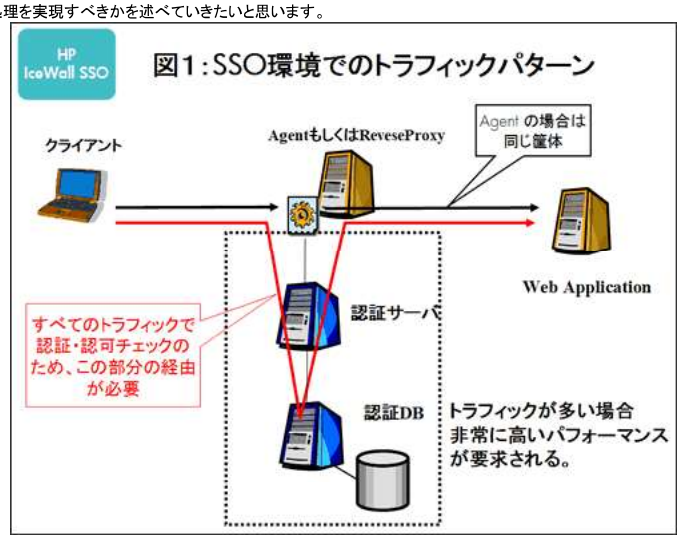
HP IceWall SSO

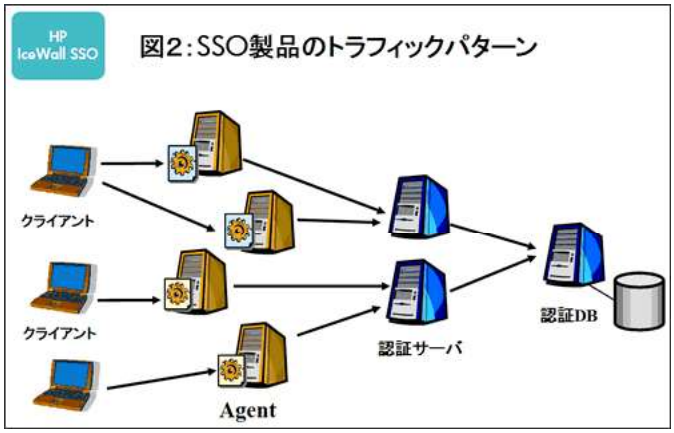
HP IceWall技術レポート：パフォーマンス特集1

SSO製品はクライアントとアプリケーションの間のすべてのトラフィックに介在し、認証やアクセス制御を行ないます（図1）。
そのトラフィック量は、大規模のシステムであれば毎秒数千件にも及びます。つまりSSO製品は、その規模のトラフィックを処理できるスケーラビリティを持つことが要求されます。ここでは、SSO製品がどのような仕組みで、その処理を実現すべきかを述べていきたいと思います。



SSO製品のトラフィックパターン

SSO製品のトラフィックは、多数のAgentもしくはReverseProxy から認証サーバー（Policyサーバー）にアクセスに行きそこでまとめられ、認証DBまで認証や認可情報を確認する流れです（図2）。



通常すべてのトラフィックで認証・認可のチェックが必要であるため、もし何も工夫せずにSSO製品を作成すると、すべてのトラフィックが毎回認証DBにアクセスすることとなります。認証DBは、データベースやLDAPが通常用いられますが、ご存知のとおり台数を増やしスケールアウトすることは容易ではありません。また処理も重くパフォーマンスも容易な向上が難しい。つまりこの部分がボトルネックとなります。
このボトルネックをいかに解消しているかが、各SSO製品のスケーラビリティに関するアーキテクチャのポイントです。
そのボトルネックの解消方法のポイントとしては、大きく以下の2点が挙げられます。

1. キャッシュを使用する
2. 認証DBとの接続の効率化

1.キャッシュを使用する

キャッシュの持ち方には、次の2つのパターンがあります。

- Agentに保持する場合
- 認証サーバーで保持する場合

Agentにキャッシュを保持した場合、ヒットすればそこで処理が完了するため、トラフィックとしては一番軽くなります。しかし、Agentのキャッシュには問題も多くあります。
ヒット率を上げるためキャッシュサイズを大きくとると、メモリ圧迫や検索によるCPU負荷が生じ、同じサーバー上のアプリケーションに影響を及ぼしてしまいます。また何十、何百ものAgentのキャッシュ間の整合性も問題です。たとえば本体でログアウトしても、Agentにキャッシュが残っている間は、アプリケーションにアクセスできてしまいます。したがってAgentのキャッシュは、そのようなことが起こらないようにアプリケーションに影響を与えず、整合性を損なわない程度に制限する必要があります。そうなるとヒット率は期待薄であり、主体は認証サーバーのキャッシュとなります。

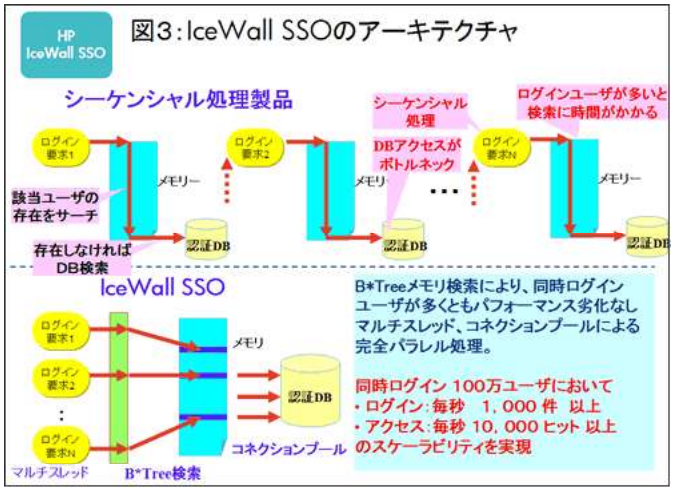
認証サーバーでのキャッシュのポイントはヒット率と検索速度です。つまり認証DBになるべく問い合わせを行かせないようにすることと、多数のAgentからの大量アクセスをどう処理するかです。ヒット率を高めるためには、認証DBに近い内容をメモリに展開することになりますが、単純に展開してしまうと、今度はキャッシュの検索に時間がかかってしまいます。たとえば、10万人分のレコードがあれば、シーケンシャルに検索した場合、毎回平均5万レコード検索しなければなりません。これを解決するためには、ツリー型など高速な検索方法が必要です。また処理効率を上げるためにマルチスレッドを採用する必要があり、当然スレッド間の排他制御も巧妙に制御する必要があります。

2.認証DBとの接続の効率化

認証サーバーと認証DBとの間がシーケンシャルな処理であれば、そこがまずボトルネックとなります。スケーラビリティを実現するためには、複数のDBアクセスを同時に実行可能とする必要があります。
一方、DBアクセスで最も重い処理は、DB接続です。従って、DB接続の負荷を軽減することがボトルネックの解消となります。DBアクセスを並列処理し、かつ、DB接続の負荷を軽減しスケーラビリティを実現するには、あらかじめ確保した複数のDB接続を各処理単位で共有して使用するコネクションプールの採用が必要となります。またコネクションプールを生かすためには、認証サーバーが並列処理、つまりここでもマルチスレッド対応していることが必須です。

HP IceWall SSO のアーキテクチャ

HP IceWall SSO はログイン時のみ認証DBにアクセスに行き、そのユーザの情報は認証サーバーにキャッシュされ、その後のアクセスは認証サーバーで終端する設計です。AgentやReverseProxy ではキャッシュを持っていないため認証サーバーにトラフィックが集中しますが、認証サーバーではB*Tree検索やコネクションプール、マルチスレッドの採用による完全並列処理を実現しており、100万人ログインしている状態で毎秒10000件の処理に耐えられる構造をもっています。シーケンシャルでの処理と比較したのが図3です。



また処理効率も非常に良くわずか1CPUで毎秒2000 件以上のアクセス処理*1を実現しています。

*1 RP2470 (HP-UX11.0i 750Mhz)での測定結果

HP IceWall SSO　最新バージョンのスケーラビリティ

HP IceWall SSO 最新バージョンの性能

集約化や企業の統合などに伴い大規模化したシステムには、以前以上の処理性能が求められます。大規模なシステムでは、毎秒1万件以上に上るトラフィックが発生するものもあります。
前述の通り、SSO製品には対象となるシステムのトラフィック量に耐えられる処理能力が必要です。HP IceWall SSOの場合、認証サーバーの処理はCPU性能に依存するため、CPUの処理能力の向上に伴い認証サーバーの処理能力も向上します。
2010年8月にリリースされた最新バージョン HP IceWall SSO 10.0を用いた実機測定では、認証サーバー1台によるシングル構成で下記の通りの結果が出ています。

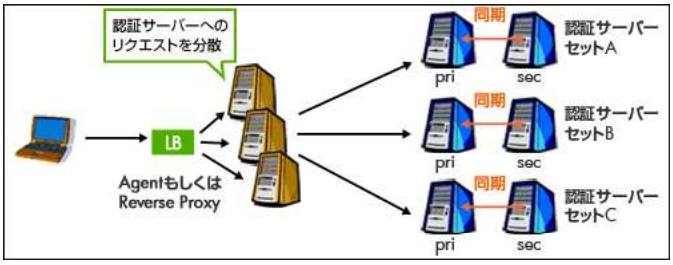
- ログイン:
  - Oracle 毎秒 3800件以上*2
  - OpenLDAP 毎秒 5000件以上*3
- アクセス:
  - 毎秒 13000ヒット以上*2

上記の結果から、HP IceWall SSO 10.0 では1CPU(4コア)で毎秒6500件以上のアクセス処理を実現が可能といえます。

*2　認証サーバーは、BL860c i2 (HP-UX 11.31 クアッドコア Intel(R) Itanium(R) Processor 9340s(1.6 GHz)×2)を使用
*3　認証サーバーは、BL460c G7 (RHEL 6.1 6コア Intel(R) Xeon(R) Processor X5670 (2.93GHz)×2)を使用

分散化によるスケーラビリティの向上

HP IceWall SSOは、リバースプロキシのみが販売開始当初よりロードバランサ配下でのスケールアウトに対応していました。
前述の通り、認証サーバーは単体でも十分に高い処理能力を持ちますが、HP IceWall SSO 10.0より新たに追加された認証サーバーの負荷分散オプション*4により、リバースプロキシからのリクエストを複数の認証サーバーセット*5へ分散させて処理できるようになりました。



分散実行する認証サーバーセットは、他の認証サーバーセットに依存せず、それぞれ並行して処理が可能です。そのため、認証サーバーセット数がn倍になると、それに比例して全体で処理可能なログイン・アクセス件数もn倍になります。
認証サーバーは単体でも100万人ログインしている状態で毎秒数万件のアクセス処理に耐えられる構造を持っています。さらに、負荷分散オプションによる複数認証サーバーセットよる分散処理で、毎秒100,000件の処理に耐える構成をとることが可能です。

本オプションにより、リーバスプロキシのみでなくSSOシステム全体でスケールアウトが可能となり、スケーラビリティの向上が実現されました。

*4　有償オプション(リバースプロキシ-認証サーバー間のロードバランサは不要)
*5　認証サーバーセットは、1台もしくはレプリケーション機能により同期された2台の認証サーバーからなる

2004.5.12 日本ヒューレット・パッカード コンサルティング・インテグレーション統括本部 IceWallソリューション部部長 小早川 直樹
2012.4.18「HP IceWall SSO 最新バージョンのスケーラビリティ」の項を加筆
日本ヒューレット・パッカード テクノロジーサービス統括本部 テクニカルコンサルタント 土居 恭子

●関連技術レポート
≫ パフォーマンス特集（1） SSO製品のスケーラビリティの考え方とHP IceWall SSOのアーキテクチャ（本トピックス）
≫ パフォーマンス特集（2） IceWall＋ロードバランサが実現するパフォーマンス
≫ パフォーマンス特集（3） HP IceWall SSOのパフォーマンス調査方法
≫ パフォーマンス特集（4） 新しいパフォーマンスモニタリングツール（iwpm）のご紹介
≫ パフォーマンス特集（5） HP-UX 11i v3におけるHP IceWall SSOのパフォーマンス