検討番号（4章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
A.01	FR4.1	CKMS設計は、実行するために設計した設定可能なオプションとサブポリシーを含むCKMSセキュリティポリシーを明記しなければならない。	4.3節	済・対象外	
A.02	FR4.2	CKMS設計は、CKMSセキュリティポリシーがCKMSによってどのように実行されるのか（例えば、ポリシーが要求する保護を提供するために使用されるメカニズム）を明記しなければならない。	4.3節	済・対象外	
A.03	FR4.4	CKMS設計は、CKMSセキュリティポリシーをサポートする他の関連するセキュリティポリシーを明記しなければならない。	4.4節	済・対象外	
A.04	FR4.5	CKMS設計は、CKMS設計によってサポートされるポリシーと、その設計によってどのようにサポートされるのかの要約を明記しなければならない。	4.5節	済・対象外	
A.05	FR4.3	CKMS設計は、CKMSセキュリティポリシーのあらゆる自動化部分についてどのように曖昧さのない表形式又は形式言語（例えばXML、ASN.1）で表現されているのかを明記しなければならない。CKMSの自動化されたセキュリティシステム（例えばtable driven又はsyntax-directed software mechanisms）がそれらを実行できるようにするためである。	4.3節	済・対象外	
A.06	FR4.6	CKMS設計は、個人の説明責任（personal accountability）がCKMSでサポートされるかどうか、及びどのようにサポートされるかを明記しなければならない。	4.6節	済・対象外	
A.07	FR4.7	CKMS設計は、CKMSでサポートできる匿名性、連結不可能性（unlinkability）、及び観測不可能性（unobservability）に関するポリシーを明記しなければならない。	4.7節	済・対象外	
A.08	FR4.8	CKMS設計は、どのCKMSトランザクションが匿名性保護を提供している、又は提供可能であるのかを明記しなければならない。	4.7.1節	済・対象外	
A.09	FR4.9	CKMS設計は、匿名性の保証を提供する場合、CKMSトランザクションの匿名性保証をどのように達成するのかを明記しなければならない。	4.7.1節	済・対象外	
A.10	FR4.10	CKMS設計は、どのCKMSトランザクションが連結不可能性（unlinkability）保護を提供している、又は提供可能であるのかを明記しなければならない。	4.7.2節	済・対象外	
A.11	FR4.11	CKMS設計は、CKMSトランザクションの連結不可能性（unlinkability）をどのように達成するのかを明記しなければならない。	4.7.2節	済・対象外	
A.12	FR4.12	CKMS設計は、どのCKMSトランザクションが観測不可能性（unobservability）保護を提供している、又は提供可能であるのかを明記しなければならない。	4.7.3節	済・対象外	
A.13	FR4.13	CKMS設計は、CKMSトランザクションの観測不可能性（unobservability）をどのように達成するのかを明記しなければならない。	4.7.3節	済・対象外	
A.14	FR4.15	CKMS設計は、同等だが異なるセキュリティ保護を提供するとみなせる他のセキュリティドメインに属するエンティティ間での鍵情報（暗号鍵及びメタデータ）の交換を許可する設計仕様を明記しなければならない。	4.9.1節	済・対象外	
A.15	FR4.16	CKMS設計は、鍵情報（暗号鍵やメタデータ）を異なるセキュリティドメインに属するエンティティ間で共有するときに実施されるソース認証ポリシー（source authentication policy）とディスティネーション認証ポリシー（destination authentication policy）を明記しなければならない。	4.9.2節	済・対象外	

検討番号（4章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
A.16	FR4.17	CKMS設計は、鍵情報（暗号鍵やメタデータ）を異なるセキュリティドメインに属するエンティティ間で共有するときに実施される機密性と完全性のポリシーを明記しなければならない。	4.9.2節	済・対象外	
A.17	FR4.18	CKMS設計は、他のセキュリティドメインのエンティティと通信するときに要求される保証要件を明記しなければならない。	4.9.2節	済・対象外	
A.18	FR4.19	CKMS設計は、ドメイン間通信が許可される前に他のドメインのセキュリティポリシーのレビューと検証をサポートするかどうか、またどのようにサポートするのかを明記しなければならない。	4.9.3節	済・対象外	
A.19	FR4.20	CKMS設計は、弱いポリシーを持つセキュリティドメインのエンティティとの通信がもたらす潜在的なセキュリティに関する影響をどのように検知、防止、又はエンティティに警告するのかを明記しなければならない。	4.9.3節	済・対象外	
A.20	FR4.26	CKMS設計は、異なるドメインのセキュリティポリシー及び異なるアプリケーションをサポートするように、鍵情報（暗号鍵やメタデータ）の管理機能を設定することができるかどうか、及びどのように設定するのかを明記しなければならない。	4.9.7節	済・対象外	
A.21	FR4.27	CKMS設計は、異なるセキュリティドメイン間のエンティティ同士との通信に適応するために、再設定によるドメインのセキュリティポリシーの変更をサポートしているかどうか、及びどのようにサポートできるかを明記しなければならない。	4.9.7節	済・対象外	
A.22	FR4.21	CKMS設計は、マルチレベルのセキュリティドメインをサポートするかどうかを明記しなければならない。	4.9.5節	済・対象外	
A.23	FR4.22	CKMS設計は、サポートするセキュリティドメインのそれぞれのレベルを明記しなければならない。	4.9.5節	済・対象外	
A.24	FR4.23	マルチレベルのセキュリティドメインをサポートしている場合、CKMS設計は、それぞれのセキュリティレベルに属する鍵情報（暗号鍵及びメタデータ）の分離をどのように保持しているのかを明記しなければならない。	4.9.5節	済・対象外	
A.25	FR4.24	CKMS設計は、鍵情報（暗号鍵及びメタデータ）のアップグレード又はダウングレードをサポートするかどうか、及びどのようにサポートするのかを明記しなければならない。	4.9.6節	済・対象外	
A.26	FR4.25	CKMS設計は、アップグレード又はダウングレード機能をどのようにドメインオーソリティ（domain authority）に制限しているかを明記しなければならない。	4.9.6節	済・対象外	
A.27	FR5.1	CKMS設計は、CKMSに用いられているそれぞれの役割と責任、及びそれぞれの役割にどのようにエンティティが割り当てられるのかを明記しなければならない。	5章	済・対象外	
A.28	FR5.2	CKMS設計は、CKMSに用いられているそれぞれの役割を満たしているエンティティが使用できる鍵情報（暗号鍵及びメタデータ）の管理機能（6.4節を参照）を明記しなければならない。	5章	済・対象外	
A.29	FR5.3	CKMS設計は、どの役割が役割分離を必要とするのかを明記しなければならない。	5章	済・対象外	
A.30	FR5.4	CKMS設計は、役割分離を必要とする役割に対してその分離がどのように保持されるのかを明記しなければならない。	5章	済・対象外	

検討番号（4章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
A.31	FR5.5	CKMS設計は、セキュリティ違反が認可された役割を実行する個人（内部者）によるのか、認可された役割がない人（外部者）によるのかを特定するための全ての自動化された対策を明記しなければならない。	5章	済・対象外	
A.32	FR2.5	CKMS設計は、CKMSの全ての主要なデバイス（例えば、メーカ、モデル、バージョン）を明記しなければならない。	2.10節	済・対象外	
A.33	FR6.9	CKMS設計は、システムで使用される日時に要求される正確さと精度を明記しなければならない。	6.2.1節	済・対象外	
A.34	FR6.10	CKMS設計は、要求される正確さを達成するためにどの権威時刻ソース（authoritative time source）を使用するかを明記しなければならない。	6.2.1節	済・対象外	
A.35	FR6.11	CKMS設計は、要求される正確さを達成するためにどのように権威時刻ソース（authoritative time source）を使用するかを明記しなければならない。	6.2.1節	済・対象外	
A.36	FR6.12	CKMS設計は、どの日付、時刻、及び機能が信頼される第三者タイムスタンプ（trusted third-party time stamp）を要求するかを明記しなければならない。	6.2.1節	済・対象外	
A.37	FR3.1	CKMS設計は、それが機能する通信ネットワークに関しての目標を明記しなければならない。	3.1節	済・対象外	
A.38	FR3.2	CKMS設計は、それがサポートすることを意図しているアプリケーションを明記しなければならない。	3.1節	済・対象外	
A.39	FR3.3	CKMS 設計は、意図するユーザ数とそれらのユーザに課する責任を一覧にしなければならない。	3.1節	済・対象外	
A.40	FR3.14	CKMS設計は、CKMSのパフォーマンス特性を明記しなければならない。それには、実装された機能とトランザクションのタイプによる処理可能な平均及びピーク時の負荷と、その負荷がかかったときの機能とトランザクションのタイプごとの応答時間を含む。	3.5節	済・対象外	
A.41	FR3.15	CKMS設計は、増大する負荷要求に応じてシステムを拡張するために、サポートされ使うことができる技術を明記しなければならない。	3.5節	済・対象外	
A.42	FR3.16	CKMS設計は、増大する負荷要求に対応してCKMSを拡張できる範囲を明記しなければならない。これは、追加される負荷、負荷に対する応答時間、及びコストの観点で表現しなければならない。	3.5節	済・対象外	
A.43	FR7.1	CKMS設計は、デバイスのインタフェース間の相互運用性の要求事項がどのように満たされるかを明記しなければならない。	7章	済・対象外	
A.44	FR7.2	CKMS設計は、サポートすることを意図しているアプリケーションとの相互運用に必要な標準、プロトコル、インタフェース、サポートする処理（service）、コマンド、及びデータフォーマットを明記しなければならない。	7章	済・対象外	
A.45	FR7.3	CKMS設計は、相互運用性を意図している他のCKMSとの相互運用に必要な標準、プロトコル、インタフェース、サポートする処理（service）、コマンド、及びデータフォーマットを明記しなければならない。	7章	済・対象外	
A.46	FR7.4	CKMS設計は、アプリケーションと他のCKMSに対する全ての外部インタフェースを明記しなければならない。	7章	済・対象外	
A.47	FR3.10	CKMS設計は、システムへの全てのユーザインタフェースを明記しなければならない。	3.4.1節	済・対象外	
A.48	FR3.12	CKMS設計は、ユーザインタフェースの設計原理を明記しなければならない。	3.4.2節	済・対象外	

検討番号（4章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
A.49	FR3.13	CKMS設計は、システムに設計された全てのヒューマンエラー防止又はフェールセーフ機能を明記しなければならない。	3.4.2節	済・対象外	
A.50	FR3.11	CKMS設計は、提案されたユーザインタフェースの使いやすさに関する、あらゆるユーザ受け入れテストの結果を明記しなければならない。	3.4.1節	済・対象外	
A.51	FR3.4	CKMS設計は、CKMSで使用される商用既製品を明記しなければならない。	3.2節	済・対象外	
A.52	FR3.5	CKMS設計は、商用既製品によってどのセキュリティ機能が実行されるのかを明記しなければならない。	3.2節	済・対象外	
A.53	FR3.6	CKMS設計は、CKMSの目標を満たすために商用既製品をどのように設定し拡張するかを明記しなければならない。	3.2節	済・対象外	
A.54	FR3.7	CKMS設計は、CKMSに使用される連邦政府標準（注：米国の場合）、国内標準、及び国際標準を明記しなければならない。	3.3節	済・対象外	
A.55	FR3.8	CKMSに使用されるそれぞれの標準に対して、CKMS設計は、どのCKMSデバイスが標準を実装しているのかを明記しなければならない。	3.3節	済・対象外	
A.56	FR3.9	CKMSに使用されるそれぞれの標準に対して、CKMS設計は、標準への適合がどのように検証されるか（例えば、第三者試験プログラムによって）を明記しなければならない。	3.3節	済・対象外	
A.57	FR4.14	CKMS設計は、CKMSが使用されることを意図する国名や地域名、及びCKMSが実行することを意図する際のあらゆる法的規制を明記しなければならない。	4.8節	済・対象外	
A.58	FR7.5	CKMS設計は、新規の、相互運用可能な、同等のデバイスへの移行のための全ての対策を明記しなければならない。	7章	済・対象外	
A.59	FR7.6	CKMS設計は、暗号アルゴリズムのアップグレード又は置き換えのために提供されるあらゆる対策を明記しなければならない。	7章	済・対象外	
A.60	FR7.7	CKMS設計は、暗号アルゴリズムの移行期間中に、どのように相互運用性をサポートするかを明記しなければならない。	7章	済・対象外	
A.61	FR7.8	CKMS設計は、暗号アルゴリズムと鍵長の使用をネゴシエーションするプロトコルを明記しなければならない。	7章	済・対象外	
A.62	FR12.1	CKMS設計は、システムに実装されたそれぞれの暗号アルゴリズムの想定されるセキュリティライフタイムを明記しなければならない。	12章	済・対象外	
A.63	FR12.2	CKMS設計は、CKMSの運用に悪影響を与えることなしに、暗号アルゴリズムのどの副関数（例えば、HMACの副関数として使うハッシュ関数）が、類似だが暗号学的に改良されている副関数にアップグレード又は置き換えを行うことができるかを明記しなければならない。	12章	済・対象外	
A.64	FR12.3	CKMS設計は、どの鍵確立プロトコルがシステムによって実装されているかを明記しなければならない。	12章	済・対象外	
A.65	FR12.4	CKMS設計は、システムに実装されているそれぞれの鍵確立プロトコルの想定されるセキュリティライフタイムを、採用されている暗号アルゴリズムの想定されるセキュリティライフタイムの観点から、明記しなければならない。	12章	済・対象外	
A.66	FR12.5	CKMS設計は、CKMSデバイスへの外部からのアクセスが許容されている範囲を明記しなければならない。	12章	済・対象外	
A.67	FR12.6	CKMS設計は、CKMSデバイスへの全ての許可された外部アクセスがどのようにコントロールされるかを明記しなければならない。	12章	済・対象外	

検討番号（4章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
A.68	FR12.7	CKMS設計は、CKMSの暗号アルゴリズムに対する量子コンピュータによる攻撃のような、新しい技術の発展の影響に抵抗又は軽減するために採用している機能を明記しなければならない。	12章	済・対象外	
A.69	FR12.8	CKMS設計は、CKMSの暗号に対する量子コンピュータによる攻撃の、現在知られている影響を明記しなければならない。	12章	済・対象外	

検討番号（5章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
B.01	FR2.4	CKMS設計は、以下を含むCKMSシステムの高レベルの概要を明記しなければならない： a) 利用するそれぞれの鍵タイプ b) 鍵が生成される場所と手段 c) それぞれの鍵タイプとの信頼関係で使用されるメタデータ要素（7.1節表 7 2参照） d) 鍵情報（暗号鍵やメタデータ）が存在しているそれぞれのエンティティのストレージにおける、鍵情報（暗号鍵やメタデータ）の保護方法 e) 配送時の鍵情報（暗号鍵やメタデータ）の保護方法 f) 鍵情報（暗号鍵やメタデータ）が配送され得る先となるエンティティの種類（例えば、ユーザ、ユーザデバイス、ネットワークデバイス）	2.5節	済 ・ 対象外	
B.02	FR6.15	CKMS設計は、CKMSの鍵が取り得る全ての状態を明記しなければならない。	6.3節	済 ・ 対象外	
B.03	FR6.16	CKMS設計は、全てのCKMS鍵状態間の遷移、及び遷移を起こすことに関係するデータ（入力と出力）を明記しなければならない。	6.3節	済 ・ 対象外	
B.04	FR6.17	CKMS設計は、実装されサポートされる鍵情報（暗号鍵及びメタデータ）の管理機能を明記しなければならない。	6.4節	済 ・ 対象外	
B.05	FR6.18	CKMS設計は、CKMSに実装されるそれぞれの鍵情報（暗号鍵及びメタデータ）の管理機能のパラメタに適用される完全性、機密性、及びソース認証（source-authentication）の処理（service）を特定しなければならない。	6.4節	済 ・ 対象外	
B.06	FR6.22	CKMS 設計は、それぞれの鍵タイプがどのように活性化されるか、及び鍵が活性化される状況を明記しなければならない。	6.4.3節	済 ・ 対象外	
B.07	FR6.23	それぞれの鍵タイプに対して、CKMS設計は、鍵活性化の通知の要求事項を明記しなければならない。それには、どの当事者に通知されるか、どのように通知されるか、どのセキュリティ処理（services）が通知に適用されるか、及び通知の期間が含まれる。	6.4.3節	済 ・ 対象外	
B.08	FR6.69	CKMS設計は、サポートされている全ての暗号機能、及びそれらの暗号機能がCKMSのどこで実行されるか（例えば、CA、ホスト、又はエンドユーザシステム）を明記しなければならない。	6.4.27節	済 ・ 対象外	
B.09	FR6.24	CKMS設計は、各鍵タイプに対して、鍵の非活性化がどのように決定されるのか（例えば、暗号鍵有効期間（cryptoperiod）による、使用回数による、又はデータ量による）を明記しなければならない。	6.4.4節	済 ・ 対象外	
B.10	FR6.25	CKMS設計は、それぞれの鍵タイプがどのように非活性化されるか（例えば、非活性化日時、使用回数、又は保護されたデータの量に基づいて、手動で行われるのか自動で行われるのか）を明記しなければならない。	6.4.4節	済 ・ 対象外	
B.11	FR6.26	CKMS設計は、それぞれの鍵タイプの非活性化日時がどのように変更できるかを明記しなければならない。	6.4.4節	済 ・ 対象外	
B.12	FR6.27	それぞれの鍵タイプに対して、CKMS設計は、鍵タイプの非活性化の事前通知の要求事項を明記しなければならない。それには、CKMSがサポートするどの役割に通知されるか、どのように通知されるか、どのセキュリティ処理（services）が通知に適用されるか、及び通知の期間が含まれる。	6.4.4節	済 ・ 対象外	

検討番号（5章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
B.13	FR6.28	CKMS設計は、いつ、どのように、どのような状況で失効が実行され、失効情報を依拠する当事者が利用可能になるかを明記しなければならない。	6.4.5節	済・対象外	
B.14	FR6.108	CKMS設計は、使用される又は使用できる鍵失効メカニズム及び関連付けられた依拠するエンティティへの通知メカニズムを明記しなければならない。	6.8.3節	済・対象外	
B.15	FR6.29	CKMS設計は、どのように、どのような状況で鍵が一時停止されるかを明記しなければならない。	6.4.6節	済・対象外	
B.16	FR6.30	CKMS設計は、どのように一時停止情報を依拠又は通信する当事者が利用可能になるかを明記しなければならない。	6.4.6節	済・対象外	
B.17	FR6.32	CKMS設計は、どのように一時停止された鍵によるセキュリティ処理（services）の実行を防止するのかを明記しなければならない。	6.4.6節	済・対象外	
B.18	FR6.31	CKMS設計は、どのように、どのような状況で一時停止された鍵が再活性化されるかを明記しなければならない。	6.4.6節	済・対象外	
B.19	FR6.33	CKMS設計は、どのように再活性化情報を依拠又は通信する当事者が利用可能になるのかを明記しなければならない。	6.4.6節	済・対象外	
B.20	FR6.38	CKMS設計は、どのように、どのような条件で鍵が意図して破壊されるか、及び破壊がコンポーネントへの局所的（local）なものであるかCKMS全体への共通的（universal）なものであるかを明記しなければならない。	6.4.9節	済・対象外	
B.21	FR6.39	それぞれの鍵タイプに対して、CKMS設計は、鍵破壊の事前通知の要求事項を明記しなければならない。それには、どの当事者に通知されるか、どのように通知されるか、どのセキュリティ処理（services）が通知に適用されるか、及び通知の時期が含まれる。	6.4.9節	済・対象外	
B.22	FR6.19	CKMS設計は、それぞれの鍵タイプに対して、CKMSで使用される鍵生成手段を明記しなければならない。	6.4.1節	済・対象外	
B.23	FR6.20	CKMS設計は、対称鍵及びプライベート鍵を生成するのに使用される元となる乱数生成器を明記しなければならない。	6.4.1節	済・対象外	
B.24	FR6.36	CKMS設計は、鍵を導出又は更新するために使用される全てのプロセス、及び鍵が導出又は更新される状況を明記しなければならない。	6.4.8節	済・対象外	
B.25	FR6.37	それぞれの鍵タイプに対して、CKMS設計は、鍵の導出又は更新の事前通知の要求事項を明記しなければならない。それには、どの当事者に通知されるか、どのように通知されるか、どのセキュリティ処理（services）が通知に適用されるか、及び通知の期間が含まれる。	6.4.8節	済・対象外	
B.26	FR6.66	CKMS設計は、どのように、どこで、どのような状況で、対称鍵やそのメタデータが検証されるかを明記しなければならない。	6.4.24節	済・対象外	
B.27	FR6.63	CKMS設計は、どのように、どこで、どのような状況で、公開鍵ドメインパラメタが検証されるかを明記しなければならない。	6.4.21節	済・対象外	
B.28	FR6.64	CKMS設計は、どのように、どこで、どのような状況で、公開鍵が検証されるかを明記しなければならない。	6.4.22節	済・対象外	
B.29	FR6.65	CKMS設計は、どのように、どこで、どのような状況で公開鍵証明書パスが検証されるかを明記しなければならない。	6.4.23節	済・対象外	
B.30	FR6.70	CKMS設計は、サポートされている全てのトラストアンカー管理機能を明記しなければならない（[RFC6024]を参照）。	6.4.28節	済・対象外	

検討番号（5章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
B.31	FR6.71	CKMS設計は、依拠するエンティティがトラストアンカーについてのソース認証（source authentication）及び完全性検証を実行できるように、どのようにそれらのトラストアンカーがセキュアに配付されるかを明記しなければならない。	6.4.28節	済・対象外	
B.32	FR6.72	CKMS設計は、依拠するエンティティのシステムのトラストアンカーストアに対して、認可された追加、変更、削除のみが行えることを保証するために、どのように依拠するエンティティのシステムでトラストアンカーが管理されるかを明記しなければならない。	6.4.28節	済・対象外	
B.33	FR6.34	CKMS設計は、どのように、どのような条件で公開鍵の有効期間が延長できるかを明記しなければならない。	6.4.7節	済・対象外	
B.34	FR6.35	それぞれの鍵タイプに対して、CKMS設計は、鍵タイプの有効期間延長の事前通知の要求事項を明記しなければならない。それには、どの当事者に通知されるか、どのように通知されるか、どのセキュリティ処理（services）が通知に適用されるか、及び通知の期間が含まれる。	6.4.7節	済・対象外	
B.35	FR6.21	CKMS設計は、鍵と所有者の識別子を結び付けるプロセスを含めて、所有者登録に関わる全てのプロセスを明記しなければならない。	6.4.2節	済・対象外	
B.36	FR6.68	CKMS設計は、どのように、どこで、どのような状況で、プライベート鍵とそのメタデータの所持が検証されるかを明記しなければならない。	6.4.26節	済・対象外	
B.37	FR6.67	CKMS設計は、どのように、どこで、どのような状況で、プライベート鍵又は鍵ペア、あるいはそのメタデータが検証されるかを明記しなければならない。	6.4.25節	済・対象外	
B.38	FR6.40	使用されているそれぞれの鍵タイプに対して、CKMS設計は、何のメタデータが鍵と関連付けられているか、どのようにメタデータが鍵と関連付けられているか、及びメタデータが鍵と関連付けえられる状況を明記しなければならない。	6.4.10節	済・対象外	
B.39	FR6.41	使用されているそれぞれの鍵タイプに対して、CKMS設計は、どのように次のセキュリティ処理（services）（保護）が関連付けられたメタデータに適用されるかを明記しなければならない：ソース認証（source authentication）、完全性、及び機密性。	6.4.10節	済・対象外	
B.40	FR6.42	CKMS設計は、関連付けられたメタデータが変更される状況を明記しなければならない。	6.4.11節	済・対象外	
B.41	FR6.43	CKMS設計は、鍵と関連付けられたメタデータが削除される状況を明記しなければならない。	6.4.12節	済・対象外	
B.42	FR6.44	CKMS設計は、関連付けられたメタデータを削除するために使われる手法を明記しなければならない。	6.4.12節	済・対象外	
B.43	FR6.45	それぞれの鍵タイプに対して、CKMS設計は、どのメタデータが認可されたエンティティによってリスト化が可能かどうかを明記しなければならない。	6.4.13節	済・対象外	
B.44	FR6.73	CKMS設計は、鍵情報（暗号鍵やメタデータ）をストレージに入れるエンティティのID認証及び認可検証に使用される手段を明記しなければならない。	6.5節	済・対象外	
B.45	FR6.74	CKMS設計は、ストレージに入力する鍵情報（暗号鍵やメタデータ）の完全性検証に使用される手段を明記しなければならない。	6.5節	済・対象外	

検討番号（5章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
B.46	FR6.75	CKMS設計は、保管された対称鍵、プライベート鍵及びメタデータの機密性保護に使用される手段を明記しなければならない。	6.5節	済・対象外	
B.47	FR6.76	鍵ラッピング鍵（又は鍵ペア）が保管された鍵を保護するために使用される場合、CKMS設計は、鍵ラッピング鍵（又は鍵ペア）を保護し、その使用を制御するために使用される手段を明記しなければならない。	6.5節	済・対象外	
B.48	FR6.77	CKMS設計は、保管された鍵情報（暗号鍵及びメタデータ）の完全性保護に使用される手段を明記しなければならない。	6.5節	済・対象外	
B.49	FR6.78	CKMS設計は、保管された鍵へのアクセスがどのように制御されるかを明記しなければならない。	6.5節	済・対象外	
B.50	FR6.79	CKMS設計は、全ての保管された鍵を訂正又は復元するために使用される手法を明記しなければならない。	6.5節	済・対象外	
B.51	FR6.46	それぞれの鍵タイプに対して、CKMS設計は、以下のことを明記しなければならない：それぞれの鍵タイプとそのメタデータが保管される状況、鍵とメタデータの保管場所、及び鍵とメタデータの保護方法。	6.4.14節	済・対象外	
B.52	FR6.47	CKMS設計は、どのように、どこで、どのような状況において鍵及びそのメタデータがバックアップされるかを明記しなければならない。	6.4.15節	済・対象外	
B.53	FR6.48	CKMS設計は、バックアップされた鍵情報（暗号鍵及びメタデータ）の保護のためのセキュリティポリシーを明記しなければならない。	6.4.15節	済・対象外	
B.54	FR6.49	CKMS設計は、鍵情報（暗号鍵及びメタデータ）のバックアップ中のセキュリティポリシーがどのように実装されるかを明記しなければならない。例えば、バックアップされた鍵情報（暗号鍵及びメタデータ）の配送及び保管中における、機密性とマルチパーティコントロールの要求事項の実装方法。	6.4.15節	済・対象外	
B.55	FR6.50	CKMS設計は、どのように、どこで、どのような状況で鍵情報（暗号鍵やメタデータ）がアーカイブされるかを明記しなければならない。	6.4.16節	済・対象外	
B.56	FR6.51	CKMS設計は、鍵情報（暗号鍵やメタデータ）のセキュアな破壊、又は新しい保管メディアに書き込まれた後の古い保管メディアのセキュアな破壊のための手法を明記しなければならない。	6.4.16節	済・対象外	
B.57	FR6.52	CKMS設計は、アーカイブ鍵の暗号鍵有効期間（cryptoperiod）の期限切れ後に、鍵情報（暗号鍵やメタデータ）がどのように保護されるかを明記しなければならない。	6.4.16節	済・対象外	
B.58	FR6.53	CKMS設計は、鍵情報（暗号鍵やメタデータ）のCKMS復元ポリシーを明記しなければならない。	6.4.17節	済・対象外	
B.59	FR6.54	CKMS設計は、鍵情報（暗号鍵やメタデータ）の復元ポリシーを実装及び実行するために使用されるメカニズムを明記しなければならない。	6.4.17節	済・対象外	
B.60	FR6.55	CKMS設計は、どのように、どのような状況で鍵情報（暗号鍵やメタデータ）がそれぞれの鍵データベース又はメタデータ保管設備から復元されるかを明記しなければならない。	6.4.17節	済・対象外	
B.61	FR6.56	CKMS設計は、鍵情報（暗号鍵やメタデータ）が復元中にどのように保護されるかを明記しなければならない。	6.4.17節	済・対象外	
B.62	FR6.57	CKMS設計は、どのように、どのような状況で鍵及びそのメタデータが確立されるかを明記しなければならない。	6.4.18節	済・対象外	
B.63	FR6.80	CKMS設計は、配送中の対称鍵及びプライベート鍵の機密性保護に使用される手段を明記しなければならない。	6.6.1節	済・対象外	

検討番号（5章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
B.64	FR6.81	CKMS設計は、配送された鍵の完全性保護に使用される手段、及びエラー検出後にどのように鍵が再構築又は置き換えられるのかを明記しなければならない。	6.6.1節	済・対象外	
B.65	FR6.82	CKMS設計は、配送される鍵素材（keying material）の受信者に、どのように鍵送信者の識別子（ID）が認証されるかを明記しなければならない。	6.6.1節	済・対象外	
B.66	FR6.83	CKMS設計は、CKMSにサポートされるそれぞれの鍵合意スキームを明記しなければならない。	6.6.2節	済・対象外	
B.67	FR6.84	CKMS設計は、鍵合意に参加するそれぞれのエンティティがどのように認証されるかを明記しなければならない。	6.6.2節	済・対象外	
B.68	FR6.86	CKMS設計は、それぞれの鍵確認が実行される状況を明記しなければならない。	6.6.3節	済・対象外	
B.69	FR6.85	CKMS設計は、他方のエンティティと正しい鍵を確立したことを確認するために使用されるそれぞれの鍵確認手段を明記しなければならない。	6.6.3節	済・対象外	
B.70	FR6.87	CKMS設計は、鍵確立と保管の目的のためにCKMSによって採用されている全てのプロトコルを明記しなければならない。	6.6.4節	済・対象外	
B.71	FR10.11	CKMS設計は、暗号鍵及びそのメタデータをバックアップ及びアーカイブするための手続きを明記しなければならない。	10.7節	済・対象外	
B.72	FR10.12	CKMS設計は、保管又は伝送された破損した鍵情報（暗号鍵及びメタデータ）を復元又は置き換えるための手続きを明記しなければならない。	10.7節	済・対象外	
B.73	FR6.102	CKMS設計は、システムによって使用されているそれぞれの鍵タイプの受け入れ可能な暗号鍵有効期間（cryptoperiod）又は利用制限（usage limit）の範囲を明記しなければならない。	6.8.1節	済・対象外	
B.74	FR6.103	それぞれの鍵に対し、CKMS設計は、セキュリティがその鍵に依存する他の鍵タイプを明記しなければならず、また初期鍵の危殆化が発生した時にそれに依存する鍵がどのように置き換えられるかを明記しなければならない。	6.8.1節	済・対象外	
B.75	FR6.104	CKMS設計は、鍵が危殆化したときに他の危殆化した鍵を特定できるための手段を明記しなければならない。例えば、鍵導出鍵が危殆化したとき、導出された鍵をどのように特定するのか？	6.8.1節	済・対象外	
B.76	FR6.105	導入されたそれぞれの鍵タイプに対して、CKMS設計は、どのメタデータ要素が危殆化（機密性、完全性、又はソース）しやすいのかを明記しなければならない。	6.8.2節	済・対象外	
B.77	FR6.106	CKMS設計は、鍵のそれぞれの危殆化しやすいメタデータ要素に危殆化（機密性、完全性、又はソース）が起こったときに、起こり得るセキュリティ結果を明記しなければならない。	6.8.2節	済・対象外	
B.78	FR6.107	CKMS設計は、それぞれの危殆化しやすいメタデータ要素での危殆化からどのように回復できるかを明記しなければならない。	6.8.2節	済・対象外	
B.79	FR6.117	CKMS設計は、それぞれのサポートされる役割に提供される、あらゆる役員・従業員による危殆化の検知機能を明記しなければならない。	6.8.7節	済・対象外	
B.80	FR6.118	CKMS設計は、それぞれのサポートされる役割に提供される、あらゆる役員・従業員による危殆化を最小化する機能を明記しなければならない。	6.8.7節	済・対象外	

検討番号（5章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
B.81	FR6.119	CKMS設計は、それぞれのサポートされる役割に提供される、CKMS危殆化からの回復能力を明記しなければならない。	6.8.7節	済・対象外	

検討番号（6章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
C.01	FR2.1	CKMS設計は、システムによって使用される全ての暗号アルゴリズムとそれぞれのアルゴリズムでサポートされる全ての鍵長を明記しなければならない。	2.1節	済・対象外	
C.02	FR2.2	CKMS設計は、鍵と鍵に結び付けられたメタデータを保護するために導入されているそれぞれの暗号技術について推定されるセキュリティ強度を明記しなければならない。	2.1節	済・対象外	

検討番号（7章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
D.01	FR6.1	CKMS設計は、使用されているそれぞれの鍵タイプを明記及び定義しなければならない。	6.1節	済・対象外	
D.02	FR6.2	システムで使用されているそれぞれの鍵タイプに対して、CKMS設計は、信頼関係のために選択される全てのメタデータ要素、メタデータ要素が作成され鍵との関連付けが満たされている状況、及び関連付けの手段（すなわち、暗号メカニズム又は信頼プロセス）を明記しなければならない。	6.2.1節	済・対象外	
D.03	FR6.13	それぞれの鍵タイプに対して、CKMS設計は、暗号鍵及びメタデータ要素に関する以下の情報を明記しなければならない： a) 鍵タイプ b) 暗号鍵有効期間（cryptoperiod）（静的鍵（static key）に対して） c) 生成手段 i. 使用した乱数生成器（RNG） ii. 鍵生成の仕様（例えば、署名鍵については[FIPS 186]、Diffie-Hellman鍵確立鍵（key establishment key）については[SP800-56A]） d) それぞれのメタデータ要素に対して、以下を含める i. メタデータのソース ii. メタデータの検証方法 e) 鍵確立（key establishment）の手段 i. 鍵配送スキーム（使用されている場合） ii. 鍵合意スキーム（使用されている場合） iii. プロトコル名（名称があるプロトコルが使用されている場合） f) 暴露に対する保護（例えば、鍵の機密性、物理セキュリティ） g) 改ざんに対する保護（例えば、MAC又はデジタル署名） h) 鍵を使用し得るアプリケーション（例えば、TLS、EFS、S/MIME、IPSec、PKINIT、SSH、等） i) 鍵の使用が許可されないアプリケーション j) 鍵保証（key assurances） i. 対称鍵保証（Symmetric key assurances）（例えば、フォーマットチェック） ・誰が保証を得るか ・保証が得られる状況 ・どのように保証を得るか ii. 非対称鍵保証（Asymmetric key assurances）（例えば、所有と有効性の保証） ・誰が保証を得るか ・保証が得られる状況 ・どのように保証を得るか iii. ドメインパラメタ有効性チェック ・誰が有効性チェックを実行するか ・チェックが実行される状況 ・どのようにドメインパラメタの有効性の保証を得るか	6.2.2節	済・対象外	

検討番号（7章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
D.04	FR6.14	CKMS設計は、CKMSによって生成、保管、伝送、処理、及びその他管理される全ての鍵タイプ及びメタデータについて、全てのシンタックス、セマンティクス、及びフォーマットを明記しなければならない。	6.2.2節	済 ・ 対象外	
D.05	FR6.3	メタデータ要素の鍵保護（Key Protections）で使用されるそれぞれの暗号メカニズムに対して、CKMS設計は、以下を明記しなければならない： i. 暗号アルゴリズム ii. 鍵パラメタ iii. 鍵識別子 iv. 保護値（protection value）：この要素は、完全性保護、機密性保護、又はソース認証（source authentication）の保護値（protection value）を含む。例えば、適切に実装されたMAC又はデジタル署名技術は、完全性保護やソース認証（source authentication）を提供し得る。 v. 保護が適用された時期 vi. 保護が検証された時期	6.2.1節	済 ・ 対象外	
D.06	FR6.5	メタデータ要素のメタデータ保護（Metadata Protections）で使用されるそれぞれの暗号メカニズムに対して、CKMS設計は、以下を明記しなければならない： i. 暗号アルゴリズム ii. 鍵パラメタ iii. 鍵識別子 iv. 保護値（protection value）（例：MAC、デジタル署名） v. 保護が適用された時期 vi. 保護が検証された時期 一般に、特に鍵とメタデータがひとまとめにされる場合、鍵とメタデータに対して同じメカニズムが使用される。	6.2.1節	済 ・ 対象外	
D.07	FR6.7	メタデータ要素の信頼関係保護で使用されるそれぞれの暗号メカニズムに対して、CKMS設計は、以下を明記しなければならない： i. 暗号アルゴリズム ii. 鍵パラメタ iii. 鍵識別子 iv. 保護値（protection value）（例：MAC、デジタル署名） v. 保護が適用された時期 vi. 保護が検証された時期	6.2.1節	済 ・ 対象外	
D.08	FR6.4	メタデータ要素の鍵保護（Key Protections）で使用される暗号学的ではないそれぞれの信頼プロセスに対して、CKMS設計は、以下を明記しなければならない： i. 他のプロセスと区別するために使用されるプロセス識別子 ii. プロセスの説明又はプロセスの説明へのポインタ	6.2.1節	済 ・ 対象外	
D.09	FR6.6	メタデータ要素のメタデータ保護（Metadata Protections）で使用される暗号学的ではないそれぞれの信頼プロセスに対して、CKMS設計は、以下を明記しなければならない： i. このプロセスを他のプロセスから区別するために使用される識別子 ii. プロセスの説明又はプロセスの説明へのポインタ	6.2.1節	済 ・ 対象外	

検討番号（7章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
D.10	FR6.8	メタデータ要素の信頼関係保護で使用される暗号学的ではないそれぞれの信頼プロセスに対して、CKMS設計は、以下を明記しなければならない： i. このプロセスを他のプロセスから区別するために使用される識別子 ii. プロセスの説明又はプロセスの説明へのポインタ	6.2.1節	済・対象外	

検討番号（8章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
E.01	FR6.88	CKMS設計は、エンティティ、ACS（アクセスコントロールシステム）、機能ロジック、及びそれらの間の接続の配置を示すことでCKMSのトポロジーを明記しなければならない。	6.7.1節	済・対象外	
E.02	FR6.89	CKMS設計は、適切な操作を保証するために実装されている鍵管理機能に対する制限を明記しなければならない。	6.7.1節	済・対象外	
E.03	FR6.90	CKMS設計は、鍵管理機能へのアクセスがどのように認可されたエンティティを制限しているかを明記しなければならない。	6.7.1節	済・対象外	
E.04	FR6.91	CKMS設計は、鍵管理機能へのアクセスを制御するためのACSとそのポリシーを明記しなければならない。	6.7.1節	済・対象外	
E.05	FR6.92	CKMS設計は、少なくとも以下を明記しなければならない： a) エンティティの粒度（例：人、デバイス、組織） b) エンティティが識別されているかどうか、及びその方法 c) エンティティが認証されているかどうか、及びその方法 d) エンティティの認可が検証されているか、及びその方法 e) それぞれの鍵管理機能のアクセスコントロール	6.7.1節	済・対象外	
E.06	FR6.93	CKMS設計は、CKMSセキュリティポリシーを適応、実装、施行するためのACSの能力を明記しなければならない。	6.7.1節	済・対象外	
E.07	FR8.19	CKMS設計は、以下を含む、使用する暗号モジュール及びそれぞれのセキュリティポリシーを特定しなければならない： a) それぞれのモジュールの実装形態（ソフトウェア、ファームウェア、ハードウェア、又はハイブリッド） b) それぞれのモジュールの完全性を保護するために使用されるメカニズム c) それぞれのモジュールの暗号鍵を保護するために使用される物理的及び論理的メカニズム d) それぞれのモジュール（セキュリティ機能を含む）で実行された第三者試験と検証、及びそれぞれのモジュールで使用される保護措置	8.4節	済・対象外	
E.08	FR6.58	CKMS設計は、どのように、どのような状況で鍵情報（暗号鍵及びメタデータ）が暗号モジュールに入力されるか、入力される形式、及び入力に用いられる手段を明記しなければならない。	6.4.19節	済・対象外	
E.09	FR6.59	CKMS設計は、（必要ならば）どのように入力された鍵とメタデータの完全性及び機密性が入力時に保護され検証されるかを明記しなければならない。	6.4.19節	済・対象外	
E.10	FR6.60	CKMS設計は、どのように、どのような状況で鍵情報（暗号鍵及びメタデータ）が暗号モジュールから出力されるか、及び出力される形式を明記しなければならない。	6.4.20節	済・対象外	
E.11	FR6.61	CKMS設計は、どのように出力された鍵とメタデータの機密性及び完全性が暗号モジュールの外部で保護されるかを明記しなければならない。	6.4.20節	済・対象外	
E.12	FR6.94	CKMS設計は、平文での対称鍵又はプライベート鍵が暗号モジュールに入力又は出力される状況を明記しなければならない。	6.7.2節	済・対象外	
E.13	FR6.62	プライベート鍵、対称鍵、又は機密のメタデータが暗号モジュールから平文形式で出力される場合、CKMS設計は、鍵情報（暗号鍵及びメタデータ）が提供される前に、呼び出しエンティティを認証するかどうか、及びどのように認証するかを明記しなければならない。	6.4.20節	済・対象外	

検討番号（8章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
E.14	FR6.95	いかなる暗号モジュールにおいても、平文での対称鍵又は平文のプライベート鍵が入力又は出力される場合には、CKMS設計は、平文鍵がどのように暗号モジュールの外部で保護され、制御されるかを明記しなければならない。	6.7.2節	済・対象外	
E.15	FR6.96	いかなる暗号モジュールにおいても、平文での対称鍵又は平文のプライベート鍵が入力又は出力される場合には、CKMS設計は、そのような動作がどのように監査されるかを明記しなければならない。	6.7.2節	済・対象外	
E.16	FR6.109	CKMS設計は、暗号モジュールの中身への物理的及び論理的アクセスがどのように認可されたエンティティに制限されるかを明記しなければならない。	6.8.4節	済・対象外	
E.17	FR6.110	CKMS設計は、暗号モジュールの危殆化からの回復のために使用される方法を明記しなければならない。	6.8.4節	済・対象外	
E.18	FR6.111	CKMS設計は、どの非侵襲攻撃がシステムで使用される暗号モジュールによって軽減されるかを記載し、どのように軽減が実行されるかの記載を提供しなければならない。	6.8.4節	済・対象外	
E.19	FR6.112	CKMS設計は、非侵襲攻撃に脆弱であるあらゆる暗号モジュールを明記しなければならない。	6.8.4節	済・対象外	
E.20	FR6.113	CKMS設計は、可能性のある非侵襲攻撃によって起きる脆弱性を受け入れる原則を明記しなければならない。	6.8.4節	済・対象外	
E.21	FR6.97	それぞれの鍵とメタデータの管理機能に対し、CKMS設計は、全ての人間による入力パラメタ、そのフォーマット、及び入力が行われないときにCKMSが取るアクションを明記しなければならない。	6.7.3節	済・対象外	
E.22	FR6.98	CKMS設計は、マルチパーティコントロール（multiparty control）を要求する全ての機能を明記し、それぞれの機能に対してkとnを規定しなければならない。	6.7.4節	済・対象外	
E.23	FR6.99	それぞれのマルチパーティ機能に対して、CKMS設計は、なぜn個中任意のk個のエンティティで望む機能を有効にできるが$k-1$個のエンティティでは有効にできないのかを示すあらゆる既知の論拠（論理、数学）を引用又は明記しなければならない。	6.7.4節	済・対象外	
E.24	FR6.100	CKMS設計は、鍵分割技術を使用して管理される全ての鍵を明記しなければならず、またそれぞれの技術に対してnとkを明記しなければならない。	6.7.5節	済・対象外	
E.25	FR6.101	使用しているそれぞれの（k, n）鍵分割技術に対して、CKMS設計は、鍵分割がどのように行われ、なぜn個中任意のk個の分割鍵で鍵を構成できるが$k-1$個の分割鍵では鍵に関する情報を何ら提供しないのかを示すあらゆる既知の論拠（論理、数学）を明記しなければならない。	6.7.5節	済・対象外	
E.26	FR9.1	CKMS設計は、システムで実行され合格した非プロプライエタリベンダテストを明記しなければならない。	9.1節	済・対象外	
E.27	FR9.3	CKMSが他のシステムとの相互運用性を主張する場合、CKMS設計は、その主張を検証するために実行し合格したテストを明記しなければならない。	9.3節	済・対象外	
E.28	FR9.4	CKMSが他のシステムとの相互運用性を主張する場合、CKMS設計は、相互運用性に必要な、あらゆる構成設定（configuration settings）を明記しなければならない。	9.3節	済・対象外	

検討番号（8章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
E.29	FR9.7	CKMS設計は、システムで実行された機能テスト及びセキュリティテスト、並びにそのテスト結果を明記しなければならない。	9.6節	済・対象外	
E.30	FR9.8	CKMS設計は、CKMSが使用される設計上の環境条件を明記しなければならない。	9.7節	済・対象外	
E.31	FR9.9	CKMS設計は、CKMSデバイスで実行された環境テストの結果を、設計上の条件を超えたストレスをデバイスに与えた時の全てのテストの結果も含めて、明記しなければならない。	9.7節	済・対象外	
E.32	FR9.5	CKMS設計は、設計者によって作成及び実装された全ての自己テスト、及びそれが正しい動作を検証する対象のCKMS機能を明記しなければならない。	9.4節	済・対象外	
E.33	FR9.6	CKMS設計は、今までにシステムで実行された全てのスケーラビリティ分析及びテストを明記しなければならない。	9.5節	済・対象外	
E.34	FR9.2	CKMS設計は、CKMS又はデバイスが今までに合格した全ての第三者テストプログラムを明記しなければならない。	9.2節	済・対象外	
E.35	FR10.8	CKMS設計は、モジュールのエラー検知及び完全性検証のために、それぞれの暗号モジュールがどの自己テストを使用するかを明記しなければならない。	10.6節	済・対象外	
E.36	FR10.9	CKMS設計は、それぞれの暗号モジュールがどのように検知したエラーに応答するかを明記しなければならない。	10.6節	済・対象外	
E.37	FR10.10	CKMS設計は、障害が起こった暗号モジュールの修理又は交換の方策を明記しなければならない。	10.6節	済・対象外	

検討番号（9章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
F.01	FR8.1	CKMS設計は、それぞれのCKMSデバイスと意図する目的を明記しなければならない。	8.1節	済・対象外	
F.02	FR8.2	CKMS設計は、CKMSコンポーネントを含むそれぞれのデバイスを保護するための物理セキュリティコントロールを明記しなければならない。	8.1節	済・対象外	
F.03	FR6.120	CKMS設計は、全てのCKMSコンポーネント及びデバイスがどのように認可されない（不正な）物理アクセスから保護されるかを明記しなければならない。	6.8.8節	済・対象外	
F.04	FR6.121	CKMS設計は、CKMSがどのように認可されない（不正な）物理アクセスを検知するかを明記しなければならない。	6.8.8節	済・対象外	
F.05	FR8.3	CKMS設計は、それぞれのCKMSデバイスに対して、全てのセキュアなOSの要求事項（いかなる必要なOS設定も含む）を明記しなければならない。	8.2.1節	済・対象外	
F.06	FR8.4	CKMS設計は、下記のどの堅牢化機能がCKMSによって実行されているかを明記しなければならない： a) 全ての必須でないソフトウェアプログラムとユーティリティをコンピュータから削除する b) 危殆化を受けやすいシステム機能及びアプリケーションに対するアクセスコントロールに最小権限の原則を適用する c) 危殆化を受けやすいシステム及びアプリケーションのファイルとデータに対するアクセスコントロールに最小権限の原則を適用する d) ユーザアカウントを合理的な運用に必要なだけに制限する、すなわち、もはや必要のないアカウントは無効化又は削除する e) 最小権限の原則でアプリケーションを動作させる f) 全てのデフォルトパスワード及びデフォルト鍵をそれぞれ強力なパスワード及びランダムに生成された鍵で置き換える g) システムの運用に必要でないネットワークサービスを無効化又は削除する h) システムの運用に必要でない全ての他の処理（service）を無効化又は削除する i) リムーバブルメディアを無効化する、又はリムーバブルメディアにおける自動実行機能を無効化しメディア挿入時の自動マルウェアチェック機能を有効にする j) システム運用に必要でないネットワークポートを無効化する k) オプションのセキュリティ機能を適切に有効化する l) セキュアにする他の設定オプションを選択する	8.2.1節	済・対象外	
F.07	FR8.5	CKMS設計は、OSの正しいインスタンス化を保証するBIOS保護機能を明記しなければならない。	8.2.1節	済・対象外	
F.08	FR8.6	CKMS設計は、それぞれのCKMSデバイスに必要なセキュリティコントロールを明記しなければならない。	8.2.2節	済・対象外	
F.09	FR8.7	CKMS設計は、堅牢化の基となるデバイス／CKMSのセキュリティ設定要求事項及びガイドラインを明記しなければならない。	8.2.2節	済・対象外	

検討番号（9章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
F.10	FR8.8	CKMS設計は、CKMSデバイスに対する以下のマルウェア防御能力を明記しなければならない： a) ウイルス対策ソフトウェア。アンチウイルススキャン、ソフトウェア更新、及びウイルスシグネチャデータベース更新を開始する時間周期及びイベントの指定を含む。 b) スパイウェア対策ソフトウェア。アンチスパイウェアスキャン、ソフトウェア更新、及びウイルスシグネチャ更新を開始する時間周期及びイベントの指定を含む。 c) ルートキット検出及び防御ソフトウェア。ルートキット検出、ソフトウェア更新、及びシグネチャ更新を開始する時間周期及びイベントの指定を含む。	8.2.3節	済・対象外	
F.11	FR8.9	CKMS設計は、OS及びCKMSアプリケーションソフトウェアに対する以下のソフトウェア完全性チェックの情報を明記しなければならない： a) ソフトウェア完全性がインストール時に検証される場合、検証がどのように実行されるかを記載する b) ソフトウェア完全性が定期的に検証される場合、検証が実行される頻度を記載する	8.2.3節	済・対象外	
F.12	FR8.10	CKMS設計は、サポートされている監査可能イベントを明記し、それぞれのイベントは固定されているか選択可能であるかを示さなければならない。	8.2.4節	済・対象外	
F.13	FR8.11	それぞれの選択可能な監査可能イベントに対し、CKMS設計は、イベントを選択する能力を持つ役割を明記しなければならない。	8.2.4節	済・対象外	
F.14	FR8.12	それぞれの監査可能イベントに対し、CKMS設計は、記録されるデータを明記しなければならない。	8.2.4節	済・対象外	
F.15	FR8.14	CKMS設計は、システムファイルの改変又はアクセスコントロールリストのようなセキュリティ属性のあらゆる改変について検知や防止をするため、危殆化を受けやすいシステムファイルに対するシステム監視要求事項を明記しなければならない。	8.2.4節	済・対象外	
F.16	FR8.13	CKMS設計は、CKMSの正しい運用及びセキュリティを評価するために、どの自動化ツールが提供されているかを明記しなければならない。	8.2.4節	済・対象外	
F.17	FR8.15	CKMS設計は、CKMSによって採用される境界保護メカニズムを明記しなければならない。	8.3節	済・対象外	
F.18	FR8.16	CKMS設計は、以下を明記しなければならない： a) 使用されるファイアウォールのタイプとファイアウォールを介して許可されるプロトコル。それぞれのプロトコルタイプの発信元（source）と宛先（destination）を含む b) 使用される侵入検知・防止システムのタイプ。ログ及びセキュリティ侵害対応の機能を含む	8.3節	済・対象外	
F.19	FR8.17	CKMS設計は、CKMSデバイスをサービス拒否（DoS）攻撃から保護するために使用される方法を明記しなければならない。	8.3節	済・対象外	
F.20	FR8.18	CKMS設計は、使用されるそれぞれの方法がどのようにサービス拒否攻撃から保護するかを明記しなければならない。	8.3節	済・対象外	

検討番号（9章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
F.21	FR9.10	CKMS設計は、以下を明記しなければならない： a) 構成制御の下に置かれているデバイス（ソースコード、スクリプト実装、実行コード、ファームウェア、ハードウェア、文書、及びテストコードを含む） b) 構成制御の下でコンポーネント及びデバイスへの認可された変更だけが行われたことを保証するための保護要求事項（例えば、形式的認可及び適切な記録保持）	9.8.1節	済・対象外	
F.22	FR9.11	CKMS設計は、以下を含む、CKMSで使用される製品のセキュアな配付の要求事項を明記しなければならない： a) 配付プロセス中に製品がタンパー（tamper）されていない、又はタンパーされたことが検知されることを保証するための保護要求事項 b) 配付プロセス中に製品が交換されていない、又は交換されたことが検知されることを保証するための保護要求事項 c) 要求されていない配付が検知されることを保証するための保護要求事項 d) 製品の配付が差し止め又は遅延していない、及び差し止め又は遅延が検知されることを保証するための保護要求事項	9.8.2節	済・対象外	
F.23	FR9.12	CKMS設計は、以下を含む、CKMSの開発環境及びメンテナンス環境におけるセキュリティ要求事項を明記しなければならない： a) 物理セキュリティ要求事項 b) 開発者、試験者、及び保守員に対する身分照会及びバックグラウンドチェックのような人的セキュリティ要求事項 c) 複数人員（multi-person）による制御、及び職掌分散（separation of duties）のような手続き的セキュリティ d) 開発環境及びメンテナンス環境の保護、及び認可されたユーザにアクセスを許可するアクセスコントロールの提供のためのコンピュータセキュリティコントロール e) ハッキングの試みから開発環境及びメンテナンス環境を保護するためのネットワークセキュリティコントロール f) 開発下のソフトウェア及びその制御データの完全性を保護するための暗号学的セキュリティコントロール g) ツール（例えば、エディタ、コンパイラ、ソフトウェアリンカ、ローダ等）が信頼でき、マルウェアのソースでないことを保証するために利用する手段	9.8.3節	済・対象外	
F.24	FR9.13	CKMS設計は、以下を含む、システムの欠陥を検知するCKMSの能力を明記しなければならない： a) 既知解テスト b) エラー訂正コード c) 異常故障診断技術 d) 機能テスト	9.8.4節	済・対象外	
F.25	FR9.14	CKMS設計は、以下を含む、欠陥を報告するCKMSの能力を明記しなければならない：ステータスレポートメッセージを機密性、完全性、及びソース認証保護付きで作成する能力、及び認可されない遅延を検知する能力。	9.8.4節	済・対象外	

検討番号（9章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
F.26	FR9.15	CKMS設計は、欠陥を分析し、かつ起こりやすい又はよく知られている欠陥に対する修正を作成／取得するCKMSの能力を明記しなければならない。	9.8.4節	済・対象外	
F.27	FR9.16	CKMS設計は、機密性、完全性、及びソース認証保護付きで修正を送信し、かつ認可されない遅延を検知するCKMSの能力を明記しなければならない。	9.8.4節	済・対象外	
F.28	FR9.17	CKMS設計は、時宜を得て修正を実装するCKMSの能力を明記しなければならない。	9.8.4節	済・対象外	
F.29	FR11.1	CKMS設計は、完全なCKMSセキュリティアセスメントの前又は同時に行われる、必要な保証実行策を明記しなければならない。	11.1節	済・対象外	
F.30	FR11.2	CKMS設計は、完全なセキュリティアセスメントが繰り返される状況を明記しなければならない。	11.1節	済・対象外	
F.31	FR11.3	CKMS設計は、あらゆるCKMSデバイスについて、認証を受けた全ての認証プログラムを明記しなければならない。	11.1.1節	済・対象外	
F.32	FR11.4	CKMS設計は、認証済みデバイスに対する全ての認証番号を明記しなければならない。	11.1.1節	済・対象外	
F.33	FR11.5	CKMS設計は、完全なセキュリティアセスメントの一部として、アーキテクチャレビューを必要とするかどうかを明記しなければならない。	11.1.2節	済・対象外	
F.34	FR11.6	アーキテクチャレビューが必要である場合、CKMS設計は、アーキテクチャレビューチームに必要なスキルセットを明記しなければならない。	11.1.2節	済・対象外	
F.35	FR11.7	CKMS設計は、必要な全てのCKMSの機能テスト及びセキュリティテストを明記しなければならない。	11.1.3節	済・対象外	
F.36	FR11.8	CKMS設計は、今までに実行された全ての機能テスト及びセキュリティテストの結果を報告しなければならない。	11.1.3節	済・対象外	
F.37	FR11.9	CKMS設計は、今までに実行されたあらゆる完了したペネトレーションテストの結果を明記しなければならない。	11.1.3節	済・対象外	
F.38	FR11.10	CKMS設計は、セキュリティレビューの周期を明記しなければならない。	11.2節	済・対象外	
F.39	FR11.11	CKMS設計は、CKMSデバイスの観点から、セキュリティレビューのスコープを明記しなければならない。	11.2節	済・対象外	
F.40	FR11.12	CKMS設計は、レビュー対象のそれぞれのCKMSデバイスに対して行われる実行策の観点で、定期的なセキュリティレビューのスコープを明記しなければならない。	11.2節	済・対象外	
F.41	FR11.13	CKMS設計は、定期的なセキュリティレビューの一部として実行される機能テスト及びセキュリティテストを明記しなければならない。	11.2節	済・対象外	
F.42	FR11.14	CKMS設計は、追加のセキュリティアセスメントが実施されるべき状況を明記しなければならない。	11.3節	済・対象外	
F.43	FR11.15	CKMS設計は、追加のセキュリティアセスメントのスコープを明記しなければならない。	11.3節	済・対象外	
F.44	FR11.16	CKMS設計は、セキュリティを維持するために、実行することが必要な堅牢化アクティビティをリスト化しなければならない。	11.4節	済・対象外	
F.45	FR6.123	CKMS設計は、あらゆるCKMSのコンポーネント又はデバイスへの物理セキュリティ侵害がCKMSによって検知されたときに、自動的に通知されるエンティティを明記しなければならない。	6.8.8節	済・対象外	

検討番号（9章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
F.46	FR6.122	CKMS設計は、CKMSがどのように暗号モジュール以外のコンポーネント及びデバイスへの認可されない（不正な）物理アクセスから回復するかを明記しなければならない。	6.8.8節	済・対象外	
F.47	FR6.124	CKMS設計は、侵害された領域がどのようにセキュアな状態に再確立できるかを明記しなければならない。	6.8.8節	済・対象外	
F.48	FR6.114	CKMS設計は、CKMSシステムハードウェア、ソフトウェア、及びデータに対する認可されない改変を検出するために利用されるメカニズムを明記しなければならない。	6.8.5節	済・対象外	
F.49	FR6.115	CKMS設計は、CKMSシステムハードウェア、ソフトウェア、及びデータに対する認可されない改変からどのようにCKMSが回復するのかを明記しなければならない。	6.8.5節	済・対象外	
F.50	FR6.116	CKMS設計は、システムによって使用されるネットワークセキュリティコントロールの危殆化からどのように回復するかを明記しなければならない。特に、 a) CKMS設計は、それぞれのネットワークセキュリティコントロールデバイスに対して考えられる危殆化シナリオを明記しなければならない。 b) CKMS設計は、それぞれの想定される危殆化シナリオに対して、この節に記載されたどの軽減技術が採用されるかを明記しなければならない。	6.8.6節	済・対象外	
F.51	FR10.1	CKMS設計は、必要な環境的、火災、及び物理的なアクセスコントロール保護メカニズム、及び損害からの基幹及び全てのバックアップ設備への回復手続きを明記しなければならない。	10.1節	済・対象外	
F.52	FR10.2	CKMS設計は、基幹及び全てのバックアップ設備に対する、電気、水道、衛生、暖房、冷房、及び空気清浄に関する推奨要求値だけでなく最小要求値についても明記しなければならない。	10.2節	済・対象外	
F.53	FR10.3	CKMS設計は、ユーザ、エンタープライズ、及びCKMSアプリケーションによる予測されるニーズに見合うサービスの運用継続を保証するために、設計内に存在し、かつ運用中に利用可能であることを要求される通信及び計算機能の冗長性を明記しなければならない。	10.3節	済・対象外	
F.54	FR10.4	CKMS設計は、バックアップの方策、及びハードウェアコンポーネント及びデバイスの障害からの回復のための方策を明記しなければならない。	10.4節	済・対象外	
F.55	FR10.5	CKMS設計は、システムソフトウェアの正しさを検証するために、CKMSによって提供されている全ての技術を明記しなければならない。	10.5節	済・対象外	
F.56	FR10.6	CKMS設計は、ソフトウェアがメモリにロードされたときにソフトウェアの改変又は破損を検知するために、CKMSによって提供される全ての技術を明記しなければならない。	10.5節	済・対象外	
F.57	FR10.7	CKMS設計は、バックアップ及び重大なソフトウェア障害からの回復のための方策を明記しなければならない。	10.5節	済・対象外	