

2025年。私たちを驚かせ、揺るがしたのは、「AIの革新的進化」と「サイバー攻撃の脅威」でした。未来のヒントとなる重要キーワードを、ここでおさらいしましょう。



2025年のビジネスシーンを席巻した、重要キーワードをピックアップしました!



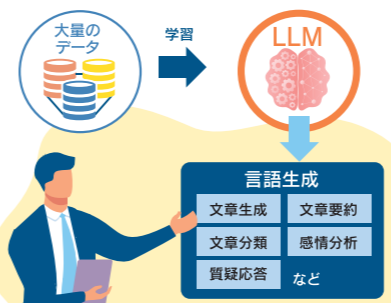
2026年も、AIの進化やセキュリティの脅威は止まることはありません。だからこそ昨年情報を整理し、しっかりと足元を固めておきましょう。

●まずはAIについて

新聞、雑誌、そしてネット。
AIの文字を見ない日はありませんでした。
わずか数ヶ月で世界を一変させた、
その驚異的な進化の「要」をおさらいします。

LLM (大規模言語モデル)

LLMは、大量のテキストデータを学習し、人間のように言葉を理解・生成するAIです。要約、翻訳、メール作成、議事録整理、FAQ作成などを自然な日本語の指示でこなします。ただし、もっともらしい誤情報(ハルシネーション)を出力する可能性があるため、数字や固有名詞、規程などは必ず一次情報での確認が必要です。

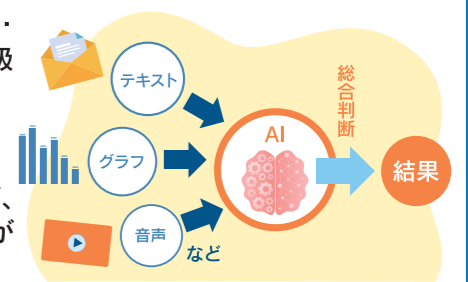


たとえ話 「超優秀な文章編集者+秘書」です。あなたが「目的(誰に何を)」と「材料(箇条書き)」を渡すと、それを読みやすく整えて形にするのが得意です。

事例 ChatGPT / Gemini / Claudeなど。
中小企業では、問い合わせ返信の下書き、社内文書の要約、議事録の清書、マニュアル原案作成、営業トークの言い回し調整などで活用されています。

マルチモーダルAI

文字(テキスト)だけでなく、画像・音声・動画など複数の種類(モード)の情報を扱えるAIです。
「画像を見て状況を説明する」
「会議音声を文字起こしして要約する」
「図表を読み取ってポイント化する」など、
入力も出力も「文字だけ」に限らない点が特徴です。



たとえ話 “目と耳もついたAIアシスタント”です。文章だけの相談員ではなく、現場の写真を見たり、実際の音声を聞いたりして状況を理解してくれます。

事例
画像 設備の写真から部品名を推定し、注意点を文章化した報告書を作成。
音声 会議録音から文字起こしを行い、要点とToDoを自動抽出。
図表 資料内のグラフや表を読み取り、要約や解説文を作成。

RAG (検索拡張生成)

RAGは、LLMに“外部の知識を思い出させる”仕組みです。回答を生成する前に、社内文書や規程、過去のFAQなどを検索して必要な部分を取り出し、それを材料にします。これにより、AIが一般論ではなく「自社のルール・自社の資料」に基づいた回答を出せるようになります。

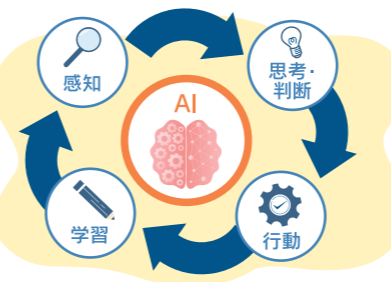


たとえ話 LLMが“文章が得意な新人”だとすると、RAGは“社内の資料棚から必要ページを渡す先輩”です。正しい資料を渡してから書かせるので、回答のズレや嘘が減ります。

事例
社内規程や就業規則を読ませ、問い合わせへの一次回答を作成。
製品マニュアルや過去の障害対応履歴から、サポートFAQを自動生成。
過去の見積条件や契約ひな形を参照し、提案書の抜け漏れをチェック。

AIエージェント (Agentic AI)

LLMが単に「文章を作る」だけでなく、目的達成のために自ら手順を考え、ツールを使って作業を進めるAIです。「メール作成→カレンダー確認→会議設定→議事録テンプレート作成」のように、複数のステップを連続して実行します。実務では、暴走を防ぐために人の承認(OK)や実行範囲の制限が重要です。

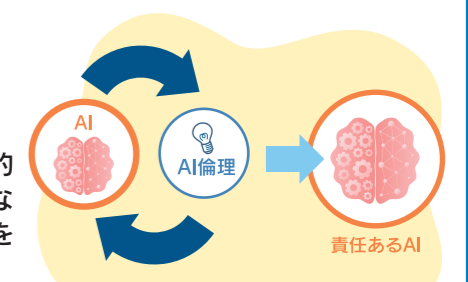


たとえ話 LLMが“相談に答える人”なら、AIエージェントは“実際に手を動かす秘書”です。ただし、勝手にメール送信や削除をしないよう、「権限」と「確認」のルールが必要です。

事例
問い合わせ内容を分類し、担当への振り分け、返信案作成、下書き保存まで実行。
月次の売上データを集計し、差異コメント案と報告メールの下書きを作成。
採用候補者の情報を整理し、面接日程候補の提示と案内文を作成。

AIガバナンス (Responsible AI)

AIを安全に使うための「社内ルール・体制・チェック(監査)」の事です。「何を入力してよいか」「誰が使えるか」「結果をどう確認するか」などを定め、情報漏えい、誤情報、著作権侵害、差別的表現などのリスクを抑えます。“使わせない”のではなく、安心して使える環境を整えるのが目的です。



たとえ話 AIは便利な“共用の高性能コピー機”のようなものです。非常に便利ですが、ルールがないと機密資料を置き忘れたり、誤って配布したりする事故が起きます。だからこそ利用手順と点検が必要です。

事例
入力禁止 個人情報・機密情報は入力しない(または専用環境に限定)。
確認ルール 社外への提出物は、人が必ず事実確認をしてから使用する。
監査 利用ログの保存、プロンプトや出力サンプルの定期点検と教育実施。

●次はサイバー攻撃とセキュリティ



大手企業への攻撃が大きなニュースとなった2025年。「セキュリティ対策はコストではなく投資である」という認識と、「誰もが被害になる」という認識が、今、確固たる常識となりました。



RaaS

RaaS(Ransomware as a Service)は、ランサムウェアの開発者(運営側)が、攻撃に必要なツールや仕組み一式を“サービス”として提供し、別の攻撃者(実行役=アフィリエイト)がそれを使って攻撃する“分業モデル”です。これにより、専門性が高くなっても攻撃を始めやすくなり、被害が拡大しやすい構造になっています。

たとえ話 「詐欺の“開業セット”を売る業者」と「それを使って実行する営業役」が分かれているイメージです。道具と手順がパッケージ化されているので、参入障壁が下がります。

事例 近年は、実行役がRaaSを利用して侵入に成功すると、社内で権限を奪いながら横展開し、最後に暗号化+情報持ち出し(公開の脅し)まで一気に進めるケースが典型です。運営側と実行役が成果配分で動くため、攻撃の“量産”につながりやすい点が特徴です。

ランサムウェア&二重恐喝

ランサムウェアは、社内データやサーバーを暗号化して使用不能にし、復旧と引き換えに身代金を要求する攻撃です。近年主流の「二重恐喝」は、暗号化に加え、事前にデータを盗み出し、「金を払わないならデータを公開する」と脅して圧力をかけます。

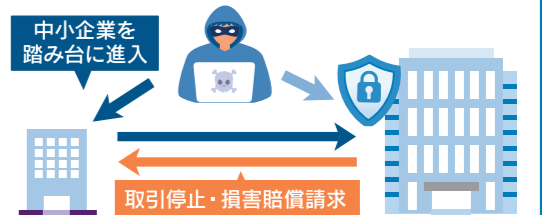


たとえ話 会社の書類を鍵付き倉庫に閉じ込めるだけでなく、同時にコピーを持ち出して“ばらまくぞ”と脅すイメージです。

事例 社内システムが広範囲に停止し、受注・出荷・会計業務が長期間ストップ。復旧対応中に「情報流出の可能性」や「データ公開の示唆」を受け、対応が複雑化・長期化するケースが多発しています。

サプライチェーン/委託先リスク

自社のセキュリティが堅固でも、委託先・取引先・ベンダーが攻撃を受け、そこを踏み台にして自社へ侵入されたり、委託先に預けたデータが漏えいしたりするリスクです。



たとえ話 正面玄関の鍵をどれだけ頑丈にしても、裏口(委託先の出入口)が開いていたら侵入される、という話です。

事例 委託先の認証情報が盗まれ、そこから本体ネットワークへ侵入されて被害が拡大した事例や、委託先がランサムウェア被害に遭い、預けていた顧客個人情報流出した事例などが報告されています。

閉域網(境界内型)セキュリティの限界

閉域網/境界内型セキュリティは、「社内ネットワークの境界(入口)を固めれば安全」という前提の守り方です。しかし、クラウド利用・テレワーク・委託先連携で業務の出入口が増え、さらに一度侵入されると内部で横展開されやすいため、境界だけでは守り切れない場面が増えています。

たとえ話 会社を塀で囲った敷地だとすると、閉域網は「門を厳重にする」対策です。ただ、出入りが増えたり、敷地内に持ち込まれたりすると、門が堅くても中で被害が広がるのが限界です。

事例 境界の入口(VPN機器など)を突破されると、攻撃者が社内で認証情報を奪い、権限を広げながら重要サーバーへ到達し、最終的に暗号化や情報持ち出しに至る——という流れが報告されています。また、メール等で端末が侵害されると、境界の内側に“入口”ができてしまい、同様に被害が拡大します。

イミュータブルバックアップ

バックアップで最も重要なのは“取る”ことより“戻せる”ことです。攻撃者はバックアップデータ自体も破壊しようとするため、書き換え不可能な形式(イミュータブル)での保管や、ネットワーク分離が必須です。また、手順通りにシステムを戻せるかを確認する「復旧訓練」も欠かせません。



たとえ話 非常食は買うだけでは不十分です。期限や保管場所、開け方を確認し、実際に「食べられるか」を試食(訓練)しておくのと同じです。

事例 ランサム被害でシステム停止後、バックアップはあったものの「戻すのに時間がかかりすぎる」「一部破損していた」などの理由で、事業再開が大幅に遅れたケースがあります。平時の訓練が復旧速度を左右します。

●Windows 10サポート終了と「2025年の崖」が重なった2025年、まさに待ったなしの年でした。ICTやAIの積極活用、そして企業生産性を高めるDXへの投資は、もはや最優先事項です。

Windows 10 サポート終了(2025/10/14)

Windows 10は2025年10月14日でサポートが終了しました。以降はセキュリティ更新や技術支援が提供されなくなるため、使い続けることは極めて危険です。

たとえ話 サポート切れOSは、メーカーの点検・部品交換が止まった車で高速道路を走り続けるようなものです。走れても、故障や事故のリスクが格段に上がります。

- 事例**
- 新たな脆弱性が修正されず、ウイルス感染や不正アクセスの標的になる。
 - 取引先や監査において「管理不備」とみなされ、信用の低下を招く。
 - 周辺ソフト(Microsoft 365など)も連動してサポート対象外となる。
 - 更新対応が遅れると、駆け込み需要による品不足やエンジニア不足、コスト増の影響を受ける。



「2025年の崖」× DX

経済産業省が警鐘を鳴らした課題です。老朽化・複雑化した既存システム(レガシーシステム)が足かせとなり、新しいデータ活用やDXが進まないと、企業の競争力が低下し、大きな経済損失につながるという問題です。

たとえ話 増改築を繰り返した古い建物のような状態です。配線が複雑に絡み合い、「リフォームしたいのに、どこを触ると電気が止まるかわからない」ため、手出しができず最新設備も入れられません。

- 事例**
- 法改正やビジネスの変化にシステムが対応できず、機会損失を生む。
 - 保守担当者の退職・高齢化により、システムがブラックボックス化(属人化)する。
 - 古いシステムの維持管理に予算と人が割かれ、攻めのIT投資(DX)にリソースが回らない。



さいごに

2025年は、AIの革新的な進化と、巧妙化するサイバー攻撃の脅威が同時に表面化し、「デジタル変革待ったなし」の年となりました。生産性向上のためのAI活用も、強固なセキュリティと最新のIT環境があって初めて実現します。

お客様が安心して未来へ踏み出せるよう、私たちはこれらの重要キーワードを基に、次のステップにつながる確かなIT基盤づくりをサポートしてまいります。

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。

