第三回　クオリティ製品分科会　議事録

日時：　2009/5/27（水）15:00～18:00

会場：　クオリティ(株) 本社 6F Mercury Room

テーマ：　QAW/QND クオリティ社内運用から学ぶ

司会・進行：　クオリティ製品分科会　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

＜第一部＞

QAW/QND 新機能の紹介とロードマップ

発表資料に沿って、以下のアジェンダにて発表、質疑応答

＜発表資料＞

QND/QAW ver9.5/3.5

１．QND/QAW の新機能

１－１．初期展開自動化

１－２．未知の PC 遮断

１－３．初期ポリシー適用

１－４．定期ポリシーチェック 是正・抑止

１－５．管理対象外除外

＜内容についての質疑応答＞

◆　管理対象外 PC において廃棄・倉庫 PC にしたものをレポートツールのようなものはないか

収納されたものを一元管理する事はできるか

⇒レポートはないが倉庫・廃棄 PC は一覧で確認できる。

◆　以前はホスト ID のみの表示だったので一旦削除したものの識別が困難だが

⇒今はコンピュータ名も表示される。

◆　PC 以外の MAC アドレスを管理対象外にできないか？

⇒今のところできない。

QND は SNMP の情報を取得するので、SNMP で通信できたものを管理除外にしてはどうか

Viper コンソールにて該当ノードを通信許可リストに追加することも可能

◆　管理対象外除外について、除外機能でゴミ箱に入った場合、どうやって分かるのか

⇒アラート、自動的に入ってもゴミ箱一覧にその旨が記述される

◆　初期展開自動化で新しいメール QP オプションを再設定できるか

⇒できない。

◆　メール対応 QP オプションを Viper で利用できるか？

⇒できない。

◆　ホワイトリストに登録するのは大変。アドレス体系ではできないか？

⇒今はできない

SNMP でインベントリを取ってもらうのがよい

MAC アドレスでホワイトリストを作成しているユーザあり

クオリティ社内運用

懲罰を目的としたセキュリティ監査ではなくリスクを押さえるのが目的。本当にできているか？

できています！といえることが大事。リスクの把握、見える化⇒社内公開し意識の啓蒙を行っている。

＜発表資料＞

１．監査項目

１－１．禁止ソフトウェアの監査

１－２．セキュリティパッチ適用の監査

１－３．ウイルス対策ソフト更新状況監査

１－４．脆弱性の監査（スクリーンセーバーパスワード）

１－５．脆弱性の監査（ハードディスクパスワード）

２．運用の基本パターン

３．必要工数：ツールを使用する時

４．必要工数：ツールを使用しない時

５．使用するクオリティ製品

６．情報セキュリティポリシ、目的の設定

７．監査方法：禁止ソフトウェア

８．違反ホストへの対応

９．是正確認

１０．運用イメージ：禁止ソフトウェア

１１．禁止ソフトウェア導入状況レポート

１２．導入許可申請

１３．グレイネットアプリケーション一覧

１４．プロセスチャート：禁止ソフトウェア

１５．インベントリ収集のタイミングと設定

１６．監査報告と是正

１７．月次セキュリティ報告書

１８．月別リスク点数推移表

１９．効果

＜内容についての質疑応答＞

◆　監査 PC200 台の監査について、社内全体で 200 台というのは事務部門だけか？開発端末の管理は？

⇒開発 PC は対象外。物理的に分けている。

＜第二部＞
ディスカッション形式による情報共有と課題解決への方策。以下、参加者からのご意見をまとめた内容になります。

【WSUS】
■前回の会議で、WSUS がうまく動かなかったが現在は QND と連携させて動かしている。しかし、強制にはしていなくバルーンをクリックするとインストールするタイプ。強制にしてよいものかどうか？を考えているところ。WSUS は、前回はサーバがうまく立ち上がっていなかったので、MS の WSUS の修正パッチを当てたら動くようになった。

■AD のコンピュータ名登録の際、クライアントの属性をスタンダードにしている。ダウンロードは WSUS から勝手に行われ、次にバルーンが出るタイプ。社内で検証・承認後、事前に案内はしておく。WSUS は IE のバージョン制御にも活用している。

■WSUS 3.0SP3
WIN2000 以降であれば、レジストリの AU の設定が 2,3,4 までしか出来なかったが、現在は 5 という設定が出来ている。(5：インストールは必須だがインストールのタイミングは選べるというもの)
その設定を QND で配布し直した。1 ヶ月は猶予があるが、それを超えると強制インストールがされる設定にしている。

■強制的にやると強制再起動がかかると問題なので、他社はその辺はどうやっているか？
（参加者へ質問）
　強制で WSUS を配布していますか？　⇒強制で配布している会社は 3 社（19 社中）
　WSUS を運用している会社は？　⇒半数以上の会社で運用

■QND でパッチを配布している。パラメータを使っている。WSUS を併用するメリットは、どのようなものがあるか？
⇒QND を使うと必ずインストールされてしまう。つまり再起動が必要なものがある場合は必ず再起動してしまう。WSUS を併用すると、いきなり再起動になってしまうのではなく、大体再起動する時間帯をあらかじめ連絡しておき、以前より運用にのった（クレームが減った）

【運用について】
■QAW
Office2007 を配布していきたいと思っていた。結局、回線上の問題があり QAW を使わずインストールした。OS も様々なので、2007 が入る PC もあれば入らない PC もあり、統一もあまり出来ない状況。

■Mac のインベントリ収集をしてみるがログインがうまく行かない。10.5 だとうまく取れたのだが、それ以前だと取れるマシンと取れないマシンがある。こちらからお願いして実行してもらわないといけないのでちょっと難しい。9.6 での Mac の Push 対応について期待します。

■SIer に初期設定をしてもらい、その後の運用を行っている。ハードウェアインベントリが取れないものがある。スケジュール実行待ちという状態になって、何日も動かなくなっている。サンプルのタスクを流すが全部とれない。スケジュール実行待ちとは何か？
⇒スケジュール実行待ちは、クライアントでスケジュールを受けられる状態になっていない為。

■USB の自動実行の禁止配布をした。Proxy サーバの IP 変更について配布を使ったりしている。
■インベントリ収集はしているが、QIV 台帳の作成をしてみたが、いまいち良いものができない。皆さんがどのように使用しているか知りたい。
⇒QIV の活用事例　次回の宿題

【オフライン PC の管理について】
■半期に 1 度、集約するようにしている。一時的に NW に繋いでもらっている。繋げられないものについては、フロッピーでやり取りをしている。
■QND の収集データ以外は社内規定で暗号化。QND に関しては、特例にして USB で取っている。各部に担当者がいて、その方にお願いして取ってもらっている。
■オフラインの PC については、直接話して電源上げてくれるようにお願いをしている。
■長期出張者の PC など棚卸しはどうやっているか。現在は戻ってきたタイミングで QND を走らせて収集
⇒ダイヤルアップ接続の場合、バックグラウンド実行収集という方法もある。
　ネットワーク接続したときに、ユーザは意識することなくできる。
⇒認めていないソフトの実態が不明な場合はそのソフトをインストールしている PC をネットワークにつながせなくする等。
■モバイル PC が多く、メール対応 QP オプションでやっていたが収集できない場合が結構ある。メールサーバが変わってしまったので、今後どのように変更しようかと考えている。勤怠を入れるときくらいしか社内 LAN に接続しない。
⇒クオリティでは、勤怠の接続時にタスクの実行をしている。ただし通信経路を確保する必要がある。
⇒過去 1 年収集できてないものはネットワークに繋がせないというルール。

【ライセンス管理について】
■ライセンス管理でアプリケーション DB を利用しているが、exe からソフトウェアが読み取れない。
　どのような管理をしているか？
⇒特定のアプリケーションを入れたときに動くプロセス名を管理するのが一番よいかも

■Office の管理をしたいと思っているが、現在 2007 であるが購入ライセンスやアップグレードライセンス等の紐付けなどのライセンス管理についてが一番大変だと思う。

■社内で標準のバージョンが決まっており、MS とのライセンス契約形態により、ダウングレードは OK,UP グレードは買い直す必要が生じる。

■QND サーバは立ち上がっているが、クライアントは展開できていないがこれからやる予定。

PC はリース資産が殆どだが、そうすると棚卸しをしないといけない。

資産棚卸しとして、資産情報と QND の情報が一緒だという事を言ってしまって良いのか？

【プリンタドライバの設定について】

■Notes 上でボタンを作っていて、それを押すとプリンタが追加される仕組み

■あまり考えず、人海戦術でやった。Mac が何台かあったので、WINDOWS のスタートアップに置くようにして毎回送付されるようにした。

■プリンタドライバには各社が提供している補助ツールがあるのでそれと QND を連携して自動設定という手もある。
