MXLOGON2 説明書

USB キーを利用した Windows ログイン

https://ribig.co.jp/mxlogon2
2018 年 12 月 1 日
有限会社リビッグ
横浜市港南区上大岡西 1-12-2

内容

1. MxLogon2 について

Windows へログインを Matrix USB キー認証とユーザ名/パスワード認証の 2 重認証によっセキュアにする認証プログラムです。

1 段階目は USB キー認証を行います。USB キー認証には PIN 入力が必要です。成功すると、2 段階目のユーザ名/パスワード認証の画面に切り替わります。USB キー認証を通らなければ、2 段階目に進むことができません。

2 段階目は Windows 標準のユーザ/パスワード認証画面でユーザ名とパスワードを入力します。2 段階が成功すると Windows にログインします。

オプション設定により、１段階目の PIN の入力を求めないようにしたり、2 段階目のユーザ・パスワード認証を既定の手入力の代わりに、自動入力させたりすることができます。

2. USB キー

MxLogon2 をインストールする前に USB キーをコンピュータに接続してください。接続すると Windows によって USB キーが認識されドライバが自動的にインストールされます。ドライバは Windows 付属のものが使われます。キーを接続する以外の操作は不要です。

3. リモートデスクトップ

Windows 付属のリモートデスクトップクライアントで MxLogon2 がインストールされたリモートコンピュータに接続すると、クライアント側に接続した USB キーでログインできます。リモート接続で USB キーログインを予定されているのであれば、MxLogon2 インストール前に、クライアントからリモートコンピュータにログインできることを確認しておいてください。

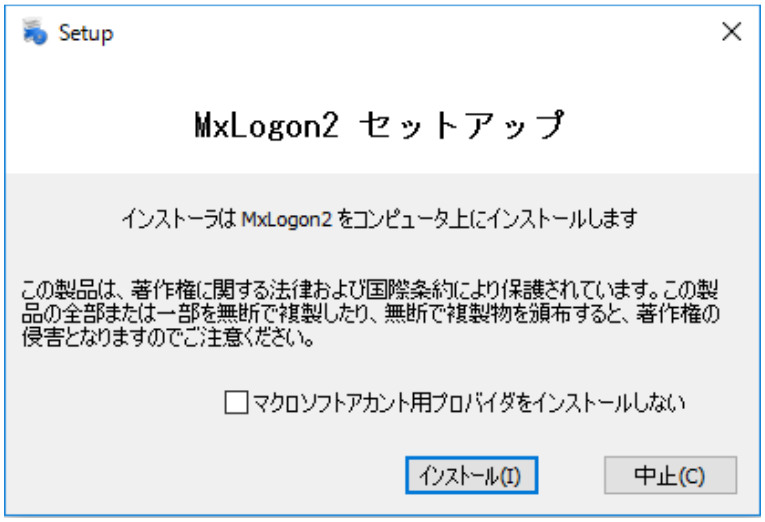
Windows Vista/7 の 64 ビット版のクライアントはローカル接続 USB キーでリモートコンピュータにログインすることはできません。

CredSSP 脆弱性の修正パッチが必要かもしれません

Windows のリモート接続の認証は既定ではネットワークレベル認証(NLA)です。しかし、USB キーログオンのためクラシック認証に切り替える必要があるかもしれません。付録１に“リモートデスクトップの２つの認証”をご覧ください。

4. MxLogon2 のインストール

配布パッケージ内の auto-setup.exe を実行してください。



“ネットワークレベル認証（NLA）用インストール”にはチェックしないでください。

MxLogon2 セットアップが起動したら [インストール]ボタンのクリックでインストールが開始します。通常、数秒で完了します。

インストールが完了したら、サインアウト/ログアウトしてください。

5. サインイン・ログイン・ロック

インストール後、ログアウト/サインアウトしたらログイン画面には MxLogon2 が含まれているはずです。Windows 8/10 ではサインインオプションで MxLogon2 を選択できます。Windows Vista/7 では MxLogon2 のアイコンが表示されます。

MxLogon2 を選択後、正当なキーが接続されていれば PIN 入力フィールドが表示されます。

既定では PIN フィールドの上に Slot1~Slot4 を選択するコンボボックスが表示されます。ＵＳＢキーは４つの異なる認証領域をもっています。このコンボボックスで、どの認証領域を利用するのかを選択してください。

すべての認証領域の既定ＰＩＮは 12345678 です。

複数の USB キーを接続している場合は、Slot 選択コンボボックスの上に USB キー選択コンボが表示されます。ログインに利用する USB キーを選択してください。既定では USB キーのシリアル番号が表示されますが、USB キー名は任意の文字列に設定可能です。

PIN を入力後、リターンするとパスワードを入力できます。正しいパスワードを入力後、リターンでサインインします。

5.1 USB キーの PIN ロック

既定では PIN を 7 回連続で間違えると USB キーはロックします。ロックする迄の誤入力回数の設定、ロック解除は USB キー設定ツールで行えます。

5.2 ロック

サインイン・ログイン中に USB キーを抜き取ると Windows は ロックします。

ロックはログインと同じように USB キーで解除できます。

6. USB キー設定

各ユーザ向けの MxLogon2 は他ユーザの USB キー認識することはありません。ユーザ専用の MxLogon2 と専用設定がされた USB キーが提供されます。しかし、すべてのユーザの USB キーの既定 PIN は同じ既定値が設定されます。セキュアな運用を行うには、初期設定 PIN を別の PIN に変更しなければなりません。

ＵＳＢキーの設定を行うには、配布メディアの「設定ツール」フォルダに USB キー設定ツール Cert.exe を利用します。

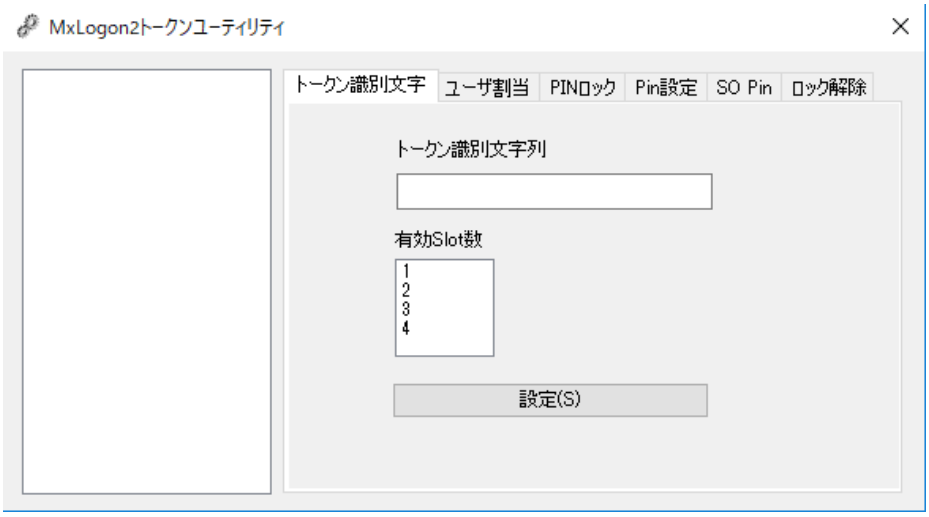
6.1 識別文字列(オプション)

USB キーを識別するために分かりやすい名前を設定します。設定した識別文字列で USB キーを見分けることができるようになります。左リストボックスで識別文字列を設定する USB キーを選択後、任意の文字列を設定してから[設定]ボタンをクリックしてください

設定しなければ USB キーのシリアル番号が識別文字列になります。

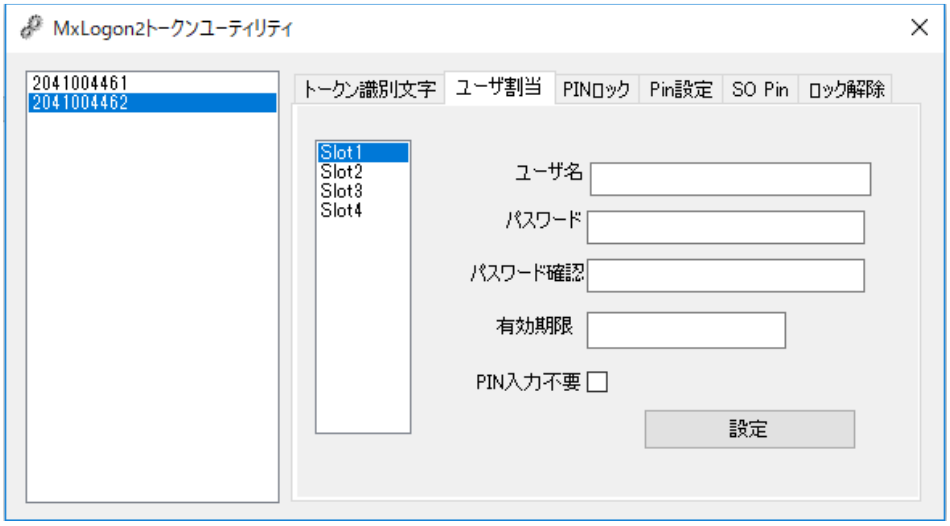
6.2 有効ＳＩｏｔ数

既定では 4 つの認証領域が有効になっています。有効にする Slot 数を選択してください。 1 つだけを有効にすると、ログイン画面では slot を選択するコンボボックスは表示されません。



6.3 ユーザ割当

既定では USB キー認証成功後、２段階目のユーザ名・パスワード入力の画面が表示されます。そこでユーザ、パスワードを手入力してログインします。ＵＳＢキーの認証領域にユーザ資格情報を割り当てると、設定した資格情報でユーザ名、パスワード認証が自動化されます。１段階目の PIN 入力を省く設定も領域毎に設定できます。



Slot 毎にユーザ名、パスワード、有効期限、PIN 入力不要チェックを設定して[設定]ボタンで保存します。

ユーザ名：

既定ではプレーンテキストで USB キーをつかってログインするユーザ名を指定します。オプション設定でログインするユーザ名を表す正規表現を設定できます（これまで既定設定は正規表現でした）

プレーンテキストでユーザ名を指定するには、ドメイン¥ユーザ名形式や UPN 形式で指定してください。ローカルドメインは “.”(ドット)で指定可能です。指定したユーザ以外ではログインできなくなります。

パスワード：

指定ユーザのパスワードを正確に入力してください。入力しなくてもかまいません。ユーザ名を指定して、パスワードを省略すると、ログイン画面のユーザ名フィールドに指定ユーザ名が

自動入力されます。ユーザ名/パスワードどちらとも指定すると自動ログインします。パスワードだけ指定することはできません。

有効期限：

yyyy/mm/dd の形式で認証領域の有効期限を設定してください。何も入力しなければ有効期限は設定されません。

ＰＩＮ入力不要：

チェックすると１段階目の ＵＳＢキー認証が自動化されます。

6.3.1 割当ユーザ削除

割当ユーザを削除するにはユーザ名を空にして[設定]ボタンをクリックしてください。

6.3.2 PIN 入力不要、ユーザ名、パスワードの同時設定

スロットのユーザ割当てで、ユーザ名/パスワードをどちらも設定、また、PIN 入力不要を有効にすると、スロット選択と同時に自動ログオンするようになります。

既定スロットは Slot1 です。USB キーを選択すると自動で Slot1 が読み込まれます。そのため Slot1 が自動ログオン設定になっていると、Slot 選択画面が表示されることなく、自動ログオンします。他の Slot は利用できません。Slot1 以外を自動ログオン設定にすると Slot 選択画面は表示されます。

複数の USB キーを接続した場合、どの USB キーが最初に選択されるか事前には分かりません。仮に USB キーの Slot1 が自動ログオンになっていたとしても、別の USB キーが選択されて、そのキーの Slot1 が自動ログオンになっていなければ USB キー/スロットを選択画面は表示されます。

6.3.3 自動パスワード管理

USB キーのスロットにユーザ名とパスワードを設定して、そのスロットで Windows にログインすると、パスワード変更は自動化されます。ログイン中に CTRL+ALT+DEL で表示されるメ

ニューで “パスワード変更” すると、自動生成された新しいパスワードに自動的に変更されます。MxLogon2 が自動生成するパスワードが設定されますので、どのようなパスワードが設定されたのかは知る方法はありません。

パスワード期限切れなどでログイン前にパスワード変更を求められる場合も、ユーザ名とパスワードを設定したスロットではパスワードは自動更新されます。

自動パスワード更新は、パスワード変更処理前に SHIFT+CTRL キーを同時に押し続けることで無効化できます。PIN 入力後、SHIFT+CTRL キーを同時に押し続けてリターンすることで新しいパスワードを手動設定できます。

6.3.4 正規表現を使ったユーザ名の指定

ユーザ名フィールドにはオプション設定で正規表現を設定することができるようになりますます（ “7.1.6 ユーザフィールドは正規表現“ 参照）。 この場合、ユーザ名フィールドには以下 2 つのどちらかを指定します。

1．2 段目で認証可能なユーザ名を表す正規表現を設定

2．2 段目で認証可能なプレーンテキストのユーザ名を設定

■正規表現の設定

スロットを使ったログインは正規表現に一致するユーザのみ許可されます。

“.” （ドット）は正規表現では特殊文字ですので、ローカルドメインにを表すことはできません。代わりに“LDMN” を指定してください。

例： (LDMN|mydomain|mydomain1)¥¥.*

ログイン可能なユーザのドメインを 3 つに限定

正規表現パターンマッチングのテストツール regex_test.exe が「設定ツール」フォルダに収められています。MxLogon2 とまったく同じ処理をしますので、事前にパターンにユーザ名がマッチするか確認できます。

■プレーンテキストのユーザ名設定

プレーンテキストでユーザ名を指定するには、先頭文字を “ (ダブルクオート)にします。2 文字目以降を MxLogon2 はユーザ名として解釈します。ユーザフィールドがプレーンテキストと解釈された場合、先頭の “ を除く 2 文字目以降のテキストがログイン画面のユーザフィールドに自動的に入力されます。

例：

“.¥user1　とユーザフィールドに設定

.¥user1 が自動的にログイン画面のユーザフィールドに入力されます。

ログイン画面でユーザ名を変更してログインしようとしてもエラーになります。指定ユーザ以外ではログインできません。

6.3.5 “他のユーザ“　設定

setup プログラムは、ログイン画面にユーザ名が表示されないような設定にします。以下レジストリをそれぞれ 1, 3 をセットすることで、“他のユーザ”が表示されるようにします。ログイン画面にユーザ名は表示されないため、ユーザ名は手入力しなければなりません。

[HKEY_LOCAL_MACHINE¥software¥microsoft¥windows¥currentversion¥policies¥system]

"dontdisplaylastusername"=dword:00000001

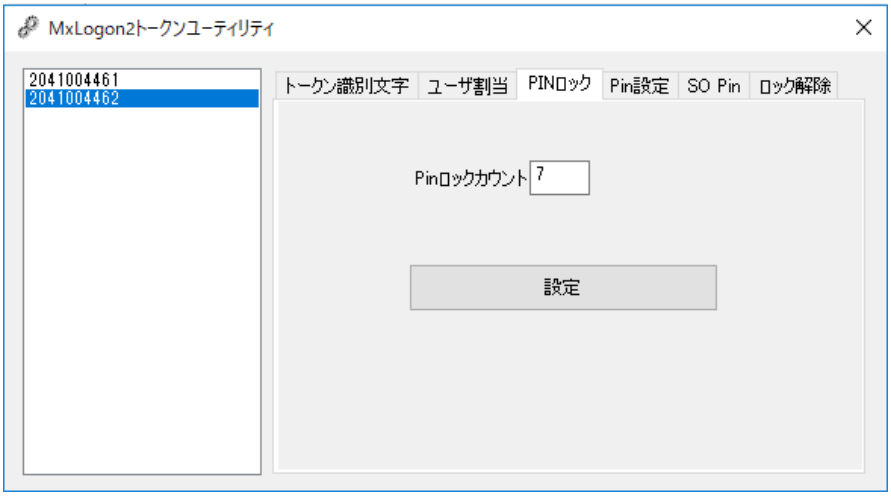
"DontDisplayLockedUserId"=dword:00000003

コンピュータに登録されているユーザがログイン画面に表示されないため、よりセキュアな設定になります。使い勝手を優先してユーザ名をログイン画面に表示させたければ、この 2 つのレジストリ値を 0 に変更してください。

6.4 PIN ロックカウント

PIN がロックするまで許される PIN 誤入力連続回数を指定します。既定は 7 回です。0 を指定すると制限なくＰＩＮ入力が可能になります。

ロックカウントは特定の認証領域の PIN 誤入力ではなく、すべての領域のＰＩＮの誤入力が指定回数連続にカウントされます。例えば、Slot1 で 3 回、Slot2 に変更して 3 回、Slot3 に変更して 1 回、連続して 7 回誤入力、次にどの認証領域で PIN の誤入力をしてもロックします。



PIN は認証領域の秘密データ（ユーザ資格情報）にアクセスするために必要です。PIN が分からなければ認証領域の秘密データにアクセスすることはできません。ロックした時点でデータ保護のため MxLogon2 は秘密データを削除します。このためロックは解除できますが、認証領域のデータは復元できません。ロック解除は PIN と認証領域の初期化を行うのみです。

6.5 ユーザ PIN と SO PIN の設定

USB キー識別文字列、ユーザ割り当て、ＰＩＮロックカウントの設定では USB キーの PIN を気にすることなく設定ができました。これは cert.exe の 3 つのタブ（USB キー識別文字列、ユーザ割当、PIN ロック）では既定ユーザ PIN（12345678）と既定 SO PIN(admin123)が USB キーにセットされていることを前提としているためです。

これらのタブで USB キーを設定には USB キーの PIN/SO PIN の初期値に戻す必要があります。また、USB キー識別文字列、ユーザ割当、PIN ロックの設定完了後、運用前までにユーザ PIN と SO（管理者）PIN は必ず変更してください。

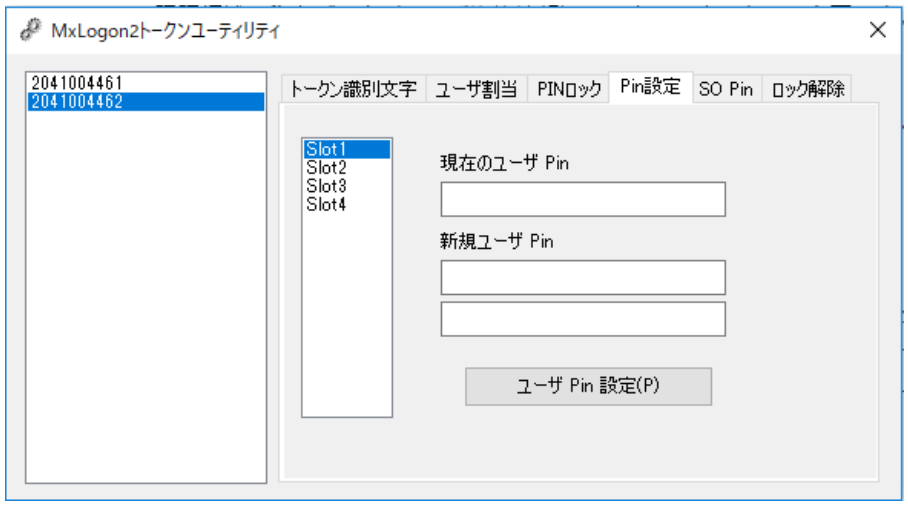
すべてのユーザ向けの MxLogon2 の PIN, SO Pin は以下の初期値にセットされます。

既定 SO （管理）PIN　　：　“admin123”

既定 ユーザ PIN　　：　“12345678”

6.5.1 ユーザ PIN 変更

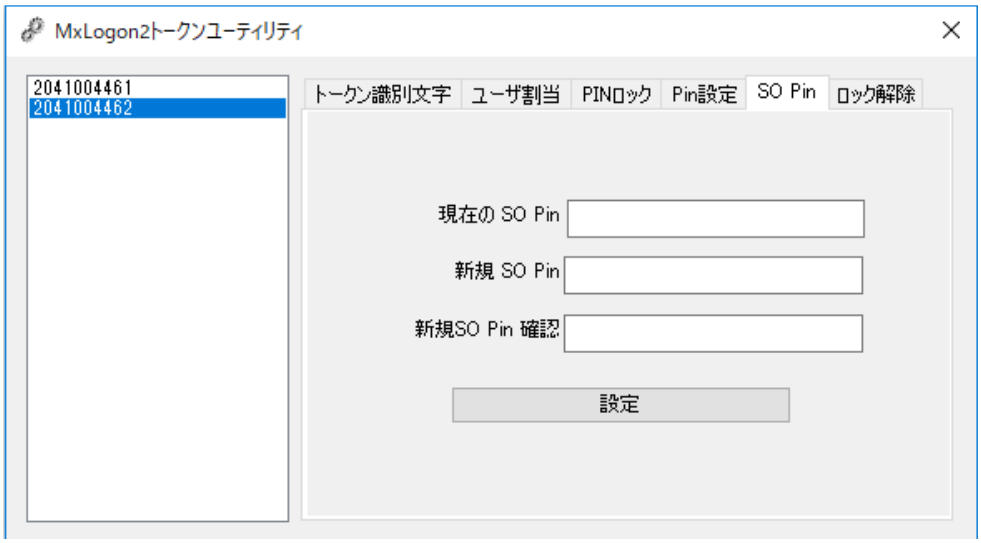
USB キーの各認証領域ごとに PIN を設定してください。



ユーザ PIN は MxLogon2 のログイン画面で変更可能です。正しいＰＩＮ入力後、”PIN 変更“をクリックすると PIN 変更ウィンドウが表示します。

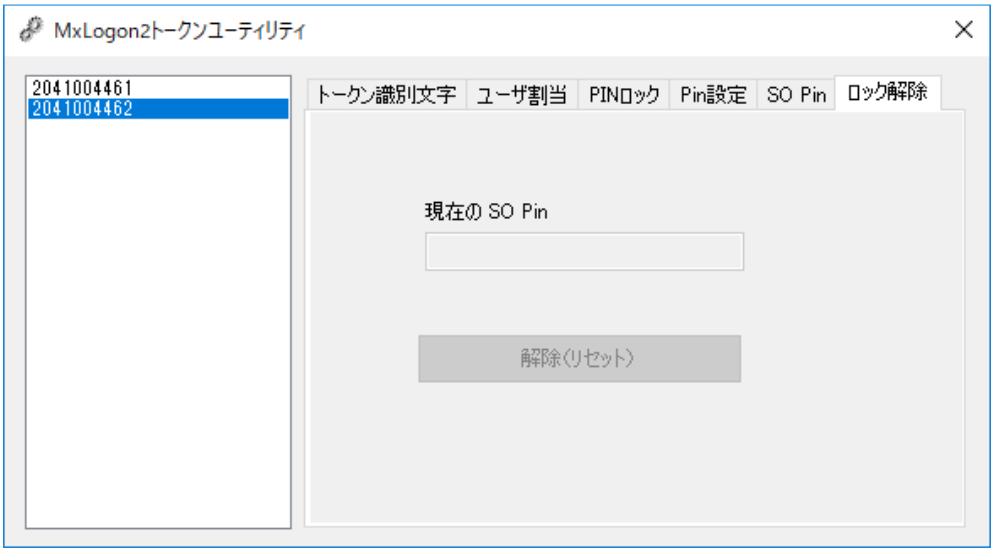
6.5.2　SO PIN の変更

SO Pin は（認証領域ではなく）キーに対する設定です。ロック解除（キー初期化）には SO Pin が必要です



6.6 ロック解除

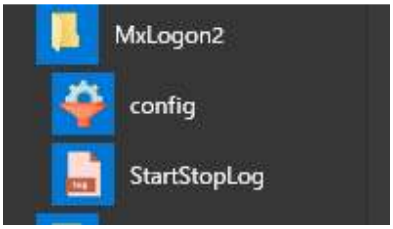
ロックしたキーを選択すると「ロック解除」タブが有効になります。



PIN ロックして時点で秘密データは削除されています。ロックを解除後は、再度認証領域のユーザ割り当て、ＰＩＮ設定を行ってください。

7　MxLogon2 の設定

管理者は「スタート」－「MxLogon2」－「設定」で MxLogon2 の設定を各コンピュータで行えます。



ファイル場所：

%Program Files%¥RiBiG¥MxLogon2¥config.exe

7.1　設定タブ

7.1.1 USB キー取り外し時処理

ログイン中に USB キーを抜き取ったときの処理を設定できます。既定ではロックしますが、サインアウト、または、何もしないように設定できます。

7.1.2　登録キーのみ利用可能

コンピュータに登録した USB キーだけを認識するようにできます。チェックすると接続 USB キーを登録したり、登録済み USB キー一覧を表示したりできます。

注意：

このオプションを有効にしたら必ず USB キーを登録してください。USB キーを登録しないままにしていると USB キーによるログインが不可能になります。

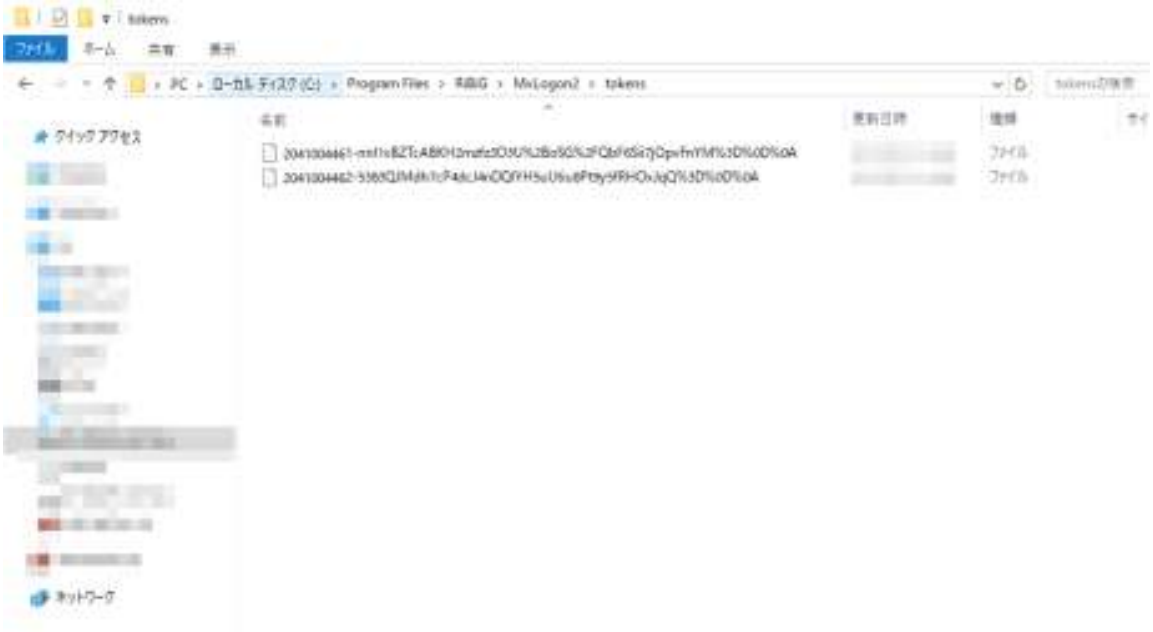
この問題を防止するため以下機能が組み込まれています。

- 登録されているキーがなければオプションは有効になりません。
- 識別文字列の末尾を “-master”とするとその USB キーは登録していなくても利用可能になります。

7.1.3　登録キー一覧

登録済みの USB キーは「登録キー一覧」リンクで確認できます。登録キー情報は MxLogon2 フォルダ内の tokens フォルダ内に書き込まれています。リンクはエクスプローラでそのフォルダを表示します。ファイル名の先頭部分が USB キーの識別名になっています。

USB キー登録を削除するには対応するファイルを削除してください。



7.1.4　接続 USB キーのコンピュータへの登録

リストボックスには現在接続されているＵＳＢキーが表示されます。「接続トークンのコンピュータへの登録」ボタンでリストに表示されているキーをすべて登録できます。

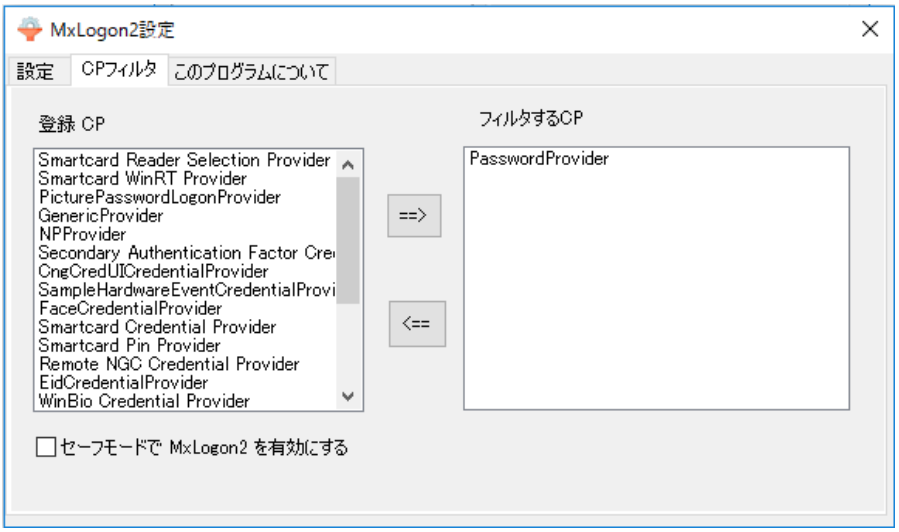
7.1.5　ワンタイムリモート PIN 無効

リモート接続では MxLogon2 は通常 PIN ではなくリモート PIN（ワンタイム PIN）を求めます。このオプションを有効にすると、リモート接続でも通常の固定 PIN を受け付けます

7.1.6　ユーザフィールドは正規表現

スロットのユーザ割当のユーザ名をプレーンテキストではなく正規表現と解釈するようになります。この場合でも、先頭文字として “ を指定すると、続く文字はプレーンテキストとして扱われます。

7.2 CP フィルタタブ



Windows には複数のログインプロバイダ(CP)が含まれています。それぞれの CP は、それぞれの設定に従ってログイン画面に表示されるようになります。複数の CP が同時に有効になっていれば、ユーザはその中から選択した CP を使ってログインできます。

Windows に USB キーがなければログインできないようにするには、MxLogon2 以外の CP がログイン画面に表示されないようにします。[CP フィルタ]タブでコンピュータに登録されているログインプロバイダをフィルタ（利用不可に）してください。

左側リストでフィルタするプロバイダを選択後、＝＞ボタンで右側リストに移動させます。
Windows 8/10 では以下 4 つをフィルタしてください。

PasswordProvider

PinLogonProvider

PicturePasswordProvider

WLIDCredentialProvider

Windows Vista/7 には PinLogonProvider, PicturePasswordProvider, WLIDCredentialProvider は存在しません。 PasswordProvider だけををフィルタしてください。

AzureAD に参加すると自動的にログイン画面に PIN 認証プロバイダが表示されます。
NGC Credential Provider をフィルタすると無効化できます。

7.2.1 “セーフモードで MxLogon2 を有効にする“

何も設定しなければセーフモードでは Windows 標準のプロバイダ以外は無効化されます。必ずユーザ名/パスワード認証が有効になります。保守目的のセーフモードでは Windows は必ず起動しなければなりません。Windows 標準のドライバ、プログラム以外が有効になっていると起動しない可能性があります。セーフモードでは起動しない原因となるこれらサードパーティのソフトを無効にして立ち上がります。MxLogon2 も無効化されます。

しかし、セーフモードで必ずユーザ名/パスワード認証が有効化されることはセキュリティ面で問題かもしれません。セーフモードで MxLogon2 を有効にするには、“セーフモードで MxLogon2 を有効にする“をチェックしてください。チェックすると MxLogon2 だけでなく、インストール済みのすべてのサードパーティのログイン認証プロバイダ（CP）が有効になります。PasswordProvider がフィルタされていれば、セーフモードでもユーザ名/パスワード認証が無効化されます。

セーフモードで MxLogon2 経由でログインすると、通常起動でのログイン同様、ログイン中に USB キーを抜き取るとロックします。

はじめて “セーフモードで MxLogon2 を有効にする“をチェックする場合、絶対に PasswordProvider はフィルタしないでください。セーフモードで MxLogon2 でログインできることを確認しないまま PasswordProvider をフィルタしてしまうと、もし、セーフモードで MxLogon2 でログインできない場合、コンピュータにログインできなくなります。必ず、PasswordProvider が有効な状態で、セーフモードでの MxLogon2 動作確認を行ってください。十分動作を確認してから PasswordProvider をフィルタしてください。

7.2.2 USB トークンによる “セーフモードで MxLogon2 を有効にする“

専用キーを使って MxLogon2 のログイン画面でセーフモードでの MxLogon2 の有効化、無効化を行うことができます。この専用キーを MxLogon2 のログインスクリーンで接続すると、“セーフモードで MxLogon2 を有効にする“が有効であれば無効に、無効であれば有効にします。

MxLogon2 が動作する限り、この専用キーがあればセーフモードでのサードパティプロバイダの有効化と無効化が可能です。セーフモードで MxLogon2 を有効化した後、PIN を忘れてしまったのでキーでログインできなくなった、他の方法でログインがなくなったという事態を回避できます。

専用キーをログインスクリーンで接続するだけでセーフモードでの MxLogon2 を無効化でき、セーフモードにおいてパスワードプロバイダによるログインが可能になります。専用キーを使えば、ログインして設定プログラムを起動することなく、ログインスクリーンで接続するだけで簡単にセーフモードでの MxLogon2 を有効化/無効が可能です。

専用キーの使用方法：

１．ログイン画面で MxLogon2 を選択。

２．“トークンを接続してください“　と表示されていることを確認

３．専用キーを接続（　**他のキーを同時に接続しないでください。エラー発生の原因となります**）

専用キーを抜き差しするごとに、セーフモードで有効になっていれば無効化、無効になっていれば有効かされます。

サウンドによる通知

専用キーのセーフモードでの MxLogon2 が 有効化されたのか、無効化されたのかは、サウンドファイルの再生によって確認できます。

有効化時　：　MxLogon2 フォルダの set.wav ファイルを再生します

無効化時　：　MxLogon2 フォルダの unset.wav ファイルを再生します

別のサウンドファイルを同名で保存してもかまいません。

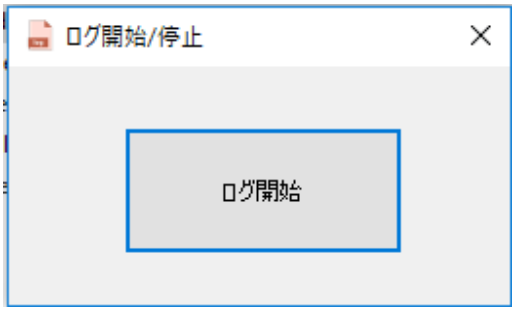
8　ログ

既定ではログは出力されません。ログを出力するには、

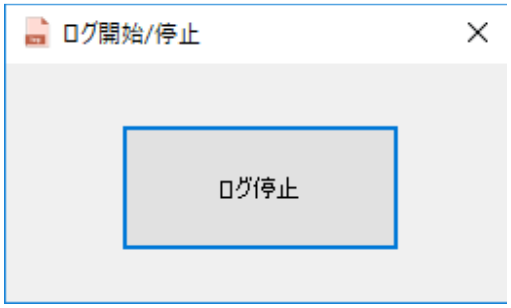
[MxLogon2]-[ログ開始停止]

%Program Files%¥RiBiG¥MxLogon2¥instEvtProvider.exe

を実行します。イベントビューアーが開いていたら実行する前に必ず閉じてください。



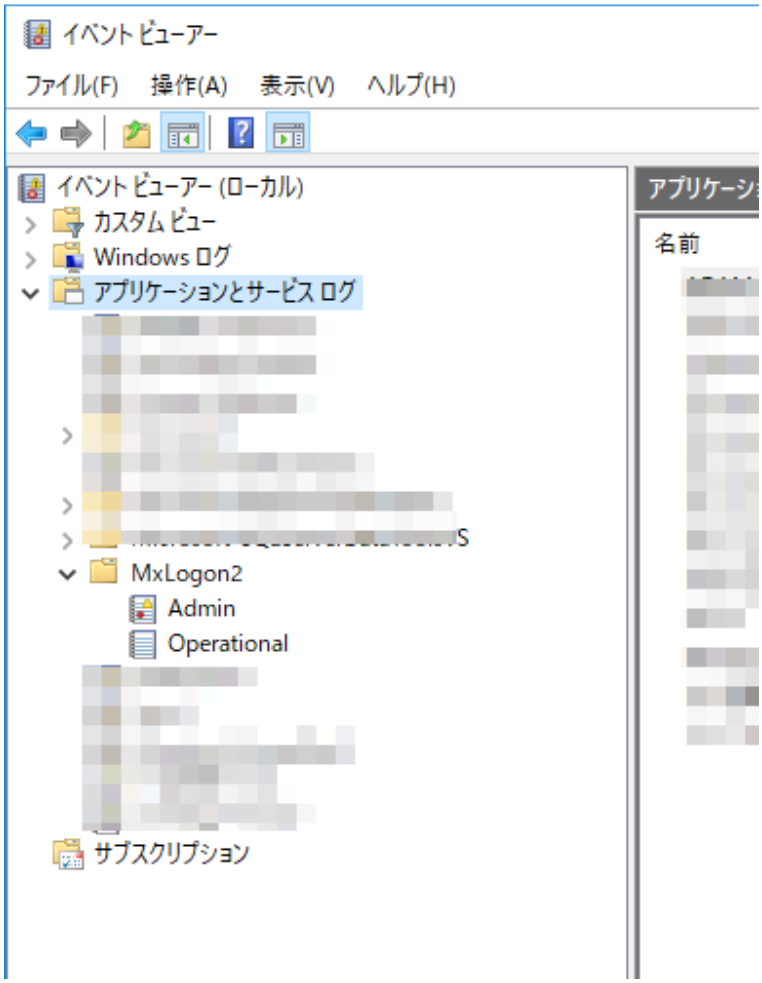
[ログ開始]ボタンをクリックすると、ログが出力されはじめます。ログ開始が既に設定されていると、ボタンは[ログ停止]になります。ボタンをクリックしてログ出力を停止できます。



ログはイベントビューアーで表示します。

ログを開始すると、イベントビューアーの左ペインの“アプリケーションとサービスログ”に MxLogon2 が表示されます。Operational にはキー操作のログイン、ログアウト、ロックが記録されます。Admin には警告、エラーが表示されます。

ログを停止するとイベントビューアーの左ペインの“アプリケーションとサービスログ”に MxLogon2 は表示されなくなります。



instEvtProvider は EventProvider.DLL の場所を登録するため、ログ開始したら停止するまでは EventProvider.DLL を移動/削除しないでください。

9　アンインストール

コントールパネルの「プログラムをアンインストール」から MxLogon2 をアンインストールできます。インストールしたアカウントでアンインストールしてください。

10 リモートデスクトップ

MxLogon 2 をインストールしたリモートコンピュータに USB キーでログインするには、クライアント側にプラグインをインストールします。

10.1 プラグインの導入

接続先リモートコンピュータが Win7(64 ビット)、Win8、Windows10

A. 配布メディアの [RDT] フォルダ内の RDTPlugin.DLL と setupClient.exe をクライアントコンピュータの任意のフォルダにコピー。 どちらも同じフォルダに置いてください。プラグイン（RDTPlugin.DLL）ソフトはリモートデスクトップクライアントを起動する度に読み込まれますので、固定ディスクのフォルダにコピーしてください。

B. SetupClient.exe を管理者として実行。このプログラムはプラグインを登録します。登録後 RDTPlugin.dll を移動、削除したりするとプラグインは読み込まれなくなりますのでご注意ください。

C. 各ユーザがユーザ権限で SetupClient.exe を実行、登録してください。SetupClient.exe を実行しないとそのユーザではプラグインは読み込まれませんのでご注意ください

接続先リモートコンピュータが Win Vista/7 の 32 ビット版

配布ディスクから OS のビット（32 ビット、64 ビット）と一致するバージョンの RDTLogon.DLL を固定ディスクにコピーしてください。そのファイルを Windows 付属の regsvr32.exe で登録します。

コマンドプロンプトで 以下のコマンドを実行

＞regsvr32 (RDTLogon.DLL へのパス)

Regsvr32.exe はシステムフォルダに入っていますのでフルパスを指定する必要はありません。

1. Regsvr32 は RDTLogon.DLL のパスを登録するだけです。
2. 登録後 RDTLogon.DLL ファイルの移動、削除したりするとプラグインは読み込まれなくなります
3. 登録には管理者権限は不要です。登録はユーザ毎に設定されますので、それぞれのユーザが登録しなければなりません

10.2 認証方式

リモートコンピュータには、クラシック認証、もしくは、ネットワークレベル認証でログインできます。

クラシック認証：リモートコンピュータに接続するとリモートコンピュータのログイン画面が表示されユーザ名、パスワードを入力してログインします。ログイン画面に入力するユーザ名/パスワードは回線に流れるため、インターネットのような公衆回線では安全ではありません。

ネットワークレベル認証(NLA)：リモートコンピュータに接続する前にクライアント側でリモートコンピュータへのログイン情報を入力します。その情報は暗号化されてリモート側に渡されます。リモート側は受け取ったログイン情報を使ってログインします。Windows では NLA が既定になっています。

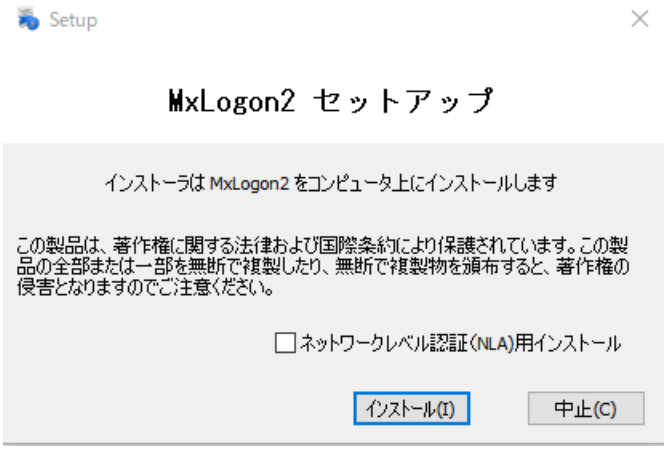
USB キーでクラシック認証を行う方法は、ローカルコンピュータへのログインとほぼ同じです。リモートコンピュータのログイン画面でローカルコンピュータのログイン画面と同じ操作を行います。

USB キーでセキュリティを損ねず、利便性を犠牲にせずに NLA 認証を行うにはキー設定によっては工夫が必要になります。これはローカル側で事前にリモートコンピュータにログインできなければならない、PIN を事前に入力することはできず画面での入力は危険であるという点をクリアしなければならないためです。

1. 自動ログオン（ユーザ名/パスワードをキーに保存）する設定になっている場合、NLA ではなくクラシック認証を使うべきです。安全性、利便性を損ねることなく利用できます。自動 PIN 設定になっていれば、ログイン画面で PIN を入力しないため安全です。PIN を画面で手入力する場合、リモート接続では、MxLogon2 の既定はリモート PIN の入力を求めます。リモート PIN はワンタイム PIN（使い捨て PIN）なので回線に流れても問題ありません。

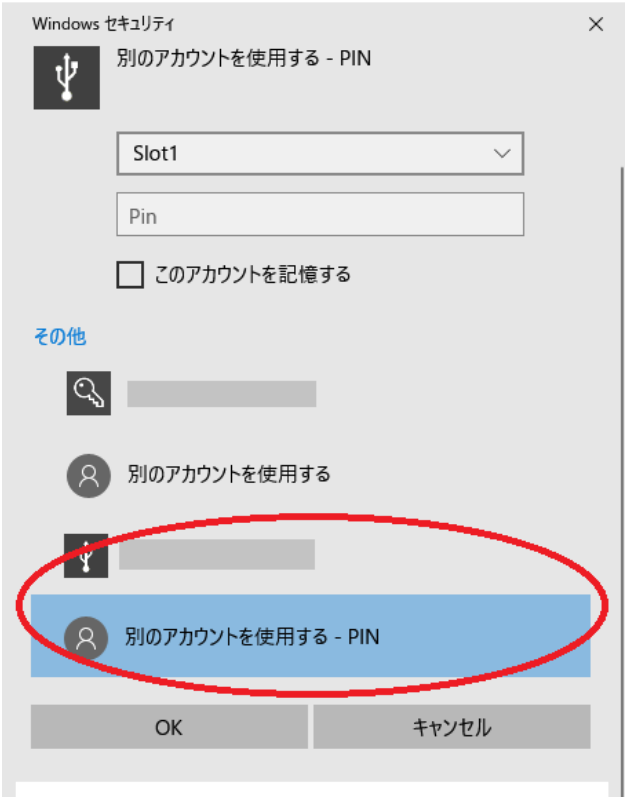
2. 自動ログオン設定になっていなければ NLA でログインします。ローカル側でユーザ名、パスワードを入力後、リモートコンピュータのログイン画面が表示されます。自動 PIN になっていれば、そのままログインします。PIN を手入力する設定になっていれば、リモート PIN を入力します。PIN 認証に成功後、クライアント側で入力したユーザ名/パスワードで自動ログオンします。Windows のバージョンによってはクライアント側で入力したユーザ名/パスワードを MxLogon2 が受け取れず自動ログインしません。ユーザ名/パスワードはクラシック認証と同じようにログイン画面で手入力しなければなりませんが、安全ではないため次の紹介する方法を検討してください。

クライアント側に MxLogon2 をネットワークレベル認証（NLA）用にインストールする方法もあります。



ネットワークレベル認証（NLA）用インストールをチェックしてから、インストールします。不要なファイルはインストールされません。

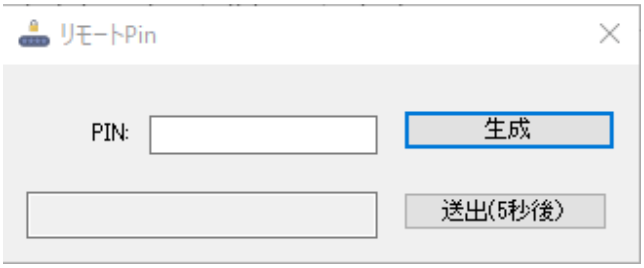
MxLogon2 を NLA 用にインストールしたコンピュータでは、ログイン、ロック解除、パスワード変更では MxLogon2 は無効化されます。NLA のローカル側認証で表示される Windows セキュリティ（CredUI） でのみ MxLogon2 が表示され、USB キー認証が可能です



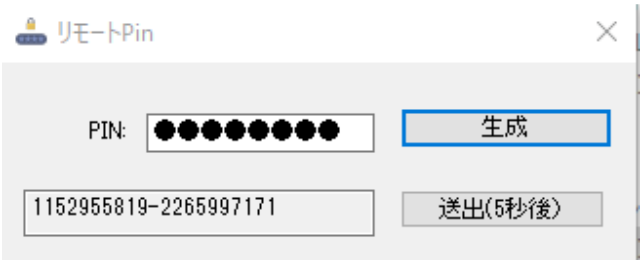
Windows セキュリティで MxLogon2 を選択します。ここでリモートコンピュータへのログイン処理をおこないます。ローカル側で事前にリモートコンピュータにログインでき、また、PIN 入力はローカル側で完結します。この方法を使うと USB キーを使った NLA 認証の問題点をすべてクリアできます。

10.3 リモートデスクトップの PIN 入力

リモートデスクトップで文字入力すると、回線にながれるため安全ではありません。リモートデスクトップで PIN を入力するには、Slot の PIN そのものを入力しないでください。代わりにワンタイムリモート PIN を入力してください。リモート PIN は配布ファイルの[RDT]フォルダ内の remotepin.exe で生成します。



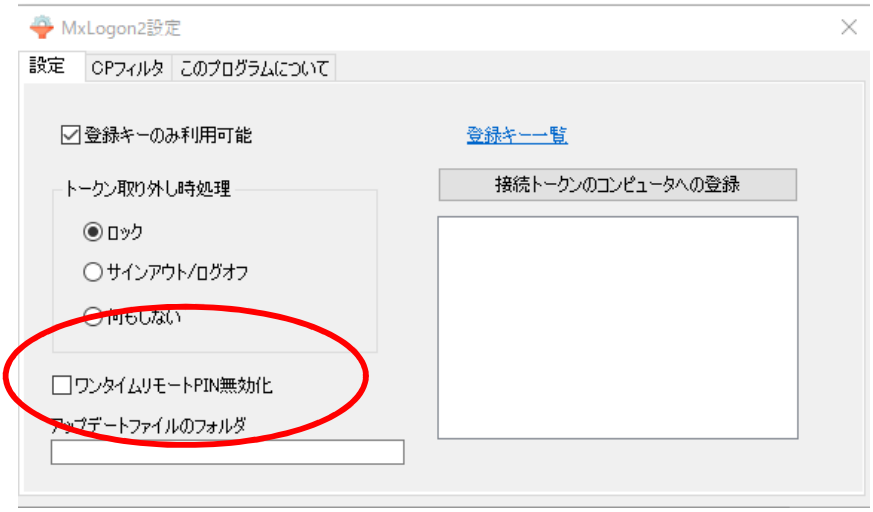
Remotepin.exe を起動してから、ＵＳＢキーの PIN を入力後、[生成]ボタンをクリックします。下のボックスにリモート PIN が表示されます。この PIN をリモートデスクトップの PIN フィールドに入力します。



リモート PIN はコピー/貼り付けするのではなく、[送出]ボタンで自動入力してください。[送出]ボタンをクリックしてから、5 秒後に入力フォーカスを持ったフィールドにリモート PIN の自動入力が開始します。ボタンをクリックしたら、リモートデスクトップクライアントの PIN フィールドをクリックして、PIN フィールドへの入力を可能にしてください。5 秒後に PIN が自動入力されます。

10.4 ワンタイムリモート PIN の無効化

利用環境によってはワンタイムリモート PIN ではなく Slot の PIN を直接入力してもかまわないかもしれません。ワンタイムリモート PIN は無効化できます。



10　MxLogon2 のアップデート

11.1 MxLogon2 の更新

Mxlogon2 には半自動更新機能があります。パスワードを設定していない USB キーでログインするときに、ユーザ名・パスワードを入力後、認証開始時に SHIFT キーを押してください。もし、指定フォルダにインストールされたファイルより新しい更新ファイルがあれば更新処理を行います。指定フォルダに対して読み込み権限のあるユーザがログイン画面で SHIFT キーを押すだけで更新作業が行えます。

＊USB キーの Slot にユーザ名とパスワードを設定してあると更新処理を行われません。パスワードが設定されておらず、ユーザ名・パスワード認証がされるときのみ更新処理が行われます。

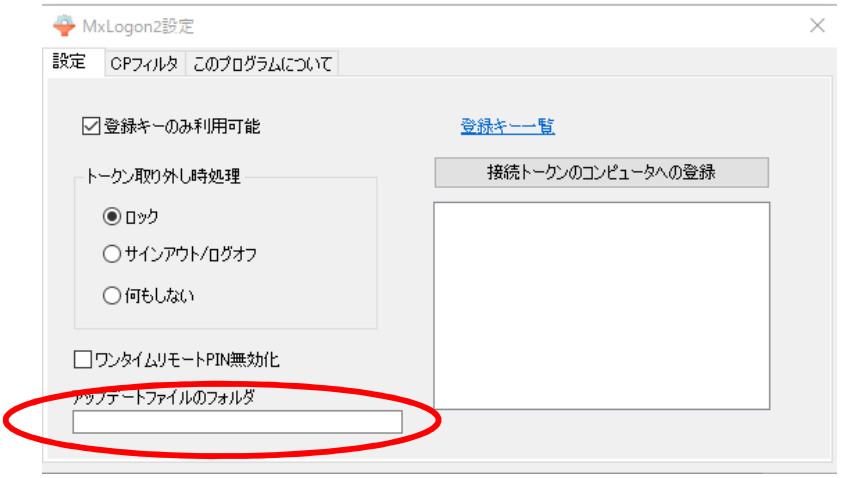
設定方法

1. 更新ファイルを置いた任意のフォルダを「設定」(config.exe) の設定タブで指定します。更新ファイルはリモートコンピュータであっても構いません。

   指定例：

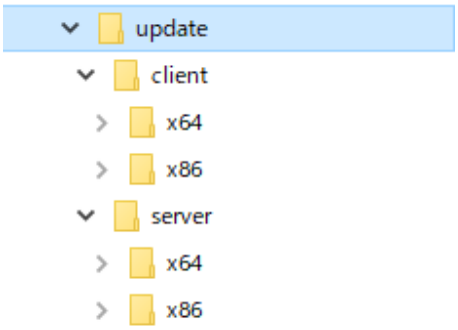
   ¥¥server¥shared¥update

   (コンピュータ server の shared フォルダ内の update フォルダ)



2. 更新ファイルを置くフォルダ配下に以下の構造のフォルダ/ファイルを設置してください。

更新フォルダ
(例¥¥server¥shared¥update)



*構造は配布ファイルと同じです。

クライアント OS は 32 ビット版、64 ビット版かによって、 client-x86 / x64 フォルダのどちらかにアクセスします。フォルダ内に配置した DLL/EXE/設定ファイル(.ini) のファイル更新日付がインストールされたものより新しいければ、新しいファイルをクライアント側にコピーしてインストールします。

ユーザ名/パスワード認証を行うときに SHIFT キーを同時に押してください。以下のようなポップアップが表示されます。

更新ファイルが見つかり、更新が完了・エラーが発生するとメッセージが表示されます。

[OK]をクリックするとユーザ名/パスワード認証画面に戻ります。

更新ファイルが見つからなければ、ポップアップ表示後にログインします。

11.2 更新フォルダの更新

手作業で新しいファイルを適当なフォルダにコピーしてください。更新フォルダには新しいファイルだけを置くだけで構いません。すべてのファイルを置く必要はありません。

手作業の代わりに自動更新することも可能です。更新ファイルだけを含む ZIP ファイルを用意して、弊社 Web サイトにアップロードします。ZIP ファイルは配布 ZIP ファイルと同じ構造でなければなりません。MxLogon2 には、このアップロードした ZIP ファイルをダウンロードして、更新フォルダに展開するプログラム(Windows サービス)が付属します。この Windows サービスを登録しておけば、定期的にアプロードされた ZIP ファイルを見に行き、もし、ZIP ファイルが新しければダウンロードして、更新フォルダに展開します。

弊社 Web サイトに置く最新 Zip ファイルは以下 URL よりアップロードしてください。アップロードするには正当なユーザ名/パスワードが必要です。

https://www.ribig.co.jp/mxlogon2/upload

11.2.1 ZIP ファイル取得、展開プログラム GetUpdateFile.exe

GetUpdateFile.exe はアプリケーションとして、または、サービスとして起動できます。

アプリケーションとして起動

GetUpdate.exe をダブルクリック

サービスとして起動

Windows サービスとして登録

>getupdatefile install

Windows サービスから削除

>getupdatefile remove

11.2.2 設定ファイル (GetUpdateFile.ini)

GetUpdateFile が ZIP ファイルをダウンロードして、更新フォルダに展開するには事前に設定ファイルで以下 3 項目を設定しなければなりません。

1 . Web サイトからダウンロードするためのユーザ名、パスワード） web_userpass

2 . 更新フォルダのパス　UpdateFolder

3 更新フォルダとしてリモートコンピュータ上のフォルダを指定した場合、リモートコンピュータにアクセスするための資格情報（ユーザ名、パスワード）userpass

また、オプションで Web サイトに更新ファイルを見に行く間隔を分単位で指定できます (UpdateIntervalInMin)

[options]

UpdateFolder=c:¥MxLogonUpdate

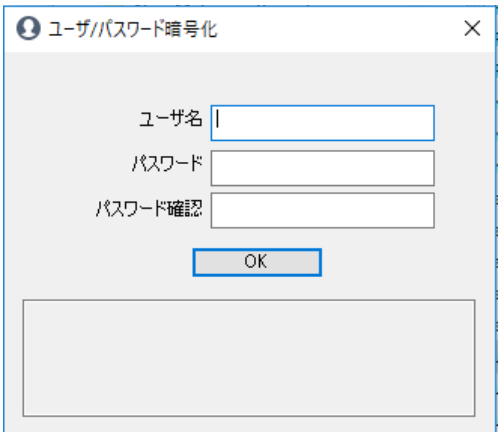
#UpdateFolder=¥¥server¥shared¥update　リモートコンピュータ上のファイル指定可

web_userpass=IZSiZ5LgNtq5fu**********

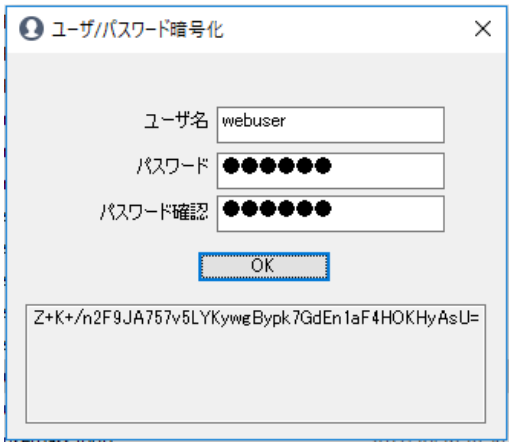
UpdateIntervalInMin=30

userpass=QfccsvTVr**********

web_userpass と userpass には、付属の UserPass.exe プログラムで暗号化した文字列を設定します。

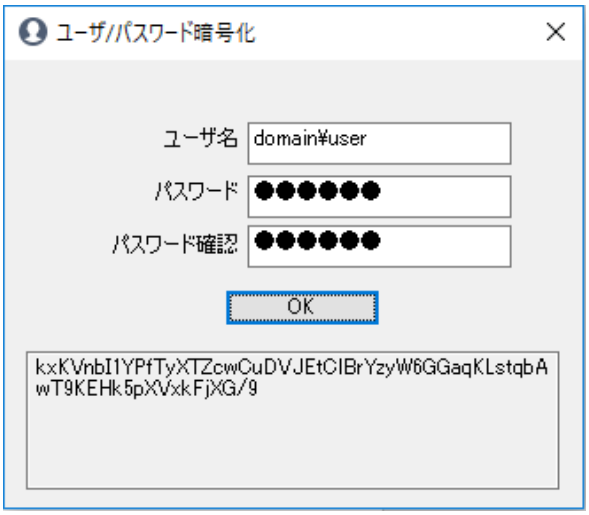


web_userpass　Web サイトから MxLogon2 の ZIP ファイルを取得するために必要なユーザ名とパスワードです。アップロードするユーザ名/パスワードと同じです。ユーザ名/パスワードを設定してから [ok]ボタンをクリックしてください。下のボックスにユーザ名とパスワードが暗号化された文字列が表示されます。その文字列をコピーして web_userpass に設定してください。



Userpass　　リモートコンピュータ上の更新フォルダを指定した場合のみ必要です。リモートコンピュータの更新フォルダにアクセスするためのユーザ名とパスワードを指定してください。指定するユーザは、更新ファルダへの読み込み権限がなければなりません。

ユーザ名はダウンレベル（domain¥user），UPN 形式でも指定できます。GetUpdateFile をアプリケーションとして起動している場合で、ログインユーザがリモートコンピュータの更新フォルダにアクセスできる場合がありますが、Windows サービスとして起動した場合は必ず必要です。リモートコンピュータ上の更新フォルダを指定した場合は設定必須と考えてください。



どちらもユーザ名とパスワードが１つの暗号化文字列になって表示されます。そのままを web_userpass, userpass に設定してください。

11.2.3 ログファイル(GetUpdateFile.log)

プログラムはメッセージを表示しません。GetUpdateFile と同じフォルダ内に作成されるログファイル GetUpdateFile.log で処理結果を確認してください。

付録１　リモートデスクトップの２つの認証

クラシック認証

リモートデスクトップクライアント起動。相手先コンピュータを指定して接続

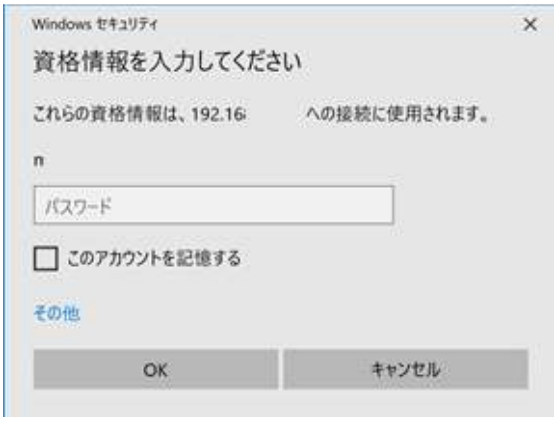
リモートコンピュータのログオン画面表示。

ログオン画面でユーザ名,パスワードを入力してサインイン

ネットワークレベル認証（ＮＬＡ）

リモートデスクトップクライアント起動。相手先を指定して接続

リモートコンピュータのユーザ認証を入力するウィンドウが表示され、ユーザ名、パスワードを設定して [OK]



リモートコンピュータはクライアントで入力した認証情報を受け取り、ユーザを自動ログオン。リモートコンピュータのログオン画面は表示されない

NLA 利点：クラシック認証は、ログオン画面でキーボードから 1 文字 1 文字入力するユーザ名、パスワードが回線に流れるため危険。ＮＬＡ認証ではクライアント側で入力したユーザ名/パスワードが暗号化されてリモートに渡る

リモートアクセスの設定

サーバ側

コントロールパネルのシステム、リモートアクセスの許可で設定

既定では NLA 認証のみ許可。クラシック認証を許可するには“ネットワークレベル認証でリモートデスクトップを実行しているコンピュータからのみ接続を許可する”のチェックを外す

クライアント側

既定ではリモートに NLA で接続する。 クラシック認証で接続するには、ドキュメントフォルダ内の リモートデスクトップクライアントの設定ファイル Default.rdp ファイルをテキストエディタで編集して、

```
enablecredsspsupport:i:0
```

を最後の行に追加。クライアントからクラシック認証モードでリモートコンピュータに接続するため、リモート側がクラシック認証を許可していればリモートの認証画面が現れる