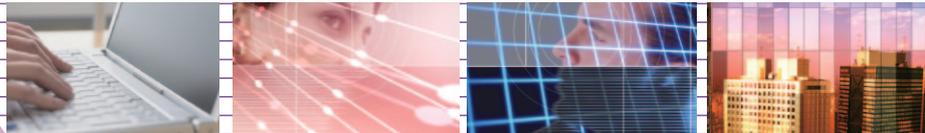


特権IDのアクセス管理ツール

SecureCube Access Check

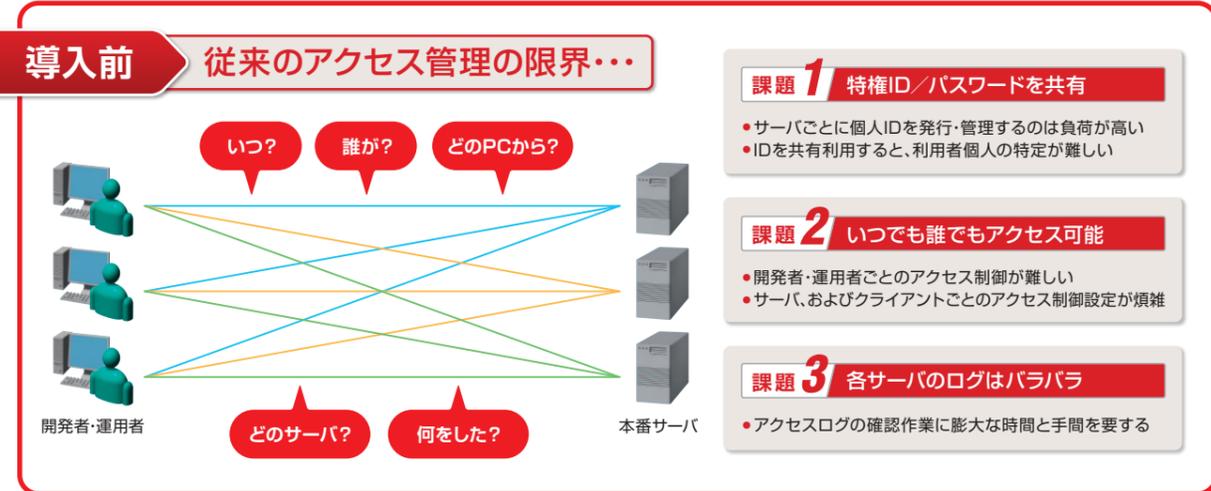


エージェントレスだから実現できる
短期・低コスト・低リスク導入



有効な統制環境へ、特権IDのアクセス管理に待ったなし。 足もとを揺るがす重大なリスクに、今すぐ現実的な対策を!

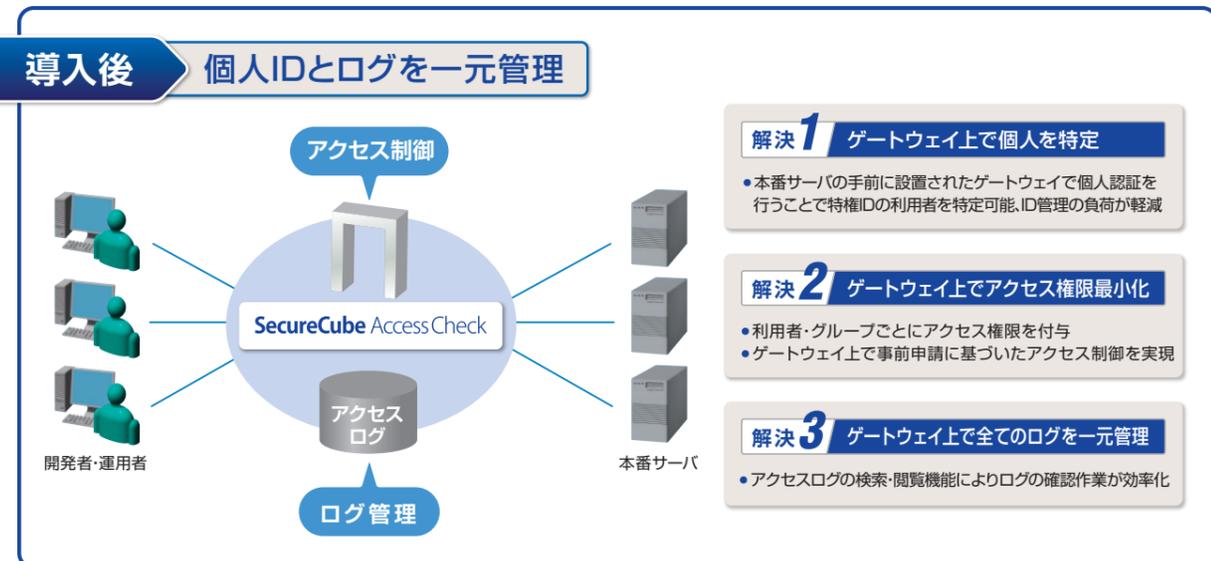
情報システムの特権IDを不正利用した情報漏えい事件・事故は後を絶たず、常に特権IDの厳格な管理が求められています。特権ID管理は、IT全般統制の観点でもアクセス管理対策として重視されるポイントであり、カード業界のセキュリティ基準である「PCI DSS」においても職務分掌を含むアクセス管理として必須要件となっています。しかし、各システムに対して個別に対策を実施すると、コストや導入期間、本番環境への影響、運用の負荷といった壁に直面し対策が遅れてしまいます。システムが安全に運用されていることを保証するとともに、増え続けるサーバ群に柔軟に対応していくためには、今こそ費用対効果の高い現実的な仕組みが必要です。



ゲートウェイ型の特権ID管理システム SecureCube / Access Checkで解決!

システム開発・運用の現場の声から生まれたアクセス管理のベストプラクティス

ゲートウェイ型のアクセス管理ツールである「SecureCube / Access Check」は、完全エージェントレスのため、既存環境に影響を与えずに短期間で導入できるのが特長です。特権ID利用者と本番サーバとの間に関所(ゲートウェイ)を配置し、その関所上で利用者の特定と厳密なアクセス制御、そしてアクセスログの管理を行います。ワークフロー機能も備えており、アクセス申請からログ監査までを一元管理するため監査業務を効率化することが可能です。



SecureCube / Access Checkの主な機能

予防的統制

アクセス制御機能

- きめ細やかな設定で不正アクセスを徹底的に排除

あらかじめ設定したポリシーに従ってアクセス制御を行います。ポリシーには、接続を許可するユーザグループとシステム(サーバ群)や、利用可能な接続元端末のIPアドレスとプロトコル、接続の際の事前承認の要否などを設定します。

アクセス申請・承認機能

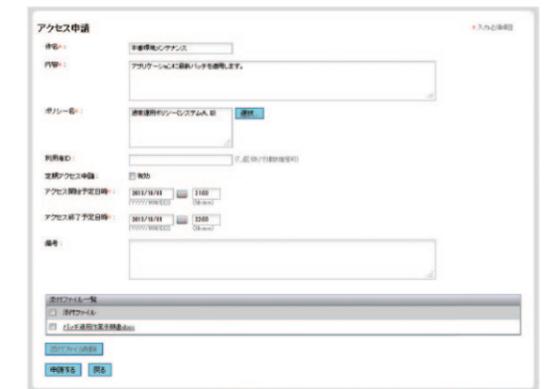
- システム開発・運用に必要な職務分掌を実現

アクセス申請・承認機能により、アクセス可能な利用者を限定します。ユーザが申請を行うと申請通知メールが送信され、管理者は承認画面から承認・却下が行えます。これにより、内部統制に不可欠な職務分掌を確立し、申請業務の効率化が図れます。申請・承認の履歴はすべて記録され、監査証跡としても有効です。

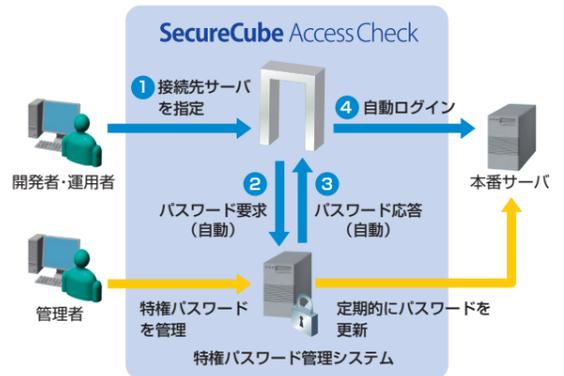
特権パスワード管理機能(オプション)

- 特権IDのパスワードを共有しない運用が可能

特権パスワード管理システムと連携することで、特権IDのパスワードを定期的に変更し、特権ID利用者へパスワードを開示しない運用が可能です。特権IDのパスワードを秘匿することで、許可されていない不正ログインを防止することができ、より強固なアクセス制御を可能にします。



アクセス申請画面



発見的統制

アクセス中継・ログ取得機能

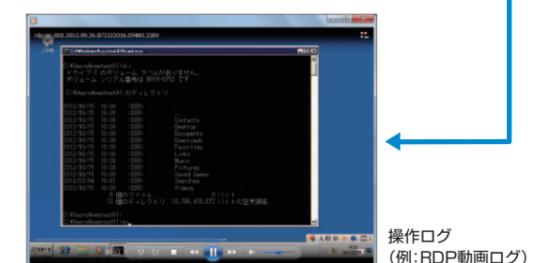
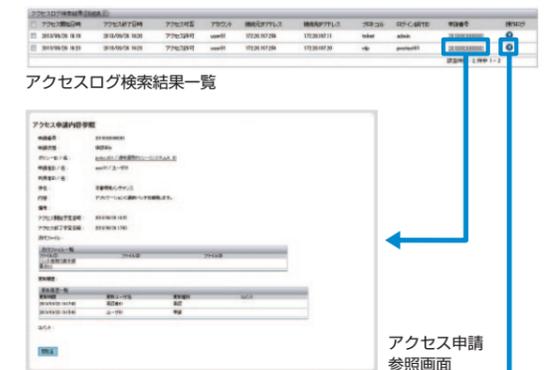
- 特権ID利用者を特定したアクセスログを一元管理

実際にサーバへアクセスするには、まずSecureCube / Access Checkへ個人IDでログインし、認証終了後、サーバを指定して接続します。アクセス終了後、いつ、誰が、どの申請に基づき、どのサーバへアクセスしたかなどのアクセスの概要を記録した「サマリーログ」と、実際の操作を記録した「操作ログ」が取得されます。

アクセスログの事後確認(監査)機能

- 膨大なログと事前申請との突合せを効率化

取得したアクセスログは、システムで自動的に申請と紐づけられ、権限を有する承認者のみ、Web画面から検索・閲覧することが可能です。また、ログの確認が完了したアクセス申請に対して、確認したことを証跡として記録することも可能です。



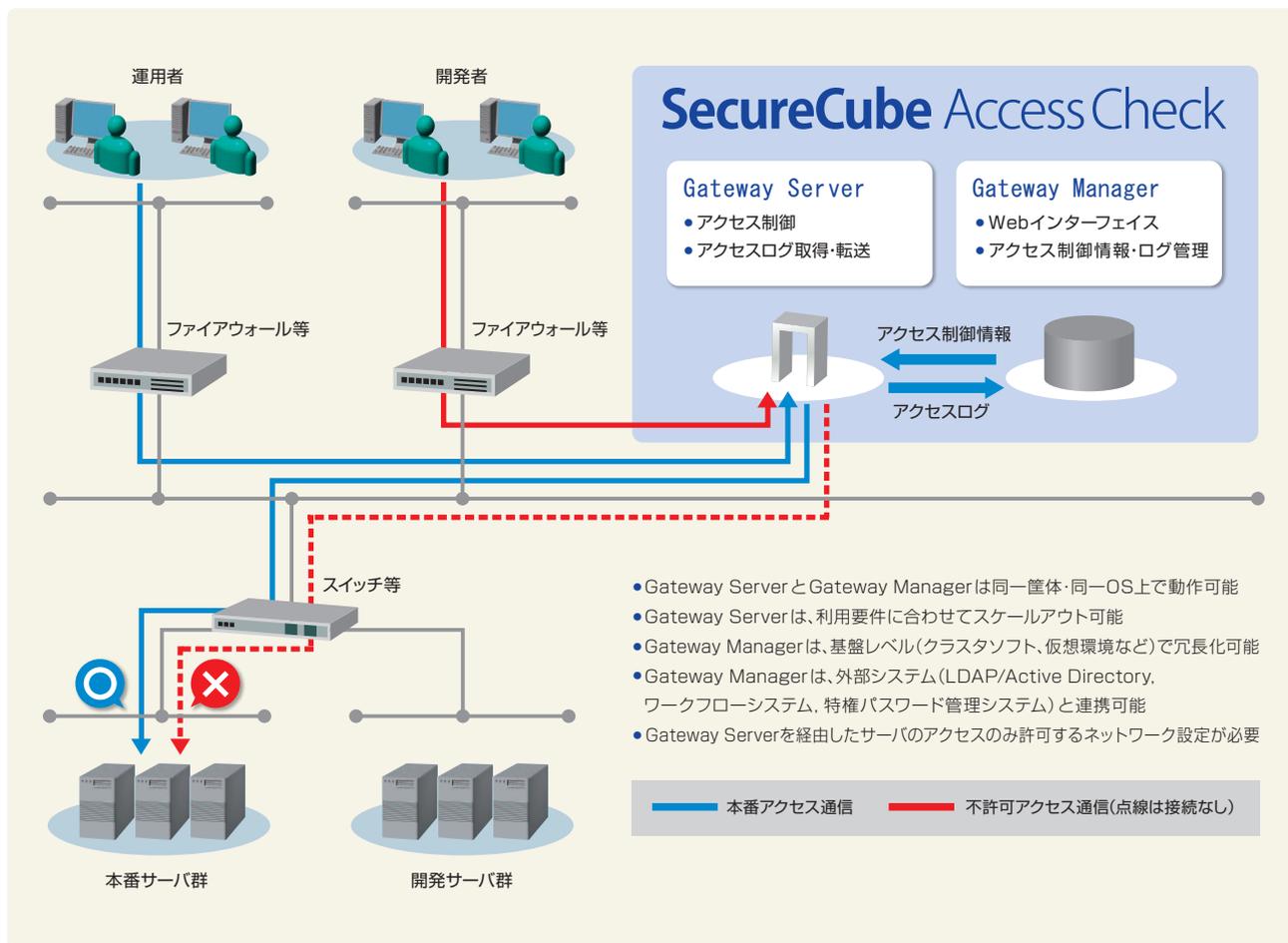
アクセス申請参照画面

操作ログ(例: RDP動画ログ)



SecureCube / Access Check システム構成

SecureCube / Access Checkは、アクセス制御を行うための各種制御情報やアクセスログを管理する「Gateway Manager」と、踏み台として中継機能を担う「Gateway Server」で構成されます。



SecureCube / Access Check 稼働環境

対応OS	Red Hat Enterprise Linux 6 (6.2以降、64bit) ※上記OSに同梱されているミドルウェア(MySQL, OpenLDAP)のインストールも必要
推奨ハードウェア	上記OSが稼働するハードウェア、または仮想環境基盤 ・CPU: 2.5GHz × Quad Core 以上 (x86_64) ・メモリ: 4GB以上 ※Gateway ServerとGateway Managerを同居させる場合は8GB以上 ・HDD: 146GB以上 ※ログ保存要件によってはディスク増設が必要 ・N/W: 1つ以上のネットワークインターフェイス
対応言語	日本語、英語、中国語(簡体字)
管理対象プロトコル	TELNET, SSH, FTP, SFTP, SCP, RDP, HTTP(S), CIFS, Oracle SQL *Plus, その他TCP

RDP(Remote Desktop Protocol): リモートデスクトッププロトコル
CIFS(Common Internet File System): Windowsファイル共有接続プロトコル

NRIセキュアテクノロジーズ株式会社

〒100-0004 東京都千代田区大手町1-7-2 東京サンケイビル
Tel: 03-6706-0500 Fax: 03-6706-0599
ホームページ <http://www.nri-secure.co.jp>
メールアドレス info@nri-secure.co.jp

※NRI, NRIロゴ, NRI SecureTechnologies, NRIセキュアテクノロジーズ, SecureCube, SecureCubeロゴは、株式会社野村総合研究所の商標または登録商標です。
※カタログに記載の会社名・商品名・ロゴマーク等は各社の日本および他国における商標または登録商標です。
※本カタログに記載の内容は予告なしに変更することがあります。

Copyright © 2014 NRI SecureTechnologies, Ltd. All rights reserved.

お問い合わせはこちら

NTTソフトウェア株式会社
特権ID管理ソリューション担当

TEL: 03-5782-7261 E-mail: tssol@cs.ntts.co.jp