



guide of your web

WitGuide SSO

www.witsign.com

© 2009 Witsign Ltd.

概略



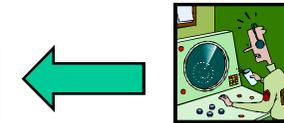
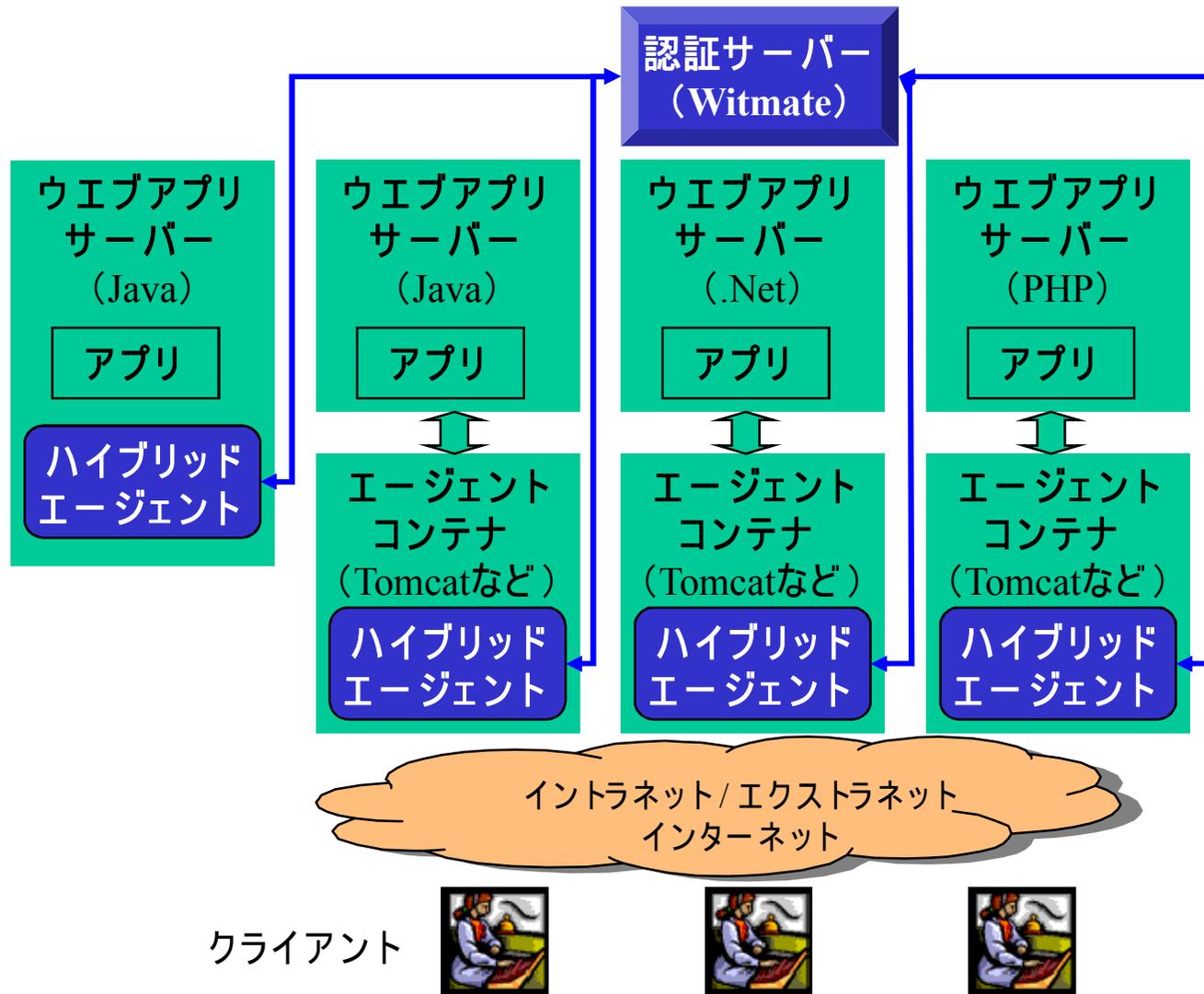
- ルールエンジンより、柔軟な複数アカウント統一管理
- 共通ログインとエラー表示のカスタマイズは可能

概略



- WitGuide.SSOは Witsign (ウィット・サイン) 社提供するSSO (Single Sign-on) 製品である
- Webコンテンツ管理製品群WitGuideの一員で、他のWitGuide製品と連動して、Webサイトコントロールシステムを即時構築は可能
- Witsign社独自のハイブリッドSSOシステム構造を持っている
 - 従来のProxy形とエージェント形構造の 利点を発展、弱点を回避
- ハイブリッド構造のメリット
 - 高性能と安全性と両立できるSSO (Single Sign-on) 製品
 - PKI (Public Key Infrastructure) +ダブル署名チェック → 高安全性
 - 分散システム構造 + 認証サーバー負担低減 → 高性能
 - アプリと簡単統合
 - アプリからWitGuideSSOのAPIなどへコールする必要はない
 - WitGuideSSOと統合するため、アプリ側の他の開発などは要らない

ハイブリッド構造



マネージメント

- ハイブリッドエージェントはパスワードが必要時だけ、認証サーバーにアクセス
- 認証サーバーとエージェントとの通信はPKI + ダブル署名チェック
- 署名した一時パスワードを利用し、パスワードなどの重要データはクライアント側に渡さない (暗号化したパスワードの渡も非安全である)
- Java、.NetとPHP以外のアプリサーバーもサポート
- マネージメントは認証サーバーとエージェントを管理

他のメリット



- Witsign社独自の高速ルールエンジン
Witmateベースの認証サーバーを利用するから：
 - 複雑の認証ルールを設定可能、変更も容易
 - RDB、LDAPなどのデータへのアクセスは簡単
- 認証キーなどの変更はマネージメントの命令ひとつで簡単出来る
 - 運用中の“何がある”時、早速に対応
 - システム設定変更は簡単

追加機能リスト



- SSOセッションをサポート
 - アプリのセッションを統一
 - 全アプリのSSOセッションを一斉終了
 - SSOセッションタイムアウト
 - 管理でリセット
- 強制／非強制SSOログインをサポート
 - 強制ログイン: 全部のアプリページをアクセス前に、SSOログインは必要。(業務システムなど)
 - 非強制ログイン: 一部のページをSSOログインしなくても、見えるし、アプリの判断より、必要時だけ、SSOログインする。(オンラインマニュアル、メールクリック・アクセスなど)
- パスワード・ルールチェック・サービスを提供

付録1：性能テスト - 環境



- WitGuide.SSOの社内性能テスト結果である
- テストホスト: WitGuide.SSOの実行環境である
 - ハード: Core Duo T2400 1.83G, 1G RAM
 - OS: Windows XP SP2
 - ソフト: Java1.5, MySQL5.0, Tomcat 5.5(PureJava)
 - WitGuide.SSO 全システムとテスト用アプリ及びアプリ用DBは全部一台のホストにインストール
- テストクライアント: テストソフト(JMeter)の実行環境である。大量のリクエストを短時間に出すため、テストクライアントは3台を使った。
 - ハード: P4 1G, 1G RAM * 3台
 - OS: Windows XP SP2
 - ソフト: Java1.5, JMeter2.2
- テストケース
 - 2400人ログイン・ログアウト同時にすること
 - 3台のテストクライアントはそれぞれ以下のJMeterスレッドグループを設定し、同時実行

A screenshot of the 'Thread Group Properties' dialog box in Apache JMeter. The dialog has a title bar 'スレッドプロパティ' and contains the following fields:

- 'スレッド数:' with a text box containing the value '8'.
- 'Ramp-Up 期間 (秒):' with a text box containing the value '1'.
- 'ループ回数:' with a radio button selected for '無限ループ' and a text box containing the value '100'.

付録1：性能テスト - 結果



- それぞれのテストクライアントの結果

- テストクライアント1

Label	# Samples	Average	Median	90% Line	Min	Max	Error %	Throughput
Show login page	800	44	30	100	0	280	0.00%	28.8/sec
login	800	109	90	220	10	531	0.00%	28.8/sec
Logout	800	74	60	140	10	490	0.00%	28.8/sec
合計	2400	76	60	160	0	531	0.00%	86.0/sec

- テストクライアント2

Label	# Samples	Average	Median	90% Line	Min	Max	Error %	Throughput
Show login page	800	58	30	101	0	1302	0.00%	28.4/sec
login	800	116	100	220	10	490	0.00%	28.4/sec
Logout	800	69	60	120	10	380	0.00%	28.4/sec
合計	2400	81	60	161	0	1302	0.00%	85.0/sec

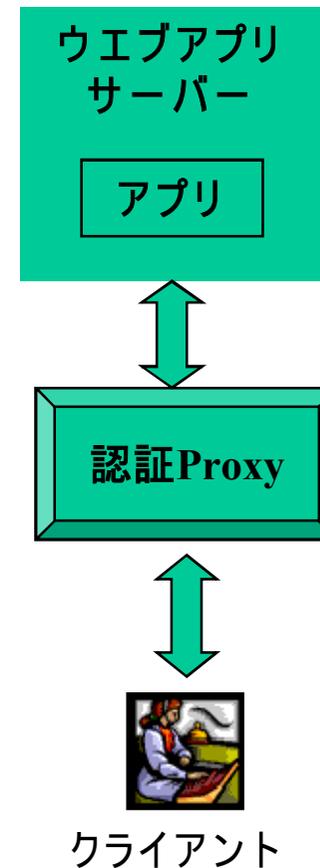
- テストクライアント3

Label	# Samples	Average	Median	90% Line	Min	Max	Error %	Throughput
Show login page	800	44	30	100	0	460	0.00%	30.9/sec
login	800	108	90	211	20	450	0.00%	30.9/sec
Logout	800	71	60	131	10	520	0.00%	30.9/sec
合計	2400	74	60	160	0	520	0.00%	92.5/sec

- 結論：平均1秒90人のログイン・ログアウトは出きった。一人の待ち時間は平均0.1秒前後、最長1.5秒以下

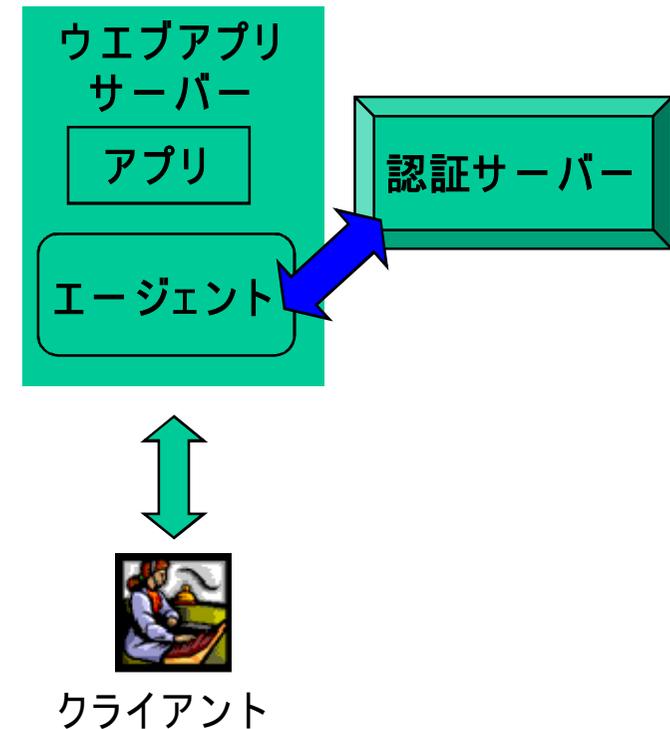
付録2: 従来形SSO - Proxy

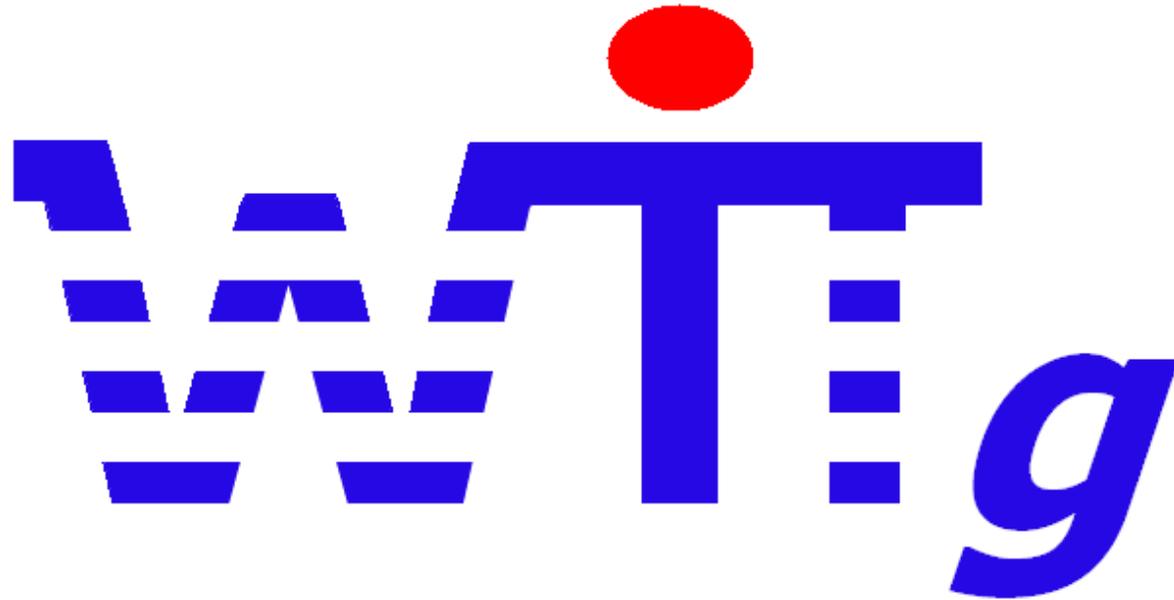
- Proxy形
- 弱点
 - 認証Proxyがアプリの前に出ますので、ファイアウォールの設定などの安全管理は難しい
 - すべての通信は認証Proxyにまとめるため、性能は低い
 - クライアントが元のアプリへのアクセスをProxyに変更する設定或いは管理は必要



付録2: 従来形SSO- Agent

- エージェント形
- 弱点
 - エージェントとアプリがひとつアプリサーバーにインストールすることは必要
 - エージェントは全部のアクセスの認証を認証サーバーに渡すので、認証サーバーの負担が大きいし、システム性能は低い
 - Java、.Netなど違うアプリサーバーに対して、各アプリサーバー用のエージェントの開発とメンテナンスが必要であるので、コストは掛かるし、リスクは増大





guide of your web

www.witsign.com