118.●セキュリティの基礎

✨118.●セキュリティの基礎（マネジメント対策）

総務部門の社員など“非エンジニア”が押さえておくとよい、実務直結の**セキュリティの基礎**を、やることベースでまとめました。社内教育にも使えるよう、１分チェックリストも付けています。

セキュリティは**マネジメント対策**と**技術的対策**による２面性が必要です。今回はマネジメント対策に主眼を置いて説明しています。

———

目的と基本概念

- **守る対象（情報資産）**：顧客情報、従業員情報（人事・給与・マイナンバー）、
  契約書、見積・請求、会計データ、機器・アカウント。

- **脅威**：誤送信・紛失、フィッシング/マルウェア、なりすまし請求（振込先変更詐欺/BEC）、
  物理盗難、災害。

セキュリティの三要素（CIA）

- 機密性：見てよい人だけが見られる

- 完全性：改ざんされていない

- 可用性：必要な時に使える

※ 併せて**責任追跡性（誰が何をしたか残す）**も重要。

まず最優先の「**5つの行動**」

1.多要素認証（MFA）：主要クラウド（メール、ストレージ、勤怠、会計）すべてに有効化。

2.パスワード管理：12文字以上のフレーズ＋**使い回し禁止**。チームでパスワードマネージャを採用。

3.添付・共有の安全化：PPAP（Zipで暗号化＋別メールでパスワード送信）はNG
PPAP=Password Protected Archive + Password
クラウドストレージ の共有リンクを必要な相手にだけ送付
有効期限設定

4.PCの暗号化と自動ロック：BitLocker / FileVault を有効、
離席は即ロック（Windows＋L / Mac ^⌘Q）。

5.不審メール対策：開かない、報告するが基本。リンクは上にマウスでドメイン確認。
迷ったら開かず**総務/情報管理窓口へ転送**。

業務で頻出するリスクと対策

(1) メール・チャット

• **誤送信防止**：送信前3秒停止→宛先/添付/件名を声出しチェック。外部宛は「外部」タグ自動付与設定を。

• **フィッシング対策の5秒チェック**

1. 差出人ドメインが公式か
2. リンク先ドメイン一致（短縮URL注意）
3. 添付拡張子（**.exe .js .lnk .cab .iso .docx .xlsxは危険**）
4. 「至急」「アカウント停止」など不安を煽る表現
5. 社内なら別経路（電話・チャット）で確認

• **請求・振込先変更依頼メール**

必ず既存の電話番号に折り返しで確認。メールの署名番号に電話しない。

(2) データの取り扱い

• **分類**：例）「特定個人情報（マイナンバー）／個人情報／社外秘／社内限定／公開」。

分類に応じ、**保存場所・共有範囲・保管期限・廃棄方法**を決める。

• **最小権限**：必要な人だけアクセス。共有リンクは「社内の特定メンバーのみ＋期限」。

• **紙**：机上放置禁止、持ち出し原則禁止、廃棄は溶解/クロスカット。

• **機密送付**：暗号化リンク＋受信者限定＋ダウンロード通知。パスワードは**別経路**（電話やSMS）。

(3) 端末・ソフト

• **更新**：OS/ブラウザ/Office/ウイルス対策は自動更新。更新保留は最長でも当日終業まで。

• **暗号化**：ノートPC・外付け媒体はフルディスク暗号化（BitLocker）。USBは原則禁止または登録制。

• **私物端末（BYOD）**：会社データは**MDM（Mobile Device Management）システム配下**
（会社で管理されているデバイス）でのみ利用。

私用クラウド/メモ帳アプリへのコピー禁止。

• **ブラウザ拡張**：業務上必要なもののみ。出所不明な拡張は入れない。

(4) クラウド・アカウント

• **アカウント発行/削除の手順**：入社・異動・退職を総務主導で即日実施。

• **共有ドライブの整理**：オーナー不明や「全員に共有」を廃止。社外共有は台帳管理。

• **監査ログ**：重要サービスは**ログ保全**を有効化（ダウンロード・共有変更・削除）。

• **デジタルフォレンジクス（Digital Forensics）**:削除されたファイル、ログ、通信履歴などを復元。

(5) 物理・来訪者

• **入退室管理・クリーンデスク・覗き見防止**（ブラインド/のぞき見防止フィルム）。

• **肩越しの盗み見**や**尾行（テイルゲーティング）**に注意。見知らぬ来訪は必ずアテンド。

• **スキャベジング体策**としてゴミ箱に書類を捨てない、必ずシュレッダーへ。

(6) 在宅/出張

• **公共Wi-Fi**はVPN必須。テザリング推奨。

• **盗難対策**として離席時は必ずロック、カフェでは背面壁側に座る。

• **紙の持ち出し**は原則禁止。どうしても必要な場合は台帳記録＋返却チェック。

(7) 生成AI/外部Webサービスの利用

• **未公開情報や個人情報を貼らない**（入力したものは相手側に残る可能性）。

• 利用可否と**社内ルール（マスキング・匿名化・機微情報不可）**を明文化。

法令・規格

• **個人情報保護法**：個人データの目的外利用禁止、安全管理義務、委託先管理、漏えい時の報告・本人通知（一定要件）。

• **マイナンバー**：特定個人情報は保管・アクセス・廃棄を特に厳格に。

• **ISMS（ISO/IEC 27001）**：会社のセキュリティを仕組みで回すための代表的規格。
総務は資産管理・入退社手続・物理制限の要。

インシデント対応（初動フロー）

1. **被害拡大の防止**：ネット切断・電源OFFにしない（ログ保存のため）・外付け機器を抜く。
2. **即時連絡**：専用窓口（情報管理/情シス/委託先）へ、**発見日時・端末・状況・見たURL/添付名**を伝える。
3. **証拠保全**：スクショ、メールヘッダ、日時メモ。
4. **関係者対応**：関係部署と連携（人事・法務・広報・取引先）。
5. **再発防止**：原因と対策を“行動”に落とし、ルールや設定を更新。

総務が行うべき運用（例）

• **毎日**：来訪者記録・クリーンデスク点検/気づき共有。

• **毎週**：共有リンクの期限切れ確認、退職者のアクセス停止確認。

• **毎月**：権限棚卸、USB・私物アプリの申請見直し、フィッシング訓練/周知。

• **四半期**：BCP訓練（災害・停電・ランサム想定）、重要帳票の棚卸と廃棄。

すぐに使えるテンプレート

誤送信時の社内初動メモ

(1) 相手に「直ちに削除・転送禁止」を依頼

(2) 上長・情報管理へ連絡（時間/宛先/件名/添付/内容）

(3) 回収可否の確認・再発防止（アドレス帳見直し、外部宛の二重承認など）

振込先変更依頼を受けたら

(1) 既存の登録番号に**こちらから**電話

(2) メール本文の番号には電話しない

(3) 取引先マスターの変更は**ダブルチェック**

よくある**NG例**

(1) 私用のGmail/LINEで社内データを送る

(2)「全員と共有」リンクの無期限運用

(3) 退職者アカウントの放置

(4) 会議室や複合機トレイへの**置き忘れ**

(5)「後でやる」アップデート保留

用語の確認

• **MFA（Multi-Factor Authentication）**：パスワード＋別要素（アプリ通知/物理キー）でログイン。

• **フィッシング**：本物そっくりの偽ページへ誘導してID/パスを盗む手口。

• **ランサムウェア**：データを暗号化し身代金を要求。バックアップと権限制御が決め手。

• **BEC**（ビジネスメール詐欺）Business Email Compromise：
取引先や経営者になりすまして振込を騙す。

• **電子署名**：電子データが「誰によって作成されたか」「改ざんされていないか」
を確認するための仕組み

本人確認（**認証**）：そのデータを「確かに本人が作った」と証明する。

改ざん検知（**完全性保証**）：データが途中で書き換えられていないことを保証する。

否認防止：署名した本人が「自分は関係ない」と否定できないようにする。

1分チェックリスト

• 主要クラウドは****MFA（多要素認証）****を有効

• パスワードは**12文字以上**・使い回しなし・管理ツール使用

• 外部共有は**期限＋相手限定**、PPAP禁止

• PCは**暗号化**・離席ロック・自動ロック≤10分

• 迷ったメールは**開かず報告**、振込変更は**折り返し確認**

• 退職/異動時は**即日アカウント棚卸**

• 紙の**持ち出し・放置なし**、廃棄は溶解/裁断

• 公共Wi-Fiは**VPN**、私物端末は**MDM配下のみ**

———