

セキュリティ管理の新たなステージに向けたチャレンジ 仮想化環境とESS RECでセキュリティリスク管理の効率化を実現

東京海上日動システムズ株式会社(以下、東京海上日動システムズ)は、東京海上グループのシステム開発・運用を担っています。2004年に東京海上と日動火災のシステムグループ会社3社が合併して設立されました。

現在、東京海上グループのビジネスを支えるオンラインシステムでは、メインフレームと2,000台を超えるUNIX/Windowsサーバーが、月間1億8,000万件を超える膨大なトランザクションを処理しています。東京海上日動システムズは、この巨大システムの開発・運用におけるセキュリティリスク管理の改善のためにESS RECを採用しました。

Profile

東京海上日動システムズ株式会社

設立 1983年(昭和58年)9月
 本社所在地 東京都多摩市鶴牧2-1-1
 多摩東京海上日動ビル
 URL <http://www.tmn-systems.co.jp>
 事業内容 東京海上日動火災保険、東京海上日動あんしん生命保険、東京海上日動フィナンシャル生命保険等、東京海上グループの情報システムの企画・提案・設計・開発・保守・運用

< 導入製品 >



ITサービス本部
 ITサービス管理部
 ソリューションプロデューサー
 梁島 泰之氏

背景

セキュリティリスク管理に対する取り組み

東京海上日動システムズは、様々な環境の変化の中でも安定したITサービスの提供を実現するために、開発・運用プロセスの確立とその改善を行ってきました。2005年以降、個人情報保護法、JISOX法の施行という背景もあり、以下の3つの原則のもとでシステム部門内のセキュリティリスク管理とガバナンスの強化を進めてきました。

- 職責の分離・牽制：開発と運用の組織分離
- 環境の分離：開発環境と本番環境の分離
- アクセスコントロール：本番環境へのアクセスコントロールとモニタリング

課題

モニタリングの非効率化とWindows環境のモニタリング

アクセスコントロールの実装は、当初システム環境によって異なる方法を採用していました。メインフレームに対しては都度IDの貸出を行うことで対応、一方UNIXサーバーは、アクセス中継サーバーを介してアクセスコントロールリストをベースに制御する仕組みを採用していました。またどちらの環境であっても、操作後に出力される「モニタリングリスト」を管理者が確認することで、アクセスコントロールの有効性をモニタリングしていました。

しかしこの方法では毎日大量に出力されるリストを確認するために多くの時間を費やす必要がある上に、モニタリングの過程でリスクを伴う操作が新たに発見されれば、それを抑止するルールが作られモニタリング対象が増えてしまうという非効率なスパイラルに陥っていることが分かりました。

「モニタリングすると新たな課題が見つかって、見つかるルールを増やします。ルールが増えるとモニタリングが増えてしまう。とにかくこれを断ち切りたいと考えていました。」(梁島氏)
 また、直接リモート接続で画面操作を行うWindowsサーバーに対しては、有効なモニタリングの手法が見つかっていませんでした。

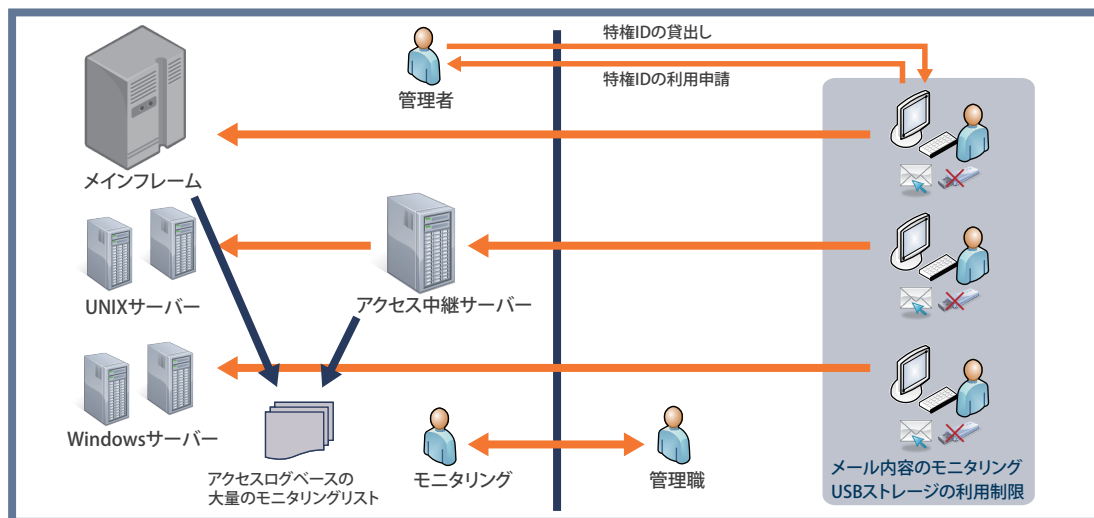


図1. ESS REC導入前のシステム構成とモニタリング実施状況

東京海上日動システムズが検討したアプローチは、リスクそのものを排除することでモニタリング対象を減らすこと、もうひとつはモニタリングの方法を変えることによる効率化でした。

機密性対策は、漏洩の経路を完全に塞ぐことでリスクそのものを最小化できるため、モニタリングを行う必要がなくなります。当初は、隔離された部屋を作るなど物理的にそのような環境が構築できないかと考えましたが、1,000名を超える開発・運用担当者に対して実行性のある方法が見つかりませんでした。

そこで採用したのが、仮想化技術を利用する方法です。開発・運用担当者は、仮想サーバー上に構築された仮想PC環境へ一旦ログインし、仮想PC上から操作対象のメインフレームやサーバーへアクセスするようにしました。この仮想PC環境は印刷、メール、外部接続媒体、社外へのネットワークなどあらゆる漏洩経路が遮断されているため、情報が外に出てしまうことはありません。

セキュリティのもう一つの要素である完全性は、経路を遮断しても対処することができません。そこでモニタリングの効率化を行うために採用したのがエンカレッジ・テクノロジーのESS RECです。

ESS RECは、システム操作を画像とテキストで克明に記録することで、高い監査性を実現します。

梁島氏は「今まで、メインフレームやサーバーについてはファイルアクセスやコマンド操作による記録をもとにモニタリングを行っており、Windows環境については画面操作のモニタリングができていませんでしたがESS RECを利用すれば、どちらも動画として記録することで、プラットフォームに依存しな

い汎用的なモニタリング環境ができる」とESS RECを評価しています。

また、梁島氏は効率化のメリットについても、次のように語られています。「録画をずっと眺めていなければモニタリングできないのであれば、効率性が落ちます。そんな時間があれば他の業務を行いたい。」

ESS RECにはモニタリングすべきコマンドや画面上にある文字列をブラックリストとして定義できます。やってはいけないことをやってしまった場合、そのアラートがあがった箇所をピンポイントでチェックする。そうすることで効率的にモニタリングできます。しかも動画が取れていますので、何をやったのか容易に判別が可能です。」

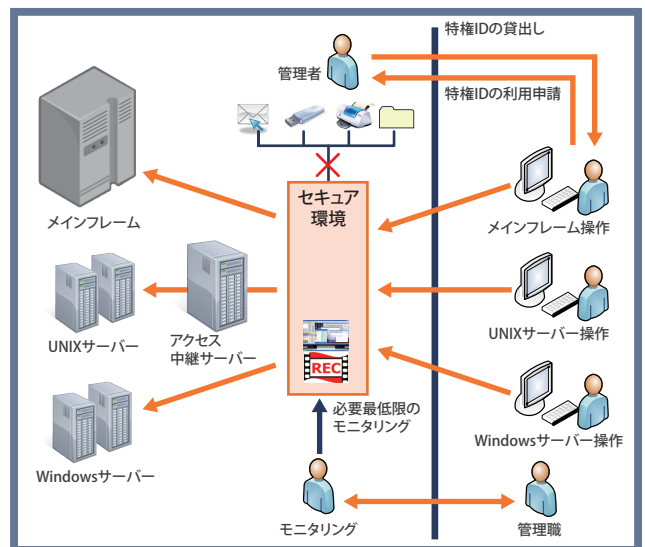


図2. ESS REC導入後のシステム構成とモニタリング実施状況

東京海上日動システムズは、仮想化技術とESS RECによる操作記録を組み合わせることで、「モニタリングが新たなルールを生み、そのルールが新たなモニタリング対象を生む」という負のスパイラルを断ち切り、開発・運用業務におけるセキュリティガバナンスを維持しつつ、効率化も追求することを考えています。

「開発・運用部門において、ルール・ポリシーとそのモニタリングのためにがんじがらめになり、非効率なことを行っている企業が多いのではないのでしょうか？」

機密性・完全性に加えて、いかに可用性を高めていくという観点からすると、私たちシステム部門の社員が効率よく仕事ができる環境を作っていくことも重要な要素であると考えています。それを可能にする技術・テクノロジーに今後も期待しています。」(梁島氏)

東京海上日動システムズは業務効率化とより安全なITサービスの提供の両立のため、セキュリティ管理の新たなステージに向けてチャレンジし続けています。

お問い合わせは

本事例に記述されている内容は2010年8月現在の情報です。
Copyright© 2002-2011 Encourage Technologies Co., Ltd.
記載の会社名・製品名は、一般的に、各社の商標または登録商標です。