

テレワーク対応・Webシステムの認証強化

ワンタイムパスワード認証や
Office365/Azure ADなどiDaaSとの認証連携



OSC2020 Online/Spring

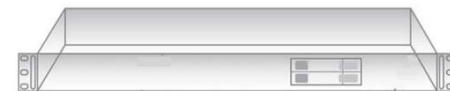
会社概要

社名 株式会社ムービット

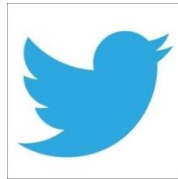
設立 1995年12月8日

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)
ソフトウェア開発



ID・パスワード > 30



amazon.com[®]



Dropbox



iCloud

流出メールアドレスチェックサイト



①



abcd@xxx.co.jp

pwned?

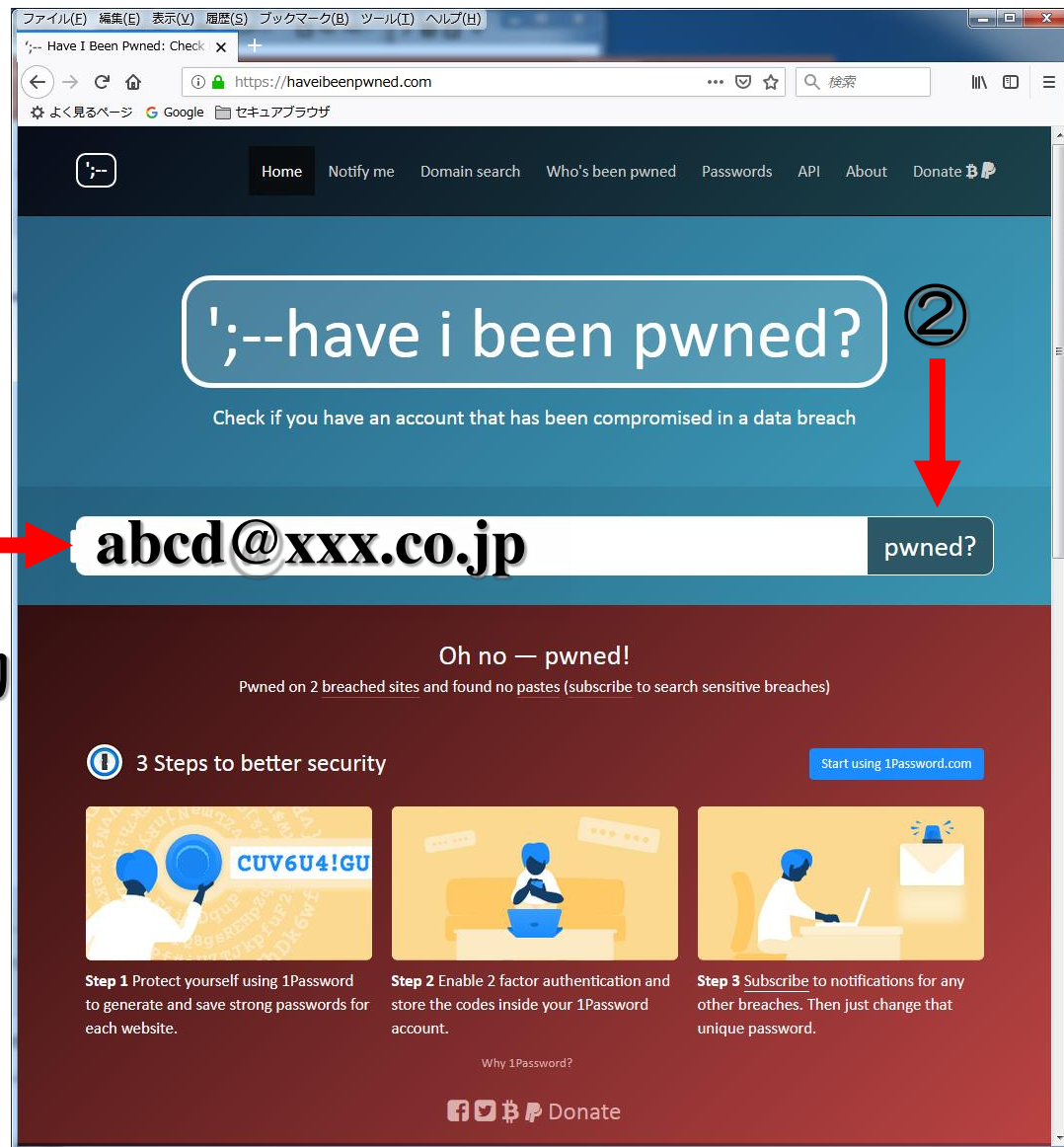
②



- ① メールアドレスを入力
- ② pwned? を押す

Oh no --- pwned !
残念でした

Good news — no pwnage
found!
大丈夫



パスワード流出チェックサイト



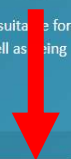
①



password

pwned?

②



Pwned Passwords

Pwned Passwords are 551,509,767 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online system. [Read more about how HIBP protects the privacy of searched passwords.](#)



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)

Password reuse and credential stuffing

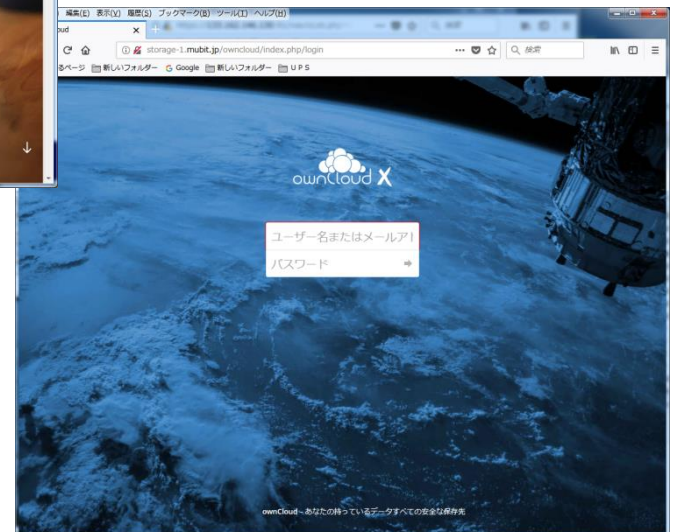
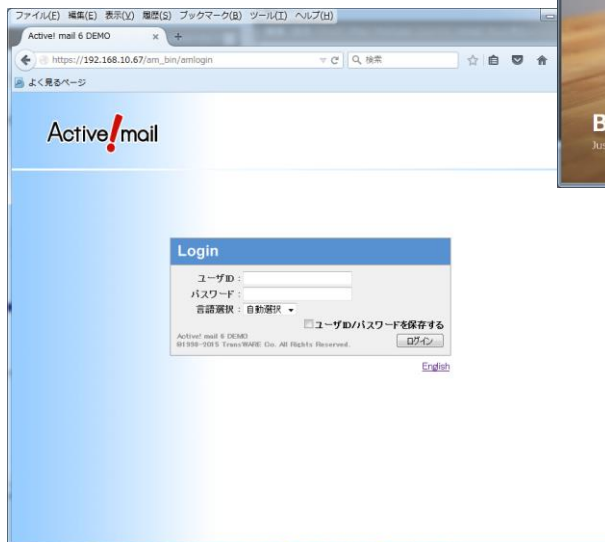
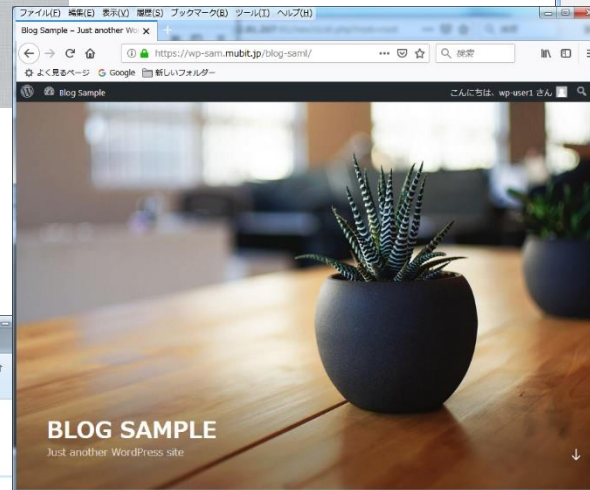
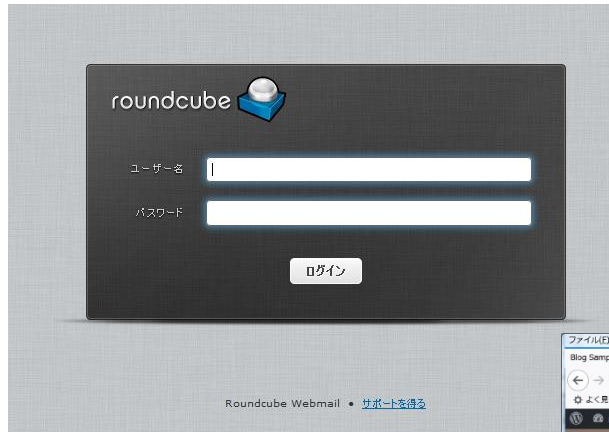
Password reuse is normal. It's extremely risky, but it's so common because it's easy and people aren't aware of the potential impact. Attacks such as [credential stuffing](#) take advantage of reused credentials by automating login attempts against systems using known emails and password pairs.

NIST's guidance: check passwords against those obtained from previous data breaches

The Pwned Passwords service was created in August 2017 after NIST released guidance specifically recommending that user-provided passwords be checked against existing data breaches. The rationale for this advice and suggestions for how applications may leverage this data is described in detail in the blog post titled [Introducing 306 Million Freely Downloadable Pwned Passwords](#). In February 2018, version 2 of the service was released with more than half a billion passwords, each now also with a count of how many times they'd

- ① パスワードを入力
- ② pwned? を押す

テレワーク 社内Web へのアクセス



社内LAN側 の Web への アクセス手法

項目	ターゲット	主な特徴
VPN	network	VPNソフトが必要
モバイル閉域網	network	モバイル端末の専用契約
SSL-VPN	Web アプリ	Web以外のアプリにも対応
リバースプロキシ	Web	アクセス先が隠蔽できる 複数の認証が適用できる WAN側の既存のWebへのアクセスにも利用できる
Worklink	Web	AWS・EC2対応 画像イメージ転送
Proxy connector	Web	Microsoft / エージェント

テレワーク 社内Web へのアクセス



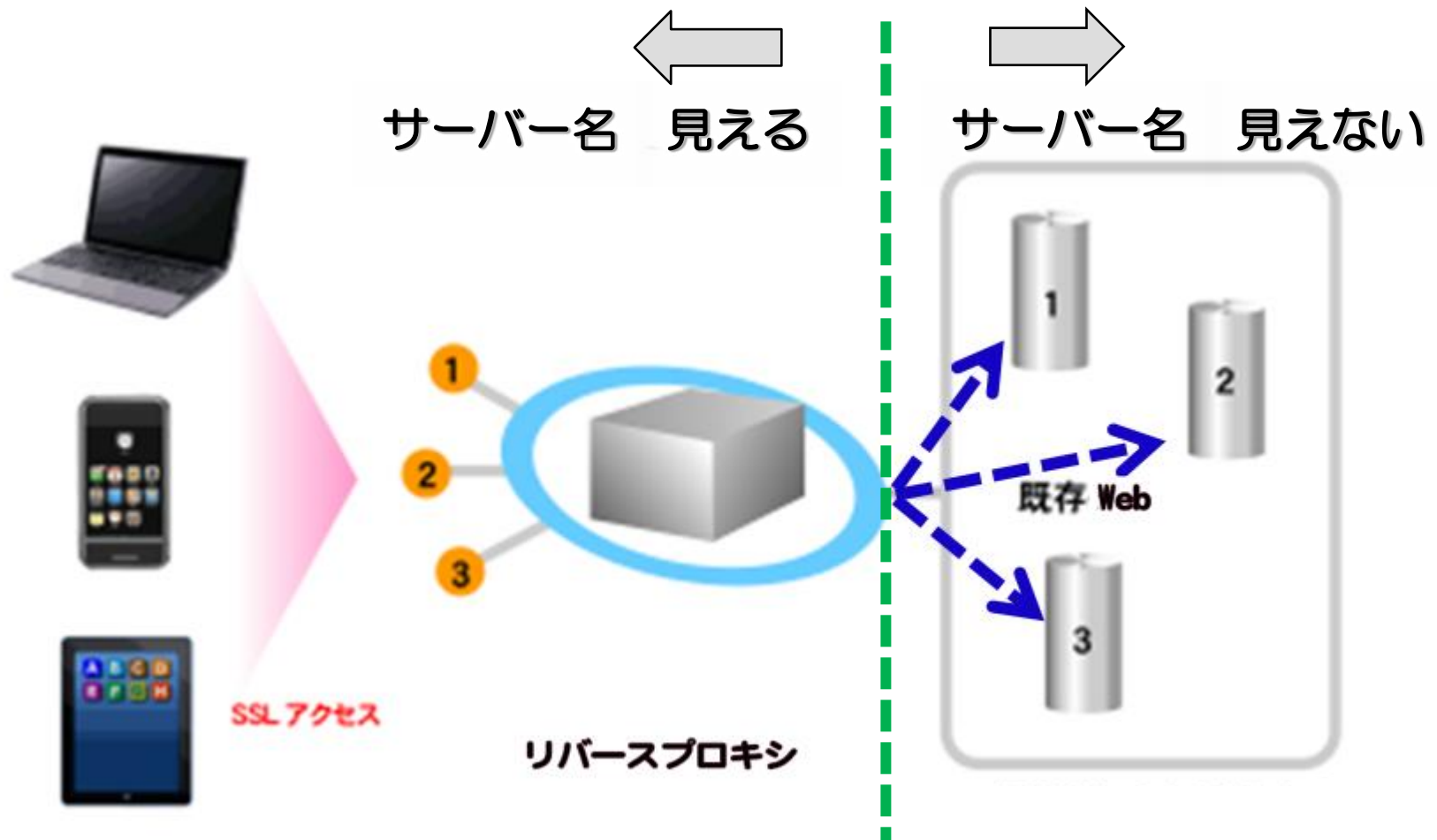
社内Webの 「認証が弱い」 もしくは 「認証がない」

けど



ブラウザを利用して自宅から、会社のWebへアクセスしたい

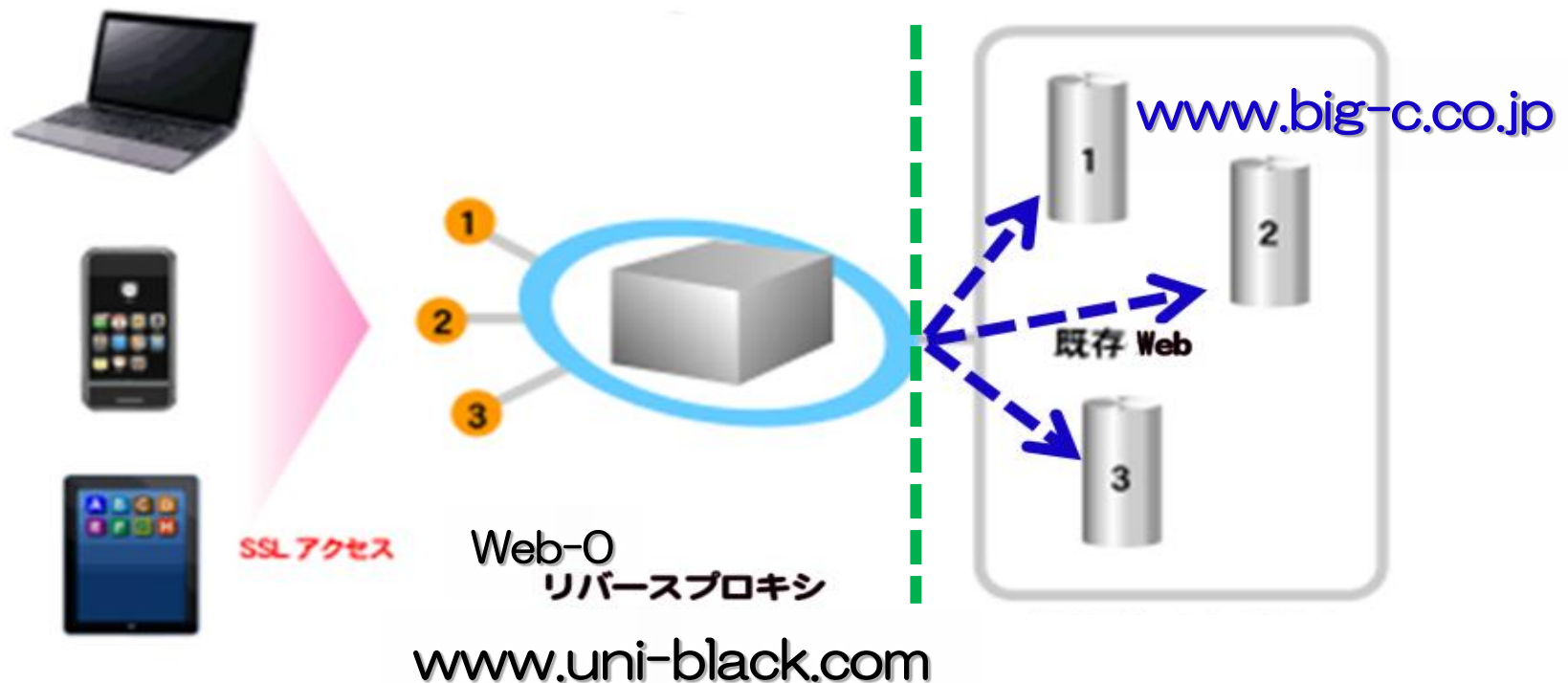
リバースプロキシ



リバースプロキシ経由で既存のWebへアクセス

リバースプロキシ先を隠蔽

リバースプロキシ例 びっくり



Web-0 リバースプロキシ

<http://www.uni-black.com/>



Web-1 リバースプロキシ先

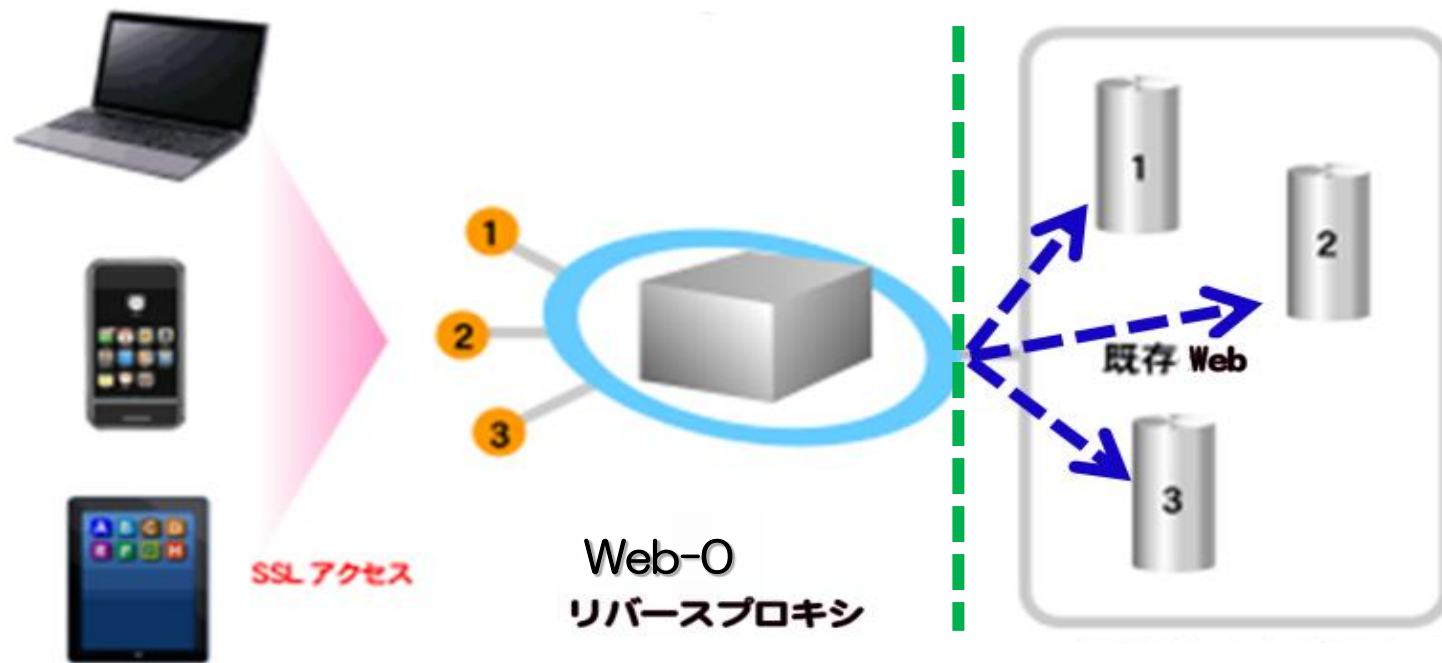
<http://www.big-c.co.jp/pc>



ブラウザへのURL表示

<http://www.uni-black.com/pc>

リバースプロキシ上での認証



- Web-0 リバースプロキシ上での認証
 OTP認証 / SSLクライアント認証 / SAML認証



- Web-1/2/3 リダイレクト

- リダイレクト先のWebの 「認証が弱い・認証がない」 構成でもOK

構築 - 1 OSSで構成の場合

OS



リバースプロキシ Apache / Nginx



OTP認証 / Google Authenticator



GOOGLE AUTHENTICATOR

SSLクライアント認証 / OpenSSL+Let's Encrypt

SAML認証 / SimpleSAML



構築 - 2 とりあえず使ってみる場合

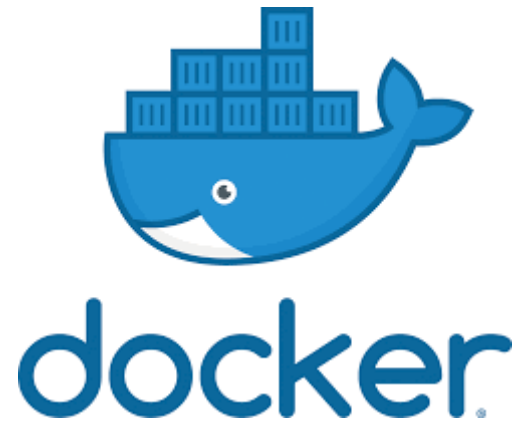
■ Docker イメージ

■ リバースプロキシ Apache / Nginx

■ OTP認証 / Google Authenticator

SSLクライアント認証 / OpenSSL+Let's Encrypt

SAML認証 / SimpleSAML



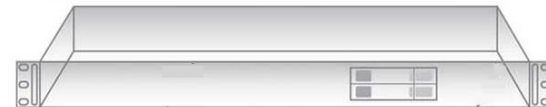
認証対応 「Powered BLUE」 アプライアンス

- ① Web / Mail / DNS 機能 / マルチドメイン対応 / GUI
- ② OTP認証 / SSLクライアント認証 / SAML認証
- ③ リバースプロキシ

認証対応Webサーバー
①+②



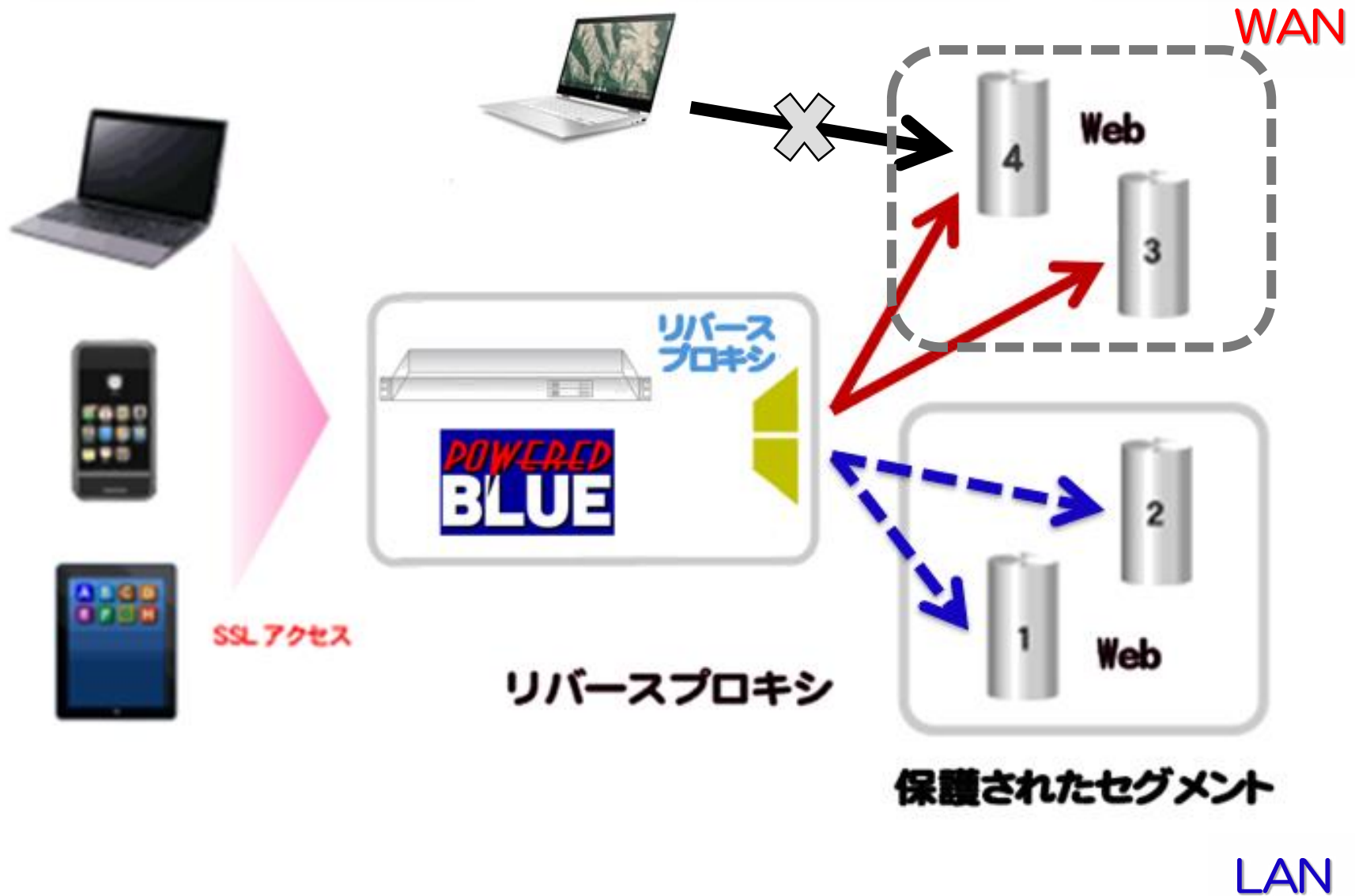
認証対応リバースプロキシ
①+②+③



認証対応 「Powered BLUE」 アプライアンス

	Webサーバー	リバースプロキシ
モデル		
インターネットサーバー機能		
Web	◎	◎
Mail	◎	◎
DNS	◎	◎
GUI	◎	◎
マルチドメイン	○	○
Web認証機能		
ワンタイムパスワード認証	○	○
SSLクライアント認証	○	○
SAML認証	○	○
リバースプロキシ		◎

リバースプロキシ経由のアクセスのみを許可



WAN側へ設置のWebサーバーでもセキュリティを確保

ワンタイムパスワード認証

■ ワンタイムパスワード

30秒間のみ有効 1回限りの使い捨てパスワード



ソフトウェアトークン



ハードウェアトークン

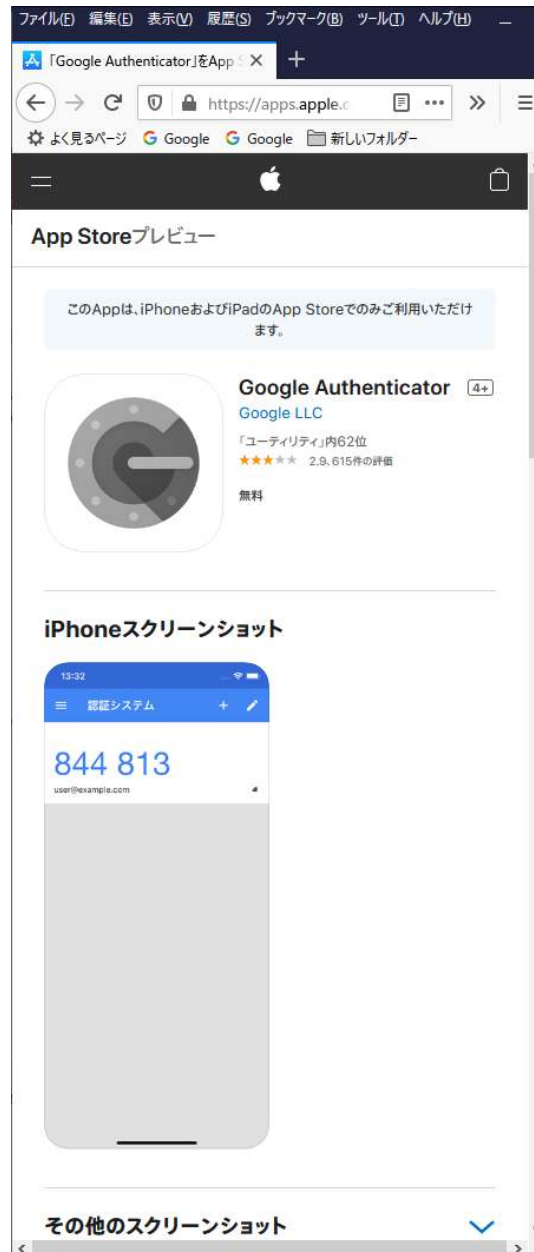
OSS や 無償 の ソフトウェア トークン

製品	iOS Android	PC	言語	対象年齢	
Google Authenticator	○		英語	3歳以上	 GOOGLE AUTHENTICATOR
IIJSmartKey	○		日本語		
Authy	○	○ Windows Mac Linux	英語		
WinAuth		○ Windows	英語		

Google Authenticator / Google Play / AppStore



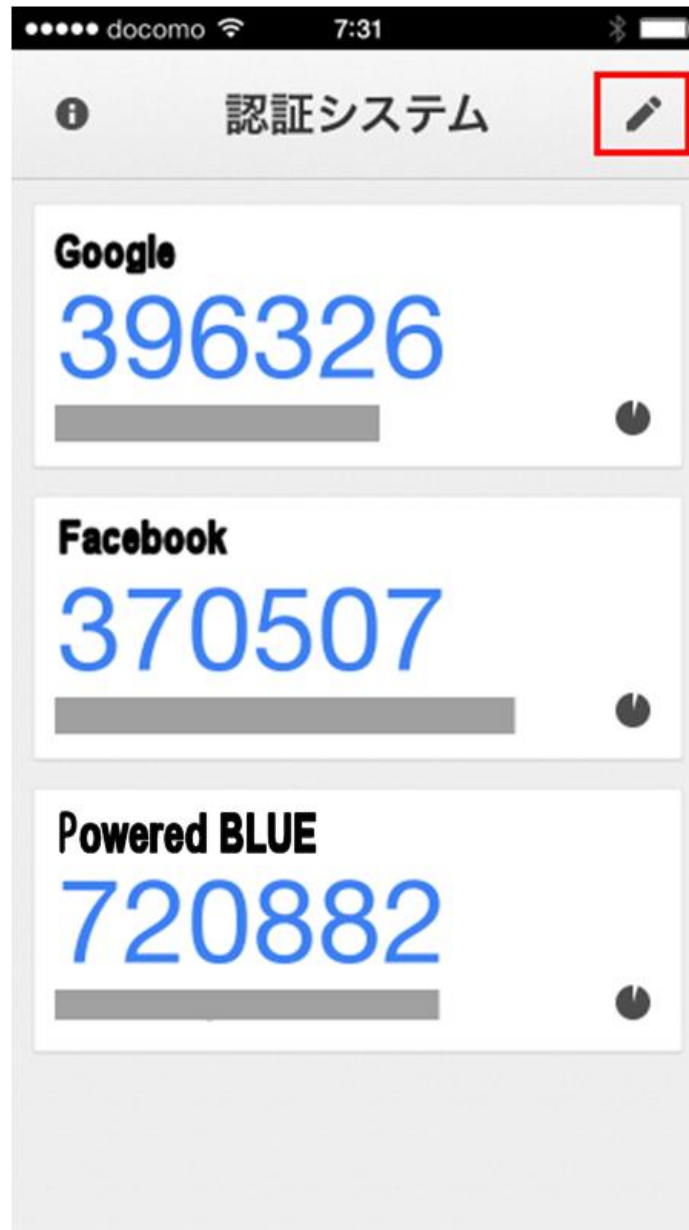
GOOGLE AUTHENTICATOR



QRコードを写メ 複数サイトの登録



GOOGLE AUTHENTICATOR



Powered BLUE サイト
ユーザーのQRコード



ワンタイムパスワード認証 + リバースプロキシ



ワンタイムパスワード認証



ワンタイムパスワード + 任意のパスワード に対応

SSL証明書

■ 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証明書発行元による相違

■ パブリック証明書

- グローバルサイン

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

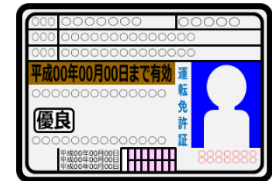
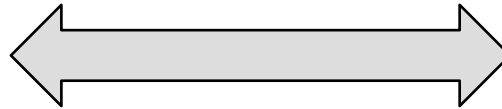
- 有効期間

日・週・月・年単位

相互に確認

■ SSLクライアント証明書

(●プライベート証明書)

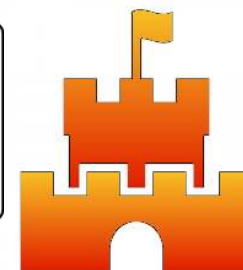


■ SSLサーバー証明書

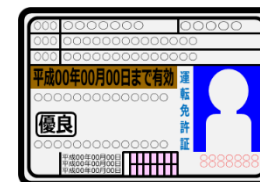
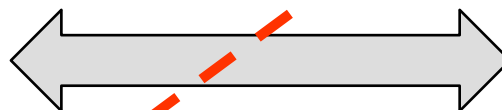
(●パブリック証明書)

■ SSLクライアント証明書

(●プライベート証明書)



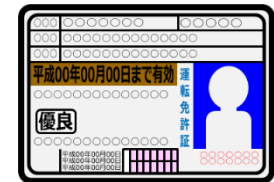
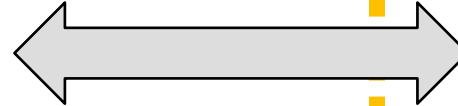
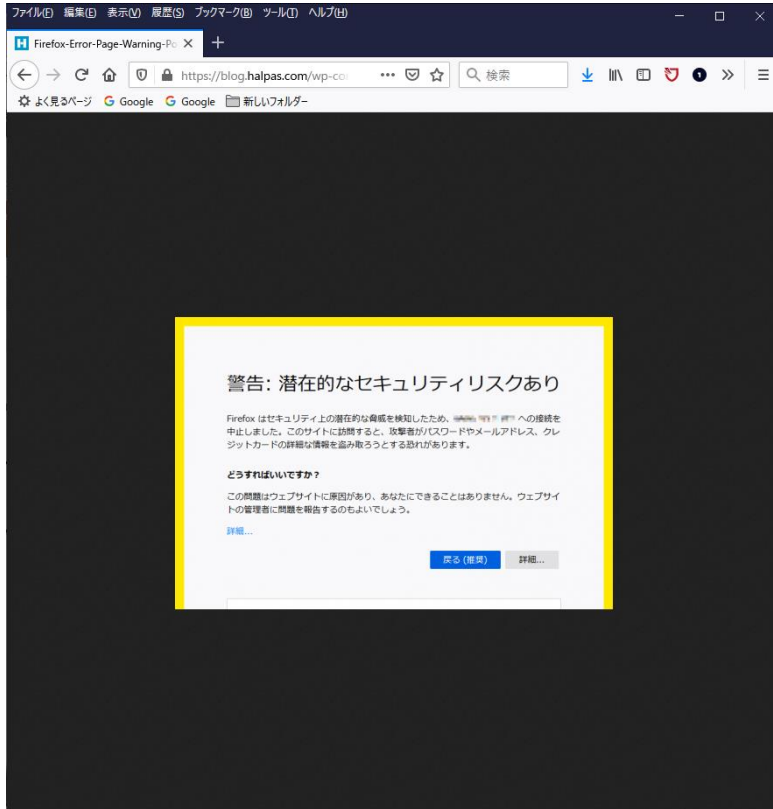
プライベート CA



■ SSLサーバー証明書

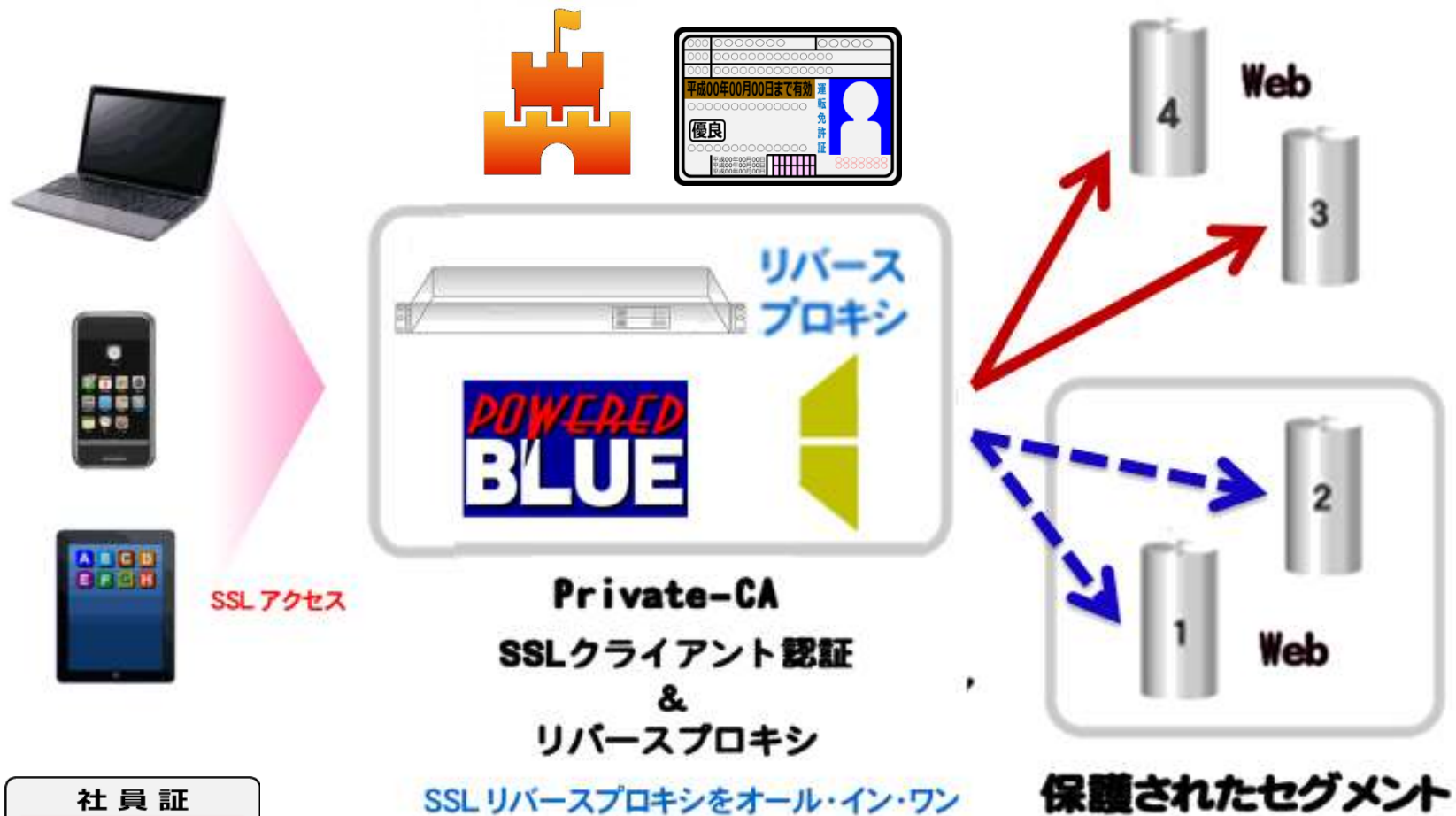
(●パブリック証明書)

プライベートSSLサーバー証明書



■ SSLサーバー証明書
(●プライベート証明書)

SSLクライアント認証 + リバースプロキシ



SSLクライアント認証例 スマートフォン



証明書 有効

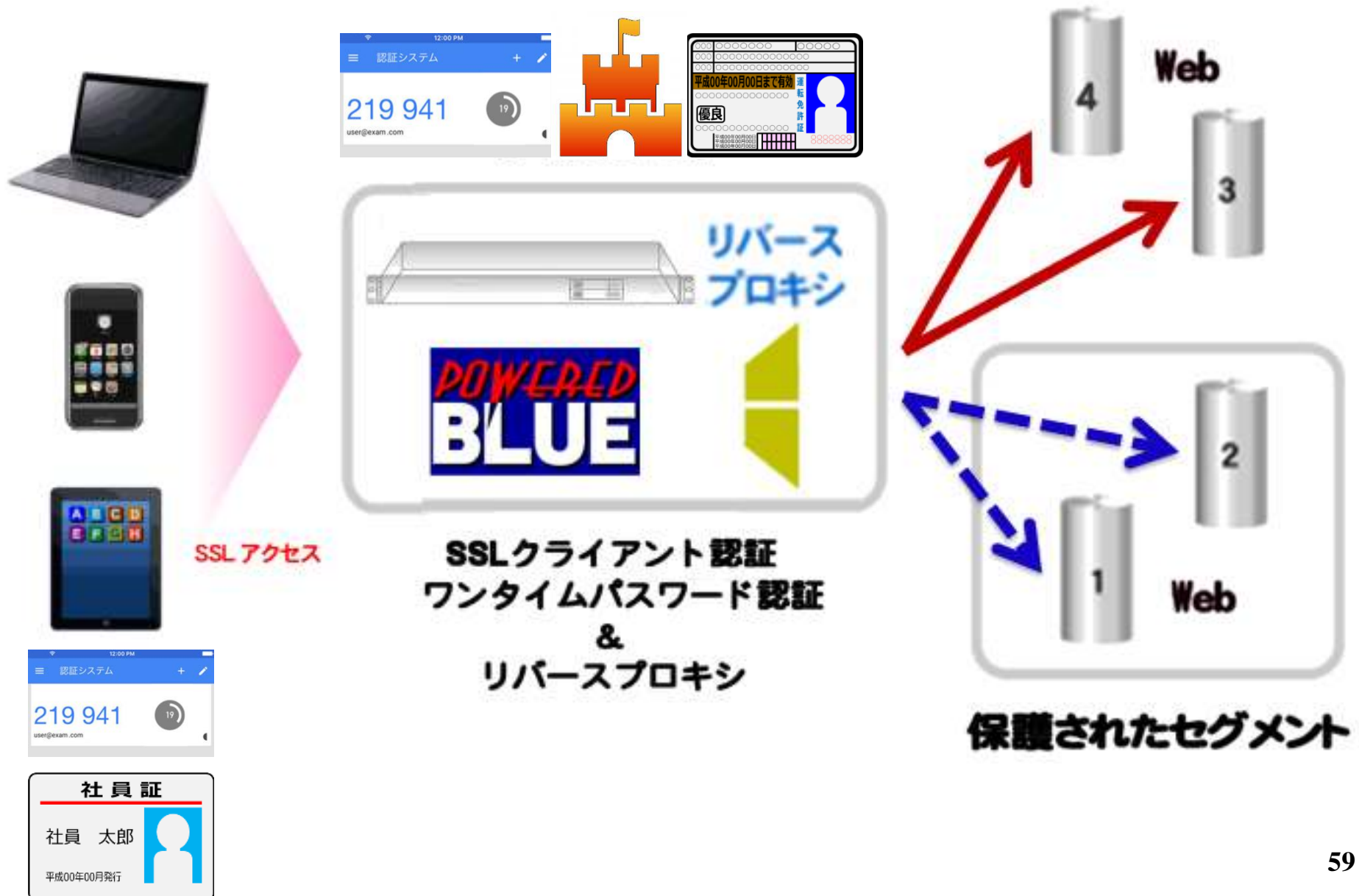


証明書 なし・失効

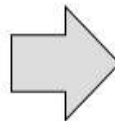
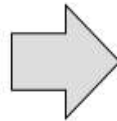
- 組織や部門でのアクセス制限
 - 曜日や時間帯でのアクセス制限
 - 特定ユーザーでのアクセス制限
- 端末を紛失したAさんのSSLクライアント証明書でのアクセス禁止

SSLクライアント認証	
基本 条件 オプション ログ	
クライアント証明書の認証条件	
組織名(会社/団体)	☐ 組織名(O)で制限する 名前
部署名	☒ 部署名(OU)で制限する リスト sales
曜日	☒ 曜日で制限する 曜日 月曜から金曜
時間帯	☒ 時間帯で制限する 開始時刻 9 終了時刻 18
排除設定	
禁止するユーザ	☒ 次のユーザ(CN)を禁止する ユーザリスト no-good@mubit.com

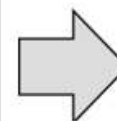
ワンタイムパスワード + SSLクライアント認証



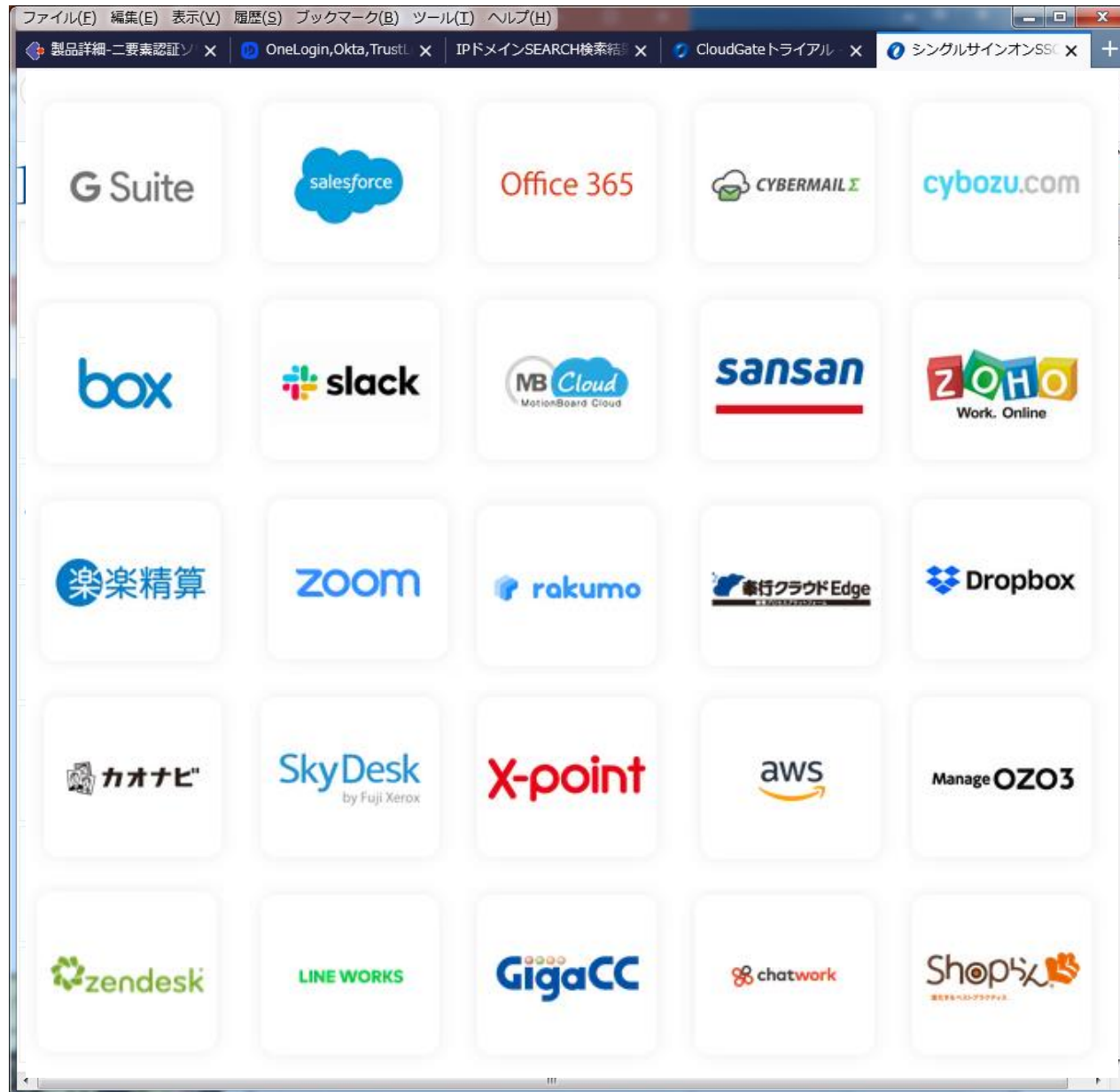
SSLクライアント認証+ワンタイムパスワード認証



SSLクライアント証明書 有効



SaaS のアプリ SSO・SAML（サムル）認証対応



(親) SAML認証 IDaaS など



G Suite

CloudGateUNO
クラウドゲートウノ

onelogin

okta

✦ HENNGE

iDaaS = Id As A Service

iDaaS 比較

	SAML	AD連携	代理入力	GUI 日本語 対応	費用 月額・人
Azure AD 米国	○	○	○	○	672-1000円
OneLogin 米国	○	○	○ IE/Chrome Firefox Safari	△	300-1000円
Okta 米国	○	○	○ IE/Chrome Firefox Safari	×	300-1000円
TrustLogin 日本	○	○	○ IE Firefox Chrome	○	0-300円
CloudGate UNO 日本	○	○	○ Chrome	○	100-1000円

親/ID管理 (IdP)



親 ユーザ管理



Identity Provider(IdP)



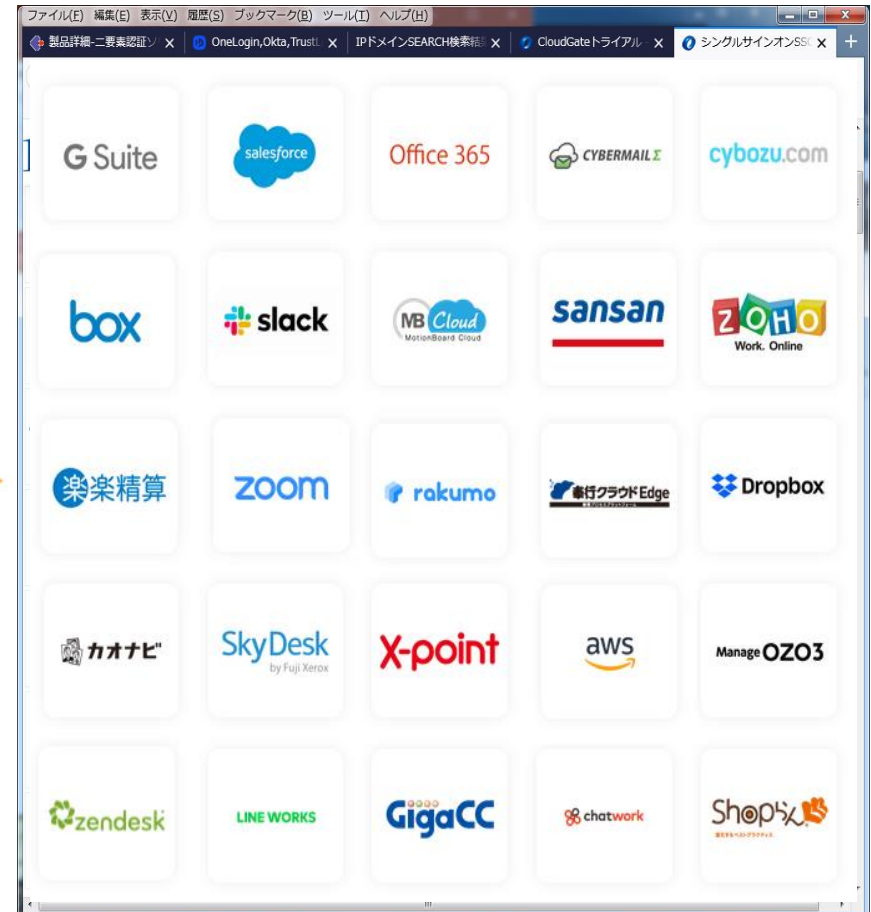
認証

ユーザー



認証

子/アプリ (SP)



親/ID管理 (IdP)

子 リバースプロキシ(SP)



親 ユーザ管理

ユーザー



認証



認証

Identity Provider(IdP)



SSO / SAML認証 + リバースプロキシ



* レガシーなWebサーバーへ、SSO対応のリバースプロキシ経由でアクセス出来ます

SP/リバースプロキシ には ユーザーアカウント不要

- SP/リバースプロキシからのアカウント漏洩の心配はなし

- グループアクセスコントロールに対応

- 営業部・開発部・支店のみにアクセスを許可
- 管理職のみにアクセスを許可
- 社員・会員・代理店のみにアクセスを許可

- SP/リバースプロキシの運用は簡単

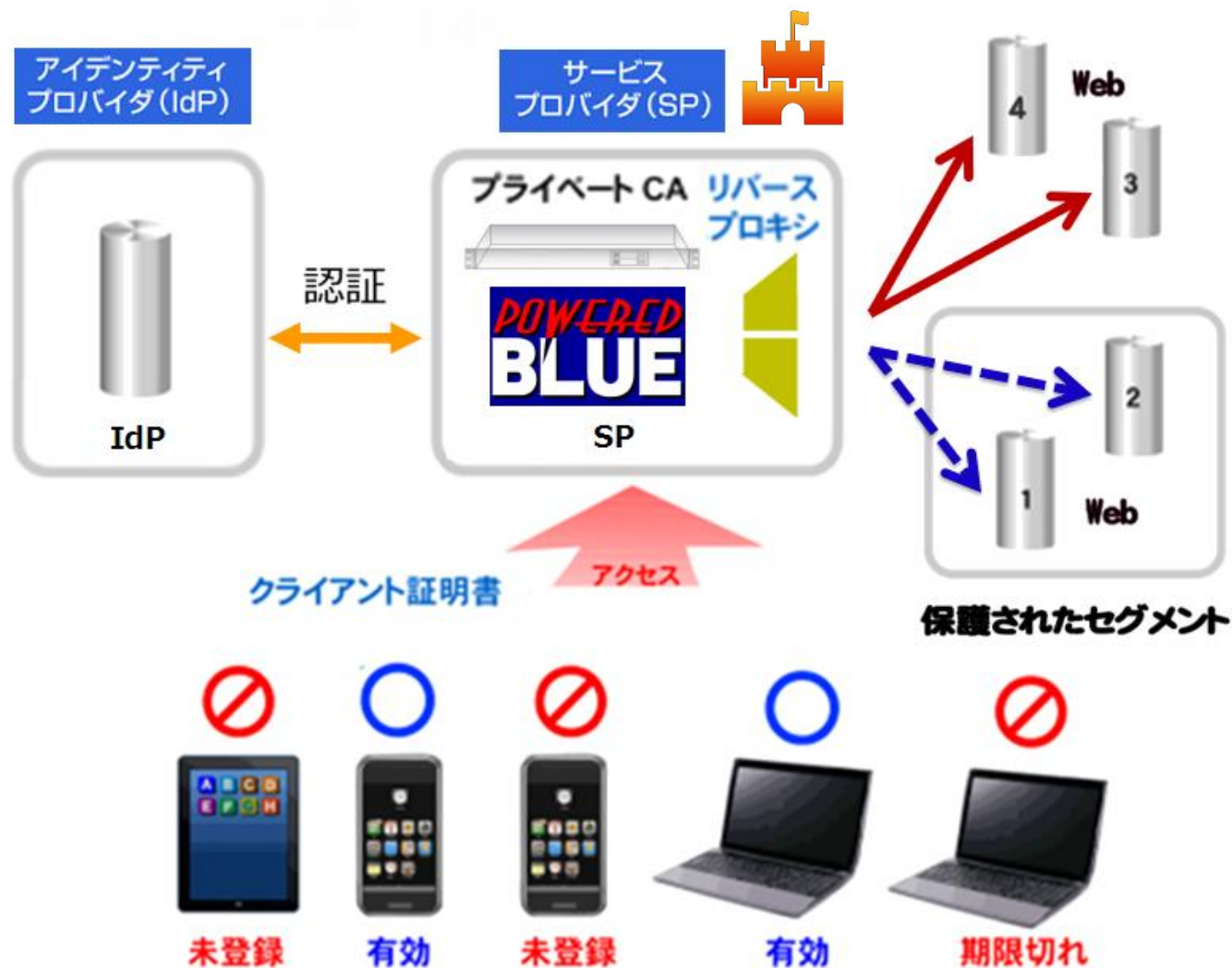


SPでの独自認証 / 社内Webへのアクセス



* idPの認証とは別にリバースプロキシ上に、SSLクライアント認証やワンタイムパスワード認証を独自設定が出来ます

リバースプロキシでの独自認証 SSLクライアント認証



* SSLクライアント認証+SAML 認証対応のリバースプロキシ経由でアクセス

SP/リバースプロキシ導入パターン - ①

- iDaaS を利用の場合 （すでに親がある場合）

Azure AD / TrustLogin / onelogin / **G suite**
CloudGate UNO / HENNGE ONE / okta / OpenAM などを利用

SP のみ 導入



- まだ親がない場合

TrustLogin （親・無償）とSPを導入



SP/リバースプロキシ導入パターン - ②

- Office 365 のid 管理を Azure AD のみで実施の場合



SP を 導入

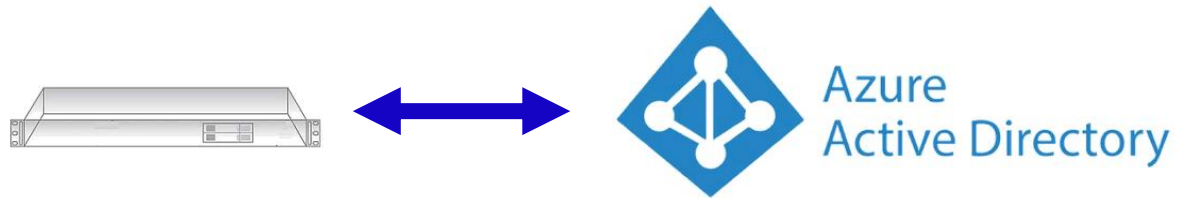


SP/リバースプロキシ導入パターン - ③

- Office 365 のid 管理を AD で実施の場合



Azure AD Connect サーバー を 導入



ADとID/Passwd 同期

SP を 導入



SP/リバースプロキシ導入パターン - ④

■ G Suiteを利用の場合



G suite を idP にする

SP を 導入



ロードバランサー + リバースプロキシ HA



マルチAZ + リバースプロキシ HA



運用先

- リージョンA / 東日本データセンター
- リージョンB / 西日本データセンター

■ 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 ■ 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

新規にWebを構築 「Powered BLUE Web サーバー」



各種の認証対応のWeb

Webアプリケーション（フリープラグイン）



The image shows the WordPress login interface. At the top is the WordPress logo. Below it is a white box containing two input fields: 'ユーザー名またはメールアドレス' (Username or email address) and 'パスワード' (Password). Below the password field is a checkbox labeled 'ログイン状態を保存する' (Remember me) and a blue 'ログイン' (Login) button. At the bottom of the box, there is a link 'パスワードをお忘れですか?' (Lost your password?) and a link 'ムービットのブログに戻る' (Return to Mubit's blog).



The image shows the Roundcube Webmail login interface. It has a dark grey background. At the top left is the 'roundcube' logo with a blue envelope icon. Below it are two white input fields labeled 'ユーザー名' (Username) and 'パスワード' (Password). Below the password field is a white 'ログイン' (Login) button. At the bottom, there is a small link 'Roundcube Webmail' and a link 'パスワードを忘れた' (Forgot password).

同一サイト内で複数の
WordPressを構築・運用

SSLサーバー証明書の
自動更新対応

WebMail

Web + ワンタイムパスワード認証



Web + SSLクライアント認証



Web + SAML認証



Web • SAML認証 + SSLクライアント認証



Webでの独自認証 SSLクライアント認証

SSO対応の「Powered BLUE Web サーバー」

親/ID管理 (idP)



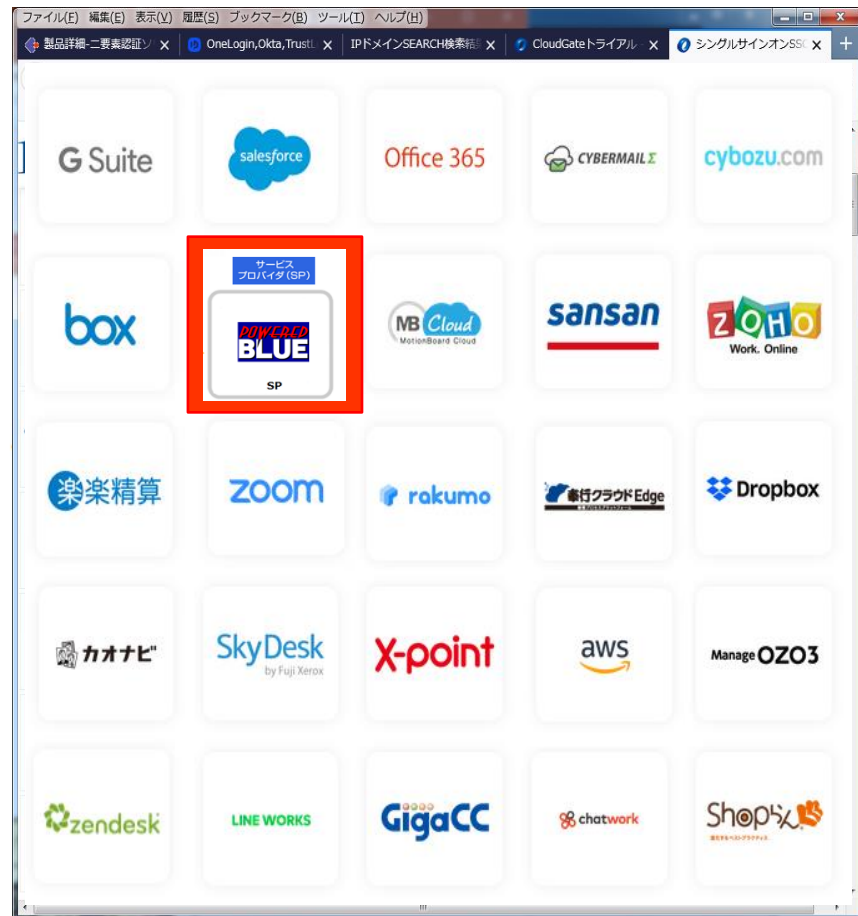
親 ユーザ管理

ユーザー

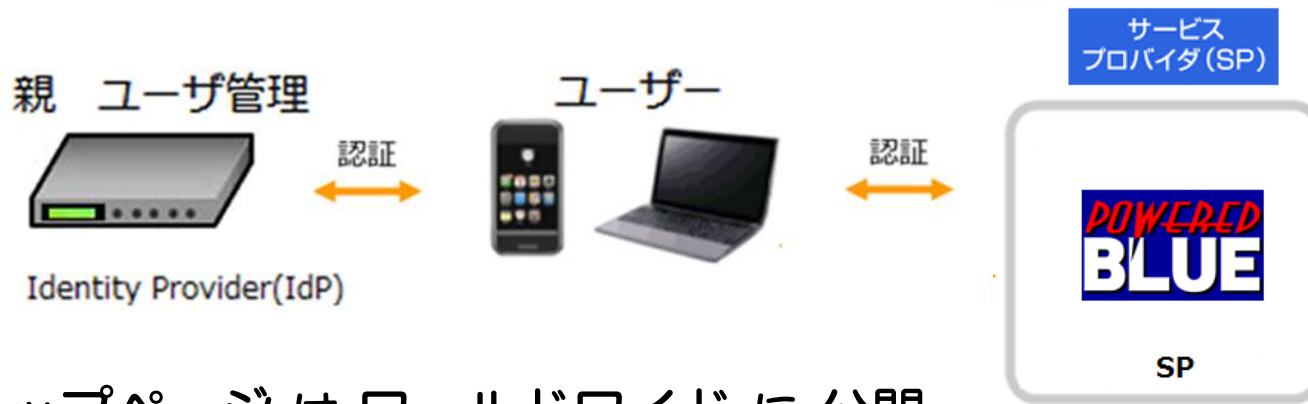


Identity Provider(IdP)

子/アプリ (SP)



こんな使い方 会員向け Web の SaaS化



- トップページはワールドワイドに公開

WordPress でWebページ作成



- 特定のdirは、会員のみにアクセス許可

ゴールド会員・シルバー会員・一般会員

- TrustLogin に 会員用のアカウントを作成 例 500名

- Webサーバー (SP) にはユーザーアカウント不要

ロードバランサー + Web HA



マルチAZ + Web HA



運用先

- リージョンA / 東日本データセンター
- リージョンB / 西日本データセンター

Powered BLUE の位置

自社運用 = オールインワンのアプライアンス

Powered BLUE (OS + GUI + アプリ)

Pass

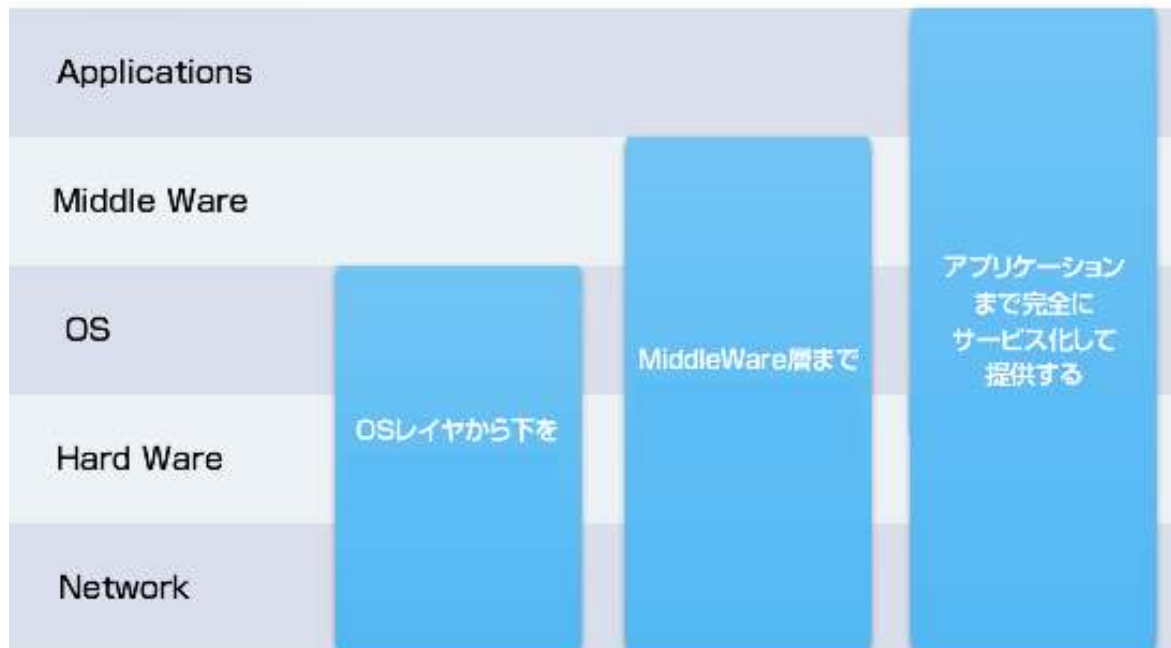
IaaS

OS まで

IaaS

PaaS

SaaS



自社の管理下で運用出来るアプライアンス

「 Powered BLUE 」 運用環境

■ 仮想アプライアンス
VMware / Hyper-V

■ クラウド対応
AWS
Azure
.....

■ オンプレ



**POWERED
BLUE**



アプライアンスでの提供・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 / 6.7

Hyper-V 7.X

クラウド環境

AWS / EC2

Azure / Microsoft

FUJITSU Cloud Service for OSS / 富士通

Enterprise Cloud / NTTcommunications

VPS / WebArena / NTTPCコミュニケーションズ

スマートコネクT VPS / NTTスマートコネクT

ALTUS / GMOクラウド

VPS 他

スペック

1 Core(min) / 2014MB mem (min) / 20GB HDD (min) / Ethernet x 1(min)

電源オンで、すぐに運用が出来ます

ひとり情シス対応

サーバーのモニタリング & サービスの自動再起動

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

パッチのアップデート

OSアップデートの設定	
自動更新設定	
更新スケジュール	☐ 毎時 ☐ 毎日 ☒ 毎週 曜日 土曜 ▼ ☐ 毎月 日 1 ▼ ☐ 設定しない
更新時間 (時)	12 ▼
更新時間 (分)	12 ▼
一般設定	
除外パッケージ (省略可)	kernel* glibc*
管理者通知	☐

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 ☒

ログサーバー機能



既存のサーバ(クライアント)のログをリモートサーバへ送る

1)冗長送信

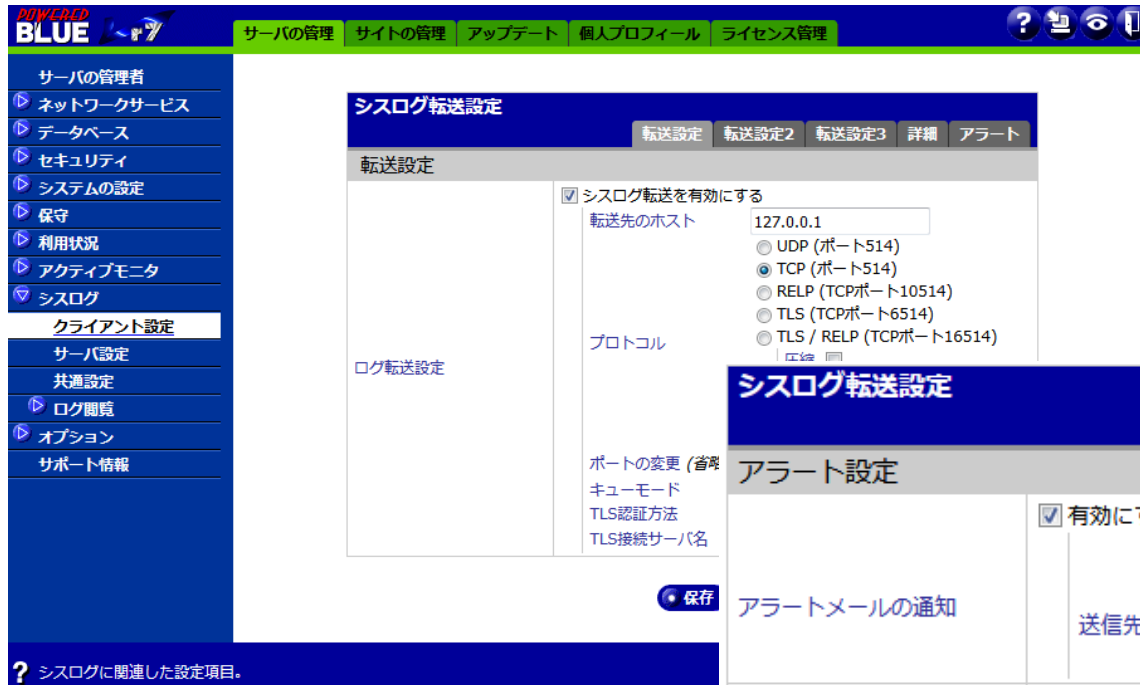
最大 3台へ同時 に送信

2)漏洩防止

TLS通信 & 機器認証

3)欠落防止

送信キュー によるログの一時保管



テレワーク関連の助成金

■ 厚生労働省の助成金

150万円 助成率 3/4

申込み 2020/12/1まで

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/roudoukijun/jikan/telework_10026.html

■ 東京都の助成金

250万円 助成率 10/10

申込み 2020/5/12まで

<https://www.nikkei.com/article/DGXMZO56550070Z00C20A3000000/>

- インターネットサーバー
Webやリバースプロキシ
- Web認証
ワンタイムパスワード認証
クライアント認証
SAML認証
- 自社運用に対応のアプライアンス
電源オン 10分 で運用開始
- 冗長化構成に対応

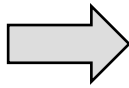
Webサイト



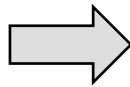
<https://www.mubit.co.jp/>

The screenshot shows the Mubit website interface. At the top, there's a navigation bar with links: ホーム (Home), 製品 (Products), 認証機能対応 (Authentication Function Support), お知らせ (Notice), ブログ (Blog), お問い合わせ (Contact Us), サポート (Support), and 会社 (Company). Below this, there's a section titled "認証機能対応 Web アプライアンス" (Authentication Function Support Web Appliance) with the Mubit logo. To the right, contact information is displayed: TEL: 03-5390-3553 and the address in Tokyo. The main content area features several product cards under the "Powered BLUE シリーズ" (Powered BLUE Series) heading. These include: "SAML / OTP / SSL 認証機能付属 Web" (SAML / OTP / SSL authentication function attached Web), "Powered BLUE 870 (標準Webサーバー)" (Powered BLUE 870 (Standard Web Server)), "SAML/OTP/SSL 対応 リバースプロキシ" (SAML/OTP/SSL compatible Reverse Proxy), "Powered BLUE プライベートCA" (Powered BLUE Private CA), and "添付ファイル暗号化" (Attachment File Encryption). Each card has a brief description of its features.

認証対応
Web



認証対応
リバース
プロキシ



■ メール

問い合わせフォームから

<https://www.mubit.co.jp/>

■ Web ミーティング

■ Powered BLUE デモ

SAML / OTP / SSLクライアント認証

Web / リバースプロキシ