

SecureVisit

管理者マニュアル



Webシステムのセキュリティ向上の為に



飛天ジャパン株式会社

著作権と保証について

Copyright© Feitian Japan Co., Ltd. All Rights Reserved.

CD-ROMに含まれているプログラムおよびマニュアルなどの著作権は飛天ジャパン株式会社に帰属します。

本書のどの部分も、いかなる形態または手段（電子的または機械的）によっても、目的を問わず、飛天ジャパン株式会社の許可なしに複製することはできません。

- SecureVisit は飛天ジャパン株式会社の登録商標です。
- Microsoft, Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- Java およびすべての Java 関連の商標は、米国およびその他の国における米国 Oracle, Inc. 商標または登録商標です。
- Adobe, Adobe Acrobat は Adobe Systems Incorporated の商標です。
- UNIX は米国ならびに他の国における The Open Group の登録商標です。
- Linux は Linus Torvalds 氏の商標です。
- Red Hat は米国 Red Hat Software, Inc. の登録商標です。
- Ubuntu は Canonical 社の登録商標です。
- その他記載の会社名、製品名はそれぞれの会社の商標もしくは登録商標です。

飛天ジャパン株式会社では、本書中の情報の正確さに万全の努力を払っておりますが、情報の誤りがあってもいかなる種類の直接あるいは間接的な損失、損害にも責任を負いません。本書に記載されている仕様などは予告なしに変更されることがあります。本書に例として記載されている名称はすべて架空であり、事実とは関係ありません。

更新履歴

日付	リビジョン	変更内容
2008 年 5 月	1.0	新規作成
2010 年 11 月	1.1	管理者画面のログイン方法の変更 付加パラメータ機能の追加 レスキューパスワード機能の追加
2011 年 6 月	1.5	SecureVisit Freescale 機能追加
2021 年 4 月	1.6	・「属性管理」削除 ・サービス拒否（DoS）攻撃の内容を修正 ・3.4.2. マッピング登録 / 変更の「変換元

		PATH]、「変換先 URL」に注意事項を追加
2021 年 10 月	1.7	<ul style="list-style-type: none"> ・「2.4.1.2.Web 管理画面へのアクセス」に Microsoft Edge 及び Google Chrome の対応説明を追加 ・「2.4.2.1.Web 管理画面へのアクセス」に Microsoft Edge 及び Google Chrome の対応説明を追加 ・「2.6.3.SecureVisit クライアントのインストール」を追加 ・「3.5.1.ログの検索」の「ステータス」に注意事項を追加 ・「3.4.8.ポートフォワーディング登録/変更」の「アクセスグループ」を修正 ・「3.1.3.Web 管理画面からのログアウト」に注意事項を追加 ・「4.1.エラーメッセージ一覧」に項目を追加
2023 年 08 月	1.8	<ul style="list-style-type: none"> ・「3.7.2. SSL 証明書」の「SSL サーバー証明書」に「中間証明書も利用する場合」について追加
2024 年 04 月	1.9	<ul style="list-style-type: none"> ・Internet Explorer に関連する説明を削除 ・Ubuntu 関連の情報を追加 ・「3.4.2. マッピング登録/変更」にクロスドメインリダイレクト機能の説明を追加
2024 年 10 月	2.0	<ul style="list-style-type: none"> ・SSL 証明書画面に「TLS モード選択」及び「TLS1.3 許可する暗号化アルゴリズム」の項目を追加 ・一部内容の改善

- 目次 -

はじめに.....	1
本マニュアルの構成について	1
マニュアルで使用している用語	1
第 1 章 システム概要.....	3
1.1. SecureVisit Web 認証システムとは.....	4
1.2. チャレンジ&レスポンス認証	6
1.3. ワンタイムパスワード認証	7
1.4. アクセスコントロール	8
第 2 章 認証システムの導入.....	9
2.1. 認証システム導入の流れ.....	10
2.2. 認証システム導入のプランニング	11
2.2.1. リバースプロキシ	11
2.2.2. USB トークンによる認証.....	11
2.2.3. PIN による USB トークンの保護.....	11
2.2.4. 認証後のアクセスコントロール.....	12
2.2.5. タイムアウト	12
2.2.6. レスキューパスワード.....	13
2.3. 認証システム導入にあたっての検討事項.....	14
2.3.1. 検討すべき事項	14
2.3.2. 検討事項及び設定方法のまとめ.....	15
2.4. 管理者による Web 管理画面の利用方法.....	17
2.4.1. 管理者用証明書をブラウザへインポートする利用方法	17
2.4.2. 管理者用 USB トークン の利用方法	22
2.5. 認証システム導入のサンプル	25
2.6. クライアント PC の利用方法.....	33
2.6.1. クライアント PC システム要件	33
2.6.2. SecureVisit クライアントのインストール.....	33
2.6.3. クライアント PC の認証	34
2.7. USB トークン一括登録ツール.....	36
2.7.1. トークン一括登録ツール概要.....	36

2.7.2.	トークン一括登録ツール利用環境	36
2.7.3.	トークン一括登録ツールのインストール	36
2.7.4.	ユーザーリスト CSV ファイル	37
2.7.5.	トークン一括登録ツールによる CSV ファイルの作成	38
2.7.6.	トークン一括登録ツールの終了	43
第 3 章	運用管理	44
3.1.	Web 管理画面概要	45
3.1.1.	Web 管理画面の機能	45
3.1.2.	Web 管理画面のヘルプ機能	46
3.1.3.	Web 管理画面からのログアウト	46
3.2.	ユーザー管理	47
3.2.1.	ユーザー一覧	47
3.2.2.	ユーザーの削除	48
3.2.3.	ユーザー登録/変更	49
3.2.4.	インポート	51
3.3.	USB トークン管理	51
3.3.1.	USB トークン一覧	52
3.3.2.	USB トークンの削除	53
3.3.3.	USB トークン登録/変更	53
3.3.4.	インポート	55
3.4.	アクセス権限設定	56
3.4.1.	マッピング一覧	56
3.4.2.	マッピング登録/変更	57
3.4.3.	マッピングの適用	59
3.4.4.	付加パラメータ	61
3.4.5.	バックエンドプール	64
3.4.6.	ポートフォワーディング	65
3.4.7.	ポートフォワーディング一覧	66
3.4.8.	ポートフォワーディング登録/変更	67
3.4.9.	アクセスグループ一覧	67
3.4.10.	アクセスグループ登録/変更	68
3.5.	ログ管理	69
3.5.1.	ログの検索	70
3.5.2.	ログインしていないユーザーの検索	71
3.5.3.	特定ファイルを参照していないユーザーの検索	71
3.5.4.	管理操作ログ	71
3.5.5.	ログの保存	73

3.6.	認証 DB・設定ファイル	75
3.6.1.	認証 DB・設定ファイルのバックアップ管理	75
3.7.	サーバー設定	77
3.7.1.	サーバー設定	77
3.7.2.	SSL 証明書	79
3.7.3.	IP フィルタ	81
3.7.4.	ライセンス	83
3.7.5.	サーバーの再起動	83
第 4 章	トラブルシューティング	84
4.1.	エラーメッセージ一覧	84
4.2.	最も頻繁に起こる問題およびその解決方法	88
4.2.1.	特定のクライアントから認証が成功できない	88
4.2.2.	保護された Web サイトの一部のページにアクセスできない	88
4.2.3.	認証画面が繰り返し再表示される	88
4.2.4.	SSL 証明書を設定したら、サーバーの再起動にて、“停止中”となる	88

はじめに

このマニュアルは、SecureVisit Web 認証システムを導入する企業や組織のシステム管理者、または SecureVisit Web 認証システムを対象に、SecureVisit Web 認証システムの計画、導入、設定、および操作について説明します。

本マニュアルの構成について

このマニュアルでは、次の内容について説明しています。

❖ システム概要

この部分は SecureVisit Web 認証システムのアーキテクチャ、概念、機能の概要などについて説明します。

❖ 認証システムの導入

SecureVisit Web 認証システムをインストールする前に、お客様のニーズに合った導入方法や設定など、導入計画を策定します。この部分では、導入のプランニング、検討事項、認証システム導入のサンプル、トークン一括登録ツール、クライアント PC の利用方法などを説明します。

❖ 運用管理

SecureVisit Web 認証システムには、Web 経由の管理画面と管理者用ツールが用意されています。この部分では、これらの Web 管理画面とツールの利用、操作方法について説明します。

❖ トラブルシューティング

この部分では、SecureVisit Web 認証システムで発生する可能性がある問題や、その対処方法について詳細に説明します。

マニュアルで使用している用語

このマニュアルで使用している用語：

❖ USB トークン

飛天ジャパン社製ドライバレス USB トークン「ePass1000ND」です。利用者はこの USB トークンを利用して認証を行います。

❖ Web 管理画面

SecureVisit Web 認証システムの Web 管理画面です。Edge/Chrome からアクセスすることで様々な設定を行うことができます。

❖ 管理者用証明書

管理者が SecureVisit Web 管理画面へログインするための電子証明書のことです。pfx フォーマットのファイル（拡張子は.pfx）で提供されます。SecureVisit Web 管理画面へログインするには事前に管理者用証明書をブラウザにインポートする必要があります。

❖ チャレンジ&レスポンス認証

本システムが採用している認証方式です。USB トークンと認証サーバー間でセキュアな認証を行います。

❖ ユーザーリスト CSV

SecureVisit Web 認証システムに登録するユーザーの一覧を CSV 形式で作成したファイルです。

❖ ユーザーデータ CSV

トークン一括登録ツールを利用して作成するユーザー一覧の CSV、または Web 管理画面からエクスポートしたユーザー一覧の CSV です。ユーザーリストとは異なり、USB トークンとユーザーの関連付け情報が追記されています。

❖ トークンデータ CSV

トークン一括登録ツールを利用して作成する USB トークン一覧の CSV、または Web 管理画面からエクスポートした USB トークン一覧の CSV です。トークンの HID（ハードウェア ID）及び認証時に必要なキー情報が記載されています。

❖ 「導入チェックリスト」

SecureVisit Web 認証システムをスムーズに導入するため、事前に認証サーバーの基本設定項目について調査し、決定するためのチェックシートです。

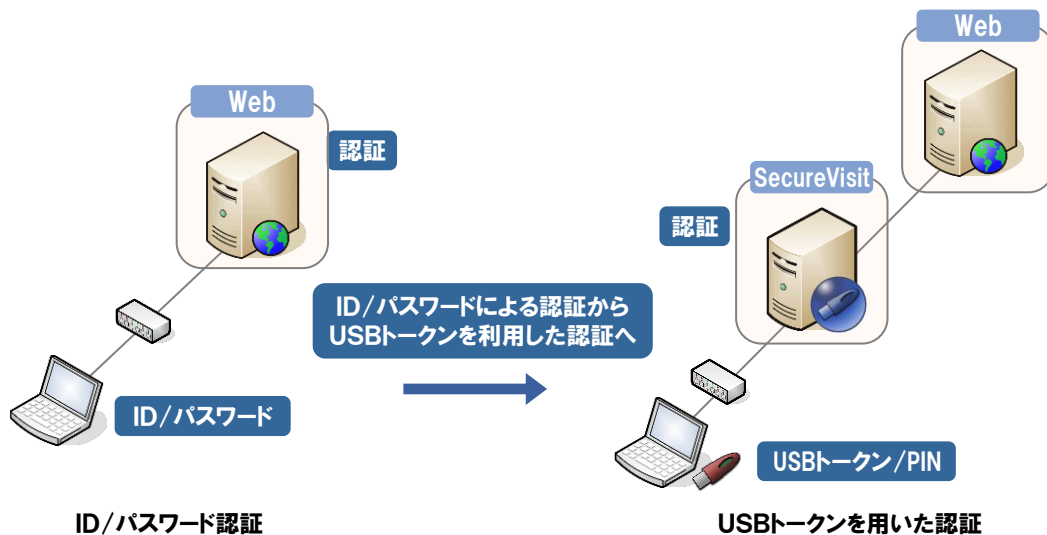
第1章 システム概要

本章では以下のトピックについて説明します。

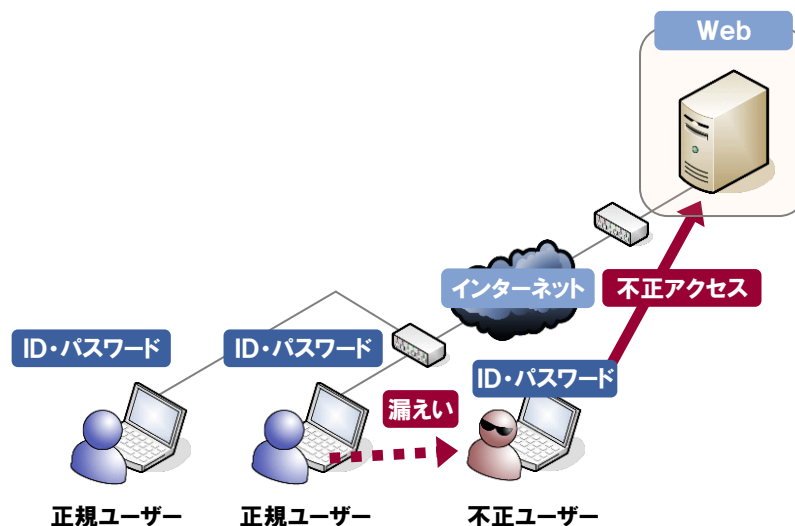
- ❖ SecureVisit Web 認証システム概要
- ❖ チャレンジ&レスポンス認証
- ❖ ワンタイムパスワード認証
- ❖ アクセスコントロール

1.1. SecureVisit Web 認証システムとは

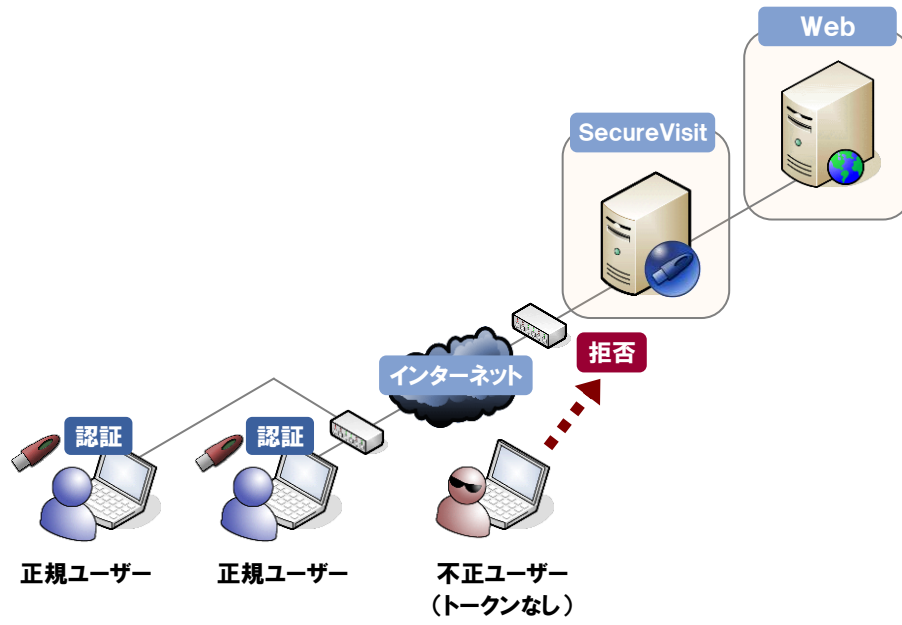
SecureVisit Web 認証システムは、飛天ジャパン社製 USB トークン ePass1000ND を利用したチャレンジ & レスポンス認証およびリバースプロキシ機能を搭載する Web 認証システムです。SecureVisit Web 認証システムを利用することで、既存の Web 環境を変更せずに、USB トークンによる認証を付加します。



通常の ID/パスワードのみの認証では、ID/パスワードなどの認証情報が漏えいしてしまうと第三者に簡単に成り済まされてしまいます。不正ユーザーが ID・パスワードを入手した場合、不正アクセスにより情報漏えいが発生する恐れがあります。



SecureVisit Web 認証システムを導入した場合は、ID/パスワードの認証に加え物理的な USB トークンによる認証を行うので、ID/パスワードが漏えいしてもなり済みを防ぐことができます。



1.2. チャレンジ&レスポンス認証

本認証システムで採用しているチャレンジ&レスポンス認証は、認証サーバーから送られてくるデータ（チャレンジ）をもとにクライアントが持っているシークレットを組み合わせで演算し、ハッシュ値を認証サーバーに「レスポンス」として返すことにより認証を行う方式です。

この方式では、実際のパスワードをネットワーク上に流す必要がない点と認証サーバーから送られてくるチャレンジの内容が毎回異なるので、チャレンジやレスポンスを盗聴されてもセキュリティリスクが非常に少ないのが特長です。

❖ チャレンジ

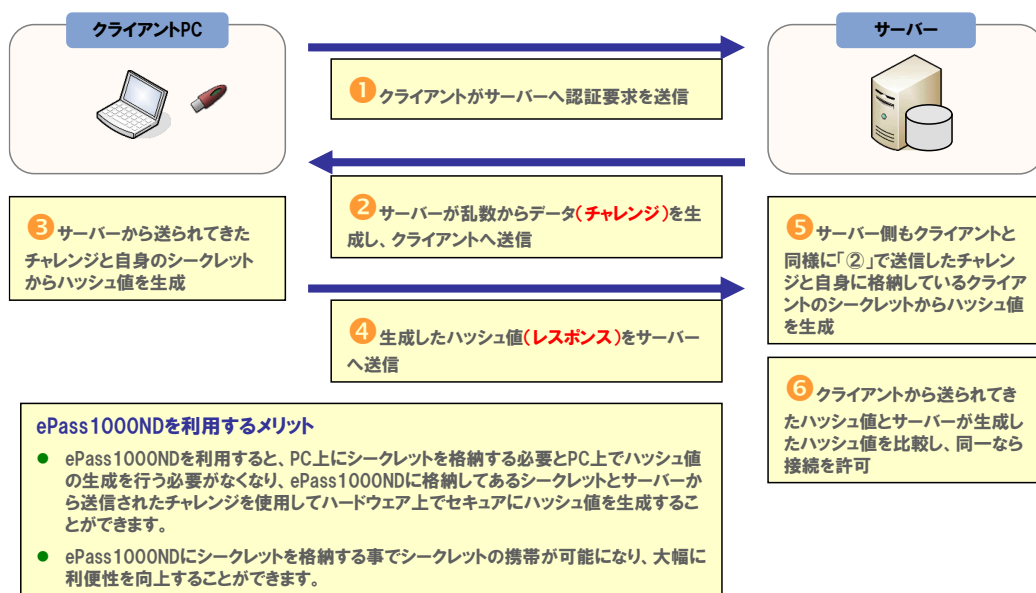
認証サーバーが乱数から作り出したデータで認証時にクライアントへ送信します。

❖ レスポンス

クライアントがシークレットとチャレンジを組み合わせ、ハッシュ値としてサーバーへ返すデータです。

❖ ハッシュ値

ハッシュ関数により生成される値で、計算結果から元のデータへ戻すことができない不可逆な値です。

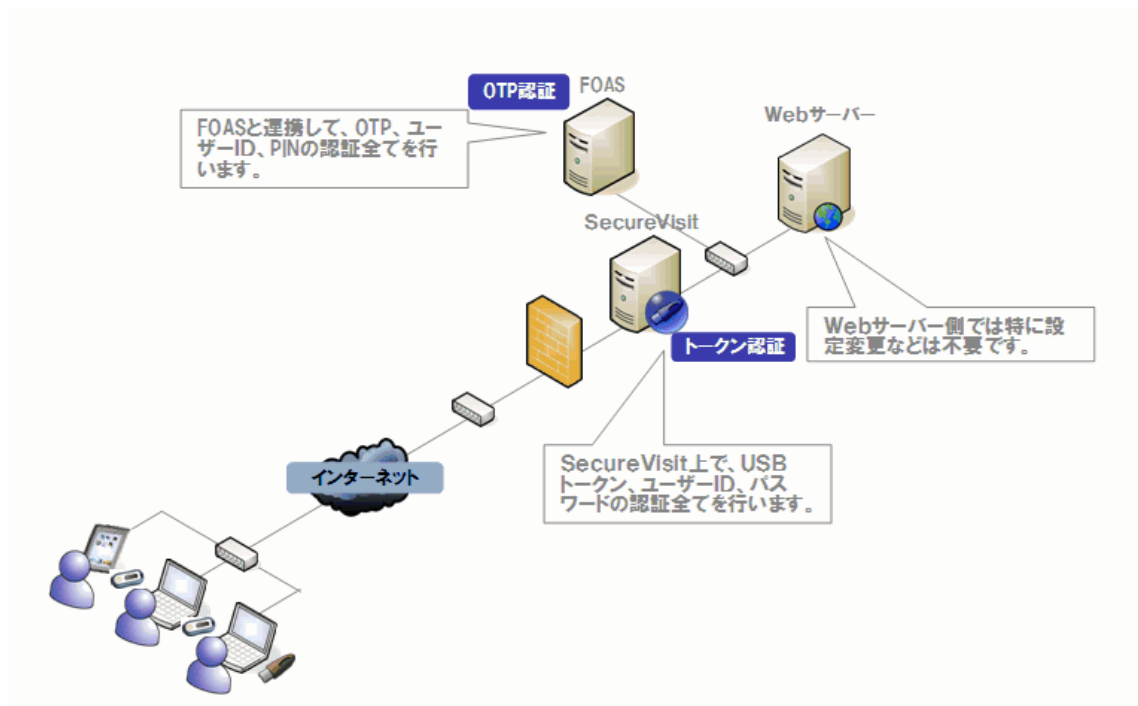


1.3. ワンタイムパスワード認証

本認証システムには、FOAS（FEITIAN OTP Authentication System）のエージェントを含みますので、FOAS と連携して、ワンタイムパスワード（OTP）方式でも認証できます。チャレンジ&レスポンス認証と一緒に使えます。

ワンタイムパスワードは、一回限りの使い捨てパスワードを生成し、ユーザーを識別することにより、認証を行う方式です。

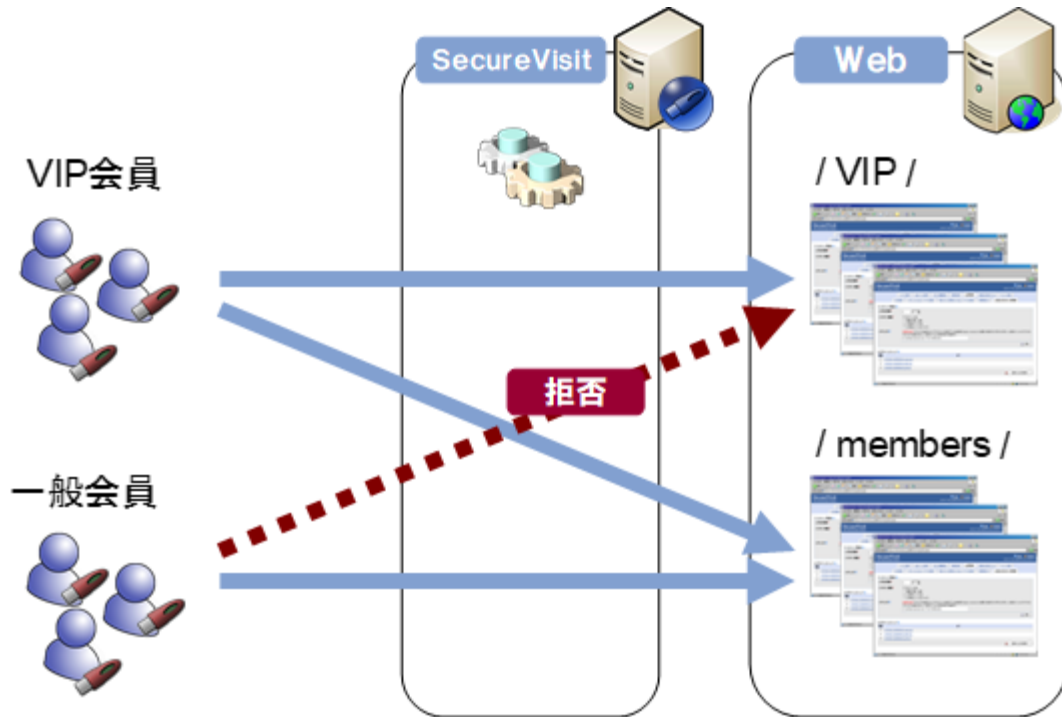
この方式では、トークンについているボタンを押すと、一回限りの使い捨てパスワードが表示され、覚える必要がありません。PC に接続しないので、エンドユーザーはドライバやアプリケーションのインストールが不要となり、様々なクライアントに対応できるのが特長です。



※OTP サーバーを別途構築必要があります、FOAS のマニュアルをご参照ください。

1.4. アクセスコントロール

認証サーバーでは、マッピングによるアクセスコントロールを行うことができます。アクセスコントロールは、ユーザーをグループに所属させ、グループに対してアクセスの許可・拒否を行います。アクセスコントロールを行うことで必要なユーザーにのみ該当コンテンツを表示させることができます。



例えば、上記の図のようなアクセスコントロールを行うには、SecureVisit 認証サーバーで以下のようにマッピングを定義します。

変換元 PATH	アクセスグループ	変換先 URL
/VIP/	GroupVIP(VIP 会 員 グ ル ー プ) & GroupMembers(一般会員グループ)	http://Web/VIP/
/members/	GroupMembers(一般会員グループ)	http://Web/members/

第2章 認証システムの導入

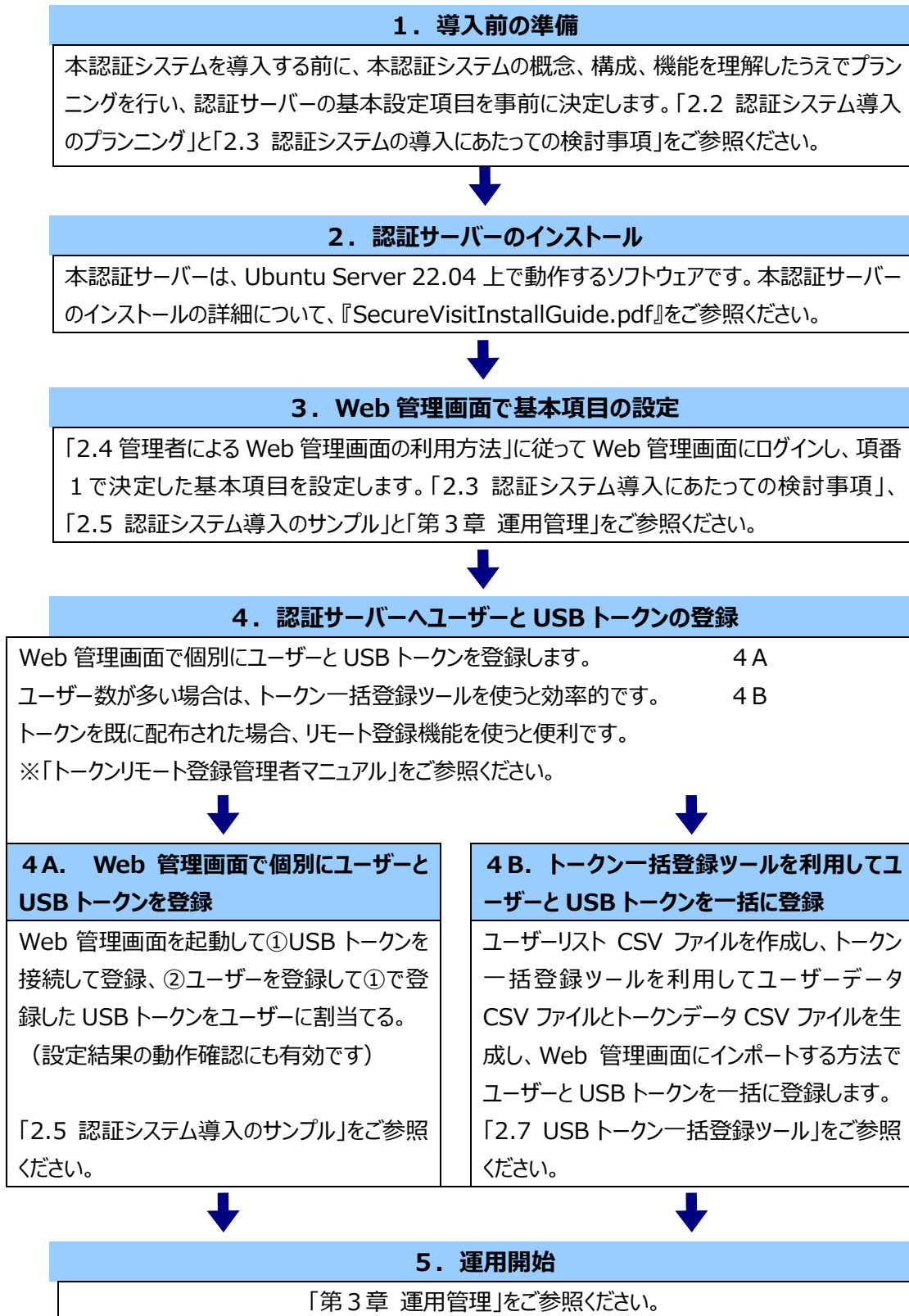
本章では認証システム導入の概要を説明します。

本章では以下のトピックについて説明します。

- ❖ 認証システム導入の流れ
- ❖ 認証システム導入のプランニング
- ❖ 認証システム導入にあたっての検討事項
- ❖ 管理者による Web 管理画面の利用方法
- ❖ 認証システム導入のサンプル
- ❖ クライアント PC の利用方法
- ❖ USB トークン一括登録ツール

2.1. 認証システム導入の流れ

認証システム導入は以下手順にて実施します。



2.2. 認証システム導入のプランニング

SecureVisit Web 認証システムを既存の Web 環境に導入する場合でも、完全に新しい環境として構築する場合でも、入念な準備が必要です。SecureVisit Web 認証システムには、さまざまな機能や設定があります。ここでは、導入段階で理解する必要のある SecureVisit Web 認証システムの代表的な機能や設定について説明していきます。

2.2.1. リバースプロキシ

SecureVisit Web 認証システムは、既存の Web アプリケーションやシステムを変えずに、USB トークンによる認証を追加することを目標として設計したシステムです。SecureVisit 認証サーバーは、保護する Web サーバーの前に置かれ、Web サーバーの代りに利用者からのアクセスを受け、認証したうえで保護する Web サーバーにそのアクセスをパスします。結果的に保護する Web サーバーは、SecureVisit 認証サーバーからのアクセスのみを受けようになります。SecureVisit Web 認証システムは HTTP/HTTPS/WebDAV プロトコルをサポートします。

2.2.2. USB トークンによる認証

SecureVisit Web 認証システムは、物理的な USB トークンによる認証を採用しています。

USB トークンと認証サーバーの間に、チャレンジ&レスポンス認証方式を採用しています。USB トークン認証は、自動的に行うので、利用者から見ると認証は「透過的」に実施されます。

USB トークンを利用者に配布する前に、USB トークンを認証サーバーに登録することが必要です。

SecureVisit Web 認証システムでは、USB トークン認証以外に、パスワード認証を追加することもできます。

2.2.3. PIN による USB トークンの保護

USB トークンに PIN（暗証番号）を指定することができます。USB トークンで認証を行う際に、該当する USB トークンの PIN を入力させることができます。USB トークンの PIN を知らないと USB トークンを持っていても認証できません。PIN は USB トークンを紛失した場合の不正利用を防ぎます。

USB トークンで認証を行う際に、PIN を入力させるか否かの指定は、USB トークンを認証サーバーに登録する時に行います。この指定は USB トークン単位となります。

注：トークン一括登録ツールでも、PIN の設定を行うことができます。詳細は「2.7 USB トークン一括登録ツール」をご参照ください。

2.2.4. 認証後のアクセスコントロール

SecureVisit 認証サーバーには、「ユーザー」、「トークン」、「アクセスグループ」という概念があります。

❖ 「ユーザー」:

「ユーザー」とは、SecureVisit Web 認証システムにおける利用者のことです。「ユーザー」は「ユーザーID」で識別します。

❖ 「トークン」:

「トークン」とは、USB トークンのことです。「ユーザー」に「トークン」を割り当てます。すなわち、特定の利用者が特定の USB トークンを持つことになります。

❖ 「アクセスグループ」:

「アクセスグループ」は、アクセス権限を制御するための「ユーザー」グループのことです。「ユーザー」は、最低一つの「アクセスグループ」に所属します。

保護する Web サーバーのコンテンツへのアクセスは、「アクセスグループ」単位でコントロールされます。コンテンツは、ディレクトリ単位で指定できますが、単一のファイル単位までも指定することができます。但し、管理が複雑になりますので、特殊な場合を除き、ディレクトリ単位での指定をお勧めします。認証サーバーに送信された URL が、保護する Web サーバーのどの URL と結びつけるかの指定を「マッピング」と呼びます。

利用者は、認証に成功した後、認証サーバーでは、その利用者の「ユーザーID」を確定できます。認証サーバーは、利用者がアクセスしようとするコンテンツに、該当する「ユーザー」の所属する「アクセスグループ」が許可されているかを「マッピング」の定義に従ってチェックします。

「ユーザー」、「トークン」、「アクセスグループ」には、有効期間を設定できます。「ユーザー」、「トークン」には、有効/無効を指定することもできます。

2.2.5. タイムアウト

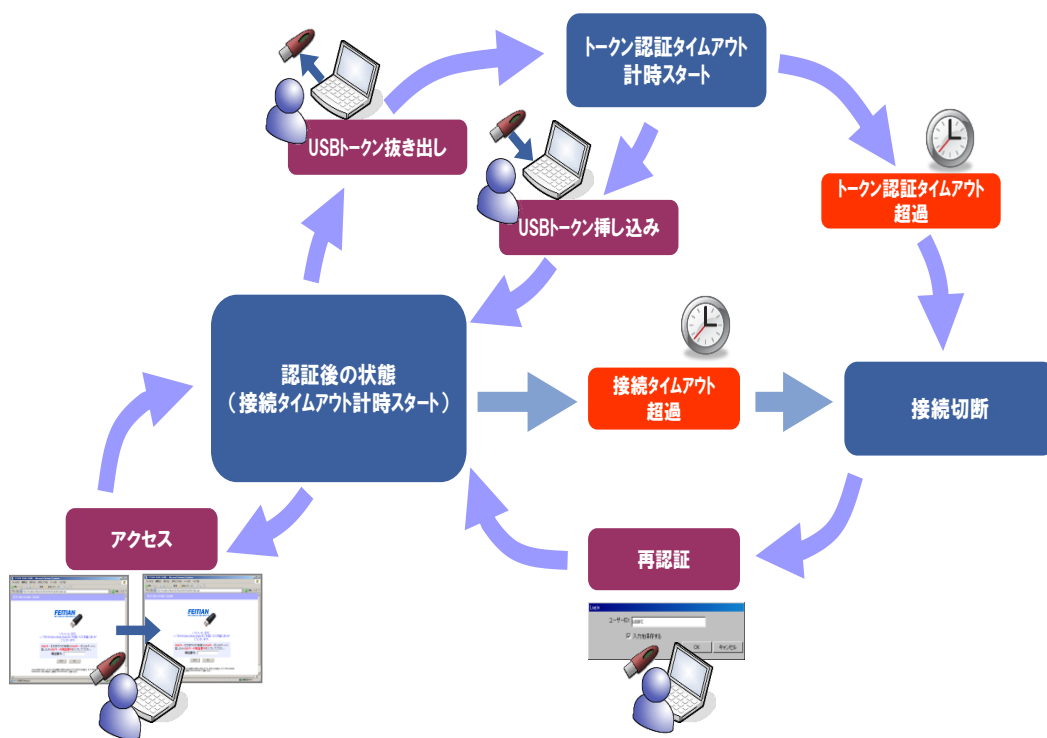
一度、認証後「ユーザー」の接続が切断される条件は、下記の通りになります。

❖ トークン認証タイムアウト:

認証後トークンの接続が外れ、このタイムアウト時間が経過し、他の保護されたページに移しようとする、アクセスできなくなります。

❖ 接続タイムアウト:

セッションタイムアウトとも呼びます。USB トークンの接続の有無に関わらず、再度認証を行います。



管理者は、この 2 つのタイムアウト値を利用することで、ページ閲覧時の定期的な USB トークン接続確認と、USB トークンを接続したまま離席したユーザーのセッション切断などを行うことができます。

2.2.6. レスキューパスワード

ユーザーが USB トークンを紛失した場合のアクセス対策です。管理者に連絡して、該当ユーザーのレスキューパスワードを設定すれば、ユーザーはレスキューパスワードで認証サーバーに一時的にアクセスできます。

2.3. 認証システム導入にあたっての検討事項

SecureVisit Web 認証システムの導入と設定を行うために、事前に検討すべき事項が幾つかあります。

ライセンスを購入する前にも決定しなければならない購入前決定事項と、購入後でも管理者が Web 管理画面で変更できる認証サーバーの基本設定事項があります。

注：「導入チェックリスト」というチェックシートが用意されています。このチェックシートを利用して検討することをお勧めします。

2.3.1. 検討すべき事項

❖ ユーザーの最大数はどのくらいですか？利用する USB トークン数はどのくらいですか？

SecureVisit Web 認証システムを導入する前に、利用者の最大数と利用する USB トークン数を明確にしなければなりません。利用する USB トークンは、1 ユーザーに 1 つの USB トークンしか割り当てることができません。

ユーザーと USB トークンの最大数は、ライセンスファイルに記載されます。これらの数を超えた運用は保証範囲外となります。ライセンスを再発行しない限り、ユーザーと USB トークンの最大数を変更することはできません。

注：OTP トークンに関しては、FOAS の管理者マニュアルをご参照ください。

❖ Web サーバーの最大同時接続数はどのくらいですか？

大量のユーザーが同時にアクセスする Web サイトには、サーバーの負荷分散 & 冗長構成が必要です。SecureVisit Web 認証システムは、複数のサーバー構成が可能です。アクセス数が増えてきたら、新たに認証サーバーを追加することができます。

❖ 認証サーバーの DNS 名は決定しましたか？

SecureVisit Web 認証システムの Web 管理画面は、SSL サーバー証明書で保護されます。SecureVisit Web 認証システムは、出荷時に自己署名の Web 管理画面用 SSL サーバー証明書が内蔵されますが、この SSL サーバー証明書にはサーバーの DNS 名が記載されません。

❖ アクセスグループは明確になっていますか？

アクセスグループは、アクセス権限を制御するためのユーザーグループです。ユーザーは必ずアクセスグループに所属します。

SecureVisit Web 認証システムでは、コンテンツへのアクセス制限はユーザー単位ではなく、アクセスグループ単位でコントロールされます。

導入後に Web 管理画面で設定、変更することはできますが、ユーザー数が多い場合は、ユーザーの初期登録時にトークン一括登録ツールを使うと便利です。

❖ **保護する Web サーバーのコンテンツはディレクトリ単位でアクセス制限を掛けられる構成になっていますか？**

SecureVisit Web 認証システムでは、保護する Web サーバーのコンテンツはディレクトリ単位でアクセス制限を掛けることができます。

❖ **PIN を利用しますか？**

PIN は USB トークンの暗証番号のようなものです。PIN を利用する場合、利用者は認証する際に USB トークンの PIN を入力しなければなりません。PIN は USB トークンを紛失した場合の不正利用を防ぎます。PIN の利用要否指定は USB トークン単位となります。該当する USB トークンを登録する時に行います。この指定は USB トークンを再登録するまで変更することはできません。「2.7 USB トークン一括登録ツール」と「3.3.3 USB トークンの登録・変更」をご参照ください。

❖ **SSL を利用しますか？**

SecureVisit Web 認証システムは、通常の HTTP Web サーバーと、SSL サーバー証明書による SSL 通信（HTTPS）を利用している Web サーバーも保護できます。保護する Web サーバーは既に SSL サーバー証明書を利用していて、その SSL サーバー証明書を続けて利用したい場合は、SSL サーバー証明書を認証サーバーに移動する必要があります。

「3.7.2 SSL 証明書」をご参照ください。

2.3.2. 検討事項及び設定方法のまとめ

項目	作成・定義・設定方法	変更方法
登録可能ユーザー数	ライセンス購入時にライセンスファイルに記載されます。	ライセンスの追加購入
登録可能トークン数	ライセンス購入時にライセンスファイルに記載されます。	ライセンスの追加購入
負荷分散&冗長構成	ライセンス購入時にライセンスファイルに記載されます。	ライセンスの追加購入
認証サーバーの DNS 名	Web 管理画面へログインするための SSL サーバー証明書に記載されます。	認証サーバーの SSL サーバー証明書の再発行
PIN	Web 管理画面の「トークン登録/変更」で USB トークンを登録する時に設定できます。	PIN の変更は、Web 管理画面で USB トークンを一旦削除してから USB トークンを再度登録する時に

	USB トークン一括登録ツールでも設定できます。	再設定することになります。 ※PIN を再設定する際、8 桁以上の半角英数字を入力してください。
アクセスグループ	Web 管理画面の「アクセスグループ登録/変更」で新規登録できます。 Web 管理画面の「アクセスグループの一覧」で検索、削除できます。	Web 管理画面の「アクセスグループ登録/変更」で変更できます。
SSL	Web 管理画面の「SSL 証明書」で設定できます。	

2.4. 管理者による Web 管理画面の利用方法

SecureVisit Web 認証システムでは、ほとんどの管理作業を Web 管理画面から行うことができます。Web 管理画面へログインするには、管理者用証明書によるクライアント証明書認証を唯一の手段とします。

通常、管理者用証明書は pfx フォーマットのファイル（拡張子は.pfx）で提供されますが、管理者用 USB トークンに格納されて提供される場合もあります。いずれかの方法をご利用ください。

2.4.1. 管理者用証明書をブラウザへインポートする利用方法

2.4.1.1. 管理者用証明書をブラウザへインポート

pfx フォーマットの管理者用証明書ファイルを利用して SecureVisit Web 管理画面へログインするには、事前に管理者用証明書をブラウザにインポートする必要があります。

注：管理者用証明書は管理者用 USB トークンに格納されて提供される場合もあります。この場合は、管理者用証明書をブラウザにインポートする必要はありませんが、事前に USB トークンのドライバをインストールする必要があります。

1. 「SecureVisit ライセンスパッケージ CD」にある管理者用証明書ファイル（client.pfx）のいずれをクリックします。
2. 証明書のインポートウィザードが開始されるので「次へ」をクリックします。



3. デフォルト設定で、「次へ」をクリックします。パスワード入力画面で、パスワードを入力せずに「次へ」をクリックします（パスワードが必要な場合はパスワードを入力します）。デフォルト設定で、「次へ」をクリックします。ウィザード完了画面で「完了」をクリックします。

← 証明書のインポートウィザード

インポートする証明書ファイル

インポートするファイルを指定してください。

ファイル名(F):
C:\Users\hutoao\OneDrive\デスクトップ\client.pfx 参照(R)...

注意: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます:

- Personal Information Exchange- PKCS #12 (.PFX, P12)
- Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B)
- Microsoft シリアル化された証明書ストア (.SST)

次へ(N) キャンセル

← 証明書のインポートウィザード

秘密キーの保護

セキュリティを維持するために、秘密キーはパスワードで保護されています。

秘密キーのパスワードを入力してください。

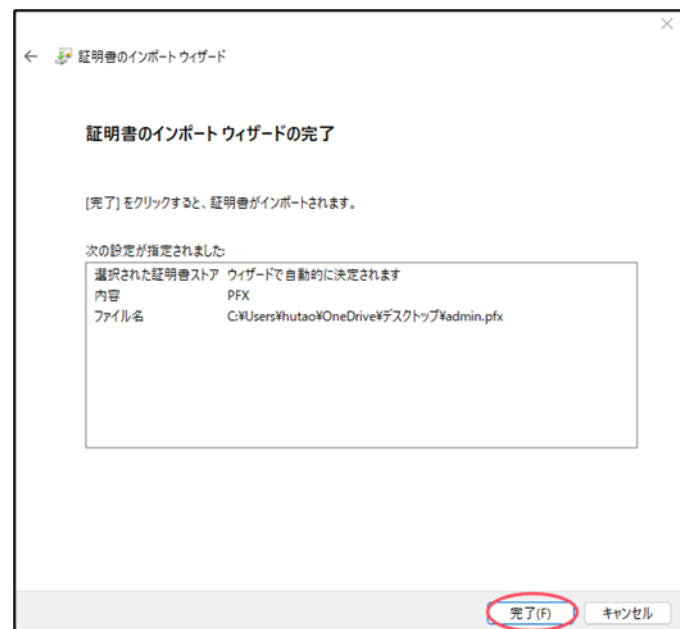
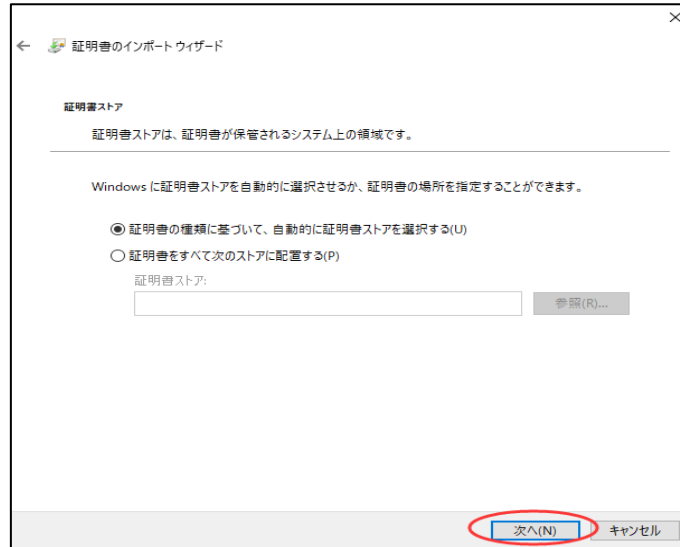
パスワード(P):
[パスワード入力欄]
☐ パスワードの表示(D)

インポート オプション(O):

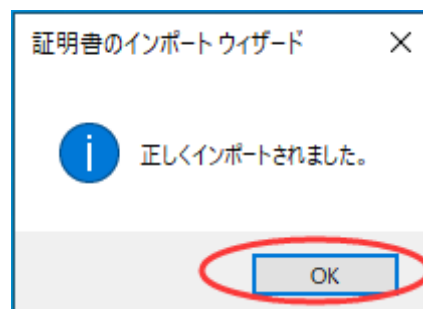
- ☐ 秘密キーの保護を強力にする(E)
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。
- ☐ このキーもエクスポート可能にする(M)
キーのバックアップやトランスポートを可能にします。
- ☐ 仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P)
- ☒ すべての拡張プロパティを含める(A)

次へ(N) キャンセル

※パスワードが必要な場合は、上記画面でパスワードを入力します。



4. インポートが正常に終了すると、以下の画面が表示されるので「OK」をクリックします。



2.4.1.2. Web 管理画面へのアクセス

1. Web 管理画面（通常はポート <https://> 認証サーバーDNS 名:8888/）へアクセスします。

注：例として、認証サーバーの DNS 名は www.ftsafe.co.jp の場合、管理画面の URL は <https://www.ftsafe.co.jp:8888/> となります。

下記画面が表示された場合、「詳細情報」をクリックし、「Web ページに移動する」を選択してください。



Microsoft Edge



Google Chrome

2. 「証明書の選択」画面が表示されます。「OK」をクリックします。



Microsoft Edge

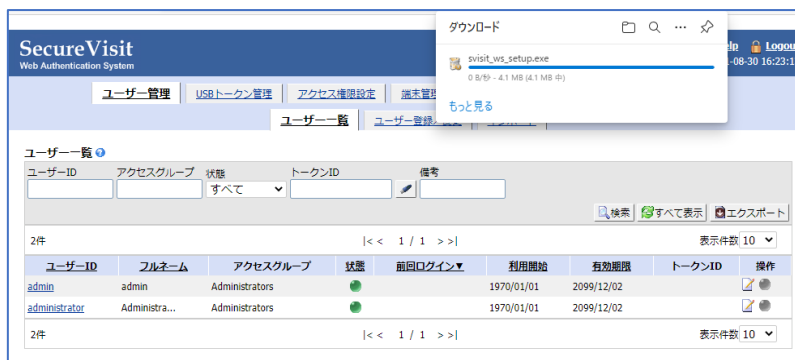


Google Chrome

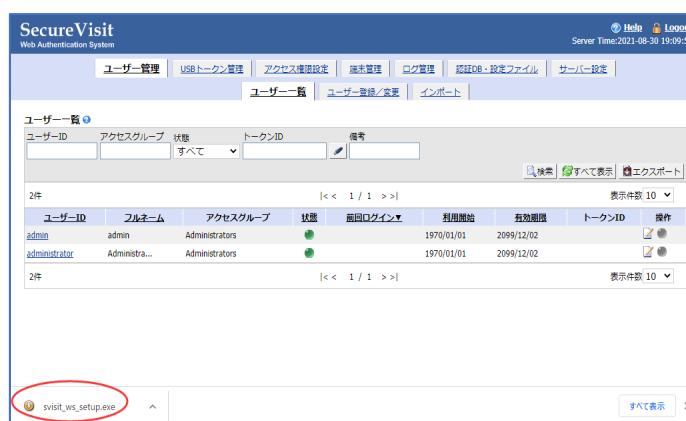
注：管理者 ID は Administrators アクセスグループに所属しているユーザーが管理者となります。（詳細は「アクセスグルー

一覧」を参照してください)

3. 認証が成功すると、管理画面が表示されます。
4. 初回アクセス時は、Microsoft Edge 及び Google Chrome を利用した場合、SecureVisit クライアントをダウンロードするメッセージが表示されます。



Microsoft Edge にて SecureVisit クライアントをダウンロードする場合



Google Chrome にて SecureVisit クライアントをダウンロードする場合

5. SecureVisit クライアントがインストールされた後、管理画面が下記のように表示されます。



2.4.2. 管理者用 USB トークン の利用方法

2.4.2.1. Web 管理画面へのアクセス

1. 管理者用 USB トークンを利用する場合は、管理者用 USB トークンを USB ポートに接続します。
2. 認証が正常に完了すると、管理画面が表示されます。Web 管理画面（通常はポート <https://認証サーバーDNS名:8888/>）へアクセスします。

注：例として、認証サーバーの DNS 名は www.ftsafe.co.jp の場合、管理画面の URL は <https://www.ftsafe.co.jp:8888/> となります。

下記画面が表示された場合、「詳細情報」をクリックし、「Web ページに移動する」を選択してください。



Microsoft Edge



Google Chrome

3. 「証明書の選択」画面が表示されます。「OK」をクリックします。

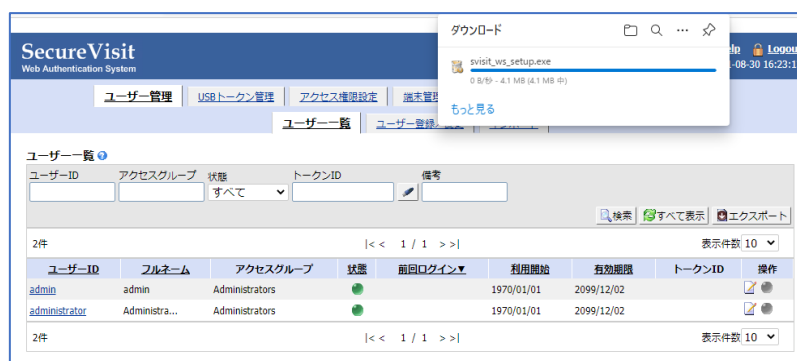


Microsoft Edge

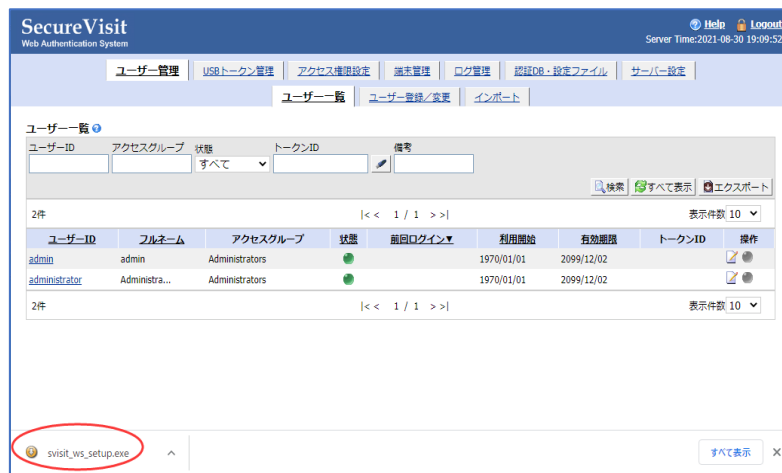


Google Chrome

4. 認証が正常に完了すると、管理画面が表示されます。
5. 初回アクセス時は、Microsoft Edge 及び Google Chrome を利用した場合、SecureVisit クライアントをダウンロードするメッセージが表示されます。
SecureVisit クライアントは自動的にダウンロードされるので、ダウンロード完了後に確認してください。

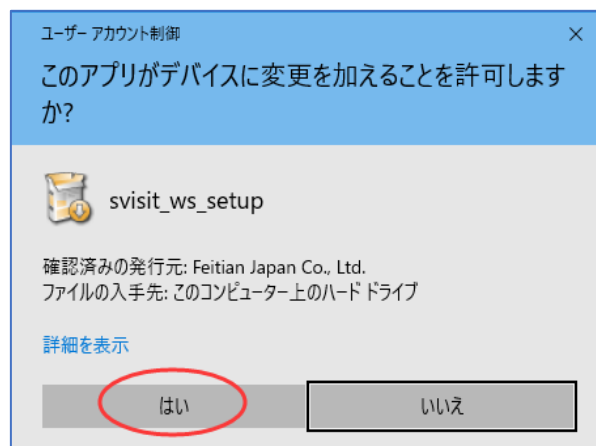


Microsoft Edge にて SecureVisit クライアントをダウンロードする場合



Google Chrome にて SecureVisit クライアントをダウンロードする場合

- SecureVisit クライアントをダウンロードすると、以下画面が表示されるので、「許可する」または「はい」をクリックします。



SecureVisit クライアントの場合

- SecureVisit クライアントがインストールされた後、管理画面が下記のように表示されます。



2.5. 認証システム導入のサンプル

SecureVisit 認証システムの導入をより理解いただくために、ここでは、飛天ジャパン株式会社の Web サイト <https://www.ftsafeco.jp> を保護したい Web サイトと仮定して SecureVisit 認証サーバーの導入を説明します。飛天ジャパン株式会社の Web サーバー www.ftsafeco.jp (IP:211.10.20.97) はバックエンド Web サーバーとなります。

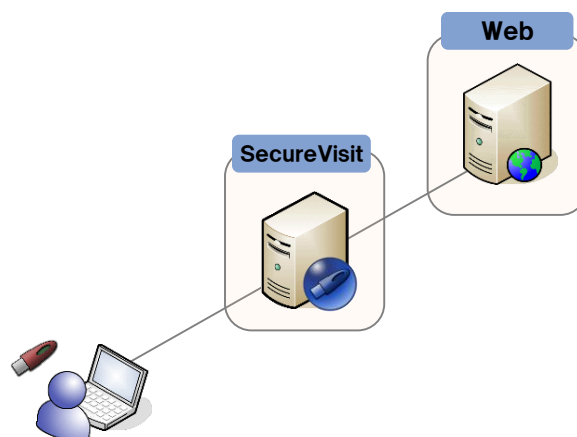
飛天ジャパン株式会社の Web サイトは以下のような構成となっています。

https://www.ftsafeco.jp	/	Web サイトのルート
	└ /support/	技術サポートコンテンツのディレクトリ
	└ /products/	製品情報コンテンツのディレクトリ
	└ /news/	会社ニュースコンテンツのディレクトリ
	└ /.....	その他コンテンツのディレクトリ

例として、以下のことを実現する要件と仮定します。

この Web サイトには、USB トークンを持っている一般会員しかアクセスできないようにします。さらに、技術サポートのコンテンツ (/support) へアクセスするには VIP 会員しかアクセスできないようにします。

この要件を実現するために、SecureVisit 認証サーバーを導入します。利用者のクライアント PC は SecureVisit 認証サーバー経由でバックエンド Web サーバーへアクセスするようにします。ここでは、SecureVisit 認証サーバーの IP アドレスを 192.168.129.176 と仮定します。利用者のクライアント PC の Hosts ファイルに「192.168.129.176 www.ftsafeco.jp」の 1 行を追加すれば、URL を変えずに (SecureVisit 認証サーバー導入前と同じく <https://www.ftsafeco.jp/>) にアクセスすると SecureVisit 認証サーバーにアクセスすることになります。



注：実際の導入では、利用者クライアント PC の Hosts ファイルを変更する代りに DNS サーバーの設定変更またはバックエンド Web サーバーの IP を変更することになります。また、バックエンド Web サーバーに SecureVisit 認証サーバーからのアクセスのみ受けるように設定します。

SecureVisit 認証サーバーの Web 管理画面にログインして、「サーバー設定」タブの「サーバー設定」画面にて以下のように設定します。

IP アドレス	192.168.129.176
ポート	443
デフォルトドメイン名	www.ftsafe.co.jp

SecureVisit
Web Authentication System

Help Logout
Server Time: 2021-09-08 16:10:35

ユーザー管理 USBトークン管理 アクセス権限設定 端末管理 ログ管理 認証DB・設定ファイル **サーバー設定**

サーバー設定 SSL証明書 IPフィルタ ライセンス サーバーの再起動

サーバー設定

IPアドレス* サーバーのIPアドレスです。
192.168.129.176

ポート* サーバーの待ち受けポートです。一般的にHTTPの場合は「80」、HTTPSの場合は「443」です。
443

デフォルトドメイン名* サーバーのドメイン名です。(例: example.com)
www.ftsafe.co.jp

トークン認証タイムアウト* USBトークンの再認証までの時間です。認証した後にトークン差込んでいない状態で再認証を行うまでの秒数を設定します。
0 秒

接続タイムアウト* ユーザー認証状態の再確認までの時間です。再確認までの分数を設定します。
10 分

ユーザーIDの入力 ユーザーIDを「入力させる」場合は、入力させたユーザーIDとUSBトークンの割り当て関係のチェックを行います。「入力させない」場合は、ユーザーにユーザーIDを入力させない、USBトークンからユーザーIDを判別します。「前回の入力を入力を記憶できるようにする」場合は、前回入力したユーザーIDの保存と自動入力ができるようになります。(デフォルト: 入力させる)
入力させる ☐ 前回の入力を入力を記憶できるようにする

パスワード認証 パスワード認証の設定です。「する」にした場合は、ユーザーにパスワードを入力させ、このサーバーで認証を行います。「しない」した場合は、このサーバーでパスワードのチェックを行いません。(デフォルト: しない)
しない

レスキューパスワードの使用 「する」にした場合は、レスキューパスワードで認証できるようになります。(デフォルト: しない)
しない
レスキューパスワード入力のリトライ回数です。
10 回

端末限定 「端末限定」にした場合は、登録された端末でどのユーザーでも認証できるようになります。「端末とユーザー限定」にした場合は、ユーザー事に制限された端末で認証できるようになります。(デフォルト: しない)
しない ☐ 端末認証を十分条件とする

OTP認証 OTP認証機能の有効/無効を選択します。(デフォルト: 無効)
無効

サービス拒否 (DoS) 攻撃* サービス拒否 (DoS)攻撃の検知と遮断に関する設定です。(デフォルト: 毎1秒間同一IPから166回以上のアクセスが発生しますとDoS攻撃として検知し、当該IPから166回以上のアクセスを遮断する)
1秒間同一IPから 10000 回以上のアクセスが発生しますとDoS攻撃として検知し、当該IPから設定した回数以上のアクセスを遮断する

クライアントIPの取得 ☐ HTTPヘッダからクライアントIPを取得する

(注意: 変更を有効にするためにサーバーの再起動が必要です。)

更新

「アクセス権限設定」の「アクセスグループ登録/変更」画面にて、以下の2つのユーザーグループを作成します。

GroupMember	一般会員
GroupVIP	VIP 会員

SecureVisit
Web Authentication System

Help Logout
Server Time: 2021-04-12 19:10:21

ユーザー管理 USBトークン管理 **アクセス権限設定** 端末管理 ログ管理 認証DB・設定ファイル サーバー設定

マッピング一覧 マッピング登録/変更 ポートフォワーディング一覧 ポートフォワーディング登録/変更 **アクセスグループ一覧** アクセスグループ登録/変更

アクセスグループ一覧

アクセスグループ名 説明
検索 すべて表示

3件 |< < 1 / 1 > >| 表示件数 10

アクセスグループ名▲	説明	操作
Administrators		
GroupMember	一般会員	
GroupVIP	VIP会員	

3件 |< < 1 / 1 > >| 表示件数 10

「アクセス権限設定」の「マッピング登録／変更」画面にてマッピングを新規登録します。

変換元 PATH	/support/
変換元ドメイン名	www.ftsafeco.jp
変換先 URL	http://211.10.20.97/support/
許可されるアクセスグループ	GroupVIP

SecureVisit Web Authentication System

Help Logout Server Time 2021-09-07 20:14:41

ユーザー管理 USBトークン管理 **アクセス権限設定** 課金管理 ログ管理 認証DB・設定ファイル サーバ設定

マッピング一覧 **マッピング登録／変更** ポートフォワーディング一覧 ポートフォワーディング登録／変更 アクセスグループ一覧 アクセスグループ登録／変更

マッピング登録

変換元PATH * ドメイン名以降のパスを指定します。(例: /products/)
/support/

変換元ドメイン名 * 変換元のドメイン名です。ユーザーがブラウザに入力するドメイン名です。(例: www.server.co.jp)
www.ftsafeco.jp

変換先URL * 変換先のバックエンドWebサーバーのURLです。アドレス部はIPアドレスで記述してください。(例: http://192.168.1.10:8080/products/)
http:// 211.10.20.97/support/

付加パラメータテンプレート 付加パラメータは認証済みのユーザーの情報としてバックエンドWebサーバーに転送するURLやフォームのBODYデータに付加することができます。この付加パラメータの機能により、フォームの自動入力などが実現できます。自動ログインに利用できます。

付加パラメータの付加方式 URL変換後の付加パラメータの付加方法を指定します。
0 0-付加しない。URL変換後に付加パラメータを付加しません。
1-リクエストがGETコマンドの場合に、クエリデータとして付加パラメータを送信します。
2-リクエストのクエリデータをポストデータへ変換し、付加パラメータをポストデータに付加して送信します。

リダイレクションURI 認証した後の移動先のURIです。(例: /system/error/s900.html)

IP認証 クライアントのIPアドレスでセッションを維持します。
しない

バックエンドのBASIC認証 バックエンドの基本認証用ユーザー名を入力ください。予約変数が入力可能です。
ユーザー名: パスワード:

バックエンドプール デフォルト変換先以外のバックエンドサーバーを指定します。
追加 削除する IPアドレス: ポート:

アクセスグループ ☐ 認証しない (匿名アクセス可) ☒ 指定されたアクセスグループのみを許可する
アクセスを許可するグループの一覧です。複数指定も可能です。
許可されるアクセスグループ: GroupVIP
アクセスグループ一覧: Administrators, GroupMember

(注意: 変更を有効にするためにサーバーの再起動が必要です。) 実行 キャンセル

「アクセス権限設定」の「マッピング登録／変更」画面にて「default」マッピングを以下のように編集します。

変換元 PATH	default
変換元ドメイン名	www.ftsafeco.jp
変換先 URL	http://211.10.20.97:8080/
許可されるアクセスグループ	GroupMember GroupVIP

SecureVisit
Web Authentication System

Help Logout
Server Time 2021-09-07 20:17:55

ユーザー管理 US8 トークン管理 **アクセス権限設定** 端末管理 ログ管理 認証DB・設定ファイル サーバー設定

マッピング一覧 **マッピング登録/変更** ポートフォワーディング一覧 ポートフォワーディング登録/変更 アクセスグループ一覧 アクセスグループ登録/変更

マッピング変更

変換元PATH * ドメイン名以降のパスを指定します。(例: /products/)
default

変換元ドメイン名 * 変換元のドメイン名です。ユーザーがブラウザに入力するドメイン名です。(例: www.server.co.jp)
www.ftsafe.co.jp

変換先URL * 変換先のバックエンドWebサーバーのURLです。アドレス部はIPアドレスで指定してください。(例: http://192.168.1.10:8080/products/)
http://211.10.20.97:8080/

付加パラメータテンプレート 付加パラメータは認証済みのユーザーの情報としてバックエンドWebサーバーに転送するURLやフォームのBODYデータに付加することができます。この付加パラメータの機能により、フォームの自動入力などが実現できます。自動ログインに利用できます。

付加パラメータの付加方式 0 URL変換後の付加パラメータの付加方法を指定します。
0-付加しない。URL変換後に付加パラメータを付加しません。
1-リクエストがGETコマンドの場合に、クエリデータとして付加パラメータを送信します。
2-リクエストのクエリデータをポストデータへ変換し、付加パラメータをポストデータに付加して送信します。

リダイレクションURI 認証した後の移動先のURIです。(例: /system/error/s900.html)

IP認証 クライアントのIPアドレスでセッションを維持します。
しない

バックエンドのBASIC認証 バックエンドの基本認証用ユーザー名を入力ください。予約変数が入力可能です。
ユーザー名: パスワード:

バックエンドプール デフォルト変換先以外のバックエンドサーバーを指定します。

アクセスグループ
☐ 認証しない (匿名アクセス可)
☒ 指定されたアクセスグループのみを許可する
アクセスを許可するグループの一覧です。複数指定も可能です。
許可されるアクセスグループ: GroupVIP, GroupMember
アクセスグループ一覧: Administrators

[注意: 変更を有効にするためにサーバーの再起動が必要です。] 実行 キャンセル

「アクセス権限設定」の「マッピング一覧」画面でアクセス権限設定を確認します。

/support/	GroupVIP
default	GroupMember GroupVIP

SecureVisit
Web Authentication System

Help Logout
Server Time:2021-04-23 18:01:13

ユーザー管理 US8 トークン管理 **アクセス権限設定** 端末管理 ログ管理 認証DB・設定ファイル サーバー設定

マッピング一覧 **マッピング登録/変更** ポートフォワーディング一覧 ポートフォワーディング登録/変更 アクセスグループ一覧 アクセスグループ登録/変更

マッピング一覧

変換元PATH	変換先URL	アクセスグループ	付加パラメータ	操作
/support/	http://211.10.20.97/support/	GroupVIP	無し	✎ ✕ ➡
default	http://211.10.20.97/	GroupMember, GroupVIP	無し	✎

[注意: 変更を有効にするためにサーバーの再起動が必要です。]

以上のように設定すると、技術サポートのコンテンツ（/support/）には、VIP 会員しかアクセスできません。その他のコンテンツ（/support/以外）には、一般会員または VIP 会員しかアクセスできません。

設定完了後に、「サーバー設定」の「サーバーの再起動」画面でサーバーを再起動し、設定を有効にします。



「USB トークン管理」の「USB トークン登録／変更」画面で、クライアント PC が使用する USB トークンの情報を登録します。

トークン ID	トークン ID (自動取得)
備考	備考欄

トークンを USB ポートに挿入し、「現在接続している USB トークンの HID を取得します。」をクリックすると、上記のように自動的にトークンの ID が取得され、トークン ID 欄に表示されます。その後「実行」をクリックし登録します。個々のトークン毎に登録します。

備考欄にはトークンの使用者の名前を記入しておくことをお勧めします。それにより「USB トークン管理」画面（次ページ）にて各 USB トークンの使用者名が表示され管理が容易になります。加えて、USB トークンそのものに使用者の名前を書いたラベルを貼り付けておくことで更に管理がしやすくなります。

「USB トークン管理」の「USB トークン一覧」画面で登録内容を確認します。



この段階では、まだトークンとユーザーは割り当てられていません。
割り当ては、次のステップ（ユーザー管理）で行います。

「ユーザー管理」の「ユーザー登録／変更」画面で各ユーザーを以下のように登録します。
パスワード認証を行う場合はパスワードも入力します。パスワード認証はデフォルトではありません。

ユーザーID	usera
フルネーム	VIP 会員 A さん
アクセスグループ	GroupVIP
割り当て USB トークン	トークン ID/状態/備考

「実行」をクリックし登録します。同様に他のユーザーも登録します。

「ユーザー管理」の「ユーザー一覧」画面で登録内容を確認します。

ユーザー毎にトークン ID やアクセスグループ等が正しく割り当てられているか確認します。

また「状態」は「有効」（緑色）でなければなりません。

SecureVisit
Web Authentication System

Help Logout
Server Time: 2021-04-12 20:12:45

ユーザー管理 USBトークン管理 アクセス権限設定 端末管理 ログ管理 認証DB・設定ファイル サーバー設定

ユーザー一覧 ユーザー登録/変更 インポート

ユーザー一覧

ユーザーID アクセスグループ 状態 トークンID 備考

検索 すべて表示 エクスポート

3件 |< 1 / 1 >| 表示件数 10

ユーザーID	フルネーム	アクセスグループ	状態	前回ログイン	利用開始	有効期限	トークンID	操作
admin	admin	Administrators	有効		1970/01/01	2099/12/02		
administrator	Administra...	Administrators	有効		1970/01/01	2099/12/02		
usera	VIP会員Aさん	GroupVIP	有効		2021/04/12	2099/12/31	8000058442F81BC1	

3件 |< 1 / 1 >| 表示件数 10

2.6. クライアント PC の利用方法

本認証システムは、事前にクライアント PC ヘドライバ及びアプリケーションのインストールは必要ありません。利用者は、Microsoft Edge 及び Google Chrome を利用した場合、初回アクセス時にのみ、SecureVisit クライアントをダウンロードするだけで、USB トークンによる認証を行うことができます。

2.6.1. クライアント PC システム要件

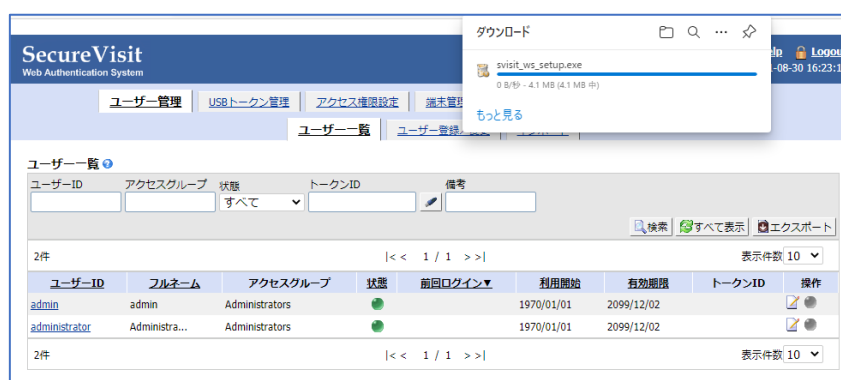
本認証システムを利用するクライアント PC は、以下の要件を満たしている必要があります。

OS	Windows10/Windows11
ブラウザ	Microsoft Edge 及び Google Chrome(92 以降) (SecureVisit クライアントが実行できること)
その他	USB 1.1/2.0/3.0 の空きポートが 1 つ以上

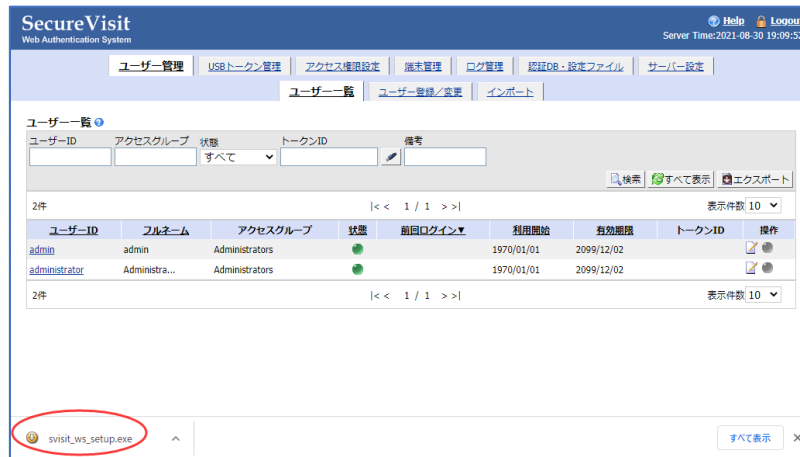
2.6.2. SecureVisit クライアントのインストール

利用者は、以下の手順で SecureVisit クライアントをダウンロードすることができます。なお、以下のダウンロード手順は Microsoft Edge 及び Google Chrome を利用した場合をもとに説明しています。利用する OS とブラウザのバージョンにより画面が異なる場合があります。

1. Microsoft Edge または Google Chrome を起動します。
2. <https://SecureVisit> 認証サーバーのドメイン名/へアクセスします。
3. 初回アクセス時は、「svisit_ws_setup.exe」をダウンロードするメッセージが表示されます。



Microsoft Edge の場合



Google Chrome の場合

4. ダウンロード完了後の「svisit_ws_setup.exe」をクリックすると、以下の画面が表示されるので、「はい」をクリックします。



以上でクライアント PC へのインストールは完了です。SecureVisit クライアントをインストールした後は、認証システムで保護した Web コンテンツにアクセスする度に、USB トークンによる認証を行うようになります。

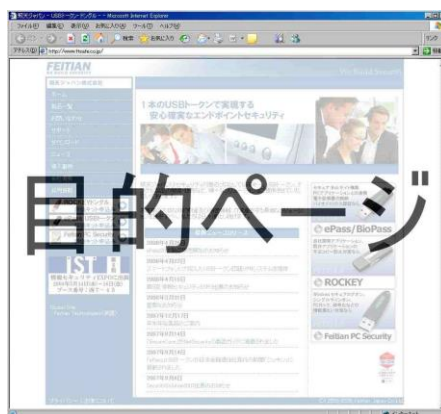
2.6.3. クライアント PC の認証

1. USB トークンをクライアント PC に接続します。
2. [https:// SecureVisit](https://SecureVisit) 認証サーバーのドメイン名/へアクセスします。
3. 認証画面が表示されるので、USB トークンに関連付けられた正しいユーザー ID/パスワードを入力し、「OK」をクリックします。



注：デフォルトはパスワードの認証は行いません。パスワードの認証を行う場合は管理画面のサーバー設定にて設定します。詳細は「3.7 サーバーの設定」をご参照ください。

4. 正しいユーザーIDとUSBトークンで認証が成功すると、保護している Web ページが表示されます。Web ページ表示後は他の Web ページ同様の操作でアクセスが行えます。



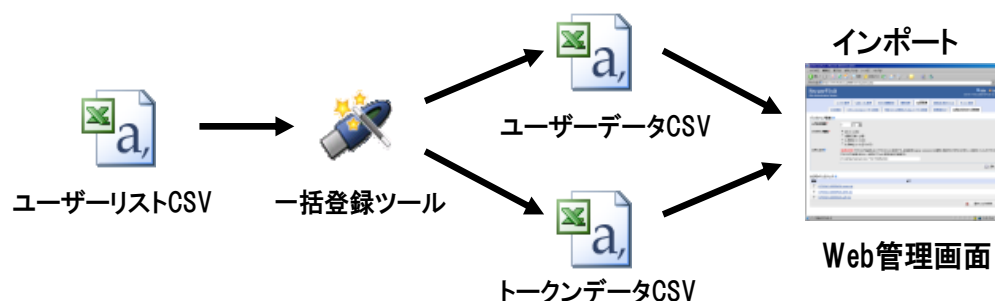
注：認証サーバーの設定により、認証ポップアップ画面の表示や認証の各種オプションを変更することができます。詳細は「3.7 サーバーの設定」をご参照ください。

2.7. USB トークン一括登録ツール

トークン一括登録ツールは、SecureVisit Web 認証システムに登録するユーザーや USB トークンの CSV ファイルを作成するツールです。このツールを使用することで、多数のトークンの登録処理を効果的に行うことができます。

2.7.1. トークン一括登録ツール概要

トークン一括登録ツールは、USB トークンを一括で登録する為の CSV を作成するツールです。このツールを利用することで、PC 側でユーザーや USB トークンの一覧を作成し、サーバーへインポートすることができます。なお、トークン一括登録ツールを利用せずに、Web 管理画面から USB トークンやユーザーを個々に登録することもできます。



トークン一括登録ツールイメージ図

ユーザーリスト CSV	各 CSV の元となるユーザー一覧のファイルで、事前に作成するファイルです。
ユーザーデータ CSV	ユーザーの一覧が記載された CSV ファイルです。個々の USB トークンとの関連付けなども記載されています。
トークンデータ CSV	トークンの一覧が記載された CSV ファイルです。どの USB トークンにどのユーザーが割り当てられているか記載されています。

Web 管理画面からのユーザーデータ CSV とトークンデータ CSV のインポート方法に関しては、それぞれ「3.2.4 インポート」と「3.3.4 インポート」をご参照ください。

2.7.2. トークン一括登録ツール利用環境

トークン一括登録ツールを利用するには、以下の環境が必要です。

OS	Windows10/Windows11
その他	USB 1.1/2.0/3.0 の空きポート 1 つ以上

2.7.3. トークン一括登録ツールのインストール

トークン一括登録ツールは、単一のアプリケーションで、インストール作業は特に必要ありません。

トークン一括登録ツールを起動するには、SecureVisit Ubuntu Setup CD の win32¥tokenWizard.exe ファイルを実行したい PC 上にコピーし、該当 EXE ファイルをダブルクリックしてください。

注：TokenWizard.exe と同じ場所に、SecureVisit Ubuntu Setup CD の win32¥FT_ND_API.dll ファイルもコピーしてください。

2.7.4. ユーザーリスト CSV ファイル

トークン一括登録ツールを利用するには、事前にユーザーリストをカンマ区切りの CSV ファイルにて作成しておく必要があります。CSV ファイルの項目は、以下の様に定義されています。

ユーザーリストの項目一覧：

列名	説明	フォーマット
userid ※	ユーザーID のフィールドです。この ID を実際にログインする際に利用します。	半角 1～32 文字
fullname	利用者名です。認証では使用しません。	全角 0～64 文字(半角 0～128 文字)
email	利用者のメールアドレスです。	半角 100 文字
access	ユーザーID/USB トークンの状態を示します。 (0=無効、1=有効、2=未登録)	半角 0、1、2
accessgroup	ユーザーID が所属するアクセスグループ名です。	0～32 文字。複数の場合は半角スラッシュ「/」で区切
startdate	ユーザーID の有効開始日です。 「2022/1/1 9:00」の形で入力します。	YYYY/MM/DD HH:MM
expire	ユーザーID の有効期限です。 「2022/12/31 23:59」の形で入力します。	YYYY/MM/DD HH:MM
memo	備考欄です。全角 100 文字まで任意に記述ができます。	全角 0～100 文字(半角 0～200 文字)
lastlogindate	最終ログイン日です。「2022/1/1 9:00:00」の形で入力します。	YYYY/MM/DD HH:MM
token1 ※	ユーザーID に割り当てるトークン番号 (HID) です。トークン登録ツールにより自動的に入力されます。	-
token2	ユーザーID に割り当てる予備トークン番号 (HID) です。	-
token3	ユーザーID に割り当てる予備トークン番号 (HID) です。	-
password	ユーザーID のパスワードです。	半角 0～32 文字
rescuepassword	レスキューパスワードです。	半角 8～32 文字

rescuetimes	レスキューパスワードの使用回数です。	半角-1～100、 (-1：無制限)
rstartdate	レスキューパスワードの有効開始日です。 「2022/1/1 9:00」の形で入力します。	YYYY/MM/DD HH:MM
rexpire	レスキューパスワードの有効期限です。 「2022/12/31 23:59」の形で入力します。	YYYY/MM/DD HH:MM
params	付加パラメータです。 「name=value」の形で入力します。	半角 0～32 文字 = '0 ～128 文字' 複数の 場合は半角スラッシュ 「/」で区切
ticket	チケットです。	半角 8～32 文字
counter	端末制限の端末数です。	0～10000

(※は必須フィールドです。“token1”はタイトルとして必須ですが、値は必須ではありません。)

<ユーザーリスト CSV の例>

```
userid,fullname,email,access,accessgroup,startdate,expire,token1
testuser1,飛天太郎,testuser1@example.co.jp,1,GroupA,2022/1/1 9:00,2025/1/1
9:00,8000058D42F81BC1
testuser2,飛天花子,testuser2@example.co.jp,1,GroupA,2022//1 9:00,2025/1/1
9:00,8000058D42F81BC2
```

注：「全角」または「半角」が明記されていない限り、「1 文字」の意味は「全角 1 文字」または「半角 1 文字」です。

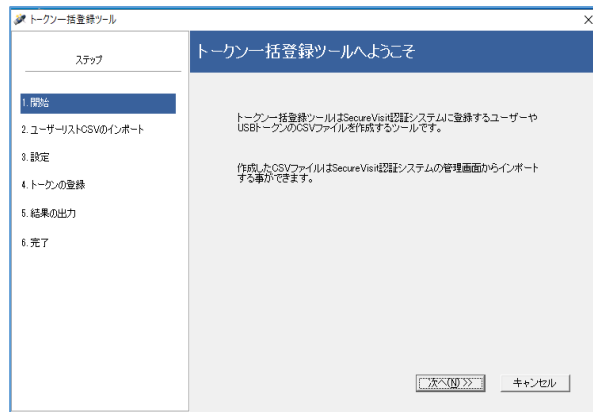
注：CSV ファイルをテキストエディタで直接編集する場合、以下の点にご注意ください。

- ・入出力 CSV ファイルはすべて Shift-JIS エンコーディングとすること。
- ・基本的にコンマで区切った部分がスペースを含めて、値であること。
- ・値にコンマやダブルクォートが含まれる場合は、値全体をダブルクォートで囲むこと。
- ・値に含まれるダブルクォートは "" 「2 つのダブルクォート」となること。

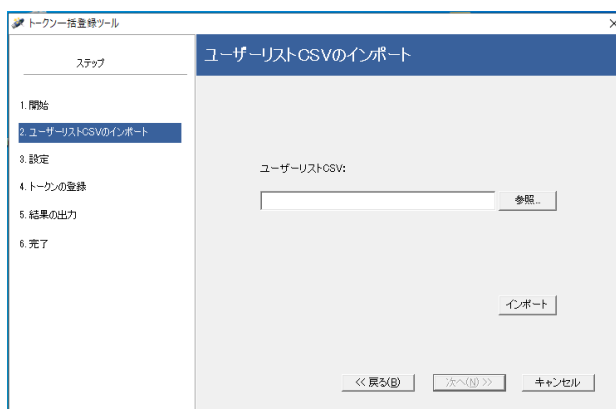
2.7.5. トークン一括登録ツールによる CSV ファイルの作成

以下では、トークン一括登録ツールを用いたユーザー/トークン一括登録用の CSV ファイル作成方法について説明します。なお、登録には、事前にユーザーの一覧が記載された CSV ファイルが必要となります。

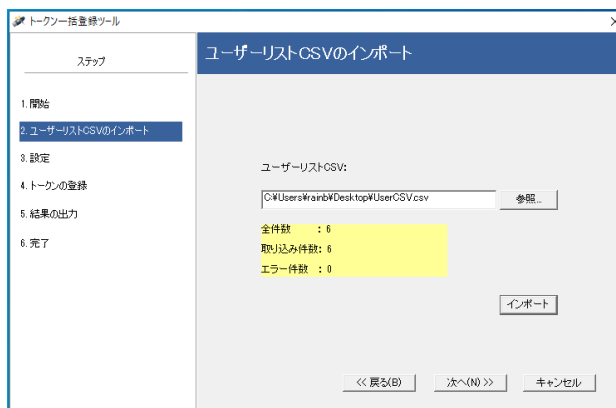
1. トークン一括登録ツールを起動します。
2. 「トークン一括登録ツールへようこそ」画面が表示されるので「次へ」をクリックします。



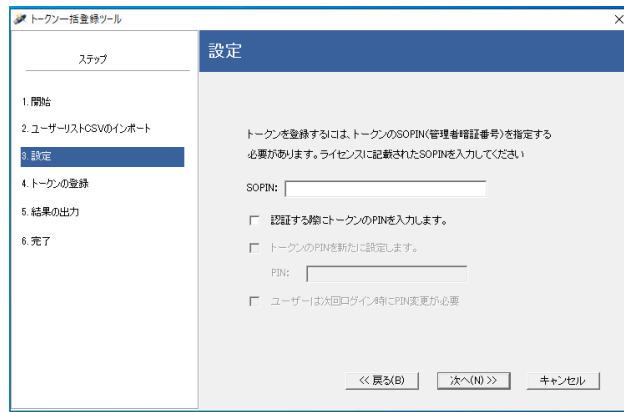
3. 「ユーザーリストCSV」に事前に作成した CSV ファイルを入力します。「参照」からファイルを参照することもできます。CSV ファイル指定後は「インポート」をクリックします。



4. インポートが完了すると、画面下に取り込み件数が表示されます。エラー件数が 0 件であることを確認し、「次へ」をクリックします。



5. 「設定」画面が表示されるので、以下項目を設定し、「次へ」をクリックします。



❖ 「SOPIN」

USB トークンを登録するには USB トークンの SOPIN を入力する必要があります。

SOPIN は SecureVisit サーバーのライセンスファイル：（ /svisit/share/svisit.lcn）の [TokenSOPIN] に記載されています。

評価版の場合は、「rockey」を入力してください。

❖ 「認証する際にトークンの PIN（暗証番号）を入力します。」

このチェックボックスをチェックすると、これから登録処理をする USB トークンで認証を行う際に、トークンの PIN を入力しなければなりません。このチェックボックスを外した場合、これから登録処理をする USB トークンで認証を行う際に、トークンの PIN を入力する必要はありません。認証画面には PIN の入力欄も表示されません。

❖ 「トークンの PIN を新たに設定します。」

このチェックボックスをチェックすると、これから登録処理をする USB トークンの PIN を新たに設定します。

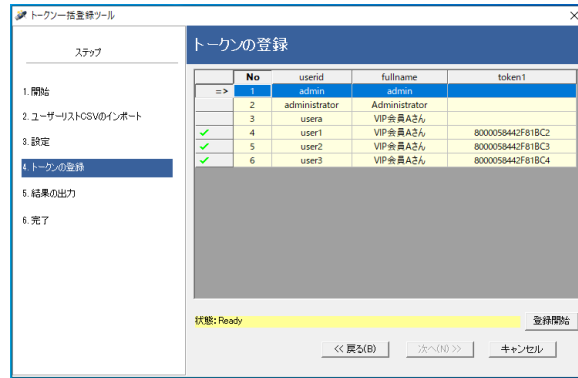
❖ 「PIN」

これから登録処理をする USB トークンに新たに設定する PIN です。半角 4 文字以上 32 文字まで入力できます。

❖ 「ユーザーは次回ログイン時に PIN 変更が必要」

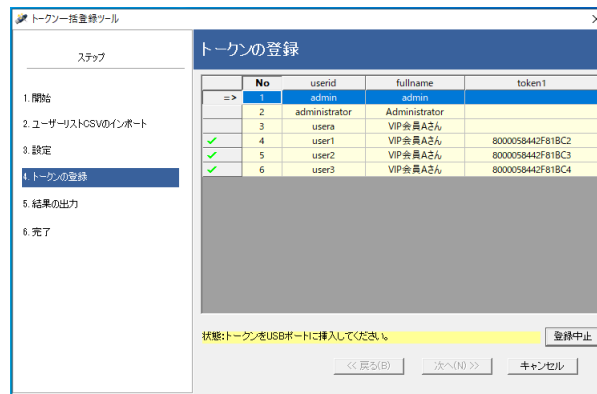
ユーザーが次回ログイン時の PIN 変更の設定です。チェックした場合、トークン一括登録ツールで登録した全てのユーザーは、次回ログイン時に強制的にトークンの PIN を変更させます。

6. 「トークンの登録」画面に表示される「状態」が「Ready」であることを確認し、「登録開始」をクリックします。



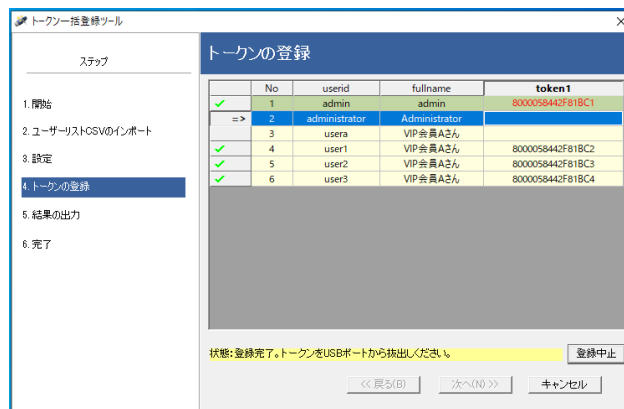
注：トークンの登録画面では「No」「UserID」「Fullname」「Token1」の4項目のみツールの画面上に表示されます。

- 「登録開始」をクリックすると、「状態」に「トークンを USB ポートに挿入してください」と表示されるので、USB トークンを挿入します。



注：USB トークンを PC に挿入すると自動的に登録が開始されます。確認画面は表示されません。

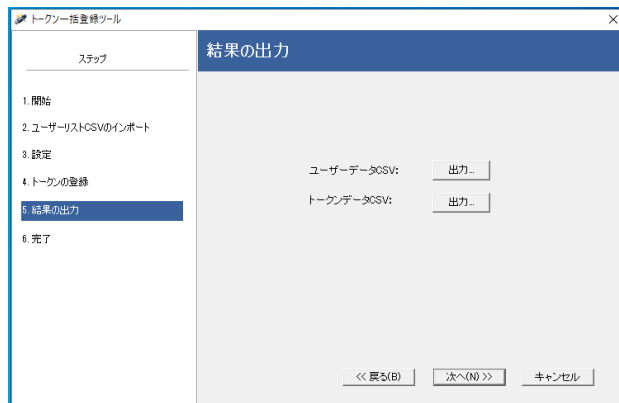
- 登録が完了すると「状態」に「登録完了。トークンを USB ポートから拔出してください」と表示されるので、PC から USB トークンを抜き出します。



- トークンが抜き出されると項番 7 に戻るので必要な回数分上記作業を繰り返します。途中で登録を中止したい場合は「登録中止」をクリックしてください。

10. 作業完了後は「次へ」をクリックします。

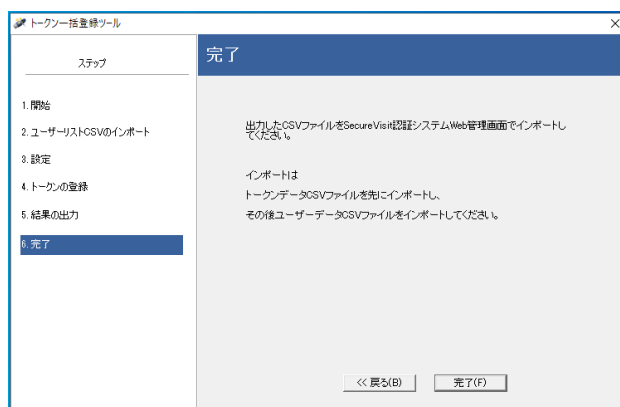
11. 「結果の出力」画面が表示されるので、「ユーザーデータ CSV」と「トークンデータ CSV」にある「出力」をクリックして CSV ファイルとしてエクスポートします。



ユーザーデータ CSV	ユーザーの一覧を記録した CSV ファイルです。インポートした CSV に加えトークンの HID（ハードウェアシリアル番号）が記載されています。
トークンデータ CSV	トークンの一覧を記録した CSV ファイルです。トークンに割り当てられたユーザー情報が記載されています。

12. エクスポート後は「次へ」をクリックします。

13. 「完了」画面が表示されるので、「完了」をクリックします。



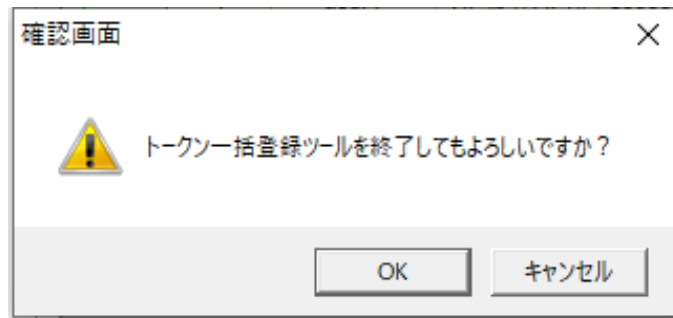
以上で、トークンの一括登録は完了です。以後は Web 管理画面からユーザーデータ CSV とトークンデータ CSV をインポートしてください。

注：CSV ファイルを Web 管理画面からインポートする際は、トークンデータ CSV ファイルを先にインポートし、その後ユーザーデータ CSV ファイルをインポートしてください。各データのインポート方法に関しては、それぞれ「3.2.4 インポート」と「3.3.4 インポート」をご参照ください。

2.7.6. トークン一括登録ツールの終了

トークン一括登録ツールを終了するには、作業完了後に表示される「完了」をクリックすることで終了することができます。

また、作業中でも画面右上の「×」をクリックするか、「キャンセル」をクリックすることでトークン一括登録ツールを終了することができます。途中で終了する場合は以下のメッセージが表示されるので「OK」をクリックします。



第3章 運用管理

本章では以下のトピックについて説明します。

- ❖ Web 管理画面概要
- ❖ ユーザー管理
- ❖ USB トークン管理
- ❖ アクセス権限設定
- ❖ ログ管理
- ❖ 認証 DB/設定ファイル管理
- ❖ サーバー設定

3.1. Web 管理画面概要

SecureVisit Web 認証システムでは、ほとんどの管理作業を Web 管理画面から行うことができます。管理者は Web 管理画面へアクセスすることで、ユーザーの登録/削除、USB トークンの登録/削除およびログ管理などを行うことができます。

Web 管理画面から実行できる主な機能

- ❖ ユーザー管理
- ❖ USB トークン管理
- ❖ アクセス権限設定
- ❖ 端末管理
- ❖ ログ管理
- ❖ 認証 DB・設定ファイル管理
- ❖ サーバー設定管理

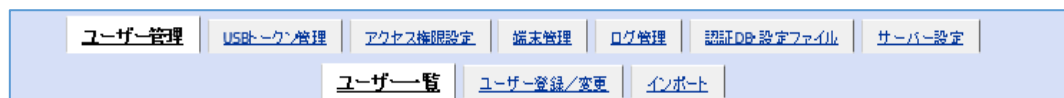
3.1.1. Web 管理画面の機能

管理画面へログインすると以下の画面が表示されます。



ユーザー管理	ユーザーの登録/削除、CSV ファイルからユーザーのインポートなどを行うことができます。
USB トークン管理	USB トークンの登録/削除、CSV ファイルからトークンのインポートなどを行うことができます。
アクセス権限設定	マッピング、ポートフォワーディングおよびアクセスグループの作成およびアクセス権限の割り当てを行うことができます。
端末管理	端末の登録/削除、CSV ファイルから端末インポートなどを行うことができます。
ログ管理	ログの検索とログのバックアップ管理を行うことができます。
認証 DB・設定ファイル	認証データベースと設定ファイルなどをインポート、エクスポートすることができます。
サーバー設定	サーバーのタイムアウト設定、SSL 証明書のインポート、IP フィルタ設定などを行うことができます。

Web 管理画面では上段のタブをクリックすることで下段に該当タブの項目が表示されます。以下の例では「ユーザー管理」を選択し、下段にユーザー管理機能の一覧を表示している例です。



また、USB トークン一覧画面などに表示される「操作」項目のアイコンは左側から「✎-編集」「●-有効/無効/未登録」「✖-削除」のボタンになっており、このボタンからも各タブをクリックした際と同様の操作が行えます。

	編集を意味します。クリックすることで該当項目の詳細ページを表示します。
	有効/無効/未登録を意味します。クリックすることで、該当項目の有効/無効/未登録を切り替えることができます。
	削除を意味します。クリックすることで該当項目の削除が行えます。削除時には確認メッセージが表示されます。

トークンID	状態	利用開始	有効期限	ユーザーID▲	備考	操作
8000058442F81BC1	有効	2021/09/07	2099/12/31	user3	Aさん用	

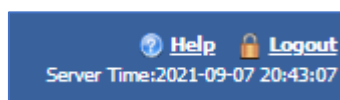
3.1.2. Web 管理画面のヘルプ機能

Web 管理画面には「🔗」マークが様々な箇所に配置されています。該当項目の詳細を確認したい場合は、「🔗」マークをクリックするとヘルプを別画面にて表示します。



3.1.3. Web 管理画面からのログアウト

Web 管理画面からログアウトを行いたい場合は、画面右側の「Logout」をクリックすることでログアウトすることができます。



注： Microsoft Edge 及び Google Chrome にて「Logout」を押すと Web 管理画面が閉じます。

3.2. ユーザー管理

ユーザー管理画面では、ユーザーの作成、変更およびユーザーのリスト（CSV ファイル）をインポートすることができます。以前にバックアップしたユーザーリストやトークン一括登録ツールを利用して作成したユーザーリストもインポートすることができます。



「ユーザー管理」タブで管理できる項目は以下の通りです：

ユーザー一覧	ユーザーの一覧を表示することができます。条件による検索なども行えます。
ユーザー登録/変更	ユーザーID を個別に登録することができます。一括して登録したい場合は、一括登録ツールを用いて登録が行えます。
インポート	一括登録ツールを用いて作成した CSV ファイルをインポートすることができます。

3.2.1. ユーザー一覧

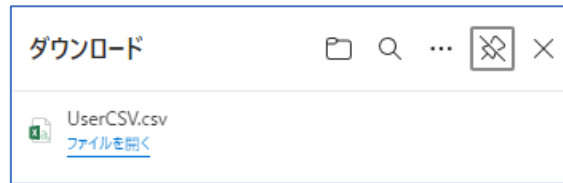
ユーザー一覧では認証システムに登録されたユーザーの一覧を表示することができます。ユーザーの一覧を表示したい場合は、「ユーザーID」や「アクセスグループ」などの一覧に検索したい文字列を入力します。

すべてのユーザーを表示したい場合は、「すべて表示」をクリックすることで、全てのユーザーリストを表示します。

なお、ユーザー一覧に表示されている USB トークンのボタン「

The screenshot displays the 'SecureVisit Web Authentication System' interface. At the top, there are navigation tabs: 'ユーザー管理' (User Management), 'USBトークン管理' (USB Token Management), 'アクセス権限設定' (Access Rights Setting), '端末管理' (Device Management), 'ログ管理' (Log Management), '認証DB設定ファイル' (Authentication DB Setting File), and 'サーバー設定' (Server Setting). Under 'ユーザー管理', there are sub-tabs: 'ユーザー一覧' (User List), 'ユーザー登録/変更' (User Registration/Change), and 'インポート' (Import). The 'ユーザー一覧' tab is active, showing a search bar with fields for 'ユーザーID', 'アクセスグループ', '状態' (Status), 'トークンID', and '備考' (Remarks). Below the search bar, there are buttons for '検索' (Search), 'すべて表示' (Show All), and 'エクスポート' (Export). A table of users is displayed with columns: 'ユーザーID', 'フルネーム' (Full Name), 'アクセスグループ' (Access Group), '状態' (Status), '前回ログイン' (Last Login), '利用開始' (Start Date), '有効期限' (Expiration Date), 'トークンID', and '操作' (Action). The table shows three users: 'admin', 'Administrator', and 'userA'. The 'userA' row is highlighted, showing a token ID of '8000058442F81BC1'. At the bottom of the table, there are pagination controls and a '表示件数' (Number of items to display) dropdown set to '10'.

検索結果を CSV ファイルに保存したい場合は、「エクスポート」をクリックすることで一覧に保存できます。CSV に保存したユーザーリストは Excel などで編集後に再度、「インポート」タブからインポートすることができます。



Microsoft Edge 及び Google Chrome を利用した場合

3.2.2. ユーザーの削除

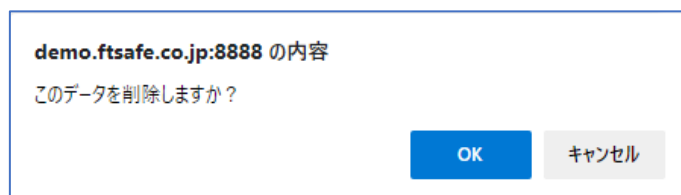
認証システムに登録されているユーザーを削除するには、以下の手順にて削除をすることができます。

ユーザー一覧画面から削除したいユーザーを表示します。

表示されたユーザーの「操作」欄にある「✕」アイコンをクリックします。



削除アイコンをクリックすると確認メッセージが表示されるので「OK」をクリックします。



Microsoft Edge 及び Google Chrome を利用した場合

注：削除したデータは復元できません。削除する際はご注意ください。

3.2.3. ユーザー登録/変更

「ユーザー登録」タブでは、ユーザーIDを個別に登録/変更することができます。新規に作成する場合は「ユーザー登録」タブを開いた後、空欄に必要な事項を入力し、「実行」をクリックします。既存ユーザーの情報を変更したい場合は「ユーザー一覧」から該当ユーザーをクリックします。

The screenshot shows the 'ユーザー登録' (User Registration) page in the SecureVisit Web Authentication System. The page has a top navigation bar with links like 'ユーザー管理', 'USBトークン管理', 'アクセス権限設定', etc. The main form area is titled 'ユーザー登録' and contains several sections:

- ユーザーID**: A text input field for the user's ID.
- 状態**: A dropdown menu for the user's status (有効, 無効, etc.).
- フルネーム**: A text input field for the user's full name.
- Email**: A text input field for the user's email address.
- 備考**: A text area for additional notes.
- 利用開始**: Fields for the start date and time of the user's ID.
- 有効期限**: Fields for the expiration date and time of the user's ID.
- パスワード**: A text input field for the user's password.
- レスキューパスワード**: A checkbox for setting a recovery password.
- 端末制限**: A checkbox for setting terminal restrictions.
- アクセスグループ**: A section for assigning the user to one or more access groups. It includes a list of available groups (Administrators, GroupMember, GroupVIP) and buttons to add or remove them.
- 付加パラメータ**: A section for adding parameters to the user's profile, including a text input for the parameter name and a dropdown for the value.
- 割り当てUSBトークン**: A section for assigning USB tokens to the user. It includes a list of available tokens and buttons to assign or unassign them.

At the bottom right of the form, there are buttons for '実行' (Execute) and 'キャンセル' (Cancel).

ユーザーID ※1	ユーザーID 名です。実際のログイン時に入力するユーザー名です。半角 32 文字まで入力可能です。 使用できる文字は、アルファベット (A～Z a～z)、数字 (0～9)、記号「-」「_」「@」「_」です。
状態 ※1	ユーザーアカウントの状態です。有効、無効、未登録から選択ができます。無効に設定されているユーザーID ではログインできません。デフォルトでは有効になっています。
フルネーム	ユーザーの名前です。全角 64 文字まで入力できます。
Email	ユーザーのメールアドレスです。半角 100 文字まで入力できます。
備考	備考欄です。全角 100 文字まで入力できます。
利用開始	ユーザーID が有効になる開始時刻です。「HH:MM:SS」のフォーマットで

	入力します。デフォルトでは現在のシステム時刻が使用されます。最大 2099/12/31 23:59:59 に設定できます。
有効期限	該当ユーザーID の有効期限です。期限が過ぎたユーザーID は利用できなくなります。期限が切れた場合もこの画面から変更することで利用再開することができます。最大 2099/12/31 23:59:59 に設定できます。
パスワード	ユーザーID のパスワードです。ここで入力されたパスワードとユーザーID を使用して認証を行います。パスワードは Web 管理画面からのみ変更できます。半角 32 文字まで入力できます。 使用できる文字は、アルファベット (A～Z a～z)、数字 (0～9)、記号「!」「#」「\$」「%」「&」「-」「_」「@」「.」「+」「*」「?」「_」です。
レスキューパスワード	ユーザーID のレスキューパスワード設定チェックボックスです。チェックしない場合はレスキューパスワード機能を使用できません。
レスキューパスワード設定 ※3	レスキューパスワードは半角 8～32 文字です。自動生成ボタンを押せば、自動的に半角 8 文字を生成できます。使用できる文字は、アルファベット (A～Z a～z)、数字 (0～9) です。
使用回数※3	レスキューパスワードでログオンすることが出来る回数です。 「設定範囲：-1～100 回 (-1：無制限)、デフォルト：20 回」
利用開始※3	レスキューパスワードが有効になる開始時刻です。「HH:MM:SS」のフォーマットで入力します。デフォルトでは現在のシステム時刻が使用されます。最大 2099/12/31 23:59:59 に設定できます。
有効期限※3	該当レスキューパスワードの有効期限です。期限が過ぎたユーザーID は利用できなくなります。期限が切れた場合もこの画面から変更することで利用を再開することができます。デフォルトでは利用開始より 24 時間で設定されます。最大 2099/12/31 23:59:59 に設定できます。
端末制限	ユーザーID の端末制限設定チェックボックスです。チェックしない場合は端末制限機能を使用できません。 ※「端末制限」をチェックした場合、「レスキューパスワード」機能が無効になります。
端末数※4	登録できる端末数と既に登録した端末数です。設定範囲：0～10000 になります。
チケット※4	端末自動登録の認証用パスワードです。半角 8～32 文字です。使用できる文字は、アルファベット (A～Z a～z)、数字 (0～9) です。
アクセスグループ	ユーザーが所属するアクセスグループです。最大で 3 つのアクセスグループに所属させることができます。
付加パラメータ	付加パラメータは認証済みユーザーの情報としてバックエンド Web サーバーに転送する URL やフォームの BODY データに付加することができます。「3.4.2 マッピング登録/変更」機能もご参照ください。タグは最大半角 32 文字まで入力できます。値は最大半角 128 文字まで入力できます。
割り当て USB トークン	ユーザーに割り当てる USB トークンです。各ユーザーには 1 つの有効な USB トークン、2 つの予備 USB トークンを割り当てることができます。

- ※1 は必須フィールドです。
- ※2 このフィールドは存在しない場合もあります。
- ※3 は該当ユーザーのレスキューパスワードチェックボックスをチェックした場合に設定できます。
ただし、「3.7.1 サーバー設定」の「レスキューパスワードの使用」を「する」に設定する必要があります。
- ※4 は該当ユーザーの端末制限チェックボックスをチェックした場合に設定できます。ただし、「3.7.1 サーバー設定」の「端末限定」を「しない」以外に設定する必要があります。

3.2.4. インポート

トークン一括登録ツールを用いて、CSV ファイルを作成した場合や、以前にバックアップしたユーザーID の CSV ファイルをインポートすることができます。

ユーザーリストをインポートするには「参照」から CSV ファイルを選択し、「インポート」をクリックします。
インポートする際には以下のオプションのどちらかを選択します。

「既にデータが存在する場合は上書きする」

認証システムの DB に同一のユーザーID が存在する場合、CSV ファイルの内容で上書きを行います。

「既にデータが存在する場合はスキップする」

認証システムの DB に同一のユーザーID が存在する場合、インポート処理を行わずにスキップします。スキップしたユーザーID はインポート後もインポート前の状態を保持します。

3.3. USB トークン管理

USB トークン管理画面では、USB トークンの登録、変更、削除などを行うことができます。また、過去にバックアップしたリストからのインポートやトークン登録ツールを利用して作成した USB トークンのリストを一括してインポートすることもできます。

「USB トークン管理」タブで管理できる項目は以下の通りです。


USB トークン一覧	USB トークンの一覧を表示します。条件による検索なども行えます。 検索結果を CSV ファイルにエクスポートすることができます。
USB トークン登録/変更	USB トークンを個別に登録/変更することができます。一括して登録したい場

	合は、一括登録ツールを用いて登録が行えます。
インポート	登録する USB トークンを CSV ファイルでインポートすることができます。 トークン一括登録ツールを用いて作成した CSV ファイル、または、エクスポートした CSV ファイルでインポートすることができます。

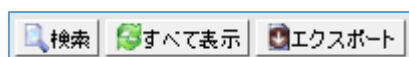
3.3.1. USB トークン一覧

「USB トークン一覧」では、認証システムに登録されている USB トークンの一覧を表示します。「トークン ID」、「ユーザーID」、「備考」に検索したい文字列を入力し、「検索」をクリックすると検索条件にマッチした USB トークンを表示します。

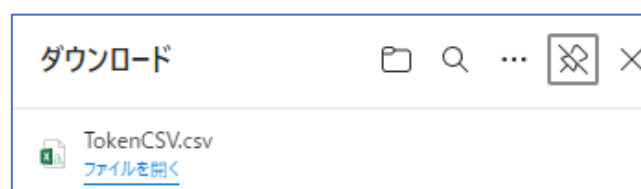


全ての USB トークンを表示したい場合は、「すべて表示」をクリックすることで認証システムに登録されている全ての USB トークンを表示します。また、ユーザー一覧に表示されている USB トークンのボタン「」をクリックすると、管理画面へアクセスしている PC に接続されている USB トークンのハードウェア ID (HID) を取得することができます。

注：USB トークンのハードウェア ID は個々の USB トークンに割り当てられているユニーク（一意）な番号になります。



検索結果を CSV ファイルにエクスポートすることで、USB トークンの情報を Excel などで編集することができます。エクスポートするには「エクスポート」をクリックし、「ファイルのダウンロード」ボックスで「保存」をクリックします。



Microsoft Edge 及び Google Chrome を利用した場合

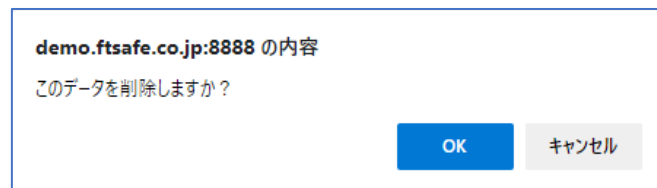
3.3.2. USB トークンの削除

認証システムに登録されているトークンを削除するには、以下手順にて削除することができます。

1. USB トークン一覧画面にて削除したい USB トークンを表示します。
2. 表示された USB トークンの「操作」欄にある「✖」アイコンをクリックします。



3. 削除アイコンをクリックすると確認メッセージが表示されるので「OK」をクリックします。



Microsoft Edge 及び Google Chrome を利用した場合

注：削除したデータは復元できません。削除する際はご注意ください。

3.3.3. USB トークン登録/変更

「USB トークン登録/変更」タブでは、USB トークンを個々に登録することができます。登録/変更を行う場合は、設定変更後に「実行」をクリックします。「キャンセル」をクリックした場合は適用されません。

「USB トークン登録」の画面：

SecureVisit Web Authentication System

Help Logout Server Time: 2021-09-07 20:55:15

ユーザー管理 USBトークン管理 アクセス権限設定 端末管理 ログ管理 認証DB・設定ファイル サーバー設定

USBトークン一覧 USBトークン登録/変更 インポート

USBトークン登録

トークンID *

状態 USBトークンの有効/無効を設定します。(デフォルト:有効)
有効

PINの入力 認証する際にUSBトークンのPIN(暗証番号)の入力要否の設定です。(デフォルト:ユーザーはログイン時にUSBトークンのPINを入力させません。)
☐ユーザーはログイン時にUSBトークンのPINを入力させます。

PINの設定 USBトークンのPINの設定です。(半角4~32文字、使用できる文字は、アルファベット(A~Z a~z)、数字(0~9)、記号「!」「#」「\$」「%」「&」「*」「+」「-」「_」「?」です。)
新しいPIN:

PINの強制変更 ユーザーが次回ログイン時のPIN変更の設定です。チェックした場合、ユーザーは次回ログイン時に強制的にトークンのPINを変更させます。
☐ユーザーは次回ログイン時にPIN変更が必要

備考 備考欄です。(全角100文字)

利用開始 USBトークンの利用開始日時です。日付は「YYYY/MM/DD」のフォーマットで、時刻は「HH:MM:SS」のフォーマットで入力してください。(デフォルト:システム日時)
日付: 時刻:

有効期限 USBトークンの有効期限です。日付は「YYYY/MM/DD」のフォーマットで、時刻は「HH:MM:SS」のフォーマットで入力してください。(デフォルト:2099/12/31 23:59:59)
日付: 時刻:

「USBトークン変更」画面：

SecureVisit Web Authentication System

Help Logout Server Time: 2021-09-07 21:00:57

ユーザー管理 USBトークン管理 アクセス権限設定 端末管理 ログ管理 認証DB・設定ファイル サーバー設定

USBトークン一覧 USBトークン登録/変更 インポート

USBトークン変更

トークンID * 8000058E42F81BC1

状態 USBトークンの有効/無効を設定します。(デフォルト:有効)
有効

PINの強制変更 ユーザーが次回ログイン時のPIN変更の設定です。チェックした場合、ユーザーは次回ログイン時に強制的にトークンのPINを変更させます。
☐ユーザーは次回ログイン時にPIN変更が必要

備考 備考欄です。(全角100文字)
Aさん用

利用開始 USBトークンの利用開始日時です。日付は「YYYY/MM/DD」のフォーマットで、時刻は「HH:MM:SS」のフォーマットで入力してください。(デフォルト:システム日時)
日付: 2021/09/07 時刻: 21:00:48

有効期限 USBトークンの有効期限です。日付は「YYYY/MM/DD」のフォーマットで、時刻は「HH:MM:SS」のフォーマットで入力してください。(デフォルト:2099/12/31 23:59:59)
日付: 2099/12/31 時刻: 23:59:59

トークン ID(16 桁) ※1	トークン ID を取得することができます。登録したい USB トークンを接続し、「現在接続している USB トークンの HID を取得します。」をクリックすると、トークン ID を取得できます。取得したトークン ID を変更することができません。
状態	トークンの状態です。有効、無効から選択ができます。無効に設定されているトークンはログインに利用できません。デフォルトでは有効になっています。
PIN の入力 ※3	認証する際に USB トークンの PIN（暗証番号）の入力要否の設定です。USB トークンの PIN の最大リトライ回数は 5 回となります。3 回目に入力を誤るとエラーメッセージが表示されます。最大リトライ回数(5 回)まで連続で入力を誤るとロックされた状態になります。PIN ロック解除するには、当該 USB トークンを削除し、改めて登録し、PIN を設定します。
PIN の設定 ※3	USB トークンの PIN の設定です。新しい PIN を指定することができます。PIN の設定条件は、半角 4～32 文字、使用できる文字は、アル

	ファベット (A～Z a～z)、数字 (0～9)、記号「!」「#」「\$」「%」「-」「_」「@」「.」「+」「*」「?」「_」です。
PIN の強制変更	ユーザーが次回ログイン時の PIN 変更の設定です。チェックした場合、ユーザーは次回ログイン時に強制的にトークンの PIN を変更させます。 ※PIN を再設定する際、8 桁以上の半角英数字を入力してください。
備考	備考欄です。全角 100 文字まで入力できます。
利用開始	トークンが有効になる開始時刻です。「HH:MM:SS」のフォーマットで入力します。何も入力しないと現在のサーバーのシステム時刻が使用されます。最大 2099/12/31 23:59:59 に設定できます。
有効期限	該当トークンの有効期限です。期限が過ぎたトークンは利用できなくなります。期限が切れた場合もこの画面から変更することで利用を再開することができます。何も指定しない場合は 2099/12/31 23:59:59 に設定されます。最大 2099/12/31 23:59:59 に設定できます。

※1 は必須フィールドです。

※2 はトークン登録時のみ表示されるフィールドです。

3.3.4. インポート

「インポート」では、トークン一括登録ツールを用いて、CSV ファイルを作成した場合や以前にバックアップした USB トークンの CSV ファイルをインポートすることができます。

USB トークンのリストをインポートするには、「参照」から CSV ファイルを選択し、「インポート」をクリックします。インポートする際には以下のオプションのどちらかを選択します。

「既にデータが存在する場合は上書きする」

認証システムの DB に同一の USB トークン ID が存在する場合、CSV ファイルの内容で上書きを行います。

「既にデータが存在する場合はスキップする」

認証システムの DB に同一の USB トークン ID が存在する場合、インポート処理を行わずにスキップします。スキップした USB トークン ID はインポート後もインポート前の状態を保持します。

3.4. アクセス権限設定

アクセス権限管理では、リクエストのあった URL に対して、アクセス制御およびバックエンドサーバーの URL マッピングを定義することができます。認証サーバーのポートとバックエンドのポートフォワーディングを定義することができます。また、アクセスグループを作成することで、グループごとのアクセス権限の設定を行うことができます。

「アクセス権限設定」タブで管理できる項目は以下の通りです。

マッピング一覧	設定されているマッピングの一覧を表示します。
マッピング登録/変更	システムにマッピング設定を追加/変更します。
ポートフォワーディング一覧	設定されているポートフォワーディング一覧を表示します。
ポートフォワーディング登録/変更	システムにポートフォワーディング設定を追加/変更します。
アクセスグループ一覧	システムに登録されているグループの一覧を表示します。
アクセスグループ登録/変更	システムにアクセスグループを追加/変更します。

3.4.1. マッピング一覧

「マッピング一覧」では、現在システムに割り当てられているマッピングに関する情報を表示します。

マッピングの順番：

マッピングの表示順を変更したい場合は、アイコン「↑」「↓」で変更が行えます。

注：マッピングの設定変更は「↑」「↓」をクリックした時点で反映されますが、有効にするには「サーバー設定」からサーバーの再起動が必要になります。

注：バージョン 2.0.0.1 以降の場合、上記の設定が無効になっております。

最後の一行には常にデフォルトマッピングが表示されます。「default」という変換元 PATH で表示されます。デフォルトマッピングとは、すべてのマッピングにもマッチしない URL にマッチする定義済みのマッピングです。



SecureVisit Web Authentication System				
Help Logout Server Time: 2021-04-21 19:16:45				
ユーザー管理 USBトークン管理 アクセス権限設定 端末管理 ログ管理 認証DB-設定ファイル サーバー設定				
マッピング一覧 マッピング登録/変更 ポートフォワーディング一覧 ポートフォワーディング登録/変更 アクセスグループ一覧 アクセスグループ登録/変更				
マッピング一覧				
変換元PATH	変換先URL	アクセスグループ	付加パラメータ	操作
/news/2021/	http://211.10.20.97/news/2021/	GroupD	無し	↑ ↓ ✕
/news/	http://211.10.20.97/news/	GroupC	無し	↑ ↓ ✕
default	http://211.10.20.97	匿名	無し	✕

(注意: 変更を有効にするためにサーバーの再起動が必要です。)

マッピングの編集：

既に登録されているマッピングの設定を変更したい場合は、「変換元 PATH」をクリックすると、編集画面が表示されます。表示されたマッピングの「操作」欄にある「✎」アイコンをクリックしても、編集画面が表示されます。

マッピングの削除:

表示されたマッピングの「操作」欄にある「✖」アイコンをクリックすると、確認メッセージが表示されるので「OK」をクリックします。

demo.ftsafe.co.jp:8888 の内容

このデータを削除しますか？

OKキャンセル

Microsoft Edge 及び Google Chrome を利用した場合

注：削除したデータは復元できません。削除する際はご注意ください。

3.4.2. マッピング登録/変更

「マッピング登録/変更」では、新規にマッピングを作成することや、既存のマッピング設定を変更することができます。なお、既存のマッピング設定変更を行いたい場合は、「マッピング一覧」から変更したいマッピングをクリックしてください。

SecureVisit
Web Authentication System

Help | Logout
Server Time 2024-04-24 11:51

ユーザー管理 | ユーザーグループ管理 | アクセスマッピング設定 | 権限管理 | ログ管理 | 証明書・設定ファイル | サーバー設定

マッピング登録 | マッピング登録/変更 | ポートフォワーディング | ポートフォワーディング/変更 | アクセスマッピンググループ | アクセスマッピンググループ/変更

マッピング変更

変換元PATH

変換元ドメイン

変換元URL

クロスドメインリダイレクト

付加パラメータテンプレート

付加パラメータの付加方式

リダイレクションURI

IP認証

バックエンドのBASIC認証

バックエンドプール

アクセスマッピンググループ

ドメイン名以降のパスを指定します。(例: /products)
default

変換元のドメイン名です。ユーザーがブラウザに入力するドメイン名です。(例: www.server.co.jp)
[入力欄]

変換元のバックエンドWebサーバーのURLです。アドレス部分はIPアドレスで指定してください。(例: http://192.168.1.10:8080/products)
[入力欄]

クロスドメインリダイレクトを設定します。
[リダイレクトされたドメイン名またはIPです。(例1: http://www.ftdemo.com) (例2: https://192.168.1.10:8080)]
[入力欄]

付加パラメータは認証済みのユーザーの権限としてバックエンドWebサーバーに転送するURLやフォームのBODYデータに付加することができます。この付加パラメータの機能により、フォームの自動入力などが実現できます。自動ログインに利用できます。
[追加] [パラメータ名: [入力欄]] [削除] [タグまたは値: [入力欄]]

URL変換後の付加パラメータの付加方法を指定します。
0
0:付加しない。URL変換後に付加パラメータを付加しません。
1:リクエストがGETコマンドの場合に、クエリデータとして付加パラメータを送信します。
2:リクエストのクエリデータをポストデータに変換し、付加パラメータをポストデータに付加して送信します。
[入力欄]

認証した後のリダイレクションURIです。(例: /system/error/500.html)
[入力欄]

クライアントのIPアドレスでセッションを維持します。
[入力欄]

バックエンドの基本認証用ユーザー名を入力してください。予約変数が入力可能です。
ユーザー名: [入力欄] パスワード: [入力欄]

デフォルト変換先以外のバックエンドサーバーを指定します。
[追加] [IPアドレス: [入力欄]] [削除する] [ポート: [入力欄]]

☐ 認証しない (匿名アクセス可)

☒ 指定されたアクセスマッピンググループのみを許可する

アクセスを許可するグループの一覧です。複数指定も可能です。
許可されるアクセスマッピンググループ
Administrators
[追加] [許可する] [許可しない]

アクセスマッピンググループ一覧
[追加] [許可する] [許可しない]

[注意: 変更を有効にするためにサーバーの再起動が必要です。]

実行

キャンセル

変換元 PATH ※	変換元のアドレス（パス）を入力します。変換元とはクライアント PC がブラウザに入力するドメイン名以降のアドレス部です。ディレクトリ全体やファイル単位で指定できます。 ※ディレクトリ全体を保護する場合、変換元 PATH の最後に「/」を追加する必要があります。
------------	---

	例 : /news/2021/
変換元ドメイン名※	変換元のドメイン名を入力します。変換元のドメイン名はクライアント PC がブラウザに入力するドメイン名を記述します。「http://」は入力せず、ドメイン名单体を入力します。
変換先 URL※	変換元ドメイン名および変換元 PATH を組み合わせた URL へアクセスがあった際に転送するバックエンドの Web サーバーのア付加パラメータアドレスを指定します。変換先の Web サーバーのポート番号が 80 以外の場合はドメイン部以降に「:」とポート番号を入力します。 ※ディレクトリ全体を保護する場合、URL の最後に「/」を追加する必要があります。 例 : http://211.10.20.97/news/2021/
クロスドメインリダイレクト	バックエンドサーバーがあり、ユーザーがサイトから外部サイトにアクセスしようとする際に、該当項目を「する」に変更すると、別のドメインにリダイレクトすることができます。 ※デフォルトでは利用しません。
付加パラメータテンプレート	付加パラメータはバックエンド Web サーバーに転送する値です。この値を URL やフォームの BODY データ等に付加できます。この付加パラメータの機能により、自動ログインを実現することができます。
付加パラメータの付加方式	URL 変換後の付加パラメータの付加方法を指定します。 0-付加しない。URL 変換後に付加パラメータを付加しません。 1-リクエストが GET コマンドの場合に、クエリデータとして付加パラメータを送信します。 2-リクエストのクエリデータをポストデータへ変換し、付加パラメータをポストデータに付加して送信します。
リダイレクション URI	認証成功した後に固定的な移転先の URI を入力します。リダイレクション URI が設定された場合、認証成功した後に変換先 URI ではなく、アクセス先はリダイレクション URI に移転します。 ※デフォルトリダイレクション URI: /usr/local/svisit/html/
IP 認証	クライアント IP 毎に認証状態を維持するかしないかの設定です。「はい」に設定した場合は、同一クライアント IP からのすべてのアクセスは同じ認証状態になります。「しない」場合は、同一クライアント IP でも、異なるブラウザウィンドウからのアクセスは別々で認証を行います。 ※Microsoft Edge の Inprivate ウィンドウと Google Chrome の シークレットウィンドウは除外
バックエンドの BASIC 認証	変換先 URL へのアクセスは BASIC 認証が必要な場合は、BASIC 認証のユーザー名とパスワードを入力します。ユーザー名の入力欄に“{userid}”を入力した場合、ユーザー名は実際に認証する際のユーザー ID となります。パスワードの入力欄に“{password}”を入力した場合、パスワードは実際に認証する際のパスワードとなります。
バックエンドプール	バックエンドサーバーが複数ある場合、変換先 URL に記載したサーバー以外のバックエンドサーバーの IP アドレスとポートを入力しま

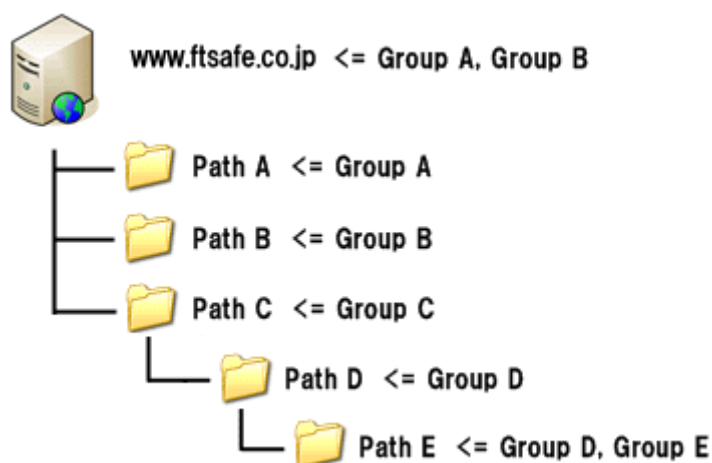
	す。
アクセスグループ	アクセス権限の設定を行います。「認証しない（匿名アクセス可）」に設定した場合は、どのユーザーでもアクセスが行えます。「指定されたアクセスグループのみを許可する」に設定した場合は、画面下にあるアクセスグループのボックスにて許可設定を定義します。

（※は必須フィールドです）

3.4.3. マッピングの適用

認証システムのマッピングは、リストの上から順に比較し、条件にマッチしたものがあればそのアクセス権限を適用します。その為、深い階層でのアクセス制限を行いたい場合は、マッピングの設定を範囲の狭いものが上位に来るように設定してください。

以下はマッピングの適用例です。



	Group A	Group B	Group C	Group D	Group E
トップページ	○	○	×	×	×
Path A	○	×	×	×	×
Path B	×	○	×	×	×
Path C	×	×	○	×	×
Path D	×	×	×	○	×
Path E	×	×	×	○	○

Group A に所属するユーザー：

Group A に所属するユーザーはトップページ（<http://www.ftsafeco.jp>）と Path A にはアクセスできますが、アクセス権の無い Path B, Path C, Path D, Path E にはアクセスできません。（Group B も同様にトップページと Path B 以外へはアクセスできません。）

Group C に所属するユーザー：

Group C に所属するユーザーは Path C 以外はトップページも含めてアクセスできません。
Path C 内の Path D もアクセスできません。

Group D に所属するユーザー :

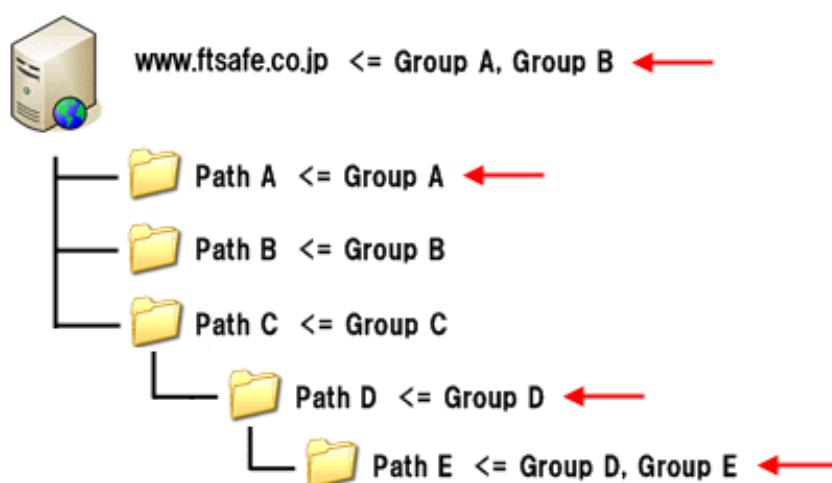
Group D に所属するユーザーは、Path D と Path E へアクセスすることはできますが、それ以外（トップページ、Path A、Path B、Path C）へはアクセスできません。


Group E に所属するユーザー :

Group E に所属するユーザーは、Path E 以外は一切アクセスができません。

なお、ユーザーは最大で 3 つのグループに所属することができ、複数のグループに所属するユーザーは、各グループに割り当てられているフォルダへアクセスすることができます。

前述の図で、ユーザーA が Group A および Group D に所属している場合、ユーザーA はトップページ、Path A、Path D、Path E にアクセスすることができます。



マッピング一覧				
変換元PATH	変換先URL	アクセスグループ	付加パラメータ	操作
/news/2021/	http://211.10.20.97/news/2021/	GroupD	無し	   
/news/	http://211.10.20.97/news/	GroupC	無し	   
default	http://211.10.20.97	匿名	無し	

認証システムのマッピングは、リストの上から順に比較し条件にマッチしたものがあればそのアクセス権限を適用します。上図の様に認証サーバーに上記設定を行い、ユーザーが `http://ドメイン名/news/2021/index.html` にアクセスした場合は、「/news/2021/」のマッピングに指定されたアクセス権限が適用されます。

注：Web サイト全体を保護したい場合は「default」の設定を編集してください。

3.4.4. 付加パラメータ

付加パラメータ機能は、クライアントからのアクセスを認証した後、バックエンド Web サーバーに、HTTP(S)リクエストで指定されたパラメータを付加して転送する機能です。「キー＝バリュー」の形で付加されます。付加できるパラメータは、SecureVisit 認証サーバーにおけるユーザー ID やパスワード以外に、管理者によって任意に定義することができます。ユーザー毎に異なるバリューを付加することもできます。

ユーザーID/パスワードの入力フォームを持つ既存の Web システムに SecureVisit を導入して、トークン認証の後にユーザーID/パスワードの入力を省略したい場合は、この付加パラメータ転送機能を利用して実現できます。

付加パラメータ転送機能の設定方法を以下の例で説明します。

既存システムにユーザーID/パスワードなどの入力項目を持つログイン画面（図 1）があると仮定します。このログイン画面で正しい認証情報（事業所 ID、ユーザーID、パスワード）を入力して「ログイン」ボタンを押せばメインメニュー画面（図 2）に遷移します。

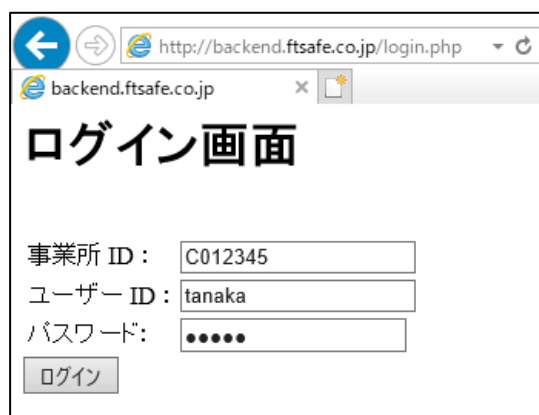


図 1 ログイン画面



図 2 メインメニュー画面

例として、ログイン画面（ソースコード：login.php）には、表示された「事業所 ID」、「ユーザー ID」、「パスワード」の入力項目以外に、「フラグ」という隠し項目があります。また、メインメニュー画面（ソースコード：mainmenu.php）には、単純にログイン画面に入力された認証情報を表示する

のみです。2つの画面のソースコードは以下の通りです。

login.php

```
<html>
<body>
<form action="mainmenu.php" method="post">
<h1>ログイン画面</h1><br>
<table>
<tr><td>事業所 ID : </td><td><input type="text" name="fcompany"
/></td></tr>
<tr><td>ユーザーID : </td><td><input type="text" name="fname"
/></td></tr>
<tr><td>パスワード : </td><td><input type="password" name="fpasswd"
/></td></tr>
</table>
<input type="hidden" name="flag" value="1"/>
<input type="submit" value="ログイン"/>
</form>
</body>
</html>
```

mainmenu.php

```
<html>
<body>
<h1>
ようこそ <?php echo $_POST["fcompany"]; ?>の<?php echo $_POST["fname"]; ?>
様!<br/>
貴方のパスワードは <?php echo $_POST["fpasswd"]; ?> です.<br/>
貴方のページフラグは <?php echo $_POST["flag"]; ?> です
</h1>
</body>
</html>
```

設定及び利用方法:

1. SecureVisit Web 管理画面の「マッピング登録」画面で保護されたページ (mainmenu.php) のマッピングを登録します。(図3)
「変換元 PATH」: /mainmenu.php
「変換先 URL」: http://<server>/mainmenu.php

「付加パラメータテンプレート」：fcompany={tag_company}
fname={userid}

fpasswd={password}
flag=1

「付加パラメータの付加方式」：2（付加パラメータを POST データに付加する）

付加パラメータテンプレート

付加パラメータは認証済みのユーザーの情報としてバックエンドWebサーバーに転送するURLやフォームのBODYデータに付加することができます。この付加パラメータの機能により、フォームの自動入力などが実現できます。自動ログインに利用できます。

fcompany={tag_company}
fname={userid}
fpasswd={password}
flag=1

追加 削除

パラメーター名:
タグまたは値:

付加パラメータの付加方式

URL変換後の付加パラメータの付加方法を指定します。

2

0-付加しない。URL変換後に付加パラメータを付加しません。
1-リクエストがGETコマンドの場合に、クエリデータとして付加パラメータを送信します。
2-リクエストのクエリデータをポストデータへ変換し、付加パラメータをポストデータに付加して送信します。

図3 「マッピング登録」画面

注：{userid} と {password} は SecureVisit 認証サーバーの規定変数です。それぞれ SecureVisit 認証サーバーにおけるユーザーID とパスワードに指します。

変換元PATH	変換先URL	アクセスグループ	付加パラメータ	操作
/mainmenu.php	http://192.168.11.2/mainmenu.php	GroupA	有り	
default	http://192.168.11.2	匿名	無し	

(注意:変更を有効にするためにサーバーの再起動が必要です。)

図4 「マッピング一覧」画面

- マッピングを登録完了してから、「サーバー設定」の「サーバーの再起動」画面で、SecureVisit を再起動して設定を有効にします。
- 「ユーザー一覧」画面で、各ユーザーID をクリックして、「ユーザー変更」画面で「付加パラメータ」のバリューを設定します。下図の例では、tag_company のバリューのみを設定しています。

付加パラメータ

付加パラメータはバックエンドWebサーバーに転送する値です。この値をURLやフォームのBODYデータ等に付加できます。「アクセス権限設定」の「マッピング登録・変更」機能にも参照下さい。

tag_company=C012345

追加 削除

タグ:
値:

図5 「ユーザー変更」画面

- 以上で付加パラメータ転送の設定は完了です。クライアントコンピューターにトークンを接続して、ブラウザ(Edge/Chrome)から「<http://<server>/mainmenu.php>」にアクセスすると、ログイン画面の表示はスキップされ、直接メインメニュー画面が表示されると、本来入力する必要があるユーザーID などの認証情報が自動的に転送されたことが分かります。



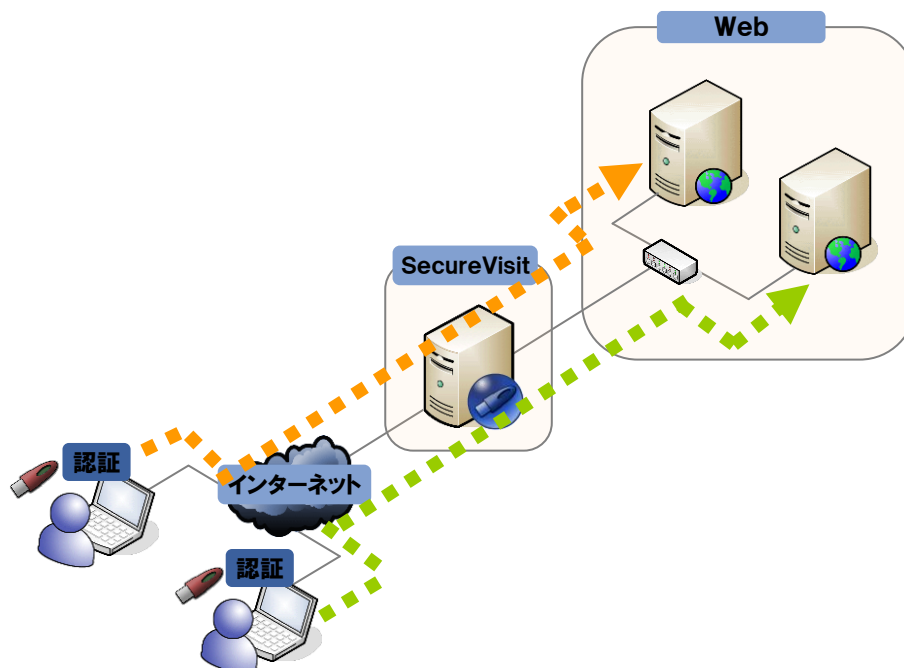
図 6 メインメニュー画面

3.4.5. バックエンドプール

SecureVisit Web 認証システムは、クライアントからのアクセスを認証した上で、複数のバックエンドサーバー間（バックエンドプールと呼ぶ）で分散させる機能があります。

バックエンドプールはマッピング単位で設定可能です。クライアントからのアクセス認証が成功した後、認証システムにより適切なバックエンドサーバーに転送します。接続が切断されるまで、同一接続からの後続のアクセスが同じバックエンドサーバーに転送されます。

同じ PC 端末（同一 IP）より初回アクセスした場合、設定した任意のバックエンドに移行し、次回からのアクセスも同じバックエンドに移行します。



マッピング変更

変換元PATH * ドメイン名以降のパスを指定します。(例: /products/) /news/

変換元ドメイン名 * 変換元のドメイン名です。ユーザーがブラウザに入力するドメイン名です。(例: www.server.co.jp) www.ftsafe.co.jp

変換先URL * 変換先のバックエンドWebサーバーのURLです。アドレス部分はIPアドレスで記述してください。(例: http://192.168.1.10:8080/products/) http://192.168.1.2/news/

テンプレート 付加パラメータは認証済みのユーザーの情報としてバックエンドWebサーバーに転送するURLやフォームのBODYデータに付加することができます。この付加パラメータの機能により、フォームの自動入力などが実現できます。自動ログインに利用できます。

バックエンドのBASIC認証 付加パラメータは認証済みのユーザーの情報としてバックエンドWebサーバーに転送するURLやフォームのBODYデータに付加することができます。この付加パラメータの機能により、フォームの自動入力などが実現できます。自動ログインに利用できます。

バックエンドプール デフォルト変換先以外のバックエンドサーバーを指定します。

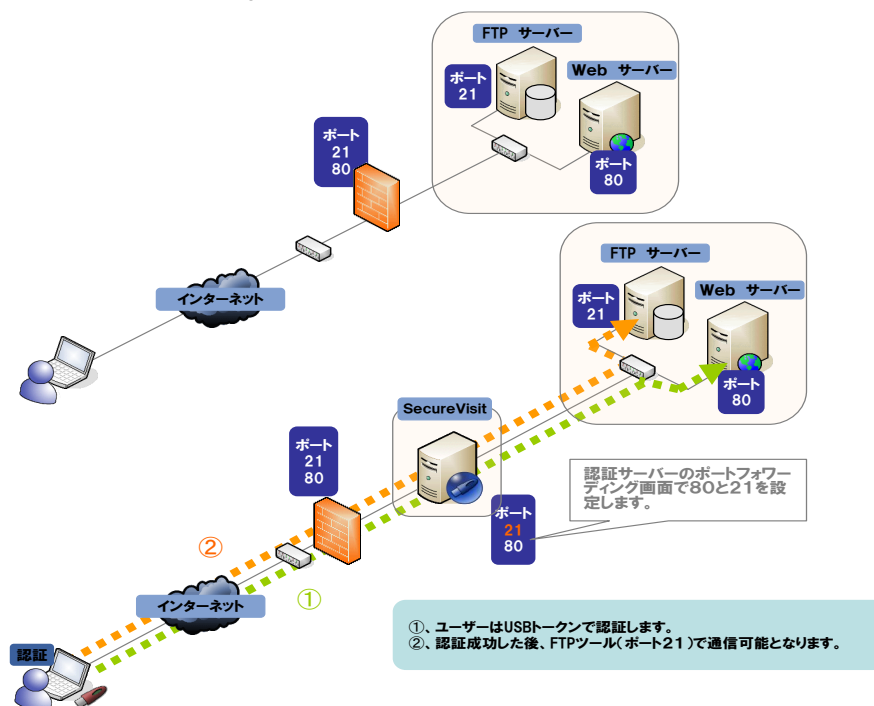
192.168.1.3:80 追加 IPアドレス: ポート:

削除する

上図のように認証サーバーに上記の設定を行った場合、クライアントから「http://www.ftsafe.co.jp/news/...」へのアクセスが認証された後に、「http://192.168.1.2/news/...」または「http://192.168.1.3/news/...」に転送されます。

3.4.6. ポートフォワーディング

SecureVisitはWebサーバー（HTTP/HTTPS）に対応しています。HTTP/HTTPS以外のアプリケーションプロトコルに対応するために、ポートフォワーディング機能を提供しています。ポートフォワーディング機能は、SecureVisitサーバーで、一旦USBトークンなどで認証した後に、同一端末からのHTTP/HTTPS以外（他のポート）のアクセスも通過するようにする機能です。ポートフォワーディング機能を利用すると、FTPサーバーやメールサーバー、ターミナルサーバーなどのTCPプロトコルに基づく通信サービス（※）もSecureVisitを利用して認証強化できるようになります。



ポートフォワーディング機能の利用イメージは、先ずユーザーは端末から USB トークンなどの SecureVisit 認証サーバーにて認証を行います。認証成功した後の一定時間内は、同じ端末であれば、SecureVisit 認証サーバーを経由してバックエンドにある FTP サーバーなどへのアクセスが許可されるようになります。SecureVisit にて認証失敗した場合は、バックエンドにある FTP サーバーなどへのアクセスが拒否されます。

※プロトコルの仕様により、一部対応していない場合があります。

注意：ポートフォワーディング機能では、端末の IP アドレスで判断しているため、端末側が NAT 構成の場合、同一 IP アドレスに変換される他の端末からのアクセスも許可します。

3.4.7. ポートフォワーディング一覧

「ポートフォワーディング一覧」では、現在システムに割り当てられているポートに関する情報を表示します。

ローカルポート	プロトコル	リモートIP	リモートポート	同時接続数	グループ	操作
3389	tcp	192.168.1.100	3389	1	GroupVIP	
21	tcp	211.10.20.97	21	1	GroupMember	

(注意:変更を有効にするためにサーバーの再起動が必要です。)

ポートフォワーディング設定の編集:

既に登録されているポートの設定を変更したい場合は、「ローカルポート」をクリックすると、編集画面が表示されます。また、表示されたポートフォワーディングの「操作」欄にある「」アイコンをクリックすると、編集画面が表示されます。

ポートフォワーディング設定の削除:

表示されたポートフォワーディングの「操作」欄にある「」アイコンをクリックすると、確認メッセージが表示されるので「OK」をクリックします。

demo.ftsafe.co.jp:8888 の内容

このデータを削除しますか？

OK
キャンセル

Microsoft Edge 及び Google Chrome を利用した場合

注：削除したデータは復元できません。削除する際はご注意ください。

3.4.8. ポートフォワーディング登録/変更

「ポートフォワーディング登録/変更」では、新規にポートフォワーディング設定を作成することや、既存のポートフォワーディング設定を変更することなどができます。なお、既存のポートフォワーディング設定変更を行いたい場合は、「ポートフォワーディング一覧」から変更したいポートフォワーディングをクリックしてください。

SecureVisit
Web Authentication System

Help Logout
Server Time 2021-10-18 11:19:45

ユーザー管理 USBトークン管理 アクセス権限設定 端末管理 ログ管理 認証DB・設定ファイル サーバー設定

マッピング一覧 マッピング登録/変更 ポートフォワーディング一覧 ポートフォワーディング登録/変更 アクセスグループ一覧 アクセスグループ登録

ポートフォワーディング登録

ローカルポート* 認証サーバーのポートです。(例: 21)
[]

プロトコル* フォワーディングのプロトコルを指定します。
tcp

リモートIP* 変換先のバックエンドサーバーのIPアドレスです。(例: 192.168.1.100)
[]

リモートポート* 変換先のバックエンドサーバーのポートです。(例: 21)
0

同時接続数 同一IPアドレスからの最高同時接続数を設定します。(デフォルト: 1)
0

アクセスグループ
◎ 認証しない (匿名アクセス可)

(注意: 変更を有効にするためにサーバーの再起動が必要です。) [実行] [キャンセル]

ローカルポート ※	認証サーバーのポートを入力します。サーバーのポート番号は半角数字 0～65535 です。
プロトコル※	フォワーディングのプロトコルを設定します。 tcp プロトコル
リモート IP※	変換先のバックエンドサーバーの IP アドレスです。
リモートポート※	変換先のバックエンドサーバーのポートです。 ポート番号は「0～65535」になります。
同時接続数	変換先のバックエンドサーバーへの同時接続数の上限です。 設定範囲は「1～65535」になります。
アクセスグループ	アクセス権限の設定を行います。「認証しない（匿名アクセス可）」に設定した場合は、どのユーザーでもアクセスが行えます。


(※は必須フィールドです)

3.4.9. アクセスグループ一覧

「アクセスグループ一覧」では、登録されているグループの一覧を表示します。アクセスグループ名、または、説明から検索を行います。全てのグループを表示したい場合は、「すべて表示」をクリックすることで、システムに登録されている全てのアクセスグループを表示します。



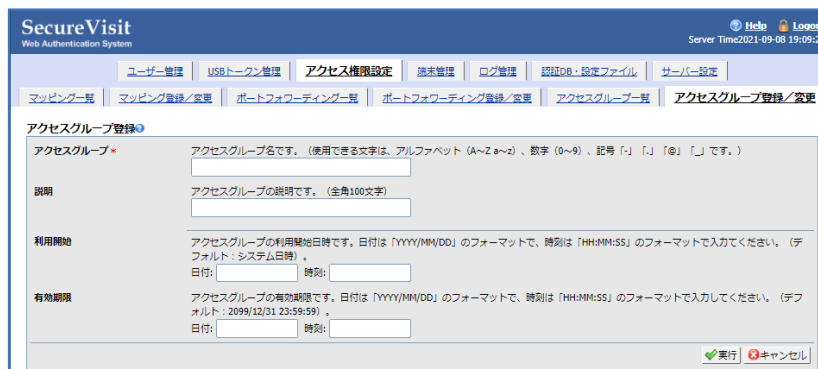
アクセスグループには、デフォルトで Administrators グループがあり、このグループに所属するユーザーは管理者として、Web 管理画面へログインすることができます。Administrators グループは他のグループと異なり削除することはできません。

操作欄にある「」のアイコンをクリックすると、該当グループに所属するユーザーを表示することができます。



3.4.10. アクセスグループ登録/変更

「アクセスグループ登録/変更」では、新規にアクセスグループを作成することや、既存のアクセスグループ設定を変更することなどができます。なお、既存のアクセスグループの設定変更を行いたい場合は、「アクセスグループ一覧」から変更したいアクセスグループをクリックしてください。



アクセスグループ ※	アクセスグループ名を入力します。半角 32 文字まで入力できます。使用できる文字は、アルファベット (A～Z a～z)、数字 (0～9)、記号
------------	---

	「-」「.」「@」「_」です。
説明	半角/全角 100 文字までアクセスグループの説明を入力できます。
利用開始	アクセスグループが有効になる開始日を設定します。日付の部分は「YY/MM/DD」で入力し、時刻の部分は「HH:MM:SS」のフォーマットで入力します。省略した場合はサーバーのシステム日時を使用します。
有効期限	アクセスグループの有効期限を設定します。日付の部分は「YY/MM/DD」で入力し、時刻の部分は「HH:MM:SS」のフォーマットで入力します。何も入力しない場合は 2099/12/31 に設定されます。

(※は必須フィールドです)

3.5. ログ管理

ログ管理では、SecureVisit が記録したログの内容を検索・表示することができます。ログの検索は、日付、URL、アクセスグループ、ユーザーID、トークン ID など様々な条件から検索が行えます。また、検索結果を CSV ファイルとしてエクスポートすることもできます。

「ログ管理」タブで以下の項目が管理できます：

ログの検索	様々な条件からログを検索することができます。 検索結果をエクスポートすることができます。
ログインしていない ユーザーの検索	指定期間内でシステムにログインしていないユーザーを検索します。 検索結果をエクスポートすることができます。
特定ファイルを参照していない ユーザーの検索	指定期間内で、指定したファイルを参照していないユーザーを検索します。 検索結果をエクスポートすることができます。

管理操作ログ	管理画面で行った操作履歴を検索します。 検索結果をエクスポートすることができます。
ログの保存	ログの保存およびログの保存間隔を指定することができます。

3.5.1. ログの検索

「ログの検索」では様々な条件からログを検索することができます。検索結果は「エクスポート」から LogListCSV.csv ファイルに保存することができます。また、各項目にあるチェックマークを外すと検索結果から非表示にすることができます。ログはアクセスログと認証ログの2種類のログが表示されています。認証ログは水色の背景で表示されます。成功した認証の認証ログのステータスに「success」と記載されています。失敗した認証の認証ログのステータスにエラーコードが記載されています。エラーコードの一覧は「4.1 エラーメッセージ一覧」をご参照ください。アクセスログは灰色の背景で表示されます。

日付 From/To	ログの日付による検索を行います。フォーマットは「YYYY/MM/DD」です。
時刻 From/To	ログの時刻による検索を行います。フォーマットは「HH:MM:SS」です。
URL	URL による検索を行います。検索は入力した文字列を含む URL を表示します。
アクセスグループ	アクセスグループ名による検索を行います。検索は入力した文字列を含むグループを表示します。
ユーザーID	ユーザーID による検索を行います。検索は入力した文字列を含むユーザーIDを表示します。
トークン ID	トークン ID による検索を行います。検索は入力した文字列を含むトークン ID を表示します。
接続元 IP	IP アドレスによる検索を行います。
ステータス	HTTP のステータスコードによる検索を行います。検索は入力した文字列を含むステータスを表示します。 ※バージョン 2.0.0.7 より、ステータスにて、コードまで表示されます。

3.5.2. ログインしていないユーザーの検索

「ログインしていないユーザーの検索」では、日付の「From」と「To」の期間内にログインを行っていないユーザーを検索します。日付に何も入力しない場合は、全期間を対象として検索を行います。検索結果は「エクスポート」から LogSOneCSV.csv ファイルに保存することができます。



The screenshot shows the 'Logins of users who did not login' search results. The search criteria are 'From: 2021/04/12' and 'To: 2009/12/31'. The results table has 7 columns: User ID, Access Group, Status, Last Login, Validity, Validity End, and Token ID. Two users are listed: 'admin' and 'administrator', both with a status of 'Success' and a last login of '1970/01/01'.

ユーザーID	アクセスグループ	状態	前回ログイン	有効開始	有効期限	トークンID	備考
admin	Administrators	成功	1970/01/01	1970/01/01	2009/12/02		
administrator	Administrators	成功	1970/01/01	1970/01/01	2009/12/02		

3.5.3. 特定ファイルを参照していないユーザーの検索

「特定ファイルを参照していないユーザーの検索」では、日付の「From」と「To」の期間内に「特定ファイルの URL」を参照していないユーザーを検索します。日付に何も入力しない場合は、全期間を対象として検索を行います。検索結果は「エクスポート」から LogSTwoCSV.csv ファイルに保存することができます。



The screenshot shows the 'Search for users who did not refer to the specified file' search results. The search criteria are 'From: ' and 'To: ' with '特定ファイルのURL' (Specific File URL) entered as '/support'. The results table has 7 columns: User ID, Access Group, Status, Last Login, Validity, Validity End, and Token ID. Two users are listed: 'admin' and 'administrator', both with a status of 'Success' and a last login of '1970/01/01'.

ユーザーID	アクセスグループ	状態	前回ログイン	有効開始	有効期限	トークンID	備考
admin	Administrators	成功	1970/01/01	1970/01/01	2009/12/02		
administrator	Administrators	成功	1970/01/01	1970/01/01	2009/12/02		

注：「特定ファイルの URL」は入力必須項目です。

3.5.4. 管理操作ログ

「管理操作ログ」では、様々な条件から管理画面で行った操作履歴を検索することができます。検索結果は「エクスポート」から LogAdminCSV.csv ファイルに保存することができます。

SecureVisit
Web Authentication System

Help Logout
Server Time: 2021-04-14 20:21:50

ユーザー管理 USBトークン管理 アクセス権限設定 細末管理 ログ管理 認証DB設定ファイル サーバー設定

ログの検索 ログにないユーザーの検索 特定ファイル参照してないユーザーの検索 管理操作ログ ログの保存

管理操作ログ

日付 From To (YYYY/MM/DD) ユーザーID

時刻 From To (HH:MM:SS) オペレーション

検索 すべて表示 エクスポート

29件 |< < 1 / 3 > >| 表示件数 10

日時	ユーザーID	オペレーション	操作内容
2021/04/14 20:05:00	administrator	AL_PF_NEW	フォワーディングポート21が新規追加されました
2021/04/14 20:02:47	administrator	AL_PF_NEW	フォワーディングポート3389が新規追加されました
2021/04/14 19:25:31	administrator	AL_TOKEN_EXPORT	トークン情報1件エクスポートされました
2021/04/14 18:59:11	administrator	AL_USER_EXPORT	ユーザー情報3件エクスポートされました
2021/04/14 17:56:23	administrator	AL_USER_EXPORT	ユーザー情報3件エクスポートされました
2021/04/14 17:15:02	administrator	AL_TOKEN_EXPORT	トークン情報1件エクスポートされました
2021/04/14 17:03:19	administrator	AL_TOKEN_EXPORT	トークン情報1件エクスポートされました
2021/04/14 16:11:49	administrator	AL_SRV_RESTART	サーバーが再起動されました(O.K)
2021/04/14 16:11:23	administrator	AL_SRV_RESTART	サーバーが再起動されました(O.K)
2021/04/14 16:02:19	administrator	AL_UM_MOD	マッピング defaultの設定が変更されました

29件 |< < 1 / 3 > >| 表示件数 10

日付 From/To	ログの日付による検索を行います。フォーマットは「YYYY/MM/DD」です。
時刻 From/To	ログの時刻による検索を行います。フォーマットは「HH:MM:SS」です。
ユーザーID	管理者ユーザーID による検索を行います。検索は入力した文字列を含むユーザーID を表示します。
オペレーション	操作の種類を示すコードです。オペレーションコードの一覧は以下の表になります。

オペレーションコード

AL_USER_EXPORT	ユーザー情報のエクスポート
AL_USER_NEW	ユーザーの新規追加
AL_USER_MOD	ユーザーの設定変更
AL_USER_IMPORT	ユーザー情報のインポート
AL_USER_DEL	ユーザーの削除
AL_TOKEN_EXPORT	トークン情報のエクスポート
AL_TOKEN_NEW	トークンの新規追加
AL_TOKEN_MOD	トークンの設定変更
AL_TOKEN_IMPORT	トークン情報のインポート
AL_TOKEN_DEL	トークンの削除
AL_UM_NEW	マッピングの新規追加
AL_UM_MOD	マッピングの設定変更
AL_UM_DEL	マッピングの削除
AL_GROUP_NEW	グループの新規追加
AL_GROUP_DEL	グループの削除
AL_GROUP_MOD	グループの設定変更
AL_DB_EXPORT	認証データベースのエクスポート
AL_CF_EXPORT	サーバーの設定ファイルのエクスポート

AL_LOG_EXPORT	ログバックアップファイルのエクスポート
AL_DB_IMPORT	認証データベースのインポート
AL_CF_IMPORT	サーバーの設定ファイルのインポート
AL_LOG_IMPORT	ログバックアップファイルのインポート
AL_SSL_CERTMOD	サーバーの SSL 証明書の設定変更
AL_SSL_ON	サーバーの SSL 通信の有効化
AL_SSL_OFF	サーバーの SSL 通信の無効化
AL_SSL_PWDMOD	サーバーの SSL 証明書のパスワードの変更
AL_SSL_CAMOD	SSL 通信用の認証局証明書の変更
AL_SSL_CRLMOD	SSL 通信用の失効証明書リストの変更
AL_SSL_DEPTHMOD	証明書チェーンの深さの変更
AL_SSL_CIPHERMOD	許可する暗号化アルゴリズムの設定変更
AL_SSL_CLIENTAUTHMOD	クライアント認証モードの変更
AL_BL_NEW	ブラックリストの追加
AL_BL_DEL	ブラックリストの削除
AL_BL_ON	ブラックリストの有効化
AL_BL_OFF	ブラックリストの無効化
AL_WL_NEW	ホワイトリストの追加
AL_WL_DEL	ホワイトリストの削除
AL_WL_ON	ホワイトリストの有効化
AL_WL_OFF	ホワイトリストの無効化
AL_WL_AUTHON	ホワイトリストの認証の有効化
AL_WL_AUTHOFF	ホワイトリストの認証の無効化
AL_WL_AUTHCUSTOMER	ホワイトリストの認証の一部有効化
AL_SRV_RESTART	サーバーの再起動
AL_ADMIN_LOGIN	管理者のログイン
AL_TERM_IMPORT	端末情報ファイルのインポート
AL_TERM_EXPORT	端末情報ファイルのエクスポート
AL_TERM_DELETE	ユーザー端末情報の削除
AL_TERM_ADD	ユーザー端末情報の登録
AL_PF_NEW	フォワーディングポートの新規追加
AL_PF_MOD	フォワーディングポートの設定変更
AL_PF_DEL	フォワーディングポートの削除

3.5.5. ログの保存

ログの保存では、認証システムが取得したログのダウンロードとアーカイブログの取得間隔を指定することができます。設定変更を行った場合は「更新」をクリックし、システムに更新を適用してください。

「ログのアーカイブ」には、アーカイブされたログの一覧が表示されます。ダウンロードしたい場合は、

該当ファイル名をクリックするとダウンロードが行えます。サーバーからログを削除したい場合は、チェックマークにチェックを入れ、「選択したログの削除」をクリックします。

「ログ保存期間」:

システムで保管するログの期間を指定します。指定期間を過ぎたログは、自動的にデータベースから削除されます。

認証ログ、アクセスログ、管理者ログの保存最大上限は「50 万行」になっています。

「アーカイブ間隔」:

ZIP ファイルに圧縮する間隔を指定します。指定した間隔でログファイルの一覧が作成されます。管理者は圧縮されたファイルを個別にダウンロードすることができます。

「ログフィルタ」:

アクセスログを記録しないアクセスのフィルタ設定です。正規表現(regular expression)の規則に準拠する文字列となります。この設定にマッチしたアクセスはアクセスログに記録しません。一般的にデフォルト設定のままで結構です。

SecureVisit
Web Authentication System

Help Logout
Server Time: 2021-08-26 15:12:45

ユーザー管理 USBトークン管理 アクセス権限設定 端末管理 ログ管理 認証DB・設定ファイル サーバー設定

ログの検索 ログインしていないユーザーの検索 特定ファイルを参照していないユーザーの検索 管理操作ログ ログの保存

ログの保存

ログ保存期間* 2 月

アーカイブ間隔

☒ 1日 (0~24時)
☐ 1週間 (日曜~土曜)
☐ 1ヶ月単位 (1~31日)
☐ 3ヶ月単位 (1~31日*3ヶ月)
(注意) 定期的にログのアーカイブファイルをダウンロードし、別のメディアへ保管することを勧めします。

ログフィルタ (高度な設定) アクセスログを記録しないアクセスのフィルタ設定です。正規表現(regular expression)の規則に準拠する文字列となります。この設定にマッチしたアクセスはアクセスログに記録しません。一般的にデフォルト設定のままで結構です。
/\\.(gif|jpeg|png|css|js).*Not Modified\$/i

更新

ログのアーカイブ

削除	ログ
選択したログを削除	

3.6. 認証 DB・設定ファイル

認証 DB・設定ファイルでは、SecureVisit で利用する各種設定ファイル、ログファイルおよび認証データベースのバックアップを取得することができます。システム再インストール時は設定ファイル、ログファイル及び認証データベースをインポートすることで環境を容易に復元することができます。

「認証 DB・設定ファイル」タブで管理は以下項目が管理できます。

認証 DB・設定ファイル・ログファイルのバックアップ管理	認証システムで利用する認証用の認証データベースや設定ファイル及びログファイルをバックアップすることやインポートすることができます。
------------------------------	---

3.6.1. 認証 DB・設定ファイルのバックアップ管理

「認証 DB・設定ファイルのバックアップ管理」では、認証システムで利用する認証データベースのエクスポート及びインポート、設定ファイルのエクスポート及びインポート、ログファイルのエクスポート及びインポートを行うことができます。



認証データベースのエクスポート	認証データベースの内容（ユーザー情報、USB トークン情報、グループ情報、ユーザーと USB トークンの関連情報、ユーザーのグループ所属情報、認証用秘密鍵等）をすべてエクスポートすることができます。エクスポートしたファイルは「db_bak.txt」になります。
-----------------	--

認証データベースのインポート	認証データベースにバックアップファイルからデータをインポートします。サーバーを再インストールした場合や、認証 DB に障害が発生した場合に、認証データベースをインポートすることができます。
設定ファイルのエクスポート	設定ファイルをエクスポートすることができます。設定ファイルは config.xml ファイルで構成されています。
設定ファイルのインポート	<p>以前にバックアップした設定ファイルをインポートすることができます。設定ファイルにはサーバーの設定情報、マッピング情報、アクセス権限の設定情報などが記録されています。</p> <p>※注意:サーバーを再起動後、インポートしたデータが反映されます。</p> <p>※バージョン 2.0.1 より、「マッピング登録/変更」の設定方法が変更になったので、以前のバージョンのデータをエクスポートして、バージョン 2.0.1 以降のバージョンにインポートする際、「3.4.2.マッピング登録/変更」を参照して設定方法を変更してください。</p>
ログファイルのエクスポート	<p>ログファイル（アクセスログ、認証ログ、管理操作ログ等）をエクスポートすることができます。</p> <p>※バックアップされたログファイルはエクスポートできません。</p> <p>※アーカイブされたログもバックアップする必要がある場合は、「ログ管理」の「ログの保存」からダウンロードしてください。</p>
ログファイルのインポート	<p>ログファイルをインポートすることができます。</p> <p>※既存ログ（アクセスログ、認証ログ、管理操作ログ）がすべて削除されます。</p>

注：データベースおよび設定ファイルは自動ではバックアップされませんので、定期的にバックアップを取得するようにしてください。

3.7. サーバー設定

「サーバー設定」タブで管理は以下項目が管理できます：

サーバー設定	認証システムのタイムアウト値やポートの設定などを行うことができます。
SSL 証明書	SSL 証明書をインストールすることで HTTPS による通信を行うことができますようになります。
IP フィルタ	アクセスを禁止する「ブラックリスト」、アクセスを許可する「ホワイトリスト」の設定が行えます。
ライセンス	ライセンスの内容を確認することができます。
サーバーの再起動	認証システムの再起動を行えます。

3.7.1. サーバー設定

「サーバー設定」では、トークン認証タイムアウトや接続タイムアウト、認証方法、サービス拒否 (DoS) 攻撃防止などの設定を変更することができます。

SecureVisit
Web Authentication System

Help Logout
Server Time:2021-09-08 16:10:35

ユーザー管理USBトークン管理アクセス権限設定端末管理ログ管理認証DB・設定ファイルサーバー設定

サーバー設定SSL証明書IPフィルタライセンスサーバーの再起動

サーバー設定

IPアドレス*

サーバーのIPアドレスです。

192.168.129.176

ポート*

サーバーの待ち受けポートです。一般的にHTTPの場合は「80」、HTTPSの場合は「443」です。

443

デフォルトドメイン名*

サーバーのドメイン名です。(例: example.com)

www.ftsafe.co.jp

トークン認証タイムアウト*

USBトークンの再認証までの時間です。認証した後にトークン差し込んでいない状態で再認証を行うまでの秒数を設定します。

0

秒

接続タイムアウト*

ユーザー認証状態の再確認までの時間です。再確認までの分数を設定します。

10

分

ユーザーIDの入力

ユーザーIDを「入力させる」場合は、入力させたユーザーIDとUSBトークンの割り当て関係のチェックを行います。「入力させない」場合は、ユーザーにユーザーIDを入力させない、USBトークンからユーザーIDを判別します。「前回の入力を入力を記憶できるようにする」場合は、前回入力したユーザーIDの保存と自動入力ができるようになります。(デフォルト: 入力させる)

入力させる

☐ 前回の入力を入力を記憶できるようにする

パスワード認証

パスワード認証の設定です。「する」にした場合は、ユーザーにパスワードを入力させ、このサーバーで認証を行います。「しない」にした場合は、このサーバーでパスワードのチェックを行いません。(デフォルト: しない)

しない

レスキューパスワードの使用

「する」にした場合は、レスキューパスワードで認証できるようになります。(デフォルト: しない)

しない

レスキューパスワード入力のリトライ回数です。

10

回

端末限定

「端末限定」にした場合は、登録された端末でどのユーザーでも認証できるようになります。「端末とユーザー限定」にした場合は、ユーザーごとに制限された端末で認証できるようになります。(デフォルト: しない)

しない

☐ 端末認証を十分条件とする

OTP認証

OTP認証機能の有効/無効を選択します。(デフォルト: 無効)

無効

サービス拒否 (DoS) 攻撃*

サービス拒否 (DoS)攻撃の検知と遮断に関する設定です。(デフォルト: 毎1秒間同一IPから166回以上のアクセスが発生しますとDoS攻撃として検知し、当該IPから166回以上のアクセスを遮断する)

1秒間同一IPから

10000

回以上のアクセスが発生しますとDoS攻撃として検知し、当該IPから設定した回数以上のアクセスを遮断する

クライアントIPの取得

☐ HTTPヘッダからクライアントIPを取得する

(注意: 変更を有効にするためにサーバーの再起動が必要です。)

更新

IP アドレス※	サーバーの待ち受け IP アドレスの設定を行えます。
ポート※	サーバーの待ち受けポートの設定を行えます。一般的に HTTP の場合は「80」、SSL の場合は「443」を利用します。
デフォルトドメイン名※	サーバーの DNS 名の設定を行えます。
トークン認証タイムアウト※	USB トークンが外れた後から再認証するまでの間隔を指定します。認証後 USB トークンが外れ、このタイムアウト時間通過すると、USB トークンが挿入されなければ接続が強制的に切断されます。 設定範囲：-1～300 秒（-1：無制限）
接続タイムアウト※	一旦認証成功してから再認証するまでの間隔を指定します。認証成功してからこのタイムアウト時間を経過すると接続が強制的に切断されます。 設定範囲：1～120 分
ユーザーID の入力	認証する際に、ユーザーID を入力させるか否かを設定します。ユーザーID に「入力させる」を選択した場合は、入力させたユーザーID と USB トークンの割り当て関係のチェックを行います。「入力させる」を選択した場合、「前回の入力を記録できるようにする」にチェックを入れることができます。「前回の入力を記録できるようにする」にチェックを入れると、前回入力したユーザーID が記録され、次回アクセスする際、ユーザーID が自動的に表示されます。「入力させない」を選択した場合は、ユーザーID を入力させません。
パスワード認証	認証システムでパスワード認証を行うか設定します。パスワード認証を「する」場合は、USB トークンによる認証以外に、パスワード認証も行います。
レスキューパスワードの使用	認証システムでレスキューパスワード認証を行うか設定します。レスキューパスワード認証を「する」場合は、レスキューパスワードを設定されたユーザーはトークンを挿入せずに、レスキューパスワードのみで認証できます。リトライ回数は一つのセッション中に数回連続して誤ったレスキューパスワードを入力した時、数秒間遮断することができます。（遮断時間は DoS 攻撃と同じです）
端末限定	「端末限定」にした場合は、登録された端末でどのユーザーでも認証できるようになります。「端末とユーザー限定」にした場合は、ユーザー毎に制限された端末で認証できるようになります。（デフォルト：しない）
OTP 認証	OTP 認証の設定です。「する」にした場合は、ユーザーに OTP を入力させ、認証を行います。「しない」にした場合は、OTP のチェックを行いません。（デフォルト：しない）OTP 管理センターが発行した「xxx.acf」ファイルをアップロードします。（FOAS のマニュアルをご参照ください）
サービス拒否（DoS）攻撃※	サービス拒否（DoS）攻撃防止の設定を行えます。設定された単位時間内に同一 IP から設定された回数以上のアクセスが発生すると DoS 攻撃とみなし、当該 IP から設定した回数以上のアクセスを遮断することができます。

	※設定する回数は「60000」に設定することを推奨しています。 「60000」以下に設定した場合、画面表示が一部欠けることがあります。
クライアント IP の取得※	HTTP ヘッダからクライアント IP を取得するか設定します。チェックした場合は、HTTP ヘッダからクライアント IP を取得し、ログなどにクライアント IP として出力します。 ※クライアント側がプロキシサーバー経由して SecureVisit サーバーにアクセスしようとする、HTTP ヘッダからプロキシサーバー IP を取得し、ログなどにプロキシサーバー IP として出力します。

(※は必須フィールドです)

注：設定変更後はサーバーの再起動が必要になります。サーバーの再起動は「サーバーの再起動」から行えます。

3.7.2. SSL 証明書

「SSL 証明書」では、認証システムで HTTPS（SSL）による通信を行うのに必要な証明書をインポートすることができます。サーバー証明書をインポートするには、「SSL サーバー証明書」に X.509 PEM 形式の証明書を貼り付けてください。また、証明書にパスワードが設定されている場合は、「証明書のパスワード」にパスワードを入力します。設定後は「実行」をクリックすることで証明書がサーバーへインポートされます。

The screenshot shows the 'SSL 証明書' (SSL Certificate) configuration page in the SecureVisit management interface. The page includes the following sections:

- SSL 通信**: Set to '有効' (Enabled).
- TLS モード選択**: Set to 'TLS1.2+TLS1.3'.
- CA 証明書**: Field for 'CA 証明書の入力' (CA Certificate Input).
- SSL サーバー証明書**: Field for 'サーバー証明書の入力' (Server Certificate Input).
- 証明書のパスワード**: Field for 'SSL サーバー証明書のパスワード' (SSL Server Certificate Password).
- 失効証明書リスト**: Field for '失効証明書のリスト' (Expired Certificate List).
- 証明書チェーンの長さ**: Set to '1'.
- 許可する暗号化アルゴリズム**: Field for '許可する暗号化アルゴリズム' (Permitted Encryption Algorithms).
- TLS1.3 許可する暗号化アルゴリズム**: Field for 'TLS1.3 許可する暗号化アルゴリズム' (TLS1.3 Permitted Encryption Algorithms).
- クライアント認証モード**: Set to '0'.

At the bottom right, there is a green '実行' (Execute) button.

SSL 通信 ※	SSL 通信を行うか設定を行います。SSL 通信をする場合は「有効」を選択します。
TLS モード選択	SSL 通信プロトコルを選択できます。TLS1.2/TLS1.2+TLS1.3/TLS1.3

CA 証明書	<p>認証局 CA の証明書の入力欄です。X.509 PEM 形式の証明書を貼り付けてください。</p> <p>中間証明書も利用する場合、中間証明書の内容をルート証明書の下に貼り付けてください。</p> <p>例：</p> <pre>-----BEGIN CERTIFICATE----- MIIDeTCCAmGg... (ルート証明書の内容) -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- MIIebzCCA1egAwI... (中間 CA 証明書の内容) -----END CERTIFICATE-----</pre>
SSL サーバー証明書	<p>SSL 通信を行うのに利用するサーバー証明書の入力欄です。X.509 PEM 形式のサーバー証明書を貼り付けてください。</p> <p>※SSL サーバー証明書と秘密鍵が別々で生成された場合は、二つの内容を連続して貼り付ける必要があります。</p> <p>※※秘密鍵は DES3 で暗号化された場合、内容を復号してから貼り付けてください。</p> <p>中間証明書も利用する場合、中間証明書の内容を SSL サーバー証明書と秘密鍵の間に貼り付けてください。</p> <p>例：</p> <pre>-----BEGIN CERTIFICATE----- MIIGgTCCBWmgA... (SSL サーバー証明書の内容) -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- MIIebzCCA1egAwI... (中間 CA 証明書の内容) -----END CERTIFICATE----- -----BEGIN RSA PRIVATE KEY----- MIIEpQIBAAKCAQ... (秘密鍵) -----END RSA PRIVATE KEY-----</pre>
証明書のパスワード	証明書のパスワード入力欄です。証明書にパスワードが設定されていない場合は空白のままにします。
失効証明書リスト	<p>認証局 CA の発行した証明書失効リスト(CRL)を指定します。X.509 PEM 形式の証明書失効リストを貼り付けてください。</p> <p>※失効証明書がない場合、初期設定値のままで設定してください。</p>
証明書チェーンの深さ※	<p>クライアント証明書の検証時に、サーバーがフォローできる証明書チェーンの深さを指定します。</p> <p>通常、CA によって直接署名された証明書だけを信用するので、「1」を設定してください。</p> <p>中間証明書を利用する場合、「2」を設定してください。</p>
許可する暗号化アルゴリズム	クライアント側が使用できる暗号化方式を指定します。優先度の高い順に区切り文字‘:’を使用して指定します。一般的にデフォルト設定のままで結構です。

TLS1.3 許可する暗号化アルゴリズム	<p>「TLS モード選択」項目が「TLS1.2+TLS1.3」または「TLS1.3」に設定されている場合、クライアント側が使用できる暗号化方式を指定します。優先度の高い順に区切り文字「:」を使用して指定します。一般的にデフォルト設定のままで結構です。</p> <p>デフォルトは以下の通りです。</p> <p>TLS_AES_128_GCM_SHA256: TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256 :TLS_AES_128_CCM_SHA256:TLS_AES_128_CCM_8_SHA256</p>
クライアント認証モード	<p>証明書認証方式を使用する際に、クライアントに対して何を確認するかを設定します。</p> <p>「0」: 認証を必要としない。</p> <p>「1」: クライアントが合法的な証明書を提示するかもしれない。</p> <p>「2」: クライアントが合法的な証明書を提示しなければならない。</p> <p>「3」: クライアントが合法的な証明書を提示するかもしれない、しかし、サーバーに格納している証明書は、合法的な認証局(CA)が発行したものでなくてもよい。</p>

(※は必須フィールドです)

注：

- 1、SSL 通信を「有効」にした場合は、「サーバー設定」のポートを「443」に設定してください。
- 2、設定に関しては [4.2.4SSL 証明書を設定したら、サーバーの再起動にて、“停止中”となる] を参照してください。

3.7.3. IP フィルタ

「IP フィルタ」では、ブラックリスト及びホワイトリストを定義することができます。ここで設定された IP は、他のアクセス設定よりも優先的に参照されます。

「ブラックリスト」:

アクセスを禁止する IP アドレスのリストです。ブラックリストに登録された IP アドレスからアクセスすることはできなくなります。ブラックリストを有効にするには、「ブラックリスト機能を有効にする（ブラックリストの IP アドレスからのアクセスを禁止する）」のチェックを入れます。チェックを入れない場合は、「禁止する IP アドレス」を設定しても無効になります。

ブラックリスト機能を有効にして、クライアントの IP アドレスが「禁止する IP アドレス」に登録された場合、またはクライアントの IP アドレスが「禁止する IP アドレス」と「許可する IP アドレス」に両方とも登録された場合は、空白画面が表示されます。

「ホワイトリスト」:

アクセスを有効にする IP アドレスのリストです。ホワイトリストに登録された IP アドレスからのアクセスは以下の設定値によるアクセス制限を行うことができます。ホワイトリストを有効にするには、「ホワイトリスト機能を有効にする」のチェックを入れます。チェックを入れない場合は、「許可する IP アドレス」を設定しても無効になります。

ホワイトリスト機能を有効にして、「ホワイトリストの IP アドレスからのアクセスのみを許可する」が

チェックされていて、クライアントの IP アドレスが「許可する IP アドレス」ではない場合は、空白画面が表示されます。

ホワイトリストの IP アドレスからのアクセスのみを許可する	<p>ホワイトリストに登録された IP アドレスからのアクセスのみの接続を許可します。正しく認証後にアクセスが可能になります。</p> <p>※例として、A はホワイトリストに登録された IP アドレスであり、B は未登録の IP アドレスである場合、A からのアクセスは認証画面が表示され、正しく認証後にアクセスできるが、B からのアクセスは認証画面が表示されない上、アクセス不可になります。</p>
ホワイトリストの IP アドレスからのアクセスは認証を行わない	<p>ホワイトリストに登録された IP アドレスからのアクセスは、認証を行わずにアクセスができます。</p> <p>※例として、A はホワイトリストに登録された IP アドレスであり、B はホワイトリストに未登録の IP アドレスである場合、A からのアクセスは認証せずにアクセスできるが、B からのアクセスは認証画面が表示され、正しく認証されてから、アクセスが可能になります。</p>
ホワイトリストの IP アドレスからのアクセスを許可し、それ以外のアクセスは認証を行わない	<p>ホワイトリストに登録された IP アドレスからのアクセスは認証を行う必要があります。正しく認証後に、アクセスが可能になります。</p> <p>※例として、A はホワイトリストに登録された IP アドレスであり、B はホワイトリストに未登録の IP アドレスである場合、A からのアクセスは認証画面が表示され、正しく認証されてからアクセスできるが、B からのアクセスは認証せずにアクセスができます。</p>

ブラックリスト・ホワイトリスト共に半角ハイフン「-」で区切ることによってアドレス範囲の指定も可能です。

注：範囲指定を行う場合は、「100.111.112.0-100.111.112.128」の様に定義します。

ブラックリスト・ホワイトリストに IP アドレスを定義する場合は、各「IP アドレス」に IP アドレスを入力し、「追加」をクリックします。ブラックリストの場合は「禁止する IP アドレス」に、ホワイトリストの場合は「許可するアドレス」に先ほど入力した IP アドレスが登録されたことを確認し、「更新」をクリックします。

ブラックリスト・ホワイトリストに同じ IP アドレスを定義した場合、ブラックリストの設定が優先的に確認され、当該 IP アドレスにアクセスすることができなくなります。

注：設定変更後はサーバーの再起動が必要になります。サーバーの再起動は「サーバーの再起動」から行えます。

3.7.4. ライセンス

認証サーバーのライセンス内容を確認することができます。カスタム ID、登録可能ユーザー数、登録可能トークン数、ライセンス発行日付、ライセンスの有効期限が表示されます。



注：ライセンスの有効期限が切れた場合、または登録したユーザーやトークンが登録可能ユーザー数や登録可能トークン数を超えた場合、管理画面のすべての画面に、以下のような警告メッセージが表示されます。（例：ライセンス期限が過ぎた場合）

ライセンスの有効期限が過ぎています。認証サーバーが起動／再起動できなくなります。

3.7.5. サーバーの再起動

「サーバーの再起動」では、認証システムの再起動を行うことができます。一部の設定では、適用後にサーバーの再起動が必要になります。設定後に再起動が必要な項目は、各設定画面の画面下部に表示されています。



バージョン	認証サーバープログラムのバージョン番号が表示されます。
サーバー状況	認証サーバープロセスの状況が表示されます。
サーバーの再起動	クリックすることで認証サーバーのサービスを再起動します。OS の再起動

は行いません。

注：サーバーの再起動時にはセッションが切断されます。

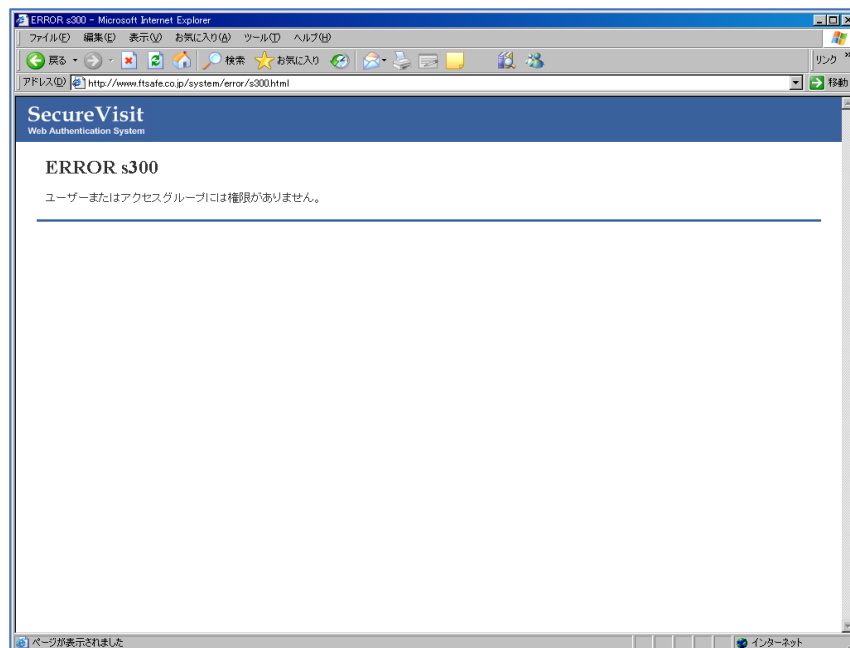
第4章 トラブルシューティング

本章では以下のトピックについて説明します：

- ❖ エラー一覧
- ❖ 最も頻繁に起こる問題およびその解決方法

4.1. エラーメッセージ一覧

認証サーバーへアクセスした際にエラーが発生すると、以下の様なエラーメッセージ（HTML）がブラウザに表示されます。エラーには、HTTP のエラーと認証サーバー側で発生したエラーの 2 つに分類されます。



以下は HTTP エラーの一覧です。

エラー番号	エラーメッセージ	エラーの意味
404	ページが見つかりません。	要求したコンテンツが存在しません。
405	HTTP メソッドは使用禁止です。	使用禁止されている HTTP メソッドがあります。
406	要求した URL の長さは設定した	要求した URL の長さが設定値を超えました。

	長さを超えました。	
500	サーバーの内部エラーです。	サーバーの内部エラーが発生しました。
503	サーバーがビジーです。	サーバーは高負荷のため、要求に応答できません。
504	サーバー通信エラーです。	サーバーはバックエンドサーバーに接続できません。 (バックエンド WWW サーバー、DNS サーバー)

注：一覧以外にも Web サーバー側で発生したエラーが表示されることがあります。

以下は認証サーバーのエラーコードの分類です。

エラー番号	エラーメッセージ
s1xx	ユーザーID またはパスワード関連のエラーです。
s2xx	USB トークン関連のエラーです。
s3xx	アクセス権限関連のエラーです。
s4xx	認証関連のエラーです。
s5xx	OTP 関連のエラーです。
s8xx	その他のエラーです。

以下は認証サーバーのエラーコード一覧です。

エラー番号	エラーメッセージ	エラーの意味
s102	ユーザーID またはパスワードが間違っています。	ユーザーリストに該当するユーザーID のパスワード（またはレスキューパスワード）が間違っています。
s103	ユーザーID またはパスワードが無効です。	ユーザーID が無効のため、認証に失敗しました。
s104	ユーザーID またはパスワードが無効です。	ユーザーID が存在していません。
s105	ユーザーID またはパスワードが有効期間外です。	ユーザーID は有効期間外です。ログオン用ユーザーID は有効期間範囲外のため、ログオン認証に利用できません。
s106	ユーザー所属したグループが有効期間外です。	ユーザーが所属しているグループの有効期間が期間外になっています。
s107	ユーザーID またはパスワードが有効期間外です。	ユーザーID のレスキューパスワードの有効期間が期間外になっています。
s112	ユーザーがまだ登録されていません。	ユーザーの状態が「未登録」のため、トークンと紐付きません。
s200	USB トークンの有効期限が過ぎています。	トークンの有効期限が有効期間外になっています。
s201	USB トークンが無効になっています。	トークンが無効になっています。
s202	利用可能な USB トークンが登録されていません。	ユーザーに有効なトークンが割り当てられていません。
s300	ユーザーまたはアクセスグループには権限がありません。	アクセス権限の無いディレクトリやファイルにアクセスしました。
s400	認証に失敗しました。USB トークンの接続や通信環境を確認してください。	認証に失敗しました。トークンの接続や通信環境を確認してください。
s401	認証が中断されました。	認証の前に認証操作が中止されました。
s500	OTP 認証失敗。	OTP の認証に失敗しました。
s503	入力された OTP が無効になりました。	OTP の認証に失敗しました。
s504	PIN 番号が無効になりました。	PIN 認証失敗しました。

s505	該当の OTP トークンは紛失されています。	OTP トークンが紛失されたので、管理者はトークンの状態を「紛失」に変更しました。
s506	該当 OTP トークンがロックされました。	トークンがロックされました。
s507	該当 OTP トークンがログアウトされました。	OTP トークンがログアウトされました。
s508	該当の OTP トークンは有効期間外です。	トークンの有効期間が切れました。
s509	該当の OTP トークンは同期作業を行う必要があります。	OTP トークンが認証サーバーと同期しないため、認証に失敗しました。
s800	コマンドバージョンが一致しません。	コマンドバージョンが一致しないため、認証を正しく行なうことができません。
s801	POST データがタイムアウトしました。	POST コマンドでデータをアップロード中にユーザーの再認証が要求され、サーバーに保存されていた POST データが廃棄されました。
s802	利用中のブラウザでこのシステムは利用できません。	サポート外のブラウザを利用しています。
s803	認証が中断されたため、ユーザーの操作がタイムアウトしました。	認証が中断されたため、ユーザーの操作がタイムアウトしました。
s804	この端末からのアクセスは許可されていません。	この端末は未登録のため、アクセスが禁止されています。

注：実際にブラウザへ表示されるのはエラー番号とエラーメッセージになります。

4.2. 最も頻繁に起こる問題およびその解決方法

4.2.1. 特定のクライアントから認証が成功できない

クライアント PC のシステム要件をご確認ください。本認証システムがサポートするクライアント OS は Windows10/Windows11、サポートするブラウザは Edge/Chrome92 以降です。

4.2.2. 保護された Web サイトの一部のページにアクセスできない

本認証システムは、一部のページが HTTP、一部のページが HTTPS のような Web サイトをサポートしていません。解決方法は、Web サイト全体を SSL 化（HTTPS を利用する）にしてから本認証システムで保護することです。

4.2.3. 認証画面が繰り返し再表示される

認証情報などを維持するために、本認証システムは Cookie を利用しています。クライアント PC の Edge/Chrome のプライバシー設定に「すべての Cookie をブロック」になっていないかをご確認ください。

4.2.4. SSL 証明書を設定したら、サーバーの再起動にて、“停止中”となる

SSL 証明書欄にコピーされた証明書は、PEM 形式の証明書かどうかを確認してください。

PEM 形式の内容は下記となります：

```
-----BEGIN CERTIFICATE-----  
...  
-----END CERTIFICATE-----  
-----BEGIN RSA PRIVATE KEY-----  
MIICXg.....（秘密鍵）.  
-----END RSA PRIVATE KEY-----
```

PEM 形式証明書が暗号化されているかどうかを確認してください。

秘密鍵は DES3 で暗号化されている場合、証明書の内容は下記となります：

```
-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
DEK-Info: DES-EDE3-CBC,...  
-----END RSA PRIVATE KEY-----
```

暗号化された場合、OpenSSL の下記コマンドを利用して、秘密鍵の内容を復号してくださ

い：

```
openssl rsa -in sslsev.key -out sslsev_new.key
```

※sslsev.key は秘密鍵の名前です。

※sslsev_new.key は復号化後の秘密鍵の名前です。

問題が解決できない場合、SecureVisit のエラーログの内容を確認してください。
/svisit/log/httpd-sv.error.log