情報セキュリティの動向について

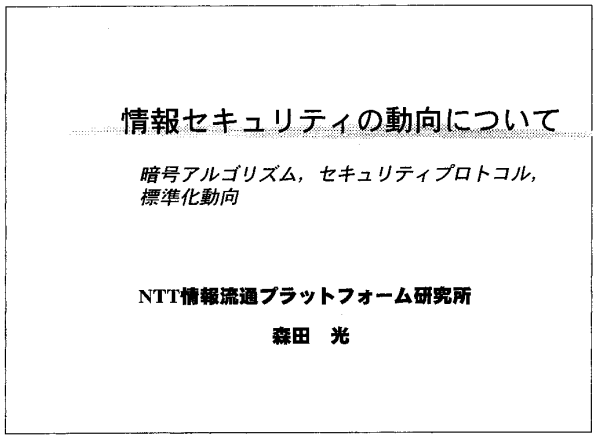
―― 暗号アルゴリズム，セキュリティプロトコル，標準化動向 ――

森田　光

司会(佐藤和洋)：それでは森田さんの講演を始めたいと思います．タイトルは「情報セキュリティの動向について」で，サブタイトルが「暗号アルゴリズム，セキュリティプロトコル，標準化動向」ということになっております．

ここで，講演にはいる前に簡単に森田さんのご紹介をさせていただきます．ご出身は東京都です．大学は北海道大学で，工学部電子工学科を昭和55年(1980年)に，そして大学院工学研究科電子工学専攻を昭和57年(1982年)にご卒業されております．それからNTTに就職され，情報セキュリティの分野一筋に研究をされております．主要な研究成果としては，暗号の安全性検証の観点からの群構造探索について，公開鍵暗号の高速化，暗号の実装，さらにはハッシュ関数の安全性検証などで，多くの論文を書いておられます．現在の役職は，NTTの主幹研究員をしつつ，電気通信大学の客員教授ということと，セキュリティ関係の委員会の幹事をやっておられるということです．それでは森田先生宜しくお願い致します．

森　田　　光　氏

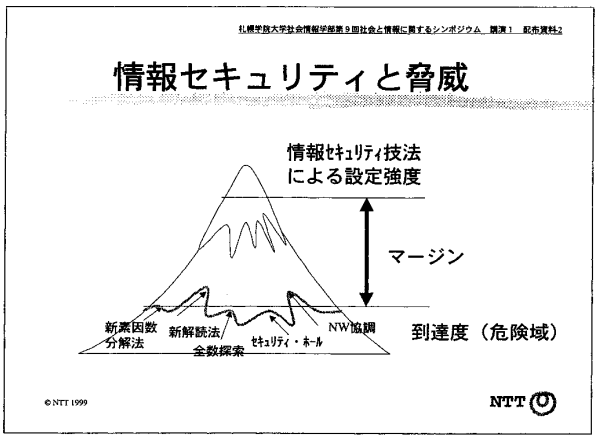


MORITA Hikaru
NTT 情報流通プラットフォーム研究所主幹研究員
電気通信大学大学院情報システム学研究科客員教授

はじめに

ご紹介に預かりましたNTTの森田です．いま佐藤先生のご紹介にあった様に，非常勤で電気通信大学大学院の情報システム学研究科情報システム運用学専攻の客員教官もやらせて頂いております．専攻の所属講座は「社会情報システム学」でして，札幌学院大学の貴学部と名称が同じであり親しみがわきます．また，理系と文系の異なるアプローチを交流させシナジー効果を狙っている点でも相通ずるところがあると思いますので，今後，つながりができればと思います．

それでは本題の「情報セキュリティの動向について」に話題を移させて頂きます．この分野はまだ技術中心であり，専門的なところですと，数式ばかりになってしまいます．本日は，本会合の趣旨にあわせ，日常生活で体感できるところから話を始め，軽く技術に触れつつ，社会との関係について述べたいと思います．

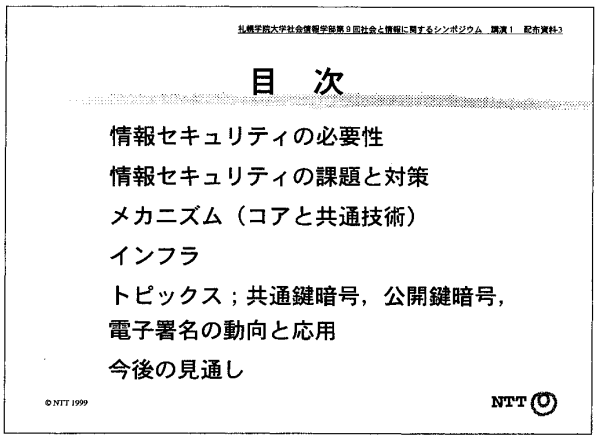


「情報セキュリティ」という分野を理解して頂くために，そのイメージをたとえ話しでお伝えしたいと思います．自分が大切にしている金塊などの宝物を隠して，泥棒から守る場合を考えて下さい．富士山，こちらで言えば羊蹄山の様な，高い山の頂上にその宝物を埋めるとします．話を簡単にする為に，宝物の持ち主は，その山が高いという事実だけで守ろうとします．

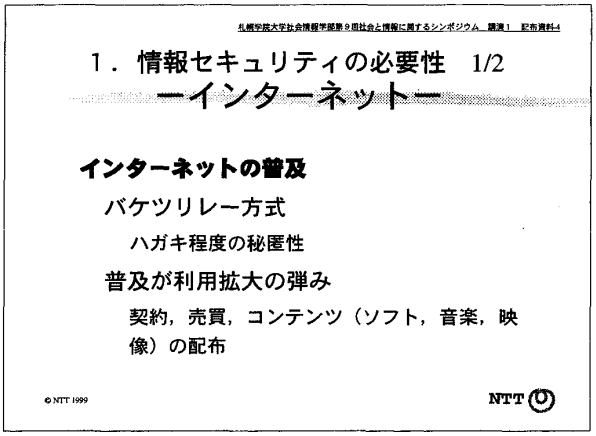
泥棒にはいろんな攻め方があります．ヘリで飛んでいく．オーソドックスな技法で登ることもできるし，素手で迅速に登る，等々．オーソドックスなアプローチでも，ルートを変えることで，攻め方が変わります．

情報セキュリティも似た所があります．新しい解読法が見つかったり，計算機の性能が上がったり，計算機を結ぶ協調計算で効果を上げたり，等々．新しいことがある度に安全性が脅かされます．従って，ある期間内では，どんなに頑張ってもここ迄しかたどり着けないという到達限界を予想し，それにマージンを加えて，設定強度を与え，いわゆる〝宝物〟を埋めることになります．

なお，守る側が，攻める側を超えて高いところに〝宝物〟を埋められる理由ですが，〝落し戸〟または〝一方向〟という暗号学的に重要な概念のお陰です．後で，少しだけ触れたいと思います．



本日の講演の目次を示します．

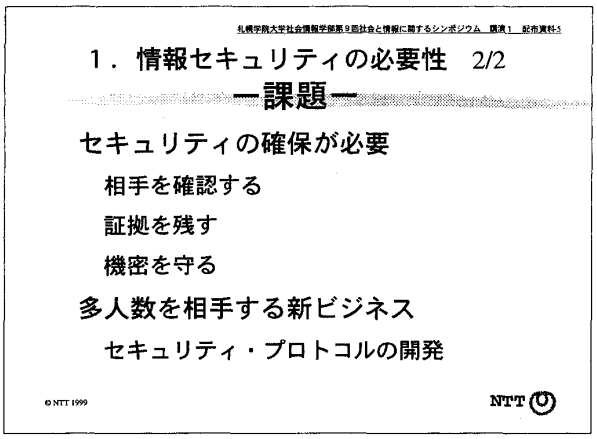


情報セキュリティというと，昔は暗号を扱う分野ということで，名前そのものは，暗号ほどポピュラーではありませんでした．しかし，最近注目されています．そのきっかけとなったのは，インターネットの普及のお陰です．

インターネットは，必ずしも大きな通信業者が一元的に提供するものではなく，大小様々な通信プロバイダが結ばれて形成されるネットワークです．その上をやり取りされる情報は，いわばハガキ程度のガードであります．亡失などの事故の責任の所在という点では，郵便に比べ劣るとさえ言えます．しかし，便利さと効率の良さから支持されているのだと思います．

元は研究者の為の通信網でしたが，数千万人規模になってみますと，一種の社会が形成され，先程，斉藤先生も言及されてた電子契約や，電子マネー，さらには音楽やゲームなどのコンテンツ配信までインターネットの上で構築されるようになっていて，その危うさは大きなものになっています．

対面処理を中心に秩序を形成してきた商取引に対して，インターネットを伝わって流れる情報だけでどう秩序を作って行ったら良いか？ まだ，我々は発展途上にあると言えないでしょうか？



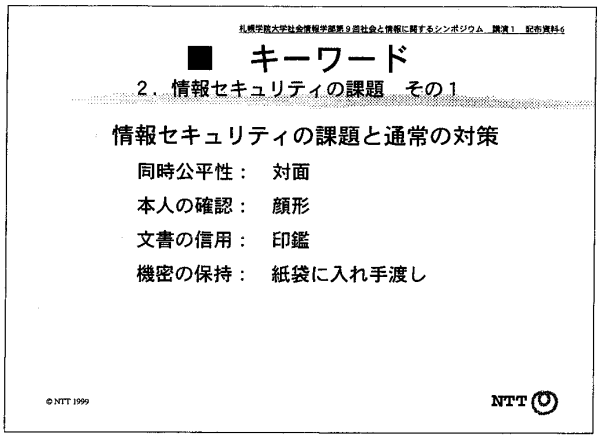
一方，最近の傾向として，携帯電話の普及があります．更に，iモードというインターネットと携帯電話を結び付ける動きすらあります．

この様な流れでは，次に挙げる3つのセキュリティの確保が重要になっています．インターネット上で画像表示はできますが，写し出された相手の顔が本物であると信じる証拠はないわけですから，どうしても情報だけで〝相手を確認〟する手段が欲しいわけです．

究極を考えると，人間を識別する手段が欲しくなるわけですが，DNA鑑定，指紋，などありますが，どれも複製可能で，信じるに足る情報手段を提供しているとは言えません．識別用のICを人に埋め込めば解決されることは多いですが，コンセンサスは得られないでしょう．

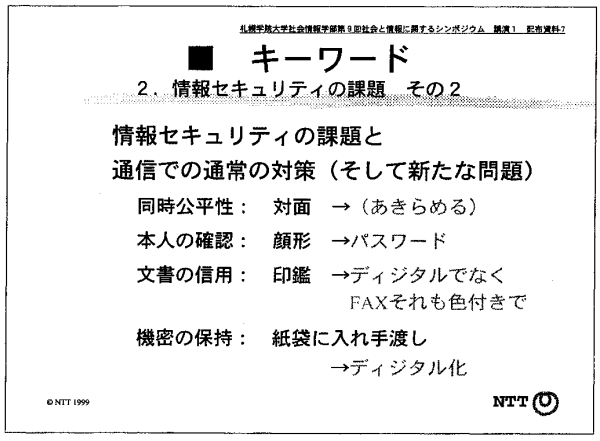
2番目は，〝証拠を残す〟ことで，契約書に印を押すことに相当します．コピーなどの技術が進歩したので，より一層，情報だけで〝証拠を残す〟必要性が増しています．3番目は〝機密を守る〟ことで，電文内容や，プライバシを守ります．

セキュリティ・プロトコルというのは，これら3つの要素の上に構築されるもので，既に述べている電子契約，電子マネー，コンテンツ配信，等を意味します．ネットワークに広がるにつれて，新しいものが今後も続々出てくると思います．



具体的に，情報セキュリティの課題を具体的にイメージして頂くために，我々の通常の生活における，〝同時公平性〟，〝本人の確認〟，〝文書の信用〟，〝機密の保持〟を考えたいと思います．対面であれば，お金と物品の交換は安心ですね．たとえ，お金だけ取られ，商品をくれなくても，追い掛けて捕まえる手段が残されているので安心です．

登録されている写真と顔が照合できれば，普通，安全と見なします．文書に約束の意味あいを付加するのに，印鑑を使います．その信用度を上げたい場合は，印鑑証明書付きの印を用います．機密の保持と言いながら，日常生活では，紙袋に入れて手渡すことが多いですね．



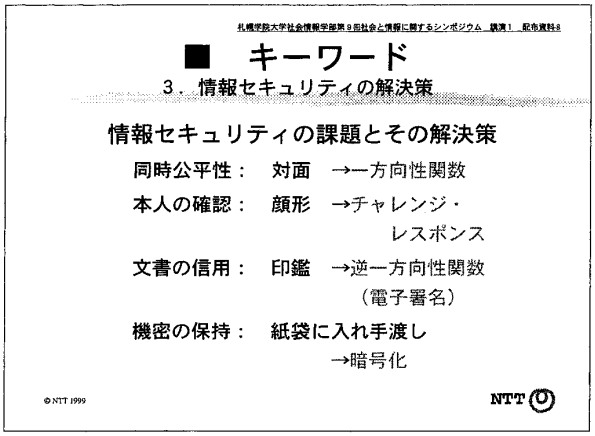
さきほどは，日常生活でセキュリティをどのように守っているかを見たわけですが，ここでは，通信相手との間で同じ機能を，通常，どの様に果たしているか振り返ってみます．どれも対策としては，不十分なところがあります．

先ず，物や情報の売買などの公平性ですが，普通，あきらめるしかない様です．相手の信用度により，クレジット番号などを教えてしまって良いか判断していると言って良いでしょう．

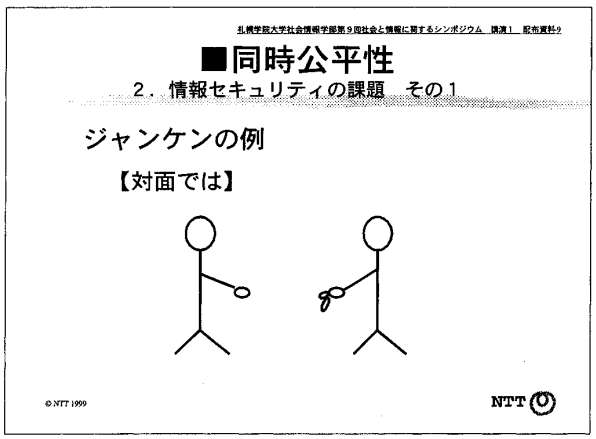
本人の確認では，パスワードや暗証番号を利用することが大変普及してます．お馴染みですね．しかし，いつも同じパスワードですと，盗難の危険がありますし，その情報が流れるところが，専用回線でなく，インターネットなどですと，盗聴＝盗難とおなじことになります．

文書の信用では，今迄の習慣通りに実行している様です．押印し，FAX で送るなどです．但し，コピーが発達したので，真贋性をはっきりさせる意味で，通常，封書で原本を交換します．

機密の保持は，媒体を紙からフロッピーに変えることで守っているという人が多い様です．無線でも，昔，アナログからディジタルに切り替わったので，普通の人には情報の中身がわからないから安心という考え方がありました．しかし，今では笑い話です．

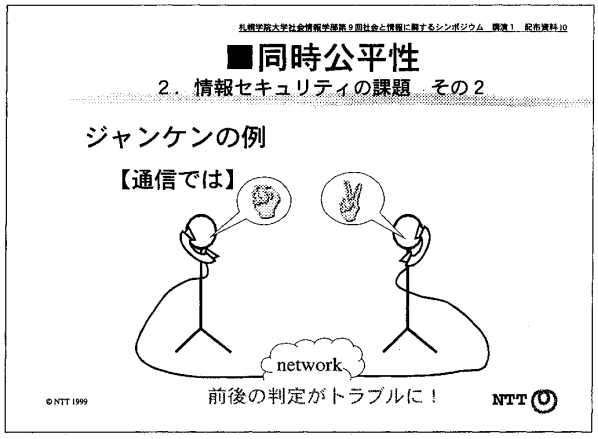


情報セキュリティの研究により，理論的にはこれらの問題は本質的に解決されています．詳しくは，この次に説明したいと思いますが，このOHPの赤（矢印の右）で示してある解決策を導入することが役立ちます．

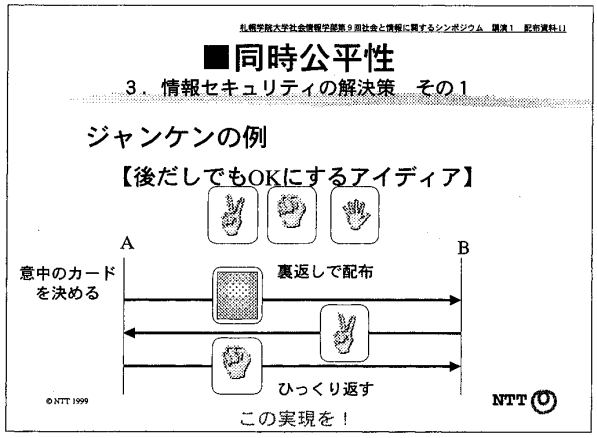


同時公平性について見てみましょう．ジャンケンを例として考えてみます．対面ですと，二人で出すタイミングを合わせようと言う気持ちも働くし，ズルしたと相手に直接クレームを言えるということで，余り問題になりません．仮に，相手が全く信用できないのならば，行事役を立ててカバーすることもできます．

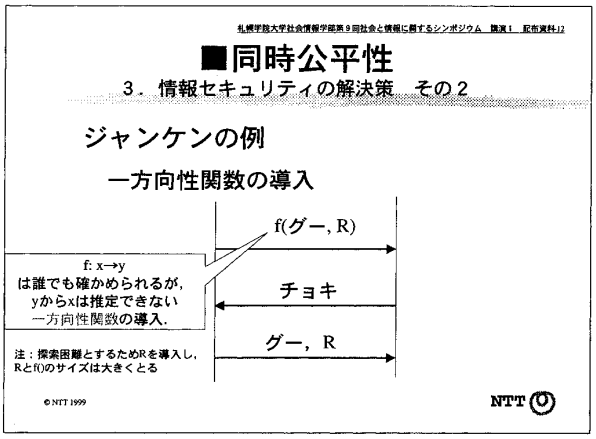
それでは，面と向かってできない通信の場合どうやって公平性を維持したら良いのでしょうか？



電話で，「グー」「チョキ」「パー」を同時に発声して決めようと言っても，決め手に欠けます．また，ここでは原理的な同時性を議論しようと思ってこの例題をだしているのですが，「電話を使ったジャンケン」の詳細化をやっても，解決を与える根本原理に至りそうもありません．



ところが，情報セキュリティの技術によれば，一種のカードゲームを考えてこの問題を解決することができます．



「一方向性関数」はOHPスライドのコラムにある通りです．入力xが，「グー」「チョキ」「パー」だけですと，例え出力yがxから想像のできない値であったとしても，f(x)を３とおり作って，それとyを比較すれば良い分けですからxは推定できます．

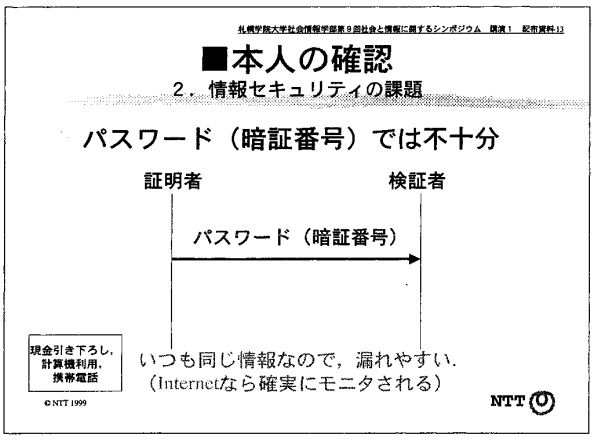
これでは困りますので，探索困難とするためOHPスライドを見て下さい．「グー」「チョキ」「パー」の３通りしかないカードですが，Aさんがそれらのカードのどれかを選択し，裏返したまま相手のBさんに渡します．Bさんは Aさんの助けなしには，表をみることができないと約束しておくと，Bさんは裏返しのカードから何の情報も得られません．Aが何をくれたか分からない状態で，Bは自分の手「チョキ」を選択し，相手に教えます．そして，Aは渡したカードをひっくり返し「グー」であったことを示します．

今の説明は，対面の場合ですが，「一方向性関数」を導入すると，等価なことが通信の場合でも実現できます．

大きな変数Rを導入します．こうして，入力xは「グー」「チョキ」「パー」と乱数Rの組とします．また，出力f(x)のサイズが大きいとします．すると，f(x)は一種の乱数の様な出力となり，Bには入力の予想がつきません．

後で，Aが「グー」という事実とともに，最初の値に対応するRを送ることにより，最初から宣言してた「グー」だと主張できれば良い分けです．この為には，２種の異なる入力x，x'を作り，f(x)＝f(x')という組み合わせが計算量的に見つけることが不可能という関数をみつけてこなくてはなりません．

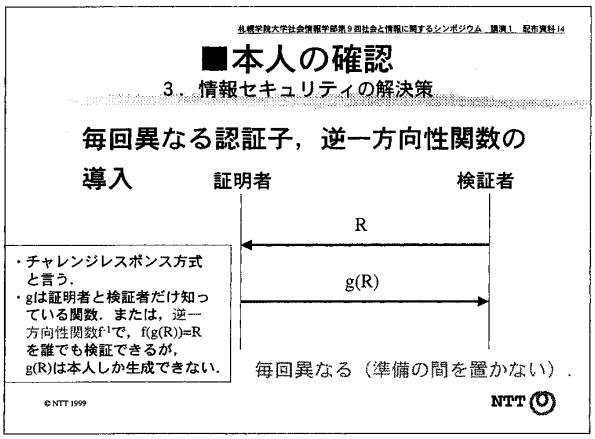
この様な定義の関数のことを「一方向性関数」と呼びます．実用上は，SHA－１の様なハッシュ関数がその目的に使えると信じられています．



次はなじみの深いパスワードのことです．現金引き下ろし，計算機利用などでは，パスワード（暗証番号）が用いられてますが，それがダイレクトに通信されているとすると，いつも同じ情報なので，漏れやすく，危ないと言わざるを得ません．

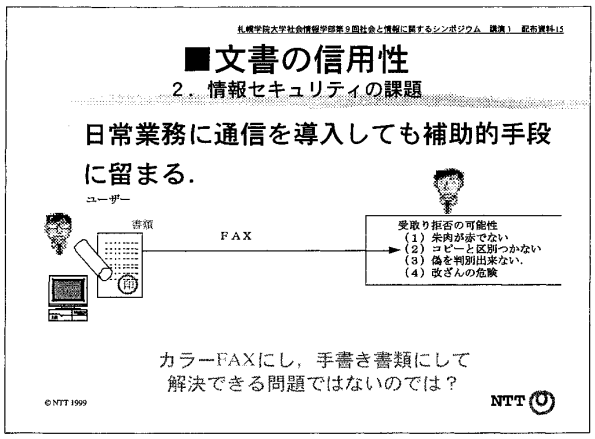
携帯電話も同じ原理でセンターが子機を確認していたとしたら，無線ですから，漏れて当然という状況になってしまいます．実際，米国で，その様な事例があり，他人名義の携帯電話を利用した犯罪があったそうです．

相手に確認のための情報を伝えたいが，それが再利用される危険を想定する必要があるわけです．



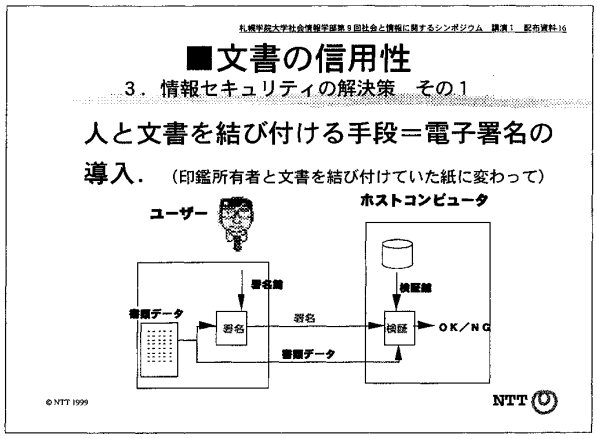
この問題を解決したのが，チャレンジ・レスポンスという技法です．検証者が乱数Rを証明者に送り，証明者はg(R)を送り返すという簡単な方式です．乱数R（チャレンジとも言う）は毎回変わるので，返すC←g(R)も毎回異なる値が出るわけで，再利用しても意味がありません．実用的には，携帯電話には当初からこの方法が用いられていて，米国の様な問題は生じていません．

関数gに関しては2通り方法があります．通信の両者だけが関数gを知っていることを前提とし，C=g(R)（右辺のgは検証者が実行）を確認する方法と，gは証明者だけが知っていて検証関数fは公けでも構わないとし，f(g(R))=Rの確認をする方法です．後者は逆一方向性関数を用いる方法です．



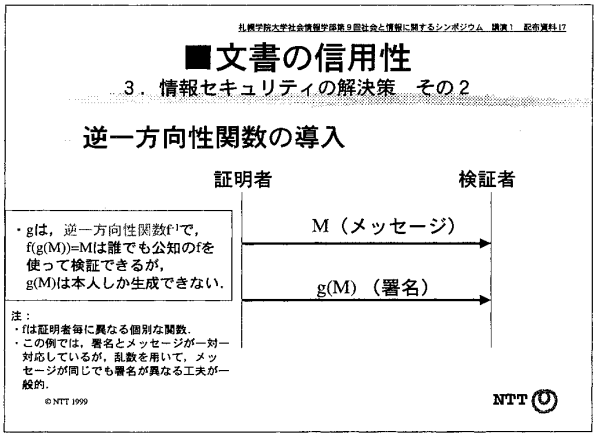
次は，文書の確認手段に話を移します．このスライドに示す様に，FAXという通信手段を導入しているにも関わらず，受け取り側を満足させることにはなっていない様です．このため，FAXした後，原本は別途郵送してくださいということになることが多いと聞きます．

一時期，カラーFAXにして，印影を赤く表示できる様にするとか，FAXの精度を上げて本物と区別できない位にするなどの対策が議論されていました．結局のところ，FAXのことを，いくら議論してみても完璧なコピーができるかどうかという話であって，オリジナルとコピーをどう区別するかという本質的な問題に解答を与えていなかったのです．

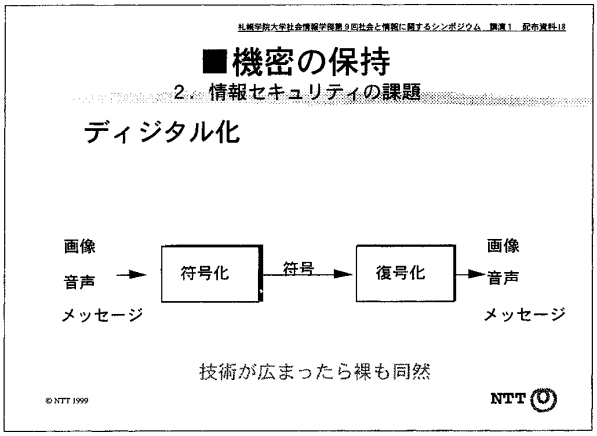


印影で与える文書の信用性とは何でしょうか？ 結局の所，印鑑所有者が，約束が書いてある文書に対して，自分が責任を持つという事実を残すということではないでしょうか？ つまり，個人または法人を印鑑を通じて，ある約束事に関して結び付けるということです．

これにディジタルな世界で解決を与えたのは電子署名の存在です．図に示す様に，署名という情報の生成には，文書自体と，唯一無二の署名鍵が関わっています．検証では，その署名情報と，文書と，対応する個人の検証鍵を使って確認を行ないます．

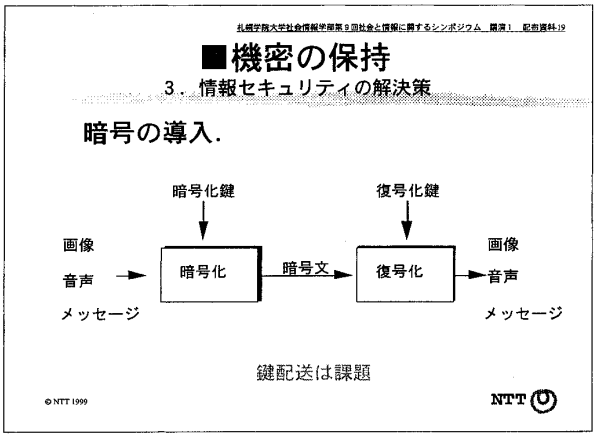


原理としては，チャレンジ・レスポンスの説明でも出て来た逆一方向性関数を利用します．



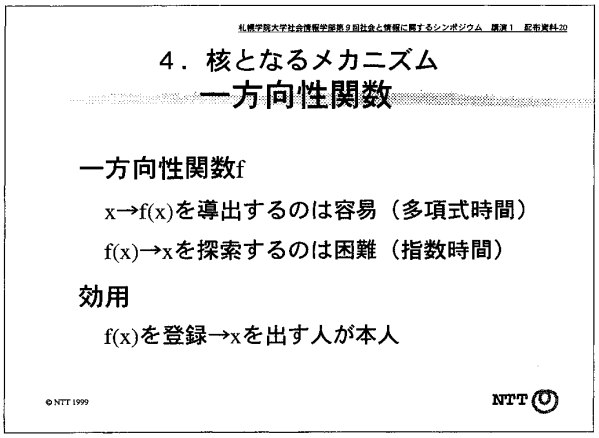
機密保持の話に移ります．マルチメディアの時代ですが，画像，音声，メッセージをディジタルの値に符号化し，その様な符号化を知る人が少ないからと言って安全だとすましているわけにはいきません．

技術はあっという間に広まるものですし，そもそも雑音や復号効率を考えて作られている符号は，セキュリティをケアする為の秘匿性は考慮されていません．



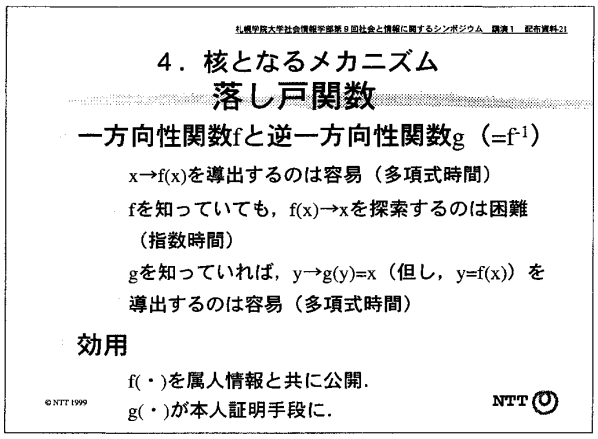
符号化の部分を暗号化に置き換えただけですが，通常次の様な作りとなります．書いてありませんが，画像や音声やメッセージはそれぞれ効率を考えた符号化を施されディジタル信号となっていて，これに暗号をかけます．暗号化と復号化は通常仕様が公開されていて，ちょうど，錠前と鍵の関係の様に，暗号処理部分は既製品としてあたえられ，鍵によって特殊化されます．

暗号化鍵と復号化鍵は，対になっていて，同じものの場合，復号鍵の配分が課題となります．暗号化鍵と復号化鍵が異なり，少なくとも，暗号化鍵から復号化鍵を類推することが困難であるものが，公開鍵暗号方式といわれるものです．この方式では，暗号化鍵を公開しても構わないので安全な鍵配送は課題として無いわけですが，通常，暗号化や復号化の処理時間が桁違いに遅いことが問題になっています．



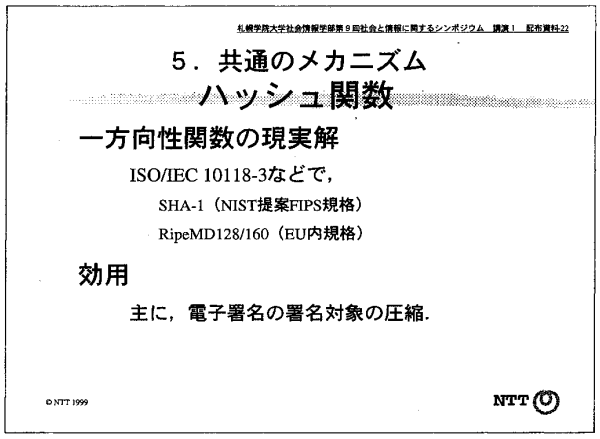
再び一方向性関数の性質について述べます．一方向性という名の由来は，$x \rightarrow f(x)$の生成はたやすいが，$f(x) \rightarrow x$は，山勘でxを沢山生成して，$f(x)$と一致するものを探索する方法ぐらしかなくて困難であるという性質に由来している．

逆に，効用としては，$f(x)$を先に登録し，あとでxを示すことで，登録者本人の確認に使う．

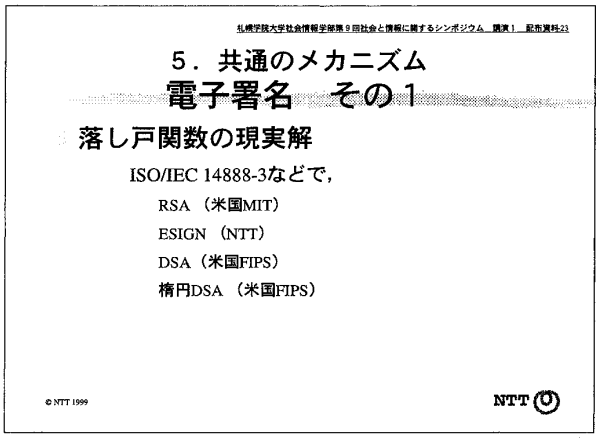


xとf(x)の関係は，xを知る人しか知り得ません．ですから，通常，xは秘密にしておきます．一方，特定の一方向性関数fによりy=f(x)の関係があり，特定の意味のあるyが得られるとしたらどうでしょうか？ xを作った人は，特定の一方向性関数fとyに関して，xにより特別な関係を示そうとしたことになります．

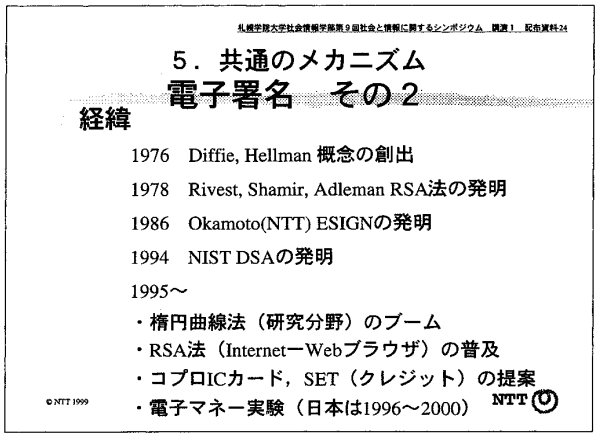
fの逆関数のgがあればそれを実現できます．例えば，g(y)をxと置けば，f(x)=f(g(y))なので，y=f(x)を出力できます．この結果，xを示すことが，関数fに対して特別な関係を持つ人がyについて署名したことの原理となります．特別な関係とは，fの逆関数gを持っていることです．



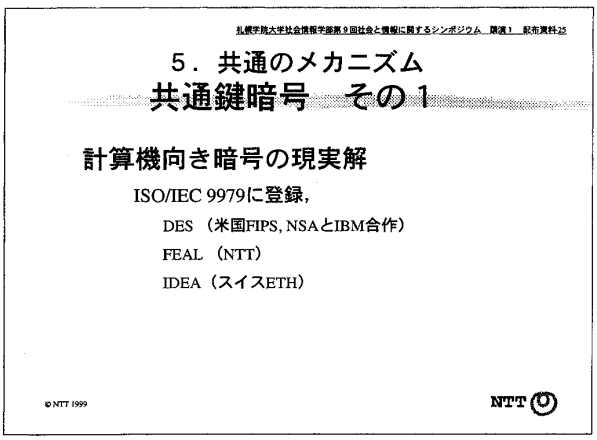
一方向性関数の現実解には，ここに示す国際規格があり，普通，一定長のビット長にデータを圧縮する性質があるので，ハッシュ関数と呼ばれます．



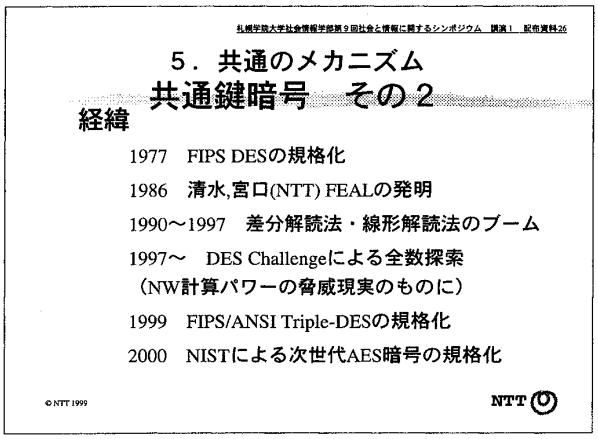
逆一方向性関数があるものは，公開鍵系アルゴリズムである電子署名(ディジタル署名)で，ここに示すものが代表例です．何れも，ある秘密を知っていれば，早く署名を生成できるが，知らない者が，署名を生成するには指数オーダの時間を要するというトリック，つまり落し戸という性質を備えます．



電子署名に関して，主な時間的な流れをここに示しています．



比較的高速な共通鍵暗号の代表例をここに示します．



時間的には，ざっとこういう流れで，来年はAES暗号に関する話題が大きく取り上げられると思います．

森田講演に対するコメントと質疑

司会(佐藤和洋)：……コメント或いは質問等ある方は最初に所属とお名前をお願いします．それでは何か質問，或いはコメントがありましたら，どうぞ．

斎藤：社会情報学科の斎藤です．先程の例ですが，1000年かかるものを1,000台で並列処理すれば1年で済みます．そこで思い出したのですけれども，暗号化の逆をアメリカのSETIで公開募集しています．宇宙の彼方から飛来する電波に何か意味あるものを発見するのにSETIだけでは大変だというので，ボランティアを募って生のデータを提供し，そこで解析処理して何か意味がありそうなものが出たらSETIに送るという呼びかけを思い出しました．暗号化をする場合，こういう研究発表をしますね．アルゴリズムがあるわけですが，常に何かイタチごっこみたいなことをしていると思うんですけれども，お話の内容は，鍵をつくるということです．だいたい人間の考えることは，普通パスワードを発想するときと同じように，そう違っていない．そうするといくら乱数を発生させていろいろハッシングをして変えても，何か早く見つかる方法が意外と考えつく可能性があります．そうしますと永遠に追いかけっこをやる可能性があるのではないかという気がしないでもないのです．本当はビットをうんと大きくしてやれば組み合わせを複雑にすることができるというのがありますからそれはわかるのですが，こうした方法は認証ぐらいは使えるのですがデータそのものについては暗号化してそれをまた復号するということは実際にはできません．そうすると多分認証化のところはかなり頻度も少ないのでそういう方法で情報量を多くしてやって組み合わせ数を多くすれば何とかなるかもしれない．その送っているデーターそのものを歪めないようにする，見てもわからないようにするのは結構難しいのではないか．

そうするともう傍から見られてもいいんだということを最初から考えて情報をつくり出しておく．だからそういうような方法が賢いのではないかと思われるのですがどうでしょうか．これは素人の発想なのですが．

森田：なかなか難しい質問です．大きく分けて暗号的なものと，そうでないものがあります．カシオ計算機だったと思いますが，何か良い暗号をつくりました．新聞に載っていたのですけれども，懸賞金付きの解読問題でした．それの平文といって元の文章を見せないで暗号文だけ見せて答えなさいというのです．世界的な意味でみんなが研究しているところと国内の先生方も含めて我々コミュニティの中でやっているコンセンサスと全然違うところでカシオ計算機暗号はやっているなと．

実は暗号というのは中がどういう暗号の処理になっているかというのは秘密にしていれば十分安全になるのです．シーザー暗号といって，たとえば「あ」を「い」と読むように読み変えます．「う」を「え」に変えますとか，そういうようレベルだったらそれはあるいは解けるかもしれません．ご存知かもしれませんけれども，エドガー・アラン・ポーが

昔どこかの新聞のコラムをもっていて，暗号の問題を挑戦として自分に送ってくるように言い，みんな解けてしまいますと言い，実際ほとんど解けました．いわゆる文学的レベルでは解けるものもあるんです．ですから，人間がちょっと考えて，あるフィールドの中ではほとんど解けるということはもう当時からわかっていたことなのです．

ちょっと話がずれちゃいましたが，逆に解けるように感じるのですが，今の計算機を使う暗号はほとんど解けないのです．先程のカシオみたいなケースですと誰も全然議論の対象外で解けるはずがないんです．暗号を計算機でちょこちょこっとやってほんの1ビットを変えるぐらいだったら見つけられるのですけれども，全体はほとんど見つけようがないんです．では我々がどのように研究発表してみんなにこういう新暗号を考えましたと出すのかというと，実は暗号のつくり方もメニューとしてみんなに見せているんです．みんなで共通にたとえば錠前と鍵にたとえるならば，錠前については実はその構造物に教えていて，それでも安心なものを皆で考えましょうというのがベースになっています．それでIBMとかDESチャレンジのDESというアメリカの方式も仕様が全部公開されていて，その鍵を効率的に求めるにはどうしたらいいのかというのが課題になっています．鍵というのはいうなれば我々のもっている鍵のギザギザの部分がどこに合うかそれを探索するようなことが目的になるので，そのギザギザの量を今までは64ビットですと，ちょっと忘れましたけれども1万年とかそれくらいのスケールなのですが，ここのところの進歩で2日ぐらいまでになってしまったというようなブレークスルーなんです．ではこれでもう駄目かというと実はそれはまだみんなで，チェックしてもらうお遊び問題なので，現実はモードオペレーションというちょっとしたひねりがあり，これも公になっているのですけれども，そういう方法で情報をもらさないようになっています．仕様まで公にし，解読の難易度も落とし，みんなの目にふれても安心なら大丈夫という感じを持とうとするポリシーがDESの1976年以後20年近く経っていますけれども世界的レベルで作られています．だからこそこういう公の場である学会とかでディスカッションしてそれで意義あるところとなっているのです．

ただそうはいっても計算機の能力もあがり，ネットワークの能力もあがり，1000年の安全が，実は10年も経ったら10年に減っちゃったということも有り得，おっしゃるとおりです．そういう面ではイタチごっこです．逆に，我々研究者の立場では永遠に仕事がなくならなくって良いことかなと思います．現実問題としては先程いったように，いろいろふたをする方法があって，パーツに分けてみんなで議論します．ですから，明日急に駄目になるというのは実はあまりありそうもありません．

先程もう1つおっしゃっていた，暗号を応用する立場でどこまで秘密にしたらいいのか，これは非常に重要なポイントだと私も前から思っています．暗号だから安全ですと同僚もすぐ考えてしまって困ることがあります．単に使っているだけでどこを使っていいか全然頭を使っていないので，暗号を三重，四重にかけても全く無意味なんですが，安全と思い込む人がいるのです．多くかけても効果は倍増しません．一方，どこまでの暗号をかけるかの問題ですが，たとえば交通情報とか雨の気象情報みたいなのがWebの上でのっています．ただ肝心の情報，たとえば雨とか曇りとかいうのは伏せ字にして，ユーザが知りたいなと思ったら10円払う．

そうこうしていくと結局，では自分が知られたくないと思って，本名をふせれば大部分はOKだなというようなところも，結構プライバシーということで考えられているので，

暗号をかけないでプライバシーをコントロールして何とかごまかせないかというところが結構今進んでいます．先程チラッとお見せしたこのインターネットキャッシュのケースでいくと，このカードには私は森田光と書いてあるのですけれども，実際このインターネットの上では仮名で，一種の乱数で自分が存在しているようになっているんです．要するに人と商取引するときに自分の名前が残らない．十二単衣じゃないですけれども，どんどん重ね着していくようなのは逆にやめたらいいのではないかというのは正におっしゃっているそういう流れで少しずつできつつあるという状況です．

司会：よろしいですか？　他にございませんか？　どうぞ．

田中：安全性というものの程度をはかる何か考え方はあるのでしょうか？．その完全な安全性がないとすれば，さしあたり比較するのは今までよりもより安全になるということだと思います．また日常のいろいろな問題，印鑑にしても100パーセント安全というものではありませんでしょうから，安全性の程度をどのようにとらえるかという，そういうことに関して行われている研究がないかとどうか伺いたい．

森田：この安全性というのは非常に重要なテーマで，先程ちらっとご紹介したDESという方式がもとは10万年などの長い強度設定だったのですが，今や現実問題として2日で解けてしまったわけです．何か我々が頭で考えている指標というのと，現実に起こる現実の世界というのは大分ギャップがある．しかも現実の方はより進んでいるというのが最近の例で，非常に問題だというふうに思っています．

ただちょっと矛盾するようなんですけれども，少なくとも64ビットの鍵というのがあるのですけれども，それと65ビットというと2進数でいう倍違いますから，倍安全というのは，これは少なくとも言えることです．そのぐらいの数値基準はあるのですが，では64ビットではなくて128ビットにしたら，とても安全かというと実は安全かどうかはわからなくて，探索していくときに最初の1個目で当たる確率だって2の128乗分の1はあるわけです．もうほとんど天文学的数字なんですけれどもゼロとか，そういう意味でいくと我々の今やっている暗号の世界というのは確率的なものであって絶対というのはほとんど存在していないというのが1つ言えると思います．

あと暗号の安全性で見ますと実は同じ計算機を，今我々みんなが同じような計算機を使っていて，正直に端から順序良くオールゼロから1，2，3，4とこういう順番で全数探索することを前提にDESチャレンジが行われたので，しかも普通の人にわかりやすいし，実際もそういうところでコンテストが行われたので，ほとんどみんなそちらの方法が解読だと思い込んでいるのですが，実はそうではなくてもっと効率的に求める方法というのが，たとえば数学的な構造の中に隠れていたりします．一種の天才がパッと目利きで解けてしまうというのは結構よくある話で，私も昔ちょっとFEALのDESとかいろんな論文についてそういう構造があったらおもしろいなと思ったので，よく研究されている群の構造などを探索したりしました．

また，もともとベースになっている素因数分解とか離散対数問題という一種のコンピューターサイエンスでやられている問題があるのですけれども，それが解けてしまったら暗号分野の何かもすぐ解けてしまうという状況に有ります．それも数十年前よりも数百倍，数千倍というぐらいものすごい勢いで効率が上がっているのです．これは何故かというと人間の知見が上がってきて，ある技法がどんどんアップしていって，解きやすくなっているんです．それに伴い暗号の安全性とい

うのは低下していっているという構造が有ります.

そういう面で楕円曲線暗号というのが流行しています.けれど,皆がRSAから楕円法へ移るか分かりません.暗号は最終的には経験科学ではないと思っています.結構人間的な,要するに人間とはどの程度知識をもつかということを前提にしている.実はRSA法については素因数分解がベースにあり,その素因数分解が考えられてきたから逆に弱くなってきている.そういう面でいくと人間というのは知見が深まるというか,つまりセキュリティって人間が知らないところをうまく使って,つまり人間の無知をうまく使ってやっていると.それが本質なのではないかと思っています.

楕円曲線暗号というと,実は例のフェルマーの最終定理が解けたことで,一種の枠組みを与えた一つのテクニックです.元々は単なる初等整数論的な格好をしていたフェルマーの大定理だったのですけれども,実際,裏側でいろいろ難しいことを,数学的な最先端のテクニックでやっと理解ができて,そういう点でうまく解けたと,そういうことなんです.

ただ,そのテクニック自体は,つまり楕円のことですが,まだ10年,20年,提案されてから50年ぐらいの世界で,ここのところ注目されているのがここ10年,20年のことなんです.ということは人間は無知の状態なのです.だからうまい具合にそちらの人間の無知を利用して,暗号を構成することは非常に良いんだということで,そういうものをベースにした暗号を使うというのです.

もう1つは固有名詞をもっている暗号のDES, FEALと先程言ったのですが,実はこれはみんなが研究する気にならないからぐちゃぐちゃにした,基本構造はきれいなのですけれども,中の構造をみるとほとんど研究する気にならないというか,ぐちゃぐちゃした構造になっているんです.そういう点で数学的に形式化しておもしろくない問題の1つです.人が勉強する気にならないと言う,悪い言い方をするとそういうところがあって,でもそんなところでも整理してセンス良くうまく探索するテクニック,つまり,差分解読法とか,線形解読法がでてきています.線形解読法は結構日本でも重要な貢献をしています.これは三菱電機に勤めている松井さんがつくった方法なのです.安全性については定量的にこうだということはちょっと言えないし,相対的にこれよりあれということは言えても,今のところ基本的には全体の流れとしては暗号とかセキュリティというのは人間が計算機を駆使しても解けないという1種の限界をみながら,いつもどんどんグレードを上げていくというようなものです.

田中:今のお答えの中に暗号の問題,あるいは安全性の問題は計算機科学の問題ではないという一言があったかと思うんですが,それは私も全くそう思うので,それに関連してちょっとコメントしたいと思います.

社会情報学の中では自己組織性ということが大変大きな問題になっているわけです.大きな問題なのですけれども,その中で自己とは何かということは方々いろいろな点から議論されておりますし,特に自己とは何かということを免疫学のアプローチの方から取り上げられて色々議論されていることがあるかと思います.実際,生物がいろんな異物を取り入れるときに,それが自己ではないということを判定するのに,実に複雑なしかも巧妙な免疫システムを用いているかと思うんですが,私はそのような生物が自分自身と自分自身でないものと区別する,その免疫システムというもの,それから実際に暗号でも使われている手法との間には随分共通性がある得るかと思います.暗号というといろんなニュアンスがその言葉に入りますけれども,自己と自己でないものとをどのように区別するかと

いう，そういう問題は単に安全性の問題に関することだけでなく，もっと非常に広い，一般的な考え方になり得るのではないかと思っているのです．

司会：ありがとうございます．今のコメントに対してはどうでしょう．

森田：ちょっと難しい話ですけれども，暗号の議論ではありませんが，先程紹介しました電子署名になるとほとんど本人確認で，免疫の機能に似ています．自分がどこかに属しているということをチェックされればいいというので権威者が１人います．日本の権威者がさらに世界の権威者にチェックされて全体として証左されるというような考え方があります．一方，友人の友人は皆友人というチェックの仕方があります．生物の免疫は，中央集権的か分権的か，排除のメカニズムはどうなっているのか？　関連もありそうな感じがします．論理面だけとは思いますが．

司会：他にどなたかご意見・ご質問ありませんでしょうか．はい，どうぞ．

野川：札幌医大情報センターの野川と言いますが，セキュリティの話で暗号になると数学理論ということでよくわかるのですが，実際に１つのコンピューターシステムとして見ると実は一番低いところが攻撃されます．それは何かと言いますと明日はパスワードを変えるとか，人にパスワードを教えるなよ，というようなソーシャルエンジニアリングというふうに言われる介入手法が一番最も進入口として多くて，それをやられるとどんなに強烈なスーパー暗号もすべておしまいというふうになるんですけれども，そこら辺を考えてシームレスに使える何か良い方法があるでしょうか．

常にいつも何か良いものはないかなと模索しているんですが．

森田：ちょっと私も中野先生からお伺いしたいという感じがするんです．とりあえずは暗号っていうのは実はちょっとを入れるにも前後が全部いろいろとシステムを計画したり面倒くさいんですけど，やっとSSL，あとplug-inがあったので，セキュリティにはRSAなどちょっと入れてくれたかな，という程度の新しさしか目に見えないという面では我々の不徳のいたす所という状況になっています．世の中，一般的な人というのはちょっとホームページでクリックするくらいなんですけど，最終的にはテレビの枠にマウスもなく，リモコンだけで使える世界にまで落ちてくれば，当然そういうシームレスな状況にしないと話にならないと思います．一般ユーザーは私らの子どもの世代とかそんなのが普通に使っているときは暗号なんて入っているんだねと，知っている人だけ知っているという程度でちょうどいい状況になると思います．

野川：結局はあれですか，今ポンポンポンと１つのマシンを複数使っていたりしているのがいかんので，携帯電話みたいに１人１台でしたら，その機械から発信しているのはそのもっている人だと．それで機械でやってしまえというのが良い．だからUNIXマシーンは１人１台で．

森田：それの究極で，私はこういうネクタイピンとか指輪とか，そういうものに認証の機能を入れれば，要するに今おっしゃったようにUNIX １人１台というのではなくて，座ったらそこを根拠に自分の窓がパッと開くようにすれば良いじゃないかというふうに思います．しかし，そもそもそんなものに入れたってだめだよということで，赤ちゃんが生まれたらその時点でどっかにICを埋め込んだら，という議論も有ります．

野川：もう１つよろしいでしょうか．今，暗号というのは１対１の通信また実際に使っているのもSSL，PGPは１対１ですね．実際にはあそこは１対多通信が多くて，１対多通信の暗号化に非常に困っているというか，PGPはまだしようがなくて，SLMIMEは結構ややこしいことをしていて，途中で入りたいと

いう人もまだ入りきれないですから，それにIPJ6で暗号がパケットにありますが，でもマルチキャストするにはどうするか．非常に疑問がおこるのですがそこら辺何か対策はどうでしょうか？

森田：その関係では大体2通りくらいの流れがあって，現実問題として存在しているんですけれども，詳しいスペックは知りませんが，WOWWOWがありますが，一応契約した人だけがやるらしいんですけれども，自分のチューナー部分に識別できるような情報があって，これは私の予想なのですが，上のサテライトがわっーと電波を散らして，ネガティブ情報を流していると思います．Aさんがお金を払ってAさんのデコーダーを通して，裏でそういう制御の情報が流れているのではないでしょうか？　逆に，契約している人のポジティブ情報で制御していたとしても，1番から1,000番まではオーケーで，1,001番はだめだから1,002番から，9,000番までは一応オーケーで，この人はOKで途中の部分がネガティブで見せないわけです．ひと月ぐらい見ていて30分間以上受信するとその辺のコントロール情報が入るという噂をちょっと聞いたことがあるので，多分そんなような情報があっていわゆるデコードする側のコントロールをうまい具合に，切り替えていると思います．

それは現実でも使われてないわけでもないということの1つの例で，現実はマルチキャストのあの辺になりますと今まさに遅ればせながら研究がやられつつあるところです．

司会：よろしいですか．他にどなたかありませんか．まだ少し時間がありますので，それでは私の方から．

先程も出ていましたが，この分野で昔の私の同僚もたくさん活躍しております．ちょっと紹介させていただきますと，同僚が書いた本が最近岩波書店から出版されました．今お話しされた内容とか，このあと中野先生がお話しされることなどがとても易しく書かれています．もしよろしかったらお求め頂ければ幸いです．さて，この中にもあるのですが，技術的な話ではないのですが，暗号系の話というのは政治のレベルで非常に重要な課題となっていると思います．昔のようなココム問題は緩和されつつありますが，今は別の意味で状況が変わってきています．特に，アメリカの色々な面における高飛車な態度です．暗号アルゴリズムに関しても圧力がかかっていると聞いています．潜在的に大きな問題を孕んでいるように思っているのですが，暗号を研究されている当事者たちは，この状況をどのように考えられておられるのでしょうか？

森田：難しい問題ですね．ある所から圧力がかかって，あるところの製品化が駄目になったという話を聞いたことがあります．立場上少々問題が有りますので，コメントは差し控えたいと思います．

司会：はい，了解しました．それでは他にどなたか？　はいどうぞ．

野川：コメントですが，いわゆる草の根プログラマーというか，そこら辺で反骨精神が旺盛ですしね，PGPなんかはちょっとごちゃごちゃがあってぱっと世の中にでると，一応輸出規制とかありながらも実は日本のftpサイトにあったりで僕も実は使っているのですけど，PGP社がですね，もともと輸出主体に，ここ国防総省の輸出制限でいろいろやっていたのですが，今度はftpとかFDは駄目だが，本は輸出できる不思議なやつで，本はフィンランドかどこかに送って全部スキャンしてもう一回入れた．SSHをつくっていると会社は，昔はアメリカだったのですが，輸出規制がいやでフィンランドに逃げたとかですね．インターネットを使っているプログラマーはNTTだとかオフィシャルな研究所で働いている人とは立場が違うという感想ですけれども．

森田：個人レベルでは，ガードが弱いのでそ

のままダウンロードしてしまって，問題は生じないかもしれません．一般的に輸出規制で貿易がコントロールされているわけですから．しかし，企業などの組織ですと，モラル的に問題が生じるかもしれません．

司会：どうもありがとうございました．時間もきましたので森田先生のお話を終わらせていただきます．短い時間の中で非常に多岐に渡っていろんなお話を頂きありがとうございました．情報セキュリティの分野での暗号のあり方は非常に重要なテーマですので，これからの一層のご活躍を期待します．それでは，午前中の講演はこれでお開きにしたいと思います．