5g-5.33.5　記録類は、記録の種類によって、また、それぞれの種類を更に詳細に、保持期間、及び許容される物理的又は電子的な記憶媒体の種類によって分類する。

5g-5.33.6　満たすべき要求に応じて、許容される時間枠内及び書式で、要求された記録を取り出すことができるような、データ保存システムを選択する。

5g-5.33.7　電子記憶媒体を選択する場合は、将来の技術変化によって読出しができなくなることを防ぐために、保持期間を通じて記録にアクセスできること（記憶媒体及び書式の読取り可能性）を確実にする手順を確立する。

5g-5.33.8　記録を保持している期間中、記録の復号を可能にするために、暗号化したアーカイブ又はディジタル署名に用いた暗号鍵及び暗号プログラムも保持する。

5g-5.33.9　記憶媒体の保存及び取扱いの手順は、記憶媒体の製造業者が示す推奨の仕様に従って実施する。

5g-5.33.10　記録の保存に用いる媒体が劣化する可能性を考慮する。

5g-5.34　プライバシー及びＰＩＩの保護

管理策：組織は、適用される法令、規制及び契約上の要求事項に従って、プライバシー及びＰＩＩの保護に関する要求事項を特定し、満たす。

目的：　ＰＩＩの保護の情報セキュリティの側面に関連する法令、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-5.34.1　組織は、プライバシー及びＰＩＩの保護に関するトピック固有の方針を確立し、全ての関連する利害関係者に伝達する。

5g-5.34.2　組織は、プライバシー及びＰＩＩの保護のための手順を策定し、実施する。

5g-5.34.3　組織は、プライバシー及びＰＩＩの保護のために策定した手順を、ＰＩＩの処理に関わる全ての利害関係者に伝達する。

5g-5.34.4　組織は、プライバシー及びＰＩＩの保護のために策定した手順の順守、並びにプライバシー及びＰＩＩの保護に関する全ての法令及び規制の順守のために、適切な役割、責任及び管理策を整備する。

5g-5.34.5　プライバシー及びＰＩＩの保護に関する責任者は、要員、サービス提供者及びその他の利害関係者に対して、それぞれの責任及び従うことが望ましい特定の手順について、手引を提供する。

（5g-5.34.5参考）　多くの場合、例えば、プライバシー担当役員のような一人の責任者を任命することによって最も達成される。

5g-5.34.6　ＰＩＩの取扱いについての責任は、関連する法令及び規制を考慮に入れて処置する。

5g-5.34.7　ＰＩＩを保護するための適切な技術的及び組織的対策を実施する。

5g-5.35　情報セキュリティの独立したレビュー

管理策：人、プロセス及び技術を含む、情報セキュリティ及びその実施の管理に対する組織の取組について、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。

目的：　組織における情報セキュリティ管理の取組の、継続的な適切性、十分性及び有効性を確実にするため。

詳細管理策

5g-5.35.1　組織は、情報セキュリティの独立したレビューを実施するためのプロセスをもつ。

5g-5.35.2　管理層は、情報セキュリティの定期的な独立したレビューを計画し、発議する。

5g-5.35.3　情報セキュリティの独立したレビューは、情報セキュリティ方針、トピック固有の方針、及びその他の管理策を含む､情報セキュリティの取組の改善の機会及び変更の必要性の評価を含む。

5g-5.35.4　情報セキュリティの独立したレビューは、レビューの対象となる領域から独立した個人・組織が実施する。

5g-5.35.5　情報セキュリティの独立したレビューを実施する個人・組織は、適切な力量をもつ。

5g-5.35.6　情報セキュリティの独立したレビューを実施する個人は、評価を行う上で独立性をもつことを確実にするため、権限をもつ系統に属さない。

5g-5.35.7　情報セキュリティの独立したレビューの結果は、レビューを発議した管理層、及び、適切な場合には、トップマネジメントに報告する。

5g-5.35.8　情報セキュリティの独立したレビューの記録は、維持する。

5g-5.35.9　情報セキュリティの独立したレビューにおいて、情報セキュリティマネジメントに対する組織の取組及び実施が十分でないことが明確になった場合には、管理層は是正処置を発議する。

5g-5.35.10　情報セキュリティの定期的な独立したレビューに加えて、組織は次の場合にも、独立したレビューの実施を検討する。

a）組織に影響する法令及び規制が変わる。
b）重大なインシデントが生じる。
c）組織が新しい事業を開始する、又は現在の事業を変更する。
d）組織が新しい製品若しくはサービスの利用を開始する、又は現在の製品若しくはサービスの利用を変更する。
e）組織が情報セキュリティの管理策及び手順を大幅に変更する。

5g-5.36　情報セキュリティのための方針群、規則及び標準の順守

管理策：組織の情報セキュリティ方針、トピック固有の方針、規則及び標準を順守していることを定期的にレビューする。

目的：　情報セキュリティを、組織の情報セキュリティ方針、トピック固有の方針、規則及び標準に従って実施し、運用することを確実にするため。

詳細管理策

5g-5.36.1　管理者及びサービス、製品又は情報の管理責任者は、情報セキュリティ方針、トピック固有の方針、規則、標準及びその他適用される規制で定められた情報セキュリティ要求事項が満たされていることをレビューする方法を特定する。

5g-5.36.2　定めに従って効率的に情報セキュリティのレビューを行うため、自動的な測定ツール及び報告ツールの使用を考慮する。

5g-5.36.3　情報セキュリティのレビューの結果、何らかの不順守を検出した場合、管理者は、次の事項を行う。

a）不順守の原因を特定する。
b）順守を達成するための是正処置の必要性を評価する。
c）適切な是正処置を実施する。
d）是正処置の有効性を検証し、不備又は弱点を特定するために、講じた是正処置をレビューする。