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

2007－DPS－130 (5)
2007－CSEC－ 36 (5)
2007／3／1

開示情報の正当性を保障するE-Discoveryシステムの提案

高塚 光幸† 向井 剛平† 多田 真崇† 佐々木 良一‡

†,‡東京電機大学工学部 〒101-8457 東京都千代田区神田錦町 2-2

E-mail: †{takatsuka, mukai, tada}@isl.im.dendai.ac.jp, ‡sasaki@im.dendai.ac.jp

あらまし 近年，インターネットや情報技術の発達に伴ってあらゆる情報が電子化されてきている．情報の電子化に伴い，デジタルデータの証拠性を確保するデジタル・フォレンジック技術が重要になってきている．さらに近年，デジタル・フォレンジック技術において電子開示手続きであるE-Discovery技術が重要になってきている．今後は文書の証拠性を確保するだけでなく，情報を適切に開示することが必要になってくると考えられている．そこで，本稿では蓄積されている文書の証拠性と開示文書の正当性を保障するE-Discoveryシステムの提案を行う．

キーワード 電子証拠，E-Discovery，Forensics，ヒステリシス署名，墨塗り

Proposal of E-Discovery System to Guarantee Integrity of Disclosed Information

Mitsuyuki TAKATSUKA† Kouhei MUKAI† Masataka Tada† and Ryoichi SASAKI‡

†,‡School of Engineering, Tokyo Denki University 2-2 Kandanishikicho, Chiyoda-ku, Tokyo,101-8457 Japan

E-mail: †{takatsuka, mukai, tada}@isl.im.dendai.ac.jp, ‡sasaki@im.dendai.ac.jp

Abstract Recently, almost all information has been computerized with development of Internet and an information technology. With computerization of information, digital forensics technique for getting evidence of digital data becomes important. Especially, E-Discovery technique to obtain an electronic disclosure procedure, which is one of the digital forensics techniques, becomes important. In future, the method not only to get evidence of a document but to guarantee the integrity of disclosed information. Thus we propose an E-Discovery system guaranteeing evidence and legitimacy of a disclosure document of an accumulated document with this report.

Keyword E-Discovery, Forensics, Hysteresis Signature, Sanitizing

1. はじめに

近年，インターネットや情報技術の発達に伴ってあらゆる情報が電子化されてきている．情報が電子化されることによって，企業等は保管場所，配信，複製や再利用などのコスト削減のメリットを享受できる．

しかしながら，あらゆる情報が電子化されたことにより，ウイルス被害や不正アクセス等の外部からの被害が増加してきている．また，組織内部からの情報漏洩事件も多発してきている．文献[1]では組織における情報漏洩の対象となり得る情報を以下の４つに大きく分類している．

① 経営情報
② 知的財産情報
③ 個人情報
④ ＮＤＡに基づいた情報

これらの情報が漏洩した場合，情報①，②は企業に対して直接的に経済的損害等を発生させうる．これに加えて情報③，④では契約相手先や顧客を中心とするユーザに対して損害を与えると同時に，信頼を損なうおそれを有している．特に情報③については個人情報保護法に代表されるように，法的な義務により組織における責任は社会的，法的な責任を有するおそれがあり，企業における責任が大きく問われてきている．

企業における責任の拡大と供に，デジタルデータの証拠性を確保し，訴訟などに備えるための技術や社会的仕組みが要求されるようになり，近年，デジタル・フォレンジック（Digital Forensics ： 以下ＤＦと略す.）が重要になってきている[2][3].

1. 1. ＤＦの新たな方向性

組織においてはＤＦを導入することにより，問題が発生した際に，証拠性を確保することによって

① 訴訟対策

② トラブル発生時の関係者への状況説明，原因究明，再発防止

といったメリットを得られることから，近年，ＤＦを導入する傾向にある.

しかしながら，ＤＦの分野において証拠性の確保だけには留まらず，適切な情報開示が必要とされてきている．例えば，民事訴訟において，情報の開示を求められた際には，適切に情報を開示できる必要がある．適切に情報が開示出来なければ，

（問題１）裁判で不利な状況になる

（問題２）蓄積された情報を必要以上に開示しなければならなくなる

以上のような問題を有している.

文献[4]では，近年，情報を適切に開示するために，訴訟や会計監査で必要とされる電子書類を迅速に用意して提出するために，企業内において電子文書を安全に保管し，必要な時に適切に，かつ迅速に探し出すE-Discoveryが拡大していくことを予測している.

2. E-Discovery

E-Discoveryとは Electronic-Discoveryの略称であり，日本語では電子開示と訳されている．しかし，本来はe-Discoveryとは，アメリカにおけるデジタルデータの開示手続きであり，アメリカでは広く使われる技術である．しかしながら，アメリカに進出した日本企業，自社製品がアメリカで販売され，使用されていて，何らかの問題を起こした場合には，日本の企業が巻き込まれる恐れがある．この際，アメリカの企業が原告側となった場合には，アメリカの法に基づいた訴訟が行われる．その為，ここではアメリカの訴訟手続きについて簡単に説明する.

アメリカにおける民事訴訟手続きの基本的流れを図１に示す．図１の④ディスカバリーが情報の開示手続きである．ここで，日本とアメリカにおける訴訟制度の大きな違いがある．日本では審理がされ，また新たな証拠提出があり審理というように，図１の④のディスカバリーと図１の⑤の審理を繰り返すが，アメリカの訴訟では審理前と審理後に明確な区別があり，審理の争点を確認するのであって，新たな証拠提出はない.

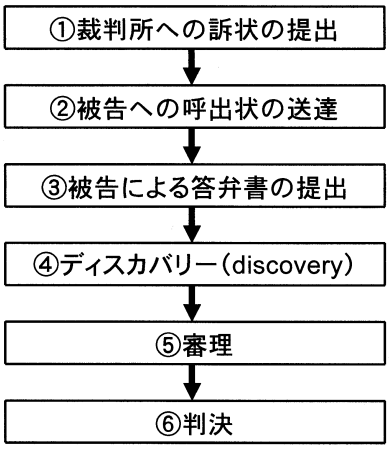

図１　アメリカの訴訟手続きの流れ

つまり，アメリカの民事訴訟制度に巻き込まれた場合には，図１の④ディスカバリーの際に証拠提出が行えない場合，証拠が不十分で敗訴し，必要以上に情報を開示しなければならなくなる可能性がある．そこで，不必要に情報を開示しないようにする為には，企業が訴訟対策を行っておく必要がある.

また，アメリカでの書類提出要求の特徴として，

① 書類の範囲が広い

② 証拠とは無関係という主張は困難

③ 機密文書も対象

④ 慌てて書類を整理・破棄等できない

以上のように，証拠とは無関係という主張が困難であり，機密文書も対象となるため，１節で示した経営情報や個人情報も書類提出の内容に含まれてしまう.

2. 1. 訴訟対策の必要性

企業において訴訟対策を行っていない場合には，電子データの特徴として改ざんや消去を容易に行うことが出来てしまう為に，蓄積している電子文書は証拠として成り立たずに裁判に敗れてしまう危険性がある．その為，証拠として成り立たせるために，被告側が不正に改ざんや消去を行っていないことを証明できることが必要となってくる.

また，必要以上に情報を開示しなくてはなった場合，電子文書の情報には，機密情報や経営情報，個人情報といった重要な情報も含まれている可能性があり，損害となる．このように企業が蓄積している文書を開示

する際には，重要な情報に対して秘匿を行うことができるシステムが必要となる．

3. 提案システム

本節では，訴訟時における開示情報の正当性を保障しつつ，情報を部分的に秘匿可能な E-Discovery システムの提案を行う．

3.1. E-Discovery システムの要件

３節に示した開示情報の正当性を保障しつつ，情報を部分的に秘匿可能な E-Discovery システムを実現する為には，以下のことが証明可能でなければならない．

① たとえ，文書の作成者であっても不正に改ざん，消去を行っていないこと．
② 情報を部分的に秘匿されたとしても，秘匿部分以外に，改ざんがされていないこと．
③ 開示要求における関連文書は全て開示がされていること．

①，②が証明出来ない場合，証拠として成り立たない．③が証明出来ない場合は，開示側にとって都合の悪い文書を隠し持っている可能性が拭いきれない．以上のことから，本提案システムの要件として以下の３つにまとめられる．

（要件１）文書が不正に改ざん・消去されていない
（要件２）情報が部分的に秘匿可能
（要件３）関連文書は全て開示されている

本稿では，以上の３つの要件を満たすシステムの提案を行う．

3.1.1. 要件１及び要件２へのアプローチ

要件１を満たす技術としては，文書の改ざんと本人性を確認できる電子署名技術が有効である．しかし，電子署名技術はいかなる改変も改ざんとみなされてしまうために，プライバシー情報を保護するための秘匿であっても改ざんとみなされてしまう．結果として，従来の電子署名技術では“開示された文書の真正性の保証”と“プライバシー情報の保護”，言い換えれば要件１と要件２が両立できず，どちらかを諦めざるをえない．このような問題を解決し，部分的に秘匿を行っても開示された電子文書の正当性を確認できる技術が電子文書墨塗り技術[5]やＣＥＳ[6]である．

3.1.2. 要件３へのアプローチ

要件３については，現行の日本の裁判において，関連する全ての文書が開示されているかどうかを確認する方法として，原告側の指定するキーワード群が含まれる文書がないかを確認する方法が取られている．そこで，電子文書でも，蓄積されている文書群に対して原告側の指定するキーワードが含まれた文書の有無を確認することにより，既に開示した文書以外に指定されたキーワード群を含む文書がないことを証明することができれば，関連文書は全て開示されていることが証明可能であると考えた．

また，電子文書に対してキーワードの検索をかける上で，従業員が使用するクライアントのコンピュータに蓄積されている電子文書に検索をかける場合には，クライアントのコンピュータ全てに対して検索をかけなくてはならなくなる．そこで，著者らは，シンクライアントの考え方で，電子文書をクライアントのコンピュータではなく，ファイルサーバを設置しファイルサーバに保管することにより，保管されている電子文書に対して効率良く，キーワードの検索をかけられるのではないかと考えた．

3.2. 適用性の検討

要件を満たす為に，文献[5]の SUMI-4 を適用し，ファイルサーバを設置すると，図２のようになる．

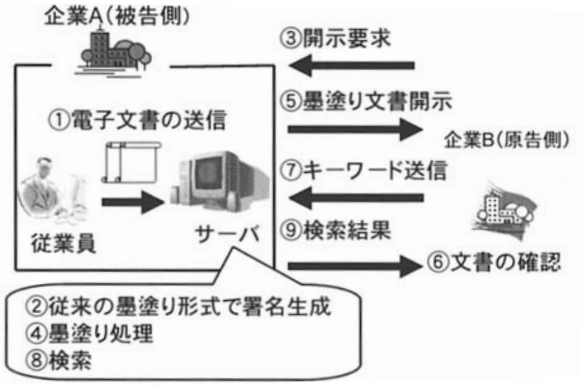

図２ 要件技術の試適用

3.2.1. 提案システムへの適用における問題点

図２に示すように，ファイルサーバに文書を蓄積する際に，開示要求があった際に従来の墨塗りの署名を施し，開示する際に部分的に秘匿が可能だったとしても，以下の問題が発生する．

（問題１）ファイルサーバから文書が削除されている可能性があり，必要なファイルが全て開示されていることは証明出来ない．
（問題２）開示前に署名を破棄し，新たに署名生成を行って開示された可能性があり証拠として不十分となる可能性がある．

（問題３）開示文書に原告側の指定するキーワードが含まれている可能性がある．

問題１は，ファイルサーバに電子文書を保管したとしても，システムの管理者であれば容易にファイルサーバに保管されている電子文書を改ざん・削除することが可能であることが原因である．従って，例え文書の作成者であったとしても改ざんや削除を行えないようにすることが必要である．

3.2.2. ヒステリシス署名

そこで著者らは，問題１を解決する方法として，文献[7]にて提案されたヒステリシス署名を応用し，文字単位ではなく，図３に示すように文書単位で署名の連鎖構造を持たせることで，文書の抜けを検知出来るようにした．

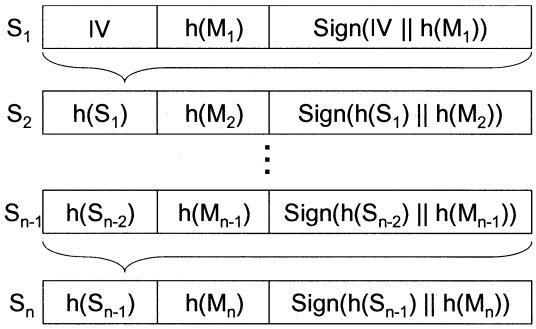

図３　文書単位のヒステリシス署名生成

図３の流れを下記に示す．

① 文書M_1がサーバに送られてくると，初期値ＩＶと文書M_1のハッシュ値ｈ（M_1）を結合した値に署名を行う．

② 文書M_2が送られてくると，図３のS_1のハッシュ値ｈ（S_1）と文書M_2のハッシュ値ｈ（M_2）との結合した値に署名を行う．

③ 以下，文書M_nが送られてくると，　S_{n-1}のハッシュ値ｈ（S_{n-1}）と文書M_nのハッシュ値ｈ（M_n）との結合値に署名を行うことを繰り返す．

このように文書単位でヒステリシス署名を行うことで，例えば文書M_1が削除された場合には，署名履歴検証に失敗する為に，不正にファイルが削除されたことが分かる．反対に言うと，署名履歴検証に成功すれば，文書が削除されていないと言える．

しかし，ヒステリシス署名を文書単位で行っただけでは問題２を解決出来ない．

3.2.3. セキュリティデバイス

問題２を解決する方法として，著者らは文献[8]にて提案された，セキュリティデバイスにヒステリシス署名を保存する方式を適用させることを考えた．

（前提条件）セキュリティデバイスは信用出来る．

3.2.3.1. セキュリティデバイスの特徴

以下の３つの機能を有している

①署名の生成・検証を行うことができる

②耐タンパー領域を持っている

③キーワードが文書に含まれているか確認できる

3.2.3.2. 運用方法

以下のようにシステムを構成し運用する

①セキュリティデバイスを外すと，ＰＣをロックする

②セキュリティデバイス内の耐タンパー領域に最終ヒステリシス署名履歴を保持する

これにより，耐タンパー領域に最終ヒステリシス署名を保持しておく為に，署名を破棄して新たに署名生成を行うことが出来なくなる．これにより不正な改ざん・消去を行った場合には検知が可能である．これにより問題２が解決可能である．

3.2.4. 電子文書墨塗り技術

文献[9]にて提案された方式として，署名された文書に対して，秘匿を行いセキュリティデバイス内において秘匿部分を復号し，署名検証を行う方式がある．これを本システムに適用し，セキュリティデバイス内において，秘匿部分を復号し，原告側の指定するキーワードが含まれていないことを確認する．これにより，開示された文書に原告側のキーワードが含まれていないことが証明可能である．

3.3. 提案システムの構成と評価

提案システムを次の３つの段階に分けて説明する．

①　文書の蓄積

②　文書の開示

③　サーバへのキーワード検索

①は，開示する為に証拠性を確保するために必要である．②は，個人情報等にあたる部分を秘匿し，原告側で秘匿部分に対してキーワードが含まれていないことを確認する．最後に③では，開示されなかった文書に原告側の指定したキーワードを含む，関連文書がないかどうかを確認する為に必要となる．全体像と全体における，①文書の蓄積，②文書の開示，③サーバへのキーワード検索の位置付けを図４に示す．

図4　提案システム全体像

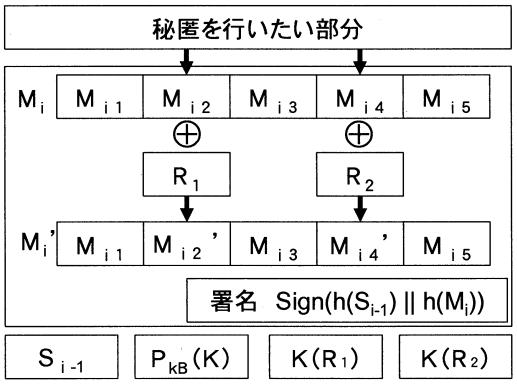

図5　開示文書及び公開情報

3.3.1. 文書の蓄積方法

3.2.2 節のヒステリシス署名と 3.2.3 節のセキュリティデバイスで示したように，図3に示したようにファイル単位で署名生成を行い，Ｓｎの署名履歴をセキュリティデバイスの耐タンパー領域に保持しておく．

文書M_iにはＳｉｇｎ（ｈ（S_{i-1}）｜｜ｈ（M_i））の署名がなされることになる．

3.3.2. 文書の開示

3.2.4 節で示した電子文書墨塗り技術を適用する．文書M_iを部分的に秘匿し，開示する方法について説明する．

① 秘匿を行いたい部分を選択する．
② 開示する部分と秘匿を行いたい部分を分けるようにブロックを分割する．
③ 秘匿を行いたい箇所の数だけ乱数を生成する．
④ 秘匿を行いたい箇所と③で生成した乱数の排他的論理和を取って秘匿（読めなく）する．これを文書M_i'として開示文書とする．
⑤ 開示文書と合わせて，鍵Ｋを生成し，開示要求者のセキュリティデバイスの公開鍵P_{kB}で暗号化したものP_{kB}（K）と，生成した乱数を鍵Ｋで暗号化したものK（R）と，　M_iの１つ前の署名履歴S_{i-1}を送る．
⑥ 原告側は，セキュリティデバイス内において，P_{kB}（K）を復号し，KからK（R）を復号し，乱数Ｒを得る．秘匿部分と乱数Ｒの排他的論理和を取り，文書Ｍを得て署名の検証を行い，秘匿部分に原告側の指定するキーワードが含まれているかどうかの確認を行う．

以上を図５，図６に示す．

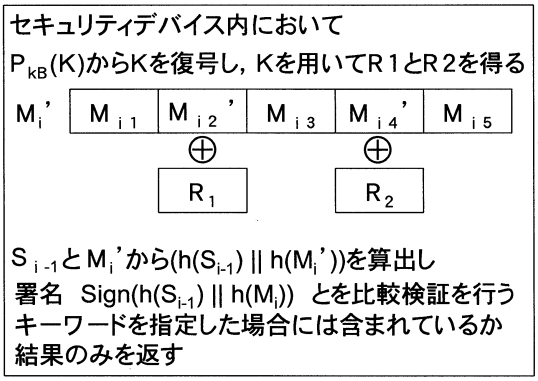

図6　開示文書の検証及びキーワードチェック

3.3.3. サーバへのキーワード検索

サーバには開示されていない文書が蓄積されている．これらの文書に開示要求がなされている関連文書がないことを示すために，3.1.2 節でも示したように原告側の指定するキーワードによる検索を行う．しかしながら，サーバに検索をかける場合には，被告側は関連する文書を隠しているのであれば，検索によって見つかることを恐れているはずである．したがって，指定されたキーワードで文書に対して検索をかけたことを証明することは非常に難しい．そこで，3.3.2 節で用いたセキュリティデバイスに，原告側が指定するキーワード群を保持させ，サーバに原告側のセキュリティデバイスを接続し，サーバにある文書に対して，原告側のセキュリティデバイス内でキーワードが含まれているかどうかを確認するという手順を取る．原告側のセキュリティデバイスには，以下の３つの情報を保持する．

① 原告側のサーバの最新のヒステリシス署名履歴 S_n
② 原告側が指定するキーワード群
③ 被告側のセキュリティデバイスの公開鍵 P_{kA}

④　ヒステリシス署名の初期値ＩＶ

3.3.3.1.　キーワード検索方法

以下の手順において，S_nを得られるか確認を行う．

① 初期値ＩＶと文書M_1からハッシュ値を算出し，S_1の署名履歴を検出する．成功すればM_1に対してキーワード検索を行う．

② 文書M_2と，①で得られたS_1からS_2の署名検証を行う．成功すればM_2に対してキーワード検索を行う．

③ 以下，同様にして，署名S_tに対して，文書ＭｔとS_{t-1}を検証し，キーワード検索を行う．これをS_nまで行う．

④ S_nが検証出来たら，保持しているS_nと一致するか確認を行う．

⑤ キーワードが含まれている文書があれば，書名を原告側のセキュリティデバイスに保持する．

以上の手順を踏むことで，サーバにある文書に不正に改ざんや削除を行っていないことが証明可能であると同時に，キーワードが文書に含まれていた際に，含まれていた文書の署名を保持させておくことで，既に開示されている文書に施されている署名意外のものが見つかれば，他に関連文書があることになる．逆に，既に開示している文書以外の署名が見つからなければ，関連する文書はすべて開示していると言える．

4. まとめ

今回，著者らは訴訟時に必要となる証拠提出において，開示文書の正当性を保障するためのシステムとして，ファイルの蓄積部分に文書単位のヒステリシス署名を耐タンパー制の領域に保持しておくことで，例え文書の作成者であっても改ざんや削除を行えなくする仕組みと，全ての文書が改ざん，削除されていないことが証明されうるサーバに対してキーワード検索を行うことで，関連する文書が開示されているかどうかを調べることにより，関連する文書が全て開示されていることを証明できるシステムの提案を行った．

4.1. 今後の課題

今後は，実装の検討を進めていきたいと考えている．セキュリティデバイス上で，本提案システムを現実的な処理時間で行うためには，どの程度の処理性能が必要であるかの検討を進めて行きたいと考えている．

また，E-Discoveryは近年，日本でも注目されてきており，日本において現状では電子文書の開示に関する強制が強いものではない．今後，E-Discoveryを日本で行っていく上で法制化の動向にも注意していく必要があると考えている．

文　献

[1] 藤村 明子，塩野入 理，金井 敦，“Digital Forensics適用を考慮にいれた電子情報の法的な安全性確保”，SCIS2005

[2] 佐々木良一「@police　第８回セキュリティ解説　デジタルフォレンジックス」http://www.cyberpolice.go.jp/column/explanation08.html

[3] ＠ＩＴ，“フォレンジックで内部不正を発見せよ”，2005.7，http://www.atmarkit.co.jp/fsecurity/special/67forensic/forensic01.html

[4] ＠ＩＴ，“EMCが狙う次の成長市場，e-Discoveryってなに？”，2005.6 http://www.atmarkit.co.jp/news/200506/03/emc.html http://www.indatacorp.com/services/efd.htm

[5] 宮崎 邦彦，洲崎 誠一，岩村 充，松本 勉，佐々木良一，吉浦 裕，“電子文書墨塗り問題”，信学技法 ISEC2003-20, pp61-67，2003

[6] Ron.Steinfeld ,Laurence.Bull,and Yuliang.Zheng, "Content Extraction Signatures"，ICISC 2001，pp285-304，2001

[7] 岩村 充，宮崎 邦彦，松本 勉，佐々木 良一，松木 武，“電子署名におけるアリバイ証明問題と経時証明問題－ヒステリシス署名とデジタル古文書の概念－”，コンピュータサイエンス誌 bit Vol32, No11，共立出版，2000

[8] 芦野 祐樹，佐々木 良一，“セキュリティデバイスとヒステリシス署名を用いたデジタルフォレンジックシステムの提案と再評価”，CSS2006

[9] 多田 真崇，高塚 光幸，増渕 孝延，佐々木 良一，“告白文書から告発者の発覚を防ぐ公益通報者保護技術の提案”，CSEC 2006，pp383-388，2006