進め方のガイド：中小企業の社内勉強会「会社のメールを、乗っ取られない形にする」

スライド：`right-fear-sme.pptx`（本編 22 枚＋管理者の手元用 7 枚〈K1〜K7〉、ノートに台本）／`right-fear-sme.pdf` ワークシート：`worksheet-sme.pdf`（A4・6 ページ。社員用 1 枚〈表裏〉を全員に、管理者用 2 枚〈表裏・1／4〜4／4〉を管理者 2 人に。直すときは `.pptx`） 元の特集：Data is CITY Media 特集「正しく怖がろう」（2026年11月17日）。中心は 5「会社の管理者が一度だけやること」。あわせてトップ・1「守れるもの、守れないもの」・2「見破れなくても、守れる」・3「今日、設定する」・4「漏れたとき・なくしたとき」 作り直し：`python3 docs/dataiscity/right-fear/teach/build/build.py sme`（.pptx）。PDF は Microsoft PowerPoint で書き出す 出典：Data is CITY（teleport.jp/dataiscity/）、CC BY 4.0

システム管理者のいない会社（社員は数人から数十人）で、社長か総務の担当者が、専門家なしで回せるように作った。スライドのノートに、話すことを、そのまま読める文で書いた。話す人は、ノートを読み上げるだけで 30〜45 分が回る。

この勉強会のゴール

終わったときに、次の状態になっている。

1. **社員全員**が、自分のスマホで - 画面ロックが「顔か指」と「6桁以上」になっている - パスワードをスマホに覚えさせる設定をオンにしている - 会社のアカウントに、パスキーか認証アプリを付けている（Google Workspace は 2 段階認証プロセスをオンにしてパスキーを作る。Microsoft 365 は「セキュリティ情報」で Microsoft Authenticator を登録し、管理者が許可していればパスキーも） 2. **社長・担当者（管理者）**は、管理者としてやることの日付と担当を決めている - 全員の 2 段階認証を必須にする日（勉強会の 1〜2 週間後） - 管理者を 2 人にする・外への自動転送を止める（今日） - 会社ならではの穴 5 つ（みんなで使うアカウント・辞めた人・ドメインの登録先・法人口座・振込先の変更）の段取り 3. 全員が、会社の決まりを知っている：**振込先の変更と急ぎの送金は、メールの外で確かめる。**おかしいと思ったら、すぐ管理者に。

ねらい

- 漏えいがこの夏から急に増え、偽の請求書とニセ社長の手口が会社に向いていることを、数字で知る（スライド3〜5）。
- 顔や指は「スマホが持ち主本人かを確かめる」だけで、守りの強さはその先でスマホが渡すもので決まることを、自分の言葉で言える。**パスワードは合言葉を渡す。パスキーは渡さない。本物が出す問題に、スマホの中の鍵がその回だけの答えを返す。偽の画面には答えない**（スライド7）。
- 一人ずつの「お願い」ではなく、管理者の画面で全員にかける、という分担を知る（スライド9・19）。
- 見破ることに頼らず、決まりで止める（スライド16・17）。

準備（1〜2 週間前と、前日まで）

ワークシートの管理者用 1／4 の「A」と同じ。業者が会社のメールを入れた会社では、社長が管理者になっていないことが多く、業者に頼むと前日では間に合わない。だから、管理者かどうかは **1〜2 週間前**に確かめる。

1〜2 週間前

1. **会社のメールが何で動いているか**を確かめる（スライド10）。会社の名前のアドレスを Gmail の画面で開いていれば Google Workspace、Outlook で開いていれば Microsoft 365。個人の Gmail・個人の LINE・プロバイダーのメールなら、まとめて設定する画面はふつうない（設定②は、仕事に使っている自分の Google アカウントでやる）。 2. **自分が管理者か**を確かめる。会社のアドレスで admin.google.com か admin.microsoft.com に入れれば管理者。入れなければ、**会社のメールを入れた業者に頼み、社長か担当者を管理者に足してもらう**（2 人に。手元用 K2・K4）。業者が管理者のままのときも、会社の人を管理者に足す。 3. **2 段階認証を必須にする日を決める**（勉強会の 1〜2 週間後）。勉強会では、この日を社員に伝える（スライド21・22）。その場では決めない。 4. **設定②の手伝い役を決める**：社員 4 人に 1 人（12 人なら、管理者のほかに 2〜3 人）。手伝い役は、前もって自分のスマホでスライド12〜14 を済ませておく。管理者 1 人で 12 人を見ると、8 分では終わらない。

前日まで

5. **Google Workspace**：管理コンソールの「セキュリティ」→「認証」→「2 段階認証プロセス」で「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」にチェックが入っているか（入っていないと、社員が当日オンにできない）。「パスワードレス」→「パスワードのスキップ」が許可されているか（手元用 K1・K2）。「適用」の日付は、3. で決めた日を、勉強会のあとに入れる。 6. **Microsoft 365**：Microsoft Entra 管理センターで「セキュリティの既定値群」が有効かを見る（手元用 K3）。有効にすると、全員が次のサインインで登録を求められ、猶予はない。まだなら、勉強会が終わってから有効にする（勉強会がその知らせになる）。パスキー (FIDO2) を使えるようにするかを決める（K4。決めていなければ、当日は認証アプリまで）。 7. **自分のスマホで、スライド12〜14 の手順を一度たどる**。画面の名前が違っていたら、公式の説明を正とする（特集3〈teleport.jp/dataiscity/right-fear-setup/〉と特集5 に公式のリンク）。 8. 会社から貸しているスマホがあれば、設定を変えてよい範囲を決めておく。 9. 会社のアカウントのパスワードを忘れている人がいたら、管理者の画面で再設定できるようにしておく。 10. 外へ自動転送している人がいないか、業務で要るものがあるか（K5）。 11. **社員に伝える**：「スマホを持ってくる」「会社のアカウントのパスワードを思い出しておく」。 12. 会場：Wi-Fi、スクリーンかテレビ、ワークシートの印刷（社員用は A4 表裏で人数分、管理者用は 2 人分）。

時間配分

社員が手を動かすのは、11（書き出す）、12〜14（自分のスマホを設定）、15（確かめる）。13 と 14 は、会社のメールに合わせて**どちらか一方だけ**を見せる。

45 分版

時間	スライド	活動	問いかけ
0〜1分	1	表紙。スマホを手元に	—
1〜2分	2	今日のゴール（社員みんな／管理者）	—
2〜4分	3	漏えいはこの夏から桁が変わった（約3億7,600万件＝去年の約7.6倍、約94%が7月以降）。AI が攻撃の仕事の8〜9割	—
4〜6分	4	ニセ社長詐欺 127件・約38億8,000万円・1件約3,100万円、ランサムウェア被害の約6割が中小企業	「私の名前で『至急送って』と来たら？」（心の中で）
6〜8分	5	一人のメールの乗っ取り → 自動転送 → 本物のアドレスから偽の請求書	—
8〜9分	6	見分け方 5 つは、もう効かない	—
9〜12分	7	パスワードは合言葉を渡す。パスキーは渡さない	—
12〜13分	8	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	—
13〜14分	9	社員みんながやること／管理者がやること	—
14〜15分	10	うちの会社のメールはどれか（13 と 14 のどちらを見るか）	—
15〜18分	11	ワークシート社員用① 仕事で使うアカウントを名前だけ書き出す	—
18〜23分	12	**設定①** 画面ロックとパスワードを覚えさせる	—
23〜31分	13 か 14	**設定②** 会社のアカウントにパスキーか認証アプリ（削らない）	—
31〜33分	15	設定の画面で確かめる（今日はログアウトしない）。社員用②に印	—
33〜35分	16	会社の決まり①：振込先の変更と急ぎの送金は、メールの外で	「前から知っている番号は、どこに控えてある？」
35〜37分	17	会社の決まり②：銀行を名乗る電話でも、教えない・入れない・かけ直す	—
37〜38分	18	おかしいと思ったら、すぐ管理者に（管理者の名前と連絡の仕方を書く）	—

時間	スライド	活動	問いかけ
38〜40分	19	管理者が一度だけやること 3 つ	—
40〜42分	20	会社ならではの穴 5 つ。「共有」に○のアカウントを聞いて管理者用 2 の D へ	「共有に○を付けたのは？」（名前だけ）
42〜44分	21	今日・今週・今月。必須にする日（前もって決めた日）を伝え、ほかの担当と日付をこの場で決める	—
44〜45分	22	まとめ。印の数を聞く。これからの日付	—

計 45 分（1+1+2+2+2+1+3+1+1+1+3+5+8+2+2+2+1+2+2+2+1）。押したら、6 と 17 を飛ばす（17 は 16 の終わりに一言だけ）。**12 と 13／14 は削らない。**

30 分版

飛ばすもの：4（数字は 3 で一言）、6、11（書き出しは家での宿題に）、17（16 の終わりに一言）、20（管理者が後でワークシートを見てやる）。

時間	スライド	活動
0〜2分	1・2	表紙・ゴール
2〜5分	3・5	漏えいの急増と、ニセ社長詐欺 127件（4 の数を一言）。一人の乗っ取りから偽の請求書
5〜8分	7・8	合言葉とパスキー。強さの順
8〜9分	9・10	分担と、会社のメールはどれか
9〜13分	12	**設定①**（4 分）
13〜21分	13 か 14	**設定②**（8 分。削らない）
21〜22分	15	設定の画面で確かめる・印
22〜24分	16	会社の決まり（銀行を名乗る電話も一言）
24〜25分	18	すぐ管理者に
25〜28分	19・21	管理者の 3 つと、今日・今週・今月の日付
28〜30分	22	まとめ

計 30 分（2+3+3+1+4+8+1+2+1+3+2）。

管理者の手元用（K1〜K7）

勉強会では見せない。管理者が一人で管理の画面を開くときに、横に置く。Google Workspace なら K1・K2・K5・K6・K7、Microsoft 365 なら K3・K4・K5・K6・K7。押す所の名前は、特集5 の本

文（Google Workspace 管理者ヘルプ・Microsoft Learn を 2026年11月17日に開いて、表記のまま写したもの）。

話す順と、台本の要点

ノートに全文がある。要の所だけ。

- **なぜ今（3〜5）**：数は特集の本文のまま。「件」は件のまま読む。いま起きていることは、いちばん新しい数（2026年の 10 月末まで、2026年 1〜6 月）で言う。怖がらせて終わらず、「だから今日ふさぐ。ふさぎ方は分かっている」につなぐ。5 は「迷惑がかかるのは、うちの会社だけではなく取引先」。
- **合言葉とパスキー（7）**：顔や指は、どちらでも「スマホを開ける」だけ。顔や指の形はサイトに送られない。パスワードは合言葉で、聞いた人なら誰でも使える。パスキーは合言葉を伝えない。本物のサイトが毎回ちがう問題を出し、スマホの中の鍵がその回だけの答えを返す。鍵はスマホの外に出ない。スマホは答える前に相手の住所を確かめ、偽の画面には答えない。「偽物かどうかを見分けるのは、目ではなくスマホ」。
- **分担（9・19）**：社員は自分のスマホと会社のアカウントだけ。管理者の画面のことは、社員は何もしなくていい。日付だけ覚えておく。
- **設定②（13・14）**：手伝い役（4 人に 1 人）が、止まっている人の横に行く。60 代の人が止まりやすいのは、スマホのブラウザを会社のアカウントに切り替える所（右上の丸）、パスワードをもう一度聞かれる所、電話番号を聞かれる所。スライド13 に手順として入れた。会社のアドレスで入る。Google は、2 段階認証プロセスのオンとパスキーの両方（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）。Microsoft は、まず認証アプリ、管理者が許可していればパスキー。
- **会社の決まり（16）**：社長が話すときは「社長がメールや LINE で送金を頼むことはない。頼まれたら、私に電話で確かめる。確かめられて怒ることは絶対にない」を、自分の言葉ではっきり言う。ここがいちばん効く。
- **段取り（21）**：必須にする日は、1〜2 週間前に決めておいた日を伝える（その場では決めない）。この場で決めるのは、ほかのことの担当と日付。勉強会のあと、Google なら決めた日を「指定した日付から適用を有効にする」に入れる。

ことばの決まり（特集の書き方の手引き〈docs/dataiscity/editorial.md〉と特集の本文に合わせる）

- 顔や指とパスキーを一つの言葉にまとめない。「顔認証の鍵」「指紋の鍵」とは言わない。
- 「パスキーなら安全」ではなく、何に効くかを付けて言い切る：「偽のサイトでは使えない」「漏れたパスワードや偽の画面で盗まれたパスワードだけでは入られない」。
- **パスキー**＝パスワードの代わりに使う、偽のサイトでは使えない鍵。**2 段階認証**＝パスワードのほかに、もう一つ確認を足すこと（Google は「2 段階認証プロセス」、Microsoft は「多要素認証」と呼ぶ）。**認証アプリ**＝30 秒ごとに変わる番号を出すアプリや、通知で承認するアプリ（Microsoft

Authenticator など)。**管理者**＝会社のメールの管理の画面に入れる人（Google は特権管理者、Microsoft はグローバル管理者)。**ドメイン**＝会社のアドレスの「@」から後ろ。

- Google Workspace と Microsoft 365 の押す所の名前は、特集 5 と特集 3 の調べ（公式ヘルプ）の表記のまま。それ以外の手順は足していない。
- 会社名や実在の画面は再現しない。スライドの画面は図形で描いた作りもの。

つまずき

- **会社のアカウントの設定を、勝手に変えない**：今日やるのは、スライド12〜14 の設定だけ。ほかの設定（転送・再設定用の連絡先・アプリの連携など）は変えない。分からなければ管理者に聞く。
- **管理者がいない・だれが管理者か分からない**：会社のアドレスで admin.google.com／admin.microsoft.com に入ってみる。入れなければ管理者ではない。契約したときに申し込んだ人が、最初の管理者になっていることが多い。ホームページや契約を手伝った会社が管理者のままのことがある。その会社に聞き、社長か担当者を管理者に足してもらう（2 人に)。管理者が分かるまで、勉強会は設定①と、個人のアカウントの設定②（自分の Google）までにし、会社のアカウントは日を改める。
- **「2 段階認証プロセス」の項目がない・オンにできない（Google)**：管理者が「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」にチェックを入れていない。その場で管理者が入れる（K1 の③)。
- **パスキーでログインできない・パスワードも聞かれる（Google)**：管理者が「パスワードのスキップ」を許可していない。パスキーは 2 段階認証の 2 つ目の確認には使える（K2)。新しいパスキーは、ログインに使えるまで 7 日ほどかかることがある。
- **当日は、ログアウトして試さない**：作ったばかりのパスキーは、すぐにはログインに使えないことがある（Google は 7 日ほどかかることがある)。ログアウトすると入れなくなって困るので、当日は設定の画面で確かめるだけにし、ログインの画面は次に入るときに見る（スライド15)。
- **スマホのブラウザが個人の Google で入っている**：右上の丸を押して会社のアドレスに切り替える。出てこなければ会社のアドレスでログインする（スライド13 の②)。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、電話番号を聞かれたら自分の携帯の番号を入れる。ここで止まる人が多いので、手伝い役が横に付く。
- **「パスキー」が選べない（Microsoft)**：管理者がパスキー (FIDO2) を有効にしていない。当日は認証アプリまで（K4)。Authenticator のパスキーは Android 14 以降、iOS 17 以降。
- **SMS しか登録していない人**：ないよりずっといい。認証アプリかパスキーを足してから、SMS を外す（Microsoft の電話の削除は、誤って消すと元に戻せない)。Google の「方法」を SMS 以外に上げるのは、全員が替えたあと（K1)。
- **会社のアカウントのパスワードを思い出せない**：その場で管理者の画面で再設定する。授業のように「家で」はできないので、前日に伝えておく。
- **家族と共有のスマホ・パソコン**：パスキーを作らない（ロックを解ける人なら誰でも入れる)。
- **会社から貸しているスマホ**：会社の決まりに従う。
- **画面や手順の名前が違う**：プランや時期で変わる。公式の説明を正とする。

- **パスワードそのもの・バックアップコード・口座番号は、ワークシートにも、人にも、見せない**。画面を見せ合うときは、先に一言注意する。ワークシートは回収しない（印の数だけ聞く）。管理者用は鍵のかかる所に。
- **社内にサーバーや VPN がある会社**：その機器の更新と管理も要る。この勉強会では扱わない。

よく出る質問と答え

- 「顔でログインしているから大丈夫？」→ 顔はスマホが本人かを確かめるだけ。パスワードの欄に●●●が入るなら、中身はパスワードの自動入力で、偽の画面に入れれば盗まれる。「パスキーでサインイン」と出て欄に何も入らなければパスキー（スライド7・15）。
- 「顔の形が会社や Google に送られるの？」→ 送られない。スマホの中で確かめるのに使うだけ。
- 「パスキーにすれば絶対安全？」→ 絶対ではない。偽のサイトでのログインに強くなる。電話で言われて自分で操作する、言われて入れたアプリに画面を操作される、は別に防ぐ（スライド17、特集2）。
- 「スマホを替えたら・なくしたら、パスキーは？」→ 同じ Apple か Google のアカウントの自分のほかの端末に、暗号をかけたまま受け渡される。会社のアカウントに入れなくなったら、管理者に（管理者が 2 人いる意味）。
- 「SMS の番号でもいいのでは？」→ ないよりずっといい。でも、偽の画面に打てば、その場で使われる。金融庁も 2026年4月の広報で「リアルタイムフィッシングに脆弱」と書いている。会社のアカウントは、パスキーか認証アプリへ。
- 「自分がログインしていないのに『承認しますか？』が来た」→ 押さない。何度も鳴らして、つい押すのを待つ手口がある。管理者に知らせる。
- 「取引先の振込先の変更を、電話で確かめるのは失礼では？」→ 偽の請求書は、本物の会社のアドレスから届くことがある。確かめるのが会社の決まりだと伝えればよい。前から知っている番号にかける。届いたメールに書かれた番号にはかけない。
- 「個人の LINE で取引先とやりとりしているが？」→ アカウントが会社のものではないので、辞めた人のアカウントを止めることも、2 段階認証を義務づけることも、会社にはできない。すぐに移せなくても、まず自分のアカウントを固める（特集3）。
- 「パスワードは何か月ごとに変えればいい？」→ 変え続けなくていい。変えるのは、漏れたと知らせが来たときと、知っている人が辞めたとき（みんなで使うアカウント）。

ワークシート（worksheet-sme.pdf、A4・6 ページ）

社員用（全員に 1 枚・表裏）

- 表：書かないことの注意／① 仕事で使っているアカウントの棚卸し（名前・会社の／個人の・いまの入り方〈パスワードだけ／SMS／認証アプリ／パスキー〉・共有・今日やった） ← スライド11
- 裏：② 今日やったことに✓　← スライド12〜15／会社の決まり 4 つ　← 16〜18／管理者の名前と連絡の仕方・必須になる日／起きてしまったら（乗っ取られたかも・なくした・漏れた）

管理者用（2 人に 2 枚・表裏。パスワード・バックアップコード・口座番号は書かない。鍵のかかる所に）

- 1／4：A 勉強会の準備（1〜2 週間前：管理者か確かめる・業者に頼む・必須の日・手伝い役／前日まで：管理の画面の確かめ・社員に伝えること）／勉強会のあとのメモ
- 2／4：B 会社のメール／C 管理者は誰と誰（パスキーかセキュリティキー・予備・再設定用・バックアップコードのしまい場所）／D みんなで使うアカウント／E ドメインの登録先
- 3／4：F 法人口座（作る人・承認する人・上限・知らせ）／G 辞めた人のアカウント／H 辞めるときにやること（Google・Microsoft の公式の手順。紙 1 枚）
- 4／4：I 今日・今週・今月の段取り表（担当・予定日・済んだ日）／J まだの人

記号は A〜J。K は使わない（スライドの「管理者の手元用 K1〜K7」とぶつかるため）。社員用の字は 10.5pt 以上。

使った事実と出典（スライドの隅にも記載）

数はすべて特集「正しく怖がろう」の本文のもの（特集の編集部が一次の出典を開いて確かめた）。

事実	出典
2026年に国内で公表されたサイバー攻撃による漏えいは 10 月末までに約 3 億 7,600 万件、2025年（4,953 万件）の約 7.6 倍、約 94% が 7 月以降の公表、認証情報は延べ約 1 億 6,100 万件で 2025年の約 31 倍	MM総研（2026-11-04）https://www.m2ri.jp/release/detail.html?id=745
10 月に公表されたサイバー攻撃などは 233 件で月の過去最多	ANN（2026-11-09）https://news.ksb.co.jp/ann/article/17033815
AI が攻撃の 80〜90% を進めた	Anthropic（2025-11-13）https://www.anthropic.com/news/disrupting-AI-espionage
ニセ社長詐欺は 2026年 1〜6 月に 127 件・約 38 億 8,000 万円・1 件あたり約 3,100 万円、手口（公開アドレスに届く・LINE などのグループ・残高を聞く・至急の送金）。ボイスフィッシング（2024年秋から）と遠隔操作のソフトの手口（2026年5月から急増）。ランサムウェアの被害企業の約 6 割が中小企業	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）https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf
メールや SMS のワンタイムパスワードは「リアルタイムフィッシングに脆弱」	金融庁の広報（2026-04-16）https://www.fsa.go.jp/news/r7/sonota/20260416-2/20260416-2.html
Google Workspace の 2 段階認証プロセスの適用・パスワードのスキップ・特権管理者・自動転送・離職のときの手順	Google Workspace 管理者ヘルプ（特集5 の参考資料。2026-11-17 に確認）https://knowledge.workspace.google.com/admin/security/deploy-2-step-verification?hl=ja ほか

事実	出典
Microsoft 365 のセキュリティの既定値群・グローバル管理者・パスキー (FIDO2)・外部メール転送・元従業員の削除	Microsoft Learn（特集5 の参考資料。2026-11-17 に確認）https://learn.microsoft.com/ja-jp/entra/fundamentals/security-defaults ほか
社員の設定（iPhone・Android のパスワード、Google のパスキーと 2 段階認証プロセス、Microsoft 365 の「セキュリティ情報」）	各社の公式の説明（特集3 の調べ、docs/dataiscity/right-fear/services.json。2026-11-16 に確認）
漏えいと乗っ取りの区別、見分け方 5 つ、合言葉とパスキー、強さの順、会社ならではの穴 5 つ、今日・今週・今月	特集「正しく怖がろう」トップ・1〜5（Data is CITY Media、2026-11-17）https://teleport.jp/dataiscity/right-fear/
IPA のビジネスメール詐欺の対策	IPA「ビジネスメール詐欺（BEC）対策特設ページ」https://www.ipa.go.jp/security/bec/about.html

今日・今週・今月の分け方と時間の目安は、特集の編集部の見立て。勉強会の時間配分は、この教材の見立て。

ライセンス

この教材（スライド・ワークシート・進め方のガイド）は、クリエイティブ・コモンズ 表示 4.0 国際（CC BY 4.0）で提供する。改変も配布も、営利目的の利用も自由。社名や日付を入れて、そのまま社内で配ってよい。使うときは「出典：Data is CITY（teleport.jp/dataiscity/）」と表示する。https://creativecommons.org/licenses/by/4.0/deed.ja

出典：Data is CITY（teleport.jp/dataiscity/）、CC BY 4.0