6Y-1

情報漏洩元の特定を可能とする電子文書管理システムの設計

今井 正樹 † 上原 哲太郎 †† 侯 書会 ‡ 津田 侑 † 喜多 一 ††
† 京都大学 大学院情報学研究科 †† 京都大学 学術情報メディアセンター ‡ 北京科技大学 数力学系

1 はじめに

企業が情報資産管理を実現する方法に電子文書管理システムがある．電子文書管理システムはアクセス制御や情報漏洩対策などの機能を備えており，情報の不正入手を困難にできる．しかし，内部不正者はアクセス権限を持つため，情報漏洩対策が困難である．そのため情報漏洩抑止が重要となる．情報漏洩抑止は情報漏洩を完全に防止するものではないが，情報漏洩のリスクを軽減できる．

内部不正者の情報漏洩抑止の対策として，電子文書にユーザを特定可能なID（以下，ユーザID）を電子透かしで埋め込む機能が提案されている‡‡．この機能は，情報漏洩発生時に情報漏洩元の特定を容易にし，ユーザIDの存在をユーザに周知することで情報漏洩を心理的に抑止する．

しかし，ユーザIDは結託攻撃 [2] と呼ばれる手法により改竄される危険性がある．そこで本稿では，結託攻撃に対処できる結託耐性符号を用いた電子文書管理システムを提案する．本システムでは結託耐性符号でユーザIDを符号化し，電子透かしによりユーザIDを電子文書に埋め込む．この機能により電子文書のID改竄が困難となり，内部不正者への情報漏洩抑止効果を向上できる．

本稿では最も広く用いられているOOXML（Office Open XML）形式の文書を対象とする．また，本稿では電子透かしを削除できるIT技術に精通した内部不正者は対象としない．

2 関連研究

2.1 電子透かし

本稿で用いる電子透かしは，結託耐性符号の前提であるMarking Assumptionが成立する必要がある．Marking Assumptionとは，符号を比較した際に異なる部分のみが改竄されるという仮定である．OOXML形式で利用可能で，この仮定が成立する電子透かしに，改行位置を調整する手法 [3]，同義語を置換する手法 [4]，Word2003形式の文書の空白文字を利用する手法 [5] などがある．このうち空白文字を利用する手法は，文書の比較により透かしを見破られる危険性があるが，文章のという点で他の２つより優れている．

2.2 電子文書管理システム

電子文書管理システムは，電子文書に作成日時などのメタデータを付与して保存し，分類可能とすることで，検索やアクセス制御，情報漏洩対策などを実現する．情報漏洩対策機能には，ログ管理，アクセス権に応じた操作制限，ユーザIDの埋込みなどがある[1]．こうした機能のうち，内部不正者に抑止効果があるのはログ管理とユーザIDの埋め込みである．しかし，ユーザIDの埋め込み機能には，ID改竄の危険があり情報漏洩抑止効果が十分ではない．

3 結託攻撃と結託耐性符号

ユーザIDの埋め込み機能は，ユーザIDの存在を周知することで情報漏洩を抑止する．内部不正者はユーザIDの存在を知っているため，ユーザIDの改竄を試みると考えられる．電子透かしの埋込みを改竄する典型的な手法に結託攻撃 [2] がある．結託攻撃とは異なるIDが埋め込まれた同一内容の電子文書を複数用意し，その比較により検出された差分を改竄する手法である．本稿ではこのような比較を結託と呼ぶ．

結託攻撃に対処する方法として結託耐性符号がある．結託耐性符号は，一定数の結託による結託攻撃ならば，利用された符号を特定できる．結託耐性符号は符号化方式より，耐えうる結託数と表現できるID数が異なり，状況に応じて符号化方式を選択する必要がある．

結託耐性符号により，結託攻撃によるID改竄を困難にしたユーザID埋込み機能を実現できる．この機能により電子文書のユーザIDは結託攻撃されてもID情報を失わない．そのため情報漏洩にはユーザIDから情報漏洩者自身に容疑がかかるリスクが伴う (図1参照)．このリスクにより，提案システムのユーザIDの埋込み機能は高い情報漏洩抑止効果を得る．

The Design of a Document Management Systems to Specify the Source of the Information Leakage
† Masaki IMAI
†† Tetsutaro UEHARA
‡ Shuhui HOU
† Yu TSUDA
†† Hajime KITA
Graduate School of Informatics, Kyoto University (†)
Academic Center for Computing and Media Studies, Kyoto University (††)
Departemnt of Mathmatics and Mechanics, University of Science and Technology Beijing (‡)

‡‡ エヌ・アール・アイ・セキュアテクノロジーズ株式会社，SecureCubeLabeling, http://www.nri-secure.co.jp/service/cube/labeling.html

[1] 日立ソリューション，秘文，http://www.hitachi-solutions.co.jp/products/hibun/

Copyright ©2011 Information Processing Society of Japan.
All Rights Reserved.

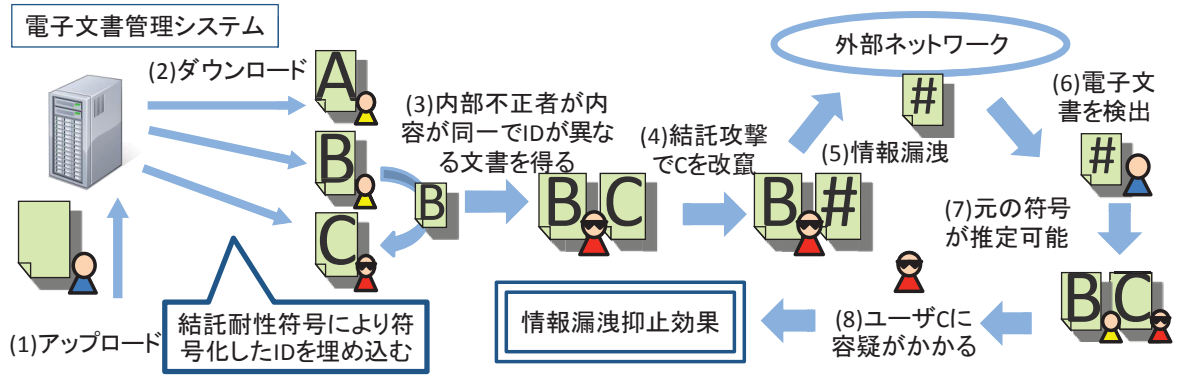

図 1: 結託耐性符号による情報漏洩抑止

4 結託耐性符号を用いた電子文書管理システム

本システムは組織内 LAN において OOXML 形式の電子文書を管理する．電子文書のダウンロード時に結託耐性符号で符号化したユーザ ID を電子透かしで埋め込む機能を備えており，この機能により情報漏洩を抑止する．以下ではこの機能において利用する結託耐性符号，電子透かし，また符号の改竄による影響について述べる．

想定する結託と結託耐性符号について述べる．自身が参照可能な電子文書を他の複数のユーザから取得するのは不自然であるため，本稿では 3〜4 個程度の少数の結託による結託攻撃を想定する．そこで本システムでは符号長に対して表現可能な ID 数が多い符号化方式を用いる．文献 [1] でそのような符号が提案されている．文献 [1] によると，10^3bit の符号により 10^4 個程度の ID が表現可能で，10 個程度の結託に耐えうる符号が生成できる．この符号を用いると数千人規模の組織に対応でき，大多数の企業に適用できる．

次に電子透かしについて述べる．電子透かしには，文章への影響が少ない空白文字の色情報を利用する手法 [5] を用いる．この手法は 1 空白文字あたり 24bit の埋込みが可能であり，文献 [5] の調査結果から，1 ページあたり 2665.5bit の埋込み容量が期待できる．この手法により 10^3bit の結託耐性符号を用いたシステムが構成可能である．

埋め込まれた符号は内部不正者の攻撃により改竄される危険性がある．想定される攻撃には，1) 埋込みをした空白文字を一部削除，2) 埋込みをした空白文字の色情報を一部改竄，3) 埋込みをした空白文字を全て削除または改竄，4) 結託攻撃，の 4 つがある 3) の場合，埋込みは消去されてしまう．4) は結託耐性符号により困難である．1)2) の場合は改変箇所を検出可能とすれば，元の符号を推定できる．結託耐性符号 [1] は特定のビットのうち 2bit により符号を特定できる．したがって最大で 998bit 改竄されても元の符号を特定できる可能性がある．本システムでは符号の複数回埋め込み，空白文字ごとのシーケンス番号の埋込みにより，改竄箇所を検出する．

5 おわりに

本稿では結託耐性符号で符号化したユーザ ID を文献 [5] の手法で埋め込む電子文書管理システムを提案した．今後はシステムを実装し，符号の埋め込み時間や，編集による電子透かしへの影響などについて評価していく予定である

参考文献

[1] HOU Shuhui. et.al. Fingerprinting codes for internet-based live pay-tv system using balanced incomplete block designs. *IEICE Transactions on Information and Systems*, Vol. 92, No. 5, pp. 876–887, 2009.

[2] 小松尚久ら. 電子透かし技術 ディジタルコンテンツのセキュリティ. 東京電機大学出版局, 2004-01.

[3] 滝澤 修ら. 改行位置の調整によるドキュメントへの情報ハイディング (情報セキュリティ特集) – (情報漏えい対策技術). 情報通信研究機構季報, Vol. 51, No. 1, pp. 153–169, 2005-03.

[4] 中川 裕志ら. 辞書変換法に基づく日本語テキストへの情報ハイディング. 情報処理学会論文誌, Vol. 41, No. 8, pp. 2272–2280, 2000-08.

[5] 北野 宗之ら. Word 2003 xml 文書への情報ハイディングシステム. 電子情報通信学会技術研究報告. ISEC, 情報セキュリティ, Vol. 105, No. 193, pp. 205–212, 2005-07.

Copyright ©2011 Information Processing Society of Japan.
All Rights Reserved.