

利用ネットワークのセキュリティポリシーを考慮した 利便性とセキュリティに対するユーザ要求に基づく端末設定方式の提案

松林 大樹[†] 加藤 弘一^{††} 勅使河原 可海^{††}

創価大学工学部[†] 創価大学大学院工学研究科^{††}

1. はじめに

近年、自宅や大学、外出先など様々な場所で端末を利用するユーザが増加している。この際、ユーザは利用する場所によって利便性とセキュリティに関する様々な要望を持つと考えられる。例えば、自宅では多くのサービスを利用するために利便性を上げたい、外出先ではセキュリティに不安があるのでセキュリティレベルを上げたいといった要望がある。しかしながら、利便性とセキュリティに関する要望を実現するためにはネットワークサービス、セキュリティ、端末の設定などに関する深い知識と経験を必要とするため、ユーザ自身が設定を行うことは難しい。

そこで本稿では、ユーザが利便性とセキュリティの要望を実現するための方式を提案する。まずユーザの要望を抽出し、ユーザポリシーとして定義する。そして、セキュリティポリシーを遵守しつつユーザポリシーを利用する端末の設定へと反映することにより、ユーザの望む端末環境を実現する。

2. 関連技術と課題

(1) Microsoft Baseline Security Analyzer (MBSA)

Microsoft がサポートしているツールであり、コンピュータのセキュリティ状態を確認し、最適なセキュリティ設定を推奨する[1]。しかし、IT プロフェッショナルが対象であり、一般ユーザ向けではない。また、推奨された設定はユーザ自身で行わなければならない。

(2) Safe XP

不要なサービスや設定を無効にして最適化とセキュリティ強化のためのツールである[2]。推奨設定などがあり、項目にチェックを入れることにより設定を行う。項目数は多くないが、難解な設定もあり、知識のない一般ユーザが設定するのは難しい。また、セキュリティ強化のためのツールであるので、利便性を上げたいというユーザの要望を実現することはできない。

3. 提案方式と動作概要

本稿では、ユーザの利便性とセキュリティに関する

要望を端末へ反映する方式を提案する。本方式では、ユーザの要望を点数として抽出し、端末設定を導き出す。そして、この点数や設定内容をユーザポリシーとして持ち歩き、利用端末に適用することで、ユーザの望む端末利用が可能となる。

本方式の動作として、ユーザの要望の抽出、ユーザポリシーの定義、端末設定項目のパラメータ算出と反映がある。本方式の動作の流れを図1示す。動作概要を以下に述べる。

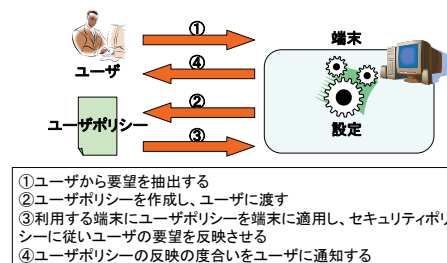


図1 提案方式の動作の流れ

3.1 ユーザの要望の抽出

ユーザの要望を抽出する際に、すべての端末設定項目についてユーザに確認する方法は、ユーザの理解や負担から見て現実的ではない。そこで、ユーザが直感的で分かりやすい点数の概念を用いてこれを解決する。

まず事前に、端末の設定項目をその役割ごとによくつかの 카테고리 に分類する。一つの設定項目が複数のカテゴリに属する場合もある。

ユーザがカテゴリごとに自身の望む利便性とセキュリティを点数として表現することで、大まかなユーザの要望を抽出する。その際、あるカテゴリ内の点数の変化が他のカテゴリの利便性やセキュリティに影響を与えることがあるため、ユーザ自身で調整を行う。さらに、その点数をもとにした端末設定の候補をユーザに提示し、ユーザの意思と異なる部分を修正することで、詳細なユーザの要望を抽出する。

3.2 ユーザポリシーの定義

ユーザから抽出した利便性とセキュリティに関する要望をユーザポリシーとして定義する。その際、ユーザの可読性が高く、かつ機械的に処理できるように記述する必要がある。また、ユーザは自身のユーザポリシーを持ち歩き、それを利用するネットワークの端末に適用させることによって、利用する端末にユーザの要望を反映させることができる。

A Proposal of a terminal setup method based on the users' requirements of Usability and Security Considering Network Security Policies

Hiroki Matsubayashi[†], Koichi Kato^{††}, Yoshimi Teshigawara^{††}

[†] Faculty of Engineering, Soka University

^{††} Graduate School of Engineering, Soka University

3.3 端末設定項目のパラメータ算出と反映

ネットワーク環境は大きく分けて、ホームネットワークなどセキュリティポリシーがないネットワークと、企業や大学などセキュリティポリシーが存在するネットワークの2つがある。前者は、特に制約がないため、ユーザポリシーをすべて端末の設定へと反映させることができる。一方、後者については、セキュリティポリシーの規定事項に該当する端末設定は変更することができず、ある決まったパラメータとなる。これを考慮した上で、ユーザポリシーを端末へと反映させる。

4. 設定項目のパラメータ算出方法

3.1 節で述べたように、各カテゴリーの利便性とセキュリティに点数を付けることで、ユーザの要望の抽出を行う。例えば、ユーザがログインの利便性を4.0点以上に設定したいという要望を持つ場合、図2のような設定パラメータが算出される。なお、利便性2.0点は、算出されたパラメータから計算された値である。

- セキュリティ4.0点、利便性2.0点
- パスワードを設定する
- ログインの失敗回数を制限しない
- 簡単なパスワードを使用しない
- ようこそ画面を使ってログインする

図2 算出された設定パラメータ

このようにユーザが点数を決めると、設定すべき項目が算出される。ユーザがこの設定を受け入れると、各カテゴリーの利便性とセキュリティの点数、および設定項目をユーザポリシーとして定義する。

5. 設定項目の点数化

5.1 端末設定に対する事前の点数割当て

ユーザが決めた点数から設定パラメータを算出するために、すべての設定項目に対し、カテゴリー分け、利便性とセキュリティに関する点数の割当てを事前に行う必要がある。まず、設定項目が属するカテゴリーごとに、利便性とセキュリティに1~5点の点数を付ける。点数が高いほど、その効果が高いことを表す。ログインカテゴリーの点数の例を表1に示す。ただし、「利」は利便性、「セ」はセキュリティを表す。また、例では点数が1点と5点だけであるが、中間的な設定項目がある場合には2~4点を付けてもよい。

表1 ログインに関する点数の例

No.		設定a	設定b
1		<input type="checkbox"/> パスワードを設定する	<input type="checkbox"/> パスワードを設定しない
	利	1	5
	セ	5	1
2		<input type="checkbox"/> ログインの失敗回数を制限する	<input type="checkbox"/> ログインの失敗回数を制限しない
	利	1	5
	セ	5	1
3		<input type="checkbox"/> ログオンで簡単なパスワードを使用しない	<input type="checkbox"/> ログオンで使用するパスワードに制限をかける
	利	1	5
	セ	5	1
4		<input type="checkbox"/> ようこそ画面を使わずにログインする	<input type="checkbox"/> ようこそ画面を使ってログインする
	利	1	5
	セ	5	1
5		<input type="checkbox"/> 直前にログインしたユーザ名を表示しない	<input type="checkbox"/> 直前にログインしたユーザ名を表示する
	利	1	5
	セ	5	1

5.2 点数と設定項目パラメータの具体例

ユーザが決めた利便性とセキュリティの点数から設定パラメータを算出するためには、点数と設定パラメータの関係を整理する必要がある。そのため、まず表1の丸印のように設定した端末の状態を、以下の計算式で点数化する。

$$\text{利便性の点数} = \frac{\text{設定項目の利便性の点数の合計}}{\text{設定項目の個数}}$$

$$\text{セキュリティの点数} = \frac{\text{設定項目のセキュリティの点数の合計}}{\text{設定項目の個数}}$$

表2 利便性とセキュリティの点数

カテゴリー	利便性	セキュリティ
ログイン	3.4	2.6

このように、設定パラメータから利便性とセキュリティの点数を算出することができる。そのため、ユーザが決めた点数となるように設定パラメータを逆算できると考える。ただし、適切なパラメータの組み合わせの算出についての検討が必要である。

5.3 点数化の考察

表1では、ログインの際にIDとパスワードを入力するように設定しているため、セキュリティの点数は比較的高くなるはずであるが、表2では2.6と低い値となっている。その原因は、それぞれの設定項目が対等な立場にあり、設定項目間での重要さの差異を考慮に入れていないからと考えられる。そのため、利便性やセキュリティへの効果の大きさや重要度を考慮するために、点数の重み付けが必要になると考えられる。現在、設定項目間の関係などを考慮にいれた点数計算方法について検討中である。

6. 本方式の利点

本方式では、知識のない一般ユーザでも端末に関する要望をユーザポリシーとして作成することができる。また、セキュリティポリシーを考慮しながら、ユーザポリシーを利用する端末に適用させることによって、ユーザはネットワーク環境に左右されることなく自身の要望を端末に反映させることができる。

7. まとめと今後の課題

本稿ではユーザの要望の抽出によるユーザポリシーの作成、セキュリティポリシーを遵守しつつ反映する方法について提案した。今後は、点数の計算方法のその妥当性について検討を行っていく。また、ユーザポリシーの記述方法についても検討を進める。

参考文献

- [1] Microsoft Baseline Security Analyzer (MBSA) : <http://www.microsoft.com/japan/technet/security/tools/mbsahome.mspx>
- [2] Theorica Software, Safe XP : <http://www.theorica.net/safexp.htm>