

3. 実践と継続的改善

(1) 裁判 IT 化に関する実務研修への参加

- **最新情報の取得と実務スキルの習得**

電子訴訟・ウェブ尋問・電子証拠提出のルールは今後もアップデートされる可能性があります。日本弁護士連合会や各地の弁護士会の研修、法務省の公開資料などを通じ、継続的なスキルアップが必要です。

- **対象職員の拡大**

弁護士だけでなく、事務職員・パラリーガルも研修対象に含めることで、事務所全体での対応力を底上げできます。

(2) インシデントレスポンス計画(IRP)とサイバーBCP の策定・訓練

- **IRP(インシデントレスポンス計画)とは**

サイバー攻撃や情報漏えいが発生した際に、誰が・何を・どう対応するかを明文化したマニュアルです。初動対応の遅れが被害を拡大させるため、計画と訓練が必要です。

- **サイバーBCP(事業継続計画)**

システム障害や攻撃により通常業務が停止した場合でも、業務継続・復旧を可能にするための計画です。たとえば、「事務所が使えない場合のリモート業務体制」や「クラウドバックアップからの復元手順」などを記載します。

- **定期的な訓練と見直し**

年 1 回以上の模擬訓練(例: マルウェア感染対応演習)を行い、計画の実効性を確認・改善します。

(3) AI 利用に関するガイドラインの策定と教育

- **ChatGPT や AI アシスタントの利用が拡大**

文書作成や調査、証拠の整理補助などに AI が活用される場面が増えていますが、誤情報のリスクや個人情報漏えいの懸念もあります。

- **AI ガイドラインの主な内容例**

- AI を業務で使用する場合の承認フロー
- クライアント情報の入力制限
- 生成物の法的責任や確認義務の明確化
- 無断使用の禁止と教育訓練の義務化

- **事務所内での研修実施**

定期的に AI のリスク・活用法に関する研修を行い、安全で有効な運用を確立します。

(4) 国際的なデータ保護規制への対応(該当する場合)

- **外国人依頼者・海外関係訴訟に関わる場合**
欧州の GDPR や米国の CCPA など、国際的なデータ保護規制に違反すれば重大な法的リスクを伴います。
 - **対応のポイント**
 - クライアント情報の取得・保存・削除に関する規定の整備
 - 海外送信時の暗号化や同意取得
 - 規制対象データの識別と管理
 - **対応すべきケースの整理**
自社の業務範囲と照らし、「海外在住クライアント」や「外資系企業の訴訟案件」など該当する場合のみ、重点的に対応を進めることが現実的です。
-

(5) サイバー保険の検討

- **損害の補償と専門家のサポート確保**
万が一情報漏洩やサイバー攻撃が発生した場合、損害賠償金・対応費用・広報対応など多大な費用が発生します。サイバー保険はこれらの補償と、弁護士・セキュリティ専門家の派遣支援などを含む場合もあります。
 - **検討時のポイント**
 - 補償範囲(ランサムウェア、漏洩、訴訟など)
 - 対応スピード(24 時間緊急対応可など)
 - 自社の情報資産規模や取り扱う機密性に応じたプラン選定
-

まとめ

この「実践と継続的改善」のフェーズでは、導入したシステムをどう安全に、長期的に活用し続けるかが最大の課題です。トラブル時の対応力・最新技術への適応力・組織の学習力が問われる段階であり、定期的な見直し・訓練・情報収集が成功の鍵となります。