情報処理学会論文誌　Vol. 50　No. 9　2257–2273 (Sep. 2009)

ユーザの望むセキュリティと利便性を実現する端末設定決定方式の提案

加藤弘一[†1]　松林大樹[†1]　勅使河原可海[†1]

多様なネットワーク環境において，ユーザの望むセキュリティと利便性を両立させることが重要である．そのため，特にネットワーク上の対策が存在しない環境下では，利用端末の適切な設定が必要となる．しかし，設定項目数は膨大であり，さらに設定項目間に複雑な関係があるため，ユーザ自身で端末を適切に設定することは難しい．本論文では，ユーザの望むセキュリティと利便性を端末上で実現するために，最適な端末設定を決定する方式を提案する．本方式は，フォルトツリー解析によるリスクと利便性の定量化をもとに，ユーザの要望を具体化し，要望を満たす設定組合せの導出とカスタマイズにより設定を決定する．また，適用実験を行い，本方式がユーザの要望を満たす効果的かつ妥当な設定を決定できることを示す．

A Proposal of a Decision Method of Terminal Setting to Satisfy User Requirements for Security and Usability

Koichi Kato,[†1] Hiroki Matsubayashi[†1] and Yoshimi Teshigawara[†1]

In various network environments, it is important to balance the security with the usability that users desire at their terminals. Therefore, a proper terminal configuration is required especially in an environment with no countermeasures. However, setting terminals appropriately is difficult for users because of the large number of parameters to be set and the complex relationships among these parameters. This paper proposes a method of determining optimal terminal settings to achieve a desirable balance between security and usability. The method objectifies users' requirements and decides terminal configurations by selecting and customizing the best combination from calculated setting combinations based on risk and usability quantification with Fault Tree Analysis. Under the experimental deployment, it has been confirmed that this method can decide effective and reasonable configuration that satisfy users' requirements.

1. はじめに

近年，ホームネットワーク，企業や大学など組織のネットワーク，公共空間における高速無線アクセスポイント（公衆無線 LAN）など，ネットワーク利用環境が整備されつつある．それにともない，複数のネットワーク環境を利用するユーザも増加傾向にある．これに対し，どのようなネットワーク環境においても，ユーザが快適に端末やサービスを利用できる十分な利便性と，ユーザや組織が保有する情報資産を保護できる十分なセキュリティを確保し，両立させることが重要となる[1)]．

筆者らはこれまで，運用ネットワーク上の対策を一時的に変更するための，セキュリティと利便性を考慮した対策選定手法を提案してきた[2)]．この手法では，通常は利用できないサービスを特別に利用するために，妨げとなっている対策を一時的に緩和し，かつセキュリティレベルを維持するために他の対策を強化する．これにより，状況に応じて組織とユーザの望むセキュリティと利便性を確保することができる．

しかし，ネットワーク上の対策だけでは，ユーザの望むセキュリティと利便性を確保することは難しい．ホームネットワークや公衆無線 LAN では，セキュリティ機能を有しない接続サービスのみの提供であることが多く，ネットワーク上での対策によるセキュリティは期待できない．そのため，ユーザ端末上でほぼすべてのセキュリティ対策を実施しなければならない．また一方で，セキュリティ機能を提供するネットワークでは，多層防御の概念より，ネットワーク上の対策と端末上の対策を併用することで，より強固なセキュリティを実現することができる[3)]．利便性についても同様に，ネットワーク上の対策を制御しても，端末の設定によっては十分なサービス利用ができない場合がある．そのため，ネットワーク上の対策の制御と合わせて，端末上でもユーザの望むセキュリティと利便性を実現することが重要となる．

ユーザ端末におけるセキュリティ対策として，ウィルス，ワーム，ボットなどへの感染に対し，OS 更新やウィルス対策ソフトの導入などは広く認識され，実施されるようになった[4)]．しかし，端末への不正ログイン，Web 閲覧履歴の解析など，セキュリティやプライバシに関するリスクは，端末の各種設定に大きく関係する．一方，リスクを低減させる設定にした場合，端末やアプリケーションの機能制限・停止につながり，快適な利用を妨げること

†1 創価大学大学院工学研究科
Graduate School of Engineering, Soka University

が多い．

さらに，平成 15 年版情報通信白書によると，セキュリティを重視するユーザが 48.6%，使い勝手（利便性）を重視するユーザが 25.7%，両立を重視するユーザが 13.7%であり，ユーザによってセキュリティと利便性に対する考え方は異なる[5]．ところが，ウィルス対策ソフト導入など比較的大きい概念でも，具体的なセキュリティ対策方法が分からないユーザも多く[4),5)]，複雑かつ膨大な端末設定をユーザ自身で適切に設定することが困難であることは想像に難くない．

これに対し，セキュリティと利便性に関するユーザの要望に応じて適切な端末設定を実現するための研究は，少なくとも我々の知る限り存在しない．また，従来の解決方法として，端末設定を支援する様々なツールが存在するが，これらは設定項目の意味を理解するための支援や，経験則的な推奨設定を促すものである．そのため，その設定により確保されるセキュリティや利便性を客観的根拠に基づいて証明することはできない．さらに，セキュリティと利便性のどちらを優先すべきかが分からないユーザも 11.9%おり[5]，このようなユーザにとっては，端末設定を提示されたとしても適切な設定かどうかを判断することさえ難しい．

そこで本論文では，ユーザの望むセキュリティと利便性を端末上で実現するために，ユーザの要望を満たす最適な端末設定を決定する方式を提案する．まず 2 章で，端末設定の決定における問題点と解決へのアプローチを明確にする．3 章では，リスク，利便性，端末設定の関係性を整理し，リスクと利便性の定量化手法を述べる．また 4 章で，端末設定を決定する方式について述べる．そして，5 章で本方式の適用実験を行い，6 章で評価・考察する．最後に，7 章で今後の課題を述べ，8 章でまとめる．

2. 端末設定の決定における問題点とアプローチ

2.1 ユーザ自身による端末設定の決定の困難さ

(a) セキュリティと利便性に対するユーザの要望が不明瞭

一般的な PC 利用者は，コンピュータやセキュリティの専門家とは限らない．そのため，端末設定がセキュリティや利便性に与える影響をすべて理解しているということは期待し難い．また，設定項目に関連するリスクや利便性をユーザに提示しても，ユーザは自身の望むセキュリティと利便性の程度について，リスク値がある値以下といった絶対評価により決定することは難しい．さらに，極端な場合には，守れるものはすべて守り，かつすべて快適に利用したいと望む可能性がある．しかし，セキュリティと利便性の間でトレードオフの関係が存在する設定項目も多く，現実的な要望として扱うことができない．最適な端末設定を決定するためには，ユーザの望むセキュリティと利便性を，実現可能な範囲において具体化できなければならない．

(b) 妥当性のある端末設定の選択が困難

端末設定の項目数は膨大である．そのため，ユーザの負担や知識不足を考えると，セキュリティと利便性を考慮して，ユーザがすべての設定を決定することは困難である．また，関連するセキュリティや利便性を限定して設定項目を少なくしたとしても，各設定がセキュリティと利便性に与える影響を正確に把握することは難しく，設定の妥当性を証明することは困難である．さらに，ある設定を選択することで新たに出現する設定が存在するなど，設定項目の間には複雑な関係があるため，設定内容により得られるセキュリティや利便性の程度を評価することは難しい．

2.2 アプローチ

2.1 節 (a) に対しては (1) と (3)，2.1 節 (b) に対しては (2) と (3) のアプローチにより，問題の解決を図る．

(1) 相対尺度によるユーザの要望の明確化

ユーザは，具体的な要望を持っていない場合や，自分の要望を理解していない場合がある．しかし，1 章で述べたように，セキュリティと利便性のどちらを重視するかという質問に対しては，回答が得られている．このことから，すべてのセキュリティと利便性を良い状態にしたいなど，矛盾を含む場合があるとしても，ユーザは潜在的に何らかの要望を持っているといえる．

このような心理的な要素は，3 段階や 5 段階のアンケート形式などで抽出されることが多い．そこで，段階的な相対尺度を用いて，どの程度のセキュリティや利便性を実現したいかという相対的な重要度として，ユーザの要望の抽出を試みる．

なお，セキュリティと利便性のどちらを優先すべきかが分からないユーザも存在する．しかし，「他人に PC を勝手に使用される可能性」など，自分の利用端末上で実際に起こりうる具体的なリスクや利便性が提示されれば，リスクの危険性や利便性の重要さを実感し，重要度を決定することが可能であると考えられる．

(2) 定量評価に基づく設定組合せの導出

設定の組合せ数は膨大であるため，まずはユーザの要望を満たす設定組合せに絞り込む必要がある．そこで，設定組合せに対するリスクと利便性をフォルトツリー解析（FTA: Fault Tree Analysis）により定量化する[6]．そして，(1) で決定されるユーザの要望と，リスクや

利便性の値を対応づけ，ユーザの要望を達成可能な設定組合せを導出する．

ここで，フォルトツリー（FT: Fault Tree）は AND と OR の論理ゲートを中心とした単純な構造で原因と結果を表現でき，複合的な事象も評価することが可能である．そのため，リスクや利便性に影響を与える設定項目，および設定項目間の複雑な関係が表現できることから，本論文では FTA を用いている．なお，本論文ではリスクの評価基準を事故発生確率（リスクが顕在化する確率）とし，利便性の評価基準は，設定による影響がない状態を基準値 1 とした割合として定義する．

(3)　フィードバックを利用した妥当な設定の決定

(2) により導出された設定組合せは，定量評価に基づき，ユーザの望むセキュリティと利便性を満たすものである．そこで，ユーザは導出された複数の設定組合せの中から適当なものを選択し，これをカスタマイズすることで，ユーザにとって最適な設定を決定する．このとき，カスタマイズにともない変化するリスクと利便性の程度をユーザに提示することで，ユーザ自身が納得のいく妥当な設定を決定する．

また，非常に強いセキュリティと非常に高い利便性を両立させたいなど，実現できない要望の場合には，(2) において該当する設定組合せを導出することができない．これは，要望が矛盾していること，実現できないことをユーザ自身が理解することにもつながり，(1) での要望の再定義と (2) での設定組合せの再導出を繰り返すことで，現実的かつユーザにとって妥当な設定を決定する．

3.　リスク，利便性，端末設定の分析，定量化およびレベル分け

2.2 節のアプローチのために，まず，リスク，利便性，端末設定の関係性を整理する．そして，リスクと利便性を定量化し，これらの値と 2.2 節 (1) で述べた相対尺度を対応づける．

3.1　リスクと利便性の分析

ログイン時の認証，Web 利用など，端末利用時に頻繁に出現する事項として，リスクを 16 個，利便性を 17 個とりあげ，FTA による分析を行った．本論文では，これらの中から例をあげて説明する．

(1)　リスクの分析

本研究におけるリスクの FT では，まず，ユーザにとって起きることが望まれない事象を対象リスクとして頂上事象におく．そして，リスクが顕在化するまでには事象の流れが存在するため，この流れに基づいて FT を展開する．さらに各事象が起きる原因について，端末が人間により受ける動作（人間が端末に対して実行する操作）や，端末が機械的に実行する動作となるまで展開し，これを基本事象とする．

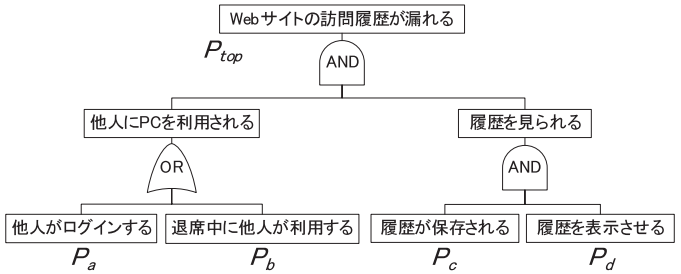

図 1　Web サイトの訪問履歴が漏れるリスクの FT
Fig. 1　Fault tree for leaking of web browsing history.

たとえば**図 1** では，まず，ユーザが望まない「Web サイトの訪問履歴が漏れる」事象を頂上事象におく．次に，この事象が起きるまでには，他人に PC を利用され，履歴を他人に見られる，という流れが存在するため，この流れに沿って FT を展開する．そして，「他人に PC を利用される」事象は，他人がログインするか，または退席中に他人が利用することが原因であるとして FT を展開し，これらは人間が端末に対して実行する操作であるので基本事象となる．一方，「履歴を見られる」事象について，何らかの理由によって履歴が表示されることで初めて履歴を見ることができるため，端末に対する操作ではなく，基本事象とはならない．そこで，この事象について分析し，端末内に履歴が保存され，さらに保存した履歴が表示されることが原因であるとして FT を展開する．履歴の保存は端末が機械的に実行する動作であり，履歴は人間の操作によって表示させられる，つまり人間が端末に対して実行する動作であるため，両者ともに基本事象となる．

また，基本事象の発生確率は，図 1 の P_a，P_b，P_d のように人間の行動に関係する場合にはその成功確率を，P_c のように端末動作に関係する場合にはその動作が確実に実行されるかどうかの度合いを示すものである．ここで，P_c について，履歴を残す日数などによって，履歴が確実に残っている期間は変化する．そのため，端末動作に関する基本事象の場合には，その動作による効力の大きさや有効期間を考慮した値となる．なお，これらの値の決定方法については 3.3 節で述べる．

(2)　利便性の分析

利便性の FT では，まずユーザが利用したい機能やサービスを頂上事象におく．次に，その機能やサービスを利用するために満たすべき端末の状態や，人間が行わなければならない

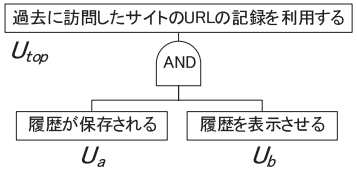

図 2　Web サイトの訪問履歴の利用に関する FT
Fig. 2　Fault tree for the use of web browsing history.

行動を展開する．ただし，各機能・サービスの利便性をユーザがとらえやすいよう，ログインに関する利便性以外は，端末を利用している状態を前提として分析する．そして，リスクの FT と同様に，端末が人間により受ける動作（人間が端末に対して実行する操作）や，端末が機械的に実行する動作となるまで展開し，基本事象とする．

たとえば**図 2** では，まず利用機能として「過去に訪問したサイトの URL の記録を利用する」という事象を頂上事象におく．次に，この機能を利用するためには，端末の状態として，端末内に履歴が保存されている必要がある．さらに，履歴を利用するためには，保存されている履歴を表示することが必要である．そこで，これらの事象を展開し，履歴の保存は端末が機械的に実行する動作であり，履歴の表示は人間により実行される操作であるため，基本事象となる．

また，基本事象の利便性の値は，端末動作に関係する場合には，その動作が確実に実行されるかどうかの度合いを示すものである．この値は，本節 (1) と同様に，その動作による効力の大きさや有効期間を考慮したものとなる．一方，人間の行動に関係する場合には，2.2 節 (2) の定義より，問題なく実行できる状態を基準値 1 とした割合が，基本事象の利便性の値となる．

3.2　リスク，利便性，端末設定の関係性

(1)　リスクと端末設定の関係

リスクの FT において，基本事象の発生確率は端末設定によって変化する．そこで，16 個のリスクに関する 49 個の設定項目を分析した．この分析の範囲において，リスクの FT の基本事象に対する端末設定の関係は，次の 4 つのタイプに分類することができた．

（タイプ A）　関連する複数の設定項目のうち，1 つの設定項目で対策をとれば基本事象の発生確率を抑制できる．

（タイプ B）　関連する複数の設定項目のうち，すべての設定項目で対策しなければ基本事象の発生確率を抑制できない．

（タイプ C）　ユーザが手動で行う対策と端末で自動的に実行される対策が混在している．手動で対策しない場合，自動で実行される対策のみが基本事象の発生確率を抑制する．一方，手動で積極的に対策する場合，手動と自動の対策のうちの強力な方によって，基本事象の発生確率が抑制される．

（タイプ D）　関連する複数の設定項目のそれぞれで対策をとるごとに基本事象の発生確率が抑制されていく．

これら 4 つのタイプを考慮して，リスクの FT を拡張する．まず，基本事象の発生確率に影響する設定項目を，基本事象の下位に展開する．このとき，複数の設定項目が関係する場合には，前述の 4 つのタイプのいずれであるかを明記してから展開する．また，ある選択肢を選択することによって新たに影響を考慮しなければならなくなる設定項目，または新たに出現する設定項目は，その選択肢の下位に展開する．なお，基本事象に関係する端末設定の洗い出しと関係性の整理は，Microsoft のマニュアルやリソースキットを参考にした[7)–10)]．

この手順により図 1 を拡張し，端末設定の関係性を明確にしたリスクの FT を**図 3** に示す．ここで，「手動」と記述されている設定項目は，ユーザの行動により効果を発揮する設定項目であり，この記述のない設定項目はすべて自動的に効果を発揮する設定項目である．また，表記については，本来の FT をベースに，設定のいずれかを選択する部分は便宜上 OR の論理記号を用いて表現し，各設定項目における選択肢は破線で明示している．なお，設定項目の選択肢に割り当てられる値については，3.3 節で述べる．

(2)　利便性と端末設定の関係

利便性の FT において，基本事象の利便性の大きさは端末設定により変化する．そこで，17 個の利便性に関する 50 個の設定を分析した．この分析の範囲において，利便性の FT の基本事象に対する端末設定の関係は，次のように (1) のタイプ D に相当するものだけであった．

（タイプ D）　関連する複数の設定項目のそれぞれで機能が制限されるたびに，基本事象の利便性が低下する．

この関係を考慮して利便性の FT を拡張する．まず，端末が実行すべき基本事象の動作に対して，関係のある設定項目を基本事象の下位に展開する．このとき，複数の設定項目が関係する場合には，タイプ D であることを明記してから展開する．また，ある選択肢を選択することによって新たに影響を考慮しなければならなくなる設定項目，または新たに出現する設定項目は，その選択肢の下位に展開する．なお，リスクと同様に，基本事象に関係する端末設定の洗い出しと関係性の整理は，文献 7)–10) を参考にした．

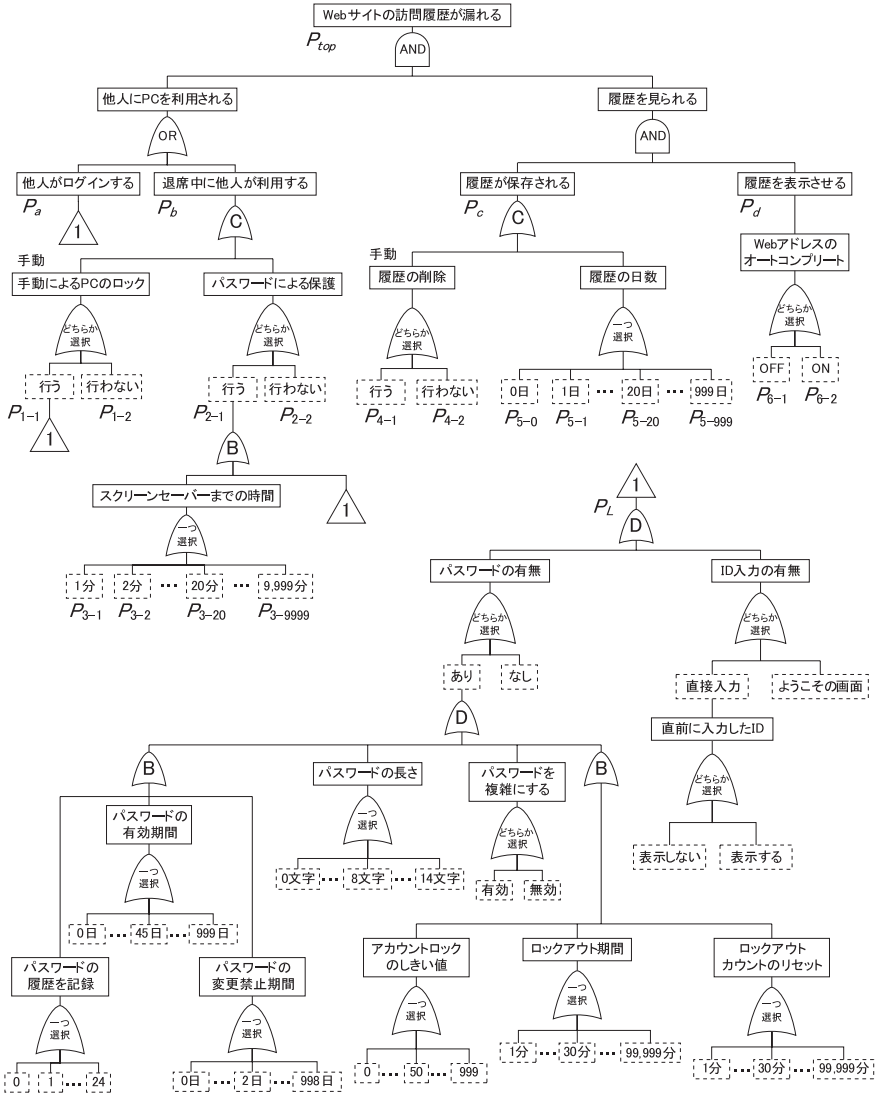

図 3　リスクと端末設定の関係
Fig. 3　Relations between risks and terminal settings.

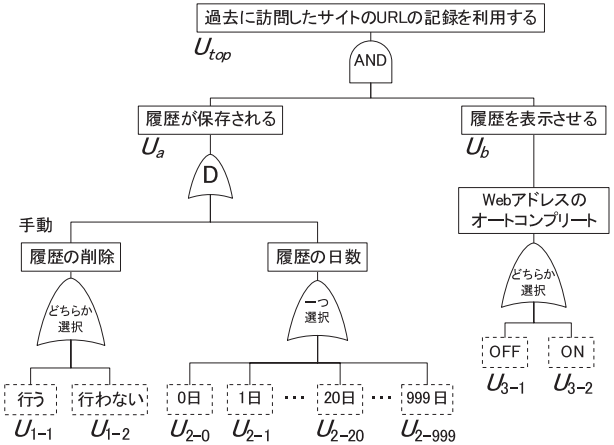

図 4　利便性と端末設定の関係
Fig. 4　Relations between usability and terminal settings.

この手順により図 2 を拡張し，端末設定の関係性を明確にした利便性の FT を**図 4** に示す．まず，履歴が保存されるという端末動作に対して，手動で削除することで履歴が消失する．また，履歴の保存日数が短くなるほど，残る履歴は少なくなる．つまり，それぞれで履歴の保存が制限されるたびに，利用に必要となりうる履歴が減少するため，タイプ D として展開されている．一方，履歴を表示させるためには，Web アドレスのオートコンプリートの機能が ON である必要があるため，この設定項目が展開されている．

ここで，「履歴が保存される」という基本事象に関係する設定項目について，図 3 ではタイプ C，図 4 ではタイプ D で展開されている．リスクについては，他人に履歴を見られること自体が問題であるととらえて，見られる可能性のある履歴がどの程度残るかという観点で分析した．そのため，削除または保存日数のうちの効果の大きい方を反映するために，タイプ C として分析した．

一方，利便性については，頂上事象の機能を利用するのは端末を利用するユーザであるため，利用する必要のない履歴が残っていても効果はほとんどなく，利用したい履歴がどの程度残るかという観点で分析している．そのため，必要な履歴がないときには履歴を削除しても影響はほとんどなく，一方で必要な履歴が生じなければ保存日数が長くても効果は小さい．つまり，利便性への影響の大きさを単純に比較することができない．そこで，それぞれ

の設定項目によって制限されるごとに，必要になる可能性のある履歴が減少するととらえ，タイプ D として分析した．

3.3　事故発生確率と利便性の定量化

(1)　事故発生確率の算出

図 1 のような FT の頂上事象の発生確率は最小カットセットをもとに求められる．最小カットセット c，最小カットセットの集合 C，ひとつの最小カットセットに含まれる基本事象 e とその集合 E_c，基本事象の発生確率 P_e とすると，頂上事象の発生確率 P_{top} は式 (1) で表される．

$$P_{top} = 1 - \prod_{c \in C} \left(1 - \prod_{e \in E_c} P_e \right) \tag{1}$$

たとえば，図 1 では最小カットセットは acd，bcd であり，式 (1) から下記のように展開される．

$$\begin{aligned} P_{top} &= 1 - (1 - P_a P_c P_d)(1 - P_b P_c P_d) \\ &= P_a P_c P_d + P_b P_c P_d - P_a P_b P_c^2 P_d^2 \end{aligned}$$

ただし，同じ事象が 2 回同時に起きるということは現象として意味をなさず，正しい確率を計算できないため，同じ変数の累乗計算をしてはならない．そのため，次式のように修正しなければならない．

$$P_{top} = P_a P_c P_d + P_b P_c P_d - P_a P_b P_c P_d$$

このように，式 (1) における P_e の乗算は，通常の乗算ではなく，べき等律などの性質を持つ，固有の計算となる．そのため，複数のカットセットに共通の基本事象が含まれる場合には，計算に注意が必要である[6]．

さらに，基本事象の発生確率 P_e は，端末設定により変化する．そこで，まず末端に位置するすべての設定項目の選択肢に対して，その設定が原因で基本事象が起きる確率を割り当てる．

そして，端末設定の関係性を考慮して基本事象の発生確率を決定するために，3.2 節 (1) で述べた 4 タイプに対して，基本事象の発生確率を算出するルールを定める．

（タイプ A の場合）　選択された設定の中で最小の確率を発生確率とする．

（タイプ B の場合）　選択された設定の中で最大の確率を発生確率とする．

（タイプ C の場合）　手動で対策を行う場合，選択された設定の中で最小の確率を発生確率とする．一方，手動で対策を行わない場合，自動で実行される対策の確率をそのまま発生確率とする．

（タイプ D の場合）　選択された設定の確率の積を発生確率とする．

表 1　端末設定と確率
Table 1　Terminal settings and probability.

	確率	設定
$P_{1\text{-}1}$	—	
$P_{1\text{-}2}$	0.9	○
$P_{2\text{-}1}$	—	○
$P_{2\text{-}2}$	1.0	
$P_{3\text{-}1}$	0.1	
$P_{3\text{-}2}$	0.1	
$P_{3\text{-}20}$	0.9	○
$P_{3\text{-}9999}$	0.9	
P_L	0.3 (※)	—

	確率	設定
$P_{4\text{-}1}$	0.1	○
$P_{4\text{-}2}$	1.0	
$P_{5\text{-}0}$	0.1	
$P_{5\text{-}1}$	0.1	
$P_{5\text{-}20}$	0.5	○
$P_{5\text{-}999}$	1.0	
$P_{6\text{-}1}$	0.1	
$P_{6\text{-}2}$	1.0	○

※便宜上の値．設定に対して割り当てた値ではない．

このルールに基づいてすべての基本事象の値を決定する．そして，式 (1) を用いて頂上事象の発生確率を求める．

たとえば，図 3 において，設定項目の各選択肢に割り当てられた確率と，選択された設定が，**表 1** のような場合を考える．ただし，ここでは説明を簡単にするため，図 3 の移行記号 1 の下位に展開されている部分から算出された値を，$P_L = 0.3$ と仮定する．

表 1 の設定のときの P_{top} を求める．まず P_a は，P_L がそのまま反映され，$P_a = 0.3$ となる．P_b は，手動の対策である「手動による PC のロック」を「行わない」設定で，自動的な対策である「パスワードの保護」を「行う」設定であるため，タイプ C のルールから，さらに下位の設定に従う．そのため，$P_{3\text{-}20}$，P_L が関係し，タイプ B のルールから $P_b = 0.9$ となる．P_c は，$P_{4\text{-}1}$，$P_{5\text{-}20}$ が関係し，タイプ C のルールから，$P_c = 0.1$ となる．P_d は，$P_{6\text{-}2}$ がそのまま反映され，$P_d = 1.0$ となる．これらの確率をもとに，前述したように累乗の計算に注意して，式 (1) から $P_{top} = 0.093$ となる．

(2)　利便性の算出

利便性についても同様に，図 2 のような利便性の FT において，基本事象 e の利便性 U_e とすると，頂上事象の利便性 U_{top} は式 (2) で表される．ただし，事故発生確率と同様に，べき等律などの性質に従った計算に注意する．

表 2　端末設定と利便性の値
Table 2　Terminal settings and the value of usability.

	利便性	設定
$U_{1\text{-}1}$	0.1	○
$U_{1\text{-}2}$	1.0	
$U_{2\text{-}0}$	0.1	
$U_{2\text{-}1}$	0.3	

	利便性	設定
$U_{2\text{-}20}$	0.5	○
$U_{2\text{-}999}$	1.0	
$U_{3\text{-}1}$	0.1	
$U_{3\text{-}2}$	1.0	○

$$U_{top} = 1 - \prod_{c \in C} \left(1 - \prod_{e \in E_c} U_e \right) \tag{2}$$

さらに，式 (2) における基本事象の利便性 U_e は，端末設定により変化する．そこで，リスクと同様に，末端に位置するすべての設定項目の選択肢に対して，その設定により得られる基本事象の利便性の値を割り当てる．

そして，3.2 節 (2) より，今回の分析の範囲において，端末設定と利便性の関係はタイプ D だけであったので，基本事象の利便性を算出するルールを次のように定める．

（タイプ D の場合） 選択された設定に与えられた値の積を利便性とする．

たとえば，図 4 に対して**表 2** のように値が割り当てられた場合における，利便性 U_{top} を求める．U_a は $U_{1\text{-}1}$ および $U_{2\text{-}20}$ が関係し，これらはタイプ D であるため，$U_a = 0.05$ となる．また，U_b は $U_{3\text{-}2}$ がそのまま反映され，$U_b = 1.0$ となる．これらの値を式 (2) に代入し，$U_{top} = 0.05$ となる．

3.4　リスクと利便性のレベル分け

ユーザの望むセキュリティや利便性を実現可能な設定組合せを決定するためには，ユーザの要望を具体化し，ユーザの要望と設定組合せを対応づける必要がある．しかし，ユーザが自身の望む事故発生確率や利便性の値を決定することは難しいため，リスクや利便性を相対的に比較しながら簡単に要望を選択できる仕組みでなければならない．そこで，アンケートなどでよく用いられているリッカート尺度を参考に，各リスクと利便性のレベルを「高」，「高–中」，「中」，「中–低」，「低」の 5 段階で選択する方法を取り入れる．

各レベルと設定組合せを対応づける方法として，事故発生確率や利便性の値でソートして組合せ数で 5 等分するレベル分け方法や，事故発生確率や利便性の値をある閾値で区切るレベル分け方法がある．前者は，レベル分けは容易だが，全組合せにおける相対的なレベルとなるため，レベルの効果や意味をとらえにくい．後者は，事故発生確率や利便性の大きさから意味的にレベルを扱えるが，閾値の設定が難しい．以後，前者を順位によるレベル分け，後者を値によるレベル分けと呼ぶこととする．

4.　端末設定決定方式

4.1　要望を満たす設定組合せの導出

3.4 節で述べた 5 段階のレベルに基づき，ユーザはリスクや利便性に対して自身の望むレベルを選択する．そして，すべてのリスクと利便性がユーザの要望するレベルを満たすような設定組合せを導出する．

この実現のため，導出すべき設定組合せを定式化する．まず，設定項目を s_i，設定項目の集合を S，設定項目の総数を m と定義する，つまり，これらの関係は

$$s_i \in S \quad (i = 1, 2, \ldots, m)$$

で表される．

次に，設定項目の選択肢 j を選択するかどうかを表す変数を $x_j \in \{0, 1\}$，s_i における選択肢の総数を n_i，s_i においていずれの選択肢を選択するかを表す変数ベクトルを $\mathbf{x}_i$ とする．このとき，すべての設定項目の選択肢を含む変数ベクトル $\mathbf{x}$ を次のように定義する．

$$\mathbf{x} = (x_1, \ldots, x_{n_1}, x_{n_1+1}, \ldots, x_{n_1+n_2}, \ldots, x_{N_{m-1}+1}, \ldots, x_{N_{m-1}+n_m})$$

ただし，

$$\mathbf{x}_1 = (x_1, x_2, \ldots, x_{n_1})$$
$$\mathbf{x}_i = (x_{N_{i-1}+1}, x_{N_{i-1}+2}, \ldots, x_{N_{i-1}+n_i}) \quad (2 \le i \le m)$$
$$N_i = \sum_{t=1}^{i} n_t \quad (1 \le i \le m)$$

である．つまり，ベクトル $\mathbf{x}$ の要素は，次元数の異なる複数のベクトル $\mathbf{x}_i$ の要素を並べたものである．

さらに，リスクを r_p，リスクの集合を R，利便性を u_q，利便性の集合を U とする．これより，リスクの総数を k，利便性の総数を l とすると，

$$r_p \in R \quad (p = 1, 2, \ldots, k)$$
$$u_q \in U \quad (q = 1, 2, \ldots, l)$$

である．そして，r_p と u_q に対してユーザが望むレベルをそれぞれ $L^{req}_{r_p}$，$L^{req}_{u_q}$，選択された設定組合せ $\mathbf{x}$ における r_p と u_q のレベルをそれぞれ $L_{r_p}(\mathbf{x})$，$L_{u_q}(\mathbf{x})$ とする．

これらをもとに，ユーザ望むリスクと利便性のレベルを満たす設定組合せの集合を X と

すると，X は次式で表される．ただし，C_0，C_1 は，ユーザ自身の要望やネットワーク規定による，選択不可，選択必須な設定選択肢の集合である．また，設定項目ごとに設定が択一で選択されるため，$\mathbf{x}_i$ の大きさは 1 でなければならない．

$$
\begin{aligned}
X = \{\mathbf{x} \mid\ & L_{r_p}(\mathbf{x}) \le L_{r_p}^{req} \quad (r_p \in R), \\
& L_{u_q}(\mathbf{x}) \ge L_{u_q}^{req} \quad (u_q \in U), \\
& x_j = \begin{cases} 0 & (j \in C_0) \\ 1 & (j \in C_1) \end{cases}, \\
& |\mathbf{x}_i| = 1 \quad (s_i \in S) \\
\}&
\end{aligned}
\tag{3}
$$

この集合 X を求めることで，ユーザの望むセキュリティと利便性を満たす設定組合せを導出することができる．

4.2　フィードバックを利用した端末設定の決定

4.1 節で導出された複数の設定組合せの中から，ユーザは自身が適当だと思う設定組合せを選択する．また，必要に応じて設定を変更するなどのカスタマイズを行う．このとき，設定変更により各リスクや利便性が変化するため，変更前と変更後の各レベルをユーザに提示し，変化を把握しながら調整する．一方，適切な設定を決定できない場合には，再度 4.1 節でのレベル調整や導出を行う．これにより，ユーザが納得のいく端末設定を決定する．

5. 本方式の適用実験

すべての設定をユーザが手動で決定する方法（以下，手動方式）と本方式の比較を通して，本方式が 2.1 節の問題点を解決しているかどうかを評価する．この評価のため，両方式によるユーザの望むセキュリティと利便性の達成度合いと，設定の決定にかかる時間を実験により確認する．なお，本方式においては，3.4 節で述べた 2 つのレベル分け方法でそれぞれ実験を行い，レベル分け方法の違いによるユーザの要望達成の差異の検証も行う．

実験の被験者は，本研究室の学生 16 名である．なお，被験者は全員，PC を日常的に使用しており，リスクや利便性を説明した際に，十分に理解できる知識を持っている．ただし，全ユーザともに実験前は設定項目のほとんどについて意味や効果を理解していなかった．

5.1　想 定 環 境

端末利用環境として，ホームネットワークや公衆無線 LAN において自身の PC を利用する場合のような，端末の設定変更に関する制約がない環境を想定する．また，利用端末の OS は Windows XP Professional，利用 Web ブラウザは Internet Explorer 7 とする．

本実験で扱うリスクと利便性は次のとおりである．

【リスク】
(R1)　他人にログインされる
(R2)　退席時にログインされる
(R3)　Web サイトの訪問履歴が漏れる
(R4)　OS の最近使ったファイルの履歴が漏れる

【利便性】
(U1)　ログインの利便性
(U2)　退席時の PC のロックにおける利便性
(U3)　過去の訪問サイトの URL の記録を利用する
(U4)　OS の最近使ったファイルの履歴を利用する

5.2　準　　備

(1)　リスクと利便性の FT 作成と定量化

まず，想定するリスクと利便性に関する FT を作成する．そして，Microsoft のマニュアルやリソースキット[7)–10)] を参考に，設定の各選択肢に対して，3.3 節のように基本事象へ反映される確率や利便性を割り当てる．そして，すべての設定組合せについて事故発生確率と利便性の値を算出する．ただし，設定組合せ数が膨大となるリスクや利便性については，現実的に存在しえない組合せを排除し，組合せを限定した．

(2)　リスクと利便性のレベル分け

(1) で算出した値をもとに，3.4 節で述べた両方法においてレベル分けを行う．たとえば，リスク R1 と利便性 U1 について，各設定組合せの事故発生確率や利便性の値を昇順にソートすると，それぞれ**図 5**，**図 6** のようになる．

順位によるレベル分け方法は，たとえば図 5，図 6 では組合せ数が 50 個であるので，順位ごとに 10 個ずつで区切ってグループ化する．一方，値によるレベル分け方法は，図 5 や図 6 の特性を考慮してそれぞれ閾値を設定し，グループ化する．両レベル分け方法における，リスクと利便性のレベルとの対応関係をそれぞれ**表 3**，**表 4** に示す．なお，レベルに対応させる順位は組合せ総数により変化する．また，順位によるレベル分けの場合における，各レベルに対応した事故発生確率と利便性は**表 5** のようになる．

(3)　ツールの開発

本実験のため，次の機能を持つツールを開発した．

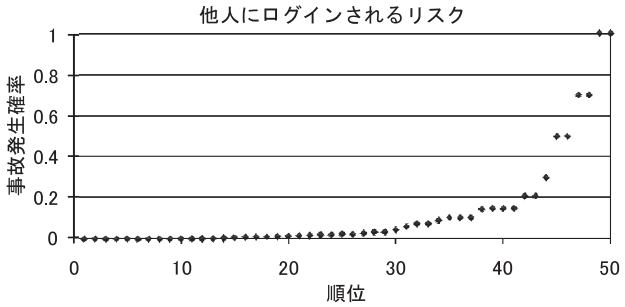

図 5　各設定組合せにおける事故発生確率
Fig. 5　Risk probability versus each setting combination.

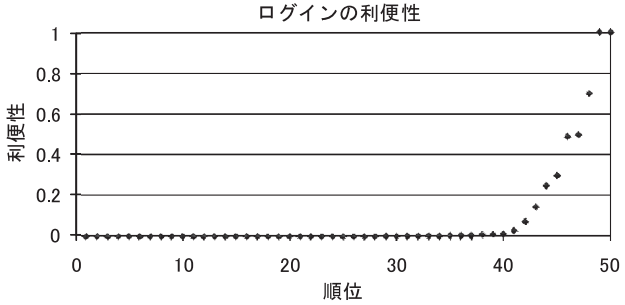

図 6　各設定組合せにおける利便性
Fig. 6　Usability versus each setting combination.

- 各リスクと利便性に対してユーザの望むレベルを選択できる機能
- ユーザの望むレベルと設定の制限（選択必須または選択不可）を満たす設定組合せを導出する機能
- 導出した設定組合せが複数ある場合に，適当と思う設定組合せをユーザが選択できる機能
- 選択した設定組合せをもとに，レベルの変化を表示しながら設定を個別に変更できる機能

表 3　リスクのレベル分け
Table 3　Classifying risk levels.

レベル	順位	値
高	41－50	0.8 以上 1.0 以下
高－中	31－40	0.6 以上 0.8 未満
中	21－30	0.4 以上 0.6 未満
中－低	11－20	0.2 以上 0.4 未満
低	1－10	0 以上 0.2 未満

表 4　利便性のレベル分け
Table 4　Classifying usability levels.

レベル	順位	値
高	41－50	0.4 以上 1.0 以下
高－中	31－40	0.2 以上 0.4 未満
中	21－30	0.1 以上 0.2 未満
中－低	11－20	0.05 以上 0.1 未満
低	1－10	0 以上 0.05 未満

5.3　実験 1：順位によるレベル分けの場合

(1)　実験手順

事前に，5.1 節で示したリスクと利便性の意味についてユーザに説明する．その後，ユーザは自身の望むリスクと利便性のレベルを「高」，「高–中」，「中」，「中–低」，「低」，「希望なし」の中から選択する．

そして，設定に関する知識の有無による影響を比較するために，端末設定に関する説明前と説明後において，それぞれの方式で実験を行う．各方式における実験の手順は，次のとおりである．

（手動方式により設定を決定する手順）

（手順 1）　ユーザに対し，5.1 節のリスクと利便性に関係する 22 個の設定項目とその選択肢を，**図 7** のようにリスクや利便性ごとに分けず一律に提示する．

（手順 2）　ユーザは，事前に決定した自身の望むリスクと利便性のレベルを考慮して，提示された各設定項目の選択肢から適切と思うものを選択する．

（本方式により設定を決定する手順）

（手順 1）　ユーザは，事前に決定した自身の望むリスクと利便性のレベルをツールに入力

表 5　順位によるレベル分けにおける事故発生確率と利便性
Table 5　Risk probability and usability of each level in classification by rank.

R1	高	0.15 以上	1 以下
	高－中	0.063 以上	0.15 未満
	中	0.0174 以上	0.063 未満
	中－低	0.003 以上	0.0174 未満
	低	0 以上	0.003 未満
R2	高	0.9 以上	1 以下
	高－中	0.5 以上	0.9 未満
	中	0.1 以上	0.5 未満
	中－低	0.0175 以上	0.1 未満
	低	0 以上	0.0175 未満
R3	高	0.09 以上	1 以下
	高－中	0.0199 以上	0.09 未満
	中	0.0075 以上	0.0199 未満
	中－低	1.22E-03 以上	0.0075 未満
	低	0 以上	1.22E-03 未満
R4	高	0.508 以上	1 以下
	高－中	0.1 以上	0.508 未満
	中	0.0484 以上	0.1 未満
	中－低	6.28E-03 以上	0.0484 未満
	低	0 以上	6.28E-03 未満

U1	高	0.03 以上	1 以下
	高－中	3.38E-03 以上	0.03 未満
	中	2.21E-04 以上	3.38E-03 未満
	中－低	2.45E-05 以上	2.21E-04 未満
	低	0 以上	2.45E-05 未満
U2	高	0.1323 以上	1 以下
	高－中	1.01E-03 以上	0.1323 未満
	中	2.19E-05 以上	1.01E-03 未満
	中－低	1.27E-07 以上	2.19E-05 未満
	低	0 以上	1.27E-07 未満
U3	高	0.1 以上	1 以下
	高－中	0.05 以上	0.1 未満
	中	0.011 以上	0.05 未満
	中－低	0.005 以上	0.011 未満
	低	0 以上	0.005 未満
U4	高	0.001 以上	1 以下
	高－中	0.0003 以上	0.001 未満
	中	5.00E-05 以上	0.0003 未満
	中－低	5.00E-06 以上	5.00E-05 未満
	低	0 以上	5.00E-06 未満

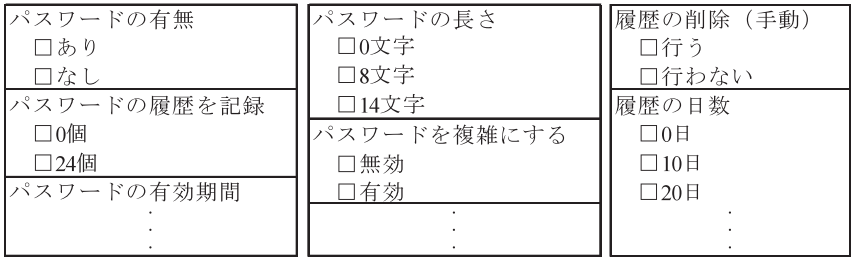

図 7　設定項目の提示形式
Fig. 7　Presentation format for setting parameters.

する．

（手順 2）　ツールによりユーザの要望を満たす設定組合せを導出し，ユーザに提示する．

（手順 3）　ユーザは，導出された設定組合せの中から，適切と思うものを選択する．また，必要に応じて個別に設定を変更する．

表 6　ユーザの要望と両方式によるレベル（実験 1）
Table 6　Levels of user's requirements and obtained levels by manual/proposed methods in the experiment No.1.

ユーザA

	希望レベル	実験 1-1	実験 1-2	実験 1-3	実験 1-4
		設定項目の説明前		設定項目の説明後	
		手動	本方式	手動	本方式
R1	低	中－低	低	低	低
R2	中－低	高	中－低	高－中	中－低
R3	中	高	中	高－中	中
R4	中－低	高	高－中	高－中	高－中
U1	中	中－低	中－低	低	中－低
U2	中－低	中	中－低	中－低	中－低
U3	中－低	高	高－中	中	高－中
U4	希望なし	高	高	高	高
満足数		3	6	4	6

(2)　実験結果

ここでは，被験者のうちの 1 名についての実験結果を例としてとりあげる．なお，全被験者の実験結果は，5.5 節で示す．

表 6 に，ユーザが最初に望んだ各リスクと利便性のレベル，および設定の説明前後において両方式により決定した設定で達成されるレベルを示す．同時に，ユーザの要望を満たしている数，つまりリスクが希望レベル以下のものと利便性が希望レベル以上のものの総数を満足数として示す．なお，希望レベルが「希望なし」の場合は，満足していると見なす．また，表 6 において，実験を行った順に実験番号（実験 1-1 など）を割り当てた．以後，この実験番号で結果を表記する．

さらに，選択された設定組合せによって得られる事故発生確率と利便性の値は**表 7** のようになる．

5.4　実験 2：値によるレベル分けの場合

(1)　実験手順

実験 1 によって，すでに被験者に対して設定に関する説明をしており，設定説明後の手動方式については実験 1-3 で行った．そこで，実験 2 では設定説明後における本方式のみ実験を行う．実験の手順は，実験 1 と同様である．

(2) 実験結果

表 6 と同じ被験者について，ユーザが最初に望んだ各リスクと利便性のレベル，および

表 7　選択された設定組合せにおける事故発生確率と利便性（実験 1）
Table 7　Risk probability and usability obtained in each selected terminal settings by manual/proposed methods in the experiment No.1.

ユーザA

	実験1-1	実験1-2	実験1-3	実験1-4
R1	4.50E-03	1.50E-03	1.50E-03	1.50E-03
R2	9.00E-01	1.00E-01	5.00E-01	1.00E-01
R3	7.20E-01	1.01E-02	5.01E-02	1.01E-02
R4	9.00E-01	1.01E-01	5.01E-01	1.01E-01
U1	1.69E-04	1.13E-04	1.13E-05	1.13E-04
U2	1.52E-04	1.13E-05	5.63E-06	1.13E-05
U3	8.00E-01	8.00E-02	5.00E-02	8.00E-02
U4	8.00E-01	8.00E-02	5.00E-02	8.00E-03

表 8　両方式によるレベルおよび事故発生確率と利便性（実験 2）
Table 8　Levels, risk probability, and usability obtained by manual/proposed methods in the experiment No.2.

ユーザA

	希望レベル	実験2-1		実験2-2	
		設定項目の説明後			
		手動	値	本方式	値
R1	低	低	1.50E-03	低	1.50E-01
R2	中－低	中	5.00E-01	低	1.50E-01
R3	中	低	5.01E-02	低	2.78E-03
R4	中－低	中	5.01E-01	低	2.78E-03
U1	中	低	1.13E-05	中－低	7.50E-02
U2	中－低	低	5.63E-06	低	2.81E-03
U3	中－低	中－低	5.00E-02	低	1.00E-03
U4	希望なし	中－低	5.00E-02	低	1.00E-08
満足数		4	－	5	－

手動方式と本方式により決定した設定で達成されるレベルと各値を**表 8** に示す．なお，手動方式の結果は，実験 1-3 で選択した設定により求まる事故発生確率と利便性の値を，実験 2 のレベル分けに対応させたものである．また，表 6 と同様に，表 8 で実験順に実験番号を割り当てており，以後はこの実験番号で結果を表記する．

ここで，各実験において，ユーザの望むレベルと両方式により得られたレベルとの距離（差異の大きさ）を**表 9** に示す．なお，ここでは 1 段階のレベルの違いについて，距離が 1 であるとし，リスクについては要望より低い場合を正，高い場合を負とし，利便性については要望より高い場合を正，低い場合を負としている．ただし，希望なしの場合は，距離を 0 とする．また，セキュリティと利便性のそれぞれの距離の総和を求め，さらに全体における距離として絶対値の総和を求めた．

表 9　ユーザの要望と両方式におけるレベルの差異
Table 9　Differences of levels between users' requirements and manual/proposed methods.

ユーザA

	実験1-1	実験1-2	実験1-3	実験1-4	実験2-1	実験2-2
R1	-1	0	0	0	0	0
R2	-3	0	-2	0	-1	1
R3	-2	0	-1	0	2	2
R4	-3	-2	-2	-2	-1	1
U1	-1	-1	-2	-1	-2	-1
U2	1	0	0	0	-1	-1
U3	3	2	1	2	0	-1
U4	0	0	0	0	0	0
リスク	-9	-2	-5	-2	0	4
利便性	3	1	-1	1	-3	-3
全体	14	5	8	5	7	7

5.5　全被験者の実験結果と検定

(1)　実験結果

全被験者の実験結果を**表 10** に示す．ただし，すべてのリスクと利便性についての結果を掲載することができないため，決定した設定により得られるレベルをもとに，希望レベルに対する満足数，およびリスク，利便性，全体の距離のみを示す．

次に，各実験で端末設定の決定に要した時間を**表 11** に示す．ここで，実験 2-1 は実験 1-3 で得られた設定組合せに対してレベル分け方法を変えただけであるため，実験 2-1 の実験時間は省略した．

実験を通して被験者から得たコメントを以下にまとめる．

（ア） 手動方式の場合，設定がどのようにリスクや利便性に影響するか分からず，設定が難しい．結果として得られたレベルを見て，要望との違いを感じた．

（イ） 本方式において，設定を変化させたときにレベルの変化が確認できるのは良い判断材料である．また，カスタマイズする中で，自分自身が納得のいく設定組合せとレベルを決定することができた．

（ウ） 本方式のツールで，要望するレベルを満たす設定がないと提示されたとき，どの要望

表 10　全ユーザの実験結果
Table 10　Results of all users in each experiment.

満足数

ユーザ	実験1-1	実験1-2	実験1-3	実験1-4	実験2-1	実験2-2
A	3	6	4	6	4	5
B	3	5	3	5	5	6
C	7	8	7	8	8	8
D	5	6	5	6	6	6
E	3	5	2	6	3	4
F	2	6	3	4	4	2
G	1	5	2	5	4	4
H	2	5	3	6	2	4
I	4	3	4	3	6	4
J	4	8	7	8	7	7
K	3	6	4	5	4	5
L	5	5	2	5	4	6
M	7	8	7	8	6	8
N	6	6	6	5	5	5
O	4	6	6	6	5	6
P	7	7	6	7	7	7
平均	4.13	5.94	4.44	5.81	5.00	5.44
標本分散	3.36	1.68	3.25	1.90	2.38	2.50

リスク

ユーザ	実験1-1	実験1-2	実験1-3	実験1-4	実験2-1	実験2-2
A	-9	-2	-5	-2	0	4
B	-11	1	-2	1	2	2
C	3	4	3	4	4	4
D	1	2	1	2	2	2
E	2	3	-10	3	-1	2
F	-3	3	2	3	3	0
G	-13	0	-13	0	0	0
H	-12	1	-12	1	-3	1
I	-3	-4	-3	-4	0	-3
J	0	1	1	1	1	1
K	-5	0	2	-1	2	-1
L	1	-5	-3	-4	4	-4
M	0	0	2	0	4	2
N	-8	-1	0	-2	0	-2
O	-2	0	0	0	0	0
P	0	4	1	4	4	3
平均	-3.69	0.44	-2.25	0.38	1.38	0.69
標本分散	26.46	6.25	25.19	5.98	4.11	5.09

利便性

ユーザ	実験1-1	実験1-2	実験1-3	実験1-4	実験2-1	実験2-2
A	3	1	-1	1	-3	-3
B	-1	-5	-4	-3	-8	-5
C	0	0	0	0	0	0
D	-6	-4	-7	-4	-7	-5
E	-10	-5	0	-5	-6	-9
F	-8	-2	-9	-8	-13	-10
G	-5	-6	-2	-6	-14	-14
H	-3	-5	-1	-3	-9	-8
I	-3	1	-3	-2	-8	-5
J	-4	2	1	2	-1	1
K	2	-1	-7	2	-7	-1
L	-7	0	-9	0	-16	0
M	2	4	0	4	-4	4
N	2	-1	-6	-2	-10	0
O	-4	-2	-4	-2	-6	-1
P	8	6	6	6	3	4
平均	-2.13	-1.06	-2.88	-1.25	-6.81	-3.25
標本分散	21.11	11.06	15.48	12.94	24.53	24.44

全体

ユーザ	実験1-1	実験1-2	実験1-3	実験1-4	実験2-1	実験2-2
A	14	5	8	5	7	7
B	16	8	10	6	10	7
C	5	4	5	4	4	4
D	9	6	10	6	9	7
E	14	12	14	8	11	11
F	11	9	13	11	16	16
G	18	6	15	6	14	14
H	15	6	15	4	12	9
I	8	9	6	8	8	8
J	6	3	4	3	2	4
K	11	3	9	9	9	4
L	8	5	12	4	20	6
M	6	4	10	4	16	6
N	10	2	6	4	10	4
O	6	2	4	2	6	5
P	10	12	11	12	11	9
平均	10.44	6.00	9.50	6.00	10.31	7.56
標本分散	14.87	9.63	13.13	7.75	20.21	12.00

が問題であるかを判断しにくい．

（エ） 本方式のツールにより導出された設定組合せ数が膨大な場合，いずれを選択すべきか判断が難しい．

（オ） 実験 2 では，実験 1 よりも設定組合せが導出されない場合が多く，すべての要望を満たすための条件が厳しいと感じられた．

（カ） ある一部のリスクや設定に関する要望だけを決め，他は自動的に決定する仕組みがあるとよい．推奨設定が提示されれば，設定を決定しやすい．

表 11　端末設定の決定に要した時間
Table 11　Time for deciding terminal settings in each experiment.

ユーザ	実験1-1	実験1-2	実験1-3	実験1-4	実験2-2
A	2分43秒	9分06秒	5分53秒	5分49秒	15分42秒
B	4分19秒	11分50秒	2分48秒	5分14秒	5分26秒
C	1分47秒	6分30秒	2分22秒	3分25秒	7分49秒
D	4分04秒	10分24秒	3分03秒	5分16秒	3分35秒
E	3分09秒	13分36秒	3分32秒	4分16秒	6分58秒
F	6分22秒	9分06秒	4分32秒	6分38秒	8分41秒
G	3分20秒	8分27秒	3分21秒	4分37秒	5分29秒
H	3分03秒	8分47秒	2分53秒	5分02秒	4分54秒
I	2分05秒	9分24秒	1分26秒	2分22秒	13分30秒
J	8分26秒	9分53秒	10分22秒	10分47秒	11分50秒
K	3分50秒	7分53秒	4分39秒	5分34秒	3分21秒
L	4分08秒	9分36秒	3分03秒	5分26秒	6分11秒
M	2分22秒	6分44秒	1分24秒	5分46秒	2分42秒
N	2分19秒	6分26秒	2分00秒	3分51秒	2分04秒
O	2分04秒	5分56秒	1分09秒	6分18秒	2分36秒
P	3分44秒	6分21秒	2分23秒	6分22秒	4分35秒
平均	3分37秒	8分45秒	3分26秒	5分25秒	6分35秒

（キ） 5 段階で提示されたレベルから，具体的なセキュリティ強度や利便性の違いを判断することが難しい．

（ク） リスクと利便性にトレードオフの関係があり，必ずしもすべては満たせるわけではないということが分かった．

(2)　結果比較のための検定

表 10 のように得られた実験結果から評価・考察する準備として，各実験結果に有意差があるかどうかを検定する．本実験では，各実験で得られる値について，母集団が正規分布に従うと仮定できるだけの被験者数とはいい難い．また，表 10 の「満足数」はユーザの要望の達成度合いの大きさを表しており，「リスク」，「利便性」，「全体」はリッカート尺度により抽出したユーザの要望をもとに，要望との距離を表している．そのため，これらの値はすべて序数尺度ととらえることができ，各実験結果は相互に対応のある標本といえる．そこで，検定手法として，符号の順位和による Wilcoxon の検定法を採用する[11]．

調査事項は，1) 本方式の方が満足数が大きいか，2) 本方式の方が全体の距離が小さいか，3) 本方式の方がリスクと利便性の距離が正の方向に増加するか，4) 手動方式では知識を得

表 12　符号の順位和による Wilcoxon 検定の結果
Table 12　Results of Wilcoxon's signed rank sum test.

実験1-1と実験1-2

調査事項	対象	N	T	T_α	検定	採択
1	満足数	13	11.5	21	片側検定	H_1
3	リスク	15	19.5	30	片側検定	H_1
3	利便性	15	70	30	片側検定	H_0
2	全体	16	28	35	片側検定	H_1

実験1-3と実験1-4

調査事項	対象	N	T	T_α	検定	採択
1	満足数	15	22	30	片側検定	H_1
3	リスク	14	46.5	25	片側検定	H_0
3	利便性	14	17	25	片側検定	H_1
2	全体	15	24.5	30	片側検定	H_1

実験1-1と実験1-3

調査事項	対象	N	T	T_α	検定	採択
4	満足数	10	15.5	10	片側検定	H_0
4	リスク	11	7.5	13	片側検定	H_1
4	利便性	13	70	21	片側検定	H_0
4	全体	13	42	21	片側検定	H_0

実験1-2と実験1-4

調査事項	対象	N	T	T_α	検定	採択
5	満足数	5	7	—	両側検定	—
5	リスク	3	2	—	両側検定	—
5	利便性	6	9.5	0	両側検定	H_0
5	全体	8	10	3	両側検定	H_0

実験2-1と実験2-2

調査事項	対象	N	T	T_α	検定	採択
1	満足数	10	6	10	片側検定	H_1
3	リスク	10	44.5	10	片側検定	H_0
3	利便性	13	7.5	21	片側検定	H_1
2	全体	10	8	10	片側検定	H_1

た方がより良い結果となるか，5) 本方式では知識の有無に関係なく同等の結果が得られるかどうかの 5 つである．なお，4) での「結果が良くなる」とは，満足数が増加すること，リスクや利便性の距離が正の方向に増加すること，全体の距離が小さくなることを意味する．

それぞれの調査に際し，次のような仮説を立てる．ここで，帰無仮説 H_0，対立仮説 H_1 とし，有意水準 α はすべて $\alpha = 0.05$ とする．

1)　H_0：両方式で満足数に差はない．
　　H_1：本方式の方が満足数が大きい．
2)　H_0：両方式で全体の距離に差はない．
　　H_1：本方式の方が全体の距離が小さい．
3)　H_0：両方式でリスク（利便性）の距離に差はない．
　　H_1：両方式でリスク（利便性）の距離が正の方向に増加する．
4)　H_0：手動方式は知識の有無により結果に差はない．
　　H_1：手動方式は知識を得ることで結果がよくなる．
5)　H_0：本方式は知識の有無により結果に差はない．
　　H_1：本方式は知識の有無により結果に差がある．

この仮説のもと，検定を行った結果を**表 12** に示す．ここで，T は検定統計量，N は標本数（差が 0 の場合は標本数から除外される），T_α は片側検定または両側検定に対応した有意水準 5%における優位点である．さらに，

$T > T_\alpha$ ならば H_0 を採択，
$T \leq T_\alpha$ ならば H_0 を棄却（H_1 を採択）

という結論を同表に示す．ただし，実験 1-2 と実験 1-4 の検定における満足数とリスクについては，両実験結果の差が 0 のものが多く，検定に必要な標本数を得られなかったため，検定ができなかった．

6. 評価・考察

本章では，5 章の実験結果から，本方式が 2.1 節で述べた問題点を解決しているかどうかを評価・考察する．また，決定した設定組合せの端末への適用についても考察する．

6.1 ユーザの要望の具体化

本実験では，ユーザの望むセキュリティと利便性を定める手段として，設定項目に関係するリスクと利便性を提示し，どのセキュリティや利便性を優先するかを相対比較しながら決定した．その結果，本実験の被験者 16 名においては，具体的にどの程度のセキュリティや

利便性を確保したいか不明瞭であっても，容易に要望を決定することができた．

さらに，ツールにより導出した設定組合せをカスタマイズする際に，同ツールでリスクと利便性のレベルの変化を明示した．このように，設定選択の過程においてリスクや利便性の変化をユーザにフィードバックすることで，コメント（ク）のようにリスクと利便性に対する理解を深めるとともに，ユーザが本来求めているセキュリティや利便性を具体化する助けとなることが確認できた．

ただし，順位によるレベル分けでは，表 5 のように各リスクや利便性のレベルに対応する値が大きく異なる．そのため，表 6 と表 7 から分かるように，あるリスクのレベル「高」と他のリスクのレベル「高」では，危険性が異なることがある．また，ユーザ間で，あるリスクが同じレベルであっても，事故発生確率が大きく異なる場合もある．以上から，レベル表示と本来の危険性や快適さにズレが生じ，実際は危険な状態であるにもかかわらずユーザが安心するような状況が生じうる．一方，値によるレベル分けでは，レベル表示に対する事故発生確率と利便性の関係が明確なため，より正確な指標として扱うことができる．しかし，値によるレベル分けの場合，本実験では簡易的に閾値を設定したが，利用環境を考慮した適切な閾値の設定が求められる．

6.2　端末設定の決定の容易さ

まず，各実験の所要時間の面から，表 11 をもとに評価・考察する．実験 1-1 と実験 1-2，実験 1-3 と実験 1-4 の時間をそれぞれ比較すると，設定の説明前後にかかわらず，本方式の方が多くの時間を要している場合が多い．これについて，手動方式ではユーザは設定を選択した後の見直しをほとんど行わなかった．一方，本方式では，設定変更時にリスクと利便性のレベルの変化を提示した結果，希望するレベルに近づくように設定組合せの見直しをユーザが積極的に行ったため，要した時間が長くなった．また，ツールによる設定組合せの導出時間が最大で 1 分程度かかっており，計算時間も本方式における時間が長くなった一因である．

一方，実験 1-1 と実験 1-3 から，手動方式では，設定に関する知識が必ずしも設定の決定時間の短縮に寄与していない．一方，実験 1-2 と実験 1-4 から，本方式では，ほぼすべてのユーザにおいて，設定の説明後の方が時間が短縮された．これは，知識を得たことで，導出された設定組合せを容易に選択・カスタマイズできるようになったためと考えられる．しかし，知識を得たという同一条件下であるにもかかわらず，実験 2-2 は実験 1-4 よりも比較的長い時間を要した．これはコメント（オ）のとおり，条件を満たす設定組合せが導出されない場合が多かったためである．

また，レベルを提示することが設定の決定に有益であるかどうかを考察する．コメント（ア），（イ）から，選択した設定がユーザの望むセキュリティと利便性を達成できているかどうかを確認できることは，設定の決定を容易にする手助けとなることが分かる．ここで，2 つのレベル分け方法の違いは，設定組合せの導出結果や導出時間，カスタマイズ時のレベル変化の特性には影響を与える．しかし，設定変更により変化するリスクや利便性のレベルは，レベル分け方法にかかわらずツールにより同じように確認できる．したがって，本方式は両レベル分け方法において，設定の決定を容易にすることができる．

以上から，本方式は手動方式よりも多少時間はかかるものの，レベルの変化をフィードバックさせることで，ユーザの望む利便性とセキュリティを達成可能な設定を容易に決定することができる．

6.3　端末設定の妥当性の評価

(1)　ユーザの要望を満たす設定組合せの決定

本方式がユーザの要望を満たす設定組合せを決定できるかどうかについて，表 12 の検定結果から評価・考察する．まず，実験 1-1 と実験 1-3 における満足数や全体の距離についての検定結果から，知識を得たとしても，手動方式ではユーザの要望をより多く満たす端末設定を決定できるようになるとは限らないことが分かる．

次に，順位によるレベル分けにおいて，端末設定に関する知識がない場合（実験 1-1 と実験 1-2），および知識を得た場合（実験 1-3 と実験 1-4）の両検定結果から，本方式は手動方式と比較して満足数が大きく，ユーザの要望との全体の距離も小さい．加えて，知識を得た後という同一条件下で行った実験 1-3 と実験 1-4，および実験 2-1 と実験 2-2 の検定結果から，両レベル分け方法において，本方式は手動方式よりも満足数が大きく，全体の距離が小さい．これらの結果から，2 つのレベル分け方法のいずれにおいても，本方式の方がユーザの要望を満たす端末設定を決定できるといえる．

さらに，実験 1-2 と実験 1-4 では，満足数について標本数が少ないため検定はできないが，両実験で満足数の差が 0 であるユーザが 11 名存在したという事実と，知識の有無によって全体の距離に差が生じるとはいえないという検定結果，および前述した満足数と全体の距離に対する本方式の優位性から，本方式では知識の有無にかかわらずユーザの要望を満たす端末設定を決定することができると考えられる．

最後に，リスクと利便性の距離について，実験 1-1 と実験 1-2 の検定結果から，端末設定に関する知識がない場合には，本方式のほうがリスクを抑制できているが，利便性が向上していることは認められない．これは，実験 1-1 では利便性を重視して設定を決定していた

が，実験 1-2 ではツールによりリスクの大きさが提示されることによって危険性を認識し，利便性を多少犠牲にしても，リスクを低減させようとしたことが要因の 1 つではないかと考えられる．

一方で，実験 1-1 と実験 1-3 の検定結果から，手動方式では，知識を得ることでリスクの距離は改善されているが，満足数や全体の距離が改善されるとはいえない．これに対し，実験 1-3 と実験 1-4 の検定結果から，本方式では，リスクの距離が改善されているとはいえないが，利便性が向上し，満足数や全体の距離も改善されている．このことから，本方式では，セキュリティと利便性のバランスを考慮して，ユーザの要望をより多く満たすような設定を決定することができる．

以上から，本方式では，レベル分け方法の違いによってレベルと値の対応関係は異なるものの，セキュリティと利便性のバランスを考慮しつつ，ユーザの要望をより多く満たす設定組合せを決定することができる．また，決定した設定により得られるセキュリティと利便性の妥当性は，レベルと対応した事故発生確率と利便性の値により保証される．

レベルと値の対応関係の妥当性の証明は難しいが，順位によるレベル分けでは，全設定組合せの中で相対的にどの程度安全な組合せであるかを示すことができる．一方，値によるレベル分けでは，ある一定の事故発生確率や利便性を保証することができる．

(2)　多様なユーザの要望への対応

被験者が初めに希望したレベルを見ると，セキュリティと利便性の両方を高レベルで望むユーザ，利便性またはセキュリティの一方のみを重視するユーザ，セキュリティと利便性のバランスを考えるユーザなど，特徴は様々であった．また，どのリスクや利便性を重視するかもユーザにより異なっていた．それでもなお，本方式では現実的に実現できない要望をユーザに理解させつつ，最終的にユーザの納得する設定を決定できた．したがって，本方式は多様なユーザの要望に対応可能であると考えられる．ただし，今回の実験では，被験者は本研究室の学生であり，偏りがある．そのため，PC 操作に対する技術力や年齢層などが異なる場合でも同様の結果が得られるかどうかについては，さらなる検証が必要である．

加えて，コメント（ウ）のように本方式で要望を満たす設定が見つからないことがあった．これは，一見問題点のようであるが，コメント（ク）のように実現不可能な要望であることをユーザ自身が理解し，利便性とセキュリティのバランスを考える機会となるため，現実的な設定につながる．ただし，コメント（エ）のように導出される設定組合せ数が膨大になり判断が難しい場合や，コメント（オ）のように実験 2 で何度も設定組合せが見つからない場合があったため，コメント（カ）のように推奨設定を利用するなど，実現可能な設定組合せを効率的に導出する仕組みが必要である．

6.4　端末への設定の適用に関する考察

本方式により決定した設定組合せが実際にユーザの望むセキュリティと利便性を実現できることを確認するためには，端末へ設定を適用し，評価することが必要である．しかし，本方式ではセキュリティや利便性の程度を 5 段階の相対尺度で表現しているため，コメント（キ）のように，レベルに対する実際のセキュリティや利便性の程度について曖昧さが残っており，ユーザによってレベルに対するとらえ方が異なる．さらに，6.1 節で述べた問題が残っており，端末への設定適用時におけるセキュリティや利便性の達成度合いについて，全ユーザに共通する評価指標を設定することが現段階では難しい．

適用時の評価を正しく行うためには，リスクや利便性の値，またレベル分けの妥当性を確保しなければならない．翻って，リスクや利便性の値と，レベル分けの妥当性が確保できれば，共通の評価指標を設定することができる．これにより，端末へ設定を適用した場合に，実際にユーザの要望を実現できるかどうかを評価することができるようになる．なお，これらは 7 章において課題として詳述する．

7.　今後の課題

(1)　発生確率や利便性の値の妥当性

リスクや利便性を正しく評価するためには，それぞれの端末設定がリスクや利便性に与える影響について，妥当な値を割り当てる必要がある．しかし，これらの値は，利用環境により異なる．また，ユーザのとらえ方も大きく関係するが，これらの値をユーザが割り当てることは，全端末設定を理解することに等しく，要望を容易に決定したいという本研究の目的と対立する．

そのため，たとえば組織のリスク分析結果を活用するなど，妥当な数値の割り当て方法を検討する必要がある．また，セキュリティや利便性に対するユーザごとのとらえ方の違いを反映できるように，事故発生確率や利便性の算出時に，重要度を用いて重み付けを行うなど，より妥当性のある定量化が必要である．

(2)　レベル分けの妥当性に関する検討

レベル分けの妥当性については，まず，リスクや利便性の値が妥当であるという前提が必要である．さらに，組織やユーザによって安全性や利便性を評価する基準が異なる可能性があるため，妥当な基準を設けることが難しい．

しかし，このレベル分けはユーザの要望の具体化や設定組合せの妥当性に関係する重要な

要素である．そのため，レベルを分ける際に考慮すべき要素を整理し，適用環境において適切なレベル分けを実現する方法について，十分な検討が必要である．

(3)　端末への設定適用による要望達成の評価

6.4 節で述べたように，決定した設定組合せを端末へ適用し，実際に端末を利用した際に，ユーザの望むセキュリティや利便性を達成できるかどうかを実験・評価する．このために，(1)，(2) の課題を解決し，端末利用時におけるセキュリティと利便性の達成度合いを評価するための指標を決定する必要がある．また，端末利用時にユーザの要望との差が生じた場合に，その差をフィードバックし，ユーザの要望をより正確に実現できる端末設定を再決定できる仕組みが必要である．

(4)　ネットワーク上の対策との連携

環境によっては，ファイアウォールや侵入検知/防御システムなどの対策が施されている．そのため，端末上での設定とネットワーク上の対策を適切に連携させることで，セキュリティと利便性を効率的かつ効果的に実現できる可能性がある．そこで，文献 2) の手法と本方式を組み合わせ，ネットワーク上の対策と端末を適切に制御する手法について検討を行う．

8. ま と め

本論文では，ネットワーク利用時にユーザの望むセキュリティと利便性を実現するために，ユーザの利用する端末に着目し，最適な端末設定を決定する方式を提案した．まず，FTA を用いてリスク，利便性，端末設定の関係性を整理し，リスクと利便性を定量化する方法について述べた．そして，セキュリティと利便性に関するユーザの要望を具体化し，この要望を達成可能な設定組合せの導出とカスタマイズにより，端末設定を決定する方式を示した．さらに，適用実験を行い，本方式がユーザの要望を具体化でき，ユーザの望む妥当な端末設定を容易に決定できることを確認した．

今後は 7 章で述べた課題に取り組み，多様なネットワーク環境においてセキュリティと利便性の両立を実現可能な方式の確立を目指していく．

参 考 文 献

1) ユビキタスネットワーキングフォーラム（編）：ユビキタスネットワーク戦略—ユビキタス NW 技術の将来展望，クリエイト・クルーズ (2002).
2) 加藤弘一，勅使河原可海：ネットワーク特別利用時におけるセキュリティと利便性を考慮した最適対策決定手法の提案，情報処理学会論文誌，Vol.49, No.9, pp.3209–3222 (2008).
3) Microsoft：Windows 2000 Server セキュリティ運用ガイド，第 2 章—セキュリティリスクとは．http://www.microsoft.com/japan/technet/security/prodtech/windows2000/staysecure/secops02.mspx
4) IPA：2008 年度第 1 回情報セキュリティに関する脅威に対する意識調査報告書．http://www.ipa.go.jp/security/fy20/reports/ishiki01/documents/200801_ishiki.pdf
5) 総務省：平成 15 年版情報通信白書．http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h15/index.html
6) 塩見　弘，島岡　淳，石山敬幸：日科技連信頼性工学シリーズ 7　FMEA，FTA の活用，日科技連 (1983).
7) Microsoft：脅威とその対策，Windows Server 2003 と Windows XP のセキュリティ設定．http://technet.microsoft.com/ja-jp/library/cc163024.aspx
8) Ed Bott, Carl Siechert, Craig Stinson（著），ユニゾン（訳）：Windows XP オフィシャルマニュアル上下巻，日経 BP ソフトプレス (2002).
9) Microsoft Corporation（著），金田芳明，川島　潤，木村尚子，松葉素子（訳）：Windows XP Professional リソースキット上巻，日経 BP ソフトプレス (2002).
10) Microsoft Corporation（著），金田芳明，川島　潤（訳）：Windows XP Professional リソースキット下巻，日経 BP ソフトプレス (2002).
11) 応用統計ハンドブック編集委員会（編）：応用統計ハンドブック，養賢堂 (1986).

(平成 20 年 12 月 1 日受付)
(平成 21 年　6 月 4 日採録)

加藤　弘一（学生会員）

2005 年創価大学工学部情報システム学科卒業．2007 年同大学大学院工学研究科博士前期課程修了．現在，同大学院工学研究科博士後期課程在学中．情報セキュリティに関する研究に従事．

松林　大樹（正会員）

2007 年創価大学工学部情報システム工学科卒業．2009 年同大学大学院工学研究科博士前期課程修了．同年アクセンチュア・テクノロジー・ソリューションズ株式会社に入社．在学中，情報セキュリティに関する研究に従事．

勅使河原可海（フェロー）

1970 年東京工業大学大学院理工学研究科制御工学専攻修了．工学博士．同年日本電気入社．コンピュータネットワーク，ネットワークアーキテクチャ，衛星データネットワーク等の開発に従事．1994〜1996 年ハワイ大学アロハシステム客員研究員，1995 年創価大学工学部教授，工学部長，工学研究科長を歴任．ユビキタスコンピューティング，グループウェア，e-learning，ネットワークセキュリティ等の研究に従事．情報処理学会，オペレーションズリサーチ学会各フェロー，電子情報通信学会，経営情報学会，IEEE，ACM 各会員．