c）トランザクション情報の紛失又は重複の防止
d）トランザクションの詳細を、公開している環境の外で保管すること
e）信頼できる専門機関を利用する場合、エンドツーエンドの証明書又は署名管理プロセスを通じたセキュリティの統合及び組込み

(8d-8.26参考)　これらの考慮事項の幾つかは、法的要求事項を考慮に入れながら、暗号を適用することによって対応することが可能である。

8d-8.27　セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則

管理策：セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの開発活動に対して適用する。

目的：　情報システムを、開発のライフサイクルにおいてセキュリティに配慮して設計し、実装し、運用することを確実にするため。

詳細管理策

8d-8.27.1　セキュリティに配慮したシステム構築の原則を確立し、文書化し、情報システム構築活動に適用する。

8d-8.27.2　セキュリティは、全てのアーキテクチャ層（業務、データ、アプリケーション及び技術）において設計する。新技術は、セキュリティのリスクを分析し、その設計を既知の攻撃パターンに照らしてレビューする。

(8d-8.27参考)　セキュリティに配慮したシステム構築の原則は、利用者認証技術、セキュリティを保ったセッション管理及びデータの妥当性確認並びにサニタイジングに関する詳細管理策となる。

8d-8.27.3　セキュリティに配慮したシステム構築の原則には、次の分析を含める。
a）特定した脅威から情報及びシステムを保護するために必要なあらゆるセキュリティ管理策
b）セキュリティ事象を防止し、検知し又はそれに対応するセキュリティ管理策の機能
c）特定の業務プロセスに必要な特定のセキュリティ管理策
d）セキュリティ管理策をどこでどのように適用するか。
e）個々のセキュリティ管理策（手動及び自動）を連携し、統合した管理策群を作る方法

8d-8.27.4　セキュリティに配慮したシステム構築の原則では、次の事項を考慮に入れる。
a）セキュリティアーキテクチャと統合する必要性
b）技術的なセキュリティ基盤
c）選択した技術を開発し、サポートする組織の能力
d）セキュリティ要求事項を満たすための費用、時間及び複雑さ
e）最新の優れた慣行

8d-8.27.5　セキュリティに配慮したシステム構築には、次の事項を含める。
a）“設計によるセキュリティ（セキュリティバイデザイン）”、“多層防御”、“デフォルトでのセキュリティ”、“デフォルト拒否”、“故障時のセキュリティ”、“外部アプリケーションからの入力を信用しない”、“導入時のセキュリティ”、“違反の想定”、“最小特権”、“利便性及び管理性”、“最小機能”などの、セキュリティアーキテクチャの原則の使用
b）情報セキュリティのぜい弱性を特定し、セキュリティ管理策を規定することを確実にし、セキュリティ要求事項を満たす助けとなる、セキュリティ指向の設計レビュー
c）要求事項を完全には満たしていないセキュリティ管理策の文書化及び正式な承認
d）システムの要塞化（hardening）

8d-8.27.6　組織は、次のような“ゼロトラスト(zero trust)”の原則を考慮する。
a）組織の情報システムは既に侵害されていることを想定し、ネットワーク境界のセキュリティだけに依存しない。
b）情報システムへのアクセスにおいて“決して信頼せず、常に検証する”取組を採用する。
c）情報システムへの要求がエンドツーエンドで暗号化されることを確実にする。
d）情報システムへの各要求を、組織の内部からのものであっても、公開の外部ネットワークから来たかのように検証する(すなわち、組織の境界の内側又は外側のいずれであれ、自動的に信頼することはしない。)。
e）“最小特権”及び動的アクセス制御手法を使用する。これは、情報又はシステムへの要求の認証及び認可を、認証情報、利用者識別情報、利用者エンドポイント機器に関するデータ、データ分類などの、状況に関する情報に基づいて行うことを含む。
f）認証情報及び利用者識別情報、利用者エンドポイント機器に関するデータ、並びにデータ分類を含めた情報に基づいて、例えば、強力な認証を実行することによって、情報システムへの要求を常に認証し、認可要求の妥当性を常に確認する。

8d-8.27.7　確立したセキュリティに配慮したシステム構築の原則は、該当する場合には、組織と組織が外部委託した供給者との間の、契約及び拘束力をもつその他の合意を通じて、外部委託した情報システムの開発にも適用する。

8d-8.27.8　組織は、供給者のセキュリティに配慮したシステム構築の行為が組織のニーズと一致することを確実にする。

8d-8.27.9　セキュリティに配慮したシステム構築の原則及び確立した構築手順は、構築プロセスにおけるセキュリティレベルの向上に有効に寄与していることを確実にするために、定期的にレビューする。

8d-8.27.10　セキュリティに配慮したシステム構築の原則及び確立した構築手順が、新規の潜在的な脅威に対抗するという点で常に最新であること、及び適用される技術及びソリューションの進展に継続して適用可能であることを確実にするために、定期的にレビューする。

8d-8.28　セキュリティに配慮したコーディング

管理策：セキュリティに配慮したコーディングの原則をソフトウェア開発に適用する。

目的：　ソフトウェアをセキュリティに配慮して作成し、それによってソフトウェアの潜在的な情報セキュリティのぜい弱性の数を減らすことを確実にするため。

詳細管理策

【セキュリティに配慮したコーディング全般】

8d-8.28.1　組織は、セキュリティに配慮したコーディングに関して優れたガバナンスを実現する、組織全体のプロセスを確立する。