公共データベースセンタにおける機密文書管理システムの提案

山田道夫† 富永英義†

本論文では，公衆網を介してアクセスされる公共データベースセンタが，複数の無関係な個人／組織によって，各自の機密保護を要する文書の管理・共有のために利用される場合に，センタのファイル管理機能を貸し金庫の概念に基づき，契約を行った正当な利用者だけに貸し出すことのできるシステムを提案する．そして，セキュリティに関する問題の一部である，登録される文書の漏洩およびセンタ機能の不正利用を解決するために，それぞれ登録文書に対するアクセスをその文書の正当な所有者あるいは正当な組織の人物のみに可能とする方策，およびセンタにおける文書の入出力・管理制御方式に対する具体的な一解決策を述べる．システム機能の実現に当たり，センタにおける認証処理の低減，身体的特徴を用いた本人確認による安全性の向上，文書登録／取り出しの許可条件の工夫と文書ごとの登録期間の指定による利便性の向上を考慮している．また，システム機能を検証するために構築した実験システムの概要とそれによる評価結果について述べる．暗号化により情報内容の機密保護を行う点に関しては従来の方法に委ね，本論文ではアクセス機能に重点をおく．

Secure Document Management for Public Database Center

MICHIO YAMADA† and HIDEYOSHI TOMINAGA†

This paper proposes how to establish a safe-deposit box system for private/group usage document, considering on keeping real security using public common database connected to a single universal network. To realize real secure system in open facility, there are two main problems, leakage and illegal occupation. The leakage means the content of document can be thrown out by somebody who is not the authorized person. The illegal occupation means an injured function of database management occurred by mass of prescribed message that have been kept and are increasing in the database storage. As one of the methods against these threats, smart card and Token are used in this system. Smart card is used for access control in terminal side. Token is data which authenticate a registered customer in database side. So private document is deposited in database securely, where deposited document is taken out only by legal user.

1. はじめに

半導体技術の進歩に伴い安価で高性能なパソコン・ワープロ等のOA機器が多数開発され，文書処理をはじめとする各種業務の効率化・合理化のためにオフィスや家庭へ急速に浸透し，OAによる情報管理システムの構築が盛んになされている．このようなシステムにおける大量の文書の入出力を行う端末は，ISDNに代表される高機能化・統合化が進むネットワークによって有機的に接続され，情報の交換・蓄積・共有がなされている．このことは，情報リソースに対してネットワーク加入者が相互に自由にアクセスできるという利便性がある反面，不当な利用者が情報の改ざんや不当な入手を行う危険性をもっていることを示している．特に，成績・財産等の個人のプライバシーを含む情報，開発・取引・人事等の重要書類等の特定個人または特定組織内で機密保護を要する情報，および特定の会員のみに有償で提供される情報を安全かつ合理的な手段で個人対応に蓄積・管理・共有することは，個人や組織の社会活動を円滑に営むために解決すべき問題の一つであるといえる．

組織として外部に知られたくない重要書類を共通のデータベースセンタに登録し，統合化されたオープンネットワークを介して正当な組織の人間が自由に共有し利用することが望ましいが，そのようなシステムを実現する場合に，現状においてはネットワークの機能を含めて物理的に閉じた構造にならざるを得ない．本論文では，貸し金庫の概念に基づき，個人あるいは組織ごとに機密保護を要する重要書類を，公衆網を介し

† 早稲田大学理工学部電子通信学科
School of Science and Engineering, Waseda University

て不特定多数の利用者がアクセスできる公共のデータベースセンタに登録し，正当な所有者や正当な組織の人物だけが自由に取り出し，共有できるシステムを提案し，安全かつ合理的な構成法に関する検討を行う．公共データベースの目的である情報の共通利用という面と，個人情報の機密性とはお互いに相反する性質を持っているため，アクセス，伝送，蓄積の各機能において，個人や組織ごとのプライバシーを保護するとともに，文書管理のセキュリティを確保する機能の実現手段を見出すことが本論文の課題である．

2. 提案システムの概要と位置付け

2.1 システム構成とその特徴

機密文書の管理形態としては，ハードコピーや記憶メディアを物理的な手段で保護された保管庫や保管室に格納するものや，ホストコンピュータに接続した個人・組織専用の記憶装置を用いるものなどが広く利用されている[1]．これらは構造的に閉じているため，一定領域あるいは一定組織の範囲内における利用に限定される．

一方，本論文で提案する公共データベースセンタを用いる管理形態はオープンな構造であり，アクセス地点の自由度が高く，個人情報の管理，特定組織内における機密文書の共有に都合がよい．また，センタを地震等の自然災害が少なく人間の活動条件と分離した場所に設置することで，システムにとって好ましい環境条件のもとで情報の管理を行うことが可能である．必要性を感じながらもコストの問題から自前のバックアップ設備を所有することができない事業体も多く，本システムは共同利用型バックアップセンタの要求[2]にも応えることができる．本論文では，公共のデータベースセンタのことを DMC とよぶ．これらの管理形態のイメージを**図1**に示す．

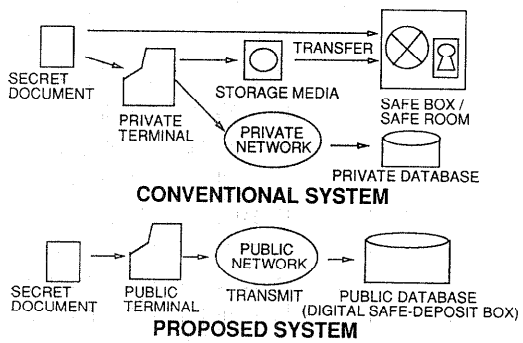


図 1 機密文書の管理形態
Fig. 1 Concept of secure document management.

本システムの主要な構成要素の前提条件を以下に挙げる．

(前提条件1) DMC，ネットワークおよび端末は公共性を有する．

(前提条件2) DMC は貸し金庫の概念に基づき，契約によってファイル管理機能を貸し出す．

(前提条件3) DMC は第三者的機関によって管理・運営され，DMC 管理者（プログラムでもよい）は決められた文書管理手順を不正なく実行する点では信頼できる．

(前提条件4) DMC が蓄積できる情報の容量には限度がある．

2.2 セキュリティに関する問題点

前提条件1により，本システムにはセキュリティに関する問題が数多く存在している．その中でも，本論文で対象とする主要な問題を以下に挙げる．

(問題点1) 利用者のプライバシー情報の漏洩，改ざん

伝送・蓄積される文書情報に対し，第三者が内容の不正入手や改ざんを行う危険性がある．また，登録される文書の所有者やタイトル等のプロファイル情報および利用履歴等の利用者のプライバシーに関する情報が，DMC の管理者やオペレータを含む第三者に対して漏洩するという問題も存在する．特に，システム管理者側からの流出は深刻な問題となっている[3]．

(問題点2) DMC のファイル管理機能の不正利用

DMC は公衆網から容易にアクセスできるため，利用契約をしていない者が不正に文書を登録したり，契約を超過して大量の文書を登録するという不正行為が可能となる．

2.3 システムが具備すべき機能とその設計条件

これらの問題を解決するために必要な主要機能を以下に挙げる．問題点1は機能1，2により，問題点2は機能 3，4，5 により解決される．

(機能1) 利用者の契約の有無および本人の正当性を認証する機能

(機能2) 登録文書内容およびそのプロファイル情報の機密を保護する機能

(機能3) DMC における文書の入出力制御機能

(機能4) DMC のオーバフロー防止機能

(機能5) DMC の利用に応じた課金機能

また，各機能の実現手段の検討に当たって考慮すべき点として以下の設計条件を設ける．設計条件1，2

は問題点1から導かれるものであり，設計条件3は前提条件1から必要となるものである．

(設計条件1) DMC 管理者は，利用者名や認証情報等の利用者に関する情報を管理せず，利用者の識別は行わない．

(設計条件2) DMC 管理者は登録文書およびプロファイル情報の内容を判読できない．

(設計条件3) DMC における認証処理が少なく，負荷の集中が抑えられている．

3. 各機能の実現手段

3.1 機 能 1

機能1はDMCの文書管理サービスの利用を要求する人物が，正規の手段で正しく契約を行っている本人であることを確認する機能である．

3.1.1 従来方式とその問題点

従来より本機能は，アクセス要求ごとに，アクセス要求者があらかじめ登録されているかどうかを確認する利用者識別処理と，既登録の場合に，その要求者が登録さする利れている真の利用者自身であるかを確認用者認証処理をセンタ側で実行することで実現されている[4]．この方法を本システムに用いた場合には，設計条件1が満たされない．また，DMC 側で利用者ごとのアクセス権チェックを行うため設計条件3も満たしているとはいいがたい．

3.1.2 本システムで用いる方式

IC カードによる端末側でのアクセス制御 本システムにおいては，端末において IC カードを用いたローカルなアクセス制御を行う．ただし本論文で用いる IC カードは，演算機能はなくメモリ保護機能のみを有するタイプとする．IC カードをシステムで利用する際には，その安全性を確保するために，利用される度に以下に挙げる2段階の認証を行う必要がある[5]．

(認証1) IC カードの利用者認証

IC カードを使用している者が，その IC カードに登録された真の所有者か否かを確認すること．

(認証2) IC カードの正当性認証

利用される IC カードが偽造されたものでなく，正規の手段で発行されたものか否かを確認すること．

認証1は利用者と IC カード間の認証，認証2は IC カードとシステム間の認証に分離して考えることができる．これらを一連の手順として捉えることも可能であるが，分離した確認手続きを行うことによって，複数の許可レベルを設定したサービスを提供することが可能となる．例えば，金融機関の現金自動入出金システムでは，入金処理はカードあるいは通帳があれば誰でも行える一方，出金処理は暗証番号による本人確認を行うようになっている．本システムにおいてもこの考え方に基づき，

- 正当な IC カードを利用している者は誰でも，文書を DMC に登録することができる．
- IC カードの正当な所有者のみが，DMC に登録された文書を取り出すことができる．

というアクセス制御を行う．すなわち，文書登録作業の代行が可能となり，システムの安全性を大きく低下させることなく利便性を高めることができる．このようなアクセス制御を実現するためには，文書登録時には認証1のみを行い，文書取り出し時には認証1および2の両方を行えばよい．

IC カードの利用者および正当性の認証方式 認証1のためには従来より利用者の記憶に頼る暗証情報が用いられているが，この方式は他人の暗証を入手することでなりすましが容易に行えることから，安全上問題があることが指摘されている．この対策の一つとして，個人の身体的特徴から生成した個人確認情報 PIN を利用する方式が注目されており[6]，本システムにおいてもこれを用いる．代表的な個人の身体的特徴としては指紋，顔および声紋等が挙げられ，筆者らはすでにこれらを用いて個人を確認するための具体的なアルゴリズムについて検討を行っている[7),8)]．

認証2のためには，従来より登録センタの認証情報が IC カード内に書き込まれている．しかし，この方法では認証情報が漏れた場合に IC カードが容易に偽造可能となる．これに対し本システムでは，ローカルにカードの正当性を確認するための一手段として透かしの概念を適用する．一般に透かしは，紙幣や有価証券等の正当性を確認する手段として利用されており，透かしを作成・付与できるのは正規の発行機関のみであるが，透かしの有無および正当性を確認することは，毎回発行機関に問い合わせなくとも容易に行えるという特徴を有する．すなわち，カードの認証情報が漏れた場合でも，それを透かしとして含む PIN を作成する方法が知られない限り，IC カードの偽造は行えないという考え方に従う．これを実現するための一アプローチとして，PIN に含まれる身体的特徴の入力誤差の範囲内で，認証データを透かしとして PIN に埋め込む方式が提案されている[9]．

3.2 機 能 2

機能2はネットワーク内伝送時およびDMC内蓄積時のそれぞれにおける，登録文書内容およびそのプロファイル情報の漏洩および改ざんを防止あるいは検出することである．

3.2.1 漏洩対策

漏洩対策として暗号を用いる点では従来と同じである．暗号方式には秘密鍵暗号方式および公開鍵暗号方式があるが，利用者と公開鍵暗号の対応リストを必要とする後者は設計条件1を満足しないことから，本システムにおいては秘密鍵暗号方式を用いる．

従来方式とその問題点

[伝送時] 秘密鍵暗号方式を用いる際には，通常は送受者間で同一の鍵情報が共有される．この場合，本システムにおいては利用者またはDMCが送受者に相当するため，DMC管理者が登録文書の内容を解読することが可能となり設計条件2を満足しない．

[蓄積時] 通常は蓄積データの暗号化はなされず，3.1.1で述べたセンタ側における利用者の識別と認証処理の後，センタ側において利用者およびデータごとのアクセス権限を規定したアクセス行列[4]によるRead権のチェックが行われる．システム管理者はすべての情報に対するアクセスが許されるため，すべての設計条件が満足されない．

本システムで用いる方式 登録される文書情報Mおよびそのプロファイル情報Hは伝送時および蓄積時ともに，個人あるいは組織ごとに固有の値をとる鍵情報Kuで以下のように暗号化された後にDMCに送信される．

$$Cm=E(M, Ku),\quad Ch=E(H, Ku). \qquad (1)$$

Eは暗号化関数である．Kuは各利用者のICカード内で安全に管理されるため，登録文書が他人の手に渡った場合でも解読されることはない．

また，本システムでは登録文書のセキュリティレベルに応じた管理を，Kuの種類を変えることによって実現する．すなわち，自分以外の誰にも知られたくない文書には自分のみに固有の秘密鍵を，組織内で共有されるべき文書にはその組織のみに共有される秘密鍵をKuとして用いる．この方式はDMCにおけるアクセス制御を一切伴わないため，設計条件3の達成度が従来方式より高い．なお，組織ごとに異なる鍵は，組織が固定的に決められる場合にはカード発行時に，組織が流動的に変化する場合には従来のグループ鍵生成方式[10]などを用いて共有され，組織名とともにKuリストとしてICカードに書き込まれているものとする．

3.2.2 改ざん対策

改ざん対策は本システムにおいても従来方式をそのまま適用することができる．

[伝送時] 認証子照合法によるメッセージ認証機能[11]を用いる．

[蓄積時] DMC内のデータベースに対する読み出し，書き込みはDMC管理者のみができるものとする．すなわち，すべての利用者はDMCのデータベースに直接アクセスすることは許されず，文書登録／取り出しサービスをDMC管理者に要求することのみができるものとする．

3.3 機 能 3

機能3は，DMCに対する文書登録／取り出し要求が，正しく契約を行った利用者から送られたものであることをDMC側において確認することである．この機能が必要となる理由は，機能1が端末側で実現されることを考慮すると，DMCは公衆網に接続されていることから，未契約者が3.1.2で述べたようなアクセス制御機能をもたない端末（以降，非正規端末）を利用して，文書登録／取り出し要求をDMCに送信することにより，文書管理機能の不正利用を行うことが可能となるためである．

3.3.1 従来方式とその問題点

本機能は従来，アクセス行列によるWrite権（文書登録時）およびRead権（文書取り出し時）のチェックにより実現されているが，この方法を本システムに適用した場合には機能1と同様に設計条件1，3が満たされない．

3.3.2 本システムで用いる方式

DMCにおける文書の入力制御 本システムでは機能3の一実現手段として切手の概念を用いる．切手は郵送料金を支払済みであることを郵便局に対して証明するものであり，切手から得られる情報だけでは差し出し人を識別することはできない．これと同様に，DMCに登録する文書データのヘッダ情報として，利用契約済であることを示すデータを付加すれば，DMC側で文書の登録資格が確認できる．本論文では，切手に相当するデータをトークンと呼ぶ．トークンTは利用契約時にICカードに格納された状態で与えられ，文書登録時に読み出される時には，通信ごとに異なるワーク鍵Kw[12]で暗号化される必要がある．

すなわち利用者側において，

$$Ct=E(T, Kw). \quad (2)$$

のように暗号化したトークン Ct を登録文書とともに DMC に送信する．ワーク鍵を用いるのは，固定の鍵で暗号化されたトークンを不正に入手した第三者が，それを後に再び使用することを防ぐためである．ワーク鍵の生成手順は 4.2 で述べる．

トークンのチェックにパスした文書に対してはトークン情報を取り除き，文書登録番号 RN を付与し，DMC 内のランダムに選んだアドレスに格納する．RN は DMC によってランダムかつユニークに決定され，文書を検索する際のインデックスとして用いられる．文書格納アドレスと RN をランダムに決定するのは，これらの情報を手掛かりとする特定文書に対する不正行為を防ぐためである．

DMC における文書の出力制御 文書取り出し要求に対しては，DMC においてなんら認証処理を行うことなく，指定された登録文書のコピーを送信する．これは，登録文書は Ku で暗号化されており，たとえ非正規端末を用いて第三者に不正に取り出された場合でも，内容を解読されることはないためである．

以上のように，DMC 側における認証処理は文書登録時のトークンのチェックによる利用契約の確認のみとなるため，設計条件 1 が満たされており従来方式より設計条件 3 の達成度が高い．

3.4 機 能 4

機能 4 は DMC 内に蓄積不要となった文書を消去することである．この機能が必要となる理由は，機能 3 の文書取り出し要求に対しては指定された文書のコピーを返送するため，DMC 内に登録される文書の量は増加する一方であり，前提条件 4 によりオーバフローとなるためである．

3.4.1 従来方式とその問題点

従来，各利用者ごとに利用可能な記憶領域の総容量を設定したテーブルを用いて，データ書き込み量を制限する方法が知られているが，これは設計条件 1.3 を満たさない．このほか，すべての登録データに対して一律に蓄積期間を設定する方法があるが，これは利用者の利便性を考えると好ましくない．

3.4.2 本システムにおいて用いる方式

本システムでは，利用者によって文書ごとに設定される登録期間 DP に基づく蓄積制御を行う．具体的には，DP と登録時刻から算出される登録終了期日 ED を登録文書のヘッダ情報として追加し，DMC 管理者は定期的に各文書の ED をチェックすることで登録期限が到来した文書を消去する．

3.5 機 能 5

機能 5 は各利用者から DMC の利用量に応じた使用料金を徴収することである．

3.5.1 従来方式とその問題点

各利用者ごとに決められた利用可能なセンタの記憶領域に応じて，その利用料を徴収する方法が一般的だが設計条件 1 が満たされない．

3.5.2 本システムで用いる方式

本システムでは，サービスの利用に先だって料金を徴収するいわゆるプリペイド方式を採用する．このため，登録可能な文書量を規定する登録可能度数 TDP を導入する．TDP は利用契約時に各利用者の支払う利用料金に応じて IC カードに書き込まれる．文書登録ごとの課金は，DP と登録文書の容量から算出される実質課金度数 RDP を TDP から差し引くことによってなされる．各利用者が指定可能な DP の大きさは，各利用者の契約の範囲内に押さえられる必要があるため，RDP が TDP を越えるような DP の指定は許されない．また，文書取り出し時には取り出した容量に応じて決められる度数 P が TDP から差し引かれる．

4. 各プロトコル

4.1 IC カードの利用者および正当性の認証手順

利用契約時に IC カードに書き込まれる登録 PIN (PINreg) は，登録センタにおいて次式に従って得られる．

$$PINreg=f(g(PH), S, Kd). \quad (3)$$

g は利用者から入力される身体的特徴 PH から PIN を生成する処理，f は透かし情報 S を PIN に埋め込む処理を示す．また，Kd は S を PIN に埋め込む際の鍵情報であり，登録センタにおいて秘密に管理される．認証手順を以下に述べる．

1. 端末は IC カードに対し，PINreg の読み出し要求とともに正規端末であることを示す認証情報 Kt を送る．
2. IC カードは Kt をチェックし PINreg の読み出しを許可する．

［認証 1］

3. 端末は処理 g により，入力された PH から PIN を生成する．これを入力 PIN (PINlive) とする．
4. 端末は PINreg と PINlive を照合し，一致している場合に利用者が IC カードの正しい所有者で

あると判定する.

[認証2]

5. 端末は処理 h と Ke により PINreg から透かし情報を抽出する. これを S′ とする.
   h および Ke は PINreg から透かし情報を抽出する処理および鍵情報である. Kd≠Ke かつ Ke から Kd を容易に求めることができなければ Ke を公開することができるが, 現時点のアルゴリズムでは Kd と Ke は等しいため, Ke は端末内に秘密に保持される必要がある. この点に関しては今後の課題に委ねる.
6. 端末は S と S′ を照合し, 一致している場合に IC カードが正当であると判定する.

4.2 マスター鍵およびワーク鍵の生成手順

ワーク鍵 Kw を共有するために必要なマスター鍵 MK は, 各利用者の IC カードに格納される. 本システムでは DMC にマスター鍵ファイルを管理することが不要な個別鍵方式[13]を利用する. 利用者 i のマスター鍵 MKi は, 利用契約時に登録センタによって次式に従って生成され, Ri と MKi が IC カードに書き込まれる.

$$MKi=E(Kc, Ri). \quad (4)$$

ただし, E は暗号化関数, Kc は登録センタおよび DMC の秘密鍵, そして Ri は利用者ごとに異なる乱数である. 以下に, DMC の正当性認証手順を含む Kw の共有手順を述べるとともに図2に示す.

1. 端末は乱数 RR を生成し, IC カードから Ri を読み出した後, RR, Ri および端末 ID (TID) を DMC に送信する.
2. DMC は式(4)を用いることによって MKi を生成し, RR を次式のように MKi で暗号化する.
$$Crr=E(RR, MKi). \quad (5)$$
3. DMC は乱数 Kw を生成し, 次式のように MKi で暗号化した後, Crr, Ckw を端末に送信する.
$$Ckw=E(Kw, MKi). \quad (6)$$
4. 端末は受信した Crr を復号化関数 D と MKi を

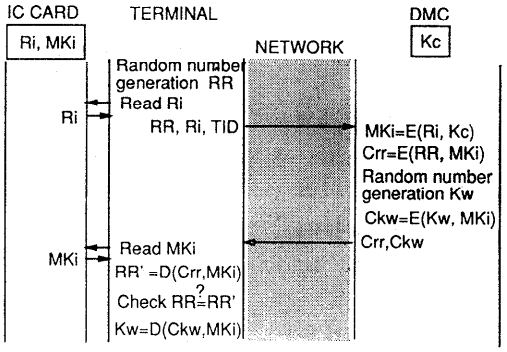


図2 ワーク鍵の生成手順
Fig. 2 Work key generation process.

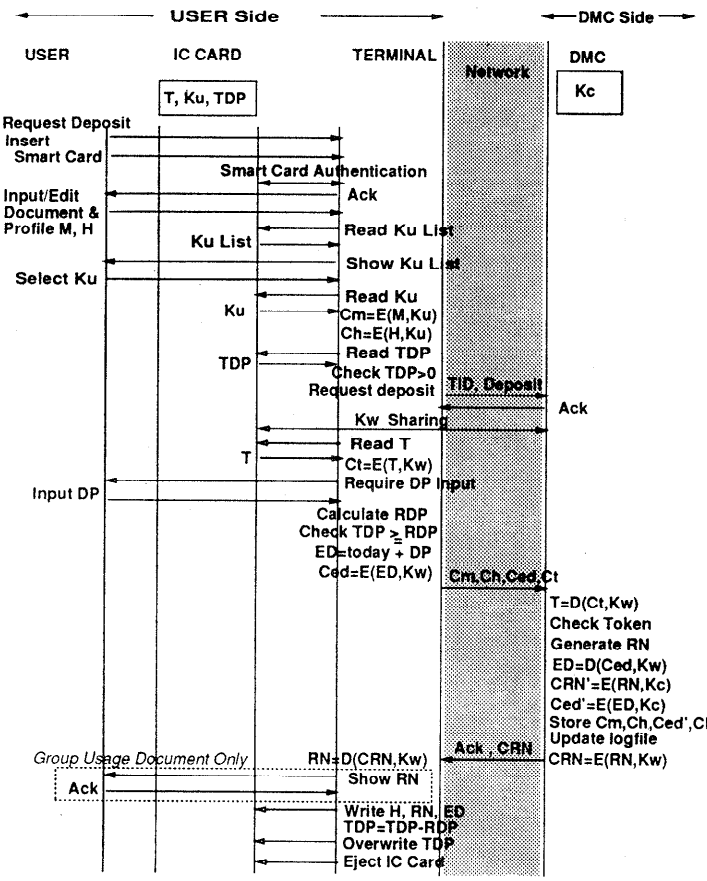


図3 文書登録手順の例
Fig. 3 An example of document registration protocol.

用いて復号し RR′ を得て，RR と RR′ が等しいことを確認した後，受信した Ckw を MKi を用いて復号し Kw を得る．
RR と RR′ は Crr が正しい MKi により生成されている場合にのみ一致する．正しい MKi を生成できるのは Kc を知る真の DMC のみであるため，通信相手が正しい DMC であると確認される．

4.3 文書登録手順

文書登録時における処理手順の一例を述べるとともに**図 3** に示す．

1. 利用者は文書登録を選択し，端末に IC カードを挿入した後，端末は IC カードの正当性認証を行う．
2. 利用者はMおよび H を入力する．H の内容は，タイトル，所有者名，作成日，コメント等である．
3. 端末は Ku のリスト（個人用鍵，組織 A，組織 B…）を IC カードから読み出してから，利用者に表示し，利用者は文書登録の目的に従い，用いる Ku を選択する．
4. 端末は指定された鍵 Ku を IC カードから読み出して M，H を暗号化し (Cm, Ch)，IC カードから TDP を読み出し，0 でないことを確認してから，DMC に TID と文書登録処理であることを通知し，DMC との間で Kw を生成する．
5. 端末は IC カードから T を読み出して Kw で暗号化し (Ct)，利用者から入力される DP から RDP を求め，RDP が TDP を越えていないことをチェックし，ED を算出して Kw で暗号化した後に (Ced)，Cm, Ch, Ced, Ct を DMC に伝送する．
6. DMC は Ct を復号化後，正当性をチェックし，RN を生成してから，Ced を Kw で復号化後 (ED)，RN と ED を Kc で暗号化する (CRN′, Ced′)．
7. DMC は Cm, Ch, Ced′, CRN′ を格納するとともに，Ri, TID を Kc で暗号化した CRi′, CTID′，および Ch, Ced′, CRN′ を登録日時とともにログファイルに追加登録した後，RN を Kw で暗号化し (CRN)，ACK とともに端末に伝送する．
8. 端末は CRN を Kw で復号化後 (RN)，組織で共有される文書を登録した場合には RN を利用者に表示し ACK をもらう．そして，H, RN, ED および TDP から RDP を差し引いた値を IC カードに書き込み，カードをエジェクトする．

ED や RN もプライバシー情報の一つと考えられることから，伝送時は Kw で，蓄積時は Kc で暗号化される．また，伝送中データの改ざん対策およびネットワーク利用料（通信料）の徴収も実際には行われるが，上記においては省略した．

4.4 文書取り出し手順

文書取り出し時における処理手順の一例を述べるとともに**図 4** に示す．

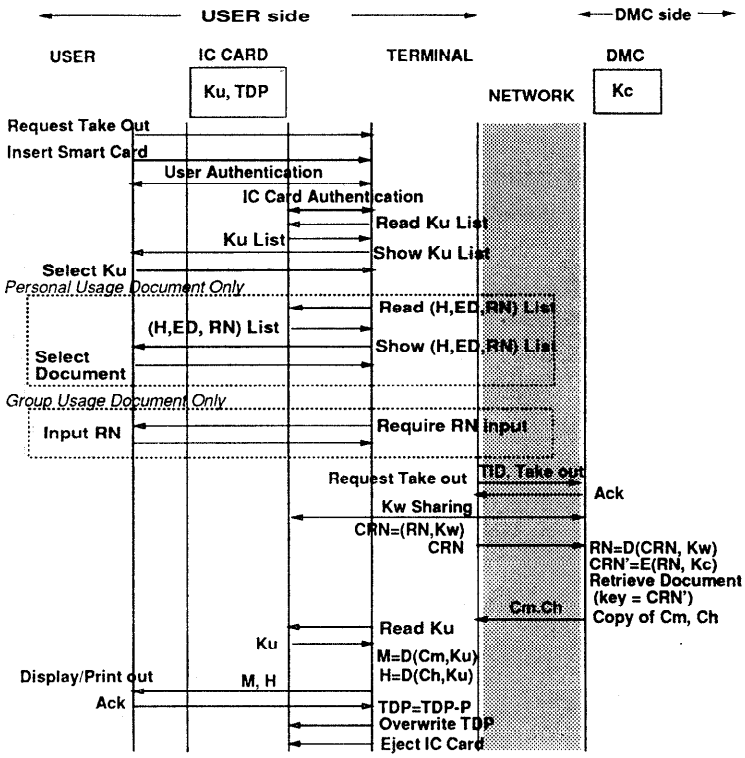


図 4 文書取り出し手順の例
Fig. 4 An example of document take out protocol.

1. 利用者は文書取り出しを選択し，端末に IC カードを挿入した後，端末は IC カードの所有者および正当性の認証を行い，IC カードから Ku のリストを読み出して表示する．そして利用者は取り出したい文書の暗号化に使われた Ku を選択する．
2. 個人の機密文書を取り出す場合，利用者は，端末が IC カードから読み出して表示する登録文書の H, RN, ED のリストの中から取り出すべき文書を指定する．
3. 組織で共有する文書を取り出す場合は，利用者は取り出すべき文書の RN を入力する．
   RN は登録を行った組織内の別の人物からあらかじめ知らされる．RN を伝送する際には暗号通信を行うことが望ましいが，他人に知られた場合でも Ku が漏れない限り文書内容の解読には至らないため，平文の伝送でも構わない．
4. 端末は DMC に TID と文書取り出し処理であることを通知し，DMC との間で Ku を生成した後，指定された文書の RN を Kw で暗号化して (CRN)，DMC に伝送する．
5. DMC は CRN を Kw で復号化後，Kc で暗号化してから (CRN′)，CRN′ をもとに指定された文書を検索し，検索した Cm, Ch のコピーを端末に伝送する．
6. 端末は選択された Ku を IC カードから読み出し，Cm, Ch を Ku で復号化後，表示/出力し，利用者からの ACK に対し，TDP から P を差し引いた値を IC カードに書き込み，カードをエジェクトする．

5. システムの評価

5.1 方式の比較とリスクの評価

各機能の実現手段を従来方式と比較したものを**表 1** に示す．各機能において従来方式では達成されない設計条件のほとんどが提案方式においては満足されることから，提案方式の優位性は明らかである．

また，主な不正行為とその条件，主な被害および対策の関係を**表 2** に示す．本システムにおいてはほとんどの認証処理を端末側で行うため，IC カードに関係する不正行為の機会が多く，これに関わる認証処理の信頼性の確保が重要である．表に挙げた不正行為のいくつかが同時に行われた場合には，そのリスクはより大きなものとなり得る．

5.2 運用実験による評価

5.2.1 実験システムの構成

システムイメージの明確化，システム機能とプロトコルの検証および問題点の洗い出しを行うことを目的として実験システムを作成した．端末機能，DMC 機能をそれぞれワークステーション上に実現し，端末側には秘密情報管理のための IC カードとそのリーダラ

表 1 各機能の実現手段の比較
Table 1 Comparison of realizing method of functions.

問題点	必要とする機能	従来の実現手段	従来方式の問題点	提案する実現手段	提案方式の利点
1	機能 1	DMC における利用者の識別と認証	設計条件 1,3 を満足せず	ＩＣカードによる端末側での利用者認証	設計条件 1,3 を満たす
	機能 2(伝送時漏洩対策)	送受者間の共通鍵による暗号通信	設計条件 2 を満足せず††	個人／組織の固有の鍵による端末での暗号化	設計条件 2 を 満たす ††
	機能 2(格納時漏洩対策)	Read 権の制御†	設計条件 1,2,3 を満足せず		設計条件 1,2,3 を満たす
2	機能 3(DMC における文書入力制御)	Write 権の制御†	設計条件 1,3 を満足せず	トークンによる利用契約の確認	設計条件 1,3 を満たす
	機能 3(DMC における文書出力制御)	Read 権の制御†		制御せず	
	機能 4	利用者ごとに登録可能容量を制限†		利用者が文書ごとに指定する登録期間による	設計条件 1 を満たす
		全文書一律の蓄積期間による消去	全文書の登録期間が一定		文書対応に任意の登録期間設定可能
	機能 5	登録可能容量の上限に応じた課金	設計条件 1 を満足せず	登録文書の量と期間に応じた課金	設計条件 1 を満たす
1,2	ＩＣカードの利用者認証方式	暗証情報の利用	なりすましが容易	身体的特徴の利用	なりすましが難しい
	ＩＣカードの正当性認証方式	ＩＣカード内の秘密情報による認証	秘密情報が漏れたら偽造可能	ＩＣカードの PIN 内に埋め込まれる透かし情報による認証	透かし埋め込みの鍵 Kd が漏れない限り偽造不可能‡

†:DMC における利用者の識別と認証を伴う，アクセス行列の利用．††: 公開鍵暗号を用いた場合には設計条件 1 も含む．
‡:Kd は登録センタにおいて秘密に管理される．透かし抽出の鍵 Ke を公開できる方式の開発が課題．

イタ，文書入出力装置および身体的特徴入力装置が接続され，DMC 側にはハードディスクが接続されている．なお，身体的特徴としては指紋を用い，筆者らが提案している指数照合方式[7]を実装した．また，文書の暗号化方式としては，固定長の画素ブロックを単位とするスクランブル方式[14]を，データの暗号化方式としては FEAL[15] を用いた．

5.2.2 評　価

研究室の 10 人の学生をモニタとする1か月間に渡る運用実験を行った結果，各機能の基本動作が確認され，プロトコルに矛盾のないことが検証された．実験では，モニタに対してできる限り不正行為を行うように指示したが，各自の登録文書に関する機密が漏れることはなかった．しかしこれは，モニタの数と不正行為の知識に依存する部分が大きいと考えられ，今後広範囲な運用実験による評価が必要である．以下に，安全性と利便性に関する評価結果を示す．

[安全性に関して]

- 文書登録時のアクセス制御方式

  IC カードが他人に不正に利用されて，文書の登録がなされた場合が2件あった．このことは，文書登録の代行を可能としている利点がある一方，他人のカードの不正使用の問題も存在することを示すものである．しかし，不正登録を行った人物にとっては，自分の文書を登録することはできても取り出し後の解読が不可能であり，かつ他人が登録した機密文書を入手できるわけでもないため何の利益も得られない．したがって，各自の IC カードの管理を徹底させれば，それほど頻繁には起こらない不正行為であると考えられる．また，他人の IC カードを用いて DMC に大量に文書を登録することによる，データベースの無駄使いが考えられるが，登録可能な文書量は高々その IC カードの所有者が契約を行った範囲内に押さえられるため，DMC からみれば通常の登録と変わりない．したがって，本システムで用いる文書登録時のアクセス制御は妥当であるものと考えられる．一つの対策としては，文書登録時の利用者確認の要不要を表す情報を IC カードに登録しておき，利用者自身に選択の余地を与えることが考えられる．

- 登録済み文書の原本の取り扱い

  利用者側における重要書類の管理を不要とする目的で文書登録する場合は，登録済み文書の原本は必要に応じて DMC から取り出せばよいため廃棄されるべきである．しかし，約半数のモニタは DMC の文書管理機能の信頼性が不安であるとして，原本も利用者側において保管していた．このことから，実用化のためには DMC における文書管理が安全，確実に行えることを利用者に対して十分実証できることが重要であるとわかる．さらには，登録文書の改ざん，漏洩，消去等の事故があった場合の責任の所在，保障のしくみを明らか

表 2　各機能に対する不正行為とその条件・被害・対策の関係
Table 2　Evaluation of system risks by attacks on each function.

不正行為内容	不正行為が可能となる条件	主な被害	対策
ICカードの紛失，盗難	ICカードの不十分な管理	利用可能度数の無断利用	検討課題
		文書取り出し不可能	ICカード内容のバックアップ
ICカード内容の漏洩	Read許可用鍵コードの漏洩	Ku，トークンの漏洩による登録文書内容の漏洩，文書の不正登録	鍵コードの桁数を長くする
偽の端末の作成	正規端末であることを証明する鍵コードKtの入手		Ktの厳重な管理，DMCによる端末の監視
暗号破り	特になし		暗号化鍵の桁数を長くする，強い暗号アルゴリズムの開発
ICカード内容の書き換え	Write許可用鍵コードの漏洩	登録可能度数書き換えによる文書の不正登録	鍵コードの桁数を長くする
トークンの漏洩	暗号破り，偽の端末の作成	文書の不正登録	複数のトークンを用意しておき，漏れたトークンを使用不可とする
ICカードの偽造	透かし作成の鍵コードの漏洩，アルゴリズムの解読	トークンか他人のKuが知られない限り問題なし	鍵コードの桁数を長くする，強いアルゴリズムの開発
利用者のなりすまし	身体的特徴の偽造	登録文書内容の漏洩	生身の身体であることの確認，複数の特徴の利用
偽のDMCの作成	正当なDMCであることを証明する鍵コードKcの入手	登録文書の紛失と漏洩	Kcの厳重管理，桁数を長く
DMCシステムへの侵入	DMC管理者のパスワード漏洩	登録文書の消去	パスワードの厳重管理，桁数を長く，データベースのバックアップ
DMCの物理的破壊	DMCへの物理的侵入		DMCにおけるデータベースのバックアップ

にする必要がある.

[利便性に関して]

- 利用者による RN の決定

  組織で共有する文書の場合はRNを組織の他のメンバに伝える必要があるため，覚えやすい番号を利用したいとの指摘があった．利用者がRNを指定すれば重複が起こり得るが，一つの対策としては，個人の機密文書の登録時にはDMCが，組織で共有する文書の登録時には利用者がRNを生成する方法が考えられる.

- ED の変更の必要性

  文書を登録する時点でDPを正確に決定するのは難しく，登録後にEDを変更したいとの指摘があった．このためには，ED の変更を要求する人物とその文書の所有者の一致確認を DMC 側で行う必要がある．この機能の一実現手段として，文書登録時にDMCはCRN′を登録証として利用者に返送し，ED変更要求とともにRNとCRN′のペアが提示された場合に変更を許可する方法が考えられる.

6. おわりに

本論文では，個人のプライベート情報や企業の重要書類等の機密文書を貸し金庫の概念を用いて管理・共有することを目的とする共同利用型機密文書管理システムを提案し，システム実現に当たってのセキュリティに関する問題点を整理し，必要とするシステム機能について検討した．具体的には，利用者のアクセス制御方式，登録文書の蓄積制御方式等に関して，特にセンタの管理者に対する利用者のプライバシーの確保，センタで認証処理負荷の集中を回避することを考慮した一実現手段を示し，そのプロトコルを明らかにするとともに，従来方式との比較および運用実験による方式の評価，基本機能の検証を行った.

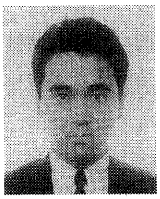
今後の課題としては，運用実験の結果新たに必要性が指摘された機能の実現，IC カード正当性/利用者認証方式の改善，端末機能のハードウェア化による処理の高速化が挙げられる．また，より多人数，広範囲に渡る大規模な運用実験による方式評価，プロトコルにおける問題点の洗い出しを行う必要があるため，現在ISDN をネットワークとして利用する実験システムを構築中である.

謝辞 本研究は一部，文部省科学研究費補助金一般研究（B）02452152 によるものである．同研究会メンバである京都工芸繊維大学笠原正雄教授，同若杉耕一郎助教授，早稲田大学平澤茂一教授，同小松尚久助教授には貴重なご意見を頂きました．ここに謝意を表します.

参考文献

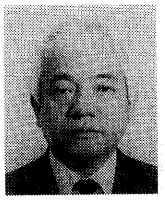
1) 田口和男，坂下善彦：OA システムと文書データベース，情報処理，Vol. 28, No. 6, pp. 721-729 (1987).
2) 渡辺義雄，宮崎欽次，森本周幸：バックアップ管理とシステム監査，日本セキュリティマネジメント学会，システム監査研究会小論文集，pp. 12-19 (May 1989).
3) 田岡俊次，内山幸男，森田良平，武藤いづみ：銀行顧客名簿漏洩の構造—シュレッダーかけずお客の秘密流れる—，*Asahi Shimbun Weekly AERA*, 1990. 6. 12.
4) Denning, D. E. R.: *Cryptography and Data Security*, Addison-Wesley Publishing Company (1982).
5) 砂川 克，菊井広行：最新特許にみる IC カード開発としくみ，工業調査会.
6) Fitzgerald, K.: The Quest for Intruder-proof Computer Systems, *IEEE Spectrum*, Vol. 26, pp. 22-26 (Aug. 1989).
7) 横里純一，山田道夫，高木伸幸，富永英義：指紋画像を用いた個人認証の一検討，画像電子学会全国大会，21 (June 1990).
8) 富永英義，木村正二，横里純一，山田道夫：動き特徴量を加えた顔画像個人照合の検討，電子情報通信学会春季全国大会，D-604 (Mar. 1991).
9) 山田道夫，富永英義：文書管理システムとそのネットワークの安全性に関する研究—第6章 IC カードの正当性認証方式—，平成元年度早稲田大学修士論文 (Mar. 1990).
10) 小山謙二，太田和夫：個人識別情報に基づき2者以上で共通鍵を生成する方式，電子情報通信学会論文誌 D-I, Vol. J 72-D-I, No. 1, pp. 50-56 (1989).
11) 小山謙二：情報セキュリティ，コンピュータ犯罪をどう防ぐ，電気書院 (1989).
12) 家木俊温：IC カードによる情報の暗号化および改ざん防止法，電子情報通信学会技術研究報告，IN 85-62, pp. 13-18 (1985).
13) 宮口庄司，岩田雅彦：IC カードの個別鍵管理方式，電子情報通信学会技術研究報告，ISEC 88-37, pp. 33-39 (1988).
14) 小松尚久，富永英義：画像のスクランブル手法を用いた機密保護ファクシミリ通信，画像電子学会誌，Vol. 17, No. 5, pp. 409-417 (1988).
15) 清水明宏，宮口庄司：高速データ暗号アルゴリズム FEAL，電子情報通信学会論文誌 D, Vol. J 70-D, No. 7, pp. 1413-1427 (1987).

(平成4年8月10日受付)
(平成5年3月11日採録)



山田　道夫

昭和40年生．昭和63年早稲田大学理工学部電子通信学科卒業．平成2年同大学院修士課程修了．平成5年同大学院博士後期課程修了．工学博士．同年日本電信電話(株)入社．在学中，主に画像符号化，画像通信における機密保護手法，身体的特徴を用いた個人識別手法などの研究に従事．電子情報通信学会，画像電子学会各会員．



富永　英義（正会員）

昭和14年生．昭和37年早稲田大学理工学部電気通信学科卒業．昭和39年同大学院修士課程修了．同年日本電信電話公社電気通信研究所入所．昭和46年早稲田大学助教授．昭和51年同教授．工学博士．主に，ISDN，テレマティークサービスの研究に従事．電子情報通信学会，画像電子学会，テレビジョン学会，IEEE各会員．