



官公庁・自治体向けの 情報セキュリティ監査

最新の脅威に対応する、
安全・安心な行政運営の実現

Introduction

近年、公共分野における情報セキュリティの重要性はかつてないほど高まっています。デジタル化の推進に伴い、行政サービスはますますオンライン化され、利便性が向上する一方で、サイバー攻撃や情報漏洩といった新たな脅威・リスクも増大しています。このような状況下で、情報資産の保護と安定した行政サービスの提供を実現するためには、情報セキュリティマネジメントの継続的な改善が不可欠です。政府機関等においてはサイバーセキュリティ基本法に基づき政府統一基準群に準拠した情報セキュリティマネジメントを維持、向上することが求められています。また、地方公共団体においては地方自治法の改正により、サイバーセキュリティの確保についての方針を定め必要な措置を講じることが明記されました。

情報セキュリティマネジメントの継続的な改善には、独立した第三者による「情報セキュリティ監査」が有効な手段となります。経験豊富な監査人が客観的な視点から現状を評価し、リスクや課題を明確化することで、組織の信頼性向上や法令遵守の徹底に寄与します。

当法人は、官公庁・自治体向けの情報セキュリティ監査において、豊富な実績と専門的知見を有するコンサルタントが多数在籍しています。情報セキュリティマネジメントの継続的な改善のため、是非当法人の「情報セキュリティ監査」をご活用ください。

情報セキュリティ監査の 重要性と背景

デジタル技術の進展により、官公庁・自治体が提供するサービスはますます多様化・高度化しています。一方、情報資産への脅威は年々増加しており、組織のセキュリティ対策に対する社会的な期待も高まっています。本ページでは、情報セキュリティを取り巻く現状と、その対策強化に不可欠な監査の役割について解説します。

官公庁・自治体における情報セキュリティの現状と課題

官公庁や自治体では、住民情報や行政サービスを守るため、情報セキュリティの確保が不可欠です。近年、ランサムウェアや標的型攻撃など、IPA「情報セキュリティ10大脅威*1」に挙げられるサイバー攻撃が継続的に発生しており、組織の規模を問わず被害事例が報告されています。また、内部不正やサプライチェーンリスクといった新たな脅威への対応も求められています。これらの脅威に対し、個人情報保護やマイナンバー制度といった法制度、住民サービスの信頼性確保の観点から、情報セキュリティ対策の強化が急務となっています。

監査基準

情報セキュリティ監査では、政府が定める「政府機関の情報セキュリティ対策のための統一基準」や、総務省・厚生労働省など各省庁が策定するガイドライン・基準を遵守することが重要です。これらの基準は、情報資産の保護、リスク管理、運用体制の構築など、行政組織に求められるセキュリティ管理の指針を明確にしています。有限責任監査法人トーマツ（トーマツ）は、こうした公的基準に加え、ISMS（情報セキュリティマネジメントシステム）など国際標準も参照し、最新の法令・ガイドラインに適合した監査を実施します。これにより、組織の実態に即した現実的なセキュリティ強化が可能となります。

監査の必要性

情報セキュリティ監査は、組織の情報セキュリティマネジメントを強化し、情報漏洩やサイバー攻撃などのリスクを未然に防ぐための重要な施策です。監査を定期的実施することで、現状の課題や改善点を明確化でき、組織全体のセキュリティ意識の向上にも寄与します。また、住民サービスの信頼性向上や、法令遵守の担保にもつながり、行政運営の透明性や説明責任を果たす上でも有効です。トーマツは、豊富な知見と実績を活かし、官公庁・自治体の特性に合わせた監査を通じて、安定した行政運営に貢献します。

| 順位 | 「組織」向け脅威 | 10大脅威での 取り扱い (2016年以降) |
|----|-----------------------|------------------------------|
| 1 | ランサム攻撃による被害 | 10年連続10回目 |
| 2 | サプライチェーンや委託先を狙った攻撃 | 7年連続7回目 |
| 3 | システムの脆弱性を突いた攻撃 | 5年連続8回目 |
| 4 | 内部不正による情報漏えい等 | 10年連続10回目 |
| 5 | 機密情報等を狙った標的型攻撃 | 10年連続10回目 |
| 6 | リモートワーク等の環境や仕組みを狙った攻撃 | 5年連続5回目 |
| 7 | 地政学的リスクに起因するサイバー攻撃 | 初選出 |
| 8 | 分散型サービス妨害攻撃（DDoS攻撃） | 5年ぶり6回目 |
| 9 | ビジネスメール詐欺 | 8年連続8回目 |
| 10 | 不注意による情報漏えい等 | 7年連続8回目 |

*1 情報セキュリティ10大脅威：
<https://www.ipa.go.jp/security/10threats/10threats2025.html>

有限責任監査法人トーマツの 情報セキュリティ監査サービス概要

有限責任監査法人トーマツ（トーマツ）は、官公庁・自治体の情報セキュリティ課題に特化したサービスを展開しています。経験豊富な監査人が、情報セキュリティの基準やガイドラインに準拠した監査を通じ、情報セキュリティマネジメントの課題を発見し、組織にあった改善策を提言します。本ページでは、当法人が提供するサービスの詳細と支援体制についてご説明します。

主なサービス内容

トーマツが提供する情報セキュリティ監査サービスは、公共領域のセキュリティ監査や支援の経験豊富な監査人が、被監査組織のセキュリティ管理体制やリスクアセスメントを踏まえた効果的かつ深度の高い監査を提供しています。監査結果報告では、発見した事実に基づいて、脅威やリスクを踏まえた実効性ある改善提案を行い、組織の情報セキュリティの改善・強化に貢献します。

監査プロセス（予備調査、現地調査、報告書作成、改善支援）

監査プロセスは、まず初めにヒアリングや関連資料の収集による予備調査を通じて情報セキュリティマネジメントの状況や監査対象の組織・情報システムの概況を把握したうえで実地監査の計画を立案します。続いて、現地での実態調査やシステムの実機調査、関係者ヒアリングを通じて、運用実態やリスクの有無を多面的に分析します。監査で発見された事項、定量・定性両面から評価し、組織の特性やリスクプロファイルに応じて、優先度の高い課題を抽出します。監査結果報告書では、総合所見や個別所見として情報セキュリティマネジメントの改善・強化に資する改善策を提言します。改善策は、短期的な対応から中長期的な施策まで段階的に整理し、組織が自律的にPDCAサイクルを回せるよう支援します。さらに、改善施策の実行段階では、フォローアップ監査を行うなど、継続的な伴走型のサポートも提供可能です。

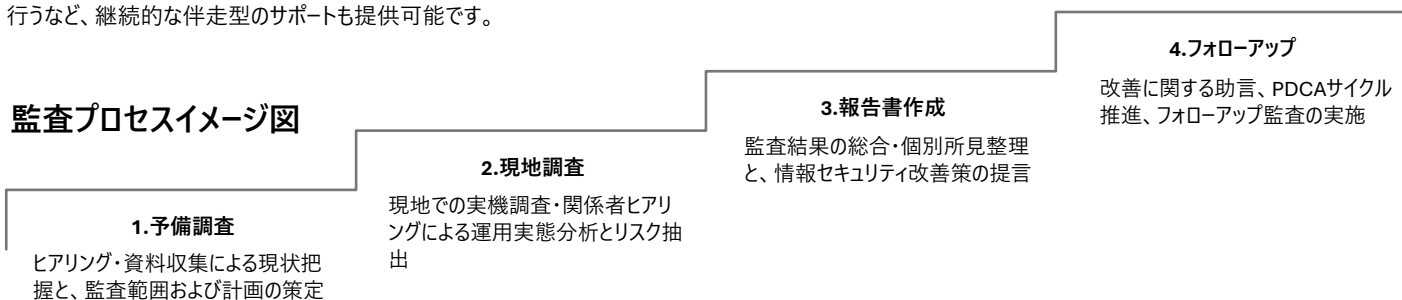
監査実績（官公庁・自治体向け事例紹介）

当法人は、中央省庁や地方自治体、独立行政法人、外郭団体など、多様な公共組織で数多くの監査実績を有しています。過去の事例では、監査を通じて組織の運用体制の見直しや、セキュリティポリシーの改定、リスク管理体制の強化など、具体的な成果を多数挙げています。豊富な経験を持つ専門家チームが、各組織の実情に合わせたきめ細やかな支援を行い、行政サービスの信頼性向上と情報資産の保護に貢献しています。

専門家チームによる支援体制

トーマツには、CISA（公認情報システム監査人）、システム監査技術者などの情報セキュリティ監査の専門資格を持つメンバーや、情報セキュリティ監査の経験豊富なメンバーが多数在籍しています。最新のセキュリティ動向や法令・ガイドラインの改定情報を常に把握し、組織ごとに最適な監査アプローチを設計します。監査の実施だけでなく、改善提案や教育・啓発活動も含めた総合的な支援体制を構築しており、行政機関の安全な運営と持続的な成長に貢献します。

監査プロセスイメージ図



※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。詳細はお問い合わせください。

Deloitte. トーマツ.

デロイト トーマツ

デロイト トーマツグループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイト ネットワークのメンバーであるデロイト トーマツ 合同会社ならびにそのグループ法人（有限責任監査法人 トーマツ、デロイト トーマツ リスク アドバイザリー 合同会社、デロイト トーマツ コンサルティング 合同会社、デロイト トーマツ ファイナンシャル アドバイザリー 合同会社、デロイト トーマツ 税理士 法人、DT 弁護士 法人およびデロイト トーマツ グループ 合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従いプロフェッショナルサービスを提供しています。また、国内約30都市に2万人超の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト、www.deloitte.com/jp をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイト ネットワーク”）のひとつまたは複数数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTL および DTTL の各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTL はクライアントへのサービス提供を行いません。詳細は www.deloitte.com/jp/about をご覧ください。

デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィック における100を超える都市（オークランド、バンコク、北京、ベンガール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、最先端のプロフェッショナルサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促進することで、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来180年の歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をバース（存在理由）として標榜するデロイトの約46万人の人材の活動の詳細については、www.deloitte.com をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、デロイト トウシュ トーマツ リミテッド（DTTL）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイト ネットワーク”）が本資料をもって専門的な助言やサービスを提供するものではありません。皆様の財務または事業に影響を与えるような意思決定または行動をされる前に、適切な専門家にご相談ください。本資料における情報の正確性や完全性に関して、いかなる表明、保証または確約（明示・黙示を問いません）をするものではありません。またDTTL、そのメンバーファーム、関係法人、社員・職員または代理人のいずれも、本資料に依拠した人に関係して直接または間接に発生し得る損失および損害に対して責任を負いません。DTTLならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体です。

Member of
Deloitte Touche Tohmatsu Limited

© 2025. For information, contact Deloitte Tohmatsu Group.



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>