

## 情報の価値に応じた印刷制御機能の開発

甲斐 賢<sup>†</sup> 笈川 光浩<sup>†</sup> 伊川 宏美<sup>†</sup>  
今一 修<sup>†</sup> 森本 康嗣<sup>†</sup> 土田 健一<sup>††</sup>  
荒井 正人<sup>†</sup> 洲崎 誠一<sup>†</sup>

ここ十年近くの企業の情報セキュリティ対策は対症療法の繰り返しであり、対策を行うほどセキュリティ運用管理コストが増していた。特に一般的なオフィスで取り扱う電子ファイルや紙文書は、コストをかけてまで守る価値のある情報と、必ずしもそうではない情報とが混在しており、価値に応じたコントロールや監査は従業員任せとなることが多かった。そこで筆者らは、情報の活用と保護の両立を目的に、情報の価値を分類・整理した上でコントロール・監査を行うための「情報資産管理基盤システム」を検討している。本稿では、本システムの一部として、情報の価値に応じた印刷制御機能をプロトタイプ開発し、有効性を確認したので報告する。

### Development of Print Control Function According to Information Assets Value

Satoshi Kai<sup>†</sup> Mitsuhiro Oikawa<sup>†</sup> Hiromi Igawa<sup>†</sup>  
Osamu Imaichi<sup>†</sup> Yasutsugu Morimoto<sup>†</sup>  
Kenichi Tsuchida<sup>††</sup> Masato Arai<sup>†</sup> and Seiichi Susaki<sup>†</sup>

The information security measures of the enterprise are the repetitions of overcoats for these ten years, and the security operation management cost has increased by security measures. Especially, the electronic file and the paper document handled in a general office are mixed into both information worth to protect with the cost and information that is not necessarily worth to do. So the employee must think the value of the information and they must control and audit the information. Then, the authors are discussing "Information Assets Management Basic System" that controls and audits the information after the value of the information is classified and arranged in order that the utilization and the protection of information will coexist. So this paper reports the print control function mounted as one function (the control and the audit), and effectiveness of the function was verified.

### 1. はじめに

企業における情報セキュリティ対策は、ここ十年近くを見渡すと対症療法の歴史であったと考えられる。初期には、インターネットからの不正侵入による Web サイト改ざんや電子メールで感染するコンピュータウイルスの脅威が増すにつれ、外部からの不正侵入対策が普及してきた。次に、個人情報保護法の施行に伴い、顧客名簿といった個人情報の流出を防ぐ対策が普及してきた。近年は特に、金融商品取引法や PCI DSS (Payment Card Industry Data Security Standard) といったビジネスを推進する上で準拠が求められるコンプライアンスのための対策が普及しつつある。このため、企業に勤める大多数を占める従業員にとって、情報セキュリティ対策として本来の業務以外にやるべきことが年々増えているのが実状であると考えられる。

一方、情報大爆発の時代と言われるように、従業員にとって業務で取り扱う情報は急速に増えていくと言われる。それらの情報に対するセキュリティ対策レベルを維持し続けるのは、ここ十年近くの対症療法的なアプローチでは限界にきていると考えられる。さらに本来、利益を生むはずの情報なのに、セキュリティ対策が足かせとなるのは経営者にとって望む姿ではないと考えられる。

よって、今後は情報の活用と保護とを両立することがますます重要となると言える。そこで筆者らは、情報セキュリティ対策の新たなアプローチとして「情報資産管理基盤システム」という構想を検討中である。本稿では以下、2章で動機を、3章で情報資産管理基盤システムの概要を、4章で関連研究を述べ、本研究の位置付けを述べる。さらに本システムの一部として実装した、情報の価値に応じた印刷制御機能の開発を5章で、その評価を6章で述べる。

### 2. 動機

企業に勤める大多数を占める従業員は、オフィスで就業時間の大半を過ごし、オフィスには様々な情報（紙としての書類や記憶媒体内の電子ファイル）が蓄積されている。文献[1]によると、書類を積み重ねた高さは、社員1人当たり4.5~6mとも、多い場合には10mを超えとも言われている。近年オフィスはPC環境が整いペーパーレス化も叫ばれているため、電子ファイルも含めるとそれ以上の量があると考えられる。

これらの情報は分類すると、文書そのものが重要かつ企業の存続に多大な影響を与える「Vital Documents」、プライバシー等の観点から個人情報で機密管理が求められる「Private Documents」、経営戦略上、内容が漏洩することで企業に多大な影響を与える

<sup>†</sup> 株式会社 日立製作所  
Hitachi, Ltd.

<sup>††</sup> 日立アイ・エヌ・エス・ソフトウェア株式会社  
Hitachi INS Software, Ltd.

と予想される「Confidential Documents」、上記以外で業務遂行のために活用する「Reference Documents」があるとされる[1]。また同文献によると、それぞれの割合は、一つの企業例としてVitalが9.5%、Privateが12.2%、Confidentialが51.8%、Referenceが26.5%と言われる。このように、オフィスでは多様な情報が混在していると言える。

このような混在した情報に対して、現在の多くのセキュリティ対策は、一律にコントロールや監査を適用する傾向が強いと考えられる。例えば持ち出し時の暗号化を例にとると、その情報に関係なく、一律に暗号化しなければならないことが定められることが多い。また、社外に送信する電子メールにファイル添付を行う際にも、その情報に関係なく、一律に上長にCC送信することが定められることが多い。このような一律にコントロールや監査を適用すると、暗号化や上長チェックしなくても良いはずの情報にまでセキュリティ対策が適用されてしまう過剰な側面や、逆に暗号化や上長チェックさえ形式的に行えばどんな情報でも持ち出せてしまう不足の側面が出てくる。つまり、混在した情報に対して一律にコントロールや監査を適用することは、セキュリティの過不足を生じさせると言える。

そのため、情報はその「価値」によって守り方も変えることが望ましい。つまり、コントロールや監査を行う前に、その情報の価値をよく見た上で適切なコントロールや監査を行う方が望ましい。このような情報の価値に応じたコントロールや監査を行う基盤を整備していくことは、情報の活用と保護の両立にも有効であると考えられる。

### 3. 情報資産管理基盤システムの概要

#### 3.1 基本的な考え方

情報資産管理基盤システムとは、2章で述べた、情報の価値に応じたコントロールや監査をITで行う基盤のことである。図1に示すように、従来のITセキュリティ対策の多くは、コントロールや監査の範囲を限定してIT化する傾向が強かったと考えられる。提案する情報資産管理基盤システムは、

- (1) 情報を分類・整理して、情報の価値を明確化する
- (2) 情報の価値に従って、コントロールや監査を適用する

のいずれもIT化することを目的とする。

このような情報資産管理基盤システムを整備することは、その効果としてセキュリティ向上に留まらない。情報大爆発という背景の中で、業務に必要な情報も分類・整理していくことで、業務効率にも向上できると期待される。よって、情報の活用と保護の両立に向けて、情報資産管理基盤システムの重要性はますます増すと考えられる。

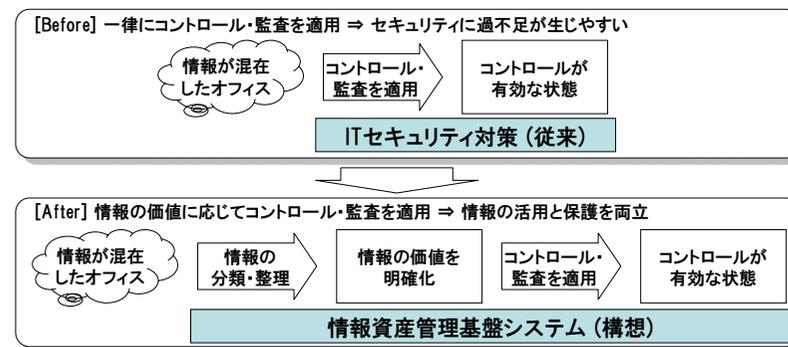


図1 情報資産管理基盤システムの考え方のイメージ

#### 3.2 情報の分類・整理のアプローチ

情報資産管理基盤システムを実現するには、情報の分類・整理が鍵となる。とくに業務で生成しオフィスに蓄積する多様な情報を、いかに正確かつ効率良く分類・整理するかが重要となる。そこで、業務で情報を生成してから、情報の価値に応じたコントロール・監査を行うまでの間、どのタイミングで情報を分類・整理するかに着目して場合分けした。その結果、以下に述べる(1)~(3)に場合分けできた。

##### (1) 情報を生成する前から分類・整理する

業務で情報を生成する時には、あらかじめ定められた特殊形式に情報を格納する。特殊形式に格納された情報の価値は、情報そのものではなく、特殊形式の方を見て判定する。このような判定後に、情報の価値に応じたコントロールや監査を行う。

例えば、帳票形式のファイルに業務で情報を入力する場合や、所定のテンプレートファイルを使って業務で計画書や報告書等を生成する場合、所定のフォルダ以下に置くファイルを何らかの情報と見なす場合、ログとして所定形式に出力する情報の場合などが該当する。

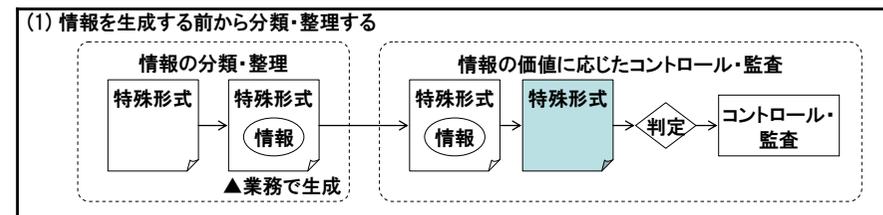


図2 情報の分類・整理のアプローチ(1)

##### (2) 情報を生成してから分類・整理する

業務で情報を生成する時には、とくに定められた特殊形式に情報を格納せずに、任

意形式に情報を格納する。その任意形式に格納された情報に対して、業務における承認等のプロセスを通じて、メタデータを付与する。任意形式に格納された情報の価値は、情報そのものではなく、メタデータの方を見て判定する。このような判定後に、情報の価値に応じたコントロールや監査を行う。

例えば、文書管理サーバへの登録やワークフロー業務によって任意形式の情報にメタデータ（取り扱いレベル、承認有無など）を付与する場合や、ファイルの属性としてメタデータを付与する場合、構成管理ツールによってソースコードにメタデータ（チェックアウト状態）を付与する場合などが該当する。

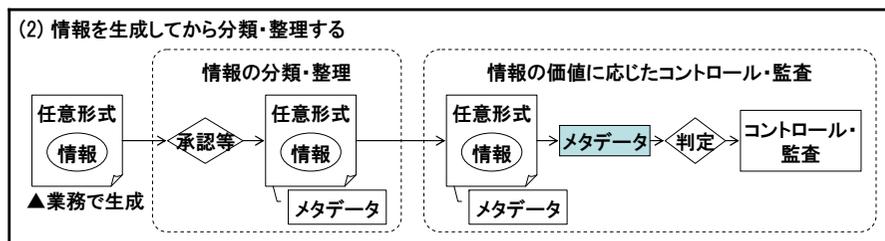


図 3 情報の分類・整理のアプローチ(2)

### (3) コントロール・監査と一体化して情報を分類・整理する

業務で情報を生成した後も、とくに何も行わない。一方で、コントロール・監査を行う直前に、情報が格納された任意形式から、情報だけを取り出し、どのような情報であるかを判定条件により判定する。このような判定後に、情報の価値に応じたコントロールや監査を行う。

例えば、電子メールサーバのフィルタリング機能によってその本文や添付ファイルの情報を点検する場合や、判定条件として守るべきファイルを登録しておき前記ファイルとの類似度を測ることで情報の価値を判定する場合[2]などが該当する。

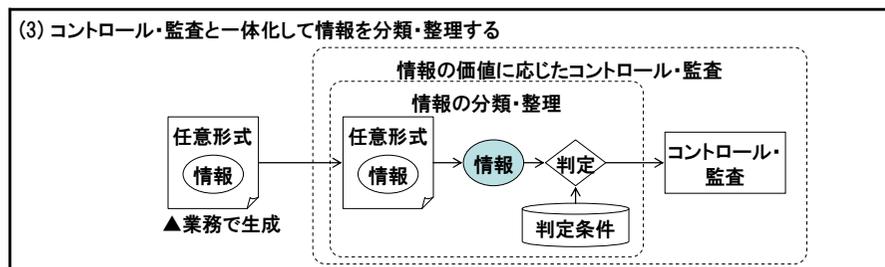


図 4 情報の分類・整理のアプローチ(3)

### 3.3 印刷制御への応用

企業にとってセキュリティリスクの一つは情報漏洩であると考えられる。文献[3]によると紙媒体による漏洩経路が半数近くを占めている。また、電子ファイルの間はアクセス制御やログ取得などのコントロール・監査を適用しやすいが、一旦印刷されてしまうと、その後のコントロール・監査は適用しにくい。そこで情報漏洩リスクを下げるには印刷時のセキュリティが重要と考え、以下では、情報の価値に応じたコントロール・監査として「印刷制御」を取り上げる。

前節で述べた情報の分類・整理のアプローチを印刷制御に応用すると、それぞれ次に示す通りとなる。

#### (1) 情報を生成する前から分類・整理する

あらかじめ印刷イメージと同じ特殊形式で情報を生成する場合が考えられる。例えば、帳票入力が典型的である。印刷制御では、どのような帳票を印刷しているかを判定することで、情報の価値を判定する。

#### (2) 情報を生成してから分類・整理する

あらかじめ電子ファイルに「Confidential」などの文字列をヘッダやフッタ領域やファイル属性に記入しておき、印刷時には、紙文書にもその文字列をメタデータとして印字されるようにする場合が考えられる。印刷制御では、どのようなメタデータを印刷しているかを判定することで、情報の価値を判定する。

#### (3) コントロール・監査と一体化して情報を分類・整理する

印刷時に情報に関わらずイメージ化しておき、そのイメージファイルを解析してコントロールや監査を行う場合が考えられる。例えば、OCR (Optical Character Reader) による文字認識が代表的である。印刷制御では、イメージファイルを解析することで、情報の価値を判定する。

こうした情報の分類・整理のアプローチのうち、(1)(2)は良く知られていると考えられる。(3)はOCRを使うとなると、形が似た文字同士の認識エラーや小さすぎる文字の認識エラーなど、エラー率を無視できないと考えられる。上記(1)~(3)は全て情報資産管理基盤システムの実現に必要な技術であり、本研究では(3)に注力することとした。

## 4. 関連研究

情報資産管理基盤システムを実現する上で鍵となる、情報の分類・整理のアプローチについては、下記に示す研究が行われている。

SNIA (Storage Networking Industry Association) [4] では2008年あたりからチュートリアルで、情報の分類 (Classification) についての議論が活発化しており、Classification技術として次のように整理している。

- ・ ファイル属性に基づく Classification (ファイル名, ファイルタイプ, 所有者,

位置、作成日など)

- コンテンツに基づく Classification (キーワードなど)

さらにコンテンツに基づく Classification では、キーワードの文脈における意味を利用することが述べられている。

SNIA が述べる Classification 技術は、情報が生成された後のタイミングでの情報の分類・整理を対象としていると考えられる。本研究では、情報が生成される前から分類・整理を行うアプローチも挙げているため、SNIA よりも幅広く情報の分類・整理のアプローチを検討している。

また、情報の分類・整理のタイミングとして、コントロールや監査と一体化して行う方法は、近年DLP(Data Loss Prevention) と呼ばれるセキュリティ製品の多くが採用している。DLP製品の機能評価レポート[5]では、電子メールの送信において、DLP製品による情報のチェックを回避しようとする様々な妨害行為に対して、妨害されたとしてもDLP製品が情報を正しくチェックできるかどうかが述べられている。

前記レポート[5]は、電子メールの送信に限定して評価が行われていると言える。一方、本研究では、印刷機能を対象にした点が異なる。電子メール送信の解析はSMTP(Simple Mail Transfer Protocol) という公開仕様をもとに行うことができるが、印刷制御は比較的的非公開な仕様であることが多い。そのため、本研究では情報の価値に応じた印刷制御機能を実装し有効性を確認した点に新規性と有用性があると言える。

## 5. 情報の価値に応じた印刷制御機能の開発

情報の価値に応じた印刷制御機能の開発に向け、コントロール・監査と一体化して情報を分類・整理するアプローチを、印刷制御でどのように実現するかが課題である。

以下、5.1節と5.2節で実現上の課題と解決方針を述べ、5.3節で実装結果を述べる。

### 5.1 情報の価値の判定方法

実現上の一つ目の課題は、情報の価値の判定方法である。文献[6]によれば、情報とは「言葉」「数字」「絵」の3種類で表されると言われる。本研究では、業務で作成する情報には「言葉」が多いと考え、情報の価値を「言葉」で判定する方法を検討した。

言葉で情報の価値を判定する方法には、一例として、表 1に示すものが考えられる。これらの方式はそれぞれメリット・デメリットがあり、どれかを一律に適用することは難しい。さらに表 1に示す以外の方法も今後は考えられる。そこで、情報の価値の判定方法は、一つに決めるのではなく、後からも容易に変更可能なカセット方式が良いと考えた。

### 5.2 印刷制御方法

実現上の二つ目の課題は、印刷時における「言葉」の取得方法である。

従来技術である OCR による文字認識も、言葉を取得するための一つの方法である。

表 1 情報の価値を言葉で判定する方法の一例

方式名	説明および特徴
キーワードマッチング方式	所定のキーワードが含まれるかどうかで、価値を判定する。分かりやすい反面、キーワードの選定が難しい。
正規表現マッチング方式	所定の正規表現に合致する文字列が含まれるかどうかで、価値を判定する。言葉よりも数字の方がマッチングさせやすい。
フィンガープリント照合方式	1 文章など意味のある区切りで特徴値を算出し、所定の特徴値が出てくるかどうかで、価値を判定する。フィンガープリントの作り次第で、精度が大きく左右される。
辞書照合方式	姓名辞書や企業名辞書などを用意し、それらの辞書にある文字列が含まれるかどうかで、価値を判定する。辞書が巨大になるほど、判定に要する時間も長くなる。

しかし、OCR では前述したように印刷イメージから文字認識する際に、形が似た文字同士の認識エラーや、小さすぎる文字の認識エラーなどを無くすることは難しい。

一方で、電子ファイルに近い箇所、印刷時における言葉を取得する方法も考えられる。しかし、この方法では、電子ファイル中の一部だけを印刷する場合や、電子ファイルにはなくても印刷時にアプリケーションが独自に追加する文字列までを取得することが困難である。

そこで、OCR による取得方法と、電子ファイルに近い箇所での取得方法との中間に位置するプリンタドライバで言葉を取得する方法を選択した。

ただし、プリンタドライバは、業務で既にインストール済みであることが多く、アドオンで実現できることが望ましい。そこで、印刷制御は文献[7]を参考に、アプリケーションから仮想プリンタドライバを呼び出し、その仮想プリンタドライバから実プリンタドライバを呼び出す方式を基礎にしつつ開発した。本方式を採用することにより、アプリケーションから印刷する際に仮想プリンタを選択するというように、通常の印刷操作性を損なわずに済む。

### 5.3 実装結果

多くのオフィスでは印刷時にWindows XPが使用されていると考え[a]、Windows XP上でプロトタイプを開発した。本プロトタイプのシステム構成を図 5に示す。

#### (1) 仮想プリンタドライバ

図 5中に示す仮想プリンタドライバは、アプリケーションからの印刷要求から言葉としてテキスト部分を抽出し、後述する自然言語処理サービスにテキスト部分を渡す。その後、テキスト部分が判定条件に該当するかどうかの判定結果を受け、もし印刷が許可されるならビットマップファイルを出力し、実プリンタドライバで印刷する。もし印刷が禁止されるなら、アプリケーションに印刷エラーを返す。

a) Windows XP は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

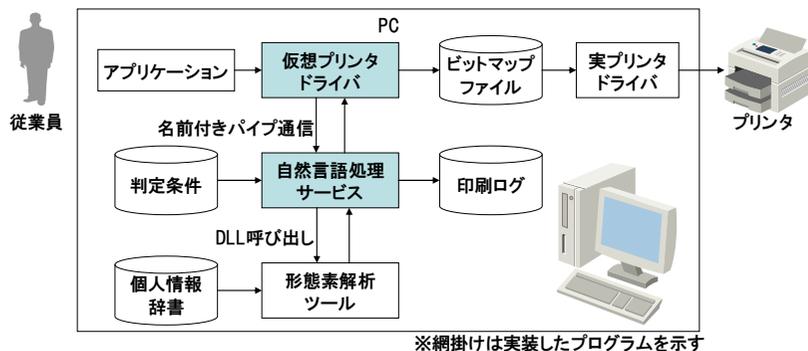


図 5 印刷制御機能のシステム構成

仮想プリンタドライバにおけるテキスト部分の抽出は、印刷のレンダリング[8]時に OEMTextOut関数を DDI (Device Driver Interface) フッキングすることで実現した。本フッキングにより、Unicode文字のテキストを取得できることを確認した。

## (2) 自然言語処理サービス

自然言語処理サービスは、渡されたテキスト部分が判定条件に合致するかどうかを判定するための常駐プログラムである。5.1節で述べたように、情報の価値の判定処理をカセットにするために、本サービスは、仮想プリンタドライバとのインターフェースの役割を持つ。

本プロトタイプでは、判定対象とする情報として「個人情報」を選択した。個人情報は、個人の姓や名が含まれると考えられ、姓に限ると上位 7,000 位までで全人口の 96.27%を占めることが知られている[9]。そのため、表 1 で述べた情報の価値を判定する方法のうち、辞書照合方式が適用できると考えた。

辞書については、本プロトタイプでは、形態素解析ツールを利用することとした。形態素解析ツールは、個人名などの固有名詞をはじめ多くの辞書を所有することが多い。また形態素解析ツールは、自然言語で書かれた文章を入力とし、その文章を品詞に分割した結果を出力とする機能を持つ。ここでは「茶釜」[10]として知られる形態素解析ツールを利用した。なお茶釜の品詞辞書を調べたところ、個人情報辞書に使える固有名詞として、32,193 単語が収録されていることを確認した。

## (3) 判定条件

自然言語処理サービスにより、印刷のテキスト部分に個人情報に該当する固有名詞がいくつ含まれているかを知ることができる。そこで、しきい値を設けることで、所定の個数以上の固有名詞が含まれている場合に、個人情報と判定することとした。プロトタイプでは、1 ページ当たり 20 個の個人情報に該当する固有名詞が含まれることをしきい値とした。

## (4) 印刷ログ

印刷ログには、仮想プリンタドライバで抽出したテキスト情報をすべて残すと共に、個人情報であるかどうかの警告レベルも記録することとした。

## 6. 評価

### 6.1 機能評価

印刷元の電子ファイルとして「名簿ファイル（個人情報に該当、表計算ファイルとして作成）」と「報告書ファイル（個人情報に非該当、ワープロファイルとして作成）」の2種類を用意して、プロトタイプによる印刷操作を試みた。その結果、印刷ログにはそれぞれのファイルのテキスト情報が記録されていることを確認した。さらに、名簿ファイルの印刷は禁止され、報告書ファイルの印刷は許可されることを確認し、印刷ログにもそれぞれの警告レベルが記録されていることを確認した。

また、名簿ファイルとして、手元にあるいくつかの「名簿ファイル」の印刷を試したところ、名簿の切れ端、つまりあるページ内に収まりきれずに次ページの先頭に印刷される場合には、個人情報と判定されないことを確認した。これは、0節(3)で述べた、1 ページ当たり 20 個未満の個人情報しか含まれないためであった。

### 6.2 性能評価

開発プロトタイプにおいて、情報の価値に応じた印刷制御を行う中心的な役割は、次に示す2つの処理が担う。

- ・ 仮想プリンタドライバでのテキスト抽出処理
- ・ 自然言語処理サービスにおける個人情報判定処理

そこで、図 6 に示すように、ビットマップ出力だけを行うプリンタドライバAと、0 節で述べたプリンタドライバBとを用意して、両者の印刷時間の差分を求めた。

測定環境を表 2 に示す。印刷元ファイルとしてページ数が「1」「5」「10」のそれぞれで試したところ、図 7 に示すようページ数に比例して、オーバーヘッドが大きくなった。一方で、1 ページ当たりの印刷時間はページ数による違いは小さいことを確認した。よって、平均すると1 ページ当たり 0.124 秒であることが判明した。

表 2 測定環境

項目	スペック
CPU	Intel Celeronプロセッサ[b] 2.0GHz
Memory	1GB
HDD	80GB (うち 20GB を C ドライブとして使用)
OS	Windows XP Professional SP3
印刷元ファイル	平均して1 ページ当たり 1,654 文字

b) Intel および Celeron は、Intel Corporation の登録商標です。

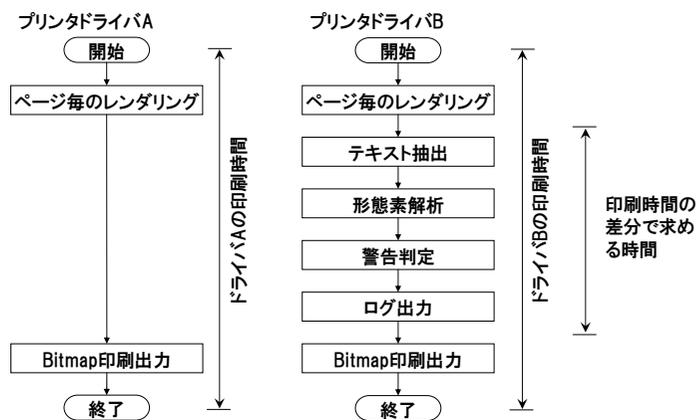


図 6 測定した時間と、求める性能評価の時間の関係

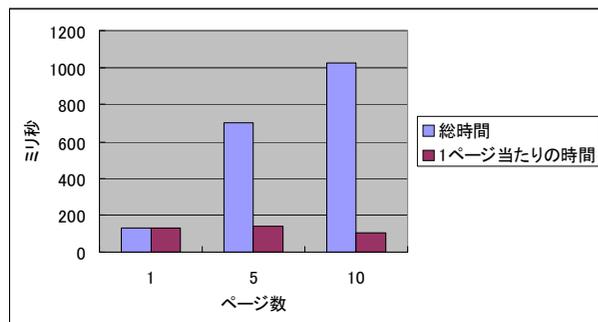


図 7 印刷制御処理のオーバーヘッド

### 6.3 考察

機能評価の結果、個人情報が多く含まれる情報については、個人情報と判定でき、1 ページ内に多く含まれない場合には、個人情報であっても個人情報と判定できないことを確認した。個人情報の場合には、数件の漏洩よりも大量の漏洩の方が企業に与える影響（顧客離れ[11]など）は大きいと考えられる。そのため、1 ページ内に多く含まれない場合には漏洩リスクを許容する運用とすることで、実適用可能と考える。

また、性能評価の結果、印刷制御のオーバーヘッドが約 0.124 秒であることを確認した。ここで、一般オフィスに多く普及していると思われる、複合機（100 万円以下）とプリンタ（20 万円以下）の印刷速度を調べたところ、平均して 1 分当たり 22.8 枚

の印刷速度であった。つまり 1 ページを印刷するには平均して 2.63 秒を要する。このため、プロトタイプを業務で使うプリンタに適用すると約 4.7%の性能低下となる。ところで文献[12]によると、IT予算のうちセキュリティ予算の割合は 3~7%が妥当と言われていることから、処理のオーバーヘッドも許容できると考えられる。

## 7. おわりに

ここ十数近くにわたる企業の情報セキュリティ対策は対症療法的だったという考えのもと、オフィスにおける情報の活用と保護の両立を目的とした、情報資産管理基盤システムの構想を紹介した。さらに、情報資産管理基盤システムを実現する上で鍵となる、情報の分類・整理のアプローチを場合分け、印刷制御への応用を試みた。その結果、情報の価値に応じた印刷制御機能をプロトタイプ開発し、個人情報という漏洩リスクから守る上で、その有効性を検証した。

今後の課題は、カセットな情報の価値判定方法を生かした、個人情報以外の業務情報を正確に判定する方式の開発である。

## 参考文献

- 1) コクヨ S&T(株)セキュリティ推進室, 池田宏: “セキュリティ時代の文書管理”, 日経 BP (2006)
- 2) Sergey Brin: “Copy Detection Mechanisms for Digital Documents”, In Proceedings of the ACM SIGMOD Annual Conference, pp398-409, 1995
- 3) NPO 日本ネットワークセキュリティ協会: “2007 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”, URL= <http://www.jnsa.org/result/2007/pol/incident/index.html>
- 4) Storage Networking Industry Association, URL= <http://www.snia.org/home>
- 5) Websense: “Information Leak Prevention Accuracy and Security Tests”, URL= [http://www.websense.com/docs/whitepapers/wp0106-0506\\_perceptlabs.pdf](http://www.websense.com/docs/whitepapers/wp0106-0506_perceptlabs.pdf)
- 6) リチャード・S・ワーマン: “それは情報ではない—無情報爆発時代を生き抜くためのコミュニケーション・デザイナー”, インプレスコミュニケーションズ (2001)
- 7) 藤井康弘, 海老澤竜, 本多義則, 洲崎誠一: “マルチベンダ紙文書漏えい対策システムの一提案”, 電子情報通信学会技術研究報告. ISEC, 情報セキュリティ, 108(161) pp.51-58 20080717
- 8) Microsoft: “Windows Driver Kit: Print Devices, Rendering a Print Job”, URL=<http://msdn.microsoft.com/en-us/library/ms801266.aspx>
- 9) 日本の苗字 7000 傑: URL= <http://www.myj7000.jp-biz.net/>
- 10) 茶釜, URL=<http://chasen-legacy.sourceforge.jp/>
- 11) ITmedia: “情報漏えいの対応費用は 1 件 200 ドル超に”, URL=<http://www.itmedia.co.jp/enterprise/articles/0902/03/news029.html>
- 12) ITPro: “「セキュリティ予算は、全 IT 予算の 3~7%が妥当」, 米 Gartner のセキュリティ担当リサーチャー”, URL=<http://itpro.nikkeibp.co.jp/article/Interview/20071203/288555/>