アンチウィルスソフトの改善に関する一提案

澤村 隆志† 吉本 道隆* 加藤 貴司‡ ベッド B ビスタ‡ 高田 豊雄‡

†‡ 岩手県立大学ソフトウェア情報学部
020-0193 岩手県岩手郡滝沢村滝沢字巣子 152 番地 52

† g031e089@edu.soft.iwate-pu.ac.jp ‡{t-kato,bbb,takata}@iwate-pu.ac.jp
* 清泉女学院大学　人間学部
381-0085 長野県長野市上野 2-120-8

yoshimoto@seisen-jc.ac.jp

あらまし　セキュリティ製品を適切に利用することはセキュリティ確保にとって重要であるが, 何らかのユーザビリティ上の問題により適切な設定・運用がなされず, 結果としてセキュリティが確保されないという問題がある. そこで本研究では現在提供されている有償のアンチウィルスソフトを取り上げ, まず, 一般ユーザが適切に使用しているかどうかを調査し, 問題点を発見する. 次に発見された問題点を改善したアンチウィルスソフトの設計と開発について述べる.

A Proposal of How to Improve Usability of Anti-Virus Software

Takashi Sawamura† Michitaka Yoshimoto* Takashi Katoh‡
Bista Bhed Bahadur‡ Toyoo Takata‡

†‡ Faculty of Software and Information Science, Iwate Prefectural University,
152-52, Sugo, Takizawa, Iwate, 020-0193 Japan

† g031e089@edu.soft.iwate-pu.ac.jp ‡ {t-kato,bbb,takata}@iwate-pu.ac.jp
* Faculty of Human Studies, Seisen Jogakuin College
2-120-8, Ueno, Nagano, Nagano, 381-0085 Japan

yoshimoto@seisen-jc.ac.jp

Abstract　To establish proper security, it is important for us to use security products or tools appropriately. Sometimes, it is often seen that a system fails to establish security because it has some usability problems that bring it into improper settings or operation.

In this paper, we investigate usability problem of commercial off-the-shelf anti-virus softwares. At first, we conduct formative evaluation of those software by employing individual non-expert users and find usability problems of them. Next, we discuss design and development of anti-virus software which solves the found problems.

1　背景

近年，マルウェアの発見数が爆発的に増加傾向にあり，エフセキュアが行った調査では，2008年は前年の 3 倍のマルウェアが発見されたと報告された [1]．2009 年も新たなマルウェアの感染が広がっている．マルウェアの多くは端末の脆弱性を利用して動作しているため，端末に侵入されない仕組みと感染した場合に直ちに検知，駆

除できる対策が必要となり，ユーザがマルウェアに対し対策する場合，アンチウィルスソフトを導入することが求められる．端末に対するアンチウィルスソフトの導入率は年々増加傾向 [2] にあり，ほとんどの有償のアンチウィルスソフトは 90 %を超える検知率である．また，アンチウィルスソフトにはパーソナルファイアウォール機能やフィッシング対策機能なども兼ね備えているケースもあり，ユーザが攻撃に遭わないための機能が提供されている．また，パターンファイルの更新時間の間隔も短くなり，最新のマルウェアに対応できる仕組みを採っている．

一方，我々の行った予備実験によるとアンチウィルスソフトの機能を使い切れずに，駆除すべきマルウェアに対して誤った選択によって駆除できずに攻撃を許してしまいかねない事例を観察している．これはアンチウィルスソフトのユーザビリティ上の問題により適切な設定，運用がなされず，結果としてセキュリティを確保されていないことが問題である．

2　アンチウィルスソフトの調査

そのため，本研究では，アンチウィルスソフトのユーザビリティ改善を採り上げる．すでに行われたセキュリティスキャナのユーザビリティの改善に関する研究 [3] で得られた知見を基に，アンチウィルスソフトの潜在的な問題点を発見する．次にその問題点を改善した新しいアンチウィルスソフトの設計と開発について述べる．具体的な問題点発見の対象として，普及率，検知率の高い有償の以下の製品から選択する．

- カスペルスキーインターネットセキュリティ 2009
- ノートンインターネットセキュリティ
- マカフィーウィルススキャンプラス
- イーセネットスマートセキュリティ
- ウィルスセキュリティ
- ウィルスバスター 2009

各アンチウィルスソフトのインストール方法，インタフェース，更新方法，頻度，また，手動スキャンや定期的な自動スキャンの方法，オプションとしてどのような機能が提供されているか，初期設定で提供されている機能についても調査する．次に，製品の中からいくつか選択し，一般ユーザに適切に使われているのかということを調査し，ユーザビリティ上の問題点をあげていく．調査方法としては，ユーザが操作中に考えたこと，感じたことを全て口に出す思考発話法 [4] を用い，開発者が想定できなかった問題点を発見する．

2.1　調査内容

同一スペックのマシンを 6 台用意し，各マシンそれぞれにアンチウィルスソフトをインストールする．インストールから再起動までのプロセス，各アンチウィルスソフトのインタフェースや，パターンファイルの更新方法，頻度を調査する．加えて，各アンチウィルスソフトがどのような機能を提供しているのか，また，初期設定で提供されている機能についても調査する．以降，製品名を記述せずに調査結果を述べる．

2.2　インストール

全製品で，旧バージョン，他製品がインストールされていた場合は，アンイストールされ最新のバージョンに更新される．インストール先の選択や，許諾契約書の同意，ユーザ登録なども共通して表示された．

2.3　インタフェース

ほとんどの製品で共通した構成となっており，左側にスキャン，更新，ヘルプといった項目が並んでいる．項目をクリックすると，その詳細，機能の実行ボタンなどが左側に表示される．端末が安全であるかを知らせるアイコンも各製品で共通していて，安全なら青色，パターンファイルを更新していない，マルウェアのスキャンを実行してないなどの場合は黄色，マルウェアを

検知したが駆除をまだ行っていない，重要な機能が動作していないなどの場合は赤色といったように，信号機の色を想起させるインタフェースとなっている．

2.4 パターンファイルの更新

全ての製品でユーザに確認することなく自動で行われる．更新頻度は製品によって異なり，1時間未満から1日に1回程度行われる．

2.5 手動スキャン

全ての製品でメイン画面から実行できる．実行の際，どの領域のスキャンを行うか選択できるようになっており，ファイルやフォルダ，ドライブを選択する方式やシステムメモリ，スタートアップオブジェクト，ブートセクタなど細かい領域まで選択できる方式もあり，スキャン領域の区分けは製品によって大きく異なる．

2.6 自動スキャン

自動スキャンは製品により多少違いがあり．全ての製品が初期から実行されるように設定されているわけではなく，自動スキャンを行うためにはユーザが設定しなければならない製品もある．一部の製品ではアイドルタイムでのみ実行されるスキャン機能を搭載しており，定期的に行われる自動スキャンは搭載されていない．自動スキャンを搭載した全製品でスキャン実行の日時を細かく設定することが可能である．

2.7 マルウェアの検知と駆除

ほとんどの製品ではポップアップメッセージでマルウェアの検知，駆除についての内容が表示される．表示後，数秒でメッセージが消えてしまう製品もある．処理方法は，一部の製品では，マルウェアの危険度が低い場合，処理方法についてユーザに問いかける内容が表示されるが，ほとんどの製品がマルウェアの検知と駆除を自動で行う．

2.8 用語の違い

意味は同じでも製品によって異なる用語を確認した．以下に例を示す．

- アクティベーションコード＝シリアル番号
- プログラムスキャン＝ウイルススキャン
- ウィルス＝マルウェア
- フォルダ，ドライブ＝オブジェクト

また，ほとんどの製品では，“ スキャン ”，“ 更新 ”，“ 設定 ”，“ ヘルプ ”といったメニューで構成されているが，一部の製品では，“ ウイルスとスパイウェアから守る ”，“ 不正侵入を防ぐ ”いったように，ユーザに理解しやすくするためと思われるメニューになっている．

3 形成的評価

形成的評価にはLeiwsらによって開発された“ 思考発話法 ”[4]を用いる．

3.1 思考発話法

思考発話法は被験者がシステムを使いながら常に考えたことを声に出していく方法である．考えを口に出すことによって，被験者がどのようにシステムを見ているのかを理解し，被験者の誤解を容易に知ることが出来る．長所は作業中，実際に何をしているのか，どうしてそれをするのかを観察でき，加えて非常に少数の被験者から多くのデータを集められることである．

3.2 実験環境と実験手順

アンチウィルスソフトがインストールされていないマシンを用意する．Windows Vistaにログインした状態にしておき，被験者にはアンチウィルスソフトのインストールから行ってもらう．評価の偏りを無くすため，被験者が普段使っていない製品を選択する．今回の実験では，被験者全員が，自分専用のPCを所持しており，有償のアンチウィルスソフトをインストールし

ている．
以下の順に実験を行う．

1. アンチウィルスソフトのインストール
2. 自由に設定させる
3. 自動スキャンの設定
4. 手動スキャンの実行
5. マルウェアの送付

これら 5 つの実験からユーザビリティ上の問題点を発見する．

なおマルウェアは 2007 年 5 月 4 日〜2008 年 11 月 30 日の間にハニーポットである Nepenthes[5] によって収集したマルウェアを使用した．

3.2.1 アンチウィルスソフトのインストール

製品によっては，インストール後に再起動し，更新や各種設定を行う．これらの設定は被験者の判断に任せた．製品によっては，サーバと通信する場面があり，中でも“ スパムの学習 ”を行う製品があった．被験者はインジケータが表示されるので，何かをやっていることはわかるが，“ スパムの学習 ”という言葉の意味は理解できなかったと答えた．一部の製品ではインストール開始のボタンが，クリックできるように見えなかったため，“ 終了 ”をクリックしてしまう，という場面もあった．

インストール先の選択，標準インストールかカスタムインストールの選択，更新方法などのインストール時の設定は全てのユーザが初期設定のままであった．これに関しては，下手に設定するのが怖い，という返答であった．

3.2.2 自由に設定させる

10 分ほど時間を設けて，被験者の自由に設定してもらう．全ての被験者が初期設定のままであった．普段の利用状況についての質問でも，アンチウィルスソフトは初期設定のまま利用していると回答した．理由はインストール時と同じで，設定を変更することで不具合が生じた場合，それを元に戻す自信がない，という返答であった．加えて，メイン画面と設定画面での項目が多すぎて，どこで何を設定できるのかわからないという返答も得られた．

3.2.3 自動スキャンの設定

自動スキャンの実行日時を試験監督者が指定する日時に設定してもらう．“ 設定 ”ボタンを探すのに多少手間取ったものの，その後はスムーズに設定できた．しかし，自動スキャンと完全スキャンを統一してほしいという意見があった．自動スキャンは設定された日時に自動でスキャンされることであり，完全スキャンとは全ての領域をスキャンすることで，通常，領域ごとに，自動スキャンするかどうかを設定する．これは，設定画面の構造に何らかの不備があり，被験者が誤解したと考えられる．他には“ 設定 ”ボタンが見にくいという意見があった．

3.2.4 手動スキャンの実行

手動スキャンを実行してもらう．手動スキャンは全ての試験者が実行できたが，スキャンの領域選択で，どの領域をスキャンすればいいのかわからない，という意見があった．この試験者が使った製品が示した領域区分では，システムメモリ，スタートアップオブジェクト，システムリストアなどに分かれており，どの領域がマシンのどの部分を指しているのかわかりにくいという意見であった．

3.2.5 マルウェアの送付

被験者にはアンチウィルスソフトのウインドウを閉じてもらい，指定した文章を入力してもらう．一定時間経ったところで，被験者のマシンに数回に分けてマルウェアを送付し，被験者の反応を観察する．マルウェアが検知されたことをアラームと右下にポップアップメッセージで知らせる製品を利用した被験者は，アラームとメッセージが表示されると，一端作業を止め，メッセージを見るが，すぐに視線を戻し作業に戻った．このような反応は複数の被験者に見ら

れたが，考えていたことには大きな違いが見られた．マルウェアを検知し，それが駆除されたことを理解した被験者もいれば，手動スキャンがされていない，更新されていないことが原因だと誤解した被験者もいた．誤解した被験者に，裏でマルウェアを送付していたことを伝えた後でも，メッセージの内容を理解できないと回答した．

一部の製品では，マルウェアの処理方法についてユーザに問い掛ける方式になっており，ディスプレイ中央に処理方法を選択するためのポップアップウインドウが表示される．この製品を使用した被験者は，ウインドウに表示された処理方法の説明を読んでも理解できず，加えて，選択肢が多すぎたため，何も出来ず，文章入力の作業も中断してしまった．これらはユーザに検知・駆除の結果の通知，または処理方法の問い掛け方と他の 4 つの実験でも見られている，使われている用語の意味がわからないことが原因である．

4　アンチウィルスソフトの改善案

各製品の調査と実験により発見された問題点を以下の 5 つに分ける．次にそれぞれの問題点に対してウェブユーザビリティのガイドライン [6] を参考に改善案を述べる．

- 意味がわからない用語
- クリック可能かわからない
- 設定項目が多すぎる
- どの領域を選択してスキャンするのか
- 検知・処理の伝え方

4.1　意味のわからない用語の問題

セキュリティ製品だから難解で高度な専門用語でも許されるというのは，大きな間違いである．ユーザに情報が伝わらなければ意味がないので，平均的なユーザのレベルに合わせた記述を心がけるべきである．わかりやすい表現に置き換えることが簡単な解決方法だが，置き換えることが難しい専門用語も存在する．その場合は，用語の上にマウスカーソルを載せると説明文が表示される，という方法により用語の意味の理解を助けることが出来る．

4.2　クリック可能かわからない

メイン画面のデザインを重視し，クリック可能なアイテムが目立った表示になっていないという問題点が発見された．また，マウスカーソルを載せると，アンダーバーが表示されたり，背景の色が変わることでクリック可能であることを知らせている製品もあったが，この場合だと，瞬時にクリック可能かどうかの判断ができず，重要なリンクを見落とす原因となる．Web ページでは，リンクにアンダーバーを付けて青字にする手法が一般化しているため，一般ユーザにもわかりやすい．またボタン風のデザインも有効である．しかし，どの手法を採るにしても，製品毎のテーマカラーやデザイン上の理由でふさわしくない場合もあるため，区別できるデザインにする必要があり，一貫性を持たせることが重要となる．

4.3　設定項目が多すぎる

アンチウィルスソフト本来の機能に加え，製品ごとにオプションとして様々な機能が追加されているため，当然，設定項目も増える．逆に，これが一般ユーザの設定意欲を阻害している要因の１つとも言える．単純に設定項目を減らすだけでは，上級ユーザの要求に応えられないため，改善案としては，“ 初級ユーザ ”と“ 上級ユーザ ”とでインタフェースや設定項目の切り替えを可能とする手法を提案する．一般ユーザが変更したいと思っている設定項目のみを“ 初級ユーザ ”の設定項目とすれば，項目数が減り，一般ユーザが容易に設定となり，詳細な設定，またはオプションの機能の設定をしたい場合は，“ 上級ユーザ ”に切り替えるという手法が考えられる．

4.4 どの領域を選択してスキャンするのか

手動スキャンは，利用しているアンチウィルスソフトが対応していない形式のファイルやUSBメモリ，感染疑いのあるドライブに対して行われる．細かな領域の選択は一般ユーザが混乱するので，設定項目と同じく“ 初級ユーザ ”と“ 上級ユーザ ”とで切り替えたときに“ 初級ユーザ ”では，“ PC 全体 ”，“ USB メモリ ”の 2 種類のみにすれば良い．

4.5 検知・処理の伝え方

基本的に，検知されたら自動で駆除する手法に問題はないと思われるが，ユーザに適切に伝えることが重要である．用語の問題と同様，一般ユーザを対象とした文章にするべきである．また，伝え方には，製品によって，目立たないポップアップメッセージや，ディスプレイ中央に大きくウインドウが表示されたり，アラームの有無などの違いがある．どれが望ましいのかは，ユーザの好みがあるため，ユーザ自身が設定する必要がある．各製品でも設定が可能であるが，4.1 での問題点があるため，インストール時の設定に加えることで一般ユーザは容易に設定できる．

5 まとめ

本論文ではアンチウィルスソフトのユーザビリティ上の問題点を発見し，改善案を述べた．ここで挙げた問題点はセキュリティ製品だけに限ったことではなく，医学や法律などの分野でも見られる．よって，他分野でのユーザビリティ改善した例も参考にする必要がある．

今後の課題として，本論文で挙げた改善案を採り入れたプロトタイプを作成し，総括的評価を行うことで，どれだけの改善が見られたか，既存のアンチウィルスソフトと比較することが挙げられる．

参考文献

[1] エフセキュア,“ エフセキュア 2008 下半期データセキュリティ総括 ”, http://www.f-secure.com/export/system/fsgalleries/pr-documents/SecurityReport20082H.pdf, 2008/12/08

[2] Information-technology Promotion Agency (IPA) Japan,“ 情報セキュリティに関する脅威に対する意識調査 (2008 年度第 2 回) ”, http://www.ipa.go.jp/security/fy20/reports/ishiki02/documents/200802_ishiki.pdf, 2009/03

[3] M.Yoshimoto, et al, “ Development and Evaluation of new user interface for security scanner with usability in human interface study ”, LNCS 4658, pp.127–136, 2007

[4] C.Lewis, “ Using the ‘ thinking-along ’ method in cognitive interface design ”, *IBM Research Report RC9265, Feb.1982*

[5] P. Baecher, et al, “ The Nepenthes Platform: An Efficient Approach to Collect Malware ”, 9th International Symposium on Recent Advance in Intrusion Detection (RAID 2006), 2006

[6] Jakob Nielsen, Hoa Loranger, Prioritizing Web Usability, Nielsen Norman Group, 2006