4. 継続的な改善と適応（長期：恒常的に実施）

（1）定期的なセキュリティ監査と脆弱性管理

- **自社システムの安全性を常に点検**
  導入したセキュリティ機器や運用ルールが、現在の脅威に対応できているかを**定期的（例：年 1～2 回）に診断・監査**します。
- **実施内容の例**
  - ソフトウェアや OS の更新状況の確認
  - ID・パスワードの管理方法チェック
  - 不要アカウント・アクセス権の棚卸し
  - 外部からの侵入テスト（ペネトレーションテスト）
- **脆弱性への対応フローの確立**
  診断で発見された脆弱性には**速やかにパッチ適用・設定変更・システム更改**などの対応を行い、その記録を残すことで監査証跡としても活用できます。

（2）最新情報の継続的なキャッチアップ

- **法制度・技術・脅威動向の定期収集**
  民事訴訟の電子化に関連する**法律・運用の変更、脆弱性情報、ツールのアップデート**などに継続的に目を配ります。
- **情報収集の方法例**
  - 日本弁護士連合会、法務省、IPA（情報処理推進機構）のウェブサイト
  - 専門誌（「ビジネス法務」「LEGAL TECH」など）
  - サイバーセキュリティベンダーや IT 系メディアのニュースレター
  - ChatGPT やニュースアラートを活用した自動収集も有効
- **所内での共有体制の構築**
  収集した情報を**所内で週報・月報として共有**し、関係者が知識をアップデートし続けられる仕組みをつくります。

（3）クライアントへの情報提供とサポート

- **依頼者への信頼構築の一環として**
  デジタル訴訟対応や情報管理体制を強化していることを、**クライアントにも適切に伝える**ことで、信頼性・安心感の向上につながります。
- **提供可能な内容の例**
  - 電子申立てに関する手続き説明

  - 電子証拠提出における形式・留意点の案内
  - ウェブ尋問の準備・環境確認のサポート
  - 個人情報や機密情報保護体制の説明
- **情報発信の手段**
  - 月 1 回のニュースレターやメールマガジン
  - 事務所ウェブサイトでの「デジタル対応方針」公開
  - 訪問時の案内文書やチェックリスト配布

まとめ

「継続的な改善と適応」は、事務所が**時代の変化に遅れず、かつ安全で信頼性の高い法務サービスを維持するための必須プロセス**です。システム導入後の運用が始まったら、それを定期的に見直し、柔軟に変化へ対応する力が求められます。