Vol.2011-CSEC-53 No.4
Vol.2011-IOT-13 No.4
2011/5/12

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提案

今井正樹[†1] 上原哲太郎[†2] 侯書会[†3]
津田侑[†1] 喜多一[†2]

情報漏洩対策機能としてユーザを特定可能な ID を電子透かしで文書に埋め込む電子文書管理システムがある．情報漏洩発生時に文書の流出元特定を容易にすることで，情報漏洩を心理的に抑止する．しかし，従来の方式で ID を符号化した場合，異なる ID を持つ文書を比較することにより ID の改竄が可能である．そこで本稿では結託耐性符号で符号化したユーザ ID を文書に埋め込む電子文書管理システムを提案する．文書形式として最も広く利用されている OOXML（Office Open XML）形式の文書を対象として，相当量の情報が埋め込み可能な電子透かし手法を示し，ユーザ ID の消去を困難にした電子文書管理システムを設計する．

The Proposal of a Document Management System to Specify the Source of Information Leakages

Masaki Imai,[†1] Tetsutaro Uehara,[†2] Shuhui Hou,[†3]
Yu Tsuda[†1] and Hajime Kita[†2]

There is a document management system witch prevent information leakages by embeding user identification in documents with digital watermark. It prevent users from information leakages by facilitating specification of the leakage source. But A comparation of same documents witch embeded different user IDs is enabled to attackeres to falsify the ID. This paper propose the document management system witch embeding user ID encoreded with anti-collusion codes in documents. This system targeted OOXML (Office Open XML) documets because it is the most widely used in the world. This paper introduce the new large capacity watermark available in OOXML, and design the document management system enhaced preventation effect on information leakages.

1. はじめに

企業などの組織が扱う情報資産の中で，文書は未だ大きな地位を占めており，文書の流通管理が問題となっている．文書の流通を管理する方法の一つとして電子文書管理システムがある．電子文書管理システムは一般的にアクセス制御機能を備えており，不正アクセスなどによる情報漏洩を防止できる．しかし，アクセス制御などの文書の流通を制御する機能では，正当なアクセス権を持つ者の情報漏洩を防止できない．このような者の情報漏洩では，情報漏洩の心理的抑止を可能とする機能が重要となる．

正当なアクセス権を持つ者に対する情報漏洩を抑止する機能としてログ管理がある．ログ管理機能は文書に対するユーザのアクセス日時や操作内容を記録し，情報漏洩経路の特定を容易にする．一方で管理外の PC などの環境では，文書に関するログ取得困難であるため，こうした環境で情報漏洩の抑止を可能とする機能が必要となる．そのような機能の一つとしてユーザ ID 埋め込みが提案されている．この機能はユーザを特定可能な ID（以下，ユーザ ID）を電子透かしで文書に埋め込み，情報漏洩発生時に漏洩した文書のユーザ ID から情報漏洩元の特定が容易であるという原理によって，情報漏洩を心理的に抑止する．しかし，従来の方法では文書に埋め込まれたユーザ ID を結託攻撃[1)] と呼ばれる手法によって改竄される危険性がある．

そこで本稿では，文書形式として最も広く用いられている OOXML（Office Open XML）を対象とし，結託耐性符号[2)] を用いて符号化したユーザ ID（以下，**耐結託 ID**）を埋め込む機能を備えた電子文書管理システムを提案する．本提案により，結託攻撃されたユーザ ID から結託したユーザ ID が特定可能となり，電子文書管理システムの情報漏洩に対する抑止効果が高まる．

2. 関連研究

2.1 電子文書管理システム

電子文書管理システムは，文書に作成日時などのメタデータを付与することで文書の検索

†1 京都大学 大学院情報学研究科
Graduate School of Informatics,Kyoto University
†2 京都大学 学術情報メディアセンター
Academic Center for Computing and Media Studies,Kyoto University
†3 北京科技大 数力学系
Departemnt of Mathmatics and Mechanics,University of Science and Technology Beijing

Vol.2011-CSEC-53 No.4
Vol.2011-IOT-13 No.4
2011/5/12

やアクセス制御などを可能とする．電子文書管理システムの情報漏洩対策機能には，データの暗号化，ログ管理，ユーザ ID 埋め込みなどがある．

秘文[*1]は文書データの暗号化やログ管理，印刷文書に対して電子透かしでユーザ情報を埋め込むなどの機能を持つ．データの暗号化機能はメールの誤送信や PC の盗難など，過失による情報漏洩が発生した際に，正当なユーザ以外の文書閲覧を困難にする．ログ管理機能はユーザの文書への操作履歴をサーバで一元的に管理し，セキュリティポリシにそぐわない不正な操作の検出や文書流通の明確化が可能であることから，情報漏洩発生時の漏洩文書の流出経路特定を容易にする．印刷文書へユーザ情報を埋め込む機能は，文書自体に印刷者の情報を埋め込むことで，ログの取得やデータの暗号化で対策が難しい紙媒体による情報漏洩の抑止を可能としている．

InfoCage[*2]は文書データの暗号化，ログ管理の他に文書に対して電子透かしでユーザ ID を埋め込む機能などを持つ．文書に対して電子透かしでユーザ ID を埋め込む機能は，文書自体に文書取得者の情報を埋め込むことで，管理外 PC などのログが取得できない環境における情報漏洩抑止を可能としている．

文書に対して正当なアクセス権を持つ者による情報漏洩はデータの暗号化では防止できない．したがってログ管理やユーザ ID 埋め込みといった機能による情報漏洩抑止が重要となる．しかし，情報漏洩抑止機能は情報漏洩を発生させないものではないため，機能を複数組み合わせ，情報漏洩のリスクを可能なかぎり軽減する必要がある．

2.2 OOXML で利用可能な電子透かし

結託耐性符号は Marking Assumption[2] という前提のもとに成り立っている．Marking Assumption とは，異なる符号を埋め込まれた文書を比較した場合に，データの異なる部分しか改竄できないという仮定であり，電子透かしを用いて埋め込んだデータは符号の最小要素ごとに比較できる必要がある．OOXML 文書で利用可能な電子透かしで，Marking Assumption が成立する手法として，改行を利用する手法[3]，同義語を置換する手法[4]，空白文字を利用する手法[5] などが提案されている．

改行を利用する手法は，文章の改行位置を調整し，改行時の文字数などを利用して情報を埋め込む．この手法はプレーンテキストでも利用可能という点で汎用性が高いが，改行位置が不自然になるという欠点がある．同義語を置換する手法は，文章中の単語を同義語と置換

*1 http://hitachisoft.jp/products/hibun/（参照日付 4 月 5 日）
*2 http://www.nec.co.jp/cced/infocage/index.html（参照日付 4 月 5 日）

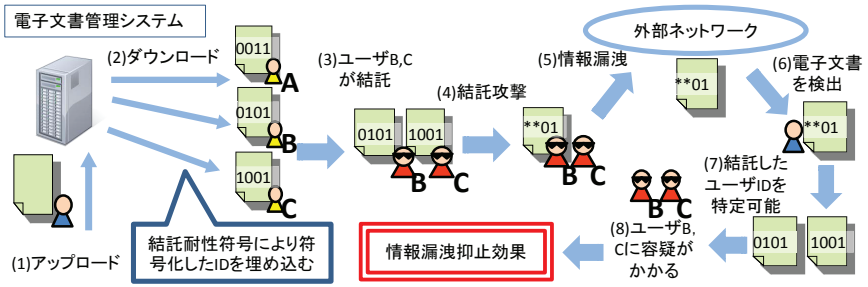

図 1 結託耐性符号による情報漏洩抑止
Fig. 1 Preventation of an information leakage using anti-collusion codes

により情報を埋め込む．この手法は文章との不可分性が高いが，文章の意味が変化する危険性がある．空白文字を利用する手法は，OOXML 文書を対象としており，空白文字の色属性の値が文章に影響を与えないことを利用する．この手法は文書に全く変化を与えないという点で優れている．

これらの手法はいずれも文書の文字数に依存して埋め込み容量が変化するため，文書の文字数によらず常に一定の埋め込み容量が必要であるユーザ ID 埋め込み機能には適さない．

3. 結託攻撃と結託耐性符号

本章では一般的に考えられている結託耐性符号の情報漏洩抑止効果が，ユーザ ID 埋め込み機能で発揮される過程と，ユーザ ID 埋め込み機能に適した結託耐性符号の符号化方式について述べる．

3.1 結託耐性符号による情報漏洩抑止効果の向上

ユーザ ID 埋め込み機能は，文書にユーザ ID が埋め込まれていることを事前にユーザに周知することで情報漏洩を抑止する．したがって，正当なアクセス権を持つユーザは情報漏洩時に文書のユーザ ID 改竄を試みると考えられる．

電子透かしに対する典型的な攻撃手法に結託攻撃がある．結託攻撃とは，内容が同一で異なる ID が埋め込まれた文書を比較し，データの異なる部分のみを改竄する手法である．既存のユーザ ID 埋め込み機能により電子透かしで文書に埋め込まれたユーザ ID は，結託攻撃により改竄される危険性がある．

結託攻撃に対処する方法として結託耐性符号[2] がある．結託耐性符号はある条件の下で，結

Vol.2011-CSEC-53 No.4
Vol.2011-IOT-13 No.4
2011/5/12

表 1 結託耐性符号の性能
Table 1 The parameter of anti-collusion codes

符号長（bit）	表現可能な ID 数	耐結託数
p^3+1	$p^2(p^2-p+1)$	$p+1$

p は素数を表す

託攻撃によって改竄された符号から結託した符号を特定できる．このある条件とは，Marking Assumption が成立しており，結託攻撃が一定の結託数以下であることである．本稿ではこの一定の結託数を**耐結託数**と呼ぶ．

耐結託 ID を用いることで，ユーザ ID 埋め込み機能の情報漏洩抑止効果を向上できる．**図 1** は電子文書管理システムからダウンロードした文書に耐結託 ID が埋め込まれることで，情報漏洩抑止効果が高まる様子を示している．

図 1(1)(2) のように電子文書管理システムにアップロードされた文書をユーザ A，B，C がダウンロードすると，ユーザが持つ文書には，ユーザ ID 埋め込み機能によりそれぞれ異なる耐結託 ID が電子透かしで埋め込まれる．このとき悪意のあるユーザ B，C が結託攻撃すると，図 1(3)(4) のように文書の耐結託 ID が改竄され，文書をダウンロードしたユーザが不明確になる．するとユーザ B，C は図 1(5) のように改竄した文書をネットワーク上に漏洩する可能性がある．

しかし，漏洩文書がネットワーク上からシステム管理者に検出されると，図 1(6)(7) のようにシステム管理者は結託耐性符号の特徴を利用して，改竄前の符号を特定できる．そのため，図 1(8) のようにユーザ B，C には漏洩文書から得られた耐結託 ID により，情報漏洩の容疑がかかる．このような原理から，ユーザ ID が耐結託 ID であることを事前にユーザに周知しておくことで結託攻撃を抑止できる．

3.2 耐結託 ID 埋め込み機能に適した符号化方式

結託耐性符号は表現可能な ID 数と耐結託数により符号長が異なるため，符号利用時には，想定される結託攻撃の結託数と必要な ID 数に応じて符号長を決定する必要がある．しかし，結託耐性符号は符号化方式が異なると，同一の符号長であっても耐結託数と表現可能な ID 数が異なるため，耐結託 ID 埋め込み機能に適した結託耐性符号の符号化方式を定める必要がある．

企業などの組織に属する従業員数は，規模の大きな組織では数十万人になる[⋆1]．一方で情報漏洩には社会的なリスクが伴うため，多くの者による結託攻撃は考えにくい．したがって耐結託 ID 埋め込み機能で用いる符号化方式は，符号長あたりの表現可能な ID 数が大きな方式が適している．そのような符号化方式が Hou らにより提案されている[6]．Hou らの方式は ACC と呼ばれる符号[7] を改良した符号である．ACC で Marking Assumption が成立するには，電子透かしで埋め込んだデータが ACC の最小単位である 0，1 ごとで比較が可能である必要がある．Hou らは 2 つの符号化方式を提案しており[6]，本稿ではより表現可能な ID 数の大きい unital code を用いた方式を利用する．ACC における unital code を用いた符号長，表現可能な ID 数，耐結託数の関係は**表 1** のようになる．

表 1 より，10^5 人分の ID 数を表現する場合，6×10^3bit 程度の符号長が必要であり，結託耐性符号を埋め込む電子透かしは 6×10^3bit 以上の情報を埋め込める必要がある．

4. 耐結託 ID を埋め込む電子透かし手法

耐結託 ID は組織によっては 6×10^3bit 以上となることが想定される．耐結託 ID 埋め込み機能では，どのような文書にもこの bit 数を埋め込み可能である必要がある．しかし，2 章で述べたような OOXML 文書で Marking Assumption が成立する既存の電子透かしは，文字数に依存して埋め込み容量が決定するため，文字数の少ない文書では耐結託 ID を埋め込むことができない．本章では，OOXML 文書で Marking Assumption が成立し，かつ文書の文字数によらない電子透かし手法を提案する．

4.1 テキストボックスを利用した電子透かし

OOXML は Microsoft Office 2007 以降が利用しているファイル形式であり，複数の XML ファイルで構成される（**表 2** 参照）．OOXML 文書にはテキストボックスとフィールドという機能がある．テキストボックスは図形に文章を挿入する機能であり，Microsoft Office Word 2007（以下 ，Word 2007）においてテキストボックスと呼ばれるテキスト入力可能なオブジェクトはこの機能を用いている．フィールドは動的な文章を記述可能とする機能であり，例えばフィールドの種別に DATE という値を書き込むことで，実際の日付を表示できる．

本手法は Word 2007 のページ外に配置したテキストボックスにフィールドを挿入し，フィールドの種別を記述する要素内に情報を埋め込む．この手法は 2 進数の文字列で符号

⋆1 日本の大企業として知られるトヨタ，パナソニック，日立は３０万人規模の従業員数を持つ．
http://www.toyota.co.jp/jpn/company/about_toyota/outline/index.html（参照日付４月５日），
http://panasonic.co.jp/company/info/about/(参照日付４月５日),
http://www.hitachi.co.jp/about/corporate/index.html（参照日付４月５日）

Vol.2011-CSEC-53 No.4
Vol.2011-IOT-13 No.4
2011/5/12

表 2 OOXML 文書を構成する XML ファイル
Table 2 XML files compose OOXML documents

ファイル名とパス
[Content_Types].xml
docProps/app.xml
docProps/core.xml
customXml/item1.xml
customXml/itemProps1.xml
customXml/rels/item1.xml.rels
word/document.xml
word/fontTable.xml
word/settings.xml
word/styles.xml
word/webSettings.xml
word/document.xml
word/theme/theme1.xml
word/_rels/document.xml.rels
_rels/.rels

```
<w:document>
  <w:body>
    <w:p>
      <w:r>
        <w:t>文章</w:t>
      </w:r>
    </w:p>
    ...
    <w:p>
      <w:r>
        <w:t>文章</w:t>
      </w:r>
    </w:p>
  </w:body>
</w:document>
```

図 2 document.xml の XML コード
Fig. 2 A XML source code of a document.xml

を埋め込むことで Marking Assumption が成立する．表 2 で示した `document.xml` は文章と文字のフォントなどを記したファイルであり，本手法ではこのファイルに情報を埋め込む．`document.xml` は**図 2** のような構造を持つ．`<w:document>`要素を root 要素として，`<w:body>`要素に文書の内容を記す．`<w:p>`は文章の段落を表し，`<w:r>`は文を表す要素であり，実際の文字は`<w:t>`要素内に書き込む．

テキストボックスは`<w:r>`の子要素であり，**図 3** のような構造を持つ．`<v:shape>`は図形を表す要素である．`<v:shape>`要素の style 属性は図形の形などを設定する属性で，style 属性の値でテキストボックスの位置が決まる．本手法では横方向の位置を示す値を，テキストボックスがページ左側外になるように設定する．図 3 のようにテキストボックスは子要素に`<w:r>`を持つ．フィールドは`<w:r>`要素の子要素として**図 4** に示す要素を宣言することで表現できる．フィールドはフィールドの種別を記述する`<w:instrText>`要素内に無意味な文字を挿入し，`<w:t>`要素を宣言しないでおくと，Word 2007 の画面に表示されないという特徴がある．そこで図 4 の`<w:instrText>`要素内に情報を埋め込み，`<w:t>`要素を消去したフィールドをテキストボックスの`<w:r>`要素に挿入する．また，テキストボックスの

```
<w:pict>
  <v:shape id=" … " style=" … " >
   <v:textbox >
    <w:txbxContent>
     <w:p>
      <w:r>
      ...
      </w:r>
     </w:p>
    </w:txbxContent>
   </v:textbox>
  </v:shape>
</w:pict>
```

図 3 テキストボックスの XML コード
Fig. 3 A XML source code of a textbox

```
<w:fldChar w:fldCharType="begin" />
<w:instrText>DATE</w:instrText>
<w:fldChar w:fldCharType="separate"/>
<w:t>5/12/2011</w:t>
<w:fldChar w:fldCharType="end" />
```

図 4 フィールドの XML コード
Fig. 4 A XML source code of a field

`<v:shape>`要素の id 属性は任意の値を利用可能で，情報の埋め込みができる．

フィールドの`<w:instrText>`要素内は文字数に制限がないため相当量の埋め込みが可能であると考えられる．しかし，フィールドは Word 2007 でフィールド選択中に右クリックした場合の表示が，文章のみを選択した場合の表示と異なる．そのため本文にフィールドを埋め込むとユーザが容易に発見可能である．一方ページ外に配置したテキストボックスは Word 2007 のクリックで選択できない，画面に表示されないという特徴を持ち，Word 2007 を利用した発見が困難である．テキストボックスには文字列での情報の埋め込み可能であるが，この方法ではテキストボックスが発見された場合に，埋め込んだ情報が容易に改竄される危険性がある．そこで本手法は文字が画面に表示されないフィールドに情報を埋め込むことで情報が改竄される危険性を軽減する．テキストボックスにはテキストボックスが書き込まれている行が選択されていれば，Word 2007 を利用した OOXML 文書から OOXML 文書への文章コピーで同時にコピーされる性質があり，本手法はコピーされた文書の流出元特定にも利用出来る可能性がある．

4.2 テキストボックスを利用した電子透かし消去の可能性

本手法で埋め込んだ情報は，Word 2007 を利用したテキストボックスの削除や OOXML を直接編集することにより消去される危険性がある．Word 2007 を利用してテキストボックスを削除するには，テキストボックスを選択，またはテキストボックスが書き込まれた行をドラッグで選択して削除する方法が考えられる．テキストボックスを選択する方法には

Vol.2011-CSEC-53 No.4
Vol.2011-IOT-13 No.4
2011/5/12

Web レイアウト表示などでページ幅を広げる，ウィンドウ外までをドラッグで選択するなど選択範囲を広げる方法と他の図形選択中に Tab キーで選択する方法が考えられる．

選択範囲を広げる方法に対してはテキストボックスをページから十分遠くに配置することで困難にできる．Web レイアウト表示ではページ右側の幅のみが拡大するため，本手法ではテキストボックスをページ左側に配置する．Tab キーで選択する方法については防ぐ方法はないが，編集に必ずしも必要な操作でないため，Tab キーによってテキストボックスが選択され，削除される危険性は低いと考えられる．テキストボックスが書き込まれた行をドラッグで選択する方法については確実な対策が難しい．文章に埋め込んだ情報が完全に削除されないためには，文章中に複数のテキストボックスを埋め込むなどして対策する必要がある．

OOXML を直接編集してテキストボックスに埋め込まれた情報を削除するには，複数の XML ファイルから `document.xml` に情報が埋め込まれていることを特定し，フィールドの `<w:instrText>` 要素内の情報を削除する必要がある．しかし，編集によっては OOXML 文書が Word 2007 で表示不可能となるため，OOXML に関する知識を持たないユーザにはこうした編集が困難であると考えられる．

4.3 Custom XML

OOXML には Custom XML という文書内に任意の文字列を格納しておく機能がある．Custom XML は表 2 で示した customXml ディレクトリ以下のファイルから成り立っており，`item1.xml` 内に自由に要素を宣言し，任意の文字列を埋め込むことができる．

Custom XML に埋め込んだ文字列は Word 2007 からの編集が困難であり，仕様上埋め込み容量も制限がない．また，符号を 2 進数の文字列で埋め込むことで Marking Assumption が成立する．しかし，customXml ディレクトリは OOXML 文書を構成するために必ずしも必要な要素ではなく，削除することによって文書が判読不可能となる可能性がないため，OOXML を直接編集する場合は容易に削除できる．

4.4 提案手法の埋め込み容量に関する検証

提案した 2 つの手法を適用した文書に半角で 10^5 字を埋め込み，企業などで利用する際に十分大きな ID 数を表現可能な結託耐性符号が埋め込み可能であるかを検証した．テキストボックスを利用した電子透かしを適用した文書は，半角で 10^5 字を埋め込んだ状態でも，Word 2007 で表示可能で，保存も可能であった．Custom XML を適用した文書も半角で 10^5 字を埋め込んだ状態で，Word 2007 で表示可能で，保存も可能であった．テキストボックスの `<v:shape>` 要素の id 属性についても情報を埋め込んだ文書を作成し，埋め込み容量を調査した．半角で 10^5 字を埋め込んだ場合，Word 2007 では表示可能であったが保存が不可能であった．しかし，半角で 254 字までは，Word 2007 で表示保存が可能であった．

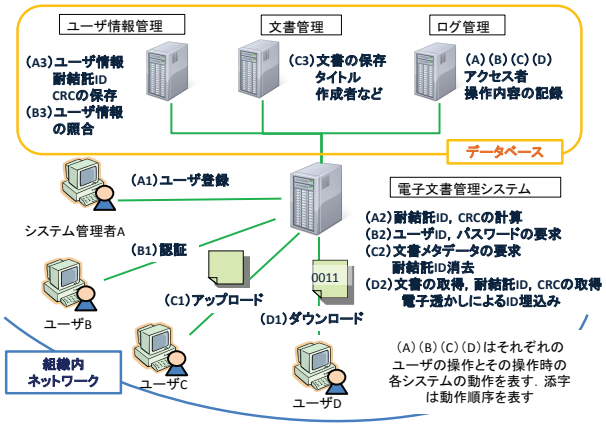

図 5 システムのイメージ
Fig. 5 An image fo the system

以上の検証より，テキストボックスを利用した手法，Custom XML を利用した手法は共に耐結託 ID 埋め込み機能に十分な埋込み容量を持ち，テキストボックスは `<v:shape>` 要素の id 属性にも，半角で 254 字の埋込みが可能である事がわかった．

5. 結託耐性符号を利用した電子文書管理システム

5.1 システムの概要

本システムは企業などの組織に属する者が組織内ネットワークから PC などの端末を用いて利用することを想定した Web アプリケーションであり，データベースを用いて OOXML 形式の文書を管理する．本システムは文書のアップロードやダウンロード，削除，検索の機能を持つ．情報漏洩対策として，ログ管理機能と耐結託 ID 埋め込み機能を備え，認証機能によりアクセス制御をする．

図 5 を用いてシステムの動作を説明する．システム利用時にはまず図 5(A1) のようにユーザ登録をする．このときシステムの効率化を図るため図 5(A2) のように，ユーザ ID から耐結託 ID とその CRC32 を計算し，図 5(A3) のようにデータベースに保存しておく．ユーザ登録されたユーザは図 5(B1) のように認証することでシステムを利用出来る．認証ではユーザ ID とパスワードを利用し，図 5(B2)(B3) のようにしてアクセス者が正当なユーザであ

Vol.2011-CSEC-53 No.4
Vol.2011-IOT-13 No.4
2011/5/12

ること確認する．認証されたユーザは図 5(C1)(D1) のように文書のアップロードやダウンロードが可能となる．アップロードでは図 5(C2)(C3) のように必要に応じてタイトルや作成者など文書メタデータの入力，耐結託 ID の消去などをして文書を保存する．ダウンロードではシステムは図 5(D2) のように要求された文書とユーザの耐結託 ID とその CRC32 を取得し，耐結託 ID 埋め込み機能を用いて文書に埋め込み，ユーザに文書を渡す．ログ管理機能は図 5 のように，システムに対するユーザの操作を記録する．

5.2 耐結託 ID 埋め込み機能

テキストボックスを利用した電子透かしと CustomXML を合わせて利用することにより，Word 2007 のユーザインターフェースのみではユーザ ID の完全な消去困難で，OOXML を直接編集した場合でも，OOXML に関する知識がなくては耐結託 ID の消去が困難，かつ，Word 2007 のユーザインターフェースを用いた文書のコピーで耐結託 ID が同時にコピーされやすいような耐結託 ID の埋め込みを実現する．

耐結託 ID はシステムのエラーやユーザの編集などにより，ランダムに改変される危険性があるため，文書には CRC32 を用いて計算した耐結託 ID の改竄検出情報を合わせて埋め込む．テキストボックスを利用した電子透かしによる符号の埋め込み手法について述べる．表 1 より，表現可能な ID 数が 10^6 個である符号であっても符号長は 3.2×10^4bit 程度である．したがって，テキストボックスを利用した電子透かしでは，大規模な組織で利用可能な ID 数を持つ符号長の大きい結託耐性符号でも，1 つのテキストボックスに埋め込み可能である．そこで本システムでは耐結託 ID と耐結託 ID の CRC32 を一つのテキストボックスに埋め込む CRC32 は 16 進数で表現し，テキストボックスの<v:shape>要素の id 属性に対して埋め込む．耐結託 ID と CRC32 を別々にすることでユーザが直接 OOXML を編集した場合に CRC32 が耐結託 ID と共に削除される危険性を下げる．耐結託 ID は 2 進数で文書に埋め込むことで Marking Assumption を成立させる．

テキストボックスを複数埋め込むことで，情報を完全に削除される危険性を抑え，コピーされた文書を追跡できる可能性を向上できる．しかし，利用するテキストボックス数を増加させると，ユーザ ID 埋め込み機能の実行時間が増加し，システムの利便性を損なうため，本システムでは 1 ページに最大 3 つのテキストボックスを埋め込む．埋め込む箇所はページの最初の<w:p>要素と最後の<w:p>要素そしてその中間の<w:p>要素である．<w:p>要素は OOXML で段落を表す要素である．<w:p>要素が 3 つ以下の場合には，1 つの<w:p>要素に 1 つのテキストボックスを埋め込む．

Custom XML では表 2 で示した customXml ディレクトリのファイルを作成し，item1.xml に耐結託 ID と CRC をあわせて埋め込む．テキストボックスを利用した電子透かしの場合と同様に耐結託 ID は 2 進数，CRC32 は 16 進数で埋め込む．

6. おわりに

本稿では，結託耐性符号を利用することで情報漏洩抑止効果を高めた電子文書管理システムが実現可能であることを示した．結託耐性符号は符号長が長く，文字数に依存して埋め込み容量が変化する既存の電子透かしでは文字数の少ない文書に対して符号を埋め込めない可能性が高かった．本稿では OOXML 形式の文書を対象としてテキストボックスを利用した電子透かしと Custom XML を利用し，規模の大きな組織でも利用可能であり，耐結託 ID が OOXML に関する知識がなくては削除が困難で，Word 2007 を利用した文書のコピーにより耐結託 ID がコピーされやすい耐結託 ID 埋め込み機能を設計した．

今後はシステムを実装し，小規模な組織での運用を通して，耐結託 ID の埋め込み時間やテキストボックスを利用した電子透かしのユーザの編集に対する強度，耐結託 ID を埋め込んだ文書を結託攻撃した場合の結託したユーザ ID の検出精度などについて調査し，大規模な組織におけるシステムの実現可能性を評価する予定である．

参 考 文 献

1) 小松尚久，田中賢一：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).
2) Boneh, D.: Collusion-secure fingerprinting for digital data, *IEEE Trans. Information Theory*, Vol.44, No.5, pp.1897 –1905 (1998).
3) 滝澤　修，松本　勉，中川裕志：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).
4) 中川裕志，木村浩康，三瓶光司，松本　勉：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).
5) 北野宗之，増田英孝，中川裕志：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).
6) Hou, S., Uehara, T., Satoh, T., Morimura, Y. and Minoh, M.: 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).
7) Trappe, W.: Anti-collusion fingerprinting for multimedia, *IEEE Trans. Signal Processing*, Vol.51, pp.1069–1087 (2003).