Vol.2010-DPS-142 No.43
Vol.2010-CSEC-48 No.43
2010/3/5

機密情報入力方式の検討

桜井鐘治[†]　　後沢忍[†]

インターネットを使った取引では，マンインザミドル攻撃や，トロイの木馬などの不正なソフトウェアを端末に送り込むことにより，利用者が意図しない取引を行う問題が指摘されている．本稿では，これらの攻撃への対策として，複数カーソルが異なる動きをする GUI を使った対話的な情報入力方式を提案する．提案方式では，利用者がサーバとの間であらかじめ共有する数値などの情報を基に GUI を使ってパスワードや口座番号などの機密情報を相対的に指定する．さらにこの GUI 上で別の任意な値を指定した後に，この任意の値について質問をすることで利用者が入力した機密情報を決定する．本稿では，提案方式の安全性についても考察する．

Input Method of Sensitive Information Online

Shoji Sakurai[†]　and Shinobu Ushirozawa[†]

In the banking transactions over the Internet, the risk of attacks that execute transfers which users do not intend is pointed out. Such attacks are done with Man-in-the-middle attack or malicious software such as Trojan horses which are sent to the user's terminals stealthily. In this paper, we propose an interactive input method of sensitive information such as passwords and account numbers against these attacks. Our method relatively decides the sensitive information that a user inputs through GUI which has different two or more cursors. The user inputs the information based on a secret between the user and a server, and moves one of the cursors from the input value to an arbitrary value, and then the server decides the user's input by questioning about the arbitrary value. Moreover, we discuss the safety of our proposed method.

1. はじめに

インターネット上でのフィッシングが大きな社会問題になってから久しいが，金融機関からなどと称して利用者に不正なサイトへの接続を促すメールを送付し，利用者のパスワードを盗み取り悪用する従来型のフィッシングは近年減少している．その一方で，利用者のPC上で密かに動作し，パスワードを不正に盗み取るキーロガーや，DNS応答の書換えにより不正なサーバに接続させてパスワードを盗み取るファーミングなどの，より高度な攻撃手法が増加している[1]．これらの攻撃への対策として金融機関などではワンタイムパスワード（以降，OTPとする）トークンの導入が進んでいる．しかしこの対策に対しても，不正なサイトでOTPを盗み取り，これを即座に使って不正を働くリアルタイムマンインザミドル（以降，MITMとする）攻撃による被害も報告されている[2][3]．一方，以前より“corrupt teller problem”などとも呼ばれてその危険性が指摘されていた問題[4]に対しても，マンインザブラウザ（以降，MITBとする）攻撃と呼ばれる攻撃が存在する．MITBについては，PCとサーバとの間での認証が確立した後に，利用者がWebブラウザに対して入力した振込先の口座番号を不正な口座の番号に書き換えて送信する“Silent Banker”と名付けられたトロイの木馬が検出[5]されている．

本稿では，今後実害の発生が予想される MITB 攻撃への対策として，複数カーソルが異なる動きをする GUI を使い，利用者がサーバとの間であらかじめ共有する数値などの情報を基にパスワードや口座番号などの機密情報を相対的に指定し，さらに別の任意な値を指定した後に，この任意の値について質問をすることで利用者が入力した機密情報を決定する対話的な入力方式を提案する．以降，2 章では，関連研究について記述し，3 章で攻撃者が攻撃の対象とするシステムのモデルについて記述する．4 章で今回提案する機密情報入力方式を示し，5 章で提案方式の信頼性について評価を行い，6 章にまとめを示す．

2. 関連研究

本章では，MITM攻撃やさらにMITB攻撃への対策として提案されている方式について簡単に紹介する．インターネットバンキングにおける不正と対策についての広範囲なサーベイは，文献6)を参照されたい．

インターネットバンキングの不正対策としては，利用者とサーバとの間で二つの異なる通信経路を用いるもの（以降，二経路認証とする）と，利用者に二つの異なる認

[†] 三菱電機株式会社　情報技術総合研究所
Mitsubishi Electric Corporation, Information　Technology　R&D　Center

Vol.2010-DPS-142 No.43
Vol.2010-CSEC-48 No.43
2010/3/5

証要素を入力させるもの（以降，二要素認証とする）に大別できる．

二経路認証としては，サーバが利用者のPCから振込要求を受けた際に，振込先口座番号と金額などの取引の一部の情報と合わせて取引毎にユニークな取引コードと呼ばれる値を利用者の携帯電話へ送信し，利用者が携帯電話の画面に表示される取引の情報を確認し，取引情報が不正に改ざんされていることに気づいた場合には，取引コードをPC上のWebブラウザへ入力せずに取引を中止にすることで不正を防ぐ対策が実施されている[7]．この対策は，携帯電話へ送信する情報について，送信元を詐称できないことと送信されるメッセージが盗聴・改ざんできないことを前提としており，さらに，携帯電話については，不正を働くソフトウェアから隔離されたセキュアなプラットフォームであることを前提としている．

一方，二要素認証としては，パスワードやPIN(Personal Identity Number)による利用者認証加えて，サーバが利用者のPCから振込要求を受けた際に，振込先口座番号と金額などの取引の一部の情報を，PCに接続したトークンとサーバとの間で双方向認証を実施して確立したSSL/TLSのセッションを使ってサーバからトークンへ送り，利用者がトークンの画面上に表示される取引の情報を確認し，取引の情報が不正に改ざんされていることに気づいた場合には，トークンの中止ボタンを押下することで不正を防ぐ対策が提案されている[8]．この対策では，PCに接続したトークンが，PCから内部の情報を不正に取得しようとする攻撃や内部のプログラムを改ざんしようとする攻撃に対して，耐性を備えていることを前提としている．

さらに，これらの対策は何れも，利用者に対して取引の情報（振込先口座番号や振込金額など）を表示し，利用者はこれらの情報と自身が PC に入力した振込要求の情報とが一致しているかを正しく確認することを前提としている．

しかしながら，このような入力した口座番号が改ざんされていないかを確認させる方法について行われた検証実験[9]では，8 桁の振込先口座番号の内の 5 桁を改ざんしても約 21%の割合で利用者が確認に失敗したことが報告されている．

これに対して，二経路認証を改良し，携帯電話上でサーバから受信した暗号化鍵を用いて取引に必要な振込先口座番号を暗号化し，これをPC上のWebブラウザからサーバへ提供し，利用者がサーバから表示される振込先口座名をPCの画面上で確認できるようにすることで，この確認誤りを防ぐ方式[10]があるが，携帯電話で暗号化された口座番号を利用者がPCへ入力することが必要であり，利便性に課題が残る．

3. モデルおよび保護対象情報の定義

本章では，攻撃者が攻撃の対象とするシステムのモデルを定義し，攻撃から保護する機密情報を定義する．図 1 にシステムのモデルを示す．

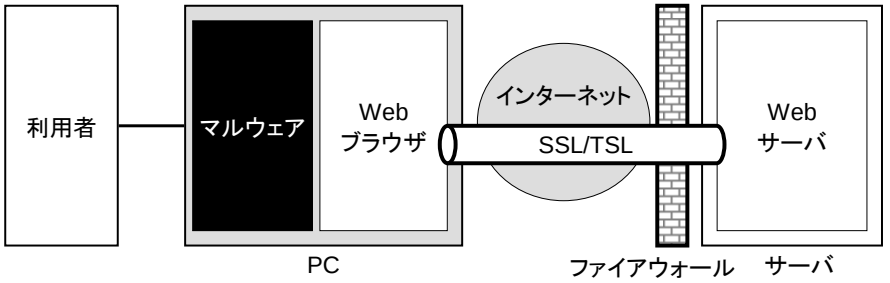


図 1　システムのモデル
Figure 1 Model of system

利用者は，PC を操作し，PC は正規の金融機関や企業が運営する正式なサーバとインターネットを介して接続されている．利用者は，PC 上の Web ブラウザを利用し，正式なサーバ上の Web サーバに対しての取引を実行する．Web ブラウザと Web サーバの間の通信は SSL/TLS により保護されており，インターネット上で取引の情報は改ざんできないものとする．金融機関のサーバはファイアウォールによってインターネットからの攻撃に対して保護されており，サーバ上で実行される取引はインターネットからの攻撃では改ざんできないものとする．一方攻撃者は，PC に対しては，利用者の取引情報を不正に改ざんしたり，利用者の秘密情報を盗んだりする不正なソフトウェア（以降，マルウェアとする）を送り込むことができるものとする．

本稿では，マルウェアによる攻撃から保護する情報として 2 種類の情報を定義する．1 つ目の情報は，振込先の口座番号であり，攻撃者は振込先口座番号を不正に変更することで利用者から不正に送金を受けることができる．2 つ目の情報は，クレジットカード番号であり，攻撃者がクレジットカード番号を不正に入手することで，利用者に成りすましてインターネット上で不正なカード支払いが可能となる．

4. 提案方式

4.1 提案方式の概念

本章では，マルウェアによる攻撃に対する対策として提案する機密入力方式について記述する．最初に提案方式の概念について示す．図 2 に，提案方式の概念を示す．

Step0：利用者とサーバは他人が知らない共有情報 $S(=s_1,s_2,\ldots,s_n)$を共有している．

Step1：利用者は，共有情報 S を変換 α により入力情報 $I(=i_1,i_2,\ldots,i_n)$に変換する．この際，変換 α は攻撃者も含めて公知であるが，共有情報 s_i から変換 α によって得られる

Vol.2010-DPS-142 No.43
Vol.2010-CSEC-48 No.43
2010/3/5

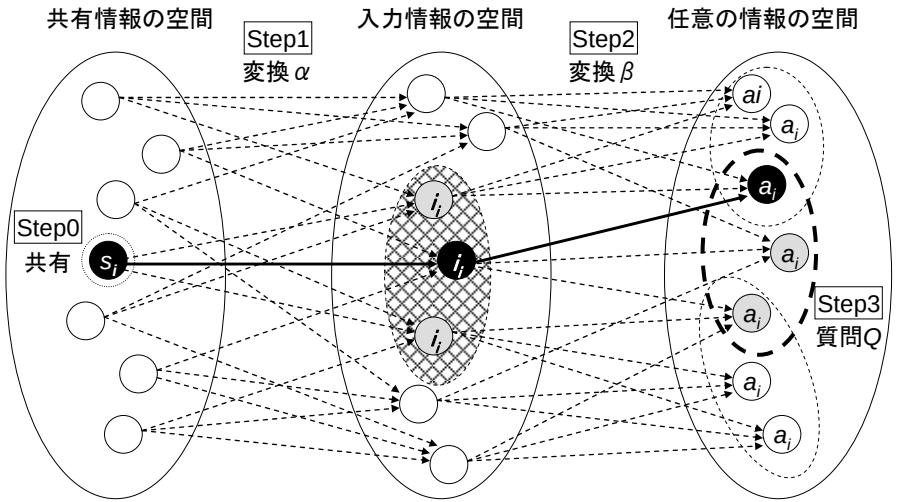


図 2 提案方式の概念
Figure 2 Concept of proposed method

入力情報 i_i は 1 つではなく複数存在する．
Step2：利用者は，変換 β により入力情報 I を任意の情報 $A(=a_1,a_2,..,a_n)$ に変換する．この際，変換 β は攻撃者も含めて公知であるが，入力情報 i_i から変換によって得られる任意の値 a_i は 1 つではなく複数存在する．
Step3：システムは，任意の情報 a_i について利用者に質問(Q)をし，質問に対する応答(R)を基に共有情報 s_i から得られる複数の入力情報 i_i の内で利用者が入力した i_i を絞り込む．

攻撃者にとっては，変換 α，変換 β と質問 Q および応答 R が判っても，共有情報 S が判らないため，利用者がどの S に対して変換 α を行い，さらにどの I に対して変換 β を行って得られた A について質問 Q と応答 R がサーバと利用者間で行われているかが分からないため，入力情報 I を一意に絞り込むことができない．

入力値 α だけの変換をした後に入力値についての質問を行うことに対して，さらに任意の値への変換 β を行った後に任意の値についての質問を行うことで，入力値の絞込みが難しくなると予想する．

4.2 具体的な例

本節では，前節で示した概念を適用した具体的な一例を示す．

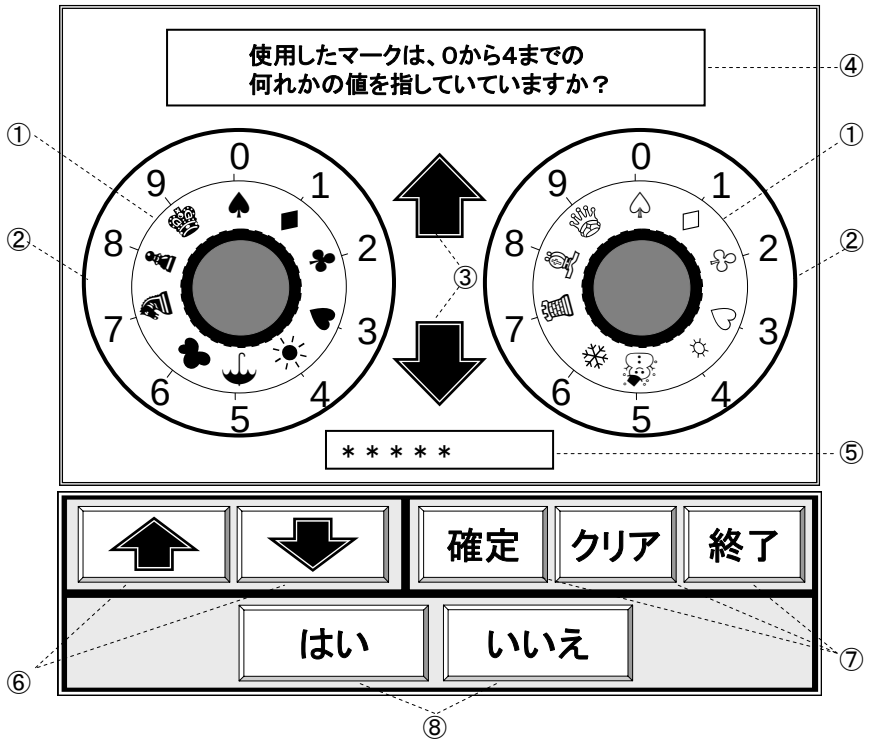


図 3 具体的な例の入力画面
Figure 3 Example of entry screen

図 3 に，具体的な例の入力画面を示す．図 3 の入力画面には，上下に分かれており，上部の画面で利用者への情報を表示し，下部の入力ボタンで利用者からの入力を受け付ける．上部の画面は，情報を入力する際にカーソルとして使用する数種類のマークを配置した内側ダイヤル(図 3 の①)と入力する値を配置した外側ダイヤル(図 3 の②)の組が複数存在し，カーソルの移動方向，つまりこの例では内側ダイヤルの回転方向を示す矢印(図 3 の③)と操作の指示や質問を表示するメッセージウィンドウ(図 3 の④)および値が確定した入力情報を“*”に置き換えて表示する確定ウィンドウ(図 3 の⑤)を配置する．一方，下部の画面で入力ボタンを提供し，各移動方向についての移動ボタン(図 3 の⑥)と，確定，キャンセル，終了を指示するための各ボタン(図

Vol.2010-DPS-142 No.43
Vol.2010-CSEC-48 No.43
2010/3/5

3 の⑦)および質問に対して応答を行う際に使用する「はい」ボタンと「いいえ」ボタン(図 3 の⑧)が配置されている．

次に，図 3 の入力画面を使った入力手順について説明する．まだ何も入力していない状態では，メッセージウィンドウには「任意のマークを選び，1 つ目の共有情報に合わせて，確定ボタンを押してください.」との指示が表示され，確定ウィンドウには何も表示されていない．図 3 の入力画面では，上向きの移動ボタンを押すと，左側の内側ダイヤルは反時計回りにマーク 1 つ分だけ移動する．同時に右側の内側ダイヤルは時計回りにマーク 1 つ分だけ移動する．逆に下向きの移動ボタンを押すと，左側の内側ダイヤルは時計回りにマーク 1 つ分だけ移動し，同時に右側の内側ダイヤルは反時計回りにマーク 1 つ分だけ移動する．

Step1：利用者は，内側ダイヤル上に配置されたマークの何れか(例えば左側の◆)を選んで，サーバと共有している共有情報 S の 1 つ目の値 s_1（例えば 5）に選んだマークが来るように移動ボタンを使って内側ダイヤルを移動させ,確定ボタンを押下すると，メッセージウィンドウの指示は「同じマークを 1 つ目の入力値に合わせて，確定ボタンを押してください.」に変化する．

Step2:利用者は，入力する情報 I の 1 つめの値 i_1（例えば 3）に選んだマーク(ここでは◆)が来るように移動ボタンを使って内側ダイヤルを移動(ここでは上向き矢印ボタンを 2 回押して左の内側ダイヤルを反時計回りに 2 つ分移動)させ,確定ボタンを押下すると，メッセージウィンドウの指示は「同じマークを適当な値に合わせて，確定ボタンを押してください.」に変化する．

Step3：利用者は，選んだマークが任意の値 a_1（例えば 1）に来るように移動ボタンを使って内側ダイヤルを移動(ここでは上向き矢印ボタンを 2 回押して左の内側ダイヤルを反時計回りに 2 つ分移動)させ，確定ボタンを押下すると，メッセージウィンドウには「使用したマークは 0 から 4 までの何れかの値を指していますか?」との質問が表示される．

Step4：利用者が，質問に対して選んだマーク(ここでは◆)についての応答を「はい」ボタンまたは「いいえ」ボタンを押すことで答える(このとき，◆は 1 を指しているので「はい」を答える)と，確定ウィンドウに“*”が追加表示されて，メッセージウィンドウには，「任意のマークを選んで，2 つ目の共有情報に合わせて，確定ボタンを押してください.」との指示が表示される．以降，利用者は 2 つ目の共有情報 s_2 を使って Step1 から Step4 の手順を行い，2 つ目の入力情報 i_2 を入力し，最後の入力値 i_n を確定するまで上記の手順を繰り返す．クリアボタンを押した際には，入力していた j 番目の値の共有値 s_j，入力値 i_j および任意の情報 a_j の確定がキャンセルされ，利用者は，共有値 s_j の入力から手順を再開することができる．なお，2 つ目以降の任意のマークは，1 つ目のマークと別のものを選んで良い．

5. 評価

本章では，提案方式のセキュリティ強度について評価する．まず，例として図 3 の画面の状態において,「はい」を押した場合に，入力操作を見ていた攻撃者が入力情報の候補として考える値について求める．図 4 に，入力値を確定してから任意の値を確定するまでの移動量に応じた入力情報候補の一覧を示す．図 4 では，図 3 の画面の状態で質問に対して「はい」ボタンで任意の値を確定する前に，入力値を入力してから上向きボタンを i 回押したとした場合の左ダイヤルにおける入力値の候補 $IP_L(i)$ と左ダイヤルにおける入力値候補 $IP_R(i)$ を各行の上下段に示す．$i=0$ の場合は，任意の値の候

i	左	♠	♦	♣	♥	☀	☂	☘	♘	♝	♚
	右	♤	♢	♧	♡	☼	☃	❄	♖	♗	♔
0	$IP_L(0)$	0	1	2	3	4	5	6	7	8	9
	$IP_R(0)$	0	1	2	3	4	5	6	7	8	9
1	$IP_L(1)$	1	2	3	4	5	6	7	8	9	0
	$IP_R(1)$	9	0	1	2	3	4	5	6	7	8
2	$IP_L(2)$	2	3	4	5	6	7	8	9	0	1
	$IP_R(2)$	8	9	0	1	2	3	4	5	6	7
3	$IP_L(3)$	3	4	5	6	7	8	9	0	1	2
	$IP_R(3)$	7	8	9	0	1	2	3	4	5	6
4	$IP_L(4)$	4	5	6	7	8	9	0	1	2	3
	$IP_R(4)$	6	7	8	9	0	1	2	3	4	5
5	$IP_L(5)$	5	6	7	8	9	0	1	2	3	4
	$IP_R(5)$	5	6	7	8	9	0	1	2	3	4
6	$IP_L(6)$	6	7	8	9	0	1	2	3	4	5
	$IP_R(6)$	4	5	6	7	8	9	0	1	2	3
7	$IP_L(7)$	7	8	9	0	1	2	3	4	5	6
	$IP_R(7)$	3	4	5	6	7	8	9	0	1	2
8	$IP_L(8)$	8	9	0	1	2	3	4	5	6	7
	$IP_R(8)$	2	3	4	5	6	7	8	9	0	1
9	$IP_L(9)$	9	0	1	2	3	4	5	6	7	8
	$IP_R(9)$	1	2	3	4	5	6	7	8	9	0

図 4 移動量に応じた入力値候補の一覧
Figure 4 Input candidates based on displacement

Vol.2010-DPS-142 No.43
Vol.2010-CSEC-48 No.43
2010/3/5

補と入力値の候補は一致し，$IP_L(0)$={0,1,2,3,4}，$IP_R(0)$={0,1,2,3,4}で，攻撃者にとっての入力値候補 $IP(0)$は，これらの候補の和となり，$IP(0)=IP_L(0)\cup IP_R(0)$ ={0,1,2,3,4}である．同様に，$IP(1) = IP_L(1) \cup IP_R(1)$ ={0,1,2,3,4,5,9}，$IP(2) = IPL(2) \cup IPR(2)$ = {0,1,2,3,4,5,6,8,9}，$IP(3) = IP_L(3)\cup IP_R(3)$ = {0,1,3,4,5,6,7,8,9}，$IP(4) = IP_L(4)\cup IP_R(4)$ = {0,4,5,6,7,8,9}，$IP(5) = IP_L(5)\cup IP_R(5)$ = {5,6,7,8,9}，$IP(6)=IP_L(6)\cup IP_R(6)$ = {0,4,5,6,7,8,9}，$IP(7) = IP_L(7)\cup IP_R(7)$ = {0,1,3,4,5,6,7,8,9}，$IP(8) = IP_L(8)\cup IP_R(8)$ = {0,1,2,3,4,5,6,8,9}，$IP(9) = IP_L(9)\cup IP_R(9)$ = {0,1.2,3,4,5,9}となる．

このように，入力情報の候補は，任意の値を確定する前の移動量に応じて変化し，候補数$|IP(i)|$は，5,7,9 の何れかで変化する．

次に，攻撃者が同じ入力情報の入力操作を複数回繰り返し見ていた場合の入力情報の候補について求めた結果を示す．攻撃者は，各回の入力操作で得られた入力情報の候補の積を求めることにより，入力候補を絞り込むことができる．

利用者は入力の際の移動量をランダムに選ぶものとして，固定の機密情報の入力を繰り返し行った場合に，攻撃者が入力操作を繰り返し見た回数を入力回数とし，この回数に対する入力候補数の推移をシミュレーションにより算出したものを図 5 に示す．シミュレーションで算出した入力候補数は，移動量を擬似乱数で生成し，各入力回後の候補数をそれぞれ 10000 個算出した平均値である．また，図 5 には，比較として入力値について直接質問と応答を行った場合の入力候補値の推移を算出したものを合わせて示す．さらに図 5 には，4 桁の PIN，7 桁の口座番号，16 桁のクレジットカード番号の入力操作を複数回見た攻撃者が，これらの機密情報を言い当てる確率の推移も合わせて示す．

入力可能な値が 10 個の場合に，入力した値に対して直接的に質問をする方式では，1 回の入力で入力候補が半分の 5 個，2 回の入力で約 3.4 個となる．これに対して，提案方式では，入力した値について直接質問をせずに，さらに別の任意な値を指定した後にこの値について質問をすることで，1 回の入力では約 7.4 個，2 回の入力でも 5.8 個の入力候補が残る．このことにより，4 桁の PIN の入力を 2 回行った場合に，攻撃者が PIN を言い当てる確率は，入力値について質問をする方式では約 130 分の 1 であるのに対し，提案方式では 1000 分の 1 以下となる．これらより，4.1 での予想が正しかったことがわかる．

一方，提案方式には，まだ少なくとも以下に示す課題がある．

提案方式は，入力値を確定した後に利用者が指定した任意の値についてサーバが質問をし，この質問に対する利用者の応答をもとに左右どちらのダイヤルを入力に使用したかを判別している．しかしながら，質問を固定とすると，共有情報によっては，入力値や任意の値が何で合っても，左右のダイヤルのどちらを使ったかを判別できない状況が発生する．具体的には，共有値が質問の範囲の真ん中の値または，その値のダイヤル上で反対の位置に該当する値の場合には，入力値およびその後に指定する任

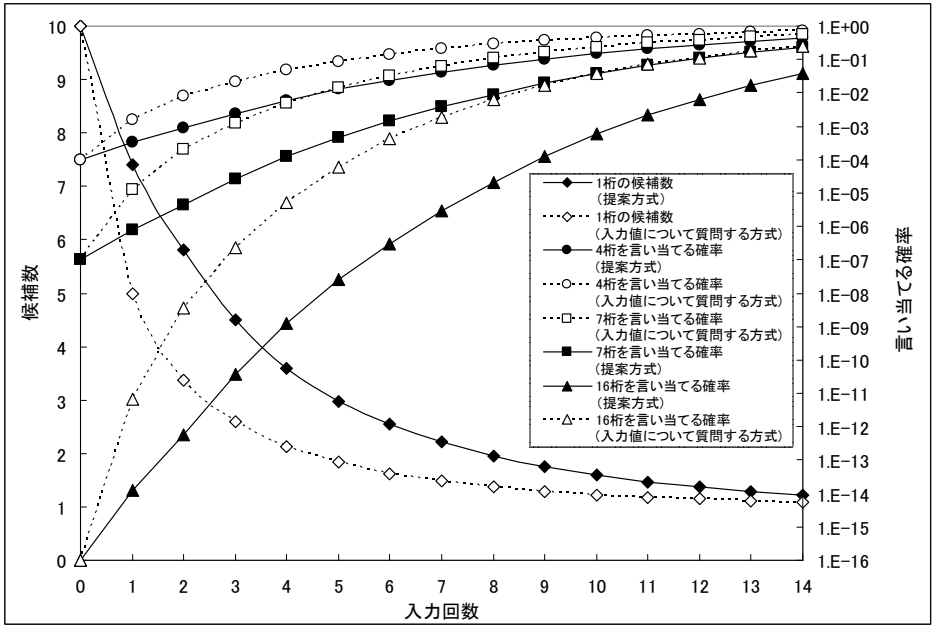
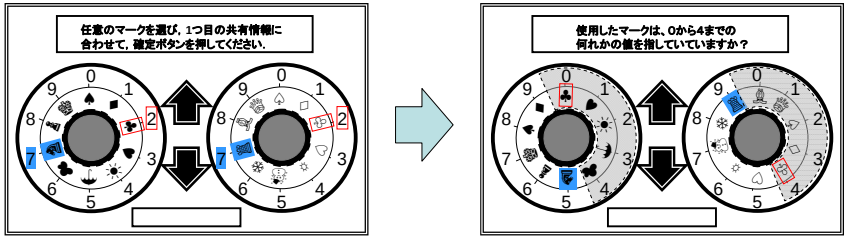


図 5 入力回数に対する機密情報の入力候補数と攻撃者が言い当てる確率の推移
Figure 5 Number of input candidates of sensitive information and probability of guessing the value right

意の値が何であっても，左右の区別が付かない．具体的な例を図 6 に示す．図 6 の例では，質問の範囲は「0 から 4 」である．このとき，共有値がこの範囲の真ん中の値，つまり 2 の時には，左側のダイヤルで共有値 2 に合わせたマークが質問の範囲「0 から 4」に含まれる場合には，右側のダイヤルで共有値 2 に合わせたマークも必ず質問の範囲に含まれる．逆に，左側のダイヤルで共有値 2 に合わせたマークが質問の範囲「0 から 4」に含まれない場合には，右側のダイヤルで共有値 2 に合わせたマークも必ず質問の範囲に含まれない．このため，2 が共有値の場合には，サーバは質問によって入力値を確定することができない．同様に，共有値がダイヤル上で 2 の反対の位置にある 7 の時にも，サーバは入力値を確定することができない． このため，サーバ側では，共有値に応じて質問の範囲を変えることが必要であり，攻撃者には質問より共有値についてのヒントを得ることができる．

また，共有値が上記に該当に相当しない値であっても，質問の範囲によっては，サ

Vol.2010-DPS-142 No.43
Vol.2010-CSEC-48 No.43
2010/3/5



(a)共有値に合わせた状態　(b)任意の値に合わせた状態

図 6　左右のダイヤルが判別できない場合の例

Figure 6 Example of case where right and left distinction is impossible

ーバ側で左右のダイヤルそれぞれについて算出した 2 つの任意の値がとも質問の範囲に含まれる場合がある．この場合にも，サーバは利用者がどちらの値を使用したのかが分からないため，入力値を確定することができない．これに対しては，サーバ側で左右の判別が付くように質問の範囲を選ぶことが必要であり，攻撃者は質問より入力値についてのヒントを得ることができる．

これらの質問の選び方によって得られるヒントの評価については今後の課題とする．

6. おわりに

本稿では，今後実害の発生が予想される MITB 攻撃への対策として，複数カーソルが異なる動きをする GUI を使い，利用者がサーバとの間で共有する情報を基にパスワードや口座番号などの機密情報を相対的に指定し，さらに別の任意な値を指定した後に，この任意の値について質問をすることで利用者が入力した機密情報を決定する対話的な入力方式を提案した．また，提案方式の安全性について評価を行った．提案方式は，入力した値について直接質問をせずに，さらに別の任意な値を指定した後にこの値について質問をすることで，攻撃者が入力を見た場合に，入力した値について直接質問する方式に比べて入力値を言い当てる確率を抑えることを示した．今後は，質問の選び方によって攻撃者に与えるヒントの影響を評価するとともに，質問の選び方による攻撃者へのヒントを減らす改良について検討を行う．

参考文献

1) Anti-Phishing Work Group (APWG): Phishing Activity Trends Report Q1/2008 (online), available from <http://www.antiphishing.org/reports/apwg_report_Q2_2008.pdf> (accessed 2010-02-03).

2) ABN-AMRO: ABN AMRO intensiveert campagne voor veilig computergebruik na virusaanval op PC's klanten (online), available from <http://www.group.abnamro.com/pressroom/pressreleasedetail.cfm?ReleaseID=278555> (accessed 2010-02-03).

3) Hegt, S.: Analysis of Current and Future Phishing Attacks on Internet Banking Services, Master Thesis, Technische Universiteit Eindhoven (2008).

4) Jakobsson, M., Myers, S.: Phishing and Countermeasures, Wiley-Interscience (2006).

5) Liam O Murchu: Banking in Silence, Symantec Corporation (online), available from <https://forums.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/181> (accessed 2010-02-03).

6) Oppliger R., Rytz R., and Holderegger T., Internet banking: Client-side attacks and protection mechanisms, Computer, vol.42, no.6, pp.27--33, 2009.

7) Bank Austria: mobileTAN information (online), available from <http://www.bankaustria.at/de/19741.html> (accessed 2010-02-03).

8) Weigold, T., Kramp, T., Hermann, R., Horing, F., Buhler, P. and Baentsch M.: The Zurich Trusted Information Channel - An Efficient Defence against Man-in-the-Middle and Malicious Software Attacks, Proc. TRUST 2008, LNCS 4968, pp.75-91 (2008).

9) AlZomai, M., AlFayyadh, B., Josang, A. and McCullagh, A: An Exprimental Investigation of the Usability of Transaction Authorization in Online Bank Security Systems, Proc. The Australasian conference on Information security (AISC2008), Australian Computer Society, Inc., pp.65-73(2008).

10) 桜井鐘治: 取引認証の改良と安全性・利便性についての考察, 2009-CSEC-44, Vol.2009, No. 20, pp.217-222(2009).