

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

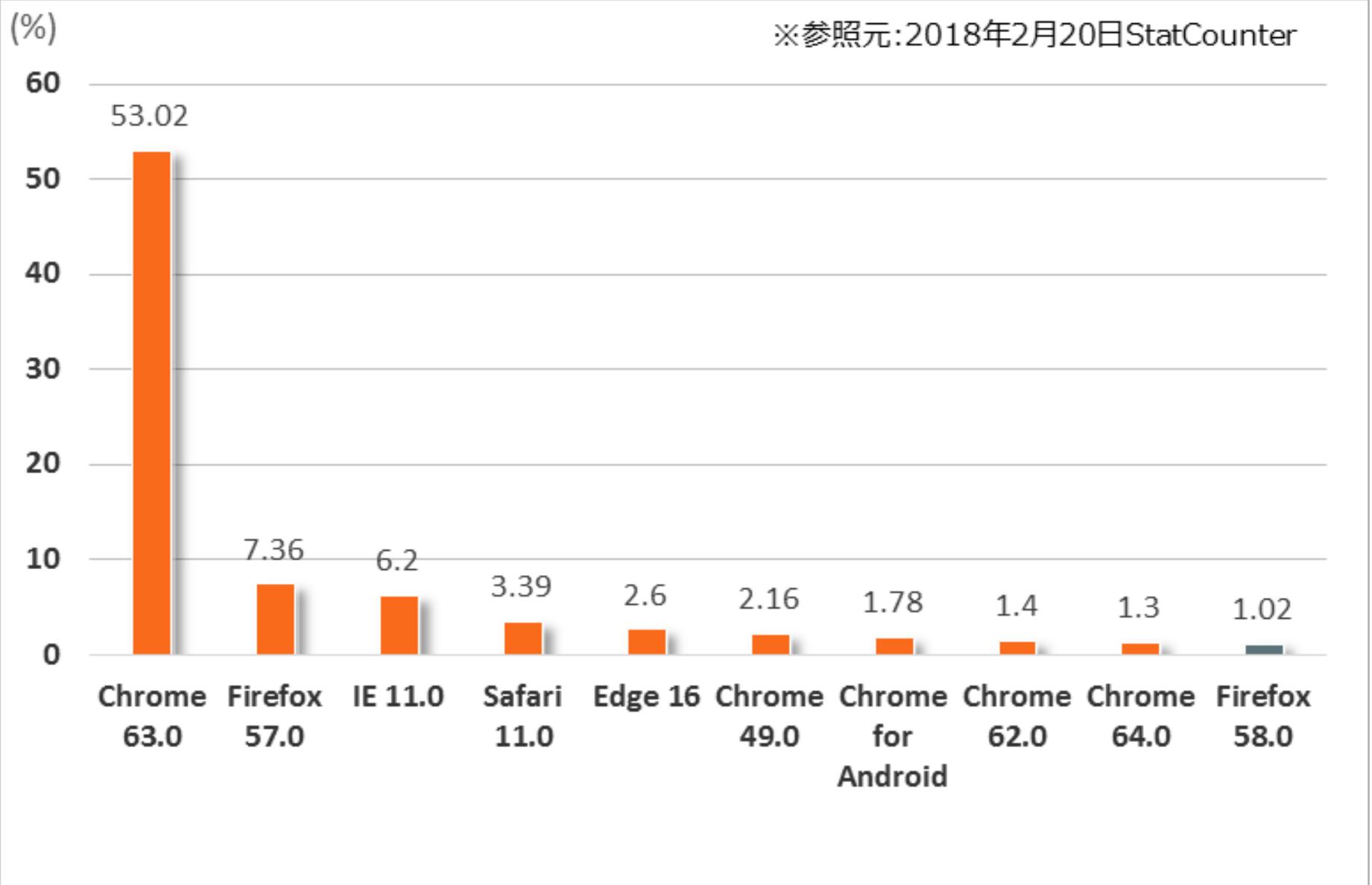
chrome

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
閲覧支援ツール

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 logo and name "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 menu items: "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 "YouTube".

The content area is divided into several sections:

- 財務省の政策**: A sidebar menu listing various policy areas such as "予算・決算", "税制", "関税制度", "国債", "財政投融资", "国庫", "通貨", "国有財産", "たばこ塩", "国際政策", "政策金融・金融危機管理", and "財務総合政策研究所".
- 注目情報**: A central section with a "注目情報" header. It contains several news items with category tags and links, such as "予算・決算" (平成29年度補正予算(第1号)が成立しました), "その他" (【重要なお知らせ】:インターネット通信回線の常時暗号化対応について), "予算・決算" (平成30年度予算政府案国会提出), "国債" (平成30年度国債発行計画の策定等を行いました), "財政投融资" (平成30年度財政投融资計画を閣議に提出しました), and "税制" (平成30年度税制改正の大綱が閣議決定されました).
- 広報・報道**: A sidebar menu with links for "大臣等記者会見", "大臣談話・ステートメント", "週間予定", and "パンフレット・出版物".
- 調達情報**: A sidebar menu with links for "申請・届出等の手続案内", "情報公開・個人情報保護等", "法令適用事前確認手続", and "パブリックコメント".
- 各種手続**: A sidebar menu with links for "申請・届出等の手続案内", "情報公開・個人情報保護等", "法令適用事前確認手続", and "パブリックコメント".
- 統計**: A sidebar menu with a link for "統計".
- 財務省の基本情報**: A sidebar menu with links for "大臣・副大臣・政務官", "財務省について", "財務省の予算・決算", "審議会・研究会等", "法律/政省令/告示/通達等", "政策評価", "所管の法人", "採用情報", "その他の財務省の取り組み", and "財務省の関連サイト".

A video player is embedded in the center, showing a man in a suit speaking at a podium with the Japanese flag in the background. The video title is "職員に向けて年頭挨拶を行う麻生大臣 (1月4日)".

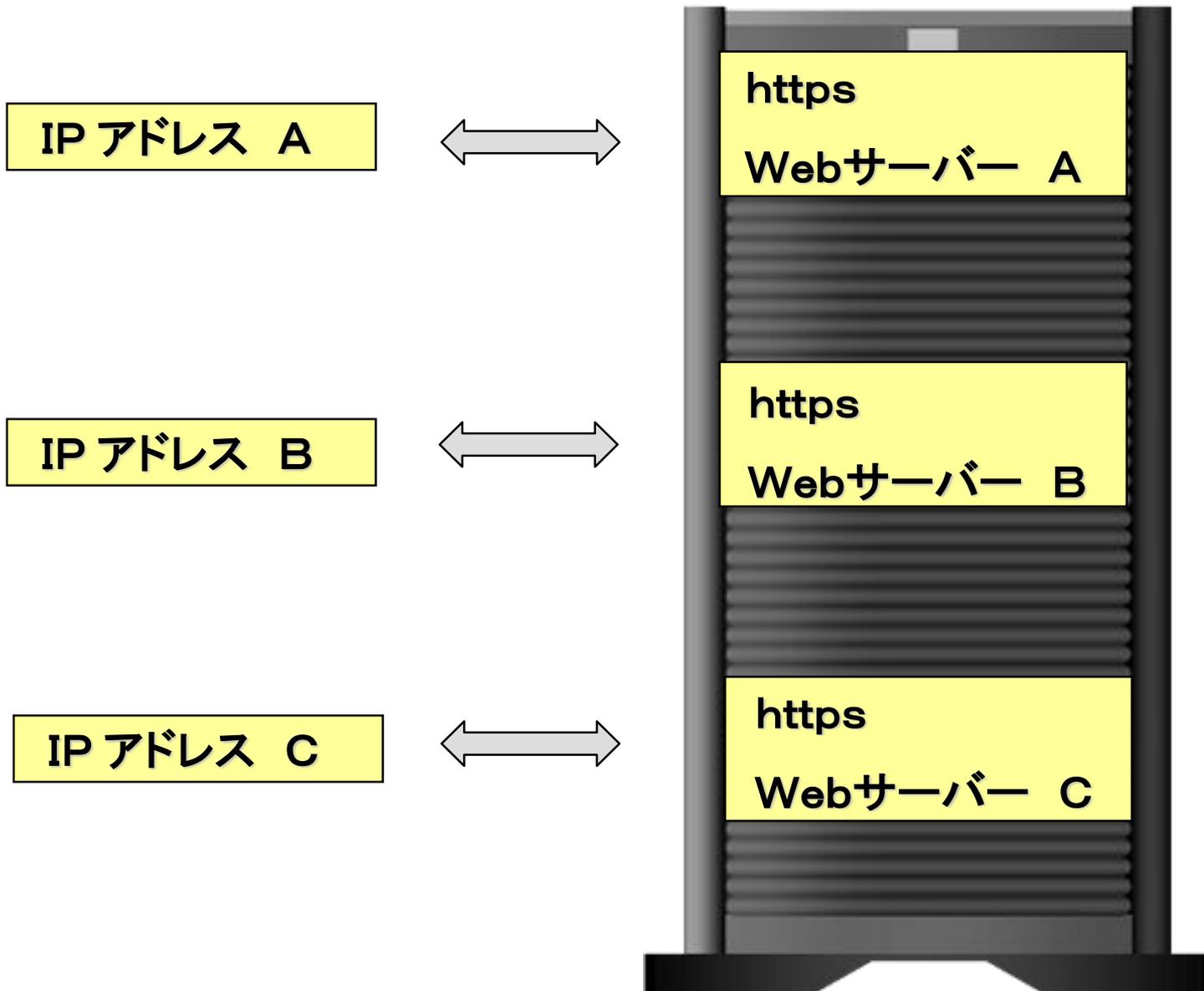
At the bottom, there is a "新着情報" section and an "RSS一覧" link.

Webの常時SSL化の問題点

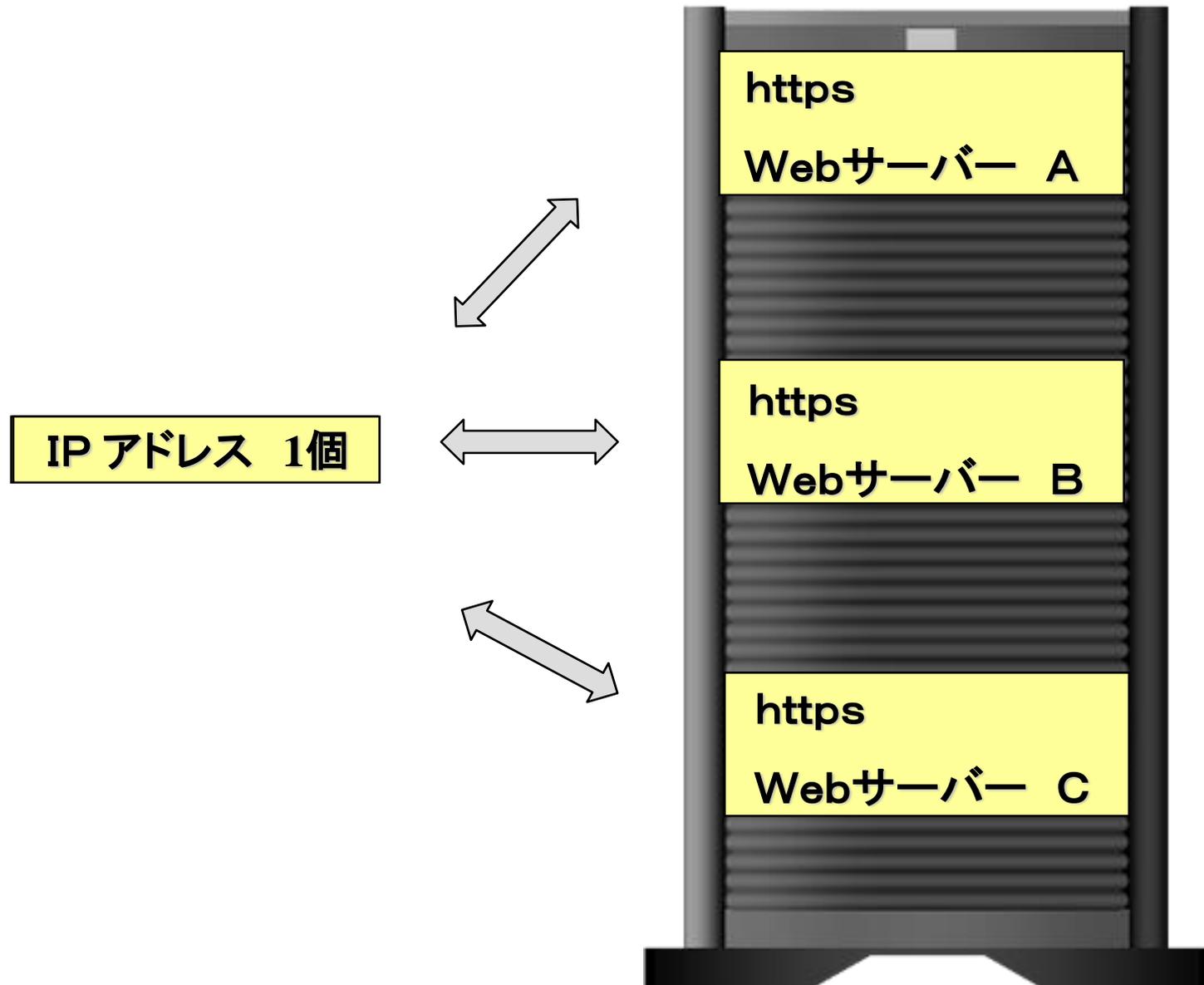
IP アドレス

Webサイトへの攻撃

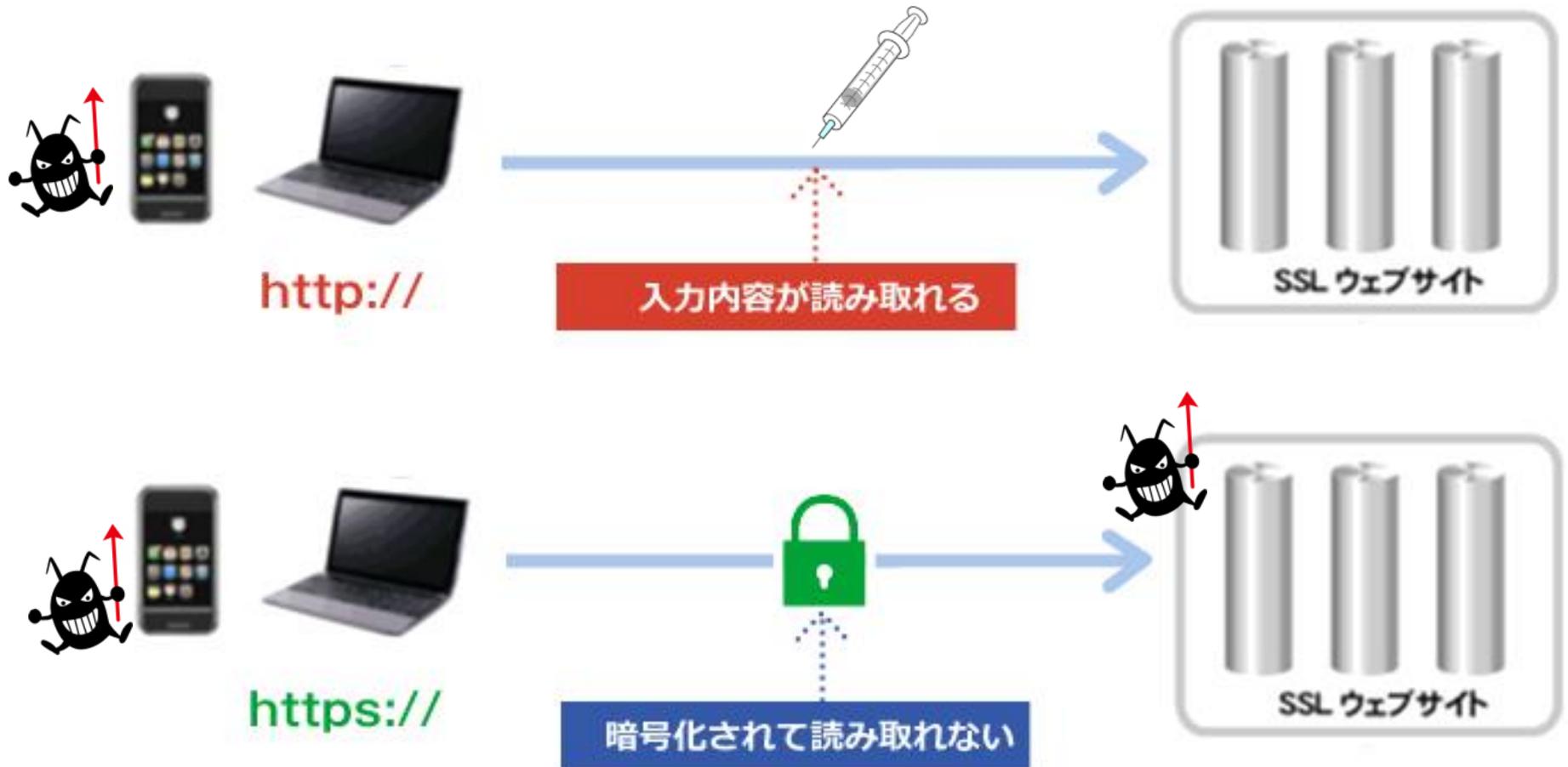
IPアドレス と SSL化Webサーバーの関係



「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

GMO CLOUD - Mozilla Firefox

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

ALTUS BASIC

通知 | admin domain

テンプレートの登録

* 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

ハイパーバイザー: XenServer

形式: VHD

OSの種類: Other (64-bit)

抽出可能:

パスワード管理有効:

起動中のサイズ変更:

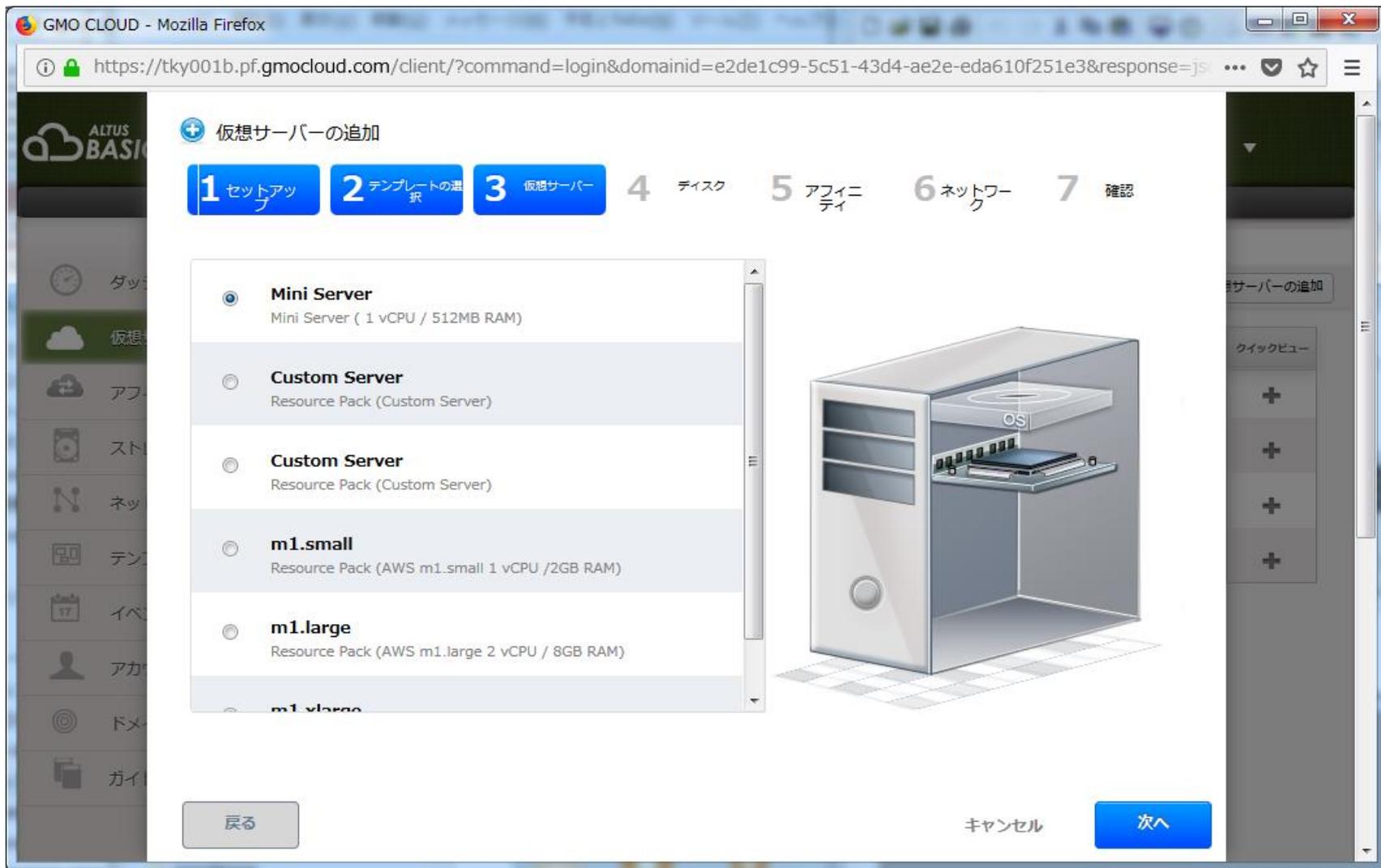
HVM:

キャンセル OK

順序	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 BASIC

+ 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**



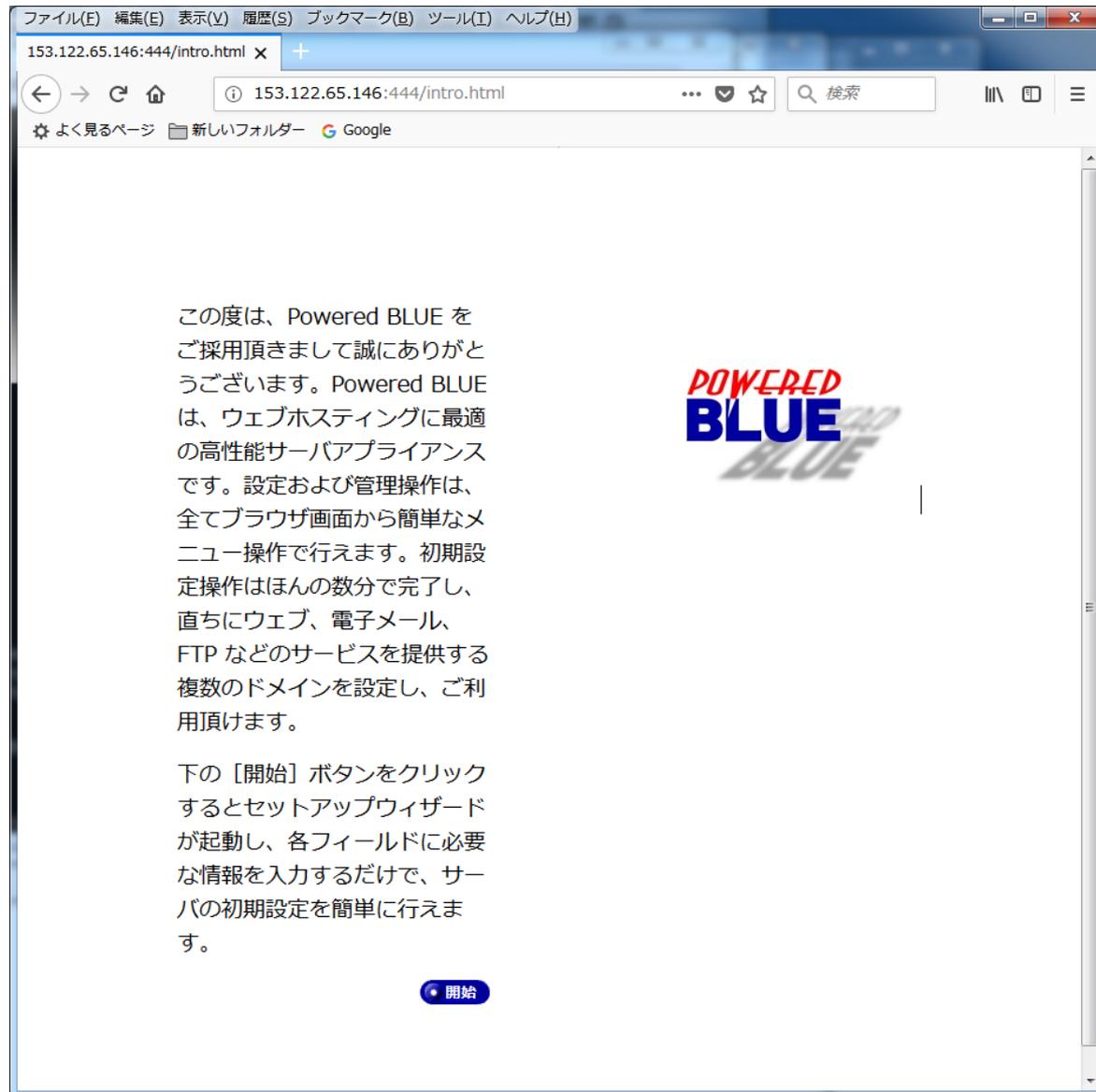
戻る

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



The screenshot shows a web browser window with the address bar displaying "153.122.65.146:444/intro.html". The page content includes a welcome message in Japanese, the Powered BLUE logo, and a "開始" (Start) button.

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'. The 'セキュリティ' tab is active, showing a 'セキュリティ設定' table with the following items:

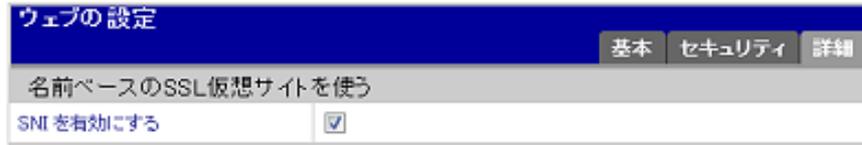
セキュリティ設定	
バージョン情報を公開しない	<input checked="" type="checkbox"/>
PHPヘッダを応答しない	<input checked="" type="checkbox"/>
HTTP Traceメソッドを無効にする	<input checked="" type="checkbox"/>
SSLセキュアレベル	TLS1.2以上を使用する(強レベル) ▼

Below the table is a blue '保存' (Save) button. At the bottom of the page, a blue banner contains a question mark icon and 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



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.

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

POWERED BLUE

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

仮想サイトのリスト

www.mubit.tv

ユーザーの管理

ユーザーのリスト

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

利用状況

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 ユーザーブログを追加する 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

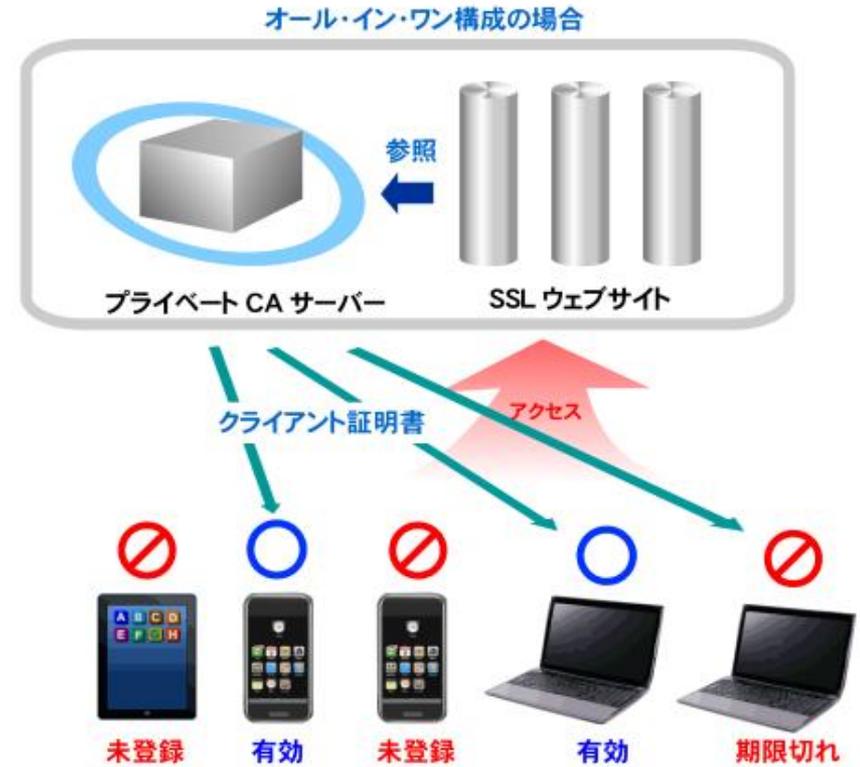


証明書 有効



証明書 無効 アクセス不可

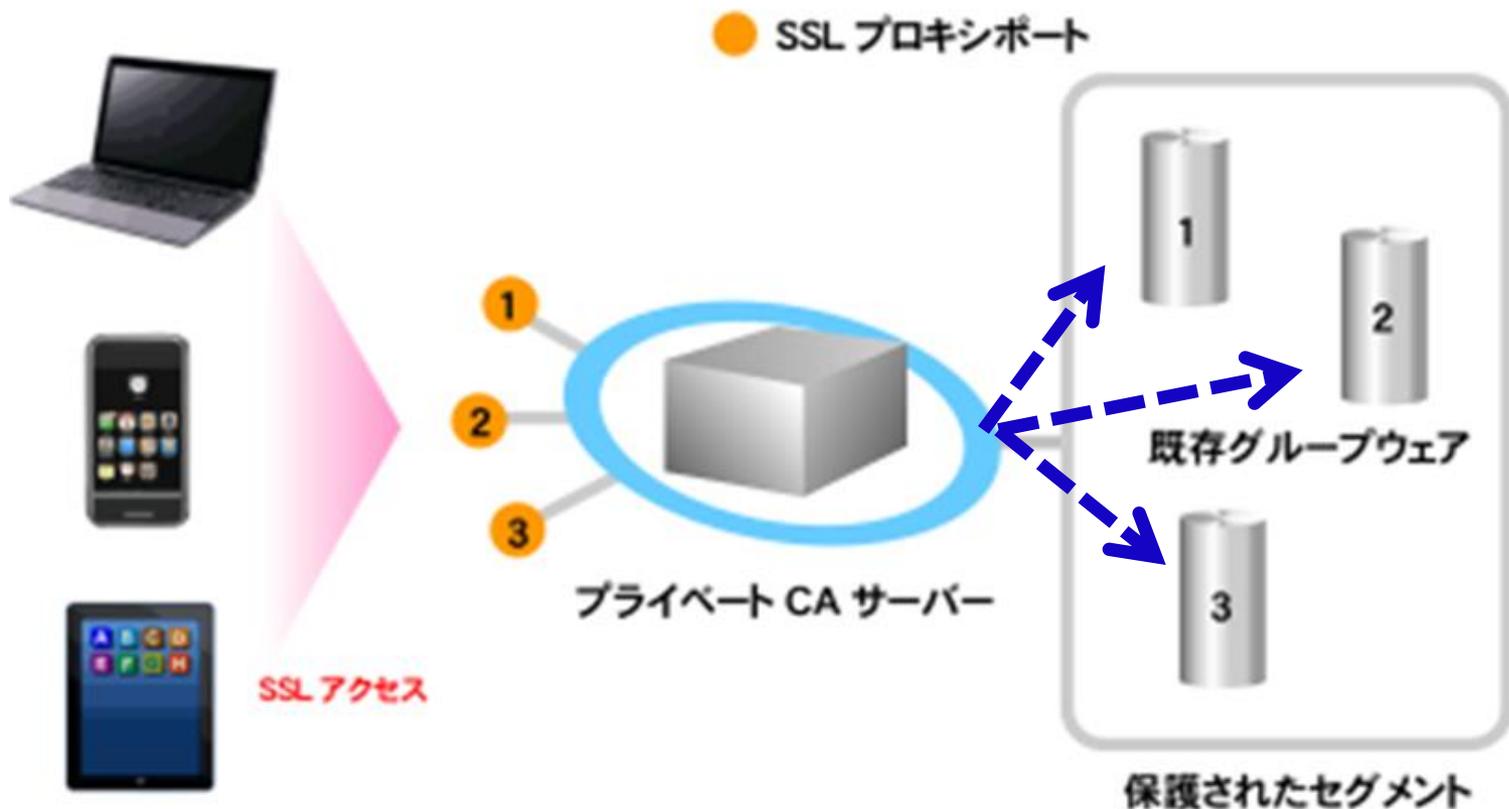
Powered BLUE プライベートCA + Web サーバー



■ オールインワン

■ CAとWebを1台での運用に対応

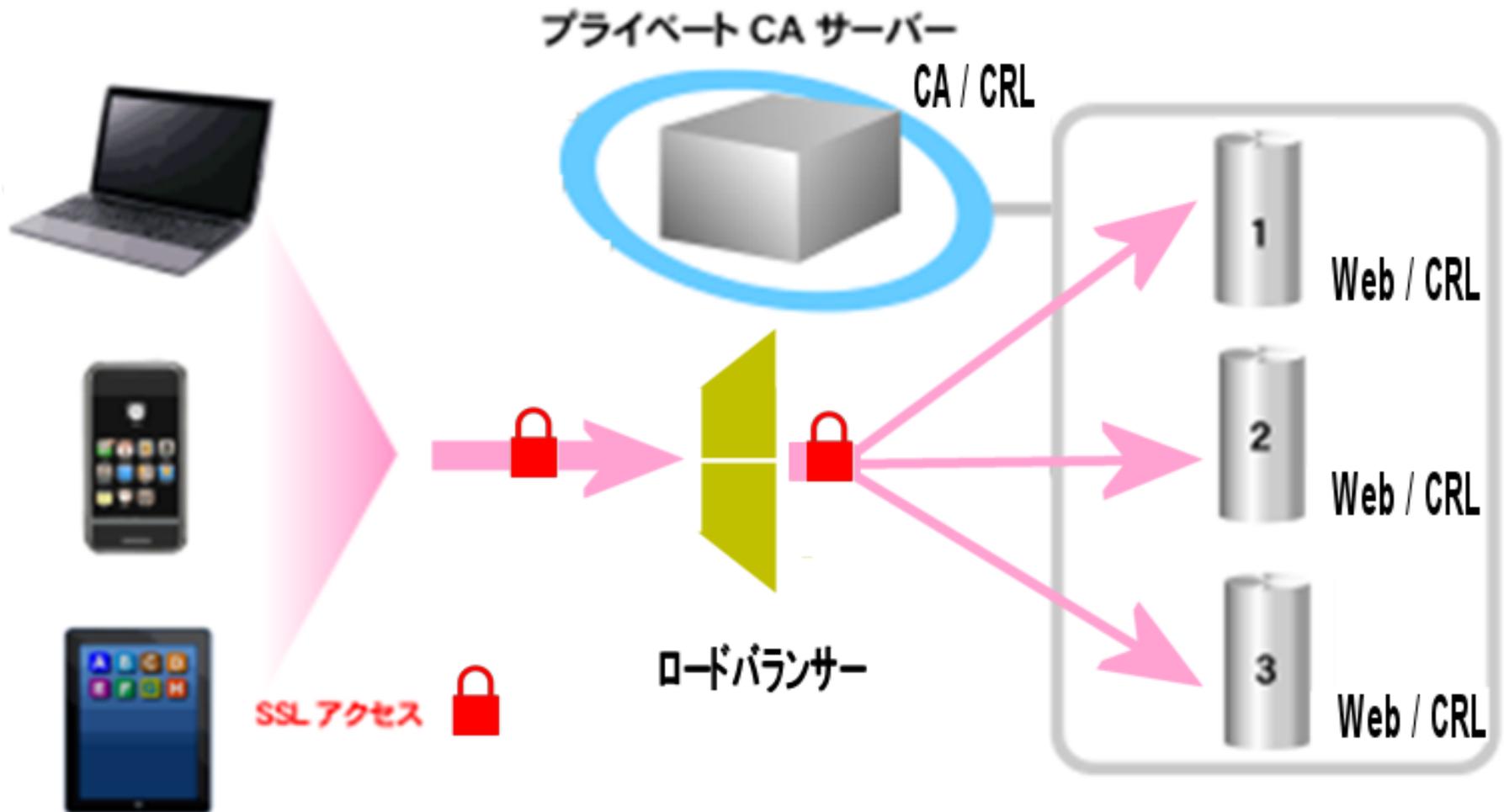
プライベート CA + リバースプロキシ



SSL リバースプロキシをオール・イン・ワンで提供可能。

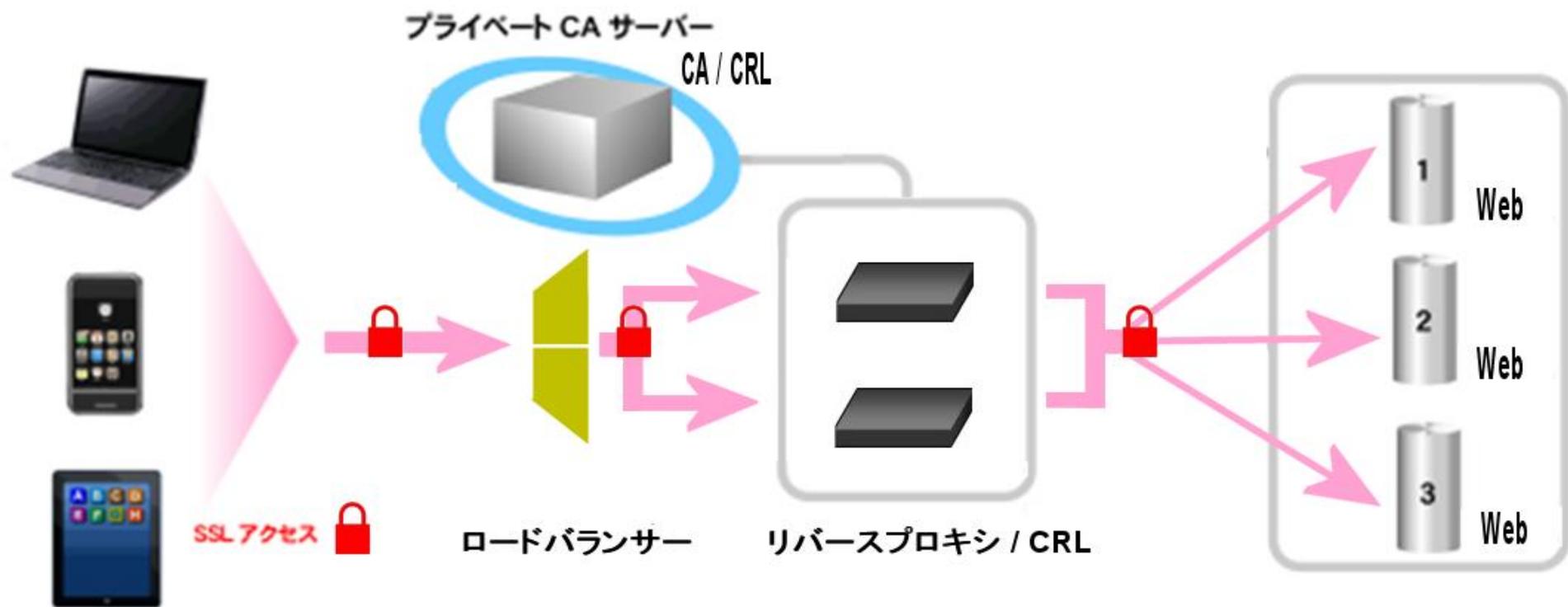
- 既存Webサーバー連携
 - CA + リバースプロキシ での運用に対応

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 ↙

