社内勉強会　特集「正しく怖がろう」から

会社のメールを、乗っ取られない形にする



全員がその場で自分のスマホを設定し、
管理者がやることの段取りを決める

30〜45分　｜　話す人：社長か総務の担当者　｜　用意：自分のスマホ・ワークシート

今日のゴール

今日の終わりに、こうなっている

社員みんな（この場で、スマホで）

① 画面ロックを、顔か指と6桁以上に

② パスワードを、スマホに覚えさせる

③ 会社のアカウントに、
パスキーか認証アプリ

④ 済ませた印を、ワークシートに

社長・担当者（管理者として、一人で）

① 全員の2段階認証を必須にする日

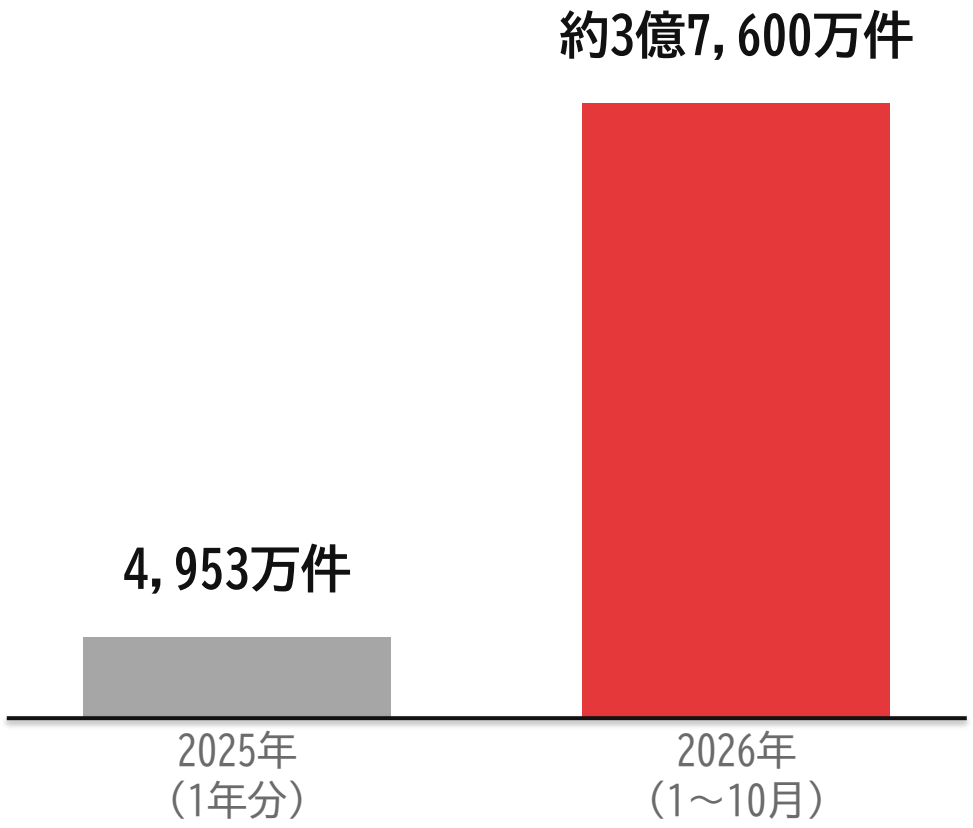
② 管理者を2人にする

③ 外への自動転送を止める

④ 会社ならではの穴5つの担当と日付

なぜ今、会社でやるのか①

漏えいは、この夏から桁が変わった。
2026年は10月末までに、去年1年分の約7.6倍



約94%
今年の件数のうち、7月以降に公表された分

約31倍
漏れたパスワード・ログインID
延べ約1億6,100万件。2025年比

8〜9割
攻撃の仕事を、AI が自分で進めた例（2025年11月）

会社のアドレスや、どこかで使ったパスワードも、もう漏れていると思って動く

出典：MM総研（2026-11-04）、ANN（2026-11-09）、Anthropic（2025-11-13）。特集「正しく怖がろう」トップ

なぜ今、会社でやるのか②

狙われるのは、大きな会社だけではない。
ニセ社長詐欺は、半年で127件

127件

ニセ社長詐欺
（2026年1～6月）

**約38億
8,000万円**

その被害額

約3,100万円

1件あたり

約6割

ランサムウェアの
被害企業のうち、
中小企業

社長になりすました
メールが届く

→

LINE などの
グループを作らせる

→

口座の残高を
聞く

→

「事業資金が至急
必要」と送金させる

手口（警察庁のコラムから）

出典：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）。特集5

なぜ今、会社でやるのか③

一人のメールが乗っ取られると、本物の会社のアドレスから偽の請求書が届く



1 社員一人のメールが、漏れたパスワードで乗っ取られる

2 外への自動転送を仕掛け、取引先とのやりとりを読み続ける

3 請求の時期に、本物のアドレスから「振込先が変わりました」

4 取引先が、偽の口座に振り込む

ふせぐ：① 全員の2段階認証（管理者がかける）　② 外への自動転送を止める
③ 振込先の変更は、メールの外で確かめる（全員の決まり）

見破れない

偽物は、もう見分けられない。
だから、見分けなくても守れる形に替える

URL を見る	鍵マーク	変な日本語	送り主の名前	電話の声
✕	✕	✕	✕	✕
似た文字・本物を中継する偽サイト	偽のサイトにも付いている	AI が書くので、もう不自然でない	偽れる。本物のアドレスからも来る	AI が流暢に話し、声もまねる

見落とすのは、注意が足りないからではない。見分けなくても守れる方法に替える

いちばん大事な仕組み

パスワードは合言葉を渡す。パスキーは渡さない

顔や指でスマホを開けるところまでは、同じ。違うのは、そのあとスマホが渡すもの

パスワード
＝合言葉を渡す

スマホが合言葉を
画面に入れる

→ 偽の画面なら、
合言葉が犯人の手に

→ 犯人は同じ合言葉で
本物の扉を開ける

パスキー
＝合言葉を
渡さない

本物のサイトが、
毎回ちがう問題を出す

→ 

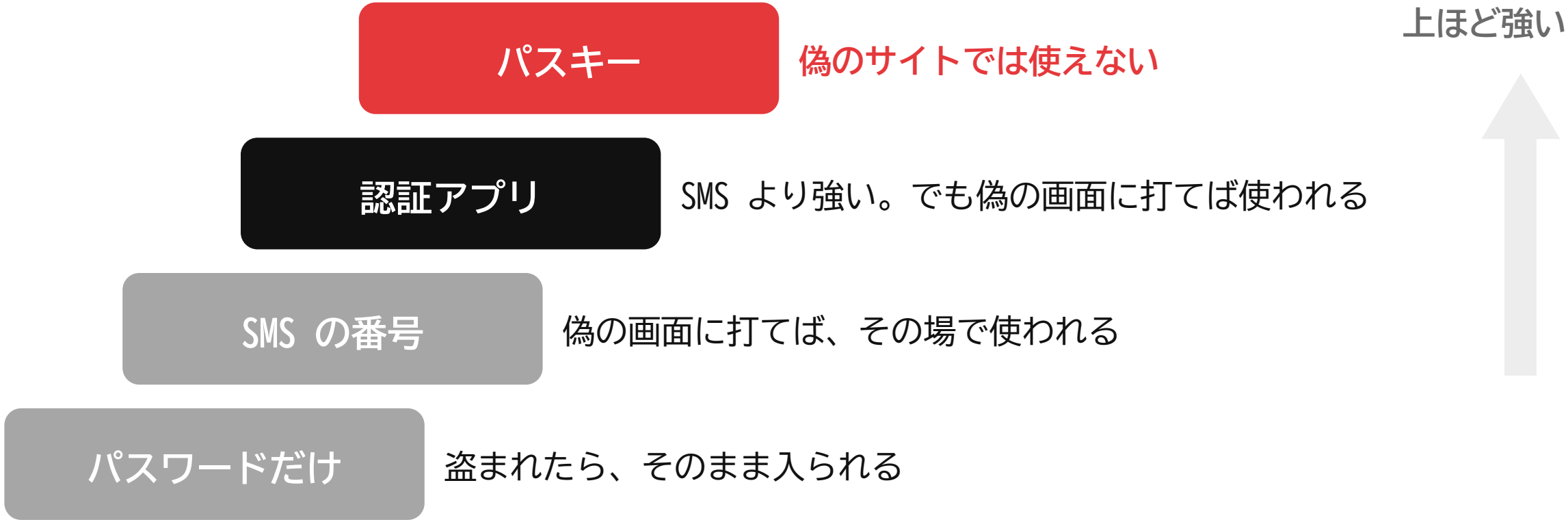
スマホの中の鍵が、
その回だけの答えを返す

→ ✕
偽の画面には、
スマホが答えない

見分け方：パスワードの欄に●●●が入る＝パスワード。「パスキーでサインイン」と出て、欄に何も入らない＝パスキー

守りの強さの順

会社のアカウントは、パスキー。
できなければ、認証アプリ



自分でログインしていないのに「承認しますか？」の通知が来たら、押さない。管理者に知らせる

今日やること

社員みんながその場でやることと、管理者が一人でやることを分ける

社員みんな（今日、この場で）

① 画面ロックを、顔か指と6桁以上に

② パスワードを、スマホに覚えさせる

③ 会社のアカウントに、
パスキーか認証アプリ

④ 決まり：振込先の変更と急ぎの送金は、メールの外で確かめる

管理者（社長・担当者が一人で）

① 全員の2段階認証を、義務にする

② 管理者を2人にし、いちばん固くする

③ 外への自動転送を止める

④ 会社ならではの穴を5つふさぐ

まず確かめる

うちの会社のメールは、どれで動いているか

会社のメール	何で動いているか	設定②で見る
会社の名前のアドレス（@会社名.co.jp など）を、Gmail の画面で開いている	Google Workspace	スライド13
会社の名前のアドレスを、Outlook で開いている	Microsoft 365	スライド14
個人の Gmail・個人の LINE・プロバイダーやサーバー会社のメール	まとめて設定する画面は、ふつうない	自分の Google で スライド13 の②

管理者かどうかは、会社のアドレスで管理の画面（admin.google.com／admin.microsoft.com）に入れるかで分かる

書き出す（ワークシート 社員用①・3分）

仕事で使っているアカウントを、名前だけ書き出す

会社のメール	会計ソフト	ネットバンキング	会社の SNS
ネットショップの管理画面	通販・宅配の法人アカウント	チャット	仕事に使う LINE

それぞれに：いまの入り方（パスワードだけ／SMS／認証アプリ／パスキー）、ほかの人と共有か

書かない：パスワードそのもの、メールアドレス、バックアップコード。書くのは名前と印だけ

みんなで設定する①（5分）

画面ロックを確かめ、パスワードをスマホに覚えさせる

先に：画面ロックが「顔か指」と「6桁以上」になっているか確かめる

iPhone

「設定」→「一般」
→「自動入力とパスワード」
→「パスワードとパスキーを自動入力」をオン

Android

Chrome を開く →「設定」
→「自動入力とパスワード」
→「Google パスワード マネージャー」
→「設定」→「パスワードを保存できるようにする」をオン

いつもは自動で入るのに出てこない：自分で打たない。偽のサイトかもしれない

手順は各社の公式の説明（特集3、2026-11-16 に確認）。画面が違っていたら、公式の説明を正とする

会社のアカウントに、2段階認証を付け、パスキーを作る

① 2段階認証プロセスをオンにする

① myaccount.google.com を開く
② 右上の丸を押し、会社のアドレスを選ぶ（なければ、会社のアドレスでログインする）
③ 「セキュリティとログイン」→「Google にログインする方法」
④ 「2 段階認証プロセスを有効にする」
⑤ パスワードをもう一度聞かれたら、会社のアカウントのパスワードを入れる
⑥ 電話番号を聞かれたら、自分の携帯の番号を入れ、届いた番号を打つ

② パスキーを作る

① myaccount.google.com/signinoptions/passkeys を開く
② 「パスキーを作成する」
③ 「パスキーを作成」
④ スマホのロックを、顔か指で解く
→ 同じページに出れば完了

両方やる：パスキーを作っても、2段階認証は自動ではオンにならない。項目が出なければ、管理者に

手順は Google の公式の説明（特集3・5、2026-11-16〜17 に確認）。画面が違っていたら、公式の説明を正とする

会社のアカウントに、認証アプリを登録する。管理者が許可していれば、パスキーも

認証アプリを登録する

① スマホに「Microsoft Authenticator」を公式のストアから入れる

② mysignins.microsoft.com/security-info（「セキュリティ情報」）を開く

③ 「サインイン方法の追加」

④ Microsoft Authenticator を選び、画面の指示に従ってアプリとつなぐ

使えれば、パスキーも

① もう一度「サインイン方法の追加」

② 「パスキー」（スマホの Authenticator に入れるときは「Microsoft Authenticator の Passkey」）

③ 顔・指・PIN で保存する

④ 「セキュリティ情報」に並べば完了

「パスキー」が選べない：管理者がまだ有効にしていない。今日は認証アプリまででよい

手順は Microsoft の公式の説明（特集3・5、2026-11-16〜17 に確認）。画面が違っていたら、公式の説明を正とする

確かめる（ワークシート 社員用②）

今日は、設定の画面で確かめる。
ログインの画面は、次に入るときに見る

今日：設定の画面で

Google：signinoptions/passkeys の
ページに、作ったパスキーが出ている

Microsoft：「セキュリティ情報」に、
認証アプリ（とパスキー）が並んでいる

済んだら、ワークシートの社員用②に印。
まだのものは、やる日を書く

次に入るとき：ログインの画面で

●●●●●●	＝ パスワード
パスワードの欄に●●●	

（何も入らない）	＝ パスキー
「パスキーでサインイン」	

今日はログアウトして試さない。作ったばかりのパスキーは、すぐには使えないことがある

特集「正しく怖がろう」2。Google のパスキーは、ログインに使えるまで 7 日ほどかかることがある（特集3 の調べ）

会社の決まり①（全員）

振込先の変更と急ぎの送金は、メールの外で確かめる

1

「振込先が変わった」
「急いで送って」と言われたら、
メールや LINE の外で確かめる。
前から知っている番号に
電話する。届いたメールの
番号にはかけない

2

社長がメールや
LINE で送金を
頼むことはない。
頼まれたら、
社長本人に
電話で確かめる

3

社長を名乗って
SNS や LINE の
グループを作るよう
言われたら、
特に疑う

見破ることに頼らず、決まりで止める。確かめられて怒る人はいない

会社の決まり②（全員）

銀行を名乗る電話でも、メールアドレスを教えない。言われたソフトを入れない

電話：「銀行です」	教えない・入れない	切って、かけ直す	管理者に知らせる
メールアドレスを聞かれる。ソフトを入れるよう言われる	公式のストアのアプリでも、電話で言われたものは入れない	通帳・カード・契約の書類にある公式の番号に、自分からかける	あったことをそのまま伝える

2026年5月から：電話で遠隔操作のソフトを入れさせ、会社のパソコンを外から操る手口が急増

社員のみなさんへ

おかしいと思ったら、一人で抱えず、すぐ管理者に

勝手に変えない	通知を押さない	すぐ知らせる	共有を教える
今日やった設定のほかは、会社のアカウントを変えない。分からなければ管理者に聞く	自分でログインしていないのに「承認しますか？」が来たら、押さずに知らせる	乗っ取られたかも・なくした・リンクを押した。早いほど、止められる。責めない	みんなで使っているアカウントは、どのサービスかを教える。パスワードは言わない

管理者：　　**連絡の仕方：**

ここから管理者の話（社員のみなさんも聞いておく）

管理者が一度だけやることは、3つある

① 全員の2段階認証を、義務にする

一人ずつの「お願い」ではなく、設定しないと入れない形に。
社員に日付を知らせてからかける

Google：2 段階認証プロセスの「適用」（K1）
Microsoft：「セキュリティの既定値群」（K3）

② 管理者を2人にし、いちばん固くする

一人が倒れても、辞めても、スマホをなくしても、
会社が自分のメールに入れるように

Google：特権管理者を2人（K2）
Microsoft：グローバル管理者を2人（K4）／固める（K6）

③ 外への自動転送を止める

乗っ取った人の「届いたメールを全部自分に送る」
設定を、会社の側で効かなくする

Google：「自動転送」のチェックを外す
Microsoft：「オフ – 転送が無効になっています」（K5）

会社ならではの穴（ワークシート　管理者用2）

管理者の画面の外にある穴を、5つふさぐ

① みんなで使うアカウント	② 辞めた人のアカウント	③ ドメインの登録先	④ 法人口座	⑤ 振込先の変更
人ごとに招待するか、会社のアドレスに付ける。辞めたら、その日に変える	その日のうちに止める。辞めるときにやることを紙1枚にする	2段階認証と自動の更新。誰がログインできるかを管理者2人が知っておく	作る人と承認する人を分ける。上限と知らせのメールを確かめる	メールの外で確かめる（決まり①）

いま：「共有」に〇を付けたアカウントを、サービスの名前だけ教えてもらい、管理者用2 の D に書く

段取りを決める（ワークシート　管理者用4）

今日・今週・今月の順でやる。担当と日付を、この場で決める

今日（1時間ほど）

- 管理者を2人にする
- 管理者2人に、パスキーかセキュリティキー。予備も
- 全員の2段階認証をかける（決めておいた日付で）
- 外への自動転送を止める

今週

- 必須の日までに、全員が登録したかを確かめる
- 振込先の決まりを伝える（今日伝えた）
- 銀行の承認と知らせの設定を確かめる

今月

- みんなで使うアカウントを人ごと・会社のアドレスに
- 辞めるときにやることを紙1枚に。残ったアカウントを止める
- ドメインの登録先に2段階認証・自動の更新

まとめ（ワークシートの印を数える）

今日できたことと、これからの日付

今日できたこと	これからの日付	今日からの決まり
・画面ロック ・パスワードをスマホに ・会社のアカウントに パスキーか認証アプリ	・2段階認証が必須になる日 月　　日 ・まだの人は、その日までに	・振込先の変更と急ぎの 送金は、メールの外で ・おかしいと思ったら、 すぐ管理者に

もっと知りたい人へ：特集「正しく怖がろう」 teleport.jp/dataiscity/right-fear/（設定の手順・なくしたとき）

この作品は クリエイティブ・コモンズ 表示 4.0 国際 ライセンスで提供されています。
出典：Data is CITY（teleport.jp/dataiscity/）
https://creativecommons.org/licenses/by/4.0/deed.ja

全員の2段階認証プロセスを「適用」にする

管理コンソール（admin.google.com）

① 特権管理者のアカウントで入る
② 「セキュリティ」→「認証」→「2 段階認証プロセス」
③ 「ユーザーが 2 段階認証プロセスを有効にできるようにする」にチェック（勉強会の前日までに）
④ 「適用」→「指定した日付から適用を有効にする」→ 決めた日
⑤ 「新しいユーザーの登録期間」→ 1週間ほど
⑥ 「方法」→ まず「制限なし」
⑦ 「保存」

確かめる

「レポート」→「ユーザー レポート」→「セキュリティ」。適用の日の前に開き、まだの人に声をかける

気をつける

「方法」を「テキスト メッセージや音声通話で受け取った確認コード以外」に上げるのは、SMS の人の受け取り方を替えてもらってから

押す所の名前は公式ヘルプのとおり（特集5、2026-11-17 に確認）。画面が違っていたら、公式の説明を正とする

特権管理者を2人にし、パスキーで入れるようにする

特権管理者を2人に

① 「ディレクトリ」→「ユーザー」→
2人目にする人の名前

② 下の方の「管理者ロールと権限」

③ 「特権管理者」の横のスライダーを
「割り当て済み」→「保存」

パスキーで入れるように

① 「セキュリティ」→「認証」→
「パスワードレス」

② 「パスワードのスキップ」

③ 「ユーザーがパスワードをスキップして
パスキーで認証できるようにする」に
チェック →「保存」

選ばない：「パスキーの制限」の「ハードウェア セキュリティ キーのみでパスキーを許可します」
（選ぶと、スマホやパソコンのパスキーが使えなくなる）。2段階認証の「適用」は、K1 で別にかける

押す所の名前は公式ヘルプのとおり（特集5、2026-11-17 に確認）。画面が違っていたら、公式の説明を正とする

「セキュリティの既定値群」が「有効」かを確かめる

Microsoft Entra 管理センター（entra.microsoft.com）

① グローバル管理者のアカウントで入る

② 「Entra ID」→「概要」→「プロパティ」のタブ
→ 下の方の「セキュリティの既定値」

③ 「組織はセキュリティの既定値で保護されて
います。」と出ていれば、済んでいる

④ 出ていなければ「セキュリティの既定値群の管理」
→「有効」→「保存」

有効になると

・全員が、次のサインインで登録を
求められる。猶予はない。
先に社員に知らせる

・古いメールソフトや、スキャンを
メールで送る複合機が送れなく
なることがある。一度試す

・「条件付きアクセス ポリシーを
使用しているため」と出たら、
すでに設定済み

押す所の名前は公式ヘルプのとおり（特集5、2026-11-17 に確認）。画面が違っていたら、公式の説明を正とする

グローバル管理者を2人にし、パスキーを使えるようにする

グローバル管理者を2人に（admin.microsoft.com）

① 「ユーザー」→「アクティブなユーザー」

② 2人目にする人を選び、「ロールの管理」

③ 「グローバル管理者」→「変更の保存」

パスキーを使えるように（entra.microsoft.com）

① 「Entra ID」→「認証方法」→「ポリシー」

② 「パスキー（FIDO2）」を有効にし、
パスキーのプロファイルを作る

③ 選ぶ所が多い。公式の説明「Authenticator での Microsoft Entra ID のパスキーの有効化とサポート」を横に開いて進める

増やすのは2人まで。パスワードの再設定だけを手伝う人には「パスワード管理者」のような、できることの少ない役割を

押す所の名前は公式ヘルプのとおり（特集5、2026-11-17 に確認）。画面が違っていたら、公式の説明を正とする

外への自動転送を、会社の側で止める

Google Workspace（最初は許可されている）

① 「アプリ」→「Google Workspace」→「Gmail」
→「エンドユーザーのアクセス」

② 「自動転送」

③ 「受信メールを自動転送することをユーザーに
許可する」のチェックを外す（社内だけなら
「内部メールアドレスのみ」）

④ 「保存」

Microsoft 365（送信スパム フィルター ポリシー）

① 値は3つ：「自動 – システム制御」（最初）・
「オン – 転送が有効になっています」・
「オフ – 転送が無効になっています」

② 「自動」のままにせず、止めるなら「オフ」

③ 場所は公式の「送信スパム フィルターの構成」

④ いま転送している人は
「自動転送メッセージ レポート」で確かめる

止める前に：業務で外へ自動転送している人がいないか、勉強会で聞いておく

押す所の名前は公式ヘルプのとおり（特集5、2026-11-17 に確認）。画面が違っていたら、公式の説明を正とする

管理者の手元用 K6

管理者のアカウントを、いちばん固くする

セキュリティキーか パスキーで入る

偽のサイトに
いちばん強い。
予備のキーも
登録し、別の
場所にしまう

一人に一つ

管理者の
アカウントを
2人で使い回さない

取り戻す準備

再設定用の電話と
メールを登録。
バックアップコード
は紙で金庫に。
ドメインの登録先の
ログインも控える

管理用を分ける

できれば、管理の
仕事にだけ使う
アカウントを、
ふだんのメールと
別に持つ

管理者が乗っ取られると、全員のアカウントが開けられる

管理者の手元用 K7（ワークシート 管理者用3 の H）

辞めた人のアカウントは、その日のうちに止める

Google Workspace

① パスワードを変える
② 再設定用のメールと電話番号を消す
③ ログイン Cookie をリセットする
④ アプリの許可（OAuth のトークン）を取り消す
⑤ セキュリティキーとアプリ パスワードを取り消す
⑥ 会社のデータが入った端末のデータを消す
⑦ 残すデータは、消す前に「停止」して移す

Microsoft 365

① サインインできないようにする
② メールの中身を残す
③ スマホのデータを消す
④ メールを別の人に転送するか、
共有のメールボックスに替える
⑤ ライセンスを外す
⑥ 最後にアカウントを消す（30日は戻せる）

あわせて：みんなで使うアカウントのパスワードを、その日に変える

特集5。Google「従業員の離職後にデータのセキュリティを維持する」・Microsoft「元従業員を削除する – 概要」