リモートサービスにおけるセキュリティ管理
～　改訂版RSSガイドラインの紹介　～
(RSS:リモートサービスセキュリティ)

（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

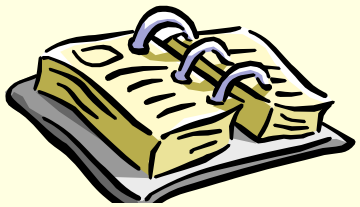
リモートサービスセキュリティ ガイドライン Ver2.0 (JESRA TR-0034-2010)

- 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の共同WGで作成しました
- 医療情報システムに対するリモートサービスが対象です
- 情報セキュリティマネジメントの手法の解説と、モデルによるリスクアセスメントの実施例を説明しています
- 本書の内容は、ISO/TR11633としてISO化されています

- **両工業会のWEBサイトで公開しています**
  - http://www.jira-net.or.jp
  - http://www.jahis.jp

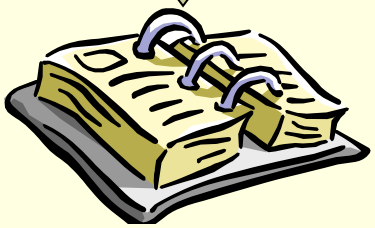
本ガイドラインへの経緯

リモートサービス
セキュリティガイド
(JESRA C0012 2003)



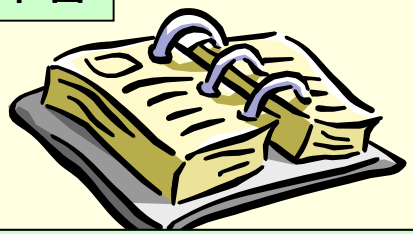
リモートサービス
セキュリティガイドライン
(JESRA C0013 2005)

国際標準化提案



ISO/TR11633(2009)

本書



リモートサービスセキュリティ
ガイドラインVer2.0
(JESRA TR0034)

リモートサービスセキュリティガイドライン

医療機器へのリモートサービスとは

- 医療施設内の医療機器に対し、院外から通信回線を通じて、サービスを行うこと

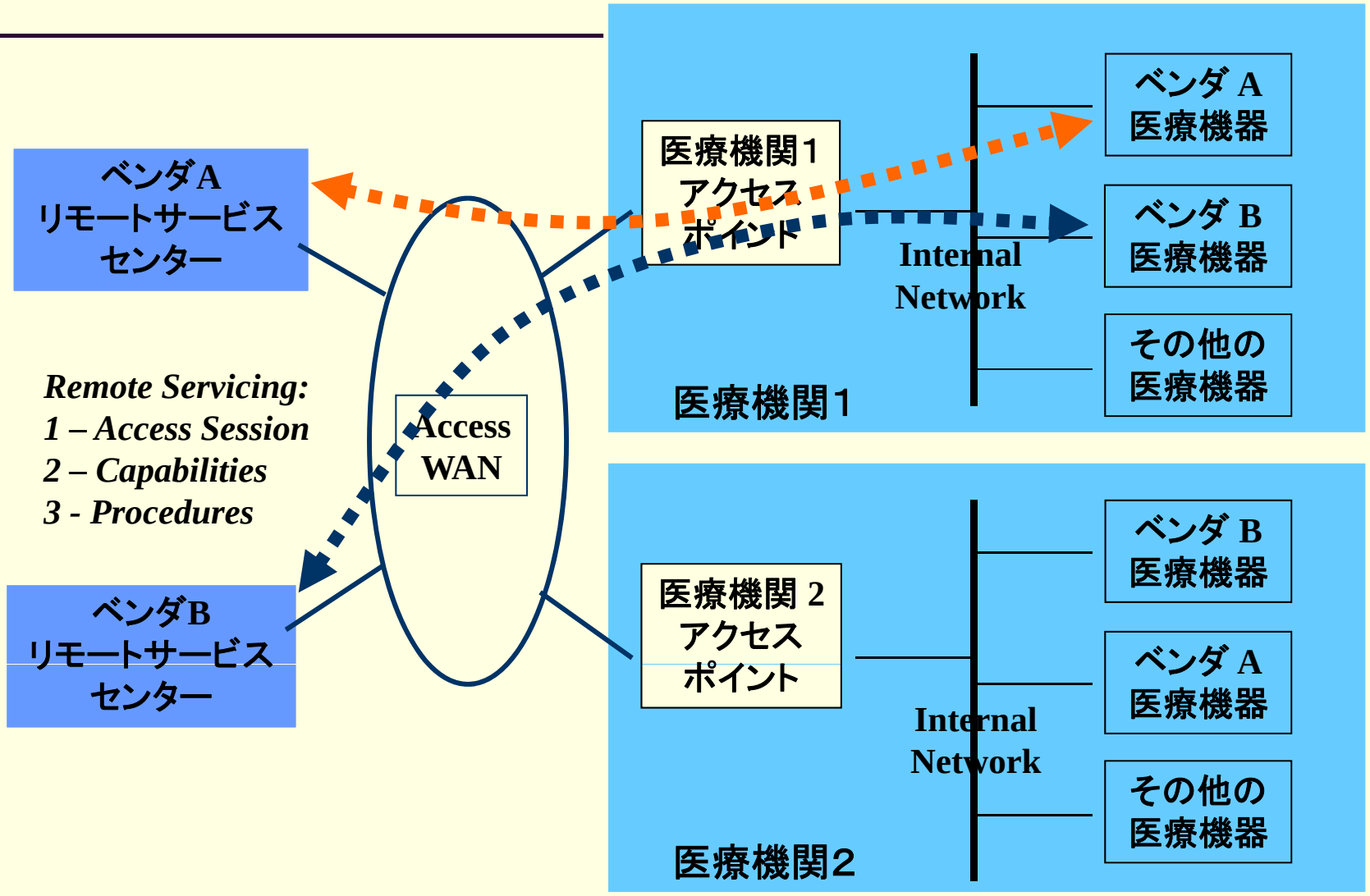
- 障害対応
  - 障害状況の情報を収集し解析を行う
- 予防保守
  - 機器の状況をモニタし、障害の兆候を事前に連絡する
- ソフトウェア改訂
  - ソフトウェアのバージョンアップ、バグ修正を行う

→

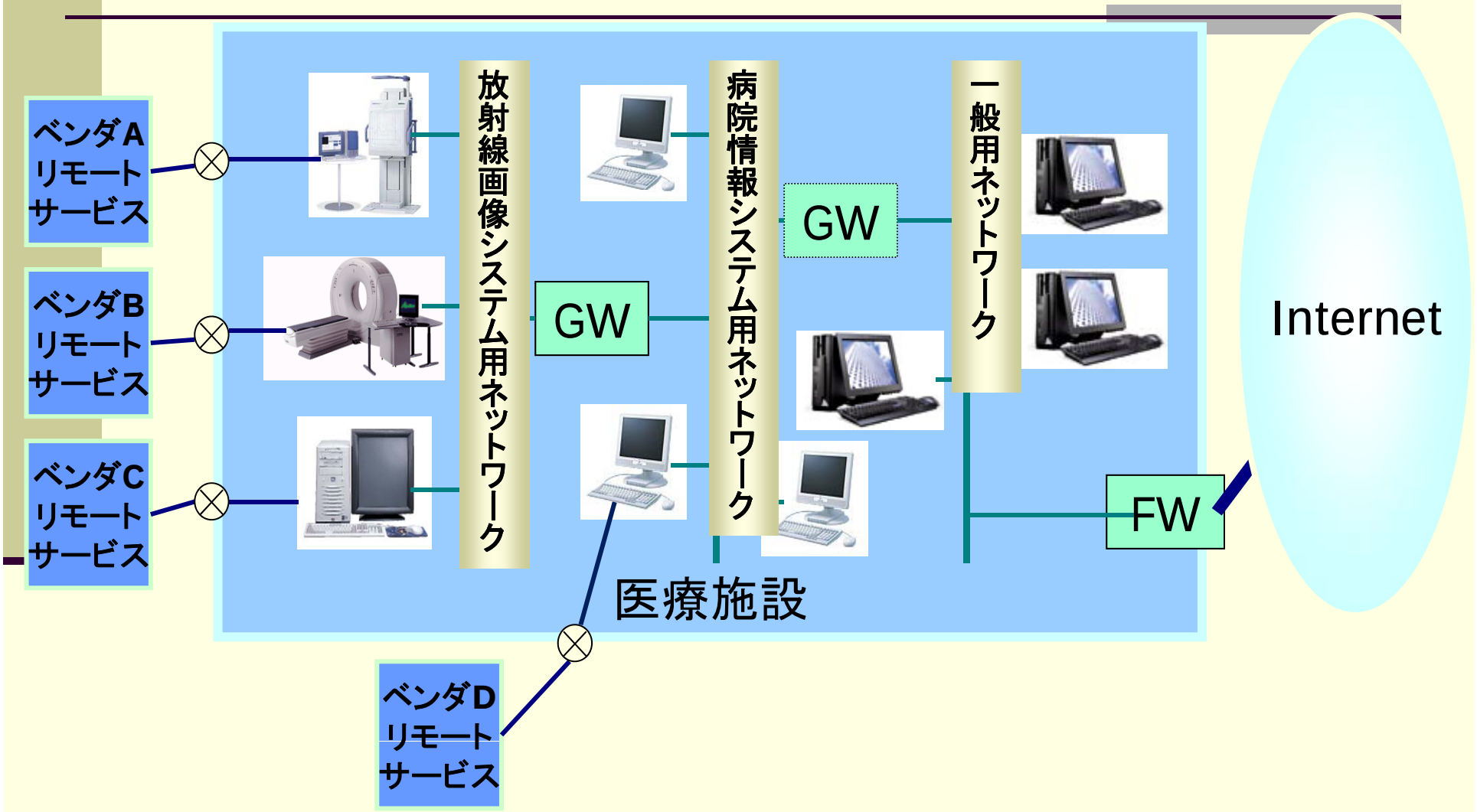
- ダウンタイムを大幅短縮
- 障害発生の事前検知
- 保守費用の大幅低減
- 施設側の対応負荷低減

本ガイドラインでのユースケース

リモートサービスの運用モデル(SPC)



医療機関のネットワークとリモートサービスの現状

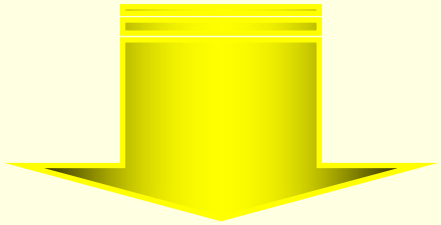


リモートサービスにおける脅威

（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…



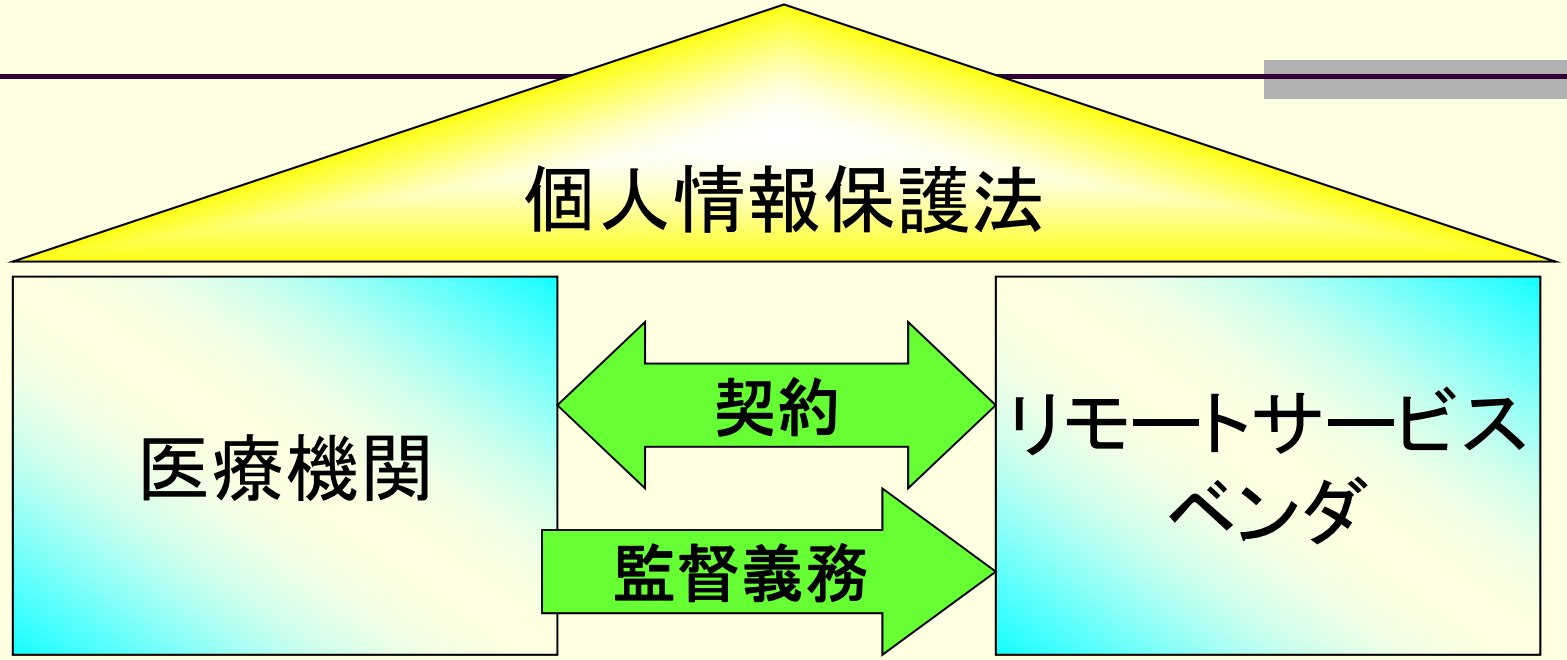
ISMS（情報セキュリティマネジメントシステム：ISO27001）に準拠したリスク分析と評価（アセスメント）によって、管理策を策定していく。

リモートサービスにおける脅威の例

- 個人情報保護の点
  - 修理記録の持ち出しによる**暴露**、保守センター等で解析中のデータの第三者による覗き見や**持ち出し**等
- 真正性の点
  - 管理者権限を悪用した意図的なデータの**改ざん**や、オペレーションミスによるデータの**改変**等
- 見読性の点
  - 意図的な**マシンの停止**や、オペレーションミスによる**サービス停止**等
- 保存性の点
  - 意図的な媒体の**破壊**及び**初期化**や、オペレーションミスによる媒体の**初期化**やデータの**上書き**等

「医療情報システムの安全管理に関するガイドライン」より

医療機関とベンダの役割分担が必要

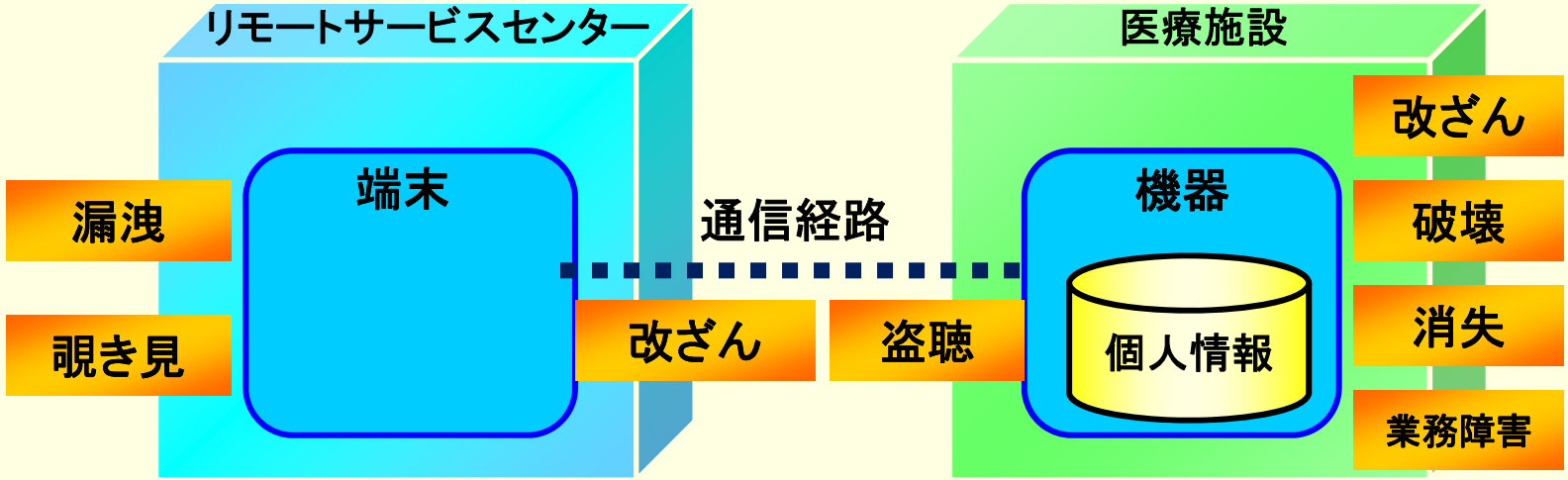


医療システムに対する安全管理措置
- 組織的安全管理措置
- 物理的安全管理措置
- 技術的安全管理措置
- 人的安全管理措置

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

セキュアなリモートサービスの構築が必要

- 診療情報に対するセキュリティの確保



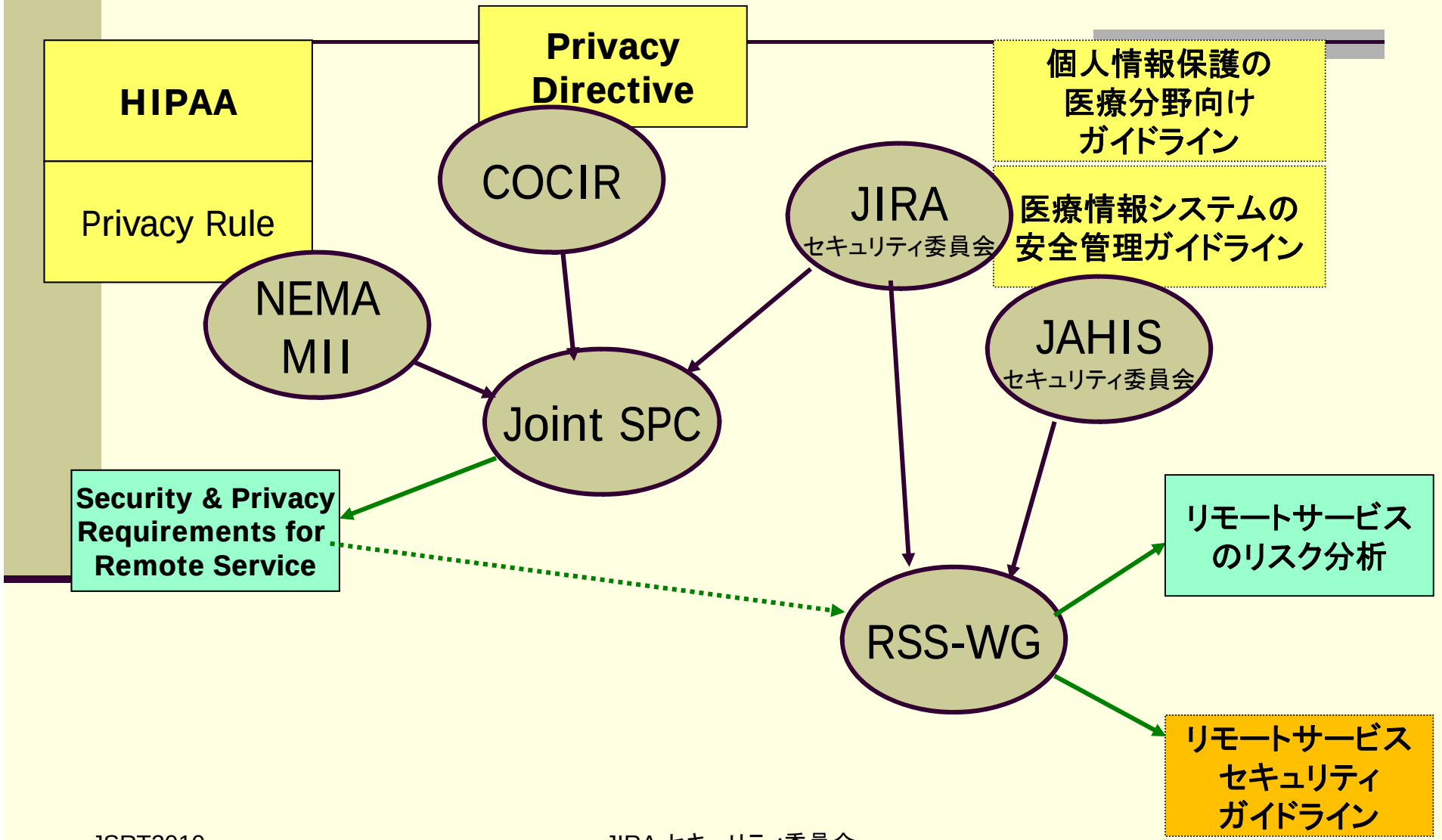
リモートサービスセンター、医療施設
共に守るべき情報資産に対して
- ・組織的安全管理措置
- ・物理的安全管理措置
- ・技術的安全管理措置
- ・人的安全管理措置

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

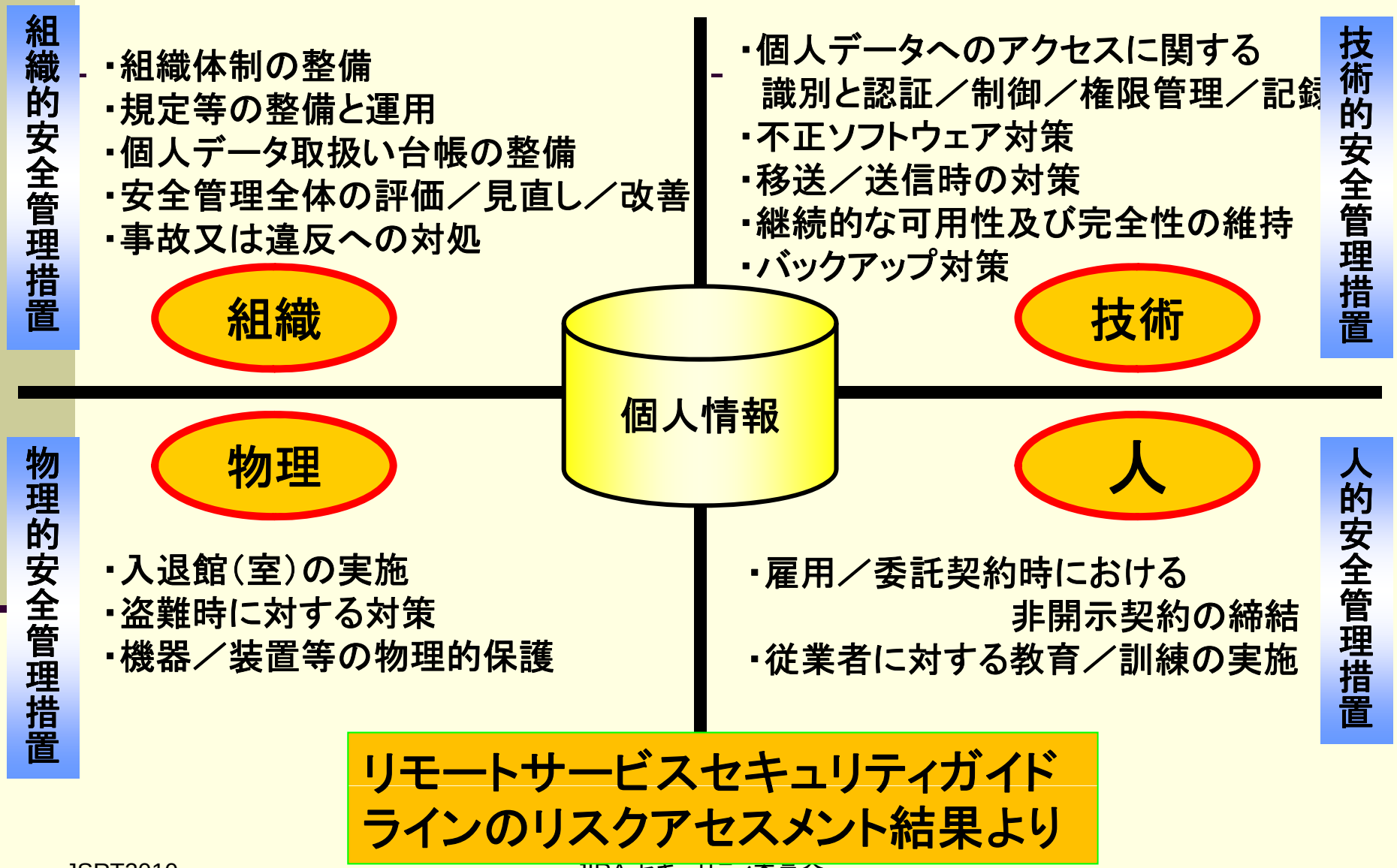
リモートサービスセキュリティの検討



情報セキュリティマネジメントシステム

- 情報セキュリティのマネジメントを行うための標準的な仕組み
- PDCAサイクルによるセキュリティ運用管理
  - Plan
  - Do
  - Check
  - Action
- ISO9000やISO14000の考え方をセキュリティ管理に適用したもの
- ISO 17799（BS7799）で国際標準化
- 第三者による認証制度がある

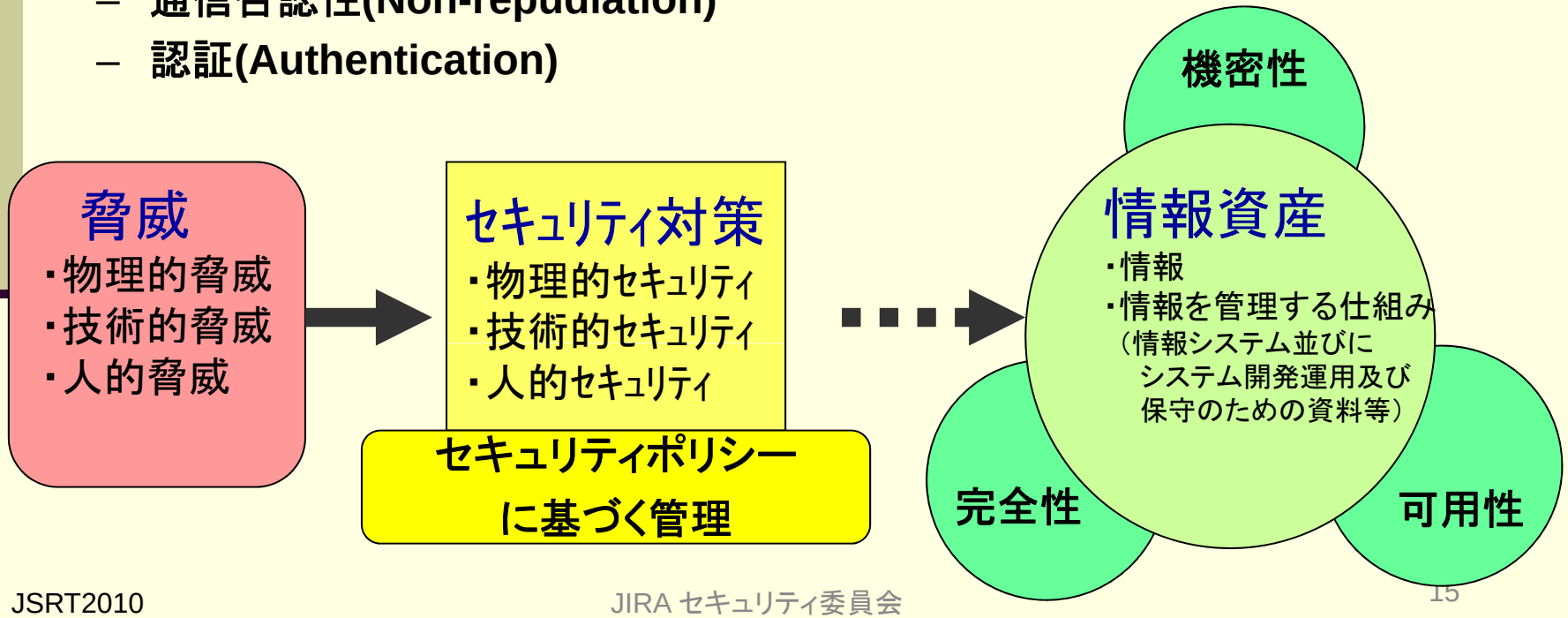
リモートサービスにおける安全管理措置の例



リモートサービスセキュリティガイドライン
のリスクアセスメント結果より

情報セキュリティとは

- 情報資産の3大要素＝C.I.A
  - 機密性（Confidentiality）
  - 完全性（Integrity）
  - 可用性（Availability）
- さらに
  - 通信否認性(Non-repudiation)
  - 認証(Authentication)



リスク値 ＝ 「情報資産の価値」 × 「脅威」 × 「ぜい弱性」

リスクマネージメント

リスクコントロール　積極的に損害を小さくする対策（管理策）を採用する

・リスク予防
　脅威や脆弱性を少なくするための対策を実施する
・損害の極小化
　リスクが発生したときの損害を少なくするための対策を実施する

リスク保有　組織としてリスクを受容する対応

・リスクファイナンス
　引当金を積むなどの対応を行う
・何もしない

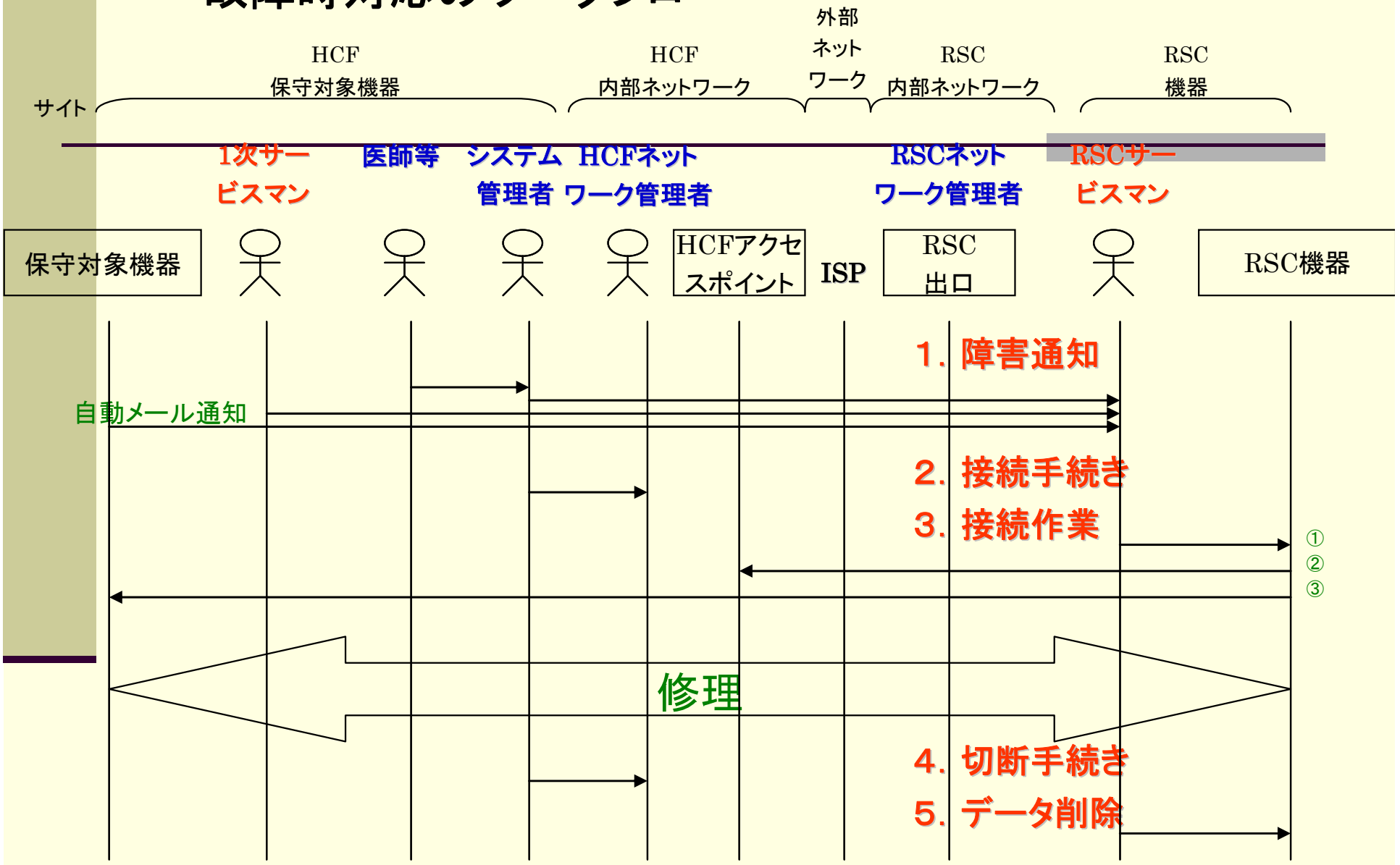
リスク移転　契約等により他社に移転する対策

・リスクファイナンス
　損害保険や責任賠償保険などに加入しリスクを移転する
・アウトソーシング
　情報資産そのものや情報セキュリティ対策を外部に委託する

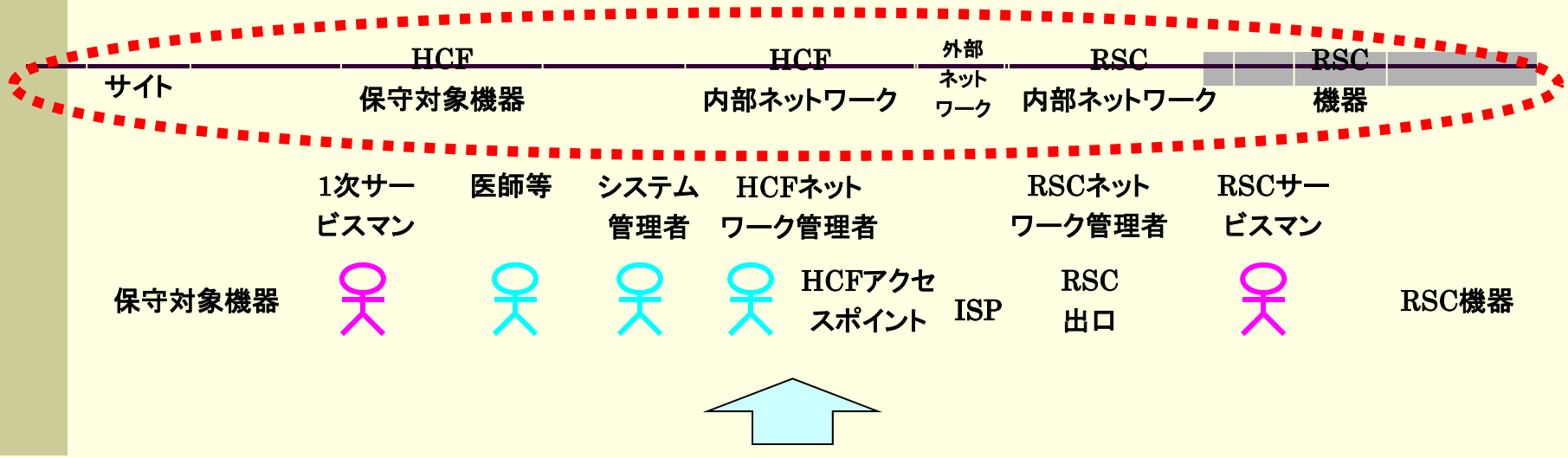
リスク回避　適切な対策が見出せない場合の対応

・業務の廃止
　業務そのものをやめてしまう
・情報資産の破壊
　管理対象物をなくしてしまう

故障時対応のワークフロー

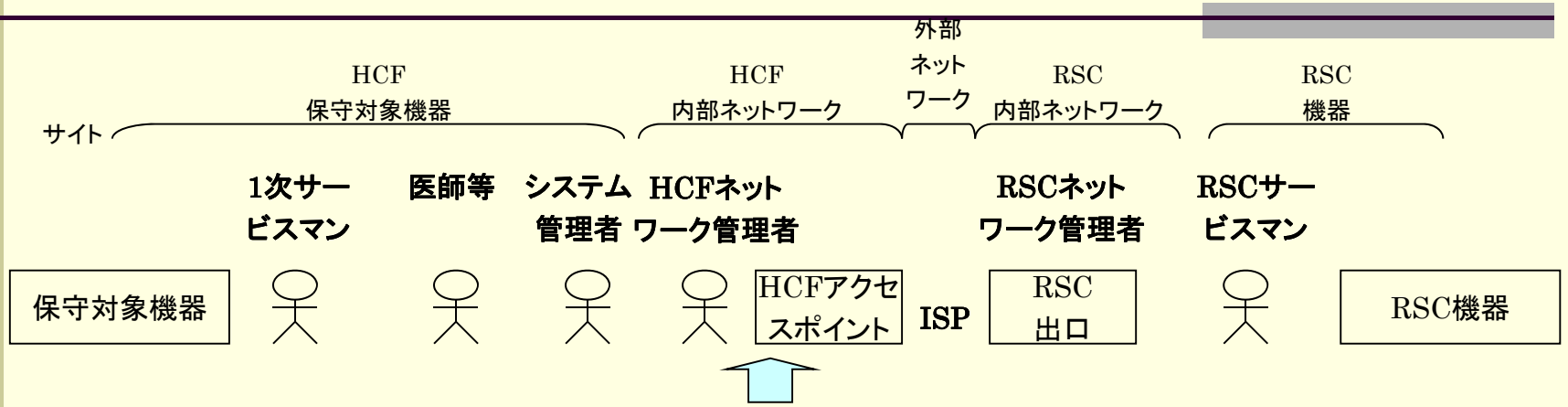


ISMS適用例（不正プログラム対策）



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I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

資産と脅威（サイト:HCF内部ネットワーク）



資産	番号	脅威（C:機密性,I:完全性,A:可用性）
HCF内部ネットワーク上のPHI情報	41	経路の覗き見C,HCF側ネットワーク機器の不正ログインC/成りすましC,タッピングCによる暴露C
上記通信トレースのメモやプリントアウトの紙	42	監視記録紙の覗き見C,持出Cによる暴露C
上記通信トレースのバックアップ媒体	43	監視記録媒体の持出Cによる暴露C
ネットワーク機器のソフトウエア	44	バックドアや情報を盗み出すプログラムの挿入Iによる暴露C
ネットワーク機器	45	持出C,タンパリングC,漏えい電磁波Cによる暴露C
	46	故障A,被災A,破壊Aによるサービス不能A
ネットワーク機器の環境設備*1	47	故障A,被災A,破壊A,ケーブル不通Aによるサービス不能A
ネットワーク機器の操作者	48	収賄による暴露C、誤設定Cによる暴露C

*1電源・防災設備を指す。

脆弱性の評価基準

	点数	評価基準
機密性	1	覗き見/盗用,不正ログイン/成りすまし,持出による暴露に対して脆弱性が無視できる
	2	覗き見/盗用,不正ログイン/成りすまし,持出による暴露に対してやや脆弱である
	3	覗き見/盗用,不正ログイン/成りすまし,持出による暴露に対して極めて脆弱である
完全性	1	改ざん,差換え,消去によるねつ造や否認に対する脆弱性が無視できる
	2	改ざん,差換え,消去によるねつ造や否認に対してやや脆弱である
	3	改ざん,差換え,消去によるねつ造や否認に対して極めて脆弱である
可用性	1	故障,災害,ケーブル不通・サービス妨害によるサービス不能に対する脆弱性が無視できる
	2	故障,災害,ケーブル不通・サービス妨害によるサービス不能に対してやや脆弱である
	3	故障,災害,ケーブル不通・サービス妨害によるサービス不能に対して極めて脆弱である

影響性（資産価値)の判断基準

影響性	1	経営・業務遂行に影響が無視できる
	2	経営・業務遂行に影響がでる可能性がある
	3	経営・業務遂行に重大な影響がでる可能性がある

発生可能性（脅威）の判断基準

発生可能性	1	起こる可能性が無視できる
	2	起こる可能性が少ない
	3	起こる可能性が多い

ガイドラインでの管理策例

A.11.アクセス制御	脆弱性	資産	脅威	評価	技術的管理策例	運用的管理作例
（脆弱性）外部経路からの全ての者によるRSC側ネットワーク機器の漏洩パスワードを用いた成りすましCが行われると、RSC側経路上のPHIが盗用Cされ（脅威）暴露Cに繋がる （脆弱性）内部経路からのRSCネットワーク管理者以外の者によるRSC側ネットワーク機器の漏洩パスワードを用いた成りすましCが行われると、RSC側経路上のPHIが盗用Cされ（脅威）暴露Cに繋がる	3→2	3	1	9→6	—	（管理策）パスワードの定期的な変更は、（機能）パスワードの強度を維持するので、（効果）RSC側ネットワーク機器の成りすましを防止できる。
A.9.物理的及び環境的セキュリティ						
（脆弱性）オンサイトでのRSCサービスマンによるPHIの削除忘れCがあると、PHIの（脅威）想定外の暴露Cに繋がる	3→2	3	1	9→6	—	（管理策）ログオフ時の自動消去は、（機能）人的ミスを防止するので、（効果）RSCサービスマンのPHIの削除忘れを防止できる。

まとめ

- **確実にセキュリティを維持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(ISMS)に則った対策を行うことが効果的である**
  - リモートサービスにおいては、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
- **両者間でISMS実施のためのガイドライン（リモートサービスセキュリティガイドライン Ver2.0）を策定したので参考にしていただきたい**