LM-008

ネットワーク接続UIの認証レベルによるユーザビリティ評価

Usability Evaluation on Authentication Level of Network Connection UI

細田 真道 *1　嶋田 郁子 *1　神田 嘉男 *1　大竹 孝幸 *1*2　池田 敬 *1
Masamichi Hosoda　Ikuko Shimada　Yoshio Kanda　Takayuki Ohtake　Kei Ikeda

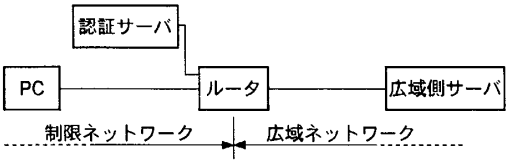

図 1　実験ネットワーク構成

1　はじめに

ホットスポット [1] や情報コンセント [2] 等で，ユーザを識別・認証したい要求や，検疫ネットワーク [3] のように，持ち込み PC をセキュリティチェック後，内部 LAN へ接続したいなどの要求がある．このために，PC をネットワーク（以下，NW と略す）に繋ぐと，一旦接続先が限定された制限 NW に接続され，認証を実施した後に，制限のない広域 NW に接続する技術が用いられる．また，認証時に広域 NW 向けアプリケーション（以下，広域アプリと略す）の設定をダウンロードし，自動設定する技術 [4] が用いられることもある．

一方，ユーザ認証を行うためには，ID, パスワードを入力させる方法，USB キーを用いる方法等があり，認証方法（認証レベル）によってセキュリティレベルが変わる．通常，認証レベルとユーザビリティはトレードオフの関係で，安全性確保のため認証レベルを上げるとユーザビリティが低下し，特に PC 初心者は操作困難になる．

本稿では，認証レベルによるユーザビリティの差を確かめ，初心者が使いやすいシステムを検討する．そのため，初心者に対し，複数の認証レベル環境を用意し，広域 NW が使用可能になるまでの所要時間等を計測する，ユーザビリティ評価実験を実施する．また，初心者が広域 NW 接続後，ウイルス等の不正ソフトウェア被害を受けてしまう可能性についてもあわせて評価する．

2　実験

2.1　環境

実験に用いた NW の概略を図 1 に示す．最初は，PC からルータを越えて広域側サーバへ接続できない．PC へ認証ツール CD-ROM を挿入すると，ツールが起動し，認証完了後，ルータを越え広域側サーバへ接続可能となる．なお，本来は，PC–広域 NW 間の NW 機器によって接続可否を切り替える必要があるが，本実験では，被験者に対して両状態を見せればよいだけなので，認証サーバで認証完了後，認証ツールが PC のデフォルトゲートウェイ設定を変更し，接続可否を切り替える方法をとった．また，今回は広域アプリの一例として電子メールを想定し，接続と同時にメール設定を行うこととした．

		ID 入力	パスワード入力	USB キー
パターン	1	無	無	無
	2	無	無	有
	3	有	無	無
	4	有	無	有
	5	有	有	無
	6	有	有	有
	VII	全設定情報手入力		
	VIII	全設定情報 USB メモリ格納		

表 1　認証レベル

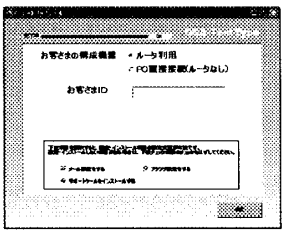

図 2　入力要求画面

図 3　USB キー要求画面

今回用意した認証レベルを表 1 に示す．まず，認証サーバを用いるものとして，ID, パスワード入力有無及び USB キー使用有無の組み合わせにより 6 パターンを用意した．ID 入力は，ユーザが誰か識別するため，パスワードは，ユーザが本物であるか確かめるためのものであり，一般的には ID+ パスワード（パターン 5）が広く用いられている．場合によっては，物理的に本人以外は使用困難な場所にある等，他の方法で本人性担保可能で，特に初心者の操作負担を減らしたい等，ID のみ（パターン 3）を用いることも考えられる．USB キーは，様々な製品があるが，今回はキーを PC に挿すだけのものを想定する．また，比較のため，認証サーバを利用しないパターンとして，電子メールも含めた全設定情報を手入力させるパターン VII, 全設定情報を USB メモリに格納して自動設定を行うパターン VIII の，2 つを別途用意した．

実験用認証ツールは，PC に CD-ROM を挿入すると自動起動し，各認証パターンに従い，ID やパスワードの入力要求画面，もしくは ID のみの入力画面，ID もパスワードも入力させない単なる進行確認画面のいずれかが表示される（図 2）．次に USB キー使用パターンでは，USB キー挿入を求める画面（図 3）が表示される．その後，認証サーバで認証処理が行われ（図 4），認証成功した場合には，広域 NW 接続とアプリ自動設定が行われ，完了画面（図 5）が表示される．

2.2　被験者

被験者は PC 初心者（PC 使用経験有かつ PC 設定経験無）36 名である．被験者の負担を考慮して 1 人につき全 8 パターンの実験は避け，半分の 4 パターンを実施した．また，各パターンは，認証レベルが違うものの，基本的に同様な操作を行うため，ツールに対する慣れの影

*1 東日本電信電話株式会社ネットワーク事業推進本部研究開発センタ，Research and Development Center, Network Business Headquarters, NTT East Corporation
*2 現在，日本電信電話株式会社研究企画部門

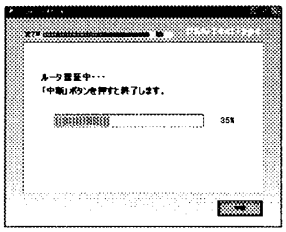

図 4　認証中画面

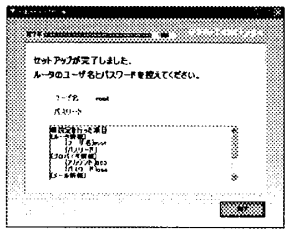

図 5　完了画面

響が考えられる．そこで，最初にツールを使用する 1 回目と，2 回目以降を分離して解析する．1 回目は 36 標本しか取れない．そこで，有意差検定できる標本サイズ確保のため，実施パターン数を 3 つに限定した．実施パターンは，最も一般的な ID とパスワードによるパターン 5, パターン 5 から USB キーによりパスワード入力を省略したパターン 4, そして，厳密な認証が不要な環境を想定した ID のみのパターン 3 とした．2 回目以降は，全パターンの実施回数が 2〜4 回目の合計で同程度になるよう調整するとともに，実施の順番やパターンが偏らないように振り分けた．

2.3　手順

被験者には，複数ツールの使い勝手を比較評価する実験である旨を知らせてから，実験を開始した．実験では，すでにケーブル接続までが完了している PC の他に，各認証レベルに対応した実験用認証ツールが格納された CD-ROM と，各種アカウント情報が印刷された紙，及び USB キーを利用する実験では USB キーが提供され，ツール起動から設定完了画面が出るまでの所要時間を測定した．設定完了後は Web やメールなどの広域アプリを使用して，利用できることを確かめてもらった．なお，マニュアル等は一切配布せず，ツールの使用方法などの質問は受け付けず，実験中に何か疑問や問題が発生しても，被験者個人で試行錯誤を繰り返して作業を完了させるように指示した．

また，不正ソフトウェア被害を受ける可能性を確かめるため，被験者への教示なしで，2 回目の試験中に不正ツール添付メール又は phishing サイトへ誘導するメールを送付し，広域 NW 確認中に添付ファイルを実行する数もしくは phishing 被害が発生する数を測定した．

最後に，実施した 4 パターンについて，1〜4 位の順位と，その理由を記述してもらう主観評価を行った．

3　結果

3.1　所要時間

3.1.1　1 回目

パターン別の所要時間分布及び平均値，標準偏差を図 6，箱ひげ図を図 7 に示す．また，タスク不達成は発生しなかった．図より，いくつか外れ値が発生したが，原因は ID もしくはパスワード入力ミスにより認証失敗が発生して所要時間が多くなったものであった．ID 入力は，ここで比較する全パターンに存在するため，ID 入力ミスが発生する確率は全て等しく，パターン間の比較のためには取り除いても影響がないと考えることができる．パスワード入力ミスは，パターン 5 のみ発生する可能性があり，本来は影響を考慮する必要が残るが，本稿では両入力ミスともに取り除いて比較する．

まず，正規分布とみなせるか Shapiro-Wilk 正規性検定を行った．表 2 に結果を示す．表より，全て $p > 0.05$ であり，正規分布とみなすことにする．次に，等分散とみなせるか Bartlett 検定を行った．結果は $p = 0.5055$ となり $p > 0.05$ なので，等分散とみなすことにする．最後に，等分散を仮定した t 検定を用いて Holm の方法で p 値を調整した対比較を行った．表 3 に結果を示す．表より，太字で示したパターン 3–4 間及びパターン 4–5 間について，有意水準 5% で有意差ありとなった．パターン 3–5 間は，p 値を調整しなくても $p = 0.1110$ となり，有意差なしとなった．

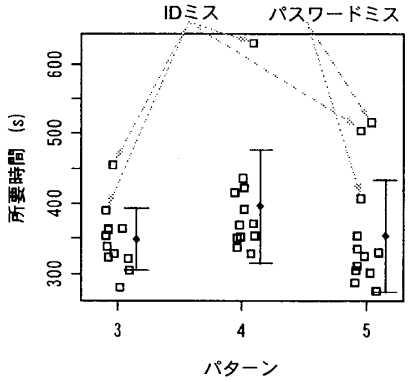

図 6　所要時間（1 回目）

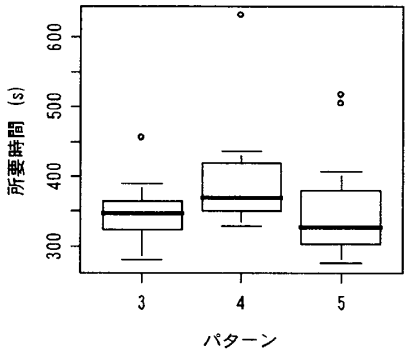

図 7　箱ひげ図（1 回目）

パターン 3	パターン 4	パターン 5
0.3338	0.3891	0.9898

表 2　Shapiro-Wilk 正規性検定の p 値

	パターン 3	パターン 4
パターン 4	**0.00938**	-
パターン 5	0.15505	**0.00038**

表 3　対比較（1 回目）の p 値

3.1.2　2 回目以降

パターン別の所要時間分布及び平均値，標準偏差を図 8，箱ひげ図を図 9 に示す．タスク不達成は，パターン 5 で 13 件中 1 件，パスワード中の英大文字入力ができなかった事象と，パターン VII で 15 件中 4 件，紙に記述されている設定項目と入力欄の対応がわからなかった事象が発生した．図より，外れ値が存在するが，発生原因が一定ではなかったため，ここでは外れ値を含んだ状態で比較する．

外れ値より，明らかに非正規分布であるため t 検定ではなく，Mann-Whitney の U 検定を用いて Holm の方法で p 値を調整した対比較を行った．結果を表 4 に示す．表より，太字で示した組み合わせが有意水準 5% で有意差ありとなった．表より，パターン VIII は他の全パターンより所要時間が有意に短く，次いで，パターン 1 が残

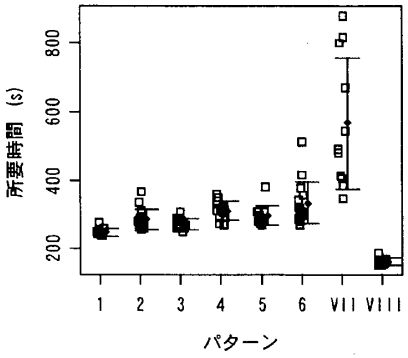

図 8　所要時間（2 回目以降）

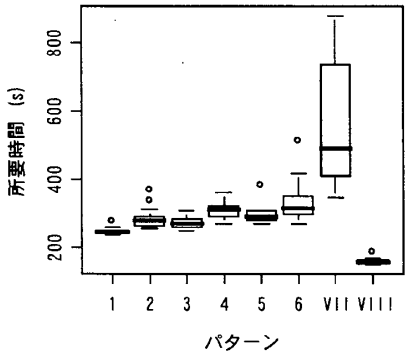

図 9　箱ひげ図（2 回目以降）

る他パターンより短い．パターン 3, 2, 5, 4, 6 は，一部で有意差がある組み合わせもあるが，全体として明確に順位が決められない．パターン VII は他の全パターンより有意に長い．これを所要時間が短い順に並べて，模式的に表すと，VIII < 1 < (3,2,5,4,6) < VII となる．

3.1.3　考察

1 回目の所要時間は，パターン 4（ID と USB キー）が他のパターン 3（ID のみ），5（ID とパスワード）よりも有意に所要時間がかかった．この理由としては，被験者が USB キー利用に手間取ったことが考えられる．一方，パターン 3–5 間では有意差が出ず，平均値，中央値ともに入力項目が多いパターン 5 の方が少なかった．これは，ツール操作のために，何をどこへ入力するか知らない被験者にとって，書類は ID とパスワードの双方が記述されており，画面も ID とパスワードの入力欄があるパターン 5 の方が，対応が取れてわかりやすかったためと思われる．また，初心者であっても，一般的に認証は ID とパスワードで行うものであると理解されており，ID のみで認証を行うパターン 3 に違和感があったことなどが考えられる．

2 回目以降の所要時間では，全体的に 1 回目と比較して所要時間が短くなっている．これは，1 回目では実際の入力操作時間よりも，どういった操作を行えばよいか，逡巡している時間が長かったのに対して，2 回目以降では，ツールに何を入力すべきか知っており，短時間で入力操作に入ることができたということが考えられる．また，これは 1 回目では有意差が出なかった，パターン 3–5 間について，2 回目以降で有意差が出た理由にもつながる．つまり，1 回目は実際の入力時間よりも，ツールの各入力欄に，書類各項目のどれを入力すればよいか，操作を逡巡している時間が長くて，入力項目の多い少ないに結果が影響されなかったのに対して，2 回目以降では，操作を逡巡する時間がなくなり，実際の入力時間が占める割合が多くなったため，入力項目数の違いが結果に影響したものと思われる．また，パターン VII は極端に所要時間を要しており，全設定項目を手入力させることは被験者にとって，大きな負担になっていることが窺われる．逆にパターン VIII は所要時間が短いが，これは認証サーバを利用しないため，設定が短時間ですんでしまうという理由による．

実験中の被験者行動	添付メール	phishing サイト
不正ツール実行	**5**	**3**
メール読まず	5	2
メール読んだが実行せず	6	9
途中で中止	1 （添付保存まで）	5 （サイト閲覧まで）
合計	17	19

表 5　実験における不正ツール実行数

自宅での行動	アンケート結果
ツールを利用	**2**
送付元を確認後，ツールを利用	**11**
ウイルスチェック後，ツールを利用	**2**
条件により利用	7
利用せず	11
合計	33

表 6　自宅での行動アンケート

3.2　不正ソフトウェア被害評価

被験者に対して，製品バージョンアップのお知らせを模した不正ツールを送付した場合に，どの程度の被験者が不正ツールの被害に遭ってしまうかを，不正ツール添付メールの場合と phishing サイト誘導メールの場合で測定した．添付メールの場合は，不正ツールそのものをメールに添付し，不正ツール実行数を測定した．phishing サイトの場合は，バージョンアップサイトを模した phishing サイト URL をメールし，サイトで認証情報を入力させて不正ツールをダウンロードし，実行させるという方法をとり，どこまで実施するか測定した．方法としては，2 回目の実験中に，模擬不正ツール添付メール又は模擬 phishing サイト誘導メールを送付した．添付ファイルの実験は被験者 17 名，phishing サイトの実験は被験者 19 名で実施した．結果を表 5 に示す．実際に不正ツールを実行してしまった被験者は，添付ファイルの場合で 5 名（約 29%），phishing の場合で 3 名（約 16%）となった．

また，被験者は，ツールの使い勝手を評価する実験である旨を知らせており，実際の環境とは不正ツール実行確率が異なる可能性があるため，実験終了後に，自宅で同様のメールが来た場合にはどのような行動をするか，アンケート調査を 33 名の被験者に対して行った．結果を表 6 に示す．表より，無条件にツールを利用するとした被験者は 2 名であったが，送付元確認，ウイルスチェック等をしてから実行するとした被験者が 13 名いた．通常，このような不正ツールは送付元を詐称して送信されるケースが多く，ウイルスチェックで検出できないケースも考えると，15 名（約 45%）もの被験者が不正ツールの被害に遭う可能性があるという結果となった．

3.3　主観評価

4 パターンの実験終了後，実施した 4 パターンについて，1〜4 位の順位と，理由を記述してもらう主観評価

		パターン						
		1	2	3	4	5	6	VII
パターン	2	**0.00066**	-	-	-	-	-	-
	3	**0.00425**	0.54065	-	-	-	-	-
	4	**0.00024**	**0.04538**	**0.00028**	-	-	-	-
	5	**0.00033**	0.39897	**0.01269**	0.34705	-	-	-
	6	**4.3×10^{-5}**	**0.00848**	**7.2×10^{-5}**	0.54065	0.21035	-	-
	VII	**0.00019**	**8.3×10^{-6}**	**4.3×10^{-6}**	**6.2×10^{-5}**	**6.2×10^{-5}**	**0.00046**	-
	VIII	**0.00028**	**9.8×10^{-6}**	**9.8×10^{-6}**	**4.0×10^{-5}**	**6.2×10^{-5}**	**9.8×10^{-6}**	**9.6×10^{-5}**

表 4　対比較（2 回目以降）の p 値

		パターン							
		1	2	3	4	5	6	VII	VIII
パターン	1							3–1	
	2			9–2			4–2	5–2	
	3	6–2							
	4	5–2	8–6	13–6			5–3	7–2	
	5	4–1		12–7	9–5		7–3	8–0	
	6	3–0						5–0	
	VII								
	VIII				3–1	6–3	4–2	3–0	

表 7　順位集計表

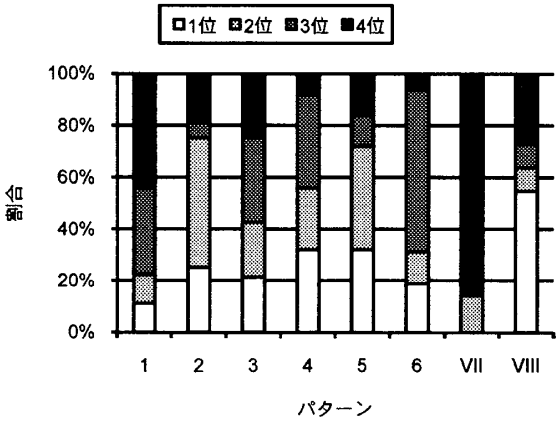

図 10　パターン別順位

を行った．各パターンについて，1〜4 位の割合を図 10 に示す．表より，1 位の割合は，パターン VIII が最も多く，続いてパターン 4 と 5 が同率で並んだ．これを模式的にあらわすと VIII > (4, 5) > 2 > 3 > 6 > 1 > VII となった．2 位までをあわせた割合を同様にあらわすと，2 > 5 > VIII > 4 > 3 > 6 > 1 > VII となった．

次に，同一の被験者が実施した 2 つのパターンについて，どちらのパターンを上位に評価したか集計したものを表 7 に示す．この表で，パターン 1 の行とパターン 3 の列の交点にある項目を見ると，黒地で 2–6 となっており，双方を実施した被験者について，行のパターン 1 を上位に評価した被験者が 2 名，列のパターン 3 を上位に評価した被験者が 6 名であったことを示している．また，各項目は，行のパターンを上位に評価した被験者が多かった場合は白地，下位に評価した被験者が多かった場合には黒地，被験者数が同数又は双方を実施した被験者がいない場合には灰地で示している．表より，他パターンと比較して最も評価が高かったパターンは VIII であり，評価の高さを模式的に表すと，VIII > 5 > 2 > 4 > 3 > 6 > 1 > VII となった．

以上をまとめると，被験者の評価としては，パターン 4, 5, VIII が高く，パターン 1, 6, VII が低いという結果であった．パターン VIII の評価が高かった理由としては，所要時間が短かったことを挙げる被験者が多く，パターン VII の評価が低かった理由としては，入力項目が最も多く，手間と所要時間を要したことが挙げられていた．また，何もしないで接続が完了するパターン 1 の評価が低いが，これは，何もやらないで完了すると「終わったと感じない」「達成感がない」などの理由によるものであった．そして，入力項目の少ないパターン 3（ID のみ）よりも，入力項目の多いパターン 5（ID とパスワード）の方が高い評価であったが，これは，通常の認証では ID とパスワードの双方を入れるものであり，これに慣れているということと，パスワードの存在により安心感が得られるという理由であった．

4　おわりに

本稿では，認証レベルによるユーザビリティの差を確かめ，初心者が使いやすいシステムを検討するため，初心者に対し，複数の認証レベル環境で，広域 NW が使用可能になるまでの所要時間を計測した．その結果，初心者が初めてツールを使用する場合には，ツール操作に逡巡する時間が長く，入力項目数の多い少ないによる入力時間の影響が少ないこと等がわかった．また，初心者が広域 NW 接続後，ウイルス等の不正ソフトウェア被害を受けてしまう可能性についてもあわせて評価したところ，多くの初心者が不正ソフトウェアの被害にあってしまう危険性があることがわかった．最後に，被験者の主観評価では，何もせずに完了するものは，終わった感じがしない，達成感がない等の理由により，評価が低いという結果となった．今後は，本研究で得られた知見を元に，よりよい認証方式を検討して行く予定である．

参考文献

[1] 大江将史，櫨山寛章，山本成一，白畑真，“IEEE802.11 ワイヤレスネットワーク管理システムの構築と検証，”信学論，vol.J87–B，no.10，pp.1607–1615，Oct. 2004.

[2] 後藤英昭，満保雅浩，静谷啓樹，“廉価なスイッチと secure shell を利用した安全な情報コンセントの構成方法，”信学論，vol.J84–D1，no.10，pp.1502–1505，Oct. 2001.

[3] 豊国明子，原田道明，時庭康久，樋口毅，“検疫ネットワークにおけるワーム拡散防止の一手法，”FIT2006，no.M–017，Sept. 2006.

[4] 吉原貴仁，神山健，東弘信，堀内浩規，“サーバ連携による宅内通信機器自動設定方式，”信学論，vol.J88–B，no.3，pp.509–520，March 2005.