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

2008－CSEC－42（8）
2008／7／24

マルチベンダ紙文書漏えい対策システムの一提案

藤井 康広† 海老澤 竜† 本多 義則† 洲崎 誠一†

†株式会社日立製作所システム開発研究所 〒244-0817 横浜市戸塚区吉田町292
E-mail: (yasuhiro.fujii.sj, ryu.ebisawa.st, yoshinori.honda.tb, seiichi.susaki.gw)@hitachi.com

あらまし： 近年、組織内からの情報漏えいが大きな問題になってきている。特に紙媒体を経由した情報漏えいは漏えい全体の43.8%にも上っており、見過ごせない問題である。紙文書の情報漏えい対策としてすでに数多くの製品が提供されているが、これらは特定のプリンタや複合機の機種でしか動作せず、互換性について考慮されていない。よって、さまざまな機種のプリンタや複合機が混在する一般的なオフィス環境では機能せず、結局紙文書の情報漏えいを防止できていないのが現状である。そこで本発表では、プリンタや複合機の機種に依らずに印刷・複写の履歴管理を行うことができるマルチベンダ紙文書漏えい対策システムの一提案を行う。提案方式を実際のプリンタ・複合機で実装したので報告する。

キーワード 情報漏えい、紙文書、印刷、複写、バーコード、透かし

A System against Leakage through Paper Documents in Multi-Vendor Environment

Yasuhiro Fujii† Ryu Ebisawa† Yoshinori Honda† and Seiichi Susaki†

† Systems Development Laboratory, Hitachi Ltd. 292, Yoshida-cho, Totsuka-ku, Yokohama-shi, 244-0817 Japan
E-mail: (yasuhiro.fujii.sj, ryu.ebisawa.st, yoshinori.honda.tb, seiichi.susaki.gw)@hitachi.com

Abstract: The leakage of confidential information has become a serious matter. In particular, the leakage through paper documents is not to be overlooked because it accounts for 43.8% of all the leakages. As measures against such threats to paper documents, many techniques that monitor printing and photocopying have been developed. Those techniques, however, are not compatible and thus do not work in a general office where various models of printers and photocopying machines are used. In this paper, a system that runs on multi-vendor environment is proposed against the leakage of paper documents. Furthermore, an implementation of the proposed system is shown.

Keyword: Information Leakage, Paper Document, Print, Photocopy, Bar-code, Watermark

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43.8%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となっている。

紙文書の情報漏えい対策として、プリンタや複合機にて印刷や複写の制御を行う製品が数多く提供されている[3-5]。しかし、これら製品は特定のプリンタや複合機の機種でしか動作しないため、さまざまな機種のプリンタや複合機が混在する一般的なオフィス環境では、結局紙文書の情報漏えいを防止できていないのが現状である。

このような現状を鑑みて、本発表では、プリンタや複合機の機種に依らずに印刷・複写の履歴管理を行うことができるマルチベンダ紙文書履歴管理システムを提案する。そして提案方式を実際のプリンタ・複合機で実装したので報告する。

第2章で紙媒体経由の情報漏えいとその対策技術について説明し、これら対策技術が機種依存であることを明らかにする。第3章でマルチベンダな対策技術を提案し、第4章で実装を紹介する。

2. 従来の紙文書漏えい対策とその課題

これまで、紙文書の情報漏えい対策技術としてさまざまな方式が研究開発されてきた。これら従来技術とその課題について説明する。

2.1. 従来の紙文書漏えい対策技術

文献[6]に従うと、従来の紙文書漏えい対策技術は以下のようにまとめることができる。

- **印刷・複写時の認証**：印刷・複写時にICカードなどで本人認証を行うことで、成りすましを防止し

たり、課金を行ったりする。

- **紙文書に情報付加**：バーコード、電子透かしなど、紙文書を識別したりユーザに注意喚起を促したりするために、紙文書自体に何かしらの情報を付加する。
- **印刷・複写制御**：電子ファイルの属性に応じて印刷を禁止する。また、紙文書に付加された識別情報をもとに複写を禁止する。情報漏えいの防止につながる。
- **履歴管理**：いつ、誰が、どんな電子文書（紙文書）を印刷（複写）したかといった印刷・複写のログを保存しておくことで、万一紙文書が漏えいしたときに漏えい元を特定可能にする。情報漏えいの抑止につながる。

特に紙文書への情報付加技術として以下のようなさまざまな方式が提案されている。

- **背景文字**：文字や図を本文と重ねて書き込む技術である。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。「社外秘」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。
- **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方式[3-5,7,8]と、埋め込み事実を視認できないように埋め込む方式[9,10]とがある。どちらの方式においても、埋め込まれた情報は紙文書のスキャン画像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。印刷情報を埋め込むことで印刷物を追跡する製品[11,12]や、複合機にて埋め込み情報を読み取って複写制御を行う製品[3-5]などが知られている。
- **バーコード**：紙文書の白紙の領域にバーコードを印刷することで紙文書に情報を付加する技術である。電子透かし同様、埋め込む情報に従って紙文書追跡や複写制御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[13]。
- **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付加する技術である[8]。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る。

2.2. 従来の紙文書漏えい対策システム

これら従来技術を用いて紙文書の情報漏えいを防止・抑止する典型的な方法は、以下の手順による[6]。

① **ポリシー設定**：文書の機密度に応じて印刷・複写に関するポリシーを設定しておく。すなわち、極秘の文書に関しては漏えいを確実に防止するために印刷を禁止する。そうでない社外秘程度の文書については、印刷を禁止してしまうと紙が持つ利便性を損なってしまうので、複写を禁止して広範囲への配布・紛失を防止する。社外秘でもない一般文書に関しては特に制限を行わない。

② **印刷**：まず認証を行い、ユーザの成りすましを防止する。次に電子透かしやバーコードなどの紙文書への情報付加技術を用いて、紙文書の識別情報を印刷物に付加して印刷する。同時にいつ、誰が、どの電子文書を印刷したかなどといった印刷のログ情報を保存しておく。漏えいを確実に防止したい機密文書に関しては印刷を禁止するなどの印刷制御を行う[3-5,11,12]。

③ **複写**：まず認証を行い、ユーザの成りすましを防止する。次に紙文書に付加された情報を検知し、どの紙文書を複写したのか明らかにし、必要に応じて複写禁止といった複写制御を行う。同時にいつ、誰が、どの紙文書を複写したかなどといった複写のログ情報を保存しておく[3-5]。

④ **情報漏えい時**：印刷を禁止した文書に関しては印刷を禁止しているため、紙媒体で情報が漏えいすることはない。印刷を許可した文書が漏えいしたとき、漏えいした紙文書に付与された識別情報や紙文書中のテキスト情報、紙文書の印刷イメージをトリガーに保存されている印刷・複写ログを検索すれば、漏えい元を特定できる[3-5,11,12]。

ただし、これらの手順、特に複写の制御・管理までカバーできるシステムはまだ少ない。これは、複合機の仕様が公開されておらず、複合機ベンダ以外に実装することが困難であるためと考えられる。詳しくは以下で考察する。

2.3. 従来の紙文書漏えい対策の課題

上記のような紙文書の漏えい対策技術の課題として以下があげられる。

- **プリンタの仕様が非統一・非公開**：紙文書へ情報を付加するためには、印刷ジョブ自体を改変する必要がある。ところが印刷ジョブの仕様はベンダごとに非統一で互いに互換性がない。さらに、印刷ジョブのフォーマットはプリンタ製造ベンダの差別化技術であり、完全に公開されていない。そのため、ベンダ以外の第三者が印刷ジョブを操作して情報を付加することは困難である。
- **複合機の仕様が非統一・非公開**：複写時における紙文書漏えい対策技術は複合機と連携しないと動作しないが、複合機の仕様もベンダごとに非統一で互いに互換性がないのが現状である。例えば、

A 社製の複合機で複写制御できるように紙文書に情報を付与したとしても、B 社製の複合機では制御できずそのまま複写できてしまう。さらに、複合機の内部仕様は複合機製造ベンダの差別化技術であり、完全に非公開である。そのため、ベンダ以外の第三者が複合機を外部から完全に制御することは難しい。なお、日本国内においては複合機の標準化団体が存在するが[14]、残念ながら標準仕様に関してはまだ議論中である。

- **情報付加方式が非統一**：紙文書への情報付加方式として電子透かしやバーコードなどがあるが、提供しているベンダごとに方式がまちまちであり互換性がない。例えば、A 社の情報付加方式で埋め込んだ情報は A 社が提供する専用のソフトウェア、もしくはそれを内蔵した複合機でしか読み取ることができない。特に電子透かし技術は、他社差別化の観点からアルゴリズムが非公開であることが多いため、あらゆる情報付加方式に対応することは困難である。

まとめると、紙文書の情報漏えい対策として、プリンタや複合機にて印刷や複写の制御を行う製品が数多く提供されているが、これら製品は互換性がなく、特定のプリンタや複合機の機種でしか動作しない。またプリンタや複合機などの仕様が非公開であるため、あとから互換性を持たせるように修正することも困難である。

そのため、さまざまな機種のプリンタや複合機が混在する一般的なオフィス環境では、例えば A 社製の複合機で複写制御できるように紙文書に情報を付与したとしても、B 社製の複合機では制御できずそのまま複写できてしまうなど、ある機種で動作する情報漏えい対策技術が別の機種で動作しない。よって、これら既存の製品では結局紙文書の情報漏えいを防止できないのが現状である。

本発表では、この互換性の問題を解決し、さまざまな機種のプリンタや複合機で動作する、マルチベンダな紙文書漏えい対策システムを提案する。

3. マルチベンダ紙文書漏えい対策システム

マルチベンダ紙文書漏えい対策システムを提案するに当たり、まず前述した従来の対策システムの課題を解決するアプローチを提案する。そして印刷時の漏えい対策方法、複写時の漏えい対策方法の詳細について説明する。

3.1. マルチベンダに向けたアプローチ

従来の対策システムの課題は、印刷ジョブや複合機の仕様が非統一かつ非公開であること、情報付加方式が非統一であることに分類できる。これらそれぞれの課題を解決するアプローチとして以下を提案する。

- **プリンタの仕様が非統一・非公開であることの解決アプローチ**：プリンタ、特に印刷ジョブが非公開である以上、印刷ジョブの種類に依らない何らかの方法を編み出さなければならない。ここで、ビットマップのような画像データであれば、OS が提供する描画機能でどのアプリケーションからでも生成可能であり、かつ、画像データへの情報の付加は非公開の印刷ジョブへの付加より容易であることに注意する。そこで、印刷時に印刷元の電子データを画像データに変換して情報を付加し、その後に実プリンタに画像データを印刷するプログラムを開発すれば、印刷に関するマルチベンダ性を実現できると考えられる（図 1）。

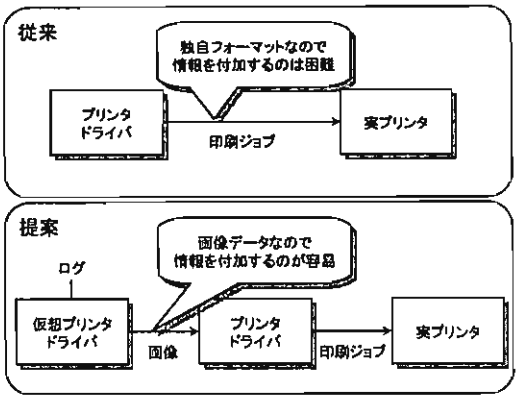

図 1　マルチベンダ印刷のアプローチ

- **複合機の仕様が非統一・非公開であることの解決アプローチ**：残念ながら複合機の仕様は完全に非公開であるため、どの複合機でも搭載しているような共通の要素を活用してマルチベンダを実現するより他ない。一般に、ほとんどの複合機は、紙をスキャンしてデジタル画像データに変換するスキャン機能と、画像データを紙に印刷するプリント機能、かつ、画像データを外部 PC に送信する送信機能を内蔵する。そこで、これら 3 つの機能だけを用いるアプローチを採用する（図 2）。なお、これら 3 機能を内蔵しない、いわゆるアナログ複写機に対しては本アプローチを適用することはできないが、文献[16]によると、平成 19 年の複合機全体の国内出荷実績 2500 億円程度のうちアナログ複写機は 9 億円程度と 0.3%しか占めていない。よって、本アプローチにより複写に関するマルチベンダ性を実現できるといえる。

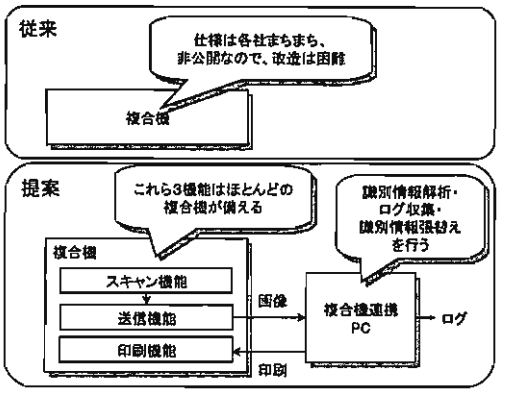

図 2　マルチベンダ複写のアプローチ

- **情報付加方式が非統一であることの解決アプローチ**：紙文書への情報付加方式として電子透かしやバーコードなどがあるが、提供しているベンダごとに方式がまちまちであり互換性がない。電子透かしに関してはまだ標準化された技術が存在しないため、ベンダ非依存の精神から、まずは国内外で標準化されており広く普及している二次元バーコード[15]を用いることにする。

以上のアプローチを踏まえて、以下で印刷・複写それぞれについてシステムの詳細を明確化していく。

3.2. マルチベンダ印刷物漏えい対策システム

プリンタの機種に依存しないマルチベンダ印刷物漏えい対策システムは主に以下の要素からなる（図 3）。

- **仮想プリンタドライバ**：印刷したい電子文書を画像データに変換してバーコードを埋め込み、実プリンタに送信するプリンタドライバ。
- **印刷ログ収集プログラム**：いつ、誰が、どの電子文書を印刷したかなど、印刷に関するログを収集して保管する。
- **識別情報発行プログラム**：印刷に関するログ情報や印刷の機密度に応じて、紙文書一枚一枚にユニークな識別情報を発行する。さらに電子文書の機密度に応じて印刷の禁止を指示する。
- **印刷ジョブ監視プログラム**：印刷スプールを監視して、仮想プリンタドライバを経ないで直接実プリンタに渡る印刷ジョブを強制削除する常駐プログラム。（文献[17]に具体的な実現方法が記載されている。）

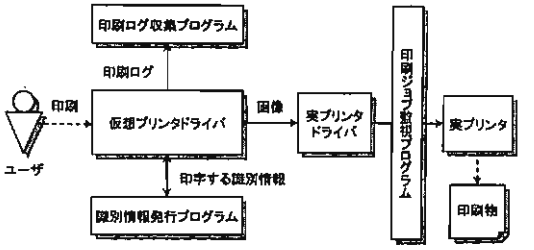

図 3　マルチベンダ印刷物漏えい対策システム

他に、印刷時の本人認証を行う認証装置や、電子文書の印刷・複写可否を判断するポリシーサーバも存在する。これらはユーザの成りすましや印刷･複写制御を行うためのものであり、マルチベンダを実現するに当たっては本質ではない。

上記要素を具備するマルチベンダ印刷物漏えい対策システムは、以下の動作フローをとる。

① **認証**：PC のログイン時や印刷時に IC カードなどで認証を行い、ユーザの成りすましを防止しておく。

② **仮想プリンタドライバ起動**：印刷時にユーザはアプリケーションから仮想プリンタドライバを選択して印刷を実行する。仮想プリンタドライバ以外の印刷は印刷ジョブ監視プログラムにより禁止される。

③ **印刷ログ収集**：仮想プリンタドライバは印刷ログ収集プログラムを起動して、印刷に関するログを収集する。

④ **識別情報発行**：仮想プリンタドライバは識別情報発行プログラムを起動して、識別情報を取得する。印刷禁止の旨を取得した場合は以降の処理を中止する。

⑤ **画像データに変換**：仮想プリンタドライバは、OS の描画機能を用いて印刷対象の電子データを画像データに変換する。

⑥ **バーコード付加**：紙文書の識別情報をバーコードに変換して画像データに埋め込む。

⑦ **印刷**：出力先の実プリンタのプリンタドライバを起動して、バーコードが埋め込まれた画像データを実プリンタに印刷する。なお、実際に紙を出力する実プリンタは、仮想プリンタドライバ側であらかじめ設定しておくか、本ステップ時にダイアログを表示してユーザに選択させる。

上記動作フローの核は、電子文書を画像データに変換する仮想プリンタドライバである。第 4 章で実装の概要を示す。

3.3. マルチベンダ複写物漏えい対策システム

複合機の機種に依存しないマルチベンダ複写物漏えい対策システムは、複合機と、複合機に連結したPC(以下複合機連携PCと呼ぶ)で構成される。前述したように、複合機は以下の機能を備えていなければならない。

- **スキャン機能**：紙をスキャンしてデジタル画像データに変換する機能。
- **プリント機能**：画像データを受信して紙に印刷する機能。
- **送信機能**：画像データを複合機連携PCに送信する機能。

複合機連携PCは以下のプログラムを備える(図4)。

- **識別情報抽出プログラム**：複合機の送信機能を介してスキャン画像データを受信し、受信した画像データを解析して識別情報を抽出する。
- **複写ログ収集プログラム**：上記抽出した識別情報をもとに、いつ、誰が、どの紙文書を複写したかなど、複写に関するログを収集して保管する。
- **識別情報発行プログラム**：複写に関するログ情報や抽出した識別情報に応じて紙文書一枚一枚にユニークな識別情報を発行する。さらに、スキャン画像から抽出した識別情報に基づいて、複写の禁止を指示する。
- **識別情報付与プログラム**：スキャン画像からバーコードを消去し、新たに発行された識別情報をバーコードの形で書き込む。新しいバーコードを書き込んだ後、複合機に画像データを返信して印刷する。

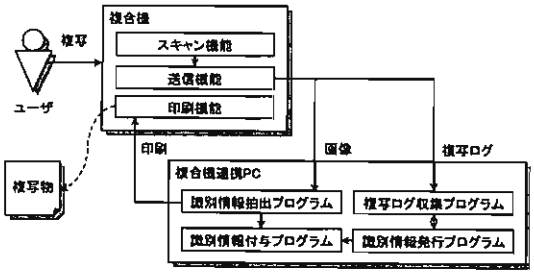

図4　マルチベンダ複写物漏えい対策システム

一般的に複写は複合機の内部でハードウェア的に行われるが、本方式では、複写をスキャンと印刷に分け、間に複合機連携PCで紙文書に付与された識別情報を解析する処理を加えた点が新規である。スキャン、画像送信、印刷はほとんどの複合機が備える機能であるためマルチベンダを実現できる。

なお、本方式を実現するためには、ユーザが複写を指示したときに、通常の複写を行う代わりにスキャン画像を複合機連携PCに送信するように、各ベンダの複合機のユーザインターフェースを修正しなければならない。すなわち、本方式を実現するためには、ユーザインターフェースの仕様について各複合機ベンダに公開してもらう必要がある。しかしこれまで、情報漏えい対策技術を独自に複合機に搭載するためには、前述のように、複合機の仕様を完全に開示してもらう必要があり、現実的でなかった。本方式は、複合機の性能の根幹にかかわらないユーザインターフェースの仕様の開示だけで実現でき、マルチベンダ対策システムをより容易に開発できる点が強みである。

マルチベンダ複写物漏えい対策システムは以下の動作フローをとる。

① **認証**：複写時にICカードなどで認証を行い、ユーザの成りすましを防止しておく。
② **スキャン**：ユーザが紙文書のスキャンを指示したとき、複合機はスキャンを開始して、複合機連携PCへスキャン画像が送信する。
③ **識別情報抽出**：複合機連携PCは、受信したスキャン画像を解析して識別情報を抽出する。
④ **複写ログ収集**：上記抽出した識別情報をもとに、いつ、誰が、どの紙文書を複写したかなど、複写に関するログを収集して保管する。
⑤ **識別情報発行**：複写に関するログ情報や抽出した識別情報に応じて紙文書一枚一枚にユニークな識別情報を発行する。識別情報から複写を禁止すべきと判断した場合には以降の処理を中止する。
⑥ **識別情報付与**：スキャン画像からバーコードを消去し、新たに発行された識別情報をバーコードの形で書き込む。
⑦ **印刷**：複合機に画像データを返信して印刷する。

なお複写制御を行う運用では、情報漏えい防止の観点から、バーコードを検出できなかった場合や不正な識別情報を抽出した場合には複写を禁止すべきである。

上記動作フローの核は、複写をスキャンと印刷に分けた点である。本方式を実際の複合機を用いて実装したので、次章で実装の概要を示す。

4. 実装イメージ

第3章で示した提案方式に基づいて実際に仮想プリンタドライバや複合機連携PCを実装したので、概要を示す。

4.1. マルチベンダ印刷物漏えい対策システムの実装イメージ

マルチベンダを実現できるかを検証するために、認証、印刷制御を行わず、印刷ログだけ取得する簡易版を開発することにした。また、紙文書の識別情報として、印刷ログをそのままバーコードの形で印字することにした。

開発環境を表 1 に示す[18]。

表 1　印刷物漏えい対策システムの開発環境

種別	詳細
PC	PC/AT 互換機
OS	Windows XP Professional SP2
開発ツール	Windows DDK(3790.1830)
プリンタ	Canon LASER SHOT LBP-2810

動作フローは以下の通りである。

① **仮想プリンタドライバ起動**：印刷時にユーザはアプリケーションから仮想プリンタドライバを選択して印刷を実行する（図 5）。

② **印刷ログ収集**：仮想プリンタドライバは印刷ログ（ログインユーザ名、PC の IP アドレス、日時）を収集して、ログを管理する外部 DB に登録する。

③ **画像データに変換**：仮想プリンタドライバは、OS の GDI エンジンを用いて印刷対象の電子データを 300dpi の DIB データに変換する。

④ **バーコード付加**：印刷ログをバーコードに変換して DIB データの右下に埋め込む。

⑤ **印刷**：出力先の実プリンタのプリンタドライバを起動して、バーコードが埋め込まれた DIB データを実プリンタに印刷する。なお、どの実プリンタに出力するかの選択は、仮想プリンタドライバのプロパティとしてあらかじめ設定しておく。

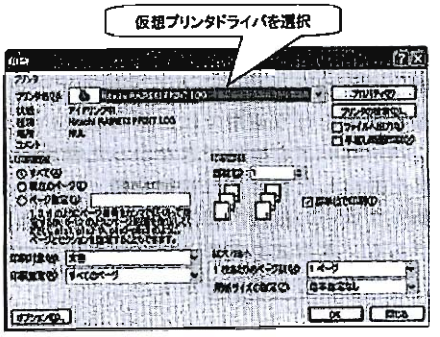

図 5　仮想プリンタの起動画面

印刷物のイメージを図 6 に示す。

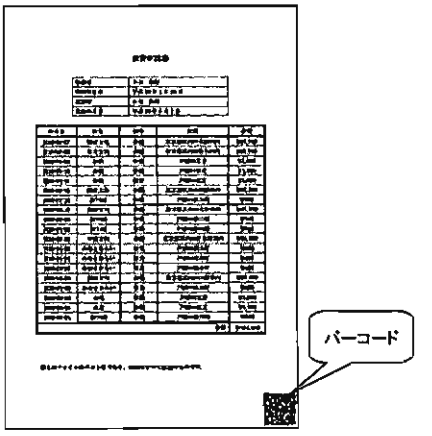

図 6　印刷物のイメージ

4.2. マルチベンダ複写物漏えい対策システムの実装イメージ

マルチベンダを実現できるかを検証するために、複写制御を行わず、複写ログだけ取得する簡易版を開発することにした。また、紙文書の識別情報として複写ログをそのままバーコードの形で印字することにした。

開発環境を表 2 に示す[19]。

表 2　複写物漏えい対策システムの開発環境

種別	詳細
PC	PC/AT 互換機
OS	Windows XP Professional SP2
開発ツール	Microsoft Visual Studio 2005
開発言語	C#

使用した複合機のスペックを表 3 に示す[20]。実装に当たっては株式会社リコーの協力を得た。まだ表 3 の一機種でしか実装できていないが、今後他の複合機ベンダにもユーザインターフェースの開示を依頼し、対応機種を増やす予定である。

表 3　複合機のスペック

種別	詳細
本体	RICOH imagio MPC4500SP
オプション	imagio マルチエミュレーションカードタイプ 5
	imagio 2000 枚フィニッシャー SR-3020
	imagio USB ホストタイプ 1
	imagio 個人認証システム（含む IC カードリーダー）
	imagio Web アクセスカード Type1

動作フローは以下の通りである。

① **認証**：ユーザは IC カードで認証をしてから紙文書のスキャンを指示する。

② **スキャン**：複合機はスキャンを開始して、複合機連携 PC 上のあらかじめ設定したパスへスキャン画像を送信する。白黒二値でスキャンしたときは TIFF 画像を、それ以外のときは JPEG 画像を送信する。解像度はいずれも 300dpi である。

③ **識別情報抽出**：複合機連携 PC は受信したスキャン画像を解析してバーコードを抽出する。

④ **複写ログ収集**：上記抽出した識別情報をもとに、いつ、どの紙文書を複写したかといった複写ログを収集して、ログを管理する外部 DB に登録する。

⑤ **識別情報発行**：複写ログ情報をもとに新しい識別情報を発行する。

⑥ **識別情報付与**：スキャン画像からバーコードを消去し、新たに発行された識別情報をバーコードの形で書き込む。

⑦ **印刷**：複合機に画像データを返信して印刷する。

複写物のイメージを図 7 に示す。

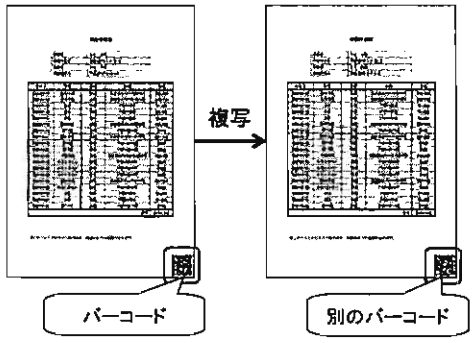

図 7　複写物のイメージ

開発したマルチベンダ漏えい対策システムでは、印刷物、複写物には一枚一枚異なるバーコードが印字されるため、バーコードを読み取って印刷・複写ログを保管する外部 DB を検索することで、紙文書がどのように印刷・複写されてきたか追跡することができる。追跡するプログラムも開発したのでその利用イメージを図 8 に示す。起点となる紙文書の複写元と複写先を検索してログを表示した例である。

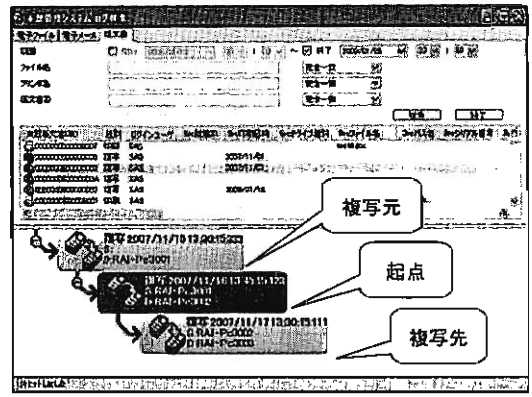

図 8　複写物の検索イメージ

今回は 1 機種のみを対象として実装したが、今後他の複合機ベンダにもユーザインターフェースの開示を依頼し、今後さまざまな機種の複合機についても実装を重ね、マルチベンダ性を検証していく予定である。

4.3. 実装システムの課題と解決案

提案システムの実装により新たに判明した課題とその解決案を以下にまとめる。

- **印刷時の処理速度の低下**：提案方式では電子データを画像に変換してから実プリンタに送信するため、画像変換によるメモリ使用量の増加や、画像データ送信によるネットワーク負荷の増大が顕著となる。例えば提案方式で文書ファイル 1 ページを A4 サイズで印刷した場合、もともとは高々数百 K バイトのデータだったのが、画像化により、白黒二値で 1M バイト、グレースケールで 8M バイト、フルカラーで 24M バイトと大幅にデータ量が増大する（300dpi の場合）。この問題に関しては、画像データの代わりに Postscript といったベクトルデータを用いる方法が考えられる。アプリケーションからベクトルデータを出力する方法、ベクトルデータを実プリンタに印刷する方法などについて今後検討していく。
- **複写時の処理速度の低下**：提案方式では、本来複合機の内部でハードウェア的に行われていた複写処理をスキャンと印刷に分割し、画像データを複合機連携 PC 間で送受信したり、画像データから識別情報を検出したり差し替えたりするため、その分処理速度が低下する。複合機連携 PC 内の画像処理の高速化を進めることで対処する。
- **バーコードに対する攻撃**：提案方式では国内外で標準化されており広く普及している二次元バーコード[15]を用いた。しかしバーコードは切り取りや改ざんといった攻撃が容易であり、その場合

紙文書の識別が失敗し、情報漏えいを防止できなくなってしまう。解決策として、バーコードの代わりに、情報の所在がわかりにくい電子透かし技術を用いる方法があげられる。標準的な電子透かし技術はまだ存在しないが、識別条件付与・検知に対する技術要件を明確化した上で最適な電子透かし方式を今後検討していく。

5. まとめ

紙媒体を経由した情報漏えいは漏えい全体の43.8%にも上っており、見過ごせない問題である。紙文書の情報漏えい対策としてすでに数多くの製品が提供されているが、これらは互換性について考慮されていないため、さまざまな機種のプリンタや複合機が混在する一般的なオフィス環境では機能せず、結局紙文書の情報漏えいを防止できていないのが現状である。

そこで本発表では、プリンタや複合機の機種に依らずに印刷・複写の履歴管理を行うことができるマルチベンダ紙文書漏えい対策システムの一提案を行った。提案方式を実際のプリンタ・複合機で実装し、検証した。今後さまざまな機種のプリンタ・複合機についても実装を重ね、マルチベンダ性を検証していく予定である。

6. 謝辞

本発表は平成19年度総務省の委託研究「情報の来歴管理などの高度化・容易化に関する研究開発」の研究成果の一部を含む。

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：「2006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://cweb.canon.jp/Product/appli/accountant/index.html

[4] http://www.ricoh.co.jp/IPSiO/related_goods/operationsvr/

[5] http://www.fujixerox.co.jp/product/aw_accounting/

[6] 海老澤竜、藤井康広、高橋由泰、手塚悟：「紙文書に対するセキュリティ技術の考察」、情報処理学会研究報告(CSEC) Vol.2006 No.81(20060720) pp.305-311 (2006)

[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 (2003)

[10] Electronic Frontier Foundation: "DocuColor Tracking Dot Decoding Guide"

[11] http://www.oki.com/jp/FSC/valcode/

[12] http://www.hitachi-ins.com/product/ekami/index.html

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

[14] BMLinkS: http://www.jbmia.or.jp/bmlinks/

[15] QR コード：JIS X 0510, ISO/IEC18004（QR コードは株式会社デンソーウェーブの登録商標です。）

[16] JBMIA: http://www.jbmia.or.jp/about/copier43.htm

[17] 土田健一、佐藤由香里：「印刷制御方法およびプログラム」、特開 2007-293673