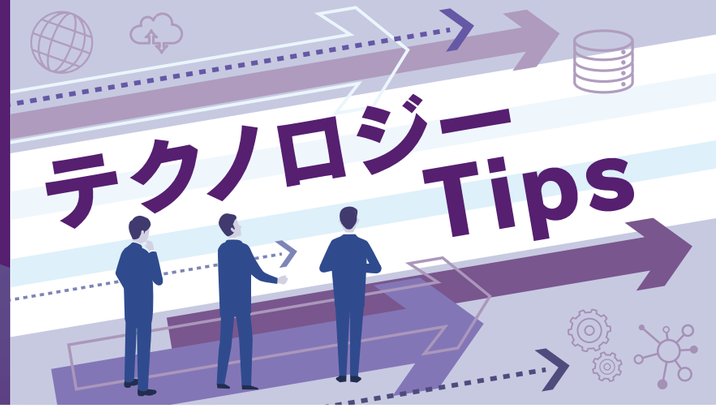
今こそ知りたい Tech Tips!

会社にあるパソコン、スマートフォン、複合機、そしてネットワークにつながっているルーター。
今、全部で何台あって、それぞれ誰が管理しているのか、すぐに答えられるでしょうか。

狙われるのは、いちばん大切な1台ではありません。誰も管理していない1台です。

今侵入者が入ってくるのは、メールの添付ファイルからではありません。社内に置かれた機器を侵入経路として狙います。まず、「どんな機器が何台あるのか？を数えてみましょう。」



1. 会社にある機器を、全部言えますか

事務所を見回してください。パソコン、社用のスマートフォン、複合機、電話機、ラックの中のルーターや無線LANの親機。倉庫には、使わなくなったパソコンがあるかもしれません。これらが全部で何台あるのか、一覧を持っている会社は多くありません。

とくに、次の4つが見えなくなります。

社員が自分で用意した機器

私物のスマートフォンで会社のメールを見る、自宅のパソコンで資料を作る。

担当者や部署が個別に買った機器・ソフト

必要に迫って買ったもので、全体の一覧には載っていない。

使われないまま残っている機器

入れ替えたあとの古いパソコン、契約だけ続いているソフト。

持ち主がいなくなった端末

退職や異動で、誰のものか分からなくなったもの。

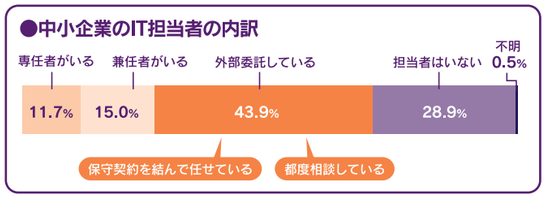
会社が把握していない機器やソフトを、一般にシャドーITと呼びます。誰かが悪意で隠しているわけではありません。仕事に必要だったものが、把握する仕組みのないまま増えた結果です。

【用語】シャドーIT　会社が把握・管理していないIT機器、ソフト、サービスを指す言い方です。法律や公的な基準で定められた言葉ではなく、業界で使われている呼び方です。

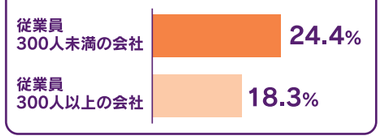
2. なぜ、把握できなくなるのか

担当者の意識の問題ではありません。
機器を見る人手が足りていない、という構造の問題です。
中小企業のIT担当者の状況は、右記のとおりです(※1)。
4社に1社以上が、社内に見る人を置いていません。
回答した会社の7割近くは、従業員20人以下です。
いちばん多い「外部委託している」の43.9%には、保守契約を結んで任せている場合と、機器を納入した会社にその都度相談している場合が、どちらも含まれます。調査では区別されていません。
前者であれば、どこまで見てもらえるかが契約書に書かれています。
後者の場合、自社に何が何台あるのかを一覧で持っている人は、社内にも社外にもいないことがあります。ルールも、これからの段階です。
情報セキュリティ対策をルール化している会社は39.2%にとどまります(※2)。
ルールがなければ、買うときの申請も、使わなくなったときの届け出も発生しません。
一覧ができないのは当然です。私物の機器についても数字があります。私用の電話番号の携帯電話を業務で使っている人は、従業員300人未満の会社で24.4%、300人以上の会社で18.3%でした(※3)。
規模の小さい会社のほうが、6.1ポイント高くなっています。

●中小企業のIT担当者の内訳



●私用携帯を業務で使用している人の割合



大きな会社との差は、意識の差ではありません。見る人がいるか、決めごとがあるかという、人手と予算の構造の差です。呼びかけでは変わりません。仕組みとして一覧を作ることが先になります。

3. 管理されていない機器が、そのまま入口になる

なぜ数える必要があるのか。攻撃者が入ってくる場所が、そこだからです。

警察庁が公表した資料より(※4)

被害組織へのアンケート結果では、侵入経路はVPN機器が約5割を占めています。さらに、インターネットに露出した箇所から攻撃者が遠隔操作でネットワーク内部に侵入する手口が多くを占め、標的型攻撃メール等の添付ファイルによる感染は少なくなっているとされています。

侵入経路

標的型攻撃メール等の添付ファイルによる感染は少なくなっている

インターネットに露出した箇所から攻撃者が遠隔操作でネットワーク内部に侵入する

攻撃者は、次の順に入ってきます。

探す
インターネット全体を機械的に調べ、社外からログインできる機器を探す（狙い撃ちではありません）

入る
更新されていない不具合を突くか、他所から漏れたIDとパスワードで入る

正規の利用者として入る
正しくログインした利用者として入るため、ウイルス対策ソフトは反応しない

【用語】ランサムウェア／VPN機器

ランサムウェアは、ファイルを勝手に暗号化して読めなくし、元に戻すことと引き換えに金銭を要求する攻撃です。VPN機器は、社外から社内のネットワークにつなぐための機器です。24時間電源が入ったまま、外部からの通信を受け付けています。

機器が狙われる理由は、4つあります。

- 常に電源が入っていて、外部とつながっている
- 画面がないため、更新のお知らせが誰の目にも触れない
- 設置した担当者が退職していると、更新できる人がいない
- 一覧にない機器は、更新が必要なことにさえ気づけない

メーカーが対策を公表しても、自社にその機器があると分かっていなければ、対応できません。数える作業は、守りの前提です。

4. 何を書き出すか

白紙から表を作る必要はありません。IPA（独立行政法人 情報処理推進機構）が、記入用のExcelを無料で公開しています。「中小企業の情報セキュリティ対策ガイドライン 第4.0版」の付録6「資産管理台帳サンプル」です（※5）。

書き出す対象ごとに、3つのシートがあります。

ハードウェア台帳
パソコン、複合機、スマートフォンなど

ソフトウェア台帳
会計ソフト、ウイルス対策ソフトなど

ネットワーク機器台帳
ルーター、無線LANの親機、VPN機器など

それぞれの記入欄は、下の表のとおりです。
被害の入口になりやすいのは、3つ目のネットワーク機器です。時間が取れない場合は、ネットワーク機器台帳から埋めてください。欄の数は多く見えますが、最初から全部を埋める必要はありません。
まずは「名称」「設置場所」「管理者名」の3つで構いません。
何が、どこにあって、誰が見ているのか。これが分かるだけで、状態は変わります。

資産管理台帳の記入欄

それぞれのシートに、次の項目を記入します。

時間がなければ、ネットワーク機器台帳から

ハードウェア台帳	ソフトウェア台帳	ネットワーク機器台帳
名　称／	名　称／	ネットワーク名／
製造元／	種　別／	所在地／
型　番／	製造元／	IPアドレス／
管理番号／	O　S／	ネットワークの利用目的／
管理部署／	インストール先／	名　称／
管理者名／	登録者名／	種　別／
保守事業者名／	ライセンス数／	製造元／
（保守事業者）担当者名／	管理部署／	製造モデル／
購入日／	管理者名／	O　S／
	保守事業者名／	設置場所／
	（保守事業者）担当者名／	管理部署／
	購入日／	管理者名／
		保守事業者名／
		（保守事業者）担当者名／
		契約情報／
		購入日／

まずは「名称」「設置場所」「管理者名」の3つから始めましょう。

5. 手順は3つです

手順1　集める
- 現物を見て回る（事務所、倉庫、ラックの中、社員の手元）
- リース契約書、保守契約書、購入時の伝票を確認する
- 両者を突き合わせる

契約書にあるのに現物がない機器、現物はあるのに契約書がない機器が出てきます。
そこが、把握できていない部分です。社員が自分で用意した機器は、「叱らないので教えてください」と先に伝えてください。責める形で聞くと、正確な申告が集まりません。
会社の端末が足りていない事情があるなら、そこから改善する話になります。

手順2　管理者と連絡先を決める
- 社内の管理部署　●社内の管理者名
- 保守をお願いしている会社名
- その担当者名
- その相手に見てもらう範囲（契約書に書かれていない場合は、ここで決めます）

IPAは、クラウドサービスについても「管理担当者を決める」「利用者の範囲を決め、どのような権限を与えるか適切に管理する」ことを求めています（※6）。
社内の機器でも、考え方は同じです。
この欄が埋まっていれば、機器が止まったとき、更新のお知らせが届いたときに、すぐ連絡できます。

手順3　使っていないものを片付ける
- 倉庫の古いパソコン
- 契約だけ残っているソフト
- 貸したまま返っていない端末

一覧ができると、使われていない機器がはっきりします。
倉庫の古いパソコン、契約だけ残っているソフト、貸したまま返っていない端末。
これらを、止める・処分する・返してもらう、のいずれかに割り振ります。

なお、IPAの台帳には、情報の重要度を「機密性」「完全性」「可用性」の3つの観点から3段階で評価する欄もあります。余力があれば、そこまで進めてください。

6. 人が入れ替わるときに、何を回収するか

IPAのガイドラインは、次のように書いています（※5）。

> 役職員の退職や派遣社員等の契約満了後における情報の不正利用を防ぐために、退職／任期満了時に情報や機器・ID・鍵等を回収し、加えて復元できない方法によりデータを消去して、チェックリストや証跡で実行状況を可視化しましょう。

やることは、3段階です。

回収する
情報、機器、ID、鍵の4つ

消去する
復元できない方法で

記録する
チェックリストと証跡で

機器とIDは、忘れられがちです。返却されたパソコンが初期化されないまま棚に置かれていたり、退職者のアカウントがそのまま生きていたりします。異動のときも同じです。ガイドラインには「従業員の異動や退職時には速やかに設定を変更（削除）する」とあります（※5）。部署が変われば、見てよい情報の範囲も変わるためです。

Column　取り組みを外に示す方法があります

IPAの「SECURITY ACTION」は、情報セキュリティ対策に取り組むことを会社が自ら宣言する制度です。

一つ星は
「情報セキュリティ6か条」への取り組みを宣言するもので、対策を始める前でも申し込めます。

二つ星は「5分でできる！情報セキュリティ自社診断」で現状を確認し、基本方針を定めて外部に公開する形です。

この宣言は、各種の補助金の申請要件にも採用されています。（※7）

※台帳の作成そのものは宣言の要件ではありませんが、二つ星の自社診断を進める過程で必要になります。

最後に、整理します。

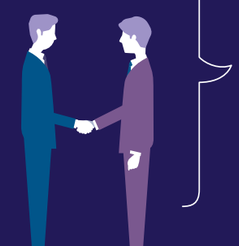
① 数える
事務所、倉庫、社員の手元まで見て回り、何が何台あるかを一覧にします。入口になりやすいネットワーク機器から始めてください。

② 決める
一行ごとに、社内の管理者と、保守をお願いしている会社の連絡先を書きます。

③ 手放す
使っていない機器と、持ち主がいなくなった端末を、止める・処分する・返してもらうのいずれかに片付けます。

次回予告

Vol.41（2026年10月度）「見えにくいのは、社外にあるサービスです（仮）」
今回は、社内にある機器とソフトを数えました。次回は、社外にあるクラウドサービスを取り上げます。誰が契約したのか分からないもの、使っていないのに料金を払い続けているもの、そして会社の許可なく使われている生成AIまで。社内の機器より、はるかに見えにくい対象です。
※内容は予告なく変更する場合があります。

出典
※1 東京商工会議所 中小企業のデジタルシフト・DX推進委員会「中小企業のデジタルシフト・DX実態調査」（2025年1月）。情報システム担当者の設置状況の設問は有効回答1,002社。
※2 独立行政法人情報処理推進機構（IPA）「2024年度 中小企業における情報セキュリティ対策に関する実態調査」（2025年5月）。有効回答4,191社。
※3 MMD研究所「2026年4月 法人向け携帯電話の利用実態調査」（2026年5月）。有効回答15,000人。
※4 警察庁「令和8年上半期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9月）。
※5 IPA「中小企業の情報セキュリティ対策ガイドライン 第4.0版」（2026年3月）および付録6「資産管理台帳サンプル」。
※6 IPA「中小企業の情報セキュリティ対策ガイドライン 第4.0版」付録7「クラウドサービス安全利用の手引き」（2026年3月）。※7 IPA「SECURITY ACTION」制度。

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。