

WANdisco Security CVS/Subversionに適切なアクセスコントロールを

IT企業やコンピュータ、制御を伴う機器を使用する企業にとって、その開発したソフトウェアのソースコードは最も重要な知的財産です。これらに対する参照やその利用を適切に行うためには、適切で効果的なアクセス・コントロールの実装とそのトラッキングが非常に重要です。WANdisco Security for CVS/Subversionは、CVS、Subversionリポジトリに対する適切なアクセス権の設定とその監査ログを提供します。

WANdisco Securityは、CVS/Subversionリポジトリに対する、効果的な認証、認可、アクセス制御、そして監査機能を提供します。また、WANdisco Securityは、Webベースの管理者コンソールを用意しており、詳細なアクセスコントロールをGUI画面で設定することが可能になります。グループ、サブ・グループ、ロールなどを設定し、CVSROOT/SVNROOT、ブランチ、モジュール、ディレクトリ、ファイルの各々のレベルについてまで設定できるため、管理の工数が削減され、また、タイムリーな管理が可能となります。

WANdisco Securityは、更にLDAPやActive Directory, NISとの連携機構をサポートしています。WANdisco Securityはこれらの認証サーバから、ユーザ情報をバルク入力する機能を備えています。また、ユーザの追加、変更、削除などを自動連係する機能も備えています。

WANdisco Securityは、WANdisco Multi-Site Replicatorと同時に使われる場合、分散された各々のレプリカ(複製)のセキュリティ設定が同じになるように自動的に同期されます。



アクセス・コントロール

WANdisco Securityは、リポジトリ・ブラウジング機能を持っており、CVSROOT, SVNROOT, ブランチ、ディレクトリおよびファイルレベルのアクセス権を簡単に設定できます。ユーザ・グループを定義する際、セキュリティ管理者はブラウザを使用してグラフィカルにアクセス権を設定する対象を選択することができます。また、ユーザは、割り当てられたロールに従ってリポジトリの資源にアクセスできるようになります。デフォルトでは、Developer(開発者)、Administrator(管理者)、QA/Release Manager (QA/リリース・マネージャ)、Auditor(監査者)、そしてProject Manager(プロジェクト・マネージャ)のロールがあります。このデフォルトのロールは、お客様の要件によって変更することができます。アクセス・コントロールは複雑な作業のため、ミスや訂正などの作業が大幅に発生しがちですが、WANdisco Securityによってこれらの工数を大幅に削減することが可能です。

さらに、グループやユーザ・レベルでのアクセス権を設定する際に、メンバーであるCVS/SubversionクライアントのIPアドレスに対して解放・マスクの設定をすることができます。特定のIPアドレス以外にも、そのクライアントが所属するネットワークや、LANのサブネットなどを、ユーザやグループに対して、選択的に設定することができます。

本機能は、特に開発を外注・アウトソースする場合に有効です。実際にアクセスしてくる方が不明(Unknown)であったり、頻繁に変更されるような場合にも適切なアクセス権を確保する事ができます。あまりに厳密すぎて、運用に耐えないものではなく、「現実解」を提供することができます。

監査レポート (Audit Reporting)

WANdisco Securityは、詳細な監査レポートを提供し、選択されたパラメータに関するアクセス日付・時間を表示します。パラメータは次の要素からの組み合わせになります。

- ・ ユーザID
- ・ クライアントマシンのIPアドレス
- ・ ディレクトリ
- ・ ファイル
- ・ ブランチ
- ・ リビジョン



time	access	command	user	ip address	dir	file	revision	branch
2006-02-13 14:09:27	allow	co	gary.han	192.168.1.103	/data/code/ CVS/e_commerce/			
2006-02-14 14:10:16	deny	update	john.doe	192.168.1.103	/data/code/ CVS/e_commerce/inarita/b/veri/src/	dodod.txt	1.4	HEAD
2006-02-14 14:10:16	deny	update	john.doe	192.168.1.103	/data/code/ CVS/e_commerce/			HEAD
2006-02-14 14:10:16	deny	update	john.doe	192.168.1.103	/data/code/ CVS/e_commerce/inarita/			HEAD
2006-02-14 14:10:16	deny	update	john.doe	192.168.1.103	/data/code/ CVS/e_commerce/inarita/b/veri/			HEAD
2006-02-14 14:10:16	deny	update	john.doe	192.168.1.103	/data/code/ CVS/e_commerce/inarita/b/			HEAD
2006-02-15 14:11:21	allow	ci	gary.han	192.168.1.103	/data/code/ CVS/e_commerce/inarita/b/veri/src/	dodod.txt	1.4	HEAD
2006-02-16 14:15:40	deny	update	gary.han	127.0.0.1	/data/code/ CVS/e_commerce/inarita/b/veri/src/	code.txt	1.4	HEAD
2006-02-16 14:16:41	allow	update	gary.han	127.0.0.1	/data/code/ CVS/e_commerce/inarita/b/veri/src/	code.txt	1.4	HEAD

アウトプットは、次のような内容を含みます。

- ・ 日付・タイムスタンプ
- ・ アクセスが許可されたか拒否されたか
- ・ 使用されたコマンド
- ・ ユーザID
- ・ クライアントマシンのIPアドレス
- ・ アクセスファイルのフルパス
- ・ リビジョン
- ・ ブランチ

認証されなかったアクセスの企ても、後の報告のために記録され、レポートされます。また、そのような場合、管理者に対して警告のメールを送ることもできます。WANdisco Securityは、SQLデータベースにこれらの監査レポートのレコードをロードするユーティリティを持っており、これを使って監査レポートに関して効率的な検索を行うことができます。

なお、本機能は米国SOX法の厳しい基準に耐えるように考慮されており、WANdisco Securityを導入することで、容易に内部統制の要請に添ったソースコード管理を実装することができます。

About WANdisco

WANdisco, Inc.

(本社)3000 Executive Parkway #520
San Ramon, CA 94583 USA

(日本)143-0023 東京都大田区山王2-1-2
OomoriStation Box 6F

URL: <http://www.wandisco.jp/>

お問い合わせ

株式会社野村総合研究所

情報技術本部

オープンソース・ソリューション・センター

横浜市保土ヶ谷区神戸町134

電話: 045-335-9538

URL: <http://www.openstandia.jp/>