資料２－３

第2回　医療等情報の二次利活用に関する技術作業班

二次利用環境における情報セキュリティ

独立行政法人情報処理推進機構
デジタル改革推進部　田辺里美

お話しする内容＝安全管理措置に関する要件

医療機関での情報システム利用の環境の変化

これまで＞＞
- 病院の中だけで完結（院内ネットワークのみ）
- 外部との接続が必要な場合は、専用の回線を利用
- サプライヤー（薬、配膳、その他備品等）とはFAX/電話でのやりとり

現在＞＞
- 様々な情報システムの利用が進み外部との連携も加速
- 従前の「外部接続なし」文化から「外部接続あり」環境を守る文化への切替えが追い付かない（体制面、費用面、マインドセット）

徳島県つるぎ町立半田病院
大阪府立病院機構 大阪急性期・総合医療センター

⇒外部との接続装置の脆弱性を利用し侵入

情報システム利用環境変化と攻撃者や手法の変化

知識追及
興味

＜スタンドアロン＞

- フロッピーディスク経由
- コンピュータの性能低下や破壊等の被害

自己顕示欲
腕自慢

＜インターネット利用＞

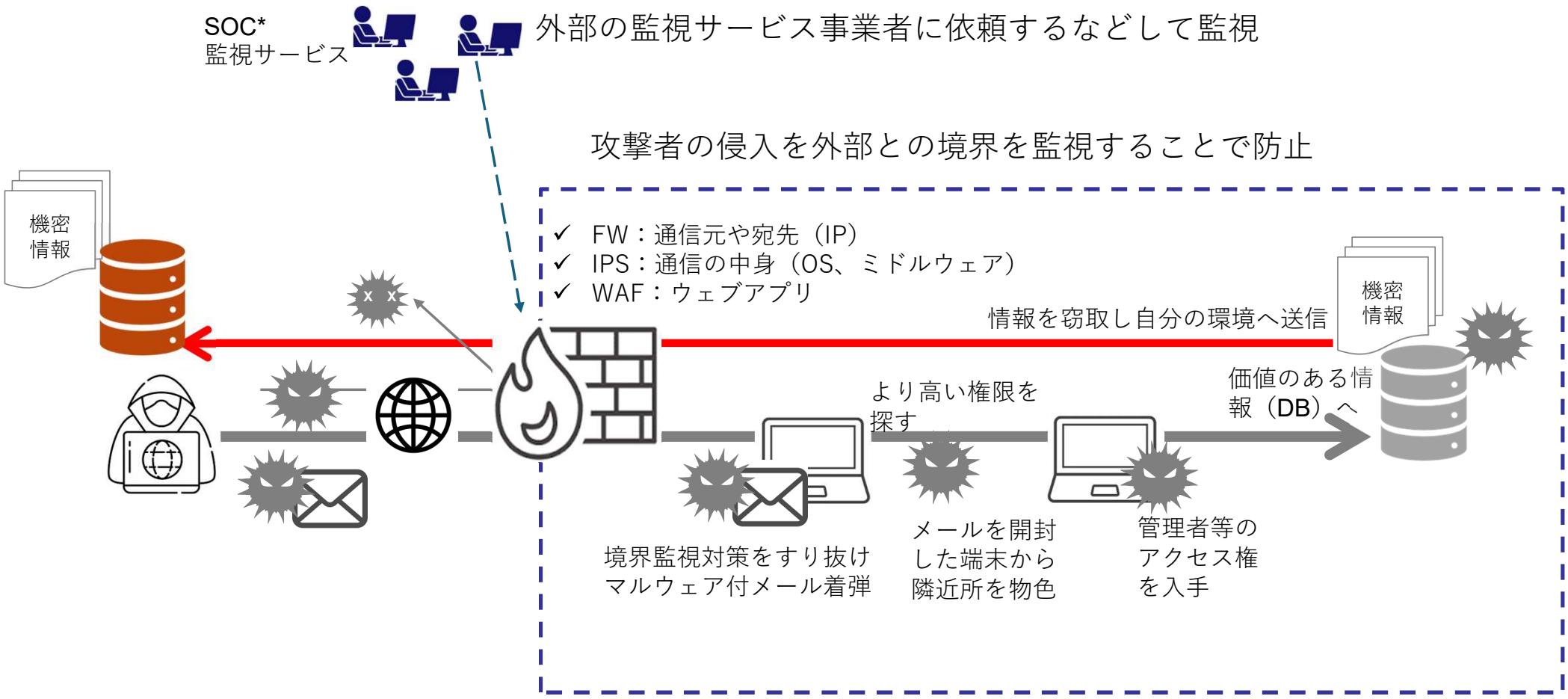
- 電子メールやホームページ経由
- コンピュータの性能低下・稼働停止による業務停止

収益化
組織化

＜クラウド利用（環境や接続先の多様化）＞

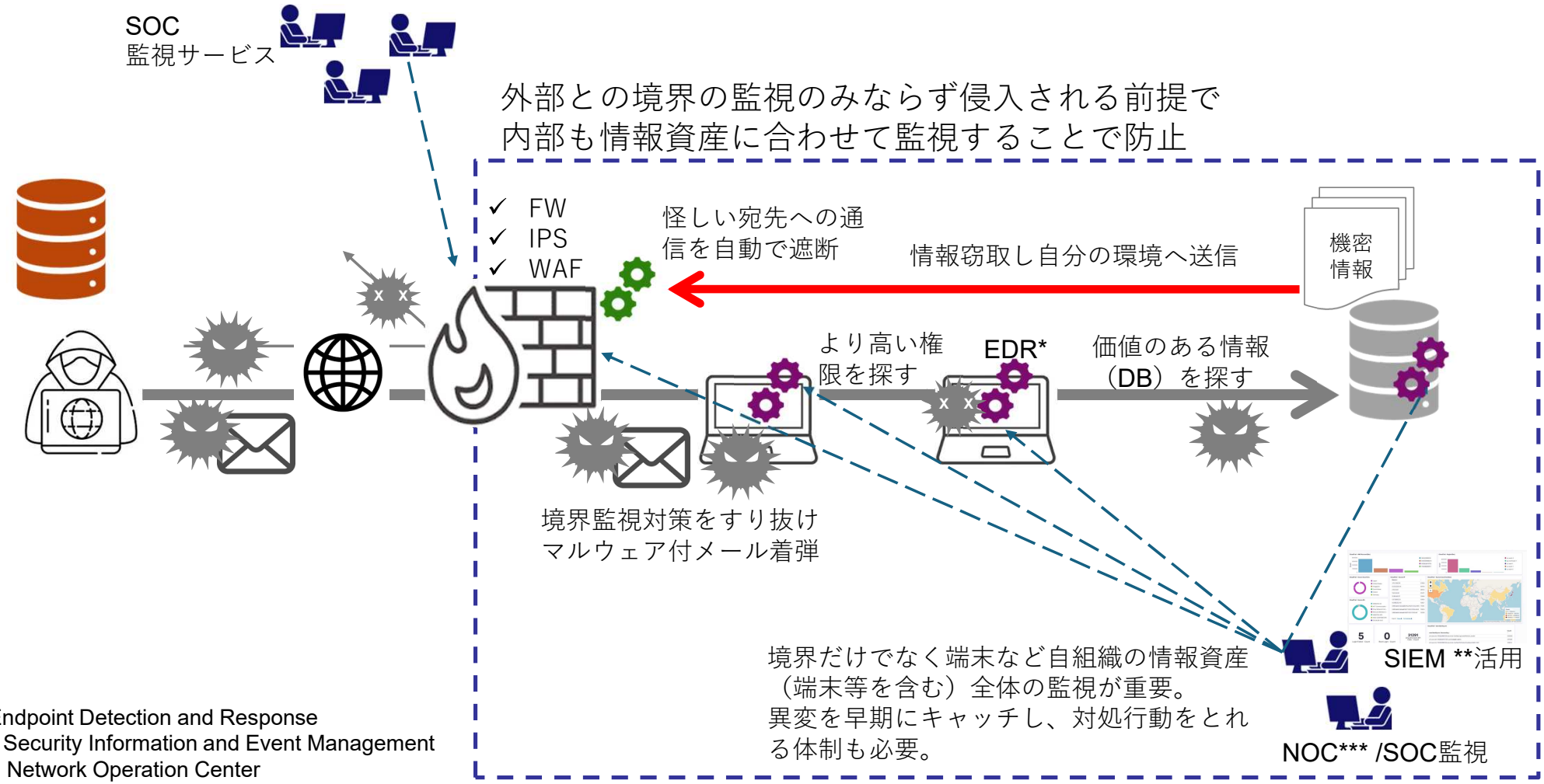
- 様々な機器・ソフトウェア等の脆弱性、電子メールなど、多様な経路
- 情報の窃取（販売目的）、業務の停止
  ⇒ゼロトラストセキュリティ

監視対象の変化（これまで：境界線の監視）



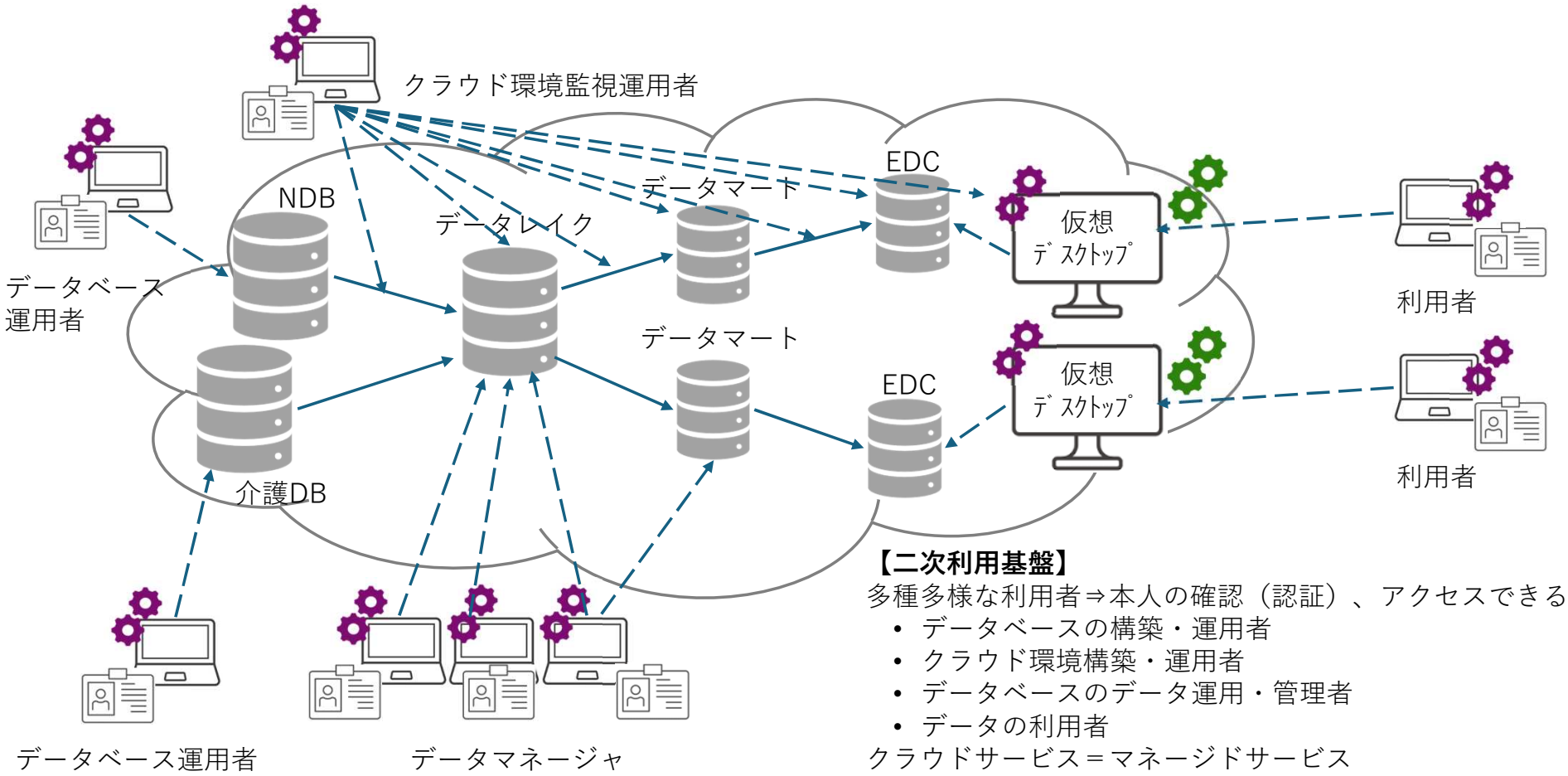
*SOC: Security Operation Center

監視対象の変化（現在：利用者端末など情報資産ごとの監視も重要）



*EDR: Endpoint Detection and Response
**SIEM: Security Information and Event Management
***NOC: Network Operation Center

「ゼロトラスト」の必要性　クラウド利用とセキュリティ



【二次利用基盤】

多種多様な利用者⇒本人の確認（認証）、アクセスできる範囲の確認（認可）

- データベースの構築・運用者
- クラウド環境構築・運用者
- データベースのデータ運用・管理者
- データの利用者

クラウドサービス＝マネージドサービス

- OSやアプリケーションなどのアップデート等は提供者が実施
- 環境の変化（アップデート）等を監視し設定不備を修正（ベスプラの活用）
- クラウド内部で発生する通信も監視し不審な挙動がないか監視が必要

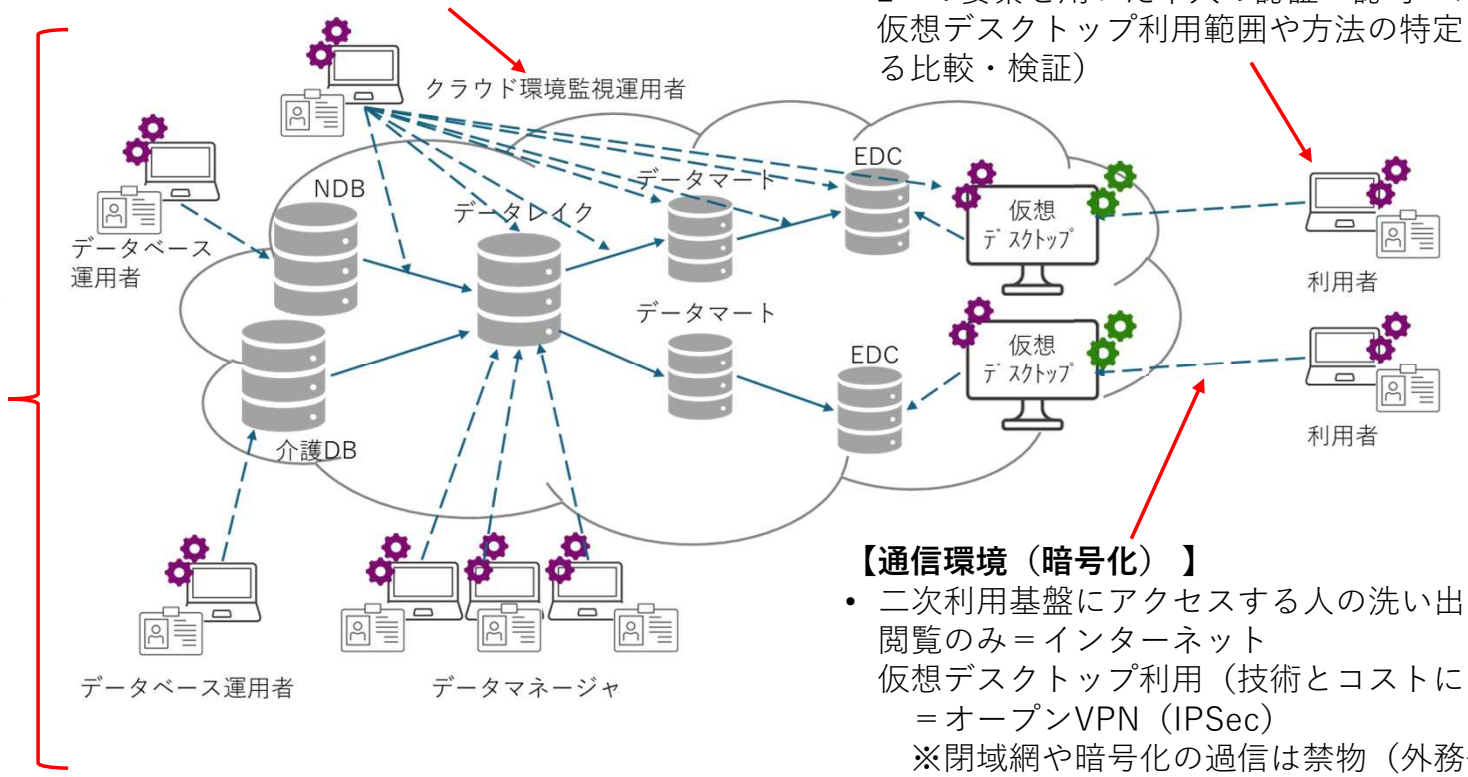
二次利用基盤セキュリティ管理の概観

【ログの活用】
- ログの活用による予防と早期発見
- 極力自動化、人手の削減
- 分析ログの取捨選択と相関分析の実施（リアルタイム）
- 証跡として保管するものの管理（アーカイブ）

【認証方法（二要素認証 ）】
- 二次利用基盤にアクセスする人の洗い出しと個別の設定
  情報閲覧のみ、仮想デスクトップ利用（利用方法の分類）等
- 2つの要素を用いた本人の認証＋認可コントロールも必要
  仮想デスクトップ利用範囲や方法の特定（技術とコストによる比較・検証）

【安全管理措置】
- 技術的
  ゼロトラスト
- 物理的
  利用場所の制限（公共の場所はNGなど）
  責任範囲の明確化（利用環境、提供環境）
- 人的
  利用前研修
  誓約書の提出
  アクセス権限別の管理
  ルール周知徹底

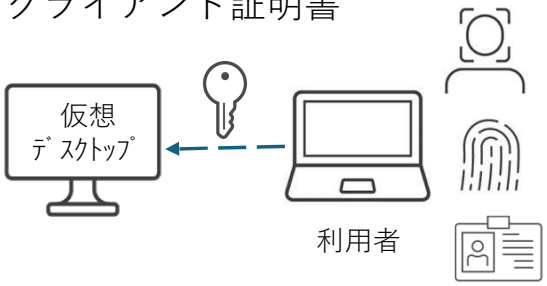
【緊急対応】
- アラート発報ルール設定
- 緊急度に合わせた対応ルール設定
- 体制整備



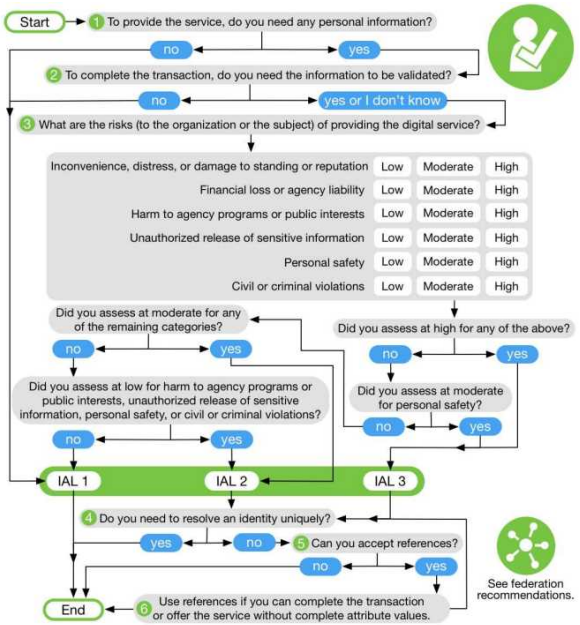
【通信環境（暗号化） 】
- 二次利用基盤にアクセスする人の洗い出しと個別の設定
  閲覧のみ＝インターネット
  仮想デスクトップ利用（技術とコストによる比較・検証）
  ＝オープンVPN（IPSec）
  ※閉域網や暗号化の過信は禁物（外務省事案）

認証方式

【二要素認証　ふたつの認証方法の組合せ】
自分が知っているもの: パスワード、暗証番号、セキュリティ質問など
自分が持っているもの:物理的なトークン、またはデジタルトークン（XXAuthenticator）、クライアント証明書
自分自身: “顔” や“指紋”、 “静脈”のような生体認証



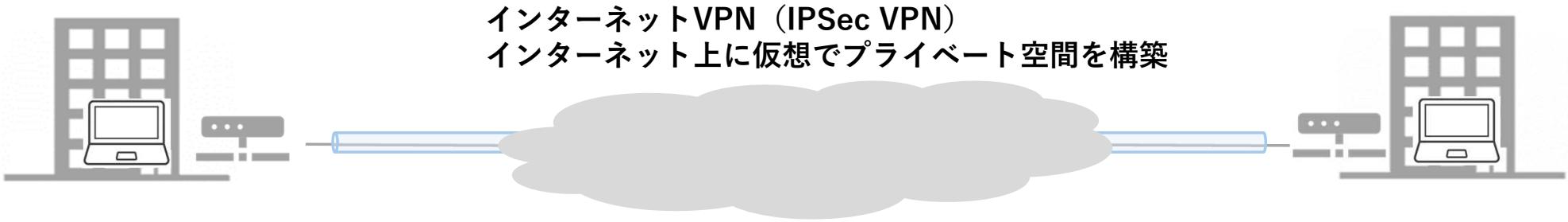
NISTSP800-63-3　電子認証に関するガイドライン　（米国国立標準技術研究所）

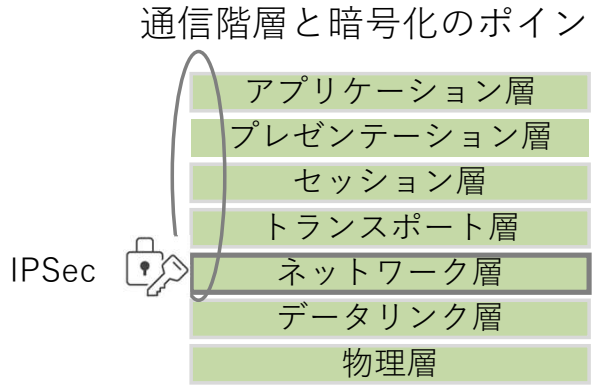


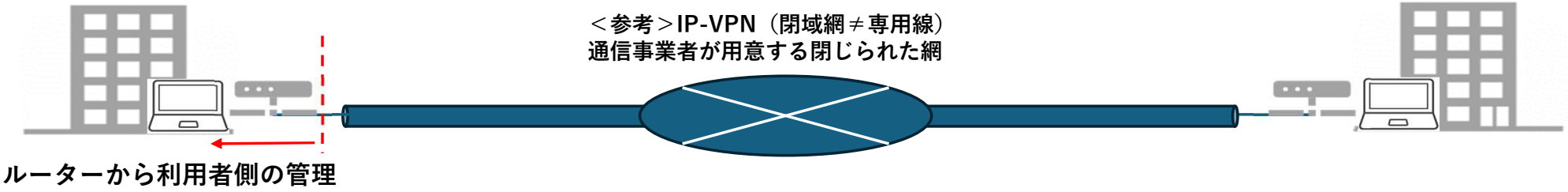
本人確認 (IAL)	Lv１：自己申告による登録でよい Lv２：リモートまたは対面による確認 Lv３：対面での有資格者による確認
認証プロセス (AAL)	Lv１：単要素 Lv２：二要素必要、二 要素目の認証手段はソフトウェアベースで可 Lv３：二要素必要、かつ二要素目はハードウェアを用いること
認証連携（ﾃﾞｰﾀ流通の仕組み） (FAL)	Lv１：アサーションへの署名 Lv２：アサーションへの署名に加えて対象のサービス提供者だけが複合できる暗号化 Lv３：上記二つに加えてさらに複雑なアサーションの利用

https://www.jipdec.or.jp/library/report/u71kba000000d8ae-att/20171127.pdf

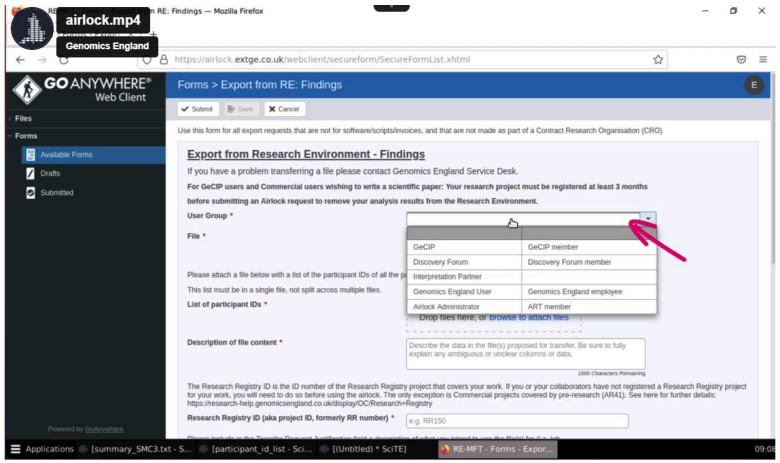
通信暗号化

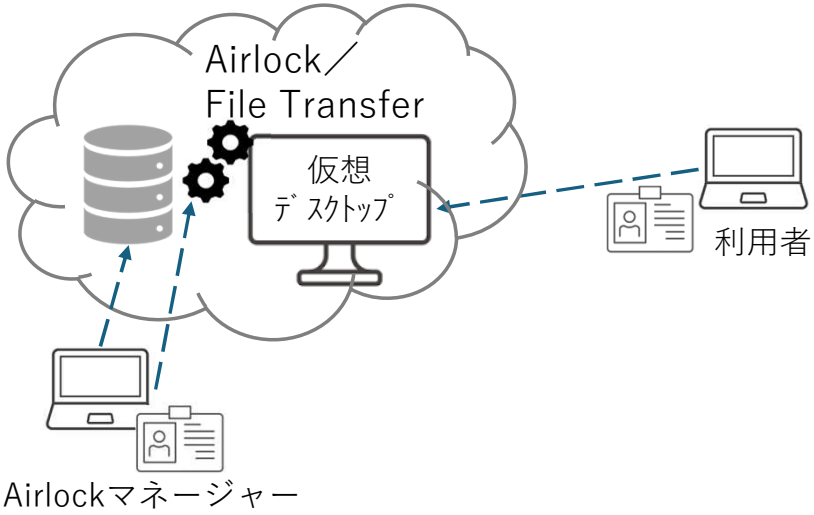

インターネットVPN（IPSec VPN）
インターネット上に仮想でプライベート空間を構築


通信階層と暗号化のポイント
アプリケーション層
プレゼンテーション層
セッション層
トランスポート層
IPSec
ネットワーク層
データリンク層
物理層


＜参考＞IP-VPN（閉域網≠専用線）
通信事業者が用意する閉じられた網
ルーターから利用者側の管理

Visiting環境データ保護のルール例　英国Genomics England（GEL）TRE 環境



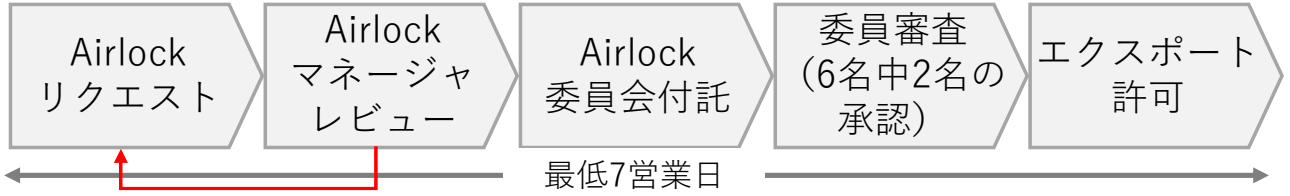


＜“ Airlock” を使用したファイルのインポートとエクスポート＞
＝解析環境は、貸出図書館ではなく、閲覧図書館であるべき＝
研究環境からエクスポートできるデータを制限するとともに、事前の承認を必須とする。
アプリケーションの画面から、必要事項を入力し申請する。

＜申請時の入力内容＞
- 研究チームまたは産業フォーラム等所属チームの番号
- 研究者登録ID
- プロジェクト番号
- エクスポートを希望するファイル（解析環境外で操作するデータや、持出し後公開する予定のもの全て）
- ファイルをエクスポートする理由とその意図（詳細に）

＜インポートする際のルール（抜粋）＞
- ウィルスチェック後のファイルであること（GEL側でもチェック）
- GEL内部でチェックし拒否の場合は理由と共に返送

意図的なセキュリティ侵害は、研究者及び所属する組織全体を利用停止に。
また個人を同定する行為は法律違反であり刑事告訴または高額の罰金刑。



https://re-docs.genomicsengland.co.uk/airlock_tool/

安全管理措置

- 利用者環境
  技術的安全管理措置
  - ✓ データダウンロード、アップロードの申請制
  - ✓ ウィルス対策ソフトの導入とスキャンの実施
  - ✓ OSの最新化
  - ✓ 端末ロックの設定
  - ✓ フリーWifiの利用禁止　など

  物理的安全管理措置
  - ✓ 公共の場所（自組織内の外来者が入れるスペース含む）での利用禁止

  人的安全管理措置
  - ✓ 利用開始前のトレーニング受講義務化
  - ✓ 利用規程の周知徹底（罰則の規定を含む）
  - ✓ 申請手続きの標準化（理解促進と厳守（守りやすい環境整備））

- 提供者環境
  ⇒各種ガイドラインに準じた対策
  医療情報安全管理ガイド、政府機関等の対策基準策定のためのガイドライン
  ⇒対策実行のモニタリング（技術：SOC（専門的な監視）　ルール：標準化と監査）

ログの活用と緊急対応

「置いただけ」「見ているだけ」にならないように

- **システムの全体構成図／情報資産のリスト**
  - どこに何があり、何を監視しているか可視化する。情報資産の増減や配置変更などがあればアップデートする。
- **収集している（できる）ログの種類の把握と発報ルール設定**
  - 個別のログを統合的に管理する。またログ分析結果に基づき対応ができるよう、分析ルールを作成する。（SIEM等の活用）
  - クラウド特有のログの管理方法がある点には十分配慮が必要。（専門知識を有する監視者による監視）
- **発報を受けた後の対応フロー設定**
  - 発報のレベルや内容によって、自動化し対応するものと、人を介して対応するものに分類し運用する。
  - どのレベルの発報があった場合エスカレーションするか、またエスカレーション先も明確にする。
- **緊急対応マニュアル・フローの作成**
  - CSIRT*立上げ基準の設定
  - CSIRT立上げ後の対応手順やフローを設定する。複数の部門等の連携が必要になる点に留意が必要。

*CSIRT: Computer Security Incident Response Team

セキュリティ対策の基本

- 日常的な監視を怠らない。
  - 常に状態を監視し、不審な挙動に早期に気づき、未然防止や被害の局所化が可能なように

- 緊急時の具体的な対策方法を規定する。
  - 問題発生時の緊急対応手順や体制（CSIRT)の整備
  - 緊急対応（意思決定）が可能なログ収集と分析（ログは一定期間保管する）
  - セキュリティの要注意情報の活用と緊急時の遮断

- 対策費用と効果のバランスのとり方
  - 情報資産の場所や機微性に照らして、対策の配置を検討
  - 人の負荷を軽減するための方策（自動化、AI）
  - 利用者の啓発

- ITは守りの「道具」。利用者及び運用者双方の手順や規程・ルールが必要。
  - 利用者及び運用者の責任範囲とその内容の明確化