システム監査：情報システムに関わる**リスク**に対するコントロールが適切に整備・運用されているかを検証すること（安全、有効かつ効率的に機能させる）

リスク：パスワードを定期的に変えているか、ソフトウェアは最新か、など

業界の安全基準が変わったら、その基準に従う

→法令順守

情報セキュリティ監査：組織が保有するすべての情報資産（紙媒体も含む）が対象

システム監査：情報システムに関するあらゆる業務が監査対象　→　監査計画に基づき、予備調査、本調査、評価・結論の手順によって実施

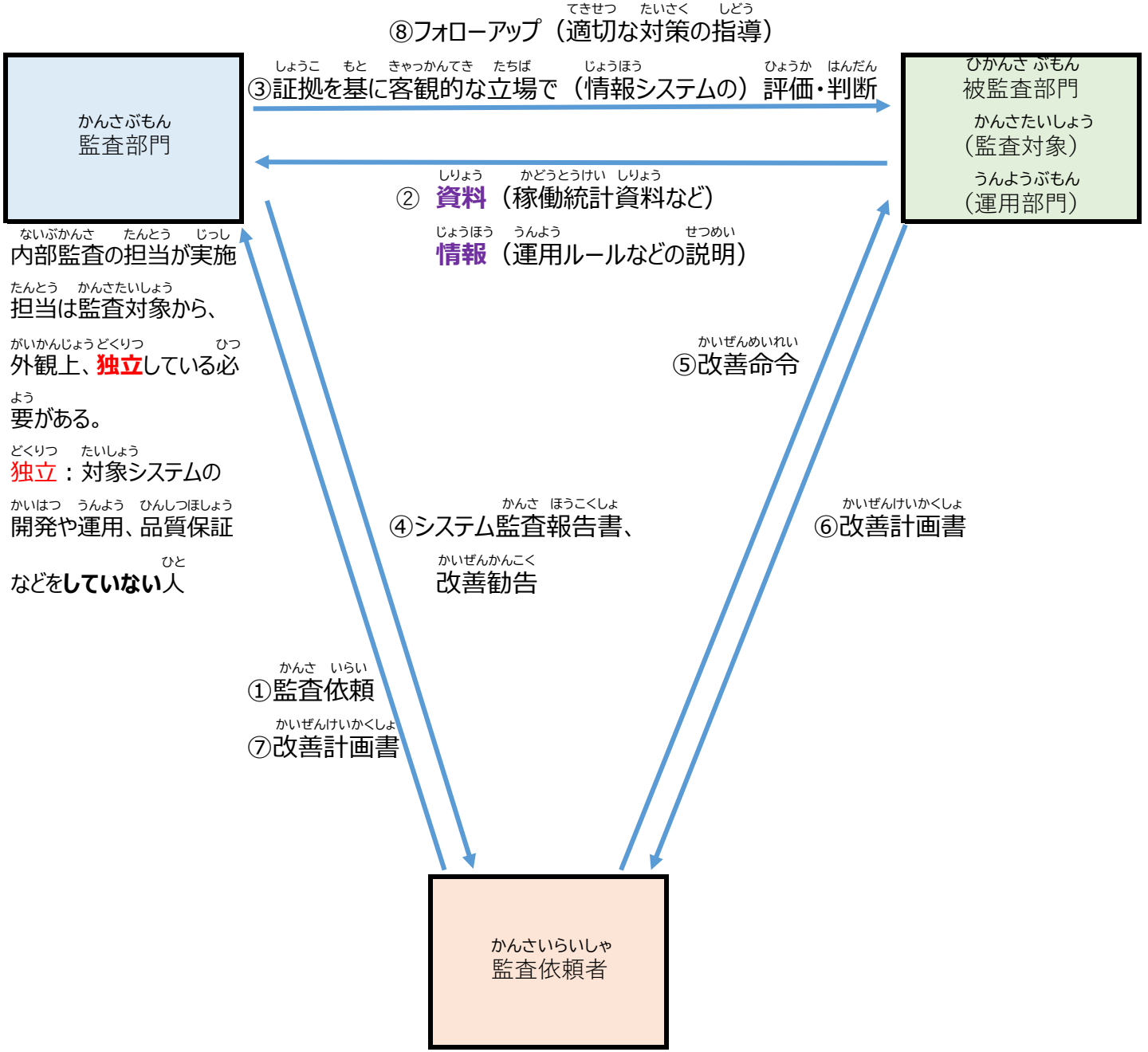
調査手段：システム監査ソフト（監査技法ソフト）、資料や文書、ヒアリング

会計監査：不正や誤りのない処理が行われているかを確認

内部監査の担当が実施

担当は監査対象から、外観上、**独立**している必要がある。

独立：対象システムの開発や運用、品質保証などを**していない**人



システム監査：情報システムに関わる**リスク**に対するコントロールが適切に整備・運用されているかを検証すること（安全、有効かつ効率的に機能させる）

リスク：パスワードを定期的に変えているか、ソフトウェアは最新か、など

業界の安全基準が変わったら、その基準に従う

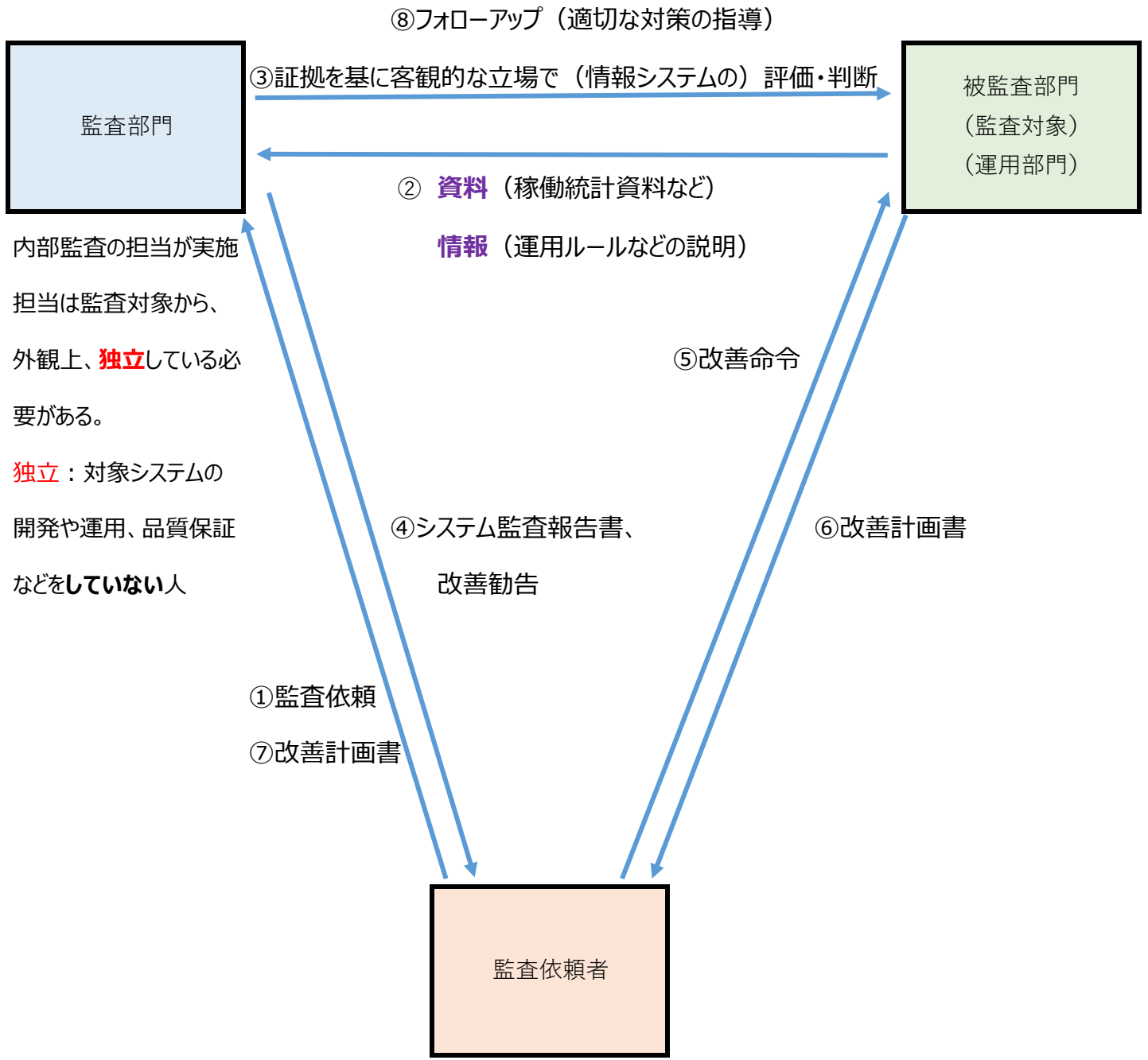
→法令順守

情報セキュリティ監査：組織が保有するすべての情報資産（紙媒体も含む）が対象

システム監査：情報システムに関するあらゆる業務が監査対象　→　監査計画に基づき、予備調査、本調査、評価・結論の手順によって実施

調査手段：システム監査ソフト（監査技法ソフト）、資料や文書、ヒアリング

会計監査：不正や誤りのない処理が行われているかを確認



System Audit: Verifying whether controls for **risks** related to information systems are appropriately designed and operated (to ensure that systems function safely, effectively, and efficiently).

Risks: For example, whether passwords are changed regularly, and whether software is kept up to date.

If industry safety standards change, the organization must comply with the new standards. → Legal compliance

Information Security Audit: All information assets owned by the organization are subject to audit, including paper-based materials.

System Audit: All operations related to information systems are subject to audit.

→ Audits are conducted based on an audit plan, following the procedures of preliminary investigation, main audit, evaluation, and conclusion.

Audit Methods: System audit software (audit tools/techniques), documents and records, and interviews.

Financial Audit: Confirms whether processing is carried out without fraud or errors.