

ワンタイムパスワード認証・Webサーバー — Powered BLUE 870 / OTP —



ワンタイム・パスワード認証対応のWebサイトを構築・運用
オールインワンの仮想アプライアンス
リバースプロキシ

ワンタイムパスワード認証の主なサービス



ワンタイムパスワードのWeb認証は

- Google
- Amazon
- Microsoft
- Facebook
- 仮想通貨のサイト インターネットバンキング etc

などのサービスで幅広く採用されています

Powered BLUE 870/OTP の特徴

インターネットサーバー機能

Web/Mail/DNS/FTP/ サーバー機能 & 認証機能を1台で運用
RedHat / CentOS 7.x (64bit) に対応

Webサイトの2要素認証機能

ワンタイムパスワード対応(発行・管理・認証)
ID/パスワード(発行・管理・認証)

仮想・クラウド対応

仮想対応 VMWare / Hyper-V

クラウド対応 AWS / Azure / VPS / 他

Webアクセス時のワンタイムパスワード認証



ワンタイムパスワード & ID/パスワードの
2要素認証機能付属のWebサーバーを簡単に構築 / 運用

汎用のトークンでの利用に対応



ユーザー側

- 高額なハードウェア・トークンは不要
- OSS/無償のソフトウェアトークン から利用出来ます

OSSや無償の主なソフトウェアトークン

製品	iOS Android	PC	価格	備考
Google Authenticator	○		無償	OSS
IISmartKey	○		無償	日本語対応
Authy	○	○ Windows/Mac/Linux	無償	
WinAuth		○ Windows	無償	

他社のワンタイムパスワードのWeb認証でも利用が可能



OSS/無償のソフトウェアトークンで使えるサービスなど

- Google
- Amazon
- Microsoft
- Facebook
- 仮想通貨のサイト インターネットバンキング etc
- **Powered BLUE 870/OTP**

秘密鍵（共有鍵）のフロー



ワンタイムパスワードの同期



ワンタイムパスワード



ワンタイムパスワードユーザーの管理

The screenshot shows the 'Powered BLUE' management interface. The top navigation bar includes 'サーバの管理', 'サイトの管理', 'アップデート', '個人プロフィール', and 'ライセンス管理'. The left sidebar lists various management options, with 'ユーザーの管理' expanded to show 'ユーザーのリスト', 'インポート', and 'エクスポート'. The main content area is titled 'ユーザー設定の修正 - suzuki' and contains a form with the following fields:

氏名	鈴木 二郎
よみがな	すずき じろう
新しいパスワード (省略可)	it's WAY too short (再度入力)
最大許容ディスク容量	20 (1 - 500)
ワンタイムパスワード認証	<input checked="" type="checkbox"/>
サイト管理者	<input type="checkbox"/>
サスペンド	<input type="checkbox"/>
備考 (省略可)	

At the bottom of the form are buttons for '保存' (Save) and 'キャンセル' (Cancel). A footer message states: 'このサイトのワンタイムパスワード(OTP)認証を有効にします。' (Enable one-time password (OTP) authentication for this site.)

- ワンタイムパスワードユーザーの一括登録

簡単なQRコードの管理

ワンタイムパスワード認証設定 - suzuki

基本 詳細 管理(QRコード)

オプション

共有鍵	<input checked="" type="radio"/> 文字列およびQRコードで表示する
共有鍵	LIXDHFGTZNUTKNAOR44FZDB
ワンタイムパスワード	<input checked="" type="radio"/> 答えを表示する



リセット

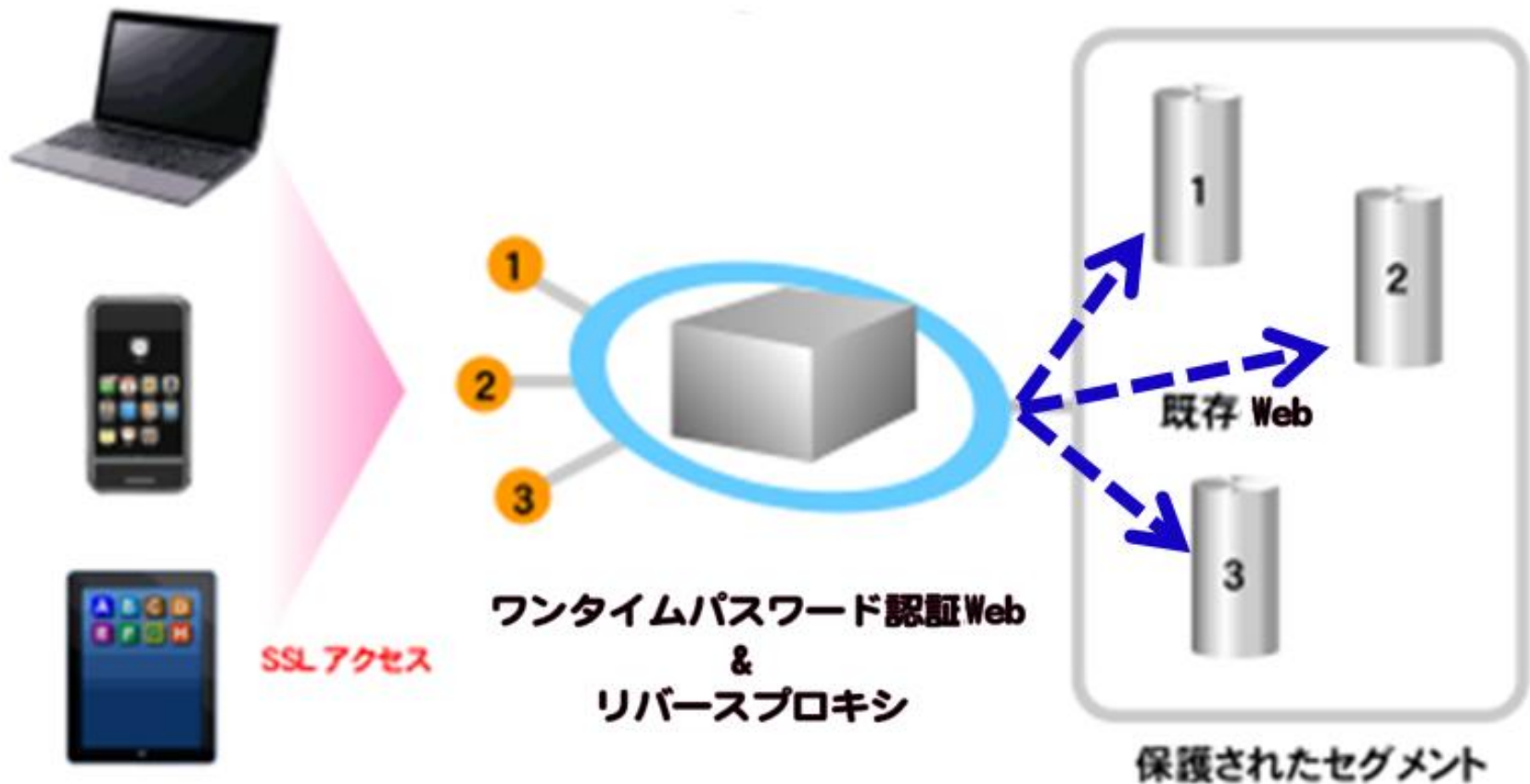
- 簡単なQRコードの管理
- スマフォ端末の機種変更をした場合の対応も簡単
- PCから利用の場合のコードの発行にも対応

Webアクセス時の手順



- ワンタイムパスワードを表示
- Webへアクセス / 2要素認証
- アカウント / ワンタイムパスワード / パスワード入力













ワンタイムパスワード認証Web + リバースプロキシ



■ 既存Webサーバー連携

■ ワンタイムパスワード + リバースプロキシ 運用に対応

リバースプロキシ 設定例

リバースプロキシ設定のリスト - reverse-no1.mubit.com			
ローカルパスの追加			6 エントリ
ローカルパス/SSLポート ▼	リモート URL	オプション	操作
ローカルパス: /	http://owncloud-mars.mubit.jp/owncloud/		 
ローカルパス: /fileblog/	http://demo.teppinet/fileblog/		 
ローカルパス: /mubit/	http://220.110.17.99/		 
ローカルパス: /proself/	https://proself.fpu.ac.jp/proself/		 
ローカルパス: /res/	http://demo.teppinet/res/		 
ローカルパス: /webmail/	http://roundcube-mars.mubit.jp/webmail/		 

 変更を適用する

■ グループウェア・Webメール

- サイボウズ
- デスクネッツ
- Active! mail
- RoundCube
- NIコラボスマート
- Aipo

■ ワークフロー

- X-point
- 楽々Workflow
- NIコラボスマート
- eValue NS
- Power egg
- wawaOffice
- NTTデータ イントラマート ワークフロー

■ オンラインストレージ

- FileBlog
- Proself
- ownCloud

■ 他

- WordPress
- Zabbix
- ホームページ

ワンタイムパスワード・仕様

項目	内容
トークン Format	Google Authenticator Format FreeOTP Format
対応	TOTP(時間ベース)有効時間指定 桁数指定 HOTP(回数ベース)
共有鍵発行	QRコード(画像・2次元バーコード) 文字列 リセット機能・再発行機能
OTPのWeb認証	Webサイト/ディレクトリ単位 ユーザー単位
2要素認証	ワンタイムパスワード認証 & ID / パスワード認証

動作環境

OS	RedHat 7.x (64bit) CentOS 7.x (64bit)
仮想環境	VMWareESXi 5.1 / 5.5 / 6.0 / 6.5 Hyper-V 7.X
クラウド環境	AWS / EC2 Azure / Microsoft FUJITSU Cloud Service for OSS / 富士通 Enterprise Cloud / NTT communications VPS / WebArena / NTTPC VPS / ALTUS / GMOクラウド
スペック	1 Core(min) / 1024MB mem (min) / 20GB HDD (min) / Ethernet x 1(min)

管理画面

Powered BLUE 7

サーバの管理 | サイトの管理 | アップデート | 個人プロフィール | ライセンス管理

サーバの管理者
ネットワークサービス
ウェブ
FTP
電子メール
DNS
シェル
データベース
セキュリティ
システムの設定
保守
利用状況
アクティブモニタ
オプション
サポート情報

ウェブの設定

基本 | **セキュリティ** | 詳細

セキュリティ設定

バージョン情報を公開しない	<input checked="" type="checkbox"/>
PHPヘッダを応答しない	<input checked="" type="checkbox"/>
HTTP Traceメソッドを無効にする	<input checked="" type="checkbox"/>
SSLセキュアレベル	TLS1.2以上を使用する(強レベル) ▼

保存

? セキュリティに関する設定を行います。

- 1) 日本語・英語の2か国語対応
- 2) パッチなどの自動アップデート機能

常時SSL化対応 セキュリティの強化

■ SNI (Server Name Indication) 機能

The screenshot shows the 'ウェブの設定' (Web Settings) page with tabs for '基本' (Basic), 'セキュリティ' (Security), and '詳細' (Advanced). Under the 'セキュリティ' tab, the option '名前ベースのSSL仮想サイトを使う' (Use name-based SSL virtual sites) is selected. Below it, the checkbox 'SNIを有効にする' (Enable SNI) is checked.

IPアドレス1個で、全WebサイトのSSL化に対応

■ Webバージョンの非公開やSSLセキュアレベルの指定機能

The screenshot shows the 'ウェブの設定' (Web Settings) page with tabs for '基本' (Basic), 'セキュリティ' (Security), and '詳細' (Advanced). Under the 'セキュリティ' tab, the 'セキュリティ設定' (Security Settings) section is visible. The following settings are shown:

バージョン情報を公開しない	<input checked="" type="checkbox"/>
PHPヘッダを応答しない	<input checked="" type="checkbox"/>
HTTP Traceメソッドを無効にする	<input checked="" type="checkbox"/>
SSLセキュアレベル	TLS1.2以上を使用する

■ HSTS (HTTP Strict Transport Security)対応

httpでアクセスを受けると、次回以降はhttpsでの接続に切り替えて、通信経路の安全を確保する機能

■ SELinux対応(セキュアOS)

The screenshot shows the 'SELinuxの設定' (SELinux Settings) page with tabs for '基本' (Basic) and '詳細' (Advanced). The checkbox 'SELinuxを有効にする' (Enable SELinux) is checked.

ひとり情室対応 簡単運用

システムの動作状況 - 概要	
4 エントリ	
▼ コンポーネント名	▼ 詳細
● CPU の使用状況	🔍
● ディスクの使用状況	🔍
● ネットワークの状態	🔍
● メモリの使用状況	🔍

サービスの動作状況 - 概要	
8 エントリ	
▼ コンポーネント名	▼ 詳細
● DNS サーバ	🔍
● FTP サーバ	🔍
○ SNMP サーバ	🔍
● Telnet サーバ	🔍
● ウェブサーバ	🔍
● サーバデスクトップ	🔍
● サーバ・ライセンス	🔍
● 電子メールサーバ	🔍

その他の動作状況 - 概要	
2 エントリ	
▼ コンポーネント名	▼ 詳細
● アンチウイルス・ゲートウェイ	🔍
● 電子メールプラス	🔍

色と意味: ○ 情報がないか、監視が無効に設定されています。

● 正常に動作中

● 問題発生

● 深刻な問題発生

サーバーのモニタリング&サービスの自動再起動

SSLサーバー証明書 Let's Encrypt (フリープラグイン)



Let's Encrypt フリーSSLサーバ証明書 - sample.mubit.tv	
	基本 詳細 ログ
サイト管理を許可する	<input type="checkbox"/>
自動更新	<input checked="" type="checkbox"/>
証明書情報	
管理用電子メール	
ドメイン	
状況	webServerIsDisabledNow
フリープラグインの情報	
URL	https://letsencrypt.org/

SSLサーバー証明書の自動更新対応

WordPress (フリープラグイン)



ユーザー名またはメールアドレス

パスワード

ログイン状態を保存する

ログイン

パスワードをお忘れですか？

ムービットのブログに戻る

ブログのリスト - www.mubit.tv					
ブログを追加する		ユーザブログを追加する		7 エントリ	
ブログのパス	状況	操作			
ブログホーム	完了	✎	🗑️		
このサイトのディレクトリ /blog	完了	✎	🗑️		
このサイトのディレクトリ /blog-3	完了	✎	🗑️		
このサイトのディレクトリ /demo-blog	完了	✎	🗑️		
このサイトのディレクトリ /blog-2	完了	✎	🗑️		
ユーザ 'maeda' のホームディレクトリ /	完了	✎	🗑️		
ユーザ 'ootani' のホームディレクトリ /angels	完了	✎	🗑️		
ユーザ 'suzuki' のホームディレクトリ /	完了	✎	🗑️		

WordPressで構築したWebページに
2要素認証も設定出来ます

「Powered BLUE 870/OTP」おさらい

- ワンタイムパスワード認証（2要素認証）
社員 や 会員 向けの 専用 Web ページ
- 汎用 の ソフトウェアトークン 対応
導入コストが低い & 使い勝手がよい
- リバースプロキシ 対応
既存Web と 連携
- 仮想アプライアンス対応
すぐに運用 & メンテナンスが簡単

■ Powered BLUE 870 / OTP

<https://www.mubit.co.jp/sub/products/blue/b870-otp.html>

■ Powered BLUE 870 / OTP 設定例

<https://www.mubit.co.jp/pb-blog/?p=3593>

■ AWSでの構築 & 設定例

<https://www.mubit.co.jp/pb-blog/?p=3684>