プロセス 1. 情報収集と対応範囲の検討

民事訴訟手続のデジタル化に対応するには、技術的な整備だけでなく、職員全体の理解・意識・行動を見直す必要があります。これにより、安全かつスムーズな運用が実現します。

(1) 改正民事訴訟法の理解と情報収集

- **背景と目的の理解**

デジタル化は、訴訟手続の迅速化・効率化・利用者利便性の向上を目的としています。改正法では、電子申立て・電子納付・オンライン送達・ウェブ尋問などが新たに導入されます。
 - **法改正情報の継続的な把握**

日弁連や各地の弁護士会が発信するガイドライン・研修・ニュースレターを継続的にフォローし、運用方法・法的リスク・スケジュールなどを常に最新の状態に保つ必要があります。
-

(2) 情報セキュリティポリシーの策定

- **セキュリティのルール作り**

電子申立てやクラウド利用の増加により、外部からのサイバー攻撃や情報漏洩リスクが高まります。まず、事務所の情報資産の棚卸しとリスク分析を行い、それをもとにセキュリティポリシーを明文化します。
 - **策定すべき主な内容**

例：
- アクセス権限管理
- パスワード管理基準
- USB や私物 PC の取り扱いルール
- クラウドサービス利用基準
- インシデント対応手順
 - **全員への共有と周知徹底**

一度策定しただけでは不十分です。全職員に説明し、理解・同意を得たうえで日常業務に定着させることが重要です。
-

(3) 全職員へのセキュリティ意識向上教育と、必要なセキュリティ基盤の検討

- **知識の習得だけでなく“慣れ”の形成も重要**

フィッシングメールやマルウェアの巧妙化に伴い、技術だけで守れない部分＝“人”の意識の強化が求められます。
- **実施すべき教育内容の例**
 - セキュリティ基礎知識(IPA 推奨教材など活用)
 - 電子訴訟システムの操作体験

- フィッシング詐欺の見分け方
 - 実際の事例に基づくケーススタディ
 - **定期的な訓練・テスト**
 - 年 1 回の形式的な研修だけでなく、**模擬インシデント対応訓練**や**定期テスト・アンケート**を通じて、**実践力と意識を定着させることが推奨**されます。
 - **知識の習得や訓練を通じて、日々の対応が重要であることを認識し、必要なセキュリティ環境をチームとして検討**します。
-

補足:

デジタル化の導入は、手間やコストがかかる一方で、長期的には**事務の効率化・証拠管理の明確化・業務の標準化**に繋がる大きなチャンスです。全職員が「ただの IT 導入」ではなく、「**業務文化の転換**」であるという認識を持つことが、成功のカギとなります。