The Leading Company of the Biometrics

【技術資料】

ActiveDirectory との連携について

DIGITAL DEVELOPMENT SYSTEMS

D061300-003A

目次

1. はじめに

本書では、UBF と Active Directory（以下 AD と略す）の間で連携して行われる、アカウントパスワードの変更操作、および UBF クライアントの動作に影響するグループポリシーについて記載します。

また、連携動作が行われない項目について「4. AD 連携が行われない操作」に記載します。

2. アカウントパスワードの変更

2.1. パスワード変更手段ごとの動作の違い

パスワードを変更する手段について、手段ごとに変更対象となるパスワード、および変更不可時※ の動作が異なります。その違いを「表 1 パスワード変更手段とパスワード変更対象」に示します。

※ パスワード変更不可時とは

以下のような場合には、AD で管理されているパスワードを変更することができません。

- UBF に登録されているパスワードと AD に登録されているパスワードが異なる場合。
  ⇒UBF に登録されているパスワードを変更前のパスワードとして AD に提示してパスワード変更を行うため、変更前のパスワード認証エラーとなり変更に失敗します。
- 実行ユーザが、権限等アカウントのパスワード変更に必要な条件を満たさない場合。
- 設定しようとしたパスワードが AD のパスワードポリシーを満たさない場合。
- AD と通信できない場合。

表 1 パスワード変更手段とパスワード変更対象

No.	パスワード変更手段	パスワード変更対象	
		UBF	AD
1	UBF ユーティリティ	○ （両方変更可能のときのみ変更）	
2	Windows パスワード変更画面 （UBF クライアントソフトインストール済み PC）	○ （両方変更可能のときのみ変更）	
3	UBF 管理ツール	○ （AD 側がエラーの場合も変更）	△ （エラーの場合変更しない）
4	ランダムパスワード設定コマンド	○ （両方変更可能のときのみ変更）	
5	インポートコマンド・UBF 管理ツールのインポート	○	× （常に変更しない）
6	AD 側でのパスワードリセット	× （常に変更しない）	○

【記号】○：変更する　△：エラーの場合変更しない　×：変更しない

次章以降に、No.1～4 の項目についての処理フローを記述します。

2.1.1. UBF ユーティリティでのパスワード変更処理フロー

ドメインユーザが UBF ユーティリティでパスワードを変更する場合の処理フローを、「図 1 UBF ユーティリティでのパスワード変更処理フロー」に示します。パスワード変更処理は、「①AD のユーザ情報」→「②指紋管理サーバ（UBF）のユーザ情報」の順で行います。AD 側でパスワード変更に失敗した場合は、UBF 側の変更処理を行わず、エラーメッセージを表示して終了します。

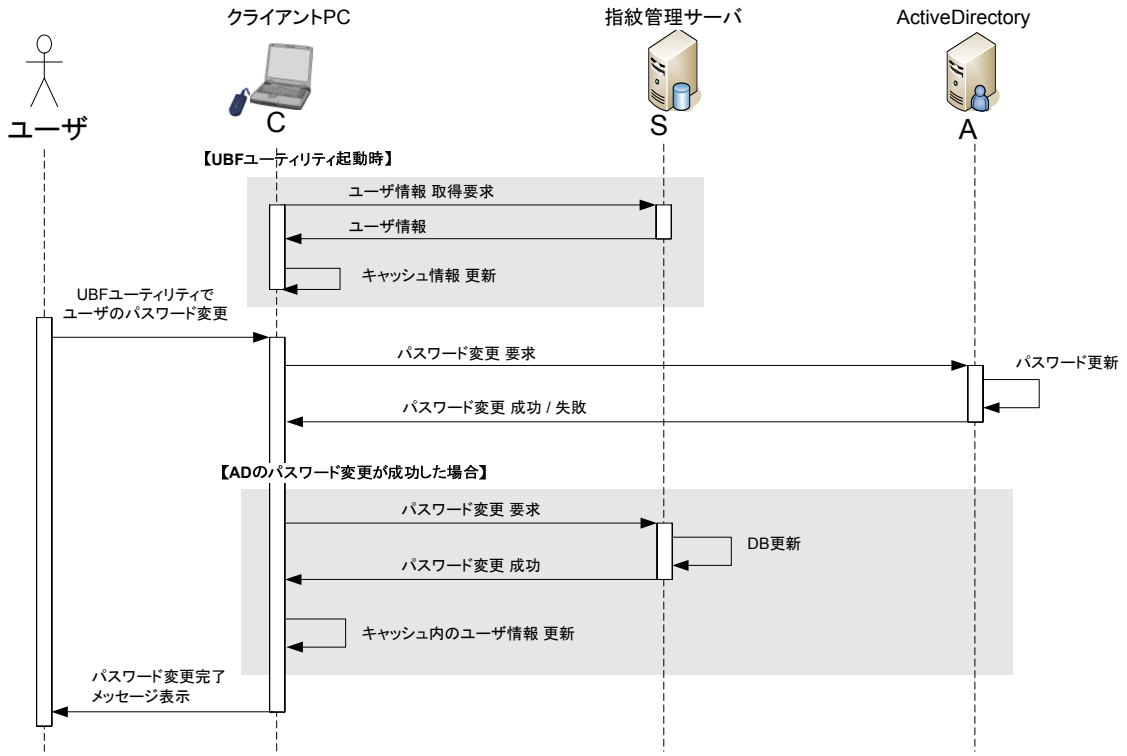

図 1 UBF ユーティリティでのパスワード変更処理フロー

2.1.2. Windows パスワード変更画面での処理フロー

ドメインユーザがWindowsパスワード変更画面※でパスワードを変更する場合の処理フローを、「図 2 Windowsパスワード変更画面での処理フロー」に示します。動作は「2.1.1. UBFユーティリティでのパスワード変更処理フロー」と同様で、AD側でパスワード変更に失敗した場合は、UBF側の変更処理を行わず、エラーメッセージを表示して終了します。

※ Windowsパスワード変更画面とは

以下のような場合にクライアントで表示されるパスワード変更画面です。

- AD でパスワードの有効期限を設定した場合。
- AD で「ユーザーは次回ログオン時にパスワード変更が必要」に設定した場合。
- Ctrl+Alt+Del キー押下時に表示される「Windows のセキュリティ画面」で「パスワードの変更」を選択した場合。

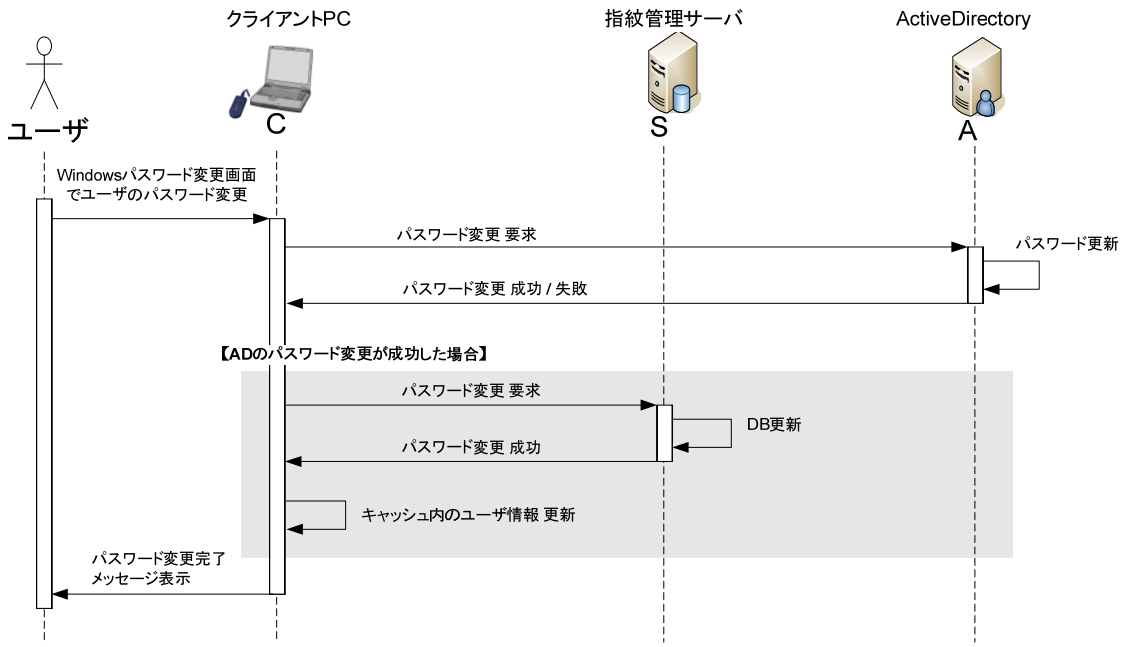

図 2 Windows パスワード変更画面での処理フロー

2.1.3. UBF 管理ツールでのパスワード変更処理フロー

管理者が UBF 管理ツールで、ドメインユーザのパスワードを変更する場合の処理フローを「図 3 UBF 管理ツールでのパスワード変更処理フロー」に示します。UBF 管理ツールでのパスワード変更処理では、AD 側のパスワード変更に失敗した場合でも、警告画面を表示し指紋管理サーバ（UBF）側の変更処理を実行します。

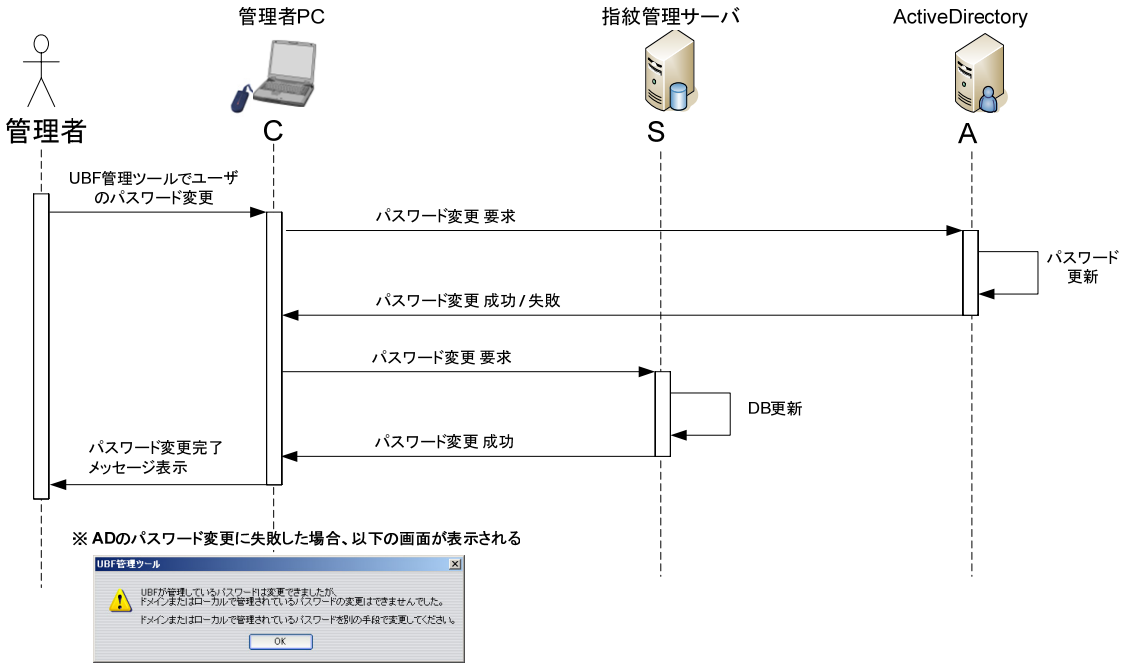

図 3 UBF 管理ツールでのパスワード変更処理フロー

2.1.4. ランダムパスワード設定コマンド実行時の処理フロー

管理者が指紋管理サーバ上で、ランダムパスワード設定コマンドを実行する場合の処理フローを「図 4 ランダムパスワード設定コマンド実行時の処理フロー」に示します。ランダムパスワードコマンドでのパスワード変更処理では、AD 側でパスワード変更に失敗した場合、指紋管理サーバ（UBF）側の変更処理を行わず、エラーメッセージを表示して終了します。

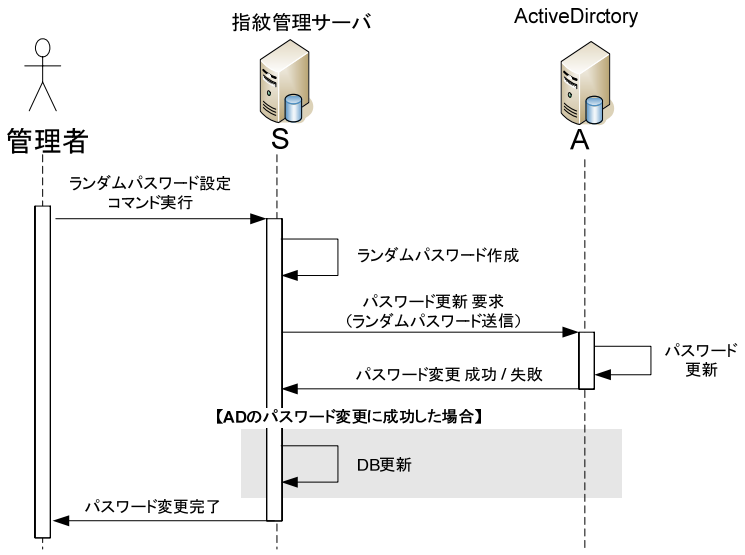

図 4 ランダムパスワード設定コマンド実行時の処理フロー

また、ランダムパスワード発行後は、利用者の次回ログオンに注意を払う必要があります。「2.2. UBF パスワード自動更新機能について」もあわせて参照ください。

2.2. UBF パスワード自動更新機能について

UBF には、ユーザが Windows ログオン時に UBF のログオン画面で入力したパスワードが Windows から有効なパスワードと判断された場合、UBF（指紋管理サーバ）で管理しているパスワードを内部的に更新する機能があります。これを「パスワード自動更新機能」といいます。上記特性について、特に以下のような場合に、意識・注意する必要があります。

2.2.1. AD 構築済み環境に UBF を新規導入する場合

管理者が運用中の AD で管理されている利用者の Windows パスワードを知らない場合でも、利用者がクライアント PC のログオン画面で正しいパスワードを入力することで、UBF へのパスワード登録を行うことができます。この場合の処理フローは以下のようになります。

(1) AD に既に登録済みのユーザ（ユーザ名：*user*、パスワード：*pass*）が存在。
(2) ユーザの AD パスワード（*pass*）を知らない管理者が、UBF のユーザ登録を実施。
（ユーザ名：*user*、UBF パスワード：*temp*）
(3) ユーザが UBF インストール済み PC にて、パスワード（*pass*）でログオン。
⇒入力したパスワード（*pass*）が Windows に有効と判断されるため、UBF の登録パスワードを更新（*temp→pass*）

ユーザが指紋登録を行い指紋認証でログオンできることを確認した後、ランダムパスワードの適用や、パスワードログオンを禁止にするなどの方法でセキュリティを高めていくことで、スムーズな運用開始とその後のセキュリティ向上が可能です。

2.2.2. ランダムパスワードコマンド・UBF 管理ツールでのパスワード変更時

管理者によるパスワード変更を実施後、次のログオン時に利用者がログオン画面で「変更前のパスワード」を入力してログオンを行った場合、タイミング（※補足情報を参照）により Windows から有効と判断されてしまう場合があります。この場合、上記「UBF パスワード自動更新機能」により「変更前のパスワード」が UBF に正式登録されてしまいます。以下の「対策」の内容を参照し、対策を行ってください。

※ 補足情報

クライアント側のWindowsで、変更前のパスワードを受け入れてしまうタイミングは、Windows XP の高速ログオン機能に由来します。（高速ログオン機能とは、ドメインコントローラと通信できる場合でも、Windowsに高速にログオンするためにログオン時にWindowsのキャッシュ情報のみでログオンする機能です。）【ご参考】Microsoft社サポートサイト http://support.microsoft.com/kb/305293/ja

高速ログオン機能が有効となっている場合（デフォルト設定では有効）には、変更前のパスワードが Windows 側から正しいパスワードであると判断されてしまいます。

<対策>

利用者がパスワードを変更したことを認識できない場合（管理者側、サーバ側で一方的に変更した場合)、以下のような方法で、利用者のパスワードの使用を禁止・制御する必要があります。

(1) 対象ユーザのパスワードログオンを禁止する
(2) パスワード欄を非表示にする
(3) 指紋認証でログオンするよう通知する

また、補足情報に示した高速ログオン機能はグループポリシーで無効にすることも可能です。「3.グループポリシー設定への対応」の No.9 を参照してください。

3. グループポリシー設定への対応

グループポリシーでも、パスワードやログオンに関するものは、UBF の動作に密接に関係します。UBF 側の動作に影響するグループポリシーを「表 2 グループポリシーの設定と UBF の動作」に示します。一般に AD のグループポリシーは、ローカルセキュリティポリシーより優先されて適用され、グループポリシーが未定義の場合はローカルセキュリティポリシーが適用されます。

各ポリシーの詳細については、OS 毎のヘルプをご確認ください。

表 2 グループポリシーの設定と UBF の動作

No	ポリシーの設定	UBF 上の動作	結果
1	パスワード変更禁止期間を設定	ユーザのパスワードを変更	UBF ユーティリティ、管理ツール
			「パスワードを変更できる権限がありません。」 と表示され、変更できません。
		ランダムパスワード設定コマンドを実行	更新に失敗します。
2	パスワードの長さを設定	ドメインユーザのパスワードを長さが設定文字数以下のパスワードに変更	UBF ユーティリティ
			「パスワードはパスワードポリシーの要件を満たしていません。パスワードの最短の長さ、パスワードの複雑性、およびパスワード履歴の要件を確認してください。」 と表示され変更できません。
			管理ツール
			「UBF が管理しているパスワードは変更できましたが、ドメインまたはローカルで管理されているパスワードの変更はできませんでした。ドメインまたはローカルで管理されているパスワードを別の手段で変更してください。」 と表示され、UBF 側のパスワードのみが変更されます。
3	「パスワードは、複雑さの要件を満たす必要がある」を「有効」に設定	ドメインユーザのパスワードを要件の満たさないパスワードに変更	UBF ユーティリティ
			「パスワードはパスワードポリシーの要件を満たしていません。パスワードの最短の長さ、パスワードの複雑性、およびパスワード履歴の要件を確認してください。」 と表示され変更できません。
			管理ツール
			「UBF が管理しているパスワードは変更できましたが、ドメインまたはローカルで管理されているパスワードの変更はできませんでした。ドメインまたはローカルで管理されているパスワードを別の手段で変更してください。」 と表示され、UBF 側のパスワードのみが変更されます。

No	ポリシーの設定	UBF 上の動作	結果
			※要件には以下のものがあります。 ・ユーザのアカウント名またはフル ネームのかなりの部分を使用しない。 ・長さは 6 文字以上にする。 ・次の 4 つのカテゴリのうち 3 つから文字を使う。 ・英大文字 (A ～ Z) ・英小文字 (a ～ z) ・10 進数の数字 (0 ～ 9) ・アルファベット以外の文字 (`~!@#^&*()_+-={}|[];'<>?/)
4	「パスワードの履歴を記憶する」を設定	ドメインユーザのパスワードを、履歴に記憶されているパスワードに変更	UBF ユーティリティ
			「パスワードはパスワードポリシーの要件を満たしていません。パスワードの最短の長さ、パスワードの複雑性、およびパスワード履歴の要件を確認してください。」 と表示され変更できません。
			管理ツール
			「UBF が管理しているパスワードは変更できましたが、ドメインまたはローカルで管理されているパスワードの変更はできませんでした。ドメインまたはローカルで管理されているパスワードを別の手段で変更してください。」 と表示され、UBF 側のパスワードのみが変更されます。
5	「シャットダウン: システムをシャットダウンするのにログオンを必要としない」を「無効」に設定	ログオン画面	シャットダウンボタンが「無効」になります。
6	「対話型ログオン: Ctrl+Alt+Del を必要としない」を設定	ログオン画面	UBF のクライアント動作設定に同じ「1001：Ctrl+Alt+Del 押下を要求しない」があり、UBF のクライアント動作設定が優先して設定されます。グループポリシーの設定は、反映されません。
7	「対話型ログオン：ドメイン コントローラが利用できない場合に使用する､前回ログオンのキャッシュ数」を「0」に設定	キャッシュ認証を行う	キャッシュ認証時、UBF 側では、指紋でもパスワードでもログオンできますが、Windows 側で「ログオンできません。ログオン先ドメイン[ドメイン名]は利用できません。」と表示され、ログオンできません。 通常の認証時は、影響ありません。
8	「対話型ログオン：最後のユーザ名を表示しない」を「有効」に設定	ログオン画面	グループポリシーで､最後のユーザ名を表示しない設定をしていても、UBF のクライアント動作設定「1002：ユーザ名履歴数」が優先されて設定されます。
9	[コンピュータの構成]>[管理用テンプレート]>[システム]>[ログオン] 「コンピュータの起動及びログオンで常にネットワークを待つ」を「無効」（または「未構成」）に設定	ドメインユーザが Windows XP の PC よりログオン	ドメインコントローラと通信できる場合でも、Windows のキャッシュ情報のみを使用して Windows のログオンが行われます。 UBF のランダムパスワードコマンド･管理ツールでパスワード変更を行った直後のログオンを行う場合は､「2.2.2.ランダムパスワードコマンド・UBF 管理ツールでのパスワード変更時」に示す UBF のパスワード自動更新機能との間の動作に注意が必要です。 左記ポリシーを「有効」に設定することで、ドメインコントローラと接続可能な場合は､ドメインコントローラの情報を確認してから Windows のログオンが行われるようになり、上記 UBF のパスワード自動更新機能との問題を回避することができます。

4. AD 連携が行われない操作

「表 3 AD 連携が行われない操作」に示す操作については、UBF と AD の間の連携動作が行われません。ご注意ください。

表 3 AD 連携が行われない操作

No	連携されない操作	備考
1	AD 側でのアカウント追加、削除	UBF 側でも同様の操作を行う必要があります。
2	UBF 側でのアカウント追加、削除	AD 側でも同様の操作を行う必要があります。 既に AD に登録されているユーザを UBF に登録する場合、登録時に設定するパスワードは AD 側には設定されません。(UBF へのユーザ登録時に設定するパスワードで、AD 側のパスワードを変更することはありません。) この場合、UBF へのユーザ登録後に以下のいずれかの方法で UBF と AD のパスワードを一致させてください。 (1) AD 側でパスワードをリセットする。 (2) UBF クライアントがインストールされた PC から、ユーザが AD に登録されているパスワードでログオンする。(この場合、「UBF パスワード自動更新機能」により UBF のパスワードが更新されます。詳しくは「2.2.1. AD 構築済み環境に UBF を新規導入する場合」を参照してください。)
3	AD 側でのパスワードリセット	AD 側でのパスワード変更・リセット時は、UBF 側で登録されているパスワードの変更が行われません。 UBF 導入中は、UBF 管理ツールでパスワードを変更するようにしてください。
4	インポートコマンドや UBF 管理ツールのインポートでのユーザのパスワード更新	UBF 側のパスワードは更新されますが、AD 側のパスワードは更新されません。インポート後に、両者のパスワードを一致させるには AD 側でインポート時に設定したパスワードを設定してください。