ポリシーベース・ドキュメントセキュリティシステムの開発

Development of Policy-based Document Security System

金井　洋一*　　斉藤　敦久*
Yoichi KANAI　　Atsuhisa SAITOH

要　　旨

組織のセキュリティポリシーに従って紙文書と電子文書のセキュリティを確保するシステムを開発した．開発したシステムでは電子文書管理サーバとドキュメントビューアが電子文書のアクセス制御をあらかじめ設定された組織のセキュリティポリシーに従って行い，ドキュメントビューアから機密文書を印刷する際にはポリシーに従ってセキュリティ処理を行うことで，印刷された紙文書を印刷者本人にポリシーに従って適切に扱わせるようにした．加えて，印刷された紙文書をデジタル複合機で複写する際にもポリシーに従ってその処理をコントロールするようにした．開発したシステムにより，一般オフィスにおいて紙文書と電子文書のセキュリティを十分確保できることを示した．

ABSTRACT

A new security system that handles paper and digital documents based on organizational security policy is developed. In the developed system, electronic document management servers and document viewers control accesses to documents based on organizational security policy. By applying security-printing functions on printing secret documents from document viewers, it is succeeded in making the printed-user to comply with the policy. Additionally, treatment of the printed paper documents on digital copier is also controlled based on the policy. It is concluded that the developed system can keep security of paper and digital documents sufficiently in general offices.

* 研究開発本部　オフィスシステム研究所
Office System R&D Center, Research and Development Group

1. 背景と目的

オフィスでの業務が電子化されるにつれ，電子的な機密文書の管理についてその重要性が増大してきている．オフィスの業務が高度に情報化される前は，機密文書の原本は紙文書であり，その紙文書原本をオフィスの鍵のかかるキャビネットで保管するなどして機密管理を行っていた．そのようにして管理された機密文書はキャビネットという物理的な保管庫によるアクセス制御がかけられ，機密文書を閲覧したり複写したりする場合には特別な許可が必要であったり，管理台帳に閲覧履歴の記録をするなどして不要なアクセスがないようにコントロールすることが可能であった．

しかし，機密文書が基本的に電子的に作成・共有されるようになった今日，電子文書管理システムやデータベース，ファイルサーバなどを用いてネットワーク上の共有サーバに機密文書を保管し，その機密文書へのアクセスを制御するようなことが一般的に行われている．その一方で，その共有サーバに保管された機密文書に対してアクセス権のあるユーザがその機密文書ファイルを共有サーバからダウンロードし，そのダウンロードしたファイルを本来アクセス権のない利用者に不用意に配布するようなことが行われるケースが横行し始め，更には機密文書を印刷したものを会議の参加者に不用意に配布するなど，機密文書の紙としてのコピーが大量に出回る事態を引き起こしている．この事態を避けるために印刷をできなくした電子ファイル，例えば印刷禁止の設定をしたPDFファイル等を共有・配布するようなことが一部で行われ始めている．

しかし現実には印刷できないファイルというのは使い勝手が悪く，例えば製品の設計書のような機密文書が印刷できない状態で電子的に配布された場合，設計レビューなどを行うのに不都合が生じるのは日常経験することである．

本来，電子文書であれ紙文書であれ，機密文書であればそれを管理している組織のセキュリティポリシーに従って適切に取り扱われるべきものであるため，電子文書だけアクセス制御を行うということでは片手落ちであると認識され始めている．

そこで，本研究では組織のセキュリティポリシーに従って電子，紙を問わず文書のセキュリティを確保できるシステム技術の開発を目的とする．

2. システムのコンセプト

多くの組織は機密文書の管理に関して，営業秘密管理規則のようなものを定めるのが一般的である．

以下に営業秘密管理規則としてよく見られる例を示す．

【マル秘の文書について】

- 「マル秘」であることを表示すること．
- 関係者のみ閲覧を許可する．
- 複写は原則禁止．
- 関係者以外に開示する場合には管理責任者の許可を受けた上で，開示履歴を記録すること．
- 部外への持ち出しは禁止．

このような営業秘密管理規則は，組織におけるドキュメントの取り扱いに関するセキュリティポリシーであると捉えることができる．このポリシーを掲げている組織は，ドキュメントの形態が電子であれ紙であれ，そのポリシーに従って適切にドキュメントが取り扱われることを求めている．

そこで，紙・電子ドキュメントを取り扱うシステム（ドキュメントシステムと総称する）において各構成要素におけるアクセスが組織のセキュリティポリシーに従って制御されるような仕組みを実現することを目標とする．

今回，組織のセキュリティポリシーに従ってアクセス制御を試みる対象としては，サーバ上でアクセス制御の管理下にあるような電子文書（これをサーバドキュメントと呼ぶ）と，ネットワーク上を流通するような電子文書（これをポータブルドキュメントと呼ぶ），そしてそのポータブルドキュメントを印刷した紙文書（これをプリントアウトと呼ぶ）とした．アクセス制御を行うアクセスの種別としては，電子文書への一般的なアクセスのほか，プリントアウトに対するデジタル複合機での複写等を含めている．

3. システムの実現方式

3-1 開発したシステムの全体概要

上述したコンセプトを実現するシステムとして，Fig.1に示すように電子文書管理サーバとクライアント，プリンタ，デジタル複合機，そして組織のセキュリティポリシーを管理し，そのポリシーに従ってアクセス制御の判断をするアクセ

ス制御サーバで構成されるドキュメントシステムを開発した．

電子文書管理サーバはクライアントからのアクセス要求があると，そのアクセスが許可されるかどうかアクセス制御サーバに問い合わせ，許可されていればドキュメントのダウンロードを許可する．また，クライアント端末においてドキュメントを印刷しようとするとドキュメントのビューアはアクセス制御サーバに権限を問い合わせ，権限があれば印刷処理を行う．ユーザがプリントアウトをデジタル複合機でコピーしようとするとそれが許可されるかどうかアクセス制御サーバに問い合わせて判断する．また，図示していないが，アクセス制御を行う前に各システムでユーザの認証を行う．

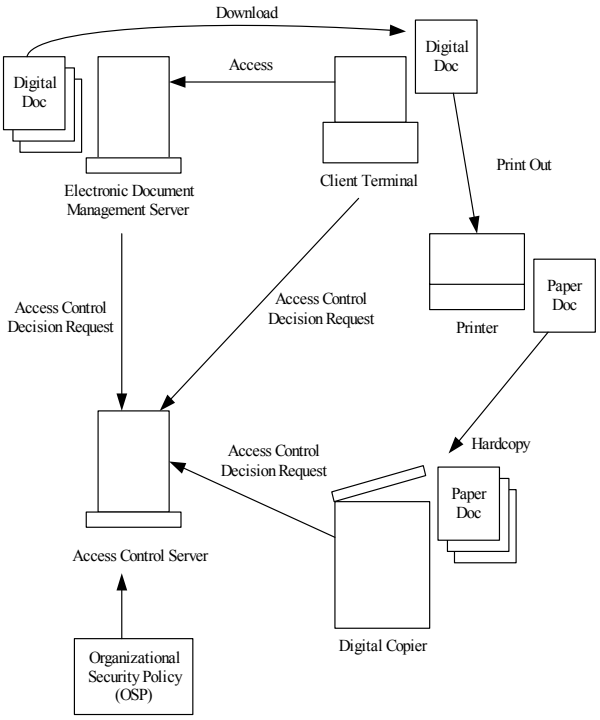

Fig.1　An overview of the developed document system.

このように，ドキュメントシステムの各構成要素においてドキュメントへの操作があるたびにアクセス制御サーバに問い合わせ，アクセス制御サーバが組織のセキュリティポリシーに従ってその操作の許可／不許可を判断することによって，ドキュメントシステム全体として，紙，電子を問わず適切にドキュメントを取り扱えるようにする．

このシステムを実現するために，組織のセキュリティポリシーをベースにしてアクセス制御を行う仕組みと，ポータブルドキュメントの印刷を制御する仕組み，プリントアウトを識別して処理を制御する仕組み，を開発した．

以下にそれぞれの仕組みについて説明する．

3-2　ポリシーの記述様式

先の営業秘密管理規則の例を見て分かるように，どのようなドキュメントはどのような利用者に対してどのようなアクセスを許可するのか／禁止するのか，また許可するための要件は何か，をポリシーとして規定できる必要がある．

アクセスの許可／不許可だけでなく許可に必要な処理を追加してアクセスを制御する仕組みは工藤らによって提案されている[1)]．また，最近ではそのようなアクセス制御ポリシーを記述するための業界標準としてXACML（eXtensible Access Control Markup Language）1.0がOASIS（Organization for the Advancement of Structured Information Standards）から提案されている[2)]．その追加処理に相当する用語は文献によってprovisionやobligationという用語が用いられているが，ここではそれらを区別せずまとめて「要件（requirement）」と呼ぶことにする．

Fig.2に今回開発したポリシー記述様式で記述した例の一部を示す．この例では以下のようなポリシーを表現している．[ ]で囲ったものは図中の対応部分を示している．

「文書カテゴリが人事関連[HUMAN_RES]で機密レベルがマル秘[SECRET]の文書については，権限レベルを問わず[ANY]，関係者[RELATED_PERSON]に対して複写[HARDCOPY]を許可するが，複写の際にログを記録すること[record_audit_data]と，複写した紙に複写したユーザ名を含む警告を印字すること[print_alarm]．」

文書の機密レベルによってその文書の取り扱いポリシーは異なるであろうし，人事関連や技術関連といった文書のカテゴリによって取り扱いポリシーを変えたいことがあると考え，ポリシーを規定する際に文書カテゴリ[DocCategory]と機密レベル[DocLevel]とで対象文書を区別することとした．同様にユーザについてもユーザ区分[UserCategory]と権限レベル[UserLevel]とで区別することとした．

また，ポリシーで規定できるドキュメントへのアクセス[Operation]としては，サーバドキュメントに対する保存，閲覧，改訂，削除といったアクセスだけでなく，クライアント

にダウンロードしたポータブルドキュメントに対する閲覧，印刷といったアクセスや，プリントアウトに対する複写[HARDCOPY]，スキャン，ファクス送信といったアクセスも含めるようにした．そしてポリシーに記載していないアクセスはそれを許可しないこととした．

また，各アクセスについて許可／不許可だけでなく要件[Requirement]を規定できるようにし，そのアクセスを許可する場合に処理しなければならない要件としてログの記録[record_audit_data]や警告文の印字[print_alarm]などを指定できるようにした．要件にはそれを補足する情報が必要な場合がある．例えば警告文の印字，という要件の場合の具体的な印字文字列などである．各要件にはそのような補足情報[Supplement]を指定できるようにした．

```
<AccRule>
  <DocCategory>HUMAN_RES</DocCategory>
  <DocLevel>SECRET</DocLevel>
  <Ace>
   <UserCategory>RELATED_PERSON</UserCategory>
   <UserLevel>ANY</UserLevel>
   <Operation>
    <Id>HARDCOPY</Id>
    <Requirement>
     <Id>record_audit_data</Id>
    </Requirement>
    <Requirement>
     <Id>print_alarm</Id>
     <Supplement>
      <Id>string_format</Id>
      <Data>"Copied by %u"</Data>
     </Supplement>
    </Requirement>
   </Operation>
   <Operation> … </Operation>
   …
  </Ace>
  <Ace> … </Ace>
  …
 </AccRule>
```

Fig.2　An example of security policy written in the developed policy language.

3-3　ポリシーに従った電子文書のアクセス制御

電子文書管理サーバのように，アクセス制御対象の電子文書に対するユーザからのアクセスをすべて仲介できるシステムの場合，ポリシーに従ってその電子文書へのアクセス制御を行うのはそれほど難しくない．

その一方で，正当な権限を持つユーザにより電子文書管理サーバからダウンロードされた電子文書，ポータブルドキュメントへのアクセス制御をポリシーに従って行うには特別な仕組みが必要である．

ポータブルドキュメントへのアクセスをポリシーに従って制御する一つの方法は，そのポータブルドキュメントにアクセスしているユーザ本人にポリシーに従ったドキュメントの取り扱いを強制することである．そのために，例えばサーバドキュメントへアクセスしたログを記録して情報漏洩の抑止力を働かせるようにすることや，サーバドキュメントにアクセスされたときに画面上に「取り扱い注意！」という表示を出してユーザ本人の注意を喚起することが考えられる．このように情報漏洩の抑止力を向上させるのはサーバドキュメントに対するアクセスに関してログ記録，警告表示といった要件をポリシーで規定しておくことで実現できる．

これは弱いポリシー強制であるが，よくセキュリティ教育が行き届いた組織で，信頼できるユーザだけがサーバドキュメントにアクセス可能であればこのような措置で十分組織のセキュリティポリシーの徹底に役立つと考えられる．もう一つの方法は，電子文書管理サーバと同じように，ポリシーに従ってアクセス制御をすることが可能な特別なドキュメントビューアでしか開けないように暗号化した電子文書ファイルを用いる方法である．

以下にその方式を説明する．

保護する必要のある電子文書ファイルを，その電子文書の文書カテゴリ，機密レベル，関係者といったセキュリティ属性とともにアクセス制御サーバに送付する．アクセス制御サーバは受け取った電子文書ファイルを暗号化し，内部の管理テーブルに文書ID，文書カテゴリ，機密レベル，関係者の情報，及び復号に必要となるパラメータを記録したエントリを作成する．そして暗号化した電子文書に文書IDを添付して暗号化電子文書ファイルにする（Fig.3）．

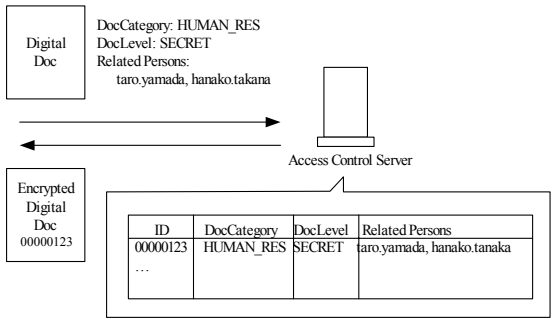

Fig.3　Protection of portable digital documents.

電子文書管理サーバはユーザからのアクセスがあったときにこの暗号化電子文書ファイルをユーザにアクセスさせる

ようにする．もちろん，必ずしも電子文書管理サーバで保護ドキュメントを管理する必要はなく，生成した保護ドキュメントは不正な流通を防ぐ安全な文書配布のためにも使用できる．

暗号化電子文書ファイルを受け取ったクライアントがそれを開こうとするとドキュメントビューアがユーザ認証を求め，ユーザ認証が成功した上で更にそのユーザがその電子文書の閲覧権限を持っているかアクセス制御サーバに問い合わせる．アクセス制御サーバはポリシーを参照してそのアクセスが許可されているかどうか確認し，許可されている場合にはポリシーで規定されている要件と暗号化電子文書ファイルを復号するためのパラメータをドキュメントビューアに送り返す（Fig.4）．

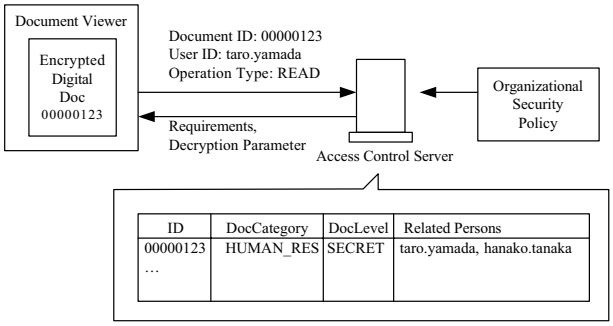

Fig.4　Policy enforcement for portable digital documents.

組織のセキュリティポリシーで規定される内容は「マル秘の文書について」，「関係者に対しては」，というように抽象度の高い記述がされている．

そのため実際にアクセス制御の判断を行うには，どの文書がマル秘なのか，その文書については誰が関係者なのか，といった個別の具体的なセキュリティ属性と，ポリシーに記載された抽象的な記述とを対応付けることが必要となる．

そこでアクセス制御サーバにおいてポリシーに従ってアクセス許可／不許可を判断する際，Fig.5に示すような抽象化のためのレイヤを設けるようにした．そのように具体的なセキュリティ属性とポリシーの記述とを分離することで，例えば「マル秘の文書は関係者であっても閲覧には許可が必要」というように後で組織のセキュリティポリシーを変更した場合に，個々の文書のセキュリティ属性を変更することなくシステム全体にポリシーの変更を反映させることが可能となる．

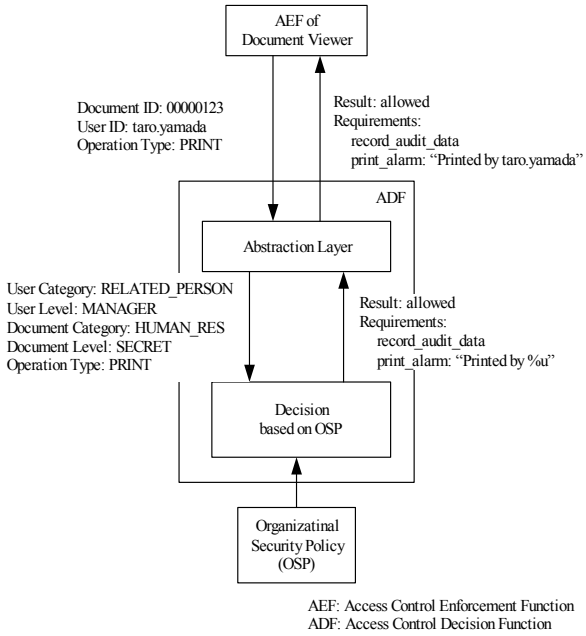

Fig.5　Schematic diagram of OSP-based access control mechanism. (OSP: Organizational Security Policy)

このポータブルドキュメントのアクセス制御方法はドキュメントビューアにより強いポリシー強制を維持することができるため，アクセス権限のあるユーザが必ずしも完全に信頼できるユーザではない，という組織において役に立つと考えられる．

アクセス権限があるのに信頼できない，というのは矛盾しているように感じられるが，情報漏洩をしないと確信できるユーザ以外にも業務遂行上アクセス権を与えることは日常よく行われることであり，今日，組織において問題となっているのは特にこのような状況である．

3-4　ポリシーに従った紙文書のアクセス制御

前節で述べたポータブルドキュメントのアクセス制御方法を拡張して利用することで，紙文書のアクセス制御も行えるようにした．その方式を以下に説明する．

ポータブルドキュメントの閲覧をする場合と同様，ドキュメントビューアはユーザから文書の印刷を要求されると，そのユーザがその文書の印刷権限を持っているかアクセス制御サーバに確認する．アクセス制御サーバはポリシーを参照してアクセス権限を確認し，その判断結果をドキュメントビューアに返す．その際，ポリシーで印刷の際の要件が規定されていればその要件を一緒に返す．

このようにして印刷の権限を持つユーザにのみ印刷を許

可することができ，プリントアウトを入手できるユーザが限定されることになる．よく教育されていて信頼できるユーザにしか印刷を許可しないようにできるのであればこのレベルで十分と考えられる．

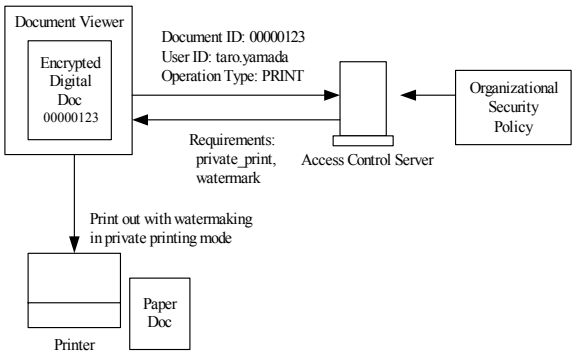

Fig.6　Policy enforcement on printing documents.

その一方で，業務遂行上印刷を禁止するわけにはいかないがそのプリントアウトを経由して漏洩する可能性を低減したい，という場合には，更に印刷時の要件を使ってその可能性を低減させることができる．例えば，機密文書をプリントアウトしたものがプリンタ上に放置されて他人に持ち去られることを避けるために，プリンタの機密印刷モードを使用して印刷することを要件としてポリシーで規定しておけば，プリンタのオペレーションパネルでパスワードを入力するなどして，印刷者本人であることの確認が取れなければプリントアウトが出力されない，というようなことが可能となる．他にも，印刷した本人による情報漏洩に対する抑止力を高めるために，印刷したユーザ名を紙面に入れたり，背景の透かしとして印字したりすることを要件としてポリシーで規定してそれを自動的に処理することもできる．

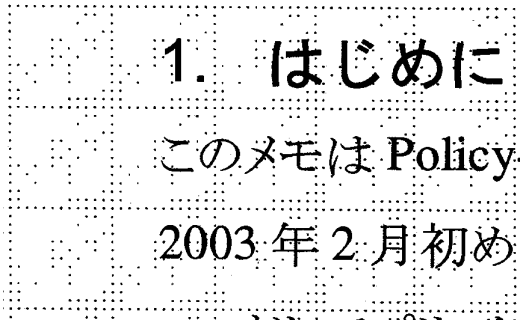

Fig.7　An example of identification pattern embedded on a printout.

この印刷時のポリシー強制を応用して，印刷する際に紙面にデジタル複合機などの紙文書を扱う機器で識別可能な識別パターンを印刷しておくことも可能である．Fig.7に今回開発した識別パターンのサンプルを示す．パターンの方向識別用のドット，個々のブロック領域識別用のドット，誤り訂正用のドットを含めて12×12のドットで56ビットの情報を格納できる．この中に識別パターン種別を8ビット，アクセス制御サーバの識別IDを16ビット，プリントアウトごとに振るプリントIDを32ビット格納した．

識別パターンのエンコード／デコードのアルゴリズムの説明は紙面の都合上割愛する．

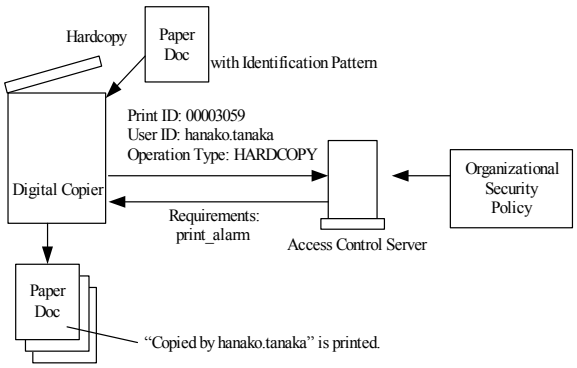

Fig.8　Policy enforcement on copying printouts.

上記の識別パターンを検知できるデジタル複合機を開発し，識別パターンが印刷されたプリントアウトを本デジタル複合機で複写しようとすると，Fig.8に示すようにその識別パターンを自動的に検知して識別し，そのユーザがそのプリントアウトを複写することをポリシーで許可されているかどうかアクセス制御サーバに問い合わせるようにした．他のアクセス権限確認と同様，アクセス制御サーバからは複写の許可／不許可と，許可する場合にはポリシーで規定されている要件を返す．デジタル複合機はアクセス制御サーバから返される要件，例えば複写したユーザ名を印字するような要件[print_alarm]，を処理して各複写紙面に“Copied by hanako.tanaka”といった文字列を印字する．

複写時にどのような要件を規定するかは組織のポリシー次第であり，もちろん文書の種別によっては複写を禁止するというポリシーでも良いが，上記のようにその紙文書を取り扱っているユーザ自身に情報漏洩の抑止力を働かせるような要件を規定することにより業務上複写が必要なケースでも組

織のセキュリティポリシーを徹底する効果を出すことができる．

今回開発したシステムではデジタル複合機の複写機能に上記の識別パターン検知機能を組み込んだが，スキャン機能，ファクス送信機能についても同様に考えることができる．

このように紙文書の取り扱いに関して，

・プリントアウトを他人に持ち去られないような処理を自動的に行わせる
・プリントアウトした本人に対するポリシー強制を強める
・複写しようとする本人に対するポリシー強制を強める

といったことを行うことで紙文書に対しても組織のセキュリティポリシーの徹底を図ることができる．

4. 開発システムの評価

開発したシステムのデモンストレーションを通して社外30団体に対してこのシステムの有効性についてインタビューを行った．その結果をTable 1に示す．

Table 1　The result of interviews.

分類	件数
電子文書に関して有効	8件
紙文書に関して有効	18件

印刷におけるセキュリティ処理に関して有効であるという意見をもらった場合には基本的に「紙文書に対して有効」と分類している．印刷を禁止する，印刷ログを取る，という電子文書へのアクセスに関するものとしても分類できる2件は双方にカウントした．

このインタビュー結果は単純な件数の集計であり，デモンストレーションのやり方や説明の仕方の影響があり，またインタビュー対象者も情報を管理する立場の人と，情報を利用する立場の人が混じっているため，この結果を単純にシステムの有効性として評価することはできないが，紙文書に対するセキュリティ要求の高さの表れとして捉えることはできる．

特に電子文書についてはアクセスの管理をすでに実施しているところが多く，関係者だけがアクセスできるように，という要求が満たされていればそれ以上のことを求める意見はあまり出なかった．その一方で，紙文書に対しては現状何の対策もとっていないところが多く，本開発システムの中で有効性を認める部分も様々に異なっていた．意見が異なるのは，紙文書についてはどのようなコントロールが情報漏洩防止に有効に働くのかまだ経験がないこと，組織の置かれている環境や文書の種別によって取り扱いのポリシーが様々に異なること，が起因していると考えられる．

5. 文書のセキュリティに関する考察

5-1　電子文書のセキュリティ

今回開発したシステムは完全には信頼できないユーザ（これをSemi-trusted Userと呼ぶ）に対するセキュリティポリシーの徹底とその自動化に焦点を当てている．

元々信頼できるユーザ（これをTrusted Userと呼ぶ）は組織のセキュリティポリシーに従って適切に文書を取り扱うため，必要であってもせいぜい注意を喚起すればよい．一方，Semi-trusted Userは不注意で関係者以外に機密文書を渡したり，共有フォルダに不用意に機密文書を保管したりする可能性がある．

このような状況に対して，本システムはポリシーを強制するドキュメントビューアでしかドキュメントにアクセスできないような仕組みを提供できるようにしたことで，ドキュメントへのアクセスが常に組織のセキュリティポリシーに従って制御されるようになり，そのようなSemi-trusted Userによる悪意のないポリシー侵害を防いでセキュリティを確保することができる．

その一方で全く信頼できないユーザ，悪意を持ったユーザ（これをMalicious Userと呼ぶ），にアクセス権限を与えている場合，たとえ印刷をさせないようにポリシーに従ってアクセス制御されていたとしても，閲覧さえできれば表示された画面をカメラで撮影する等，他の手立てでポリシーを侵害するような情報漏洩行為が可能である．したがって，少なくともMalicious Userに対してはアクセス権限を与えないようにしなければならない．

5-2　紙文書のセキュリティ

紙文書については，前節の電子文書と異なり暗号化など文書をプロテクトする方法がないため，ポリシーに従ったアクセス制御を技術的に強制することができない．そのため，その紙文書の持ち主にポリシーに従った取り扱いを強制する必要がある．

Trusted Userが印刷する場合には，電子文書と同様，やはりせいぜい取り扱いを注意するように印刷時に注意を促せばセキュリティポリシーに従った取り扱いをするであろう．その一方で，Semi-trusted Userが印刷する場合には，不注意で関係者以外に印刷した機密文書を配布したり，放置したりする可能性がある．

このような状況に対して，本システムは印刷時に本人が関係者以外に機密文書を配布しないよう抑止力を働かせるような印刷処理，例えば印刷者名を自動的に印刷するなどを行う仕組みを提供することによりポリシー侵害を防ぐ．また，印刷者本人を確認しないとプリントアウトが出力されないように制御することで機密文書が放置される可能性を低減し，更には放置されている機密文書を持ち主以外が複写しようとしたときに，そこに設置されているデジタル複合機が紙文書を識別してセキュリティポリシーに従ったアクセス制御を行うことで，ポリシー侵害を防いでセキュリティを確保することができる．

Semi-trusted Userにとって，自分の名前が入ったような機密文書が信用できない他人（Malicious Userを含む）に渡ることは自分に非常に不利になるため紙文書の配布には十分な配慮をすることになるであろう．そして，放置されている機密文書をMalicious Userが入手して漏洩させる可能性については，インタビューの中でも「机に置いてある紙文書を持ち出すと持ち主に気づかれるが，コピーなら軽い気持ちでとってしまう可能性がある」，「外部に書類を持ち出して複写するというのは敷居が高い」という意見があり，機密文書を扱う部門のデジタル複合機に本システムの機能が備わっていれば，情報漏洩に対して一定の効果が期待できる．

6. まとめ

組織のセキュリティポリシーに従って紙・電子のドキュメントのセキュリティを確保するシステムについて，開発したシステムの仕組みを説明した．そしてポリシーに従ったアクセス制御において許可／不許可だけでなく要件を規定するようにし，その要件をユーザの情報漏洩抑止力を高めるため及び電子文書の印刷時にセキュリティ処理を強制するために利用することで，電子文書だけでなく紙文書の取り扱いまで一貫して組織のセキュリティポリシーを徹底させる効果を発揮できることを示した．

また，開発したシステムが提供する電子文書，紙文書に対するセキュリティ効果の考察を通して，一般的なオフィスにおいて十分な効果が期待できることを示した．

また，最近では組織の情報セキュリティマネジメントシステムを構築する動きがISMSの適合性評価制度[3)]の広まりとともに盛んになってきているが，セキュリティポリシーを徹底する教育を行うと同時に本システムを活用することで，高い情報漏洩防止効果を発揮できると考えられる．

今後，本システムの有効性と情報漏洩を防止する効果の検証を，実証実験を通して行っていきたい．

参考文献

1) 工藤道治，羽田知史，“必須処理付きセキュリティポリシーのためのアクセス制御モデル”，CSEC研究会，No.14，pp.149－156，July 2001.

2) OASIS Standard, “eXtensible Access Control Markup Language (XACML) Version 1.0”, http://www.oasis-open.org/committees/xacml/repository/, 18 February 2003

3) （財）日本情報処理開発協会，“情報セキュリティマネジメントシステム（ISMS）適合性評価制度”，http://www.isms.jipdec.or.jp/