HIXOR

三重・桑名のセキュリティ＆自動化スタジオ

サンプルレポート

SECURITY CHECKUP

セキュリティ健康診断
診断レポート

お客様

株式会社サンプル製作所　様

対象サービス	セキュリティ健康診断＋SECURITY ACTION自己宣言支援
診断期間	2026年10月（ヒアリングシート回答および設定確認による）
発行日	2026年11月4日
文書番号	HIX-SAMPLE-001
発行	HIXOR（ヒクサー） 代表 ヒロセ　ユウジ

本書はサンプルレポートです。
登場する企業名・数値・状況はすべて架空のもので、実在の企業・団体とは関係ありません。「セキュリティ健康診断＋SECURITY ACTION自己宣言支援」（¥30,000・税抜）をご検討の方に、納品物である診断レポートの形式と内容の例をお示しするために作成しました。

1. 本レポートについて

本レポートは、ヒアリングシート（セキュリティ追加設問）へのご回答と、機器・アカウントの設定確認の結果を、HIXORの確認チェックリスト（A〜G・全35項目）に沿って整理したものです。各項目の状態は ○ できている ／ △ 一部できている ／ × できていない ／ ― 対象外、で示しています。

チェックリストの内訳は、日常の運用を確認する31項目（領域A〜F）と、 SECURITY ACTIONの宣言に関する4項目（領域G）の、合計35項目です。なお、このチェックリストはHIXOR独自のもので、 IPAが公開している情報セキュリティ自社診断（25項目）とは別のものです（IPA自社診断の実施状況は、領域Gで確認しています）。

各項目の確認方法は、所見（p.5〜7）の「確認方法」欄に、次の区分で示しています。 ヒアリング お客様への聞き取りと、ヒアリングシートへのご回答による確認／ 証跡 設定画面のスクリーンショットなど、お客様から提示いただいた証跡による確認／ 直接 HIXORが設定を直接確認したもの。本診断では、ヒアリングと証跡の提示による確認を行っており、 HIXORがお客様の環境に直接アクセスして設定を確認した項目はありません。

なお、パスワードそのもののような秘密情報は、本診断ではお預かりしていません。 確認は「管理の方法」についてのみ行っています。また本レポートは、現時点の対策状況を整理するものであり、 情報セキュリティ事故が発生しないことを保証するものではありません。

2. お客様プロフィール

会社名	株式会社サンプル製作所　様
業種	金属部品のプレス・切削加工（自動車部品・産業機械部品）
従業員数	16名（役員2名・正社員11名・パート3名）　うちPC利用者 13名
拠点	本社工場・営業所の2拠点
PC・機器	業務用PC 14台（Windows 11：13台／Windows 10：1台）、ファイルサーバー用NAS 1台
メール・グループウェア	Microsoft 365（主にメールを利用）
業務ソフト	弥生会計（経理用PCにインストール）、Microsoft 365アプリ
ファイルの保管	社内NASが中心。一部は個人PCにも保存
ウイルス対策	ウイルスバスター クラウド（全14台に導入）
診断の対象範囲	本社・営業所のPC 14台、NAS 1台、Microsoft 365テナント、共有・バックアップの運用

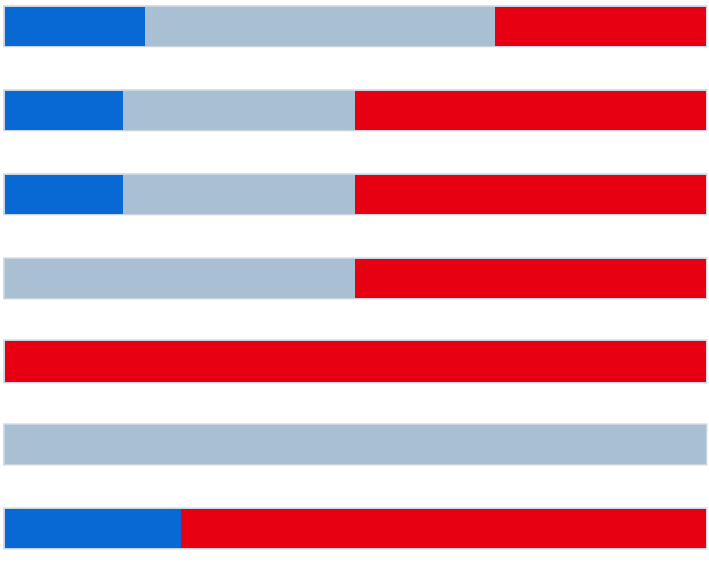
診断の進め方（本サービスでの標準的な流れ）

ヒアリングシート送付 → ご回答 → 設定の確認（メール／チャット）→ 本レポートの作成・納品 → ご希望に応じて、基本方針の文案と90日改善計画をもとに宣言・改善を支援します。ご相談の初期段階のやり取りは、メールまたはチャットで行います。

3. 結果サマリー

全31項目（領域A〜F）の結果は、○ **4項目**・△ **13項目**・× **14項目**でした。 ウイルス対策ソフトの導入のように「入っている」対策がある一方で、アカウントの守りとバックアップの運用に、 優先して埋めるべき穴が集中しています。

○ できている（全31項目中）	△ 一部できている	× できていない
4	13	14



A. 情報セキュリティ6か条 基本の6つの柱の土台	○2 △5 ×3（10項目）
B. 端末・ネットワーク PCとネットワーク機器	○1 △2 ×3（6項目）
C. アカウント・情報管理 IDと情報の置き場所	○1 △2 ×3（6項目）
D. 従業員ルール・教育 人の動きのルール	○0 △2 ×2（4項目）
E. バックアップ・復旧 戻せるかどうか	○0 △0 ×3（3項目）
F. 委託先・廃棄 社外との受け渡し	○0 △2 ×0（2項目）
G. ★★宣言に向けた確認 SECURITY ACTION 二つ星	○1 ×3（4項目）

まずやること（上位3つ）

1. **アカウントの守りを固める** — Microsoft 365の全アカウントで二要素認証（MFA）が未設定で、パスワードの使い回しもあります。侵入の入口を塞ぐ最優先事項です。
2. **バックアップを「戻せる」形にする** — 月1回の手動コピーで、復元は未確認です。ランサムウェア等で暗号化された場合、業務データを戻せないおそれがあります。
3. **退職者のアカウントとPCを整理する** — 退職者のMicrosoft 365アカウントが有効なまま残り、その方のPCもログインできる状態で置かれています。

※ 領域G（4項目）は、SECURITY ACTION二つ星の宣言に向けた確認であり、上記31項目の集計には含まれていません。 本チェックリスト（全35項目＝A〜Fの31項目＋Gの4項目）はHIXOR独自のもので、IPAの公式の情報セキュリティ自社診断（25項目）とは別のものです。

※ 領域ごとの詳しい所見は p.5〜7、リスクの説明と至急対応は p.8、改善計画は p.10 に記載しています。

4. 情報セキュリティ6か条 チェック結果

IPA「中小企業の情報セキュリティ対策ガイドライン」の「情報セキュリティ6か条」に沿った確認結果です。 SECURITY ACTIONの一つ星（★）は、この6か条への取り組みを宣言するものです。

#	項目	状態	コメント
1	OSやソフトウェアは常に最新の状態にする	△	13台は自動更新が有効です。工場の検査用PC 1台が、サポートの終了したWindows 10のまま残っています（A-1／A-2）。
2	ウイルス対策ソフトを導入する	○	全14台にウイルスバスター クラウドを導入済みで、定義ファイルの自動更新も確認できました（A-3／A-4）。
3	パスワードを強化し、使い回しをしない	×	複数のサービスでパスワードの使い回しがあり、長さも8文字前後が中心です。二要素認証（MFA）も未設定です（A-5／C-2）。
4	共有設定を見直す（不要な共有を止める）	△	「リンクを知る全員」が有効な共有が3件残っています。社外との共有ルールは未策定です（A-7／A-8）。
5	バックアップを取る	△	NASから外付けHDDへ月1回、手動でコピーしています。ただし直近の実施は約2か月前で、復元は試したことがありません（A-9／E-2／E-3）。
6	脅威の手口を知る	△	社長と工場長は偽請求書メール等の手口を把握していますが、従業員への共有はこれからです（A-10）。

6か条の見方

6項目のうち ○ 1項目・△ 4項目・× 1項目です。「対策ソフトを入れる」ところまでは進んでいますが、 「アカウントの守り」と「共有・バックアップの運用」が追いついていません。p.10 の90日改善計画では、 この6か条を土台として先に固める順番にしています。

5. 領域別所見（1）

チェックリストの項目ごとに、状態・確認内容（根拠）と確認方法を記録しています。確認方法の区分は p.2 で説明しています。改善計画（p.10）は、この所見の△／×項目から作成しています。

A. 情報セキュリティ6か条の確認（10項目：○2・△5・×3）

No.	確認項目	状態	確認方法	確認内容
A-1	OSはサポート期間内で、自動更新が有効	△	ヒアリング	13台は自動更新が有効。検査用PC 1台がWindows 10のまま（サポート終了）。
A-2	業務ソフトの更新が滞っていない	△	ヒアリング	Microsoft 365アプリは自動更新。PDF閲覧ソフト1台で旧版が残存。
A-3	全PCにウイルス対策ソフトがあり、定義が自動更新	○	証跡	ウイルスバスター クラウドを全14台に導入し、自動更新を確認。
A-4	契約切れ・未導入のPCがない	○	証跡	ライセンス数（14台分）と導入台数が一致。未導入PCなし。
A-5	主要アカウントのパスワードは長く、使い回しがない	×	ヒアリング	使い回しがあり、長さは8文字前後が中心（聞き取りによる。パスワード自体は確認していません）。
A-6	初期パスワードのままの機器がない	×	ヒアリング	NASの管理者パスワードが初期設定のまま。ルーターは変更済み。
A-7	不要な「リンクを知る全員」共有がない	△	証跡	取引先送付用の共有リンクが3件残存。
A-8	社外とのファイル共有ルールが決まっている	×	ヒアリング	ルールはなく、担当者の判断に委ねられている。
A-9	バックアップを取り、保管場所がPC本体と別	△	ヒアリング	NAS→外付けHDDへ月1回手動コピーし別場所に保管。直近の実施は約2か月前。
A-10	経営者・担当者が最近の手口を知っている	△	ヒアリング	社長・工場長は把握。従業員への共有は未実施。

B. 端末・ネットワーク（6項目：○1・△2・×3）

No.	確認項目	状態	確認方法	確認内容
B-1	私物PC・スマホの業務利用ルールがある	×	ヒアリング	私物スマホでメールを確認する従業員がいるが、ルールは未策定。
B-2	ログインパスワード／PINと離席時ロック	△	ヒアリング	全PCにログインパスワードあり。自動ロックは一部のPCのみ。
B-3	ルーター等のファームウェアが最新化	×	証跡	本社ルーターは導入時（2021年）から未更新。
B-4	ルーター管理画面が外部から開けない	○	証跡	インターネット側から開けない設定であることを確認。
B-5	Wi-Fiの暗号化とパスワード管理が適切	△	ヒアリング	WPA2で暗号化。ただしパスワードが工場内に掲示されている。
B-6	使っていないPC・機器が放置されていない	×	ヒアリング	2025年3月の退職者のPC 1台が、ログインできる状態で倉庫に置かれている。

5. 領域別所見（2）

C. アカウント・情報管理（6項目：○1・△2・×3）

No.	確認項目	状態	確認方法	確認内容
C-1	管理者アカウントと日常業務用が分かれている	×	ヒアリング	経理・総務の担当者が、日常業務でも管理者アカウントを使用。
C-2	主要アカウントで二要素認証（MFA）が有効	×	証跡	Microsoft 365の全アカウントで未設定（社長のアカウントを含む）。
C-3	共有アカウントの一覧があり、利用者を把握	△	ヒアリング	共用アカウントが3件あるが一覧はなく、口頭での把握にとどまる。
C-4	退職・異動時のアカウント停止手順がある	×	証跡	手順は未策定。2025年3月の退職者のMicrosoft 365アカウントが有効なまま残っている。
C-5	重要な情報の保管場所が決まっている	△	ヒアリング	顧客図面の置き場所はNASの共有フォルダだが、一部が個人PCのデスクトップにも保存。
C-6	紙書類の施錠保管と廃棄ルールがある	○	ヒアリング	見積書・図面は施錠キャビネットに保管し、不要書類はシュレッダーで廃棄。

D. 従業員ルール・教育（4項目：○0・△2・×2）

No.	確認項目	状態	確認方法	確認内容
D-1	不審なメールを開かないルールが周知	△	ヒアリング	口頭での注意のみで、文書のルールはない。
D-2	振込先変更はメール以外でも確認するルール	×	ヒアリング	ルールがなく、メールだけで判断する運用になっている。
D-3	情報の持ち出しルールが決まっている	×	ヒアリング	USBメモリ・私物クラウドでの持ち出しルールは未策定。
D-4	事故・紛失時の連絡先と手順が決まっている	△	ヒアリング	社長へ電話連絡することにはなっているが、文書化されておらず、不在時の扱いも未定。

この領域で特に注意したい点

C-2（MFA未設定）とC-4（退職者アカウントの残存）は、どちらも「アカウント経由の侵入」に直結します。パスワードの使い回し（A-5）と組み合わさると、1件の漏えいがそのまま社内への侵入につながりかねません。 この2件は、p.8 の「至急対応」として、90日計画に先立って直ちに対処する位置づけにしています。

5. 領域別所見（3）

E. バックアップ・復旧（3項目：○0・△0・×3）

No.	確認項目	状態	確認方法	確認内容
E-1	バックアップの対象データが一覧化	×	ヒアリング	対象の一覧がなく、NAS全体を漠然とコピーしている。
E-2	自動で定期実行され、失敗に気づける	×	ヒアリング	月1回の手動作業で、失敗に気づく仕組みがない。直近の実施は約2か月前。
E-3	復元手順が分かり、テストした記録がある	×	ヒアリング	バックアップからの復元（リストア）を試したことがない。

F. 委託先・廃棄（2項目：○0・△2・×0）

No.	確認項目	状態	確認方法	確認内容
F-1	委託先に渡す情報の範囲と管理を確認	△	ヒアリング	協力会社へ図面データをメールで渡しているが、取り扱いの条件は取り決めていない。
F-2	PC・媒体の廃棄時にデータ消去を行う	△	ヒアリング	廃棄は業者に任せており、データ消去の証明は受け取っていない。

G. SECURITY ACTION 二つ星（★★）の宣言に向けた確認（4項目：○1・×3）

★★の宣言には、宣言の前に実施する「前提要件」（G-1〜G-3）と、前提が揃ったあとに行う「宣言手続き」（G-4）があります。G-4は要件ではなく、手続きそのものです。なお、SECURITY ACTIONは事業者自身が取り組みを表明する自己宣言の制度であり、IPAが審査・認定するものではありません。

前提要件 ― 宣言までに実施すること（3項目）

No.	確認項目	状態	確認方法	確認内容
G-1	IPA自社診断を実施し、結果を保管	○	証跡	本診断に合わせて、IPA「5分でできる！情報セキュリティ自社診断」をご担当者に実施いただきました。結果票はお客様で保管しています。
G-2	情報セキュリティ基本方針を策定	×	ヒアリング	未策定です。本レポート p.11 に文案（抜粋）を添付しています。代表者の承認をもって策定となります。
G-3	基本方針を外部に公表	×	ヒアリング	未実施です（策定後に、自社サイト等で公表します）。

宣言手続き ― 前提が揃ったあとに行うこと（1項目）

No.	確認項目	状態	確認方法	確認内容
G-4	SECURITY ACTIONの宣言・ロゴ取得	×	ヒアリング	未実施です。前提要件（G-1〜G-3）が揃った段階で、SECURITY ACTION管理システムからお客様ご自身に宣言いただきます（p.12）。

領域Eについて

バックアップは「取っている」ものの、自動化されておらず、復元も未確認でした。 ランサムウェアの被害では、社内NASごと暗号化される例が多く報告されています。 「取っている」から「戻せる」へ変えることが、この領域の改善の目的です（p.9 提案2）。

6. 主なギャップとリスク（優先順）

△／×の項目のうち、被害の大きさと起こりやすさから、優先して対処すべきものを6件に絞りました。 専門用語を避け、「何が起きうるか」で説明しています。

至急対応 ― 90日計画を待たず、直ちに実施してください

次の4件は、侵入や被害に直結しやすく、放置する期間が長いほど危険な項目です。 p.10 の改善計画に先立って、まず封じ込めを行ってください。残作業（全アカウントへの展開、手順の文書化、自動化の仕組み化）は、計画の中で完了させます。

1. **退職者のMicrosoft 365アカウントを直ちに停止する**（C-4／ギャップ3）
2. **NASの管理者パスワードを初期設定から変更する**（A-6／ギャップ4）
3. **管理者・代表者のアカウントに二要素認証（MFA）を直ちに有効化する**（C-2／ギャップ1）
4. **最新のバックアップを手動で取得し、復元テストを行う**（E-2・E-3／ギャップ2）

1. アカウントの入口が開いている（MFA未設定＋パスワードの使い回し）

どこかのサービスで漏れたパスワードが、メール（Microsoft 365）でも試されるのが最近の典型的な手口です。 二要素認証がないと、正しいパスワードを入れられた時点でそのまま侵入されてしまいます。社長のアカウントも対象に含まれます。

根拠： C-2（MFA未設定）／A-5（使い回し）／C-1（管理者アカウントの常用）

2. バックアップが「戻せる」状態になっていない

手動コピーは約2か月止まっており、復元は一度も試していません。ランサムウェアでNASごと暗号化された場合、受注・図面・経理のデータを戻せず、業務が止まるおそれがあります。

根拠： E-1／E-2／E-3（領域Eは全項目×）

3. 退職者のアカウントとPCが残っている

退職した方のメールアカウントが今も有効で、その方のPCもログインできる状態です。 「誰が使ったか分からない侵入経路」が残っている状態であり、まず止めるべき項目です。

根拠： C-4（停止手順なし・アカウント残存）／B-6（PCの放置）

4. 機器の「鍵」と「更新」が手つかず（NAS初期パスワード／ルーター未更新）

NASの管理者パスワードが初期設定のままだと、社内に入られたときに全ファイルを触られかねません。 ルーターのファームウェアも2021年から未更新で、既知の弱点が残っている可能性があります。

根拠： A-6／B-3

5. サポートの切れたWindows 10 PCが残っている

検査用PC 1台は、セキュリティ更新が提供されない状態です。ネットワークにつながっている以上、 社内への侵入の足がかりにされるおそれがあります。

根拠： A-1

6. 振込先変更をメールだけで判断している

「振込先が変わりました」という偽のメールで別口座に送金させる詐欺（ビジネスメール詐欺）が中小企業でも起きています。 電話など別手段で確認するルールを決めるだけで、防げる種類の被害です。

根拠： D-2

7. 優先改善のご提案

ギャップへの対処を優先順に示します。ご自身で進められるものと、HIXORの支援メニューが向くものを分けています。 金額はすべて税抜の概算で、正式なお見積もりは別途見積書にて提示します。

#	改善項目	内容	対応方法／概算（税抜）
1	**アカウント防御の整備**	Microsoft 365の全アカウント（13名分）に二要素認証（MFA）を有効化し、パスワードマネージャーを導入して使い回しをやめる。管理者アカウントと日常業務用アカウントも分離する。	HIXOR支援： アカウント防御セットアップ ¥50,000〜 ※ 10名までの料金です。対象13名のため、追加分は別途お見積りとなります
2	**バックアップの自動化と復元テスト**	対象データを一覧化し、3-2-1の考え方（3つのコピー・2種類の媒体・1つは別場所／クラウド）で自動バックアップを組み、実際に復元できることをテストで確認する。	HIXOR支援： バックアップ＆ランサムウェア対策セットアップ ¥50,000〜80,000 ※ 対象データ量・NAS構成により確定します
3	**退職者アカウント・PCの整理**	退職者のMicrosoft 365アカウントを停止し、放置PCはデータの要否を確認して初期化または廃棄する。今後の退職・異動時の手順もあわせて決める。	お客様にて対応 手順の案内は90日計画に付記します
4	**機器の初期設定と更新の是正**	NASの管理者パスワードを変更し、ルーターのファームウェアを最新化する。あわせてWi-Fiパスワードの掲示を取りやめる。	お客様にて対応 手順の案内は90日計画に付記します
5	**Windows 10 PCの入替え**	検査用PCをWindows 11対応機へ入れ替えるか、ネットワークから切り離した単独運用に変更する。	お客様にて対応 機器のご購入はお客様にてお願いします
6	**振込先変更の確認ルールの策定**	「振込先の変更連絡は、電話など別手段で確認してから処理する」ルールを文書にし、経理担当者へ周知する。社外共有・持ち出しのルールもあわせて文書化する。	お客様にて対応 基本方針の策定支援の中で文案作成をお手伝いできます

費用をかけずに先に効くもの

提案3・4・6は、費用をかけず今日から着手できます。まずはこの3件で「開いている入口」を閉じ、 費用の必要な提案1・2は見積書で範囲を確定してから進める順番をおすすめします。 なお、提案3の退職者アカウントの停止と提案4のNASパスワードの変更は、p.8「至急対応」として計画に先立って直ちに行ってください。 提案1のMFAも、管理者・代表者のアカウント分は至急対応に含みます。

8. 90日改善計画

無理なく実行できる件数に絞っています。計画は目安であり、業務状況に応じて順序の入れ替えは可能です。 完了した項目はチェックを入れて保管してください。なお、p.8「至急対応」の4件は、本計画の期間を待たず直ちに実施してください。30日以内の各項目は、至急対応の残作業（全アカウントへの展開、手順の文書化など）を完了させる位置づけです。

30日以内（すぐ効くもの・止血）

#	改善項目	具体的アクション	担当	HIXOR支援メニュー
1	アカウント防御の整備	MFAを全アカウントに有効化し、パスワードマネージャーを導入。管理者アカウントを日常業務用と分離する。	お客様／HIXOR	アカウント防御セットアップ
2	退職者アカウントと放置PCの整理	退職者のMicrosoft 365アカウントを停止。放置PCのデータ要否を確認し、初期化または廃棄する。退職時の手順をメモに残す。	お客様	（手順案内を本計画に付記）
3	機器の初期設定・更新の是正	NASの管理者パスワードを変更し、ルーターのファームウェアを最新化する。Wi-Fiパスワードの掲示を取りやめる。	お客様	（手順案内を本計画に付記）

60日以内（仕組み化）

#	改善項目	具体的アクション	担当	HIXOR支援メニュー
1	バックアップの自動化と復元テスト	対象データを一覧化し、3-2-1構成で自動バックアップ化。復元テストを実施し、結果を記録する。	お客様／HIXOR	バックアップ＆ランサムウェア対策セットアップ
2	Windows 10 PCの入替え	検査用PCをWindows 11対応機へ入れ替える（またはネットワークから切り離す）。	お客様	—
3	共有と確認ルールの文書化	「リンクを知る全員」共有を棚卸しし、社外共有ルールを決める。振込先変更の電話確認ルールも文書化し周知する。	お客様／HIXOR	基本方針の策定支援に含む

90日以内（定着・文書化）

#	改善項目	具体的アクション	担当	HIXOR支援メニュー
1	従業員への手口共有とルール周知	偽請求書メール・サポート詐欺等の手口を朝礼等で共有し、不審メールと事故時の連絡ルールを文書で周知する。	お客様	—
2	基本方針の公表とSECURITY ACTIONの宣言	基本方針（p.11 文案）を代表者が承認し公表する。そのうえでSECURITY ACTIONの宣言を申請する（申請はお客様自身）。	お客様／HIXOR	自己宣言支援（本サービスに含む）

次期候補（90日以降）

- 共有アカウント（3件）の一覧化と、利用者の定期的な見直し
- 私物端末の業務利用ルールの策定
- PC廃棄時に、データ消去の証明を受け取る運用への変更
- 協力会社へ渡す図面データの取り扱い条件の取り決め

9. 情報セキュリティ基本方針 文案（抜粋）

SECURITY ACTIONの二つ星（★★）では、情報セキュリティ基本方針の「策定」と「外部への公表」が要件になります。 本サービスでは、お客様の実態に合わせた文案を作成します。以下は本サンプルのお客様向け文案からの抜粋です （実際の納品では全11条の文案をお渡しします）。実態と合わない条項は、策定の際に削除・修正します。

情報セキュリティ基本方針

株式会社サンプル製作所（以下「当社」といいます）は、事業活動を通じてお預かりするお客様の情報および当社の情報資産を、 事故・災害・犯罪などの脅威から守るため、本基本方針を定め、全従業員がこれを遵守します。

1. 目的　本方針は、当社の情報資産を適切に管理し、情報セキュリティ上の事故を防止するとともに、 万一事故が発生した場合の影響を最小限にとどめることを目的とします。

2. 適用範囲　本方針は、当社の事業活動で取り扱うすべての情報（電子データおよび紙媒体）と、 それを取り扱う役員・従業員・業務委託先に適用します。

3. 管理体制　情報セキュリティに関する責任者は代表取締役とし、対策の決定と見直しを行います。 従業員は、本方針および別途定める運用ルールを遵守します。

5. アクセス管理と認証　情報システムのアカウントは利用者ごとに発行し、共用を避けます。 管理者権限は必要最小限の者に限定し、日常業務用アカウントと分けて運用します。パスワードは十分な長さとし使い回しを禁止します。 主要なサービスでは二要素認証を利用します。退職・異動の際は、速やかにアカウントの停止・変更を行います。

7. バックアップ　重要なデータは定期的にバックアップを取り、保管場所を元データと分離します。 バックアップからの復元手順を確認し、定期的にテストします。

10. 事故発生時の対応　情報漏えい・紛失・不正アクセス等の事故が発生した場合は、 速やかに責任者へ報告し、被害の拡大防止と原因の究明、関係先への連絡を行います。

（抜粋ここまで。全文は全11条で構成されます。）

株式会社サンプル製作所
代表取締役

制定日：（代表者の承認後に記入します）

※ この文案はサンプル企業向けの例です。本文書のまま公表するものではありません。 実際のお客様では、実態に合わせて条項を調整し、代表者の承認を得てから公表します。

10. SECURITY ACTION 宣言までのステップ

SECURITY ACTIONは、IPA（独立行政法人 情報処理推進機構）の制度で、事業者自身が取り組みを宣言する **自己宣言** の仕組みです。IPAが審査して星を授与するものではなく、診断結果の数値（スコア）で星が決まるものでもありません。 本サービスでは、宣言に必要な診断・方針策定・公表の準備を支援します。申請の操作は、お客様ご自身に行っていただきます。

区分	要件と、本サンプルのお客様の現在地
一つ星 ★	情報セキュリティ6か条への取り組みを、SECURITY ACTION管理システムから自己宣言します。 宣言は「取り組みを表明する」もので、6か条の実施がすべて完了している必要はありません。 本サンプルのお客様は、×が1項目（パスワード）・△が4項目あるため、まず90日計画の30日枠に着手したうえで宣言する進め方を推奨しています。
二つ星 ★★	一つ星の取り組みに加えて、（1）IPA自社診断の実施、（2）情報セキュリティ基本方針の策定、（3）基本方針の外部への公表、を行って宣言します。本サンプルのお客様は（1）が実施済みです。 （2）は本レポート p.11 の文案を代表者が承認することで、（3）は自社サイト等への掲載で揃います。

※ 申請はIPAのSECURITY ACTION管理システムから行います。申請にはGビズIDプライムまたはメンバーが必要です。 宣言が受理されると、SECURITY ACTIONのロゴマークを使用できます。デジタル化・AI導入補助金（旧：IT導入補助金）等の申請で宣言が要件になる場合は、 申請期限から逆算したスケジュールを最初に確認します（補助金の申請そのものは本サービスの支援範囲外です）。

11. 次のステップ

1. 本レポートの内容について、ご質問はメールまたはチャットで承ります。
2. 改善のご支援をご希望の場合は、対象メニューの見積書を発行します（見積書 → 注文書 → 着手金30% → 作業 → 検収 → 残金70%の流れです）。
3. 本レポートは「セキュリティ健康診断＋SECURITY ACTION自己宣言支援」（¥30,000・税抜）の納品物です。 業務自動化診断（¥10,000・税抜）と同時にお申し込みの場合は、+¥20,000（税抜）で追加できます。

HIXOR（ヒクサー）
代表 ヒロセ　ユウジ
三重県桑名市
info@hixor.jp
セキュリティに関するご連絡: security@hixor.jp
インボイス登録番号： T6810468076229

文書番号： HIX-SAMPLE-001
発行日： 2026年11月4日
本書はサンプルレポートです（全12ページ）