

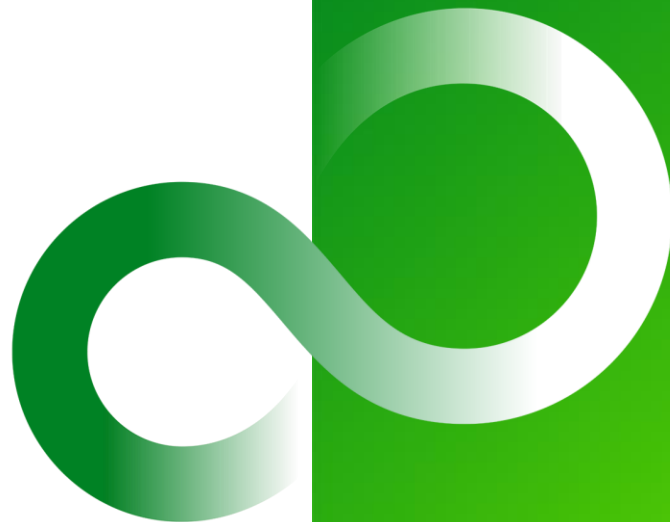
医療サイバーセキュリティ協議会 御中

FUJITSU

医療機関における マネージドセキュリティサービス

2022年11月1日

富士通株式会社



セキュリティ10大脅威と医療機関の対応状況

●ランサムウェアや標的型攻撃の脅威を感じるも対応は後手の傾向

順位	2022年の10大脅威	医療機関の対応状況	
1位 →	ランサムウェアによる被害		インシデント発生後に検討着手の傾向
2位 →	標的型攻撃による機密情報の窃取		インシデント発生後に検討着手の傾向
3位 ↗	サプライチェーンの弱点を悪用した攻撃		今後の検討ポイント
4位 ↘	テレワーク等のニューノーマルな働き方を狙った攻撃		今後の検討ポイント
5位 ↗	内部不正による情報漏えい		今後の検討ポイント
6位 ↗	脆弱性対策情報の公開に伴う悪用増加		システムベンダー連携で対応
7位 NEW	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）		今後の検討ポイント
8位 ↘	ビジネスメール詐欺による金銭被害		研修対応など実施
9位 ↘	予期せぬIT基盤の障害に伴う業務停止		システムのサービスレベル設計で対応
10位 ↘	不注意による情報漏えい等の被害		研修対応など実施

※ 独立行政法人 情報処理推進機構. “情報セキュリティ10大脅威 2022” <https://www.ipa.go.jp/security/vuln/10threats2022.html>

● 外部からの攻撃に加えて、ルール不備による情報漏えいも多数発生

医療機関でのセキュリティ事故件数
(2019年1月～2022年3月で集計)

132 件

外部から
の攻撃

標的型攻撃 : 13 件

不正アクセス : 13 件

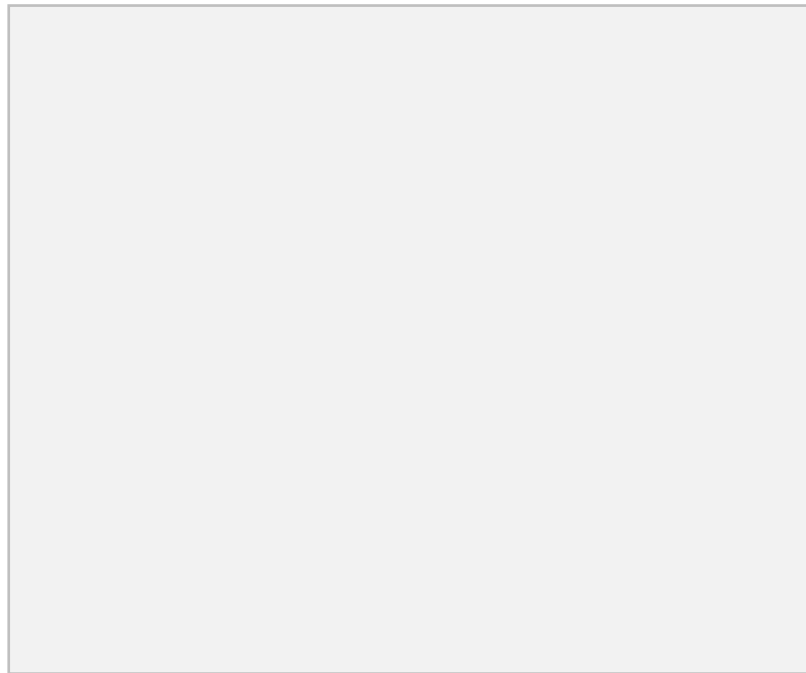
人為的事故

内部不正 : 2 件

ルール等の不備 : 49 件

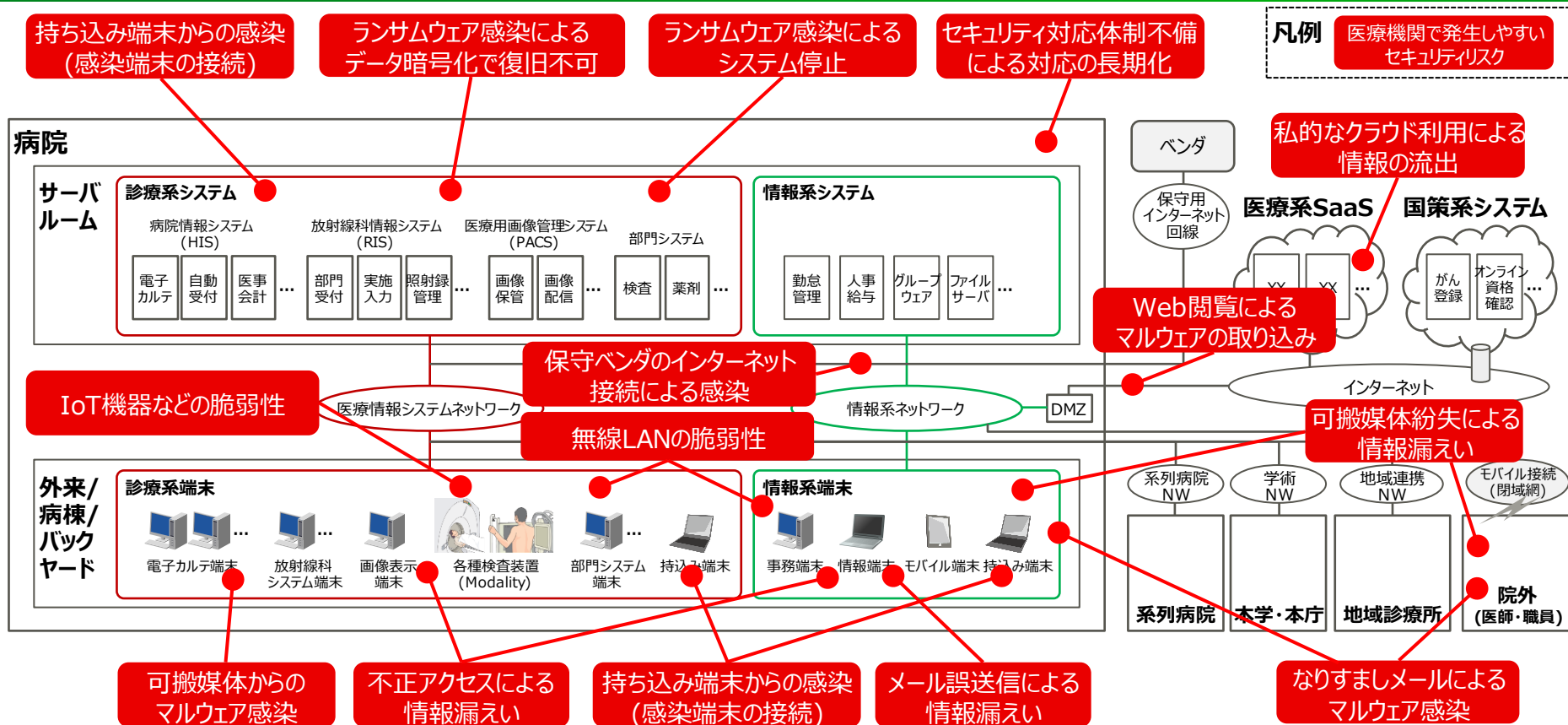
他 (過失等) : 55 件

～ 例 ～

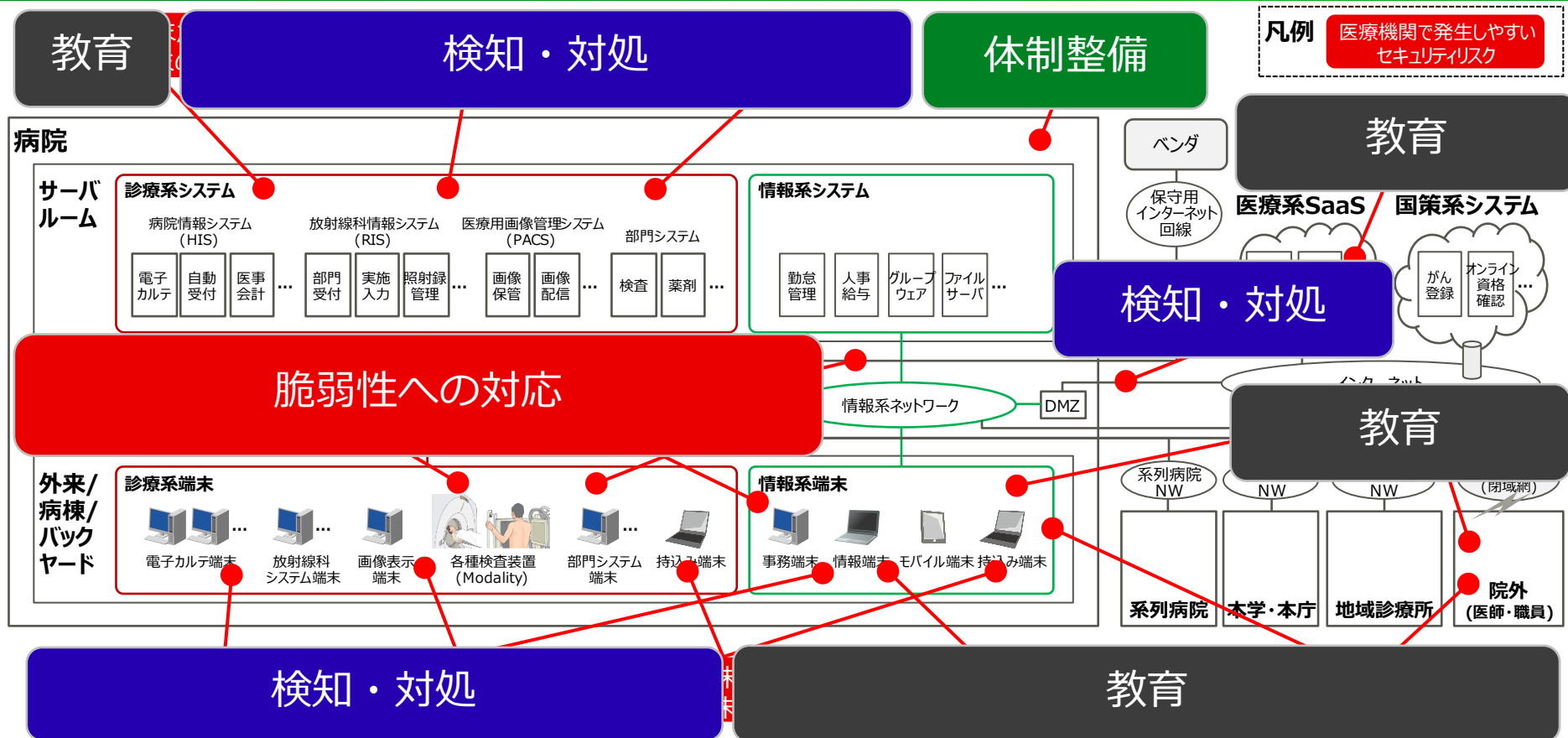


※出所: Security NEXTより <https://www.security-next.com/category/cat191>

医療機関のセキュリティリスクポイント



医療機関のセキュリティリスクポイント



セキュリティ対策に対する富士通の考え方

●被害を極小化するために早期に対処できる仕組み作りが重要

- ガイドラインへの対応を前提に従来対策の見直し、強化に加え、新たな攻撃手段に対応することで攻撃を早期検知し、増大する運用負荷の軽減と迅速な対処を可能にします

従来対策の 棚卸	・既存のウイルス対策の見直し ・ファイアウォール(外部ネットワークとの出入り口)の設定、ネットワーク構成、バックアップ構成等の見直し ・各システムにおける脆弱性の管理		脆弱性 への対応
新たな 攻撃への 対応	・従来の方法で防げない未知のマルウェア対策 ・乗っ取られた脆弱なIoT機器からの攻撃への対応 ・医療機関で増加しているサイバー攻撃への対策の検討		検知・対処
運用負荷の 軽減	・セキュリティ運用を効率化するための仕組みの導入 ・侵入されたあとの迅速な復旧体制の構築 ・新たな脅威に対応できる人材の育成		体制整備 教育

- 厚労省ガイドラインにおいても、運用面の対応が多く記載あり、医療機関にて検討が必要な状況

医療情報システムの安全管理に関するガイドライン 5.2版

※[B.考え方]部分を抜粋

記載項目	6.5. 技術的安全対策			6.6. 人的安全対策		6.10. 災害、サイバー攻撃等の非常時の対応	
	アクセスログ	不正ソフトウェア対策	NW上からの不正アクセス	教育		サイバー攻撃を受けた際の対応	非常時に備えたセキュリティ体制の整備
具体的な作業	ログ収集・管理	スキャン用ソフトウェアの適切な運用	脆弱性への定期的な診断	サイバー攻撃に対して従業員への教育		影響の波及防止のためのネットワーク切断・業務システム停止	情報セキュリティ責任者の設置
	ログ分析	脆弱性へのパッチ適用	FW/IPS/IDSの導入			情報漏洩防止のための当該機器の隔離	緊急対応体制の整備
	緊急時にアラート発動	EDR/振る舞い検知の導入	内部脅威監視によるモニタリング			非常時に備えたバックアップ・復元	脆弱性情報収集・対策

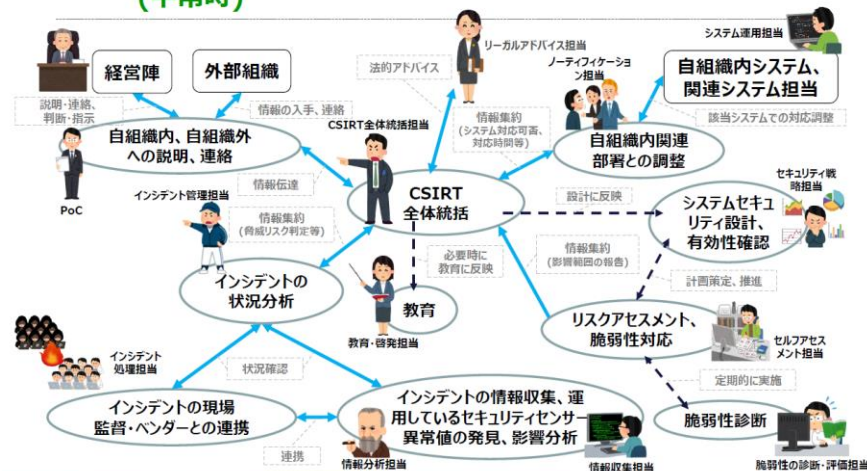
セキュリティ体制を整えるには

- セキュリティ体制を構築するには、多くの機能・役割(人材)を有する必要

平常時

4.19 CSIRTの役割と業務内容の関連図 (平常時)

実線は活動時の情報の流れ。
点線は必要時に実施する活動の流れ。



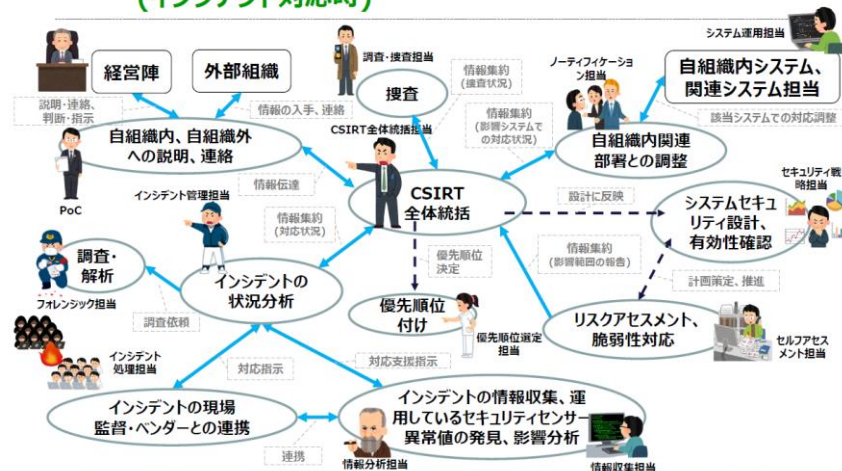
※ CSIRT運営管理担当は上記活動のバックグラウンドとして必要である。図には記載していない。
※ システム運用担当は、「自組織内システム、関連システム担当」と同じ場合もある。上記は同じ場合を示した。



インシデント対応時

4.19 CSIRTの役割と業務内容の関連図 (インシデント対応時)

実線は活動時の情報の流れ。
点線は必要時に実施する活動の流れ。



※ インシデントが発生し、CSIRTが対応している状態を「インシデント対応時」と定義。
※ 法的確認が必要な場合には、各役割からリーガルアドバイザーに支援を要請する。



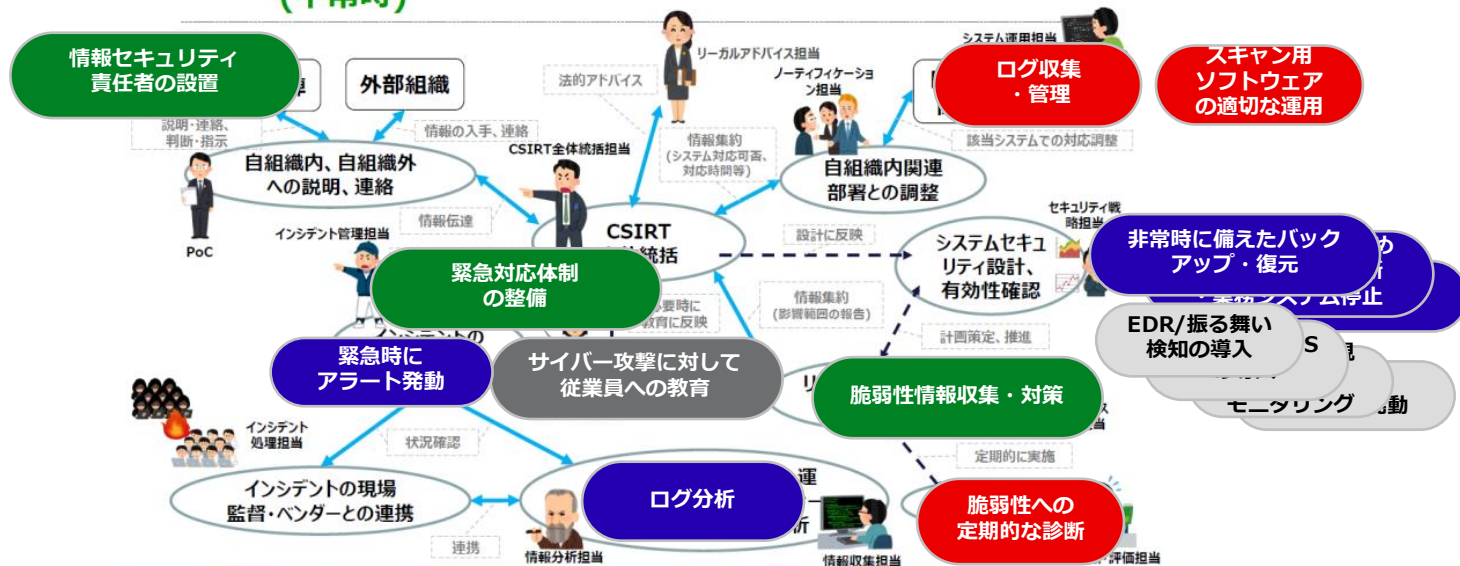
出典：日本コンピュータセキュリティインシデント対応チーム協議会「CSIRT人材の定義と確保 (Ver.2.1) (https://www.nca.gr.jp/activity/imgs/recruit-hr20201211.pdf)

セキュリティ体制を整えるには

- ガイドラインに記載のある項目をすべて対処しようとする・・・

4.19 CSIRTの役割と業務内容の関連図 (平常時)

実線は活動時の情報の流れ。
点線は必要時に実施する活動の流れ。



※ CSIRT運営管理担当は上記活動のバックグラウンドとして必要である。図には記載していない。
※ システム運用担当は、「自組織内システム、関連システム担当」と同じ場合もあれば、別の場合もある。上記は同じ場合を例示した。

- 自治体からの要請でセキュリティ強化を求められており、情報セキュリティポリシーの策定をしたい

- リスクアセスメントの実施
- 情報セキュリティポリシーの体系化
- CSIRT構築支援まで

運用の為の
課題整理

- 次世代FWを導入したものの、セキュリティ運用の知見を有する専門家がいらない

- アラート情報妥当性の判断ができない
- ログによるネットワーク上の不審な挙動の特定が難しい

SOC
サービス

お客様傾向

- ✓ **脆弱性対策など運用面への意識向上**
 - 脆弱性対策を検討
- ✓ **緊急対応体制(CSIRT等)の確立**
 - エスカレーション手順・体制の検討
- ✓ **EDR導入検討ユーザの増加**
 - EDR検討にあわせてSOC検討も
- ✓ **系列病院のセキュリティガバナンス強化**
 - 複数病院の情報系システムの統一化

サービスのニーズ

- ✓ **まずは現状の課題整理の為のサービス**

課題整理

 - 脆弱性診断
 - 体制・方針検討(コンサルティング)
 - 教育
- ✓ **SOCについてはまだ黎明期**

SOC

 - まだ一部のお客様にて検討している状況
 - EDR検討により広がっていく可能性あり
 - 複数病院のガバナンス強化は増加傾向
 - HIS閉域環境からの脱却も起点になる可能性あり

Thank you

