

# パッチマネジメント ソリューション

アウトソーシングビジネスユニット  
インフラ構築センター

平瀬 謙次



## 1. はじめに

数年前まで、各企業のシステム管理者は、外部からのアタックやウイルス対策にフォーカスを当て、ファイアウォールやゲートウェイ型のウイルス対策ソフトを導入していた。社外とのネットワーク上の境界線にセキュリティ対策を実施すれば十分であると考えたのである。

しかし、ある時期よりクライアントPCでのセキュリティ対策も重要であると考えられるようになった。そのきっかけは、2003年8月に世界中でMSBlaster\*1が蔓延したことにある。

日本でも多数の企業が感染して、その影響で混乱が生じ、最悪の場合業務が停止するという被害にあった。ある企業では、その駆除に追われ、完全に復旧するまでに1週間以上を要したという。その損失（営業機会損失を含む）は、多大なものだったのではないだろうか。

それ以前にも、セキュリティホール情報の情報や、それに対するパッチもリリースされていたが、タイムリーに適用していた企業のほうが少数派であった。Blasterの蔓延をきっかけに、システム管理者はセキュリティパッチの適用の重要性に気づき、多くの工数をかけ自社の穴を塞ぐために日々努力している。

しかし、情報システム部門の本来の業務はこのような作業ではなく、経営企画部門と連携し企業のIT戦略立案を実現することだ。パッチ適用に時間をとられている場合ではない。では、それを解決するにはどうしたらよいか？

そうした考えから「パッチマネジメント ソリューション」を開発した。本ソリューションの導入により、顧客は、本来の業務に注力可能となり、CACは、顧客内に深耕し、かつ長い付き合いをさせていただくチャンスが生まれる。それ以外の案件の掘り起こしにも有用となり、とまさにWIN-WINの関係を築くことができると考える。

## 2. マイクロソフトの考え方

Windows XP SP2がリリースされた時、パーソナルファイアウォールの実装等によるセキュリティ強化が多く行われた。そのためにネットワークを介すさまざまなアプリケーションが稼動しなくなったことは記憶に新しい。これについてマイクロソフト社は、「今までのOSは利便性を最重要と考え追求してきたものであったが、今後はセキュリティをより強固なものとし利便性よりも優先し、セキュリティを確保するための設計を行っていく」としている。つい先日リリースされた Windows Server 2003 SP1も今まで以上に強固なセキュリティを実装したものである。

マイクロソフトに限らず、業界の目はセキュリティに強く向けられていると判断して良いだろう。

## 3. 各企業でのパッチ適用の実情

MSBlasterやNet SKYなどが蔓延したときには、セキュリティホール情報がすでに公開され、セキュリティパッチもリリースされていた。これらのワームは、セキュリティ

\*1) MSBlasterは、それ以前のウイルスやワームのような、クライアントPC上でウイルスプログラム（たとえば、メールに添付されたプログラムやスクリプト）を実行しなければ感染しないタイプと異なり、OSのセキュリティホールを利用してネットワークに入り込み、セキュリティパッチを適用していないPCに次々と感染させてしまうタイプのワームである。



### 5.1 パッチマネジメントプロセス整備支援サービス

パッチを適用する際の問題点を解決するには、何をどうすればよいか。

システム管理者たちは、毎月1回とはいえ、パッチの適用を行わなければならない。パッチがリリースされる度に、前月の展開方法は？前月の適用率は？前回出たエラーは？と、作業記録簿やメール等を引っ張り出してから計画を立て、四苦八苦しながら展開しているのが実情だ。通常の業務に加え、それまで行ってこなかったこれらの作業は、かなりの負荷になるだろう。それを軽減するためには、プロセスを定型化して実施するのが得策である。

プロセス整備支援サービスでは、現状のパッチマネジメントプロセスをヒアリングし、ITILのベストプラクティスと照らし合わせて分析を行い、強みと弱みをはっきりさせ顧客に提示する。同時に、短期的・中長期的な改善点を提示する。これにより、各顧客に適合した提案活動に結びつけることが可能となる。

パッチ適用を実施していくためには、プロセスをきちんと定型化し、かつ効率良く継続的に実施していくことが重要である(図3)。「パッチマネジメントプロセス整備支援サービス」は、その解決策として非常に有用である。

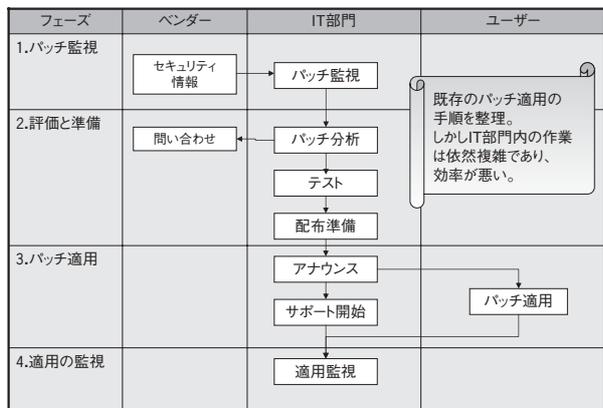


図3 プロセス化されたパッチマネジメント

### 5.2 パッチマネジメントシステム構築サービス

さて、プロセスが定型化されたら、次はプロセス終了までの期間を短縮し、かつ完璧なものを目指していきたい。定型化されたプロセスでも実際には人の手が多く介入している。このシステム構築サービス導入の目的は、ツールの使用を促し、人の介入を最小限にすることにある。また、前述した2つの前提条件に関しても、本サービスで提供することも可能である。

たとえば、クライアントのインベントリ情報を収集するために、毎月クライアントPCの棚卸を実施するわけにはいかないし、パッチの展開作業のために、毎日パッチの適用の実施に支店や事業所を回って全国行脚を繰り返すわけ

にもいかない。きちんとパッチが適用されたか、社内すべてのPCを確認して回るわけにもいかないだろう。それを解決するために、ツールの実装を提供する。

マイクロソフト社のSUS+MBSAの組み合わせであれば、最小限のコストで、パッチの配布と展開の確認が実施可能となるし、クオリティ社のQNDであれば、上記機能に加え管理者権限の問題もクリアされる。加えて、クライアントPCのハードウェア、およびソフトウェアのインベントリ情報までも収集することが可能となる(図4)。

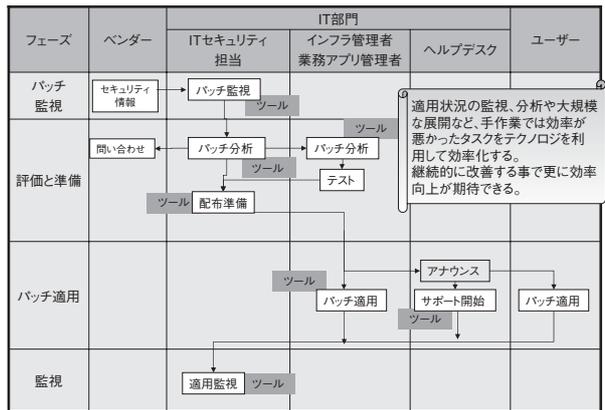


図4 ツール導入後のパッチマネジメント

このように、ベンダーにとらわれずに、顧客の要望に沿ったシステムを提案し、構築できることが当社の強みといえるであろう。

また、同様な要件の場合は横展開が容易なことも本サービスの特徴といえる。

### 5.3 パッチマネジメントシステム運用サービス

プロセスが定型化され、システムの構築が行われたら、その後は、システムを運用していかなければならない。

そこで、CACの運用要員が顧客のシステムを運用していく「パッチマネジメントシステム運用サービス」の導入を提案したい。

たとえば、購読というタスクでは、当社要員が顧客に代わって日々さまざまなソースから情報を収集する。多数の顧客で運用を手がけるCACには、さまざまなセキュリティ情報が集約される。その中から各顧客のベースラインに関係するものを適宜案内することが可能だ。

また、ベースラインが同じ企業があれば、関連性評価や、リリースの開発も1社分の作業工数で数社をまかなうことができる。展開に関しても、定型的部分を横展開することで安価に提供でき、作業時間の短縮も図れる。本サービスを導入することによる展開期間の短縮は、計り知れないメリットだろう。

以上3つのサービスが組合わさった「パッチ管理メ

トソリューション」の導入は、顧客側担当者にとり、本業をおろそかにすることなく、短期間で、かつ的確に全社のクライアントPCに対しパッチの適用を実施することを可能とするのである。

## 6. ターゲット顧客

本サービスのターゲット顧客は、拠点数が10拠点程度、クライアントPCの数にして1,000台規模が適切であると考えられる。なぜなら、このような規模の企業では、情報システム部門は10人程度で構成されており、インフラ、基幹システム、業務アプリケーション等を、各個人が複数担当しており、日々の運用で多忙となり、システムの改修まで手が回らないことが多い。そのため、運用していく中で、多くのシステム構築、アプリケーション開発という案件が掘り起こされる可能性も多い。

## 7. 他ソリューションとの組み合わせ

クライアントPCに関連するソリューションとして、「PCホスティングサービス」がある。以下にサービス内容を紹介する。

各企業のクライアントPCの使用形態には、次の2パターンがある。1つは、PCを資産として購入・管理・使用するケース、もう1つは、リース会社と契約し、料金を支払いながらPCを使用するケース。どちらのケースでも、誰がどこの拠点でいつから使用しているのか、今月のリース代金はいくらなのか、等の管理業務、また故障時の修理対応やヘルプデスク等の業務が付随してくる。企業では、これらの煩雑な業務に多大な時間がかかっており、これはクライアントPCの数が増加すればするほど、業務として

大きな負担となる。

その負担を解消するために、OS、MSOffice、業務アプリケーション等の設定を施したPCを月額使用料のみで貸し出す、それが「PCホスティングサービス」である。PCが故障した際には、故障受付、代替機の準備と発送、ベンダーとの調整、修理対応等も実施する。さらに、インベントリ情報の管理や、企業内ヘルプデスクサービス、オンラインの修理対応であるデスクトップサービスもオプションとして提供する。

故障時の修理対応等、予算化できない経費の発生はどの企業でも歓迎できないと思うが、本サービスは、PC1台当たりいくら、という定額料金で利用でき、ユーザーにとっては変動費化できる点を特徴として挙げられる。

こうして、「セキュリティパッチマネジメントソリューション」と「PCホスティングサービス」の2つのソリューションを併せて導入した場合には、クライアントPCに関する煩雑な作業がすべてアウトソースできるため、情報システム要員は本来の業務に注力することが可能になる。

## 8. 終わりに

パッチ適用やクライアントPCの管理については、どの企業でもいろいろな道を模索している段階で、何かをやらなければならないという意識がある。ここで紹介したパッチマネジメントソリューションのうち、その部分的なサービスを提供するベンダーは数多いが、当社のような包括的サービスを提供している会社は多くはない。CACとしては、各顧客の情報システム要員の方々が本来の業務に注力する事ができるように、本ソリューションを推進していきたいと考えている。