

ISO/IEC 27001 (ISMS) 構築支援

ヒアリング診断用

20XX年X月
NPO東京ITC

ISMSの構築についてのヒアリング

- ISMS構築の準備 (現状確認)
- ISMS構築の準備 (社内業務の仕組み調査)
- ISMS構築の基本的な考え方
- ISMS構築のための組織と役割
- ISMS構築のスケジュール
- ISMS構築の手順

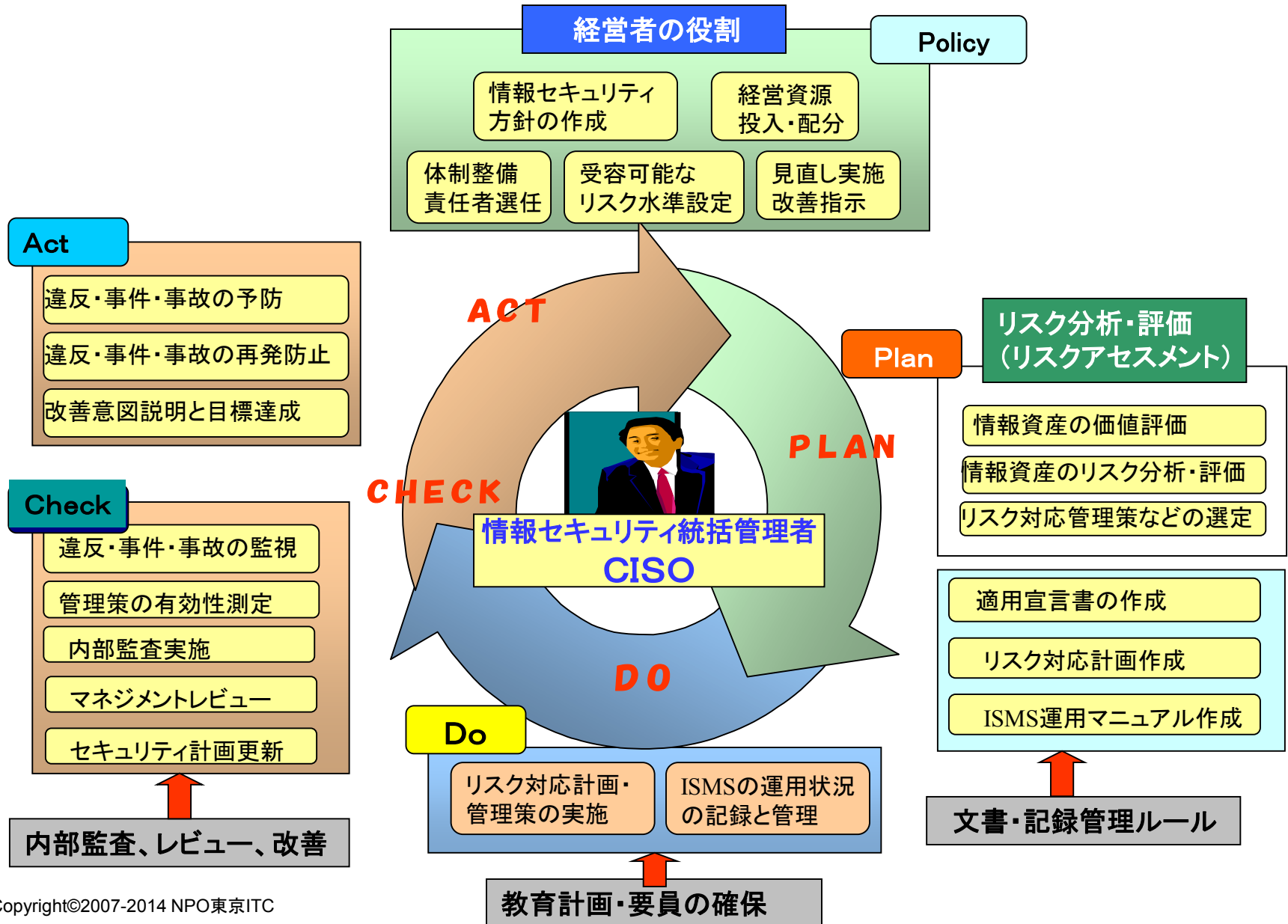
ISMS構築の準備（現状確認）

- 1.経営トップによるISMS構築の宣言
- 2.構築プロジェクトの目標設定
適用範囲概略、期間、運営方針、責任と権限、成果物
- 3.構築プロジェクトの編成
- 4.業種、企業規模、拠点配置の現状把握とセキュリティニーズ
業界ガイドライン調査
- 5.ITの活用状況、情報システム・インフラの運用状況の現状把握
- 6.情報セキュリティ対策の現状把握
- 7.予算措置の検討、審査機関の検討

I SMS構築の準備（社内業務の仕組み調査）

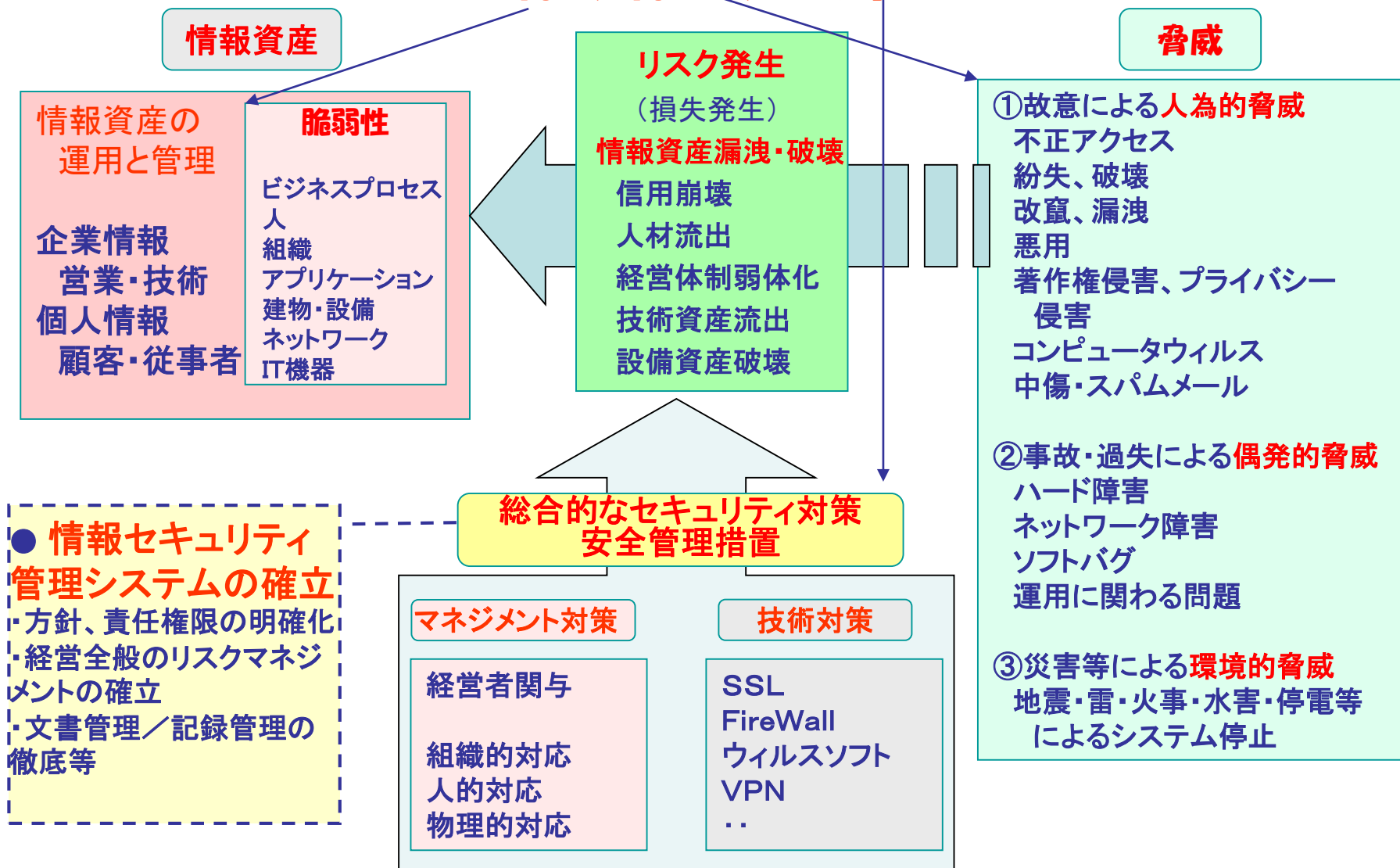
1. 社内組織図と社内委員会制度の概要
2. 業務分掌、職務規定、権限規定、稟議規定、意思決定プロセス
3. 業務記述書、業務マニュアル、業務フロー図
4. 就業規則、誓約書、入退出管理規則
5. 委託先契約書、守秘契約書、覚書、委託先選定基準
6. 委託元との契約書、守秘契約書、覚書
7. IT戦略・IT方針・IT計画、情報セキュリティポリシー（別途）
8. IT部門規定、IT開発規定・IT利用規定・IT運用規定
9. 全社システム体系図、ネットワーク図、導入システム・機器・ソフト台帳
10. ユーザマニュアル、操作マニュアル
11. システム概要説明書、システム仕様書、プログラム仕様書、運用マニュアル
12. システム運用記録、各種申請書、伺い承認記録帳票
13. システム各種変更記録（申請、承認）
14. その他システム関係書類（業務委託契約書、SLA、仕様書等）

ISMSが求めていること



情報セキュリティ・リスクへの体系的対応

何を、何から、どう守るか？



ISMSの標準構築プロセス

ISO27001ベース(改1)

ISMS確立フェーズ

2~3ヶ月

[P]

PJ準備

トップの関与

審査登録
機関決定

- ① 適用範囲境界定義
- ② ISMS基本方針策定
- ③ リスクアセスメント方針策定
- ④ リスクの識別
- ⑤ リスクの分析評価
- ⑥ リスク対応選択肢評価
- ⑦ リスク対応管理策選択
- ⑧ 残留リスク等の承認
- ⑨ 導入運用の経営陣の許可
- ⑩ 適用宣言書の作成

現状の情報資産・HW/SWなど

成果物例

- ① 適用範囲定義書
- ② 情報セキュリティ基本方針
・情報セキュリティ基本規定
- ④ 情報資産目録(台帳)
- ⑤ リスク評価シート
- ⑥ リスクアセスメント報告書
- ⑦ リスク対応シート
・情報セキュリティ対策規程
- ⑧ 残留リスク一覧
- ⑩ 適用宣言書

手順書例

- ・情報資産管理手順書
- ・リスクマネジメント手順書
- ・情報セキュリティ対策基準

ISMS導入・運用フェーズ

1~2ヶ月

[D]

- ① リスク対応計画策定
- ② リスク対応計画の実施
- ③ 管理目的・管理策の実施
- ④ 有効性測定方法規定
- ⑤ 教育訓練の実施
- ⑥ 運用状況の管理
- ⑦ 経営資源の管理
- ⑧ セキュリティ事件事故対応

- ① リスク対応計画書
・情報セキュリティ運営体制案
・事業継続計画書
- ⑤ 情報セキュリティ教育・訓練計画書
・情報セキュリティ教育・訓練報告書
- ⑥ 情報セキュリティ運用状況報告書
- ⑧ 情報セキュリティ事件・事故報告書

- ・情報セキュリティ教育・訓練手順書
- ・ISMS文書管理手順書
- ・その他手順書

ISMS監視・見直しフェーズ

1~2ヶ月

[C]

- ① 監視手順確立と実施
- ② ISMSの有効性見直し
- ③ 管理策の有効性測定
- ④ 残留リスク等の見直し
- ⑤ ISMS内部監査の実施
- ⑥ マネジメントレビュー実施
- ⑦ セキュリティ計画更新
- ⑧ ISMS実施状況の記録

- ⑤ 内部監査計画書
・内部監査実施報告書
- ⑥ マネジメントレビュー議事録
- ⑦ セキュリティ計画改訂版
- ⑧ ISMS実施報告書

- ・内部監査手順書
- ・内部監査チェックリスト
- ・運営委員会実施手順

ISMS維持・改善フェーズ

フェーズ2~3ヶ月

[A]

維持審査
更新審査

- ① ISMS改善策実施
- ② 是正・予防処置の実施
- ③ 実施処置の伝達・合意
- ④ 改善目標の達成

予備審査

登録審査

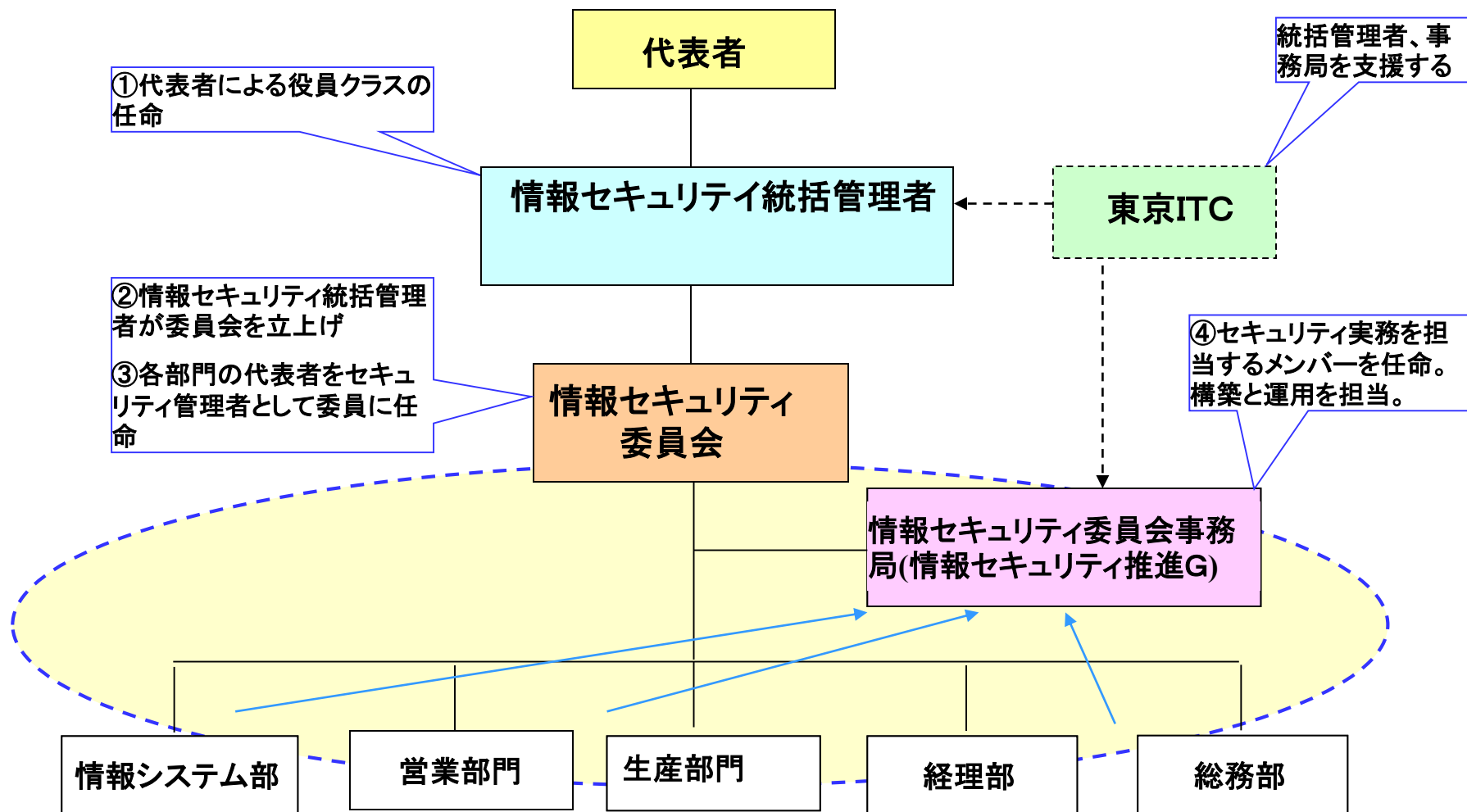
認証取得

- ① 改善計画/実施報告書
- ② 是正・予防処置報告書

ISMS文書体系

| | ISMS文書 | 実施記録等 | 関連規程・マニュアルにおけるセキュリティ関連事項 | 実施記録 |
|--------|------------------------------------------|-------------------------------------------|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| ポリシー | 情報セキュリティ方針 | ISMS構築稟議書 ISMS構築社内通達 | | |
| | 情報セキュリティ基本方針 情報セキュリティ基本規程 基本方針文書規程 | 情報セキュリティ方針書 ISMS適用範囲規程書 ISMS適用宣言書 | 情報システム構築規程 | 情報システム関連規程 情報システム取得・開発規程 物理・環境のセキュリティ管理規程 外部サービス規程 各種申請書 入退出管理記録 契約書・SLA |
| スタンダード | 情報セキュリティ対策規程 | リスク対応計画書 管理策別目標・有効性評価表 | 情報システム運用規程 | 基幹システム運用規程 利用者ID管理基準 ユーザ認証基準 ウィルス対策基準 バックアップ基準 暗号化管理規程 情報システム運用記録 アクセスログ 利用者ID申請書 特権パスワード管理台帳 |
| | 情報セキュリティ委員会規程 マネジメントレビュー規程 | 委員辞令 委員会議事録 レビュー議事録 | | バックアップ記録 |
| | セキュリティ事象対応規程 緊急時・異常時対応規程 | セキュリティ事象事故報告書 | 情報システム利用規程 | 情報資産調達規程 基幹システム利用規程 OAシステム利用規程 グループウェア等利用規程 安全管理規程 情報資産購入申請書 基幹システム利用申請書 |
| | 事業継続計画規程 | | | グループウェア等利用申請書 |
| | 適用法令規程 | | | |
| | ISMS教育規程 | 教育計画書 教育実施報告書 | 情報システム維持規程 | 変更管理規程 情報システム保守規程 保守報告書 |
| | ISMS内部監査規程 | 監査計画書 監査実施報告書 是正処置報告書 | ネットワーク管理規程 | 社内ネットワーク管理規程 外部ネットワーク利用規程 ネットワーク監視報告書 |
| | ISMS文書・記録管理規程 | 規程文書一覧 記録帳票一覧 | | |
| プロシジャー | 情報セキュリティ対策実施手順 | | | 業務関連規程 |
| | 情報資産管理手順書 リスクマネジメント手順書 | 情報資産調査票／台帳 情報資産目録 リスク管理票 残留リスク一覧 | 就業規則 職務規程 各種業務マニュアル 外注・購買管理規程 個人情報保護関連規程 その他社内規定 | 罰則規程 人的セキュリティ対策規程 個別業務別マニュアル 外部委託規程 外部委託先選定基準 各種規程・細則 社内稟議規程 誓約書(社員) 誓約書(外部) 職務定義書 各種手順書 外部委託契約書 秘密保持契約書 稟議書 |

I SMS構築の推進体制（例）



付 ISMS認証基準ver.2からISO27001への変更ポイント

| 項目 | ISO27001における要求事項 | 影響 |
|-------------------------------------------------------------------------------|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| 適用宣言書の見直し 4.2.1.j)2) | 「 現在実施されている管理目的と管理策 」を明らかにすること | <ul style="list-style-type: none"> ・適用宣言書の選択管理策に実施状況を追記 ・未実施の理由と予定の追記 |
| リスクマネジメントの見直し 4.2.1.c)2) | 「 リスクアセスメント 」の方法は 比較可能で再現可能 であること | <ul style="list-style-type: none"> ・リスクマネジメント手順の明文化 ・手順書の版管理 ・作業結果との紐付け |
| 管理策の有効性評価 4.2.2.d 4.2.3.c 4.2.3.d)5) 4.3.1.g) 7.2.f) 7.3.e) | 管理策を実施するだけでなく、「 管理策の有効性の評価とその監視・測定 」が加わった | <ul style="list-style-type: none"> ・管理策の有効性についての評価基準 評価方法 管理目標 監視・測定方法の設定運用 ・有効性評価を容易にする管理策のグルーピング |

| 項目 | ISO27001における要求事項 | 影響 |
|------------------------------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| セキュリティ事象の監視 4.2.3.a)4) A14.1.2 | セキュリティ事故・事件の「 予兆としてのセキュリティ事象 」を検出し、予防すること | <ul style="list-style-type: none"> ・ 予防措置体制の確立 ・ セキュリティ事象の定義 ・ 当該事象の監視方法明確化 ・ 当該事象の判定基準値設定 ・ 当該事象の監視、記録 |
| 第三者が提供するサービスの管理手順見直し A10.2 | 外注委託先の管理の強化要請により、「 アウトソーシング等のサービスレベル、監視、レビュー、変更管理の手順を明確化 」すること | <ul style="list-style-type: none"> ・ 提供サービスについて ・ サービスのセキュリティ管理策 ・ サービスの定義、SLA明確化 ・ 監視・監査 ・ 変更管理 |
| 全般 | 上記の変更に伴う整合性追加記録体制の確立 | <ul style="list-style-type: none"> ・ 規定の見直し ・ 追加記録帳票の準備 |