f）許可したアクセスのレベルが、アクセス制御に関するトピック固有の方針に適していること、及び職務の分離などのその他の情報セキュリティ要求事項と整合していることの検証
g）認可手順が問題なく完了した後にだけ、アクセス権を有効にする
h）情報及びその他の関連資産にアクセスするために利用者識別子（ＩＤ、論理的又は物理的）に与えられたアクセス権の、一元的な記録の維持
i）役割又は職務を変更した利用者のアクセス権の変更
j）物理的及び論理的アクセス権の削除又は調整
k）利用者の論理的及び物理的アクセス権の変更の記録の維持

【アクセス権のレビュー】

5c-5.18.2　物理的及び論理的なアクセス権の定期的なレビューでは、次の事項を考慮する。
a）同じ組織内での何らかの変更後又は退職後の利用者のアクセス権
b）特権的アクセス権の認可

【雇用の変更又は終了前の考慮事項】

5c-5.18.3　情報及びその他の関連資産への利用者のアクセス権は、雇用の変更又は終了の前に、次に示すリスク因子の評価に基づいて、レビューし、調整又は削除する。
a）雇用の終了又は変更が、利用者の側によるものか又は経営側によるものかどうか、及び雇用の終了の理由
b）利用者の現時点の責任
c）現在アクセス可能な資産の価値

5d　供給者管理

5d-5.19　供給者関係における情報セキュリティ

管理策：供給者の製品又はサービスの利用に関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め、実施する。

目的：　供給者関係において合意したレベルの情報セキュリティを維持するため。

詳細管理策

5d-5.19.1　組織は、供給者関係に関するトピック固有の方針を確立し、関連する全ての利害関係者に伝達する。

5d-5.19.2　組織は、供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するためのプロセス及び手順を特定し、実施する。

5d-5.19.3　供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するためのプロセス及び手順は、組織によるクラウドサービスプロバイダの資源の利用にも適用する。

5d-5.19.4　供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するためのプロセス及び手順は、組織が実施するもの、並びに供給者の製品若しくはサービスの利用の開始又は供給者の製品及びサービスの利用の終了に関して供給者が実施することを組織が要求するものを含む。

（5d-5.19.4参考）　プロセス及び手順に含まれる内容の例として、次がある。
a）組織の情報の機密性、完全性及び可用性に影響を与える可能性のある供給者の種類の特定及び文書化
b）情報、製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択する方法の確立
c）適切な情報セキュリティ管理策を備えた供給者の製品又はサービスの評価及び選択、並びにそれらのレビュー。特に、供給者が実施する管理策の正確性及び完全性、それによって供給者の情報及び情報処理の完全性を確実にし、ひいては組織の情報セキュリティを確実にすること。
d）供給者がアクセス、監視、管理又は使用する可能性のある組織の情報、ＩＣＴサービス及び物理的インフラストラクチャの定義
e）組織の情報の機密性、完全性及び可用性に影響を与える可能性のある、供給者が提供するＩＣＴ基盤の構成要素及びサービスの種類の定義
f）次の事項に関連する情報セキュリティリスクの評価及び管理
1）潜在的な悪意のある供給者の要員に起因するリスクを含む、組織の情報及びその他の関連資産の供給者による使用
2）供給者が提供する製品（これらの製品で使用されるソフトウェア構成要素及びサブ構成要素を含む。）又はサービスの誤動作又はぜい弱性
g）第三者のレビュー及び製品の妥当性確認を含む、供給者の種類ごと及びアクセスの種類ごとに確立した情報セキュリティ要求事項の順守の監視
h）供給者の不順守の低減。これは監視を通じて検知されたか、又は他の手段によって検知されたかによらない。
i）供給者の製品及びサービスに関連するインシデント及び不測の事態への対処。これには、組織及び供給者の両方の責任を含める。
j）供給者の情報及び情報処理の可用性、並びにそれによって組織の情報の可用性を確実にするための、レジリエンスに関する対策、並びに必要な場合には、回復及び不測の事態に関する対策
k）供給者の要員とやり取りする組織の要員を対象とした、職務に関する適切な規則、トピック固有の方針、プロセス、手順及び行動についての、供給者の種類並びに供給者による組織のシステム及び情報へのアクセスのレベルに基づく、意識向上及び訓練
l）情報、その他の関連資産及び移動が必要なその他のものの転送の管理、並びにその転送期間全体にわたって情報セキュリティの維持を確実にすること
m）次の事項を含む供給者関係のセキュリティに配慮した終了を確実にするための要求事項
1）アクセス権の回収
2）情報の取扱い
3）契約中に開発された知的財産の帰属の決定