HIXOR

セキュリティ＆自動化スタジオ

SAMPLE REPORT

SECURITY CHECKUP

セキュリティ診断レポート

法人向け｜オンライン診断シート方式

お客様	株式会社サンプル製作所 様（架空）
診断日	2026年11月11日
チェック	31項目＋業態別4項目
文書番号	HIX-SAMPLE-B-001
確認方法	診断シートのみ／技術的検証なし

本書はサンプルです。登場する情報・数値・回答は架空のものです。診断シートへの回答から作成した例であり、実機確認・脆弱性スキャン・侵入テスト・安全性保証は行っていません。

01 / 本レポートについて

本レポートは架空の法人を想定した納品物サンプルです。セキュリティ対策の実施状況を、オンライン診断シートのご回答だけから整理しています。

項目	内容
業種	金属部品の加工・製造
従業員規模	6〜20名（架空の設定：16名）
業務用端末規模	6〜20台（架空の設定：14台）
主なデータ保管	社内NASとクラウドを併用
業態分岐	リモート接続あり／生産設備ネットワークあり
Webサイト	診断対象のWeb運用なし
確認方法	お客様の回答のみ。証跡・画面・ログ・アクセスなし。

結果の読み方

表記	意味
実施	実施している
一部	一部実施している
未実施	実施していない
未確認	分からない
対象外	対象外

重要な限界

本診断は「安全である」「脆弱性がない」と保証するものではありません。回答者が把握していない設定は「未確認」とし、未実施と断定しません。

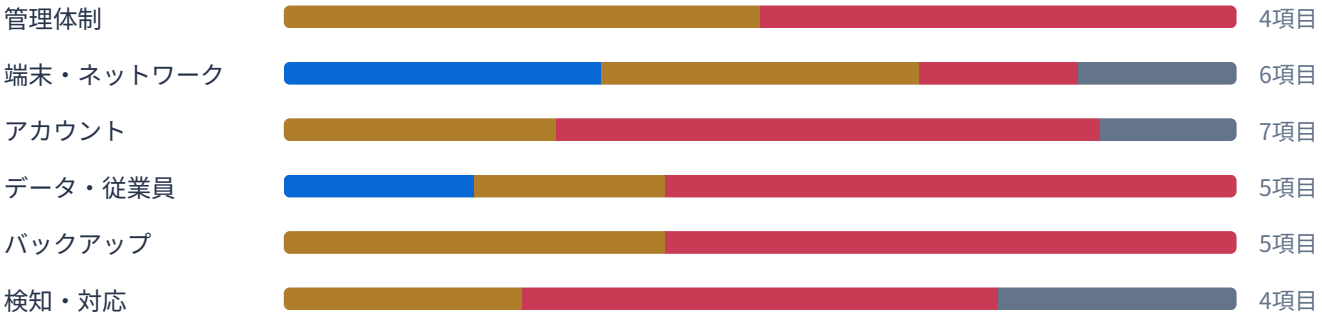
02 / 結果サマリー

法人向け基本31項目の集計。総合安全度スコアではなく、回答状況を示しています。

3	10	15	3	0
実施	一部	未実施	未確認	対象外



領域別の実施状況



重要な見方

基本31項目：実施 3／一部 10／未実施 15／未確認 3／対象外 0。条件質問（遠隔接続・工場）4件は別集計。

優先的に進めたいこと

- 管理者アカウントへの多要素認証（MFA）設定
- 退職・異動時のアカウント停止手順づくり
- バックアップの分離保管と復元確認
- 工場の設備ネットワークと業務ネットワークの接続状況の確認

各項目はお客様の回答に基づく仮の優先順位です。実際の設定状態は確認していません。

03 / 優先リスク

「実施していない」との回答があった項目を中心に、事業の停止・データ損失につながり得る課題を優先しました。

優先	所見／回答に基づく根拠	先に行うこと
最優先	B12：管理者アカウントのMFAが未実施との回答	管理担当者がMFAの設定対象と有効化を確認する。
高	B16：退職・異動時のアカウント停止手順が未実施との回答	利用中アカウントを自社で点検し、停止の担当・期限を決める。
高	B25／B27：分離保管・復元テストが未実施との回答	バックアップ方式を見直し、業務に影響しない復元試験を行う。
高	B22：振込先変更の別経路確認が未実施との回答	既知の連絡先へ電話する等の確認ルールを導入する。
高	M01：生産設備ネットワークの分離が未実施との回答	設備メーカー・社内担当者と接続状況を整理する。

判定の限界

ここでの「最優先」「高」は問診による初期評価です。HIXORが侵入・故障・設定不備を技術的に発見したことを意味しません。

費用をかけずに着手できる対策

- 退職時にアカウント停止担当者を決める。
- 振込先の変更連絡は既知の連絡先に別途確認する。
- 機器の設定状況を保守会社へ「実施済みかどうか」だけ確認する。

04 / 領域別所見（前半）

すべての確認方法は「オンライン診断シートへの回答」です。下の「実施」は検証済みを意味しません。

ID	質問内容	回答
管理体制		4項目
B01	情報セキュリティの責任者または担当者は決まっていますか？	一部
B02	情報セキュリティに関する社内ルールが文書化され、従業員に共有されていますか？	未実施
B03	過去12か月以内に、従業員へのセキュリティ教育や注意喚起を実施しましたか？	一部
B04	外部委託先に対して、情報の取扱いやアクセスに関するルールを定めていますか？	未実施
端末・ネットワーク		6項目
B05	業務で使用するPC・スマートフォン・サーバー等を一覧で管理していますか？	実施
B06	業務用PCのOSは、すべてセキュリティ更新を受けられる状態ですか？（延長更新を含む）	一部
B07	OSや業務ソフトのセキュリティ更新を定期的に実施していますか？	一部
B08	業務用PCには適切な保護機能が導入され、更新されていますか？	実施
B09	ルーターなどのネットワーク機器について、定期的に更新状況を確認していますか？	未実施
B10	インターネット側から社内機器の管理画面へ接続できないよう、適切に制限していますか？	未確認
アカウント		7項目
B11	業務用メールやクラウドサービスで多要素認証（MFA）を利用していますか？	未実施
B12	管理者権限を持つアカウントにも多要素認証を設定していますか？	未実施
B13	サービスごとに異なるパスワードを使い、適切に管理していますか？	一部
B14	ルーターやNASなどの機器で、初期パスワードを変更していますか？	未確認
B15	管理者用アカウントと日常業務用アカウントを使い分けていますか？	未実施
B16	退職・異動時に不要なアカウントを速やかに停止する仕組みがありますか？	未実施

質問の要約ではなく正規の質問文と回答状況を示しています。

05 / 領域別所見（後半）

基本31項目のうち、残り15項目の回答を記録しています。業態別の追加4項目は次ページに掲載しています。

ID	質問内容	回答
アカウント		7項目
B17	アクセス権限を業務上必要な範囲に限定し、定期的に見直していますか？	一部
データ・従業員		5項目
B18	重要な業務データの保管場所と、利用できる人の範囲を把握していますか？	実施
B19	社外向けファイル共有の公開範囲や共有期限を管理していますか？	一部
B20	私物PC・スマートフォンを業務利用する場合のルールがありますか？	未実施
B21	USBメモリや個人用クラウドへの情報持ち出しに関するルールがありますか？	未実施
B22	振込先変更の連絡は、電話など別の方法で確認する運用ですか？	未実施
バックアップ		5項目
B23	バックアップが必要な重要データを把握していますか？	一部
B24	重要なデータを定期的にバックアップしていますか？	一部
B25	元データが攻撃されても守れるよう、バックアップを分離して保管していますか？	未実施
B26	バックアップの失敗や未実施を確認できる仕組みがありますか？	未実施
B27	過去12か月以内に、バックアップから実際に復元するテストをしましたか？	未実施
検知・対応		4項目
B28	不審なログインや警告を確認する担当者・仕組みがありますか？	未確認
B29	情報漏えい・端末紛失等が起きた際の連絡先は決まっていますか？	一部
B30	サイバー攻撃が疑われる場合の初動対応手順がありますか？	未実施
B31	重要なシステムが止まった場合の復旧優先順位を決めていますか？	未実施

05 / 領域別所見（条件質問）

遠隔接続と生産設備ネットワークに関する追加4項目。基本31項目の集計には含めていません。

ID	質問内容	回答
追加：遠隔接続・工場ネットワーク		4項目
R01	社外からの接続に多要素認証等の保護を利用していますか？	未実施
R02	委託先のリモートアクセス権限を必要な期間だけ有効にし、管理していますか？	未実施
M01	生産設備と一般業務のネットワークを必要に応じて分離していますか？	未実施
M02	設備メーカーや保守業者の接続を承認・管理していますか？	未確認

回答から読み取れること

R01・R02・M01は「未実施」、M02は「未確認」です。これらはお客様の回答内容を示すものであり、HIXORによる機器・設定の検証結果ではありません。

遠隔アクセスや工場ネットワークの変更は、業務停止につながることがあります。必要に応じて社内担当者・保守業者に相談し、作業範囲と影響を確認したうえで進めてください。

06 / 未確認と改善計画

まず確認が必要な情報（未確認）

ID	お客様が社内で確認すること	HIXORが要求しないもの
B10	外部から管理画面にアクセスできる設定かどうか	ルーター管理画面・IPアドレス
B14	NASやルーターの初期パスワード変更状況	パスワード自体
B28	不審ログインの通知を受ける担当者の有無	ユーザー名・アラートログ
M02	設備メーカーの遠隔接続の承認方法	VPN情報・接続設定の画像

30／60／90日計画

30日以内

MFAの優先設定、退職時アカウント停止手順、振込先変更の確認ルール。

60日以内

バックアップ保管方式の点検と復元テスト、管理画面公開状況の確認。

90日以内

生産設備ネットワークの接続範囲見直し、役割と運用手順の文書化。

担当者：お客様の経営者・IT担当・設備担当で決定。上記は推奨目標であり、HIXORによる設定変更作業は本診断に含みません。

07 / SECURITY ACTION

SECURITY ACTION（IPA）に関する確認は、セキュリティ実施状況の31項目と分けて記録します。

ID	確認事項	回答
G01	IPA公式25項目の自社診断を実施し、結果を保管していますか？	未実施
G02	情報セキュリティ基本方針を策定し、代表者が承認していますか？	未実施
G03	情報セキュリティ基本方針を外部に公表していますか？	未実施
G04	SECURITY ACTION管理システムで自己宣言を完了していますか？	未実施

制度上の位置づけ

- 一つ星：情報セキュリティ6か条に取り組むことを自己宣言する制度。
- 二つ星：IPA公式の25項目自社診断を実施し、情報セキュリティ基本方針を策定・外部公開したうえで自己宣言する。
- HIXORの31項目はIPAの公式25項目の代替ではない。
- IPAがセキュリティ能力を審査・認定したと表示しない。

回答の読み方

本サンプルではG01〜G04がすべて「未実施」との回答です。★★宣言の前提が整ったとは判断しません。

参考：IPA SECURITY ACTION https://www.ipa.go.jp/security/security-action/entry/

08 / 次のステップ

次のステップ

- 本レポートの「未確認」に挙げた事項をお客様の管理担当者が社内で確認する。
- 直ちにできる対策を実施し、日付・担当・完了状況をお客様で記録する。
- 追加の設定変更や復旧テスト等を外部へ委託する場合は、別途作業範囲と料金を合意する。
- SECURITY ACTIONはお客様ご自身の自己宣言として手続きを進める。

サービスの範囲と料金表示

本サンプルは「セキュリティ診断」（法人向け・30,000円／税抜）の納品イメージです。技術的な検証、ログ調査、脆弱性診断、MFA設定代行、バックアップ構築等は含みません。

診断の限界と免責

> 本診断はお客様の自己申告に基づき、対策状況と潜在的な課題を整理するものです。端末・システムへのアクセス、直接の設定確認、脆弱性スキャン、侵入テストは行っていません。結果は事故が発生しないことを保証しません。

文書番号：HIX-SAMPLE-B-001 ｜ 版：1.0.1
架空データ・サンプル用途のみ。実際のお客様への正式な診断結果ではありません。