「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

V2.0.0

インターネット EDI 普及推進協議会
Japan internet EDI Association (JiEDIA)

目　次

1.　要旨 1
1.1.　はじめに 1
1.2.　利用ガイドライン作成の背景と目的 1
1.3.　適用範囲 1
1.4.　本ガイドラインが対象とする組織と想定する読者 1
1.5.　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 2
2.1.　プロトコル概要 2
2.2.　セキュリティ対策の代表的な方式と特徴 3
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 7
3.5.　認証方法 8
3.6.　エラーの扱い 8
3.7.　脆弱性対応 8
3.8.　証明書 9
3.9.　まとめ 10
4.　SSL/TLS 方式における運用ガイドライン 10
4.1.　証明書の運用 10
4.2.　セキュリティについての取り決め 11
4.3.　PSTN 網特有機能の代替え 12
5.　相互接続試験 13
5.1.　試験の目的 13
5.2.　試験構成 13
5.3.　事前調整 13
5.4.　試験項目 15

一般社団法人 情報サービス産業協会（JISA） EDI タスクフォースが作成した「全銀協標準通信プロトコル利用ガイドライン SSL/TLS 方式編 V1.1.0」を、インターネット EDI 普及推進協議会（JiEDIA／ジェディア）が引き継ぎ、更新を行っています。
よって、表記上 EDI タスクフォースで作成した部分も JiEDIA 作成と位置付けております。

1. 要旨

1.1. はじめに

東日本電信電話株式会社ならびに西日本電信電話株式会社より、2024年から2025年にかけて公衆電話回線網（PSTN）をIP網に移行する方針が発表された。これに合わせてEDI用途でも広く利用されている「INSネットディジタル通信モード（ISDN）」もサービス提供終了が発表されており、各業界団体において対応策が検討されている。

インターネットEDI普及推進協議会（JiEDIA）では「通信回線のEDI利用」という視点から検討を行い、IP網に対応したプロトコルへの移行推進を基本方針として活動を行っている。

1.2. 利用ガイドライン作成の背景と目的

「INSネットディジタル通信モード（ISDN）」サービス提供終了を受けて各業界団体で対応方針が検討されている中で、一般社団法人全国銀行協会（以下、全銀協）よりオンラインデータ交換に利用されている通信手順「全銀協標準通信プロトコル」を広域IP網に対応する方針が発表された。具体的には、「全銀協標準通信プロトコル（TCP/IP手順）」（以下、全銀TCP/IP手順）をベースに、広域IP網で利用可能なプロトコルとして、「全銀協標準通信プロトコル（TCP/IP手順・広域IP網）」（以下、広域IP網対応版全銀手順）が制定された。

現在、「全銀協標準通信プロトコル」は銀行とのオンラインデータ交換のみならず幅広いデータ交換において利用されているため、今後各業界団体で対応方針の検討が行われるものと考えるが、業界団体が存在しない場合でも安定かつ円滑な移行の一助となるよう、JiEDIAは広域IP網対応版全銀手順に準拠し利用するための本ガイドラインを作成した。

なお、広域IP網対応に伴って、「全銀協標準通信プロトコル（ベーシック手順）」と全銀TCP/IP手順は、2023年12月末をもってサポート終了することが、全銀協より明示されている。

本書の内容は逐次改定を加える予定である。本書を引用する場合は、
「出典：「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　VX.X.X（インターネットEDI普及推進協議会）」と出典を明記していただきたい。

1.3. 適用範囲

本ガイドラインは広域IP網対応版全銀手順の主に暗号化接続レイヤに対して補完するものであり、その他のレイヤについては基本的に言及しない。特に、全銀プロトコル（図表1の「アプリケーション」「機能制御」「通信制御（サブレイヤ）」）は、全銀TCP/IP手順より仕様が変更されていないため、本ガイドラインの対象外とする。

「広域 IP 網対応版全銀手順」のプロトコルレイヤ



図表 1 プロトコルレイヤにおける本ガイドラインの適用範囲

1.4. 本ガイドラインが対象とする組織と想定する読者

本ガイドラインは「広域IP網対応版全銀手順」に準拠した製品を開発する企業ならびに、広域IP網対応版全銀手順を利用してシステムを構築・運用する企業向けに記載する。

1.5. 本ガイドラインが対象とする接続方式

「広域IP網対応版全銀手順」をEDIで利用する場合、複数の接続方式が選択可能である。本ガイドラインではその中でも専用環境が基本的に不要であり、相互接続性が高い「SSL/TLS方式」を中心に記述する。

2. プロトコル概要

2.1. プロトコル概要

「広域IP網対応版全銀手順」は、INSネットディ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。

広域IP網対応版全銀手順が従来の全銀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	広域 IP 網対応版全銀手順
適用回線	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 手順との並行運用を考慮して「5020」以外のポート番号を利用する場合もある。 （「3.4.TCP ポート番号」参照）
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が前提で、当事者間または業界団体で最適な方式を選択し、適時見直しされることを期待

図表 2　プロトコル仕様差異

セキュリティ対策については、各業界団体や当事者間で具体的な方式を決める必要があるため、本ガイドラインでは代表的な方式の特徴を記載する。

[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。

2.2. 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。各方式の差異を以下の表にまとめる。

	SSL/TLS 方式	インターネット VPN 方式	IP-VPN 方式
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（パスフレーズ）、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 3　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。SSL/TLSに対応した全銀TCP/IP手順パッケージか、SSLアクセラレータと全銀TCP/IP手順パッケージの組み合わせで実現可能である。認証方式には、電子証明書を利用するため、少なくとも応答側（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行う必要がある。

●インターネットVPN方式の特徴

インターネットVPN方式は、プロトコルのトンネル技術を用いて、インターネット上にプライベートネットワークを実現するための手段の総称である。プライベートネットワーク上では、TCP/IP通信が可能なため全銀TCP/IP手順によるデータ交換が可能となる。インターネットVPNを実現するためのプロトコルは、PPTP、IPsec、L2TP/IPsecなど複数存在する。インターネットVPNは、OS標準機能としてプロトコルが実装されており、認証方式に共通鍵（パスフレーズ）を選択できるなど、要求側（クライアント側）の導入コストを抑えた運用も可能となっている。ただし、プロトコルによっては、UDPポートを使ったり、複数のTCP/UDPポートを使ったりするため、ファイアウォール等のネットワーク設計が煩雑となる場合がある。また、同じメーカーの通信機器同士でしか接続ができないケースもあり、複数接続先がある場合は運用負荷になる可能性があるため、インターネットVPNの採用は注意が必要である。

●IP-VPN方式の特徴

IP-VPN方式は、通信事業者が用意した閉域IP網を利用することで専用線と同じようにインターネットとは別の専用ネットワークを構築できることが特徴である。従って、性能要件やセキュリティ要件が極めて高い場合にIP-VPNを選択するケースが考えられる。インターネットVPN

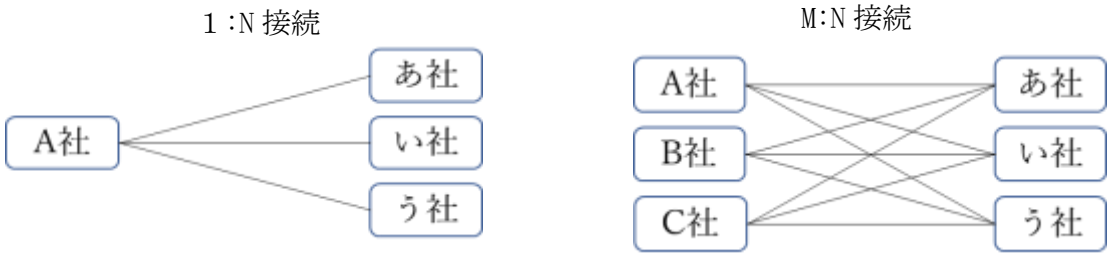
同様、全銀TCP/IP手順によるデータ交換が可能である。ただし、IP-VPNの場合接続先も同じ通信事業者が提供する閉域IP網を利用することが必要となるため、一般的な用途で採用することは難しいと考えられる。

	IP-VPN 方式	インターネット VPN 方式		SSL/TLS 方式
		IPsec	L2TP/IPsec	
接続形態	サイト間接続	サイト間接続	リモートアクセス	リモートアクセス
特徴	通信事業者が提供する閉域 IP 網を利用し、インターネットに接続することなく構築された拠点間の仮想プライベート通信網。 MPLS によりフレームやパケットを分離させており安全ではあるが、データ自体は暗号化されない。	インターネットなどの TCP/IP ネットワーク上で暗号化通信を行うためのプロトコル。 インターネット回線上の通信を暗号化することで、拠点間の VPN 構築を行う。	IPsec で暗号化された通信経路内に、トンネリングを行う L2TP を組み合わせ、クライアント―拠点間の VPN を構築する。 現在では多くの機器が対応しており、クライアントからの VPN 接続の主流になりつつある。	インターネットなどの TCP/IP ネットワーク上で暗号化通信を行うためのプロトコル。
メリット	・クライアント側で接続操作を意識する必要がない。 ・専用線のような常時接続で利用できる。 ・インターネット網を経由しないため、盗聴や改竄の可能性が極めて低い。	・クライアント側で接続操作を意識する必要がない。 ・安価なインターネット回線を利用して、専用線のような常時接続で利用できる。	・OS 側に機能が実装されていることが多く、専用機器が不要で接続手段を容易に確保できる。	・専用回線が不要。 ・OS 等の環境に依存しない。
デメリット	・ネットワークに接続されている端末は、インターネット接続が出来ない。	・社内 LAN などの NAT/NAPT 環境では接続できない可能性がある（開放されているポートや、IPsec パススルーなどルータの機能に依存）。 ・接続元となるクライアント側のルータについて、異なるベンダー機器の相互接続確認など、サポート範囲を明確にしなければならない。	・社内 LAN などの NAT/NAPT 環境では接続できない可能性がある（開放されているポートや、IPsec パススルーなどルータの機能に依存）。 ・接続中は、クライアント側の LAN にアクセスできなくなる。	・証明書の管理が必要。
セキュリティ	◎ 暗号化自体は上位レイヤ依存となるが、インターネット網を経由しないため高い。	○ 暗号化レベルが高い。	○ 暗号化レベルが高い。	○ 暗号化レベルが高い。
コスト	△ イニシャルコスト、ランニングコストが非常に高価。	○ IP-VPN と比較して安価ではあるが、クライアント側で IPsec を終端するためのルータ機器の導入が必要。	◎ クライアント側にルータ機器等が不要なため安価。	○ 証明書の費用が必要。
運用負荷	△ 接続拠点、クライアントいずれも同一通信事業者の閉域網に接続されている必要があるため（閉域網をまたいでの接続はできない）、ネットワーク回線の導入および管理が必要。	○ 拠点単位で接続設定と管理が必要。	△ クライアント単位でユーザー設定と管理が必要。 また、ユーザー環境が多種多様で、OS 依存の不具合が発生しやすい。	○ クライアント単位でユーザー設定と管理が必要。
ユーザー負荷	◎ 物理的な配線のみ。	△ IPsec に対応した VPN ルータ機器の導入および設定が必要であり、一定のコストと技術が必要。	○ 接続のための設定や操作が必要。	○ 接続のための設定や操作が必要。
VPN に関わるリスク・課題	・端末が常時接続となるため、クライアント側の接続ルールについて運用を徹底する、またはタイムアウトの設定が可能か検討する必要がある。 ・一度接続が確立するとネットワーク内の全端末が双方向で通信可能となるため、セキュリティを考慮した設計が必要である。 ・マルウェアに感染している端末がネットワーク内に存在している場合、サーバ等を介してサブネット内の全端末が間接的に感染する恐れがある。 ・ネットワーク内での通信について、IP アドレスやポートでのフィルタリング等を徹底する必要がある。 ・ユーザー環境が多種多様であり、サポート側の運用負荷が高い。 ・ネットワーク設計等の専門知識を有しないユーザーに対してのサポートが必要。 ・接続保証について、OS やプロトコルレベルの表記をどのようにするのか検討が必要。			

図表 4　（参考）セキュリティ方式ごとの特徴

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。その負担を低減するため、各業界団体ではEDIの標準化と普及活動に努めている。

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 5　1:N 接続と M:N 接続

M:N接続でEDIを利用する場合、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、SSL/TLS方式が有利となる。

本ガイドラインではM:Nでの接続性に優れているSSL/TLS方式について、詳細を記述する。（以下、広域IP網対応版全銀手順（SSL/TLS方式））

セキュリティ方式	ユースケース	EDI 用途
SSL/TLS	・M:N 接続のデータ交換	○
インターネット VPN	・社内やグループ企業など 1:N 接続でのデータ交換 ・要求側（クライアント側）の導入コストを抑えた運用を重視した場合のデータ交換	△
IP-VPN	・社内やグループ企業など 1:N 接続でのデータ交換 ・セキュリティ要件や性能要件が非常に厳しい場合のデータ交換	△

図表 6　セキュリティ方式ごとのユースケース

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

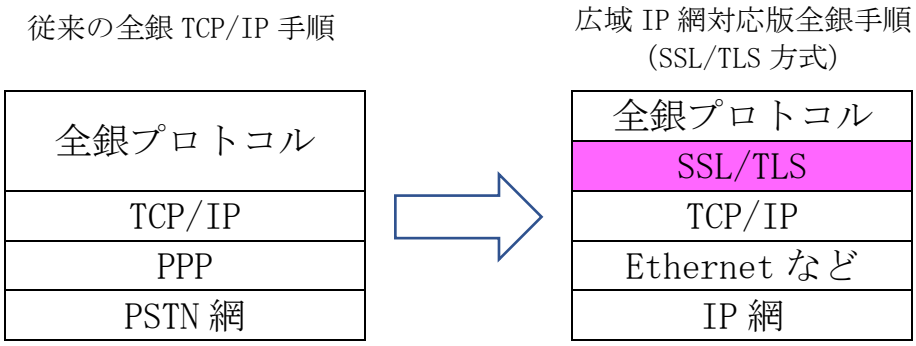
SSL/TLSは、インターネットを利用する際のセキュリティリスクとなる「盗聴」「改ざん」「なりすまし」「否認防止」のうち、「盗聴」「改ざん」「なりすまし」について防止する機能をもっている。

	従来の全銀 TCP/IP 手順 （公衆・ISDN 回線）	広域 IP 網版全銀手順（SSL/TLS 方式） （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 7　SSL/TLS 方式のセキュリティ対策

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。

広域IP網対応版全銀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 8　プロトコルレイヤ図

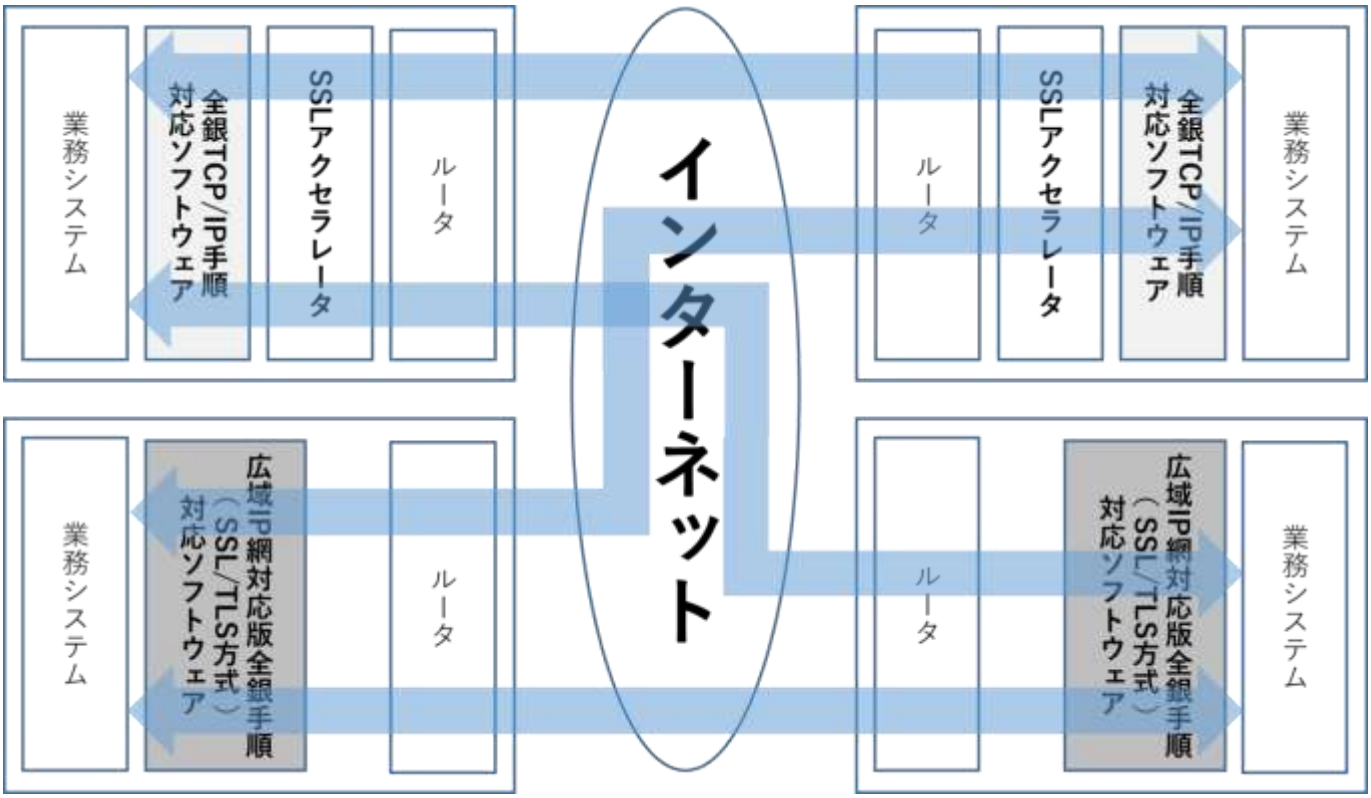
3.2. 対応方法

広域IP網対応版全銀手順でセキュリティ方式に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でも構わないが、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、ハードウェア型ではサーバ側のみ対応している場合が一般的である。



図表 9　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、応答側（サーバ側）は、要求側（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。要求側（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内から接続可能であるため、インターネット上にシステムを公開する必要や、グローバルIPアドレスを応答側（サーバ側）に通知する必要は基本的にはない。

また、ホスト名による接続について特に制限はなく、応答側（サーバ側）がホスト名で運用することも可能である。IPアドレスのバージョンはIPv4に加えてIPv6にも対応することが望ましい。

3.4. TCP ポート番号

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。広域IP網対応版全銀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移行期においては新旧プロトコルが混在する期間が発生することが予想される。

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」番以外に最大２つのTCPポート番号を用意する必要がある。

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、ポート番号を予約しておくなど、競合しないような対策が必要である。）

プロトコル	認証方法	ポート番号
従来の全銀 TCP/IP 手順	―	5020
広域 IP 網版全銀手順 (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 10　TCP ポート番号例

従って、アプリケーション側では、複数のTCPポート番号が管理できること、TCPポート番号を変更できる設計となっていることが望ましい。また、運用上、ポート番号の変更が発生することも考えられるため、上述したTCPポート番号はあくまで参考として参照されたい。

3.5. 認証方法

なりすまし防止のため、認証方法として証明書を用いることを推奨する。

証明書を利用する場合、

① サーバ認証のみ

② サーバ認証＋クライアント認証

という2つの考え方があるが、本ガイドラインでは要求側（クライアント側）のなりすまし防止も可能な「②サーバ認証＋クライアント認証」を推奨する。ただし、各業界団体・各企業によってセキュリティポリシーが異なることが考えられるため、セキュリティ要件やコスト等を総合的に判断した上で決定することを推奨する。

また、証明書の認証方法についてもいくつかパターンが考えられるため、セキュリティポリシーに応じて事前に取り決めておくことが重要である。実装にあたっては、認証方法が柔軟に選択できるような作りになっていることが望ましい。

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が望ましい。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を実装することは推奨しない。なぜなら、構成によってはエラーを処理できない可能性があり、特に外部にSSLアクセラレータを用いる構成を取った場合、相互接続性が下がることが考えられるためである。

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、都度対応が必須である。（直近ではSSL3.0が非推奨となり、TLS1.x以上を推奨する方針に移行したことが記憶に新しい。）

通信パッケージを開発する場合、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設計にしておくことを推奨する。また、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。
特に、応答側（サーバ側）は、要求側（クライアント側）の全てのSSL/TLSバージョン・暗号化アルゴリズム・鍵長に対応する必要があるため、１社でも脆弱性のあるバージョンやアルゴリズムしか使えない企業からの接続がある場合、応答側（サーバ側）はその脆弱性のあるバージョン・アルゴリズムを許容せざるを得ない可能性がある。その結果、応答側（サーバ側）にセキュリティリスクが生じる危険があるため、十分に留意する必要がある。

3.8. 証明書

アプリケーションで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付く（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。そのため、アプリケーション側でも更新時期が近付いていることがわかるような設計とすることが望ましい。
また、CA証明書や中間CA証明書についても同様の対応を行うことが望ましい。

（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。
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を推奨する。

（３）クライアント証明書管理
複数業界にわたってEDIを利用する場合、業界ごとに証明書が異なる可能性がある。また、応答側（サーバ側）ユーザー独自の証明書を利用する可能性もある。そのため、各業界やユーザー毎に複数枚のクライアント証明書を持つケースが考えられる。要求側（クライアント側）アプリケーション側ではクライアント証明書を複数登録でき、接続先単位に切り替えられることが望ましい。

（４）失効
証明書の秘密鍵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）が取得できるが、アプリケーション側では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ような設計となっていることが望ましい。

3.9. まとめ

SSL/TLS方式のプロトコル実装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	応答側	要求側
IP アドレス	IPv4・IPv6 の双方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。 ※要求側（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（サーバ証明書のみ、サーバ証明書＋クライアント証明書、など）を、複数の認証方法より選択できること。 ※要求側（クライアント側）は接続先毎に選択できること。	○	○
	SSL/TLS バージョン・各種アルゴリズム・鍵長やハッシュデータ長を選択できること。(脆弱性のあるアルゴリズム等を利用不可にできること。) ※要求側（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. 証明書の運用

証明書(サーバ／クライアント)にはパブリック証明書とプライベート証明書の2種類がある。機能的にはどちらも同じだが、パブリック証明書は中立的な機関が第三者的な立場から真正性を証明しており、セキュリティレベルはより高くなっている。

どちらを利用するかは各業界団体・各企業のセキュリティポリシー次第だが、各業界で取り決めた標準的な証明書が利用可能な場合はそちらを利用することを推奨する。

なお、証明書の詳細仕様に関しては公開鍵基盤（PKI）関連文書を参照されたい。

（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、更新時期が近付く（一般的に1ヶ月から3か月）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に発生するため、運用管理者はあらかじめスケジュールを認識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、今後同じような対応が必要となる可能性がある。

（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。

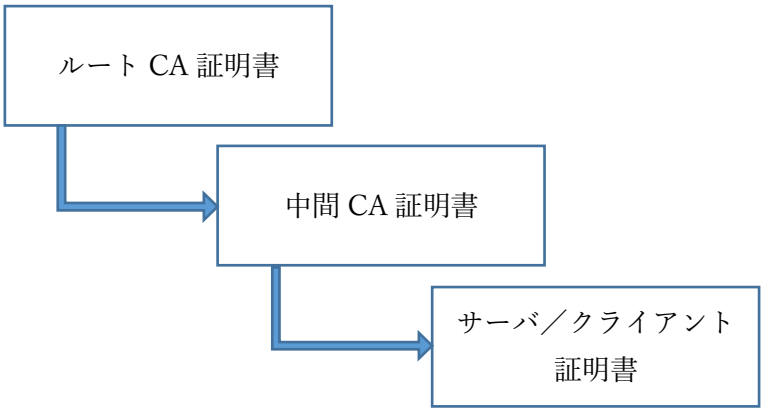
（3）失効

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[2]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なためである。



図表 12　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寄る。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。

4.2. セキュリティについての取り決め

証明書の運用以外に、事前に取り決めが必要な認証や暗号アルゴリズムといった要素を以下に記載する。

（1）TLSバージョンとアルゴリズム

情報漏えいや改ざんといったセキュリティリスクにつながることから、セキュリティ脆弱性を含むプロトコルや暗号アルゴリズムなどは利用しないことが望ましい。例えばCRYPTRECが公開している「CRYPTREC暗号リスト」などを参照し、利用可能なプロトコルや各種アルゴリズムを決定する必要がある。また、独立行政法人情報処理推進機構（IPA）といった団体から定期的

[2] 証明書チェーンとは、クライアント／サーバ証明書から中間 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に例えている。

に報告される脆弱性情報を参照し、状況に応じて見直しを行うことが望ましい。

（２）クライアント認証の有無

要求側（クライアント側）のなりすまし防止のためにはクライアント認証が必要である。（クライアント認証は応答側（サーバ側）で検討が必要な項目である。）インターネットを利用する場合、全銀パラメータによる認証だけではなく、クライアント認証を組み合わせることによってセキュリティ強度を高めることが可能であるため、基本的にはクライアント認証の実施を推奨する。

（３）証明書の認証方法

証明書による認証方法には複数のパターンがあるが、2つの例を以下に記載する。

①サーバ証明書／クライアント証明書の完全一致を厳密に確認する方法

②信頼するCA証明書のチェーンだけを確認する方法

①の方法では、証明書を完全一致で確認するため、セキュリティレベルは高くなる。ただし、サーバ証明書やクライアント証明書を全て管理する必要があり、運用は煩雑化する。

②の方法では、信頼する認証局から発行された証明書であることを確認する方法で、セキュリティレベルは①と比べて低くなるが、CA証明書のみを管理すればよいため、運用は簡素化する。

なお、セキュリティ要素の組み合わせによって上記２方式以外にも認証方法が考えられるため、実際に利用するソフトウェアの実装状況を確認するとともに、自社のセキュリティポリシーにあった認証方法を選択することが望ましい。

4.3. PSTN 網特有機能の代替え

PSTN網やISDN回線・TAなどに特有の機能のうち、広域IP網化によって使用できなくなる機能や回線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
・帯域保証

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、要求側（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は、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、クラスタ構成（仮想IPアドレス）やロードバランサによる振り分け設定で同様の仕組みを実現できる。

（4）帯域保証

ISDN回線の伝送速度は常時64Kbpsが担保されている。これに対してインターネットは基本的にベストエフォート方式であり、帯域保証はないが、通信速度が飛躍的に向上するため、実際には通信時間が短縮するものと考える。IP-VPNなどのサービスでは帯域保証が利用可能である。ただし、接続先側のネットワークの影響を受ける可能性がある（接続先側がベストエフォート方式の場合、帯域保証にはならない）ため、確実ではない。

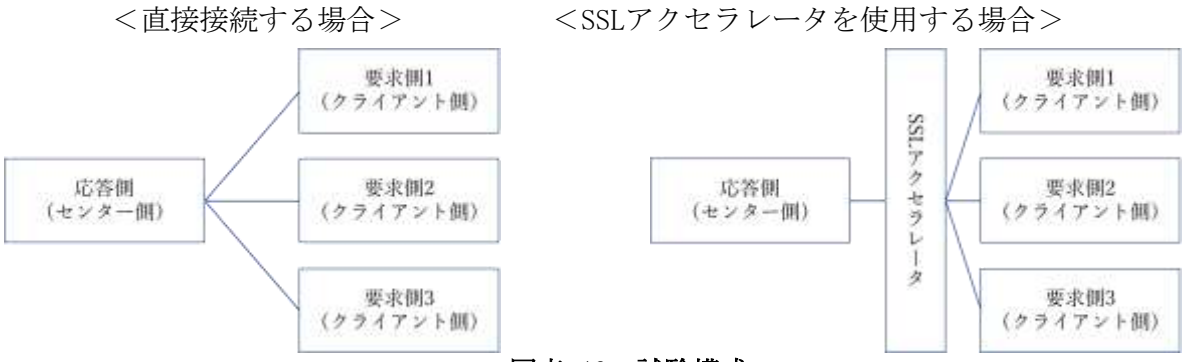
5. 相互接続試験

5.1. 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。

5.2. 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 13　試験構成

5.3. 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)】

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 14　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 15　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 16　通信設定リスト例

5.4. 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ーに対し「受信通信」を行う	S→C	○	ー	・TLSハンドシェイクが行われること ・サーバー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ーに対し「送信通信」を行う	C→S	○	ー	・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ーに配置されること
3	センター通信	正常系	クライアントからサーバーに対し「受信通信」を行う	S→C	○	○	・TLSハンドシェイクが行われること ・サーバー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ーに対し「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ーに配置されること
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通信を行う ※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	○	ー	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通信を行う ※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 17　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ーに対し「受信通信」を行う	S→C	○	ー	・TLSハンドシェイクが行われること ・サーバー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ーに対し「送信通信」を行う	C→S	○	ー	・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ーに配置されること
3	クライアント通信	正常系	クライアントからサーバーに対し「受信通信」を行う	S→C	○	○	・TLSハンドシェイクが行われること ・サーバー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ーに対し「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ーに配置されること
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通信を行う ※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	○	ー	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通信を行う ※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 18　テスト項目例：要求側（クライアント側）

以上

「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

2019年7月　発行

インターネット EDI 普及推進協議会

Japan internet EDI Association (JiEDIA)

本資料に関する問い合わせは、下記までお願いします。

JiEDIA 事務局：一般社団法人 情報サービス産業協会
https://www.jisa.or.jp/tabid/2821/Default.aspx

〒101-0047
東京都千代田区内神田 2-3-4
S-GATE 大手町北 6F
TEL：03-5289-7651（代表）
FAX：03-5289-7653