

best practices | blog | browser
code | content | cookie | persis
data center | decryption | denial
dynamic infrastructure
bal | green IT | hardware | HT
detection | IPsec | IPv6 | rules
open source | optimization

SSL公開鍵長の2048ビット移行と BIG-IPによるSSLオフロードの価値について



IT agility. Your way.

best practices blog browser
code content cookie persis
data center decryption denial
dynamic infrastructure
bal green IT hardware HTT
n detection IPsec IPv6 iRules
open source optimization



セキュリティガイダンス、およびその影響



IT agility. Your way.

暗号アルゴリズムにおける2010年問題

■ 2010年問題

現在使われている暗号アルゴリズムが将来的に使用できなくなることに伴って発生する諸問題のこと

■ 暗号アルゴリズムの安全性は低下していき、寿命を迎える

(理由)暗号アルゴリズムの強度は「計算量」に依存するが、コンピュータの性能向上によって単位時間当たりの計算量は増加し、暗号解読技術の進展によって解読に必要な計算量が低下するため

■ 暗号アルゴリズムに関する最近のインシデント

1. 「一般的なRSA暗号は近い将来破られる」

—768ビット素因数分解に成功

NTTなどが世界記録を更新、「より強度が高い暗号を利用する必要あり」

<http://www.ntt.co.jp/news2010/1001/100108a.html>

2. 「SHA-1の安全性は低下」

<http://www.h-online.com/security/news/item/Attacks-on-SHA-1-made-even-easier-741997.html>



SECURITY The IT open source security In association
Last 7 days News Archive Features Forums Newsletter RSS

11 June 2009, 14:20

« previous | next »

Attacks on SHA-1 made even easier

Australian researchers have described a new and faster way of provoking collisions of the SHA-1 hash algorithm. With their method, a collision can be found using only 2^{22} attempts. This makes practical attacks feasible and could have an impact on the medium-term use of the algorithm in digital signatures.



公開鍵長のガイダンス、ベストプラクティス

- 2011年1月1日までに2048ビットキー長への移行を推奨
Special Publication 800-57 Part 1 Table 4



- マイクロソフトは、2048ビットキーを使用および推奨
NISTのガイドラインに基づき、すべてのサーバおよびその他の製品が対象
- Red HatはRSAを使用するキーに対して 2048ビット以上の長さを推奨



NOTE

Longer RSA keys are required to provide security as computing capabilities increase. The recommended RSA key-length is 2048 bits. Though many web servers continue to use 1024-bit keys, web servers should migrate to at least 2048 bits. For 64-bit machines, consider using stronger keys. All CAs should use at least 2048-bit keys, and stronger keys (such as 3072 or 4096 bits) if possible.

- SSLの脆弱性に関する注目記事
「Researcher Dan Kaminsky illuminates flaws in X.509 authentication」



認証局は2048ビット証明書のみを発行

- VeriSign
2006年から2048ビットキーに注目、2010年10月までに移行を完了
移行はNIST推奨のベストプラクティスに基づくことを表明
- GeoTrust
2048ビットキーのみに移行する理由を明確に表明(2010年6月)
- Entrust – 同様に、移行を表明
- GoDaddy
「新しく発行および更新される証明書すべてを2048ビットとする新しいポリシーを施行しました」
- Extended Validation (EV) 2048ビットキーを2009年1月1日から要件化



best practices blog browser
code content cookie persis
data center decryption denial
dynamic infrastructure
bal green IT hardware HTT
n detection IPsec IPv6 iRules
open source optimization



パフォーマンスへのインパクト



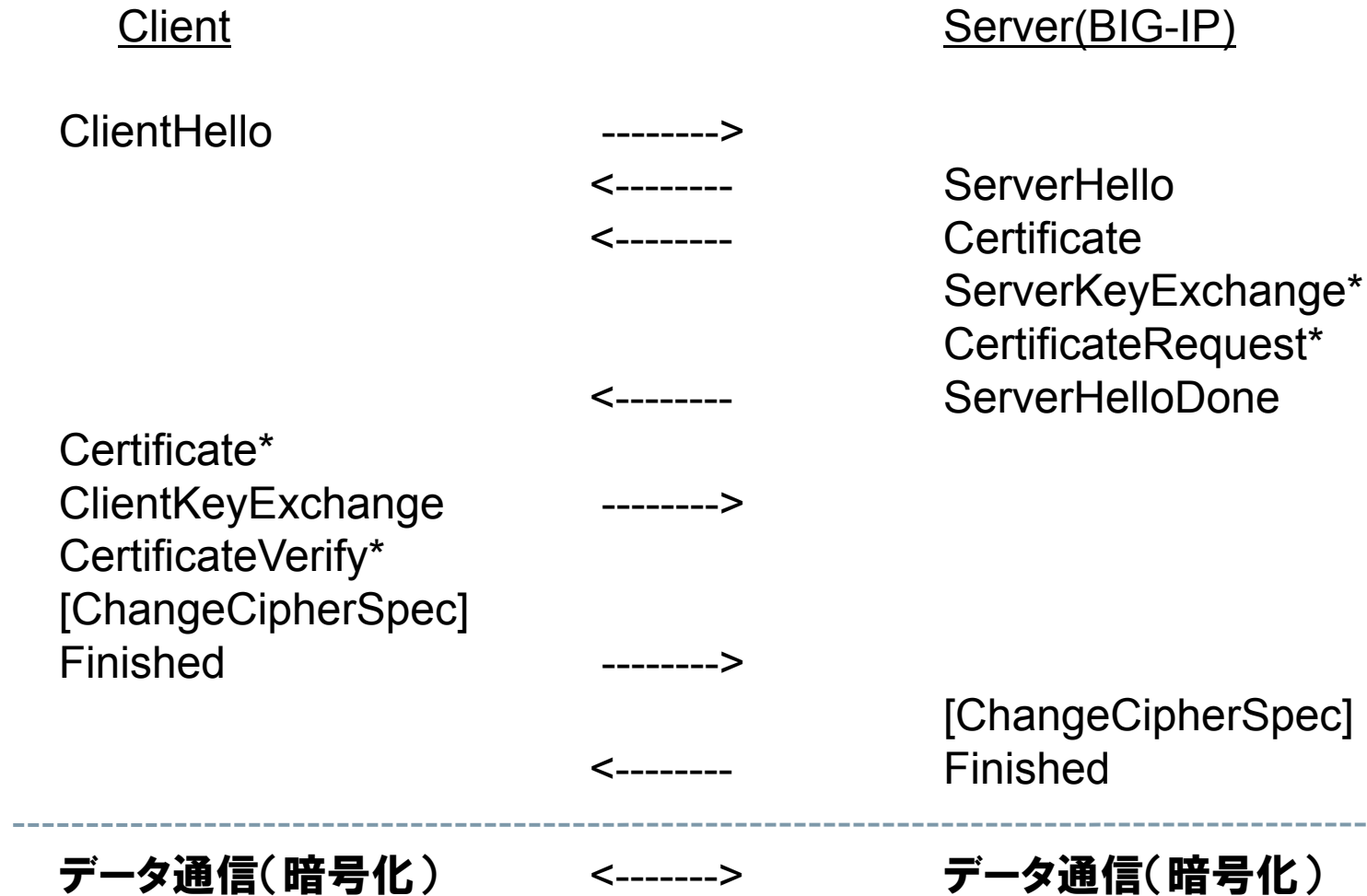
IT agility. Your way.

公開鍵の長大化によるパフォーマンスへの影響

- 1024から2048ビットキーへの移行により、SSL TPSパフォーマンスが平均1/5のパフォーマンスとなる
- 2048ビットキーは、ソフトウェア処理のみ、または仮想化環境には適さない
- TPSパフォーマンスは、トラフィックタイプ(SSLセッション再利用)にも影響を受ける



<参考>SSLハンドシェイクプロセス



* Optionとして必要な際、利用される。



<参考>SSL ハンドシェイクプロセス概要解説

サーバ認証時のSSLハンドシェイク

- Client Hello :
クライアントは、サーバに接続のリクエストを送る。
Cipher suite リストを送信する
- Server Hello :
サーバは、Cipher suiteリストからアルゴリズムを選択し
Client Helloに対して返信する。
- Server Certificate :
選択された鍵交換アルゴリズムにより、暗号化されたCAの署名済み証明書と公開鍵をクライアントに送信する。
- Client Key Exchange :
クライアントは受け取った証明書と公開鍵を復号化し、証明書が信頼するCAから発行されたものかどうかを調査。
その後、正常な証明書として確認できれば、サーバからの公開鍵によりpre_master secret を作成し、サーバへ送信する。
- Finished :
Finishメッセージを双方で送信するし、ハンドシェイクの内容をハッシュしたMACを送信し、ネゴシエーションの正常性をチェックする。
- その後、データ通信前にCipher suiteリストから選択した暗号化方式により作成された鍵によりデータを暗号化し、以降の暗号化通信を実施する。



BIG-IPによるSSLオフロードの価値

- **セキュリティ、パフォーマンス**
 - 完全なSSL通信の統合によるセキュリティ強化
 - SSLアクセラレーションにより、セキュリティに必要な処理のボトルネックを解消
- **証明書の一元管理**
 - SSL証明書を1つのBIG-IP製品で管理し、管理業務を大幅に簡素化
- **コストの削減**
 - サーバごとにSSL対応のサーバソフトウェアを使用する必要がなくなる
- **暗号化されたトラフィックの検査と変更**
 - パケットの復号化に対して業界で最もきめ細かな制御を提供し、再暗号化や配信前の処理を可能にする



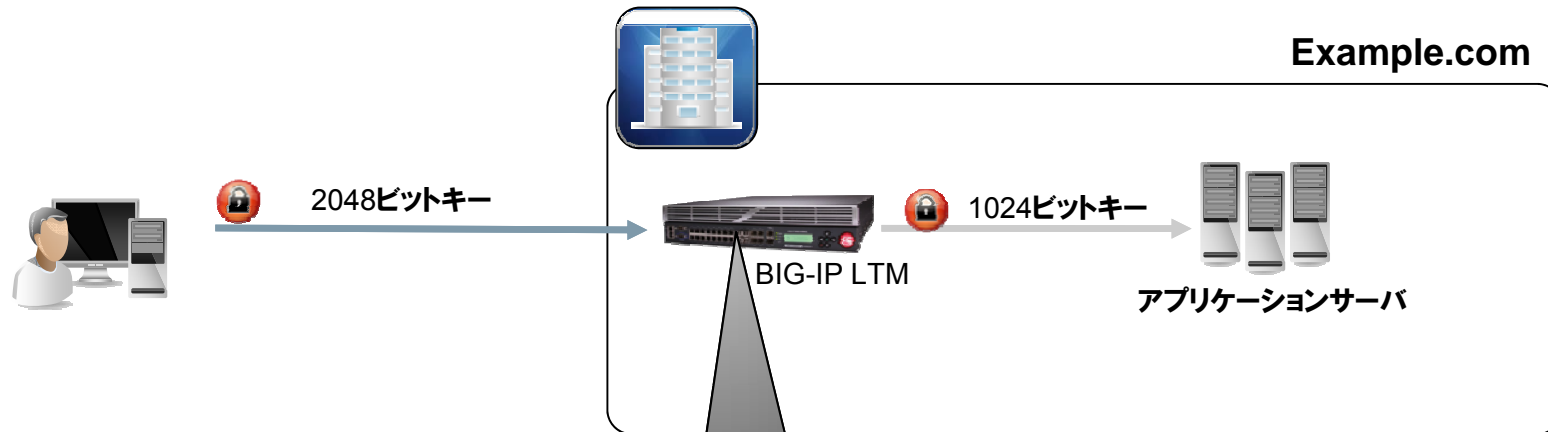
F5は2048ビット鍵長でのSSLオフロードで優位

- BIG-IPはSSL処理専用ハードウェアを搭載
 - 新しいプラットフォーム(8900、11050、VIPRION)へのアップグレードにより、最高レベルのパフォーマンスを維持
- Enterprise Managerは証明書管理を合理化
 - ステータスの表示とキーの有効期限管理
 - サイジングにおけるTPS履歴および使用状況の収集
- BIG-IPによる柔軟なSSL処理
 - 2048ビットキーを使用しつつ、バックエンドサーバに1024ビットキーを保持
 - エンド・ツー・エンドの暗号化が必要な場合、長大なキーをBIG-IPで保持して、1024キーをサーバで保持
- DNSSEC
 - DNSSECを使用したドメイン名検証によるセキュリティ強化
- IIS証明書のインポート
 - IIS証明書を簡単な手順でBIG-IPに直接インポート



再暗号化への柔軟な対応

柔軟性の高い方法でエンドツーエンドの暗号化要件に準拠



2KキーをBIG-IP
で復号化して、
サーバ用に1K
キーで再暗号化

ソリューション

エンド・ツー・エンドの暗号化の拡張

- 2Kキーをサポートしないレガシー・アプリケーション用に、2KキーをBIG-IP LTM上で保持して、1Kキーをバックエンドサーバで使用するという柔軟性を提供

Enterprise Managerは証明書管理を合理化

証明書の有効期限の表示、および長時間のTPSデータの収集

The screenshot shows the F5 Enterprise Manager interface. The top navigation bar includes 'Main', 'Help', and 'About'. The main content area is titled 'Enterprise Management >> Certificates : Traffic Certificates'. Below this, there are tabs for 'Traffic Certificates', 'System Certificates', 'Options', and 'Export'. A 'Filter' input field is present above the table. The table lists various certificates with their respective details.

Status	Name	Device	Common Name	Organization	Expiration
🟢	Cauthorn-Encrypt-Test	Audrey2.f5.com	cauthlab.localhost.net	bar	Sun Jun 24 18:44:38 PDT 2018
🟡	Global_Sign_Partners_CA	Audrey2.f5.com	GlobalSign Partners CA	GlobalSign nv-sa	Wed Jan 28 04:00:00 PST 2009
🟢	Nico	viper.f5net.com	test.f5.com	F5 Networks	Fri Oct 1 06:02:17 PDT 2010
🟢	Nico_cert	viper.f5net.com	test.f5.com	F5 Networks	Fri Oct 1 06:02:17 PDT 2010
🟡	affiliates.dotv	Audrey2.f5.com	affiliates.dotv.com	PPM Technology Group, Inc	Tue Dec 18 17:50:17 PST 2007
🟢	affiliates.streamray	Audrey2.f5.com	affiliates.streamray.com	Streamray Inc	Sat Dec 11 15:59:59 PST 2010
🟢	billing.bondage.com	Audrey2.f5.com	billing.bondage.com	Friend Finder Network	Fri Oct 15 16:59:59 PDT 2010
🟡	cauthorn-ca-cert	Audrey2.f5.com	Matt Cauthorn	F5	Thu Nov 20 11:54:29 PST 2008
🟢	default	em.f5lab.com	localhost.localdomain	MyCompany	Sat Jul 4 08:16:21 PDT 2020
🟢	default	liver.f5net.com	localhost.localdomain	MyCompany	Mon Mar 16 11:22:06 PDT 2020

Page 1 of 3



IIS証明書を簡単な手順でBIG-IPに直接インポート

IIS証明書のインポート

Hostname: BIGIP1.f5net.com Date: Aug 2, 2010 User: admin
IP Address: 172.27.11.210 Time: 10:22 AM (PDT) Role: Administrator

Unit: Active

Main Help About

Local Traffic >> SSL Certificates >> Import SSL Certificates and Keys

Overview
Access statistics, performance graphs, and links to helpful tools.

Templates and Wizards
Create common application traffic and system configurations.

Local Traffic

- Network Map
- Virtual Servers >
- Profiles >
- iRules >
- Pools >
- Nodes >
- Monitors (+)
- Traffic Class (+)
- SNATs >
- SSL Certificates (+) >

SSL Certificate/Key Source

Import Type: Select...
Cancel

- Select...
- Key
- Certificate
- PKCS 12 (IIS)
- Archive



F5が公表しているTPS数値と2048ビットへの移行の注意

- **現在のSSL TPSに関するパフォーマンスデータ**
RSA 1024ビット - RC4 - MD5
- **2048ビットに移行する際には、**
SSL TPSパフォーマンス要件に注意



パフォーマンス指標(一般的な商用ハードウェア)

キーのサイズ (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	—	8008 TPS	—
1024	525 TPS	1 / 4.5	1570 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

注：パフォーマンス結果の予測値です。



TPSパフォーマンス指標 (F5 BIG-IPシリーズ)

- BIG-IPのSSLキーサポート

1024ビットは公表値どおり、2048ビットで1/5、4096ビットで1/17

キーのサイズ (ビット)	6900シリーズ	8900シリーズ	11050シリーズ	VIPRION (PBx4 100)
1024	25,000 TPS	58,000 TPS	100,000 TPS	200,000 TPS
2048	5,000 TPS	11,600 TPS	20,000 TPS	40,000 TPS
4096	1471 TPS	3412 TPS	5882 TPS	11,765 TPS

注: 数値は予測値



BIG-IPハードウェアのラインナップ

ビジネス価値の高い優れたパフォーマンス

BIG-IP 1600



デュアルコアCPU
4 10/100/1000 + 2x1GB SFP
4GBメモリ
1K SSL @ 5K TPS
2K SSL @ 1K(予測)
1Gbps最大ソフトウェア圧縮
1Gbps L7トラフィック

BIG-IP 3600



デュアルコアCPU
8 10/100/1000 + 2x1GB SFP
4GBメモリ
1K SSL @ 10K TPS
2K SSL @ 2K TPS(予測)
1Gbps最大ソフトウェア圧縮
2Gbps L7トラフィック

BIG-IP 3900



クアッドコアCPU
8 10/100/1000 + 4x1GB SFP
8GBメモリ
1K SSL @ 15K TPS
2K SSL @ 3K TPS(予測)
3.8Gbps最大ソフトウェア圧縮
4Gbps L7トラフィック



BIG-IPハードウェアのラインナップ

統合アプリケーション・デリバリ・プラットフォーム

BIG-IP 6900



2 x デュアルコアCPU
16 10/100/1000 + 8x1GB SFP
8GBメモリ
1K SSL @ 25K TPS
2K SSL @ 5K TPS(予測)
5Gbps最大ハードウェア圧縮
6Gbps L7トラフィック

BIG-IP 8900



2 x クアッドコアCPU
16 10/100/1000 + 8x1GB SFP
16GBメモリ
1K SSL @ 58K TPS
2K SSL @ 12K TPS(予測)
8Gbps最大ハードウェア圧縮
12Gbps L7トラフィック

BIG-IP 8950



2 x クアッドコアCPU
16 10/100/1000 + 8x1GB SFP
16GBメモリ
1K 50K+ SSL TPS
2K 10K+ SSL TPS(予測)
12Gbps最大ソフトウェア
圧縮
20Gbps L7トラフィック

BIG-IP 11050



2 x クアッドコアCPU
16 10/100/1000 + 8x1GB SFP
16GBメモリ
1K SSL @ 100K TPS
2K SSL @ 20K TPS(予測)
48Gbps最大ソフトウェア
圧縮
42Gbps L4トラフィック
40Gbps L7トラフィック



best practices blog browser
code content cookie persis
data center decryption denial
dynamic infrastructure
bal green IT hardware HTT
n detection IPsec IPv6 iRules
open source optimization



例



IT agility. Your way.

SSL TPSの定量化でお客様を支援

- **BIG-IP LTMを利用する多くのお客様は、サポートされる1秒あたりのSSLトランザクション数について完全な利用状況を把握していない**
 - BIG-IP上およびEnterprise Managerで、平均およびピーク時のSSL TPSを判定するための数値を確認
 - 基本SSLライセンス数を超過していないことの検証ログ（基本ライセンスの制限超過に関するレポート）
 - 新しい2Kキーのパフォーマンスの影響を考慮した、デバイスの最大TPSの計算
 - 最大TPSがライセンスまたは平均TPSを下回らないことの確認



公開鍵2048ビットキーに対するサイジング例

お客様: BIG-IP 3600(デュアルコア)
基本SSLライセンス(500TPS/コア – 合計1,000 TPS)
1Kキーに対する最大10,000TPSのSSLをサポート

- **ステップ1:**
EMにより、現在247TPSであることを特定
- **ステップ2:**
最大3600(10,000)のSSLを採用し、2Kキーの場合5で分割 = 新しいSSL TPSは最大2000
- **ステップ3:**
新しいSSL最大値が基本ライセンス数または平均TPSに影響するかどうかを判定
- **ステップ4:**
影響しないか、新しいSSL TPS最大値は、基本ライセンス数および平均TPSを超えているかを判断





®

IT agility. Your way.