4）供給者又は内部委託の変更における情報の移行性
5）記録管理
6）資産の返却
7）情報及びその他の関連資産のセキュリティに配慮した処分
8）機密保持の要求の継続

n）供給者の要員及び設備に期待する要員セキュリティ及び物理的セキュリティのレベル

5d-5.19.5　代替の製品又はサービスの手配の遅延を回避するため、供給者がその製品又はサービスを提供できなくなった場合に情報処理を継続するための手順を検討する。

5d-5.20　供給者との合意における情報セキュリティの取扱い

管理策：供給者関係の種類に応じて、関連する情報セキュリティ要求事項を確立し、各供給者と合意する。

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-5.20.1　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明確な理解が得られる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。

（5d-5.20.1参考）　特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。

a）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
b）組織の分類体系に従った情報の分類
c）組織の分類体系と供給者の分類体系との間の対応付け
d）法令、規制及び契約上の要求事項、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
e）契約の各当事者に対する、合意した一連の管理策の実施の義務、及び供給者に対する、組織の情報セキュリティ要求事項の順守の義務
f）情報及びその他の関連資産の許容される利用に関する規則。必要な場合、許容されない利用についての規則も含める。
g）供給者の要員による組織の情報及びその他の関連資産の使用を認可する場合及びその認可を解除する場合の手順又は条件
h）供給者のＩＣＴ基盤に関する情報セキュリティ要求事項。特に、組織の事業上のニーズ及びリスク基準に基づき、個々の供給者との合意の基礎となる、情報の種類及びアクセスの種類それぞれについての最小限の情報セキュリティ要求事項
i）請負業者が要求事項を満たさなかった場合の補償及び是正
j）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）
k）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
l）下請負供給者の使用に関する合意など、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定
m）情報セキュリティに関する連絡先担当者も含む、関連する連絡先
n）法的に許容される場合、供給者の要員の選考に関する要求事項。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も含める。
o）供給者のプロセスに関連する情報セキュリティ要求事項についての第三者立証の証拠及び保証の仕組み、並びに管理策の有効性に関する独立した報告書
p）合意に関わる、供給者のプロセス及び管理策を監査する権利
q）管理策の有効性について、報告書を定期的に提出する供給者の義務、及び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合意
r）合意上の問題点の解決及び紛争解決のプロセス
s）組織のニーズに合わせたバックアップの提供（頻度及び種類並びに保管場所の点で）
t）主要設備と同じ脅威にはさらされない代替設備（すなわち、災害回復サイト）の可用性を確実にすること、及び主要管理策が失敗した場合のフォールバック管理策（代替管理策）の考慮
u）組織への事前通知を確実にする変更管理プロセスをもつこと、及び組織が変更を受け入れない可能性
v）情報の分類に合った物理的セキュリティ管理策
w）物理的輸送又は論理的送信中に情報を保護するための情報の転送の管理策
x）記録管理、資産の返却、情報及びその他の関連資産のセキュリティに配慮した処分、並びに継続的な機密保持義務を含む、合意締結時に定める終了条項
y）供給者が保存している組織の情報を、不要になり次第､セキュリティに配慮して破壊する方法の規定
z）契約の終了時に、別の供給者又は組織自らへの引継ぎの支援を確実にすること

5d-5.20.2　組織は、自らの情報がどこへ渡っているかを追跡するために、外部関係者との合意の登録簿を作成し、維持する。

5d-5.20.3　組織はまた、外部関係者との合意を定期的にレビューし、妥当性を確認し、更新して、それらが依然として必要であり、関連する情報セキュリティ条項によって目的に適合することを確実にする。

5d-5.21　ＩＣＴサプライチェーンにおける情報セキュリティの管理

管理策：ＩＣＴ製品及びサービス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-5.21.1　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に加えて、ＩＣＴサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。

a）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。