

運用管理のプロフェッショナル企業が 内部統制強化を支援するソリューションを展開 — ESS REC により統制活動の効率化が可能に —

NTTデータとの連携で培った高度なシステムマネジメントノウハウや多彩な技術を活かした運用トータルソリューションのプロフェッショナル企業として事業展開するNTTデータ東京SMS。本稿では、同社が提供する情報漏洩防止や内部統制の強化に向けたソリューション「SMOOS SecureAssist」のうち、特に監査証跡や不正操作抑止など内部統制強化に有効な操作記録ソリューション「ESS REC」の概要を紹介する。

運用トータルソリューションの プロフェッショナル企業

1995年の設立以来、システム運用管理を中心とした運用トータルソリューションのプロフェッショナル企業として豊富な実績を築いてきたNTTデータ東京SMS。特に、NTTデータグループの一員として、大企業、官公庁などの大規模システムを扱い、高度な運用管理技術を蓄積してきた実績は、同社の最大の特長であり、大きな強みだ。こういったNTTデータとの連携で培ったハイレベルなシステムマネジメントノウハウや多彩な技術を活かして、高品質で安定性に富んだソリューションをグローバルに提供する「運用トータルソリューションベンダー」を目



NTTデータ東京SMS(株)ソリューションサービス本部 サービス企画部
(右) 部長 二ノ宮 尊徳氏
(左より) 営業企画担当 徳田 香織氏 井上 高氏 川上 昌章氏

指して事業展開している。現在、同社のコアコンピタンスであるマネジメント・技術・人材の3つの力を組み合わせ、より広範囲の顧客に最適な運用トータルサービス「SMOOS (System Management One to One Service)」を提供している。

「私どもNTTデータ東京SMSは、運用管理のベストプラクティスであるITIL (IT Infrastructure Library) をいち早く取り入れ、ITIL準拠の高品質な“運用維持管理サービス”、上流の企画・設計段階から参加し、より効果的で高品質な運用管理を行う“運用企画・設計支援/構築・導入サービス”、企業にとって極めて重要なリモート監視・インフラ構築・セキュリティの3つのソリューションについて設

計・構築～運用・保守までワンストップで行う“ソリューションサービス”、24時間フルタイムの“システム監視サービス”、システムスペース問題を解決する“ハウジングサー

ビス”からなるSMOOSをご提供し、お客様のお役に立つことを目指しています。」(NTTデータ東京SMS(株)ソリューションサービス本部 サービス企画部 二ノ宮 尊徳部長)

ワンストップソリューションサービス 「SMOOS Assistシリーズ」

NTTデータ東京SMSでは、維持・運用面を含め、企業の基盤系インフラの課題解決を支援するワンストップソリューションサービスとして、「SMOOS Assistシリーズ」を提供している。

「SMOOS Assistシリーズは、導入しやすいコスト、高い品質、柔軟性、拡張性のあるサービス体系を特色とし、現在、LAN/サーバ・クライアント構築サービス：SMOOS InfraAssist、情報セキュリティソリューションサービス：SMOOS SecureAssist、ネットワーク/サーバ遠隔監視サービス：SMOOS RemoteAssistを提供しています。今後もお客様のニーズに合わせ、順次ソリューションを拡充していく予定です。」(NTTデータ東京SMS(株)ソリューションサービス本部 商品

ビジネス部 三浦 譲部長)

SMOOS Assistシリーズの中でも、情報漏洩防止や内部統制強化の観点から最近特に注目を集めているのがSMOOS SecureAssistだ。本ソリューションは、情報セキュリティシステムの構築から運用までをトータルサポートするもので、適用シーン（レイヤ）に合わせ、下記のソリューションとプロダクトを提供している。

- ・インフラセキュリティレイヤ
検疫ネットワークソリューション：
「NOSiDE Inventory Sub System」
- ・コンテンツセキュリティレイヤ
情報漏洩防止ソリューション：
「TotalSecurityFort」
- ・オペレーションセキュリティレイヤ
操作記録ソリューション：
「ESS REC」

以下、これらソリューションのうち、内部統制強化を支援する操作記録ソリューション「ESS REC」について紹介する。

内部統制強化に有効な操作記録ソリューション「ESS REC」

ESS RECは、エンカレッジ・テクノロジー社（NTTデータ東京SMSも出資）が開発したオペレーション・トレーサビリティ・システムで、PC操作を監視カメラで記録するイメージのシステムだ。すでに、NTTデータ東京SMSの「SMOOSセンタ（統合運用管理センタ）」に導入・運用しており、確実に分かりやすい監査証拠の保存、操作ミスや不正操作の抑止に威力を発揮している。

● ESS RECの主な特長

ESS RECは、他の操作ログ収集ツールにはない特有の機能を含め、以下のような特長を持っている。

- ・ PCの操作画面を“動画像”で記録。

動画再生することでテキストログやスナップショットログにはない分かりやすさで操作の妥当性や不正・誤操作を監査することが可能で、監査証拠として活用できる。また、万一の情報漏洩事故にも、原因追求のためのトレーサビリティの確保が可能。

- ・ 操作ミスや悪意を持つ不正操作などの人為的な脅威を抑止することが可能。
- ・ 業務上操作が必要な利用者に対して、機能を制限（禁止／拒否）することなく、セキュリティ対策を実現することができる。
- ・ 記録データの再生・逆再生、コマ送りなどの機能に加え、一括検索機能によって、問題操作画面を瞬時に再生することが可能。
- ・ 記録データは暗号化して保存。
- ・ 記録データは、フル画面で秒間0～2KBに圧縮して保存。MPEGフォーマットの動画像と比べ1/6～1/10と非常に小さい。標準設定（取得したすべての情報を記録）



NTTデータ東京SMS(株)ソリューションサービス本部 商品ビジネス部 (左より) ソリューション開発担当

室本 悠氏 牛越 貴之氏 高原 雅志氏 久保田 啓五氏

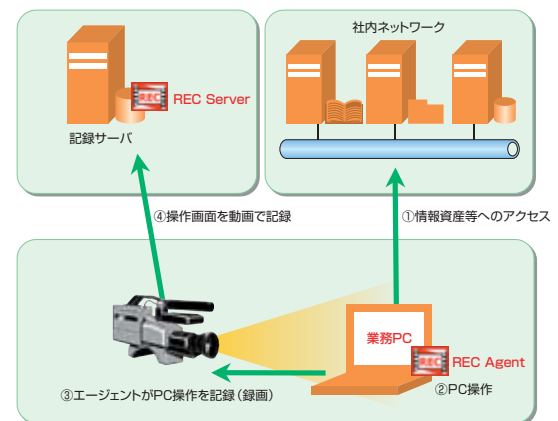


図1 ESS RECの対策イメージ

- の場合、1台あたり8時間分の操作記録データの容量は40～80MB程度であり、7～10年という長期保存への対応も難しくない。
- ・ PCに常駐して操作を記録するエージェント（REC Agent）はメモリ上で稼働するため、体感上のCPU使用率は1%未満を実現。
- ・ REC Agent稼働時はサーバと直接通信させないことも可能であり、モバイル環境でもPCの操作を監視することができる。

● ESS RECのシステム構成

ESS RECのシステム構成を図2に示すが、ESS RECは、4つのモジュール（REC Agent、REC

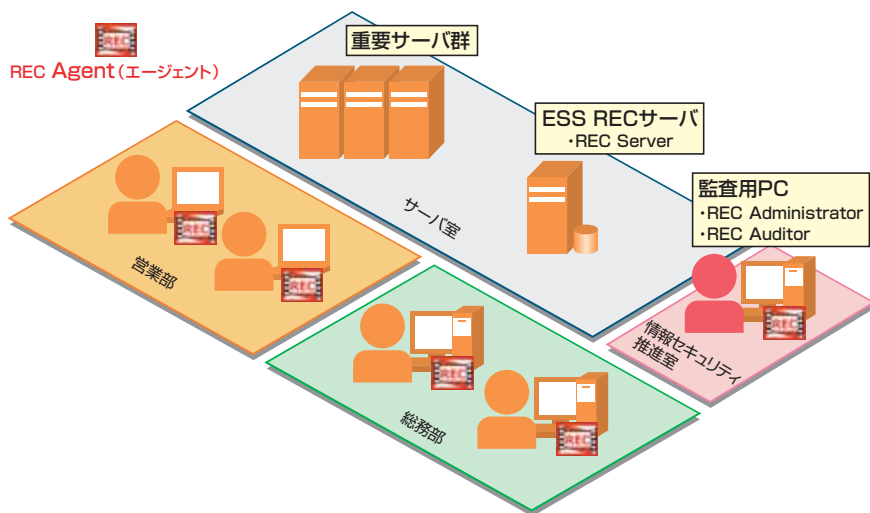


図2 ESS RECのシステム構成

Server、REC Administrator、REC Auditor) で構成され、それぞれ以下のような役割を担っている。

・REC Agent

クライアントPC / Windowsサーバに常駐して操作を記録しながら、8種類（キーボード操作、ドライブの接続、ネットワークの接続、ファイルアクセス、画面表示文字、プロセスの起動、操作の時間帯 [土日深夜]、USBデバイスの接続・切断）の監視。操作全体の流れを含む克明な記録を残すと同時に、監査可能な記録としてREC Serverに送信する。

・REC Server

REC Agentで記録したデータを蓄積するサーバ。REC Serverは、各クライアントPC / Windowsサーバに常駐するREC Agentからリアルタイムで送られてくる操作履歴を蓄積し一元管理する。REC Agentが収集した記録データは暗号化・圧縮されており、長期間でも安全に効率よく管理することができる。

・REC Administrator

記録データの再生やルールの設定等を行う管理者用モジュール。REC Administratorを用いて報告された検査結果をもとに網羅性・重要性等の観点から点検・監査を行い、監査報告書を作成する。

・REC Auditor

収集された全クライアントPC / Windowsサーバの操作記録を監査ルールに基づき定期的に自動検査するモジュール。検査結果について、

点検・監査レポート（サマリー・詳細）を自動作成する。

統制活動の効率的実施に有効な
「ESS REC」の主要機能

ESS RECは、統制活動を効率的に実施するために有効な様々な機能を提供している。

●3つの記録モードを搭載

ESS RECは、3種類の記録モードから選択して運用することを可能にしている。

・連続記録モード

クライアントPC / Windowsサーバの操作と状態を常に記録するモード。キーストロークをはじめ、全操作と画面の動画像、ネットワークの接続状況、プロセスの起動、ドライブの接続などを詳細に記録する。

・可変記録モード

連続記録モードでありながら、操作を行っていない時間を自動的に検知して作業の状態を記録する間隔を広げて記録データを少なくするモード。マウス、キーボードの操作を再

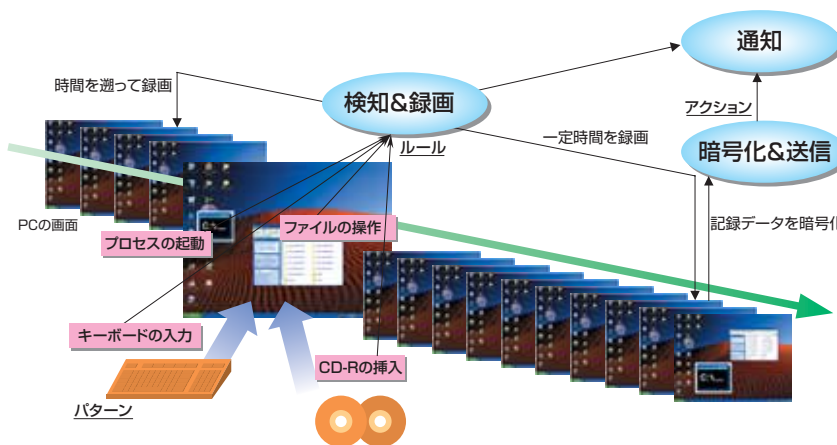


図3 検知記録モードの動作イメージ



図4 管理者用画面の記録表示例

開すれば自動的に連続記録モードへ移行する。

・検知記録モード

イベントにより操作内容の全てを記録するモード。ルールにヒットしない間は監視データが破棄され、操作内容や表示内容がルールにヒットした時にその60秒前（変更可）からの全ての状態を記録する（図3参照）。

●克明な記録とビデオデッキ感覚の動画の再生操作

ESS RECは、画面操作を含む以下の情報を克明に記録。しかも、管理者は記録した動画データの再生操作をビデオデッキ感覚で行え、ユーザーのPC操作の一部始終を把握し監査することが可能だ（図4参照）。
記録項目：画面（動画）／画面表示文字／キーボード操作／通信ポートの状態／プロセスの状態／ドライブの状態／USBポートの状態／ファイルアクセス／マウスの軌跡／ログオンユーザー名／コンピュータ名／IPアドレス／MACアドレス／時刻

●様々な監査記録レポートの自動作成機能を標準装備

様々な監査記録レポート（サマリ



図5 操作証跡レポートの出力例

ー・詳細）が自動作成される。監査担当者は、不正操作が試みられたと思われる前後の操作について、クリックするだけで記録データを再生でき、意図があったかを知ることができる。また、あらかじめ指定された操作を探し出し、レポートすることもでき、日々の監査業務の負荷を軽減することが可能だ。レポートは標準で用意されたフォーマットで容易に作成ができる。

図5に操作証跡レポートの出力例を示す。

●疑わしい操作を通知・遮断

あらかじめルール設定した操作を検知した場合、記録データの送信のほか、管理者へのメール送信、イベントログ出力、ポップアップの表示、外部コマンドの実行、監視システムESSへの送信などを行うことができる。また、ルールに抵触する操作に対して、画面をロックし操作の継続を抑制することも可能だ。なお、

画面をロックされたユーザーは、キーワードを管理者に知らせることで、解除コードを発行してもらうことができる。

以上、ESS RECの概要を紹介した。すでに述べたように、ESS RECは、システム運用時の不正操作や誤操作の発見、事故発生時の原因究明、再発防止策の実施といった統制活動を効率的に実施するために極めて有効なソリューションだ。NTTデータ東京SMSでは、金融機関、データセンターの運用管理部門、大手企業の人事部など、高レベルな内部統制が必要な企業・部門に対し、積極的な提案活動を展開していく方針である。

お問い合わせ先

NTTデータ東京SMS(株)
ソリューションサービス本部
サービス企画部 営業企画担当
Tel：03-6803-5025
E-mail：sales_1@nttdata-sms.co.jp
<http://www.nttdata-sms.co.jp/>