第三回 クライアント管理勉強会 議事録

日時: 2012/4/18(水)14:00～17:00

会場: 大阪丸紅ビル 13F E 会議室

テーマ: ここだけは押さえたいクライアント管理

～IT 資産管理と情報セキュリティの第一歩～

講演者: 大阪市立大学大学院 創造都市研究科 都市情報学専攻 博士(後期)課程

「システム管理者の眠れない夜」(技術評論社)著者

柳原 秀基 氏

司会・進行: クライアント管理勉強会座長

PFU ライフエージェンシー株式会社 IT サービス事業部

小玉 稔 氏

当研究会の運営方針により、個人/会社名を特定できる発言、および発表者から公開の許可を得られなかった内容は 議事録より削除されています。あらかじめご了承ください。

◆第1部

講師ご講演

＜第一部、講演の中で質疑応答＞

Q：初期の導入時のキッティングの際にPC型番の標準化やActive Directoryのグループポリシー設定などのルールを決めているところはありますか？

→（約過半数が挙手）

■VNC等のリモートデスクトップ

Q：接続ツールを運用で利用しているところはありますか？

→（3名が挙手）

◆第2部

※柳原氏からのコメントが、右側に記載されております。

Q（M社）：アプリケーションが有償・無償、もしくはフリーウェア等を識別することはできますか？

キッティング後、プリインストールから勝手にインストールされたアプリを把握したいです。

→（柳原氏）：PCをキッティングして渡した時の状態のデータを管理側で持っておく事が必要です。その後の情報との差分を取り分析する、RDP等を用いてアプリケーションの確認を行うことが必要となります。

■PC情報の取得

ソフトの識別はフリーソフトではできません。定期的にデータを取得するのであれば、Active Directory のDomain Controllerログオンスクリプトを使って、psinfo.exe -s のパラメータ指定で実行します。この際、定期的にログオンスクリプトを指定することが必要となります。また、実行するPCのファイル一覧を出力し、過去のデータと現在のソフト一覧を参照して確認をします。CPU負荷は高くありません。ただし、3台を超えてしまうと、負荷かかかってしましますので、ADを構築すべきと提案しています。

→M社：元ベンダーの立場からしても10台からでもADは必要だと感じています。

コメント [HY1]: プリインストールされているアプリに加えて、ユーザが勝手にインストールしたアプリの把握がしたいです。

コメント [HY2]: PC の台数が少ないのであれば､RDP(リモートデスクトップ)

コメント [HY3]: ソフトの識別ができるフリーソフトは無いと思います。

コメント [HY4]: ただ、PC の台数が増えると操作の負荷がどんどん増えてきますので、私は 3 台以上の PC があるのなら AD を構築すべきだと提案しています。

→（小玉氏）：有償ソフトやフリーソフト等の識別は、資産管理メーカで出している辞書などを行うことが必要です。
→柳原氏：「psinfo-s」の注意点として、これは、レジストリのuninstallのキー以下にあるソフトウェア情報を取得するものです。sysinternalsにあるアプリケーション情報は取得できません。
→M社：自社内で用いている資産管理ツールを利用して、ユーザが勝手にアプリケーションをインストールした場合、管理者にアラートが上がるようにしています。
→（小玉氏）：ネットワークの入り口に関しても制御が可能です。USBメモリの利用に関してADであればポリシーで制御ができます。上記の意味を含め、ADの構築運用はクライアント管理上必須です。
→F社：業務上必要なソフトウェアについては、社内で申請をして貰いリスト化します。基本的には申請していないものはブラックリストとして扱っています。
URL:※柳原さんに確認

■ユーザへのシステム利用に関して効果的な周知方法
→（小玉氏）：ユーザへの周知に関しては、社内システムに違反した人を掲示することが効果的です。
→M社：ユーザへの周知を行っていますが、効果がありません。
→（小玉氏）：継続することが重要です。管理職以上のレベルの会議でIT部門からのセキュリティインシデントがあった事を各マネージャに報告し、各部門で問題があった場合は監督責任を持たせ、各マネージャに指導を行わせるようにします。また、情報システム部門だけでなく人事との連携も必要です。
→大槻：社内掲示版上に問題がある人TOP20を掲示して運用している事例があり、結果的に利用者のリテラシーは向上したと聞いております。
→L社：メールなどでの警告では効果が薄いので、違反した時にユーザへ違反内容を記載した紙を配布しています。やはり、物的な証跡を残すことが必要ですね。
→（小玉氏）：ある会社は、違反した際にイエローカードを渡し、一定枚数を超えると罰則をしているところがあります。
→（柳原氏）：証跡を残すことは資産管理ツールを用いて可能ですが、周知徹底するためには人事などを巻き込むことが必要です。情報システム部門としては第一部で紹介したキーログの取得やインベントリ取得を行うなどの積極的にクライアントPCからデータを取得することが必要です。

Q（B社）：アプリケーションの追加と削除に表示されないソフトウェアはクオリティ社の資産管理ツールで取得できますか？
→大槻：下記のソフトウェアなどに関して取得できます。
- ・スタートメニュー登録されているアプリケーション
- ・デスクトップからショートカットで起動するアプリケーション
- ・EXEファイルをパス指定で取得
- ・「*.exe」等の指定をすることで全EXEを取得可能（時間は掛かる）

■不正アクセス等の防止方法
→（小玉氏）：不正アクセスを防止するために、普段からクライアントの情報を蓄積しておく必要があります。かつ、業務用PCはプライバシーがないことを情シスから社員に徹底することが必要です。この前提があれば、ログ取得に抵抗があったとしても、あらゆるログ取得を行おうが苦情などがありません。

コメント [HY5]: Sysinternals のアプリケーションのように、インストーラが無く、単に実行ファイルがあるだけ、というようなアプリケーション情報は取得できません。

→（柳原氏）：ただ、学校は統制が難しいです。
→L社：学内に個人用端末を持ち込み、端末を学内のネットワークに接続しトラブルにもなっています。非常勤講師に関しても同様のトラブルがあります。
→（柳原氏）：学生に対しては難しいかもしれませんが、非常勤講師の方等にPCの持込などに関してリテラシー教育行うことが必要です。
→F社：持込PCの統制をする為に、仮想デスクトップの導入は検討されませんでしたか？
→L社：はい。学内のPCは仮想デスクトップでしか接続できないようにしています。持込のPCなどに関しては、学内ネットワークと別のネットワークに無線で接続させるようにする予定です。

■対外的なセキュリティインシデントが発生した時の対応（座長）
→何も対策を実施していなければ、インシデント発生時に言い訳できませんので、ここまでは対策をしていたということを証明する必要があります。
→Q（M社）：企業規模ごとのセキュリティ対策の水準はありますか？企業規模とのセキュリティ対策を行う水準の判断が難しいです。特に一人で情報システム部門を担当するとなると判断が難しい時があります。
→（小玉氏）：某会社が情報漏洩事件のあとのセキュリティ対策で予算を組む際には、経営トップは、ブランドを守るためと言っていました。同様に、各企業の経営トップが判断したセキュリティ対策の水準により情報システム部門の水準が決まると、上層部に対して告知を行う必要があります。
→F社：経営層に判断させるために、判断出来る材料を情シスから経営トップに掲示し続けることが最も重要です。そして、経営側にセキュリティレベルの判断を任せることが必要です。
→（柳原氏）：情報システム部門はPCの利用者に対して目を配りすぎてしまう部分があるかもしれないです。しかし、その分、経営層に対して社内情報システムの運用状態などについて説明できていない部分もあります。トップは忙しいので、その分情報システム部門が調査し、定期的にITの方針を提示すべきです。（ただし、トップがITに精通してないことは多いので、十分な配慮が必要となります。）

・Q（座長）：定期的に情報を経営層やユーザに情報を提示している企業はありますか？
→（約3/4が挙手）

・Q（座長）：経営に対して情報システム部門の取り組むなどをプレゼンしているところはありますか？
→（1/2くらいが挙手）

・（小玉氏）ある方は、最近の経営者はソフト・ハードの両面で情報システムの安定稼動を求めており、安定稼動を行うための仕組みや手順、予算などを明確にして、セキュリティインシデントが起きている状態をグラフなどで経営者に示すことが必要だと言っていました。世間で情報漏洩事故などのニュースがあると、経営側は、自社は大丈夫かどうか訪ねてきます。そのような時事的な情報漏洩事故などを防ぐために、自社内の状況を把握し、対策を練ることが必要ですし、大変ではありますが、定期的に経営者側、利用者側にエスカレーションを行うことが必要です。

■MSからのライセンス監査について
Q（D社）：MSからライセンス監査の案内が届いた人はいますか？

→（5名が挙手）

→MSの監査を行うとき、ネットワーク側の実たな卸しと紙でのたな卸しを行いましたが、プロダクトIDごとに購入ライセンス数及び利用中のライセンス数を記載する必要があります。また、資産管理ツールを導入しているMSのライセンス監査の証書の項目が細かいため、すぐに記入できない部分もありました。サーバ本体に貼ってあるラベルの番号を取得しなければならず、非常に苦労をしました。初め、2年期限切れのオープンライセンスがでてきたため、ライセンス数が欠落していました。最終的には見つかりましたが、ライセンス証書がなければ追加で購入するところでした。