厚生科学研究研究費補助金

厚生科学特別研究事業

医療分野における個人情報保護のあり方に関する研究

平成１２年度　総括・分担研究報告書

主任研究者　　開原　成允

平成１３年３月

目　　次

平成１２年度厚生科学研究費補助金（特別研究事業）

総括研究報告書

医療分野における個人情報保護ガイドライン作成に関する研究

主任研究者　　開原成允　医療情報システム開発センター理事長

研究要旨　現在日本においても個人情報保護法が成立しようとしているが、それに伴って医療分野においてもこの法案を充たす形のガイドラインの作成が急務となっている。一方米国においてもHealth Insurance Portability and Accountability Act (HIPAA) が1996年に成立し、現在それを受けた形でのガイドラインが作成された。この個人情報保護ガイドラインは日本におけるガイドラインを作成する上で大きな参考となるため、ＨＩＰＡＡを研究すると共に、日本のガイドラインについて研究し、その第一次案を作成した。

分担研究者

大江和彦	東大医学部	教　授
樋口範雄	東大法学部	教　授
山本隆一	大阪医科大学	助教授
桐生康生	MEDIS　研究開発部第２課長	

Ａ．研究の目的

高度情報通信社会の急速な進展、米国HIPAA法の動向等から医療情報分野での個人情報保護のあり方に関して、国際動向や現在のセキュリティ技術水準を踏まえた一定の方向性を示すことが緊急かつ重大な課題となっている。そして、我が国における個人情報保護法制定の動向を鑑みると、今年度中にガイドラインをまとめる必要がある。

Ｂ．研究方法

研究は、次の三つの方向で行った。第一は、米国において検討されているＨＩＰＡＡ法のガイドラインを研究し、日本における適用性を検討することである。

また、第二は、日本で成立しようとしている個人情報保護法を日本の医療に適用した場合の問題点について検討することである。

そして第三に、これらの検討を経て日本における医療における個人情報保護のガイドラインを作成することである。

ここでいうガイドラインは、診療の場面におけるガイドラインを想定しており、医学研究、検診などの保健分野、また福祉分野における個人情報保護の問題は含まない。

（１）個人情報保護法制定に関する現状及び問題点に関する調査

「我が国における個人情報保護システムの在り方について（中間報告）」（平成１１年１１月、高度情報通信社会推進本部個人情報保護検討部会）、「個人情報保護基本法制に関する大綱案」（平成１２年９月、ＩＴ戦略本部個人情報保護法制化専門委員会）、厚生科学審議会先端医療技術部会「疫学的手法を用いた研究等における個人情報のあり方に関する専門委員会」等を基に、医療分野、特に実地の臨床の中での個人情報保護の現状やセキュリティ技術・個人情報保護対策の現状等を概括するとともに、問題点を整理する。

（２）米国HIPAA法に関する動向調査

米国HIPAA法の概要、セキュリティ及び個人情報保護の基準等について調査を行う。必要に応じて米国で調査を行うとともに、重要文献を翻訳する。

（３）個人情報保護に関するガイドラインの作成

（１）、（２）を基に、医療分野、特に実地の臨床の中での個人情報保護に関するガイドラインを作成する。

C．研究結果及び　D．考察

第一のＨＩＰＡＡについては、ＨＩＰＡＡ法が成立した背景を考察すると共に、その中のセキュリティのガイドライン及び個人情報保護のガイドラインの主要な部分について考察した。

ＨＩＰＡＡとは、Health Insurance Portability and Accountability Act の略称で、1996 年に成立した連邦法である。この法律は、医療の枠組みを変えるようなものではないが、実務的には、米国の医療に大きな影響があると考えられている。

この法律ができた経緯は、色々な背景があるが、最も直接的には、医療保険が乱立し、被保険者が退職して別の企業に移った場合に、医療保険が使えなくなることであり、これがPortability の意味である。このため、医療保険のデータの形式や診療コードなどを全国的に標準化して、その間の移動を可能にするようにすることとなった。また、最近のＩＴを最大に利用し、保険請求もコンピュータの利用を前提として、システムを構築することとしたのである。

しかし、コンピュータを利用するとなると、個人情報保護の問題と交換時のセキュリティが問題になる。このため、この問題も一緒に扱うこととなった。

米国政府（ＤＨＨＳ）は Administrative Simplification という名前の組織を設け、ここが中心になって「Standard（基準)」と呼ばれる文書を作りはじめた。「基準」には、大きく分ければ、電子的データ交換、セキュリティ、個人情報保護の三つがあり、この他に実際に使われるコード表などが指定された。現段階では、電子的データ交換と個人情報保護の基準が完成している。因みに、この法律が実施されるのは、２００３年ということになっている。

今回の研究と直接関係ないので、本研究では「データ交換の基準」については述べないが、関係あるため、ここに簡単にその概要を記すと、これは、米国医師会、医療保険業界、学会、産業界が協力して作成した。この中では、保険機関コード、薬剤コード、検査コード、病名、医学用語などの他に、交換様式も定められており、それをどのような機関がどのように改訂していくかについても、きちんと定められている。また、これ以外のコードなどを使ってはならないという罰則規定まであるから、この法律が施行された時には、医療機関や保険者の間で診療情報が電子的に交換できることになる。

個人情報保護の基準は、診療から研究まで、さまざまな場合の規則が詳細に定められている。この中では、単に禁止するのみでなく、どういう場合には患者の了解を得ないで診療情報を使ってもよいかということもきちんと書かれている。

これらのガイドラインは、日本と米国という社会事情が異なっている中にあっても、十分参考になる内容を含むものであることが明らかになった。

また、個人情報保護法に関する考察は、現在の診療の現場にこれをそのまま適用した場合には多くの混乱を招く恐れがあることが明らかとなり、至急医療特有のガイドラインが必要であることが明らかとなった。

これに基づいて、ガイドラインの第一次案を作成したが、これはまだ十分な検討を経たものではなく、今後議論を続ける中で、できるだけ早い時期にガイドラインの原案を発表する必要がある。

E　結論

個人情報保護のガイドラインの作成を急いで行う必要があり、その作成の上には、米国のＨＩＰＡＡ法のガイドラインが参考になることが明らかになった。

その成果を参考にして、ガイドラインの第一次案を作成した。

平成１２年度厚生科学研究費補助金（特別研究事業）

分担研究報告書

米国における個人情報保護の動向　－　HIPAA法の概要

分担研究者　　樋口範雄（東京大学法学部）

研究要旨　　米国で１９９６年に成立したＨＩＰＡＡ法の意義について考察し、またその後、この法案の要請によって成立した個人情報保護のガイドラインを日本の診療との関連において考察した。

A.研究目的

米国で１９９６年に成立したＨＩＰＡＡ法（Health Insurance Portability and Accountability Act）は我が国の医療における個人情報保護の問題を考える上で参考になるので、その成立の背景などについて調査・研究することが本研究の目的であった。

B.研究方法

インターネット上で本法律に関する様々な意見を収集し、考察を加えた。

C.研究結果及びD.考察

1　HIPAA法の法的背景

①　アメリカにおける連邦制度の意義

HIPAA法（Health Insurance Portability and Accountability Act）の法的意義を理解するためには、アメリカにおける連邦制度の意義を知る必要がある。

この点で、最近の２つのアメリカ最高裁判決は示唆に富む。

第１は、１９９５年のロペス判決である（United States v. Lopez, 514 U.S. 549 (1995)）。この事件では、小中高校の周囲３００メートルの範囲内に銃器を持ち込むことを連邦犯罪として抑えようとした連邦法が違憲とされた。第２は、家庭内暴力の抑制を図ろうとした連邦法が問題とされた２０００年のモリソン判決である（United States v. Morrison, 120 S.Ct. 1740 (2000)）。ここでも、連邦最高裁は、連邦議会の作った法律を違憲とした。

いずれの事件でも、連邦最高裁は、法律の内容を問題としたのではない。連邦議会の法律制定権を問題としたのである。アメリカ合衆国憲法の第１編は、「この憲法によって認められるすべての立法権は連邦議会に属する（All legislative powers herein granted shall be vested in a Congress of the United States）」との規定で始まる。これを、わが国の憲法４１条、「国会は、国権の最高機関であって、国の唯一の立法機関である」と比べると、アメリカ憲法には、「この憲法によって認められる」、英語でいえば「herein granted」という明示的な制約が付けられている点で、大きな相違のあることに気づく。

要するに、アメリカの連邦議会は、何でも立法できる機関ではなく、アメリカ連邦憲法が認めた事柄しか立法できないということである。では、特に認められた事柄が憲法のどこに規定されているかといえば、主要な規定は、合衆国憲法第１編第８節であり、そこには、貨幣鋳造や関税その他の徴税、あるいは郵便制度や特許権に関わる事柄など１８項目が並べられている。このうち、最も汎用性の高い条項は、州際通商条項(interstate commerce clause)だとされ、州境を越える通商については連邦政府の規制権が認められてきた。

前記の２つの判決が問題とした家庭内暴力の抑制のための法律や学校近辺での銃器規制法も、この州際通商に関係するという名目で制定されたのだが、それはほとんど関係のない事柄であり、したがって、連邦議会は制定権限のない法律を作ったことになるとして違憲無効とされて

しまったのである。同様の内容の法律を作るとすれば、連邦議会ではなく、州の議会で作ることになる。

憲法第１編８節の１８項目の中に、家族に関することや子どもの安全に関わることという規定があれば、そもそも何ら問題はなかったはずである。だが、アメリカでは、これらは伝統的に州の権限とされており、憲法にはこれらの事項への言及はない。同じことが医療の場面にも当てはまる。やはり１８項目の中に医療に直接関連する規定はなく、医療問題も、伝統的には州政府が管轄することだとみなされてきた。

② 医療に関わる主要な連邦法とHIPAA

そこで、第二次大戦後制定された、医療に関わる主要な連邦法は、以下に掲げるものに過ぎない。

①医学研究を促進する連邦機関、National Institute of Healthを設立する法律。

②病院建設への補助を行う Hill-Burton Act。

③社会保障法の一部として、高齢者医療と貧困者医療のシステムを構築する法律。

④企業の退職年金法に付加して、医療給付を認めるエリサ法

そして、最も直近の重要な法律が１９９６年のHIPAA法である。

当時のクリントン政権は全面的な医療保険改革を志して果たせず、唯一、医療保険の維持拡充を、転職による不利益の除去という形で図ることに成功した。すでに企業の退職年金法に関連して医療給付がなされており、転職の際に今まで掛けてきた医療保険が引き継がれるか否かは、個人にとって重要であった。転職がアメリカ社会において普通のことであり、転職は州境を越えて行われるのも通常であること、企業の医療給付体制を連邦法が規制しているという実績もあって、このような法律を作ることには、法理論的にも大きな問題はなかった。

しかしながら、事の実質を見ると、HIPAA とそれに基づく連邦規則は、アメリカにおいて歴史的な意義をもつ可能性が強い。というのは、医療保険の引継は、それまでの医療費の請求や支払いに関わる事柄だけでなく、個人の医療情報をすべて引き継ぐことになるので、きわめて広い意味で、医療情報の取り扱いに関する連邦の規制が認められることになったからである。

転職に伴う医療保険の引継という、ごくテクニカルな印象を与える問題が、実は、史上初めて、医療分野における連邦政府の権限の大幅な拡大の可能性を開く道筋となったというように評価できる。

アメリカにおいて、HIPAA 法に基づく連邦政府規則に関し、今後強い異論が上がるとすれば、規制に伴うコスト増を厭う医療機関の経済的な考慮とともに、連邦政府の権限論が再浮上する可能性もあることになる。

③ HIPAA法と連邦厚生省規則の関係

HIPAA 法の概要については、次項でふれられるはずであるから、ここでは、２０００年にクリントン政権末期に制定された連邦政府の厚生省(DHHS, Department of Health and Human Services)規則との関係につき一言する。

HIPAA法自体は５つの編に分かれる。

Title

Ⅰ Portability

Ⅱ Adiministrative simplification; fraud prevention

Ⅲ Tax

Ⅳ Application and enforcements

Ⅴ Revenue Offsets

これらは、医療保険が転職に伴い、医療保険の受益者と共に移転する体制を保障し、そのための手続きを簡素化し、他方で、医療保険詐欺を防止しようとするものである。同時に、医療情報につきプライバシー保護などの規定の整備が必要だと宣言し、１９９９年８月までの時限で、連邦議会に行動を促すとしている。そして、連邦議会が何らかの理由で法律制定に動かない場合の補充措置として、厚生省に規則制定権限を認めた。実際、連邦議会は新たに法制定に動かなかったので、厚生省が、規則の要綱を作成公表し、広くパブリック・コメントを求め、それを採り入れて規則を公表したのである。手続き簡素化のための標準化などの部分が公表された後、プライバシー保護の部分は、クリントン

政権末期の２０００年１２月２０日に公表され、１２月２８日の連邦政府公報(Federal Register)に掲載された。

これらは、次の点で特色を持つ。

第１に、繰り返しになるが、医療保険に関して初の連邦規制であり、対象は広く全国の医療機関、医療保険関連機関に及ぶ。

第２に、州法との関連でいえば、企業退職年金法であるエリサ法は、同法の対象分野につき連邦法の専占領域とし、かつ強行規定を含む、いわば連邦政府による強い規制をかけるものであるのに対し、HIPPA 法とそれに基づく連邦規則は、一定の範囲で州法を排除する効果はもつものの、州政府による規制と共存を図り、連邦の定めは規制の最小限度だとしている。

第３に、医療保険に関する手続きを簡素化しコストダウンを図るためには、情報化・標準化が不可欠であるとして、医療情報のコンピュータ化を推進している。その結果、情報の流通促進と保護という重い課題を自ら担うことにもなった。

この規則が円滑に実施されるか否か、実施されたとして所期の効果を上げ得るか、さまざまな懸念は現実化しないかという諸点が注目される。

２　個人情報保護ガイドラインの中の同意を得ずに利用できる情報―ガイドライン１６４．５１２条

ＨＩＰＡＡ法の要請に基づいて作られた個人情報保護のガイドラインは、個人の同意を厳しく要求しているが、その一方で、同意を得ないで利用・開示できる場合もきちんと規定されている。この部分については特に興味があるので、以下にその条文について記す。

１６４．５１２条は、「情報の使用や開示にあたって、(医療実施に関わる治療・支払いについて使用開示の）同意、(それ以外の場合の）許可、および同意・反対を表明する機会のいずれも必要とされない場合」と題されている。言い換えれば、ここでは個人を識別できる医療情報について、当該個人の同意が必要とされない場面を列挙している。

同条の構造は、具体的には、(a)基準から(l)（エル）基準までの、１２個の基準を設定する。本人同意の不要な場合を１２類型並べているわけである。

(a)基準：法によって使用や開示が求められる場合
(b)基準：公衆衛生上の医療活動のための使用と開示
(c)基準：虐待、遺棄、または家庭内暴力の被害者に関する情報の開示
(d)基準：医療監督活動のための使用と開示
(e)基準：司法および行政手続のための開示
(f)基準：法の執行を目的とする開示
(g)基準：死者に関する情報の使用および開示
(h)基準：死体解剖のための、臓器、眼球または体細胞組織の提供を目的とする、情報の使用および開示
(i)基準：研究を目的とする使用および開示
(j)基準：健康または安全に対する重大な脅威を避けるための使用および開示。
(k)基準：特殊な政府機能を目的とした使用および開示。
(l)基準：労災補償のための開示

これらを見ると、個人情報保護規則が、プライバシーの主張と医療情報活用の必要性を説く主張との間でバランスをとろうとしていることがわかる。

医療をめぐる個人情報の扱いは、大きく分けて、次の３種類の対応がなされる。

①治療や保険による医療費支払い、医療機関の業務に関し個人情報を利用する場合には、同意原則を維持し、本人による同意を得ることが必要であるとした（１６４．５０４条)。最終規則の前の段階では、これらの場面では同意原則をとらないこととしていた。同意原則をとっても患者は同意せざるを得ない場合がほとんどであり、原則とする意味がないこと、さらに、同意といっても十分な情報なく得られる場合が多く、その意味でも、原則とする価値がないとの判断であった。それに代わって、いかなる利用

がなされているかの本人への通知（情報開示）を義務づける方向がとられた。しかし、中間案に対しては、同意を得る慣行が医療現場ですでに行われていることや、現代の医療倫理において、患者の同意原則は基本的であるとの批判が強く、最終規則では、治療や支払いという医療の基本的な場面で同意原則が維持された。

②本条、１６４．５１２条においては、先に述べたように同意を不要とする場面が列挙されている。それが１２項目にわたり、ガン登録などを含む公衆衛生上の情報収集や情報開示、医学研究などで、本人同意の原則をはずしている。もちろん医学研究などではそれに代わる安全装置（病院内倫理審査委員会などの関与）を要求するなど、それぞれに配慮が見られる。だが、これらの規定は、同意原則だけがプライバシー保護と結びつくわけでないことと、プライバシー保護自体に一定の限界があることを真正面から認めたものである。さらに、本条の最初の項目、「法によって使用や開示が求められる場合」には州法も含まれるから、連邦法の情報保護規制が州法によって減少していく可能性、全国一律の情報保護という状況がいっそう実現しがたくなるという可能性がある。

③上記２種類の場合、同意原則の適用される場合と適用されない場合を除いて、個人情報の使用と開示には、原則として本人の許可(authorization)が必要とされる（１６４．５０８条)。本規則は、許可と同意が別物であると説明しているが、本人が主導権を握っているという意味で、区別はないように思われる。ここでは、個人の情報コントロール権が認められていると考えられる。翻って、１６４．５１２条によって医療情報活用が認められる範囲が合理的な範囲であるとすれば、全体として、個人情報保護規則は、文字通り個人の情報保護で格段の進展を見せたものと評価することもできる。

E.結論

米国で成立したＨＩＰＡＡ法の背景を述べると共に、その個人情報保護ガイドラインの中の個人の同意を得ないで情報が利用・開示できるとした部分について考察を加えた。

平成１２年度厚生科学研究費補助金（特別研究事業）

分担研究報告書

HIPAAの概要 セキュリティー基準の概要

分担研究者　　大江和彦（東大病院中央医療情報部）

研究要旨　　米国において１９９６年に成立したＨＩＰＡＡ法の要請によって作られたセキュリティのガイドラインについて研究し、その基本を解説すると共に、日本における今後のセキュリティのガイドラインについて考察を加えた。

A.研究目的

米国で１９９６年に成立したＨＩＰＡＡ法（Health Insurance Portability and Accountability Act）のガイドラインの中のセキュリティガイドラインについて調査・研究することが本研究の目的であった。

B.研究方法

インターネット上で本法律に関する様々な意見を収集し、考察を加えた。

C.研究結果及びD.考察

HIPAA のセキュリティー基準(Security Standards)は、1998 年 8 月 12 日に Proposed Rule が公開され同年 10 月 13 日までパブリックコメントを公募していた。その後、現在までに公式な進展はないようであるが、この Proposed Rule に記載されていた Security Matrix は米国内の多くの保健医療情報関係サイトで広く参照されているようである。ここでは、この Proposed Rule の概要、そして HIPAA Security Matrix を説明する。

１．Proposed Rule の概要

HIPAA Security and Electronic Signature Standards; Proposed Rule (45CFR Part142) は、医療提供者（医療機関など）、ヘルスプラン（種々の健康保険者）、クリアリングハウス（データ加工業者）によって使用される個人健康情報のセキュリティーと電子署名に関する基準を提示したものである。医療提供者、ヘルスプラン、クリアリングハウスはすべての種類の個人健康情報のセキュリティーを開発し維持していくためにこのセキュリティー基準を使うことになる。電子署名基準は HIPAA1996 で定義された特定の情報交換と一緒に使用される場合で、電子署名がなくてはならないと規定されている場合にだけ適応可能な基準である。

Proposed Rule は、表1のように 14 セクションと3つの付録からなるが、第 6 セクションがこのセキュリティー基準の基本的な考え方を述べたものであり、第7セクションから第 11 セクションが基準の各論である。第 11 セクションはこのセキュリティー基準を実施するにあたって他の基準へ影響を与える可能性について分析している。付録1は第7セクションから第 11 セクションで順にとりあげられる要件と実装特性について表にして整理したものであり、HIPAA SECURITY MATRIX と呼ばれている。簡単にいえば本セキュリティー基準は HIPAA SECURITY MATRIX はすべてであり、その解説が第7～11 セクションにあるわけである。付録 2 はセキュリティー基準中に出てくる主要な用語について用語辞書を掲載したもので大変ためになる。付録3は、HIPAA SECURITY MATRIX に記載の実装特性を実現するために直接関連する既存の標準規格を参考までにマッピングしたものであり、現実にはこれが役に立つ。

1	Summary and Introduction
2	Background
3	Provisions of this Proposed Rule
4	Definitions
5	Effective Dates--General
6	Security Standard--General
7	Administrative Procedures
8	Physical Safeguards to Guard Data Integrity, Confidentiality, and Availability
9	Technical Security Services to Guard Data Integrity, Confidentiality, and Availability
10	Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted over a Communications Network
11	Electronic Signature Standard
12	Impact Analysis
13	Collection of Information Requirements
14	Regulation Text
App. 1	HIPAA SECURITY MATRIX
App. 2	HIPAA SECURITY AND ELECTRONIC SIGNATURE STANDARDS GLOSSARY OF TERMS
App. 3	HIPAA SECURITY MATRIX-mapping

表１．HIPAA Proposed Rule of Security Standard の構成

２．HIPAA セキュリティー基準の総論

２．１　基本的な考え方

本 ProposedRule 第 6 セクションでは、HIPAA セキュリティー基準の作成するにあたっての以下のような３つの基本的な考え方が述べられている。

１）基準は包括的であること（The standard must be comprehensive.)

セキュリティーはたとえば装置の物理的な保全だけをカバーするだけとか、通信の秘匿性だけを保護するとか、といった断片要素だけのセキュリティーを確保しても全体のセキュリティーは得られない。しかし一方でどの単一の標準規格策定組織もあらゆるセキュリティー局面を保護するような単一のセキュリティー基準を作成していないので、特定の標準を採用するだけでは満たされない状況にある。

２）基準は特定の技術から中立であること（The standard must be technology-neutral.)

セキュリティ技術はめまぐるしく変わっているので、提案する基準は特定の技術を参照するようにしたり主張したりはしてはいけない。医療提供者側、健康保険者、クリアリングハウスに対して、自分たちの技術解決方法を選択できるような柔軟性を与えたい。１個あるいは複数の特定の技術に依存するような基準は、将来の進歩のためを考えると柔軟性に乏しい。

３）基準はスケーラブルであること（The standard must be scalable.)

単一のアプローチのみを推奨するようなただ一つの基準で、小さな診療所から大規模なデータを扱う健康保険者まですべてをカバーできるようにすることは無理である。大規模な健康保険者には必要な基準であっても、小さな地域診療所にとっては技術的には実現可能でも経済的に実現不可能あるいは経済的に見合わないような実現方法もあることを肝に銘じ、小さな地域診療所の能力や経済力を十分に配慮する必要がある。

２．２　基本方針

前述の３つの基本的な考え方にもとづいて、セキュリティ基準を、医療提供者（providers)、ヘルスプラン（健康保険者)、およびクリアリングハウスがそれぞれの業務において含まなければならないセキュリティー要件とそれをインプリメンテーション特性（実装のための個別の特性；Implementation features）をセットにしたものとして定義している。

インプリメンテーション特性は、要件の特定の局面(aspect)に言及するものであるが、特定の技術を参照したり、主張したりはしていない。また特定の利用組織が特定の特性を実装するべき

範囲についても言及していない。基本的に、各関連する利用組織がそれ自身のセキュリティ・ニーズおよび危険を評価し自身のビジネス要件に取り組むために適切なセキュリティを考案し、実装し、維持することを要求している。つまり、個々のセキュリティ要件がどの程度十分なものか、あるいはどの技術を使用するべきかは、各利用組織が自身の責任で経費と有効性のバランスの中で決定しなければならないビジネス上の決定であるとしている。

提案されたセキュリティー基準は、データの完全性、秘匿性および可用性を保護するための要件とそのインプリメンテーション特性からなり、説明の便宜上、以下の４つのカテゴリーに分けられている。

１）管理上の手続き：データ、およびデータの保護に関係する人員の行為を保護するためのセキュリティー対策の選択と実行を管理する、ドキュメント化されたフォーマルな実施策。

２）物理的な安全装置：物理的なコンピューター・システムや、関連のある建物と設備を、侵入だけでなく火および他の自然環境上の危険から守ることと関連した装置群。物理的な安全装置には、さらにロック、キー、およびコンピューター・システムおよび設備へのアクセスをコントロールするために使用される管理上の手段の使用も含まれている。

３）技術的なセキュリティーサービス：情報アクセスを保護し、コントロールしモニターするために適所に置かれるプロセスサービス。

４）技術的なセキュリティ・メカニズム：通信ネットワーク上に送信されるデータへの無許可のアクセスを防ぐために適所に置かれるプロセス。

ただし、以上の４つのカテゴリーに含まれる要件を利用機関はそれぞれの業務態様にあわせて取捨選択し組み合わせて実現すればよいのであり、ここに表れるすべてを実現する必要があるというわけではないとしている。

以上の４つのカテゴリー別に要件とインプリメンテーション特性を列挙した４つの表と、電子署名に関する表の計５つの表が HIPAA Security Matrix と呼ばれるものである。

3．HIPAA Security Matrix

3．1　管理上の手続き

要求 (REQUIREMENT)	実装特性(IMPLEMENTATION FEATURES)	関連する既存規格番号
証明 Certification		47
信頼パートナー合意の連鎖 Chain of trust partner agreement		12,47
臨時対策計画（実装特性はすべて実装されなくてはならない) Contingency plan (all listed implementation features must be implemented).	アプリケーションとデータの危機分析 Applications and data criticality analysis.	17,47,53
	データのバックアップ計画 Data backup plan.	12,17,47
	災害時復旧計画 Disaster recovery plan.	12,17,47,53
	緊急モードでの操作計画 Emergency mode operation plan.	47,53
	テストと修正 Testing and revision.	12,17,47
レコード処理のために正規のメカニズム Formal mechanism for processing records.		12, 17
情報アクセス・コントロール（実装特性はすべて実装されなくてはならない) Information access control (all listed implementation features must be implemented).	アクセス認証 Access authorization.	12, 17, 47, 53
	アクセス確立 Access establishment.	17, 47, 53
	アクセス修正 Access modification.	12, 17, 47, 53
内部監査 Internal audit		12, 17, 43, 44, 47
人員セキュリティー（実装特性はすべて実装されなくてはならない） Personnel security (all listed implementation features must be implemented).	認可され知識が法風な人物によって保守人員を監督すること Assure supervision of maintenance personnel by authorized, knowledgeable person.	17, 47
	アクセス認証記録の管理 Maintenance of record of access authorizations.	12, 17, 47

	操作や保守人員が適切なアクセス認証をしていること Operating, and in some cases, maintenance personnel have proper access authorization.	17, 47
	人員クリアランス手続き Personnel clearance procedure.	
	人員のセキュリティー方針または手続き Personnel security policy/procedure.	12, 17, 47, 53
	セキュリティーの訓練を受けた保守人員を含むシステム利用者 System users, including maintenance personnel, trained in security.	12, 17, 47, 53
セキュリティ構成情報の管理（実装特性はすべて実装されなくてはならない）Security configuration mgmt. (all listed implementation features must be implemented).	ドキュメンテーション Documentation	12, 17, 47, 53
	ハードウェア/ソフトウェア設置&メンテナンス調査およびセキュリティ特性のためのテスト Hardware/software installation & maintenance review and testing for security features	12, 17, 47
	構成一覧説明表 Inventory	12, 17
	セキュリティ試験 Security Testing	12, 17, 47
	ウイルスチェック Virus checking	12, 17, 47, 53
セキュリティ事案手順（実装特性はすべて実装されなくてはならない）Security incident procedures (all listed implementation features must be implemented).	報告書手続き Report procedures.	12, 17, 47
	レスポンス手続き Response procedures.	17, 47
セキュリティ管理プロセス（実装特性はすべて実装されなくてはならない）Security management process (all listed implementation features must be implemented).	リスク分析 Risk analysis.	12, 17, 47, 53
	リスク管理 Risk management.	17, 47
	制裁ポリシー Sanction policy	12, 17, 47, 53
	セキュリティーポリシー Security policy.	17, 47, 53

終了手順（実装特性はすべて実装されなくてはならない）Termination procedures (all listed implementation features must be implemented).	数字組合わせ鍵の変更 Combination locks changed.	12, 17
	アクセスリストの破棄 Removal from access lists.	12, 17, 47, 53
	利用者アカウントの破棄 Removal of user account(s).	12, 17, 47
	アクセスを許可する鍵、トークン、カードの返却 Turn in keys, token or cards that allow access.	12, 17, 47
トレーニング（実装特性はすべて実装されなくてはならない） Training (all listed implementation features must be implemented)	全人員（管理者を含む）へのセキュリティー意識のトレーニング Awareness training for all personnel (including mgmt).	12, 17, 18, 47, 53
	定期的なセキュリティー注意喚起 Periodic security reminders.	12, 18
	ウイルス防護に関するユーザー教育 User education concerning virus protection. ログインの成功／失敗の記録のチェックの重要性やその不一致の報告方法についてのユーザ教育 User education in importance of monitoring log in success/failure, and how to report discrepancies.	12, 17, 18
	パスワード管理に関するユーザ教育 User education in password management.	12, 18, 47

3．2　物理的な安全装置

要求 (REQUIREMENT)	実装特性(IMPLEMENTATION FEATURES)	関連する既存規格番号
割り当てられたセキュリティ責任 Assigned security responsibility		47
メディア・コントロール（実装特性はすべて実装されなくてはならない） Media controls (all listed implementation features must be implemented).	アクセス・コントロール Access control.	17, 47, 53
	説明責任（トラッキング・メカニズム） Accountability (tracking mechanism).	17, 18, 47
	データバックアップ Data backup	12, 17, 47, 53
	データ記憶装置 Data storage	12, 17, 47
	処分 Disposal.	17, 47, 53
物理的なアクセス・コントロール（制限的アクセス）（実装特性はすべて実装されなくてはならない） Physical access controls (limited access) (all listed implementation features must be implemented).	災害復旧 Disaster recovery.	17
	緊急モード・オペレーション Emergency mode operation.	17
	設備コントロール(サイトの中への、およびサイトからの)Equipment control (into and out of site).	17, 47
	設備セキュリティ計画 Facility security plan.	12, 17, 47
	物理的なアクセスに先立ったアクセス認証の確認のための手順 Procedures for verifying access authorizations prior to physical access.	17, 18, 47
	メンテナンスレコード Maintenance records.	17
	知っているべき人員アクセスのための手順 Need-to-know procedures for personnel access.	12, 17, 47, 53
	訪問者や同伴者の入室許可 Sign-in for visitors and escort, if appropriate.	17
	テストと修正 Testing and revision	17, 47
ワークステーション使用に関するポリシー／ガイドライン Policy/guideline on work station use		18
安全なワークステーション位置 Secure work station location		17, 53

セキュリティ意識のトレーニング Security awareness training		12, 17, 47

3．3　技術的なセキュリティーサービス

要求 (REQUIREMENT)	実装特性(IMPLEMENTATION FEATURES)	関連する既存規格番号
アクセス・コントロール（実装特性のうち*は必須、さらに暗号以外の３つのうち１つは必須）Access control (The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: Context-based access, Role-based access, User-based access. The use of Encryption is optional).	状況に基づいたアクセス Context-based access.	5, 12, 14, 16, 17, 40, 47
	暗号化 Encryption.	1, 6, 12, 14, 17, 21, 22, 23, 24, 26, 36, 28, 29, 30, 31, 47, 49, 53, 54, 55
	緊急アクセスの手順　*Procedure for emergency access.	14, 17, 53
	役割に基づいたアクセス Role-based access.	14, 16, 17, 40, 41, 47, 53
	利用者に基づいたアクセス User-based access.	11, 12, 14, 16, 17, 40, 41, 47, 53
監査コントロール Audit controls		12, 14, 18, 47, 53
承認コントロール（実装特性のうち１つは必須）Authorization control (At least one of the listed implementation features must be implemented).	役割に基づいたアクセス Role-based access.	5, 14, 16, 17, 47, 53
	利用者に基づいたアクセス User-based access.	14, 16, 47, 53
データ認証 Data Authentication		11, 53

エンティティー認証（自動ログオフと個人 ID 識別は必須、さらに残りのうち１つは必須） Entity authentication (The following implementation features must be implemented: Automatic logoff, Unique user identification. In addition, at least one of the other listed implementation features must be implemented).	自動ログオフ Automatic logoff.	14, 16, 17, 18, 40, 53
	生物学的認証 Biometric.	14, 16, 18, 40, 47, 53
	パスワード認証 Password.	14, 16, 17, 18, 19, 40, 47, 53
	個人 ID 番号認証 PIN.	14, 16, 18, 19, 40, 47
	電話コールバック Telephone callback.	14, 17, 18, 47, 53
	トークン認証 Token.	14, 17, 47, 50, 53
	ユニークなユーザ識別 Unique user identification.	14, 47, 53

３．４　技術的なセキュリティ・メカニズム：通信ネットワーク経由で送信されるデータを許可されない者がアクセスすることに対する保全対策
TECHNICAL SECURITY MECHANISMS TO GUARD AGAINST UNAUTHORIZED ACCESS TO DATA THAT IS TRANSMITTED OVER A COMMUNICATIONS NETWORK

要求 (REQUIREMENT)	実装特性(IMPLEMENTATION FEATURES)	関連する既存規格番号
通信/ネットワークコントロール（もし通信またはネットワークが使われるのであれば、完全性コントロールとメッセージ認証が必須。さらに、アクセスコントロール、暗号化のどちらか一つは必須。さらにもしネットワークが使用されるのであればアラーム、監査記録、エンティティー認証、エベントレポートの４つは必須。[訳注：ネットワークとはインターネット、通信とは回線契約による１対１通信と思われる]）Communications/network controls (If communications or networking is employed, the following implementation features must be implemented: Integrity controls, Message authentication.	アクセスコントロール Access controls.	14, 17, 22, 23, 39, 47, 48, 53
	アラーム（傍受についての警報）Alarm.	14, 17, 18, 35, 36, 37, 38, 44
	相互参照監査記録 Audit trail.	
	暗号化 Encryption.	1, 6, 12, 14, 17, 21, 22, 23, 24, 26, 27, 28, 29, 30, 31, 47, 49, 52, 53
	エンティティー認証 Entity authentication.	12, 14, 17, 18, 20, 22, 23, 31, 32, 34, 33, 51, 53
	エベントレポート Event reporting.	
	完全性コントロール Integrity controls.	14, 15, 17, 18, 22, 23, 45, 46

In addition, one of the following implementation features must be implemented: Access controls, Encryption. In addition, if using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, Event reporting).		
	メッセージ認証 Message authentication.	14, 15, 17, 18, 22, 23, 25, 45, 46, 52