平成13年度厚生科学研究費補助金

政策科学推進研究事業　研究報告書

公衆衛生活動・調査研究における個人情報保護と利活用に関する研究

2002年3月

主任研究者　玉腰　暁子（名古屋大学大学院医学研究科）

目　　次

総　括　報　告

公衆衛生活動・調査研究における個人情報保護と利活用に関する研究

主任研究者　玉腰　暁子　名古屋大学大学院医学研究科予防医学／医学推計・判断学

研究要旨

疫学研究は人間集団を対象とし、健康障害の発生状況・発生／予防要因をさまざまな手法を用いて検討することにより、最終的には個人レベルだけでなく集団レベルでの健康水準の向上を目指すものである。したがって、人の情報を用いない疫学研究はありえないが、その情報を用いる際のインフォームド・コンセントのあり方、個人情報の収集・管理、得られた結果の還元に関しての検討は立ち遅れている。そこで、研究に際しての実際の個人情報保護のあり方、倫理審査委員会の在り方に関する検討、疫学研究の周知に取り組んだ。個人情報保護システムに関しては、理論的な構築上の問題に加え、システム管理上のソフト的な検討も今後さらに進める必要があることが明らかになった。倫理審査委員会に関しては、各施設で委員会に関与している方からの聞き取り調査を実施した。周知活動に関しては、PR リーフレットの試作版を完成させた。また疫学研究の成果を論文に公表した研究者を対象に結果の還元方法に関する調査を実施した。

分担研究者／研究協力者
石川　鎮清　自治医科大学地域医療学
尾島　俊之　自治医科大学公衆衛生学
掛江　直子　国立精神・神経センター精神保健研究所
菊地　正悟　愛知医科大学医学部公衆衛生学
小橋　　元　北海道大学大学院医学研究科老年保健医学
齋藤有紀子　北里大学医学部医学原論研究部門
佐藤　恵子　国立がんセンター中央病院・臨床試験管理室
杉森　裕樹　聖マリアンナ医科大学予防医学
内藤真理子　京都大学大学院医学研究科医療システム情報学
中村　好一　自治医科大学公衆衛生学
中山　健夫　京都大学大学院医学研究科医療システム情報学
丸山　英二　神戸大学大学院法学研究科
武藤　香織　北里大学医学部医学原論研究部門
山縣然太朗　山梨医科大学保健学 II
鷲尾　昌一　九州大学大学院医学研究院

目　的

疫学研究は人間集団を対象とし、健康障害の発生状況・発生／予防要因をさまざまな手法を用いて検討することにより、個人レベルだけでなく集団レベルでの健康水準の向上を目指すものである。したがって、人の情報を用いない疫学研究はありえないが、その情報保護の方法、得られた結果の還元方法についての検討はほとんどなされていない。また、厚生労働省、文部科学省合同で疫学研究の倫理指針が策定されつつあるが、多くの判断を委ねられる倫理審査委員会の適切なあり方についての検討課題は大きい。そこで、本研究では、健康情報を含む個人情報を用いた疫学研究が情報の保護と利活用の適切なバランスの上で遂行されるために必要と考えられる

1. 研究参加を決める際の前提条件となる個人情報保護対策の具体的な方策を立てること
2. 具体的な倫理指針を提案するとともに疫学に対する倫理的審査のありかたを検討し、研究の倫理性を確保すること
3. 一般市民の間で疫学に対する理解を深めること

を目的とする。具体的には、

1. 個人情報の保護はいずれの指針も当然とされているが、現場での状況、具体的かつ最善の方法などは今までに検討されていない。そこで、現状の把握、具体的な情報漏洩システムの構築と提案を目的とする。
2. 現在各大学医学部・医科大学に設置されている倫理審査委員会の体制にはばらつきがあり、指針で推奨される審査体制の構築に向けては段階的な努力が必要である。さらに、疫学研究は地域ベース、多施設共同で行われるものも数多いが、その場合の倫理審査のあり方については早急な具体的提言が求められている。そこで、疫学研究に対する倫理審査委員会の審査体制の把握と、審査結果の質の向上を目的とする。
3. 疫学研究の多くは一般市民を対象とすることから、研究の意義に関し対象者の理解を求めることも重要であり、インフォームド・コンセントに際しても、疫学研究そのものの認知が低ければ、研究概要の説明や意思決定をめぐる回答の質への疑問も生じることになる。そこで、様々な媒体を用いてヘルス・リテラシーを効果的に促進することも目的とする。

これらの研究がバランスよく遂行されることにより、根拠に基づいた公衆衛生活動のために必要な疫学的手法を用いた調査研究が、個人情報を十分に保護し、対象者への倫理的配慮をしつつ、実施する適切な手段を提案できると期待される。また、集団を対象とする疫学研究実施の際には、研究の必要性や意義などを対象者が十分に理解することが必要である。しかし、研究参加時の短時間の説明のみで疫学研究を理解することは困難であることから、日頃からの啓発活動は重要であり、その方法を確立する意義は大きい。

研究成果

1. 疫学研究における個人情報保護のあり方の検討

国内外の他分野を参考にしたほか、IT 関連企業のシステムエンジニア等から専門的知識の提供をうけ、疫学研究を遂行する上で必要となる情報漏洩防止システムを検討し、さらに内部の情報処理に対する管理体制の整備を民間業者の取り組みを参考に考察した。その結果、情報漏洩防止システムは、技術的なしくみパスワードやファイアウオール等の基本的なセキュリティ技術の実装は勿論のこと、加えて①PKI（128 ビット暗号化による SSL)、②VPN の実装も不可欠である。さらに将来的には③バイオメトリクス認証等の高度なセキュリティ技術も組み合わせたシステム構成が望ましいと考えられた。また、Web を用いた疫学研究において、望ましい情報漏洩防止システムを構築するには、外部からの脅威に対する技術的な対応だけでは不十分であり、内部の情報処理に対する管理体制の整備が不可欠である。今後、疫学研究分野でも IT 化が進行するものと予想されるが、その際にはプライバシーマーク制度、BS7799、Information Security Management System (ISMS)、チーフ・プライバシー・オフィサー

（CPO）などの検討が、望ましい個人情報保護の管理体制づくりのあり方に必要であると考えられた。

2. 疫学研究の倫理性を担保するための方策の検討

①倫理審査委員会のインタビュー調査

倫理審査委員会における審査の現状や問題点、疫学研究の審査経験などを明らかにすることを目的として、国内の倫理審査委員会を訪問し、半構造化面接における聞き取り調査を行った。近年になって少数ながら疫学研究の審査も行われるようになっているが、疫学に詳しい委員がいないところでは、疫学研究の審査のポイントが明確でないところも多く、既存の指針の普及も十分であるとはいえなかった。疫学に限らず、委員や申請者に対して、倫理的な原則、審査のポイント、倫理指針の理解などについての教育はほとんど行われていなかったが、この点は大きな問題であろう。また、倫理審査委員会の答申立場が多様であったことから、倫理審査委員会のスーパービジョンを行うシステムの構築が必要であると考えられた。

②コンセントフォームの雛形開発に向けた資料収集

疫学研究における説明・同意文書のひな型の開発に向けて、まずその基礎資料として、実際の疫学研究に用いられている「説明者用説明資料」、「患者さん（協力者用）説明文書」、「同意文書」を集め、遺伝子解析をともなう研究かどうかで分けて検討した。研究実施時期が遅いものほどガイドラインや指針の内容が反映していた。疫学研究の種類や対象者の属性により、説明・同意文書に必要な項目が異なることが示唆された。

3. 疫学研究の理解と周知方法の検討

①疫学研究を紹介する印刷物の作成

疫学研究の意義、方法などとともにこれまでの疫学研究の成果を知らせる広報のためのリーフレットを試作した。対象を一般の集団とし、また配布場所として疫学研究が実施される現場となる保健所や自治体の窓口を想定した。今年度は、昨年度の試作版を研究者および研究者以外の意見を聞くことによって改訂を加え、完成を目指した。

②疫学研究成果の社会への還元についての調査

国際誌に発表された近年の疫学研究の成果が、一般社会に向けてどのように発信されているか明らかにするために、論文著者に対する質問票調査を施行した。質問票はWeb上で回答できるシステムを構築し、Eメールで依頼状を送り、調査への参加を呼びかけた。2000年7月～12月に専門国際誌5誌に発表された原著論文448編から、Eメールアドレス不明、重複を除く384人の著者を対象として選定した。現在、依頼のEメールを送付し、回答を集約中である。

4. その他の研究

①「疫学研究におけるインフォームド・コンセントに関するガイドライン（ver 1.0）」の評価に関する研究

我々が2000年4月に公表したガイドラインを疫学の講義を受けている看護大学生に読んでもらい感想を求めた。本ガイドラインに対する共感、ガイドラインがうまく働くための提言が示された。しかし、その一方で、ガイドラインに対する批判、ガイドラインがあってもなお残る不安も見られた。ガイドラインの批判の中には、違反した場合の罰則がないことや今まで疫学者がきちんとした倫理のガイドラインを作っていなかったことに対する批判が含まれていた。看護大学生はおおむね本ガイドラインに好意的なものの、ガイドラインがあってもなお残る不安を持っている者も少なくなかった。

②疫学研究における倫理的問題についての意識と疫学についての知識に関する調査

質問票を用いて疫学研究における倫理的問題についての意識と疫学についての知識を調査し、一般大学生、看護大学生、看護職で互いの結果を比較した。看護職には准看護婦も含まれ、疫学についての知識が少ないにもかかわらず、倫理的基準に看護大学生と差を認めなかったことは、看護の現場でインフォームド・コンセントなどの倫理的配慮が実際に行われているためだと考えられた。一般大学生では、倫理的な問題について、厳格な対応を求める人がいる一方で、かなり寛容な意識の人も多く、各人による意

識の幅が広かった。疫学者は、一般大学生や一般国民に対して、教育・情報提供を通じて、疫学研究の意義と、個人情報が不適切に使用される場合の問題点の両方を良く理解してもらい、合理的な自己決定を行うことができるように支援していく必要がある。

考　察

疫学研究は人間集団を対象とし、健康障害の発生状況・発生／予防要因をさまざまな手法を用いて検討することにより、最終的には個人レベルだけでなく集団レベルでの健康水準の向上を目指すものである。したがって、人の情報を用いない疫学研究はありえないが、その情報を用いる際のインフォームド・コンセントのあり方、個人情報の収集・管理、得られた結果の還元に関しての検討は立ち遅れている。今年度は、厚生労働省、文部科学省が合同で疫学研究の倫理指針策定を進めている。その進行状況をにらみながら、我々は、実際の個人情報保護のあり方、倫理審査委員会の在り方に関する検討、疫学研究の周知に取り組んだ。

個人情報保護システムに関しては、現状行われているものに関する検討をほぼ終了した。理論的な構築上の問題に加え、システム管理上のソフト的な検討も今後さらに進める必要があることが明らかになった。そこで、来年度は実際に仮想データを用いてシステムを構築し、運用に当たっての問題点を具体的に提示する予定である。

倫理審査委員会に関しては、各施設で委員会に関与している方からの聞き取り調査を実施した。委員会の構成や審査方法に関して、共通の悩みも見られたが、一方で倫理審査委員会の答申立場が多様であることが明らかになった。今後、倫理審査委員会のスーパービジョンを行うシステムの構築が必要であると考えられた。また委員への教育が不十分である可能性があり、来年度、教育プログラムの開発に取り組む予定である。別に疫学研究におけるコンセントフォームの開発に向けて、資料収集を行った。それらを参考に来年度は必要項目を列挙し、雛形を提示する予定である。このような取り組みを続けていくことが、疫学研究の意義を、社会一般の人々に対して周知していくことにもつながるであろう。

周知活動に関しては、PR リーフレットの試作版を完成させた。今後、一般の方々を対象に配布し、疫学研究に対する認知の向上を目指したい。また更に、よりきめ細かなニーズに対応した研究対象者別の啓発ツール作成に向けて、検討を重ねていく予定である。その結果として、一般住民の研究協力への理解を深めていくことが期待される。また疫学研究の成果を論文に公表した研究者を対象に結果の還元方法に関する調査を実施した。その結果を早いうちにまとめ公表する予定である。

分　担　報　告

疫学研究における情報漏洩防止システムのあり方についての検討（Ⅰ）
－情報漏洩防止システムにおける技術的な仕組み－

杉森　裕樹　聖マリアンナ医科大学
玉腰　暁子　名古屋大学大学院医学研究科
丸山　英二　神戸大学大学院法学研究科
佐藤　恵子　国立がんセンター中央病院
菊地　正悟　愛知医科大学医学部
齋藤有紀子　北里大学医学部

研究要旨

ネットワークを用いたオンライン症例登録・割付システム構築について、情報漏洩防止と個人情報保護の技術的担保の仕組みをシステム面から検討した。パスワードやファイアウオール等の基本的なセキュリティ技術の実装は勿論のこと、加えて①PKI（128ビット暗号化によるSSL）、②VPNの実装も不可欠である。さらに将来的には③バイオメトリクス認証等の高度なセキュリティ技術も組み合わせたシステム構成が望ましいと考えられた。

研究目的

平成13年11月29日に「医療制度改革大綱」[1]が政府・与党改革協議会において出され、厚生労働省・保健医療情報システム検討会では、情報技術を活用した今後の望ましい医療の実現を目指して「保健医療分野の情報化にむけてのグランドデザイン」を取りまとめた[2]。ここでは「情報化が我が国医療の将来に大きな影響を与えるものであることを踏まえ、これを国として戦略的に進めていくことが極めて重要」とし、保健医療分野の情報化のために、次の5つのアクションを設定した。

1　医療における標準化の促進
2　情報化のための基盤整備の促進
3　モデル事業の展開
4　情報システム導入・維持費の負担の軽減
5　理解の促進

特に「2　情報化のための基盤整備の促進」に関しては、質の高い効率的な医療提供体制を目指し、具体的には、平成15年度までに電子カルテ等の医療施設内の情報化基盤整備とともに、医療施設のネットワーク技術を活用した新たな基盤整備を提言した。その際、「患者の診療情報利用に当たっては、まず患者本人の同意が必要であり個人情報の保護に細心の注意を払うとともに、権限のない人が患者の情報を閲覧したり、持ち出したりすることがないよう厳重な管理体制を確立する必要がある」[2]とし、国民が安心できる安全な医療情報の運用管理体制の基盤整備を重視している。

これらの保健医療分野における高度情報化の動向は、疫学研究のあり方にも影響を与えるものである。そこで、本研究では、対象者の理解を得て疫学研究を遂行する上で必要となる情報漏洩防止システムの条件を、「技術的な仕組み」を中心に、近年運用され始めた国内外のネットワーク技術を活用したオンライン症例登録・割付システムの例を参考に考察した。

方　法

現在、国内外で既に運用されているオンライン症例登録・割付システムの例として

①大学病院医療情報ネットワーク（UMIN）におけるインターネット医学研究データセンター（INDICE）[3]

② CASE-J （Candesartan Antihypertensive Survival Evaluation in Japan）

③愛知医科大学インターネット情報収集データベースシステム

④EORTC（Europe Organizatipon Reasearch Trial Center）[4]

を紹介し、インターネットを用いたオンライン症例登録・割付システムにおける情報漏洩防止システムの現状と課題について検討した。しかしこれらのシステム情報自体が機微（sensitive）であり、詳細については多くは公開されてない。そこで、一般的な技術的課題についても触れた。

結　果

①大学病院医療情報ネットワーク（UMIN）におけるインターネット医学研究データセンター（INDICE）[3]

研究者主導で、臨床・疫学研究の症例登録（割付）・データ収集を支援する目的で開設され、UMINが運営するセンターである。（図1）症例登録と調査にインターネットまたはFAXを用いる。平成13年4月以降の運用開始プロジェクト（図2）については、UMINのIDとパスワード、及びINDICE専用パスワードがあれば参加可能である。研究者は別途に、独自の研究ホームページを立ち上げて運用し、そこで研究プロトコールの内容、問い合わせ先、研究に関してのFAQ等の詳細について案内する。

情報漏洩防止システムの中心には、SSL（Secure Socket Layer）-HTTPとVPN（Virtual Private Network）があり、SSL-HTTPで暗号化した上で、VPNの仮想回線の部分で二重に暗号化する仕組みを採用している。VPNについては、参加施設（平成12年7月現在は国立大学病院のみ）のファイアウォール内に限定されている。

脳神経外科学会の事業である日本未破裂脳動脈瘤悉皆調査：UCAS Japan[5]も、INDICEで運営されている代表的な研究プロジェクトであり、動脈瘤の自然歴の把握と、本邦での診療の実態の把握を目的としている。2001年1月1日から調査が開始され、2001年9月25日現在1563人の患者が登録されて

運用開始 運用終了	専門領域	研究デザイン	症例数区分	状態
2001/08 ----/--	心臓血管外科	症例登録	1万-10万例	運用中
2001/08 ----/--	泌尿器科	無作為化比較臨床試験	100-1000例	運用中
2001/11 ----/--	泌尿器科	無作為化比較臨床試験	100-1000例	運用中
2001/11 ----/--	循環器内科	無作為化比較臨床試験	100-1000例	運用中
2002/01 ----/--	脳神経外科	無作為化比較臨床試験	100-1000例	運用中
2002/04 ----/--	血液内科	無作為化比較臨床試験	100-1000例	運用中
2002/04 ----/--	消化器外科	無作為化比較臨床試験	100-1000例	運用中
2002/04 ----/--	循環器内科	無作為化比較臨床試験	1000-1万例	準備中
2002/05 ----/--	心臓血管外科	無作為化比較臨床試験	100-1000例	準備中

図2．INDICEの研究プロジェクト例

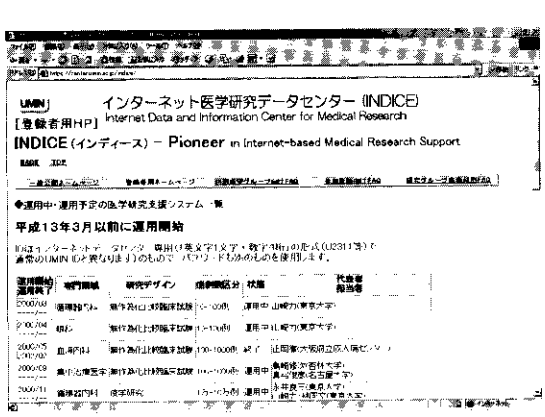


図1．UMINのINDICE

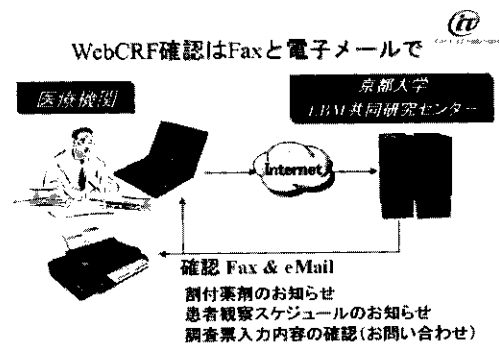


図3．CASE-J

いる。人力状況の調査および安全監視のため、安全監視委員会（データモニタリングコミッティー）が設置されており、毎年無作為に全国10施設を選択し調査員を派遣し調査している。

②CASE-J（Candesartan Antihypertensive Survival Evaluation in Japan）

日本高血圧学会[6]が後援し、京都大学EBMセンターが中心となって運営している。高リスク本態性高血圧患者（II型糖尿病／高度な高血圧／脳・心・腎・血管のいずれかの障害を合併する患者）4000名を対象として、無作為にARB群（カルデサルタンシレキセチル群）とCa拮抗薬群（ベシル酸アムロジピン群）に割り付け、3年間以上追跡して心血管イベント（突然死、脳・心・腎・血管障害の新規発症または再発・増悪）抑制効果を検討する大規模な無作為介入臨床試験である。症例登録と調査にインターネットを用いる。2002年12月までに登録が完了され、2005年12月まで検討予定である。全国537医師が契約締結し、患者1171例が登録済みである。（2002年2月現在）

ここでは、IRB承認がなされ、契約締結後、医療機関から京都大学EBM共同研究センターへ、対象者属性（医療機関名、診療科名、担当医師氏名医療機関の臨床検査基準値範囲）を連絡し、京都大学EBM共同研究センターから医療機関へ、認証情報（ID、パスワード）の連絡および資料（調査票記載見本、調査票記載マニュアル、症例登録用調査票、バーコードブック等）が発送されるシステムである。

③愛知医科大学インターネット情報収集データベースシステム

愛知医科大学のインターネット情報収集データベースシステムは、インターネットのホームページを利用して全国の病院、診療所などから疾病に関する情報を収集するシステムである。

情報の盗聴、改ざん、なりすましなどの脅威を考慮し、患者名等の個人識別情報は、病院等の施設毎に設定する個人IDとともに、インターネットとは

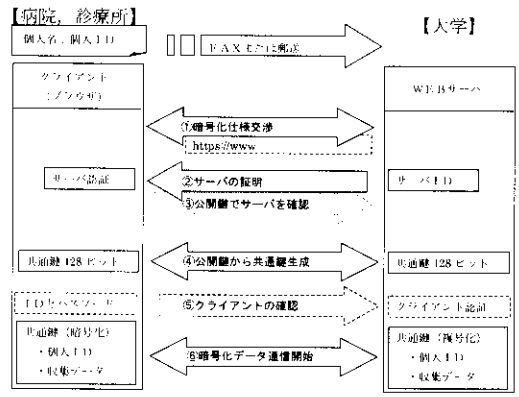


図4．愛知医科大学におけるシステム

別手段（郵送など）で対応している。インターネットの利用は、個人ID及び収集データの登録に限定している。また、SSLにより、暗号化したデータ通信を行っている。

④EORTC（Europe Organizatipon Reasearch Trial Center）[4]

国際的には、EORTC data centerが管理運営するORTA（On-line Randomized Trial Access）が知られている[4]。（図5）これはEORTC clinical trialsにおける患者の登録と無作為化を促進するために構築されたweb-basedシステムである。登録／無作為化の過程は、研究者の認証と患者の適格性をチェックし、その上で治療プロトコールと患者を割り付ける。アクセスはuser's nameとパスワードで制限され、実際の割り付けはデータ管理者の認証リストの検証による。登録・ランダム割り付けはwebブラウザー上で、ログオン、識別、適性確認、割り付けの4つのステップからなる。施設番号、プロトコール、ステップ、責任医師氏名、患者イニシャル、患者チャート番号、患者生年月日が収集される。

EORTC data center内にThe Institutional Review Board（IRB）があり、対象患者の人権擁護の目的で設立されている。特に、対象患者の個人データのプライバシーと個人情報保護に留意している。また運営システムの安全評価も毎年行っている。

D. 考　察

電子化された保健医療情報は、紙ベース情報とは

異なった情報保護（情報漏洩防止、セキュリティ）対策が必要であり、その情報の内容の重要性に応じて適切な仕組みを用いた安全対策を講じる必要がある。今回調査したオンライン症例登録・割付システムでは、情報漏洩防止を技術的に担保する仕組みとして、基本的なパスワード等の認証に加え、

①PKI（Public Key Infrastructure）

②VPN(Virtual Private Network)

等の仕組みが共通して講じられていた。

本考察では、まずインターネットを用いて、個人情報を取扱う場合の、システム構築に関する脅威を定義する。そして、これらの脅威から、オンライン症例登録・割付システム等の個人情報を保護する上で、必要となるいくつかの情報漏洩防止技術の条件を考察した。

Ⅰ．情報システムにおける脅威
Ⅱ．ファイアウォール
Ⅲ．PKI
Ⅳ．VPN
Ⅴ．認証トークン
Ⅵ．バイオメトリックス認証
Ⅶ．パスワードの管理

Ⅰ．情報システムにおける脅威

情報システムにおける脅威を大きく分類すると、①システムの脅威（ハードウェアの故障やソフトウェアの不具合）と、②人為的な脅威（意図的なもの、偶発的なもの、盗難、破壊など）となる。今回は、代表的な人為的脅威（表1）に対する技術対策を考察する。

「盗聴」は、個人医療データ等の機微な情報を、他人が盗み見る。「改竄（ざん）」は、個人医療データ等の書き換えである。治療データや、論文等の研究結果のデータが書き換えられた場合、evidenceの信頼性が損なわれ、臨床的に大きな脅威である。「なりすまし」は、文字通り第三者が正当なユーザーに成り済まして情報システムに侵入する。「否認」は、「盗聴」、「改ざん」、「なりすまし」等の不正行為を行った後、その発覚を恐れ、これらのアクセス事実を隠す。（足跡の消去）

表1．想定される人為的脅威(論理的脅威)例

- 情報の盗難／盗聴／漏洩
  - 個人情報の漏洩や機密情報の漏洩
- 情報の改竄／消去／破壊
  - ホームページ改竄や重要情報の消去
- 情報の利用不能
  - DoS攻撃によるシステムの停止
- アクセスの否認
  - 商取引の否認、アクセス事実の否認
- ウィルス感染
  - ウィルス感染によるシステムの破壊、情報の盗難
- 踏み台として悪用
  - SPAMメールの踏み台、不正アクセスの踏み台として悪用
- システムへの侵入
  - なりすましによる侵入、アクセス制御回避による侵入

Ⅱ．ファイアウォール

図6に、インターネットと接続する場合の、3つのネットワーク基本構成要素を示す。ネットワーク間の四角斜線は、ファイアウォールを示す。

1. インターネット（外部ネットワーク）は、セキュリティー上最も危険な部分である。
2. DMZ（DeMilitarized Zone「非武装地帯」）ネットワークは、ファイアウォールによって外部ネットワーク（インターネット）からも内部ネットワーク（組織内のネットワーク）からも隔離された中立的なネットワークのことである。
3. 内部ネットワークは、セキュリティー上最も安全な部分である。外部ネットワークからファイアウォール経由でDMZネットワークを介して、再度DMZネットワークと内部ネットワーク間のファイアウォール経由で情報のやり取りをする部分である。

このように、ファイアウォールは、セキュリティーレベルの異なるゾーン間に設置され（ゾーニング）、

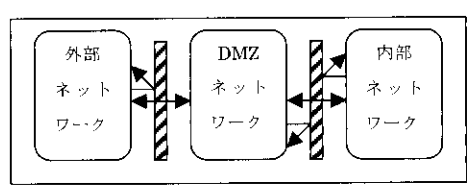


図6．ネットワークのシステム構成要素

ゾーン間の通信を可能にしながらセキュリティを確保する技術である。ファイアウォールのゾーニングにより、異なるゾーン間での不正アクセスを困難にする。また、複数のゾーンを跨いだ直接的な攻撃を防いだり、1つのシステムが侵入された場合でも他のゾーン内のシステムへの影響を最小限に抑えることができる。

ファイアウォール技術には2つあり、「パケットフィルタリング型」ファイアウォールは、送信元や送信先のIPアドレス、ポート番号などによって通信データを通過させるかどうかを判断し、不正アクセスを防ぐ方式である。一方「アプリケーションゲートウェイ型」ファイアウォールは、通信を中継するプロキシサーバを利用し、社内ネットワークとインターネットの間で直接通信をできないようにする方式である。

ファイアウォールの特徴は、定義された設定範囲内でセキュリティーを確保するものであり、あらゆる攻撃に対する防御は不可能である。例えば、許可されたIPアドレスやポートへの不正アクセスや、許可された範囲でのアプリケーション層に対する攻撃には弱い。また、最大の欠点は、ファイアウォールが攻撃された場合、攻撃されたことをリアルタイムで検知できない点である。管理者のスキルにも依存するが、膨大な量のログから攻撃を受けた原因を探し出すのは容易ではない。

オンライン症例登録・割付システム等で、ファイアウォール技術を用いる際に、①個人の健康情報など機微な情報は、内部ネットワーク内のサーバーに保管する。②外部とのアクセスが必要な公開用サーバーやDNSサーバーは、DMZネットワーク上に設置する。メールサーバーも同様である。③侵入された時の影響を考え、1台のサーバーで複数の機能を実現しない、等の考慮が不可欠である。

Ⅲ. PKI (Public Key Infrastructure) (図7)

PKIは「公開鍵基盤」と訳される。インターネット上で安全に情報通信するための暗号技術である。「鍵」はデータを暗号化したり、解読したりする際の一種のパスワードで、本人しか知らない「秘密鍵」と誰でも手に入れることのできる「公開鍵」とを組み合わせて使用する。PKIは公開鍵暗号による「電子証明書（所謂、お役所の印鑑証明みたいなものである）」（X.509規格）を発行・管理・運用する

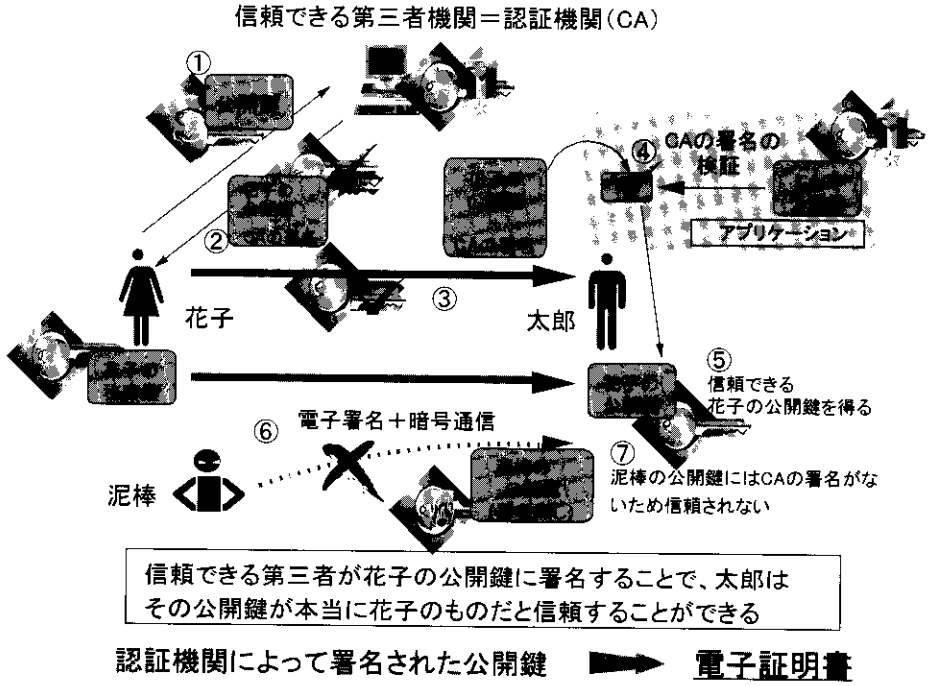


図7．PKI

ことで、①本人確認（なりすまし対策）と②通信暗号化、のセキュリティ機能を実現する。当然ながら信頼できる第三者機関すなわち認証機関（Certification Authority: CA）により、電子署名が発行されていることが前提である。現在、政府機関や民間では社会的インフラストラクチャーが整備されつつあるが、医学や疫学研究の分野においても、「医療（疫学）公開鍵インフラストラクチャー」が必要であろう[2]。

現在、PKI に対応したアプリケーションとして、既に商用化されている Verisign 社の SSL（Secure Socket Layer）がデファクトスタンダードに近い形で、各社のブラウザーに実装されている。（Netscape Navigator4.7 以降、Internet Explorer 5.01 以降）今回調査したオンライン症例登録・割付システムでも多く利用されていた。

SSL は現在 2 種類の暗号化サービスを提供している。①セキュア・サーバー ID（鍵長標準 40 ビット以上暗号化）と②グローバル・サーバー ID（鍵長 128 ビット暗号化）である。UMIN-INDICE や愛知医大情報収集システムでは、②の鍵長 128 ビット（2×10128）による暗号化通信を用いている。グローバル・サーバー ID（128 ビット暗号化）を使用した場合、100 万ドルの専用ハードウエアを利用して、しらみつぶしに暗号鍵を調べても、暗号を解くのに必要な時間は、コンピュータの進化を想定しても、2030 年で 1011 年の時間を必要とする[7]。②グローバル・サーバー ID による SSL の安全性は信頼されている。しかし、PKI で全てのセキュリティが担保されるわけではない[8]。不特定多数の利用者からネットワークを保護するためのファイアウォールやウイルスチェック等は、PKI とは別に構築する必要がある。

Ⅳ. VPN (Virtual Private Network)

VPN は、複数のポイント間に一種の専用線に似た安全の確保されたネットワークを提供する技術である。前述の SSL と異なり、IP パケットを暗号化する。したがって、利用するアプリケーションを意識することなく暗号化できるメリットがある。当然ながら暗号化される経路は、サーバーとクライアント間の経路のうち、VPN が適用されている部分だけである。VPN には、あらたに専用機器とソフトウェアの設置が必要である。しかし、直接回線を繋げなくても、インターネットを介して接続可能なため、コスト面でもメリットがあるとされる。

今回検討したオンライン症例登録・割付システム（たとえば UMIN 等）では、SSL と VPN を併用することで、情報漏洩防止を相乗的に強化する措置をとっている。

Ⅴ. 認証トークン

図 8 に、RSA セキュリティ㈱ の RSA SecurID 認証トークンを示す。このトークンはユーザーに配布され、ユーザーごとに認証が異なる。予測不可能かつ 1 回限り有効なコードが 60 秒ごとに生成され、ネットワーク接続時に、このトークンに表示された数値と暗証番号を加えたものをパスワードとして使用する。（二要素認証）RSA ACE ／Server は、このパスワードを参照してユーザーの認証を行い、ネットワークへの接続を許可する。この数値は動的に割り当てられているため、不正にアクセスをしようにも、ある一時点に正しい数値を推測することは事実上不可能である。VPN との相性も良く、併用することで相乗効果が期待できる。

Ⅵ. バイオメトリックス認証

最後に、近い将来に広く普及し、利用可能と思われるセキュリティ技術を紹介する。近年、生物学的特徴（バイオメトリクス）の個人特異性を利用した認証システムが多く開発されてきた。指紋認証、声紋認証、網膜認証、虹彩認証等である。これらは導

図 8．RSA SecurID 認証トークン

入費用やシステム規模の課題が残るものの、技術的に解決されれば、PKI以上の高いセキュリティーを担保する可能性も秘める。

① 指紋認証：パスワードの一種と考えることができる。指紋認証は2つの種類がある。①特徴点抽出（指紋にある特徴的な情報をとらえ、その方向などから判別する方式）、②パターンマッチング（指紋を画像として取り込み、画像同士を重ね合わせて照合を行う方式）である。いずれの方法も指紋を識別するセンサーを利用し、識別された情報は、特定のサーバーによって認証され各種のアプリケーションが利用できるようになる。装置としてはパソコン側に指紋識別の装置が必要になり、ユーザーの情報を登録する必要がある。但し、パスワードと異なり、各自固有の情報を有することになるので、運用は軽減される。指紋の特徴は万人不同であり同一人物の他の指や双子の兄弟でも同じ指紋は存在しないし、終生不変（身体の成長や歳月の経過によっても紋様は変化しない）点を利用している。

② 声紋認証：特殊センサーを利用して、個人を識別するものである。一部では「ボイスプリント」と呼ばれる。あらかじめ言葉を登録する。例えば「私の声がパスワード」と登録する。声紋照合の過程で声の波形を解析し照合するため、別の言葉でも識別することが可能である。声紋認証は、他のバイオメトリクスと異なり、本人が意識しないで認証することも可能である。但し、他のバイオメトリクスと異なりノイズに弱い点が課題である。

③ 網膜認証：個人により網膜の形状が異なることを利用して、センサーにより個人を識別するものである。目を利用した認証技術は、主に網膜（眼底の毛細血管の模様を用いる方式）と、虹彩(アイリス)を利用した方式がある。網膜が認証に適している理由は、現在のところ網膜に関する病気が少ないこと、網膜に関する手術も困難なことである。網膜認証の過程では、対象者がサングラスやコンタクトレンズをしていても影響されない。取り込まれた画像データはグリッドに分割され、分割された各エリアの白黒情報からバーコードを作成する。そして、データベースに格納されている網膜データのバーコード情報との照合を行う。

これらのバイオメトリクス認証は、例えば、指紋認証では指紋自体が個人情報として登録され、厳重に管理する必要がある。指紋情報は一般的な文字列のパスワードと異なり、プライバシーの侵害につながる可能性がある点は留意が必要である。

Ⅶ. パスワード管理

パスワード管理は、基本的なセキュリティーの手段であるが、システム構築時に適切なルールを策定し、システム構築と運用に反映させる必要がある。主な考慮点について考察したものを列記する。

- 桁数の指定：最少の桁数（例：8桁以上）を決める。
- パスワードの構成：最低1桁の英字または数字で構成する。最初と最後は数字で構成されない。同一文字を複数回使用させない。
- 前回のパスワード：前回使用したパスワードの履歴を取り、類似したパスワード（例：同じ文字列が3文字以上ある場合）は、新規のパスワードとして認めない。
- 特定の文字列の使用禁止：ユーザーIDや生年月日など個人を特定できる文字列の使用を禁止させる。
- 有効期限の設定：システム構築時に特定の期限（例：1ヶ月）を設定し、必ずこの有効期限内にパスワードを変更させる。また、有効期限を過ぎたユーザーは使用停止に、本人から申請が無い限り使用は認めない。
- パスワード入力ミスの回数の制限：パスワードの入力を複数回誤った場合は、該当のユーザーの使用を強制的に停止する。この場合、本来のユーザー以外のものがアクセスしたことが想定されるので、システム管理者が本人に対して確認をとる。本人からの申し出は、受け付けないことを原則とする。

最後に、UMINのパスワード管理については、「パスワードが変更されるには1時間かかる」とあり、パスワード管理をシステム内でバッチ処理していると考えられる。変更直後のシステム障害等が発生した場合の処置に対してやや不安を感じる。また、各大学のUMINの担当者連絡先として、担当者のE-mailアドレスが掲載されている。一般的にこのような情報は、ユーザーIDを予想させうる格好の糸口である。よって、「なりすまし」を容易にするリスクを孕んでいる。パスワードの有効期限、入力ミスの回数制限等も一般的に有効である。一方、パスワードを失念した場合、Faxで申請書を送信する手続きをする必要があるが、こちらはなりすましリスクを軽減させる。

個人の保健医療情報等のsensitive情報を扱う以上、ネット社会の「性悪説」に立ってあらゆるリスクを予想し対策を立て、慎重を期してシステム構築をすべきである。

結　論

ネットワークを用いたオンライン症例登録・割付システム構築について、情報漏洩防止と個人情報保護の技術的担保の仕組みをシステム面から検討した。パスワードやファイアウオール等の基本的なセキュリティ技術の実装は勿論のこと、加えて①PKI(128ビット暗号化によるSSL)、②VPNの実装も不可欠である。さらに将来的には③バイオメトリクス認証等の高度なセキュリティ技術も組み合わせたシステム構成が望ましいと考えられた。

研究協力者

高橋　太　日本アイビーエム㈱

参考文献

1　医療制度改革大綱。http://www.mhlw.go.jp/shingi/0112/s1213-2c.html
2　保健医療分野の情報化にむけてのグランドデザイン。http://www.mhlw.go.jp/shingi/0112/s1226-1.html
3　大学病院医療情報ネットワーク（UMIN）におけるインターネット医学研究データセンター(INDICE)。http://www.umin.ac.jp/indice/
4　EORTC data center. http://www.eortc.be/
5　日本未破裂脳動脈瘤悉皆調査。http://ucas-j.umin.ac.jp
6 日本高血圧学会会報。http://www.bcasj.or.jp/hr/hr_n22hp.pdf
7　Bruce Schneier. E-Mail Security: How to Keep Your Electronic Messages Private, 1995.
8　坂井司監修。宮脇訓春，加藤研也著。日本総合研究所編。電子認証が日本を変える，PKIで変わる暮らしとビジネス。生産性出版（東京)。2001.

疫学研究における情報漏洩防止システムのあり方についての検討（Ⅱ）
－プライバシー・ポリシー及びセキュリティ・マネージメント－

杉森　裕樹　聖マリアンナ医科大学

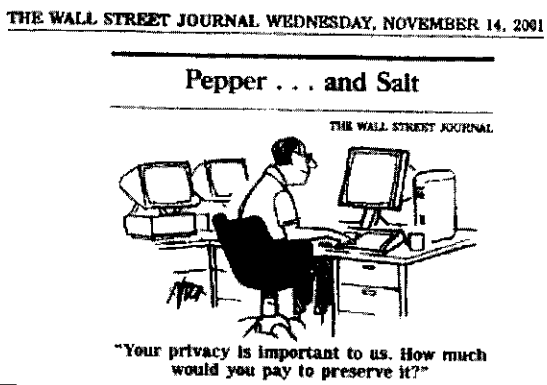
研究要旨

Webを用いた疫学研究において、望ましい情報漏洩防止システムを構築するには、外部からの脅威に対する技術的な対応だけでは不十分であり、内部の情報処理に対する管理体制の整備が不可欠である。本研究ではプライバシーマーク制度、BS7799、Information Security Management System（ISMS）、チーフ・プライバシー・オフィサー（CPO）を検討し、Webを用いた疫学研究における、望ましい個人情報保護の管理体制づくりのあり方を考察した。

研究目的

対象者の理解を得て疫学研究を遂行する上で、個人情報保護の条件は最低限担保される必要がある。Webを用いた疫学研究において、望ましい情報漏洩防止システムを構築するには、外部からの脅威に対する技術的な対応だけでは不十分であり、内部の情報処理に対する管理体制の整備が不可欠である。

近年、多くの民間事業者がWebページの中で、その事業者の個人情報に対する管理体制の姿勢を表明した文書、すなわち「プライバシー・ポリシー」を掲載している。（トップページの最下段にリンクが張られていることが多い）そのプライバシー・ポリシーの内容を見て、自分や家族の個人情報を提供すべきかどうかを個々人が判断できるようになりつつある。


THE WALL STREET JOURNAL WEDNESDAY, NOVEMBER 14, 2001

Pepper . . . and Salt

THE WALL STREET JOURNAL

"Your privacy is important to us. How much would you pay to preserve it?"

図１．The Wall Street Journal

しかしながら、あくまでも〝自己申告〟でありプライバシー・ポリシーを掲載していることが安全性を保証する訳ではない。その辺の事情を皮肉ったcartoonが昨年、The Wall Street Journalに掲載された。現時点での、ネット社会における個人情報保護の困難さや危うさをうまく表現している。（図1.「我々にとって、あなたのプライバシーは大切です。プライバシーを保護するためにあなたは、いくら支払ってくれますか？」）

本研究では、国内外のwebのプライバシー・ポリシー及びセキュリティ・マネージメントに関する、「第三者認定」や「ガイドライン（自主規制）」の動向を検討した。そしてWebを用いた疫学研究における、望ましい個人情報保護の管理体制づくりのあり方を考察する。（技術面については前項「疫学研究における情報漏洩防止システムのあり方についての検討（Ⅰ）」を参照）

方　法

プライバシー・ポリシー及びセキュリティ・マネージメントに関する、国内外の「第三者認定」や「ガイドライン（自主規制）」について、文献、インターネット等により検討した。

Ⅰ．1999年より通産省が導入したJIS Q15001とそのガイドラインに準拠した日本情報処理開発協会（JIPDEC）による「プライバシーマーク制度[1]

Ⅱ．BS7799[2]

Ⅲ．Information Security Management System (ISMS)[3]

Ⅳ．IBMコーポレーションのチーフ・プライバシー・オフィサー（CPO）[4]

結果および考察

Ⅰ．個人情報保護に関するコンプライアンス・プログラムの要求事項（JIS Q15001）準拠のプライバシーマーク制度（Pマーク）

財団法人日本情報処理開発協会（JIPDEC）は、1998年4月から通産省の「民間部門における電子計算機処理に係わる個人情報の保護に関するガイドライン」に準拠して、個人情報の取り扱いを適切に行っている企業に対して「プライバシーマーク（Pマーク）」の使用を第三者認定するプライバシーマーク制度を開始した。業界団体毎にJIPDECが認定した指定機関を設立し、業界に属する事業者がプライバシーマークを取得希望の時、この機関に対して取得の申請を行うものである。

事業者単位で付与され、JISQ15001に準拠した個人情報の取り扱いに関するコンプライアンスプログラム（個人情報保護措置：事業者が自ら保有する個人情報を保護するため方針、組織、計画、実施、監査および見直しを含むマネージメントシステム全体と定義される）に基づいて、従業員への教育と運用実績があることが認定の条件となっている。認定後も消費者からの苦情に基づいて、運用改善命令が出されるなど制度の実効性を保証する仕組みがなされている。

図２．Pマーク

Pマークの目的は、大きく分けて次の3点である。

① 個人情報の保護に関する、事業者・従業員の個々の意識の向上を図る

② 民間事業者の個人情報の取り扱いに関する適切性の判断の指標を各人に与える

③ 民間事業者に対してコンプライアンスプログラムへのインセンティブを与える

コンプライアンスプログラムでは、個人情報の特定、個人情報処理業務の把握、脅威の洗い出し、対処法の選定・評価・決定、運用・実行、レビューと言ったPlan、Do, Check, Action（PDCA）サイクルを継続的に行い、改善を図って行くことが重要とされる。（図3）

PDCAサイクルの結果、内部規定を定めることが重要である。以下の例は最低限盛り込むべきであろう。

a） 事業者の各部門および階層における個人情報を保護するための権限および責任の規定

b） 個人情報保護の収集、利用、提供および

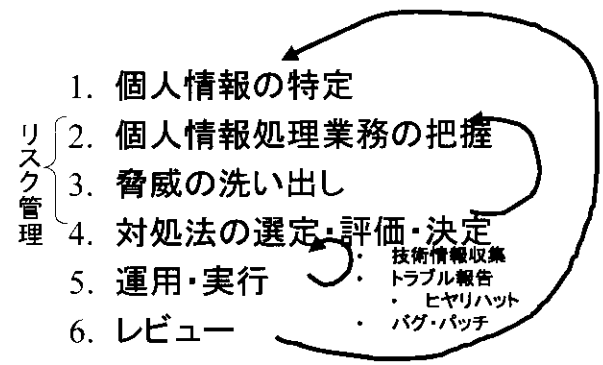


図３．大中小のPDCAサイクル（JIPDEC）

管理の規定

c) 情報主体からの個人情報に関する開示、訂正および削除の規定

d) 個人情報保護に関する教育の規定

e) 個人情報保護に関する監査の規定

f) 内部規定の違反に関する罰則の規定

図4に、各部門および階層における個人情報保護の権限・責任の組織体制の例を示す。また、以下のものは適切な文書管理が要求される。

1. 個人情報保護指針
2. 個人情報特定の手順
3. 法令その他の規範
4. 内部規定
5. 計画者
6. 役割・責任および権限
7. 情報主体に対する書面（直接、間接）
8. 情報主体からの同意の書面
9. 範囲外への利用・提供の場合の書面
10. 委託処理での契約書
11. コンプライアンス・プログラム
12. 監査報告書

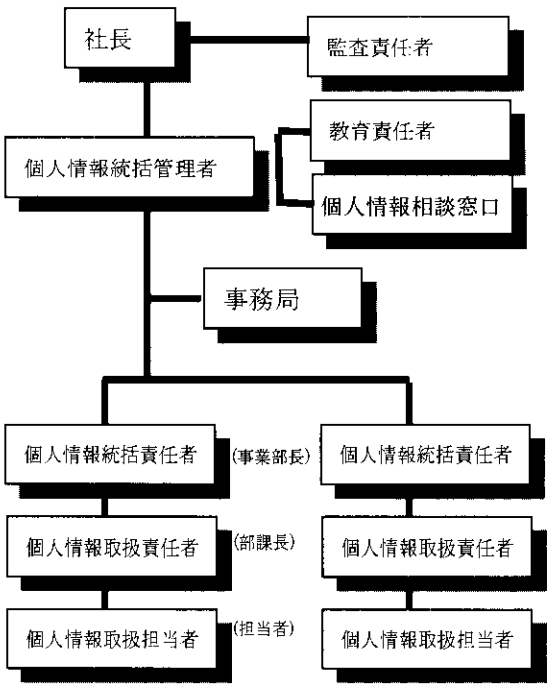


図4．個人情報保護に関する組織体制図

Pマークでは海外制度との相互認証出来る仕組みが進められている。米国との間でJIPDECとBBBOnlineが、それぞれ米国企業、日本企業に向け付与できるようになる。また現在シンガポールや韓国との間でも協議が進められている。

図5．BBBOnline

Ⅱ．BS7799

BSI（英国規格協会）によって規定される、企業・団体向けの情報システムセキュリティ管理のガイドラインである。

- BS7799-1：情報セキュリティ管理「実施基準」であり、ISO／IEC17799として発行
- BS7799-2：情報セキュリティ管理「システム仕様」であり、日本でもISMS（Information Security Management System）適合性評価制度として派生

BS7799はISO／IEC15408と並んで現在最も注目されているが、特にセキュリティの運用管理に重点が置かれている点が特徴である。また電子媒体に限定せず紙媒体など様々な情報資産をセキュリティの対象としている。

Ⅲ．情報セキュリティマネージメントシステム（ISMS：Information Security Management System）

JIS X 5080（国際規格ISO／IEC 17799：2000）及び前述したBS7799-2：1999（Specification for information security management system）を参照し、第三者の審査登録機関が本制度の認証を希望する事業者の適合性を評価するための基準である。以前の「情報処理サービス業情報システム安全対策実施事業所認定制度（安対制度）」に代わる評価認定制度である。現在、JIPDECを中心に運用されている。

ISMSは、技術対策とは別に、組織マネジメントとして自らリスク評価し、必要なセキュリティレベ

ルを定め、計画を立て、資源配分してシステムを管理運用するものである。また、「組織が保護すべき情報資産について、機密性、完全性、可用性をバランス良く維持し改善することがISMSの要求する主なコンセプトである」と設定している。

機密性・完全性・可用性とは、以下のような内容である。

機密性：アクセス権を持つ者だけが、情報にアクセスできることを確実にすること。

完全性：情報および処理方法が正確であることおよび完全であることを保護すること。

可用性：認可された利用者が、必要なときに、情報および関連する資産にアクセスできることを確実にすること。

ISMSの認定取得を希望する事業者は、JIPDECの指定する審査登録機関に、認定取得に当たっての申請を行い、ISMSに基づく審査と監査を行う。審査機関からの結果報告を受けて、JIPDECが事業者を認定済み事業者としての登録を行う。

ISMSの最大の特徴は「自主性」である。これまでの安対制度では、定められた基準を実施すればよいが、ISMSでは自社に適したものを選択して（＝ポリシー策定）、自らの責任で決めることが要求される。具体的には、ポリシー策定→ISMS適用範囲決定→リスク評価→管理リスク決定→管理策決定の5ステップを経て、実施に至ることになる。安対制度が、適用範囲決定→基準適用→実施の3ステップと比較すると、より深い調査作業が必要である。調査作業には、**リスク値**（＝**「情報資産の価値」**×**「脅威」**×**「脆弱性」**）のような客観的指標とリスク特徴を見極めて対策（リスクの許容、低減、移転、回避）を取る。

図6、7に、ISMSとプライバシーマーク制度の関係を示した。セキュリティのインフラがISMSであり、その整備のもと個人情報に関するコンプライアンスがプライバシーマークである。両者が整備されることで、より望ましい個人情報保護の管理体制づくりが為されうる。

Ⅳ. IBMのChief Privacy Officer（CPO）

IBMコーポレーションでは、2000年11月に、Chief Privacy Officer（CPO：最高プライバシー責任者）という役職をつくった。CPO（初代Harriet Pearson女史）は同社のプライバシー・ポリシーの策定・実施を指揮統括する。また、多くの事業部門や事業展開地域で進められているプライバシー対

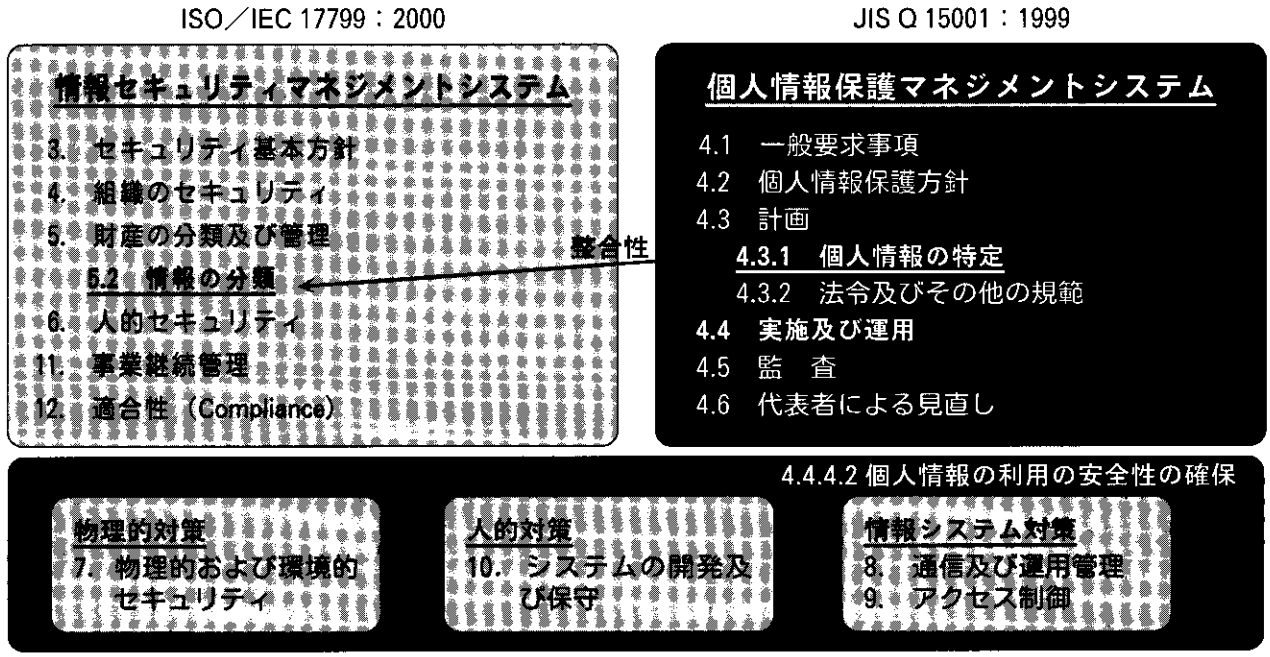


図6. Pマーク（JISQ15001）とISMS（ISO17799）の関係（JIPDEC資料）