8a-8.6.8　容量・能力を増強するには、次の事項を考慮する。
ａ）新しい要員を雇用する。
ｂ）新しい施設又は場所を取得する。
ｃ）より強力な処理システム、メモリ及びストレージを取得する。
ｄ）容量・能力の課題に直接に応えるという特性があるクラウドコンピューティングを利用する。クラウドコンピューティングは、特定のアプリケーション及びサービスで利用できる資源を要求に応じて迅速に拡張し、削減することを可能とする、弾力性及びスケーラビリティをもっている。

8a-8.6.9　組織の資源に関する需要を減らすために、次の事項を考慮する。
ａ）古いデータの削除（ディスクスペース）
ｂ）保持期間を満了したハードコピー記録の処分（棚スペースを空ける。）
ｃ）アプリケーション、システム、データベース又は環境の廃止
ｄ）バッチのプロセス及びスケジュールの最適化
ｅ）アプリケーションコード及びデータベースへの問合せの最適化
ｆ）重要でない場合、大量の帯域を必要とするサービスに対する帯域割当ての拒否又は制限

8a-8.6.10　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。

8b　情報資産運用に関する管理

8b-8.7　マルウェアに対する保護

管理策：マルウェアに対する保護を実施し、利用者の適切な認識によって支援する。

目的：　情報及びその他の関連資産をマルウェアに対して保護することを確実にするため。

詳細管理策

8b-8.7.1　マルウェアに対する保護は、マルウェアの検出・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く。

（8b-8.7.1参考）　通常、マルウェアの検出・修復ソフトウェアを単独で使用することは十分ではない。

8b-8.7.2　マルウェアに対する保護については、次の手引を考慮する。
ａ）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規則及び管理策の実施
ｂ）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の実施
ｃ）マルウェアに付け込まれる可能性のあるぜい弱性を減らす。
ｄ）システム、特に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について、定常的な自動化された妥当性確認の実施。承認されていないファイル又は認可されていない変更の存在を調査する。
ｅ）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に対する保護対策を確立する。
ｆ）コンピュータ及び電子記憶媒体をスキャンするための、マルウェアの検出・修復ソフトウェアの導入及び定常的な更新。次の事項を含む定常的なスキャンを実施する。
1）ネットワーク経由又は何らかの形式の電子記憶媒体を通じて入手した全てのデータに対する、マルウェア検出のための使用前のスキャン
2）電子メール及びインスタントメッセージング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スキャン。このスキャンは、様々な場所で、及び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アクセスの際のマルウェア検出のためのスキャン
ｇ）リスクアセスメントの結果に基づき、かつ、次の事項を考慮して、マルウェアの検出・修復ツールの配置及び構成を決定する。
1）特に効果的である場合には、多層防御の原則。例えば、これはネットワークゲートウェイ、並びに利用者エンドポイント機器及びサーバにおいて、マルウェアの検出につながる可能性がある。
2）攻撃者がマルウェアを送り込むための回避技術、又はマルウェアの送信における暗号化プロトコルの使用
ｈ）マルウェアに対する通常の管理策をう（迂）回する可能性がある、保守及び緊急時の手順中におけるマルウェアの入り込みの防止に注意を払う。
ｉ）例外承認権限、文書化した正当性の提示、及びレビューの日付を含む、マルウェアに対する一部又は全ての対策の一時的又は恒久的な無効化を認可するプロセスを実装する。これは、マルウェアに対する保護によって通常の運用が中断・阻害される場合に必要になる可能性がある。
ｊ）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の策定。これには、必要な全てのデータ及びソフトウェアのバックアップ（オンラインとオフラインとの両方のバックアップを含む。）並びに回復の対策を含める。
ｋ）壊滅的な影響が生じる可能性のある環境の隔離
ｌ）システム上でマルウェアに対する保護を扱う手順及び責任の定義。これには、手順の使用、報告及びマルウェア攻撃からの回復に関する訓練を含む。
ｍ）マルウェアに感染した電子メール、ファイル又はプログラムの受信、送信又はインストールを特定し、可能ならば軽減する方法について、全ての利用者に意識向上又は訓練を提供する。
ｎ）定常的に新種のマルウェアに関する情報を収集するための手順の実施
ｏ）警告情報などマルウェアに関する情報が適格で定評のある情報源から来ており、正確かつ役立つことを検証する。