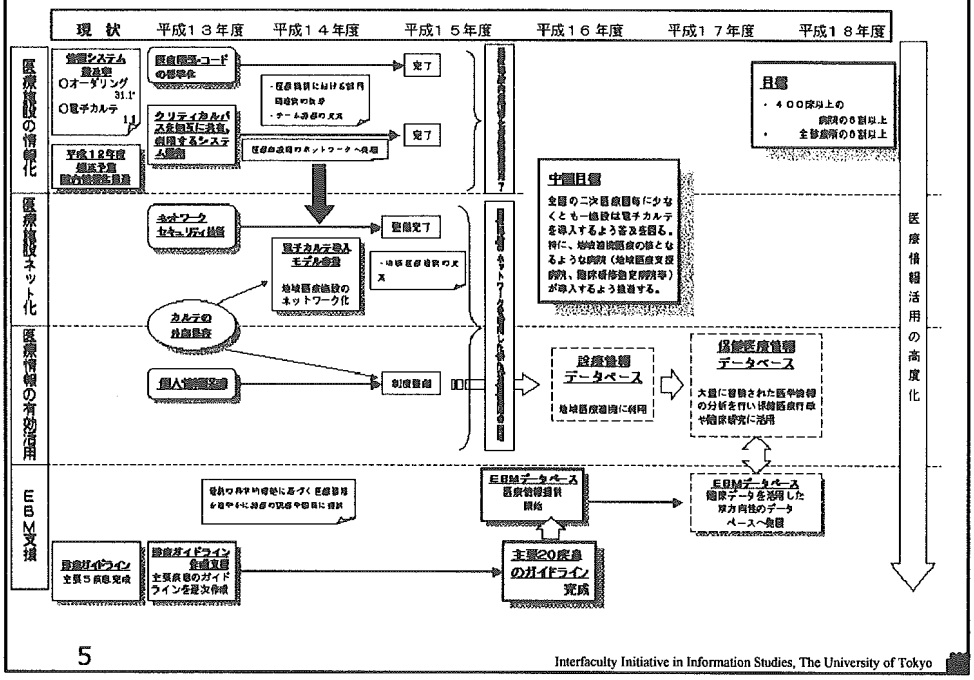


5

外部保存容認通知(H14. 4. 3)

- 原則は平成11年の電子保存と同じ
  - 真正性・見読性・保存性・プライバシー保護・自己責任・運用規程
- 事故等があった場合の責任の所在の明確化(契約等)
- オンライン電子保存は限定的
  - 個人情報保護法が未整備
  - 安全性の実証が必要
  - 見直しを明記
- 紙・フィルム媒体に関しては現状追認？

6

E-Japan 戦略II（平成15年）

e-Japan戦略 II

先導的取り組み（1）

1. 医　療

1. 急者基点の総合的医療サービス、継続的治療等

・超IT基盤整備、電子カルテのネットワーク転送・外部保存の容認（2005年まで）

2. 医療機関の経営効率と医療サービスの向上

・医療機関情報の国民への開示（第3者機関による審査）

3. 診療報酬請求業務の効率化

・診療報酬請求業務のオンライン化開始（2004年度から）、医療機関100%対応可能（2010年まで）
・電子レセプトを担保にした金融機関からの融資

2. 食

1. トレーサビリティシステムの構築による豊かで安心できる食生活の実現

・100%の国産牛について、BSE発生等における移動履歴の追跡体制の整備（2004年まで）
・100%の国産牛の豚肉（機肉・小間切を除く）の生産履歴情報を確認できる体制の整備（2005年まで）
・牛肉以外の食品について、その特性に応じたトレーサビリティシステムの開発
・日本発の安全な食品流通の仕組みの輸入食品への普及

2. 食品の取引の電子化、農林漁業経営のIT化による消費者利益の増大

・食品流通業者の半数が電子的取引を実現（2005年度まで）
・通関監視システム等の導入による農林漁業経営のIT化

3. 生　活

1. 温かく見守られている生活の実現、家庭でのサービスの選択肢拡大

・希望する高齢者単身世帯に通院ビデオ会話システムの導入等（2008年度まで）
・センサー等を通じた高齢者の在宅健康管理
・ガス、水道、電気等の通関検針（2005年まで）、希望する世帯に実施可能（2008年まで）
（メーターのコストダウンに係る規制緩和）
・家庭内電力線の高速通信への活用（実用上の問題がないことが確保されたもの）
・家庭内外のサービス等の相互連携や一括管理、全体最適化

2. 緊急時の通報・連絡システムの確立

・ITによる緊急通報の環境整備

3

7

行政手続き等における情報通信技術の利用に関する法律（2002. 12成立　2003.2施行）

- ＞ オンライン行政手続きに関する通則法
- ＞ オンライン申請を原則可とする。（包括法）
- ＞ 書類の電子的作成・保存・縦覧・閲覧

第六条　行政機関等は、作成等のうち当該作成等に関する他の法令の規定により書面等により行うこととしているものについては、当該法令の規定にかかわらず、主務省令で定めるところにより、書面等の作成等に代えて当該書面等に係る電磁的記録の作成等を行うことができる。

2　前項の規定により行われた作成等については、当該作成等を書面等により行うものとして規定した作成等に関する法令の規定に規定する書面等により行われたものとみなして、当該作成等に関する法令の規定を適用する。

3　第一項の場合において、行政機関等は、当該作成等に関する他の法令の規定により署名等をすることとしているものについては、当該法令の規定にかかわらず、氏名又は名称を明らかにする措置であって主務省令で定めるものをもって当該署名等に代えることができる。

8

E-Japan II 加速化パッケージ(2003)

- **e一文書イニシアティブ**
  法令により民間に保存が義務付けられている財務関係書類、税務関係書類等の文書・帳票のうち、電子的な保存が認められていないものについて、近年の情報技術の進展等を踏まえ、文書・帳票の内容、性格に応じた真実性・可視性等を確保しつつ、原則としてこれらの文書・帳票の電子保存が可能となるようにすることを、統一的な法律(通称「e-文書法」)の制定等により行うこととする。このため、電子保存の容認の要件、対象範囲等について早急にとりまとめ、2004年6月頃を目途にIT戦略本部に報告を行い、法案を早期に国会に提出する。(内閣官房及び関係府省)
- **診療情報の電子化など医療分野でのIT利用促進**
  医療の質の向上と効率的な医療提供体制の構築に向けて、処方せん、診断書、出生証明書をはじめとする様々な診療情報の電子化など医療分野のIT利用促進を図るための方策を包括的に検討し、2004年9月までに結論を得る。(厚生労働省)
- **電子的手段による資格保有等証明の推進**
  重要情報のオンライン転送にあたり、医師、弁護士等の本人性、資格保有等の証明を電子的にできるようにするため、既存認証制度に対する属性情報追加等のニーズ把握を早期に行うとともに、制度の在り方について検討し、2004年中に結論を得る。(内閣官房、総務省、法務省、経済産業省及び関係府省)

E一文書法(161国会提出)

- 通則法
  民間事業者が行う書面の保存等における情報通信の技術の利用に関する法律
- 整備法
  民間事業者が行う書面の保存等における情報通信の技術の利用に関する法律の実施に伴う関係法律の整備等に関する法律

E－文書法 （通則法案）

- 作成・保存等が義務付けられた文書を原則として電子的に作成し、電磁的に保存することを認める。
  書面で作成し、電磁的に保存することも可。
  署名・捺印も電子的な方法（電子署名）でOK。

- 主務省令で定めたものに限る。

- 診療録等の電子保存通知は電子的に作成したものを電磁的に保存することを認めたもの。
  署名捺印が法令で明記されたものは不可？

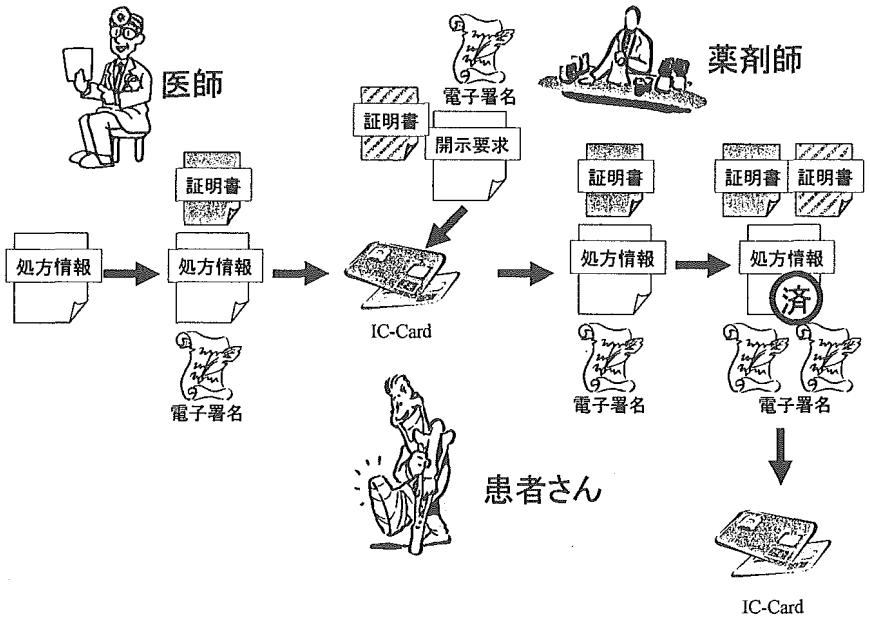
E－文書法厚労省令
（厚生労働省令第四十四号 2005.4）

- 電子的に作成・保存
- スキャナ等で電子化して保存

- 見読性（必ずしも印刷は必要ない）
- 真正性
- 保存性
- 記名・押印は電子署名で可
- 処方せん（院外）は除外
- 個人情報保護は法律・指針あるために記載なし

今後の医療情報ネットワーク基盤のあり方について
医療情報ネットワーク基盤最終報告

- Ⅰ はじめに
  - フリーアクセスを担保し、情報セキュリティの確保及び個人情報保護を前提とした情報伝送の技術的及び運用管理上の基盤が必要
- Ⅱ 医療における公開鍵基盤について
  - 電子署名法に適合した電子署名
  - 国際的標準を念頭に置いたヘルスケアPKI認証局開設を目指す
  - 医療の公的資格台帳の電子化とICカードによる資格認証
- Ⅲ 医療に係る文書の電子化
  - 放射線の照射録、臨床修練外国医師の診療録、及び様々な制度下に交付・運用される診断書等は電子署名で可
  - 処方箋は現状では不可であるが、処方情報の電子化を進める
  - E－文書法への対応
- Ⅳ 医療に係る文書の電子保存
  - ガイドライン等の見直し(わかりやすく、個人情報保護法に対応)
  - オンライン外部保存に、公的機関等を追加
- Ⅴ おわりに



Ⅲ 医療に係る文書の電子化 1

> 電子保存対象外であった文書
放射線照射録、診療情報提供書等
署名捺印が法令で明記されている文書
→ 電子署名法に適合した電子署名で可

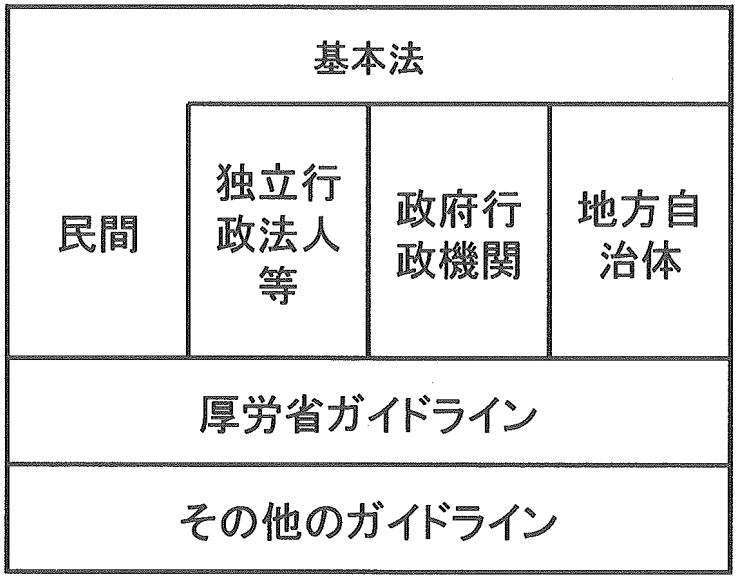
> 処方箋(院外処方箋)
プレーヤーが3者(医師、薬剤師、患者)
フリーアクセスの保障
無診療投薬の防止
→ 現状では不可
処方情報の電子化と電子的流通を促進
環境の整備を進める

Ⅲ 医療に係る文書の電子化 2
(E一文書法への対応)

> 都度発生する書面(フィルム)のスキャン
原則は可。
技術的に診療に差し支えない精度。
文書は300DPI フルカラースキャナ
日本医学放射線学会電子情報委員会の指針
電子署名による責任の所在の明確化。

> すでに蓄積された書面(フィルム)のスキャン
原則は不可。
技術的に診療に差し支えない精度。
電子署名等による責任の所在の明確化。
計画から監査まで第三者監査に相当する
厳格な監視。

個人情報保護法



17

Ⅲ　医療・介護事業者の責務

> 安全管理・従業者の監督

- 組織的、人的、物理的、および技術的安全管理措置。
- リスクに応じ、必要かつ適切な措置。
- 従業者には理事や派遣労働者を含む。
- 規定の整備と公表。
- 組織体制の整備（CPO，委員会）。
- 一定期間毎の監査。（必要に応じて外部監査）
- 問題発生時の報告連絡体制。苦情処理との連携。
- 雇用契約、就業規則での個人情報保護規定の整備。
- 派遣労働者を含めて教育研修の実施。
- 入退室管理、盗難の予防、機器・装置の物理的保護。
- アクセス管理、アクセス記録の保存、ファイアウォール。
- 媒体劣化の防止、検索可能性の維持。
- 不要な場合の復元不可能な破棄（機器も含む）。
- 医療情報システムに関しては別に指針を定める。

18

医療情報システムの安全管理のためのガイドライン

- 平成11年の電子保存ガイドライン、平成14年の外部保存ガイドラインのいずれもが技術ニュートラルにこだわったためにわかりにくかった。(医療ネットワーク基盤検討会最終報告 2004年9月)

  トレンドの技術にも触れて理解しやすいものに

- 個人情報保護法実施のために安全管理指針が必要(2004年12月)
- E-文書法で通知から法律になり、また要件が追加された。(厚生省令 2005年3月)

医療情報システムの安全管理のためのガイドライン

- 1. はじめに
- 2. 本ガイドラインの読み方
- 3. 本ガイドラインの対象システムおよび対象情報
- 4. 自己責任について
- 5. 情報の相互利用性と標準化について
- 6. 医療情報システムの基本的な安全管理
- 7. 電子保存の要求事項について
  真正性、見読性、保存性、電子署名
- 8. 診療録および診療諸記録を外部の保存する際の基準
- 9. 診療諸記録をスキャナ等で電子化して保存する場合について
- 10. 運用管理について
- 付表1. 一般管理における運用管理の実施項目例
- 付表2. 電子保存における運用管理の実施項目例
- 付表3. 外部保存における運用管理の実施項目例

医療情報システムの安全管理のためのガイドライン

> 対象は患者情報を扱う全システム
1～6章 ＋ 10章(付表)

> 電子保存を行う場合は
7章 ＋ 10章(付表)

> 外部保存を行う場合は
8章 ＋ 10章(付表)

> スキャナ／デジタイザによる電子化
9章 ＋ 10章(付表)

構成

> A. 制度上の要求事項
法律・通知・他の指針など

> B. 考え方
要求事項の解説および原則的な対策

> C. 最低限のガイドライン
Aの要求事項を満たすためにかならず実施しなければならない事項

> D. 推奨されるガイドライン
実施しなくても要求事項を満たすことはできるが、説明責任の観点から実施したほうが理解が得やすい対策

6. 医療情報システムの基本的な安全管理

> A. 個人情報保護法
　方針の制定、情報の把握、リスク分析
> 組織的安全管理対策
　B. ーー、C. ーー、D. ーー
> 物理的安全管理対策
　B. ーー、C. ーー、D. ーー
> 技術的安全管理対策
　B. ーー、C. ーー、D. ーー
> 人的安全管理対策
　B. ーー、C. ーー、D. ーー

技術的安全対策

> B.　考え方
　(1)利用者の識別および認証
　・認証強度の考え方
　・ICカード等のセキュリティ・デバイスを配布する場合の留意点
　・バイオメトリックスを利用する場合の留意点
　(2)情報の区分管理とアクセス権限の管理
　(3)アクセスの記録
　(4)不正ソフトウエア対策

技術的安全対策

- C.　最低限のガイドライン
  - (1)利用者の識別および認証
  - (2)動作確認等での漏洩への留意
  - (3)職種による権限の設定とアクセス管理
  - (4)アクセスの記録と定期的な確認
  - (5)時刻情報の要件
  - (6)ウイルスなどの不正ソフトウエア対策
- D.　推奨されるガイドライン
  - (1)情報の区分管理、区分単位でのアクセス管理
  - (2)ウイルスなどの不正ソフトウエアの対策の実効性の確認
  - (3)離席の場合のクローズ処理

6　情報システムの基本的な安全管理

- 6．1　方針の制定と公表
- 6．2　情報の取り扱いの把握とリスク分析
- 6．3　組織的安全管理
- 6．4　物理的安全管理
- 6．5　技術的安全管理
- 6．6　人的安全管理
- 6．7　情報の破棄
- 6．8　情報システムの改造と保守
- 6．9　外部と個人情報を含む医療情報を交換する場合の安全管理

7 電子保存(E-文書法)の要求事項について

- 7．1 真正性の確保
- 7．2 見読性の確保
- 7．3 保存性の確保
- 7．4 法令で定められた記名・押印を電子署名で行うことについて

8 診療録および診療諸記録を外部に保存する際の基準

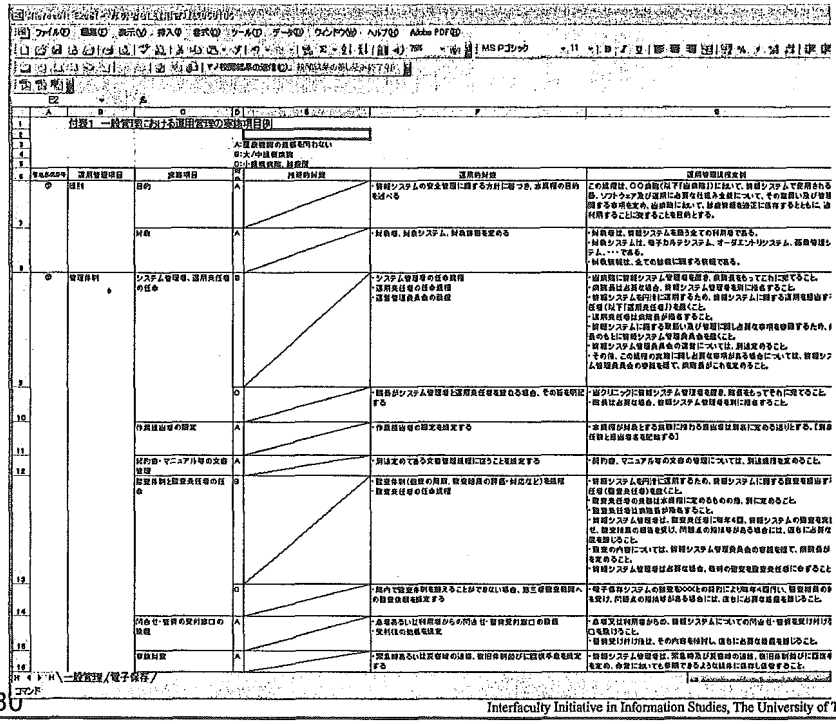
- 8．1 電子媒体による外部保存をネットワークを通じて行う場合
- 8．2 電子媒体による外部保存を可搬型媒体を用いて行う場合
- 8．3 紙媒体のままで外部保存を行う場合
- 8．4 外部保存全般の留意事項について
- 8．5 外部保存契約終了時の処理について
- 8．6 保存義務のない診療録等の外部保存について

9 E文書法への対応(スキャナによる電子化)

> 都度発生する書面(フィルム)のスキャン
- 技術的に診療に差し支えない精度。
  - 文書は300DPI フルカラースキャナ
  - 日本医学放射線学会電子情報委員会の指針
- 電子署名による責任の所在の明確化。

> すでに蓄積された書面(フィルム)のスキャン
- 技術的に診療に差し支えない精度。(同上)
- 電子署名等による責任の所在の明確化。
- 計画から監査まで第三者監査に相当する厳格な監視。

> 第三者監査に相当する監視?
- システム監査技術者、Certified Information System Auditor (ISACA認定)等による外部監査


付表1 一般管理における運用管理の実施項目例

付表

- 1. 運用管理項目
  安全管理上の要求事項で多少とも運用的対策が必要な項目
- 2. 実施項目
  上記管理項目を実施レベルに細分化したもの
- 3. 対象
  医療機関の規模の目安
- 4. 技術的対策
  技術的に可能な対策、ひとつの実施項目に対して選択可能な対策を列挙した
- 5. 運用的対策
  4. の技術的対策をおこなった場合に必要な運用的対策の要約
- 6. 運用管理規程文例
  運用的対策を規定に記載する場合の文例

電子署名法に準拠した電子署名

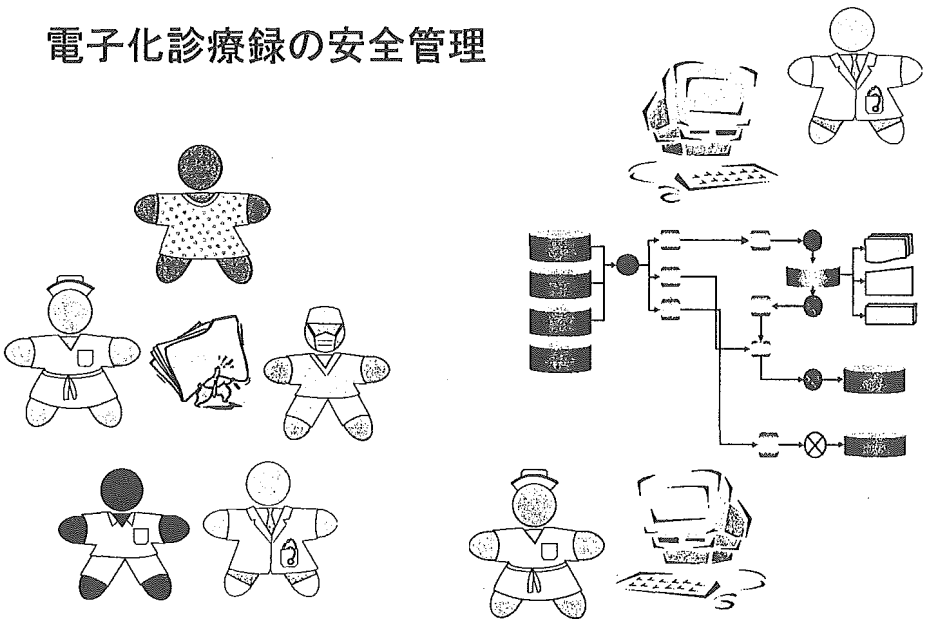
- 7. 4および9
- 単に真正性を確保する目的の署名は対象外
- 認定特定認証事業者等の発行する電子証明書を用いて署名
  公的個人認証サービスは注意が必要
- タイムスタンプ（日本データ通信協会認定）
- タイムスタンプ時点で有効な電子証明書を用いること。

電子化医療情報の安全管理

> 機密性・可用性・完全性

> 個人の情報だが、高度の安全管理が必要
> 責任の所在が重要　だれがどの資格で・・
> アクセス権が動的に変化する
> 医療従事者の特殊なメンタリティ
　　個人の責任意識がきわめて強い
　　組織の影響力は弱い？
> 高度の可用性が最優先される

電子化診療録の安全管理



6 情報システムの基本的な安全管理

- 6.1 方針の制定と公表
- 6.2 情報の取り扱いの把握とリスク分析
- 6.3 組織的安全管理
- 6.4 物理的安全管理
- 6.5 技術的安全管理
- 6.6 人的安全管理
- 6.7 情報の破棄
- 6.8 情報システムの改造と保守
- 6.9 外部と個人情報を含む医療情報を交換する場合の安全管理

6.1 方針の制定と公表

- 個人情報保護方針の一部として必要

6．2 情報の取り扱いの把握とリスク分析

> すべてリストアップ
> 分類（場所、管理形態、重要度）
> リスク分析
  想定される脅威
  とられている対策
  残存脅威
  脅威が現実化した場合の損害

6．3 組織的安全管理

> 責任者・担当者の明確化
> 規定の整備
  入退管理
  アクセス管理
  業務委託
  個人情報記録媒体
  脅威が発見された場合の対処

6．4　物理的安全管理

> 保存場所の適切な施錠と入退室管理
> 入出力可能な区画の管理（施錠・監視）
> 盗難防止対策（チェーン固定等）
> 離席時の対策

> D:防犯カメラ、自動侵入監視装置

6．5　技術的安全管理　1

> 利用者識別と認証

ID + Password
- 推奨されない

ICカード等
- PINコードと併用、破損時などの緊急アクセスに配慮

Biometrics
- 1対1照合で用いること。
  他の方法との組み合わせが有効

> 動作確認時の漏洩に注意
> アクセス権限の管理

職種による権限管理等

6．5　技術的安全管理　2

> アクセスログの記録と定期的確認
　時刻、利用者、対象となる患者を記録すること
> アクセスログに用いる時刻は信頼できること

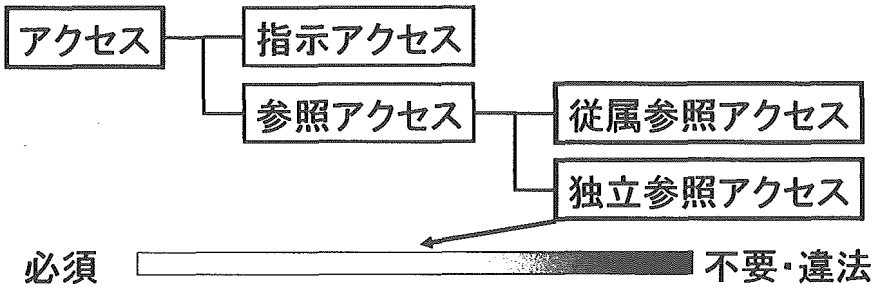
サンプリング検査

VIP、職員関係者、事件性・・・・

全数検査

ログと監査

> セキュリティの基本は認証とログ監査
> 東大病院のログ
　利用者のアクションごとに1レコード
　→　300万レコード　／　月



当該患者と利用者の関連性を追跡可能にすることが必要

6.5 技術的安全管理 3

- 不正ソフト(ウイルス等)対策
  - システム構築時
  - メディア使用
  - ネットワーク
- パスワード管理(推奨されないが・・・)
  - システム内で暗号化されていること
  - パスワード発行する場合の本人確認
  - 利用者のパスワードが類推できないこと
  - パスワードは最長でも2ヶ月以内に変更
  - 8バイト以上の可変長文字列
  - 類推しやすい文字列の使用禁止

6.5 技術的安全管理 D

- 情報の区分管理と区分毎のアクセス制御
- 詳細なアクセスログの記録と監査
- 常時不正ソフトの侵入を防止
- 離籍時のクローズ処理
- ファイアウォール
  - ステートフルインスペクション
  - ACL管理
- パスワードインターフェイス
  - 連続チャレンジの防止
- 認証方法の複数組み合わせ推奨