第三種郵便物認可　明治二十五年三月三十一日

10.1.1.5　暗号の利用に関する方針は、この方針の実施の責任や鍵生成を含めた鍵管理に対する責任など、役割及び責任を考慮して定める。

10.1.1.6　暗号の利用に関する方針は、組織全体にわたって効果的に実施するために採用する標準類（業務プロセスに用いるソリューションの選択）を考慮して定める。

10.1.1.7　暗号の利用に関する方針は、暗号化した情報を用いることの、情報内容の検査（例えば、マルウェアの検出）に依存する管理策への影響を考慮して定める。

10.1.1.8　暗号に関わる組織の方針を実施するときには、世界の様々な地域における暗号技術の利用、及び国境を越える暗号化された情報の流れに関する問題に適用される、規制及び国内の制約を含める。

10.1.2　暗号鍵の利用、保護及び有効期間（lifetime）に関する方針を策定し、そのライフサイクル全体にわたって実施する。

10.1.2.1　方針には、暗号鍵の生成、保管、保存、読出し、配布、使用停止及び破壊を含むライフサイクル全体にわたって必要となる、セキュリティを保ったプロセスにおいて、暗号鍵を管理するための要求事項を含める。

10.1.2.2　最適な慣行に従って、暗号アルゴリズム、鍵の長さ及び使用法を選定する。

10.1.2.3　全ての暗号鍵は、改変及び紛失から保護する。

10.1.2.4　鍵の生成、保管及び保存のために用いられる装置は、物理的に保護する。

10.1.2.5　鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保った手法に基づき、種々の暗号システム及び種々のアプリケーションのための鍵を生成する。

10.1.2.6　鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保った手法に基づき、公開鍵証明書を発行し、入手する。

10.1.2.7　鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保った手法に基づき、意図するエンティティに鍵を配布する。これには、受領時に、鍵をどのような方法で活性化するか（使える状態にするか。）についても含める。

10.1.2.8　鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保った手法に基づき、鍵を保管する。これには、認可されている利用者がどのような方法で鍵にアクセスするかも含める。

10.1.2.9　鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保った手法に基づき、鍵を変更又は更新する。これには、鍵をいつ、どのような方法で変更するかの規則も含める。

10.1.2.10　鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保った手法に基づき、危険になった鍵に対処する。

10.1.2.11　鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保った手法に基づき、鍵を無効にする（例えば、鍵が危険になった場合、利用者が組織を離脱した場合。後者の場合には、鍵は保存する。）。これには、鍵をどのような方法で取消し又は非活性化するかも含める。

10.1.2.12　鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保った手法に基づき、紛失した鍵又は破損した鍵を回復する。

10.1.2.13　鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保った手法に基づき、鍵をバックアップ又は保存する。

10.1.2.14　鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保った手法に基づき、鍵を破壊する。

10.1.2.15　鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保った手法に基づき、鍵管理に関連する活動を記録し、監査する。

10.1.2.16　不適切な使用を起こりにくくするために、鍵の活性化及び非活性化の期日を定め、これによって、鍵管理の方針で定めた期間内でだけ鍵を使用できるようにする。

10.1.2.17　秘密鍵及びプライベート鍵は、認可されていない利用及び開示から保護するためセキュリティを保って管理し、公開鍵は、真正性を保つ。

10.1.2.18　公開鍵証明書を発行する認証局は、要求された信頼度を提供するために適切な管理策及び手順を備え、認知された組織であることを確認する。

10.1.2.19　暗号サービスの外部供給者（例えば、認証局）とのサービスレベルに関する合意又は契約の内容は、賠償責任、サービスの信頼性及びサービス提供のための応答時間に関する事項を含める。

11　物理的及び環境的セキュリティ

11.1　セキュリティを保つべき領域

目的：組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため

11.1.1　取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。

11.1.1.1　情報及び情報処理施設のある領域を保護するために、境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に基づいて、それぞれの物理的セキュリティ境界の位置及び強度を定める。

11.1.1.2　情報及び情報処理施設のある領域を保護するために、情報処理施設を収容した建物又は敷地の境界は、物理的に頑丈にする（すなわち、境界には隙間がなく、又は容易に侵入できる箇所がない。）。具体的には、以下の４点を行う。

１．敷地内の屋根、壁及び床は、堅固な構造物とする。

２．外部に接する全ての扉を、開閉制御の仕組み（例えば、かんぬき、警報装置、錠）によって、認可されていないアクセスから適切に保護する。

３．要員が不在のときには、扉及び窓を施錠する。

４．窓（特に一階の窓）については外部から保護する。

11.1.1.3　情報及び情報処理施設のある領域を保護するために、敷地又は建物への物理的アクセスを管理する。具体的には、以下の２点を行う。

１．有人の受付又はその他の手段を備える。

２．敷地及び建物へのアクセスは、認可された要員だけに制限する。

11.1.1.4　情報及び情報処理施設のある領域を保護するために、認可されていない物理的アクセス及び周囲への悪影響を防止するために、物理的な障壁を設置する。

11.1.1.5　情報及び情報処理施設のある領域を保護するために、以下の２点を行う。

１．セキュリティ境界上にある全ての防火扉は、該当する地域標準、国内標準及び国際標準が要求するレベルの抵抗力を確立するために、壁と併せて、警報機能を備え、監視し、試験する。

２．防火扉は、その地域の消防規則に従って、不具合が発生しても安全側に作動するように運用する。

11.1.1.6　情報及び情報処理施設のある領域を保護するために、以下の４点を行う。

１．全ての外部に接する扉及びアクセス可能な窓を保護するために、侵入者を検知する適切なシステムを、地域標準、国内標準又は国際標準に沿って導入する。

２．定めに従って試験を実施する。

３．無人の領域では、常に警報装置を作動させる。

４．セキュリティ上重要な他の領域（例えば、コンピュータ室、通信機器室）にも、常に警報装置を作動させる。

11.1.1.7　情報及び情報処理施設のある領域を保護するために、組織が自ら管理する情報処理施設は、外部関係者が管理する施設から物理的に分離する。