令和５年度医療情報セキュリティ研修 及び
サイバーセキュリティインシデント発生時初動対応支援・調査等事業

【はじめに】

今年度のシステム・セキュリティ管理者向け研修について

受託事業者：一般社団法人ソフトウェア協会

今年度のシステム・セキュリティ管理者向け研修

- 今年度の研修は、システム・セキュリティ管理者全体の底上げを行うために、IT管理や運用に関する基本的な内容理解から、昨年度同様に、今できるセキュリティ対策や心がけに焦点を当てて研修を提供します。
- 前半は根本的なセキュリティ管理や運用を理解するために、IT環境における組織の管理やアクセス制御など、基本的なセキュリティ体制や考え方を理解します。
- 後半は、大阪急性期・総合医療センターに学ぶ防御設定として、グループポリシーや脆弱な医療機器の保護方法など、さらに具体化された対策について言及していきます。

今年度の研修の構成

開催回	カテゴリ	概要	講師
第１回	オリエン	IT環境における組織の管理	萩原健太 インターバルリンク（株）、(一社)ソフトウェア協会
第２回	基礎	ID管理やアクセス制御	村澤 直毅 後藤 昌宏 日本マイクロソフト(株)
第３回	基礎	脅威や脆弱性	村澤 直毅 後藤 昌宏 日本マイクロソフト(株)
第４回	基礎	効果的なセキュリティの実現	村澤 直毅 後藤 昌宏 日本マイクロソフト(株)
第５回	実践	Windows標準機能の活用	板東 直樹 アップデートテクノロジー(株)、(一社)ソフトウェア協会
第６回	実践	脆弱な機器の守り方	板東 直樹 アップデートテクノロジー(株)、(一社)ソフトウェア協会
第７回	実践	インシデントに備える体制	板東 直樹 アップデートテクノロジー(株)、(一社)ソフトウェア協会

※内容は変更する場合がございます。

【第１回】システム・セキュリティ管理者向け研修

IT環境における組織の管理

一般社団法人ソフトウェア協会
萩原 健太

（（株）ビジネスブレイン太田昭和、インターバルリンク（株））

目的・アジェンダ

【目的】

システム・セキュリティ管理者としての心がけや昨今の動向をとらえ、
実施可能な対応策の概要を知る。

【アジェンダ】

- はじめに
  - 医療界における組織管理の苦悩
- 過去からちゃんと学ぶ
  - もし大阪急性期・総合医療センターで〇〇〇〇の対応をしていたら…？
- 組織での管理に向けて
  - 国の動向やガイドライン等の理解を深める
  - クラウドとゼロトラストの理解

自己紹介

萩原健太（はぎはらけんた）

法政大学大学院公共政策研究科修士課程修了

【経歴】

セキュリティベンダーにてマーケティングや渉外、CSIRT*の構築や運用支援などを行い、現在もサ イバーセキュリティに関する助言や講演などを数多く行っている。主に組織的なサイバーセキュリ ティを専門としている。また経営戦略の立案やマーケティング支援なども行い、現在は兼業しなが らセキュリティや経営・マーケティング支援などを行う。 またつるぎ町立半田病院の調査および報告書作成に携わり、大阪急性期・総合医療センターのラン サムウェア感染のアクシデントには、厚生労働省から政府派遣チームの一員として現地にかけつけ 初動対応を行っている。 初動に係る政府派遣終了後には、同センターのセキュリティアドバイザーに就任し、調査報告書の 作成や継続的にセキュリティの助言などを行っている。 *Computer Security Incident Response Team

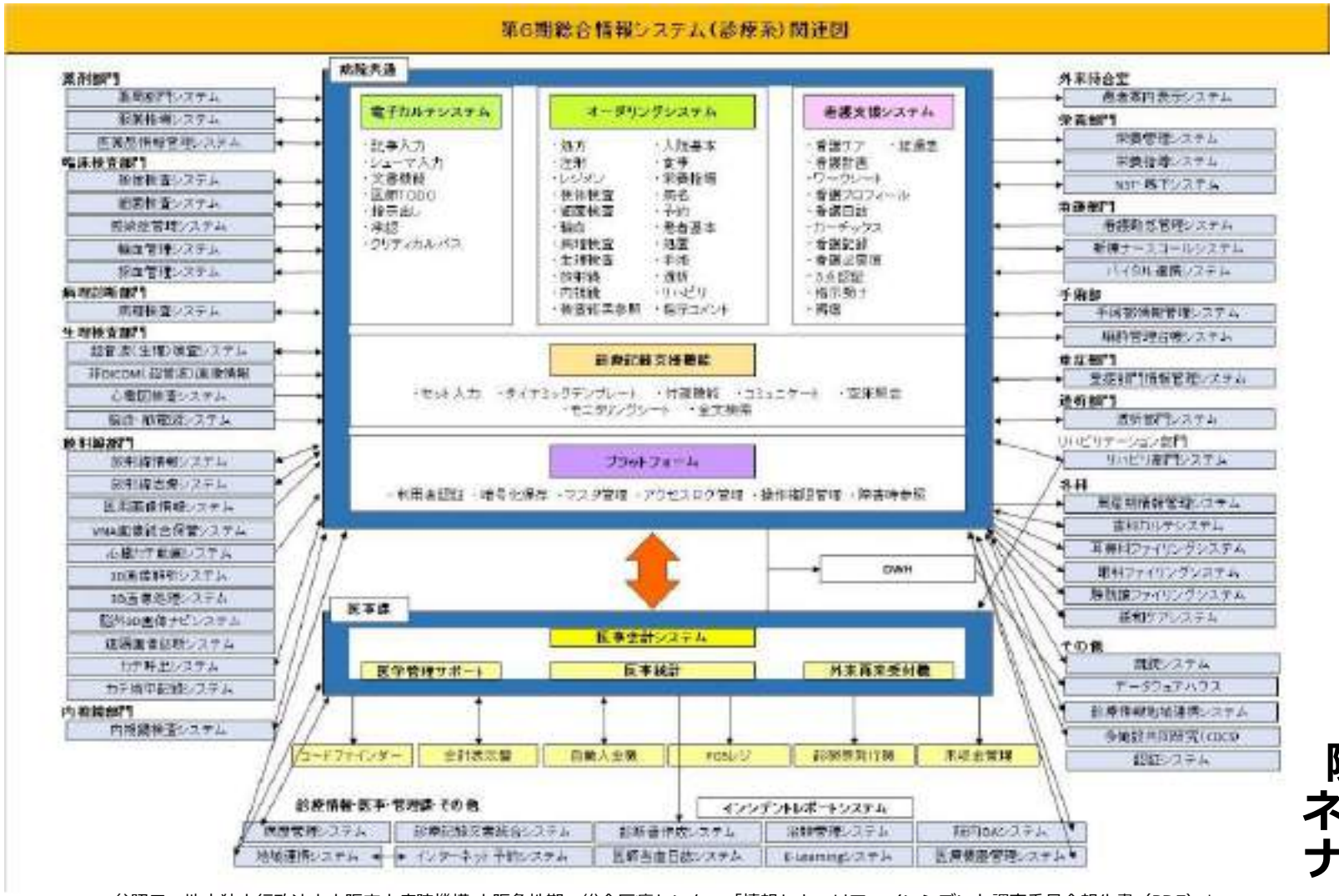
【書籍（共著）】 技術評論社『今からはじめるインシデントレスポンス』（2020） 日本経済新聞出版社『経営者のための情報セキュリティ Q&A45』（2019）

【論文】 情報処理学会『サイバーセキュリティ対策のための研究用データセット「動的活動観測2014 ～ 2017」』（2019） 情報処理学会『CSIRTの最低要件』（2017）など

【主な役職】 （一社）ソフトウェア協会 理事・Software ISAC 共同代表 （一社）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 運営委員長 （国研）情報通信研究機構 ナショナルサイバートレーニングセンター 招聘専門員 （地独）大阪急性期・総合医療センター セキュリティアドバイザー （株）ビジネスブレイン太田昭和 CMO インターバルリンク（株） 代表取締役

はじめに
～医療界における組織管理の苦悩～

システム・セキュリティ管理者の苦悩と現実①



【代表的なシステム】

電子カルテシステム
＋
部門システム
＋
事務系システム
＋
検査機器

院内の全ての機器やシステム・ネットワークを把握し、「ITガバナンス」を確立する必要がある。

参照元：地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター「情報セキュリティインシデント調査委員会報告書（PDF）」
https://www.gh.opho.jp/pdf/report_v01.pdf

システム・セキュリティ管理者の苦悩と現実②

項目	つるぎ町立半田病院（半田病院）	大阪急性期・総合医療センター（大阪急性期C）
病床数	120床	865床
診療科	12	36
職員数	159人	2014人
システム担当職員数 （*インシデント発生当時）		
病院の特徴	災害拠点病院、徳島DMAT指定病院、 へき地医療支援病院、救急指定病院　など	基幹災害拠点病院、高度救命救急センター、地域周産期母子医療センター、地域医療支援病院など
報告書	コンピュータウイルス感染事案有識者会議調査報告書 https://www.handa-hospital.jp/topics/2022/0616/index.html	情報セキュリティインシデント調査委員会報告書 https://www.gh.opho.jp/important/785.html

情報システム部門の人数（正社員,2022年）

全国情シス実態調査
https://www.iij.ad.jp/svcsol/survey/all-it/2022/

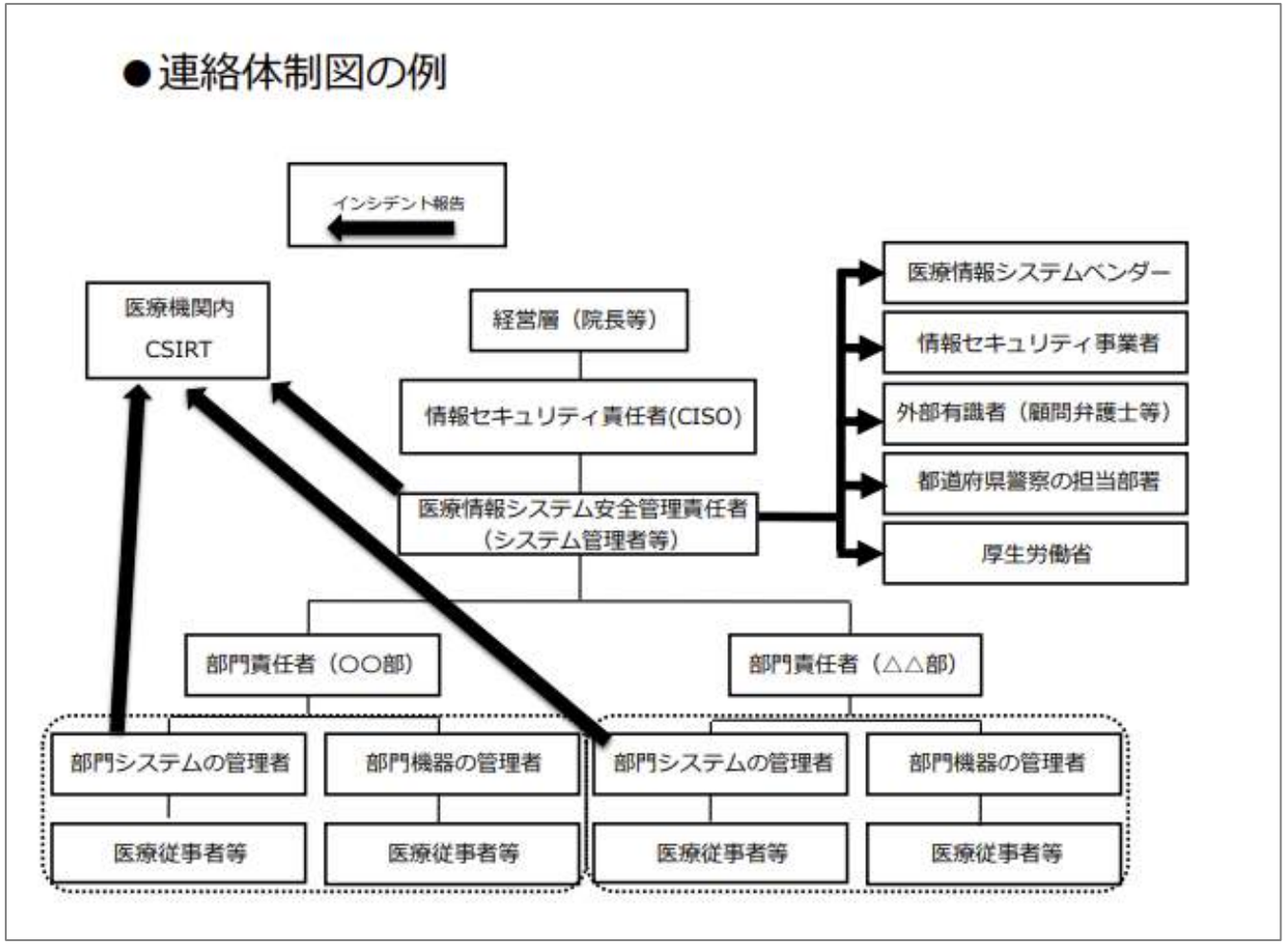
つるぎ町立
半田病院

大阪
急性期C

従業員規模	情報システム部門の人数
100人未満	3.9人
100人～500人	4.1人
501人～1,000人	9.8人
1,001人～3,000人	21.0人
3,001人～5,000人	95.4人
5,001人～10,000人	98.2人
10,001人以上	112.8人

皆さんの病院はいかがですか…？

セキュリティの仕事を知る



- CSIRT: 「Computer Security Incident Response Team」の略。
  - コンピュータセキュリティにかかるイシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をする。
- CISO: 「Chief Information Security Officer」の略。
  - 最高情報セキュリティ責任者。施設や組織における情報セキュリティを統括する責任者を指す

事業継続計画に基づく行動で乗り切ったのが
これまでのインシデント。

サイバーBCPを検討しセキュリティ活動を
推進するか、もしくは事業継続計画への
サイバー攻撃の反映を考える必要がある。

医療機関におけるサイバーセキュリティ対策チェックリストマニュアル ～医療機関・事業者向け～
３ インシデント発生に備えた対応（１）インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）の連絡体制図がある。
https://www.mhlw.go.jp/content/10808000/001105752.pdf

セキュリティの仕事

- セキュリティの仕事はたくさんある・・・

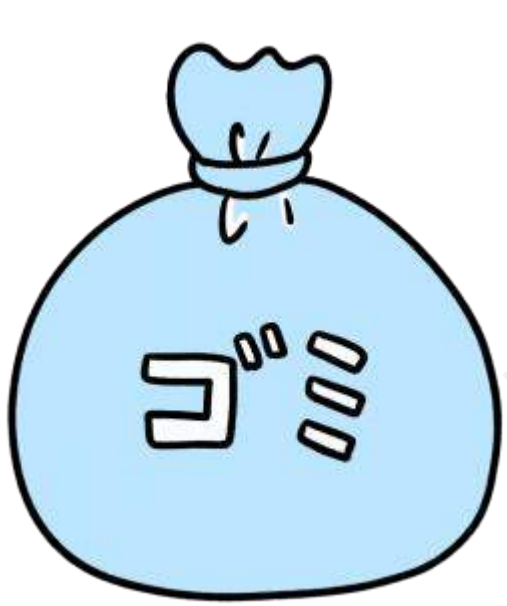
インシデント 事後対応サービス	インシデント 事前対応サービス	セキュリティ品質向上 サービス
・インシデントハンドリング ・コーディネーション ・コンピュータ・フォレンジックス ・オンサイトインシデントレスポンス ・インシデントレスポンスサポート ・アーティファクトハンドリング ・脆弱性情報ハンドリング	・セキュリティ関連情報提供 ・インシデント/セキュリティイベント検知 ・技術動向調査 ・セキュリティ監査/査定 ・セキュリティツールの管理 ・セキュリティツールの開発	・リスク評価分析 ・事業継続性、災害復旧計画作成・改変 ・セキュリティコンサルティング ・セキュリティ教育/トレーニング/啓発活動 ・製品評価・認定

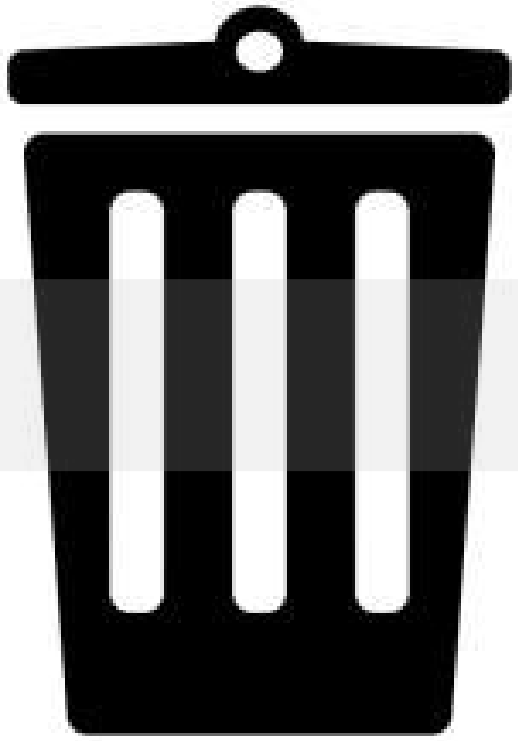
表 1 CSIRT のサービス概要

（一社）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スタータキット」
https://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf

経営者と技術者のギャップ

「ゴミ箱理論(仮)」＊





神戸市「家庭ごみの出し方ルールブック（ワケトンブック）」
https://www.city.kobe.lg.jp/documents/1347/book-ru-ruchirashi_202106.pdf

＊講師のこれまでの経験による私見です

セキュリティの仕事

- セキュリティの仕事はたくさんある。

インシデント 事後対応サービス	インシデント 事前対応サービス	セキュリティ品質向上 サービス
・ インシデントハンドリング ・ コーディネーション ・ 脆弱性情報ハンドリング	・ セキュリティ関連情報提	・ リスク評価分析 ・ 事業継続・事業復旧計画

セキュリティには、経営者の理解と覚悟、
そしてその準備と体制が必要。

是非、これらの情報を経営者に先に伝えておいてください！

表 1 CSIRT のサービス概要

（一社）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スタータキット」
https://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf

そのために…

初学者等向け研修	•誰でも知っておくべきセキュリティの基礎知識や過去のインシデントなどからわかりやすく学ぶ
システム・管理者向け研修	•7回の研修（オリエン・基礎・実践）＋ 演習を開発・実施（24年1月19日、2月1日）現地視察会を実施（23年11月9日開催）
経営者	•ITガバナンスやリーダーシップなど、経営者として知っておくべき内容をご提供 •現地視察会を実施（23年11月21日開催）
導入研修	•立入検査対策（アーカイブ配信） •大阪急性期・総合医療センター事例

＋e-learning

Medical Information Security Training

https://mhlw-training.saj.or.jp/

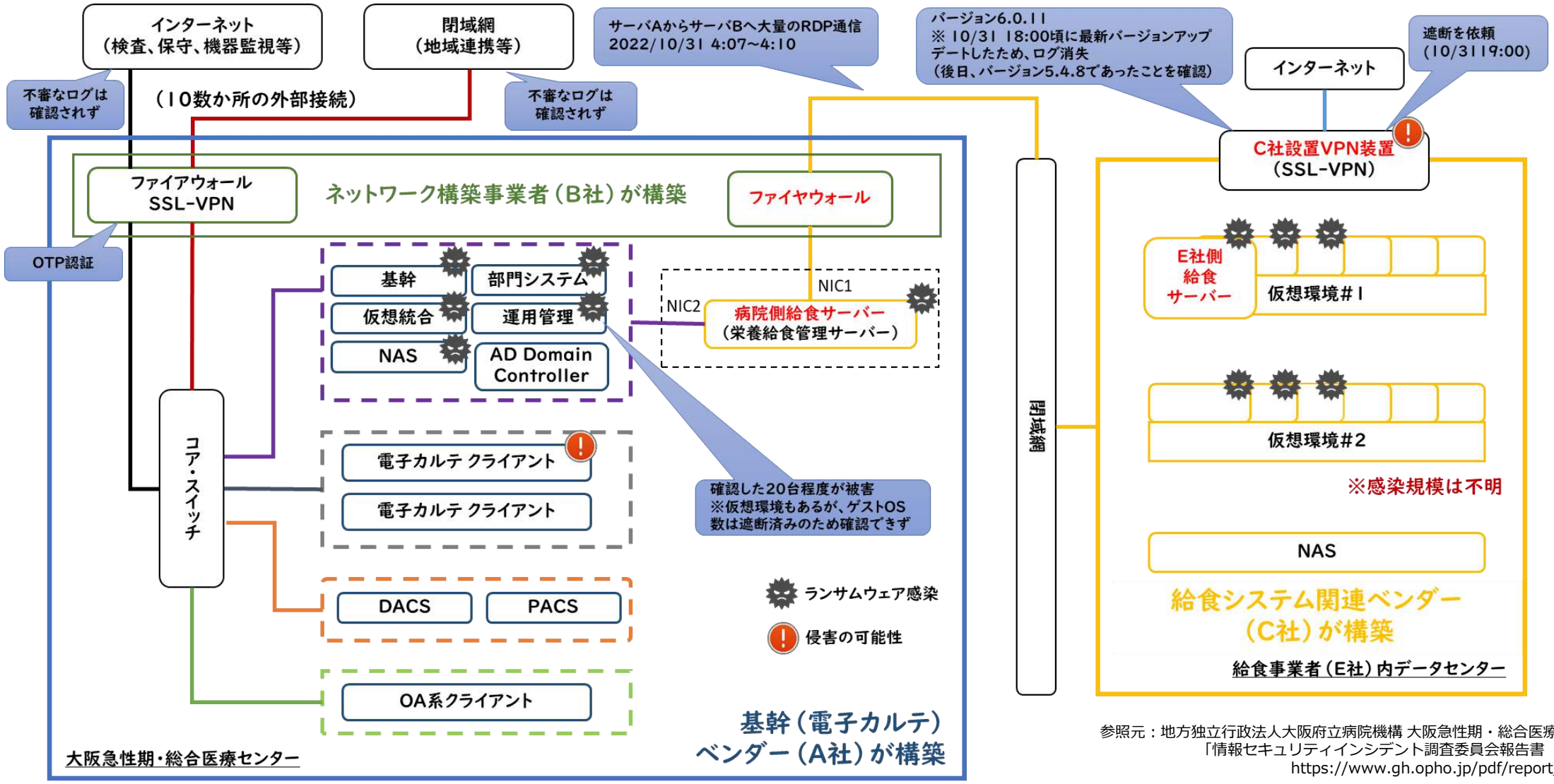
組織の管理のポイント

1. 経営者に現場責任者・担当者の苦労を伝える・説明する。
   （たとえ最初は聞く耳を持たなくても、たとえ一方的な話でも…）
2. これまでの医療界のセキュリティの常識は、他の業界での非常識。
3. ほとんどのインシデントは「高度なサイバー攻撃」ではなく、
   「**設定や対応の不備**」から起きている。
4. どの業界でも「人材不足」。まずはできることからやる。
   （セキュリティを足し算から掛け算にする。）
5. 己を知ることから始まる。敵を知っている場合ではない。
6. サイバーセキュリティは医療を止めないための一手段。
7. 「ITガバナンス」や「ゼロトラスト」は一日にしてならず。

過去からちゃんと学ぶ

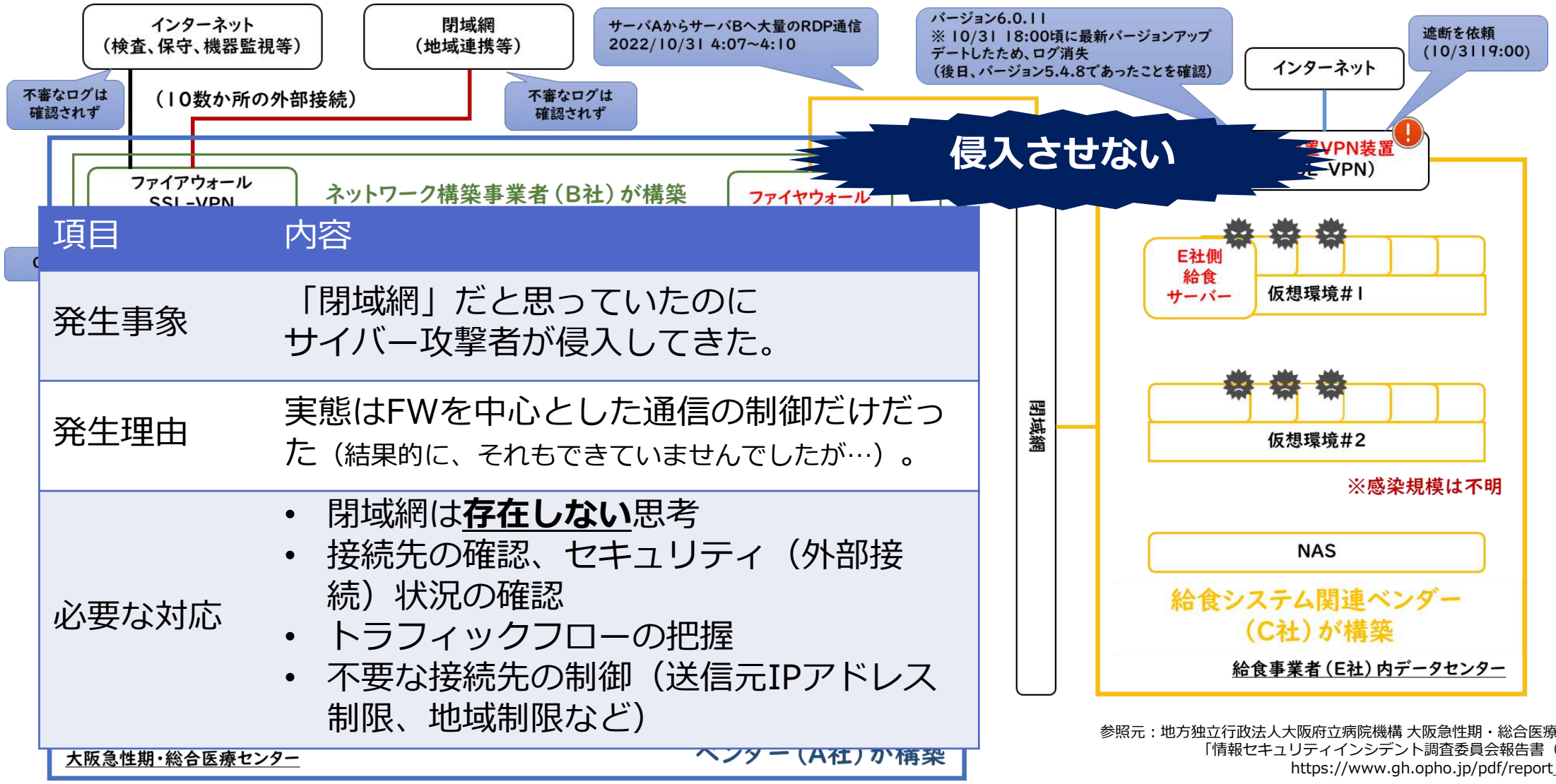
～もし大阪急性期・総合医療センターで〇〇〇〇の対応をしていたら…？～

大阪急性期・総合医療センターからの学び①



参照元：地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター
「情報セキュリティインシデント調査委員会報告書（PDF）」
https://www.gh.opho.jp/pdf/report_v01.pdf

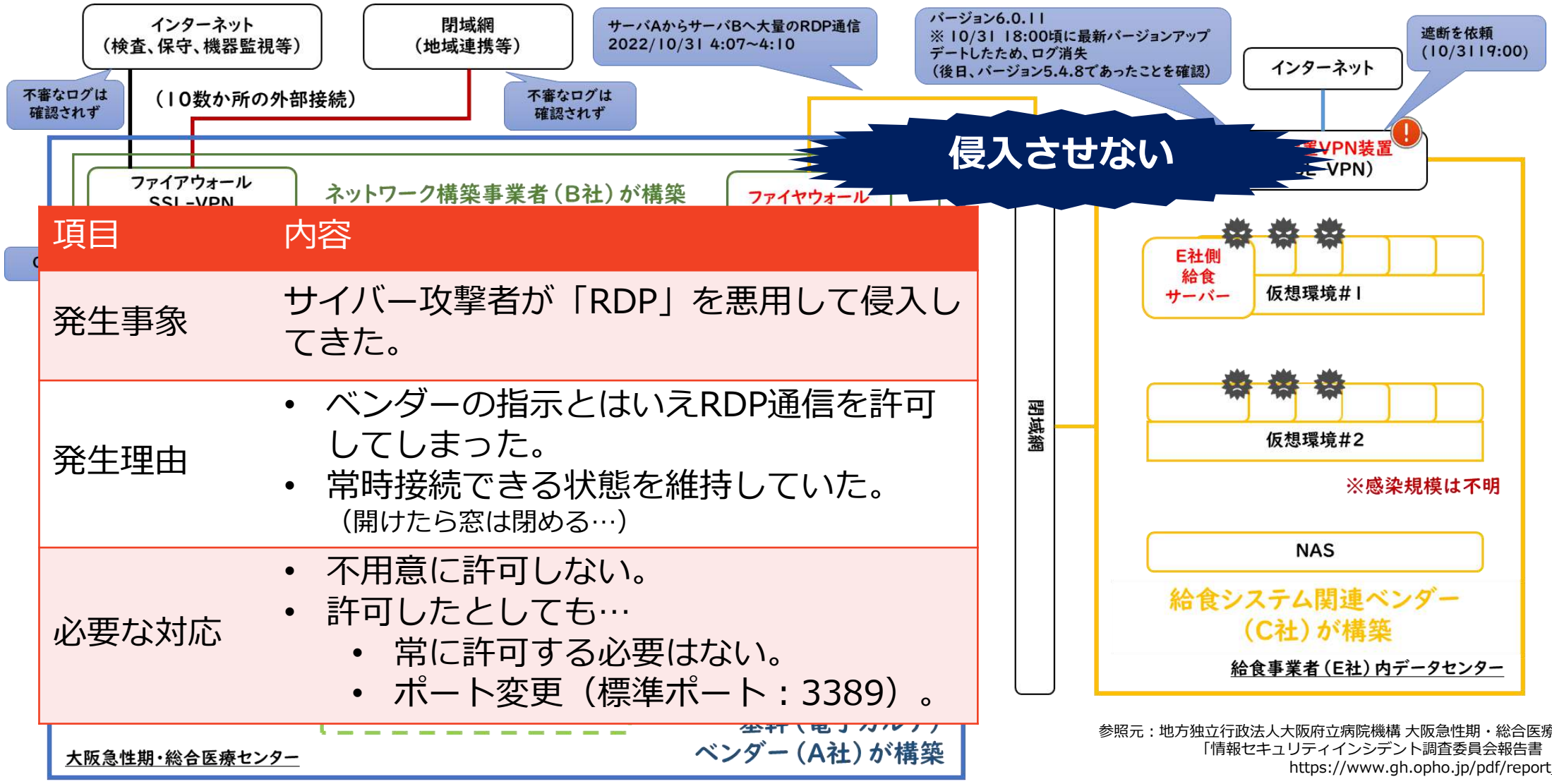
大阪急性期・総合医療センターからの学び②



項目	内容
発生事象	「閉域網」だと思っていたのにサイバー攻撃者が侵入してきた。
発生理由	実態はFWを中心とした通信の制御だけだった（結果的に、それもできていませんでしたが…）。
必要な対応	• 閉域網は**存在しない**思考 • 接続先の確認、セキュリティ（外部接続）状況の確認 • トラフィックフローの把握 • 不要な接続先の制御（送信元IPアドレス制限、地域制限など）

参照元：地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター
「情報セキュリティインシデント調査委員会報告書（PDF）」
https://www.gh.opho.jp/pdf/report_v01.pdf

大阪急性期・総合医療センターからの学び③

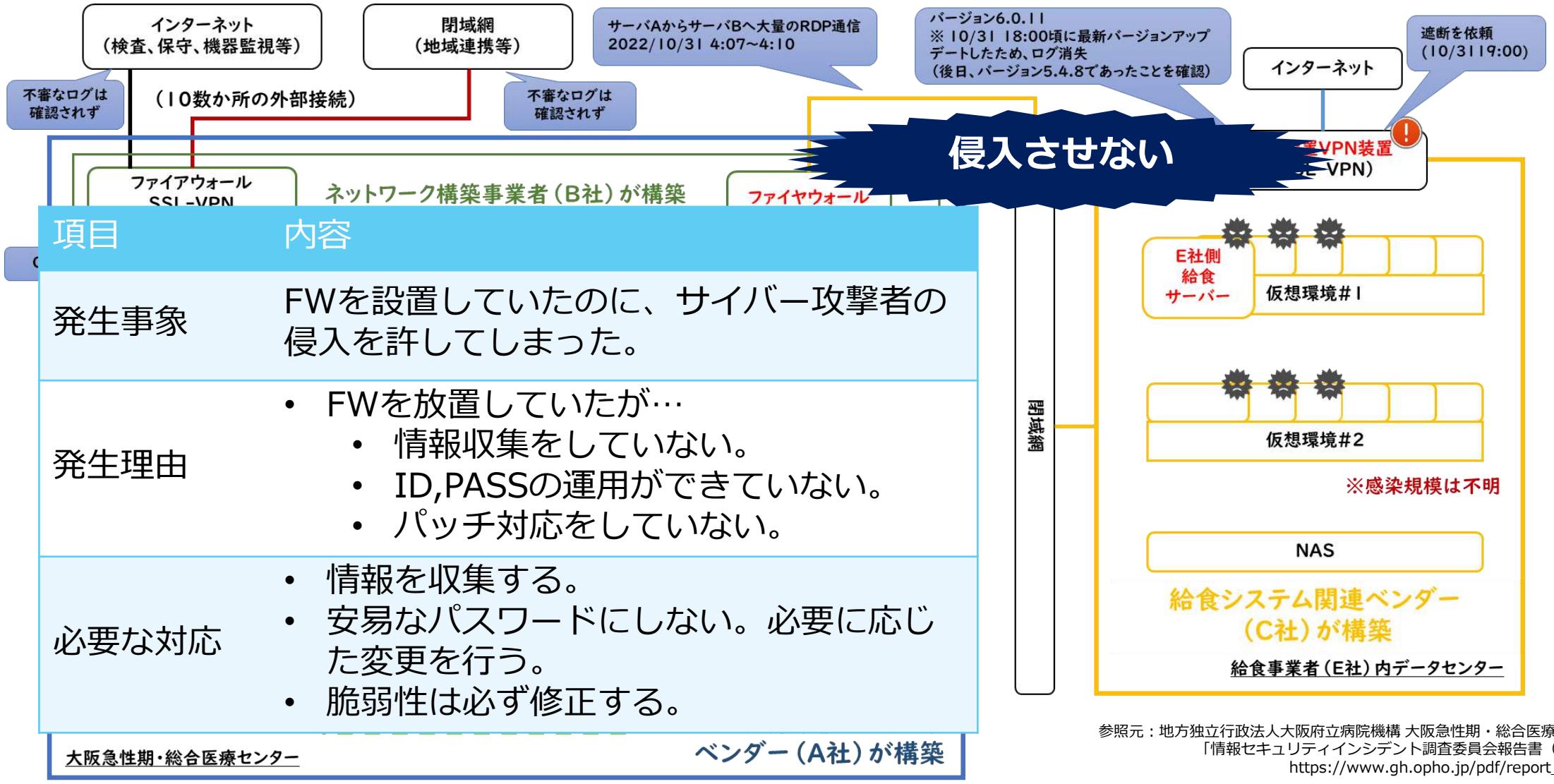


項目	内容
発生事象	サイバー攻撃者が「RDP」を悪用して侵入してきた。
発生理由	• ベンダーの指示とはいえRDP通信を許可してしまった。 • 常時接続できる状態を維持していた。 （開けたら窓は閉める…）

必要な対応	• 不用意に許可しない。
	• 許可したとしても…
	  • 常に許可する必要はない。
	  • ポート変更（標準ポート：3389）。

参照元：地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター
「情報セキュリティインシデント調査委員会報告書（PDF）」
https://www.gh.opho.jp/pdf/report_v01.pdf

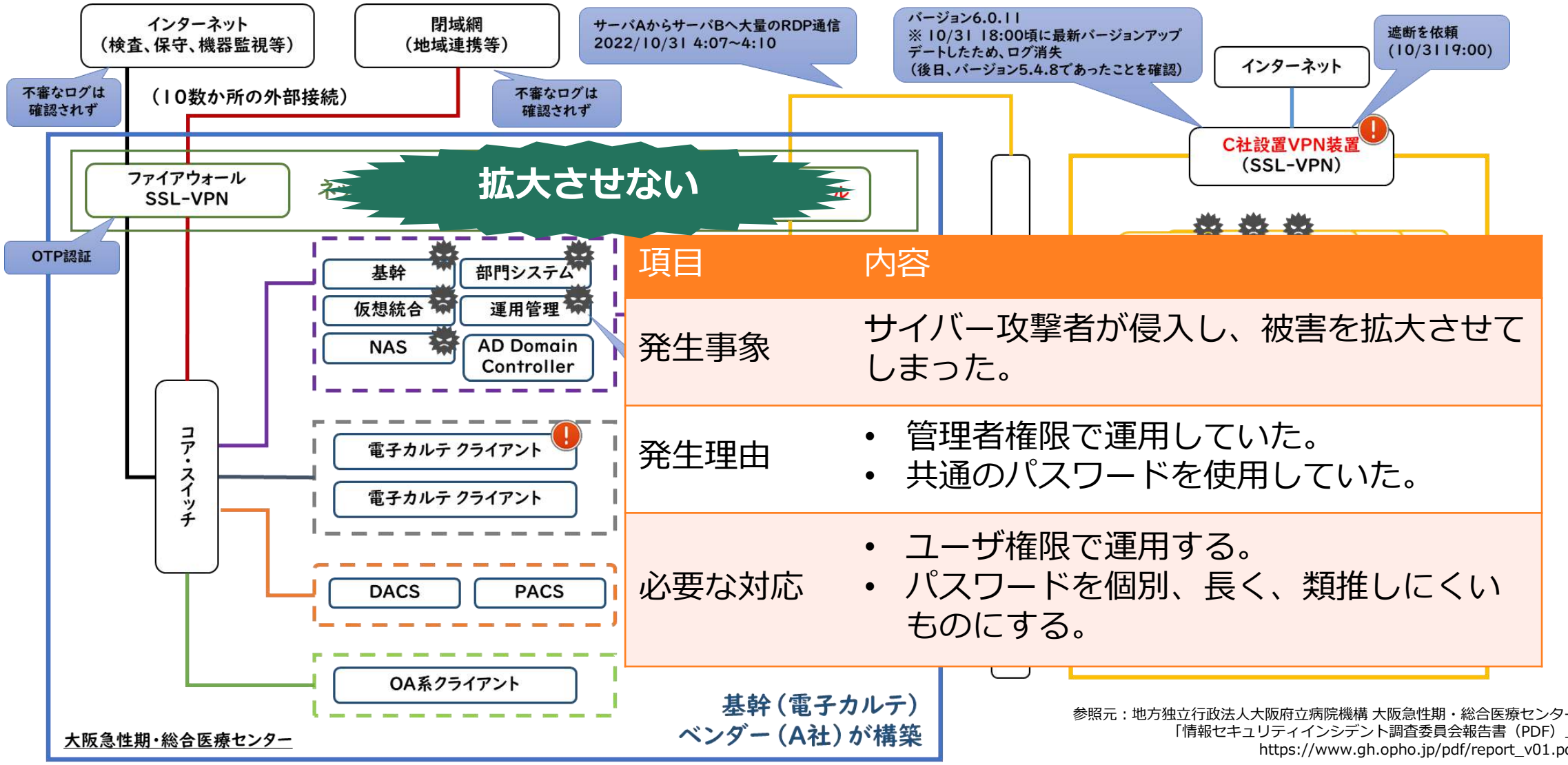
大阪急性期・総合医療センターからの学び④



項目	内容
発生事象	FWを設置していたのに、サイバー攻撃者の侵入を許してしまった。
発生理由	• FWを放置していたが… 　• 情報収集をしていない。 　• ID,PASSの運用ができていない。 　• パッチ対応をしていない。
必要な対応	• 情報を収集する。 • 安易なパスワードにしない。必要に応じた変更を行う。 • 脆弱性は必ず修正する。

参照元：地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター
「情報セキュリティインシデント調査委員会報告書（PDF）」
https://www.gh.opho.jp/pdf/report_v01.pdf

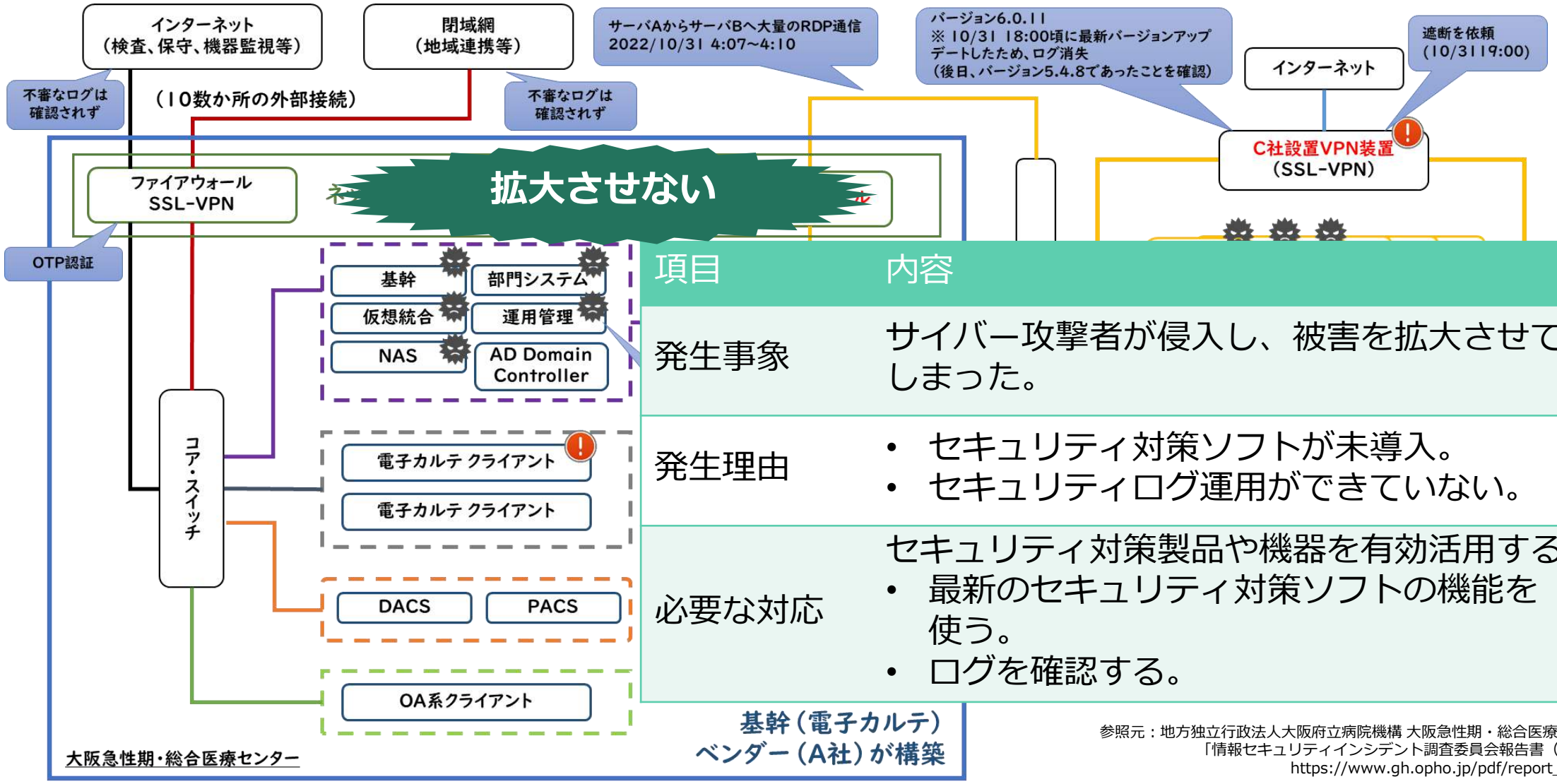
大阪急性期・総合医療センターからの学び⑤



項目	内容
発生事象	サイバー攻撃者が侵入し、被害を拡大させてしまった。
発生理由	• 管理者権限で運用していた。 • 共通のパスワードを使用していた。
必要な対応	• ユーザ権限で運用する。 • パスワードを個別、長く、類推しにくいものにする。

参照元：地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター
「情報セキュリティインシデント調査委員会報告書（PDF）」
https://www.gh.opho.jp/pdf/report_v01.pdf

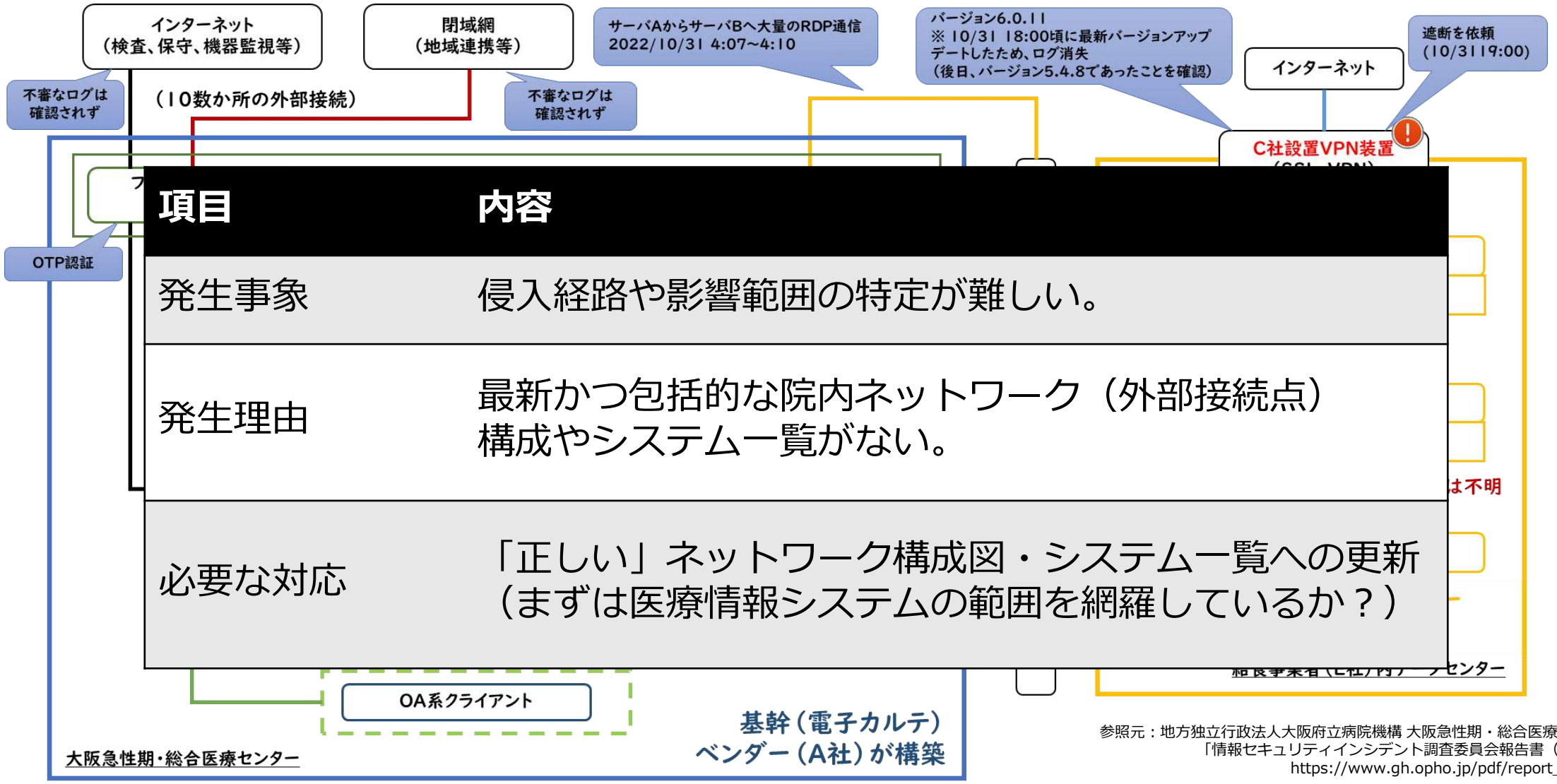
大阪急性期・総合医療センターからの学び⑥



項目	内容
発生事象	サイバー攻撃者が侵入し、被害を拡大させてしまった。
発生理由	• セキュリティ対策ソフトが未導入。 • セキュリティログ運用ができていない。
必要な対応	セキュリティ対策製品や機器を有効活用する。 • 最新のセキュリティ対策ソフトの機能を使う。 • ログを確認する。

参照元：地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター
「情報セキュリティインシデント調査委員会報告書（PDF）」
https://www.gh.opho.jp/pdf/report_v01.pdf

大阪急性期・総合医療センターからの学び⑦



項目	内容
発生事象	侵入経路や影響範囲の特定が難しい。
発生理由	最新かつ包括的な院内ネットワーク（外部接続点）構成やシステム一覧がない。
必要な対応	「正しい」ネットワーク構成図・システム一覧への更新（まずは医療情報システムの範囲を網羅しているか？）

参照元：地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター
「情報セキュリティインシデント調査委員会報告書（PDF）」
https://www.gh.opho.jp/pdf/report_v01.pdf

事例からちゃんと学んで活動

確認の必要性

- 閉域網は本当に閉域網なのか？ 構成や設計時の思想から時代は変わっていないか？

脆弱性の有無

- 運用における管理・設定不備はないか？導入後放置されているものはないか？

連携の必要性

- 経営層と連携はできているか？

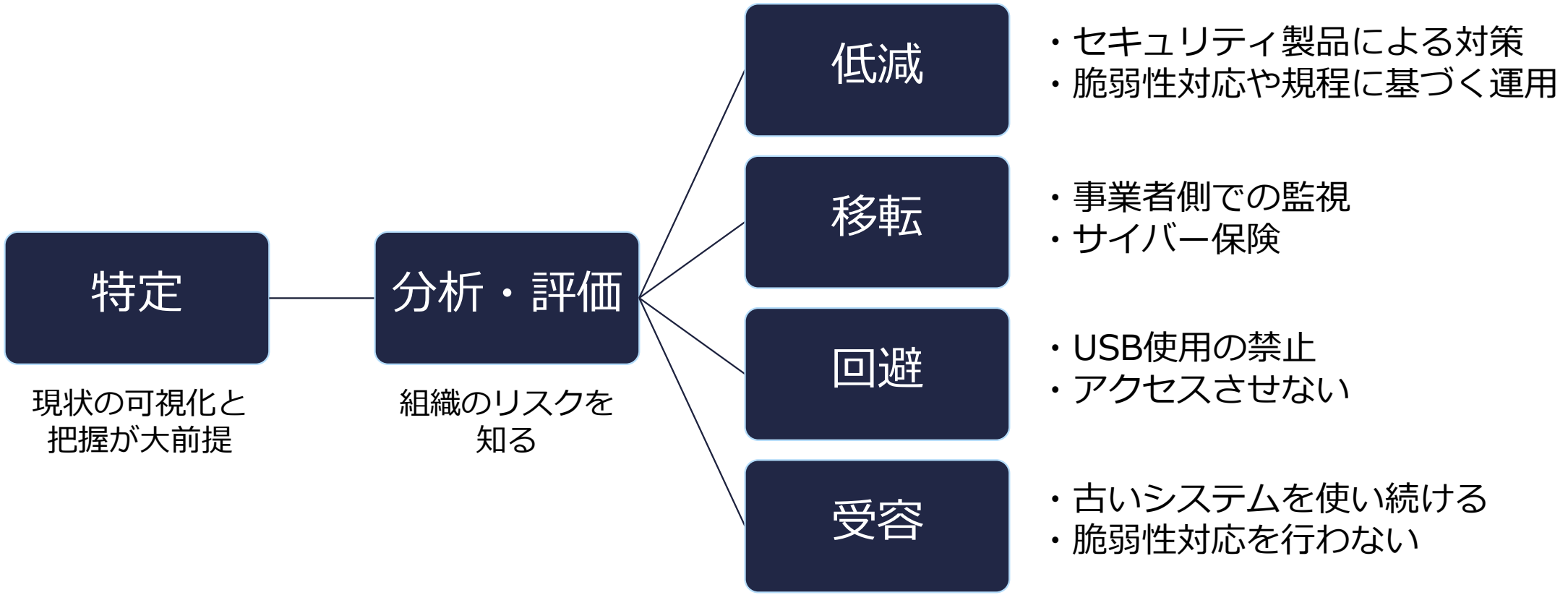
  問題が起きた際の連携や相談窓口は用意されているか？

組織での管理に向けて

～国の動向やガイドライン等の理解を深める～

情報資産・リスクの把握・分析から始まる

- **リスクベースアプローチ**に基づいたリスクマネジメントプロセスを定義
- 正しい共通理解と明示的な合意のもと医療情報システム等を運用するために、リスクコミュニケーションを実施

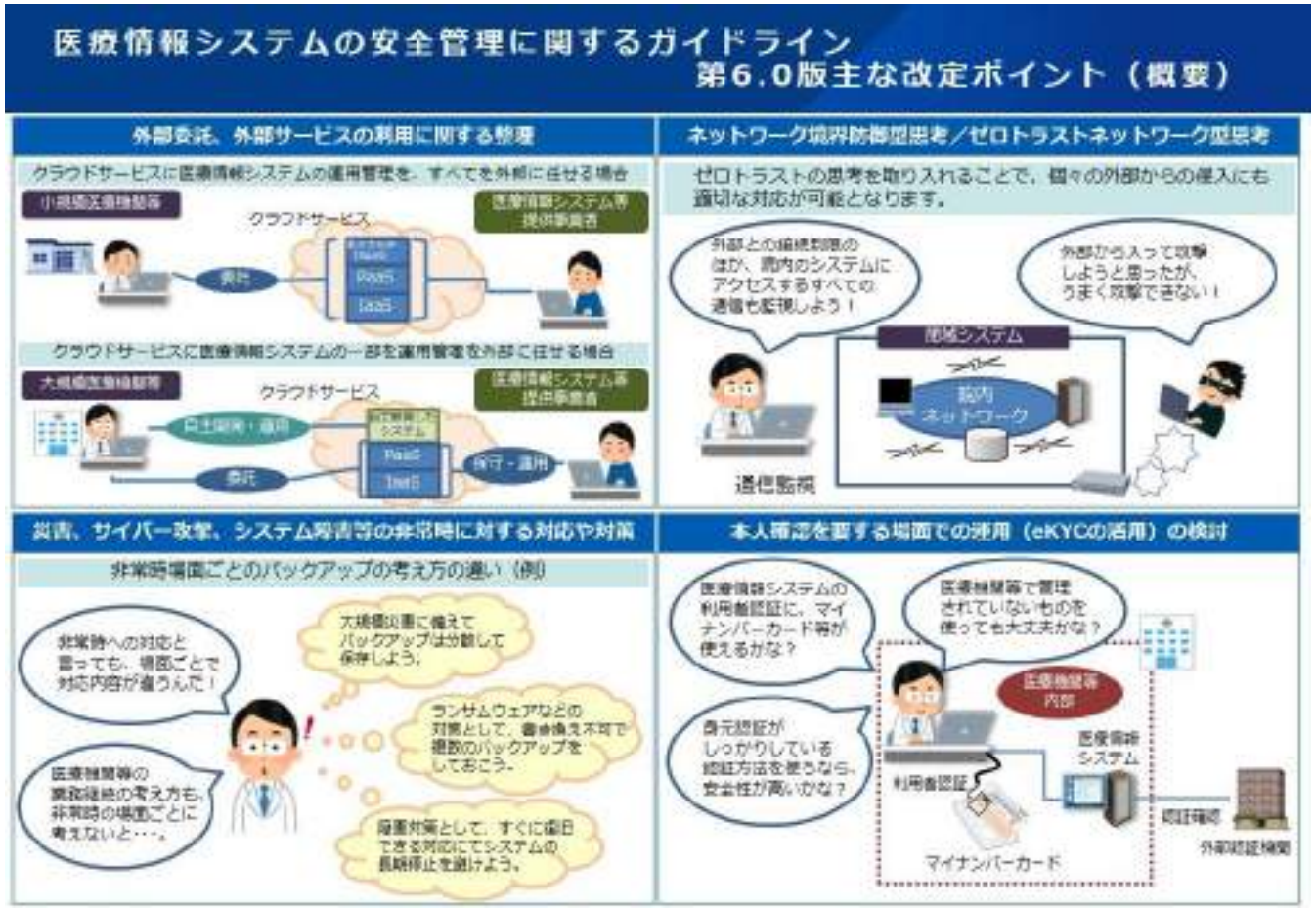


理解すべき前提

- 契約書や仕様書などに記載がない限りベンダーは基本対応しない。
- インシデントが起きたときに…
  - どの程度助けてくれるのか？
  - サプライチェーン側が原因でも調査ができるのか？
- おさえるべきガイドライン
  - **医療情報システムの安全管理に関するガイドライン（厚生労働省）**
  - 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン （経済産業省・総務省）
  - 医療機関における医療機器のサイバーセキュリティ確保のための手引書について（医政参発 0331 第１号,薬生機審発 0331 第 16 号,薬生安発 0331 第８号）

医療情報システムの安全管理に関するガイドライン

- 医療情報システムの安全管理に関するガイドライン（厚生労働省）
  - 医療機関が医療情報を委託する先に求めるべきセキュリティ対策として組織体制や設置基準、外部委託時に外部事業者と定める契約内容等を示したもの



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
（令和5年5月）

- 概説編（Overview）
- 経営管理編（Governance）
- 企画管理編（Management）
- システム運用編（Control）

目を通しておきましょう

厚生労働省「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」（2023/5)より

クラウドの誤解と経営者への説明

外部のシステムで医療情報を取り扱うのはリスクが高い？	**何もしない環境より危険？ 経験がないだけ？**
運用費が下がる？	**クラウドは常に 変化しているのに？**
全体のシステム構築費用は下がる？	**無駄なサーバ代はなくなる。 設計をしっかりと。**
BCPを考えたらクラウドは必須？	**電気や通信、筐体そして 空調などすべてがそろうか？**

日本のクラウドを理解する

● 責任共有モデル

クラウドサービスは、
- クラウド事業者
- 利用者

それぞれで**運用責任を共有**しており
二人三脚で成り立っているサービスです。

管理するデータや設定情報などについては利用者側の責任であることを
意識する必要があります。

基本的なクラウドサービスの責任共有モデルの考え方

● ステークホルダー

とりわけ日本においては、
システムインテグレーター（SIer）が
利用者から業務を請け負い、
クラウド事業者に代わりクラウドサービスを
提供するケースが少なくありません。

サービス利用に係る**それぞれのステークホルダーがどのような契約関係**にあるのか、
留意するようにしましょう。

クラウドサービスに係るステークホルダーの例

- 利用者側の責任や対応がなくなるわけではない。
- 実装形態をよく理解する。

- 誰が、どのようなことを、いつまでなど、契約をきちんと確認する。
- 使用許諾もできる限り読む。（事故発生時の対応、損害賠償、保守等）

NISC「クラウドを利用したシステム運用に関するガイダンス【概要】」
https://www.nisc.go.jp/policy/group/infra/cloud_guidance.html

ゼロトラスト

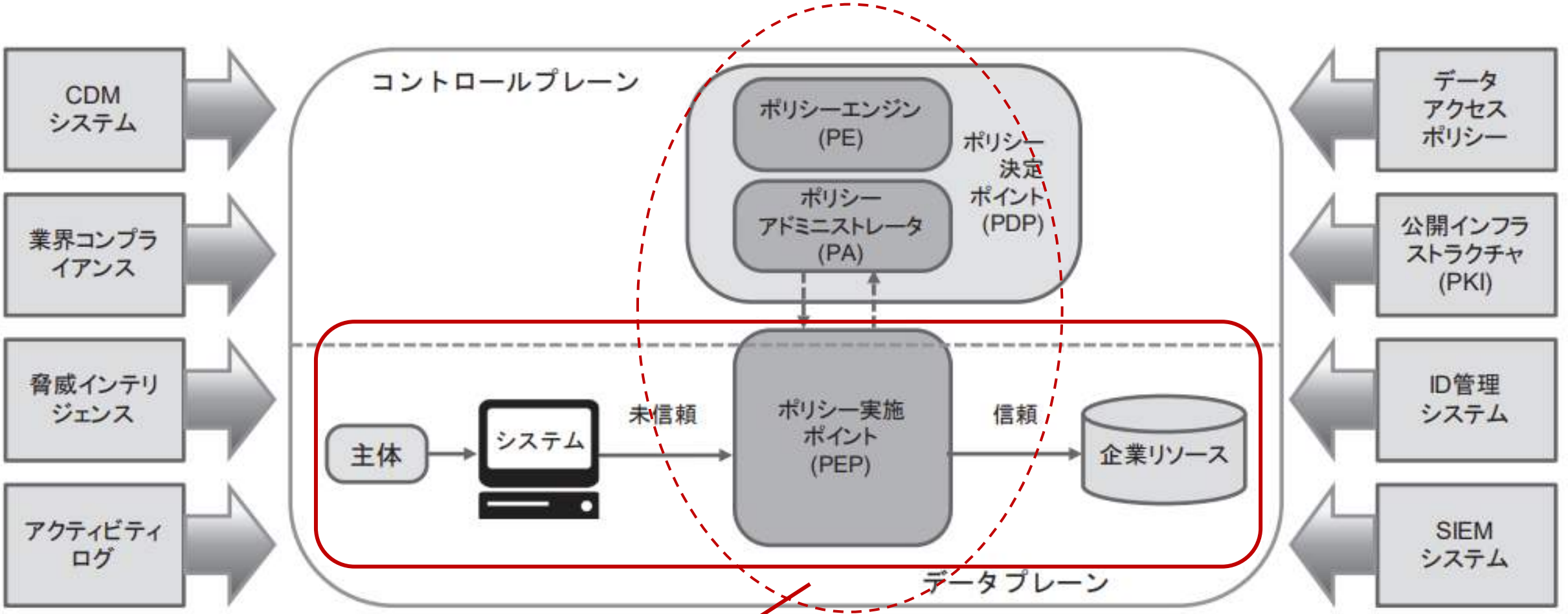
- **Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated.**
  - **ゼロトラストとは、リソース保護に焦点を当てたサイバーセキュリティのパラダイムであり、信頼は決して暗黙のうちに付与されるものではなく、継続的に評価されなければならないという前提である。**

- **Zero trust architecture is an end-toend approach to enterprise resource and data security that encompasses identity (person and nonperson entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure.**
  - **ゼロトラストアーキテクチャーは、アイデンティティ（人と人以外のエンティティ）、クレデンシャル、アクセス管理、運用、エンドポイント、ホスティング環境、および相互接続インフラストラクチャーを包含する、企業のリソースとデータのセキュリティに対するエンドツーエンドのアプローチである。**

- **The initial focus should be on restricting resources to those with a need to access and grant only the minimum privileges (e.g., read, write, delete) needed to perform the mission.**
  - **最初の焦点は、アクセスする必要のある者にリソースを制限し、ミッションの実行に必要な最小限の権限（読み取り、書き込み、削除など）のみを付与することである。**

参照：NIST「NIST SP800-207 Zero Trust Architecture」
*翻訳は機械翻訳

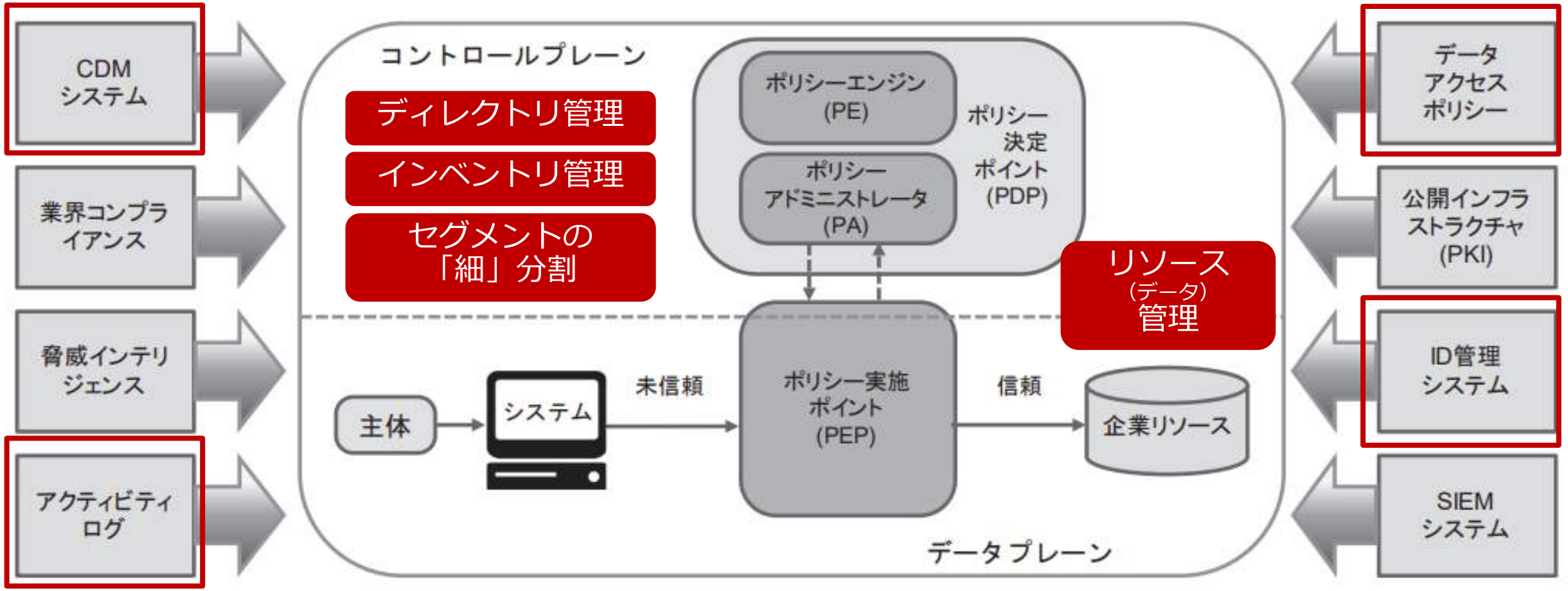
ゼロトラストの論理コンポーネント



組織のポリシーに応じて、許可、拒否等を決める

NIST SP800-207「ゼロトラスト・アーキテクチャ」
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/assets/pdf/zero-trust-architecture-jp.pdf

ゼロトラストの論理コンポーネント



*CDM(継続的診断および対策)システム：適切なパッチ適用済みOSを実行してるか、承認したソフトウェアコンポーネントの完全性、脆弱性があるかないかなど

NIST SP800-207「ゼロトラスト・アーキテクチャ」
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/assets/pdf/zero-trust-architecture-jp.pdf

ゼロトラストの考え方

全てのデータソースとコンピューティングサービスは**リソース**

ネットワークの場所に関係なく、**すべての通信**を保護

企業リソースへのアクセスは、**セッション単位**で付与

リソースへのアクセスは、ID、アプリケーション等を含めた**動的ポリシー**によって決定

全ての資産の整合性とセキュリティ動作を**監視し測定**

リソースへの認証と認可は動的に行われ、アクセスが許可される前に厳格に実施

可能な限り多くの**情報を収集**し、セキュリティ対策の改善に利用

すぐソリューションを入れたら「ゼロトラスト」が実現するわけではない。

↓

これまで（またはこれから）の<u>セキュリティの積み上げ</u>なしに「ゼロトラスト」実現はありえない。

参照：NIST「NIST SP800-207 Zero Trust Architecture」

組織の管理のポイント（再掲）

1. 経営者に現場責任者・担当者の苦労を伝える・説明する。
（たとえ最初は聞く耳を持たなくても、たとえ一方的な話でも…）
2. これまでの医療界のセキュリティの常識は、他の業界での非常識。
3. ほとんどのインシデントは「高度なサイバー攻撃」ではなく、「設定や対応の不備」から起きている。
4. どの業界でも「人材不足」。まずはできることからやる。
（セキュリティを足し算から掛け算にする。）
5. 己を知ることから始まる。敵を知っている場合ではない。
6. サイバーセキュリティは医療を止めないための一手段。
7. 「ITガバナンス」や「ゼロトラスト」は一日にしてならず。

ありがとうございました。

次回は10月26日(木)、
管理や設定について具体的に深掘りしていきます。

※本日の講義でご紹介したリンク先は、アンケートに記載しております。
本研修ではリアルタイムでの質問はお受けしておりません。
ご質問のある方は、アンケートにご記入ください。

https://forms.gle/rN3kaD3JPSUnhtWo7