

第二回 クオリティ製品研究会 議事録

日時: 2011/1/26(水)15:00~18:00

会場: クオリティ(株) 本社 6F 会議室

テーマ: QAW を使って未知の PC を検知/遮断! ~ユーザーより事例講演~

講演者: 日本オフィス・システム株式会社

情報システム 田中 英樹 氏

司会・進行: クオリティ製品研究会 座長

国際興業株式会社 総務部 情報システム課 仲谷 美乃里 氏

クオリティ製品研究会副座長

株式会社シーズ・スリー 情報システムサービスセンター 運用管理ルーム

マネージャー 岡本 宏明 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。

◆Viper 機能の事例紹介

<Viper 導入の背景>

- ・他社システムを導入し検疫ネットワークを作るには、インフラの強化が必要であった(コスト高、数千万単位)
- ・他社システムを導入する場合、DHCP サーバ構築が必要であった
- ・他社システムを導入する場合、クライアントのメモリが 1G 必要であった
 - 結局、他の仕組みだと大きなシステム変更が必要だった→QAW の Viper 機能の採用を決定
 - Viper 環境の構築に約半年かかった

<Viper 機能導入で苦労した点>

- ・環境構築のテストに時間が掛かった
- ・未知/管理台帳の登録に無い機器を判断・確認するのに時間が掛かった
- ・ホワイトリストから削除する際、通信禁止ホストに変更した後、削除する必要があった(機能不十分か?)

<Viper 機能導入のメリット>

- ・構築が低コストであった(通常の 1/3 ぐらいか)
- ・モラルの向上(以前は固定 IP を勝手に割り振り繋いでしまうことが見受けられた等が改善)
- ・QAW をインストールしていない PC がなくなった

◆Viper 機能の事例紹介への質疑応答(回答は田中氏)

Q : 導入はどのぐらいの人員で行ったか?

A : 3 名で行った(PC の配置等は各拠点で)。

Q : ホワイトリスト作成がポイントだと思うが、その後の追加の運用はどうか。

複数の機器管理 DB をマージする際等の苦労があるのではないかと? (PC、他機器等)

A : Notes に全部登録しているので、準備はそれほど大変ではなかった。

Q : 機器を遮断する際の、明確な判断ポイントはどのようにやっているか?

A : まず検知をさせる事により、現状を洗い出すことを先にやった。

一覧が出てくるので、その Notes の ID を許可して行き、不明なもののみ調査をして判断した。

QAW クライアントを自動で許可をする事も出来るが、現場移動をする場合もあるので、

あえて手動管理とした。

Q : ノードサーバは専用の PC を準備したのか？

A : 専用で 2 台ずつ用意した。

Q : アップルトークは？

A : MAC が無いので分からない。

Q : PC 移動や、テストはどうやったのか？

A : セグメントを移った場合、IP アドレスを変更した場合等のチェックをした。

Q : 遮断設定画面で、QAW のホストの期限設定との同期は行えるのか？

A : 現在の機能では難しい。

Q : ノードサーバはどこにおく必要があるのか？

A : セグメント毎に 1 台以上必要。

Q : ノードサーバには QND モジュールは必須か？

A(※事務局) : 必須ではないが、QND モジュールが入っていれば、ノードサーバインストールが容易にできる。

Q : アップル等の PC はどうなるのか？

A (※事務局) : ARP を検知するので、問題ない。

◆ライセンスガード機能紹介(事務局より発表)への質疑応答

Q : 既に用意している辞書以外は登録できるのか？

A : 登録可能。

Q : ライセンスの許諾が変わった場合は？

A : WEB サイト等で公開する予定。

Q : 期限付きのライセンス登録は出来るのか？

A : 可能。

Q : ライセンス管理は、これで利益を生まないという事でなかなか上を説得できない。

何か良い方法はありませんでしょうか？

A : ソフト会社から調査票が届いたということを理由にするのはどうか。

Q : QAW を導入している最中なので、参考にしていただければ・・・

→以前はインベントリ収集ツールは自前ツール使っており、プログラムの追加と削除情報、レジストリのみを NotesDB で管理をしていた。同時使用ライセンス等があると数が合わなかった。

LG 機能はセカンド、フローティング等で役立つと思う。仮想化のライセンス管理には、様々なライセンス管理の考

え方があるので、これが今後の課題である。

Q : ソフトバンク様等、全員 iPad のライセンスが必要になりそう。

A : 現状、インベントリ収集が出来ないので、対象には出来ないが、ニーズはあるので、今後の課題です。

◆お悩み相談・フリーディスカッション

Q : 人間の移動が頻繁にある。スタートアップに QND を入れている。自動的に削除できますか？

A : 可能です。期限付きにして、ネットワークにログオンさせないようにしている。(180 日で)

Q : AT&T をインストールしている PC にリモートコントロールが出来ないようだ。ファイアーウォール設定等は OK にしてあるのだが、なぜだろうか？

A : 過去事例を調査します。(下記、回答)

1. QAW/QND コンソールで対象ホストを選択し、右クリックしてホスト状態を選択します。プロセス一覧の中に acpcd.exe が表示されていることをご確認ください。

(アプリケーションモードで運用している場合は、リモートコントロール欄から、[起動]ボタンをクリックして、[画面の更新]ボタンを押して、acpcd.exe が表示されることをご確認ください)

2. ファイアーウォール設定には、問題ないとのことなのですが、Windows Personal Firewall の他に、AT&T のプログラム側で、ファイアーウォール設定などの機能はございませんでしょうか。

AT&T のプログラム側で、ファイアーウォール設定機能がある場合は、こちらでも例外設定を行っていただく必要がございます。

設定ポートにつきましては、製品 CD 内の Windows ファイアーウォール設定変更.pdf

[3-1. 引数]の項をご参照ください。

Q : Windows 7 に変えた PC に対してリモートコントロールが出来ない。XP SP 3→7 に繋がらない。

繋がっても途中で落ちてしまう状態がある一度落ちると繋がらない場合がある

A : 調査します。(下記、回答)

QAW3.6i/QND9.6i 以降に付属されている Windows ファイアウォール設定変更ツールを使って、状況が変わるかお試しください。

Vista 以降の OS で FW の仕様変更が行われているため、QAW3.6i/QND9.6i 以降に付属されている Windows ファイアウォール設定変更ツールもこの仕様変更に合わせて、機能拡張しております。

Q : リモコンで Ctrl+Alt+Del が効かないのは？

A : Vista と 7 は信号を送っても反応しない仕様になっています。2011 年の 7 月バージョンで対応予定です。

Q : 4 年程前に導入したが、ホスト情報の左側が歯抜けになっているものがある。なぜでしょうか？

A : ハードウェアインベントリを取得していない可能性がある。

以前、QAW 2.7 の際にウイルスワクチンソフトとバッティングして DB が破損する事象があった

Q : 皆様は PC の管理簿のようなものは使っていませんか？

A : QAW、NotesDB (IP)、PC 管理と資産管理の為に AS/400 の 3 つを持っている。

A : MAC や他の機器等の管理もあるので、大変です。皆さんどうやられているのだろうか？

A : Notes の台帳が基本、キッキングの際に INI ファイルを埋め込み、Notes 台帳と紐付け。

今後は QAW を活用して INI ファイル情報収集して紐付けを行う考え。

◆参加者→事務局クオリティへ

- ・フィルタを削除しようとする、「スケジュールが掛かっているから削除できません」となるが、どのスケジュールかが分からない為に削除するのが容易でない。
- ・スケジュールがいっぱいになるので、良く分からなくなる。これが整理できるとうれしい。
- ・スケジュールリストにツリー表示とリスト表示があり、うまく同期しない事があるので、分かりやすくしてほしい。