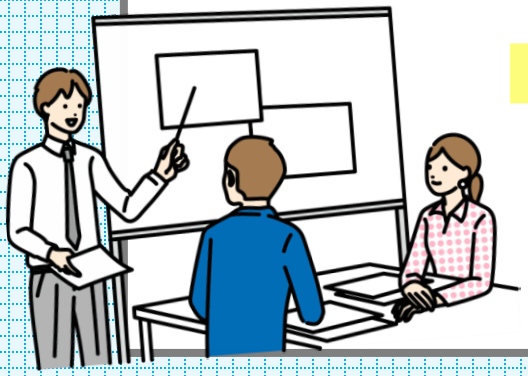
自社のセキュリティ、
リスク管理は万全？

セキュリティ
向上のために
今自社で
できることとは？

ISMS の観点から見る！中小企業 のための

情報セキュリティ管理 入門セミナー



ARM Standard

目次

はじめに

■ 情報セキュリティ管理に取り組む必要性

情報セキュリティを取り巻く環境は日々変化

- ランサムウェアやフィッシングなどのサイバー攻撃の増加
- 個人情報や顧客データの漏えい事故の頻発
- 法規制の強化（例：個人情報保護法、GDPR、サイバーセキュリティ基本法）

情報を「守ること」は企業や組織の責任であり、
信頼を維持するための重要な要素です。

ISMSとは？ – 簡単ISMS紹介 –

ISOとは？

ISOとは国際標準化機構のこと

製品・サービスなどの標準化を推進している民間組織であり、

この組織で世界共通の基準を制定しています。

→ ISO国際規格

洗濯絵表示
(ISO3758)

ネジ
(イソネジ)

非常口
(シンボルマーク)

製品規格

➡ モノに対する製品・品質・仕様を定めた規格

世界のどこにあっても同じ規格（サイズ、仕様など）のモノが使えます。

マネジメントシステム規格

➡ 企業・組織の運営の仕組み・やり方を定めた規格

要求事項を土台として仕組みを整えることで、世界共通のマネジメントの仕組み / 体制をつくることができます。

(Plan→Do→Check→Act)

2-2 ISMSとは？ －簡単ISMS紹介－

■ ISMSとは？

ISMS(Information security management system)**とは**
組織の情報セキュリティをマネジメントする仕組みのこと。
国際規格であるISO/IEC27001を基準として構築、運用、監視、改善を実施していきます。

ISO/IEC27001とは
国際標準化機構（Internaional Organizetion for Standardization）によって
制定された情報セキュリティマネジメントシステムに関する国際規格

JIS Q 27001とは
ISO/IEC27001を日本国内で使用することを目的として日本語に翻訳されたもの

その他のISOマネジメント規格

ISO9001	品質マネジメントシステム	ISO14001	環境マネジメントシステム
ISO/IEC20000	ITサービスマネジメントシステム	ISO45001	労働安全衛生マネジメントシステム　等

2-3 ISMSとは？ －簡単ISMS紹介－

Pマークと ISMS認証（ISO/IEC27001) の違い

	Pマーク（プライバシーマーク）制度	ISMS適合性評価制度
規格	JIS Q　15001：2023	ISO/IEC 27001：2022+Amd1:2024（JIS Q 27001:2025）
	国内規格であり、日本のみで適用される	**国際標準規格として全世界で適用される**
対象	組織が保有する個人情報（顧客・従業員）	適用範囲にある個人情報を含めた情報資産（紙、データ、ソフト、ハード、サービス等）
	対象範囲は組織全体	**適用範囲は事業部、業務等選択が可能**
運用	合理的な安全対策	93の管理策を中心に対策を適用
	規格で手順が厳格に決められている	組織の業務形態に合わせて運用を構築
要求	**適切な個人情報の取り扱い**	**情報の機密性・完全性・可用性の維持**
	個人情報の取得、利用、共同利用、委託、提供、安全管理（情報セキュリティ）、開示等要求対応、苦情対応など	情報資産の重要性、リスクに応じた適切な情報セキュリティ管理
法令	**個人情報保護法**	**業務に関連する法令を選択**
	プライバシーマークを取ることで個人情報保護法に関連する対応が実施され、個人情報保護法に対する認識が深まる。	刑法、民法、個人情報保護法、不正アクセス禁止法、不正競争防止法、番号法等、業務に関連する法令の遵守

このような企業様におすすめ！

ECサイトで顧客情報をたくさん保有している

要配慮個人情報を保管しなければならない

このような企業様におすすめ！

社内で情報の管理方法が統一されておらず、標準化したい

会社の状況に合わせたルール作りや継続的な改善ができる

3-1 情報の３要素と対策の重要性

ISMSが定義する情報セキュリティとは？

情報の**機密性**，**完全性**及び**可用性**を維持すること

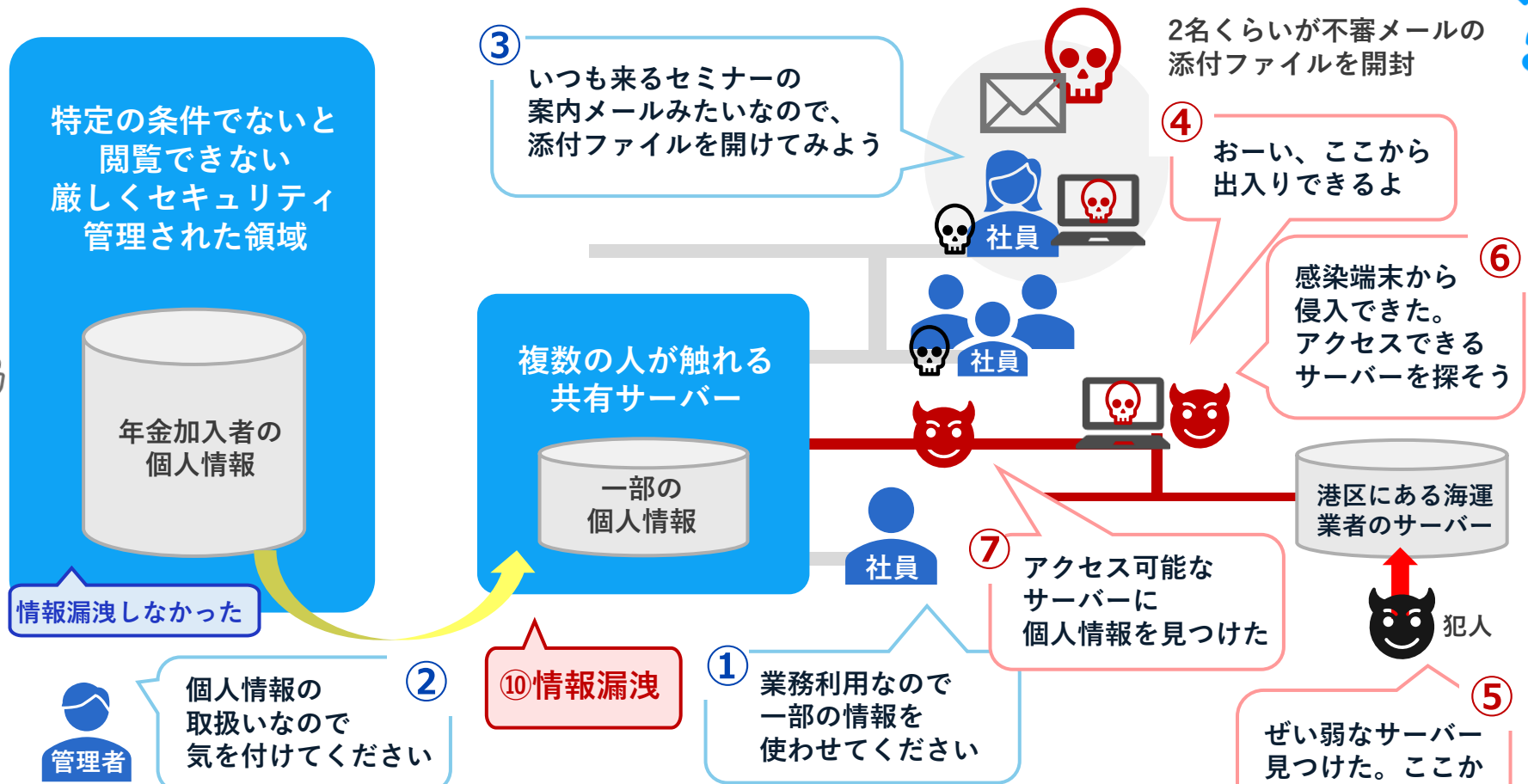
（JIS Q 27000情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語）

機密性	情報の開示範囲が適正に保たれていること
完全性	情報や情報の処理方法が正確で、不足が無い状態を保つこと
可用性	許可された者が必要な時に情報や情報資産を使える状態を保つこと

➡ 情報の３要素が毀損されることの無いように、自社の状況に即した管理体制を講じていくことが重要です。

情報の３要素と対策の重要性

情報セキュリティ事故例 －日本年金機構情報漏洩を振りかえる－



4-1 ISMSから考える組織のセキュリティ体制

ISOの規格構成と紹介

0　序文	
1　適用範囲	
2　引用規格	
3　用語及び定義	
4 組織の状況	4.1 組織及びその状況の理解 4.2 利害関係者のﾆｰｽﾞ及び期待の理解 4.3 情報ｾｷｭﾘﾃｨﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑの適用範囲の決定 4.4 情報ｾｷｭﾘﾃｨﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ
5 ﾘｰﾀﾞｰｼｯﾌﾟ	5.1 ﾘｰﾀﾞｰｼｯﾌﾟ及びｺﾐｯﾄﾒﾝﾄ 5.2 方針 5.3 組織の役割、責任及び権限
6 計画	6.1 ﾘｽｸ及び機会に対処する活動 6.2 情報ｾｷｭﾘﾃｨ目的及びそれを達成するための計画策定 6.3 変更の計画策定
7 支援	7.1 資源 7.2 力量 7.3 認識 7.4 ｺﾐｭﾆｹｰｼｮﾝ 7.5 文書化した情報
8 運用	8.1 運用の計画及び管理 8.2 情報ｾｷｭﾘﾃｨﾘｽｸｱｾｽﾒﾝﾄ 8.3 情報ｾｷｭﾘﾃｨﾘｽｸ対応
9 ﾊﾟﾌｫｰﾏﾝｽ評価	9.1 監視、測定、分析及び評価 9.2 内部監査 9.3 ﾏﾈｼﾞﾒﾝﾄﾚﾋﾞｭｰ
10 改善	10.1 継続的改善 10.2 不適合及び是正処置

※ 規格本文の箇条4~10が、
ISMSに関する要求事項となっています。

箇条4~10のいかなる要求も除外できません。

附属書 A　　93項目　管理策

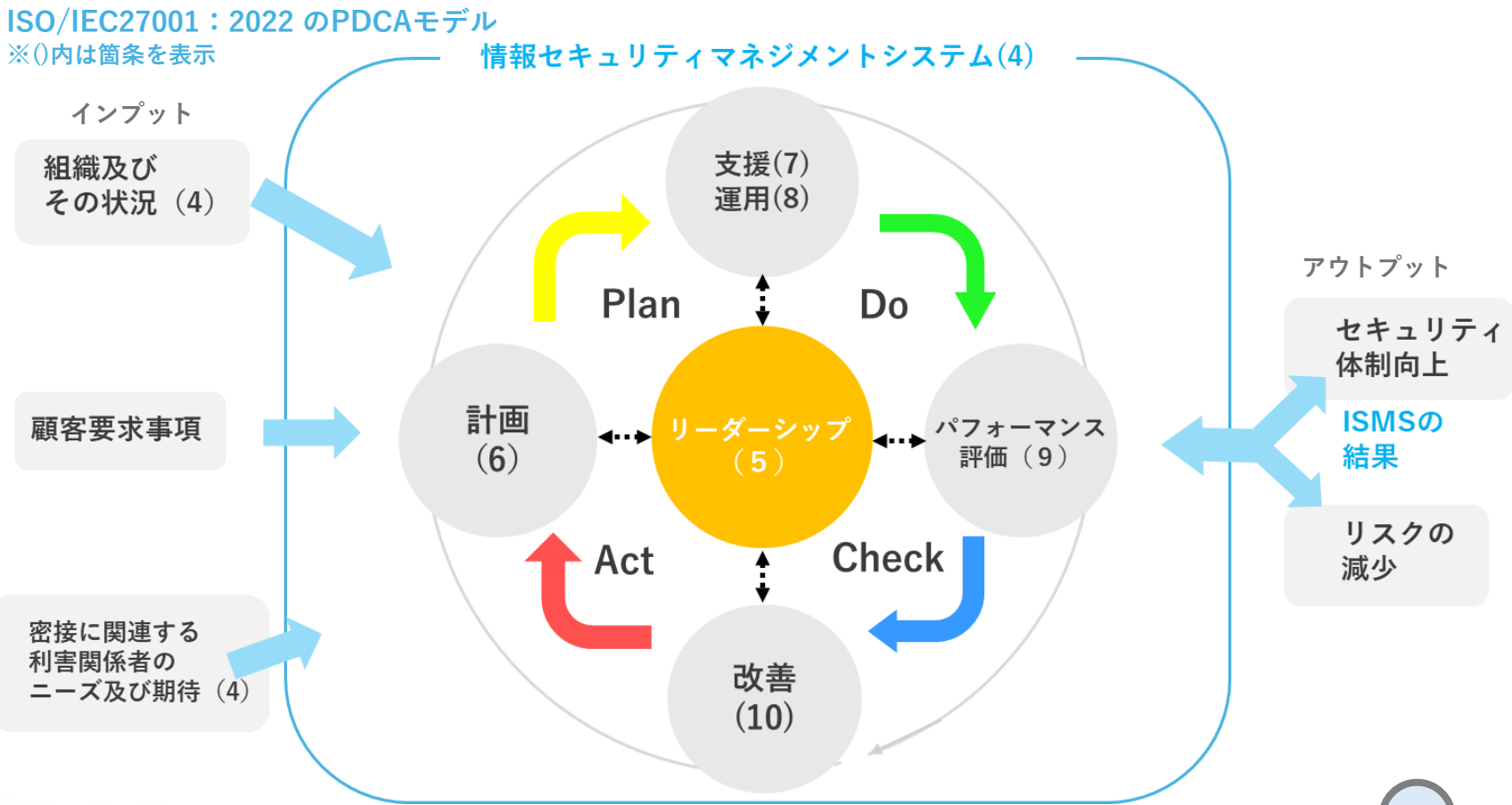
リスクに対応した実施策に関する要求事項

正当な理由を示せば、採用しないことも選択可

4-2 ISMSから考える組織のセキュリティ体制

ISMSの箇条：PDCAサイクルを基に構成

実践することで、継続的改善やしっかりしたセキュリティ体制を実現することができます。



5-1 PICK UP! リスクアセスメントについて紹介

■ リスクアセスメントとは？

リスクアセスメントとは、情報資産を取り扱う場面において
発生可能性のあるリスクを抽出し、**実際に起こった場合の影響度**と
現実的な起こりやすさからリスク値を算出すること。
リスクの大きさを知ることで、リスクに対応する優先順位を決定していくことができます。

■ リスクアセスメントの手順

リスク特定 → リスク分析 → リスク評価

一緒に取り組んでみましょう！

5-2 情報資産の評価

ISMSが定義する情報セキュリティとは？

情報の**機密性**，**完全性**及び**可用性**を維持すること

（JIS Q 27000情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語）

基準値や内容は企業が
決定しますが、仮として
１～３で評価点を付けてみましょう

＜記入例＞

要素	レベル	クラス	説　明
機密性	3	極秘	ISMS適用者の中で特定の関係者（管理責任者など）のみに，利用・立入・開示・提供可能なもの
	2	社外秘	ISMS適用外の社内の人に，利用・立入・開示・提供可能なもの
	1	公開	社外の人に，利用・立入・開示・提供可能なもの
完全性	3	高	トラブルの発生や情報の内容を変更された場合，ビジネスへの影響が深刻かつ重大であるもの
	2	中	トラブルの発生や情報の内容を変更された場合，ビジネスへの影響が大きいもの
	1	低	トラブルの発生や情報の内容を変更された場合，ビジネスへの影響がさほど大きくないもの
可用性	3	高	必要なときに，必ず利用できることを保証するもの
	2	中	必要なときでも，1時間利用できなくても許容されるもの
	1	低	必要なときでも，1日利用できなくても許容されるもの

5-3 PICK UP! リスクアセスメントについて紹介

STEP1 リスク特定

1. 守るべき会社の情報資産を洗い出す

① 情報資産を洗い出しましょう

情報資産とは？

例えば…

顧客情報・社内情報・
システム・文書・
ソフトウェア・個人PC
私用しているサービス　等

作成日：　　作成者名:

	資産グループ	情報資産	資産形態（紙、データ等）	評価値				リスク分析				リスク対応	
				機密性（C）	完全性（I）	可用性（A）	資産価値	脅威	業務への影響度	発生頻度 起こりやすさ	リスク値	選択肢	管理策(対策)
例		顧客リスト	紙										
例		製品設計図	データ										
		発注伝票	紙										

5-4 PICK UP! リスクアセスメントについて紹介

② 社内の情報資産ごとに評価値を付けてみましょう
また、ＣＩＡのすべてを足し、情報価値の比較をしてみましょう

☑ 機密性＋完全性＋可用性 ＝ 資産価値

基準値は企業が決定しますが、仮として１～３で評価値を付けてみましょう

作成日：　　作成者名:

資産グループ	情報資産	資産形態（紙、データ等）	評価値				リスク分析			
			機密性（C）	完全性（I）	可用性（A）	資産価値	脅威	業務への影響度	発生頻度 起こりやすさ	リスク値
	顧客リスト	紙								
	製品設計図	データ								
	発注伝票	紙								

情報漏洩　データ改ざん　盗難

③ 情報資産ごとに考えうる脅威を書き出してみましょう

「脅威」とは、情報セキュリティが脅かされる直接の原因となるものをいいます。
情報資産ごとに、考えられる脅威を記入してみましょう。

PICK UP!　リスクアセスメントについて紹介

STEP2 リスク分析

2. 特定した脅威が実際に発生してしまった場合、その脅威が業務に与える影響およびその発生頻度を考える

① 脅威の影響度と脅威の発生頻度の評価点をつけてみましょう

脅威の業務への影響度　※例

評価点	内容
3	脅威が発生した場合、業務への影響は深刻かつ重大である
2	脅威が発生した場合、業務への影響はあるものの会社内で対応が可能である
1	脅威が発生した場合、業務への影響はほとんど無い

脅威の発生頻度（起こりやすさ）※例

評価点	内容
3	頻繁に発生する（目安：週１回）
2	たまにある（目安：年１回）
1	ほとんどない（目安：１０年に１回）

基準値は企業が決定しますが、仮として１～３で評価点を付けてみましょう

5-6 PICK UP! リスクアセスメントについて紹介

② リスク値を算出してみましょう。

☑ リスク値 ＝

CIA喪失による影響度（資産価値） × 脅威の業務への影響度 × 脅威の発生頻度

＜記入例＞

作成日： 作成者名:

資産グループ	情報資産	資産形態（紙、データ等）	評価値				リスク分析				リスク対応	
			機密性（C）	完全性（I）	可用性（A）	資産価値	脅威	業務への影響度	発生頻度（起こりやすさ）	リスク値	選択肢	管理策（対策）
	顧客リスト	紙	2	2	2	6	情報漏洩	3	1	18		
	製品設計図	データ	2	2	2	6	改ざん	2	2	24		
	発注伝票	紙	1	1	1	3	紛失	2	2	12		

PICK UP!　リスクアセスメントについて紹介

STEP3 リスク評価

3．リスクのうちどれから対応するべきか優先順位をつける

① 例えば、リスク値が小さいものへの対応の必要性を考慮し、
リスクの受容基準を決めましょう

リスクが大きい

- 資産価値も高い、リスクが生じたときの影響度も大きい
- リスクは小さいけれど、資産価値が比較的高い

受容基準

受容基準を超えた部分は
対応する必要があります

- 対応の必要はなし

リスクが小さい

PICK UP!　リスクアセスメントについて紹介

■ リスク対応

3．受容基準を超えるリスクについて対応を考える

① 受容基準を超えるリスクについて、
リスク値を小さくできるような対応を考える

受容　現状のまま特段の対策は行わない

例. 停電に備えた自家発電機によりリスク
低減を図ったが、予算の都合で導入は翌年に回す

➡今年度は、リスクを「受容」したといえる
※基準以下のリスクは自ずと「受容」になります

軽減　対策を講じて影響度や発生頻度を変える

例. 停電に備えた自家発電機の導入により
リスクを低減する。
アクセス権限に制限を設ける

回避　リスク源そのものを取り除く

例. データへの損害というリスクに対し、
外部アクセス自体を遮断してしまったり、
安全な地域へ引っ越す等

移転　リスクに関連する業務をアウトソース化する

例. データの流出というリスクに対し、
外部へデータを委託し、管理を委ねる

5-9 PICK UP! リスクアセスメントについて紹介

■ リスクアセスメントやリスク対応を行うことのメリット

重大な事故の未然防止	● リスクを事前に把握 ● 後手対応を防止 ● 信頼とブランド維持
組織全体のセキュリティ意識向上	● 従業員の意識向上促進 ● 自分事として認識
ムダのないコスト最適化	● 効率的な資源配分 ● 対策優先順位化

➡ 経営資源を活かし、的確にリスクへ備えることができます

6-1 情報セキュリティ対策のチェックの仕方

■附属書Aの活用

附属書Aとは、情報セキュリティリスク対応となる実効手段を掲載したもの

下記の観点を参考にして、**必要な情報セキュリティ管理策において見落としているポイントがないか、自社が策定した対策と照らし合わせてチェック**することができます！

ISO/IEC 27002:2022	項目数	分類内容
5　組織的管理策	37	組織全体で管理すべきもの
6　人的管理策	8	要員が携わるもの
7　物理的管理策	14	有形物に関するもの
8　技術的管理策	34	電磁的なプロテクト手段
合計	93	

6-2 情報セキュリティチェックポイント紹介

組織的管理策

※一部抜粋

ISO/IEC27001:2022　附属書A		
組織的管理策	5.1	情報セキュリティのための方針群
	5.2	情報セキュリティの役割及び責任
	5.3	職務の分離
	5.5	関係当局との連絡
	5.6	専門組織との連絡
	5.7	脅威インテリジェンス
	5.25	情報セキュリティ事象の評価及び決定

人的管理策

※一部抜粋

ISO/IEC27001:2022　附属書A		
人的管理策	6.1	選考
	6.2	雇用条件
	6.3	情報セキュリティの意識向上、教育及び訓練
	6.5	雇用の終了又は変更後の責任
	6.8	情報セキュリティ事象の報告

情報セキュリティチェックポイント紹介

物理的管理策

※一部抜粋

ISO/IEC27001:2022　附属書A		
物理的管理策	7.1	物理的セキュリティ境界
	7.2	物理的入退
	7.3	オフィス、部屋及び施設のセキュリティ
	7.4	物理的セキュリティの監視
	7.5	物理的及び環境的脅威からの保護
	7.6	セキュリティを保つべき領域での作業
	7.7	クリアデスク・クリアスクリーン

技術的管理策

※一部抜粋

ISO/IEC27001:2022　附属書A		
技術的管理策	8.1	利用者エンドポイント機器
	8.2	特権的アクセス権
	8.3	情報へのアクセス制限
	8.4	ソースコードへのアクセス
	8.5	セキュリティを保った認証
	8.6	容量・能力の管理
	8.7	マルウェアに対する保護

7-1 ISO認証審査における主な確認ポイント

審査では下記ような点を確認し、
より磐石な情報セキュリティ管理を目指し、改善に向けた着眼点を提言します！

- 外部及び内部の課題、利害関係者のニーズ及び期待の変化（4.1、4.2）
- 認証範囲の適切性（4.3）
- 情報セキュリティ方針群のレビュー状況 （5.2、管理策5.1）
- リスクアセスメントの実施状況（6.1.2（8.2））
- リスク対応の状況（6.1.3（8.3））
- 監視・測定・分析及び評価の実施状況（9.1）
- 内部監査の実施状況（9.2）
- マネジメントレビューの実施状況（9.3）
- 不適合及び是正処置の実施状況（10.2）
- インシデント対応（管理策5.24～5.28、管理策6.8）
- 事業継続計画の検証、ICTの備え（管理策5.29）
- 適用法規制の把握・見直し状況（管理策5.31～5.36）
- 業種に応じた管理策の実施状況（管理策5-管理策8）

※（）内は箇条を表示

8-1 情報セキュリティに取り組むメリット

■ ISO/IEC27001の取得にはメリットが多くあります

1. 情報の取扱ルールの標準化

- 「何を・誰が・どう守るのか」が全社員に浸透
- 機密情報や個人情報の管理レベルが均一に

2. 情報漏えいリスクが“見える化”される

- 業務ごとのリスクを洗い出し、対策を明文化
- 予防措置と対応フローが整い、安心感が生まれる

3. インシデント発生時の対応がスムーズに

- 対応手順・連絡体制が決まっているから初動が早い
- 記録と振り返りが残り、再発防止にもつながる

4. 社員のセキュリティ意識が向上

- 業務に携わる人々が実態に沿った改善提案をする機会を得る
- USB・パスワード・持ち出しなど日常的なリスク行動が減少

5. 情報資産の棚卸と整理整頓が進む

- 「どこに何があるか」が明確になり、ムダなデータや危険な管理が激減
- 業務の効率化にも好影響

9-1 まとめ

■ ISMSの考え方を取り入れるだけでも、
セキュリティを強化していくことができます。
少しのことから取り組みセキュリティ管理に取り組んでみてください。

本日はセミナーにご参加くださり、ありがとうございました。

アカデミーコースでは、より詳細な
セキュリティ知識を身に着けることができます

ホームページでは、内部監査セミナーやeラーニングを
紹介しております
https://www.armstandard.com/

サービスに関するお問い合わせ
contact@armstandard.com

企業情報
〒103-0012
東京都中央区日本橋堀留町
1-10-15 JL日本橋ビル

TEL：03-3666-8814
FAX：03-3666-8752

ARM Standard

サービスに関するご質問やご不明点等ございましたら、
お気軽にお問い合わせください