5a-5.7.3　脅威インテリジェンスは、次の事項を満たす。
a）課題に応える（すなわち、組織の保護に関係する。）。
b）十分な情報を含む（すなわち、脅威の状況に関する正確かつ詳細な理解を組織に提供する。）。
c）状況認識を与えるような状況情報を含む（すなわち、事象の発生時間、場所、以前の経験及び同様の組織における傾向によって、情報に状況を加える。）。
d）対応可能である（すなわち、組織が情報に基づいて迅速かつ効果的に対応可能である。）。

5a-5.7.4　脅威インテリジェンス活動は、次の事項を含む。
a）脅威インテリジェンスの構築の目的を確立する。
b）脅威インテリジェンスの構築に必要な情報を提供するのに必要かつ適切な内部及び外部の情報源を特定し、吟味し、選択する。
c）内部及び外部のいずれかによらず、精選した情報源から情報を収集する。
d）収集した情報を、分析に備えて処理する。
e）情報を、それが組織にどのように関係し、意味をもつかを理解するために分析する。
f）関係する個人に分析した結果を理解可能な形式で伝達し、共有する。

5a-5.7.5　脅威インテリジェンスを分析し、次のとおりに使用する。
a）脅威インテリジェンスの情報源から収集した情報を組織の情報セキュリティリスクマネジメントプロセスに含めるプロセスを実施することによって。
b）ファイアウォール、侵入検知システム、マルウェア対策ソリューションなどの技術的な予防及び検知の管理策への追加の入力として。
c）情報セキュリティテストのプロセス及び手法への入力として。

5a-5.7.6　組織は、脅威インテリジェンス全体を改善するために、脅威インテリジェンスを他の組織と相互に共有する。

5a-5.8　プロジェクトマネジメントにおける情報セキュリティ

管理策：情報セキュリティをプロジェクトマネジメントに組み入れる。

目的：　プロジェクトのライフサイクル全体を通して、プロジェクトマネジメントにおいて、プロジェクト及び成果物に関連する情報セキュリティリスクに効果的に対処することを確実にするため。

詳細管理策

5a-5.8.1　プロジェクトマネジメントの一部として情報セキュリティリスクに対処することを確実にするために、情報セキュリティをプロジェクトマネジメントに組み入れる。

（5a-5.8.1参考）　これは、プロジェクトの複雑さ、規模、期間、分野又は適用領域にかかわらず、あらゆる種類のプロジェクトに適用可能である。

5a-5.8.2　用いるプロジェクトマネジメントでは、次の事項を要求する。
a）情報セキュリティリスクを、プロジェクトリスクの一部として、プロジェクトのライフサイクル全体を通じて、早い段階で及び定期的にリスクアセスメント及びリスク対応を実施する。
b）情報セキュリティ要求事項には、プロジェクトの早い段階で対処する。
c）内部及び外部への伝達の側面のセキュリティなど、プロジェクトの実行に伴う情報セキュリティリスクを、プロジェクトのライフサイクル全体を通じて考慮し、処理する。
d）情報セキュリティリスク対応の進捗状況をレビューし、対応の有効性を評価及び試験する。

5a-5.8.3　情報セキュリティの考慮及び活動の適切性は、あらかじめ定めた段階において、適切な人物又はプロジェクト運営委員会などのガバナンス機関がフォローアップする。

5a-5.8.4　プロジェクトに関連する情報セキュリティの責任及び権限を定義し、規定された役割に割り当てる。

5a-5.8.5　プロジェクトが提供する製品又はサービスの情報セキュリティ要求事項は、情報セキュリティ方針、トピック固有の方針及び規制から順守すべき要求事項を導出することを含む、様々な方法を用いて決定する。

5a-5.8.6　プロジェクトが提供する製品又はサービスの情報セキュリティ要求事項は、脅威のモデリング、インシデントのレビュー、ぜい弱性の深刻度の使用、緊急時対応計画策定などの活動から導き出すことができ、それによって、情報システムのアーキテクチャ及び設計を運用環境における既知の脅威から保護することを確実にする。

5a-5.8.7　情報セキュリティ要求事項は、ＩＣＴ開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。
a）どのような情報が関係するか（情報の決定）、それに対応する情報セキュリティのニーズは何か、及び適切なセキュリティの欠如から生じる可能性のある事業への潜在的な悪影響
b）特に機密性、完全性及び可用性の観点から、関係する情報及びその他の関連資産に必要な保護のニーズ
c）認証の要求事項を導き出すための、エンティティが提示する識別情報に求める信頼又は保証のレベル
d）顧客及びその他の潜在的な業務上の利用者のほか、関係するプロジェクトメンバ、潜在的な運用スタッフ、外部供給者などの特権をもつ、又は技術をもつ利用者に対する、アクセスの提供及び認可のプロセス
e）利用者に対する、各自の義務及び責任の通知
f）トランザクションのログ取得及び監視、並びに否認防止の要求事項のような、業務プロセスに由来する要求事項
g）他の情報セキュリティ管理策によって必要になる要求事項
h）組織の活動に適用される法令、規制及び契約上の条件の順守
i）第三者との合意又は契約における関連セキュリティ箇条を含む、組織の情報セキュリティ方針及びトピック固有の方針を満たす上で必要な、第三者に求める信頼又は保証のレベル