ｆ）誤りのリスクを減らすために、メニューに適切な環境識別ラベルを表示する。
ｇ）取扱いに慎重を要する情報は、開発システム及びテストシステムに同等の管理策が備わっていない限り、その開発システム環境及びテストシステム環境にはコピーしない。

8d-8.31.3　全ての場合において、開発環境及びテスト環境は、次の事項を考慮して保護する。
ａ）全ての開発、統合及びテストツール（ビルダ、インテグレータ、コンパイラ、構成システム及びライブラリを含む。）のパッチ適用及び更新
ｂ）システム及びソフトウェアのセキュリティに配慮した構成
ｃ）環境へのアクセスの制御
ｄ）環境の変更及びそこに保存されているコードの監視
ｅ）環境の、セキュリティに配慮した監視
ｆ）環境のバックアップをとること

8d-8.31.4　一人の人間が、事前のレビュー及び承認なしに、開発環境及び本番環境の両方に変更を加えることができないようにする。

（8d-8.31.4参考）　これは、例えばアクセス権の分離又は監視を伴う規則によって達成可能である。

8d-8.31.5　通常と異なる状況では、認可されていない変更を検出し、対処するために、詳細なログ取得、リアルタイム監視などの追加の対策を実施する。

8d-8.32　変更管理

管理策：情報処理設備及び情報システムの変更は、変更管理手順に従う。

目的：　変更を実行するときに情報セキュリティを維持するため。

詳細管理策

8d-8.32.1　新しいシステムの導入及び既存システムに対する重要な変更は、文書化、仕様化、テスト、品質管理及び管理された実装についての合意された規則及び正式な手続に従う。

8d-8.32.2　情報処理設備及び情報システムの全ての変更を良好に管理することを確実にするように、管理責任及び手順を設ける。

8d-8.32.3　変更管理手順は、情報処理設備及び情報システムにおける情報の機密性、完全性及び可用性を確実にするために、設計の初期段階からその後の全ての保守作業までのシステム開発のライフサイクル全体にわたって文書化し、実装する。

8d-8.32.4　実施可能な場合には、ＩＣＴ基盤及びソフトウェアの変更管理手順を統合する。

8d-8.32.5　変更管理手順には、次の事項を含む。
ａ）全ての依存関係を考慮した、変更の潜在的影響に関する計画策定及び評価
ｂ）変更の認可
ｃ）関連する利害関係者への変更の伝達
ｄ）変更のテスト及びテストの受入れ
ｅ）導入計画を含む変更の実施
ｆ）フォールバック手順（代替手順）を含む緊急時及び不測の事態の考慮
ｇ）上記の全てを含む変更の記録の維持
ｈ）運用文書類及び利用者手順が、適切な状態であるように、必要に応じて変更することを確実にすること
ｉ）ＩＣＴ継続計画並びに対応及び復旧手順が、適切な状態であるように、必要に応じて変更することを確実にすること

8d-8.33　テスト用情報

管理策：テスト用情報は、適切に選定し、保護し、管理する。

目的：　テストの適切な実施、及びテストに使用する運用情報の保護を確実にするため。

詳細管理策

8d-8.33.1　テスト結果の信頼性及び関連する運用情報の機密性を確実にするように、テスト用情報を選択する。

8d-8.33.2　取扱いに慎重を要する情報（ＰＩＩを含む。）を、開発環境及びテスト環境へ複製しない。

8d-8.33.3　運用情報の複製をテスト目的で用いる場合は、その保護のために、テスト環境を組織内又はクラウドサービス上のいずれに構築しているかにかかわらず、次の事項を適用する。
ａ）運用環境に適用するものと同じアクセス制御手順をテスト環境に適用する。
ｂ）運用情報の複製をテスト環境に置く場合は、その都度認可を受ける。
ｃ）運用情報の複製及び利用は、監査証跡とするためにログをとる。
ｄ）テストに使用する場合、取扱いに慎重を要する情報は、削除又はマスキングによって保護する。
ｅ）テスト用情報の認可されていない使用を防止するために、テストの完了直後にテスト環境から運用情報を適切に削除する。

8d-8.33.4　テスト用情報は、セキュリティに配慮して保存し（結果を無効にする可能性がある改ざんを防止するため）、テスト目的でだけ使用する。

8d-8.34　監査におけるテスト中の情報システムの保護

管理策：運用システムのアセスメントを伴う監査におけるテスト及びその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意する。

目的：　監査及びその他の保証活動が運用システム及び業務プロセスに与える影響を最小限に抑えるため。

詳細管理策

8d-8.34.1　監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。
ａ）システム及びデータへのアクセスに関する監査要求は、適切な管理層の同意を得る。
ｂ）技術監査におけるテストの範囲を、合意し、管理する。
ｃ）監査におけるテストは、ソフトウェア及びデータの読出し専用のアクセスに限定する。必要な情報を取得するために参照専用のアクセスを利用できない場合、監査人に代わって必要なアクセス権をもつ経験豊かな実務管理者がテストを実行する。
ｄ）アクセスを許可する場合、許可する前にシステムへのアクセスに使用する装置・機器のセキュリティ要求事項を確立し、検証する。