1F-2

「Web ベースのコントロールパネル用セキュリティ診断・設定システム」の提案と課題

祢宜　知孝　　河内　清人　　藤井　誠司*
三菱電機株式会社　情報技術総合研究所†

1. はじめに

本稿では，近年中小企業を中心に利用が活発になってきたホスティングサーバに対し，より簡便に，より確実に運用・管理可能なシステムを提案する．さらに，本システムを実現する上での機能要件と，その課題について述べる．

1.1. 背景

近年の急速な IT 化により，電子商取引が活発に行われている．事実，企業規模に関わらずインターネットやエクストラネットが利用されており，電子商取引は大企業のみならず中小企業にまで波及している．また，個人情報保護法の施行や J-SOX 法の成立，機密情報保護の観点から企業に対してセキュリティ対策が強く求められている．民衆も個人情報に対して非常に神経質になってきており，今や企業規模に関わらずセキュリティ対策が必須となっている．全ての企業は，しっかりとセキュリティ対策を実施しなければ，もはや生き残れない．

このような社会情勢の下，大企業は自前でサーバを設置し，IT 技術に精通したサーバ管理専任者を雇用する事によってセキュリティ対策を確実に実施している．一方，中小企業の中には経済的な理由から，自前でサーバを設置し，IT 技術に精通したサーバ管理先任者を雇用する事ができない企業も存在する[2]．その為，中小企業を中心にホスティングサービスが多く利用されるようになってきた[1]．中小企業に関わらず，大企業でもホスティングサービスを利用する場合がある．そして，ホスティングサービスを利用している中小企業の多くは，比較的パソコンに詳しい社員にサーバの管理を兼務させている．さらには，セキュリティポリシを定めていない中小企業も少なくない．

一方，ホスティングサービス提供会社の大多数は，ホスティングサービスユーザに対して SSH(Secure Shell)や Telnet によるコマンドラインベースのサーバ管理機能の他に，**コントロールパネル(Web ベースのサーバ管理インタフェース)**を提供している．確かに GUI 機能を有したコントロールパネルは，サーバの管理負荷を多少なりとも低減させている．その為，ホスティングサービスユーザは，主にコントロールパネルを用いてサーバを管理・運用している．

1.2. 既存の問題点

しかしながら，本コントロールパネルには下記に挙げる問題が存在する．

1. コントロールパネルを利用するにしても，サーバに関する専門知識が必要である．その為，専門知識の無い管理者が設定作業を行うと設定ミスや設定漏れが発生する．
2. Web ベースである為，リンクを一つ一つ辿りながら目的の管理画面にアクセスする必要がある．一方で，コントロールパネルのリンク関係が非常に複雑であり，目的の管理画面に辿り着く迄に，管理者は非常な労力を要する．

つまりコントロールパネルは，機能性や操作性において十分とは言えない．故に，サーバ管理者は，サーバ上の様々なパラメータを適正に設定・変更をしたり，パラメータが正しく設定されている事を確認したりする為に，専門知識と多大なる労力を必要とする．特に，専属のサーバ管理者を配置できない中小企業にとっては，サーバ管理が非常に大きな負荷となる．

以上で述べた問題点により，ホスティングサーバのパラメータ設定ミスや設定抜けが存在し，外部からの攻撃に弱い脆弱なサーバを用いて電子商取引が執り行われている恐れがある．そこで，本稿ではコントロールパネルから従来よりも簡便にサーバのセキュリティ診断や設定・変更を可能とするシステムを提案し，ホスティングサーバの安全性向上を目指す．

2. システム提案

本章では，以上で述べた問題点を解決する事を目的とした「Web ベースのコントロールパネル用セキュリティ診断・設定システム」を提案する．始めに動作概要を述べる，次にシステム機能要件に関して述べる．

2.1. システム動作概要

図 1は，本システムの動作環境を例示した図である．セキュリティ診断・設定システムは，ホスティングサービスユーザが使用するパソコン上で動作し，インターネットを介してホスティングサービス提供会社が提供するコントロールパネルにアクセスする．セキュリティ診断・設定システムとコントロールパネルとは，VPN や SSL によって接続される．

本節では，本システムの動作を“ホスティングサービスユーザが本システムにセキュリティポリシを入力し，ホスティングサーバの設定・変更を行う”場合を例に述べる．

1. ユーザは，セキュリティポリシやコントロールパネルの URI(Uniform Resource Identifier)，管理者のユーザ ID，パスワードを入力する．
2. 本システムは，セキュリティポリシから設定・変更すべきパラメータとパラメータ値を導出し，ユーザの実行命令を受けてコントロールパネルにアクセスする．
3. 次に本システムは，管理者のユーザ ID とパスワードを用いてコントロールパネルにログインし，コントロールパネルのトップページから順にリンクを辿りながら，該当パラメータを設定・変更するページを探索する．
4. 本システムは，該当パラメータを設定・変更するページを発見すると，パラメータの設定・変更を行う．

Study of the Security Analyzing & Setting System for a Web-based server administration interface

* Tomonori NEGI, Kiyoto KAWAUCHI, and Seiji FUJII
† Mitsubishi Electric Corporation Information Technology R&D Center

5. 本システムは，パラメータの設定・変更を完了するか全てのページにアクセスし終えるまで，ページ探索とパラメータの設定・変更を繰り返す．

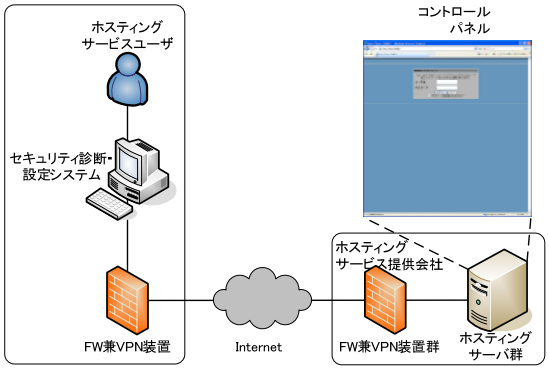

図 1. 動作環境

2.2. システム機能要件

本システムを実現する為には，大きく分けて下記の 2 つの機能を要する．

1. 自然言語で記述されたセキュリティポリシから設定や変更，又は確認すべきパラメータとパラメータに対応するパラメータ値を導出する機能．
2. コントロールパネルのトップページからリンクを辿りながら，該当するパラメータの設定・変更ページやパラメータ値取得ページを見つけ出し，パラメータの設定・変更や取得を行う機能．

上記 2 件の機能要件は，いずれも実現に至るまでに多くの解決すべき課題がある．本システムは，機能要件 2 を実現しなければ，機能要件 1 を実現しても無意味である．その為，以降では機能要件 2 に着目し，詳細を述べる．

3. 実現上の課題

コントロールパネルは，ホスティングサービス提供会社によって構成が全く異なる．さらには，同一のホスティングサービス提供会社であっても，利用するサービスやオプションによってコントロールパネルの構成が異なる．また，コントロールパネルでは，CGI やスクリプトが多用されており，動的に生成されるページが多い．

その為，本システムは，コントロールパネルの構成に依存せず，かつ動的に生成されるページへのリンクをも辿りながら，目的のパラメータ設定・変更ページやパラメータ値取得ページを見つけ出さなければならない．同様の既存技術として，Web ページのリンクを辿る“クローリング技術”が存在する[3]．しかし，既存のクローリング技術は，HTML(Hyper Text Markup Language)で記述された Web ページのコンテンツを一切認識しない．本システムを実現する上では，下記のような Web ページ認識技術が必要であり，その実現方法を検討しなければならない．

1. コントロールパネルの中には，ログイン画面の URI とログイン後の URI が同じ場合や，URI の引数が異なるだけで実質的には同一の Web ページが存在する．しかし，既存のクローリング技術では，Web ページの同異性を認識しない．その為，同じ Web ページに対し何度もアクセスをする事によってページ探索に長時間を要したり，探索が完了したと誤認識する事によってページ探索が途中で終了してしまったりする．従って，ページの同異性を認識する必要がある．
2. 本システムでは，指定されたページを探索し，発見する事が必要不可欠である．しかしながら，既存のクローリング技術は，Web ページのコンテンツを認識しないため，取得した Web ページが何を意味するページであるかを判別できない．その為，何を意味する Web ページであるかを認識する必要がある．
3. 多くの Web ページは，体裁を整える目的で，本来“表”や“リスト”を表現するためのタグ(*<table>* や *<dl>*)が用いられている．だが，既存のクローリング技術は，Web ページ中に“表”や“リスト”などが存在する事を認識しない．一方で，本システムは“表”や“リスト”を認識し，パラメータの設定・変更やパラメータ値の収集をする必要がある．従って，正確に“表”や“リスト”である箇所を抽出し，何の“表”や“リスト”であるかを認識する必要がある．
4. コントロールパネルでは，“プルダウンメニュー”や“ラジオボタン”などに正しい値を設定した上で次ページへアクセスしなければ，不正なデータ設定・削除が生じる．その為，“プルダウンメニュー”や“ラジオボタン”など各フォーム構成要素が何を意味しているかを認識する必要がある．その上で，処理に必要な項目だけを選択し，ページ探索を行う必要がある．
5. ホスティングサービス提供会社毎にコントロールパネルの作りや，使用される用語や言語が異なる．しかし，既存のクローリング技術は，如何なる言語で如何なる内容が記載されているかを判別しない．その為，用語や言語の違いを吸収し，Web ページに如何なる内容が記載されているかを認識した上でページ探索を行う必要がある．
6. コントロールパネルには，システムを停止させる(Shutdown など)ためのページなどアクセスしてはならないページが存在する．しかし既存のクローリング技術は，これらリンク先の Web ページの意味を認識せず，システムの停止などによりページ探索が停止する．その為，リンク先の Web ページの内容を認識し，アクセスの是非を判断する必要がある．

4. おわりに

本稿では，ホスティングサーバの安全性向上を目的とし，従来よりも簡便に Web ベースのサーバ管理インタフェースからサーバのセキュリティ診断や設定・変更を可能とするシステムを提案し，本システムを実現する為に必要な機能要件を挙げた．さらに，機能要件の内，Web ページ探索機能を実現するための課題を列挙した．

今後，我々は本稿で洗い出した課題を一つ一つ解決し，さらには本稿では述べるに至らなかったパラメータ導出機能に関しても検討していく．そして，誰もが容易に利用できるセキュリティ診断・設定システムを実現する予定である．

参考文献

1) IDC Japan:国内通信事業者による iDC サービス市場規模予測(2003),http://www.ciojp.com/contents/?id=00000349;t=30
2) 藤田 佳彦:「不動産賃貸管理業務に対する ASP 用システム」の開発及び実証実験,IPA 中小企業経営効率改善支援ソフトウェア開発・実証事業(2000),http://www.ipa.go.jp/SPC/report/00fy-pro/projects/efficie/005/005.pdf
3) Marc Najork and Allan Heydon:High-Performance Web Crawling(2001),COMPAQ Systems Research Center,