マルチメディア通信と分散処理 71−14
（１９９５．７．１３）

逐次捕捉型モーバイルコンピューテイング環境に於けるセキュリテイ方式の考察

田窪昭夫、石川　睦、水野忠則（静岡大学工学部）

Security System for Mobile Computing Environment

Akio Takubo, Mutsumi Ishikawa and Tadanori Mizuno (Shizuoka University)

概　要

コンピュータとネットワークの進展の結果、コンピュータはネットワークを介して相互に接続され、データがリアルタイムで相互に行き来している．コンピュータシステム利用は、端末を介してと言うことで、端末の側でありさえすれば、いつでも利用できる．一方、コンピュータシステム利用の必要性は、端末の配置とは無関係にあらゆる場面で生じている．端末を離れた場所でのコンピュータシステム利用必要性に対応したモーバイルコンピューテイング環境の例を挙げて、サーバＩＤ/ユーザＩＤ付与方式によるユーザ認証方法を提案する．

Abstract

The computers are connected with each other by the network according to the progress of technology in the field of the compurter and network, and then all of the data to be processed are transfered quickly and at the real-time through the computer system network. Against the truth that the user can use at any time, the user must be to attend aside the computer system to use the facility of the computer system. The nesecities for using the computer system exist anywhere and anytime regard less the location of the computer system. For this requirement the mobile computing system are hoped. In this article the examples of mobile computing environment and its user certification model by the user ID assignment related to the server ID.

まえがき

コンピュータとネットワークの進展の結果、コンピュータはネットワークを介して相互に接続され、データがリアルタイムで相互に行き来している．コンピュータシステムの利用は、端末（以下、エンド、または、Ｅｎｄ）を介してと言うことで、Ｅｎｄ（端末）の傍でありさえすれば、コンピュータシステム利用の必要性が生じれば、すぐ利用できる．一方、コンピュータシステム利用の必要性は、Ｅｎｄ（端末）の配置とは無関係にあらゆる場面で生じている．こうしたＥｎｄ（端末）を離れた場所でのコンピュータシステム利用の必要性に応えるシステムとして、モーバイルコンピューティングシステムが考えられる．

従来のコンピュータシステム環境では、Ｅｎｄ（端末）の設置場所が固定されており、コンピュータシステム利用のためには、わざわざそこまで足を運ばなけ

ればなない．このようなコンピュータシステムを、ＦＣＥ（fixed computing environment）と呼ぶのに対比して、Ｅｎｄ（端末）の設置場所を離れて、どこからでもコンピュータシステムを利用出来る環境を、ＭＣＥ（mobile computing environment）と呼ぶ（図.１）．また、ＦＣＥに関わるネットワークをＦＮ（固定網）とよび、ＭＣＥに関わるネットワークを、ＭＮ（モーバイルネットワーク）と呼ぶ．

ここでは、ＭＣＥの利用環境の例を挙げて、ＦＣＥとの違いを述べると共に、ＭＣＥに必要とされるセキュリテイ方式について考察する．

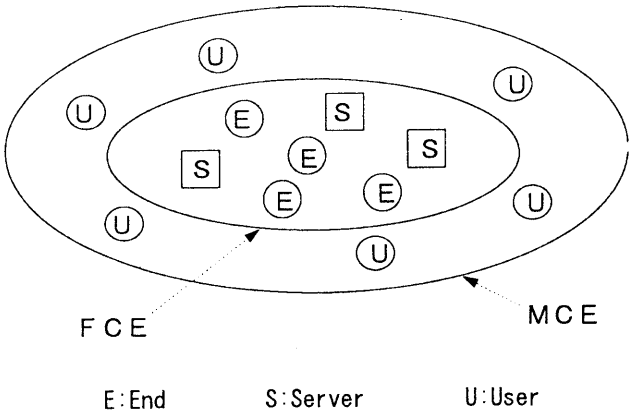

図.１　ＭＣＥモデル

２．利用形態

ＦＣＥ環境での利用形態は、次のように分類される．コンピュータ利用の基本が、サーバへのログインすることにより利用環境が設定されることにあるということでは、Ｅｎｄ（端末）の設置場所へ赴き、Ｅｎｄ（端末）から、登録サーバへ、登録したユーザＩＤとパスワードでログインすることから始まる．登録されていないサーバへはログイン出来ないのが一般的である．登録されていないユーザＩＤでのログインの例として、たとえば、ゲストＩＤとして、ＧＵＥＳＴをユーザＩＤとして利用している場合がある．また、ＦＴＰサーバの例に見られるように、ａｎｏｎｙｍｏｕｓをユーザＩＤと利用している場合がみられる．これらの場合、通常の登録ＩＤでログインする場合と比べ、受けられるサービスの内容に制限が設けられている．

また、登録サーバへ登録ＩＤでログインした場合、その登録サーバを経由して、他のサーバへのログイン（リモートログイン）を可能している場合がある．このリモートログインも、ログイン先の登録ユーザであれば、その登録ＩＤで、また、そうでなければ、ＧＵＥＳＴ・ＩＤなどでログインする（表.１）．

ＭＣＥの場合は、Ｅｎｄ（端末）の設置場所とは無関係に、任意の場所から、サーバへログインする．こ

表.１　ＦＣＥでの利用形態

(1) 登録サーバへ、登録ＩＤでログインする	
非登録サーバへのログインはできない	
所定のサービスが受けられる	
他のサーバへは、当該登録ＩＤで再ログイン（リモートログイン）出来る	
ＧＵＥＳＴで、他のサーバへ再ログインも出来る	
(2) ＧＵＥＳＴで、任意のサーバへログインする	
サービスは限定される	
他のサーバへの再ログイン（リモートログイン）は出来ない	

の場合、効率の観点から、都度遠く離れた場所から登録サーバへログインするのではなく、最寄りのサーバ（非登録サーバ）を経由してログイン出来れば、都合が良い．この場合、単に（登録サーバへの）登録ＩＤだけではなく、登録サーバも指定してログインすることを考える．こうすることにより、ログインされたサーバは、指定された登録サーバへ問い合わせて、登録ＩＤの有効性を確認して、ｏｋであれば、ログイン操作を継続する．登録サーバへの問い合わせでは、登録ＩＤの有効性確認と共に、当該パスワードが返されるようにしておくことも考えられる．登録ＩＤの有効性の確認により、当該ユーザの身元保証が得られたと言うことで、通常のログインの場合と同じように、引き続きパスワード入力をプロンプトして、正しいパスワード入力で、正常ログイン完了とする．

正常にログインされた後は、当該サーバを経由して、登録サーバへのアクセスを行う（中継サービス）．また、身元保証の範囲で、ログイン先のサービズを受ける（上記リモートログインの逆）．更に、登録サーバ経由にすべきところを、当該サーバを経由して、他のサーバへログインして、サービスを受ける（ショートカットログイン）（表.2）．

表.2 ＭＣＥでの利用形態

表.1 ＦＣＥでの利用形態に加えて、

(3) 非登録サーバへ、登録サーバ、登録ＩＤを名乗ってログインする
　登録サーバ、登録ＩＤ保証の範囲で、サービスを受けられる．

(3.1) 非登録サーバを中継して、登録サーバへログインする（中継サービス）

(3.2) 登録サーバ、登録ＩＤを保証として、ログインサーバのサービスを受ける
　(1)のリモートログインの逆

(3.3) 登録サーバ、登録ＩＤを保証として、他のサーバへログインする
　登録サーバからログインすべきところを、ショートカットしてログインする

3．利用者認定

端末からサーバにアクセスする環境では、ユーザが正当なアクセス権限の保持者であることを確認するため、ユーザ・リストがサーバに保持されている．端末からのアクセス毎に、端末で入力されたユーザＩＤ、パスワードが正しいかどうかを、ユーザ・リストと照合して、正しければアクセスを許可し、正しくなければ、アクセスを拒否する．

複数のサーバが通信回線などで互いに接続されたコンピュータ・ネットワークでは、サーバ毎に、当該サーバのユーザ・リストを保持しておく．ユーザは、コンピュータ・ネットワークにアクセスする場合、自分が登録されているサーバに接続する．接続が許可された後、接続先のサーバを経由して、他のサーバへ

表.3 ＭＣＥとＦＣＥの分類

	ＦＣＥ	ＰＨＳ	ＭＣＥ１	ＭＣＥ２	ＭＣＥ３	ＭＣＥ４
End固定 移動	○	○	○	○	○	○
End主導 相手固定	○	○	○	○		
End受動 常時捕捉	○	○			○	
End受動 逐次捕捉						○
End 単一	○				○	
End 複数		○				○

アクセスする.

この方式では、端末（ユーザ）の所在には無関係に、必ず自分が登録されたサーバに繋ぎ込んで（ログイン）、コンピュータ・ネットワークに入らなければならない. 端末の位置が固定されている従来のコンピュータ環境（ＦＣＥ）で、一般的に採られている方式である.

一方、端末（ユーザ）の位置が固定されておらず、絶えず移動して、その位置を変えているモーバイル・コンピュータ環境（ＭＣＥ）では、必ず登録先のサーバを経由しないことには、コンピュータ・ネットワークのサーバの利用者リストを保持することも考えられるが、運用の観点からは、適切な方法とは言いがたい. また、いちいち全てのサーバへ利用者確認の照会をしていたのでは効率が悪い.

あるいは、ユーザＩＤと一緒に、登録サーバを指定したログインの方法も考えられるが、ＦＣＥの場合と同じように、ユーザＩＤだけでのログインを考える.

ここで、ユーザＩＤ（とパスワード）の付与に工夫を凝らすことを考える. ＩＤは、ユーザだけに付与されるものではなく、サーバにもＩＤが付与されている. これらのＩＤは、たとえば、ＩＰアドレスの例に見るように、いずれも同じ体系にあるものとする. サーバＩＤに変換を施して、ユーザＩＤ（とパスワード）を生成する. また、この変換では、互いに異なる複数のユーザＩＤ（とパスワード）も生成出来る. 逆に、いずれのユーザＩＤ（とパスワード）にも逆変換を施せば、一意にサーバＩＤが引き出せる.

こうしたユーザＩＤ（とパスワード）の付与方式では、それぞれのサーバは、ネットワーク接続された、すべてのサーバＩＤ（たとえば、ＩＰアドレス）だけを保持しておくだけで、移動ユーザからのアクセスに対して、常に登録先サーバが特定・確認でき、ユーザの正当性確認に代えることが出来る.

4. ＩＤの表現と生成

ユーザＩＤ、サーバＩＤは、それぞれ、ｎビットの数値で表されるものとし、これを、ｎ次の多項式で、次のように表現する.

$$C(x) = a_{n-1} * x^{(n-1)} + a_{n-2} * x^{(n-2)} + \cdots + a_1 * x + a_0$$

$$a_i = 0 \text{ or } 1 \quad (i = 0, 1, 2, \cdots n-1)$$

ここで、生成多項式 Ｔ（ｘ）を考え、次の操作で、新たなＩＤを生成することを考える.

$$T(x) * C(x) \mod x^n - 1$$

Ｃ（x）にＴ（x）を乗じた結果を、ｘ^ｎ－１で除算した結果の剰余を、新たなＩＤとする. サーバＩＤを、Ｃ０(x) として、次のように、ユーザＩＤ Ｃ１（x）、Ｃ２（x）、Ｃ３（x）、.... を生成する. 除算結果の剰余を新たなＩＤとすることから、次のように、ｋ番目のＣｋ（x）は、元のＣ０（x）に戻る. このｋを、当該Ｃ０（x）で生成されるＩＤ群（グループ）のエントリ数と呼ぶ.

$$C1(x) = T(x) * C0(x) \mod x^n - 1$$
$$C2(x) = T(x) * C1(x) \mod x^n - 1$$
$$C3(x) = T(x) * C2(x) \mod x^n - 1$$
$$C4(x) = T(x) * C3(x) \mod x^n - 1$$

$$Ck(x) = C0(x)$$

ここで、ｎ＝6, Ｔ（x）＝x, Ｃ０（x）＝x^3＋x^2＋１ の場合の例を、以下に示す. この場合、当該ＩＤ

グループのエントリ数は、k＝6となる.

C 0 (x) = x^3 + x^2 + 1 ---------- 001101
C 1 (x) = x^4 + x^3 + x ---------- 011010
C 2 (x) = x^5 + x^4 + x^2 ---------- 110100
C 3 (x) = x^5 + x^3 + 1 ---------- 101001
C 4 (x) = x^4 + x + 1 ---------- 010011
C 5 (x) = x^5 + x^2 + x ---------- 100110
C 6 (x) = x^3 + x^2 + 1 = C 0 (x) ------- 001101

T(x) = x と言うのは、上の例から分かるように、C i(x) のビット列を、サイクリックに左シフトすることに対応している. この例では、たとえば、サーバＩＤを、C 0(x)=００１１０１ に設定した場合、当該サーバのユーザＩＤを、C 1(x)、C 2(x)、C 3(x)、C 4(x)、C 5(x) の中から選択することにより、ユーザＩＤ単独で、サーバＩＤを引き出すことが可能になる.

5. サーバＩＤとユーザＩＤの例

n＝6の場合（表.4）、サーバＩＤ、ユーザＩＤのグループは、6エントリのグループが9グループ、3エントリのグループが2グループ、2エントリのグループが1グループ、それぞれ設定出来ることがわかる. また、n＝7の場合（表.5）は、7エントリのグループが18グループ設定できる.

nが素数の場合は、nエントリのグループが、（2^n - 2）/ n グループ設定出来ることが分かる. 一般的に任意の数nについては、その因数に対応したエントリ数のグループに分かれる. また、ここでは、nビット全てが1のビット列、あるいは、0のビット列は、無意味なので、対象から外して置く.

表.6に、各nに対応した、エントリ数とグループ数の組み合わせをまとめた.

6. おわりに

モーバイルコンピューティング環境の例として、ユーザ主導で、任意の場所、任意の時間に、コンピュータシステムへログインする場合における、ユーザの確認方法の試みとして、ユーザＩＤに工夫を施すことにより、ユーザＩＤのみから登録サーバを割り出すことが出来ることが示された. 引き続き、モーバイルコンピューティング環境モデルを設定して、当該ＩＤ付与方式によるユーザ認証の可能性について考察していきたい.

参考文献

水野、田窪：モーバイルコンピューテイングシステムモデルの提案、情報処理学会研究報告 95-DPS-68,95-GW-9, Vol.95,No.13,平成7年1月

表.6 エントリ/グループのリスト

n	ｴﾝﾄﾘ/ｸﾞﾙｰﾌﾟ	n	ｴﾝﾄﾘ/ｸﾞﾙｰﾌﾟ
6	2/1,3/2,6/9	20	2/1,4/3,5/6,10/99,20/52,377
7	7/18	21	3/2,7/18,21/9,858
8	2/1,4/3,8/30	22	2/1,11/186,22/190,557
9	3/2,9/56	23	23/364722
10	2/1,5/6,10/99	24	2/1,3/2,4/3,6/9,8/30,12/335,24/698,870
11	11/186	25	5/6,25/1,342,176
12	2/1,3/2,4/3,6/9,12/335	26	2/1,13/630,26/2,580,795
13	13/630	27	3/2,9/56,27/4,971,008
14	2/1,7/18,14/1,161	28	2/1,4/3,7/18,14/1.161,28/9,586,395
15	3/2,5/6,15/2,182	29	29/18,512,790
16	2/1,4/3,8/30,16/4,080	30	2/1,3/2,5/6,6/9,10/99,15/2,182,30/35,790,267
17	17/7,710	31	31/69,273,666
18	2/1,3/2,6/9,9/56,18/14,532	32	2/1,4/3,8/30,16/4,080,32/134,215,680
19	19/27,594		

水野、田窪：モーバイルコンピューテイング、２０１０年マルチメディア通信と高速・知能・分散協調コンピューティングシンポジウム　Vol.94,No.7,平成６年９月

W.Wesley Peterson : Error Corecting Codes, John Wiley & Sons, Inc.,1961.

表.４　ｎ＝６の場合のＩＤリスト

000001	000011	000101	000111	001001	001011	001101	001111	010101	010111	011011	011111
000010	000110	001010	001110	010010	010110	011010	011110	101010	101110	110110	111110
000100	001100	010100	011100	100100	101100	110100	111100		011101	101101	111101
001000	011000	101000	111000		011001	101001	111001		111010		111011
010000	110000	010001	110001		110010	010011	110011		110101		110111
100000	100001	100010	100011		100101	100110	100111		101011		101111

表.５　ｎ＝７の場合のＩＤリスト

0000001	0000011	0000101	0000111	0001001	0001011	0001101	0001111	0010011	0010101	0010111
0000010	0000110	0001010	0001110	0010010	0010110	0011010	0011110	0100110	0101010	0101110
0000100	0001100	0010100	0011100	0100100	0101100	0110100	0111100	1001100	1010100	1011100
0001000	0011000	0101000	0111000	1001000	1011000	1101000	1111000	0011001	0101001	0111001
0010000	0110000	1010000	1110000	0010001	0110001	1010001	1110001	0110010	1010010	1110010
0100000	1100000	0100001	1100001	0100010	1100010	0100011	1100011	1100100	0100101	1100101
1000000	1000001	1000010	1000011	1000100	1000101	1000110	1000111	1001001	1001010	1001010

0011011	0011101	0011111	0101011	0101111	0110111	0111111
0110110	0111010	0111110	1010110	1011110	1101110	1111110
1101100	1110100	1111100	0101101	0111101	1011101	1111101
1011001	1101001	1111001	1011010	1111010	0111011	1111011
0110011	1010011	1110011	0110101	1110101	1110110	1110111
1100110	0100111	1100111	1101010	1101011	1101101	1101111
1001101	1001110	1001111	1010101	1010111	1011011	1011111