ISMSの概要〈1〉

- 以下はISMSの要求事項の構成ですが、ここに注目しましょう。

0. 序文
1. 適用範囲
2. 引用規格
3. 用語および定義
4. 情報セキュリティマネジメントシステム
4.1 一般要求事項
4.2 ISMSの確立および運営管理
4.3 文書化による要求事項
5. 経営陣の責任
5.1 経営陣のコミットメント
5.2 経営資源の運用管理
6. ISMS内部監査
7. ISMSのマネジメントレビュー
7.1 一般
7.2 レビューへのインプット
7.3 レビューからのアウトプット
8. ISMSの改善
8.1 継続的改善
8.2 是正処置
8.3 予防処置 ★

8.3 予防処置
（略）
予防処置の優先順位は，
リスクアセスメントの結果に基づいて
決定しなければならない。

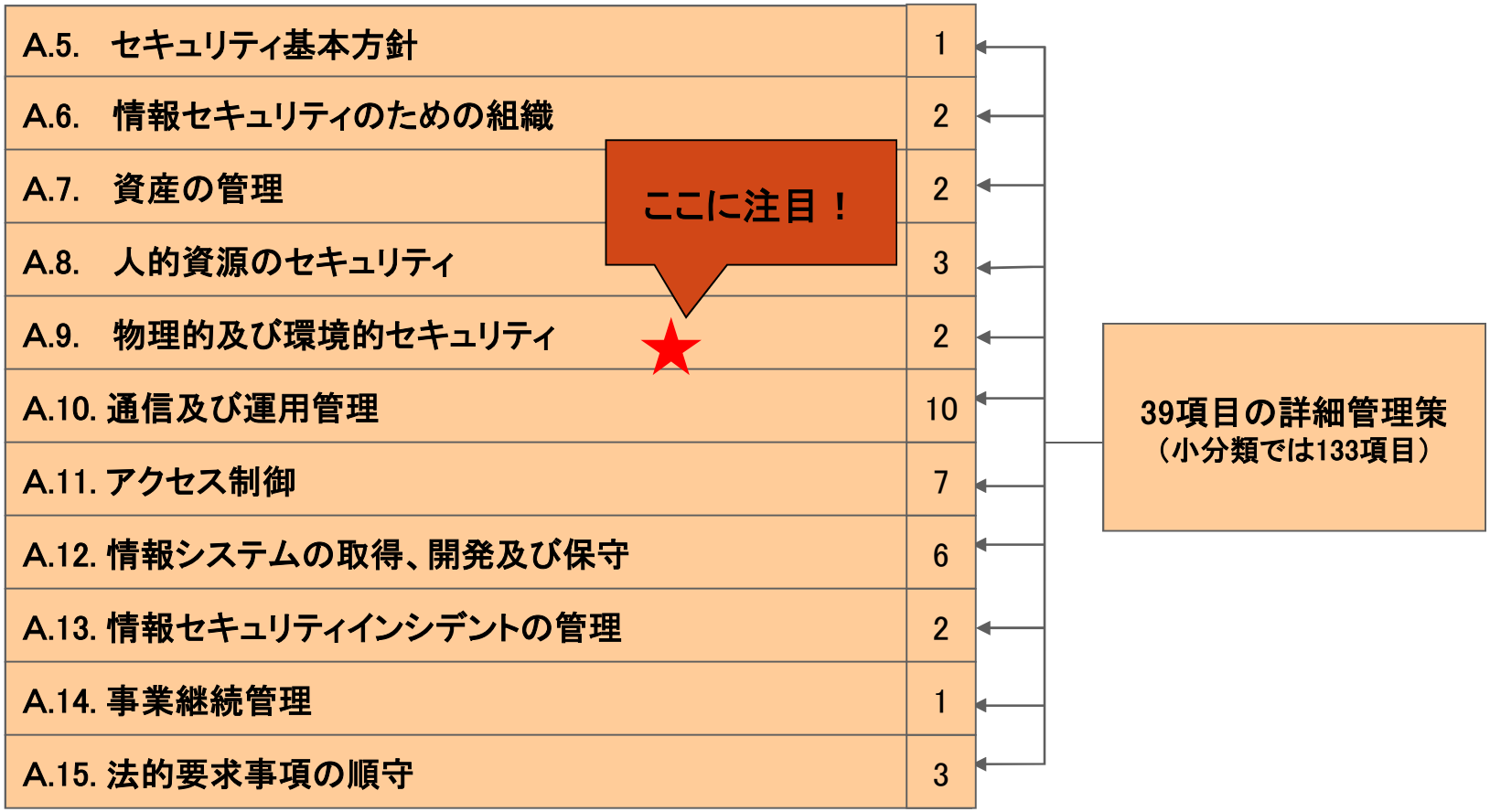
注記 不適合を予防するための処置は，多くの場合，是正処置よりも費用対効果が大きい。

（ISO/IEC 27001：2005より引用）

是正処置よりも予防処置の方が
効果がある、ということを言っています。
レイアウトについてもリスクを分析しましょう！

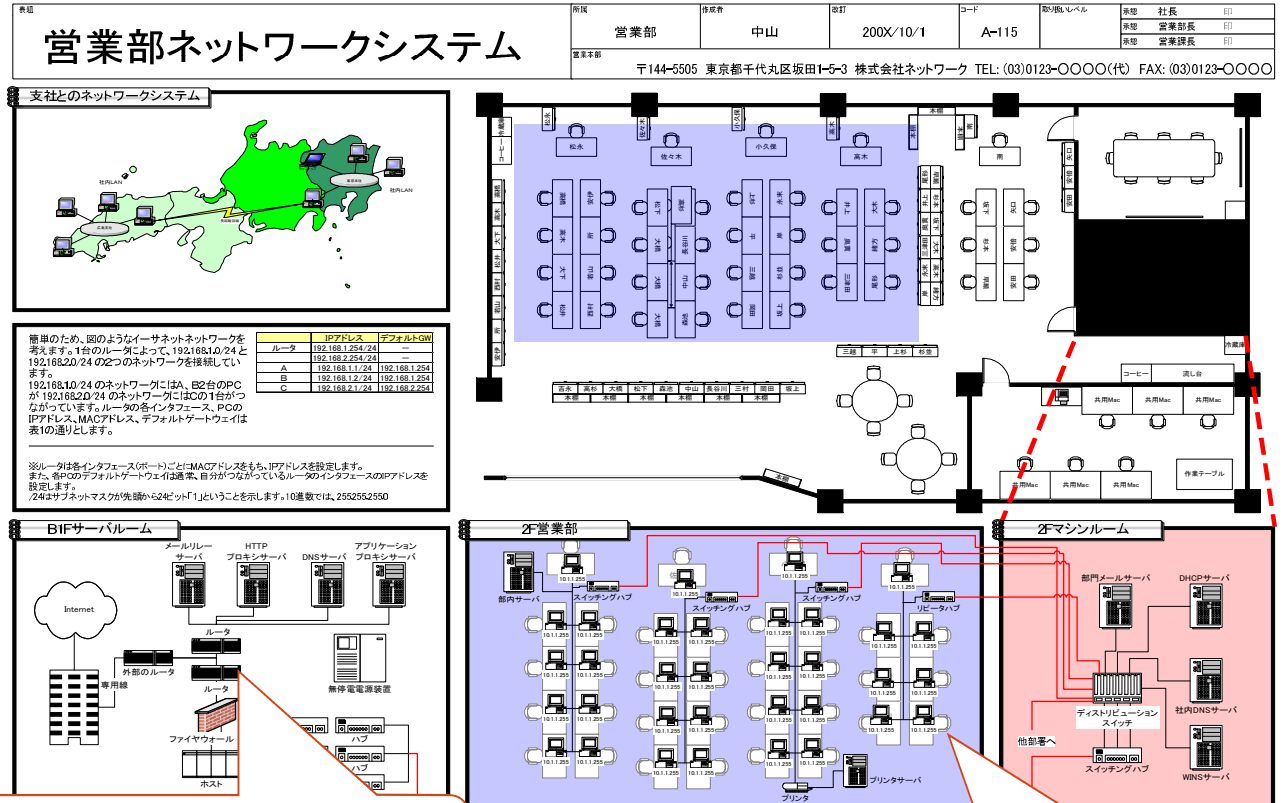
ISMSの概要〈2〉

- リスクアセスメントに基づき、以下の管理策を選択して実施します。



ISMSのポイント

- 情報セキュリティの脆弱性を探って問題点を解決する仕組みです。



パスワードはきちんと 割り当てられていますか？

レイアウトは大丈夫ですか？

まとめ

- ISMSは、リスクマネジメントのツールです。
- すなわち、事業を継続する上で欠かせない予防処置と言えます。
  事後処理では、取り返しのつかないことになる危険性が高いのです。
- 組織によって、対応できるリスク対策は異なります。自組織にとって、リスクとは何かを明確化させ、リスク発生の要因を洗い出し、対策と効果を認識しましょう。それに基づき、ISMSを確立させます。
  身の丈に合ったシステムを構築することがポイントです。
- 情報セキュリティ向上の最も重要なポイントは、人的セキュリティの向上です。教育が全ての基本となります。