印刷データと印刷物のセキュリティ

西山　由高　　横山　信征
金井　邦夫　　渡邉　泰介

近年，インターネットのブロードバンド接続に代表されるネットワーク接続機器の急増とコンピュータウィルスの蔓延，さらには，各国の個人情報保護に関する法制度面から，電子データや通信プロトコルに関するセキュリティ機能や情報漏洩防止への関心が高まっている（参考文献1を参照）。

プリンタやMFP*1),コピー機等の印刷装置においても，印刷データを格納したハードディスクの盗難，印刷物の盗み見や持ち出し等による情報漏洩が問題視されている。そのため，印刷装置内のデータの暗号化や上書き消去，利用者IDや印刷装置情報を印刷物に重ね合わせることによる情報漏洩抑止といったセキュリティ機能の提供が求められている。

本稿では，情報漏洩防止のためにプリンタが提供している暗号化認証印刷，ディスク消去，ログオン情報強制印刷の各機能について紹介する。

暗号化認証印刷機能

本章では，印刷時にPCからプリンタに送信される印刷データの盗聴や印刷物の盗難による情報漏洩，印刷データの改竄への対策として有効な暗号化認証印刷機能について述べる。

(1) 印刷時のセキュリティ上の脅威と対策

一般に，ネットワーク接続された共有プリンタを用いて，第三者に見られたくない機密情報を含んだ文書を印刷する場合，**図1**のような印刷データの改竄や機密情報漏洩の脅威がある。そのため，印刷データを第三者に見られても内容が分からないようにするとともに［盗聴対策］，印刷データが改竄されたか否かを確認する必要がある［改竄対策］。また，第三者が印刷物を取得できないようにする必要もある［印刷物の盗み見・盗難対策］。

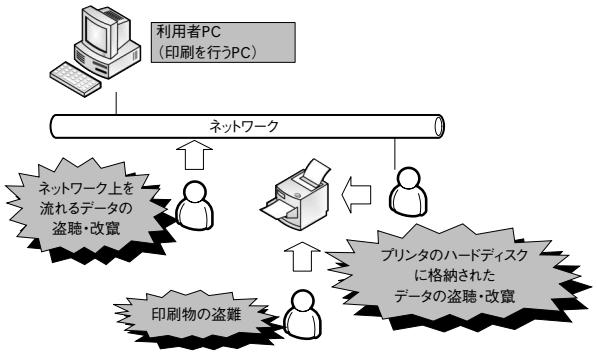

図1　印刷時のセキュリティ上の脅威

このようなセキュリティ対策上の目的から，プリンタには下記のような機能を持たせている。

- 盗聴対策としての印刷データの暗号化
- 改竄対策としてのメッセージ認証コード（Message Authentication Code。以降，MACと呼ぶ）の付加と検証
- 印刷物の盗み見・盗難対策としてのパスワードによる認証印刷

以下では，これら3つのセキュリティ機能について，もう少し詳しく説明する。

印刷データの暗号化は，ネットワーク上で送信中の印刷データやプリンタ内蔵ハードディスクに格納された印刷データが第三者に見られても，印刷データからは印刷内容が分からないようにするためのものである。暗号化は，印刷データを送信する利用者のPC上で行われる。暗号化アルゴリズムには，共通鍵暗号方式の1つであるAES（Advanced Encryption Standard）を使用している。暗号化鍵は利用者が入力するパスワードから生成され，その鍵生成方式は，暗号標準であるPKCS#5（Public Key Cryptography Standard #5）v2.0にしたがっている。詳細は参考文献2を参照のこと。

MACとは，前述の暗号化鍵と暗号化された認証印刷データから算出したハッシュ値である。暗号化鍵を知らないとデータに対応するMACを計算することはできない。MACは，印刷時に利用者PC上で計算され，プリンタに送信される。プリンタでは，暗号化された印刷データか

*1)MFP：（Multi- Function Product / Printer / Peripheral）スキャナ，プリンタ，FAX，コピーの機能のうち2つ以上の機能を有する複合機の略称。

らMACを計算し，その値がPCから送信されたMACの値と一致するか否かを確認することによって，印刷データの改竄の有無を検出する。MACの値が一致すると改竄されていないと判断される。

認証印刷は，使用者がプリンタの操作パネルからパスワードを入力し，そのパスワードに合致する印刷データのみを印刷する機能である。利用者PCから送信されてきた印刷データは，プリンタの内蔵ハードディスク上に一旦格納され，合致するパスワードが入力されるまでは印刷されない。つまり，印刷時にPC上でパスワードを設定した利用者が，プリンタの場所に移動して，操作パネルから同じパスワードを入力して初めてデータが印刷される。そのため，印刷された内容が第三者に盗み見られたり，印刷物が盗まれたりする可能性は極めて小さい。

(2) 暗号化認証印刷とは

暗号化認証印刷は，前述の3つのセキュリティ機能を組み合わせたものである。**図2**は，暗号化認証印刷時の利用者の操作と，利用者PCおよびプリンタ内部での処理の流れを示したものである。

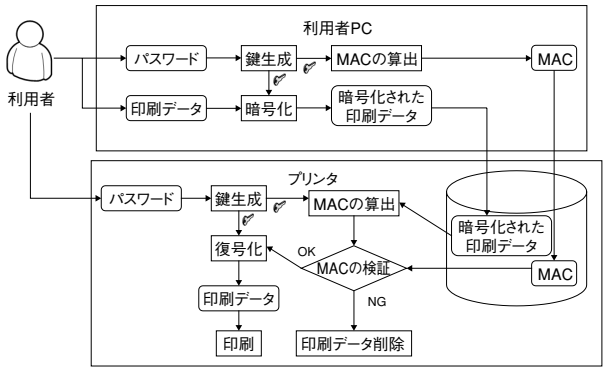

図2　暗号化認証印刷の処理

暗号化認証印刷の利用者は，まず，PCから印刷を行う場合に，プリンタドライバの画面でパスワードを入力する。**図3**にプリンタドライバから暗号化認証印刷の指定をする場合の画面を示す。

プリンタドライバでは，入力されたパスワードを用いて暗号化鍵を生成し，その鍵で印刷データを暗号化して送信する。この時，MACも計算してプリンタに送信されるが，パスワードは送信されない。したがって，ネットワーク上で印刷データが盗聴されても暗号化されているため，印刷内容が漏れる心配はない。

プリンタは，暗号化された印刷データとMACを内蔵

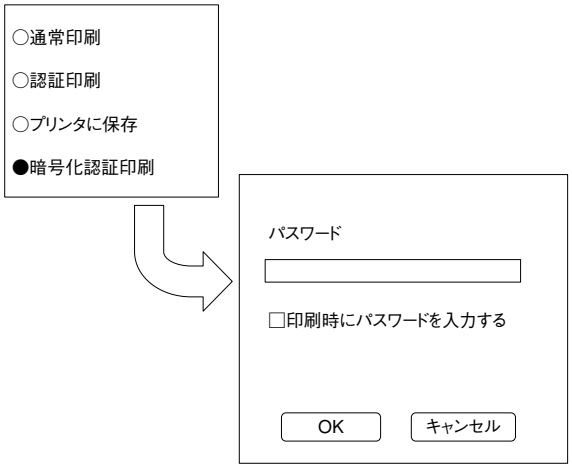

図3　暗号化認証印刷の指定画面

ハードディスクに一旦格納する。このとき，印刷データは暗号化されたまま内蔵ハードディスクに格納されるため，第三者が内蔵ハードディスクを盗んだり，ハードディスク上の印刷データを読み出したりしても，印刷内容が漏れる心配はない。

次に，利用者は，送信データの印刷を開始するために，送信先プリンタの設置場所に移動し，プリンタの操作パネルから，送信時にPC上で入力したのと同じパスワードを入力する。プリンタは，入力されたパスワードから暗号化鍵を生成する。その後，プリンタはその暗号化鍵を用いて，ハードディスクから読み出した暗号化された印刷データのMACを計算し，利用者PCが送信してきたMACと一致するか否かを調べる。MACが一致した場合，プリンタは暗号化された印刷データを復号化し，印刷する。MACが一致しない場合，プリンタは，印刷データは改竄されているものと判断し，印刷することなくデータを削除する。

このように，暗号化認証印刷では，利用者がプリンタにパスワードを入力した後に印刷が開始されるため，印刷物の盗難や印刷内容の盗み見による情報漏洩を防止できる。

ディスク消去機能

プリンタの内蔵ハードディスクには，先に述べた暗号化認証印刷データ以外にも，暗号化されていない通常の印刷データや利用者情報等のデータが格納されている。そのため，ハードディスクが盗難に遭ったり，暗号化データのパスワードが漏洩したりした場合，ハードディスクから利用者情報や印刷データが読み出されてしまう可能性がある。

本章では，このような情報漏洩を防止するために，ハードディスク内のデータが不要になった際に，上書きによってデータを確実に消去するディスク消去機能について述べる。このディスク消去機能では，ファイル単位のデータ消去とハードディスク全体のデータ消去が可能である。

(1) ハードディスク内のデータ漏洩の脅威と対策

一般に，ハードディスク上のデータは，ファイルシステムによって管理されており，データを格納しているファイルは，管理情報と格納対象のデータに分けて格納されている。

通常，ハードディスク（ファイル）に格納されたデータを削除した場合，ファイルの管理情報が消されるだけで，データの中身はハードディスク内に残ったままとなる。そのため，ハードディスクやファイルシステムに精通した技術者ならば，そのような状態のハードディスクから削除されたデータを読み出すことが可能である。

このようなデータ読み出しの対策としては，データを削除する際に，データが格納されている領域に別のデータを上書きする方法が有効である。ただし，データを1回上書きしただけでは，ハードディスクを分解して，特殊な装置でハードディスクの記録媒体上に残った磁気痕跡を読み取ることによって，元のデータを復元できる可能性がある。このような磁気痕跡からのデータ復元を防止するためには，複数回データを上書きするのが有効である。

(2) データ消去方式

ディスク消去機能では，データの消去方式として，以下に示す3通りの方法を提供している。

●単純消去

上書きを行わずファイルの管理情報のみを書き換える方法である。管理情報のみが上書きされるだけであるから処理は高速だが，データの中身はハードディスク上に残ったままとなる。

●クリア（Clear）

米国防総省がDoD5220.22-Mで規定する消去方式の1つで，固定データ「0x00」を1回上書きする。削除するデータ全体の上書きをするため，管理情報のみを削除する場合にくらべ，削除するデータのサイズに比例した処理時間（ハードディスク1へのデータ書き込みに要する）がかかる。DoD5220.22-Mで規定される消去方式の詳細は参考文献3を参照のこと。

●サニタイズ（Sanitize）

米国防総省がDoD5220.22-Mで規定する消去方式の1つで，固定データ「0x00」，「0xFF」，乱数を順に上書きし，最後に書込んだデータが正しく読み出せることを検証する。セキュリティ強度は，3つの消去方式の中で最も高く，磁気痕跡から元のデータ復元される可能性をきわめて低くすることができる。ただし，データを3回上書きした後，データ読み出しによる検証を行うため，3つの消去方法の中で最も処理時間がかかる。

(3) 暗号化認証印刷データの自動消去機能

前記の説明では述べなかったが，暗号化認証印刷では，プリンタの内蔵ハードディスク上に保存された印刷データ（暗号化されている）の削除方法も指定できる。削除方法はプリンタドライバから指定することが可能で，印刷終了後の印刷データの消去方法を，前述の単純消去，クリア（1回上書き），サニタイズ（3回上書き）の中から選択できる。特に，サニタイズを選択した場合，ハードディスク内に残った磁気痕跡から機密データが漏洩する可能性をきわめて低くすることができる。

(4) 内蔵ハードディスク内の全データ消去

内蔵ハードディスク内の全データ消去機能はプリンタのレンタルサービスやプリンタの廃棄を行う場合など，内蔵ハードディスク内に残っている全てのデータを消去したい場合に使用する機能である。本機能を使用することで磁気痕跡から機密情報が漏洩することを防止することができる。

ログオン情報強制印刷機能

印刷データなどの電子ファイルの漏洩防止はサーバ，利用者PCのセキュリティ管理徹底，電子ファイルのコピー防止，暗号化などで対策することができる。しかし，一旦，印刷された紙媒体（印刷物）のコピーや持ち出しによる情報漏洩については各社とも方策を模索している状況である。

本章では，利用者IDや印刷文書名等の情報を印刷物に埋め込むことによって，利用者のセキュリティ意識を高め，印刷物持ち出し等による情報漏洩を抑止することができるログオン情報強制印刷機能について述べる。

(1) 機能概要

ログオン情報強制印刷機能は，プリンタドライバと，設定ユーティリティにより構成される。

専用プリンタドライバは，印刷するドキュメント上に付加情報をウォーターマークとして強制的に付加して印刷する。付加情報には，システムにログオンする際のID，印刷物のドキュメント名，印刷時間などがある。これら

図4　ログオン情報強制印刷機能を使用した印刷例

の付加情報を印刷イメージ上に背景として重ね合わせて印刷する。**図4**はログオン情報強制印刷機能を使用した場合の印刷例である。

印刷されたイメージ上に印刷を行った利用者IDなどの付加情報が視認できるため，心理面から利用者の印刷物管理意識の向上や，持ち出し抑止の効果があり，印刷物による情報流出抑止に役立つ。また，万が一，印刷物が流出したときは，付加情報から流出元を容易に特定できる。

（2）利用環境

本機能は，プリンタドライバと，設定ユーティリティのみをシステムにセットアップするだけで利用可能になるため，きわめて容易かつ安価に情報漏洩牽制の環境を構築することができる。

（3）付加情報設定方法

印刷する付加情報の項目や書式などはシステム管理者が設定ユーティリティを使って任意に設定することができる（**図5**）。これにより，プリンタドライバがセットアップされたシステムから文書を印刷すると，特別な操作なしに付加情報が全ての印刷文書データ上に常に印刷

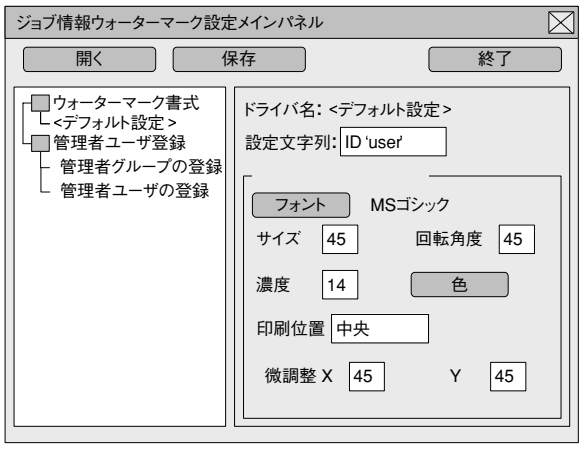

図5　ユーティリティによるジョブ情報設定画面

される。ただし，利用者はこの機能を解除することはできない。

また，顧客に提出する文書や会議の正式資料等，付加情報を印刷したくない場合，特定の利用者に対してのみ権限を与えることで，付加情報なしで印刷することができる。この設定も，システム管理者が設定ユーティリティ（**図5**）を使って任意に変更することができる。

ま と め

以上，プリンタが提供している印刷データおよび印刷物による情報漏洩の防止機能について幾つか紹介した。

印刷装置の高機能化に伴い，印刷装置が，各種サーバや利用者PCと同様に，文書管理システムや業務システムの主要構成要素となっている。そのため，認証サーバやログサーバと連携した高度セキュリティ機能が，印刷装置にも求められている。今後はこのようなシステム連携のためのセキュリティ機能開発を行う所存である。 ◆◆

■参考文献

1）中里博彦，他：“ユビキタスネットワーク時代におけるプリンティングソリューション”，沖テクニカルレビュー204号，Vol.72 No.2，pp.28–31，2005年10月
2）PKCS#5：
http://www.rsasecurity.com/rsalabs/node.asp?id=2127
3）DoD 5220.22-M：
http://www.dtic.mil/whs/directives/corres/html/522022ms.htm chapter 8

●筆者紹介

西山由高：Yoshitaka Nishiyama. 株式会社沖データ ソフトウェア開発センタ ソフトウェア開発第二部 部長
横山信征：Nobuyuki Yokoyama. 株式会社沖データ ソフトウェア開発センタ ソフトウェア開発第一部 チームリーダ
金井邦夫：Kunio Kanai. 株式会社沖データ ソフトウェア開発センタ ソフトウェア開発第一部
渡邉泰介：Taisuke Watanabe. 株式会社沖データ ソフトウェア開発センタ ソフトウェア開発第二部