印刷物へのセキュリティ技術の動向

Trends in Security Technologies for Printed Matters

名古和行* 本田和正* 岩崎圭介* 北村義弘*
Kazuyuki Nako Kazumasa Honda Keisuke Iwasaki Yoshihiro Kitamura

要　旨

企業からの機密情報，個人情報の漏洩事件は後をたたず，単に企業の資産が流出するという問題にとどまらず，お客様の信頼を失い，企業活動に深刻な影響を与えている。また，近年のデジタル技術の発達はめざましく，手軽に高性能なスキャナとプリンタが手に入る環境にあり，チケット，紙幣などの不正コピーの問題もある。このような背景から，デジタル複合機にも「原本性の保証」,「不正コピーの防止」,「情報漏洩の防止」といったセキュリティ機能を求める声が高まっている。本稿では印刷物に焦点をあて，セキュリティ技術の動向を述べる。

Leakage of personal and corporate information has become a perennial threat to business, which could do serious damage through loss of assets and consumer trust. Among other security problems is unauthorized copying of valuable papers such as tickets and banknotes.

These concerns lead to increasing demand for digital multifunction printers with security functions such as verification of document originality and prevention of unauthorized copying and inadvertent disclosure.

In this paper, the authors describe trends in security technologies, focusing on those for printed matters.

まえがき

紙幣や株券などには，その価値を守るため，様々な偽造防止技術が用いられている。しかしながら，近年のデジタル技術の発達はめざましく，誰もが手軽に高性能なスキャナやプリンタを使用して，高品質なコピーを行うことが可能になっている。このため，さらに高度な偽造・不正コピー防止技術が求められている。

また，デジタル技術の発達がコンピュータの使用を広めたため，より多くの機密情報や個人情報をコンピュータで取り扱うようになっている。このため，機密情報や個人情報をプリンタで印刷するなどして持ち出される危険がますます高まっている。昨今の機密情報，個人情報の漏洩事件を見るように，ひとたびこのような事件が発生すると，単に企業の資産が流出するという問題にとどまらず，お客様の信頼を失い，企業活動に深刻な影響を与える結果となるため，情報漏洩を防止する技術が求められている。

このように，印刷物の持つ情報や価値を，偽造，不正コピー，漏洩などから守るためのセキュリティ技術はますます重要視されるようになっている。

本稿では，印刷物を守るためのセキュリティ技術の動向について説明する。

１．印刷物に求められるセキュリティの３要素

「印刷物のセキュリティ」と一口に言っても，紙幣・株券などの有価証券，証明書，機密文書それぞれで求められるセキュリティ機能は異なるが，大きく分けて「原本性の保証」,「偽造・不正コピーの防止」,「情報漏洩の防止」の３要素に分類できる。

これら3要素は全く独立な技術ではなく，互いに関連しあっている場合も多い。

以下にその３要素について説明する。

（１）原本性の保証

原本性の保証とは，印刷物そのものが本物であるということを保証することである。それに加えて，証明

* 技術本部　デバイス技術研究所　第５研究室

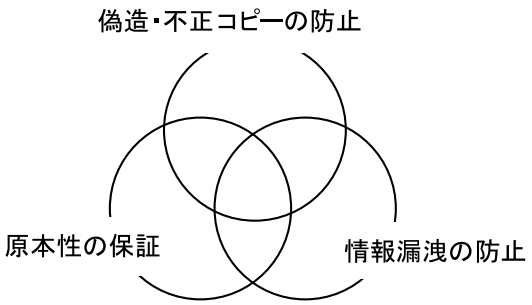

図1　印刷物に求められるセキュリティの3要素
Fig. 1　3 elements of printed matter security.

書などでは印刷物自体も重要であるが,場合によってはコピーが認められているように,印刷されている内容自体が重要視される場合がある。このため,内容が改ざんされたり,書き加えられたりしていないかを保証することも原本性の保証に含まれる。

（2）偽造・不正コピーの防止

原本の裏返しが偽物,コピーであるため,原本性の保証と偽造・不正コピーの防止は密接な関係がある。

偽造・不正コピーの防止技術は,同じものを作ることを困難にしたり,不正にコピーしてもひと目で分かる技術である。

（3）情報漏洩の防止

機密文書など,内容自体が漏れることが問題となる場合,情報漏洩の防止が必要となる。

この手法の一つとして,印刷物に,印刷・コピーに使用した装置を特定するIDや,誰宛の文書なのかなどの情報を埋め込むことで心理的にコピーを抑止し,情報漏洩を防止する方式がある。

また,不正コピーの防止技術の中のコピー自体を禁止する技術は情報漏洩の防止技術の1つでもある。

2．印刷物の偽造・不正コピー防止技術

誰もが手軽に高性能なスキャナやプリンタを利用して,精細なコピーを行うことが可能となってきていることから,より高度な偽造・不正コピー防止技術が求められている。

例えば,紙幣は偽造・不正コピーに対抗するため,定期的に改刷が行われており,常に高度な偽造・不正コピー防止技術が使用されている。このため,紙幣は印刷物の偽造・不正コピー防止技術の集大成とも言える[1)]。紙幣に限らず,株券,有価証券,チケットなどにもさまざまな偽造・不正コピー防止技術が用いられている。

以下に具体的な印刷物の偽造・不正コピー防止技術について紹介する。

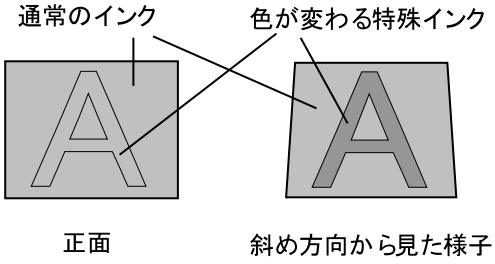

図2　変色する特殊インクを利用した潜像模様
Fig. 2　Latent image with special ink.

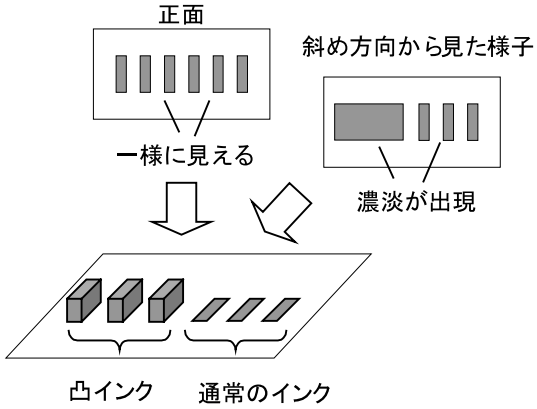

図3　凸インクを利用した潜像模様の原理
Fig. 3　Latent image with pile of ink.

（1）すき入れ

いわゆる（電子的ではない）「透かし」のことである。紙をすくときの厚みを変えることで模様を埋め込む技術であり,光を透過させることで埋め込んだ模様を出現させることができる。

（2）特殊インク

見る角度によって色の変わるインクを使用することで,文字の色を変化させたり,ある方向から見たときだけ模様を出現させることができる。

また,特殊発光インクを用いることで,紫外線をあてたときに模様を発光させることもできる。

（3）潜像模様

見る角度によって色の変わる特殊インクと見る角度を変えても色の変わらない通常のインクを組み合わせて印刷することで,見る角度によって模様を出現させることができる（**図2**）。

また,凹版印刷によるインクの盛り上がり（凸インク）を利用しても,見る角度によって模様を出現させることができる（**図3**）。

（4）ホログラム

レーザで干渉縞をフィルムなどに照射することで像を記録したもの。立体や,見る角度によって文字が変わるような像を記録することができる。

（5）微細文字・模様

非常に微細な文字,線,模様。模様の一部を微細な

文字にしたり,非常に細かい線で肖像画を描いたりすることなどで実現する。

これら，すき入れ紙，特殊インク，凹版印刷による潜像模様，ホログラム，微細文字・模様による効果はスキャナで読み取ることができず,また一般的なプリンタで再現することができないため，偽造・不正コピーを防止することができる。

3．プリンタ・デジタル複合機で実現可能な偽造・不正コピー防止技術

一般的な印刷技術では，特殊インク，凹版印刷，ホログラムなどの手段が利用できるが,印刷プロセスに制約のあるプリンタ,デジタル複合機にはそれらの技術をそのまま適用することはできない。

以下に，プリンタ，デジタル複合機で実現可能な偽造・不正コピー防止技術について紹介する。

3・1　コピーすると出現する潜像模様

潜像模様は，住民票，車検証などの証明書を始めとして，様々なところで利用されている技術である。スキャナの解像度限界を超える細かい点と,同じ濃度に見える粗い点を組み合わせて印刷することで潜像を埋め込んでいる。粗い点は一つ一つの点として読み取れるが，細かい点は，点として読み取れないため，途中の画像処理で消えてしまう。その結果粗い点だけが残り，埋め込んだ潜像が出現する（**図 4**）。「複写」などの文字を埋め込んでおけばコピーすると文字が浮かび上がり,ひと目でコピーしたものであることが分かるため，不正コピーを抑止することができる。

ただし，プリンタ，デジタル複合機でこの潜像模様を実現する場合，同一，もしくは同様の装置を入手することが容易であるため,完全に偽造を防止することはできない。このため，他の技術と組み合わせて用いることが望ましい。

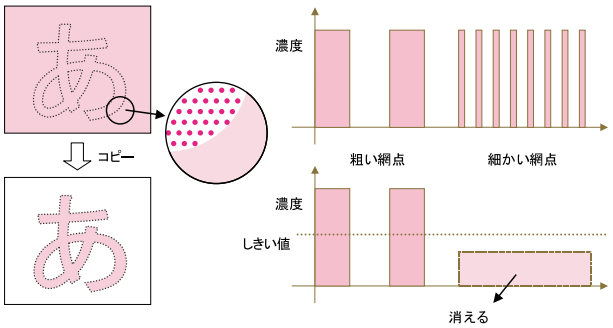

図 4　コピーすると出現する潜像模様の原理
Fig. 4　Latent image visible on copying.

3・2　光沢の違いを利用した潜像模様

カラープリンタのトナーの光沢の有無を利用して潜像模様を埋め込む技術が考案されている[2)]。原理的には**図 2** と同様で，同じ色の，光沢のあるトナーと光沢のないトナーを組み合わせて像を印刷しておくと,光のあて方を変えることで像が現れたり消えたりし,潜像が知覚されるようになる。

見る角度によって見た目が変わるため,スキャナで完全に読み取ることができない。そのため，不正コピーを防止することができる。また，一般ユーザには印刷時のトナーの組み合わせを制御することは困難であるため，偽造防止の効果が高い。

4．情報埋め込み技術

印刷する画像や文書に,情報を埋め込む技術が従来から研究されている[3)4)]。埋め込みには，埋め込む対象となる画像などのコンテンツが持つ冗長性を利用する。改変しても，人間が知覚しづらい冗長な情報を操作して,元データの品質を保ちながら別の情報を持たせるのである。

埋め込む情報の利用方法はいろいろある。例えば，画像などの作品に,著作者情報としてデジタル署名情報を埋め込んでおけば,確かにその著作者の作品であるということを保証することができるし，機密文書に，印刷・コピーに使用した装置を特定するID，誰宛の文書なのかといった情報を埋め込んでおけば,誰から漏洩したのかということがわかるため,心理的に情報漏洩の抑止につながる。このような，原本性の保証や情報漏洩防止の目的で，画像，文書に情報を埋め込む技術に電子透かし技術などがある。

以下，情報埋め込み技術について紹介する。

4・1　画像への情報埋め込み

画像への情報埋め込みの手法はいくつかあるが,その一例として,周波数領域上で数値を変化させて情報を埋め込む技術が挙げられる。変換して得られる周波数成分を見ると,文字や画像の輪郭部分は高い周波数成分を多く含み,滑らかに見える部分は低い周波数成分を多く含んでいる。一般的に画像は，低い周波数成分が多く，高い周波数成分は少ないという特徴があり，また人間の視覚には，高い周波数成分の違いほどわかりにくいという特性がある。

そこで,周波数領域上の特徴を利用したごく簡単な情報埋め込みの例として，画像にあまり含まれず，かつ違いのわかりにくい,高い周波数成分の値を操作することによって情報を埋め込む方法が考えられる。その手順は以下のようになる（**図 5**）。まず原画像を周

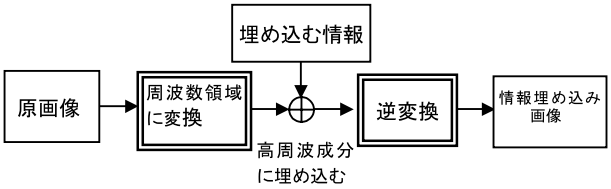

図５　周波数領域上の特徴を利用した情報埋め込みの原理
Fig. 5　Information embedding in frequency domain.

波数領域に変換する。次に，変換した画像の高周波成分の値を，埋め込む情報によって変化させる。これを逆変換すれば，高周波成分に情報が埋め込まれた画像を得ることができる。情報の抽出はまったく逆の操作をすればよい。

周波数領域に変換する技術としては，ウェーブレット変換や離散コサイン変換（DCT）が用いられる。ウェーブレット変換は新しい画像圧縮方式であるJPEG2000でも採用されており，これまで用いられてきたDCTに比べて，情報埋め込みによるノイズや歪みを抑えることができるといった特徴がある。

４・２　文字への情報埋め込み

テキスト文書へ情報を埋め込む技術もある。印刷時の文字の形や配置などを変化させ，情報を埋め込むのである。その例をいくつか紹介する。

まず，文字の形状に注目する方法である（**図６ａ**）。文字は画素の集まりとして表示されるが，曲線となっている部分においては，輪郭を形成する画素の配置に自由度がある。そこで，0を埋め込む部分と1を埋め込む部分で配置を変化させることによって情報を埋め込む。

また，文字幅や間隔を変え，そこに情報を埋め込むという方法も考えられる。文字幅に情報を埋め込むには，例えば0を当てはめる文字は横幅を長くして，1を当てはめる文字は横幅を短くすればよい（**図６ｂ**左）。この例では，文字の横幅Wと縦幅Hの比の値がある値Kより大きいか小さいかによって0と1を区別している。文字の間隔に情報を埋め込むには，0を当てはめる部分は文字間隔を狭く，1を当てはめる部分は広くすればよい（**図６ｂ**右）。先ほどの例と同様に，文字の間隔Sと縦幅Hの比の値と，ある値Kを比較して0と1を区別している。

４・３　コード化した情報との重ね合わせによる情報埋め込み

電子情報をコード化し，印刷する文書に重ね合わせて印刷する技術が考案されている。例えば，文書の内容を電子情報としてコード化し，それを重ねて印刷すれば，コード化した内容と文書の内容を比較することによって改ざんの有無を検出することが可能となる。

重ね合わせる方法としては，二次元コードでコード化して印刷の際文書の空白部分に重ねたり，微細なドットパターンにコード化して，その微細なパターンを並べたものを背景画像として印刷データ全面に重ねあわせる手法などがある。

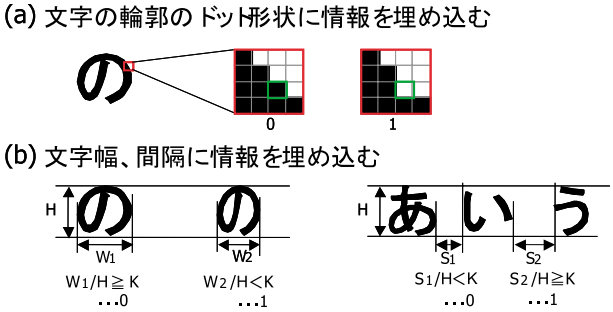

図６　文字への情報埋め込みの原理
Fig. 6　Information embedding into characters.

これまで述べてきたように，印刷物に対するセキュリティ技術として，原本性の保証，偽造・不正コピーの防止，情報漏洩防止を目的とした技術は，広く研究されている。

むすび

昨今，デジタル複合機に対するセキュリティ機能を求める声が高まっている。その中でも，高性能なスキャナ・プリンタの普及により，従来にも増して「紙」の情報のコピーや転用が容易になっており，今後急速に，印刷物に対するセキュリティ機能へのニーズが高まると想定される。本稿では，この印刷物に対するセキュリティ機能についての技術動向を説明した。当社においても，デジタル複合機に対するセキュリティ機能の一環として，既に実用化されているデータセキュリティに加え，ここで述べた印刷物に対するセキュリティ技術を検討していきたい。

参考文献

1）　日本銀行，“新しい日本銀行券（一万円券）の偽造防止技術”，（オンライン），<http://www.boj.or.jp/money/03/bnnew3.htm>，（2004）.

2）　MYCOM PC WEB，“米Xeroxが印刷技術でホログラム効果を実現”，（オンライン），<http://pcweb.mycom.co.jp/news/2003/08/01/51.html>，（2004）.

3）　松井甲子雄，“電子透かしの基礎”，森北出版（1998）.

4）　画像電子学会，“電子透かし技術”，電機大出版局（2004）.

（2004年5月25日受理）