2. IT インフラとシステムの整備

裁判手続の電子化に対応するには、**セキュリティ・可用性・操作性の高い IT 環境**を整える必要があります。これにより、電子申立て、ウェブ尋問、証拠書類の提出・保管・閲覧などを安全かつ効率的に行えます。

---

(1) 安定稼働を第一とした‘止まらない’ネットワーク構築や見直し

- **安定したネットワーク回線の確保**
  電子訴訟システムやウェブ会議の使用には、高速かつ安定したインターネット接続が必要です。可能であれば**専用回線**や**冗長回線**を整備します。
- **ハードウェアの見直し**
  旧式の PC や周辺機器では最新のソフトウェアに対応できない可能性があります。**セキュリティ機能付きの PC やルーター、業務用 NAS（共有ストレージ）**など、適切な機材への更新が必要です。
- **無停電電源装置（UPS）やバックアップ体制の整備**
  突発的な停電・障害にも備え、業務を継続できるようにします。

---

(2) （必要であれば）デジタル文書管理システムの導入と移行

- **電子ファイルによる文書の一元管理**
  訴訟資料・証拠・依頼者とのやりとりなどをデジタルで保存・検索・共有できるよう、**クラウド型文書管理システム（DMS）**の導入が求められます。
- **紙文書からのスキャン・OCR 処理によるデータ化**
  既存の紙書類についても、可能な限り電子化し、全文検索・自動分類できる体制に移行します。
- **アクセス制限と履歴管理機能の確保**
  文書へのアクセス権を細かく制御できるシステムを選定し、不正閲覧や改ざんを防止します。

---

(3) （必要であれば）オンラインコミュニケーション・事件管理ツールの導入

- **ウェブ会議ツール（Zoom, Teams 等）**
  ウェブ尋問、打ち合わせ、依頼者との面談などに備え、セキュアで使いやすいツールを選定し、事務所内で運用ルールを定めます。
- **事件管理システム（CMS）**
  訴訟の進捗・スケジュール・期日・証拠・報酬などを一元管理できるツールを導入します。
  TreeeS、弁護士ドットコムのクラウドサービス等が選択肢です。
- **チャット・情報共有ツール**
  Slack や Chatwork など、安全なチャットツールによって所内の情報連携を迅速化します。

(4)(必要であれば)エンドポイントセキュリティの強化

- **端末ごとのセキュリティ対策の徹底**
  弁護士や事務員が使うPCやスマートフォンには、**ウイルス対策ソフト・ファイアウォール・暗号化・リモートワイプ機能**などを導入します。
- **私物端末(BYOD)への制限または管理強化**
  職員が私用端末を業務に使う場合は、MDM(モバイルデバイス管理)を導入してセキュリティを担保します。
- **OSやソフトの定期更新**
  Windows・macOSなどの基本ソフトやAdobe、Office等についても、**脆弱性対策として定期的なアップデートが必須**です。

---

(5)(必要であれば)ログ管理システムの導入

- **操作履歴・アクセス履歴の記録と監視**
  誰が、いつ、どのファイルやシステムにアクセスしたかを記録・保存し、不正操作や情報漏洩の早期発見に役立てます。
- **内部不正・ミスへの対応**
  職員による誤送信や誤操作も想定し、**ログを活用した事後検証・教育材料の提供**が可能な体制を整えます。
- **ログの改ざん防止・長期保存**
  改ざんができない形式(例:クラウド上で暗号化保存)や、3年以上の保存対応が可能なシステムを推奨します。

まとめ

技術面の整備は、「セキュリティ」「業務効率」「訴訟手続の正確性」のすべてに関わる重要な柱です。小規模事務所でも段階的に取り組むことができ、**無料ツールの活用やクラウドサービスの選定**など、コストと効果のバランスを見極めた導入がカギとなります。