2015 年度
グローバルネットワーク相互運用検討サブタスク
活動報告書

SIPS

サプライチェーン情報基盤研究会

はじめに

本書は、2015 年度「国際連携 TF 相互運用性検討サブタスク」の活動記録である。

本サブタスクは、2014 年度からメッセージング基盤 TF の機能を引き継ぎ、活動を始めた。初年度の活動は 2014 年度の活動報告にまとめている。

2015 年度は、昨年から継続している「パブリッククラウドの相互運用調査」と新たな「証明書の運用・管理」をテーマとした。

以上

2016 年 3 月

国連 CEFACT 日本委員会

サプライチェーン情報基盤研究会

国際連携タスクフォース

委員

2015 年度　国際連携タスクフォース
グローバルネットワーク相互運用検討サブタスク 委員

リーダー	湊本　智昭	株式会社 ワイ・ディ・シー
幹事会員	藤野　裕司	株式会社データ･アプリケーション
幹事会員	遠城　秀和	NTT データシステム技術株式会社
正会員	永壽　拓宏	株式会社オージス総研
正会員	松井　宏樹	株式会社オージス総研
正会員	宮崎　暁久	富士通エフ・アイ・ピー株式会社
正会員	江崎　紀雄	富士通エフ・アイ・ピー株式会社
正会員	清水　みか	富士通エフ・アイ・ピー株式会社
賛助会員	川内　晟宏	特定非営利活動法人 IT コーディネータ協会

目次

第一編.　　パブリッククラウドの相互運用調査

1.　目的

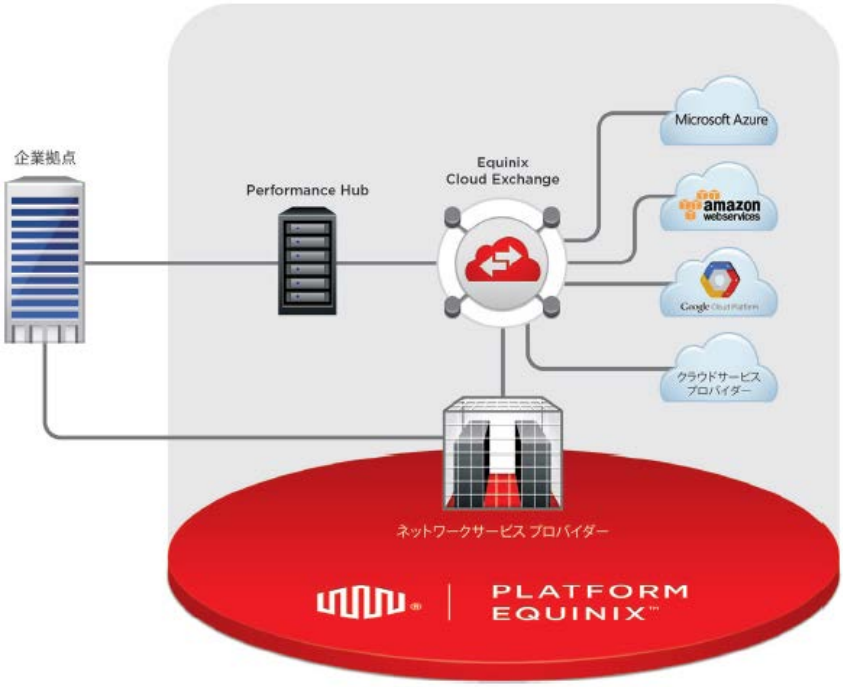
本編は、企業が各々異なる ESP やクラウドと契約しているとき、企業と企業が EDI を行うには複数の ESP やクラウドを経由することとなる。その折、企業間ではその送達確認ができない。ここでは、ESP やクラウド間でどのような準備をすれば、企業がエンド to エンドで最終的な必要情報を共有できるかを調査検討する。

本年度は、パブリッククラウド間で相互に情報連携し、異なる企業が相手側企業の契約するクラウドがどこであろうと気にすることなく相手と情報連携するための技術があるかどうかの調査から始めた。

2.　成果

エクイニクス・ジャパン社へのヒアリング

EQUINIX CLOUD EXCHANGE というサービスについてヒアリングを行った。このサービスはエクイニクスと企業拠点を専用線で結び、複数のクラウドへの直接接続する環境を提供するものであった。このサービスを利用する企業では、複数のクラウドで稼働するシステムをシステム間連携することが実現できるが、異なる企業が利用するクラウド間を相互接続するサービスではないことを確認した。



アマゾン データ サービス ジャパン社へのヒアリング

アマゾン ウェブ サービス（AWS）にて異なる企業が利用するクラウド間を相互接続（AWS-AWS 間、AWS-他のクラウドサービス間）の有無についてヒアリングを行った。AWS では日々新たなサービスが生み出されているが、ヒアリングを行った 2015 年 10 月時点では、該当するサービスは提供されていないと判断した。

3. 今後の方針

今年度は、パブリッククラウドを連携するサービスを調査した。その結果、クラウド間で直接接続し緊密な情報連携を実現する技術は、現時点ではだ提供されていないことが分かった。本件については、いったんここでペンディングとする。

今後は異なる ESP と契約する企業が、互いに情報を共有するためには、ESP や各企業にどのような機能があればよいかを調査し、それを実現するためにはどうすればよいかを具体的に検討していきたい。

第二編.　　証明書の運用・管理

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時は、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。

しかし、取引の国際化が進むにつれ、海外と通信可能なインターネット経路による 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。証明書交換の運用負荷が高いため、インターネット EDI 普及の阻害要因となっている。

効率的で確実な証明書運用を規定することで、インターネット EDI 普及を促し、EDI が国際取引業務推進の足枷にならないよう整備する。そのため、証明書交換運用に関する課題を洗い出し、最も効果的と思われる対策を考案し提案する。

2.　成果

インターネット EDI における証明書運用の課題

2_2_1_証明書更新課題一覧.xlsx

証明書交換運用ガイドラインの項目案

2_2_2_証明書交換運用ガイドライン（項目案）.txt

3.　今後の方針

2015 年度では、証明書交換運用における課題を洗い出し、一覧にまとめた。その課題解決の 1 つとして、運用のガイドライン化を行うことにした。交換運用の大きな枠組みを標準化することで、業界に関わらず適用可能となり、業際取引の効率化に貢献できる。運用手順の再作成や手探り運用の撤廃を目指す。

2016 年度では、証明書交換運用に関する課題を公開し、インターネットで EDI を行うにあたっての問題を広く認識してもらう。証明書交換運用ガイドラインを詳細化しパブリックレビューなどを通して、広く意見を募る。内容によっては実証実験などで運用性を検証する。

2_2_1 証明書更新課題一覧

インターネットEDIにおける証明書運用の課題

2016年3月
SIPS　国際連携WG　相互運用ST

No	課題カテゴリ	課題名	課題内容	対象者 受	対象者 発	証明書種類 サ	証明書種類 ク	証明書種類 署	備考
1	証明書交換	交換形式	受け取る証明書ファイルの形式が不統一、発行側もどの形式が適切か不明	○	△	▲	△	○	ebXMLの時はCPAに証明書を含めるので、サーバ証明書も関係する
2		交換粒度	1ファイル内に含まれる証明書のツリーが不統一	○	△		△	○	
3		交換方法	セキュアでない方法（メール添付）で送付されてくる	○	△		△	○	
4		ファイル名	ファイル名が不統一、本番用かテスト用か不明な場合がある	○	△		△	○	
5	証明書検証	検証方法	検証基準がないため、受領した証明書を信じるしかない	○				○	
6			キーストアなどに設定した証明書の動作確認が実際の伝送までできない、単体テスト的に確認したい	○				○	
7	証明書整備	期限切れ証明書	期限切れ証明書の削除が怖い、手動ではなく自動でできないか	○	○	○	○	○	
8	テスト/切替	テスト環境	テスト環境と本番環境の2回実施が必要（1回で済ませられないか）	○	○	○	○	○	
9		テスト実行	本番環境は、「切替→テスト→そのまま運用開始」といった運用も多いため、何かあったらその場で解決しないと延期になってしまう	○	○	○	○	○	
10			エラーメッセージがわかりずらく解決に時間が掛かる	○	○	○	○	○	
11			EDI標準にテストメッセージがないため、ダミーデータor本番データを実際に伝送してテストすることになる	○	○	○	○	○	
12			クライアント証明書の接続エラーの場合、サーバ側で検知できない（問い合わせがあった場合にサーバ側で問題ないことを確認する手段がパケットキャプチャのみ）		○		○		
13		テスト範囲	取引先毎にテストが必要なので接続数に比例して負荷が増える		○	○	○	○	
14			本来は疎通のみで十分だが、心配であるという理由でテスト範囲は広がる場合がある	○	○	○	○	○	
15	証明書仕様	有効期限	短いと交換運用負荷が高いが長過ぎは脆弱となるため→何年にしたら良いかは各社に委ねられている		○	○	○	○	
16	証明書運用	並行稼動	1つのバージョンしか保持できないため、全接続先一斉切り替えするしかない。新旧並行運用し、切り替えを確認したら旧証明書を削除したい	○	○	○	○	○	

受：証明書受領者
発：証明書発行者（期限切れによる更新者）
サ：サーバ証明書
ク：クライアント証明書
署：署名検証用証明書

証明書の種類

サーバ証明書	SSL暗号化に利用
クライアント証明書	アクセスしてきたクライアントがサーバに提示し、自身が信用できることを証明するために利
署名検証用証明書	否認防止のために利用

2_2_2　証明書交換運用ガイドライン（項目案）

2016 年 03 月

SIPS 国際連携 WG 相互運用 ST

■証明書交換運用ガイドラインの概要（案）

●目的

証明書交換手順や取り決めを統一化することで、運用の信頼性と効率性を向上する

●スケジュール

有効期限 60 日前：期限切れ検知

有効期限 45 日前：接続先連絡

有効期限 30 日前～1 週間前：切替

→EDI アプリケーションに自動的に検知・通知する仕組みが実装されるのが望ましい

●証明書受渡形式

pkcs#7（拡張子：p7b）

ルート証明書から格納する

●受領した証明書を信用するために最低限チェックすべき項目

（今後検討する）

●テスト範囲

疎通確認のみ

→証明書更新による影響は通信のみなので、通信レベルの確認のみ実施する

●テスト例

流通 BMS の場合

Chem eStandards の場合

AS2 の場合

●切り戻し基準

更新者に問題がなければ戻しは行わない

通信エラーとなった接続先とは別途調査・復旧する

→全接続先と再度の日程調整は難しいため、個別対応となる事象の場合は全体的な効率を重視して戻しは行わない

■その他提言

●ロギング

通信レベルのエラーメッセージ詳細化

伝送に使用した証明書情報のログ出力

平成 28 年 3 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