d）対応する全てのプログラムソースライブラリを更新する。
e）全ての運用ソフトウェアの管理を維持するために、システム文書の管理と同様に、構成管理システムを利用する。
f）変更を実装する前に、ロールバック計画を定める。
g）運用ソフトウェアの更新の全てについて、監査ログを維持する。
h）ソフトウェアの旧版は、緊急時対応の手段として、及び保管しているデータをそのソフトウェアで読み込む又は処理する必要がある間は、全ての必要な情報及びパラメータ、手順、設定の詳細並びにサポートソフトウェアとともに保管しておく。

8b-8.19.2　新リリースにアップグレードするとの決定には、その変更に対する事業上の要求及びそのリリースのセキュリティを考慮に入れる。

8b-8.19.3　情報セキュリティ上のぜい弱性を除去するか、又は低減するために役立つ場合には、ソフトウェアパッチを適用する。

8b-8.19.4　外部から供給されるソフトウェア及びパッケージに依存するソフトウェアは、情報セキュリティのぜい弱性をもたらす可能性があるため、認可されていない変更を回避するために監視し、管理する。

8b-8.19.5　運用システムで利用するソフトウェアの版を、ソフトウェア業者(供給者）がサポートする版に維持する。

8b-8.19.6　組織は、サポートのないソフトウェアに依存することのリスクを考慮する。

(8b-8.19.6参考)　ソフトウェア業者は、徐々に古い版のソフトウェアのサポートを中止する。

8b-8.19.7　運用システムで使用するオープンソースソフトウェアは、最新で適切なリリースの使用を維持する。

(8b-8.19.7参考)　時間の経過とともに、オープンソースコードが維持されなくなるにもかかわらず、オープンソースソフトウェアリポジトリで引き続き利用できる場合がある。

8b-8.19.8　組織は、運用システムで使用する場合、保守がなされないオープンソースソフトウェアに依存するリスクも考慮する。

8b-8.19.9　供給者がソフトウェアの導入又は更新に関与する場合、物理的又は論理的アクセスは、必要なときに、適切な認可を得た場合にだけ許可する。

8b-8.19.10　供給者の活動を監視する。

8b-8.19.11　組織は、利用者が導入できるソフトウェアの種類について、厳密な規則を定め、施行する。

8b-8.19.12　特権の許可は最小限にするという原則を、運用システムへのソフトウェアの導入に適用する。

8b-8.19.13　組織は、ソフトウェアのインストールの種類のうち、許可するもの、及び禁止するものを特定する。

8b-8.19.14　特権は、利用者の役割に基づいて付与する。

8c　情報システムの適正利用の管理

8c-8.20　ネットワークセキュリティ

管理策：システム及びアプリケーション内の情報を保護するために、ネットワーク及びネットワーク装置のセキュリティを保ち、管理し、制御する。

目的：　ネットワーク及びそれを支援する情報処理設備において、情報をネットワークを通じた侵害から保護するため。

詳細管理策

8c-8.20.1　ネットワークにおける情報のセキュリティを確実にし､接続したネットワークサービスを認可されていないアクセスから保護するために、管理策を実施する。

8c-8.20.2　ネットワークセキュリティの管理策では、特に、次の事項を考慮する。

a）ネットワークごとに、扱ってよい情報の種類及び分類レベル
b）ネットワーク装置及び機器の管理に関する責任及び手順を確立する。
c）ネットワーク図及び装置・機器の構成ファイルを含む最新の文書を維持する。
d）適切な場合には、ネットワークの運用責任は、ＩＣＴシステムの運用から分離する。
e）公衆ネットワーク、第三者ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及びアプリケーションを保護するために、管理策を確立する。
f）情報セキュリティに影響を及ぼす可能性のある行動、又は情報セキュリティに関係のある行動の記録及び検知ができるように、適切なログを取得し、監視する。
g）組織に対するサービスを最適にするため、また、管理策を情報処理基盤全体に一貫して適用することを確実にするために、様々なネットワーク管理作業を綿密に調整する。
h）ネットワーク上のシステムを認証する。
i）ネットワークへのシステムの接続を制限し、フィルタリングする。
j）ネットワークへの装置及び機器の接続を検出し、制限し、認証する。
k）ネットワーク装置・機器の要塞化（hardening）
l）ネットワーク管理の経路を他のネットワークトラフィックから分離する。
m）ネットワークが攻撃を受けた場合、重要なサブネットワークを一時的に分離する。
n）ぜい弱なネットワークプロトコルを無効化する。

8c-8.20.3　組織は、仮想化ネットワークの使用に、適切なセキュリティ管理策を適用することを確実にする。

(8c-8.20.3参考１)　仮想化ネットワークには、ソフトウェア定義ネットワーク（ＳＤＮ、ＳＤ-ＷＡＮ）も含む。

(8c-8.20.3参考２)　仮想化ネットワークは、物理的ネットワーク上での通信の論理的分離を可能にすることから、セキュリティの観点で望ましい場合があり、特に分散型コンピューティングを用いて実装したシステム及びアプリケーションにおいてこのことが該当する。