CISO STRATEGY

企業のリスクをマネージする戦略考

ネットワークやシステムの管理作業のオーバーヘッドを軽減するために、これまで種々の管理ツールが開発されてきた。しかし、たとえばネットワーク管理を考えてみると、いまだに熟練管理者が使うツールはping、traceroute、telnetが主流である。これではいつまでたっても管理ツールは普及しない。一方で、管理ツールが必要とされ、実際に管理作業に使われている環境も登場してきている。管理ツールの導入の成功の秘訣はどこにあるのか。

第十一回 管理ツールの高度化

text : 山口英 奈良先端科学技術大学院大学情報科学研究科教授

UNIX系ツールを使いこなす「腕」

ネットワーク管理者が使用する管理ツールには三種の神器がある。それはUNIX系OSで用意されているping、traceroute、telnetである。これらのツールのうち、traceroutだけが多少新しく、10年ほど前にリリースされたものだが、それ以外は4.3BSD時代（1990年頃）から長い間使われてきたツールである。UNIXのネットワーク管理を学んだユーザーであれば、誰もがこの3つのツールについては自由自在に使いこなせるようになっているに違いない。

というのも、そのくらい誰もが利用し、また、誰もが後進に管理者としての使い方を教授してきたツールだからだ。

その特徴は、現在さまざまなサービスを提供する管理ツール（システム）と比較すると、極めて単純なツールとして開発されている点にある。もともとUNIXは、単機能の単純なツールをいくつも用意し、シェルスクリプト等で複数のツールを組み合わせ、より高度なツールを各利用者が目的に応じて作り上げていくようなシステム環境として構築されている。

このようなシステム設計になった理由はいろいろあるが、最大の理由はプログラマーが使って十分に納得して満足できるプログラム開発環境であるようにと開発されたOSであるからだ。つまり、UNIXを使いこなすユーザーであれば、当然プログラミング能力を備えていると仮定していたと言えよう。そのため、各ツールをシェルスクリプトで組み合わせて利用するのは当然のこととしても誰も困らなかったのである。このことは、ある1つの事実を浮き彫りにする。

UNIXのツールを100パーセント使いこなすためには、実はプログラマーとしての素養を持ち、それを日々の業務の中で実践することが必要なのである。その意味では、UNIXの標準ツールは、使いこなすのにはそれなりの「腕」が必要であるということなのである。

大抵のネットワーク管理者は、ping、traceroute、telnetを使うことができるが、しかしツールの使い方も人によって千差万別である。また、同じ使い方をしているように見えても、ツールの実行結果から得ている情報とその解釈が管理者ごとに大きく異なるような状況もよく目の当たりにする。このことからも、UNIX系ツールの多くは、使う人の技量によって効力が左右されると言っても言い過ぎではない。

なぜツールを使うのか

さて、なぜシステム管理で私たちはツールを使うのか。これは、システム管理の品質アップと大きく関係している。

1つの理由は、管理作業の効率化である。もともとツールは、同じことを何度も繰り返したり、あるいは、いくつものツールを使った手間のかかる作業を一度に処理したりするために利用とするのである。ツールを使うことによって、管理者は1つの作業にかかる時間を短縮でき、ひいては管理作業の品質を高めることができる。

たとえば、自分の管理環境に同じベンダーから供給されたルーターが30台あったとしよう。フィルタリングの設定を30台すべて設定しなければいけないとしたら、あなたはどのようにするだろうか。30台のルーターにtelnetを使って順

次アクセスし、手作業で設定ファイルを書き換えるだろうか。しかし、大抵はツールを使ったり、ちょっとしたシェルプログラムを書いて対応したりするのが普通だろう。このように、ツールを使うことで、作業時間を短縮させるだけではなく作業で単純ミスを避ける効能もある。

もう1つの理由は、管理作業において、その経験を継承するためにツールを利用するということである。ソースコードが提供されている管理ツールの場合、そのツールを作った人が何を考えて、どのように問題解決に至ったかを紐解くことができる。言い換えると、このようなツールの中味を学ぶことで、先人たちが行ってきた管理作業を直接学ぶことができるのである。

実際、筆者自身の経験でも、システム管理用には多くのシェルスクリプトやPerlプログラムを用意し、それらを使ってアカウント管理やネットワーク管理を行うようにしている。そして、実際にこのようなスクリプトを用意することで、同じシステムを共用している他のユーザーに、私が管理作業で何を行っているかが理解できるような糸口を与えているとも言えよう。

特に長年運用してきたシステムともなると、大変昔から継承されてきたツールが必ず1つや2つは存在するだろう。

誰もが使えるツールの重要性

ところが、現在のインターネット管理は、必ずしもプログラミングの素養がある人たちばかりが行っているわけではない。むしろ最近では、商用インターネットの基盤環境の急速な広がりによって、どちらかといえばソフトウェア開発の経験も素養もないネットワーク管理専業の管理者がネットワーク管理業務作業を行っていると言ってもよいだろう。

このような人たちがネットワーク管理作業に携わった場合、既存のツールを使って効率的な管理作業を行うことはできるものの、ツールのソースコードから管理作業の中味を理解して継承することはできない。特に、古いツールを使っている場合には、そのツールがなぜ作られたのかも忘れ去られてしまうし、さらにはツールのメインテナンスに支障をきたしてしまうことも間違いない。

このため、いくら先人たちが優秀なツールを作って継承していたとしても、ネットワーク管理作業に携わる素人であっても使いこなせるツールを使うようにしているケースが、現在ではほとんどだ。

そして各管理者の前提知識や能力に関係なく、管理作業を効率よく行い、さらには何らかの形で経験を継承できるようにしようとする企業や組織が増えてきている。

戦略1 ネットワーク管理ツールは、最近は誰もが使えるツールを基盤にして活動・展開することが重要だ。これにより、ツールを使った効率的な管理作業が可能で、同時に、管理者同士での経験の継承にも役立つ。

もう1つ重要なのが、使用しているツールのメインテナンス作業も同時に行うことだ。特に古い環境で稼働していたツールについては注意が必要である。もしも自分が開発したツールであるのならば、OSのバージョンアップやネットワーク構成の変化によってツールが使えなくなるような状態を極力避けて、メインテナンス作業を行わなければならない。

また、新しいツールに対して機能を継承させようとするならば、新しいツールに機能を移植しなければならない。

戦略2 使用しているツールについては、できる限りきちんとメインテナンスを実行する。場合によっては、誰もが使えるツールあるいはプラットフォームへの移植も検討する。

自動化は福音となるか？

かなり強力な管理ツールを使い始めると、いろいろな管理作業を自動化しようとする試みを誰もが一度は経験すると言ってよい。ところがこれにはいろいろな落とし穴が潜んでいる。

自動化の最大の問題点は、設計あるいは期待どおりに作業の自動化が行われているように見えて、実際には大きなトラブルを発生させてしまうことがあるという点だ。そして、それは結構見つけにくいことなのである。

10年ほど前、私のスタッフがUNIXサーバーの管理作業の自動化で起こったできごとを紹介しよう。

その当時、システムの規模は現在のシステムとは比べ物にならないくらい小さなものであった。とは言うもののシステムのバックアップはそれなりに大変な作業であった。特に、テープなどへのバックアップは時間もかかり、その作業自体が忍耐を必要とするものであった。

さて、筆者たちが当時利用していたサーバーは、私のオフィスのスタッフのA君が作業をしていた。彼はサーバーのバックアップ作業を任されていたのだが、ある日バックアップを自動化するツールを作ったというので、早速使い始めることにした。

彼の計画では、家に帰る前にテープをセットすれば次の日の朝には安全な形でバックアップが行われているというものであった。

このシステムも彼がプライベートに作ったプログラムであったので、大したコードレビュー（コード検査）もしないで運用に入ってしまった。しかし、ここに大きな落とし穴があったのだ。

実は、このプログラムは24時間に一度決められた時刻に単純にバックアップを作るようなものであったので、テープ

は、必ずA君が毎日入れ替えなければならなかった。

しかし、ある日、A君が大騒ぎして私のところにやって来た。

「先生、バックアップテープが壊れてしまいました」。

バックアップ作業中にシステムがクラッシュしたのだ。さらに最悪なことに、A君は前日にテープの交換をし忘れていた。このため、前日のバックアップテープがそのまま使われた。前日のバックアップデータはすべて廃棄され、改めて今日のバックアップを始めたのだ。そして、バックアップ作業中にシステムがクラッシュしてしまったので、このバックアップテープの内容は不完全なものになってしまったのである。

この実際にあった話から見出せる問題点は次のとおりである。

(1)テープの入れ替えをA君が自分自身で行う方法をとっていたにもかかわらず、人的ミスへの対応が考えられていなかったこと。
(2)実際にシステムを動かすまでのテスト段階で、この問題を発見できなかったこと。
(3)仮に単一のエラーを発生させてしまっても、そこから問題なく復旧することができる代替手段を確保してなかったこと。

このようなことから、管理作業の自動化をするのであれば、本当にスモールスタート、つまり、さまざまなチェックを事前に試めせる小さな規模でスタートするのが一番よいだろう。

そして十分に慎重な「設計」「実装」「テスト」を行い、さらに運用状態になったら、最初はさまざまなテストをして正しく動いているかどうかを何度も確認するほうがよいだろう。

戦略3 管理作業の自動化は、相当慎重に行ったほうがよい。仮に管理作業を自動化しなければならないのであれば、そのシステムの「設計」「実装」「テスト」「運用」の各フェーズで誰かが責任を持ち、徹底してトラブルを排除することが必要である。

成長するツールに知見が集約

また、ヒューレット・パッカード社のOpenViewのような大規模なネットワーク管理ツールを使った場合、何人もの管理者が協力し合って、ツールそのものをどんどん成長させるという共通の目的をもって取り組んでいってもよいだろう。

たとえばOpenViewであれば、ネットワークの構成機器とSNMP(Simple Network Management Protocol)というネットワーク監視・制御用プロトコルで通信することで、ネットワーク内の機器の状態を把握する。OpenViewを導入すると、最初はすべてのネットワーク機器とSNMPで通信ができ、次に、ネットワーク機器をネットワーク構成(トポロジー)図として表示するところまでは必ずできるだろう。

しかし、OpenViewが本当の力を見せるのは、さらに管理者が念入りな設定をし始めたときである。たとえば、特定のネットワーク機器にSNMPとSNMP trap発生条件を設定し、特定の回線がダウンしたならば、即座に携帯電話にメールを送って管理者に注意を促すような仕組みも作れる。OpenViewの場合、その設定も管理者がOpenViewを正しく学べば可能となる。

このように、管理ツールも単純に通り一遍の設定だけではなく、管理者が管理ツールをしっかりと学び、そして設定を行っていくことで、さまざまな機能を実装できる。その意味では、成長するツールとしてシステムあるいはネットワーク管理ツールと付き合っていくほうが、長期間にわたる知見の蓄積が可能となることも多い。

戦略4 ツール自体が長い時間の中で成長するようなものの場合、うまく使うことでツール上に知見の集約が可能となる

セキュリティー管理で使うツール

さて、この連載の本題である「セキュリティー管理」であるが、以前は比較的手作業による管理作業が大半であったが、最近は少しずつツールを使いながら作業を進めることができる。

1つは最近のアカウント管理のように、単純にコンピュータのログインアカウントだけでなく多種多様な作業が含まれるようになったものでは、ツールを積極的に使うようなっている。

たとえば組織内ポータルでのアカウント管理を考えてみれば、ICカードが認証システムと連携して本人確認を行う手続きが入り、さらにはネットワーク環境に対するログインと経路設定を端末ごとに行うというような処理が発生することも十分考えられる。このような一連の処理をいちいち手作業で行うのは大変な手間がかかってしまう。そのため、ツールを用意して一連の作業を漏れなく行うシステムにしているところも多い。

2つ目に利用頻度の多いツールは、ファイアーウォールやIDS(Intrusion Detection System、侵入検知システム)などのセキュリティー製品に付属するデータ解析ツールや、セキュリティーポリシー設定ツールなどであろう。

これらは、高度な機能を持ったネットワークシステムの機能を補助するソフトウェアとして開発されていることが多い。

3つ目は、ネットワーク管理ツールと一体になって、不正アクセスやDoS(Denial of Service、サービス妨害)攻

撃などを検知して管理者に通知するシステムである。

これはIDSとは多少異なり、従来のSNMPを基盤としたネットワーク管理システム上に構築され、特別なポートへのアクセスや、閾(しきい)値を超えたトラフィックの受信などを検知する機構になっている。

この機構は、ネットワーク管理のプラットフォームを積極的にセキュリティー管理に利用しようというものだ。

これは、これまでも多くのネットワーク管理者に実行されてきた方法で、特に、既存のネットワーク管理ソフトウェアとの相性がよく、導入コストが低いということで、多くの企業や組織でこの方法が使われている。

整合性を確認するツールはない

ところが、セキュリティー管理では、現時点でツールではどうしてもできないことがある。

大規模なネットワーク管理において、特にセキュリティー面での設定が「セキュリティーポリシーに照らし合わせてみて整合性があるかどうかを検証する作業」がある。

たとえば、管理対象のネットワークに30台のルーターがあったとしよう。ここで、30台のルーターには、セキュリティー管理の立場から、さまざまなパケットフィルターが設定されているとする。この場合、30台のルーターに設定されているパケットフィルターが、セキュリティーポリシーと整合性を保ちながら、矛盾がないように設定されているかどうかを検証したいと思うことはよくあることだ。

しかし、現時点ではセキュリティーポリシーとの整合性を確認するためのツールは存在しない。

より高度なツールに期待

さらに現時点では実現できていないが、研究開発が続けられているツールもある。

たとえば、source IP addressを偽装した分散型DoS攻撃が発生した場合に、そのDoSトラフィックが生成されたホストを発見する「IP trace-back」いう技術があるが、これを実現するツールはいまだ現れない。

また、シンプルかつ非常に強力なユーザー認証の方式も長年検討されてきたが、本当の意味で問題可決を果たしたツールは登場していない。

このようなことから、まだまだネットワークが絡んだ分散型情報処理システムに対しては、有効性の高いツールが何でも提供されているわけではないのだ。

緊急対応でのツール利用も

なんらかのセキュリティートラブルが発生したときに、利用すると役立つツールもいくつか存在している。

緊急対応時に必要なことの1つに、実施した作業の内容についての記録を作成することがある。これは、特に大規模なトラブルになればなるほど、複数のチームが分散して緊急対応に携わることになるが、記録は正確に残しておかなければならない。

そこで、「トラブルチケットシステム」あるいは「クレームトラッキングシステム」というツールを使うと、観測された事象とその対応を順次記録していくことができる。

機能集約型のツールが魅力

今回は、ネットワーク管理と、特にセキュリティー管理で役立ちそうなツールを概観してきた。筆者は、近年のネットワーク管理用のツールについては、二極化が著しいと考えている。

一方はウィンドウズベースで、誰もが使える管理ツールを用意して発展させていく組織もあるだろう。また、一方では、プログラミング能力を前提としたUNIX型の複数のツールを組み合わせるシステムも依然として広く使われている。

しかし、ネットワーク管理者がネットワーク管理を専業として扱うようになってきている現在では、プログラミング能力を前提としたシステムでは、管理者も管理作業を行えないことになってしまう。そこで、誰もが使えるプラットフォームに機能を集約していくことが、今後は強い魅力となってくるに違いない。

ネットワーク管理ツールはこれまでの長い開発の歴史の中で、一定のレベルと機能を安定して提供できるようになった。しかし、セキュリティー管理の助けとなるツールの提供はまだまだ少ないと言える。特に、セキュリティーポリシーでの記述と、実際のコンピュータやルーターでの設定には、その抽象度に大きく乖離があることから、セキュリティーポリシーとシステムの設定の整合性を確認するためには人間の手によって行うしかない。セキュリティーポリシーをコンピュータ上で処理できるための記述方法の定義や整合性確認のためのツール、さらに各種設定の整合性チェックを行うツールは、いまだ提供されていない。

さらに、インターネット環境での不法パケット送信者の発見ツールなどは、まだまだ研究開発の真っ最中にある。この意味では、今後多くのツールがいろいろな研究開発の成果を基にして提供されてくるに違いない。それを期待しながら、現在の管理基盤環境を構築していくことが必須であろう。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp