Deloitte.
デロイト トーマツ

トーマツ.

情報セキュリティ監査支援サービス

「情報セキュリティ管理基準」に基づく情報セキュリティ監査

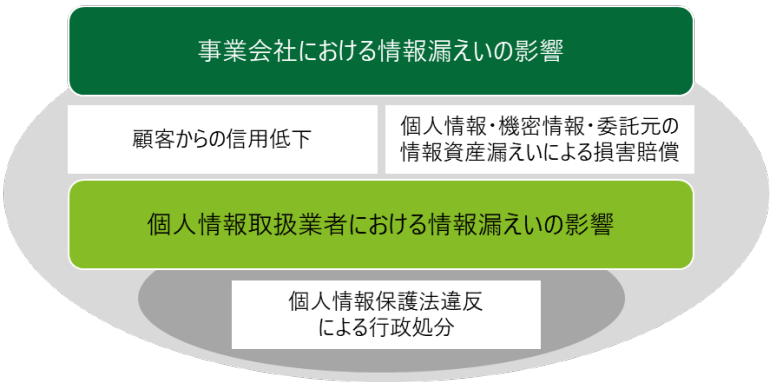
有限責任監査法人トーマツ

リスクに応じた情報セキュリティ監査を実施するために

情報セキュリティマネジメントシステムの必要性

近年、ウィルス・ランサムウェアの感染などによる情報漏洩の事件が相次いで発生し、組織が被害を受けるケースは少なくありません。
これらのセキュリティインシデントの影響は、組織にとって多額の損害賠償請求や行政処分にとどまらず、社会的信用の低下といった様々な影響を及ぼします。
セキュリティインシデントを防止するには、ファイアーウォールやデータ暗号化等の技術的な対策だけでは不十分であり、リスク分析と費用対効果を考慮した対策立案、環境変化に応じた対策の継続的な見直しが必要です。
これらの活動を組織として継続していくために、一過性の技術的な対策の推進ではなく、情報セキュリティマネジメントシステムの構築が重要な要因となります。

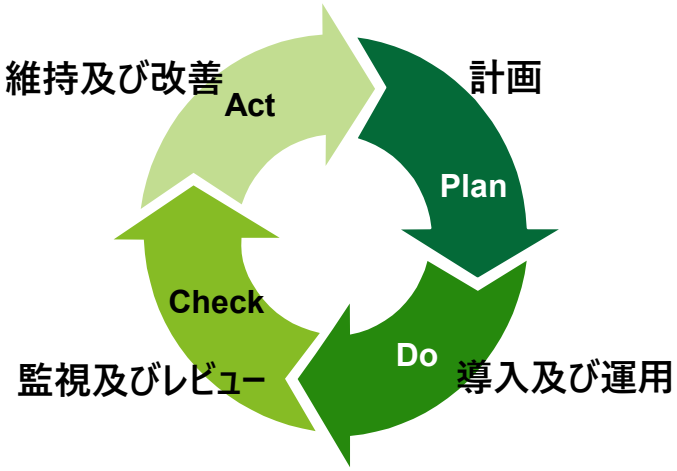
情報漏えい時の影響



「情報セキュリティ管理基準」（経済産業省）の改訂

「情報セキュリティ管理基準」は、組織が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロールを整備・運用する規範として策定されました。
一方で組織を取り巻く環境も変化しており、DX推進、サプライチェーンなどの新しいテーマに関連する課題も考慮しなければなりません。
令和7年改正版では、これらの要素を含む情報セキュリティマネジメントに関する国際規格であるISO/IEC27001,ISO/IEC27002の改訂を受け、JISQ27001:2023及びJISQ27002:2024に準拠した内容となっています。

情報セキュリティマネジメントシステムのPDCAサイクル



内部監査における「情報セキュリティ管理基準」

「情報セキュリティ管理基準」に沿った監査は、組織の課題を識別し改善活動に有効です。
「情報セキュリティ管理基準」はガバナンス基準、マネジメント基準、管理策基準と構成されており、組織の情報セキュリティ管理態勢を確認することとなります。
そのため、内部監査員は技術的な知識に加え、幅広い情報セキュリティの知識・経験を持つことが求められます。

「情報セキュリティ管理基準」概要

ガバナンス基準

- ✓ 情報セキュリティガバナンスを確立するための目的及びプロセスについて示す
- ✓ ISO/IEC 27014:2020における規程事項を参考に策定

マネジメント基準

- ✓ 情報セキュリティマネジメントの計画、実行、点検、処置に必要な実施事項を定める
- ✓ ISO/IEC 27001:2023を基に、情報セキュリティ監査を実施・受ける組織など幅広い利用者を想定した記述

管理策基準

- ✓ 情報セキュリティマネジメント確立段階において、リスク対応方針に沿った管理策を選択する際の選択肢を与える
- ✓ JISQ27001:2023付属書A「管理目的及び管理策」、JISQ27002:2024を基に既存のISMS認証との整合性、専門家の知見を考慮作成

「情報セキュリティ監査」サービス

「情報セキュリティ監査」サービスでは、「情報セキュリティ管理基準」に沿った情報セキュリティ監査を提供しています。

また、情報セキュリティ監査で課題を洗い出すだけではなく、フォローアップ活動として、組織の状況に応じた課題に対する改善策及び課題改善に向けたアプローチ案を提示または支援する等、個別ニーズに即したサービスの提供も可能です。

情報セキュリティ監査に関する主な提供サービス

1. 情報セキュリティ監査（外部調査）の実施
2. 情報セキュリティ監査（内部監査）のコソース
3. 情報セキュリティ監査後のフォローアップ

リスクアプローチに基づく情報セキュリティ監査

トーマツでは、リスクアプローチに基づく情報セキュリティ監査を実施します。
予備調査を実施し、組織や事業の概要及びリスクを把握し、リスクに対応した監査手続きを立案します。
本調査では監査手続きを実施しながら、課題を識別し、改善策及び改善に向けたアプローチを検討します。

情報セキュリティ監査アプローチ例

	1.予備調査	2. 調査手続検討	3. 本調査	4. 課題検討	5. 調査結果報告
	調査対象の概要把握	調査手続の具体化	調査手続に従った検討の実施	調査結果の分析と課題検討	報告書作成と報告会
当監査法人の作業内容	■ 調査対象の概要把握（システム概要、管理手続等の閲覧）	■ 運用状況調査時に実施する調査手続を質問書（調査手続書）として準備	■ 調査手続の実施	■ チーム内での課題検討 ■ 調査対象部門と問題点、改善案を協議	■ 報告書作成 ■ 報告会での報告
貴社の作業	■ 本調査で必要な資料の収集	■ 対象部門への通知、協力依頼	■ 本調査対象部門への連絡、協力依頼 ■（調査対象部門）質問への回答、関連資料のご提供	■ 事実確認会のセッティング	■ 報告会の開催 ■ 調査結果の経営者への報告

トーマツのサービス提供事例

トーマツでは、情報セキュリティ監査に関連する豊富な実績を有しており、これらに基づく実効性の高いサービスを提供します。

情報セキュリティ管理基準の他、PマークやISO各種規格に応じた内部監査、個人情報取扱等のテーマ監査、個別の事業における情報セキュリティ監査など組織のニーズに対応したサービスの提供も可能です。

情報セキュリティ監査に関する提供事例概要

業種	サービス提供概要
物流業	株式上場に伴うIT統制整備・ISMS認証取得の指導・助言（内部監査含む）
情報通信業	情報セキュリティ内部監査に関する助言 ISMS認証に関する内部監査コソース
医療・福祉	ISMS認証に関する指導・助言（内部監査含む）
サービス業	ISMS認証に関する指導・助言（内部監査含む）
金融業	システムリスクに対する内部監査に関する助言 委託先等を含む情報セキュリティ内部監査に関する助言 内部監査員に対する情報セキュリティ監査研修
不動産業	セキュリティ管理態勢に関する外部評価
教育・学習支援	情報セキュリティ自己点検に関する指導・助言

※サービス提供事例の一部を記載しております

トーマツのサービス提供品質・強み

トーマツでは「情報セキュリティ監査」の他にも「セキュリティコンサルティング」と「J-SOXや上場準備」の双方を高いクオリティで提供しています。

デロイト トーマツ グループのプロフェッショナルを最大限に活用し、組織が持つ固有の課題を解決するチームを編成することも可能です。

トーマツの強み

※貴社および貴社との関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、本サービス内容が提供できない可能性があります。詳細はお問合わせください。

Deloitte. トーマツ.
デロイト トーマツ

有限責任監査法人トーマツ
デジタルアシュアランス事業部

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
http://www.bsigroup.com/clientDirectory