EDI におけるデジタル証明書交換運用への要求

国際／業界横断 EDI タスクフォース

相互運用性検討サブタスク

SIPS

サプライチェーン情報基盤研究会

はじめに

本書は、2016年度「国際／業界横断EDIタスクフォース 相互運用性検討サブタスク」での検討事項に関し、広く意見を募るために公開する資料である。

以上

2016年11月

国連CEFACT日本委員会

サプライチェーン情報基盤研究会

国際／業界横断タスクフォース

１．　目的

企業間のデータ自動連携による業務効率化が検討され始めた当初は、データ伝送可能な通信経路は電話回線網しかなかった。その後、長年に渡り電話回線網が EDI の通信経路を担ってきた。

安価で常時接続が可能なインターネット回線の普及に伴い、インターネット EDI のニーズが高まってきた。電話回線網は NTT 局内という閉域網なため、第 3 者による盗聴などの心配はなかったが、インターネットはオープンな通信網なため、第 3 者からデータを守る必要がある。

暗号化技術を用いてデータ保護を実現したが、その鍵となる証明書には実効性担保のため有効期限が設けられているので、定期的に交換していかなければならない。しかし、多くの EDI 標準では、伝送における証明書の利用方法は定義していても、その交換運用には触れていないことが多い。そのため、個別ルールや場当たり的な運用が行われており、結果として証明書交換の運用負荷が高くなり、効率的なインターネット EDI 運用の阻害要因となっている。

効率的なインターネット EDI の運用を促し、EDI が業務の足枷にならないことを目的として、「EDI におけるデジタル証明書交換運用への要求」を策定した。

なお、EDI において、証明書をどのように利用するか、すなわちセキュリティレベルをどの程度に設定するかは、各 EDI 標準で策定するものとし、本書の範囲外とする。

２．EDI におけるデジタル証明書交換運用への要求

インターネット EDI の実施を検討する事業者が、運用要件のインプットとして参考にすることを想定する。

カテゴリ	No	要求	要求仕様	証明書用途		
				サーバ	クライアント	署名
証明書交換	1	証明書交換運用を明確にする	証明書の交換方法・交換ファイル形式を明確にする。証明書用途（サーバ証明書/クライアント証明書/署名証明書）および適用環境（本番環境/テスト環境）毎に定義する。	●	●	●
証明書検証	2	交換した証明書の検証基準を明確にする	受け取った証明書が信用できるとするためにチェックする項目を明確にする。	●		●
EDI テスト	3	テスト伝送用の仕様を策定すること	実データによる伝送を行わずに、使用している証明書で伝送できることが確認できる。	●	●	●
	4	証明書エラーメッセージを策定すること	証明書によるエラーパターンと、その際に出力されるメッセージを定義する。	●	●	●
	5	証明書交換によるテスト仕様を定義すること	証明書を交換した場合のテスト仕様（特に範囲）を定義する。	●	●	●
証明書仕様	6	証明書の標準有効期限を定めること	長過ぎず、短過ぎない期間に統一する。（クライアント証明書は 1 年）	●		●
並行稼動	7	接続先を順次切替できること	新旧証明書を同時に扱えるようにする。	●		●
	8	証明書整備負荷が最小化されること	有効期限切れの証明書は、一定期間経過後に自動削除される。	●		●
緊急対応	9	緊急セキュリティ対応の方針を明確にしておくこと	緊急セキュリティ事案が発生した場合に即時対応できるような組織体を定義する。	●	●	●

平成 28 年 11 月　発行

発行元　一般社団法人

サプライチェーン情報基盤研究会