

IDaaS利用で 社内WebもSSO



Powered BLUE Web for SSO/ IDaaS

株式会社ムービット

SSO (Single Sign On)



* 自社のWebサーバーをSSO対応にすることが出来ます

連携出来るIDaaSなど

TrustLogin

Azure Active Directory

onelogin

CloudGate

okta

HENNGE

idP側はSAML2.0に対応していれば連携出来ます

「Powered BLUE Web for SSO/ IDaaS」



- ① Powered BLUE 870 インターネットサーバー機能
- ② SSO認証対応Web サーバー
- ③ SSLクライアント認証 / ワンタイムパスワード認証

① Powered BLUE 870

インターネットサーバー機能

Web/Mail/DNS/FTP/ サーバー機能を1台で運用

RedHat / CentOS 7.x (64bit) に対応



フリープラグイン

Let's Encrypt (無償SSLサーバー証明書 / 自動更新)

WordPress (CMS / ブログ / ホームページ)

ownCloud (オンラインストレージ)

Roundcube (Web Mail)



サードパーティソフト

サイボウズ デスクネッツ 監視ソフト UPS 他

② SSO対応Web サーバー

1) SSO

SAML 2.0 対応

③ オプション SSLクライアント認証 / OTP認証

1) Private CA 機能

SSLクライアント証明書発行・管理

2) SSLクライアント認証 機能

リバースプロキシのSSLクライアント認証

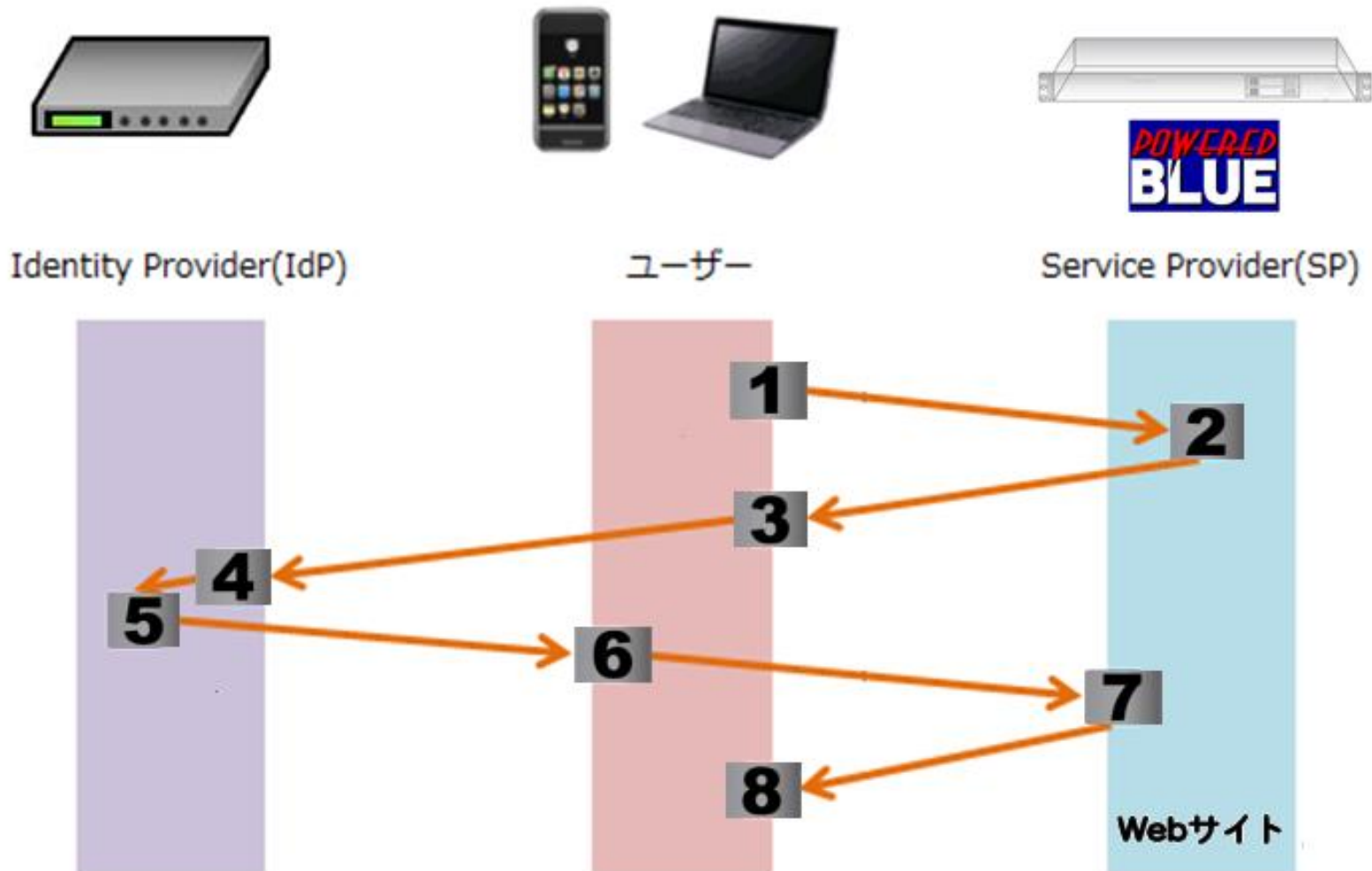


3) ワンタイムパスワード認証

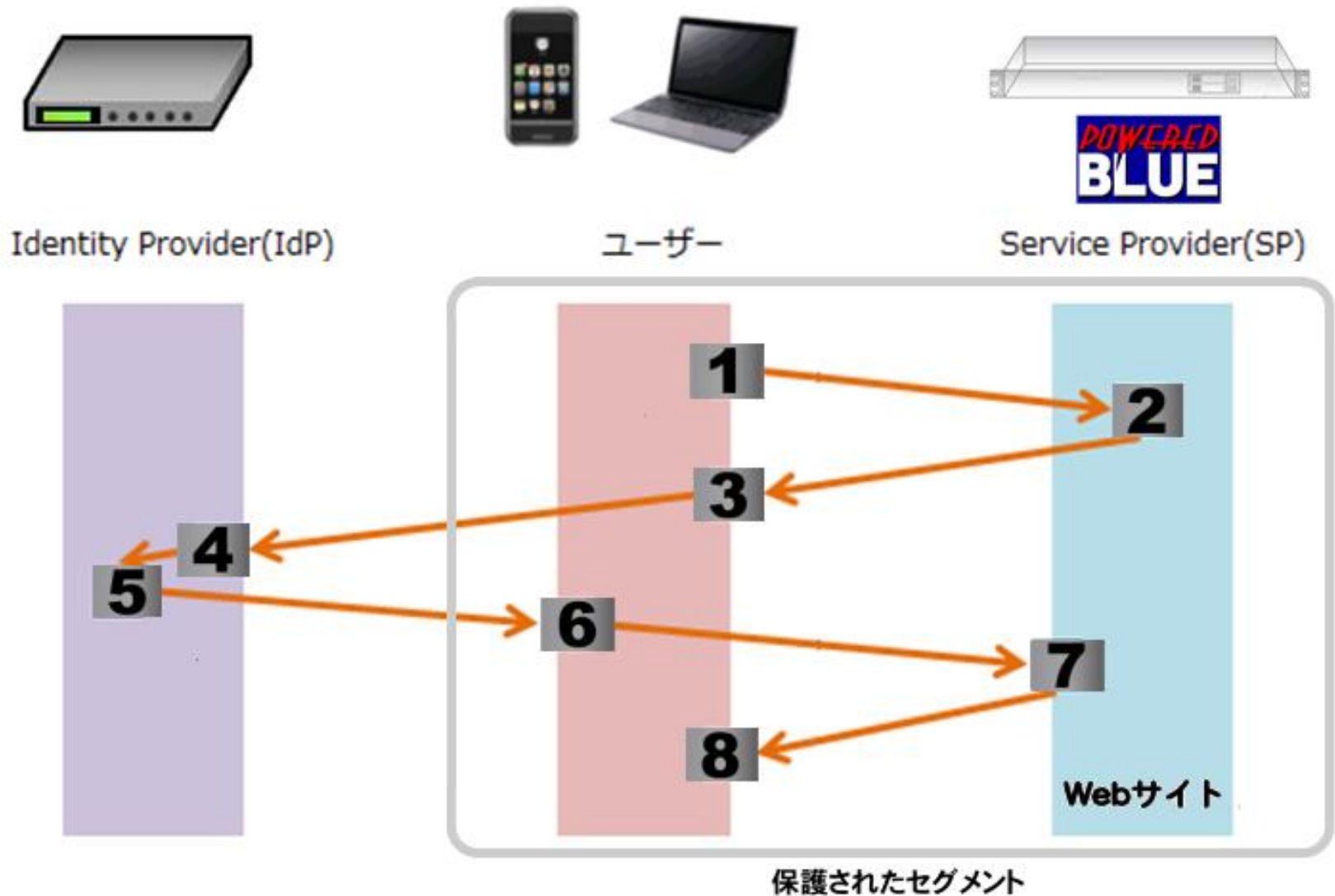
リバースプロキシのワンタイムパスワード認証



① SAMLの通信手順（SP-initiated SAML）

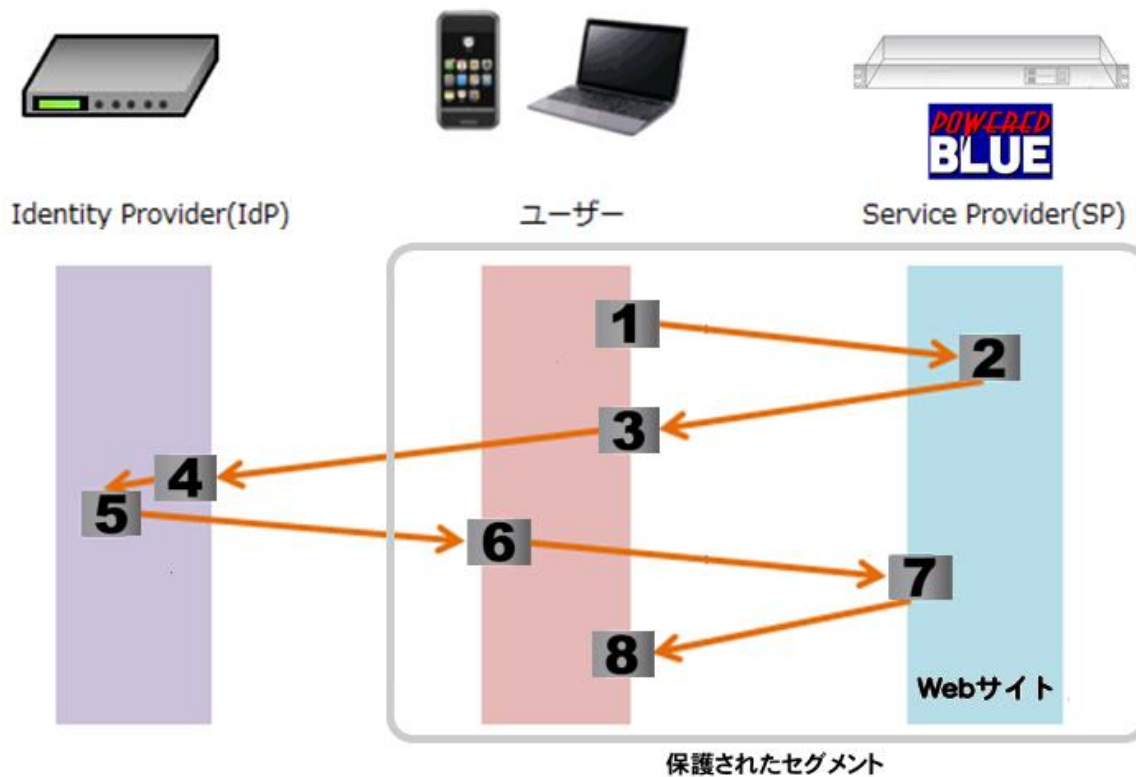


① Powered BLUE Web for SSO/IDaaS 設置場所



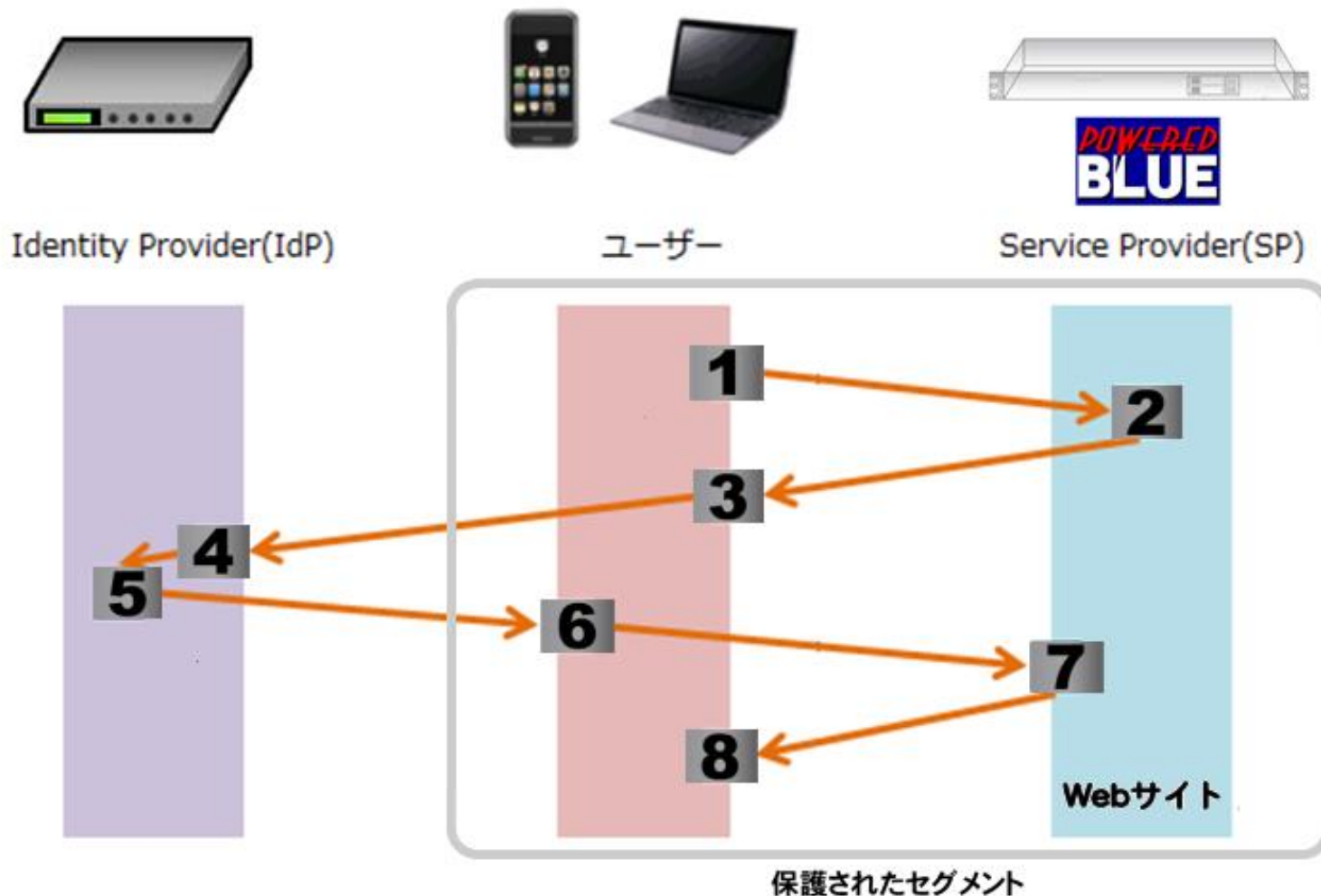
①社内用のWebサーバーをLAN内に設置の場合

- LAN側のWebサーバー（SP）の認証をWAN側のidPで行う
- グループ毎のWebサイトへのアクセス認証を設定
- Webサーバー（SP）にはユーザーアカウント不要



①社内用のWebサーバーをLAN内に設置の場合

- LAN側のWebサーバー（SP）の認証をWAN側のidPで行う
- Webサーバー（SP）には、ユーザーアカウント不要



① Powered BLUE Web for SSO/IDaaS 設定手順



- SSO対応WebサイトにWordPressを組み込む



- 作成したWebサイトはLet's EncryptでSSL化



- 作成したサイトをidPへ登録してSAML2.0連携

① Powered BLUE Web for SSO/IDaaS 使い方



● WAN側にWebサーバー(SP)を設置

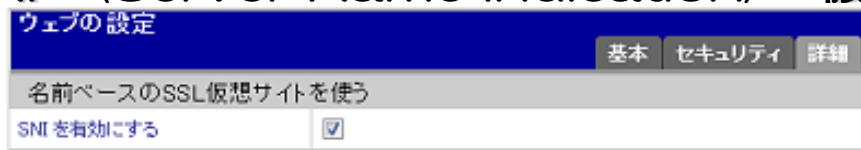
トップページはワールドワイドに公開
特定のディレクトリは、社員や会員のみ閲覧を許可
Webサーバーには、アカウント不要

● LAN側にWebサーバー(SP)を設置

営業部・開発部・総務部など部門毎にアクセス制限を設定
Webサーバーには、アカウント不要

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 ☒

ひとり情シス対応

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

仮想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 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 スマートコネクトVPS / NTTスマートコネクト 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)

仮想環境にインポートするだけで、すぐに運用が出来ます

Powered BLUE Web for SSO/ IDaaSの位置

SaaS

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仮想アプライアンス