ワークフローによるシステム変更管理の実践
―予防的統制を実現する「Senju Service Manager」―

IT全般統制でいうところの予防的統制について、その必要性は理解してもさまざまな理由から実際には取り組みが進まない企業は多い。予防的統制は、ソフトウェアリリース管理などの「変更管理」が大きな要素となる。本稿では、野村総合研究所（以下、NRI）の運用管理製品「Senju Service Manager」を使った変更管理フロー構築の事例を紹介する。

変更管理のためのプロセスの“見える化”

予防的統制の主要素である変更管理は、あらかじめ決められたフローに従って、承認された変更を行うことである。変更管理の実現には、プロセスを明確化し“見える化”することが必要である。すなわち、日々の業務プロセスを明確なフローとして組み立て、そのフローを担当者に徹底させ、職務を分掌して役割を明確にする。それによって、「いつ、誰が、誰の承認を得て、何をするのか」が“見える化”され、統制された運用が可能になる。

変更管理の取り組みの事例

以下では、変更管理の構築により予防的統制を実現した、ある電気設備事業者（以下、A社）の取り組みを紹介する。

A社では、社内のシステムを構成するサーバーに対して、日々メンテナンス業務が発生している。ソフトウェアモジュールのリリースを行う場合、開発者はEメールで変更申請を起票し、承認を得るという手順をとっていた。しかし、この変更申請フローでは、「誰が、いつ、何をしたのか」といった証跡・履歴は各担当者のメールボックスだけに残る。そのため、申請に関わった当事者以外の人が証跡・履歴をチェックできないことに加え、証跡・履歴の削除や改ざんが可能な状態になっており、内部統制の監査時に不備を指摘される可能性があった。

そこでA社はNRIのサービスデスクツール「Senju Service Manager」を導入し、Eメールで行っていた変更申請・承認フローを改め、以下のように変更管理フローを構築した。なお、サービスデスクとは、ユーザーから受け付けた質問や報告の分析・分類と対応、およびそのフローを管理する機能のことである。

(1) 運用に合わせた管理画面の設計

「Senju Service Manager」は2007年末のバージョンから、インストールしてすぐにサービスデスク業務を開始できるよう、ITIL（システム運用・管理業務に関するベストプラクティスの体系的ガイドライン）をベースとしたプロセス（インシデント管理、問題管理、変更管理など）ごとに、必要な管理項目を網羅したデフォルト画面が用意されている。このデフォルト画面を基に、各社の運用形態に合わせた画面構成にカスタマイズできる機能も実装されている。さらに、管理項目の増減や変更だけでなく、表示項目の並べ替え、参

レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © 2009 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.

野村総合研究所
システムマネジメント事業本部
運用自動化推進部
副主任システムエンジニア
大平　亮（おおひらりょう）
専門はITILをベースとしたITサービスマネジメント

照専用・編集可能などの設定も可能である。

A社も、以上のような機能により、自社の運用フローに合わせて管理項目を整理し、管理画面を設計することから始めた。

(2) 承認フローの拡張

A社では、変更承認のフローだけでなく、承認が得られた後のリリースのプロセスもフローとして管理・記録したいという要望があった。リリースには、サーバーへのログイン、モジュールのリリース、テストといった作業が発生するが、「承認後の作業が適切に実行されているのか」という観点でプロセスを“見える化”したいということである。

「Senju Service Manager」には、変更申請の承認・却下といった機能に加えて、フローの項目を任意に編集する機能（作業アクション機能）が実装されている。この機能を利用すれば、「開発担当者による変更申請起票→開発管理者の承認→運用担当者の変更作業→運用管理者の承認」といった多段階フローの構築も可能である。

A社では、作業アクション機能を利用して、変更申請の承認後にリリースの結果を記録するフローを構築し、承認された変更が正しく実行（リリース）されているかをチェックできるようにした。

(3) 作業対象の管理

A社では、通常時は各サーバーへのアカウント（アクセスするためのID）は利用できない状態になっている。変更申請が承認されると、作業者がリリース対象サーバーにアクセスできるようにアカウントが開放される。このアカウント開放がいつ、どのサーバーに対して行われたかの履歴を管理する機能が「構成アイテム管理」「アカウント管理」である。

「構成アイテム管理」「アカウント管理」は、各構成アイテム（サーバーなど）やアカウントの履歴情報を管理していつでも閲覧できる仕組みを提供している。また、その構成アイテムやアカウントの利用日時および利用してない日時について履歴を管理する機能も有している。A社では、構成アイテムのサーバーに対して、「いつ、誰が、どのアカウントを使ってログインしたか」の証跡を残すようにしている。

A社では以上の(1)～(3)の取り組みにより、業務の効率化と、プロセスが“見える化”された運用が実現された。

さらなる統制された運用を目指して

以上に述べた変更管理の仕組みによって予防的統制が可能になるが、変更管理がつねに正しく運用されていることを定期的にチェックすることも重要である。本稿で紹介したA社の場合も、不正なアクセスや承認されていない変更が行われていないかを確認するために、リリース対象サーバーへのアクセスログを自動的にチェックする仕組みを構築することなど、さらなる統制された運用に向けた取り組みを検討している。■

レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © 2009 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.