デジタル複合機におけるネットワークセキュリティへの対応

Application of Network Security to Digital Multi Function Peripheral Equipment

的 場 和 男*
Matoba, Kazuo

要旨

オフィスにおけるネットワーク上の脅威が問題になってきており，これに対抗できるセキュリティ技術をデジタル複合機に適用していくことが重要な課題になってきている。そこで本稿では，基本的なセキュリティ技術である暗号技術，電子署名及び電子認証の技術内容を説明し，これらをデジタル複合機へ適用することにより，

・ネットワーク通信の暗号化
・認証可能な紙文書の電子化
・文書データの検証

等のセキュリティ機能がデジタル複合機で実現できることを示す。また，ユビキタスネットワークが発展していく中で，デジタル複合機が取り組むべき新たなセキュリティ技術を明らかにする。

Abstract

Various menaces to network communication are arising in offices. Under these circumstances, to implement security technology into digital MFP (multi function peripheral equipment) has become an important issue. This report describes fundamental security technologies to be implemented into the MFP. Three security functions of:

1) encrypting network communication,

2) digitizing paper document with electronic signature and

3) verifying accuracy of received data, will be realized on the MFP by implementing these technologies.

This report also refers to newer technology to be applied to the MFP under progress of ubiquitous network environment.

*コニカミノルタビジネステクノロジーズ㈱
制御開発本部　制御第1開発センター　第13開発部

1　はじめに

デジタル複合機は，コピー，プリント，スキャン及びFAXの機能をネットワークの通信機能と共に一体化した製品であり，ネットワーク上の複数のパーソナルコンピュータ（PC）によりプリント機能を共有できるだけでなく，スキャンして電子化されたデータをPCやサーバに送信したり，内蔵のハードディスクに蓄積してPCからアクセスしたりできることから，紙文書と電子データを相互に交換できるネットワーク端末としてオフィスで広く利用されるようになってきている。

従来は比較的安全とされていたオフィス内のネットワーク環境であるが，悪意を持った人間の不正行為による情報の漏洩や改変などの問題発生が懸念されており，不正アクセスやネットワーク上の通信データに対する盗聴や改ざんなどの脅威に対抗できるセキュリティ対応が進められている。これに伴って，デジタル複合機に対しても同様のセキュリティ対応が求められており，一部の製品ではユーザの認証機能や通信データの暗号化機能を搭載してきている。また，紙文書を電子化したデータを原本として取り扱うことができるｅ-文書法の施行により，データの偽造や改ざんを防止する機能の導入も求められている。更に，ユビキタスネットワークの発展に伴い，オフィス内のネットワークだけでなく，インターネット上の端末機器と直接かつ安全に通信するための新たなセキュリティ技術への対応もデジタル複合機における課題となってきている。

本稿では，以上述べたような背景をもとに，ネットワーク上の通信データに関するセキュリティを中心にして，主な脅威に対する基本的な対応技術を示し，この技術の適用によりデジタル複合機で求められるセキュリティ機能が実現できることを示す。また，ユビキタスネットワーク環境に向けた新たなセキュリティ技術の内容と，その技術のデジタル複合機への展開を述べる。

2　ネットワークセキュリティの基本技術

2．1　ネットワークへの脅威

ネットワークに対する主な脅威として，次の3つが挙げられる。

➢盗聴
ネットワーク上に流れている通信データを不正に収集して読み取ること。通信データは一般的にプレーンテキスト（平文）で転送されるため容易に内容が読み取られてしまう。
➢改ざん
ネットワーク上に流れている通信データを横取りして内容を不正に変更し受信者に転送すること。送信者及び受信者に気付かれることが無い様にできるため，コミュニケーションの混乱を引き起こすだけでなく送信者の信用問題にもなりかねない。
➢なりすまし
他人のIDやパスワードを盗用し，その人を装ってネットワークに侵入することにより，受信者をだまして不正な情報を送信したり，逆に正規の受信者のふりをして重要情報を騙し取ったりすること。騙された側の送信者または受信者には気付かれることが無い様にできるため，情報漏洩や信用問題にもなりかねない。
これらの脅威に対抗するために，暗号技術，電子署名及び電子認証の対策技術が用いられる。以下，これらの技術について説明する。

2．2　暗号技術

暗号技術とは，通信データを第三者にとって意味不明なデータ（暗号）に変換することにより，正規の当事者以外にはデータの有用性を失わせる技術である。この方式には，共通鍵暗号方式と公開鍵暗号方式がある。

2．2．1　共通鍵暗号方式

共通暗号鍵方式では，同一の暗号鍵（共通鍵）によりデータの暗号と復号を行う（**Fig. 1**）。

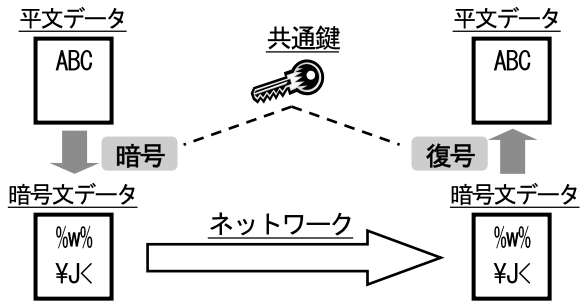

Fig.1 Common key encryption

この方式では，共通鍵が第三者に知られてしまうと暗号文が盗聴されるので，共通鍵の受け渡しや管理に細心の注意を払う必要がある。

2．2．2　公開鍵暗号方式

公開鍵暗号方式では，2つの暗号鍵が用いられ，一方の暗号鍵で暗号化されたデータは，もう一方の暗号鍵でないと復号できない（**Fig. 2**）。また，互いに双方の暗号鍵を容易に特定できない構成となっている。そこで，一方の暗号鍵を公開鍵として公開し，もう一方の暗号鍵を公開せずに手元に秘密鍵として保持しておけば，秘密鍵を保持する人だけが安全に暗号文データを復号できる。

公開鍵暗号方式のこのような非対称性は，後述する電子署名や電子認証におけるデータの正当性を保障することに応用されている。

公開鍵暗号方式は，前節の共通鍵方式に比べて，暗号鍵の配信を安全に行うことができる上に，複数の通信相手に対して通常は1つの公開鍵で運用できるため管理が容易となるが，アルゴリズムが複雑であることから，処理時間が数百倍となり，現状では実用的なパフォーマンスが得られない。

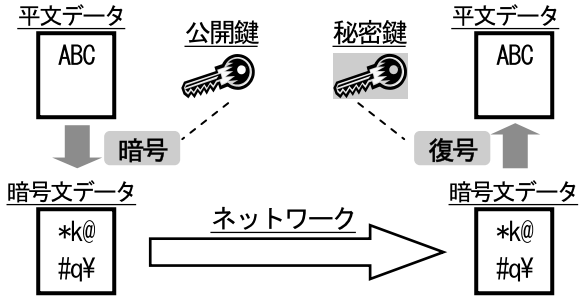

Fig.2 Public key encryption

2．3　電子署名

電子署名とは，送信者の秘密鍵によりデータのダイジェストを暗号化してデータと共に送信し（**Fig. 3**），受信者側では同じ送信者の公開鍵により復号して得られたダイジェストを検証する（**Fig. 4**）ことにより，データが改ざんされていないことを保障する技術である。

ダイジェスト算出のためのハッシュ処理では，データを一定長のサイズに要約する一方向性関数が利用され，データの僅かな違いでも大きく異なったダイジェストを生成する。送信者の秘密鍵によって暗号化されたダイジェストは，送信者の公開鍵でなければ復号できない。このため，送信者の秘密鍵を知らない第三者によるデータへの不正操作があった場合はダイジェストが一致せず，改ざんされたことを簡単に判別できる。

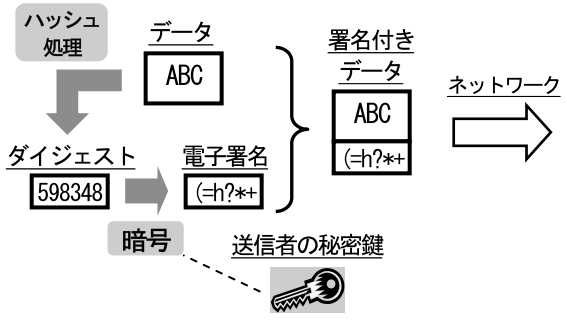

Fig.3 Creating electronic signature by sender

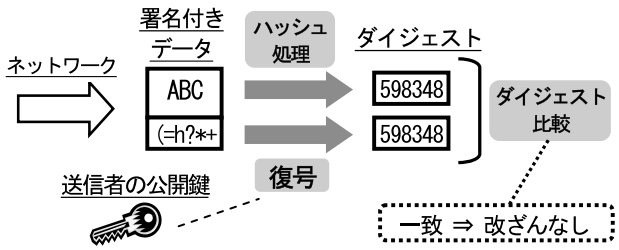

Fig.4 Authenticating electronic signature by receiver

2．4　電子認証

電子認証とは，ネットワーク上で通信相手の存在証明と本人性を第三者が証明することをいう。この存在証明と本人性の確認手段として，前節の公開鍵暗号方式による電子署名と，第三者として公開鍵の正当性を保証する電子認証局からなるシステムが広く利用されている。本節では，このようなシステムについて説明する。

上述した公開鍵暗号方式と電子署名では，通信相手の公開鍵を入手して利用することになるが，セキュリティを確保するためには，その公開鍵が正しく相手本人のものであるかを検証できることが必要である。そこで，公的に信頼できる電子認証局（Certification Authority: CA）を介して公開鍵とその所有者との整合性を保障できる機構が用いられる。

Fig. 5 に認証の流れを示す。送信者が自身の情報と共に公開鍵をCAに送ると，CAではCA固有の情報も合わせて，CAの秘密鍵で暗号化して電子署名を生成する。これらの情報を全てあわせたものが公開鍵証明書である。

送信者は公開鍵証明書を送信し，受信者はCAの公開鍵により内容が改ざんされてないことが確認できれば，公開鍵証明書の公開鍵を送信者のものとして利用する。以上の公開鍵暗号方式を利用したデータの暗号化，電子署名並びに電子認証の安全な運用を可能にするための基盤技術のことをPKI（Public Key Infrastructure）という。PKIの要素として，既に述べた公開鍵証明書やCAなどが挙げられる。

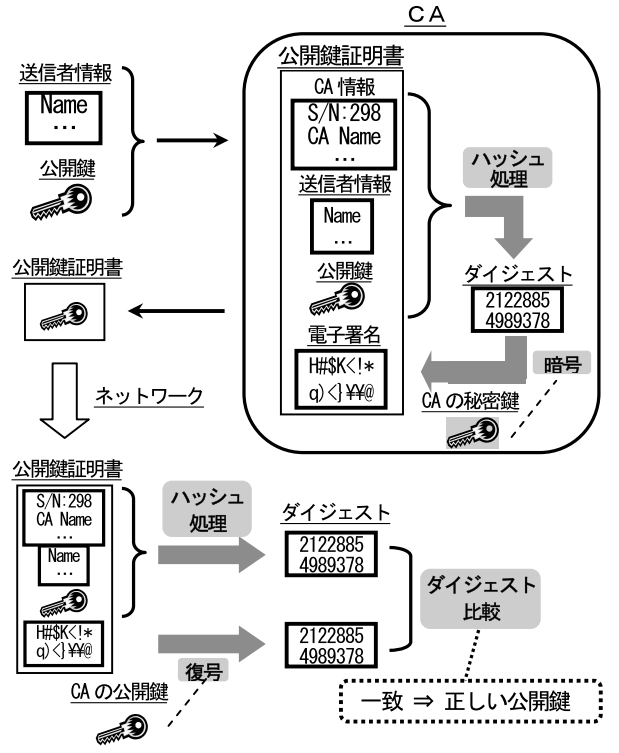

Fig.5 Public key certification

3　デジタル複合機に求められるセキュリティ機能

3．1　ネットワーク通信の暗号化

ネットワーク通信を暗号化する技術はいくつか実用化されており，代表的なところではSSL/TLS(Secure Socket Layer/Transport Layer Security）が挙げられる。この技術は，ネットワークプロトコルの標準モデルであるOSI（Open Systems Interconnection）参照モデルのセッション層で機能し，上述した公開鍵暗号の技術を利用してネットワーク通信の脅威に対抗できるものとなっている。SSL/TLSの動作の概略を**Fig. 6** に示す。

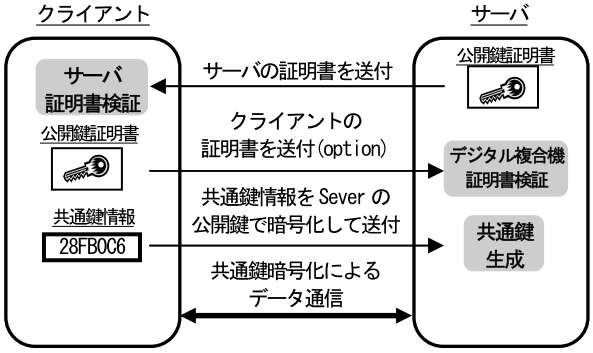

Fig.6 Sequence of SSL/TLS

SSL/TLSでは，公開鍵証明書を検証することにより相手を認証し，データ通信は共通鍵により暗号化する。ここで，共通鍵を相手の公開鍵で暗号化することにより，第三者に知られることなく共通鍵を配送することができる。データ通信に共通鍵暗号方式を利用するのは，実用的なパフォーマンスが得られるからであり，既に述べた様に，公開鍵の場合は暗号処理がかなり大きく，現在のところ実用的なパフォーマンスが得られないからである。

弊社でも，この機能をデジタル複合機製品に搭載し，重要な情報に対するネットワーク通信のセキュリティを確保している。

3．2　認証可能な紙文書の電子化

2005年4月に施行されたe-文書法により，財務や税務関連の書類及び帳票をスキャンして電子化する際に一定の技術要件を満たせば，それらの紙文書に代わって電子情報を原本とみなせることが可能となった。この技術要件の基本は，偽造や改ざんのないことを保障する完全性と，効率的な検索と一定水準の画質による表示または印刷を可能にする検索性と見読性を確保することにある。ここでは，この完全性の確保に対してデジタル複合機に求められる機能を述べる。

完全性の確保のために，e-文書法では，作成者の電子署名及びタイムスタンプへの対応がデジタル複合機に要求される。この対応の例を**Fig. 7** に示す。

デジタル複合機は，紙文書をスキャンして得られた文書データのダイジェストを作成者のスマートカードに転送し，作成者の電子署名を取得した後，この電子署名と文書データのダイジェストをTSA（Time Stamp Authority）と呼ばれる時刻認証局に転送して，TSA電子署名を取得する。そして，これらの電子署名と元の文書データを合わせて送信する。

スマートカードは，信頼できる機関から発行されたものであり，作成者の秘密鍵保持と電子署名処理が可能な電子回路が内蔵されている。当然，作成者の公開鍵はCAに登録されて公開鍵証明書として入手可能でなければならない。秘密鍵の保持と確実な電子署名ができる方式としてスマートカードを例に説明したが，これが必須の方式ではない。

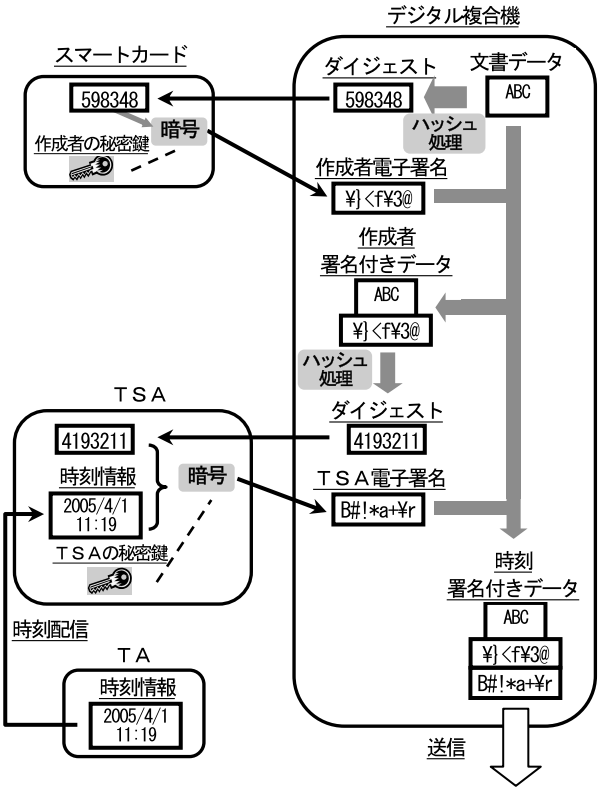

Fig.7 Signing process for e-Document law

TSAは信頼できる時刻配信局（Time Authority: TA）から時刻配信を受けており，その時刻情報と文書データのダイジェストを合わせて電子署名を行う。デジタル複合機とTSAの間はネットワークにより情報が交換されるが，このためのプロトコルとしてTSP（Time Stamp Protocol）がRFC3161で規定されている。また，文書データの長期保証を実現するために，タイムスタンプを繰り返し適用するための方法とフォーマットがRFC3126で規定されている。

3．3　文書データの検証

前節では，デジタル複合機から署名付きの文書データを送信する場合を示したが，デジタル複合機がそのようなデータを受信した場合に，添付された電子署名を検証できることも，セキュリティ対応のためには必要である。これには，作成者およびTSAの公開鍵証明書の正当性を確認できなければならない（**Fig. 8**）。

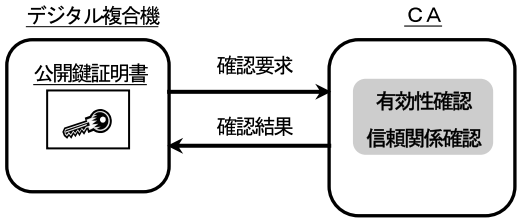

Fig.8 Verifying public key certificate

ネットワークを通して，公開鍵証明書の検証をCAあるいは適切なサーバに委託できるプロトコルとして，RFC2560で規定されているOCSP（Online Certificate Status Protocol）の他に，SCVP（Simple Certificate Validation Protocol）などがある。デジタル複合機においても，これらの機能に対応していくことが必要である。

4　ネットワークセキュリティの今後の展開

ユビキタスネットワークの発展に伴い，インターネットを越えてデジタル複合機が携帯端末と直接通信したり，あるいは他のデジタル複合機からデータを直接受信したりするなどのP2P（Peer to Peer）通信への要望が高まっている。このため，通信を開始してからのセキュリティ対応だけでなく，通信開始前に接続相手を判断して，望まない相手とはネットワーク通信を拒絶することが重要となってきている。

この一例として，NTTコミュニケーションズ株式会社は，SIP（Session Initiation Protocol）のセキュリティ機

能を強化したm2m-x（Machine-to-Machine Communication for any [thing | place | time]）と呼ぶP2P通信のためのフレームワークを提案している（**Fig. 9**）。

m2m-xでは，マネージメントサーバを介してSIPによる呼制御を確立することにより，IPアドレス情報の交換を行って，P2Pによるデータの転送を行う。

望まない通信相手に対しては，マネージメントサーバで通信を拒絶するので，IPアドレス情報などが知られることもない。また，SIPの通信はすべて暗号化されているので，第三者がその内容を盗聴することができない。

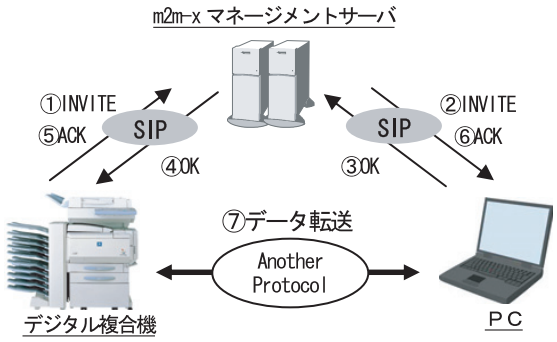

Fig.9 Connection form by m2m-x

5　まとめ

以上，ネットワークのセキュリティ技術とそのデジタル複合機への適用と共に，これからのデジタル複合機で求められるセキュリティ機能のあり方を示した。

今後も，より安全かつより利便性の高いネットワーク機能の開発を行う所存である。

●参考文献

1）岩田 彰（監修），鈴木春洋，奥野琢人，若山公威，高須紀樹，杉江 修，村瀬晋二，“インターネット暗号化技術 ～PKI，RSA，SSL，S/MIME，etc～”，第1版，株式会社ソフト・リサーチ・センター，東京，2002

2）タイムビジネス推進協議会，“概説 e-文書法”，第1版，NTT出版株式会社，東京，2005

3）独立行政法人 情報処理推進機構セキュリティセンター，“PKI関連技術解説”，http://www.ipa.go.jp/security/pki/index.html，東京，2005

4）阪田史郎（監修），金森重友，斉藤允，佐野勝大，“SIP/UPnP情報家電プロトコル”，第1版，株式会社秀和システム，東京，2005