参考資料１

既存のセキュリティ要求基準について

ISO/IEC 27017:2015
（クラウドサービスのための情報セキュリティ管理策の実践の規範）

参考情報Ⅰ ： ISO/IEC 27017:2015

項番/管理策	昨年度検討との関連
5．情報セキュリティのための方針群（Information security policies)	
5.1.1 情報セキュリティのための方針群(Policies for information security)	–
6．情報セキュリティのための組織(Organaization of information security)	
6.1.1 情報セキュリティの役割及び責任 (Information security roles and responsibilities)	–
6.1.3 関係当局との連絡(Contact with authorities)	–
7．人的資源のセキュリティ(Human resource security)	
7.2.2 情報セキュリティの意識向上、教育及び訓練 (Information security awareness, education and training)	–
8．資産の管理（Asset management)	
8.1.1 資産目録(Inventory of assets)	–
8.2.2 情報のラベル付け(Labelling of information)	–

※ISO/IEC 27002を参照している項目以外を抜粋

参考情報Ⅰ ： ISO/IEC 27017:2015

項番/管理策	昨年度検討との関連
９．アクセス制御（Access control）	
9.1.2 ネットワーク及びネットワークサービスへのアクセス (Access to networks and network services)	–
9.2.1 利用者登録及び登録削除(User registration and deregistration)	機能②
9.2.2 利用者アクセスの提供(User access provisioning)	機能①
9.2.3 特権的アクセス権の管理(Management of privileged access right)	–
9.2.4 利用者の秘密認証情報の管理 (management of secret authentication information of users)	機能②
9.4.1 情報へのアクセス制限(Information access restriction)	機能①
9.4.4 特権的なユーティリティプログラムの使用 (Use of privileged utility programs)	–
１０．暗号（Cryptographic controls）	
10.1.1 暗号による管理策の利用方針 (Policy on the use of cryptographic controls)	機能③
10.1.2 鍵管理(Key management)	機能⑤、⑥
１１．物理的及び環境的セキュリティ（Physical and environmental security）	
11.2.7 装置のセキュリティを保った処分又は再利用 (Secure disposal or reuse of equipment)	–

※ISO/IEC 27002を参照している項目以外を抜粋

参考情報Ⅰ ： ISO/IEC 27017:2015

項番/管理策	昨年度検討との関連
１２．運用のセキュリティ（Operations security)	
12.1.2 変更管理(Change management)	–
12.1.3 容量・能力の管理(Capacity management)	–
12.3.1 情報のバックアップ(Information backup)	機能⑥
12.4.1 イベントログ取得(Event logging)	機能④
12.4.3 実務管理者及び運用担当者の作業ログ (Administrator and operator logs)	–
12.4.4 クロックの同期(Clock synchronization)	–
12.6.1 技術的ぜい弱性の管理(Management of technical vulnerabilities)	–
１３．通信のセキュリティ（Communications security)	
13.1.3 ネットワークの分離(Segregation in networks)	–
１４．システムの取得、開発及び保守（System acquisition, development and maintenance)	
14.1.1 情報セキュリティ要求事項の分析及び仕様化 (Information security requirements analysis and specification)	–
14.2.1 セキュリティに配慮した開発のための方針(Secure development policy)	–

※ISO/IEC 27002を参照している項目以外を抜粋

参考情報Ⅰ ： ISO/IEC 27017:2015

項番/管理策	昨年度検討との関連
１５．供給者関係（Supplier relationships)	
15.1.1 供給者関係のための情報セキュリティの方針 (Information security policy for supplier relationships)	–
15.1.2 供給者との合意におけるセキュリティの取扱い (Addressing security within supplier agreements)	–
15.1.3 ICTサプライチェーン (Information and communication technology supply chain)	–
１６．情報セキュリティインシデント管理 （Information security incident management)	
16.1.1 責任及び手順(Responsibilities and procedures)	–
16.1.2 情報セキュリティ事象の報告(Reporting information security events)	–
16.1.7 証拠の収集(Collection of evidence)	–
１７．事業継続マネジメントにおける情報セキュリティの側面	
１８．順守（Compliance)	
18.1.1 適用法令及び契約上の要求事項の特定 (Identification of applicable legislation and contractual requirements)	–
18.1.2 知的財産権(Intellectual property rights)	–
18.1.3 記録の保護(Protection of records)	–
18.1.5 暗号化機能に対する規制(Regulation of cryptographic controls)	–
18.2.1 情報セキュリティの独立したレビュー (Independent review of information security)	–

参考情報Ⅱ：検討内容（昨年度の調査結果を詳細化：書き下しイメージ）

- 10.暗号（Cryptographic controls)
  - 10.1.1　暗号による管理策の利用方針
    (Policy on the use of cryptographic controls)
    - 電子政府推奨暗号リストに記載された公開鍵暗号による署名方式を用いることが求められ、安全な署名結果を得るために重要である（レベル3相当）。
    - さらに安全性を求める場合（レベル4）は、電子署名用証明書の用途を電子署名のみに限定することが求められる。
    - （昨年度の検討では、電子署名・認証ガイドラインを参照し書き出した）
  - 10.1.2　鍵管理(Key management)
    - 署名鍵管理機能は、署名鍵IDと署名鍵を管理する。
    - 署名鍵管理機能は、署名鍵IDに対応した署名鍵を格納しているDB-2を制御する。
    - 署名鍵等の管理には、登録、更新/再発行、失効を含む。
    - 利用者の署名鍵IDの関連付け情報を格納しているDB-2は保護する必要があり、アクセスを限定する必要がある。
    - DB-2へのアクセスは必ず署名鍵管理機能を介して行われる必要があり、DB-2の登録者及び管理者に限定される。

参考情報Ⅱ：検討内容（昨年度の調査結果を詳細化：書き下しイメージ）

- 12.運用のセキュリティ（Operations security)
  - 12.3.1　情報のバックアップ(Information backup)
    - 署名鍵は署名者以外に利用できない（活性化できない）ように保管する必要あり、署名者以外に知り得ない状態でバックアップ保管することが求められることに注意する必要がある。
    - （昨年度の検討では、欧州のCEN/TS 419 241 を参照し書き出した）
  - 12.4.1　イベントログ取得(Event logging)
    - サーバ署名で正しく署名をしたことのログを残すことは安全性の観点から重要であるため、少なくとも署名生成に関する一連の処理のすべてをログとして保存することが必須とした。
    - なお、ログの対象や保管期間及び完全性や改ざん検知等については利用形態に基づき別途検討する必要がある。
    - （参照した欧州のCEN/TS 419 241の内容）
    - レベル1では、署名生成に関する一連の処理のすべてをログとして保存することが規定されている。
    - レベル2ではレベル1に追加して、署名鍵へアクセスするすべての動作をログとして保存することが規定されている。

参考情報Ⅲ：検討内容

（１）現行の電子署名法に関する検討項目

（２）利活用モデルと第三者による安全性の確認に関する検討項目

（３）リモート署名事業者に求められる業務要件に関する検討項目

（４）鍵ペア生成や設置及び保管状態に関する検討項目

（５）鍵のバックアップ及びログ機能に関する検討項目

（６）利用者情報に関する検討項目

（７）利用者に求められる制約や要件に関する検討項目

（８）その他の必要と考えられる検討項目

参考情報Ⅲ： 検討内容－詳細（１）～（２）

（１）現行の電子署名法に関する検討項目

仕様書上の要求(検討) 事項

①電子署名制度で想定されている法令体系

③現行の電子署名制度で定められる電子署名とリモート署名との差異

昨年度の検討結果

１９．電子署名法との関連	5.10.4

（２）利活用モデルと第三者による安全性の確認に関する検討項目

仕様書上の要求(検討) 事項

②リモート署名の認定制度に対するニーズ（金融、医療、建築等の分野における国の認定を受けたリモート署名の利活用モデルを含む。）

⑫第三者によるリモート署名の安全性の確認方法

別途アンケートやヒアリング調査を実施予定（小川）

昨年度の検討結果

1．	リモート署名のプレイヤ・役割の整理	5.5
2．	リモート署名提供者の要件・保証レベル	5.6.1
3．	署名の利用用途に応じたレベルの検討	5.6.2

参考情報Ⅲ ：検討内容－詳細（３）～（４）

（３）リモート署名事業者に求められる業務要件に関する検討項目

仕様書上の要求(検討) 事項	昨年度の検討結果
④リモート署名を実施する事業者に求められる設備・人員等の業務要件	４．　リモート署名の構成・設置環境の検討　5.6.3

（４）鍵ペア生成や設置及び保管状態に関する検討項目

仕様書上の要求(検討) 事項	昨年度の検討結果
⑤ＨＳＭによる鍵ペアの生成・保管を行う場合に求められる機能要件 ⑥ソフトウェアによる鍵ペアの生成・保管を行う場合に求められる機能要件及びＨＳＭによる場合との差異 ⑪鍵ペアのインポートを実施する場合に、複数の事業者又は利用者を経由してなお安全性を確保することができる具体的要件	１１．利用者の署名鍵の設置　5.8.2 １２．利用者の署名鍵の保護対策　5.8.3

参考情報Ⅲ ：検討内容－詳細（５）～（６）

（５）鍵のバックアップ及びログ機能に関する検討項目

仕様書上の要求(検討) 事項	昨年度の検討結果	
⑦署名鍵のバックアップ方法	７． 署名鍵のバックアップ機能の有無	5.7.3
⑧署名生成・管理に係るデータのログの保管期間・方法等	８． 署名生成ログ機能の有無	5.7.4

（６）利用者情報に関する検討項目

仕様書上の要求(検討) 事項	昨年度の検討結果	
⑨利用者情報の管理及び利用者の正確な認証方法	１０．利用者登録方法	5.8.1
	１４．利用者認証方法	5.9.2
	１５．利用者情報と署名鍵情報の保護対策	5.9.3

参考情報Ⅲ ：検討内容－詳細（７）～（８）

（７）利用者に求められる制約や要件に関する検討項目

仕様書上の要求(検討) 事項

⑩リモート署名利用者に求められる制約や要件

昨年度の検討結果

５． 署名機能要件	5.7.1
１３．署名指示の要件	5.9.1

（８）その他の必要と考えられる検討項目

仕様書上の要求(検討) 事項

⑬その他本調査研究の過程で、具体的な安全基準等を検討するに当たり、客観的に、さらなる調査研究が不可欠と本年度報告・検討会で判断された事項

昨年度の検討結果

１６．利用者環境での分散署名処理	5.10.1
１７．利用者による署名対象データの確認	5.10.2
１８．長期署名の適用	5.10.3

９． 署名付きデータの送信機能の有無	5.7.5
６． 署名検証機能の有無	5.7.2

a）必要に応じて検討
が求められる検討項目

b）リモート署名の最低限必要と考えられる
機能ではなかった項目を再度確認？

関連情報

- METI/経済産業省　電子署名法研究会
  http://www.meti.go.jp/committee/kenkyukai/mono_info_service.html#denshishomeihou

- 平成２７年度サイバーセキュリティ経済基盤構築事業
  （電子署名・認証業務利用促進事業（電子署名及び認証業務に関する調査研究等））調査報告書
  http://www.meti.go.jp/committee/kenkyukai/shoujo/denshishomeihou/pdf/h27_004_01_00.pdf