ISMS と
ISO27001 の違い

同じもの？本当の関係性とは

仕組み・規格・制度・管理策 93 を解説



同じものでしゅよね？

仕組みと規格、別物だ。



【解説に入る前に】サービスのご紹介

セキュリティプロ・フリーランス

セキュリティに特化したフリーランス案件の
マッチングサービス

- 最高月収 150 万円・月額 80 万円以上の案件が 80% 以上
- リモート率 80% 以上、フルリモート案件多数
- セキュリティに精通した専任エージェントが営業・単価交渉・契約を代行

詳細を見る →

セキュリティプロ・テンショク

セキュリティエンジニア / コンサルタントに
特化した転職エージェント

- 最高想定年収 1,200 万円・利用者の 85% 以上が年収アップ
- 取扱求人の約 7 割が非公開求人
- 技術がわかるアドバイザーが書類添削・面接対策・年収交渉を代行

詳細を見る →

**どちらも登録・利用は完全無料。在職中・フルリモート希望でも相談できます。
まずは市場価値の無料相談から。**

© 2026 スプラッシュエンジニアリング

ISMS と ISO27001 の本質的な違い

ISMS

情報を守る仕組み

- リスクを見極め対策を回す
- 認証なしでも存在しうる
- PDCA サイクルが実体

VS

ISO/IEC 27001

ISMS の要求事項の規格

- 良い ISMS を測るものさし
- 要求事項の基準集
- 第三者審査の判断基準



関係の核心

規格が審判、 ISMS が主役だ。逆に考えるな。

混同しがちな 3 つの用語を整理する

ISMS

情報資産を守る仕組みそのもの。運用として存在する。



ISO/IEC 27001

ISMS が満たすべき要求事項。文書としての基準集。

ISMS 適合性評価制度

適合を審査・認証する制度の枠組み。

仕組みを整えたいのか認証を取りたいのか、目的で使い分けろ。



Pマークと ISMS の違いは守る対象

Pマーク

個人情報保護に特化

- JIS Q 15001 が基準
- 事業者全体が対象
- 国内中心の認定制度

VS

ISMS （ISO27001）

全情報資産が対象

- ISO/IEC 27001 が基準
- 部門・事業単位でも取得可
- 国際的に通用する



選択の核心

守る対象で選べ。個人情報ならPマーク、全資産なら ISMS 。

アドオン規格の位置づけ



ISO/IEC 27017

クラウド管理策を追加。 ISMS 前提のアドオン認証。



ISO/IEC 27701

個人情報管理（ PIMS ）認証。単独取得も可。



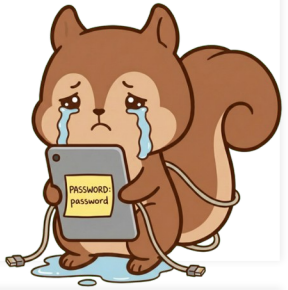
アドオンの核心

27017 は ISMS が前提。 27701 は単独取得可。

管理策が 114 から 93 へ再編された内容

114→93 に整理

重複を統合して圧縮。対応範囲は広がっている。



4 カテゴリに再分類

組織的・人的・物理的・技術的管理策に整理。

改訂の核心

数は減った、やることは増えた。 114 で止めるな。

新設された 11 の管理策

1. **脅威インテリジェンス**
   5.7 - 脅威情報の収集と分析活用
2. **クラウドサービス管理**
   5.23 - クラウド利用の情報セキュリティ
3. **ICT 事業継続の備え**
   5.30 - 事業継続のための ICT 準備
4. **物理的監視**
   7.4 - 物理的セキュリティの監視強化
5. **構成管理**
   8.9 - IT 資産の構成情報を一元管理
6. **情報の削除**
   8.10 - 不要になった情報の適切な削除
7. **データマスキング**
   8.11 - 機密データの匿名化・仮名化
8. **データ漏えい防止**
   8.12 - DLP によるデータ流出対策
9. **監視活動**
   8.16 - 異常の検知・対応体制の整備
10. **ウェブフィルタリング**
    8.23 - 悪意あるサイトへのアクセス制御
11. **セキュアコーディング**
    8.28 - 開発時のセキュリティ実装

認証取得の流れと期間の目安

準備フェーズ

現状把握・文書化・体制構築に 3 〜 6 か月。

審査フェーズ

内部監査〜第二段階審査まで 2 〜 3 か月。

継続の核心

取って終わりではない。 3 年ごとの更新審査が続く。

費用は初期と維持に分けて把握する

初期費用

コンサルティング

文書化・体制構築を支援する外部費用

審査費用

第一・第二段階審査の認証機関報酬

社内教育

従業員トレーニング・研修コスト

年間維持費用

維持審査費用

毎年のサーベイランス審査費用

運用人件費

内部監査・管理策の継続運用コスト

更新審査費用

3 年ごとの認証更新審査費用

ISMS 運用スキルのキャリア価値

評価される実務経験

リスクアセスメント設計・内部監査・審査通過の実績。



希少性が生む市場評価

審査を通せる人材は少なく、 GRC 領域で高評価。

希少性の核心

知識は多くの人が持つ。審査を通した経験が差を生む。

フリーランス案件の月額単価レンジ

職種別中央値

要件定義
中央値 115 万円（70 ～ 180 万円）

PMO
中央値 100 万円（65 ～ 130 万円）

設計・構築
中央値 92.5 万円（65 ～ 180 万円）

運用実績が単価を上げる



ISMS 関連で求められるスキル

審査対応支援
文書化・適用宣言書の整備

内部監査実施
是正のフォローまで完結させる経験

新管理策の知見
DLP ・脅威インテリジェンスの実務力

まとめ

- ISMS は仕組み、 ISO27001 は規格。上下関係であり二択ではない
- 管理策は 93 ・ 4 カテゴリに再編済。 114 で止めていると現場で通用しない
- ISMS 運用実績は中央値 92.5 万円の案件単価に直結する希少スキル

NEXT ACTION

まずは市場価値の無料相談・登録

セキュリティプロ・フリーランス ＞

セキュリティプロ・テンショク ＞

