**ISO 27002 情報セキュリティ
ガイドライン チェックリスト テンプレート**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ISO 27001 管理番号** | **ランク** | **優先度** | **所有者** | **割り当て日** | **期日** | **遵守していますか？** | **ステータス** | **備考** |
| **5. セキュリティ ポリシー管理** |
| 5.1 - 経営陣からコンプライアンスに対する指示やサポートがありましたか？ |  |   |  |   |   |   |  |   |
| **6. 企業セキュリティ管理** |
| 6.1 - 内部情報セキュリティ タスク フォースは立ち上げられていますか？ |   |   |   |   |   |   |  |   |
| 6.2 - 組織のモバイル デバイスやネットワークを保護するための対策は講じられていますか？ |   |   |   |   |   |   |  |   |
| **7. 人的セキュリティ管理** |
| 7.1 - 雇用前にセキュリティを確認するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 7.2 - 雇用中のセキュリティを確保するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 7.3 - 退職時のセキュリティを確保するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| **8. 組織の資産管理** |
| 8.1 - 企業資産に関するポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 8.2 - 情報分類の方法に関するポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 8.3 - 物理的なメディアを制御するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| **9. 情報アクセス管理** |
| 9.1 - ビジネス要件の情報アクセス管理に関するポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 9.2 - 全ユーザーのアクセス権を管理するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 9.3 - ユーザー認証に関するポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 9.4 - システムへのアクセスを制御するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| **10. 暗号化ポリシーの管理** |
| 10.1 - 暗号化された制御およびキーの使用を管理するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| **11. 物理的セキュリティ管理** |
| 11.1 - 物理的セキュリティ管理に関するポリシーは確立されていますか？  |   |   |   |   |   |   |  |   |
| 11.2 - 組織の設備を保護するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| **12. 運用上のセキュリティ管理** |
| 12.1 - 運用上のセキュリティ管理の手順および責任に関するポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 12.2 - 組織をマルウェアから保護するためのポリシーは確立されていますか？  |   |   |   |   |   |   |  |   |
| 12.3 - 定期的にバックアップ コピーを作成するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 12.4 - ログを使用してセキュリティ イベントを記録するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 12.5 - 組織の運用ソフトウェアを制御するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 12.6 - 組織の技術的な脆弱性に対処するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 12.7 - 監査アクティビティの影響を最小限に抑えるためのポリシーは実施されていますか？ |   |   |   |   |   |   |  |   |
| **13. ネットワーク セキュリティ管理** |
| 13.1 - ネットワークおよび施設を保護するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 13.2 - 情報転送を保護するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| **14. システム セキュリティ管理** |
| 14.1 - 情報システムの本質的な部分のセキュリティを確保するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 14.2 - システム開発アクティビティを保護・制御するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 14.3 - システム テストを目的として使用されるデータを保護するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| **15. サプライヤーとの関係管理** |
| 15.1 - サプライヤーとセキュリティ契約を締結するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 15.2 - サプライヤーのセキュリティとサービス デリバリを管理するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| **16. セキュリティ インシデント管理** |
| 16.1 - 情報セキュリティ インシデントを特定し、対応するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| **17. セキュリティの継続性管理** |
| 17.1 - 情報セキュリティの継続性を管理するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 17.2 - 情報処理施設の冗長性構築のためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| **18. セキュリティ コンプライアンス管理** |
| 18.1 - 法的セキュリティ要件を遵守するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |
| 18.2 - セキュリティ コンプライアンスのレビューを実行するためのポリシーは確立されていますか？ |   |   |   |   |   |   |  |   |

**– 免責条項 –**

Smartsheet がこの Web サイトに掲載している記事、テンプレート、または情報などは、あくまで参考としてご利用ください。Smartsheet は、情報の最新性および正確性の確保に努めますが、本 Web サイトまたは本 Web サイトに含まれる情報、記事、テンプレート、あるいは関連グラフィックに関する完全性、正確性、信頼性、適合性、または利用可能性について、明示または黙示のいかなる表明または保証も行いません。かかる情報に依拠して生じたいかなる結果についても Smartsheet は一切責任を負いませんので、各自の責任と判断のもとにご利用ください。

このテンプレートはサンプルとしてのみ提供されています。このテンプレートは、決して法的またはコンプライアンス上のアドバイスを意味するものではありません。このテンプレートのユーザーは、必須の情報および目的を達成するために必要な情報を見極める必要があります。