

# SBIC® West Japan - News Release -

2026年1月28日

各 位

大阪中小企業投資育成株式会社  
代表取締役社長 小林利典  
(大阪市北区中之島3-3-23)

## 投資先企業景況アンケート結果の発表

下記の通り、当社投資先企業に対して景況アンケートを実施いたしました。  
結果については次頁以下をご覧ください。

調査時点：2025年12月中旬

調査対象先：当社投資先企業1,189社

回答数：678社

回収率：57.0%

---

◇本発表に関するお問い合わせ先

事業ソリューション部

福山 裕人

電話：06-6459-1700

メール：pr@sbic-wj.co.jp

## 景況感は緩やかに改善も、収益面はなお力強さを欠く

投資先企業の2025年度第3四半期の景況アンケートによると、2025年10～12月の売上実績D.I.、利益実績D.I.、業況判断D.I.はいずれも前期から改善し、業況判断D.I.はプラス圏に転じた。売上面では持ち直しの動きが見られる一方、利益面ではコスト上昇の影響が残り、回復にはなお時間を要している。国内需要は底堅さを維持するものの、海外景気の減速懸念、物価高の長期化、人手不足の深刻化などから先行きの業況は慎重な見通しとなっている。

## 売上及び利益実績・業況判断のD.I. (前年同期比) の推移



## 利益実績の増減割合(前年同期比)の推移



① 2025年10～12月期の売上実績D.I.（増収企業割合－減収企業割合）は、前期の0.9から5.5へと改善した。利益実績D.I.は▲7.2から▲0.9へとマイナス幅が大きく縮小し、業況判断D.I.も▲1.6から0.7へとプラス圏に転じた。価格転嫁の進展や需要の底堅さを背景に売上環境は改善したが、人件費や原材料費の上昇が続き、収益の回復にはなお時間を要している。

利益実績D.I.を業種別に見ると、食品、金属製品、建材・金物、産業資材、運輸・倉庫の5業種がプラス圏となった。特に運輸・倉庫は▲4.3から+25.0へと大幅に上昇した。一方、マイナス圏となった4業種のうち、建設・不動産は前期のプラスからマイ

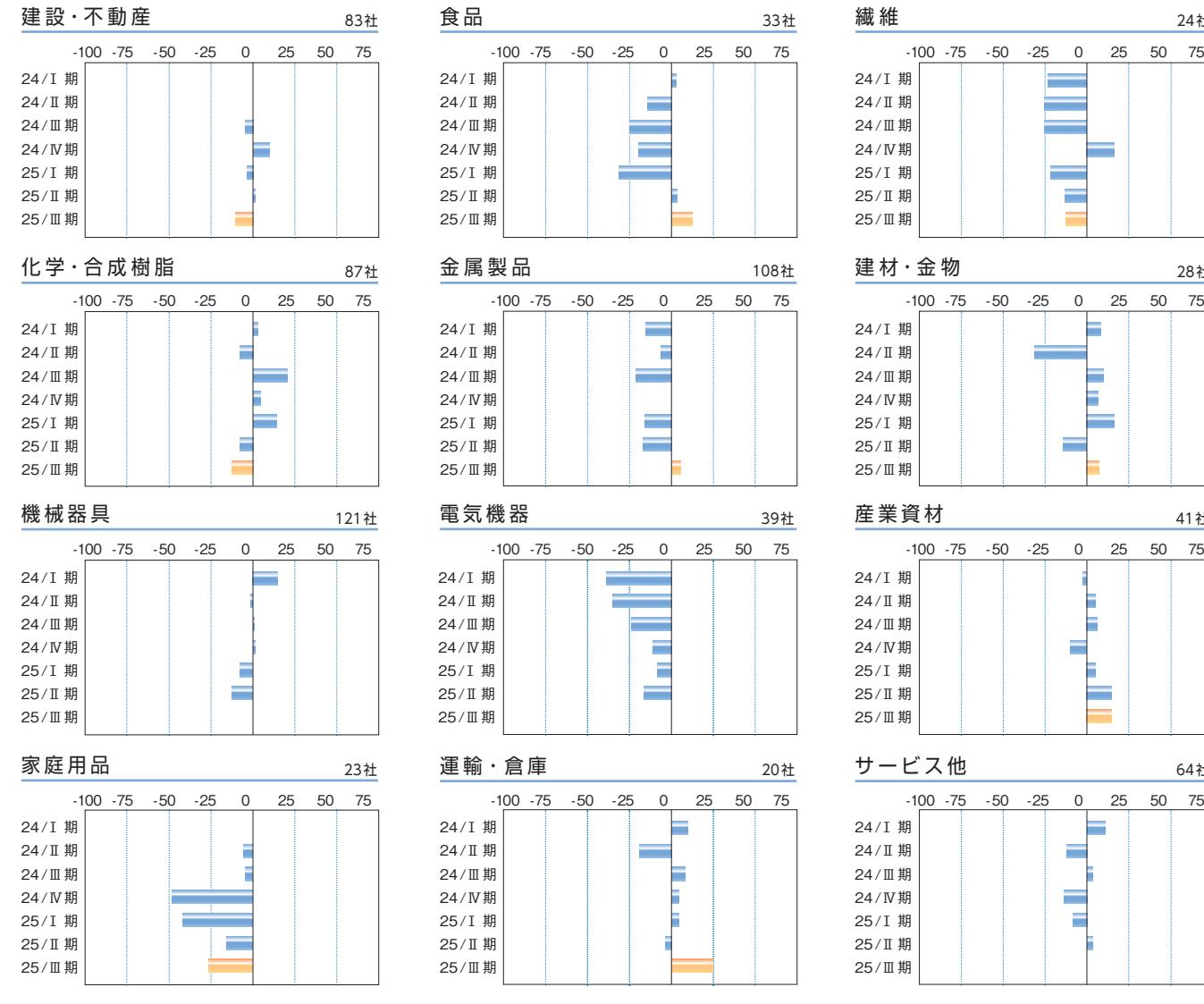
ナスに転じ、繊維、化学・合成樹脂、家庭用品は引き続きマイナス圏にとどまった。

② 2026年1～3月期の見通しD.I.では、2025年10～12月実績と比較して売上実績D.I.は5.5から3.4へとやや低下し、利益実績D.I.は▲0.9から▲2.7へと再びマイナス幅が拡大する見込みとなった。業況判断D.I.も0.7から▲0.7へとマイナス圏に戻る。国内需要は底堅さを維持するものの、海外景気の減速懸念、物価高の長期化、人手不足の深刻化などから先行きは慎重な見通しとなっている。

中小企業においては、先行き不透明な環境下で持続的な成長を実現するため、省力化投資やDXの推進に加え、人材の確保・育成や働きやすい職場づくりに向けた取り組みが一層重要となる。コスト上昇局面においても、生産性向上を通じて競争力を維持できるかが、今後の業況を左右する鍵となる。

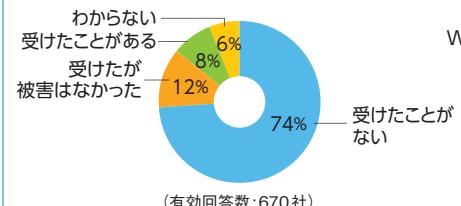
利益実績の増減割合で見ると、増益を見込む企業の割合は20.1%と、10～12月実績から6.6ポイント低下した。一方で、減益を見込む企業の割合は22.8%で、前

## 主要業種別利益実績のD.I. (前年同期比) の推移



## IT活用リスク・サーバー攻撃について

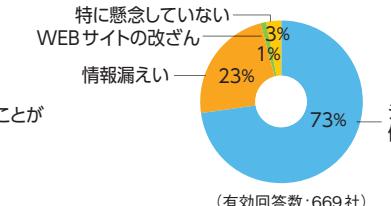
## ● サイバー攻撃・被害を受けたことがありますか



近年、企業のデジタル化が進む一方で、サイバー攻撃による被害は中小企業にとっても無視できない経営リスクとなっています。ITシステムの停止や情報漏えいは、事業継続に大きな影響を及ぼす危険性があり、経営者として適切な対策を講じることが求められています。そこで今回は、中小企業におけるサイバー攻撃の実態やリスク認識、対策状況についてアンケートを実施しました。

サイバー攻撃や被害の経験については、「受けたことがない」が74%と大半を占めました。一方で、「受けたが被害はなかった」が12%、「受けたことがある」が8%、約2割の企業が何らかの形でサイバー攻撃を経験

## ● ITの活用で、どのようなリスクを懸念していますか

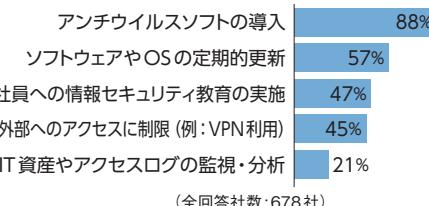


しています。また、「わからない」と回答した企業も6%あり、被害の有無を把握しきれていないケースも見受けられます。

IT活用において懸念しているリスクは、「システムの停止、障害」が73%と最も多く、業務への影響を強く意識している企業が多い結果となりました。次いで「情報漏えい」が23%となり、顧客情報や機密情報の管理に対する不安も示されています。一方で、「WEBサイトの改ざん」は1%、「特に懸念していない」は3%にとどまり、多くの企業で何らかのリスクを意識している状況が明らかになりました。

実施しているサイバー攻撃対策について

## ● どのようなサイバー攻撃対策を実施していますか (複数回答)



は、「アンチウイルスソフトの導入」が88%と最も多く、「ソフトウェアやOSの定期的更新」(57%)や「社員への情報セキュリティ教育の実施」(47%)、「外部へのアクセスに制限」(45%)が続きました。一方で、より高度な対策である「IT資産やアクセスログの監視・分析」は21%にとどまり、対策の深度には差があることがうかがえます。

サイバー攻撃は年々巧妙化しており、単一の対策だけでは十分とはいえません。IT活用を安心して進めいくためには、基本的なセキュリティ対策の徹底に加え、社員教育やアクセス管理など多層的な防御体制の構築が求められています。

2025年12月調査