8b-8.16.5　監視ツールによる継続的監視を使用し、次の事項を考慮する。
a）監視は、組織のニーズ及び能力に応じて、リアルタイム又は定期的な間隔で行う。
b）大量のデータを取り扱い、常に変化する脅威の状況に適応し、リアルタイムで通知することを可能にする機能をもつ監視ツールを利用する。
c）特定のシグネチャ及びデータ、又はネットワーク若しくはアプリケーションの動作パターンも認識できる監視ツールを利用する。

8b-8.16.6　自動監視ソフトウェアは、あらかじめ定めたしきい値に基づいて警告を発するように構成する。

8b-8.16.7　警告システムは、誤検出を最小限にするために、組織の基準に合わせて調整し、学習させる。

8b-8.16.8　要員は警告への対応に専念させることが望ましく、インシデントの可能性がある事象を正確に判定できるように適切に訓練を受けさせる。

8b-8.16.9　警告通知を受信し、対応するための冗長性のあるシステム及びプロセスを備える。

8b-8.16.10　監査、セキュリティ評価、ぜい弱性スキャン及び監視を改善するために、異常な事象を関係者に伝達する。

8b-8.16.11　情報セキュリティに対する有害な事象の影響を最小にするために、その存在を示す監視システムからの通知に時機を失せず対応する手順を確立する。

8b-8.16.12　将来の誤検出の数を減らすために監視ソフトウェアを調整するなど、誤検出を特定し、対処する手順も確立する。

8b-8.17　クロックの同期

管理策：組織が使用する情報処理システムのクロックは、組織が採用した時刻源と同期させる。

目的：　セキュリティ関連の事象及びその他の記録されたデータの関係付け及び分析を可能にし、情報セキュリティインシデントの調査を支援するため。

詳細管理策

8b-8.17.1　時刻の表現、信頼できる同期及び正確さに関する、外部及び内部の要求事項は、文書化し、実装する。

（8b-8.17.1参考）　この要求事項は、法令、規制、契約、標準及び内部監視のニーズに由来する可能性がある。

8b-8.17.2　ビル管理システム、入退出システム、及び調査を支援するために使用できるその他のシステムを含む全てのシステムに対して、組織内で基準とする時刻源を考慮して定める。

8b-8.17.3　国の原子時計又は全地球測位システム（ＧＰＳ）から配信される時刻に基づくクロックを、ログ取得システムの基準クロック、すなわち、正確なタイムスタンプを確実にする一貫性のある信頼できる日付及び時刻源として使用する。

8b-8.17.4　ネットワークで接続された全てのシステムを基準クロックと同期させるために、ネットワークタイムプロトコル（ＮＴＰ）又は高精度タイムプロトコル（ＰＴＰ）などのプロトコルを使用する。

（8b-8.17.4参考）　組織は、外部クロックの信頼性を改善し、変動を適切に管理するために、二つの外部時刻源を同時に使用することが可能である。

8b-8.17.5　クラウドサービスの利用によりクロックの同期が困難となる場合、不一致から生じるリスクを軽減するために、各サービスのクロックを監視し、差を記録する。

（8b-8.17.5参考）　複数のクラウドサービスを使用する場合、又はクラウドサービス及びオンプレミスサービスの両方を使用する場合には、クロックの同期が困難なことがある。

8b-8.18　特権的なユーティリティプログラムの使用

管理策：システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。

目的：　ユーティリティプログラムの使用が、システム及びアプリケーションについての情報セキュリティ管理策に害を与えないことを確実にするため。

詳細管理策

8b-8.18.1　システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。
a）可能な限り少人数の信頼できる認可された利用者だけに限定した、ユーティリティプログラムの使用制限
b）ユーティリティプログラムを使用する要員の一意の識別を含む、ユーティリティプログラムの識別、認証及び認可手順の使用
c）ユーティリティプログラムの認可レベルの明確化及び文書化
d）ユーティリティプログラムを臨時に用いる場合の認可
e）権限の分離が必要な場合に、システム上のアプリケーションにアクセスする利用者に、ユーティリティプログラムの使用を不可とする
f）全ての不要なユーティリティプログラムの除去又は無効化
g）少なくとも、アプリケーションソフトウェアからのユーティリティプログラムの論理的分離。実施できる場合、ユーティリティプログラムのネットワーク通信をアプリケーショントラフィックから分離
h）ユーティリティプログラムの使用の制限
i）ユーティリティプログラムの全ての使用に関するログ

8b-8.19　運用システムへのソフトウェアの導入

管理策：運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順及び対策を実施する。

目的：　運用システムの完全性の維持を確実にし、技術的ぜい弱性の悪用を防止するため。

詳細管理策

8b-8.19.1　運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。
a）運用ソフトウェアの更新は、適切な管理層の認可に基づき、訓練された実務管理者だけが実施する。
b）運用システムには、承認された実行可能なコードだけを導入し、開発用コード又はコンパイラは一切導入しないことを確実にする。
c）ソフトウェアは、十分なテストに成功した後に導入し、更新する。