
日立IDパスワード・マネージャーを用いた企業規模のパスワード管理



▶ 要旨

ユーザーが多くのシステム、アプリケーションをアクセスするに従って、パスワードがいくつもたまってきます。ユーザーパスワードは、システム毎に、異なる値で、異なるスケジュールでの変更が必要で、また、異なる構成ルールに従っています。この複雑さの結果、ユーザーは頻繁にそのパスワードをどこかに書いておいたり、または、忘れてしまったりしてしまい、これが、セキュリティ上及びサポートコスト上の大きな問題に発展します。

効果的なパスワード管理は、パスワードの複雑さに起因する問題を解決します。：パスワード同期化はユーザーが覚えるパスワードを単一、堅固にし、頻繁に変更ができるようにします。セルフサービス・パスワード・リセットは、パスワードを忘れてロックアウトしてしまったユーザーに、ヘルプデスクに電話を掛けることなく、自ら復旧できるようにします。補助パスワードリセットは、ヘルプデスクコールを短く簡単なものにし、問い合わせ者がサービスを受ける前に確実に認証される信頼性を保証します。

イントロダクション

このホワイトペーパーは、日立 ID パスワード・マネージャーというパスワード管理ソフトウェアについて記述しています。パスワードシステムの操作に関連するビジネス上の課題を明確にして、これらの問題に日立 ID パスワード・マネージャーの機能をつかってどのように解決するかを記述しています。

日立 ID パスワード・マネージャーは、総合的なパスワード管理ソリューションです。パスワードシステムの運用コストを削減し、同時にセキュリティを向上させるのが目的です。これらは、次の機能により実現されます。：

- ▶ **パスワード同期化**：ユーザーの複数のログインIDに跨って単一の堅固なパスワードを管理すればよいようにサポートします。
- ▶ **パスワードポリシー**：すべてのシステムに対して、もとのそれぞれのパスワードポリシー機構の機能に関わらず、堅固なパスワード文法、期限と履歴ルールを施行します。
- ▶ **セルフサービス・パスワード・リセット**：自分のパスワードを忘れたか、侵入者ロックアウトに掛かったユーザーに、ヘルプデスクに参与してもらうことなく、自身の認証と問題解決をできるようにします。
- ▶ **補助パスワードリセット**：ヘルプデスクに対するパスワード・リセットのコールを簡素化し、ヘルプデスクをセキュアで、負担を最少にします。

日立 ID パスワード・マネージャーは、比較的人数が限られた複雑なイントラネットユーザー環境に展開（通常、ログインID/パスワードのペアが5~7程度もつユーザーが、100万人以下程度）できます。日立 ID パスワード・マネージャーは、また、単純なユーザーの集合である大規模なエクストラネットのユーザー環境（一般的に100万人以上、但し、一人について単一のLDAP IDで、頻繁でないログイン）にも適用することもできます。

ビジネス上の動機：パスワードシステムの操作をサポート

複数のパスワードを管理するのは煩雑な作業を伴います。この煩雑さは、生産性、安全性、コスト上の問題を生じさせます。

ユーザーは、通常多数のパスワードを持っています。それぞれのパスワードは異なるスケジュールで利用期限が訪れ、異なるユーザーインタフェースで更新が求められ、パスワードの構成と再利用に関しては、異なるルールが適用されている場合があります。

あるシステムでは、ユーザーに簡単に想像できないパスワードの利用を強制しますが、他は違う場合もあります。あるシステムでは、パスワードの変更をユーザーに頻繁に要請しますが、他は終了を強制できないものもあります。

こうした複雑さにより、ユーザーは、平凡なパスワードを選んだり、パスワードの変更を避けたり、パスワードを紙に書き残したりするようになってしまいます。ユーザーがこのようなことなく、セキュリティポリシーを破らない場合は、ユーザーはパスワードを忘れてしまい、結果として非常に多量のヘルプデスクコールを発生させることになりかねません。

パスワードの問題は、多くのITヘルプデスクの上位の問題の一つであり、ITサポートコールの25%程度を占めると言われています。

それらの操作上の問題に加えて、ユーザーは、単に沢山のパスワードを覚えたり、繰り返しタイプするのを好みません。沢山のパスワードを覚えたりタイプすることは、ユーザーがIT利用をネガティブに考える要因になります。

パスワードは、長い間、非常に広範に利用されており、今後も利用されるのは明らかです。他の認証技術、例えば、生体認証、スマートカード、2方式トークンは、一般的に二次的認証手段（例：生体認証+パスワード、トークン+パスワード/PIN）として、または、主要方式が使えない場合のバックアップ認証手段（例：スマートカードリーダーが使えない場合、スマートカードの代わりにバックアップパスワードを利用）としてパスワードを必要としています。

その結果、パスワード管理問題に取り組むことは非常に重要です。：他の認証技術が普及したとしてもこの問題が切なくなることは考えられません。

技術的課題： パスワードのサポートは難しい

中央集権のサーバーでパスワードの同期化とセルフサービスリセットを行うのは 比較的単純です。技術的な問題は、ロックアウトされたユーザー、モバイル ユーザー、キャッシュされたクレデンシャル(証明書)やPKIの扱いにあります。

ロックアウトされたユーザー

ユーザーは、しばしば初期ネットワークログインパスワードを忘れるか、不注意で侵入者ロックアウトをかけてしまう場合があります。こうしたユーザーでは、ネットワークやローカルパスワードをリセットし、侵入者ロックアウトを解き、通常業務に戻るよう支援を受ける必要があるかもしれません。

こうしたユーザーは、ワークステーションログインに問題があるため、そもそも問題解決するための基本的なウェブブラウザーや、クライアント/サーバーアプリケーションにアクセスすることができなくなります。こうしたユーザーの問題は、どのようにしてユーザーインタフェースにたどり着くかにあり、一旦たどり着けば、ログイン問題を解決することができ、続いて自分のワークステーションデスクトップのアクセスをすることができます。

こうした問題は、キャッシュドメインパスワードをワークステーションサインインに用いていて、コーポレートネットワークに接続されていないときにパスワード失念問題を起したモバイルユーザーに対して特に顕著です。

キャッシュされたクレデンシャル(証明書)

Windowsワークステーションは、ログインパスワード-- 一般的にActive Directoryか、NetWare NDS パスワード -- をキャッシュします。これは、次の理由で行われます。

1. ネットワークから切り離されている間にもユーザーがワークステーションにログインできるように(例:トラベル用ラップトップ)
2. 共有ファイルやプリンターサービスといった資源にユーザーに対して、ユーザーがパスワードを再入力することなく、自動サインインをするため、

ユーザーがワークステーション上のネットワーククライアントソフトウェアを使ってパスワードを変更しようとしたとき(e.g., ctrl-alt-del 方式)、ネットワーククライアントは自動的にキャッシュされたパスワードを更新します。

一方、ユーザーがワークステーションにログインし、同時にネットワーク上のどこかでパスワードをリセットしたとき、-- 例えば、ヘルプデスクにより、またはユーザー自身によりワークステーション上に2番目の同時ログインがされたとき、ワークステーション上のキャッシュされたパスワードは無効化されます。

無効なキャッシュされたパスワードはいくつかの問題を引き起こします。:

1. ユーザーがネットワーク資源へのアクセスしようとしたとき、ワークステーションはキャッシュされたパスワードでのサインインを試みます。キャッシュされたパスワードは正しくないため、この試みは、“不正ログイン試行回数”としてユーザーのネットワークプロフィールにカウントされてしまいます。
2. ネットワークへの繰り返しのアクセスは、侵入者ロックアウト機構により、ユーザーのログインIDを一時的に利用不可能にしてしまいます。このような事象は、ユーザーの介入なしに起こってしまいます--例えば、MS Outlookなどのメールクライアントは、キャッシュされたパスワードを使ってメールサーバーとの同期を取ろうとします。
3. ユーザーがネットワークからコンピュータを外したとすると、ユーザーは、新しいパスワードでワークステーションに入ろうとするかも知れませんが、これは使えません。

複製の遅れ

Active Directoryは、解決した侵入者ロックアウトフラグをすぐに伝播することはありません。これは、不注意にロックアウトを生じ、中央のヘルプデスクに支援をもとめたりリモートユーザにとっては問題となります。ヘルプデスクは通常ユーザーのロックアウトをヘルプデスクの近くのドメインコントローラーで解決します。このロックアウト解決は、ユーザーが認証されるどころか、ユーザーがアクセスしたいサービスネットワークリソースの属するドメインコントローラーに到達するまで長時間(数時間)かかるかもしれません。

この問題は、ユーザーサポート機能を集中的に司る何百ものドメインコントローラーを持つグローバル企業や組織では特に顕著です。

注記:ADパスワード変更の複製は、次のようになります。:

<http://technet2.microsoft.com/windowsserver/en/library/1465d773-b763-45ec-b971-c23cdc27400e1033.aspx?mfr=true>

モバイル、非接続ユーザー

旅行が多いユーザーは、一般的にキャッシュされたパスワードを用いてワークステーションにログインします。もしキャッシュされたパスワードを忘れたときには、リモート(例えば電話で)彼らをサポートするのは、コストがかかりまた安全ではありません。:

1. **高コスト:** ユーザーは物理的に(または郵送で)ラップトップPCをドメイン認証が可能な会社のどこかの場所に持ち込む必要があります。
2. **安全でない:** 別の手段として、ヘルプデスクが旅行中のユーザーに対して、代替または、管理者用ログインIDやパスワードを電話で伝えることができますが、信用、安全上の妥協が必要となります。

旅行中のユーザーに対するパスワードリセット事故はそれほど頻繁に起こるものではありませんが、事故が起こった際のコストは、ネットワーク接続されたユーザに比べて10倍にも100倍にもなり得ます。

PKI パスワードの管理

公開キー基盤では、一般的にユーザーのワークステーションに証明書ファイルを展開します。これは、ユーザーが暗号化ドキュメントやe-mailをアクセスしたり、オフラインの間に認証された安全なメッセージを送ることを可能にします。

証明書ファイルは一般的にユーザーの個人パスワードを用いて暗号化、及び解読を行います。言い換えると、ユーザーは、サーバー上に格納される必要のない“PKIパスワード”を持つことを意味します。パスワードはユーザーの個人証明書ファイルをアンロックするのに用いられます。

これは、標準的なPK(例えば、x.509証明書を使って)や、固有なPKI (例えば、Lotus Notes IDファイル)でも同じことが言えます。

Lotus Notes ID ファイルパスワードを含む“PKI パスワード”は、管理上リセットすることが出来ないため、サポートが難しいものとなっています。

1. PKI 証明書は複数の場所に存在することがあります(例えば、複数のワークステーション、ユーザーのホームディレクトリ、フラッシュデバイス等)。
2. それらのいくつか、または、すべての格納場所は、中央のネットワークに接続したパスワード管理システムからアクセスすることが出来ない場合があります。
3. PKI 証明書は、新しいパスワードで暗号化が行われる前に、現在のパスワードを用いて解読する必要があります。言い換えれば、現在のパスワードの認識がなく、管理用パスワードのリセットという概念はないということになります。

日立 ID パスワード・マネージャー の機能

日立 ID パスワード・マネージャー は、パスワードシステムのコスト削減とセキュリティの向上達成のために設計されています。

パスワード同期化

パスワード同期化は、企業ネットワークにおけるパスワード管理上の問題を解決する効果的なメカニズムです。:

- 同期化されたパスワードを持つユーザーは、そのパスワードを覚えるだけですみます。
- 簡略化されたパスワード管理はヘルプデスクに対するパスワード関連のコールを飛躍的に減少させます。
- ユーザーが覚えなくてはならないパスワードが一つか二つに限られれば、パスワードをメモに残す必要もなくなります。

パスワード同期化の実現には次の2つの方法があります。:

- 透過的パスワード同期化、これは共通システムで既に発生したネイティブパスワード変更を自動的にたのシステムやアプリケーションに伝播するものです。
- ウェブベースパスワード同期化、これは、パスワード変更するネイティブツールをすぐに利用することなく、ユーザーにウェブアプリケーションを用いて、すべてのパスワード変更をしてよいか否か尋ねるやりかたです。

日立 IDの日立 ID パスワード・マネージャーの中核的機能の一つはパスワードの同期化です。

日立 ID パスワード・マネージャー は、透過的及びウェブベースの両方のパスワード同期化機能を提供します。

セルフサービス・パスワード・リセット

セルフサービス・パスワード・リセットとは、自分のパスワードを忘れてしまったか、侵入者ロックアウトにかかったユーザーが別の手段によって認証を受け、問題を自分で解決できるようにするプロセスまたは、テクノロジーのことを言います。

パスワードを忘れたか、ロックアウトされたユーザーは、ワークステーションログイン画面の拡張を使うか、自分かほかのユーザーのウェブブラウザを使うか、または、電話を使って、セルフサービスアプリケーションを起動することが出来ます。ユーザーは、忘れてしまったか、使えなくなったパスワードを用いずに、一連の個人的な質問に回答するか、ハードウェア認証トークンを用いるか、または、生体認証情報などにより個人識別を行います。そして、ユーザーは、新たな、ロックされていないパスワードを指定するか、ランダム生成されたパスワードを設定します。

セルフサービス・パスワード・リセットは、問題が発生したあと、問題解決に迅速に対応できるほか、ヘルプデスクコールの低減することが出来ます。また、パスワードの問題の解決が堅固なユーザー認証を前提としてのみ解決できることを保障し、多くのヘルプデ

スクに存在する顕著な脆弱性(社会的工学的攻撃)をも排除します。

日立 ID の日立 ID パスワード・マネージャー の中核的な機能の一つがこのセルフサービス・パスワード・リセットです。

補助パスワード・リセット

日立 ID パスワード・マネージャーはヘルプデスクのパスワードをリセットするコンソールを保持しており、ヘルプデスク・アナリストがターゲットシステムへの直接アクセス権限を持たずに、発信者を援助することができます。

- ▶ ヘルプデスク・アナリストは日立 ID パスワード・マネージャーにウェブブラウザ上でサインインします。
- ▶ アナリストは日立 ID パスワード・マネージャー 内のIDとパスワードで認証されます。もしくはパススルー認証を既存のシステムに対して使用します。
例として、ヘルプデスク・アナリストはActive Directory IDとパスワードを用いて、日立 ID パスワード・マネージャーにサインインすることが可能です。同時に日立 ID パスワード・マネージャーは指定されたADセキュリティ・グループ内で各アナリストのメンバーシップを認証し、そのグループ・メンバーシップに基づいた適切な日立 ID パスワード・マネージャー権限を付与します。
- ▶ 日立 ID パスワード・マネージャーのウェブ・インターフェースから、ログインIDやフルネームをもとに、アナリストは発信者のプロフィールを検索することができます。
- ▶ アナリストは発信者を認証しなければならない場合があります。たとえば、ユーザーの個人的な質問に対する回答を入力するとき、日立 ID パスワード・マネージャーは内部データベースか外部ディレクトリに対して認証を行います。
同様でも異なっている、重複していたとしても、質問と回答のデータは補助パスワード・リセットやセルフサービス認証に使用されることがありますので、留意してください。
- ▶ アナリストと発信者の両方が認証されたら、アナリストは発信者のパスワードのリセットや、発信者の日立 ID パスワード・マネージャーへのアクセスのロック/ロック解除、発信者のプロフィールの更新が可能になります。補助パスワード・リセットは新しいパスワードを期限切れにして、次のログインでユーザーにパスワードの変更を促すために構成されることもあります。
- ▶ すべての処理 -- アナリストのログイン、ユーザー・プロフィールの参照、パスワードのリセットの成功や失敗、ユーザーやアナリスト、もしくはセキュリティ担当者などのサードパーティへのメール送信。同様のイベントがヘルプデスクの通話追跡システム内でチケットの自動作成、更新、終了のトリガーになります。
- ▶ 単純なウェブ・インターフェースが単体で使用されているので、補助パスワード・リセットは通常1-2分で完了します。
- ▶ ユーザー・フィルターとアカウント・フィルターのプラグインは利用可能です。パスワード・リセットの権限をマネージャーやプラットフォーム管理グループ、または地域のヘルプデスクに委任できるようになります。また該当のグループが適切なパスワード・リセットやユーザー・プロフィール参照権限のみを受けていることを保証します。
- ▶ パスワードがリセットされている最中のシステムへの管理権限は、そのプロセスのいかなる時点においてもアナリストは必要ではありません。その代わりに、日立 ID パスワード・マネージャーは独自の証明書を使用して対象のシステムにサインインしますが、この証明書は日立 ID パスワード・マネージャー内部データベースに暗号化されています。

補助パスワード・リセットは、パスワードに関するサポートコールのコストを減らし、そのような電話の処理が、一貫性のある安全な手段で均一に行われることを保証します。

パスワードポリシー施行

日立 ID パスワード・マネージャーは、通常、すべての新規パスワードがすべてのシステムに受け付けられるように、単一の、グローバルパスワードをサポートするように構成されます。これによりユーザーに最も明確に理解しやすい環境を提供します。日立 ID パスワード・マネージャーは、グローバルパスワードポリシーに合致しないパスワードをまったく受け付けないようにしたり、または、そうしたパスワードを伝播するように試みたりするように構成することもできます。

例えば、Windows Active Directory(AD)とOS/390パスワードの両方を持つ組織のケースでは、ユーザーは、ADには非常に長いパスワードを入力し、メインフレームには、8文字しか入力できません、この場合日立 ID パスワード・マネージャーは、8文字しか必要としません。あるいは、日立 ID パスワード・マネージャーは長大パスワードをサポートできますが、メインフレームを更新するときには、8文字に切り詰めることとなります。(ユーザーは一般的に、長さのルールをあらかじめ定義しておくほうを好みます。自動的な切り詰めよりも理解しやすいからです。)

一般的に、システムは、次の二つのうちの一つのパスワードルール形式を強制します。:

- ▶ 複雑性要件、容易に想像できるパスワードを選ばないようにする。このルール例は:ユーザーのログインIDの並べ替えやパスワード履歴の利用禁止、文字と数字の混在を要求、辞書に含まれる単語の利用禁止 等。
- ▶ 表現上の制約、特定のシステムのパスワード欄に物理的に格納できるものに制限を加える。通常次の二つのルールがあります:最大長制限、許容可能キャラクターセット

グローバルパスワードポリシーは、通常、ポリシーに影響を与える各システムから最適な複雑性要件を組み合わせ、強化することにより生成されます。日立 ID パスワード・マネージャーは、これらを結合し、最も制限的な表現上の制約を持つもちます。この強制によりユーザーは、もっとも堅固な、安全なパスワードを全システムに選択することができます。

代わりに、すべてのターゲットシステムに異なるパスワードポリシーを定義することは、ユーザーには、アンフレンドリです。これらのパスワードを更新するには、ユーザーは、システムを選択し、パスワードを選び、パスワードの更新完了をまって、再度認証し、次のシステムを選択し、異なるパスワードを選択し、等々しなくてはなりません。ユーザーは、また、複数のパスワードを覚えていなくてはならず、引き津好き多くのパスワード問題を体験することになります。すでも経験している通り、多数のパスワードを持つユーザーは、パスワードを紙に書き込むという傾向を助長することになります。

パスワード有効期限 / 期間・期限の施行

パスワード期限の強制施行とユーザーにウェブベースのパスワード同期化を起動させるため、日立 ID パスワード・マネージャーは、個々のシステム(例: WindowsやNetWareサーバー、LDAPディレクトリ)で次に来るパスワード期限を検知し、ユーザーには、個々のネイティブのパスワード変更画面を使って一つずつ変更させるのではなく、日立 ID パスワード・マネージャー ウェブ GUIを用いて一度にすべてのパスワードを変更するように促すように構成されます。

一般的にパスワードの有効期限は、ユーザーが日立 ID パスワード・マネージャーでパスワード変更を、他のアプリケーションやシステムパスワードよりも短期間のスケジュールで出来るように構成します。これにより、ユーザーは、日立 ID パスワード・マネージャーからか、または、日立 ID パスワード・マネージャーの透過的パスワード同期を自動的に起動するシステム以外からは一切パスワード変更が要求されないこととなります。

早期に次に来るパスワード期限の通知は、パスワード同期を透過的に実行する代替手段となります。特にユーザーが最も頻繁につかっている主要ログインシステムから同期を起動するのが不可能な場合には有効です。

ユーザーは、e-mailにより次に来るパスワードの期限を知らされます。あるいは、ネットワーク上で現在ログインしているユーザーが、“近々期限を迎える”ユーザーのリストに含まれているかを常にチェックする小さなクライアントプログラムをグローバルネットワークログインスクリプトに追加し、そのチェックが該当していたら、日立 ID パスワード・マネージャーを使って、そのユーザーに、デフォルトウェブブラウザを開き、ウェブGUIでパスワードを変更を促すURLに導きます。

ユーザーは、ネットワークにサインインしているときに自分のパスワードを変更するように求められます。ユーザーのワークステーションでは、キオスクモード・ウェブブラウザが開かれ、パスワード変更画面に導かれ、ブラウザを閉じる前にパスワード変更をすることが求められます。

パスワード期限のタイミングは、ユーザーが日立 ID パスワード・マネージャーを使って行った最も直近のパスワード変更に加え、管理対象システムの次に来る期限をベースに計算されます。

パスワードの再利用

日立 ID パスワード・マネージャーでは、パスワード履歴はデフォルトで“無限”となっています。特に許容しない限り、ユーザーはパスワードの再利用は完全に禁止されています。パスワードの再利用を許す場合は、パスワードの変更回数ではなく、時間間隔をベースにしています。パスワード履歴は、一方向、非可逆ハッシュ(SHA-1 plus 64-bit random salt)で格納されます。

パスワード同期化: テクニカルアークテクチャー

ウェブブラウザ・パスワード同期化

ユーザーは、パスワードのすべてまたは、一部を通常のパスワード変更を行う日立 ID パスワード・マネージャー ウェブインタフェースを使って、同期化することができます。パスワードポリシーは、画面上に明確に表示され、即座に強制されます。該当ユーザーがログインIDを持っている各システムは、名前とチェックボックスで表されます。

ウェブブラウザからのパスワード変更 及び 同期化は、次のように行われます。:

1. **ユーザー:** パスワード変更しようとするか、または、e-mailで促されるか、ログインプロセス中に“ウェブ・ポップアップ”が出る。
2. **ユーザー:** 手動で、または、自動的にウェブブラウザを開き、イントラネットから日立 ID パスワード・マネージャー アプリケーションにたどり着く。
3. **日立 ID パスワード・マネージャー ウェブサーバー:** ユーザーにネットワーク・ログインIDを入力するように促す。
4. **ユーザー:** ネットワーク・ログインIDを入力する。
5. **日立 ID パスワード・マネージャー ウェブサーバー:** ユーザーに現在のNOSパスワード入力を促す。
6. **ユーザー:** 現在のパスワードを入力。
7. **日立 ID パスワード・マネージャー ウェブサーバー:** 指定されたシステムへのパスワードを検証。
... 認証に失敗したら、繰り返し、頻繁に繰り返す場合、ロックアウトする。
8. **日立 ID パスワード・マネージャー ウェブサーバー:** ユーザーに新規パスワードの入力を促す。
9. **ユーザー:** 新規パスワードの入力、アカウントの一部か全てかを選択。
10. **日立 ID パスワード・マネージャー ウェブサーバー:** パスワード属性を評価し、必要なら前のステップに戻る。

11. 日立 ID パスワード・マネージャー ウェブサーバー: パスワードを選択されたシステムのパスワードを新しい値でリセット。
12. 日立 ID パスワード・マネージャー ウェブサーバー: ユーザーに状況ページを表示
13. 日立 ID パスワード・マネージャー ウェブサーバー: コールトラッキングシステムにチケットを記入。
14. 日立 ID パスワード・マネージャー ウェブサーバー: ユーザーに確認e-mailを送付。

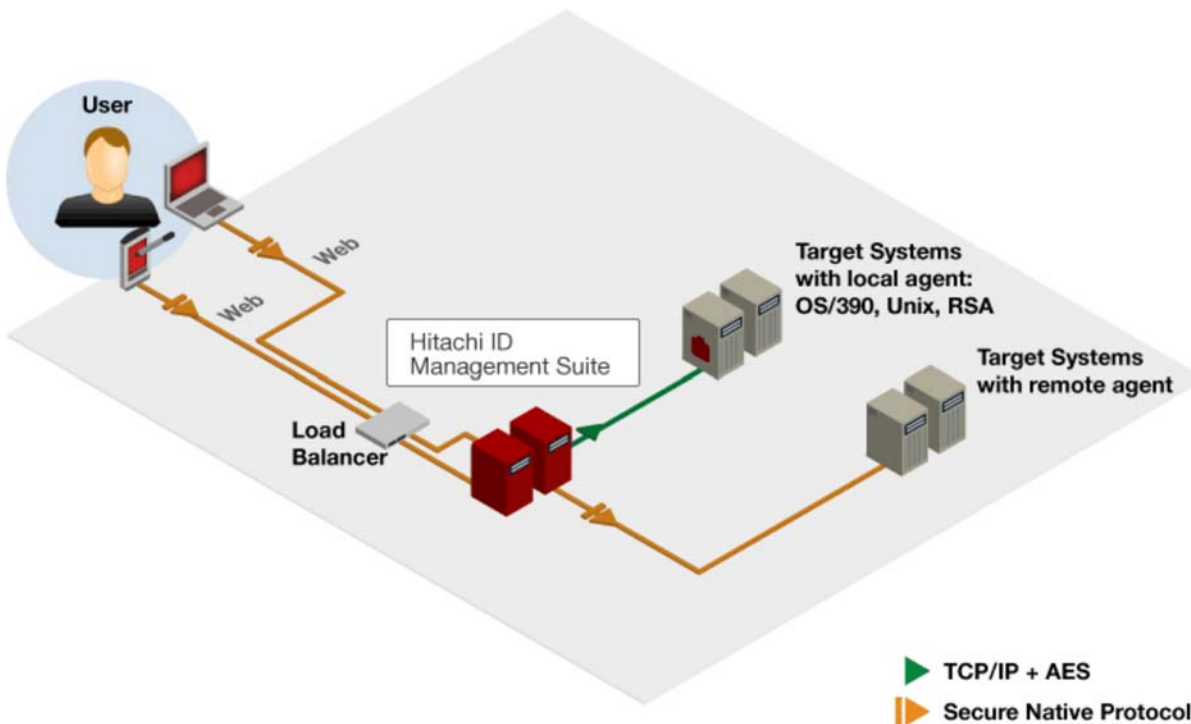
日立 ID パスワード・マネージャー では、Win32バイナリーとしてコンパイルされ、Windowsプラットフォーム上の標準準拠のウェブサーバー上で実行可能なCGIプログラム群を内在したウェブユーザーインタフェースを提供します。 Apache, IIS 及びSun Oneウェブサーバーをすべてサポートしています。

CGI ユーザーインタフェースプログラムは、入力フォーム、スキンファイルを使った新たなスクリーンのアセンブル(下記参照)、新たなフォームの表示が可能で、CGIプログラムは、日立 ID パスワード・マネージャー サーバーのアイデンティティ・キャッシュにある、アイデンティティプロフィールデータをアクセスします。これらのデータは、LDAPディレクトリやデータベースサーバーから取り込まれるものです。また、日立 ID パスワード・マネージャー サーバーの各サービスと連絡をとり、データを他のシステム(例えば、e-mail, ヘルプデスクシステム、SMSメッセージ)に送付するためのエージェントやプラグインプログラムを実行します。

上述したとおり、日立 ID パスワード・マネージャーのユーザーインタフェースは、HTMLの記述を含んだテキストファイルであるスキンファイルとして構成されます。複数のスキンファイルを日立 ID パスワード・マネージャーの構成要素としてインストールすることができ、複数言語サポートを初め、複数の“ルック&フィール”をサポートすることができます。

スキンファイルのHTML記述は、極めて通常のもので、管理上の及びカスタマイズの手間を削減するため、マクロファイルからテキストマクロシステム(m4)を使って、生成します。マクロは、ページヘッダーやフットノート、テーブルヘッダーやフットノート、ボタン表示、色の指定、フォント、等の構成を定義します。

日立 ID パスワード・マネージャーによって生成されるすべてのテキストは、スキンファイルから生成されます。マクロシステムでは、すべての言語テキストは、メッセージファイルから参照されたものです。新たな言語を日立 ID パスワード・マネージャーユーザーインタフェースに追加するために翻訳する必要があるのは、このファイルです。メッセージファイルには、マークアップ(校正文字等)はありませんので、翻訳者がこのファイルを扱いは容易であり、この点がこのやり方の利点でもあります。すべてのHTMLマークアップとボタンイメージは自動的にこれらのメッセージファイルから生成されます。



Web アクセスアーキテクチャダイアグラム

透過的パスワード同期化

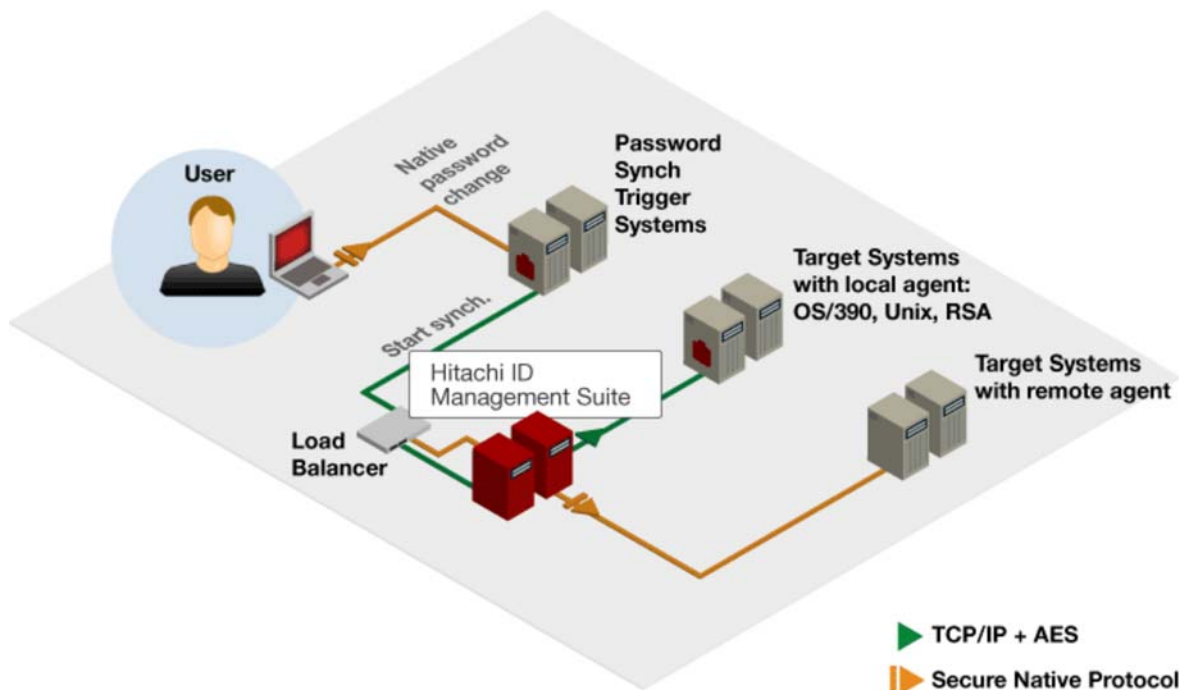
ユーザーがWindows NT, Active Directory (32-bit, 64-bit)、Sun LDAP、IBM LDAP、Oracle Internet Directory、Unix (種々の)、OS/390 and OS/400 のパスワードを変更するとき、新しいパスワードはシステムのネイティブポリシーに加えてグローバルパスワードポリシーに則ったものである必要があります。もし新しいパスワードがそれに満足すると、新しいパスワードは初期システム及び、自動的にユーザーがログインIDを持つすべての他のシステム上でも変更がかけられます。

既存の親しみやすいユーザーインタフェースを使ってパスワードを変更することは、トレーニングの必要性をなくし、高い適用比率

(100%)を保障します。

モニター対象システム上でネイティブパスワードの変更を契機とする透過パスワード同期化は次のように動作します。:

1. **ユーザー**: パスワードの変更すると判断するか、ログインプロセスの間に促される。
2. **ユーザー**: ログインIDを入植し、現在のパスワードと希望する値を投入。
3. **Login server**: (例えば、Windows NT, Active Directory (32-bit, 64-bit), Sun LDAP, IBM LDAP, Oracle Internet Directory, Unix (各種), OS/390, OS/400で) パスワードをシステムの内部的基準に合うか検証し、その後日立 ID パスワード・マネージャー ライブラリをコールし、その他の条件に合致するか検証する。
4. **日立 ID パスワード・マネージャー ライブラリ**: 日立 ID パスワード・マネージャー サーバーと連絡し合い;暗号接続を確立し;パスワードポリシー合致検証要求を転送する。
5. **日立 ID パスワード・マネージャー サーバー**: パスワード品質検証を行い;結果を返す。ポリシー違反が起こったときには、日立 ID パスワード・マネージャー は、ユーザーに直接e-mailまたは、Windowsのポップアップメッセージによりメッセージを返す;コールトラッキングシステムに記入する 等々
6. **Login サーバー**: ユーザーのパスワード領域が内部的に更新されると、日立 ID パスワード・マネージャー ライブラリをコールし、変更成功の旨通知する。 注記: 日立 ID パスワード・マネージャー ポリシーの合致の失敗は、通常、初期パスワードの変更実行をブロックします。
7. **日立 ID パスワード・マネージャー ライブラリ**: 日立 ID パスワード・マネージャー サーバーと連絡し; 暗号接続を確立し;パスワード同期化要求を転送する。
8. **日立 ID パスワード・マネージャー サーバー**: 同期化のための新規パスワードをキューに登録する。
9. **日立 ID パスワード・マネージャー サーバー**: ユーザーのためにセットされるパスワードのリストに対して、シングルキュー事象を解決する。(変更はアカウント毎に一つに限る)
10. **日立 ID パスワード・マネージャー サーバー**: 管理上、各システムのユーザーパスワードを新しい値に変更する。
11. **日立 ID パスワード・マネージャー サーバー**: 失敗したとき、キューに再登録し、リトライを行う;ユーザーに対して一通以上の問題を通知するe-mailを送る;コールトラッキングシステムに対しチケットを発行し、問題の対象者に警報を上げる。



透過的同期化アーキテクチャダイアグラム

パスワードリセット: テクニカルアーキテクチャー

パスワードを使わないユーザー認証

ユーザーは次のように認証します:

- ウェブGUI上で:
 - 信頼されたシステム(例えば、Windows / Active Directory, OS/390, RADIUS, 他)に対して現在のパスワードを入力

- システムが選択した個人的な質問に答える。その答えは、日立 ID パスワード・マネージャーの内部に格納されているか、既存システム(Oracle, LDAP, メインフレーム その他)により有効とされる。
 - セキュリティートークンを用いる (例: SecurID pass-code またはその他デバイス)
 - PKI証明書または、スマートカードを用いる
- 電話を用いる:
- 一つ以上の個人認証番号をキーインする(例: 従業員番号、入社日付、運転免許書番号)
 - 認証時に抽出した声紋サンプルと事前にファイルに記録されたものを照合することによる(生体声紋認証)

それに加えて、ユーザーがヘルプデスクを呼び出した場合は、日立 ID パスワード・マネージャー は、そのユーザーのQ-Aプロファイルを用いて、サポートスタッフによる認証が出来るように準備されます。

質問/応答データモデル

日立 ID パスワード・マネージャーはチャレンジレスポンス認証において、複数の質問セットをサポートします。

- 各質問セットはユーザーが質問と回答のペアを定義したり、ユーザーに事前定義済みの質問をいくつか答えさせることができます。
- 事前定義済みの質問を保有する各質問セットは、重複しない質問のリストです。
- 質問は書式上の制約がある場合もあります。例: IVR(インタラクティブ・ボイス・レスポンス)システムにおいては、すべてタッチトーン付の数字入力。
- 質問セットはさまざまな場面で使用されます。セルフ・サービス認証やヘルプデスク認証、ヘルプ・デスクのスタッフに表示されたり、必須入力したりする場合もあります。
- ユーザーは各質問セットにおいて、最低数の質問の回答を求められることがあります。例えば、20の質問があるセットの場合は、ユーザーは最低でも5つに回答しなければならないという場合です。
- 認証中に、定義された数の質問が関連のある質問セットからランダムに引き出され、認証を実行します。
- 質問セットは認証画面に割当可能です。これによって認証プロセスを連載できます。例えば、自由回答の質問に答える前に、ユーザーは事前定義済みのセットからいくつか質問に正解しなければならないということです。これによって、たとえ他の質問に対する回答がわかりはじめる前でも、攻撃者に回答を強制的に妥協させることができます。
- 各質問セットの質問と回答のデータは異なる場所に保管されています。たとえば、質問セット1つのデータが部局的に日立 ID パスワード・マネージャーサーバーにあり、第二データはLDAPディレクトリーに、第三データはHRアプリケーションに対して有効になっているかもしれません。
- 質問セットの数やセットあたりの質問数、ユーザーあたりの回答数には制限がありません。

十分想定しにくいパスワードを設定したり、定期的に変更するなど、チャレンジレスポンス認証には詳細な設定が不可欠です。

ロックアウトされたユーザーのアクセス

初期ネットワークパスワードを忘れてしまい、ワークステーションへのサインインができないユーザーに対して、ウェブブラウザーへのアクセスが可能で、セルフサービス・パスワード・リセットURLへのアクセスができる場合、いくつかの支援策が用意されています。

用意された解決策はそれぞれ、ユニークで、有利、不利な点があります。:

オプション	利点	欠点
	<ul style="list-style-type: none"> ➤ Inexpensive, nothing to deploy. 	<ul style="list-style-type: none"> ➤ ヘルプデスクは引き続き高いパスワード・リセット・コールに見舞われます。 ➤ ローカルパスワードやモバイルユーザーに対する解決策はなし。
	<ul style="list-style-type: none"> ➤ Inexpensive, no client software to deploy. 	<ul style="list-style-type: none"> ➤ ユーザーは、一人であるいは長時間格闘します。 ➤ ローカルパスワードまたは、モバイルユーザーに対する解決策はなし。 ➤ 一人に比べ、二人のユーザーの時間が無駄。 ➤ 組織によっては、セキュリティポリシーを侵害。

パスワードがないための"ヘルプ"。キオスクモードを開始

- 簡単、展開の手間が掛からない、クライアントソフトウェアが要らない。
- ユーザーがローカル、ネットワークパスワードの両者をリセット可能。
- ネットワーク上に"一般"アカウントを設定、但し、これは、いかにうまくロックダウンできるとしても、ポリシーを侵害するかも知れません。
- あるユーザーが"ヘルプ"アカウントでロックアウトを引き起こすと、パスワードリセットを要求する他のユーザのサービスも拒絶されてしまう。
- モバイルユーザーを救済しない。

例えば、ネットワークパスワードを忘れたユーザーがそのユーザー名称フィールドに 従業員番号を使い、誕生日とSSNの最後の4桁をパスワードフィールドに入れてログインします。ログイン時、ユーザーには、セルフサービス・パスワード・リセット用のキオスクモードウェブブラウザインターフェイスが表示されます。

- より複雑ですが、それほど手間を要しない展開が可能、クライアントソフトウェアは不要
- ユーザーは、ローカルとネットワークパスワード両者をリセットできる。
- 個人SKAアカウントは静的なパスワードを持つが、ポリシーを侵害する可能性あり。
- モバイルユーザーを救済しない。

- 集中基盤の簡単な展開
- 再利用か、既存のIVR(Interactive Voice response)システムの再利用か拡張
- リモートユーザーへの簡易ソリューションの提供
- 新規の物理基盤が必要 New physical infrastructure is required.
- ユーザーは一般的に"機会に話す"のを好まないの、普及率はウェブUIより低い
- ローカルパスワードやモバイルユーザーの解決策にならない。

ドメインユーザーの "ヘルプ"に対してローカルユーザー "ヘルプ"

- ドメイン全体に及ぶ"一般"アカウントを無くし、したがってセキュリティポリシーを侵害しない。
- ユーザーはローカル、ネットワークパスワードの両者をリセット可能
- 自動的に一時的、フィルタードVPN接続を設定でき、モバイルユーザーの支援も構成可能
- "一般"アカウントを排除できる。Eliminates any "generic" account.
- 物理的に存在するが認証できないユーザー(例えば、電話番号簿、バッジ管理、等)に適しており、複数のアプリケーションで利用可能。May be used by multiple applications that are suitable for physically-present but unauthenticated users (e.g., phone directory lookup, badge management, etc.).
- クライアントソフトウェアが必要、そのため、すべてのデスクトップイメージと展開するワークステーション上でのテストが必要となる。
- 展開にコストが掛かる。-- 多くの場所にハードウェア要 Costly to deploy -- hardware at many locations.
- ローカルパスワードやモバイルユーザーに対応しない Does not address local passwords or mobile users.
- ユーザーは、物理的なキオスクに行くよりも、ヘルプデスクコールの方が望ましい、

ログイン時に追加のユーザーインターフェイスコンポーネントが表示。これによりユーザーは、ワークステーションログイン応答から、セルフサービス・パスワード・リセットUIを起動できる。

- セルフサービスに対して、ユーザーフレンドリーでわかりやすいアクセスができる。
- ユーザーはローカルパスワードのリセットが可能
- 自動的に一時的なフィルタードVPN接続を確立でき、モバイルユーザーへの支援構成が可能
- すべてのワークステーションに余分なソフトウェアの展開要
- GINA (Graphical Identification and Authentication library) 拡張か、ラッパーのインストール失敗は、ワークステーションにダメージを与え、ログインを不能にする可能性がある。--ワークステーションの再設定が必要

となり、これには手間が掛かる。

- ワークステーションからセルフサービス・パスワード・リセットUIを起動 ログオン応答
 - ▶ セルフサービスへのユーザーフレンドリーで直感的なアクセス
 - ▶ ユーザーはローカルパスワードのリセットが可能
 - ▶ 自動的に一時的なフィルタードVPN接続を確立でき、モバイルユーザーへの支援構成が可能
- ▶ すべてのワークステーションに余分なソフトウェアの展開要

ユーザー登録

多くの企業や組織では、パスワード管理システムの展開にはユーザーの登録プロセスを必要とします。ユーザーは、認証のための質問に対する回答(パスワードを忘れて、ロックアウトしてしまった際の認証に用いる)などの個人データを提示しなければならないかもしれません。ユーザーは、プロフィールに標準的でないIDを割当てられるように求められるかもしれません。ユーザーは、将来起こりうるパスワード問題に対処するために、非パスワード認証のための生体情報サンプルなどを提示しなければならないかもしれません。最後に、ユーザーは、例えば、パスワード共用に関して、あるいは、パスワードの記載に関してなどの、コーポレートポリシーを読み、承諾することを求められるかもしれません。

登録が必要だとすれば、パスワード管理システムで、誰が登録されなくてはならないかを確認し、登録したりするための必要な人を招待または、喚起することにより、強固な認証登録ユーザインタフェースを提供するなどのプロセスを自動化するのは効果的です。

日立 ID パスワード・マネージャー には、ユーザーの登録プロセスを自動的にかつ安全に管理する基盤機能が組み込まれています。:

- ▶ 一つ以上のシステムのレコードをモニタリングすることにより、日立 ID パスワード・マネージャー は、自動的に新規プロフィールIDを作成したり、古いプロフィールIDを削除したりします。
- ▶ 新規ユーザーと既存ユーザーでの不完全なプロフィールは自動的にプロフィールが完全になるように促されます。(例えば、説明要求/応答 の認証用データを提示するなど)
- ▶ ユーザーにe-mailで登録への案内を送付することができます。
- ▶ ユーザーがネットワークにログインしたときに、ウェブブラウザが自動的に登録ページを表示するなど、ユーザーに対してより有効に登録喚起を促すことができます。
- ▶ ユーザーは、ネットワークにサインインしたときに、キオスクモードのウェブブラウザを開いて登録ページにアクセスするようになるか、ユーザーがプロフィールの記入を完了するまでWindowsデスクトップのアクセスをブロックしてしまうなどによって、ユーザーに登録を強制することもできます。
- ▶ 登録するには、ユーザーはまず認証されなければなりません。これは通常既存の強力な認証機能 --例えば、ネットワークパスワードまたは、トークンなどによって行われます。
- ▶ 単一の統合化された登録システムでは、説明要求/応答プロフィール、ログインID一致、声紋サンプルをサポートします。

ログインIDリコンサイレーション

すべてのID管理システムは、その機能に関わらず、ログインIDリコンサイレーション機能をサポートする必要があります。ユーザーは種々のシステムにログインアカウントや他のレコードを持っており、ユーザーセントリックのIDシステムを構築するためには、これらの情報は単一のプロフィール情報に結び付けられなければなりません。標準的でないログインIDと他のユーザーIDを単一プロフィールに結びつける処理をログインIDリコンサイレーションと呼んでいます。

日立 ID パスワード・マネージャーは、ログインIDリコンサイレーションのために次のように複数のオプションをサポートしています。:

- ▶ 自動的に、一般的なログインIDのマッチング
- ▶ SSN,従業員IDなどの他の属性でのマッチング
- ▶ 外部データを参照してのマッピング--例えば、ある組織では、マッピングテーブルやスプレッドシートにそうした情報を管理
- ▶ セルス・サービス・リコンサイレーション機能を用いて

セルス・サービス・ログインID・リコンサイレーションは、必要な場合、次のように機能します。:

- ▶ ユーザーは自動的に自らのプロフィールを生めるように促されます。--例えば、埋め込みURLを持つe-mailを受信するなどして
- ▶ ユーザーは、主要ログインIDとパスワードまたは、他の認証手段を使って、登録システムにサインインします。
- ▶ ユーザーは、追加のID/パスワードのペアを入力するように求められます。各々の入力されたID/パスワードのペアは、自動的

に管理対象システムから引き出された保守インベントリと比較され、ユーザーが入力したログインIDがそのシステムにあり、そのユーザーのプロフィールに組み込まれていないインスタンスを探します。日立 ID パスワード・マネージャーは、ユーザーが入力したパスワードでそのシステムへのサインインを試みます。もしログインが成功したら、ユーザープロフィールにそのシステムIDとユーザーが入力したログインIDを追加します。

セルフサービス・リコンサイレーションは、手間が掛からず(ユーザー毎に5分間程度)、信頼性があり、完全に自動化でき(ユーザーは、実際に行うまで登録をリマインドされます)、また非常に安全です。

セルフサービスと管理者ログインIDリコンサイレーションの両方とも記録されます。他のログインIDリコンサイレーションの形式としては、一般的にバッチ形式のものがあり、これは、必要に応じて記録させることが出来ます。

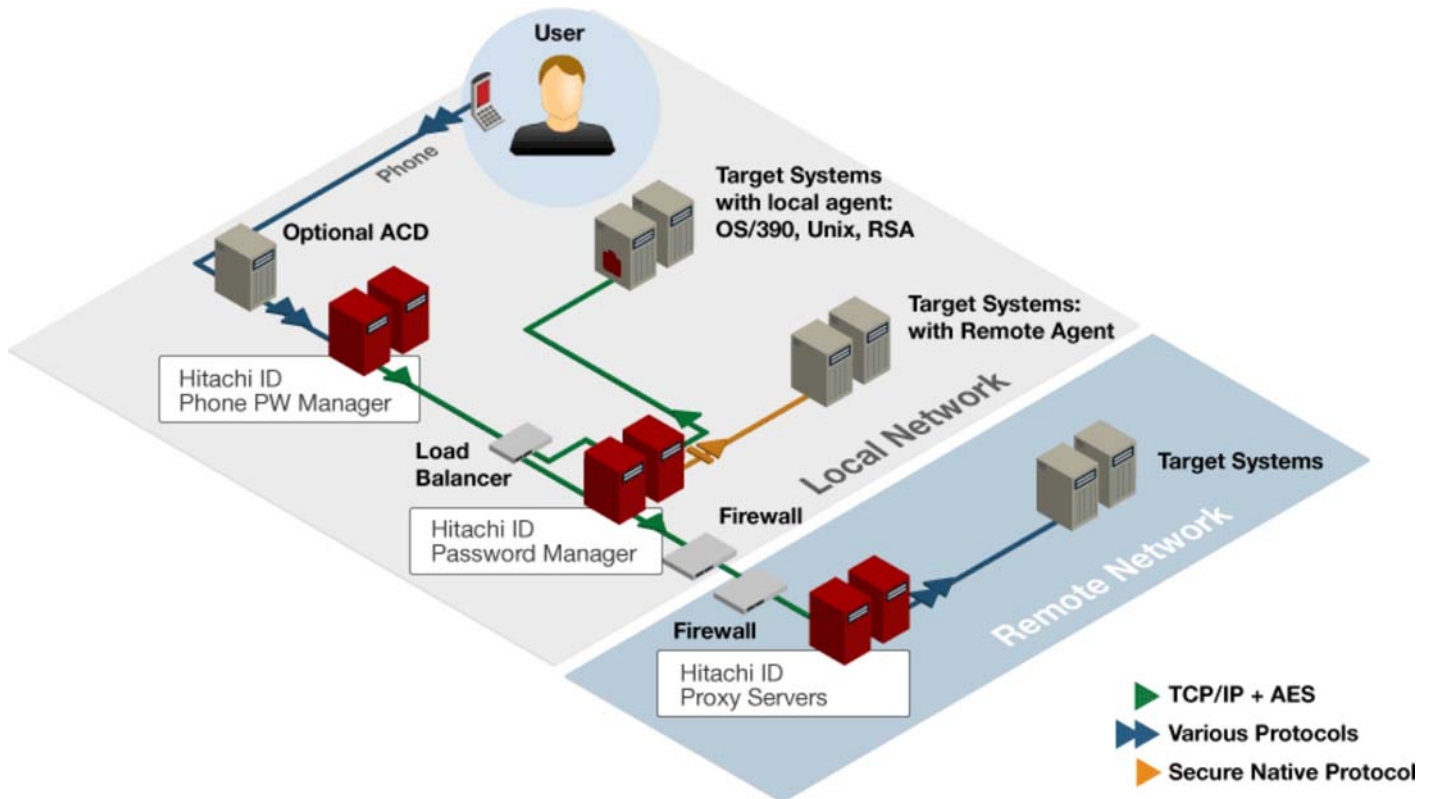
注記:管理対象システム上のユーザープロフィールの属性のマッチングで行うログインIDリコンサイレーションの試みは、コストがかかり、また、特にパスワード管理システムとの混在では、安全ではありません。

- 一般的に、すべてのシステムで共通に用意されている属性は、ユーザーのフルネームだけです。これは、システム間で不整合がある場合もあり、また大きな組織体では、ユーザー間で同じフルネームが、ときには同じ場所に存在することがあります。
- 自動的にアカウントの関連付けに失敗すると手動のリコンサイレーションに引き渡されますが、これは、手間が掛かります。
- 正しくない関連付けは、あるユーザーが他のユーザーのパスワードをセットすることになり、重大なセキュリティ侵害につながります。

セルフサービス・ログインID・リコンサイレーションは、処理に手間が掛からない(25,000ユーザーが各々5分使うだけでコストは最小限ですが、一人のコンサルタントが何週間も何ヶ月も費やすのは非常に高価です)ばかりか、間違いがありません(エラーフリー。IDは、パスワードで確認されます)。このプロセスは、日立 IDの知りうる限り最良であり、ユニークな手法です。

電話 / IVR インテグレーション

ロックアウトされたユーザーにパスワード・リセット・サービスを提供する一般的なオプションとしては、電話で、IVR(Interactive Voice Response)システムを使う方法があります。パスワードを忘れたユーザーはIVR(インタラクティブ・ボイス・レスポンス)システムに電話をかけパスワードリセットをすることが出来ます。個人の秘密情報のタッチトーン入力か、声紋認証を使った個人認証がサポートされています。既存のIVR(インタラクティブ・ボイス・レスポンス)システムは、日立 ID パスワード・マネージャー リモートAPI (アプリケーション・プログラミング・インターフェース) または、日立 ID フォーン・パスワード・マネージャー -- パスワードリセット用に設計されたターンキーのIVRシステム をつかって拡張することができます。



電話アクセス (IVR) アーキテクチャダイアグラム

声紋照合を用いたパスワード・リセット・プロセス

電話によるパスワードリセット、声紋でのコーラー認証、パスワードのランダム生成(電話による英文字入力を最小限にするため)

は、次のように機能します。:

1. **ユーザー**: パスワードを忘れたか、侵入者ロックアウトが掛かる
2. **ユーザー**: サポート番号に電話をし、"パスワードに関する問題" のセクションに進む。
3. **日立 ID フォーン・パスワード・マネージャー サーバー**: ユーザーに個人IDの入力を促す、例えば、従業員番号、または、ユーザのログインIDの英数字を数字にマッピングしたもの (例: smith01 は、7648401 にマッピングされる。)
4. **ユーザー**: IDをキー入力
5. **日立 ID フォーン・パスワード・マネージャー サーバー**: 日立 ID パスワード・マネージャー サーバーに接続
6. **日立 ID パスワード・マネージャー サーバー**: ユーザープロフィールを探索
7. **日立 ID パスワード・マネージャー サーバー**: ユーザーの質問のサブセットをランダムに選択ユーザーに選択された質問事項への回答を促す
8. **日立 ID フォーン・パスワード・マネージャー サーバー**: ユーザーに選択された質問事項への回答を促す
9. **ユーザー**: 電話に口頭で回答する
10. **日立 ID フォーン・パスワード・マネージャー サーバー**: ファイルに保存された声の特長と回答を比較する
... 失敗したら繰り返す、成功したら、続ける、ロックアウトの場合あり
11. ユーザーが新しいパスワードを選択するプロセスは以下の通り:
 - a. **日立 ID フォーン・パスワード・マネージャー サーバー**: 日立 ID パスワード・マネージャー にユーザーのためにランダムパスワードの生成を依頼
 - b. **日立 ID パスワード・マネージャー サーバー**: ランダムでポリシーに合致したパスワードストリングを提供
 - c. **日立 ID フォーン・パスワード・マネージャー サーバー**: ユーザーにパスワードを発音し、受け入れるか/リトライするかをたずねる
 - d. **ユーザー**: パスワード選択の受付に対応する数字を押下
 - e. **日立 ID フォーン・パスワード・マネージャー サーバー**: 日立 ID パスワード・マネージャー に、選択されたシステムと要求されたパスワードストリングで、ユーザーのパスワードリセットを依頼
 - f. **日立 ID パスワード・マネージャー サーバー**: パスワードリセットを即座に実行し、必要であれば、リトライのためのキューに登録
 - g. **日立 ID パスワード・マネージャー サーバー**: "パスワード期限切れ" フラグを新しいパスワードに設定することができ、これにより、ユーザーが次にログインしたときに新しいパスワードを設定するようにする。
 - h. **日立 ID パスワード・マネージャー サーバー**: コール追跡システムにチケットを登録
 - i. **日立 ID パスワード・マネージャー サーバー**: ユーザーに確認 e-mail を送付

タッチトーン照合と用いたパスワード・リセット・プロセス

タッチトーンコーラー認証とランダムパスワード生成(電話機での英数字インプットを最小化するため)による電話によるパスワードリセットは次のように機能します。:

1. **ユーザー**: パスワードを忘れたか、侵入者ロックアウトが掛かる
2. **ユーザー**: サポート番号に電話をし、"パスワードに関する問題" のセクションに進む。
3. **日立 ID フォーン・パスワード・マネージャー サーバー**: ユーザーに個人IDの入力を促す、例えば、従業員番号、または、ユーザのログインIDの英数字を数字にマッピングしたもの (例: smith01 は、7648401 にマッピングされる。)
4. **ユーザー**: IDをキー入力
5. **日立 ID フォーン・パスワード・マネージャー サーバー**: 日立 ID パスワード・マネージャー サーバーに接続
6. **日立 ID パスワード・マネージャー サーバー**: ユーザープロフィールを探索
7. **日立 ID パスワード・マネージャー サーバー**: ユーザーの質問のサブセットをランダムに選択
8. **日立 ID フォーン・パスワード・マネージャー サーバー**: ユーザーに選択された質問事項への回答を促す
9. **ユーザー**: 質問事項に数字で回答する
10. **日立 ID フォーン・パスワード・マネージャー サーバー**: 回答を 日立 ID パスワード・マネージャー サーバーに転送する
11. **日立 ID パスワード・マネージャー サーバー**: 登録されたデータと回答を比較
... 失敗したら繰り返す、成功したら、続ける、ロックアウトの場合あり

12. ユーザーが新しいパスワードを選択するプロセスは以下の通り:

- a. **日立 ID フォーン・パスワード・マネージャー サーバー**: 日立 ID パスワード・マネージャー にユーザーのためにランダムパスワードの生成を依頼
- b. **日立 ID パスワード・マネージャー サーバー**: ランダムでポリシーに合致したパスワードストリングを提供
- c. **日立 ID フォーン・パスワード・マネージャー サーバー**: ユーザーにパスワードを発音し、受け入れるか/リトライするかをたずねる
- d. **ユーザー**: パスワード選択の受付に対応する数字を押下
- e. **日立 ID フォーン・パスワード・マネージャー サーバー**: 日立 ID パスワード・マネージャー に、選択されたシステムと要求されたパスワードストリングで、ユーザーのパスワードリセットを依頼
- f. **日立 ID パスワード・マネージャー サーバー**: パスワードリセットを即座に実行し、必要であれば、リトライのためのキューに登録
- g. **日立 ID パスワード・マネージャー サーバー**: "パスワード期限切れ" フラグを新しいパスワードに設定することができ、これにより、ユーザーが次にログインしたときに新しいパスワードを設定するようにする。
- h. **日立 ID パスワード・マネージャー サーバー**: コール追跡システムにチケットを登録
- i. **日立 ID パスワード・マネージャー サーバー**: ユーザーに確認 e-mail を送付

既存のIVRシステムとのインテグレーション

日立 ID パスワード・マネージャー には、IVRプラットフォームや他のサードパーティアプリケーション等の既存システムに組み込み可能なクライアントライブラリが備わっています。このAPIにより、外部(例:IVR)システム上で次のことを行うネイティブコードを実現可能です。:

- ユーザープロフィールの探索
- ユーザーのための認証用の質問群の操作
(一般的にIVR(インタラクティブ音声応答)アプリケーションでは、数字による回答を用意)
- 質問に対してのユーザーに入力された回答の審査
- ユーザーに対するランダム生成パスワードの発行要求
- ユーザーのパスワードリセット要求

このライブラリは 日立 ID パスワード・マネージャー サーバーに対してシェアドソケットキーをベースに暗号TCPソケットのセキュアリモートプロシジャーコールで実行されます。

日立 ID パスワード・マネージャー API (application programming interface) は、Windows(DLL)および、Unix (Lucent/Avaya製品で用いられているUnixWareを含むUnixタイプのシェアドオブジェクトライブラリ)のC-言語バインディングを含みます。SOAPウェブサービス及びActiveX コンポーネントにも適用できます。

日立 ID フォーン・パスワード・マネージャー: ターンキー・パスワード・リセット IVR ソリューション

概要:

日立 ID フォーン・パスワード・マネージャーは、日立 ID パスワード・マネージャーパスワードリセットシステムのターンキー電話ユーザーインタフェースです。これにより、企業や組織では、簡単に、手間を掛けずに、また既存の電話交換システム基盤に大きな変更を加えずに、電話を用いたセルフサービス・パスワード・リセットをユーザーに提供できます。

日立 ID フォーン・パスワード・マネージャーは、ユーザーが自分の主要なワークステーションログインのパスワードを忘れ、入力できなくなった場合に最適な手段です。また、モバイルユーザーや、自宅で従事するユーザーがヘルプデスクに電話を掛けることなく接続上の問題を解決することができます。

機能:

企業の既存のヘルプデスクのACD(Automatic Call Distribution)システムで、パスワードリセット、侵入者ロックアウトまたは、RSAトークン管理の問題に関する電話コールをメインヘルプデスク番号からターンキー日立 ID フォーン・パスワード・マネージャーサーバーに転送するように設定します。

日立 ID フォーン・パスワード・マネージャーが電話呼び出しを受けると、ユーザーに、言語の選択、問題のタイプの指定、自身の認証と問題解決を促します。日立 ID フォーン・パスワード・マネージャーはユーザーに、自身の一つ以上のシステム上のパスワードのリセット、複数のアカウントでの侵入者ロックアウトの解除し、RSA SecurIDトークンの管理を許します。

日立 ID フォーン・パスワード・マネージャーは、日立 ID パスワード・マネージャー ユーザープロフィールに格納してあるQ-A (Question-and-Answer)データを使うか、2方式トークン(例:SecurIDトークンあるいは、他のハードウェアデバイス)を用いてコーラーを認証します。オプションの生体声紋認証エンジンも日立 ID フォーン・パスワード・マネージャーには用意されており、企

業や組織がコーラーを、予め格納してあるユーザーの声の声紋サンプルと電話の声を比較して認証することもできます。

日立 ID フォーン・パスワード・マネージャーで用いられるコーラーの認証データは、定期的に他のシステムから日立 ID パスワード・マネージャーに導入されるか、管理された日立 ID パスワード・マネージャーのユーザー登録の一連の作業中に集められます。これは、ネットワークパスワードで日立 ID パスワード・マネージャーウェブページに認証し、個人データを入力するようフォローアップするe-mailリマインダにより行われます。声紋サンプルもやはりユーザーにe-mailで登録を促し日立 ID パスワード・マネージャーウェブアプリケーションに導くことで登録します。Web認証ユーザーからの声紋の収集は電話に限られます。

日立 ID フォーン・パスワード・マネージャーは、複数の言語を話すユーザーをサポートするように構成可能で、各音声プロンプトの複数バージョンを録音可能です。

日立 ID フォーン・パスワード・マネージャーで実装されているコールフローは、カスタマイズ可能です。:

- ▶ ユーザーインターフェースは、単一言語にも複数言語にも対応できます。
- ▶ ユーザーは、英数字のネットワークユーザーIDか、従業員番号等の数字識別子で識別されます。
- ▶ コーラーは、すべてのパスワードをリセットするか、リセットする一つのパスワードを選択することもできます。
- ▶ 新規パスワードは、日立 ID パスワード・マネージャーによりランダムに生成されたものか、ユーザーがタッチトーンキーパッドを使って入力するものとすることができます。
- ▶ ユーザーは、侵入者ロックアウトの解除をパスワード変更をしないで行うオプションを選択することができますが、そうでない場合、必ずパスワードのリセットが必要です。
- ▶ 新規パスワードは、予め期限切れとしているか、または、通常の一定期間が過ぎると期限切れになります。

日立 ID フォーン・パスワード・マネージャーは、既存の電話基盤機能とのインテグレーションが可能です。企業PBXシステムに日立 ID フォーン・パスワード・マネージャーを適合させるために、適切なIntel Dialogic テレフォニーカードが必要となります。Dialogicカードは、アナログ、デジタル電話システムのように容易されており、カード毎に単一回線から32回線をカバーしています。Dialogicカードは、日立 ID からかまたは、電話機器業者から入手可能です。

日立 ID フォーン・パスワード・マネージャーは、日立 ID パスワード・マネージャーと物理的に同じサーバーか、個別のWindows/Intelサーバーにインストールすることができますが、一つ以上のIntel Dialogic テレフォニーボードの追加が必要です。複数の日立 ID フォーン・パスワード・マネージャーサーバーを複数の日立 ID パスワード・マネージャーサーバーにインテグレートすることも可能です。

日立 ID フォーン・パスワード・マネージャーは、日立 ID パスワード・マネージャーと同じ場所にある必要はありません。日立 ID フォーン・パスワード・マネージャーと日立 ID パスワード・マネージャーの間の通信は、単一の、暗号化TCP/IPソケットで行われます。結果として、WAN上で、インターネット及び/あるいはファイアウォールを介して安全に接続することで、日立 ID フォーン・パスワード・マネージャーサーバーを複数の場所に展開し、単一クラスターの日立 ID パスワード・マネージャーサーバーにインテグレートすることが可能となります。

利点:

日立 ID フォーン・パスワード・マネージャーは、モバイルユーザー、自宅勤務のユーザー、主要ワークステーションのログインからロックアウトされたユーザーがヘルプデスクを呼び出すことなく、自身の問題を解決できるようにします。

日立 ID フォーン・パスワード・マネージャーは、電話を使ってセルフサービス・パスワード・リセットを行う展開が容易なソリューションです。既設のIVR基盤を持っていないか、IVRコールロジックを変更するのは、大変で、高価である企業/組織にとっては、日立 ID フォーン・パスワード・マネージャーは、単に既存の電話交換基盤の最少の変更が必要なみの魅力的な代替手段であると言えます。

PKI 証明書パスワードの管理

PKI標準は、一般的に証明書フォーマットと、利用(証明書の管理でなく)、発行、ユーザーへの配送、PCやスマートカード上へのインストールと無効化に関係したものです。残念ながら、PKIの主要なコストは、この証明書の管理のプロセスそのものに起因します。

日立 ID パスワード・マネージャーは、PKI証明書を管理(プロヴィジョン、パスワードやその他属性情報の管理、ユーザーへの配送とディプロビジョン)するための重要かつ十分な基盤機能を持っています。

必要に応じ、この基盤は、個々のPKI製品をサポートするために、プロセスと証明書の格納に関連した一般的な機能やプラットフォームに依存したバインディングと結合します。現在、日立 IDでは、現在最も広く普及している(標準をベースにしていなくても) Lotus Notes ID ファイルのプラットフォームバインディングを提供しています。

Lotus Notesは、実際には各ユーザー毎に二つの別のパスワードを用います。

- ▶ Notes/Dominoサーバーに格納される、HTTPパスワードハッシュ

これらは、NSFのフィールドにある単純なパスワードハッシュです。日立 ID パスワード・マネージャー は、これらのパスワードを直接検証、変更、リセットするように構成できます。

- IDファイルを暗号化するためのパスワードで一般的にユーザーワークステーションに格納される。これらは、管理上リセットができません。
 - 日立 ID パスワード・マネージャー は、企業や組織がすべてのユーザーIDファイルの格納庫を設定、管理するための技術をIDファイルを回復する暗号化パスワードと共に提供しています。
 - 日立 ID パスワード・マネージャーは、格納庫からIDファイルを取り出し、格納庫のパスワードでそれを開き、パスワードを新しい値に変更し、ユーザーに対する新しいIDファイルを届けることで、IDファイルのパスワードリセットシミュレートしています。
 - ユーザーからのIDファイル、及び格納庫で管理し、ユーザーに更新IDファイルとして戻されるIDファイルの集合の両者共、ファイル同期化と共有のステージングディレクトリ(クライアントソフトウェアは必要ありません)、ユーザーワークステーションにインストールされたNotes Extension DLL(即座に無言の配送、収集)などを經由する複数のメカニズムをサポートしています。

日立 ID パスワード・マネージャーは、IDファイルパスワードリセットばかりでなく、IDファイル格納庫の構築と保守を自動化する唯一の製品です。

日立 IDは、日立 ID パスワード・マネージャーの汎用的PKI管理基盤機能とMicrosoft, Entrust, Verisign, GeoTrustや他のPKIベンダからの他のPKI製品の接続に関して開発を続けています。残念ながら、どのPKI製品も現時点では、広く使われている状況になく、日立 IDのPKIインテグレーションへのニーズは限られたものとなっています。

モバイル、非接続ユーザーのサポート

ユーザーがオフサイトにおいて、企業ネットワークに接続していないとき、ユーザーはテレフォニーソリューション(IVR (Interactive Voice Response))でRASやVPNパスワードを変更できます。但しこれは、ユーザーがローカルワークステーションパスワードや、キャッシュされたドメインパスワードで引き起こした問題には対応できません。

ローカル展開のセキュア・キオスク・アカウント(LSKA (Local, Secure Kiosk Account))が、モバイル、オフサイトユーザーが自分のワークステーションにサインインするパスワードを忘れたときに支援するために用意されています。LSKA(Local, Secure Kiosk Account)は、一時的ネットワーク接続を確立し、ロックダウンウェブブラウザを立ち上げ、ユーザーに認証とパスワードリセットができるようにします。このパスワードは、ネットワーク認証サービス(例: Windows / Active Directory ドメインコントローラ)及びローカルキャッシュ(つまり、ワークステーションがネットワークから切り離されているときにユーザーを認証するのに用いるキャッシュされたパスワード)として適用されるものです。LSKA (local, secure kiosk account) の利用形態は次のようになります。:

- ユーザーのワークステーションは物理的に電話線につながれているか、インターネット接続(Ethernet)接続されているけれども、企業ネットワークに接続されていない。
- ユーザーがローカルパスワードあるいはキャッシュされたドメインパスワードを忘れた。
- ユーザーは、ワークステーションに"help"としてサインインし、予め設定された覚えやすいパスワードか、ブランクをパスワードに入力する。あるいは、ユーザーは、GINAサブシステムとしてユーザーインタフェース上に設定されている、"パスワードを忘れた"ボタンを起動する。
- LSKA (Local, Secure Kiosk Account) が起動する。これが、ダイヤラーラッパーかVPNラッパーを起動する。
- ダイヤラーラッパーかVPNラッパーがレジストリから接続オプションを探しだし、ユーザーに接続の選択を求める。ユーザーが見るであろうメニューの例は:
 - 通話料無料電話番号：1-800-123-4567
 - 直通回線電話番号：1-234-456-7890
 - VPN 接続
- ユーザーが電話オプションを選択した場合、LSKA (Local, Secure Kiosk Account)大やリングプリフィックスをタイプするように求めます。デフォルト値は通常"9"でユーザーは3桁までタイプ可能です。(注記: 桁数を制限することでユーザーが本当の電話番号に掛けて、サービスを誤用するのを防ぎます。)
- ダイヤラー/VPNラッパーは、RASまたはVPNクライアント(マイクロソフトまたは、サードパーティ製)を起動し、電話番号とダイヤルプリフィックス、または、VPNサーバーのIPアドレスと、レジストリから得た証明書を渡します。
- ダイヤラー/VPNラッパーは、接続を待ちます。(接続が成功するか否かのレジストリー構成の次のようなテストが用意されています。インタフェースの"up"状態のチェック、与えられたIPアドレスのPING、与えられたIPへのTCP接続の試行、等)
- ダイヤラー/VPNラッパーは、有効な接続が得られなかった場合、エラーダイアログを表示し、ウィンドウを閉じます。
- ダイヤラー/VPNラッパーは、ロックダウン、キオスクモードウェブブラウザを起動する日立 ID パスワード・マネージャー プログラ

ムである、runurlを起動します。この初期URLは、日立 ID パスワード・マネージャーサーバーのセルフサービス・パスワード・リセットページに導きます。

- ▶ ダイアラー/VPNラッパーは、ユーザーのやり取り(ウェブブラウザから日立 ID パスワード・マネージャー ウェブサーバーへ)がN分以内の間に完了するのを待ちます。もしN分以上たった場合、ユーザーセッションをハングアップし、ワークステーションログイン応答に戻ります。
- ▶ 残りのプロセスは、通常の日立 ID パスワード・マネージャーウェブベースのセルフサービス・パスワード・リセットのプロセスと同じです。これには、パスワードリセットに成功したあとワークステーションのキャッシュされたドメインパスワードの更新を行う AcriveXコンポーネントへの参照を含みます。

ワークステーション上で実行可能なシーケンスは、既に説明されていますが、次の通りです。:

1. ダイアラー/VPNラッパーは、ローカルヘルプユーザーのためのシェルとして起動されます。(新規)
2. RASまたは、VPNクライアント(既存)
3. 一つ以上の接続テストプログラム(新規)
4. RUNURL, PCをロック解除し、キオスクモードブラウザを起動(新規)
5. ユーザーのデフォルトウェブブラウザ(既存)

LSKA(Local, Secure Kiosk Account)ソリューションは、レジストリエントリーのセットを使って構成されます。-- 接続サービス毎に一つのレジストリキー(LSKA(Local, secure Kiosk Account)がワークステーションにインストールされたときに設定されます。) LSKA(Local, secure Kiosk Account)レジストリキーは、次を含みます。

- ▶ タイプ (ダイヤル vs. VPN)
- ▶ 電話番号
- ▶ ログイン ID
- ▶ パスワード
- ▶ 表示名称、ユーザーに適切なコネクションタイプをたずねるダイアログボックスのため
- ▶ コマンドライン(変数付き)、接続の呼び出しのため、ダイヤリングプリフィックス、電話番号/IP, ユーザーid, パスワード接続を %ARG% 拡張で示す。
- ▶ RUNURLに渡すURL
- ▶ タイムアウト(分または秒)、ハングアップするまでの時間
- ▶ コマンドライン(変数付き)、接続をテストするか、動作中か/失敗したか判断する。

Active Directory 複製

Active Directory は、侵入者ロックアウトフラグの解消を即座には伝播しません。これは、不用意にロックアウトしてしまったりリモートユーザーにとっては問題となり、結果として中央のヘルプデスクに支援を求めることになります。ヘルプデスクは、ユーザーロックアウトをヘルプデスクの近隣のドメインコントローラ上で当該ユーザーのロックアウトを解消します。このロックアウトが、当該ユーザーが認証を受けたいか、ユーザーがアクセスしたいサービスネットワーク資源の属するドメインコントローラに伝えられるまで、長時間(数時間)掛かってしまうことがあります。

この問題は、何百ものドメインコントローラを有し、中央の一箇所でユーザーサポート機能を司るようなグローバルな企業や組織では特に顕著です。

注記:ADパスワード変更の複製処理は、次のように説明されています。

<http://technet2.microsoft.com/windowsserver/en/library/1465d773-b763-45ec-b971-c23cdc27400e1033.mspx?mfr=true>

日立 ID パスワード・マネージャー は、Active Directoryのドメインコントローラー間の侵入者ロックアウトの解消遅延問題を、ユーザーが最も頻繁にアクセスすると選択したドメインコントローラーの集合に対してパスワードリセットを自動的に指示する、というユニークな手法で解決しています。:

- ▶ ユーザーのホームサイトのDC、ユーザーのホームディレクトリUNCとこのUNCをホストするサーバーのIPアドレスをベースに判断
- ▶ ユーザーの現在の場所のDC、ユーザーのウェブブラウザのIPアドレスをベースに判断(これは、セルフサービス・パスワード・リセットにのみ有効)
- ▶ 管理構成ルール群によりマップされたDC、例えば、グローバルまたは地域データセンター。

拡張性

PSYNCHIは、非常に大きな企業、組織で展開されています。 そうした大規模な拡張性を要求された主な事例には、次のものがあり

ます。:

- 単一の日立 ID パスワード・マネージャー システムで250,000以上の日立 ID パスワード・マネージャー ユーザー管理している企業では、たった2台のサーバーでロードバランスを行っています。
- ユーザーは6大陸に分散しています。
- 一つの日立 ID パスワード・マネージャー システムは単一のサーバーで稼働し、500以上のパスワードシステム上のパスワードを管理しています。
- 20の日立 ID パスワード・マネージャーサーバーを展開している顧客では、サーバー間でのリアルタイムのデータ複製を行っており、ユーザーは、ネットワークアクセスができない場合でもシステムアクセスへのアクセス可能です。

日立 ID パスワード・マネージャーの拡張性を支えるアーキテクチャ的特長には次のものがあります。:

- サーバー語とに複数のシステムをインストールできる機能
- システムを複数のサーバーに跨ってインストールすることができる機能、その場合、グループ内の各サーバーは機能的に同一（同じユーザー、システム、機能をサポート）です。features.
- 組み込まれた、高性能のアイデンティティキャッシュ、これは、リアルタイムのサーバー間データ複製機能を持っています。
このエンジンはWindows/Intelサーバー上で数百万件更新/秒のベンチマーク結果を示しています。データベースは、既存のリポーティング、解析ツールとの互換性を保障する標準のオープンフォーマットのファイル(xBase/DBF)を使っています。
- サーバー状態をモニターし、DNSレコードをダイナミックに更新する組み込みサービス;例えば、誤動作しているサーバーをロードバランスローテーションから外すなどのため

加えて、日立 ID パスワード・マネージャーは、直接性能には無関係ですが、大企業、組織で要求される沢山の機能と連携して動作します。

- ファイアウォールを跨いで操作する機能:ユーザーと日立 ID パスワード・マネージャー間、及び日立 ID パスワード・マネージャーと管理対象システム間
- スピードが遅く、安全でないWANを隔てて、一箇所にある一つの日立 ID パスワード・マネージャーサーバーが全体を管理することが出来る、プロキシサービスの提供
- サーバー構成毎に複数のユーザーインターフェースとUI言語をサポート
- 管理対象システム上のユーザーIDの自動ディスカバリ機能、これにより、手作業の管理を削減し、初期の構成に伴う作業を最小化することができます。
- 初期NOSログインパスワードを忘れたユーザーにデスクトップソフトウェアを用意することなくセルフサービス・パスワード・リセットをサポートする機能(セキュア・キオスク・アカウント)
- 21のユーザーインターフェース言語のサポート

セキュリティ技術

日立 ID 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、ユーザー入力フィルタリング、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 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 パスワード・マネージャー は、インストール時に入力を必要とする、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。

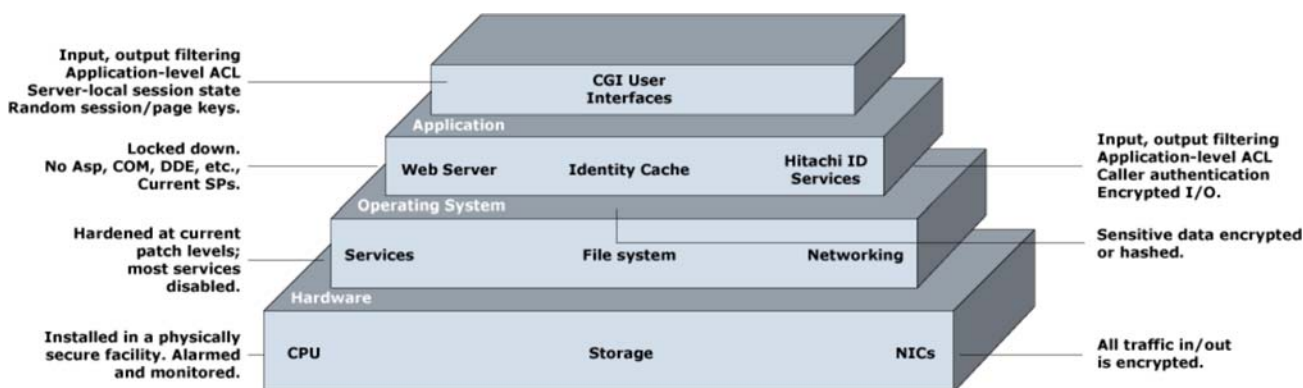


図4. ネットワーク・アーキテクチャ・セキュリティ・ダイヤグラム

暗号

暗号は、格納された日立 ID パスワード・マネージャー データを保護するために次のように用いられます：

Data	Algorithm	Key
ターゲットシステムにログインするために用いられる特権パスワード	128-bit AES	128-bit random
ユーザー認証 Q-A (Question-and-Answer) プロフィール 回答	128-bit AES	128-bit random
ユーザーの旧パスワード履歴	SHA-1	64-bit random salt

ネットワーク上の 日立 ID パスワード・マネージャー から、または、へのデータ転送は次のように暗号保護されます。：

To/From	Algorithm	Key length
Interactive sessions		
User browser	SSL (varies)	128 bits.
Trigger password synchronization		
From Win2K/2K3 AD DC	128-bit AES	128-bit shared secret.
From OS/390		
From Unix		
From LDAP server		
From WinNT DC		
Set passwords, Create/update users		
To Unix agent	128-bit AES	128-bit shared secret.
To OS/390 task		
To RSA Authentication Manager		
To proxy server		
API (application programming interface) Session - socket		
From calling system / IVR (interactive voice response)	128-bit AES	128-bit shared secret.
API (application programming interface) Session - web services		
From calling system / IVR (interactive voice response)	HTTPS	128 bits.
Set passwords, Create/update users		
To target system	native	Varies. Use proxy server when native protocol is inadequate.

ユーザーインタフェース入力保護

CGIプログラム(すべての日立 ID パスワード・マネージャーユーザーインタフェースを司る)は、処理前にすべての入力を検証するために、スペシャルストリングライブラリを用います。これには、可変長のフィルターリングアウトする特別な文字列が含まれます。

貴社のコスト削減を概算するには、オンラインカリキュレータをお試しください。:

<http://Password-Manager.Hitachi-ID.com/roi/>

プラットフォームサポート

日立 ID パスワード・マネージャー は、ほとんどのシステムのパスワードを直接 管理できます。以下に挙げるシステムの組み込みサポートを含みます。

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, HPUNIX, 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,

日立 ID パスワード・マネージャー には、いくつかのフレキシブルエージェントがあります、それぞれはプログラマブルです(つまり SDK (software development kit)を備えています)。これらのエージェントは、企業や組織に、最小限のプログラムやスクリプト開発で、迅速に、顧客個別のあるいはパーティカルマーケットアプリケーションに日立 ID パスワード・マネージャー を統合することができようになります。

フレキシブルエージェントは、次のようなプロセスを実行します。:

- 既存の管理API(application programming interface)と連携します。(Java, Win32, Unix, COM, etc.)
- スクリーンスクラッピング: Telnet, TN3270, TN5250, SSH 及び TCP ソケット接続
- ウェブベースの管理用ユーザーインタフェースを介してのナビゲーション(cookiesをサポートし、parsing, redirects など形成するHTTP 及び HTTPSを用いての)
- Oracle, Sybase, MSSQL, DB2/UDB, Informix 及び他の(ODBC) タイプのデータベースに対する任意のSQLコードの実行
- Unix(ローカルエージェントを介して)やWin32(日立 ID パスワード・マネージャー サーバー上で)上でのコマンドライン管理プログラムの実行
- LDAPディレクトリでの任意の属性の操作

- › ウェブサービスに更新を投入(SOAP または、HTTP or HTTPS上の他の XML 言語で)
- › MQ Seriesを用いてメッセージを送信

顧客専用または、バーティカルマーケットアプリケーションのために、まったく新しいエージェントの開発を望む企業や組織は、好ましい開発環境(J2EE, .NET, Perl, 等)を使って作成することができ、また、適切な日立 ID パスワード・マネージャーフレキシブルエージェント を使って、それをコマンドラインかWebサービスターゲットとして起動することが可能です。

日立 ID パスワード・マネージャー をカスタムアプリケーションか、バーティカルマーケットアプリケーションに統合するには、通常、4時間~4日間の作業しか要しません。これは、競合製品と比較すると格段に手間が掛かりません。そうした製品では、個別のJavaあるいは、3GLコネクターを最初からプログラミングしなければならず、これに何週間~数ヶ月を要し、新しいフレームワークやAPIを即座に習得する能力を持つ豊富なプログラミング経験を持つ日立 ID パスワード・マネージャー 管理者を必要とするような

その他のインテグレーション

日立 ID パスワード・マネージャー は、既存のIT基盤とも緊密にインテグレート できます。

ヘルプデスク・システム

日立 ID パスワード・マネージャー は、各種のヘルプデスク・コール管理システムで、既存のコールレコードを更新、新規レコードを作成ができます。100種 類以上のイベントタイプがこのインタフェースを起動でき、定義された各イベントは異なるビジネスロジックでインプリメントされています。

バイナリーインタフェース、ODBCデータベース更新、e-mail インテグレーションがサポートされています。日立 ID パスワード・マネージャーは、現在、次の チケットングアプリケーションのバイナリーインタフェースを持っています。

- › Axios Assyst
- › BMC Service Desk Express (各バージョン)
- › CA Unicenter Help Desk
- › Clarify eFrontOffice (現在は version 8のみ)
- › FrontRange HEAT (各バージョン)
- › HP Service Desk
- › HP ServiceCenter (各バージョン)
- › BMC/Remedy ARS (各バージョン)
- › Siebel ERM (Webサービスを用いる各バージョン)
- › SupportSoft (Webサービスを用いる各バージョン)
- › Tivoli Problem Management / Service Desk (各バージョン)
- › ... 他

認証機器

日立 ID パスワード・マネージャー は、RSA SecurID トークンと密接に統合して います。セルフサービス機器にアクセスしたいユーザーは、SecurID パスコード で認証することができます。ユーザーは、ネットワークパスワードか、質問プロ フィールによって認証された後、自身のSecurID トークンを管理することもできます。

日立 ID パスワード・マネージャー は、RADIUS認証もサポートしており、ユー ザーは、他の(非RSA)トークンでサインインすることができます。

電子メール

日立 ID パスワード・マネージャー 全体を通して163以上のイベントで自動通知が発行されます。これらは、ユーザー、要求者、受領者、認可者、管理者、セキュリティ管理者他へのe-mailなどです。e-mail受領者を指定するために、簡単なスクリプト言語が用いられています。e-mail受領者の特定のためやメッセージ内容の作成のために、通知エクジットは、どんなデータソースからデータを取ってきたり、要求属性を組み入れたり、どんなロジックを提供したりすることが可能です。

メタディレクトリ

日立 ID パスワード・マネージャー は、ユーザーがどこにログインアカウントを持っているか、そのアカウントがなんと呼ばれるか、を既存のメタディレクトリにアクセスすることができます。つまり、これらの情報は自動的に日立 ID パス ワード・マネージャーに収集され管理されることができ、また、Microsoft ILM のようなメタディレクトリにアップロードすることもできます。

迅速な展開

日立 ID ソリューションは迅速な展開が出来るように最適化されており、それが、すべての私たちの製品の中核となる設計思想となっています。ダイナミックワークフローなどの機能はロールエンジニアリングの必要性をなくし、自動ディスカバリやセルフサービス・ログインID調整機能などは、実運用化での製品情報の収集により生ずるコストや遅れを防ぐために用意されています。

日立 ID パスワード・マネージャー は早期展開が出来るように設計されています。:

- ▶ クライアントソフトウェアは必要ありません。ワークステーションログインプロンプトからのセルフサービスパスワードリセットでも不要です。
- ▶ 自動ディスカバリ 全ての管理し打て無の全てのIDに対して夜間に行われます。
- ▶ セルフサービス ログインID 調整(リコンサイレーション) 異なるシステム上のログインIDが全て異なり、事前に定義された既存の関連データがなくても、関連付けが可能です。
- ▶ 組み込みアイデンティティキャッシュ ユーザープロフィールデータを収集するので、日立 ID パスワード・マネージャー をインストールする前にデータベースや、ディレクトリをインストールする必要はありません。
- ▶ 70種以上のシステムに対応する組み込み済みエージェント機能 顧客は、共通の、一般販売されているターゲットシステム用に専用コネクタを開発する必要がありません。
- ▶ リモートエージェント 日立 ID パスワード・マネージャー は、各ターゲットシステム上に追加のローカルソフトウェアをインストールせずに、ユーザーとパスワードを管理することができます。
- ▶ フレキシブルエージェント これにより、企業や組織が日立 ID パスワード・マネージャー をカスタムアプリケーション、パーティカルマーケットソフトウェア、アプリケーションサービスプロバイダ(ASPs)、サービスビューローなどに早期に統合すること可能にします。—ターゲットシステム毎に2時間から4日間で実現が可能です。

ユーザーの利用を確実に推進

日立 ID は、お客様にend-to-endのアイデンティティ(ID)管理ソリューションを提供することにお約束しています。 初期に必要なとされるディスカバリ(システムの調査)から、ソリューション設計、製品の展開、そして弊社独自のAdoption Maximizer(AdMax)プログラムを通してお客様をサポートいたします。

アイデンティティ(ID)管理システムの成功例は、効果的なユーザーの実行プランによって支えられなければなりません。 10年以上に渡って、日立 IDは、すべての産業分野での、中規模企業から大企業に至るまで、柔軟なソリューションを展開し、お客様に多大なビジネス価値をお届けしてまいりました。この経験をもとに、日立 IDは、AdMaxプログラムを開発してまいりました。

AdMax は、日立 ID のお客様に、その目的を達成していただくため、プロジェクト全体のライフサイクルを通じて、そのエンドユーザーを効果的に引き込むお手伝いを致します。:

- ▶ すべてのユーザーグループやコンピュータ環境全体に対しセルフサービス機能(パスワードリセット、アカウント登録、生体認証による加入、等)の最大限の採用を推進する。
- ▶ 一般的に90日で80% - 90%に達します。
- ▶ 改善により早期のROIが得られるようになります。:
 - ヘルプデスク生産性
 - 管理スタッフの生産性
 - エンドユーザーの生産性
- ▶ ユーザー満足度を最大化します。

日立 IDのAdMax プログラムの展開は、ディスカバリ(調査)フェーズに開始され、システムが展開された後に完了し、日立 IDとおお客様の双方が、ロールアウトが完了したことを確認します。

AdMaxソリューションデリバリープロセスには、6つのコンポーネントがあります。:

- ▶ ニーズ評価
- ▶ AdMax ツールキット
- ▶ ワークフロー最適化とGUIカスタマイゼーション
- ▶ すべての受益者に対するコミュニケーション計画
- ▶ エンドユーザー動機付け
- ▶ フィードバックと効果測定

AdMaxプログラムは、ユーザーの導入率を、支援なしの典型的な展開に比べて少なくとも50% 改善します。AdMaxは、日立 IDのソリューションデリバリー部隊により、スタンドアローンのソリューションとしてか、完全なソリューションデリバリープログラムの一部として提供されます。

 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