

---

特権パスワード管理システムのデータ・リプリケーション



## ▶ 結論

特権パスワードの格納は、次の配慮が必要です。:

1. 暗号化:
2. 複製化:

リプリケーション(複製)は、次の配慮が必要です。:

1. 最低離れた2か所での格納
2. すべてのパスワードの格納
3. リアルタイムでの実行.
4. 安価で管理が簡単なこと.

複製プロトコルは、次の配慮が必要です。:

1. 暗号化すること
2. 低帯域幅でも許容すること
3. 高パケットレイテンシーでも許容すること.
4. ネットワーク瞬断から回復できること.

OracleやMicrosoftデータベースのネイティブリプリケーション機能は上記の条件を満たさず、アプリケーションレベルのリプリケーションが求められます。日立 ID 特権パスワード・マネージャーには、最適なリプリケーション技術が備わっています。

## 背景： 特権パスワードの管理

1,000台のサーバーがあり、各サーバーに5つずつ管理者パスワードがあることを考えてみてください。これらを安全に運用するには、パスワード管理プログラムが各5000個のパスワードに対して毎日、新しい、ランダムな値を選択することが考えられます。このプロセスは、次の点でセキュリティを改善します。:

1. ユーザーは、その仕事に応じて必要な重要パスワードだけを知ることができる。
2. 単一のパスワード / ログインID / システムの毀損をシステム全体の毀損に導くことがない。
3. ユーザーが管理アクセスをする期間を限ることができる。

言い換えると、ランダム化されたパスワードにより、基本的なセキュリティ原則を日々守ることができる。:

1. **認証:**  
特権パスワードが必要なユーザーは、アプリケーションやサーバーのパスワードが開示される前に、最初に認証されなければなりません。
2. **承認:**  
システムは、パスワードを開示する前に、アクセスコントロールルール あるいは/または、承認プロセスを適用する機会があります。
3. **アカウントビリティ**  
すべてのパスワード開示は記録し、ITユーザーに特権アクセスを用いて行ったシステム変更に関して説明責任を持たせることができます。

## ビジネス上の課題

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。

## ソリューションのアプローチ

上記課題は、次のように解決されます。:

### 重要データ

特権パスワードは、暗号化しなければなりません。暗号キーの管理には種々のやり方が、また、もちろん暗号アルゴリズムにも多種を用いることができます。但し、暗号化とキー管理は、本書の範囲外です。

### ビジネスの中断

サーバー障害--ディスククラッシュ、停電、CPUオーバーヒート等、すべてデータ損失を誘発します。これは、少なくとも、特権パスワードデータを頻繁にバックアップする必要があることを意味します。

### 定期的なバックアップ

最近のバックアップソフトウェアは、フルと増分バックアップで実現されます。各バックアップは、ある一時点の保護された状態のスナップショットを表現します。例えば、データベースのフルバックアップを週次で行い、増分バックアップを日次で行うといった運用をします。データは、最も最近のフルバックアップと一連の増分バックアップによって復元されます。

この方式--一日に一回の頻度で定期的なバックアップを取る--は、ほとんどのデータが毎日変更されることがない環境では十分なものです。ここでは、すべてのパスワードが毎日変更される特権パスワード管理システムについて考えなければなりません。

バックアップが午前3時に5000個の特権パスワードが毎日、ランダムな時間にランダム化されることを考えてみてください。一つのデータベースがすべての特権パスワードを持っており、データベースサーバーが2時59分にクラッシュしたとすると、24時間以内に更新されたすべてのパスワード--ほとんどすべて--が失われてしまいます。もしデータベースが午後3時にクラッシュしたとすると、約50%のパスワードが失われることになります。

### ローカル・リプリケーション

単一サーバーのクラッシュとすべての特権パスワードがその中に格納されているリスクを低減するために、すべてのパスワードを二つのサーバーにコピーすることが考えられます。あたらしいパスワードがデータベースにコミットされたとき、実際には二つのデータベースにコミットされ、一台のサーバーが失われても、致命的な状況ではなくすることができます。

これは、ほとんど陳腐化したデータのバックアップに頼る方法よりも確かにましですが、致命的なデータ破壊のリスクをまだ残しています。もし、火災、洪水、地震などの施設障害が起こったとすると、一か所のサイトにあるすべてのサーバーが破壊され、すべてのパスワードが失われてしまうかもしれません。もし、このサーバーが特権パスワード管理ソフトウェアをホストしており、単に接続できなくなったら(より可能性がある事象)、他のサイトユーザーも他のサイトにあるサーバーへのアクセスさえ出来なくなってしまいます。

単一のデータセンタでの、すべてのサイトのすべての特権パスワードのアクセスの損失問題は、大きな、不必要なビジネスリスクです。

### リモートリプリケーション

単一施設による問題や、一台サーバーによるハードウェア障害が引き起こすパスワード損失といった惨事を防ぐには、すべての特権パスワードを最低2台、最低2か所にコピーを持たせることが考えられます。

また、それらのサーバーを出来るだけ離して置いておくことも現実的です。--それにより、1995年の神戸地震や、2005年にニューオーリンズを襲ったカトリーナハリケーン、2003年の東部のパワーブラックアウトなどの、天災や、地域的なインフラストラクチャ障害でも、大企業/組織では、すべての特権パスワードアクセスアクセスを不能にすることはなくなります。

## リプリケーション・アーキテクチャ

今までの章をまとめると、特権パスワードは、センシティブで、アクセス出来なくなることは、大きな損害を招きます。これらは、定期的に変更が加えられるため、次のように保護するしなければなりません。

1. 暗号ストレージと暗号化転送
2. 複数サーバーへの複製格納
3. 物理的に離れた場所へのサーバーの配置

こうした保護のすべてを実現できない場合は、特権パスワード管理システムだけでなく、ITインフラストラクチャ全体のサポートと管理機能に対して壊滅的な障害を与えかねません。

上記を勘案し、複製パスワード格納システムでは、次のような重要な技術的特徴を配慮しなければなりません。

1. リプリケーションは、ニアリアルタイムで行う、特権パスワードデータは定期的に変更されるため
2. リプリケーションは、暗号化する、サーバーは、遠隔にあり、安全でないネットワークセグメントを介して接続されるかもしれないため、
3. リプリケーションは、次のような広域ネットワークでも実現可能でなければならない。:
  - a. 接続は、信頼性が低いかもしれない(データロスが発生する)
  - b. 帯域が限られている。
  - c. パケット転送遅延が高い。
4. リプリケーションはデータのサブセットでなく、すべてである必要がある。一部の特権パスワードを複製することは、されなかったものの損失を意味する。
5. すべてのサーバーは、独立に、パスワードのランダムイズ、パスワードの開示を独立に行える必要がある。これにより、サーバー障害やデータセンター障害時にも企業/組織が活動を続けることができる。

また、リプリケーションが備えなければならないビジネス的特徴は、:

1. リプリケーションは、安価で、企業/組織が実現をためらうようなものであってはならない。
2. リプリケーションは、構成や管理が容易で、管理者が設定を間違えることがないようにしなければならない。

## ネイティブDBMSリプリケーションの限界

主要なRDBMS製品(Oracle, Microsoft SQL Server, IBM DB2/UDB)の最新版は、すでにリプリケーション機能を備えています。特権パスワードのリプリケーションストレージをしてこれらの製品のネイティブ機能を使うのを最初に選ぶのは自然です。

リプリケーションテクノロジーとデザインチョイスの概要は、次に述べられています。:

[http://research.microsoft.com/%PERCENT\\_gray/WICS\\_99\\_TP/18](http://research.microsoft.com/%PERCENT_gray/WICS_99_TP/18)

Oracleに限定した有用な参考文献をは下記にあります。:

<http://www.wikibon.org/Best>

ネイティブ・リプリケーション機能は非常に強力ですが、残念ながら、特権パスワード管理の要件を十分に満たすことは出来ません。:

## Oracle データベースリプリケーション


### コスト

効果的なリプリケーションの管理のためには、リプリケーション管理モジュールを持つ Oracle Enterprise Editionが必要です。Enterprise Editionは、Standard Editionと比べて極めて高額です。

データ暗号化機能は、Oracle Enterprise Editionにはありません。この機能を追加するためには、Oracle Advanced Security を購入し、展開する必要があります。

### 複雑さ

Oracleのリプリケーション機能は非常に複雑です。オブジェクトタイプ、テーブル、行、列毎に複製するフィルタリング機能をもっています。異なるリプリカを異なるデータセットのために構成することが可能です。リプリカは、リード/ライトまたは、リードオンリーにすることができます。単一サーバーで、そのデータの異なるサブセットを異なるサーバーに複製することができます。

こうした複雑さにはコストが伴います。下記、Oracleのドキュメンテーションを参照ください。 <http://www.oracle.com/technology/books/pdfs/book> >  <http://www.oracle.com/technology/books/pdfs/book/> > (note)

マルチ・マスター・リプリケーション (MMR) について次に書かれています。:「管理要件が非常に増大します。データベースに問題が見つかったとき、DBAは、リプリケーションが原因でないか、他のデータベースにその原因を複製しないかを確認しなくてはなりません。データベースの性能チューニングと問題解決は、非常に複雑になります。」

他のコストとしては、パフォーマンスです。このタイプのリプリケーションでは、特権パスワード管理問題領域に最も適切なリプリケーションのタイプは、マルチ・マスター・リプリケーションです。Oracleの資料によれば、「MMRでは、トリガーとプロシージャを利用するので、データベース性能に影響します。どのくらいのデータを複製したいかによりますが、この性能への影響は、相当なものとなり得ます。」

### セキュリティ / 暗号化転送

デフォルトでは、Oracleのリプリケーションは、平文で送信されます。これを暗号化データにすることは可能ですが、他の製品: Oracle Advanced Security、を購入し、展開、管理することが必要です。

### 帯域幅/レイテンシーの要件

同じOracleの資料では、:「潜在的に大きなネットワーク帯域幅が必要。サイト間のマルチ・マスター・プッシュ、プル変更だけでなく、通知情報やその他の管理データの通信が必要です。」

つまり、MMRは、WAN展開、特に、WANで高帯域幅と低いレイテンシーを保証しない場合は、適切な方法ではないということになります。 .

## Microsoft SQL Server のリプリケーション

### コスト

リプリケーションには、SQL Server Standard Edition もしくはそれ以上が必要になります -- SQL ServerのExpress かWorkgroup Editionより高価になります。

### 複雑さ

SQL Server リプリケーションの最も適切なモデルは、PullモードでなくPushを使ったマージタイプのものです。

次の資料によれば、 <http://technet.microsoft.com/en-us/magazine/cc162477.aspx>:

「リプリケーションには、専任のDBAがいない環境では課題となる特別な知識が必要です。リプリケーションは、トラブルシューティングが複雑で、とくに高信頼化オプションとして用いるには、高度な設計を必要とします。」

### セキュリティ / 暗号化転送

Microsoft SQL Server のリプリケーションは平文で行われます。企業/組織では、転送レイヤーに暗号化機能を追加することが求められます。これは、つまり、SQL Serverのリプリケーションは安全なWAN展開には適さないということの意味します。

## 帯域幅/レイテンシーの要件

Microsoft SQL Server のリプリケーションは、SQL Serverの生成するログデータで3倍の帯域を必要とし、これは、サイト間の帯域が限られている場合には、多すぎるものです。

## 日立 ID 特権パスワード・マネージャー リプリケーション機能

### 高可用性とリプリケーション

日立 ID 特権パスワード・マネージャー は、一度展開されると、何千ものネットワーク機器の特権パスワードを唯一管理するものとなるため、組織のIT基盤の重要な一要素となります。日立 ID 特権パスワード・マネージャーの停止は、一連の機器の管理者アクセスが中断されることになり--ITサービスの重大な事故になります。

サーバーは時としてダウンすることがあるため、日立 ID 特権パスワード・マネージャーは、複数物理サーバー間でのロードバランスや、データリプリケーションをサポートしています。証明書データベースに対する全ての更新はリアルタイムに全サーバー上に複製されます。

まとめると、日立 ID 特権パスワード・マネージャーは、可用性が高い、複製機能、マルチマスターアーキテクチャを備えています。

データ複製をより簡易に提供するため、日立 ID 特権パスワード・マネージャーは複数インスタンス間でデータ複製を行うデータベースサービスを内在しています。このサービスは、物理格納機構としては、Oracleまたは、Microfost SQLサーバーを用いて構成されます。日立 IDでは、日立 ID 特権パスワード・マネージャー サーバー毎に、通常日立 ID 特権パスワード・マネージャー 自身と同じ物理ハードウェア上に、ひとつの物理データベースインスタンスを持つことをお奨めします。

日立 ID 特権パスワード・マネージャー の複製データサービスは、物理的なデータ格納を次のSQLデータベースエンジンを使って構成することが可能です：

- Oracle 10g, Enterprise Edition, R2.
- Microsoft SQL Server 2005, Enterprise Edition.
- Oracle 10g, Express Edition, R2 ( <http://oracle.com/>からの無償ダウンロード).
- Microsoft SQL Server 2005, Express Edition, with Advanced Services (<http://microsoft.com/>からの無償ダウンロード).

日立 ID 特権パスワード・マネージャー のデータリプリケーション・システムは、異なる物理的サイトにある各サーバーを使って複数に分散し、高信頼日立 ID 特権パスワード・マネージャーサーバークラスターを構築するのを、容易にするとともに、組織にとっては、これは賢明な方法です。複製のための通信は、WANの展開に適応するように、暗号化され、認証され、帯域効率もよく、遅延に対する耐性もあります。

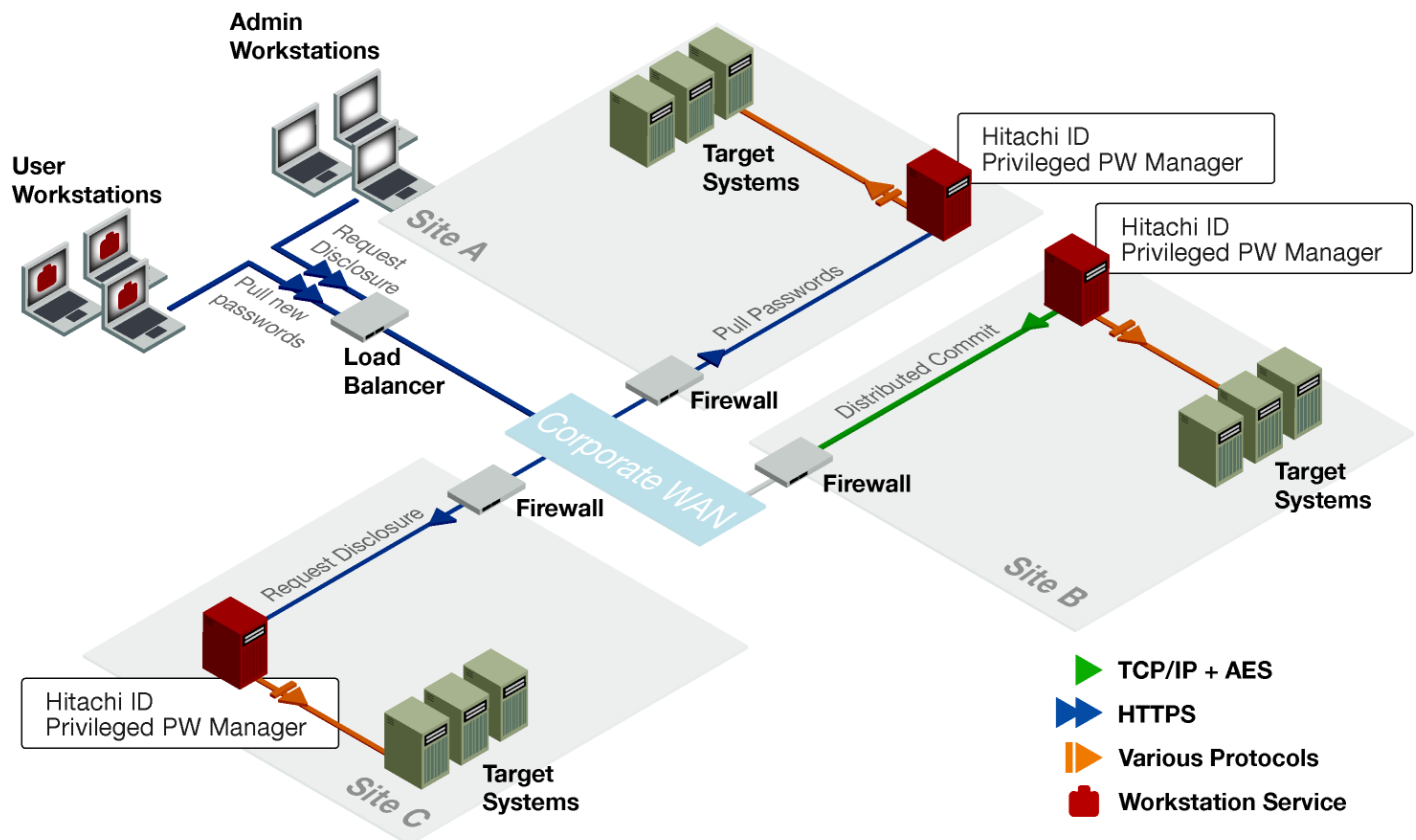
このマルチサイト、マルチマスター・リプリケーション は、追加日立 ID 特権パスワード・マネージャー サーバー 用のハードウェアを用意するほかは、追加コストなしに構成でき、管理上の手間も掛かりません。

### アーキテクチャ概要

サーバー(つまり、固定アドレスでネットワークに接続されているIT資産)上の特権パスワードの管理のために、各日立 ID 特権パスワード・マネージャーのサーバーは、パスワード更新サービスを実行します。このサービスは定期的に、やはり日立 ID 特権パスワード・マネージャーのサーバー上にあるコネクタを実行します。このコネクタは、単一のターゲットサーバーと通信し、単一のパスワード変更を行います。新しいパスワードが設定されると、このサービスは、日立 ID 特権パスワード・マネージャーのサーバーを新しいパスワードで更新し、ITスタッフにこれを提供できるようにします。新しいパスワードは、他のすべての日立 ID 特権パスワード・マネージャーのサーバーに自動的に、即座に、かつ安全に複製されます。

このプロセスは、異なるタイプのサーバー(Windows, Unix, Linux, DBMS, メインフレーム、アプリケーション、等)に対して、異なるタイプのコネクタを使って、日に何千回も繰り返されます。日立 ID 特権パスワード・マネージャーには、113以上のタイプのサーバーやアプリケーションのコネクタが装備されています。

日立 ID 特権パスワード・マネージャー のネットワークアーキテクチャは、下図 [\[link\]](#)に示されています。



### 日立 ID 特権パスワード・マネージャー のネットワークアーキテクチャ

サーバー(つまり、固定アドレスでネットワークに接続されているIT資産)上の特権パスワードの管理のために、各日立 ID 特権パスワード・マネージャーのサーバーは、パスワード更新サービスを実行します。このサービスは定期的に、やはり日立 ID 特権パスワード・マネージャーのサーバー上にあるコネクタを実行します。このコネクタは、単一のターゲットサーバーと通信し、単一のパスワード変更を行います。新しいパスワードが設定されると、このサービスは、日立 ID 特権パスワード・マネージャーのサーバーを新しいパスワードで更新し、ITスタッフにこれを提供できるようにします。新しいパスワードは、他のすべての日立 ID 特権パスワード・マネージャーのサーバーに自動的に、即座に、かつ安全に複製されます。

このプロセスは、異なるタイプのサーバー(Windows, Unix, Linux, DBMS, メインフレーム、アプリケーション、等)に対して、異なるタイプのコネクタを使って、日に何千回も繰り返されます。日立 ID 特権パスワード・マネージャーには、113以上のタイプのサーバーやアプリケーションのコネクタが装備されています。

©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](http://www.Hitachi-ID.com)