

SEIKO

機能解説書

Function Reference Manual

UST

SC-8279 / SC-8259

全銀 TCP/IP 広域 IP 網(TLS 編)

第2版

2020年6月

U00143113401

セイコーソリューションズ株式会社

©2020 セイコーソリューションズ株式会社

セイコーソリューションズ株式会社の文書による許可なく、本書の全部または一部の複製、転載および改変等を行うことはできません。

本書の内容については予告なしに変更することがあります。

本書の使い方

- ・本書は、SC-8279/8259 プロトコルコンバータ全銀 TCP/IP 広域 IP 網接続(TLS)用の標準パラメータに関する機能解説書です。標準パラメータとは弊社が提供するユーティリティにて設定できるパラメータで、この範囲内で使用する場合は、お客様にてセットアップができます。他のプロトコルを使用した UST では弊社内でのプレインストールができますが、全銀 TLS 対応 UST の場合、証明書・秘密鍵をインストールする必要がある弊社でのプレインストールはできません。
- ・本書の読者は、全銀 TCP/IP プロトコル、TLS、ネットワークについて基本的な知識を必要とします。

イーサネット (Ethernet) は、米国ゼロックス社の登録商標です。

UST、IXSAM、WINSAM、ROS³ はセイコーソリューションズの登録商標です。

その他の会社名、製品名は、各社の商標または登録商標です。

目次

第1章 概要	1
1. 1 特徴.....	1
1. 1. 1 全銀 BSC・全銀 TCP/IP 接続から全銀 TLS 接続へのスムーズな移行.....	1
1. 1. 2 クライアント/サーバー機能同時使用が可能.....	1
1. 1. 3 同時接続数.....	1
1. 1. 4 アクセスログ/トラップ機能.....	1
1. 2 位置付け.....	2
1. 3 基本機能.....	3
(1) プロトコル変換機能.....	3
(2) 通信制御機能(上位サーバー側).....	3
(3) 通信制御機能(全銀 TLS 側).....	4
(4) セキュリティ機能.....	4
第2章 機能解説	5
2. 1 基本仕様.....	5
2. 2 設定項目.....	5
2. 2. 1 インターネット側の設定.....	5
2. 2. 2 TLS の設定.....	6
2. 2. 3 全銀 TCP/IP(TLS)の設定.....	7
2. 2. 4 上位サーバーの設定.....	7
2. 2. 5 リモート情報設定.....	8
2. 2. 6 サーバー証明書等の設定.....	9
2. 2. 7 即時反映する設定項目.....	11
2. 2. 8 SNMP 設定.....	12
2. 2. 9 Sntp 設定.....	12
2. 3 上位サーバー伝送仕様.....	13
2. 3. 1 全銀 TCP/IP 伝送仕様.....	13
2. 3. 2. 1 設定情報のホットスタート機能.....	14
2. 3. 2. 2 通信異常終了通知の情報内容.....	14
2. 3. 2. 3 入力確認センス(SENSE)の扱い.....	14
2. 3. 2. 4 発呼完了のステータス.....	15
2. 3. 2. 5 データのブロッキング、デブロッキング.....	15
2. 3. 2. 6 UST からの EOT データ.....	19
2. 3. 2. 7 ACT テーブルロード時の動作.....	19
2. 3. 2. 8 アクセスログの転送.....	20
2. 3. 2. 9 SC-8279 での本番・予備基板.....	20
2. 3. 2. 10 全銀 TLS(TCP/IP)使用時の上位サーバー宛て TCP ポート番号.....	20
2. 3. 2. 11 UST での同一基板のチャンネル折り返しはできません.....	20

2. 4 動作シーケンス.....	21
(1) 発信(クライアント機能) (SC-8279/8259 → 相手全銀機器)	21
(2) 着信(サーバー機能) (SC-8279/8259 ← 相手機器)	22
(3) 発信により接続後のデータの流れ	23
(4) 着信時のデータの流れ	24
(5) 切断時のデータの流れ	25
2. 5 全銀 TLS(TCP/IP)用 UST の電源投入と電源の落とし方(現行 UST との違い)	27
2. 5. 1 全銀 TLS 接続用 UST の電源投入	27
2. 5. 2 全銀 TLS 接続用 UST の電源の落とし方	27
2. 6 ScUTIL2 を使用して設定情報書込み時の注意点(全銀レガシー時と異なります)	28
2. 6. 1 UST から設定情報を読み込んでから設定変更を実施	28
2. 6. 2 設定情報作成時の注意点	28
2. 6. 3 UST への設定情報の書込み	29
2. 6. 4 SC-Util2 終了時の注意	29
2. 7 ScUTIL2 を使用してメンテナンス情報取得時の注意点	30
2. 7. 1 メンテナンス情報の取得方法	30
2. 7. 2 情報取得時 TFTP を使用	30
2. 7. 3 メンテナンス情報の参照	30
2. 8 設定情報の暗号化	30
APPENDIX-A (全銀レガシーUST との相違点まとめ)	31
APPENDIX-B (規約)	32
APPENDIX-C.....	32

「空白」

第1章 概要

本章は、SC-8279/8259(USTと明記することがあります)プロトコルコンバータの、「全銀協標準通信プロトコル TCP/IP 手順・広域 IP 網」で規定された暗号化通信方式の、SSL/TLS 通信をサポートした製品です。

上位サーバーは、全銀ベーシック用のアプリケーションをそのまま使用し、全銀 BSC・全銀 TCP/IP に対応した UST と同様に扱うことができますので、接続相手の全銀端末プロトコルを意識しないで全銀データの伝送を行うことができます。

以降、SSL/TLS 通信をサポートした UST を全銀 TLS 接続 UST と明記します。

1. 1 特徴

1. 1. 1 全銀 BSC・全銀 TCP/IP 接続から全銀 TLS 接続へのスムーズな移行

全銀 TLS 対応 UST は、全銀 BSC 対応 UST、全銀 TCP/IP 対応 UST で使用しているサーバーアプリケーションをそのまま使用して、全銀 TLS 対応機器と手順を使用することができます。移行時の平行運用など柔軟に対応することができます。

全銀 TLS 接続用 UST は、SC-8279/8259 での対応となりますので、SC-8278/58 では使用することができません。

以降の表記に関して、全銀 BSC 対応・全銀 TCP/IP 対応 UST を、全銀レガシーUSTと明記します。

1. 1. 2 クライアント/サーバー機能同時使用が可能

上位サーバーのアプリケーションは全銀レガシーAPを使用しますので、サーバーからの起動時、USTはクライアントとして動作します。

クライアント機能時、上位サーバからの発呼指令内の電話番号から、あらかじめUSTに登録した電話番号とTLSで接続する相手IPアドレス対応表に従い、該当する相手とTLSを確立して全銀データ伝送を行います。

相手からの起動時は、USTはサーバーとしてTLS通信を行い、上位サーバーとは全銀レガシーUSTと同じように着呼通知(接続通知)による制御を行い、全銀データ伝送を行います。

1. 1. 3 同時接続数

全銀レガシーUSTと同様に、最大同時接続数は4となります。

1. 1. 4 アクセスログ/トラップ機能

TLS手順はUSTで終了しますので、TLSハンドシェイクの失敗など異常が発生しても、上位サーバーでは状況が何もわかりません。

USTはTLSが正常に確立した場合、ハンドシェイクで失敗して接続が失敗した情報をアクセス

ロ

グ/トラップとして転送することができます。

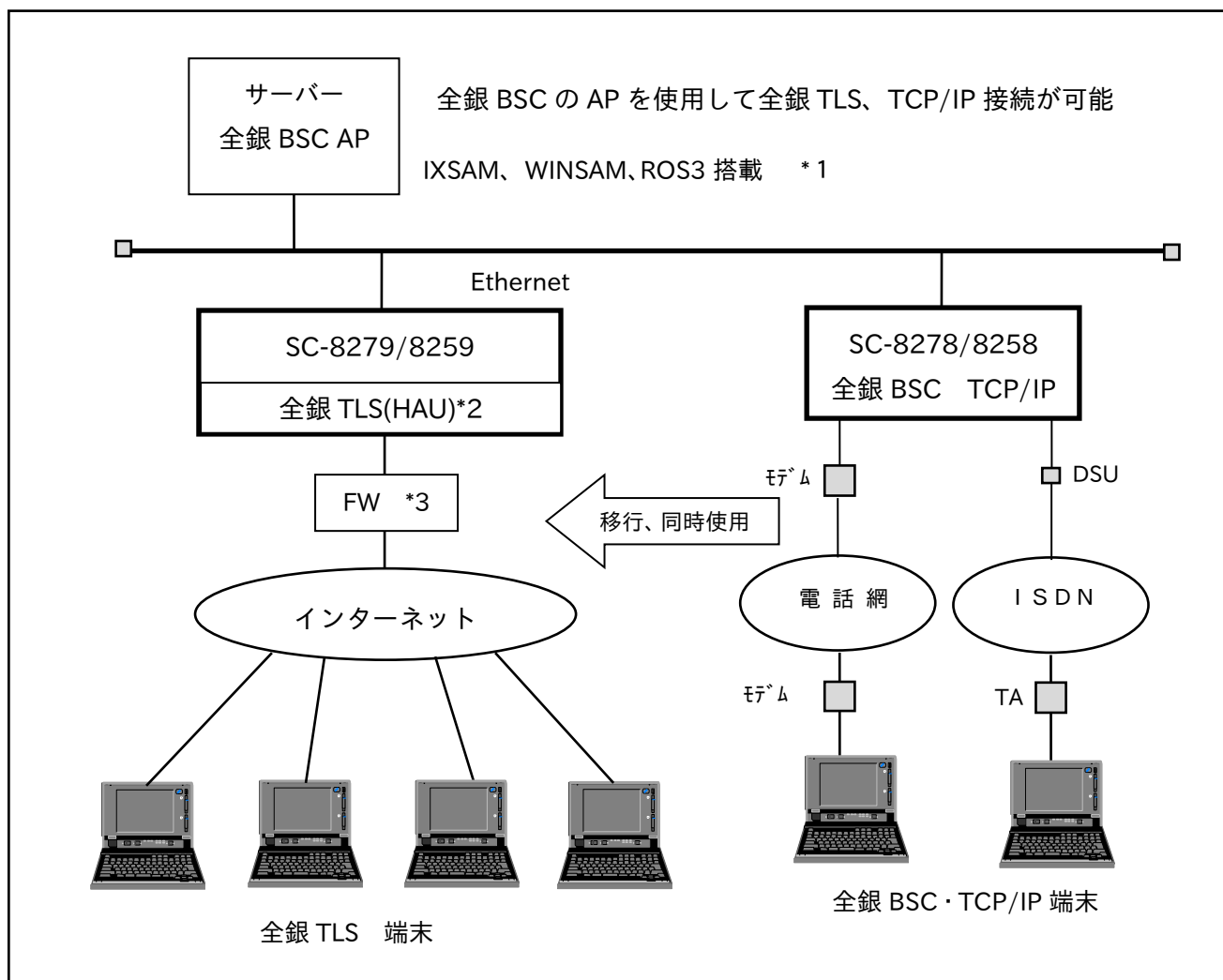
1. 2 位置付け

SC-8279/8259 全銀 TLS 接続用 UST は、既に UST を使用して全銀レガシー接続しているサーバ一環境をそのまま使用して、全銀 TLS 接続ができます。

下記のように SC-8278/8258 を使用して全銀レガシー接続しているシステムで、全銀 TLS 接続用 UST を追加することで全銀 TLS への移行ができます。

SC-8278/8258 をそのまま利用して全銀レガシー接続の同時運用も可能です。

図 1. 1 システム構成



*1 IXSAM : UST 制御用のミドルウェア。UNIX/Linux 用。

WINSAM : UST 制御用のミドルウェア。Windows 用。

ROS³ : 全銀/JCA 用の集配信パッケージ。

*2 全銀 TLS(HAU) : HAU はインターネット接続用の LAN ポートを実装した通信基板。

*3 FW : ファイヤーウォール(ルーターも含まれます)

UST にはファイヤーウォールの機能はありません。

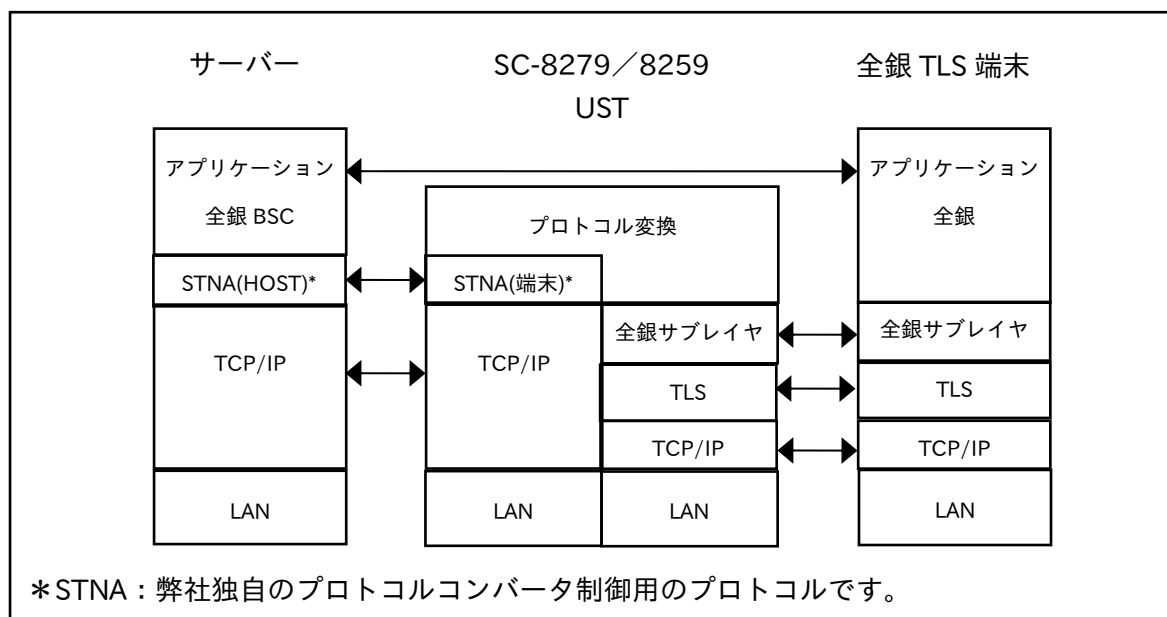
1. 3 基本機能

(1) プロトコル変換機能

SC-8279/8259 全銀 TLS 接続用 UST は、全銀 TCP/IP を TLS 化して伝送する端末システムと、全銀 BSC 機能を持つ上位サーバーとの中継を行います。

これにより、サーバーは全銀手順のデータリンク層を意識することなく、全銀アプリケーションを使用することができます。

図 1. 3 プロトコル構成(全銀 TLS 接続時)



(2) 通信制御機能(上位サーバー側)

全銀レガシー接続 UST と同様に、上位サーバーのアプリケーション制御に関する事項の設定が可能です。

使用する LAN ポートは、SC-8279 の場合は実装した全ての通信基板と同様に、1000Base-T のポートとなります。

SC-8259 の場合も同様に、実装した全ての通信基板と同様に、Ch0 のポートとなります。

	設定項目	設定内容
1	着呼制御の使用	あり／なし
2	通信異常終了通知の使用	入力しない／入力する
3	発呼完了ステータスの追加機能の使用	追加なし／追加あり
4	入力確認センスをサーバーが制御	する／しない

注意)通信異常終了通知のステータス内容は、全銀レガシーの内容とは異なります。

着呼制御ありの設定でも TLS ハンドシェイクを行います。

(3) 通信制御機能(全銀 TLS 側)

全銀 TLS 接続 UST は、全銀 TCP/IP を TLS 化して、サーバー機能、クライアント機能を同時に使用することができます。

TLS で必要なサーバー証明書/秘密鍵・ルート証明書・クライアント証明書/秘密鍵は UST にインストールします。

クライアント機能時は、相手旧電話番号と IP アドレス、クライアント証明書の対応設定を行い、該当するサーバーへ該当するクライアント証明書を使用してアクセスします。

(4) セキュリティ機能

インターネット側は、HAU 基板の LAN1 ポートを使用します。

下記のポート番号のみ Listen し、その他のポートは閉じていますが、ファイヤーウォールの機能は有りません。

LAN1 側ではルーターのファイヤーウォール機能などを設定してください。

① インターネット側からのアクセス時

- ・全銀 TLS 伝送用のポート番号を Listen
- ・NTP 設定時のみポート 123(UDP)Listen

上位サーバー側に NTP サーバーの設定をしても Listen します。

上位サーバー側の伝送は、筐体共通の LAN ポートを使用します。

② 上位サーバー側からのアクセス時

- ・Listen するポート番号

上位サーバーとの伝送、SC-Util2(UST 用のユーティリティー)で使用するポート番号のみ Listen します。(デフォルト設定時ポート 999)

UST では TFTP/FTP など使用しますがいずれもクライアント機能で動作しますので Listen しません。

①と②はそれぞれ終端していますので、①のネットワーク機器から②のネットワーク機器へのアクセスはできません。

第2章 機能解説

本章は、SC-8279/8259 の全銀 TLS 接続 UST で使用する標準パラメータについての解説を記述しています。

UST の設定は、SC-Util2 を使用して各種設定、指定した PC のディレクトリにサーバー証明書やクライアント証明書を置き、UST への書込みを行います。

2. 1 基本仕様

全銀協標準通信プロトコル(TCP/IP 手順・広域 IP 網)に基づいて、セキュリティ対策として SSL/TLS の暗号化方式を使用します。

(1) 適用回線

インターネット(IPv4)

UST に設定する IP アドレスは、グローバルで使用できる IP アドレスとしてください。

(2) 暗号化方式

TLS1.2 を使用して暗号化を行います。

(3) サーバー/クライアント機能

UST は同時にどちらの機能も動作します。

最大同時接続数は合計 4 になります。

2. 2 設定項目

2. 2. 1 インターネット側の設定

インターネット側は、通信基板(HAU)の LAN1 ポートを使用します。

設定項目は下記のようになります。

N o.	項 目	設定内容	標準設定値
1	装置 IP アドレス	インターネット側の IP アドレス/ネットマスクを設定します。 グローバルで特定できる IP アドレスを使用してください。	
2	LAN1 速度設定	LAN1 ポートの通信速度を設定します。 Auto/100F/100H/10F/10H	Auto
3	DNS サーバー	CRL 更新時の設定で使用します。 プライマリー/セカンダリー	
4	Proxy サーバー	CRL 更新時の設定で使用します。 IP アドレス/ポート番号	

注意)

- ・ Proxy サーバーを使用して CRL 更新する場合、Proxy サーバーが更新しない場合があります。
- ・ 通信基板の LAN2 ポートは使用できません。

2. 2. 2 TLS の設定

TLS 通信で必要な情報を設定します。

SC-Util2 から設定情報を書込み後、即時反映する設定が有りますので、下記参照ください。

No.	項目	設定内容	標準設定値
1	クライアント認証	サーバーモード時にクライアント認証する/しないを設定します。 どちらか一方の選択となります。 再起動が必要です。	しない
2	TLS バージョン	サーバーモード時にクライアントからの許容する TLS バージョンを設定します。 再起動が必要です。	TLS1.2
3	サーバー証明書	・有効なサーバー証明書名(ディレクトリ名) ・転送する証明書名設定とパスフレーズ 証明書は SC-Util2 の指定したディレクトリに置く必要があります。 有効な証明書名、証明書とも即時反映します。	scert001
4	失効リスト更新	失効リスト更新用の URL、更新インターバル時間を設定します。最大 8 か所の登録ができます。 更新できない URL の設定はしないでください。 即時反映し、CRL 取得を行います。	なし 10 分
5	クライアント証明書	・クライアントモード時に、接続する相手サーバー 毎にクライアント証明書を設定します。 ・クライアント証明書を設定しなければ、クライアント 認証しない設定との混在ができます。 証明書は SC-Util2 の指定したディレクトリに置く必要があります。 証明書は即時反映します。 2.2.5 のリモート情報の設定は再起動が必要です。	なし
6	暗号スイート	使用する暗号スイートを登録します。 UST から最初に読込まないと表示されません。 即時反映します。	UST が持ちます

2. 2. 3 全銀 TCP/IP(TLS)の設定

全銀 TLS 時の全銀 TCP/IP の設定

No.	項目		標準設定値
1	全銀 TLS サーバー時 ポート番号	サーバー機能時の Listen するポート番号を設定します。	5020
2	全銀 TLS クライアント時 ポート番号	クライアント機能時、接続先相手毎にポート番号を設定します。(2.2.5)	5020
3	最大テキスト長	伝送する全銀レコード長を設定します。 256/512/1024/2048/4096/8192/32768 4096 以上は拡張全銀手順になります。 2.2.4 の 7 項と連携して設定してください。	2048
4	連続受信回数	論理 ACK 無に連続して受信できる値 サーバモード時、クライアントモード時共通で 0~15	0

2. 2. 4 上位サーバーの設定

上位サーバーとの伝送は Ch0 の LAN ポートを使用します。

現行の全銀レガシー設定に合わせて設定してください。

No.	項目		標準設定値
1	IP アドレス	上位サーバー側の IP アドレス/ネットマスク	なし
2	上位サーバー IP アドレス	上位サーバーの IP アドレスを設定します。 登録は 1 ヶ所になります。	なし
3	ポート番号	Listen ポートと宛先ポートを設定します。 通常はデフォルト設定で使用ください。	999/999
4	全銀コネクション数	使用する最大 PA 数(同時接続数)を設定します。 最大 4 です。	4
5	ゲートウェイ情報	ゲートウェイを登録します。 ・インターネット側にデフォルトゲートウェイを設定してください。 ・上位サーバ側のゲートウェイ設定は、ネットワーク指定などで登録してください。	なし
6	シスログサーバー	TLS のアクセス情報を転送します。 ・TLS 正常時、異常時の情報を転送します。 ファシリティ/レベル設定	なし
7	最大テキスト最大	上位サーバーとの最大テキスト長を設定します。	2048

	テキスト長	最大は 4096 バイトです。 2.2.3 の 3 項と連携して設定してください。	
8	入力確認センス	上位サーバーへの入力時のセンス制御。 使用/不使用	不使用
9	着呼許可待ち タイマー	着呼制御する設定時に有効。 着呼許可を監視。	29
10	センス待ちタイマー	センス待ちを監視。	255
11	通信異常終了通知	TCP・TLS 異常切断時に、切断通知入力前に、通信異常終了通知を入力する/しないを選択します。	入力しない
12	無通信タイマー	回線接続後、データ伝送が一定時間無い時に切断 します。	30
13	着呼制御	・電話を接続する概念が無い場合、TLS ハンドシェイク完了時に着呼通知を入力します。 ・着呼拒否する場合もハンドシェイクまで実施 します。 2.4(2)の動作シーケンスを参照ください。	なし
14	発呼完了ステータス	発呼完了のステータス情報を追加する/追加なし を選択します	なし

2. 2. 5 リモート情報設定

クライアントモードで使用する場合に、全銀レガシーで発信時に使用していた相手先電話番号と、全銀 TLS で使用する相手先 IP アドレス、ポート番号、クライアント証明書を対応付けて設定します。

編集対象 No.を指定して、最大 500 件登録できます。

N o.	項 目		標準設定値
1	端末電話番号	全銀レガシーで使用していた電話番号を登録 します。	なし
2	接続先 IP アドレス	接続先 IP アドレスを登録します。	なし
3	接続先ポート番号	相手先ポート番号を登録します。	5020
4	クライアント証明書	クライアント認証する場合は、クライアント証明 書を置くディレクトリ名を登録します。 ・指定しなければクライアント認証しません。	ccert001

2. 2. 6 サーバー証明書等の設定

全銀 TLS 設定時、UST にインストールする証明書関連は下記に従って、該当するフォルダーに証明書を置き、UST へ書込む必要があります。

証明書関連は UST へ書込み後、即時反映されます。

UST からの読み込み/書込みともに、設定情報と証明書類が全ての情報となりますので、証明書類だけの読み込み/書込みはできません。

Sc-Util2 を終了する場合に Cert フォルダーは削除されますのでご注意ください。

(1) 証明書の形式

pem 形式の証明書に対応しています。

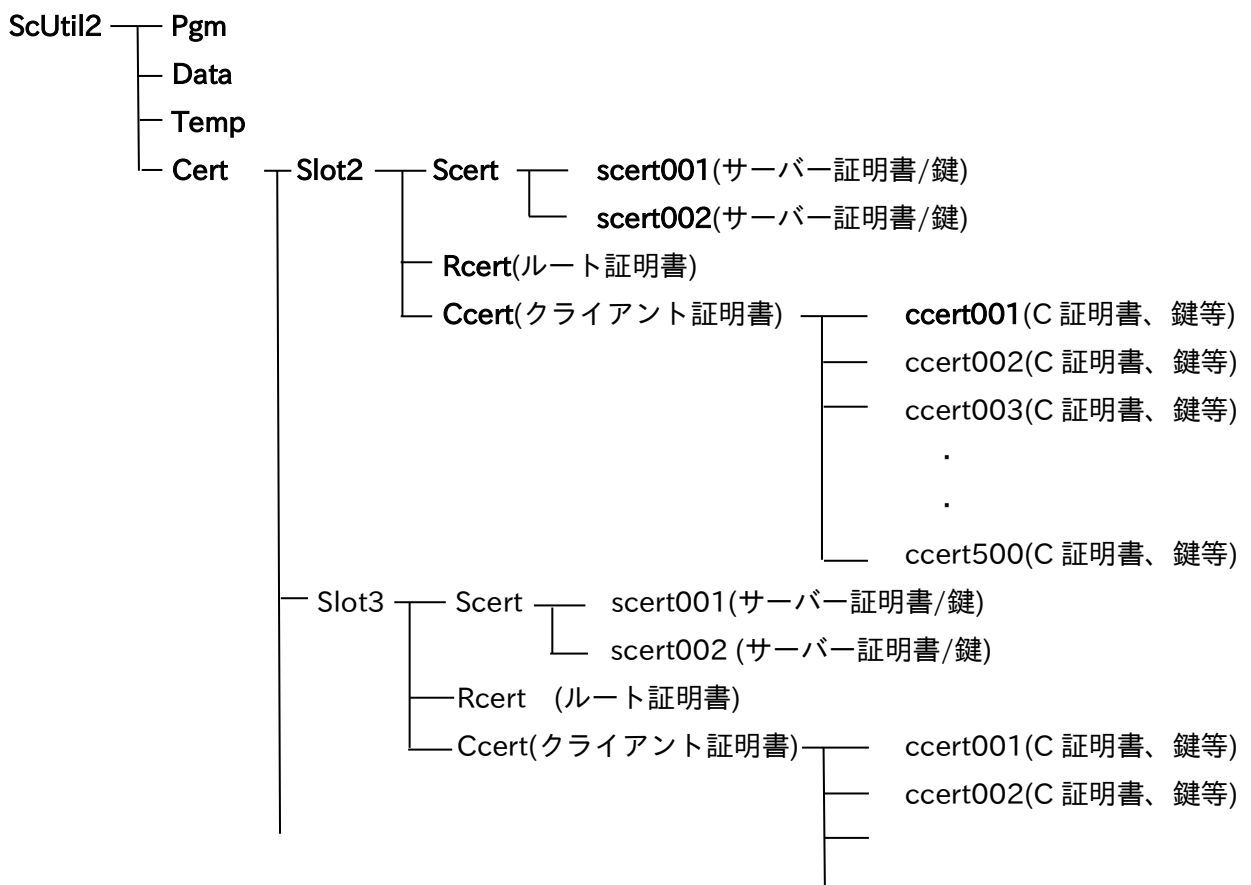
(2) 証明書を置くフォルダー

下記 ScUtil2 のフォルダー構成で ScUtil2 起動時に、下記太文字フォルダーは自動で作成します。

サーバー証明書に関しては下記 scert001 または scert002 のフォルダーに証明書ファイルを置きます。

同様にクライアントルート証明書は Rcert のフォルダーに置きます。

クライアント証明書は Ccert フォルダーに、ccert001 は自動で作成しますが、ccert002 以降は自動生成しません。
フォルダーを作成してクライアント証明書を置いてください。



(3) 証明書ファイル名

①サーバー証明書名

フォルダー名は scert001、scert002 と分けますが、ファイル名は固定のファイル名で

- ・証明書ファイル名「server.crt」
- ・鍵ファイル名「server.key」

として該当フォルダーに置いてください。

中間証明書がある場合、ファイル名は

- ・中間証明書ファイル名「chain1.crt」
- ・中間証明書ファイル名「chain2.crt」

として該当フォルダーに置いてください。2つまで登録できます。

②ルート証明書

クライアント機能時に接続先の CA 局が全て同一であれば、ファイル名は

- ・証明書ファイル名「rootca001.crt」

として該当フォルダーに置いてください。

複数ある場合は、ファイル名を rootca002.crt と数字をアップし、最大 rootca100 まで登録できます。

③クライアント証明書

(2) で設定したクライアント証明書のフォルダーに、ファイル名は

【PEM 形式の場合】

- ・証明書ファイル名「client.crt」
- ・鍵ファイル名「client.key」

【PKCS#12 形式の場合】

- ・証明書/鍵ファイル名「client.p12」
 - ・パスワードが有る場合は、パスワードをファイルにして「client.pwd」
- として置いてください。

SC-Util2 では Csert/ccert001 のフォルダーは自動で作成しますが、ccert002 以降は自動作成しませんので、フォルダーを作成してから証明書類を置いてください。

! ワンポイント

UST の設定を変更する場合は、UST から設定情報を読み込んでから設定し、該当ディレクトリに

証明書ファイルがあることを確認してから UST に書込むようにしてください。

! 注意

全銀 TLS 版は、UST への書込み後、即時反映する項目が 2.2.7 に明記しています。

その他の設定変更時は、再起動により設定情報の変更が有効になります。

！ 注意

ScUtil2 を使用した設定情報の読み込み/書き込みは、設定情報の他に証明書類も同時に転送します。

設定情報だけ、証明書類だけの読み込み/書き込みはできません。

！ 注意

証明書を開いて編集する場合、改行コードは LF としてください。

「メモ帳」で編集開いて書込むと改行コードが CRLF となり正しく動作しません。

！ 注意

ScUtil2 を終了する場合、Cert 以下のフォルダーを削除し、セキュリティを確保します。

該当するフォルダーを開いている場合、注意のポップアップが表示されます。

Cert 以下のフォルダーが残った場合は、削除してください。

2. 2. 7 即時反映する設定項目

UST から設定情報を必ず読み込んでから設定変更してください。

ScUtil2 設定項番	設定内容
通信(2)	失効リスト URL インターバル 対象証明書
通信(2)	有効な証明書 証明書設定 パスフレーズ
暗号スイート	使用する暗号スイート選択
証明書/秘密鍵	設定情報を UST へ書込む場合、下記情報の書込みを行います。 ・ Scert 以下のディレクトリ ・ Rcert 以下のディレクトリ ・ Ccert 以下のディレクトリ 注意)UST への書込み時ディレクトリに証明書が無いと UST 側の証明書が無くなりますので注意ください。

2. 2. 8 SNMP 設定

SNMP マネージャの設定は最大 3 か所まで登録することができます。

TLS のアクセスログとしてトラップを出すことができます。

	設定項目	内容
1	SNMP 設定	無効/有効 SNMP の設定が有効か無効の選択
2	ドメイン名	ドメイン名を登録します。
3	連絡先	連絡先を登録します。
4	設置場所	設置場所を登録します。
5	SNMP マネージャ設定	無効/有効 各マネージャの設定が有効か無効かの選択(最大 3)
		IP アドレス
		コミュニティ
6	SNMP トラップ設定	無効/有効 各マネージャの設定が有効か無効かの選択(最大 3)
		IP アドレス
		ポート番号
		コミュニティ
7	トラップ通知設定	電源投入時の cold start を通知する/通知しない

2. 2. 9 SNTP 設定

NTP サーバーと時刻合わせをする場合に設定します。

本設定は SC-8259 のみ有効です。(SC-8279 は MCU 基板に設定します)

	設定項目	内容
1	SNTP 設定	無効/有効 SNTP の設定が有効か無効の選択
2	タイムサーバーIP	タイムサーバーの IP アドレスを設定します。

2. 3 上位サーバー伝送仕様

上位サーバーとUST間の通信で使用する制御コマンドを明記します。

使用するコマンドは、全銀レガシーで使用する制御コマンドと同様ですが、一部セットする情報内容が異なります。

下記データ伝送時にはSTNAで使用するヘッダー(FCH)が付加されます。

2. 3. 1 全銀TCP/IP 伝送仕様

項番	コマンド名	サーバー	UST	CMND (HEX)	PUA (HEX)	ユーザーデータ部		備考
1	通常入力データ	←		00	40	ETB電文		中間ブロック
					80	ETX電文		中間・最終ブロック
2	通常出力データ	→		00	40	ETB電文		中間ブロック
					80	ETX電文		中間・最終ブロック
					82	ETX電文		中間・最終ブロック EOT付
3	EOT 通知 指令	← →		00	02	-----		EOT通知は全銀TCP制御データ受信時に発生します。*7
4	接続通知	←		05	00	-----		
5	切断 通知 指令	← →		08	00	-----		
6	発呼指令	→		09	00	電話番号長	発信先電話番号	最大26桁（バイナリ指定） 発呼アドレス（JISコード指定） *3
7	発呼完了	←		0A	00	*1		正常終了
					01	*1		異常終了（データ/モデム異常）
					02	*1		異常終了（接続不可）
8	着呼通知	←		09	00	発信者番号 *6		着呼制御時のみ使用
9	着呼許可	→		05	00	-----		着呼制御時のみ使用
10	通信異常終了通知	←		04	00	Phase 1バイト	Event 1バイト	伝送制御マトリックスの状態と事象をセット *2
11	出力完了	←		(FCHのみ)				正常完了/異常完了 *4
12	SENSE	→		(FCHのみ)				*5

*1：発呼完了ステータスを追加する設定の場合、『表1 発呼完了詳細ステータス情報』を付加します。

*2：通信異常終了通知のPhase,Eventは全銀BSC時とは異なります。

Appendix-Cの表2を参照してください。

*3：発呼指令内の発信先電話番号にはISDN回線使用時のサブアドレスも含まれます。

電話番号とサブアドレスの区切りとして '/' (2F)hを使用してください。

電話番号は数字のみで - や () は使用できません。

*4：サーバーからUSTへの全ての出力データに対して、USTが返す出力確認応答データです。

*5：デフォルトの設定では、SENSEと全銀TCP/IPの論理ACKは連携していません。

APIはUSTから入力されたコマンド(出力完了のみ対象外)に対して、SENSEを出力してください。

*6：発信者番号は通知されません。

*7：起動集信時の終了要求、応答配信の終了回答に関しては EOT 通知を入力しません。

2. 3. 2 全銀レガシーUST と上位サーバーとの伝送仕様の相違

上位サーバーとの伝送仕様で、全銀 TLS 接続 UST と全銀レガシー接続 UST で、動作が変わる部分を明記します。

AP としては定義の修正が必要なものもありますのでご注意ください。

2. 3. 2. 1 設定情報のホットスタート機能

全銀 TLS 接続 UST の設定は、サーバー証明書/クライアント証明書などの証明書/秘密鍵に関して、設定書込み後、直ぐに反映します。

併せて即時反映する項目は 2. 2. 7 の内容となります。

2. 3. 2. 2 通信異常終了通知の情報内容

異常発生時の全銀 TLS 用の情報をセットします。

2. 3. 2. 3 入力確認センス(SENSE)の扱い

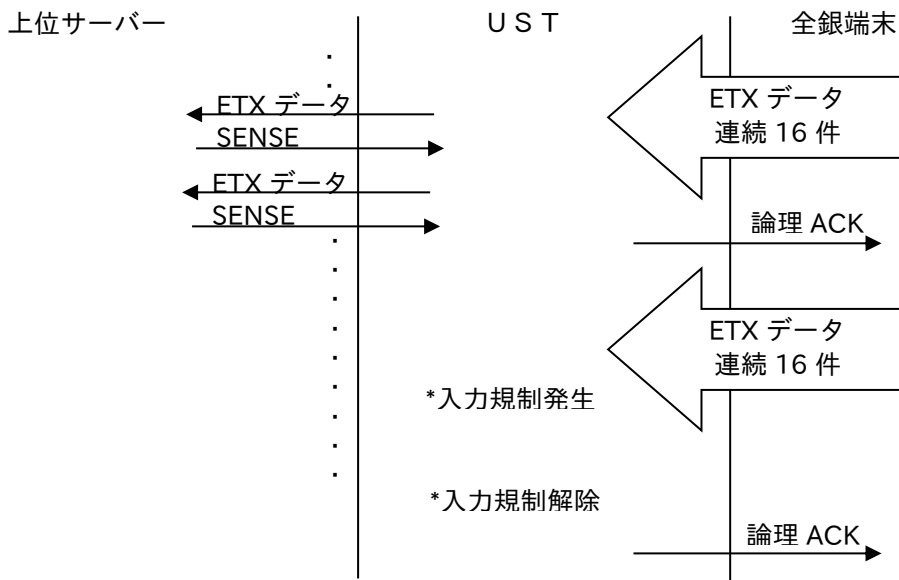
全銀 TLS では、デフォルト設定では論理 ACK とセンスは連動していません。

センスが遅れた場合は、UST のフロー制御が働き、論理 ACK の伝送は停止しますので、相手全銀機器からの入力は抑止されます。

オプション設定で、センスと論理 ACK を連携することもできますが、論理 ACK の伝送が遅れ、全体の伝送時間が増えます。

☆デフォルト設定時

ETX データ受信後の ACK 送信タイミングに使用



注意)

SENSE がサーバーから発生しない状態でも論理 ACK は送信するため UST にデータが滞留します。

2. 3. 2. 4 発呼完了のステータス

発呼が失敗したときのステータスは全銀レガシーと異なります。

上位サーバーのアプリケーションでステータスにより異なる処理を行っている場合アプリケーションの変更が必要となる場合があります。

2. 3. 2. 5 データのブロッキング、デブロッキング

全銀 TLS の場合は全銀 TCP/IP と同様となりますので、全銀 BSC からの移行時ご注意ください。

上位サーバーからのデータを BSC 側最大長に合わせて ETB/ETX 伝送します。

全銀 BSC 端末からは ETB 電文受信時、ETX 電文までデータを溜めこみ上位サーバーへ入力します。

全銀 TLS(TCP/IP)の場合、全銀端末からのデータは、上位サーバーの最大長に分割して入力します。

上位サーバからの ETB 電文は ETX 電文まで溜めこみ、全銀 (TLS) TCP/IP 端末へ 1 ブロックとして伝送します。

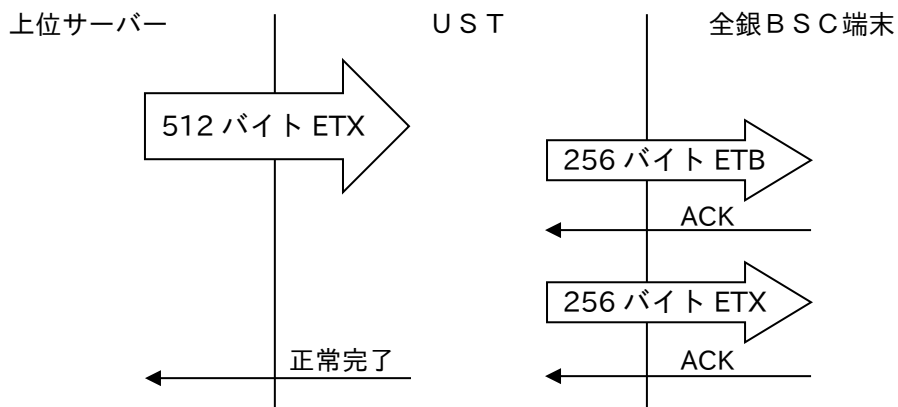
(1) 全銀 BSC の場合

設定によって下記のようにブロッキング・デブロッキングを行います。

☆UST の設定

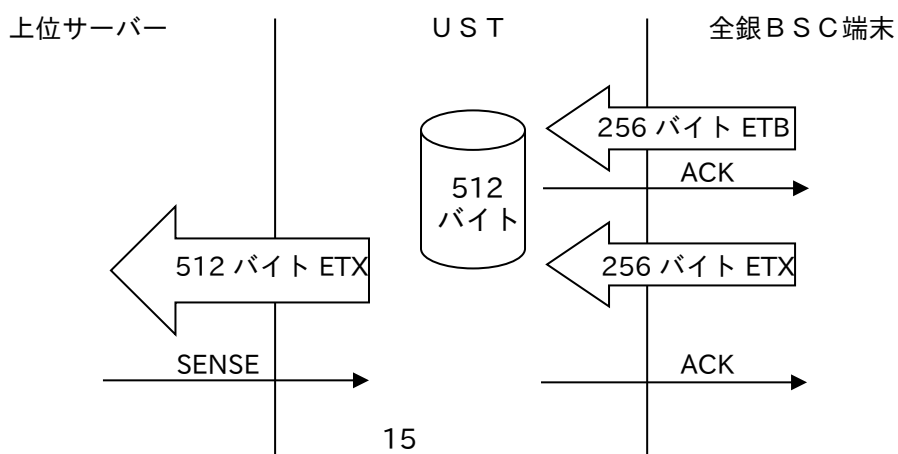
- ①デブロッキングする設定でデブロッキングサイズを指定する。

デブロッキングサイズは 256 とする



- ②ブロッキングする設定でブロッキング数を指定する。

ブロッキング数は 2 とする



(2) TLS(TCP/IP)の場合

全銀 TLS(TCP)最大テキスト長と上位サーバー最大テキスト長および上位サーバーからの出力データ区分(ETB/ETX)により自動的にブロッキング・デブロッキングを行います。

ブロッキング/デブロッキングの方向が全銀 BSC とは異なりますのでご注意ください。

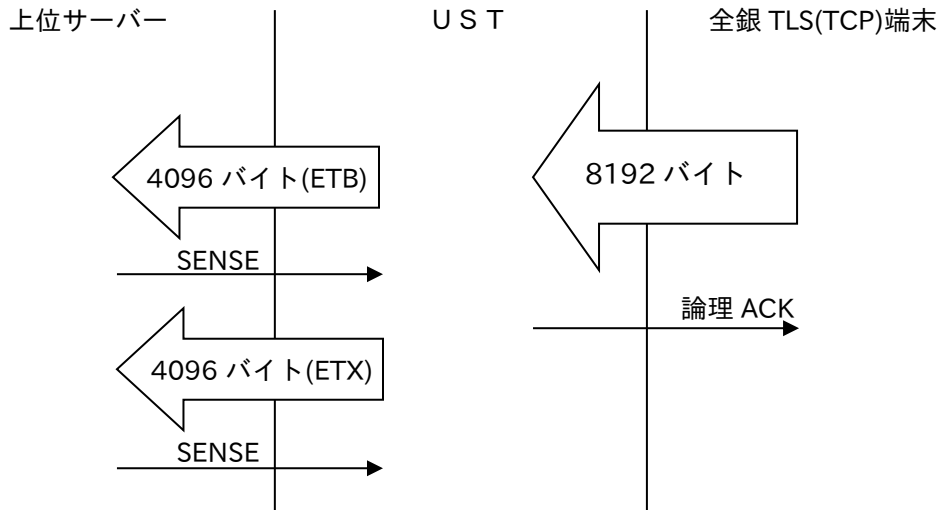
設定内容によってはエラーとなり異常終了することがありますのでご注意ください。

使用する上位サーバーパッケージによって、サポートできない機能がありますので確認ください。

全銀 TCP 最大テキスト長は、UST から全銀 TCP 端末にデータを送信する際のブロッキングサイズです。(全銀 TCP 端末から受信可能な最大データサイズは 32k バイト固定です)

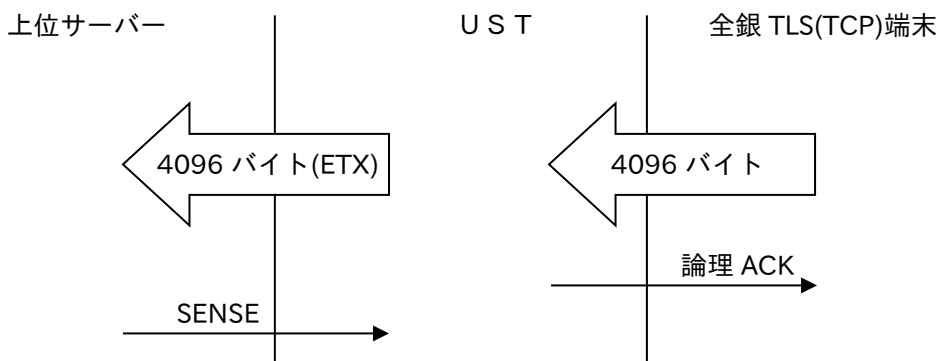
- ①上位サーバー最大テキスト長 < 全銀 TCP 端末から受信したデータサイズ
(最大 4096 バイト) (最大 32k バイト)

例) 全銀 TCP 端末から 8192 バイト受信時、上位サーバーへは 4096(ETB)、4096(ETX)に分割入力。



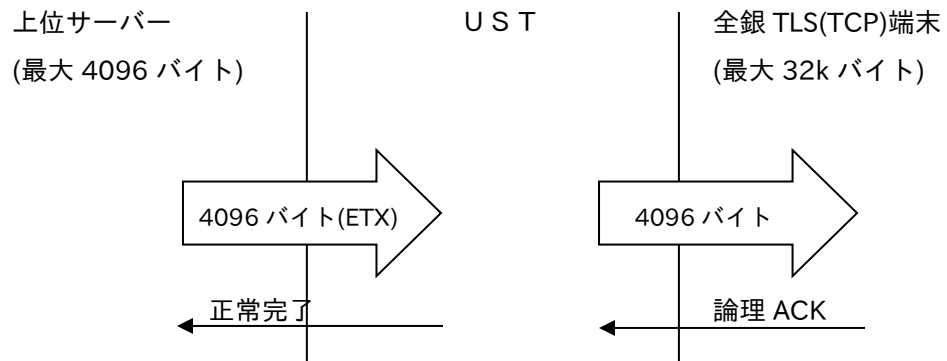
- ②上位サーバー最大テキスト長 = 全銀 TCP 端末から受信したデータサイズ
(最大 4096 バイト)

例) 全銀 TCP 端末から 4096 バイト受信時、上位サーバーへは 4096(ETX)で入力。

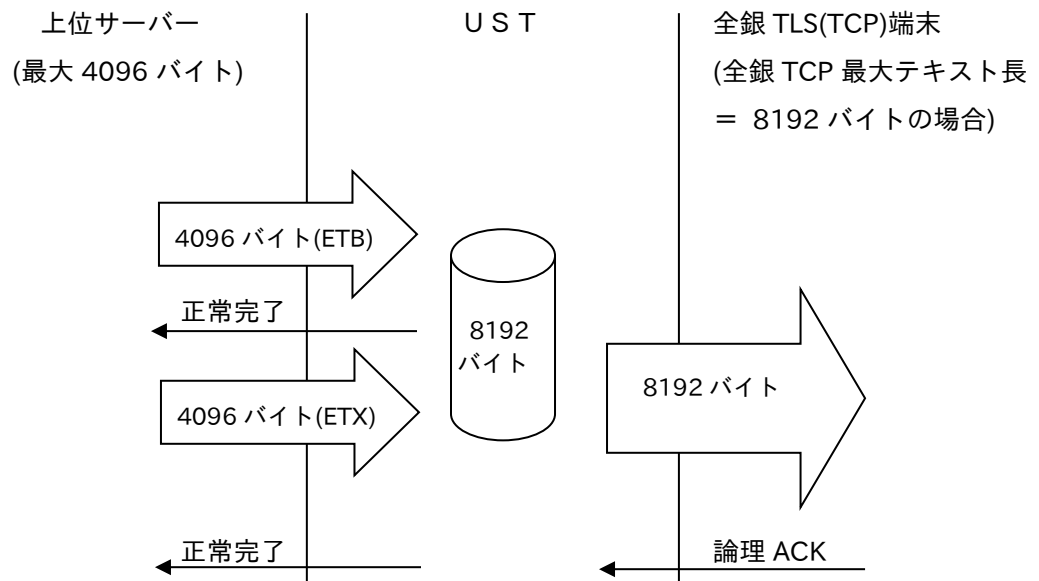


③上位サーバー最大テキスト長 < 全銀 TCP 最大テキスト長の動作
 (最大 4096 バイト) (最大 32k バイト)

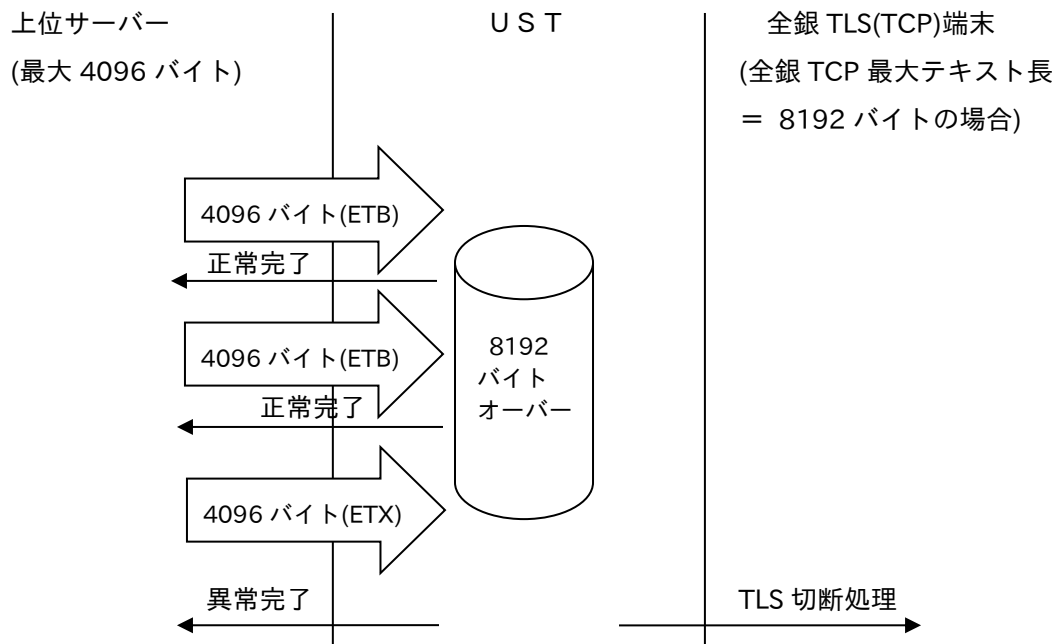
例) 上位サーバーから出力データ区分が 4096(ETX)の場合そのまま全銀 TCP/IP 端末へ送信



例) 上位サーバーから出力データ区分が ETB/ETX の場合 2つのデータをバッファリングして送信

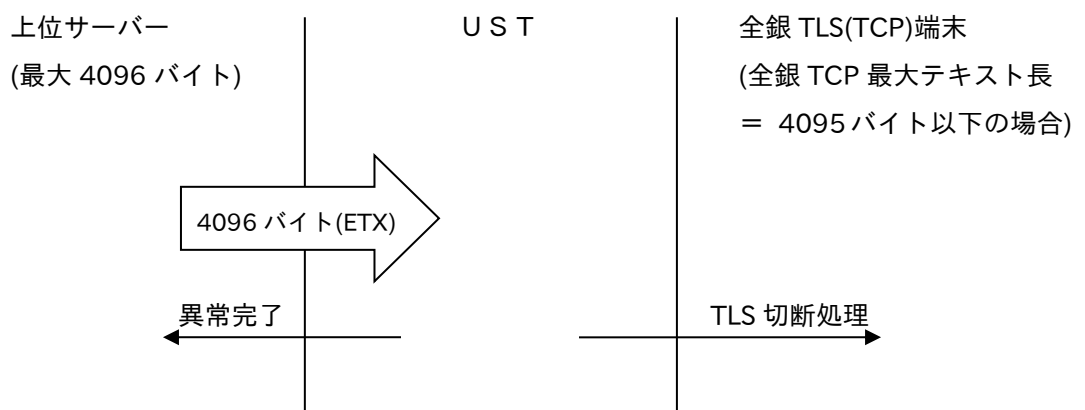


例) 上位サーバーから出力データ区分が ETB/ETB/ETX で全銀 TCP 最大データ長オーバー時バッファリングサイズをオーバーした時は ETX データに対して異常完了を入力し回線を切断します。



④上位サーバー最大テキスト長 > 全銀 TCP 最大テキスト長の動作 (最大 4096 バイト)

例) 上位サーバーから出力データ区分が ETX の場合

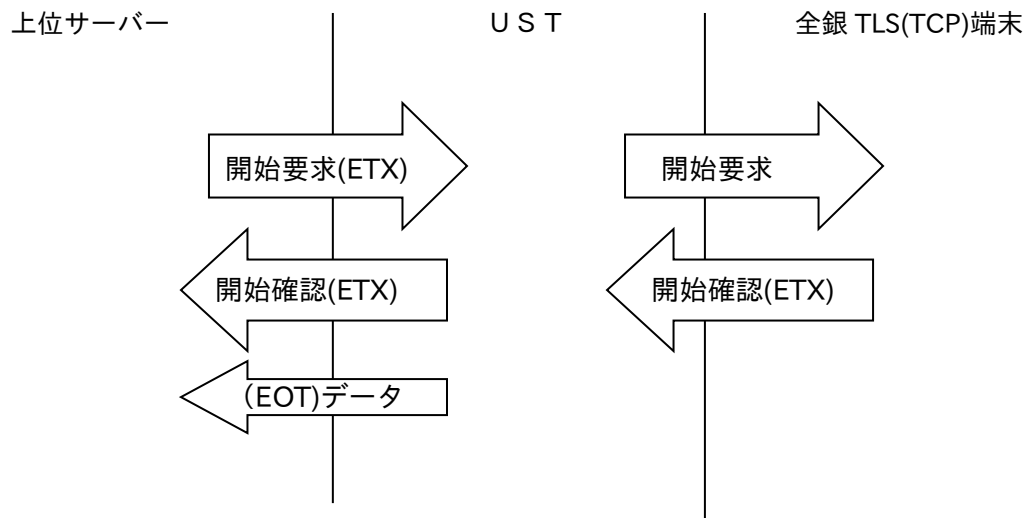


注意)

上位サーバー最大テキスト長 > 全銀 TCP 最大テキスト長の設定をしたとき上記のようにデータ伝送ができません。このような設定はおこなわないでください。

2. 3. 2. 6 USTからのEOTデータ

全銀 BSC では EOT データを上位サーバーへ入力していますが全銀 TLS(TCP/IP)の場合は全銀制御電文時に EOT データとして入力します。



*)全銀制御電文

閉局要求/応答、開始要求/応答、終了要求/応答、閉局要求/応答です。

2. 3. 2. 7 ACT テーブルロード時の動作

ACT テーブルロード時に宛先の上位サーバーが変わりますが影響範囲が変わりますので下記明記します。

①全銀 BSC

宛先が変わる前の上位サーバーとの接続は切断せず、切り替わった上位サーバーに接続を確立して伝送が切り替わります。

②全銀 TCP/IP

宛先が変わる時に、全ての上位サーバーとの接続を切断し、切り替わった上位サーバーに接続を確立して伝送が切り替わります。

注意)

シリアルポート毎に宛先上位サーバーが異なる場合に 1 か所の宛先を変更した場合に変更を行わない上位サーバーの接続も切断されます。

③全銀 TLS

全て同一の上位サーバーとの伝送になりますので、接続を切断し、切り替わった上位サーバーに接続を確立して伝送が切り替わります。

2. 3. 2. 8 アクセスログの転送

TLS のアクセスがあった場合に正常接続や、TLS のハンドシェイク時の異常で接続できない場合に、アクセス元 IP アドレス情報も含めてログ転送ができます。

同様に SNMP の TRAP としても伝送できます。

2. 3. 2. 9 SC-8279 での本番・予備基板

SC-8279 では筐体を実装する際に本番基板と予備基板の構成をとることができます。

設定情報を引き継ぐことで本番基板複数枚に対して 1 枚の予備基板を共用することができますが全銀 TLS で使用する場合、本番基板 1 枚に対して予備基板 1 枚の構成となりますのでご注意ください。

設定情報についても証明書関連の情報引継ぎができませんので、事前に同一の情報を設定しておく必要があります。

2. 3. 2. 10 全銀 TLS(TCP/IP)使用時の上位サーバー宛て TCP ポート番号

全銀 TLS(TCP/IP)使用時に UST からコネクション要求時のソースポート番号は 997 となります。

IXSAM/WINSAM の term_def.dat の UST 定義にある 999:999 を 999:997 に変更して使用してください。

2. 3. 2. 11 UST での同一基板のチャネル折り返しはできません

全銀 BSC 基板の場合は、同一基板内(CH1-CH2 間等)で上位サーバーからの伝送確認ができますが、全銀 TLS(TCP/IP)基板は IP アドレスが関連しますので、同一基板内での折り返しテストはできません。

2. 4 動作シーケンス

以下に SC-8279/8259 における動作シーケンスを示します。

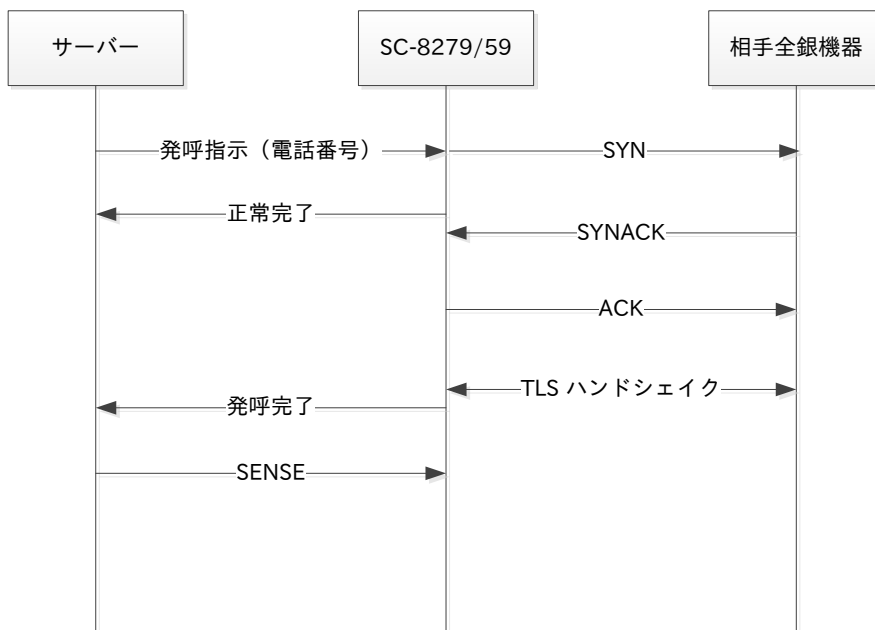
(1) 発信(クライアント機能) (SC-8279/8259 → 相手全銀機器)

サーバーからの発呼指示により、UST はクライアントとして相手全銀機器と接続確立します。

発呼指示の電話番号を、UST に登録した電話番号と IP アドレス対応設定から検索して、該当する

IP アドレスに TCP 接続要求を行います。

接続確立後、TLS ハンドシェイクが完了した時点で、上位サーバーに発呼完了を返します。



入力確認 SENSE をサーバーで制御する場合で明記しています。入力確認 SENSE は入力タイミングに使用しています。

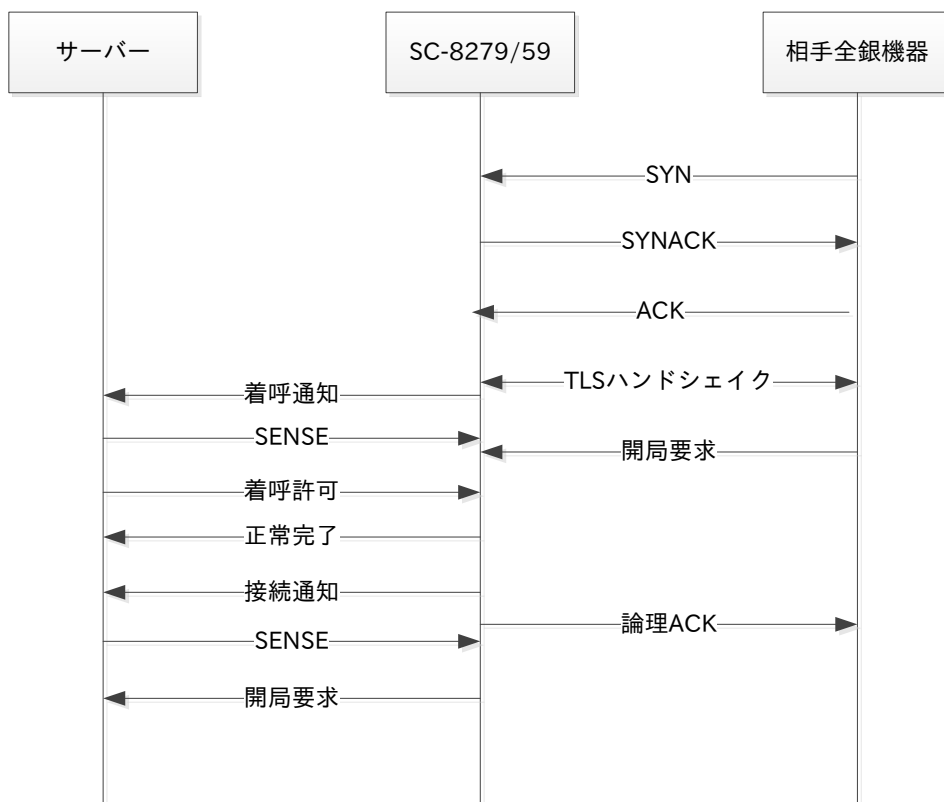
UST 設定テーブル

電話番号	IP アドレス	クライアント証明書
0312341000	192.168.0.10	ccert001
0312341500	192.168.0.11	ccert002
0312341510	192.168.0.12	なし
.	.	.

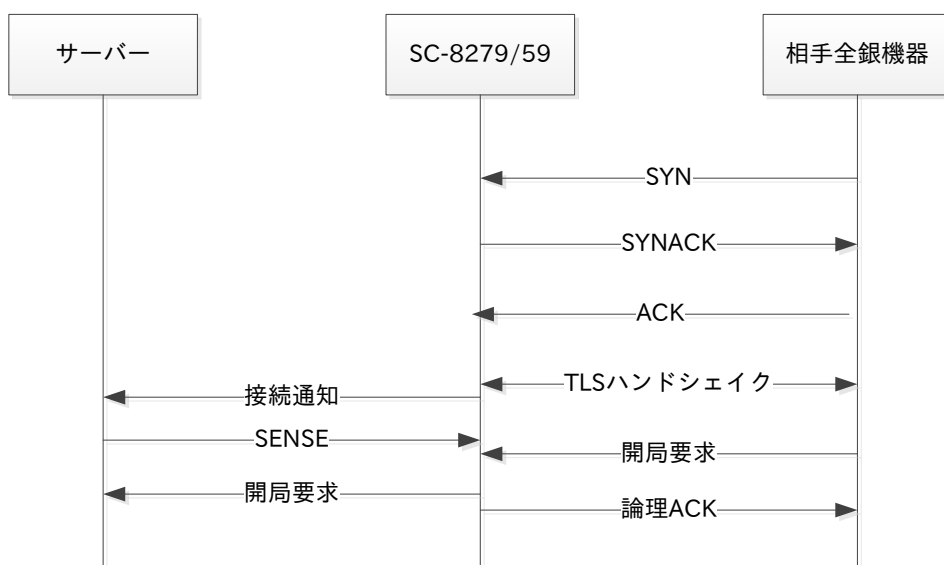
(2) 着信(サーバー機能) (SC-8279/8259 ← 相手機器)

着呼制御は可能ですが、着呼通知を入力するタイミングは、TLSのハンドシェイク完了時です。
全銀 TLS では、着呼通知に発電話番号は通知できませんが、上位サーバーの応答に従って動作します。

①着呼制御を行う場合

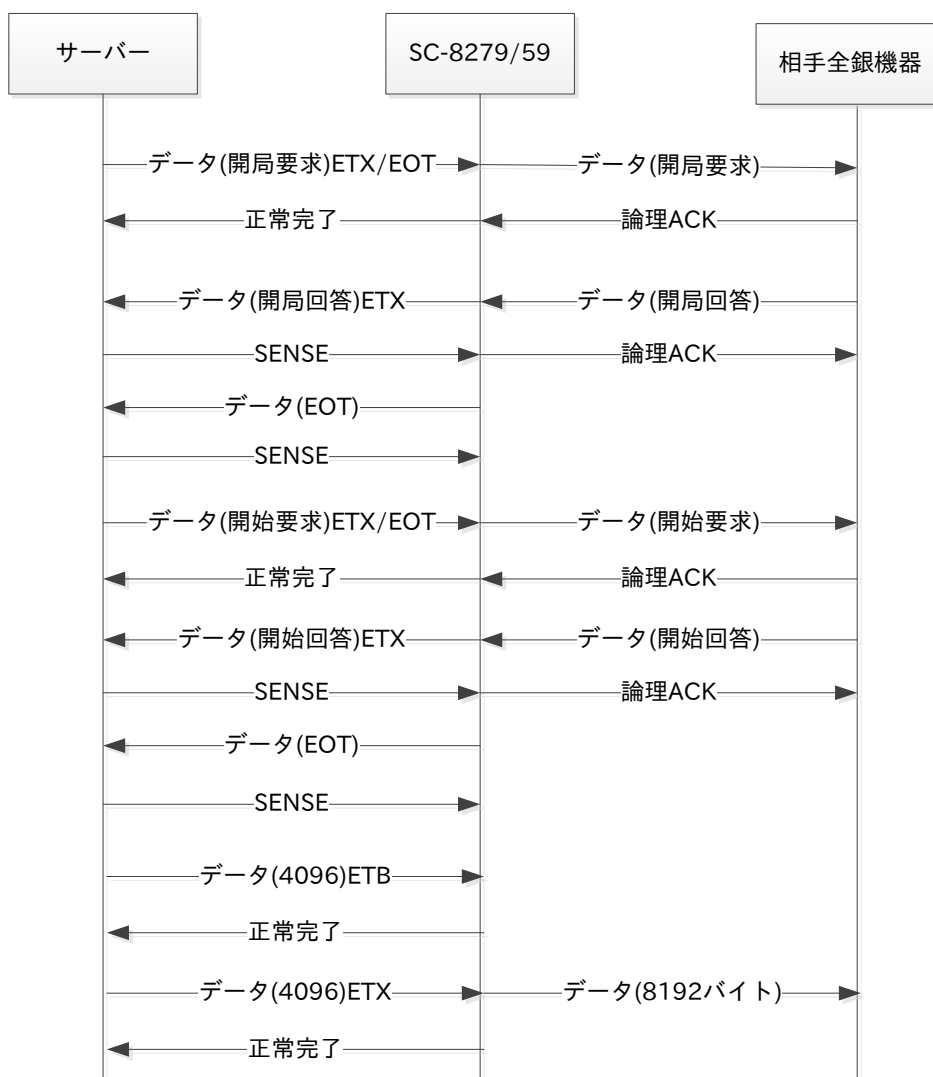


②着呼制御を行わない場合



(3) 発信により接続後のデータの流れ

UST の設定として上位サーバー最大テキスト長(4096 バイト)≦全銀 TCP/IP 最大テキスト長の動作(8192 バイト)とした場合の動作を明記します。



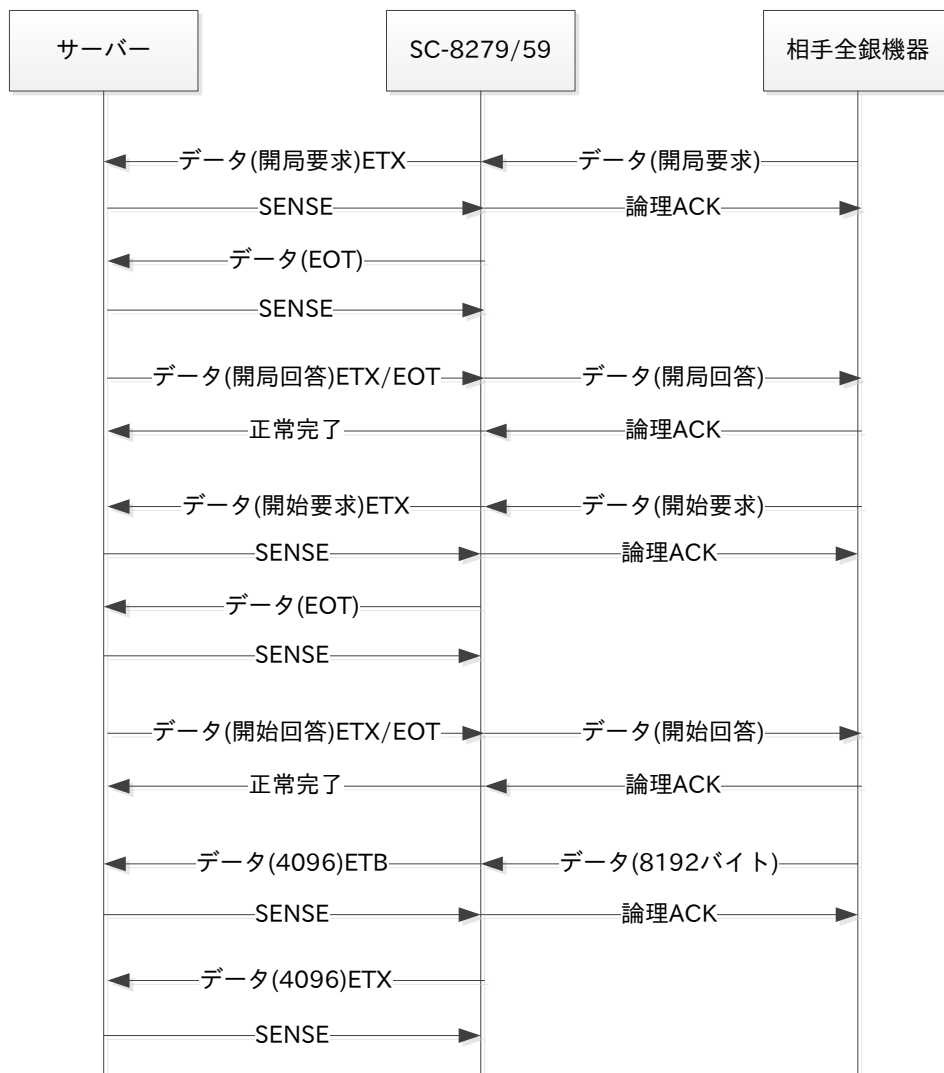
注意)

- ① デフォルトでは SENSE と論理 ACK は連携していません。
- ② 全銀制御コード(開局/開始/終了/閉局)を判断してサーバーへ EOT データを入力します。
- ③ 前提のような最大テキスト長設定の場合、サーバーから ETB/ETX データ伝送することで全銀 TCP 側へブロッキングして送信します。ETX データはブロッキングしません。
- ④ 正常完了入力タイミング
 - ・全銀制御コードの場合
相手からの論理 ACK 受信と連携しています。
 - ・ユーザーデータの場合
端末へ正常送信時に正常完了を入力します。送信できない場合は異常完了になります。

(4) 着信時のデータの流れ

UST の設定として

上位サーバー最大テキスト長(4096 バイト) ≤ 全銀 TCP/IP 最大テキスト長の動作(8192 バイト)とした場合の動作を明記します。

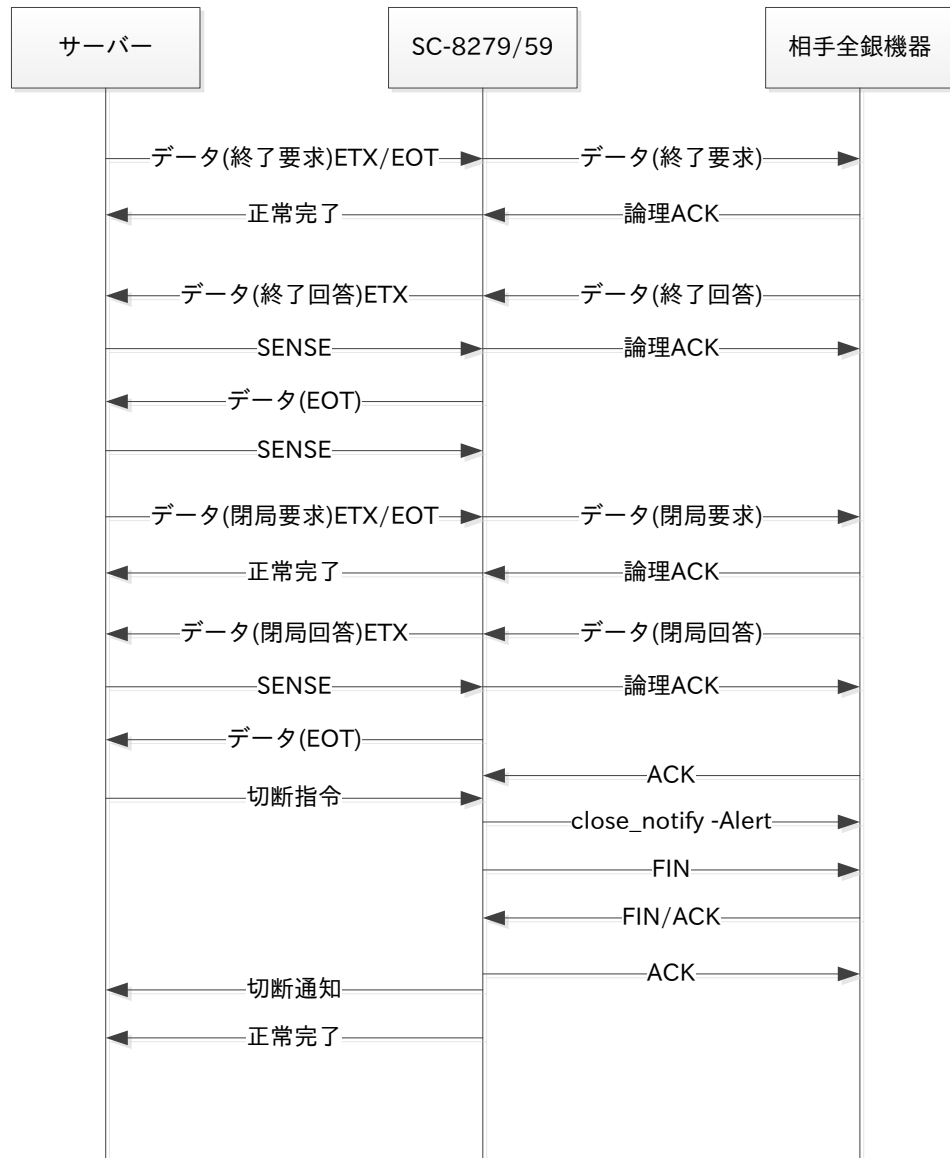


注意)

- ① デフォルトでは SENSE と論理 ACK は連携していませんが、SENSE の遅れにより UST にデータが一定量溜まると、フロー制御により論理 ACK の応答は停止します。
- ② 全銀制御コード(開局/開始/終了/閉局)を判断してサーバーへ EOT データを入力します。
- ③ 前提のような最大テキスト長設定の場合、相手から 8192 バイトのデータを ETB/ETX データにブロッキングしてサーバーへ伝送します。
4096 バイト以下のデータはブロッキングしません。
- ④ 正常完了入力タイミング
 - ・全銀制御コードの場合
相手からの論理 ACK 受信と連携しています。

(5) 切断時のデータの流れ

1) クライアントモード時切断時の動作を下記に示します。

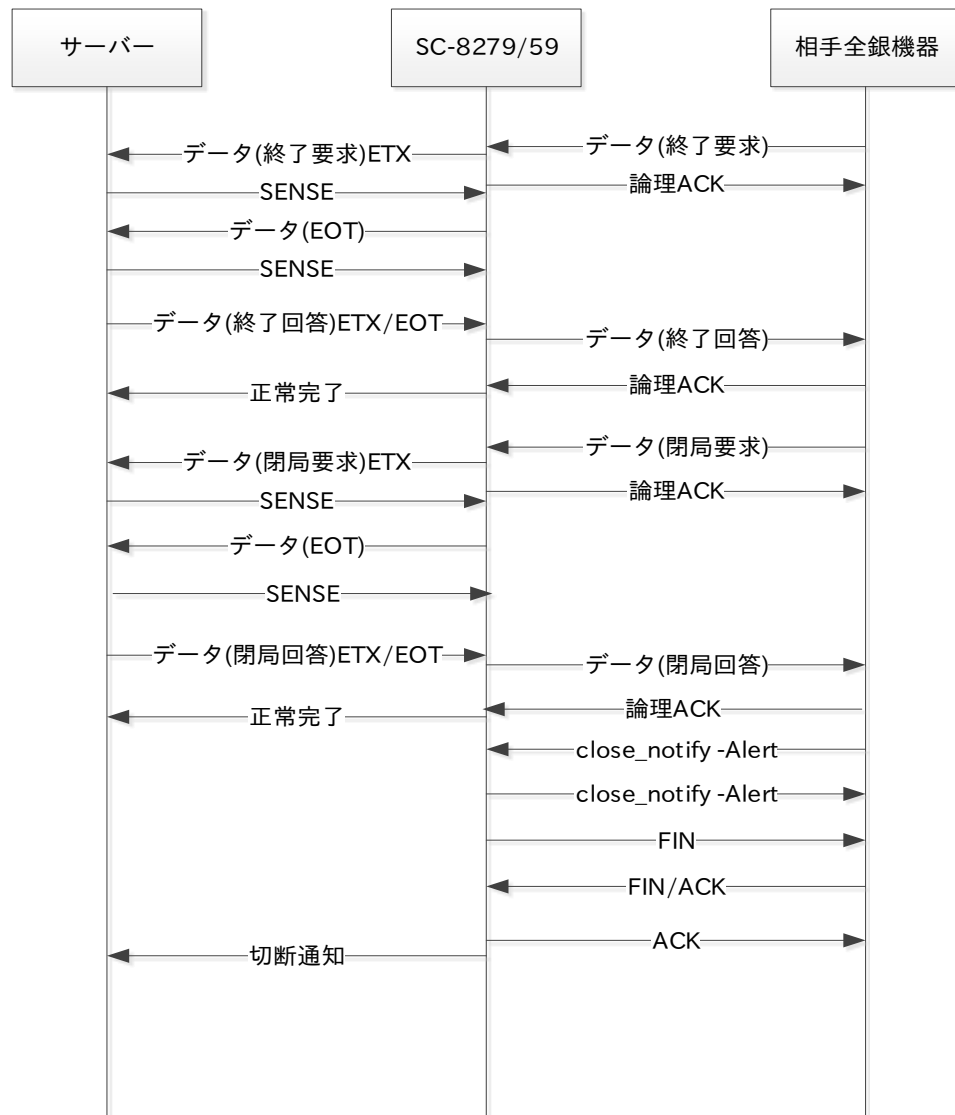


注意)

- ① デフォルトでは SENSE と論理 ACK は連携していません。
- ② 全銀制御コード(開局/開始/終了/閉局)を判断してサーバーへ EOT データを入力します。
- ③ 正常完了入力タイミング
・全銀制御コードの場合
相手からの論理 ACK 受信と連携しています。
- ④ 上位サーバーからの切断指令により、SSL/TLS の close-notify Alert を送信し、TCP コネクションを開放します

2) サーバーモード時切断時の動作を下記に示します。

相手から TLS 切断時の、close_notify-Alert 受信時は、UST からも close_notify-Alert を伝送します。



2. 5 全銀 TLS(TCP/IP)用 UST の電源投入と電源の落とし方(現行 UST との違い)

SC-8278/58 等の UST をお使いのお客様で、SC-8279/59 の全銀 TLS(TCP/IP)接続用 UST を使用する場合に、電源投入時にシステムの立ち上がりまでの時間がかかることがあります。

また、電源を落とす際の注意点などを明記しましたので確認ください。

2. 5. 1 全銀 TLS 接続用 UST の電源投入

SC-8259/79 に全銀 TLS 接続用基板を挿入した場合に、起動時間が他の通信ボード使用时よりも長く、約 60 秒かかります。

SC-8259 の場合、全銀 TLS 接続用の通信ボードが実装されていると、電源投入後前面の表示管に Initializing の表示が続き、起動後に 0901 表示に変わります。

証明書類のインストールを行いますので、1000 表示から 1001 表示後動作可能となります。

全銀 TLS の表示はその後、日付が変わった 0999 表示となり設定情報を書込む度に、1000 表示から 1001 表示となります。

2. 5. 2 全銀 TLS 接続用 UST の電源の落とし方

SC-8259/79 に全銀 TLS 接続用基板を挿入している場合は、必ずシャットダウンしてから本体の電源を落としてください。

シャットダウンせずに電源を OFF した場合、一部の情報が取得できない場合があります。

シャットダウン操作は前面キーを使用して行ってください。

(基板単位のシャットダウンは導入・運用の手引きをご参照ください)

①シャットダウンキー操作

F4 D ENT を入力すると画面表示が下記ようになります。

```
ALL SHUTDOWN OK?
      0=YES  1=NO
```

0(YES)を入力すると画面表示が下記ようになります。

```
SHUTDOWN PROCESS
              OK
```

シャットダウン中は OK が表示されず、シャットダウン処理が終了すると OK の表示に変わります。

②電源の OFF

OK の表示になりましたら裏面の電源スイッチを OFF にしてください。

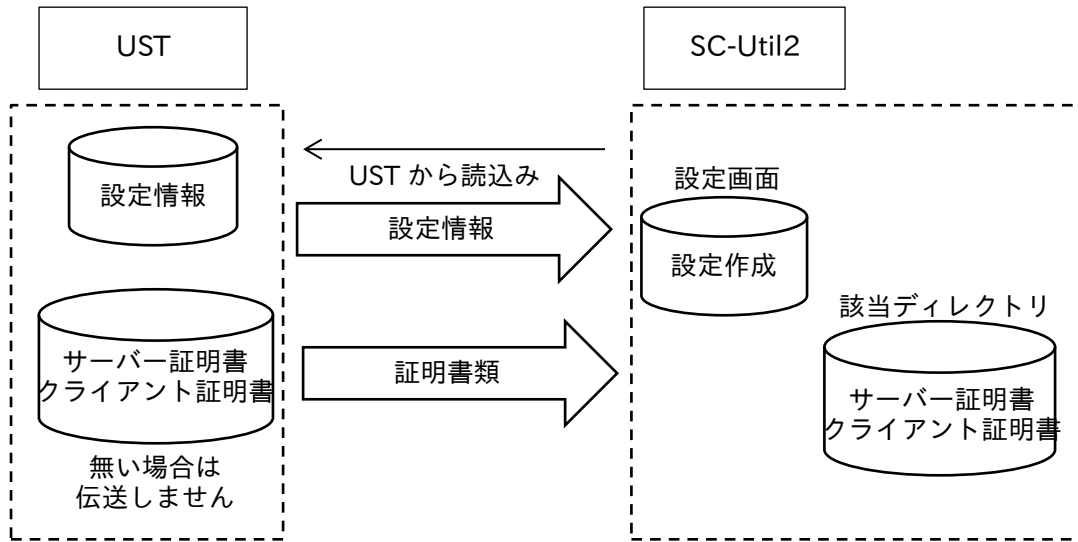
2. 6 ScUtil2 を使用して設定情報書込み時の注意点(全銀レガシー時と異なります)

全銀 TLS は、設定情報の読み込み/書き込み時に設定情報の他、サーバー証明書、クライアント証明書を毎回伝送します。

また設定情報書込み後、サーバー証明書など即時反映する項目が有りますので、操作に注意する必要があります。

2. 6. 1 UST から設定情報を読み込んでから設定変更を実施

UST 側のみに持つデフォルト設定が有るため、導入時の設定、設定済み情報の変更を行う場合、必ず UST から読み込んでから設定作業をしてください。



注意)証明書類の変更時も同様に、設定情報を読み込んでから証明書類を変更してください。

2. 6. 2 設定情報作成時の注意点

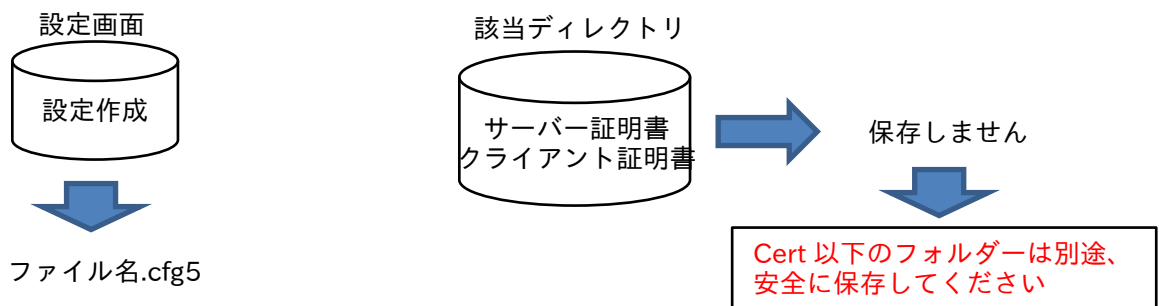
通常の設定は、SC-Util2 の設定画面から行いますが、サーバー証明書/クライアント証明書関連のファイルは、規定されたディレクトリに置いてください。

証明書の該当するディレクトリには 1 組の証明書/秘密鍵とし、2 組以上は置かないでください。

証明書を削除する場合は、削除する証明書のディレクトリを削除してください。

設定情報を保存する場合、設定画面で設定した設定情報は保存しますが、証明書類のファイルは保存しません。

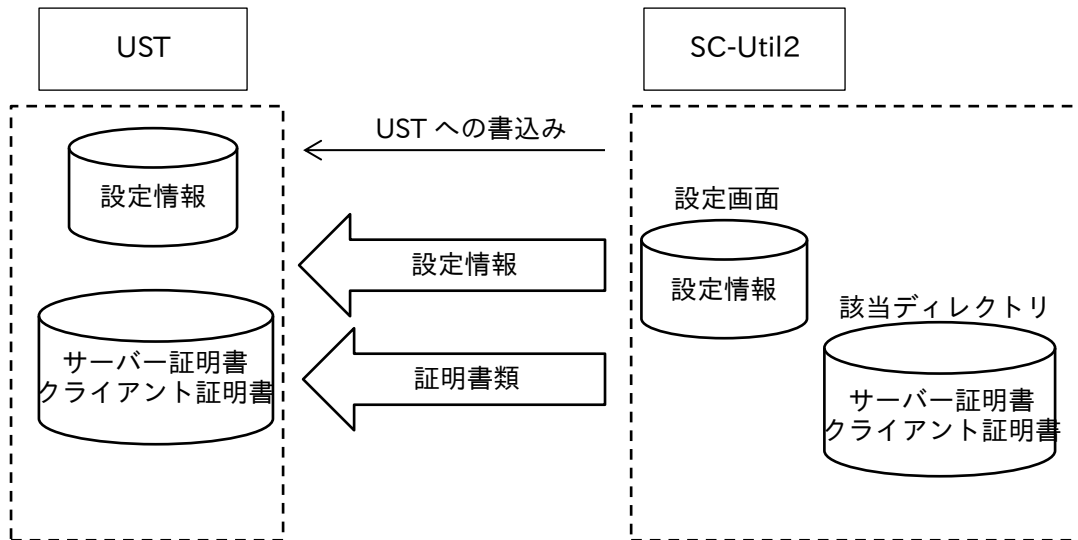
証明書類のファイルは別途保存してください。



2. 6. 3 UST への設定情報の書込み

全銀 TLS では、SCUtil2 から UST への設定情報書込み時、2.2.7 に明記した証明書類はホットスタートで反映されますので、運用中の設定変更は注意してください。

2.2.7 以外の設定情報の反映は再起動が必要です。



注意)

SC-Util2 の証明書類の該当ディレクトリに、証明書類を置いておかないと、証明書無として UST に伝送されます。

設定情報を書き込んだ時点で、証明書無として新たなコネクションを受けなくなる場合があります。

2. 6. 4 SC-Util2 終了時の注意

SC-Util2 の作業終了し、終了する場合の注意があります。

①証明書類は自動保存しません

設定情報を保存しても、証明書類は保存しませんので、別途バックアップを取り適切に管理してください。

②SC-Util2 指定の証明書フォルダーを開いたままにしないでください。

証明書類を置くフォルダーを開いている場合、証明書フォルダーの削除ができない場合があります。

残ってしまった Cert 以下のフォルダーを消去するようにしてください。

2. 7 ScUtil2 を使用してメンテナンス情報取得時の注意点

全銀 TCP/IP で ScUtil2 を使用する場合に全銀 BSC とは異なる部分がありますので下記に示します。

2. 7. 1 メンテナンス情報の取得方法

メンテナンス情報の取得はネットワーク経由での取得が可能です。

シリアルポートからは一部の情報しか取得できませんのでご注意ください。

2. 7. 2 情報取得時 TFTP を使用

ScUtil2 を使用してメンテナンス情報時に TFTP を使用します。

ネットワークのセキュリティ設定で TFTP をフィルターしている場合に正常に取得できませんのでご注意ください。

2. 7. 3 メンテナンス情報の参照

全銀 TLS で取得したメンテナンス情報は ScUtil2 のフォルダーに置かれます。

システムバージョン、ヒストリーは ScUtil2 の画面から参照することができますが、その他の情報は圧縮ファイルとして tmp フォルダーに作成されますので、解凍してテキストエディターで参照してください。

2. 8 設定情報の暗号化

全銀 TCP/IP の設定情報を ScUtil2 と連携して暗号化することができます。

ScUtil2 と UST 間の設定情報の伝送も含めセキュリティを確保することができます。

Appendix-A (全銀レガシーUST との相違点まとめ)

全銀ベーシック手順と全銀 TCP/IP での相違点を以下にまとめます。

項番	機能	全銀 TLS(TCP)	全銀 BSC
1	使用するポート番号	Listen : 999 Destination : 999 Source : 997(固定)	Listen : 999 Destination : 999 Source : 999(固定)
2	同一基板のチャンネル折り返し動作	できません	可能です
3	本番、予備基板の扱い	本番基板 1 枚に対して予備基板 1 枚。 設定引き継ぎできません	本番基板複数枚に対して 1 枚の予備基板が可能。
4	上位サーバー側との TCP 再送時間と リトライ回数(SYN パケット)	再送間隔はリトライ回数により 1,2,4,8,16 秒で 4 回リトライし 5 回目にリトライアウトとなります。 合計 31 秒です。	・ 同一ネットワーク 3 秒 4 回で 12 秒 ・ 異なるネットワーク 10 秒 4 回で 40 秒
5	上位サーバー側との TCP 再送時間と リトライ回数(データ送信後 ACK 待)	再送間隔はリトライ回数により 0.6,1.2,2.4,4.8,9.6 秒で 4 回リトライし 5 回目にリトライアウトとなります。 合計 18.6 秒です。	・ 同一ネットワーク 3 秒 4 回で 12 秒 ・ 異なるネットワーク 10 秒 4 回で 40 秒
6	SYN パケット衝突時	(TLS)セッション空きあれば 接続します。 (TCP) IP アドレスの第 4 オクテットからの大小。(デフォルト) 相手からの接続優先。(オプション設定)	後からの接続要求を優先
7	発呼指令の電話番号とサブアドレスのセパレータ	"/" 0x2F	"*" 0x2A
8	SCUtil2 使用時の伝送	メンテナンス情報取得時に tftp を使用します。 tftp 伝送ができるようにポート番号 69 を透過できるようにしてください。	tftp は未使用です
9	使用するポート番号	999 サーバーとの伝送用 69 メンテナンス情報取得 その他は設定により NTP、SNMP、FTP を使用	999 サーバーとの伝送用 その他は設定により NTP、SNMP を使用
10	設定情報の反映タイミング	(TCP)再起動 (TLS)証明書関連は即時反映 その他の設定は再起動後。	再起動後

Appendix-B (規約)

その他の規約	内容
全銀プロトコル	全銀協標準通信プロトコル -TCP/IP 手順・広域 IP 網-

Appendix-C

表 1. 発呼完了詳細ステータス情報一覧

コマンド名	CMD	PUA	ユーザーデータ部		意味
発呼完了正常	0A	00	00	00	発呼後、TCPコネクション接続
発呼完了異常1	0A	01	01	01	ダイヤル番号フォーマット・桁数異常
			03	04	着信中
			04	01	接続中
発呼完了異常2	0A	02	06	02	相手機器無応答 (コネクション異常)
			70	01	SSLタイムアウト
			70	02	SSL証明書の不備
			7X	XX	その他SSL通信異常

表 2 通信異常終了通知のPhase、Event一覧

・ Phase コード

	意味
07h	接続中

・ Event コード

	意味
50h	出力データ (ETX または ETX+EOT)
51h	出力データ (ETB)
52h	出力データ (EOT)

「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