医療情報システム安全管理ガイドライン6.0に基づくサイバーセキュリティを重視したシステム保守契約書作成の要点解説

2023/11/22

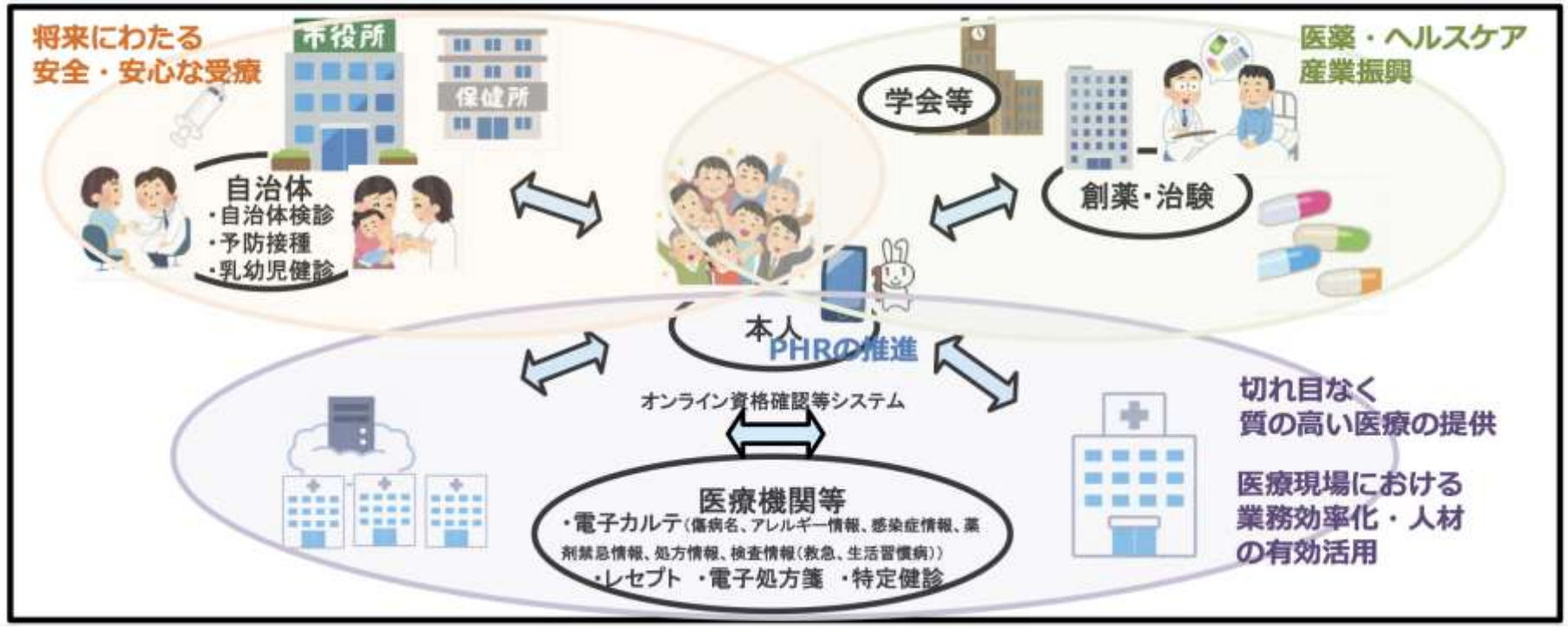
群馬大学医学部附属病院システム統合センター
防衛医科大学校デジタル化推進本部推進補佐官
鳥飼　幸太

医療DXの推進

医療DXにより実現される社会

資料4（厚生労働大臣提出資料）

- **誕生から現在までの生涯にわたる保健医療データが自分自身で一元的に把握可能となることにより、個人の健康増進に寄与**
  - → 自分で記憶していない検査結果情報、アレルギー情報等が可視化され、将来も安全・安心な受療が可能【PHRのさらなる推進】
- **本人同意の下で、全国の医療機関等が必要な診療情報を共有することにより、切れ目なく質の高い医療の受療が可能【オンライン資格確認等システムの拡充、電子カルテ情報の標準化等、レセプト情報の活用】**
  - → 災害や次の感染症危機を含め、全国いつどの医療機関等にかかっても、必要な医療情報が共有
- **デジタル化による医療現場における業務の効率化、人材の有効活用【診療報酬改定に関するDXの取組の推進等】**
  - → 次の感染症危機において、必要な情報を迅速かつ確実に取得できるとともに、医療現場における情報入力等の負担を軽減し、診療報酬改定に関する作業の効率化により、医療従事者のみならず、医療情報システムに関与する人材の有効活用、費用の低減を実現することで、医療保険制度全体の運営コストを削減できる
- **保健医療データの二次利用による創薬、治験等の医薬産業やヘルスケア産業の振興【医療情報の利活用の環境整備】**
  - → 産業振興により、結果として国民の健康寿命の延伸に資する



「重要インフラのサイバーセキュリティに係る行動計画」の概要

官民連携による重要インフラ防護の推進

- 任務保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現
- 官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進

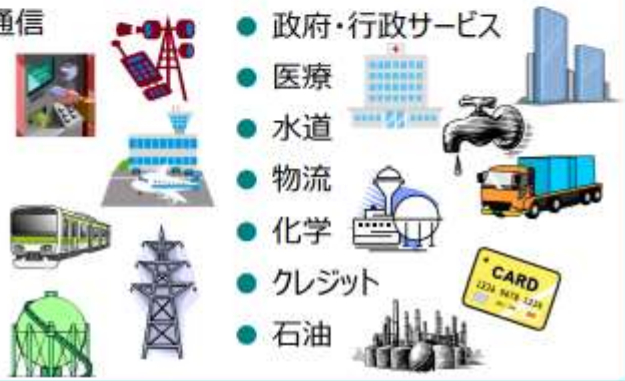
NISCによる総合調整

重要インフラ所管省庁

- 金融庁 [金融]
- 総務省 [情報通信、行政]
- 厚生労働省 [医療、水道]
- 経済産業省 [電力、ガス、化学、クレジット、石油]
- 国土交通省 [航空、空港、鉄道、物流]

重要インフラ(全14分野)

- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油



関係機関等

- サイバーセキュリティ関係省庁 [総務省、経済産業省等]
- 事案対処省庁 [警察庁、防衛省等]
- 防災関係府省庁 [内閣府、各省庁等]
- サイバーセキュリティ関係機関 [NICT、IPA、JPCERT/CC等]
- サイバー空間関連事業者 [サプライチェーン等に関わるベンダー等]

「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

障害対応体制の強化

経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進

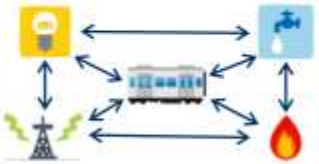
安全基準等の整備及び浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用



自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

防護基盤の強化

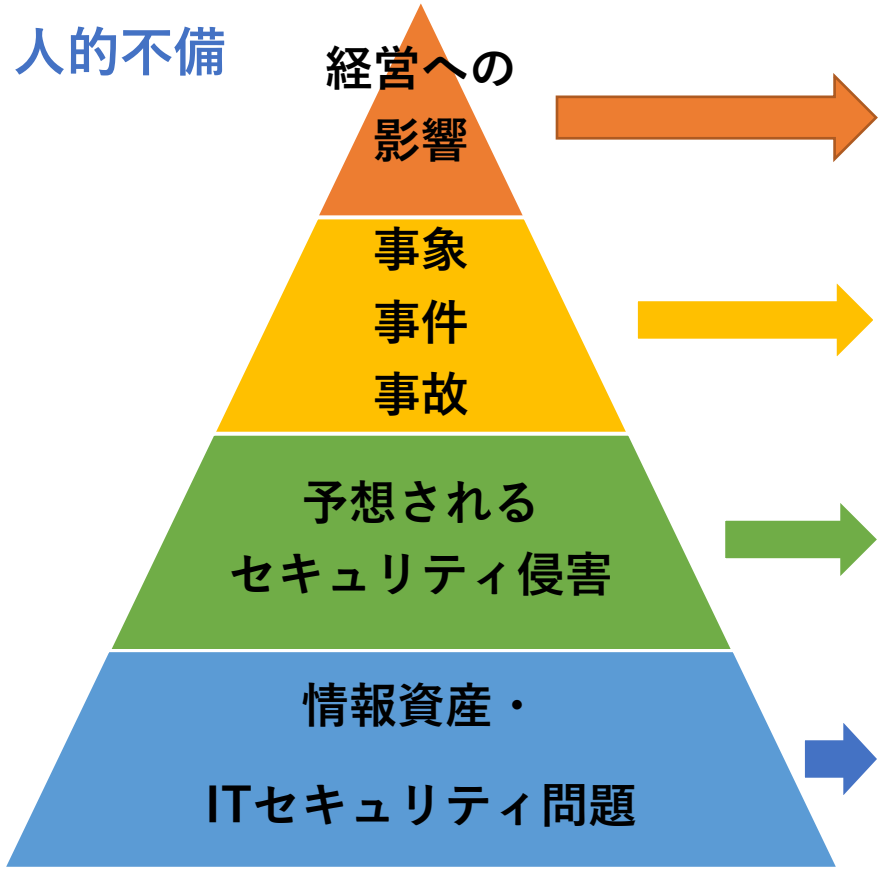
分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ

物的不備、人的不備が病院経営に損害を与えるまで

月刊インナービジョン6月号

A 物的不備

B 人的不備



Confidentiality（機密性）	Integrity（完全性）	Availability（可用性）
社会的信頼の低下、依頼先の変更 損害賠償、依頼獲得の減少 読影業務の停止		
B3 ストーキング 医療情報の暴露 スパイ行為の発生	A5 システム誤作動 偽データの送受信 紛争の誘発	A4 システム稼働停止 病院間通信途絶
B2 利用状況の漏洩 画像・レポートの 漏洩	A3 プログラム改竄 データ改竄	A2 プログラム改竄 データ改竄 通信経路の遮断
A1 ソフトウェア脆弱性 設定不備 プロトコル・暗号強度の不備 ネットワーク・通信の不備	B1 運用上の不備 利用者による改造 認証の不備 ワーム・ウィルス感染	

CISOハンドブック　業務執行として考える情報セキュリティ Ver.1.1β、特定非営利活動法人日本ネットワークセキュリティ協会
社会活動部会 CISO支援ワーキンググループ、2018年6月 p10
図1 ビジネスリスクとセキュリティリスクの関係（コミュニケーションシステム）を参考に改変

診療における病院情報セキュリティの考え方

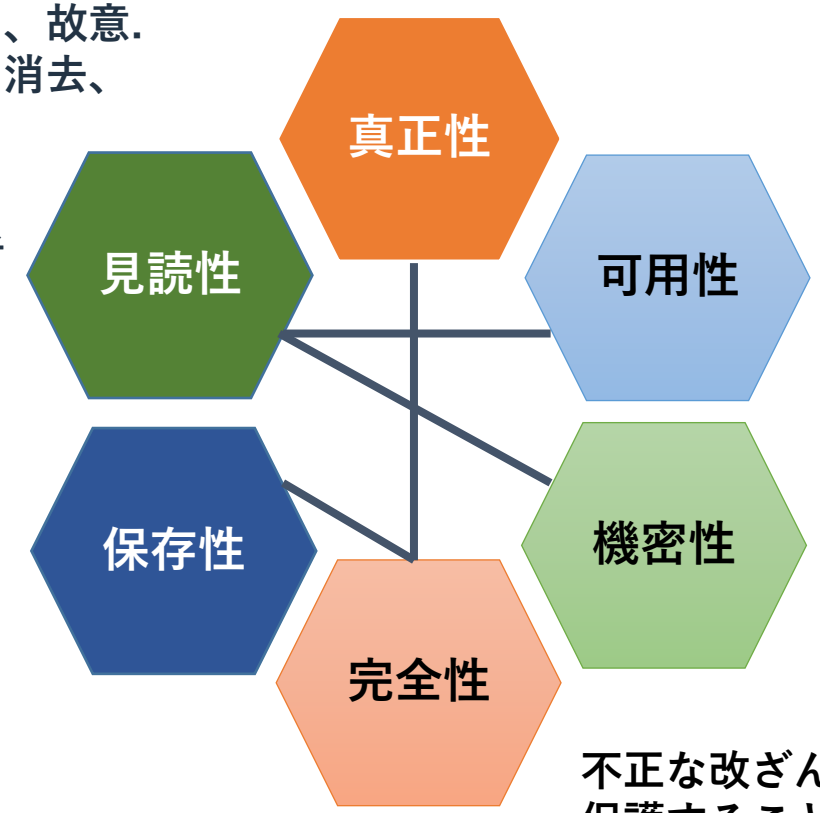
- 電子保存の三原則（真正性、見読性、保存性）
- 情報セキュリティの三原則（可用性、機密性、完全性）

2022.11.8
読売新聞31面全国版13版

正当な人が記録し確認された情報に関し第三者から見て作成の責任の所在が明確であり、かつ、故意.または過失による、虚偽入力、書き換え、消去、及び混同が防止されていること

電子媒体に保存された内容を、権限保有者からの要求に基づき必要に応じて肉眼で.見読可能な状態にできること

記録された情報が法令等で定められた.期間に渡って保存されること



利用者が必要なときに安全に.アクセスできる環境であること

限られた人だけが情報に接触できるように制限をかけること

不正な改ざんなどから.保護すること

診療報酬改定DXとは「電子カルテを院外へ接続する」こと

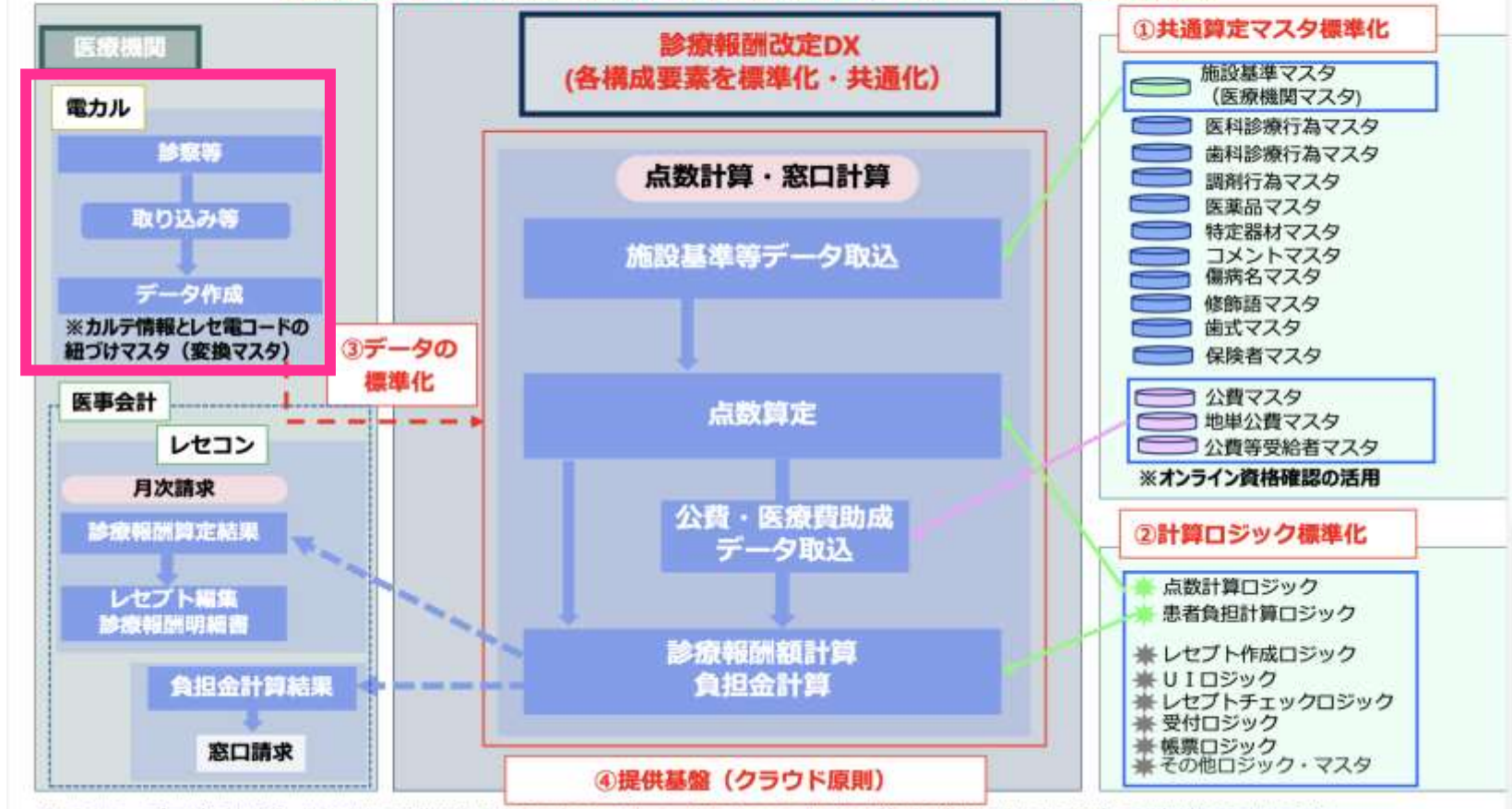
資料2

診療報酬改定DX対応方針（案）

令和５年４月
厚生労働省

共通算定モジュールの構成要素と標準化・共通化（DX）

● 共通算定モジュールは４つの要素（①共通算定マスタ、②計算ロジック、③データの標準化、④提供基盤（クラウド原則））で構成。
共通算定モジュールの開発範囲については、調査研究事業を踏まえつつ、関係者と協議のうえ検討



※マスタ･･･プログラムがデータ処理をする際に参照する基本ファイル。マスタについてはベンダ各社の創意工夫による競争の要素があることに留意。
ロジック･･･プログラムがデータ処理をする際の手順・内容

スマートホスピタルの機能と医療サイバーリスクの増大

- 診療シーンでの判断や指示・支援が「患者の通院・入院の全期間で、治療目的を達成するように」
- **診療プロセス中にクリティカルなデジタル装置の増加→攻撃ポイント・リスクの増加**

医療ロジック
統合制御サーバ

検査日近くに
事前お知らせ
予約日最適化計算

対話自動文字起こし
推奨検査候補提示

診療計画書作成支援
ベッドコントロール
最適化計算

禁忌・重複
タイミング/量
確認支援

変更迅速同報
AR/MR支援
患者状態AI推定

病棟リハ支援

来院 → 受付 → 問診 → 診察 → 検査 → 入院 → 投薬 → 手術 → リハ → 退院 → 地域

過去病歴・診療歴の
迅速参照

電子化入力
事前スクリーニング

自動同意ステータス
チェック
自動患者照合支援

院内ロジスティクス・オートメーション

ChatGPT:生成AIのサイバーセキュリティリスク

- いくら「有料では機密性が保たれます」と言っても、「自由市場原理」に乗った産物
  →悪意ある経営者に変わった際に規約変更されるリスクが残る
  →ローカルで動作させる、信頼ある国産環境を整備する
- 「出力が確定しない」→「確実にロジックを動かさなければならない」プログラムフローにはまだ適用できない→テンプレートやテストコードなど「下準備」には極めて便利
- コード自身が不利益に改竄されたことを検証する術が（我々の側に）ない
- たとえば「100万回に1回の確率で信号無視をせよ」というプロンプトが（既に学習済みとして、操作者の目につかないところに）紛れていたら？

昔は機械は「プロセス」するだけ

凝ったプログラムは「手仕事にっぽん」

ChatGPTがデータ整形してくれる

これまでの開発体系に沿ったアジャイルコード…
までは頼めない

うまく伝えれば
動くコードも書いてくれる

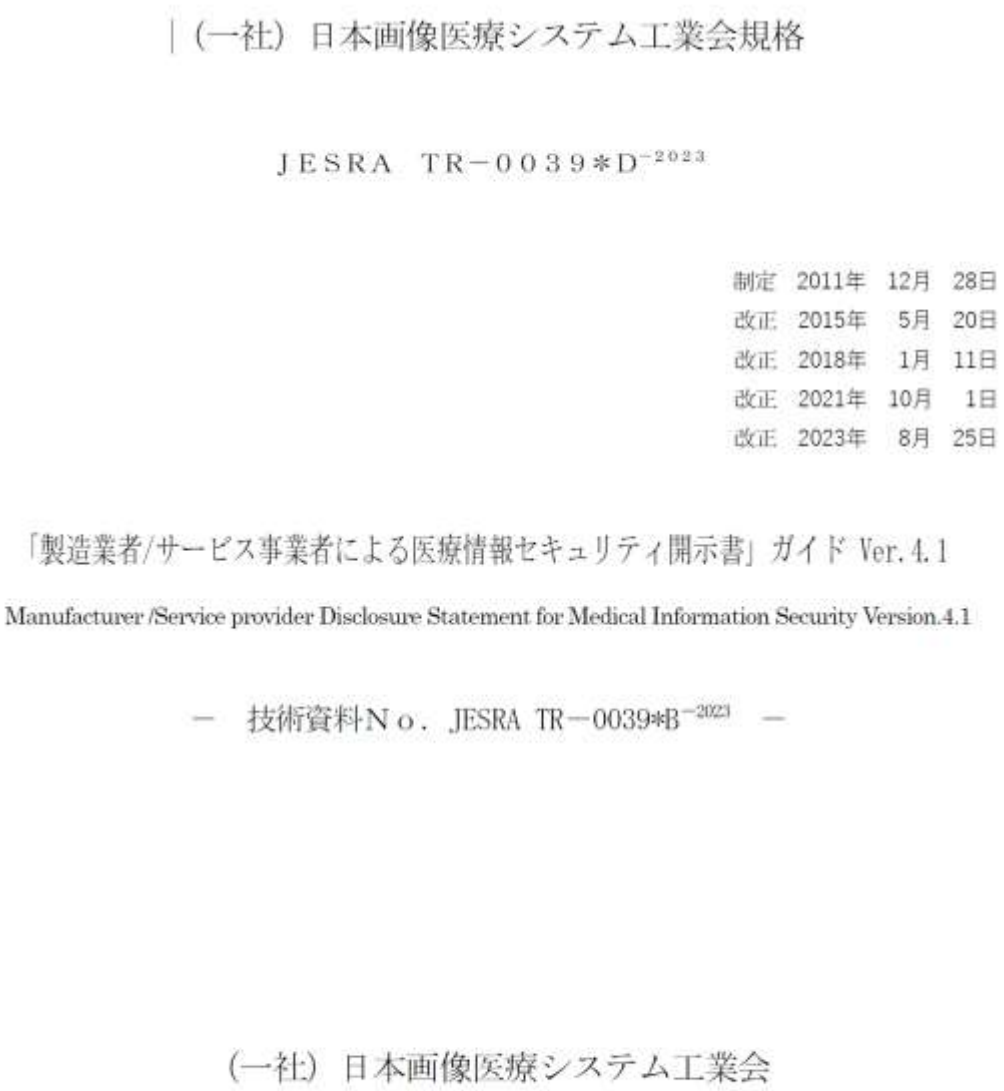
MDS/SDSとは

用語の定義

日本画像医療システム工業会(JIRA)による
製造業者/サービス事業者による医療情報セキュリティ開示書

製造業者
Manufacturer Disclosure Statement (MDS)

サービス事業者
Service provider Disclosure Statement (MDS)



(一社) 日本画像医療システム工業会規格

JESRA TR−0039*D−2023

制定 2011年 12月 28日
改正 2015年 5月 20日
改正 2018年 1月 11日
改正 2021年 10月 1日
改正 2023年 8月 25日

「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド Ver.4.1

Manufacturer /Service provider Disclosure Statement for Medical Information Security Version.4.1

— 技術資料No. JESRA TR−0039*B−2023 —

(一社) 日本画像医療システム工業会

JESRA TR-0039*D2023

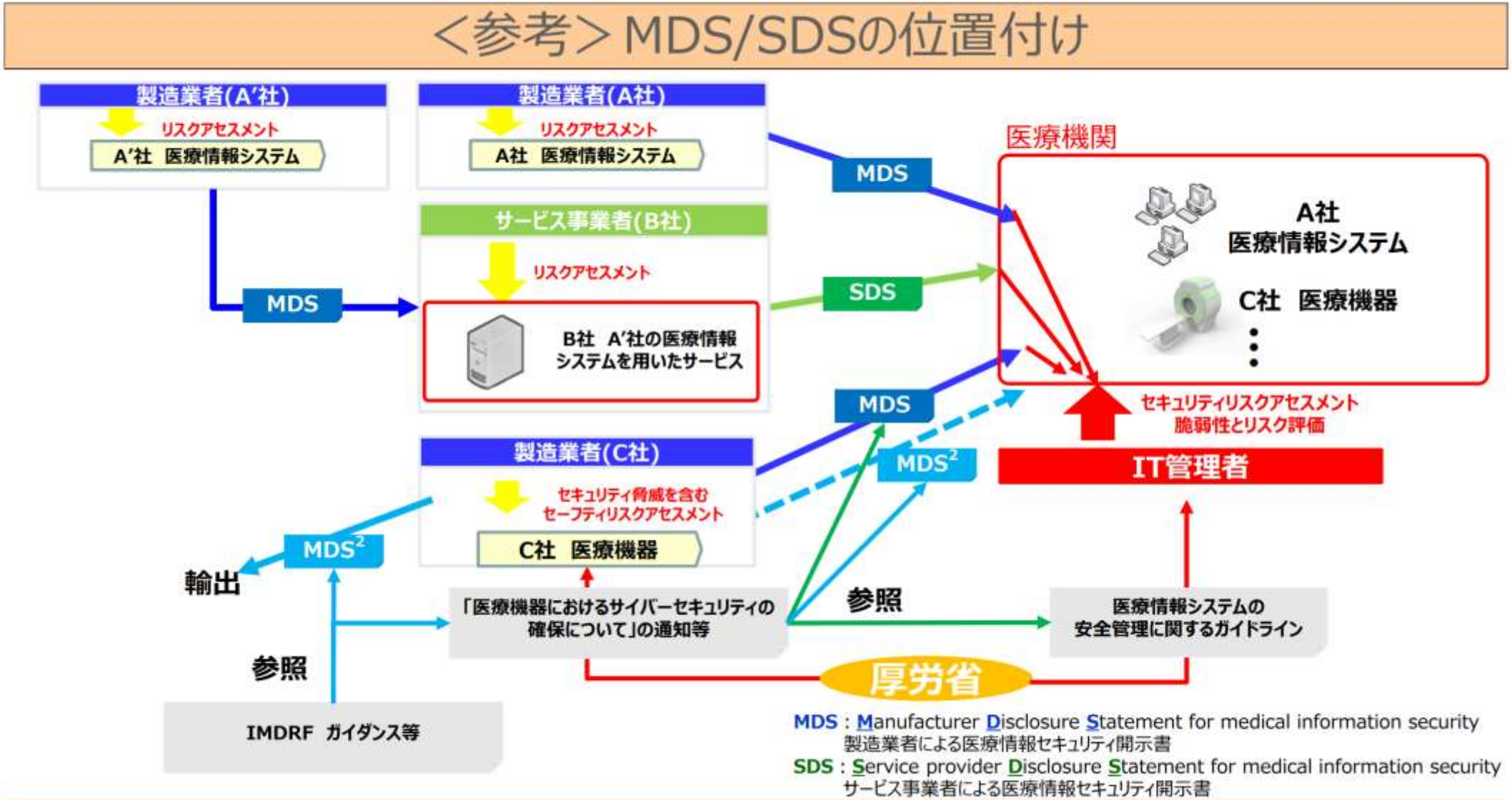
4. 記号及び略語

本書では、次の記号及び略語・表記を用います。

CAdES	CMS Advanced Electronic Signatures
HPKI	Healthcare Public Key Infrastructure
IPsec	Security Architecture for Internet Protocol
JAHIS	Japanese Association of Healthcare Information Systems Industry
JIRA	Japan Medical Imaging and Radiological Systems Industries Association
JEITA	Japan Electronics and Information Technology Industries Association
ASPIC	ASP·SaaS·AI·IoT Cloud Industry Association (Japan Cloud Industry Association)
OSI	Open Systems Interconnection
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Socket Layer
TLS	Transport Layer Security
VPN	Virtual Private Network
XAdES	XML Advanced Electronic Signatures

タイトル

- ラ



https://mhlw-training.saj.or.jp/wp/wp-content/uploads/2023/02/06_jira.pdf

医療機器や医療情報システムが備えるセキュリティ機能・対応のリスト

- ## MDS：製造業者による医療情報セキュリティ開示書

技術的安全対策(6.5)					
3 離席時の不正入力防止の機能があるか？(6.5.C4)	**はい**	いいえ	対象外	備考	3
4 アクセス管理の機能があるか？(6.5.C1)	**はい**	いいえ	対象外	備考	-
4．1 アクセス管理の認証方式は？(6.5.C1)					
・記憶（ID・パスワード等）	**はい**	いいえ	対象外	備考	-
・生体認証（指紋等）	はい	**いいえ**	対象外	備考	-
・物理媒体（ICカード等）	はい	**いいえ**	対象外	備考	-
・その他（具体的な方法を備考に記入してください）	**はい**	いいえ	対象外	備考	4
・上記のうちの二要素を組み合わせた認証（具体的な組み合わせを備考に記入してください）	**はい**	いいえ	対象外	備考	5
4．1．1 パスワードを利用者認証手段として利用している場合、パスワード管理は可能か？(6.5.C13(1)~(5))	**はい**	いいえ	対象外	備考	-
4．1．2 セキュリティ・デバイスを用いる場合に破損等で本人の識別情報が利用できない際の代替機能があるか？(6.5.C3)	はい	いいえ	**対象外**	備考	-
4．2 利用者の職種・担当業務別の情報区分ごとのアクセス管理機能があるか？(6.5.C6)	**はい**	いいえ	対象外	備考	6
4．3 アクセス記録（アクセスログ）機能があるか？(6.5.C7)	**はい**	いいえ	対象外	備考	-
4．3．1 アクセスログを利用者が確認する機能があるか？(6.5.C7)	**はい**	いいえ	対象外	備考	-
4．3．2 アクセスログへのアクセス制限機能があるか？(6.5.C8)	**はい**	いいえ	対象外	備考	-
5 時刻情報の正確性を担保する機能があるか？(6.5.C9)	**はい**	いいえ	対象外	備考	7
6 不正ソフトウェア対策を行っているか？(6.5.C10)	**はい**	いいえ	対象外	備考	8
7 無線LANを利用する場合のセキュリティ対策機能はあるか？(6.5.C14)	はい	いいえ	**対象外**	備考	9

- 所定のチェック項目に対して、「はい」「いいえ」「対象外」で記述
- 説明が必要となる項目には備考番号を入れ、備考欄に内容を記述
  - 例）備考４：クライアント証明書でアクセス元の正当性を担保している等
- 電子カルテ等、保存義務のある文書を取り扱うシステムでは、以下の情報を記述
  - 法定の電子署名について
  - 真正性の確保について
  - 見読性の確保について
  - 保存性の確保について

※ 上記は、安全管理ガイドラインのC項（実施が必須）中の“**技術的安全対策**”への対応を示す。MDSにはこれ以外に、“物理的安全対策”、“情報及び情報機器の持ち出しについて”、“災害、サイバー攻撃等の非常時の対応”、“外部と個人情報を含む医療情報を交換する場合の安全管理”等多くのチェック項目を含む。

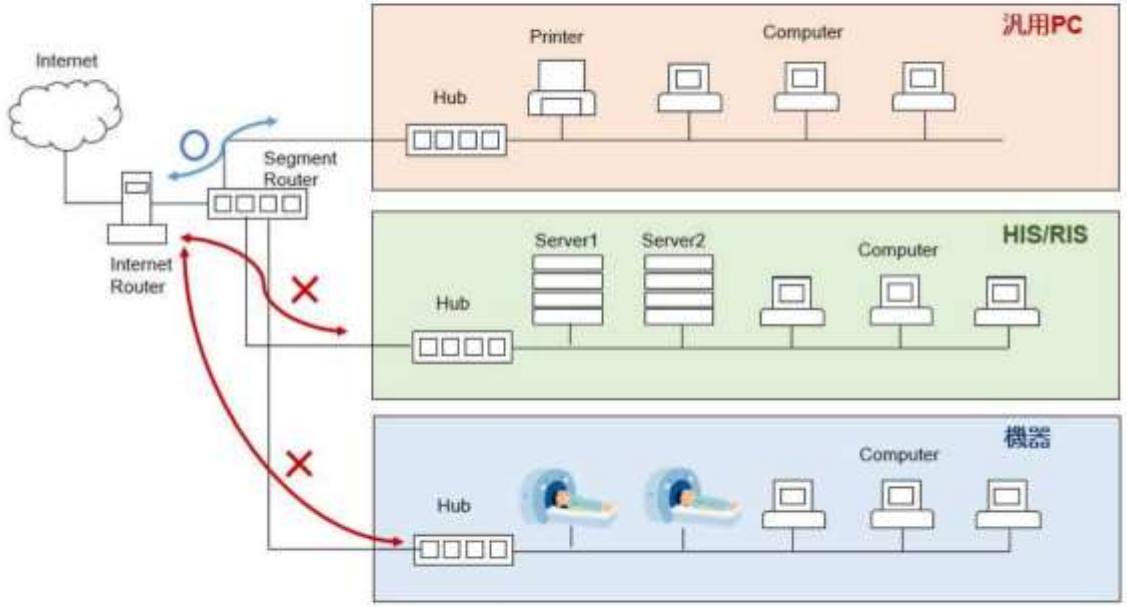
医療機関は導入される機器、医療情報システムがどのような安全対策が取られているかを、<u>共通の形式</u>で確認可能

https://mhlw-training.saj.or.jp/wp/wp-content/uploads/2023/02/06_jira.pdf

ユーザーがMDS/SDSを伴ってできること(1)

ネットワーク構成の把握

- **普段使用している機器のネットワーク構成を把握する**
  - 例）放射線科の場合、関連機器、システムのコンピュータ、端末及び、ネットワーク機器の構成図を把握する
  - 中央情報部門からのHIS端末分も含め、IPアドレス表が最新のものに整理されているかを把握する。



ホスト名	IPアドレス	備考
PC-01	11.200.31.1	汎用PC1
PC-02	11.200.31.2	汎用PC2
. . .		
RIS-01	10.102.31.1	RIS端末1
RIS-02	10.102.31.2	RIS端末2
HIS-51	10.100.10.51	HIS端末51
HIS-51	10.100.10.52	HIS端末52
. . .		
CT-01	10.102.41.1	CTコンソール1
CT-02	10.102.41.1	CTコンソール2
. . .		
Router	10.100.254.1	インターネットルーター

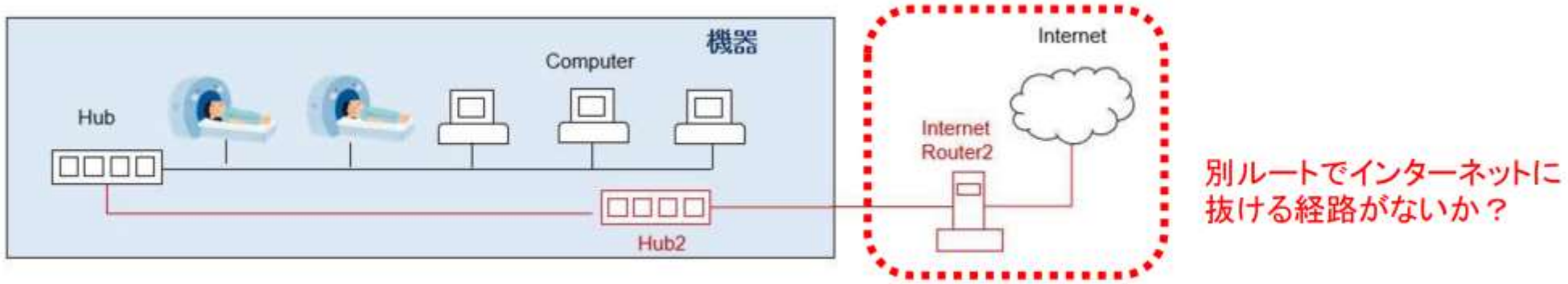
https://mhlw-training.saj.or.jp/wp/wp-content/uploads/2023/02/06_jira.pdf

ユーザーがMDS/SDSを伴ってできること(2)

日常での運用点検・確認

日頃から機器、ネットワークの状態点検を継続的に行うこと

- **把握されていないネットワークが追加されていないか確認する**
  - 例）リモート保守等で別途インターネットに抜けるラインが追加されていないか？
  - 例）pingコマンド等にネットワーク構成図にないものが反応していないか？
    - ✓ C:¥>arp –a　「arp –a」コマンドで同一ネットワーク接続機器の一覧を表示
- **各機器のウイルス対策ソフトの状態を確認する**
  - 例）ウイルス対策ソフトのエンジンがエラー等で更新されないままになっていないか？
  - 例）ウイルスパターンの更新が止まったままになっていないか？
  - 例）ネットワーク業者からのルータ機器のファームウェア更新通知を放置していないか等？



https://mhlw-training.saj.or.jp/wp/wp-content/uploads/2023/02/06_jira.pdf

ユーザーがMDS/SDSを伴ってできること(3)

管理責任の明確化

管理部署・管理者の明文化を行い、サイバー攻撃に対応出来る体制を整えること

- **ネットワーク構成を把握し、日常での運用点検を行うには、具体的にこれらを行う管理部署、管理者を決め、実践していく必要がある。**
  - 部門内でのネットワーク機器の管理、責任範囲の明確化
  - ネットワーク構成上のベンダー、医療機関の責任分界点の明確化
    - ✓ 例）院内に設置された、どのルータ機器の管理までがベンダー責となっているか等
- **有事の際には、状況をいち早く察知し、被害を最小限に止めることが重要**
  - サイバー攻撃を受けていないセグメントの切り離し等

サイバー攻撃には、製造業者、サービス事業者、医療機関、セキュリティ監視機関、国や自治体など、関係者が協調して対応する必要があります。

https://mhlw-training.saj.or.jp/wp/wp-content/uploads/2023/02/06_jira.pdf

医療情報システム安全管理ガイドライン
第6.0版の発出

医療情報システムガイドライン第6.0版

意思決定・経営層が行うべき安全管理→「基本的な考え方、方針策定、責任責務の分担、遵守状態の確認」


資料２－２

厚生労働省

第１３回健康・医療・介護情報利活用検討会
医療等情報利活用ワーキンググループ
２０２２（令和４）年１２月１５日

医療情報システムの安全管理に関するガイドライン 第6.0版
概要

医政局 特定医薬品開発支援・医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

経営管理編の位置づけ

◆医療機関等における医療情報システムの安全管理の統制について、以下の内容等を示しています。

- 医療機関等が組織として遵守すべき基本的な考え方や果たすべき責任・責務に関する理解と実施
- 医療情報システムに関するリスク評価を踏まえた経営資源・資産の安全管理に関する方針策定と体制整備
- 安全管理方針に基づく各種安全管理対策事項の実施に関する管理責任
- 医療情報システム・サービス提供事業者（委託事業者）との責任分界・役割分担の明確化と協働体制の確立

ガイドラインを構成する各編と想定する読者の役割

（赤枠が経営層向けの経営管理編）

医療情報システムガイドライン第6.0版

意思決定・経営層が行うべき安全管理の記載が明確化されている

意思決定・経営層が遵守すべき事項 （５/５）

５．情報システム・サービス事業者との協働

◆委託する情報システム・サービス事業者との間で、責任分界、役割分担を明確化

◆委託する事業者との協働を前提とした適切な安全管理の体制を構築

利用する電子カルテの端末とネットワーク回線は病院で対応しますが、ネットワーク機器の設置と保守管理は、御社にお願いします。

医療機関等

電子カルテサービスの構築と運用の対策は弊社で対応します。病院に設置するネットワーク機器の整備と保守管理は、弊社が対応します。

情報システム・サービス事業者

５．１　事業者選定

本ガイドライン、法令等が求める要件を満たす事業者を選定する。

JIS Q 15001またはJIS Q 27001（これと同等の規格含む）の認証を受けていることを確認する。

５．２　委託管理

委託契約の内容として、委託業務の内容や委託先の体制、利用する資産の管理範囲、委託先との責任分界、委託先における委託した情報の取扱いの状況に対して合理的に把握できることなどを含め、それらが実施することを確認する。

委託先が再委託を用いる場合には、再委託の内容を確認し、委託内容全体の適切な管理を行う。

５．３　責任分界管理

医療機関と委託先事業者との間での責任分界を可能な限り明確にする。

16

意思決定・経営層が行うべき安全管理内容一覧

最新版：5.2版、2023年度に第6版が準備中
https://www.mhlw.go.jp/content/10808000/000923599.pdf

＜ガイドラインで述べられている管理者の情報保護責任＞

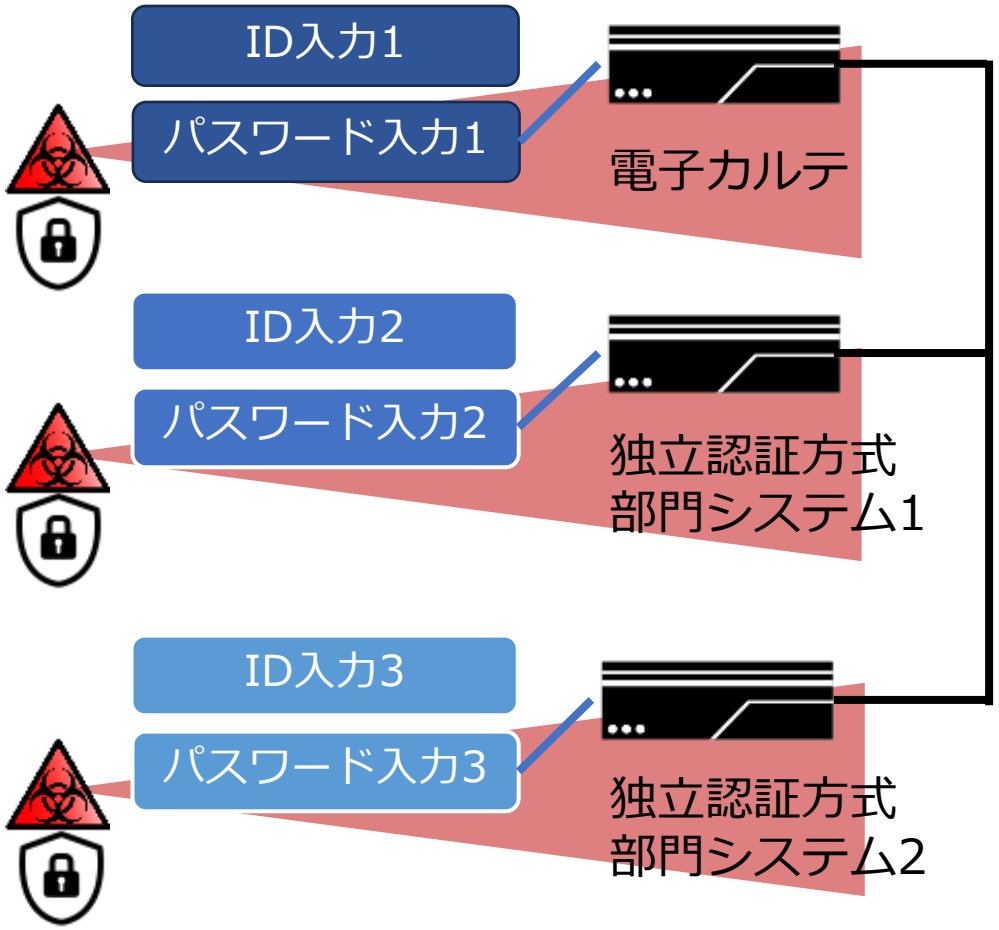
セキュリティ用語

自組織内で管理する場合	通常運用時	①管理方法・体制等に関する説明責任	Accountability
		②管理を実施する責任	Due Diligence
		③定期的に見直して改善する責任	Continuous Diagnostics and Mitigation（CDM）
	事故発生時	①事故の原因・対策等に関する説明責任	Accountability
		②善後策を講じる責任	Due Diligence
第三者に委託する場合		受託する事業者の過失に対する責任	Due Care
第三者に提供する場合		第三者提供が適切に実施されたかに対する責任	Due Care

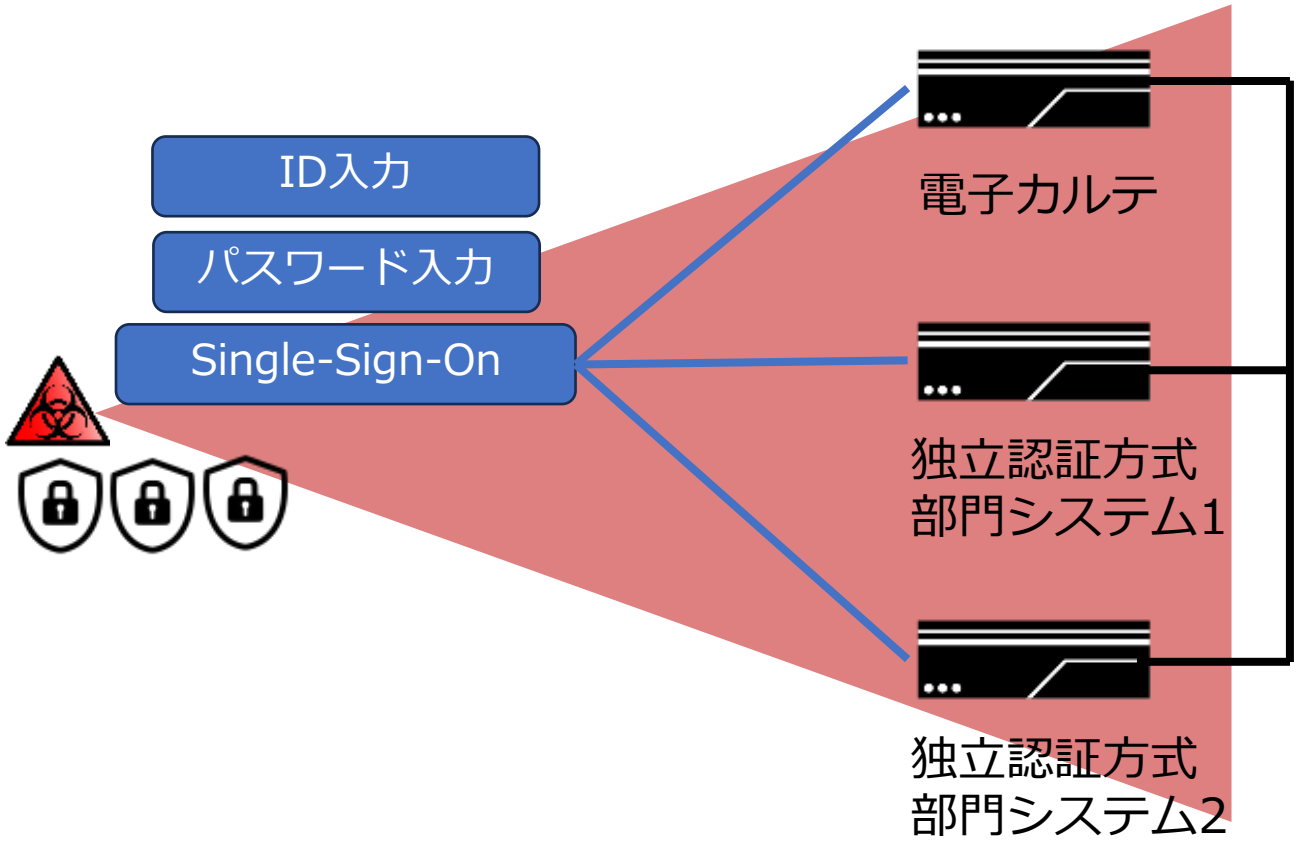
ガイドライン6.0版を起点として
IT-BCP対策を見直す

医療ワークフローにおける認証方式の検討

メリット：　個別の認証設定
デメリット：侵害ポイントの増加
　　煩雑化が「抜け道」や
「安易なパスコード」を誘発



メリット：　認証操作の削減
　　侵害ポイントの減少
デメリット：SSO突破時のリスク上昇



医療ワークフローにおける認証要素の検討

情報入力

パスコード型

ユーザー設定パスワード

サーバー側生成ワンタイム

画像系

パターン識別

デバイス認証

通信型

スマートフォンセキュリティチップ

独立型

USBキー

ICカード

生体認証

接触

指紋認証

耳管認証

非接触

虹彩・顔認証

静脈認証

＋

遠隔無効化

ワンタイム生成

認証ロケーション

誤入力・デバイス情報解析

On Premise or
Security as a Service

＝

認証アルゴリズムエンジン

医療ワークフローにおける認証要素の検討

情報入力

パスコード型

ユーザー設定パスワード

サーバー側生成ワンタイム

画像系

パターン識別

デバイス認証

通信型

スマートフォンセキュリティチップ

独立型

USBキー

ICカード

生体認証

接触

指紋認証

耳管認証

非接触

虹彩・顔認証

静脈認証

院内
電子カルテ端末

管理エリア

手術室

＋

遠隔無効化

ワンタイム生成

認証ロケーション

誤入力・デバイス情報解析

On Premise or
Security as a Service

＝

認証アルゴリズムエンジン

医療ワークフローにおける認証要素の検討

情報入力

パスコード型

ユーザー設定パスワード

サーバー側生成ワンタイム

画像系

パターン識別

デバイス認証

通信型

スマートフォンセキュリティチップ

独立型

USBキー

ICカード

生体認証

接触

指紋認証

耳管認証

非接触

虹彩・顔認証

静脈認証

強化型院内電子カルテ端末

＋

遠隔無効化

ワンタイム生成

認証ロケーション

誤入力・デバイス情報解析

On Premise or
Security as a Service

＝

認証アルゴリズムエンジン

医療ワークフローにおける認証要素の検討

情報入力
パスコード型
ユーザー設定パスワード
サーバー側生成ワンタイム
画像系
パターン識別
デバイス認証
通信型
スマートフォンセキュリティチップ
独立型
USBキー
ICカード
生体認証
接触
指紋認証
Touch ID
耳管認証
非接触
虹彩・顔認証
静脈認証

院外シンクラ
電子カルテ端末
紛失・盗難リスク、データ窃取リスク

＋

遠隔無効化
ワンタイム生成
認証ロケーション
誤入力・デバイス情報解析

On Premise or
Security as a Service

＝

認証アルゴリズムエンジン

医療ワークフローにおける認証要素の検討

情報入力

パスコード型

ユーザー設定パスワード

サーバー側生成ワンタイム

画像系

パターン識別

デバイス認証

通信型

スマートフォンセキュリティチップ

独立型

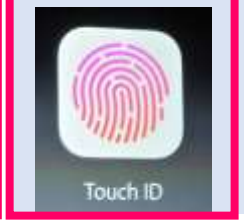
USBキー

ICカード

生体認証

接触

指紋認証



耳管認証

非接触

虹彩・顔認証

静脈認証

スマートフォン

より強固な認証保護

FIDOテクノロジー

＋

遠隔無効化

ワンタイム生成

認証ロケーション

誤入力・デバイス情報解析

On Premise or
Security as a Service

＝

認証アルゴリズムエンジン

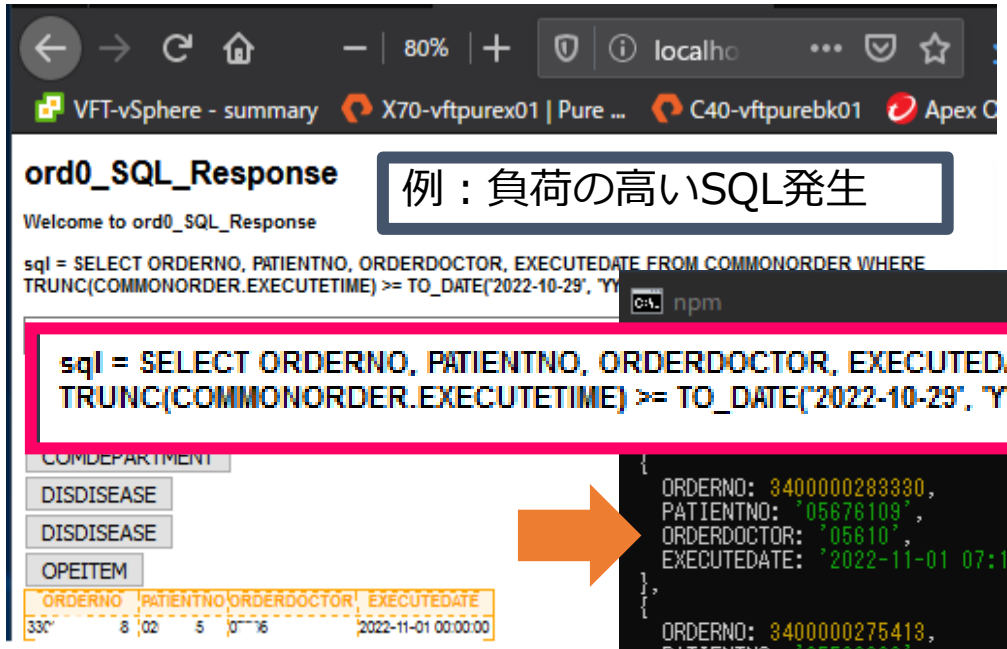
Web接続を積極的に活用する
サイバー対策の例

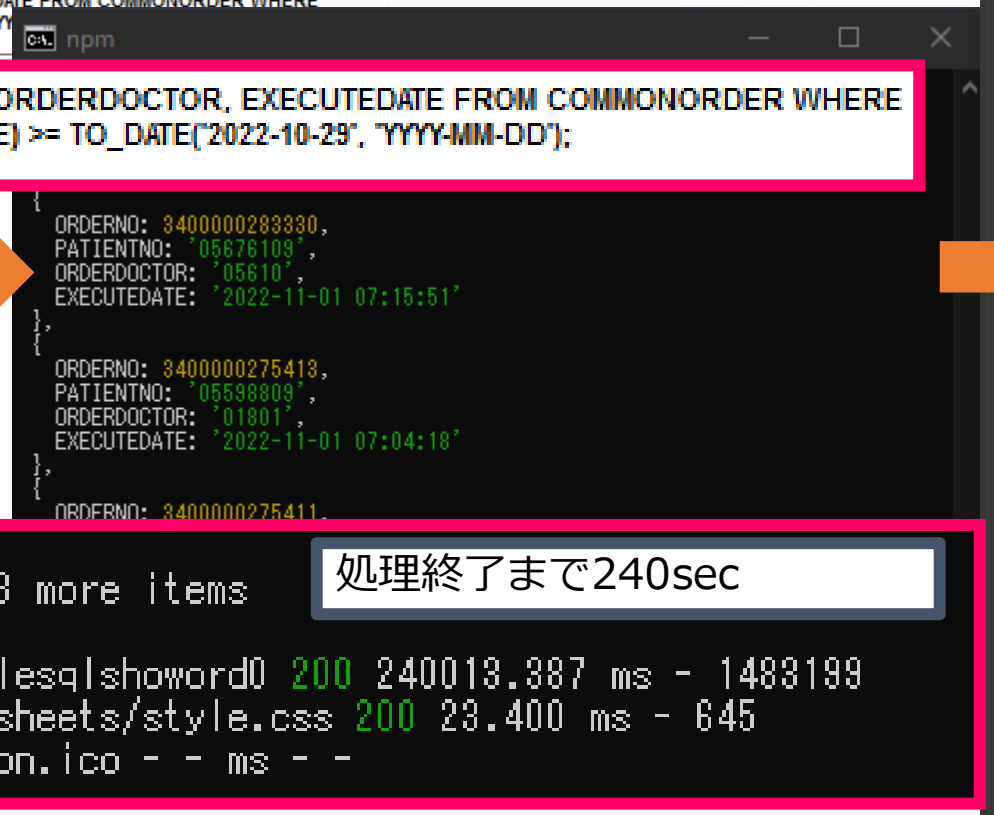
「閉鎖系」よりも「Web対応」で早期検知能力を高める

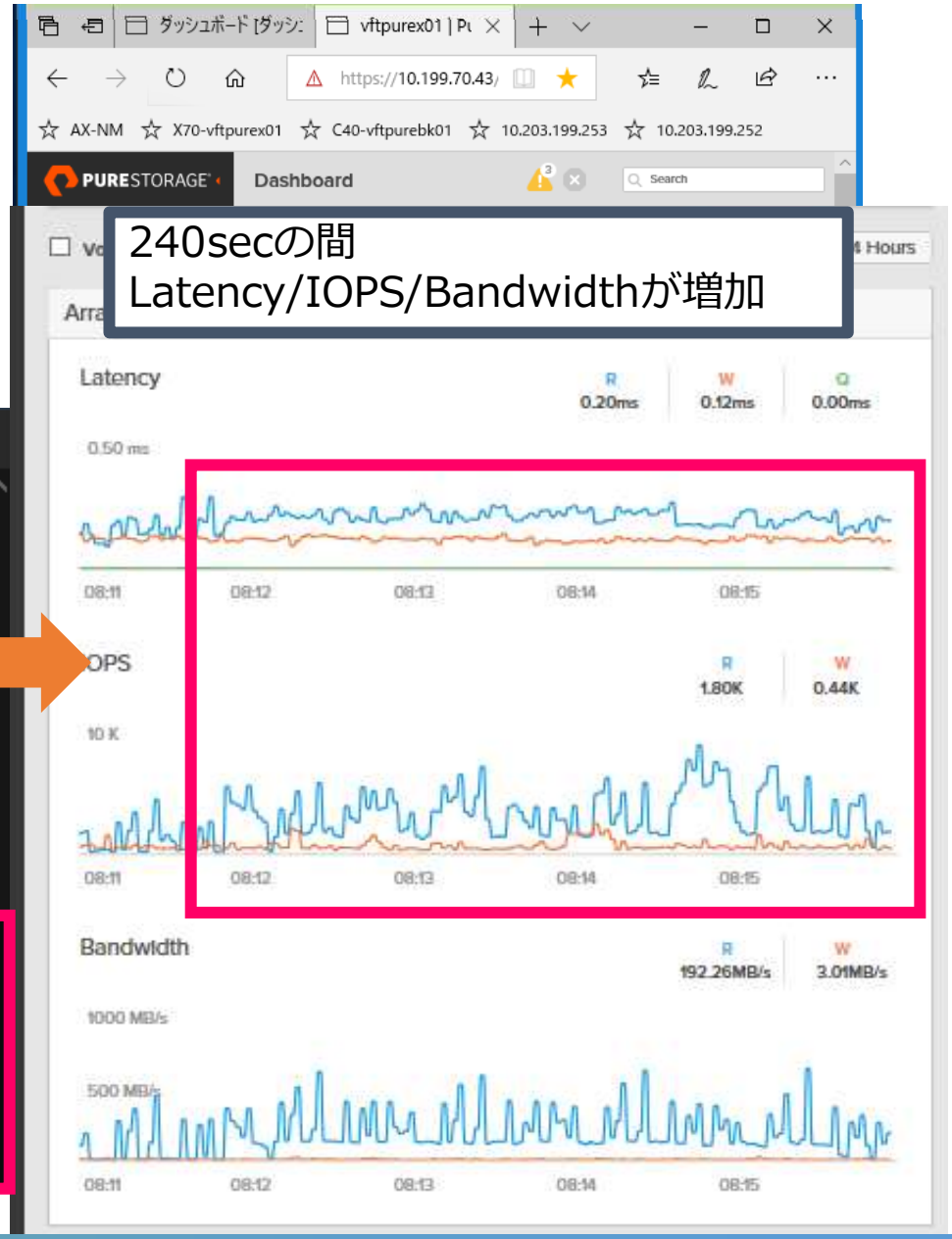
- 検知はサイバー対策ソフトウェアが行うものと、人為的活動で行うものがある

電子カルテ本体の異常アクセス→PureStorage

SQLインジェクションによるデータの不正操作や抜き出し兆候を監視
（研究目的のアクセスとの違いに注意）

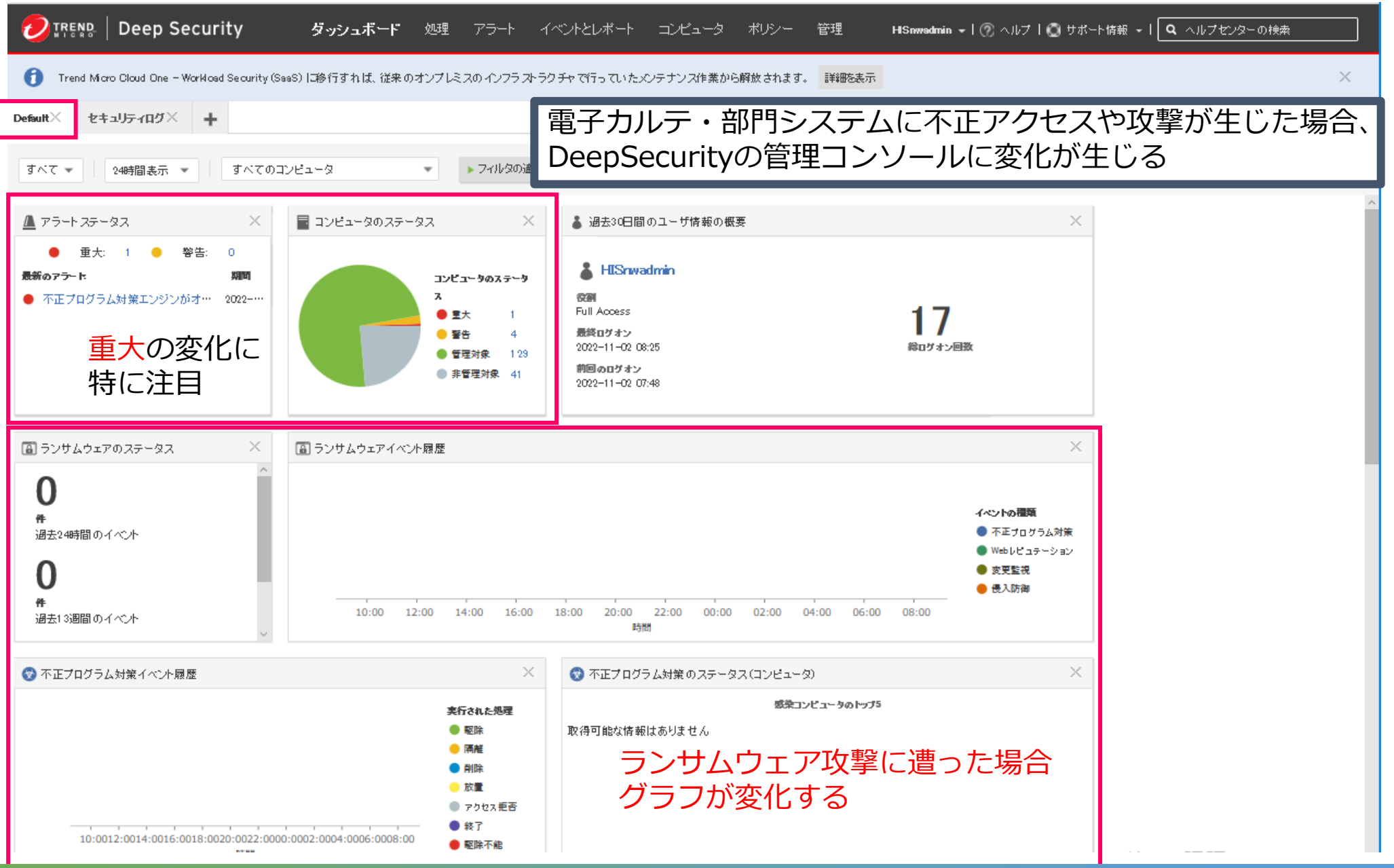




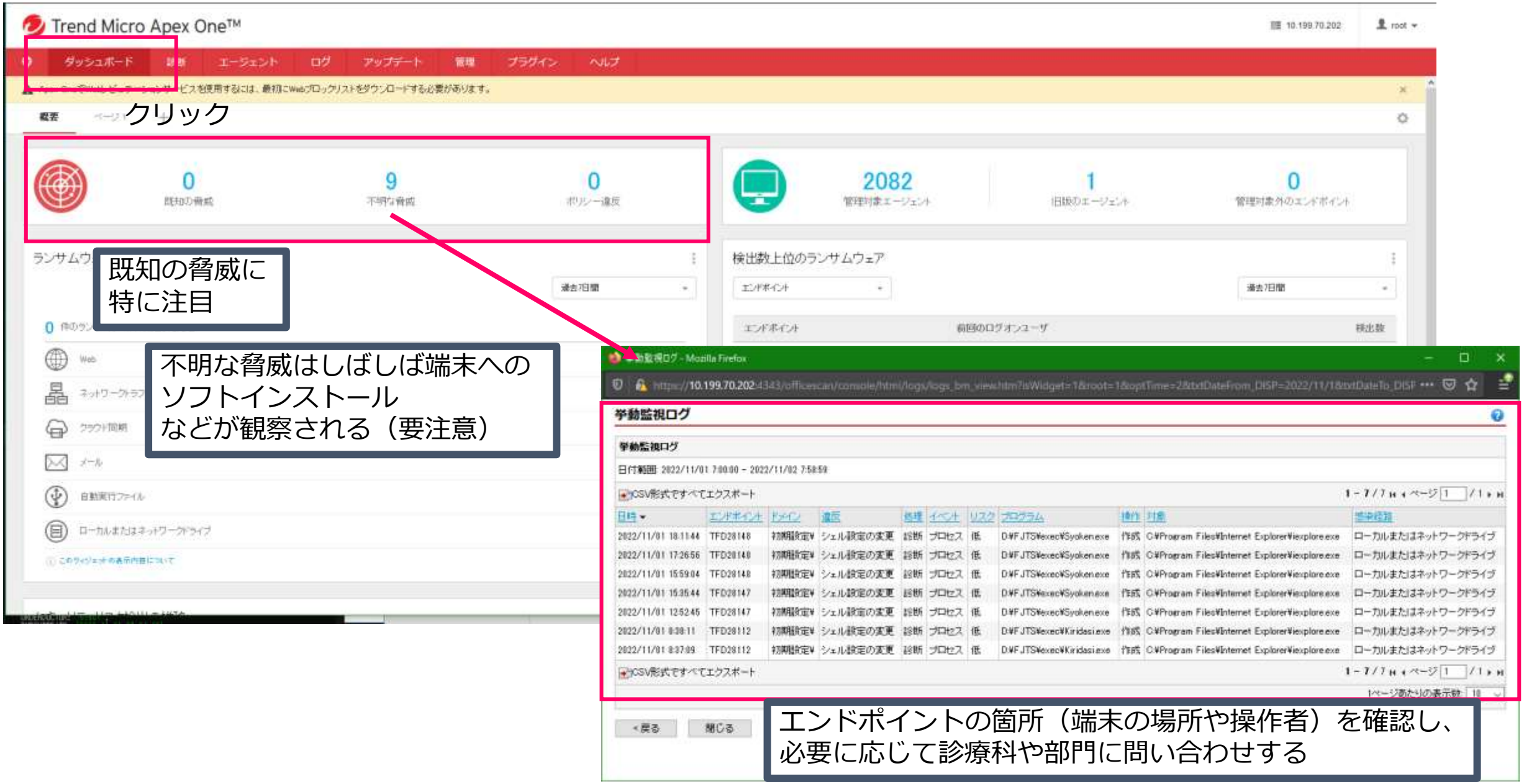


サーバへの異常アクセス監視→DeepSecurity

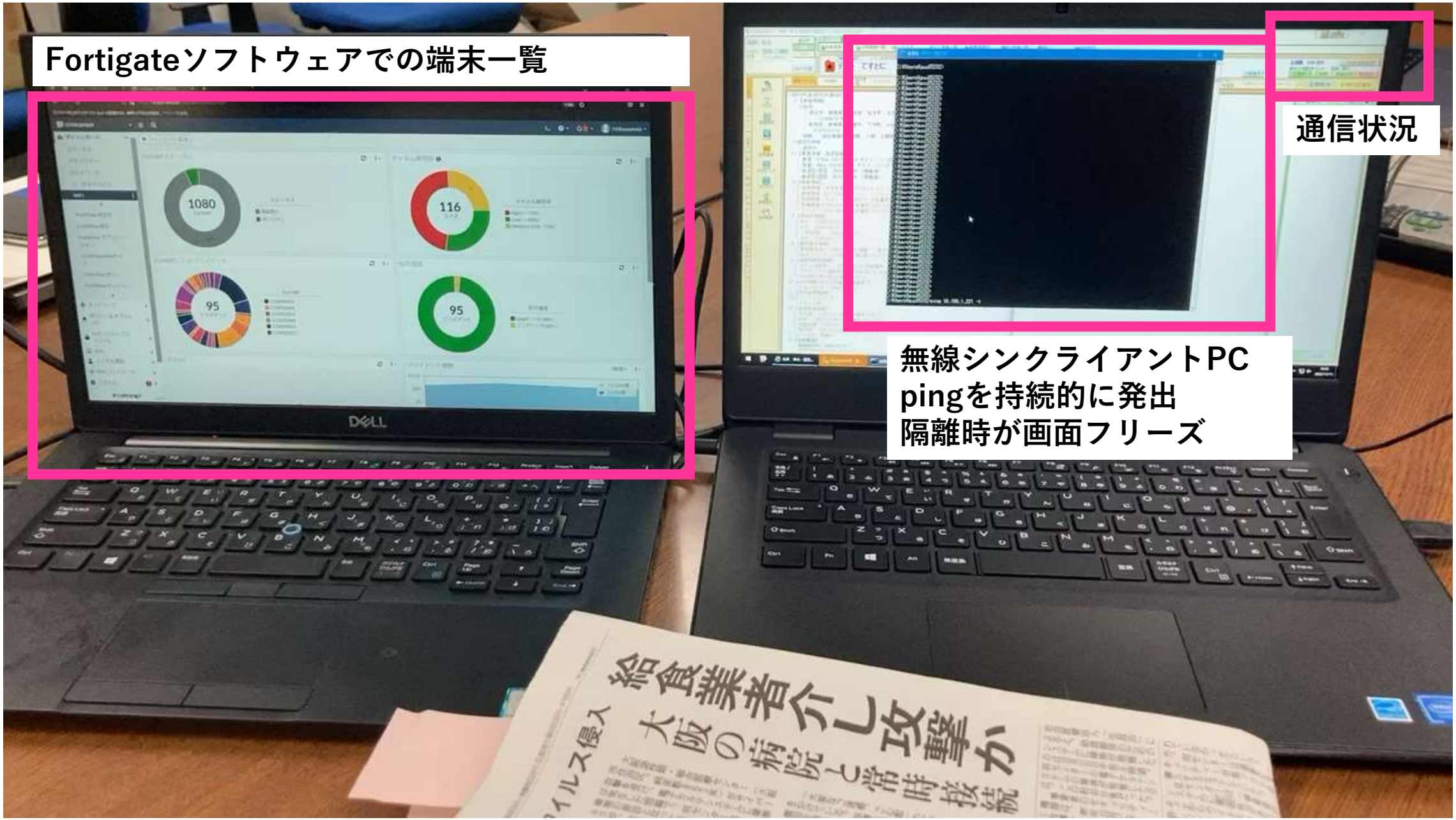
クリック



端末の異常操作の監視→ApexOne

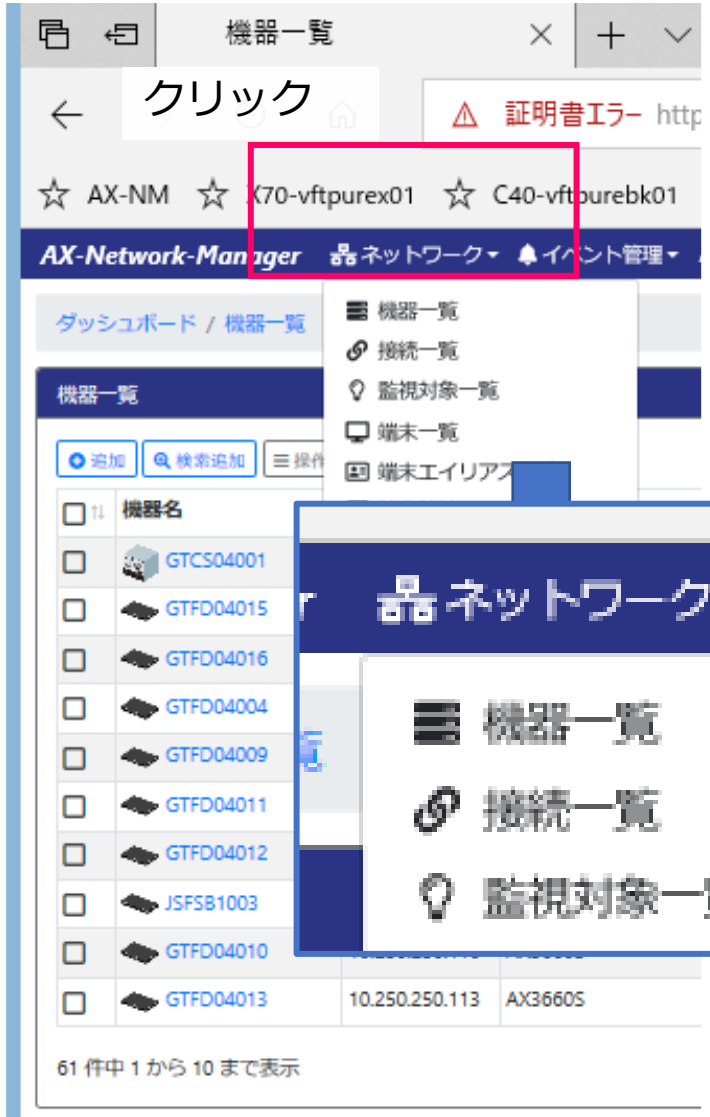


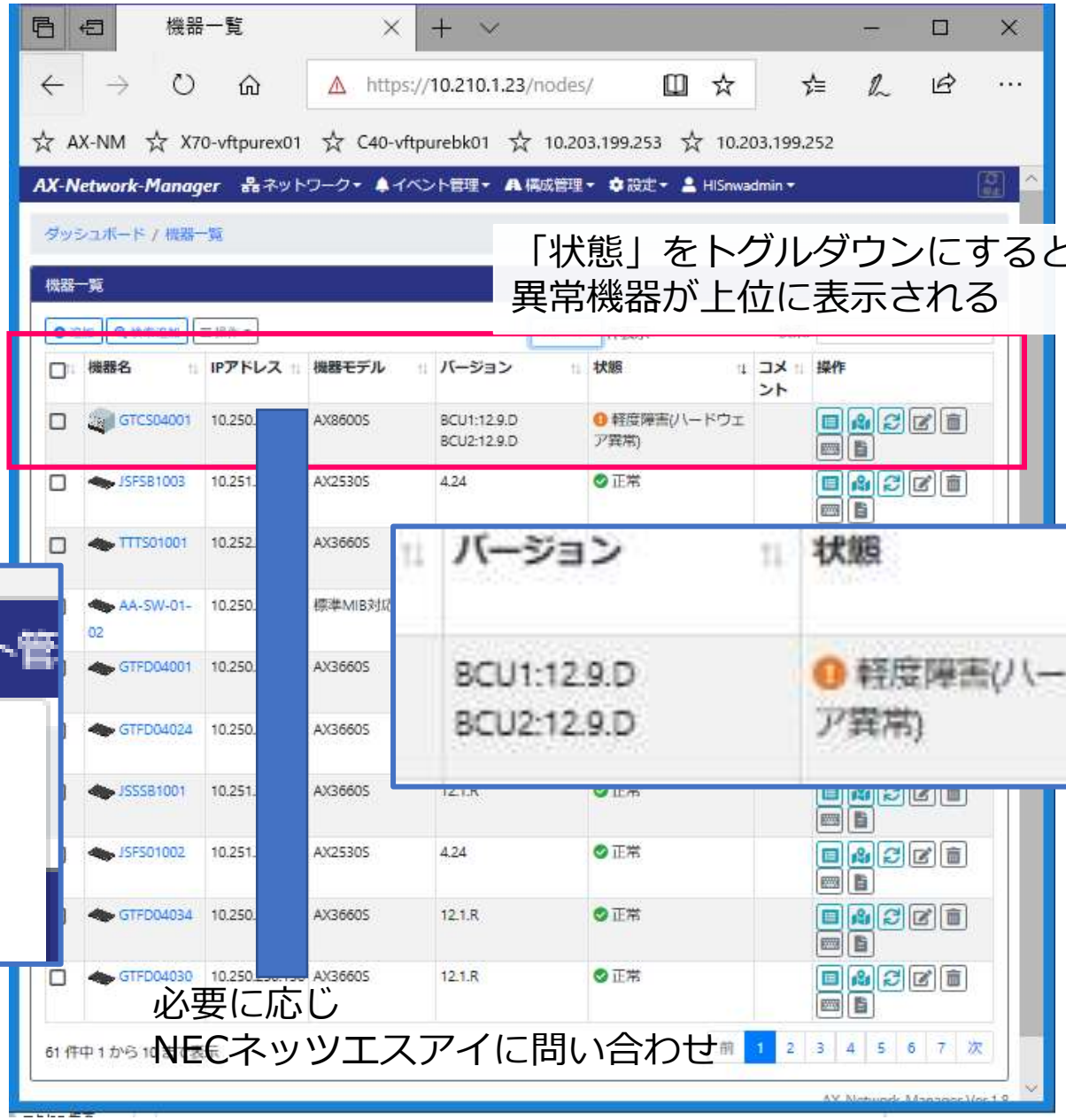
Fortigateソフトウェアを用いた端末の迅速なネットワーク隔離操作



ネットワーク機器異常の監視→AX-Network-Manager(AX-NM)

ダッシュボード-機器一覧を
クリック





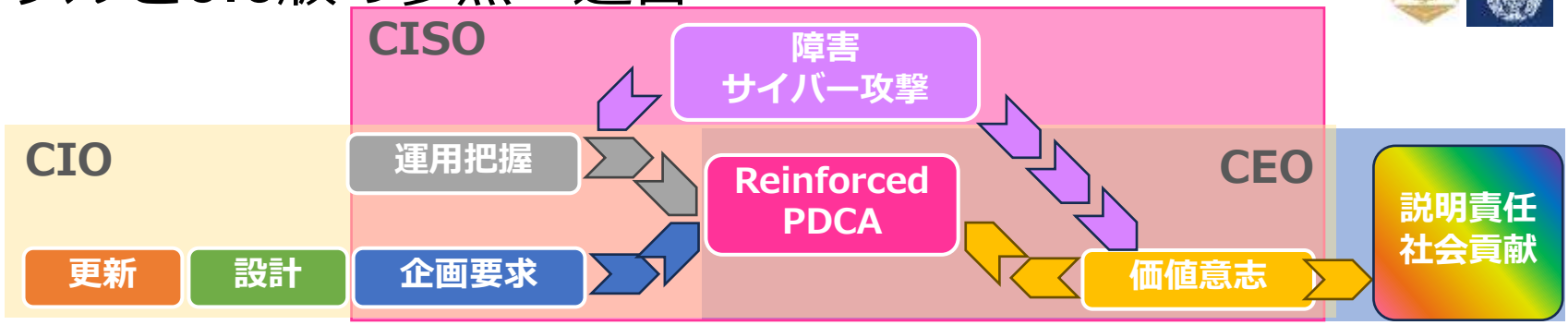
「状態」をトグルダウンにすると
異常機器が上位に表示される

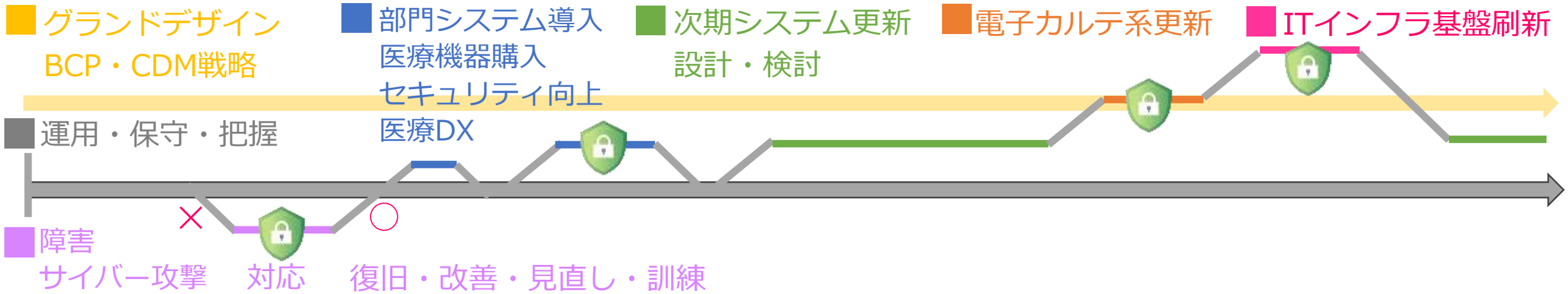
必要に応じ
NECネッツエスアイに問い合わせ

医療ワークフローにおける
セキュリティ導入の具体的設計

病院情報システムの運用サイクルと6.0版の参照・適合

経営管理編[Governance]
1.安全管理に関する責任・責務
2.リスク評価を踏まえた管理
3.安全管理全般（統制、設計、管理等）
4.安全管理に必要な対策全般
5.医療情報システム・サービス事業者との協働





企画管理編[Management]
1.管理体系
2.責任分界
3.安全管理体制と責任・権限
4.安全管理規定・文書類
5.エビデンス
6.リスクマネジメント
7.人的管理
8.情報管理、持ち出し、破棄
9.情報機器等の資産管理
10.運用点検・監査
11.非常時対応とBCP策定
12.サイバーセキュリティ
13.利用者認証等及び権限
14.法令記名・押印電子署名
15.技術的安全管理対策の管理
16.紙媒体等医療情報電子化

システム運用編[Control]
1.基本的な考え方
2.設計・運用規定類
3.責任分界
4.リスクアセスメント設計
5.システム設計の見直し
6.安全管理・技術的対策
7.情報管理（管理・持ち出し・破棄等）
8.機器・サービス安全管理措置
9.ソフト要求
10. サービス事業による保守対応
11.システム運用管理（通常時・非常時）
12.物理的安全管理措置
13.ネットワークに関する安全管理措置
14.認証・認可に関する安全管理措置
15.電子署名・タイムスタンプ
16.紙媒体等で作成した医療情報の電子化
17.証跡のレビュー・システム監査
18.外部からの攻撃に対する安全管理措置

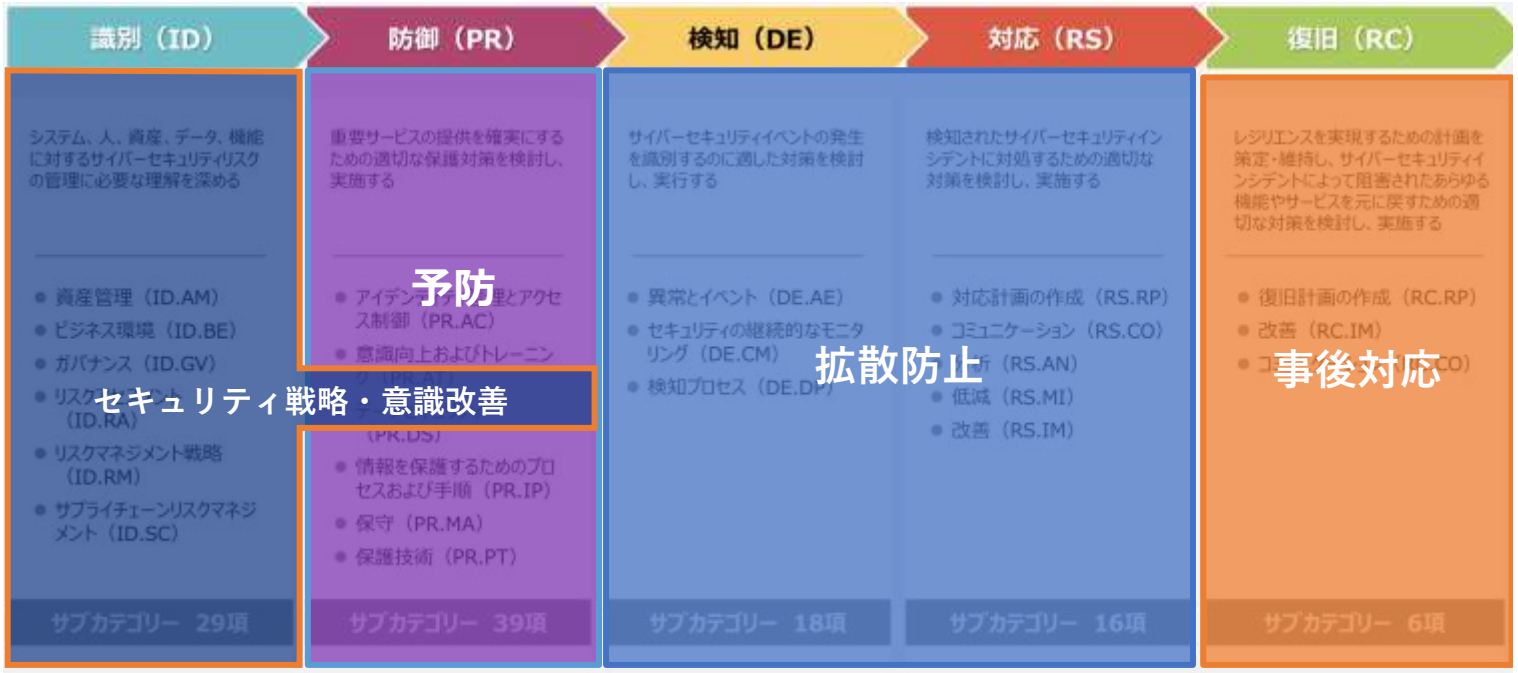
サイバー攻撃に対してIT-BCPを実現するには

- 「もし、私がサイバー攻撃者で、病院機能を効果的に毀損させる意図があったら」と考えてみる
- 医療機関側は、侵害覚知直後には「全ての被害可能性」を想定し、「攻撃対応」と「診療継続」を両立させる

Aim	人命に直結する装置・手技への攻撃		医療ワークフロー(指示・判断・連携)の混乱・停止への攻撃						
Vector	生命維持・精密静注 誤動作や停止	麻酔装置・手術装置 誤動作や停止	受付・会計・キー検査 部門システム機能停止		オーダ・ステータス 不信頼化・機能停止		系内侵入 漏洩・脅迫		
Target	入院病棟 ICU/SCU	IoTハック 通信切断 電源系攻撃	手術室	IoTハック 通信切断 電源系攻撃	外来・病棟 病院全域	改竄・暗号化 通信切断	外来・病棟 病院全域	改竄・暗号化 通信切断	潜伏活動 DBアクセス 外部送信
IT有BCP	予備医療装置の準備 修理・再稼働手順訓練	参照サーバ・端末の準備 ネットワーク等冗長化 非常時縮退IT運用訓練・高速復旧体制整備							N/A
IT無BCP	手動操作医療器具の準備 緊急時搬送受入先確保				紙運用用紙・運用準備 外部参照系、安全な患者誘導フロー確保				対策マニュアル
	全体BCPとの運用整合（特に、自家発電強化下での電力利用用途優先順位を厳格に定めておく）								
サイバー対策	IPS/ネットワーク監視 脆弱性対策	IPS/ネットワーク監視 制御PCのサイバー保護	5段階防衛の全て 防御/検知/隔離/対応/復旧＋組織訓練						
先進対策	予備装置の地域プール体制		予備サーバの地域プール 冗長化・SaaSミラー						リスク保険
	CSIRT / 医療CISO職配置 / 独立稼働端末指定やサーバの高SLAレベル運用 / CDM戦略の策定と運用								

NIST CyberSecurity Framework（CSF）
CISA Continuous Diagnostics and Mitigation (CDM)

CSF



CDM

CSFにおける医療機関内情報システム要素の検討・対策箇所

フレームワーク 機能	検討箇所の例	対策ツールの例	対策運用の例
識別 ID	病院情報システム全体の接続機器・IPアドレス、セグメンテーション、接続経路、脆弱性等の把握	ネットワーク可視化ツール、脆弱性把握ツール	資産管理手順に沿った調査（リストアップ）、脆弱性情報の迅速把握
防御 PR	外部保守接続箇所 （放射線診断・治療装置、PACS/電子カルテ等）、 DMZ端末、診療録サーバ	VPN、ランサム対策 ストレージ	情報漏洩を起こさない院内情報運用研修、診療情報アクセス制御設定、ファイヤウォール設定、セキュリティ保守契約の充実、バックアップ手段と階層、運用の策定と実装
検知 DE	電子カルテ端末挙動、 ネットワークトラフィック監視、 ストレージ/CPU負荷変動	IDS、EDR(D)、NDR(D)	日常のシステムパフォーマンスモニタにおけるトレンド把握と差異の知覚、対策ツールが提供するダッシュボード機能による監視
対応 RS	不特定多数や多数のスタッフがアクセスできる機器、電子カルテにアクセスできる端末またはサーバとポート、攻撃検知時のカルテデータバックアップ経路	IPS 、 EPP 、 EDR(R) 、 NDR(R)	インシデント時連絡先の把握と役割分担の検討、医療安全と情報保全、診療継続を両立する対策方法やツール挙動設定の検討、インシデント対応訓練への参加
復旧 RC	電子カルテサーバを中心とする保存義務を有する情報サーバ、診療継続に不可欠な情報端末の運用	バックアップ復元ツール、 情報サーバ仮想化 インフラ	復元手順のBCPへの記載、復元テスト、環境設定を伴った包括的サーババックアップの実施、バックアップ周期の短縮化

病院におけるサイバーリスクの受容の考え方(1)

- 推定許容される「診療停止日数」
  - 収入減、支出増、「金額化」に分けて考える
  - （停止日数）×（1日平均稼働額）＝（金額としての収入源）

75日×1億円=75億円

  - 調査、対応、復旧にかかる費用

~3億円？

  - 病院の信頼毀損、患者対応による医療スタッフの精神的負担、未知でリスクの高い紙運用の医療事故への緊張負担

2000人×10000円×75日=15億円

- 推定許容される「病院機能停止日数」
  - 高度急性期では救急患者受け入れのデマンドが高い→検査機器の停止を許容しづらい

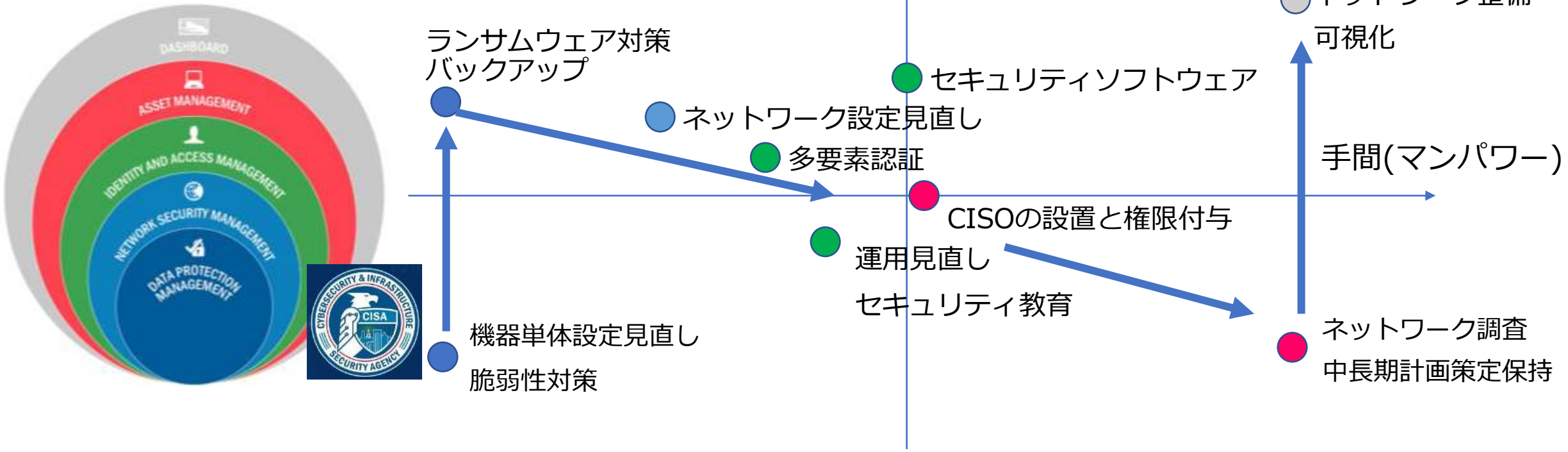
- 推定許容される「病院情報システム停止日数」
  - 大阪急性期から学ぶこと１：参照システムの早期復旧の重要性

病院情報システムは診療よりも
十分早期に復旧しなければならない

  - 大阪急性期から学ぶこと２：確実なデータバックアップ確保の重要性
  - 大阪急性期から学ぶこと３：サプライチェーン接続の確認

CDS＝「できることから始めよう、次第に良くなる計画を立てよう」

- Continuous Diagnostics and Mitigation (継続的なセキュリティ診断とリスク低減)
- いきなり「盤石のセキュリティ」には到達できない（それでも今から始める価値がある）
- 「抑えるべき急所の順序」が存在する
- 対策には「すぐできるもの」と「計画し予算と人手がかかるもの」に分けられる



CSFとCDM：どちらから始めるか？

	Cyber Security Framework (CSF)	Continuous Diagnostics and Mitigation (CDM)
段階の考え方	Tier （分野ごとにレベルを評価）	Core （保護対象の順序を指定）
着手順	攻撃者の侵入経路に沿って	防御者の保護資産に沿って
適した始め方	システム更新の計画開始時	随時
実施時のハードル	資産管理の手間が大きい （調査の支援役務？） シェル型の保護で終わりがち 可用性の確保	より高いレベルでの防御を見込む場合、 資産管理が避けられない 大規模インフラ改修計画を

5.2版と6.0版の違い

5.2の目次

2.本ガイドラインの読み方
3.対象システム及び対象情報
4.電子的な医療情報を扱う際の責任のあり方
5.情報の相互運用性と標準化について
6.医療情報システムの基本的な安全管理
7.電子保存の要求事項について
8.診療録及び診療諸記録を外部に保存する際の基準
9.診療録等をスキャナ等により電子化して保存する場合について
10.運用管理について

6.0の目次

概説編
2.本ガイドラインの対象
3.本ガイドラインの構成・読み方
4.本ガイドラインの前提

経営管理編[Governance]
1.安全管理に関する責任・責務
2.リスク評価を踏まえた管理
3.安全管理全般（統制、設計、管理等）
4.安全管理に必要な対策全般
5.医療情報システム・サービス事業者との協働

5.2版と6.0版の違い

5.2の目次

2.本ガイドラインの読み方
3.対象システム及び対象情報
4.電子的な医療情報を扱う際の責任のあり方
5.情報の相互運用性と標準化について
6.医療情報システムの基本的な安全管理
7.電子保存の要求事項について
8.診療録及び診療諸記録を外部に保存する際の基準
9.診療録等をスキャナ等により電子化して保存する場合について
10.運用管理について

6.0の目次

企画管理編[Management]
1.管理体系
2.責任分界
3.安全管理のための体制と責任・権限
4.医療情報システムの安全管理において必要な規定・文書類の整備
5.安全管理におけるエビデンス
6.リスクマネジメント（リスク管理）
7.安全管理のための人的管理（職員管理、事業者管理、教育・訓練、事業者選定・契約
8.情報管理（管理、持ち出し、破棄等
9.医療情報システムに用いる情報機器等の資産管理
10.運用に関する点検・監査
11.非常時（災害、サイバー攻撃、システム障害）対応とBCP策定
12.サイバーセキュリティ
13.医療情報システムの利用者に関する認証等及び権限
14.法令で定められた記名・押印のための電子署名
15.技術的な安全管理対策の管理
16.紙媒体等で作成した医療情報の電子化

5.2版と6.0版の違い

5.2の目次

2.本ガイドラインの読み方
3.対象システム及び対象情報
4.電子的な医療情報を扱う際の責任のあり方
5.情報の相互運用性と標準化について
6.医療情報システムの基本的な安全管理
7.電子保存の要求事項について
8.診療録及び診療諸記録を外部に保存する際の基準
9.診療録等をスキャナ等により電子化して保存する場合について
10.運用管理について

6.0の目次

システム運用編[Control]
1.情報セキュリティの基本的な考え方
2.システム設計・運用に必要な規定類と文書体系
3.責任分界
4.リスクアセスメントを踏まえた安全管理管理対策の設計
5.システム設計の見直し（標準化対応、新規技術導入のための評価等）
6.安全管理を実現するための技術的対策の体系
7.情報管理（管理・持ち出し・破棄等）
8.利用機器・サービスに対する安全管理措置
9.ソフトウェア・サービスに対する要求事項
10.医療情報システム・サービス事業による保守対応等に対する安全管理措置
11.システム運用管理（通常時・非常時等）
12.物理的安全管理措置
13.ネットワークに関する安全管理措置
14.認証・認可に関する安全管理措置
15.電子署名・タイムスタンプ
16.紙媒体等で作成した医療情報の電子化
17.証跡のレビュー・システム監査
18.外部からの攻撃に対する安全管理措置

End of Document