解　説

プライバシーとデータ保護*

小笠原　謙蔵**

1. まえがき

コンピュータ利用に伴うプライバシー保護問題が世の関心を集めており，この関心は今後ますます増大するものと思われる．またこの問題は我が国のみならず，諸外国や国連などにおいても等しく関心の的となっている．

最近，行政管理庁によるプライバシー問題に関する意識調査が行われ，その結果が新聞で報道された．その中で少数の人々ではあるが，過去にプライバシーの侵害を受けた経験として次の事柄を挙げている．それらは特急券の二重売り，銀行預金やガス・水道・電力の料金，それに税金などの間違いである．手作業によって事務処理を行った場合でもこの種のミスは起り得る．ましてこれらの例は，プライバシーとは全く無関係である．

一般に情報公害とか，コンピュータのプライバシー問題として取り上げられる事柄は，その内容を吟味してみると，コンピュータの誤り，コンピュータに関係した犯罪，管理社会に対する不安・脅威といったものが漠然と含まれているように思われる．

コンピュータ・システムは多くの分野に導入され，広く使われており，直接・間接的に我々の日常生活と深いかかわりあいを持つに至っている．コンピュータの持つ高度の機能といったイメージから，ややもするとそれは万能であり，完璧なものであるという錯覚に陥る危険性がある．また，これまでコンピュータの機能と能率の向上を追求するあまり，その利用のもたらす社会的なインパクトについては，おろそかに考えるきらいがあった．

ここでは，プライバシーとデータ保護，それにコンピュータの完全性保持といった要素について，問題を明確に区別するとともに，データ保護対策についてふれ，さらに IBM の共同研究レポートの概要について紹介したいと思う．

2. 機械文明の発達とプライバシー

もともとプライバシーという言葉は，考えてみればきわめて曖昧な意味をもっている．だいいち，日本語に訳そうとしても，適切な言葉が見あたらないし，それに人によって違った意味をもつことがあるので，簡単に定義できそうもない．プライバシーの意味や，概念について論ずることはともかくとして，機械文明の発達とプライバシーの関係について考えてみることにしよう．

1890年に，アメリカ合衆国の D. ブランダイス判事は，機械文明のもたらすプライバシー侵害の脅威について Harvard Law Review に論文を寄せている．当時，議論の対象となった文明の利器は，新聞印刷機であり，カメラであり，電話であった．この事からも判る通り，赤外線カメラ，ラジオ，テレビ，テープ・レコーダー，複写機といった，およそ音と映像に多少とも関係のある機械の発明は，それらがもたらす便利さとともに，一方では常に個人に対するプライバシー侵害の恐れを併存して今日に至っている．しかもこれらの機械の普及は価格の低廉をもたらし，プライバシーの侵害をそれだけ容易なものとしてきた．

コンピュータが世に現われてから，およそ 20 年になる．その間，エレクトロニクス技術の発展はめざましいものがあり，情報処理システムの機能は，プログラム技術の発展とあいまって飛躍的に増大した．

1956 年から今日までの約 20 年間を見ると，百万字の情報を磁気ディスク上に 1 ケ月間記憶させておくための費用は，当時の 45,000 円から現在の 1,400 円へと 1/32 に低下した．同じように，磁気ディスク上の情報アクセス・タイムは，800 ミリセカンドから 30 ミリセカンドに，27 倍も速くなった．

---

* Privacy and Data Security by Kenzo OGASAWARA (I. B. M Japan Co., Ltd. Data Communication Relations Mgr.)

** 日本アイ・ビー・エム（株）データ通信企画担当

いうまでもなく，コンピュータは大量のデータを蓄積し，多目的利用のためのファイル構成能力を持ち，情報のダイナミックな管理を可能にし，記録情報に対する経済的な索引手段を提供する．

これらの能力の向上は，ファイルの集中化傾向を促進させ，データ通信技術の発展に支えられて多数の遠隔端末装置との間で，情報のやりとりを行うようになった．

情報処理システムは，今後ネットワーク化の傾向を強め，異なった地点に存在する複数の情報源を通信網を介して結合することにより，それらのリソースを相互に関連づけて働かせるようになるであろう．

情報処理システムの機能が増大し，利用技術とデータ通信技術が発展するにおよんで，これまでの手作業ではとうてい不可能であった情報の山の中から，必要な項目を抜き出し，意味のある関連性をきわめて短時間に，しかも経済的に見い出す有力な手段が提供されることになった．

コンピュータは，企業や行政機関において増大する情報処理の需要に対処する目的で，今後ますますその利用が要求されるであろう．しかし，コンピュータはその取扱う対象が情報であるだけに，機能の向上と広範囲の利用は，多くの不安と問題を社会になげかけることになる．

3. 情報化社会とプライバシー

行政，雇傭，医療，警察，福祉，流通といった分野で，情報処理システムが利用される場合，情報蓄積の規模が大きくなり，集中化がすすむにつれて，情報の多目的利用により能率は大幅に増大する．

しかし，一方では個人，企業および政府に関する各種の情報は組織的に記録され，それらの情報は常に機密の漏えいと悪用の不安におびやかされることになる．特に個人情報を含む大規模なデータ・バンクの設立は，もしその運用を誤ると圧制の道具となりかねない危険性をも含んでいる．

これまで個人情報に関するプライバシーの保護は，比較的容易であった．それは，伝統的に個人についての情報が大量に収集されることはなかったので，必要な情報が多くの場合完備されていなかったしたとえ入手可能であったとしても，それらは相互の関連なしに，独立した様態で記録・保管されてきた．したがって，情報の分散はそれ自体，情報の機密性に対する保護作用として働いてきたとみることができよう．

プライバシーの定義や概念は，きわめて曖昧で決めることのむずかしい事は前述した．しかし，あえて簡単にそれを言い表すならば，「他人に邪魔されずに個人生活をおくるための権利」とでもいうことができよう．

アメリカのウイリアム・プロッサーという学者は，かってプライバシーの侵害を次の四つの類型に分けている．すなわち，

(1) 一人でいたいという権利の侵害．
(2) 通常の礼儀を踏まずに他人の私事を公表すること．
(3) 作為的文書により，ある個人の考えに反することを伝え，誤ったイメージを一般に持たせること．
(4) 許可なく氏名や肖像のような，個人の人格的要素の一部を商売に利用すること．

これらの分類は，個人の信条，思想，感受性といったものを保護しようとする立場に立脚しており，それなりに適切と考えられる．しかし，これらの行為が防止されるとしても，コンピュータ・システムの中にいかなる個人情報が蓄積され，それらがいかなる目的に使用されるのか，といった人々の不安は解消できない．したがって以上のカテゴリーは，消極的な意味でのプライバシーの概念の把え方，ということができよう．

情報化社会におけるプライバシー保護とは，個人やグループに関するいかなる情報が，記録や処理のために収集され，それらの情報がいかなる目的に使用されるか，を問う法的そして社会的な問題であると考えられる．

この重要にして，むずかしい問題の検討にあたっては，処理方法がコンピュータによるもののみならず，手作業による場合も含め，広い範囲を想定する必要があろう．また，政府機関と他の組織による情報取り扱いの違いも，慎重に考慮する必要がある．

国民は，情報の提供と利用を認めることによって，福祉やサービスを期待しており，またそれと同時に，個人情報の利用について，監視と制限を行う権利を主張することになる．プライバシーの論議は，公的サービスを受益する権利と，個人情報の保護に関する権利を，いかにバランスさせるかという問題に帰結する．

プライバシー保護にかかわる要素には，次の事柄が含まれる．すなわち，

(1) どんな情報が，どのようにして集められるか．

(2) 誰によって，いかなる目的に個人情報が使われるか．

(4) 情報の内容確認，変更そして訂正は，どのように行われるべきか．

これらの課題に対する解答は，国民のコンセンサスによって決められるべきであり，法律，政治，教育，倫理面などの幅広い検討を必要とする．

4. コンピュータの性質と機密保護

情報処理システムは，すぐれた性能をもっている一面，他方ではきわめてもろい性質をもっている．

たとえば，操作の途中で電源電圧がごく短時間であっても，急激に変動するようなことがあると，データが消えたり，まちがったり，機械が動作しなかったりすることがある．それにもまして，電源を完全に停めてしまったら，さしものコンピュータも，手も足も出ないことになる．

磁石の一片を，磁気テープやディスクの表面に近づけるだけで，記録データは消去されてしまう．コンピュータ機器のある部分は，ちょっとしたほこりに弱いし，ときには動かなくなったり，まちがって作動したりすることがある．コンピュータやデータ記録媒体は，もともと火や水，それに温度（高温や温度差）に弱い性質をもっている．

プログラマーのほんのちょっとした不注意から，プログラムの作成過程で，あるいはオペレータが入力する過程で記号を一ヵ所間違えたとすれば，宇宙衛星ロケットの打ち上げは失敗するし，化学プラントは爆発の危険にさらされることにもなる．

コンピュータについて勉強し，プログラムやデータ・ベースへのアクセスを知っている者にとって，コンピュータ・コードを解読したり，データを横取りしたり，内容を変えたりすることは，さしてむずかしいことではない．

コンピュータは，企業や政府機関などで，それらの活動の中枢神経的役割をもって利用されている．大学の大型計算機センターや，丸の内の大企業のコンピュータ室が，過激派団体の格好の目標物として，ねらわれることも考えなければならない．このように微妙で，しかもきわめて脆弱な性質を有するコンピュータを破壊する方法は，なにも露骨な手段だけとは限らないであろう．

従来の手作業とファイルによる情報の保管方法に比較して，コンピュータにのせられる情報は，破壊や，不法介入や，漏えいに対して弱点をもつことになる．それらの要点を挙げると，次のようになる．

(1) 文字や数字で表示される情報をコード化し，入力する過程で，データは不法侵入の可能性のあるいくつかの操作段階を通る．

(2) 記録媒体には高密度の情報がつめ込まれている．磁気テープやディスクの内容は，証拠を残さずに短時間で複写されたり，横取りされたりする可能性がある．

(3) 企業などにおいて，最も価値の高い情報を集約して記録保管しているため，機密情報が競争相手に流れた場合，その影響が甚大である．

(4) 研究・開発に関する情報などの場合，産業スパイにねらわれる．

(5) 個人情報であっても，一たんコンピュータ・システムの中に取り入れられると，限られた目的だけに使われるとは保証されない．

コンピュータは，情報に対する不法侵入や，破壊に対してもろい一面をもっているが，他方コンピュータそれ自身，文字通りきわめて機械的，システム的であり，さらに高速性という特性から，各種の防禦措置を組み込みやすい特徴を備えていることも事実である．

5. データ保護について

データ保護の問題は，権限のない者により，故意または偶発的に，機密情報が暴露されたり，横取りされたり，破壊されたり，変えられたりすることから防ぐことであり，機密情報を保護する責任は，情報システム（コンピュータ利用のいかんを問わず）を管理する企業なり機関にある．

そこでは，どのような情報がいかに収集・記録され，また，誰がどのような目的に情報を使うかを決めるとともに，必要なデータ保護対策を立てる責任がある．

データ保護の対策としては，コンピュータ自身に関係する技術と，管理運営および保安環境といった周辺部分に関係するものがある．それらを列挙すると次のようになる．

(1) 記録方法について安全策を講じる．

(2) 情報へのアクセスを制御する．

(3) 利用者の権限を確認する．

(4) 利用者や端末機を識別・照合する．

(5) 情報を暗号化する．

(6) 入出力における不法介入を監視する．

（7） システムの稼動状況を記録・管理する．

（8） 出力資料の取り扱いを管理する．

たとえプライバシー侵害に対する法的・社会的整備が行われたとしても，実際に個人情報や機密情報を取り扱う情報処理システムとその周辺問題に，適切なデータ保護と保安対策が講じられないと，不法に情報がねじまげられたり，漏えいしたりする危険からまぬがれることはできない．

6. コンピュータの完全性について

データ保護対策が万全であっても，コンピュータ自体が信頼性の低いものである場合には，努力は無意味になる．したがって，この問題はコンピュータの信頼性の技術ということになろう．

ハードウェア上の故障，ソフトウェア上の不完全さのような内部の原因によって，コンピュータが間違って作動したり，記憶されているプログラムが，相互干渉によって破壊されたりすることから防ぐ問題がこれに該当する．

コンピュータの内部で，あるデータが消え失せてしまったり，間違えて処理を実行してしまったり，別のファイルを更新してしまったりする危険は未然に防止しなければならない．

コンピュータで使われる種々の検査機能から，情報の復元，操作の復元などの手法も，またこの問題に含まれる．データの変換，入力，集計，出力，伝送のそれぞれの段階で，完全性保持のためにいかに多くの考慮が払われているかを我々はよく知っている．

コンピュータの内部要因のみならず，コンピュータそのものや，磁気テープ，カードなどの記録媒体を，災害や破壊，紛失から保護する外部的条件も考慮しなければならない．

コンピュータの完全性をおびやかす主な原因としては，次の事柄を挙げることができる．

（1） ハードウェアのエラー

（2） コントロール・プログラム上のエラー

（3） アプリケーション・プログラム上のエラー

（4） 操作上のエラー

（5） 入力情報のエラー

（6） プログラム設計時の不適切なパラメータの設定

（7） 処理能力を超える負荷

（8） その他の外部要因

このように考えてみると，コンピュータにかかわる保護の問題は，プライバシー保護，データ保護それにコンピュータの完全性保持といった三つの要素から成り立つことがはっきりする．

これらの関連性は，情報処理システムが中心にあり，それを取り巻いて完全性保持の技術とデータ保護技術があり，さらに物理的な環境保全と管理運営上の対策が，それぞれ層をなして取り囲み，外周に法的・社会的環境整備が位置づけられると考えられる．

7. 技術面からみた保護対策

プライバシー保護を，コンピュータ・システムの中に組み込むことはできないが，データ保護とシステムの完全性保持を目的として，各種の方策をハードウェア／ソフトウェア上に組み込むことは可能である．もちろん，完全無欠なデータ保護対策をほどこすことは不可能であるが，ユーザはシステムの利用目的に応じて，かなりの範囲の手段の選択性を有している．

データ保護対策を考える場合，コンピュータのハードやソフトに関係する部分は，問題解決のほんの一部にしかすぎない．また，技術的に複雑な方法を使って情報にアクセスすることは可能であるが，一般にはもっと簡単な方法で情報を入手できる．したがって，高度の技術対策がほどこされたからといって，防禦は十分であると安心することはできない．

技術対策の多くは，管理運営上の手順と密接な関連性をもっている．次にデータ保護の具体的手法の主なものを挙げることにしたい．

（1） 記憶区域の仕切

システムに記憶されているデータ・ベースやプログラムに対して，記憶区域を仕切って割り当てる方法は広く利用されている．マルチプログラミングシステムにおいては，複数のプログラムの相互干渉を防ぐ上からもこの方法は有効である．

（2） 記憶内容の保護

記憶装置に読み込まれたデータおよびプログラムを，不法介入による変更や，横取りから守る目的でパスワードにより，情報へのアクセスを制限できる．

（3） 制御プログラムの保護

制御プログラムの中の重要な部分や，保護機構の組み込まれている部分については，特別の制御言語を使ってシステムを働かせることができる．

(4) 診断用プログラムの活用

オペレーション診断用のプログラムの中に，保護策が万全かどうかを試す手順を組み込んでおく方法である．機械のトラブル，またはプログラム上の欠陥により，機密情報が漏えいすることを未然に防ぐことにもなる．

(5) 鍵・バッジカードの使用

権限外の者による端末機使用を防止する目的で，鍵を取付ける方法は一般的である．銀行用窓口端末機には，この方法が使われている．バッジカードと照合手順を組み合わせる場合は，より確実な方法となる．

(6) 端末機識別コード

端末機の設置場所によって処理可能な業務の範囲を限定する．重要な情報の取り扱いは，特定の端末機から，決められた手順に従って入出力する．役席者端末がこの例である．

(7) パスワード／ロックワード

ユーザの識別番号とともに，与えられた権限レベルを確認する方法として，パスワードもしくはロックワードが使われる．これらのコードによって，特定の情報に関する検索や変更の権限を限定することもできる．パスワードなどのコードは，一定期間内に変更した方が安全である．

(8) 印字禁止機構

最近のキーボード印刷端末機や，ディスプレイ端末機では，機密コードやパスワードを入力したとき，印刷と表示を避けることができるように設計されている．

(9) 伝送の暗号化

オンライン・システムにおいて，データ伝送上の機密保護のために，伝送符号を暗号化することができる．銀行用の自動現金引出機においては，必要な場合暗号装置が取付けられる．またこれに類する技術として，伝送エラーの検出や復元を目的とした検査方式がいくつか挙げられる．

8. 管理面からみた保護対策

管理運営面からの対策は，情報の保管・処理を行う組織の性格によって，いくらかの違いがあろう．しかしここでは，一般的な保護対策として重要な点のみを取り上げることにする．

広い意味での管理面からみた保護対策には，設備上の保安問題も含まれる．火災，水害，地震といった災害から，データとシステムを護り，バックアップと回復について考えることは重要な課題であるが，これらの点については紙面の都合で割愛したい．

手作業による情報処理の場合においても，情報管理の目的は，情報の紛失，まちがい，不正，欠陥といった事柄を未然に防止するか，または直ちに発見できるようにすることにある．これに対する有力な手段は，情報がどのように変化したか，追跡検査ができるような手順を講じておくことである．

情報管理は，入力，処理，出力および手順についての四つに大別される．

手順上の管理について，もっとも重要な事は，責任分担体制の確立であろう．責任の分担は，不正の防止や発見に役立つばかりでなく，エラーの発見にも有効である．

機密情報へアクセスした記録を保存しておき検査する方法や，ルールに違反するような事象がたび重なって発生する場合に分析データを記録する方法がある．疑わしい状態が検出されたとき，強制的に操作を中断させたり，ロックしてしまう手段を組み込むこともできる．

情報処理システムの稼動状況を記録しておくことは，システム・リソースの不正使用を発見できるばかりでなく，システムの効果的運用面からも重要である．

多くの企業においては，情報処理の管理面を専門に担当するグループを設定し，計算機室に出入りする業務の流れを調整するとともに，結果のチェック，入出力資料の管理，プログラム・ライブラリーの管理などを行っている．

情報処理の過程で，処理されずにはじき出された例外データの取り扱いは，ルーティン・ワークのいそがしさにまぎれて，十分な注意が払われていない場合が多い．これらのデータは，エラーや不正の原因となることがあるので，訂正や解決のための明確な手順を決めておく必要がある．この段階における手順をおろそかにすると，機密情報の漏えいにつながる盲点を残すことになる．

データ通信による遠隔情報処理を行っている場合には，管理面からも特別の考慮を必要とする．その一例として，ユーザを確かめる意味で，端末装置から識別コードを入力すると，コンピュータ・システムは一た

ん通信回線の接続を切断し，システム内の照合ルーティンを通して自動的にコールバックする方法がある．

その他，処理終了時にコア・メモリに残っている記憶内容を消去するとか，入出力資料の取り扱いについてルールを確立するとか，機械室への出入りをバッジカードで記録しそれをコンピュータでチェックするといった事柄は基本事項である．特に磁気テープや，ディスクパックなどの可搬物は，不正持ち出しに対して防止策を考えるべきである．

9. IBM の共同研究レポート

アメリカの 1972 年 Spring Joint Computer Conference において，IBM の当時の会長リアソン氏は，データ保護に関する調査と研究のために，向う 5 年間にわたって 4,000 万ドルの投資を行うと発表した．

この投資の一部は，2 年間の共同研究に費やされ，その研究成果が報告書として 1974 年に発表された．MIT，イリノイ州，TRW 社の 3 つの外部機関と，IBM の FSD (Federal System Division) の合計 4 ヵ所が委託研究の対象となった．

MIT における研究は，主として Authorization の問題であり，与えられた仕事に必要なシステム・リソースに限ってユーザに使用させるためには，いかなるコントロールを必要とするかについて研究した．

イリノイ州マネージメント・インフォメーション部における研究は，データ保護のための必要条件と経済性の問題に焦点をあて，コストと事務上・組織上の効果について研究した．

TRW 社における研究は，システムが実際にどの程度安全であるか，計量的に把握する問題を追求した．

IBM の FSD は，多数の端末装置とマルチプログラミングを使用した現有の大型情報処理システムに，複雑な保護対策を組み込んだ場合，オペレーション上の能率低下とインパクトはどうなるかを測定した．

MIT の研究チームは，問題の調査研究にあたって次の 3 つのアプローチを採用した．

第一は，学内のユーザがデータにアクセスする際のコントロールを行う Authorization 機構を取り上げ，アクセス制御の一般的な問題点の探究を行った．この成果は，データ保護のためにオペレーティング・システムは，どのような条件と機能を備えていなければならないかを示す重要な資料として役立つであろう．

第二に，大学は金融，医療，教育，データセンターといったそれぞれの分野において，データ保護の実状と関心度について調査を行った．

第三に，調査研究の成果と学内のコンピュータ・センターにおける，RSS (Resource Security System) を使用しての経験をつき合わせ，アクセス制御を通してデータを保護する具体的な手法を開発し，実行している．

イリノイ州の研究では，州政府としての立場から，各州において情報が収集・管理されている環境で，プライバシー保護法といった政府の法的措置によって，行政事務処理が規制される際に直面するいろいろな問題について研究した．

問題を一般化し，具体的な解決方法や必要な対策について多くの提案がなされている．したがって，その成果はプライバシーとデータ保護について，行政機関のみならず他の一般分野において，有益な資料を提供することになろう．

イリノイ州の SAFE という名の研究チームは，この問題の重要性を人々に認識させるためには，環境作りが重要であることを認め，教育用のビデオテープ 9 巻を開発した．

またプライバシーとデータ保護は，トップマネージメントの関心なしには達成できないという立場から，組織，予算，監査といった面で 10 ステップのチェックポイントを提案している．

TRW 社の研究は，コンピュータ・システムの各種の脆弱性について分析している．同時にそれらの弱点をカバーし，保護するためのハードウェア／ソフトウェア上の要件と技術について，詳細に研究している．また，コンピュータ・システムについて，完全性に関する必要条件を満たしているかどうかを評価し，保証を与える際のいろいろな困難な問題点を論じている．

研究報告書によると，もっとも信頼性の高いシステムは，コンピュータの OS に，最初から設計の一部として，信頼性の技術とデータ保護策を組み込んだものでなければならず，後から付け加えただけでは不十分である点を指摘している．

TRW System Group は，広い分野において，コンピュータ・システムの設計開発と運用に，豊富な経験を有しており，ハードウェアから OS にいたる広い観点から，コンピュータ・システムの信頼性について研究している．

OS のテストに関する提案や，モジューラー・プログラミング，トップダウン・プログラミングなど，いろいろなシステム開発手法について，一般ユーザにと

っても興味深い内容を報告している．

IBM の FSD は，RSS の導入と使用経験にもとづく各種の提案を報告している．RSS は MIT，イリノイ州，TRW 社でも使用しており，それらの使用経験もまとめて報告されている．RSS は実験的な試みであるが，今後のアクセス制御の手段を開発する上で，その使用経験は大いに役立つことになろう．

これらの研究は，データ保護問題のほんの一部の疑問に答えるものであり，完全な解決策を提示しているわけではない．しかし，プライバシーとデータ保護について，いろいろな観点からなされた今回の研究成果は，今後さらにこれらの問題を研究し，検討する上で貴重な示唆を与える資料となろう．

なお MIT の報告書の巻末には，コンピュータとデータ保護に関する，尨大な参照文献のリストを提供している点を付言しておきたい．

10. むすび

これまで主に，プライバシーとデータ保護にかかわるいろいろな要素について，問題点を明確に区別することを目的として述べてきた．

情報処理システムと利用技術について，深いかかわりあいを持つ我々にとって，これらの問題の解決にはたすべき役割について考えてみたい．

プライバシー保護について，情報処理システムの特徴と利用面における功罪を認識し，プライバシー問題の健全な世論の喚起を行い，政府やその他の機関による個人情報保護に関する検討や，立法活動に積極的に協力することである．

例えば，行政事務処理において，手作業による場合とコンピュータ利用による場合を比較して，いかなる個人情報が，いかにして集められ，それらがいかなる目的に使われているかといった調査研究を実施することが，大学やその他の機関に期待されよう．

さらに，プライバシー保護について法的措置が講じられた場合，我々は法の理念を遵守し，コンピュータの利用者に適切なアドバイスを与える責任がある．

データ保護と完全性確保の技術について，コンピュータ・メーカのはたす役割はきわめて大きい．情報処理システムで取り扱われる情報の種類や，管理運営上の規則について，メーカは決めることはできないが，利用者がシステムを導入する際に考慮すべきデータ保護対策について，メーカは適切な助言と援助を提供する立場にあり，またその義務をもっている．

コンピュータ利用のもたらす，社会的な利益とサービスを向上させ，罪悪面を抑制するために，我々に課せられた責任は重大である．

参考文献

1) The Considerations of Data Security in Computer Environment, IBM 出版物 G 520-2169
2) The Considerations of Physical Security in a Computer Environment, IBM 出版物 G 520-2700
3) Data Security and Data Processing (7冊) Vol. 1, Introduction and Overview G320-1370; Vol. 2, Study Summary G 320-1371; Vol. 3, Part 1 Executive Summary G 320-1372; Vol. 3, Part 2 Study Results; State of Illinois G 320-1373; Vol. 4, Study Results; Massachusetts Institute of Technology G 320-1374; Vol. 5, Study Results; TRW Systems, Inc. G 320-1375; Vol. 6, Evaluation and Installation Experience; Resource Security System G 320-1376
4) 「情報産業における秘密保護調査報告書」，日本情報開発協会（昭和44年6月）
5) "情報化とプライバシー特集"，「データ通信」誌（1975年1/2月合併号）
6) IBM Data Security Forum, Denver, Colorado (Sep. 1974, G 520-2965-0)
7) 米国 IBM 副社長 ルイス・ブランスコム："プライバシーとデータ保護"「無限大」IBM 出版物，No. 20 (1974年9月)

（昭和50年4月4日受付）