WHITE PAPER

ウェブサーバの暗号アルゴリズムの選び方

サイト管理者が押さえておくべき選定のポイント

VeriSign®
A SYMANTEC AFFILIATED COMPANY

WHITE PAPER

WHITE PAPER

CONTENTS

1．はじめに

SSL 通信ではデータが送受信される経路を暗号化して情報を保護します。その SSL 通信を確立するための過程（ネゴシエーション）でも暗号処理が行われています。

このような暗号化の場面で用いられる暗号アルゴリズムはどのように選択されているのでしょうか。そして、安全な通信を実現するにはどのような設定と管理が必要になるのでしょうか。

本ホワイトペーパーでは、暗号処理の概要から、SSL 通信で使用される暗号アルゴリズムの紹介やアルゴリズムを選定する際のポイントについて記載しています。

2．SSL 通信における暗号処理

暗号アルゴリズムの選び方に入る前に、SSL 通信と暗号処理について確認しておくことにします（詳しい説明はホワイトペーパー「SSL を理解するための基礎 ～暗号化通信がはじまるまで～」をご覧ください）。

（1）https のページが表示されるまで

「https」から始まる URL のページがブラウザで表示されるまでには、クライアント（ブラウザ）とサーバの間で主に次のようなやり取り（ネゴシエーション）が行われます。

1） ブラウザ（クライアント）がサーバに https のリクエストを送信

2） ブラウザ / サーバ間で利用される暗号方式の決定

3） サーバからブラウザに SSL サーバ証明書と公開鍵を送付

4） ブラウザからプリマスターシークレットを送付し、ブラウザとサーバで共通鍵を生成

5） ブラウザ/サーバは共通鍵を用いてコンテンツ(データ)を暗号化、送受信

暗号アルゴリズムは、データの暗号化・復号だけでなく、証明書や共通鍵の信頼性の確認、データが改ざんされていないことの確認などにも使用されています。

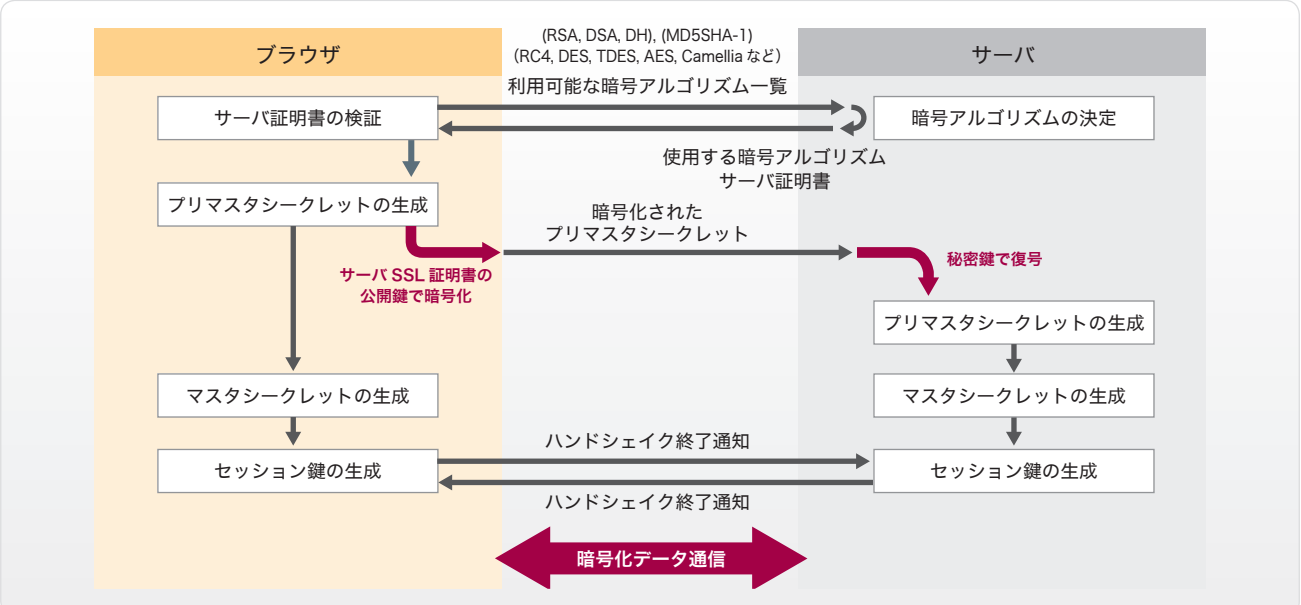

図 1 SSL 通信のハンドシェイクシークエンス

（2）使用される暗号アルゴリズムの決定メカニズム

一般にクライアントとサーバは複数の暗号アルゴリズムに対応しています。そのため、通信を始める前に使用するアルゴリズムを決定するというプロセスが必要となります。

暗号アルゴリズムは次のような手続きで決定されます。

1）クライアントがサーバに SSL 通信をリクエストするときに、サーバへ利用可能な暗号アルゴリズムの一覧を送付します。

2）サーバは、そのなかから使用するアルゴリズムを選択、決定します。

3）サーバは、SSL サーバ証明書と利用暗号アルゴリズムをクライアントに送付します。

4）クライアントはサーバから受信した情報に従って、アルゴリズムを適用します。

（3）Cipher Suite – 利用するアルゴリズムの組み合わせ

「Cipher Suite」とは、SSL 通信に使用するこの暗号アルゴリズムの組み合わせのことです。SSL 通信でクライアントから送付される対応可能なアルゴリズムの一覧には、この組み合わせ、Cipher Suite が記載されています。

表 1 openssl に登録されている Cipher Suite

SSLv3.0 の Cipher Suite	
規格で定められた Cipher Suite	Openssl の中での文字列
SSL_RSA_WITH_NULL_MD5	NULL-MD5
SSL_RSA_WITH_NULL_SHA	NULL-SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5	EXP-RC4-MD5
SSL_RSA_WITH_RC4_128_MD5	RC4-MD5
SSL_RSA_WITH_RC4_128_SHA	RC4-SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5	EXP-RC2-CBC-MD5
SSL_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-DES-CBC-SHA
SSL_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-DSS-DES-CBC-SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA	EDH-DSS-CBC-SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	EDH-DSS-DES-CBC3-SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-RSA-DES-CBC-SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA	EDH-RSA-DES-CBC-SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	EXP-ADH-RC4-MD5
SSL_DH_anon_WITH_RC4_128_MD5	ADH-RC4-MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	EXP-ADH-DES-CBC-SHA
SSL_DH_anon_WITH_DES_CBC_SHA	ADH-DES-CBC-SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	ADH-DES-CBC3-SHA

TLSv1.0 の Cipher Suite	
規格で定められた Cipher Suite	Openssl の中での文字列
TLS_RSA_WITH_NULL_MD5	NULL-MD5
TLS_RSA_WITH_NULL_SHA	NULL-SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5	EXP-RC4-MD5
TLS_RSA_WITH_RC4_128_MD5	RC4-MD5
TLS_RSA_WITH_RC4_128_SHA	RC4-SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	EXP-RC2-CBC-MD5
TLS_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-DES-CBC-SHA
TLS_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-DSS-DES-CBC-SHA
TLS_DHE_DSS_WITH_DES_CBC_SHA	EDH-DSS-CBC-SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	EDH-DSS-DES-CBC3-SHA
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-RSA-DES-CBC-SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA	EDH-RSA-DES-CBC-SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA

クライアントから送付されるアルゴリズムは、優先度の順に並んでいます。サーバは、一覧のなかからサーバ側で設定している優先度の一番高いアルゴリズムを選択します。

多くの Cipher Suite は「DHE-RSA-AES256-SHA」というように、アルゴリズムの組み合わせを表すような名前が付けられています。

3．SSL 通信で利用できる暗号アルゴリズム

SSL 通信で利用可能な暗号アルゴリズムは、第三者による解読技術の進歩やコンピュータ性能の向上にともなって、常に更新されています。ここでは、現在使用されている主なアルゴリズムを紹介します。

（1）主な暗号アルゴリズム

日本国内における電子政府推奨暗号の安全性を評価や暗号技術の適切な実装法・運用法を調査・検討するプロジェクト「CRYPTREC」が発表している「電子政府推奨暗号リスト」には、次の表のようなアルゴリズムが記載されています。

表 2 電子政府推奨暗号リストに分類されているアルゴリズム（一部）

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS1-v1_5
	鍵共有	DH
		ECDH
		PSEC-KEM(注 2)
共通鍵暗号	64 ビットブロック暗号(注 3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES
	128 ビットブロック暗号	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	ストリーム暗号	MUGI
		MULTI-S01
		128-bit RC4(注 5)
その他	ハッシュ関数	RIPEMD-160(注 6)
		SHA-1(注 6)
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

（注 2）KEM（Key Encapsulation Mechanism）-DEM(Data Encapsulation Mechanism) 構成における利用を前提とする。
（注 3）より長いブロック長の暗号が使用できるのであれば、128 ビットブロック暗号を選択することが望ましい。
（注 5）128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。
（注 6）より長いハッシュ値のものが使用できるのであれば、256 ビット以上のハッシュ関数を選択することが望ましい。

最新リストに記載されているアルゴリズムが現在主に使用されているものです。推奨されているものだけでもこれだけのアルゴリズムが存在しています。この表を見ると署名や鍵の暗号化、データの暗号化など用途に応じて利用されるアルゴリズムは異なることが分かります。

（2）暗号アルゴリズム進化の背景

暗号化されたデータを復号するには鍵が必要になります。裏を返せば、鍵がわかってしまえば解読できることになります。しかし、鍵がわからなくても、鍵として送付されるデータの長さ（ビット長）が分かれば、ビット長を手掛かりに、すべてパターンを総当たりで調べることで、理論的には鍵を探し出すことが可能です。

例えば、4桁の数字の暗証番号のような長さの鍵であれば、最大でもわずか1万回（0000 ～ 9999）の繰り返しで、鍵を探し出すことができます。この程度の計算処理ならば、家庭で使用されるコンピュータでも一瞬のうちに完了します。これでは暗号としての意味がありません。

そこで、現在使用されている暗号は、鍵長を長くして、世界最高速のコンピュータで解析しても何年も処理が終わらないようなものが開発・使用されています。

しかし、コンピュータの性能が向上したり、新しい技術が登場したりすることで、その暗号も安全ではなくなる可能性もあります。暗号アルゴリズムは、コンピュータの進化や解読技術の強化を予測して、常に進化しています。

しばらくは 1024 ビット長の公開鍵が主流でしたが、コンピュータ性能の向上にともなって、2010 年にはそれも解読可能な状況になると考えられました。そのため、現在では 2048 ビット長の鍵が主流になっています（いわゆる「暗号の 2010 年問題」、詳細はホワイトペーパー「暗号アルゴリズムにおける 2010 年問題」で説明されています）。暗号は常に進化し続けなければ、安全ではないということです。

（3）さまざまな暗号アルゴリズムが存在する理由

SSL 通信などに使用される暗号アルゴリズムは公開されています。非公開だと、暗号の安全性に関する検証が不十分で脆弱性が残ってしまう恐れがある、各種システムに実装することができない、あるいは実装に非現実的なコストがかかる、といった問題があるからです。

暗号データは、暗号化、復号に使用される鍵でその秘密が守られています。アルゴリズムがわかっているのですから、鍵がわかってしまえば、暗号化の意味はなくなってしまいます。

前述したように鍵長を長くすれば、暗号も解読されにくくなります。しかし、暗号化、復号に何時間もかかるようでは実用的な通信には向きません。そこで安全で実用的な暗号を求めて、様々なアルゴリズムが開発されています。前掲した CRYPTREC の電子政府推奨暗号リストは、2010 年に技術公募が行われており、2013 年をめどとしたリスト改訂も検討されています。

盗聴を試みる者（あるいは安全性を確認しようとする人）は、さまざまな方法で、暗号を解読しようとします。暗号の開発者は、解読されないような工夫を積み重ねていきます。その繰り返しが暗号アルゴリズムを進化させ、さまざまなアルゴリズムが開発される要因となっています。

（4）適用されるアルゴリズムと優先順位の確認

SSL 通信に使用される暗号アルゴリズムは、サーバ OS、クライアント OS、サーバアプリケーション、クライアントアプリケーションなどのソフトウェアが管理しています。

代表的な OS やブラウザなどのアプリケーションで利用可能な Cipher Suite とその優先順位は、ネット上で公開されている情報などで確認することができます。

4．暗号アルゴリズムの選択と設定

SSL 通信で使用される暗号アルゴリズムに関する情報は、サーバやブラウザなどに設定されていて、通常は意識することなく利用されています。OS やアプリケーションをアップデートすれば、その情報も最新のものに更新されます。

しかし、場合によっては、サーバ担当者が暗号アルゴリズムを意識的に選択する必要がでてきます。

どのような場合に選択が必要となるのか、どのように設定すればいいのかを考えて見ましょう。

（1）アルゴリズムの選択が必要となる場合

通常は、暗号アルゴリズムは OS や SSL モジュール、アプリケーションなどで管理されていて、アルゴリズムを意識することはほとんどありません。

しかし、次のような場合は、アルゴリズムを意識して選択する必要があります。

- 自社のターゲットとなるクライアントが利用できるアルゴリズムに制限がある場合
- 携帯電話や組み込み型システムのアプリケーションでソフトウェアのアップデートが難しい場合
- 安全性の低いアルゴリズムの適用を回避して、より安全な通信を実現したい場合
- 通信相手のサーバなどの制限で利用できるアルゴリズムが限定されている場合
- セキュリティ上の問題に迅速に対応したい場合

SSL 暗号化処理を行うアプリケーションを独自に開発しているような場合や DB サーバなど他サーバとの連携処理を行うアプリケーションを開発しているような場合は、その開発・運用環境に合わせて、設定の要・不要を確認することも重要です。

（2）通信対象・環境にあわせたアルゴリズムの選択

携帯電話やゲーム機、カーナビシステムのような組み込み型システムでは、コンピュータの処理性能やメモリなどのリソースの不足、アップデート環境の未対応など、新しいアルゴリズムが適用できない場合も考えられます。

また、企業・組織などでは、費用や互換性の問題から、古いシステムを使い続けている場合も多くあります。ウェブで提供するサービスの対象を比較的古い OS やブラウザにも広げたいような場合もその古い OS やブラウザに合わせるために古いシステムを使い続けるかもしれません。

このような状況では、最新のアルゴリズムに未対応の可能性があるため、対象や環境に合わせたアルゴリズムの選択が必要になります。

（3）優先順位の確認と設定

UNIX 系 OS で openssl 関連モジュールがインストールされている場合は、<openssl ciphers> コマンドで利用可能な Cipher Suite の一覧を確認できます。表示順はサーバでの優先順位になりますが、< Cipher Suite-spec > コマンドを利用して、優先順位を変更することも可能です。

```
$ openssl ciphers -v | sort
AES128-SHA              SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
AES256-SHA              SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
（略）
DHE-DSS-AES128-SHA      SSLv3 Kx=DH       Au=DSS  Enc=AES(128)  Mac=SHA1
DHE-DSS-AES256-SHA      SSLv3 Kx=DH       Au=DSS  Enc=AES(256)  Mac=SHA1
DHE-RSA-AES128-SHA      SSLv3 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA1
DHE-RSA-AES256-SHA      SSLv3 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA1
EDH-RSA-DES-CBC-SHA     SSLv3 Kx=DH       Au=RSA  Enc=DES(56)   Mac=SHA1
EDH-RSA-DES-CBC3-SHA    SSLv3 Kx=DH       Au=RSA  Enc=3DES(168) Mac=SHA1
EXP-DES-CBC-SHA         SSLv3 Kx=RSA(512) Au=RSA  Enc=DES(40)   Mac=SHA1 export
EXP-EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH(512)  Au=DSS  Enc=DES(40)   Mac=SHA1 export
EXP-EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH(512)  Au=RSA  Enc=DES(40)   Mac=SHA1 export
```

図 3 openssl -cipher コマンドの出力例

Windows に関しては、Microsoft の開発者向けサイトで、利用できる Cipher Suite の情報が公開されています。優先度の変更や使用制限の方法なども説明されています。

5．より安全な通信のために

SSL 通信をより安全に行うにはどのような運用・管理が必要なのでしょうか。より安全な通信のために必要なことを考察します。

（1）やぶられない暗号はない

暗号は秘密鍵が分かりさえすれば、解読できてしまいます。

秘密鍵が入手できなくても、鍵のパターンを総当たりで調べれば、探し出すことは不可能ではありません。

十分な時間と機材があれば、SSL 通信で使用されている暗号は解読することができてしまいます。

しかし、現状の主流となっている暗号アルゴリズムでは、世界最高水準のコンピュータを使用しても、秘密鍵を探し出すのに数年かかると報告されています。一般的なパーソナルコンピュータで探そうとすると天文学的な時間がかかるため、少なくとも現状では安全であるということができます。

現状で安全だからといって、それで安心することはできません。技術はたえず進歩しています。最新の動向に注意して、使用するアルゴリズムを選択していくことが重要になります。

（2）変化する技術・環境への対応の必要性

現在安全とされているアルゴリズムでも、コンピュータの性能が向上すると解読されてしまう可能性があります。最近まで主流だった 1024 ビット長の公開鍵は、現在でも十分安全ですが、世代交代の時期にさしかかっていて、徐々に 2048 ビット長の公開鍵が主流になってきています。コンピュータ環境は年々進化し、暗号アルゴリズムもそれに対応して進化し続けています。

クライアントの環境は、パーソナルコンピュータだけでなく、携帯電話、スマートフォン、タブレット端末、携帯ゲーム機など多様化しています。一方、サーバ側の環境も、クラウド化、仮想化など多様化しています。有効なサービスを提供しつづけるには、環境や技術の変化に対応していくことが重要です。

（3）「最強」に設定すればいいというわけではない

安全だからといって、ウェブサイトにアクセスした時にブラウザに表示されるまでしばらく待たなくてはいけないようでは実用的ではありません。クライアントに対応したアルゴリズムを選択する必要があります。

コンピュータリソースが貧弱な利用環境に、最新で最強のアルゴリズムを利用すると、暗号化・復号に時間がかかり、実用性・利便性が犠牲になってしまうことも起こり得ます。安全性を追求し過ぎたがために利用できなくなってしまい、ユーザが減ってしまうということも考えられます。現状の利用者環境を調査して、最適のアルゴリズムを選択することが必要です。

（4）情報源と更新時期の判断

情報通信セキュリティに関する動向は、国内では IPA（情報処理推進機構）のサイトや CRYPTREC のサイトで確認できます。米国の動向は NIST（米国商務省標準技術研究所）のサイトなどで確認できます。

動向を確認して、追加、削除されているアルゴリズムなどがあれば、対応していくことが必要です。

OS やブラウザに関する動向は、それぞれのサポートサイトで確認できます。OS やブラウザは、最新のアップデートを適用すれば、現状でもっとも安全な環境に更新されます。安全であるためには、セキュリティアップデートへの素早い対応が必要ですが、他環境に影響を与える可能性もあるので、適用前に十分な調査が必要です。

確認を怠っていると、脆弱性が報告されている古いアルゴリズムを許可してしまうことや解読されてしまっている短いビット長のアルゴリズムを含んでしまう可能性があります。優先順位の設定によっては、こういった安全ではないアルゴリズムが使われてしまう可能性がありますので、サーバに対して Cipher Suite のリストから削除するなど設定の変更を反映させる必要があります。

6．日本ベリサインからの提言

日本ベリサインでは、現在の暗号強度の妥当性、ルート証明書の市場での普及などを考慮し、最適なアルゴリズムを用いた証明書を提供しています。

原則として、日本ベリサインでは、CRYPTREC が推奨する暗号方式をベースとした SSL サーバ証明書を提供しています。CRYPTREC の推奨暗号方式は時間とともに変化していきますが、2012 年 2 月現在、公開鍵は RSA、共通鍵は AES や 3Key Triple DES、ハッシュ関数は SHA-1 や SHA-2 などの形式を利用することが安全性と可用性のバランスの観点から、推奨されています。

7．まとめ

SSL 通信で使用される暗号アルゴリズムは、より安全なものへと日々進化しています。安全な通信の実現には、現状の安全性や利用環境を考慮して、適切なアルゴリズムを選択、利用することが大切です。

SSL 通信で使用される暗号アルゴリズムは、クライアントから送信された利用可能なアルゴリズムの一覧のなかから、サーバが最適なものを選択することで決定されます。サーバ担当者はサーバ側で利用可能なアルゴリズムの一覧を編集することで、利用されるアルゴリズムや優先順位を指定することができます。

現在使用されている主なアルゴリズムは、CRYPTREC や NIST などが提供する情報で確認できます。技術の進歩や利用環境の多様化にあわせて、現状で最適のアルゴリズムを選択することが重要です。

WPAlgorithm2012_1202

日本ベリサイン株式会社
https://www.VeriSign.co.jp/
〒104-0028　東京都中央区八重洲 2-8-1
Tel : 03-3271-7017
E-mail : websales@verisign.co.jp