

情報資産管理台帳

IPA『中小企業の情報セキュリティ対策ガイドライン 第4.0版』付録6 の様式・計算式に準拠 / 作成 2026-09-29 株式会社サンプル企業

業務分類	情報資産名称	備考	利用者の範囲	管理部署	管理者	媒体・保存先	機密性	完全性	可用性	重要度	脅威の発生頻度	脆弱性	被害発生可能性	リスク値	判定	保存期限
設計・製造	客先支給の図面データ	取引先から秘密として提供された情報。142 社ぶん	生産管理・現場	製造部	製造部長	共有フォルダ（NAS）	3	3	3	3	3	3	3	9	リスク大	期限なし
設計・製造	NC プログラム	自社の独自ノウハウ。段取りの勘所が入っている	現場（旋盤・フライス）	製造部	製造部長	各機械のメモリと NAS	3	3	3	3	2	3	2	6	リスク大	期限なし
設計・製造	検査成績書	客先に提出する品質の記録	生産管理・検査	製造部	製造部長	NAS	2	3	2	3	2	2	1	3	リスク小	7 年
営業	受注台帳.xlsx	2,847 行。単価が入っている	営業 2 名・生産管理	営業部	営業課長	共有フォルダ	2	3	3	3	3	3	3	9	リスク大	7 年
営業	取引先リスト・単価表	営業秘密（不正競争防止法）	営業 2 名・代表	営業部	代表	共有フォルダ	3	3	2	3	2	3	2	6	リスク大	期限なし
営業	見積書・注文書 PDF	商取引の記録	営業 2 名	営業部	営業課長	共有フォルダ	2	3	2	3	2	2	1	3	リスク小	7 年
製造	実績.xlsx	18,402 行。工程の実績時間	生産管理	製造部	製造部長	共有フォルダ	1	2	2	2	2	3	2	4	リスク中	7 年
人事	従業員の個人情報	個人情報保護法の対象。38 名ぶん	総務・代表	総務	代表	会計ソフト・書棚（施錠）	3	3	2	3	2	2	1	3	リスク小	退職後 5 年
人事	給与データ	個人情報。マイナンバーを含む	総務・代表	総務	代表	会計ソフト（PC 1 台）	3	3	2	3	2	2	1	3	リスク小	7 年
経理	会計データ・決算書	自社の会計情報	経理・代表	総務	代表	会計ソフト（PC 1 台）	3	3	2	3	1	2	1	3	リスク小	10 年
経理	銀行のインターネットバンキング	送金ができる	代表のみ	総務	代表	代表の PC	3	3	3	3	2	2	1	3	リスク小	—
共通	電子メール（chuumon@ ほか）	注文書が届く経路	全社	総務	代表	レンタルサーバ	2	2	3	3	3	3	3	9	リスク大	3 年
共通	共有フォルダ（NAS 本体）	上記の大半がここに入っている	全社	総務	代表	事務所内 NAS 1 台	3	3	3	3	2	3	2	6	リスク大	—
共通	バックアップ用 外付け HDD	NAS の複製。週 1 回	総務	総務	代表	事務所の書棚	3	3	2	3	2	3	2	6	リスク大	—
共通	無線 LAN のパスワード	全社で 1 つを共用している	全社	総務	代表	事務所に掲示	2	1	2	2	3	3	3	6	リスク大	—
共通	製品カタログ・会社案内	公開情報	全社	営業部	営業課長	ホームページ	1	1	1	1	1	1	1	1	リスク小	—

重要度 = MAX(機密性,完全性,可用性) / 被害発生可能性 = ROUNDUP(脅威の発生頻度 ÷ (4 - 脆弱性), 0) / リスク値 = 被害発生可能性 × 重要度 / 判定: 5 超=リスク大・4=リスク中・それ以下=リスク小

出所: IPA『中小企業の情報セキュリティ対策ガイドライン 第4.0版』付録6 の計算式をそのまま使用

評価値の付け方

IPA の基準をそのまま使う。迷ったら上の段（重い方）を選ぶ。

観点	評価値	基準
機密性	3	法律で安全管理が求められる／守秘義務の対象／自社の営業秘密
	2	漏えいすると事業に大きな影響がある
	1	漏えいしても事業にほとんど影響はない
完全性	3	法律で安全管理が求められる／改ざんされると深刻な影響
	2	改ざんされると事業に大きな影響がある
	1	改ざんされてもほとんど影響はない
可用性	3	利用できなくなると深刻な影響
	2	利用できなくなると事業に大きな影響がある
	1	利用できなくなってもほとんど影響はない
脅威の発生頻度	3	通常の状態が発生する（年に 1 回以上）
	2	特定の状態が発生する（数年に 1 回）
	1	通常の状態ではまず発生しない
脆弱性	3	対策をしていない
	2	部分的に対策している
	1	対策している

当社での例
客先の図面・個人情報・取引先リスト・単価表
見積書・仕入価格・受注台帳
製品カタログ・会社案内
個人情報・会計データ・客先の図面・NC プログラム
受発注・実績データ
廃番品のカタログ
共有フォルダ・メール・NC プログラム
設計図・実績データ
廃番品のカタログ
メールによるウイルス・誤送信
端末の紛失・盗難
事務所への侵入
無線 LAN のパスワードを全社で共用している
バックアップは取っているが戻す訓練はしていない
会計ソフトは PC 1 台に限定し施錠した部屋に置いている

リスク値の大きい順に、何をするか

台帳のリスク値は式で計算される。対策を打って脆弱性を下げると、この表の

順	情報資産名称	リスク値	判定
1	客先支給の図面データ	9	リスク大
2	受注台帳.xlsx	9	リスク大
3	電子メール（chuumon@ ほか）	9	リスク大
4	NC プログラム	6	リスク大
5	取引先リスト・単価表	6	リスク大
6	共有フォルダ（NAS 本体）	6	リスク大
7	バックアップ用 外付け HDD	6	リスク大
8	無線 LAN のパスワード	6	リスク大
9	実績.xlsx	4	リスク中

対策を打ったら、台帳の『脆弱性』を下げる。リスク値が自動で下がり、順番
リスク大（リスク値 5 超）の 8 件すべてと、リスク中の 1 件を載せている。

いま何が起きうるか

142 社ぶん。持ち出しの記録が無く、USB にも入れられる

単価が入っている。全社の誰でも開けて、上書きもできる

注文書が届く経路。ウイルス付きのメールが月 3~5 通届いている

自社のノウハウ。各機械のメモリにあり、複製の記録が無い

営業秘密。共有フォルダに置かれ、退職者も見られる状態だった

資産の大半がここ 1 台にある。誰でも全部が見える

週 1 回取っているが、**戻す訓練を一度もしていない**

全社で 1 つのパスワードを共用し、事務所に掲示している。退職者も知っている

工程の実績時間。バックアップは NAS 任せ

打つ手	いつまでに	誰が
USB への書き出しを止める。持ち出しは管理者の承認制にする	2027-02-28	製造部長
営業部と生産管理だけが書き込めるようにする。他は読み取りのみ	2026-12-31	営業課長
多要素認証を入れる。添付の開き方を 1 枚にして全員に配る	2026-12-31	代表
NAS 側を正本と決め、機械からの持ち出しを記録する	2027-03-31	製造部長
アクセスできる人を 3 名に限る。退職時の権限削除を手順に入れる	2027-01-31	代表
部署ごとにアクセス権を分ける。まず人事・経理のフォルダから	2027-01-31	総務
年 1 回、実際に戻す訓練をする。暗号化もかける	2027-03-31	総務
業務用と来客用を分ける。業務用は端末の登録制にし、掲示をやめる	2026-11-30	代表
共有フォルダの権限整理に合わせて扱う（3 番と同時）	2027-01-31	総務