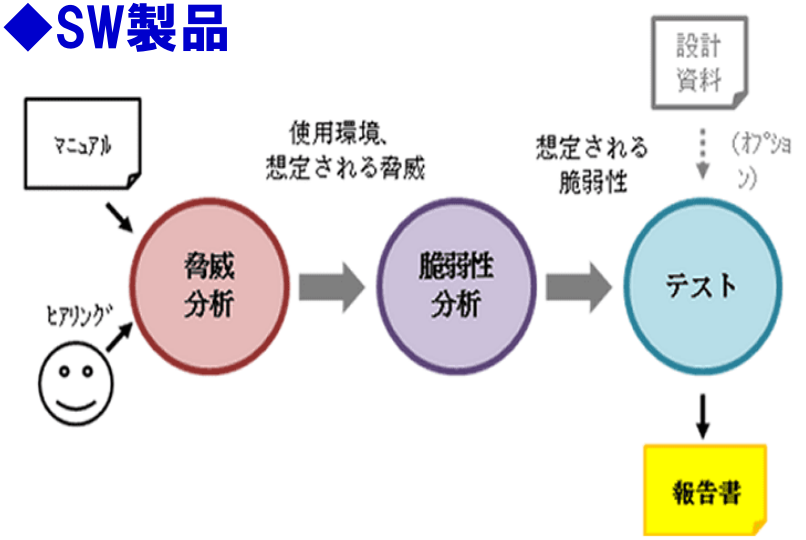
個別技術
サイバーセキュリティ関連

脆弱性評価

開発製品が、利用を想定する環境での脆弱性を、脆弱性評価/脆弱性診断で評価します。
これにより、対策すべき機能やブロックの明確化に貢献します。
この脆弱性評価/脆弱性診断は認証を取るためにも必須な作業です。

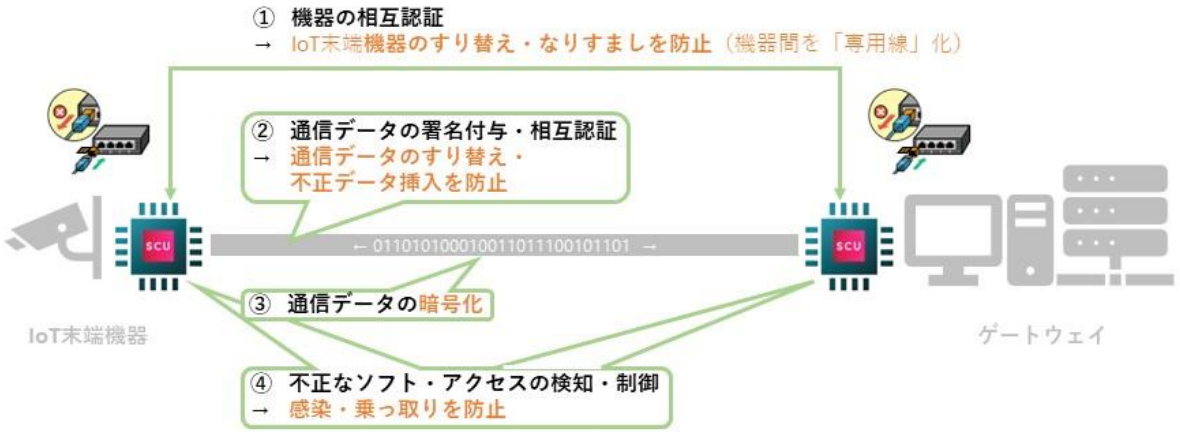
◆HW製品（LSIデバイス）

◆SW製品



ID認証＆鍵交換（セキュリティアダプタ）

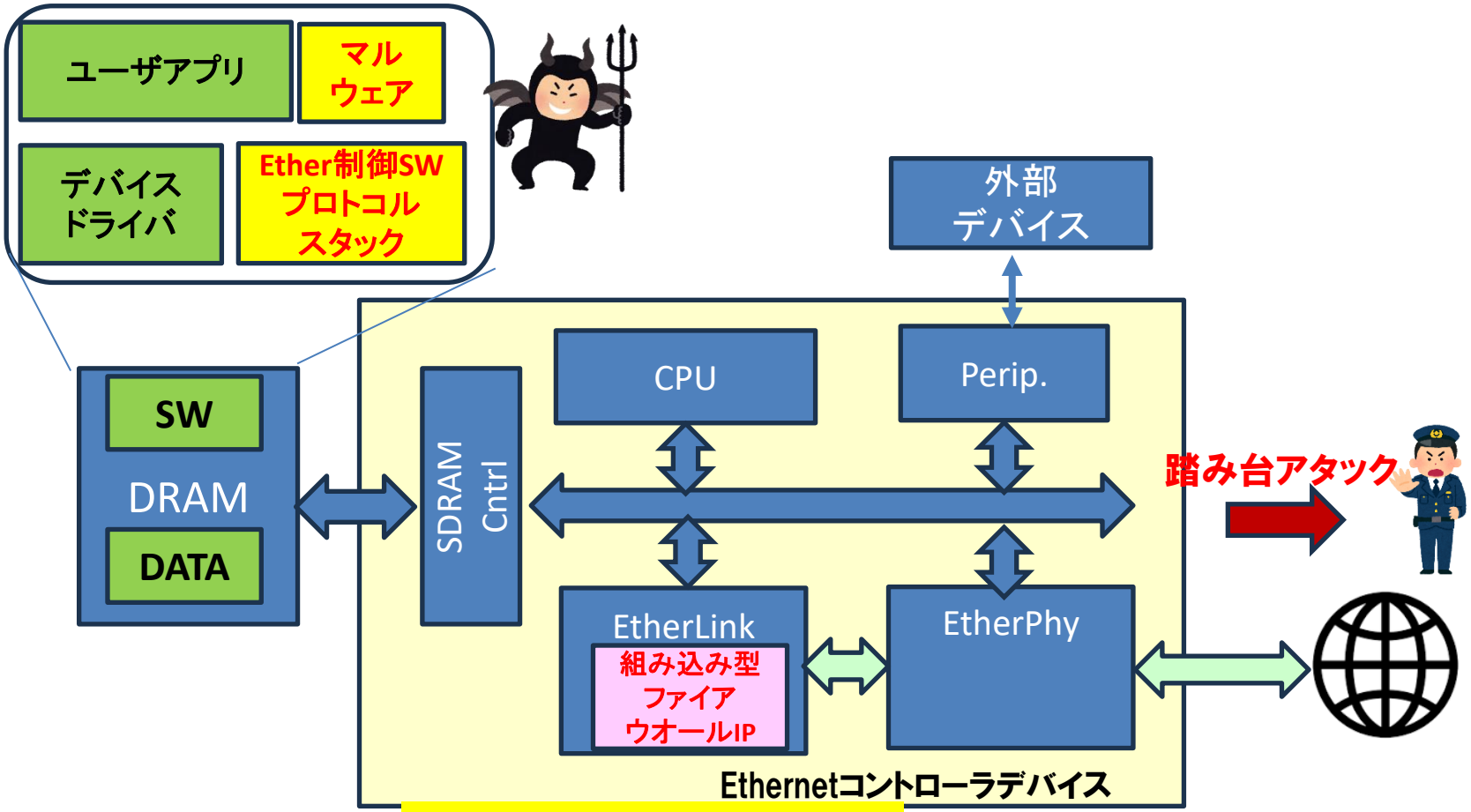
■ SCUの機能・効能



- ゼロトラスト対応技術であるID認証方式を実現。認証された機器同士以外の接続をブロック。
- リアルタイム通信で使用される、共通鍵方式の暗号化（AES等）では、共通鍵の漏洩がセキュリティリスクとなるが、本方式では、公開鍵方式を用いて、秘密裏に共通鍵の交換が高頻度で可能。

組み込み型ファイアウォールHW

Ethernet通信には、マスタースレーブの概念がない。
CSアタックにより機器が乗っ取られると、LAN接続した機器に対する攻撃源となりうる



- ブロードキャスト機能のマスク
- アクセス先IPアドレスの限定
- 不審アクセスの検出＆通知

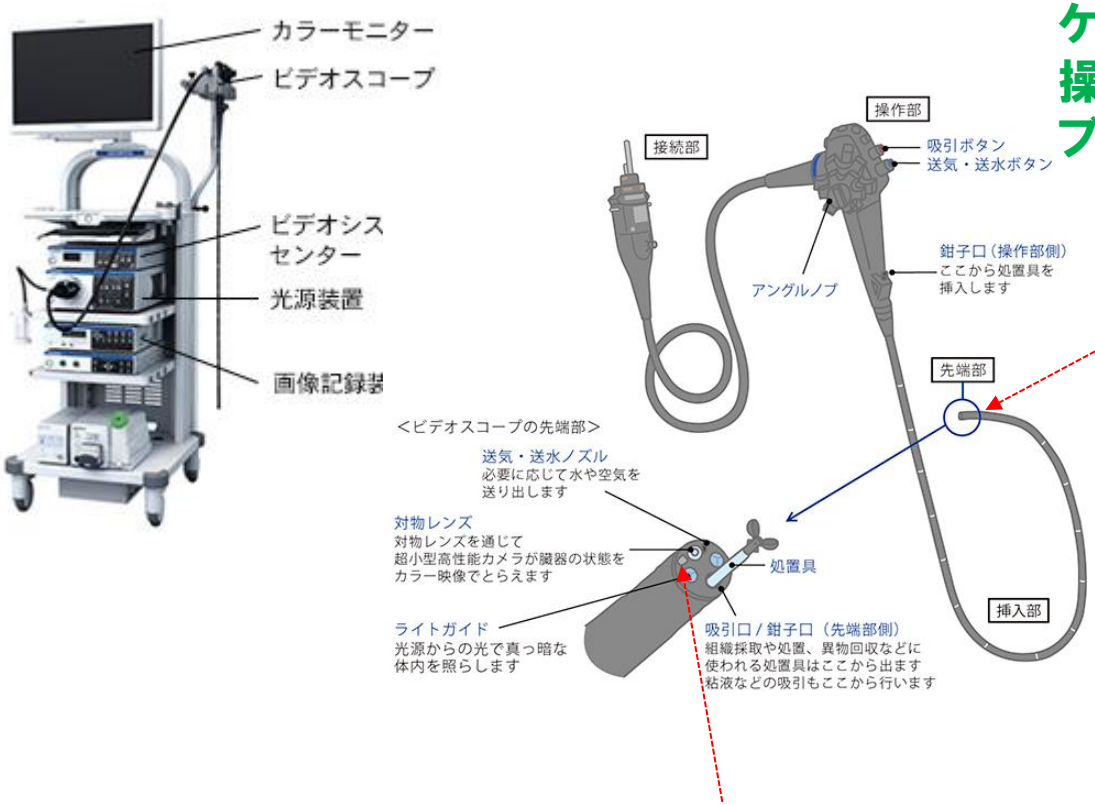
個別技術
故障検知・故障予知

高速シリアル通信の故障予知

特許出願済

内視鏡における故障頻発部位(推定)

https://www.onaka-kenko.com/endoscope-closeup/endoscope-technology/et_01.html



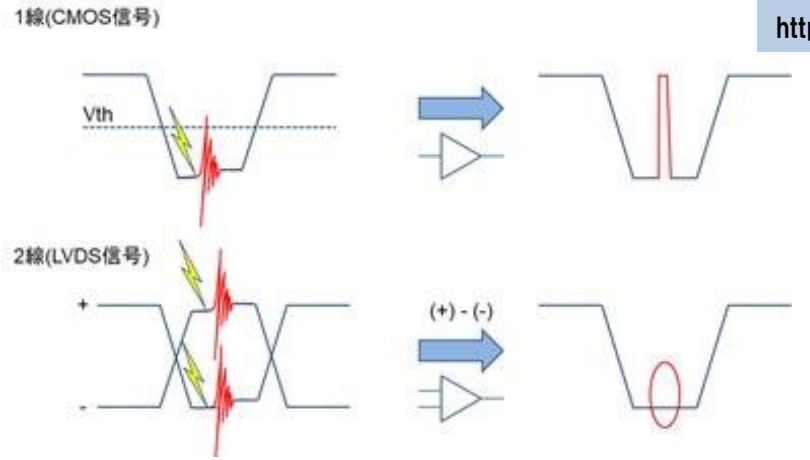
挿入部の中に、高速シリアルIFのケーブルが格納されている。
操作時の曲げ延ばしにより、ケーブルの品質が、徐々に劣化する。

先端部にセンサーデバイスを設置

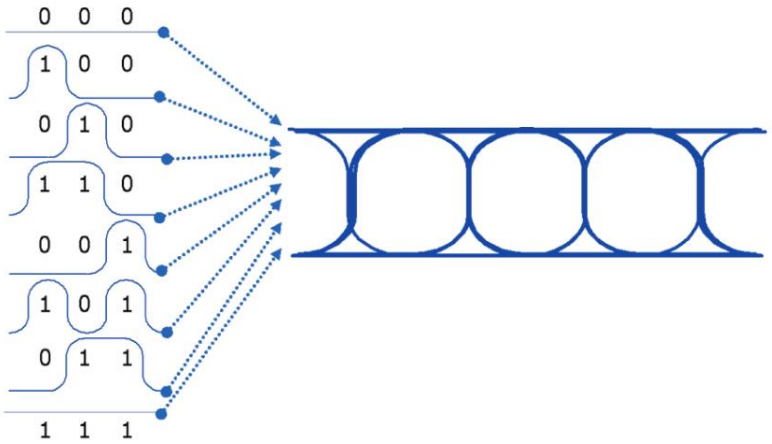
高速シリアル通信の信号劣化の表出

高速通信の基本方式:LVDS(Low Voltage Differential Signal)

https://emb.macnica.co.jp/articles/7396/

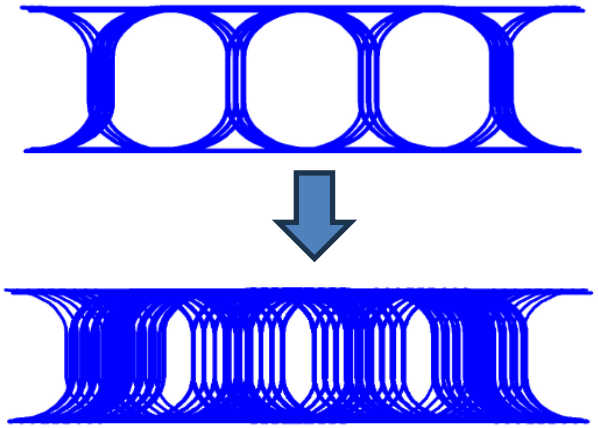


アイパターン



https://www.tek.com/ja/documents/application-note/anatomy-eye-diagram

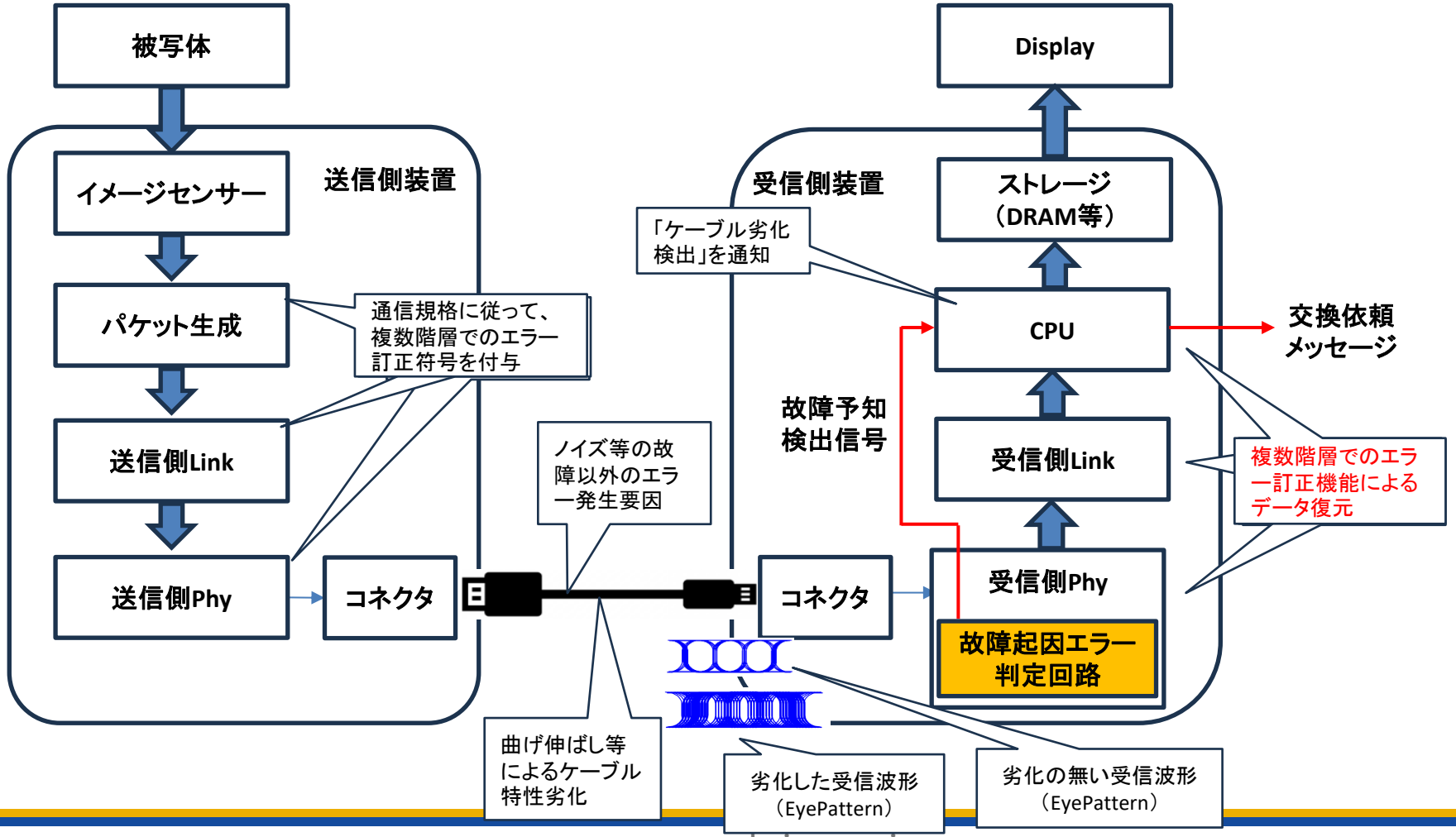
LVDS信号の劣化の表出



アイパターンの開口部が狭くなり、
ビット変化時の信号誤認が増える。

故障検出方法：全体像

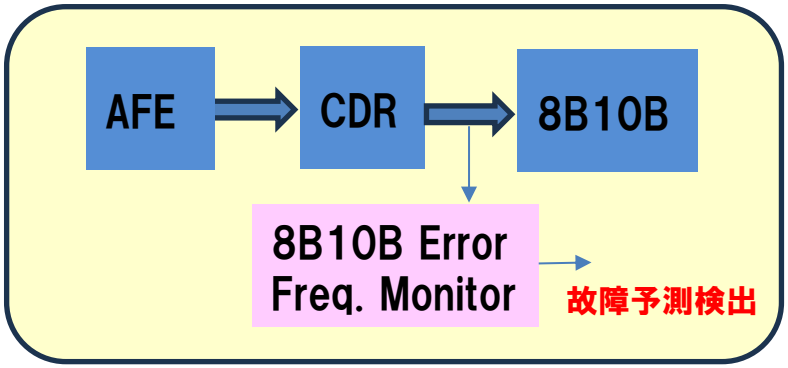
高速シリアルIFを利用する各種プロトコルでは、エラー訂正符号が実装してある。このため、伝送品質の劣化により通信エラーが発生している状況でも、システム側ではエラー発生が把握できない。⇒　Phy部に故障予測機能を実装し、ケーブル劣化の検出を可能とする。



故障検出方法：詳細

CDR直後のデータをモニタ、8B10Bに違反したデータを検出

構成



8B10B符号

8B/10B の符号

8B/10B エンコードには、データ文字と K 符号が含まれます。8 ビットの値は 10 ビットの値にコード化され、シリアル ラインの DC バランスを保ちます。K 符号とは、CHARISK で指定された特殊なデータ文字です。これらは、特定の情報を示す場合に使用します。次の表に、有効なデータ文字と K 符号を示します。

表: 有効なデータ文字

データ バイト名	ビット HGF EDCBA	現在の RD – abcdei fghj	現在の RD + abcdei fghj
D0.0	000 00000	100111 0100	011000 1011
D1.0	000 00001	011101 0100	100010 1011
D2.0	000 00010	101101 0100	010010 1011
D3.0	000 00011	110001 1011	110001 0100
D4.0	000 00100	110101 0100	001010 1011
D5.0	000 00101	101001 1011	101001 0100
D6.0	000 00110	011001 1011	011001 0100
D7.0	000 00111	111000 1011	000111 0100

■故障予測方法：
- **8B10Bの規則に違反した信号の発生頻度をモニタ**
- **発生頻度は、ケーブルの劣化に従って、徐々に増えてくるはず。**
- **発生頻度が閾値を超えると、「故障予知検出」のアラートを発生。**
- **短期的な頻度アップはノイズとして無視**

■長所
- **アナログに近い箇所をモニタしているので、有効性が高い**

■短所
- **8B10BはPhy内部に実装されており、Phy自体の改修が必要**

機能安全設計と故障検出

機能安全設計実績

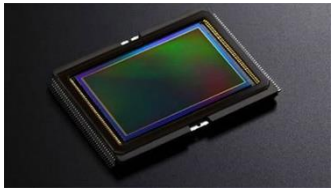
機能安全設計とは、機器の故障が発生しても、安全状態に導ける設計の事。
弊社は、この分野において、規格のコンサルを含め、多数の実績あり。

①IEC61508対応の産業用ロボット用FPGA開発　SIL-2

-IEC61508の導入サポート
-技法の解説書及びチェックリスト作成
-システムの分析結果に基づいたアーキテクチャ仕様書及び設計仕様書作成
-設計、検証及びFPGAデータ作成
　　モニター回路の組込み及びカバレッジの算出
-**開発期間及び開発コスト30%削減**

②ISO26262対応のイメージセンサー開発　ASIL-B(D)

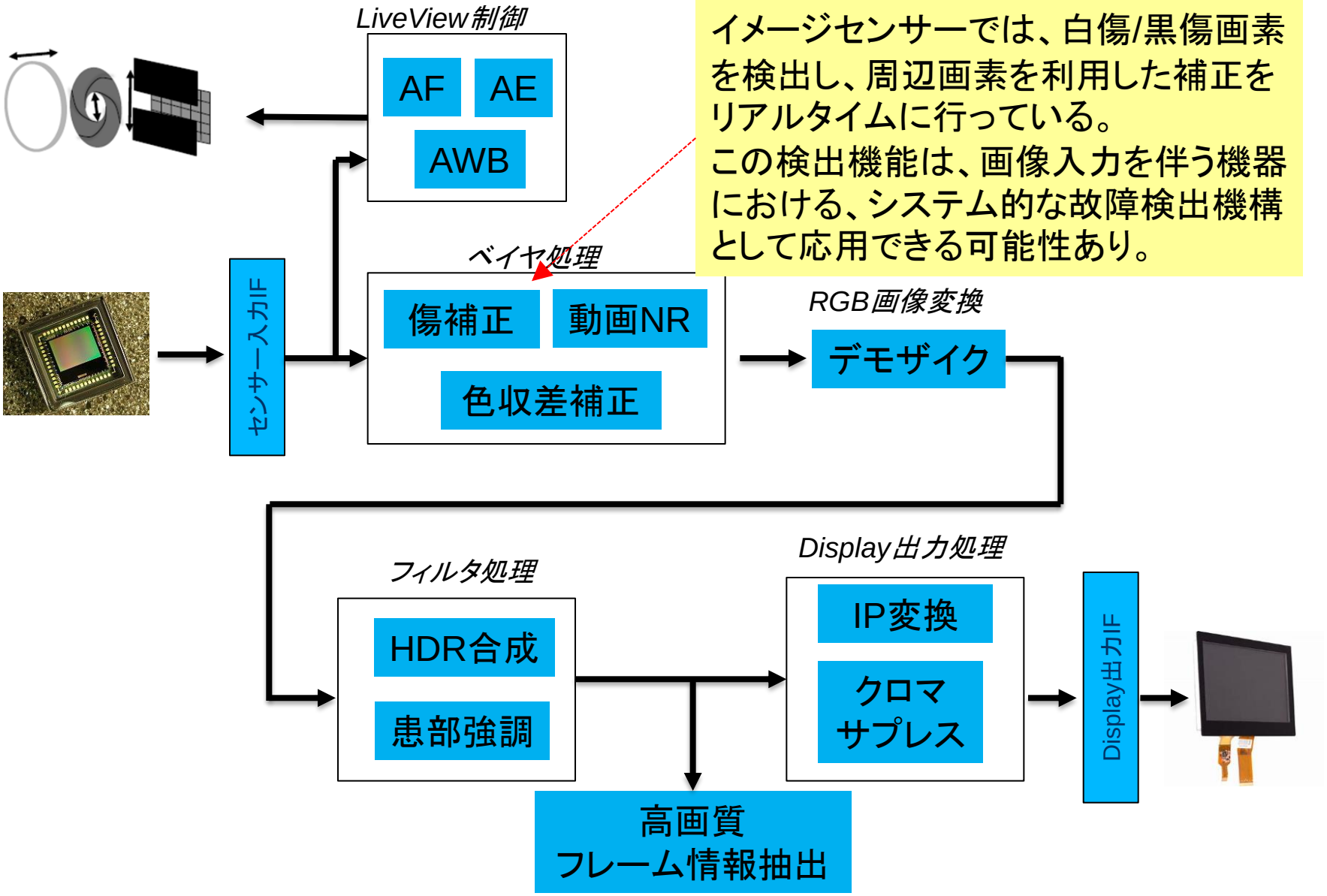
-安全分析
-安全設計及びSafety Mechanismの要求仕様作成
-Safety Mechanismを含む設計、検証
-**コンサルが提案した単純な2重化と比べてチップサイズ＆消費電力30%減**



③ISO26262対応の次世代ヘッドライトシステム開発　ASIL-B

-**開発部門と品質部門に対してISO26262導入サポート**
-安全分析
-安全設計及びSafety Mechanismの要求仕様作成
-Safety Mechanismを含む設計、検証
-開発メンバーの機能安全トレーニング

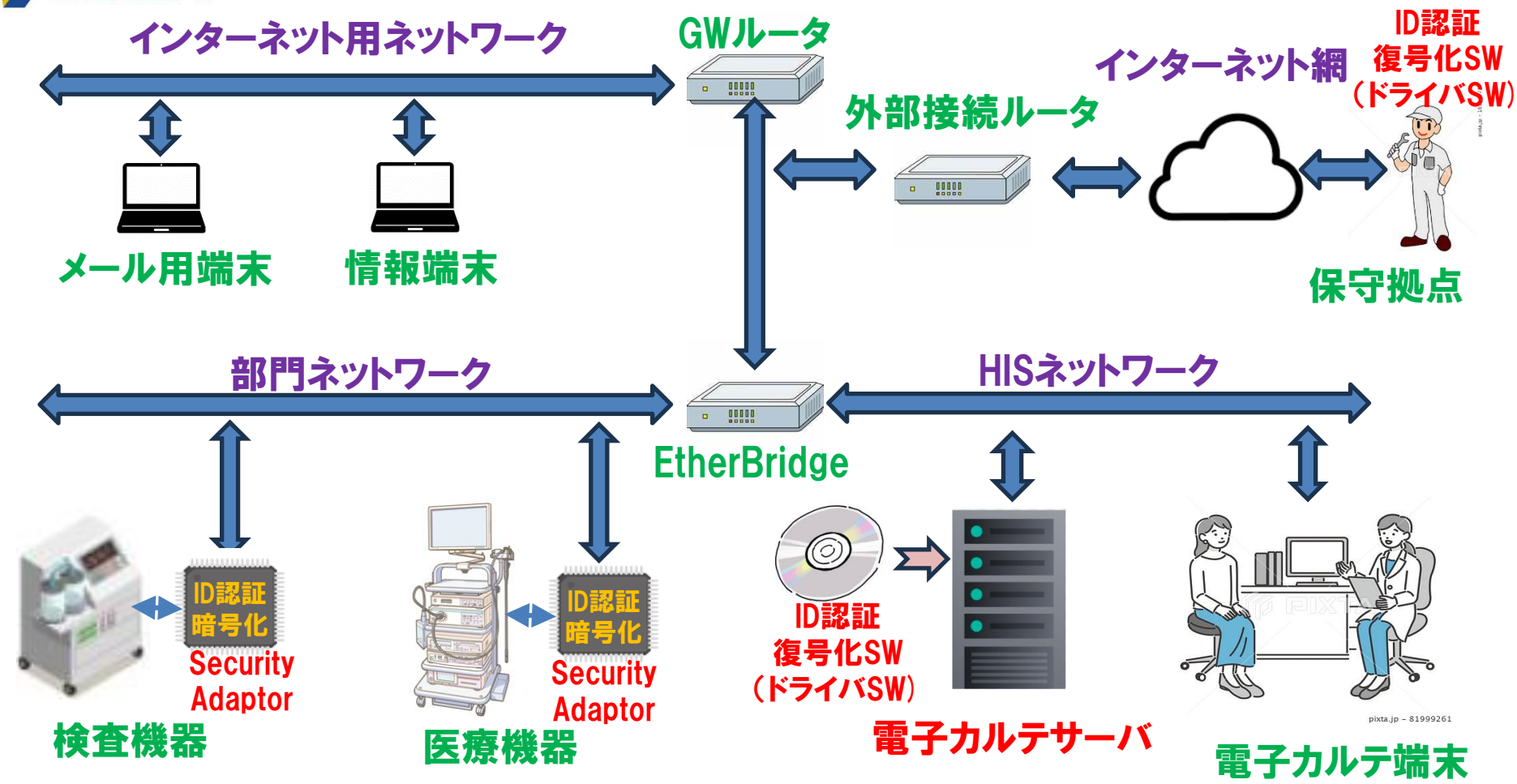
画像処理実績と故障検出への応用



イメージセンサーでは、白傷/黒傷画素を検出し、周辺画素を利用した補正をリアルタイムに行っている。
この検出機能は、画像入力を伴う機器における、システム的な故障検出機構として応用できる可能性あり。

電子カルテ連携
～電子カルテメーカに打診中～

SecurityAdaptorとサーバの接続イメージ



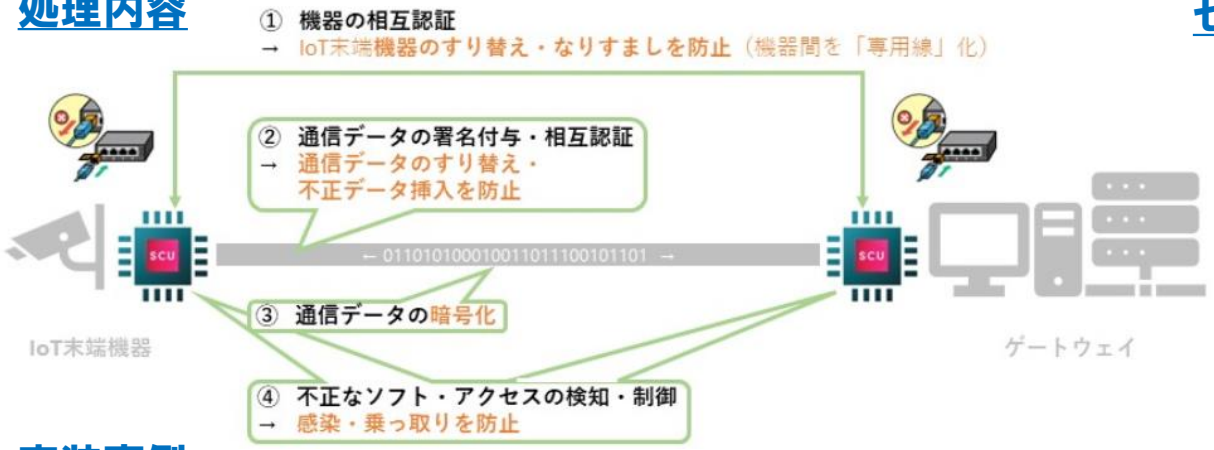
■現状
医療機器のネットワーク接続先は電子カルテだが、電子カルテ接続のためのCSの標準規格がなく、CS対策無で接続。（IEC81001-5-1に完全準拠しきれていない状況が発生）

■本提案
ID機器認証＋暗号化による、非常に強力なCS対策を実現。

セキュリティアダプタ詳細

セキュリティアダプタ詳細

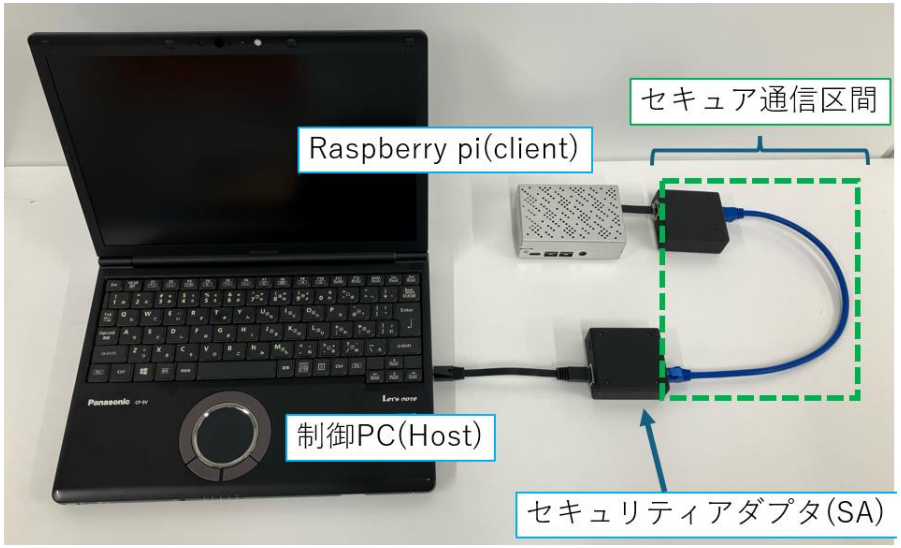
処理内容



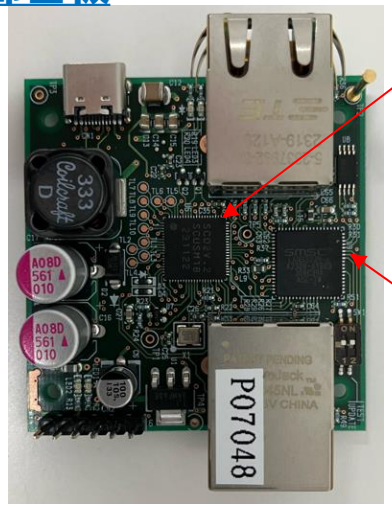
セキュリティアダプタ

サイズ：60 x 55 x 24mm

実装事例



内部基板



SCUチップ
データ暗号化が必要な場合、10Mbps程度になる

SCSC EtherSwitch
100Mbpsサポート

- 上図は、SecurityAdaptorが両端に接続された形態になっているが、処理速度の制約もあり、CPU性能が高いサーバへの接続の場合、SWドライバでの実装を想定。

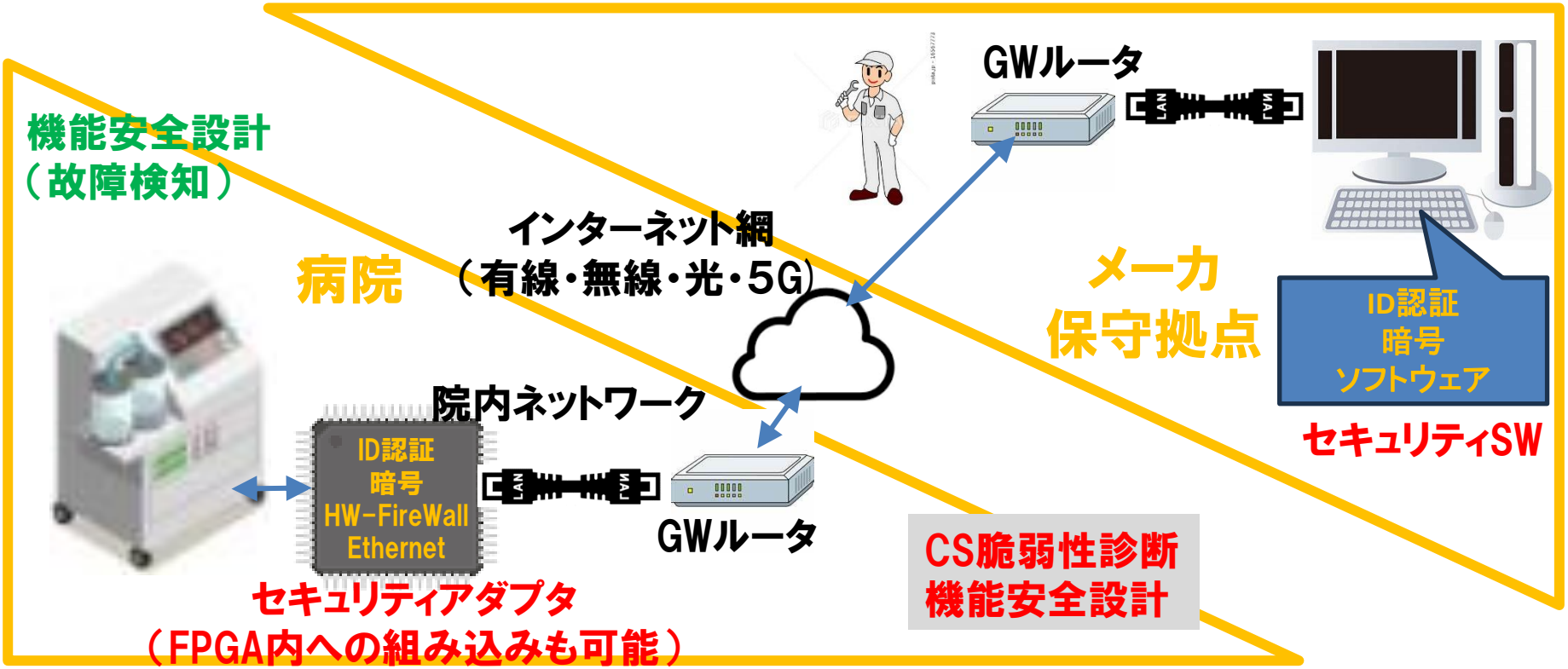
セキュリティアダプタ：構成比較

現時点での製品は、外付けボックス型のVSA-BOXだけだが、FPGAへIPとして組み込む構成（VSA-IP）や、SWとしての実装版（VSA-SW）を開発中。

名称	VSA-BOX	VSA-IP	VSA-SW
			
構成	Etherポートへの外部接続型	FPGA内実装用のIP版	SWでの実装版
推奨用途	既存製品（デバイス側）のCS強化策	新規開発品（デバイス側）のCS強化策	VSA-BOX, VSA-IPと通信を行うサーバ側への実装
実装容易性	◎	×	○
処理速度	×（※1）	○	○（※2）
1対多接続	×	×	○
脆弱性検出時の対応容易性	×	○	○
耐タンパ性	◎	○	×

※1　暗号化無の場合100Mbps, 有の場合10Mbps
※2　ホストCPU性能依存

最後に



本ソリューションの一部のサービスや機能についてでも良いので、ご興味があるようであれば、是非、個別提案させてください。

ベリフィケーションテクノロジー株式会社

■本　社
〒222-0033　横浜市港北区新横浜2-3-12　新横浜スクエアビル5F
TEL：045-470-8310　　FAX：045-470-8319

□関西支社
〒600-8813　京都市下京区中堂寺南町134　KRP2号館2階
TEL：075-950-0430　　FAX：075-950-0431