リモートサービスにおける セキュリティについて

(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

JIRA セキュリティ委員会の活動

- 医用画像情報システムにおける情報セキュリティの検討
  - 診療録などの電子保存への対応
  - DICOM WG14 Securityへの対応
  - ISO/TC215 /WG4 Securityへの対応
  - 個人情報保護法への対応
  - リモートサービスにおけるセキュリティの検討
  - 日米欧の工業会での協調：Joint SPC

今回の発表内容

- リモートサービスにおけるセキュリティについて
- 画像医療機器におけるコンピュータウィルス対応について
- 医用画像データにおける個人情報保護に対する留意点

リモートサービスセキュリティガイド

- JIRAとJAHIS（保健医療福祉情報システム工業会）との共同で作成
- 画像医療システムを含む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

- 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

医療機器におけるリモートサービス

- 画像医療機器
  - 画像診断：診療に必要不可欠な存在
  - 診療の円滑な運用を確保するためには
  - ダウンタイムの大幅短縮が必要
  - 壊れないこと
  - 迅速な修理
  - 機器の高度化による問題解決に時間がかかる
  - リモートサービスへの期待

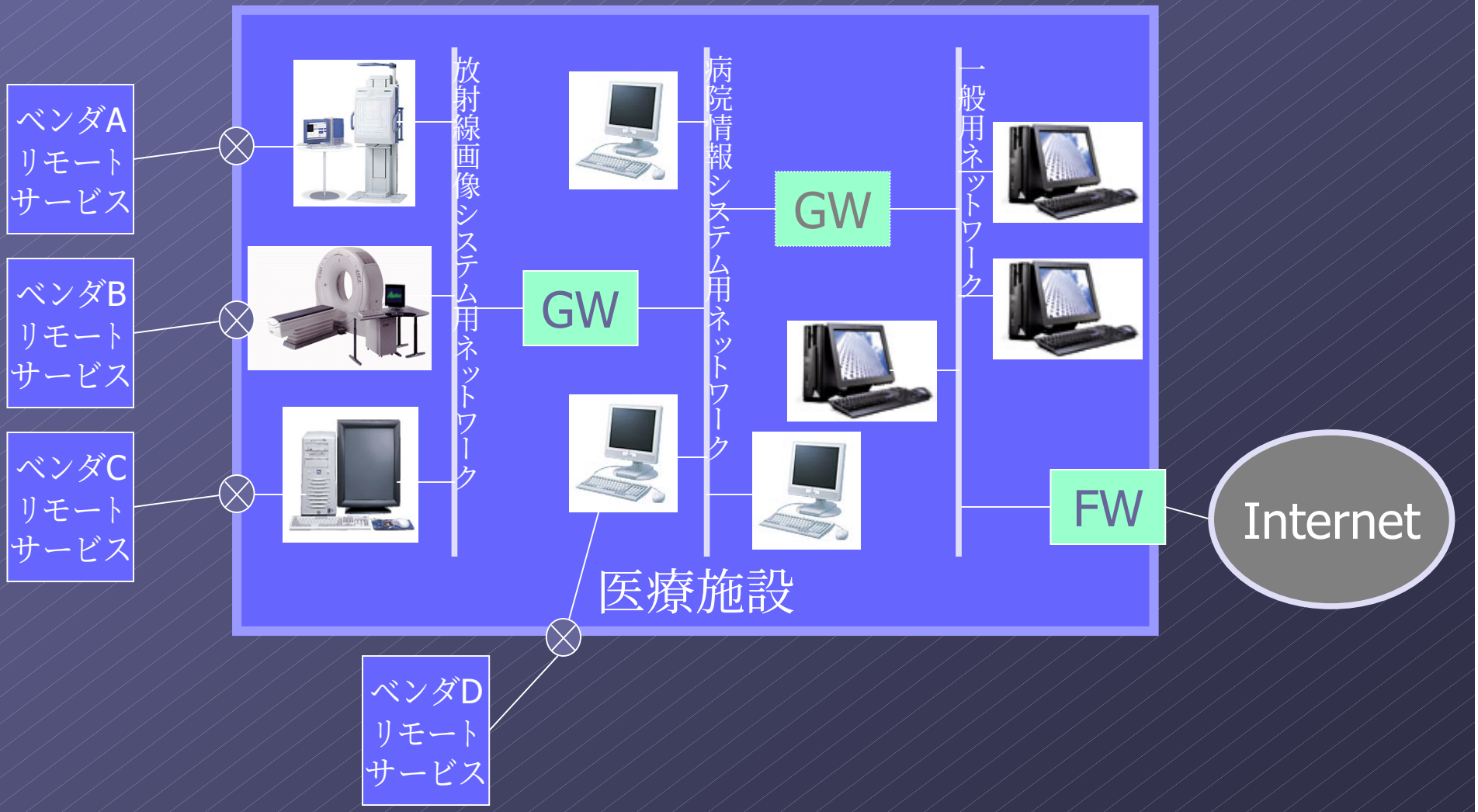
医療機器におけるリモートサービス

- 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

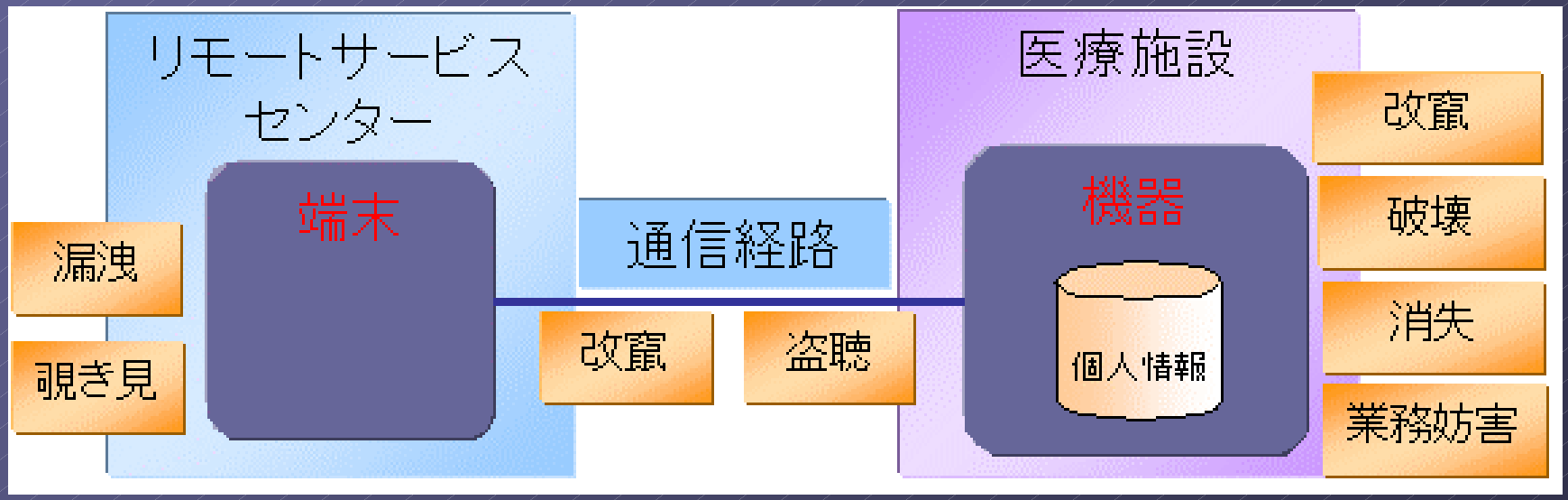
- ダウンタイムの大幅短縮
- 障害を予防することが可能
- 保守費用の大幅低減
- 医療施設側の対応も低減

医療機関でのネットワークセキュリティとリモートサービス

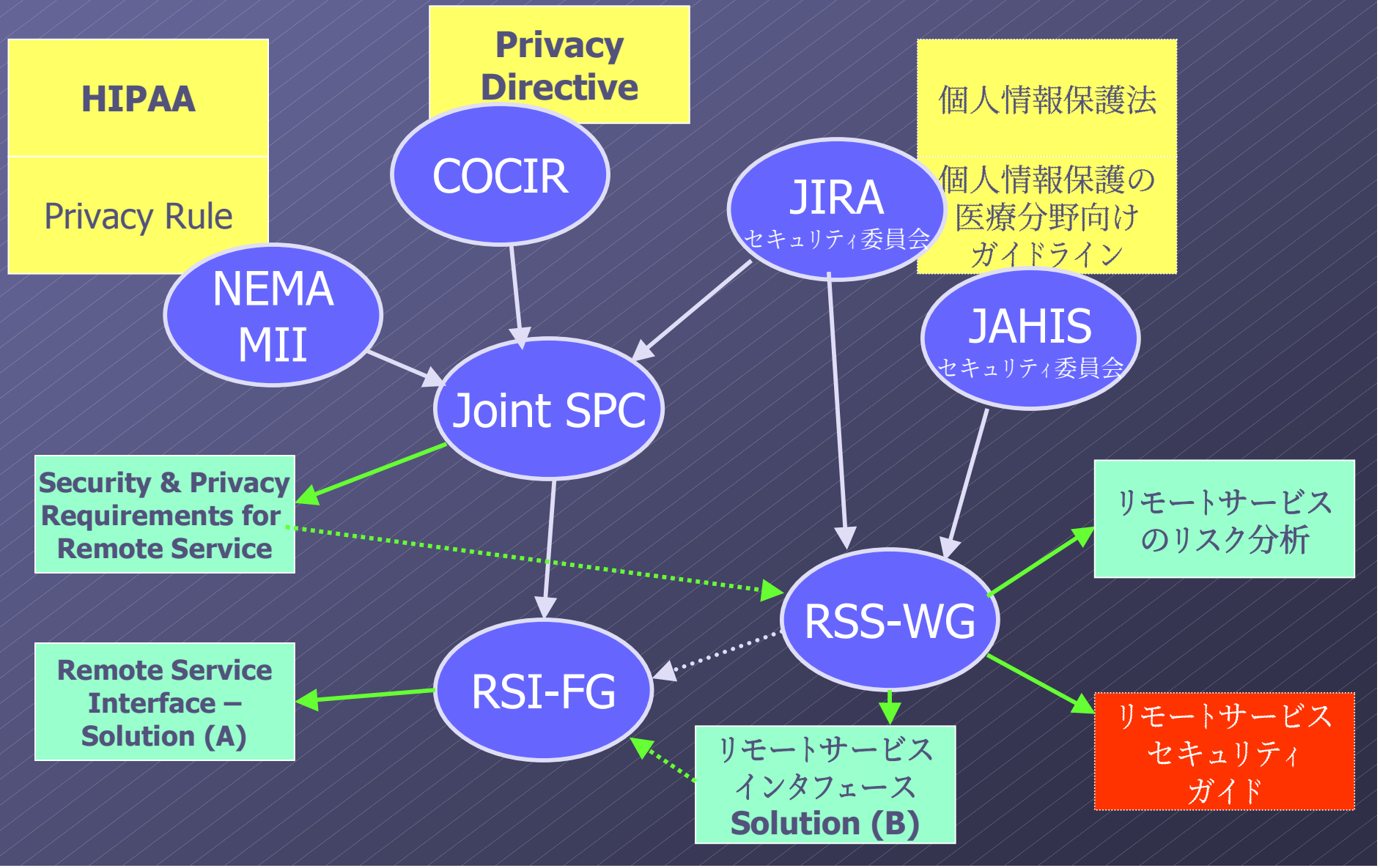


リモートサービスの課題

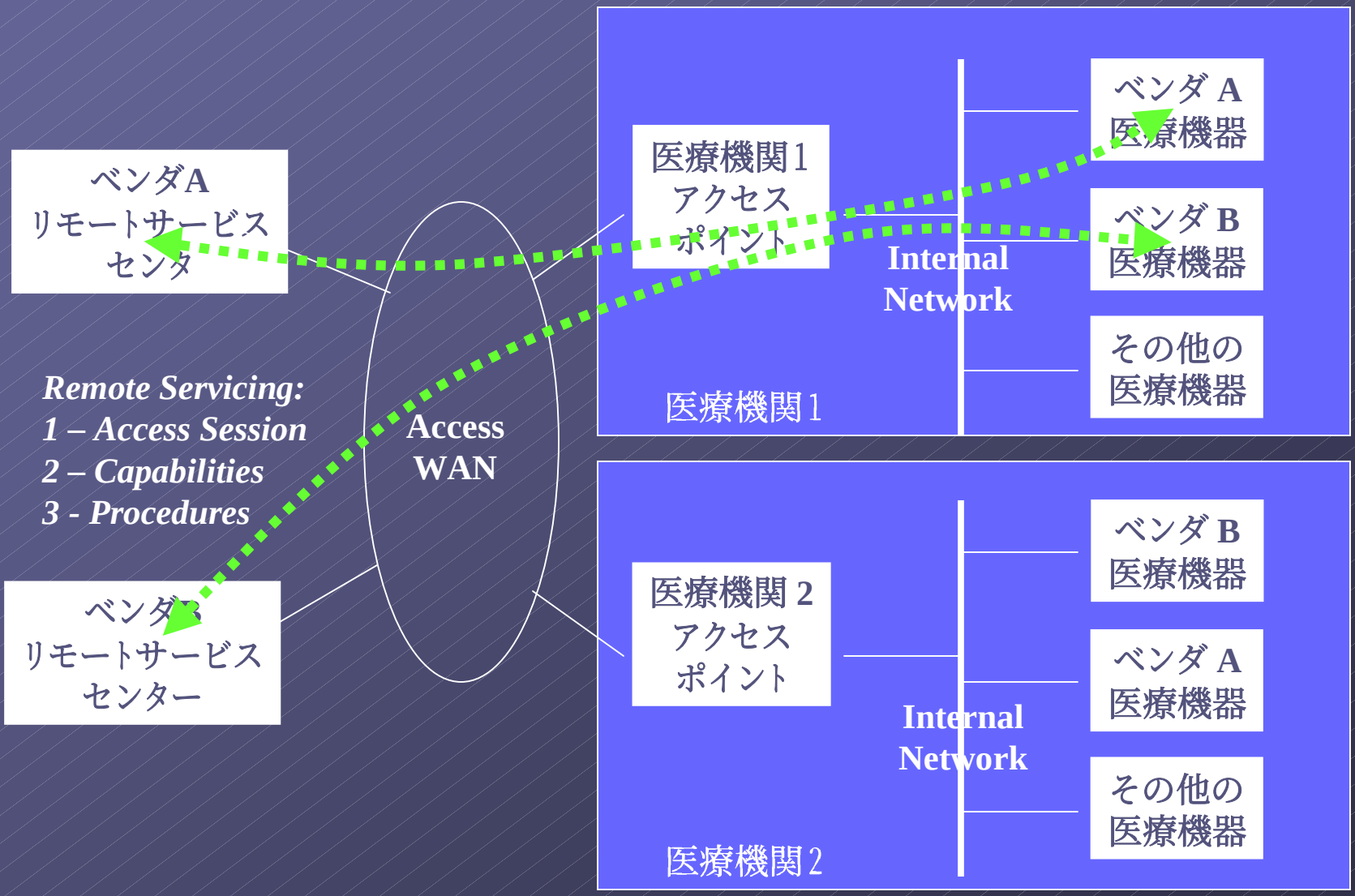
- 診療情報に対するセキュリティの確保



リモートサービスセキュリティの検討



SPC:リモートサービスのガイドライン



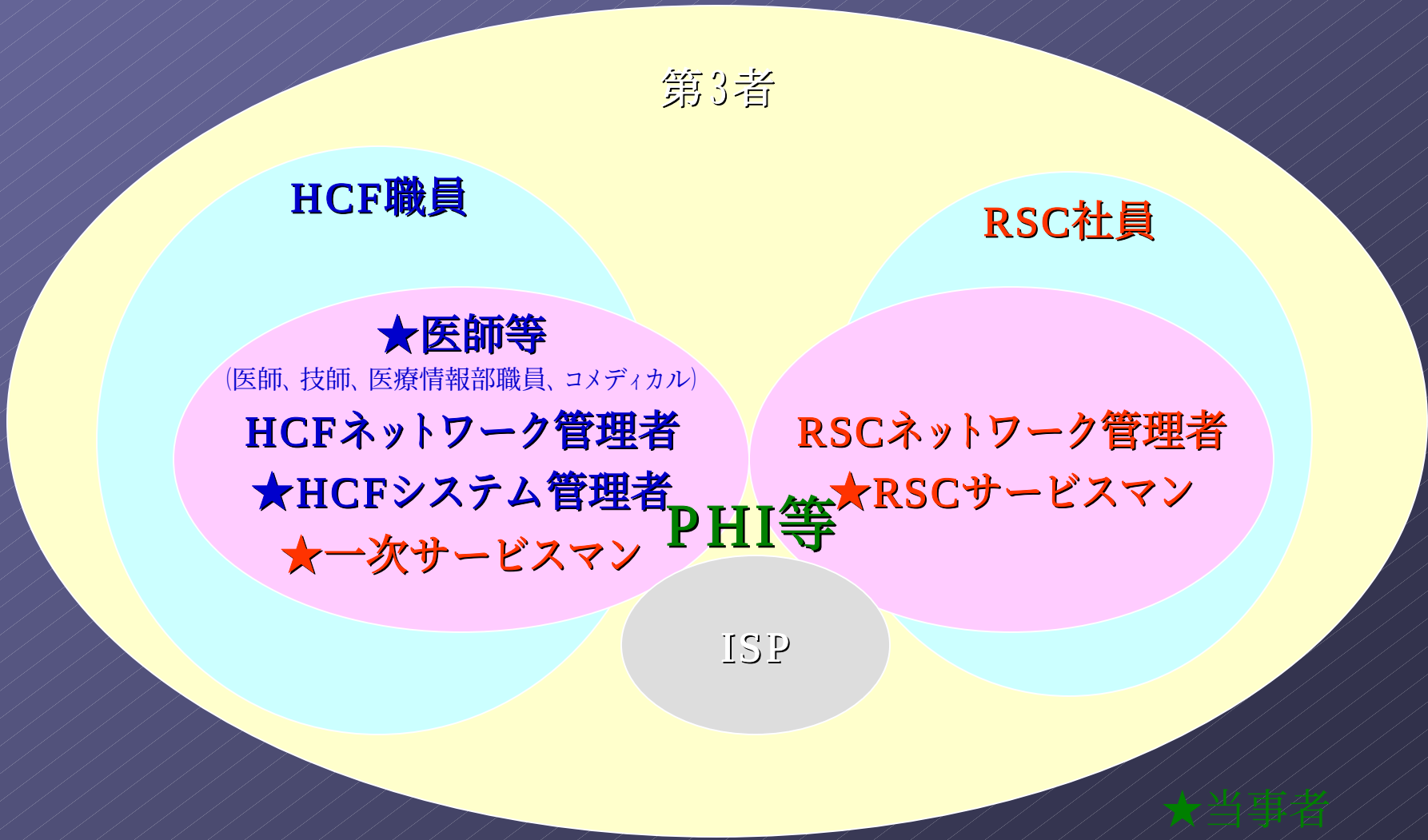
第5章 セキュリティ対策の策定

- セキュリティポリシ
- セキュリティ対策標準
- セキュリティポリシのマッピング
- ソリューションの選定
- 運用実施規定
- セキュリティ監査基準
- セキュリティ監査と監査証跡

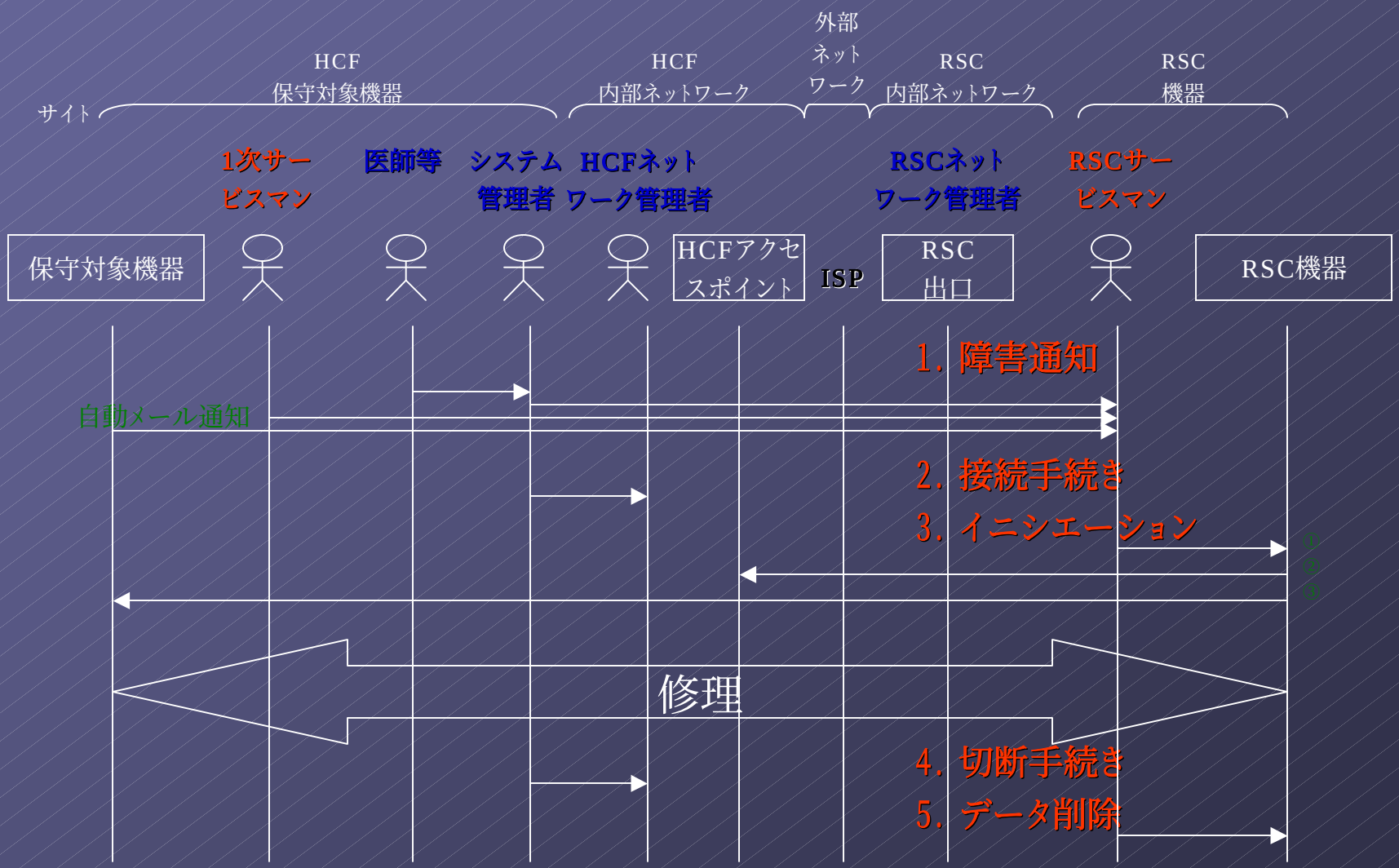
リモートサービスモデルのリスク分析

- 適切なセキュリティ対策の実施に必要
  - SPCガイドラインのモデル化
  - 情報セキュリティ上の脅威分析
  - 対策案の検討
  - 技術ソリューションの立案（検討中）
  - 個人情報保護法に対応したガイドライン作成

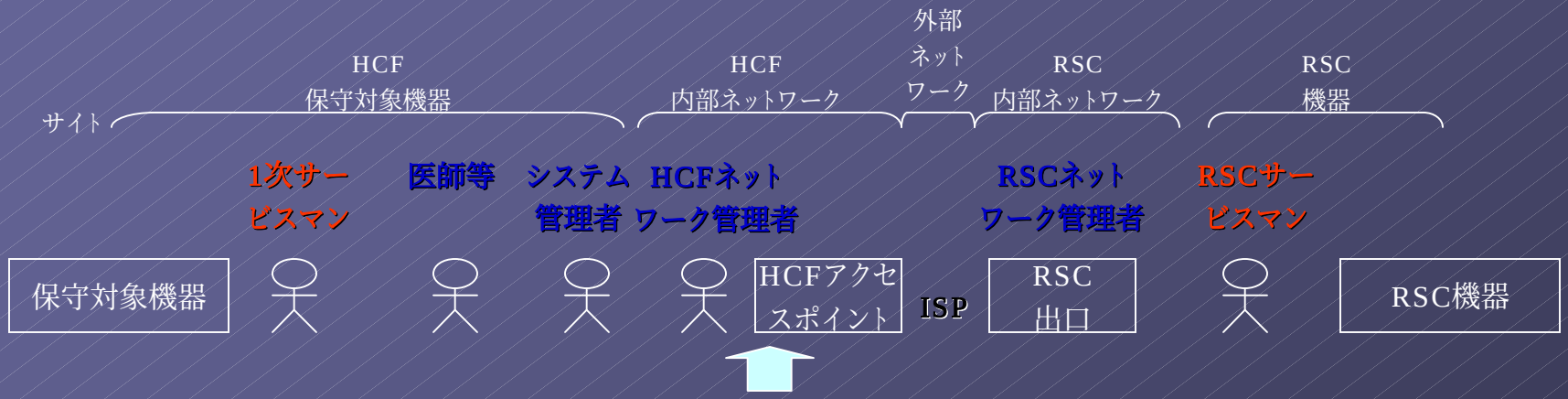
リモートサービスにおけるエンティティの関係



ユースケース(修理)


サイト
HCF
保守対象機器
HCF
内部ネットワーク
外部
ネット
ワーク
RSC
内部ネットワーク
RSC
機器
1次サー
ビスマン
医師等
システム
管理者
HCFネット
ワーク管理者
RSCネット
ワーク管理者
RSCサー
ビスマン
保守対象機器
HCFアクセ
スポイント
ISP
RSC
出口
RSC機器
1．障害通知
自動メール通知
2．接続手続き
3．イニシエーション
①
②
③
修理
4．切断手続き
5．データ削除

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。

リスク評価基準(脆弱性)

■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極めて脆弱である
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脆弱性が無視できる

■完全性

1	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
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する脆弱性が無視できる

■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して極めて脆弱である
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する脆弱性が無視できる

リスク評価基準(影響性、発生可能性)

■影響性

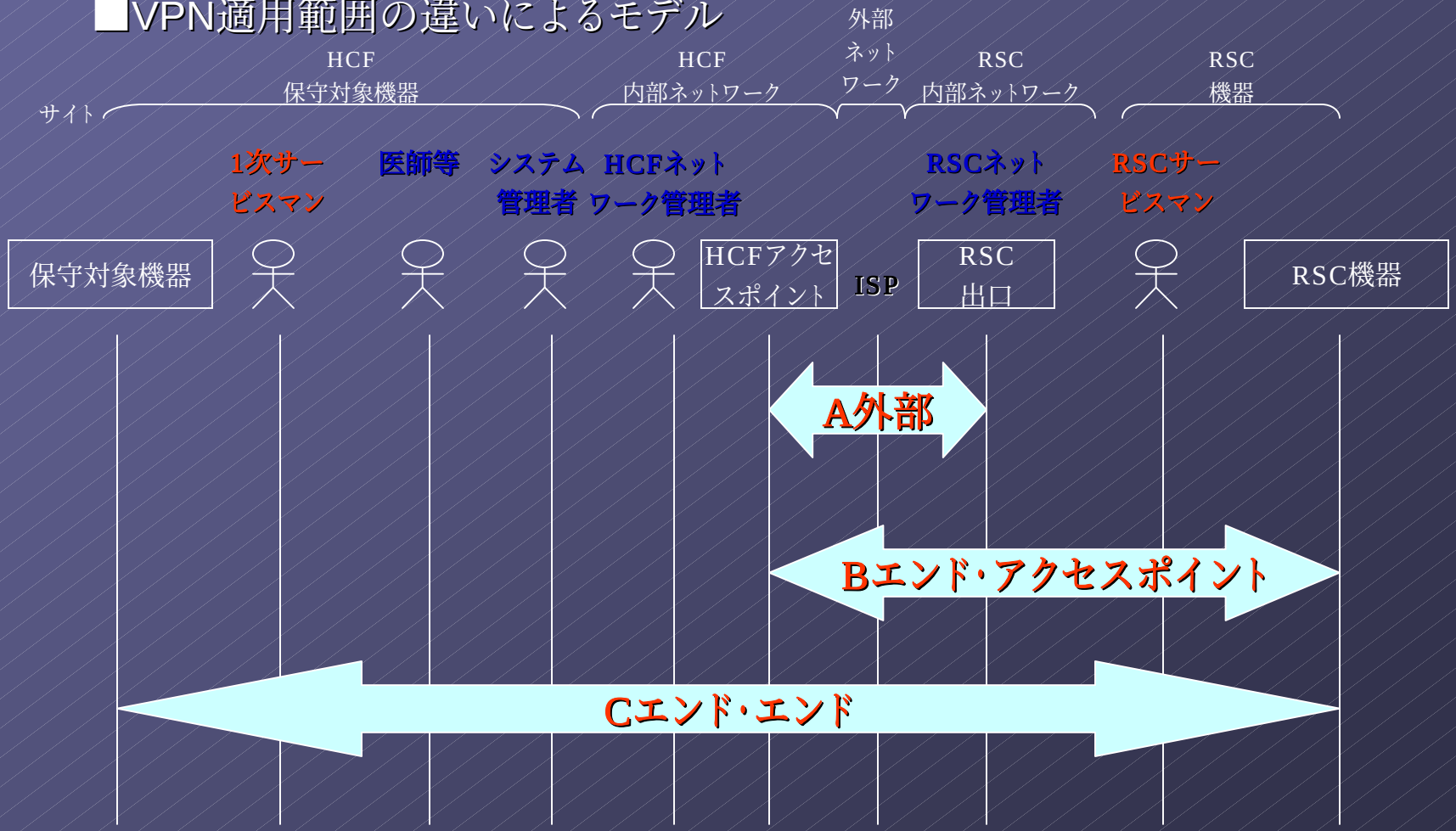
1	経営・業務遂行に重大な影響がでる可能性がある
2	経営・業務遂行に影響がでる可能性がある
3	経営・業務遂行に影響が無視できる

■発生可能性

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

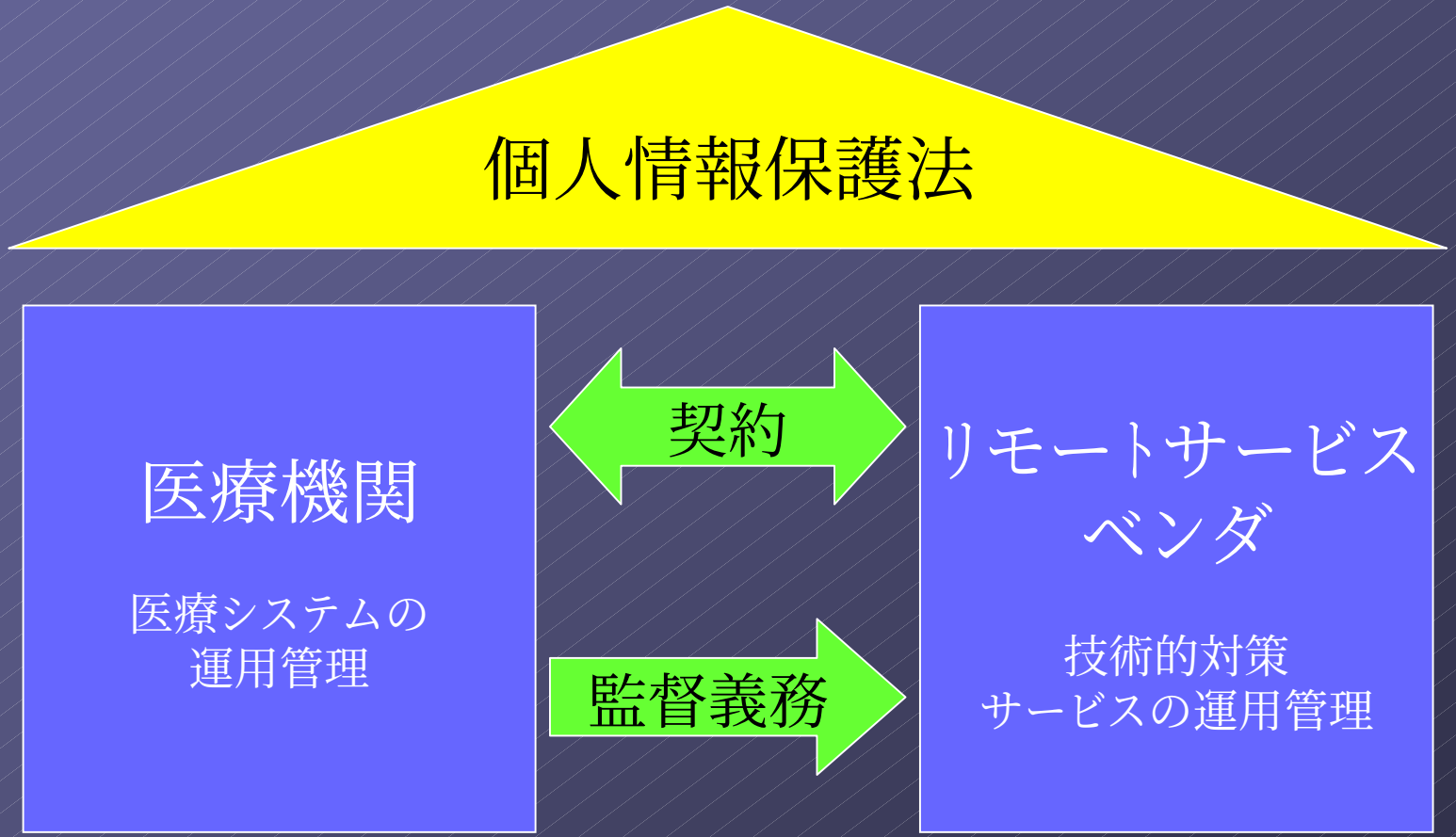
対策の検討（VPN）

■VPN適用範囲の違いによるモデル



注. 今回Cは対象外とする

医療機関とベンダの役割分担

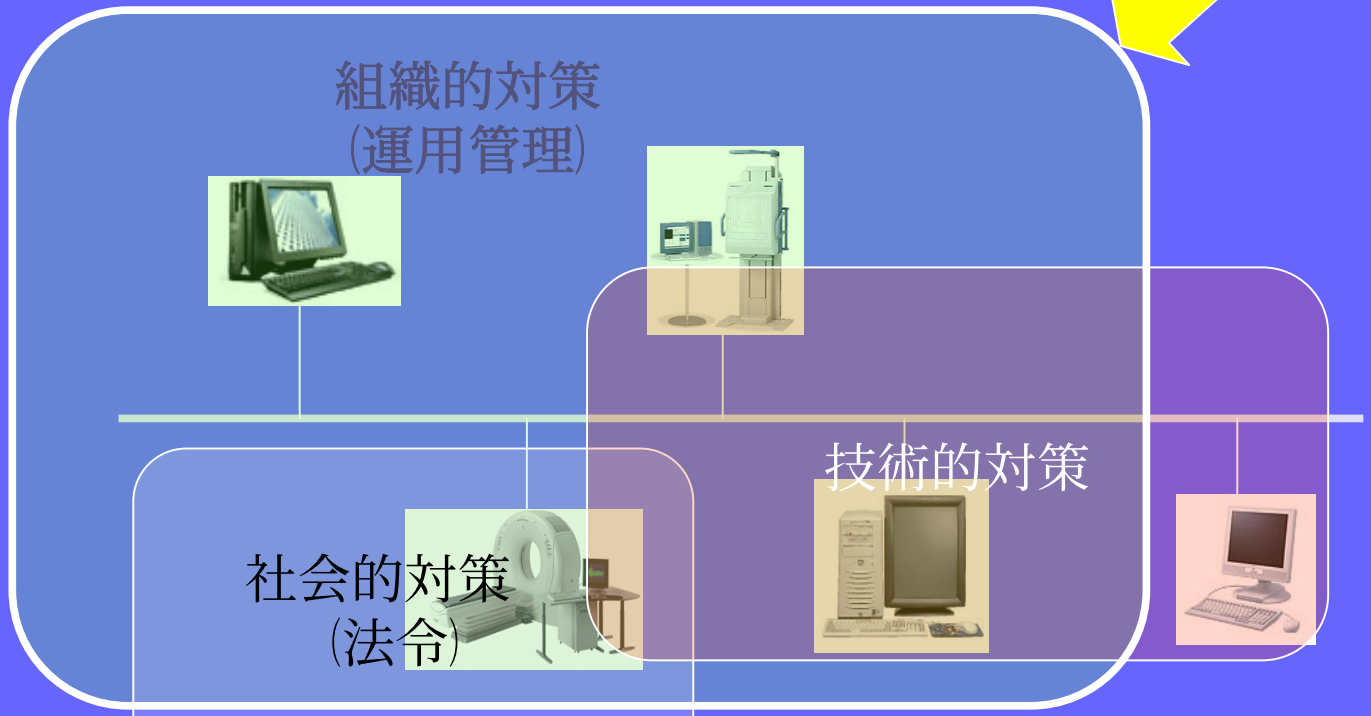


情報セキュリティ対策の考え方

医療機関の情報セキュリティ

セキュリティ
ポリシ

守るべき情報資産の範囲



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

セキュリティマネジメントの第三者認証

- プライバシーマーク制度
  - JIPDEC
  - MEDIS-DC
- ISMS認定制度
  - JIPDEC
- 情報セキュリティ監査制度
  - JASA

まとめ

- リモートサービスにおけるセキュリティ確保のためのガイドを作成した
  - http://www.jira-net.or.jp
  - http://www.jahis.jp
- サービスを提供するベンダ側の技術的対策だけでなくサービスを受ける医療施設側の運用による対策も重要である
- 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