

アクセス証明：権限蓄積を対処するプロセス



イントロダクション

このドキュメントは、権限蓄積のビジネス上の問題と、規制上の要求が益々増加する組織において、そのIT問題への影響について説明するものです。

このドキュメントでは、このビジネス上の問題を定義した上で、Sarbanes-Oxley, HIPAA, 21CFR11やGLBなどの規制に準拠しつつ、権限蓄積に対応するためのアクセス証明のプロセスを紹介しています。

課題

規制環境

沢山の新しい規定、規則に関連して、プライバシー保護(例: HIPAA, GLB, PIPEDA, EU Privacy Directive) とコーポレートガバナンス(例: Sarbanes-Oxley, 21-CFR-11)の動きがあります。プライバシーは、顧客、患者、投資家、従業員等に関連します。良好なガバナンスは、財務データ、臨床プロセス、安全手順等に関連します。

コンプライアンスには、AAAが必要です。

プライバシー保護とコーポレートガバナンスは両者とも効果的な内部統制に基づいています。こうした質問に対する課題は、:

Who can access sensitive data?	How are these users authenticated?	What can they see and modify?	Are users held accountable for their actions?
--------------------------------	------------------------------------	-------------------------------	---

これらのリクワイヤメントは、AAA(認証、承認、監査)の問題と言い換えることができます。

AAAに関わる問題

AAAインフラストラクチャは、特段新しいものでなく、古くからすべてのマルチユーザーアプリケーションに存在しているものです。システムやアプリケーションの数が増えるにしたがって、またスタッフの異動が頻繁になるなかで問題が顕在化し、既存のAAAインフラストラクチャのなかでは、ユーザーデータの管理がより難しいものとなってきました。

弱いパスワード、ヘルプデスクに掛けてくる人の識別に対する信頼性欠如、孤立アカウント、不適切なアクセス権限、不整合のログインIDなどの存在によって、AAAシステムは、しばしば誤ったタイミングで誤ったルールを強いてきました。この脆弱性は、AAAの技術にあるわけではありません。――AAAが対象としているユーザーデータを管理するビジネスプロセスが問題なのです。

AAAに関わる問題への対処にはID管理が必要

AAAデータの問題に焦点を当てると、ユーザに関するデータを、正しいユーザが正しいデータのみを、正しい時間にアクセスすることが出来る、しっかりとしたプロセスを実装することに尽きます。

これは、次の手段によって実現できます。:

- より堅固なパスワード
- ヘルプデスクに掛かってくる人を特定、認証する信頼性のあるプロセス
- ユーザーがどのようにログインアカウントとセキュリティ権限にアクセスしたり、それがいつ失効するかについてのより良い制御手段
- 管理者及びアプリケーションオーナーに委ねられるユーザーアクセス権限への定期的な監査
- 監査記録が人に対応付けられるように、システムに跨るユーザーオブジェクトの関連付け、
- 法的監査をサポート可能な、現在及び過去のアクセス権限の記録

日立 ID アクセス証明プロセス

日立 IDアクセス認証プロセスは過度のアクセス権限の特定と除去の問題を解決します。

認証プロセスは以下の単純な前提を基盤にしています。ビジネス・ステークホルダーが、ビジネス上で親密な関係にあるユーザーに割当てられている不適切な権限を特定できること。

日立 ID アクセス・サーティファイアはこのように基礎的な観察やアクセスレビューの異属、そして組織上のマネージャやアプリケーション・オーナーへのクリーンアップと認証の上に構築されています。3タイプのビジネス・ステークホルダーが以下の3タイプのアクセス認証を導きます。

▶ 組織中心認証Org-centric Certification

日立 ID アクセス・サーティファイアは組織チャートデータを活用して、マネージャと部下の間の関係を特定します。このデータを使用することにより、マネージャは部下のアクセス権限のレビューを求められることができます。マネージャに送信された要求も、リマインダーも、認証変更もすべて日立 ID アクセス・サーティファイアワークフロー・エンジンを使用します。

組織中心認証における日立 ID アクセス・サーティファイアプロセスは以下の様に実行されます。

- 日立 ID アクセス・サーティファイアは定期的に(企業ポリシーによって四半期や半期など)マネージャにスタッフのアクセス権限のレビューを求めます。認証要求はEメールで送信され、ワークフロー・エンジンは自動リマインダーを送信し、応答しなかったマネージャより上に要求をエスカレートします。
- 自身のネットワークもしくはディレクトリログインIDとパスワードで日立 ID アクセス・サーティファイアにサインインすることで、マネージャは応答します。
- ダッシュボード・インターフェースはマネージャにスタッフのリストを提供し、組織ですでに働いていないスタッフ(ユーザー・プロファイル)を特定するように求めます。選択したものは後ほど消去されます。
- 残りの正式なユーザには、日立 ID アクセス・サーティファイア対象システム上のログイン・アカウントのリストとともに、アクセス・プロファイルが表示されます。対象システムには、名称、ビジネス機能の摘要、そして外部のHTMLページへのリンクなどの情報が記述されます。そのページにはスクリーンショットやより長い摘要など、固体識別に関するより詳細な情報が含まれています。
- マネージャは不要になったアカウントを特定し、後ほど削除するためにアカウントにフラグをつけます。
- マネージャは配下のスタッフが対象システム上に保有しているセキュリティ・グループ・メンバーシップのリストを見ます。ログイン・アカウントと同様に、セキュリティ・グループも名称、ビジネス機能、ポップアップのHTMLヘルプ・ページへのリンクによって判別されます。マネージャは適切ではなくなったグループ・メンバーシップを特定するように求められます。
- マネージャは直属の部下に対して上記のプロセスを完了し、「アクセスレビューが完了しました。」という旨のメッセージを読み終えたあとに、電子署名を発行します。そして 残りのユーザー、アカウント、グループ・メンバーシップが正しいことを認証します。
- マネージャがレビューと認証を完了した後、提案された変更(ユーザー削除、アカウント停止、グループ・メンバーシップ削除)はセキュリティ変更要求にひもづけられ、日立 ID アクセス・サーティファイアワークフロー・エンジンに送信されます。これらの要求は、システム・オーナーや上層マネージャなどから、ハイレベルな許可が通常必要になります。最終的にはユーザー、アカウント、グループ・メンバーシップが対象システムから削除されることとなります。
- 認証は組織階層を追って収集されます。マネージャAは自身の部下(B,C,...)が彼らのアカウントからサインオフしない限り、自身のアカウントからサインオフできません。これは組織の下層へレビュー・プロセスを完了するようにプレッシャーを与えます。これはSOX法やHIPAAなどの規制上の要件が上層のマネージャの動機付けになっており、この動機が認証プロセスをグローバル全体での完了へ導きます。
- 直属の部下の数があまりにも大きくなるマネージャはいないので、このプロセスは相当巨大な組織に対しても有効です。企業全体に渡る監査の完了に要する時間は、組織のサイズよりも組織構造の深さに依存します。

▶ アプリケーション中心認証Application-centric Certification

日立 ID アクセス・サーティファイアは個別アプリケーション内でユーザーアカウントやセキュリティ・グループ・メンバーシップのレビューを要求するために構成されます。日立 ID アクセス・サーティファイアワークフロー・エンジンによって、アプリケーション・オーナーはレビューの実行を促されます。

アプリケーション中心認証の日立 ID アクセス・サーティファイアプロセスは以下の様に実行されます。

- 日立 ID アクセス・サーティファイアは定期的に(企業ポリシーによって四半期や半期など)アプリケーション・オー

ナーに自身のアプリケーションへログインするアカウントを所有するユーザーと、同アプリケーション内のセキュリティ・グループ・メンバーシップの一覧をレビューすることを求められます。レビューは一度にひとつのアプリケーションに対してのみ実行されます。

- アプリケーション・オーナーは、自身のネットワークもしくはログインIDとパスワードを用いて日立 ID アクセス・サーティファイアーへサインインして、認証プロセスを始めます。
- アプリケーション・オーナーははじめに自身のアプリケーションのログイン・アカウントを保有するユーザーのリストをレビューし、後ほど削除するために、アクセスがないユーザーにフラグをつけます。
- 残りのユーザーに対しては、アプリケーション・オーナーはセキュリティ・グループ・メンバーシップをレビューし、後ほど削除するために、不適切なグループ・メンバーシップにフラグをつけます。
- グループ・メンバーシップはID、詳細な名称、ビジネス機能に関する適宜長めな説明を含むHTMLページへのリンク(オプション)によって判別されます。
- アプリケーション・オーナーはレビュー・プロセスを完了し、「アクセスレビューが完了しました。」という旨のメッセージを読み終えたあとに、電子署名を発行します。そして残りのログイン・アカウントとグループ・メンバーシップが適切であることを認証します。
- アプリケーション・オーナーがレビューと認証を完了した後、提案された変更(アカウント停止、グループ・メンバーシップ削除)はセキュリティ変更要求にひもづけられ、日立 ID アクセス・サーティファイアーワークフロー・エンジンに送信されます。これらの要求は、各ユーザーのマネージャーなど、ハイレベルな許可が通常必要になります。
- アプリケーション中心認証は、適度なユーザー数を保有するアプリケーションに対して有効であることに注意してください。適度なユーザー数とはアプリケーション・オーナーがユーザーを個別で認識でき、どのアクセス権限が各ユーザーに適切であるか理解できるほどのレベルです。組織全体に及ぶような巨大なアプリケーションやシステムに対しては、以下の認証がより適切にサポートします。
 - 組織中心認証
 - グループ中心認証(適度なサイズのユーザー・グループ用)
 - アプリケーション認証(アプリケーションがより細かい構成単位に区分され、それぞれにオーナーがいる場合)

● グループ中心認証

日立 ID アクセス・サーティファイアーは各グループ・オーナーによるセキュリティ・グループ内のユーザー・メンバーシップのレビューを要求するために構成されます。グループ・オーナーはこれらのレビューを日立 ID アクセス・サーティファイアーワークフロー・エンジンによって促されます。

グループ中心認証の日立 ID アクセス・サーティファイアープロセスは以下のように実行されます。

- 日立 ID アクセス・サーティファイアーは定期的に(企業ポリシーによって四半期や半期など)グループ・オーナーに自身のグループのメンバーシップを持つユーザーの一覧をレビューすることを求められます。レビューは一度にひとつのグループに対してのみ実行されます。
- グループ・オーナーは、自身のネットワークもしくはログインIDとパスワードを用いて日立 ID アクセス・サーティファイアーへサインインして、認証プロセスを始めます。
- グループ・オーナーはグループ・メンバーシップをレビューし、後ほど削除するために、不適切なものにフラグをつけます。
- グループ・オーナーはレビュー・プロセスを完了し、「アクセスレビューが完了しました。」という旨のメッセージを読み終えたあとに、電子署名を発行します。そして残りのグループ・メンバーシップが適切であることを認証します。
- グループ・オーナーがレビューと認証を完了した後、提案された変更(アカウント停止、グループ・メンバーシップ削除)はセキュリティ変更要求にひもづけられ、日立 ID アクセス・サーティファイアーワークフロー・エンジンに送信されます。これらの要求は、各ユーザーのマネージャーなど、ハイレベルな許可が通常必要になります。
- グループ数が多い環境では、既存のソースからグループ・オーナーシップに関するデータを記述すると便利です。日立 ID アクセス・サーティファイアーはグループ・オーナーに関するデータを対象システム(例: Active Directory)から引き出すことが可能です。これによって、グループ中心認証を数千の個別グループすべてに対して構成できます。
- グループ中心認証は、適度なユーザー数を保有するグループに対して有効であることに注意してください。適度なユーザー数とはグループ・オーナーがユーザーを個別で認識でき、どのアクセス権限が各ユーザーに適切であるか理解できるほどのレベルです。より大規模なグループに対しては、組織中心認証がより適切にサポートします。

アクセス証明の利点

アクセス証明は、従来の方法に比べて多大な利点があります。:

- ▶ 日立 ID アクセス・サーティファイアー では、永続的に発生するセキュリティ問題に対し、実践的なソリューションを提供しており、その展開は容易です。
- ▶ 実用的なソリューションは、ユニークなものです。企業等の組織は、終わることのないロールエンジニアリングプロジェクトの泥沼にはいることなく、2-3週間のうちにアクセス証明書の展開をすることができます。
- ▶ だれがどのシステムに何のアクセス権を持っているかの、完全、正確、最新の情報を既に存在するたった一つのリポジトリから取り出します。
- ▶ すべての孤立アカウント、休眠アカウントを特定し、削除することによってネットワークセキュリティを強化します。
- ▶ 結果として、既存の認証、承認、監査(AAA)システムのユーザーアクセス、権限データを完全にクリーンなものにします。
- ▶ Sarbanes-Oxley(SOX準拠)、HIPAA準拠、21 CFR Part 11, PIPEDA, Gramm-Leach-Bliley (GLB準拠)、その他のコンプライアンスに対応します。

従来の方法

従来の過剰なアクセス権限の探索や削除の問題は、通常、ポリシーの強制、特にポリシーベースのプロビジョニングに焦点があてて試みられてきました。

ポリシーベースのプロビジョニングは次のように定義されます。:

- ▶ すべてのユーザー、すべての管理対象システムにフルアクセス要件が満たされるに十分に細かく、ロールのセットを定義します。
- ▶ ユーザーをロールに分類、アクセス要件はロールメンバーシップの指定により示されます。
- ▶ ユーザーが管理対象システムに実際にもつアクセス権限に対して、アクセス権限ポリシーモデルにより想定できるアクセス権限を調整します。結果として生じた差分のセットを、管理対象システムに直接戻すか、承認ワークフローを介して間接的に戻します。

企業規模では、数千(数万)のユーザー、従業員、コントラクターや、経営者がおり、継続的に雇い入れられ、解職されており、ユーザーの分類は非常に困難です。

ユーザーの責任範囲が微妙に異なり、基盤が常に変化している環境では、ロール定義は、同様に非常に難しく、あるいは、不可能です。

アクセス調整には、可能ではありますが、完了するのに何日も何週間も掛かり、プロセスを実用化するには、時間が掛かりすぎます。

ポリシーベースのプロビジョニングのアプローチは、企業環境では失敗してきました。このプロセスに必要なデータが単純に難しすぎて、保守するには手間が掛かりすぎるからです。

アクセス証明アプローチの優位性

日立 ID アクセス・サーティファイアーには、企業/組織が享受できるいくつかの優位性があります。:

- ▶ **展開が容易** -- 重要なビジネス上の問題に対処する実践的なアプローチです。: 放置されたユーザー権限を見つけてだし、削除します。企業/組織は、日立 ID アクセス・サーティファイアーを僅か2-3週間で展開でき、時間と手間が掛かるロール定義やユーザー分類化プロジェクトなどの泥沼にはまる必要がありません。
- ▶ **正確で最新** -- 誰がどのシステムに対して何をアクセスするかの情報は、々のアプリケーション運用から距離を置いたITスタッフからではなく、直接関連しているマネージャーからの情報を用いています。
- ▶ **監査可能** -- プロセスは100%トレース可能で、権限の整理プロセスそのものの妥当性について上級幹部にも完全な信頼を提供することができます。

日立 ID アクセス証明プロセスと日立 IDの一貫したID管理ソリューションについてお知りになるには、日立IDにご連絡をお願いいたします。

日立IDシステムについて

日立 IDシステムズ (旧社名 M-Tech Information Technology, Inc.) は、ITセキュリティー業界をリードするアイデンティティー管理ソフト開発会社です。日立 ID の製品は、ネットワークセキュリティーの強化、ITサポートコスト削減、ユーザー生産性向上の面で、企業等のお客様のお役にたっております。日立 ID のお客様は、ユーザーパスワード管理、ユーザ認証機能、ユーザアクセスの設定及び無効化、ユーザーアクセス特権の管理機能などの自動化やセルフサービス化を図ることで、より効果的な管理を実現されております。日立 ID の製品は、現在、世界各国で780社を超える企業に導入頂いております。

M-Tech Information Technology, Inc. は1992年に設立、2008年に (株)日立製作所の傘下に入りました。現在、日立 ID システムズ という社名でアイデンティティー管理ソリューションのリーディング企業として活動しております。日立 ID の最初のID管理製品である、

日立 ID パスワード・マネージャー (旧商品名 P-Synch) は1995年より市場にリリースされています。今日、日立 ID はITセキュリティー業界をリードするパスワード管理ソフトウェアやアイデンティティー管理ソリューションソフトウェアのベンダです。

日立 ID の社員数は現在約140名。日立 ID は、過去64期連続の四半期で、成長と利益を得ており高業績を維持しています。

日立 IDの本社はカナダのカルガリーにあり、加えて、カナダ：バンクーバー、オタワ、モントリオール；米国：デンバー、ダラス、ニューヨーク；豪州：ブリスベン にオフィスがあります。

日立IDの顧客には、Best Buy, Bristol-Myers Squibb, Cadence Design Systems, Ford Motor Company, Kimberly-Clark Corporation, NCR Corporation, Pitney Bowes, Schering-Plough Pharmaceuticals, Sears Roebuck, Symantec, United Technologies Corporation, Wendy's International 他多数がいらっしゃいます。日立 ID,及びその製品についてお知りになりたい方は、<http://Hitachi-ID.com/> をご覧になるか、1.403.233.0740 にお電話ください。

 **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