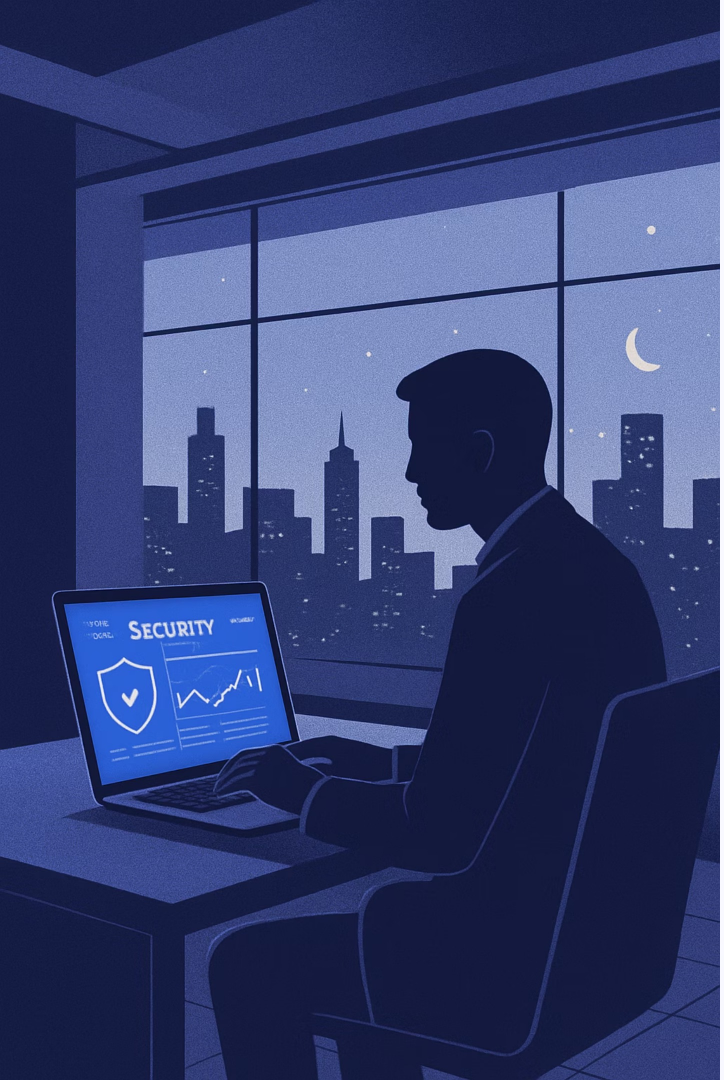


急なトラブルでも会社を止めない

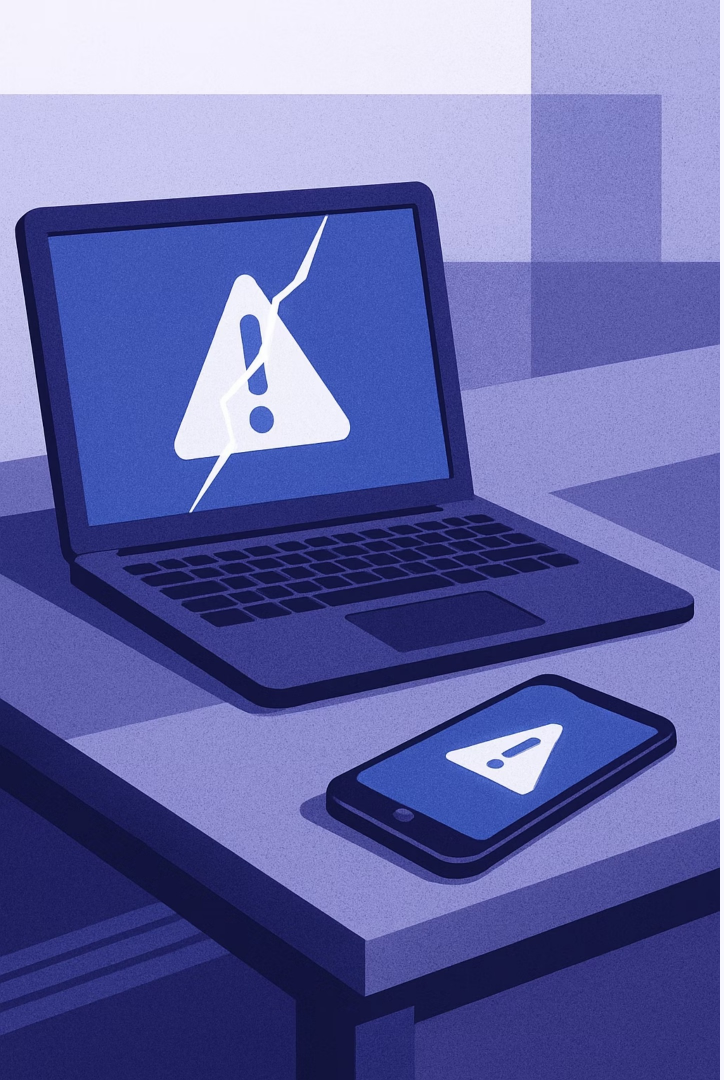
デジタル時代の経営防衛術

騙されない・止めない・漏らさないために
経営者が今日から確認すべきこと

今日のテーマは3つです

🚫 騙されない	⚡ 止めない	🔒 漏らさない
詐欺・フィッシング・なりすましから会社を守る	業務を継続させる仕組みとバックアップ体制	情報管理とAI活用の正しいルール

ITの専門知識がなくても、この3点を押さえるだけで会社のリスクは大幅に下がります。



会社を止める原因は、**災害だけではありません**

スマホの紛失
連絡先・認証アプリが一瞬で使えなくなります

パソコン故障
そのPCにしかないデータが消えるリスク

メール詐欺・クラウド障害
外部サービス停止や不正アクセスで業務が麻痺

担当者不在・パスワード不明
属人化が最大の弱点。後継者が誰もいない状態

第1章：騙されない

経営者を狙う詐欺の手口

経営者は決裁権を持つため、詐欺師の格好の標的です。手口は年々巧妙化しています。

偽SMS・偽メール

公的機関や金融機関を装った偽の通知

偽請求書・なりすまし

取引先を装い、振込先の変更を要求

サポート詐欺・QRコード詐欺

「ウイルス感染」と脅し、遠隔操作を誘導

詐欺の合図 — この6つを感じたら要注意

詐欺の手口は異なっても、**心理的な誘導パターン**は共通しています。
以下のサインを感じたら、すぐに立ち止まってください。

急がせる
「今すぐ」「本日中に」と焦らせる

怖がらせる
「口座が凍結」「訴訟になる」と脅す

得をさせる
「当選した」「還付金がある」と誘惑

秘密にさせる
「他の人には言わないで」と孤立させる

リンクを押させる
不審なURLへ誘導し情報を盗む

振り込ませる
緊急を装い、不正口座へ送金させる

⚠ この6つのうち1つでも感じたら、一度立ち止まり、必ず別の手段で相手に確認しましょう。

守るべき入口 — 6つのデジタル玄関

不正アクセスの入口は必ずこの6つのどれかです。すべてに対策を講じることで、会社のデジタルリスクは大きく低減します。

→ メール・スマホ

二段階認証を設定し、不審な連絡には即応しない

→ パスワード・銀行認証

使い回し禁止。パスワードマネージャーを導入する

→ SNS・LINE・クラウド

アクセス権限を最小化し、退職者のアカウントは即削除

第2章：止めない

会社が止まる本当の原因

災害より怖いのは、**「その人にしか分からない」という属人化**です。

社長・担当者しか知らない

パスワード、手順、取引先情報が頭の中にしか存在しない

そのPCやスマホにしかない

端末が壊れた瞬間、すべてのデータが消滅するリスク

バックアップが戻せない

「取っている」と思っていても、復元できないケースが多数

止まると困る業務を把握していますか？

まず「何が止まると一番困るか」を経営者自身が把握することが出発点です。

1

顧客連絡・予約・納期

信頼を失う前に代替手段を用意する

2

請求・入金確認

キャッシュフローに直結する最優先業務

3

仕入・発注・給与

遅延が連鎖的なトラブルを引き起こす

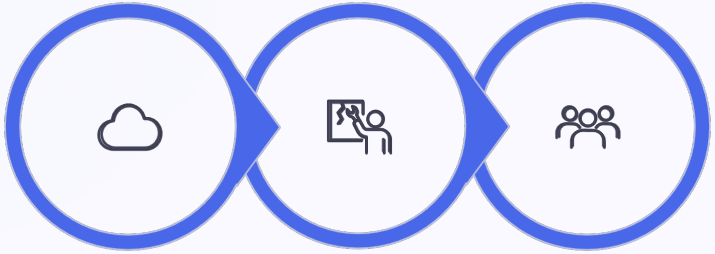
4

契約書・重要書類

紙とデジタルの両方で安全な場所に保管する

これらの業務について、「担当者が急に倒れても翌日から動けるか」を確認してみてください。

バックアップは「取る」より「戻せる」が重要



バックアップを取る　復元を確認　手順を共有

バックアップは「存在する」だけでは不十分です。いざというときに**実際に復元できるか**が問われます。

- どこにあるか・誰が戻せるか

  保管場所と担当者を書面で明確にしておく

- いつのデータか・復元済みか

  定期的に復元テストを実施し、手順を確認する

- パスワードは分かるか

  復元に必要なパスワードを安全な場所に記録する

第3章：漏らさない

AIに入れてよい情報・ダメな情報

✅ 入力してよいもの

- 一般的な文章・あいさつ文
- アイデアのたたき台
- FAQや社内マニュアルの草案
- 業界の一般知識に関する質問

🚫 絶対に入力しないもの

- 顧客情報・個人情報
- 契約書・見積書・図面
- パスワード・認証情報
- 社外秘・未公開の経営情報

⊗ AIに入力した情報は、サービスの学習データに使われる可能性があります。社外秘情報は絶対に入力しないでください。

AIの答えは「正解」ではなく「**たたき台**」

AIは非常に便利なツールですが、**最終判断は必ず人間が行う**という原則を忘れてはなりません。

01

鵜呑みにしない

AIの回答には誤りや古い情報が含まれる場合があります。

02

最後は人が確認

出力内容を必ず担当者または経営者がチェックする。

03

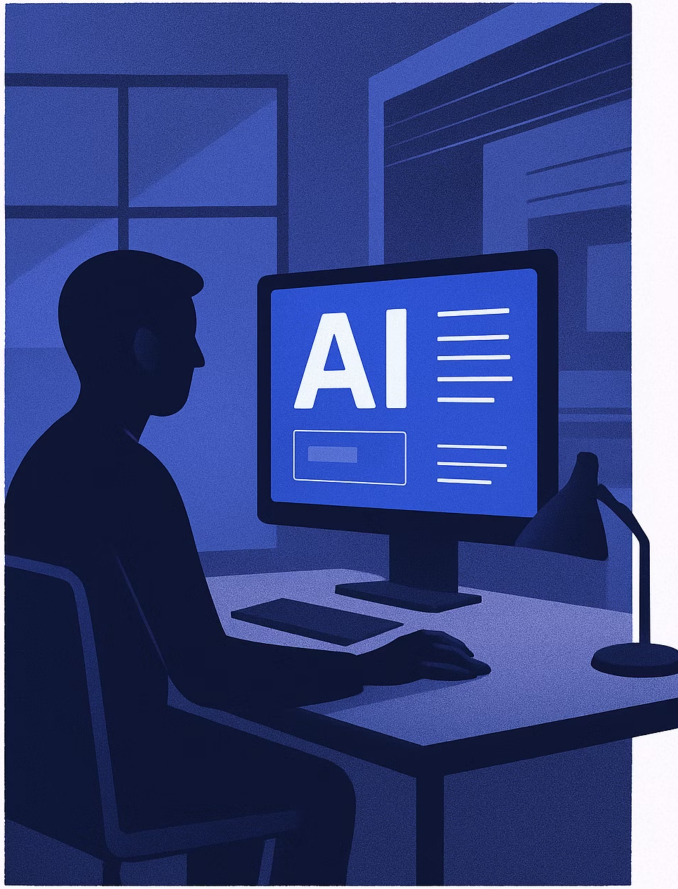
専門領域は専門家へ

法律・税務・契約に関する判断は必ず専門家に相談する。

04

経営判断は経営者が行う

AIはあくまで補助ツール。最終決定権は常に経営者にある。



今日からできる10の点検項目

難しい技術は不要です。まず、この10項目を確認するところから始めてください。

1. パスワード管理
   使い回し・メモ帳保存をやめる
2. 二段階認証
   主要サービスに設定する
3. スマホ紛失対応
   リモートロック手順を確認する
4. 怪しいメール確認
   社内ルールを決めて共有する
5. 振込先変更の電話確認
   必ず既知の番号で折り返す
6. 顧客情報の保管場所
   誰がどこで管理しているか把握する
7. バックアップ復元テスト
   実際に戻せることを確認する
8. 請求・入金業務の代替
   担当者不在でも回る体制を作る
9. AI利用ルール
   入力してよい情報を社内で決める
10. IT相談先
    頼れる専門家の連絡先を確保する

まずはここから始めましょう

10項目すべてを一度に対応する必要はありません。
最も影響が大きい5つから着手してください。

- AI利用ルールの策定
- 請求・入金業務の属人化解消
- メール・SMS詐欺対応ルール
- バックアップと復元確認
- パスワードの見直しと二段階認証

まとめ：3つの原則

🚫 騙されない

怪しい連絡には、**すぐに反応しない**。急かされたら一度立ち止まり、別の手段で確認する習慣を持つ。

⚡ 止めない

重要業務と情報の場所を**見える化する**。「自分しか知らない」状態を解消し、誰でも対応できる体制を作る。

🔒 漏らさない

AI・クラウドに入れる情報を**社内でルール化する**。一度漏れた情報は取り戻せないことを全員が認識する。

会社を守る第一歩は、今日から始まります

> セキュリティというと、難しいシステムの話に聞こえるかもしれません。
> でも、経営者が最初に見るべきことは、もっと身近です。

スマホ、メール、パスワード、バックアップ、AIの使い方。**ここを見直すだけでも、会社の守りは大きく変わります。**

会社を守る第一歩は、「何が止まると困るのか」を知ることです。
今日をきっかけに、ぜひ一度、自社のデジタルまわりを点検してみてください。