



リスクマネジメント

操作証跡ソリューション



これまでのログ収集・管理システムでは、ユーザーアカウントの運用や特権ユーザーの扱いにおいて、十分に対応できていませんでした。操作証跡ソリューションは、必要なログを確実に採取・管理し、監査やIT全般統制への対応を支援します。

利用シーン: IT全般統制強化のため、システム管理者がサーバに対して実施した作業ログの採取。

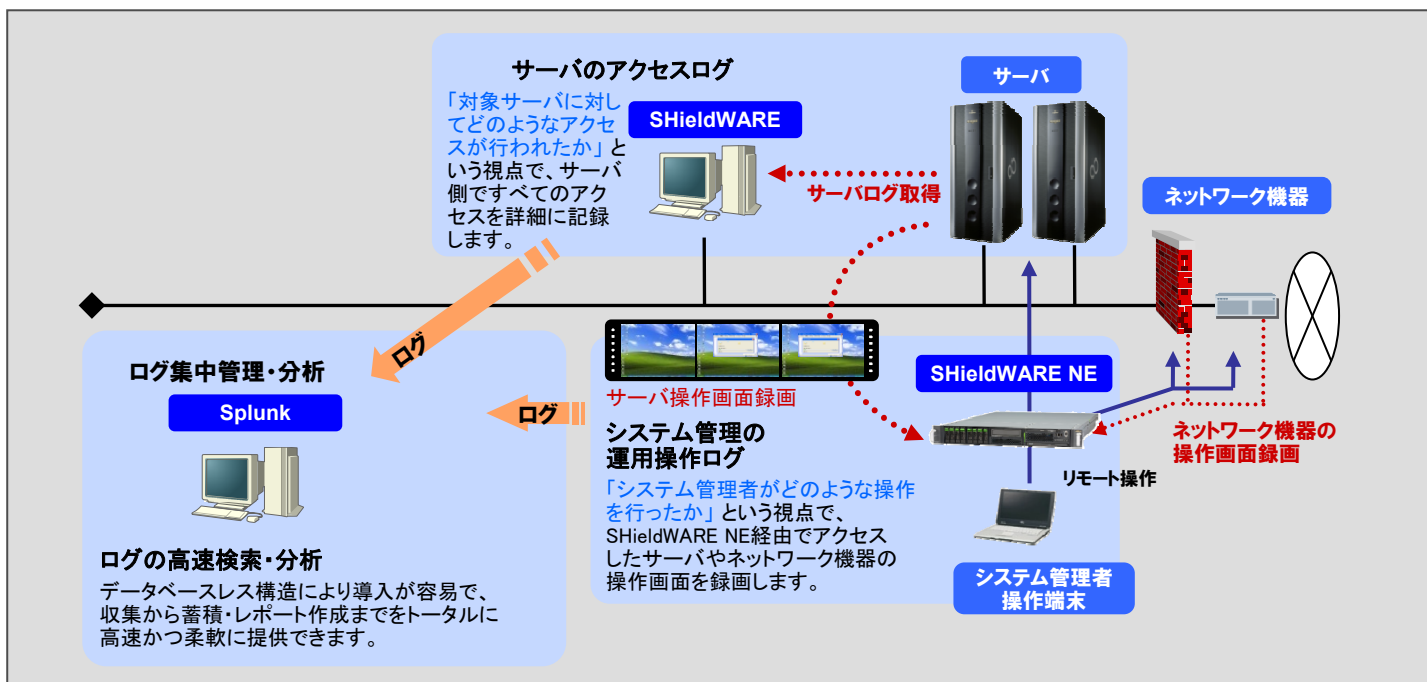
お客様の課題

- あらゆる権限を持つ特権ユーザーの操作記録ができていない。
- 特権ユーザーに対してログの改ざん保護がされていない。
- 複数人でアカウントを共有しているため、本当の使用者が分からない。
- 膨大なログを取得するだけで、内容のチェックができていない。

解決策

- ✓特権ユーザーを含む、あらゆるユーザーの操作履歴を、コマンドレベルのテキストログや動画にて詳細に記録します。
- ✓特権ユーザーに対してサーバ資産へのアクセスを制御することで、大切なログやデータを守ります。
- ✓共有されている特権ユーザーアカウントの操作も、独自のアカウント管理により個人を特定することができます。
- ✓高速検索機能やレポートでログを分析し、内部監査や監査人による評価作業を効率化します。

ソリューションの概要イメージ



導入により対策が可能となるリスクマネジメント分野

- | | | | |
|--|--|--|----------------------------------|
| <input type="checkbox"/> 認証・ID管理 | <input type="checkbox"/> Web・メールセキュリティ対策 | <input type="checkbox"/> 不正アクセス対策 | <input type="checkbox"/> 情報漏えい対策 |
| <input checked="" type="checkbox"/> 運用管理対策 | <input checked="" type="checkbox"/> セキュリティ監査 | <input checked="" type="checkbox"/> その他:(IT全般統制) | |

ソリューションの特長

- サーバ上での操作を詳細に記録
 - ・サーバ上での全ての操作をコマンド、ファイルアクセスレベルで詳細に記録するため、アクセスログから不正侵入阻止の履歴まで、確実に取得できます。
- 運用者の操作画面を完全録画
 - ・サーバ運用者の、GUI操作を含むすべての操作画面を、映像として録画することができます。
 - ・ネットワーク機器などの操作も記録可能です。
- 短時間でログ監査システムを導入
 - ・エージェントレスで運用者の端末とサーバの間に仮想アプライアンス製品を設置する方式のため、短時間で導入可能です。

ソリューション素材

素材名 (開発元)	概要	動作環境
SHieldWARE (富士通SSL)	<p>監査証跡: サーバ上での操作をOSのコマンドレベルで詳細に記録します。</p> <p>強制アクセス制御: rootやAdministratorといった特権ユーザーに対してもアクセス制御が可能です。 役割に応じた必要最小限の権限を付与することで、誤操作などによる被害を最小限にすることが可能です。</p>	<p>エージェント</p> <ul style="list-style-type: none"> Solaris™ 8 Operating System (SPARC64™) Solaris™ 9 Operating System (SPARC64™) Solaris™ 10 Operating System (SPARC64™) Red Hat® Enterprise Linux® AS v.4/ES v.4 (for x86, for Intel64, for Itanium) Red Hat® Enterprise Linux® 5 (for x86, for Intel64, for Intel Itanium) Microsoft® Windows® 2000 Server Microsoft® Windows Server® 2003/2003 R2 (x86, x64) Microsoft® Windows Server® 2008 (x86, x64) Microsoft® Windows Server® 2008 R2 (x64) <p>統合管理サーバ</p> <ul style="list-style-type: none"> Red Hat® Enterprise Linux® AS v.4/ES v.4 (for x86, for Intel64) Red Hat® Enterprise Linux® 5 (for x86, for Intel64) <p>管理端末</p> <ul style="list-style-type: none"> Microsoft® Windows® 2003/2003R2, 2008/2008R2, XP, Vista, 7
SHieldWARE NE (富士通SSL)	<p>監査証跡: サーバやネットワーク機器などの操作履歴を動画で記録し、閲覧が可能です。</p> <p>共有ID管理: 複数の運用者で共有している特権ユーザーのログも、個人ユーザーをヒモ付けすることで操作者の特定が可能です。</p> <p>一時貸出IDの払出し: 一時的に利用できるIDを払い出すことが可能です。一時貸出IDは承認者の承認のもとで払出すことが可能です。</p>	<p>VMware vSphere4に搭載可能なVA(Virtual Appliance)として提供</p>
Splunk (Splunk,Inc.)	<p>高速かつ柔軟な検索: テキスト形式のままログデータを収集し、膨大なログデータの高速で柔軟な検索・分析が可能です。</p> <p>レポート: ログデータをパソコンの画面上から検索、その結果をグラフや表、テーブルなどを使用してレポート表示します。</p>	<ul style="list-style-type: none"> Solaris 9, 10 (x86, SPARC) Linux Kernel vers 2.6.x以上 (x86, x64) FreeBSD 6.1, 6.2 (x86, x64) Windows 2003, 2008 (x64) WindowsXP (x86), Vista (x86, x64) MacOS X 10.5, 10.6 (x86) AIX 5.2, 5.3 HP-UX 11iv2(11.22), 11iv3(11.31) (PA-RISC, Itanium)

※SHieldWAREは富士通SSLの登録商標です
 ※記載の会社名、商品名は、各社の商標または登録商標です。
 ※記載された情報は、予告なく変更することがあります。
 ※記載の内容は、2011年10月現在のものです。

 SafetyValue とは、安心・安全・信頼・事業継続分野における富士通株式会社のブランドです。
 操作証跡ソリューションの一部の製品は、SafetyValueの一環としてご提供しております。
 PoweredSolutionは、富士通SSLのソリューション商品体系の名称です。

お問い合わせ先

株式会社 富士通ソーシャルサイエンスラボラトリ (富士通SSL)

お問い合わせ総合窓口

〒211-0063 川崎市中原区小杉町1-403 武蔵小杉タワープレイス

E-mail : ssl-info@cs.jp.fujitsu.com

T E L : 044-739-1251

当社ホームページ <http://www.ssl.fujitsu.com>