コンピュータセキュリティ　10－18
(2000.　7.　25)

画像の位置情報による本人認証方式の研究開発

画像パスワードGATESCENE（ゲートシーン）

鹿島　一紀
(株)富士通ソーシアルシステムエンジニアリング
東京都品川区東五反田一丁目22番1号 五反田ANビル
電話：03-3443-3527
E-mail：kashima@fss.fujitsu.co.jp

あらまし　IDとパスワードに代わる本人認証システムとしては、指紋などを利用するバイオメトリックス認証の実用化が進んでいる。これは個体特有の特徴をシステムで認証することで、別人がなりすますことをほぼ完全に防御できるという期待感からと考えられる。しかしバイオメトリックス認証には、普及しづらい本質的な5つの課題がある。そこで従来のIDとパスワードの課題を再考し、これらの課題にも対応できるソリューションが必要と考え、画像の位置情報を利用した新しい本人認証方式を開発した。本稿は、その開発背景、認証方式、およびその有用性について報告するものである。

キーワード　画像パスワード，スマートカード，ゲートシーン，画像，位置情報，本人認証

Next generation visual password tool
GATESCNE　－The Image Password－

Kazunori Kashima
Fujitsu Social System Engineering
Gotanda AN Bldg., 1-22-1 Higashi Gotanda, Shinagawa-ku, Tokyo 141-0022
Telephone number: 03-3443-3527
E-mail：kashima@fss.fujitsu.co.jp

Abstract

For our passwords, we are apt to register birthdays or telephone numbers because these are easy to remember. These overly simple codes have fostered the illegal use of stolen or lost credit cards. A five, six or seven digit PIN may seem more secure but its user-friendliness is highly questionable. Sophisticated fingerprint recognition systems are also too invasive for everyday use. The advanced Gatescene system is not be based on user's personal attributes and yet still be fast, friendly and intuitive.

key words　image password, GATESCENE, advanced PIN, smart card, friendly interface

1．はじめに

社会システムのコンピュータへの依存度が高まるにつれ、社会公共分野のコンピュータを狙った犯罪活動も現実味を帯びてきた。中央官庁をはじめとするWebサイトへの不正アタックなどセキュリティシステムへのソリューションの提供は、今後ますます重要視されてきているところである。

特に最近では、セキュリティ意識の向上に伴って、本人認証の手段として広く利用されている従来のIDとパスワードだけでは不充分と考える企業や利用者が多くなってきていた。

2．バイオメトリックス認証の本質的課題

IDとパスワードに代わる本人認証システムとしては、個人を特定する指紋や網膜文様などを使ったバイオメトリックス認証の実用化が進んでいる。これは個体特有の特徴をシステムで認証することで、別人がなりすますことをほぼ完全に防御できるとの期待感と、短時間での認証が可能であるからだろう。

しかし指紋などのバイオメトリックス認証には、利用がなかなか普及しづらい本質的な課題がある。それは、認証のために利用される指紋や網膜文様という個体固有データが、システムで管理された際に、どこかに流出する危険性は皆無なのか、ということに代表される。

たとえ指紋などの個体データが、その一部の特徴抽出にすぎないとしても、その一部データが認証に利用されていることに変わりはない。個体データがインターネットを通して流出した、などの噂が発生しただけでも特殊なプライバシーのデータであるだけに、その利用者に与える脅威は、IDとパスワード方式とは比べ物にならない可能性がある。

またバイオメトリックス認証は、個体データの読み取りのために特別な認識装置が必須となるため、その認識装置と個体データ間との認証設定(閾値)や保守を含めたコスト負担を考慮せざるを得ない。

以下にこれらの課題を下表に示す。

［表１：バイオメトリックス認証の本質的課題］

項番	課題	概要
1	個体データ(指紋等)の更新ができない。	ネットワークを介して悪用(盗難)されると、個体データそのものは真正であるため、利用したシステム全体の信頼性が崩壊する。
2	システム管理者の運用管理負担が大きい。	管理者によるデータ管理に細心の注意義務が生じる。特に利用者の退会時には、速やか、かつ確実な個体データの削除履行義務と利用者への通知（証明）が必要となる可能性が高い。また個体データは事前収集が必須なため、遠隔地の利用者などには運用上不都合が生じる。更に認識装置としてのハードウェア保守のコスト負担も考慮する必要がある。
3	個体データの認識率が、利用者の物理的状態や環境を考慮した認識装置間との設定値（閾値）で左右される。	指紋の場合、けが，乾燥，水滴，静電気，手荒れ等の磨耗・変質，指の置き方，設置面の汚れ，残存指紋など、誤認の恐れを調整した閾値の設定が必要となる。
4	心理的・生理的抵抗感	犯罪者以外に指紋などの個体データを収集される経験が少ないため、個体データの採取自体に抵抗感を覚える場合がある。特に公共機関から採取される場合に当傾向が強い。また指紋だけの認証行為は、プライバシー侵害の恐れがある、との意見もある。
5	個体データ毀損（指切断）の脅威	個体データの認証により保護すべき情報や物品が重要または換金性が高い場合、その指紋などを得るために利用者自身の指を切断するなど、身体的被害が発生する脅威がある。

3．IDパスワード長所と短所

本人認証技術として必要な要件を抽出するため、従前に利用している ID パスワード方式についても、その長所・短所を整理し考察を行う。

先ず ID パスワード方式の最大の長所は、次の２点に集約される。

第１に、社会的およびシステム的に十分普及しており、利用者の理解が比較的得られやすいことである。特にパソコンに習熟している利用者であれば、その操作に関しても不自由なく利用できる。

第２に、バイオメトリックス認証が、認識装置と個体データ間で設定する認証の閾値、すなわち認証グレーゾーンが存在することに対し、パスワードのような記憶による認証行為には、ＯＫ，ＮＧのみで認証のグレーゾーンが無いこと、が考えられる。

一方 ID パスワード方式の最大の短所は、次の２点に集約される。

第１に、記憶による認証行為を行うため、当該パスワードを忘却しないように従業員番号や名前、生年月日、電話番号など利用者本人の属性に沿ったパスワードにする傾向が無くならない、ということである。

言うまでもなくこのような行為は、不正行為者からの格好の標的となりやすく、当該利用者自身はもとより、ネットワークシステム全体が脅威にさらされることにもなる。殊に、銀行・クレジットカードのような４ケタの暗証番号は、利用者の本人属性に沿ったものにしがちであり、かつ複数枚のカードの暗証番号を全て同一にしていることも多い。

第２に、ID パスワード方式だけでは、なりすましを防ぐことが困難であるということである。通常、このパスワードの遺漏による不正行為を未然に防止するため、パスワードの定期的な更新を利用者に促す、ということをシステムの管理者から依頼するが、システム的に強制しない限り、利用者自身が更新することは、まれである。

4．本人認証技術の必要要件

バイオメトリックス認証と従来の ID パスワード認証という代表的な本人認証技術を概括してきたが、ここでそれらの特徴をふまえ、本人認証技術を適用する場合の必要な考察要件を下表に示す。

［表２：本人認証技術の必要な考察要件］

項番	必要な考察要件	概要
1	脅威対抗性	暗号エンジン等を備え、不正改造・不正アタックからの防護などについて適切な策が講じられ、改ざん、なりすまし、盗聴などを防止できること。またこれら脅威の増加に備え、他のセキュリティシステムとも柔軟に連携できること。
2	社会的受容性	利用者のプライバシーに配慮し、心理的・生理的抵抗感を払拭する適切な仕組みが講じられ、利用者へ当該システムの利用に対して脅威が無い旨を示せること。また利用者の国籍・年齢・性別に因らず、利用しやすいインターフェイスを備えること。
3	認識率	真正な本人が過誤なく当該本人認証システムを利用した場合、その認識率は１００％であること。また認識装置などを介して本人認証を実施した場合、その認識率の設定について合理的な説明ができること。
4	利用者利便性	当該本人認証システムを利用する場合は、利用者が出来るだけ簡易に、かつ短時間で認証行為が行えるような仕組みが講じられていること。
5	導入・運用コスト	当該システムを利用する場合の導入において、利用者・管理者の運用負荷をできるだけ軽減できる策を講じること。また運用コストにおいても同様に、軽減できる仕組みであること。

５．実態的なセキュリティとその利用範囲

一般にセキュリティの強度は、コストの負担に比例して上がると言われている。しかし実態的には無限のコスト負担はあり得ないため、システムの設置者は、セキュリティポリシーなどに基づいて、利用する仕組みを取捨選択することになる。

例えばＩＤパスワード方式でも、前記に挙げた短所を補うため、磁気カードやスマートカード（ＣＰＵ付きＩＣカード）など、その所有物と組み合わせた認証行為を実施していることが多い。このような場合は、先ず当該カードを持っている人を本人と見做し、その本人確認の手段としてパスワード入力をさせることで本人認証を行っていることとなる。

さらに銀行カードなどの換金性が高い本人認証場面では、防犯カメラの設置など不正行為者を牽制する仕組みを有し、万一、暗証番号を何度も間違えるなどの行為で不正利用と見做した場合は、当該カードをＡＴＭに引き込み、場合によっては防犯ベルを鳴動するなどの二重三重の処置が採られている。

このように実態的なセキュリティは、その利用場面に応じたシステムの組合せによって、その強度を上げているのである。

しかしながら今日のＩＴにおけるビジネスシーンは、従来想定していた利用場面だけではなく、様々な利用シーンに急速に適合させる必要性も生じさせてきた。前述の銀行などの例では、コンビニエンスストアなど従来の銀行専用の空間以外での現金の引き出しを可能にした。またモバイルバンキングは、銀行カードが無くても、モバイルパソコンや携帯電話などから、その機能の一部を利用できるようにした。

すなわちこれからの本人認証技術は、これらの動向とも歩調を併せ、その利用場面に適した認証技術を導入していかなければならない、と考えられる。

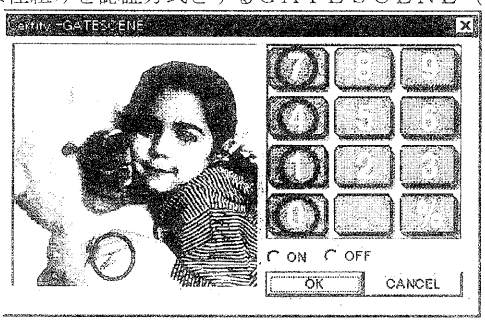
６．新しい本人認証・ＧＡＴＥＳＣＥＮＥの開発背景

前述のように従来の英数字によるパスワードでは、本人が覚えやすくできるように、生年月日や電話番号など個人の属性情報を利用する傾向がある。その最も身近な入力例は、やはり銀行やクレジットカードでＡＴＭを操作する際の４ケタの暗証番号であろう。暗証番号は、０～９までの１０種類の数字から４つを選択するので、確率的には、１０の４乗通り、すなわち１万通りの組合せであるが、利用者の多くは暗証番号を忘れないようにするため、『電話番号や生年月日』などを設定しがちだ。またカード類は、財布などに入れることが多く、財布ごとカードを落としたり盗まれたりした場合、『財布自体が、これら本人の属性情報の宝庫』であるため、前述のような暗証番号ではその機能は無いに等しい。

しかし４ケタの暗証番号を８ケタにするとなれば、『覚えきれない』などの事象が発生する。一方、暗証番号の代わりに指紋認証を行うとすれば、指紋を管理されプライバシーを侵害されることへの『心理的・生理的抵抗感』がどうしても発生してしまう。いくらセキュリティのためと言われても、自治体やクレジットカード会社に、指紋データをなかなか預ける気にはなれないのではないだろうか。

なお自筆サインを認証技術に利用するものもあるが、サインの文化に慣れていない日本などでは、やはり普及しづらい。

これらの課題背景に応えるために、バイオメトリックスを使用せずに、ＩＤパスワード方式の欠点を補う本人認証システムが必要と考え、本人の属性に依存しない、画像の位置をパスワードに設定できるという単純な仕組みを認証方式とするＧＡＴＥＳＣＥＮＥ（ゲートシーン）が開発された。下図参照。



［図１：画像パスワード利用画面例１］

パスワード
「手，７，４，１，０」

記憶例
（縦の一列ビンゴと手）

7．GATESCENEの基本原理

人間が得る情報は、８０％が視覚映像によるものであると言われている。パッと見て記憶に残る情報は実は非常に多く、色や形や位置情報など多岐にわたる。同じ４ケタの暗証番号でも、着色されているかどうかで、記憶のされ方が全く異なる。さらに数字の形や大きさを変えれば、俄然、印象が変わる。この印象、すなわちパッと見て覚えられる直感的なイメージこそが、他人が容易に知ることができないものであり、かつ本人の電話番号など静的な本人属性情報から離れたもので、再現性が要求されるパスワードとなり得るものと考えた。

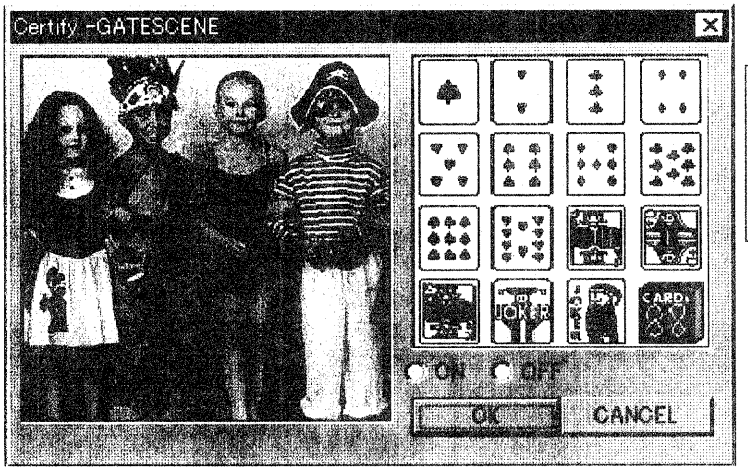
すなわちGATESCENEのパスワード生成の基本原理は、この視覚による直感的なイメージ記憶を本人認証に応用したものと言える。

8．基本構成と特長

GATESCENEは、２つの画面から構成される。左の画面は、４×４のメッシュで区切ることもできる画像であり、好みの画像(利用者自身にとって思い入れの深い画像)を使うことが出来る。右の画面は、トランプやドレミ音符など、個々のボタンに意味がある画像である。利用者は左右の画像の位置情報と順番情報をパスワードとして設定することができる。(どちらか一方の画面でのパスワード設定も可能)

パスワードの利用例を以下に示す。例では４人の子供の写真画像を入れた。右側の画像は、トランプであるが、これはあらかじめ用意された画像コンテンツ(テンキーやドレミ音符等)から、利用者が選択したものである。標準では左右の画面で各９種類の画像が用意されている。

これらの画像のどこを選択(クリック)するかをパスワードとして組み込むことで、本人には覚えることが容易であるが、本人以外には予測のつきにくいパスワード設定が可能となる。



パスワード
「顔，５，２，７，４」

記憶例
（帽子からジグザグ）

［図２：画像パスワード利用画面例２］

パスワードの設定例として、左の写真画像は、帽子を被った子供の顔を一番目のパスワードとした。右のトランプは、数字を電話番号で設定しても良いが、もっと簡単に「帽子から始まるジグザグ」と覚えても良い。こうすることで、暗証番号（４桁）の記憶の壁を、簡単に突破し、本人の属性情報から依存しないパスワードも簡単にできることとなる。このようなGATESCENEのパスワード生成の特長は、以下に列挙することができる。これらは先に挙げた本人認証技術の必要な考察要件を満たすものと考える。

①単純な操作でも高度なセキュリティを実現。(トランプ版：８文字選択で１兆通りの組合せ)
②直感的でスムーズな操作が可能。
③本人の属性（電話番号等）に依存しない。
④専用の認識装置（ハードウェア）は不要。
⑤好みの画像を入れることで愛着のあるパスワード設定が可能。
⑥プライバシー侵害の恐れは皆無。

⑦指紋押捺等の身体的特徴管理による心理的・生理的抵抗感が無い。
⑧小学生や高齢者などキーボード操作が利用者でも操作しやすいバリアフリーインターフェイス。
⑨性別、年齢、国籍などを問わないワールドワイドなインターフェイス。
⑩DES等の暗号エンジン，改ざん検出機能，不正アタック時のロック機能，連携インターフェイスなどを装備。

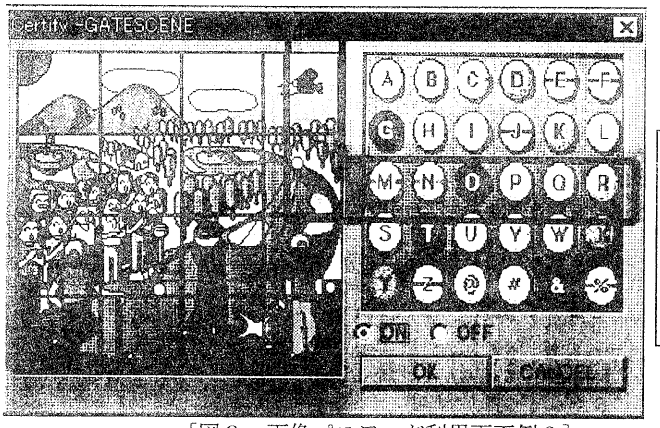
9．GATESCENE(画像パスワード)の信頼性と安全性

一般的にパスワードセキュリティの信頼性は、総当たりの確率論に帰結しがちだ。しかしこれは、あくまで数学上の確率論であって、実態論ではない。なぜならパスワードの入力回数を無制限に許可してしまうシステムは、社会システムでは存在しないからだ。実際のシステムでは、数回のエラー入力で、入力はロックされる。注目すべきは、ロック機能をすり抜けて不正利用があるという事実の方である。

４ケタの数字だけの暗証番号は、１万通りの組合せがあると前述したが、これは仮に『無制限に暗証番号の入力を許可するシステムがあるとすれば』という条件付であり、現実にはそのようなＡＴＭは存在しない。したがって本人属性から離れた暗証番号（パスワード）を簡単に設定できるか、ということは、現実的なセキュリティの面では大変重要なことである。

なお数学的な総当たりの確率論という面から見ても、ＧＡＴＥＳＣＥＮＥの信頼性は、英数字を利用するのと遜色なく利用することが可能だ。

具体例を挙げれば、図３のような画像ならば、１６個のメッシュに区切られた左の画像（１６種）と、記号を含むアルファベットを表示した右の画像（３０種）の合計は、４６種となるためで、これは英数字（３６種）のパスワードよりも多い入力環境となり、実質的にはキーボードで入力するパスワード環境と大差がない。



パスワード
「カラス，ボール，M,N,O,P,Q,R」

記憶例
（カラスからＬ字型）

［図３：画像パスワード利用画面例３］

もちろん文字種を、より多くしたコンテンツをさらに用意しても良いが、実質は前述のように確率論だけでセキュリティが守られているわけではないので、文字種を増やす有用性は少ない。

むしろ利用者が入力するパスワードの記憶の負担を少なく出来て、簡単に４ケタを超えて暗証番号を設定できることの方が重要な要素である。画像の位置による認証は、文字の意味だけでなく、色や形での選択や図形を描くような操作(例えばＬ字型)での認証行為も可能とする。さらにシステムのロック機能を組み合わせると、実態的なセキュリティ強度は確実に増していく。

また左右の性質の異なる２画面は、不正利用者への防犯牽制効果を考慮しているためである。仮にパスワードをどちらか一方の画面でしか設定していなくても、不正利用者にとってみれば、他方の画面からもパスワード入力の試行機会を与えることとなる。これは、不正利用者による推測を困難にさせる心理を働かせる。つまり動作していない防犯カメラでも牽制効果を発揮することと同様な効果を発揮する。

なお利用時の画像データ(左の画面)を自分の写真やアミューズメント性の高いものとすることで、楽しみながら利用できることと、その画像を交換するタイミングで、利用者が自発的にパスワードも更新する契機とすることができる、というのも見逃せない長所であろう。

１０．容易なシステム連携

GATESCENE は、設定した画像のパスワードを既存の文字列のパスワードに結びつけることが可能である。つまりバックボーンのシステムを変更することなく、フロントエンド(利用者画面)のみを画像パスワードに変更することができる。これは、GATESCENE での認証結果がＯＫであれば、既存システムで利用していたパスワードを、GATESCENE からセキュアに送信することができる機能を有しているためである。

１１．ＧＡＴＥＳＣＥＮＥの適用分野

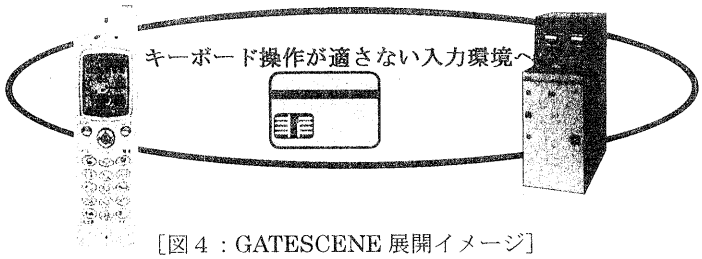
GATESCENE は、Windows にログオンするための製品「Logon GATESCENE」を開発したところであるが、Web ページ上でのアクセス制御への利用や、自治体や銀行等のカード(スマートカード)での認証や携帯電話での認証など、広範な場面での利用が考えられている。特に今後は、携帯電話やスマートカードが情報端末として重要になってくると考えられ、これらキーボード操作が適さない入力環境に対する認証に、特に適しているインターフェイスと考える。

スマートカードは、ＩＣチップ内に、ＣＰＵとＯＳ及びプログラム等が格納できるようになっており、GATESCENE のプログラムもこのチップ内に格納される。現在スマートカードは、磁気カードからの移行期を迎えているが、スマートカードになれば、電子商取引をはじめとする様々なサービスの提供が可能になると言われている。また同時にチップ内に格納できるデータ量も磁気カードと比べ圧倒的に増加する。（約８０００文字の情報が格納可能）

しかしセキュリティの面から言えば、これは保護すべき機能やデータが増えたことを意味しており、特定機能しかない磁気カードで４ケタの暗証番号で保護していたことを、そのまま多機能のスマートカードに移行するならば、その分、逆にセキュリティ上の脅威を増していることに他ならない。

なおスマートカードは、不正利用者からの保護機能として、数回、暗証番号を誤入力すれば、ロックされるという機能がある。しかしこのロック機能も現状と同様の４ケタの暗証番号で、しかも生年月日などを設定していたならば、スマートカードに移行したとしても、推測によるなりすましを防ぐ、というセキュリティ上の効果は認められない。現在もカードの不正利用額は増加の一途を辿っているが、その犯罪の手段は、ネットワークに進入を試みるような高度な技術を要するものでは無く、より原始的なパスワード破りなのである。

我々は、このような人間とコンピュータの接点である本人認証の分野でのセキュリティソリューションが、社会公共的に有用と考え、この分野での GATESCENE の適用を推進中である。



［図４：GATESCENE 展開イメージ］

１２．おわりに

本稿では本人認証の必要要件をまとめ、GATESCENE という新しい本人認証のインターフェイスを紹介した。しかしセキュリティに万全は無い。したがって必ず適材適所のセキュリティソリューションが必要となるはずである。GATESCENE は、その意味では、１つの認証ツールに過ぎないとも言える。

しかしながら、シンプルな機能だけに様々な分野への応用も可能だ。今後ともセキュリティの需要に適合したソリューションを提供していく所存である。

以上