13.2.1.11　情報転送のために通信設備を利用するときに従う手順及び管理策には、ファクシミリ又はそのサービスの利用に伴う問題（ファクシミリの受信文の取出し装置への認可されていないアクセス、特定の番号にメッセージを送る故意又は偶然のプログラミング、誤ダイアル、又は間違って記憶した番号を用いることによる、誤った番号への文書及びメッセージの送付）について要員に意識させることを含める。

13.2.1.12　公共の場所、並びにセキュリティが確保されていない通信経路、出入りが自由なオフィス及び会議室では、秘密の会話はしないほうがよいことを要員に意識させる。

13.2.1.13　情報転送サービスは、関連するいかなる法的要求事項についても順守する。

13.2.2　合意では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱う。

13.2.2.1　情報転送に関する合意に、送信、発送及び受領についての管理及び通知を行う責任を含める。

13.2.2.2　情報転送に関する合意に、追跡可能性及び否認防止を確実にするための手順を含める。

13.2.2.3　情報転送に関する合意に、こん（梱）包及び送信に関する必要最小限の技術標準を含める。

13.2.2.4　情報転送に関する合意に、預託条項を含める。

13.2.2.5　情報転送に関する合意に、運送業者を確認する規準を含める。

13.2.2.6　情報転送に関する合意に、情報セキュリティインシデントが発生した場合（例えば、データの紛失）の責任及び賠償義務を含める。

13.2.2.7　情報転送に関する合意に、取扱いに慎重を要する又は重要な情報に対する、合意されたラベル付けシステム（ラベルの意味を直ちに理解すること、及び情報を適切に保護することを確実にするもの。）の使用を含める。

13.2.2.8　情報転送に関する合意に、情報及びソフトウェアの記録及び読出しに関する技術標準を含める。

13.2.2.9　情報転送に関する合意に、取扱いに慎重を要するもの（例えば、暗号鍵）を保護するために必要とされる、特別な管理策を含める。

13.2.2.10　情報転送に関する合意に、転送中の情報についての、管理状況の履歴の維持を含める。

13.2.2.11　情報転送に関する合意に、容認できるアクセス制御のレベルを含める。

13.2.2.12　情報転送に関する合意においては、転送中の情報及び物理的媒体を保護するための方針、手順及び標準類を確立及び維持し、参照する。

13.2.2.13　情報交換に関する、いかなる合意における情報セキュリティの事項も、関連する業務情報の取扱いに慎重を要する度合いを反映する。

13.2.3　電子的メッセージ通信に含まれた情報は、適切に保護する。

13.2.3.1　電子的メッセージ通信のための情報セキュリティでは、組織が採用している分類体系に従った、認可されていないアクセス、改ざん又はサービス妨害からのメッセージを保護する。

13.2.3.2　電子的メッセージ通信のための情報セキュリティでは、正しい送付先及びメッセージ送信を確実にする仕組みを整備する。

13.2.3.3　電子的メッセージ通信のための情報セキュリティでは、サービスの信頼性及び可用性を確保する。

13.2.3.4　電子的メッセージ通信のための情報セキュリティでは、法的考慮（例えば、電子署名のための要求事項）を含める。

13.2.3.5　電子的メッセージ通信のための情報セキュリティでは、誰でも使える外部サービス（例えば、インスタントメッセージ、ソーシャルネットワーク、ファイル共有）を利用する際の、事前承認を取得する。

13.2.3.6　電子的メッセージ通信のための情報セキュリティでは、公開されているネットワークからのアクセスを制御する、より強固な認証レベルを決定する。

13.2.4　情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューし、文書化する。

13.2.4.1　秘密保持契約又は守秘義務契約には、法的に強制できる表現を用いて、秘密情報を保護するための要求事項を取り上げる。

13.2.4.2　秘密保持契約又は守秘義務契約は、外部関係者又は組織の従業員に適用する。

13.2.4.3　秘密保持契約又は守秘義務契約の当事者の種類、並びに当事者に許可される秘密情報のアクセス及び取扱いを考慮して、契約の要素を選定又は追加する。

13.2.4.4　秘密保持契約又は守秘義務契約には、保護される情報の定義（例えば、秘密情報）を含める。

13.2.4.5　秘密保持契約又は守秘義務契約には、秘密を無期限に保持する場合も含めた、契約の有効期間を含める。

13.2.4.6　秘密保持契約又は守秘義務契約には、契約終了時に要求する処置を含める。

13.2.4.7　秘密保持契約又は守秘義務契約には、認可されていない情報開示を避けるための、署名者の責任及び行為を含める。

13.2.4.8　秘密保持契約又は守秘義務契約には、情報、企業秘密及び知的財産の所有権、並びにこれらの秘密情報の保護との関連を含める。

13.2.4.9　秘密保持契約又は守秘義務契約には、秘密情報の許可された利用範囲、及び情報を利用する署名者の権利を含める。

13.2.4.10　秘密保持契約又は守秘義務契約には、秘密情報に関する行為の監査及び監視の権利を含める。

13.2.4.11　秘密保持契約又は守秘義務契約には、認可されていない開示又は秘密情報漏えいの、通知及び報告のプロセスを含める。

13.2.4.12　秘密保持契約又は守秘義務契約には、契約終了時における情報の返却又は破棄に関する条件を含める。

13.2.4.13　秘密保持契約又は守秘義務契約には、契約違反が発生した場合にとるべき処置を含める。

13.2.4.14　組織の情報セキュリティ要求事項に応じて、秘密保持契約又は守秘義務契約に必要な要素を含める。

13.2.4.15　秘密保持契約又は守秘義務契約は、その法域において適用される法令及び規制の全てに従う。

13.2.4.16　秘密保持契約又は守秘義務契約に関する要求事項は、定期的に及びこれら要求に影響する変化が発生した場合に、レビューする。

14　システムの取得、開発及び保守

14.1　情報システムのセキュリティ要求事項

目的：ライフサイクル全体にわたって、情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには、公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。

14.1.1　情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含める。

14.1.1.1　情報セキュリティ要求事項は、方針及び規則に由来する順守の要求事項、脅威のモデリング、インシデントのレビュー、又はぜい弱性の限界の使用のような、様々な方法を用いて特定する。