8b-8.15.7　管理策は、次の事項を含む、ログ情報の認可されていない変更及びログ取得機能の運用上の問題から保護することを目指す。
a）記録されたメッセージ形式の変更
b）ログファイルの編集又は削除
c）ログファイルを保持している記憶媒体の記録容量を超過した場合のイベント記録の不具合又は過去のイベント記録への上書き

8b-8.15.8　ログは保護することとし、その手法として、次の使用を考慮する。
a）暗号技術によるハッシュ化
b）追加専用及び読取り専用ファイルへの記録
c）公開透明性ファイルへの記録

（8b-8.15.8参考）　ログは、データ保持に関する要求事項、又は証拠の収集及び保持のための要求事項によって、保存が求められる場合がある。

8b-8.15.9　組織がエラーのデバッグ又はトラブルシューティングを支援するために、システム又はアプリケーションのログを業者に送信する必要がある場合、利用者名、インターネットプロトコル、ＩＰアドレス、ホスト名、組織名などの情報について、業者に送信する前に、可能な場合はデータマスキング手法を使用してログの非識別化を行う。

8b-8.15.10　イベントログは、取扱いに慎重を要するデータ及びＰＩＩを含む可能性があるため、適切なプライバシー保護対策を講じる。

【ログ分析】

8b-8.15.11　ログ分析は、侵害の可能性がある通常とは異なる活動又は異常な挙動を特定する助けとなるように、情報セキュリティ事象の分析及び解釈を含む。

8b-8.15.12　事象の分析は、次の事項を考慮して実施する。
a）分析を実施する専門家に必要な技能
b）ログ分析の手順の決定
c）各セキュリティ関連事象の必要な属性
d）既定の規則の使用を通じて特定される例外事象
e）異常な活動及び挙動と比較する利用者及びエンティティの挙動分析（ＵＥＢＡ）、既知の挙動パターン及び標準ネットワークトラフィック
f）傾向分析又はパターン分析の結果
g）利用可能な脅威インテリジェンス

8b-8.15.13　ログ分析は、次の事項を含む、異常な挙動を特定し、分析する助けとなる監視活動によって支援する。
a）保護された資源への成功及び失敗したアクセスの試みをレビューする。
b）ボットネットのコマンドアンドコントロールサーバ（以下、Ｃ＆Ｃサーバと表す。）への接続のような、悪意のあるサーバへのアウトバウンドネットワーク接続を特定するために、ＤＮＳログを確認する。
c）システム及びネットワーク内の異常な活動に関するサービス提供者からの使用状況報告を調べる。
d）より正確な検知及びインシデント分析を確実にするために、入口、出口などの物理的監視のイベントログを含める。
e）効率的で非常に正確な分析を行えるように、ログを相互に関係付ける。

8b-8.15.14　情報セキュリティインシデントの疑い、及び実際の情報セキュリティインシデントを特定し、更なる調査を行う。

8b-8.16　監視活動

管理策：情報セキュリティインシデントの可能性を評価するために、ネットワーク、システム及びアプリケーションについて異常な挙動がないか監視し、適切な処置を講じる。

目的：　異常な挙動及び情報セキュリティインシデントの可能性を検出するため。

詳細管理策

8b-8.16.1　監視のために、次の事項を行う。
a）監視の範囲及びレベルは、業務及び情報セキュリティの要求事項に従い、関連する法令及び規制を考慮して決定する。
b）監視を記録する。
c）監視記録は、定めた保持期間にわたって維持する。

8b-8.16.2　監視システムに含めるものとして、次の事項を考慮する。
a）アウトバウンド及びインバウンドの、ネットワーク、システム及びアプリケーションのトラフィック
b）システム、サーバ、ネットワーク装置、監視システム、重要なアプリケーションなどへのアクセス
c）重要な又は実務管理者が扱うシステム及びネットワークの構成ファイル
d）セキュリティツールからのログ
e）システム及びネットワークの活動に関するイベントログ
f）実行しているコードがそのシステムでの実行を認可されていること、及びそれが改ざんされていないことの確認
g）資源の使用及びそれらの動作状況

8b-8.16.3　組織は、正常な挙動の基準を確立し、この基準に照らして異常を監視する。基準を確立する場合、次の事項を考慮する。
a）通常時及びピーク時のシステムの使用率
b）各利用者又は利用者グループの通常のアクセス時間、アクセスの場所、アクセスの頻度

8b-8.16.4　監視システムは、次のような異常な挙動を特定するために、確立した基準に照らして構成する。
a）プロセス又はアプリケーションの計画外の終了
b）既知の悪意のあるＩＰアドレス又はネットワークドメインから送信されるマルウェア又はトラフィックに典型的に伴う挙動
c）既知の攻撃の特性
d）異常なシステム動作
e）ボトルネック及び過負荷
f）システム又は情報への認可されていないアクセス又はその試み
g）業務アプリケーション、システム及びネットワークの認可されていないスキャン
h）保護された資源への成功及び失敗したアクセスの試み
i）想定される挙動に対して、利用者及びシステムの異常な挙動