12.1.2.8　組織、業務プロセス、情報処理設備及びシステムの変更管理には、インシデントの解決のために必要な変更を、迅速にかつ管理して実施できるようにするための、緊急時の変更プロセスの提供を含める。

12.1.2.9　組織、業務プロセス、情報処理設備及びシステムに対するあらゆる変更の十分な管理を確実にするために、正式な責任体制及び手順を備える。

12.1.2.10　組織、業務プロセス、情報処理設備及びシステムに対する変更がなされたときには、変更に関わる全ての関連情報を含んだ監査ログを保持する。

12.1.3　要求された主要なシステム資源の使用を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測する。

12.1.3.1　事業におけるシステムの重要度を考慮に入れて、その容量・能力に関する要求事項を特定する。

12.1.3.2　システムの可用性及び効率性を確実にするため、また、改善のために、システム調整及び監視を適用する。

12.1.3.3　適切な時点で問題を知らせるために、検知のための管理策を備える。

12.1.3.4　将来必要とされる容量・能力の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理の能力についての現在の傾向及び予測される傾向を含める。

12.1.3.5　管理者は、特別な注意を払う必要のある主要なシステム資源（入手時間がかかるか又は費用がかかる資源）の使用を監視する。

12.1.3.6　管理者は、使用の傾向、特に業務用アプリケーション又は情報システムの管理ツールに関連した傾向を特定する。

12.1.3.7　システムセキュリティ又はサービスに脅威をもたらすおそれのある、潜在的なあい（隘）路（bottlenecks）及び主要な要員への依存度合いを特定し、回避するために、管理者は、上記の監視及び傾向を特定した情報を利用して、適切な処置を立案する。

12.1.3.8　業務上必須のシステムについては、容量・能力の管理計画を文書化することを検討する。

12.1.4　開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために、分離する。

12.1.4.1　運用上の問題を防ぐために必要な、開発環境、試験環境及び運用環境の間の分離レベルを特定し、それに従って分離する。

12.1.4.2　ソフトウェアの開発から運用の段階への移行についての規則は、明確に定め、文書化する。

12.1.4.3　開発ソフトウェア及び運用ソフトウェアは、異なるシステム又はコンピュータ上で、及び異なる領域又はディレクトリで実行する。

12.1.4.4　運用システム及びアプリケーションに対する変更は、運用システムに適用する前に、試験環境又はステージング環境（運用環境に近い試験環境）で試験する。

12.1.4.5　例外的な状況以外では、運用システムで試験を行わない。

12.1.4.6　コンパイラ、エディタ、及びその他の開発ツール又はシステムユーティリティは、必要でない場合には、運用システムからアクセスできないようにする。

12.1.4.7　利用者は、運用システム及び試験システムに対して、異なるユーザプロファイルを用いる。

12.1.4.8　メニューには、誤操作によるリスクを低減するために、適切な識別メッセージを表示する。

12.1.4.9　取扱いに慎重を要するデータは、試験システムに同等の管理策が備わっていない限り、その試験システム環境には複写を禁止する。

12.2　マルウェアからの保護

目的：情報及び情報処理施設がマルウェアから保護されることを確実にするため

12.2.1　マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施する。

12.2.1.1　マルウェアに対する検出・修復ソフトウェア、情報セキュリティに対する認識、及びシステムへの適切なアクセス・変更管理についての管理策に基づき、マルウェアから保護する。

12.2.1.2　認可されていないソフトウェアの使用を禁止する正式な方針を確立する。

12.2.1.3　認可されていないソフトウェアの使用を防止又は検出するための管理策を実施（例えば、アプリケーションのホワイトリスト化）する。

12.2.1.4　悪意のあるウェブサイトであると知られている又は疑われるウェブサイトの使用を、防止又は検出するための管理策を実施（例えば、ブラックリスト）する。

12.2.1.5　外部ネットワークから若しくは外部ネットワーク経由で、又は他の媒体を通じてファイル及びソフトウェアを入手することによるリスクから保護し、どのような保護対策を行うことが望ましいかを示す組織の正式な方針を確立する。

12.2.1.6　マルウェアに付け込まれる可能性のあるぜい弱性を、技術的ぜい弱性管理などを通じて低減させる。

12.2.1.7　重要な業務プロセスを支えるシステムのソフトウェア及びデータの、定めに従ったレビューの実施。未承認のファイル又は認可されていない変更があった場合には、正式に調査する。

12.2.1.8　予防又は定常作業として、コンピュータ及び媒体を走査（scan）するために、マルウェアの検出・修復ソフトウェアの導入及び定めに従った更新として、以下の３点を行う。

１．ネットワーク経由又は何らかの形式の記憶媒体を通じて入手した全てのファイルに対する、マルウェア検出のための使用前の走査

２．電子メールの添付ファイル及びダウンロードしたファイルに対する、マルウェア検出のための使用前の走査。この走査は、様々な場所（例えば、電子メールサーバ、デスクトップコンピュータ、組織のネットワークの入口）で実施する。

３．ウェブページに対するマルウェア検出のための走査

12.2.1.9　システムにおけるマルウェアからの保護、保護策の利用方法に関する訓練、マルウェアの攻撃の報告及びマルウェアの攻撃からの回復に関する手順及び責任を明確にする。

12.2.1.10　マルウェアの攻撃から回復するための適切な事業継続計画を策定する。

12.2.1.11　マルウェアの攻撃から回復するための適切な事業継続計画には、必要な全てのデータ及びソフトウェアの、バックアップ及び回復の手順を含める。

12.2.1.12　常に情報を収集するための手順を実施（例えば、新種のマルウェアに関する情報を提供するメーリングリストへの登録又はウェブサイトの確認）する。

12.2.1.13　マルウェアに関する情報を確認し、警告情報が正確かつ役立つことを確実にするための以下の２つの手順を実施する。

１．管理者は、単なるいたずらと真のマルウェアとを識別するために、適切な情報源（例えば、定評のある刊行物、信頼できるインターネットサイト、マルウェアの対策ソフトウェア供給者）の利用を確実にする仕組みを整備する。

２．管理者は、マルウェアではなく、いたずらの問題及びそれらを受け取ったときの対応について、全ての利用者に認識させる仕組みを整備する。

12.2.1.14　壊滅的な影響が及ぶ可能性のある環境を隔離する。