5e-5.28.5　保存した証拠の価値を強化するために、入手可能であれば、要員及びツールの適格性を示す証明書又はその他適切な手段を追求する。

5e-5.28.6　ディジタル証拠が組織の枠又は法域を越える場合、組織は必要とされる情報をディジタル証拠として収集することが法的に認められていることを確認する。

5f　事業継続における情報セキュリティ管理

5f-5.29　事業の中断・阻害時の情報セキュリティ

管理策：組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画する。

目的：　事業の中断・阻害時に情報及びその他の関連資産を保護するため。

詳細管理策

5f-5.29.1　組織は、事業の中断・阻害時に情報セキュリティ管理策を適応させるための自らの要求事項を決定する。

5f-5.29.2　情報セキュリティ要求事項は、事業継続マネジメントプロセスに含める。

5f-5.29.3　中断又は障害後に重要な事業プロセスにおける情報のセキュリティを維持又は復旧するために、計画を策定し、実施し、試験し、レビューし、評価する。

5f-5.29.4　情報のセキュリティは、必要なレベル及び必要な時間内に復旧する。

5f-5.29.5　組織は次の事項を実施し、維持する。

a）事業継続計画及びＩＣＴ継続計画における情報セキュリティ管理策、支援システム及びツール

b）事業の中断・阻害時に既存の情報セキュリティ管理策を維持するためのプロセス

c）事業の中断・阻害時に維持できない情報セキュリティ管理策を補う管理策

5f-5.30　事業継続のためのＩＣＴの備え

管理策：事業継続の目的及びＩＣＴ継続の要求事項に基づいて、ＩＣＴの備えを計画し、実施し、維持し、試験する。

目的：　事業の中断・阻害時に組織の情報及びその他の関連資産の可用性を確実にするため。

詳細管理策

（5f-5.30参考）　事業継続に関するＩＣＴの備えは、事業の中断・阻害時にも組織の目的が継続して満たされることを確実にするための、事業継続マネジメント及び情報セキュリティマネジメントの重要な構成要素である。

5f-5.30.1　ＩＣＴ継続の要求事項を、事業影響度分析（ＢＩＡ）の結果をもとに規定する場合、そのＢＩＡプロセスでは、影響の種類及び評価基準を用いて、製品及びサービスを提供する事業活動の中断・阻害から生じる影響を経時的に評価する。

5f-5.30.2　事業の中断・阻害の結果として生じる影響の大きさ及び期間を用いて優先する活動を特定し、これに目標復旧時間（ＲＴＯ）を設定した後、ＢＩＡでは、優先する活動の支援にどの資源が必要かを決定する。

5f-5.30.3　優先する事業活動を支援する資源にもＲＴＯを定め、これらの資源の一部としてＩＣＴサービスを含める。

（5f-5.30参考）　ＩＣＴサービスに係るＢＩＡを拡張して、事業の中断・阻害時の活動を支援するために必要な、ＩＣＴシステムのパフォーマンス、容量・能力の要求事項、及び情報の目標復旧時点（ＲＰＯ）を定めることが可能である。

5f-5.30.4　ＩＣＴサービスに関わるＢＩＡ及びリスクアセスメントの結果に基づいて、組織は、事業の中断・阻害の前、中断・阻害中及び中断・阻害の後の選択肢を考慮したＩＣＴ継続戦略を特定し、選択する。

5f-5.30.5　ＩＣＴサービスに必要な可用性レベルを満たし、重要なプロセスの中断又は失敗後に求められる時間内に回復するために、この戦略に基づいて計画を作成し、実装し、試験する。

（5f-5.30.5参考）　事業継続戦略は、一つ以上のソリューションから成る可能性がある。

5f-5.30.6　組織は、次の事項を確実にする。

a）事業の中断・阻害に備え、それを緩和し、それに対応するために、必要な責任、権限及び力量をもつ要員が支援する適切な組織構造を備えている。

b）組織がＩＣＴサービスの中断・阻害を管理する方法を詳述した、対応及び復旧手順を含むＩＣＴ継続計画について、次を実施する。

1）演習及びテストを通じた定期的な評価

2）経営陣による承認

c）ＩＣＴ継続計画は、次のＩＣＴ継続に関する情報を含む。

1）ＢＩＡで特定した事業継続の要求事項及び目的を満たすためのパフォーマンス及び容量・能力の仕様

2）優先するＩＣＴサービスそれぞれのＲＴＯ及びそれらの構成要素を復旧する手順

3）情報として定義された優先するＩＣＴ資源のＲＰＯ及び情報を復旧する手順

5g　コンプライアンス管理

5g-5.31　法令、規制及び契約上の要求事項

管理策：情報セキュリティに関連する法令、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ための組織の取組を特定し、文書化し、また、最新に保つ。

目的：　情報セキュリティに関連する法令、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

【コンプライアンス管理全般】

5g-5.31.1　法令、規制又は契約上の要求事項を含む外部の要求事項は、次の場合に考慮に入れる。

a）情報セキュリティの方針群及び手順の策定

b）情報セキュリティ管理策の設計、実施又は変更

c）内部のニーズ又は供給者との合意のために情報セキュリティ要求事項を設定するプロセスの一部としての、情報及びその他の関連資産の分類

d）情報セキュリティリスクアセスメントの実施、及び情報セキュリティリスク対応活動の決定

e）情報セキュリティに関連する役割及び責任に従ったプロセスの決定

f）組織、並びに供給を受ける製品及びサービスの範囲に関係する、供給者の契約上の要求事項の特定