

株式会社サンプル企業

情報セキュリティ基本方針・関連規程

第 1.0 版

作成	AI 活用推進担当
日付	2026-09-29
版	1.0
機密区分	社内限り

目次

1. この文書について

- 1.1 目的
- 1.2 読み手
- 1.3 範囲
- 1.4 範囲に含まないもの
- 1.5 前提と制約
- 1.6 改訂履歴
- 1.7 用語

2. 情報セキュリティ基本方針

3. 守るものを決める（情報資産の管理）

- 3.1 台帳を作る
- 3.2 重要度を評価する
- 3.3 見直す

4. 守り方を決める

- 4.1 持ち出しと保存先
- 4.2 誰が見られるかを決める（アクセス制御と認証）
- 4.3 無線 LAN
- 4.4 電子メールとインターネット
- 4.5 バックアップ
- 4.6 委託先に情報を渡すとき
- 4.7 従業員の責務と、退職するとき

5. 起きたときにどうするか

- 5.1 気づいたら、すぐ伝える
- 5.2 何をするか
- 5.3 個人情報が漏れたときの届出

6. IPA のサンプルから外した章と、その理由

6.1 教育

7. 論点と未決

8. 次にやること

1. この文書について

1.1 目的

当社が守るべきことを、**38 名が実際に守れる分量**で定める。

1.2 読み手

- ・全従業員（38 名）
- ・代表・製造部長・営業課長（管理責任者）
- ・取引先（求めがあったとき）

1.3 範囲

- ・当社が扱うすべての情報資産
- ・全従業員、派遣・アルバイト、役員
- ・委託先に情報を渡す場合の取り決め

1.4 範囲に含まないもの

ここを書かないと、読み手は「書いていないこと=やること」と読みます。

- ・IPA 付録 5 のうち、当社に当てはまらない章は入れていない（6 に一覧）
- ・テレワーク規程 — 現在テレワークを行っていないため。始めるときに追加する
- ・特権アカウントの分離運用 — 情報システムの担当者がいないため実施できない。代わりに 4.2 で「代表が持つ」と定めた

1.5 前提と制約

前提が崩れたら、この文書の結論も崩れます。崩れたら作り直します。

#	前提	崩れたらどうなるか
1	情報システムの専任担当者がいない	専門知識を前提にした条文は守られない。本規程は「誰でもできること」だけで構成している

#	前提	崩れたらどうなるか
2	現場 22 名は業務で PC を使わない	PC 利用に関する条文の対象が 16 名になる。全社向けに書くと過剰になる
3	情報資産管理台帳（別ファイル）が作られ、毎年見直される	本規程の第 5 章が空文になる。台帳が無ければ何を守るのが決まらない

1.6 改訂履歴

版	日付	作成	承認	変更の要旨
0.3	2026-09-05	AI 活用推進担当	—	IPA 付録 5 を土台に起案。当社に当てはまらない章を外した
0.8	2026-09-19	AI 活用推進担当	代表	情報資産管理台帳の結果を反映。リスク大 8 件に対する条文を入れた
1.0	2026-09-29	AI 活用推進担当	高梨 亮	制定

1.7 用語

語	この文書での意味
情報資産	当社の事業に必要な情報と、それを扱う機器・記録媒体・システム
管理責任者	その情報資産について、誰に見せるか・どこに置くかを定める人
インシデント	情報が漏れた・壊れた・使えなくなった、またはその恐れがある出来事
IPA 付録 5	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 5「情報セキュリティ関連規程（サンプル）」

結論

状況 当社は客先から図面の提供を受けて加工している。142 社ぶんの図面と、38 名の個人情報を預かっている。これまで情報の扱いに関する文書上の定めが無かった。

問題 情報資産管理台帳を作って評価したところ、**16 件のうち 8 件が「リスク大」**だった。最も大きいのは **客先の図面・受注台帳・電子メール（いずれもリスク値 9）**。取引先 2 社から、**情報の取り扱いに関する文書の提出を求められている**。

問い 何を、どこまで定めるか。

答え IPA の公式サンプルは 59 ページあるが、当社版は本文 5 章・13 ページとした。守れない規程を作ると、破られた実績だけが残ри、かえって弱くなる。リスク大 8 件に直接効く条文だけを残し、当てはまらない章は削ったことを明記して外した。

	IPA サンプル	当社版
章の数	9 章 + 別編 6 章	本文 5 章
ページ数	59 ページ	13 ページ
対象にした資産	—	16 件（台帳で特定）
リスク大への対応	—	8 件すべてに条文あり

2. 情報セキュリティ基本方針

当社は、お客様からお預かりした図面その他の情報、および当社の従業員と取引に関する情報を、事業を続けるうえで欠かせない資産と位置づけ、次のとおり取り扱います。

- ・ **法令を守ります。** 個人情報保護法、不正競争防止法その他の法令およびお客様との契約上の義務を守ります。
- ・ **守るものを決めます。** 情報資産を洗い出し、重要度を評価した台帳を作り、**年 1 回見直します。**
- ・ **できることを決めます。** 当社の規模でできる対策を定め、**守れないことは定めません。**
- ・ **起きたときに動きます。** 万一の事態に備え、誰が何をするかを決めておきます。
- ・ **全員で取り組みます。** 年 1 回、全従業員に教育を行います。

制定 2026 年 9 月 29 日 株式会社サンプル企業 代表取締役 高梨 亮

| この 1 枚は、求めがあれば取引先にお見せする。以降の章は社内限りとする。

3. 守るものを決める（情報資産の管理）

3.1 台帳を作る

- ・ 総務は、当社が扱う情報資産を洗い出し、**情報資産管理台帳**に記録する。
- ・ 台帳には、資産の名称・利用できる人の範囲・管理責任者・保存先・保存期限を記載する。
- ・ 台帳に載っていないものは、**守る対象として認識されていないということである。**気づいた者は総務に申し出る。

3.2 重要度を評価する

- ・ 各資産について、**機密性・完全性・可用性**を 1～3 で評価し、**その最大値を重要度**とする。
- ・ 評価の基準は台帳の「評価の基準」シートによる（IPA の基準をそのまま用いる）。

- ・脅威の発生頻度と脆弱性を 1～3 で評価し、**リスク値 = ROUNDUP(脅威 ÷ (4 - 脆弱性)) × 重要度** を算出する。
- ・リスク値が 5 を超えるもの（リスク大）には、必ず打つ手と期限と担当を決める。

3.3 見直す

- ・総務は**毎年 4 月**に台帳を見直し、代表の承認を受ける。
- ・新しい業務・システム・取引先が増えたときは、**そのつど**台帳に追加する。
- ・対策を打ったら、台帳の『脆弱性』の値を下げる。リスク値が下がることが、効いた証拠である。

4. 守り方を決める

この章の条文は、すべて台帳のリスク大 8 件に対応している。対応先を各条の末尾に示す。

4.1 持ち出しと保存先

図表 1 情報資産の持ち出し

対象	決まり	対応する資産
客先から預かった図面	USB 等への書き出しを禁じる。持ち出しが必要なときは管理責任者（製造部長）の承認を得る	図面データ（9）
NC プログラム	正本は共有フォルダに置く。機械のメモリへの複製は業務上必要な範囲に限り、持ち出しは記録する	NC プログラム（6）
取引先リスト・単価表	閲覧できる者を代表・営業 2 名に限る。社外への持ち出しを禁じる	取引先リスト（6）
個人情報・給与データ	会計ソフトを入れた 1 台の PC でのみ扱う。書類は施錠した書棚に保管する	個人情報・給与（3）

資料: —

4.2 誰が見られるかを決める（アクセス制御と認証）

- ・共有フォルダは、**部署ごとにアクセスできる範囲を分ける**。とくに人事・経理のフォルダは総務と代表に限る。

- ・業務で使う PC には、**1 人 1 つの利用者アカウント**を設ける。共用しない。
- ・パスワードは **8 文字以上**とし、他のサービスと同じものを使わない。**定期的な変更は求めない**（付箋に書かれる方が危ないため）。
- ・電子メールと銀行のインターネットバンキングには、**多要素認証**を設定する。
- ・**特権的な権限（管理者アカウント）は代表が持つ**。専任の担当者がいないため分離できないことを承知のうえで、代表以外には渡さないことで代える。
- ・従業員が退職するときは、その日のうちに**アカウントを止める**。手順は 4.7 による。

対応する資産: 受注台帳（9）・電子メール（9）・共有フォルダ（6）・取引先リスト（6）・無線 LAN（6）

4.3 無線 LAN

- ・業務用と来客用を分ける。
- ・業務用は、**あらかじめ登録した機器のみ**接続できるようにする。
- ・パスワードを事務所に掲示しない。
- ・来客用は業務用のネットワークから切り離す。

対応する資産: 無線 LAN のパスワード（6）

4.4 電子メールとインターネット

- ・身に覚えのない差出人からの**添付ファイルを開かない**。判断に迷ったら、開く前に総務に相談する。
- ・**送信先を送信前に必ず確認する**。とくに複数の宛先に送るときは、宛先を Bcc にする。
- ・業務で使うクラウドサービスは、**総務に届け出**てから使う。
- ・**会社の情報を個人のメールアドレスやクラウドに置かない**。

対応する資産: 電子メール（9）

4.5 バックアップ

- ・共有フォルダは、**週 1 回**外付けの記録媒体に複製する。

- ・複製した媒体は**暗号化**し、施錠した書棚に保管する。
- ・**年 1 回、実際に戻す訓練を行う**。戻せることを確かめていない複製は、複製とは言えない。
- ・訓練の結果は記録し、代表に報告する。

対応する資産: バックアップ用 外付け HDD (6) ・共有フォルダ (6)

4.6 委託先に情報を渡すとき

- ・外注先に図面その他の情報を渡すときは、**秘密保持の取り決めに文書で交わす**。
- ・渡す情報は**業務に必要な範囲に限る**。
- ・再委託を行う場合は、**事前に当社の承認を得ることを条件とする**。
- ・委託先の一覧を作り、年 1 回見直す。

4.7 従業員の責務と、退職するとき

- ・入社時に、本規程を読み、**秘密保持に関する誓約書**を提出する。
- ・退職時の手順（その日のうちに） — ①アカウントを止める ②貸与した機器・鍵・記録媒体を返却する ③持ち出した情報が無いことを確認する ④共有フォルダの権限から外す
- ・退職後も、在職中に知り得た情報を他に漏らしてはならない。

2026 年の台帳作成で、退職者が知っている無線 LAN のパスワードがそのまま使われていることが分かった。この節はその反省から書いている。

5. 起きたときにどうするか

5.1 気づいたら、すぐ伝える

図表 2 連絡の順路

誰が	何をするか	いつまでに
気づいた人	自分で解決しようとしな い 。ただちに上長または総務へ口頭で伝える	ただちに
上長・総務	代表へ報告する	30 分以内
代表	対応する人を決め、記録を始める	1 時間以内

誰が	何をするか	いつまでに
代表	必要に応じて取引先・IPA・個人情報保護委員会へ届け出る	状況に応じて

資料: —

隠すことがいちばん被害を大きくする。報告したことで不利に扱うことはしない。これは代表が明言する。

5.2 何をするか

- ・ **広がり进行止める** — 感染が疑われる機器はネットワークから外す（LAN ケーブルを抜く）。電源は切らない（証拠が消えるため）。
- ・ **記録する** — いつ・何が・どこで起きたか、誰が何をしたかを時刻とともに書く。
- ・ **戻す** — 複製から戻す。手順は 4.5 による。
- ・ **知らせる** — 客先の情報が関わる場合は、代表が客先に連絡する。
- ・ **繰り返さない** — 1 か月以内に原因と再発防止をまとめ、必要なら台帳と本規程を直す。

5.3 個人情報漏れたときの届出

図表 3 届出先

どこに	いつ	何を
個人情報保護委員会	速報: 速やかに（3～5 日以内） / 確報: 30 日以内（不正アクセス等は 60 日以内）	個人情報保護法第 26 条に基づく報告
本人	速やかに	漏れた内容と、当社の対応
IPA（情報セキュリティ安心相談窓口）	任意	相談

資料: 個人情報保護法第 26 条、個人情報保護委員会の規則

この期限は法律で決まっている。社内の判断で遅らせられない。

6. IPA のサンプルから外した章と、その理由

抜けているのではなく、外した。当社の状況が変わったときに戻せるよう、理由とともに残す。

図表 4 外した章

IPA 付録 5 の章	外した理由	戻す条件
2. 監査・点検（内部監査の体制）	監査を行える人員がいない。代わりに 3 の年 1 回の台帳見直し で代える	従業員 100 名を超えたとき
6.7 特権アカウントの分離運用	情報システムの担当者がいないため分離できない。4.2 で「代表が持つ」と定めて代える	担当者を置いたとき
6.9 端末のタイムアウト機能	事務所は施錠された 1 室で、来客が単独で入ることはない	来客の出入りが増えたとき
7.2 SNS の個人利用	当社は SNS を業務で使っておらず、個人利用を制限する根拠がない	業務で SNS を使うとき
9.9 事業継続計画（BCP）	別の文書として作る。情報セキュリティの規程に混ぜると、地震・火災の対応が埋もれる	2027 年度に別途作成する
別編 6. テレワークにおける対策	現在テレワークを行っていない	テレワークを始めるとき
別編 5. 人材育成	セキュリティ専門の人材を育てる計画がない。 年 1 回の全員教育（6.1） で代える	担当者を置いたとき

資料: 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 5 と照合

6.1 教育

- ・ **年 1 回**、全従業員に情報セキュリティの教育を行う（**30 分**）。
- ・ 内容は、本規程の要点と、その年に実際にあった出来事とする。
- ・ **現場 22 名には、PC を使わない前提の内容**（持ち出し・私物の機器・不審な電話への対応）を別に行う。
- ・ 実施した記録（日付・出席者・内容）を残す。

7. 論点と未決

決まっていないことを、決まっていないと書きます。埋めてから出すと、決めた人が誰もいないまま進みます。

#	論点	選択肢	決める人	期限
1	事業継続計画（BCP）を誰がいつ作るか	① 2027 年度に AI 活用推進担当が起案／② 保険会社の様式を使う／③ 当面作らない	代表	2027-03

#	論点	選択肢	決める人	期限
2	サイバー保険に入るか	リスク大 8 件のうち、対策後も残るものをどう扱うか。年 12～18 万円の見込み	代表	2027-01
3	委託先（熱処理 1 社）との秘密保持の取り決め	現在、文書を交わしていない。既存の取引基本契約書に秘密保持条項があるか要確認	代表	2026-11-30

8. 次にやること

#	やること	誰が	いつまでに
1	本規程を全従業員に配り、30 分の説明会を行う	代表	2026-10-31
2	秘密保持に関する誓約書の様式を作る	AI 活用推進担当	2026-10-17
3	無線 LAN を業務用と来客用に分ける	代表	2026-11-30
4	熱処理の外注先との契約書に秘密保持条項があるか確かめる	代表	2026-11-30
5	台帳のリスク大 8 件について、対策の進み具合を毎月確認する	総務	毎月末