JCCH・セキュリティ・ソリューション・システムズ

プライベートCA Gléas ホワイトペーパー

Windowsスマートカードログオン

Ver.1.2

2011 年 9 月

目次

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベートCA Gléas」で発行した電子証明書とGemalto .NET（ドットネット）製品を利用して、Microsoft CorporationのWindowsにおけるスマートカードログオンを行う環境を構築するための設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例としてご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、最終項のお問い合わせ先までお気軽にご連絡ください。

1.2. 本書における環境

本書における手順は、以下の環境で動作確認を行っています。

- 【ドメインコントローラ】Microsoft Windows Server 2008 R2 Standard SP1
  ※以後、「ドメインコントローラ」と記載します
- 【認証局】JS3 プライベートCA Gléas （バージョン1.7）
  ※以後、「Gléas」と記載します
- 【クライアントPC】Microsoft Windows 7 Professional SP1
  ※以後、「クライアントPC」と記載します
- 【認証デバイス】Gemalto .NETカード
  ※以後、「認証デバイス」と記載します
  ※.NET製品には、ICカードタイプとUSBトークンタイプがあり、どちらでも同様の動作となります（サードパーティのICカードリーダのインストールを除く）
  ※本環境では、ICカードリーダにGemalto PC Twin Reader（USB接続）を利用しています

以下については、本書では説明を割愛します。

- ドメインコントローラのセットアップ
- Gléasでのユーザ登録やクライアント証明書発行等の基本操作
- Windows 7でのネットワーク設定等の基本設定
- 認証デバイスのパーソナライズ等の基本操作

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

1.3. 電子証明書の発行時における留意事項

Gléasで電子証明書を発行する際に以下の点に留意する必要があります。

- ドメインコントローラ証明書の発行には、「Microsoftドメインコントローラ」テンプレートを用います。その際には、ドメインコントローラのホスト名、CRL配布ポイント、GUID（Global Unique Identifier）を正しく設定する必要があります

  以下は「dc01.js3-test.local」という名前のドメインコントローラ上でGUIDを取得するVBスクリプトサンプルです。

  ```
  Set objUser = GetObject("LDAP://CN=dc01,OU=Domain Controllers,DC=js3-test,DC=local")
  Wscript.Echo objUser.GUID
  ```

- スマートカード用証明書の発行には、「スマートカードログオン」テンプレートを用いて証明書を発行します。その際には、UPN（ユーザプリンシパル名）、CRL配布ポイントを正しく設定する必要があります

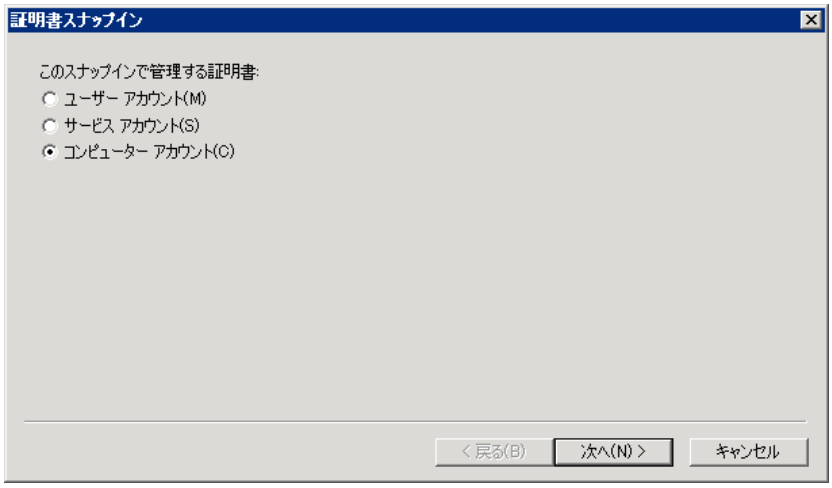
2. ドメインコントローラでの設定

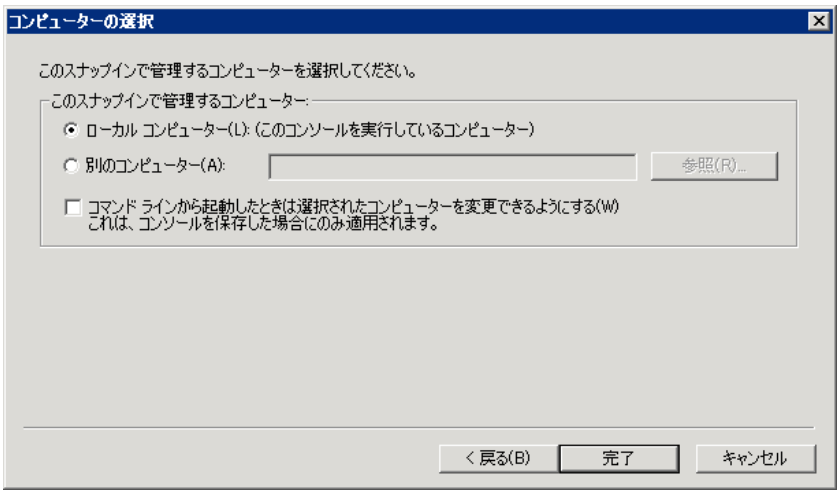
2.1. サーバ証明書のインポート

ドメインコントローラにドメインコントローラ証明書と、今回利用するクライアント証明書のトラストアンカとなるルート証明書をインポートします。

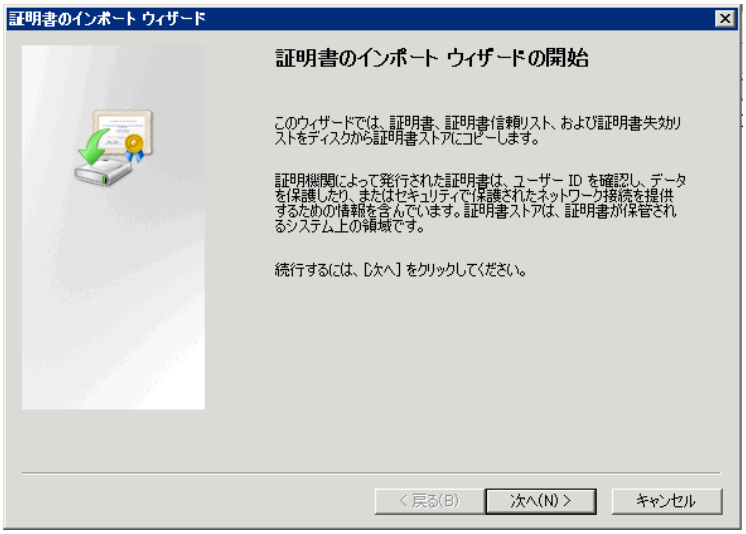
ドメインコントローラで MMC（Microsoft Management Console）を開き、メニューの[ファイル(F)] > [スナップインの追加と削除(N)]より[証明書]を追加します。

「証明書のスナップイン」では、[コンピューター アカウント(C)]を選択し、次の「コンピューターの選択」では、[ローカルコンピューター(L)]を選択し、[完了]をクリックします。



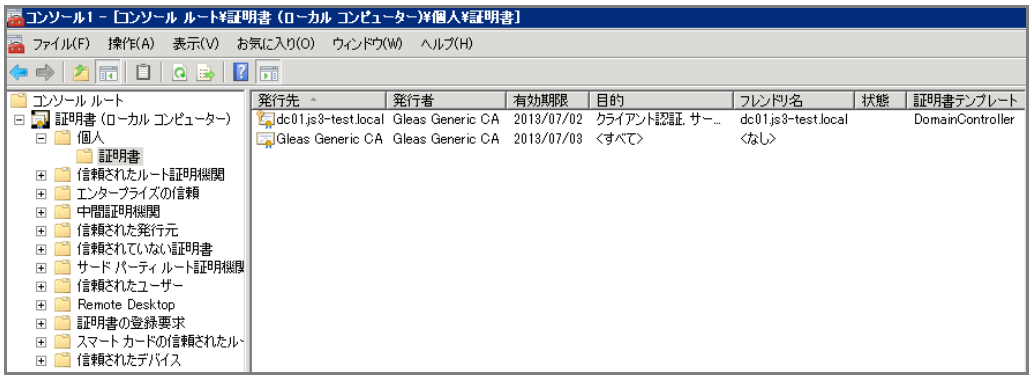


スナップインが追加されたら左側のペインより[証明書] > [個人]と展開し、右側のペインで右クリックして、[すべてのタスク(K)] > [インポート(I)]をクリックします。「証明書のインポートウィザード」が開始されるので、サーバ証明書とルート証明書をインポートします。



ページ	設定
証明書のインポートウィザードの開始	[次へ(N)]をクリック
インポートする証明書ファイル	Gléas よりダウンロードした PKCS#12 ファイル（拡張子：p12）を指定して、[次へ(N)]をクリック
パスワード	Gléas から PKCS#12 ファイルをダウンロードする際に設定したパスワードを入力して、[次へ(N)]をクリック
証明書ストア	[証明書をすべて次のストアへ配置する(P)]を選択し、[証明書ストア]で[個人]が選ばれていることを確認し、[次へ(N)]をクリック
証明書インポートウィザードの終了	[完了]をクリック

完了後、[個人]に Gléas よりダウンロードしたドメインコントローラ用証明書と、Gléas のルート証明書（発行元と発行先とが同じ名前の証明書）がインポートされていることを確認します。

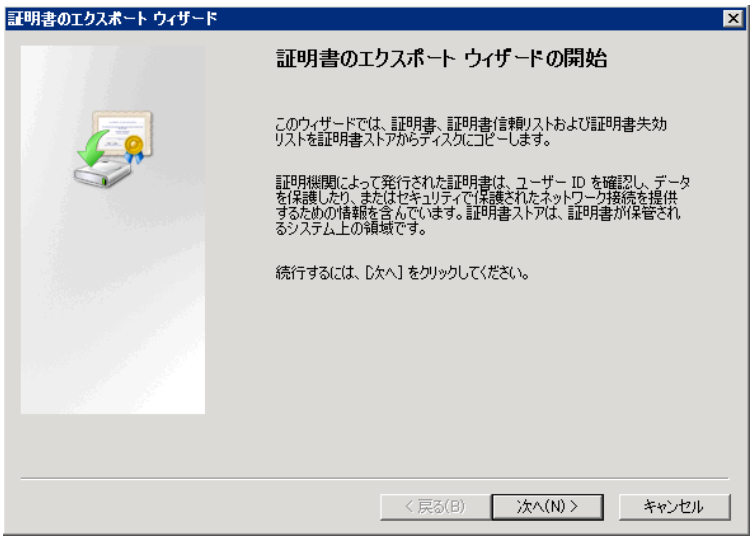


2.2. ルート証明書のエクスポート

次に、ルート証明書をファイルとして取得します。

※既に Gléas よりルート証明書をダウンロードしてある場合は、エクスポートを行う必要はありません。この場合はルート証明書を削除して 2.3 に進んでください。

インポートされた Gléas のルート証明書を右クリックし、[すべてのタスク(K)] > [エクスポート(E)]をクリックします。「証明書のエクスポートウィザード」が開始されるので、ルート証明書をエクスポートします。



ページ	設定
証明書のエクスポートウィザードの開始	[次へ(N)]をクリック
エクスポートファイルの形式	DER encoded binary X.509(.CER)か、Base64 encoded X.509(.CER)を選択し、[次へ(N)]をクリック
エクスポートするファイル	保存先を指定して、[次へ(N)]をクリック
証明書エクスポートウィザードの終了	[完了]をクリック

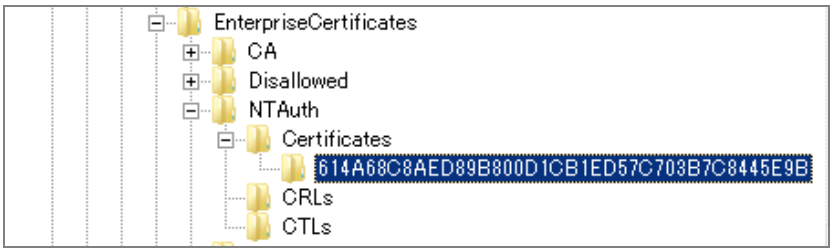
エクスポートが終了したら、[個人]に入っているルート証明書は不要なため削除します。

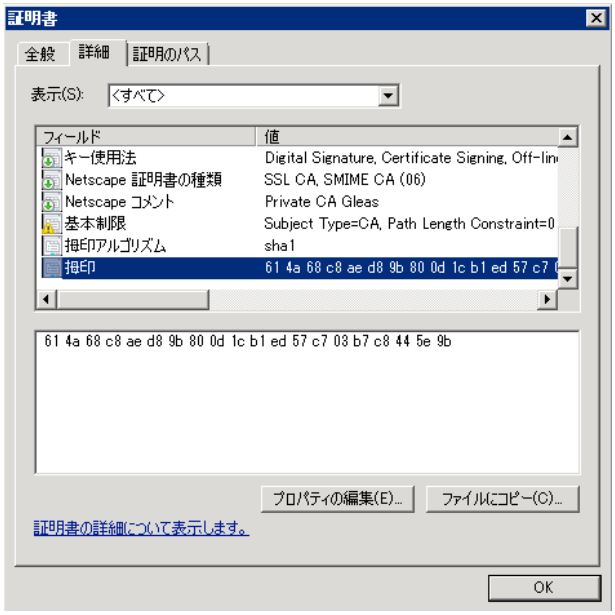
2.3. NTauth ストアへのインポート

次に、Windows ドメインとして信頼するルート認証局の証明書を NTauth ストアと

呼ばれる格納領域に登録します。
コマンドプロンプトを開き、以下のコマンドを入力し NTauth ストアにルート証明書を格納します。
certutil -dspublish -f [*filename*] NTAuthCA
※[filename]には、エクスポートしたルート証明書を指定します。

コマンド実行後、以下のレジストリにルート証明書の拇印と同じ名前のレジストリキーが追加されます。
HKLM¥SOFTWARE¥Microsoft¥EnterpriseCertificates¥NTAuth¥Certificates
※追加されない場合は、gpupdate コマンドでポリシーの更新を行ってください。



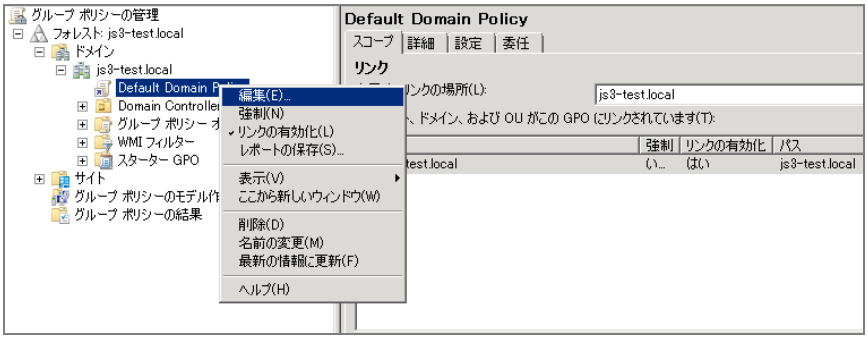


2.4. グループポリシーの設定

ドメインに参加しているコンピューターに対して信頼するルート認証機関を追加する設定を行います。

[スタートメニュー] > [管理ツール] > [グループポリシーの管理]を開き、対象となるグループポリシーオブジェクトを選択し右クリックし、[編集]をクリックします。

以下は Default Domain Policy を編集する場合の例です。



グループポリシー管理エディターが開きますので、左側ペインより[コンピューターの構成] > [ポリシー] > [Windows の設定] > [セキュリティの設定] > [公開キーのポリシー] > [信頼されたルート証明機関]を開きます。
次にメニューより[操作(A)] > [インポート(I)]を選択すると、証明書のインポートウィザードが起動するので、ルート証明書を登録します。

ページ	設定
証明書のインポートウィザードの開始	[次へ(N)]をクリック
インポートする証明書ファイル	エクスポートしたルート証明書ファイルをを選択し、[次へ(N)]をクリック
証明書ストア	[証明書をすべて次のストアへ配置する(P)]を選択し、[証明書ストア]で[信頼するルート認証機関]が選ばれていることを確認し、[次へ(N)]をクリック
証明書インポートウィザードの終了	[完了]をクリック

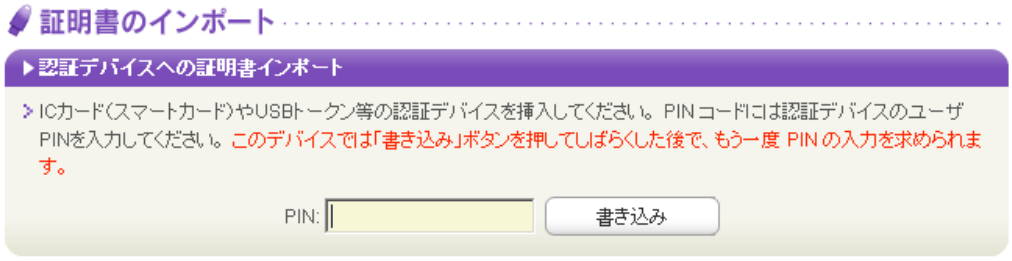
以上でWindows Serverの設定は完了です。

3. Gléasでの認証デバイスの準備

3.1. 認証デバイスへの電子証明書インポート

GléasのRAにログインし、スマートカード用に発行した証明書の詳細画面まで移動します。
エンドユーザ用の認証デバイスを管理者端末に接続し、画面上部の[トークンへのインポート]をクリックします。
※事前に認証デバイスのパーソナライズを行っている必要があります。

認証デバイスに事前に設定したPIN（暗証番号）を入力し、証明書のインポートを行います。



元の画面に戻ればインポートは成功です。
この時に画面を下にスクロールしていくと、インポート先のデバイス情報が付加されています。

また[認証デバイス]メニューでは、この認証デバイスにインポートした証明書を確認することが可能となります。

以上で、認証デバイスの準備は終了です。
※Gléasでは、パーソナライズした認証デバイスをエンドユーザに配布し、エンドユーザに証明書のインポートを行わせることも可能です。詳細はJS3までお問い合わせください

4. クライアントPCでの作業

4.1. 認証デバイスのセットアップ

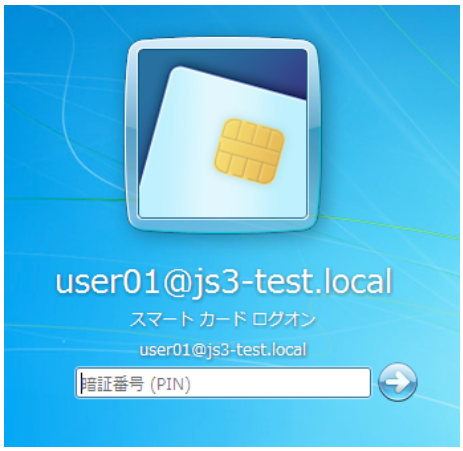
認証デバイスのドライバインストールを行います。
詳細は弊社提供のマニュアル等を参照してください。

なお、Widnows7では認証デバイスを挿した状態でクライアントPCを起動するとログオン前に自動的にドライバ類のインストールが行われます（要インターネット接続）。

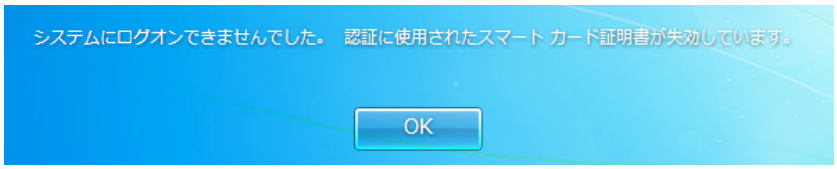
4.2. スマートカードログオンの利用

ドライバがインストールされた状態でクライアントPCを起動すると、認証デバイスが自動的に読み込まれログオンユーザ名が表示されるのでクリックします。
※これまでログオンしていたユーザでのログオン画面が表示される場合は、[ユーザの切り替え(W)]をクリックし、スマートカードログオンするユーザを選択します（この時、認証デバイスはクライアントPCに挿しておきます）。

ログオン画面が表示されるので、認証デバイスに予め設定しているPINを入力してログオンします。



失効しているスマートカード証明書でログオンしようとすると、以下のメッセージが表示されエラーとなります。

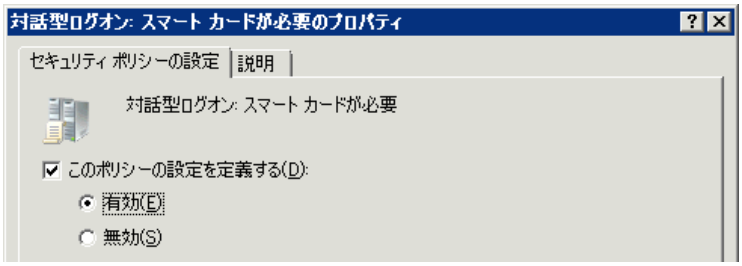


5. その他設定

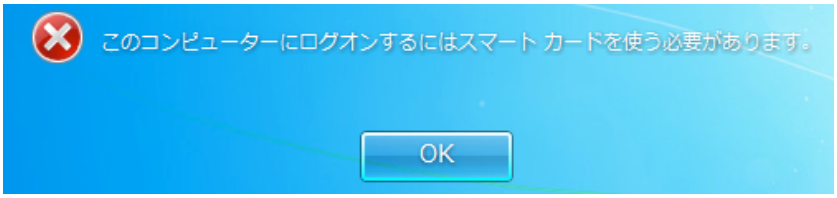
5.1. クライアント PC のログオンをスマートカードに限定する設定

[スタートメニュー] > [管理ツール] > [グループポリシーの管理]を開き、対象となるグループポリシーオブジェクトを選択し右クリックし、[編集]をクリックします。

グループポリシー管理エディターが開きますので、左側ペインより[コンピューターの構成] > [ポリシー] > [Windowsの設定] > [セキュリティの設定] > [ローカルポリシー] > [セキュリティオプション]を展開し、右側ペインの[対話型ログオン：スマートカードが必要]を有効に定義します。



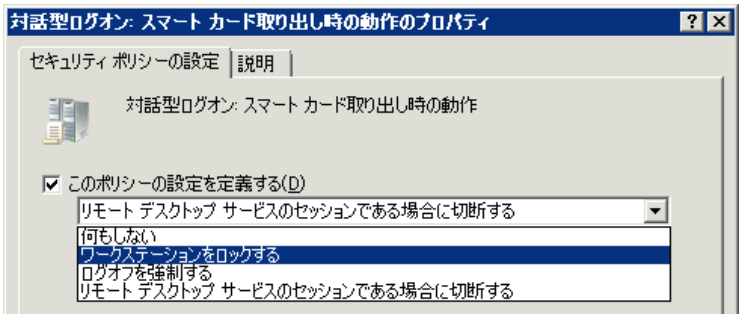
このポリシーが適用されたクライアントPCでは、ユーザID・パスワードによるログオンが拒否されるようになります。



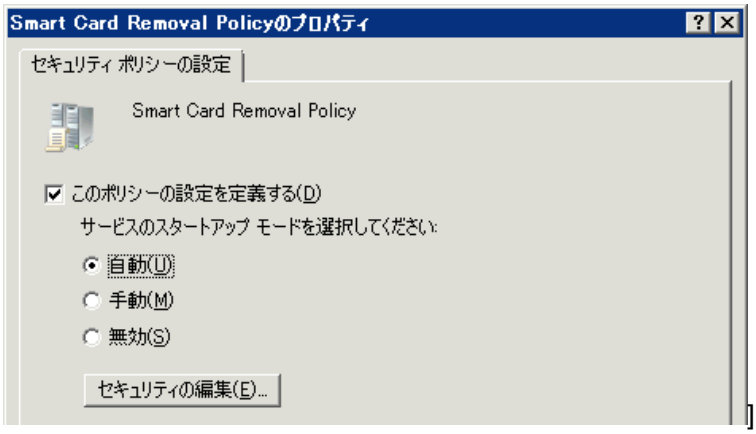
5.2. スマートカード取り出し時の動作の設定

[スタートメニュー] > [管理ツール] > [グループポリシーの管理]を開き、対象となるグループポリシーオブジェクトを選択し右クリックし、[編集]をクリックします。

グループポリシー管理エディターが開きますので、左側ペインより[コンピューターの構成] > [ポリシー] > [Windowsの設定] > [セキュリティの設定] > [ローカルポリシー] > [セキュリティオプション]を展開し、右側ペインの[対話型ログオン：スマートカード取り出し時の操作]を以下のどれかに定義します。



このポリシーはSmart Card Removal Policyサービスが起動していないと動作しないので、このサービスも自動起動するようにします。
グループポリシー管理エディターで、左側ペインより[コンピューターの構成] > [ポリシー] > [Windowsの設定] > [システム サービス]と展開し、右側ペインでSmart Card Removal Policyを自動起動するよう定義します。

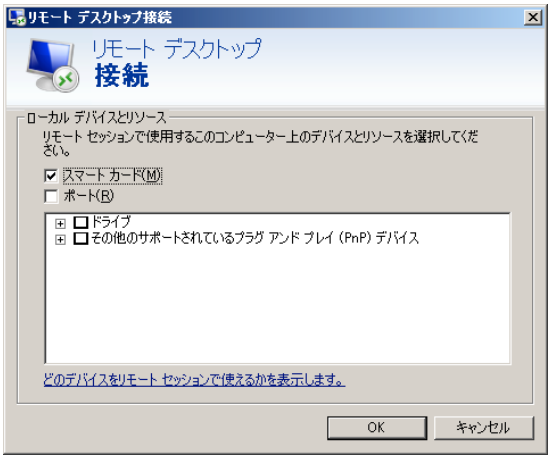


このポリシーをクライアントPCに適用すると、定義した通りの動作を行います。

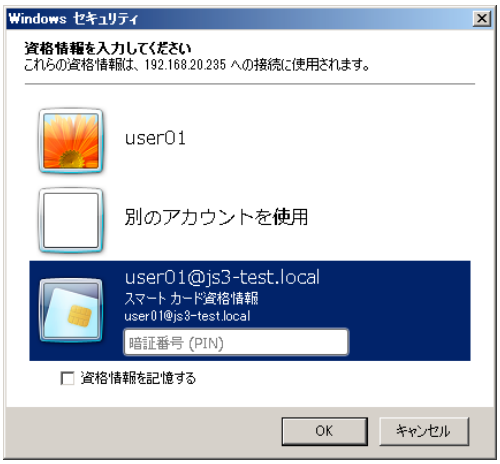
5.3. スマートカードログオンが有効な PC にリモートデスクトップをする設定

※同じドメインに参加しているPCより行ってください

リモートデスクトップ接続を起動し、[オプション] > [ローカルリソース]タブ > ローカルリソースとデバイスの[詳細]をクリックし、開いた画面で[スマートカード(M)]にチェックを入れ、接続します。



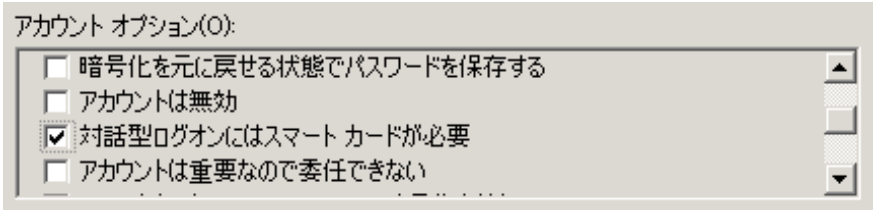
「資格情報を入力して下さい」というダイアログボックスが表示されたらスマートカードを選択し、PINを入力しログオンします。



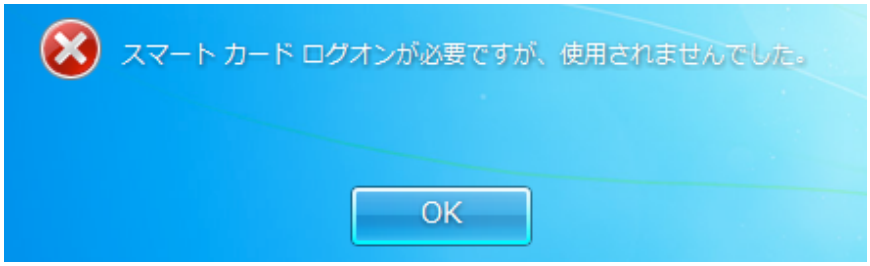
5.4. 特定のユーザに対しスマートカードログオンを強制する設定

[スタートメニュー] > [管理ツール] > [Active Directory ユーザーとコンピューター]を開き、対象となるユーザオブジェクトを選択し右クリックし、[プロパティ(R)]をクリックします。

そのユーザのプロパティが開きますので、 [アカウント]タブをクリックし [アカウントオプション(O):]項目の[対話型ログオンにはスマートカードが必要]にチェックを入れます。



この設定がされたユーザアカウントでは、ユーザID・パスワードによるログオンが拒否されるようになります。



6. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■Gléasや検証用の証明書に関するお問い合わせ

株式会社JCCH・セキュリティ・ソリューション・システムズ
Tel: 050-3821-2195
Mail: sales@jcch-sss.com