【法令及び規制】

5g-5.31.2　組織は、次の事項を行う。

a）自らの事業の種類に対する要求事項を認識するために、組織の情報セキュリティに関連する全ての法令及び規制を特定する。

b）組織が次のとおりである場合に、関連する全ての国における順守を考慮する。

―他国で事業を行っている。

―法令及び規制が組織に影響を与える可能性がある、他国の製品及びサービスを利用している。

―法令及び規制が組織に影響を与える可能性がある、法域との境界を越えて情報の移転を行う。

c）変更に追随し、新しい法令を特定するために、特定した法令及び規制を定期的にレビューする。

d）これらの要求事項を満たすためのプロセス及び個々の責任を定義し、文書化する。

【暗号化】

5g-5.31.3　暗号化は、次の項目に関連する合意、法令及び規制の順守を考慮に入れる。

a）暗号機能を実行するためのコンピュータのハードウェア及びソフトウェアの、輸入又は輸出に関する規制

b）暗号機能を追加するように設計されているコンピュータのハードウェア及びソフトウェアの、輸入又は輸出に関する規制

c）暗号利用に関する規制

d）暗号化された情報への、国の当局による強制的又は任意的アクセス方法

e）ディジタル署名、ｅシール及びディジタル証明書の有効性

（5g-5.31.3参考１）　暗号化は、多くの場合、固有の法的要求事項をもつ分野である。

（5g-5.31.3参考２）　関連する法令及び規制の順守を確実にするために、特に暗号化された情報又は暗号化ツールを法域の境界を越えて転送する場合、法的な助言を求めることが推奨される。

【契約】

5g-5.31.4　情報セキュリティに関する契約上の要求事項には、次のものに記載されている要求事項を含む。

a）顧客との契約

b）供給者との契約

c）保険契約

5g-5.32　知的財産権

管理策：組織は知的財産権を保護するための適切な手順を実施する。

目的：　知的財産権及び権利関係のある製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするため。

詳細管理策

5g-5.32.1　知的財産となり得るものを保護するために、次の事項を考慮する。

a）知的財産権の保護に関するトピック固有の方針を定め、伝達する。

b）ソフトウェア製品及び情報製品のコンプライアンスにのっとった利用を定めた、知的財産権の順守の手順を発行する。

c）著作権を侵害しないことを確実にするために、ソフトウェアは、知名度の高い、かつ、定評のある供給元だけを通して取得する。

d）適切な資産登録簿を維持管理し、知的財産権の保護が求められている全ての資産を特定する。

e）使用許諾を得ていることの証明及び証拠、手引などを維持・管理する。

f）使用許諾で許可された最大利用者数又は資源数を超過しないことを確実にする。

g）認可されているソフトウェア及び使用許諾されている製品だけが導入されていることを確実にするためのレビューを行う。

h）適切な使用許諾条件を維持・管理するための手順を定める。

i）ソフトウェアの処分又は他人への譲渡についての手順を定める。

j）公衆ネットワーク及び外部供給元から入手するソフトウェア及び情報の使用条件を順守する。

k）著作権法又は適用される使用許諾が認めている場合を除いて、商用記録（ビデオ、録音）を複製、他形式に変換、又は抜粋しない。

l）著作権法又は適用される使用許諾が認めている場合を除いて、規格、書籍、記事、報告書又はその他文書の全部又は一部を複写しない。

5g-5.33　記録の保護

管理策：記録は、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護する。

目的：　記録の保護及び可用性に関連する、法令、規制及び契約上の要求事項の順守、並びにコミュニティ又は社会の期待に応えることを確実にするため。

詳細管理策

5g-5.33.1　組織は、自らの事業の状況及び自らの管理の要求事項が時間の経過とともに変化するため、記録の真正性、信頼性、完全性及び使用可能性を保護するために次の段階を踏む。

a）記録の改変の防止を含む、記録の保存、受渡記録の取扱い及び記録の処分に関する指針を発行する。これらの指針は、記録管理及びその他の記録の要求事項に関する組織のトピック固有の方針に沿っている。

b）記録及びそれらの記録の保持することが望ましい期間を明確にした保持計画を作成する。

5g-5.33.2　記録を保存し、取り扱うシステムは、国又は地域の法令又は規制、及び該当する場合には、コミュニティ又は社会の期待も考慮に入れて、記録及びその保持期間の特定を確実にする。

5g-5.33.3　記録の保持期間が終了した後、組織にとって必要ない場合には、そのシステムは、記録を適切に破棄できるようにする。

5g-5.33.4　具体的な組織の記録の保護について決定する場合は、組織の分類体系に基づき、その情報に適用されている情報セキュリティ分類を考慮する。