



myuToken 説明書



Ver 1.3.1.4 版

(株) iCanal 平山 直紀



=====

iCanal Type1 使用許諾書(2010/09/13)

=====

本使用許諾書は、本ソフトウェアの開発者である 平山 直紀 とユーザとの間の本ソフトウェアに関する使用許諾等について定めます。本ソフトウェアとは、コンピュータ ソフトウェアだけでなく、ドキュメントを含みます。本ソフトウェアをインストール、複製、または使用することによって、ユーザーは本使用許諾書の条項を承諾されたものとします。本使用許諾書の条項に同意されない場合、開発者はユーザーに本ソフトウェアのインストール、使用または複製のいずれも許諾できません。

第1条 著作権

本ソフトウェアは著作権法により保護されています。著作権は開発者の平山 直紀に帰属します。

第2条 使用条件

- (1) 本ソフトウェアは、フリーウェアです。
- (2) ユーザーは、本ソフトウェアを配布する会社には迷惑がかからないようにしてください。本ソフトウェアに関する、ご意見等は、直接、開発者のほうへご連絡ください。

第3条 禁止事項

本ソフトウェアをリバース エンジニアリング、逆コンパイル、逆アセンブルすることは禁止します。

第4条 再配布

ユーザーは、本ソフトウェアに含まれるすべてのファイルを配布されたそのままの状態でのみ再配布することができません。

第5条 転載

ユーザーが本ソフトウェアを雑誌、書籍などに転載していただいても構いませんが必ず開発者にご連絡ください。

第6条 輸出規制

- (1) 本ソフトウェアを日本国およびその他の国のすべての法律・規則（以下「輸出関連法規」といいます）に違反して輸出しないこと
- (2) 核兵器、化学兵器、生物兵器の拡散防止に関する規定を含む輸出関連法規によって禁じられている用途で使えないこと

上記(1)(2)の両方を保証すると共に、それらの諸規制等を遵守しなくてはなりません。

第7条 免責事項

開発者は、本ソフトウェアに関して発生したいかなるトラブルや損失などについても、一切の責任を負わないものとします。本ソフトウェアに欠陥があったとしても同様です。既知でない不具合を報告していただいた場合、修正することはありますが義務は負いません。本ソフトウェアのサポートについては、メールで問い合わせれば、回答をすることはありますが義務は負いません。



1. 概要	4
1-1. myuToken とは	4
1-2. 動作環境	4
1-3. 必要なハードウェア	4
1-3-1. フラッシュメモリカード	5
1-3-2. USB メモリ	5
1-3-3. IC カード	5
2. インストールとアンインストール	5
2-1. インストール	5
2-2. アンインストール	7
3. フラッシュメモリカード、USB メモリの設定	8
3-1. USB カードリーダーを IC カードリーダーに設定	8
3-2. シミュレーションモード	14
3-3. USB リーダ最大同時接続数	14
3-4. マルチリーダーの動作	14
3-5. Windows2000 における USB メモリ	14
4. カード鍵変更	15
5. カードフォーマット	15
6. IC カードにタイトルを設定	17
7. CSP	18
7-1. PKCS#12 ファイルのインポート	18
7-2. 証明書の表示	19
7-3. PIN 変更	20
7-4. CA証明書のIEストアへの転送	20
7-5. CA証明書のファイルへの出力	21
7-6. ブロック状態のカードの解除	21
8. ポリシー設定	22
9. IE ストアー一括削除	23
10. 自己署名証明書発行(PKCS#12 ファイル)	24
11. リードオンリーの IC カード	24
11-1. リードオンリーのカードの作り方	25
11-2. RO リライト	25
12. PKCS#11 icardmodpk.dll	26
13. デーモン再起動	27
14. iCanal CSP 優先	27
付録 A S/MIME の設定	28



1. 概要

1-1. myuToken とは

myuToken は USB メモリや SD カードなどのフラッシュメモリカードを IC カードにするソフトウェアです。miniSD やコンパクトフラッシュ、スマートメディアなどほとんどのメモリカードが利用できます。また本物の IC カード(myuCard) のミドルウェアとしても機能し、同様の操作で利用できるといった特徴があります。IC カードへのアクセスインターフェースは業界標準の MS-CAPI (BaseCSP、Microsoft Base Smart Card Crypto Provider)や CNG(KSP)や PKCS#11 が利用できます。カーネルモードのデバイスドライバのレベルでエミュレーションを行うため、USB メモリやフラッシュメモリカードは、セキュリティ以外は本物の IC カードと同じになります。電子証明書をいれて S/MIME や Office のデジタル署名で利用したり、プログラム開発向けや教育向けにも便利です。

最新情報は以下の URL

<http://www.icanal.co.jp/myutoken/>

<http://www.icf.jpn.org/web/icanal/myuToken/>

USB メモリや SD カードがなくても、ソフトウェアだけで IC カードをシミュレートする SiMyuCard もあるのでご利用ください。

<http://www.icanal.co.jp/SiMyuCard/>

<http://www.icf.jpn.org/web/icanal/SiMyuCard/>

1-2. 動作環境

CPU	x86 / x64
OS(32bit)	Windows 8.1 Windows 8 Windows 7 Windows Vista SP2 以降 WindowsXP SP3 以降 Windows2000 SP4 InternetExplorer6 SP1 (注 1)
OS(64bit)	Windows 8.1 Windows 8 Windows 7 Windows Vista SP2 以降 WindowsXP SP2

(注 1) 動作検証が行われているのは、日本語版 Windows と英語版 Windows のみ

1-3. 必要なハードウェア

フラッシュメモリカード、USB メモリ、IC カードのいずれか 1 つが必要です。あるいは IC カードシミュレータ



SiMyuCard(<http://www.icanal.co.jp/SiMyuCard/index.html>)であればソフトウェアのみで動作します。

IC カードは、機種によってハードウェアの機能が異なるため、フラッシュメモリカードや USB メモリと完全互換な動作が保証されているわけではありません。

1-3-1. フラッシュメモリカード

IC カード	SD カードや、コンパクトフラッシュ、メモリスティックなどのフラッシュメモリカード (16MByte 以上 かつ 2TByte 以下) ソフトウェア RSA 1024 / 2048bit データ格納容量 8KByte 以上
カードリーダー	フラッシュメモリカード用カードリーダー(バルクオンリー方式) ※一般に売られているカードリーダーのほとんど全てがバルクオンリー方式

1-3-2. USB メモリ

IC カード	USB メモリ (16MByte 以上 かつ 2TByte 以下) ソフトウェア RSA 1024 / 2048bit データ格納容量 8KByte 以上
カードリーダー	USB メモリ

1-3-3. IC カード

IC カード	(株)iCanal myuCard http://www.icanal.co.jp/myuCard.html MC-8K: ハードウェア RSA512 / 1024bit データ格納容量 4KByte
カードリーダー (推奨)	(株)日立製作所 USB タイプ HX-520UJ.K (株)日立製作所 USB タイプ HX-520UJ.J (株)日立製作所 PC カード TypeII (PCMCIA) HX-780PJ.J

2. インストールとアンインストール

2-1. インストール

Setup.exe ファイルをダブルクリックして実行します。

 Setup Setup Launcher Unicode iCanal Inc.	32bit 日本語版 (Windows2000以外)
 Setup_ENU Setup Launcher Unicode iCanal Inc.	32bit 英語版 (Windows2000以外)
 Setup64 Setup Launcher Unicode iCanal Inc.	64bit 日本語版 (Windows2000以外)

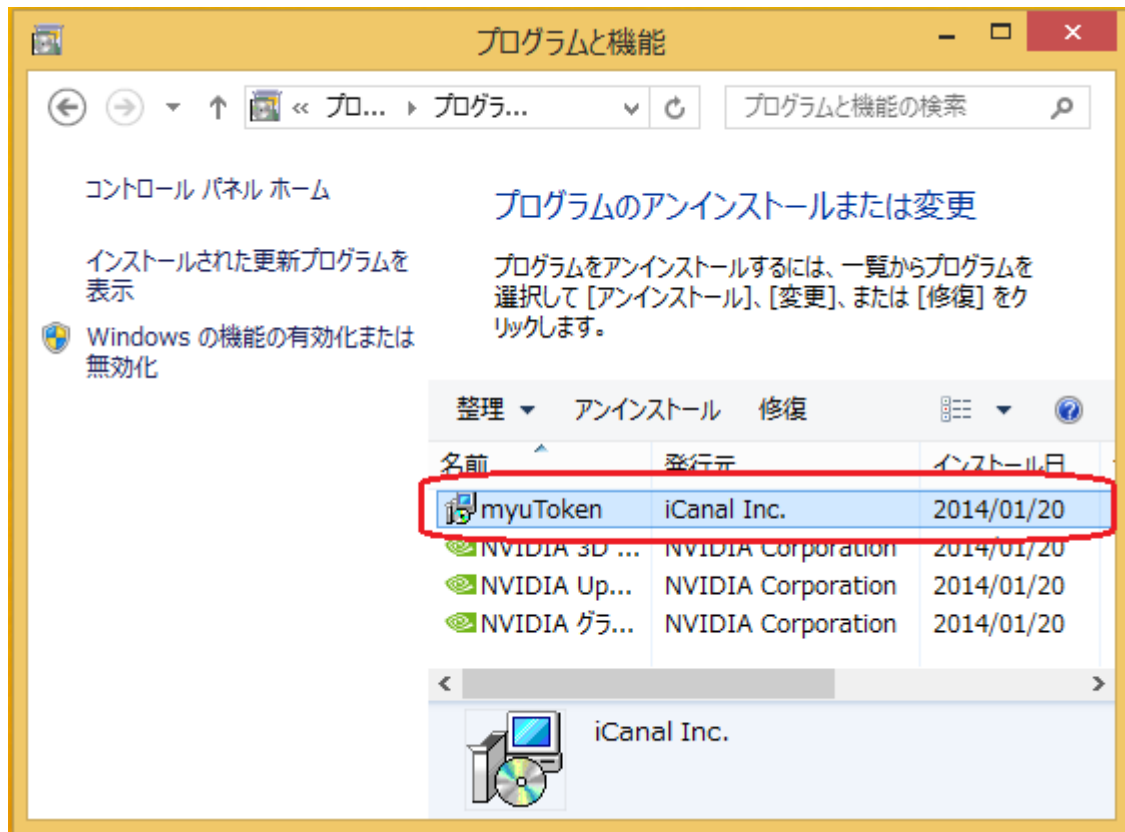
 Setup64_ENU Setup Launcher Unicode iCanal Inc.	64bit 英語版 (Windows2000以外)
 Setup2K 自己解凍実行ファイル 5.25.0.0	32bit 日本語版 (Windows2000用)
 Setup2K_ENU 自己解凍実行ファイル 5.25.0.0	32bit 英語版 (Windows2000用)

2-2. アンインストール

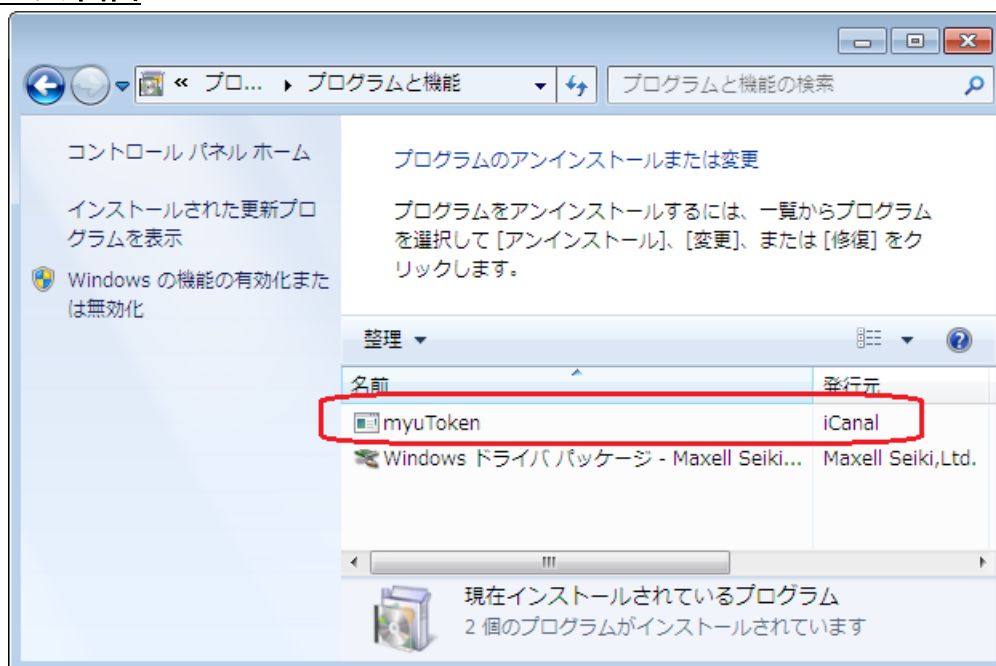
「コントロールパネル」からアンインストールを行います。

「myuToken」を選択して、「削除」ボタンをクリック。アンインストールには管理権限が必要です。

Windows 8.1 での画面



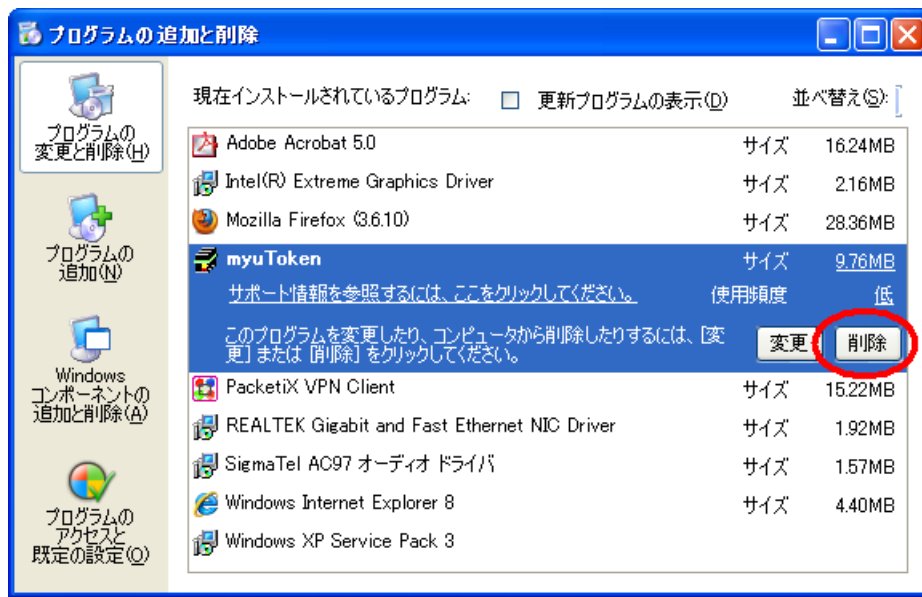
Windows 7 での画面



Windows Vista での画面



Windows XP での画面



3. フラッシュメモリカード、USB メモリの設定

IC カードエミュレータとして利用する場合のみ、カードリーダー設定が必要です。

3-1. USB カードリーダーを IC カードリーダーに設定

Windows 8.1(64bit)

次の方法で OS を再起動させます。

マウスカーソルを右上に移動させ、「設定」-「PC 設定の変更」-「保守と管理」-「回復」-「PC の起動をカスタマイズ」今



すぐ再起動する」-「トラブルシューティング」-「詳細オプション」-「スタートアップ設定」で再起動後、「ドライバー署名の強制を無効にする」を選択。

以降の操作は、Windows 8.1(32bit) / Windows 8(32bit) / 7 / Vista の手順と同じです。その後、OSを再起動させてください。

Windows 8(64bit)

次の方法で OS を再起動させます。

マウスカーソルを右上に移動させ、「設定」-「PC 設定の変更」-「全般」-「PC の起動をカスタマイズ 今すぐ再起動する」-「トラブルシューティング」-「詳細オプション」-「スタートアップ設定」で再起動後、「ドライバー署名の強制を無効にする」を選択。

以降の操作は、Windows 8.1(32bit) / Windows 8(32bit) / 7 / Vista の手順と同じです。その後、OSを再起動させてください。

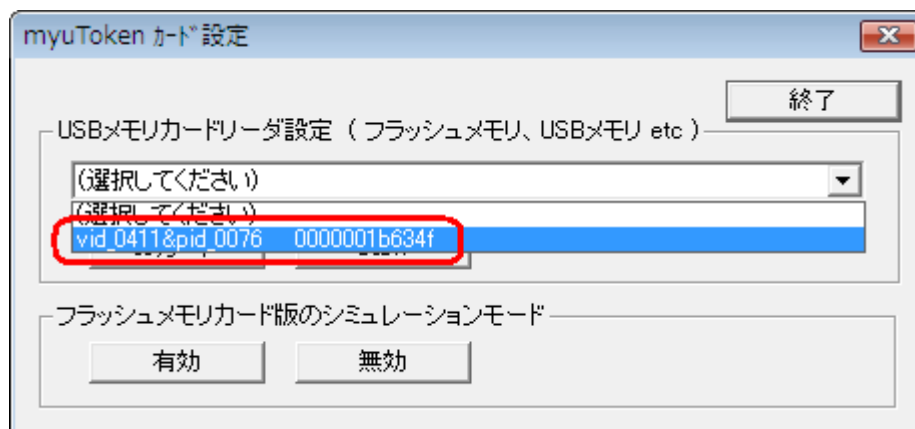
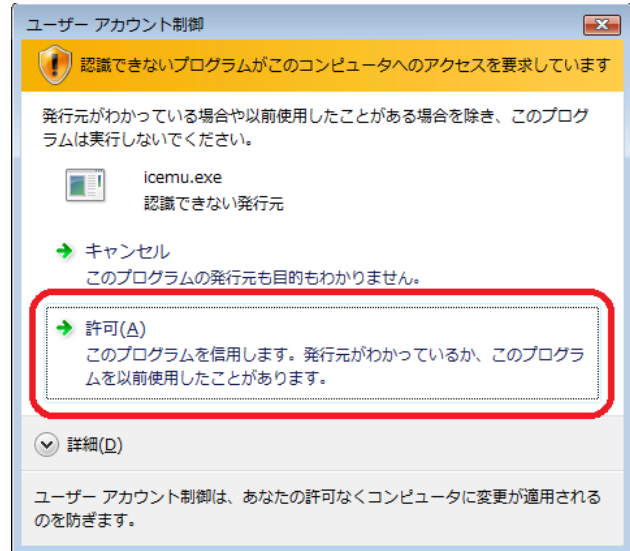
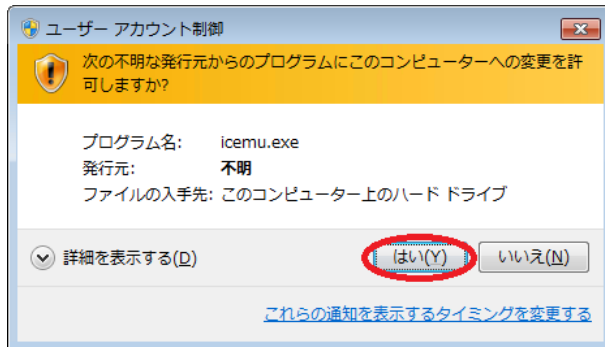
Windows 8.1(32bit) / 8(32bit) / 7 / Vista

設定は、USB リーダごとに必要です。なるべく他の USB 機器をはずし、対象の USB リーダだけを接続して「スタート」 - 「すべてのプログラム」 - 「iCanal」 - 「myuToken」を起動し[カードリーダー設定]ボタンをクリック [カードリーダー設定]ボタンをクリックします。

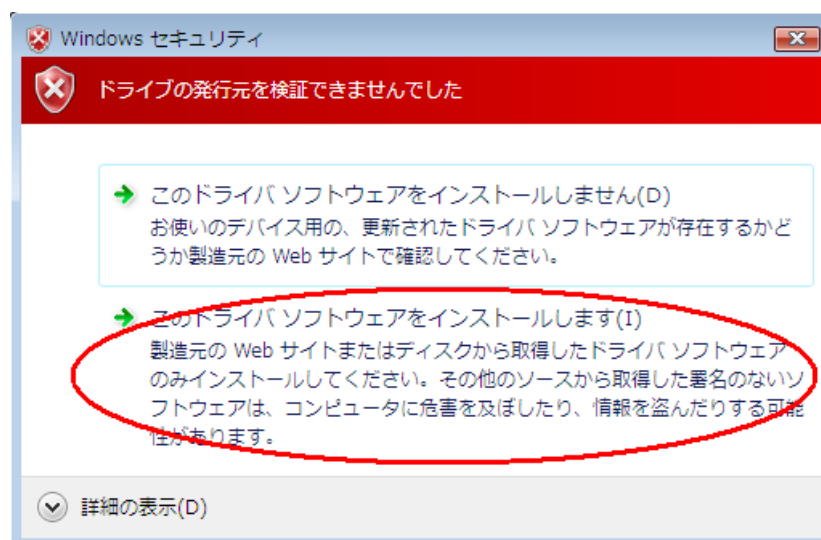


ユーザーアカウント制御の画面が表示される場合があるので「はい」をクリック

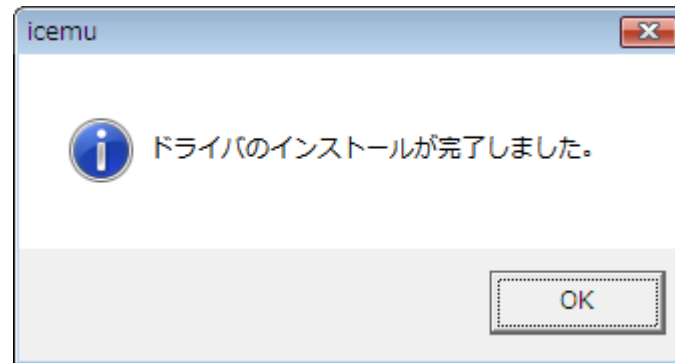
Windows Vista では「許可」を選択してください。



リストに、USB リーダのベンダ ID、プロダクト ID、シリアル番号の情報が1つだけ表示されるならおそらく対象の USB リーダであるので、選択して、「IC カード」ボタンをクリックしてください。検証できないというメッセージがでますが、かまわず「このドライバソフトウェアをインストールします」を選択。

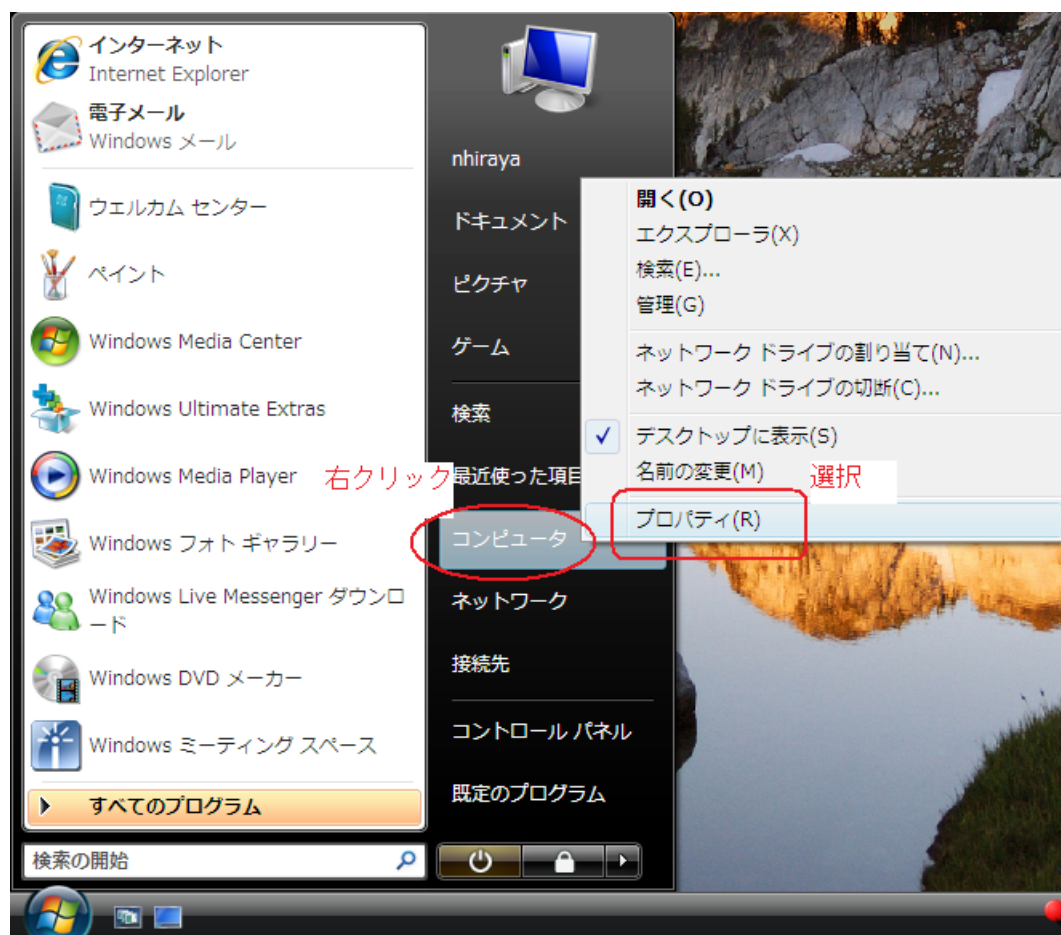


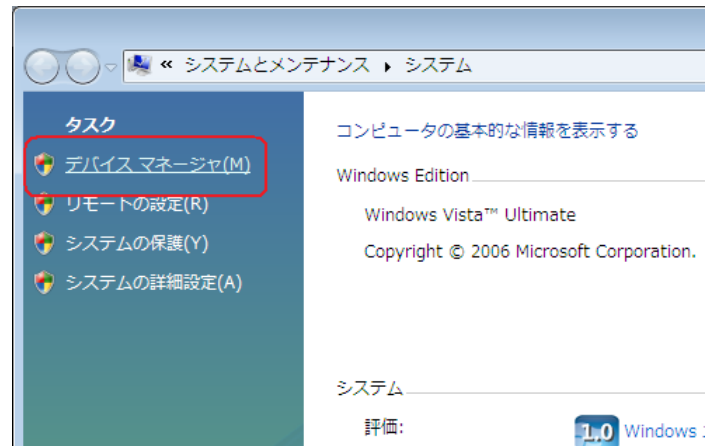
しばらくして次の画面が表示されれば OK です。



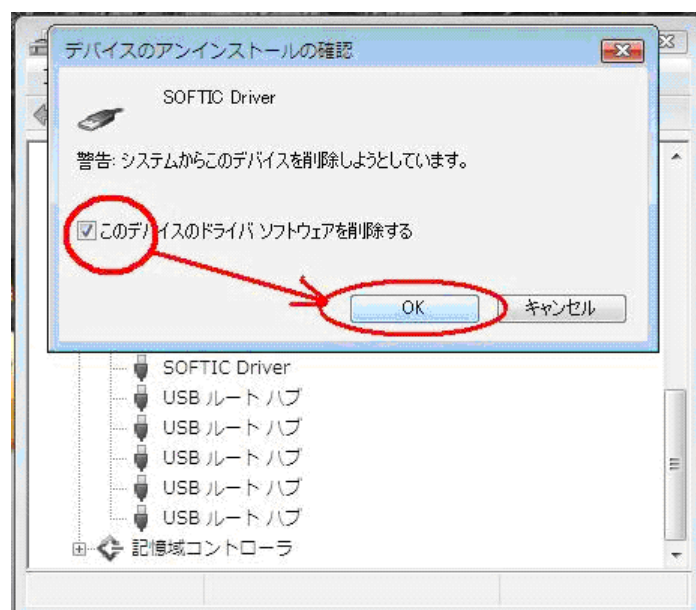
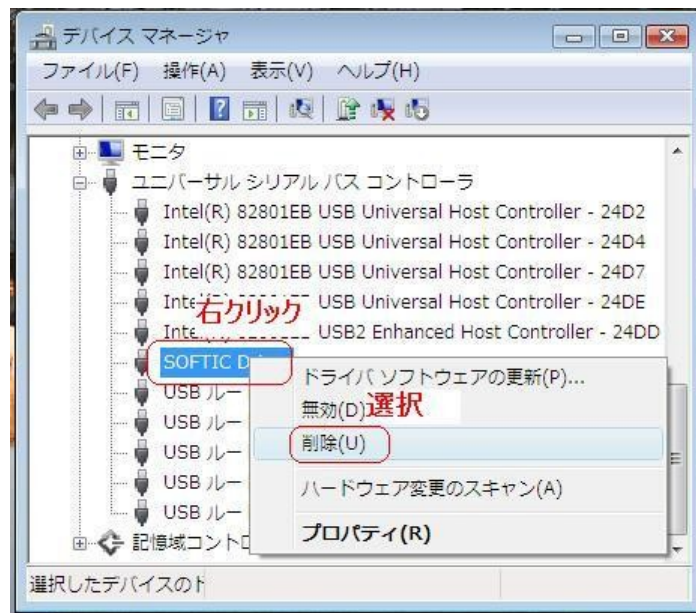
Windows 8.1 / 8 / 7 / Vista ディスクの設定に戻す方法

デバイスマネージャの起動



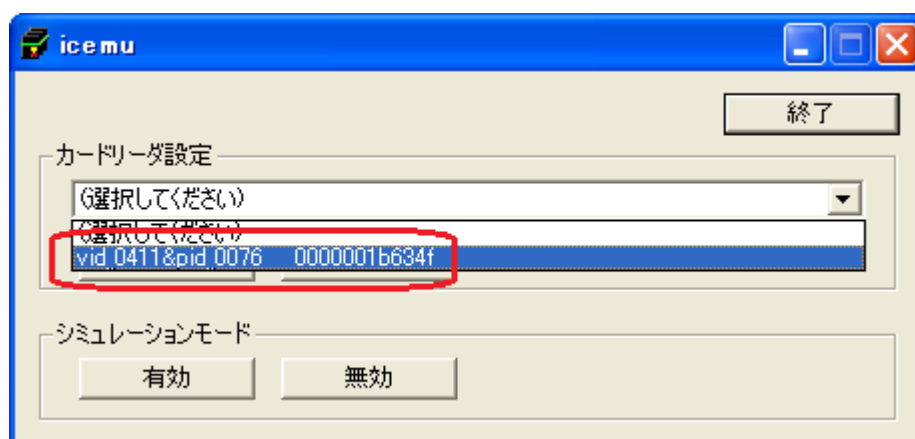


ユニバーサル シリアル バスコントローラにある「SOFTIC Driver」を削除してください。

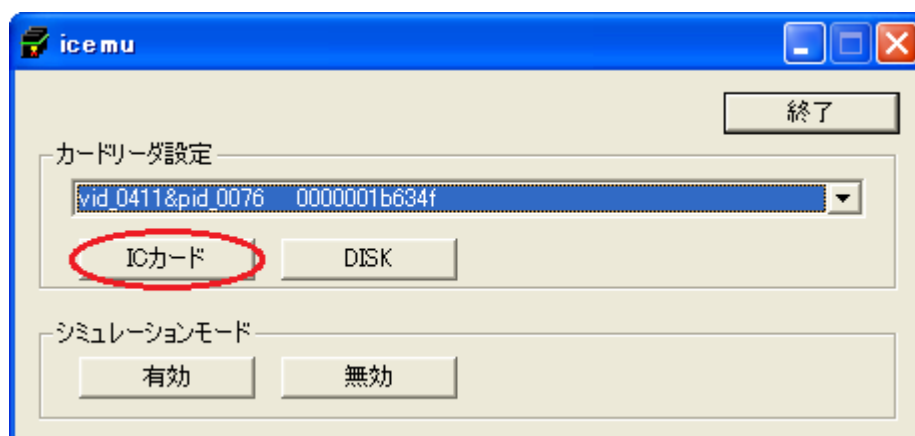


Windows XP / 2000

設定は、USB リーダごとに必要です。なるべく他の USB 機器をはずし、対象の USB リーダだけを接続して「スタート」 - 「すべてのプログラム」 - 「iCanal」 - 「myuToken」を起動し[カードリーダー設定]ボタンをクリック



リストに、USB リーダのベンダ ID、プロダクト ID、シリアル番号の情報が1つだけ表示されるならおそらく対象の USB リーダであるので、選択して、「IC カード」ボタンをクリックしてください。





成功したら、USB リーダは自動的に切り離されるので、いったん USB リーダを抜いて、再度、挿入してください。その時点から、IC カードリーダーとして動作します。

リストに、複数のリーダーが表示される場合は、対象のリーダーを抜いてリストを確認してください。対象のリーダーがリストからなくなっているはずなので、なくなったリーダーが対象の USB リーダですので、再度、対象の USB リーダを挿入し、[カードリーダー設定]で、対象のリーダーを選択して「IC カード」ボタンを押してください。

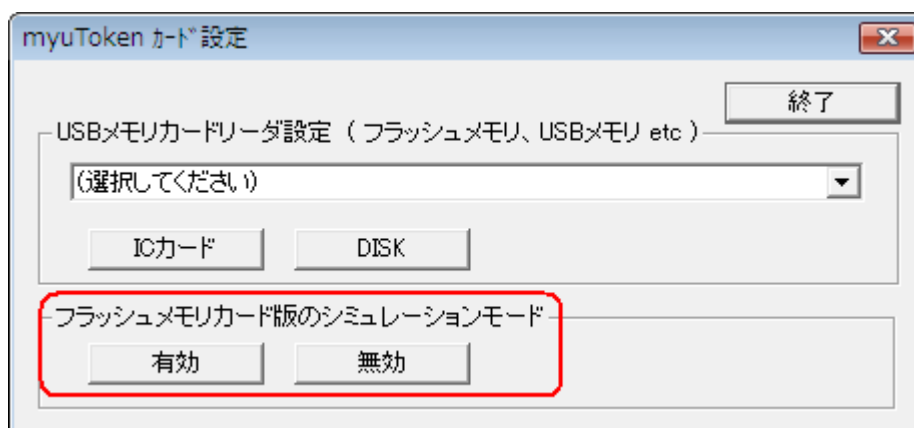
USB リーダをディスクに戻す場合は、USB リーダを選択して、「ディスク」ボタンを押します。

myuToken をアンインストールすると、IC カード設定したリーダーすべてディスクの設定に戻ります。

3-2. シミュレーションモード

フラッシュメモリカード、USB メモリ、SiMyuCard(IC カードシミュレータ)では、Microsoft Base Smart Card Crypto Provide(Base CSP)の管理者(admin)鍵をサポートしていません。つまり管理者(admin)鍵によるブロック解除はできません。しかしながらシミュレーションモードにすることにより Microsoft Base Smart Card Crypto Provider の管理者(admin)鍵の機能を有効にすることができ、限りなく本物の IC カードと同じ動作になります。ただしセキュリティは無いので IC カードのシミュレータとしてのみ利用できます。

「スタート」 - 「すべてのプログラム」 - 「iCanal」 - 「myuToken」を起動し[カードリーダー設定]ボタンをクリック、フラッシュメモリカード版のシミュレーションモードを選択し、[有効]ボタンをクリックして、myuToken を再起動してください。また元に戻すには、[無効]ボタンをクリックします。



3-3. USB リーダ最大同時接続数

フラッシュカードの USB リーダの最大接続数は、2 個までとなっています。それ以上、IC カード設定したリーダーを同時に接続しても認識されるのは 2 台までです。

3-4. マルチリーダーの動作

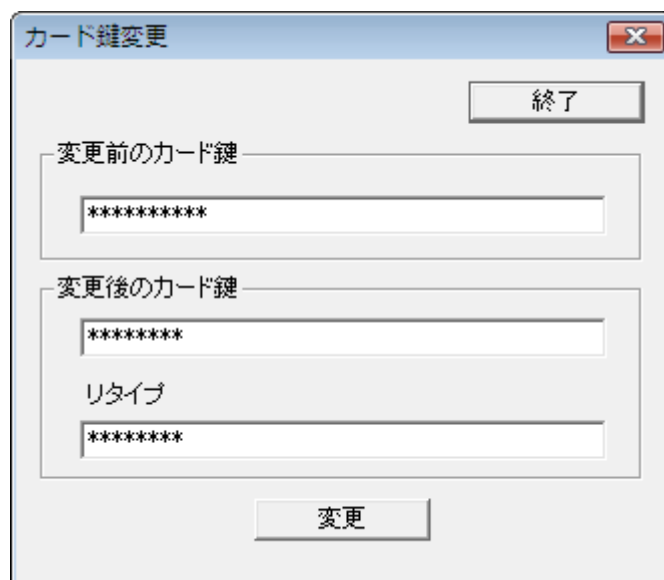
複数種類のフラッシュカードが読み書きできるマルチリーダーを IC カード設定しても、1 台のリーダーとして認識されます。どのフラッシュカードのスロットも有効ですが、同時に利用できるのは、1 スロットです。

3-5. Windows2000 における USB メモリ

Windows2000 では、USB メモリを引き抜くと「デバイスの取り外しの警告」が表示されますが、気にせず無視してください。

4. カード鍵変更

カード鍵変更が必要なのは IC カード myuCard 8K のみです。**IC カードを使用する前に、必ずカード鍵変更を行ってください。**変更後の値は、忘れないよう記録することをお薦めします。**忘れた場合、IC カードは使用不能になります。**カード鍵には英数字が利用できます。カード鍵の工場出荷値は **1111111111** です。デスクトップ上のショートカットか、「スタート」 - 「すべてのプログラム」 - 「iCanal」 - 「myuToken」で myuToken を起動。[カード鍵変更]ボタンをクリック



5. カードフォーマット

カードをフォーマットすると Microsoft Base Smart Card Crypto Provider の機能が利用できるようになります。フラッシュメモリカードや USB メモリでは一度、フォーマットをすると、アンフォーマットしても MBR は、復元されません。通常、それでも問題は起きませんが、MBR を使う携帯やデジカメでは問題が起きる可能性があります。そういった機器で利用するフラッシュメモリカードは使用しないか、機器で MBR まで初期化できることを確認してください。

デスクトップ上のショートカットか、「スタート」 - 「すべてのプログラム」 - 「iCanal」 - 「myuToken」で myuToken を起動。[カードフォーマット]ボタンをクリック



[フォーマット]ボタンをクリック



フォーマットが完了すると、Microsoft Base Smart Card Crypto Provider の管理者(admin)鍵が表示されます。Microsoft Base Smart Card Crypto Provider のユーザ(user) PIN を忘れてしまった場合の解除(ブロック解除)などに利用されるので、記録してください。



フォーマット後は、必ず[終了]ボタンをクリックしたあと、カードを一度、抜いてください。

6. IC カードにタイトルを設定

デスクトップ上のショートカットか、「スタート」 - 「すべてのプログラム」 - 「iCanal」 - 「myuToken」で myuToken を起動。[カードタイトル]ボタンをクリック



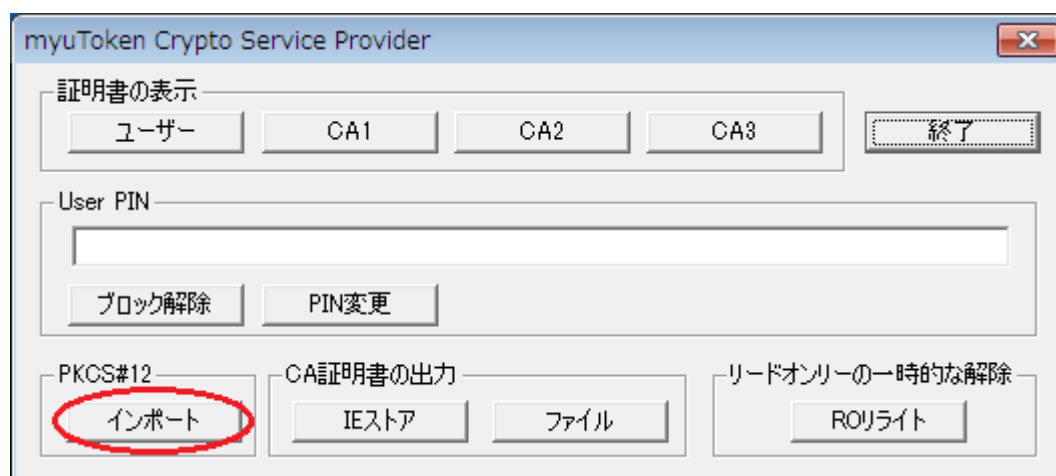
わかりやすくなるようなタイトルを書いて、[適用]ボタンをクリック



7. CSP

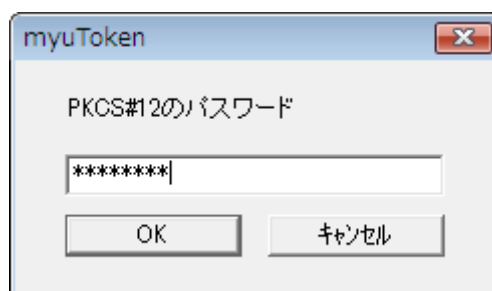
7-1. PKCS#12 ファイルのインポート

デスクトップ上のショートカットか、「スタート」 - 「すべてのプログラム」 - 「iCanal」 - 「myuToken」で myuToken を起動。[CSP]ボタンをクリック



[インポート]ボタンをクリック、PKCS#12 のファイルを選択します。

PKCS#12 のパスワードを入力

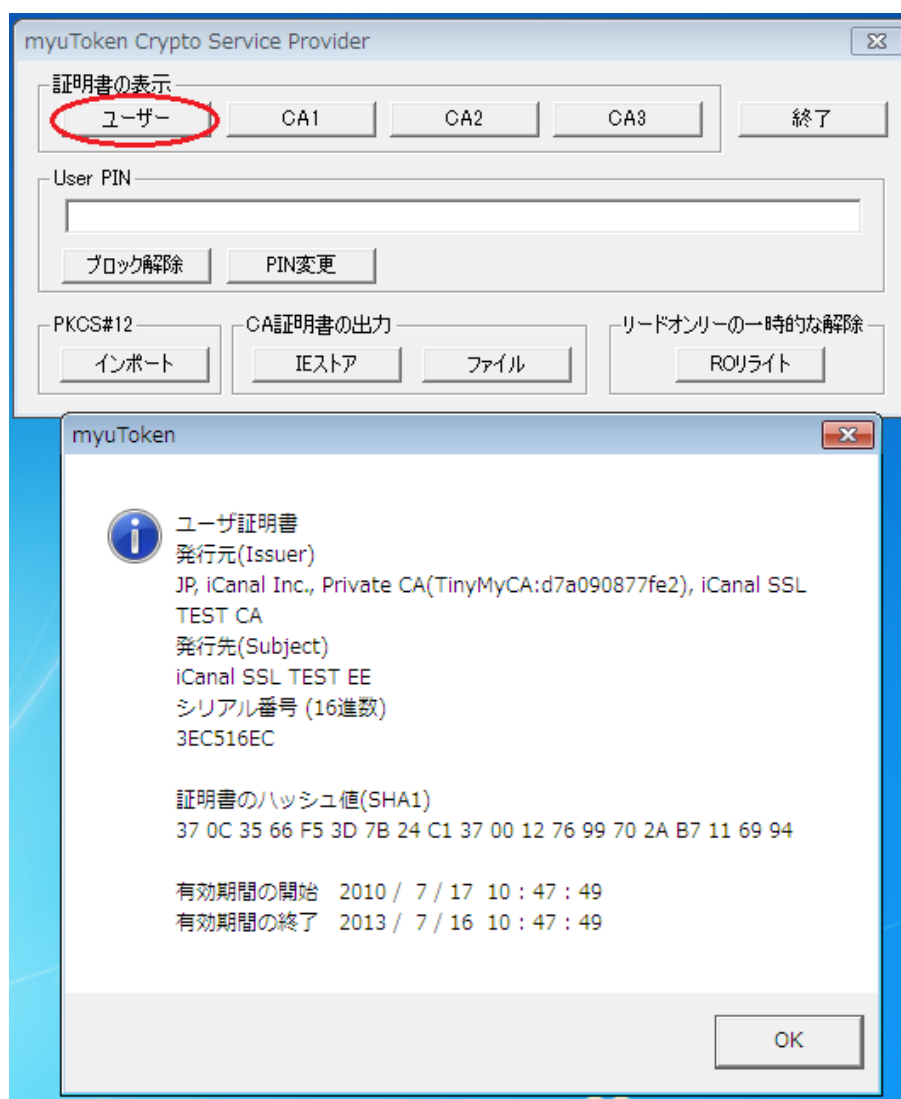


Microsoft Base Smart Card Crypto Provider(Base CSP)のユーザ(user)PINを入力、カードフォーマット後に、PIN 変更していなければ「 iCanal 」



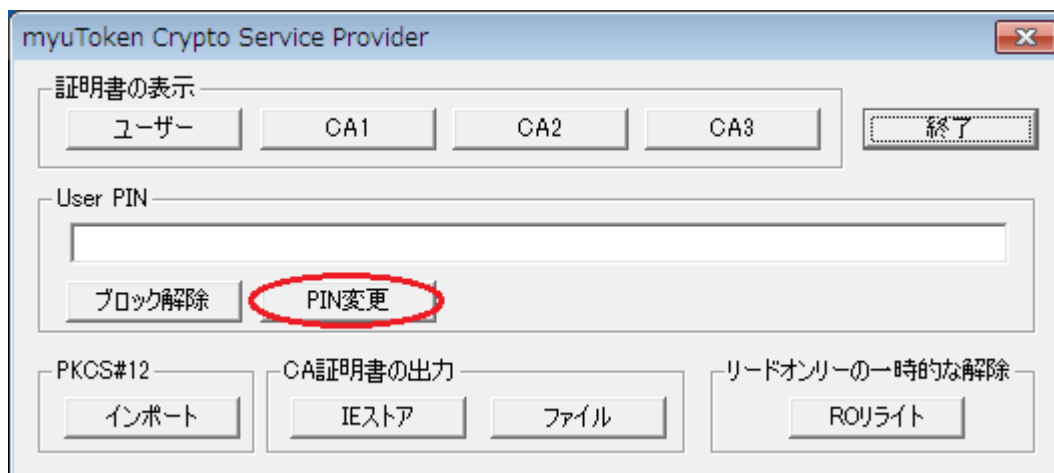
7-2. 証明書の表示

“証明書の表示”欄にある[ユーザー]ボタンをクリックします。CA の証明書についても[CA1]、[CA2]、[CA3]ボタンをクリックすることで表示できますが、PKCS#12 でインポートした場合のみ。



7-3. PIN 変更

[PIN 変更]ボタンをクリック、現在のパスワード、新しいパスワードを入力するとパスワードの変更が行えます。

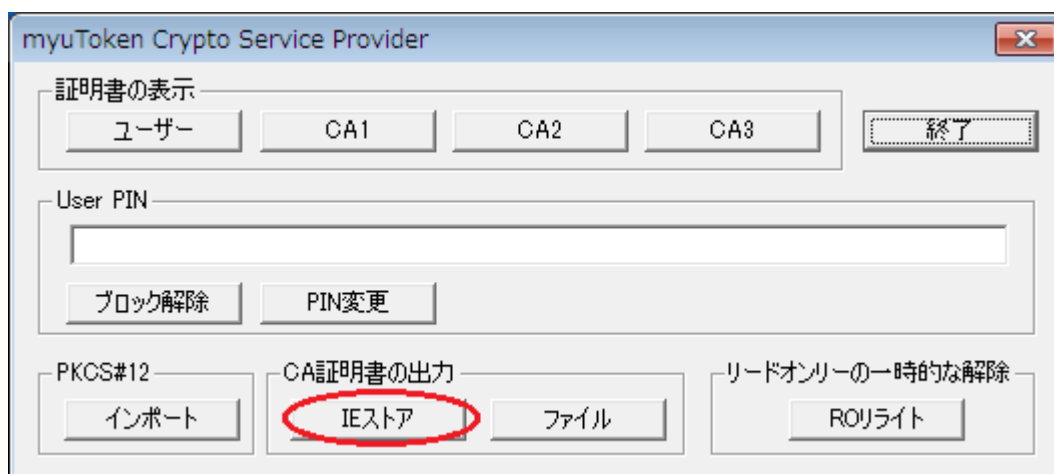


7-4. CA証明書のIEストアへの転送

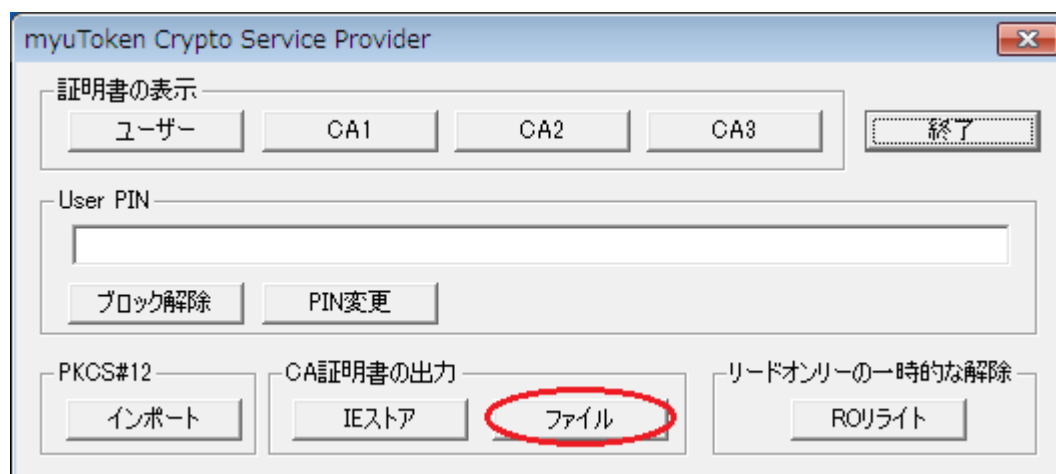
アプリケーションによっては、CA の証明書がIEの ROOT ストアにある必要があるものがあります。

CA 証明書の出力 [IE ストア]ボタンをクリックすると、CA 証明書が転送されます。CA の証明書は1回だけで良く、毎回転送を行う必要はありません。

むやみに CA 証明書を ROOT ストアに転送することは、セキュリティの低下を招くので、必要な CA の証明書だけ ROOT ストアへ転送するようにしましょう。



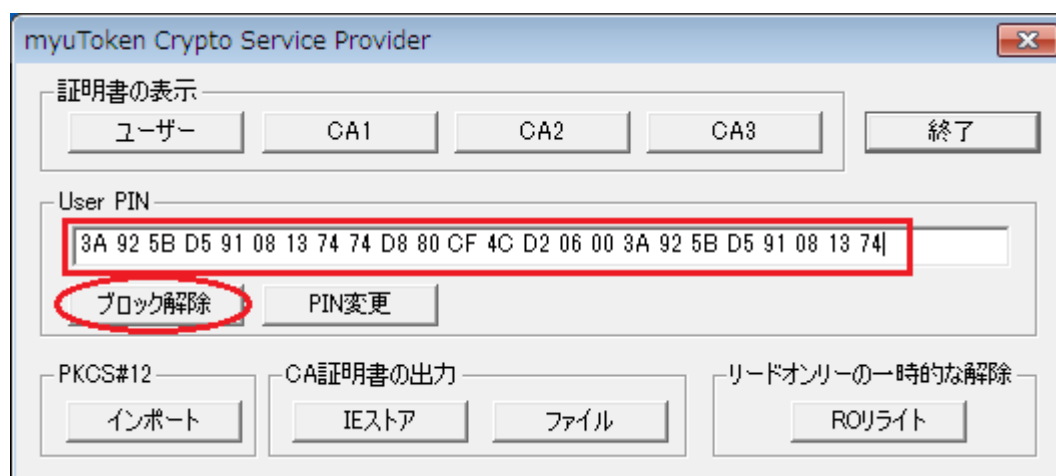
7-5. CA証明書のファイルへの出力



[ファイル]ボタンをクリックします。CA 証明書がファイルで出力します。

7-6. ブロック状態のカードの解除

カードのフォーマットのときに表示された Microsoft Base Smart Card Crypto Provider の管理者(admin)鍵を入力し、[ブロック解除]ボタンをクリックします。

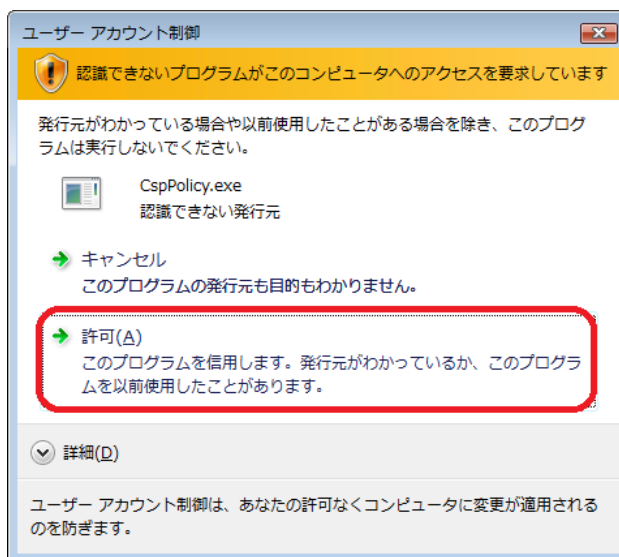
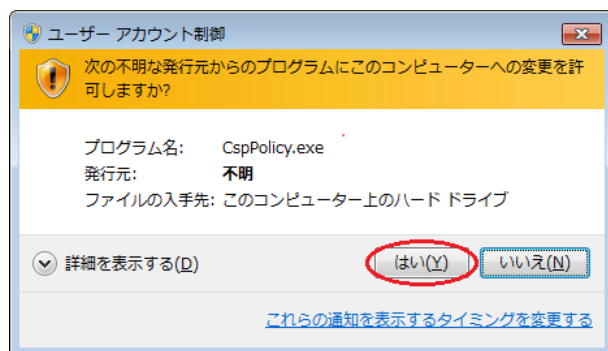


8. ポリシー設定

外部アプリケーションによって IC カードに電子証明書をインポートする場合、CryptImportKey0を使う場合があります。デフォルトの設定では CryptImportKey0は使用不可です。次の手順で CryptImportKey0を利用できるようにします。デスクトップ上のショートカットか、「スタート」 - 「すべてのプログラム」 - 「iCanal」 - 「myuToken」で myuToken を起動。[ポリシー設定]ボタンをクリック



ユーザーアカウント制御の画面が表示される場合があるので Windows7 では「はい」をクリック
Windows Vista では「許可」を選択してください。



「可」を選択して、[設定]ボタンをクリックしてください。



9. IE ストア一括削除

[IE ストア一括削除]ボタンをクリックすると IE の個人ストアにある Microsoft Base Smart Card Crypto Provider の証明書を削除します。削除されても IC カードを挿入すれば IC カードから証明書が転送されます。

(注) Microsoft Base Smart Card Crypto Provider の証明書に対応する他の IC カードの証明書も消去します。



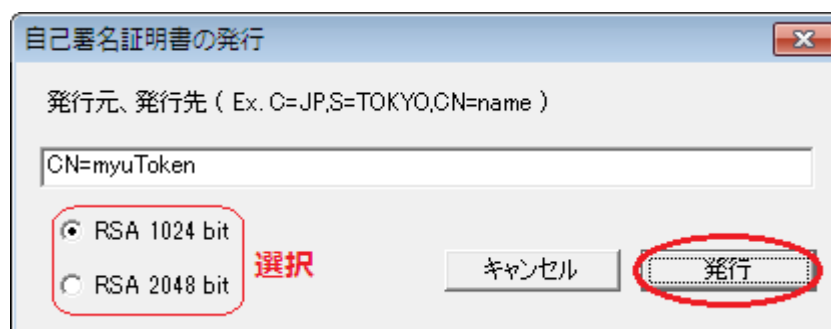
10. 自己署名証明書発行(PKCS#12 ファイル)

PKCS#12 形式の自己署名証明書を発行します。

「スタート」 - 「すべてのプログラム」 - 「iCanal」 - 「myuToken」を起動、[PKCS#12]ボタンをクリック



自己署名証明書の発行元(発行先)を入力して、[発行]ボタンをクリック



出力する PKCS#12 のファイル名を選択し、PKCS#12 のパスワードを入力

11. リードオンリーの IC カード

Microsoft Base Smart Card Crypto Provider や PKCS#11 のユーザ(user)PIN の認証が成功すると、IC カード内にある電子証明書や秘密鍵の書き換えが可能です。認証目的の用途であれば、悪意あるウィルスに書き換えられたとしても、それほど大きな問題にはなりません。暗号化や電子署名では問題になるケースがあります。このためユーザ(user)PIN の認証が成功しても IC カードのデータの書き換えができないようなリードオンリーの IC カードが作れるような独自機能を用意しました。myuCardなどの IC カードではハードウェア的にリードオンリーにしているため安全です。ただし強制的に書き込みができないようにしているためデータの書き込みが必要なアプリケーションは動作しない可能性があります。USB メモリやフラッシュメモリカードや SiMyuCard(IC カードシミュレータ)では、ハードウェア的に書き込みができなくなることはありませんが、IC カード(myuCard)と動作が同じになるようにソフトウェア的に書き込みができないようにしています。一度、リードオンリーのカードにしてもフォーマットによって元に戻るため気軽にリードオンリーの IC カードを作ることができます。

11-1. リードオンリーのカードの作り方

フォーマットするときに[フォーマット]の代わりに[RO フォーマット]ボタンでフォーマットします。

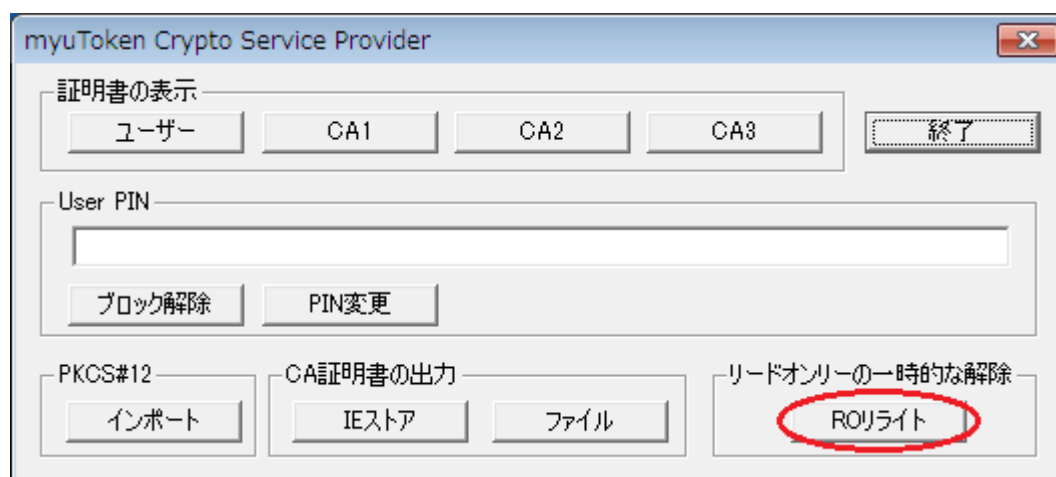


[RO フォーマット]では IC カード(myuCard)を引き抜いた瞬間にリードオンリー化します。

USB メモリやフラッシュメモリカード、SiMyuCard(IC カードシミュレータ)では、カードを引き抜いてもリードオンリー化されません。[カードタイトル]によってタイトルを設定するとリードオンリー化されます。

11-2. RO リライト

RO フォーマットでは、IC カードを引き抜くと Read Only カードになってしまうため電子証明書をインポートすることができない状態です。そこで RO リライトを使って Read Only カードを再度、書き込みができる状態にします。RO リライト後、IC カードを引き抜くと、再び Read Only カードになります。USB メモリやフラッシュメモリカード、SiMyuCard(IC カードシミュレータ)では、IC カードを引き抜いても Read Only にはならないので、RO リライトは不要です。



カードタイトルも[RO リライト]で再書き込みできるようになります。



12. PKCS#11 icardmodpk.dll

PKCS#11 のアプリケーションを利用するためには、C:\Windows\System32 にある icardmodpk.dll のファイルを PKCS#11 のファイルとしてアプリケーションに登録します。icardmodpk.dll は、Microsoft Base Smart Card Crypto Provider とエリアを共用しています。しかしながら PacketiX VPN では PKCS#11 から証明書をインポートすることは可能です。ただし Certificate オブジェクトや PrivateKey オブジェクトは、1 個ずつしか格納できません。CA などの証明書はデータとして格納すれば、格納できます。

推定動作可能アプリケーション

アプリケーション名	バージョン
FireFox	3.6 以降
ThunderBird	3.1 以降
PacketiX VPN	3.0
TrueCrypt	7.0a

動作しないアプリケーション

アプリケーション名	バージョン
DriveCrypt	全バージョン

64bit OS で、32bit の PKCS#11 アプリケーションを動作させるためには、64bit 版の icardmodpk.dll ではなく 32bit OS 版の icardmodpk.dll を指定する必要があります。32bit 版の icardmodpk.dll は、通常 C:\Windows\SysWOW64 にあります。

13. デーモン再起動

リモートデスクトップ接続する場合は、接続後、デーモンの再起動が必要な場合があります。

IC カードを挿入しているにもかかわらず証明書が見つからない場合、「デーモン再起動」をクリックしてください。

PKCS#11 や CSP を直接アクセスするアプリケーションでは、デーモンの再起動は不要です。



14. iCanal CSP 優先

Windows XP のみ「iCanal CSP 優先」をチェックすることが可能です。チェックをすると Base CSP よりも iCanal CSP を優先します。Windows Vista/7 では Base CSP でも SHA-256 などの新しいハッシュによる署名が可能です。Windows XP の Base CSP では SHA-256 などの新しいハッシュをサポートしません。そこで iCanal CSP を優先させることで SHA-256 などの新しいハッシュにも対応させる機能です。ただし iCanal CSP は、Base CSP と完全互換ではないためアプリケーションによってはうまくいかない場合もあります。



付録 A S/MIME の設定

S/MIME では、CA の証明書が IE の ROOT ストアにインポートされている必要があるので、
「7-4. CA証明書のIEストアへの転送」で説明される方法で CA 証明書を IE ストアに転送します。大抵の S/MIME 証明書では、あらかじめ ROOT ストアに入っていることが多いので、その場合にはこの操作は不要です。

ThunderBird では証明書ストアを独自に持っているため CA 証明書を IE の ROOT ストアにインポートしても認識されません。独自証明書ストアに CA 証明書が入っていない場合、「7-5. CA証明書のファイルへの出力」をつかって手動で CA 証明書をインポートしてください。