

---

# 弁護士事務所向け ITリスク自己診断チェックシート【完全版】

---

事故を防ぐために、まず現状を整理する

# はじめに

このチェックは、「できている／できていない」を評価するものではありません。

現在の事務所運営を整理し、「気づき」を得るための資料です。



## 本資料の目的

- 本資料は、ITの知識や正解を問うテストではありません。
- ご自身の事務所の「現在の状態」を整理・可視化するためのチェックです。
- 完璧に答える必要はありません。



## 「分からない」は重要な回答です

- 「誰が担当しているか分からない」
- 「ルールがあるか分からない」

※ こうした状態そのものが、リスクに気づくための大切なサインです。



## ITトラブルは「技術」より「運用」で起きています

ITトラブルの多くは、  
次のような理由から起こります。

- 高度な技術が足りないからではありません。
- 最新ツールを使っていないからでもありません。

実際の原因は、

- 運用ルールが曖昧
- 誰が判断するか決まっていない

といった、日常的な運用の不明確さであることがほとんどです。



## チェックの使い方

- 本チェックは、ITシステムの技術的な優劣を測るものではありません。
- 事務所内で「誰が」「何を」「どのように」**管理・判断**しているかを整理するためのものです。
- 現状を把握することで、より安全な事務所運営に向けた一歩を踏み出すことを目的としています。

## ① 端末・アカウント管理 (1/2)



1. 業務に使うPC、スマートフォン、タブレットの範囲（事務所所有、個人所有）が明確に決まっている。

はい     いいえ     分からない



2. 個人所有の端末を業務で使う場合のルール（申請方法、セキュリティ対策の義務）が定められている。






はい     いいえ     分からない



3. 業務に使うPC、スマートフォン、タブレットにウイルス対策ソフトが導入され、常に最新の状態になっている。

はい     いいえ     分からない

## ① 端末・アカウント管理 (2/2)

-  4. 職員の入社の際に、PCや各種システムのアカウントを発行する手順が決まっている。  
 はい     いいえ     分からない
-  5. 職員が退職・異動する際に、利用していたアカウントを速やかに停止・削除する手順が決まっている。  
 はい     いいえ     分からない
-  6. 事務所で利用しているクラウドサービス（ファイル共有、Web会議）の一覧を把握している。  
 はい     いいえ     分からない
-  7. パスワードの作り方や管理に関する簡単なルール（使い回しをしない、生年月日にしない）がある。  
 はい     いいえ     分からない
-  8. 端末・アカウント管理の責任者が決まっている。  
 はい     いいえ     分からない

## ② データ管理・バックアップ (1/2)



9. 依頼者情報や事件記録など、重要データがどこに（例：事務所サーバー、特定のPC、クラウド）保存されているかを説明できる。

はい  いいえ  分からない



10. データの重要度に応じて、アクセスできる職員を制限している。

はい  いいえ  分からない



11. 重要なデータは定期的にバックアップ（複製を保存）している。

はい  いいえ  分からない

## ② データ管理・バックアップ (2/2)



12. バックアップを取得する頻度（例：毎日、週1回）を把握している。

はい  いいえ  分からない



13. バックアップデータは、元のデータとは物理的に別の場所（例：クラウド、事務所と違う地域）にも保管している。

はい  いいえ  分からない



14. 過去1年以内に、バックアップからデータを元に戻す（復元する）テストを試したことがある。

はい  いいえ  分からない



15. バックアップデータの保管場所の記録、復元方法に関する手順書が存在する。

はい  いいえ  分からない



16. データ管理・バックアップの責任者が決まっている。

はい  いいえ  分からない

### ③ ネットワーク・外部接続(1/2)



17. 事務所のインターネット回線や通信機器について、管理・設定を担当する人（または会社）が決まっている。

はい  いいえ  分からない



18. 事務所のWi-Fiは、職員が使うものと来客（お客様）が使うものを分けて設定している。

はい  いいえ  分からない



19. 事務所のWi-Fiに、セキュリティ設定を把握していない機器を接続していない。

はい  いいえ  分からない

### ③ ネットワーク・外部接続(2/2)



20. 外部（自宅、出張先など）から事務所内のデータにアクセスする方法を把握している。

はい  いいえ  分からない



21. 外部からアクセスする場合のルール（例：VPN接続が必須など）がある。

はい  いいえ  分からない



22. 公衆Wi-Fiなど、安全性が確認できないネットワークを利用して業務を行うことを禁止している。

はい  いいえ  分からない



23. 事務所のWi-Fiに、許可なく私物の機器（個人のPC・スマホ、ゲーム機）を接続させないルールがある。




はい  いいえ  分からない







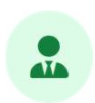
24. ネットワーク管理の責任者が決まっている。

はい  いいえ  分からない






## ④ 職員ルール・教育(1/2)

-  25. 情報の取り扱いやPC利用に関する、ルールを定めた書類（セキュリティポリシーなど）が存在する。
- はい     いいえ     分からない
-  26. 職員の入社の際に、事務所のIT利用ルールや情報管理の注意点を説明する機会がある。
- はい     いいえ     分からない
-  27. 職員が不審なメールを受信したり、PCのトラブルに遭った際に、相談できる担当者や窓口が決まっている。
- はい     いいえ     分からない

## ④ 職員ルール・教育(2/2)

-  28. PC操作に関して「やってはいけないこと」のルールがある。  
(例：生成AIの使い方、不審なメールの添付ファイルを開く、フリーソフトを勝手にインストールするなど)
- はい  いいえ  分からない
-  29. メール誤送信を防ぐための具体的な対策を行っている。  
(例：宛先を複数人で確認する、送信前に確認を促すツールを導入するなど)
- はい  いいえ  分からない
-  30. USBメモリなど、外部記憶媒体の利用に関するルールがある。(例：暗号化を必須とする、利用を原則禁止するなど)
- はい  いいえ  分からない
-  31. 定期的に(年1回など)、情報セキュリティに関する注意喚起や簡単な研修を行っている。
- はい  いいえ  分からない
-  32. 職員へのルール周知や教育の責任者が決まっている。
- はい  いいえ  分からない

## ⑤ トラブル時の対応体制

-  33. 「PCがウイルスに感染したかもしれない」といったITトラブルが発生した際の、初動対応（例：まずネットワークから切断する、担当者に報告するなど）が決まっている。
- はい     いいえ     分からない
-  34. システムや機器の保守を依頼している外部業者（ITベンダーなど）の連絡先が、すぐに分かるように整理されている。
- はい     いいえ     分からない
-  35. サイバー攻撃などによる情報漏えいの可能性がある場合に、相談できる専門家に心当たりがある。
- はい     いいえ     分からない
-  36. トラブル発生時に、事務所内での情報共有に関するルールがある。
- はい     いいえ     分からない
-  37. トラブル発生時に、最終的な判断を行うかの責任者が決まっている。
- はい     いいえ     分からない

# チェック結果の考え方

チェック結果で「いいえ」「分からない」が複数あった場合でも、それはITに関する知識やスキルが不足している、あるいはセキュリティ対策が「弱い」ことを直接意味するものではありません。

**IT事故の多くは、知識不足よりも「誰が判断するのか決まっていない」状態で起きています。**

本チェックは、事務所のIT運用や判断の「状態」を整理し、今後の対策を考えるための「気づき」を得ることを目的としています。

## ☰ チェック結果から “断定すべきでない”こと

- ITの技術力や知識が不足している
- セキュリティ対策が「弱い」
- 現時点で「問題がない」

## 💡 チェック結果から “考えられる”こと

(運用や判断の構造に関する示唆)

- 判断や管理の責任が、特定の一人に集中している
- 誰が責任を持つのが明確に決まっていない
- 小規模な事務所では、日常的に起こりやすい運用状態

## ☰ 注意喚起

重要なのは、結果の良し悪しではなく、「どこに判断や運用の曖昧さがあるか」に気づくことです。

「気づき」は、事務所のIT運用を見直すための最初の一步になります。

# おわりに



## 一般的な視点

ITやセキュリティの問題は、「知っているかどうか」よりも、「誰が、どこで判断するのか」が曖昧なまま積み重なることでリスクになります。今回のチェックは、その“曖昧さ”に気づくためのものです。



## 判断に迷う場面

- ・「これで大丈夫か」と感じたとき
- ・事務所の運用を一度整理してみたいとき

こうした場面では、外部の視点を一時的に取り入れるという選択肢もあります。

本資料が、事務所のIT運用を見直すひとつのきっかけになれば幸いです。必要なときに、必要な形で、専門家の視点を活用することも、健全な事務所運営の一つの形です。