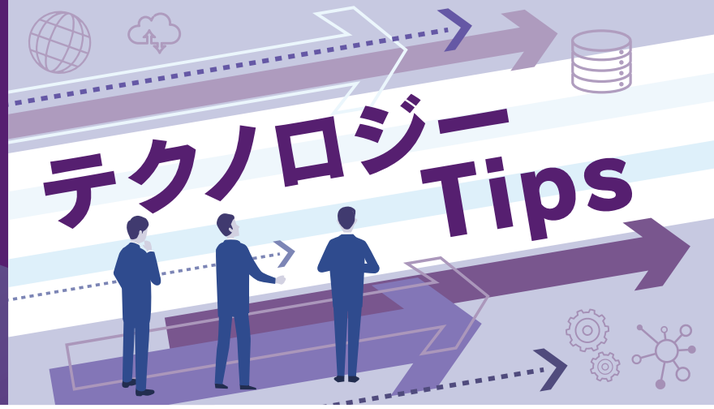
会計、勤怠、ファイルの共有、Web会議、そして生成AI。御社が会社の外で使っているサービスを、すべて書き出せるでしょうか。

会社の大切な情報は、いま社外のサービスの中にあります。そのIDを、誰が管理しているでしょうか。



社外のサービスは、IDとパスワードさえあれば、どこからでもログインできます。
会社が把握していないアカウントは、パスワードの変更も、利用の停止もできません。



今こそ知りたい Tech Tips!



冒頭の断り

今回は、いつもより強い言葉でお伝えします。国内で不正アクセスによる情報漏えいの公表が相次ぎ、IPA（独立行政法人 情報処理推進機構）が経営者に至急の点検を求めているためです。本号は、IPAの資料に沿ってご案内します。

【おさらい】社内の機器の守り方

- **数える**：何が何台あるかを一覧にする
- **決める**：1台ごとに、管理者と保守会社の連絡先を書く
- **手放す**：使っていない機器を片付ける

今回は、同じことを社外のサービスで行います。

1. 会社の情報は、社外のサービスの中にあります

会計、給与計算、勤怠管理、顧客管理、メール、ファイルの共有。多くの業務が、インターネット上のサービス（クラウドサービス）で行われています。
従業者100～299人の企業の79.9%が、クラウドサービスを使っています（※1）。社外のサービスは、目に見えません。

次の3つが、把握できなくなりがちです

- 誰が契約したか分からないサービス



- 使っていないのに、料金を払い続けているサービス

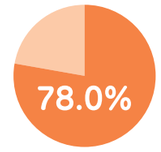


- 辞めた人、異動した人のアカウント



SaaS（インターネット経由で使うソフト）を導入している企業に勤める1,021人のうち**78.0%が使われていないアカウントが自社に「ある」と答えています**（※2）。
※従業者100人以上の企業が対象の調査





2. IPAが10月9日、至急の点検を求めました

IPAは2026年10月9日、不正アクセスによる情報漏えいが相次いでいることを受けて、注意喚起を出しました（※3）。

攻撃の起点

「外部公開しているアプリケーションやサービスの侵害、アカウントの侵害が起点となっていることがうかがえます」



経営者への要請

対策の点検と見直しを「至急実施願います」



主な対象は大量の情報を持つ事業者ですが、外部サービスの点検は、会社の規模を問わず当てはまります。

IPAが求める、外部サービスの点検

① 使っている外部サービスを、すべて洗い出す



部署単位で使っているものも含めます。

② 利用の記録（ログ）を確かめる



ログインの失敗が急に増えていないか。ふだんと違う場所や時間からログインされていないか。

③ アカウントを確かめる



作った覚えのないアカウントはないか。削除したはずのアカウントが使える状態になっていないか。

④ 異常があれば、すぐにセキュリティ事故として扱う



専門の会社に調査を依頼します。

異常がなかった場合も、多要素認証などの強化、アカウントを渡す範囲の見直し、アカウントの棚卸しの見直しを求めています。

3. 社外のサービスは、IDとパスワードで入れてしまう

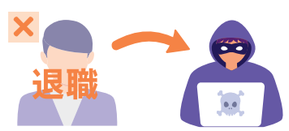
社外のサービスは、どこからでもログインできます。
正しいIDとパスワードがあれば、攻撃者も正規の利用者として入れます。
不正アクセスの被害を受けた企業の36.8%が、手口として「ID・パスワードをだまし取られた」を挙げています(※4)。

IPAの資料にある、入られる場面です。

- 他のサービスから流出したID・パスワードを使われる(※5)



- 辞めた人のアカウントを消しておらず、外から使われる(※6)



- 1つのアカウントを何人かで使っていて、誰が操作したのか分からない(※6)



- 共有や権限の設定ミスを突かれる(※5)



用語 多要素認証
パスワードに加えて、スマートフォンや指紋など別の手段を組み合わせてログインする方法です。パスワードが漏れても、それだけではログインできません。



4. IPAの手引きが求める、5つの管理

IPAの「中小企業のためのクラウドサービス安全利用の手引き」から、
使い始めてからの管理4つと、やめるときの1つです(※7)。

- ☑ **管理担当者を決める** No.7 設定や操作が分かる担当者を、社内に置きます。
- ☑ **利用者の範囲を決める** No.8 使う人と、与える権限を決めます。手引きの例は「販売管理のアカウントは社長と販売部門だけ。承認の権限は上司だけ」です。
- ☑ **利用者の認証を厳格に行う** No.9 IDとパスワードを共有しません。2段階認証などがあれば、必ず使います。
- ☑ **バックアップに責任を持つ** No.10 サービスが止まっても困らないよう、重要な情報を手元にも残します。
- ☑ **利用終了時のデータを確保する** No.13 解約するとき、全データを返してもらえるかを、契約の前に確認します。

パスワードは、IPAの基準が「英数字記号含めて10文字以上」です(※5)。
長いほど破られにくいため、16文字以上を目安にしてください。



5. 一覧を作り、点検する

IPAの規程のサンプルには、クラウドサービスを含む社外のシステムについて「一覧を作成し、適切に管理する」と書かれています(※7)。一覧に載せる内容は、次の4つです。

一覧に載せる内容(付録5)	ソフトウェア台帳(付録6)で書く欄
基本情報	No.／名称／種別／購入日(『資産状態』は列を足す)
利用・管理者情報	管理部署／管理者名／登録者名
保守契約情報	保守事業者名／(保守事業者) 担当者名(『契約期間』『契約番号』『連絡先』は列を足す)
ライセンス情報	ライセンス数／購入日

※OS、インストール先の欄は、クラウドサービスでは空欄で構いません。

使う道具も、IPAが無料で公開しています(※7)。

記入する台帳
付録6「資産管理台帳(サンプル)」のExcelにある「ソフトウェア台帳」。足りない欄(契約期間、契約番号など)は、列を足してください



1つずつの点検
付録7の「クラウドサービス安全利用チェックシート」(15問)



手順は3つです。

手順1 契約を拾い出す
経費精算、カードの明細、請求書から拾います。
- 各部署に聞きます。責める形で聞くと、正確に集まりません
- 無料で使っているものも書きます。会社の情報が入っているためです

手順2 アカウントを点検する
管理画面でアカウントの一覧を出し、社員名簿と1行ずつ突き合わせます。次のアカウントが見つかったら、その場で対応してください。

辞めた人のアカウント	すぐに止めます。データが必要な場合は、引き継ぐ人に移してから削除します
異動した人のアカウント	前の部署で使っていた権限を外します。IPAも「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」としています(※5)
何人かで使っている共用のアカウント	「info」「sales」などで始まるものです。誰が使っているかを書き出し、パスワードを変えて、使う人だけに伝えます。できれば1人1つのアカウントに分けます
管理者の権限を持つアカウント	何人いるかを数え、必要な人だけに絞ります。管理者のアカウントには、必ず多要素認証を設定します
長い間ログインしていないアカウント	管理画面で、最後にログインした日を確かめます。一定期間使われていないものは、持ち主に確認して止めます
作った覚えのないアカウント	IPAの点検項目にあるとおり、セキュリティ事故として扱い、専門の会社に相談します(※3)

最後に、多要素認証が全員分設定されているかを確かめます。設定していない人には、期限を決めて設定してもらいます。
点検した日と、止めたアカウントは、台帳に記録しておきます。

手順3 使っていない契約を止める
- データを移してから解約します
- IPAは「不要な情報は持たない」ことを基本原則としています(※3)

最初から全部を埋める必要はありません。まずは「名称」「責任者名」「契約期間」の3つで構いません。人が辞めたとき、新しく契約したときに更新してください。

最初から全部を埋める必要はありません。まずは「名称」「責任者名」「契約期間」の3つで構いません。人が辞めたとき、新しく契約したときに更新してください。

Column IPAが解説資料を公開しました

IPAは9月30日、「情報セキュリティ6か条」と「5分でできる!情報セキュリティ自社診断」の解説編を公開しました(※5)。
6か条の第4条「共有設定を見直そう!」には、クラウドサービスの設定ミスの解説があります。
自社診断のNo.23は、外部サービスを安全・信頼性を把握して選んでいるかを問う設問です。
自社の状態を確かめるときに、お使いください。



出典
※本誌の内容は、2026年10月15日時点でIPA等が公表している情報にもとづきます。※1 総務省「令和7年通信利用動向調査」(2026年5月)。常用雇用者規模100人以上の企業が対象。※2 マネーフォワードi「SaaS管理に関するアンケート調査」(2023年6月)。SaaSを利用する企業に所属する経営者・役員・会社員1,021名。
※3 IPA「不正アクセスによる漏えい等の事案を踏まえ、速やかに実施すべき対策等について」(2026年10月9日)。※4 IPA「2024年度中小企業等実態調査結果」速報版(2025年2月)。2023年度に不正アクセスの被害を受けた企業419社の回答(複数回答)。※5 IPA「情報セキュリティ6か条(解説編)」「5分でできる!情報セキュリティ自社診断(解説編)」(2026年9月)。
※6 IPA「情報セキュリティ10大脅威 2026」組織編 解説書(2026年3月)。※7 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5「情報セキュリティ関連規程(サンプル)」、付録6「資産管理台帳(サンプル)」、付録7「中小企業のためのクラウドサービス安全利用の手引き」(2026年3月)。



まとめ ー3本の柱ー

① 書き出す
社外のサービスを、部署単位のものまで一覧にします。

② ログインを固める
管理者を決め、多要素認証を設定し、辞めた人のアカウントを止めます。

③ 定期的に点検する
覚えのないアカウントや、ふだんと違うログインがないかを確かめます。使っていない契約は、データを移してから解約します

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。

