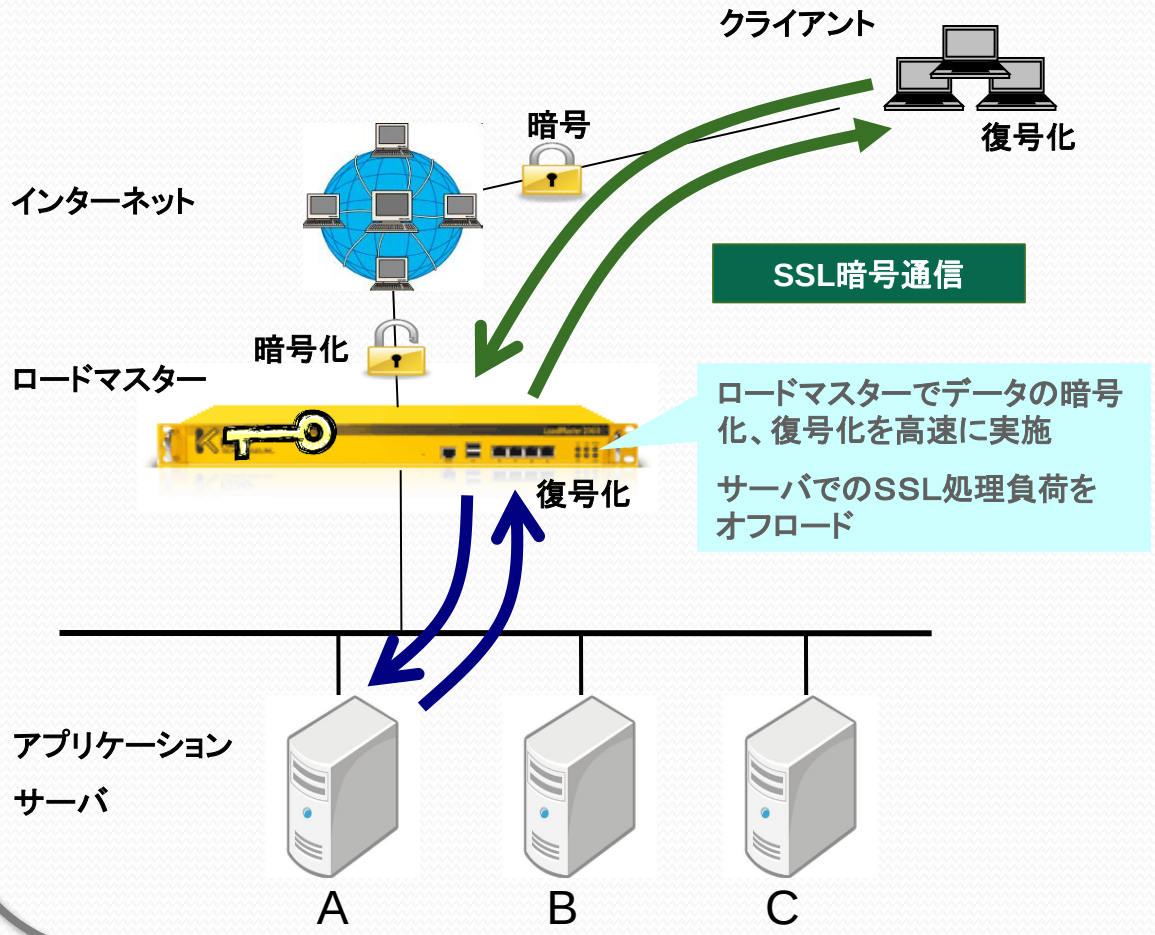
第27回スクエアfreeセミナー

SSLアクセラレータとしてのLoadMaster活用

株式会社OPENスクエア　http://www.opensquare.co.jp
東京都千代田区神田紺屋町17番　SIA神田スクエア2F
お問合せ先：　info_os@opensquare.co.jp

SSLアクセラレータとは？

SSLによる暗号通信で送受信されるデータの暗号化・復号を高速に行う専用ハードウェア。
ネットワーク上に設置するタイプのSSLアクセラレータには、負荷分散機能など、クライアントからの要求により効率的に応答できるようサポートする機能を備えているものが増えています。



SSLアクセラレーション

SSLによるデータの暗号化・復号には膨大な処理が必要なため、サーバで処理を行うと多くのサーバリソースを暗号化・復号に費やしてしまい、暗号化しない場合に比べ著しくパフォーマンスが低下します。このため、暗号処理のみを行うハードウェアを用意することによって、サーバの負荷を軽減します。

SSL通信の利用

- HTTPS
- POP3S
- IMAPS
- SMTPS　などなど色々、、、

また、WAF/IDS/IPSでも複合する必要があります。

暗号化アルゴリズムに関する2010年問題

今や一般的に使われている電子認証や署名の暗号技術は、コンピュータの性能や解読技術の向上により、暗号技術の安全性が徐々に低下していきます。
暗号の安全性だけを考えると、より安全な暗号技術への移行が望ましいと考えられます。

【米国国立標準技術研究所(NIST)の見解】
現在利用されている米国政府使用の暗号技術を、2010年末までにより安全なアルゴリズムへ移行させる方針を打ち出しています。

【日本の内閣官房情報セキュリティセンター(NISC)や総務省の見解】
電子署名法関係における対応として、より安全性の高い暗号化技術を採用し、「2014年度早期までにより安全性の高い暗号技術による電子署名に係る特定認証業務を開始する」との対応を予定しています。

※安全性の低下が懸念されている具体的な暗号技術
　〇公開鍵：1,024bit
　〇ハッシュアルゴリズム：SHA-1

認証局は2048ビット証明書のみ発行に移行

公開鍵の2048ビットキーのパフォーマンスは？

SSL証明書の公開鍵が1024から2048ビットキーへ移行すると、
SSL TPSのパフォーマンスが平均1／5に！！

一般的なパフォーマンス指針

キーサイズ（ビット）	32ビット商用ハードウェア	パフォーマンス劣化	64ビット商用ハードウェア	パフォーマンス劣化
512	2、357 TPS	―	8、008 TPS	―
1024	525 TPS	1／4．5	1、570 TPS	1／5．1
2048	96 TPS	1／5．5	273 TPS	1／5．8
4096	15 TPS	1／6．4	38 TPS	1／7．2

SSL証明書の公開鍵を1024から2048ビットキーへ移行すると、
単純に試算して、サーバを1台から5台に増やす必要があります。

LoadMaster（SSLアクセラレータ）の優位点

当然ながらLoadMasterも同じです、、、

モデル	1024ビットキー	2048ビットキー	パフォーマンス劣化
LM-2200	200 TPS	50 TPS	1／4
LM-2600	2，000 TPS	2，000 TPS	1／1
LM-3600	5，000 TPS	2，722 TPS	2．16／4
LM-5300	9，300 TPS	5，022 TPS	2．08／4

でも、LoadMasterを導入すると

1．**サーバのパフォーマンス向上**
　サーバの増設が不要になり、且つ、サーバからSSL処理の負荷が無くなりますので、従来よりサーバで処理能力が向上します。
2．**SSL通信の集中管理**
　各サーバでSSL通信の設定が不要ですので、サーバの設定や管理が容易になります。
3．**証明書の一元管理**
　全ての証明書はLoadMasterに設定するだけですので、SSL証明書の更新処理などの工数が削減できます。
4．**コストの削減**
　サーバ台数分の証明書が不要になります。（SSL証明書のライセンスポリシーにより異なる場合があります。）

当然ですが、負荷分散装置としても使えます。

ご清聴ありがとうございました

当社では、SSL証明書（セコムパスポート）も取扱ております。
SSLアクセラレータ、負荷分散装置のご相談はOPENスクエアまでお問合わせ下さい。

お問合わせ先：
株式会社OPENスクエア
Eメール ： salese_os@opensquare.co.jp
電話 ： 03－6413－1840
担当 ： 田中昭造