
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 アプライアンスサーバー（Linux） ソフトウエア開発

HTTPS

をランキング シグナルに使用します

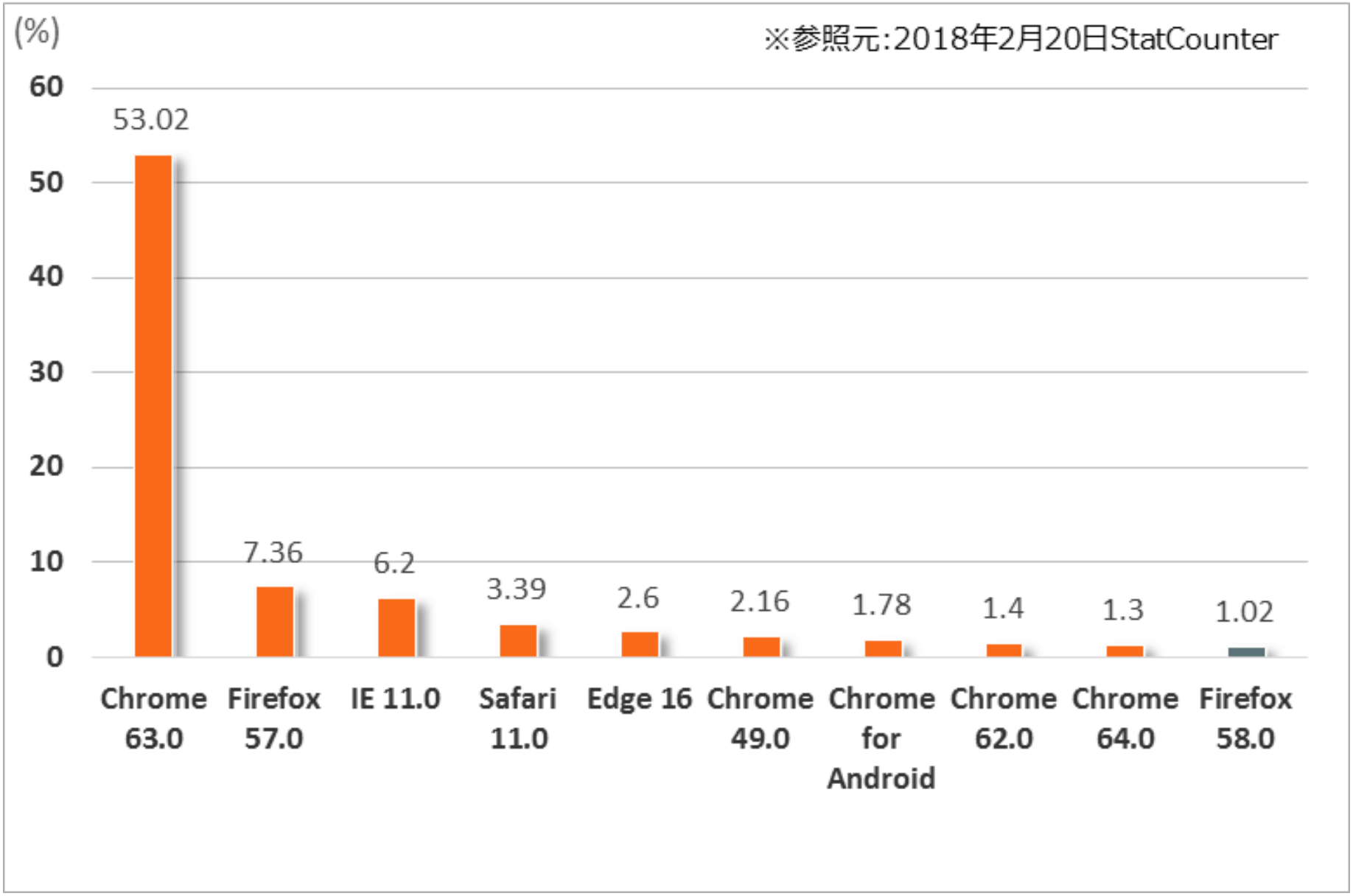
chrome

Googleは2018年7月にリリースの
「Chrome 68」から

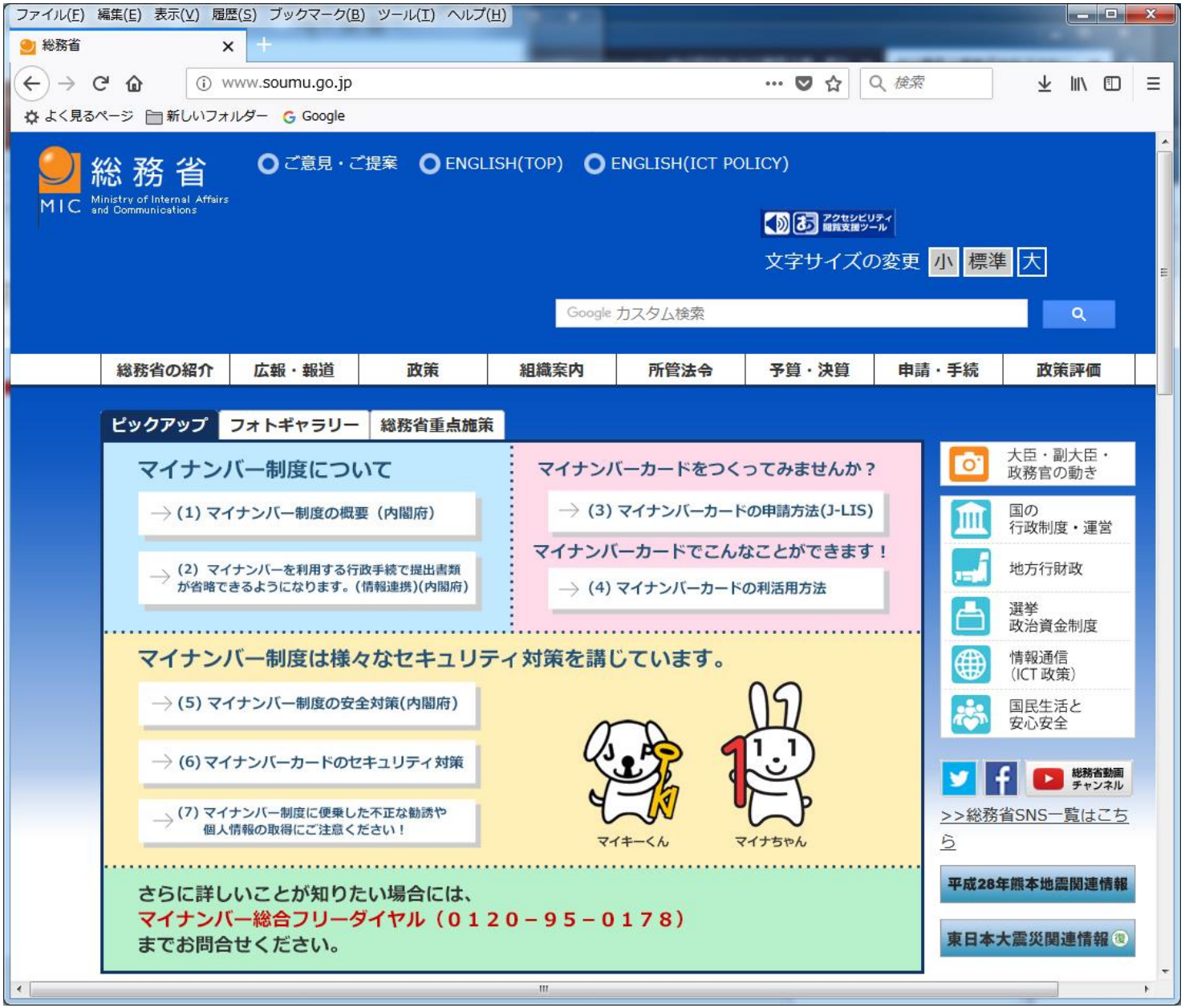
「http://」で始まるすべてのWebサイトで
「保護されていません」警告を表示する

と発表しました。

ブラウザのシェア


(%)
※参照元:2018年2月20日StatCounter
60
50
40
30
20
10
0
53.02
7.36
6.2
3.39
2.6
2.16
1.78
1.4
1.3
1.02
Chrome 63.0
Firefox 57.0
IE 11.0
Safari 11.0
Edge 16
Chrome 49.0
Chrome for Android
Chrome 62.0
Chrome 64.0
Firefox 58.0

SSL　未対応のWebサイト-2



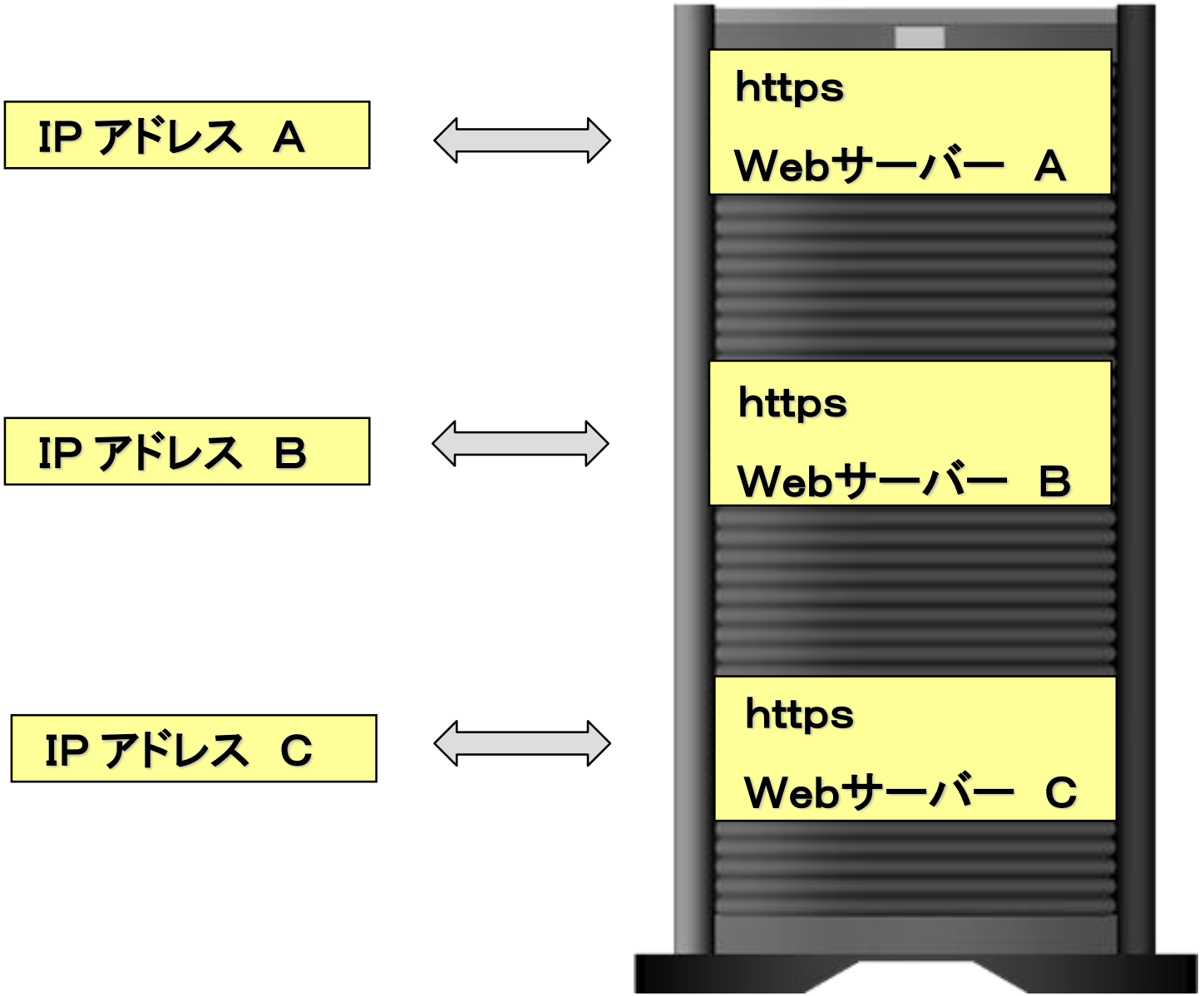
SSL　対応のWebサイト

Webの常時SSL化の問題点

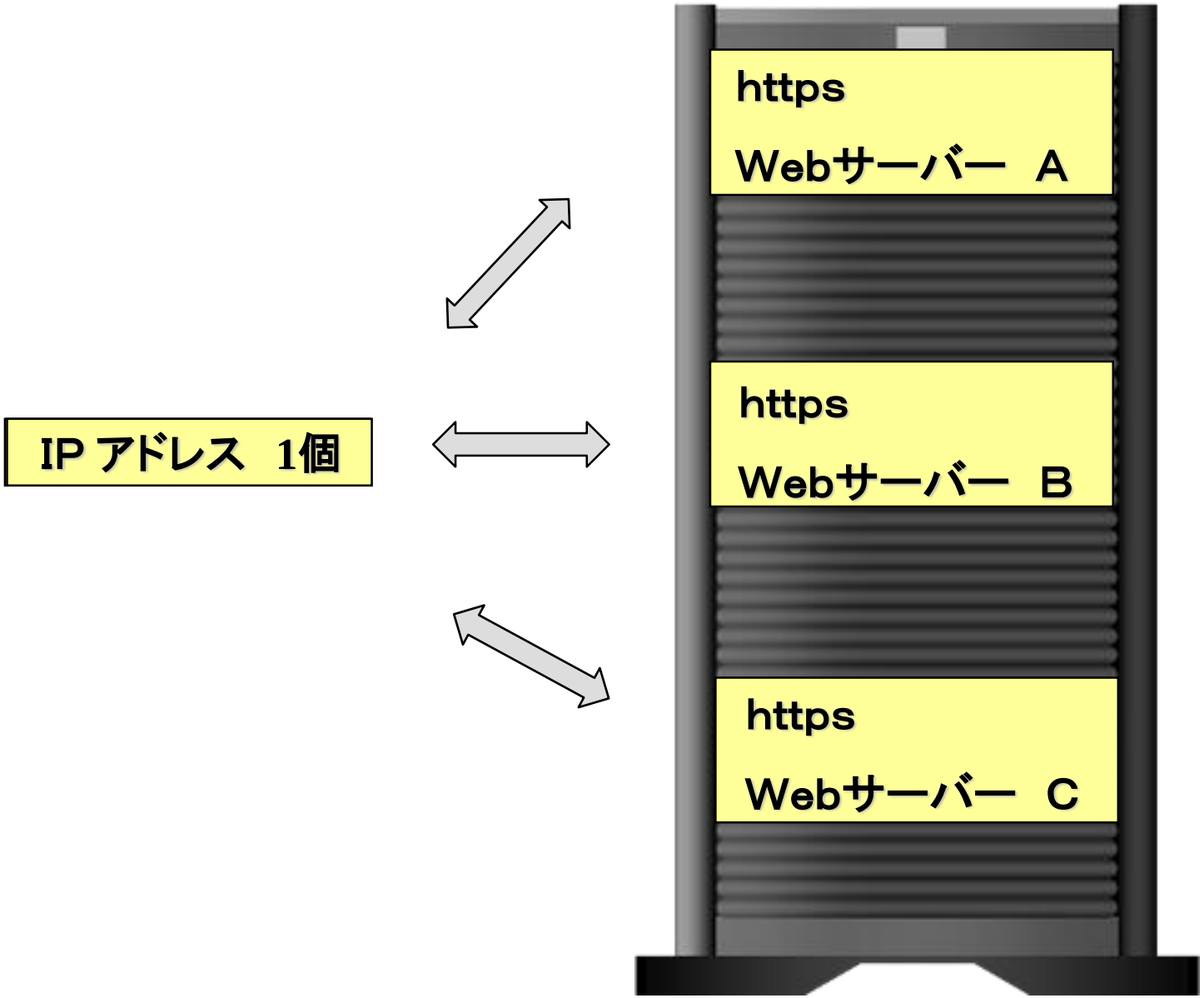
IP アドレス

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アプライアンスの特徴

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

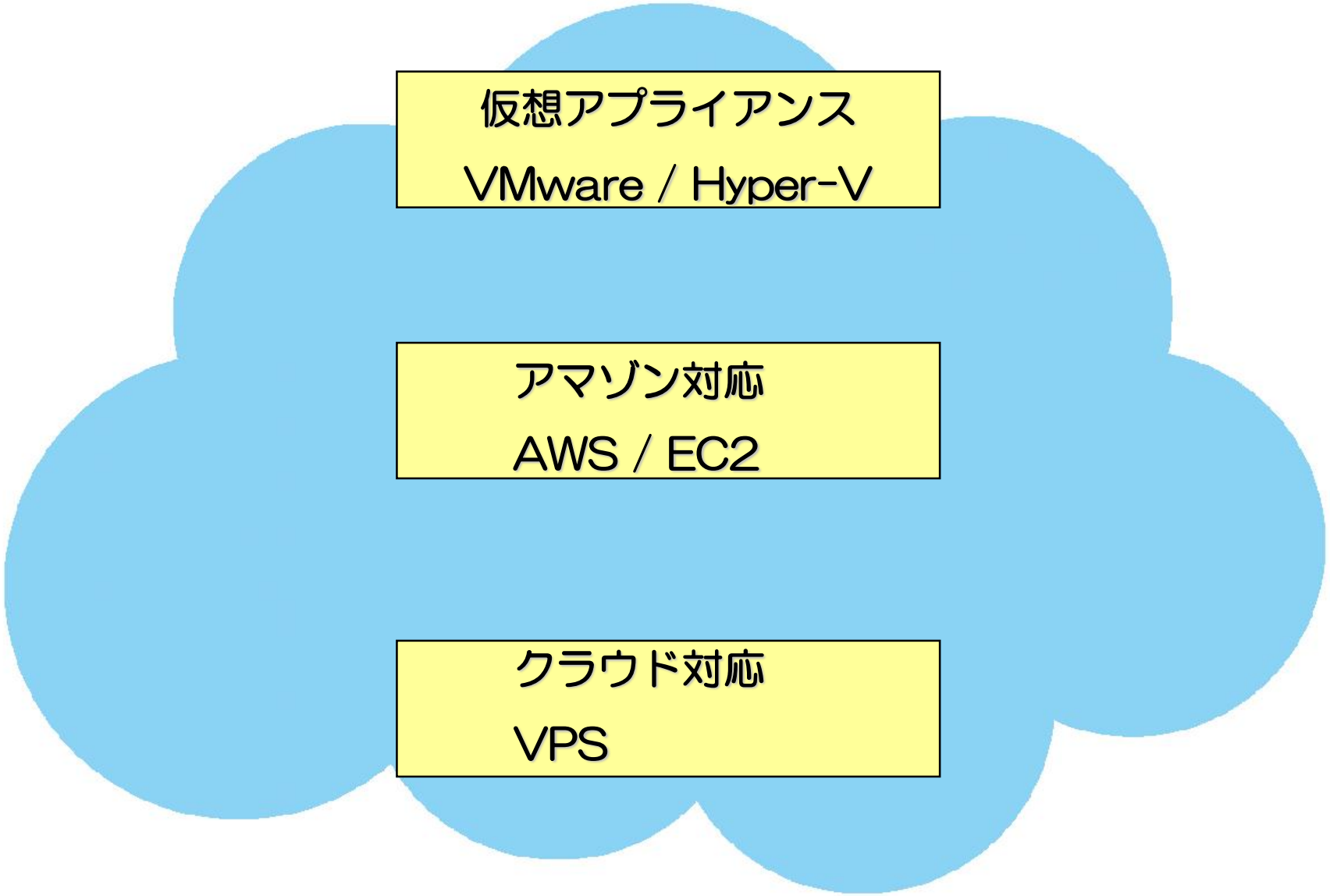
仮想・クラウド対応

仮想アプライアンス

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

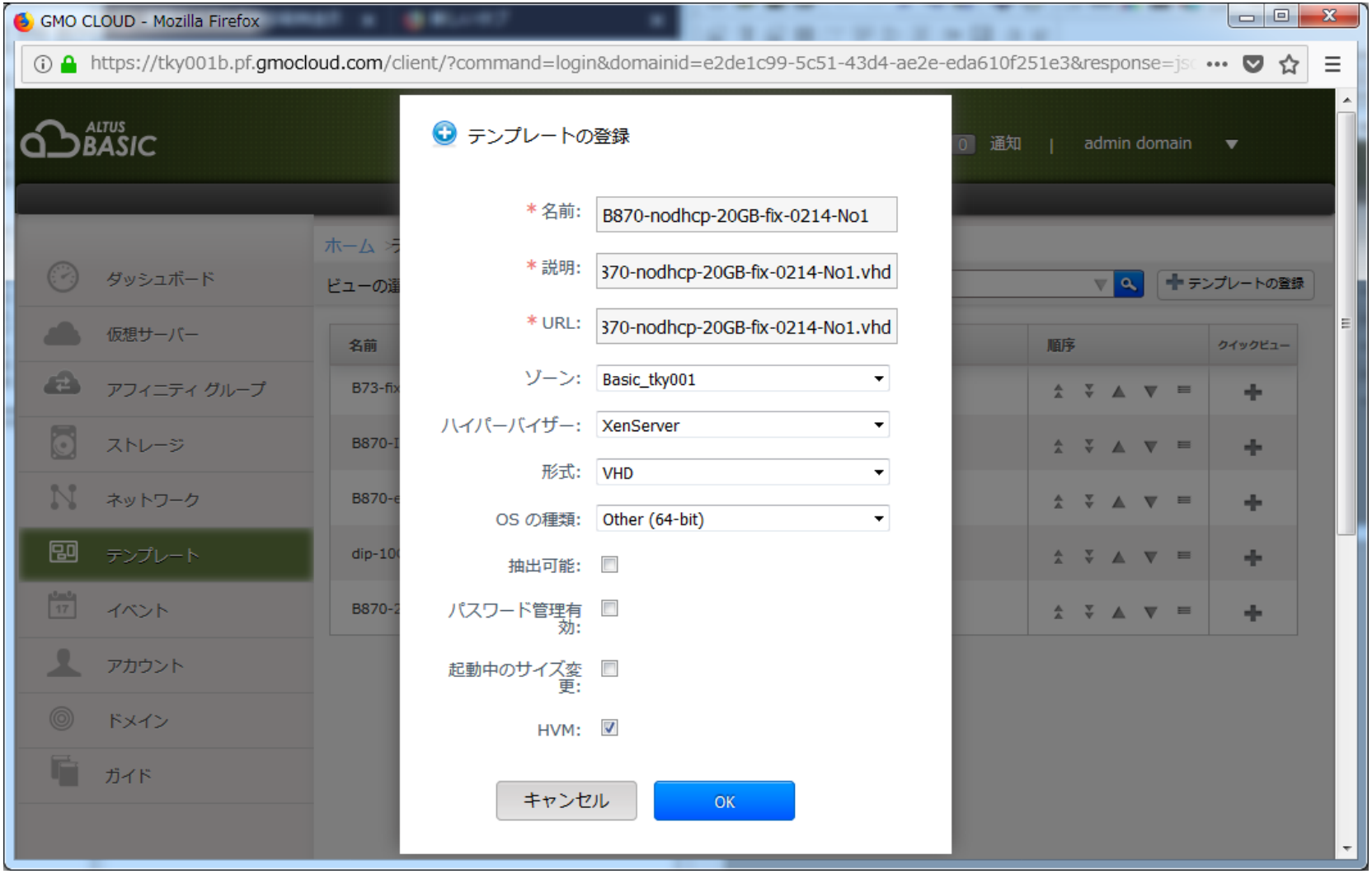
「Powered BLUE 870 Webアプライアンス」運用環境



10分で運用開始

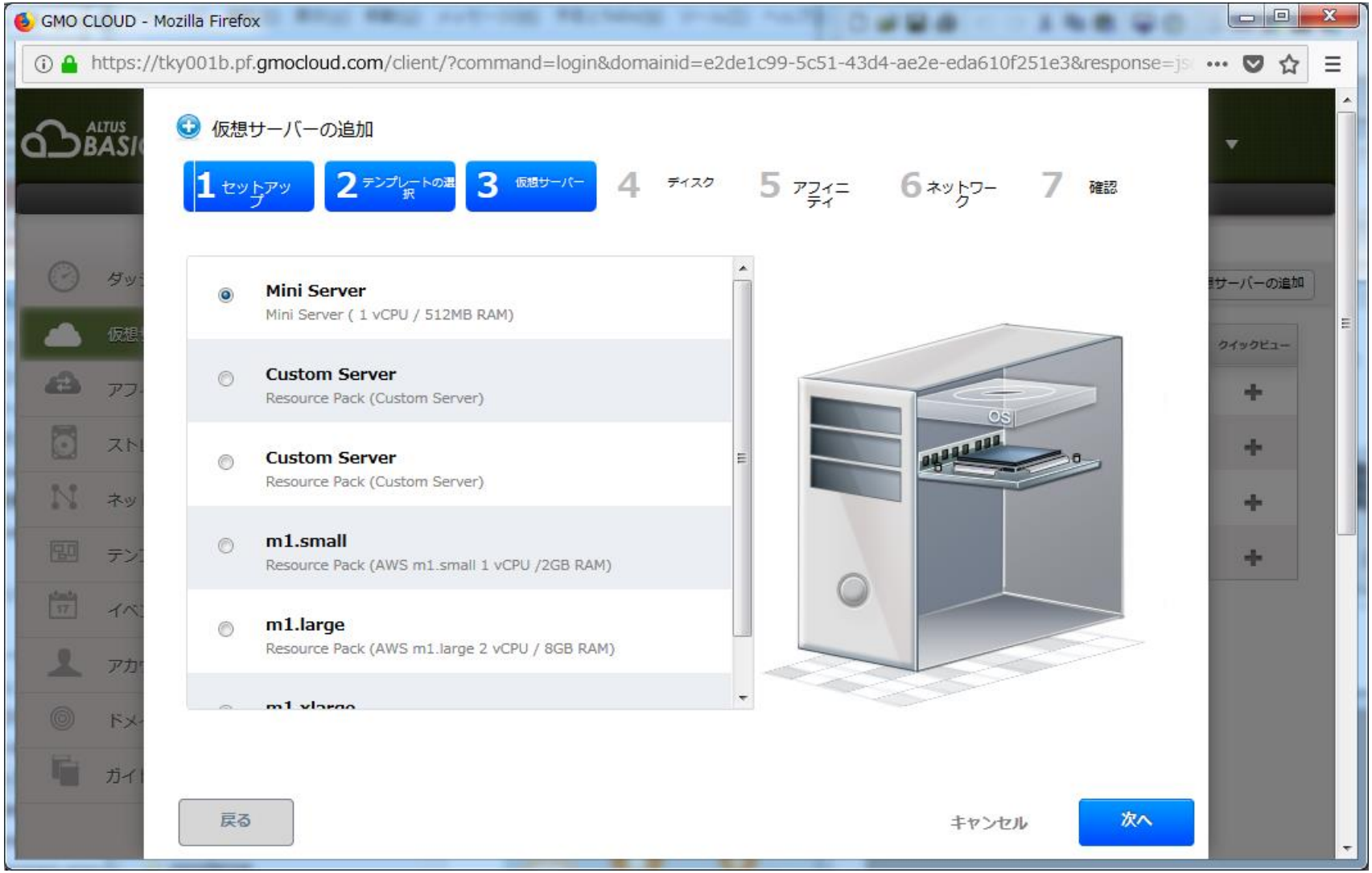
GMOクラウド・ALTUSの場合

仮想アプライアンスイメージのインポート



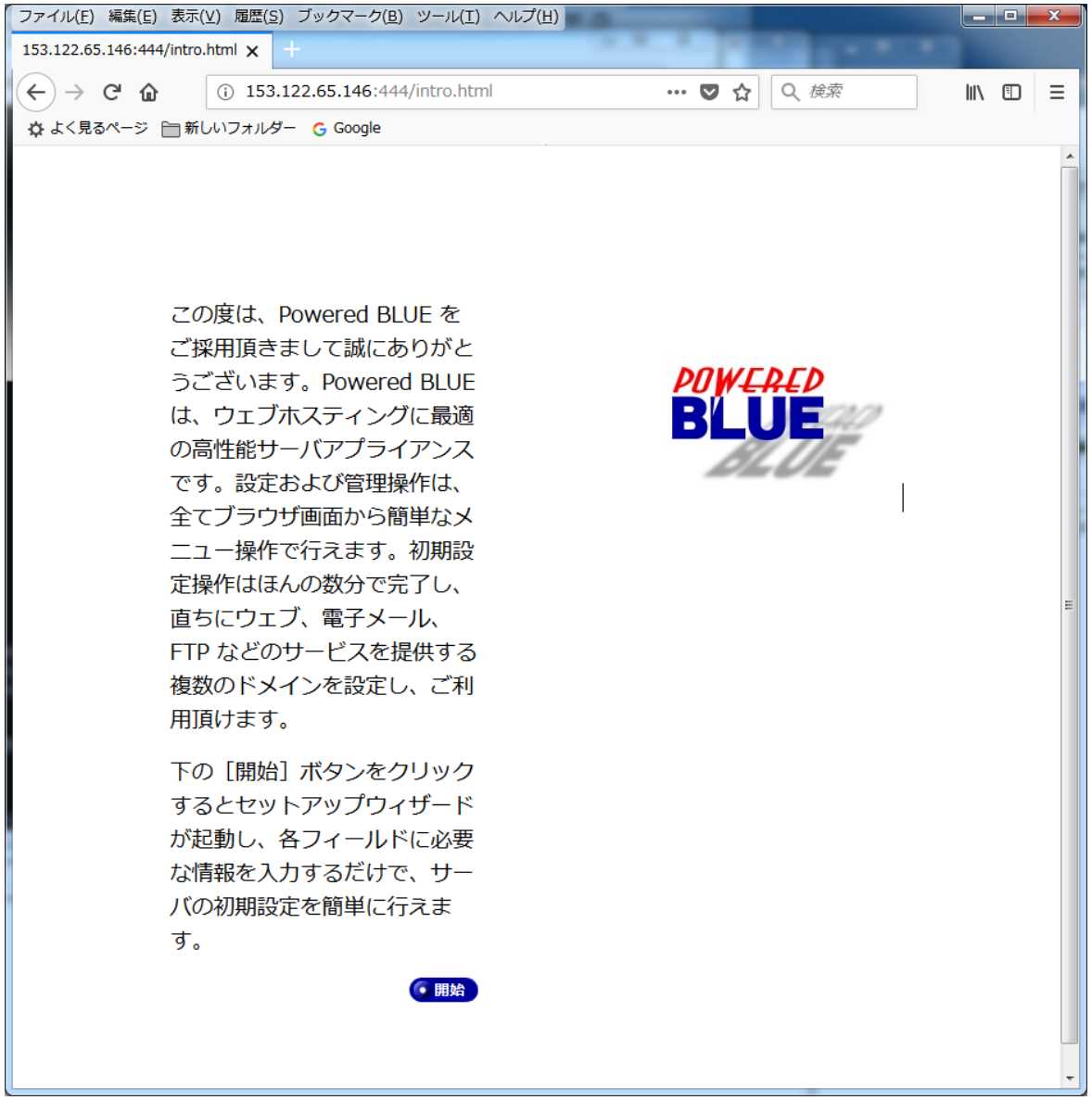
GMOクラウド・ALTUSの場合

Server Spec： 1core / 512MB Memory

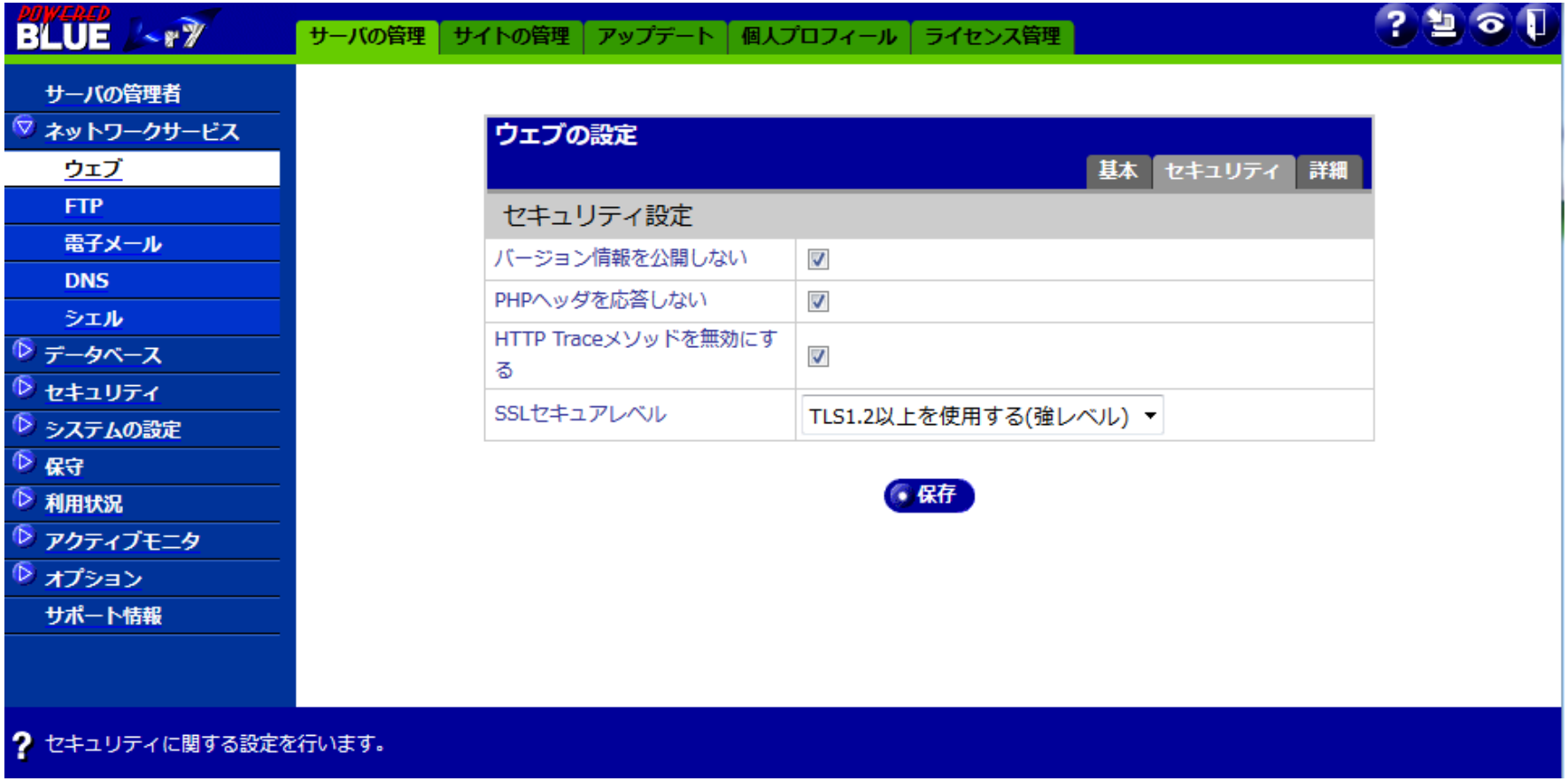


GMOクラウド・ALTUSの場合

電源オン・サーバーセットアップ



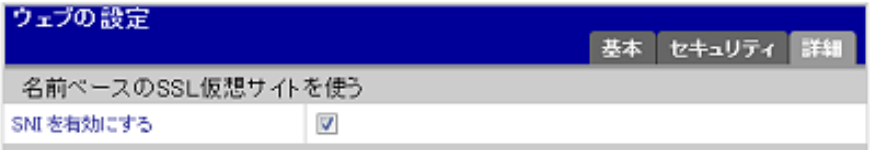
管理画面



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



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

■ 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)

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

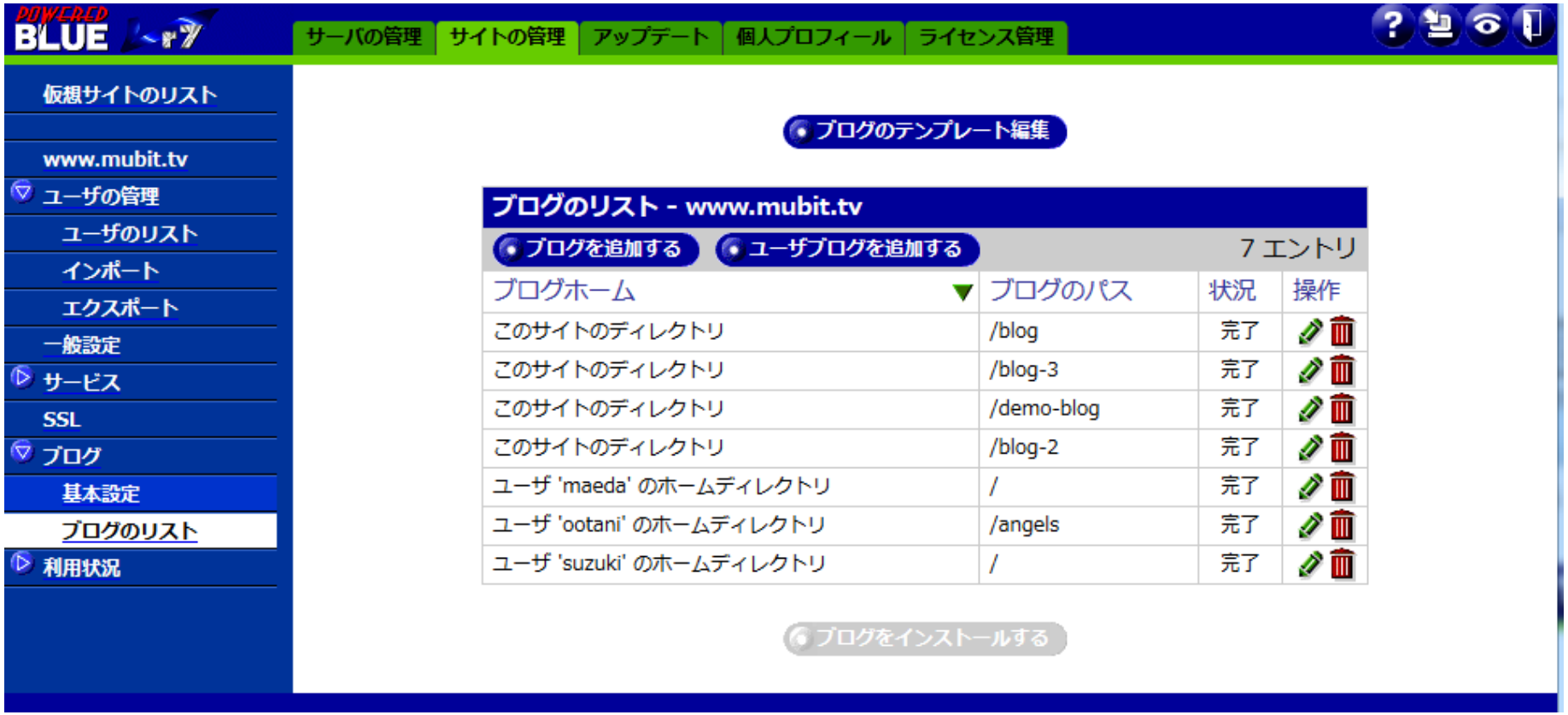
コンポーネント名	詳細
アンチウィルス・ゲートウェイ	
電子メールプラス	

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）

WordPress マルチサイト・マルチユーザー対応



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

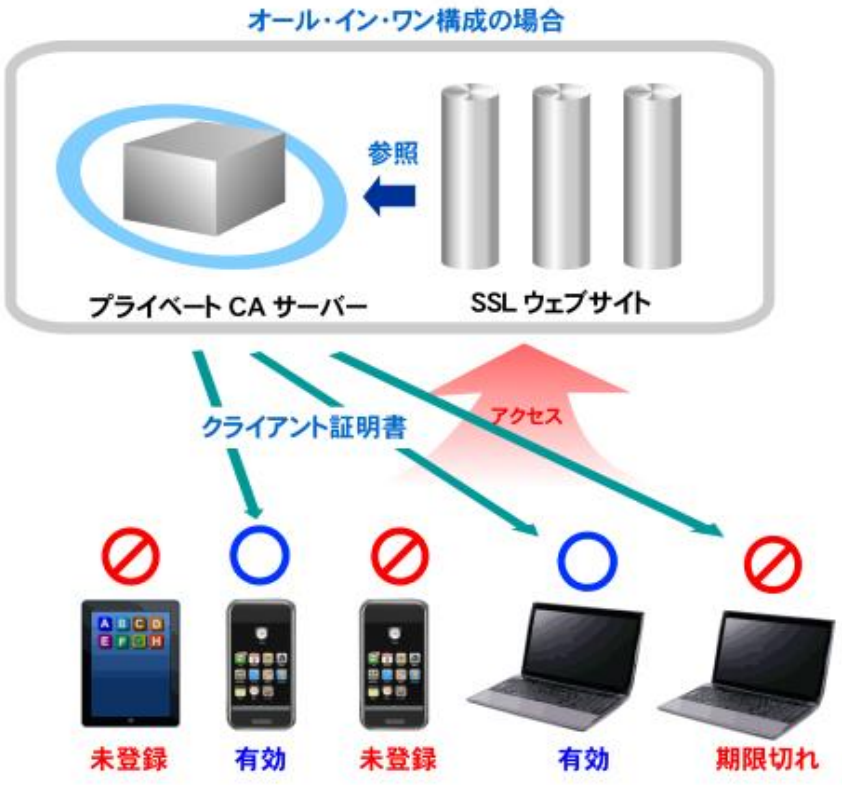
Webサーバーアクセス	証明書	アクセス可否
SSL クライアント証明書	有効	○　社内・部門内
SSL クライアント証明書	失効	×　端末紛失・社員退職
	なし	×　部外者

SSLクライアント認証例　スマートフォン

証明書　有効

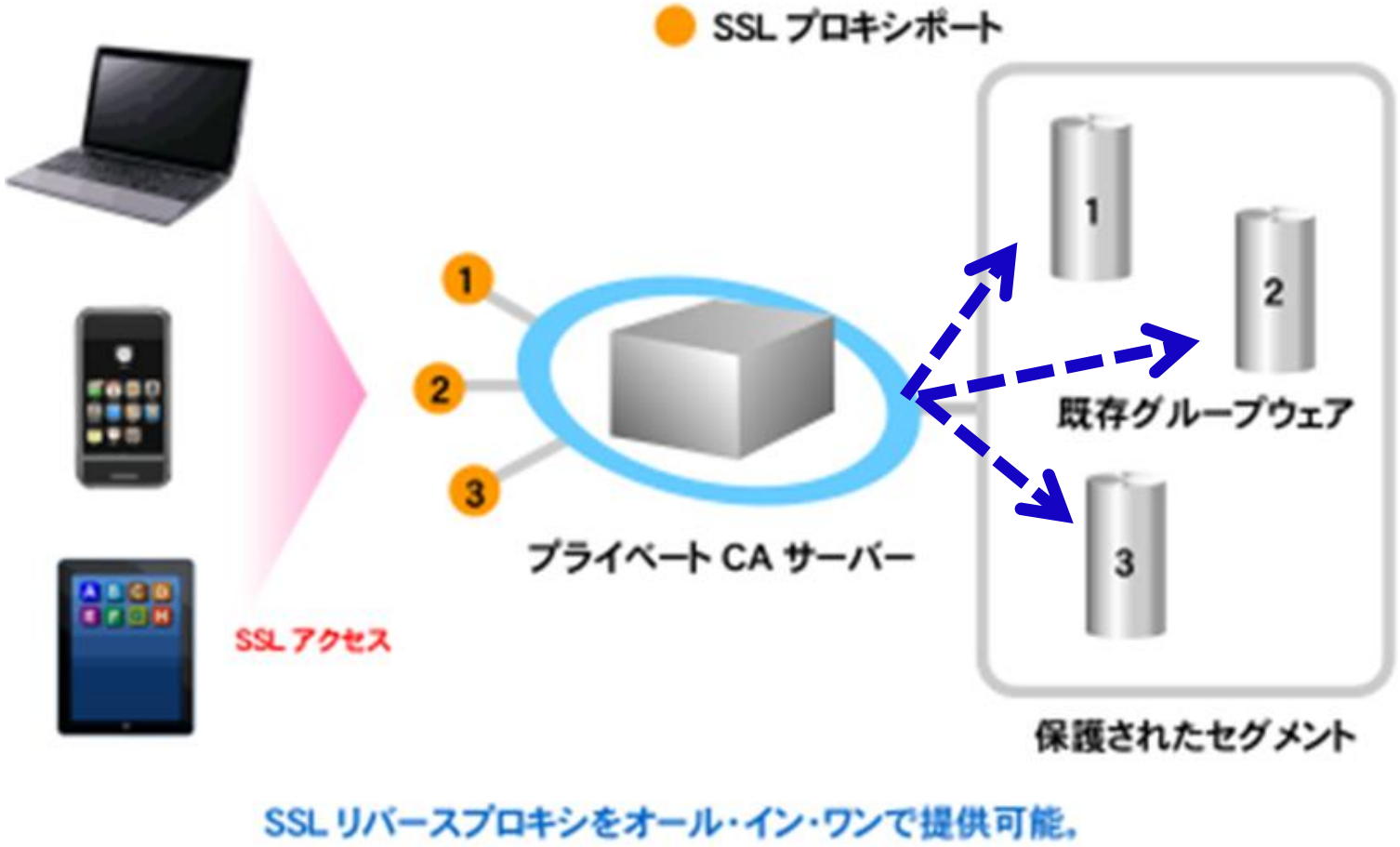
証明書　無効　アクセス不可

Powered BLUE プライベートCA　＋　Web サーバー



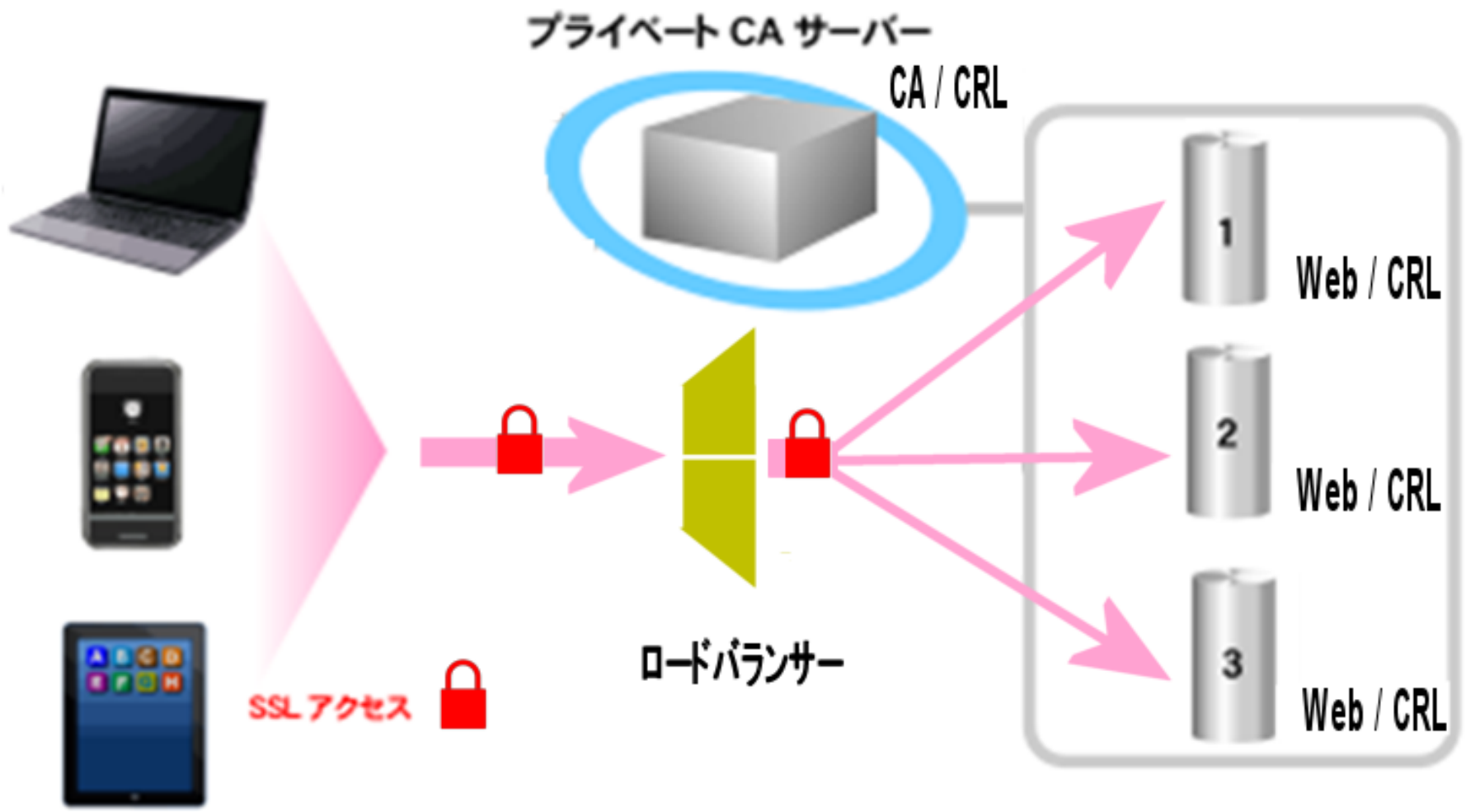
- オールインワン
  - ＣＡとWebを1台での運用に対応

プライベート CA　＋　リバースプロキシ



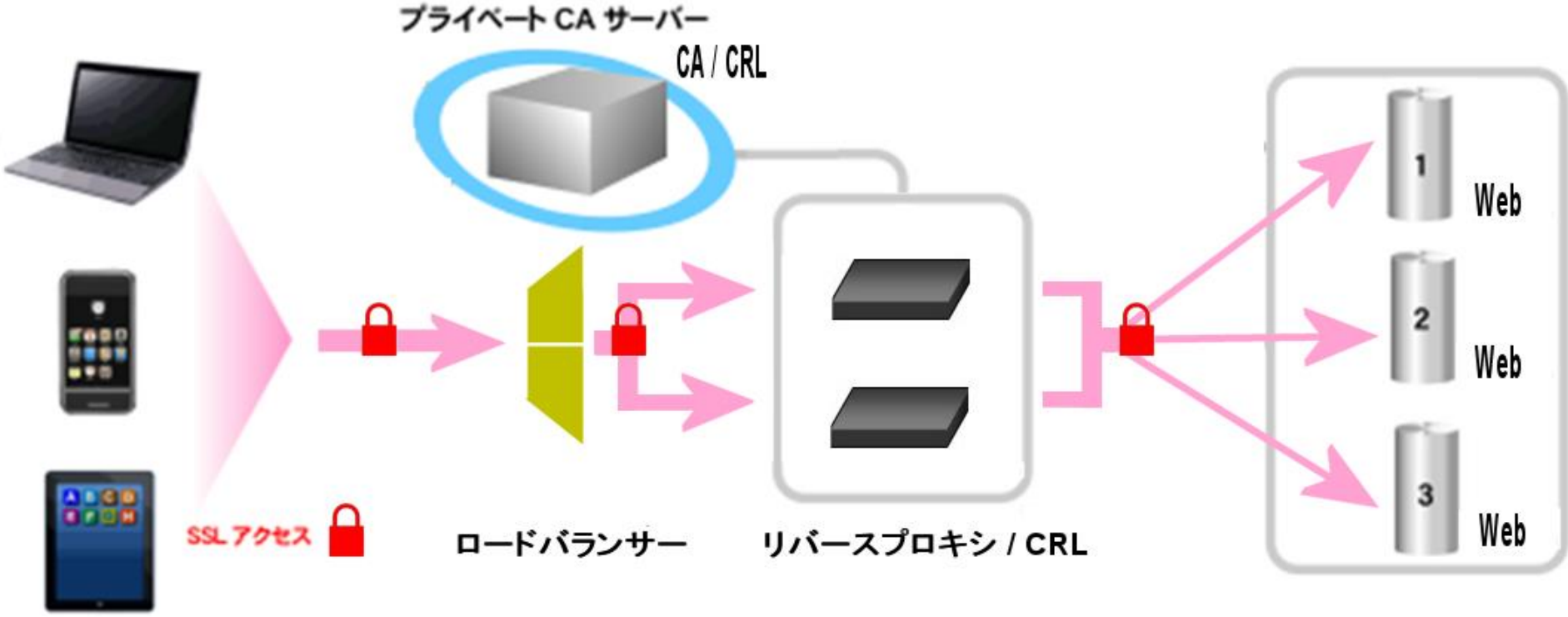
- 既存Webサーバー連携
  - ＣＡ ＋ リバースプロキシ での運用に対応

プライベートCA　＋　ロードバランサー

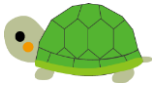


- CA / CRL の分離運用に対応

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
リバースプロキシー	○	既存Webサイトへのリダイレクト

SSLクライアント認証例

グループウエア・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
- 楽NI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

「 Powered BLUE 870 Webアプライアンス」 おさらい

- マルチドメイン ゃ 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 ゃ 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

- 192.168.56.141