

オープンソースで実現する Windowsログオンと SSOと ID管理



OSSTech

オープンソース・ソリューション・テクノロジー株式会社
代表取締役 チーフアーキテクト 小田切 耕司

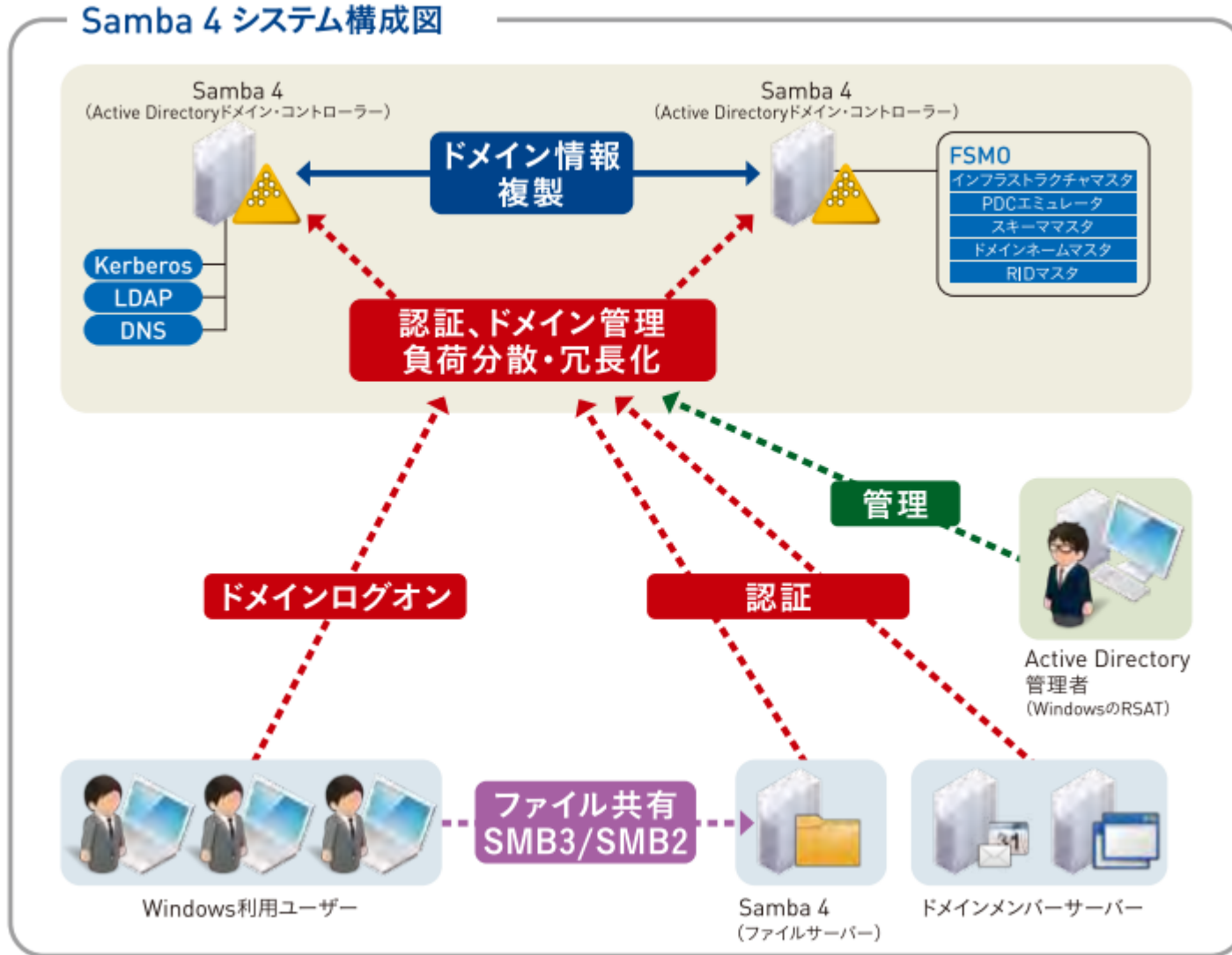
お問い合わせ info@osstech.co.jp

Linux上でADを実現

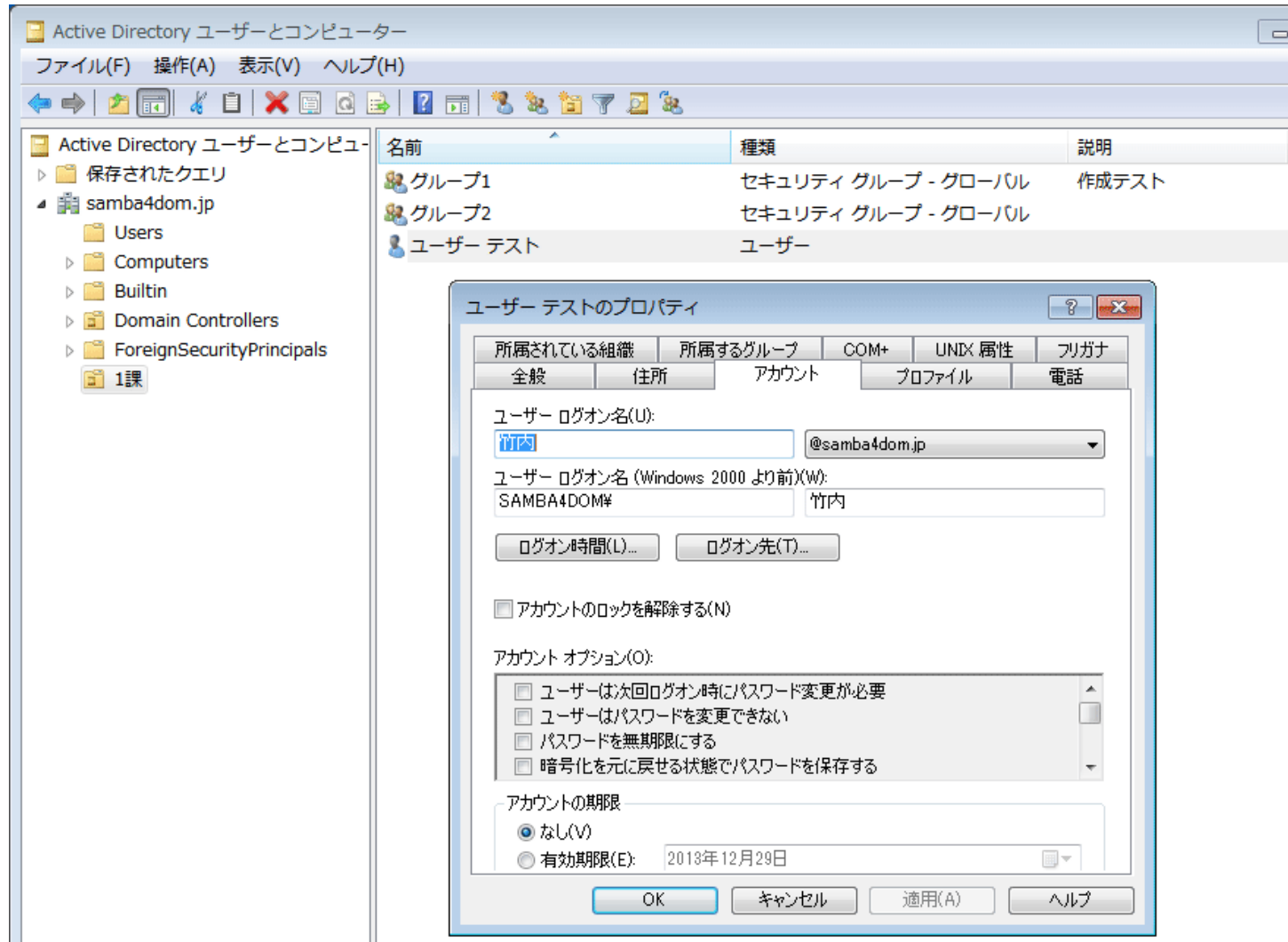
Samba 4紹介

- Active Directory互換のオープンソース・ソフトウェア製品
- ADからの移行だけではなく、OpenLDAPやSunJavaDirectorySever (Oracle Directory Server) などのLDAP製品の置き換えも可能

Samba 4とは？



Samba 4はWindowsクライアントのGUI(RSAT: リモートサーバー管理ツール)で簡単操作



Samba 4とは？

Active Directory互換

- Linuxサーバー上でActive Directoryサーバーを動作させることが可能
- 管理はWindowsクライアントのGUI(RSAT:リモートサーバー管理ツール)で行えるので操作を新しく覚える必要がない
- CAL (Client Access License) が不要
- ADとしてのみ利用する場合はアンチウィルスソフト購入不要
- AmazonのCloud DirectoryはSamba 4

OpenAM連携: (Kerberos認証による)DesktopSSOが可能

- Windowsログインのみでブラウザのログインを不要に

LDAPv3準拠

- TLSによる暗号化通信 (ldaps接続が可能)
- UNICODE対応、スキーマの拡張やアクセス制御機能

OpenLDAPやOracle (旧SunJava) Directory ServerなどのLDAPも置換可能

- 初期導入がコマンド1つで可能(TOPツリーのLDIF投入不要)
- マルチマスター対応で、冗長化もコマンドひとつで可能
- 管理はWindows GUIのRSATで可能
- 構築や運用がOpenLDAPより簡単

Samba3と4の違い

機能	Samba 3	Samba 4
ファイルサーバ機能	Samba3.6からSMB2対応	SMB2,SMB3 (Windows8) 対応
	NASとしての実績が現時点では多い	サーバーサイドコピーなどに対応
		CTDBによるクラスター機能対応
ドメインコントローラ機能	NTドメイン互換	Active Directory (Win2008R2) 互換
	NTLMv2認証	Kerberos認証(Kerberosサーバー内蔵)
	システムポリシー	グループポリシー
	冗長化には外部のLDAPが必要	LDAPを内蔵しているためSambaのみで冗長化が可能
Windows GUIによる管理機能	Windows2000のUSRMGR Windows 7,8,10で動作しない	RSAT対応 Windows 7,8,10で動作可能
名前解決機能	NTドメイン互換なのでWINSサーバーが必要	ADドメイン互換なのでDNSによる名前解決が必要
	SambaがWINSサーバー機能を持つ	WINSサーバーは不要 SambaがDNSサーバー機能を内蔵
	DNSでSamba3 DCを見つけることはできない	DNSがないとSamba4 DCを見つけられない

参考資料：日経BP Samba 4による Windowsネットワーク 構築

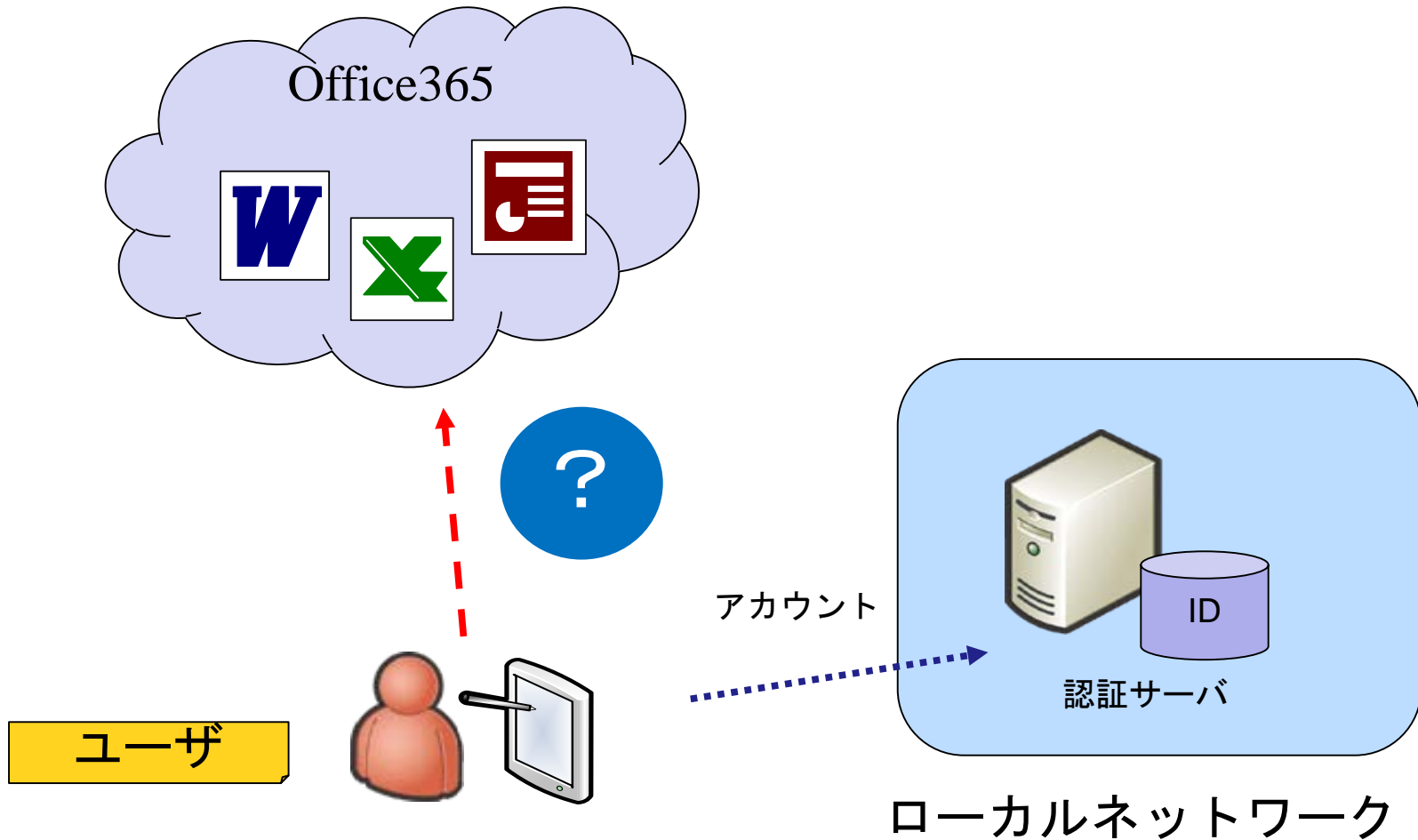
<http://itpro.nikkeibp.co.jp/article/COLUMN/20131018/511929/>



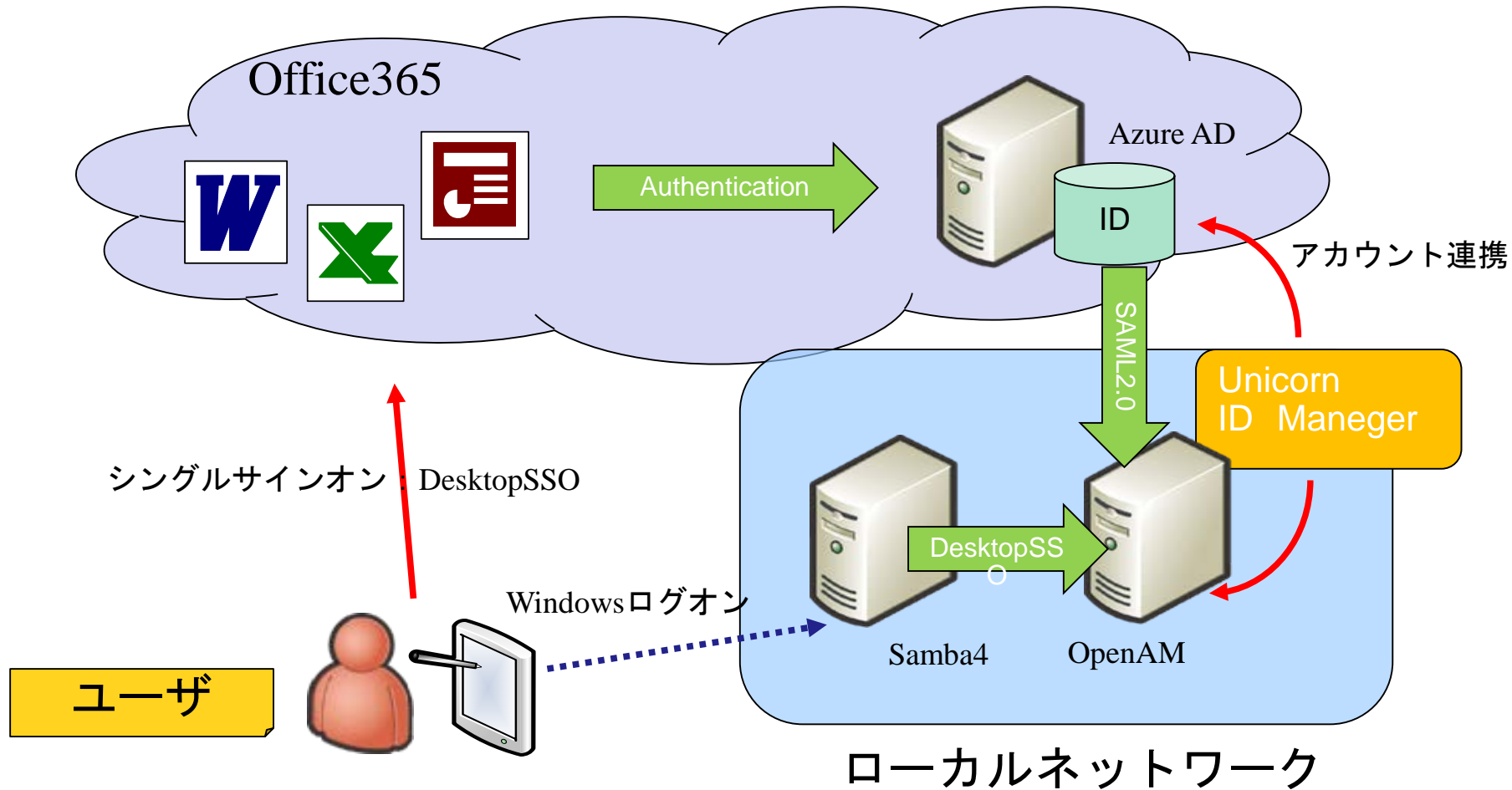
OpenAMとSamba4 OSSで実現する Office365連携

Unicorn ID Managerも Office365に対応！

Office365利用での認証連携要件

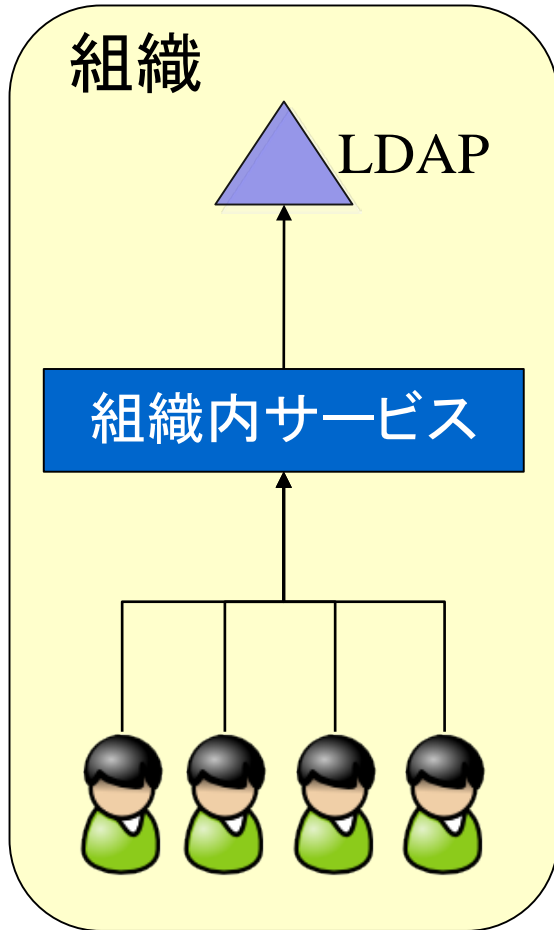


Office365利用での認証連携

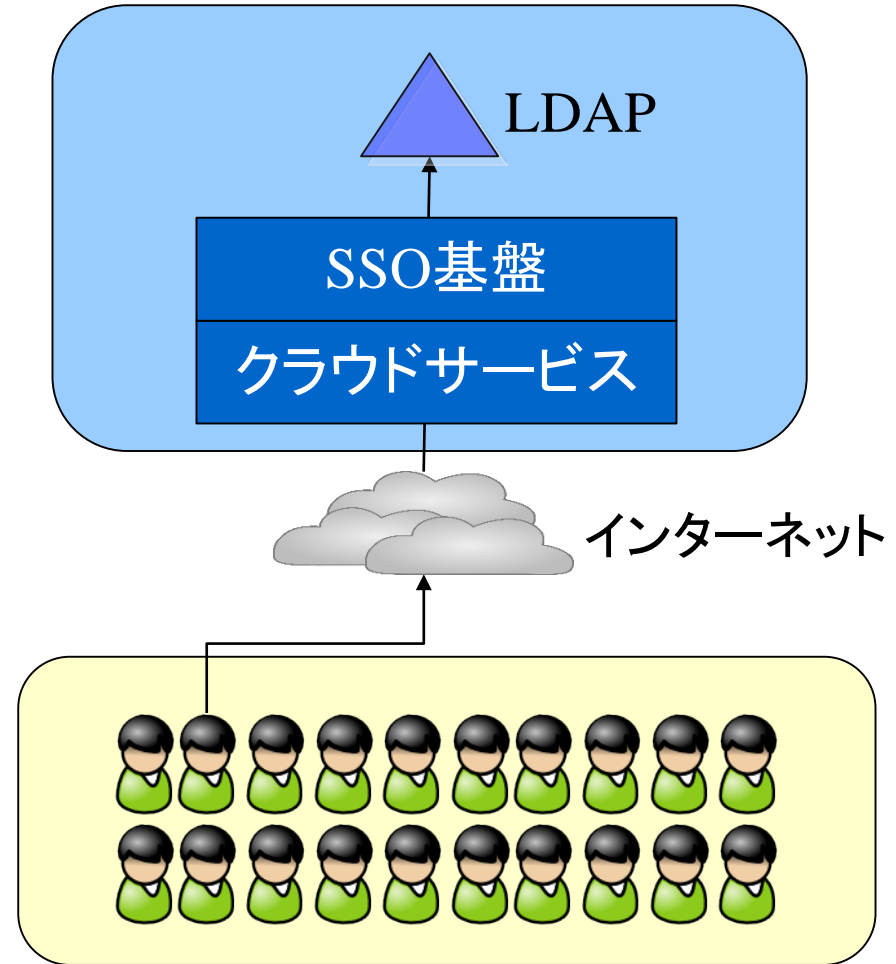
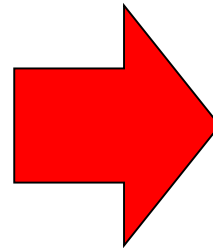


**ローカルネットワーク
オンプレミスにはWindowsサーバー不要！**

クラウドとOpenLDAPの性能向上必要性



社員等：数万人程度



利用ユーザー：数十万人～数百万人

OSSTechの取り組み

OpenLDAP の WiredTiger バックエンドの開発

... 只今、開発中

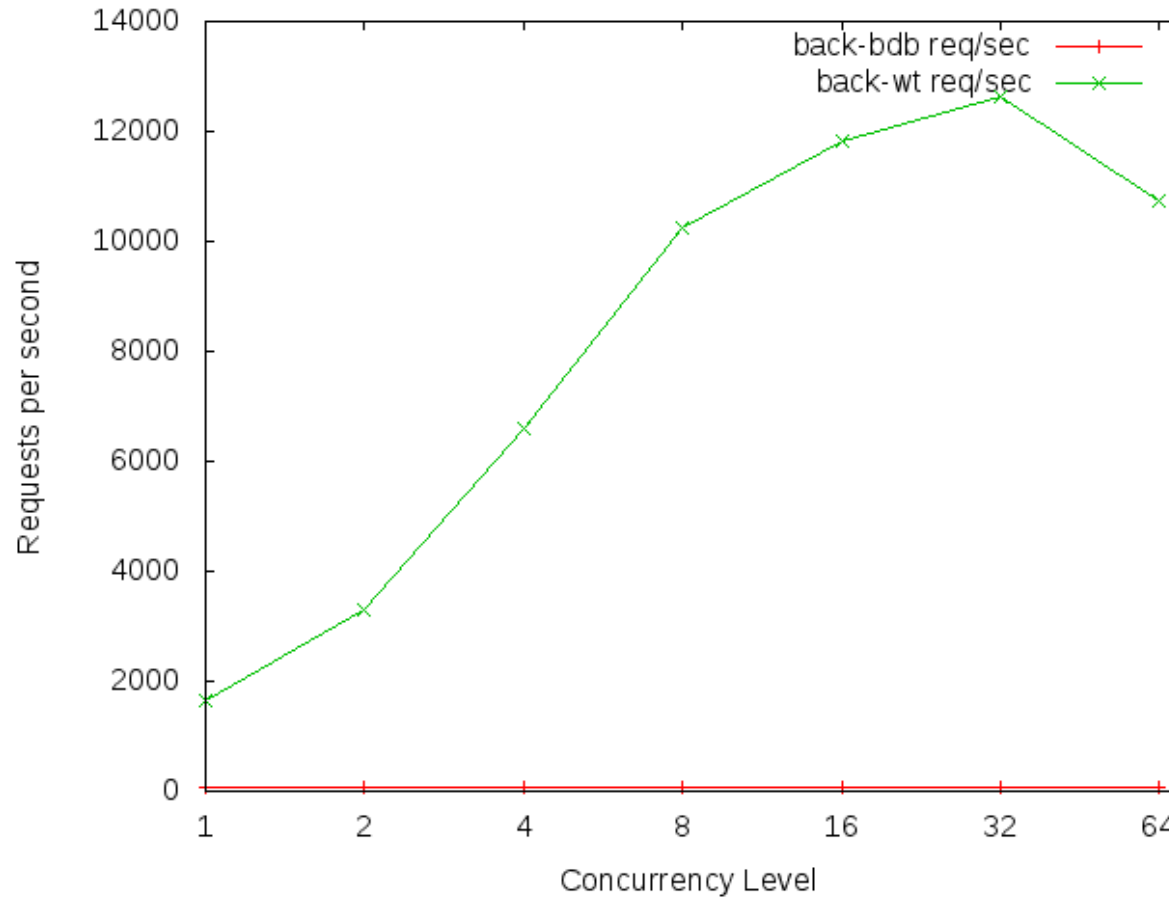
<http://github.com/osstech-jp/openldap>

WiredTigerとは...

- WiredTiger社開発の新ストレージエンジン
- 開発者
 - Michael Cahill氏、Keith Bostic氏
 - BerkleyDBの開発者 (Sleepycat, ORACLE)
- OSS:GPL v3 / v2 Dual License
- Key - Value方式のストレージエンジン
- 高い並行処理性能
 - マルチコア、大容量メモリ、ディスク環境向け
 - メモリ上のキャッシュ方式を採用
 - Multi Versioned dataによる処理の競合回避
 - ◆ トランザクション間のブロックによる処理遅延を防ぐ
- 効率的なディスク利用
- ジャーナリングによるデータ保護
 - Checkpoint / Write ahead logging

OpenLDAP Benchmark

Add性能



https://github.com/osstech-jp/openldap/wiki/back_wt-benchmark

WiredBackendによる高性能化

- ・ パッチはすでにOpenLDAPコミュニティに取り込まれた
- ・ 11月のLDAPCon2015で発表予定

LDAPCon
2015

Edinburgh 11th to 13th
November

LDAPCon 2015

Accepted Papers <

Tutorials

Poster Sessions

Venue and Travel

Prices and Booking

Sponsorship packages

Sponsors

Previous Conferences

Programme Committee

Contacts

LDAP
conference EDINBURGH
2015

LDAPCon 2015 > Accepted Papers > WiredTiger Backend for OpenLDAP – HAMANO Tsukasa

WiredTiger Backend for OpenLDAP

HAMANO Tsukasa

Open Source Solution Technology Corporation, Japan

Abstract

This paper introduces WiredTiger backend for OpenLDAP. WiredTiger is an embedded database having the characteristics of multi-core scalability and lock-free algorithms. We implemented a new OpenLDAP backend called back-wt that is using WiredTiger database and then measured the performance.

Motivation



OSSTech

「オープンソースソフトウェア」の新しい価値を創造し、高機能・高品質を追求する

統合認証

シングルサインオン

アイデンティティ管理ソリューション

OpenAMはオープンソース・ソリューション・テクノロジー株式会社の日本での登録商標です。(登録 第5398965号)



オープンソース・ソリューション・テクノロジー株式会社 Open Source Solution Technology Corporation

〒141-0031 東京都品川区西五反田1-29-1 コイズミビル 8F Tel:03-6417-0753 Fax:03-6417-0754 Mail:info@osstech.co.jp