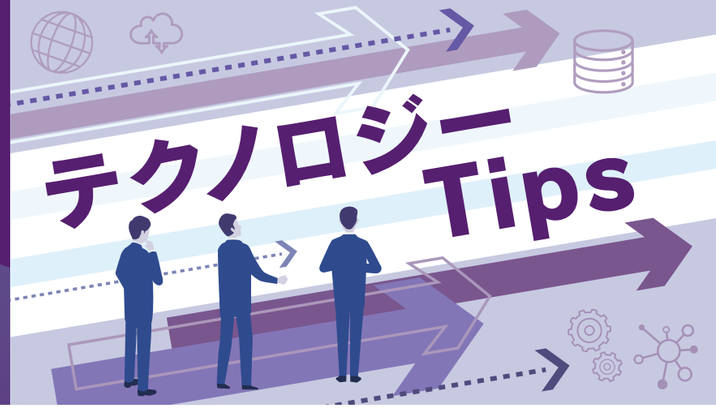
今こそ知りたい Tech Tips!

仕入先、外注先、業務の委託先、そして毎日使っているクラウドサービス。御社は今、何社とつながって仕事をしていますか？

なぜ中小企業がサイバー攻撃の最大のターゲットになるのでしょう。

守るべきものは、自社の情報だけではありません。
取引先とのつながりもまた、長い時間をかけて築いた大切な資産です。



1. サプライチェーンとは、そもそも何を指す言葉か

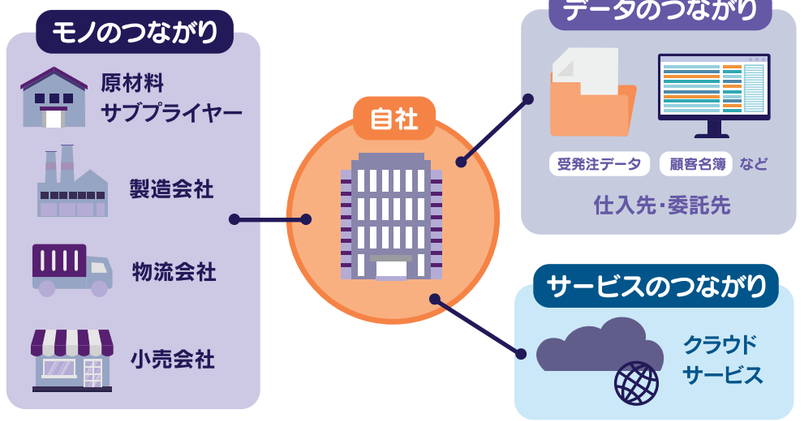
サプライチェーンは、日本語では「供給連鎖」と訳されます。原材料の供給者から、部品の製造、組み立て、輸送、販売を経て、最終的に消費者の手元に届くまで。**複数の企業がそれぞれの工程を分担しながらつながっていく、一連の流れ全体**を指す言葉です。経営の用語として広まったのは1980年代の米国で、当初は「サプライチェーン・マネジメント」、つまり供給の流れ全体をどう管理するかという文脈で使われていました。

なぜ、企業はつながるようになったのか

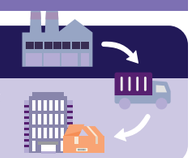
もともと経済学には、分業という基本的な考え方があります。
1社ですべての工程を抱え込むよりも、各社がそれぞれ得意な工程に専念したほうが、全体としての生産性は高くなる、という考え方です。日本のものづくりは、この分業を非常に高い水準まで磨き上げてきました。
部品ごとに専門の会社が担い、必要なものを、必要なときに、必要な量だけ受け渡す。余分な在庫を持たない仕組みは、原価を下げ、品質を高め、日本製品の競争力を支えてきました。
ここで見落とされがちなことがあります。
この連鎖の大部分を担っているのは、中小企業だという事実です。2025年版の中小企業白書によれば、中小企業は日本の雇用のおよそ7割を担っています（出典①）。
つまりサプライチェーンとは大企業のための言葉ではなく、それを支える一社一社の話なのです。

効率を高めるほど、余裕は減っていく

ただし、分業と在庫の圧縮を突き詰めていくと、連鎖のどこか一箇所が止まったときに、その影響が全体へ及びやすくなります。これは仕組みの欠陥ではなく、効率と余裕を交換した結果です。
そして近年、この連鎖に乗るものが増えました。かつては材料や部品といったモノが中心でしたが、今はデータとサービスも同じ連鎖の上を流れています。
整理すると、どの業種の会社にも次の3つのつながりがあります。



モノのつながり



部品、原材料、商品の仕入先です。相手が止まれば、自社の出荷も止まります。

データのつながり

受発注データ、図面、顧客名簿、給与計算。取引先や委託先と、日常的に情報をやり取りしています。

サービスのつながり

会計ソフト、勤怠管理、クラウドストレージ、パソコンの保守業者。自社の業務は、外部の会社が提供する仕組みの上で動いています。

ここで一度、手を止めて数えてみてください。取引している会社、業務を任せている会社、契約しているクラウドサービス。全部で何社になりますか。多くの会社で、20社を超えるはずです。

2. つながりが生む、2種類のリスク

サプライチェーンのリスクには、性質のまったく違う2つの顔があります。ここを分けて考えないと、対策を打つ場所を間違えます。

リスクA：止まるリスク

取引先が止まると、自社も止まります。相手が被害に遭っただけで、自社には何の落ち度がなくても、仕事が進まなくなります。原因はサイバー攻撃に限りません。
地震、水害、火災、取引先の廃業。どれも同じ結果をもたらします。

リスクB：広がるリスク

自社が攻撃を受けると、被害は取引先へと流れていきます。自社のパソコンから盗まれた情報の中には、取引先の図面や顧客名簿が含まれています。自社のメールアカウントが乗っ取られれば、取引先に偽の請求書が届きます。このとき自社は、被害者であると同時に、取引先から見れば被害を広げた側になってしまいます。

情報処理推進機構（IPA）が2025年2月に公表した調査では、サイバー被害を受けた中小企業975社のうち、**およそ7割が「取引先に影響があった」**と回答しています（出典②）。
被害は、自社の中だけでは収まりません。

3. なぜ、中小企業が被害に遭うのか

中小企業自身が守るべきものを持っています。

長年かけて積み上げた顧客名簿、独自の加工技術や図面、見積の単価表、従業員の個人情報、そして銀行口座の情報。これらはどれも、事業の土台そのものです。
攻撃する側から見れば、十分に価値のある標的です。実際、身代金を要求する攻撃の多くは、規模の大小を問わず、業務が止まって困る会社であれば誰でも標的になります。

そのうえで、もう一つの事情があります。

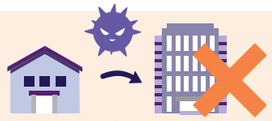
取引先とのつながりです。長い取引で得た信用があるからこそ、自社から送られたメールは開かれ、自社からの接続は許可されます。この信用そのものが、攻撃する側にとっては利用価値を持ってしまいます。攻撃する側の行動を順に追うと、次のようになります。

1 本命の標的として、規模の大きなA社を選ぶ。

2
A社は専門部署を置いて対策を固めているため、正面からは攻めない。

3
A社と取引のある会社を調べる。会社案内や導入事例、取引先一覧が手がかりになる。

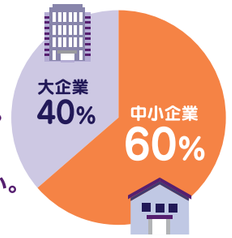
4
その中から、外部との接続に古い機器を使っているなど、突破しやすい経路を持つ会社を選ぶ。

5 
業務上のつながりを伝ってA社へ入る。あるいは、その会社を止めることでA社の生産を止める。

この進み方は「島渡り」と呼ばれます。守りの固い本丸を避け、手前の足場から順に渡っていく攻め方です。

事実として、被害の中心は中小企業に移っています。

警察庁が2026年3月に公表した資料によれば、2025年に報告されたランサムウェア被害226件のうち、**およそ6割が中小企業でした**（出典③）。
前年の資料でも、中小企業の被害は前年比で37%増加し、同じ期間に大企業の被害は減少しています（出典④）。
この差は、対策の意識の差ではありません。
大企業は専任の担当者と予算を確保できる一方、中小企業では総務や経理の担当者が他の業務と兼任しているのが実情です。人手と予算の構造的な違いが、そのまま被害件数の差に表れています。
したがって「うちは小さいから狙われない」という見方は、数字の上では成り立ちません。
守るべきものがあり、かつ対策に人手を割きにくい。この2つが重なっているのが、多くの中小企業の現在地です。



4. どのような手口で入ってくるのか

手口1 取引先・委託先から入ってくる。

取引先や委託先、子会社のネットワークに侵入し、業務上の接続をたどって本命へ進みます。入口として最も多いのは、社外から社内へつなぐための通信機器です。
警察庁の同じ資料では、**侵入経路の6割以上がこの種の機器でした**（出典③）。
何年も設定を見直していない機器が、そのまま入口になっています。

手口2 使っているソフトの提供元から入ってくる。

ソフトを開発している会社に侵入し、出荷前の製品や更新プログラムに不正なプログラムを混ぜ込む手口です。利用する側は「いつもの更新」として自らインストールしてしまいます。メーカーの正規の電子署名が付いているため、ウイルス対策ソフトも異常とは判断しません。

手口3 保守業者やクラウド事業者から入ってくる。

保守業者やクラウドサービスの提供元は、多数の顧客システムに入れる管理権限を持っています。ここが破られると、その管理の仕組みを使って、契約している全社へ一斉に被害が配られます。利用する側から見れば、信頼している業者の正常な通信にしか見えません。

3つに共通しているのは、入ってくる経路が「日常的に使っている正規のつながり」だという点です。だからこそ、その場で見破ることは容易ではありません。

5. 実際に、何が起きたのか

事例1 部品メーカー1社が止まり、完成車メーカーの全工場が止まった（2022年）

大手自動車メーカーの一次部品メーカーが、ランサムウェアの被害を受けました。侵入の起点は、その会社の子会社が独自に導入していたリモート接続機器の脆弱性でした。子会社のネットワークから親会社へ侵入され、翌週、完成車メーカーの国内全14工場28ラインが停止しました（出典⑤）。
1台の機器の管理漏れが、国内最大級の生産ラインを止めた事例です。

事例2 物流が12日間止まり、小売店の棚から商品が消えた（2026年7月）

大手の冷凍食品・物流会社がシステム障害により、冷蔵倉庫の入出庫と出荷業務を停止しました。復旧までおよそ12日間。
同社は業績への影響を、売上高で約50億円、営業利益で約8億円と公表しています（出典⑥）。
影響は取引先の外食チェーンや小売店にも及び、店頭の品切れという形で消費者にまで届きました。

事例3 ファイル受け渡しソフトの欠陥から、約9,600万人分が漏れた（2023年）

企業間で大きなファイルをやり取りするためのソフトに欠陥が見つかり、世界で2,773組織、のべ約9,579万人分の個人情報が盗まれました（出典⑦）。
自社が直接攻撃を受けていなくても、委託先がこのソフトを使っていれば、自社が預けた情報が流出します。

Column 国も、この問題に手を打ち始めています。

経済産業省は2026年3月27日、企業のセキュリティ対策の状況を共通の基準で評価し、見えるようにする制度の構築方針を公表しました（出典⑧）。
取引先ごとに異なるチェックシートへ回答する負担を減らすことも目的の一つです。対策の状況を説明できることの重みは、これから確実に増していきます。

最後に、整理します。

❶つながりは、どの業種にもある モノ、データ、サービス。自社は必ず、どこかの連鎖の一部です。

❷リスクは2種類ある 取引先が止まって自社も止まる。自社が破られて取引先へ広がる。

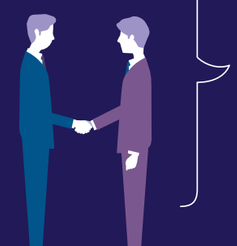
❸被害の中心は中小企業に移っている 守るべきものがあり、そのうえでつながりも狙われています。

出典

① 中小企業庁「2025年版 中小企業白書・小規模企業白書の概要」（2025年）
② 情報処理推進機構「2024年度 中小企業における情報セキュリティ対策の実態調査」（2025年2月公表）
③ 警察庁「令和7年におけるサイバー空間をめぐる脅威の情勢等について」（2026年3月公表）
④ 警察庁「令和6年におけるサイバー空間をめぐる脅威の情勢等について」（2025年3月公表）
⑤ 当該部品メーカー「システム停止事案調査報告書（第1報）」（2022年3月）および完成車メーカー公表資料（2022年2月）
⑥ 当該企業公表資料・決算説明会資料（2026年7月）⑦ Emsisoft 集計（2024年6月時点）
⑧ 経済産業省「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」（2026年3月27日公表）

次回予告

Vol.40（2026年9月度）「サプライチェーンリスクに、何から手をつけるか（仮）」

つながりの書き出し方から、契約と連絡ルートの整え方、止まったときの備えまで。今号で見たリスクに対して、実際に何をすればよいのかを扱う予定です。※内容は予告なく変更する場合があります。

ぜひ、ご相談ください！
御社のAI×DX伴走パートナーであり続けます。