BeyondTrust

日本版SOX法/内部統制 対策　UNIX/Linux Root Access Control

Privilege Management for Unix & Linux Servers

旧称：PowerBroker

対象利用者

高権限者（開発者・運用管理者・保守担当者）

用途・目的

IT内部統制、データ改ざん防止、イベントログや全てのキー操作を記録、監査用ログ証跡、自らの正当性の証明として

UNIX/Linuxサーバの証跡管理は万全ですか？

どのログが必要なのか、どのように保管するのかをコントロール

Privilege Management for Unix & Linux Servers(以下PMUL)は、“いつ”、“誰が”、“どの”アクセスを承認、または拒否されたかを記録し、そのアクセスが“どこから”行われていたかを記録します。
キー操作ログは、全ての操作を再現することが可能ですので、不正操作などの追跡調査が容易になります。　また、追跡時のコマンド入力の癖や入力者の技術レベルを判断するヒントにも利用できます。
重要なシステムの操作や、技術レベルに不安が残る従業員が作業をする場合はリアルタイムのリモート監視（モニタリング）もできます。
また、肝心なときに必要なログが削除されていたり、改ざんされていたのでは意味をなしません。
PMULでは、イベントログとキー操作ログを安全に一元管理し、確実な監査証跡として保存します。

“いつ”、“誰が”、“何を”　しているのかをコントロール

PMULはルート権限を含めたユーザのアクセス管理を可能にします。
ユーザには、それぞれ個人が業務上必要とする最小限の権限を、許された時間帯に委譲します。
不正アクセスを“防御”し且つ“検知”する事で危険度を下げるお手伝いをします。

既存のシステムに　一切負担を掛けず、導入が簡単

システムの再起動となると、思わず気が重くなる方もいらっしゃるでしょう。
PMULならカーネルに一切の変更を加えませんので、サーバの再起動は必要なくなるのです。
ですからインストールも、各社独自の個別設定等も平日の業務時間中に実施できます。

イベントログとキー操作ログのリプレイ表示（GUI,CUIの両方で可能）

イベントログを確認することで、“いつ”、“誰の”、“どの”、作業の成否が確認できます

キー操作ログを確認することで、ユーザ操作を確認できます

Privilege Management for Unix & Linux Servers

PMUL 運用面の特徴

カーネルへの変更なし!!(安全運用)

・製品導入によるシステムへの影響がないため
　システム全体のテスト不要
・導入・アップグレードに伴うリブートなし
　(作業の中断がない)
・他製品の導入・アップグレードでも関連テスト不要

ポリシー定義情報の集中管理と安心設計!!

・複数のUNIX/Linuxのアクセス制御情報を一元管理
・フェールオーバ機能で障害の自動復旧

充実したログ管理!!

・集中ログサーバ設置による複数UNIX/Linuxログ一元管理
・ブラウザ・ベースGUIによるログの閲覧

PMUL の機能

業務内容ごとに分割した必要最小限の権限設定

・安全な環境による２種類のログ管理機能
・緊急時におけるキー操作ログのReplay機能
・ファイル、ディレクトリの保護
・プログラムの実行制御
・日付、曜日、時間等による利用制限
・電子メール・集中監視システムによる監視

サポートOS環境

UNIX

HP-UX
IBM AIX
Oracle Solaris

Linux

Debian GNU/Linux
Ubuntu
Centos
Red Hat Ent Linux
Oracle Linux
SUSE Linux Ent Server
IBM zSeries RHEL
Amazon Linux 2 in AWS
Red Hat 8 ARM Graviton2 in AWS

詳細バージョンは弊社までお問い合わせください

PMUL の実績について

海外：2,000社以上　200,000ライセンス以上
主要ユーザは商業銀行、最大規模の航空宇宙及び防衛関連業、最先端の医療・薬品メーカ、通信会社、データセンタ等に導入されている。
国内：100社　5,000ライセンス
業種：金融業（銀行・証券・消費者金融・カード・生保）、航空業、通信業、自動車、メーカ

ユーザ使用例

	ユーザ	事例
1	某製造業	要件：SOX法への対応として、高権限者の操作履歴取得が必須。特に監査で指摘されるモニタリングの観点から全てのキー操作ログを取得し、監査対応を行う。 適用：管理対象サーバ200台に適用。キー操作ログ収集、アクセス管理。
2	某保険関連	要件：センター内のUNIXサーバに内在する顧客情報を保護。　証跡管理を目的とし、Telnetでログインするユーザ全てのキー操作ログ、イベントログを取得する。キー操作をリアルタイム監視し、また、ポリシベースで違反を検知し、警告メッセージを監視ツールに上げる。悪質な場合は、セッションを遮断する。 適用：マスタ管理とログ管理用に各々サーバを立て、管理対象サーバ50台を一元管理。

［2022年10月現在］

株式会社ブロード
［Company Site］broad-corp.co.jp
［BROAD Security Square］bs-sque.jp
〒100-0014 東京都千代田区永田町 1-11-30 サウスヒル永田町 7F
TEL：03-6205-7463(代表)　EMAIL：broad@broad-corp.co.jp

お問い合わせは下記まで