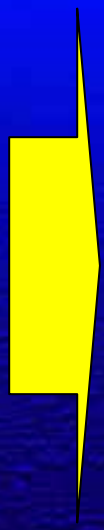
リモートサービスにおけるセキュリティ

(社) 日本画像医療システム工業会
医用画像システム部会
セキュリティ委員会

医療機器におけるリモートサービス

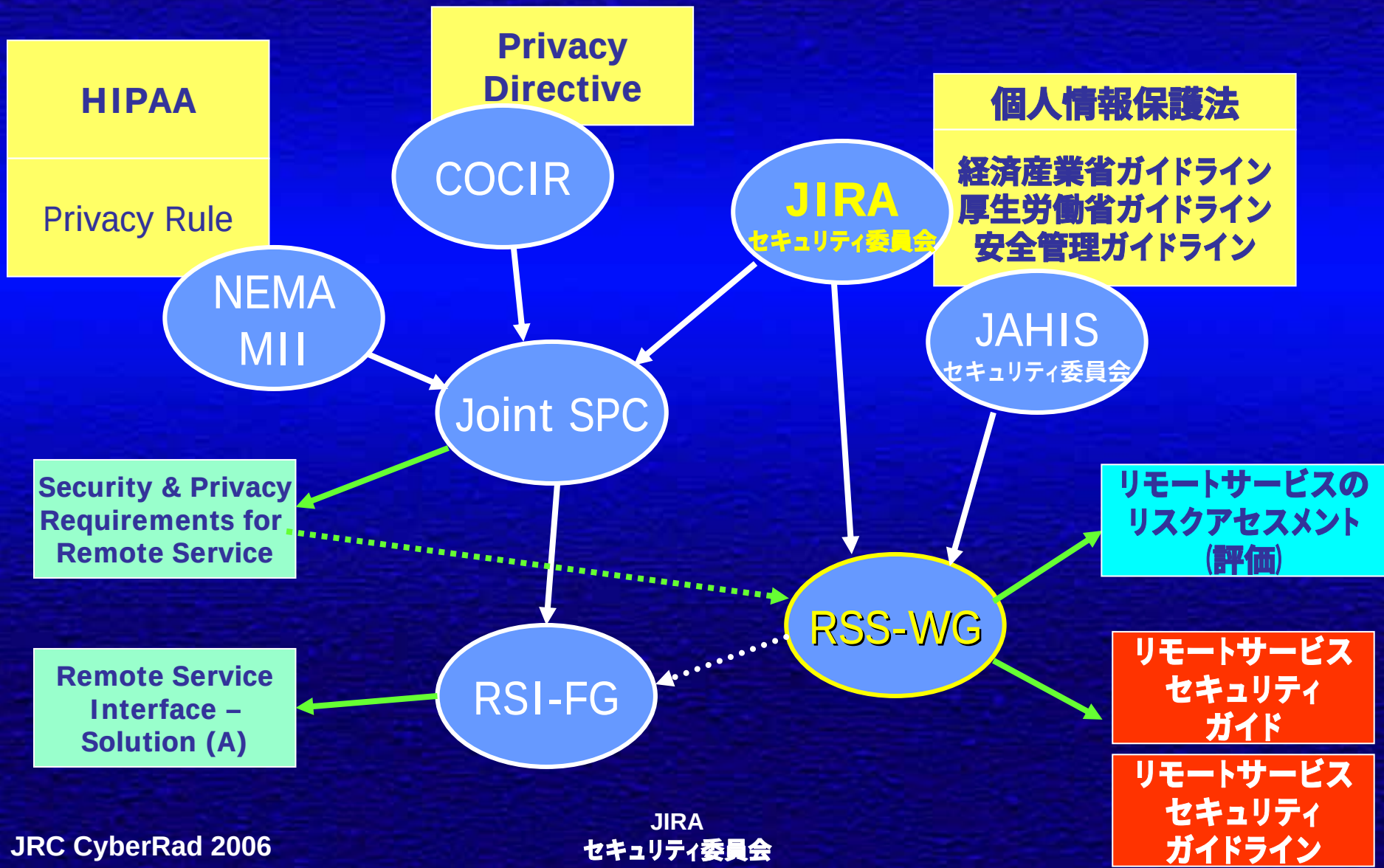
- **医療機関内の医療機器に対し、院外から通信回線を通じてアクセスしサービスを行うこと**
  - **障害対応**
    - 障害状況の情報を収集し解析を行う
  - **予防保守**
    - 機器の状況をモニタし、障害の兆候を事前に連絡する
  - **ソフトウェア改訂**
    - ソフトウェアのバージョンアップ、バグ修正を行う



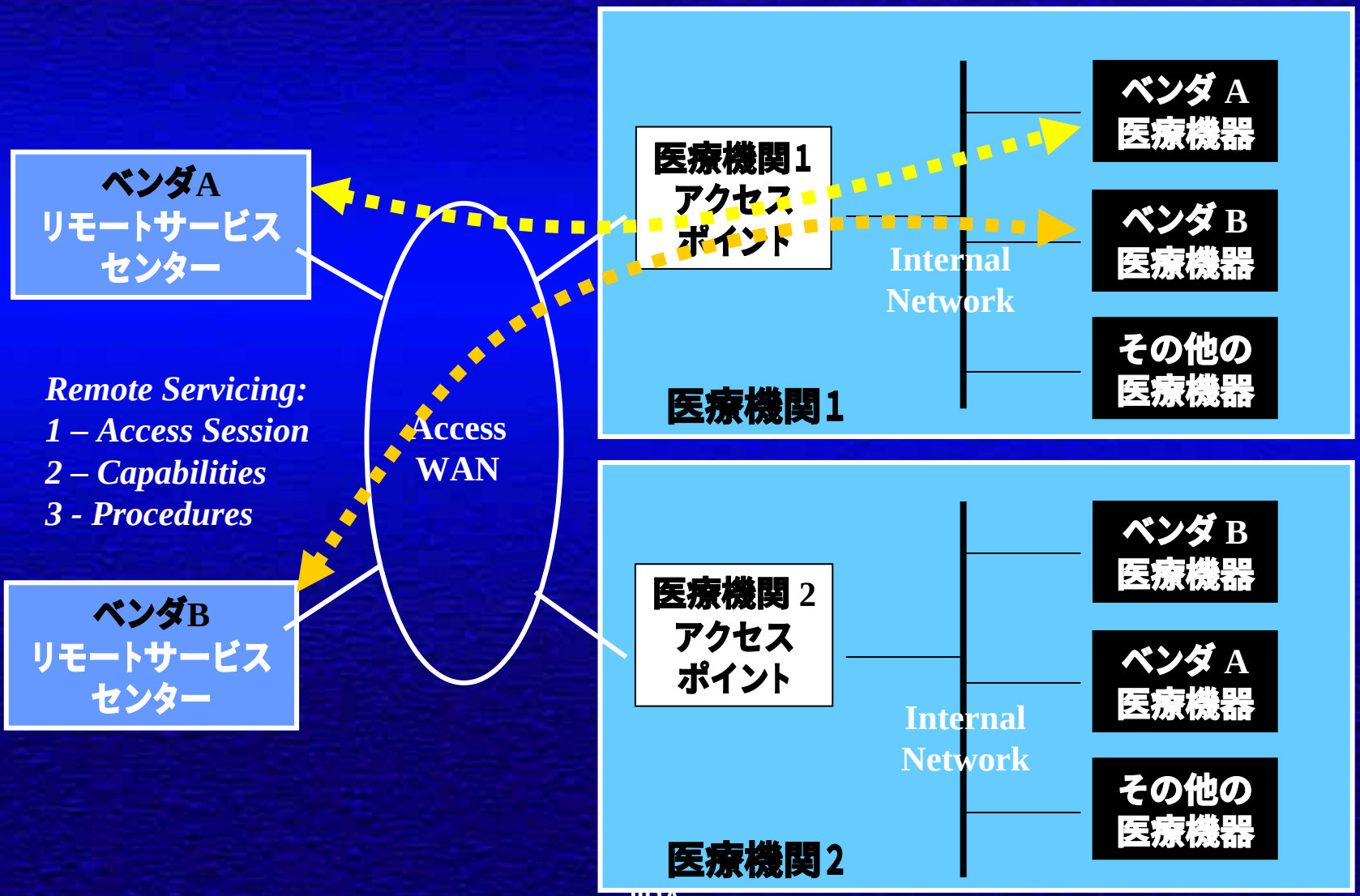
- ダウンタイムの大幅短縮
- 障害を予防することが可能
- 保守費用の大幅低減
- 医療施設側の対応も低減

リモートサービスへの期待

リモートサービスセキュリティの検討



リモートサービスの運用モデル



医療機関のネットワーク とリモートサービスの現状

セキュアなリモートサービスの構築

診療情報に対するセキュリティの確保

リモートサービスセンター、医療施設
共に守るべき情報資産に対して
- 組織的安全管理措置
- 物理的安全管理措置
- 技術的安全管理措置
- 人的安全管理措置

を行うためのルールが必要

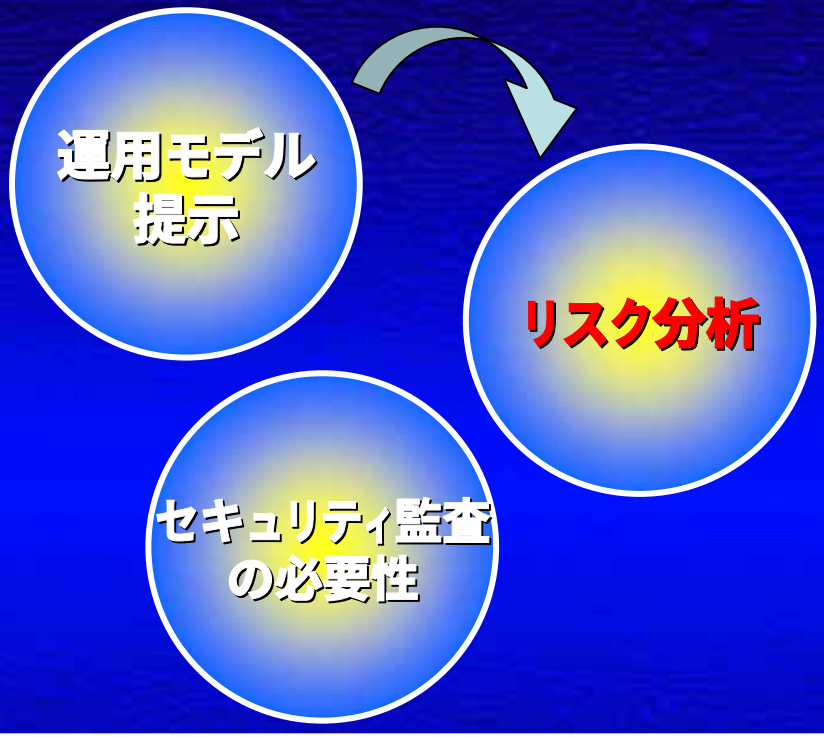
守るべき情報資産は何か？
◎患者情報等の個人情報
◎接続する医療機器やそのサイト

総合的な「リスクアセスメント」が必要

リモートサービスセキュリティガイド
リモートサービスセキュリティガイドライン

- JIRAとJAHIS（保健医療福祉情報システム工業会）の両セキュリティ委員会にて共同でRSS-WGを発足し作成
  - リモートサービスセキュリティガイド（JESRA C-0012-2004）
  - リモートサービスセキュリティガイドライン（JESRA C-0013-2006）
- リモートサービスを行う医療情報システムが対象
- 両工業会のWEBサイトで公開される予定
  - http://www.jira-net.or.jp
  - http://www.jahis.jp

リモートサービスセキュリティガイド



内容

はじめに
第1章　医療分野におけるリモートサービス
第2章　リモートサービスセキュリティの課題
第3章　リモートサービスにおけるリスク分析
第4章　日本におけるリモートサービスのあり方
第5章　セキュリティ対策の策定
第6章　リモートサービスセキュリティの実際の運用
第7章　第三者機関を利用した公的監査の推進
第8章　本ガイドの技術的･制度的変化への対応
付録（リスク分析、セキュリティ監査）

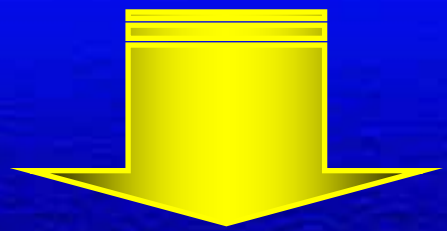
リモートサービスセキュリティガイドライン

内容

はじめに
第1章　リモートサービスガイドラインの必要性
第2章　リモートサービスセキュリティの要件
第3章　リモートサービスへのISMSの適用
第4章　管理目的と管理策の選択
第5章　残存リスクの承認
第6章　セキュリティ監査のガイドライン
第7章　本ガイドの技術的･制度的変化への対応
参照規格および法規
付録（リスクアセスメント表）

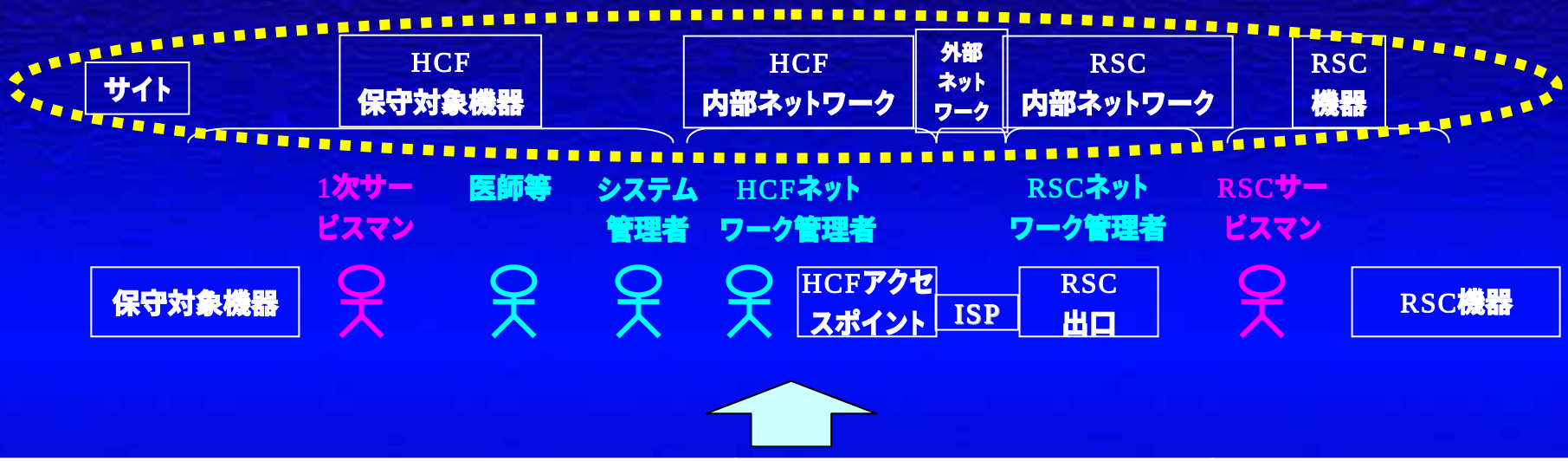
リモートサービスにおける脅威

(A) **機密性**：覗き見／盗用、不正ログイン、持ち出し
(B) **完全性**：改ざん、差換え、消去、ねつ造、否認
(C) **可用性**：故障、火災、サービス不能 etc…



ISMS（情報セキュリティマネジメントシステム：ISO17799/27001）に準拠したリスク分析と評価（アセスメント）によって、管理策を策定していく。

ISMS適用例（不正プログラム対策）



ISMS			リスク評価			対策例
要項	目的	コントロール	対象範囲	脆弱性評価	定量化	技術的管理策
6.3悪意のあるソフトウェアからの保護　※	ソフトウェア及び情報の完全性を保護するため	1) 悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること	サイトと資産内容	(脆弱性) バックドアや情報を盗み出すプログラムが挿入されると、PHIの (脅威) 暴露Cに繋がる	脆弱性 影響性 頻度 評価	(管理策) コンピュータウィルス対策は、(機能) コンピュータウィルスを検出し駆除するので、(効果) バックドアや情報を盗み出すプログラムを検出し駆除できる

リモートサービスにおける安全管理措置

組織的安全管理措置

- 組織体制の整備
- 規定等の整備と運用
- 個人データ取扱い台帳の整備
- 安全管理全体の評価／見直し／改善
- 事故又は違反への対処

組織

技術的安全管理措置

- 個人データへのアクセスに関する識別と認証／制御／権限管理／記録
- 不正ソフトウェア対策
- 移送／送信時の対策
- 継続的な可用性及び完全性の維持
- バックアップ対策

技術

物理的安全管理措置

物理

- 入退館（室）の実施
- 盗難時に対する対策
- 機器／装置等の物理的保護

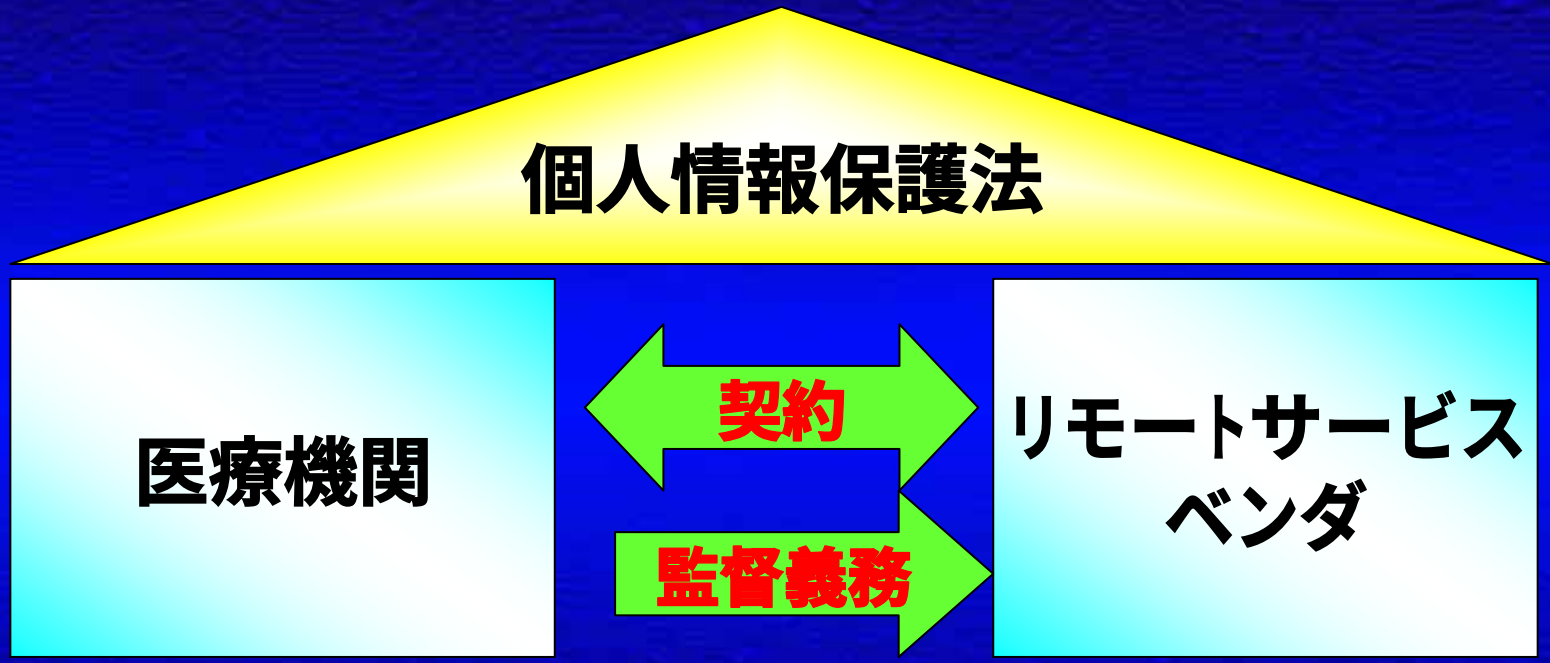
人的安全管理措置

人

- 雇用／委託契約時における非開示契約の締結
- 従業者に対する教育／訓練の実施

RSS-WGのリスクアセスメント結果より

医療機関とベンダの役割分担



医療システムに対する安全管理措置
- 組織的安全管理措置
- 物理的安全管理措置
- 技術的安全管理措置
- 人的安全管理措置

マッピング

リモートサービスの安全管理措置
- 組織的安全管理措置
- 物理的安全管理措置
- 技術的安全管理措置
- 人的安全管理措置

まとめ

- 守るべき情報資産に対しては、サービスを提供するベンダ側の安全管理対策だけでなく、サービスを受ける医療施設側の安全管理対策も重要である
- セキュリティを確保する運用を行うためには、情報セキュリティマネジメントシステムに則った対策を行うことが効果的である