1. インフォメーションハイディングの概要

松本　勉　横浜国立大学大学院環境情報研究院
tsutomu@mlab.jks.ynu.ac.jp

■インフォメーションハイディングとは

◇古くて新しい技術

インフォメーションハイディング（Information Hiding）とは，直接的には「情報を隠す」セキュリティ技術全般を指すが，密かな情報伝達手段であるステガノグラフィ（Steganography）や，情報の改ざん検出や追跡の手段であるウォーターマーキング（Watermarking）とフィンガープリンティング（Fingerprinting），さらにその他の技術を含む裾野の広い技術領域を指す言葉でもある．各種のインフォメーションハイディング技術はさまざまな分野において多様な目的を持って開発されてきたために，あるいは，これらの技術自体がオープンな研究に馴染まないという認識が支配的であったという状況のために，いろいろな概念や用語が飛び交っているのが現状であり，研究者によって整理の仕方が相当に異なるように思われる．本稿では，インフォメーションハイディング（以下，情報ハイディングと記す）の概念について，研究仲間との日頃の議論を通じて得た筆者の考えに基づき，説明を試みる．

◇隠したい情報と隠す場所

情報ハイディングにおいて，「隠したい情報」と「情報を隠す場所」を指し示す言葉が必要である．たとえばビット列を画像に隠す場合は，隠したい情報がビット列で，隠す場所が画像である．しかし，この場合の画像も情報ではないかと考えると，言葉の整理が必要だということが明らかである．そこで，「情報を隠す場所」が情報であっても，その表現方法自体に関心があることを考えて，「情報を隠す場所」のことを，「情報を隠すメディア」と仮に呼ぶことにしよう．

◇情報とメディア

一般に，情報を表現する手段，すなわち情報を伝える媒体である，

(1) 紙やモノ，
(2) ディジタルな（電子的な）オブジェクトである，データ，画像データ，映像データ，音楽データ，テキスト，ハイパーテキスト，プログラム，回路データ，インターネットプロトコル，暗号・署名方式，暗号プロトコル，システム，

他，を「メディア」と呼ぶことにする．これらはキャリアと呼ばれることもある．さて，ここでいう情報そのものの表現には階層がある．たとえば人間が直接扱いやすいテキスト，音，画像，映像などをとってみると，**図-1** のようにさまざまな情報の表現の階層があり，したがって情報ハイディングにおける「情報を隠すメディア」をどの層のメディアとするかにも図-1 の太い矢印のような多様性があることが分かる．

◇埋込データとカバーメディアとステゴメディア

「隠したい情報」の表現は通常あまり問題ではないので，「隠したい情報」のことを単純に「埋込情報」（embedded information）といったり，メディアの代表としてデータという用語を用いることとして，「埋込データ」（embedded data）といったりする．

これに対して，埋込データを隠すメディアのことを「カバーメディア」（cover media）という．メディアを具体的に指定したい場合は，たとえば，一般的にデータといいたい場合には「カバーデータ」，画像だということを陽に示したい場合には「カバー画像」，テキストやプログラムやプロトコルの場合はそれぞれ「カバーテキスト」，「カバープログラム」，「カバープロトコル」といった具合である．

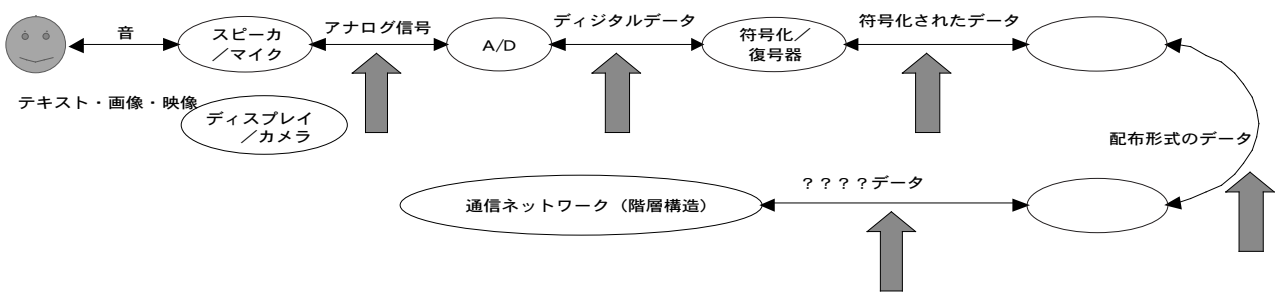


図 -1　情報ハイディングのなされる場所

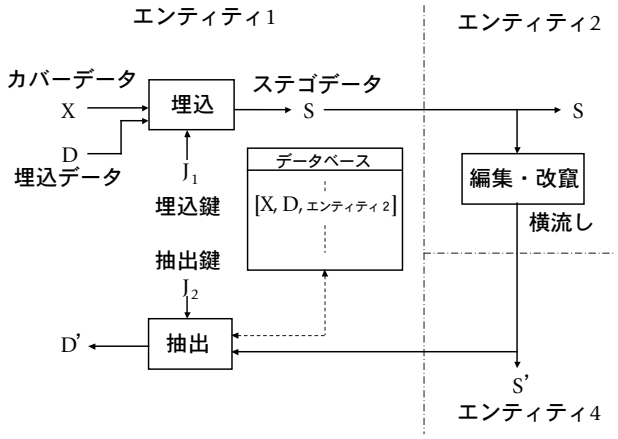


図 -2　情報ハイディング（1）

ところで，埋込データをカバーメディアに隠したとき，埋込データと一体化したカバーメディアが生まれるわけであるので，それを指し示す用語も必要である．これを「ステゴメディア」(stego media) という．メディアに応じて，ステゴデータ，ステゴ画像，ステゴテキスト等の言葉も使われる．

以下，本稿では誤解の恐れのない限り，「埋込データ」，「カバーデータ」，「ステゴデータ」を例として用いて説明をすることにする．

◇埋込と抽出と鍵

さて，埋込データとカバーデータからステゴデータを作成することを「埋込」(embedding) といい，ステゴデータから埋込データを復元することを「抽出」(extraction) という．抽出の際にカバーデータが用いられる場合もある．ここで 1 つ考えなければいけないことがある．それは，埋込や抽出が誰でも実行できてよいのか，という点である．埋込や抽出の具体的方法，すなわち情報ハイディングの方式を非公開にしておき，方式を知っている者だけが埋込や抽出を行えるとする考え方がある．しかし，採用している情報ハイディングの方式がいったん知られてしまったらそれでもうその方式は使えないことになるので，通常は，「埋込鍵」(embedding key)，「抽出鍵」(extraction key) という知識を用意して，埋込鍵が使える場合には埋込ができ，そうでない場合には埋込ができず，抽出鍵が使える場合には抽出ができ，そうでない場合には抽出ができない，というメカニズムを導入することが多い．埋込鍵と抽出鍵を総称して「ステゴ鍵」(stego key) という．以上をまとめると，**図 -2** および **図 -5** のように表すことができる．

◇情報ハイディングと暗号

一般に，ある知識，すなわち「鍵」が利用できるか否かによってある作業が効率よく実行できるかできないかを制御する情報セキュリティ技術を総称して「暗号」(Cryptography) という．このように考えると，情報ハイディング技術は暗号の特別なクラスに相当すると考えられる．ところが，暗号を，メッセージを通常とは別のデ

ータ（暗号文）に変換して情報セキュリティを達成しようとする技術である，と狭義に捉えるならば，情報ハイディング技術で，暗号に属さないものがあると，考えることもできる．暗号文を見てもメッセージの意味が分からないという技術が暗号で，ステゴデータを見ても埋込データが存在しているかどうか分からないという技術が情報ハイディングである，といった解釈が，この意味では成り立つ．しかしこのような解釈しか許さないとすると，情報ハイディングの持つ多様な特性を語るには少々窮屈であると筆者は考える．

■情報セキュリティ

◇ 情報セキュリティの項目

ここで発信された情報の管理にあたって必要とされる情報セキュリティのいくつかの項目を示そう．発信された情報は，文書，音楽，画像，映像，プログラム等さまざまであろうが，ここではこれらを総称して，単にメッセージと呼ぶことにする．

(1) エンティティの認証：受け取ったメッセージの文面には付随情報として作成者であるエンティティ（人または組織）の名前などが書かれていたとする．作成者が本当にそのエンティティなのかが確認できることを「エンティティ認証」ができるという．

(2) メッセージの認証：メッセージが作成されたときから変わっていないか確認できることを「メッセージ認証」ができるという．

(3) メッセージの追跡：メッセージが作成されたままでなかったとしても，作成時のメッセージとの対応がとれることを「メッセージの追跡」ができるという．

(4) メッセージ内容の守秘：メッセージ内容が意図した相手以外には「読めない」（聞けない，見えない）ようにできることを「メッセージ内容の守秘」が保たれるという．

(5) メッセージ存在の秘匿：メッセージが存在しているのか否かが意図した相手以外には判定できないようにできることを「メッセージ存在の秘匿」ができるという．

これら以外にも，メッセージの授受に関する紛争の解決とか，メッセージがある時刻に存在していたことの証明とか，さまざまな情報セキュリティの項目がある．

◇ モノの性質を利用した古典的技術

メッセージと一体化した紙などのモノを運ぶことによってメッセージを伝えるのが，伝統的な通信や保管の方法であった．メッセージが紙などに書いてあって，手書き署名や捺印があればその手書き署名や印鑑を照合することによって，エンティティ認証ができるであろう．

メッセージを一部分消して書き換えるというようなことが行われれば，その痕跡が残るために検出できるだろうし，書き換えでなく追記がなされたとしても，前から書かれていた部分と追記された部分でインクの経年変化の様子が異なることなどで見分けがつくから，メッセージ認証もできる．残された痕跡を手がかりに，メッセージの追跡もできる．

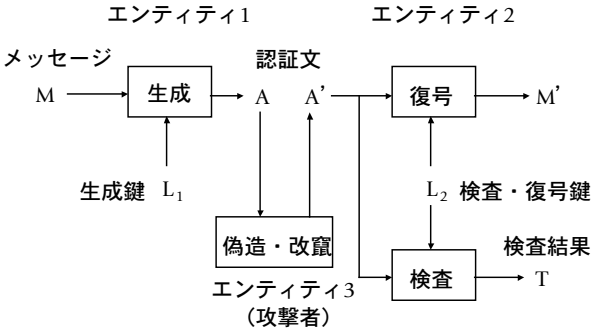


図 -3　暗号による認証方式

メッセージと一体化したモノを，金庫などに入れて物理的に保護した状態で輸送することにより，メッセージの守秘が達成できる．あぶり出しや水にぬらすと文字が現れるインクを使えばメッセージ存在の秘匿もできる．

◇ モノと切り離された発信情報の管理

IT 技術の進展に伴い，情報としてモノとは切り離された状態で，電気や光などの物理現象を利用して蓄積したり伝送したりすることがきわめて楽にできるようになった．モノと切り離された情報を保護するには，情報そのものに細工を施さなければならないことは明らかであろう．すなわち暗号が必然的に登場する．暗号とはすでに情報ハイディングと暗号の節で述べたが，エンティティ認証やメッセージ認証やメッセージの守秘のための方法として情報そのものに細工を施し，鍵が利用できるか否かがポイントとなる技術である．暗号について以下で概観する．

なお，モノと情報がまったくかかわらないという世界は現実には考えにくく，中間的な場合ももちろん無視できず，プリント文書，銀行券，ID カード，パスポート，証書，その他のきわめて多様で重要な技術領域があるが，本稿の範囲を超えるのでこれ以上は触れない．

<u>暗号による認証</u>

暗号は認証の実現のために利用できる（**図 -3**）．ある知識 L2 による検査に合格しかつ L2 によりメッセージ M に戻る認証文 A を，与えられた M に対して生成することが，L2 に対応する知識 L1 を用いれば容易であるが貧弱な知識では非常に困難であるという仕組みを認証

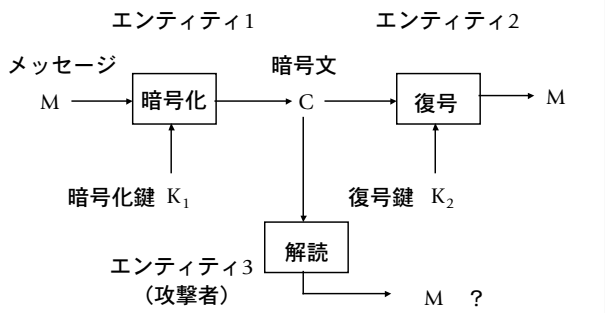


図 -4　暗号による守秘方式

系といい，L1 を生成鍵，L2 を検査鍵という．生成鍵 L1 によるメッセージ M の認証文 A への変換を認証文生成，検査鍵 L2 による，受け取られた認証文 A’ の M’ への変換を復号，A’ の検査を認証文検査という．検査結果 T は，合格，不合格の 2 値をとり，T が合格のとき，A’ ＝ A かつ M’ ＝ M であると判断する．

認証文には，L1 と圧縮した M とに依存する短い認証子 S を M に連接させた形式 [M, S] を用いることが多い．送り主であるエンティティ 1 が M に対し L1 により生成した A を，L1 を利用できない攻撃者が改変や破壊して A’ に変えたり別の認証文 A’ を偽造したりしても，あて先のエンティティ 2 は L2 によりそれを検出できる．つまり，認証文の送り主が L1 を持つ者か否かを検査するエンティティ認証と，復号メッセージ M’ が送り主が送出した M か否かを確認するメッセージ認証が行える．

生成鍵が検査鍵に等しいか検査鍵から簡単に導ける認証系を対称認証系または共通鍵認証方式という．一方，検査鍵から生成鍵を導出するために莫大な計算量がかかると信じられ検査鍵を公開してもよい認証系を非対称署名系または公開鍵（ディジタル）署名方式という．「署名」が用いられるのは，認証文を作れる者が生成鍵を利用できる送り主だけであり，生成鍵の使えないエンティティ（あて先も含む）には行えないため，認証文がメッセージに対する送り主の「署名」の機能を持つからである．認証文を署名文，または（ディジタル）署名という．署名文 A の形式も，[M, S] という分離型とそうでない一体型とがある．

暗号による守秘

暗号は，守秘の手段としても利用できる（**図 -4**）．ある知識 K1 により暗号文 C に変換されたメッセージ（平文）M を C から復元することが，K1 に対応する知識 K2 を用いれば容易であるが，貧弱な知識では困難である仕組みを暗号系といい，K1 を暗号化鍵，K2 を復号鍵という．K1 による M の C への変換を暗号化，K2 による C の M への変換を復号という．

指定あて先のエンティティ 2 が K2 を使えるようにしておけば，K1 を利用できるエンティティ 1 は M を C に暗号化して送り出すことにより，K2 を利用できない攻撃者には内容を知られることなくエンティティ 2 だけに情報を伝えられる．攻撃者が C を M に戻そうと努力する行為を解読といい，復号鍵 K2 を求めようとする行為も含む．「復号」と「解読」は異なることに気をつけていただきたい．

復号鍵が暗号化鍵に等しいか暗号化鍵から簡単に導ける暗号系を対称暗号系または共通鍵暗号方式という．

一方，暗号化鍵から復号鍵を導出するために莫大な計算量がかかると信じられ暗号化鍵を公開しても使える暗号系を非対称暗号系または公開鍵暗号方式という．

■情報ハイディングの登場（図 -5 参照）

◇コンフィデンシャリティの問題の所在

メッセージ M の存在の秘匿を達成しようとしたとき，暗号化で十分であろうか．通常，暗号文は乱数のように見えるものが普通であるので，メッセージ自体が乱数のようなデータであれば，通信路上を見ていても流れてくるデータが何らかのメッセージに対応する暗号文なのか，それともただの乱数なのか区別をつけることは困難である．このような場合には，通常の暗号化で十分である．たとえば，暗号の鍵を配送するプロトコルなどではこのような状況が利用できることがある．しかし，多くの場合，乱数のようなデータが観測されれば，それが暗号文である可能性が高く，それを復号してメッセージを得ることはできないまでも，暗号文であること，つまり，何らかのメッセージが存在していること自体は知ることができるであろう．よって，情報ハイディング技術が登場する．

◇ステガノグラフィとステガナリシス

情報が通信されていること自体を隠すことを目的にした情報ハイディング技術を，「ステガノグラフィ」(Steganography) という．ステガノグラフィにおいて主役は埋込データであり，カバーメディアは攻撃者にとって不自然に見えない媒体であれば何でもよい．計算機システムから外部への情報漏えいのシナリオではカバーチャネル（covert channel）という用語が，また，暗号方式や署名方式のプロトコルを利用する場面ではサブリミナルチャネル（subliminal channel）という用語が使われることもある．

与えられたデータがステゴデータであるかそうでないかの「判定」，あるいは，「検出」が，抽出鍵なしに行え

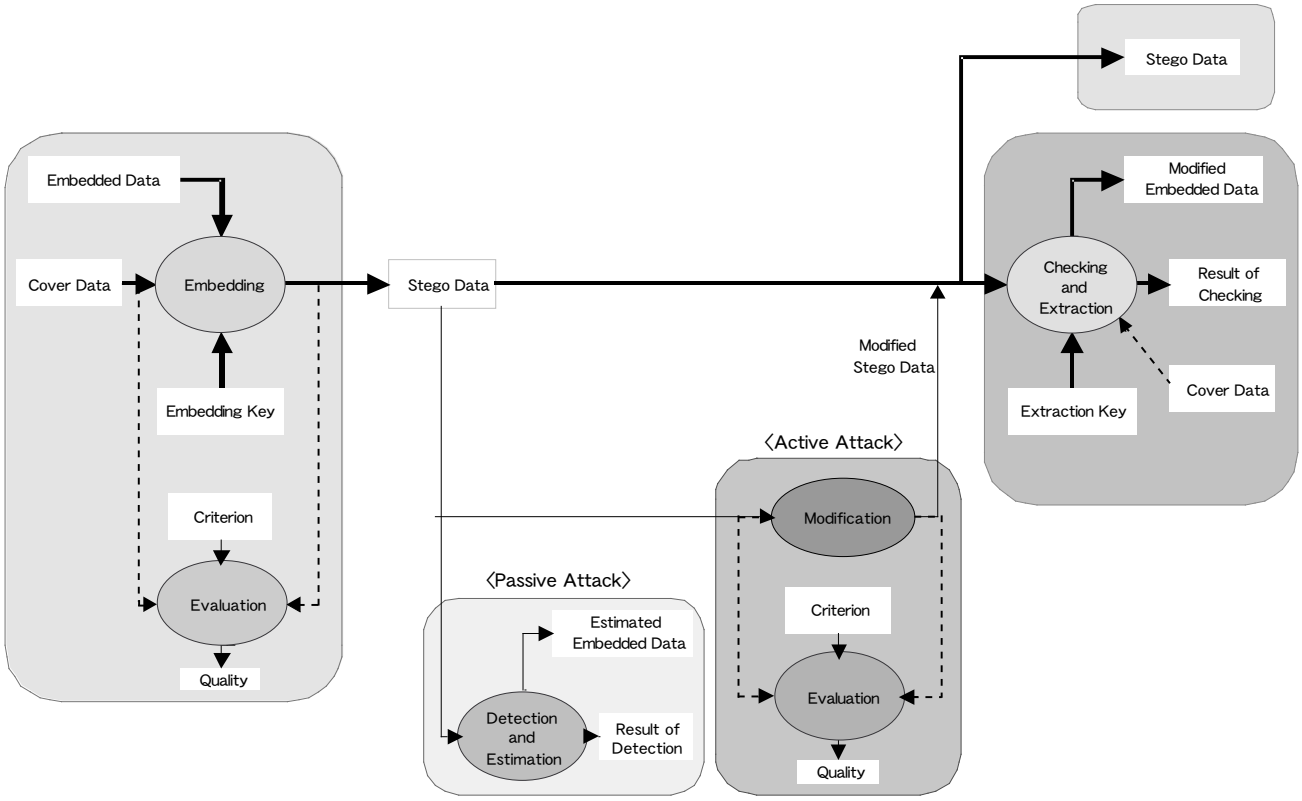


図 -5　情報ハイディングの全体像

るかどうかがポイントとなる．また，検出はできなくても，通信されているデータがステゴデータであった場合にそれを介して通信している者に情報伝達を許さないという目的で妨害を加えることもあり得る．これを「無効化」といい，完璧に防ぐことは困難である．これは後述のインテグリティ問題のための方式における「耐性」と対応する．検出や無効化といった攻撃のことを「ステゴ解析」または「ステガナリシス」(steganalysis) という．

◇インテグリティの問題の所在

メッセージＭが，音楽コンテンツや映像コンテンツあるいはプログラムやその他の著作権管理を必要とするものであった場合，普通の暗号系や認証（署名）系だけでは，メッセージの追跡ができるとは限らない．たとえば次のような状況を考えよう．保護対象のデータＸにＸの管理情報Ｄ（著作権者名や配布先名などのデータ）を付加したものをメッセージＭとし，これに対して認証文Ａを生成し，Ａを暗号化して利用者に配信することを考える．復号ができるのは料金を払う利用者だけとしたいので，通常，耐タンパーモジュールというハードウェアまたはソフトウェアで，内部の不正読み出しや不正改ざんができない環境を用意する．耐タンパーモジュールの中に復号機能を実現し，料金を払った者だけが復号機能を働かせられるようにする．また，暗号文の復号の結果得られる認証文Ａの検査・復号も行い，得られたコンテンツ管理情報Ｄに矛盾しないようにデータＸの利用を管理する．

しかし，このような仕組みでは，いったん耐タンパーモジュールからデータＸが出力されたなら，Ｘが横流しされても追跡できない．Ｘを微妙に細工または編集して，品質としては同等のコンテンツデータＹに変えて巧妙に海賊版を作られれば，ＹがＸに由来するものだということをデータレベルで証明することはきわめて難しい．

◇インテグリティ技術としての情報ハイディング方式

そこで，情報ハイディングの登場となる．すなわち，保護対象データＸをカバーデータとし，その管理に用いる情報などを記した埋込データＤとＸとを一体化させ，その結果できたステゴデータＳはそのままでＸと同じようにコンテンツあるいはプログラムなどとして利用できるようにすることが考えられる．つまり，埋込デ

ータを秘密にしておくこと自体よりはむしろ，埋込データとカバーデータとを分離困難なように結合する目的に情報ハイディング技術を使うのである．これが情報ハイディングによるデータ追跡のアイディアである．**図-6** および図-2 を参照されたい．このような方法は，ウォーターマーキング，電子透かし，ディジタル透かし，データハイディング，フィンガープリンティングなどと呼ばれることもあり，埋込データは，ウォーターマーク，透かしデータ，あるいはフィンガープリント（指紋）などと呼ばれることもある．このタイプの情報ハイディングのための方式は通常，次の条件を満たすことが求められる：

(1) 品質：あらかじめ定めておいた品質評価基準 R に照らしてステゴデータ S がカバーデータ X と同等の品質を持っているとの結果 Q が得られること（図-6 参照）．ここで，同じ品質を持つとは，たとえばステゴデータが音楽を表していれば，受容者である人間にとって同じように聞こえることを，また，ステゴデータが画像を表している場合には，同じように見えるということを指す．テキストデータの場合には元のテキストの意図を損なわないことであり，プログラムの場合にはその機能が変わらないことである．たとえば入力された暗号文を内蔵する秘密の復号鍵を用いて復号するプログラム（デコーダ）はステゴプログラムになっても暗号文の復号に関してはカバープログラムと同じ機能を有している必要がある．このデコーダに関する技術は「不正者追跡」(traitor tracing) という名称で研究されている．

(2) 耐性：ステゴデータに対して攻撃者が行う可能性のある改ざんに対して，十分な強度を維持していることが必要である．すなわち，ある 1 つの未知のカバーデータに対して作られた 1 つまたは複数のステゴデータが与えられたとき，そのどれとも埋込データが異なるが同じ品質を持つデータを作成することが攻撃者にとって困難であることが必要である．あるカバーデータと同じ意味を持つデータが与えられたとき，それがどのステゴデータに由来するものであるのかが正しく判定できれば，攻撃を受け「横流し」されたデータの追跡に役立てられるため，攻撃者の特定や不正行為の抑止に効果を発揮し得るからである（図-2 参照）．

ただし，保護対象のカバーデータ内の多数の部分に耐性が低いかたちで埋込データを埋め込み，もしカバーデータに改ざんが行われたなら，どの部分が攻撃を受けたのかを明らかにするといった，壊れやすい電子透かしの方法（fragile watermarking）も考えられている．

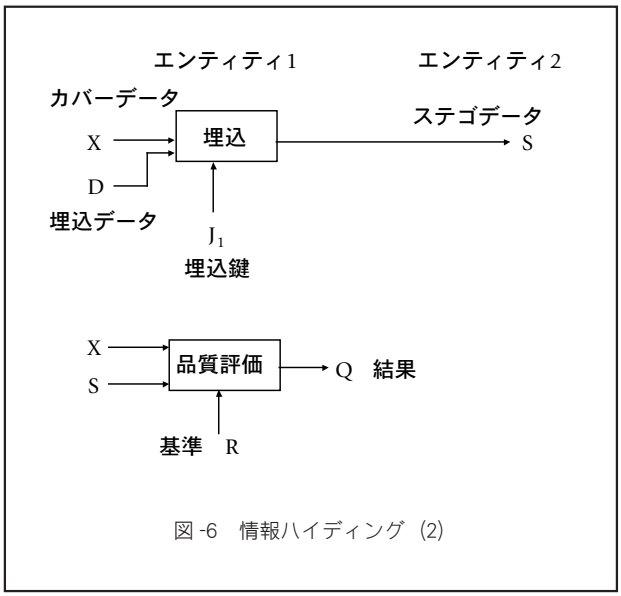


図-6 情報ハイディング（2）

ウォーターマーキングとフィンガープリンティング

「電子透かし；ウォーターマーキング」(Watermarking) は，「透かし」というアナロジーからも示唆されるように，埋込データに著作権者名を含む情報ハイディング方式を指し，主としてカバーデータの作成者側の情報がステゴデータから分離できないようにすることを狙った応用に用いられる言葉である．これに対し，「フィンガープリンティング」(Fingerprinting) は，たとえば書類を素手で受け取ると書類に指紋がつき，誰が受け取ったかが後で分かるようになるのと同じように，あるデータを多数のエンティティにネットワーク等を介して配布する際に，あるエンティティに配布したステゴデータと別のあるエンティティに配布したステゴデータとが区別できるように，ステゴデータを個別化する方式を示す．もちろん，フィンガープリンティングの場合の埋込データとして配布者側の情報を入れることもできるから，フィンガープリンティングの特別な場合としてウォーターマーキングがあるともいえよう．

ステガノグラフィ，ウォーターマーキング，フィンガープリンティングの方法

● カバーデータの種類に依存する部分

カバーデータ，ステゴデータがどんなメディアであるかに応じて埋込の方法は千差万別である．ただし，基本は，カバーデータに存在する冗長性を利用し，異なった表現ではあるがほぼ同じ品質のデータを作成するというものである．

● 埋込データの符号化：結託耐性符号

埋込データにどのようなパタンを用いるか，すなわち，埋込データにはどのように冗長度をつけるかが問題となる．これは，符号（code）の問題になるので，組合せ論が活躍する領域である．無効化に対抗したり耐性を上げるためには誤り訂正符号が活躍する．

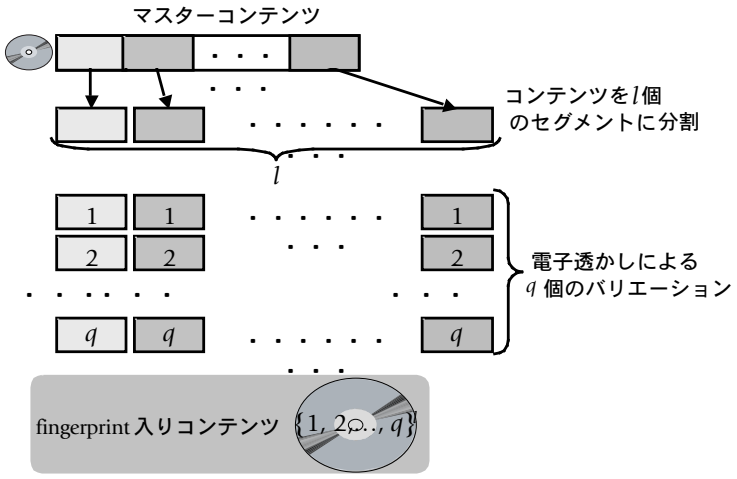


図 -7　q 元符号によるフィンガープリンティングの例

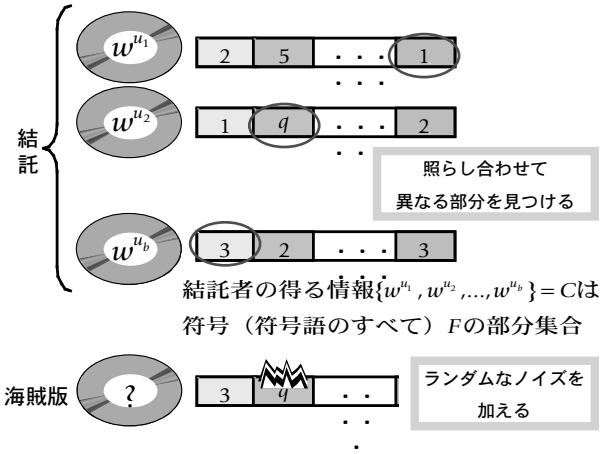


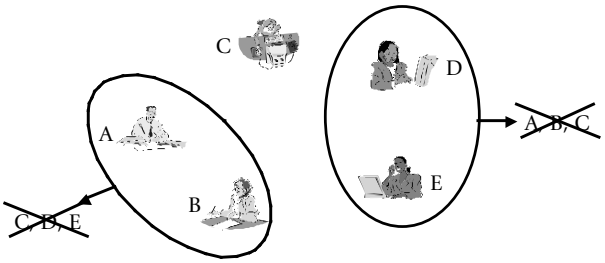
図 -8　攻撃

また，フィンガープリンティングのためには符号（符号語（＝数値の組）の集合）を用意し，たとえば，**図 -7** のようにカバーデータに埋め込む．この例ではカバーデータをマスターコンテンツと表示している．マスターコンテンツを複数のセグメントに分け，各セグメントを符号語の対応する成分の値に応じて変形する．このようにしてできたコンテンツがステゴデータである．ステゴデータは符号語の個数だけ作ることができるので，たとえば利用者 1 には 1 番目の符号語を割り当て，利用者 2 には 2 番目の符号語を割り当てて，というようにできる．ステゴデータを入手した利用者の何人かが結託すると**図 -8** のようにして個々のステゴデータの違いを見て違いがあるセグメントを変更することにより品質のあまり変わらないデータを得る．このデータから攻撃者たちの身元が割れなければ攻撃者側の勝ちである．符号の種類により，さまざまなタイプの攻撃への耐性が考えられている．**図 -9** ～**図 -13** を参照されたい．

■機能面から見た情報ハイディング技術の位置づけ

以上をまとめて，各種の情報セキュリティ技術の中での情報ハイディング技術のそれぞれは次のように位置づけられるのではないかと考える．

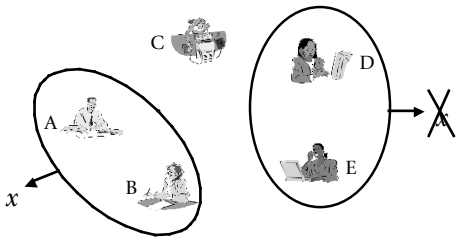
c人までの結託によっても結託者以外に配られた
符号語を作れない符号を*c*-frameproof符号という.



2-frameproof 符号の例

図 -9　c-frameproof 符号

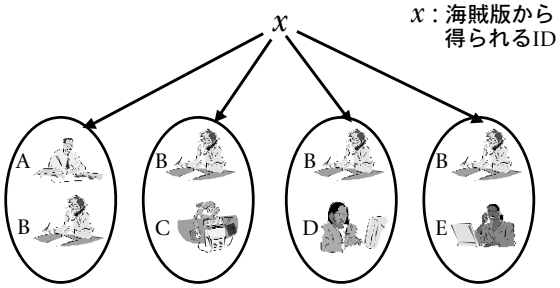
攻撃に対して以下のような性質を持つ符号を
c-secure frameproof 符号という.



2-secure frameproof 符号の例

図 -10　c-secure frameproof 符号

c人までの結託攻撃に対し以下のような性質が成り立つ
符号を*c*-IPP符号という



x を作ることができる結託のリスト

図 -11　c-IPP 符号

c人までの結託攻撃に対して以下のような性質を
持つ符号を*c*-TA符号という

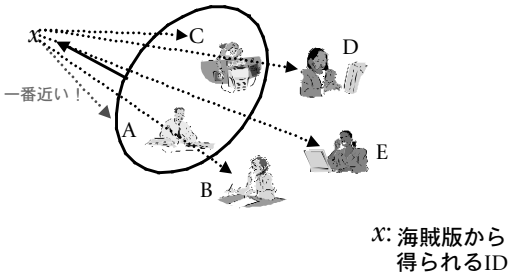


図 -12　c-TA 符号

x を入力として，*F* の符号語1つを出力するアルゴリズ
ムTを追跡アルゴリズムと呼ぶ.

以下が成り立つような追跡アルゴリズムT(*x*)が存在する
とき，符号*F*はtotally *c*-secure 符号であるという.

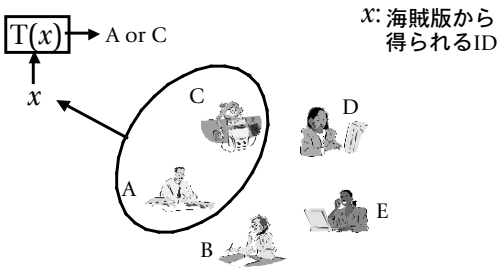


図 -13　c-secure 符号

◇インテグリティのためのメカニズム

(1) 情報を消去・改変・偽造することが非権限者にとって困難であることをねらう技術

●情報とメディアのバインディング技術としての情報ハイディング技術（制約条件：ステゴデータの利用可能性を維持しつつ）

○ウォーターマーキング Watermarking

○フィンガープリンティング Fingerprinting

○トレイタートレイシング Traitor Tracing

○機能改変困難性のある耐タンパーソフトウェア Tamper Resistant Software

●誤り訂正符号（鍵なし）Error Correcting Codes

(2) 情報の消去・改ざん・偽造を検出することをねらう技術

●情報ハイディング技術

○フラジャイル・ウォーターマーキング Fragile Watermarking

●暗号による認証メカニズム

○ MAC（共通鍵認証方式）Message Authentication Codes

○ディジタル署名（公開鍵署名方式）Digital Signature Scheme

●誤り検出符号（鍵なし）Error Detecting Codes

◇コンフィデンシャリティのためのメカニズム

(1) 情報が運ばれているかどうかの判定が当事者以外には困難であることをねらう技術

●通信の存在を秘匿するための情報ハイディング

○ステガノグラフィ（伝えられるデータの姿を加工）Steganography

○サブリミナルチャネル（暗号プロトコルをメディアとする）Subliminal Channel

○カバートチャネル Covert Channel

○追跡困難通信 Untraceable Communication

○匿名通信（送信者匿名性，受信者匿名性，・・・）Anonymous Communication

●スペクトル拡散通信（無線信号の検出自体を問題にする）Spread Spectrum Technology

(2) 情報の内容を知ることが困難であることをねらう技術

●暗号による守秘メカニズム

○共通鍵暗号 Common Key Cryptosystems

○公開鍵暗号 Public Key Cryptosystems

■課題

情報ハイディングの各種の技術はすでに各所に適用されているが，採用されている埋込や抽出の方式は公表されていないことが多い．方式が分かった時点で攻撃にさらされる危険が高いという方法を採用せざるを得ないという技術レベルにあるからである．それゆえ，脆弱性あるいは安全性の評価が十分に行われていない方式，あるいは，評価結果が一般ユーザに公表されていない方式も多数利用されている模様である．そうであったとしても，著作権保護などの応用においては，攻撃者にとっては不正行為が捕捉されるおそれを否定できないので攻撃の抑止効果にはなるのだという意見もある．しかし，かつて方式を非公表とすることが常識であった暗号においては，方式を公表しても鍵さえ適切に管理すれば安全に利用できる方式が普通に使われているという現状を見れば，方式が公表されたとしても攻撃に耐えられる情報ハイディング技術の確立が，夢では終わらないようにも考えられる．そのための理論が着実に発展することを望む．

参考文献（情報ハイディングを詳しく知るためのヒント）

1) Katzenbeisser, S., Fabien, A. and Petitcolas, P. : Information Hiding, Artech House (2000).
2) Johnson, N. F., Duric, Z. and Jajodia, S.: Information Hiding, Kluwer Academic (2000).
3) Cox, I. J., Miller, M. L. and Jeffrey, A. : Bloom, Digital Watermarking, Morgan Kaufmann (1999).
4) 松井甲子雄：電子透かしの基礎，森北出版（株）(1998).
5) 情報処理振興事業協会：インフォメーションハイディングの技術調査報告書，http://www.ipa.go.jp/security/fy10/contents/crypto/report/Information-Hiding.htm (1998).
6) Information Hiding Workshop: Proceedings (Springer-Verlag: Lecture Notes in Computer Science, No.1174, No.1525, No.1768, No.2137など)
7) Neil Johnson 氏のサイトからリンクされたサイト：http://www.jjtc.com/Steganography/
8) Fabien Peticolas 氏のサイト：http://www.cl.cam.ac.uk/%7Efapp2/steganography/index.html

（平成 15 年 2 月 20 日受付）