

サンプル トランザクションおよびパケット交換による SSL の概要

内容

[概要](#)

[SSL レコードの概要](#)

[レコード形式](#)

[レコード タイプ](#)

[レコード バージョン](#)

[レコード長](#)

[レコードのタイプ](#)

[ハンドシェイク レコード](#)

[CCSレコード](#)

[アラート レコード](#)

[アプリケーション データ レコード](#)

[サンプル トランザクション](#)

[Hello 交換](#)

[クライアント交換](#)

[暗号の変更](#)

[関連情報](#)

概要

このドキュメントでは、セキュア ソケット レイヤ (SSL) プロトコルの基本概念について説明し、トランザクションとパケット キャプチャの例を示します。

SSL レコードの概要

SSL 内のデータの基本単位がレコードです。各レコードは 5 バイトのレコード ヘッダーとその後続くデータで構成されます。

レコード形式

- Type:uint8 – 値リスト
- バージョン:uint16
- Length:uint16

Type バージョン 長さ

T VH VL LH LL

レコード タイプ

SSL には 4 つのレコード タイプがあります。

- ハンドシェイク (22、 0x16)
- 暗号仕様変更 (20、 0x14)
- アラート (21、 0x15)
- アプリケーション データ (23、 0x17)

レコード バージョン

レコードバージョンは16ビットの値で、ネットワーク順にフォーマットされます。

注：SSLバージョン3(SSLv3)の場合、バージョンは0x0300です。Transport Layer Security Version 1(TLSv1)の場合、バージョンは0x0301です。Cisco Adaptive Security Appliance(ASA)は、SSLバージョン2(SSLv2)をサポートしませんバージョン0x0002、またはTLSv1より大きいTLSの任意のバージョン。

レコード長

レコード長は 16 バイト値で、ネットワーク順序でフォーマットされます。

理論上、これは 1 つのレコードを最大 $65,535 (2^{16} - 1)$ バイトの長さに行うことができることを意味します。TLSv1 RFC2246 では、最大長が $16,383 (2^{14} - 1)$ と規定されています。Microsoft 製品 (Microsoft Internet Explorer とインターネット インフォメーション サービス) はこの制限を超えていることが知られています。

レコードのタイプ

ここでは、4 種類の SSL レコードについて説明します。

ハンドシェイク レコード

ハンドシェイク レコードには、ハンドシェイクに使用される一連のメッセージが含まれています。次に、メッセージとその値を示します。

- Hello Request (0、 0x00)
- Client Hello (1、 0x01)
- Server Hello (2、 0x02)
- Certificate (11、 0x0B)
- Server Key Exchange (12、 0x0C)
- Certificate Request (13、 0x0D)
- Server Hello Done (14、 0x0E)
- Certificate Verify (15、 0x0F)
- Client Key Exchange (16、 0x10)
- Finished (20、 0x14)

シンプルなケースでは、ハンドシェイク レコードが暗号化されません。ただし、Finished メッセージを含むハンドシェイク レコードは、常に暗号仕様変更 (CCS) レコードの後ろに出現するため、必ず暗号化されます。

CCSレコード

CCSレコードは、暗号暗号の変更を示すために使用されます。CCSレコード以降のすべてのデータが新しい暗号を使って暗号化されます。CCSレコードは暗号化される場合とされない場合があります。1回のハンドシェイクによるシンプルな接続では、CCSレコードが暗号化されません。

アラートレコード

アラートレコードは、ある状態が発生したことをピアに知らせるために使用されます。一部のアラートは警告ですが、その他は致命的で、接続が失敗します。アラートは、暗号化される場合とされない場合があります、ハンドシェイク中やデータ転送中に発生する可能性があります。アラートには次の2種類があります。

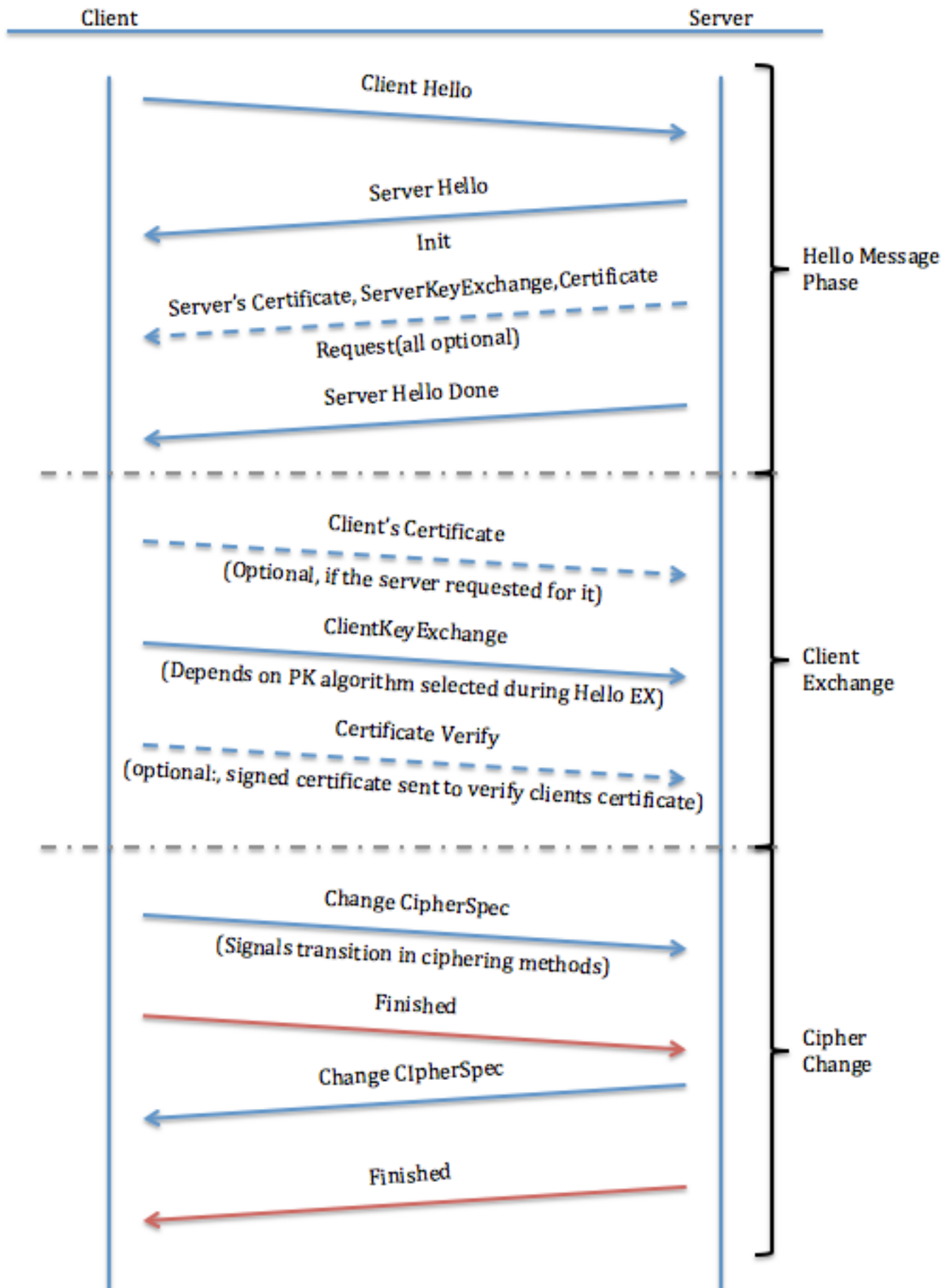
- **クロージャアラート**: トランケーション攻撃を防ぐためには、クライアントとサーバ間の接続が正しく閉じられている必要があります。送信者がその接続ではこれ以上メッセージを送信しないことを示す `close_notify` メッセージが受信者に送信されます。
- **エラーアラート**: エラーが検出されると、検出側から相手側にメッセージが送信されます。致命的な警告メッセージが送信または受信されると、両当事者は即座に接続を閉じます。エラーアラートの例は次のとおりです。
 - `unexpected_message` (致命的)
 - `decompression_failure`
 - `handshake_failure`

アプリケーションデータレコード

このレコードには実際のアプリケーションデータが含まれています。これらのメッセージは、レコード層で伝送され、現在の接続状態に基づいて、フラグメント化、圧縮、または暗号化されます。

サンプルトランザクション

ここでは、クライアントとサーバ間のサンプルトランザクションについて説明します。



Hello 交換

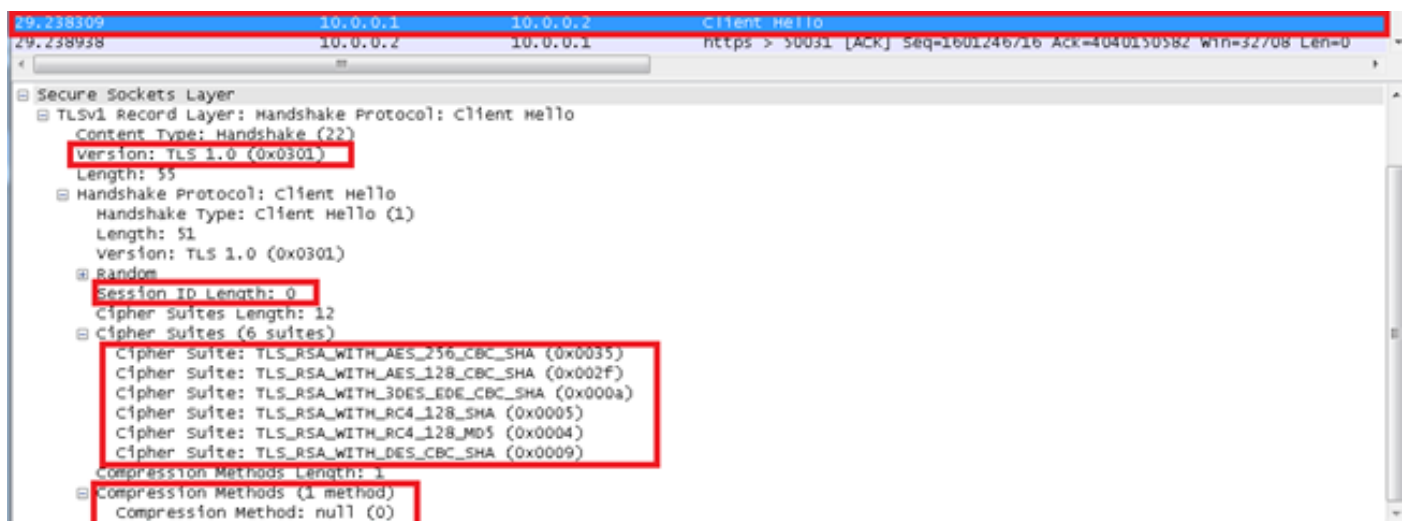
SSLクライアントとサーバが通信を開始すると、プロトコルバージョンに合意し、暗号化アルゴリズムを選択し、オプションで互いを認証し、公開鍵暗号化技術を使用して共有秘密を生成します。これらのプロセスはハンドシェイクプロトコルで実行されます。要約すると、クライアントが Client Hello メッセージをサーバに送信します。このメッセージには Server Hello メッセージで応答する必要があり、そうしない場合は致命的なエラーが発生して接続が失敗します。Client Hello と Server Hello は、クライアントとサーバ間でセキュリティ拡張機能を設定するために使用されます。

Client Hello

Client Hello は、次の属性をサーバに送信します。

- **プロトコルバージョン**：クライアントがこのセッション中に通信する SSL プロトコルのバージョン。
- **Session ID**：クライアントがこの接続に使用するセッションの ID。交換の最初のクライアント Hello では、セッション ID は空です（注の後のパケットキャプチャ画面を参照）。
- **暗号スイート**：これは、Client Hello メッセージでクライアントからサーバに渡されます。これには、クライアントのプリファレンス（最優先選択肢）の順番でクライアントでサポートされる暗号化アルゴリズムの組み合わせが含まれています。暗号スイートごとに、キー交換アルゴリズムと暗号仕様の両方が定義されます。サーバは、暗号スイートを選択するか、受け入れ可能な選択肢がない場合は、ハンドシェイク障害アラートを返して、接続を閉じます。
- **圧縮方式**：クライアントでサポートされる圧縮アルゴリズムのリストが含まれています。サーバがクライアントから送信された方式をサポートしていない場合は、接続が失敗します。圧縮方式は null にすることもできます。

注：キャプチャ内のサーバ IP アドレスは 10.0.0.2 で、クライアント IP アドレスは 10.0.0.1 です。



Server Hello

サーバは次の属性をクライアントに送り返します。

- **プロトコルバージョン**：クライアントがサポートする SSL プロトコルの選択されたバージョン。
- **Session ID**：これは、この接続に対応するセッションの ID です。Client Hello でクライアント

から送信されたセッション ID が空でない場合は、サーバがセッション キャッシュで一致するものを探します。一致するものが見つかって、サーバが指定されたセッション状態を使用して新しい接続を確立する場合は、クライアントから提供されたものと同じ値で応答します。これは、セッションが再開されたことを示し、パーティが直接 Finished メッセージに進む必要があることを示します。そうでない場合は、このフィールドに新しいセッションを識別する別の値が設定されます。サーバは、空の session_id を返すことによって、セッションがキャッシュされないために再開できないことを示す場合があります。

- 暗号スイート：クライアントから送信されたリストからサーバが選択したもの。
- 圧縮方式：クライアントから送信されたリストからサーバが選択したもの。
- 証明書要求：サーバは、クライアントに、設定されているすべての証明書のリストを送信して、認証に使用する証明書の選択を許可します。

```
29.238309 10.0.0.1 10.0.0.2 Client Hello
29.238938 10.0.0.2 10.0.0.1 https > 50031 [ACK] Seq=1601246716 Ack=4040150582 win=32708 Len=0
29.239787 10.0.0.2 10.0.0.1 Server Hello
29.328209 10.0.0.1 10.0.0.2 https > 50031 [ACK] Seq=4040150582 Ack=1601247252 win=65392 Len=0
29.443515 10.0.0.1 10.0.0.2 https > 50031 [ACK] Seq=4040150582 Ack=1601247252 win=65392 Len=0
```

Secure Sockets Layer

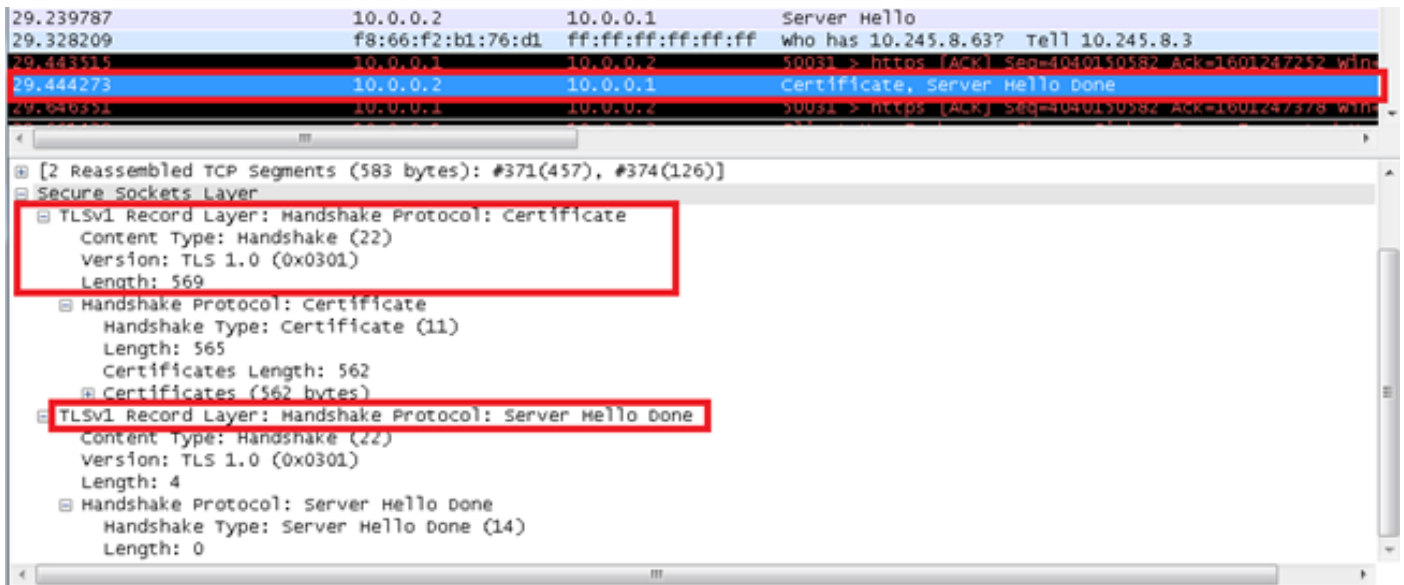
- TLsv1 Record Layer: Handshake Protocol: Server Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 74
 - Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 70
 - Version: TLS 1.0 (0x0301)
 - Random
 - Session ID Length: 32
 - Session ID: caf9e8d321497a554c29e108b34774c266b5ae05db2e5935...
 - Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
 - Compression Method: null (0)

SSL セッション再開要求の場合：

- サーバはクライアントに Hello 要求も送信できます。これは、都合の良いときに、Client Hello 要求を使って再ネゴシエーションを開始する必要があることをクライアントに知らせるためだけのものです。クライアントは、ハンドシェイク プロセスがすでに進行中であれば、サーバからの Hello 要求を無視します。
- ハンドシェイク メッセージは、アプリケーション データの伝送より優先されます。再ネゴシエーションは、最大長アプリケーション データ メッセージの伝送時間の 1 ~ 2 倍以内で開始する必要があります。

Server Hello Done

Server Hello Done メッセージは、Server Hello と関連するメッセージの終わりを示すためにサーバによって送信されます。このメッセージの送信後に、サーバはクライアントの応答を待ちます。Server Hello Done メッセージを受信すると、クライアントは、必要に応じて、サーバから有効な証明書が提供されたことを確認し、Server Hello パラメータが受け入れ可能かどうかをチェックします。



Server Certificate、Server Key Exchange、および Certificate Request (オプション)

- **サーバ証明書** : サーバが認証される必要がある場合 (通常は認証される場合)、サーバはサーバのHelloメッセージの直後に証明書を送信します。証明書の種類は、選択された暗号スイート キー交換アルゴリズムに適している必要があり、通常は X.509.v3 証明書が使用されます。
- **Server Key Exchange: Server Key Exchange**メッセージは、証明書がない場合にサーバーから送信されます。Diffie-Hellman(DH)パラメータがサーバ証明書に含まれている場合、このメッセージは使用されません。
- **証明書要求** : サーバは、選択した暗号スイートに適している場合、クライアントから証明書を必要に応じて要求できます。

クライアント交換

Client Certificate (オプション)

これは、Server Hello Done メッセージの受信後にクライアントが送信する最初のメッセージです。このメッセージは、サーバが証明書を要求した場合にだけ送信されます。適切な証明書が使用できない場合は、クライアントが代わりに **no_certificate アラート**を送信します。このアラートは単なる警告です。ただし、クライアント認証が必要な場合は、サーバが致命的なハンドシェイク障害アラートで応答する可能性があります。クライアント DH 証明書は、サーバ指定の DH パラメータと一致する必要があります。

Client Key Exchange

このメッセージの内容は、Client Hello メッセージと Server Hello メッセージ間で選択された公開キーアルゴリズムによって異なります。クライアントは、Rivest-Shamir-Addleman (RSA) アルゴリズムで暗号化されたプレマスターキーと、キーの同意と認証用の DH のどちらかを使用します。RSA がサーバ認証とキー交換に使用される場合は、48 バイトの **pre_master_secret** がクライアントによって生成され、サーバ公開キーに基づいて暗号化され、サーバに送信されます。サーバは、秘密キーを使用して、pre_master_secret を復号化します。その後で、両方のパーティが **pre_master_secret** を **master_secret** に変換します。


```
29.444273      10.0.0.2      10.0.0.1      Certificate, Server Hello Done
19.661429      10.0.0.1      10.0.0.2      50031 > https [ACK] Seq=4040150582 Ack=1601247378 Win=65766 Len=0
19.661429      10.0.0.1      10.0.0.2      Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

Transmission Control Protocol, Src Port: 50031 (50031), Dst Port: https (443), Seq: 4040150582, Ack: 1601247378, Len: 190
Secure Sockets Layer
  TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 134
    Handshake Protocol: Client Key Exchange
      Handshake Type: Client Key Exchange (16)
      Length: 130
      RSA Encrypted PreMaster Secret
        Encrypted PreMaster length: 128
        Encrypted PreMaster: 8293da22dfb73f3d724cfb707dcd8c1e1c6917a8d1578520...
  TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.0 (0x0301)
    Length: 1
    Change Cipher Spec Message
  TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 40
    Handshake Protocol: Encrypted Handshake Message
```

Certificate Verify (オプション)

クライアントが署名可能な証明書を送信すると、デジタル署名された Certificate Verify メッセージが送信され、証明書が明示的に確認されます。

暗号の変更

暗号仕様変更メッセージ

暗号仕様変更メッセージがクライアントによって送信され、クライアントは保留中の暗号仕様 (新しい仕様) を現在の暗号仕様 (これまで使用されていた仕様) にコピーします。暗号仕様の変更プロトコルは、暗号化戦略の移行を信号で通知するために存在します。このプロトコルは、現在の (保留中ではない) 暗号仕様で暗号化および圧縮された単一のメッセージで構成されます。このメッセージを受信すると、受信側はread pending状態をread current状態にコピーします。クライアントは、ハンドシェイクキー交換および証明書検証メッセージ (ある場合) の後に Change Cipher Specメッセージを送信し、サーバは、クライアントから受信したキー交換メッセージを正常に処理した後に送信します。1つ前のセッションが再開されると、暗号仕様変更メッセージが Hello メッセージの後に送信されます。キャプチャでは、Client Exchange、Change Cipher、および Finished の各メッセージがクライアントから1つのメッセージとして送信されています。

Finished メッセージ

Finished メッセージは、キー交換プロセスと認証プロセスが成功したことを確認するために、常に暗号仕様変更メッセージの直後に送信されます。Finishedメッセージは、最も最近ネゴシエートされたアルゴリズム、キー、およびシークレットを含む最初の保護パケットです。Finishedメッセージの確認応答は必要ありません。パーティは、Finishedメッセージの送信直後に暗号化されたデータの送信を開始できます。Finishedメッセージの受信側は、その内容が正しいことを確認する必要があります。

29.444273	10.0.0.2	10.0.0.1	Certificate, Server Hello Done
29.646351	10.0.0.1	10.0.0.2	50031 > https [ACK] Seq=4040150582 Ack=1601247378 win=65766 len=0
29.661429	10.0.0.1	10.0.0.2	client key exchange, change cipher spec, Encrypted Handshake Message

Transmission Control Protocol, Src Port: 50031 (50031), Dst Port: https (443), Seq: 4040150582, Ack: 1601247378, Len: 190			
Secure Sockets Layer			
TLSv1 Record Layer: Handshake Protocol: Client Key Exchange			
Content Type: Handshake (22)			
Version: TLS 1.0 (0x0301)			
Length: 134			
Handshake Protocol: Client Key Exchange			
Handshake Type: Client Key Exchange (16)			
Length: 130			
RSA Encrypted PreMaster Secret			
Encrypted PreMaster length: 128			
Encrypted PreMaster: 8293da22dfb73f3d724cfb707dcd8c1e1c6917a8d1578520			
TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec			
Content Type: Change Cipher Spec (20)			
Version: TLS 1.0 (0x0301)			
Length: 1			
Change Cipher Spec Message			
TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message			
Content Type: Handshake (22)			
Version: TLS 1.0 (0x0301)			
Length: 40			
Handshake Protocol: Encrypted Handshake Message			

関連情報

- [RFC 6101 - セキュア ソケット レイヤ プロトコル バージョン 3.0](#)
- [Wireshark SSL Wiki:WiresharkでSSLパケットを復号化](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)