17.1.1.4　事業継続及び災害復旧に関する正式な計画が策定されていない場合において、情報セキュリティ要求事項が変わらず存続すると定められない場合には、情報セキュリティの側面について事業影響度分析を実施し、通常の業務状況とは異なる困難な状況に適用できる情報セキュリティ要求事項を定める。

17.1.2　組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立し、文書化し、実施し、維持する。

17.1.2.1　組織は、必要な権限、経験及び力量を備えた要員を用い、中断・阻害を引き起こす事象に備え、これを軽減し、これに対処するための十分な管理構造を確実に設ける。

17.1.2.2　組織は、インシデントを管理し、情報セキュリティを維持するための責任、権限及び力量を備えたインシデント対応要員を確実に任命する。

17.1.2.3　組織は、経営陣が承認した情報セキュリティ継続の目的に基づいて、組織が中断・阻害を引き起こす事象を管理し、その情報セキュリティを既定のレベルに維持する場合の方法を計画及び手順に詳細に記して、計画、対応及び回復の文書化した手順を確実に策定し、これらを承認する。

17.1.2.4　組織は、情報セキュリティ継続に関する要求事項に従って、事業継続又は災害復旧のためのプロセス及び手順、並びにこれらを支援するシステム及びツールにおける情報セキュリティ管理策を確立し、文書化し、実施し、維持する。

17.1.2.5　組織は、情報セキュリティ継続に関する要求事項に従って、困難な状況において既存の情報セキュリティ管理策を維持するための、プロセス及び手順の変更並びにそれらの実施の変更を確立し、文書化し、実施し、維持する。

17.1.2.6　組織は、情報セキュリティ継続に関する要求事項に従って、困難な状況において維持することが不可能な情報セキュリティ管理策を補うための管理策を確立し、文書化し、実施し、維持する。

17.1.3　確立及び実施した情報セキュリティ継続のための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために、組織は、定められた間隔でこれらの管理策を検証する。

17.1.3.1　運用に関するものか、継続に関するものかを問わず、組織、技術、手順及びプロセスの変更が、情報セキュリティ継続に関する要求事項の変更につながる場合、変更後の要求事項に照らして、情報セキュリティのためのプロセス、手順及び管理策の継続性をレビューする。

17.1.3.2　組織は、情報セキュリティ継続のためのプロセス、手順及び管理策の機能が情報セキュリティ継続の目的と整合していることを確実にするために、これらの機能を実行し、試験する。

17.1.3.3　組織は、情報セキュリティ継続のためのプロセス、手順及び管理策を機能させる知識及びルーチンを実行及び試験し、そのパフォーマンスが情報セキュリティ継続の目的に整合していることを確実にする仕組みを整備する。

17.1.3.4　組織は、情報システム、情報セキュリティのプロセス、手順及び管理策、又はＢＣＭ・ＤＲＭのプロセス及びソリューションが変更された場合には、情報セキュリティ継続のための手段の妥当性及び有効性をレビューする。

17.2　冗長性

目的：情報処理施設の可用性を確実にするため

17.2.1　情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。

17.2.1.1　組織は、情報システムの可用性に関する業務上の要求事項を特定する。

17.2.1.2　組織は、既存のシステムアーキテクチャを利用しても可用性を保証できない場合には、冗長な構成要素又はアーキテクチャを構築する。

17.2.1.3　組織は、一つの構成要素から別の構成要素への切替え（failover）による冗長の場合、それが意図したとおりに動作することを確実にするために、冗長な情報システムを試験する。

18　順守

18.1　法的及び契約上の要求事項の順守

目的：情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため

18.1.1　各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保つ。

18.1.1.1　各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項を満たすための具体的な管理策及び具体的な責任について定め、文書化する。

18.1.1.2　管理者は、事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。

18.1.1.3　組織が他の国で事業を営む場合には、管理者は、関連する全ての国における法令、規制及び契約上の要求事項を順守する。

18.1.2　知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施する。

18.1.2.1　ソフトウェア製品及び情報製品の合法利用を明確に定めた知的財産権順守方針を公表する。

18.1.2.2　著作権を侵害しないことを確実にするために、ソフトウェアは、知名度の高い、かつ、定評のある供給元だけを通して取得する。

18.1.2.3　知的財産権を保護するための方針に対する認識を持続させ、それらの方針に違反した要員に対して懲罰処置をとる意思を通知する。

18.1.2.4　適切な資産登録簿を維持・管理し、知的財産権の保護が求められている全ての資産を特定する。

18.1.2.5　使用許諾を得ていることの証明及び証拠、マスタディスク、手引などを維持・管理する。

18.1.2.6　使用許諾で許可された最大利用者数を超過しないことを確実にするための管理策を実施する。

18.1.2.7　認可されているソフトウェア及び使用許諾されている製品だけが導入されていることのレビューを行う。

18.1.2.8　適切な使用許諾条件を維持・管理するための方針を定める。

18.1.2.9　ソフトウェアの処分又は他人への譲渡についての方針を定める。

18.1.2.10　公衆ネットワークから入手するソフトウェア及び情報の使用条件に従う。

18.1.2.11　著作権法が認めている場合を除いて、商用記録（フィルム、録音）を複製、他形式に変換、又は抜粋しない。

18.1.2.12　著作権法が認めている場合を除いて、書籍、記事、報告書又はその他文書の全部又は一部を複写しない。

18.1.3　記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護する。

18.1.3.1　具体的な組織の記録の保護について決定する場合は、組織の分類体系に基づき、その情報に適用されている分類を考慮して決定する。

18.1.3.2　記録類は、記録の種類（例えば、会計記録、データベース記録、トランザクションログ、監査ログ、運用手順）によって、また、更にそれぞれの種類での保持期間及び許容される記憶媒体の種類（例えば、紙、マイクロフィッシュ、磁気媒体、光媒体）の詳細によって分類する。