14.1.1.2　情報セキュリティ要求事項の特定作業の結果は、文書化し、全ての利害関係者によってレビューする。
14.1.1.3　情報セキュリティ要求事項及び情報セキュリティ管理策には、関連する情報の業務上の価値、及びセキュリティが不十分だった場合に業務に及ぶ可能性のある悪影響を反映する。
14.1.1.4　情報セキュリティ要求事項及び関連するプロセスの特定及び管理は、情報システムプロジェクトにその初期段階で統合する。
14.1.1.5　情報セキュリティ要求事項においては、利用者認証の要求事項を導き出すために、利用者が提示する識別情報に対して求める信頼のレベルを定める。
14.1.1.6　情報セキュリティ要求事項においては、業務上の利用者のほか、特権を与えられた利用者及び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を定める。
14.1.1.7　情報セキュリティ要求事項においては、利用者及び運用担当者に対する、各自の義務及び責任の通知を明確にする。
14.1.1.8　情報セキュリティ要求事項においては、関連する資産の保護の要求、特に、可用性、機密性及び完全性に関する保護の要求を明確にする。
14.1.1.9　情報セキュリティ要求事項においては、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を定める。
14.1.1.10　情報セキュリティ要求事項においては、他のセキュリティ管理策によって義務付けられる要求事項を定める（例えば、ログ取得及び監視のインターフェース、情報漏えい検知システム）。
14.1.1.11　公衆ネットワークを介してサービスを提供するアプリケーション、又はトランザクションを実施するアプリケーションについては、14.1.2及び14.1.3の管理策を考慮して決定する。
14.1.1.12　製品を入手する際には、正式な試験及び調達プロセスに従う。
14.1.1.13　製品の供給者との契約は、明確にされたセキュリティ要求事項を規定する。
14.1.1.14　提案された製品のセキュリティの機能性が指定された要求を満たさない場合は、発生するリスク及び関連する管理策を、製品を購入する前に再考する。
14.1.1.15　当該システムにおいて稼働するソフトウェア及びサービスと整合する製品のセキュリティ構成に関して、入手可能な手引を用いて、これを評価し、実施する。
14.1.1.16　製品を受け入れる基準は、特定したセキュリティ要求事項を満たすことの確証を与える機能の観点で定める。
14.1.1.17　製品は、入手する前に製品を受け入れる基準に照らして評価する。
14.1.1.18　機能の追加によって、許容できない追加のリスクを取り込まないことを確実にするために、レビューする。
14.1.2　公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護する。
14.1.2.1　公衆ネットワークを経由するアプリケーションサービスは、各当事者が提示する自らの識別情報について、それぞれが互いに要求し合う信頼（例えば、認証）のレベルを定める。
14.1.2.2　公衆ネットワークを経由するアプリケーションサービスは、重要な取引文書の内容の承認、その発行、及びその文書への署名を誰が行うかについての認可プロセスを明確にする。
14.1.2.3　公衆ネットワークを経由するアプリケーションサービスは、サービスの提供又は利用が認可されていることを通信業者に十分に通知していることを確実にする仕組みを整備する。
14.1.2.4　公衆ネットワークを経由するアプリケーションサービスは、入札手続、契約手続などにおいて、重要な文書の機密性、完全性及び発送・受領の証明、並びに契約の否認防止に関する要求事項を決定し、それを達成する。
14.1.2.5　公衆ネットワークを経由するアプリケーションサービスは、重要な文書の完全性についての、信頼のレベルを定める。
14.1.2.6　公衆ネットワークを経由するアプリケーションサービスは、秘密情報の保護に関する要求事項を定める。
14.1.2.7　公衆ネットワークを経由するアプリケーションサービスは、注文のトランザクション、支払い情報、納入先の宛名情報及び受領確認の機密性及び完全性を維持する。
14.1.2.8　公衆ネットワークを経由するアプリケーションサービスは、顧客から提供された支払い情報を検証するための、適切な検査の度合いを定める。
14.1.2.9　公衆ネットワークを経由するアプリケーションサービスは、不正行為を防ぐための、最も適切な支払いの決済形式を選択する。
14.1.2.10　公衆ネットワークを経由するアプリケーションサービスは、注文情報の機密性及び完全性を維持するために要求される保護のレベルを定める。
14.1.2.11　公衆ネットワークを経由するアプリケーションサービスは、トランザクション情報の紛失又は重複を防止する。
14.1.2.12　公衆ネットワークを経由するアプリケーションサービスは、不正なトランザクションに関する賠償義務を明確にする。
14.1.2.13　公衆ネットワークを経由するアプリケーションサービスは、保険の要件を決定する。
14.1.2.14　アプリケーションサービスに関する当事者間の取決めは、権限の詳細も含め、合意したサービス条件を両当事者に義務付ける合意書によって裏付ける。
14.1.2.15　攻撃に対する対応力（resilience）の要求事項（関連するアプリケーションサーバを保護するための要求事項、及びサービスの提供に必要となるネットワーク相互接続の可用性を確実にするための要求事項を含む。）を定める。
14.1.3　アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護する。
・不完全な通信
・誤った通信経路設定
・認可されていないメッセージの変更
・認可されていない開示
・認可されていないメッセージの複製又は再生
14.1.3.1　アプリケーションサービスのトランザクションでは、トランザクションに関わる各当事者による電子署名を利用する。
14.1.3.2　アプリケーションサービスのトランザクションでは、トランザクションの種々の面において、以下を確実にする仕組みを整備する。
１．全ての当事者の秘密認証情報は、有効であり、かつ、検証を経ている。
２．トランザクションが秘密に保たれている。
３．全ての当事者に関係するプライバシーを守っている。
14.1.3.3　アプリケーションサービスのトランザクションでは、関わる全ての当事者間の通信経路を暗号化する。
14.1.3.4　アプリケーションサービスのトランザクションでは、関わる全ての当事者間で使われる通信プロトコルのセキュリティを維持する。