D10-3

検疫システムの導入とその効果

内海 太祐, 岡原 武, 福井 宗明、色川雄樹

湘北短期大学 ICT 教育センター
utsumi@shohoku.ac.jp

概要：大規模大学では検疫システムの導入は各部署の独立性が高いため全学への導入は難しい。しかし、中小規模の大学や短期大学であれば必要なセキュリティ要件を満たしたＰＣのみを学内ＬＡＮへ接続許可する検疫システムは大学のセキュリティを確保する上で有効な手段の一つとなりうる。しかし、検疫システムの導入には細心の注意を払わなければ混乱を招くと考えられる。導入までに配慮すべきポイントや必要な調査など、検疫システム導入までの過程を本学の事例を基に報告する。また、導入して１年経った時点での効果についても報告する。

1　導入の背景

湘北短期大学は学生数 1150 名程度、教職員数は常勤 80 名程度、総端末数は 600 台程度の規模の短期大学である。学内 LAN は早くから整備されていたが、2009 年度にネットワークの全面再構築事業を行った。その際に問題になっていた点の一つとして、十分なセキュリティ設定がされていない PC がネットワークに接続されることによる危険性が挙げられていた。

実際に導入準備を進めていた 2008 年 12 月 8 日に USB フラッシュメモリを介してクライアントおよびサーバが大規模感染した。この感染が拡大した理由は学校に常設されている PC とは異なり、ICT 教育センターの管理下にない一部の PC で Windows Update やウィルス対策ソフトの更新処理が適切に実行されていないことにあった。その後、パッチなどのあたっていなかったサーバや教員 PC などに感染が拡大し、事態の収束を見たのは 12 月下旬であった。あと数か月でシステム入れ換えというタイミングでの大規模感染は担当者に対する大きな負担となった。

この時点で検疫システムの導入はすでに決定していたが、学内のセキュリティに対する意識はかなり高まり、導入への障壁はそれ以前より低くなったといえる。

2　検疫システムの特徴と選定

検疫システムは OS のアップデートやセキュリティ対策ソフトの更新など、組織が決めたポリシーを遵守していない端末を組織内のネットワークに直接接続させないシステムである。ポリシーに違反した端末は検疫ネットワークに接続し、強制的にポリシーの遵守を求める場合もある。

このような検疫を行う場合、最も問題になるのはポリシーの策定である。ウィルスに感染し、異常なパケットパターンを出力している端末を「問題あり」としてポリシーに違反すると考える場合がある。これはエージェントレス型と呼ばれるタイプのものである。大学などで導入されるのは主にこのエージェントレス型である。なぜなら、多くの大規模大学では接続される端末がどのようなものであるか仮定することは難しいためである。

このようなエージェントレス型にはもちろん一定の効果があり、何も対策を施さない場合と比べると、危険な端末を接続させない点で優れている。

しかし、エージェントレス型の場合基本的にポリシーの守られていない端末にポリシーを守らせるという動作にはなっていない。ウィルス感染のために学内 LAN へ接続できなくなったモバイル端末でも検疫のかかっていない外部ネットワークへは依然接続できるままになっている。

したがって、より厳密な検疫を行うには端末にエージェントを導入し、端末がポリシーに抵触していないかを検査できるようにする必要がある。しかし、一般的には大学ではエージェント方式の運用は難しい。エージェントの導入作業や接続できなくなった時の対応に追われるため管理者の負担は非常に大きなものとなるからである。

中小規模の大学では大規模大学に比べてより肌理の細かい管理が可能なはずだが、一方で企業ほど接続端末の種類を仮定することは難しく、どのような運用形態が最適であるかはかなり慎重に決めなくてはならない。

3 湘北短期大学内 LAN への導入

湘北短期大学では学内の OA 教室の PC 約 480 台、職員用 PC 約 40 台、及び教員 PC の約半数の 20 台程度は Windows ドメインに所属させることができる。これらの PC にはエージェントを導入し、802.1X 認証と MAC 認証を合わせた強いポリシーの適用をおこなう（タイプ 1)。一部の貸し出しノート PC、ネットカフェ用 PC は Windows ドメインには参加しない Windows 端末であり、MAC 認証とエージェントレス検疫を行っている（タイプ 2)。また、一部 Mac 端末や Linux などの端末、外部から持ち込まれる端末などについては Web 認証とエージェントレス検疫を併用するようになっている（タイプ 3)。タイプ 3 の端末に対しては認証を通過した後も HTTP のみを通す。このため Web インターフェースのシステムを除き、学内の重要なリソースにはアクセスできないようになっている。（表 1）

表 1 学内 LAN にへのアクセス制御

タイプ	主な対象	制御内容
タイプ 1	学内常設 PC（Windows ドメイン参加の OA 教室、教職員 PC など)	・802.1X 認証 ・MAC 認証 ・エージェントレス検疫
タイプ 2	マルチブート端末、研究室 PC など	・MAC 認証 ・エージェントレス検疫
タイプ 3	外部持込み PC	・Web 認証（ID/パスワード認証） ・エージェントレス検疫 ・アクセスセグメントとポートの制限

これを実現するための製品としては ForeScout 社の CounterACT を使用している。この製品は強いポリシー制御からエージェントレス検疫まで対応しているだけでなく、ポリシーに抵触した端末に対するアクションも「隔離」という強い制御以外に、警告を出すだけ、ログをとるだけ、などいくつかのレベルに応じて柔軟な制御ができるためであった。

4 学内への導入の経過

CounterACT の導入を決めたとはいっても、すぐに運用を開始したわけではなかった。まずは全学的な更新を行ったネットワーク環境を安定化させる作業を優先し、CounterACT の運用を 1 年間ほど見合わせていた。

検疫システムについてはそれほど多くの情報があったわけではないのと、その時点では優先順位が高かったためである。実際の導入への検討は 2010 年 5 月に学内ネットワーク運用スタッフの教育からはじめ、2010 年 7 月にログの取得を開始した（図 1)。

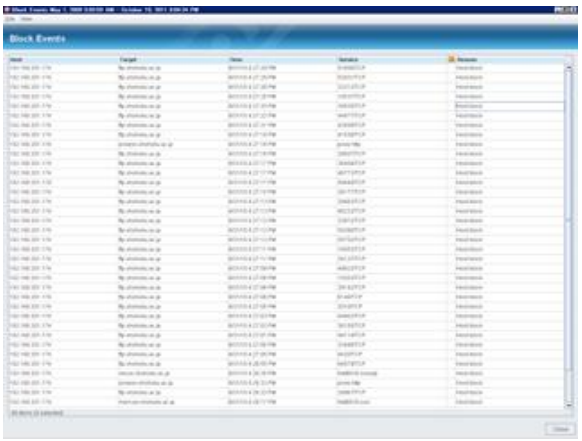

図 1 CounterACT のログ画面

これらのログの解析をもとに、2010 年 10 月に湘北短期大学で必要とされる検疫について検討を重ねた。その結果、当面は隔離という強い制御は行わず、学内のポリシーに抵触した場合には警告を出し、確認ボタンを押した後、2 日間は通信できる、という制御にした。

ログの結果から当初学内ポリシーに違反する端末は 40 以上だったが、検疫の事前周知で 10 程度に減った。これらの周知の下で運用を開始したのは 2010 年 12 月 10 日からである。

実際に運用後から 2011 年 10 月 12 日前後での状況を示す。これは Windows Update を適切にかけていない端末を検出し、警告を出した端末を表す。

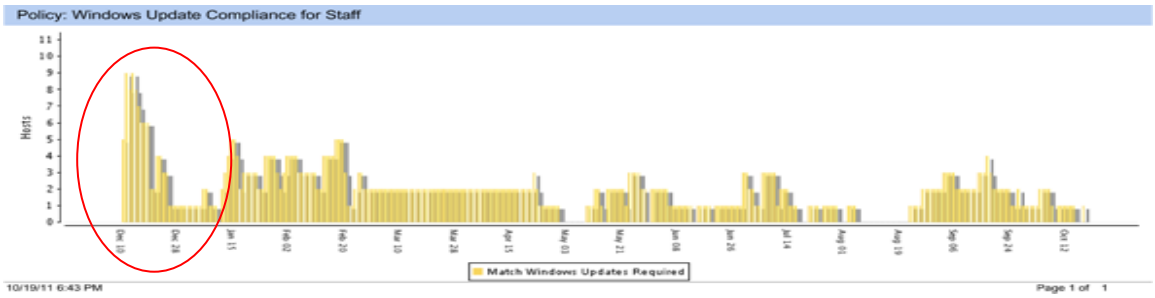

図 2 CounterACT 運用開始後のポリシーに抵触した端末数の推移

これを見ても分かる通り、運用開始時では Windows Update が実行されていない端末数は 10 を切っており、実行開始後 1 台にまで減っている。その後もそれほど多くない数で推移し、2011 年度に入ってからは多くても 4 台程度となっている。

ここまで少なくなっている場合にはそれほど問題にせずに静観するか、長い間 Windows Update を実行していない端末については個別に対応することもできる。

また、導入後大きなセキュリティ上の問題は起こっていない。

4 導入に対する考察

検疫システムの導入はセキュリティの確保に大きな効果をもたらす一方、安易に導入すると運用上のひずみをもたらす可能性がある。

しかし、端末の種類を

1. 情報システム管理部門の直接の管理下にある端末
2. デュアルブートしたり、OS を特定できなかったりするが、ほぼ設置場所の決まっている端末
3. 外部から持ち込まれたりする端末

などのいくつかに分類することにより、中小規模の大学では細かい制御ができると考えられる。また、運用スタッフの検疫に対する知識やスキルの向上も重要な点として挙げられる。

5 今後の課題

最近ではスマートフォンやタブレットなどの新しいタイプのモバイル端末も増えてきている。これらの端末を教育や業務で使用することを推進しようとすると、現在のポリシーや端末の分類では不足してくる。

これらの新しいモバイル端末に対する検疫システムは、ようやく製品が出始めたところと言っても良いだろう。

学内への新しいタイプのモバイル端末の使用推進とセキュリティの確保のバランスは今後の大きな課題の 1 つである。

5 参考文献

参考文献

[1] 佐藤 聡，横山 憲彦，真中 剛司，中井 央，片岸 一起，板野 肯三、「学生宿舎への認証・検疫ネットワークシステムの導入」、情報処理学会研究報告. IOT, [インターネットと運用技術] 2008、72、41-46、2008

[2] 「日経コミュニケーション」、515、30-39、日経 BP、2008