



FAQ:2048ビットSSLキー

F5はどのようにSSLをサポートしますか？

F5には、SSLの負荷を軽減する機能があります。つまり、通常はサーバごとに行うSSL認証を、BIG-IP LTMに集中的管理して、必要な認証にかかるコストだけでなく、サーバのソフトウェア/ハードウェアの追加が必要になった場合のコストも削減します。BIG-IP LTMには、エンドツーエンドの暗号化が必要だけれどもアプリケーションの変更は望ましくないかまたは変更できない場合に、さまざまな鍵長を使用してバックエンドサーバへの再暗号化を行う機能もあります。

今、鍵長が重要なのはなぜでしょうか？

- National Institute of Science and Technology – セキュリティおよび暗号化に関連する項目のガイダンスを提供し、脆弱性に関する権威とみなされています。NIST¹および学術的、公的な他のセキュリティ機関によれば、1024ビットキーはすでに十分なセキュリティを提供していないと広く認められています。しかし、1024ビットから2048ビットへ移行すれば、ビットの長さは2倍になるだけですが、安全性は 2^{32} 増加します(43億倍)。²
- NISTは世界的な組織ではありませんが、多くの科学機関や教育機関と同じように世界的に通用するガイダンスを提供しており、Common Criteria for Information Technology Security Evaluation(セキュリティ評価のための評価基準、略称Common Criteria:CC)の一部を構成しています。CCは、コンピュータ・セキュリティ認証のための国際標準(ISO/IEC 15408)です。評価基準は、ITSEC、CTCPEC、およびTCSECの3つの基準から始まり、これらがNBSに組み込まれて、最終的にNISTになりました。CCは、カナダ、フランス、ドイツ、オランダ、英国、および米国により開発されました。

商用認証局(CA)はどのように変化していますか？

商用認証局(CA)は、Webブラウザで信頼される、SSLおよびTLS証明書を発行します。発行された証明書は、chain of trust(信用の連鎖)を通じて認証されます。多くの証明書が通常、この信用の連鎖を通じてDNSルートゾーンまでたどることができます。もっともよく目にするCAベンダは、VeriSign、Entrust、Comodo、GoDaddy、Thawte、およびGeoTrustなどです。これらのCA証明は、NISTなどのセキュリティ協議会が提供するガイダンスに従って、1024ビットキーの発行から2048ビットキーのみの提供へと移行しています。たとえば、VeriSignは2010年10月をもって1024ビットキーの認証をとりやめ、GeoTrustは2010年6月に中止しました。

VeriSignのWebサイトでは128ビットと256ビット暗号化の利点に言及していますが、2048ビットキー長でないのはなぜですか？

SSLはまず、1024ビットまたは最近では2048ビット証明書を交換しているクライアントとサーバの間の会話することによって動作し、クライアントとサーバのこの「ハンドシェイク」の後で、128ビットまたは256ビットの一時的な共有プライベートキーで暗号化されたデータを交換します。このキーはハンドシェイクとは別の物です。VeriSignが言及しているのは、ハンドシェイク後の暗号化に使用されるこの128ビットまたは256ビットの一時キーのことで、

¹ http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf 表 4

² http://www.javamex.com/tutorials/cryptography/rsa_key_length.shtml
http://www.rsa.com/rsalabs/faq/files/rsalabs_faq41.pdf

鍵長はどのようにパフォーマンスに影響しますか？

鍵長が長いほど、キーを破ろうとする試みに対する防御は強力になります。ただし、1024ビットから2048ビットへの移行により、計算処理が一桁増加します。そしてこの計算処理は、パフォーマンスに影響します。2048ビット証明書の処理は、1024ビットの処理に比較してSSLトランザクションが5～6分の1に減少し、そのため2048ビットでは1024ビットに比べてSSL TPSの数値は、20%になります。

SSL TPSが影響するのは、初期ハンドシェイク、再ネゴシエーション、およびSSL再開のみです。これらが発生するのは、新しいTCP接続ごとのみです。一度このハンドシェイクが実行されれば、すべてのトラフィックは128ビットまたは256ビットの暗号(SHAまたはMD5など)により暗号化され、SSL TPSではなくバルク暗号化スループットとして測定されます。このバルク転送のファイルサイズが小さいと、実際の「バルク」がごく小さいため、SSL処理の負荷の中でハンドシェイクが大きな割合を占める場合があります。しかし、ファイルサイズが大きくなれば、暗号化スループットに対するハンドシェイクの影響は減少します。SSL TPSのバルク暗号化スループットへの影響は、ファイルが非常に大きい場合はほとんどゼロになります。

SSLパフォーマンスについて、ソフトウェアとハードウェアではどのような違いがありますか？

ソフトウェアSSL暗号化および復号化は1024ビットキーより大きいと、システムリソースの大部分を消費して、許容範囲を超過します。2048ビット以上の場合、特別なハードウェアソリューションの一部として特殊なSSLチップの使用をお勧めします。

F5のハードウェアはどのようにSSLをサポートしますか？

F5 BIG-IP LTMには、SSL暗号化および復号化専用で、そのために最適化された特殊なSSLチップがあります。これらのチップは、鍵長が長くなり、商用ハードウェアでは暗号化/復号化の数学的負荷によりシステム全体のパフォーマンスが低下して、ユーザの操作性やその他のサーバタスクに影響するような場合でも、SSLレベルでは優れたパフォーマンスを提供します。

F5 BIG-IP LTMは、SSLを暗号化/復号化する場合に必ずハードウェアを使用しますか？

サポートされている暗号を使用している場合は、必ずハードウェアを使用します。

ソフトウェアで実行されるSSL TPSオプションはありますか？

ありません。ライセンスされたTPSには関わりなく、F5ではサポートされている暗号を使用する場合は必ずハードウェアを使用します。

2048ビットキーが優れているなら、なぜ4096ビットキーが推奨されないのですか？

NISTによれば、2048ビットキーによって今後20年脆弱性を防ぐ十分な複雑さが提供できるはずですが、またこのキーは処理能力を4～5倍消費します。BIG-IPでは4096ビットキーをサポートしますが、強力な業務上のニーズがない限り、最適なパフォーマンスと保護を提供するため2048ビットキーをお勧めします。

今後2048ビットキーを管理できるように、高速のCavium Nitrox SSLチップにより下位機種に搭載される予定はありますか？

下位機種については、新しいチップで更新することを検討していますが、近い将来の予定はありません。上位機種(BIG-IP 11000シリーズおよびVIPRION)の機能は、ロードマップに従って強化されています。

この鍵長の変更は、FIPS準拠のBIG-IP LTMにはどのように影響しますか？

FIPS要件は通常、セキュリティポリシーによって実施され、組織内に専用のセキュリティ機能を提供する特殊なデバイスとみなされます。FIPS TPSは、標準SSL TPSと同じで、1024ビットから2048ビットキーへの移行によりパフォーマンスが5分の1に低減します。

ハードウェアをアップグレードすべきか追加すべきか、顧客はどのようにして評価できますか？

まず、現在のSSLトラフィックのレベルのベースラインを定めることをお勧めします。SSL TPS要件が何であるか、あるいはその限界レベルがどこにあるかについて詳細な情報を持ち合わせていない事が多くあります。Enterprise Managerは、この数字を決定するのに役立ちます。ベースラインの評価は既存の1024ビット長のTPS処理数の精査を行います。この数値をBIG-IPプラットフォームにおける2048ビット鍵長処理時のSSL TPSと比較します。この比較により、現行のSSLトラフィックを2048ビットキーで処理するためにハードウェアを追加する必要があるかどうかわかります。

他のADCベンダはSSLサポートに対してどのように対応していますか？

他の全てのADCベンダも同様に、鍵長が1024ビットから2048ビットへ移行するに伴い、SSL TPSのパフォーマンスは1/5になります。これは数学的に処理が増大する為に必ず発生します。

BIG-IP LTMが提供する、サーバのSSL処理に対する差別化は何ですか？

BIG-IP LTMは、サーバ側SSL処理に対していくつかの明らかなメリットがあります。

- 特殊なSSLチップによってパフォーマンスが達成され、サーバベースのSSL処理に比べてパフォーマンスのメリットがあります。
- キーをBIG-IP上で使用し、複数のバックエンドサーバで共有できるため、SSL処理に伴う負荷が削減されます。
- キーの集中レポジトリ、およびBIG-IP LTMデバイスまたはEnterprise Managerでのキー管理により、管理の改善が実現しています。Enterprise Managerはメトリクスと履歴も提供するため、パフォーマンスに応じたサイズ設定や計画が可能になり、使用している他のBIG-IPについて証明書ライフサイクルの管理が容易になります。
- また、他のBIG-IPが使用されている場合もメリットがあります(地理的な負荷分散を実現するBIG-IP GTM、インテリジェントなルーティングを可能にする地理的情報、およびセキュリティに貢献するDNSサービス)。
- また、BIG-IPの柔軟性により、2048ビットキーが使用できるとともに、アプリケーションまたはサーバを修正せずにエンドツーエンドの暗号化を行うため、バックエンドサーバには1024ビットキーも保持できます。

BIG-IP LTMが提供する、他のベンダに対するSSL負荷軽減についての差別化は何ですか？

- F5は、高度なアベイラビリティと冗長電力を備え、エラーが起きてもVIPRIONのブレード間で処理を共有できるため、業界トップのSSLスループットを実現しています。
- F5のBIG-IPは、SSL処理および負荷分散の他にも複数の用途に利用できます(地理的負荷分散を実現するBIG-IP GTM、インテリジェントなルーティングを可能にする地理的情報、セキュリティに貢献するDNSサービス)。
- 差別化要因の1つは、BIG-IPの柔軟性です。これにより2048ビットキーが使用できるとともに、アプリケーションまたはサーバを修正せずにエンドツーエンドの暗号化を行うため、バックエンドサーバには1024ビットキーも保持できます。