

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版主な改定ポイント（概要）

外部委託、外部サービスの利用に関する整理

クラウドサービスに医療情報システムの運用管理を、すべてを外部に任せる場合

小規模医療機関等

クラウドサービス

医療情報システム等
提供事業者



クラウドサービスに医療情報システムの一部を運用管理を外部に任せる場合

大規模医療機関等

クラウドサービス

医療情報システム等
提供事業者

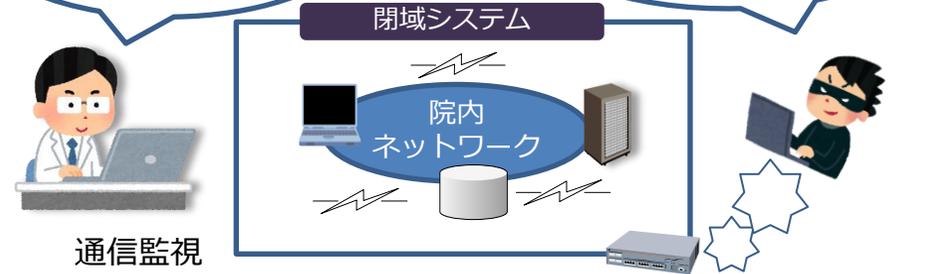


ネットワーク境界防御型思考／ゼロトラストネットワーク型思考

ゼロトラストの思考を取り入れることで、個々の外部からの侵入にも適切な対応が可能となります。

外部との接続制限のほか、院内のシステムにアクセスするすべての通信も監視しよう！

外部から入って攻撃しようと思ったが、うまく攻撃できない！



災害、サイバー攻撃、システム障害等の非常時に対する対応や対策

非常時場面ごとのバックアップの考え方の違い（例）

非常時への対応と言っても、場面ごとに対応内容が違うんだ！

大規模災害に備えてバックアップは分散して保存しよう。

ランサムウェアなどの対策として、書き換え不可で複数のバックアップをしておこう。

障害対策として、すぐに復旧できる対応にてシステムの長期停止を避けよう。

医療機関等の業務継続の考え方も、非常時の場面ごとに考えないと・・・



本人確認を要する場面での運用（eKYCの活用）の検討

医療情報システムの利用者認証に、マイナンバーカード等が使えるかな？

医療機関等で管理されていないものを使っても大丈夫かな？

身元認証がしっかりしている認証方法を使うなら、安全性が高いかな？

