情報処理学会論文誌　Vol. 49　No. 9　3191–3198 (Sep. 2008)

開示情報の墨塗りと証拠性確保を両立させるe-Discoveryシステムの提案

高塚光幸[†1]　多田真崇[†1]　佐々木良一[†1]

近年，デジタル・フォレンジック技術において証拠の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．開示する文書の中には，機密情報やプライバシ情報などが含まれている場合が多く，これらの情報を保護するために部分的に秘匿（これを「墨塗り」という）をしたい場合は多い．しかし，通常のデジタル署名を施している状況で，墨塗りを許すと，墨塗り以外の部分を改ざんしても，その改ざんを検知できないという問題がある．一方で墨塗りを許すと，過剰な墨塗りを行い，開示対象文書の提出を逃れる可能性も出てくる．そこで本稿では，セキュリティデバイスを用いて，開示情報の墨塗りと，証拠性の確保の両立を可能とする e-Discovery システムの提案を行う．

Proposal of the e-Discovery System for Sanitizing Disclosure Information and for Securing Evidence

Mitsuyuki Takatsuka,[†1] Masataka Tada[†1] and Ryoichi Sasaki[†1]

In late years the e-Discovery technique which is an electronic disclosure procedure of evidence in digital forensic technique becomes important. In a document to disclose, there is much it when wanting to do concealment (this is called “sanitizing”) partially so that a lot of cases that privacy information or privacy information are included in protect these information. However, there is a problem not to be able to detect the manipulation even if I tamper with moiety except a sanitizing method of coating when I allow you to a sanitizing method of coating in circumstances making normal digital signature on. On the other hand, I do a surplus sanitizing method of coating when I forgive a sanitizing method of coating, and potency escaping from presentation of an object document comes out. Thus, by this thesis, I use a security device and suggest an e-Discovery system enabling compatibility of security of a sanitizing method of coating of disclosure information and evidence nature.

1. はじめに

近年，インターネットや情報技術の発達にともなってあらゆる情報がデジタル化されてきている．これにともない，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であるデジタル・フォレンジック（Digital Forensics：以下 DF と略す）[1] が重要になってきている．DF の分野において，今後は証拠性の確保だけにはとどまらず，適切な情報開示が必要になってくると考えられる．民事訴訟において，情報開示を求められた際には，適切に情報が開示できなければ次のような問題が生じる．

（問題 1）　原告側から指定されたキーワードなどを含む証拠文書があるにもかかわらず，それを開示しなければ裁判で大変不利な状況になる．

（問題 2）　蓄積されたすべての情報を無条件に開示すれば，個人情報の漏洩や，ライバル関係にある原告側にビジネス上の重要な情報を不必要にもたらすことになる．

このような問題を解決するため，原告側から指定のあったキーワードなどを含む必要な文書は，必ず開示しなければならないが，機密情報やプライバシ情報などの保護のために部分的に秘匿したい場合は多い．この部分的な秘匿のことを墨塗りという．

しかし，文書全体に通常のデジタル署名を施している状況で，墨塗りを許すと，次のような問題が生じうる．

（問題 3）　通常のデジタル署名を行うだけでは，墨塗りを行った後，墨塗り部分以外の部分を改ざんしてもその改ざんを検知できない．墨塗り自体が改ざんと見なされ，それ以外の部分に改ざんがあったかどうか判断できなくなるからである．

（問題 4）　キーワード部分に墨塗りを行い，キーワードを含んでないように見せかけ，開示対象文書の提出を逃れる可能性がある．

本稿では，上記の 4 つの問題を解決し，開示情報の墨塗りと，証拠性の確保の両立を可能とする e-Discovery [2,3] システムの提案を行う．

墨塗りと証拠性の確保の両立を可能とし，しかも，墨塗り部にキーワードを含んでないことを検証できる e-Discovery システムの提案は，従来なかったものである．

†1 東京電機大学
Tokyo Denki University

2. 提案システムの概要

本章では，アメリカにおける民事訴訟を対象とし，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．本稿では米国の民事訴訟モデル[4] を取り扱うが，日本の企業が米国に進出し，米国において訴訟に巻き込まれた場合，米国の訴訟制度に従う必要がある．

2.1 日米の民事訴訟手続きの流れ

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に大きな違いがある．日本では審理がされ，また新たな証拠提出があり審理されるというように，図 1 の ④ のディスカバリと図 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，新たな証拠提出は通常ない．このため，1 度しかないディスカバリの際にすべての証拠を適切に開示しなければならない．証拠が不十分であるとされ，再提出を繰り返した例では，意図的な証拠の隠蔽であると見なされて多大な賠償請求を求められた例もある[5]．

つまり，日本の企業が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 ディスカバリの際に証拠提出を適切に行えなかった場合，証拠が不十分で敗訴してしまうといわれている．そのため，企業が事前に訴訟対策を行い，必要十分な情報を早急に提出できるようにしておく必要がある．また，日米の訴訟制度の違いとして，日本の訴訟においては，文書を開示しなかった場合の罰則規定がないことがあげられる．このため，e-Discovery の重要性は日本においては低いといえる．しかし，米国の訴訟に巻き込まれた場合には，ディスカバリの際に証拠を適切に開示することが非常に重要となってくるため，日米の訴訟制度の違いを正しく認識し，対策を行っておくことが重要であると考える．現実に，日本の企業が米国の民事訴訟に巻き込まれている例も少なくない．

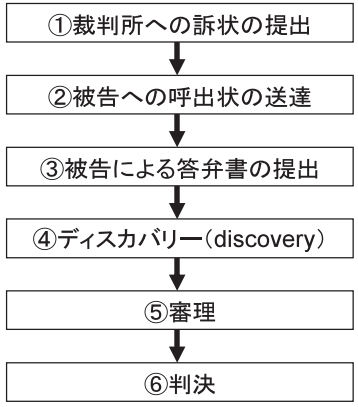

図 1　米国の民事訴訟の流れ
Fig. 1　Civil action flow in the USA.

この情報開示を，コンピュータなどを用いて実施することを e-Discovery という．米国における e-Discovery の手順は**図 2** に示すとおりである．

2.2 日米の民事訴訟手続きの流れ

被告側は，図 2 に示すように，弁護士やフォレンジックコンサルタント企業と協力して，情報開示を実施していく．この過程で，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ためには，以下の要件を満足しなければならない．

（要件 1）　作成された文書は，すべて，ログとして残っている．
（要件 2）　その後，被告側企業において，それらの文書に，改ざん，削除，追加がなされていない．
（要件 3）　原告側から指定されたキーワードを含む文書は，すべて証拠として提示される．
（要件 4）　提示する文書の一部を墨塗りしたとしても，墨塗り部分以外に，改ざんがされていないことが証明できる．

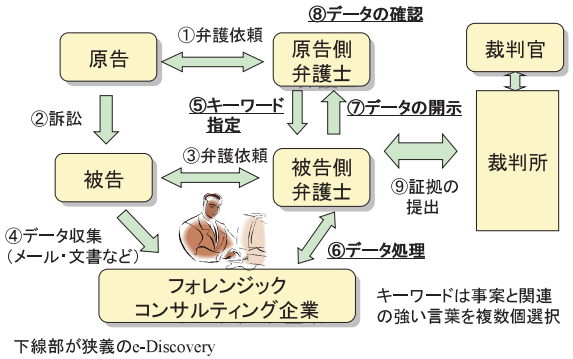

図 2　e-Discovery の手順
Fig. 2　e-Discovery procedure.

（要件 5）　キーワード部分に墨塗りを行い，キーワードを含んでないように見せかけ，対象文書の提出を逃れることを防止できる．

（要件 6）　原告側の処理によって墨塗り部分の発覚および類推がされない．

2.3　実現方式の検討

2.2 節の要件への対応方法は以下のとおりである．

（1）要件 1，2

要件 1 と 2 を満足するための方法として，セキュリティデバイスとヒステリシス署名[6]を組み合わせて用いる方式[7]を適用した．これによって従来の電子署名における改ざんが検知できるだけではなく，文書の抜け，つまり文書の削除が検出可能となる．これにより要件 1，2 を満足できる．

（2）要件 3

Trusted Third Party としてスマートカードなどのセキュリティデバイスを利用し，キーワードを含む文書をログファイルから確実に取り出すことにより実現する．

（3）要件 4

要件 4 を満たす既存技術としては，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見なされてしまうために，プライバシ情報を保護するための秘匿であっても改ざんと見なされてしまう．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 “機密情報，プライバシ情報の保護”，の両立ができず，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[8]や CES[9]である．これらの方式を導入することにより要件 4 を満足することは可能である．

（4）要件 5

キーワード部分に墨塗りを行い，キーワードを含んでいないように見せかけ，開示対象である文書の提出を逃れることを防止できなければならない．この機能は，従来の電子文書墨塗り技術[8]や CES[9]で持たせることはできない．したがって，要件 4 と 5 を同時に満足する方式が必要となる．

（5）要件 6

被告側が開示した文書に対して，原告側が不特定多数のキーワードを入力することで墨塗り部分に対して攻撃しようとしても，内容の発覚や類推されないことを，セキュリティデバイスを用いることによって実現する．

要件 3，4，5，6 を同時に満足する方式については，3 章で詳しく説明する．

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）開示文書へのキーワード検索

（1）は，開示するために証拠性を確保するために必要である．（2）は，個人情報などにあたる部分の秘匿，関連のない文書への秘匿を行い，原告側に開示する．最後に（3）では，開示された文書に抜けや改ざんがなく，また墨塗り部分に対して不正にキーワードが墨塗り処理された部分に含まれていないか確認する．全体像と全体における，（1）文書の蓄積，（2）文書の開示，（3）開示文書へのキーワード検索の位置付けを**図 3** に示す．

3.1　前 提 条 件

（前提条件 1）　文書を開示すべきかどうかは原告側が指定するキーワードを含むかどうかによって判断を行う．

（前提条件 2）　セキュリティデバイスは，耐タンパ性が高く，その持ち主であっても，その中に含まれる鍵などの情報を知ることはできない．

（前提条件 3）　コンピュータ内やセキュリティデバイス内のプログラムは正しいものが使われ改ざんされていない．

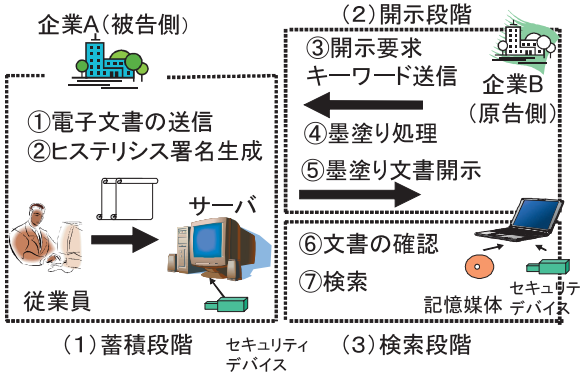

図 3　提案システムの全体像

Fig. 3　Overview of the proposed system.

（前提条件 4）　原告側も，被告側もそれぞれ異なるセキュリティデバイスを持つ．

前提条件 3 は一般的でないが，これを可能にするため文献 10) では，① 不正プログラムの起動命令に対する API フック機能と，② PC などのマザーボード上に実装されているセキュリティチップである Trusted Platform Module（以下，TPM）を用いて信頼性を向上させたプログラムによって，③ 正しいプログラムのみが稼働しているように制御する方式を提案しており，これが利用可能であると考えている．

3.2 表記方法

本節では，本稿における表記方法を**表 1** にまとめる．

表 1　鍵および処理の表記方法
Table 1　The notation used in formal representations.

表記	説明
S_A	企業 A（被告側）のセキュリティデバイスの秘密鍵
P_A	企業 A（被告側）のセキュリティデバイスの公開鍵
S_B	企業 B（原告側）のセキュリティデバイスの秘密鍵
P_B	企業 B（原告側）のセキュリティデバイスの公開鍵
H	ハッシュ関数
K	共通鍵
W_t	原告側の指定するキーワード
Mij	i 番目の文書の j 番目のブロック
Rij	Mij のブロックを墨塗りする為の乱数
Encrypt(S_A,M)	M を鍵 S_A を使って暗号化
Decrypt(P_A,C)	C を鍵 P_A を使って復号
Sig(S_A,W_t)	W_t に対して鍵 S_A を使って署名
Verify(P_A,W_t)	W_t に対して鍵 P_A を使って署名検証

3.3 文書の蓄積

3.3.1 被告側による不正方法

被告側の不正として以下の 2 つが考えられる．

（不正 1）　開示したくない文書を削除し，あたかも開示対象となる文書が存在しないように見せかける．

（不正 2）　開示対象である文書を改ざんし，新たに署名を生成しなおす．

これらの不正が行われた場合，第三者の不正ではないため，従来の電子署名では解決できない．

3.3.2 ヒステリシス署名によるアプローチ

ヒステリシス署名とセキュリティデバイスを組み合わせて用いる方式[7] を文書蓄積側（被告側）に適用する．ヒステリシス署名は，署名に連鎖構造を持たせることができるため，署名の検証が行えた場合にはサーバに保持されている文書は改ざんや削除による抜けがないことが証明可能となる．このとき，記憶媒体には文書 M_i とヒステリシス署名 $S_i = \mathrm{Sig}(S_A, H(S_{i-1}) \,||\, H(M_i))$ が残る（$i = 1, 2, \cdots, n$）．これにより，3.3.1 項の不正 1 は検出可能となる．また，セキュリティデバイス内の耐タンパな領域に最新のヒステリシス署名履歴 S_n を保持させておく．耐タンパな領域を用いることにより，たとえ持ち主であっても内容を不正に改ざんすることはできない．これにより，改ざんをし，新たに署名を生成した場合，耐タンパな領域に保持されている署名履歴と，文書に付与されている署名が異なるため，不正が検出可能になる．ここで，M_i は i 番目に生じた文書，S_i は i 番目のヒステリシス署名履歴である．作成された文書は，すべてログとして残り，蓄積された文書の，改ざん，削除，追加がなされていないことの検証方法など詳しくは文献 7) を参照いただきたい．

3.4 文書の開示

文書を開示する際に，**図 4** に示すような手順で処理を行い，開示文書を作成し，記憶媒体の形で原告側に公開する．

ここで**図 5** を例に i 番目の文書に対する墨塗り処理を説明する．

① 秘匿を行いたい部分を選択し，開示する部分（図 5 では M_{i1} と M_{i3}，M_{i5}）と秘匿を行いたい部分（図 5 では M_{i2} と M_{i4}）を分けるようにブロックを分割する．

② 秘匿を行いたい箇所の数だけ乱数を生成する．

③ 秘匿を行いたい箇所と② で生成した乱数の排他的論理和をとって秘匿（墨塗り）する．これを文書 M_i' として開示文書とする．このとき，暗号化した箇所の位置情報をログファイルに保存しておく．

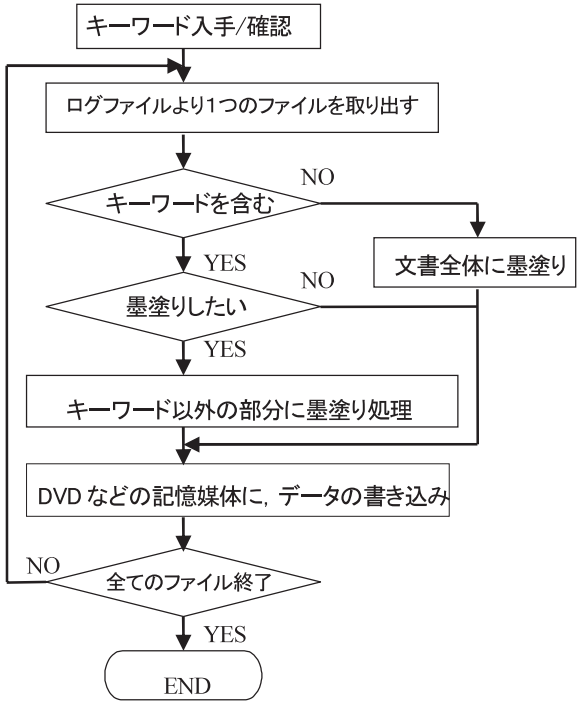

図 4　開示処理の流れ
Fig. 4　Disclosure process flow.

④　開示文書と合わせて，鍵 K を生成し，開示要求者（原告側）のセキュリティデバイスの公開鍵 P_B で暗号化した $C1 = \mathrm{Encrypt}(P_B, K)$ と，生成した乱数を鍵 K で暗号化した $C2 = \mathrm{Encrypt}(K, R_{i2})$，$C3 = \mathrm{Encrypt}(K, R_{i4})$ と，1 つ前の署名履歴 S_{i-1} を記憶媒体に書き込む．

ここで，キーワードを含まない場合は，全体を秘匿してよいので，M_i 全体に乱数が与えられる場合に相当する．また，墨塗りしない場合は，生成すべき乱数がない場合に相当する．

また，通常ではファイルへアクセスしただけでタイムスタンプが変更されるが，提案方式ではタイムスタンプが変更されることに関しては影響を受けない方式である．ヒステリシス署名を用いることで，文書の内容については改ざんがないことが証明可能であるため，本方式ではタイムスタンプなどは対象外とする．

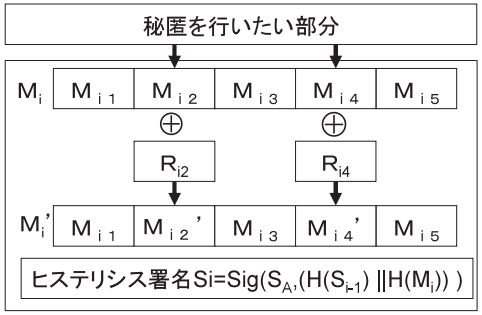

図 5　開示文書および公開情報
Fig. 5　Disclosure document and disclosed information.

3.5　開示文書へのキーワード検索

原告側において墨塗りされて開示された文書群に対して改ざんや抜けがないか，またキーワードが含まれる部分に対して不適切に墨塗りが施されていないかを検証する．検証にあたり，PC に墨塗り文書を書き込んだ記憶媒体を設置し，セキュリティデバイスを同じく設置する．

セキュリティデバイス内には，秘密鍵 S_B が耐タンパな領域に設置されており，この情報は，その持ち主でも分からないものとする．ここで，セキュリティデバイスへの入力や構成などについては**図 6** を参照していただきたい．

ここでは，セキュリティデバイス内の処理を図 5 の文書 M_i' を例に説明する．

①　文書 M_i' と $C1 = \mathrm{Encrypt}(P_B, K)$，$C2 = \mathrm{Encrypt}(K, R_{i2})$，$C3 = \mathrm{Encrypt}(K, R_{i4})$ をセキュリティデバイスに読み込む．

②　原告側のセキュリティデバイスの秘密鍵 S_B を用い $\mathrm{Decrypt}(S_B, C1)$ から K を復号する．そして，$\mathrm{Decrypt}(K, C2)$ と $\mathrm{Decrypt}(K, C3)$ より R_1 と R_2 を得る．

③　ログファイルから暗号文の位置情報を読み込み，M_{i2}'（$= M_{i2} \oplus R_{i2}$）と M_{i4}'（$= M_{i4} \oplus R_{i4}$）に対して $M_{i2}' \oplus R_{i2}$，$M_{i4}' \oplus R_{i4}$ を算出し M_{i2} と M_{i4} を復号し，これらを用いて M_i を得る．

④　得られた M_i の墨塗りされていた箇所に，キーワード W_t（$t = 1, 2, \cdots, m$）が含まれているかを検証する．もし含まれていればアラームを表示し，含まれていなければ処理を続ける．

⑤　ヒステリシス署名 S_i を鍵 P_A を用いて検証する．（$= \mathrm{Verify}(P_A, S_i)$）．

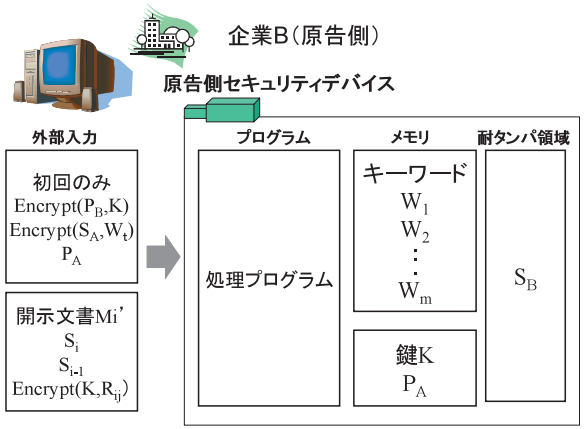

図 6　セキュリティデバイスの構成
Fig. 6　Structure of security device.

⑥　検証に失敗すればアラームを表示し，成功すれば次の文書へと処理を続ける．

すべての文書に対して署名検証が成功すれば，すべての文書が抜けなく開示され，また改ざんがないことが証明可能である．また，キーワードが墨塗り部分に含まれていないことが証明可能となる．さらに，セキュリティデバイス内においてのみ復号が可能であるので，墨塗り部が何であるかを原告側は知ることができない．

しかし，ここで原告側が開示文書に対して不特定多数の文字をキーワードとしてセキュリティデバイスに入力し，検証を行うことで墨塗り部分の内容を類推される危険性がある．そのような攻撃を回避するための方式を 3.6 節で説明する．

3.6　プログラムによるキーワード制御

キーワードを制御する方法としては次の 2 つの方式が考えられる．

(1)　セキュリティデバイスのプログラムにより，キーワードの検索をかけられる回数に制限をかける方式

(2)　キーワードの検索を行うためには被告側の協力が必要となる方式

方式（1）は訴訟により原告側が指定するキーワードの数は異なるため，回数を一意に定めることは困難である．そこで，方式（2）を採用することとした．

本稿では，被告側が協力していることを確認するための方式として，被告側がキーワードに対して署名を行い，署名付きのキーワードを原告に返す方式を考えた．提案方式の詳細は以下のとおりである．

①　原告側は被告側に対してキーワード W_t を送る．

②　被告側は，企業の保有する秘密鍵 SK_A を用いてキーワード W_t に署名し，$\mathrm{Sig}(SK_A, W_t)$ を原告側に送る．

③　原告側はセキュリティデバイスに $\mathrm{Sig}(SK_A, W_t)$ を入力する．

④　セキュリティデバイス内では入力された W_t に対して鍵 PK_A を用いて検証を行う．

⑤　検証に成功すれば，W_t をキーワードとしてセキュリティデバイス内に保存する．

これにより，両者が合意したキーワードだけがチェックできるので，膨大なキーワードを与え，墨塗り部を類推するという攻撃を防止することができる．ここで，セキュリティデバイスのプログラムは正しく，被告側の公開鍵 PK_A で検証されなければキーワードとしてメモリ上に設定できないものとする．

しかしこの方法では，原告が自分の公開鍵 PK_B と秘密鍵 SK_B のペアを別に用意して，多くのキーワードに自分の秘密鍵である SK_B で署名し，原告側の公開鍵 PK_B と，一緒にセキュリティデバイスに読み込ませ自由にキーワード検索を行うという問題が考えられる．

なぜならば，セキュリティデバイスでは，確かに署名が付与されており，それに対応する鍵が入力されるため，署名検証に成功し，キーワードを保持し，復号された部分に対してキーワードが含まれているかどうかを検証し，結果を返してしまう．このような攻撃は，たとえプログラムが正しかったとしても回避できない．このような問題を解決するためには，セキュリティデバイスに入力される情報が正しい入力であることを保証できなければならない．そこで，入力情報を制御するための方法を 3.7 節で詳しく説明する．

3.7　被告側の鍵によるキーワード制御

3.6 節であげた問題を解決するために，必要な処理を行うためには必ず，被告側の公開鍵をセキュリティデバイスに入力しなければならない方式を検討した．

被告側が処理を行っている処理は，墨塗り処理である．そこで，3.5 節の $C1$（$=\mathrm{Encrypt}(P_B, K)$）をさらに被告側の保有する秘密鍵 SK_A を用いて暗号化し，$C1' = \mathrm{Encrypt}(SK_A, C1)$ を $C1$ の代わりに送る．これにより，原告側は，開示された文書をセキュリティデバイス内で復号し，検証とキーワードの有無を確認する処理を行うためには，被告側の公開鍵である PK_A を正しく原告側のセキュリティデバイスに読み込ませなければならない．

そして，セキュリティデバイス内のプログラムは，公開鍵を後から入れ替えられないような構造にしておけば，被告側の公開鍵がセキュリティデバイス内に保管されるようになる．

これにより，被告側の協力なしに，キーワードの検索を行えなくなる．したがって，原告側と被告側が協力した公平なキーワードの制御が可能となった．

4. 実装のための検討

本章に実装するにあたっての問題点とその検討方式を述べる．

4.1 実装上の問題

実装を行うにあたって以下の問題点が発生することが考えられる．

(1)　性能の問題

e-Discovery において，開示対象となる文書の量が膨大であり，スマートカードでは実現は可能であると考えられるが，処理が現実的な時間内で終わらない．

(2)　墨塗りの方法

墨塗り部分をどのように指定し，どのようにブロック分割を行うべきかが不明確である．

(3)　墨塗り部分のデータ長から内容が類推される危険性

墨塗り部分に同程度の乱数を生成し，墨塗りを行った場合，墨塗り部分の文字列の長さからの類推による漏洩の危険性がある．

4.2 実装における対策

4.1 節であげた問題を解決するための対策を本節で述べる．

(1) 性能の問題

セキュリティデバイスにおける必要機能は下記のとおりである．

1. 耐タンパな領域を有していること
2. メモリを有していること
3. 処理演算装置を有していること
4. プログラムとして，排他的論理和演算，署名検証，文書へのキーワード検索機能を有していること

これら 4 つの機能を用いて行う処理は複雑なものは必要としないが，取り扱うデータが膨大なため，高速な I/O と演算能力を必要とする．このため，現在あるようなスマートカードでは処理時間の問題で実用性に問題がある．この点については，PC などを改良した専用ハードを開発することで高速化を行い実現できるのではないかと考えている．

(2) 墨塗りの方法

墨塗り部分を指定する方法については，人手で行うことを考えている．墨塗りを行いたい文書の内容を表示し，墨塗りを行いたい部分をマウスなどの入力装置により選択状態にし，ボタンを押すことでその部分を墨塗り箇所として選択する．墨塗り箇所を選択が終われば，選んだ墨塗り部分である非開示部分と，それ以外の開示部分にブロックを分割し，非開示部分に墨塗りを行う方法を考えている．

(3) 墨塗り部分が類推される危険性

墨塗り部分のブロック Mij に対して，乱数 Rij を用いて $(Mij \oplus Rij)$ として暗号化した場合，ビット長から文字列の長さが類推される危険性がある．これに対し，$(Mij \oplus Rij)$ ではなく，新たに乱数 rij をビット長を不規則に変更しながら生成し，$((Mij \,||\, rij) \oplus (Rij \,||\, rij))$ のようにとることで計算機内のデータをチェックすることによる類推を困難にできる．また，rij の長さにより，墨塗り部分の表示の長さを変えるようにしておけば目で見ても墨塗り部分の長さが分からなくなる．

5. おわりに

本稿では，e-Discovery システムに電子文書墨塗り技術を適用することにより，情報を部分的に秘匿可能かつ開示文書の証拠性を確保できるシステムの提案を行った．従来の電子文書墨塗り技術であれば，署名時にブロックの分割を行っており，ブロックの分割を自由に行えないが，本方式では開示を行う際にブロックの分割を行っており，セキュリティデバイスを用いることにより自由にブロックの分割を行い墨塗りが可能である．

また，従来方式でも秘匿を行うことは可能であるが，e-Discovery 適用するにあたり，墨塗り部分にキーワード含まれていれば，これを検知できなければならないという問題がある．このような問題は，従来の電子文書墨塗り技術では解決できない．

このような問題を解決するために，セキュリティデバイスを用いることにより，著者らは従来では行われていなかった墨塗り部分の復号を行い，中身の確認を行うことで原告側の指定するキーワードが含まれていないことを証明可能にした．また，キーワードの確認を行ううえでの処理において，不特定多数のキーワードにより墨塗り部分が類推される危険性を指摘し，解決するキーワードを制御するための方式を提案した．

今後は，本方式に基づく実装を行いたいと考えている．特に，開示対象データが膨大な量であることを考慮した実現方式を検討していきたいと考えている．

参 考 文 献

1) 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

2) EnCase,「eDiscovery とは」. http://www.encase.jp/glossary/eDiscovery.html
3) @ 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
4) 中山義壽：訴訟社会アメリカと日本企業，新評論 (2002).
5) ITmedia：J-SOX 時代のデジタル・フォレンジックとは (2007.2). http://www.itmedia.co.jp/enterprise/articles/0701/17/news006_4.html
6) 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，Vol.32, No.11, 共立出版 (2000).
7) 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* (2006).
8) 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，信学技報，ISEC2003-20, pp.61–67 (2003).
9) Steinfeld, R., Bull, L. and Zheng, Y.: Content Extraction Signatures, *ICISC 2001*, pp.285–304 (2001).
10) 藤田圭祐，芦野佑樹，上原哲太朗，佐々木良一：不正プログラムの起動制御機能を持つ DF システムの提案，*CSS2007* (2007).

(平成 19 年 11 月 29 日受付)
(平成 20 年 6 月 3 日採録)

高塚　光幸

平成 20 年 3 月東京電機大学大学院工学研究科修士課程修了．同年 4 月に NEC ソフト株式会社入社．在学中は，デジタル・フォレンジック技術についての研究に従事．

多田　真崇

平成 20 年 3 月東京電機大学大学院修了．同年 4 月新日鉄ソリューションズ株式会社入社．在学中は主に，セキュリティ面から内部告発者の支援を行うシステムの研究に従事した．中国で開催された I3E2007 では，「Proposal of a Whistleblower Protection System to Prevent the Exposure of an Accuser from Signing an Indictment Document」の題で，文書の機密性を保持し，内部告発者のプライバシを確保しつつも，信頼できる内部告発を実現する方式を発表した．

佐々木良一（フェロー）

昭和 46 年 3 月東京大学卒業．同年 4 月日立製作所入所．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．平成 13 年 4 月より東京電機大学工学部教授，平成 19 年 4 月より未来科学部教授．工学博士（東京大学）．平成 10 年電気学会著作賞受賞．平成 14 年情報処理学会論文賞受賞．平成 19 年総務大臣表彰（情報セキュリティ促進部門）．平成 19 年度「情報セキュリティの日」功労者表彰．著書に，『インターネットセキュリティ』（オーム社，1996 年），『インターネットセキュリティ入門』（岩波新書，1999 年），『IT リスクの考え方』（岩波新書，2008 年）等．情報処理学会コンピュータセキュリティ研究会顧問，日本セキュリティ・マネージメント学会会長，情報ネットワーク法学会理事長，日本学術会議連携会員，日本ネットワークセキュリティ協会会長．