大容量耐タンパ装置 HiGATE の試作と e-Discovery への適用

†桜井裕唯　＊芦野佑樹　††上原哲太郎　＊＊吉浦裕　†佐々木良一

†東京電機大学大学院未来科学研究科情報メディア学専攻

〒101-8457 東京都千代田区神田錦町 2-2

＊日本電気　　††京都大学　　＊＊電気通信

E-mail：†sakurai@isl.im.dendai.ac.jp

あらまし　従来，PC の持ち主はデータの処理を自由に行い，その入力や中間結果を自由に見ていた．しかし，疫学調査や e-Discovery などのように個人情報や企業秘密などのデリケートなデータを２つ以上の団体が扱わなければならない場合、そのような行動をされてしまうと都合が悪い．これを解決するためには，公開かぎ暗号を用い暗号化されたデータを、特定の耐タンパ装置内のみで復号や種々の処理を行うことで基本的対応が可能である．このような機能を持つものとして IC カードがあるが、処理速度や記憶容量に制限があり望ましい処理ができない。そこで，筆者らは管理者または使用者であってもデータの中身を見ずに大量のデータの処理を行うことができる PC ベース型大容量耐タンパ装置 HiGATE の構想を示した。あわせてその試作を行い，e-Discovery へ適用したので結果を報告する．

HiGATE (High Grade Anti-Tamper Equipment) Prototype and Its Application to e-Discovery

†Yui Sakurai, Yuki Ashino, Tetsutaro Uehara,

Hiroshi Yoshiura and Ryoichi Sasaki†

†The Dept. of Information Systems and Multimedia design, School of Engineering, Tokyo Denki University

2-2 Kanda-Nisikicho, Chiyoda-Ku, Tokyo, 101-8457, Japan

E-mail：†sakurai@isl.im.dendai.ac.jp

Abstract In the past, computer owners were free to process data as desired and to observe the inputted data as well as the interim results. However, the unrestricted processing of data and accessing of interim results even by computer users is associated with an increasing number of adverse events. These adverse events often occur when sensitive data such as personal or confidential business information must be handled by two or more parties, such as in the case of e-Discovery, used in legal proceedings, or epidemiologic studies. To solve this problem, a provider of the data should encrypt it, and the owner of the computer for processing should decrypt the encrypted data only in the anti-tamper area of the computer. Although, as Anti-tamper equipment, smart card is well-known, the function of the smart card is very limited. Accordingly, the authors present the concept of PC-based High Grade Anti-Tamper Equipment (HiGATE), which allows data to be handled without revealing the data content to administrators or users. To verify this concept, an e-Discovery application on a prototype was executed.

１　はじめに

今日，多くのデータはデジタル化されコンピュータによってさまざまに処理されている．従来，コンピュータの持ち主はデータの処理を自由に行い，その入力や中間結果を自由に見ていた．しかし，コンピュータの利用者であっても自由な処理や中間結果の自由な閲覧が都合の悪い事象が増えてきつつある．これは，個人情報や企業秘密などのデリケートなデータを２つ以上の団体が扱わなければならない場合に生じることが多い．たとえば次のような場合である．

（１）疫学調査：（ａ）各個人に関する職場での被曝線量などの身体的負荷と（ｂ）病院やフィールド調査で得られた癌などの疾病の発生の事実をつき合わせ，それらの間の相関を調べたいような場合は多い．しかし，それぞれのデータを相手あるいは第３者に渡し，通常の処理を行ったのでは，入力や中間結果で個人情報がコンピュータを用いてデータ処

理を行っている人にわかってしまい，個人情報保護の観点から問題となりうる．このため，現状ではこれらのデータのやり取りができないということになっており，疫学調査を，国民の健康の向上に役立てることができないという問題が発生している．この問題を解決するためには，(イ）本来の持ち主によってすべてに暗号化を施したデータを相手あるいは第３者に渡し，(ロ）相手あるいは第３者はコンピュータにそれを入力し，復号した後，ある定められた処理を行い相関値のみを出力し，中間結果などはコンピュータの利用者でも見られないようにできればよい．

（２）e-Discovery：日本の企業も巻き込まれることの多い，米国の民事裁判では，審理に先立ち，被告側と原告側がお互いの電子的証拠を開示し合う e-Discovery を行う．その際，原告側から指定されたキーワードなどを含む電子的な証拠文書があるにも関わらず，それを開示しなければ裁判で大変不利な状況になる．一方，蓄積された全ての電子データ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．このため，電子文書に部分的に暗号技術を用いて墨を塗ることが考えられている[4]．このような，すみ塗りを行った電子文書を受け取った原告側は，墨塗り部分にキーワードが含まれていないことをコンピュータで確認したいが，復号を行い自由に墨塗り部分を見ることを許すと被告側の秘密を不当に知ってしまうこととなる．このような問題を解決するためには，コンピュータの処理において，墨塗り部分にキーワードを含むかどうかの判断は可能であるが，墨塗り部分の解読などそれ以外の処理はできず，中間結果も見られなくすればよい．

疫学調査はデータすべてに暗号化するのに対して、e-Discovery は部分的に暗号化するなどの違いはあるが、これらの問題を解決するために共通するのは，情報を提供する側が暗号化を行い，コンピュータの持ち主は復号を行う．そして，そのデータに対し，ある定められた処理だけを行い，その結果以外を知ることができなくすることである．これらを実現するために考えられる手段の１つが，暗号化されたデータに対して特定の PC でのみ復号を可能とする公開鍵暗号の使用し、復号はコンピュータのメモリ内のみで行われることによって使用者の不正を防ぐ方法である．しかし，メモリ内のみで復号する場合であっても，メモリに対する攻撃によって復号データを見ることは可能である．よって，持ち主でも処理を変更したり，中間結果を見たりすることのできない耐タンパ装置を用いる．耐タンパ装置として一般に用いられているのがスマートカード（IC カードともいう）である．スマートカードの中にユーザでも知ることのできない秘密鍵を持ち公開鍵暗号を用いて正しくデジタル署名を施すということは一般に行われている．

しかし，スマートカードは，処理が遅く，メモリ量が少なく，一般の人による通常のコンピュータ言語を用いたプログラミングが困難であるという問題がある．そこで，ＰＣのハード，ソフトに改良を加え，これらの問題を克服することのできるシステムを開発することとした．それがＰＣをベースにしたハードと，著者らが先に開発したプログラムの起動制御機能(BCF=BootControlFunction)[11]などのソフトからなる大容量耐タンパ装置 ”HiGATE(High Grade Anti-Tamper Equipment)”である．

本論文は HiGATE の構想を示すとともに，その試作を行い，e-Discovery へ適用した結果を報告する．個人情報や機密情報の扱いに関する関心が高まっており，今後 HiGATE の適用対象は増大していくものと予想される．なお，コンピュータの利用者でも自由な処理や中間結果の閲覧を防止するのに本研究と同様なアプローチは調査した範囲においてはない．同じ目的を達成するために暗号プロトコルを用いる方法も考えられるが，適用できる範囲が非常に狭くここで扱うような問題には適用できないと考えている．

2 提案システムの概要

2.1 HiGATE の要件

HiGATE の要件として以下の 5 つが挙げられる．

1. 持ち主でも見ることのできない耐タンパな領域を有していること
2. 計算に十分なメモリを有していること
3. 演算処理が早い
4. 持ち主ではなく信頼できる第３者なら自由なプログラミングを行うことができる
5. 実現が容易

要件 1 を満たすものとしてスマートカードが挙げられる．しかしスマートカードは問題点が 2 つ存在する．まず，一つ目は処理能力が問題点としてあげられる．これは e-Discovery のような大量のデータを扱い，処理に期限があるものの場合，深刻な問題である．また，２つ目は，スマートカードのプラグラムにはマイクロプログラミングなどの特殊な技能が必要であり，一般の人は自由なプログラ

ミングを行えない点である．このため，スマートカードでは適用できない上記の５つの要件を満足するHiGATEの開発が必要となった．

2.2 要件への対応方法

(要件1)

要件1を満足するために必要なHiGATEの機能を以下に示す．

①ハードウェア機能

装置のケースを開けていないことを証明できる．

②ソフトウェア機能

1. アプリケーションプログラムの起動制御機能
2. ハードディスク（HDD）全体の暗号機能
3. 演算処理機能
4. 計算の入力や中途計算結果の残るファイルの末梢機能

これらの機能は3章で詳しく記述する．

(要件2,3,4,5)

要件2,3,4,5は開発をPCベースで行うことで自動的に可能なる．すなわち，ＰＣベースで開発を行うことによって，入出力や演算速度が速く，大量データの蓄積が可能になることや，特殊なプログラミングではなく，C言語，JAVAなどのプログラムを自由に使用可能である，などが挙げられる．また，PCベースであるから特殊な機材をあまり必要とせず容易に導入することができる．ここではOSは著者らが多くのノウハウをもつWindowsを搭載することとした．

3 HiGATEの構成

3.1 前提条件

(前提条件1)BIOS,OSは正しく稼働している

(前提条件2)HiGATE設定時に不正を行わない

(前提条件3)HiGATEに不正なプログラムが入っていない

上記の状況の下でHiGATEを運用する．

3.2 考えられる不正

HiGATEに対する攻撃方法は以下の４つが考えられる．

(不正1)ケースを無理やり開け，メモリ内の情報を抜き出す

(不正2)HiGATEのHDDを抜き出し，他のPCに接続し，HiGATE内のデータ，プログラムなどのデータを抜き出す

(不正3)不正プログラムを立ち上げ，プログラム改竄や情報の盗み見を行う

3.3 不正に対する対策機能

(対策1）ケースを開けていないことを証明する

不正１のようにケースを開けメモリ内の情報を盗み見ることが考えられる．そのため，ケースを開けさせないことが重要になってくる．これを実現するものとしてはつぎの２つの方法が間がられる．

（１）無理にケースを開けると電源などがダウンしメモリ内の情報が消えるようにする．これを実現する方法として，(a)マイクロスイッチによりケースの開放を検知する，(b)リードスイッチとケースの蓋の磁石により検知する，(c)光により蓋の開放を検知する，ことなどにより電源を落とす方法がある．

（２）シールによりケースを開けるとすぐに分かるようにする．この既存技術として開封防止ラベルがある．これは開封防止ラベルをはがした場合，開封済みという文字が残る仕組みであり，これによってケースを開けているかどうかの判別ができる．何者かによって，シールを切られる，剥がされた場合，そのHiGATEの持つデータは効力を失うということにすることで使用者の不正は防ぐことは可能である．

今回は簡単に実現できる方式（２）を採用することにした．今後，方式（１）と組み合わせさらに安全性を向上させることも可能である．

(対策2)ＨＤＤの暗号化

不正2のようにHiGATEで使用しているHDDを持ち出し，別のPCに取り付けて改竄，または情報の取得を防ぐ目的でHDDの暗号化を行う．既存技術にはBitLockerがあり，これは『Windows Vista Enterprise』『Windows Vista Ultimate』のエディションのみにある機能である.HiGATEのOSはWindows Vista Ultimateを搭載する．

(対策3）起動制御(BCF/Vista)

不正３のように不正プログラムを立ち上げ，プログラム改竄や情報の盗み見を行うことが考えられる．これを防ぐ既存の技術として著者らが開発したBCF/Vistaがある[7]．BCF/Vistaに関しては3.4に詳しく記述する．

その他の機能としてファイル末梢と演算機能がある．ファイル末梢はHiGATEで扱うHDD内にあるデータを抹消する機能である．これはHiGATE使用者がデータ使用後にデータを残さないためのものである．HiGATEは使用者であっても見てはならないデータを扱う．よって，いつまでも使用者が所持するHiGATEに残しておくことは不正につながる．演算機能は

適用する場面によって使用方法は違うものであり，プログラム開発者が自由に開発することができる部分である．またキーボードを利用した巧妙な不正が考えられるが，Windows VistaUltimate の機能であるデバイスドライバのインストール制限機能を使用することによって回避が可能であると考える．

3.4 BCF/Vista

BCF/Vista はデジタルフォレンジックシステム Dig-Force[2][3]を開発する過程でその一部として開発したものである．BCF/Vista では設定時に起動を行うプログラムのハッシュ値を計算し，ホワイトリストに登録を行い，ホワイトリスト全体にデジタル署名を施しておく．OS が立ち上がり，その次に立ち上がるよう設定された BCF/Vista が立ち上がった後，アプリケーションプログラムなどが立ち上がろうとするとそのプログラムのハッシュ値を BCF/Vista は計算し，あらかじめ登録されているホワイトリストの正当性を署名検証によって行った後，その内のハッシュ値との比較を行う．登録されているハッシュ値と同じであればそのプログラムを起動し，登録されていなければ APIHook を使い起動を阻止する．これにより不正なプログラムを起動させようとしても，前提条件１の「BIOS, OS は正しく稼働している」が成立するなら不正なプログラムの稼動を防止することができる．BCF/Vista の詳しくは文献[7]を参照いただきたい．

3.5 機能構成

HiGATE は 2.2 で記述した①ハードウェア機能と②ソフトウェア機能の 4 つの機能を持つことで HDD 内に存在する OS，演算機能であったり，メモリ内に存在する鍵，データなどを守るための耐タンパな領域を実現することが可能である．よって HiGATE は耐タンパな領域内でプログラム開発者が作成した演算プログラムを不正されず正しい状態で実行することができる．ここで HiGATE の機能構成を図 1 に示すとともに，スマートカードと HiGATE の機能比較を行った．それらを表１，２に示す．

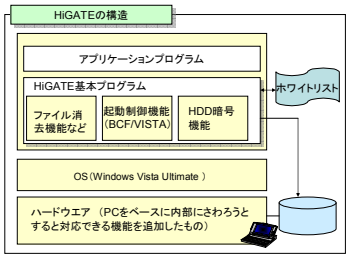

図1.　HiGATE構成図

表１.　スマートカードと HiGATE の共通点

共通点	IC カード	HiGATE
決められたプログラムの起動	読み出し専用半導体メモリ	BCF/Vista
メモリに外部からアクセスができない	暗号回路やメモリの１チップ化	開封防止ラベルなどで，ケースを開けさせなくする
偽環境を作成させない	ＣＰＵによるアクセス制御	HDD 暗号
耐タンパな領域	ＣＰＵによるアクセス制御	・BCF/Vista ・HDD 暗号 ・開封防止ラベル

表２.　スマートカードと HiGATE の相違点

相違点	IC カード	HiGATE
ＯＳ	ＥＭＶ仕様	WindowsVista Ultimate
プログラム言語の開発環境による制限	制限される	制限されない
メモリ	RAM(1MByte)	RAM(3Gbyte)

4 HiGATE の運用

この項では HiGATE の運用の記述する．

① HiGATE 製造フェーズ
② プログラム導入フェーズ
③ 設定フェーズ
④ 使用フェーズ

上記の①～④の HiGATE の運用に関わる登場人物として，製造者，プログラム制作者，使用者が存在する．

① 製造フェーズ

製造者は HiGATE 用 PC に HiGATE に必要である OS(WindowsVista),BCF/Vista を入れておき，プログラム開発者に HiGATE を渡す．

② プログラム導入フェーズ

プログラム制作者は製造者から HiGATE を受け取り，HiGATE を適用する事柄で必要な処理プログラムを HiGATE に導入する．

③ 設定フェーズ

プログラムの導入を行ったあと HiGATE と BCF/Vista に必要な設定を行う．この時プログラム製作者は管理者ユーザの権限で設定を行う．

(1)BIOS の設定

PC 上にインストールされた Windows Vista 以外の OS が起動できないように，以下の設

定をBIOSに対して行うこととした.「BIOSパスワードを設定する」「ブートするストレージをHDDに限定する」なお,BIOSパスワードはプログラム製作者のみが知っているものとする.

(2)ユーザアカウントの設定

操作者がPCを操作する時に利用するユーザアカウントからWindowsサービスやタスクスケジューラを操作できないようにするために,ユーザアカウントには管理者権限を与えない.

(3)各プログラムのインストール

BCF/Vistaを構成するコントローラのプログラムファイル,エージェントのプログラムファイル,ホワイトリストのファイルのインストールを行う.これらのファイルは,後述するBitLockerによって暗号化されたドライブに保存した上で,ユーザアカウントから書き換えや削除ができないように読み取り専用として設定する.

(4)BitLockerの設定

BitLockerとは,ドライブを暗号化するWindows Vista Ultimateの機能である.攻撃者がPCのHDDを取り出して別のPCでBCF/Vistaを構成するプログラムを変更できないようにするために,BitLockerを使ってHDDに存在するドライブの全てを暗号化する.

(5)Windowsサービスの設定

コントローラをWindowsサービスに登録するため,株式会社軟式のフリーウェアsexeを利用した.登録した際は,MonitoringControllerという名前で登録した(以下,MCサービス).こうすることで,Windows Vistaが起動した後に,コントローラが自動で起動するようになる.しかし,このままではユーザアカウントがセーフモードでログインしてしまうと,MCサービスが起動しない.そこで,Windowsレジストリに MCサービスの情報を追加することで,セーフモードでもMCサービスが起動するようする.

(6)タスクスケジューラの設定

タスクスケジューラを使ってエージェントがユーザアカウントのログインと同時に起動するようにする.

これら6つの設定を行った後,HiGATEの開封可能ポイントすべてに開封防止ラベルを張る.

④ 使用フェーズ

使用者は設定が行われたHiGATEを使用する.このとき使用者は管理者権限のないユーザアカウントを使用する.

これらが運用フェーズである.関与者たちをこのような役割に配置することで関与者による不正をなくすことができる.HiGATE使用者は管理者権限を持っていないため,データに対して不正を行うことは難しい.また,プログラム製作者はHiGATEを持っていないために使用者が扱うデータに何かしらの不正を行うことはほぼ不可能である.よって関与するすべての人間がHiGATEを使用し扱うデータに対して不正を行うことができない.これはBCF/Vistaの管理者が不正をしないという前提条件を可能とするシステムである.

5 e-Discoveryへの適用

この節ではHiGATEをe-Discoveryへ適用を行う.またここで扱う e-Discovery システムは高塚らが提案した「開示情報の墨塗りと,証拠性の確保を両立する e-Discovery システム」[1]とする.

5.1 e-Discovery

e-Discoveryとは,2006年12月,連邦民事訴訟規則(FRCP)が改正され,米国の民事訴訟において,企業は民事訴訟の審理開始前に行われる証拠開示(Discovery)の際に,電子証拠を開示することが義務付けられた.これが電子情報開示「e-Discovery」である[5][6].e-Discoveryの基本的流れを図2に示す.

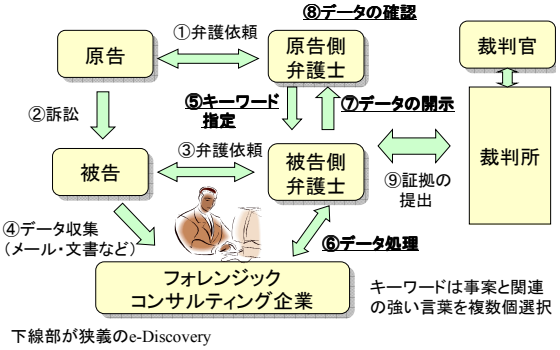

図2. e-Discoveryの手順

5.2 高塚らが提案するe-Discoveryシステム

最初に原告側が被告側に事案と関係のあるキーワードを指定する.その後,被告側はそのキーワードを使用し,事案と関係のあるファイルを開示する.しかし,この時,会社の機密情報などどうしても開示したくない情報が含まれる場合がある.これを解決する方法として電子的墨塗り技術[4]を使用する.被告側はキーワードを含まない文書にはすべて墨塗りを行い,キーワードを含む文書で,かつ,どうしても隠したい部分がある場合部分的に墨塗りを行う方式にした.このように行うことによって,必要最低限のデータのみを開示

することが可能になる．しかし，現存する墨塗り技術では墨塗りを行った場所にキーワードが含まれている可能性があり，それを確認することがほぼ不可能に近い．高塚らはその問題を墨塗りの内データを暗号化することによって解決した．暗号機能付き墨塗り処理を行ったデータ類は原告側に開示する．原告側はそのデータを受け取り，データの確認を行う．この時，墨塗り内にキーワードが含まれていないことを確認する．

しかし，その過程で墨塗り箇所の復号結果を不正に見られてしまう可能性がある．そこで，耐タンパを持ったセキュリティデバイスを使用し，中間結果を見られないようにする．このセキュリティデバイスとしてHiGATEを用いる．ここではHiGATEにおいてe-Discovery向けに開発したプログラム部を含むHiGATEをHiGATE/e-Discoveryと呼ぶ．

5.3 HiGATE/e-Discoveryの運用

この項ではHiGATEをe-Discoveryに適用した際の運用を記述する．HiGATEを適用する場所は，セキュリティデバイスとしてHiGATEを使用する．HiGATEを適用することによって，原告側のデータ類への干渉と処理時間などのスマートカードの問題点を解決することができるためである．

1) HiGATE/e-Discoveryの製造とプログラムロード
   製造者がプログラム開発者にHiGATEを渡す．プログラム開発者はe-Discovery用ソフトをHiGATEにロードする．e-Discoveryのソフトの機能としては，キーワードファイルの署名検証，墨塗り部分の復号，復号部分のキーワードの有無の検証，証拠性の検証，事案と関係のあるファイルの抽出など計５つの機能を持ったプログラムである．
2) HiGATE/e-Discoveryの設定
   HiGATEの設定に関しては4項で記述したことを行う．またe-Discoveryのキーワードの受け渡し，原告側と被告側の相互の公開鍵の交換なども行う．
3) HiGATE/e-Discoveryの使用
   原告側は被告側から受け取ったデータをHiGATE/e-Discoveryに入力し，プログラムの実行を行う．これにより，墨塗り部にキーワードが含まれていないかどうか確認することができる．その後，事案と関係のあるデータのみを閲覧し，裁判を行う．

これらの検討を通じ，e-Discoveryに対し，HiGATEが適用可能である見通しを得た．

6 おわりに

本稿では，耐タンパ機能を有し，ハードウェアの持ち主であっても改竄できず，入出力や演算処理が早く，大量データの蓄積が可能であり，またプログラミングがとＰＣと同様にでき，安価かつ容易に開発できるハードウェアを提案した．この試作を行い，e-Discoveryへ適用した結果を報告した．

今回開発したHiGATEの基本プログラムは最低限の機能しか持っておらず，今後拡張を行い，使いやすさと安全性の向上を図りたいと考えている．HiGATEはファイルや処理に対して管理者が関与していないことを証明する技術が必要な場面に対しての適用ができると考えている．e-Discovery以外にも，疫学調査のデータマッチングなど多分野に適用できると考えている．

参考文献

[1] Mitsuyuki Takatsuka, Masataka Tada, Ryoichi Sasaki “Proposal of the e-Discovery System for Sanitizing Disclosure Information and for Securing Evidence” The 2007 International Workshop on Forensics for Future Generation Communication Environment (2008)

[2] Yuki Ashino,Ryoichi Sasaki “Proposal of Digital Forensic System Using Security Device and Hysteresis Signature” The Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (2007)

[3] Keisuke Fujita, Yuki Ashino, Tetsuro , Uehara, Ryoichi Sasaki “Proposal of Digital Forensic System with a Boot Control Function against Unauthorized Programs” 4th Annual IFIP WG11.9 Conference on Digital Forensics (2008)

[4]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

[5] ＩＴ用語辞典 e-WORD デジタルフォレンジック【digital forensics】 http://e-words.jp/w/E38387E382B8E382BFE383ABE38395E382A9E383ACE383B3E382B8E38383E382AF.html,2008.2

[6]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,2008.2

[7] Yuki Ashino, Keisuke Fujita, Maiko Furusawa,Tetsuro Uehara, Ryoichi Sasaki “Extension and Evaluation of Boot Control for a Digital Forensic System” 5th Annual IFIP WG11.9 Conference on Digital Forensic (2009)