SEIKO

機能解説書
Function Reference Manual

SX-3945-ZT

第 3 版

2023 年 3 月

U00144561302

セイコーソリューションズ株式会社

本　書　の　使　い　方

・本書は全銀広域 IP 網接続の暗号化方式 TLS に対応した製品、SX-3945-ZT の機能解説書です。
本製品にインストールするサーバー証明書・秘密鍵、クライアント証明書・秘密鍵、CA 証明書などはご用意ください。
本製品の設定は WUI/CLI を使用してお客様にてセットアップができます。

・本書の読者は、SSL/TLS、全銀 TCP／IP プロトコル、ネットワークについて基本的な知識を必要とします。

－目　次－

「空白」

第１章　概要

本章は、SX-3945-ZT の概要を記述しています。

１．１　特徴

１．１．１　全銀 TCP/IP 環境から全銀 TLS 対応へのスムーズな移行

SX-3945-ZT は、全銀 TCP/IP の伝送を TLS 伝送に変換するアクセラレータです。
全銀 TCP/IP のサーバー環境に本機を設置することで、全銀 TLS に対応した機器との伝送を可能にします。
全銀固有の接続方法であるサーバー起動は、TLS クライアントとして TLS 暗号化処理を行い、相手起動時は TLS サーバーとして TLS 処理を行い全銀 TCP/IP サーバーと伝送します。

１．１．２　冗長化構成

本製品を２台で使用し、VRRP を利用したマスター、バックアップの冗長構成で使用することが可能です。
また、設定情報の同期機能をサポートしています。

１．１．３　証明書有効期限チェック

サーバー証明書・クライアント証明書の有効期限をチェックして syslog 転送します。

１．１．４　TLS 処理基板

ハードを使用した TLS 処理を行っていますので、同時接続が発生してもストレスなく処理が行えます。

１．２　構成例

SX-3945-ZT は、既に全銀 TCP/IP 接続で使用しているサーバー環境に設置することで全銀 TLS に対応した機器と接続ができます。

図　１．１　システム構成(ブリッジ型接続)

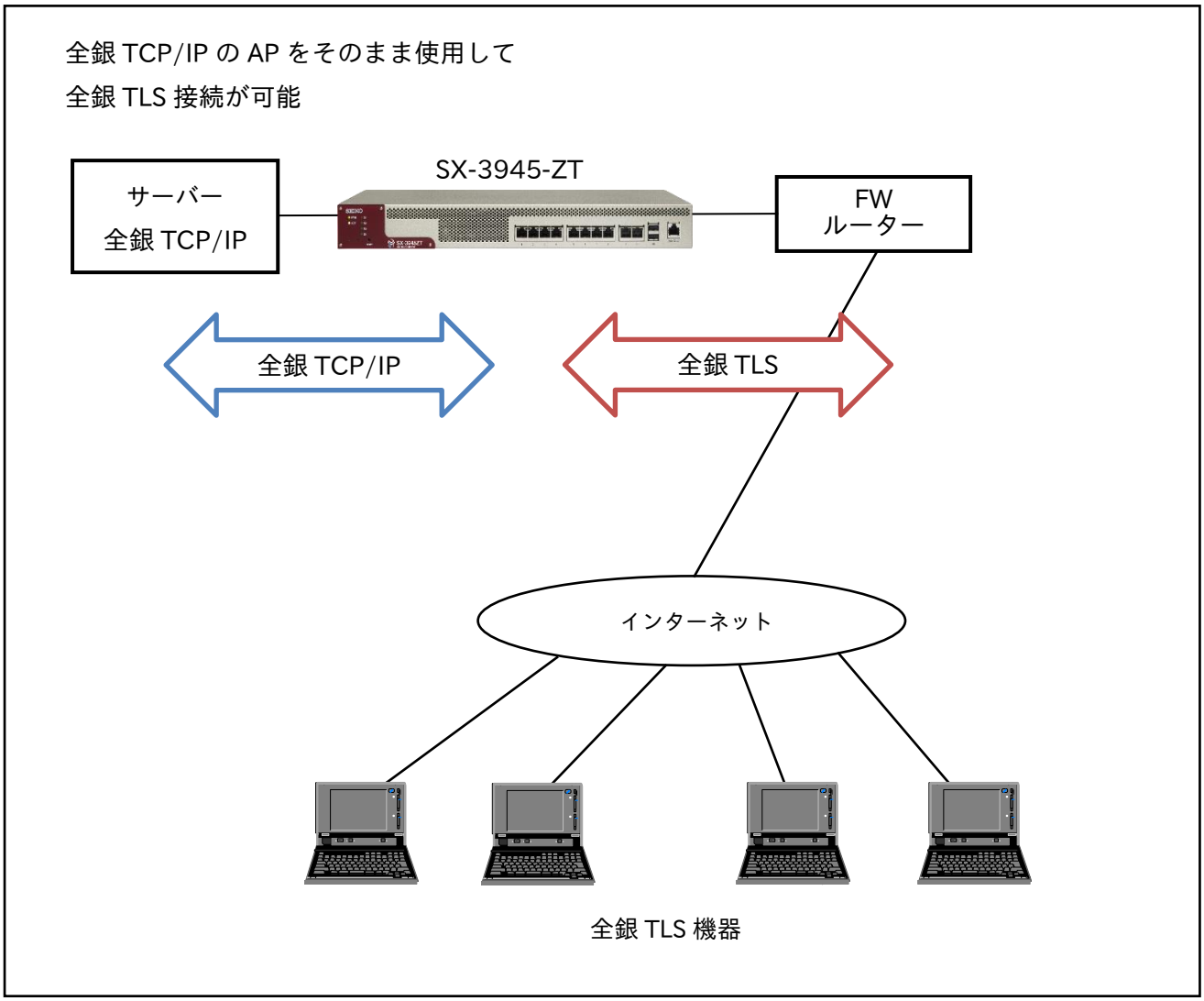
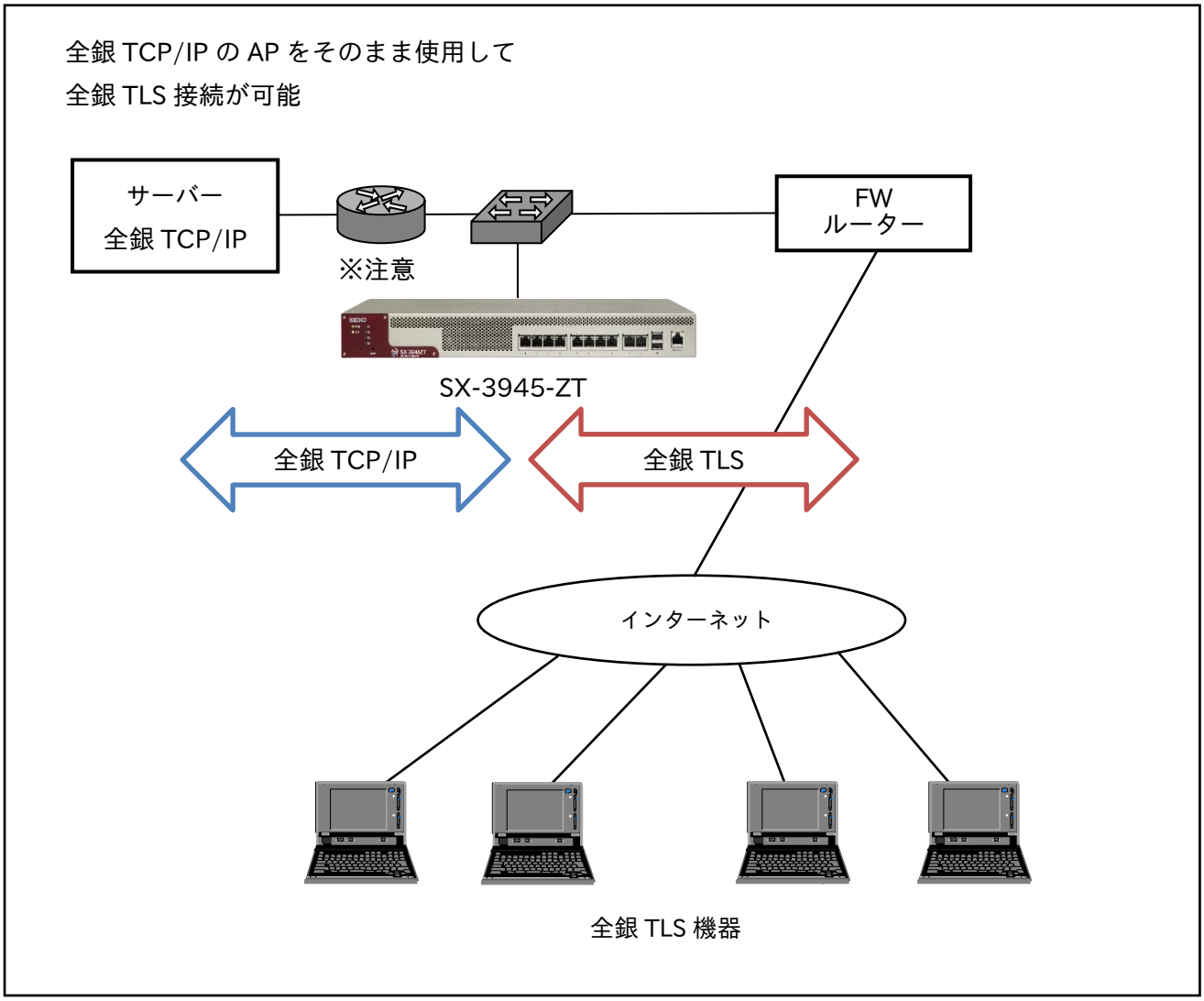


図　1．2　システム構成(ワンアーム型接続)

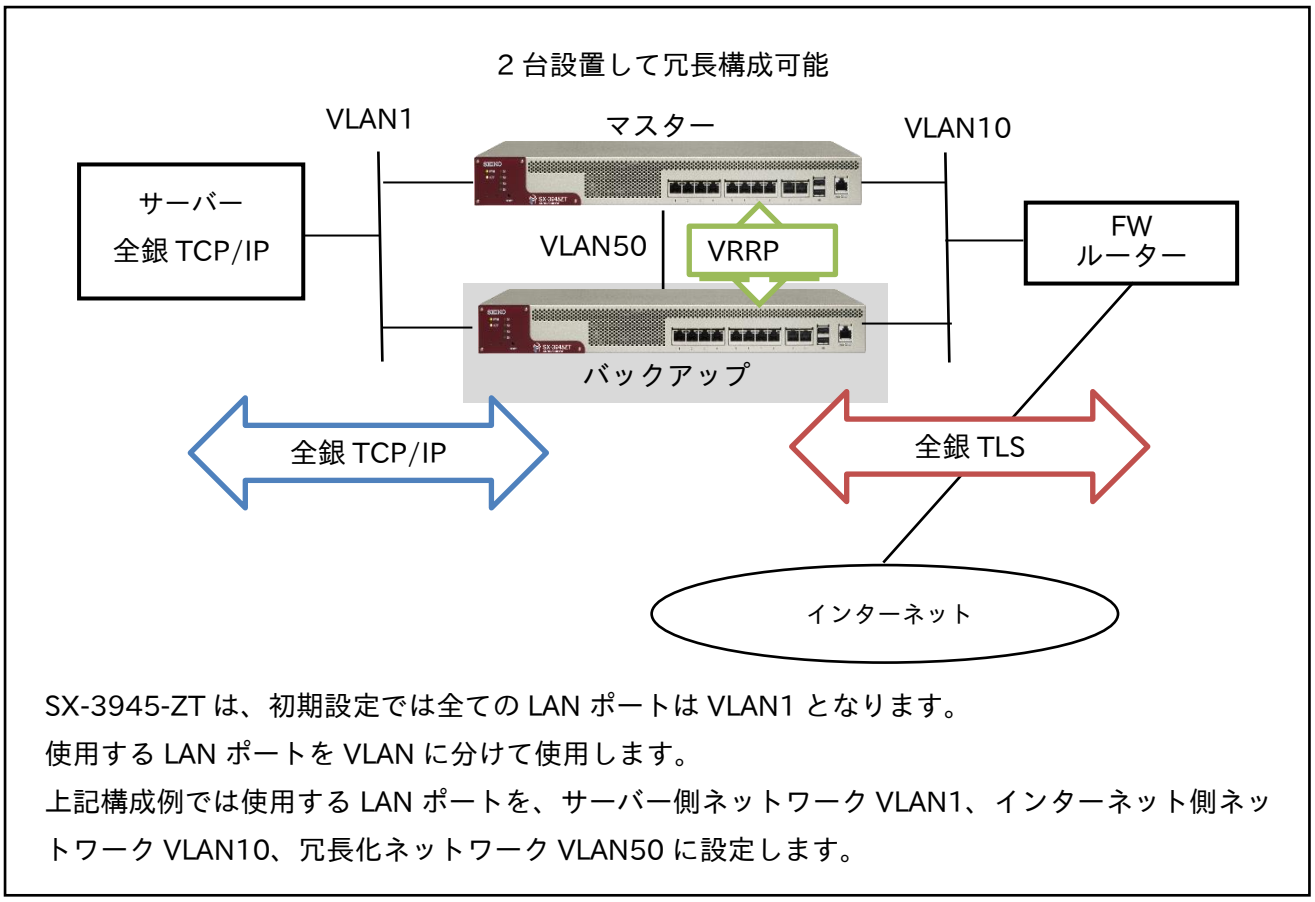


注意

ワンアーム構成で、クライアントモードを使用する場合、全銀 TCP/IP クライアントからのアクセスが本製品向けになるように、Gateway 設定が必要です。
全銀 TCP/IP クライアントと本製品は同一ネットワークで使用するようにしてください。
異なるネットワークで使用する場合、ルーターで宛先 IP アドレス(またはポート番号)で本製品を通過するようにしてください。

下記ブリッジ型、冗長構成可能です。

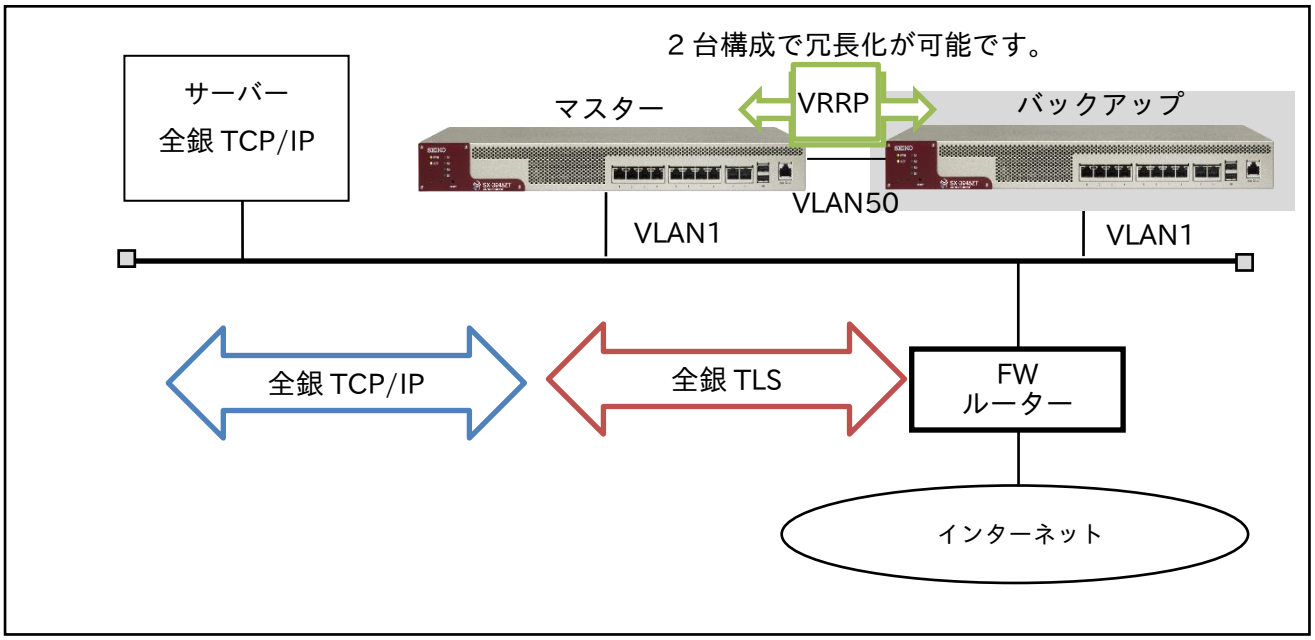
図　１．２　ブリッジ型構成例（冗長）



SX-3945-ZT は、初期設定では全ての LAN ポートは VLAN1 となります。
使用する LAN ポートを VLAN に分けて使用します。
上記構成例では使用する LAN ポートを、サーバー側ネットワーク VLAN1、インターネット側ネットワーク VLAN10、冗長化ネットワーク VLAN50 に設定します。

下記ワンアーム型、冗長構成可能です。

図　１．３　ワンアーム型構成例（冗長）



１．３　基本機能

（１）プロトコル変換機能

SX-3945-ZT は、全銀 TCP/IP 手順を持つサーバーと、全銀 TLS に対応した端末と伝送できるように TLS 処理を行います。

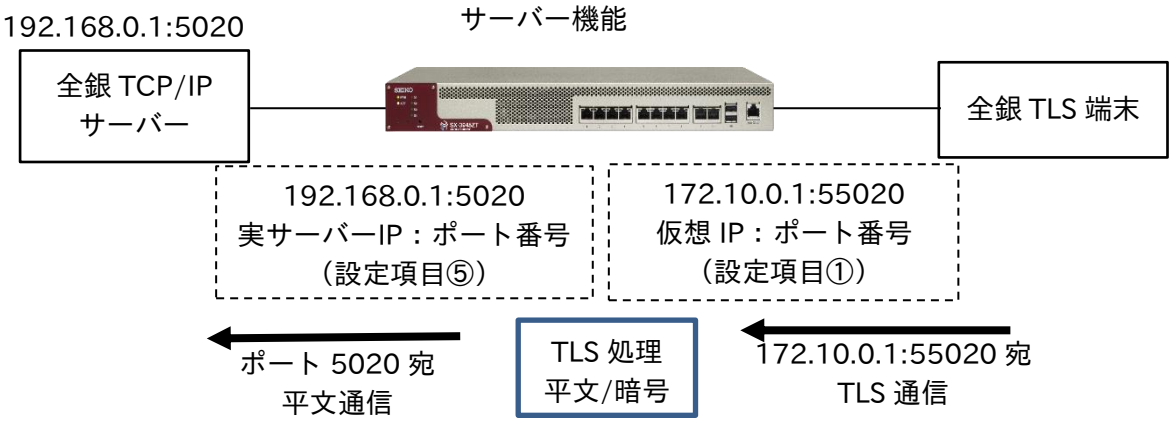
全銀 TCP/IP サーバーから起動する場合は、TLS クライアント機能で動作し、全銀 TLS 端末起動時は TLS サーバー機能で動作します。

（２）全銀 TLS サーバー機能

全銀 TLS 端末から起動する場合、本装置の TLS サーバー機能で動作します。

TLS サーバー機能は、TLS 処理を行う仮想サーバー情報として、IP アドレスとポート番号を設定し、該当するアクセスの場合は TLS アクセラレートして、全銀 TCP/IP サーバーへは平文で伝送します。

TLS サーバー機能時は、アクセス元を認証するために、クライアント認証することもできます。

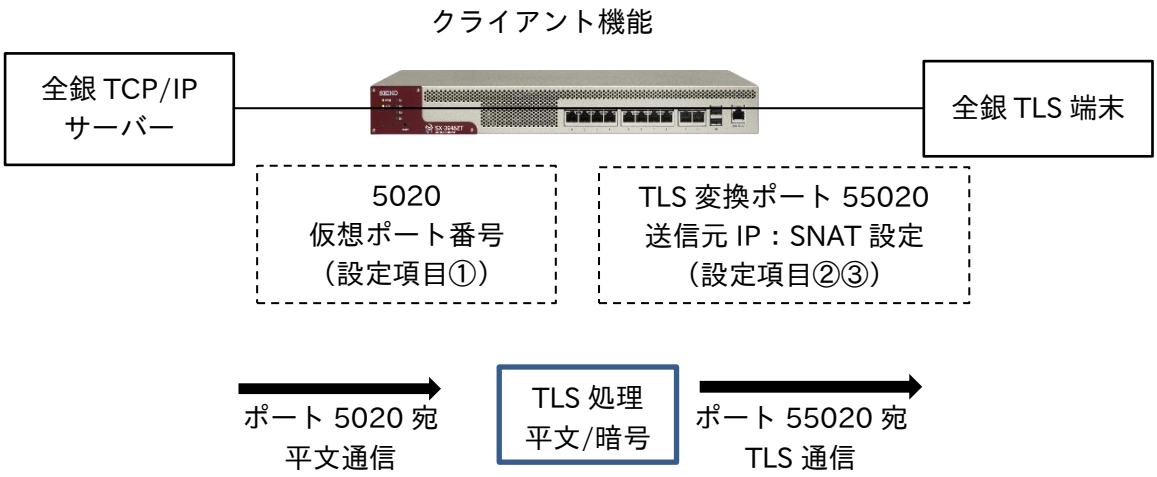


	設定項目	設定内容
1	仮想サーバーIP アドレス：ポート番号	端末が接続する IP アドレス：ポート番号
2	サーバー証明書	お客様で取得したサーバー証明書、中間証明書、秘密鍵をインストールします。
3	サーバー中間証明書	
4	秘密鍵	
5	実サーバーIP アドレス：ポート番号	全銀 TCP/IP サーバーの設定
6	クライアント認証	する/しない
6-1	・クライアント認証する場合	クライアント証明書を発行したルート CA 証明書をインストール
7	クライアント証明書失効確認	OCSP/CRL/失効確認しない
7-1	・OCSP で行う	合わせて DNS 設定、時刻同期設定が必要
7-2	・クライアントからの失効リスト(AIA)情報無	異常/失効確認しない
7-3	・CRL 設定	CRL 記述すれば CRL となる。

は必須設定項目（中間証明書は不要の場合あり）

（３）全銀 TLS クライアント機能

全銀 TCP/IP サーバーから起動する場合、TLS クライアント機能で動作します。
全銀 TLS クライアント機能は、TLS 化する宛先ポート番号を設定することで、該当する宛先ポート番号を TLS 化します。宛先の IP アドレスは TLS 化に影響はしません。
全銀 TCP/IP サーバーからの該当する宛先ポート番号のアクセスを、TLS に変換して伝送します。



	設定項目	設定内容
1	仮想クライアントポート番号	TLS クライアントで動作するポート番号
2	TLS 変換後のポート番号	TLS 動作時の宛先ポート番号
3	起動元 IP アドレス(SNAT)変更	する。(仮想サーバーIP アドレス)
3-1	・SNAT する	発の IP アドレスを設定(仮想サーバーIP アドレス)
4	相手サーバーのルート CA 証明書	接続するサーバー全てのルート CA 証明書
5	相手サーバーの中間 CA 証明書	接続するサーバー全ての中間 CA 証明書
6	クライアント認証	する/しない
6-1	・使用するクライアント証明書を選択	IP アドレス設定/サーバーからの要求
7	サーバー証明書失効確認	OCSP/失効確認しない
7-1	OCSP で行う	合わせて DNS 設定、時刻同期設定が必要
7-2	・サーバーからの失効リスト(AIA)情報無	異常/失効確認しない

は必須設定項目

（４）証明書有効期限チェック

SX-3945-ZT にインストールしているサーバー証明書/クライアント証明書の有効期限をチェックし、有効期限が近づくと syslog で通知します。

（５）クライアント証明書自動更新

SFTP サーバーと連携してクライアント証明書の自動更新ができます。

この機能を使用するためには、SFTP サーバーにクライアント証明書を置き、適切に更新してサーバーに置く必要が有ります。

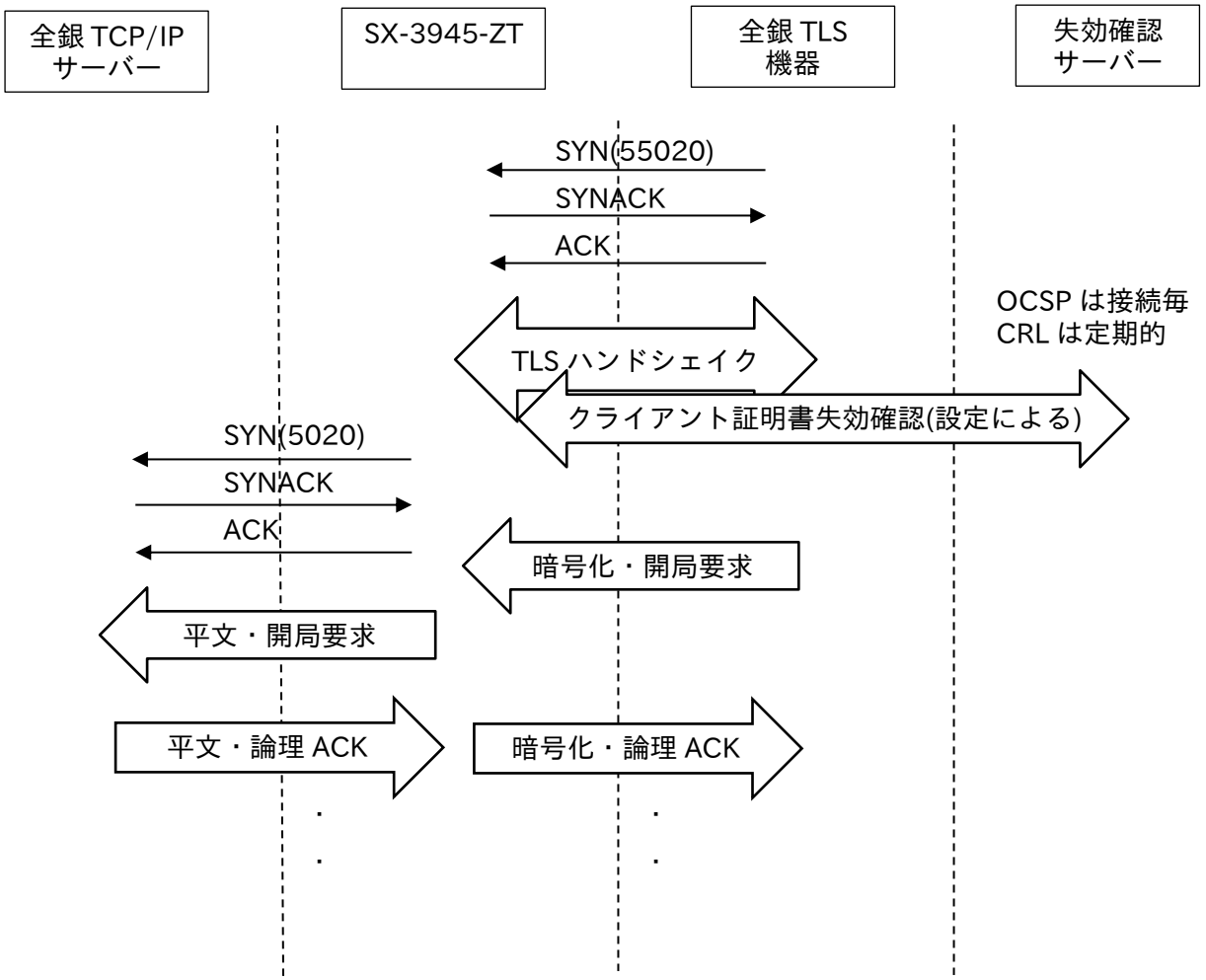
第２章　機能解説

本章では、SX-3945-ZT を使用した場合のシーケンスを明記します。

２．１　TLS サーバー機能の動作概要

TLS サーバー機能用に設定した、IP アドレス/ポート番号(55020)へのアクセス時、TLS サーバー機能で動作します。（ポート番号は設定により変更可能）

TLS ハンドシェイク中に、クライアント認証する設定であれば、失効確認サーバーと連携して失効確認を行います。



２．１．１　TLS サーバー機能の仕様

①対応する TLS バージョン

通常は TLS1.2 を使用します。

②対応する証明書形式

☆サーバー証明書

・DER Encoded Binary X.509（鍵・証明書）。
・Base64 Encoded X.509（鍵・証明書）。
・PKCS#12（鍵＋証明書）
・Base64 Encoded PKCS#10（署名要求のエクスポート）

☆CA 証明書

・DER Encoded Binary X.509（証明書）
・Base64 Encoded X.509（証明書）
・RSA（1024/ 2048/ 4096bit）、 ECDSA（p-256, p-384）

③対応する暗号スイート

使用する暗号スイートは設定により選択することができます。

暗号スイート
DES-CBC-SHA
DES-CBC3-SHA
AES128-SHA
AES256-SHA
DHE-RSA-AES128-SHA
DHE-RSA-AES256-SHA
AES128-SHA256
AES256-SHA256
DHE-RSA-AES128-SHA256
DHE-RSA-AES256-SHA256
AES128-GCM-SHA256
AES256-GCM-SHA384
DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA
ECDHE-ECDSA-AES256-SHA
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES128-SHA256
ECDHE-ECDSA-AES128-SHA256

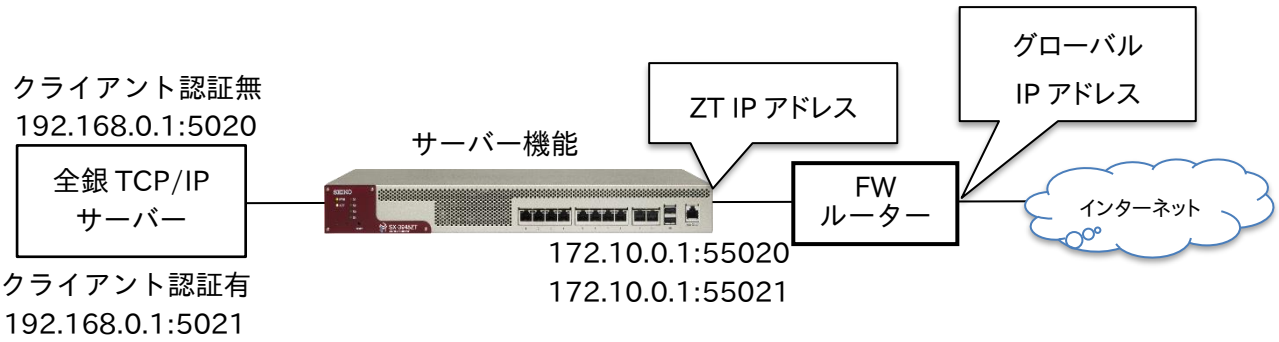
"クライアント認証が無効の時は、"DHE-RSA-AES128-SHA"、"DHE-RSA-AES256-SHA"の暗号スイートは TLS ネゴシエーション時に選択されません。

２．１．２　サーバー機能時の動作概要

ZT をサーバー機能で使用する場合は仮想サーバーの設定をします。

下記例では、全銀 TLS 端末がポート番号 55020 でアクセスする場合を想定します。

FW/ルーターでグローバル IP アドレス：55020 宛のパケットを ZT のプライベート IP アドレス：55020 に伝送するようにします。



ZT の概略設定は、仮想サーバー設定で TLS アクセラレートする IP アドレス：ポート番号を作成してサーバー証明書、アクセラレート後に伝送する全銀 TCP/IP サーバーの情報と連携します。

この条件のアクセスであれば、複数のアクセスがあっても同じ条件でアクセラレートします。

クライアント認証しない、クライアント認証するの両方をサポートする場合は、下記のように仮想サーバ設定を追加して、ポート番号 55021 はクライアント認証して、ポート番号 5021 で全銀 TCP/IP サーバーと伝送します。

クライアントルート証明書をインストールすると、クライアント認証を行います。

仮想サーバ設定　172.10.0.1:55021
サーバー証明書
クライアントルート証明書※
全銀 TCP/IP サーバ
192.168.0.1：5021

※接続する相手分のクライアントルート証明書が必要です。

２．１．３　クライアント証明書の失効リストの確認

クライアント認証する場合に、クライアント証明書が失効リストに載っていないかをチェックし、失効リストに載っているクライアント証明書のアクセスを拒否します。

失効リストの確認方法は２つあります。

①CRL を使用する

失効リストを参照する CRL を記述して、定期的に失効リストを更新します。

CRL はドメイン名で入力しますので、DNS サーバーの設定が必要です。

②OCSP を使用する

クライアント認証時に、クライアント証明書の情報から失効リストをチェックする OCSP レスポンダーの情報を使用して失効確認をします。

OCSP レスポンダー情報はドメイン名となりますので、DNS サーバーの設定が必要です。

プロキシサーバー経由でのアクセスも可能です。

重要)OCSP レスポンダーとの伝送は、時刻情報は正確であることが条件となります。

NTP サーバーと同期するように設定してください。

また、OCSP 情報が設定されていない場合は、エラーと判断します。

これを許容する場合は「AIA 拡張領域を持たない証明書を許容する」設定としてください。

CRL(Certificate Revocation List)

・有効期限よりも前に失効させたデジタル証明書の一覧。

定期的に更新して失効確認します。

OCSP：Online Certificate Status Protocol

OCSP は、X.509 公開鍵証明書の失効状態を取得するための通信プロトコル。

OCSP レスポンダに対して TLS 接続時にデジタル証明書の有効性を確認します。

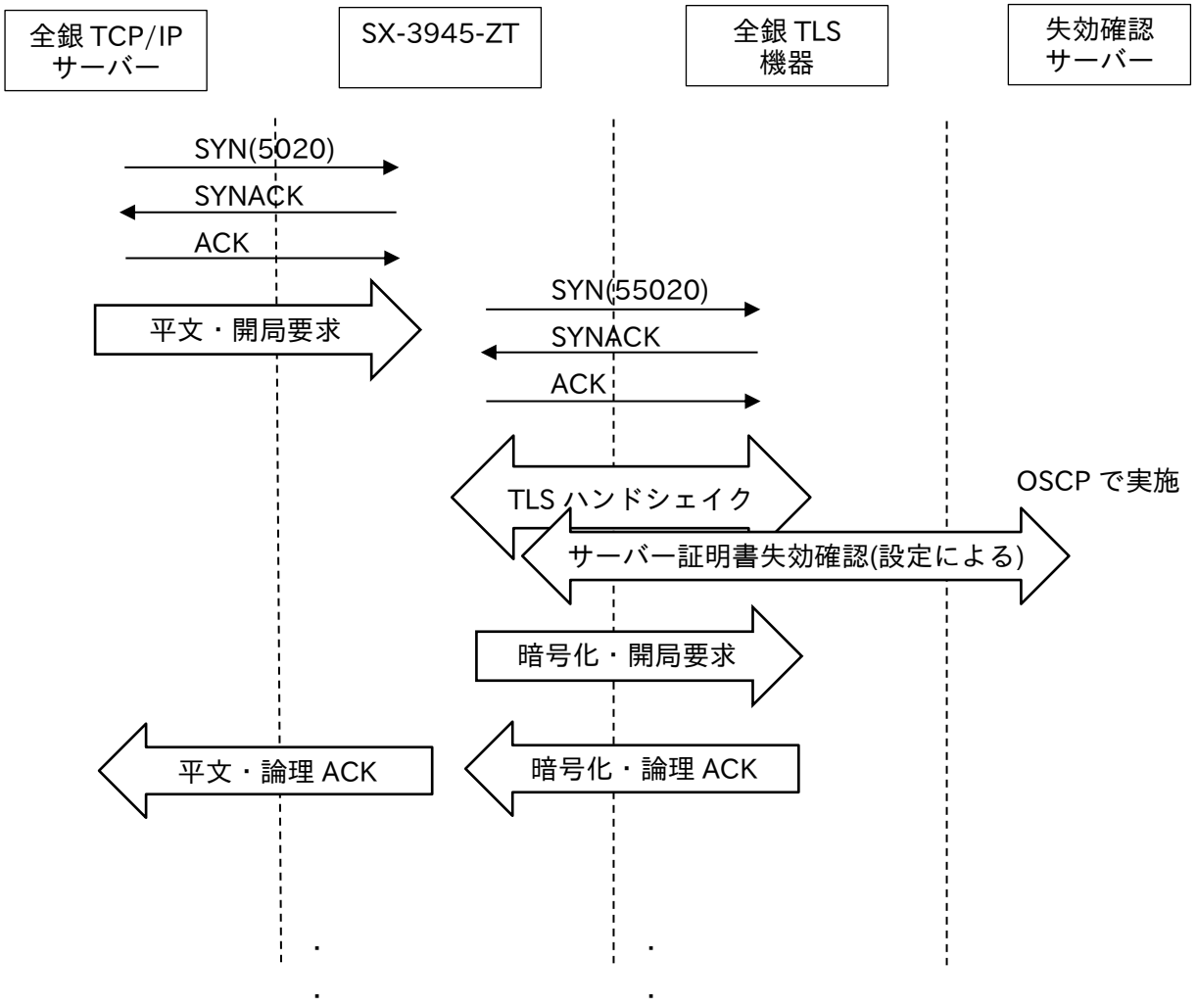
AIA 拡張領域：OCSP の接続先を通知するため、OCSP のアドレスが証明書の拡張領域の認証機関アクセス情報 (AIA: Authority Information Access) に URI 形式で記載されます。

２．２　TLS クライアント機能の動作概要

TLS クライアント機能用に設定した、宛先ポート番号(5020)へのアクセス時、TLS クライアント機能で動作します。（ポート番号は設定により変更可能）

クライアント機能時 TLS ハンドシェイク中に、使用するクライアント証明書を設定により使い分けることができます。

サーバー証明書の失効確認は失効確認サーバーと連携して行います。



２．２．１　クライアント機能の仕様

①対応する TLS バージョン

TLS1.2 で要求します。

②対応する証明書形式

☆CA 証明書

・DER Encoded Binary X.509（証明書）

・Base64 Encoded X.509（証明書）

・RSA（1024/ 2048/ 4096bit）、ECDSA（p-256, p-384）

☆クライアント証明書と秘密鍵

・DER Encoded Binary X.509（証明書）

・Base64 Encoded X.509（証明書）

・PKCS#12（鍵＋証明書）

・RSA（1024/ 2048/ 4096bit）、ECDSA（p-256, p-384）

③対応する暗号スイート

使用する暗号スイートは設定により選択することができます。

暗号スイート
AES128-SHA
AES256-SHA
AES128-SHA256
AES256-SHA256
AES128-GCM-SHA256
AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES128-SHA256
ECDHE-ECDSA-AES128-SHA256

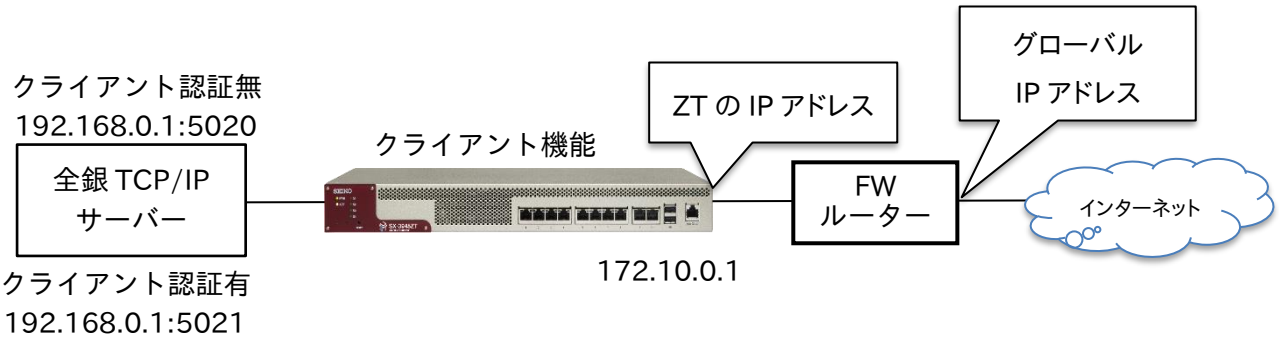
２．２．２　クライアント機能時の動作概要

ZT をクライアント機能で使用する場合は仮想クライアントの設定をします。

２．１．２章にクライアント機能も対応する形で明記します。

全銀 TCP/IP サーバーからクライアント認証しない場合(ポート番号 5020)と、クライアント認証する場合(ポート番号 5021)の設定イメージです。

クライアント機能の場合は、発 IP アドレスを ZT の IP アドレスに NAT する必要が有ります。



仮想クライアント設定　5020
　サーバールート証明書※
　NAT(ZT の IP アドレス)設定
　アクセラレート後のポート番号　55020

※接続する相手分のサーバールート証明書が必要です。

概略設定としては、仮想クライアント設定で TLS 化するポート番号で作成し、サーバールート証明書、アクセラレート後の宛先ポート番号を、NAT 情報を設定します。

全銀 TCP/IP からのポート番号 5020 パケットが TLS 化の対象で宛先 IP アドレスはチェックせず、複数のアクセスがあっても同じ条件で TLS 化します。

クライアント認証しない、クライアント認証するの両方をサポートする場合は、下記のように仮想クライアント設定を追加して、ポート番号 55021 はクライアント認証して、ポート番号 5021 で全銀 TCP/IP サーバーと伝送します。

仮想クライアント設定　5021
　サーバールート証明書※1
　NAT(ZT の IP アドレス)設定
　クライアント証明書※2
　アクセラレート後のポート番号　55021

※1 接続する相手分のクサーバールート証明書が必要です。

※接続する相手分のクライアント証明書が必要です。

２．２．３　クライアント証明書の選択

通常は、サーバーからの要求に従って本装置にインストールされている適切な認証局が発行したクライアント証明書を自動選択します。

全銀 TCP/IP サーバーから複数の起動先が有る場合、起動先毎にクライアント証明書を指定することができます。
下記の例では、接続先(Dst)IP アドレスにより、使用するクライアント証明書を使い分けます。
全銀 TCP サーバーの（Src）IP アドレスは特定しません。

通番	接続先 IP アドレス Dst-IP アドレス	全銀 TCP/IP サーバー Src-IP アドレス	クライアント証明書名 （証明書、鍵を保存）
1	172.16.0.1	0.0.0.0（Any）	seiko-sol.crt seiko-sol.key
2	200.1.1.1	0.0.0.0（Any）	hoge.crt hoge.key
3	100.2.2.1	0.0.0.0（Any）	seiko-ns.crt seiko-ns.key

.crt=クライアント証明書
.key=秘密鍵

※Dst/Src が共に 0.0.0.0 は設定できません。

２．２．４　サーバー証明書の失効リストの確認

サーバー証明書が失効リストに載っていないかをチェックし、失効リストに載っているサーバー証明書のアクセスを拒否します。

失効リストの確認方法は OCSP のみとなります。

①OCSP を使用する

サーバー認証時に、サーバー証明書の情報から失効リストをチェックする OCSP レスポンダーの情報を使用して失効確認をします。

OCSP レスポンダー情報はドメイン名となりますので、DNS サーバーの設定が必要です。

プロキシサーバー経由でのアクセスも可能です。

重要)OCSP レスポンダーとの伝送は、時刻情報は正確であることが条件となります。

NTP サーバーと同期するように設定してください。

また、OCSP 情報が設定されていない場合は、エラーと判断します。

これを許容する場合は「AIA 拡張領域を持たない証明書を許容する」設定としてください。

OCSP：Online Certificate Status Protocol

OCSP は、X.509 公開鍵証明書の失効状態を取得するための通信プロトコル。

OCSP レスポンダに対して TLS 接続時にデジタル証明書の有効性を確認します。

AIA 拡張領域：OCSP の接続先を通知するため、OCSP のアドレスが証明書の拡張領域の認証機関アクセス情報（AIA: Authority Information Access）に URI 形式で記載されます。

２．２．５　ソース NAT の設定

TLS クライアント機能使用時はソース NAT の設定をしてください。

TLS サーバー機能使用時に全銀機器がアクセスする仮想 IP アドレスを、ソース NAT のアドレスに設定することで、同一の IP アドレスで運用できます。

２．３　冗長構成

本製品を２台で使用し、VRRP を利用したマスター、バックアップの冗長構成で使用することが可能です。
ワンアーム構成、ブリッジ構成どちらでも冗長化が可能です。
設定情報に関しては同期機能をサポートしていますので、１台の設定変更で冗長相手の設定も反映されます。

２．４　証明書有効期限監視

SX-3945-ZT にインストールしているサーバー証明書/クライアント証明書の有効期限をチェックし、有効期限の N 日前から syslog で通知します。
デフォルト設定は 30 日、1 日～365 日の間で設定可能。

２．５　クライアント証明書自動更新

SFTP サーバーと連携してクライアント証明書の自動更新ができます。
クライアント証明書を一元管理する場合に有効です。
サーバーは、ローカルネットワーク側またはインターネット側どちらでも設置することができます。
※SFTP サーバーはお客様用意となります。

２．６　ネットワーク構成例と設定項目

設定例に関しては、SX-3945-ZT　導入運用の手引を参照ください。

Appendix-A（基本機能まとめ）

項番	機能	設定値	最大
1	TLS バージョン	TLSv1.2(楕円曲線暗号対応)	
2	TLS アクセラレーション	クライアント/サーバー（同時使用可能）	
3	ネットワーク構成	ワンアーム/ブリッジ接続	
4	サーバー機能時	仮想サーバーIP アドレス/ポート番号設定	256※1
4-1	・クライアント認証	する/しない	
	・クライアント CA 証明書	クライアント CA 証明書をインポート	64
4-2	・クライアント証明書失効確認	OCSP/CRL/失効確認しない	
4-3	OCSP 情報無	失効確認する/しない	
5	クライアント機能時	仮想クライアント　ポート設定	64※2
5-1	・サーバーCA 証明書	サーバーCA 証明書をインポート	64
5-2	・サーバー証明書失効確認	OCSP/失効確認しない	
5-3	OCSP 情報無	失効確認する/しない	
5-4	・クライアント証明書	クライアント証明書をインポート	64
5-5	・使用するクライアント証明書選択	IP アドレス指定/サーバーからの指定/しない	
5-6	・ソース NAT	通常は仮想サーバーと同じ IP を設定	16
6	Proxy サーバー	失効リスト確認など Proxy 経由の場合	
7	DNS サーバー	失効リストのチェックはドメイン名です	
8	NTP サーバー	OCSP 利用時は時刻同期が必要です	

※1　接続相手から発信する際の宛先となる仮想 IP とポート番号の組み合わせの数となります。
接続が 256 に制限されることはありません。

※2　自局の全銀 TCP/IP サーバーから発信する際の待ち受けポート番号と TLS 化にする際に変換するポート番号の組み合わせ数となります。
接続先が 64 に制限されることはありません。

「空白」

SEIKO
セイコーソリューションズ株式会社
〒261-8507 千葉県千葉市美浜区中瀬 1-8
support@seiko-sol.co.jp