株式会社サンプル企業

社内限り ｜ 2026-11-16

情報セキュリティ基本方針・関連規程

基本方針と、組織的・人的・物理的・技術的対策の規程

この書類の結論

IPA の公式サンプル（59 ページ）の 4 分類に沿い、当社が守れる条文だけを残す。リスク大 9 件にはすべて条文と担当・期限を付け、当てはまらない章は理由とともに外す。基本方針は IPA の 5 項目の形にし、取引先にそのまま示せる 1 ページにした。

作成	AI 活用担当
日付	2026-11-16
版	1.1
機密区分	社内限り

目次

1. この文書について 3
1.1 目的 3
1.2 読み手 3
1.3 範囲 3
1.4 範囲に含まないもの 3
1.5 前提と制約 4
1.6 改訂履歴 4
1.7 用語 4
2. 情報セキュリティ基本方針 6
3. 組織的対策 7
3.1 体制と役割 7
3.2 情報資産の管理 7
3.3 アクセス制御と認証 8
3.4 委託先の管理 8
3.5 事故（インシデント）への対応 9
4. 人的対策 10
5. 物理的対策 10
6. 技術的対策 11
7. 様式 11
8. 年間の予定 13
9. IPA のサンプルから外した章と、その理由 13
10. 論点と未決 14
11. 次にやること 14

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。基本方針（1 ページ）は取引先にも示せる形にし、規程は社内で使う。

1.2　読み手

- 全従業員（38 名）
- 代表・製造部長・営業課長・総務（管理責任者）
- 取引先（基本方針の提示を求められたとき）

1.3　範囲

- 当社が扱うすべての情報資産（紙・電子データ・機器）
- 役員・従業員・派遣社員・アルバイト
- 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**（9 章に一覧と、戻す条件）
- **テレワークの規程** — テレワークを行っていない。始めるときに足す
- **地震・火災などで事業が止まったときの対応** — 事業継続計画（BCP）に書く。本規程は目標復旧時間だけを合わせる

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」と、保守事業者に頼むことで組んでいる**
2	現場 22 名は業務で PC を使わない	PC に関する条文の対象は 16 名。現場には持ち出し・私物の機器・不審な電話を別に教える
3	情報資産管理台帳（別ファイル）が毎年 4 月に見直される	台帳が古くなると、何を守るかがずれる。見直しは 3 章で定める

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 活用担当	代表	情報資産管理台帳の結果を反映。リスク大に対する条文を入れた
1.0	2026-09-29	AI 活用担当	高梨 亮	制定
1.1	2026-11-16	AI 活用担当	高梨 亮	基本方針を IPA 付録 2 の 5 項目に、規程を第 4.0 版付録 5 の 4 分類に組み替えた。様式 6 点と年間の予定を足した

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
情報セキュリティ責任者	情報セキュリティの最終的な判断と責任を負う者。当社では代表
管理責任者	その情報資産について、誰に見せるか・どこに置くかを決める者（台帳の「管理者名」）
インシデント	情報が漏れた・壊れた・使えなくなった、またはそのおそれがある出来事
多要素認証	パスワードに加え、スマートフォンへの確認など別の要素も使う本人確認
IPA 付録 2・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』（2026-03-27 公開）の付録 2「情報セキュリティ基本方針（サンプル）」と付録 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を預かって加工している。142 社ぶんの図面と、38 名の個人情報を持つ。取引先 2 社から、情報の取扱いを定めた文書の提出を求められている。

問題　情報資産管理台帳で 18 件を評価したところ、**9 件が「リスク大」**、1 件が「リスク中」だった。最も大きい（リスク値 9）のは **客先支給の図面データ・受注台帳.xlsx・電子メール（chuumon@ ほか）**。

問い　何を、どこまで定めるか。

答え　**IPA の公式サンプル（59 ページ）の 4 分類に沿い、当社が守れる条文だけを残す。**リスク大 9 件にはすべて条文と担当・期限を付け、当てはまらない章は理由とともに外す。基本方針は IPA の 5 項目の形にし、取引先にそのまま示せる 1 ページにした。

2.　情報セキュリティ基本方針

株式会社サンプル企業（以下、当社）は、お客様からお預かりした図面その他の情報と、当社の情報資産を、事故・災害・犯罪などの脅威から守り、お客様と社会の信頼に応えるため、次の方針に基づき全社で情報セキュリティに取り組みます。

1. 経営者の責任

当社は、代表が先頭に立ち、組織的かつ継続的に情報セキュリティの改善・向上に努めます。

2. 社内体制の整備

当社は、情報セキュリティを保つための体制を定め、守るべきことを社内の正式な規程として定めます。

3. 従業員の取組み

当社の従業員は、情報セキュリティに必要な知識と技術を身につけ、日々の業務で確かに実行します。

4. 法令及び契約上の要求事項の遵守

当社は、個人情報保護法・不正競争防止法その他の法令と、お客様との契約上の義務を守り、お客様の期待に応えます。

5. 違反及び事故への対応

当社は、法令違反・契約違反・事故が起きたときは適切に対処し、原因を確かめて再発を防ぎます。

制定日　2026 年 9 月 29 日　　改定日　2026 年 11 月 16 日

株式会社サンプル企業　代表取締役　高梨 亮

> **この方針は、求めがあれば取引先にお見せする。**次の章からの規程は社内限りとする。形は IPA 付録 2（情報セキュリティ基本方針のサンプル）の 5 項目に合わせた。

3.　組織的対策

3.1　体制と役割

図表 1　情報セキュリティの体制

役割	誰が	何をするか
情報セキュリティ責任者	代表（高梨 亮）	方針と規程を承認する。事故のときの最終判断と、取引先・当局への連絡
推進担当	総務	台帳と規程の見直し、教育、記録の保管。保守事業者との窓口
管理責任者	製造部長・営業課長・総務	台帳の「管理者名」の資産について、見せる範囲・置き場所・持ち出しを決める
全従業員	役員・従業員・派遣・アルバイト	本規程を守る。おかしいと思ったら、すぐ上長か総務に伝える

資料: IPA 付録 5 組織的対策 1（情報セキュリティのための組織）を当社の人数に合わせた

IPA のサンプルが置く「情報セキュリティ委員会」は設けない。代わりに、毎月の部門横断の会議（第 2 水曜）の議題に、リスク大の対策の進み具合を入れる（組織と KPI の設計と同じ会議）。

点検と見直し

- 推進担当は**毎年 4 月**に情報資産管理台帳を見直し、情報セキュリティ責任者の承認を受ける。
- 同じく 4 月に、IPA「5 分でできる！情報セキュリティ自社診断」（付録 3）を PC を使う 16 名で行い、点数を記録する。
- 新しい業務・システム・取引先・委託先が増えたときは、**そのつど**台帳に足す。
- 次のときは規程を見直す: 取引先から新しい求めがあったとき／法令が変わったとき／事故が起きたとき／対策が守られていないと分かったとき。
- 規程を改めたときは、変えた点を全従業員に知らせる。

3.2　情報資産の管理

- 推進担当は、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（IPA 付録 6 の様式）。
- 各資産の機密性・完全性・可用性を 1〜3 で評価し、**最大値を重要度**とする。**個人情報を含む資産は重要度 3** とする。
- 脅威と脆弱性から **リスク値 ＝ 切り上げ（脅威 ÷（4 − 脆弱性））× 重要度** を出す。**リスク値が 6 以上（リスク大）の資産には、対策・担当・期限を必ず決める。**

- 対策を終えたら、台帳の「脆弱性」を書き換える。リスク値が下がることが、効いた証拠である。

図表 2　持ち出しと保管の決まり

対象	決まり	台帳の資産（リスク値）
客先から預かった図面	**USB 等への書き出しを禁じる。持ち出しは製造部長の承認を受け、様式 2 に記録する**	客先支給の図面データ（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	**見られる者を代表・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・単価表（6）
個人情報・給与データ	**会計用の PC 1 台でのみ扱う。**書類は施錠した書棚に置く	従業員の個人情報・給与データ（3）

資料: 情報資産管理台帳（2026-09-29）のリスク値算定

3.3　アクセス制御と認証

- 共有フォルダは、**部署ごとに見られる範囲を分ける。**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、共用しない。
- パスワードは **8 文字以上**とし、名前・電話番号・誕生日など推測できるものと、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）。
- 電子メール・インターネットバンキング・クラウドサービスには、**多要素認証**を設定する。
- **管理者のアカウントは代表が持ち、12 文字以上のパスワードと多要素認証を使う。**専任者がいないため権限を分けられないことを承知のうえで、代表以外に渡さないことで代える。
- 退職・異動の日に、その者のアカウントと権限を止める（4 章の退職の手順）。

パスワードの文字数と多要素認証は IPA 付録 5 の標準（一般アカウント 8 文字以上・特権 12 文字以上）に合わせた。

3.4　委託先の管理

- 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を文書で交わす。**
- 選ぶときは、秘密保持・再委託の制限・事故のときの連絡の 3 点を、様式 4（委託先の確認票）で確かめる。
- 渡す情報は**業務に必要な範囲に限り**、終わったら返却または廃棄を求める。
- **再委託は、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**、様式 4 で見直す。

3.5　事故（インシデント）への対応

図表 3　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。上長または総務に口頭で伝える**	**ただちに**
上長・総務	情報セキュリティ責任者（代表）に報告し、様式 3（事故の第一報）を書き始める	**30 分以内**
代表	対応する者を決め、広がりを止める指示を出す	**1 時間以内**
代表	客先の情報が関わるときは客先へ連絡する。必要に応じて当局・相談窓口へ届け出る	状況に応じて

資料: IPA 付録 5 組織的対策 9.3〜9.6、付録 8「セキュリティインシデント対応の手引き」

> **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。

- **広がりを止める** — 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・無線を切る）。電源は切らない（記録が消える）。
- **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様式 3 に書く。
- **戻す** — 複製から戻す（6 章のバックアップ）。
- **繰り返さない** — 1 か月以内に原因と再発防止をまとめ、台帳と本規程を直す。

図表 4　個人情報が漏れたときの届出

どこに	いつ	根拠
個人情報保護委員会	速報: 速やかに（目安 3〜5 日）／確報: 30 日以内（不正の目的によるものは 60 日以内）	個人情報保護法 第 26 条第 1 項と委員会規則
本人	速やかに	同 第 26 条第 2 項
IPA（情報セキュリティ安心相談窓口）	任意	相談

資料: 個人情報の保護に関する法律（e-Gov 法令検索で確認）、個人情報保護委員会の規則とガイドライン

> **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。届け出るかどうかの判断に迷うときは、顧問の弁護士に相談する。

事業継続との関係

- 地震・火災などで事業が止まったときの対応は、**事業継続計画（BCP）**に書く。本規程とは別の文書にする（混ぜると埋もれる）。
- **共有フォルダ（NAS）の業務データは、3 営業日以内に戻せる状態を保つ。**BCP の目標復旧時間（中核事業の再開 7 営業日）の内側に置くため。
- 失ってよい業務データは**最大 1 週間分**とする（週 1 回の複製に合わせた）。これより短くするなら複製の回数を増やす。

4.　人的対策

- **雇うとき** — 本規程を説明し、様式 1（秘密保持に関する誓約書）を提出してもらう。派遣社員は派遣元との契約で同じことを求める。
- **働いている間** — 本規程を守る。違反したときの扱いは、**就業規則の懲戒の定め**による。
- **退職するとき（その日のうちに）** — 様式 6 で、①アカウントを止める ②貸与した機器・鍵・記録媒体を返してもらう ③持ち出した情報が無いことを確かめる ④共有フォルダの権限から外す。退職後も、在職中に知った秘密を漏らしてはならない。

> **2026 年の台帳づくりで、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と分かった。**退職の手順はその反省から書いている。

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）を様式 5 に残す。欠席者には 1 か月以内に個別に行う。

5.　物理的対策

- **事務所** — 最後に出る者が施錠する。来客は受付で記帳し、社員が付き添う。記帳は 1 年間とっておく。
- **机と画面（クリアデスク・クリアスクリーン）** — 帰るときは図面・注文書を机に出したままにしない。離席するときは画面を閉じる。PC は 5 分で画面が鍵付きで閉じるように設定する。
- **FAX と複合機** — 受信した注文書を受信トレイに置いたままにしない（台帳の「注文書（紙）」）。
- **捨てるとき** — 書類はシュレッダーか、溶解処理の業者に出す。PC・HDD・USB メモリは、消去ソフトで消すか物理的に壊し、台帳（ハードウェア）に処分日と方法を書く。業者に出すときは消去の証明書をもらう。

施錠・付き添い・画面の自動ロック（5 分）は IPA 付録 5 物理的対策 1・5 の標準に合わせた。

6.　技術的対策

図表 5　技術的対策の決まり

項目	決まり	台帳の資産（リスク値）
ソフトウェアの更新	OS とソフトは自動更新にする。サポートが終わったソフトは使わない。ソフトウェア台帳で年 1 回確かめる	—
ウイルス対策	全 PC で OS 標準のウイルス対策を有効にし、定義ファイルを自動で更新する	電子メール（6）
無線 LAN	**業務用と来客用を分ける。業務用は登録した機器だけを接続し、パスワードを掲示しない**	無線 LAN のパスワード（9）
工場の LAN	NC 機械への転送用の LAN は、事務所の LAN と分ける	NC プログラム（6）
電子メール	身に覚えのない添付は開かない。迷ったら開く前に総務に聞く。送る前に宛先を確かめ、複数の社外宛ては Bcc にする	電子メール（6）・注文書（電子）（6）
クラウドサービス	使う前に総務に届け出る。多要素認証を設定する。会社の情報を個人のアカウントに置かない	—
バックアップ	共有フォルダを週 1 回、暗号化した外付け HDD に複製し、**1 台は社外に置く**。年 1 回、実際に戻す訓練をする	共有フォルダ（6）・外付け HDD（6）

資料: IPA 付録 5 技術的対策 2〜5、ガイドライン本編の「情報セキュリティ 6 か条」（第 4.0 版で「バックアップを取ろう！」が加わった）

> **戻せることを確かめていない複製は、複製とは言えない。**戻す訓練の結果は記録し、代表に報告する。

7.　様式

どの様式も、紙でも表計算でもよい。記入例を 1 行入れてある。保管は総務（期間は様式ごとに示す）。

図表 6　様式 1　秘密保持に関する誓約書（入社時）

記入欄	記入例・書き方
守ること	在職中・退職後とも、業務で知った客先の図面・取引条件・個人情報を漏らさない
持ち出さないこと	会社の許可なく、情報を私物の機器・個人のメール・クラウドに移さない
返すもの	退職時に、貸与された機器・鍵・記録媒体と、業務の資料をすべて返す
日付・氏名	2026 年 4 月 1 日　（本人の署名）

資料: 当社作成（IPA 付録 5 の記録の項目を参考）。保管: 在職中と退職後 5 年。文言の最終確認は顧問の社会保険労務士

図表 7　様式 2　情報の持ち出し記録

日付	持ち出す人	情報	媒体	目的	承認	返却日
2026-10-06	生産管理 B	図番 MK-2847 の図面	紙（コピー 1 部）	外注先との打合せ	製造部長	2026-10-06

資料: 当社作成（IPA 付録 5 の記録の項目を参考）。保管: 1 年

図表 8　様式 3　事故の第一報

記入欄	記入例・書き方
いつ・誰が気づいたか	2026-10-14 9:20　営業 A
何が起きたか	注文書の PDF を、別の取引先 1 社に誤って送った
影響	単価が 1 件分見えた。個人情報は含まない
取った処置	9:35 誤送信先に電話し、削除を依頼。削除の返信を受けた
報告先と時刻	9:30 代表へ口頭／10:00 本様式を提出

資料: 当社作成（IPA 付録 5 の記録の項目を参考）。保管: 5 年

図表 9　様式 4　委託先の確認票（年 1 回）

記入欄	記入例・書き方
委託先・渡す情報	熱処理の外注先 1 社・図面（加工部分のみ）
秘密保持の取り決め	取引基本契約書の秘密保持条項で足りるかを確認中（足りなければ覚書を交わす）
再委託	無し（ある場合は当社の事前承認）
返却・廃棄	加工完了後 1 か月以内に図面を返却
事故のときの連絡先・確認日	先方 品質課長・2026-11-30 確認

資料: 当社作成（IPA 付録 5 の記録の項目を参考）。保管: 取引終了後 3 年

図表 10　様式 5　教育の記録

日付	内容	対象	出席	欠席者への対応
2026-10-21	本規程の要点・誤送信の事例	PC を使う 16 名	15 名	11 月中に個別に説明

資料: 当社作成（IPA 付録 5 の記録の項目を参考）。保管: 5 年

図表 11　様式 6　退職時の確認

確認すること	確認した人・日付
アカウント（PC・メール・クラウド）を止めた	総務・退職日
貸与した機器・鍵・記録媒体を返してもらった	総務・退職日
共有フォルダの権限から外した	総務・退職日
持ち出した情報が無いことを確かめ、誓約を再確認した	上長・退職日

資料: 当社作成（IPA 付録 5 の記録の項目を参考）。保管: 退職後 5 年

8.　年間の予定

図表 12　情報セキュリティの年間の予定

いつ	やること	誰が	記録
毎年 4 月	台帳の見直し・自社診断（付録 3）・規程の見直し	総務・代表	台帳・診断の点数
毎年 6 月	安否確認の訓練（BCP と一緒に行う）	総務	訓練の記録
毎年 9 月	バックアップから実際に戻す訓練	総務・保守事業者	訓練の記録
毎年 10 月	全従業員の教育（30 分）	総務	様式 5
毎年 11 月	委託先の確認	代表	様式 4
毎月	リスク大の対策の進み具合を部門横断の会議で確かめる	代表	議事録
そのつど	入社（様式 1）・退職（様式 6）・持ち出し（様式 2）・事故（様式 3）	総務・本人	各様式

資料: 当社作成

9.　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 13　外した章

IPA 付録 5 の章	外した理由	戻す条件
組織的対策 2. 監査（内部監査の体制）	監査を行える人員がいない。毎年 4 月の台帳の見直しと自社診断で代える	従業員が 100 名を超えたとき
組織的対策 6.7 特権アカウントの分離	**専任者がいないため分けられない。代表が持ち、12 文字以上と多要素認証で代える**	担当者を置いたとき
組織的対策 7.2 SNS の個人利用	業務で SNS を使っておらず、個人の利用を制限する根拠がない	業務で SNS を使うとき

IPA 付録 5 の章	外した理由	戻す条件
組織的対策 9.9 事業継続計画	外したのではなく、**事業継続計画（BCP）という別の文書に置いた**	—
人的対策 5. 人材育成	専門の人材を育てる計画がない。年 1 回の全員教育で代える	担当者を置いたとき
人的対策 6. テレワーク	テレワークを行っていない	テレワークを始めるとき
技術的対策 3. IT 基盤の運用管理（ログの管理を含む）	サーバー室も専任者もない。ルーターのログの保存は保守事業者との契約で代える	社内にサーバーを置くとき
技術的対策 6. システム開発及び保守	自社でシステムを開発していない	開発を始めるとき

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』（2026-03-27 公開） 付録 5 の目次と照合（2026-11-17）

10.　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	サイバー保険に入るか	リスク大 9 件のうち、対策後も残るものをどう扱うか（移転）。年 12〜18 万円の見込み	代表	2027-01-29
2	**熱処理の外注先との秘密保持の取り決め**	取引基本契約書に秘密保持条項があるかを確かめる。無ければ覚書を交わす	代表	2026-11-30
3	ルーターのログを何日とっておくか	保守事業者との契約に 90 日以上の保存を入れるか	代表	2027-03-31

11.　次にやること

#	やること	誰が	いつまでに
1	改定した本規程を全従業員に配り、15 分で変わった点を説明する	代表	2026-11-30
2	無線 LAN を業務用と来客用に分ける	代表	2026-11-30
3	PC の画面の自動ロック（5 分）を全台に設定する	総務	2026-12-11
4	外付け HDD の 1 台を社外に置く運用を始める	総務	2026-12-25
5	台帳のリスク大の対策の進み具合を、毎月の会議で確かめる	代表	毎月第 2 水曜