（№　L-2017-015）

CI-NET LiteS実装規約改善要求書（CHANGE REQUEST）

|  |  |
| --- | --- |
| 発信者記入欄 | 事務局記入欄 |
| 発　信　日　　2018年　2月　9日 | 受　信　日　　2018年　2月　9日 |
| 会 社 名　LiteS規約WG | 改訂対象： |
| 企業識別コード |  |  |  |  |  |  | Ver. | 2 | . | １ | ad. | 8 |
| 部 署 名  | 事務局処理記入欄 |
| 担当者名 |
|  TEL:連 絡 先 FAX: |
| 件　　名　新暗号アルゴリズムへの移行に伴うセキュリティ方式および電子証明書プロファイルの改訂 |
| ◎ 改善要求内容（問題点、改善案、理由について詳しくお書き下さい）【要求内容】内閣官房情報セキュリティセンター(NISC)が、2008年4月22日に「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」を公開したことを受けて、2014年度9月下旬以降に政府機関などで使用する電子証明書とその利用システムが新暗号方式へ更新された。これにより、暗号アルゴリズムSHA-1およびRSA1024に対応した製品やサービスが廃止される懸念から、CI-NETにおいても新暗号アルゴリズムSHA-2およびRSA2048への対応が進められている。これに伴い、電子証明書に格納する属性に変更が生じたため、以下のとおり改訂することを要求する。(1) 改訂対象* セキュリティ方式について、「暗号アルゴリズムSHA-1およびRSA1024」のみの記載を「暗号アルゴリズムSHA-2およびRSA2048」との併用とする記載に改訂する。
* 電子証明書プロフィールの記載内容を改訂する。

(2) 改訂内容以下のとおり変更する。なお、本CRの一部に、CR管理No. L-2016-002にて承認済みの改訂内容を含んでいる。＜CI-NET LiteS実装規約Ver.2.1 ad.7 P. 2＞

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 変更前 | ＜本文＞　表 1 CI-NET LiteS実装規約の概要

| 規約 | 内容 |
| --- | --- |
| Ａ.情報伝達規約 | 通信方式 | ■通信方式は、送信時においてSMTP、受信時においてPOP3プロトコル■電子メールのサブジェクトは、BPID機関名（=CINT）と情報区分コードで構成【例】CINT0301：購買見積依頼　CINT0302：購買見積回答 |
| セキュリティ方式 | ■セキュリティ方式はS/MIMEに準拠* ダイジェスト・アルゴリズムはSHA-1
* ダイジェスト暗号アルゴリズムはRSA、鍵長は1024 bit
* 鍵暗号アルゴリズムはRSA、鍵長は1024 bit
* コンテント暗号アルゴリズムはDES、鍵長は56 bit

・証明書はX.509 Version3、データの取り出し、取り込み形式はPKCS#7 |
| 技術データ | ■圧縮・解凍方式・Windows上の自己解凍方式 |

 |
| 変更後 | ＜本文＞　表 1 CI-NET LiteS実装規約の概要

| 規約 | 内容 |
| --- | --- |
| Ａ.情報伝達規約 | 通信方式 | ■情報伝達手段は、電子メール方式またはebMS方式■電子メール方式における通信~~方式~~プロトコルは、送信時においてSMTP、受信時においてPOP3~~プロトコル~~■ebMS 処理方式における通信プロトコルは、ebXML Message Service v2.0 およびebXML CPPAv2.0■電子メール方式における電子メールのサブジェクトは、BPID機関名（=CINT）と情報区分コードで構成【例】CINT0301：購買見積依頼　CINT0302：購買見積回答 |
| セキュリティ方式 | ■セキュリティ方式はS/MIMEに準拠* ダイジェスト・アルゴリズムはSHA-1またはSHA256
* ダイジェスト暗号アルゴリズムはRSA、鍵長は1024 bitまたは2048 bit
* 鍵暗号アルゴリズムはRSA、鍵長は1024 bitまたは2048 bit
* コンテント暗号アルゴリズムはDES、鍵長は56 bit
* 証明書はX.509 Version3、データの取り出し、取り込み形式はPKCS#7
 |
| 技術データ | ■圧縮・解凍方式・Windows上の自己解凍方式・ZIP方式による圧縮 |

 |

＜CI-NET LiteS実装規約Ver.2.1 ad.7 P. 27、P.45＞

|  |  |
| --- | --- |
| 変更前 | ＜本文＞　4. 暗号化アルゴリズムCI-NET LiteSで使用する暗号化アルゴリズムは以下の通り。(a) データ部のメッセージ・ダイジェストを作成するダイジェスト・アルゴリズムはSHA-1またはSHA-2。(b) ダイジェスト暗号化アルゴリズムはRSA。鍵長は1024 bitまたは2048bit。(c) 共通鍵暗号化アルゴリズムはRSA。鍵長は1024 bitまたは2048bit。(d) コンテント暗号化アルゴリズムはシングルKey DES。鍵長56 bit。エンコーディング方式CBC。 |
| 変更後 | ＜本文＞　4. 暗号化アルゴリズムCI-NET LiteSで使用する暗号化アルゴリズムは以下の通り。(a) データ部のメッセージ・ダイジェストを作成するダイジェスト・アルゴリズムはSHA-1またはSHA256。(b) ダイジェスト暗号化アルゴリズムはRSA。鍵長は1024 bitまたは2048bit。(c) 共通鍵暗号化アルゴリズムはRSA。鍵長は1024 bitまたは2048bit。(d) コンテント暗号化アルゴリズムはシングルKey DES。鍵長56 bit。エンコーディング方式CBC。 |

＜CI-NET LiteS実装規約Ver.2.1 ad.7 P. 28、P.46＞

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 変更前 | ＜本文＞　5. 電子証明書(a) CI-NET LiteSで使用する電子証明書はISO/IEC規定のX.509 Version3フォーマットを使用する。(b) 電子証明書プロフィールは以下の通り。表A- 3電子証明書プロフィール

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | フィールド名 | 設定者 | 区分 | 設定値 |
| 証明書基本部 |
|  | バージョン（version） | 認証局 | 必須 | V3 |
|  | シリアル番号（serialNumber） | 認証局 | 必須 | 正の整数 |
|  | 署名（signature） | 認証局 | 必須 | sha1 with RSA Encryption(1.2.840.113549.1.1.5) |
|  | 発行者（issuer） | 認証局 | 必須 | CN=発行者 |
|  | 有効期間（validity） | 認証局 | 必須 | 開始時刻（例：年月日時分秒）終了時刻（例：年月日時分秒） |
|  | 所有者 | 認証局 | 必須 | C=国名（例：JP） |
|  | （subject） | 登録局 | 必須 | O=組織名（例：CI-NET） |
|  |  | ユーザ/登録局 | 必須 | OU=「CompanyCode-」とユーザの標準企業コード（12桁） |
|  |  | 登録局 | 必須 | CN=ユーザ名または識別コード |
|  |  | 登録局 | 必須 | E=ユーザの電子メールアドレス |
|  | 所有者公開鍵（subjectPublicKeyInfo） | 顧客/登録局 | 必須 | ＲＳＡ公開鍵（例：1024ビット） |
| 証明書標準拡張部 |
|  | 認証局鍵識別（authorityKeyIdentifier） | 認証局 | 任意 | keyID=（例：発行者の公開鍵のSHA-1ハッシュ（160bit））authorityCert=発行者のDN（識別名）とシリアル番号 |
|  | 所有者鍵識別（subjectKeyIdentifier） | 認証局 | 任意 | （例：公開鍵のSHA-1） |
|  | 鍵種別（keyUsage） | 認証局 | 必須 | digitalSignature, keyEncipherment (0xA0) |
|  | 拡張鍵種別（extendedKeyUsages） | 認証局 | 任意 | － |
|  | 証明書ポリシー（certificatePolicies） | 認証局 | 任意 | 認証局のOID |
|  | 所有者別名（subjectAltName） | 顧客/登録局 | 任意 | rfc822name=ユーザの電子メールアドレス |
|  | 基本制約（basicConstraints） | 認証局 | 任意 | cA=FALSEpathLenConstraint=フィールドなし |
|  | ＣＲＬ分配点（cRLDistributionPoints） | 認証局 | 任意 | （例：URL等） |
|  | netscape-cert-type | 認証局 | 任意 | － |

 |
| 変更後 | ＜本文＞　5. 電子証明書(a) CI-NET LiteSで使用する電子証明書はISO/IEC規定のX.509 Version3フォーマットを使用する。(b) 電子証明書プロフィールは以下の通り。表A- 3電子証明書プロフィール注1. 8、9、11行：OU=CPN-(ユーザ企業名)、OU=CMN-(法人番号・枝番相当)、OU=TID-(端末ID）は、使用しないものでも 接頭語は「あり」とし、パラメータはなし(Null)とする。 OUの記載例8行ユーザ企業名:CPN-abc(全部で60桁)xyz　(ユーザ企業名:abc(全部で60桁)xyz)9行法人番号:CMN-1234567890123+123456　(法人番号:1234567890123、枝番:123456)11行ユーザ標準企業コード:CompanyCode-123456789012　(ユーザ標準企業コード123456789012)
2. 11行：端末IDは機種により一律な設定にできないため、接頭語は「MAC-、IMEI-、UDID」等の検討が必要である。
3. 12行：CI-NET仕様では、CI-NET電子証明書は、職務権限者を証明する。ただし、CNに個人名を記載することも許容する。個人名記載の場合、異動、退職などにより、都度発行が発生し請負契約や物品調達等の円滑な運用に適しない。また、建設産業の調達業務では、業務フローの各場面で職務権限者が異なり、業務は調達、施工、支払と遷移するが、ひとつの案件はひとつの電子証明書で処理を行うことが一般的である等の理由により、企業内で定めた職務権限者(SHOKUMU-KENGENSHA)をCNに記載し、電子証明書はそれを証明する。
4. 17行：利用用途を指定する。 digitalSignature 電子署名利用nonRepudiation 否認防止keyEncipherment 重要情報送信(例えば、共通鍵、パスワード等短い情報に限る)
 |

 |

|  |
| --- |
| ◎ 改善要求内容（問題点、改善案、理由について詳しくお書き下さい）【要求の理由】内閣官房情報セキュリティセンター(NISC)が、2008年4月22日に「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」を公開したことを受けて、2014年度9月下旬以降に政府機関などで使用する電子証明書とその利用システムが新暗号方式へ更新された。これにより、暗号アルゴリズムSHA-1およびRSA1024に対応した製品やサービスが廃止される懸念から、CI-NETにおいても新暗号アルゴリズムSHA-2およびRSA2048への対応が進められている。これに伴い、電子証明書に格納する属性に変更が生じたため、改訂を行う必要が生じた。【既存ユーザ等への影響】すべてのユーザが新暗号アルゴリズムに移行する必要があるため、すべてのユーザに対して、電子証明書の更新時に文書で通知する等、十分に周知を図る必要がある。 |

（L-2017-015）

CI-NET標準ビジネスプロトコルおよびCI-NET LiteS実装規約に係る

改訂チェックリスト

CI-NET標準ビジネスプロトコルおよびCI-NET LiteS実装規約に係る改訂に関して、下記に示す項目についてチェック（○、×）を行い、問題がある場合にはその内容および改善の方向等について「指摘事項等」の欄に記載するものとする。

|  |  |
| --- | --- |
| 審議･検討日 | 2018年2月9日 |
| 審議機関 | （委員会／WG名等を記載）標準委員会 |

|  |  |
| --- | --- |
| 改訂内容 | （提案者、対象メッセージ、新規項目名称・摘要等を記載）新暗号アルゴリズムへの移行に伴うセキュリティ方式および電子証明書プロファイルの改訂 |

| チェック項目 | ﾁｪｯｸ | 指摘事項等 |
| --- | --- | --- |
| 1.既存ユーザへの影響度合い | ①実稼動しているシステムの改修度合 | △ | 実稼動しているシステムの改修が必要である。 |
| ②業務の見直し、変更への影響度合 | ○ | 業務の見直し、変更は生じない。 |
| ③いずれのユーザの負担が大きいか | △ | システムベンダーに負担を生じる。 |
| ④及ぼす影響の具体的な範囲や内容が見えているか否か | ○ | 及ぼす影響の範囲は明確化されている。 |
| ⑤即時の対応が可能か否か | △ | 新暗号アルゴリズムへの移行が段階的に進められていることと併せての対応となる。 |
| ⑥立場の違いなく対応が可能か否か | ○ | 立場の違いによる対応の差異は特にない。 |
| 2.各社固有の業務要件か | ①他ユーザの賛同の有無 | ／ |  |
| ②業務の変更による対応可否の検討有無 | ／ |  |
| 3.印刷要件か | ①各社の帳票出力に依存する項目が否か | ／ |  |
| 4.二重要件か | ①他項目での類似機能がないか | ／ |  |
| 5.定義の明確化 | ①類似項目との違いは明確か | ／ |  |
| ②規約全体を通して定義を明確にしているか | ／ |  |
| 6.改訂の緊急度 | ①即時対応の必要性の有無 | △ | 新暗号アルゴリズムへの移行と併せて対応される必要がある。 |

|  |  |
| --- | --- |
| 審議結果 | (単に承認／非承認だけでなく、そのような結果となった理由等も記載)新暗号アルゴリズムSHA-2およびRSA2048への移行に関するCRは平成28年度までに承認されており、これに対応した記述改訂となる本CRは承認された。また、技術データの圧縮・解凍方式にZIP形式を追加することについても、CRは平成28年度までに承認されており、これに対応した記述改訂となる本CRは承認された。 |
| 今後の対応 | (上部審議機関への申し送り事項／差戻しの場合の再審議ポイントの提示など)新暗号アルゴリズムSHA-2およびRSA2048への移行は既に2017年4月より開始されており、早急にCI-NET LiteS実装規約を改訂すべきである。なお、新暗号アルゴリズムへの移行は2020年3月に完了見込みであることから、2020年4月以降に旧暗号アルゴリズムSHA-1およびRSA1024に関する記述をCI-NET LiteS実装規約から削除する改訂を行う必要がある。また、技術データの圧縮・解凍方式をZIP形式とするサービスの提供を求めるユーザの声が強いことから、サービス提供開始に先駆けて、早急にCI-NET LiteS実装規約を改訂すべきである。 |

|  |
| --- |
| 【チェック欄の凡例】○：問題なし△：やや問題あり／指摘事項に対する配慮があるとよい／：対象外／該当しない×：問題あり／指摘事項への対応が必要 |