15.1.1.14　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報、情報処理施設及び移動が必要なその他のものの移行の管理、並びにその移行期間全体にわたって情報セキュリティが維持されることの確実化を含める。

15.1.2　関連する全ての情報セキュリティ要求事項を確立し、組織の情報に対して、アクセス、処理、保存若しくは通信を行う、又は組織の情報のためのＩＴ基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意する。

15.1.2.1　関連する情報セキュリティ要求事項を満たすという両当事者の義務に関し、組織と供給者との間に誤解が生じないことを確実にするために、供給者との合意を確立し、これを文書化する。

15.1.2.2　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、提供し又はアクセスされる情報の記載、及び提供方法又はアクセス方法の記載を含める。

15.1.2.3　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、組織の分類体系に従った情報の分類（必要な場合、組織の分類体系と供給者の分類体系との間の対応付け）を含める。

15.1.2.4　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、法的及び規制の要求事項（データ保護、知的財産権及び著作権に関する要求事項を含む。）、並びにこれらの要求事項を満たすことを確実にする方法についての記載を含める。

15.1.2.5　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、契約の各当事者に対する、合意した一連の管理策（アクセス制御、パフォーマンスのレビュー、監視、報告及び監査を含む。）の実施の義務を含める。

15.1.2.6　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、情報の許容可能な利用に関する規則（必要な場合、許容できない利用についての規則も）を含める。

15.1.2.7　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、組織の情報にアクセスする若しくは組織の情報を受領することが認可されている供給者の要員の明確なリスト、又は供給者の要員による組織の情報へのアクセス若しくはその受領を認可する場合及びその認可を解除する場合の手順・条件を含める。

15.1.2.8　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、それぞれの契約に関連する情報セキュリティのための方針群を含める。

15.1.2.9　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、インシデント管理の要求事項及び手順（特に、インシデントからの回復中の通知及び協力）を含める。

15.1.2.10　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、インシデント対応手順、認可手順などの、特定の手順及び情報セキュリティ要求事項についての訓練及び意識向上に関する要求事項を含める。

15.1.2.11　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、実施する必要のある管理策を含む、下請負契約に関する該当する規制を含める。

15.1.2.12　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、情報セキュリティに関する連絡先担当者も含む、合意における相手方の担当者を含める。

15.1.2.13　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、必要に応じて、供給者の要員の選考に関する要求事項を含める（この要求事項には、選考を実施する責任、及び選考が完了しなかった場合又は選考の結果、疑い若しくは懸念が生じた場合に行う通知の手順を実施する責任も含める。）。

15.1.2.14　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、供給者が実施する、合意に関わるプロセス及び管理策を監査する権利を含める。

15.1.2.15　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、合意上の問題点の解決及び紛争解決のプロセスを含める。

15.1.2.16　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、報告書で提起された問題を適時に修正することに関する管理策及び合意の有効性について、独立した報告書を定期的に提出する供給者の義務を含める。

15.1.2.17　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、組織のセキュリティ要求事項を順守するという供給者の義務を含める。

15.1.3　供給者との合意には、情報通信技術（以下「ＩＣＴ」という。）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含める。

15.1.3.1　供給者との合意には、供給者関係に関する一般的な情報セキュリティ要求事項のほかに、ＩＣＴ製品又はサービスの取得に適用する情報セキュリティ要求事項を定めることを含める。

15.1.3.2　供給者との合意には、ＩＣＴサービスに関して、供給者が組織に提供するＩＣＴサービスの一部を下請負契約に出す場合には、そのサプライチェーン全体に組織のセキュリティ要求事項を伝達するよう供給者に要求することを含める。

15.1.3.3　供給者との合意には、ＩＣＴ製品に関して、その製品に他の供給者から購入した構成部品が含まれる場合には、そのサプライチェーン全体に適切なセキュリティ慣行を伝達するよう供給者に要求することを含める。

15.1.3.4　供給者との合意には、提供されたＩＣＴ製品及びサービスが規定のセキュリティ要求事項を順守していることを確認するための、監視プロセス及び許容可能な監視方法を実施することを含める。

15.1.3.5　特に、直接の供給者が製品又はサービスの構成要素を他の供給者に外部委託する場合（製品又はサービスの機能を維持するために重要な構成要素に対しては、組織の外で作られる場合に注意及び精査の強化が求められるため。）、供給者との合意には、重要な構成要素を特定するためのプロセスを実施することを含める。

15.1.3.6　供給者との合意には、重要な構成要素及びその供給元が、サプライチェーン全体を通じて追跡可能であるという保証を得ることを含める。

15.1.3.7　供給者との合意には、提供されるＩＣＴ製品が期待どおりに機能し、予期しない又は好ましくない特性をもたないという保証を得ることを含める。

15.1.3.8　供給者との合意には、サプライチェーンについての情報、並びに組織と供給者との間で生じる可能性のある問題及び妥協についての情報を共有するための規則を定めることを含める。

15.1.3.9　供給者との合意には、ＩＣＴ構成要素のライフサイクル及び継続的な使用、並びにこれに関連するセキュリティリスクを管理するための具体的なプロセスを実施することを含める。このプロセスには、その構成要素が入手できなくなる（供給者が事業を営まなくなる、又は技術進歩によって供給者がその構成要素を提供しなくなる。）というリスクを管理することも含める。

15.2　供給者のサービス提供の管理

目的：供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため

15.2.1　組織は、供給者のサービス提供を定常的に監視し、レビューし、監査する。

15.2.1.1　供給者のサービスを監視及びレビューすることによって、その合意における情報セキュリティの条件の順守、並びに情報セキュリティのインシデント及び問題の適切な管理を確実にする仕組みを整備する。

15.2.1.2　供給者のサービスの監視及びレビューは、合意の順守を検証するために、サービスのパフォーマンスレベルを監視することを含める。