GAUTHLOGON マニュアル

導入手順・操作

Ver. 2.1.0.2

有限会社リビッグ

横浜市港南区上大岡西 1-12-2

https://ribig.co.jp/gauthlogon

tel: 045-843-7122　Fax: 045-843-7142

目次

1. 概要

GAuthLogon は Windows ログインをワンタイムパスワードでセキュリティ強化するソリューションです。2 要素（2FA）認証でログインする Web アプリと同じように、ユーザ名/パスワード認証成功後、Authenticator アプリが表示するワンタイムコードの入力でサインインが完了します。

ユーザ/パスワード認証

コード認証

コード認証には RFC 6238 準拠の TOTP（時間ベースワンタイムパスワード）対応アプリ（ Google Authenticator や Microsoft Authenticator 等）が表示するワンタイムコードを入力します。

ローカルサインインだけでなく、リモート接続のサインインでもライアントにコード入力を求めることができます。

ローカル、リモートどちらの認証のセキュリティも GAuthLogon で強化できます。

1.1 インストール要件

A. システム設定に変更を加えるためインストールには管理者ユーザ権限が必要です。

B. Authenticator アプリ(Google/Microsoft 等) が Android/iOS デバイスにインストールされていなければなりません。インストール前に準備してください。

C. GAuthLogon をインストールするコンピュータの時間と Google Authenticator アプリが動作するデバイスの時間は正確でなければなりません。どちらかが数分以上ずれているとワンタイムパスワードは認証できません。スマートフォンはインターネット時刻と同期します。コンピュータの時間もできるだけインターネット時計と同期させるようにしてください。設定は付録１をご参照ください。

1.2 ライセンス表記/謝辞

このプログラムは次のライブラリ/ソースを利用しています。

libqrencode ライブラリで QR コードのビットマップデータを生成しています。
http://fukuchi.org/works/qrencode/index.html.ja

Sha1

```
/*
* Copyright 2010 Google Inc.
* Author: Markus Gutschke
*
* Licensed under the Apache License, Version 2.0 (the "License");
* you may not use this file except in compliance with the License.
* You may obtain a copy of the License at
*
*     http://www.apache.org/licenses/LICENSE-2.0
*
```

```
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
* WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
* See the License for the specific language governing permissions and
* limitations under the License.
*
*
* An earlier version of this file was originally released into the public
* domain by its authors. It has been modified to make the code compile and
* link as part of the Google Authenticator project. These changes are
* copyrighted by Google Inc. and released under the Apache License,
* Version 2.0.
*
* The previous authors' terms are included below:
*/

/*****************************************************************************
*
* File:    sha1.c
*
* Purpose: Implementation of the SHA1 message-digest algorithm.
*
* NIST Secure Hash Algorithm
*   Heavily modified by Uwe Hollerbach <uh@alumni.caltech edu>
*   from Peter C. Gutmann's implementation as found in
*   Applied Cryptography by Bruce Schneier
*   Further modifications to include the "UNRAVEL" stuff, below
*
* This code is in the public domain
*
*****************************************************************************
*/
```

Hmac

```
/ HMAC_SHA1 implementation
```

```
//
// Copyright 2010 Google Inc.
// Author: Markus Gutschke
//
// Licensed under the Apache License, Version 2.0 (the "License");
// you may not use this file except in compliance with the License.
// You may obtain a copy of the License at
//
//      http://www.apache.org/licenses/LICENSE-2.0
//
// Unless required by applicable law or agreed to in writing, software
// distributed under the License is distributed on an "AS IS" BASIS,
// WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
// See the License for the specific language governing permissions and
// limitations under the License.
```

Base32

```
// Base32 implementation
//
// Copyright 2010 Google Inc.
// Author: Markus Gutschke
//
// Licensed under the Apache License, Version 2.0 (the "License");
// you may not use this file except in compliance with the License.
// You may obtain a copy of the License at
//
//      http://www.apache.org/licenses/LICENSE-2.0
//
// Unless required by applicable law or agreed to in writing, software
// distributed under the License is distributed on an "AS IS" BASIS,
// WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
// See the License for the specific language governing permissions and
// limitations under the License.
```

GAuthLogon V2 からは　OpenSSL ライブラリは使用しません。

インストール

1.3 GAuthLogon の配布ファイル

クライアント OS 用 (client.zip)とサーバ OS 用(server.zip)を提供します。

ダウンロードした ZIP ファイルはブロックされています。解凍前にブロックを解除するか、解凍後に実行ファイルのブロックを解除してください。解除しないままインストールすると Windows Server OS では警告が毎回表示されてしまいます。

ZIP ファイルのブロックを解除しないまま解凍すると、解凍後のファイルはブロックされます。その場合、各ファイル毎にブロックを解除してください。

1.4 セキュリティオプションの設定

インストーラは以下２つのセキュリティオプションをインストール後の混乱を避けるため自動設定しません。GAuthLogon はログオン/ロック画面でユーザ名が表示されていない状態でご利用ください。２つのセキュリティオプションは手動で設定してください。

対話型ログオン: 最後のサインインを表示しない

https://docs.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/interactive-logon-do-not-display-last-user-name

対話型ログオン: セッションがロックされているときにユーザーの情報を表示する

https://docs.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/interactive-logon-display-user-information-when-the-session-is-locked

1.5 インストール開始

管理者ユーザとしてログインして配布ファイル内の Auto-setup.exe を実行してください。実行するには管理者権限が必要です。OS と一致する Setup.exe が起動します。インストールは数秒で完了します。

[OK]ボタンをクリックすると、Authenticator アプリを設定するプログラムが起動します。

一般ユーザでログイン、別の管理者ユーザとして資格昇格して Auto-setup を実行した場合は、プログラムを終了させてください。このプログラムはログインユーザのための設定を行います。別の管理者ユーザとして資格昇格した状態では、auto-setup はこの管理者ユーザが実行したことになり、ログインユーザのための設定を行えません。一度プログラムを閉じてから、プログラムを再度開いてください。

管理者ユーザとしてログイン、同じユーザが資格昇格した場合は、そのまま続行できます。

プログラムを起動するには、スタートメニュの GAuthLogon-トークン設定を選択します。

または、%ProgramFiles%¥RiBiG¥GAuthLogon¥addtoken.exe を実行します。

[生成]ボタンを押すと、QR コードを表示、パスワードフィールドに値をセットして設定データを自動保存します。

表示した QR コードを Authenticator アプリでスキャンします。

QR コード表示ウィンドウのテキストボックスには、既定ではユーザ名が表示されます（資格昇格していると、ログインユーザとは異なるユーザ名が表示されます。そのような場合、設定をクリアしてからプログラムを閉じてください）。ユーザ名に全角文字を使っていると QR コードを Authenticator アプリは正しく読み取れません。テキストボックスの文字列を編集してください。

テキストボックスの文字列は、Authenticator アプリが表示するコードのラベルとして表示されます。

任意の文字列を設定できますが、どのユーザのための QR コードかを判別できるような文字列にしておくべきです。

テキストボックスの文字列変更後は、必ず、再描画で QR コードを更新してください。再描画しないと QR コードに文字列はエンコードされません。

QR コードウィンドウを閉じても、パスワードフィールドをダブルクリックすることで QR コードは再表示できます。

回復コードの設定

16 桁以上の任意文字列の回復コードを設定できます。回復コードは、認証デバイスを紛失するなどしてワンタイムコードを入力できなくなった場合、ワンタイムコードの代わりに利用できるコードです。設定した回復コードは認証デバイスがなくなった場合、残された最後のログイン手段です。設定は必須ではありませんが、できるだけ設定するようにしてください。設定後、必ず保存ボタンで保存してください。

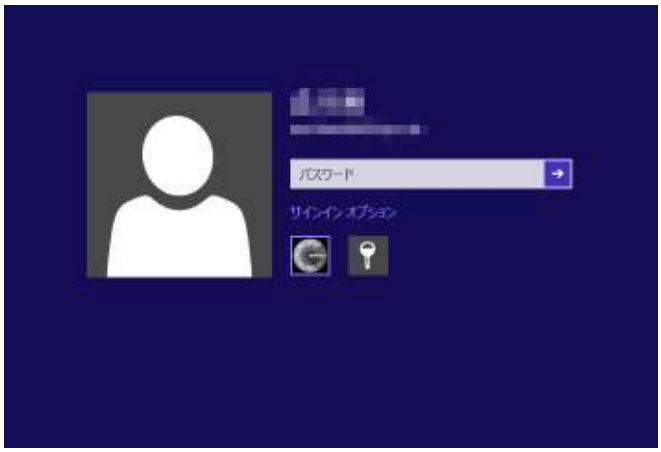
Ini_Mode は設定データの保管方法を指定します。とりあえず既定の userdomain のままにしておいてください。

以上で setup.exe を実行したユーザは GAuthLogon でワンタイムコード認証できるようになります。Authenticator アプリは、ユーザ毎にの設定しなければなりません。他のユーザは各自それぞれログイン後に AddToken.exe ユーティリティで Authenticator を設定してください。

2. ログイン

インストールされていることを確認するために、サインアウトしてください。 [サインインオプション]をクリックすると GAuthLogon のアイコンが表示されます。

Windows 8.x / 2012



Window Vista/7/2008

GAuthLogon 選択後、ユーザ名/パスワードを入力してください。認証に成功すると認証コードを入力する画面に切り替わります。

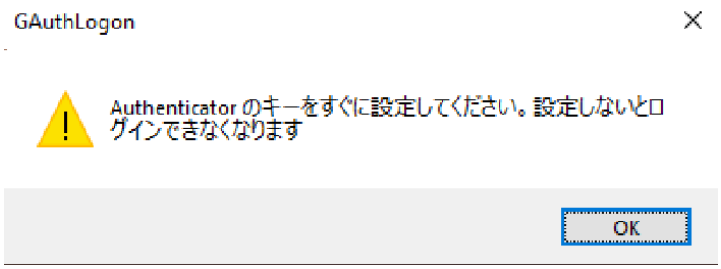
Windows 8.x / 2012

Authenticator アプリが表示する認証コードを入力します。前に戻るには、コードが空のままリターンするか、"前に戻る"をクリックします。

認証コードが正しければリターンでサインインします。

2.1 Authenticator アプリ未設定ユーザのサインイン

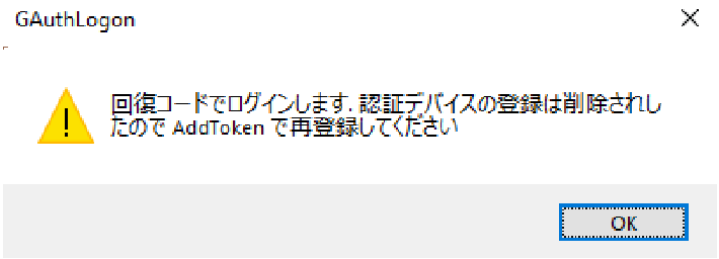
Authenticator アプリを設定していないユーザが GAuthLogon でログインすると、ユーザ/パスワード認証が成功するとワンタイムコード入力画面には切り替わらずに、以下メッセージが表示されます。



導入直後、Authenticator アプリが設定されていなくても何回かのログインではコード認証は求められません。しかし、上限回数（既定 7 回）を超えるとログインできなくなります。ログインできる間に AddToken で設定してください。

2.2 回復コードでサインイン

認証コードの代わりに、回復コードを入力できます。回復コードでログインすると、設定が削除されます。



何もしなければ Authenticator アプリを設定していない状態になります。回復コードでログインしたら、すぐに AddToken を起動して Authenticator アプリを再設定してください。

3. Authenticator アプリの設定

スタートメニュの GAuthLogon - トークン設定を選択します。

または、%ProgramFiles%¥RiBiG¥GAuthLogon¥addtoken.exe を実行します。

設定が済んでいなければ[生成]ボタンで QR コードを生成できます。設定データは自動保存されます。

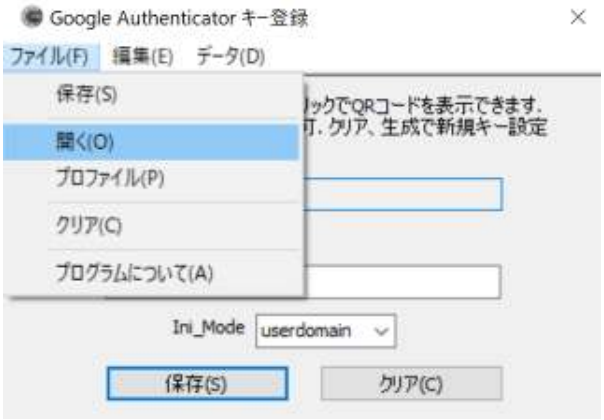
既に設定が済んでいると、設定データが読み込まれます。

回復コードは変更できます。回復コードのフィールドを空にして、保存ボタンで保存してください。入力文字が見えるようになります。また、フィールドが空の状態でダブルクリックすると自動で回復コードが入力されます。回復コードを変更したら必ず[保存]ボタンで保存してください。

設定データは、ユーザのプロファイルフォルダの以下ファイルに保存されます。

%UserProfile%¥AppData¥Roaming¥RiBiG¥GAuthLogon¥gauthlogon.ini

[ファイル]-[開く]を選択すると、設定データファイルを NotePad で開きます。



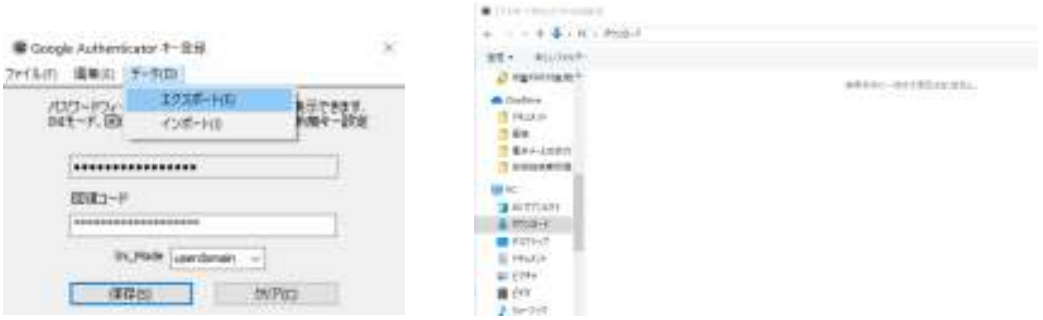
設定データファイルはテキストファイルです。自動設定されているデータは手動では変更しないでください。ユーザ固有の設定の追加にはデータファイルを編集します。

Ini_Mode が userdomain の場合、設定データをエクスポートして、別のコンピュータの同じドメイン/ユーザの設定としてインポートできます。 ドメイン名、ユーザ名が異なっているとインポートしたとしても、正しい設定データとして認識されません。ローカルユーザの場合、ユーザ名が一致すれば、他のコンピュータの同名ユーザが設定をインポートできま

す。例えば、コンピュータ A のローカルユーザ user の設定データは、他のコンピュータのローカルユーザ user にインポートできます。

3.1 設定のエクスポート方法：

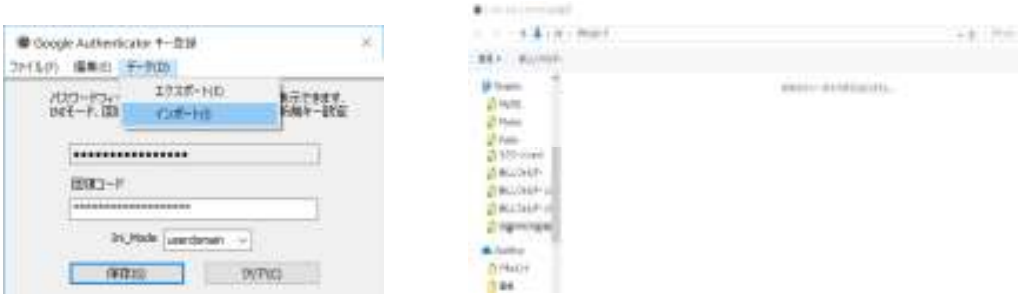
[データ]-[エクスポート]を選択後、エクスポート先のファイルを指定します。



出力先を指定後、エクスポートデータを暗号するパスワードを設定してから[了解] で完了します。

3.2 設定のインポート方法：

別のコンピュータの同じドメインユーザか、同じ名前のローカルユーザは、設定をインポートできます。別のコンピュータで Addtoken の[データ]-[インポート]選択、エクスポートファイルデータを選択、パスワードを設定して了解ボタンをクリックして完了です。



エクスポート/インポートされるのは基本データのみです。他のオプションデータは手動で設定してください。

エクスポート/インポートは、ユーザ間の設定データのコピーにすぎません。インポートしたユーザは、設定を自由に変更できますが、他のユーザの設定に影響を与えることはありません。ユーザ間で設定データを共有するには、設定のリダイレクトを有効にします（「11. 設定ファイルのリダイレクト」参照）

Ini_Mode が unique になっていると、現在のログインユーザのみが利用できるように設定データを保存します。最もセキュアな保存方法です。ただし、設定データをエクスポートすることはできません（　する意味がありません、バックアップは設定ファイルのコピーで可能です　）。リダイレクト設定を有効にすることもできません。

Ini_Mode が share になっていると、同じコンピュータであれば設定ファイルを他のユーザのプロファイルフォルダにコピーできます。別のコンピュータに設定を持っていくには、エクスポート後、別のコンピュータでインポートします。インポートしたユーザから同じコンピュータのユーザに設定ファイルをコピーできます。

3.3 別ユーザとして実行

ログインユーザとは別のユーザの設定を行うことができます。起動時に［SHIFT］キーを押し下げてください。指定ユーザとして実行というウィンドウが表示します。

設定を行いたいユーザの名前とパスワードを入力して [了解]をクリックすると、指定したユーザが　AddToken が実行したことになり、設定はそのユーザにプロファイルに保存されます。

4. ワンタイムコード入力の必須化

GAuthLogon をインストールしただけでは、ワンタイムコードを入力しなくても Windows にサインインできてしまいます。ログイン画面で GAuthLogon 以外のプロバイダを選択できるためです。例えば、Windows 標準のユーザ名/パスワードプロバイダを選択すれば、サインインに認証コードの入力は不要です。認証コードの入力を必須とするには、GAuthLogon 以外のプロバイダをログイン画面で選択できないようにします。

スタートメニューの GAuthLogon―設定を選択します。

または、%ProgramFiles%¥RiBiG¥GAuthLogon¥config.exe を実行します。

プログラム起動後、[ＣＰフィルタ]タブを選択してください。

左リストに現在 Windows に登録されているプロバイダの一覧が表示されます。ログイン画面の[サインインオプション]で表示させたくないプロバイダを右側のリストに移動させます。左側リストで選択後、 [==>] ボタンで右のリストに移動させます。

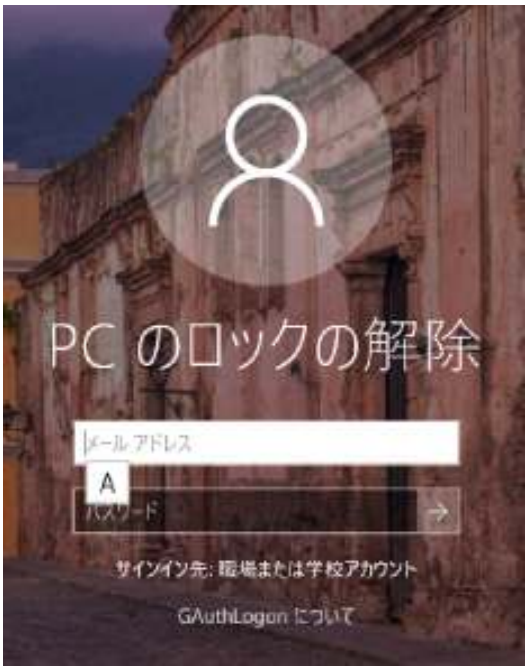
ワンタイムコードを必須化させるには、以下プロバイダをフィルタしてください。
＊試用版は最大２つまでフィルタ可能です。２つ以上の CP はフィルタできません。

PasswordProvider
PicturePasswordLogonProvider (Win8 以降)
PINLogonProvider (Win8 以降)
WLIDCredentialProvider (Win8 以降)

Windows を AzureAD に参加させると、ログイン画面で PIN ログインが選択できるようになります。この PIN ログインを無効にするには“NGC Credential Provider”をフィルタします。

変更は自動的に保存されます。

ログオフすると、ログイン画面には[サインインオプション]が表示されていないか、表示されていても標準のユーザ名/パスワードプロバイダ、ピクチャパスワード、PIN、Windows LiveID プロバイダは現れなくなります。



GAuthLogon 以外でサインインできないため、これでコード認証が必須化されました。

セーフモードで GAuthLogon の有効化

セーフモードではサードパーティーのクレデンシャルプロバイダは既定で無効化されます。これは、サードパーティーのクレデンシャルプロバイダが原因でログイン画面が表示されないといった事態が発生しても、セーフモードではログインできるようにするためです。

セーフモードで GAuthLogon を有効にすると、セーフモードで起動した場合でもサードパーティのすべてのプロバイダが有効になります。これはサードパーティのログオンプロバイダが原因でセーフモードでログインできない可能性がでてくることを意味します。

このような理由から、このオプション有効化は慎重に行う必要があります。最初は必ず PasswordProvider をフィルタしないでオプションを有効化してください。

セーフモードで GAuthLogon で何度かログインできることを確認し、さらに、リカバリーコードで GAuthLogon を解除できること等の作業を行い、問題がないことを確かめてください。また、このオプションを有効化する際には、問題発生時の対策を検討しておいてください。

管理者ユーザはプライベート設定で DisableGAuthInSafeMode を有効にできます。このオプションが有効になっていると、回復コードでログイン時、GAuthLogon のセーフモードでの有効化を解除することができます。

5. リモートデスクトップ

ローカルログインでコード認証が必須化されていると、リモートログインに対しても認証コード入力が必須となります。

リモート接続を開始すると、ネットワークレベル認証によってクライアント側でユーザ名/パスワード入力を求められます。認証が成功すると、リモートコンピュータに接続します。

リモートコンピュータのサインイン画面が表示され、GAuthLogon が認証コード入力を求めます。正しいコードを入力するとリモートコンピュータにサインインします。

- 2017 年の Windows 10 Fall Update (バージョン 1709) リモートデスクトップのサーバ側の OS がｋの Windows バージョンの場合、リモートコンピュータのログイン画面でユーザ名/パスワード入力を求められます。ネットワークレベル認証によってクライアント側で入力したユーザ名/パスワードが、リモート側の GAuthLogon に伝わらないためです。ログイン画面でのユーザ名・パスワード入力はセキュアではありません。OS のアップデートをお勧めします。

6. GAuthLogon のオプション設定

オプションはすべてのユーザに適用されるグローバル設定と各ユーザに適用されるプライベート設定の 2 種類あります。グローバル設定は GUI により設定できます。

6.1 グローバル設定

1. 「Program Files」－「RiBiG」－「GAuthLogon」内の config.exe を起動するか、スタートメニュの[GAuthLogon]-[設定]を選択してください。

ロック解除時コード認証不要	ログイン時のみコード認証を求められます。ロック解除ではコード認証は求められません。
リモートログイン時のみコード認証	コンソールログイン/ロック解除ではコード認証は求められません。
リモードログイン時の自動ログイン無効	既定では、ネットワークレベル認証でクライアント側で入力した資格情報で自動ログイン後にコード認証画面を表示します。オプションを有効にすると自動ログインせずにユーザ名/パスワード入力を求めます。
CredUI でのパスワードプロバイダ常時有効化	ログイン中に表示される資格情報ウィンドウでパスワードプロバイダが有効になります。
LiveID 認証	有効化すると LiveID 資格情報で LiveID 認証が行われます。無効にすると LiveID 認証は失敗します。
AzureAD 認証	有効化すると Azure AD 資格情報で Azure AD 認証が行われます。無効にすると Azure AD 認証は失敗します。 AzureAD に参加した PC でのみ有効にしてください。
コード入力タイムアウト	コード入力画面は一定時間が経過するとユーザ/パスワード画面に自動的に戻ります。その時間を指定できます。
コード未入力での最大ログイン回数（ユーザ）	一般ユーザが Authenticator アプリを設定しないままログインできる回数を指定します。
コード未入力での最大ログイン回数（管理者）	管理者ユーザが Authenticator アプリを設定しないままログインできる回数を指定します。

エラーログファイルパス	問題発生時、エラーの原因を調査するためのログファイルの場所を指定します。フルパスで指定してください。指定ファイルは存在しなければなりません（事前に空ファイルを作成する等）

グローバル設定は %%Program Files%%¥RiBiG¥GAuthLogon¥gauthlogon.ini に保存されます。

6.2 プライベート設定

各ユーザのホームフォルダ下の以下設定ファイルを直接編集することで設定します。

%HOMEPATH%¥AppData¥Roaming¥RiBiG¥GAuthLogon¥gauthlogon.ini

ロック解除時コード認証不要

グローバル設定を同じオプションを上書きします。

```
[Google Authenticator]
NoCodeAuthForUnlock=yes
```

コード認証の有効化

グローパル設定で“リモートログイン時のみコード認証“を有効にするとコンソールログインではコード認証を求められません。そのような設定がされていても、このオプションを有効にしたユーザはコード認証を求められるようになります。

```
[Google Authenticator]
ForceCodeAuth=yes
```

管理者ユーザのコード認証無効化

管理者ユーザのみ設定可能なオプションです。有効化するとコード認証を求められなくなります。一般ユーザで設定してもオプションは無視されます

```
[Admin]
NoCodeAuth = yes
```

管理者ユーザのログイン時でのセーフモードでの GAuthLogon 無効化

管理者ユーザのみ設定可能なオプションです。このユーザが回復コードでログインすると、セーフモードで GAuthLogon が有効であれば無効化するかどうか確認を求めてきます。必要であればその場で無効化できます。

```
[Admin]
DisableGAuthInSafeMode= yes
```

7. 設定ファイルのリダイレクト

この設定ファイルのリダイレクトは GAuthLogon が実装する機能です。これとは別にドメイン環境における Windows のフォルダダイレクトや移動ユーザプロファイルを利用してサーバ上に GAuthLogon 設定を保存することが可能です。また、Rclone を利用してクラウドストレージに設定ファイルを保存する方法もあります。

ドメイン環境ではフォルダダイレクト/移動ユーザプロファイルを利用してサーバ上に GAuthLogon 設定を保存することを推奨します。

ドメイン環境のフォルダダイレクト/移動ユーザプロファイルを利用しておらず、インターネットに常時接続されていれば、Rclone を利用してクラウドストレージに設定ファイルを保存する方法を推奨します。

詳しくは “設定データの同期“マニュアルをご覧ください。

ここで説明する GAuthLogon の設定ファイルのリダイレクトは最後の手段として利用してください。

AddToken で生成した設定データは、既定ではユーザのプロファイルディレクトリに保存されます。

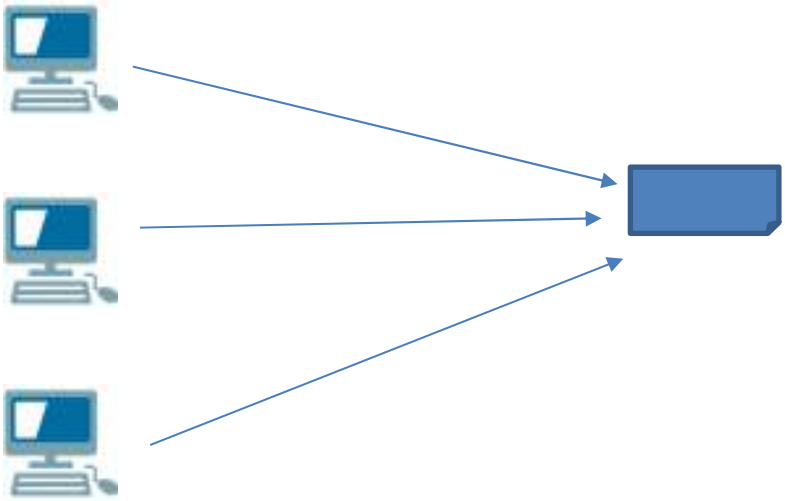
%UserProfile%¥AppData¥Roaming¥RiBiG¥GAuthLogon¥gauthlogon.ini

それぞれのユーザは AddToken で QR コードを生成して Authenticator アプリを設定しなければなりません。Authenticator アプリを設定すると同時に PC のユーザプロファイルフォルダ内の gauthlogon.ini が更新されます。あるユーザと同一の設定を流用するには、設定のエクスポート/インポートを行います。流用元の設定をエクスポートして、その設定をインポートします。この場合、設定はコピーされるだけです。設定をインポートしたユーザが設定変更しても、元の設定は自動的に変更されることはありません。同期させるにはエクスポート、インポートを繰り返す必要があります。

設定ファイルをリダイレクトさせることで、ユーザ間で設定を共有できます。リダイレクト設定を行うと、あるユーザが設定を変更すると、設定を共有しているすべてのユーザの設定が変更されることになります。

Ini_Mode が unique になっていると、設定ファイルはリダイレクトできません。
Unique 設定は、エクスポートすることも、共有することも不可です。

1 つの設定ファイルを複数のコンピュータ上の GAuthLogon で共有



外部コンピュータに設定ファイルを置くと、ネットワークの問題で設定ファイルを読み込めない可能性があります。GAuthLogon はリダイレクトを有効すると、リダイレクト先と同じ設定データをローカルのプロファイルフォルダにも保存します。

ログイン処理

1. リダイレクト先にアクセスできると設定データをプロファイルフォルダの設定ファイルにコピー、そのローカルデータを用いてコード認証

2. リダイレクト先にアクセスできなければ、ローカル設定を使ってワンタイムードを認証

ローカル設定を用いてコード認証を行うため、ネットワーク環境から離れて、スタンドアローン状態になってもコード認証は可能です。このため常にリダイレクト先のデータと同じ設定データがローカルにも保存されるようになっています。

1. AddToken は設定データ保存時に、リダイレクト先とローカルに保存
2. サインイン処理でリダイレクト先の設定データをローカルにコピー

Ini_Mode=userdomain

同一ドメインユーザ、または、同じ名前のローカルユーザが設定ファイルを共有できます。異なるユーザ間では共有できません。回復コードはリダイレクト先のファイルに保存され、共有されます。

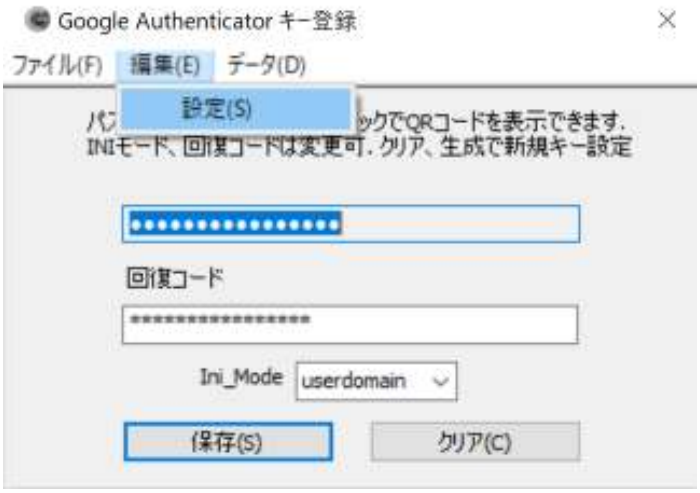
回復コードでログインすると、ローカルの設定データが削除されます。回復コードでログインしたコンピュータでは、設定が失われ、何もしなければ次回ログイン時、キーが見つかりませんという警告が表示されます。リダイレクト先の設定は削除されませんので、他のコンピュータは影響を受けません。

サインイン処理では、リダイレクト先の設定データをローカルにコピーするのが通常の処理です。ローカル設定が空になっているとリダイレクト先設定はコピーされません。
GAuthLogon はコード認証をローカル設定で行いますので、キーが見つかりませんという警告が表示されます。

リダイレクトを有効にしたら、常にリダイレクト先のデータと同じ設定データがローカルにも保存されるようにしなければなりません。ローカル設定が空の場合、リダイレクト先のデータとローカル設定は不整合な状態になります。自動では解消されません。
AddToken を起動して手動で解消します。AddToken はローカルコピーが空でも、リダイレクト先から設定データを取り出します。取り出された設定を保存すると、リダイレクト先とローカル設定が同期して、不整合を解消できます。

回復コードでログインした場合、できるだけ別の回復コードに変更するようにしてください。いずれかのコンピュータで回復コードを変更すると、リダイレクト先に保存されますので、設定ファイルを共有している他のコンピュータでも変更後の回復コードを利用できます。

リダイレクト設定方法：
[編集]-[設定]を選択します。



表示されるウィンドウでリダイレクト先ファイルを指定します。

[了解]をクリックすると、現在有効な設定をリダイレクト先に設定します。

リダイレクト先の共有方法：

別のコンピュータで同じリダイレクト先を共有するには、リダイレクトを設定したコンピュータで設定をエクスポート、そのエクスポートして設定をインポートします。

もし、別のコンピュータでリダイレクトを設定してしまうと、そのコンピュータの設定が有効になり、リダイレクト設定ずみコンピュータの設定は無効になります。必ず、1 台のコンピュータでリダイレクトを設定、その設定をエクスポートして、他のコンピュータにインポートするようにしてください。

リダイレクトの無効化：

AddToken で[編集]-[設定]　を選択後、設定ファイルパスを空にしてから[了解]をクリックします。

Ini_Mode=share

すべてのユーザが設定ファイルを共有できます。異なるユーザが設定を共有することになるため、回復コードはリダイレクト先のファイルには保存されません。ローカルのユーザプロファイルフォルダに保存されます。リダイレクト先を共有する各ユーザは回復コードをコンピュータ毎に設定してください。回復コードでログインした場合の動作は

userdomain と同じです。不整合状態は AddToken を起動して解消します。設定ファイルのリダイレクト設定、共有方法も userdomain の場合と同じです。

8. 設定の保存/切り替え

現在の設定は名前を付けて保存したり、保存済み設定に切り替えたりすることができます。「ファイル」-「プロファイル」を選択してください。

新規保存

[現在設定を名前を付けて保存]の下の編集ボックスの任意の名前を入力して、ボタンをクリックします。現在の設定がプロファイルとして保存され、名前が左側リストに表示されます。最大 8 個のプロファイルを保存できます。

切り替え

左側リストでプロファイル名をダブルクリックすると、そのプロファイルが読み込まれ、現在の設定になります。

上書き保存

左側リストでプロファイル名を選択すると、右側の編集ボックスに名前が入力されます。同一名で設定を保存すると、既存のプロファイルを上書きします。

削除

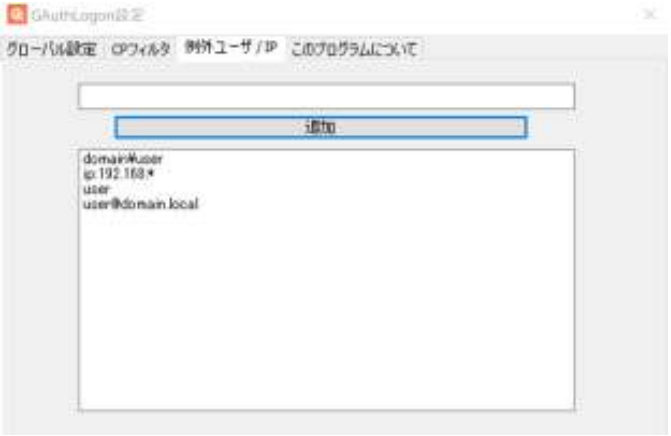
リストボックスでプロファイルを選択後、[プロファイル削除]で保存プロファイルを削除できます。

9. コード認証除外ユーザ/IP

管理者ユーザは任意のユーザをコード認証例外ユーザとして設定できます。また、特定のクライアントのリモート接続に対してコード認証を不要とすることもできます。この指定はグローバル設定として保存されます。

設定プログラムを開いてください。
「Program Files」－「RiBiG」－「GAuthLogon」内の config.exe を起動するか、スタートメニュの[GAuthLogon]-[設定]を選択します。

[例外ユーザ]タブを選択します。



既に設定されているユーザ名/IP はリストボックスに表示されます。

例外ユーザ追加

編集ボックスにログイン時に入力するユーザ名を設定して、[追加]ボタンで追加します。
クライアント IP は、“ip:192.168.1.1” のように 先頭 3 文字を “ip:”とします。IPv6 も同様に先頭 3 文字を “ip:”にして入力してください(例：ip: 2001:0DB8:AC10:FE01::1)
IP にはワイルドカード文字(*)を指定できます(例：192.168.1.＊)

例外ユーザ削除

リストボックスでユーザ名をダブルクリックします。

10. ライセンスファイルのインストール

GAuthgLogon はライセンスファイルがインストールされていないと評価版として動作します。評価版は起動時やログイン時に“評価版“ウィンドウが表示されます。生成される暗号鍵はランダムな値ではなく、固定の値になります。このため評価版ではコード認証時、すべてユーザは同一認証コードを求められることになります。

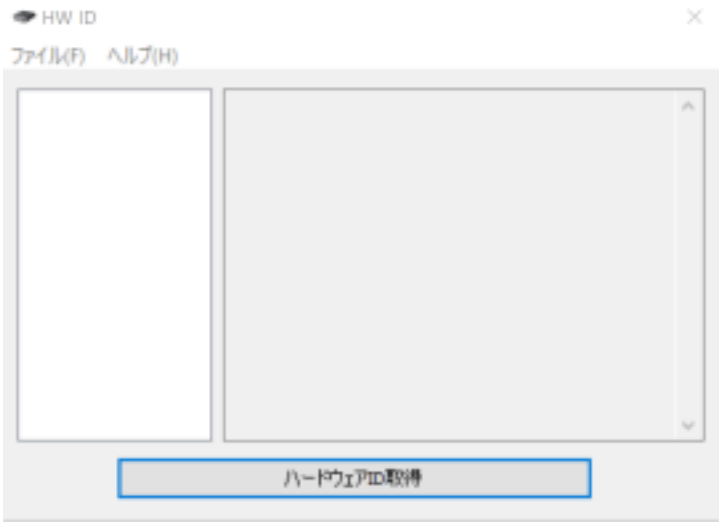
ライセンスファイル取得には以下３つの処理が必要です。

1. ライセンスを紐づけるコンピュータのハードウェア ID 生成
2. ライセンス発行ページでハードウェア ID を指定してライセンス発行
3. ライセンス発行サイト用アカウント作成

ライセンスが発行されるとライセンスファイルがダウンロードされます。このファイルを正しくインストールすることで、ライセンス設定されます。

10.1 ライセンスを紐づけるコンピュータのハードウェア ID 生成

ライセンスはそれぞれのコンピュータに紐づけられます。ライセンスを発行するにはコンピュータを識別するハードウェア ID（文字列）を指定、そのハードウェア ID に対してライセンスは作成されます。ハードウェア ID の生成にはインストールパッケージに含まれる hwid.exe を実行します。



＊従来のバージョンでは MAC アドレスを検出していましたが、現在バージョンは MAC アドレスを利用しません。左側リストボックスには何も表示されません。

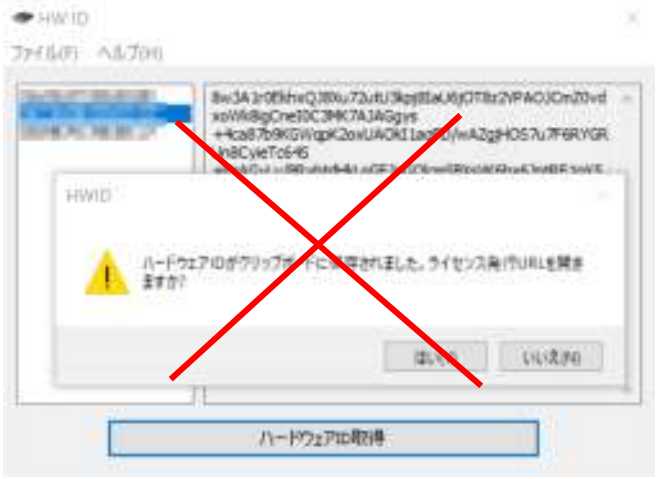
[ハードウェア ID 取得]ボタンのクリック後、MAC アドレスが検出すると左側リストボックスに表示します。

[OK]をクリックするとコンソールが開いて“ipconfig /all”の結果が表示されます。どの機器に MAC アドレスが割り当てられるか確認できます。ライセンスと紐づけする MAC アドレスを選択してから再度[ハードウェア ID 取得]ボタンをクリックしてください。

MAC アドレスが 1 つだけの場合、そのアドレスをリストに表示、自動選択してハードウェア ID を生成します。

ハードウェアＩＤは不可逆的なハッシュを算出することで生成されます。ハッシュがハードウェアＩＤ生成につかわれます。逆にハードウェア ID からはユーザＰＣを特定することはできません。

~~ハードウェア ID が生成されるとクリップボードにコピーされ、同時にライセンス発行 Web ページを開くかどうか尋ねてきます。~~



ハードウェア ID は自動でクリップボードにコピーされません。プログラムでクリップボードにコピーする操作は、アンチウィルスプログラムによって悪意のあるコードと誤検出されてしまいます。これを避けるためクリップボードにコピーする処理は行いません。

10.2 ライセンス発行ページでハードウェア ID を指定してライセンス発行

ライセンス発行ページが開いたら、ハードウェア ID フィールドに張り付けてください。Window2008 Server の IE ではライセンス発行ページの https のバージョンに対応して

いないため開けないかもしれません。そのような場合、別ブラウザ（Chrome ブラウザ等）を使ってください

アカウント名とパスワードを設定して、ハードウェア ID フィールドにハードウェア ID をペーストしたら[ライセンス発行]ボタンをクリックします。

既定設定では、ライセンスは無効化不可です。V2.1.0.1 以前のバージョンのライセンスはすべて無効化不可でした。V2.1.0.1 以降のみ無効化可能ライセンスを認識します。

10.2.1 無効化可能ライセンス

無効化可能ライセンスの利点は、有効期限の残っているライセンスを無効化して、そのライセンスの有効期限を引きつぐ別の PC 用のライセンスを発行できるところです。また、有効期限の残っているライセンスの期限残を新規ライセンスに持ち越すことも可能になります。

ライセンスの無効化は弊社ライセンスサーバで行います。ライセンスが無効か有効であるかは、ライセンスサーバに問い合わせをしなければなりません。無効化可能ライセンスをインストールすると、必ず、プログラム起動時、ライセンスサーバへの問い合わせ処理が発生

します。PC がインターネットに接続していないと、この処理に失敗します。

10.2.2 無効化不可ライセンス

無効化可能のチェックを外して発行したライセンスをインストールすると、ライセンスサーバへの問い合わせは発生しません。スタンドアローン PC でもライセンスは認証されます。しかし、ライセンスをインストールした PC を使わなくなると（故障、入替等）、PC のハードウェア ID に関連づけられたライセンスも使えなくなります。

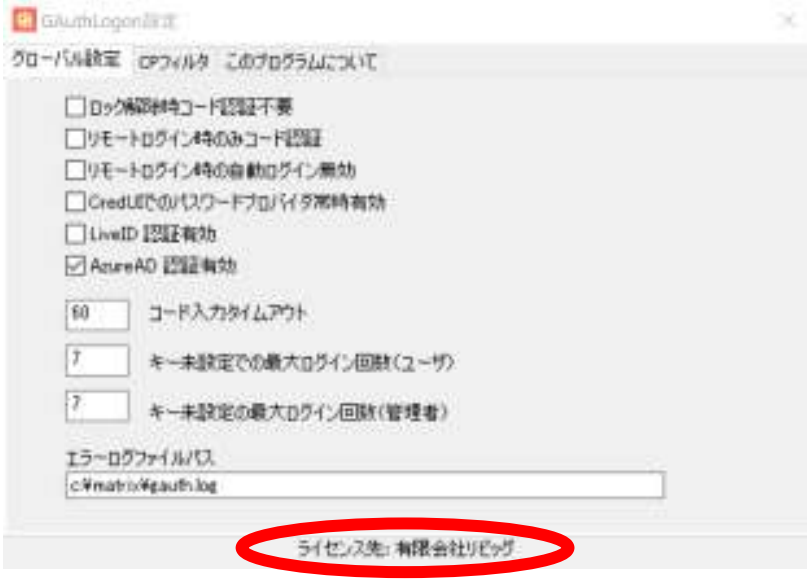
ライセンスファイルは license.txt という名前でダウンロードされます。

10.3 ライセンス発行サイト用アカウント作成

ライセンスを発行するには事前にアカウントを作成しなければなりません。

10.3.1 新規アカウント作成

ライセンス発行先名はプログラムで“ライセンス先”として表示されます。

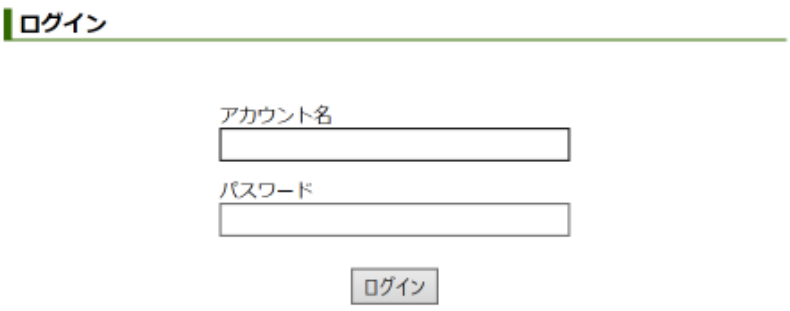


アカウントが作成されると設定メールアドレスにアカウントを有効化するリンクが含まれるメールが送付されます。リンクを開くと、アカウントにログインできるようになります。

テストアカウントのチェックを付けてアカウントを作成すると、無償のクライアントライセンスが３つ、サーバライセンスが１つ付与されます。

10.3.2 ログイン

アカウントを作成し、アカウント有効化後、ログインできます。



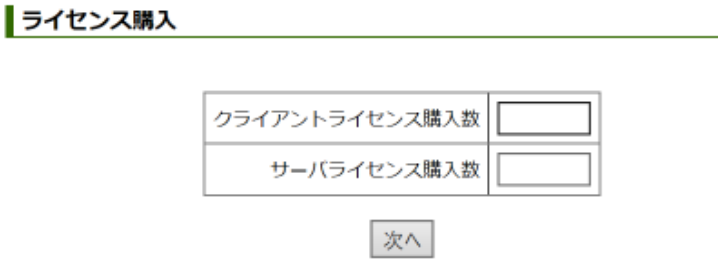
10.3.3 ライセンス一覧

ログインすると、購入ライセンスと発行ライセンスの一覧ページが表示します。一覧の見方はヘルプページをご覧ください。

テストアカウントでは、自動で３つのクライアントライセンス、１つのサーバライセンスが購入済みになります。すぐにライセンス発行ページでライセンスを発行できます。

10.3.4 ライセンス購入

テストアカウントではライセンスは購入できません。正規アカウントに移行してください。正規アカウントでは、“ライセンス購入”ページを選択できます。



購入するクライアント/サーバライセンス数を入力してください。[次へ] ボタンで確認ページが表示されます。

[Paypal Check Out]をクリックすると Paypal サイトに移動します。Paypal アカウントにログインして決済方法を確認してください。

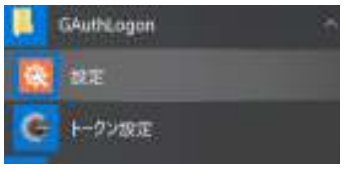
確認後、弊社サイトの最終確認ページに移動します。[支払実行]ボタンで支払いが完了し、アカウントに購入したライセンスが追加されます。ライセンス一覧でご確認ください。また、指定メールアドレスにアカウント作成完了のメールが送付されます。

10.4 ダウンロードしたライセンスファイルの設置方法

ダウンロードしたライセンスファイルはインストールしなければなりません。手動では設置できません。"設定"プログラムでインストールします。

"設定"プログラムを起動してください。

1. スタートメニュの [GAuthLogon]-[設定]



2. %Program Files%¥RiBiG¥GAuthLogon¥config.exe 実行

プログラムが起動したら、ウィンドウ下部のライセンス先と表示されている部分をダブルクリックします。

ファイル選択ウィンドウが開きます。ダウンロードしたライセンスファイルを選択してください

正当なライセンスファイルが選択されると、ファイルが配置されライセンス先としてアカウント作成時に設定したライセンス先文字列が表示されます。

以降、起動時に評価版というウィンドウは表示されません。

ライセンスファイル場所

%ProgramFiles%¥RiBiG¥GAuthLogon¥License.txt

ダウンロードされるライセンスファイルと同名ですが、内容は異なります。

10.5 無効化可能ライセンスの認証

無効化可能ライセンスがインストールされていると、プログラム起動時、ライセンスサーバへの問い合わせが発生します。問い合わせは HTTPS プロトコールが使われます。

10.5.1 問い合わせ頻度

GAuthLogon のプログラムが起動時に常に問い合わせをすると、ライセンスサーバへのアクセスが頻繁に発生する可能性があります。問い合わせは数日間ごとに発生するようになっています。

```
発生              発生              発生
 +-----+-----+-----+----+-----+-----+-----+
 1     2     3     4    5     6     7     8
```

これに合わせて、ライセンスの無効化の日付は問い合わせが発生する日になるように調整されます。上の例で、２の日にライセンスを無効化すると、即座に無効化されるのではなく、無効化日は４の日に設定されます。無効化しても、２と３の日は、サーバへの問い合わせは発生しません。４の日にライセンスサーバへの問い合わせが発生するためです。

無効化したライセンス ID を指定して、別 PC のライセンスを発行するには、無効化日以降に行わなければなりません。２の日に無効にしたライセンスは４の日まで有効です。２，３の日に無効化したライセンス ID を指定して、別 PC のライセンスを発行することはできません。

10.5.2 HTTPS プロトコール

HTTPS プロトコールでライセンスサーバに問い合わせをします。HTTPS でライセンスサーバに接続できるようになっていなければなりません。通常のアプリとして動作する GAuthLogon プログラムは IE のプロキシー設定を使います。ログイン画面で動作する GAuthLogon 本体は、誰もログインしていない状態で起動します。IE のプロキシー設定を読み込むことはできません。

プロキシーサーバが設置されている場合、別途、WinHTTP のプロキシーサーバの設定を行ってください。**管理者プロンプト**を開き netsh winhttp コマンドで設定します。

利用可能なコマンドを表示

```
>netsh winhttp
```

表示されたコマンドを入力して実行すると、さらに利用方法が表示されます。

ログインユーザの IE 設定をインポート：

```
>netsh winhttp import proxy source=ie
```

手動設定例

>netsh winhttp set proxy proxy-server=”192.168.x.x” bypass-list="*.local"

プロキシーサーバが正しく設定されていないと、ライセンスサーバに接続できません。ユーザ認証後、コネクションタイムアウトするまで止まったような状態になります。

タイムアウトは GAuthLogon インストールフォルダ内の gauthlogon.ini ファイル [Remote License Auth] セクションで設定できます。

[Remote License Auth]
ResolveTimeout=10000
ConnectTimeout=10000 // 10 秒
SendTimeout=10000
ReceiveTimeout=10000

10.5.3 ライセンスサーバに接続できない場合

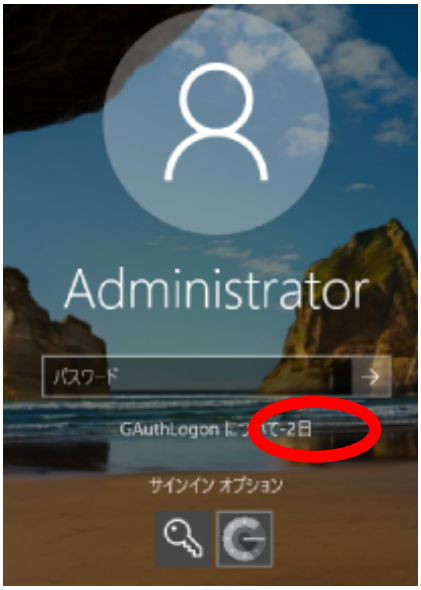
有効なライセンスファイルがインストールされていて、インターネットに接続していない、何かしらの原因でライセンスサーバに接続できないと、ログインすることができなくなります。ログインできるようにしてしまうと、インターネット接続を手動で無効することでライセンスサーバへの問い合わせを回避可能になってしまうためです。

ライセンスサーバへの問い合わせができないために GAuthLogon でログインできなくなったら、セーフモードで起動してください。セーフモードでは GAuthLogon はライセンスサーバへの問い合わせをしません。

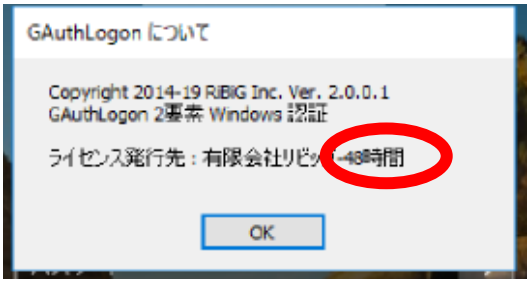
有効なライセンスファイルの名前を変更する、削除すると、評価版モードで起動します。評価モードではライセンスサーバへの問い合わせは発生しません。

10.6 ライセンスの期限確認

サーバライセンスの既定有効期限は 1 年です。設置したライセンスの有効期限が切れる約５日前から GAuthLogon ログイン画面の “GAuthLogon について“リンクの横に残り日数が表示されるようになります。



リンクのクリックで表示されるウィンドウにライセンス先の横に時間で残り有効期限を表示します。



10.7 ライセンス有効期限切れ

ライセンスの有効期限が切れると評価版モードで動作します。評価版モードでは製品版の設定は読み込めませんので、ユーザ/パスワード認証後、コード認証画面が表示されずにログインします。コード認証画面を表示させるには、次のいずれかを行ってください

1. 新規ライセンスファイルを取得してインストール
2. 有効期限の切れたライセンスファイルを削除、AddToken で評価版設定を行う

製品版設定を後日利用する可能性があれば、設定ファイルをバックアップしてください。

設定ファイル

%UserProfile%¥AppData¥Roaming¥RiBiG¥GAuthLogon¥gauthlogon.ini

評価版設定を行った後、新規ライセンスファイルを取得したら、バックアップファイルを設定ファイルとすることができます。

11. GAuthLogon 更新

コンソールログイン

GAuthLogon フォルダ(%ProgramFiles%¥RiBiG¥GAuthLogon) 内のファイルは上書き更新できます。必要に応じて、GAuthLogon ZIP パッケージ内の新しいファイルで GAuthLogon フォルダ内のファイルを上書きしてください。例えば GAuthLogon ZIP パッケージ内に新しい GAuthLogon.DLL があれば、そのファイルで GAuthLogon フォルダ内の GAuthLogon.DLL を上書きしてください。 これで GAuthLogon 本体が更新されます。

すべてのプログラムファイル(DLL/EXE) は上書き可能です。%ProgramFiles%フォルダへの書き込みには管理権限が必要です

リモートデスクトップログイン

リモートデスクトップのサーバ側では GAuthLogon が常にロードされた状態になっています。そのため、リモートデスクトップクライアントは、サーバ側の GAuthLogon フォルダ(%ProgramFiles%¥RiBiG¥GAuthLogon) 内の GAuthLogon.DLL を上書きすることはできません。
GAuthLogon をアンインストールしてからリモートコンピュータを再起動してください。起動後に更新 GAuthLogon をインストールしてください。アンインストール前に設定ファイルをバックアップ、インストール後にバックアップした設定ファイルをリストアしてください。

12. GAuthLogon のアンインストール

必要であれば、アンインストールする前にライセンスファイル、グローバル設定ファイル、アンインストールを行う管理者ユーザのプライベート設定ファイルをバックアップしてください。

コントロールパネルの「プログラム」ー「プログラムのアンインストール」を選択して、GAuthLogon をアンインストールしてください。

アンインストールが終わったら、必ず一度ログオフしてください。ログオフすることで、アンインストールが完了します。

付録１　コンピュータ時刻の自動設定

インターネットに接続しているコンピュータは、インターネット上のタイムサーバと時刻を自動同期させることで、常に正しい時刻が設定されます。

タスクバーの時間/曜日/日付が表示されている部分を右クリック。日付と時刻の調整を選択。

“時刻を自動的に設定する”をオンにしてください。

メインに参加しているコンピュータは、ドメインコントローラと時間が同期しますので、ドメインコントーラの時計が正確な時間になるように設定してください。