11.2　装置

目的：資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止するため

11.2.1　装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、保護する。

11.2.1.1　装置を保護するために、装置は、作業領域への不必要なアクセスが最小限になるように設置する。

11.2.1.2　装置を保護するために、取扱いに慎重を要するデータを扱う情報処理施設は、施設の使用中に認可されていない者が情報をのぞき見るリスクを低減するよう、その位置を慎重に定める。

11.2.1.3　装置を保護するために、認可されていないアクセスを回避するよう、保管設備のセキュリティを保つ。

11.2.1.4　装置を保護するために、特別な保護を必要とする装置は、それ以外の装置を分離するか、若しくは装置間に障壁を設ける。

11.2.1.5　装置を保護するために、潜在的な物理的及び環境的脅威（例えば、盗難、火災、爆発、ばい（煤）煙、水（又は給水の不具合）、じんあい（塵埃）、振動、化学的汚染、電力供給の妨害、通信妨害、電磁波放射、破壊）のリスクを最小限に抑えるよう管理策を採用する。

11.2.1.6　装置を保護するために、情報処理施設の周辺での飲食及び喫煙に関する指針を確立する。

11.2.1.7　装置を保護するために、情報処理施設の運用に悪影響を与えることがある環境条件（例えば、温度、湿度）を監視する。

11.2.1.8　装置を保護するために、全ての建物に、落雷からの保護を適用する。全ての電力及び通信の引込線に避雷器を装着する。

11.2.1.9　装置を保護するために、作業現場などの環境にある装置には、特別な保護方法（例えば、キーボードカバー）を使用する。

11.2.1.10　装置を保護するために、秘密情報を処理する装置は、電磁波の放射による情報漏えいのリスクを最小限にする。

11.2.2　装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。

11.2.2.1　サポートユーティリティ（例えば、電気、通信サービス、給水、ガス、下水、換気、空調）は、装置の製造業者の仕様及び地域の法的要求事項に適合しているものを採用する。

11.2.2.2　サポートユーティリティは、事業の成長及び他のサポートユーティリティとの相互作用に対応する能力を、定期的に評価する。

11.2.2.3　サポートユーティリティは、適切に機能することを確実にするために、定期的に検査及び試験する。

11.2.2.4　サポートユーティリティは、必要であれば、不具合を検知するための警報装置を取り付ける。

11.2.2.5　サポートユーティリティは、必要であれば、物理的な経路が異なる複数の供給元を確保する。

11.2.2.6　非常用の照明及び通信手段を備える。

11.2.2.7　非常口又は設備室の近くに、電源、給水、ガス又はその他のユーティリティを遮断するための緊急スイッチ及び緊急バルブを設置する。

11.2.3　データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。

11.2.3.1　情報処理施設に接続する電源ケーブル及び通信回線は、地下に埋設するか、又はこれに代わる十分な保護手段を施す。

11.2.3.2　ケーブル間の干渉を防止するために、電源ケーブルは、通信ケーブルから隔離する。

11.2.3.3　取扱いに慎重を要するシステム又は重要なシステムのために、以下の４点を行う。

１．外装電線管を導入し、点検箇所・終端箇所の施錠可能な部屋又は箱へ設置する。

２．ケーブルを保護するための電磁遮蔽を利用する。

３．ケーブルに取り付けられた認可されていない装置の技術的探索及び物理的検査を実施する。

４．配線盤、端子盤及びケーブル室への管理されたアクセスを実施する。

11.2.4　装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。

11.2.4.1　可用性及び完全性を継続的に維持することを確実とするために、装置は、供給者の推奨する間隔及び仕様に従って保守する。

11.2.4.2　可用性及び完全性を継続的に維持することを確実とするために、認可された保守要員だけが、装置の修理及び手入れを実施する。

11.2.4.3　可用性及び完全性を継続的に維持することを確実とするために、故障と見られるもの及び実際の故障の全て、並びに予防及び是正のための保守の全てについての記録を保持する。

11.2.4.4　可用性及び完全性を継続的に維持することを確実とするために、装置の保守を計画する場合には、この保守を、要員が構内で行うのか、又は組織の外で行うのかを考慮して、適切な管理策を実施する。その装置から秘密情報を消去するか、又は保守要員が十分に信頼できる者であることを確かめる。

11.2.4.5　可用性及び完全性を継続的に維持することを確実とするために、保険約款で定められた、保守に関する全ての要求事項を順守する。

11.2.4.6　可用性及び完全性を継続的に維持することを確実とするために、保守の後、装置を作動させる前に、その装置が改ざんされていないこと及び不具合を起こさないことを確実にするために検査する。

11.2.5　装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さない。

11.2.5.1　資産を構外に持ち出すことを許す権限をもつ従業員及び外部の利用者を特定する。

11.2.5.2　資産の持出し期限を設定し、また、返却がそのとおりであったか検証する。

11.2.5.3　資産が構外に持ち出されていることを記録し、また、返却時に記録する。

11.2.5.4　資産を扱う又は利用する者について、その識別情報、役割及び所属を文書化し、構外へ持ち出した装置、情報又はソフトウェアとともに返却させる。

11.2.6　構外にある資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、セキュリティを適用する。

11.2.6.1　情報を保管及び処理する装置（組織が所有する装置、及び個人が所有し組織のために用いる装置）を組織の構外で用いる場合は、管理層の認可を得る。

11.2.6.2　構外に持ち出した装置及び媒体は、公共の場所に無人状態で放置しない。

11.2.6.3　構外にある装置の保護のために、装置の保護（例えば、強力な電磁場にさらすことに対する保護）に関する製造業者の指示を常に守る。

11.2.6.4　構外にある装置の保護のために、在宅勤務、テレワーキング及び一時的サイトのような構外の場所についての管理策を、リスクアセスメントに基づいて決定し、状況に応じた管理策（例えば、施錠可能な文書保管庫、クリアデスク方針、コンピュータのアクセス制御、セキュリティを保ったオフィスとの通信）を適切に適用する。

11.2.6.5　構外にある装置の保護のために、構外にある装置を、複数の個人又は外部関係者の間で移動する場合には、その装置の受渡記録を明記した記録（少なくとも、その装置に対して責任を負う者の氏名及び組織を含むもの）を維持する。

11.2.6.6　リスク（例えば、損傷、盗難、傍受）は、場所によってかなり異なる場合があるため、それぞれの場所に応じた最も適切な管理策は、リスクを考慮して決定する。