

---

PF5200 シリーズ

【別冊】 OpenFlow 機能 TLS 対応編

## ■対象製品

このマニュアルは、PF5200 シリーズの OpenFlow 機能の TLS 対応版に関する運用手順について記載しています。必ず、「PF5200 シリーズ ソフトウェアマニュアル」と併せてお読みください。ソフトウェア機能は、ソフトウェア OS-F3PA によってサポートする機能について記載します。

## ■輸出時の注意

本製品は、外国為替及び外国貿易法に基づくリスト規制の該当貨物ですので、輸出（又は非居住者への技術の提供あるいは外国において技術の提供をすることを目的とする取引）を行う場合には、経済産業大臣の輸出許可（又は役務取引許可）が必要となります。

また、本製品には米国の輸出関連法令の規制を受ける技術が含まれており、輸出する場合輸出先によっては米国政府の許可が必要です。

## ■商標一覧

Microsoft は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標です。

UNIX は、X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。

「プログラマブルフロー」および「ProgrammableFlow」は、日本電気株式会社の登録商標または商標です。

その他、各会社名、各製品名は、各社の商標または登録商標です。

## ■マニュアルはよく読み、保管してください。

製品を使用する前に、安全上の説明をよく読み、十分理解してください。

このマニュアルは、いつでも参照できるよう、手近な所に保管してください。

## ■ご注意

このマニュアルの内容については、改良のため、予告なく変更する場合があります。

## ■電波障害について

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

## ■高調波規制について

高調波電流規格 JIS C 61000-3-2 適合品

適合装置：

- PF5240F-48T4XW
- PF5240R-48T4XW

## ■発行

2011 年 10 月（初版）NWD-126045-001

## ■著作権

Copyright (C) 2010-2011, NEC Corporation. All rights reserved.



# はじめに

---

## ■対象製品およびソフトウェアバージョン

このマニュアルは PF5200 シリーズを対象に記載しています。ソフトウェア機能は、ソフトウェア OS-F3PA によってサポートする OpenFlow 機能の TLS 対応版に関する運用手順について記載しています。

操作を行う前にこのマニュアルをよく読み、書かれている指示や注意を十分に理解してください。また、このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。

## ■このマニュアルの訂正について

このマニュアルに記載の内容は、ソフトウェアと共に提供する「リリースノート」および「マニュアル訂正資料」で訂正する場合があります。

## ■対象読者

TLS 対応版 OpenFlow 機能を運用するシステム管理者の方を対象としています。

また、次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

## ■マニュアルの読書手順

本装置の導入、セットアップ、日常運用までの作業フローに従って、それぞれの場合に参照するマニュアルを次に示します。

- 装置の開梱から、初期導入時の基本的な設定について知りたい

PF5200 シリーズ  
クイックスタートガイド

(NWD-126031-001)

- ハードウェアの設備条件、取り扱い方法について知りたい

PF5200 シリーズ  
ハードウェア取扱説明書

(NWD-126033-001)

- ソフトウェアの機能、コンフィグレーションの設定、運用コマンドについて知りたい

PF5200 シリーズ ソフトウェアマニュアル  
コンフィグレーションガイド Vol.1

(NWD-126034-001)

PF5200 シリーズ ソフトウェアマニュアル  
コンフィグレーションガイド Vol. 2

(NWD-126034-002)

PF5200 シリーズ ソフトウェアマニュアル  
コンフィグレーションガイド Vol. 3

(NWD-126034-003)

- コンフィグレーションコマンドの入力シンタックス、パラメータ詳細について知りたい

PF5200 シリーズ ソフトウェアマニュアル  
コンフィグレーション コマンドレファレンス Vol.1

(NWD-126037-001)

PF5200 シリーズ ソフトウェアマニュアル  
コンフィグレーション コマンドレファレンス Vol. 2

(NWD-126037-002)

- 運用コマンドの入力シンタックス、パラメータ詳細について知りたい

PF5200 シリーズ ソフトウェアマニュアル  
運用コマンドレファレンス Vol.1

(NWD-126039-001)

PF5200 シリーズ ソフトウェアマニュアル  
運用コマンドレファレンス Vol.2

(NWD-126039-002)

- メッセージとログについて知りたい

PF5200 シリーズ ソフトウェアマニュアル  
メッセージ・ログレファレンス

(NWD-126041-001)

- MIB について知りたい

PF5200 シリーズ ソフトウェアマニュアル  
MIB レファレンス

(NWD-126042-001 )

- ソフトウェアアップデートを行う手順について知りたい

PF5200 シリーズ  
ソフトウェアアップデートガイド

(NWD-126047-001)

- ネットワーク接続のセキュアな運用管理について知りたい

PF5200 シリーズ  
Secure Shell (SSH) ソフトウェアマニュアル

(NWD-126044-001 )

- トラブル発生時の対処方法について知りたい

PF5200 シリーズ  
トラブルシューティングガイド

(NWD-126043-001)

- Secure Channel の TLS 接続について知りたい

PF5200 シリーズ  
【別冊】 OpenFlow 機能 TLS 対応編

(NWD-126045-001 )

## ■このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second *bpsと表記する場合があります。
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
E-Mail	Electronic Mail
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPv6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode

LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations, Administration, and Maintenance
OFC	OpenFlow Controller
OFS	OpenFlow Switch
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PFS	Programmable Flow Switch
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSI	Real Switch Instance
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SElector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol



SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
VSI	Virtual Switch Instance
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WoL	Wake on LAN
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

## ■ 常用漢字以外の漢字の使用について

このマニュアルでは、常用漢字を使用することを基本としていますが、次に示す用語については、常用漢字以外を使用しています。

- 溢れ（あふれ）
- 迂回（うかい）
- 筐体（きょうたい）
- 毎（ごと）
- 閾値（しきいち）
- 溜まる（たまる）
- 輻輳（ふくそう）
- 漏洩（ろうえい）

## ■ kB(バイト)などの単位表記について

1kB(キロバイト), 1MB(メガバイト), 1GB(ギガバイト), 1TB(テラバイト)はそれぞれ 1024 バイト, 1024<sup>2</sup> バイト, 1024<sup>3</sup> バイト, 1024<sup>4</sup> バイトです。



## 目次

1	運用手順	1
1.1	概要	2
1.2	運用手順	4
1.3	TLS 利用条件	5
2	クライアント証明書・鍵の作成と登録	7
2.1	作成環境	8
2.2	作成手順	9
2.2.1	OpenSSL 入力情報	9
2.2.2	OpenSSL 操作方法	10
2.3	クライアント証明書・鍵の登録	13
2.3.1	クライアント証明書と鍵の登録	13
2.3.2	クライアント証明書と鍵の削除	13
2.4	OpenFlow 機能 Secure Channel の TLS 接続設定	14
3	コンフィグレーションコマンドレファレンス	15
	controller	16
4	運用コマンドレファレンス	19
	set openflow certificate	20
	erase openflow certificate	22
	show openflow certificate	24
	show openflow	27
	show openflow statistics	30
5	メッセージログレファレンス	33
6	トラブルシューティング	35
	付録	37
	付録 A 謝辞 (Acknowledgments)	38



# 1

## 運用手順

---

1.1 概要

---

1.2 運用手順

---

1.3 TLS 利用条件

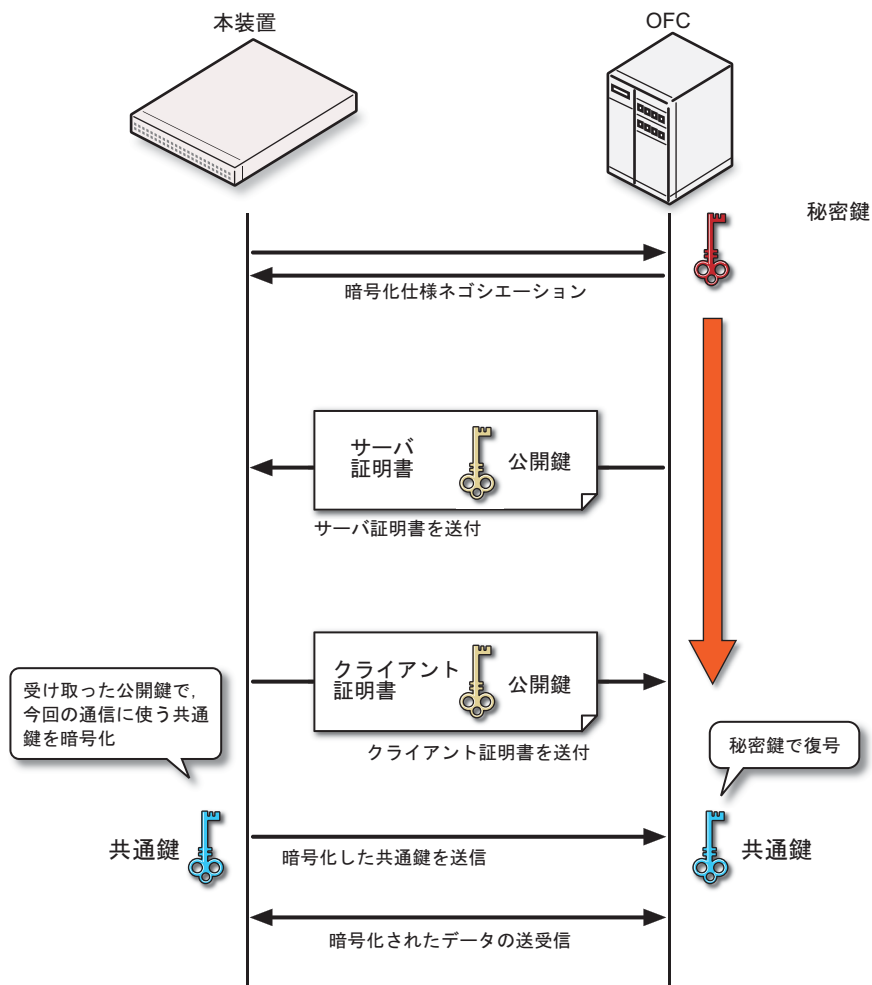
---

## 1.1 概要

OpenFlow 機能における Secure Channel 接続で、PF5200 シリーズと OpenFlow コントローラ (OFC) 間の通信を他者からガードするために TLS 接続が使用できます。

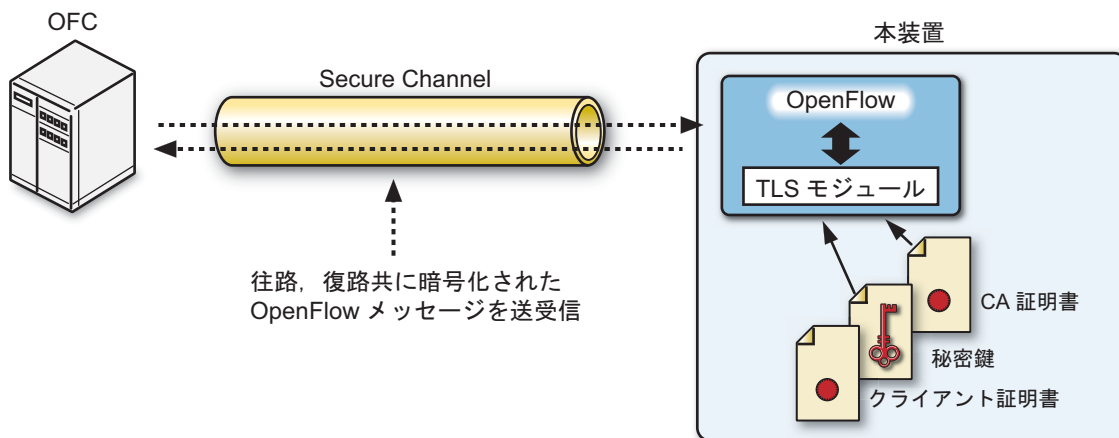
Secure Channel の TLS 接続では、OFC をサーバに見立てて、本装置および OFC 間で双方向認証を実施します。その後 OFC のサーバ証明書と鍵を用いて Secure Channel の通信暗号化が行われます。

図 1-1 TLS の動作



Secure Channel を TLS 接続した場合、Secure Channel を通過する OpenFlow メッセージパケットは図 1-2 に示すように暗号化されネットワークを流れます。

図 1-2 TLS 接続時の Secure Channel 通信状態



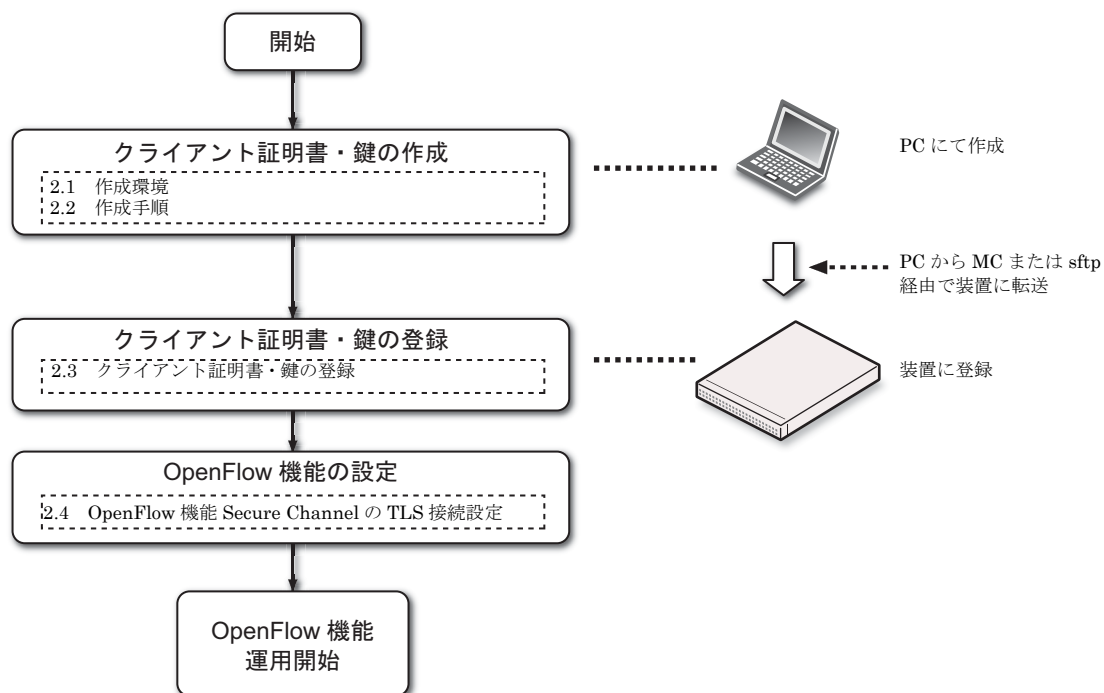
【注意】

TLS 接続を使用するにあたっては、本装置にクライアント証明書と秘密鍵および CA 証明書を登録する必要があります。また OFC 側にはサーバ証明書と秘密鍵および CA 証明書を登録する必要があります。OFC の設定については OFC のマニュアルにてご確認ください。

## 1.2 運用手順

OpenFlow 機能の Secure Channel を TLS 接続するにあたっては、次の手順に沿って作業を行ってください。

図 1-3 運用手順





## 1.3 TLS 利用条件

OpenFlow 機能の TLS 利用条件を表 1-1 ，表 1-2 に示します。

表 1-1 TLS 利用条件

項番	機能名		備考
1	TLS バージョン	TLS1.0	-
2	鍵交換アルゴリズム		-
(1)	DH	512 bit	-
(2)	RSA	512 bit	-
3	公開鍵暗号方式		認証に用います
(1)	RSA	1024 ～ 4096 bit(注 <sup>1</sup> )	-
(2)	DSA	3072 bit	-
4	共通鍵暗号方式		通信路の暗号化に用います
(1)	AES	128 bit	-
(2)	AES	256 bit	-
(3)	DES	40 bit	-
(4)	DES	56 bit	-
(5)	3DES	168 bit	-
5	メッセージ認証コード (MAC) 方式		データの改ざん防止に用います
(1)	SHA-1	160 bit	-
6	証明書		-
(1)	PKCS#12		スイッチ, コントローラの証明書
(2)	PEM		コントローラの証明書

(注<sup>1</sup>) 鍵長はセキュリティ上安全とされる値を指定してください。

表 1-2 TLS でサポートする暗号アルゴリズムの組み合わせ

No	アルゴリズム名	鍵交換 アルゴリズム (SSLv3 Kx)	公開鍵 暗号方式 (Au)	共通鍵 暗号方式 (Enc)	ハッシュ関数 (Mac)
1	DHE-RSA-AES256-SHA	DH(512)	RSA(2048)	AES(256)	SHA1
2	DHE-DSS-AES256-SHA	DH(512)	DSA(3072)	AES(256)	SHA1
3	AES256-SHA	RSA(512)	RSA(2048)	AES(256)	SHA1
4	EDH-RSA-DES-CBC3-SHA	DH(512)	RSA(2048)	3DES(168)	SHA1
5	EDH-DSS-DES-CBC3-SHA	DH(512)	DSA(3072)	3DES(168)	SHA1
6	DES-CBC3-SHA	RSA(512)	RSA(2048)	3DES(168)	SHA1
7	DHE-RSA-AES128-SHA	DH(512)	RSA(2048)	AES(128)	SHA1
8	DHE-DSS-AES128-SHA	DH(512)	DSA(3072)	AES(128)	SHA1
9	AES128-SHA	RSA(512)	RSA(2048)	AES(128)	SHA1
10	EDH-RSA-DES-CBC-SHA	DH(512)	RSA(2048)	DES(56)	SHA1
11	EDH-DSS-DES-CBC-SHA	DH(512)	DSA(3072)	DES(56)	SHA1
12	DES-CBC-SHA	RSA(512)	RSA(2048)	DES(56)	SHA1
13	EXP-EDH-RSA-DES-CBC-SHA	DH(512)	RSA(2048)	DES(40)	SHA1
14	EXP-EDH-DSS-DES-CBC-SHA	DH(512)	DSA(3072)	DES(40)	SHA1
15	EXP-DES-CBC-SHA	RSA(512)	RSA(2048)	DES(40)	SHA1

# 2

## クライアント証明書・鍵の作成と登録

---

2.1 作成環境

---

2.2 作成手順

---

2.3 クライアント証明書・鍵の登録

---

2.4 OpenFlow 機能 Secure Channel の TLS 接続設定

---

## 2.1 作成環境

---

本章では、例として共通鍵暗号方式 AES256bit、鍵長 2048bit のクライアント証明書、および鍵の作成と登録方法について示します。

TLS 用クライアント証明書と鍵を作成するには、OpenSSL が動く環境が必要です。OpenSSL が動作する OS は次の通りであり、下記 OS が動作する環境下で、OpenSSL を実行してクライアント証明書と鍵を作成します。(OpenSSL の構築に関しては、オープンソースである OpenSSL のドキュメントを参照してください)

### [ 動作 OS ]

UNIX 系 OS

Windows 系 OS(cygwin が動作必須)

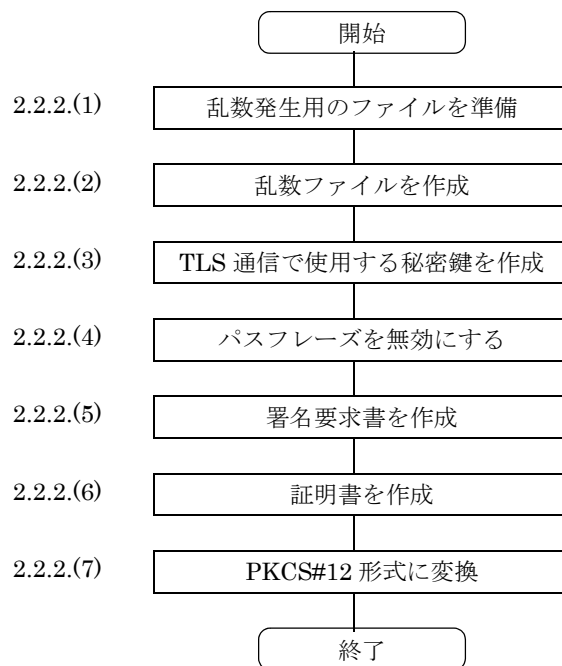
### [OpenSSL 版数]

OpenSSL 0.9.7i 以降のバージョンを使用してください。

## 2.2 作成手順

TLS 用クライアント証明書と鍵は次の手順で OpenSSL が動作する環境で作成します。

図 2-1 クライアント証明書・鍵の作成手順



### 2.2.1 OpenSSL 入力情報

クライアント証明書・鍵の作成にあたり、OpenSSL に次の情報を入力します。

なお、表 2-1 OpenSSL 入力情報に示した入力例は、本書の操作を示すために用いたものです。実際の入力に際しては、CA 局が発行する CA 証明書との照合に必要な情報を入力してください。

表 2-1 OpenSSL 入力情報

名称	内容・意味	入力例
pass phrase for client.key	クライアント用パスワード	aaaa123
Country Name	国コード	JP
State or Province Name	都道府県名	TOKYO
Locality Name	市区町村名	MINATOKU
Organization Name	団体名または、会社名	NEC
Organizational Unit Name	部署名	PF5200
Common Name	本装置の URL または、IP アドレス	192.168.1.1
Email Address	管理者の電子メールアドレス	nec@nec.jp.com
challenge password	(入力不要)	—
optional company name	(入力不要)	—

## 2.2.2 OpenSSL 操作方法

OpenSSL の操作方法是次の通りです。

なお、クライアント証明書・鍵を作成する OpenSSL 動作環境とスイッチの環境とを区別するために OpenSSL 動作環境のプロンプトを” unix# “と表示します。

### (1) 乱数発生用のファイルを準備

乱数発生用に ASCII コードで書かれているテキストファイルを作成します。(数行程度のテキストファイルで内容は問いません)

### (2) 乱数ファイルを作成

乱数用テキストファイル名を `moto.txt`, 乱数ファイル名を `rand.dat` とした実行例を示します。

```
unix# openssl sh1 moto.txt > rand.dat
```

乱数ファイル

### (3) TLS 通信で使用する鍵を作成

AES 256bit, 鍵長 2048bit とした鍵 (秘密鍵 : ファイル名 `:client.key`) の実行例を示します。

```
unix# openssl genrsa -aes256 -out client.key -rand rand.dat 2048
Loading 'screen' into random state - done
48 semi-random bytes loaded
Generating RSA private key, 2048 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
Enter pass phrase for client.key: ←クライアント用のパスワードを入力します。
Verifying - Enter pass phrase for client.key: ←クライアント用のパスワードを再度入力
                                         します。
```


### (4) パスフレーズを無効

鍵 (ファイル名 `:client.key`) のパスフレーズを無効とする実行例を示します。

```
unix# openssl rsa -in client.key -out client.key
Enter pass phrase for client.key: ←(3)で入力したクライアント用のパスワードを入力し
                                         ます。
writing RSA key
```

## (5) 署名要求書を作成

秘密鍵 (ファイル名 :client.key) から署名要求書 (ファイル名 :client.csr) を作成する実行例を示します。



```
unix# openssl req -new -key client.key -out client.csr
```

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank. For some fields there will be a default value, If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:JP ←国コードを入力します。

State or Province Name (full name) [Some-State]:TOKYO ←都道府県名を入力します。  
(例: 'TOKYO')

Locality Name (eg, city) []:MINATOKU ←地域を入力します。(例: 'MINATOKU')

Organization Name (eg, company) [Internet Widgits Pty Ltd]:NEC ←会社名を入力します。(例: 'NEC')

Organizational Unit Name (eg, section) []:PF5200 ←任意の名称を入力します。(例: 'PF5200')

Common Name (eg, YOUR name) []:192.168.1.1 ←スイッチのIPアドレスを入力します。

Email Address []:nec@nec.jp.com ←e-mailアドレスを入力します。  
(例: 'nec@nec.jp.com')

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password []: ←何も入力しません。

An optional company name []: ←何も入力しません。

## (6) CA の署名付きクライアント証明書を作成

CA によって署名されたクライアント証明書 (ファイル名 :client.crt) を作成する実行例を示します。



```
unix# openssl ca -in client.csr -keyfile private/cakey.pem -cert cacert.pem -out client.crt
```

## (7) PKCS#12 形式の証明書に変換

クライアント証明書 (ファイル名 :client.crt) と秘密鍵 (ファイル名 :client.key) を 1 つの PKCS#12 形式の証明書 (ファイル名 :client.p12) に変換する実行例を示します (OpenFlow 機能の TLS 利用条件については、表 1-1 および表 1-2 を参照)。

```
unix# openssl pkcs12 -export -in client.crt -inkey client.key -out client.p12 -descert
```

3DES を使用して暗号化

Enter Export Password: ←エクスポート用のパスワードを入力します。

Verifying - Enter Export Password: ←エクスポート用のパスワードを再度入力します。



## 2.3 クライアント証明書・鍵の登録

### 2.3.1 クライアント証明書と鍵の登録

(1) 準備した証明書類を媒体 (MC), ftp または sftp など装置に転送します。本装置がサポートする証明書フォーマットは以下の通りです。

表 2-2 本装置がサポートする証明書フォーマット

証明書種別	証明書フォーマット	説明	証明書ファイル名の例
switch	PKCS#12	PKCS#12 ファイルは証明書と秘密鍵を含みます。 拡張子は「.p12」です。	switchcert.p12
controller	PKCS#12 または pem	PKCS#12 フォーマットか pem フォーマットのどちらでも指定することができます。 PKCS#12 ファイルは証明書と秘密鍵を含みますが、証明書だけが抽出されます。 拡張子は「.p12」です。 pem ファイルは証明書のみを含みます。 拡張子は「.pem」です。認証局の証明書かルート証明書のどちらでも指定することができます。	ctrlcert.p12

(2) set openflow certificate コマンド（「4. 運用コマンドレファレンス」参照）で証明書類を登録します。

なお、証明書類の登録後、元ファイルはセキュリティの観点より削除するようにしてください。

### 2.3.2 クライアント証明書と鍵の削除

(1) 登録済みの証明書類は、erase openflow certificate コマンドで削除することができます。

## 2.4 OpenFlow 機能 Secure Channel の TLS 接続設定

OpenFlow 機能のコンフィグレーションコマンドにて TLS 接続の設定をします。

OpenFlow スイッチインスタンスを作成した後、`controller` コマンドによる接続 OFC の設定を TLS 接続モードで行い、「2.3.1 クライアント証明書と鍵の登録」で登録した証明書類を指定します。

以下に設定例を示します。

### [ 設定例 ]

1. 装置に転送済みの証明書類を登録します。

```
# set openflow certificate switch switchcert.pl2 1
# set openflow certificate controller ctrlcert.pl2 64
```

2. コンフィグレーションコマンドにて OpenFlow スイッチインスタンスを作成し、TLS 接続を行う OFC および、登録した証明書の ID を指定します。

```
# configure
(config)# openflow openflow-id 1 real-switch
!(config-of)# controller controller-name cont1 1 192.168.132.1 tls
switch-id 1 controller-id 64
```

スイッチの  
証明書の ID

コントローラの  
証明書の ID

```
!(config-of)# openflow-interface gigabitethernet 0/1-4
!(config-of)# enable
!(config-of)# save
(config-of)# end
#
```

※ PF5200 シリーズでは、16 の OpenFlow スイッチインスタンスに対してそれぞれ 4 つの OFC を指定できます。スイッチの証明書の ID(1 ~ 16) およびコントローラの証明書の ID(1 ~ 64) に対応する証明書類を登録することで、各 OpenFlow スイッチインスタンスに指定したそれぞれの OFC への接続設定に対して、別々の証明書類を指定することが可能となります。

※登録した証明書類の情報は、`show openflow certificate` コマンドで確認することができます。

# 3

## コンフィグレーションコマンドレ ファレンス

---

controller

---

# controller

---

接続先 OpenFlow コントローラを指定します。

## [入力形式]

情報の設定・変更

```
controller controller-name <controller name> <priority> <ipv4 address>
[port <port no>] [{tcp|tls switch-id <id> controller-id <id>}]
```

情報の削除

```
no controller controller-name <controller name>
```

## [入力モード]

(config-of)

## [パラメータ]

**controller-name <controller name>**

Secure Channel の接続を行うコントローラの名前を指定します。

同一 OpenFlow ID では、同じ値を設定できません。

1. 本パラメータ省略時の初期値

省略できません。

2. 値の設定範囲

Secure Channel の接続を行うコントローラの名前を指定します。

指定できるパラメータは 16 文字以内の文字列とし、「半角英数字」「-」「\_」「.」以外の文字を含めないようにしてください。

**<priority>**

Secure Channel の接続を行うコントローラに優先順位を設定します。

値の大きい方が高優先となります。

同一 OpenFlow ID では、同じ値を設定できません。

1. 本パラメータ省略時の初期値

省略できません。

2. 値の設定範囲

1 ~ 255

**<ipv4 address>**

Secure Channel の接続を行うコントローラの IPv4 アドレスをドット記法で指定します。

1. 本パラメータ省略時の初期値

省略できません。

2. 値の設定範囲

IPv4 アドレスをドット表記で記載します。

**port <port>**

Secure Channel の接続を行うコントローラの TCP ポート番号を指定します。

1. 本パラメータ省略時の初期値

接続ポート番号として、6633 を使用します。

## 2. 値の設定範囲

1 ～ 65535

[{tcp|tls switch-id <id> controller-id <id>}]

Secure Channel の接続を行う際、暗号化の有無を選択します。

### 1. 本パラメータ省略時の初期値

tcp を選択します。

### 2. 値の選択

tcp

コントローラとの間の Secure Channel を TCP 非暗号化にて接続します。

tls switch-id <id> controller-id <id>

コントローラとの間の Secure Channel を TCP 暗号化にて接続します。

switch-id <id>

スイッチ本体の証明書の id を指定します。

### 1. 本パラメータ省略時の初期値

省略できません。

### 2. 値の設定範囲

1 ～ 16

controller-id <id>

コントローラ本体の証明書の id を指定します。

### 1. 本パラメータ省略時の初期値

省略できません。

### 2. 値の設定範囲

1 ～ 64

## [コマンド省略時の動作]

なし

## [通信への影響]

1. 本コマンドを設定していない場合は、Secure Channel の接続を行いません。
2. OpenFlow スイッチインスタンスが有効時に、使用中のコントローラと異なる IP アドレスまたは TCP ポート番号を設定した場合は、Secure Channel を切断します。
3. 削除設定の場合は、Secure Channel を切断します。
4. 同一の OpenFlow スイッチインスタンス内に有効なコントローラの設定が複数存在する場合は、最も優先順位の高いコントローラへ再接続を行います。
5. tls 指定時は、証明書 id の設定がない場合でも設定は可能です。

ただし、tls にて指定されているコントローラに対する接続は行わず、syslog メッセージでコンフィグレーション不足を示すエラーメッセージを表示します。エラーメッセージ表示後は、TCP 接続時のエラーと同様、次コントローラの設定が存在する場合はそちらへの接続を行います。

## [設定値の反映契機]

設定値変更後、すぐに運用に反映されます。

### [注意事項]

1. 同一 OpenFlow スイッチインスタンスに対して設定できるコントローラは最大 4 つです。
2. コントローラを複数設定する場合、同じ <controller name> の設定は不可となります。
3. コントローラを複数設定する場合、同じ <priority> の設定は不可となります。
4. コントローラを複数設定する場合、同じ <ipv4 address> かつ port<port no> の設定は不可となります。
5. コントローラを複数設定する場合、TCP/TLS 混在は許容します。

### [関連コマンド]

なし

# 4

## 運用コマンドレファレンス

---

set openflow certificate

---

erase openflow certificate

---

show openflow certificate

---

show openflow

---

show openflow statistics

---

# set openflow certificate

OpenFlow 機能における Secure Channel の TLS 接続に使用する証明書の登録を行います。

証明書のファイルの有効期限チェックは行いません。

## [入力形式]

```
set openflow certificate {switch | controller} <file name> <id>
[keep-controller-session]
```

## [入力モード]

装置管理者モード

## [パラメータ]

{switch | controller}

登録を行う証明書の種別を指定します。

switch : スイッチの証明書

controller : コントローラの証明書

<file name>

登録を行う証明書のファイル名を指定します。

表 4-1 ファイル名説明

証明書種別	証明書フォーマット	説明	証明書ファイル名の例
switch	PKCS#12*1	ファイル指定にはパスを含むこともでき、 相対パス絶対パス共に使用できます。 パスの指定がない場合、カレントディレクトリのファイルが指定されます。 ファイル名称は、拡張子を含み 16 文字以内とし、「半角英数字」「-」「_」「.」以外の文字は使用できません。 パスワード確認メッセージが表示されるので、パスワードを入力します。パスワード確認後ファイルの登録が行われます。	switchcert.p12
controller	PKCS#12*1 または pem*2	ファイル指定にはパスを含むこともでき、 相対パス絶対パス共に使用できます。 パスの指定がない場合、カレントディレクトリのファイルが指定されます。 ファイル名称は、拡張子を含み 16 文字以内とし、「半角英数字」「-」「_」「.」以外の文字は使用できません。 ファイルは PKCS#12 フォーマットか pem フォーマットのどちらでも指定することができます。 PKCS#12 ファイルは証明書だけが抽出されます。 pem ファイルは認証局の証明書かルート証明書のどちらでも指定することができます。	ctrlcert.p12

\*1 PKCS#12 フォーマット : 証明書と秘密鍵を含みます。拡張子は「.p12」です。

\*2 pem フォーマット : 証明書のみです。拡張子は「.pem」です。



<id>

証明書ファイルの管理番号を指定します。

登録を行う証明書の種別が **switch** だった場合、管理番号で指定できる範囲は 1～16 です。

登録を行う証明書の種別が **controller** だった場合、管理番号で指定できる範囲は 1～64 です。

この ID は OpenFlow コンフィグレーションの設定時に、各 OpenFlow スイッチインスタンスに対して別々の証明書を利用するために用います。

#### Keep-controller-session

証明書をコネクション切断せずに更新します。

### [実行例]

図 4-1 証明書ファイルの登録例

```
# set openflow certificate switch switchcert.p12 1 [Enter] キー押下
Importing certificate...
Enter Import Password: <パスワード入力>
Importing private key...
Enter Import Password: <パスワード入力>
```

### [表示説明]

なし

### [通信への影響]

なし

### [応答メッセージ]

表 4-2 コマンドの応答メッセージ一覧

メッセージ	内容
Can't execute.	コマンドを実行できません。再実行してください。
Timeout occurred due to busy OpenFlow daemon.	コマンドの応答タイムアウトです。
Connection failed to OpenFlow daemon.	CONNECTION エラーが発生しました。

### [注意事項]

なし

# erase openflow certificate

---

OpenFlow 機能における Secure Channel の TLS 接続に使用する証明書の削除を行います。

## [入力形式]

```
erase openflow certificate {{switch|controller} [<id>]}  
[keep-controller-session] [-f]
```

## [入力モード]

装置管理者モード

## [パラメータ]

{switch | controller}

削除を行う証明書の種別を指定します。

switch : スイッチの証明書

controller : コントローラの証明書

<id>

登録の際に設定した証明書の ID を指定します。

削除の種別で switch を指定した場合、指定可能範囲は 1 ~ 16 です。

削除の種別で controller を指定した場合、指定可能範囲は 1 ~ 64 です。

Keep-controller-session

証明書の削除を、コネクションを切断せずに行います。

-f

証明書削除確認メッセージを出力せず、証明書の削除を行います。

## [実行例]

### 図 4-2 証明書ファイルの削除例

```
# erase openflow certificate switch 1 [Enter]キー押下  
remove certificates? (y/n): y [Enter]キー押下
```

## [表示説明]

なし

## [通信への影響]

なし

## [応答メッセージ]

表 4-3 コマンドの応答メッセージ一覧

メッセージ	内容
Can't execute.	コマンドを実行できません。再実行してください。
Timeout occurred due to busy OpenFlow daemon.	コマンドの応答タイムアウトです。
Connection failed to OpenFlow daemon.	CONNECTION エラーが発生しました。

## [注意事項]

なし

## show openflow certificate

---

登録されている証明書を表示します。

### [入力形式]

```
show openflow certificate [{switch | controller} [< id>]]
```

### [入力モード]

装置管理者モード

### [パラメータ]

{switch | controller}

参照を行う証明書の種別を指定します。

switch : スイッチの証明書

controller : コントローラの証明書

<id>

登録の際に設定した証明書の ID を指定します。

証明書の種別で switch を指定した場合、指定可能範囲は 1 ~ 16 です。

証明書の種別で controller を指定した場合、指定可能範囲は 1 ~ 64 です。

すべてのパラメータ省略時の動作

すべての証明書の内容を表示します。

## [実行例]

図 4-3 証明書ファイルの参照例

```
# show openflow certificate switch 1 [Enter]キー押下
Date 2010/12/01 15:30:00 UTC

[switch]
[certificate 1]
Subject:
    Country: JP
    State/Province: Tokyo
    Organization: NEC Corporation
    OrganizationalUnit: Admin
    CommonName: PFS1
    EmailAddress: sample@sample_switch.com
Validity
    Not Before: May 24 12:02:37 2006
    Not After  : May 23 12:02:37 2009

# show openflow certificate controller 1 [Enter]キー押下
Date 2010/12/01 15:30:00 UTC
[controller ]
[certificate 1]
Subject:
    Country: JP
    State/Province: Tokyo
    Organization: Private_CA
    OrganizationalUnit: Admin
    CommonName: Private_CA
    EmailAddress: server@sample_server.com
Validity : ** invalid! **
    Not Before: May 24 12:02:37 2006
    Not After  : May 23 12:02:37 2009
```

## [表示説明]

表 4-4 証明書の表示内容

表示項目	意味	表示詳細情報
Subject:	証明される対象情報	Country : 国
		State/Province : 都道府県
		Organization : 組織
		OrganizationalUnit : 組織単位
		CommonName : 組織・サーバ名
		EmailAddress : 管理者メールアドレス
Validity	証明書有効期限	Not Before : 開始日時
		Not After : 終了日時
		証明書が期限外（期限切れ or 未来）の場合 「** invalid! **」を表示します。

## [通信への影響]

なし

## [応答メッセージ]

表 4-5 コマンドの応答メッセージ一覧

メッセージ	内容
The specified certificate doesn't exist.	指定された証明書は存在しません。
Can't execute.	コマンドを実行できません。再実行してください。
Timeout occurred due to busy OpenFlow daemon.	コマンドの応答タイムアウトです。
Connection failed to OpenFlow daemon.	CONNECTION エラーが発生しました。

## [注意事項]

なし

# show openflow

---

OpenFlow 情報を表示します。

## [入力形式]

```
show openflow [openflow-id <openflow id>] [detail]
```

## [入力モード]

一般ユーザモードおよび装置管理者モード

## [パラメータ]

openflow-id <openflow id> ※ VSI 使用時のみ指定可能

指定した OpenFlow ID の情報を表示します。指定できる範囲は、1 ～ 16 です。

detail

OpenFlow の詳細な情報を表示します。

すべてのパラメータ省略時の動作

すべての OpenFlow ID のサマリ情報を表示します。

## [実行例]

図 4-4 OpenFlow サマリ情報 (RSI) の表示例

```
> show openflow [Enter]キー押下
```

```
Date 2010/12/01 15:30:00 UTC
```

```
Switch Protocol Version : 0x01
```

```
Flow Detection Mode      : openflow-1
```

```
[OpenFlow 1 Real]
```

```
OpenFlow Software State   : enable
```

```
      :                               :
```

```
      :      (中略)                :
```

```
      :                               :
```

```
Controllers :
```

```
#1 : Cntl1 192.168.0.254 (port 6633, pri 1, ver 0x01) is connected
```

```
connection method          : TLS
```

```
session connect time 0day 0:01:15
```

```
session reset time 2011/09/01 13:28:45 JST
```

```
connect retry count        : 1
```

```
connect retry timer(max/current) : 1 sec/ 0 sec
```

```
deterrence level           : 0
```

```
band limit for paket-in     : unlimited
```

```
asynchronous message :
```

```
NONE
```

```
      :                               :
```

```
      :      (省略)                :
```

```
      :                               :
```



## [表示説明]

下記以外の OpenFlow サマリ情報 (RSI) の表示内容については、「運用コマンドレファレンス Vol.1 25 OpenFlow 機能」の「show openflow」を参照してください。

表 4-6 OpenFlow サマリ情報 (RSI) の表示内容

表示項目	詳細情報	意味
Controllers	コントローラ構成	設定されているコントローラ構成を表示します。コントローラの情報は、コントローラ名、IP アドレス (L4 ポート番号、優先度、コントローラにおける OpenFlow Protocol バージョン) で表現されます。 controller name : 16 文字 IP アドレス : 0.0.0.0 ~ 255.255.255.255 ポート番号 : 1 ~ 65535 優先度 : 1 ~ 255 バージョン : Spec v1.0 では、"0x01" #1 ~ #4 : コントローラの設定順序 is disconnected : 未接続 is connected : 接続 is version-mismatched : バージョン不一致
connection method	接続種別	コントローラとの接続種別を表示します。 TCP TLS

## [通信への影響]

なし

## [応答メッセージ]

表 4-7 コマンドの応答メッセージ一覧

メッセージ	内容
OpenFlow is not configured.	OpenFlow が設定されていません。 コンフィグレーションを確認してください。
Specified OpenFlow ID is not configured : <openflow id>.	指定 OpenFlow ID は設定されていません。 <openflow id> : OpenFlow ID
Can't execute.	コマンドを実行できません。再実行してください。
Timeout occurred due to busy OpenFlow daemon.	コマンドの応答タイムアウトです。
Connection failed to OpenFlow daemon.	CONNECTION エラーが発生しました。

## [注意事項]

なし

## show openflow statistics

---

OpenFlow Controller との通信に関する統計情報を表示します。

### [入力形式]

```
show openflow statistics [openflow-id <openflow id>]
```

### [入力モード]

一般ユーザモードおよび装置管理者モード

### [パラメータ]

openflow-id <openflow id>

指定した OpenFlow ID の情報を表示します。

指定できる範囲は、1 ～ 16 です。

すべてのパラメータ省略時の動作

すべての OpenFlow ID について、統計情報を表示します。

### [実行例]

図 4-5 統計情報の表示例

```
> show openflow statistics [Enter] キー押下
```

```
Date 2010/12/01 15:30:00 UTC
```

```
[OpenFlow 1]
```

```
<Discard counter>
```

```
Packet In 4294967295
```

```
#1 : openflow-1 129.168.0.254 (port 6633, priority 10) is connected
```

```
<Sent messages counter>
```

```
Hello 4294967295
```

```
Echo Request 4294967295
```

```
:
```

```
: (中略)
```

```
:
```

```
<Received messages counter>
```

```
Hello 4294967295
```

```
Echo Request 4294967295
```

```
<Secure Channel Disconnected counter>
```

```
Secure Channel 4294967295
```

```
TCP Session 4294967295
```

```
TLS Session 4294967295
```

```
>
```

[表示説明]

下記以外の統計情報表示項目については、「運用コマンドレファレンス Vol.1 25 OpenFlow 機能」の「show openflow statistics」を参照してください。

表 4-8 統計情報表示項目

表示項目	意味	表示詳細情報
<Secure Channel Disconnected counter>	Secure Channel 関連のエラー回数	-
TLS Session	TLS Session 接続失敗回数	0 ～ 4294967295

[通信への影響]

なし

[応答メッセージ]

表 4-9 コマンドの応答メッセージ一覧

メッセージ	内容
OpenFlow is not configured.	OpenFlow が設定されていません。 コンフィグレーションを確認してください。
Specified OpenFlow ID is not configured : <openflow id>.	指定 OpenFlow ID は設定されていません。 <openflow id> : OpenFlow ID
Can't execute.	コマンドを実行できません。再実行してください。
Timeout occurred due to busy OpenFlow daemon.	コマンドの応答タイムアウトです。
Connection failed to OpenFlow daemon.	CONNECTION エラーが発生しました。

[注意事項]

なし



# 5

## メッセージログレファレンス

---

メッセージログレファレンス

---

# メッセージログレファレンス

OpenFlow 機能の運用中に障害等が発生した場合、以下のログを出力します。

表 5-1 ログメッセージ一覧

項番	イベントレベル	イベント発生部位	メッセージ識別子	付加情報上位 4 桁	メッセージテキスト
内容					
1	E4	SOFTWARE	2f100003	1001	Secure Channel <openflow id> <controller name> <ipv4 address> is not connected : <error string>.
<p>Secure Channel の接続が出来ませんでした。</p> <p>[ メッセージテキストの表示説明 ]</p> <p>&lt;openflow id&gt; OFS の識別子</p> <p>&lt;controller name&gt; Secure Channel 接続対象のコントローラ名称</p> <p>&lt;ipv4 address&gt; 接続先コントローラの IPv4 アドレス</p> <p>&lt;error string&gt;</p> <ul style="list-style-type: none"> <li>• Cannot connect TCP session : TCP セッションが接続できない</li> <li>• Cannot connect TLS session : TLS セッションが接続できない</li> <li>• No notify of Hello : Hello が通知されない</li> <li>• Version negotiation failure : Version 不一致</li> <li>• Permission error : パーミッションエラーが発生した</li> <li>• Private key file error : 秘密鍵ファイルエラー</li> <li>• Certificate file error : 自装置証明書ファイルエラー</li> <li>• CA file error : CA 証明書ファイルエラー</li> </ul> <p>[ 対応 ]</p> <p>本装置とコントローラ間でネットワーク的に導通できるか確認してください。</p>					
2	E4	SOFTWARE	2f100004	1001	Secure Channel <openflow id> <controller name> <ipv4 address> is disconnected : <error string>.
<p>Secure Channel との切断が発生しました。</p> <p>[ メッセージテキストの表示説明 ]</p> <p>&lt;openflow id&gt; OFS の識別子</p> <p>&lt;controller name&gt; Secure Channel 接続対象のコントローラ名称</p> <p>&lt;ipv4 address&gt; 接続先コントローラの IPv4 アドレス</p> <p>&lt;error string&gt;</p> <ul style="list-style-type: none"> <li>• Connectivity to controller is lost : コントローラへの接続性が失われた</li> <li>• TCP session is disconnected : TCP セッションが切断された</li> <li>• TLS session is disconnected : TLS セッションが切断された</li> <li>• Receipt of bad version error : コントローラからバージョンエラーを受信した</li> </ul> <p>[ 対応 ]</p> <p>本装置とコントローラ間でネットワーク的に導通できるか確認してください。</p> <p>バージョンのエラーの場合は、スイッチあるいはコントローラがサポートする OpenFlow バージョンを確認してください。</p>					

# 6

## トラブルシューティング

---

トラブルシューティング

---

# トラブルシューティング

TLS 通信用クライアント証明書と秘密鍵の運用に関する障害対応発生時は、次の表に示す障害解析に従って原因の切り分けを行ってください。

表 6-1 障害対応発生時の障害解析

項番	発生事象	確認内容・コマンド	対応方法
1	openssl コマンドで作成したクライアント証明書と秘密鍵を用いて登録したが、Secure Channel 接続が行えない	openssl の作成手順で操作抜け、あるいは、設定情報の間違いがないかを確認してください。	・本書に記載しています操作手順通りの操作かを確認してください。
2	openssl コマンドで本書に書かれているパラメータが指定できない	openssl version コマンドで OpenSSL のバージョンを確認してください。	・ OpenSSL 0.9.7i 以降のバージョンを使用してください。



# 付録

---

付録 A 謝辞 (Acknowledgments)

---

---

## 付録 A 謝辞 (Acknowledgments)

### LICENSE ISSUES

=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

### OpenSSL License

-----

```
/* =====
 * Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in
 * the documentation and/or other materials provided with the
 * distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 * software must display the following acknowledgment:
 * "This product includes software developed by the OpenSSL Project
 * for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 * endorse or promote products derived from this software without
 * prior written permission. For written permission, please contact
 * openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 * nor may "OpenSSL" appear in their names without prior written
 * permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 * acknowledgment:
 * "This product includes software developed by the OpenSSL Project
 * for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
```

\* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY  
 \* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE  
 \* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR  
 \* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR  
 \* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,  
 \* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT  
 \* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;  
 \* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)  
 \* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,  
 \* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)  
 \* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED  
 \* OF THE POSSIBILITY OF SUCH DAMAGE.

\* =====

\*

\* This product includes cryptographic software written by Eric Young  
 \* (eay@cryptsoft.com). This product includes software written by Tim  
 \* Hudson (tjh@cryptsoft.com).

\*

\*/

Original SSLeay License

-----

/\* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

\* All rights reserved.

\*

\* This package is an SSL implementation written

\* by Eric Young (eay@cryptsoft.com).

\* The implementation was written so as to conform with Netscapes SSL.

\*

\* This library is free for commercial and non-commercial use as long as

\* the following conditions are aheared to. The following conditions

\* apply to all code found in this distribution, be it the RC4, RSA,

\* lhash, DES, etc., code; not just the SSL code. The SSL documentation

\* included with this distribution is covered by the same copyright terms

\* except that the holder is Tim Hudson (tjh@cryptsoft.com).

\*

\* Copyright remains Eric Young's, and as such any Copyright notices in

\* the code are not to be removed.

\* If this package is used in a product, Eric Young should be given attribution

\* as the author of the parts of the library used.

\* This can be in the form of a textual message at program startup or

\* in documentation (online or textual) provided with the package.

\*

\* Redistribution and use in source and binary forms, with or without

\* modification, are permitted provided that the following conditions

\* are met:

\* 1. Redistributions of source code must retain the copyright

\* notice, this list of conditions and the following disclaimer.

\* 2. Redistributions in binary form must reproduce the above copyright

- \* notice, this list of conditions and the following disclaimer in the
- \* documentation and/or other materials provided with the distribution.
- \* 3. All advertising materials mentioning features or use of this software
- \* must display the following acknowledgement:
- \* "This product includes cryptographic software written by
- \* Eric Young (eay@cryptsoft.com)"
- \* The word 'cryptographic' can be left out if the routines from the library
- \* being used are not cryptographic related :-).
- \* 4. If you include any Windows specific code (or a derivative thereof) from
- \* the apps directory (application code) you must include an acknowledgement:
- \* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
- \*
- \* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND
- \* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
- \* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
- PURPOSE
- \* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
- \* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
- CONSEQUENTIAL
- \* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
- GOODS
- \* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
- \* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
- STRICT
- \* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
- \* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
- \* SUCH DAMAGE.
- \*
- \* The licence and distribution terms for any publically available version or
- \* derivative of this code cannot be changed. i.e. this code cannot simply be
- \* copied and put under another distribution licence
- \* [including the GNU Public Licence.]
- \*/