認証局認定制度ガイドライン

V1.0.0

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.　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 年に公衆電話回線網（PSTN）を IP 網に移行する方針が発表された。これに伴い、企業間電子データ交換（以下 EDI とする）において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。

一般社団法人情報サービス産業協会（以下 JISA とする）では「通信回線の EDI 利用」という視点から対応策を検討、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きたが、2019 年より活動の場を「インターネット EDI 普及推進協議会（JiEDIA)」に移行し、各業界団体がそれぞれ定めた業界標準方式をユーザー企業が採用、導入促進を支援する活動を行っている。

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：認証局認定制度ガイドライン」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。

1.2.　インターネット EDI 推進

「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、JISA／EDI タスクフォースでは以下のような活動を行ってきた。

①通信回線の検証
→　NTT 東西が 2024 年以降に提供を予定している補完策や、
継続提供予定のアナログ回線の検証など。

②産業界で利用できる広域 IP 網に対応した全銀 TCP/IP 手順の策定

③国際標準として策定されたインターネット対応通信手順の動向把握

①の結果、2024 年の IP 網移行後も継続して通信は可能であることが確認できた。しかし、通信遅延が発生するため実運用上 EDI で利用することは難しいと思われる。（詳細は以下の表を参照）

（1）全銀BSC検証結果

	補完策利用時通信可否/処理時間 （ISDN回線利用時比較）			
伝送ブロック長	伝送速度			
	64Kbps		9,600bps	
	通信可否	処理時間	通信可否	処理時間
133Byte	－	－	可	240%程度
256Byte	可	310%程度	可	260%程度
1,925Byte	－	－	可	140%程度
2,048Byte	可	210%程度	可	130%程度

（２）全銀TCP/IP検証結果

	補完策利用時通信可否/処理時間（ISDN回線利用時比較）	
伝送ブロック長	伝送速度	
	64Kbps	
	通信可否	処理時間
120Byte	可	400%程度
133Byte	可	210%程度
256Byte	可	220%程度
1,925Byte	可	130%程度
2,048Byte	可	120%程度
4,096Byte	可	110%程度
32,000Byte	可	110%程度
32,700Byte	可	110%程度

こういった状況を踏まえ、インターネット EDI 普及推進協議会ではインターネット通信手順への移行を推奨する。

1.3.　セキュリティ対策の必要性

インターネットを利用して EDI を行う場合、ネットワークの特性から適切なセキュリティ対策を講じることが必要である。どのレベルまでセキュリティ強度を高めるべきかについては、利用ユーザーの環境や考え方、通過するデータの重要性によって大きく異なるが、本項では一般的に認識されているリスクと対応策について記載する。

■インターネットを利用する際の４つのリスク

①盗聴

インターネットはオープンネットワークであり、その上を流れるデータは第三者によって盗み見られる可能性がある。盗聴を防ぐためには、伝送経路を「暗号化」する必要がある。

②改ざん

インターネット上を流れるデータはデジタル情報であるため、紙とは異なり容易に書き換えることが可能である。改ざんを防ぐためには、電子データに「デジタル署名」を付ける必要がある。

③なりすまし

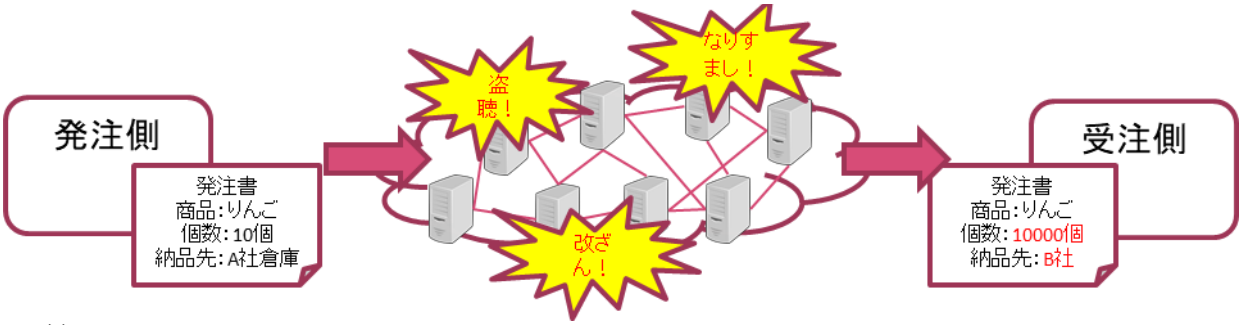
インターネット越しに相手を見ることはできないため、第三者が当事者になりすましていたとしても見分けることができない。なりすましを防ぐためには、本人しかわからない複雑な「パスワード」や、電子データに「デジタル署名」を付ける必要がある。

④否認

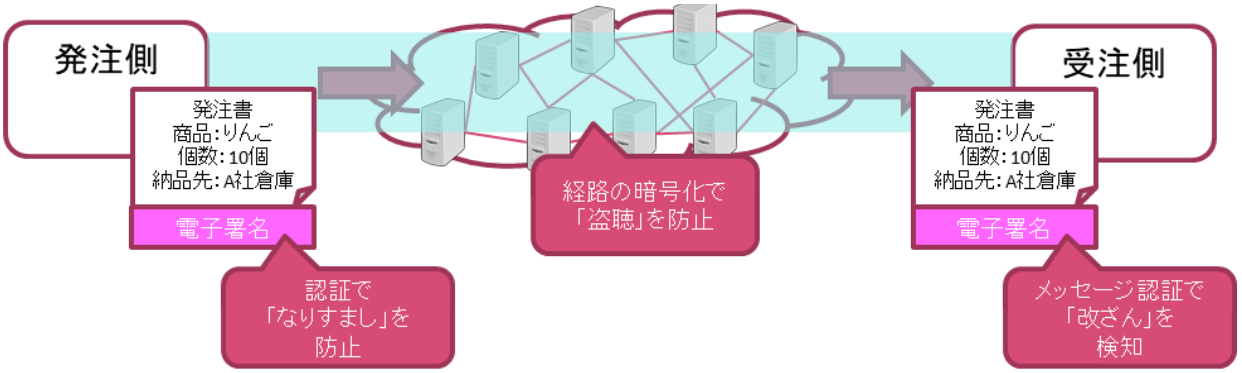
悪意のある当事者が自身の行為を認めないことがある。（注文をしていない

と嘘を付く、など。）否認を防ぐためには、「デジタル署名」を組み合わせた対応が必要である。

■対策をしていないと…

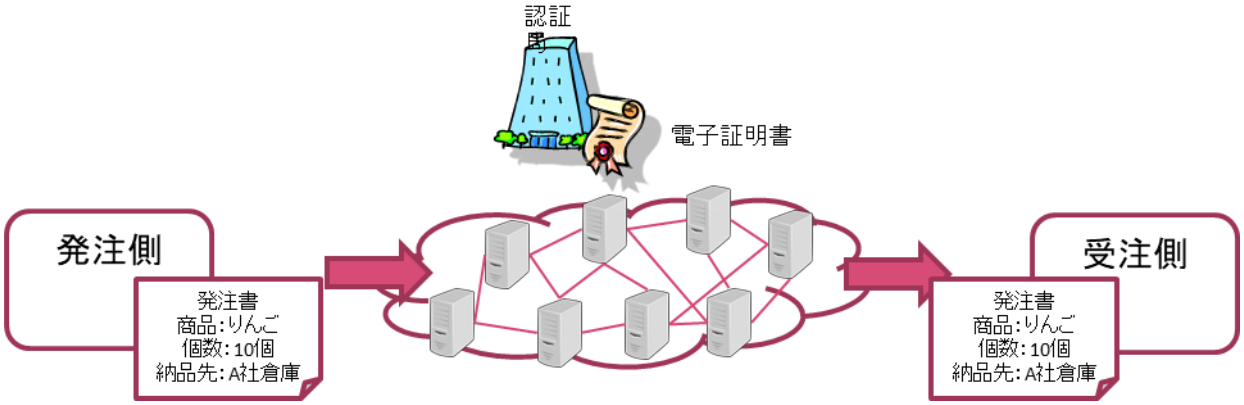


■対策が必要



1.4.　電子証明書の役割

前章で記載したインターネット利用時のリスクを防ぐためには、電子証明書を利用した公開鍵基盤の仕組みを使ってセキュリティ対策を行うことが一般的である。



2. 認証局認定制度の概要

2.1. 背景と目的

前章でセキュリティ対策はユーザー自身がどういったデータをどの程度、どういった手段で守るのか？考える必要があること、またセキュリティ対策として電子証明書を利用することが一般的であることを述べた。

電子証明書はインターネットEDIの普及にあわせて徐々に利用が進んでおり、国内では流通業界において先行して普及が進んでいるが、同時に以下のような運用上のリスクがあることも見えてきた。

利用者側：証明書更新の作業ミス・作業忘れ、
業界コロニー毎・認証局毎に発行された証明書の相互接続性の低下など
運用側：認証局事由による想定外のタイミングでの証明書更新の発生など

今後インターネットEDIの更なる普及により、上記のようなリスクに起因するトラブルが頻発することが予想される。

電子証明書を利用したセキュリティ対策を実現するためには、技術に加えてセキュリティに関する広範な知識を持った人材が不可欠だが、経済産業省の報告書にも記載されている様に、将来的にIT人材が不足することが予想されており、十分に検討がされていない状態でインターネットEDIに移行した結果、情報セキュリティ事故につながる可能性がある。

そこで、JiEDIAでは電子証明書の標準化と課題解決がインターネットEDIの普及にとって不可欠であると考え、認証局認定制度を構築し、電子証明書の普及推進に取り組んでいる。

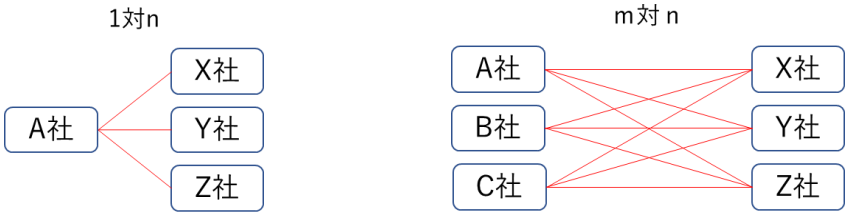
なお、本認定制度は民間企業間のEDIにおいて利用する電子証明書の利便性向上を目的とするものであり、e-Govイーガブ「電子政府の総合窓口」など公共機関向けの認証局認定制度などと同期するものではない。

2.2. 課題

インターネットEDIの普及が進んでいく中で、以下のような課題が発生することが想定される。

①自社証明書が複数化することにより、運用負荷が増大する。
例えば特定のグループ内でのみEDIを行うような場合（1対n接続)、運用負荷はそれほど大きくならないが、一般的にはm対nで接続するケースが多いため、自社及び取引先の運用負荷を考慮し、標準的な証明書を利用することで運用負荷の低減を図ることが望ましい。また、ユーザー企業が複数業界に渡

って事業を行っている場合も証明書の複数化現象が起きやすいため、運用負荷の増大には注意が必要である。



②ルート／中間証明書更新時の取り込み忘れにより、通信ができなくなる。
③認証局事業者が証明書発行を終了した場合、移行先を探す必要がある。

認証局認定制度はこれらの課題を解決し、ユーザー企業の利便性向上を図るためのものである。

2.3. 流通 BMS との関係性

流通 BMS とは、経済産業省の「流通システム標準化事業」によって 2007 年 4 月に制定された、流通業界における EDI の標準仕様である。流通 BMS ではメッセージや通信手順、セキュリティといった各種仕様の標準化が行われたが、その中で電子証明書の認定制度が行われている。インターネット EDI 普及推進協議会ではこの認定制度を継承し、流通業界以外においても汎用的に利用できるようセキュリティポリシーを改定、認証局認定を行う。

2.4. ドキュメントの構成

本ガイドラインは、以下のドキュメントで構成される。

■インターネット EDI 普及推進協議会で新たに作成したドキュメント
- 認証局認定ガイドライン（本資料）
- 認定基準チェックリスト

■流通 BMS 協議会から継承したドキュメント
- 相互セキュリティ基盤に関する検討・認証局構築_第一部
- 相互セキュリティ基盤に関する検討・認証局構築_第二部
- データ交換共通認証局証明書ポリシー
- 適合性チェックリスト

今後のドキュメント管理はインターネット EDI 普及推進協議会で行う。

3. 審査概要

3.1. 審査対象

JiEDIA ではプライベート認証局を審査対象とし、パブリック認証局は認定対象としない。

3.2. 認証局審査基準

インターネット EDI 普及推進協議会で認証局を認定するにあたり、以下の基準を満たしていることを条件とする。

＜認定基準＞

No	チェック項目	内容	提示資料
1	JISA 会員である		JISA 会員番号
2	適合性チェックリストに適合する	原則として全ての項目に適合していること	実施済みの適合性チェックリスト
3	セキュリティ基準を取得している	以下のいずれかの基準を取得していること ・WebTrust for CA ・ISMS/ISO27001	WebTrust for CA または ISMS/ISO27001 を 取得していることを示す資料
4	認証局の運用実績が 10 年以上である		10 年以上前に他組織に対して発行した利用者証明書など
5	事業継続の責任	・最後に発行した証明書の有効期限が切れるまで事業を継続すること ・事業終了後の継承先を検討すること ・ユーザーには事業終了の 3 ヶ月前、認証局審査部会には事業終了の半年前に通知すること	具体的な検討資料があれば望ましい
6	財務的健全性	認証局を安定して運営できること	財務的健全性を有していることを説明できる 資料（財務諸表 3 期分）

＜認定のポイント＞

①JISA 会員であること

インターネット EDI 普及推進協議会で認定を希望する認証局事業者は JISA 会員であること。これは、インターネット EDI 普及推進協議会が JISA 会費によって運営されていることによるものである。

入会の詳細に関しては JISA 事務局まで問い合わせのこと。

②適合性チェックリストに適合すること
インターネット EDI 普及推進協議会の認証局認定制度は流通 BMS の認定制度を継承しているため、流通 BMS 事業で作成された基準を元にインターネット EDI 普及推進協議会で加筆、改定した「認証局証明書ポリシー」ならびに「適合性チェックリスト」に準拠していること。

※「認証局証明書ポリシー」ならびに「適合性チェックリスト」については別紙を参照。

③セキュリティ基準を取得していること
本認定制度ではプライベート認証局を認定対象とするが、信頼性を高めるために一定のセキュリティ基準以上で運営されていることがのぞましい。そのため、「WebTrust for CA」もしくは「ISMS/ISO27001」のいずれかを取得していること。

④認証局の運用実績が 10 年以上であること
認証局事業者として 10 年以上の運営実績を証明できる資料を提示する。一例としては 10 年以上前に他組織に対して発行した利用者証明書など。

⑤事業継続の責任
認証局事業を終了する場合、最後に発行した証明書の有効期限が終了するまでサポートを提供すること。有効期限中にサポートを終了する場合、ユーザー企業に事業継承先を提案すること。また、事業終了後の継承先を明確化すること。

⑥財務的責任
認定を希望する認証局は経営安定性を証明するため、財務諸表もしくはそれに相当する資料を一定期間分（3 年が望ましい）提出すること。

3.3. 更新審査について

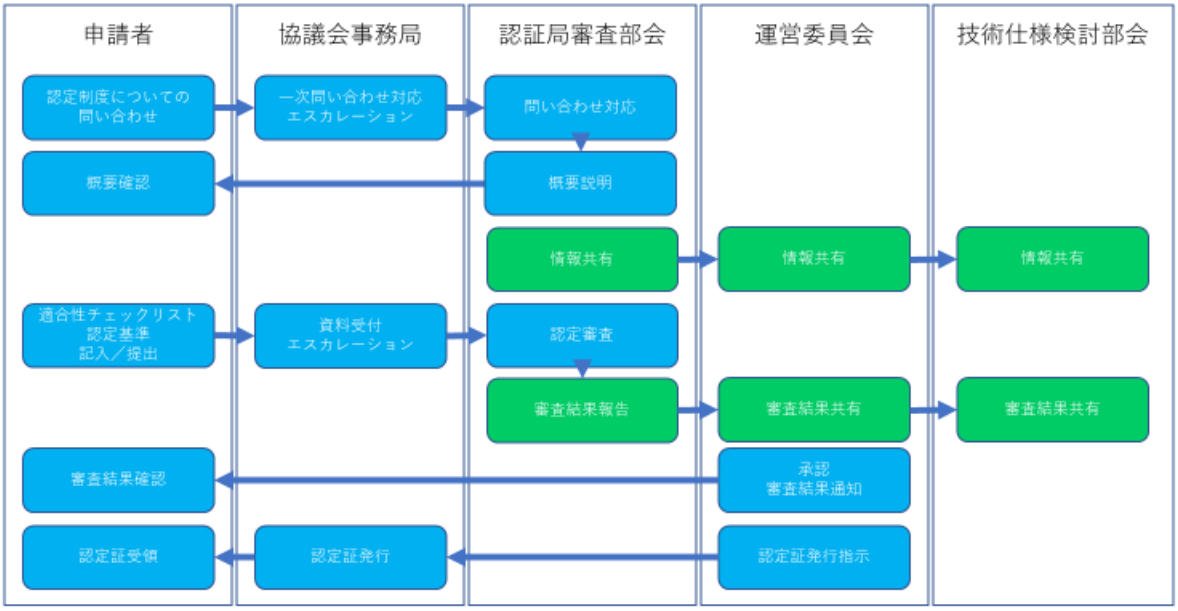
認定を受けた認証局事業者に対し、3 年ごとに更新審査を実施する。
審査基準は最新の認定基準に基づくものとする。

3.4. 認定プロセス

認証局認定は以下に記載する認定フロー図に基づき実施する。
審査は認証局審査部会で行うが、最終的な判断は運営委員会において行う。

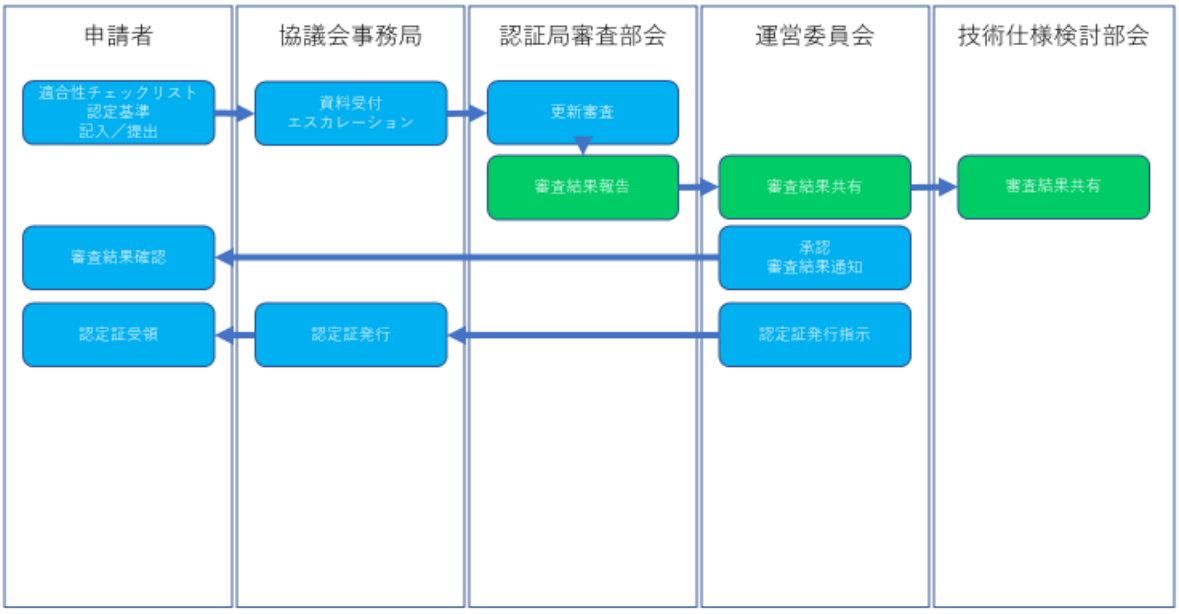
■新規審査手順

認証局審査フロー（新規）



■更新時の審査手順

認証局審査フロー（更新）



■退会時の手順
　認証局審査部会は、退会を希望する認証局事業者より以下の報告を受けた場合、退会承認の判断を行う。

＜報告内容＞
・退会の意思。
・最終発行した証明書の有効期限終了までサポートを続ける、他の認定認証局に業務を引き継ぐ、等の方針。
・認証局業務終了までのスケジュール。

3.5.　運用上の注意点
認証局として認定された場合、以下の運用に準拠すること。

■中間証明書のリポジトリへの登録
インターネット EDI 普及推進協議会のサイトに各認定認証局の中間証明書を公開しているリポジトリへのリンクを公開する。
■セキュリティインシデント発生時の速やかな情報共有
各認定認証局において、重大なセキュリティインシデントが発生した場合、インターネット EDI 普及推進協議会に速やかに報告する。

3.6.　費用について
認証局審査にあたり、費用は発生しない。ただし、認定証の発行を希望する場合は実費を請求する。

4. 責任の制限
　インターネット EDI 普及推進協議会は、認定認証局に対し認定証やロゴの提供を行う場合があるが、認定認証局が CPS および標準 CP に規定した責任を果たさなかったことに起因するトラブル等については、いかなる責任も負わない。

改訂の要約

・V1.0.0（2021 年 4 月公開）作成
  - 新規作成

認証局認定制度ガイドライン

2021年4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