令和7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

【システム・セキュリティ管理者向け研修】

クラウドサービスの活用とセキュリティの考え方

2025年10月9日
一般社団法人ソフトウェア協会

目的

- クラウドサービスの基本的な種類（IaaS、SaaSなど）と、それぞれの特徴を理解する
- 医療機関におけるクラウドサービス導入の考慮点を把握する
- 個人情報保護、データ可用性、インシデント対応といった、医療分野に特化したクラウドセキュリティの重要事項を把握する
- クラウド事業者の選定時や契約時に確認すべきセキュリティに関する具体的なポイントを理解する
- クラウドサービスを安全に運用するための管理体制や継続的な対策の重要性を認識する

目次

- クラウドサービスの基本と医療現場での活用
- IaaS利用におけるリスク管理と実践
- SaaS利用におけるリスク管理と実践
- クラウド導入検討・評価時に確認すべきセキュリティのポイント

クラウドサービスの基本と医療現場での活用

クラウドサービスとは？

クラウドコンピューティングの概念

クラウドとは、インターネット経由でサーバー、ストレージ、データベース、ソフトウェアといったコンピューティングリソースを利用できるサービス

オンプレミス

- ハードウェアの購入、設置、運用、メンテナンスを自院で行う必要がある

クラウド

- 必要な時に必要な分だけリソースを借りて利用する

クラウドサービスとは？

3つの主要なサービスモデル

クラウドサービスは、提供されるリソースの範囲によって、大きく3つのモデルに分類されます。それぞれの特徴と責任範囲を明確にすることで、管理者がセキュリティ対策を検討する際の基盤を提供します。

区分	IaaS	PaaS	SaaS
設定	ポリシー	ポリシー	ポリシー
	設定	設定	設定
	端末	端末	端末
アプリ	データ	データ	データ
	アプリケーション	アプリケーション	アプリケーション
環境	ランタイム	ランタイム	ランタイム
	ミドルウェア	ミドルウェア	ミドルウェア
	コンテナ管理機能	コンテナ管理機能	コンテナ管理機能
OS	オペレーティングシステム	オペレーティングシステム	オペレーティングシステム
仮想化	仮想化ソフトウェア	仮想化ソフトウェア	仮想化ソフトウェア
	ハードウェア	ハードウェア	ハードウェア

利用組織が管理　クラウド事業者が管理

【出展元】
国家サイバー統括室
クラウドを利用したシステム運用に関するガイダンス
https://www.nisc.go.jp/policy/group/infra/cloud_guidance.html

クラウドサービスとは？

IaaS（Infrastructure as a Service）

- 基盤（サーバー、ストレージ、ネットワーク）の管理はクラウド事業者
- OS、アプリケーション、データのセキュリティは利用者の責任

区分	IaaS	PaaS	SaaS
設定	ポリシー	ポリシー	ポリシー
	設定	設定	設定
	端末	端末	端末
アプリ	データ	データ	データ
	アプリケーション	アプリケーション	アプリケーション
環境	ランタイム	ランタイム	ランタイム
	ミドルウェア	ミドルウェア	ミドルウェア
	コンテナ管理機能	コンテナ管理機能	コンテナ管理機能
OS	オペレーティングシステム	オペレーティングシステム	オペレーティングシステム
仮想化	仮想化ソフトウェア	仮想化ソフトウェア	仮想化ソフトウェア
	ハードウェア	ハードウェア	ハードウェア

【出展元】
国家サイバー統括室
クラウドを利用したシステム運用に関するガイダンス
https://www.nisc.go.jp/policy/group/infra/cloud_guidance.html

利用組織が管理　クラウド事業者が管理

クラウドサービスとは？

PaaS（Platform as a Service）

- OS、ミドルウェア、開発環境までをプラットフォームとしてクラウド事業者が管理
- アプリケーション、データのセキュリティは利用者の責任

区分	IaaS	PaaS	SaaS
設定	ポリシー	ポリシー	ポリシー
	設定	設定	設定
	端末	端末	端末
アプリ	データ	データ	データ
	アプリケーション	アプリケーション	アプリケーション
環境	ランタイム	ランタイム	ランタイム
	ミドルウェア	ミドルウェア	ミドルウェア
	コンテナ管理機能	コンテナ管理機能	コンテナ管理機能
OS	オペレーティングシステム	オペレーティングシステム	オペレーティングシステム
仮想化	仮想化ソフトウェア	仮想化ソフトウェア	仮想化ソフトウェア
	ハードウェア	ハードウェア	ハードウェア

【出展元】
国家サイバー統括室
クラウドを利用したシステム運用に関するガイダンス
https://www.nisc.go.jp/policy/group/infra/cloud_guidance.html

利用組織が管理　クラウド事業者が管理

クラウドサービスとは？

SaaS（Software as a Service）

- 基盤（サーバー、ストレージ、ネットワーク）や、OS、ミドルウェア、アプリケーションの管理もクラウド事業者
- データのセキュリティは利用者の責任

区分	IaaS	PaaS	SaaS
設定	ポリシー	ポリシー	ポリシー
	設定	設定	設定
	端末	端末	端末
アプリ	データ	データ	データ
	アプリケーション	アプリケーション	アプリケーション
環境	ランタイム	ランタイム	ランタイム
	ミドルウェア	ミドルウェア	ミドルウェア
	コンテナ管理機能	コンテナ管理機能	コンテナ管理機能
OS	オペレーティングシステム	オペレーティングシステム	オペレーティングシステム
仮想化	仮想化ソフトウェア	仮想化ソフトウェア	仮想化ソフトウェア
	ハードウェア	ハードウェア	ハードウェア

利用組織が管理　クラウド事業者が管理

【出展元】
国家サイバー統括室
クラウドを利用したシステム運用に関するガイダンス
https://www.nisc.go.jp/policy/group/infra/cloud_guidance.html

クラウドサービスとは？

医療分野での活用例

- 電子カルテシステム（SaaS）
  クラウド型の電子カルテは、災害時のBCP（事業継続計画）対策にも有効
- バックアップ（IaaS）
  電子カルテデータや医療画像をクラウドに保管
- 遠隔医療・地域医療連携（SaaS・IaaS）
  クラウドを通じて場所を問わずデータを共有し、遠隔診療や連携を行う
- 研究・データ分析（SaaS・IaaS）
  医療データをクラウドに集約し、AIによる診断支援や研究に活用

医療機関におけるクラウド導入の考慮点

- 財務の視点から見るIT投資
- 運用負荷
- 可用性と災害対策

医療機関におけるクラウド導入の考慮点

財務の視点から見るIT投資

① クラウド導入の利点
- 固定資産を増やさず、自己資本比率やROAへの影響を抑えられる
- 初期投資を抑え、定額支出によるキャッシュフローの安定と予算管理が容易

② クラウド導入の課題
- IaaS上で稼働する業務システムを外注する場合、結果的にコスト抑制が困難になる可能性がある

③ クラウド導入の考慮点
- 費用対効果を明確にし、間接費・運用コストも含めて評価する（外注による運用コストを考慮しているか？）

医療機関におけるクラウド導入の考慮点

運用負荷

① クラウド導入の利点
- ・SaaSモデルの利用で多くの作業をクラウド事業者に任せることができ、院内の限られたIT人材を戦略的な業務に集中できる

② クラウド導入の課題
- ・クラウド事業者が担うべき安全管理措置に不備があった場合、医療機関は監督責任を問われる

③ クラウド導入の考慮点
- ・契約でクラウド事業者・外注先の責任範囲を明確にする
- ・セキュリティ対策が適切に講じられているか確認する
- ・継続的な監督と監査体制を構築する

医療機関におけるクラウド導入の考慮点

可用性と災害対策

① クラウド導入の利点
- ・分散配置されたクラウド基盤により、災害時でもサービスを継続できる
- ・バックアップと復旧機能により、情報の損失を防げる

② クラウド導入の課題
- ・災害時の通信インフラ障害により、クラウドへのアクセスが困難になる可能性がある
- ・外注先の対応力や復旧体制が不十分な場合、業務に支障をきたす恐れがある

③ クラウド導入の考慮点
- ・災害が発生した場合、地理的影響を受けず利用継続が担保されるか確認する
- ・外注先との契約において、災害対策・復旧時間の保証（SLA）の明確化が必要

医療情報システムの安全管理に関するガイドラインにおけるクラウドの位置づけ

- クラウド利用が許容される条件
- 責任の所在
- クラウド事業者との契約の重要性

医療情報システムの安全管理に関するガイドラインにおけるクラウドの位置づけ

クラウド利用が許容される条件

- 情報の保管場所は、国内に限定されているわけではない
- 海外のクラウドサービスを利用する場合、日本の法令やガイドラインの適用を契約で明示する必要がある

医療機関（日本）

- 国内／海外のクラウドサービス
- 医療情報を保存
- 契約で法令遵守明記

契約

クラウド事業者（国内／海外）

- 日本の法令・ガイドライン準拠
- セキュリティ対策
- BCP・監査対応

医療情報システムの安全管理に関するガイドラインにおけるクラウドの位置づけ

責任の所在

- クラウドサービスを利用する場合でも、個人情報保護法やガイドラインに基づく責任は医療機関側にある
- 情報漏洩などが発生した場合、医療機関が説明責任を負う

医療情報システムの安全管理に関するガイドラインにおけるクラウドの位置づけ

クラウド事業者との契約の重要性

◆責任分界の明示
- データ保管・暗号化・障害対応はクラウド事業者、アクセス権管理は医療機関

◆個人情報の取り扱いに関する取り決め
- 保存する情報の種類、暗号化方式、第三者提供の条件など

◆監査・報告義務
- クラウド事業者による定期的なセキュリティ監査と医療機関への報告

◆インシデント対応
- 情報漏洩時の通知、対応手順、協力体制

◆契約終了時のデータ処理
- データの削除・返却方法、バックアップの取り扱い

IaaS利用における
リスク管理と実践

IaaSの特性と管理者責任

OS（オペレーティングシステム）の管理

◆パッチ管理
- OSの脆弱性を修正するためのセキュリティパッチを適用し、常に最新の状態を保つ

◆設定管理
- 不必要なサービスやポートを無効化するなど、セキュリティを考慮した設定

アプリケーションの管理

◆脆弱性管理
- 稼働するアプリケーションに脆弱性がないかを確認し、必要に応じて修正やアップデート

◆設定管理
- アプリケーションの認証、認可、ログ設定など

IaaSの特性と管理者責任

データの管理

◆機密性
- データが不正にアクセスされないよう、アクセス制御、暗号化などの対策

◆完全性
- データが改ざんされないよう、適切なアクセス権限設定やログ監視

◆可用性
- データ損失に備え、定期的なバックアップや災害復旧（DR）計画の策定・実行

IaaSの特性と管理者責任

ネットワーク設定とアクセス管理

◆ファイアウォール
- 外部からの不正アクセスを防ぐため、仮想ネットワーク上のファイアウォール設定

◆アクセス制御
- 誰がどのサーバーにアクセスできるかを厳密に管理し、多要素認証（MFA）を導入するなど、認証情報を強化

◆ログ監視
- サーバーやネットワークのログを継続的に監視し、不審な挙動がないか確認

セキュリティ上の課題と対策

不正アクセス対策	
課題	IaaS環境では、構築したサーバーやネットワーク機器が外部攻撃の標的となりやすく、アクセス制御やパスワードの管理不備があると、重大な情報漏洩やシステム破壊に直結する
対策	• 多要素認証（MFA）の適用 • 最小特権の原則 • VPN（仮想プライベートネットワーク）の利用 • セキュリティグループ/ファイアウォール設定

脆弱性管理	
課題	IaaS環境では、OSやミドルウェアの脆弱性が常に発見されるため、パッチ適用などの対応を怠ると、システム乗っ取りのリスクが大幅に高まる
対策	• 定期的なパッチ適用 • 定期的な脆弱性スキャン • リスク評価と対応

セキュリティ上の課題と対策

ログ管理と監視	
課題	システムに異常が発生した際、ログ管理が不十分だと、原因究明や被害特定に必要な情報が不足し、迅速なインシデント対応が困難になる
対策	• ログの一元管理 • リアルタイム監視

データ保護と可用性	
課題	サイバー攻撃などにより、重要なデータが破損・利用不能になるリスクがあるため、患者情報などの機密データは、法的にも厳重な保護が義務付けられている
対策	• 保管データの暗号化 • 通信データの暗号化 • 定期的なバックアップ • 災害復旧計画の策定

SaaS利用における リスク管理と実践

SaaSの特性とクラウド事業者の責任

クラウド事業者の責任範囲(1/2)

◆アプリケーションのセキュリティ
- SaaSアプリケーション自体の脆弱性管理と修正
- ソフトウェアのセキュリティアップデートとパッチ適用
- アプリケーションの不正アクセス対策

◆インフラストラクチャのセキュリティ
- 基盤となるサーバー、ネットワーク、ストレージの管理
- 物理的なデータセンターのセキュリティ
- OSや仮想化レイヤーのセキュリティ管理

SaaSの特性とクラウド事業者の責任

クラウド事業者の責任範囲(2/2)

◆データ可用性の確保
- システムの冗長化とバックアップ体制の構築
- ディザスタリカバリ（災害復旧）計画の策定と実施

◆コンプライアンスと認証
- ISMAP（政府情報システムのためのセキュリティ評価制度）への対応
- ISO/IEC 27017（クラウドサービスのための情報セキュリティ管理策）などの取得と維持

SaaSの特性とクラウド事業者の責任

ユーザーの責任範囲

◆アカウント管理とアクセス制御
- ユーザーIDの管理、パスワードポリシーの設定、多要素認証の導入など

◆データ利用の管理
- どのデータがクラウドに保存され、誰がアクセスできるかを管理

◆設定ミス
- アプリケーション内の共有設定や公開設定の誤りによる情報漏洩

セキュリティ上の課題と対策

アカウント管理の不備	
課題	退職者のアカウント放置、推測されやすいパスワードや使い回しといった不適切なアカウント・パスワード管理は、不正アクセスのリスクを増大させる
対策	• 多要素認証（MFA）の義務化 • シングルサインオン (SSO) の導入 • パスワードポリシーの徹底

設定ミスによる情報漏洩	
課題	共有設定のミスにより、ファイルやデータが意図せず公開されたり、過剰なアクセス権限が付与されたりすることで、情報漏洩やデータ改ざんのリスクにつながる
対策	• アクセス権限の最小化 • 共有設定の確認と制限 • 定期的な設定レビュー

セキュリティ上の課題と対策

データプライバシーとコンプライアンス	
課題	クラウド事業者の海外拠点利用は、日本の法規制（ガイドラインなど）への準拠が不明確になるリスクを伴い、通信やデータの暗号化がされていない場合は情報漏洩のリスクを高める
対策	• データの保存場所の確認 • ガイドライン対応の確認 • 暗号化機能の確認

クラウド事業者との連携不足	
課題	サービスの停止やサイバー攻撃が発生した際、クラウド事業者からの情報共有や対応手順が不明確であると、迅速なインシデント対処ができなくなる
対策	• 契約・SLAの確認 • セキュリティ情報の共有体制 • セキュリティ認証の要求・評価

クラウド導入検討・評価時に確認すべきセキュリティのポイント

クラウド事業者選定時のチェックリスト

- 契約内容
- セキュリティ認証
- 災害対策・事業継続計画（BCP）
- インシデント対応体制
- 技術的セキュリティ対策

クラウド事業者選定時のチェックリスト

契約内容

◆SLA（サービスレベル合意書）
- サービスの可用性（稼働率）、応答時間、インシデント発生時の対応時間など、サービス品質に関する項目が明確に記載されているか

◆データ保護とプライバシー
- データの保存場所（国内か海外か）、データの暗号化、個人情報の取り扱いに関する規約が、日本の個人情報保護法や医療情報に関するガイドラインに準拠しているか

◆データ所有権と返還・消去
- サービス利用終了後、データが確実に返却されるか、または完全に消去されるか
  また、その手続きが明確になっているか

◆監査権
- 利用者がクラウド事業者のセキュリティ対策を監査する権利があるか、又は第三者機関の監査レポートを提供できるか

◆責任範囲の明確化
- クラウド事業者と利用者（医療機関）の責任範囲（責任共有モデル）が明確に定義されているか

クラウド事業者選定時のチェックリスト

セキュリティ認証

◆ISMAP（政府情報システムのためのセキュリティ評価制度）
- クラウドサービスを評価・登録する日本政府の制度に登録されたサービスか

◆ISO/IEC 27001（ISMS認証）
- 情報セキュリティマネジメントシステムに関する国際規格の認証を取得しているか

◆ISO/IEC 27017（クラウドサービスのための情報セキュリティ管理策）
- クラウドサービスに特化した情報セキュリティ管理策の国際規格の認証を取得しているか

◆ISO/IEC 27018（クラウドサービス上での個人情報に関する国際規格）
- クラウド上の個人情報保護に関する国際規格の認証を取得しているか

クラウド事業者選定時のチェックリスト

災害対策と事業継続計画（BCP）

◆冗長性
- 別拠点でのバックアップ構成があるか（例：東西リージョン）
- サーバーやストレージが別ラック・別建屋で冗長化されているか（システム）
- 複数キャリアも含む通信経路の冗長性が確保されているか（ネットワーク）
- 電源が多重化されているか

◆バックアップと復旧
- データのバックアップが定期的に行われているか

◆BCPの公開
- クラウド事業者の事業継続計画（BCP）が策定されており、その概要が公開されているか

クラウド事業者選定時のチェックリスト

インシデント対応体制

◆連絡体制
- セキュリティインシデント発生時の緊急連絡先、対応窓口、連絡フローが明確か

◆対応プロセス
- インシデントの検知、調査、封じ込め、復旧、報告までのプロセスが明確に定められているか

◆証拠保全
- インシデント発生時に、ログなどの電子証拠が適切に保全され、利用者に提供される体制があるか

◆報告義務
- セキュリティインシデントが発生した場合、クラウド事業者から利用者への報告義務が契約に明記されているか

クラウド事業者選定時のチェックリスト

技術的セキュリティ対策

◆暗号化
- データの保存時（保存データの暗号化）と通信時（通信経路の暗号化）の両方で、強固な暗号化が行われているか

◆アクセス制御
- ユーザー認証 (多要素認証など) 、アクセス権限管理、特権ユーザー管理の仕組みが適切に整備されているか

◆脆弱性管理
- クラウド事業者が提供するサービスやプラットフォームの脆弱性スキャン、パッチ管理が定期的に実施されているか
- SBOM（ソフトウェア部品表）を取得して、サポート切れコンポーネントがないか

◆ログと監視
- 誰が、いつ、何にアクセスしたかのログが適切に記録・保存され、異常なアクティビティを監視する仕組みがあるか

◆その他
- SDS（サービス事業者による医療情報セキュリティ開示書）の提出が可能か

導入後の運用管理のポイント

セキュリティ設定の定期的な見直し

- 権限設定の見直し
  退職者や異動者のアカウントが適切に削除・変更されているか、不必要な特権アクセスが付与されていないか、定期的に棚卸しを行う

ログ管理と監視体制の強化

- ログの統合管理
  クラウドサービスから出力されるアクセスログや操作ログを、統合管理する
- 異常検知とアラート設定
  普段とは異なる不審なアクセス（例：夜間や海外からのログイン、大量データのダウンロードなど）を検知した場合に、管理者へ自動的にアラートが通知されるよう設定する

導入後の運用管理のポイント

従業員へのセキュリティ教育と周知徹底

- 定期的なセキュリティ研修
  クラウドサービスの安全な利用方法、情報漏洩の事例、パスワード管理の重要性などをテーマに、従業員向けの定期的な研修を実施する
- 注意喚起と報告体制の確立
  フィッシング詐欺や不審なメールに関する注意喚起を継続的に行い、少しでも不審な点に気づいた場合は、速やかに担当部門へ報告する体制を徹底する

導入後の運用管理のポイント

クラウド事業者との連携と情報収集

- 脆弱性情報の確認
  クラウド事業者のセキュリティ情報サイトやメーリングリストを定期的に確認し、新たな脆弱性やそれに伴う対策情報をいち早く把握する
- アップデート情報の追跡
  新しい機能やセキュリティ強化策が提供された場合、それが自院の運用にどのように影響するか評価し、必要に応じて設定を更新する
- サポート体制の確認
  インシデント発生時の連絡先や対応フローを事前に確認し、有事の際に迅速な連携が取れるように準備する

導入後の運用管理のポイント

【参考】チェックリストの活用

- 医療法に基づく立入検査時に使用される
  チェックリストを活用

令和７年度
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

事業者確認用

＊以下項目は令和7年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
＊「いいえ」の場合、令和7年度中の対応目標日を記入してください。

	チェック項目	(日付) 確認日	(日付) 目標日	備考
1 体制構築	事業者内に、医療情報システム等の提供に係る管理責任者を設置している。(1-①)	はい・いいえ (/)	(/)	
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**			
	リモートメンテナンス（保守）している機器の有無を確認した。(2-②)	はい・いいえ (/)	(/)	
	医療機関に製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出した。(2-③)	はい・いいえ (/)	(/)	
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。※管理者権限対象者の明確化を行っている(2-④)	はい・いいえ (/)	(/)	
	退職者や使用していないアカウント等、不要なアカウントを削除または無効化している。(2-⑤)	はい・いいえ (/)	(/)	
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-⑥)	はい・いいえ (/)	(/)	
	パスワードは英数字、記号が混在した8文字以上とし、定期的に変更している。※二要素認証、または13文字以上の場合は定期的な変更は不要(2-⑦)	はい・いいえ (/)	(/)	
	パスワードの使い回しを禁止している。(2-⑧)	はい・いいえ (/)	(/)	
	USBストレージ等の外部接続機器や情報機器に対して接続を制限している。(2-⑨)	はい・いいえ (/)	(/)	
	二要素認証を実装している、または令和９年度までに実装予定である。(2-⑩)	はい・いいえ (/)	(/)	
	サーバについて、以下を実施している。			
	アクセスログを管理している。(2-⑪)	はい・いいえ (/)	(/)	
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-⑫)	はい・いいえ (/)	(/)	
	端末PCについて、以下を実施している。			
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-⑫)	はい・いいえ (/)	(/)	
	ネットワーク機器について、以下を実施している。			
	接続元制限を実施している。(2-⑬)	はい・いいえ (/)	(/)	

まとめ(1/3)

クラウド利用における「責任共有モデル」を理解する

◆オンプレミス環境と異なり、クラウドでは「責任共有モデル」が非常に重要
◆IaaS（例：AWS, Azure, GCP）
- 基盤（サーバー、ストレージ、ネットワーク）の管理はクラウド事業者の責任
- その上に乗るOS、アプリケーション、データのセキュリティはすべて利用者の責任
- パッチ適用やログ監視など、従来のオンプレミス環境での管理作業の多くは、引き続き管理者自身の役割

◆SaaS（例：電子カルテクラウド、Microsoft 365）
- アプリケーションやOSの管理はクラウド事業者側
- アカウント管理やアクセス権限の設定、そして不適切な設定による情報漏洩の防止は、利用側の重要な責任

区分	IaaS	PaaS	SaaS
設定	ポリシー	ポリシー	ポリシー
	設定	設定	設定
	端末	端末	端末
アプリ	データ	データ	データ
	アプリケーション	アプリケーション	アプリケーション
環境	ランタイム	ランタイム	ランタイム
	ミドルウェア	ミドルウェア	ミドルウェア
	コンテナ管理機能	コンテナ管理機能	コンテナ管理機能
OS	オペレーティングシステム	オペレーティングシステム	オペレーティングシステム
仮想化	仮想化ソフトウェア	仮想化ソフトウェア	仮想化ソフトウェア
	ハードウェア	ハードウェア	ハードウェア

まとめ(2/3)

契約・運用前に確認すべき3つの重要ポイント

◆クラウドサービスを導入する際は、クラウド事業者のセキュリティ対策を鵜呑みにせず、以下の3点を必ず確認しましょう

①契約内容の確認

✓SLA（サービスレベル合意書）やデータ所有権、インシデント発生時の連絡・協力体制が明確に定義されているか確認します

②セキュリティ認証の確認

✓クラウド事業者が適切なセキュリティ管理を行っているかの客観的な指標として、ISMAPへの登録や、ISO/IEC 27017といった第三者認証を取得しているか最新レポートの提出を求めましょう

③医療情報に関する対応状況

✓医療情報ガイドラインに準拠しているか、医療情報の取り扱いについて具体的な対応実績があるかなどを確認し、医療機関に特有の要件を満たしているかを把握します

まとめ(3/3)

導入後も継続的な対策が不可欠

◆クラウド導入は、セキュリティ対策の終わりではなく運用が始まってからが本番

◆定期的な設定の見直し

- サービスの設定が初期値のままになっていないか、過剰な権限が付与されていないかを定期的に見直す

◆アクセス権限の棚卸し

- 異動や退職者が出た際に、不必要なアクセス権が残っていないか定期的に確認し、最小権限の原則を徹底する

◆従業員への教育

- 従業員に対し、クラウドサービスの安全な使い方やパスワード管理の重要性について継続的に教育を行い、人為的なミスを防ぐ