第３分科会

セキュリティ問題とは何か？

～　セキュリティパッチ管理及びその他の問題事例から　～

What is security problem?

~ Security patch management and other problem examples ~

分科会メンバー

主査	田山　晴康	（株式会社日立製作所）
副主査	相原　一博	（株式会社セゾン情報システムズ）
研究員（リーダ）	横井　賢一	（株式会社アスプコミュニケーションズ）
（サブリーダ）	中嶋　寛直	（株式会社セゾン情報システムズ）
	澤中　克之	（東京海上日動システムズ株式会社）
	小川　泰子	（株式会社ＣＩＪ）

概要

情報システムの脆弱性を対策するためのパッチ適用にあたっては、システムへの変更による影響を抑えつつ、迅速な対応を行なうための管理が必要である。本研究では、標準的な管理基準として米国標準技術院（NIST）のパッチ適用基準について学び、日本企業での適用での問題点を探った。また研究の過程で、様々なセキュリティ問題事例についての研究員相互の議論を通して、企業全体でのセキュリティ対策推進の必要性を再認識した。

Abstract

Applying security patches to fix the vulnerability of information system, it needs the appropriate management method for suppressing the influence of change impact by the patches. In this research, with study of the patch application management standard published from U.S. National Institute of Standards and Technology, we explored the problem of applying the NIST management standard in Japanese business field. Moreover, in process of research, we recognized the necessity of whole company's security counter measure through the discussion between the researchers about various security incident issues.

1. 研究課題の選定理由と背景

現在, 情報システムにはネットワーク･インフラストラクチャとして様々なコンポーネント, 例えば，ルータ，ファイヤウォール，スウィッチ，侵入検知システム，サーバ，プリンタ，クライアント, そしてＵＮＩＸ, ＬＩＮＵＸ, Ｗｉｎｄｏｗｓ等多種多様な要素が混在している。

一方，不正アクセス，改ざん，コンピュータウィルス等ソフトウェアの脆弱性を悪用したセキュリティの問題が大きくなっている。2005 年 4 月から，いよいよ，個人情報保護法が施行

され技術面，管理面，運用面でのセキュリティ対策が必須の状況にある。

本分科会では，ネットワークシステム管理業務に従事しているメンバーが日頃悩んでいる問題を出し合い，そこから共通の項目として「PC クライアントのパッチ管理について標準を纏めよう」と考えた。そのため， NIST(米国標準技術院)の文献を参考にしてマイクロソフト社に特化することなくパッチ管理を考えるとともに，日々発生しているソフトウェアの脆弱性やセキュリティ問題について事例学習を行ない，セキュリティ対策への取り組みの必要性について学んだ。

2. 本年度の活動目標

分科会の活動目標を以下のように定めた。

（1）PC クライアントでのパッチ管理のベストプラクティスを提案する。

システム管理の現場では、次々に公開されるパッチの情報を追いかけ適用していかなくてはいけない状況がある。一方、パッチの副作用のために障害が発生し、かといってパッチ検証等で適用を遅らせることでワームに感染してしまう等難しい問題がある。「こういう問題を起こさないための手順はないだろうか」ということから本目標を定めた。

（2）セキュリティ問題をメカニズムや世の中の情報を含めて理解する。

パッチ適用の必要なソフトウェアの脆弱性とはどういうメカニズムで起こるのか。そもそもパッチを適用しないで対応できる方法があるのではないか。そのためには「セキュリティ問題のメカニズムや今起こっていることをテクニカルな面から捉えてみることが重要ではないか」ということから本目標を定めた。

3. 活動内容

目標達成に向けて実施した活動内容を以下に示す。

（1）PC クライアントでのパッチ管理のベストプラクティスを提案

- PC クライアント管理で各メンバーが悩んでいることを討議した。
- NIST の文献 SP800-40（Procedures for Handling Security Patches：米国国家の連邦組織利用のパッチ適用標準）を調べた。
- システム管理者用チェックリストを作成した。

（2）セキュリティ問題のメカニズムや世の中の情報を含めた理解

- 主査を講師として勉強会を行ないセキュリティ問題事例，メカニズムの基本を学習した。
- 学んだことに対するメンバー間の議論、各社での事例を元にした対応方法の議論を通じて、自社でも起こり得るセキュリティ問題をより深く理解した。

4. 研究成果および考察

パッチ管理を行う上で、まずその標準的なものが存在しないかという事を調査した。結果、複数の企業より標準的な文献が公開されている事が判った。その中から、マイクロソフト社の標準についての調査を行ったが、マイクロソフト社の標準は、同社の WindowsＯＳに特化されたもの

であり、それ以外への適用が難しい事が判った。ほか企業の文献についても、同社製品の標準であるという点で同じであった。その後、標準書を再度調査した結果、米国標準技術院(NIST)のSP800-40（米国国家の連邦組織利用のパッチ適用標準）という文献がある事が分かり、同文献の調査を進める事となった。

(１)NIST 標準の概要

NIST SP800-40 には、行うべき事が次の章立てで記載されている。

１．組織におけるハードウェアとソフトウェア資産の作成。
２．新規の脆弱性とそれに対応するセキュリティパッチの識別。
３．パッチ適用の優先づけ。
４．組織固有のパッチデータベースの作成。
５．(資源の許す範囲で)機能と安全性についてパッチをテストする。
６．各地の管理者向けパッチと脆弱性情報の配布。
７．パッチの適用をネットワーク及びホストに対する脆弱性スキャンで検証せよ。
８．脆弱性情報ＤＢの使用方法をシステム管理者に教育。
９．(可能であれば)パッチ適用の自動化。
10．(可能であれば)アプリケーションの自動更新。

それぞれのシステム管理者が行うこと（※分科会にて注目した３項目）

１．ＰＶＧによって指定されたパッチを適用する。
（ＰＶＧ：パッチを管理するための組織をNISTではPVGと呼んでいる。）
２．限定された対象システムでのパッチを試験する。
３．PVGでは監視されていないソフトウェアについても、パッチと脆弱性を情報入手せよ。

4.1. NIST 適用での問題

NIST 標準は英文である為、研究メンバで分担して和訳を行い、その和訳に基づいて疑問点や議論すべきと判断した個所を列挙する方法で議論を進めていった。(「付録１　システム管理者用チェックリスト」を参照)

また、NIST に記載されている方法は原則正しいが、概要の「それぞれのシステム管理者が行うこと」に記載された方法等を日本企業に当てはめようとした場合、事実上できない事もあるという事に気が付く（技術・コスト等々)。その点を下記に箇条書きにて書き出してみた。

①NIST は米国連邦組織を対象としているため、対応する大企業への適用が想定されている。

・日本では、中小企業がベースになる必要がある。システム管理者の人数は少ないが、その人数ですべて見ているのが現状であり、中小企業をベースとしたアプローチ方法が必要。
・テスト環境に、本番システムと同様に形成されたシステムを求められる。
・入手したパッチはベンダー、または信頼ある提供者が提供したものであるかという確認が必要になるが、その手段がない。
・適用後に脆弱性が修正されたかという確認は、非常に専門的で高いスキルが必要になる。

・各ＯＳ、各ネットワーク機器、各ソフト毎とそれぞれ適用方法が異なる為、非常に工数が多くなる。
②月に出る脆弱性情報は 300 件を超える。
・管理者に対して、脆弱性情報を収集し分析することが求められる。
・英語の壁がある。中国語、ロシア語などは手に負えない。
・アンダーグラウンドにしか情報が流れていない場合もある。
・企業として、どこまでの情報収集を必要としているかを決定した上で実施する必要がある。

以上がその例となる。

NIST 標準に記載されている内容は、パッチ管理上「行うべき事」を全て網羅しているものである。全てを行おうとした場合、人・システム等において、多額のコストが発生する事が問題として浮かび上がってしまう。その為、企業が利用するに当たって「行うべき事」に対する「どこまで行うか」という点を、企業のセキュリティポリシーの範囲で決定する必要がでてきてしまう。その事からも、日本企業の現状に即したパッチ管理標準（日本版の NIST 標準）が必要であると考える。

4.2. 議論と勉強会

分科会の中では、議論に必要とする知識や情報を共有する為、多くの時間が勉強会や情報収集の場として利用された。ここでは、議論や勉強会の議題となっていた４項目について、記載する事とした。なお、議論の詳細を全て列挙はできないため、「付録２ セキュリティ問題事例に関する議論での話題一覧」を参照されたい。

代表的な議論
①WEB サイトの脆弱性の議論

WEB サイトは企業の入り口であり、重要な位置づけとなっている。代表的な議論として３例を挙げる。

・ 情報セキュリティ早期警戒パートナーシップ。
・ SQL インジェクション。
・ 組み込み系のセキュリティについての議論。

②組み込み系製品の脆弱性議論

組み込み系とネットワークを組み合わせた製品は、今後世の中に多く広がって行く。その事からも今後は組み込み系のセキュリティが主になってくると想定し、議論した。代表的な議論として次の例をあげる。

・ HDD&DVD ビデオレコーダー事件。

4.3. セキュリティ問題事例の学習によって得たこと

■情報セキュリティ早期警戒パートナーシップ

情報セキュリティ早期警戒体制の拡充、強化の一環として、ソフトウェア製品や Web サイトなどに内在する脆弱性への対応を促進するために、平成 16 年 7 月 7 日に経済産業省から「ソフトウェア等脆弱性関連情報取り扱い基準」が告示され、7 月 8 日より施行された。その実施運用体制として、独立行政法人 情報処理推進機構（IPA）および有限責任中間法人 JPCERT コーディネーションセンター（JPCERT/CC）が指定されている。また IPA からは 7 月 8 日に、この基準に基づく脆弱性取り扱いに関する詳細を記述した「情報セキュリティ早期警戒パートナーシップガイドライン」が公表されている。

この基準およびガイドラインでは、ソフトウェア製品および Web サイトの脆弱性を発見した場合の届け出と対策に関する手順を示している。ソフトウェアを開発販売する企業のみならず、Web サイトを持つ企業全てがこの基準およびガイドラインに沿って対応することが要請されている。その概要を図３－１に示す。

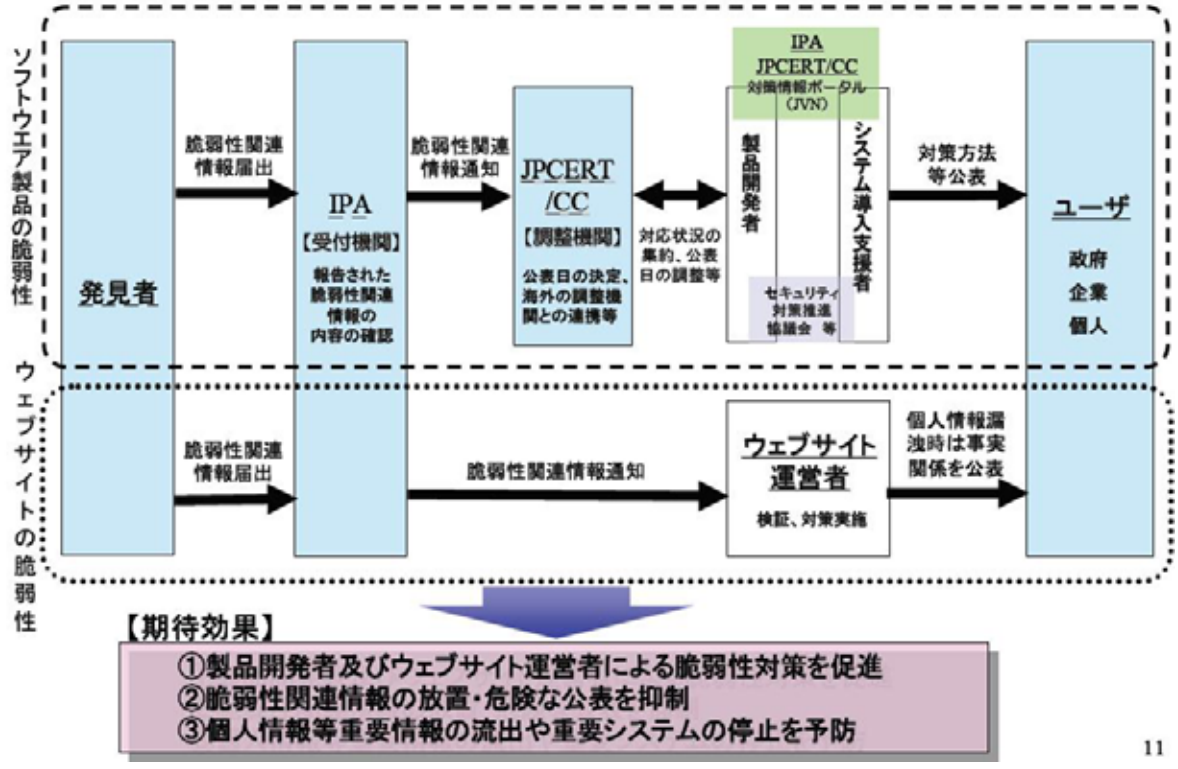

図３－１　情報セキュリティ早期警戒パートナーシップ

出典：経済産業省情報セキュリティ政策室

ソフトウェア等脆弱性関連情報取扱基準とガイドラインの概要説明

この体制により、企業が運営する WEB サイト等に脆弱性が発見された際に通知される事、その通知に対して、どのような対応を打つか等の検討・修正を行い、修正終了等の報告が必要になる事、そして、そのような通知があった際の対応を決めておく等の体制作りも必要であることを知ることが出来た。

なお、当議論を WEB サイトの議論としてピックアップしたのは、個人情報の漏洩は、企業内からの持ち出しだけでなく、WEB サイトからも多いという点からである。各企業は、便利であるはずの WEB サイトが企業の信頼低下に繋がらないように、情報セキュリティ早期警戒パートナーシップによる通知に対する体制作りが必要である。

■SQL インジェクション

SQL インジェクションとは、Web サイトへのリクエストパラメータに SQL 文を与えて SQL データベースを不正に操作する攻撃、またはその攻撃を可能にする入力値未チェックの脆弱性のことを言う。

この手法は、WEB サイトからの情報漏洩原因やリクエスト改ざんの手法として知られている。この手法の知識を得る事で、いかに簡単に情報が漏洩してしまうかという点をしることができた。そのメカニズム事例を図３－２に示す。

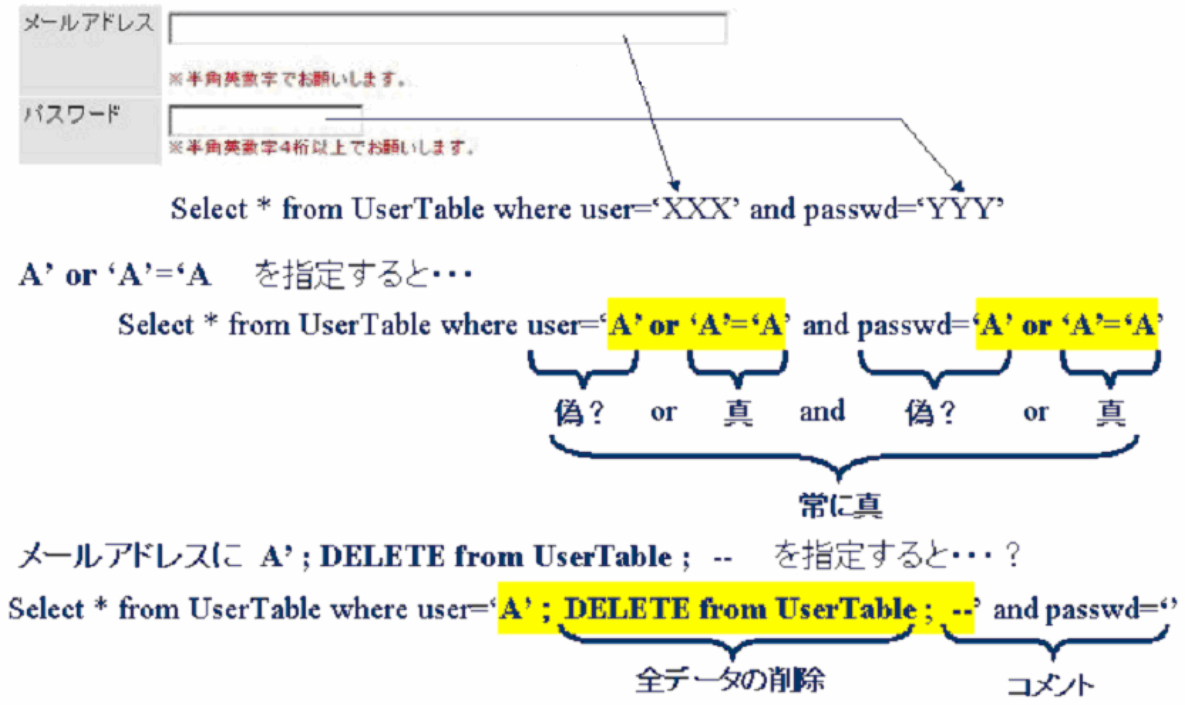

図３－２　SQL インジェクションのメカニズム（認証バイパスの例）

図３－２の例では、入力されたメールアドレスとパスワードが一致するものをデータベースから探し出し、ヒットすれば登録されているものとして処理している。しかし、データベース検索の SQL 文の条件式として合致する形式であれば常に条件が真になるようにすることができるため、入力文字列を工夫することで常にヒットさせることができてしまう。

SQL インジェクション以外にも hidden タグの値を変更する方法やクロスサイトスクリプティング問題によって発生するフィッシング詐欺、あるいはディレクトリトラバーサル等の様々なメカニズムについて学んだ。これらの防御方法としては、入力情報のチェックをサーバサイドで行わせる方法等がもっとも有効となる。JavaScript 等ブラウザ上でのチェックでは、そのチェック

後の情報を改ざんされてしまう危険性があるからだ。WEB アプリケーションを作成する場合は、上記のような点に注意して作成する事が必要になってくる。

■HDD&DVD ビデオレコーダー事件

Web アプリケーションに関する問題は一般的な Web サイトのみで発生すると思われがちであるが、組み込みソフトウェア分野でもセキュリティ問題が発生するようになってきている。ここで取り上げた HDD&DVD ビデオレコーダー事件は、開発元で組み込まれたネットワークの基本機能にセキュリティ的な措置が行われていなかった事から、ネットワーク上の想定外の利用方法により、悪意ある操作の踏み台になってしまったという事件である。その概要を図３－３に示す。

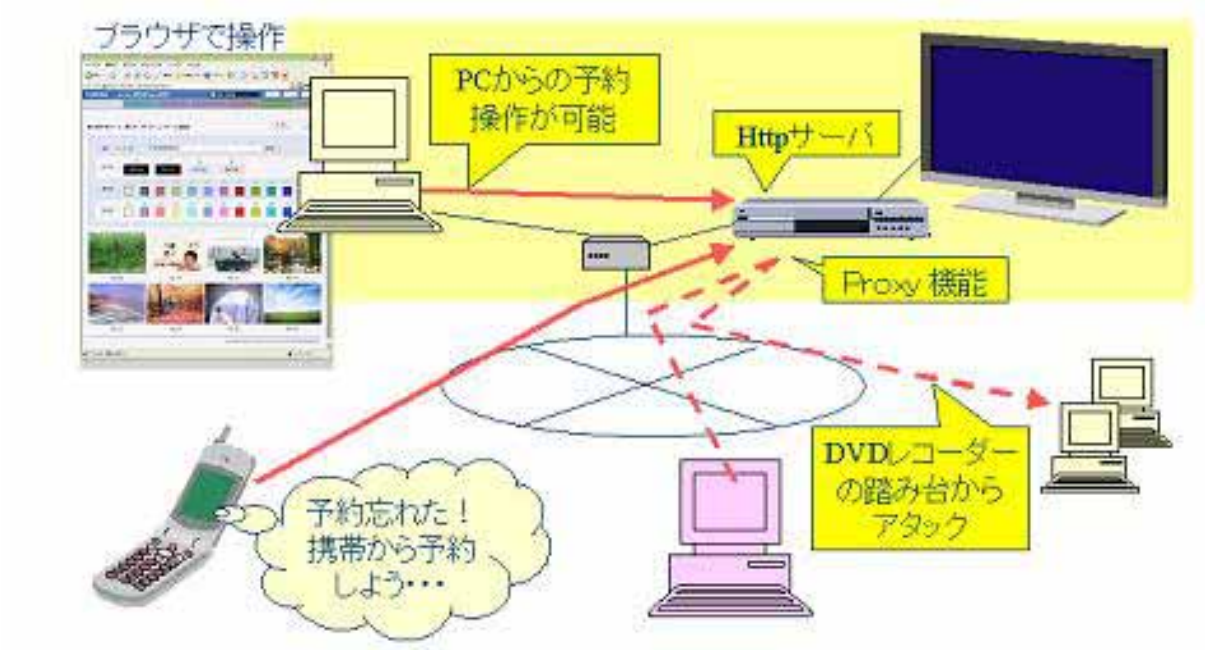

図３－３　HDD&DVD ビデオレコーダー事件の概要

この問題のポイントは以下であると推測される。

(1) メーカーの意図

操作性向上のために、家庭内の PC から操作する機能を追加した。

HDD＆DVD レコーダと PC をネットワーク接続し、PC 上のブラウザからレコーダ上の Web サーバへ接続することで操作ができるようにした。

(2) ユーザによる利用範囲の拡大

ネットワーク経由での操作は家庭内に限られず、インターネットへ接続することで家庭の外から操作が可能になる。

録画予約を忘れていても、携帯電話等でインターネットからレコーダを遠隔操作できる。

（この時点で、メーカーの意図した利用シーンがユーザの手によって拡大した）

(3) レコーダ製品の技術的問題

レコーダ内に組み込まれた Web サーバは録画予約などのリクエストを受けるためにあるが、機能的に不要な Proxy 機能も有効になっていた。

Proxy 機能を利用することで、リクエストをネットワーク上の別の PC や機器に対して中

継させることが可能であった。
利用に関する認証機能にバイパスされるケースがあった。

(4) 悪意の第三者による悪用
インターネット上に繋がったレコーダーへは誰でもがアクセス可能である。
ユーザは自分自身だけが占有的に利用していると思っているので、わずらわしい認証設定等はしない。
レコーダーを踏み台として、インターネット上にある掲示板等に対してスパム書き込み等を行った。

メーカーは、家庭の中で利用する事を想定しており、インターネットに接続される事は想定外であった。

この事件のポイントとしては、「想定利用シーンは変化する」という点と、「脅威の分析が必要である」という２点。特に後者の方は、ネットワークに繋げる事ができるという利便性のみを見ず、ネットワークに接続する事で膨れる脅威をしっかりと見るべきであるという結論になる。

ユーザが自ら、脅威に対する対策「パッチ」を適用するとは思えない。ネットワーク接続という事で想定できる脅威は、現在の PC・ネットワークの脅威と同様だ。その点を考慮してゆく必要がある。

5. 目標の達成度合い

当分科会の研究課題は、クライアント端末のセキュリティ管理における『パッチ管理』をメインテーマにして、パッチ管理における一般的なガイドラインを NIST 標準を元に理解する事を第一目標として活動をしてきた。

結果的に、パッチ管理におけるベストプラクティスを提案するまでに至らなかったのは残念ではあるが、この研究を通じて、パッチ管理については自動化などシステム的な対応を考える以前に、パッチ適用時に、その適用に伴う検証をどのレベルまで実施すべきかの判断が難しく、また適用しない場合でもその理由を明確に整理する必要があるという点から

- 常日頃からセキュリティホールやパッチに関する情報収集が重要
- 考慮すべき内容が多く、その範囲も広いということが一般的

である事を理解出来たのは、非常に有意義であった。

また、特にクライアントＯＳのデファクトスタンダードである Windows についてはパッチの品質の低さによる問題があるといった点を事例研究などを通じて理解を深める事が出来た。

このように、パッチ管理に関して深く掘り下げ理解を深める事が出来たが、それだけにとどまらず、セキュリティ問題の全般的な話題に関して、組み込み機器や家電に関するセキュリティなど今後のトレンドを視野に入れた学習や事例研究などを通じて、各メンバの視野を広げる事が出来た。

その結果、当初の目標であった『セキュリティ問題のメカニズムおよび世の中の情勢に関する理解を深める事』について、十分に達成できたと考える。

6. 反省と今後の課題

各メンバの担当している業務が様々であり、セキュリティに関するスキルレベルも異なっていたため、多くの時間をセキュリティに関する学習や事例紹介に費やしてしまう結果となった。
それ自体は、個々人のスキルアップに繋がったが、研究そのものに費やす時間が限られてしまった事で、幅広い内容の研究課題をテーマとして掲げられなかった事は残念であった。

今回の研究課題である『パッチ管理』については、NIST 標準のガイドラインを主に参考にして研究をしたが、パッチ適用前の検証にかかるロードを考慮すると、ワームやウィルスの発生するスピードに対して､対応が後手に回ってしまう可能性が高いという事が結論として見えてきた。
そのため、パッチ管理にのみフォーカスを当てても、正しい『解』は導けないという事になる。
構成管理・ポリシー管理など含めたクライアント管理全般、あるいは、情報保護の観点から暗号化やドキュメント公開範囲の制限などについて把握するために、より広い意味での『セキュリティ』を研究していく必要があり、その結果、パッチ管理を含めたクライアントのセキュリティ対応の一つの『解』が導き出せるのではないかと考える。
また、クライアント管理のみに着目するのではなく、企業のＬＡＮに対して不正アクセスがある事を前提とした『全社的に影響を与えないネットワーク構成の研究』や、さらに掘り下げて、一般的なユーザが通常の使い方をしても管理できるように、そもそもセキュリティに対する強固なシステムとは何か？といった本質論を研究することを、今後の課題として考えていきたい。

7. 参考文献

(a) 「Procedures for Handling Security Patches」、
Recommendations of the National Institute of Standards and Technology、
Peter Mell and Miles C. Tracy 、
National Institute of Standards and Technology Special Publication 800-40、August 2002
http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf

(b) 経済産業省 ： 告示第 235 号「ソフトウェア等脆弱性関連情報取扱基準」、2004 年 7 月 7 日
http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf

(c) 経済産業省 ： 告示第 236 号、2004 年 7 月 7 日

(d) 独立行政法人 情報処理推進機構(IPA)、有限責任中間法人 JPCERT コーディネーションセンター(JPCERT/CC)、社団法人 電子情報技術産業協会(JEITA)、社団法人 日本パーソナルコンピュータソフトウエア協会(JPSA)、社団法人 情報サービス産業協会(JISA)、特定非営利活動法人 日本ネットワークセキュリティ協会(JNSA) ： 「情報セキュリティ早期警戒パートナーシップガイドライン」、2004 年 7 月 8 日
http://www.ipa.go.jp/security/ciadr/partnership_guide.pdf

(e) JPCERT/CC ： 脆弱性関連情報取扱ガイドライン、2004 年 8 月 25 日
http://www.jpcert.or.jp/vh/guideline.pdf

(f) JEITA-JISA ： 「製品開発ベンダーにおける脆弱性関連情報取扱いに関する体制手順整備のためのガイドライン」、2004 年 10 月 13 日
http://it.jeita.or.jp/infosys/info/0407JEITA-guideline/