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

【導入研修】

大阪急性期・総合医療センター事例
＜概要編＞

2024年1月12日

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））

※本コンテンツで利用する写真等については本研修の投影のみです。

本研修の構成

開催回	日程	概要	講師
第１回	2024年1月12日 18時～	概要編	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	2024年1月22日 18時～	技術編	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３回	2024年2月5日 18時～	組織編	加藤 智巳 (株)ラック、(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。

２つの報告書

つるぎ町立半田病院

https://www.handa-hospital.jp/topics/2022/0616/index.html

大阪急性期・総合医療センター

https://www.gh.opho.jp/important/785.html

本研修の目的

インシデント報告書を読んでいない方も理解する

報告書の記載内容の重要なポイントをつかむ

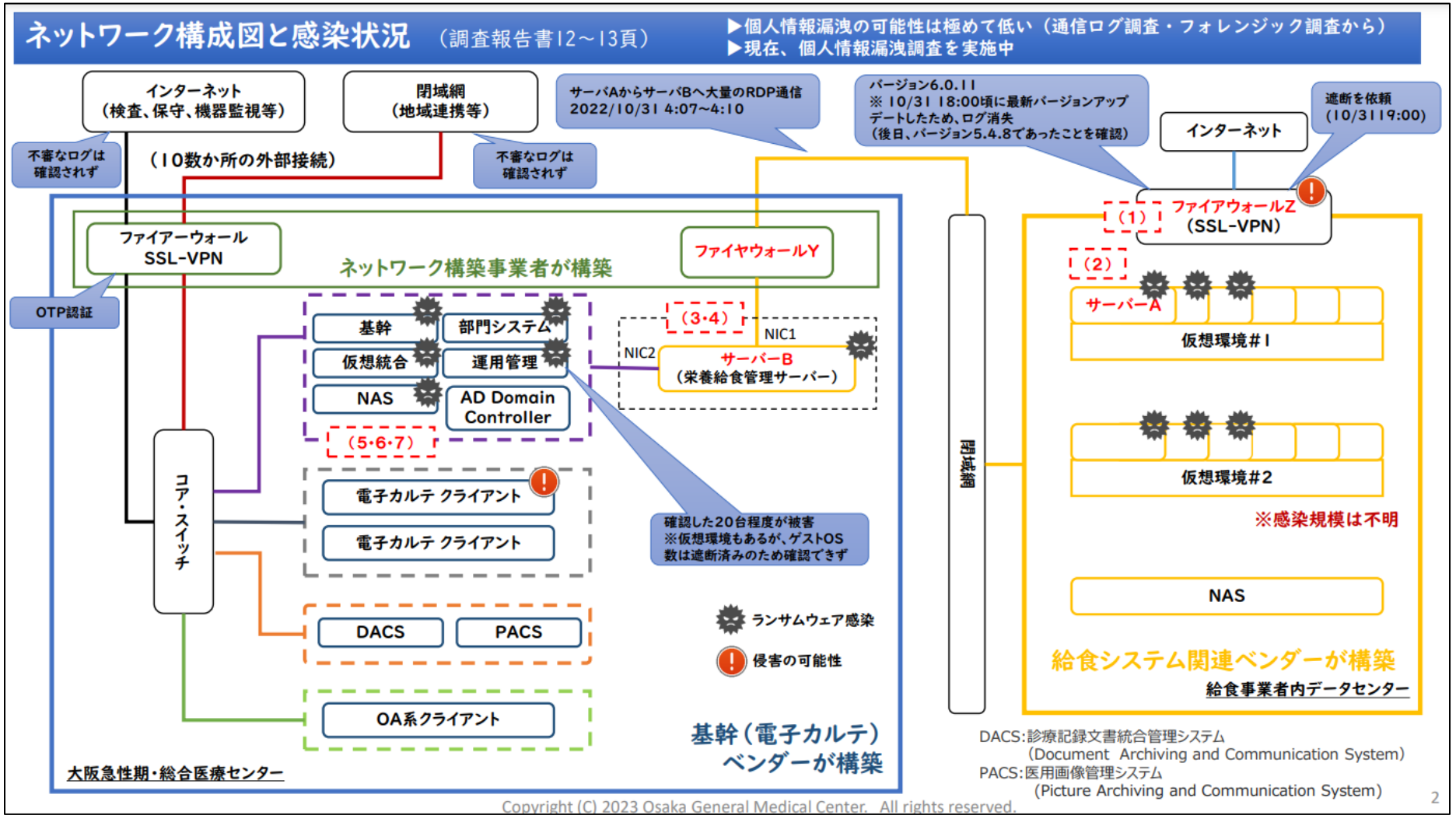
あれから１年…継続的な取り組みを知ることができる

agenda

- インシデントの振り返り
- 広報対応
- 様々な学び
  - 本当に紙カルテ運用をするのか／バックアップはデータだけではない／参照環境をすぐ構築できるのか／マニュアルは手元にあるか／どこで会議や作業を行うのか　など
- 法的な対応の必要性

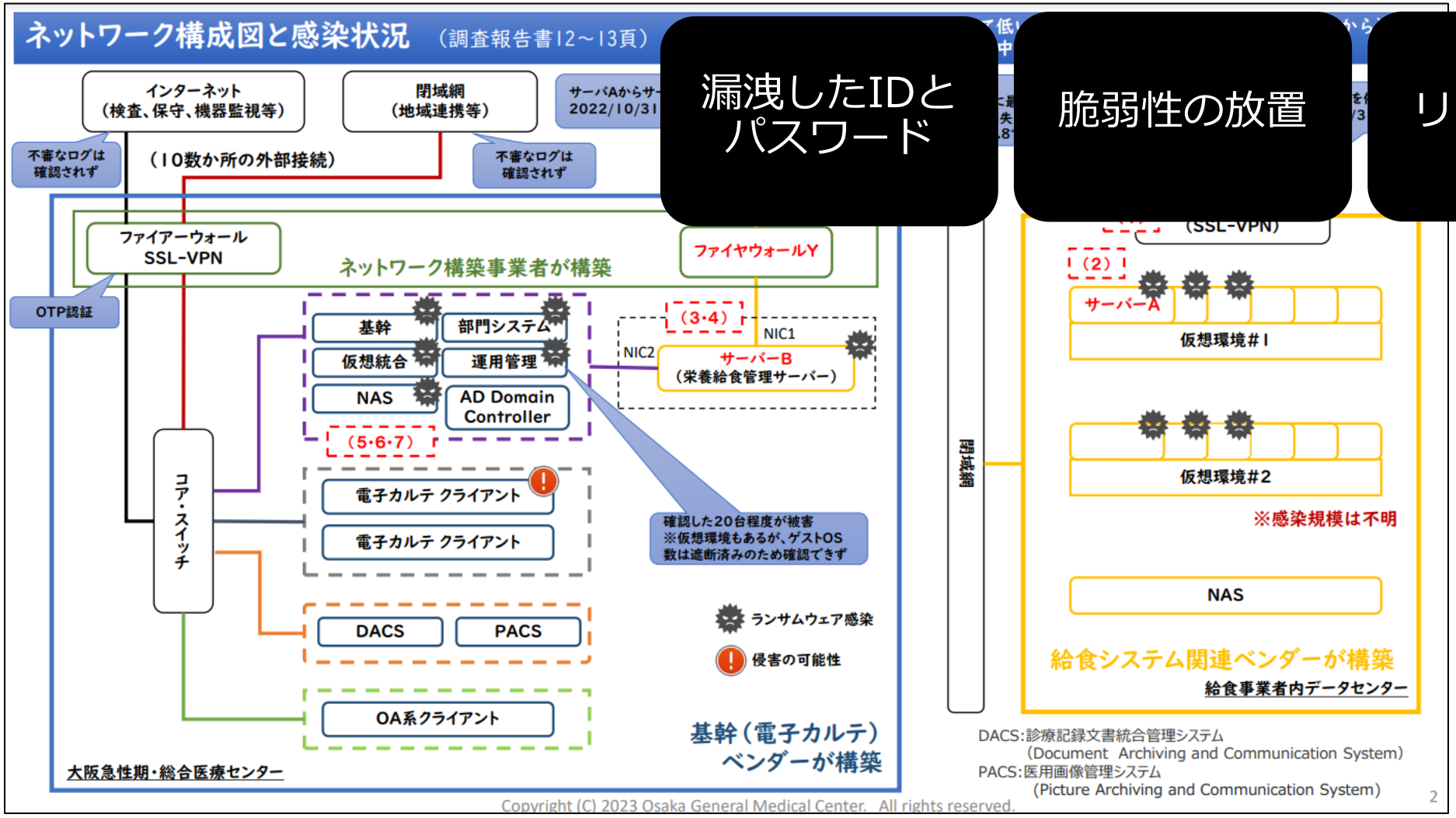
大阪急性期・総合医療センターのインシデント

情報セキュリティインシデント調査委員会報告書について | 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 (opho.jp)



大阪急性期・総合医療センターのインシデント

情報セキュリティインシデント調査委員会報告書について | 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 (opho.jp)



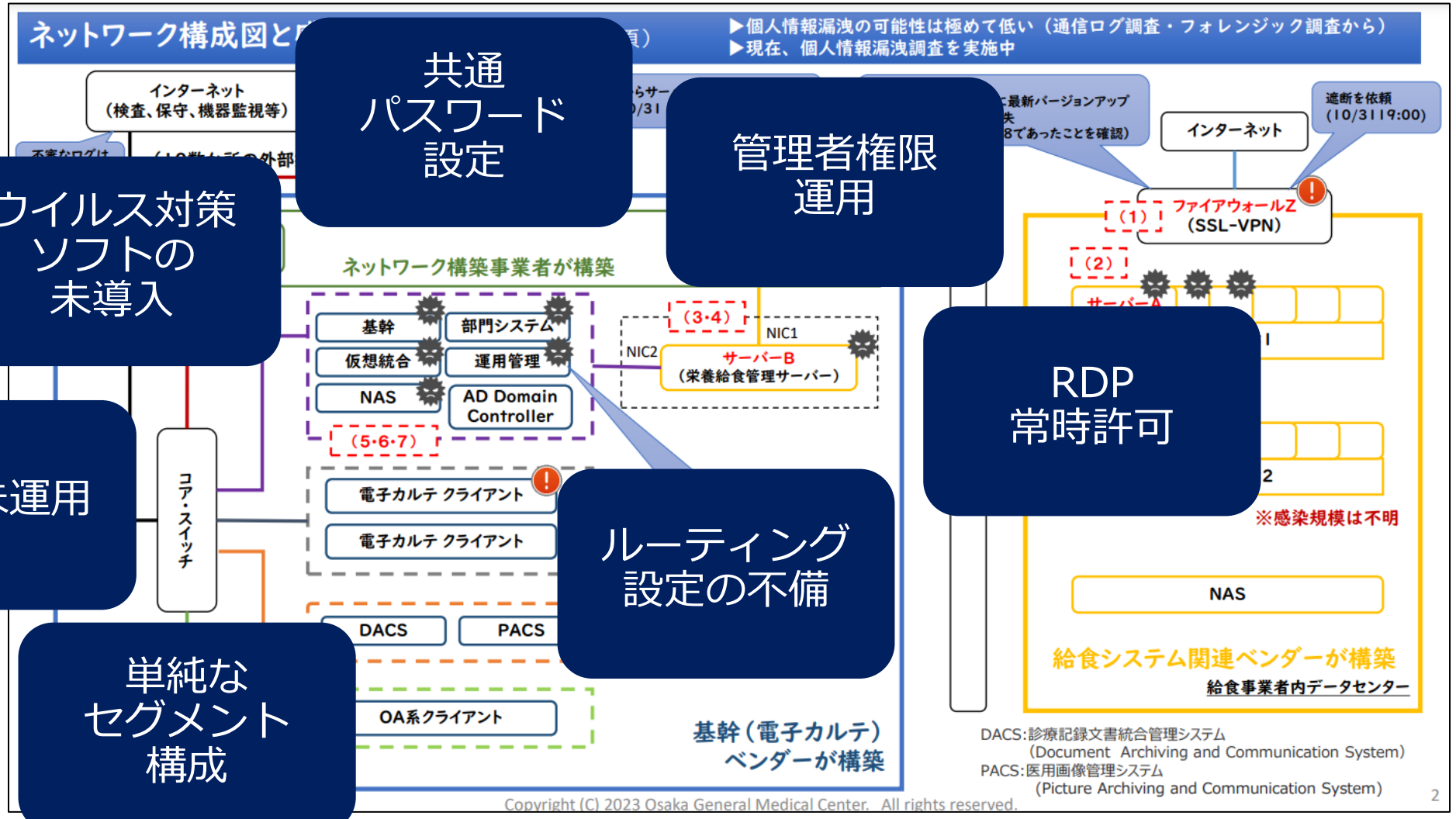
漏洩したIDとパスワード

脆弱性の放置

(甘い)
リモート接続環境

大阪急性期・総合医療センターのインシデント

情報セキュリティインシデント調査委員会報告書について | 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 (opho.jp)



共通
パスワード
設定

管理者権限
運用

ウイルス対策
ソフトの
未導入

RDP
常時許可

ログの未運用

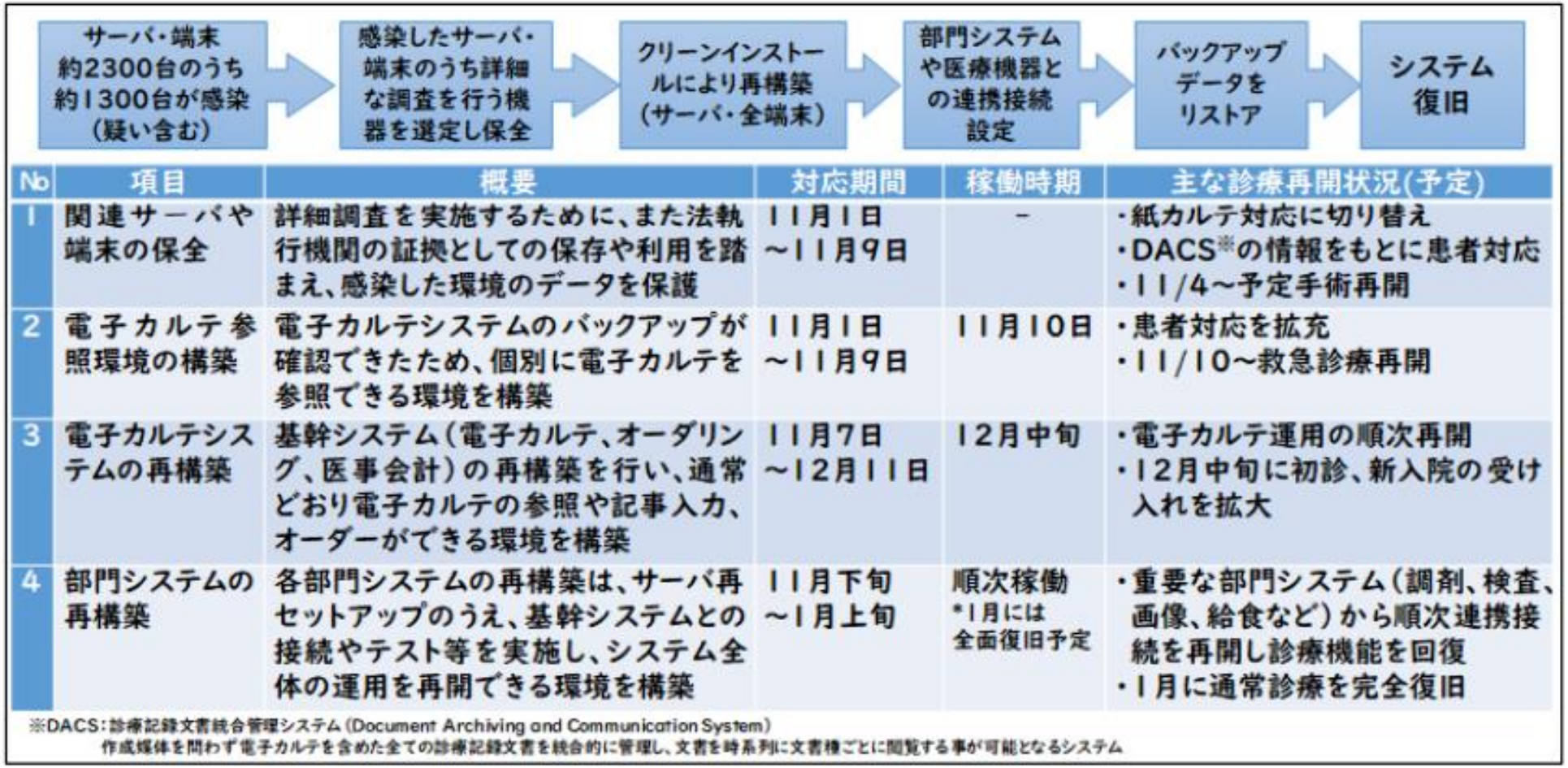
ルーティング
設定の不備

単純な
セグメント
構成

※詳細は技術編

復旧までの流れ

情報セキュリティインシデント調査委員会報告書について | 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 (opho.jp)



No	項目	概要	対応期間	稼働時期	主な診療再開状況(予定)
1	関連サーバや端末の保全	詳細調査を実施するために、また法執行機関の証拠としての保存や利用を踏まえ、感染した環境のデータを保護	11月1日 ～11月9日	-	・紙カルテ対応に切り替え ・DACS※の情報をもとに患者対応 ・11/4～予定手術再開
2	電子カルテ参照環境の構築	電子カルテシステムのバックアップが確認できたため、個別に電子カルテを参照できる環境を構築	11月1日 ～11月9日	11月10日	・患者対応を拡充 ・11/10～救急診療再開
3	電子カルテシステムの再構築	基幹システム(電子カルテ、オーダリング、医事会計)の再構築を行い、通常どおり電子カルテの参照や記事入力、オーダーができる環境を構築	11月7日 ～12月11日	12月中旬	・電子カルテ運用の順次再開 ・12月中旬に初診、新入院の受け入れを拡大
4	部門システムの再構築	各部門システムの再構築は、サーバ再セットアップのうえ、基幹システムとの接続やテスト等を実施し、システム全体の運用を再開できる環境を構築	11月下旬 ～1月上旬	順次稼働 *1月には全面復旧予定	・重要な部門システム(調剤、検査、画像、給食など)から順次連携接続を再開し診療機能を回復 ・1月に通常診療を完全復旧

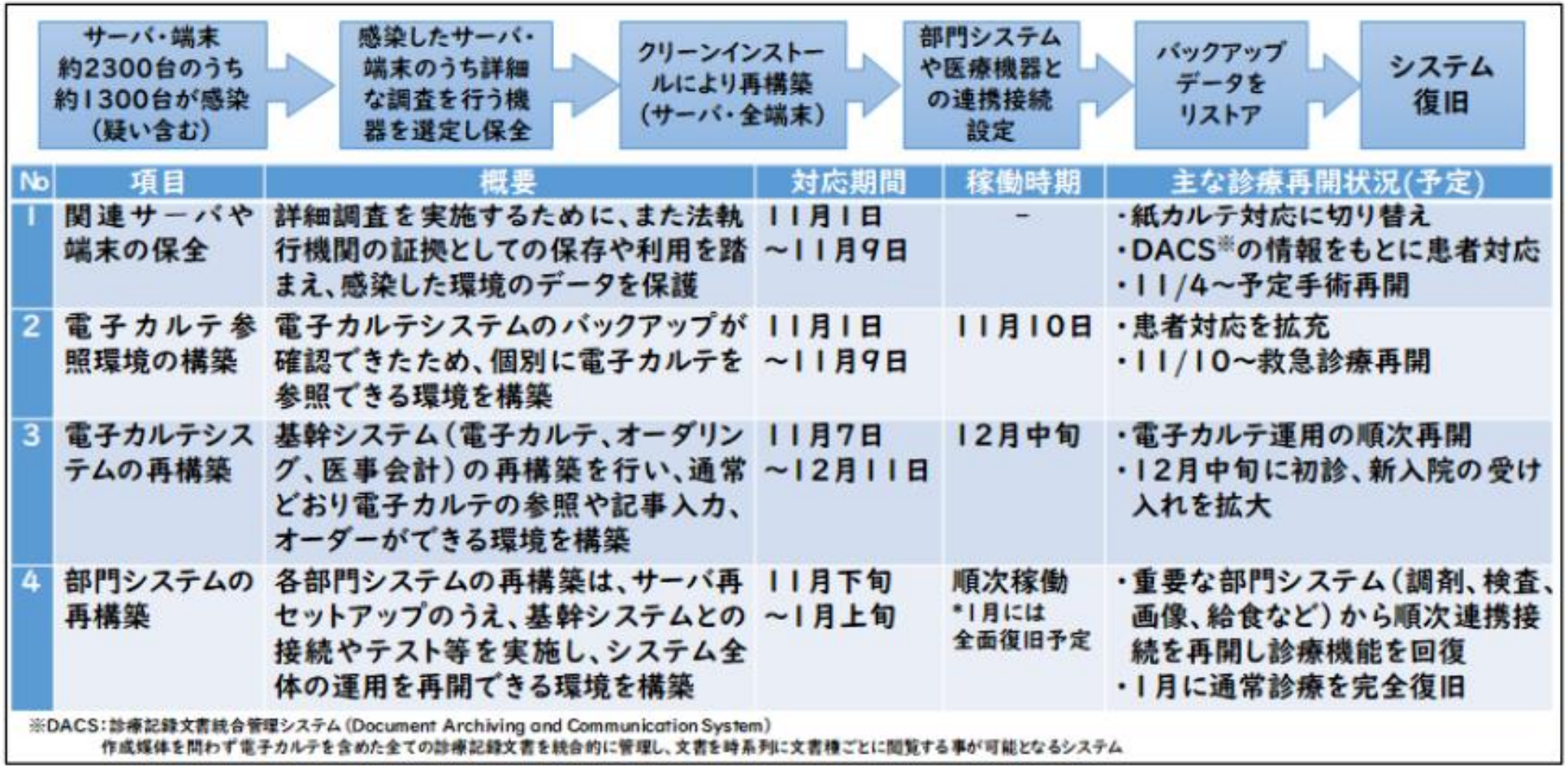
※DACS:診療記録文書統合管理システム (Document Archiving and Communication System)
作成媒体を問わず電子カルテを含めた全ての診療記録文書を統合的に管理し、文書を時系列に文書種ごとに閲覧する事が可能となるシステム

図 9　システム復旧方針

※詳細は技術編

復旧までの流れ

情報セキュリティインシデント調査委員会報告書について | 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 (opho.jp)



No	項目	概要	対応期間	稼働時期	主な診療再開状況(予定)
1	関連サーバや端末の保全	詳細調査を実施するために、また法執行機関の証拠としての保存や利用を踏まえ、感染した環境のデータを保護	11月1日 ～11月9日	-	・紙カルテ対応に切り替え ・DACS※の情報をもとに患者対応 ・11/4～予定手術再開
2	電子カルテ参照環境の構築	電子カルテシステムのバックアップが確認できたため、個別に電子カルテを参照できる環境を構築	11月1日 ～11月9日	11月10日	・患者対応を拡充 ・11/10～救急診療再開
3	電子カルテシステムの再構築	基幹システム(電子カルテ、オーダリング、医事会計)の再構築を行い、通常どおり電子カルテの参照や記事入力、オーダーができる環境を構築	11月7日 ～12月11日	12月中旬	・電子カルテ運用の順次再開 ・12月中旬に初診、新入院の受け入れを拡大
4	部門システムの再構築	各部門システムの再構築は、サーバ再セットアップのうえ、基幹システムとの接続やテスト等を実施し、システム全体の運用を再開できる環境を構築	11月下旬 ～1月上旬	順次稼働 *1月には全面復旧予定	・重要な部門システム(調剤、検査、画像、給食など)から順次連携接続を再開し診療機能を回復 ・1月に通常診療を完全復旧

※DACS:診療記録文書統合管理システム (Document Archiving and Communication System)
作成媒体を問わず電子カルテを含めた全ての診療記録文書を統合的に管理し、文書を時系列に文書種ごとに閲覧する事が可能となるシステム

図 9　システム復旧方針

※詳細は技術編

ITガバナンスの欠如

情報セキュリティインシデント調査委員会報告書について | 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 (opho.jp)

組織的発生要因と予防に向けた提案 （調査報告書15～17頁）

①ITガバナンスの欠如

No	ITガバナンスにおける主な問題点	予防に向けた提案
1	各契約単位で、保守や脆弱性管理といったセキュリティに関する責任分界点と役割が明確になっていない領域が存在した。	契約毎に、受注者と「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（総務省・経済産業省）」に基づいたサービス仕様適合開示書及びサービス・レベル合意書（SLA）により双方の責任分界点や役割を明確にし、文書化すること。
2	複数のベンダーが関与する契約において、そのプロジェクトマネジメント体制が明確になっていない状況があり、重要なセキュリティに関する事項について、関係者による十分なリスク評価が行われていないケースがあった。	合同企業体（JV）によるプロジェクトの場合（構築だけでなく保守も含む）は、受注側のプロジェクト体制を明確にさせるなど、責任の所在を明確にすること。
3	医療機器やその保守に係るセキュリティ仕様が、総合情報システムにおけるセキュリティ仕様に適合していないケースがあり、運用が共通化されていなかった。	調達が行われる場合には、病院共通のセキュリティポリシーに基づく共通仕様を作成し、共通運用となるような調達を行うこと。
4	医療情報部で調達している情報資産以外の医療機器（リモート保守用機器を含む）や建築関係の情報システムについて、一元管理されていなかった。	診療情報系のネットワークに接続されている機器やシステムはすべて情報資産としてリストアップしたうえで、安全管理上の重要度に応じて分類し、リスク分析を実施すること。
5	総合情報システムの仕様における「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）」は第4.3版であるが、現時点では第5.2版まで更新されている。第5.2版についてベンダーを交えて組織的に検証されている状況が確認されなかった。	ガイドライン改定時には組織的に適合状況を確認し、不足している項目があれば改善に向けたPDCAサイクルを回す活動を行うこと。
6	2022年4月より診療報酬で位置づけられた医療情報システム安全管理責任者について、その役割等の組織内での認知が不十分のようであった。	医療情報システム安全管理責任者を軸としたITガバナンスを効率的効果的に運用する組織体制を構築すること。

4

※詳細は組織編

広報対応

インシデント当日の速報対応

幹部会での対応決定後、即座にWeb対応。

速報として診療停止のお知らせ。

システム障害のため、本日は 診察を停止しております。

ご迷惑をおかけしますが、ご理解いただきますようお願いいたします。

明日以降の診察は、当センターホームページをご確認ください。

https://www.gh.opho.jp/（2022年10月31日）

２回実施した記者会見

記者会見の実施

- 情報をより多くの人に届けるため（特に高齢者など）
- 基幹病院としての社会的な説明責任を果たすため
- 当日は発生内容を、1週間後には原因や対応方針を伝えるため
- 情報公開に対する誠意を示すため

ホームページの更新

表 9　ホームページ掲載経過

日付	報数	内容
10 月 31 日	速報	システム障害のため、診察停止を案内。
	第 1 報	緊急以外の手術や外来診療の一時停止など通常診療ができない状況。
11 月 1 日	第 2 報	復旧目途が立っていない状況。
11 月 2 日	第 3 報	予定手術は一部再開も、引き続き、外来診療については一時停止の状況。
11 月 4 日	第 4 報	予定手術を 5 件実施も、引き続き、外来診療については一時停止の状況。
11 月 9 日	第 5 報	11/10 から電子カルテの参照可能になる状況。
11 月 6 日	第 6 報	11/10 から三次救急受入再開、11/17 から一般救急患者の受け入れ再開へ。
12 月 12 日	第 7 報	12/12 から電子カルテを含めた基幹システムが再稼働。外来から順次電子カルテ端末を設置し、電子カルテの参照や記事入力、一部のオーダーが可能になる。
12 月 22 日	第 8 報	通常診療の再開へ。 電子カルテ端末の再配置と部門システムの復旧が進み、ほぼすべての診療科において外来の初診患者受付を再開。病棟においても電子カルテ運用を再開し、紙運用を終了。
1 月 10 日	第 9 報	1/11 からの診療体制復旧を宣言（図 8）。

情報セキュリティインシデント調査委員会報告書について | 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 (opho.jp)

様々な学び

災害対応に迅速にシフトできた

【実際の対応】
22年10月31日 8時40分：ネットワーク遮断　→　8時50分：幹部会議招集・方針決定

【対応に向けた準備】
- サイバー攻撃においてもすぐに対応できる体制にあるか
- 迅速に必要な人を集められる、連絡ができるか
- クロノロジーが書ける（人やモノなど）があるか

紙カルテ運用

準備（定期的な訓練、紙など）

電子カルテが動作しない

紙カルテ運用へ移行

紙カルテ運用時の課題

ワープロ不足

- 電カル端末すべてが疑義端末になったため、安全といえる端末がなかった（そこまでの準備ができていなかった）。

紙・トナー不足

- 一気に、また長期的な紙運用になったので、紙や印刷に使うトナーが不足した。

字が読めない

- 人の字はそれぞれで、また急いで書いていたりすると、内容や指示に誤りが生じる可能性

経験が浅い

- 特に若い先生は電子カルテがメインで紙カルテの記入や運用に慣れていなかった。

医療継続に向けた検討と準備

1. ワープロ機能としてでもPCを準備する
2. インシデント発生時の調達数や調達元を協議・決定する
3. BYODを一時的に認めるか協議・決定する
   - 許可する場合はどのようにインシデント対応機関のセキュリティを担保するのかも含め

バックアップ

医療情報をどのように保管するか議論していた

オンライン環境×　オフライン環境〇

遠隔地保管のオフラインバックアップから復旧

バックアップと言っても色々

データ

設定情報

ソフトウェア

ハードウェア

ネットワーク

備品

電気

そもそも戻せるのか…？

医療継続に向けた検討と準備

1. オフラインバックアップの検討
2. クラウドの活用検討
   - オンプレミス環境とクラウド環境でのバックアップの負荷の違いを考える。
   - 抵抗があるのであれば、緊急時には一時的に許可するなどの検討と決定を行う。
   - クラウド電カルの活用検討

参照環境

準備（サーバ、環境など）

DACS環境構築・電カルサーバ調達

DACS利用・電カル参照環境の構築

参照環境を考えるときに…

データ

設定情報

ソフトウェア

ハードウェア

ネットワーク

備品

電気

＋

人的、物理的側面は大丈夫か？

- 【人的】対応できる人材がいるか【物理的】空調、ラック、機器等を設置する場所 等

医療継続に向けた検討と準備

1. 組織としてのクラウド活用の方針・考え方の明確化
2. 特にオンプレミス環境において、全サーバや端末が感染したことを想定して、どのように参照環境を構築するのか検討と決定
   - ハードウェアも直ぐには調達はできない
   - サーバルームが使えなかったら、どのように冷却するのか　など

災害用紙様式・マニュアル類の確保

災害用の紙様式データやマニュアル類が、電子カルテ上にあるグループウェアや、
各所属の端末に保存

自然災害用の紙様式はあったが、短期間を見据えた様式で、
定期的な見直しもできていない

府立病院機構全体のネットワーク上にあるグループウェアを活用

医療継続に向けた検討と準備

1. 電力ルシステムの情報共有に依存していないか。
2. マニュアルや各種テンプレートは最新の形式で、すぐに確認できる状況になっているのか。
3. 長期間の停止を想定したオペレーションになっているか。
4. 代替案を準備し、緊急時に動ける体制にあるか。

様々な混乱

外来受付

患者情報

電話回線

会議室の確保

法的な対応の必要性

契約や仕様のあいまいな表現の回避

「＊＊ガイドライン」に準拠することからより詳しく、より細かく

- セキュリティ設定は、どの組織がどの程度実施してくれるのか。（過去のインシデント報告書を参考にインシデントが起きにくい環境を構築してくれるのか。）
- パスワードや脆弱性対応、ログの確認など、日々の運用はどのように行うのか、またどの程度実施してくれるのか。
- 部門システムをはじめとした再委託に相当する組織はどのようなセキュリティを実施するのか。また、インシデント発生時には調査が可能な体制であるか。
- 外部接続を伴う場合、どのように接続を行ってくるのか。接続元のセキュリティ状況は。

特に今回課題となったポイントは検討が必須

1. セキュリティ設定
2. 強固なパスワードの設定と運用
3. ロックアウトの設定
4. 権限管理（管理者権限の最小化）
5. サプライチェーンも含めた（外部接続）監視、監督、対応
6. 安全なリモート接続の設定、監査
7. OS、アプリケーションのバージョン管理

日進月歩の変化に対応するために

各種ガイドラインは定期的に更新や、新たな公開が行われている

- きちんと更新や公開の情報を確認する体制にあるか。
- 変更が生じた場合、対応の議論を行っているか。
- ベンダーはどこまで、その変化や対応に向き合ってくれるのか。
- 厚生労働省が公開している「医療情報システムの安全管理に関するガイドライン」や通達は勿論のこと、インシデントの報告書などを参照しているか。

医療にかかわるベンダーの必読書

- **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（医政発 0331 第１号,薬生機審発 0331 第 16 号,薬生安発 0331 第８号）
- コンピュータウイルス感染事案有識者会議調査報告書（つるぎ町立半田病院）
- 情報セキュリティインシデント調査委員会報告書（大阪急性期・総合医療センター）

→仕様書にもきちんと含め、ベンダーの理解と対応を求める。

セキュリティを継続する組織に向けて

医療情報システム安全管理委員会の設置

- 医療情報システムに係る導入や変更
- 適正利用に関する継続的な監視
- 各種ガイドラインに関する対応
- 外部接続の承認や管理
- セキュリティ対策やバックアップの管理
- インシデント発生時の対応　など

本日のより詳しい内容は技術編と組織編でご紹介します。本日もご参加ありがとうございました。

次回は１月22日「技術編」です。

※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/f31nBfrQPHLV6Zon9