しくみ製作所

怖くないISMS

ISMS規格アップデートについて

しくみ製作所 / 情報セキュリティハブ

0000.00.00

発表内容について

1. そもそもISMSとは？
2. 適用宣言書とは？
3. 適用宣言書の紹介
4. ISMSの具体的な運用例
5. おわりに

そもそもISMSとは？

ISMSとは？

しくみ製作所

ISMS：**I**nfomation **S**ecurity **M**anagement **S**ystem

情報セキュリティマネジメントシステムのこと

⇩

組織が情報セキュリティを管理するためのしくみ

国際規格が定められていて、審査を通過すると**認証**がもらえる

ISMS-AC

ISMSとは？

しくみ製作所

ISO27001：組織に求められる要求事項　＝　教科書

ISMSの認証を取得するにはこういうルールを守る必要があるよ！

ISO27002：要求事項の実践規範　　＝　参考書

ISMSの具体的な管理策はこういうことを考慮するといいよ！

なぜISMSに取り組むのか？

①　情報セキュリティリスクを適切にマネジメントできる

資産やリスクを洗い出し、リスクアセスメントすることで高リスクな業務プロセスを認知できる
組織の状況が透明化され、適切なマネジメントにつながる

②　業務プロセスを改善することができる

インシデントが発生した場合、確実に組織としての改善につなげることができる
組織内メンバーの意識向上につながる

③　組織外に、信頼感や安心感をアピールできる

案件によっては、ISMSの認証取得が入札参加の必須条件になっている例もある
認証されていない企業との差別化になる

ISMSの年間スケジュール

しくみ製作所

3月	マネジメントレビューと外部監査の結果から年間計画を策定
4月～12月	年間計画に従って改善事項を対応
10月	内部監査計画の策定
11月～12月	内部監査計画に従って内部監査を実施
1月	改善事項の対応結果と内部監査の結果をもって マネジメントレビューを実施
2月	内部監査の結果とマネジメントレビューの結果をもって 外部監査の実施

適用宣言書とは？

しくみ製作所

適用宣言書とは

組織がISO27001（教科書）で定められた情報セキュリティ管理策に対して
組織がどれを適用してどれを除外するのか宣言した文書

管理策	内容	適用	理由
A	組織は・・・のために、・・・しなければならない。	する	・・・で対応しているため。
B	要員は・・・のために、・・・しなければならない。	する	・・・規程で定めているため。
C	インシデントは・・・しなければならない。	する	・・・ガイドラインで定めているため。
D	オフィスは・・・しなければならない。	しない	・・・のため。

しくみ製作所

2022年のISO27001,27002改定内容①

１４項目あった管理策カテゴリが４項目に集約

組織的管理策	組織（しくみ製作所）が取り組むべき管理策
人的管理策	組織で働く人（全ての構成員）に関する管理策
物理的管理策	情報システムのハードウェアや建物、設備に関する管理策
技術的管理策	技術面（ネットワークや暗号化など）に関する管理策

しくみ製作所

2022年のISO27001,27002改定内容②

既存の管理策が統廃合され、新たに１１項目の管理策を追加

- 脅威インテリジェンス
- クラウドサービス利用のための情報セキュリティ
- 事業継続のためのICTの備え
- 物理的セキュリティの監視
- 構成管理・情報の削除・データマスキング・データ漏洩防止
- 監視活動・Webフィルタリング・セキュアコーディング

しくみ製作所

2022年のISO27001,27002改定内容③

- クラウドサービスへの対応: クラウドサービスの使用に関する情報セキュリティ管理策が追加
- 技術進歩への適応：新技術と脅威に対応するため、セキュリティに関する項目を更新
- オンプレミス環境の項目整理：従来のオンプレミス環境に関する管理策を削減

適用宣言書の紹介

権限

5.3 職務の分離

5.15 アクセス制御

5.18 アクセス権

概要

- 相反する職務は同一人物では行わない
- 許可されない情報資産にアクセスされないように管理する
- 不必要に大きな権限持たせないようにする

権限

適用理由

- 情報セキュリティ管理策の不正，エラー及び回避のリスク軽減
- 認可されていないアクセスの防止
- 業務上の要求事項に適した権限管理

具体策：クラウドサービス利用ガイドライン

- 権限規定を追加
  - 例）Notionのオーナーは代表取締役と総務リードのみ
- 各サービスでの機密情報の取り扱いを追加
  - 例）ChatGPTに社外秘の情報を投稿することを禁止

しくみ製作所

5.10 情報及びその他の関連資産の許容される利用
5.33 記録の保護

概要

- 情報及び関連資産の取り扱い手順を明確にしよう
- 記録データについて、消失、改ざん、不正アクセス、流出から保護しよう

情報資産の管理

適用理由

- 情報資産が適切に保護、利用されることを確実にするため
- 法令・規制・契約上の要求事項、記録の保護・可用性に関連する共同体又は社会の期待を順守するため

具体策：リスクアセスメント管理規定

- 情報資産にリスク値の項目を追加
  - リスク値が高く、対策が不十分な情報資産について管理を見直す

インシデント

5.24 情報セキュリティインシデント管理の計画策定及び準備

5.25 情報セキュリティ事象の評価及び決定

5.26 情報セキュリティインシデントへの対応

5.27 情報セキュリティインシデントからの学習

概要

- 事故・ヒヤリハットについて報告し、分析・評価・改善を行う

しくみ製作所

適用理由

- 将来のインシデントの起こりやすさ又は影響を減らすため

具体策：インシデント報告・対応ガイドライン

- 詳細を聞く必要がある場合はインシデントヒアリング会を設置
- 全社で対応を行う必要があると判断した場合は「しくみバックログ」にて他のロールに協力を依頼
- インシデント対応時は忙しいので、一段落してからの起票で大丈夫

しくみ製作所

5.7 脅威インテリジェンス
8.8 技術的ぜい弱性の管理

概要

- 情報セキュリティの脅威に関する情報収集・分析
- 利用している情報システムのぜい弱性に関する評価・対応

脅威インテリジェンス

適用理由

- 適切なリスク低減処置を講じることができるように，組織の脅威環境についての認識をもつため
- ぜい弱性の悪用を防止するため

具体策：「脅威インテリジェンス」プロセス

- #a-security-trend に各ハブの専門領域に関する情報セキュリティの脅威を投稿
- 必要であれば関係者へ共有

しくみ製作所

5.2 情報セキュリティの役割及び責任

概要

- 情報セキュリティの役割と責任を定める

しくみ製作所

適用理由

- 組織内における情報セキュリティの実施・運用及び管理のために定義・承認され、理解される構造を確立するため

具体策：情報セキュリティ体制

- しくみ各メンバーの役割と責任を記載

5.29 事業の中断・阻害時の情報セキュリティ
5.30 事業継続のためのICTの備え

概要

- 事業の中断・阻害時の情報セキュリティレベル維持
- 事業の中断・阻害時の情報資産への可用性維持

しくみ製作所

適用理由

- 事業の中断・阻害時に情報及びその他の関連資産を保護し、可用性を確実にするため

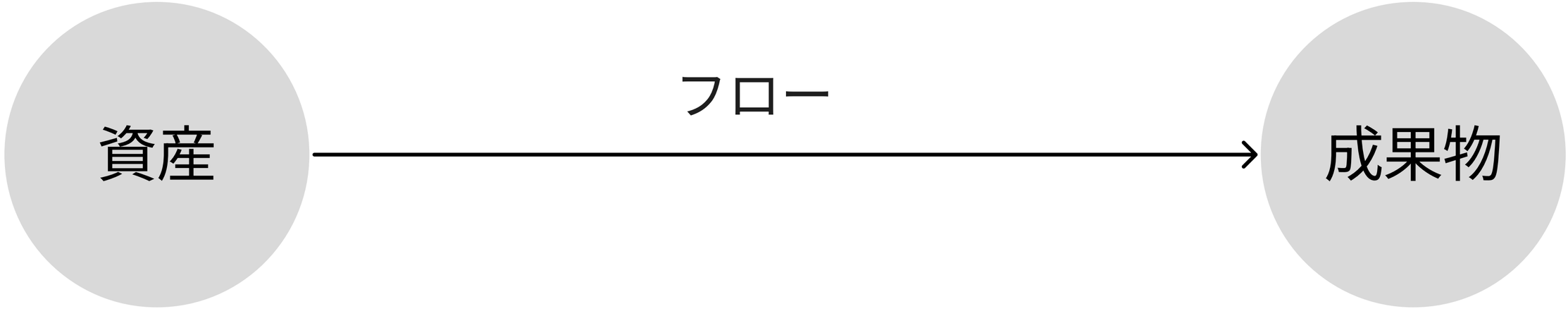
具体策：事業継続計画（BCP）

- 緊急事態（災害など）への事前対策・責任者を定義

ISMSの具体的な運用例

ロールによる活用

プロセスとは、資産を用いて業務の目的物(成果物)を作る一連の動き



資産のリスクが高い = プロセスのリスクが高い = 注視すべき業務

- 資産の把握、リスク管理が必要
- インシデント発生時は、プロセスそのもの見直しが必要

想定ケース

しくみ製作所

想定インシデント:
スマホをコワーキングスペースに置いてきた

発生後の流れ:

- 一次対応: PC/スマホの紛失の手順にて対応
- 全社対応: 紛失しても被害のない状態 > 機器管理チェック等見直し
  - 紛失モードをオン
  - PCのHDDを暗号化
  - 個人情報をPC内に保管しない etc

プロジェクトによる活用

1. セキュリティチェックリストの活用
- 目的: サービスリリースにて、一定程度の品質を担保するため
- 対応プロセス: リリース前のセキュリティチェック

2. インシデント報告
- 目的: 既存プロセスを見直し、今後の全社レベルのインシデント発生防止に役立てるため
- 対応プロセス: インシデントについて

おわりに

しくみ製作所

本日お話させていただいたことについてのドキュメントは
Notionの「ISMS（情報セキュリティマネジメントシステム）」に
掲載されております

ご清聴ありがとうございました