

---

日立 ID 特権パスワード・マネージャーを用いた特権パスワード管理



#### ▶ 要旨

日立 ID 特権パスワード・マネージャー 多数のデバイスに跨った特権パスワードを安全に管理するためのシステムです。日立 ID 特権パスワード・マネージャー は、ワークステーション、サーバー、アプリケーションの特権パスワードを定期的にランダムマイジングします。ランダムパスワードは、最低2台のサーバー上に暗号化されて格納され必要に応じて開示されます。:

1. 管理者には、認証され、その要求が許可されたときに開示されます。
  2. アプリケーションには、組み込みパスワードが変更されたときに開示されます。
  3. ワークステーション、サーバーに対しては、サービスを実行するときに開示されます。
- パスワード変更と開示は、ポリシーと規制要件に従って行われます。

## 特権パスワード管理

特権パスワードは、組織の中の他のデータに比べてより堅固に保護しなければなりません。:

### 1. センシティブデータ:

特権パスワードは、他の全てのデータをアンロックできることから、組織のなかでは、ほぼ間違いなく最もセンシティブなデータと言えます。不適切な開示は、大惨事に繋がる可能性があります。

### 2. ビジネスの中断:

特権パスワードへのアクセスが出来なくなることは、少なくとも、パワーダウンするか、“ハッキング”するまで、特権パスワードがアクセスするシステムの管理できなくなることを意味します。企業すべてのroot または、Administratorパスワードが永続的に失われる惨事が起こった場合のITサポートにおけるインパクトを考えてみてください。

### 3. 頻繁な変更:

もし特権パスワードが絶えず変更されたら、定期的なバックアップメカニズムは、履歴データしか格納できず、最新のパスワード値の格納が出来ません。

日立 ID 特権パスワード・マネージャー により企業などの組織体は特権パスワードを安全に管理することが出来ます。

- ▶ 定期的にすべての特権パスワードをランダムマイジングします。その対象は、70種類以上のタイプのサーバーやワークステーションに及びます。
- ▶ ITユーザーは重要なパスワードが必要になったときに日立 ID 特権パスワード・マネージャーにサインインします。
- ▶ 一連のプロセスは、どのパスワードが誰に提示されたかを管理する堅固な、個人認証(Authentication)、及び認可(Authorization)を行い、個々のアクセスの履歴の監査(Audit)を可能にします(3つの機能を AAA と呼ぶ)。

## 特権パスワード管理の技術的課題

このようなセキュリティー問題に対してのソリューションは、当然 解読しやすいパスワードや、固定のパスワードを削除することしかありません。実際にこれを実現し継続するに技術的に難しいのは確かですが :

### ▶ 何千もの管理者用パスワードが存在する:

これらの管理をするには自動化が必要です。

### ▶ 複数の違ったシステムに使われているパスワードがある:

自動化は多種、多様なシステムに対応出来なければならなりません。(Windows、UNIX、SAP、メインフレーム、Oracle など) レーム、Oracle など)

### ▶ ほとんどの管理者用パスワードはワークステーションに含まれている.

ワークステーションパスワードには特別な課題があり:

- ワークステーションの電源が落ちているかもしれません。
- ワークステーションがネットワークに繋がっていないかもしれません。
- ワークステーションがファイアーウォールにブロックされて、中央のネットワーク基盤からアクセスできないかもしれませ

ん。

#### ➤ ターゲットシステムへの接続性:

- ターゲットシステムは常時作動していない場合もあります。
- ターゲットシステムがパスワード管理システムからアクセスできない場合があります。具体的に、ターゲットシステムが異なるネットワークセグメントにあり、パスワード管理システムから複数のファイアーウォールによってブロックされている可能性があります。

#### ➤ 安全で、信頼できる格納:

一度、周期的なパスワード変更が自動化されれば、次はパスワードの保管に関する技術的な難題に取り組む必要があります。パスワード保管システムは下記の条件を満たしていないといけません。

- **セキュアであること:** もし厳重なセキュリティーのないストレージに不正アクセス者が入れれば、全てのデバイスで使える管理用アクセス権を得ることができてしまいます。
- **信頼できること:** クラッシュや、突然の停電などで保管システムに影響が出ると、管理者IDが全て使えなくなってしまうます。
- **きめ細かなアクセスコントロールが出来ること:** 認証が行われた後に、正当な管理者だけがアクセスできる正しいパスワードを得ることができるようにすること。
- **パスワード開示の記録を探ること:** 特権パスワードのアクセスは、妥当性検証のため記録する必要があります。

## 特権パスワード管理システムに求められる機能要件

特権パスワード管理には、うまく統合された機能セットが必要です。

1. 既存のシステムで定期的にパスワードをランダム化する必要があります。-- センシティブパスワードは、ユニークで、一時的なものであるべきです。
2. パスワードは、正しい条件の下で、適切なユーザー、ソフトウェアエージェントに開示する必要があります。
  - a. 割当てられた適切なアクセス権限を持っているITスタッフに、
  - b. 永続的なアクセス権限は割当てられていないが、一時的な許可が与えられたITスタッフに
  - c. 新たに更新されたパスワードでサービスが再起動できるように、サービスを起動するプログラム(Windows Service Control Manager, Scheduler, IIS 等々)に、
  - d. プログラムやスクリプトに組み込まれたパスワードを入れ替えるために、アプリケーションに、
3. 上記を実現するために、静的なアクセスコントロールモデルと動的な承認ワークフローが必要です。
4. システムは、パスワード更新と開示の両方を記録する必要があります。パスワード開示記録はアカウントビリティを確立すると同時に、更新の失敗は基盤の問題を特定するのに用いられます。
5. システムは、一つのパスワードの同時開示を制御する必要があります。-- 例えば、同時にサーバーを管理する人数を制限するなど、

## 日立 ID 特権パスワード・マネージャー パスワードランダムイゼーション

日立 ID 特権パスワード・マネージャー は、重要なパスワードを定期的にランダム化することにより安全に保ちます。:

1. **サーバーやアプリケーションのためのプッシュモードでは、:**
  - a. 定期的に -- 例えば、毎晩3時~4時の間に
  - b. ユーザーがパスワードを戻した際に
  - c. ユーザーが特定のパスワード値を要求した際に
  - d. 管理者による緊急終了のイベント発生時
2. **ワークステーション及び他の機器に対するプルモードでは、:**
  - a. 定期的に -- 例えば、毎日
  - b. 日立 ID 特権パスワード・マネージャー サーバーへの集中アクセスを防いで、一日のうちランダムに
  - c. ワークステーションから日立 ID 特権パスワード・マネージャーへのネットワーク接続が確立した時点で任意のタイミ

ングで

日立 ID 特権パスワード・マネージャーは、複数のパスワードポリシーを適用することができます。資源グループに対してグローバルポリシー、ローカルポリシー、最優先ポリシーを設定できます。パスワードポリシーは、ランダム選択、または、手入力パスワードの両方の形態を設定できます。文字タイプ(ローケース、アッパーケース、数字、句読点)指定のほか、最少文字数、最大文字数、や他の特長、さらには、特に手入力パスワードに関連しては、ディクショナリ、履歴チェックを行うことも可能です。

## 日立 ID 特権パスワード・マネージャー のパスワード開示

日立 ID 特権パスワード・マネージャーは特権パスワードを安全に保管したりランダム化するためだけでなく、適切な認証と承認後にユーザーやプログラムに対して特権パスワードを開示するように設計されています。パスワード公開の機能範囲は以下の通りです。

1. ウェブ・インターフェースを使用するユーザーに対しては、アクセス制御ポリシーに従属させます。
2. 事前プログラム済みのパスワード公開権利を保有しないウェブユーザーに対しては、事前定義済みの承認者からの承認後、パスワード公開を実行します。
3. アプリケーションに対しては、埋め込まれたパスワードを差し替えるため、API(アプリケーション・プログラミング・インターフェース)を使用します。そのAPI上ではアプリケーション認証はOTP(ワンタイム・パスワード)を使用し、事前定義済みのIPアドレスの範囲からしか接続できないようになっています。
4. Windowsサービス・コントロール・マネージャーのような、サービス開始プログラムに対しては、パスワード変更の成功後に、新しいパスワードの値を適切なロケーションに置くことでパスワード公開を実行します。

### 一般ユーザーのアクセス制御

日立 ID 特権パスワード・マネージャーにおいて最も使用されるアクセス制御はリソース・グループに基づいています。リソース・グループとは 特権パスワードが管理され、ポリシーが適応されているデバイスの名前を付けられた集合体です。

リソースはグループに明示的に割り当てられるか(例: ワークステーションWKSTN01234をリソース・グループRGWKSTNSに割り当て)、もしくは暗黙的にエクスプレッションを用いて割り当てます。エクスプレッションはOSの種類やIPアドレス、MACアドレス、もしくはワークステーション名を基準にしています。(例: サブネット10.1.2.3/24内でWindows XPが稼動しているワークステーションをすべてリソース・グループXに割り当て)

リソース・グループに割り当てられるポリシーは以下のものを含みます。

- a. どのアカウントのパスワードをランダム化するか
- b. ランダムなパスワードをどのように構成するか(例: 長さ、複雑さなど)
- c. パスワードの開示に成功、または失敗した場合にどのようなアクションをとるか

デバイスのグループをより自然に表現にする仕組みとして、リソース・グループはネストが可能です

日立 ID 特権パスワード・マネージャー ユーザーは明示的もしくは暗黙的にコンソール・ユーザーのグループに割り当てられます。(例: Active Directoryのように対象システム上のユーザー・グループのメンバーシップを経由。)コンソール・ユーザーのグループはリソース・グループに対して特定の権利を付与されます。その権利とはメンバーデバイスの一覧や、パスワードとアクセス状況の監視権限を含みます。

異なるIT管理者グループ間における職務範囲の切り分けなど、ビジネス・ポリシーはユーザーを個別のユーザー・グループに割り当て、それぞれ異なるパスワード(重複しない)パスワードのセットを持たせることによって定義できます。

### 限定開示のためのワークフロー

日立 ID 特権パスワード・マネージャーはその他日立 ID製品(日立 ID アイデンティティ・マネージャー、日立 ID アクセス・サーティファイアー、日立 ID グループ・マネージャー)で使用されるものと同様の認証ワークフロー・エンジンを保有しています。ワークフローはユーザーの付与パスワード・リリースの要求を可能にします。実行時には、一人もしくは多数のユーザーが招待され(Eメール経由)、要求のレビューと承認を行います。承認された要求はEメールをパスワード受理者に送信します。そのEメールには日立 ID 特権パスワード・マネージャーへのURLが記載されており、ユーザーが再認証し、要求されたパスワードを表示します。

ワークフローのプロセスは以下の一連のステップで表現されます。

- a. ユーザーUAがサインインし、システム(S)のアカウント(LA)にログインに必要なその当時のパスワードを、ある一定の時間後(T)、ユーザーUBも使用可能にする要求を発行します。
- b. 日立 ID 特権パスワード・マネージャーはS上のLAに関連している承認者を探します。
- c. 日立 ID 特権パスワード・マネージャーはビジネス・ロジックを実行し、承認者リストを補完します。承認者はUAもしくはUB用の管理チェーンの誰かかもしれません。承認者の最終リストはLAです。N数の承認者がいますが、LAにパスワードを開示するためなら、M数( $M \leq N$ )だけの承認があれば十分です。
- d. 日立 ID 特権パスワード・マネージャーはEメールで承認者LAに招待します。
- e. 承認者が応答しない場合は、承認者は自動的にリマインダーのEメールを受信します。
- f. 承認者が引き続き応答しない場合は、日立 ID 特権パスワード・マネージャーはビジネス・ロジックを発行し、代理を探します。効率的に要求をエスカレートしていき、同時に代理の承認者を招待します。
- g. 承認者は招待Eメールを受信し、そこに記載されているURLをクリックします。そして自身を日立 ID 特権パスワード・マネージャーウェブ・ログイン・ページに承認して、要求のレビューと承認もしくは拒否を行います。
- h. 承認者が要求を拒否した場合は、Eメールが全参加者(UA、UB、LA)に送信され、要求は終了されます。
- i. 承認者Mがリクエストを承認した場合は、お礼Eメールが全参加者に送信されます。特別なEメールがUBに送信されます。そのEメールにはパスワード開示ページへのURLが記載されています。
- j. UBはEメール上のURLをクリックし認証をします。日立 ID 特権パスワード・マネージャーログイン・ページでパスワードが表示されます。

### 並行制御-- チェックイン/チェックアウト

日立 ID 特権パスワード・マネージャーは時間を問わず付与されたパスワードが開示された人数の追跡・管理のために構成されることもあります。これはパスワードのチェックアウトとチェックインの概念を用いて行われます。

- a. 管理されたパスワードを単に開示するのではなく、ユーザーはチェックアウトを求められます。チェックアウトはポリシー管理にもなります。
  - i. パスワードがチェックアウトされたらいつでもカウンターの値は増加して、一人以上がパスワードを現在所有していることを知らせます。
  - ii. 同時にチェックアウトできる人数は制限されます。例: 一度に二人まで。
  - iii. ユーザーがパスワードを保持できるインターバルは制限されます。例: 2時間以下。
- b. パスワードの使用が終わると、ユーザーはパスワードのチェックインを求められます。
  - i. パスワードのチェックアウト・カウンターの値は減少します。
- c. チェックインとチェックアウトはITワーカー間の調整を助けます。
  - i. 日立 ID 特権パスワード・マネージャーは新規チェックアウト対象のパスワードを所有しているユーザーに知らせます。例としては、自分たちがすでに作業しているシステムで誰かほかの人がこれから作業するというお知らせです。
  - ii. 日立 ID 特権パスワード・マネージャーは誰がすでにパスワードを所有しているかを要求者に表示できます。
- d. パスワードのチェックアウトは時間制限があり、許可された時間が経過したあとにパスワードは自動的にチェックし戻されます。
- e. パスワードはチェックアウト・カウンターが0に戻ると、自動的にランダム化されます。これは現在パスワードを知っているユーザーがいらないはずだということです。

チェックインとチェックアウトは、同一システム上で作業をするITワーカー間の調整をより楽にします。

### プログラム上での開示のためのAPI

日立 ID 特権パスワード・マネージャーはパスワードの開示や保管中の静的なプレーンテキストのパスワードを消去するために設計されたAPIを備えています。日立 ID 特権パスワード・マネージャーのAPIを使用することで、定期的にパスワードのランダム化を行い、一方ではそのパスワードを使用しているアプリケーションが必要に応じてパスワードを開示します。

日立 ID 特権パスワード・マネージャー APIはHTTPS上のSOAPを利用してアクセスされます。

たとえば、日立 ID 特権パスワード・マネージャーはOracle DBMSのログインパスワードを24時間毎にランダム化することもできます。データベースへの接続を確立するためにパスワードを使用するウェブ・アプリケーションは、個別の証明書(下記参照)を用いて日立 ID 特権パスワード・マネージャーへサインインし、現在のOracleログインパスワードを取得します。

特権パスワードを回収するAPIを実装する際の重要な設計ポイントは、パスワード開示を要求するクライアント(上記の例ではウェブ・アプリケーション)がどのように自身をAPIに認証させるかという点です。日立 ID 特権パスワード・マネージャーはこのプロセスをACL、ワнтаイム・パスワードとIPサブネットの組合せによって安全なものにします。:

- a. APIクライアントは自身のIDを使って日立 ID 特権パスワード・マネージャーにサインインします。
- b. これらのIDはコンソール・ユーザー・グループと割当済みACLに含まれており、正しいパスワードを開示できるようにします。
- c. APIクライアントのログインIDはワнтаイム・パスワード(OTP)が割り当てられており、サービスによって日立 ID 特権パスワード・マネージャーへサインインするために使用されます。それぞれのAPI接続上で新規かつランダムな文字列にAPIは変化していきます。
- d. APIクライアントのログインIDはIPサブネットに割り当てられています。APIには付与されたIPレンジからしかサインインできません。

加えて、アプリケーション開発者は暗号化(固定キー、アプリケーション埋め込み)とファイルシステム・アクセス制御によってOTP文字列を保護することが推奨されます。

### サービスパスワードの更新

Windowsオペレーティング・システムでは、サービス・プログラムは以下の2通りのログインIDで実行されます。最高特権を保有するがパスワードのないログインID「SYSTEM」か、ユーザー各々のログインIDとパスワードを使用し、制限された特権の範囲内で実行します。これはつまり、Windowsのワークステーション上とサーバー上それぞれに、多数のサービス・アカウントが存在し、ウェブ・サーバーやバックアップ補助ツール、ウィルス対策ソフトなどのサービス・プログラムを実行するために、アカウント独自のパスワードを保有しているということです。

サービス・アカウント・パスワードと管理者パスワードは、最低2箇所のロケーションに保管されているという点で異なります。そのロケーションは以下の通りです。

- a. セキュリティ・データベース。例: ローカルのSAMデータベースやActive Directory。
- b. サービス開始プログラム(Service Control Managerなど)がサービスのスタート時にパスワードを読み出す場所であるレジストリやその他のロケーションすべて。例: Service Control Managerや同等のもの。

日立 ID 特権パスワード・マネージャーは\_サービス・アカウント・パスワードを管理するために設定されることもあります。具体的には、オペレーションのモードによって、以下の2つの事柄を指します。

- a. プル・モードでは、日立 ID 特権パスワード・マネージャーワークステーション・サービスは、中心の日立 ID 特権パスワード・マネージャーサーバー・クラスターに対応して、定期的にサービス・アカウント・パスワードをローカル内でスクランブル化します
- b. プッシュ・モードでは、日立 ID 特権パスワード・マネージャーサーバーは、サービス・アカウントのパスワードを変更するために、定期的にリモートでWindowsサーバーに接続します。

どちらの場合も、日立 ID 特権パスワード・マネージャーは、新規パスワードを付与されたサービス・アカウントを立ち上げるプログラムに通知しなければなりません。理由は、システムの次回起動時、もしくは管理者が問題のサービスを手動で停止と再起動する際に、そのプログラムが正しくサービスを立ち上げられるようにするためです。

プッシュ・モードでは、日立 ID 特権パスワード・マネージャーは終了プログラムを実行します。終了プログラムは問題のサーバーにリモートで接続し、サービス・パスワードの第二ストレージを更新します。終了プログラムがリモートで更新する対象は以下の通りです。

- a. Windows Service Control マネージャー
- b. Windows Scheduler.
- c. IIS ウェブ・サーバー

日立 ID 特権パスワード・マネージャーの実装者は、追加の終了プログラムを書き、別場所の他プログラムに使用される

パスワードを更新することができます。

ブル・モードでは、日立 ID 特権パスワード・マネージャーワークステーション・サービスはローカル・パスワードの更新のためにDLLの使用が可能です。DLLはWindows上の同一コンポーネント(例:終了プログラム)に提供され、実装者は新規のDLLを作成し、他のパスワードを更新することもできます。

## 堅固な認証

日立 ID 特権パスワード・マネージャー は、認証、認可のために既存のユーザーディレクトリを生かした構成をとることができます。:

- ユーザーは、日立 ID 特権パスワード・マネージャー にActive Directoryまたは、LDAPのログインIDとパスワードを使ってサインインすることができます。
- この場合、ユーザーは、認証のため、RSA SecureID トークンのようなツーフaktorテクノロジー(2方式による認証技術)が必要かもしれません。
- 日立 ID 特権パスワード・マネージャー のセキュリティグループのユーザーメンバーシップ、及びそれに付随してユーザー権限は、ADまたは、LDAPのユーザーメンバーシップに依存することになります。

ユーザー識別、認証、認可に既存の外部の機能を用いることは、日立 ID 特権パスワード・マネージャー の展開するための管理工数を著しく削減することができます。

管理者(ITスタッフ)は、日立 ID 特権パスワード・マネージャーのウェブGUIに対して次のように認証します。:

- 現在のネットワークOSかディレクトリのパスワードをタイプ
- パスワードをタイプすることにより、それと日立 ID 特権パスワード・マネージャー自身の内部に格納されているパスワードハッシュと正当性をチェック
- セキュリティトークンを用いる。
- PKI証明書または、スマートカードを用いる。

## 監査と規定準拠

日立 ID 特権パスワード・マネージャー は、試みられた、及び完了したすべてのパスワード更新処理を記録します。このデータは、ワークステーション、サーバーの現在の管理者パスワードのみならず、機器のIPアドレスやネットワーク接続に関してトラックするのに用いられます。日立 ID 特権パスワード・マネージャーは、また、ユーザーが機器を検索したり、パスワードを表示させたりするすべての試みに対しても記録します。 これにより、誰がいつどの機器をアクセスしたかを明確にし、説明責任を確立します。

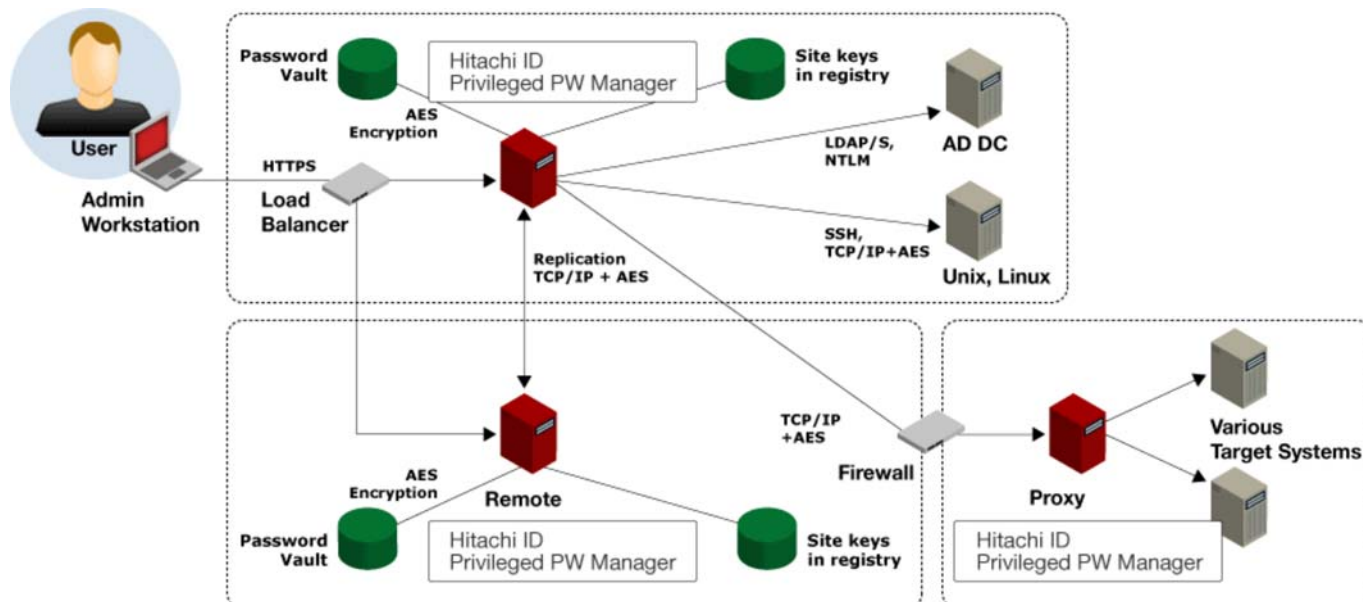
日立 ID 特権パスワード・マネージャーには、イベント報告機能があり、誰がどの資源に対してパスワードを開示したか、パスワードがどれだけの頻度で開示されたか、いつどのようにしてターゲットシステム上でパスワードが変更されたか、ユーザーがどれくらいの頻度で日立 ID 特権パスワード・マネージャーにサインインしようとしているか、その認証試行の結果はどうかなどの情報を見ることができます。

キーとなるシステムへの管理的なアクセスを記録する必要があるったり、また、あるケースでは、アクセスに対して、複数の人の許可が必要な場合があります。日立 ID 特権パスワード・マネージャーは、プライバシー保護情報や、財務データを含んでいるセンシティブシステムへのアクセスを制限したり、記録することが出来ます。 この制御機能は、HIPAA、SOX、PCI他の規定に準拠するのに役立ちます。

## 日立 ID 特権パスワード・マネージャー アーキテクチャー

### ネットワークアーキテクチャー

図 [link] は、典型的な日立 ID 特権パスワード・マネージャーの活用におけるネットワークコミュニケーションパスを示しており、日立 ID 特権パスワード・マネージャーがパスワードをターゲットシステムや、アプリケーション、ネットワーク機器などにプッシュする様子を示しています。



日立 ID 特権パスワード・マネージャー プッシュモード・ネットワーク・アーキテクチャ・ダイアグラム

この図では、:

- 三つの異なる物理的なサイトが示されており、それぞれは、破線で囲まれています。
- 二つの日立 ID 特権パスワード・マネージャーサーバーが二箇所に展開されています。ハードウェア障害、または、どちらかのサイトの停電を想定して、リアルタイムの複製を提供します。
- 日立 ID 特権パスワード・マネージャーサーバーは、Windows 2003 または、Windows 2008で動作します。このふらっとフォームは、最も広範なクライアントソフトウェアを提供しており、日立 ID 特権パスワード・マネージャーが多種のターゲットシステムとのインテグレーションを可能とします。
- 格納されるパスワードは、暗号化されます(AESを利用)。暗号キーは、各日立 ID 特権パスワード・マネージャーサーバーのレジストリに保管され、それ自身が日立 ID 特権パスワード・マネージャーソフトウェアに組み込まれたキーで暗号化されます。
- 各日立 ID 特権パスワード・マネージャーサーバーは、すべての構成情報とともにすべてのパスワードデータベースの完全な、ローカルコピーを持ちます。
- データの複製のための二つのサーバー間のやり取りは暗号化され、中間に介在しうる攻撃からの覗き見や、改竄を防止します。
- 定期的に、各日立 ID 特権パスワード・マネージャーサーバーは、ターゲットシステムにつながり、新規のパスワードをプッシュします。ターゲットシステムによって、用いられるプロトコルは異なります。二つの例を挙げると:Windowsサーバーでは、LDAPSかNTLM、UnixまたはLinuxサーバーではSSHを用い、SSHサービスがないけれど、ローカルな日立 ID 特権パスワード・マネージャーリスナーを持っているUnixターゲットには、暗号化TCP/IP接続を用います。
- いくつかのターゲットシステムには、ファイアウォールの介在により直接接続することができません。このような場合には、ターゲットシステムと同じ場所にある日立 ID 特権パスワード・マネージャープロキシサーバーを用いて間接的に接続します。このやり方では、主日立 ID 特権パスワード・マネージャーサーバーからターゲットシステムへのコミュニケーションは、専用番号によるTCP/IP接続と共有キーを用いたAES暗号を介して行われます。この接続では、プロキシから、ターゲットシステムのネイティブプロトコルを使ってターゲットシステムに、伝えられます。
- 日立 ID 特権パスワード・マネージャークライアント、例えば、IT従事者や埋め込みのパスワードの変わりに日立 ID 特権パスワード・マネージャーを用いるアプリケーションは、日立 ID 特権パスワード・マネージャーとHTTPSで接続します。複数の日立 ID 特権パスワード・マネージャーサーバーが存在し、各々が完全なデータを持っているため、この接続は一般的にロードバランスが適用されます。

## プッシュモードとプルモード

日立 ID 特権パスワード・マネージャー は、サーバーパスワードを"プッシュモード"で、ワークステーションを"プルモード"で管理します。:

サーバーのパスワードを管理する場合、日立 ID 特権パスワード・マネージャーは、通常 "プッシュモード" で操作を行います。つまり、日立 ID 特権パスワード・マネージャーサーバーは、日立 ID 特権パスワード・マネージャーサーバーにローカルにインストールされているエージェントプログラムを使って各ターゲットシステムと定期的にコミュニケーションを開始し、ターゲットシステムの管理者パスワードをランダム化します。

新しいパスワードは、暗号化され、ITスタッフがアクセスすることのできる日立 ID 特権パスワード・マネージャーサーバーの複製ストレージに保管されます。

ワークステーション上のパスワードを管理する場合、日立 ID 特権パスワード・マネージャーは、通常"プルモード"で操作します。これでは、ローカルエージェントが各ワークステーション上にインストールされ、このエージェントソフトウェアが定期的に、HTTPSを用いて、中央の日立 ID 特権パスワード・マネージャーサーバーと通信し、新しい管理者パスワード要求を行います。

同じアプローチがワークステーションだけでなく、多種に渡る、散発的にしかネットワーク上でアクセスできないいなるタイプの装置に対しても取られます。例としては、Windows または、Unixサーバーの"サーバーファーム"や、リモートロケーションにあるターゲットシステムなどです。

一度、ローカルパスワードが設定されると、確認が新しい値を格納している日立 ID 特権パスワード・マネージャーサーバーに送られます。この新しいパスワードは、ITスタッフがアクセス可能な日立 ID 特権パスワード・マネージャーの重複ストレージに暗号化され格納されます。

### 日立 ID 特権パスワード・マネージャー ホストプラットフォーム

日立 ID 特権パスワード・マネージャー は、Windows 2003 または、Windows 2008 サーバーにインストールする必要があります。

Windows 2003または、Windows 2008にインストールすることで、日立 ID 特権パスワード・マネージャーは、"Wintel"プラットフォームだけに用意されているほとんどのターゲットシステムに対するクライアントソフトウェアの恩恵にあずかることができます。言い換えれば、日立 ID 特権パスワード・マネージャーでは、サーバー側にエージェントをインストールすることなく、ターゲットシステムのパスワードやアカウントを管理できることを意味します。

日立 ID 特権パスワード・マネージャー サーバーは、ウェブサーバーとともに構成されなくてはなりません。日立 ID 特権パスワード・マネージャーアプリケーションがCGI実行可能形式で実装されているため、いかなるウェブサーバーでも機能します。日立 ID 特権パスワード・マネージャーインストールプログラムは、自動的にIIS, Apache, Sun ONE ウェブサーバーを認識し、構成を行います。

日立 ID 特権パスワード・マネージャー は、セキュリティサーバーで、それに相応しくロックダウンされなくてはなりません。日立 ID 特権パスワード・マネージャーをそのようにするための詳細は、日立 IDドキュメントを参照ください。簡単に述べると、ネイティブWindowsサービスは、わずかなアタックサーフェイス、つまりたった一つのTCP/IP(443)インバウンドポートを残してを、リムーブされ、またはされるようにしなければなりません。:

- a. IISは必須ではありません (Apache は、適当な代替となります。)
- b. ASP, JSP または PHP は用いられていません。したがって、これらのエンジンは不活性化することが出来ます。
- c. .NET はウェブUIのために必須ではありません。従ってIIS上では不活性化することができます。
- d. ODBCやDCOMは、インバウンドの必要はなく、これらのサービスは最低でも フィルターされなくてはなりません。
- e. File 共有も不活性化しなくてはなりません。
- f. リモートレジストリサービスも不活性化しなくてはなりません。
- g. インバウンドコネクションは、ポート443とターミナルサービス(特定な構成タスク用に)以外はフィルターするようにします。

日立 ID 特権パスワード・マネージャー は、安全を配慮して設計させています。複数階層のセキュリティアーキテクチャを採用しており、堅牢なOS上での動作、ACLsファイブシステムの利用、堅固なアプリケーションレベルのユーザー認証、ユーザーインプットのフィルタリング、重要データの暗号化、アプリケーションレベルのACLsの強制、無期限のログデータの蓄積 などの対策を講じています。

日立 ID 特権パスワード・マネージャー は、プレーンテキストパスワードを構成ファイルやスクリプトに格納するようなことはしないばかりか、プレーンテキストパスワードはどこにも格納されるようなことはありません。日立 ID 特権パスワード・マネージャー は、インストール時に入力が必要とする、デフォルト管理パスワードと一緒に出荷されるようなこと

もありません。

これらのセキュリティに関する対策を図4. [link] に示します。

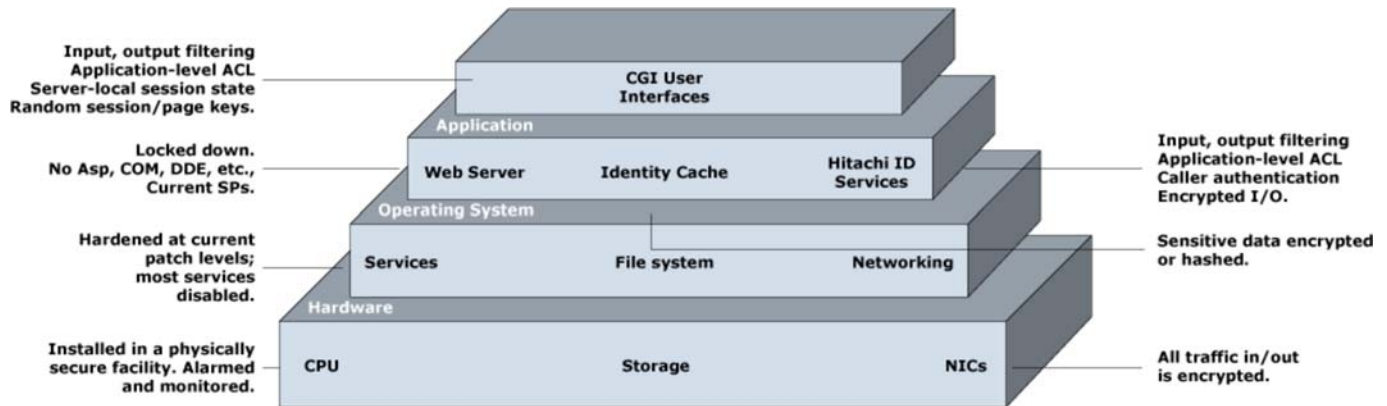


図4. ネットワーク・アーキテクチャ・セキュリティ・ダイアグラム

### サポートするターゲットシステムのタイプ

日立 ID 特権パスワード・マネージャーは、次のオペレーティングシステムでは、日立 ID 特権パスワード・マネージャーサーバークラスターから新規の、ローカル管理者パスワードを入手(プル)する前提で、クライアントソフトウェアを同梱しています。:

- a. Windows 2000, XP, Vista, 2003 及び 2008
- b. Unix 及び Linux

Windows のブルモードサービスは、Windows サービスコントロールマネージャーとIIS上でパスワードを更新するプラグインを含んでいます。他のプラグインの追加は容易です。


日立 ID 特権パスワード・マネージャー・サーバーにインストールされ新しいパスワードを固定アドレスのターゲットシステムに書き込むために開発された、プッシュモードエージェントには、次のものがあります。:

ディレクトリー	ファイル/プリント	メインフレーム
LDAP (any), Active Directory, Windows NT domains, Novell eDirectory, Novell NDS, Unix NIS and NIS+, Kerberos/DCE (any)	Windows NT/2000 /2003/2008, Novell NetWare, OS2 LanManager, Samba	MVS / OS/390 / zOS, RACF, CA-ACF2, CA-TopSecret, VM/ESA, Siemens BS2000, Tandem NonStop, Unisys MCP
Unix	ミッドレンジ	データベース
AIX, DGUX, Digital Unix, HPUX, IRIX, Linux, NCR, OSF4, SCO OS, Solaris, SunOS, Tru64, UnixWare, Unisys, passwd, shadow, Trusted Computing Base	HP MPE, OS/400/iSeries, OpenVMS	DB2/UDB, Informix, MSSQL, ODBC, Oracle, Sybase
ERP	メッセージング	WebSSO
SAP R/3 4.0+, PeopleSoft 7.5+, Oracle Applications 11i+, JDE OneWorld	MS Exchange 5.5, MS Exchange 2000/03/07, Novell GroupWise, Lotus Domino/HTTP, Lotus Notes/ID files, HP OpenMail	IBM TAM, RSA ClearTrust, Entrust getAccess, CA SiteMinder, Oracle COREid, SAP portal
フレキシブルエージェント	ハードウェアトークンとスマートカード	その他

API (application programming interface) integration, LDAP attributes, MQ Series, SQL commands, Telnet/TN3270 /TN5250 sessions, Unix/Windows cmd-line integration, web forms, web services (SOAP, XML)

RSA SecurID, Secure Computing SafeWord, Vasco Digipass, GemPlus, Precise Biometrics

BMC Service Desk Express, Clarify eFrontOffice, Connected Backup, IBM OLAP, IBM Tivoli Access Manager, Local and cached Windows passwords, HP ServiceCenter, RADIUS (various), BMC Remedy ARS and Tivoli ADSM,

 **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](http://www.Hitachi-ID.com)