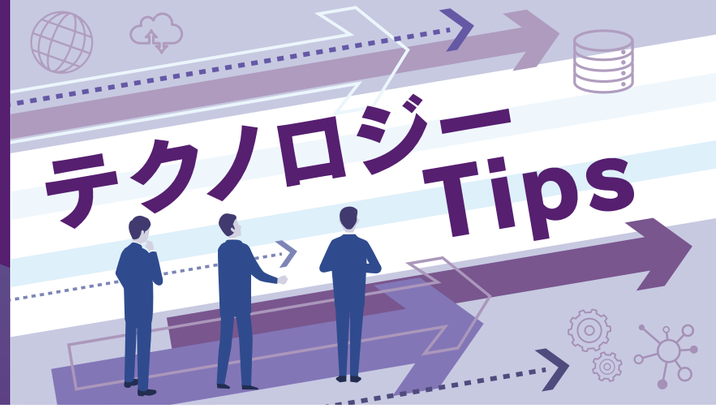
今こそ知りたい
Tech Tips!

ログインのたびに、違うID・パスワード。覚えきれず「使い回し」や「付箋メモ」になっていませんか？
―― それ、会社のセキュリティの“弱点”かもしれません。

# 今さら聞けない「IDaaS（アイダース）」！

## 増えすぎたID・パスワードを、ひとつにまとめる。

日々のセキュリティ対策の、その“次の一歩”。クラウドと生成AIの時代に
欠かせない認証の土台「IDaaS」を、基本からやさしく解説します。




### 1. そもそも「ID」とは？ なぜそれほど大切なのか

「ID」とは、デジタルの世界での“名札”であり“身分証”です。
会社に入るときの社員証をイメージしてください。システムはこの名札で「あなたが誰か」を判断し、入ってよい場所・触ってよい情報を決めています。ここで大事なのが、IDとパスワードの関係です。
IDが「あなたが誰か（名札）」を表すのに対し、パスワードは「本当に本人だ」と証明する“鍵”の役割を持ちます。名前を名乗り（ID）、本人確認の鍵を見せる（パスワード）。
この2つがそろって、はじめてログインが許されます。
問題は、鍵が「パスワード1つだけ」だと、盗まれたり、推測されたり、使い回したりした瞬間に、誰でも“あなたのふり”ができてしまうこと。だからこそ「誰が、どの入口の鍵を持っているか」を管理することが、セキュリティの出発点になります。


### 2. なぜ今、「ID管理」が経営課題になったのか

ひと昔前は、会社のパソコン1台にログインすれば、ほとんどの仕事ができました。鍵は実質1つで足りた時代です。ところが今は、会計ソフト、グループウェア、チャット、クラウドストレージ、各種クラウド、そして生成AIツールまで、使うサービスは10も20も当たり前。そのすべてに別々のID・パスワードが要ります。結果、覚えきれず使い回す、簡単な文字列にする、付箋に貼る…。どれか1つ漏れれば、芋づる式に突破されます。

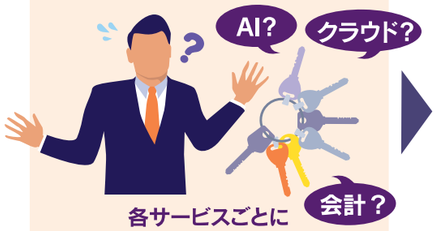

**！** さらに、生成AIに社内データを扱わせる場面が増えました。「誰が、どのIDでAIにアクセスし、何を入力したか」を管理できなければ、それ自体が漏えいの温床になりかねません。

ID管理は「便利のため」だけでなく、「会社を守るため」の経営テーマへと変わったのです。

### 3. IDaaS（アイダース）とは？

IDaaS（Identity as a Service）とは、クラウド上で社内のID・認証をまとめて管理する仕組みです。
あちこちに散らばった“鍵束”を、1つの信頼できる「受付」に集約するイメージです。主な働きは次の通りです。

**散らばった“鍵束”**




各サービスごとにID・パスワードがバラバラ。管理も大変で、リスクも高い状態。

**IDaaSという「受付」に集約**


IDaaSが、すべてのID認証をまとめて管理。安全に、シンプルに。

**マスターキー1本でOK!**

一度の認証で、必要なサービスへ安全・快適にアクセスできる。

#### SSO（シングルサインオン）

一度の認証で、つながった複数サービスへ自動ログイン。何本もの鍵を“マスターキー1本”にまとめる感覚です。


#### MFA（多要素認証）

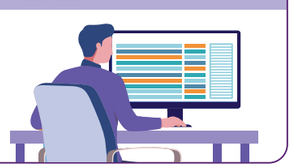
パスワードに加え、スマホ承認や生体認証など「もう1つの要素」で確認。万一パスワードが盗まれても、それだけでは入れません。

#### ID一元管理・自動連携

入社時に必要なIDを一括発行し、退職時には一括停止。「止め忘れ」を防げます。


#### ログ管理

誰が・いつ・どこにアクセスしたかを記録し、後から点検できます。



基本的なセキュリティ対策を一通り終えた会社にとって、IDaaSはまさに「次の一歩」と言える存在です。

## 4.「社内は安全」はもう古い —— ゼロトラストという新常識

これまでのセキュリティは「境界型防御」が主流でした。社内は安全、社外は危険。その境目に“壁”を築いて守る考え方です。
しかしテレワークやクラウドの普及で、「社内」と「社外」の境界そのものが薄れました。そこで広まっているのがゼロトラストです。
ゼロトラストは「何も信頼しない」を原則とし、社内からのアクセスでも、誰が・どの端末で・何にアクセスしようとしているかを毎回検証するモデルです。ポイントは、守る対象が「ネットワークの境界」から「ID」へ移ったこと。
誰であるかを確かめる仕組み＝IDaaSが、その中核を担います。
この考え方は2010年に提唱され、米国のNIST（SP 800-207）が体系化したもので、日本でもデジタル庁が適用方針を示すなど、一時の流行りではなく公的にも“標準的な設計思想”です。なお、ゼロトラストは「壁（ファイアウォール）を取り払うこと」ではなく、あくまで“考え方の転換”です。


## 5. なぜ、ID管理に今こそ取り組むべきか

IDをきちんと管理することには、現実的で切実な理由があります。

### 退職者アカウントの放置

辞めた人のIDが生きたままだと、不正アクセスの入口に。
一元管理していれば、退職と同時に確実に止められます。

### “見えない”ツールの利用（シャドーIT）

社員が無料サービスを勝手に使うと、会社は把握も統制もできません。
IDの基盤を整えることが第一歩です。

### 取引先からの要求

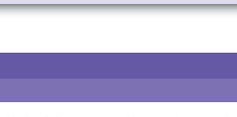
IPA「情報セキュリティ10大脅威 2026」では、取引先を踏み台にする“サプライチェーン攻撃”が2位に挙げられ、対策の有無が取引継続の条件になりつつあります。

### サイバー保険の条件化

近年は加入条件にSSO・MFAの導入が含まれるケースも増えています。

これらは「脅し」ではなく、「だからこそ、IDの守りが当たり前の前提になりつつある」という事実としてお伝えしたい点です。

### Column 生成AIを使うなら、まず「ID」を固めるべき理由



生成AIは、社内の文書やデータを読み込ませて使う時代。ここで見落とされがちなのが、「AIは“その人のID（権限）”で動く」という事実です。あるIDで見られる情報は、そのIDで使うAIにも見えてしまう。
逆に言えば、ID管理がゆるい会社では、AIが“見えてはいけない情報”まで扱えてしまうのです。

- ! 退職者のIDが生きていれば、その人のAI経由で社内情報に触れられる
- ! IDを共有・使い回していれば、「誰がAIに何を入力したか」を追えない
- ! 権限が未整理なら、AIの便利さがそのまま“漏えいの近道”になる

高度なAIセキュリティ製品を入れる前に、まず「誰が・どのIDで・何にアクセスできるか」を正すこと。それが、生成AIを安全に活かすうえで最も効果が大きく、基本となる対策です。AI活用の安全性は、ID管理から始まる—そう言っても過言ではありません。

## 6. 小さく始める、IDの守り方

いきなり大がかりな仕組みは要りません。順番はシンプルです。

### ❶ 棚卸しする

どんなサービスを、誰が、どのIDで使っているかを書き出す。
まずは現状把握から。

### ❷ 重要なものから守る

全部を一度にやらず、メールやグループウェアなど“中核の1～2サービス”からSSOとMFAを有効に。

### ❸ ルールにする

退職時のID停止手順、推測されにくいパスワード、MFA必須などを小さなルールとして定める。


見落とされがちなのが、「実は、今お使いのツールにIDaaSの機能が備わっている」ケースが多いこと。たとえばMicrosoft 365なら、上位プラン（Business Premiumなど）にSSO・多要素認証・アクセス管理が標準で含まれます。Google Workspaceでも、Googleの認証基盤（Cloud Identity）でSSOや多要素認証を一元管理できます。多くの会社にとって最初の一歩は「新しい製品を買うこと」ではなく、「すでに払っているプランの“眠っている機能”を有効にすること」なのです。

**お使いのMicrosoft 365 / Google Workspaceに、実は入っています。**

最後にひとつ

セキュリティは“コストを削るところ”ではなく、会社を守るための投資です。無料・無防備のまま放置せず、必要なところに正しく手当てしながら、小さく・着実に始めましょう。

## まとめ IDの管理は、難しい専門技術の話ではありません。

**要は「会社の“入口”を、誰が通れるのかをきちんと管理すること」です。**
それは守りの土台であると同時に、クラウドや生成AIを安心して使うための前提でもあります。
鍵を一本化し、現場の負担を減らしながら安全性を高める——その現実的な“次の一歩”が、IDaaSです。

IDaaSがもたらす 3本の柱

- **守りの土台**：バラバラの“鍵”を一本化し、会社の入口をまとめて守る。
- **活用の前提**：クラウド・生成AIを、安心して使いこなすための足場になる。
- **小さく始められる**：中核サービス1つ＋MFAから、今日からでも踏み出せる。

参照 IPA「情報セキュリティ10大脅威 2026」／NIST SP 800-207「Zero Trust Architecture」／デジタル庁「ゼロトラストアーキテクチャ適用方針」／IPA「ゼロトラスト移行のすゝめ」

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。