社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34 (42)
2006／7／21

紙文書に対するセキュリティ技術の考察

海老澤 竜† 藤井 康広† 高橋 由泰† 手塚 悟†

†日立製作所システム開発研究所 〒212-0058 川崎市幸区鹿島田 890

E-mail: (rebisawa, fujii, yoshiyas, tezuka)@sdl.hitachi.co.jp

あらまし：個人情報保護法の施行や日本版 SOX 法の適用が見込まれる中、情報の漏えいや偽装などの不正が問題になってきている。特に紙媒体を経由した個人情報漏えいは、漏えい全体の 45.9%にも上っており、見過ごせない問題である。このような紙文書の脅威に対して、複写牽制文字、電子透かしなど印刷物自体に工夫を施す対策や、印刷機器利用時の本人認証、またはそれと連携した印刷履歴管理などのデジタルなセキュリティ対策がある。本発表ではこれら、紙文書に対するセキュリティ対策を整理分類してその課題を明確にし、今後の技術の目指すべき方向について議論する。

キーワード 情報漏えい、改ざん、電子透かし、複写牽制文字、本人認証

A Study on Security Technologies for Paper Documents

Ryu Ebisawa† Yasuhiro Fujii† Yasuhiro Fujii† and Satoru Tezuka†

† Systems Development Laboratory, Hitachi Ltd. 890 Kashimada, Saiwai-ku, Kawasaki, 212-0058 Japan

E-mail: (rebisawa, fujii, yoshiyas, tezuka)@sdl.hitachi.co.jp

Abstract: While the administration of the Privacy Law and the expected application of J-SOX (Japanese version of The Sarbanes-Oxley Act of 2002) are drawing much attention, leakage and fraudulent handling of information has become a serious matter. In particular, personal data leakage through paper documents is not to be overlooked as it accounts for 45.9% of all the leakage. There are, as measures against such threats to paper documents, technologies that add special function to the printed matter itself such as copy deterrent characters and digital watermarks, and also digital security measures such as user identification functions for printing machines and print log management in coordination with the identification. In this paper, security measures for paper documents are categorized to clarify their challenges, and the directions to which the technologies must aim are discussed.

Keyword: Information Leakage, Data Falsification, Digital Watermark, Copy Deterrent Characters, User Identification

1. はじめに

2005年の個人情報保護法の施行や日本版SOX法の適用が見込まれる中、公共機関や民間企業における情報の漏えいや不正が問題になってきている[1]。情報漏えいの原因、経路は複数ありえるが、その中でも紙媒体を経由した個人情報漏洩は全体の45.9%にも上っており[2]、コンプライアンスの観点からも大きな問題でとなっている。

情報漏えいなどの脅威に対して、印刷機器利用時の本人認証、またはそれと連携した印刷履歴管理などが紙文書に対するデジタルなセキュリティ対策として考えられてきた。しかし、たとえ電子文書をアクセス制御技術、ファイアウォール技術、PKI、電子署名技術などでセキュアに管理したとしても、一度紙文書として印刷されてしまえば、情報漏えいや改ざん・偽造が可能になってしまうことが容易に想像できる。そこで紙文書自体のセキュリティ対策が求められ、複写牽制文字、電子透かしなど印刷物自体に工夫を施す対策が注目されてきている。

本文ではこれら、紙文書に対するセキュリティ対策を整理分類してその課題を明確にし、今後の技術の目指すべき方向について議論する。

2. 紙文書

2.1. 紙文書の役割

計算機がオフィスに普及し、文書を電子的に作成、編集、閲覧することが通常業務で頻繁に行われるようになった。しかし、依然として文書を紙に出力する行為はなくなってはいない。その理由をここで考察する。

まず、電子文書は、

- 省スペース、大容量
- 検索が容易
- 広範囲への配布が容易

といった利点と、

- 物理的実体がみえなく、情報のありかが直感的

表1：紙文書に対する脅威

脅威		内容		脅威対象文書	例
行為	偽造	偽のものを作ること。		—	契約書の偽造
	複製	正規に印刷されたものと（外見が）同じものを偽造すること。		—	複写、スキャン/プリント
	改ざん	情報を（悪意をもって都合の良いものに）置き換え不正な紙文書を作成すること。		—	納税証明書の税金額を改変
インシデント	不正利用	正規の紙文書保持者ではない者が正規の紙文書保持者を装うこと。なりすまし。		契約書、証明書	他人の住民票を利用して申請
		正規の紙文書保持者が不正な紙文書を利用すること。		契約書、証明書、申込書	借用書の数値を改ざんし、提示
	情報漏えい	正規の情報保持者ではない者が情報を参照できてしまうこと。	不注意（置き忘れ・送信操作ミス、廃棄し忘れ、紛失、盗難など）	機密情報・社外秘・顧客情報などを含む文書	顧客情報の記録された書類の廃棄忘れ、紛失
			故意（不正コピー・不正送信、持ち出しなど）		社員が顧客名簿を複写し持ち出し

に分かりづらい

・変更、複製が容易かつ痕跡が残りづらい

などの欠点がある。これに対して情報媒体としての紙には

・入出力が容易、参照性が高い

・情報の存在が直感的に分かりやすい

・情報を手軽に渡せる

・情報の不変性を示唆することができる

という特徴がある。

紙文書には、思いついたことをその場でメモ書きできる、重要な項目に下線を引くことができる、というように情報に直接的に触れることができ、人にとって直感的にわかりやすいという利点がある。また、ページをめくりながら文書全体を広範囲に見渡すことができ、注目範囲の変更も目を移すだけであり容易である。さらに、安価で取り扱いが簡単であるため、誰にでも対面で情報を手渡しできる。

紙に情報を載せると、「情報の不変性を示唆することができる」というのも重要な特徴である。依頼書や契約書のような重要文書は通例紙に出力されるが、これは情報を紙に印刷すると、その紙を金庫などの物理的なセキュリティで守ることができること、紙に対する改ざんでは痕跡が残りやすいこと、などがその理由である。

このように紙文書の情報インターフェイスとしての役割は電子文書ではとって変われない部分を持っているため、我々の生活から紙文書がなくなることはないと考えられる。

2.2. 紙文書の分類

セキュリティ技術で守られるべき紙文書にはどのようなものがある考察するために、紙文書の分類を考える。「電子のままではなく、紙に出力して利用する理由」の観点で分類を行った。

・参照性重視

読みやすさをその理由として一時的に紙に印刷された文書。（連絡・通達書、文字量の多い文章など）情報を対面で手軽に渡せることも利便性を高めている。（カタログ類）

また、一時的に印刷された会議資料には、経営情報・顧客情報など、が記載される場合が多く、利用後は直ちに廃棄することが望ましい。

・不変性重視

文書の情報に変更がないことを示唆するために紙に印刷された文書。法律により保存を義務付けられているものもある。最近では帳簿の電子保存も認められてはいるが、まだまだ紙での保存が主流である。許可、認可を伴い押印される場合が多い。（帳簿類・契約書・申込書・証明書など）

3. 紙文書に対する脅威

表1に紙文書に対する脅威を示す。表は「行為」と「インシデント」の二項目に分かれている。さらに「行為」は三項目、「インシデント」は二項目に分類される。ここに示した「行為」などを手段として、「インシデント」が引き起こされる、という関係にある。

紙文書の「偽造」とは、例えば実際には存在しない偽の契約書を本物らしく作る、などというように偽の

表2：紙文書の脅威に対応する技術の要件

脅威			対応技術の要件
行為	偽造		偽造・複製防止機能 （抑止効果）偽造・複製検知機能
	複製		
	改ざん		改ざん検知機能
インシデント	不正利用	正規の紙文書保持者ではない者が正規の保持者を装うこと。なりすまし。	偽造・複製防止機能、偽造・複製検知機能 電子文書の権限管理、本人認証 注意喚起
		正規の紙文書保持者が不正な紙文書を利用すること。	複製防止・検知機能 改ざん検知
	情報漏えい	不注意（置き忘れ・送信ミス、廃棄し忘れ、紛失、盗難など）	注意喚起 （抑止効果）紙文書追跡
		故意（不正コピー・不正送信・持ち出しなど）	複製防止機能 （抑止効果）紙文書追跡、複製検知機能

文書を作ることを指す。

紙文書の「複製」とは、正規に印刷されたものと外見が同じものを偽造することであり、複写機でのコピーや、スキャナでの読み込みとプリンタ出力などで実現される。

紙文書の「改ざん」とは、正規の紙文書の保持情報を別の情報に置き換えて不正な紙文書を作成することである。スキャナ読み込みで得られた画像を電子的に処理変更して、再び紙に印刷するなどの手法で実現される。

紙文書の「不正利用」は二種類に分かれる。紙文書の正規の保持者ではない者が正規の保持者を装うこと、紙文書の正規の保持者が不正な紙文書を利用すること、である。前者は、正規の紙文書そのものを不正に入手するか、偽造・複製することで実現される。後者は、正規の紙文書を複写や改ざんし、その保持者が利用することにあたる。

「情報漏えい」には不注意が原因のものと故意のものとがある。不注意による情報漏えいとは、紙文書の置き忘れ、送信ミス、廃棄し忘れ、紛失、盗難などが原因で起こる情報漏えいであり、故意の情報漏えいとは不正コピー、不正送信、持ち出しなどによる情報漏えいを表す。

4. 紙文書に対するセキュリティ技術

4.1. 技術の機能要件

表1に示した紙文書の脅威に対応するセキュリティ技術に求められる要件を表2に示す。

偽造・複製に対応するために、偽造・複製防止機能が必要である。また防止機能よりもセキュリティレベルは下がるが、偽造・複製検知機能には抑止効果が見込める。

改ざんに対応するためには、改ざんを検知する機能が必要である。さらには、改ざん箇所、改ざん前の情報までも明らかにする機能があることが望ましい。

正規の紙文書保持者ではない者が正規の保持者を装うことに対応するためには、正規の紙文書の偽造・複製とともに、不正入手も防がなければならない。電子文書へのアクセスに関する適切な権限管理や正しい本人認証ができることが要件となる。また不注意による情報漏えいに対応する要件と等しく、正規の紙文書が正規の紙文書保持者の管理外に出てしまうことを防ぐために、保持者の注意を喚起することも要件となる。

正規の紙文書保持者が不正な紙文書を利用することに対応するためには、不正な紙文書の生成を防ぐことが必要である。要件としては複製の防止・検知、改ざん検知である。

情報漏えいへの対応として、紙文書を追跡する機能が抑止効果を発揮する。加えて、不注意による情報漏えいに対応するためには、正規の紙文書保持者に対して注意喚起を行えること、故意の情報漏えいに対応するためには複製防止・検知、が要件となる。

また紙文書に対するセキュリティ技術には、紙文書のセキュリティを担保しつつも紙文書の利便性を極力損なわないこと、悪意のある攻撃に対する耐性を持ち合わせること、が望ましいであろう。

4.2. セキュリティ技術

表3に紙文書に対するセキュリティ技術とその効果、課題を示す。

4.2.1. 背景文字

文書の行間、余白部分などの背景部分に、文字や図を本文と重ねて埋め込む技術である。埋め込まれた情報が目視でそのまま理解できる特徴を持っている。「社

表3：セキュリティ技術の効果とその課題

セキュリティ技術		効果				課題	
		紙文書追跡	改ざん検知	偽造・複製対策	その他		
背景文字		○	−	−	注意喚起	外見損なう	
複写牽制文字		−	−	複写検知	複写牽制	外見損なう、浮き出しが弱い場合がある	
電子透かし	見える	○	○	複写制御	不正抑止	外見損なう	情報抽出失敗の可能性、複写制御は複写機依存技術
	見えない	○	−	−	−	情報量少	
二次元バーコード		○	○	−	−	付加情報と文書コンテンツが切り離せる	
ICタグ		−	−	−	紙文書管理	高コスト、特殊なハードウェアが必要	
特殊印刷		−	−	偽造・複製防止	−		
認証・アクセス制御		−	−	−	権限管理、本人認証	紙文書と技術が空間的に乖離	
操作履歴管理		−	−	−	不正抑止、操作履歴蓄積		

外秘」、「持ち出し禁止」などと印字すれば注意喚起の効果を与えるほか、印刷情報（印刷者のID、印刷時間、印刷プリンタ名など）を背景に埋め込むことで情報流出元を特定でき、紙文書の追跡が可能となる。

課題としては、

・元の文書が読みにくくなる場合がある
・文書の見栄えを損なう
・文書によっては背景文字が見づらい

などが挙げられる。

4.2.2. 複写牽制文字

文書の背景部分に特殊なマスクパターン（地紋）を印刷し、その紙文書が複写された場合に複写物の背景に「無効」などの文字を浮かび上がらせる技術である[3]-[6]。紙文書中の微小点は複写されずに白抜きになるという複写機の特性を利用して、文字などが浮かび上がるようにマスクパターンを印刷する。

複写物では元の紙文書にはない文字などが浮かび上がっているため、元の紙文書とその複写物を区別することができるようになる。複写を禁止したい紙文書を印刷する場合にこの複写牽制文字を埋め込むことで、複写に対する注意喚起が可能となり、複写を心理的に抑制する効果がある。

背景文字と同様に

・元の文書が読みにくくなる場合がある
・文書の見栄えを損なう

という課題があり、さらに

・複写される前の紙文書でも牽制文字が浮き出て見えてしまうことがある
・プリンタ・複写機の組み合わせによっては文字などの浮き出しが弱いことがある

という課題もある。

4.2.3. 電子透かし

紙文書に電子的な情報を埋め込む技術である。埋め込み方法としては、情報の埋め込み事実が目に見える形である埋め込み方式と、一見埋め込み事実が視認できないように埋め込む方式とがある。前者は元の文書と透かし埋め込み後の文書の見た目の違いが認知できるので、特別な処理が施されていることが一目で分かり、後者は従来通り自然な見た目のまま情報を埋め込む方法である。ここでは前者を「見える電子透かし」、後者を「見えない電子透かし」を呼ぶこととする。

どちらの電子透かしにおいても、埋め込まれた情報は紙文書のスキャンイメージを専用のソフトウェアで解析することによって抽出される。

・見える電子透かし：

文書の背景部分などにマスクパターンを描くことで電子情報を埋め込む[7][8]。埋め込む情報の違いにより、以下のような異なる機能を持つ。

・埋め込み情報を利用して、紙文書が改ざんされた場合にそれを検知する機能
・印刷情報を埋め込むことによる紙文書の追跡機能
・複写機にて埋め込み情報を読み取り、複写制御を行う機能。例えば、特定のコードが埋め込まれた印刷物の複写を禁止する機能

また、透かし処理が施されていることが一目で分かるため、不正を心理的に抑止する効果も期待できる。

・見えない透かし：

文書に含まれるフォント・図形の位置・形・階調のわずかな変更により、電子情報を埋め込む[8][9]。また、

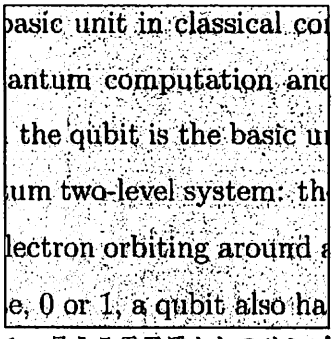
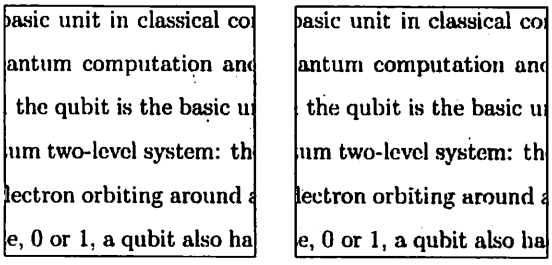


図１：見える電子透かしのサンプル



（左：オリジナル、右：電子透かし埋め込み済み）

図２：見えない電子透かしのサンプル[4]

図３：二次元バーコードのサンプル

上記見える電子透かしのようにマスクパターンを用いて情報を埋め込むが、それを人間の目に目立たない色で印刷する電子透かしもここに分類される[10]。

目立たないように情報を埋め込むため、埋め込み情報量は見える電子透かしに比べて少ない傾向がある。印刷情報を埋め込むことにより、紙文書の追跡機能を実現する製品が市場に出ている[11]。

電子透かしの課題としては、程度の差はあるが、背景文字、複写牽制文字と同様に、

・元の文書が読みにくくなる場合がある
・文書の見栄えを損なう

があげられ、また、

・印刷物の歪み、複写による画質劣化、紙の汚れ・しわなどが原因で埋め込み情報の読み取りが難しい場合がある
・埋め込み情報を利用した複写制御は、特定の複写機でしか実現できない

ことも課題である。

4.2.4. 二次元バーコード

紙文書の白紙の領域に二次元バーコードと呼ばれる、デジタル情報を保持した画像を印刷することにより、紙文書に情報を付加する技術である。埋め込む情報に従って、紙文書追跡や改ざん検知の機能を実現することができる。韓国でこの技術を利用したソリューションの導入例がみられる[12]。

しかし、

・二次元バーコード部分を切り離すなどの方法で付加情報を文書のコンテンツと切り離すことができ、追跡を逃れることが容易である
・情報埋め込み位置が視認できるため、攻撃をすべき箇所が明らかである

などの課題がある。

4.2.5. IC タグ

電子的な情報を保持することが可能な IC タグや、磁性ワイヤーを紙に漉き込むなどして、紙文書に電子情報を添付する技術である[8][13][14]。保持情報は専用のセンサーで読み取る。タグ等が保持する情報によって紙文書管理を実現でき、持ち出し、盗難、紛失などを検知できる。

紙一枚一枚に IC タグ等をつけること、保持する電子情報の抽出に専用のセンサーが必要なこと、などが原因で高コストであることが課題である。また、印刷内容の消去と再印刷が可能な特殊用紙にタグ等を埋め込むことで再利用を可能としコストダウンを図ることも考えられてはいるが、印刷・印字消去に専用機器が必要であり、利用シーンが限られる。

4.2.6. 特殊印刷

印刷する用紙やインクに特殊なものを用いることによって偽造・複製を防止する技術である。ホログラムや、角度によって特殊な見え方をするインク・用紙などがあり、主に金券になどに採用されている[15]。

得られるセキュリティのレベルが非常に高い反面、印刷にあたって特殊なインク・機器が必要であること、特殊な加工紙であること、などが原因でコストが高いことが課題であり、一般の紙文書に採用することは難しいと思われる。

4.2.7. 認証・アクセス制御

電子文書をデータベースで一括管理し、パスワード、IC カード、生体情報などを利用して利用者の本人認証を行い、あらかじめ登録された権限に応じてアクセス

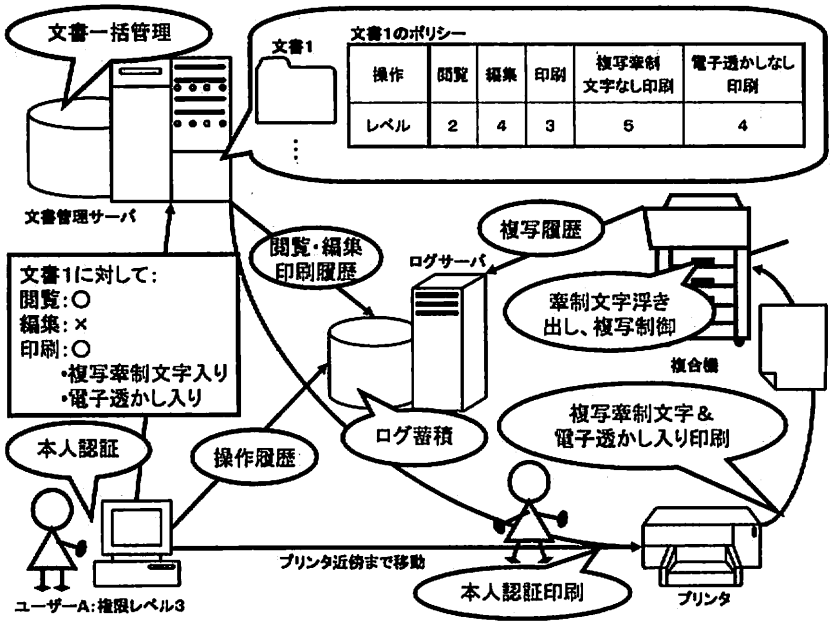


図４：想定イメージ

を許可するシステム技術である。またプリンタで印刷を開始する際にも、印刷機器の近傍で印刷者の本人認証を行った後に印刷を開始するようにもする。

この技術によって以下のことが実現できる

・本人認証により成りすましを防止
・印刷機器回りの紙文書の盗難、取り忘れの防止
・権限管理を行うことで、文書に対して許可されたユーザーにのみ閲覧・編集・印刷を許可

4.2.8. 操作履歴管理

紙文書の印刷記録を収集・蓄積する技術を用いて印刷日時や印刷文書のイメージをログに残すシステム技術である。印刷紙文書を用いた不正が発生した場合に活用できる証拠を蓄積しておけることとなり、また、不正な印刷を抑止する効果がある。

さらにこれを拡張して、印刷だけではなく PC のあらゆる操作を履歴に残すことにより、電子的な不正をも抑止するトータルな抑止力を期待できる。

認証・アクセス制御・履歴管理に共通する課題として、紙文書と各技術の存在が空間的に乖離しているため、電子的に担保したセキュリティが紙に出力した文書について回ることができない、ということが挙げられる。

5. 考察

以上、紙文書に対するセキュリティ技術の効果、課題を示した。

筆者は、今後これらのセキュリティ技術の目指すべき方向は、

・個々の技術において課題のクリア
・電子・紙のセキュリティ技術の組み合わせ

であると考える。

例えば背景文字、複写率制文字、電子透かし技術については、

・画質向上を目指す
・対応プリンタ・複写機の幅を広げて汎用性を向上させる

ことが必要である。電子透かしについては、埋め込み情報量の増大、情報検出精度の向上なども望まれる。

二次元バーコードの改ざん検知効果については、文書コンテンツと付加情報が可分であることは問題とならない。これは、二次元バーコードが取り除かれた契約書や証明書は無効とすればよいからである。しかし、バーコード自体を改ざんされる脅威は依然として残るため、付加情報の暗号化などが必要であると考える。

IC タグ、特殊印刷についてはその高コストと引き換えに高いセキュリティが実現できている。コストダウンのための技術開発と並行して、そのコストでも十分適用価値のあるシーンを想定し、適用システムを構成することが必要である。

電子的なセキュリティ技術である、認証・アクセス制御、操作履歴管理技術の課題は、担保したセキュリ

ティを印刷紙文書に付加したままにできないことであった。そこで、これら電子的なセキュリティ技術と、背景文字、複写牽制文字、電子透かし、二次元バーコードなどの印刷のセキュリティ技術を組み合わせることが求められる。

これは、文書管理サーバにて電子文書を一括管理し、さらに以下のような特徴を併せ持つシステムを構成することである。

- 利用者の本人認証をPC、プリンタで行う
- 利用者ごとに権限レベルを適切に設定する
- 電子文書ごとにポリシーを設定する
- ユーザーの権限レベルと電子文書のポリシーに応じて、閲覧・編集・印刷などを許可し、さらに印刷のセキュリティ技術を制御する
- 印刷を含む、利用者の各種操作の履歴を管理する

個々の電子文書のポリシーにおいて、閲覧・編集・印刷のレベルが設定されていて、ユーザーの権限レベルがそのレベル以上でないと各種操作を許可しない。さらに印刷が可能であっても、ユーザーの権限レベルが設定された印刷のセキュリティ技術の解除レベル以上でないと、背景文字・複写牽制文字・電子透かし、二次元バーコードなどを自動的に埋め込むようにする。

例として図4に、その想定イメージを示す。ユーザーAの権限レベルが3であるので、文書1の閲覧、印刷は許可されるが、編集は許可されない。さらには文書1のポリシーにて設定された、複写牽制文字なし印刷・電子透かしなし印刷のレベルをユーザーの権限レベルがともに超えていないため複写牽制文字・電子透かしが自動的に埋め込まれる。

このように複数のセキュリティ技術を組み合わせ、電子と紙のセキュリティをシームレスに保証するシステムの開発が、今後技術の目指す方向だと筆者は考える。そのためには、複数の対策技術が一つの紙文書に同時に施された場合にそれぞれが有効な状態で共存できるように、それぞれの技術の研究を進める必要もあると考える。

6. おわりに

以上、紙文書に対するセキュリティ技術を整理分類し、その課題、今後の技術の目指すべき方向について議論した。

IT化が進み、技術の進歩とともに効率・利便性が向上してゆくと同時に、セキュリティに対する新たな脅威が生まれてこないとも限らない。引き続き数々の対抗技術、システムの開発が必要になると考える。

文　献

[1] 電子情報技術産業協会，“コンピュータセキュリティの市場・技術に関する調査報告書”

[2] ＮＰＯ日本ネットワークセキュリティ協会，“2004 年度情報セキュリティインシデントに関する調査報告書”

[3] http://www.canon-sales.co.jp/Product/appli/truststamp/

[4] http://www.fxpsc.co.jp/solution/solutions/solution03.html

[5] http://www.ricoh.co.jp/imagio/security/

[6] http://www.i-love-epson.co.jp/products/offirio/sw/security/sec03.htm

[7] 須崎雅彦，須藤正之，“印刷文書への透かし埋込および抽出方法，” 電子情報通信学会論文誌，A Vol.J87-A，No.6，pp.778-786，2004

[8] 伊藤健介，左右田宏之，井原富士夫，木村哲也，布施マリオ，“富士ゼロックス テクニカルレポート，” No.15，pp.32-41，2005

[9] 藤井康広，中野和典，越前功，吉浦裕，手塚悟，“局所特徴量を用いた二値画像用電子透かしの画質維持方式，” 情報処理学会論文誌，vol.44，no.8，pp.1872-1883，Aug.2003.

[10] Electronic Frontier Foundation, "DocuColor Tracking Dot Decoding Guide," http://www.eff.org/Privacy/printers/docucolor/

[11] http://www.hitachi.co.jp/Prod/comp/Secureplaza/sec_prod/densisukasi/index.html

[12] http://www.markany.com/eng/e-Page%20Safer/e-PageSafer%20CaseStudy.pdf

[13] http://www.dnp.co.jp/ictag/ictag_basic/ictag.html

[14] http://www.hitachi.co.jp/Prod/comp/traceability/

[15] 日本印刷技術協会(JAGAT)，"JAGATinfo 2001 年 5 月号より" http://www.jagat.or.jp/story_memo_view.asp?StoryID=2075