



2026年、ITは「道具」から「経営の生命線」へ

# AIという「新たな労働力」と、セキュリティという「信頼の証」を手にするために



人手不足を解決し、取引先から選ばれ続ける会社であるために。中小企業の現場を変える「攻め」と「守り」の最重要キーワードを、事例とともにやさしく解説します。

## 攻めのIT AIは「画面の中」から「現場」へ

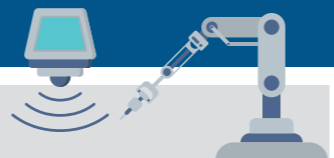


これまでのAIは「チャットで質問に答えてくれるすごい辞書」でしたが、2026年は「手足を動かし、自ら考えて仕事をする」段階へ進化します。

### ①フィジカルAI (Physical AI)

#### ①用語概説

これまで画面の中にいたAIが、ロボットやドローン、センサーといった「物理的な体」を持って現実世界で動く技術のことです。



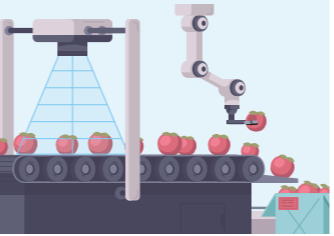
#### ②具体的な事例・活用方法

##### 倉庫工場

従来のアームロボットとは違い、「これは壊れやすいトマトだ」とAIが判断して、優しく掴んで箱詰めするロボット。

##### 建設点検

人が登るには危険な屋根や鉄塔の点検を、ドローンが自律飛行で行い、サビやヒビをAIが即座に見つける。



#### ③中小企業へのインパクト・メリット

人手不足が深刻な「現場仕事」の救世主です。重労働であったり危険を伴う仕事をAIロボットに任せることで従業員の健康管理、安全、そして定着率向上が期待できます。また24時間稼働による生産性アップが現実的な価格で導入可能になりつつあります。

### ②AIエージェント (自律型AI)

#### ①用語概説

指示されたことだけをやるのではなく、「目標」を与えれば、そこに至るまでの手順を自分で考えて実行してくれるAIです。「優秀な秘書」のような存在です。

#### ②具体的な事例・活用方法

##### 出張手配

「来週の大阪出張、予算3万円で頼む」と言うだけで、新幹線の時刻を調べ、ホテルを比較し、予約まで完了させてカレンダーに登録する。

##### 受発注業務

在庫が減ってきたら、過去の売れ行き予測を加味して、自動で仕入先に発注メールを送る (人は最終確認ボタンを押すだけ)。



#### ③中小企業へのインパクト・メリット

社長や管理職が本来やるべき「経営判断」や「営業」に集中できます。事務作業にかかる時間を劇的に減らせるため、少人数精鋭の組織でも大企業並みのスピードで業務を回せるようになります。

### ③ソブリンAI (AI主権)

#### ①用語概説

海外の巨大IT企業 (GoogleやOpenAIなど) だけに依存せず、「自国のデータは自国のルールで守り、自国の言語・文化に強いAIを使う」という考え方です。国産AIモデルなどがこれにあたります。

#### ②具体的な事例・活用方法

##### 行政・法務手続き

日本の複雑な法律や商習慣、独特な言い回し (「善処します」など) を正確に理解できる国産AIを使って、契約書チェックや申請書類を作成する。

##### 機密データ管理

顧客データが海外のサーバーに渡るのを防ぐため、国内サーバーで完結するAIサービスを利用する。



#### ③中小企業へのインパクト・メリット

「情報漏洩リスク」の低減です。特に官公庁や重要インフラ企業と取引がある場合、「データがどこにあるか」が厳しく問われるため、国産AIの活用が取引継続の条件になる可能性があります。

### ④エッジAI (オンデバイスAI)

#### ①用語概説

インターネット (クラウド) にデータを送らず、手元のパソコンやカメラ、スマホの中 (エッジ) でAI処理を完結させる技術です。

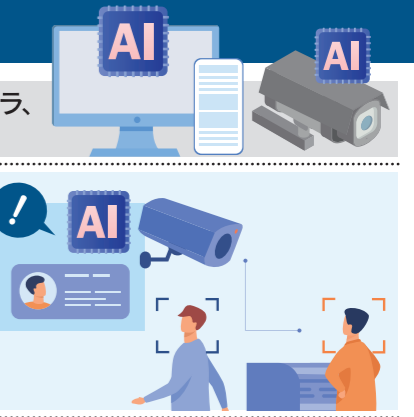
#### ②具体的な事例・活用方法

##### 店舗工場

ネットが不安定な場所でも、監視カメラが「不審者」や「不良品」を瞬時に検知してアラートを鳴らす。

##### 社内PC

インターネットに繋がらないPC内で、議事録の要約や翻訳を行う (情報が外部に出ない)。



#### ③中小企業へのインパクト・メリット

最大のメリットは「速さ」と「安さ」と「安心」です。通信費がかからず、反応がリアルタイム。そして何より、カメラ映像や社内データが外部に送信されないため、プライバシーや機密保持の観点で非常に導入しやすくなります。

# 守りのIT セキュリティは「防御」から「信頼の証」へ

攻撃手法が巧妙化した2026年において、セキュリティ対策は「コスト」ではなく「取引のためのパスポート」になります。

## ①ゼロトラストセキュリティ (Zero Trust)

### ①用語概説

「社内ネットワークだから安全」という考えを捨て、「誰も信用しない(ゼロトラスト)。全てのアクセスをその都度確認する」というセキュリティの考え方です。

### ②具体的な事例・活用方法

#### ログイン強化

IDとパスワードだけでなく、スマホへの通知承認(多要素認証)を必須にする。

#### チェック機能強化

社長のPCであっても、ウイルス対策ソフトが最新でなければ社内システムにアクセスさせない。



### ③中小企業へのインパクト・メリット

テレワークや出張先からのアクセスが当たり前になった今、「どこで仕事をしていても安全」な環境を作れます。万が一IDが盗まれても、簡単には侵入されないため、被害を最小限に抑えられます。



## ②ランサムウェア対策 (二重恐喝型)

### ①用語概説

データを暗号化して使えなくするだけでなく、「身代金を払わないと、盗んだデータをネットに公開するぞ」と脅す(二重恐喝)手口です。

### ②具体的な事例・活用方法

#### バックアップの隔離

ネットワークから切り離れたHDDや、書き換え不可能なクラウドストレージにバックアップをとる(犯人がバックアップまで消せないようにする)。

#### データの暗号化

盗まれても中身が見られないよう、ファイル自体を暗号化しておく。



### ③中小企業へのインパクト・メリット

「バックアップがあるから大丈夫」が通用なくなっています。顧客情報が漏れれば信用は地に落ちます。対策を強化することは、自社の存続だけでなく、取引先や顧客を守ることに直結します。

## ③AI駆動セキュリティ

### ①用語概説

AIを使って攻撃を仕掛けてくるハッカーに対し、こちらもAIを使って24時間365日防御することです。「AIの強い警備員さん」に守ってもらイメージです。

### ②具体的な事例・活用方法

#### メール防御

AIが作った巧妙な詐欺メール(日本語が完璧で、上司になりすましたものなど)を、防御側のAIが見破って隔離する。

#### 異常検知

夜中の3時に突然大量のデータ通信が始まったなど、普段と違う動きをAIが即座に検知して遮断する。



### ③中小企業へのインパクト・メリット

専任のセキュリティ担当者を雇う余裕がない中小企業こそ恩恵があります。人間が監視しきれない脅威をAIが自動で防いでくれるため、低コストで高度なセキュリティを実現できます。

## ④サプライチェーンセキュリティ評価認証

### ①用語概説

大企業が取引先(中小企業)を選定する際、「セキュリティ対策がしっかりできているか」を評価・格付けする仕組みです。いわば「セキュリティの健康診断書」です。

### ②具体的な事例・活用方法

#### 取引条件

親会社から「セキュリティチェックシート(評価制度)」へ、回答を求められ、一定の点数以上でないとなし発注が止まる。

#### 第三者認証

「SECURITY ACTION」や「ISMS」などの認証マークを取得し、名刺やHPに掲載する。



### ③中小企業へのインパクト・メリット

これが最も経営に直結します。対策が不十分だと「仕事が取れない」時代になります。逆に言えば、しっかり対策して認証を得ておけば、競合他社に対する強力なアピールポイント(差別化)になります。

### Column

経済産業省のWebサイト、「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)」を参照・要約してみました。

<https://www.meti.go.jp/press/2025/12/20251226001/20251226001.html>を、できるだけ忠実に要約した文書になります。

### 背景・目的

- **背景** 取引先に波及するサイバー攻撃の頻発により、サプライチェーン全体の対策強化が必須。
- **課題** 発注元の「状況把握の難しさ」と、委託先の「多様な要求への対応負担」の解消。
- **目的** 対策状況を可視化する「SCS評価制度」により、全体のセキュリティ水準を向上させる。

### 制度の仕組み (3段階の対策)

- **★3(基礎)** 全企業が最低限実装すべき、防御と体制整備。(専門家確認付き自己評価)
- **★4(標準)** 標準的な目標。ガバナンスや検知・対応を含む包括的対策。(第三者評価)
- **★5(高度)** 到達目標。リスクベースでの改善とベストプラクティスの実施。(第三者評価、2026年度以降に具体化)



### 最初の一歩!

始めてみてはいかがでしょうか?

#### 1. 【AI活用】事務作業を「1つ」楽にする

いきなり会社全体を自動化する必要はありません。「AIエージェント」のような機能を使い、面倒な事務作業をひとつだけ任せてみてください。

#### 2. 【セキュリティ】「健康診断」で現状を知る

セキュリティ対策も、難しく考える必要はありません。自社のセキュリティ状況のチェック(健康診断)を行ってみてください。



ぜひ、ご相談ください!  
御社の  
DX伴走パートナーで  
あり続けます。

