
Aillis

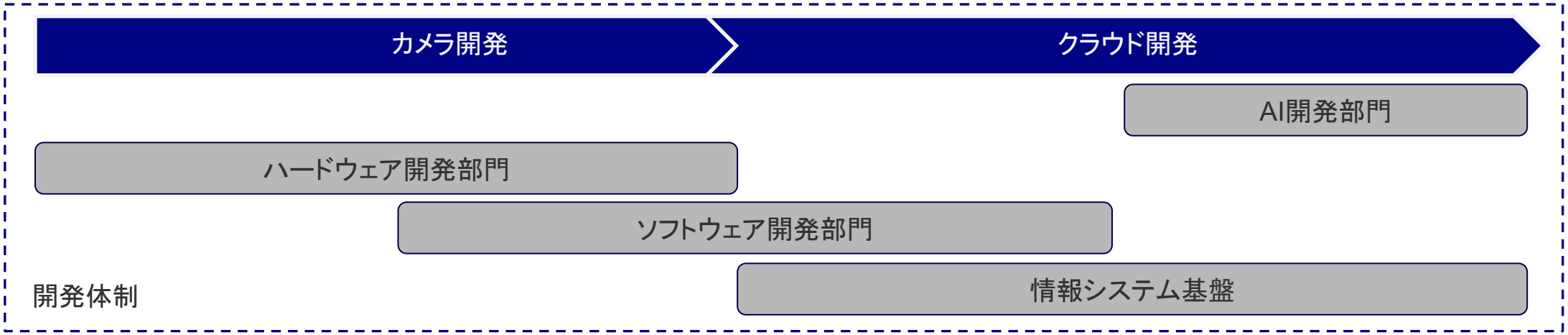
当社が取り組む医療機器セキュリティ対策の事例紹介

アイリス株式会社（Aillis, Inc.）

情報システム基盤 部門長

有川 晃貴

当社の開発体制は AI開発 / ハードウェア開発 / ソフトウェア開発 / 情報システム基盤 の4部門で構成しています。
情報システム基盤部門は主に製品のインフラストラクチャ・医療機器セキュリティ及び全社の情報システム・
情報セキュリティに関連した活動を担当しています。



会社情報

アイリス株式会社（Aillis, Inc.）

業許可・登録：

第一種医療機器製造販売業（許可番号：13B1X10294）

高度管理医療機器等販売・貸与業（許可番号：第5502230964号）

医療機器製造業*（登録番号：13BZ201786）

医療機器修理業*（登録番号：13BS201695）

（*神田事業所）

代表者：

沖山 翔

設立：

2017年11月

本金：

1億円（2022年10月末時点）

所在地：

東京都中央区八重洲2-2-1 八重洲セントラルタワー7階

みんなで共創できる、
ひらかれた医療をつくる。

医療は、決して医療関係者だけのものではありません。

たとえば、不調を感じた患者さんが診察を受けること。
その診療データはAIを進化させ、
未来の診断をより正確なものにできる。
患者さんの協力も、
医療を前に進めることができるのです。

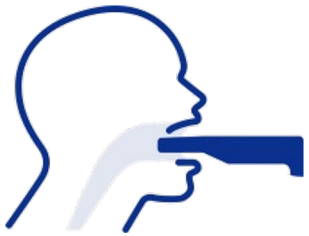
私たちが目指すもの。
それは、医療をみんなでつくれる未来。

医師も、患者も、健康な人も。
すべての人が、所属や立場、国境を超え、
医療を発展させる可能性を秘めている。

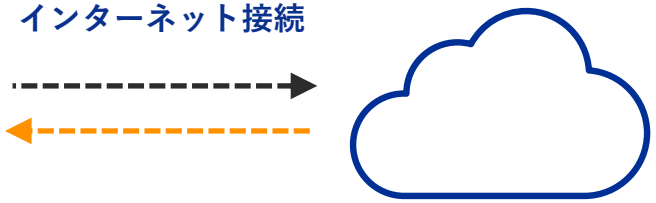
アイリスは、
そんな一人ひとりが持つ医療への可能性を、
テクノロジーの力でひらいていきたい。

みんながつくっていける。みんなが使っていける。
風通しのいい、ひらかれた医療のために、
私たちは挑戦を続けます。

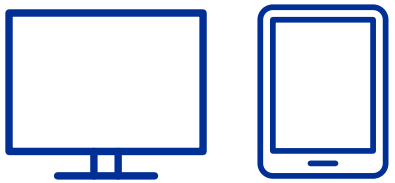
製品 のしくみ（AI・感染症診断）



Wi-Fiでの
インターネット接続



Wi-Fiまたは有線での
インターネット接続



**咽頭専用
カメラ**

**専用
クラウドサーバー**

**通信機能をもつ
汎用タブレットもしくは汎用PC**

STEP 2 クラウドからカメラへ
患者情報をDownload

STEP 3 カメラからクラウドへ
咽頭画像をUpload

咽頭画像の撮影を行う

STEP 4

問診情報と咽頭画像から
クラウドAIの推論を実施

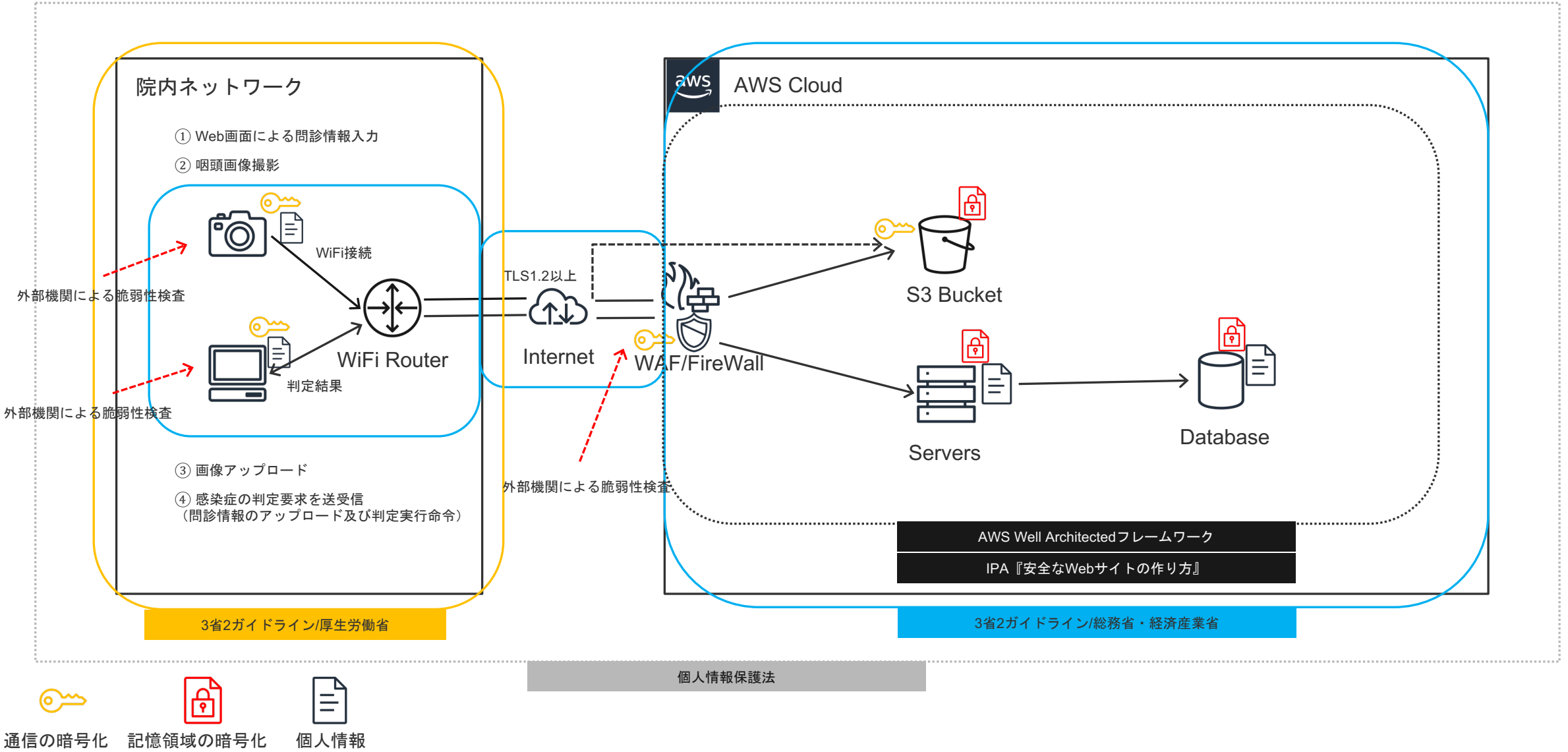
STEP 1 端末からクラウドへ
患者情報と問診情報をUpload

STEP 5 クラウドから端末へ
咽頭画像と判定結果をDownload

問診データの閲覧・入力、咽頭画像の閲覧、
感染症判定の実行・判定結果の閲覧

セキュリティ対応・取り組みのご紹介

製品とセキュリティ概要



当社のセキュリティ対応・取り組み

■3省2ガイドライン等

- 3省2ガイドラインの準拠とその範囲の調査（6ヶ月以上のPJT発足）
- 自社製品の設計とセキュリティ設計が3省2ガイドラインの何に遵守しているのか調査（400項目以上）
- 遵守事項に関しては可能なかぎり対応、推奨事項については追って整備していく方向性
- AWSに掲載の『日本の医療情報ガイドライン』を制度上の要求事項として参考にした

■社内規程等

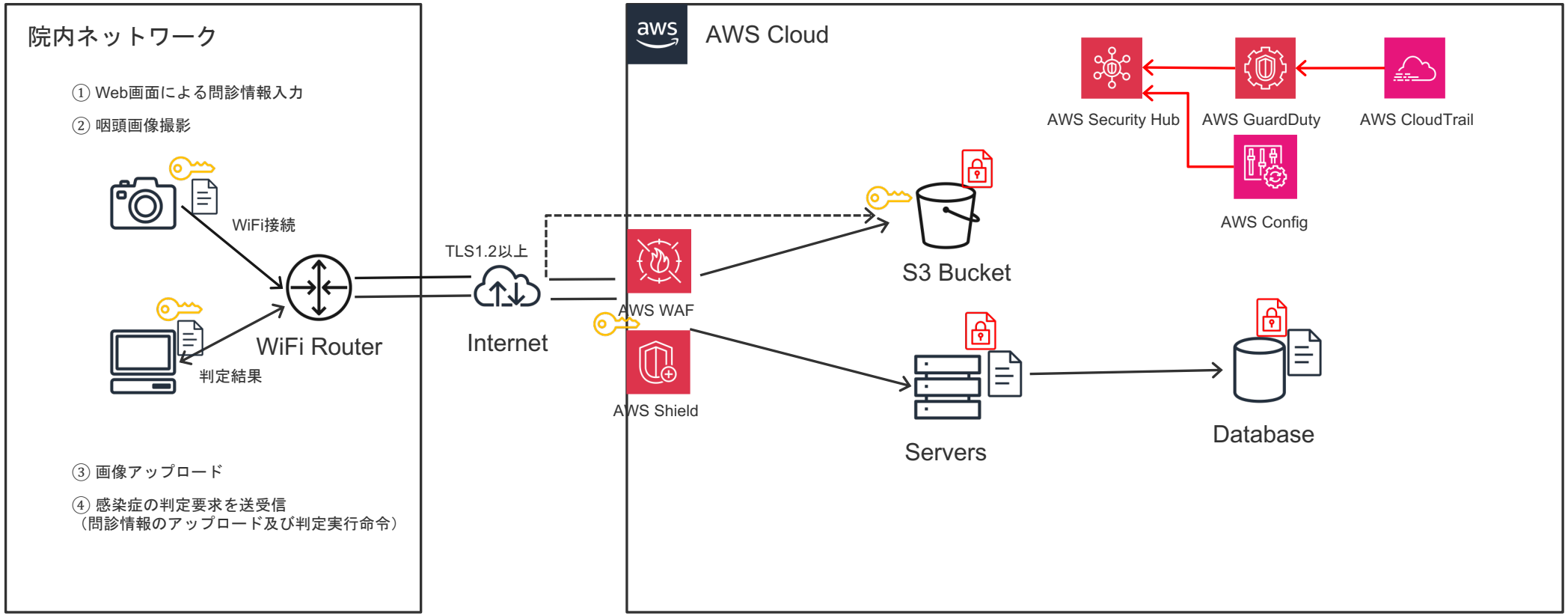
- 「AWS Well-Architected フレームワーク」を元にAWS設計・運用の自社ルールを整備、チーム内に展開
- 運用管理規程に準ずるものとして「システム管理マニュアル」を制定しエンジニア部門へ展開
- 情報セキュリティ規程、マニュアルなどを制定し全社へ展開

■主なセキュリティ対策

- 個人情報を扱う通信やそれを格納する記憶領域の暗号化
- 外部からの不正アクセスを防御・検知する仕組みを実装
- AWSは国内リージョンに限定
- アクセスは国内IPからのみ受け付ける設定
- システムにアクセスできる人員は限定し操作ログ（コンソールログ含む）を取得する
- 外部機関による脆弱性検査を実施し安全を確認

AWS機能を用いたセキュリティ対策

AWS セキュリティ対策



通信の暗号化　記憶領域の暗号化　個人情報

AWS セキュリティ対策　防御

AWS WAF

- AWS WAFを用いて主にL7以上の不正アクセスに備える
- IPアドレス制限など
- WAFのシグネチャ・ルールに反した通信はアラート通知
- 定期的に通信ログを確認しMTGなどで傾向をチーム内で共有

AWS Shield

- 不正な通信(Dos,DDosなど)はAWS Shieldの機能に任せる
- レイヤー3及び4を標的とした既知の攻撃すべてから包括的に保護

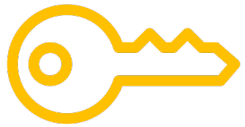
AWS セキュリティ対策　検知・暗号化

Amazon GuardDuty

- AWSのS3やVPCアカウント全体、アカウント内の異常な動きを分析
- システム運用者の操作や通信ログから、不正利用やマルウェア感染など疑わしい動きを検知
- 設定変更などもアラート通知、意図した動きかどうかチーム内で確認

記憶領域の暗号化

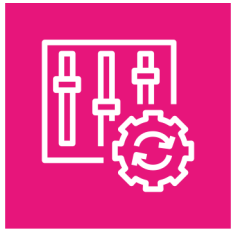
- サーバー記憶領域(EBS)の暗号化
- DBクラスターの暗号化
- S3バケットの暗号化



通信の暗号化

- 通信はACM等を用いてHTTPS化

AWS セキュリティ対策　監査・管理

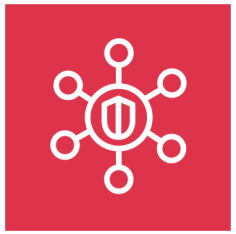


AWS Config

- あらかじめ定義したルールセットを監視
- 設定の不備などを発見し通知

AWS CloudTrail

- AWSコンソールなどの変更履歴を取得
- 取得したデータはCloudWatchに反映し通知



AWS Security Hub

- 検出結果の集中管理ツール機能
- GuardDutyの通知,CloudTrailのセキュリティ機能の一部通知、AWSConfigの通知などを集約
- Security Hub 標準機能を活用しセキュリティスコア対応

主なセキュリティ対策　まとめ

- カメラ及びWeb画面の通信（画像・患者情報）は暗号化（TLS1.2以上）をしている
- FireWall及びWAFにより外部からの不正なアクセスをブロックし監視している
- クラウド及びカメラは国内のIPアドレスのみアクセスできる状態にしている
- クラウドに格納されるデータは国内リージョンに限定している
- クラウドに格納されるデータ及びDBは記憶領域の暗号化をしている
- システムにアクセスできる人員は限定し操作ログ（コンソールログ含む）を取得している
- 外部機関による脆弱性検査を実施している

今後の課題

■ガイドライン等

- 3省2ガイドラインの改正箇所のキャッチアップが必要、仕組みや体制から検討
- サービス適合開示書など求めに応じて開示する情報をより精緻にまとめていく
- 薬機法における基準の改正により2024年4月以降は医療機器のセキュリティ対策は必須

■技術面

- SBOM（Software Bill Of Materials）の管理及びアップデート
- EOS（End of Support）/ EOL（End of Life）の管理

■運用面

- セキュリティ検知・通知内容の視認性を向上させる活動
- アラート通知の粒度調整と初動体制の構築・運用（CERT体制）

ご清聴ありがとうございました。