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

2005－DPS－122（65）
2005－CSEC－28（65）
2005／3／23

属性の伝播を利用した電子文書の柔軟な利用制御方式の提案

鷲尾知暁　除補由紀子　大嶋嘉人　金井敦
NTT 情報流通プラットフォーム研究所

アブストラクト：機密情報の漏洩が深刻化しており、それに従って，多くの企業が漏洩防止対策を強化している．情報漏洩の典型例の一つである，企業内部の人間の故意あるいは過失による機密文書の漏洩を防止することを主な目的として，利用者端末上での文書操作を制限・禁止する利用制御機構が検討され，導入されつつある。しかし，このような機構の導入により，正当な利用者による正当な業務遂行が困難になり、その効率が低下することが懸念される．本稿では，文書属性の伝播というコンセプトに基づいた利用制御方式を提案する。本方式により，情報漏洩を防止しながらも，従来と同様の利便性を持った情報の利活用が可能となる．

A Proposal of a Usage Control Method that Utilizes a Propagation of Document Attributes

Tomoaki WASHIO　Yukiko YOSUKE　Yoshihito OSHIMA　Atsushi KANAI
NTT Information Sharing Platform Laboratories, NTT Corporation

ABSTRACT: As the leakage of the classified information becomes serious, a lot of enterprises have strengthened the measures to prevent the leakage. To prevent mainly the leakage by person in the enterprise (e.g. employees) which is one of the typical cases of the information leakage , usage control mechanisms which control the document operation on the user terminal are examined and adopted. By adoption of such mechanisms, however, the right business operations might be obstructed or its efficiency might decrease. In this paper, a usage control method is proposed which utilizes a propagation of document attributes. The method achieves both the prevention of the information leakage and the operation of documents with conventional convenience.

1.　はじめに

近年，企業からの機密情報の漏洩が深刻化している．企業内では，ファイルサーバ上の機密文書の参照や，電子メールに添付された重要文書の受け取りなどが，業務の過程で日常的に行われ．よって，社員が通常使用しているクライアントに機密情報が一時的あるいは永続的に格納されることも多い．クライアントに格納された情報は，CD/DVD や USB メモリ等の可搬媒体への複製や紙への印刷等により容易に外部に持ち出せることから，漏洩の危険性が高い．そのため，漏洩対策の一環として，クライアントでの情報利用が制限されるケースが多くなっている[1][2]．しかし，端末における漏洩対策の実施は，正当な目的で行われる機密情報の利活用を制限してしまい，利便性や作業効率を低下させることが懸念される．

そこで本稿では，文書属性の伝播というコンセプトを導入することにより，機密情報の漏洩を防止しつつも，既存電子文書の積極的な利活用を可能とする，柔軟性の高い利用制御方式を提案する．

2.　情報漏洩への対策とその問題

2.1. 機密情報の漏洩と対策

機密情報の漏洩には，外部の人間による場合と，内部の人間による場合とがある．外部の人間による漏洩は，通信の盗聴や外部からの社内ネットワークへの不正アクセス等，攻撃者により意図的に行われることが多い．これらに対しては，通信路の暗号化やファイアウォールの設置などのセキュリティ対策が従来から実施されている．

これに対し，内部の人間に起因する漏洩は，もともと機密情報へのアクセス権限を有しているユーザによる故意・過失により引き起こされるものである．

内部からの漏洩は，主に以下のような手段により行われる．

・ネットワーク経由で外部に送信する

・可搬媒体に複製して外部に持ち出す

・印刷した上で紙媒体として外部に持ち出す

・PC やハードディスクごと持ち出す

これらは，その行為だけを見てみると，いずれも業務の遂行上，日常的に行われるものである．そのため，正当に行われる機密情報の利用との区別がしにくく，外部からの攻撃に比べ対策が難しい．また，特定の権限者により一元的に管理されるサーバ上の機密文書に比べ，クライアント上に存在する文書は，クライアントそのものの管理が各ユーザの裁量に任されることが多いこともあり，漏洩の危険性が高い．そのため，クライアントにおける漏洩対策が重要となる．

その具体的な方法として，ファイルの利用に対し以下のような制限を設ける手法が従来より考えられている．

・読み込み制限

ファイル内容の参照を禁止することで，クライアントへの機密情報の伝達を防ぐ．旧来より行われている，いわゆるアクセス制御はこれに該当する．

・書き出し制限

ハードディスクや可搬記憶メディアへの複製，プリンタによる印刷，ネットワーク経由での送信等を禁止することで，クライアントから機密情報が外部に出力されるのを防止する．

・データ複製制限

クリップボードの使用もしくはコピー・ペースト操作を禁止することで，機密文書の一部が他の文書に複製されることを防止する．

従来からアクセス制御として行われている読み込み制限については，ユーザの資格や所属などの属性を用いて条件設定を行うなど柔軟な制御を行えるようにしたものが多い．一方，書き出し制限やデータ複製制限は，操作対象の文書が機密情報か否かといった単純な区分でのみ，あるいは，そういった区別も無くクライアント上で一律に制限されることが多い．

2.2. データ複製制限の詳細

書き出し制限を行う場合，一律に禁止をしてしまうと会議資料が印刷できないなど業務に多大な支障が出る．そこで，極めてセキュリティレベルの高い環境でもない限り，機密文書と一般文書との区分に応じて書き出しを禁止したり，書き出せるメディア（方法）を変えることが多い．しかし，外部への書き出しが禁じられている機密文書の一部が，クリップボードなど共有メモリを介して，一般文書に複製されることにより，機密情報が一般情報に紛れて漏洩してしまう危険性がある（図1）．

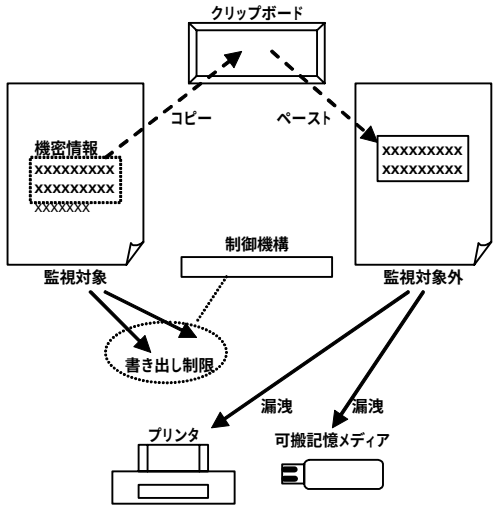


図1　データ複製による機密情報の漏洩

このように，コピー・ペースト操作やクリップボードの使用は，漏洩の間接的な手段として利用される可能性があるため，従来の漏洩対策では，書き出し制限に加えてデータ複製の制限も行われることが多い（図2）．データ複製の制限は，通常コピー操作（クリップボードへの書き込み操作）に対して行われ，例えば，区分が機密文書に該当する文書からのコピーは禁止する，といった形で制御されることが多い．

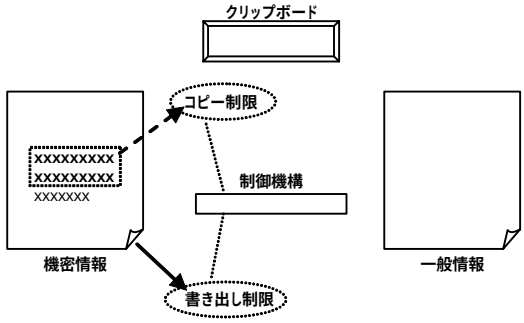


図2　データ複製の禁止

2.3. 情報の利活用に対する弊害

企業において扱われる情報の多くは，編集・再利用されるものであり，機密情報であっても例外ではない．しかし，前述のようにデータ複製が制限されることにより，情報の編集や再利用が妨げられる恐れがある．

例えば，電子文書の編集作業において，文中の一部を他の部分にコピー・ペーストする行為は，特に意識することなく多用されている．もし仮にコピー・ペーストが禁止されると，同じような文章を一から入力しなければならない，あるいは，文章の前後関係を入れ替えるにも，文章の大半を再投入する必要があるなど，作業効率が大幅に低下する恐れがある．

また，既存の電子文書の一部を，別の電子文書中で再利用すること

や, 複数の電子文書をひとつにまとめて新たな電子文書を作成することも多い. 機密文書からの部分的なコピーが禁止された場合, ほぼ同じ内容の電子文書を一から作成することにもなりかねない.

「編集が容易」, 「データの部分的な再利用が可能」といったデジタル情報の特徴は, 本来, ドキュメント編集作業の効率を高める要素であるが, 漏洩対策が施されたクライアントでは, これらの利点を有効に活かせず, 作業効率の低下につながる可能性がある. これらは, 漏洩対策の実施に伴う情報の利活用への弊害といえる.

3. 解決のアプローチ

漏洩対策の目的の本質は, 機密情報の外部への不正な漏洩を防止することである. 機密情報が複製されたり, 機密文書の一部が複製され他の文書に転用されたとしても, それらの情報が元の機密文書に課されるべき制限を逸脱する形で外部に出ない限り問題とはならない. つまり, 保存や印刷など, クライアント外部への出力が行われる時点で, 対象の電子文書が保護すべき情報を含むか確認し, それに必要に応じて出力を制限すれば十分であり, コピー・ペースト操作やクリップボードの使用による情報の複製や転用を一律禁止する必要はないと考えられる.

そこで, 我々は, データ複製を監視·追跡し, データ複製先の電子文書に対して, データ複製元の電子文書に対して行われる制御と同様の出力制御を実施するアプローチを採用する (図3). これにより, 情報漏洩を防止しながら, 先に述べたような情報の利活用に対する弊害を生じない対策が可能と考える.

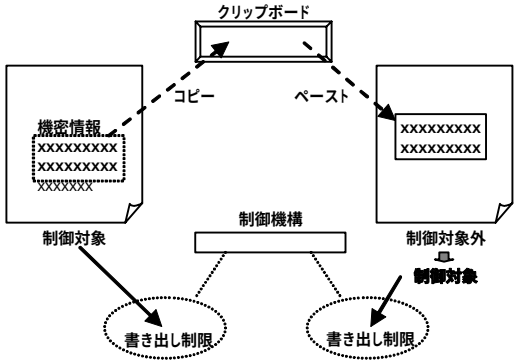


図3 データ複製の監視·追跡による制御

4. 文書属性の伝播を用いた利用制御方式

提案する利用制御方式は, 大きく分けて, 書き出し制御部と文書属性伝播部の二つのコンポーネントからなる. 以下, それぞれについての概略を紹介した後, これらの組み合わせからなる利用制御方式の全体について述べる.

4.1. 出力制御

出力制御部では, 所定の規約, すなわち, 出力の可否判断 (認可) の基準となる制御ポリシに基づいて, クライアントにおける書き出しを制御する. 制御対象とする書き出し処理は, クライアント内のハードディスクや CD/DVD や USB メモリ等の外部接続の記憶メディア, およびプリンタ等への書き出しである.

我々は, ポリシを個々の文書に対応付けるのではなく, 文書の属性 (作成者, 管理組織, 機密レベルなど) や利用者の属性 (所属, 役職など) などと対応させる, いわゆる属性ベースのポリシを採用している. これは, OASIS で規定された XACML(eXtensible Access Control Markup Language)[4]等と同様のモデルである. 例えば, 「文書属性『機密レベル』の値が『高』の文書については, 利用者属性『役職』の値が『マネージャ』の利用者による『印刷』操作を許可する」などといった記述が可能である.

このような属性ベースのポリシを採用することにより, きめ細かい出力制御と柔軟でメンテナンスが容易なポリシ管理の両立が可能となる.

4.2. 文書属性の伝播

3章で述べたように, 本方式では, コピー・ペースト操作やクリップボードの使用を禁止するのではなく, これら操作により文書の一部データが複製された先の文書に対して, 少なくとも複製元の文書と同程度の出力制限を行うというアプローチを取る. すなわち, データ複製先の文書に対して, 複製元の文書に対する利用規約を課すことが本方式の最も重要な特徴である.

上記を実現するため, 本利用制御方式では, 電子文書間で共有メモリ (クリップボード) を介してデータの複製が行われる場面において, 複製元の文書から複製先の文書へと文書属性を伝播させる機構 (文書属性伝播部) を設ける (図4).

データ複製元の電子文書の文書属性をデータ複製先の電子文書の文書属性に伝播することにより, 複製されたデータを含む電子文書には, 元々の文書属性の他に, データ複製元の電子文書の文書属性が追加的に関連付けられることとなる. 前節で述べた通り, 出力制御で用いるポリシは文書属性と対応付けられているため, 複製されたデータを含む電子文書をアプリケーションが書き出す際には, 双方の文書属性に対応付けられたポリシが取得され, 両ポリシに基づいた認可判定の結果を総合的に判断して出力制御が行われる.

文書属性の伝播を行うことにより, 書き出しが制限される機密情報を含んだ電子文書のデータが, 書出しが制限されない電子文書に複製されても, 機密情報を含む電子文書は結果的に書き出しが制限されるため, 情報漏洩に繋がることはない. また, コピー・ペースト操作やクリップ

ボードの使用が許容されることから，機密情報であっても編集作業が妨げられず，他の電子文書への転用も行え，積極的な情報の利活用が可能となる．

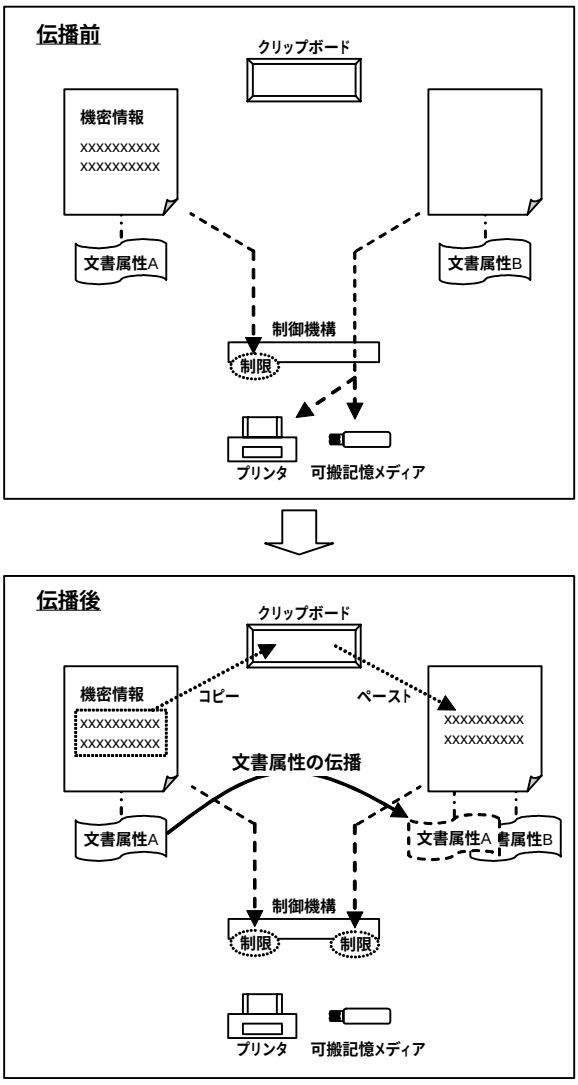


図4　文書属性の伝播

4.3. 制御の仕組み

本節では，出力制御部と属性伝播部を含む，本利用制御方式の全体についてより詳細に説明する（図5）．

本方式では，オペレーティングシステム（OS）が電子文書の入出力処理用にアプリケーション等に提供しているインターフェースの監視を行う．監視対象のインターフェースに向けてアプリケーションが行う電子文書の読み込み要求を捕捉し，これを契機に制御を開始する．捕捉した要求から，読み込み対象となる電子文書を特定するとともに，要求を行ったアプリケーションを特定する．クライアントでは，格納されている電子文書と電子文書に関連付けられている文書属性の対応をテーブルで管理しておき，捕捉した読み込み要求から特定した電子文書について，テーブルを参照し，アプリケーションに読み込まれた電子文書の文書属性を特定する．特定した文書属性は，電子文書を読み込んだアプリケーションとともに，アプリケーションが電子文書を閉じるまで記憶しておくこととする．この時点で，電子文書を読み込んだアプリケーションは監視対象となり，その後の動作が制御されることとなる．

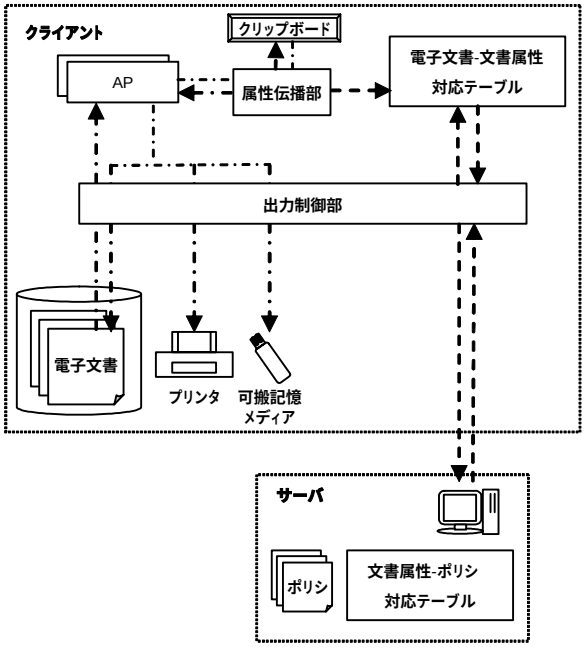


図5　システム概要

アプリケーションが電子文書の書き出しを行う際には，読み込み時と同様に書き込み要求が捕捉される．捕捉した要求からは，書き出し先を特定する情報（書き出し先パス）を取得するとともに，要求を行ったアプリケーションを特定する．読み込み時に記憶しておいたアプリケーションと文書属性の対応を参照することにより，どのような文書属性の電子文書が，どこに書き出されようとしているのかが分かる．この後，要求された書き出しについて，処理を実施するか否かの認可判定を行う．本方式では，文書属性とポリシを関連付けてサーバ等で管理することとし，クライアントは書き出されようとしている電子文書の文書属性と関連付けられているポリシをここから取得する．取得したポリシに基づきアプリケーションからの処理要求についての認可判定を行い，判定結果に応じて要求処理を実施，または拒否する．

次に，文書属性の伝播の具体的な仕組みについて説明する．電子文書間でのデータ複製は，各電子文書を読み込んでいるアプリケーションの一方が，共有メモリ（クリップボード）へのデータ書き込みを行い，他方が共有メモリからのデータ読み出しを行うことにより実現する．そこで，前述の電子文書の入出力制御の場合と同様に，OS が共有メモリへの入出

力用に提供しているインターフェースの監視を行う.

監視対象のインターフェースに向けてアプリケーションが行うデータ書き込み要求を捕捉し, 要求を行ったアプリケーションを特定する. 各アプリケーションが開いている電子文書の文書属性は, 前述のとおり, アプリケーションと文書属性の対応を管理していることから, これを参照することにより特定できる. そこで, 共有メモリへのデータ書き込みを行ったアプリケーションが現在読み込んでいる電子文書の文書属性を特定することにより, 共有メモリに書き込まれたデータが, どのような文書属性を持つ電子文書の一部であるかを把握することができる. データ複製が行われる際には, ここで特定した文書属性を, データ複製先の電子文書に伝播させる.

共有メモリからのデータ読み出し要求についても同様に, 要求の捕捉とアプリケーションの特定を行い, 特定したアプリケーションが現在読み込んでいる電子文書に関連付けられる文書属性として, 前述の共有メモリ上のデータの文書属性を追加する. もともと文書属性が関連付けられていない電子文書については, 新規に文書属性との対応付けを行う.

5. プロトタイプ

5.1. 実装方法

提案方式に基づき, Windows 環境で動作する利用制御システムのプロトタイプ実装を行った. 今回のプロトタイプは, 主に文書属性の伝播についての実現性を確認することを目的としている. そのため, ポリシ記述, および認可機構は簡易なものとなっている. また, サーバからのポリシ取得は行わず, クライアント内に置かれたポリシに基づき認可判定を行う.

ハードディスクや外部接続の記憶メディア等のデバイスに対する入出力の監視は, Windows OS のユーザモードとカーネルモードの境に位置するシステムサービスにより提供される API を監視することにより実現する. 特定のシステムサービス API を監視することにより, ユーザモードで提供されている WIN32API 等の様々な API に対してアプリケーションが行う電子文書の入出力要求を集約した形で捕捉できる.

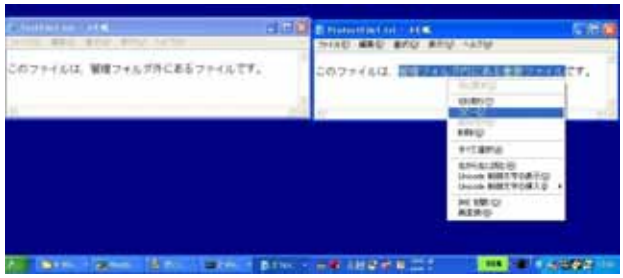
また, クリップボードに対する入出力の監視は, アプリケーションによる Win32API の関数呼び出しを監視することにより実現する.

プロトタイプでは, 各種メディアへの書き出し制限の他に, 印刷制限等も可能である.

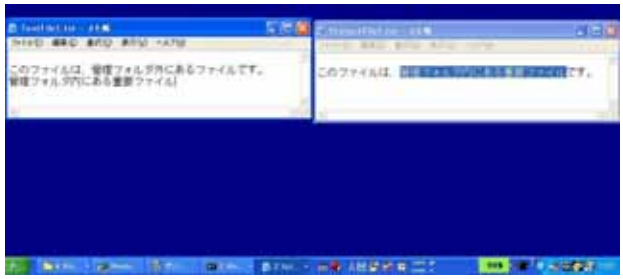
5.2. 動作例

書き出しが制限されている電子文書から, 一部データを複製した場合に, 文書属性の伝播によりデータ複製先電子文書の書き出しが制限される様子を示す (図6).

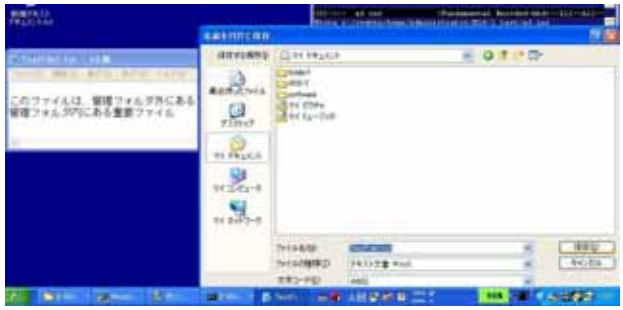
(a)



(b)



(c)



(d)

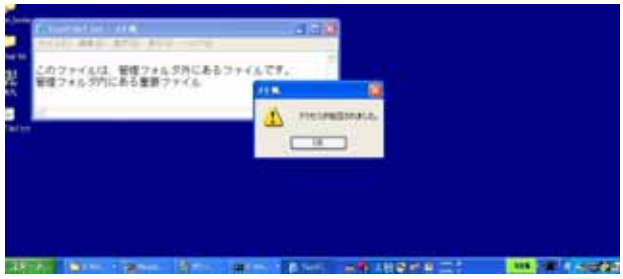


図6 動作例

機密情報に見立てた一方の電子文書 A(図中右のファイル)の文書属性には, 以下のような内容のポリシが対応付けられており, 特定のフォルダ (管理フォルダ) 以外への書き出しを制限するよう設定している.

・管理フォルダへの書き出し:許可

・管理フォルダ外への書き出し:不許可

・印刷による書き出し:不許可

また, 一般情報に見立てた他方の電子文書B(図中左のファイル)には

文書属性を関連付けておらず，全ての操作が制限されずに行える状態となっている．

・管理フォルダへの書き出し：許可

・管理フォルダ外への書き出し：許可

・印刷による書き出し：許可

このような状況において，電子文書 A の一部データをコピーし（図6a），電子文書 B にペーストする（図6b）と，電子文書 A に関連付けられている文書属性が伝播し，電子文書 B の文書属性として関連付けられる．これにより，電子文書 A のデータを含む電子文書 B を管理フォルダ以外に保存しようとすると（図6c），追加された文書属性に対応付けられているポリシに基づく認可判定が行われるため，判定結果として「不許可」が返却され，管理フォルダ外への書き出し要求は拒否される（図6d）．ここで，保存先を管理フォルダとした場合には，判定結果が「許可」となるため，拒否されることなく書き出しが行える．

コピー・ペースト操作やクリップボードの使用は制限されないため，機密情報，一般情報にかかわらず，通常通りの編集作業が可能である．また，機密情報であっても他の情報へのデータ複製・転用が可能であることから，指定された格納先に保存さえすれば，情報の利活用を制限されることはなく，ユーザの利便性を損なわずに情報漏洩を防止することが可能である．

6. 考察

提案した利用制御方式を採用した場合，電子文書間でのデータ複製が許容されることから，様々なポリシにより管理されている複数の電子文書を，一つの電子文書に併合することが可能である．複数の電子文書のデータを含んだ電子文書には，文書属性の伝播により，各電子文書の文書属性が追加される．

しかしながら，この時，制限事項や利用条件が緩く設定されている電子文書から，制限事項や利用条件が厳しく設定されている電子文書へのデータ複製が行われるような場合，属性伝播が行われることにより，セキュリティレベルが低下することも考えられる．そのため，このような場合には，データ複製の操作は許容するが，属性伝播は行わないなどのルールを定めておく必要も考えられる．

また，属性伝播が行われ，1 つの電子文書に対し複数の文書属性が関連付けられた場合，電子文書の利用時の認可判定において判定結果を一意に決定できない認可の競合[5]が生じる可能性がある．例えば，それぞれの文書属性に関連付けられたポリシの一方で「グループ A に所属するユーザであれば許可」とあり，他方で「グループ A に所属するユーザは不許可」とある場合，条件が同じであるにもかかわらず，認可判定の結果は矛盾する．両方のポリシ（文書属性）を尊重した場合，この電子文書は誰も利用できないものになってしまう可能性もある．情報漏洩の防止を目的とした利用制御では，複数のポリシについて認可判定を行った結果，一つでも「不許可」がある場合には，最終的な判定結果として「不許可」を導出するようなアルゴリズムを設けておくことにより，この問題を整理することも考えられるが，認可判定に矛盾を生じさせないためにも，このような事象が起こりえる電子文書間でのデータ複製については制限することも考えられる．

このように，文書属性の伝播では，安全性の低下や認可の競合が起こらぬように，各文書属性に関連付けられたポリシを事前に解釈する必要もあるかもしれない．

7. まとめ

本稿では，漏洩対策の実施によるクライアント環境での利便性の低下について触れ，情報の利活用を妨げない漏洩対策の必要性について述べた．さらに，文書属性の伝播というコンセプトを導入し，情報漏洩を防止しながらも，情報の積極的な利活用を可能とする利用制御方式を提案し，その実現方法，およびプロトタイプ実装について述べた．今後は，ネットワーク上での情報共有も含め，安全性と利便性を両立する情報管理のための利用制御方法について検討を行う．

参考文献

[1]青柳慶光，鮫島吉喜：”機密ファイル持出し防止システムの検討”，コンピュータセキュリティシンポジウム 2004.

[2]荒井正人，甲斐賢，永井康彦，冨田理：”情報漏洩防止システムの提案”，DPS-117/CSEC-24(2004).

[3]FUJITSU JOURNAL VOL.30, NO.1 (2004) http://journal.fujitsu.com/267/top_security/03.html

[4]OASIS eXtensible Access Control Markup Language TC. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

[5]双紙正和，加藤丈治，前川守：”ディアルラベルを利用したアクセス制御モデル”，情報処理学会論文誌，Vol. 40, No. 3, pp. 1305-1313 (1999).