

---

特権パスワード管理のベストプラクティス



## はじめに

本書は、特権パスワード管理システムに関連したビジネス上の問題について記述しています。その後、パスワード管理、特権アカウントのパスワード管理、特権パスワードを安全に格納する方法、パスワード開示、特権ログインセッションの実行方法等を行うためのポリシー定義、施行について説明していきます。

特権アカウントは、管理者用アカウント、サービスプログラムを実行させるアカウント、他のシステムに接続するために使われる埋め込まれたアカウントを含みます。

日立 ID 特権パスワード・マネージャーは、多数のシステムに跨る特権アカウントへのアクセスに関するポリシーの定義、施行を可能にしたセキュリティ製品です。この製品により、企業は、特権アカウントにアクセスできるユーザーとプログラムの指定、いつアクセスの許可するか、どのようにアクセス有効、無効にするかなどの条件をコントロールすることができます。全てのアクセスは作業履歴に残され、監査報告の対象となります。

本書の大半は、一般的なもので、他社の特権パスワード管理システムにも該当します。日立 ID 特権パスワード・マネージャーに限定した内容は、その旨を記述しています。:

文書内でベストプラクティス例は以下の  マークで表示されているので参照ください。

## リスクマネージメント

### 基本的なリスク

企業は日々のITオペレーションにおいて、従来にないレベルのセキュリティ問題に直面しています。例えば多数のシステム管理者が、数千もの機器に跨った特権アカウントのパスワードを共有しているかもしれません。このような場合、システム管理者の誰かが退職した後もパスワードは変更されず、同じパスワードを引き続き使用していることが多々あります。このため元職員や元契約社員よってのシステムへの不正侵入、データ改変などの攻撃を受けるリスクを高めてしまいます。

管理者用アカウントに関するその他のセキュリティ問題:

- ▶ 複数の管理者が1つの共通のパスワードを使用している場合、一時的であってもパスワードを必要とする管理者にとって使用不可能な状態にならないように変更の調整を行うことが難しくなります。
- ▶ 管理者用アカウントがロックアウトしてしまうことは、大惨事につながる恐れがあります。そのような事情から、管理者用パスワードは定期的な変更、または不正侵入をロックアウトするポリシーの適応外となっている場合がよくあります。このため管理者用パスワードの安全性がユーザーパスワードよりも低い場合があります。:

特権アカウントのアクセス権を複数の管理者で共用している場合、変更を行った管理者を特定する事は不可能です。このようなアカウントビリティに欠ける状況は、内部統制要件から逸脱してしまう可能性があります。

企業の中には重要なパスワードを定期的に変更し、パスワードを書き留めて金庫に保管、管理している場合もあります。このような方法は安全なように思われますが、様々なビジネスリスクを引き起こす可能性があります。:

- ▶ 業務時間外に管理者がシステムの修理を依頼された場合、容易に特権パスワードにアクセスすることが出来ません。これでは、システム管理者が迅速、かつ効率的にシステムの問題を解決する能力を大きく損なうことになりかねません。
- ▶ 特定の地域で地震、台風、火災、水害などの大災害が起こり、その地域のオフィスが災害の影響を受けた場合、他のオフィスで特権パスワードを使用できなくなる可能性もあり、業務への被害をさらに拡大させる恐れがあります。

ITシステム管理者が使用する特権アカウントに加え、他のアプリケーションに接続する為に 使われる特権アカウントがあります。例えば、多くのウェブアプリケーションは、データベースや ディレクトリ、またはウェブサービスに接続する際にログインIDとパスワードを必要とします。これらのアカウントは、それぞれ独自のセキュリティリスクを持っている可能性があります。:

- ▶ 埋め込みパスワードは、暗号化されていないテキストファイルで格納されている場合がよくあります。不正アクセス者によって、アプリケーションがインストールされているオペレーティングシステムのセキュリティが破られた場合、アプリケーションが常時接続されているネットワークサービスの健全性が同時に失われてしまいます。

迅速な処理を行い、フォールトトレランス(耐故障性)を高めるために、アプリケーションは複数のサーバーに複製されていることがあります。その場合、ログインIDとパスワードのコピーを複数のアプリケーションサーバーがプレーンテキストで格納していることとなります。このため、バックエンドシステムと複数のフロントエンドシステム間で毎回変更を調整しなくてはならないため、パスワードの変更が非常に難しくなります。

最後に、バックグラウンドプロセスが起動しているWindowsシステムも、ログインIDとパスワードによって実行されます。サービ

スアカウント、スケジュールされたタスク、ウェブコンテンツへの匿名アクセス等が含まれます。多くのアプリケーションは、上記のサービスに特権が与えられた時のみに実行可能になります。この状況も、以下のビジネスリスクを発生させます：

- ▶ サービスアカウントがローカルシステムアカウントの場合、サービスパスワードを変更する際はこのアカウントを使用する全てのサービスとの調整が必要になります。多くのWindowsのコンポーネント(Service Control Manager, Windows Scheduler, IIS、サードパーティ製ソフトウェア等)にその影響が及ぶ為、パスワード変更は困難になります。
- ▶ サービスプログラムをドメインコントローラ上で実行したり、Active Directory証明書を使用して実行する場合、1つのパスワード変更の際でもActive Directoryドメインに参加するコンピューターのWindowsコンポーネントに、新しいパスワードの通知をする必要があります。

上記の各ケースにおいて、リスクは、次のように要約することができます：

- ▶ . 脆弱なパスワード管理とは、最もセンシティブな情報であるパスワードが嚴重に保管、保護されていないことを言います。
- ▶ 複数のユーザーとプログラムとの間で、最もセンシティブな特権パスワードの変更を調整することは技術的に困難です。
- ▶ 機密性の高いデータであるパスワードを安全に管理しなければ、企業はセキュリティに関する脆弱性を露呈することになります。
- ▶ 特権パスワードを保管する堅固なマニュアルコントロール(手動制御)は、時として予期せぬリスクを発生させてしまう場合があります。例としてあげられるのが、ITオペレーションにおけるサービスレベルの低下、一箇所で起こった災害による企業全体への物理的被害拡大などです。
- ▶ システムの変更を行った管理者を特定できないということは、内部統制要件を逸脱する可能性があります。

### 特権パスワードを安全に格納する方法

特権パスワード管理システムは、上記で説明した基本的なリスクの回避に役立ちます。：

- ▶ 特権アカウント用のパスワードは定期的にランダム化されます。そのため、平文のテキストファイルでのパスワード共有、または保管することが出来なくなります。
- ▶ アクセス制御ルールとワークフロープロセスを組み合わせることによって、特権アカウントへのシングルイベントとマルチイベント両方のアクセス開示のサポートします。
- ▶ 特権アカウントのアクセス要求、承認、またはアクセス権を取得する前に、ITスタッフは個別に認証されます。これによって、特権アカウントを使用して何らかの変更が行われた際のアカウンタビリティを確立することができます。
- ▶ アクセス開示は様々な形式で行われます。必ずしもユーザーにパスワードを表示するということではありません。




パスワード変更は、バックエンドシステムとそれを使うプログラム(フロントエンドシステム)間で調和して行われます。

### 特権パスワード管理自動後の新たなリスク

特権パスワード管理システム導入後の基本的なリスクは本書で説明していますが、今後起こりうる新たなリスクも考慮しなければなりません。：

- ▶ 特権パスワードを管理するデータベースの情報漏洩によって、不正アクセス者が特権IDを使用できるユーザーになりますことも出来るため、企業は多大な被害にあってしまう可能性があります。
- ▶ 特権パスワード用データベースへの損害や、データベースへのアクセスができなくなった場合、管理者が全てのシステムからロックアウトされてしまい、企業全体に係わる業務に多大な悪影響を及ぼしてしまうこともあります。

### 特権パスワード管理システムの保護

- ▶ 特権パスワード管理システムのデータベースは、情報漏洩を防止するために保護する必要があります：
  - 特権パスワード管理システムは、最小限のサービスの実行、物理的に安全な場所に置く、コンソールへの管理者用アクセス権の取得を最少人数に抑える、など、安全なプラットフォームにインストールする必要があります。
  - 全ての機密なデータ、特に格納されているパスワードは暗号化する必要があります。
  - 暗号鍵は、堅固に保護しなければなりません。
  - 認可に関するポリシーでは、特権パスワード管理システムにログインできるユーザーを特定し、どのユーザーがどの特権アカウントへのアクセスを取得できるかを統制しなければなりません。
  - ワークフローのルールでは、異例のアクセス要求では、アクセス権が付与される前に、必ず認証、確認、認可されるよう制御する必要があります。
- ▶ 特権パスワード管理システムは、全体的に可用性を高めるようにデザインしなければなりません：
  - 障害誘発箇所がないこと：
    - システムのデータベースは、最低2台のサーバーで複製される必要があります。

- 複数の特権パスワード管理サーバーは物理的に異なったサイトに設置しなければなりません。それにより、一箇所で自然災害が起きた場合でも、他の場所から特権パスワードにアクセスすることが出来ます。
- 一箇所のパスワード管理システム、またはデータベースがオフラインの場合、承認されたユーザーには別の箇所からアクセス開示を行うことが出来ます。
  - 新規のパスワード値が複製されていない場合は、パスワード変更は延期されます。1つのサイトのみでパスワード値を保管することは、障害箇所を発生させる恐れがあるからです。
- パスワードの変更プロセスは、競合状態を防がなければなりません。✔
  - ターゲットシステム上でパスワード更新が失敗した場合には、データベースに新規パスワードが保管されるようなことがあってはなりません。
  - パスワード更新が成功したか判断できない稀なケースに対処するため、データベースに新旧両方のパスワードを保管する必要があります。
- パスワードの変更プロセスは、バックアップメディアからのシステム回復をサポートしなければなりません。
  - システムのバックアップコピーが必要となる場合に備えて、長期間使用されていない古いパスワードも履歴テーブルに残しておくべきです。

## サーバーインフラストラクチャー

このセクションでは、どのように特権パスワード管理システムを構成し、どのように高可用性、高拡張性をサポートしていくのか説明します。

### サーバーの台数と配置

特権パスワード管理システムは、基本的に2台以上の、出来れば物理的に異なる場所に設置されたサーバーに導入する必要があります。このような配置によりコンポーネントの障害によるシステム障害を防止します。✔

- 1台のサーバー上でのハードウェア障害
- ユーザーと1台のサーバー間のネットワーク接続障害：
- 物理障害、ネットワーク故障、停電などにより、サイト全体の断絶

複数のサーバーでは、ほぼリアルタイムでのデータの複製を行うべきです。サーバー数が増えると、複製のためのトラフィック量も増加します。サーバーは物理的に異なる場所に設置されているため、複製トラフィックはWAN回線上に転送されます。最低2台のサーバーが必要ですが、逆にサーバーが多すぎる場合はシステム全体のパフォーマンスを著しく低下させることになります。このため複製した特権パスワード管理用サーバーの設置は3台以下とすることを推奨します。✔

次の課題は、ネットワーク上でのサーバーの設置場所です。全く同一のネットワークポロジリーは存在しないため、ここでは一般的なガイダンスを示します。：

- 複製によるパフォーマンス低下を最小限に抑えるために、複数の複製されたサーバー間の接続速度は高くなければなりません。
  - パスワード管理用サーバーは、高帯域幅を持つWANに接続されたサイトに設置する必要があります。✔
- パスワード管理サーバーとそれが管理するパスワードの対象機器間の接続は高速でなければなりません。システムの中には、低帯域や、遅延時間が長い場合に、パスワード更新プロトコルが機能しない場合があるためです。
  - このため、パスワード管理サーバーは、主要データセンターでは、出来るだけ管理対象システムのそばにインストールする必要があります。✔
- エンドユーザーとパスワード管理用サーバー間の接続は、通常、低帯域帯、長い遅延時間に対応できるHTTPSを使用して、行われます。
  - つまり、パスワード管理サーバーは、ユーザーと同じ場所に設置する必要はなく、ターゲットシステムの近くに設置することが、より重要になります。✔

### データベースの種類と配置

上記の説明は、他社の特権パスワード管理システムにも該当しますが、この後の記述は日立 ID 特権パスワード・マネージャー に限定した内容です：

- > 日立 ID 特権パスワード・マネージャーは2種類のデータベースをサポートします：
  - Microsoft SQLサーバー（現在のサポートバージョン：2005）とOracle サーバー（現在のサポートバージョン：10g）
  - “Enterprise”と無償の “Express”エディションの両サーバーをサポートします。
  - 特権パスワード管理システムの重要性から、MicrosoftまたはOracle社からのサポートを受けられない “express”バージョンのデータベースをプロダクション環境で使用することはお勧め致しません。
  - Microsoft、Oracleデータベースの選択は、企業の規範に基づくべきです。Windows サーバー上にSQL Serverを設置している企業はSQL Serverを使用すべきであり、ミッション・クリティカルアプリケーションとしてOracleデータベースを好む企業は、Oracleデータベースを使用するとよいでしょう👍。
- > 企業/組織は次のようなオプションを採用することもできます。：
  - 日立 ID 特権パスワード・マネージャーアプリケーションと同じサーバー上に、データベースサーバーのソフトウェアをインストールする(図1参照 [\[link\]](#))； または
  - IDARCHIVEアプリケーションサーバーに物理的かつ論理的に近い場所に設置した専用サーバーに、データベースサーバーソフトウェアを、インストールする(図2 [\[link\]](#))； または
  - 既存の複製 “Enterprise規模”のデータベースサーバーを活用し、各日立 ID 特権パスワード・マネージャーサーバーを構成し、既存のインフラストラクチャに接続するように構成することができます(図3 [\[link\]](#)を参照)。

[ppm-config-1]

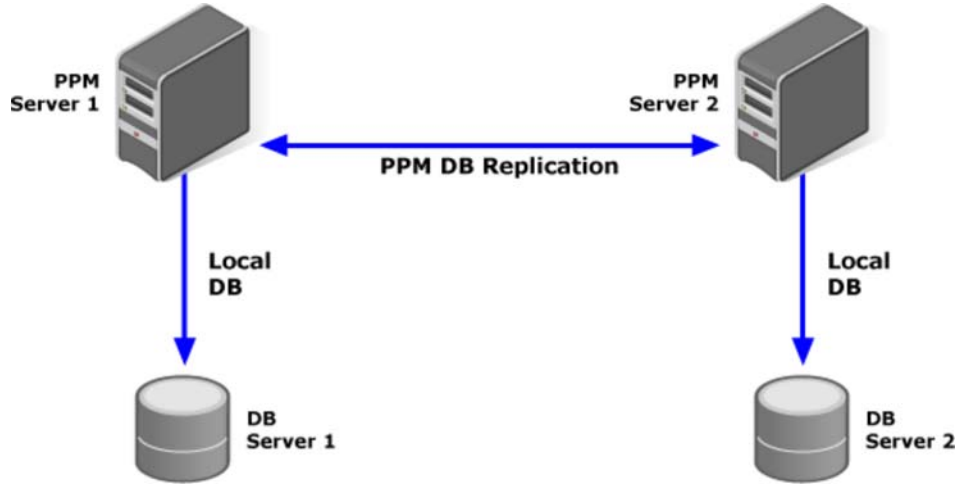


図1： 2台の\_IDARCHIVEPPMサーバーがそれぞれのデータベースをホストしている

[ppm-config-2]

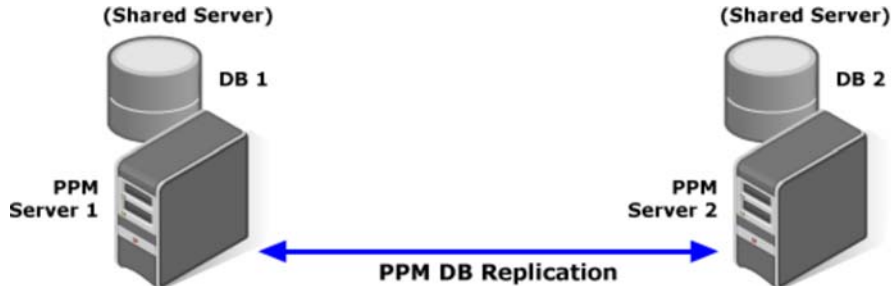


図2： 2台のPPMサーバーに加え、2台のデータベースサーバーを使用

[ppm-config-3]

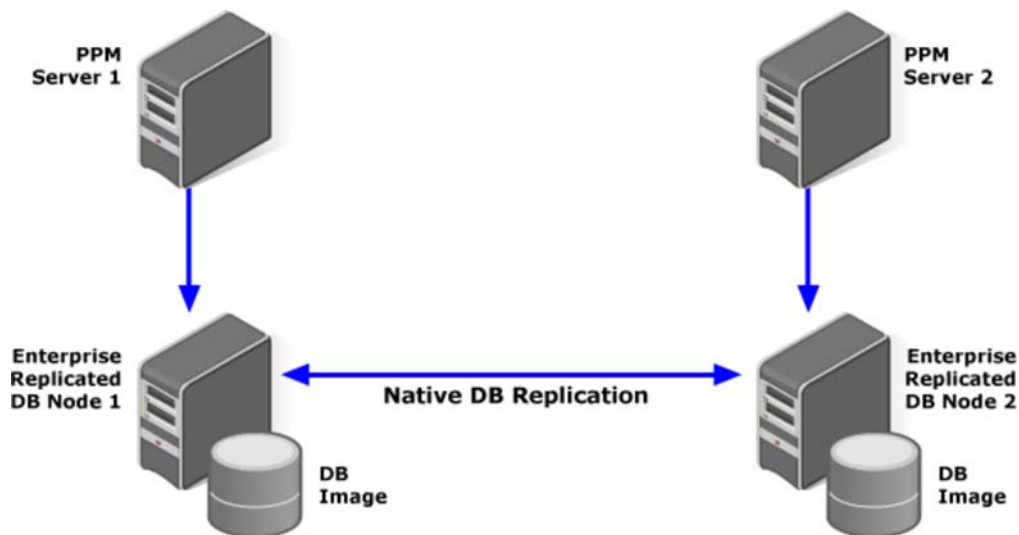


図3: 共有のデータベースインフラストラクチャに接続された2台のPPMサーバー

- > 上記3通りの構成は、全て技術的に実現が可能です
  - 物理的に異なるデータベース・インスタンスを持つ日立 ID 特権パスワード・マネージャーサーバーの構成は、障害箇所 (Enterpriseデータベースのインフラストラクチャおよび、またはインフラストラクチャへの接続性は単一障害点を構成) を減らし、信頼性を高めます。
  - 日立 ID 特権パスワード・マネージャーに物理サーバー (非仮想サーバー) 用いている場合、日立 ID 特権パスワード・マネージャーソフトウェアとデータベース間でハードウェアを共用することによりハードウェアコストを削減することができ、その際のパフォーマンスの低下は10%から20%に留まります。
- > 日立 ID 特権パスワード・マネージャーデータベースを日立 ID 特権パスワード・マネージャーアプリケーションサーバーと別に設置する場合は、同じネットワークセグメント上に設置する必要があります。
  - これにより、アプリケーションとデータベース間での通信遅延を低減させ、結果的には実行時のパフォーマンスを向上させることができます。

## ファイアウォールの使用

特権パスワード管理システムは、機密情報の開示を制御する機能を持っています。このとき、使用する場合はどのようにファイアウォールが管理システムのセキュリティ強化の為に、ファイアウォールを使用すべきか、また使い場合どのようにファイアウォールを構成すべきかの課題が残ります。

エンドユーザーと特権パスワード管理システム間にファイアウォールを設置するのが一般的な方法です。ユーザーインターフェイスをポートTCP/IP 443上のHTTPSで使用する場合、インバウンドコネクションをポート443のみに制限するのが直接的な方法です。

さらに、アプリケーションレベルのファイアウォール (リバースウェブプロキシとして構成) は:

- > 任意でユーザーからのSSL接続を切断することができます。
- > 外部からの通信をチェックし、不当なHTME形式のペイロード、クッキー等をブロックします。

特権パスワード管理システムとパスワード管理対象機器間において、ファイアウォールを使用することも可能です。各ターゲットシステムは異なったプロトコルを使用することもあるため、特権パスワード管理システムが開始した接続は許可し、その他のシステムが開始した接続はブロックするようにファイアウォールを構成する事も可能です。

最後に、特権パスワード管理システムとその内部のデータベース間にファイアウォールを設置することは、以下の理由で推奨しません:

- > 特権パスワード管理システムは、パスワードの格納と開示、設定の変更等を行うために無制限のデータベースアクセスを必要とするので、ほとんどまたは全くセキュリティ上の恩恵がないことがあげられます。
- > 性能、信頼性の問題が発生する可能性があります。例えば、非アクティブのデータベースへの接続をファイアウォールが間違っって切断する恐れがあります。その場合、特権パスワード管理システム上で行われるさまざまなアクティビティは、このエ

ラー状態の影響を受けることになります。このような問題の原因を 解明することは容易ではありません。  
 複数の日立 ID 特権パスワード・マネージャーサーバーを保護する理想的なファイアウォールの設定は、図4 [\[link\]](#)を参照して下さい。

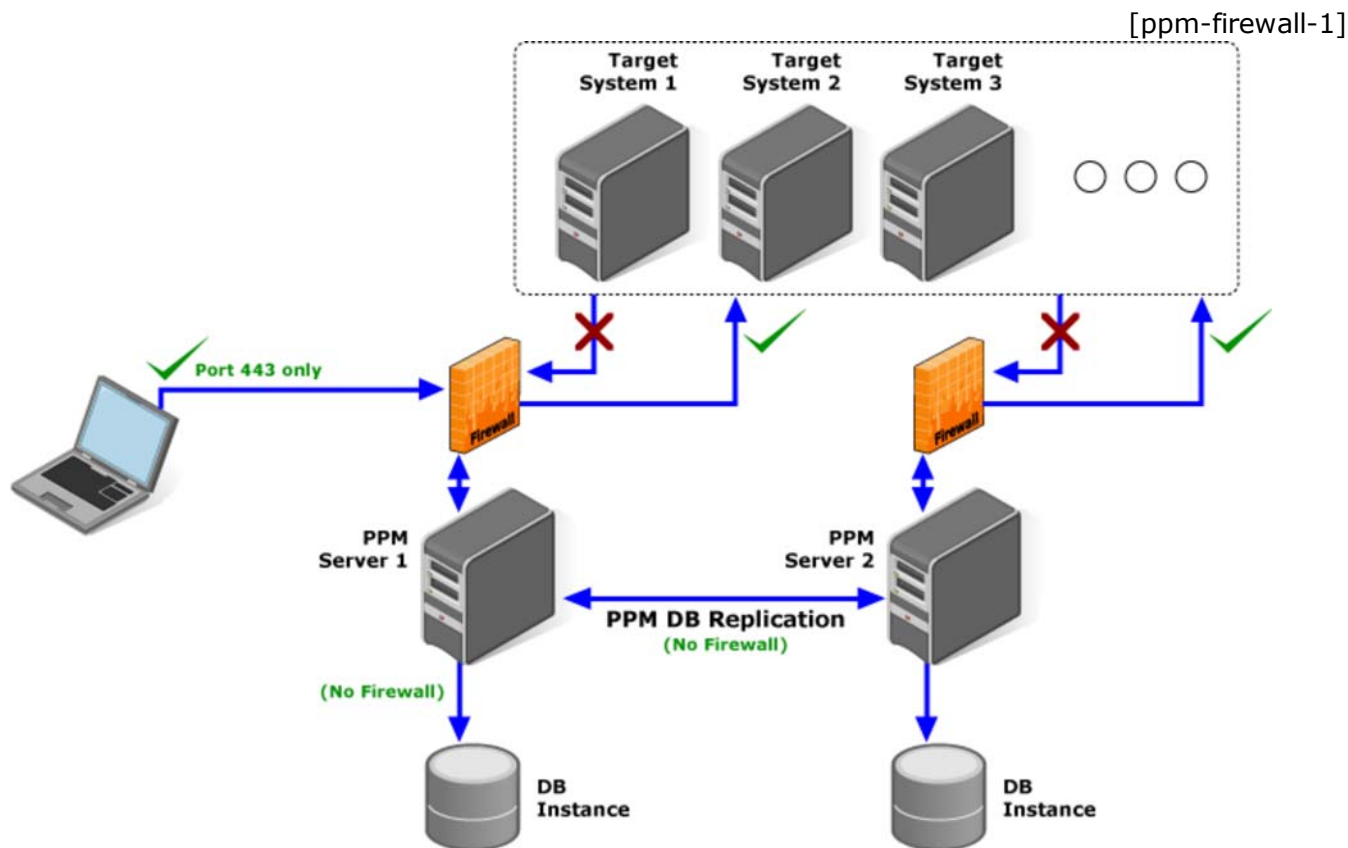


図4： 日立 ID 特権パスワード・マネージャーサーバーをファイアウォールで保護する方法

## 仮想サーバー 対 物理サーバー

以下の説明は、日立 ID 特権パスワード・マネージャー限定の内容です：

- ▶ 日立 ID 特権パスワード・マネージャーは、VMWare ESX servers等のバーチャルマシン上で既にテストを行っており、実行マシンとしてサポートしています。
- ▶ バーチャルサーバーは物理サーバーと比較すると、通常(必ずではありませんが)2倍から3倍近くのI/O性能が遅くなります。
- ▶ バーチャルサーバーに日立 ID 特権パスワード・マネージャーを設置することは可能ですが、仮想インフラストラクチャーがデータベースの稼働、自動ディスカバリ、パスワード変更、アクセス開示要求などの負荷要件に対応できることが条件となります。
- ▶ データベースサーバー(Microsoft SQL ServerまたはOracle データベース)が、仮想サーバー上で十分に機能するかという事は考慮すべき重要な点ですが、この件に関しては日立 IDではなくMicrosoft社、またはOracle社にお問い合わせ下さい。日立 IDは、“テストを行った際、ハードウェアに比べるとかなりのパフォーマンス低下が見られた。”とコメント出来るだけです。
- ▶ 上記を実践的課題として考えてみると、5千ものパスワードを毎日ランダム化するシステムは、2台の単一CPUを持つ複製バーチャルサーバー上にIDARCHIVEとSQL Serverと同時に稼働するよう構成するのが妥当です。

## ネットワークとストレージへのインパクト

日立 ID 特権パスワード・マネージャーが一つのパスワードをランダム化する度に、データベースレコード(現在のパスワード値、パスワード履歴、ログイベント等)は、Microsoft SQL サーバーで5.1キロバイト、Oracle データベースは3.1キロバイトの容量を使います。

1つのパスワード変更に約6キロバイトを必要とするので、企業が5千の特権パスワード管理を希望し、毎日パスワードの変更

を行い、3年間パスワードの保管データを保持する場合、以下の容量を持つデータベースが必要となります：

- 6キロバイト×5,000パスワード/日×365日×3年
- = 32,850,000キロバイトのデータベースディスク容量
- = 32,850メガバイトのディスク容量
- = 33ギガバイトのディスク容量

ワークフローリクエスト、システム構成等の予期しないオーバーヘッド(安全性を高めるため、要件の倍の容量を推奨)が生じることを仮定して、使用するデータベースの種類を問わず、60ギガバイトのディスクで上記のシステムを設定することをお勧めします。

Microsoft SQLサーバー、Oracle データベースのExpressエディションは、2ギガバイト以下のデータベースに限られる為、プロダクション環境ではExpressエディション(テスト、QA等にのみ 適しています)ではなく、StandardまたはEnterpriseエディション導入の必要性が非常に高くなります。

同様に、日立 ID 特権パスワード・マネージャーが変更したパスワードをサーバー間で複製する為に、1パスワード毎に1キロバイト弱の通信が行われます。上記の企業例に当てはめると、パスワード変更に伴い複製の為に使われる通信量は1日に約5メガバイトと推定することが出来ます。しかしワークフローリクエスト、ログイン監査記録、アクセスの開示等の複製が必要になる場合は5メガバイト以上必要になり、複製に使われる通信量は1日に約100メガバイトとなります。

上記の帯域幅は、サーバー間の複製のみに使用された場合です。更に日立 ID 特権パスワード・マネージャーとターゲットシステム間(パスワードをランダム化するため)やエンドユーザーと日立 ID 特権パスワード・マネージャー間(特権アクセスの要求と取得のため)で帯域幅は使用されます。：

- ADまたはUnix上で1つのパスワードのリセットをする： 約10キロバイト
- 特権パスワードシステムにログインできるようにする為、AD上の全ユーザーをリストアップする： 1,000人のユーザーに対して500キロバイト
- 自動管理が行われるように、AD上の全コンピューターをリストアップする： 1,000台のコンピューターに対し500キロバイト
- 1台のWindowsコンピューターのローカルサービスと管理者用アカウントをリストアップする：100キロバイト弱 (少数のアカウントと仮定する)
- 特権パスワード管理システムのウェブユーザーインターフェイスから特権パスワードのアクセス権を要求する： 500キロバイト弱

ネットワークへの総合的なインパクトは、上記の概算基準(予測された特権パスワードシステムのワークロードによって変化します)を基に、システムに予想される負荷を掛け合わせることで推定できます。

## サーバー規模

上記のディスカッションは、日立 ID 特権パスワード・マネージャーとデータベースをどこに配置するかを決める際に 有効ですが、各サーバーのハードウェアをどのように構成するかという課題が残ります。以下では、2010年1月におけるコンポーネントの費用を基に、コストとパフォーマンスのバランスを保つ適切な構成方法を説明していきます：

- Quad core CPU.
- 4GB RAM.
- ミラーリング設定された2つの600GB 10K RPM シリアル接続 SCSIディスク
- ギガビット(Gigabit) NIC.
- RPS冗長電源装置
- Windows 2003 standard edition.

上記のように構成された1台のサーバーは、少なくとも10万個のパスワードをターゲットシステム上で常時管理することが可能であり、同時におよそ100人のインタラクティブ性のあるユーザーセッションの サービスを行うことができます。日立 ID 特権パスワード・マネージャーウェブユーザーインターフェイスへのユーザーセッションは、通常最低約2分とすると、8時間業務日の間、このサーバーは24,000回の特権アクセスを処理できることとなります。

導入の際、データベースのレプリカと日立 ID 特権パスワード・マネージャーソフトウェアを搭載した最低2台のサーバーを設置する必要があります。各サーバーはそれぞれ別の場所にインストールします。

バーチャルマシンは、物理サーバーと同様なディスク、I/O、CPU、メモリ容量で構成します。

## ロードバランシング(負荷分散)と複製

次の課題は、2台以上の特権パスワード管理システム用サーバーを設置し、それぞれ常時アクティブである場合、両サーバーへのアクセスを可能にするには、どのようにロードバランシングの設定を行えばよいですか。

次のような様々な方法でロードバランシングを実現させることが可能です：

- 図5 [link]で複数のIPアドレス(1台のサーバーにつき1アドレス)と1つのDNS名の関連づけを示します。
  - 例えば、ユーザーが次のURL `https://ppm.acme.com/` に接続しようとした場合、DNSアドレス `ppm.acme.com` は、2つのIPアドレスの中からランダムに選んだ1つのアドレスに関連づけを行います。
- リバースウェブプロキシをロードバランシング用機器と同様に使用する方法(すなわち上記の方法と同様ですがIPレベルのプロトコルではなくTCPを使用します)を図6 [link]で示しています。
- 全ての接続要求はまず1つのIPアドレスに送られ、そのアドレスにあるネットワーク機器であるロードバランサーを使用し、負荷分散アルゴリズムを用いて複数のサーバーに接続を転送します。図7 [link]を参照下さい。

[ppm-load-balance-1]

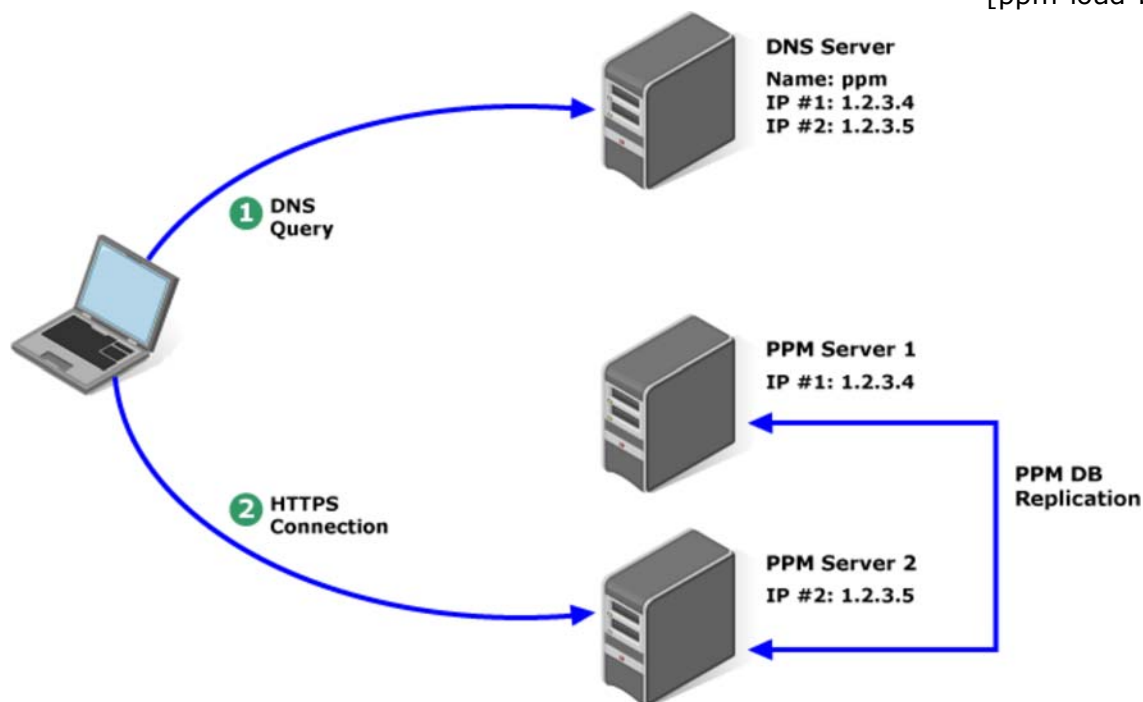


図5: 1つのDNS名を複数のIPアドレスに対応させてロードバランシングを行う

[ppm-load-balance-2]

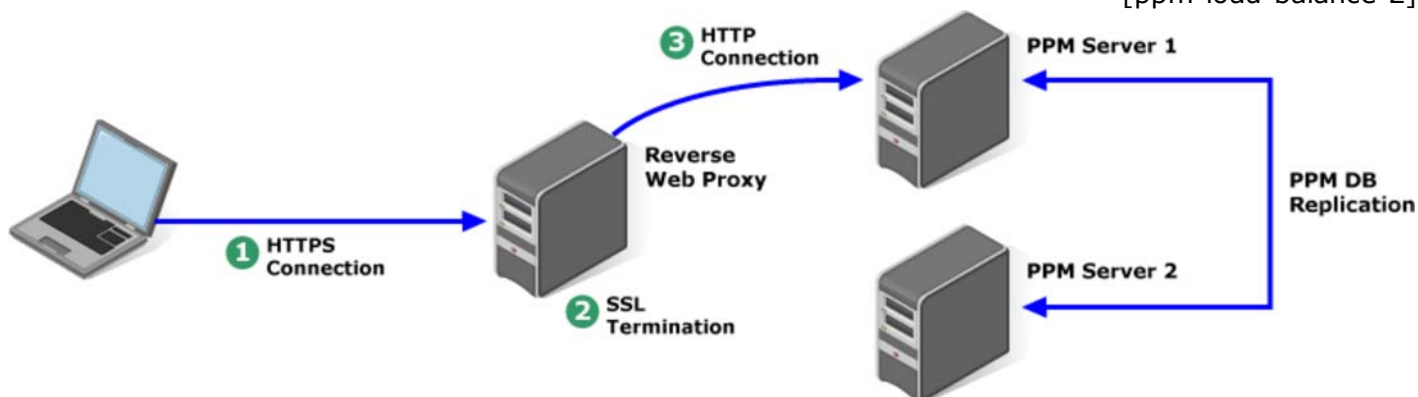


図6: リバースウェブプロキシを使用してロードバランシングを行う

[ppm-load-balance-3]

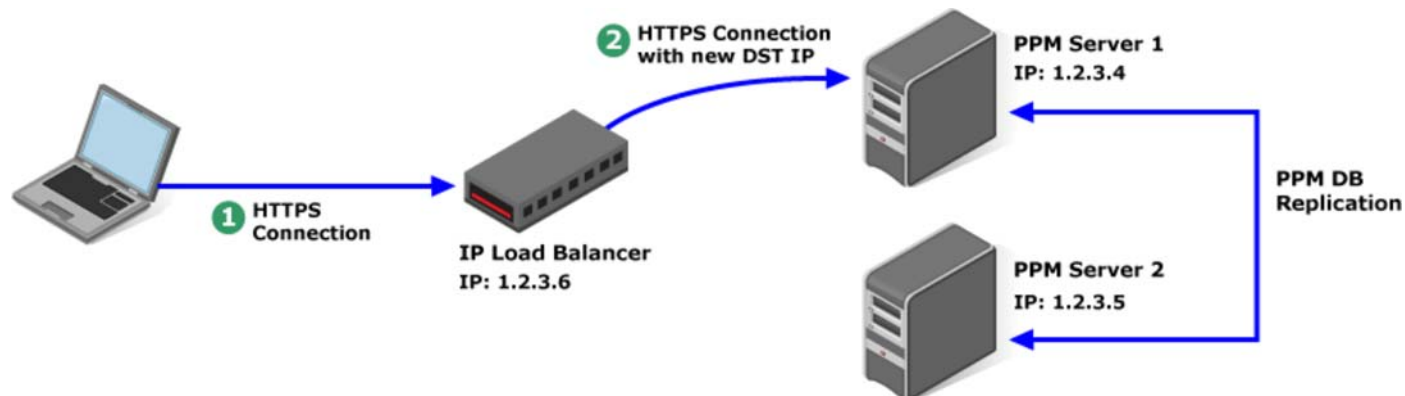


図7: 異なったIPアドレスにルーティングしてロードバランシングを行う

上記のどの方法も実現可能ですが、DNSの使用をお勧めします。使用するDNSサーバーのソフトウェアによりますが、特別のインフラストラクチャを必要としないこと、それぞれのDNSクエリから返却されたサーバーのIPアドレスがユーザーに最も近いサーバーとして選択されるように設定することが可能であるからです。

例をあげて詳しく説明していきます:

- ▶ ニューヨークとロンドンの2つのデータセンターを持つ企業があります。
- ▶ 各データセンターに、以下のDNS名とIPアドレスを持つ特権パスワード管理サーバーを導入したと仮定します。:
  - ppm-nyc.acme.com at 10.10.10.1
  - ppm-lon.acme.com at 10.20.20.1
- ▶ 両サーバーのDNS名を適切なIPアドレスに解決するようにDNSサーバーを構成します。
- ▶ ppm.acme.comへのリクエストを受信すると、ppm-nyc.acme.com、またはppm-lon.acme.comのいずれかにPTRレコードを発行するようにDNSサーバーを設定します。
  - DNSクライアント(ロンドンまたはニューヨーク)のIPアドレスに基づいて、どちらにPTRレコードを発行するかの最適化を行います。
  - 一方のPPMサーバーがオフラインだった時のために、ニューヨークのユーザーはppm-lonに、ロンドンのユーザーはppm-nycにそれぞれリクエスト出来るようになっています。
  - 全サイトがオフラインの場合、デフォルトである負荷分散アルゴリズムがアクセス可能なローカル日立 ID 特権パスワード・マネージャーサーバーに対応づけを行います。

どの負荷分散技術を使うかに関らず、クライアントとPPMサーバ間でのセッションは"固定"される必要があります。。すなわちセッション中は、常時同じPPMサーバーの使用が不可欠です。これにより複数のPPMサーバー間でセッションデータの複製を行う必要がなくなるため非常に重要になります。✔

## 特権パスワードをいつ、どのようにランダムマイズするか

特権パスワード管理システムの目的は、定期的の特権パスワードをスクランブル化することにより安全に管理することです。ユーザーまたはプログラムが実際にパスワードを必要とするまで現在のパスワード値は開示されず、パスワード開示の際には承認が必要となり、その記録が残ります。

次の問題点が挙げられます: いつパスワードはランダムマイズされ、ランダムパスワードはどのように構成されるべきでしょうか。

- ▶ パスワード変更と、安全性の高いランダムパスワード値は、ディスクスペースやネットワークの帯域幅をさほど使用しません。そのため特権パスワードの変更は頻繁に(例: 24時間毎に)行うことが 適切です。✔
- ▶ 以下の場合はパスワード変更を行うべきではありません: ✔
  - ユーザーまたはプログラムがパスワード使用中である場合
  - 例えばネットワークがダウンしている場合など、新しいパスワード値の格納を複製する事が出来ないため、1台のサーバーに格納された新しいパスワードは障害誘発箇所になってしまう可能性があります。

- 各管理者セッション終了後にパスワード変更が行われる必要があります。例えば、ある管理者がパスワードを1時間チェックアウトし、30分後にチェックインした際、特権パスワード管理システムが直ちにパスワードのランダム化を行います。この機能により、疑問のある管理者によりシステム変更が行われないことを保証し、ある管理者が使ったかが明確にわかる時間ウィンドウを縮めることができます。✔
- 簡単にパスワードを予測(人に)されたり、クラック(機械的に)を受けたりしないよう、ランダムパスワードはできるだけ長く、複雑化する必要があります。しかしパスワードは、実際にパスワードの開示が必要となった時に(例えば、物理的に分離したサーバーのコンソールにサインインする)、人が短時間に書きとめたり、タイプすることが出来る適切な長さであるべきです。
  - 例えば、16の大文字、小文字、数字で構成されたランダムパスワードは、 $4.76 \times 10^{28}$  の組み合わせがあるため、パスワード予測による攻撃を防ぐ事ができます。
  - ほとんどのシステム(IBMメインフレームを除く)この形式をサポートします。:



## アクセス開示の安全化

### 個人識別(Identification)、認証(Authentication)、認可(Authorization)

特権パスワード管理システムの役目は、特権パスワードのランダム化、その格納だけでなく、ユーザー、アプリケーション、サービスを実行するインフラストラクチャへのパスワードの開示も行います。さもなければ、パスワードが安全に格納された特権アカウントが使えなくなってしまう。







パスワード開示は制御しなければなりません:

- ユーザーやプログラムが特権アカウント(クライアント)のアクセス権を取得する場合は、あらかじめ本人識別が必要になります。
- 識別が終わると、本人であることを証明する為にクライアント認証が行われます。
- 特権パスワード管理システムは、認証済みのクライアントがどの特権アカウントへのアクセス権が許可されるかを決定します。
- 特権パスワード管理システムは、アカウントビリティの証跡を残すため、全てのアクティビティ(ユーザー確認、認証、認可、アクセス開示など)の記録を行います。

次は個人識別(Identification)認証(Authentication)プロセスのベストプラクティスを説明します。✔

- 新規のユーザー識別子とパスワードの組み合わせを使用することは、プロセスを複雑化させるためお勧めしません。
- 特権パスワード管理システム導入予定の企業が、社内でもアクティブディレクトリ等のユーザーディレクトリを既に所有しているとします。このディレクトリのユーザー識別子を有効に利用して、特権パスワード管理システムを使用するユーザー識別を行うのが適切です。
  - ADドメインが1つの場合、samAccountNameまたはuserPrincipalNameの属性が使用できます。
  - 複数のADドメインまたは他にもディレクトリを持つ場合、完全修飾されたEメールアドレスのような、ドメイン修飾された識別子が最適です。
- ユーザー(人)識別終了後、認証も必要になります。
  - 違うシステム上のログインアカウントが適切に相互関係が解決されている場合、ユーザー識別に使用されるディレクトリで認証を行う必要はありません。
  - セキュリティの水準が低い企業では、Kerberos トークンをなどの統合Windows認証 (IWA)を利用することができます。注意しなければならないのは、数時間前にユーザー認証が行われ、そのユーザーがワークステーションから離れた場合、ユーザーのスクリーンセーバーがアクティブ化され、スクリーンがロックされるまでは、ユーザーのワークステーションの物理的な場所のセキュリティレベルでしかありません。
  - 中程度のセキュリティ基準を持つ企業においては、ユーザーのアクティブディレクトリパスワードの再入力を行い (HTML形式による認証)、アクティブディレクトリ、その他のシステムまたはアプリケーション(例:LDAP、Lotus Notes、PACF、Oracleデータベースなど)の確認を行います。この場合新規の認証となるため、IWAと比較すると多少安全性が

高まります。

- 堅固なセキュリティを必要とする企業では、ワンタイムパスワード(使い捨てパスワード)と呼ばれる認証技術 (RSA SecurIなどを搭載したハードウェアトークン、またはスマートカードを使用します。これらの二ファクター認証技術は、利用時の簡易性は劣り、トークンまたスマートカードの紛失、盗難などにより、困難な条件下になる場合がありますが、なりすまし行為のリスクは低くなります。
- ♪ アクセス開示を承認する2通りの方法があります：
  - ユーザーは無期限のアクセス権を割り当てられる場合があります。例えば、あるユーザーグループは、Windowsサーバーへのアクセスが必要な際、いつでもローカルの管理者アカウントにアクセスできるように 定義される場合などです。
  - ユーザーは一時的なアクセス権を要求することもあります。例えば、プログラマーが、バージョンのアップグレード、またはプロダクションシステムの問題解決のために、プロダクションアプリケーションサーバーへのアクセスを4時間間隔で要求する場合などです。
- ♪ アクセス制御リスト(ACL)を使用することで、最も適切に無期限のアクセス権の付与を行います 
- ♪ 各ユーザーは複数のユーザーグループに割り当てられます。
  - Active Directory等の既存のシステムのオフロード(肩代わり)をさせることができる。
- ♪ 特権パスワードを管理する各サーバーは、リソース・グループに割り当てられます。
  - サーバー名、IPアドレス、OSタイプまたはパッチレベルなどのデータに基づいた標記を用いて自動化されます。
- ♪ 指定したユーザーグループは、指定したリソース・グループのリソースへのアクセス権を 割り当てられます。
  - 例えば、ADアカウントがITのメンバーであるユーザーは、リソース・グループNYCに属するサーバー上の管理者用アカウントのパスワードを引き出すことができます。
- ♪ 一時的なアクセス権は、以下のリクエストを用いることにより、適切に付与されます 。
  - 要求を行うには、要求者、アクセス権受領者、承認者の3名の構成を必要とします(兼任する場合があります)。：
    - アクセス開示の要求を記入する要求者
    - 要求が承認された場合、一時的なアクセス権受領者
    - 要求者、アクセス権受領者の識別、と要求に示されたリソースに基づき、一人もしくは複数の承認者が選ばれます。
  - 要求に対して、チケット番号、アクセスを行う時間帯などの補足情報を記載が必要な場合もあります。
  - 使用可能なサーバーのリストが社内機密、あるいは社内で高甲斐されているかによりますが、全てのユーザーがアクセス要求可能、あるいは特定のユーザーのみ可能のように設定することができます。
  - 一般的に承認者は、要求されたリソースとアクセス権受領者のアイデンティティに基づいて選ばれます。
  - 要求の承認には、特定の一人の承認者だけでなく、複数の承認者に依頼すべきです。ある承認者が多忙か不在の場合に、他の承認者が応答することが可能になるからです。
    - 例として、各リソースグループで3人の承認者を割り当て、いずれの承認者もアクセス開示を許可する権限を持たせるようにするといったことです。
  - 一人の承認者に依頼し、その応答を待つのではなく、同時に依頼を関連の全ての承認者に送ることが適切です。 
    - 例えば、アクセス権受領者の上司とリソースオーナー3人中一人からの承認が必要な場合、一度に全員に依頼することが最適です。
  - しばしば承認者が休暇、会議中等で応答できない場合も仮定されます。以下のような状況に対応できるようにすることが重要ます：
    - 招待状を送る前に、承認者のEメールのステータスが不在に設定されていないかを確認します。もし、不在だと確認出来たら、次に依頼状を送ります。 
    - 承認者が引き続き応答しない場合は、代理の承認者に依頼します。 
  - 依頼した承認者が引き続き応答しない、またはの不在の場合、代理の承認者を検索するメカニズムが必要です。 

- 一般的な方法は、承認者が不在の時は承認者の上司を招待します。
- 他の方法として、への応答が無いすべての要求をセキュリティチームに転送することも考えられます。

## アクセス開示メカニズム

特権パスワード管理システムは、通常、ITスタッフやプログラムによる特権アカウントへのアクセス制御をおこなうために構成されます。前章では、特権アカウントへのアクセスが必要なユーザーの認証と認可について説明しました。残っている問題として、どのようにアクセス開示を行うかについては以下で説明して行きます。

アクセス開示を行う方法は、数種類あります。

- ▶ 特権アカウントへのアクセスが、人のシステム管理者に開示される場合：
  - 最も簡単な方法は、スクランブル化された特権アカウント用の最新のパスワード値を表示することです。
    - この方法は、ネットワーク上でアクセスできないシステムに特権アカウントがある場合に適しています。システム管理者は、システムのコンソールにパスワードを入力しなければなりません。✔
    - ショルダーサーフィン(他人が入力しているパスワードや暗証番号などを肩越しに盗み見ること)のリスクを回避するため、パスワードが表示された後は、システム管理者の画面から短時間後に自動的に消去されるようにすべきです。✔
  - ターゲットシステムへの接続性が確立されている場合、特権パスワードの表示は避けるべきです：
    - 1つの方法としては、特権パスワード管理システムが管理者用のコピーバッファーに特権パスワードのコピーを置くことです。これにより、管理者はパスワードを全く見ることなくログインプロンプトにパスワードを貼り付けることができます。✔
    - その他の方法は、特権パスワード管理システムのユーザーインターフェイスから管理者がRDP, SSH等のリモートコントロールセッションを起動させることです。それによりユーザーはパスワードへのアクセスが必要なくなります。✔
  - 直接パスワードを表示、または管理者用のコピーバッファー、あるいはリモートセッションにパスワードを貼り付けて開示を行う代わりに、もう一つの方法としては、ターゲットシステム上で管理者の個人のログインIDに一時的な管理者特権を付与する方法があります。例えば、一時的にWindowsサーバー上のローカル管理者グループに、管理者のActive Directoryアカウントを追加する、あるいは管理者のSSH公開鍵をUnixまたはLinuxサーバー上のauthorized\_keysファイルに、ルートユーザーとして一時的に追加することです。
- ▶ サービスアカウント用パスワードが変更した場合：
  - 次回にサービスを実行するアカウントが使用された際に、プロセスを開始し、正しいパスワードが利用できるようにWindows Service Control Manager, Scheduler, IIS,またはその他のWindowsコンポーネントにおいて新規のパスワード値の更新を行なう必要があります。
  - サードパーティ製品のプロセス起動を可能にするため、拡張性のあるメカニズムが必要になります。Windowsでプロセスを開始するためには、ログインIDとパスワードが常に必要になります。
- ▶ 埋め込まれたアプリケーションアカウント用パスワードが変更された場合：
  - パスワードの変更があったサーバーに接続できるように、APIを用いて、クライアントのアプリケーションが新規パスワードを引き出せるようにする必要があります。

## 並行開示(チェックイン/チェックアウト)

特権パスワード管理システムは、複数の特権アカウントへのアクセス開示を制御できますが、何人の管理者が同時に同じ特権アカウントへのアクセス権を取得できるかといったことも制御することもできます。:

- ▶ これにより、管理者がシステム変更時の調整を適切に行わなかった際の混乱を防ぐ事ができます。
- ▶ 特定の時間内に変更を行う責任を持つ管理者の数をを限定することで、アカウントビリティを向上させることができます。

以下のベストプラクティスを参考にしてください。:

- ▶ ほとんどのシステムでは、同時には一人の管理者のみがアクセス権を持つ(ログインする)ように制限されています。それによりアカウントビリティを最大限に高め、システム構成エラーの原因となる不適当な調整を回避することができます。✔
- ▶ 頻繁に変更が行われる規模の非常に大きなシステムでは、管理者を制限する人数を2名から3名とを高く設定する必要があります。

あります。その場合、2番目の管理者がセッションを開始した際、別の管理者がセッションを行っていることを特権パスワード管理システムのユーザーインターフェイスにおいて知る必要があり、最初にセッションを開始している管理者には、EメールまたはSMSメッセージで新規セッションの開始通知を受け取るようにする必要があります。✔

並行制御を用いる場合、管理者の一人が特権アカウントへのアクセスをチェックアウトし、セッションをアクティブにしたまま、帰宅、昼食に出るなどで作業を止めた場合にリスクが発生します。最初にアクセスした管理者がセッションをアクティブにしたまま席を離れ、別の管理者が同じ時間内に同じシステムへのアクセスが必要となった場合、アクセス出来ません。このようなリスクを回避する為には、通常は1時間、最高4時間まで等の時間制限を行うことが重要になります。これにより、セッションがオープン中に不使用のために起こる、非管理期間を最小限にとどめることが可能です。

2番目に考慮する点は、特権アカウントのアクセス権を取得したユーザーにパスワードを表示する場合はどのように並行制御を施行すべきかということです。パスワードのチェックアウト時間が経過した後も、管理者がパスワードを持っていることになり、管理者セッションを確実に終了させるためには、以下を行うことが重要です。:



- ▶ 管理者がアクセス権の有効時間が切れる前チェックインした場合、または
- ▶ 許可された時間が経過した場合です。
- ▶ もし技術的に可能であれば(時に不可能な場合があります。)管理者に対しても受け入れられる方法であれば、オープンになったままの管理者とシステム (SSH等)間の接続を強制終了します。✔
- この方法は、特権パスワード管理システムが管理対象システムに接続することができ、そしてリモートでa)セッションを特定でき ?? (b)セッション強制終了を行える、場合のみ実行が可能です。
- 管理者の行う作業が予定以上の時間がかかる場合もあり、セッションを強制終了させることで作業中の仕事への影響を与える可能性もあるため、上記の方法の実行は好ましくない場合もあります。

## アクセス開示の報告

特権パスワード管理システムが基本機能の一つは、特権アカウントを共有する管理者のアカウントビリティを確立することです。(a) 全てのアクセス開示を記録すること (b)この開示についてレポートを作成すること によって行われます。

特権セッションに関する報告書は、次の2通りの方法で生成されます:

- ▶ ランダムサンプル(任意抽出法)を用いて、管理者が適切なリソース内でのみアクセスを行っているかを定期的に検証します。✔
- この方法は電車で行われる切符の点検と同じです: 車掌は数名の乗客をランダムにチェックし、全ての乗客が切符を購入しているかというコンプライアンスを確認している訳です。
- サンプルングを行う頻度は、そのリソースの重要度により変えるべきです。例えば、非常に重要なシステムにおいては、頻繁なサンプルングを行い、低リスクのサーバーではサンプルング頻度を 低くするべきでしょう。
- ✔
- なにか事象が発生した直後に行う。
- 疑わしい事象に関連した変更を行った可能性のある管理者を確認する。

次の重要な課題は、アクセス開示に関するレポート生成の権限を誰に許可するかです。報告書は、誰がどのような変更を行ったではなく、単に誰がどこにアクセスしたかを記すものです。したがって、他のユーザーのアクティビティに関する報告を行えるように、全てのITユーザーにレポート生成の権限を許可するポリシーをデフォルトで設定しても良いかも知れません。ITスタッフ間で管理者用セッションは“公の情報”であるため、このプロセスを透明化することでユーザーの正しい行いを奨励することにつながります。管理者がシステムの設定に関する問題を発見した場合、即座に誰が何のために変更を行ったのか調べることができるため、透明化されたポリシーはトラブルシューティングにも大変役立ちます。✔

報告書の透明化において唯一の例外は、少人数の管理者チームが他の管理者に 知られたくない機密の変更を行う必要がある場合です。例えば、企業が大規模なレイオフの計画中で、管理者数人がレイオフの対象になっている場合、この情報は機密扱いする必要があります。このようなシナリオは稀ではありますが、管理者の行いに関するポリシーの透明化をまず 基本とし、異例な状況が起こった時のみポリシーを変更するように設定することが 適切です。

他に考慮すべき点は、アクセス要求、特権アクセスセッション、生成済みのレポート等の記録をどの位の期間保存するかです。ディスク等のハードウェアは比較的安価なため、少なくとも数年間のデータをオンラインで保管することが好ましいでしょう。



最後に、ITユーザーがレポート生成の許可をすることに加えて、ITセキュリティ監査と社内のリスク担当の幹部・役員にも同じレポートを生成できる権限を与えるべきです。実際にシステムにアクセスせずに、ITスタッフが何を行っているかを見ることが出来るからです。言い換えると、レポートを生成できる権限は、特権アカウントにアクセスできる権利が前提である必要はありません。

## システムのモニタリングとメンテナンス

### システムのモニターとメンテナンスを行うスタッフの割り当て

特権パスワード管理システムを有効に管理するためには、1/4から1人のFTE(Full Time Equivalent)要員が必要になります。システム管理をしていく役割として、プロジェクトコーディネーターとテクニカルシステムアドミニストレーターの2つのタスクを担う必要があります。

特権パスワード管理システムのプロジェクトコーディネーターとしての役割は以下を含みます：

- システムの長所、ベネフィットなどをITスタッフに詳しく説明し、知識を広めて利用普及を図る。
- ステークホルダー(利害関係者)やユーザーからのシステムの機能や統合に関する質問に答える。
- ターゲットシステムとの新規インテグレーション追加を調整する
- ITユーザーが適切なトレーニングを受けるよう推進する
- ITセキュリティや監査グループに、アクセス権に関するレポートやトレーニングを提供し、彼らが自らレポートを生成できるようにする。
- セキュリティの改善と監査能力等のためにシステムへのインパクトを測る。
- ITアーキテクチャ計画に関するミーティングにこのシステムを代表して出席する。
- 新しいバージョン、サポート上の問題提起などに関してソフトウェア販売者とコーディネートする。

プロジェクトコーディネーターは、基本的、適格なITプロジェクトマネジメントの能力が必要となります。

特権パスワード管理システムのテクニカルアドミニストレーターの役割は以下を含みます：

- サーバーの健康状態をモニターする。
  - 例として、CPU使用度、ディスク容量、ネットワークのバンド幅使用量などです。
- イベントログをモニターする
  - 例えば、ターゲットシステムの変更の失敗、パスワード開示要求の拒絶、データ複製に関する問題などです。
- ユーザーインターフェイスのカスタム化を行う。
- ソフトウェアのバージョンアップの計画と実行。
- 新しいターゲットシステム(インテグレーション)の追加
- 定期的なデータベースのメンテナンス(バックアップ、復旧作業など)

テクニカルシステム管理者の技能は以下を含みます：

- 設計：
  - セキュリティポリシー
  - ネットワークとデータアーキテクチャー
  - ITサポートインフラストラクチャーとプロセス
- インストレーション、継続的な運用管理：
  - Windows / Active Directoryの管理
  - ウェブサーバー構成と管理
  - ウェブアプリケーション

- ▶ 初期のインテグレーションと継続的に行う更新、拡張：
  - Windows, Unix/Linux, ルーター等の管理対象システムの専門知識
  - ITサポートインフラストラクチャとプロセス
  - Eメールのインフラストラクチャ
- ▶ ビジネスロジックの開発：
  - プログラミング、またはスクリプティング (Perl, VB, Java等)
  - データソースに関しての精通: LDAP, RDBMS等
  - HTML、インタラクティブなUIをサポートするためにオプションとしてJavaScriptを含むにウェブアプリケーションに精通していること

## システムの健康状態をモニタリング

特権パスワード管理システムのプロダクションは、常時正しく機能しているかモニターする必要があります。



- ▶ プラットフォームのモニタリング：
  - ディスク使用量(使用度が高い場合、エラーが発生しやすくなります)
  - メモリの使用量(使用度が高いとスワップが発生しパフォーマンスが低下します)
  - 実行中のプロセス数(プロセスが適切に終了していないことで、スパイクが発生している可能性があります)
  - オープン・ネットワークの接続数(ターゲットシステムへの接続が正しく終了していない場合に スパイクが発生することがあります)
- ▶ アプリケーションのモニタリング：
  - アプリケーション・ユーザーによるログインの失敗
  - コンピューターの自動検出機能の問題
  - 社内ディレクトリ、またはデバイス上でのユーザー検索に関する問題
  - ターゲットシステムでのパスワードリセットの問題
  - 長期間接続されていないターゲットシステム
- ▶ セキュリティのモニタリング：
  - アクセス権の要求が異常に多いユーザー
  - ログイン試行回数(有効または無効)が異常に多いユーザー
  - 拒絶された全てのアクセス要求

HP OpenViewまたはMicrosoft Operations Manager等の一般的なモニタリングシステムを利用して、プラットフォームのモニタリングを行うのが最も有効です。

何らかの問題が起こった場合にメールの通知、またはトラブルチケットを発行するように特権パスワード管理システムを構成し、アプリケーションモニタリングを行うことが最も有効になります。

セキュリティモニタリングは、ログデータのレポートを定期的に生成し、セキュリティーオフィサーに提供することが最も有効な手段です。

## ターゲットシステムとのインテグレーションの構成

システムの統合が進むと同時に、特権パスワード管理システムの有用性も高まります。1,000台のシステムを対象に特権パスワード管理を行った時の効果を、100台の場合と比較すると明らかにより大きなセキュリティ上の恩恵を受ける事ができます。

統合化されたシステム数が増加すると、追加、維持、削除などを手動で行った場合、費用も同時に上昇します。数百以上もの統合が必要なシステムに拡張するためには、自動化が不可欠です


インテグレーションの自動化とは、下記のタスクの自動化を図ることを意味します：

- ▶ ターゲットシステムの自動検出

- 各検出されたターゲットシステムにおいて、下記を自動検出：
  - 管理者用アカウント(全てのプラットフォーム)
  - サービスアカウント(Windows限定の要件)
- 特権パスワード管理システムに、新規のインテグレーションと関連IDをバッチでローディング
- 現存しないインテグレーション(N日間応答がない)を自動的に識別し、パスワード変更プロセスから削除

中～大企業の多くは、毎日ワークステーションとサーバーの追加、削除が行われます。したがって、24時間毎に自動検出プロセスを実行することが適切です。

サーバー検索の技術的アプローチがいくつかあります。利用可能なインフラストラクチャにより、適切な方法を選んでください。:

- 特にWindowsシステムを使用の場合は、リストは一般的にActive Directoryで管理されています。
- Unix/Linuxシステムを使用の場合は、一般的にDNSまたはマスターファイル/etc/hostsでリストが管理されています。
- 上記の技術が利用できない、または十分に含まれていない環境においては、単一または複数ネットワークセグメントに対するTCP/IPスキャンが適しています。
  - nmapは、この目的のために使うことができる無償の優れたツールです。 <http://nmap.org/>."> <http://nmap.org/>."> (note)
- IT資産やインテグレーションの必要なデバイスに関する正確、詳細かつ最新の情報を持つ在庫管理システムが導入されている環境もあります。その場合はこのシステムからそうした情報をインポートすることも可能です。

上記で説明したメカニズムを用いてシステムを検出した後の次のステップは、ログインアカウントのリストを初期にそして定期的に生成し、どのアカウントが「特権」であるかを見極めることです。それらのアカウントは管理者レベルのグループに属し、数字によるIDを持ち、サービスまたはスケジューラされたタスクの実行に使用されています。

IDを列挙し、特権を与えるメカニズムはシステムにより異なります。例えば、UnixやLinuxでは、SSHスクリプトを使用してUIDが0のユーザーなのか、またはwheel, rootまたはadminのようなグループに属するのかがチェックすることができます。一方Windowsシステムに適するのは、グループメンバーシップ、Windows Service Managerの構成、スケジューラーの構成、そしてIISの構成を確認するRPC上で接続されたプログラムを使用することです。


不正に生成されたIDを発見できるように、ターゲットシステムでの特権IDの列挙は頻繁に行う必要があります。一方、自動検出プロセスは実行回数を削減し、ネットワークへのインパクトを最小限に抑えるため、頻度を低くする必要もあります。このような相反する要件においては、1日1回、または週1回程度に行うことがリーズナブルです。✔

その他問題となるのが、各ターゲットシステムに初めて接続する際に、いつターゲットシステムの自動検出を行いどのクレデンシャル(証明書)使用するかです。適切なオプションは:

- ドメインメンバーであるWindowsサーバーが稼働している場合は、各システムにサインインできるドメインレベルのアカウントを使用して下さい。✔
  - 特権パスワード管理システムは、各システムのIDをローカルに生成し使用することができます。これにより、各システムは、初期設定後は、ローカルな特権を持つドメイン管理者アカウントに頼る必要性がなくなります。
- 他のタイプのシステムを使用している場合は、システム管理者に、特権パスワードシステム専用のアカウントを開設するよう依頼してください。パスワードは、まず予想可能で固定されたものを設定してください。✔
  - 各システムへ最初に接続する際は、特権パスワード管理システムは、他のパスワードと一緒に上記の固定されたパスワードをスクランブル化させる必要があります。


特権パスワード管理システムは、パスワードの変更の際にインテグレーションしたシステムへの接続を試行するため、インフラストラクチャをモニタリングする装置として使用することができます。これによりターゲットシステムに接続できなかった場合に警告することができます。この場合、管理者にEメールで連絡、またはヘルプデスクにトラブルチケットを発行する等により注意を促すことができます。

ターゲットシステムが引き続き使用不可能の場合、通常のパスワードローテーションプロセスから自動的に削除されます。これによりデータベースをクリーンな状態に保つことができます。システムが一定の時間を超過してもオフラインの状態の時、またはシステムがその後回復した時の為、過去のパスワードのデータは、各システムにおいて保持されている必要があります。✔

応答しないターゲットシステムを識別するために、定期的にレポートを生成する必要があります。これにより、システム管理者は応答のないターゲットシステムのリストと、停止されたとわかっているシステムのリストを照らし合わせることができます 。

## 本番環境への移行

特権パスワード管理システムは、企業にとって非常にセンシティブなインフラストラクチャの一部です。本番環境に移行する前に、まず最初にテスト環境での展開を行い、システム構成の検証を行うことが不可欠です。

プロダクションに移行した後は、段階的にシステムを使用することが適切です 

- まずはテストモードから開始して下さい。テストアカウントをインテグレートしたシステムに開設し、パスワードを頻繁(数分間毎)にスクランブル化させて、システムが確実に機能しているかを確認できた場合のみ、パスワード管理をプロダクション環境に移行させます。
- システムライブ化前のテストに失敗した場合：
  - 特権パスワード管理システム用サーバーからネットワークアダプタを切断し、データが失われていないかを確認する。
  - 特権パスワード管理システム用サーバーの電源を切り、他のサーバーからパスワードを回収できるかを確認する。
  - システムをプロダクション環境に移行する前に、電源を入れ直し、上記のデータベース復旧のテストを行って下さい。
- 特権パスワード管理システムの管理下でない管理者用アカウントを、各システムに1つ設定して下さい。システムが故障した場合のバックアップアカウントとして使用します。プロダクション環境でのオペレーションが安定した後、2~3か月後にこのアカウントを削除することもできます。
- パスワード変更は低頻度(例:週1回程度)からを開始して下さい。システムが正常に作動しているのを確認した後に、毎日パスワード変更を行って下さい。
- 永続的なアクセス制御ルール(例としてグループXに属するユーザーは、グループYに属するシステムへの管理者用アクセス権を取得できるなど)に基づいてアクセス開示を開始して下さい。システムの基本的な機能が確立された後に、ワークフローを導入して下さい。
- WindowsとLinuxの簡単なインテグレーションから開始して下さい。その後他種のシステムの徐々に追加していきます。

## APIの考慮事項

APIは特権パスワード管理システムに、ひとつのアプリケーションが他に接続するときに、認証に用いるセキュリティパスワードを設定します。例えば、電子商取引専用アプリケーションは、在庫のデータを読み取る為にデータベースサーバーにサインインする必要があります。このような場合は、通常ログインIDとパスワードを使用して認証を行います。

1つのアプリケーションが認証にパスワードを使用する場合のセキュリティ問題：

- コンフィギュレーション・ファイルがプレーンテキストで保管されている。
- 複数のサーバー間で複製され、アプリケーションのインスタンスとして実行されている。
- 複数のウェブ、データベースサーバー間での更新の調整をすることが困難なためスタティック(状態が変化しない)な状態になっている。

これらの問題を避けるために、埋め込まれたアカウント用のパスワードを定期的にスクランブル化するために特権パスワード管理システムを使用することができます。APIは、電子商取引専用アプリケーションの各インスタンスが、特権パスワード管理システムからデータベースに接続するのに必要な最新のパスワード値を取得できるようにします。これにより固定されたパスワード、またはプレーンテキストのパスワードを排除することが出来ますが、新たな課題を提起します：

- どのようなプラットフォームのどのようなランタイム環境で、APIは利用できるか？
- 電子商取引専用アプリケーションのインスタンスは、どのように特権パスワード管理システムへの認証を行うか？
- 電子商取引専用アプリケーションは、パフォーマンス上のボトルネックが発生するまでに、どの位の頻度で特権パスワード管理システムに接続できるか？ その頻度がパスワードを必要とする頻度よりも低い場合、パスワードは変更される間どのように安全にキャッシュ化すべきか？
- 電子商取引専用アプリケーションが特権パスワード管理システムに接続できない場合は、どのように対処すべきか？言い換えると、特権パスワードシステムが新たな単一障害要因を発生させることになるのか？

- ▶ 特権パスワード管理システムは、いつパスワードのスクランブル化を行うのが安全か？
- ▶ アプリケーションサーバクラスタに対して1つのパスワードを持たせるべきか、あるいは各サーバが別のパスワードを持つべきか？
- ▶ 上記で取り上げた電子商取引専用アプリケーションは、一例に過ぎず、どのようにすれば、何百ものアプリケーションをサポートするインフラストラクチャに拡張できるのか？、そしてどのようにアプリケーションのソースコードの変更(APIをコールするため)の調整が行うべきか？

上記に疑問点に対して、どのケースにも適応するような答えを出す事はできません。企業は独自のプライオリティを持ち、各アプリケーションはそれぞれ制約を持っているため、上記への答えも当然変わってきます。以下は、上記の質問に対する一般的な解決方法であり、全てに適する方法ではありません。✔。

#### ▶ プラットフォーム/ランタイムのサポート t:

- APIは、各クライアント・プログラム、各種プラットフォームで使用可能であるべきです。これに対応する最適な方法は、SOAP(simple object access protocol)のようなプラットフォームニュートラルなAPIフォーマットを使用することで。(例えば、ウェブサービス上のXML)
- SOAPは現代の全プログラミング言語とランタイム環境からのアクセスが可能です。いくつかのケースでは、SOAPを呼び出すことは、少々複雑になります。そのような場合は、SOAPトランスポートをラップした「ヘルパー」ライブラリにより、システム開発にかかる手間と時間を削減することができます。

#### ▶ 認証API:

- クライアントアプリケーションが、アプリケーション用と同じログインIDとパスワードを用いて特権パスワード管理システムへの認証を行う場合、1つのパスワードをランダム化をせずに別の(静的?)パスワードに置き換えるだけのため、恩恵はほとんどありません。
- その他の方法として、クライアントアプリケーションの新規パスワードをランダム化して定期的に生成することです。例として、特権パスワード管理システムは、クライアントアプリケーションが認証するために使用しなければならない新規のランダムストリングを毎回生成するようにします。
- 他の補完的な方法として、特権パスワード管理システムがログイン時に、クライアントアプリケーションのIPアドレスを確認することです。限定されたサーバ上でアプリケーションが実行されるため、IPアドレスの予測ができ、認証の一つの要素としての利用することができます。

#### ▶ パスワード変更のためのアクセス頻度とキャッシュ化:

- アプリケーションはデータベースへの接続を1秒間に数千回以上行うため、全てのデータベース処理に新規のパスワードを取得することはかなり極端な方法かもしれません。
- 適切な方法は、新規パスワードを一時間程度ごとに取得し、その間パスワードをキャッシュ化することです。
- キャッシングは、キャッシュ化されたパスワードをどのように保護するかという疑問を提起することになります。1つのオプションは、メモリ上のみで保管し、コアダンプにより取り出すことを困難にするため 特別な文字コードに変換して保存した(アプリケーションに埋め込まれた)ものを使用します。
- 他の方法は、ディスクにキャッシュ化されたパスワードを保管することです。特権パスワード管理システムがオフラインの状態の時でも、キャッシュ化されたパスワードの使用ができるため、以下で説明するシステムの可用性をサポートします。
- キャッシュ化されたパスワードをどのようにディスク上で保護するかに関する1つの提案は、実行中のプログラム、またはパスワードを必要とするスクリプトのチェックサムの計算をし、そのチェックサムを利用してキャッシュ化されたパスワードの暗号化と暗号解読を行います。大切なのはパスワードを特別な文字コードに変換して保存するメカニズムです。機密性の高いアルゴリズムを使用してチェックサムを生成する必要があります。

#### ▶ 高い可用性について:

- 業務処理を完了させるために、特権パスワード管理システムのパスワード貯蔵庫からパスワードを取得する必要とする場合、特権パスワード管理システム自体およびAPIへの接続性が、スムーズなアプリケーション操作を行う不可欠な要素になります。
- 上記で説明したように、特権パスワードシステムのAPIで取得したパスワードをキャッシュ化し、実行中のプログラムの

チェックサム等見つけることが困難な暗号鍵を利用して暗号化することが必要です。

#### ▶ パスワード変更のスケジュール:

- ▶ パスワード変更のプロセス中は、クライアントアプリケーションが無効なパスワードを保持し続けるという競合状態が発生するリスクを伴います。
- ▶ このような問題を避けるためには、どのクライアント・アプリケーションがパスワードのチェックアウトを行ったか、どの位の時間使用することを許可されたかを追跡する必要があります。特権パスワード管理システムは、パスワード使用中はパスワードのスクランブル化を行わず、パスワードが変更されている間は新しいパスワードのチェックアウトを許可しません。
- ▶ 更に、プロセス処理の少ない時間(午前3時または日曜日の午前中など)にパスワード変更を行ようにスケジュールする必要があります。

#### ▶ 共用パスワード 対 クライアント毎のパスワード:

- ▶ 限られた時間内でのパスワード変更を調整するという難題、そして認証要素としてアプリケーションサーバーのIPアドレスを用いるという提案を考慮すると、それぞれのアプリケーションのインスタンスに証明書を付与し特権パスワードシステムのAPIに接続するという方法が適切です。
- ▶ また同様に、特権パスワード管理システムが各システムの複数アカウントのパスワードのスクランブル化を行い、安全な格納を行う必要があります。それにより、各クライアントアプリケーションは他のアプリケーションインスタンスのパフォーマンスに影響を与えずに、それぞれのPPM証明書を用いて接続を行い、バックエンド(データベース等)の証明書を取得することができます。

#### ▶ ソースコードの変更:

- ▶ 特権パスワードを保持する最もシンプルなアプローチは、証明書を必要とするアプリケーションのソースコードの修正を行い、直接またはconvenience/wrapperライブラリを通して 特権パスワード管理システムのAPIを呼び出すことです。
- ▶ サードパーティー製のアプリケーションを使用しているため上記の修正が出来ない場合、wrapperを使用してパスワード(プレーンテキスト等)を保管しているアプリケーションのファイルまたはその他のロケーションの変更を行うことも可能です。これはなにもしないよりは良いですが、好ましい方法ではありません。
- ▶ その他のアプローチとして、アプリケーションを起動させる前にアプリケーションのバイナリを修正し、テンプレートストリングを現在のパスワード値に置き換えることです。これは、インラインのソースコード制御の手間を削減しますが、バイナリか構成ファイルがそのパスワードを保持している場合にのみ有効です。これは、一見うまくいきそうですが、よりシリアスなセキュリティ問題を起こす可能性を秘めています。
- ▶ 一般的には、ソースコード管理システムを使用し、変更の追跡を行うことが最適です。この場合バージョンのアップデートもサポートできます。
- ▶ またアプリケーションの優先順位を設定し、プレーンテキストのパスワードを最もセンシティブなアプリケーションのAPIコールに置き換えることが適切です。

## まとめ

特権パスワード管理システムは、周知された、固定的かつ安全性の低いパスワードを使用するプロセスから、頻繁なパスワード更新、堅固な個人認証、きめ細かい認可ロジック、詳細な監査履歴を持つプロセスへの転換を可能にします。

このようなシステムの展開は、システムに大きく影響をあたえます。――機密性、統合性、可用性におけるシステム障害は、大惨事に発展する恐れがあります。そのため、堅固で、フォルトトレランス、安全性を考慮し他注意深い展開手段を取ることが求められます。

本書は、特権パスワード管理システムを安全で高い可用性で、安全に、拡張性が高く、効率的に管理できることを目的としたベストプラクティスを網羅的に説明したものです。

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)