Annex1\_Compliance\_Guidelines\_Matrix\_19102009.xlsと

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bと | | シーディーイー | | | Hと | Iと | Jと | Kと | Lと | Mと |
| 1と | ワオ  プロセスステップ  (順序を調整できる) | ビジネス実装クラスB-D | | | なぜ(リスク) | 何(要件) | どのように(制御) | 参考例。 注。ここに挙げた例は、網羅的なものではなく、想定される対策の種類を示すためにのみ提供されている。 | 追加ガイダンス[「コンプライアンス・ガイドラインの解説書」 参照] | 実装の適用性[自己評価に使用] |
| 2と |  | Bと | Cと | Dと |  | | | | |  |
| 3と | すべて(仕入先および購買担当サイド) |  |  |  |  | | | | |  |
| 4と | 0-一般 | xと | xと | xと | ITシステムに関する一般的なリスク | 一般的な商用優良セキュリティ基準をサポートする | ビジネス・システムのセキュリティ、継続性、整合性のためのグッド・プラクティスに基づいて、認められた標準を実装する。これらの慣行は、健全なコントロールの枠組みを提供するために、認められた優良事例の要件に沿って適用され、監査されなければならない。 | 組織の規模と性質を考慮して、適切な(一般的なIT)管理が実施されるべきである。 | 7.3 .1について  7.3.7 |  |
| 5と | 0-一般 | xと | xと | xと | サービスプロバイダには、サプライヤと購入者の両方に対する責任があり、利益相反の可能性があります。 | 各当事者の責任は明確に示されなければならない。 | 供給者と購入者の要求事項を実施するプロセスは、別々の監査記録、別々の保管庫、別々の管理管理パラメータにより明確に分離可能であり、別々の管理役割の下で運営されなければならない。分離は手続き的でなければならず、物理的または論理的であってもよい。 | 誰の代理機能が実装されているかを明確に文書化する |  |  |
| 6と | 0-一般 | xと |  | xと | 適用されるプロセスおよび手順は文書化されていないため、監査できません。 | プロセスと手順の文書化が行われるべきである。 | 保存期間中にすべてのE-Invoiceについて、企業環境内でどのプロセスが有効であったかを監査人が理解できるように、日付参照のあるバージョン管理システムを含むドキュメント管理のグッドプラクティスを使用して、プロセスとシステムのドキュメントを維持する必要があります。 |  |  |  |
| 7と | A-取引先オンボード | xと | xと | xと | 取引先は事前の識別と承認なしに電子請求システムを使用します。 | 貿易相手国は、適切な貿易相手国の特定及び通関を確保しなければならない。 | 取引先はお互いを受け入れ、知っていなければなりません。識別及び通関は、例えば、商業登記簿及び/又は商業的に入手可能な裏付けデータを通じて行うことができる。 | DUNSルックアップ、取引登録簿または商工会議所などのチェック-これらのプロセスは、取引先のためにサービスプロバイダによって実行することができます |  |  |
| 8と | A-取引先オンボード | xと | xと | xと | 電子請求書は、それを受け入れない取引先に送信されます。 | E-Invoicesの送信および受信の決定は監査可能です。 | 合意されたルール (例:。一般条件) |  |  |  |
| 9と | A-取引先オンボード | xと | xと | xと | 取引先は、税金、データの使用と機密性、サービス提供者と変更管理の責任、および両当事者の変更管理など、権利と責任を規制する十分な契約なしに、電子請求システムにアクセスできます。 | 貿易相手国は、貿易相手国のシステムへのアクセスを提供する前に、他の貿易相手国が包括的かつ執行可能な協定に署名することを確保すべきである。税金関連部品をサービス・プロバイダに外注する場合は、明示的な合意が必要です。 | オンボーディング段階の結果として合意が成立していることを確認するためのプロセスがある。 | [この目的のためのモデル協定を策定すべきである] |  |  |
| 10と | A-取引先オンボード | xと | xと | xと | 取引先には、主要な担当者に対する十分な研修なしに電子請求システムへのアクセスが与えられる。 | 取引先/サービス提供者は、問題となっている取引先が、エラーおよび例外処理のプロセスを含む必要なシステム活動を実行するように訓練されていることを確実にすべきである。 | 取引先/サービス提供者は、取引先が関連スタッフを効果的に訓練できるように、文書またはその他の適切な学習ツールを利用可能にしなければならない。最低限の技能レベルは、主要な職員によって検証可能に得られなければならない。 | オンラインドキュメントとツールチップ、多言語サポートにより、テストアカウントと本番アカウントを明確に区別してユーザーIDをマークできます(本番アカウントにテスト・アカウント・メッセージを送信できない)。 |  |  |
| 11と | A-取引先オンボード | xと | xと | xと | 脆弱性を残す当事者間の情報交換のセキュリティの一貫性のない適用。 | E-インボイスの交換に関与する当事者間で採用されるセキュリティメカニズムは、識別されたリスクに一貫した方法で対処しなければならない。 | 電子請求書の交換に関与する当事者は、情報交換に対する特定された脅威に対処するために適用されるセキュリティメカニズムまたは管理について合意するものとする。 |  |  |  |

1/12個

Annex1\_Compliance\_Guidelines\_Matrix\_19102009.xlsと

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Bと | シーディーイー | | | Hと | Iと | Jと | Kと | Lと | Mと |
| 1と | ワオ  プロセスステップ  (順序を調整できる) | ビジネス実装クラスB-D | | | なぜ(リスク) | 何(要件) | どのように(制御) | 参考例。 注。ここに挙げた例は、網羅的なものではなく、想定される対策の種類を示すためにのみ提供されている。 | 追加ガイダンス[「コンプライアンス・ガイドラインの解説書」 参照] | 実装の適用性[自己評価に使用] |
| 12と | A-取引先オンボード | xと | xと | xと | 取引先は、事前に合意された基準に基づいて通信のテストに成功することなく、e-請求システムへのアクセスを与えられます。 | e-請求システムへの貿易相手国のアクセスの適切な技術的機能は、生産前に確保されるべきである。 | 取引先・サービス提供者のテスト計画とテスト結果は、両者の合意が必要です。 | オンラインテストと厳格な管理;分離テスト・生産勘定;テストE請求書を作成するセルフ・サービス機能。 |  |  |
| 13と | A-取引先オンボード | xと |  |  | EDI E-Invoicesは、交換契約なしでバイヤーに発行されます。 | EDI E-Invoiceを送受信する場合は、交換契約が必要です。それ以外の場合、E-Invoiceは有効ではありません(付加価値税法)。 | EDI E-Invoicesの送信を開始する手順で、このリスクに対処してください。 | モデル契約 | 7.2.1.1 |  |
| 14と | A-取引先オンボード |  |  | xと | 取引先は異なるEDI構造を使用 | 貿易相手国のEDI構造の適切な技術的機能は、生産の前に確保されるべきである。 | 取引先のテスト計画およびテスト結果が合意されるものとします。 | オンラインテスターと厳密なコントロール;分離テスト・生産勘定;テストE請求書を作成するセルフ・サービス機能。 |  |  |
| 15と | 仕入先サイド |  |  |  |  | | | | |  |
| 16と | 1-請求書データの準備 | xと | xと | xと | 請求書を必要とする供給に対して請求書データが準備されていない場合 | VAT目的でE-Invoiceを発行する義務があるすべてのサプライ品について、E-Invoiceが発行されることを保証する必要があります。 | アプリケーション監査と内部統制活動。供給から請求済供給までの監査証跡。 | システムは、発注ごとの請求書残高+仕入先のERP (エンタープライズリソースプランニング)システム管理を示します。未履行受注および未請求搬送のレポート |  |  |
| 17と | 1-請求書データの準備 | xと | xと | xと | 供給がE-請求済であるが、GL/VAT申告に報告されていない場合 | E-請求書の準備と支払の受入との間で職務を分離することで、供給から報告済収益までの監査証跡が可能になります。 | 職務分掌は会社の規模に適合しなければならない。論理的なアクセス制御は、適切な職務分離にマップされる必要があります。これは、エンドツーエンドの監査証跡によって証明されます。 | 定義されたユーザー・ロールのユーザー名およびパスワードへのマッピング (ロールに適したデータおよび機能へのアクセス権を付与);ロールに不適切なデータや機能へのアクセスを防止します。 |  |  |
| 18と | 1-請求書データの準備 | xと | xと | xと | 権限のないユーザーは、請求書データを追加、変更、または削除できます。 | 供給者は、電子請求書の内容に対する許可されていない変更を防止するための措置を講じなければならない。 | 職務分掌は会社の規模に適合しなければならない。論理的なアクセス制御は、適切な職務分離にマップされる必要があります。これは、エンドツーエンドの監査証跡によって証明されます。 | 定義されたユーザー・ロールのユーザー名およびパスワードへのマッピング (ロールに適したデータおよび機能へのアクセス権を付与);ロールに不適切なデータや機能へのアクセスを防止します。 |  |  |
| 19と | 1-請求書データの準備 | xと | xと | xと | 請求書データには、すべての必須情報が含まれているわけではありません。 | 請求書データには、少なくとも準拠法で規定されたデータが含まれている必要があります。 | コントロールは、E-Invoice作成前に必要なデータをチェックするために使用され(取引先がクラスCコントロールを使用している場合は、作成の最後のステップとして電子署名)、制約は条件付きフィールドに使用され、E-Invoiceにすべての必須データが表示されるようにします。データフィールドの完成は、アプリケーションで保証されなければなりません。 | オンラインおよび[XML/EDI]構文コントロールは、必要なデータを検証します。バイヤーVAT IDなどの条件付きフィールドは、範囲と形式のチェックに基づいて検証され、必要に応じて検証アルゴリズムも含まれます。 |  |  |
| 20と | 1-請求書データの準備 | xと | xと | xと | 請求書データが時間通りに作成されていません。 | 電子請求書の発行は、適用法によって定められた期間内でなければならない。 | アプリケーション監査と内部統制活動。サービスから請求書回転率までの監査証跡。 |  |  |  |
| 21と | 1-請求書データの準備 | xと | xと | xと | データセットを準備する責任者は、イベント後に識別できません。 | 個人は、各電子請求書に対応可能である必要があります(手動か自動か)。 | 責任者を識別する監査証跡。 | ユーザーのID (またはプロセス)を含む、アプリケーションまたはDBMS (データベース管理システム)でのアクセスとアクティビティの監査ログの保持。責任者を記録する |  |  |
| 22と | 1-請求書データの準備 | xと | xと | xと | 請求書データが変更され、ソース取引データと請求書データの間の監査証跡が中断されます。 | 請求書データは、常にソース取引データと一致している必要があります。 | 出願の技術的設計は,これを保証しなければならない。;データ・フローは明確でなければなりません。 | ERP (エンタープライズリソースプランニング)システムでは、見積、受注、搬送、E-Invoice、またはその他のビジネス文書が相互参照されます。 |  |  |
| 23と | 1-請求書データの準備  訂正請求書データの準備 | xと | xと | xと | オリジナルの送り状を参照しない修正送り状データセット(クレジット・ノートを含む)を作成する。 | 修正用E-Invoiceデータ・セットには、元のE-Invoiceデータ・セットを識別するための参照が含まれています。訂正E-請求書を識別できる必要があります。 | アプリケーション統制と内部統制活動。少なくとも、元のE-Invoice番号を参照することをお勧めします。 | 例:。元のE-Invoice番号を参照することにより、  当初のE-Invoice日付。  訂正E-のための個別シリーズのE-Invoice番号  請求書。  監査証跡。 |  |  |

2/12個

Annex1\_Compliance\_Guidelines\_Matrix\_19102009.xlsと

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bと | シーディーイー | | | Hと | Iと | Jと | Kと | Lと | Mと |
| 1と | ワオ | プロセスステップ  (順序を調整できる) | ビジネス実装クラスB-D | | | なぜ(リスク) | 何(要件) | どのように(制御) | 参考例。 注。ここに挙げた例は、網羅的なものではなく、想定される対策の種類を示すためにのみ提供されている。 | 追加ガイダンス[「コンプライアンス・ガイドラインの解説書」 参照] | 実装の適用性[自己評価に使用] |
| 24と |  | 2-1マイル | xと | xと | xと | サプライヤからサービスプロバイダに転送された請求書データは、転送中に変更または追加できます。 | 送信中の請求書データの信頼性と整合性を確保します。 | 請求書データは、次の方法で転送するものとする。   1. 通信されるデータの整合性を保護します。 2. データのソースを認証します。 | 1. パスワードによるトランスポート層セキュリティ(RFC 4346)。 2. 署名付きのインターネット利用可能性宣言1, 2, 3によるビジネスデータ交換(RFC 3335、RFC 4130、RFC 4823) 3. 付加価値ネットワークサービスプロバイダが提供する安全なネットワークサービス。 4. ITU-T X .400またはS/MIME (RFC 3851)などのセキュリティで保護されたメッセージングサービス。 5. ハッシュ合計や調整の概要などの整合性メジャー 6. TS 102 640で定義されているような登録済みEメール | 7.3 .8 |  |
| 25と |  | D:完全性と完全性の管理 |  | xと |  | 請求書署名者は、鍵および証明書のセキュリティに関する義務を負いません。  秘密(署名)鍵は、単独の制御を保証する方法では保持されない | 請求書署名者は、秘密鍵の単独管理を保証し、セキュリティおよび潜在的な侵害の報告に関する義務を遵守する必要があります。 | 請求書署名者は、秘密鍵のセキュリティおよび潜在的な侵害の報告に関する義務を遵守するものとします。  さらに、署名は、鍵の保護を保証するために、詐欺に関連する識別されたリスクに対応するメカニズムを使用して作成されなければならない。 | 請求書の受領者となる可能性のあるすべての取引先には、使用されている署名鍵の侵害が疑われる場合には、その旨を通知する。   1. 秘密鍵に対する唯一の制御を保証する国際的に認められた標準に準拠している暗号装置 (例えば、。FIPS 140-2レベルが少なくとも2または3、共通基準EALが少なくとも4) または 2. キーが請求書を発行するビジネスエンティティの単独の制御下にあるように保護された環境に保持されるシステム上に保持されるソフトウェアキー。 |  |  |
| 26と |  | D:完全性と完全性の管理  証明書の管理(CA発行) |  | xと |  | 電子請求書のAdESに使用される証明書は、その運用を適切に管理していないCA (証明機関)によって発行されます。 | CAは、PKI (公開鍵インフラストラクチャ)システムのための優良事例の下で運用されなければならない。 | 署名は、承認された優良事例に対して活動する認証機関によって発行された証明書によって裏付けられなければならない。証明書は,署名を適用する法人の身元を含まなければならない | 認定されているグッドプラクティスの例:ETSI TS 102 042、TS 101 456、またはAICPA/CICA Webtrust。 | 7.3 .3関連項目 |  |
| 27と |  | D:完全性と完全性の管理  証明書の管理(CA発行) | xと |  | xと | 請求書データ交換を保護するために使用される証明書は、その運用を適切に管理していないCAによって発行されます。 | データ交換を保護するために使用される証明書を発行するCAは、PKIシステムの優れたプラクティスの下で動作する必要があります。 | データは、承認された優良事例を扱う認証機関によって発行された証明書によって保護されなければならない。 | 一般に認められているグッドプラクティスの例:ETSI TS 102 042、TS 101 456、またはCA/Browser Forumで定義されているAICPA/CICA WebtrustのExtended Validity Certificates (SSL/TLS証明書用)。 | 7.3 .3関連項目 |  |
| 28と |  | D:完全性と完全性の管理  証明書の管理(自己署名の) |  | x (自己記号  ed) |  | 署名者の身元を偽って不正に作成された証明書 | 自己署名証明書を使用する前に、信頼できる発行元から発行された証明書としてすべての取引先に認証される必要があります。  自己署名証明書の使用は、すべてのEU加盟国で認められているわけではない。 | 自己署名証明書に付随する秘密鍵は、CAの(証明機関)に関して認められた優良事例と同等のレベルで、オンボーディングプロセスにおいて取得された身元の証明と結び付けられるべきである。証明書は、ソースの身元を認証する方法で、事前に当事者間で交換されるものとする。 | CAが認識している優良事例の例:ETSI TS 102 042、TS 101 456、またはAICPA/CICA Webtrust。 |  |  |
| 29と |  | 3-電子請求書の作成 | xと | xと | xと | 電子請求書に実行可能コードが含まれています;電子請求書の完全性が保証されなくなります。 | E-Invoiceに実行可能コードが含まれていないことを確認します。 | 電子請求書の作成者は、電子請求書に実行可能なコードが存在しないことを保証するための措置を講じなければならない。取引先との契約では、E-Invoiceに実行可能コードを含めないことを明記する必要があります。 | 電子請求書内でのマクロの使用を無効にします。  ウイルスやその他の悪意のあるコードがないか、E-Invoiceをスキャンします。  非表示を保持できるドキュメント形式を使用しない  コードとマクロです。 | 7.3 .6 |  |
| 30と |  | 3-電子請求書の作成 | xと | xと | xと | 電子請求書は 「オリジナル」 として複数回作成されます。 | E-Invoiceは、「写し」と記載されていない場合、一度しか作成できないようにする必要があります。何が元の電子請求書を構成するのかを当事者間で明確にしなければならない。 | ワークフローでは、電子請求書または紙媒体のいずれであっても、電子請求書が必ず1回作成されるようにする必要があります。 |  |  |  |
| 31と |  | 3-電子請求書の作成 | xと | xと | xと | 仕入先に代わって発行されたすべてのE-Invoiceが、仕入先によってOracle General Ledgerでレポートされるわけではありません。 | 発行されたE-請求書を検証する方法 | 契約上および内部統制上の措置。発行されたE-Invoiceの仕入先へのレポート。 |  |  |  |

3/12個

Annex1\_Compliance\_Guidelines\_Matrix\_19102009.xlsと

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bと | シーディーイー | | | Hと | Iと | Jと | Kと | Lと | Mと |
| 1と | ワオ | プロセスステップ  (順序を調整できる) | ビジネス実装クラスB-D | | | なぜ(リスク) | 何(要件) | どのように(制御) | 参考例。 注。ここに挙げた例は、網羅的なものではなく、想定される対策の種類を示すためにのみ提供されている。 | 追加ガイダンス[「コンプライアンス・ガイドラインの解説書」 参照] | 実装の適用性[自己評価に使用] |
| 32と |  | 3-電子請求書の作成  サービス・プロバイダが作成した電子請求書 | xと | xと | xと | サービス・プロバイダは、サプライヤが用意した請求書データ以外の請求書データを追加します(合意された濃縮サービスの外部)。 | サービス・プロバイダは請求書データを追加しない(合意された濃縮サービスの外部) | 供給者によって準備または合意されていない電子請求書の作成を防止および検出するための措置が講じられていなければならない。  サービス提供者と供給者間の契約はそれを防止しなければならない。サービスプロバイダシステムでの論理アクセス制御。  論理的なアクセス制御は、適切な職務分離にマップされる必要があります。これは、エンドツーエンドの監査証跡によって証明されます。 | サービス・プロバイダが保管する電子請求書へのレポートおよび/またはアクセスを監査して、仕入先が準備した電子請求書データに基づく電子請求書のみが発行されていることを確認します。 |  |  |
| 33と |  | 3-電子請求書の作成  サービス・プロバイダが作成した電子請求書 | xと | xと | xと | サービス・プロバイダが作成した電子請求書には、合意されたすべてのデータが含まれているわけではありません。 | サービス・プロバイダが作成する電子請求書には、合意されたすべてのデータが含まれている必要があります。 | コンバージョンプロセス、監査証跡、契約のルールを管理します。 | 多数の電子請求書の実体テスト | 6.6 .2 |  |
| 34と |  | 3-電子請求書の作成  サービス・プロバイダが作成した電子請求書 | xと | xと | xと | サービス・プロバイダがすべての電子請求書を作成するわけではありません。 | サービス・プロバイダは、仕入先から提供されたすべてのE-Invoiceを作成する必要があります。 | コンバージョンプロセス、監査証跡、契約のルールを管理します。 | E-Invoicesの発行完了を監査するための合計を生成します。 | 6.6 .2 |  |
| 35と |  | 3-電子請求書の作成  サービス・プロバイダが作成した電子請求書 | xと | xと | xと | サービス・プロバイダがE-Invoiceにデータを追加または変更する場合、そのサプライヤはこの情報を持っていません。 | E-Invoiceの内容の正確性と完全性については、サプライヤが引き続き責任を負います。仕入先は、(〜することができる) E-請求書のすべてのデータにアクセスする必要があります。 | コンバージョンプロセス、監査証跡、契約のルールを管理します。供給者は、発行された電子請求書に常にアクセスできるものとする。変換プロセスは、承認されたマッピングプロセスに従って実行する必要があります。マッピングプロセスは、テストおよび監査が可能で、電子請求書の形式のみを変更し、受信者の必須情報を識別する機能は変更しません。 | 多数の電子請求書の実体テスト | 6.6 .2 |  |
| 36と |  | 3-電子請求書の作成 |  | xと |  | 署名は作成されません。 | E-Invoiceには、整合性と完全性を保護するための高度な電子署名が用意されています。 | アプリケーションは、署名が適用されていることを確認する必要があります。署名は,国際的に認められた標準署名フォーマットに従って作成しなければならない。多数の電子請求書の署名を確認します。 | -ETSI TS 101 733で定義され、TS 102 734でプロファイルされているCAdES-T  -XAdES T (ETSI TS 101 903で定義) およびTS 102 904でのプロファイル  -ISO 32000で規定され、ETSI TS 102 788でプロファイル化されたPDF署名 | 7.2.3.1および7.2.3.4, 7.2.3.5#7.2.3.1オヨビ# |  |
| 37と |  | 3-電子請求書の作成 |  | xと |  | 無効または期限切れの証明書を使用して署名が作成されています | 電子請求書には、有効な証明書付きの高度な電子署名が必要です。 | サプライヤが署名時にCA発行の証明書の有効性を容易に証明できるように、署名当事者は署名を適時に検証して、署名の再検証に必要な情報が容易に入手可能であることを保証する必要があります。 | (サブプロセス) AdESのプロセスステップのアーカイブと監査可能性を参照してください。  現代のアプリケーションや標準がこれを自動的に処理します。 | 7.2.2.8 |  |
| 38と |  | 3-電子請求書の作成 |  | xと |  | すべての必須E-請求書データが署名されているわけではありません。 | 適用法に基づくすべての必須データに署名する必要があります。 | アプリケーションでは、必須の電子請求書データがすべて署名されていることを確認する必要があります。 |  |  |  |
| 39と |  | 3-電子請求書の作成 | xと |  |  | E-Invoiceの構造が、現行の相互交換契約で合意されているE-Invoiceの構造と異なる | 電子請求書の構造は、現行の相互交換契約で合意された電子請求書の構造に準拠している必要があります。 | 構造を交換免除承諾に対して自動的に検証するには、正しい検証メカニズムを維持する必要があります。Commentary report, figures 1&2のsection 5にあるオンボーディングプロセスのステップ (A) における試験要件も参照のこと。 |  |  |  |
| 40と |  | 3-電子請求書の作成 | xと |  |  | 要約ドキュメントの完全性と真正性は保証されない場合があります。形態にかかわらず;紙または電子 | 要約文書が完全性を証明するために用いられる限り、要約文書の完全性と真正性(報告書)が保証されなければならない。 | 対策は、要約文書の完全性と真正性を確保すべきである。 | 要約に適用される拡張電子署名  ドキュメント。  仕入先ステーショナリーに印刷された要約文書。 | 7.2.1.3 |  |
| 41と |  | 3-電子請求書の作成  サービス・プロバイダが作成した電子請求書 | xと | xと | xと | 電子請求書は、仕入先とサービス・プロバイダの両方によって作成されます(合意に従わない)。 | E-Invoiceは、契約で指定された発行者のみが作成できるようにする必要があります。電子請求書を発行する当事者間で明確である必要があります。 | この管理では、E-Invoiceの作成/発行が1回のみであることを確認する必要があります。 |  |  |  |

4/12個

Annex1\_Compliance\_Guidelines\_Matrix\_19102009.xlsと

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Bと | シーディーイー | | | Hと | Iと | Jと | Kと | Lと | Mと |
| 1と | ワオ  プロセスステップ  (順序を調整できる) | ビジネス実装クラスB-D | | | なぜ(リスク) | 何(要件) | どのように(制御) | 参考例。 注。ここに挙げた例は、網羅的なものではなく、想定される対策の種類を示すためにのみ提供されている。 | 追加ガイダンス[「コンプライアンス・ガイドラインの解説書」 参照] | 実装の適用性[自己評価に使用] |
| 42と | 4-送信または使用可能にする | xと | xと | xと | 作成されたE-Invoiceは期限内に送信されないか、利用できません。 | 供給者は、適用される法律に従って適時に、電子請求書が送付または利用可能にされることを確実にしなければならない | 適切な場合には、サービス提供者との申請または契約に含まれる内部統制の行動。 |  |  |  |
| 43と | 4-送信または使用可能にする | xと | xと | xと | 電子請求書が送信されたかどうか、または利用可能になったかどうかに関する論争。 | E-Invoiceを送付/提供する必要があります。 | E-請求書の送信/取得の監査レコードを保守します。 | 電子請求書の送信または検索、および関連する確認が記録されます。  可能な場合には、送付及び、該当する場合には、送達についての信頼できる証拠を提示するシステムを利用することが望ましい。ETSIは、2008 TS 102 640の後半に、送信されたE-Invoicesにこのような証明を提供するのに適したRegistered E-Mail (レム)メカニズムの条項を規定した複数パートの技術仕様を発行します。 |  |  |
| 44と | 4-送信または使用可能にする | xと |  |  | 信頼性は、無効または期限切れの証明書に基づいています。 | 署名されていないE-Invoiceの転送を保護するために証明書を使用する場合、その証明書は有効である必要があります。 | 証明書の有効性の内部管理。 | (サブプロセス) AdESのプロセスステップのアーカイブと監査可能性を参照してください。  現代のアプリケーションや標準がこれを自動的に処理します。 | 7.2.2.8 |  |
| 45と | 4-送信または使用可能にする | xと |  |  | 誤った請求データは、仕入先を装ったパーティによって送信されるか、輸送中に変更されます。 | 電子請求書の真正性と完全性は、EDIプロセス内で保証されなければならない。 | 請求書データは、次の方法で転送するものとする。   1. 通信されるデータの整合性を保護します。 2. データのソースを認証します。 | 1. パスワードによるトランスポート層セキュリティ(RFC 4346)。 2. 署名付きのインターネット利用可能性宣言1, 2, 3によるビジネスデータ交換(RFC 3335、RFC 4130、RFC 4823) 3. 付加価値ネットワークサービスプロバイダが提供する安全なネットワークサービス。 4. ITU-T X .400またはS/MIME (RFC 3851)などのセキュリティで保護されたメッセージングサービス。 5. ハッシュ合計や調整の概要などの整合性メジャー 6. TS 102 640で定義されているような登録済みEメール | 7.3 .8 |  |
| 46と | 4-送信または使用可能にする | xと |  | xと | 購入者は、電子請求書が使用可能になっていることを知りません。 | E-Invoiceが送付されたとき、または利用可能になったときは、取引先間での理解が必要です。 | 通知の送信;アプリケーションでこのリスクに対処することは良いプラクティスです。;いつ、誰に通知が送信されたかを記録します。  契約上のルール。 | 通知に電子メールを使用する場合は、受信者からの電子メールで配信確認を要求します。 |  |  |
| 47と | 4-送信または使用可能にする |  |  | xと | 提示されたE-Invoicesはバイヤーによるレビューを受けません。 | 受入処理を正しく実行するために、購買担当はE-Invoicesをレビューする必要があります。 | E-Invoiceをレビューするのはバイヤーの責任であることをバイヤーに明確に理解してもらうことをお勧めします。  電子請求書へのアクセスをログに記録します。 | Web環境では、E-Invoicesの表示に関する監査証跡を表示できます。特定の期間内に電子請求書にアクセスしない場合は、アプリケーションでアラートを生成します。 |  |  |
| 48と | 4-送信または使用可能にする |  |  | xと | 電子請求書は2回提示されるため、購入者はVATを2回請求できますが、サプライヤはVATを1回しか報告しません。 | 電子請求書は一度しか提出できず、一意に識別できるものでなければなりません。 | ワークフローでは、電子請求書が1回表示され、取引が正しく処理されていることを確認する必要があります。提示されたE-Invoiceは、オリジナルのE-Invoiceです。したがって、提示されたE-Invoicesは、文書名や一意の番号などから一意に識別できる必要があります。 |  |  |  |
| 49と | 4-送信または使用可能にする |  |  | xと | すべての電子請求書が表示されるわけではありません。訂正E-請求書に対する特別な注意。 | すべての電子請求書を提示する必要があります。訂正E-Invoiceに対する特別な注意。 | アプリケーション監査と内部統制活動。 |  |  |  |
| 50と | 4-送信または使用可能にする |  |  | xと | 間違ったWebサーバが調査される(スプーフィング) | E-Invoicesにアクセス可能なサーバは、購入者に対して検証可能な方法で認証を受ける必要があります。 | ウェブサーバを認証するための仕組みがあること。整合性と完全性の管理の要件(Commentary reportのセクション5、図1および図2のプロセスステップD)も参照してください。 | 十分に強力なサーバー証明書を使用したSSL/TLSによる認証。  電子請求書が保管されているサーバは、購入者が電子メールのリンク(一部の加盟国の法的要件)を使用して利用できるようにしておく必要があります。  CAブラウザフォーラムで定義された拡張検証証明書を使用することをお勧めします。 | 七・三 |  |
| 51と | 4-送信または使用可能にする |  |  | xと | Webサーバーに保持されている間に電子請求書が変更されました | Webサーバー上では、電子請求書を承認された方法で変更することはできません。 | Webシステムは、Webサーバのセキュリティに関して認識された優良事例の下で動作し、E-Invoiceへのアクセスを制御します。 |  |  |  |

5/12個

Annex1\_Compliance\_Guidelines\_Matrix\_19102009.xlsと

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bと | シーディーイー | | | Hと | Iと | Jと | Kと | Lと | Mと |
| 1と | ワオ | プロセスステップ  (順序を調整できる) | ビジネス実装クラスB-D | | | なぜ(リスク) | 何(要件) | どのように(制御) | 参考例。 注。ここに挙げた例は、網羅的なものではなく、想定される対策の種類を示すためにのみ提供されている。 | 追加ガイダンス[「コンプライアンス・ガイドラインの解説書」 参照] | 実装の適用性[自己評価に使用] |
| 52と |  | 4-送信または使用可能にする  サービス・プロバイダが作成した電子請求書 | xと | xと | xと | 誰がE-Invoiceを発行したかは不明  処理に使用される請求書データがオリジナルのE-Invoiceと異なる | E-Invoiceは、契約で指定された発行者のみが発行できるようにする必要があります。電子請求書を発行する当事者間で明確である必要があります。  バックエンド・システムでの自動データ処理には変換が必要ですが、変換後のE-Invoiceを監査できる元のE-Invoiceを保持する必要があります。 | 取引相手とサービス提供者との間の契約における規則は、誰が電子請求書を発行するかについて明確にしなければならない。電子請求書には、第三者がサプライヤの名義で発行したことを記載できます(これはいくつかの加盟国で必須である)。  コンバージョン処理、監査証跡、契約のマッピング・ルールを制御します。供給者と購入者は、常に元の電子請求書にアクセスできるものとする。 | 1. 適切に文書化され、バージョン管理され、テストされたマッピングを使用します。 2. 換算済請求書内で、オリジナルの電子請求書を単一の署名済フィールド文字列(区切り記号付き)として表します。変換された請求書データは、元の請求書データと自動的に照合されます。 | 6.6 .2  7.3 .1,6.6 .2#7.3 .1# |  |
| 53と |  | 4-送信または使用可能にする | xと | xと | xと |
| 54と |  | 4-送信または使用可能にする | xと | xと | xと | 換算済E-Invoiceは、アプリケーションまたは換算済E-7.3 .1と換算済E-7.3 .2の日次カウントの比較に含まれる内部統制の処理に換算が必要です。  必要に応じて、サービス・プロバイダとの契約に基づいてデータを自動的に処理します。 請求書  請求書はバックエンド・システムでは使用できませんが、  元のE-Invoiceではなく、仕入先または購買担当 (あるいはその両方) が、元のE-Invoiceを単一の署名付きフィールドとして表示している必要がある  変換後のE-Invoiceにおいて、オリジナルと同様に利用可能であり、(区切り記号付き)という文字列を使用することで、  監査の場合、オリジナルEとは異なる-個別のE-Invoiceメッセージ (オリジナル  電子請求書は、すべてのパーティによって請求書が提示され、換算されます。)  各当事者のオリジナルとして | | | | |  |
| 55と | すべて | (仕入先および購買担当サイド) |  |  |  |  | | | | |  |
| 56と |  | 汎用-データ/メッセージ転送  この処理ステップは、E-Invoice転送チェーンの当事者間のデータ交換に適用されます。 | xと |  | xと | チェーン加入者間で転送された請求書データまたはE-請求書は、転送中に変更または追加できます。 | 送信中のデータの信頼性と整合性を確保します。 | データは,次の方法で転送される。   1. 通信されるデータの整合性を保護します。 2. データのソースを認証します。 | 1. パスワードによるトランスポート層セキュリティ(RFC 4346)。 2. 署名付きのインターネット利用可能性宣言1, 2, 3によるビジネスデータ交換(RFC 3335、RFC 4130、RFC 4823) 3. 付加価値ネットワークサービスプロバイダが提供する安全なネットワークサービス。 4. ITU-T X .400またはS/MIME (RFC 3851)などのセキュリティで保護されたメッセージングサービス。 5. ハッシュ合計や調整の概要などの整合性メジャー 6. TS 102 640で定義されているような登録済みEメール 7. AdESが適用された場合、受信側で整合性を検証可能 | 7.3 .8 |  |
| 57と |  | C:アーカイブと監査機能 |  | xと |  | 電子請求書の署名時または受領時に証明書が有効であったことを確認することはできません。 | 高度な電子署名は、保存期間中も検証可能でなければならない。 | 電子請求書を発行する場合は、使用した署名を検証する必要があります(前述のプロセス・ステップ 「E-Invoiceの作成」 を参照してください。;Commentary report, figures 1&2のセクション5のステップ3。)。署名時又はその前後に署名の有効性を再検証するために必要なすべての情報を容易に入手することができるものとする。 | -証明書および失効情報の記録  -ETSI TS 101 733のCAdES-C、CAdES-A、またはCAdES-XおよびTS 102 734のプロファイル  -ETSI TS 101 903に定義されているXAdES-C、XAdES-A、またはXAdES-XおよびTS 102 904にプロファイルされているXAdES-C  注意：PDF署名の長期的な検証を目的とした(パッド) CAdES/XAdES-C~-Aと同等のフォームは、ETSIの2009年第3四半期より発行される予定です。 | 7.2.2.8、7.3 .4#7.2.2.8# |  |
| 58と |  | C:アーカイブと監査機能 |  | xと |  | E-Invoiceの整合性を検証することはできません。 | 高度な電子署名は、保存期間中も検証可能でなければならない。 | 署名を再検証するために使用される情報(前述のプロセス・ステップ 「E-Invoiceの作成」 を参照してください。;Commentary reportのセクション5の図1と2の3。)を含め、署名された電子請求書の完全性は、署名アルゴリズムおよび証明書の存続期間を超えて維持されるものとする。 | 1. ETSI TS 101 733で定義されており、TS 102 734でプロファイルされているCAdES-Aの署名にアーカイブタイムスタンプを適用する 2. ETSI TS 101 903で定義されており、TS 102 904でプロファイルされているXAdES-Aでの署名へのアーカイブタイムスタンプの適用 3. 監査可能なアーカイブ・プロセス内でのWORMデバイスの使用。 4. データのアーカイブに信頼できるサード・パーティ・サービス (例:。公証人) 5. データの完全性を維持するアーカイブシステムの採用   注意：PDF署名の長期的な検証を目的とした(パッド) CAdES/XAdES-XLおよび-Aと同等のフォームは、2009年第3四半期にETSIから発行される予定です。 | 7.2.2.8、7.3 .4#7.2.2.8# |  |

6/12個

Annex1\_Compliance\_Guidelines\_Matrix\_19102009.xlsと

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Bと | シーディーイー | | | Hと | Iと | Jと | Kと | Lと | Mと |
| 1と | ワオ  プロセスステップ  (順序を調整できる) | ビジネス実装クラスB-D | | | なぜ(リスク) | 何(要件) | どのように(制御) | 参考例。 注。ここに挙げた例は、網羅的なものではなく、想定される対策の種類を示すためにのみ提供されている。 | 追加ガイダンス[「コンプライアンス・ガイドラインの解説書」 参照] | 実装の適用性[自己評価に使用] |
| 59と | C:アーカイブと監査機能 | xと | xと | xと | 電子請求書は、法定アーカイブ期間にはアーカイブされません。 | 発行されたE-請求書および受領されたE-請求書は、適用法に基づく法定保管期間中に保管しなければなりません。 | これは、目的のアーカイブ手順に合わせて対処する必要があります。 |  |  |  |
| 60と | C:アーカイブと監査機能 | xと | xと | xと | 合理的な期間内に電子請求書を入手できない | 税務調査官の要請があれば、電子請求書は義務期間全体にわたって速やかに利用可能にしなければならない。 | 照会は、合理的な期間内に行うことができる。 | オンライン・アクセスを使用して、迅速なアクセス、E-Invoice番号によるアクセス、取引先および日付範囲を提供 |  |  |
| 61と | C:アーカイブと監査機能 | xと |  | xと | アーカイブE請求書は、合意されたアーカイブ期間内に変更または削除できます。 | 保管されたE-Invoicesの内容の真正性と完全性は、保管期間を通じて保証されなければなりません。 | 電子請求書および電子請求書の取り扱いに関する監査記録 (実施された認証チェックに関する情報を含む) は、保管期間を通じてデータの完全性を保証する仕組みによって保護されるものとする。 | -WORM (Write Once Read Many (書き込み1回読み取り複数回))タイプデバイスの使用-セキュアなアーカイブストレージ。  -完全性が損なわれていることを示す要約文書又はタイムスタンプ | 7.2.1.3,7.3 .4#7.2.1.3# |  |
| 62と | C:アーカイブと監査機能 | xと | xと | xと | 電子請求書は監査できません。 | 電子請求書は、要求に応じて合理的な期間内に監査可能でなければならない。 | 電子請求書が権限のある税務当局にとって読みやすいものであることを確保するための措置が実施されなければならない。 | UNレイアウトキーなどでオンラインで利用可能なビューア。所轄税務当局の監査ソフトウェアがインターペットできる書式を使用してください。 |  |  |
| 63と | C:アーカイブと監査機能 | xと | xと | xと | 人間が読める形式は、機械が処理する形式と同じではありません。 | 人間が読むことができる形式が符号化された形式と同じであることが証明できなければならない。 | 電子的E-Invoiceから可視形式へのマッピングが正しいことを実証できるものとする。同一の可読形式を再現することが可能でなければならない。  使用されているコードが正しいことは証明できるものとする。使用するコードは、次のいずれかでなければなりません。-正式な仕様または公開されている仕様で標準化されていること。  または、真正性と完全性がE-Invoicesの保存と同じセキュリティ・レベルで保護されている内部文書で指定されている。 | 信頼性の高いスタイルシートまたはPDFドキュメントを組み合わせて使用する |  |  |
| オンラインビューアを使用して |
| 64と | C:アーカイブと監査機能 | xと | xと | xと | E-Invoiceは、パラメータ、コード・テーブル、計算ルールなどのマスター・データの保存が歴史的に不適切であるため、正確かつ完全には再現できません。 | E-Invoicesは、保存期間中、正確かつ完全に利用可能である必要があります。 | すべてのデータを請求アプリケーションから分離するか、履歴を含む正確なデータストレージに保存します。 | 1つのファイルにすべてのE-Invoiceデータを保存(構造化されたデータを含むXMLまたはPDF)-E-Invoiceを参照する別のファイルとして保存されたE-Invoice履歴+年次履歴レポートが作成および保存される |  |  |
| 65と | C:アーカイブと監査機能 | xと | xと | xと | 監査証跡が正しく維持されていない | 保存期間中、適切な監査証跡が利用可能でなければならない | 監査証跡を保持する | マッピング、日付の記録、ログなどのキー・プロセス情報を保持します。また、次のようなドキュメントも保持します。  発注、発送通知、...。 | 7.3.7 |  |
| 66と | バイヤー側 |  |  |  |  | | | | |  |
| 67と | 5-受領書及び技術的検証 | xと | xと | xと | 購買担当の環境では、E-請求書を受信できません。 | 電子請求書を受領するための技術的可用性が確保されなければならない。電子請求書の正確、完全かつ迅速な受領が適切に保証されなければならない。 | Commentary report, figures 1&2のセクション5のプロセスステップGeneric (0) およびOn-boarding (A) も参照してください。受領したE-Invoiceおよびクレジット・ノートの完全性に関する手順またはアプリケーション・チェック。 |  |  |  |
| 68と | 5-受領書及び技術的検証 | xと | xと | xと | 電子請求書は複数回受信されます。 | 電子請求書の複数受入を検出する必要があります。複数のE-請求書を削除し、以降の処理から除外する必要があります。 | アプリケーション・チェックにより、複数回受信したE-Invoiceを検出し、原因を徹底的に分析して以降の処理から除外します。 |  |  |  |

7/12個

Annex1\_Compliance\_Guidelines\_Matrix\_19102009.xlsと

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Bと | シーディーイー | | | Hと | Iと | Jと | Kと | Lと | Mと |
| 1と | ワオ  プロセスステップ  (順序を調整できる) | ビジネス実装クラスB-D | | | なぜ(リスク) | 何(要件) | どのように(制御) | 参考例。 注。ここに挙げた例は、網羅的なものではなく、想定される対策の種類を示すためにのみ提供されている。 | 追加ガイダンス[「コンプライアンス・ガイドラインの解説書」 参照] | 実装の適用性[自己評価に使用] |
| 69と | 5-受領書及び技術的検証 | xと | xと | xと | 電子請求書は技術的な理由で拒否されます。 | 電子請求書は、さらに処理される前に技術的に正確である必要があります。拒否されたE-請求書は、個別に識別できる必要があります。 | 電子請求書の技術基準についての完全な合意が存在し、適切にテストされなければならない。  技術的な不正確さを迅速に検出し、何らかの形の通知 (例:。XML応答または電子メール) 。受信したE-Invoiceの処理を停止する必要があります。送信者は、正しいE-Invoiceを再度送信するか、クレジット・ノートと訂正E-Invoiceを発行する必要があります。 |  |  |  |
| 70と | 5-受領書及び技術的検証 | xと | xと | xと | 購入者またはサービス・プロバイダがすべてのE-請求書を受け取っているわけではありません(クレジット・ノートを含む)。 | 購入者またはサービス・プロバイダは、送信されたすべての電子請求書を受け取る必要があります。 | すべての電子請求書が適切に受領されることを確実にするための適切な手続きが存在しなければならない。すべての受信E-Invoiceの登録 | 可能であれば、E-Invoiceを受け取った際のハンドシェークまたは確認。 |  |  |
| 71と | 5-受領書及び技術的検証 | xと | xと | xと | 電子請求書が受信されたかどうかに関する論争。 | 呼び出しの受信/取得の監査レコードを保持します。 | E-Invoiceの受領または検索、および関連する確認が記録されます。 | 可能であれば、E-Invoiceを受け取った際のハンドシェークまたは確認。  ETSI TS 102 640 (レム)は、メッセージの配信および送信者の証拠を提供するメカニズムを提供します。 |  |  |
| 72と | 5-受領書及び技術的検証 | xと | xと | xと | 電子請求書に実行可能コードが含まれています。 | E-Invoiceに実行可能コードが含まれていないことを確認 | 受信者は、電子請求書に実行可能コードがないことを確認するものとする。取引先との契約では、実行可能コードが電子請求書の一部にならないことを明記する必要があります。 | 請求書エンコードでのマクロの使用を無効にする;ウイルスやその他の悪意のあるコードがないか、E-Invoiceをスキャンします。 | 7.3 .6 |  |
| 73と | 5-受領書及び技術的検証 | xと | xと | xと | 正式な受け取りの時期は不明です。 | 輸送における真正性と完全性の測定は、正式な受領の瞬間まで実施されるべきである。E-Invoiceを正式に受領した時点から、元のE-Invoiceへの変更を防止することにより、完全性と信頼性を確保する必要があります。 | 契約上のルール | -ETSI TS 102 640 (レム)は、納品時点の証拠も提供します。  -AS 2は、メッセージ受信時にタイムスタンプ付きメッセージ配信(MDN)を提供します。 |  |  |
| 74と | 5-受領書及び技術的検証 |  | xと |  | 電子請求書に(または無効)署名がないか、発行者が特定できない | 電子請求書の真正性と完全性は、高度な電子署名によって保証されなければならない。認証メカニズム(購入者に)は、発行者の明確な識別を保証しなければならない。 | アプリケーションを処理またはチェックインします。電子請求書または電子メールに高度なデジタル署名があることを確認します。それ以外の場合は、電子請求書を拒否します。 |  | 7.2.2.1から7.2.2.8 |  |
| 75と | 5-受領書及び技術的検証 |  | xと |  | 署名が検証された時間の間の不確実性と、それによる証明書の状態の曖昧さの可能性。 | 高度な電子署名が検証された時間を記録します。(EU加盟国によってルールは異なる。) | 検証の正確な時刻が記録されていることを保証する | 署名がまだタイムスタンプまたは信頼されたタイムマークを含んでいない場合、信頼されたタイムマークまたはタイムスタンプを適用することができる。  (例:。CAdES、XAdESまたはPAdESの長期形態で指定されている場合) | 7.2.2.8 |  |
| 76と | 5-受領書及び技術的検証 |  | xと |  | 署名を検証する際に適用される規則に対する不確実性。 | 高度な電子署名を検証するために適用されるプロセス/ソフトウェアは、識別可能かつ信頼できるものでなければならない。 | 署名の検証に用いたプロセス/ソフトウェア(バージョンとパッチを含むソフトウェア)の記録を保管すること。 | CEdES、XAdES、およびPAdESのEPES形式のように、署名ポリシー識別子を含めます。 | 7.2.2.1 |  |

8/12個

Annex1\_Compliance\_Guidelines\_Matrix\_19102009.xlsと

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Bと | シーディーイー | | | Hと | Iと | Jと | Kと | Lと | Mと |
| 1と | ワオ  プロセスステップ  (順序を調整できる) | ビジネス実装クラスB-D | | | なぜ(リスク) | 何(要件) | どのように(制御) | 参考例。 注。ここに挙げた例は、網羅的なものではなく、想定される対策の種類を示すためにのみ提供されている。 | 追加ガイダンス[「コンプライアンス・ガイドラインの解説書」 参照] | 実装の適用性[自己評価に使用] |
| 77と | 5-受領書及び技術的検証 | xと |  |  | アプリケーションで電子請求書を処理できません。 | 電子請求書は、現行の相互交換契約の(テクニカル)要件に準拠している必要があります。 | E-Invoiceは、Commentary reportのセクション5、図1および図2のProces step A Trading partner Onboardingでテストされます。  いかなる誤りも、何らかの形で送信者に通知すべきである (例えば、。XML応答または電子メール) | 要件は、例えば、保護、登録簿へのE-Invoicesの登録、必須項目、証拠としてのEDI報告書の受理可能性に関連するかもしれない。例えば、勧告94/820/EC参照 |  |  |
| 78と | 5-受領書及び技術的検証 | xと |  | xと | 転送中に元の電子請求書の内容または形式が変更された場合 | 発行されたE-Invoiceが転送中に変更されたかどうかを検出できる必要があります。 | 購入者のプロセス内で、合意された安全なメカニズムが適用されていることを確認/チェックする必要があります。 | 1. パスワードによるトランスポート層セキュリティ(RFC 4346)。 2. 署名付きのインターネット利用可能性宣言1, 2, 3によるビジネスデータ交換(RFC 3335、RFC 4130、RFC 4823) 3. 付加価値ネットワークサービスプロバイダが提供する安全なネットワークサービス。 4. ITU-T X .400またはS/MIME (RFC 3851)などのセキュリティで保護されたメッセージングサービス。 5. ハッシュ合計や調整の概要などの整合性メジャー 6. TS 102 640で定義されているような登録済みEメール。EDIの場合は、要約文を使用して保護することもできます。 | 7.3 .8 |  |
| 79と | 5-電子請求書データの受領および技術的検証の変換 | xと | xと | xと | 元の電子請求書が変換され、元の電子請求書の新規インスタンスとして処理されます。 | オリジナルのE-Invoiceは1つのみで、オリジナルとそれから派生した請求書データのセットの間に監査証跡を保持する必要があります。 | オリジナルのE-Invoiceをアーカイブします。監査証跡。 | 多数の電子請求書の実質的なテスト | 6.6 .2 |  |
| 80と | 5-電子請求書データの受領および技術的検証の変換 | xと | xと | xと | 請求書データが不完全または正しく変換されていません。 | 請求書データの変換によって、元の電子請求書の内容が変更されることはありません。完全性と相互性の測定は検証可能なままでなければならない。 | 詳細なプロセス・ステップとマッピングは、監査証跡で定義およびトレースする必要があります。 |  | 6.6 .2 |  |
| 81と | 5-電子請求書データの受領および技術的検証の変換 | xと | xと | xと | 請求書データに新しいデータが追加されます。 | E-Invoiceですでに入手可能なデータのみを購入者のシステムに変換する必要があります。 | オリジナルのE-Invoiceをアーカイブします。変換が正しく完了していることを確認します。監査証跡。内部ビジネス・データを電子請求書に追加できます。;これにより、既存の必須データが損なわれることはありません。 | 多数の電子請求書の実質的なテスト | 6.6 .2 |  |
| 82と | 5-受領書及び技術的検証 |  |  | xと | E-Invoiceにアクセスできない (サプライヤ/プレゼンタ環境では、提示された請求書をチェックできない) | 電子請求書はアクセス可能である必要があります | 協定及び一般供給条件。契約後の条件については、Commentary report, figures 1&2のセクション5のprocess step Off-boarding Eも参照。 |  |  |  |
| 83と | 5-受領書及び技術的検証 |  |  | xと | 次の場合、通知を受信した後にE-Invoiceにアクセスできない(速やかに)  Webアクセス | すべての通知によって、E-Invoiceにアクセスする必要があります。 | 手順とガイドライン。 | アクセスの監査証跡を提供するオンライン・ソリューション |  |  |
| 84と | 5-受領書及び技術的検証 |  |  | xと | 誰が電子請求書を使用可能にしたかを確認することはできません。 | オンライン電子請求書は、身元と真正性が確認できるウェブサイトでのみ閲覧できます。 | アプリケーション/Webブラウザのチェックイン | 十分に強力なサーバー証明書を使用したSSL/TLSによる認証。CAB Forumで定義されている拡張検証証明書を使用することをお勧めします。 | 七・三 |  |
| 85と | D:完全性と完全性の管理  証明書の管理(自己署名) |  | x (自己記号  ed) |  | 高度な電子署名を検証するために必要な自己署名証明書は信頼できません。 | 署名検証では、既知の信頼できる取引先からのものとして認証された自己署名証明書のみを使用する必要があります。(自己署名証明書の使用は、すべてのEU加盟国で認められているわけではない。) | 自己署名証明書は、  認可されたCAのグッドプラクティスに匹敵するレベルでのオンボーディングプロセス。  証明書は、ソースの身元を認証する方法で、事前に当事者間で交換されるものとする。 | CAのグッドプラクティスには、ETSI TS 102 042、TS 101 456、またはAICPA/CICA Webtrustが含まれます。 |  |  |

9/12個

Annex1\_Compliance\_Guidelines\_Matrix\_19102009.xlsと

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bと | シーディーイー | | | Hと | Iと | Jと | Kと | Lと | Mと |
| 1と | ワオ | プロセスステップ  (順序を調整できる) | ビジネス実装クラスB-D | | | なぜ(リスク) | 何(要件) | どのように(制御) | 参考例。 注。ここに挙げた例は、網羅的なものではなく、想定される対策の種類を示すためにのみ提供されている。 | 追加ガイダンス[「コンプライアンス・ガイドラインの解説書」 参照] | 実装の適用性[自己評価に使用] |
| 86と |  | D:完全性と完全性の管理  証明書の管理(CA発行) |  | xと |  | 署名の検証に必要なCA証明機関の証明書が信頼されていません。 | 署名検証は、その運用を適切に管理するCAによって発行された証明書を使用しなければならない。 | 署名検証システムには、優良事例として認められた認証機関からの証明書のみを設定するものとする。 | CAでは、ETSI TS 102 042、TS 101 456、またはAICPA/CICA Webtrustを推奨しています。 | 7.3 .3関連項目 |  |
| 87と |  | D:完全性と完全性の管理  証明書の管理(自己署名) |  | x (自己記号  ed) |  | 署名証明書の失効状態が不明です。 | 署名の検証では、証明書の状態を確認する必要があります。  (自己署名証明書の使用は、すべてのEU加盟国で認められているわけではない。) | 鍵が危殆化した場合や証明書が無効であると考えるその他の理由がある場合には、購入者に通知するという契約上の誓約が署名者からなされるべきである。 |  |  |  |
| 88と |  | D:完全性と完全性の管理  証明書の管理(CA発行) |  | xと |  | 署名証明書の失効状態が不明です。 | 署名の検証では、証明書の状態を確認する必要があります。 | 署名検証ソフトウェアは、署名証明書のステータスをチェックする必要があります。 | 有効期間および証明書失効リスト(X.509とIETF RFC 3280で定義されている)またはOCSPサーバー(IETF RFC 2560)を確認します。 | 7.2.2.6および7.2.2.7 |  |
| 89と |  | D:完全性と完全性の管理  証明書の管理(自己署名) |  | xと |  | 電子請求書データ交換を保護するために使用される証明書は、自己署名した発行者のものではありません。 | データ交換は、信頼できる証明書発行者からの証明書を使用して保護する必要があります。(自己署名証明書の使用は、すべてのEU加盟国で認められているわけではない。) | データは、信頼できる供給者によって発行された証明書によって保護されなければならない。信頼できる供給者は、認証局のために認められたグッドプラクティスと同等の実践を行っている。証明書は、ソースの身元を認証する方法で、事前に当事者間で交換されるものとする。 | CAのグッドプラクティスには、ETSI TS 102 042、TS 101 456、またはAICPA/CICA Webtrust、CA/Browser Forumによって定義されたExtended Validity証明書などがあります。 |  |  |
| 90と |  | B-マスター・データ | xと |  |  | E-Invoiceでは、パラメータ、コード表、計算ルールなどのマスター・データの保存がこれまで正しく行われていなかったため、正確かつ完全には再現できません。 | 参照データを含む正しい電子請求書を複製することが可能でなければならない | マスタデータバージョンの履歴を保持する |  |  |  |
| 91と |  | 6-正式な検証 | xと | xと | xと | 電子請求書には、すべての必須データが含まれていないか、間違った法人宛のものが含まれていません。 | 電子請求書は、国固有の必須データに準拠する必要があります。 | アプリケーションでは、電子請求書を処理する前に、VAT法に従って電子請求書にすべての必須データが含まれていることを確認する必要があります。 |  |  |  |
| 92と |  | 6-正式な検証 |  | xと |  | 電子請求書は修正されるか、または別の当事者が発行者になりすましている可能性があります。 | 電子請求書の出所の認証および完全性は、高度な電子署名を検証することによって検証されなければならない。 | AdES署名の有効性をチェックし、検証時間と情報 (例:。CRLまたはOCSPと証明書) を使用して署名を検証します。 | 可能であれば、検証者は、失効が報告されたことを保証するために、署名が有効であることを確認するまで猶予期間を待つべきである。ただし、自動化されたビジネス・プロセスのためにこれが現実的でない場合は、電子請求書の発行者と受信者の間で、署名キーに対する潜在的な侵害が受信者に直ちに報告されるという合意がある必要があります。 | 7.2.2.6 |  |
| 93と |  | 6-正式な検証 |  | xと |  | 電子請求書には、すべての必須データを保護しない署名があります。 | すべての必須データの完全性は、高度な電子署名によって保護されるものとする。買い手はこれを確認するものとする。 | 手順またはアプリケーションのチェック。 |  |  |  |
| 94と |  | 6-正式な検証 | xと |  |  | 電子請求書が変更されているか、別の当事者が供給者になりすましている可能性があります。 | 電子請求書の出所の認証は、チャネルを検証することによって検証されなければならない  電子請求書が受信されるトラフ。 | 電子請求書発行者の認証された身元、およびすべての完全性チェックコードがチェックされ、認証時刻を含む結果が記録されるものとする。 |  |  |  |
| 95と |  | 6-正式な検証 | xと |  |  | 購買担当は、相互交換契約なしで仕入先からE-Invoiceを受け入れます。 | 電子請求書は、相互交換契約がある仕入先から発行されている必要があります。 | アプリケーションチェック;EDI業者として知られています。固定データの入力および変更手順。プロセスステップのオンボーディングAも参照してください。 |  |  |  |

10/12個

Annex1\_Compliance\_Guidelines\_Matrix\_19102009.xlsと

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Bと | シーディーイー | | | Hと | Iと | Jと | Kと | Lと | Mと |
| 1と | ワオ  プロセスステップ  (順序を調整できる) | ビジネス実装クラスB-D | | | なぜ(リスク) | 何(要件) | どのように(制御) | 参考例。 注。ここに挙げた例は、網羅的なものではなく、想定される対策の種類を示すためにのみ提供されている。 | 追加ガイダンス[「コンプライアンス・ガイドラインの解説書」 参照] | 実装の適用性[自己評価に使用] |
| 96と | 6-正式な検証 |  |  | xと | 電子請求書は修正されるか、または別の当事者が発行者になりすましている可能性があります。 | 電子請求書の出所の認証は、チャネルを検証することによって検証されなければならない  Webサーバーにアクセスするトラフ | ウェブシステムは、ウェブサーバのセキュリティのために認められた優良事例の下で動作し、電子請求書へのアクセスを管理します。E-Invoiceは、次のような安全なチャネルを通じて送信されます。   1. 購入者または購入者のサービス・プロバイダまでの電子請求書の整合性を保護します。 2. 電子請求書の発行者を購入者または購入者のサービス・プロバイダに認証します。これは次のいずれかです。   o認証情報は、 | 1. パスワードによるトランスポート層セキュリティ(RFC 4346)。 2. 署名付きのインターネット利用可能性宣言1, 2, 3によるビジネスデータ交換(RFC 3335、RFC 4130、RFC 4823) 3. 付加価値ネットワークサービスプロバイダが提供する安全なネットワークサービス。 4. ITU-T X .400またはS/MIME (RFC 3851)などのセキュリティで保護されたメッセージングサービス。 5. ハッシュ合計や調整の概要などの整合性メジャー | 7.3 .8 |  |
| 97と | 6-正式な検証 | xと | xと | xと | 遅延電子請求書支払 | 電子請求書の受領者は、取引先との合意に基づき、文書レベルまたは明細項目レベルのいずれかで文書の受理または拒否を許可されるべきである。 | 購入者および供給者は、電子請求書の一部支払を受け入れるか、または電子請求書の短期支払を許可/拒否するかについて合意することができる。様々な規模の供給者の様々なキャッシュフロー、運転資本要件、および回収プロセスは、買い手のシステムによって決定されるべきではない。  地方の立法がこの要件をどのように扱うかによって違いがあるかもしれない。 |  |  |  |
| 98と | 7-最後のマイル | xと | xと | xと | サービスプロバイダによって購入者に転送された請求書データは、転送中に変更または追加することができる。 | 送信中の請求書データの完全性と整合性を確保します。 | 請求書データは、次の方法で転送するものとする。   1. 通信されるデータの整合性を保護します。 2. データのソースを認証します。 | 1. パスワードによるトランスポート層セキュリティ(RFC 4346)。 2. 署名付きのインターネット利用可能性宣言1, 2, 3によるビジネスデータ交換(RFC 3335、RFC 4130、RFC 4823) 3. 付加価値ネットワークサービスプロバイダが提供する安全なネットワークサービス。 4. ITU-T X .400またはS/MIME (RFC 3851)などのセキュリティで保護されたメッセージングサービス。 5. ハッシュ合計や調整の概要などの整合性メジャー 6. TS 102 640で定義されているような登録済みEメール | 7.3 .8 |  |
| 99と | 8-材料検証および処理 | xと | xと | xと | E-Invoiceが2回発生 | 各E-Invoiceの記帳は1回のみ | (アプリケーション)重複するE-Invoiceを検出し、処理されないようにするためのコントロール |  |  |  |
| 100と | 8-材料検証および処理 | xと | xと | xと | 電子請求書の内容が適時にチェックされず、処理されない | 各トランザクションとコンテンツの整合性は、受信時に適切な時間内にチェックして処理する必要があります。 | (アプリケーション)注文、物品受領等の管理及び調整。 |  |  |  |
| 101と | 8-材料検証および処理 | xと | xと | xと | 「不正または不正」 -請求書が処理される | ビジネス上の期待に対応するE-Invoiceのみを処理 | E-Invoiceの内容は、バイヤーの社内買掛金/未払金マスター・データに対して検証できます。大きな差異がある場合は、承認ワークフローをさらに処理および実行しません。アプリケーションは、サプライヤのマスターデータを変更するためのチェックと手順を行います。 |  |  |  |
| 102と | 8-材料検証および処理 | xと | xと | xと | E-Invoiceの処理責任者を特定できない | 説明責任者は、特定可能である必要がある | 電子請求書の受領、監査および処理に関連するすべての内部統制記録を保持する必要があります。 |  |  |  |
| 103と | すべて(仕入先および購買担当サイド) |  |  |  |  | | | | |  |

11/12個

Annex1\_Compliance\_Guidelines\_Matrix\_19102009.xlsと

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Bと | シーディーイー | | | Hと | Iと | Jと | Kと | Lと | Mと |
| 1と | ワオ  プロセスステップ  (順序を調整できる) | ビジネス実装クラスB-D | | | なぜ(リスク) | 何(要件) | どのように(制御) | 参考例。 注。ここに挙げた例は、網羅的なものではなく、想定される対策の種類を示すためにのみ提供されている。 | 追加ガイダンス[「コンプライアンス・ガイドラインの解説書」 参照] | 実装の適用性[自己評価に使用] |
| 104と | E-取引先オフボード | xと | xと | xと | 取引および格納されたE-Invoicesは、十分な管理なしで紛失、重複または処理されます。必要なシステムまたはプロセスの監査機能が法的に利用できなくなる;監査証跡および説明文書は、もはや管轄当局からアクセスできない。 | 貿易相手国は、税務管理と監査可能性の観点から、関係の適切な終了を確保しなければならない。完全性と整合性は、ストレージ期間中も検証可能である必要がある | 取引先は、E-Invoiceのライフサイクルにおいて、あるトランザクションまたはストレージ・サービス/環境から別のトランザクションまたはストレージ・サービス/環境に移動する必要がある場合、適切な移行のための最小限の手順について合意する必要があります。同様に、取引先は、電子請求書/請求書プロセスが移動されたかどうかに関係なく、適用法に基づく電子請求書の強制保管期間の残りの期間、過去の取引および保管プロセスの重要な監査証跡および文書証拠が保持されるようにする必要があります。 | これらの問題は、電子請求プロセスを開始する前に締結される、取引先間および各取引先とそのサービス提供者との間の明示的な合意の中で規制されるべきである。 |  |  |
| 105と | E-取引先オフボード |  |  | xと | バイヤーは提示された「原本 」 E-請求書にアクセスできません。 | 契約終了のために物理的接続が使用できない場合でも、E-Invoicesは保存期間全体にわたって使用可能である必要があります。これには、信頼性と整合性の特性が含まれる必要があります。 | 契約で合意する必要があります。Commentary reportのセクション5、図1および図2の 「監査可能性Cのアーカイブ」 の手順も参照してください。 |  |  |  |
| 106と |  | | | | | | | | | |
| 107と |  |  | | |  |  |  |  |  |  |
| 108と |  |  | | |  |  |  |  |  |  |
| 109と |  |  | | |  |  |  |  |  |  |
| 110と |  |  | | |  |  |  |  |  |  |
| 111と |  |  | | |  |  |  |  |  |  |
| 112と |  |  | | |  |  |  |  |  |  |
| 113と |  |  | | |  |  |  |  |  |  |
| 114と |  |  | | |  |  |  |  |  |  |
| 115と |  |  | | |  |  |  |  |  |  |
| 116と |  |  | | |  |  |  |  |  |  |
| 117と |  |  | | |  |  |  |  |  |  |
| 118と |  |  | | |  |  |  |  |  |  |
| 119と |  |  | | |  |  |  |  |  |  |
| 120と |  |  | | |  |  |  |  |  |  |
| 121と |  |  | | |  |  |  |  |  |  |
| 122と |  |  | | |  |  |  |  |  |  |
| 123と |  |  | | |  |  |  |  |  |  |
| 124と |  |  | | |  |  |  |  |  |  |
| 125と |  |  | | |  |  |  |  |  |  |
| 126と |  |  | | |  |  |  |  |  |  |
| 127と |  |  | | |  |  |  |  |  |  |
| 128と |  |  | | |  |  |  |  |  |  |
| 129と |  |  | | |  |  |  |  |  |  |
| 130と |  |  | | |  |  |  |  |  |  |
| 131と |  |  | | |  |  |  |  |  |  |
| 132と |  |  | | |  |  |  |  |  |  |
| 133と |  |  | | |  |  |  |  |  |  |
| 134と |  |  | | |  |  |  |  |  |  |
| 135と |  |  | | |  |  |  |  |  |  |

12/12個