医療情報ネットワーク基盤検討会

検討状況の中間とりまとめ

（文中で使用した用語の補足解説）

※この解説は、医療情報学等における学術的な正確さというよりは、報告の文脈上に位置づけられた該当する用語の意味・意義等を理解するための補足的な内容となっていますので、ご了知下さい。

項目		用語	用語の解説
I. 検討の経緯と基本姿勢 1.背景と現状	1-1	医療情報	医療では幅広い多様な情報が取り扱われているが、医療の提供者に関する情報（医療機関の情報など）、診療に関する情報（個々の患者の診療記録など）、医学知識等（疾患の情報など）に大別できる。本中間取りまとめでは、主として、情報通信技術によるネットワークを通じて交換される、医療施設等が保有する検査、診断、治療に関連した情報を指している。
	1-2	ファイアウオール	インターネットから特定のシステムへのアクセス、および特定のシステムからインターネットへのアクセスを制限する仕組みで、不正な侵入や意図しない情報の流出を防止するもの。
	1-3	改ざん	悪意を持って、または責任を明確にせずに情報を書き換えること。
	1-4	なりすまし	情報ネットワーク利用者のパスワードを本人の許可を得ないで使用することなどにより、ネットワーク上でその利用者本人のふりをすることであり、情報を盗み見たり、悪用をすることにより利用者本人に責任が及ぶことがある。
	1-5	暗号化	情報ネットワークを通じて電子化されたデータ（文書、画像など）のをやり取りする際に、その途中で第三者にデータを盗み見られたり改ざんされたりすることを防止するため、正当な利用者だけが元に戻すことができる一定の規則に従ってデータを変換すること。
	1-6	電子署名	電子的に記録された文書について、押印のようにその作成者が内容に対して責任の所在を示す目的で行われる暗号化等による措置であって、その文書の改変の有無を確認できるものをいう。現在一般に用いられているのは公開鍵暗号を用いたデジタル署名で、署名者は私有の秘密鍵を用いて文書のダイジェストを暗号化した署名を文書と一緒に送り、受取者は署名者の公開された鍵を用いて署名を復号し内容の真正性を確認することで、第三者による改ざん等を防いだり、署名者が確かに文書作成者であることの証明に用いることができる。
	1-7	認証基盤	情報ネットワーク上において、受信側から見て送信側が本当に本人であるか、医師などの公的資格を有しているか等を電子的に確認し、認証する仕組みのこと。
I. 検討の経緯と基本姿勢 2.本検討会における検討状況と基本姿勢	2-1	電子署名及び認証業務に関する法律	通称、電子署名法。電子商取引等の情報ネットワークを通じた社会経済活動の円滑化を図ることを目的として平成12年5月に成立。電子文書等は、本人による一定の電子署名が行われているときは、手書き署名や押印と同等とし、真正に成立したものと推定できるとした。また、認証業務（電子署名が本人のものであることを証明する業務）のうち、法律で定める一定の基準（本人確認方法等）を満たす業務を主務大臣（総務大臣、法務大臣、経済産業大臣）が認定でき、認定を受けた業務のその旨の表示ができるほか、認定の要件、認定を受けた者の義務等を定めている。さらに、主務大臣は、認証業務の認定に際して、認定の基準に適合していることを確認するために実地の調査を指定調査機関に行わせることができる。

	2-2	公開鍵基盤(PKI) (Public key Infrastructure)	公開鍵暗号を用いて、ネットワーク上で電子署名、認証、タイムスタンプ、暗号化等の安全対策を行うためのシステムの総称で、電子的な印鑑証明書に相当する公開鍵証明書の形式とその運用システムが中心である。
	2-3	ベンダー(またはベンダ)	情報関連のシステム製品(ハードウエアやソフトウエア)を販売するに際して、その製品やシステム動作等を保証するメーカーや販売会社を指す。
Ⅱ.医療における公開鍵基盤(Public Key Infrastructure:PKI)のあり方の検討状況	Ⅱ 1-1	公的個人認証サービス	行政手続をオンラインにて行うための情報ネットワーク上の課題(成りすまし、改ざん、送信否認など)を解決するための本人確認サービスを、全国どこに住んでいる人に対しても安い費用で提供する、電子政府・電子自治体の基盤であり、従来、窓口に出向く必要があった行政手続を、家庭や職場からインターネットで可能とするためのサービス。
	1-2	ISO/TS 17090	ISOの技術委員会215のワーキンググループ4(セキュリティ領域)で準備された技術仕様書(Technical Specification)であり、医療情報分野の公開鍵基盤を対象とするもの。
	1-3	hcRole	公開鍵証明書の特別な拡張項目として、保健医療分野での資格属性を指定する目的で定義したもの。
	1-4	証明書ポリシ	公開鍵基盤において、認証局、証明書等を設計、運用するための基本方針や規則を記載した文書。
Ⅲ.医療に係る文書の電子化についての検討状況	Ⅲ 1-1	ICカード	プラスチック・カードにIC(Integrated Circuit)を埋め込んだ情報記憶媒体。従来の磁気カードに比べて、記憶容量が大きく、セキュリティが確保できる。今後は、データカードとしての用途よりはネットワーク上での認証カードとしての機能が期待されており、住基カードなどで使われている高機能かつ多機能なICカードは、数ミリ角のICチップに、CPU(中央演算装置)、プログラム、データ記録メモリなどが組み込まれており、安全な超小型パソコンとも言うことができる。セキュリティ確保に必須な暗号処理をカード内部で実施すること、暗号鍵はカードから取り出せないこと、接続するコンピュータを相互に確認できること等により、安全性が高い。
	1-2	電子タグ	一般的には極小のICチップを埋め込んだ電子荷札のことを指し、内部に格納されたアンテナによって、情報読み取り及び書き込み用装置と無線でやり取りすることができる。
Ⅳ.医療に係る文書の電子保存についての検討状況 2.紙文書のスキャナーによる電子保存について	Ⅳ 2-1	スキャナー	紙媒体に書かれた図形や文字、または写真を読み取り、画像(イメージ)データとしてパーソナルコンピュータなどに転送する装置。
	2-2	タイムスタンプ	事柄の発生時刻を証明するためのタイムスタンプ発行機関による署名付き時刻証明書のこと。