「インターネットを利用した
安心できるファイル交換」について

（株）さくらケーシーエス

■ 執筆者１Ｐｒｏｆｉｌｅ ■

水島　望

2005 年　現在 取締役
産業システム事業部担当

■ 執筆者２Ｐｒｏｆｉｌｅ ■

多井　剛

1988 年　現（株）さくらケーシーエス入社
グループウェアなどを開発
2004 年　兵庫県立大学 非常勤講師
2005 年　現在 事業推進部 所属
ニュービジネス推進室長

■ 論文要旨 ■

これまで医療・福祉・金融機関の親展郵便のような機微情報を含むダイレクトメール（DM）の発送を外部に委託する際に、その過程で情報が流出する懸念があった。

そこで、インターネットを利用した安心できるファイル交換システム（以下PALne/PS）を開発した。

特徴は、データの暗号化・復号化（暗号化されたデータを元に戻す）に必要な鍵を４人のデータ取扱者が持つ IC カードに分割して管理する「割符方式」（特許出願）にある。

送信・印刷・発送過程で人手を減らし、リスクを軽減するとともに、使用するパソコンを専用端末化して誤操作を極限まで抑えてある。

個人認証機関として公的データセンターを用いるビジネスモデルを確立し、自治体の印刷業務アウトソーシングや、データ処理アウトソーシングなど、ファイル転送を行う場面で幅広く利用できると考えている。

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　個人情報保護法の施行に関して

2005 年 4 月 1 日に個人情報保護法が施行され、個人情報処理を外部委託する医療、福祉、金融機関や、以前から取り組んでいた自治体も改めて委託先情報処理企業と一緒に個人情報の取り扱いについて、その漏洩防止に努力している。

現在、情報漏洩は外部のハッカーの犯行よりも委託先従業員のミスや、ちょっとした興味本位の行動結果であったりすることのほうが多いため委託先での安全なデータの取扱が保証されない限り、委託先へのデータ持ち出しがきつく制限されることになる。

１．２　個人情報の授受の問題点

顧客とのデータの転送において、従来のメディア搬送では多くのセキュリティホールが存在した。例えば、多くの従業員が個人情報に触れる可能性があるという点である。（図 1）

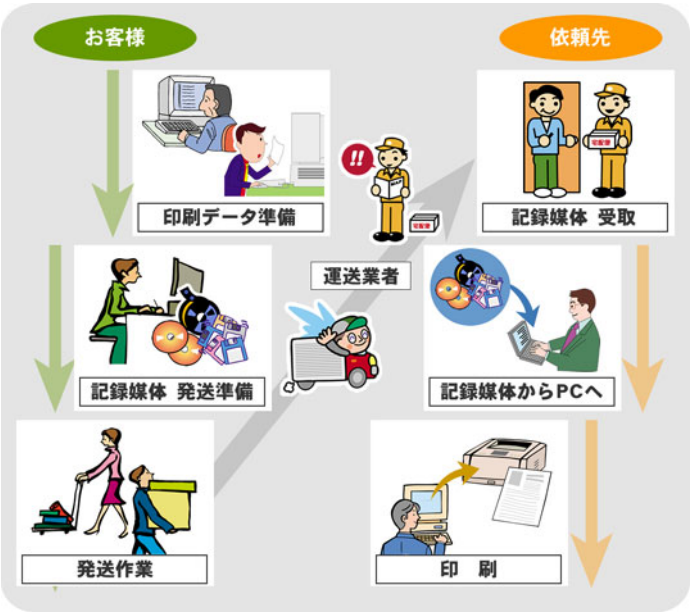

図 1　情報漏洩のリスク

この場合、媒体管理のための帳票や媒体授受のための帳票など、管理にかかるコストもばかにならない。しかも配送中の事故のリスクなど、すべて完全にマネージメントされなければ、委託元の担当者は心配なのである。

そこで「委託先業者を信頼しなくてもいい仕掛け」として開発したのが「PALne/PS」である。

２．PALne/PS の目的

インターネットを利用したファイル交換において「委託先業者を信頼しなくてもいい仕掛け」を PALne/PS では、次の方針により、設計を行った。

(1) 委託元担当者は、信用できない者とし、委託元管理者及び、委託先の認証によりファイルを送信する事ができる。

(2) 委託先担当者は、信用できない者とし、委託元の認証、委託先管理者の認証により、ファイルを受信及び、復号が可能とする。

(3) ファイル交換データは、暗号文を用い、暗号化キィーは、セキュリティを強化するための（委託元）送信側２名、（委託先）受信側２名の乱数により生成し、強度の高い共通キィー暗号方式を用いたシステムとする。

(4) 暗号化キィーは、可能な限り守秘とし、セキュリティ効果を高める。

(5) （委託元）送信側、（委託先）受信側は、お互いの動きが見え、相互確認ができる。

(6) ハードウェア面で、セキュリティを強めたシステムとする。

この方針により、委託元のリスクをシステム上軽減し、委託元担当者の精神的負担を減らすことを目的としてシステム開発を行った。

３．構成

３．１　全体の構成

方針に基づき実現方法を検討した。送信側、受信側共、パーソナルコンピュータを用いた伝送システムとし、送信側と受信側は、１対１とはせず、発展性を考慮し、複数組織での送受信システムとしている。また、この複数組織間通信ため、中央に共同のファイルサーバーシステムを持つ形で構築を進めた。（図２）

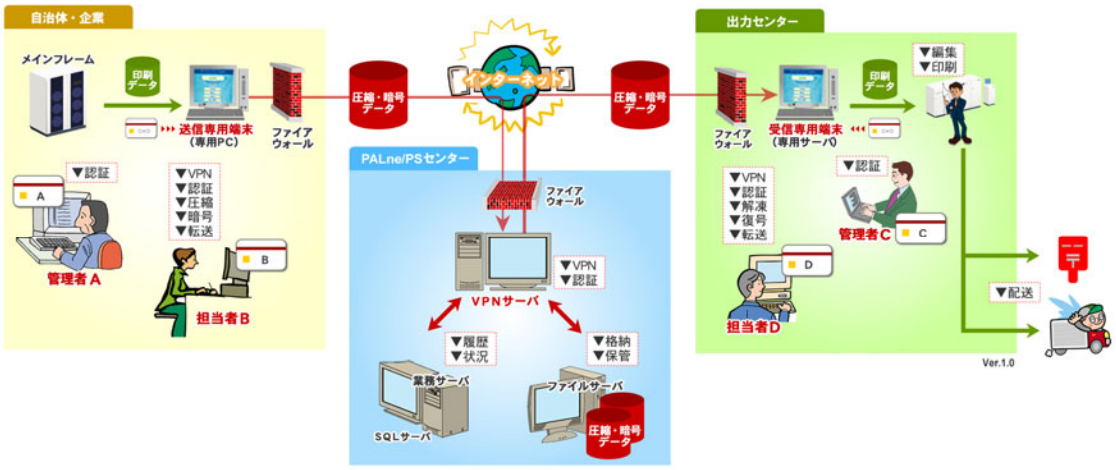

図 2　全体の構成

コンピュータネットワークはインターネットを用いるが、端末認証を得るためにトンネリング技術を用い、結果として VPN を構成している。個人情報を含むファイルについては、VPN にかかわらずネットワーク内で常に暗号化がされており、中央のファイルサーバからファイルを盗まれても復号できない仕組みを提供する。

３．２　送信方法

送信手順は次のようになる。（図 3）

(1)（委託元）送信担当者は、送信データを送信専用端末（パソコン）内へコピーする。
(2)（委託元）送信担当者が、（委託先）受信側、及び送信側管理者からの許可を得た後に操作に入る。
(3) 送信データを圧縮し、暗号文に変換した後、センターサーバーへ伝送する。この状況は、送信管理ファイルに出力され、受信側で状況を確認する事ができる。

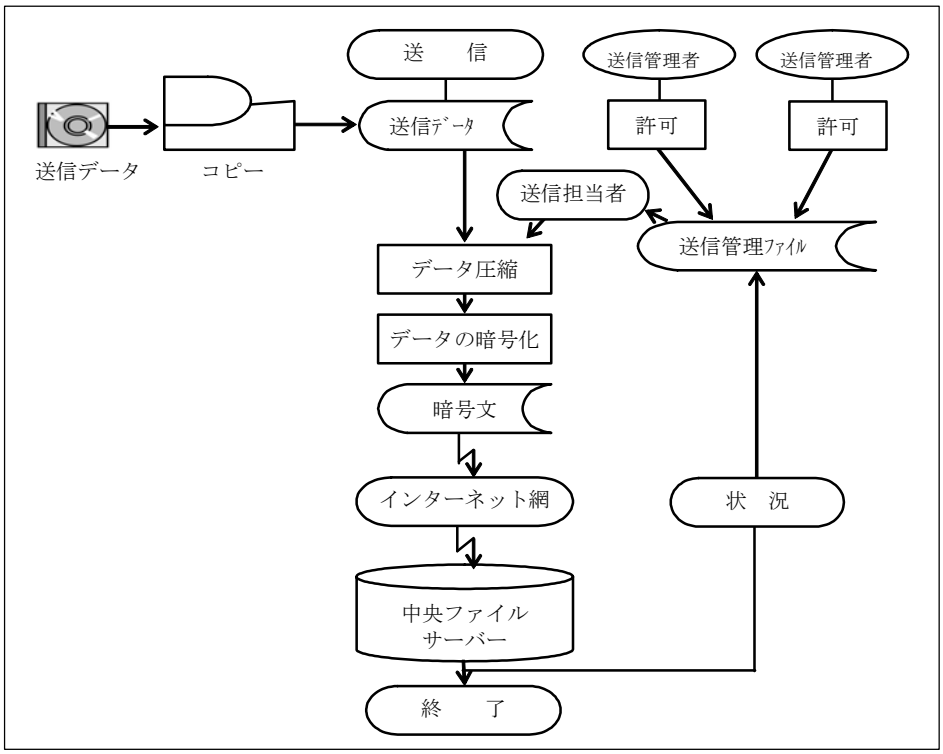

図 3　送信の手順

３．３　受信方法

受信手順は次のようになる。（図 4）

(1) 受信担当者は、送信管理ファイルの照会で送信データの存在が分かる。受信管理者の受信許可を得て、中央ファイルサーバーより、データを受信する。
(2) この後、データを解凍し暗号文を復号する。この状況は受信管理ファイルに出力され、送信側は状況を照会し確認することができる。

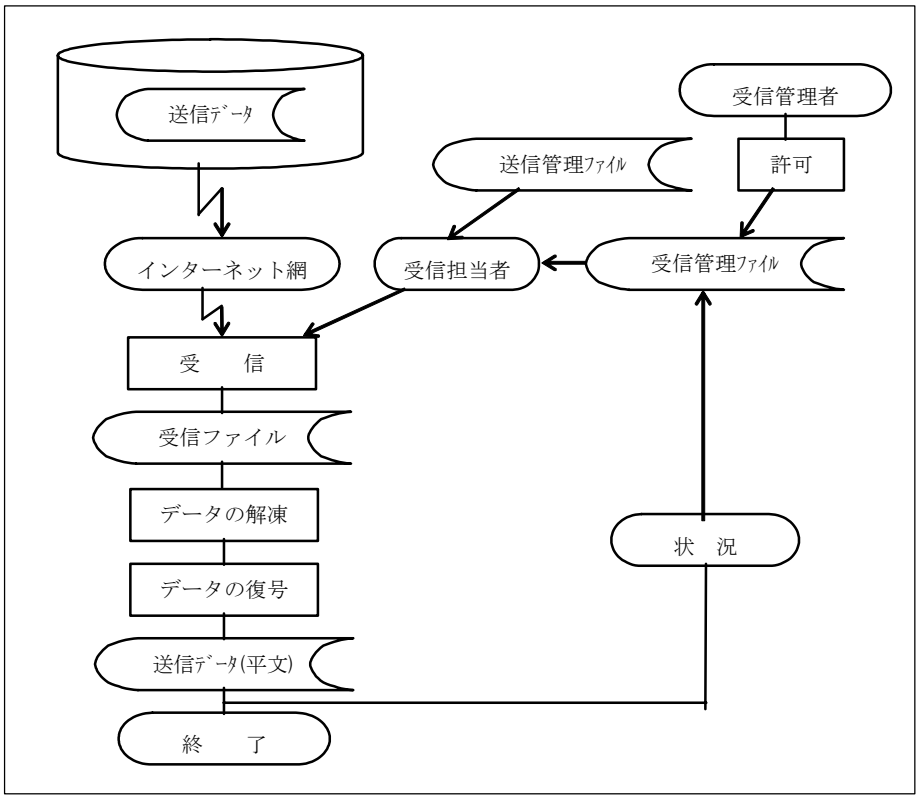

図 4　受信の手順

３．４　暗号化

送信データは一旦圧縮され暗号化の後送信される。暗号化の安全性の強化として、送信ファイル毎に暗号キィーを算出するいわゆる「ワンタイムキィー」を採用した。

３．４．１　４名での合成暗号方式

PALne/PS では暗号キィーを、各々、送信・受信関係者の４名が発生した乱数を合体させ、１つの共通キィーとして生成する。具体的には、４名の発生させた２バイト（１６ビット）をつなぎ合わせる。４人の乱数のつなぎ合わせは全くの乱数となる。

この方法であれば、関係者に暗号キィーが見えないという大きなメリットを持ち、さらに４名のキィーの集合体はコンピュータ内部メモリでのみ保持すればよいため、外部記憶媒体に保存されるリスクを回避する。

暗号化・復号化を行うための共通キィーは誰にも知られないので、暗号文の安全性は大きい。

この方式を割符方式と呼んでいる。

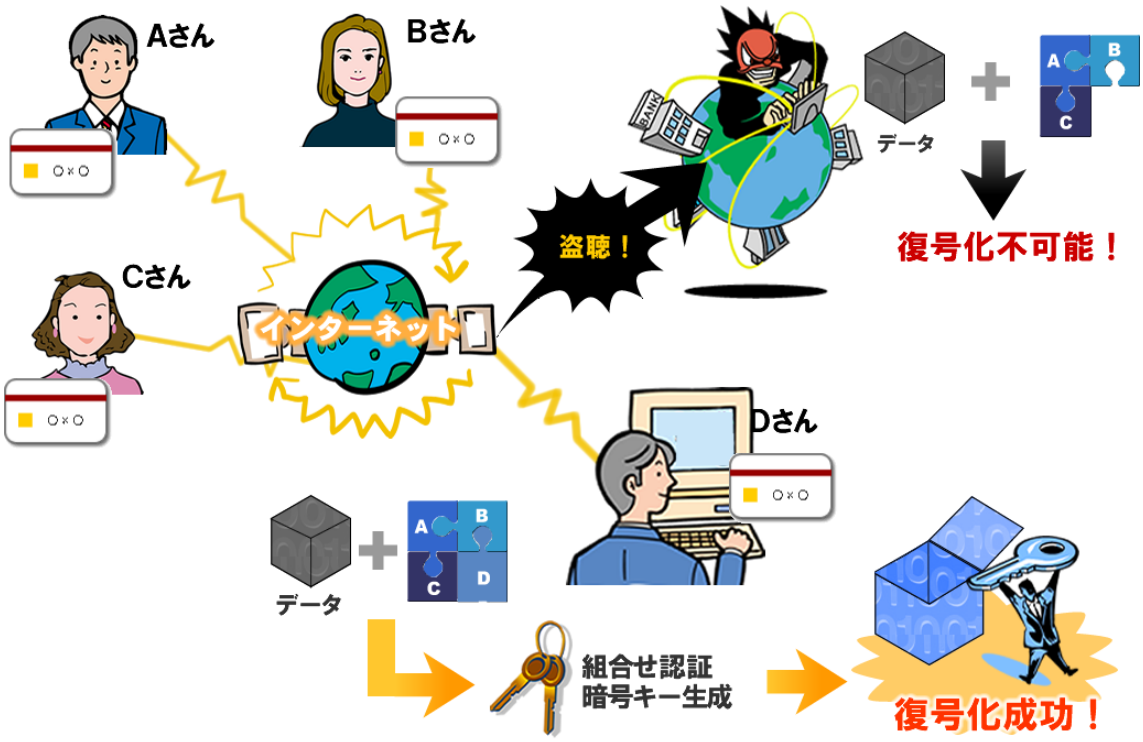

図 5　割符方式

３．４．２　公開鍵方式によるキィーの送受

４人の乱数を送受する際に盗まれない様にしなければならない。

対策として PALne/PS では乱数の受渡しに公開鍵暗号方式を採用している。乱数自体が１６ビット(２文字)と短いため、公開鍵暗号方式でも CPU に負担をかけない。

送信側の送信（＝暗号化）担当者を除く３名は、送信担当者の公開鍵を用いて自分の乱数を暗号化する。これを復号できるのは送信担当者の秘密キィーであるため、送信担当者しか解読できない。

送信担当者の秘密キィーは、送信担当者が持つ IC カードに格納されており、このほかの外部記憶装置に取り出すことはできない。

３．４．３　乱数を隠す方法

共通キィーを構成する４名各々の乱数を隠す必要がある。

対策として PALne/PS では乱数を自分の公開キィーで暗号化して保持している。この暗号化された乱数は本人の秘密キィーでしか復号できない。（図 6）

乱数を盗もうとしても本人の秘密キィーを知らない限り、復号は不可能である。

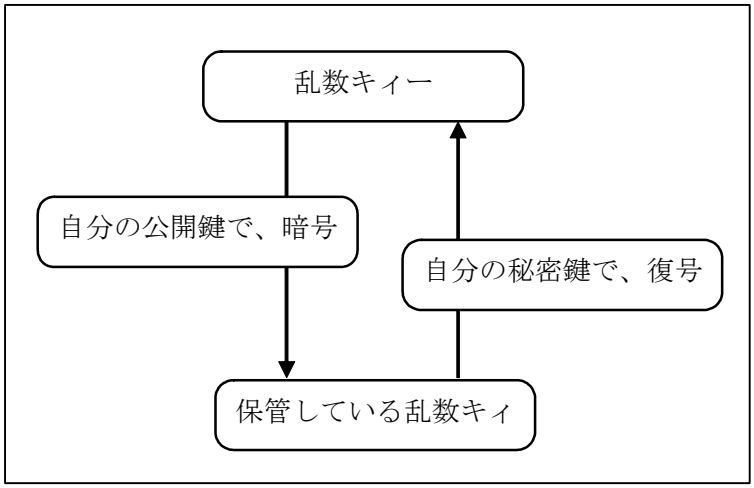

図 6　乱数を隠す方法

３．４．４　復号の方法

送信側より、４つの内の２つの乱数が受信側に渡された後に、受信側の管理者が受信（＝復号化）担当者の信用を検査した上で、自分の秘密キィーで乱数を復号して３個目の乱数をシステムに渡す。

４番目の受信担当者は、自ら持っている４番目の乱数を自分の秘密キィーで復号し受信専用端末に渡すこと（IC カードを挿入すること）によって、４つの乱数からメモリ上に共通キィーを生成する。

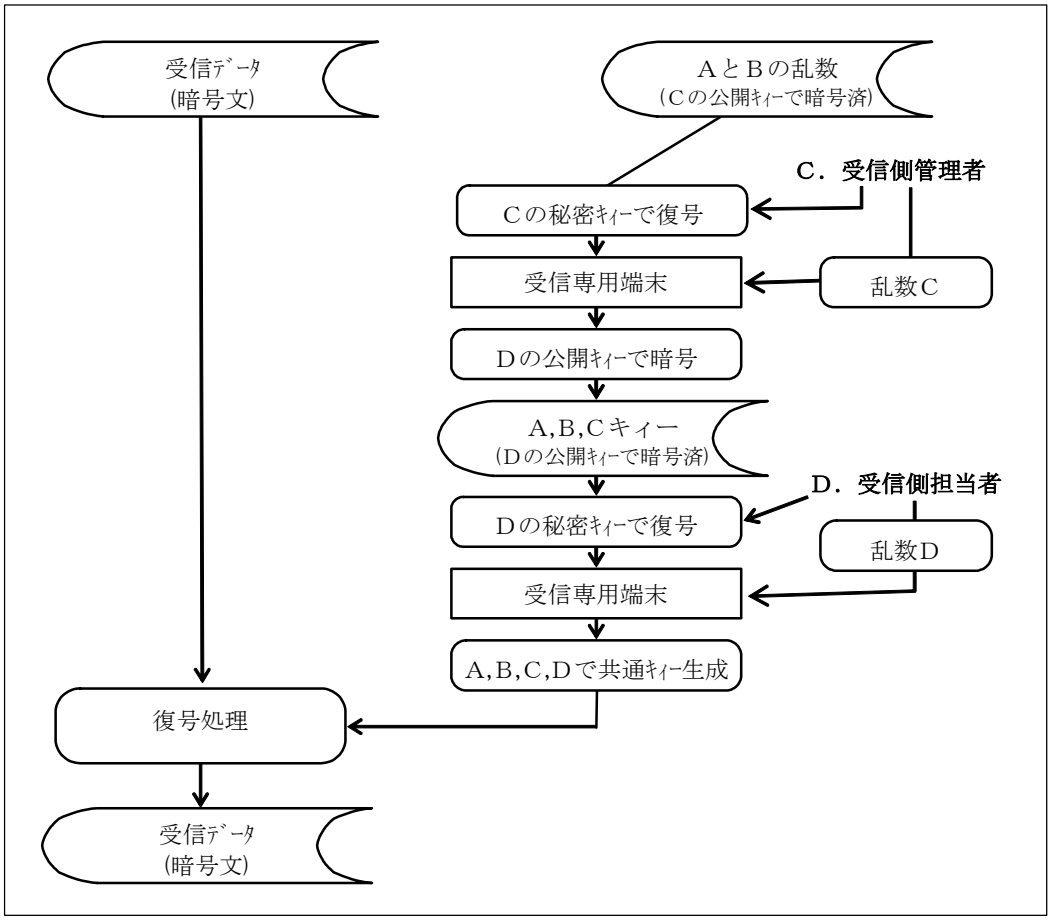

図 7　復号の方法

３．４．５　ＩＣカードの発行

PALne/PS ではビジネスモデルとして、ＩＣカードの発行を信頼できる第三者機関で行っている。委託元も委託先もこの第三者機関からＩＣカードの供給を受ける。このことによって委託元も委託先もカードの複製ができず、不正侵入も監視されているため、不正利用防止のための牽制効果が高い。

４．今後の展望

４．１　事業

現在、PALne/PS を用いて自治体などから受託を受け個人情報を印刷する事業の展開に取り組んでいる。協賛する企業とコンソーシアム（共同事業体）を結成し、データの印刷から配送までを信頼の高い事業者で請け負う。

今後は、医療機関、金融機関や通販企業などでの利用を期待している。

４．２　システム

現在の PALne/PS では、ファイルを受信して復号したときに脆弱性が発現する。今後は後工程のシステムと連携し、監視と暗号化が最終工程（印刷、搬出など）まで維持できるようシステム化を図っていく。