リモートサービスにおけるセキュリティ

㈳ 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
野津　勤

本RSS Guidelineの前提となる文書類

1. HIPAAによるRemote ServiceへのFDA規制
2. SPC(Joint NEMA-COCIR-JIRA Security and Privacy Committee)のRemote Servicing Paper、Solution-A
   ：医療機関側とサービス提供社側の対応
   ：RSS用アクセスポイントを一つに集約した場合のシステム構成
3. 個人情報保護法
   第三者提供の制限、人的安全管理措置：業務委託契約
4. 医療情報システムの安全管理に関するガイドライン
   人的安全対策：業務委託先の監督、保守業務での守秘義務契約
5. 情報セキュリティ
   ：ISO17799(一般企業向け)、ISO27799(医療機関向け)
6. 医療機関向けISMSユーザーズガイド
   ：JIPDEC

医療機器におけるリモートサービス

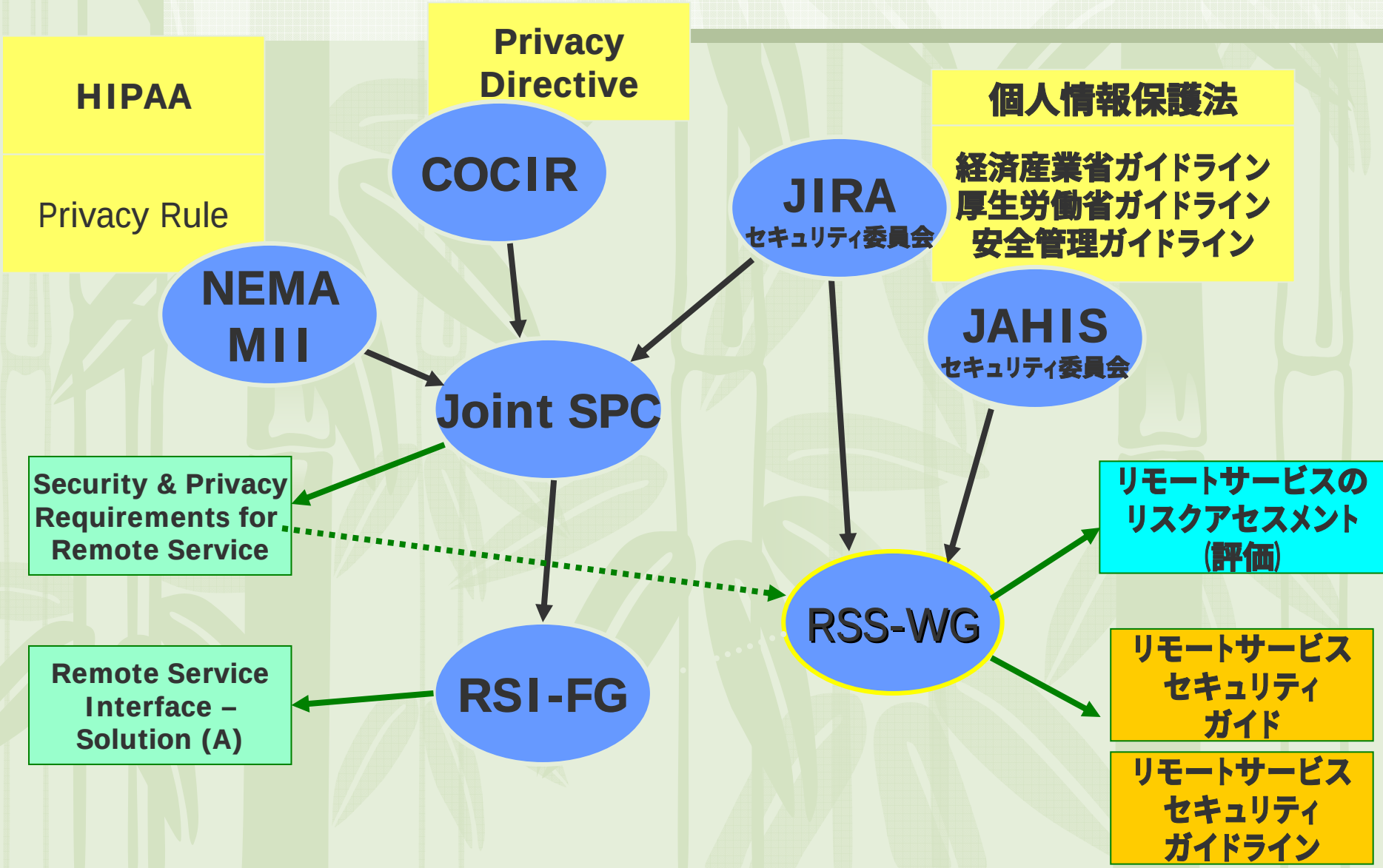
- 医療機関内の医療機器に対し、院外から通信回線を通じてアクセスしサービスを行うこと

- 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

リモートサービスへの期待

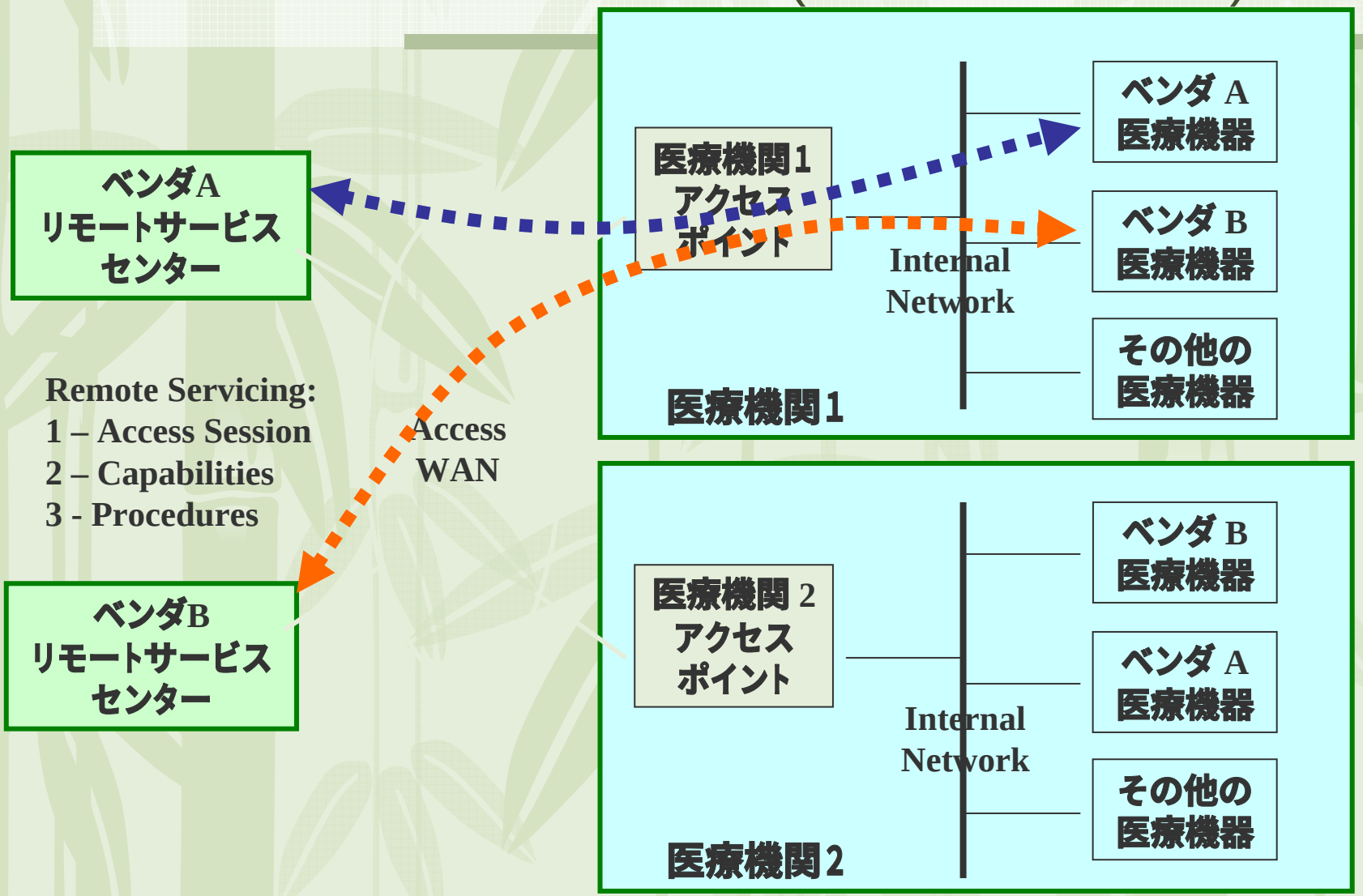
- ダウンタイムの大幅短縮
- 障害を予防することが可能
- 保守費用の大幅低減
- 医療施設側の対応も低減

リモートサービスセキュリティの検討

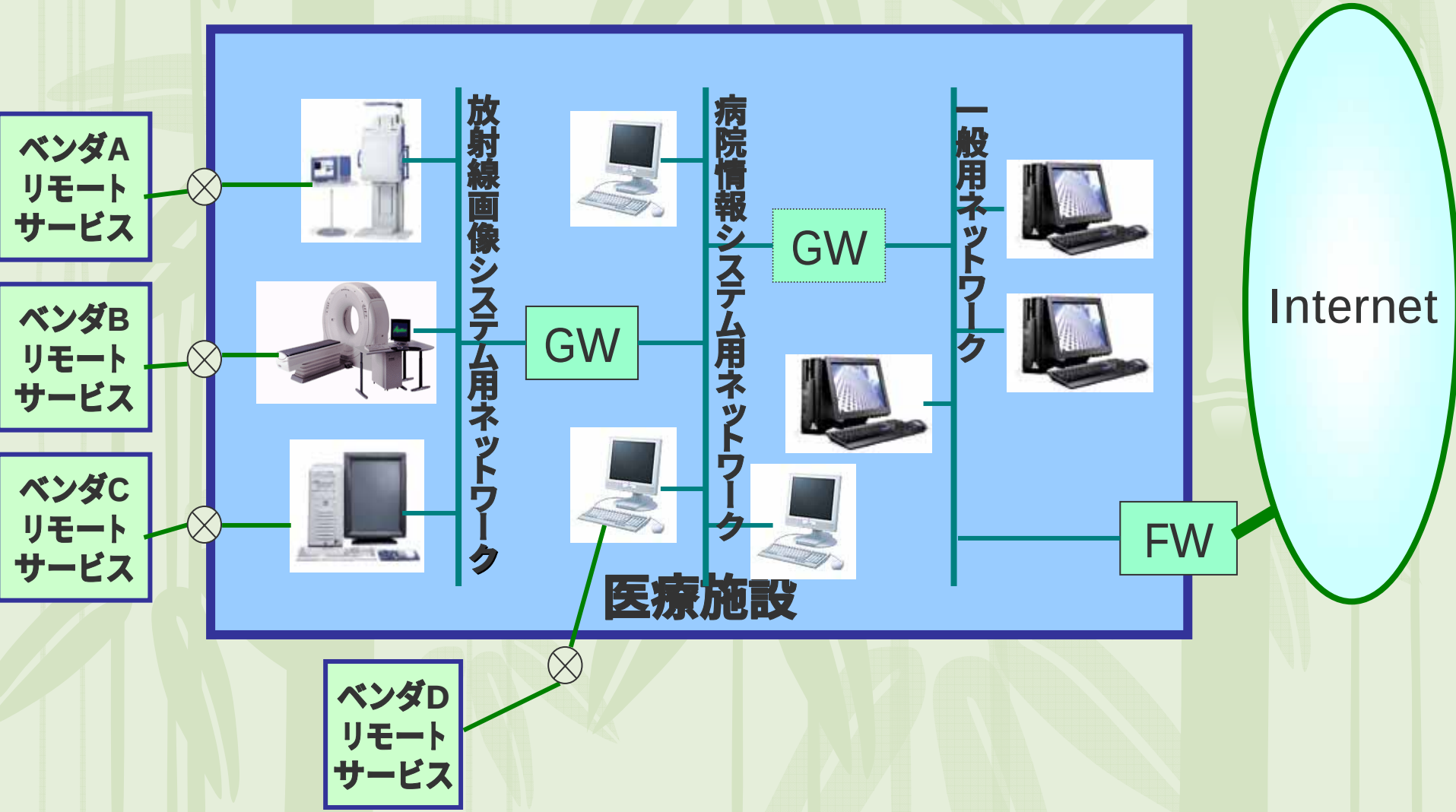


リモートサービスの運用モデル

(SPCでのSolution-A)

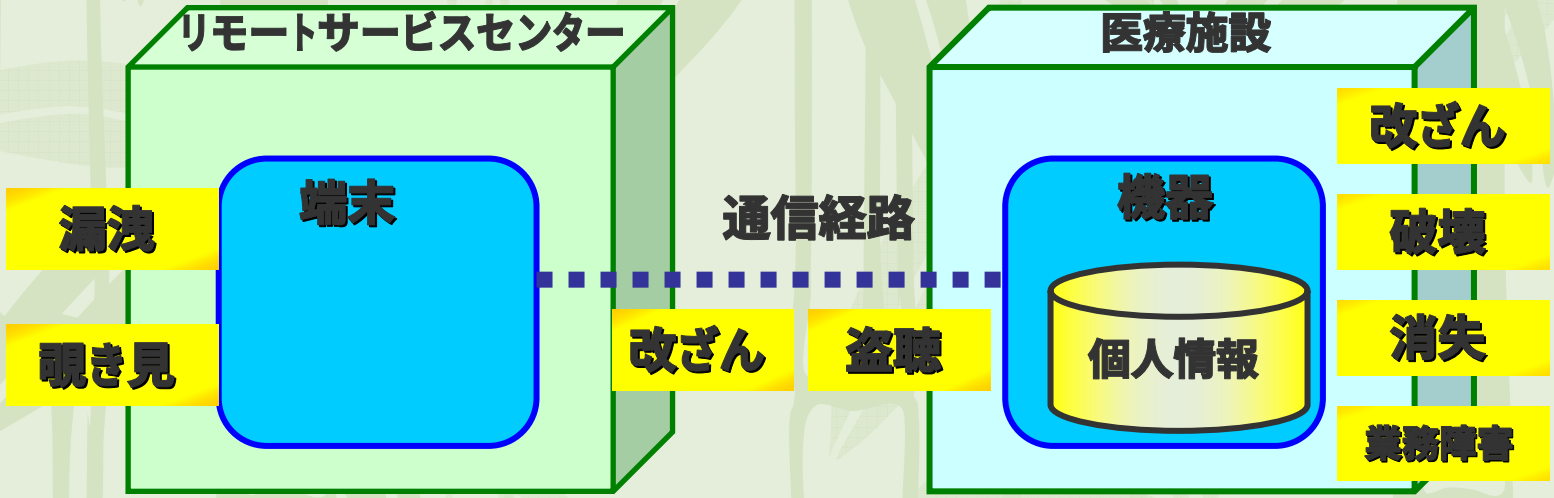


医療機関のネットワークとリモートサービス
(現状の殆ど)



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



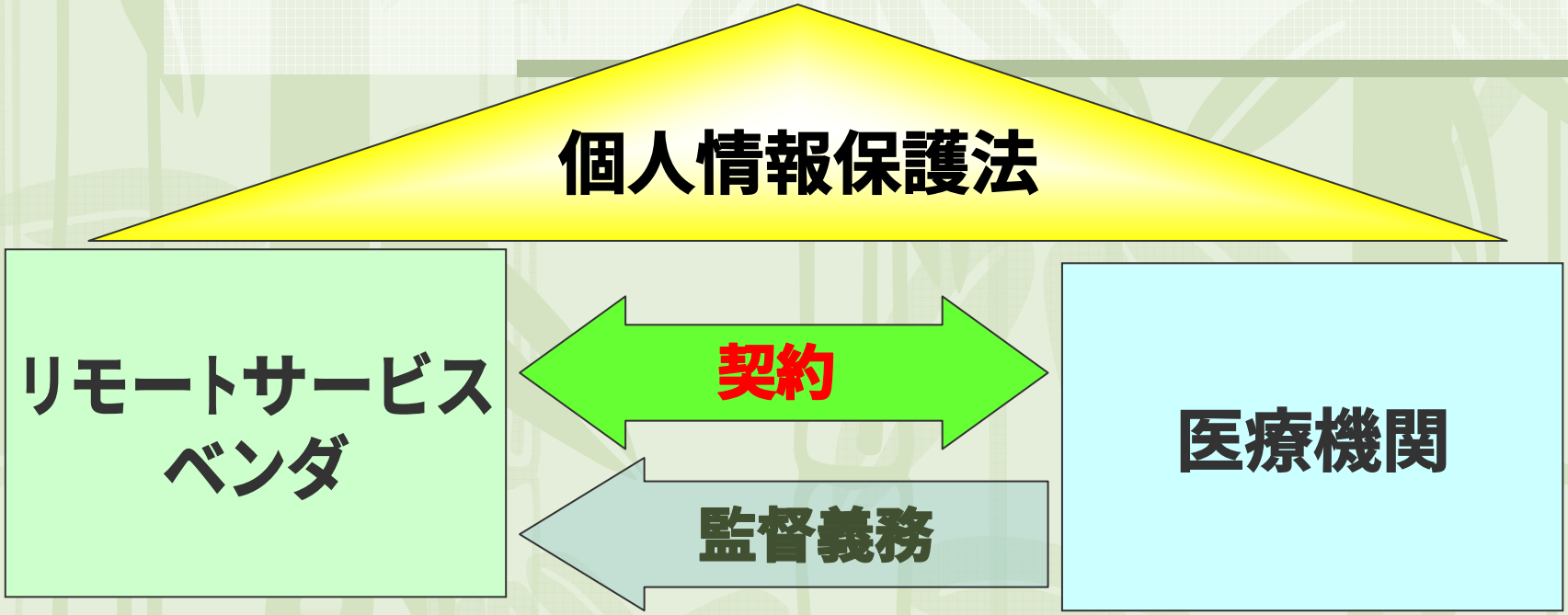
リモートサービスセンター、医療施設共に
守るべき情報資産に対して
- ・組織的安全管理措置
- ・物理的安全管理措置
- ・技術的安全管理措置
- ・人的安全管理措置

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<u>個人情報</u>
◎接続する<u>医療機器やそのサイト</u>

<u>総合的な「リスクアセスメント」が必要</u>

医療機関とベンダの役割分担



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

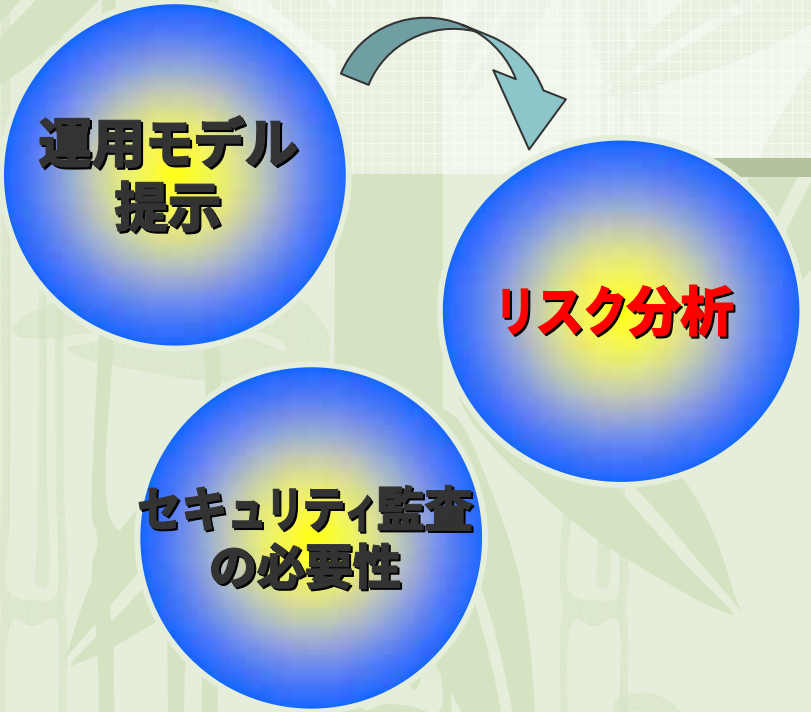
マッピング

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

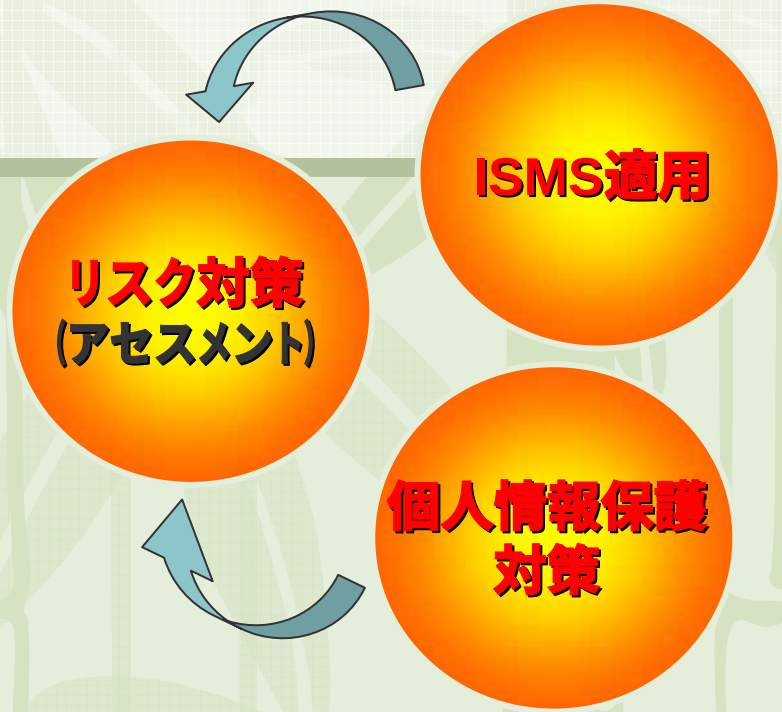
- JIRAとJAHIS（保健医療福祉情報システム工業会）の
  両セキュリティ委員会にて共同でRSS-WGを発足し作成
  - リモートサービスセキュリティガイド（JESRA C-0012-2004）
  - リモートサービスセキュリティガイドライン（JESRA C-0013-2006）
- リモートサービスを行う医療情報システムが対象
- 両工業会のWEBサイトで公開される予定
  - http://www.jira-net.or.jp
  - http://www.jahis.jp

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



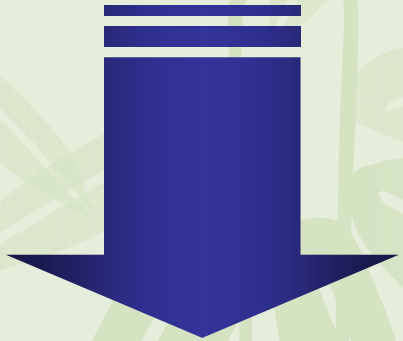
内容
はじめに
第1章　リモートサービスガイドラインの必要性
第2章　リモートサービスセキュリティの要件
第3章　リモートサービスへのISMSの適用
第4章　管理目的と管理策の選択
第5章　残存リスクの承認
第6章　セキュリティ監査のガイドライン
第7章　本ガイドの技術的･制度的変化への対応
参照規格および法規
付録 (リスクアセスメント表)

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

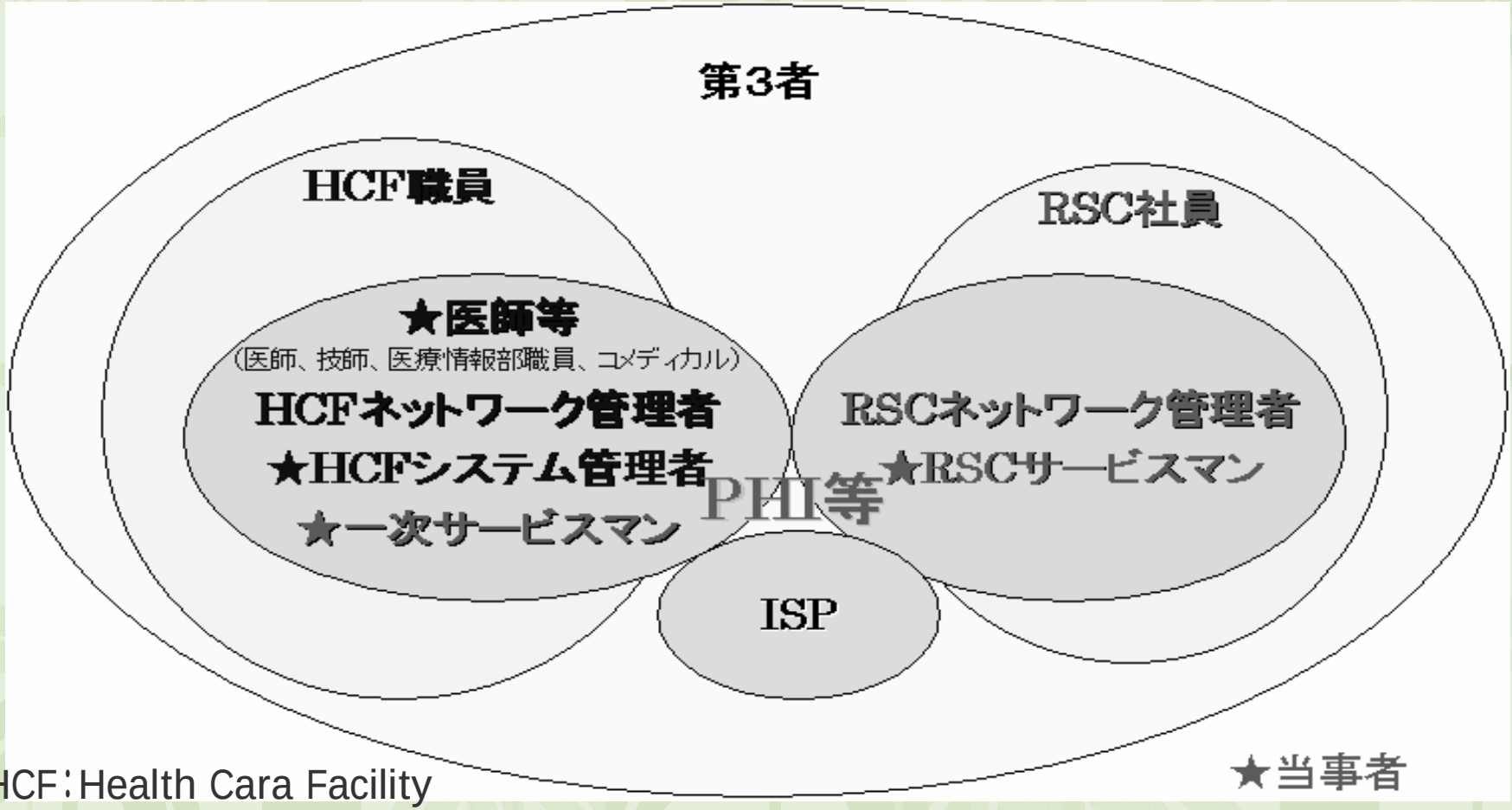
(B) **完全性**：改ざん、差換え、消去

(C) **可用性**：故障、利用不能



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。

リモートサービスの運用モデル



HCF：Health Cara Facility
RSC：Remote Service Center
PHI：Protected Healthcare Information
ISP：Internet Service Provider

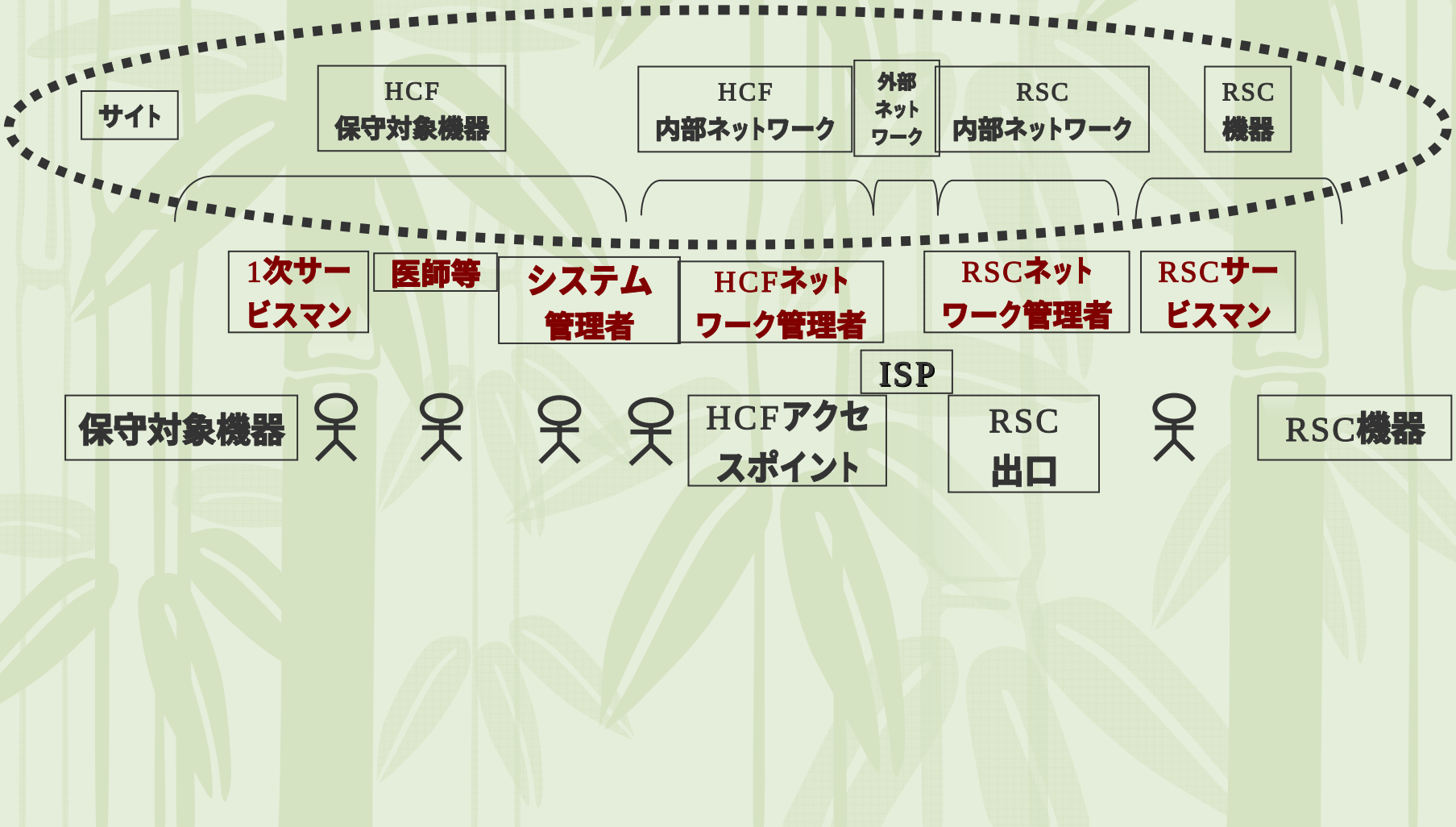
リモートサービスの運用モデル

ガイドラインでは、

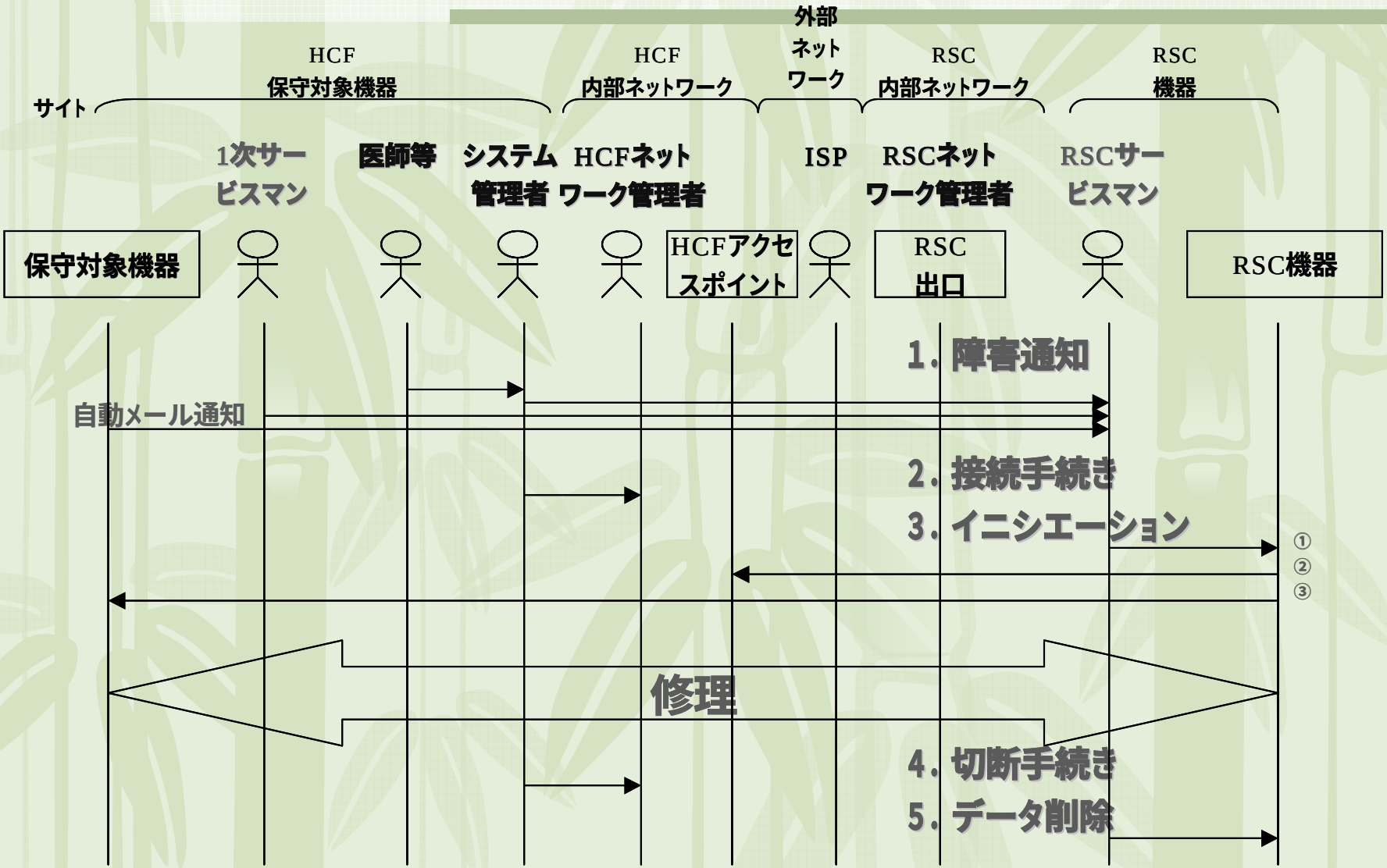
サイト分類別に情報資産の洗出し、脅威と脆弱性を分析。

- 情報資産の重要度：すべて同じレベルと想定
- サイト：RSC機器・内部ネットワーク、外部ネットワーク、HCF内部ネットワーク・保守対象機器
- 脅威の対象範囲：リモートサービスで扱うPHIに対する、HCFサイト外からのアクセス
  - 即ち、HCFサイトの関係者（医師等、HCFシステム管理者、HCFネットワーク管理者、HCF職員、一次サービスマン）を除外
  - HCFが行う行為を除外
  - PHIを扱う機器やソフトウェアの可用性にかかわる脅威を除外
  - コンピュータウィルスにかかわる脅威を除外
  - 採用・教育・訓練にかかわる要員の脅威を除外

リモートサービスの関係者



例：故障時の対応のワークフロー



例：障害対応時のワークフロー

HCFからの問題発生の連絡を受ける（電子メールによる自動通知の場合もある）
HCFにリモートサービスのためのネットワーク接続を申請
RSCからネットワーク接続（図中①→②→③）
ネットワークを介して、調査、対策、確認を行う。
（A）自己診断プログラムの実行
（B）当該機器からの関連情報の取得
（ア）動作ログ
（イ）画像データ
（ウ）設定ファイル／システムコンフィグレーション
（エ）データベース内容
（C）問題を切り分ける。
（D）問題がソフトウェア起因の場合には、当該機器の変更・更新作業
（ア）設定ファイル変更
（イ）S/W更新
（ウ）データ修復
（E）問題がH/W起因の場合には、1次サービスマンに故障部品の手配・交換を依頼
（F）修理後の動作確認
HCFへ作業結果の報告
リモートサービスのためのネットワーク接続の切断
HCFにリモートサービスのためのネットワーク接続切断を申請
RSC側にPHI情報を転送した場合には、それらのPHI情報を全て削除

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

個人情報

物理的安全管理措置

物理

- 入退館（室）管理の実施
- 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

ガイドラインでのリスク評価表

	点数	評価基準
機密性への脆弱性	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
完全性への脆弱性	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
可用性への脆弱性	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
資産価値(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
脅威(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

5．物理的及び環境的セキュリティ

	脆弱性	資産	脅威	評価	技術的管理策例	運用的管理作例
(前提) 修理の都合または分離不可で当該資産を残した時、(脆弱性) 第3者,RSC社員,RSCネットワーク管理者による覗き見C、持出Cが行われると、PHIの (脅威) 暴露Cに繋がる	3→2	3	1	9→6	—	(管理策) 入室管理は、(機能) 権限の無い者の入室を防止するので、(効果) 第3者,RSC社員,RSCネットワーク管理者による入室を阻止して紙の覗き見や持出を防止できる。
(前提) 修理の都合または分離不可で当該資産を残した時、(脆弱性) 第3者,RSC社員,RSCネットワーク管理者による持出Cが行われると、PHIの (脅威) 暴露Cに繋がる	3→2	3	1	9→6	—	(管理策) 施錠保管は、(機能) 権限の無い者の接触を防止するので、(効果) 第3者,RSC社員,RSCネットワーク管理者による接触を阻止して媒体の持出を防止できる。

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