

WordPress対応
常時SSL化とSSLクライアント認証に対応の
Webサイトを10分で構築&運用する方法の解説



会社概要

社名	株式会社ムービット
設立	1995年12月8日
所在地	東京都北区王子1-28-6
主な製品	Powered BLUE シリーズ アプリケーションサーバー (Linux) ソフトウェア開発

HTTPS

をランキング シグナルに
使用します

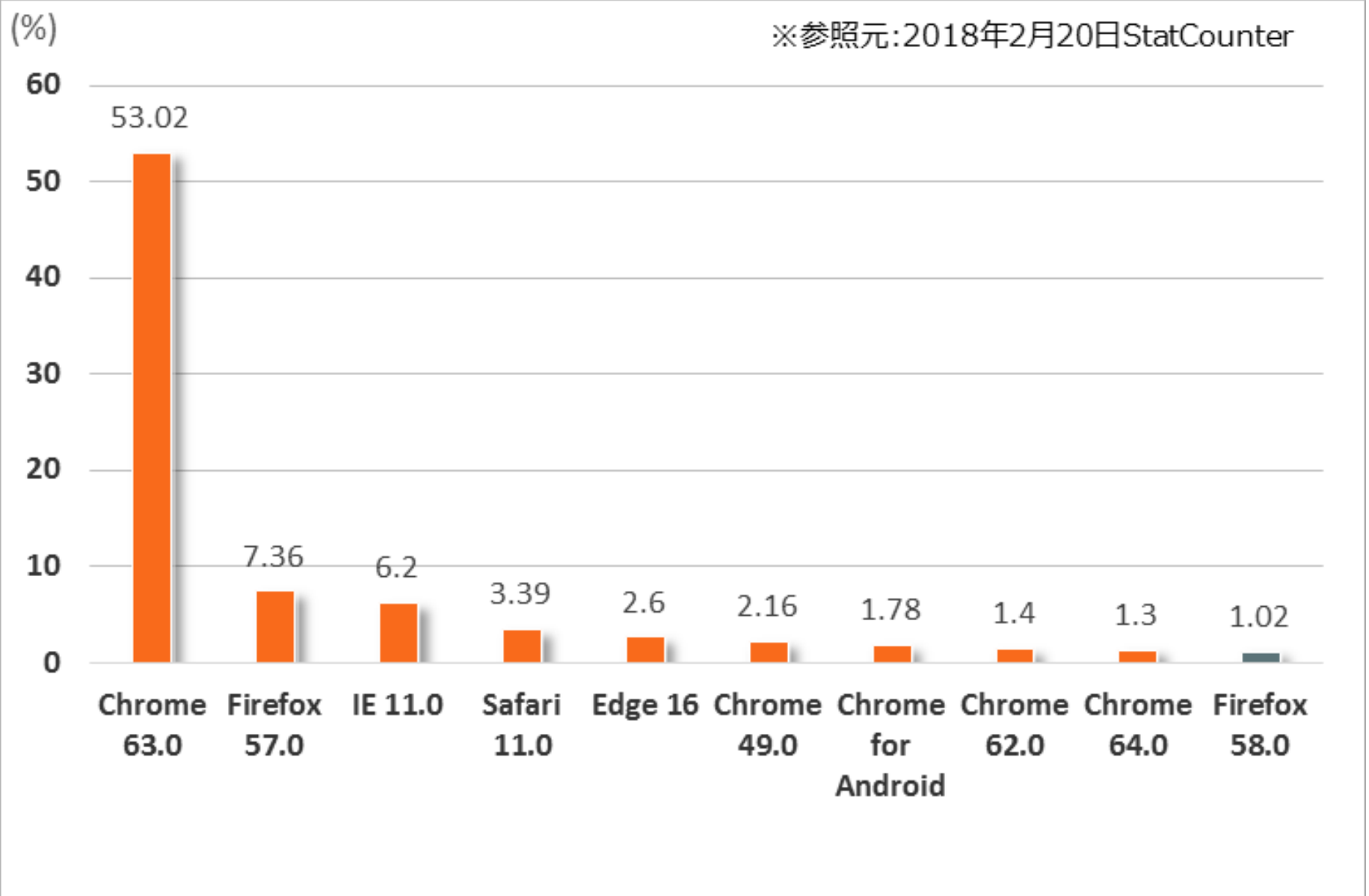
chrome

Googleは2018年7月にリリースの
「Chrome 68」から

「http://」で始まるすべてのWebサイトで
「保護されていません」警告を表示する

と発表しました。

ブラウザのシェア



SSL 未対応のWebサイト-2

ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(I) ヘルプ(H)

総務省 x +

www.soumu.go.jp

よく見るページ 新しいフォルダー Google

総務省 MIC Ministry of Internal Affairs and Communications

ご意見・ご提案 ENGLISH(TOP) ENGLISH(ICT POLICY)

アクセシビリティ 障害支援ツール

文字サイズの変更 小 標準 大

Google カスタム検索

総務省の紹介 広報・報道 政策 組織案内 所管法令 予算・決算 申請・手続 政策評価

ピックアップ フォトギャラリー 総務省重点施策

マイナンバー制度について

- (1) マイナンバー制度の概要 (内閣府)
- (2) マイナンバーを利用する行政手続で提出書類が省略できるようになります。(情報連携)(内閣府)

マイナンバーカードをつくってみませんか?

- (3) マイナンバーカードの申請方法(J-LIS)
- マイナンバーカードでこんなことができます!
- (4) マイナンバーカードの利活用方法

マイナンバー制度は様々なセキュリティ対策を講じています。

- (5) マイナンバー制度の安全対策(内閣府)
- (6) マイナンバーカードのセキュリティ対策
- (7) マイナンバー制度に便乗した不正な勧誘や個人情報の取得にご注意ください!

マイキーくん マイナちゃん

さらに詳しいことが知りたい場合には、**マイナンバー総合フリーダイヤル (0120-95-0178)** までお問合せください。

大臣・副大臣・政務官の動き

国の行政制度・運営

地方行財政

選挙 政治資金制度

情報通信 (ICT 政策)

国民生活と安心安全

総務省動画チャンネル

>>総務省SNS一覧はこちら

平成28年熊本地震関連情報

東日本大震災関連情報

SSL 対応のWebサイト

The screenshot shows a web browser window displaying the official website of the Ministry of Finance, Japan. The browser's address bar shows the URL <https://www.mof.go.jp/index.htm>, indicating a secure connection. The website header includes the text "財務省 Ministry of Finance, JAPAN" and navigation links for "English", "財務省FAQ", and "サイトマップ". A search bar is also present.

The main navigation bar features several buttons: "トップページ", "日本の財政を考える", "身近な税", "個人向け国債", "財務省について", "広報・報道", "統計", and a "YouTube" icon.

The content area is divided into several sections:

- 財務省の政策** (Ministry's Policy): A vertical list of policy areas including "予算・決算" (Budget/Accounts), "税制" (Tax System), "関税制度" (Customs System), "国債" (Government Bonds), "財政投融资" (Fiscal Investment and Financing), "国庫" (Treasury), "通貨" (Currency), "国有財産" (Public Property), "たばこ塩" (Tobacco/Salt), "国際政策" (International Policy), "政策金融・金融危機管理" (Policy Finance/Financial Crisis Management), and "財務総合政策研究所" (Research Institute for Comprehensive Financial Policy).
- 注目情報** (Spotlight Information): A list of recent news items with category tags like "予算・決算", "その他", "国債", "財政投融资", and "税制".
- 広報・報道** (Public Relations/Press): A list of events and publications such as "大臣等記者会見" (Ministerial Press Conference), "大臣談話・ステートメント" (Ministerial Statements), "週間予定" (Weekly Schedule), and "パンフレット・出版物" (Pamphlets/Publications).
- 調達情報** (Procurement Information): A list of procedures including "申請・届出等の手続案内" (Application/Notification Procedures), "情報公開・個人情報保護等" (Information Disclosure/Personal Information Protection), "法令適用事前確認手続" (Legal Application Confirmation Procedures), and "パブリックコメント" (Public Comments).
- 各種手続** (Various Procedures): A list of administrative processes.
- 統計** (Statistics): A section for statistical data.
- 財務省の基本情報** (Basic Information of the Ministry of Finance): A list of key personnel and organizational details, including "大臣・副大臣・政務官" (Minister/Deputy Minister/Secretary of State), "財務省について" (About the Ministry of Finance), "財務省の予算・決算" (Ministry Budget/Accounts), "審議会・研究会等" (Advisory Committees/Research Conferences), "法律/政省令/告示/通達等" (Laws/Regulations/Orders/Notices), "政策評価" (Policy Evaluation), "所管の法人" (Institutions under Supervision), "採用情報" (Recruitment Information), "その他の財務省の取り組み" (Other Ministry Initiatives), and "財務省の関連サイト" (Related Ministry Websites).

A video player is embedded in the center, showing a press conference by Masuda Naohiko (麻生大臣) on January 4th, with the caption "職員に向けて年頭挨拶を行う麻生大臣 (1月4日)".

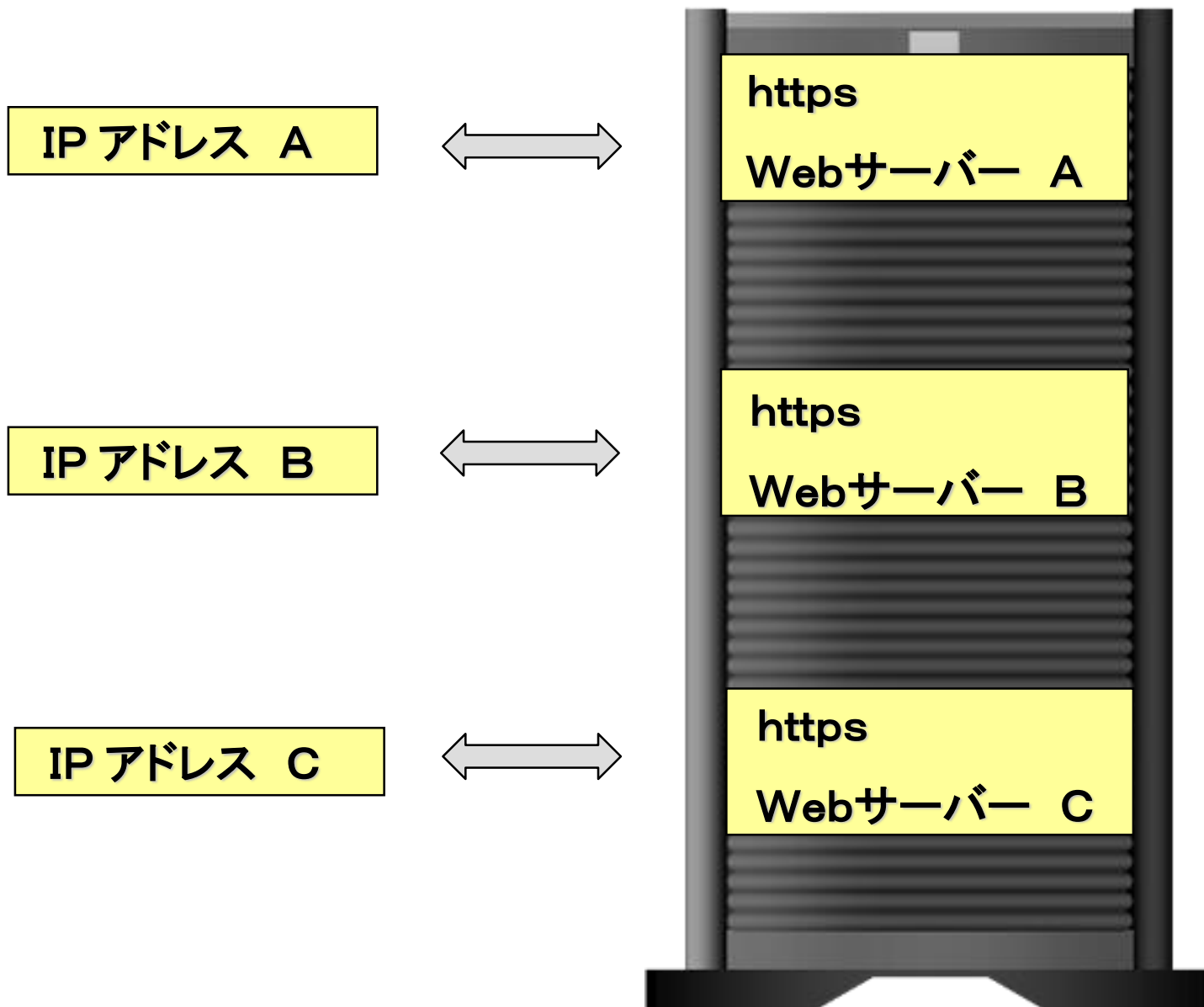
At the bottom, there is a "新着情報" (New Information) section and an "RSS一覧" (RSS List) button.

Webの常時SSL化の問題点

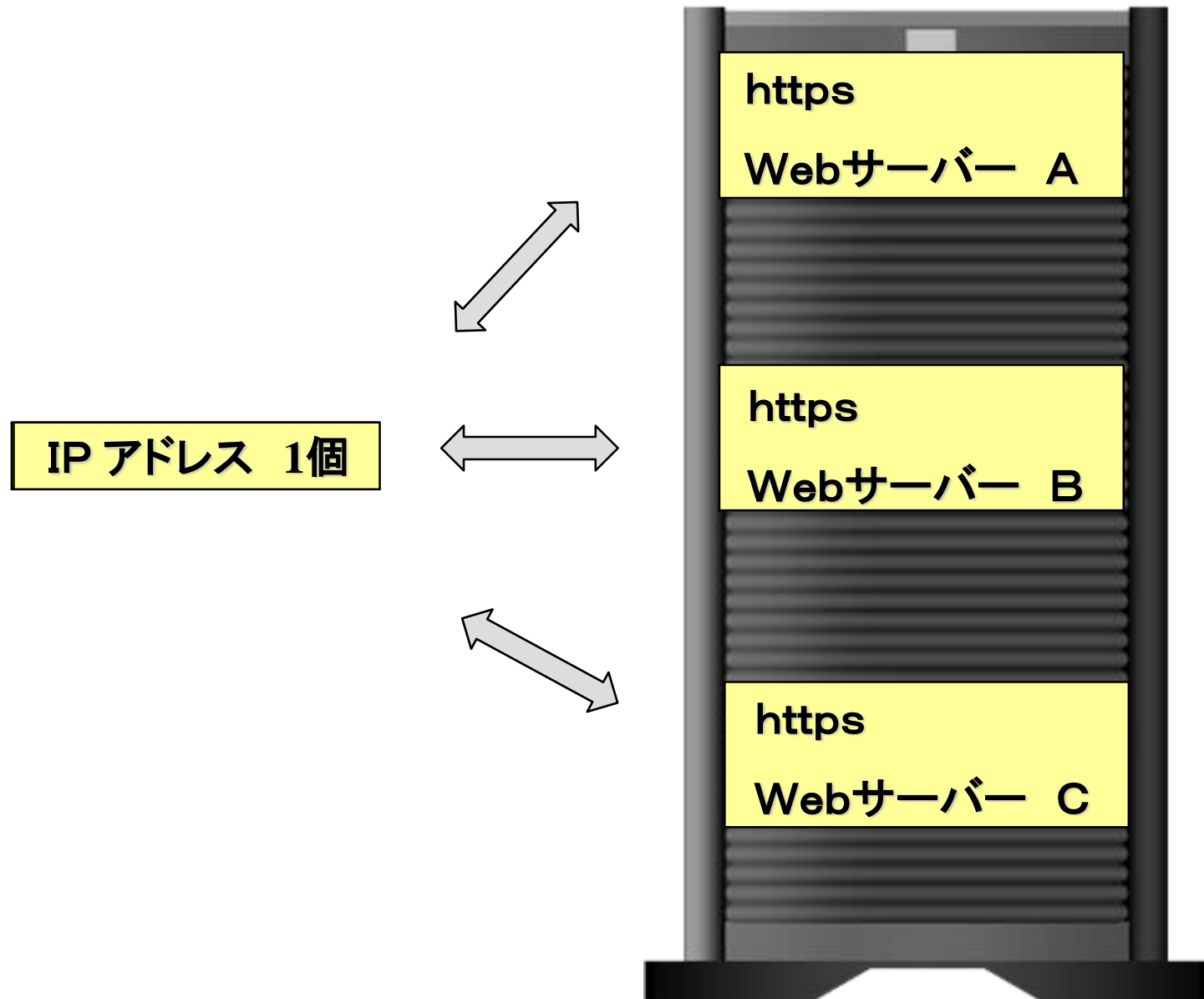
IP アドレス

Webサイトへの攻撃

IPアドレス と SSL化Webサーバーの関係



「SNI / Server Named Indication」対応のWebサーバー



通信経路のSSL暗号化 とWebサーバー



SSL証明書を使おう

■ SSLのサーバー証明書

- サーバーにインストール
- アクセス先のサーバーの身元を証明



■ SSLのクライアント証明書

- クライアントの機器にインストール
- アクセス元のクライアントの身元を証明



「SSLクライアント認証」での Webアクセス



2要素認証

- 1要素の認証

- ID / パスワード認証

- 2要素の認証

- SSLクライアント認証

SSL証明書発行元による相違

■ パブリック証明書

- シマンテックなど

公的にも利用

- 発行・失効

時間がかかる

- 有効期間

年単位

■ プライベート証明書

- 自社などで発行

私的な利用

- 発行・失効

迅速

- 有効期間

日・週・月・年単位

SNI 設定 Apache ssl.conf の場合

```
LoadModule ssl_module modules/mod_ssl.so
Listen 443
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl .crl
SSLPassPhraseDialog builtin
SSLSessionCache shmcb:/var/cache/mod_ssl/scache(512000)
```

```
.....
.....
```

SSLクライアント認証 Apache ssl.conf の場合

```
SSLCACertificateFile /etc/pki/exampleCA/cacert.pem
SSLCARevocationFile /etc/pki/exampleCA/crl.pem
<Directory /var/www/html/secret>
  SSLRequireSSL
  SSLVerifyClient require
  SSLUserName SSL_CLIENT_S_DN_CN
  Satisfy Any
  Allow from All
  SSLRequire %{SSL_CLIENT_S_DN_CN} in {"yone", "foo", "bar"}
</Directory>
```

```
.....
.....
```

サーバーの管理

コマンドラインでの管理
パッチの適用

数百枚の証明書の管理

発行
失効
配布

Powered BLUE 870 Webアプリケーションの特徴

インターネットサーバー機能

Web/Mail/DNS/FTP/ サーバー機能

リバースプロキシ-

Private CA 機能

SSLクライアント証明書管理

仮想・クラウド対応

仮想アプリケーション

動作スペック

OS	RedHat 7.x (64bit) CentOS 7.x (64bit)
スペック	1 Core(min) / 512MB mem (min) / 20GB HDD (min) / Ethernet x 1

「Powered BLUE 870 Webアプリケーション」運用環境

仮想アプリケーション

VMware / Hyper-V

アマゾン対応

AWS / EC2

クラウド対応

VPS

10分 で 運用開始

GMOクラウド・ALTUSの場合

仮想アプライアンスイメージのインポート

The screenshot shows the 'テンプレートの登録' (Template Registration) dialog box in the GMO CLOUD ALTUS BASIC interface. The dialog is centered over a blurred background of the dashboard. The dialog contains the following fields and options:

- * 名前: B870-nodhcp-20GB-fix-0214-No1
- * 説明: 370-nodhcp-20GB-fix-0214-No1.vhd
- * URL: 370-nodhcp-20GB-fix-0214-No1.vhd
- ゾーン: Basic_tky001 (dropdown)
- ハイパーバイザー: XenServer (dropdown)
- 形式: VHD (dropdown)
- OSの種類: Other (64-bit) (dropdown)
- 抽出可能:
- パスワード管理有効:
- 起動中のサイズ変更:
- HVM:

At the bottom of the dialog are two buttons: 'キャンセル' (Cancel) and 'OK'.

The background interface shows the 'ALTUS BASIC' logo and a sidebar with navigation items: ダッシュボード, 仮想サーバー, アフィニティグループ, ストレージ, ネットワーク, テンプレート (highlighted), イベント, アカウント, ドメイン, ガイド. The main content area shows a table with columns '順序' and 'クイックビュー'.

GMOクラウド・ALTUSの場合

Server Spec : 1core / 512MB Memory

GMO CLOUD - Mozilla Firefox

https://tky001b.pf.gmocloud.com/client/?command=login&domainid=e2de1c99-5c51-43d4-ae2e-eda610f251e3&response=js...

ALTUS BASIS

+ 仮想サーバーの追加

- 1 セットアップ
- 2 テンプレートの選択
- 3 仮想サーバー
- 4 ディスク
- 5 アフィニティ
- 6 ネットワーク
- 7 確認

- Mini Server**
Mini Server (1 vCPU / 512MB RAM)
- Custom Server**
Resource Pack (Custom Server)
- Custom Server**
Resource Pack (Custom Server)
- m1.small**
Resource Pack (AWS m1.small 1 vCPU / 2GB RAM)
- m1.large**
Resource Pack (AWS m1.large 2 vCPU / 8GB RAM)
- m1.xlarge**

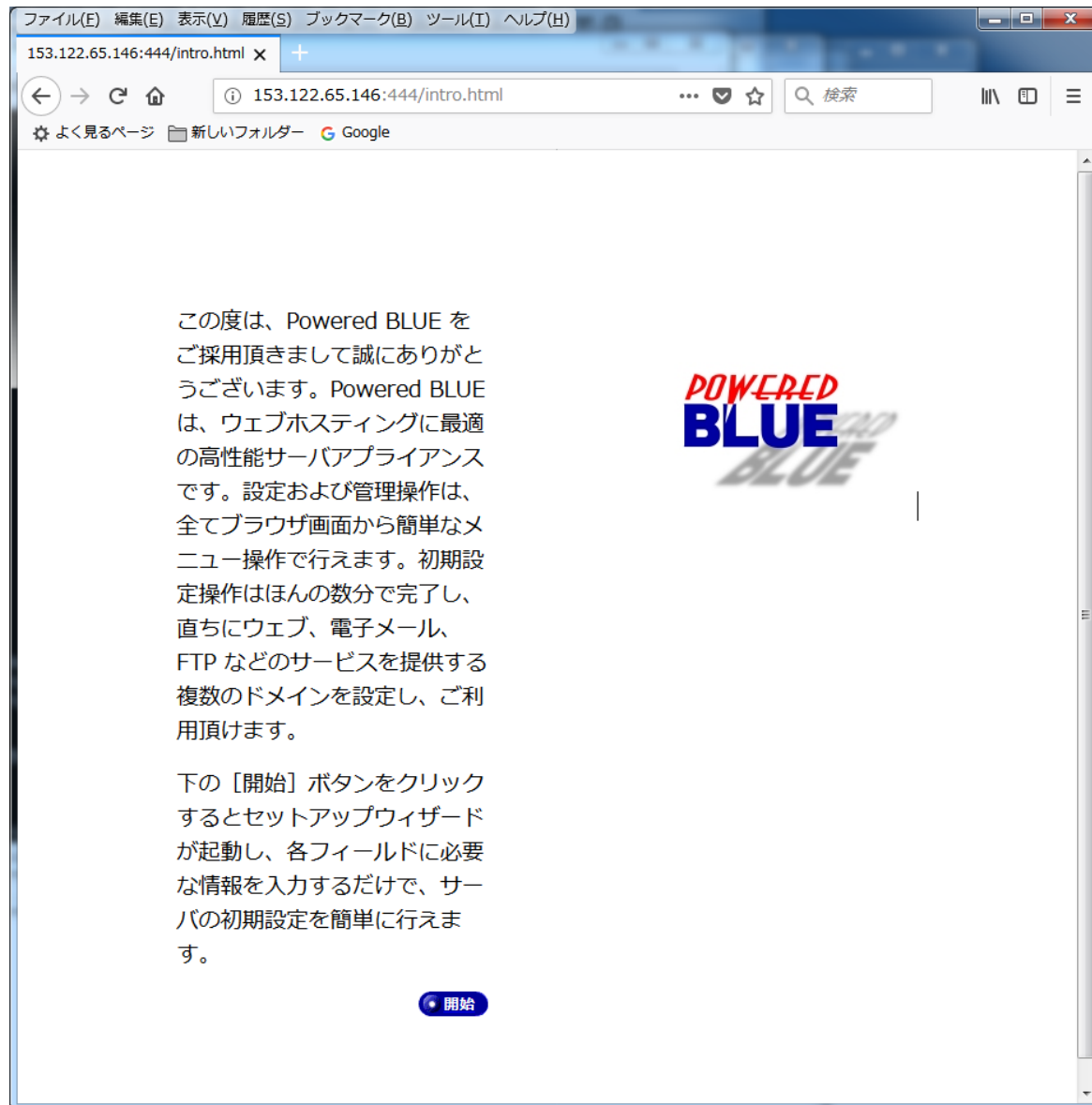
戻る

キャンセル

次へ

GMOクラウド・ALTUSの場合

電源オン・サーバーセットアップ



ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(I) ヘルプ(H)

153.122.65.146:444/intro.html x +

153.122.65.146:444/intro.html 検索

よく見るページ 新しいフォルダー Google

この度は、Powered BLUE をご採用頂きまして誠にありがとうございます。Powered BLUE は、ウェブホスティングに最適な高性能サーバアプライアンスです。設定および管理操作は、全てブラウザ画面から簡単なメニュー操作で行えます。初期設定操作はほんの数分で完了し、直ちにウェブ、電子メール、FTP などのサービスを提供する複数のドメインを設定し、ご利用頂けます。

下の [開始] ボタンをクリックするとセットアップウィザードが起動し、各フィールドに必要な情報を入力するだけで、サーバの初期設定を簡単に行えます。

[開始](#)

管理画面

The screenshot shows the management interface for POWERED BLUE. 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 services: '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', and 'サポート情報'. The main content area is titled 'ウェブの設定' and has tabs for '基本', 'セキュリティ', and '詳細'. Under the 'セキュリティ' tab, there is a 'セキュリティ設定' section with the following items:

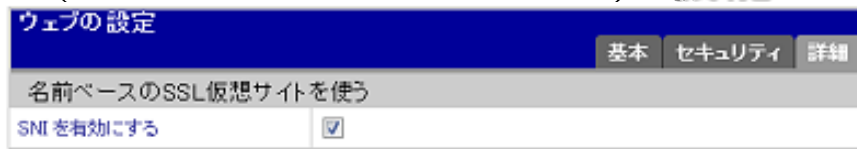
バージョン情報を公開しない	<input checked="" type="checkbox"/>
PHPヘッダを応答しない	<input checked="" type="checkbox"/>
HTTP Traceメソッドを無効にする	<input checked="" type="checkbox"/>
SSLセキュアレベル	TLS1.2以上を使用する(強レベル) ▼

Below the table is a '保存' (Save) button. At the bottom of the page, a blue banner contains the text: '? 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



ウェブの設定

基本 セキュリティ 詳細

名前ベースのSSL仮想サイトを使う

SNIを有効にする

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



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

PHPヘッダを応答しない

HTTP Traceメソッドを無効にする

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)



SELinux の設定

基本 詳細

SELinuxを有効にする

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

CMS 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](#)

WordPress マルチサイト・マルチユーザー対応

The screenshot shows the WordPress Multisite administration interface. The top navigation bar includes links for '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 contains a menu with options like '仮想サイトのリスト', 'www.mubit.tv', 'ユーザの管理', 'ユーザのリスト', 'インポート', 'エクスポート', '一般設定', 'サービス', 'SSL', 'ブログ', '基本設定', 'ブログのリスト', and '利用状況'. The main content area displays 'ブログのリスト - www.mubit.tv' with a table of 7 entries. The table has columns for 'ブログホーム', 'ブログのパス', '状況', and '操作'. Each entry shows a directory path and its status as '完了' (Completed).

ブログのテンプレート編集

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

ブログホーム	▼ ブログのパス	状況	操作
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	 

ブログをインストールする

同一サイト内で複数のWordPress/ブログを構築・運用の例

プライベートCAの機能

■ プライベートCAの機能

- SSLクライアント証明書の発行/失効/管理
 - SSLクライアント認証
-

■ Webサーバー機能

- Webサーバーの運用&アプリの運用

■ 既存サーバー連携機能

- 既存Webサーバーへのリダイレクト運用

プライベートCA



Webサーバーアクセス

証明書

アクセス可否

SSL クライアント証明書

有効

○ 社内・部門内

SSL クライアント証明書

失効

× 端末紛失・社員退職

なし

× 部外者

SSLクライアント認証例 スマートフォン

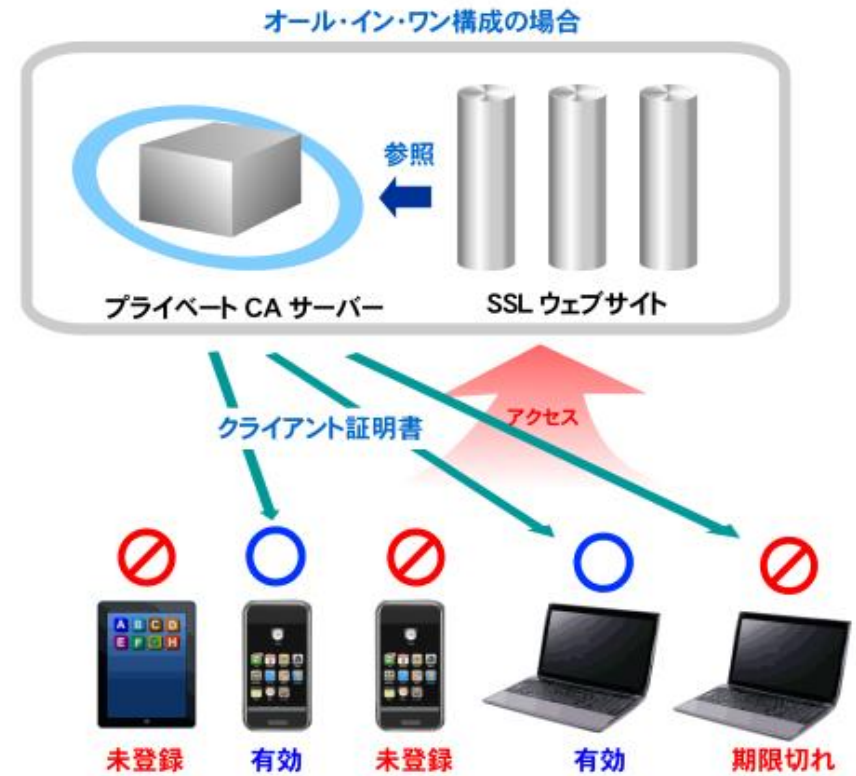
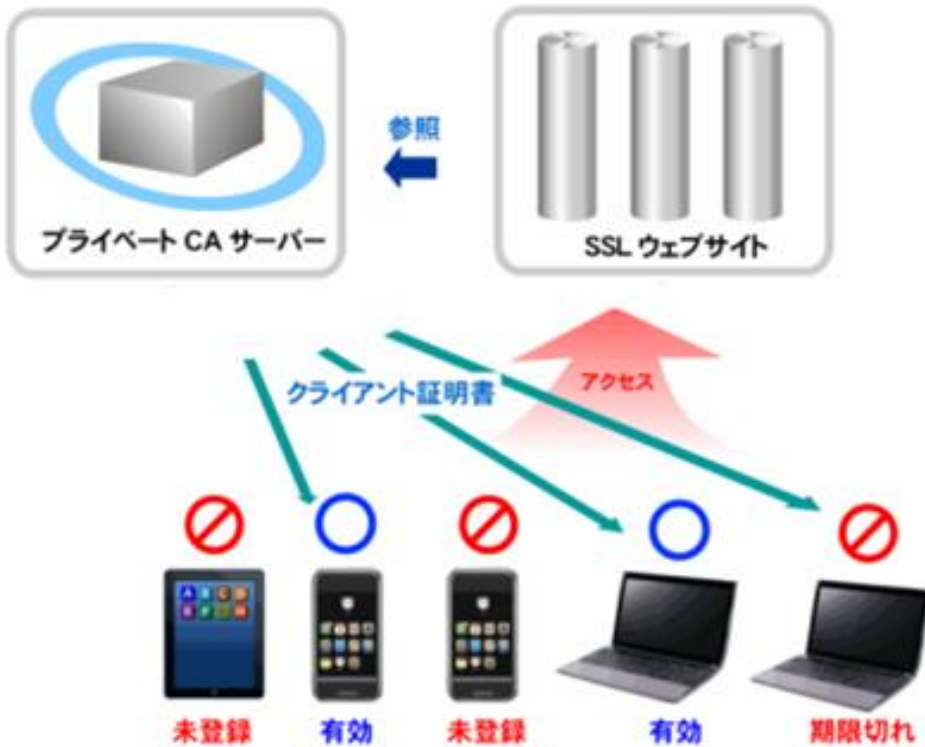


証明書 有効



証明書 無効 アクセス不可

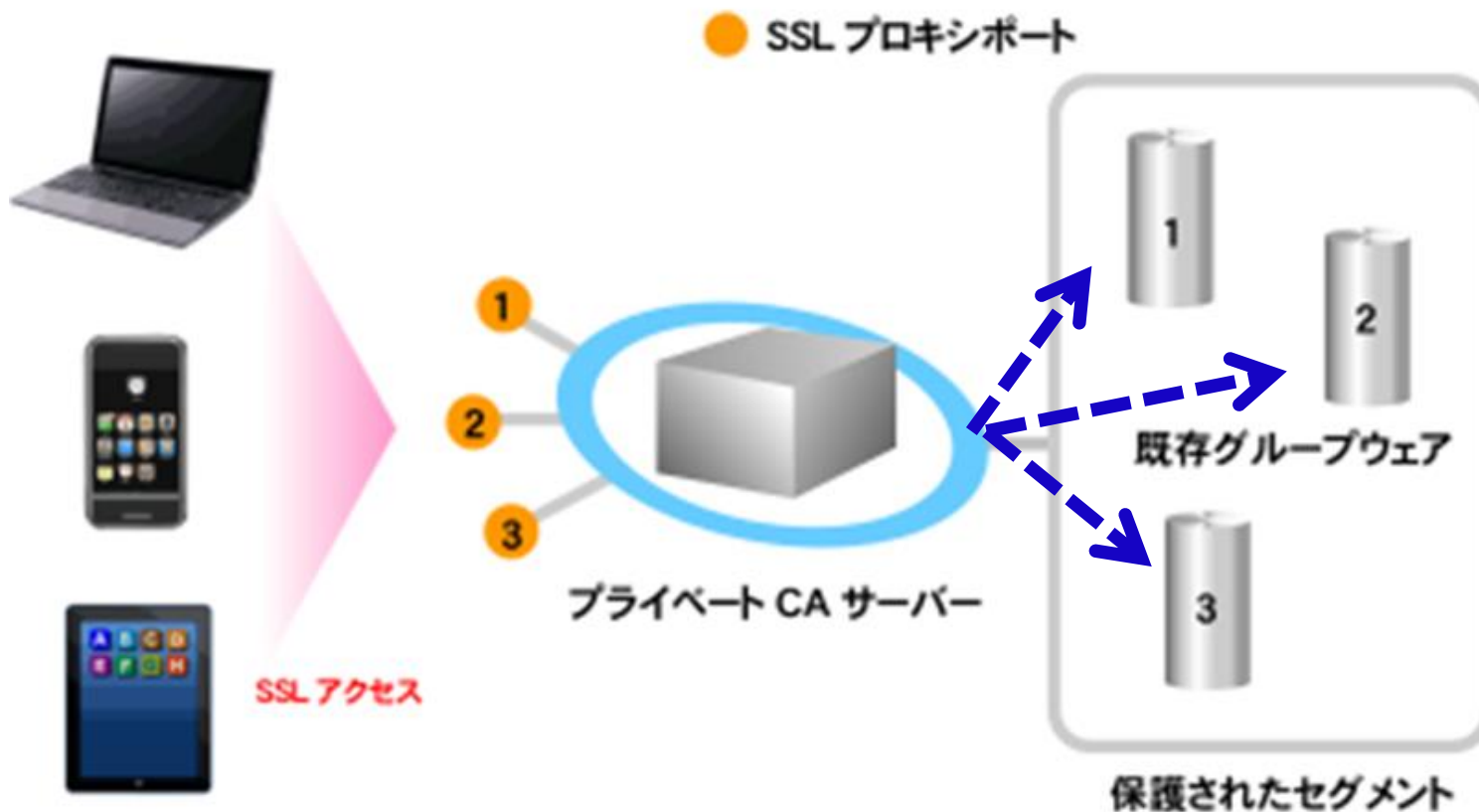
Powered BLUE プライベートCA + Web サーバー



■ オールインワン

■ CAとWebを1台での運用に対応

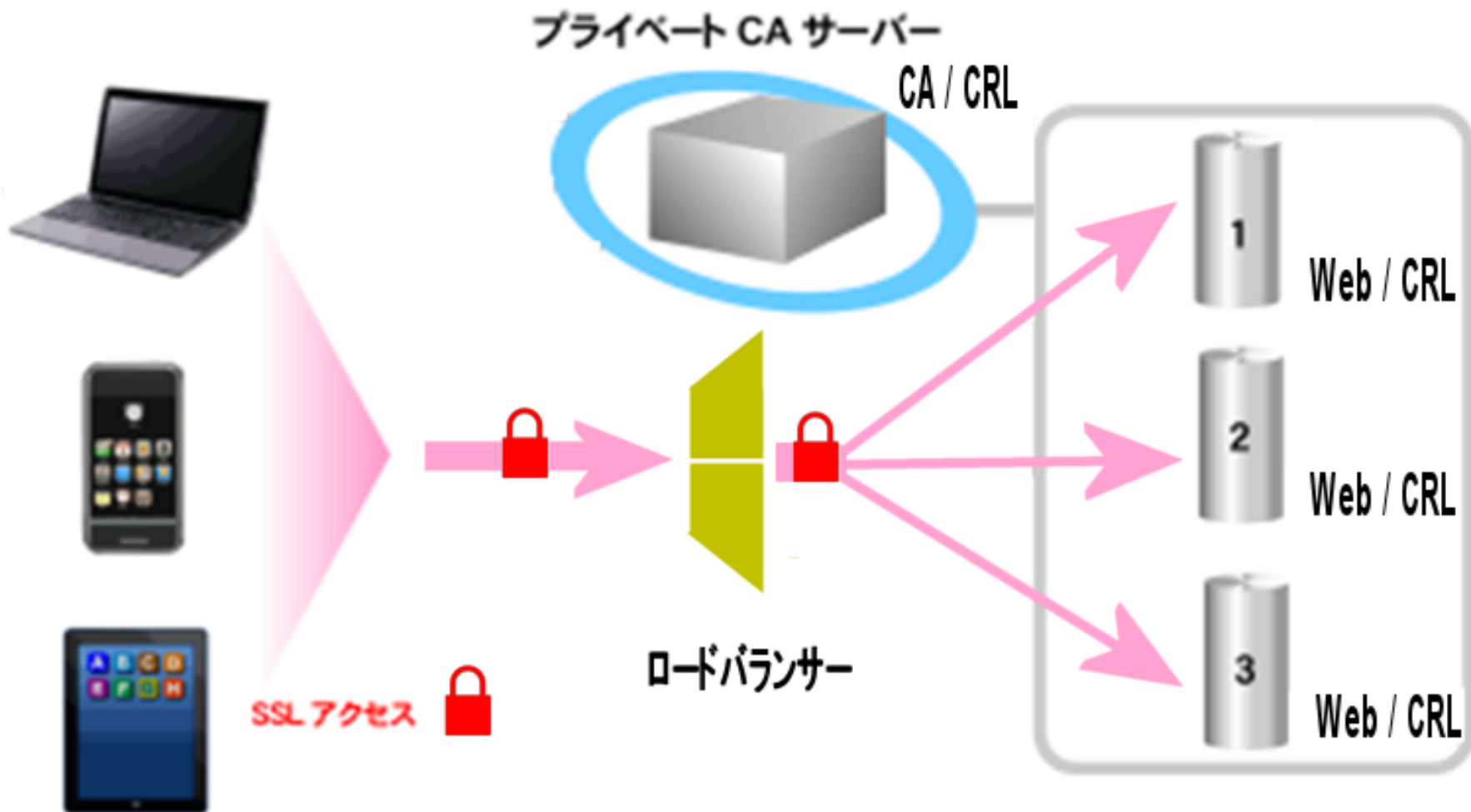
プライベート CA + リバースプロキシ



SSL リバースプロキシをオール・イン・ワンで提供可能。

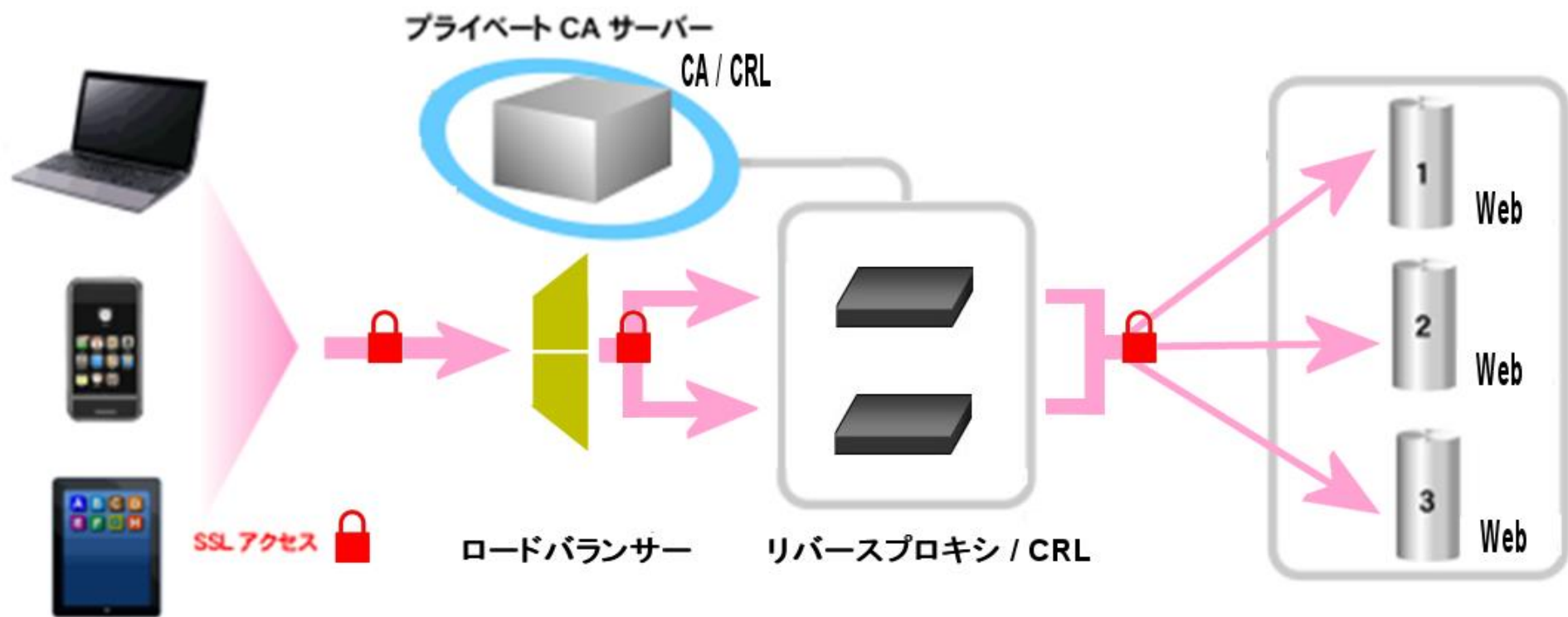
- 既存Webサーバー連携
 - CA + リバースプロキシ での運用に対応

プライベートCA + ロードバランサー



■ CA / CRL の分離運用に対応

プライベートCA + リバースプロキシ + ロードバランサー



- リバースプロキシのLB対応
 - エンド to エンド のSSL運用も可能



インターネットサーバー機能

項目	有無	内容
動作OS		RedHat 7.x / CentOS 7.x (64bit)
標準		
http /https Server	◎	マルチドメイン・マルチサイト対応
DNS Server	◎	
SMTP(S)/POP(S)/IMAP(S)	◎	Postfix・SMTP Auth・Submission port
メールの中継設定	◎	ドメイン・アドレスごとの配送設定可能
Firewall 機能 / SPF レコード	◎	
SNI機能	◎	
仮想サイト管理者での設定	◎	仮想サイトごとに権限移譲可能
OSアップデート	◎	スケジュールアップデート
フリープラグイン		
WebMail	○	RoundCube
WordPress	○	CMS

Powered BLUE プライベートCA 機能

機能	有無	内容
証明書発行機能		
CA機能	◎	CRL(分離運用可能・スケジュールアップデート)
クライアント証明書発行	◎	証明書形式(X.509.ver.3)
	◎	PKCS#12
	◎	証明書の個別発行・部門での一括発行
有効発行枚数(年間)	◎	100枚/250枚/500枚/1000枚/2500枚/5000枚...
	◎	ユーザーごとの証明書のダウンロード機能
サーバー証明書発行	◎	PKCS#12/PEM
アルゴリズム	◎	SHA1/SHA224/SHA256/SHA384/SHA512
検索・失効機能		
証明書の検索	◎	
証明書の失効機能	◎	
マルチドメイン・マルチサイト	◎	複数のCAを構築・運用
	◎	仮想サイトの権限移譲
リバースプロキシ	○	既存Webサイトへのリダイレクト

SSLクライアント認証例

■ 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
 - ニコラボスマート
 - Aipo
-

■ ワークフロー

- X-point
 - 楽々Workflow
 - 楽ニコラボスマート
 - eValue NS
 - Power egg
 - Seagull Office
 - 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

- マルチドメイン や マルチサイトWeb
WordPress対応
- 複数のWebサイトのSSL化
IP アドレス 1個 で運用
- SSLクライアント認証
社員 や 会員 向けの 専用Web ページ

製品のサイト

■ Powered BLUE 870 Webアプライアンス

<https://www.powered.blue/sub/products/blue/b870.html>

■ Powered BLUE 870 プライベート CA

<https://www.powered.blue/sub/products/ca/b870-ca.html>

■ Powered BLUE 870 Public CA

<https://www.powered.blue/sub/products/ca/b870-globalsign-auth.html>

デモ環境

■ 管理サーバー
192.168.56.140

■ 仮想サイト
192.168.56.140

プライベート CA & リバースプロキシ

WordPress

ホームページ

■ 192.168.56.141

サイボウズ ↙