情報セキュリティ関連規程

株式会社はじめての LangChain

Ver. 1.0|改訂日：2025-06-22

目次

組織的対策

適用範囲：全社・全従業員

1.1 情報セキュリティ委員会の設置

- 代表取締役を委員長とする「情報セキュリティ委員会」を設置し、全社的な情報セキュリティ対策を統括する。
- **委員会構成（例）**

役職	役割
情報セキュリティ責任者（代表取締役）	対策方針決定・最終責任者
部門責任者（各部長）	自部門の運用管理責任
システム管理者	技術的対策の導入・運用

教育責任者	社員教育の企画・実施
監査責任者	規程遵守状況の監査・報告
インシデント対応責任者	インシデント対応指揮

1.2 監査と改善

- 監査責任者は年 1 回、規程の遵守状況を点検し、委員会へ報告する。
- 不備が判明した場合、委員会は改善計画を策定し、経営層へ報告する。

1.3 情報共有

- IPA／JPCERT/CC など外部機関からの脅威情報を収集し、必要に応じて社内周知する。

人的対策

適用範囲：全従業員（役員・正社員・契約社員・派遣・アルバイトを含む）

12. **雇用条件**入社時に秘密保持契約（NDA）を締結する。
13. **従業員の責務**規程違反時の懲戒は就業規則に基づく。営業秘密・個人情報を無断で第三者へ提供しない。
14. **雇用終了時**退職時にすべての機密情報・媒体を返却／消去する。
15. **教育・啓発**年次でセキュリティ教育計画を策定し、入社時・定期で実施。フィッシング・標的型攻撃等の最新脅威を随時周知。
16. **人材育成** IPA 情報処理安全確保支援士／情報セキュリティマネジメント試験など資格取得を推奨。

- 入社時に秘密保持契約（NDA）を締結する。
- 規程違反時の懲戒は就業規則に基づく。
- 営業秘密・個人情報を無断で第三者へ提供しない。
- 退職時にすべての機密情報・媒体を返却／消去する。
- 年次でセキュリティ教育計画を策定し、入社時・定期で実施。
- フィッシング・標的型攻撃等の最新脅威を随時周知。
- IPA 情報処理安全確保支援士／情報セキュリティマネジメント試験など資格取得を推奨。

情報資産管理

適用範囲：全社・全従業員

17. **情報資産の特定と機密性評価**「情報資産管理台帳」を整備し、機密性を 3（極秘）～1（公開）で評価。
18. **分類表示**電子データ：保存フォルダ名に機密区分を付与。書類：バインダ背表紙等に機密区分を表示。
19. **社外持出し**社外秘：部門長承認、極秘：代表取締役承認。媒体持出し時は暗号化と物理管理を徹底。
20. **媒体処分・再利用**廃棄：紙は裁断、電子媒体は破壊または専用ツールで完全消去。再利用：完全消去後のみ可。
21. **バックアップ**対象・方法・保管先を台帳化し、定期的にリストアテストを実施。

- 「情報資産管理台帳」を整備し、機密性を 3（極秘）～1（公開）で評価。
- 電子データ：保存フォルダ名に機密区分を付与。
- 書類：バインダ背表紙等に機密区分を表示。
- 社外秘：部門長承認、極秘：代表取締役承認。
- 媒体持出し時は暗号化と物理管理を徹底。
- 廃棄：紙は裁断、電子媒体は破壊または専用ツールで完全消去。
- 再利用：完全消去後のみ可。
- 対象・方法・保管先を台帳化し、定期的にリストアテストを実施。

アクセス制御及び認証

適用範囲：機密情報を扱うシステムおよび利用者

22. **最小権限の原則**– 業務に必要な最小限のアクセス権を付与。
23. **個人アカウントの義務化**– 共用アカウントは禁止。
24. **パスワードポリシー（例）**一般：10 文字以上、大文字・小文字・数字・記号を混在。特権：12 文字以上、過去 1 年間の再利用禁止。ロックアウト：5 回連続失敗で 1 時間停止。
25. **端末認証**– 無線 LAN は MAC／証明書認証を併用。
26. **アカウント管理**– 不要アカウントは翌営業日までに無効化。

- 一般：10 文字以上、大文字・小文字・数字・記号を混在。
- 特権：12 文字以上、過去 1 年間の再利用禁止。
- ロックアウト：5 回連続失敗で 1 時間停止。

物理的対策

適用範囲：全事業所

レベル	対象エリア	入退室管理	備考
1	受付・応接室	最終退室者が施錠	機密書類放置禁止
2	執務室・工場	入退室記録、警備会社通報	来客用名札必須
3	サーバールーム	常時施錠、監視カメラ	モバイル媒体持込禁止

IT 機器利用

27. **標準ソフトウェアのみ利用。**追加導入はシステム管理者承認。
28. **ウイルス対策**– 定義ファイル自動更新、外部媒体接続時は全スキャン。
29. **クリアデスク／クリアスクリーン**– 離席時は画面ロック、退社時は施錠保管。
30. **インターネット利用**– 不審サイトはフィルタリング。社外秘送信時は暗号化。
31. **私有デバイス**– 業務利用は禁止／事前承認制。（※どちらか選択）

IT 基盤運用管理

32. **パッチ管理**– OS／ミドルウェアは月例で更新、緊急パッチは 14 日以内。
33. **ログ管理**– 通信・イベントログを 3 年保存。
34. **クラウドサービス評価**– ISMS 認証等を確認し、責任分界を明確化。
35. **機器廃棄**– データ完全消去証明書を取得。

システム開発及び保守

36. **開発工程**– 要件 → 設計 → 実装 → テスト → 承認 → 本番。
37. **脆弱性対策**– OWASP Top 10 等を考慮、静的／動的解析を実施。
38. **環境分離**– 開発・テスト・本番を物理／論理的に分離。

39. **変更管理**– 影響分析・バックアウト手順を文書化。

委託管理

40. **委託先評価**– ISMS／P マーク取得等の基準で選定。
41. **契約条項**– 守秘義務・再委託制限・事故報告・終了時返却／消去を明記。
42. **定期評価**– 「委託先対策状況確認リスト」で年 1 回確認。

情報セキュリティインシデント対応及び事業継続管理

43. **体制**– 代表取締役（最高責任者）、インシデント対応責任者、システム管理者。
44. **報告フロー**– 発見 → 責任者報告 → 影響分析 → 是正処置 → 再発防止。
45. **事業継続計画（BCP）**– 重要業務復旧時間目標（RTO）を設定し、年 1 回訓練。

テレワークにおける対策

46. **接続**– 会社支給端末＋ VPN 必須、多要素認証を利用。
47. **作業環境**– 覗き見防止、家族等の端末共用禁止。
48. **媒体持出し**– 極秘情報のローカル保存禁止、クラウド暗号化ストレージを使用。