



Self-Service AD Group Management



▶ 要旨

日立 ID グループ・マネージャーは、日立 ID グループ・マネージャーのターゲットシステム(主にAD(アクティブディレクトリー)に存在するグループでメンバーシップの管理を行う 日立 ID のソフトウェアです。これにより、ユーザーは、セキュリティーインフラの知識を持たなくても、セルフサービスで、セキュリティーの変更要求(ネットワークオペレーティングシステムのセキュリティグループに参加したり、退場したりする。)を作動させたりすることが出来るようになります。

日立 ID グループ・マネージャーによりユーザーがフォルダーやプリンター、配布リスト、他のネットワーク資源へのアクセスを、ユーザー・グループのメカニズムをうまく活用して容易に管理することができます。

大規模なActive Directory グループ管理の課題

多くの企業では、WindowsサーバーとActive Directoryを展開し、それらのプラットフォームが持つ強力なアクセスコントロール基盤を使ってユーザーのデータアクセスを管理しています。この基盤では、ユーザーのリソースへのアクセスに、セキュリティグループという概念を用いています。:

- ▶ グループは、Active Directoryのなかでビジネス機能や組織構造を反映するように定義されます。
- ▶ グループは、共有部分、フォルダー、プリンターなどのネットワーク資源に割当てられます。
- ▶ ユーザーは、業務の内容に従ってグループに割当てられます。
- ▶ グループは、管理を容易にするためにネストされることがあります。

時間経過にしたがって、グループ数は増加し、企業/組織のなかでは、ユーザーの総数を上回ってしまうことさえあります。さらに、ダイナミックな組織では、頻繁にユーザーの責任範囲の変更が起こり、新しいプロジェクトにアサインされます。こうしたことは、さらなる複雑さをもたらします。:

- ▶ ユーザーの要求はグループのユーザーメンバーシップの変更に反映される必要があります。
- ▶ ユーザーサポートグループは、ユーザーを適切なグループに割当てることでユーザーアクセス問題に対応するように生成されなくてはなりません。
- ▶ ユーザーは、セキュリティ基盤を意識していません、したがって、彼らのヘルプデスクへの問い合わせの際に訊ねる最初の一言は、“アクセス拒否”のエラーが出た”というのが一般的です。
- ▶ 問題解決には時間が掛かります。:最初にユーザーの問題の内容をネットワークUNCにマッピングし、そのリソースの権限を持つグループを探し、そして、そのグループの所有者を探し、当該ユーザーを割り付けてよいかの許可を取ります、最後にユーザーをそのグループに割り付けます。

多数のセキュリティグループの変更管理の複雑さは、深刻なビジネス上の問題を引き起こします。:

- ▶ 多量のコールボリュームを処理するための、ユーザーアクセス管理の要員コスト
- ▶ ユーザーが必要なアクセス権限を得るまでの何時間か何日にも及ぶ待ち時間の長期化と生産性の損失
- ▶ 変更承認プロセスの不履行の結果として、不適切なアクセス権限を持つユーザーの存在

セルフサービスを使った複雑さの解決

セキュリティ管理グループにおいてセルフサービスソリューションを提供することによって、グループメンバーシップ管理の複雑さを 格段に低減することができます。:

- ▶ イン트라ネットウェブアプリケーションにサインイン
- ▶ アクセスしたい資源を探索または、ブラウズ
- ▶ アクセス権限を直接要求
- ▶ 自動的に適切な承認者、すなわち適切なADセキュリティグループの所有者、に要求を転送
- ▶ e-mail及びウェブベースのワークフローをつかって承認者に要求を直接送る

- ▶ 承認時に自動的に当該ユーザーを要求されたグループに割り付ける

セルフサービスの展開によりグループメンバーシップ管理の複雑さを低減し、次の課題を排除することができます。:

- ▶ ユーザーがセキュリティ基盤を理解しなければならないこと
- ▶ セキュリティ管理グループの運営コスト
- ▶ 認可されていないグループメンバーシップの存在に起因するセキュリティ上の問題
- ▶ 認可変更に時間を要することによる生産性の低下

日立 ID グループ・マネージャーの紹介

日立 ID グループ・マネージャーは、日立 ID グループ・マネージャーのターゲットシステム(主にAD(アクティブディレクトリー)に存在するグループでメンバーシップの管理を行う 日立 ID のソフトウェアです。これにより、ユーザーは、セキュリティーインフラの知識を持たなくても、セルフサービスで、セキュリティーの変更要求(ネットワークオペレーティングシステムのセキュリティグループに参加したり、退場したりする。)を作動させたりすることが出来るようになります。

日立 ID グループ・マネージャーによりユーザーがフォルダーやプリンター、配布リスト、他のネットワーク資源へのアクセスを、ユーザー・グループのメカニズムをうまく活用して容易に管理することができます。

日立 ID グループ・マネージャーは、ネットワーク資源へのユーザー要求を効率化するために設計された日立 ID 管理スイートのコンポーネントの一つです。

日立 ID グループ・マネージャーを用い、ユーザーは、セキュアウェブアプリケーションにサインインし、シェア、フォルダー、プリンターや、メール配布リストなどのネットワーク資源への新規アクセスを要求します。日立 ID グループ・マネージャーウェブフォームから、ユーザーは、最初に資源コンテナ(例:シェア; ディレクトリ OU)を選択し、特定の資源(例: フォルダー、メールDL)に辿りつくまでトリー表示をブラウズします。ユーザーが資源を選択すると、要求の提示をしたこととなります。

ユーザーが資源を選択すると、日立 ID グループ・マネージャーは、:

- ▶ 動的にユーザーの資源選択と特定の管理対象ターゲットシステム及び、そのシステムのセキュリティグループをマッピングします。
- ▶ 当該セキュリティグループが既に日立 ID グループ・マネージャーアクセス制御下にあるか判断し、そうでない場合、自動的にワークフローシステムにグループを追加します。
- ▶ 少なくとも一人の承認者がそのグループに定義されているかをチェックし、そうでない場合、自動的に管理対象システムから新規の承認者リストを引き出します。(例:グループ所有者を特定)
- ▶ ワークフロー要求を開始し、適切な承認者にユーザーが当該グループに加入することが許されるかを質問します。

日立 ID グループ・マネージャーワークフローシステムは、自動的に承認変更を記録し、要求された変更が許可された場合、要求されたグループにユーザーを追加します。

日立 ID グループ・マネージャー produces real, concrete business value:

日立 ID グループ・マネージャー:

- ▶ 短期的に責任分掌が変わる場合や、プロジェクト/業務に必要なアクセス許可を敏速かつ柔軟に発行する必要がある場合の、契約社員や正規社員の管理に最適です。
- ▶ ユーザー自身がグループメンバーシップ管理をすることで、IT管理者の仕事量を減らすことができます。
- ▶ ネットワーク資源にアクセスが必要な全てのユーザーにとって、アクセスが制限されたときに比べて生産性を向上させることができます。

日立 ID グループ・マネージャー のテクノロジー

日立 ID グループ・マネージャー は、現在は単一プラットフォーム(Active Directory)向けに設計されています。 ユーザーインターフェースから、ADグループのユーザーメンバーシップを使ってにアクセスできるリソースを操作できるようになっています。:

- ▶ ファイルサーバーのシェア
- ▶ フォルダー階層を含む、共有ファイル上のフォルダー

- AD上に定義されているプリンター及びプリンターサーバーキュー
- MS Exchange等で用いられるメール配布リスト

日立 ID グループ・マネージャー は、ターゲットプラットフォームと接続するためにプラグインを用います。Windows/AD リソース・ディスカバリ・プラグインは、Active Directory上でWindowsベースのネットワーク資源を探索し、どのグループがどのリソースにアクセスできるか、グループ所有者はだれかを調べます。日立 ID グループ・マネージャー に準備されている、日立 ID 管理スイート Active Directory コネクタは、ADユーザーとグループを比較し、AD パスワード認証により、ADグループメンバーシップを更新します

ユーザーインタフェースワークフロー

日立 ID グループ・マネージャー は、複数の異なるタイプの資源を管理するのに用いられます。プラグインプログラムは、日立 ID グループ・マネージャーを、Active Directoryのグループのメンバーシップにより制御される、Windows シェアなどの特定のタイプの資源に括り付けます。他の資源の例としては、ネットワークプリンタやメール配布リストなどがあります。

詳細は具体的な例で示します。:

ユーザー	日立 ID グループ・マネージャー	資源-タイププラグイン	ターゲットシステム
1	ネットワーク ログインIDと パスワードで サインイン	証明書を認証	
2	新規の資源 アクセス要求 を開始		
3		Windowsファイルサーバーとシェア を構成する記述名のリストを表示	
4	シェアを選択		
5		選択されたシェアからフォルダーのト リービューを表示	
6	ブラウズして アクセスを行 いたいフォル ダーを選択	会話的にトリービューを表示	選択されたシェアからサブディレクトリのリ ストを繰り返し提供
7	要求に対す る権限と認可 者のセットを 選択	..ユーザー入力を表示..	シェアに対する権限をもちセキュリティ権 限(リードオンリー? リード・ライト?)が 割当てられたグループのリストを提供。 各グループに一人以上の所有者(認可 者)が提供される。
8		認可変更をトラックするワークフロー	
9		(変更は許可) ユーザーグループメン バーシップを更新するエージェントを 実行。確認のe-mailを該当ユーザー とすべての所有者/認可者に送付。	権限の更新。ユー ザーは、当該フォル ダーにアクセス することができま

す。

要求ワークフロー: 複数承認者による並行承認

Windows 2003SP1 からは、ユーザーのグループを他のグループの所有者として 割り付けることが可能になりました。これは、事実上、ADグループは、複数の 所有者/承認者を持つことができることを意味します。

日立 ID グループ・マネージャー は、複数所有者、及び/あるいは、特定のサブ セット(例: 5人の承認者の内の1, 2、または、3人)による許可をサポートしています。

日立 ID グループ・マネージャー は、パラレル及びシリアル変更承認の両者をサポートしますが、日立 ID は、お客様にパラレル承認の利用をお勧めします。

パラレル承認でもシリアル承認でも、すべての承認者は、変更を実行前に許可しなければなりません。結果として、どちらの方法を使ってもセキュリティ上の影響はありません。

パラレルとシリアル承認の違いは、パラレル承認は、より効率的なSLAを提供しますが、シリアル承認では、誤った要求が仮に出された場合、早い段階での承認者がそれを却下することで、後に続く承認者の関与を防ぐことができます。

日立 ID の経験では、ユーザーは自身の要求は明確であり、承認されないような誤った要求を発行することはほとんどありません。したがって、偽の要求は、実質上ゼロに近く、後の承認者にこうした誤った要求をシールドすることによる効率上の利点はほとんどないことになります。結果として、パラレル承認の優位点 – SLAの向上とプロセスの複雑さの低減 – が採用判断要因となります。

最低限言えるのは、パラレル承認はよりよいSLAを日立 ID customerに提供し、構成及び保守も簡単です。したがってより好ましいと言えます。

要求ワークフロー: エスカレーションと委譲

ユーザーがネットワーク資源へのアクセスを要求すると、ワークフロープロセスが走り出し、適切な承認者(ADグループ所有者)に要求の審査を促します。

時々、承認者は、すぐに応答しないことがあります。ITサービスレベルアグリーメント(SLAs)を満足するためには、要求は自動リマインダー、自動エスカレーション、承認の手動委譲によってサポートされるべきです。

日立 ID グループ・マネージャー ワークフローエンジンは、自動リマインダー、エスカレーション、委任を実現する組み込み機能を持っています。:

- 変更要求の承認が依頼されているにも関わらず応答をしない承認者には、応答するように自動リマインダーを送ります。リマインダー発行間隔はプログラムで設定可能です。
- 引き続き応答を返さない承認者は、エスカレーションビジネスロジックを用いて特定の代替承認者に自動的に置き換えられます。エスカレーションは、通常外部データアクセスを起動し実行されます。 -- 例えば、コーポレートディレクトリから元の承認者のマネージャーまたは、同等の者を探索します。
- 承認者は、一時的に(スケジュールにより、限定期間、例えば予定休暇等)または、永続的に(例えば、承認者の担当業務が変更された場合)他の代替者に委任することもできます。委任を実行する前には、新規の承認者が応答し承諾する必要があります。
- ワークフローマネージャーは、要求をいつでも異なる承認者に割当てることができ、委任ルールを管理、設定したり消去したり出来ます。

日立 ID グループ・マネージャーのインストール、構成、と管理

日立 ID グループ・マネージャーは、構成及び管理が非常に簡単です。例えば、Active Directoryのグループメンバーシップを管理したり、ユーザーがグループコントロールされているファイルフォルダーにアクセスするためには、次のことを行うだけです。:

- Active Directory を 日立 ID グループ・マネージャー ターゲットシステムとして設定する。
- 日立 ID グループ・マネージャーがアクセスを管理すべき個々のシェアのベースUNCを入力。

- 個々のADユーザーグループに所有者フィールドが正しく設定されていることを確認する。

日立 ID グループ・マネージャー の展開は通常非常に迅速に行えます。:

- 製品のインストール
- プライマリターゲットシステムの構成 -- a Windows / Active Directory ドメイン
- 資源ロケーションプラグインのインストール (現時点では、Windows resource プラグインがあり、フォルダー、プリンター、の共有、メール配布リストの交換をサポートしています。)
- 資源ブラウジングのためのルートノードの構成、例えば、UNCs
- グループ所有者が正しくADに定義されているかの検証、なお、これらの人々は承認者として用いられます。 people will be used as authorizers.
- インストールが適当か否かのテストとデバッグ

全体の処理は、技術構成作業のため、通常2~3日の時間が掛かります。

ロギングとリポーティング

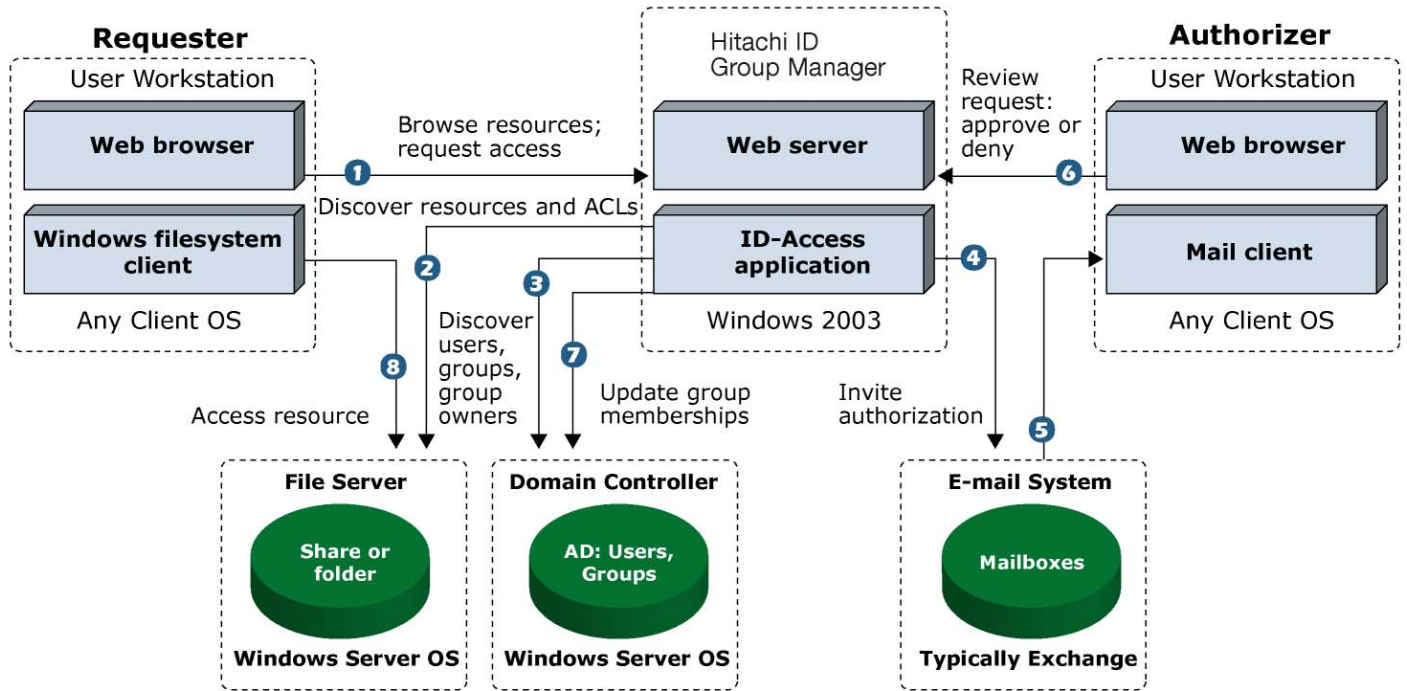
日立 ID グループ・マネージャー ログは、グループメンバーシップに関して試みられた、また、完了したすべての要求を記録しています。組み込み日立 ID グループ・マネージャー ワークフローエンジンは、次の内容を示す報告機能を備えています。:

1. 要求サマリー
2. 要求ライフサイクル
3. 要求統計
4. 要求詳細
5. 実行者サマリー

すべてのワークフロー要求は、無期限に保存され、いつでもレポート可能です。

ネットワークアーキテクチャー

日立 ID グループ・マネージャーのネットワークアーキテクチャーを図 [link]に示します。



日立 ID グループ・マネージャー ネットワークアーキテクチャダイアグラム

図では:

1. 要求者は、日立 ID グループ・マネージャーにサインインし、サーチとブラウジングすることにより、興味の対象のネットワーク資源を位置づけます。
2. 要求者は資源のアクセスについて問い合わせます。
3. 日立 ID グループ・マネージャーは、当該リソースのACLを見て、どのグループメンバーシップが適切かを判断します。
4. 日立 ID グループ・マネージャーは、グループの所有者を見て、要求者が興味のある対象の資源にアクセスできるように、要求者に代わって所有者にe-mailを送付し、そのグループに要求者をアタッチするように要求します。
5. しばらくして、グループ所有者はe-mailを受け取り、日立 ID グループ・マネージャーにサインインし、要求を許可するか拒絶します。
6. 要求が受け付けられたら、日立 ID グループ・マネージャーは、ADの中のユーザーとグループオブジェクトを更新し、新たなグループメンバーシップを生成します。

要求者と承認者の日立 ID グループ・マネージャーへのアクセスは通常、HTTPS 上のHTMLです。

要求者と日立 ID グループ・マネージャーの双方によるネットワーク資源への問い合わせアクセスは、SMB, DFS または、LDAPです。

プラットフォームサポート

日立 ID グループ・マネージャーは、現在 Windows2000, Windows 2003 で動作するADのActive Directory グループメンバーシップ管理をサポートしています。

また、次もサポートしています。:


1. SMB 及び DFS ベースのファイルシステム
2. ネステッドグループ、ユーザー 及び/または、どのメンバーシップが要求されるかを選択するポリシープラグイン

3. 共有（シェア）へのアクセス（例、シェア-レベル ACLs）
4. フォルダーへのアクセス（例、NTFS フォルダーレベル ACLs）
5. プリンターへのアクセス（例、ADが生成したプリントキュー上のAD-ACLs）
6. メール配布リストへのアクセス（例、AD のメール DL のメンバーシップ）

日立 ID グループ・マネージャー の開発ロードマップ

他のプラットフォームのサポート、例えば、NetWare/NDS/eDirectory は、近い将来サポート予定ですが、時期は顧客ニーズによります。

プラグインアーキテクチャーは、日立 ID グループ・マネージャーで、ユーザーが様々なタイプのリソースをブラウズしたり、アクセスを要求をしたりできるようにするたねに適しており、様々なタイプのLDAPで用いるグループ、様々な ネットワークアクセス可能なファイルシステム、様々な複雑なアプリケーション ACLsに対応できます。

 Hitachi ID Systems, Inc.

500, 1401 - 1 Street SE, Calgary AB Canada T2G 2J3 Tel: 1.403.233.0740 Fax: 1.403.233.0735 E-Mail: sales@Hitachi-ID.com

www.Hitachi-ID.com