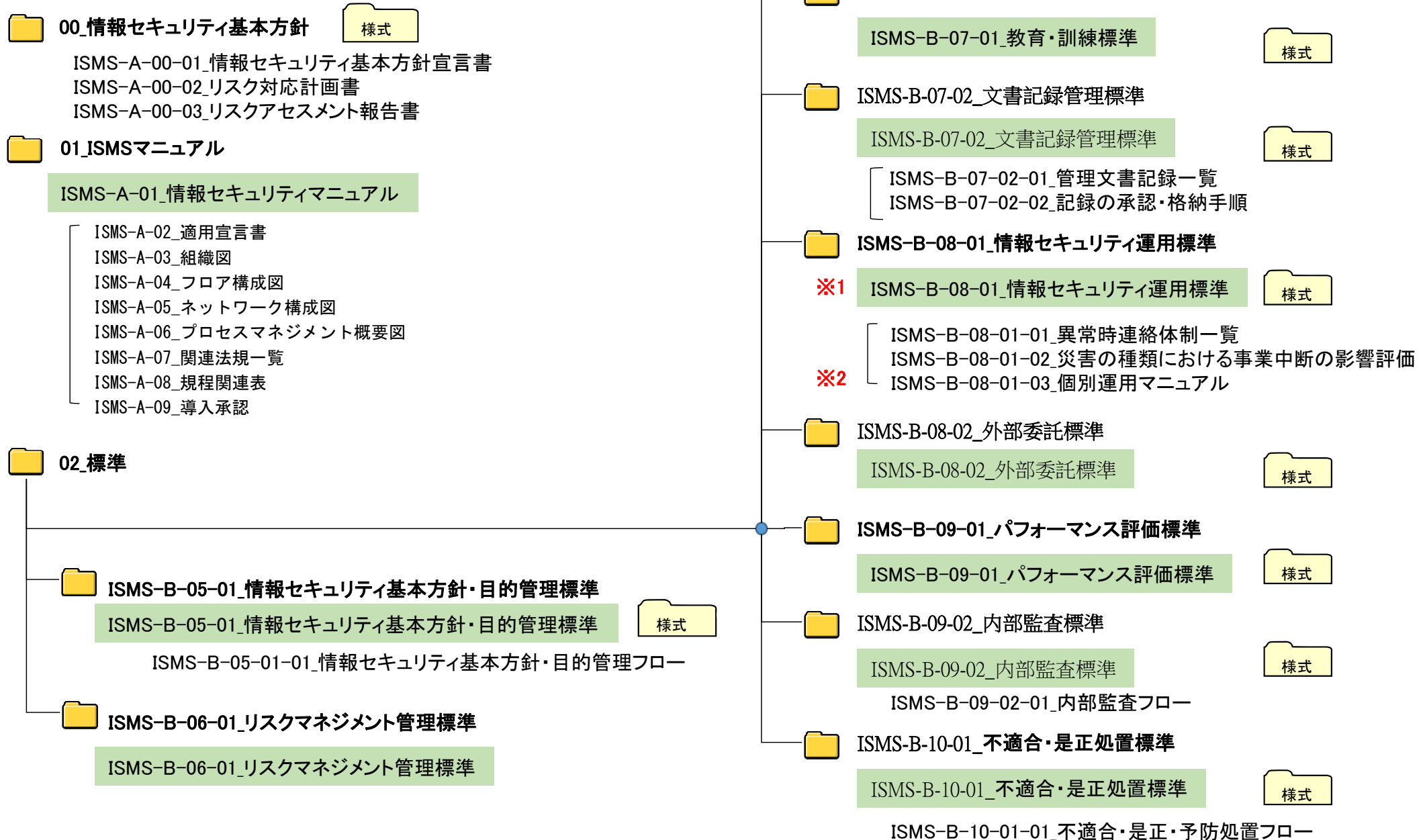


ISMS 管理文書 一覧 : 2014 (1/3)



※ リリース時には、構成、内容が一部変更、追加される場合があります。

※1 ISMS-B-08-01_情報セキュリティ運用標準

【組織 共通運用標準】

1. 施設への入退室

1.1 施設への入場

- (1) 適用部門への入場

1.2 作業エリアのセキュリティ

- (1) オフィス、部屋及び施設
- (2) セキュリティが保たれた領域での作業
- (3) 電子メールの取扱いについて
- (4) 電子オフィスシステムの取扱いについて

2. 情報資産の取扱い

- (1) 納品物の取扱い
- (2) 顧客借用資産の取扱い

3. 媒体の取扱いについて

- (1) 媒体の種類
- (2) 媒体の取扱い
- (3) 媒体の処分
- (4) 媒体の搬送

4. 携帯端末の利用

- (1) 携帯端末の所有
- (2) 携帯端末の利用
- (3) 社外からのリモート接続
- (4) 携帯端末の保管

5. アクセス制御

- (1) アクセス制御の方針
- (2) アクセス制御の対象
- (3) サーバへのアクセス制御
- (4) 運用端末へのアクセス制御
- (5) 接続経路の管理

6. 暗号化に関する方針

7. ソフトウェアの取扱い

- (1) ソフトウェアの導入・使用
- (2) ソフトウェアの管理
- (3) ソフトウェアの処分・譲渡
- (4) マルウェアの影響をうけた場合
- (5) ソフトウェアのインストールの制限

8. システムセットアップ作業手順書

9. 監視について

- (1) システム監視概要
- (2) システム監視対象
- (3) システム監視対象項目
- (4) システム監視方法と確認間隔
- (5) 監視ログ保管
- (6) 性能管理

10. 運用記録

- (1) 運用の記録
- (2) 記録の報告

11. 障害・事件・事故時の対応 (インシデント管理)

11.1 障害時の対応

11.2 セキュリティ事件・事故時の対応

- (1) 個人情報漏洩した場合
- (2) コンピューターウイルスに感染した場合

11.3 天災等の災害時の対応

- (1) 自然災害による場合

11.4 障害・事件・事故からの学習

- (1) セキュリティ事件からの学習
- (2) セキュリティ事件における証拠の収集

11.5 障害の検知

12. 事業継続計画

12.1 事業継続の管理

- (1) 目的
- (2) 適用範囲
- (3) 事業継続計画の策定
- (4) 事業継続計画の見直し
- (5) 事業継続計画の管理
- (6) 事業継続計画の周知
- (7) 情報セキュリティ委員会での検討
- (8) 記録

12.2 事業継続の手順

13. 法的要求事項遵守

- (1) 法的要求事項遵守の記録手順
- (2) 法令の見直し

ISMS-B-08-01_情報セキュリティ運用標準

※2 ISMS-B-08-01-03_個別運用マニュアル

【運用部門 個別標準】

※ 運用形態は組織によって多種多様です。
対象組織の運用形態に合わせ、本テンプレートを活用ください。

1. 施設入退室管理手順
2. 装置の保守手順
3. ハードウェアの管理手順
4. 備品等の鍵の管理手順
5. 技術的脆弱性に関する対策の手順
6. 運用業務装置起動・停止手順
7. ログインユーザID/パスワード設定、アクセス権の管理
8. PC時刻設定手順
9. バックアップ手順
10. ソフトウェア購入及びライセンス管理手順
11. プログラムソースコードの管理手順
12. 運用システムの変更管理手順
13. OS入替手順
14. 電子メールの使用基準
15. ホームページ管理手順
16. 第三者の提供するサービスの管理手順
17. 情報システムの監査手順
18. システムの監査ツールの保護手順
19. 監視ログの取得方法
20. 障害の検知方法
21. システム及び機器の障害対応(報告・復旧・リカバリー)手順
22. セキュリティに配慮したシステム開発のための手順
 - ① セキュリティに配慮したシステム開発方針
 - ② 開発プロジェクトのセキュリティ
 - ③ 開発システムのセキュリティ要求事項の管理
 - ④ 顧客借用資産の管理手順
 - ⑤ 開発ソフトウェアの正確な処理手順
 - ⑥ ソフトウェアの変更管理手順
 - ⑦ 外部委託による開発
 - ⑧ システムセキュリティの試験