運用管理ツールで実現する発見的統制

大方 潤

IT（情報技術）全般統制では、本番機への不正なアクセスや設定変更などを後からも調査でき、統制が有効であることを証明する発見的統制が必要である。これの実態は、ログの照合であり、人手に頼らざるをえない、負荷が高い作業というのが現状である。しかし、Senju Familyの構成情報取得ツールや、申請・承認の電子化、不備を診断できるツールを組み合わせることで、発見的統制の負荷を軽減でき、人手では難しかった統制の網羅性も実現できる。その結果、この発見的統制活動を日々の運用に無理なく取り込むことが可能となる。

稼動の監視だけでは不十分

IT全般統制は、その作業自体、特別なものでも難しいものでもない。たとえば、システムがきちんと稼働しているかを監視することは、企業として行っていて当然であろう。しかし、IT全般統制が有効に機能していることを「証明」するためには、稼働の監視だけでは不十分といわれている。

たとえば、許可のない者がシステムにアクセスできないようにするには、アカウントの管理、ファイアウォールの設置などが必要になり、このような予防措置は、世にあるさまざまなツールを利用すれば実現できる。もちろん、実際に導入するには既存のシステム環境や運用方法に、多少なりとも変更が必要であり、かなりの労力を要することにはなるが。

それに対して、予防措置の有効性を証明するのはさらに大変である。実際に、許可のない者のアクセスを正しく予防できていたかを、後から調べて証明できなくてはならない。いわゆる発見的統制が必要となってくる。

作業負荷が大きい発見的統制

発見的統制を行うには、単純に考えれば各機器のアクセスログなどを調べ、それぞれのアクセスが承認されたものかどうかを確かめればよい。作業は単純だが、アクセスされる機器の数やアクセス数が増えれば作業負荷は小さくない。

たとえば、サーバーが10台程度の比較的小さなシステムでも、1台当たり1日に10件のアクセスがあれば、1日に調べなくてはならないログは100件である。

この程度であれば、一つひとつ人手で確認しても1日で処理できるかもしれないが、作業担当者は、業務時間のほとんどをこの作業に費やすことになるであろう。しかも、サーバー数やアクセス数は増えていくのが普通であるから、この作業の負荷はときが経つほど膨大なものになり、その調査結果の保管も必要になる。

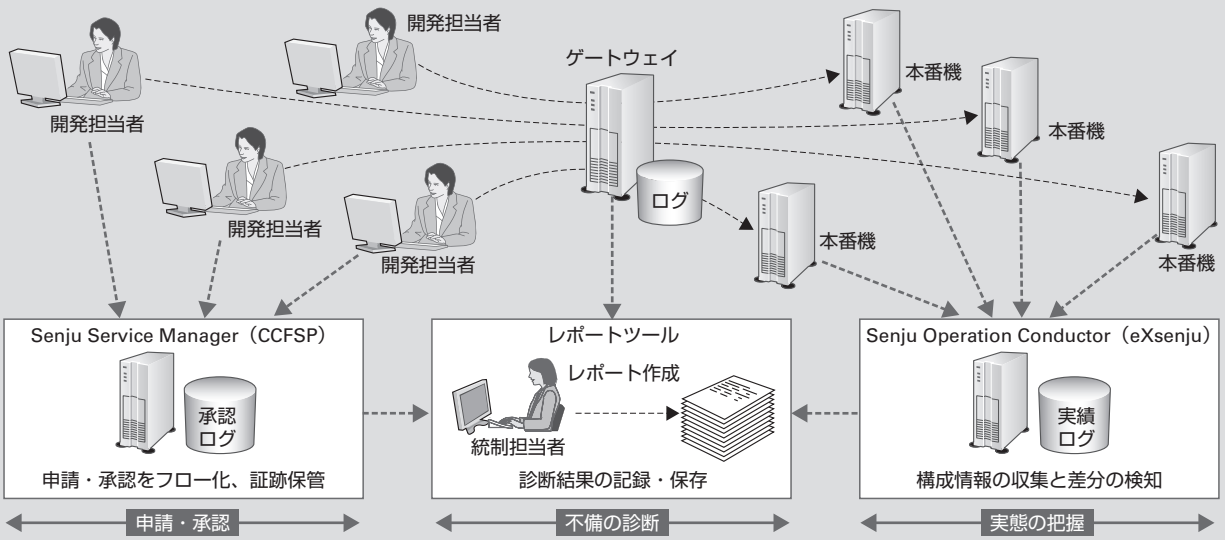
このような作業は、作業量に程度の差こそあれ、今後どの企業でも実施しなくてはならないものと考えられる。

発見的統制のためのソリューション

そもそもIT全般統制は、システムが正しく運用されていることを保証するものである。それにはさまざまな方法が考えられるが、効果的な方法は、データや設定ファイルが不正に書き換えられていないことを証明することであろう。

前述のように、いつ、誰がシス

図1　新生「Senju Family」を活用した発見的統制ソリューションの実現方法



注）http://senjufamily.nri.co.jp/を参照

テムにアクセスして、どのような操作をしたかをすべて管理し、それぞれの操作が誰の承認のもとに実施されたかを人手によってチェックするのは、現実的には不可能である。そのため､アクセス管理、リリース管理をシステム的に自動化する以下の方法が有効である（図１）。

①ファイル（設定ファイルやデータ、実行ファイルなど）の情報やアクセスログを定期的に取得し､変更を検知する（実態の把握）。

②リリース申請やアクセス申請を電子化し、承認のログを取得できるようにする（申請・承認の電子化）。

③検知された変更と承認ログを照合し、承認のもとにファイルの変更や本番機へのアクセスが行われたかをチェックする（不備の診断）。

ここでは、構成情報を取得できるだけでなく、変更を検知できること、変更を承認ログと照合できることが重要である。これによって統制が機能していることが証明できる。

構成情報を取得するツールや、申請・承認を電子化するツールはすでに世の中にある。ポイントは、これらに、さらに変更と承認のデータを照合できるツールを組み合わせることであり､それによって、人手に頼らざるをえなかった発見的統制を大幅に効率化することができる。

IT全般統制は、一度実施すれば終わりではなく、継続して実施していかなくてはならないものである。したがって、このような機能を持った運用管理ツールを選択し、将来にわたり発生する業務を効率化することが、IT全般統制の実運用における重要なポイントとなるであろう。

『ITソリューションフロンティア』2007年12月号より転載

大方　潤（おおかたじゅん）
千手・アウトソーシング営業部主任システムエンジニア