

石化協版

「全銀協標準通信プロトコル(TCP/IP 手順・広域 IP 網)」

利用ガイドライン SSL/TLS 方式編

v1.1.0

石油化学工業協会

情報通信委員会

目 次

1. 要旨	2
1.1. はじめに	2
1.2. 利用ガイドライン作成の背景と目的	2
1.3. 本ガイドラインが対象とする接続方式	2
2. プロトコル概要	3
2.1. プロトコル概要	3
2.2. セキュリティ対策の代表的な方式と特徴	4
3. SSL/TLS 方式におけるプロトコル実装ガイドライン	6
3.1. SSL/TLS 方式の概要	6
3.2. 対応方法	7
3.3. IP アドレス	7
3.4. TCP ポート番号	8
3.5. 認証方法	8
3.6. エラーの扱い	9
3.7. 脆弱性対応	9
3.8. 証明書	10
3.9. まとめ	12
4. SSL/TLS 方式における運用ガイドライン	13
4.1. 当事者間事前取り決め事項	13
4.2. 証明書の種類	14
4.3. 証明書の運用	15
4.4. PSTN 網特有機能の代替え	17
4.5. BCP システムへの対応	17
ご参考情報	19
試験の目的	19
事前調整	20
試験項目	21
5. 改訂履歴	22

1. 要旨

1.1. はじめに

総務省は「固定電話網の円滑な移行の在り方」～最終形に向けた円滑な移行の在り方～^[1]について情報通信審議会電気通信事業政策部会に諮問を行い、2017年9月27日、二次答申を受けたことを発表した。これを踏まえ、同年10月17日、東日本電信電話・西日本電信電話(NTT東西)は「固定電話のIP網への移行後のサービス及び移行スケジュールについて」^[2]をプレス発表した。

本件について石油化学工業協会(石化協)情報通信委員会の活動としては、2013年にCEDI小委員会で問題が提起され、2015年度からは専門のワーキンググループを立ち上げて、総務省、インターネットEDI普及推進協議会(JiEDIA)、NTT東西、関係業界団体等と協調し、石油化学業界で利用しているEDI方式の対応方針の検討を進めてきた。

2018年5月22日の第27回CEDI/ITフォーラムにおいて、固定電話網のIP網移行における石油化学業界EDIの対応方針を提示した。

- ☐ 通信フォーマット : 通信フォーマットは現状維持
- ☐ 通信プロトコル : 全銀協標準通信プロトコル(TCP/IP 手順・広域 IP 網)
- ☐ セキュリティ : 原則、クライアント証明書・サーバ証明書を採用
- ☐ 推奨スケジュール : 2022年12月までの完了を目標

1.2. 利用ガイドライン作成の背景と目的

本書は、上記対応方針に従い、石油化学業界で利用しているEDI方式を実施しているユーザ企業が通信フォーマット、運用ルールは現行を踏襲し、インターネット経由の通信プロトコルに切り替えを安定かつ円滑に実現するためのガイドラインであり、インターネットEDI普及推進協議会(JiEDIA)発行の『「全銀協標準通信プロトコル(TCP/IP 手順・広域 IP 網)」利用ガイドライン SSL/TLS 方式編 v2.0.1』^[3]をベースとして作成したものである。

1.3. 本ガイドラインが対象とする接続方式

「全銀協標準通信プロトコル(TCP/IP 手順・広域 IP 網)」-「SSL/TLS 方式」とする。

2. プロトコル概要

2.1. プロトコル概要

全銀協標準通信プロトコル(TCP/IP 手順・広域 IP 網)(※以降、インターネットに対応した全銀 TCP/IP 手順と記す※)は、INS ネットデジタル通信モード提供終了を受けて、従来の全銀 TCP/IP 手順をインターネットや IP-VPN などの広域 IP 網(*1)でも利用可能とするために策定された。

インターネットに対応した全銀 TCP/IP 手順が従来の全銀 TCP/IP 手順と異なるのは、

- ・回線に広域 IP 網(インターネットや IP-VPN)を利用すること
- ・暗号化などのセキュリティ対策が施されていること

の2点である。仕様の差異を以下の表にまとめる。

	従来の全銀 TCP/IP 手順	インターネットに対応した全銀 TCP/IP 手順
適用回線(*2)	公衆回線、ISDN 回線	インターネット、IP-VPN
データリンク仕様	PPP	規定なし
TCP ポート番号	5020	5020 ただし、従来の全銀 TCP/IP 手順との変更運用を考慮して、「5020」以外のポート番号を使用する場合もある
IP アドレス	IPv4 のグローバルアドレスかプライベートアドレス	IPv4 のグローバルアドレスかプライベートアドレス、または IPv6 のグローバルアドレス
暗号化接続方式	規定なし ※必要性がなかったため	全銀の電文シーケンスや電文制御手順に影響を与えないセキュリティ対策方式をとることを前提とする

図表 1 プロトコル仕様差異

*1 IP-VPN は本来閉域 IP 網だが、「全銀協標準通信プロトコル(TCP/IP 手順・広域 IP 網)」では“広域 IP 網”という表現をしているため、本ガイドラインでも同じように表記する。

*2 適用回線の記載については『全銀協標準プロトコル -TCP/IP 手順・広域 IP 網-』の「Ⅱ.ネットワーク基準⇒1.適用回線仕様⇒(1)適用回線」に基づき記載。

『全銀協標準プロトコル -TCP/IP 手順・広域 IP 網-』については、出典([4])を参照。

2.2. セキュリティ対策の代表的な方式と特徴

回線を含めた具体的なセキュリティ対策方式として、

- ・SSL/TLS
- ・インターネット VPN
- ・IP-VPN

の3つが挙げられるが、石化協としては、SSL/TLS 方式を採用する。

	SSL/TLS 方式	インターネット VPN 方式	IP-VPN 方式
適用回線	インターネット	インターネット	通信事業者提供の閉域 IP 網
接続方式	リモートアクセス	サイト間接続、リモートアクセス	サイト間接続
動作環境	SSL/TLS に対応した全銀 TCP/IP 手順パッケージソフトウェア、もしくは SSL アクセラレータ機器	VPN 接続用ソフトウェアもしくは機器	VPN 接続用機器
接続性	ソフトウェア・機器を選ばずに接続が可能	メーカーが異なる機器の場合、接続できない可能性あり	接続相手先も同じ通信事業者が提供する IP-VPN サービスへの接続が必要
認証方式	電子証明書	電子証明書、共通鍵(パズフレーズ)、ID・パスワードなど	—
通信品質	ベストエフォート型	帯域保証型／ベストエフォート型	帯域保証型／ベストエフォート型

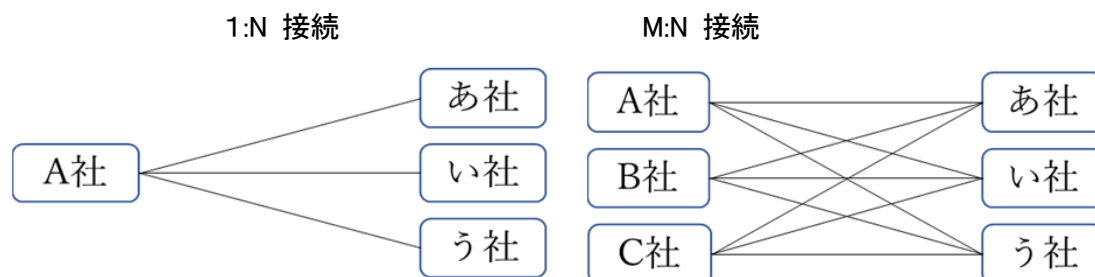
図表 2 セキュリティ対策方式の差異

●SSL/TLS 方式の特徴

SSL/TLS 方式は、HTTP における HTTPS と同様に、全銀 TCP/IP 手順を SSL/TLS で暗号化したものである。この方式は SSL/TLS に対応した全銀 TCP/IP 手順をサポートしているパッケージソフトウェアを使用するか、SSL アクセラレータと従来の全銀 TCP/IP 手順をサポートしているパッケージソフトウェアを組み合わせることで利用可能となる。認証方式には、電子証明書を利用するため、少なくとも着信側(サーバ側)は電子証明書の取得が必要となる。TCP ポート番号は、センター側にて決定し、接続を開始する際に利用者側へ通知が必要である。利用者は、センター側の設定にあわせて、ファイアウォール越えなどの設計をおこなう必要がある。

EDI 利用において接続先ごとに接続方式が異なると、接続方式ごとにシステムを構築することとなり、企業の EDI 構築時の負担が増える。また、運用におけるコストも増えることとなる。

例えば自社が複数の接続先と EDI によるデータ交換を行っており、相対する接続先も別の複数社と EDI によるデータ交換を行っている状態を「M:N 接続」と呼ぶ。



図表 3 1:N 接続と M:N 接続

M:N 接続で EDI を実施する場合、自社や接続先が複数の方式に対応しなくても良いように足並みを揃えることが重要である。インターネット VPN 方式や IP-VPN 方式では接続先が専用の接続環境を構築する必要があるが、SSL/TLS 方式では専用環境が基本的に不要のため、接続性が高い。(接続方式の乱立が避けられる。)EDI 利用企業全体の最適化を考えた場合、石化協でも採用した SSL/TLS 方式が有利となる。

3. SSL/TLS 方式におけるプロトコル実装ガイドライン

3.1. SSL/TLS 方式の概要

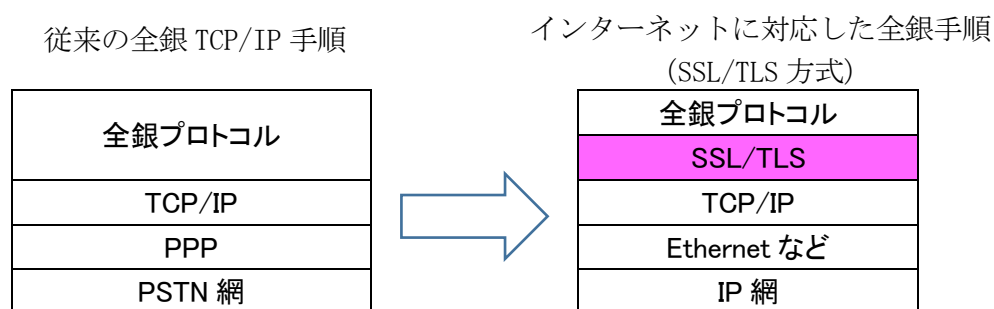
SSL/TLSは、インターネットを利用する際のセキュリティリスクとなる「盗聴」「改ざん」「なりすまし」「否認防止」のうち、「盗聴」「改ざん」「なりすまし」について防止する機能をもっている。

手順名	従来の全銀 TCP/IP 手順	インターネットに対応した全銀 TCP/IP 手順 (SSL/TLS 方式)
適用回線	公衆回線・ISDN 回線	インターネット
盗聴	なし ※ただし、公衆回線を利用するため盗聴されにくい。	暗号化により防止
改ざん	なし ※ただし、公衆回線を利用するため改ざんされにくい。	MAC (Message Authentication Code) を用いた改ざん検知が可能
なりすまし	PPP 認証、電話番号認証、センターコードなどの全銀パラメータによる認証	電子証明書による認証、センターコードなどの全銀パラメータによる認証
否認防止	なし	なし

図表 4 SSL/TLS 方式のセキュリティ対策比較

従って、SSL/TLSを使えばインターネット上で安全に通信を行うことができる。ただし、プロトコルバージョンや暗号アルゴリズムは常に進化しているため、セキュリティリスクを回避するために技術的な追従は必要である。

インターネットに対応した全銀TCP/IP手順のセキュリティ方式にSSL/TLSを用いる場合、プロトコルレイヤは下記のイメージとなり、全銀プロトコルの電文シーケンスや電文制御手順に影響を与えることはない。



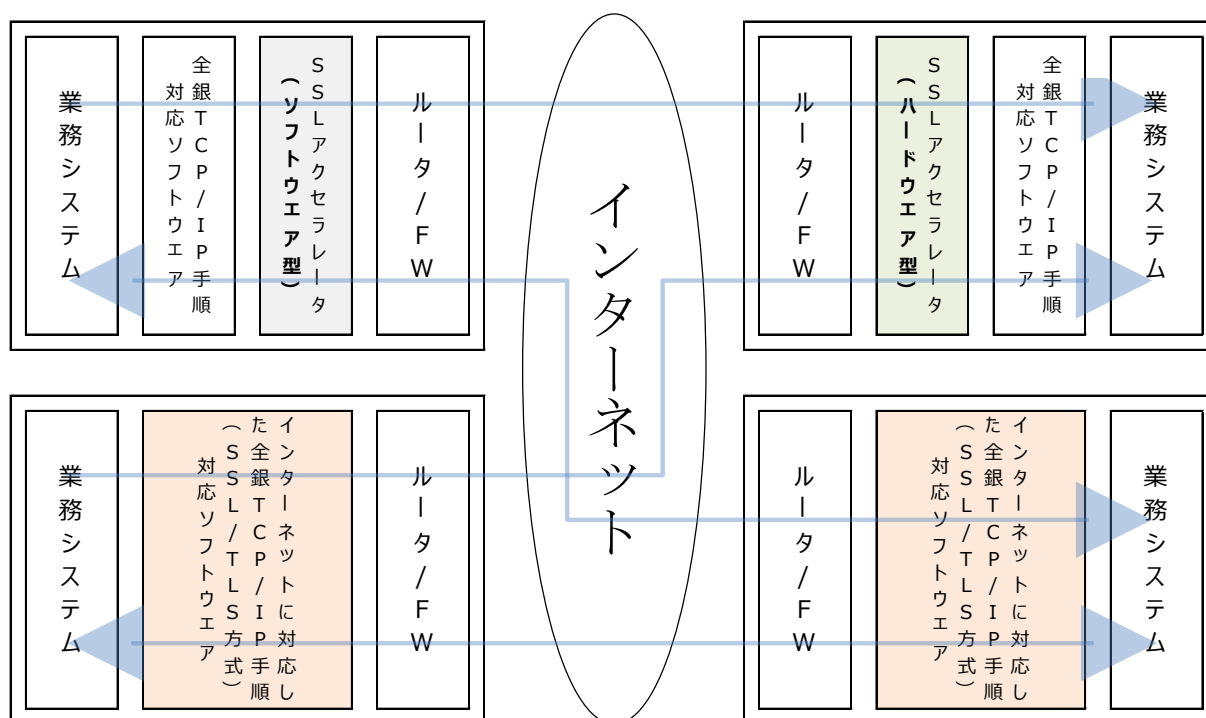
図表 5 プロトコルレイヤ図

3.2. 対応方法

インターネットに対応した全銀TCP/IP手順を用い、セキュリティ方式としてSSL/TLSを利用する場合、

- ① SSL/TLSに対応した全銀TCP/IP手順パッケージソフトウェアで対応する
- ② SSLアクセラレータで対応する

という2つの対応方法があり、これらは相互に接続が可能となっている。なお、SSLアクセラレータはハードウェア型とソフトウェア型のどちらを用いても構わないが、一般的にはハードウェア型の方がソフトウェア型に比べ処理性能が優れている。ただし、ハードウェア型は着信側（サーバ側）機能のみに対応している場合が一般的である。



図表 6 SSL/TLS 方式による接続方法

3.3. IP アドレス

従来の全銀TCP/IP手順では、プライベートIPアドレスを使用していたケースが多かったが、インターネットを利用する場合はグローバルIPアドレスが必須となる。特に、着信側（サーバ側）は、発信側（クライアント側）がインターネット経由で接続できるように、グローバルIPアドレスを割り当てたサーバシステムをインターネット上に公開する必要がある。発信側（クライアント側）については、ネットワークの設定を考慮しておけばLAN内からの接続も可能であるため、インターネット上にシステムを公開する必要はない。また、基本的には発信側（クライアント側）のグローバルIPアドレスを着信側（サーバ側）に通知する必要もない。

さらに、ホスト名による接続についても特に制限がないため、着信側（サーバ側）がホスト名で運用することも可能である。

なお、IPアドレスのバージョンはIPv4を基本として扱い、これに加えてIPv6にも対応できていることが望ましい。

3.4. TCP ポート番号

従来の全銀TCP/IP手順では通信ポート番号として「5020」番が指定されている。インターネットに対応した全銀TCP/IP手順においても同様に「5020」番を使用するが、インターネットEDI移行期においては、両プロトコルが混在する期間が発生すると予想される。

プロトコルごとにサーバを用意できる場合はポート番号が同じでも問題はないが、同一サーバで運用する場合はポート番号を分ける必要がある。また、クライアント認証のあり／なしによってもポート番号を分ける必要があり、「5020」番以外のTCPポート番号の利用についても考慮する必要がある。

例えば、SSL/TLS方式のTCPポート番号として「5020」番とは別に、「55020」番（クライアント認証なし）と「55021」番（クライアント認証あり）を用意して問題を回避するようなことが考えられる。（ただし「55020」「55021」は動的ポートの範囲に含まれる可能性が高いため、ポート番号の事前予約など、競合しないような対策が必要となる）

プロトコル	認証方法	ポート番号
従来の全銀 TCP/IP 手順	—	5020
インターネットに対応した 全銀 TCP/IP 手順 (SSL/TLS 方式)	サーバ認証のみ	55020
	サーバ認証／クライアント認証	55021

図表 7 複数 TCP ポート番号利用例

こうした運用を検討する場合は、複数のTCPポート番号管理を可能とする設計、TCPポート番号の変更が行える事を前提とした設計とすべきであり、これを前提としたアプリケーション開発を行うことを強く推奨する。

3.5. 認証方法

セキュリティ強化対応を目的に以下2パターンの認証方式を検討した。

- ◆ 「サーバ認証＋クライアント認証＋全銀認証」方式
- ◆ 「サーバ認証＋全銀認証」方式

石油化学業界としては、上記パターンの内「サーバ認証＋クライアント認証＋全銀認証」方式の採用を強く推奨する。サーバ認証＋全銀認証方式については使用を推奨しない。

■ 認証方式説明

1. サーバ認証：サーバ証明書を用いた認証※¹
2. クライアント認証：クライアント証明書を用いた認証※¹

※¹. 各証明書はいずれも信頼される第三者機関が発行した証明書を用いる事を推奨する

3. 全銀認証：全銀プロトコルで定められた項目値の相互確認

■全銀認証必須項目

石油化学業界で利用する全銀認証としては、以下項目の相互確認を必須とする。

項目名	備考
当方センター確認コード	Hex(7byte)で設定すること
相手センター確認コード	Hex(7byte)で設定すること
(全銀)パスワード	Hex、Bin、Char(6byte)で設定すること
(全銀)ファイル名	Hex、Bin、Char(12byte)で設定すること
ファイルアクセスキー	Hex、Bin、Char(6byte)で設定すること

※Hex:ヘキサデシマル(16進数)、Bin:バイナリ(2進数)、Char:キャラクタ

図表 8 全銀認証必須項目一覧

※項目名称および、備考については『全銀協標準プロトコル -TCP/IP 手順・広域 IP 網-』の「Ⅶ.フォーマット仕様及びⅧ.コード体系仕様」に基づき記載。

『全銀協標準プロトコル -TCP/IP 手順・広域 IP 網-』については、出典([4])を参照。

上記 5 項目以外の設定については、全銀協標準通信プロトコル(TCP/IP 手順・広域 IP 網)出典([4])に記載されている内容をベースに当事者間で事前に確認し、合意した上で相互確認項目として用いることとする。

3.6.エラーの扱い

各レイヤで発生したエラーはそのレイヤで処理することとし、全銀プロトコル側で変更が必要になるようなエラーハンドリングは行わないこととする。

例えば、SSL/TLSレイヤにおいてハンドシェイク時にエラーが発生した場合、そのエラーはSSL/TLSレイヤにおけるエラーとして処理を行うこととし、全銀プロトコル側にエラーコードを新設するような処理の追加実装は行わない。

3.7.脆弱性対応

インターネットを取り巻く環境は日々変化しており、悪意を持った利用者による新たなセキュリティリスクが現れることは珍しくない。その結果、各種プロトコルや暗号化アルゴリズムも日々進化を続けており、都度対応が必要である。

石油化学業界として、インターネットに対応した全銀TCP/IP手順を使用する場合、脆弱性のある暗号アルゴリズムを無効にできるなど、プロトコルバージョンや各種アルゴリズム・鍵長を制限できるようなパッケージソフトウェアもしくは、同等の機能を保持したインターネットに対応した全銀TCP/IP手順を提供するサービスを利用することを強く推奨する。また、常に新しいプロトコルバージョンの追従を心がけ、セキュリティリスクに対応することを推奨する。

■暗号化通信プロトコル(SSL/TLSバージョン)一覧

バージョン	利用可否	備考
SSL v3.0	×	セキュリティ脆弱性リスクがあるため利用禁止
TLS v1.0	×	セキュリティ脆弱性リスクがあるため利用禁止
TLS v1.1	×	セキュリティ脆弱性リスクがあるため利用禁止
TLS v1.2	○	採用を強く推奨
TLS v1.3	○	採用を推奨

※上記一覧情報は2022年1月31日時点のもの

図表 9 暗号化通信プロトコル(SSL/TLS バージョン)一覧

■暗号スイート一覧

TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256

※上記一覧情報は2018年09月06日時点のもの

図表 10 暗号スイート一覧

石油化学業界としては、上記暗号化通信プロトコルと暗号スイートとの組み合わせを用いた形でのインターネットに対応した全銀TCP/IP手順の利用を強く推奨する。

ー暗号化通信プロトコル＋暗号スイート組み合わせ例ー

TLS v1.2 + TLS_RSA_WITH_AES_256_CBC_SHA256

なお、本書に掲載されている情報はそれぞれ註釈ある日付時点のものとなるため、最新情報について以下に記載する参考WEBサイトなどを確認し、当事者間で合意の元、最新版への追従を行っていくことを強く推奨する。

ー参考WEBサイトー

IPA SSL/TLS暗号設定ガイドライン～安全なウェブサイトのために(暗号設定対策編)

https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

<https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3001-2.0.pdf>

3.8. 証明書

アプリケーション側に求める証明書管理機能を実装する際は、以下の項目について特に注意されたい。

(1) 更新時期の通知

証明書の更新時期が近づく(一般的に1ヶ月から3ヶ月前)と証明書発行機関から更新についての案内が送られてくるが、担当者変更などで案内を見落としてしまうなどの懸念がある。

こうした事象を未然に防ぐ事を目的として、アプリケーション側では更新時期が近付いていることがわかるような設計を用いる事を推奨とする。

なお、CA証明書や中間CA証明書についても同様の対応をとれるようにしておく。

(2) 更新期間のオーバーラップ

証明書の更新時を意識して、アプリケーション側で更新前証明書と更新後証明書をオーバーラップして保持できるような設計を推奨する。

これは、例えば接続先が1社(1対1接続)しかない場合であれば、2社間で調整したタイミングで同時に更新することが可能だが、接続先が複数社(1対N)となる場合、全社同時に更新することは難しい。そのため、新旧証明書のオーバーラップ期間を設けることとする。

(3) セキュリティ証明書管理

石油化学業界としては、信頼されている第三者機関が発行するセキュリティ証明書(サーバ証明書および、クライアント証明書)を用いることを前提とする。

発信側(クライアント側)アプリケーションについては、他業界とのインターネットEDI接続業務を加味し、クライアント証明書を複数登録でき、かつ接続先単位に切り替えられる仕組みを持てるよう設計することを推奨する。

なお、これは以下3点の懸念事項への対応を目的としたものである。

1. 複数業界にわたってEDIを利用する場合、業界ごとに用いる証明書(ルート、中間など証明書発行機関の認証局証明書含む)が異なる可能性があること
2. 着信側(サーバ側)が独自証明書(例: 自己認証証明書)を利用する(※石化協としては認めていない運用)可能性があること
3. 急な証明書変更要望(例: 認証局変更)にも柔軟に対応できるように備えること

(4) 失効

証明書の秘密鍵が漏洩した場合など、セキュリティリスクが高まる状況に至った場合は、緊急で証明書の失効作業を実施する事になる。一般的には証明書の発行機関から、失効リスト(CRL)を入手できるため、失効リストの取り込みや失効している証明書の認証拒否など、失効についての対応ができる機能を有するアプリケーションを利用することを強く推奨する。

3.9.まとめ

SSL/TLS方式のプロトコル利用ガイドラインとして、これまで記載した内容の要点を下表にまとめる。

分類	対応のポイント	着信側	発信側
IP アドレス	IPv4(必須)・IPv6(推奨)に対応していること。	○	○
TCP ポート 番号	任意のポート番号を設定できること。 ※発信側(クライアント側)は接続先毎に設定できること。	○	○
SSL/TLS	認証レベル(サーバ証明書+クライアント証明書+全銀認証)を利用できること。	○	○
	SSL/TLS バージョン・石化協指定の暗号スイートを選択できること。 脆弱性のあるアルゴリズム等を利用不可にできること。 ※発信側(クライアント側)は接続先毎に選択できること。	○	○
証明書	証明書の有効期限切れを事前に通知できること。	○	○
	証明書のオーバーラップ登録が可能であること。	○	○
	接続先毎に、認証で使用するクライアント証明書を選択できること。	—	○
	証明書の失効リスト登録が可能であること。	○	○

図表 11 SSL/TLS 方式対応のポイント

4. SSL/TLS 方式における運用ガイドライン

4.1. 当事者間事前取り決め事項

実際に SSL/TLS 方式を運用するに当たっては、事前に詳細を取り決めておくべき事項が幾つかあり、それによりセキュリティレベル、運用方法が決まるため、通信を行う当事者間に相互で取り決め(認識あわせ)をしておくことを推奨する。

以下に石化協にて想定する SSL/TLS 方式運用に向けた事前相互確認事項を記載する。

■事前相互確認事項

相互確認項目	概要	確認内容
TLS のバージョン	第 3 章参照	石化協推奨の TLS バージョンを選択しているか
暗号スイート	第 3 章参照	石化協推奨の暗号スイートを選択しているか
認証方法	第 3 章参照	石化協推奨の「サーバ認証＋クライアント認証＋全銀認証」を選択しているか
証明書チェーン※ (サーバ証明書)	証明書のどこまでを認証するか ◆基本は当事者間で合意のもと対象範囲を取り決め運用するものとする ◆事前に安全な方法で入手した証明書を前提としてチェーンチェックを行う	証明書チェーンをどこまで認証するか
証明書チェーン※ (クライアント証明書)	証明書のどこまでを認証するか ◆基本は当事者間で合意のもと対象範囲を取り決め運用するものとする ◆石化協では認証局証明書とのチェーンチェックを必須とする ◆クライアント認証時の証明書内容のチェックについては、当事者間の合意により取り決めるものとする。	証明書チェーンをどこまで認証するか

図表 12 事前相互確認一覧

※「証明書チェーン」については、後述の 4.3(4)を参照のこと

4.2. 証明書の種類

証明書(サーバ/クライアント)には、パブリック証明書と特定用途向け証明書(以降、本書ではプライベート証明書と記載)の2種類がある。

どちらを利用するかは各企業のセキュリティポリシー次第だが、利用に際しては当事者間でよく話し合い、認識を共有した上で利用することを強く推奨する。

なお、石化協としてはセキュリティ強度(信頼性)/運用面の効率性を考慮し、パブリック証明書もしくはプライベート証明書の利用を推奨し、自己認証証明書(いわゆる「オレオレ証明書」)については利用を禁止する。

■パブリック証明書とプライベート証明書の利点と課題

	パブリック証明書	プライベート証明書	(参考) 自己認証証明書
概要	大手パブリック認証局が提供する証明書でroot/中間証明書はあらかじめWEBブラウザなどに導入されているケースが多い 例) DigicertやGMOなどで発行された証明書	特定の組織や用途のみで有効な認証局が提供する証明書。 root/中間証明書はあらかじめ導入されていない事が多く、その場合は、利用者が認証局から提供されるroot/中間証明書を自分で導入する事が必要 例) 流通BMS用証明書	証明書の信頼性が著しく低く、相手を認証する為に利用すべきではなく、石化協としては使用を禁止する
利点	<ul style="list-style-type: none"> ・セキュリティ強度が高い ・失効の取り扱いが容易 ・鍵管理(認証局証明書)が容易 	<ul style="list-style-type: none"> ・(一般的にパブリック証明書と比較して)安価 ・認証局証明書のみ確認でよい、運用が容易 	<ul style="list-style-type: none"> ・個社管理が可能 ・(表面的には)一番安価
課題	<ul style="list-style-type: none"> ・(一般的にプライベート証明書と比較して)高価 ・サーバ認証用、クライアント認証用を各々持つ必要がある ・認証局に依存する運用となる 	<ul style="list-style-type: none"> ・用途ごとに異なる証明書を準備する必要がある(証明書の統一性) 	<ul style="list-style-type: none"> ・信頼性がない ・証明書(認証局)乱立の恐れあり

図表 13 パブリック証明書とプライベート証明書の利点と課題

4.3. 証明書の運用

(1) 更新時の注意点

証明書は一定の年数(一般的に1年から3年)で更新時期を迎え、更新作業が必要になる。

(証明書を更新することによって危殆化を防ぐ目的)

更新を怠ると、接続先からの認証に失敗し通信エラーとなってしまうため、十分に注意が必要である。通常は、更新時期が近づく(一般的には1ヶ月から3か月前)と証明書発行機関から更新についての案内が送られてくる。証明書の更新は定期的が発生するため、運用管理者はあらかじめ自社、および、取引先の証明書更新スケジュールを管理しておくことが望ましい。

また、通常の更新時とは別に、「脆弱性対応による証明書の変更」が発生する場合がある。その場合、該当するCA証明書を含めたすべての証明書の変更が必要になり、その際のシステム対応・テスト・移行・対応費用の予算化などを計画的に行う必要がある。

直近では、脆弱性が露呈したSHA-1からSHA-2への移行がそれに該当するが、今後同ような対応が必要となる可能性がある。

更新時には接続テストを実施することが望ましいため、確認用のデータ種別など、前述の通り、事前に対応費用の予算化を含めた計画を検討した上で、事前にテスト環境を準備しておくことが望ましい。

(2) 更新期間のオーバーラップ

証明書更新時には、一般的に更新前証明書と更新後証明書の有効期限がオーバーラップしている場合が多い。そのため、証明書の入れ替えはオーバーラップ期間中に実施することとなる。

有効期限の異なる新旧の証明書が同時に導入できる事が望ましいが、システムのポリシー上難しい場合(新旧証明書の同時導入ができない場合)、自社・取引先と当事者間で更新タイミングを合わせる必要がある。

(3) 失効

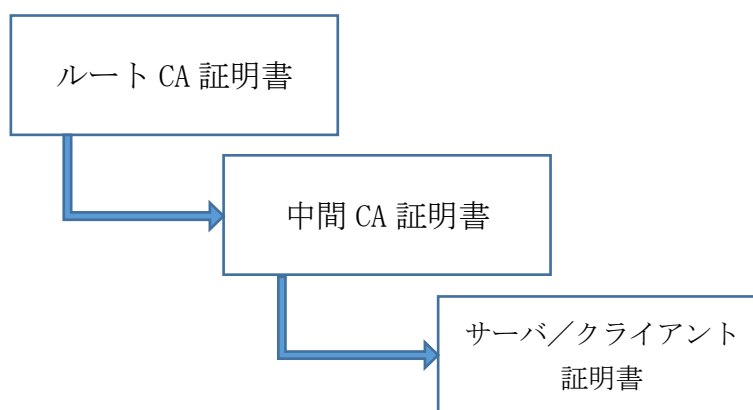
証明書が漏洩した場合など、緊急で失効作業が必要になる。一般的には証明書の発行機関から失効リスト(CRL)が取得できるため、失効リストの更新作業を定期的に行うことが望ましい。

(4) 証明書の交換について

PKI(Public Key Infrastructure)では、「信頼するCAから発行された証明書は全て信頼する」という考え方が基本である。つまり、証明書を交換するという行為は本来必要ない。ただし、データ交換においてプライベートCAを利用する場合、CA証明書は公開されていないことが多いため、CA証明書はプライベートCAから入手する必要がある。

さらに、EDI利用においては認証を強化するために、サーバ／クライアント証明書を交換するケースも考えられる。例えばサーバ／クライアント証明書の完全一致を確認する場合、事前にサーバ／クライアント証明書の入手が必要となる。

その際に証明書チェーン^[1]を交換することで、運用を簡便化することが可能である。
証明書チェーンを交換する理由は、どこまで証明書を必要とするかは接続先のセキュリティポリシー次第であり、証明書チェーンを渡しておけば接続先自身の判断で取捨選択が可能となるためである。



図表 14 証明書チェーン

証明書交換時に受領した証明書を利用するかどうかは、認証方式を決定する自社のセキュリティポリシーに依る。従って、接続先の証明書管理が必要かどうかは自社側に責任があることを認識する必要がある。

^[1] 証明書チェーンとは、図表 14 のようにサーバ／クライアント証明書から中間 CA 証明書、ルート CA 証明書を含めたものを指す。証明書発行機関によっては、中間 CA 証明書が存在しない場合もある。証明書の発行元がルート CA までたどれるため、証明書がつながっている様子をチェーン(つながれた鎖)に例えている。

4. 4. PSTN 網特有機能の代替え

PSTN網やISDN回線・TA(Terminal Adaptor)などが持つ特有機能のうち、インターネットを適用回線とすることで使用できなくなる機能や回線事業者のサービスがいくつかある。代表的なものを以下に記載する。

- ・発信番号認証
- ・代表番号
- ・転送

システム管理者は、これらの機能・サービスが利用できなくなることを意識して、移行を検討する必要がある。

(1) 発信番号認証

発信番号認証は、発信側(クライアント側)の電話番号を認証に利用する仕組みである。代替策としては、ファイアウォールによるIPアドレスフィルタリングや、証明書認証がある。インターネットはPSTN網と比べてなりすましが比較的容易であるため、クライアント・サーバともに証明書による認証の実施が望ましい。

(2) 代表番号

代表番号は、1つの電話番号への着信を複数の電話番号に振り分ける仕組みである。インターネットでは、複数セッションの同時接続が基本のため、この機能自体意識する必要がない。

※複数システムなどへの振り分け用途に使用していた場合、代替策としてロードバランサによる振り分けを検討されたい。

(3) 転送

転送は、ある電話番号にかかってきた電話を別の電話番号に転送する仕組みであり、主に災害対策やシステム切り替え時等に利用されている。代替策としては、DNS切替、クラスタ構成(仮想IPアドレス)、ロードバランサによる振り分け設定などを組み合わせて同様の仕組みを実現できるように考慮する。

4. 5. BCP システムへの対応

取引先側、および自社システムにおいて、遠隔にある2拠点でシステム運用を行うDR構成を採用している場合は、証明書運用(同一証明書が利用できるのか)についても考慮する必要がある。

取引先側、および自社システムの構成により対応方法が変わるため、この点についても考慮のうえ当事者間で事前相互確認をすることを推奨する。

■ 参考情報－証明書内容例－

項目	備考
【基本領域】	
Version	証明書規格のバージョン情報
serialNumber	証明書の一意の管理番号
Signature	署名のアルゴリズム
Validity	当該証明書の有効期限
Issuer	当該証明書発行認証局名
Subject	証明書被発行者名
subjectPublicKeyInfo rsaEncryption	公開鍵情報
issuerUniqueID	認証局の ID 利用しないのを推奨されることが多い
subjectUniqueID	被発行者の ID 利用しないのを推奨されることが多い
【拡張領域】	
authorityKeyIdentifier	認証局の識別子
subjectKeyIdentifier	被発行者の識別子
keyUsage	公開鍵の利用用途 digitalSignature (電子署名)、keyEncipherment (鍵暗号化)、dataEncipherment (データ暗号化) など
extendedKeyUsage	詳細利用用途
privateKeyUsagePeriod	秘密鍵有効期間
certificatePolicies	証明書ポリシー 運用規定への URL
policyMapping	証明書発行者とユーザのポリシー対応付け
subjectAltName	証明書被発行者の別名
issuerAltName	証明書発行者の別名
basicConstraints	CA 証明書の識別
nameConstraints	他 CA 証明時の名前識別の指定
policyConstraints	他 CA の所持する証明書ポリシーを制限
cRLDistributionPoints	CRL 配布情報 (URI など)
subjectDirectoryAtributes	証明書被発行者の属性情報
AuthorityInfoAccess	認証局へのアクセス方法 URI 指定など

出典 : <https://tools.ietf.org/html/rfc5280>

ご参考情報

インターネット EDI 普及推進協議会 (JiEDIA) 発行の『「全銀協標準通信プロトコル (TCP/IP 手順・広域 IP 網)」利用ガイドライン SSL/TLS 方式編 v2.0.1』^[3] には相互接続試験に関する「試験目的」、「事前調整」、「試験項目」についての記載がある。参考情報として本書にも転載するので、有効にご活用いただきたい。なお、インターネット EDI 普及推進協議会 (JiEDIA) 発行の資料の最新版はホームページを参照すること。

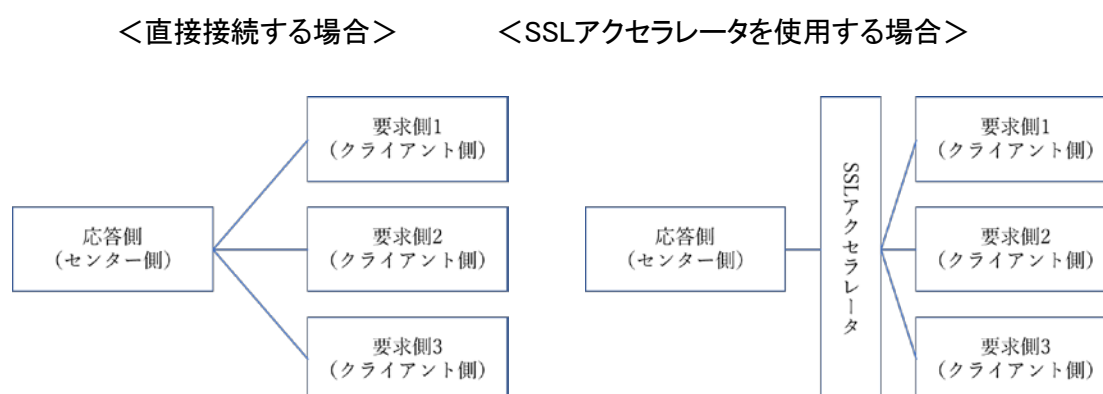
// 以降転載 //

試験の目的

広域IP網対応版全銀手順 (SSL/TLS方式) はIP網上で通信が行われるため、SSL/TLSレイヤを経由してセキュリティ対策が行われる。そのため、事前にSSL/TLSレイヤにおける接続性確認を目的とした相互接続試験を行うことが望ましい。以下にJiEDIAで行った試験の概要を参考までに記載する。

試験構成

製品単体の場合と、SSLアクセラレータを使用する場合で構成は異なるが、基本的には参加企業がそれぞれセンターとクライアント (パッケージによってはどちらか一方のみ) になり、ローカルエリアネットワーク、またはインターネット経由で一定の試験項目に従って疎通確認を実施した。



図表 15 試験構成

事前調整

試験にあたり、事前に下記事項について調査ならびに調整を実施した。また、テストに使用する証明書(今回はPKCS7形式)はプライベート証明書を各社で発行、交換を実施した。

【調査シート(センター用)】

【調査対象システム】					
エントリ番号					
企業名					
製品名					
製品バージョン					テスト時の製品バージョンを記載
通信設定	センターコード	正常系	クライアント認証なし		0パディング+エントリ番号(2桁)+00
			クライアント認証あり		0パディング+エントリ番号(2桁)+01
		異常系	クライアント認証なし		0パディング+エントリ番号(2桁)+10
			クライアント認証あり		0パディング+エントリ番号(2桁)+11
	全銀パスワード				会社名+9でパディング
	全銀ファイル名（送信）				SENDDATA+9パディング
	全銀ファイル名（受信）				RECVDATA+9パディング
	ファイルアクセスキー				会社名+9でパディング
	IPアドレス		予備(必要な場合のみ)		
	ポート番号		クライアント認証なし	55020	
			クライアント認証あり	55021	
	レコード長			251	251固定
テキスト長			256	256固定	
証明書	サーバ証明書				証明書を貼り付ける
	中間CA証明書				証明書を貼り付ける
	ルートCA証明書				証明書を貼り付ける

図表 16 機能調査シート例:応答側(センター側)

【調査シート(クライアント用)】

エントリ番号				
企業名				
製品名				
製品バージョン				テスト時の製品バージョンを記載
通信設定	センターコード			1パディング+エントリ番号(2桁)
証明書	クライアント証明書			証明書を貼り付ける
	中間CA証明書			証明書を貼り付ける
	ルートCA証明書			証明書を貼り付ける

図表 17 機能調査シート例:要求側(クライアント側)

調査項目	詳細
メーカー	
センター確認コード	
全銀パスワード	
全銀ファイル名(送信)	
全銀ファイル名(受信)	
ファイルアクセスキー	
IPアドレス	

図表 18 通信設定リスト例

試験項目

試験項目の一例を下記に記載する。

No	画面/処理	正常系/異常系	テスト項目	伝送方向	サーバ認証	クライアント認証	確認事項
1	センター通信	正常系	クライアントからサーバに対し「受信通信」を行う	S→C	○	—	・TLSハンドシェイクが行われること ・サーバに配置しているファイルがクライアントに受信されること
2	センター通信	正常系	クライアントからサーバに対し「送信通信」を行う	C→S	○	—	・TLSハンドシェイクが行われること ・クライアントから送信されたファイルがサーバに配置されること
3	センター通信	正常系	クライアントからサーバに対し「受信通信」を行う	S→C	○	○	・TLSハンドシェイクが行われること ・サーバに配置しているファイルがクライアントに受信されること
4	センター通信	正常系	クライアントからサーバに対し「送信通信」を行う	C→S	○	○	・TLSハンドシェイクが行われること ・クライアントから送信されたファイルがサーバに配置されること
5	センター通信	異常系	サーバ側のルート証明書/中間証明書がクライアントアプリケーション側に未設定の状態で行う ※クライアント側でサーバ側の中間/ルート証明書をセットしない	S→C	○	—	サーバ/クライアント側で認証エラーとなること
6	センター通信	異常系	クライアント側のルート証明書/中間証明書がサーバアプリケーション側に未設定の状態で行う ※クライアント側で間違った証明書をセットしておく	C→S	○	○	サーバ/クライアント側で認証エラーとなること

図表 19 テスト項目例: 応答側(センター側)

No	画面/処理	正常系/異常系	テスト項目	伝送方向	サーバ認証	クライアント認証	確認事項
1	クライアント通信	正常系	クライアントからサーバに対し「受信通信」を行う	S→C	○	—	・TLSハンドシェイクが行われること ・サーバに配置しているファイルがクライアントに受信されること
2	クライアント通信	正常系	クライアントからサーバに対し「送信通信」を行う	C→S	○	—	・TLSハンドシェイクが行われること ・クライアントから送信されたファイルがサーバに配置されること
3	クライアント通信	正常系	クライアントからサーバに対し「受信通信」を行う	S→C	○	○	・TLSハンドシェイクが行われること ・サーバに配置しているファイルがクライアントに受信されること
4	クライアント通信	正常系	クライアントからサーバに対し「送信通信」を行う	C→S	○	○	・TLSハンドシェイクが行われること ・クライアントから送信されたファイルがサーバに配置されること
5	クライアント通信	異常系	サーバ側のルート証明書/中間証明書がクライアントアプリケーション側に未設定の状態で行う ※クライアント側でサーバ側の中間/ルート証明書をセットしない	S→C	○	—	サーバ/クライアント側で認証エラーとなること
6	クライアント通信	異常系	クライアント側のルート証明書/中間証明書がサーバアプリケーション側に未設定の状態で行う ※クライアント側で間違った証明書をセットしておく	C→S	○	○	サーバ/クライアント側で認証エラーとなること

図表 20 テスト項目例: 要求側(クライアント側)

以上

5. 改訂履歴

版数	改訂日	改訂内容
v 1.0.0	2019 年 05 月	初版発行
v 1.0.1	2020 年 04 月	JISA EDI タスクフォースの活動が JiEDIA へ移管されたことをうけ、参考資料掲載元の内容を変更
v 1.1.0	2022 年 01 月	通信暗号化プロトコル(SSL/TLS バージョン)について、TLS v1.1 の利用についてセキュリティ脆弱性リスクを考慮し禁止へ変更。その他、軽微な修正を実施。

出典

^[1] 総務省ホームページ

「固定電話網の円滑な移行の在り方」～最終形に向けた円滑な移行の在り方～
(http://www.soumu.go.jp/main_content/000509967.pdf)

^[2] NTT東西ホームページ

「固定電話の IP 網への移行後のサービス及び移行スケジュールについて」
NTT東日本 (https://www.ntt-east.co.jp/release/detail/pdf/20171017_01_01.pdf)
NTT西日本 (<https://www.ntt-west.co.jp/news/1710/pdf/171017a.pdf>)

^[3] インターネット EDI 普及推進協議会 (JiEDIA) ホームページ

<https://www.jisa.or.jp/jiedia/tabid/2822/Default.aspx>

『「全銀協標準通信プロトコル (TCP/IP 手順・広域 IP 網)」利用ガイドライン SSL/TLS 方式
編 v2.0.1』(2020 年 1 月発行)

一般社団法人 情報サービス産業協会 (JISA) EDI タスクフォースの活動は、2019 年 7 月よりインターネット EDI 普及推進協議会 (JiEDIA) へ移管されました。なお、石油化学工業協会が参考とした JiEDIA 発行ドキュメントは上記の通りです。最新版ドキュメントについては、JiEDIA サイトより確認いただけます。

^[4] 一般社団法人 全国銀行協会 発行『全銀協標準プロトコル -TCP/IP 手順・広域 IP 網-』

https://www.zenginkyo.or.jp/fileadmin/res/abstract/efforts/system/jba_protocol.pdf

石化協版

「全銀協標準通信プロトコル(TCP/IP 手順・広域 IP 網)」

利用ガイドライン SSL/TLS 方式編

2022年1月 発行

石油化学工業協会 情報通信委員会 CEDI-WG
(2024-WGは2020年度よりCEDI-WGに統合されております)
本資料に関する問い合わせは下記までお願いいたします。

<p>CEDI 事務局 (石油化学工業協会内) 電話 : 03-3297-2011 メール : cedi_information@jpca.or.jp</p>
