AIMConsulting

ISMS監査の進め方と監査上の留意点

Account
Information & Intelligence
Management
Consulting

エイアイエムコンサルティング株式会社
コンサルティングサービス事業部
ビジネスコンサルティンググループ

Agenda

- **ISMSの基礎知識**
  - ISMSとは
  - ISMSで求められること
  - ISMSのPDCAサイクル
  - ISMSにおける内部監査部門の役割
- **これから始めるISMS監査**
  - ISMS監査の対象範囲
  - これから始めるISMS監査の監査手続～情報資産の管理～
  - これから始めるISMS監査の監査手続～人的資源の管理～
  - これから始めるISMS監査の監査手続～リスク評価～
  - これから始めるISMS監査の監査手続～クラウドセキュリティ～
  - これから始めるISMS監査の監査手続～データ削除～
- **ISMS監査の留意点**
  - 内部監査部門向けISMS監査の留意点
  - ISMS監査他社事例

AIM Consulting Co, Ltd, All Rights Reserved.

ISMSの基礎知識

ISMSとは

◆ ISMS（Information Security Management System）とは

情報セキュリティを担保するために、**IT技術対策の他**に、**リスクアセスメントにより必要なセキュリティレベルを決め**、組織の**経営資源を適切に配分して、仕組みを運用**することである。（情報マネジメントシステム認定センターより一部引用）

◆ 主な認証規格との違いと共通点

	ISMS	ISMSクラウドセキュリティ認証	QMS	プライバシーマーク
認証規格	国際標準規格 ISO/IEC27001 日本産業規格 JISQ27001	国際標準規格 ISO/IEC27017	国際標準規格 ISO/IEC9000 日本産業規格 JISQ9000	日本産業規格 JISQ15001
適用範囲	**全ての情報資産全般** （ハードやソフト、個人情報も含まれる）	クラウドサービスに関するセキュリティ （クラウドサービスの提供・利用に特化）	製品やサービス （顧客満足度の向上が目的）	企業内のすべての個人情報 （従業員の個人情報も含まれる）
認証単位	事業所・部門の単位でも取得可能	事業所・部門の単位でも取得可能	事業所・部門の単位でも取得可能	企業全体
要求事項	機密性・完全性・可用性の維持 （ISMSの確立・維持・継続的な改善）	クラウドサービスの安全性確保 （適切なクラウドサービスの維持・改善）	製品・サービスの提供管理 （品質を継続的に改善していく仕組み）	適切な個人情報の取り扱い （個人情報保護体制の維持・改善）
更新期間	3年ごと	2年ごと	3年ごと	2年ごと

各認証規格で適用範囲は異なるが、**PDCA（Plan-Do-Check-Action）というマネジメントシステムにて管理・運営するという共通点**がある。適用範囲に対する保証だけでなく、**仕組みや継続的な運用・維持・改善**が求められている。

AIM Consulting Co, Ltd, All Rights Reserved.

ISMSで求められること

◆ ISMSで求められること

情報セキュリティを担保するために、**3要素を維持・確保することが必要**とされている。情報セキュリティの**3要素をバランス良く保つことが重要**であり、そのために、**仕組みを確立し、運用すること（PDCAサイクル）**が求められている。

● 情報セキュリティの3要素

機密性

認可されていない者に対して情報を使用させない・開示しない特性（アクセス権の制御等）

完全性

改ざんや過不足のない正確な情報が保持されている状態（不正アクセスの検知等）

可用性

認可された者が、いつでも情報にアクセスすることができるという特性（業務復旧計画等）

◆ ISMSの要求事項（ISMS認証・更新のために実現すべきこと）

適用範囲	ISMSが有効に機能する範囲（企業全体か、一部の組織に絞るか等）	**計画**	ISMS達成やリスク対応に向けた手順や費用等、計画を明確にすること
引用規格	規格が引用する文書（ISO27001等）	**支援**	情報セキュリティ実施体制の整備や従業員に対する教育訓練の実施
用語および定義	マニュアルの文書で用いる用語の定義（ISO27001用語集等）	**運用**	計画通りにISMSを運用すること、問題点が生じた場合の対応方法の明確化
組織の状況	組織の内部・外部の状況を分析し、ISMSの目的達成を阻害する課題を把握すること	**パフォーマンス評価**	情報セキュリティの目標等を達成するための計画に対する監視・測定・分析および評価
リーダーシップ	ISMS構築を進めるうえでのトップマネジメントが積極的に関与していくこと	**改善**	是正処置やリスクおよび機会、規格不適合があった場合の対処方法

ISMSの確立・運用・維持・管理および継続的な改善を実現するために要求事項が定められている。ISMSの認証・更新を行うためには、**要求事項を理解したうえで、情報システム部門・現場部門等と連携しながら、仕組みの構築・運用を行う**。

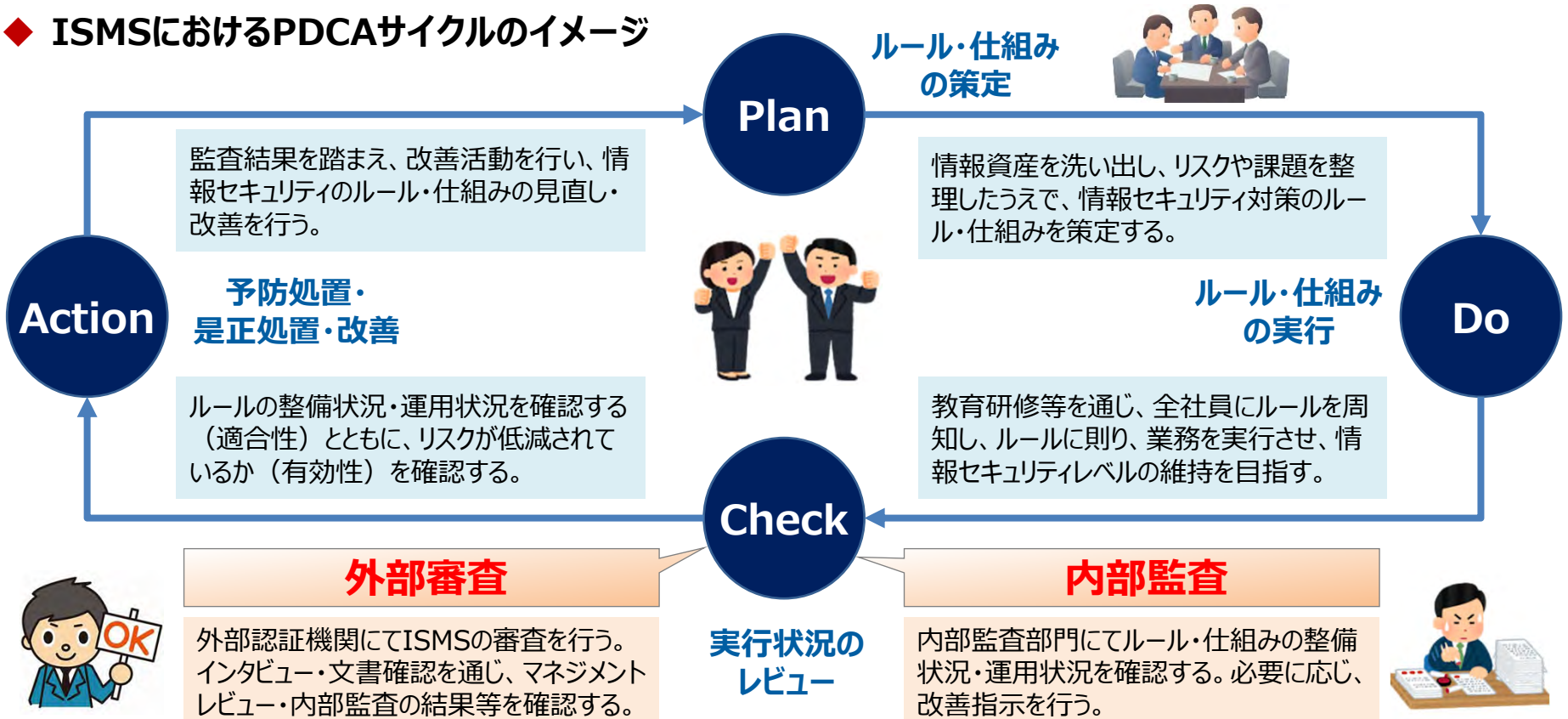
AIM Consulting Co, Ltd, All Rights Reserved.

ISMSのPDCAサイクル

◆ ISMSにおけるPDCAサイクルとは

ISMS要求事項において、**PDCAサイクルの構築・運用**が求められている。情報セキュリティを担保し、かつ、レベルを向上させるために、**ルールや仕組みを策定・実行するだけでなく、定期的にチェックを行い、改善を進める**ことが必要となる。

◆ ISMSにおけるPDCAサイクルのイメージ



ISMSの外部審査においても**PDCAサイクルが回っているかが重視**されている。PDCAサイクルを回すための**重要な要素として内部監査**がある。外部審査では、**内部監査の結果も重要視されるため、内部監査の実施は必須**となる。

AIM Consulting Co, Ltd, All Rights Reserved.

ISMSにおける内部監査部門の役割

◆ ISMSにおける内部監査

内部監査部門には、組織上の独立的な立場から、ルールや仕組みが**ISMSの要求事項を満たしているか（整備状況）**、ISMSの**ルール通りに実施されているか（運用状況）の確認を行う**ことが求められる。

◆ ISMSにおける内部監査部門の役割

ISMSにおける内部監査部門の役割

監査計画の策定		情報漏洩等のリスクや情報資産の保有状況等を踏まえ、監査項目・スケジュールを検討する。監査項目を基に、監査手続・対象部署を決定し、監査計画書に取り纏める。
適合性の判定		ISMSの要求事項を網羅し、情報セキュリティのルールや仕組みが整備されているか、環境変化等を踏まえ、現行ルールの見直しが行われているかの監査を行う。
有効性の判定		ルールや仕組みが効果的に機能し、リスクが低減されているかの監査を行う。ツールの設定等、ITの専門知識が強く求められ、内部監査部門では対応できない側面もある。
監査結果の報告		監査の実施結果を監査報告書に取り纏める。監査結果については、被監査部署に報告するとともに、マネジメントレビューとして、経営トップへの報告も必要となる。
改善指示		監査の結果、指摘事項が検出された場合は、被監査部署に改善是正の指示を行う。被監査部署にて実施した改善状況について、適宜フォローアップ監査を行う。

ISMS監査においては、**適合性と有効性の判定**が中心となる。**ITの専門知識が強く求められる局面**もあり、**内部監査部門は、適合性の判定を中心**としつつ、**有効性の判定については、監査項目の内容によって対応可否を判断**する必要がある。

AIM Consulting Co, Ltd, All Rights Reserved.

これから始めるISMS監査

ISMS監査の対象範囲

◆ ISMS監査の対象範囲について

ISMS監査の対象範囲は、情報セキュリティのルールに関する項目から人的な項目、システム管理業務、IT技術に関連する項目等、**多岐にわたる。**監査項目の内容を踏まえながら、**内部監査部門で対応すべき項目を峻別**していく。

◆ ISMSの監査項目と内部監査部門が対応すべき項目

内部監査部門主体で監査を行う項目（J-SOXと同様）	ファイルサーバやBIツール等のように**J-SOX範囲外の基盤もISMSの対象**になるが、**J-SOX（IT統制）評価の知見を活かし、同じ視点や進め方で確認できる項目もあるため、内部監査部門でも十分対応可能**である。 **セキュリティルール** / **インシデント管理** / **アクセス制御** / **物理的セキュリティ** / **OS・DBの管理** **システム運用** / **外部委託先管理** / **システム開発** / **システム変更** / **事業継続**
情報システム部門主体で監査を行う項目	システム上の設定値やプログラム内容等を踏まえ、リスクが低減できているかを確認する監査項目になる。**IT技術の知見がないと、リスクが低減されているかの判断が難しいため、情報システム部門が主体となり、監査**を行う。 構成管理 / 監視活動 / ウェブ・フィルタリング / コーディング / 暗号化
内部監査部門主体で監査を行う項目	**J-SOX（IT統制）の評価項目に見られない内容**になるが、**IT技術に関する専門的な知識がなくても、監査手続を理解すれば、内部監査部門で監査を行うことが可能**な監査項目である。 **情報資産の管理** / **人的資源の管理** / **リスク評価** / **クラウドセキュリティ** / **データ削除**

ISMS監査における**IT技術に関する監査項目は、情報システム部門が対応しないと難しい**側面がある。内部監査部門では、IT技術に関する知見がなくとも対応できる監査項目を対象にし、**監査項目の監査手続を理解して対応**を行う。

AIM Consulting Co, Ltd, All Rights Reserved.

これから始めるISMS監査の監査手続～情報資産の管理～

◆「情報資産の管理」の概要

情報資産とは、企業活動を行う中で、収集・作成される情報で、営業情報・技術情報・人事情報・財務情報等が該当する。情報漏洩・情報流出の**リスクが想定される情報資産の授受に関する統制状況を監査**する。

◆「情報資産の管理」における監査手続（例）

監査項目		監査手続（例）
情報資産の管理ルール	**適合性判定**	情報資産の授受に関するルール（管理対象となる情報、授受方法、有効期限、アクセス権の付与、パスワード設定等）が定められているかを確認する。
情報資産の授受	**有効性判定**	顧客や外部委託先、または契約先等の外部と情報をやり取りする場合、ルールに基づき、専用の共有サーバで実施しているか、パスワードを付して授受を行っているか等を確認する。
共有サーバのアクセス権	**有効性判定**	情報資産の授受ができるユーザーのアクセス権は、申請（申請書類・ワークフロー等）により行われ、適切な決裁者の承認を経て、付与されているかを確認する。
機密レベルのラベリング	**有効性判定**	電子データ・紙等、媒体を問わず、ルールに基づき、情報資産の機密レベルに応じ、ラベリング（社外秘を付す等）を行い、情報資産の管理が行われているかを確認する。（サンプリングで確認）

情報資産の内容（機密情報や個人情報を含む場合と含まない場合）で、**管理方法が異なることがある**。各部署で取り扱っている**情報資産の内容を確認したうえで、情報資産の管理ルールに合わせて監査手続を設定**する。

AIM Consulting Co, Ltd, All Rights Reserved.

これから始めるISMS監査の監査手続～人的資源の管理～

◆「人的資源の管理」の概要

人的なミスにより、情報漏洩や情報流出等の事故が発生していることも多くあり、**人的管理は重要視されている。**情報セキュリティを維持するためには、従業員の**雇用前・雇用中・雇用終了のそれぞれのタイミングでの監査**が必要となる。

◆「アクセス管理」における監査手続（例）

監査項目		監査手続（例）
人的セキュリティのルール	**適合性判定**	雇用手続に、情報セキュリティに関する事項があるかを確認する。また、情報セキュリティルールの違反行為に対する懲戒手続（違反内容や重要度に応じた基準等）が定められているかを確認する。
雇用前の管理	**有効性判定**	雇用契約書の雇用条件に、情報セキュリティに関する項目（機密情報の保持等）を設け、責任や義務が文書化されており、合意を得ているかを確認する。
雇用中の管理	**有効性判定**	情報セキュリティの啓蒙・教育に関する計画が定められており、教育訓練が定期的に実施されているかを確認する。（教育プログラムや教育訓練の参加者リスト等を確認する）
雇用終了時の管理	**有効性判定**	雇用終了となった際に、情報資産（PC・スマートフォン等）の返却や、利用しているシステムに対するユーザーアカウントの削除が遅滞なく行われているかを確認する。

従業員の情報リテラシー（情報の活用・管理に関する意識）が低いことが、情報セキュリティ事故の原因となっている。セキュリティレベルを高めるためには、情報リテラシーの向上が必要であり、**内部監査を通じ、意識を向上させる**ことが求められる。

AIM Consulting Co, Ltd, All Rights Reserved.

これから始めるISMS監査の監査手続～リスク評価～

◆「リスク評価」の概要

重要度の高いリスクに対し、充分に経営資源（人的リソース・費用等）を投入していくために、**情報資産への脅威や脆弱性の観点からリスクの分析・評価を行っているか、リスクに対する情報セキュリティ対策を講じているかを確認**する。

◆「リスク評価」における監査手続（例）

監査項目		監査手続（例）
リスク評価の管理ルール	**適合性判定**	情報セキュリティリスクに対する評価方法やリスク対応の優先基準等、リスク評価に関わる対応手順や判断基準、対応の決定方法等が定められているかを確認する。
情報資産の洗い出し	**有効性判定**	保有する情報資産を洗い出し、資産の種類（電子・紙）や重要度、リスク発生時の影響度合い等を分析した「情報資産台帳」が作成・更新しているかを確認する。
リスク評価	**有効性判定**	情報資産への脅威となる事象（パソコンの紛失やメールの誤送信、自然災害によるデータの消失等）を把握し、リスク評価報告書等の文書にまとめ、経営者に報告が行われているかを確認する。
脆弱性の把握	**有効性判定**	脆弱性（情報資産を脅威から守ることができない弱点）を把握し、重要度・優先度を踏まえ、ツール等の導入や運用手順を見直す等、対応計画を定めているかを確認する。

情報セキュリティに関するリスクは変化が早く、新たな脅威が発生しているため、**定期的にリスク評価が行われ、適切に脆弱性を把握**しているかが求められている。また、**把握した脆弱性への改善計画が定められているかを確認**する。

AIM Consulting Co, Ltd, All Rights Reserved.

これから始めるISMS監査の監査手続～クラウドセキュリティ～

◆「クラウドセキュリティ」の概要

外部のクラウドサービスを利用することが多くなっている一方、サービスが停止した場合、事業が企業における影響は大きくなる。クラウドサービスの**利用開始時に、品質が担保されているか、継続的な監視**が行われているかを監査する。

◆「クラウドセキュリティ」における監査手続（例）

監査項目		監査手続（例）
クラウドサービスの利用ルール	**適合性判定**	クラウドサービスの導入時・利用のプロセスやクラウドサービス利用・管理に関する役割・責任や利用範囲、セキュリティの要求事項、監視方法等のルールが定められているかを確認する。
サービス利用契約	**有効性判定**	クラウドサービスの利用にあたり、契約書類において、SLA（サービス品質保証）や水準未達の場合の対応、インシデントや事故が発生した場合の報告・対応が明確になっているかを確認する。
クラウド事業者からの報告	**有効性判定**	クラウド事業者において、情報セキュリティに関する監視活動が定期的に行われており、クラウド事業者から結果報告を適時に受領できる仕組み・運用（連絡フロー等）となっているかを確認する。
事業継続計画	**有効性判定**	情報システムの機能不全、災害・テロ・パンデミック等による稼働不全が発生した際、適切に報告が行われるとともに、業務復旧に向けた対応計画が明確になっているかを確認する。

クラウドサービスを利用するにあたっては、**クラウド事業者との役割分担を明確にしておく**ことが重要である。また、企業側においても、クラウド事業者のセキュリティ状況を**定期的に監視し、問題があれば、改善されているかを確認**する必要がある。

AIM Consulting Co, Ltd, All Rights Reserved.

これから始めるISMS監査の監査手続～データ削除～

◆「データ削除」の概要

データを保有していること自体が、情報漏洩や情報流出等、セキュリティ上のリスクになる。不要となったデータ（サーバ上のデータだけでなく、記憶媒体等を含め）がルールに基づき、**不要となった時点で削除されているかを確認**する。

◆「データ削除」における監査手続（例）

監査項目		監査手続（例）
データ削除のルール	**適合性判定**	業務上、データが不要となった際に削除するルールを定めており、削除方法（削除実施の基準・データ削除の実施手順）を明確にしているかを確認する。
利用データの棚卸	**有効性判定**	情報資産台帳に、業務上、利用しているデータの内容や利用期間が明記されており、定期的に見直し・更新が行われているかを確認する。
データ削除の実施	**有効性判定**	情報資産台帳を参照し、利用期間を超えているデータがサーバから削除されているかを確認する。また、記録媒体・個人PCのローカルディスク等に保存されているデータがないかを確認する。
委託先保有のデータ削除	**有効性判定**	外部委託先との契約が終了した際、ルールに基づき、データの返却や消去が行われているかを確認する。また、貸与していたPCやツール等が返却され、使用不可となっているかを確認する。

業務都合を優先し、不必要にデータを保管していることがある。組織内にデータがなければ、漏洩・流出等のリスクはなくなる。**サーバ上のデータおよび個人PCの内部、記憶媒体や外部委託先を含め**、データ削除のルールに基づいているかを確認する。

AIM Consulting Co, Ltd, All Rights Reserved.

ISMS監査の留意点

内部監査部門向けISMS監査の留意点

◆ これからISMS監査を実践するうえでの留意点

情報セキュリティ ルールの 周知・浸透

情報セキュリティに関するルールが周知・浸透されていないことによる事故が多く発生している。

情報セキュリティに関するルールが周知・浸透されていないことにより、情報漏洩等の事故が発生している。ISMS監査を通じ、ルールの理解・運用状況を確認し、ルール通りに実行できていなければ、改善指摘を行っていくべきである。

全部署に対する 毎年の 監査実施

監査の実施期間が空くと、ルールの定着が進まないため、全部署を対象に毎年監査を行う必要がある。

ISMSの更新は3年ごとになるが、ルールを定着させるためには、全部署を対象にして毎年監査を行うべきである。情報資産の重要性（機密情報の有無等）により、優先度を踏まえて濃淡をつけながら、効率的に内部監査を実施すべきである。

情報システム部門と内部監査部門の分担

情報システム部門は設定状況等、IT技術に係る内容を確認し、内部監査部門は実施記録等を確認する

内部監査部門だけでは有効性の判定を行うことが難しい項目もある。内部監査部門では、適合性の判定を中心としつつ、有効性の判定については、対応可能な項目を取捨選択し、実施記録の確認等、監査手続を理解して対応を進めるべきある。

ISMSにおけるPDCAサイクルを回していくため、毎年監査を行う必要がある。関連部署と協力しながら、内部監査部門が主体となって対応を進めて行くのが望ましい。

AIM Consulting Co, Ltd, All Rights Reserved.

ISMS監査他社事例

◆ 会社概要

創業： 1997年2月（12月決算）　**市場**：東証プライム市場　**売上高**：1兆9,278億円
従業員数：約28,000名 (連結)　**業種**：ITサービス業　　**ISMS取得時期**：2006年12月

監査対象組織	200組織（グループ子会社を含む） Aグループ（個人情報や機密情報等、重要な情報資産を保持している組織）：65組織 Bグループ（個人情報や機密情報等、重要な情報資産を保持していない組織）：135組織

ISMSの特性を踏まえ、情報資産の重要度に応じて監査手続・監査項目に濃淡をつけて実施している

◆ ISMS監査事例

グループ区分	監査方法	監査項目
Aグループ	往査（対面）により、インタビューおよび実地確認を行うとともに、別途、証憑収集・確認を行い、監査を実施 （内部監査部門にて、重点的に監査を実施）	情報資産の管理/アクセス管理/インシデント管理/ 物理的セキュリティ管理/外部委託先管理/運用のセキュリティ/ 通信のセキュリティ/人的資源管理/OS・DB/システム開発・導入
Bグループ	Web会議を利用したリモート監査で対応。Web会議上で、インタビュー・証憑確認を行い、簡易的に監査を実施 （外部リソースも活用しながら、各組織の監査を実施）	情報資産の管理/アクセス管理/インシデント管理/ 物理的セキュリティ管理/外部委託先管理

情報セキュリティルールの浸透を図るため、全組織を対象に、毎年、ISMS監査を実施している。**内部監査部門の知見を踏まえてグループ区分に応じた監査を実施**しており、外部を活用しながら重要度の低いBグループを担当している事例である。

AIM Consulting Co, Ltd, All Rights Reserved.

AIMC

AIM Consulting

エイアイエムコンサルティング株式会社

https://www.aimc.co.jp

不明点等につきましては、下記よりお問合せください。

http://www.aimc.co.jp/inquiry/