

スタッフサービス・エンジニアリング様向け

ハンズオンガイド

3日目 インシデントの初動と報告文

架空の会社で起きたランサムウェアの被害を題材に、最初の1時間の動きを決めます。事実だけを並べた時系列メモから、Geminiで経営層への第一報を作り、言い切りを点検します。

2026年11月27日（金）

オンライン（ZOOM）

個人演習 [40min]

 Gemini

目次

本日のゴール

本日の学び
作るもの

当日の流れ

進め方

始める前の準備

配布フォルダを開く
Geminiに文面を送る

S04 インシデントの初動と報告文

ねらい
できあがりの目安
使うファイルと作るファイル
STEP 1 シナリオと検知メモを読む
STEP 2 最初の1時間にする行動を選ぶ
STEP 3 時系列メモを作る
STEP 4 Geminiで第一報の下書きを作る
STEP 5 メモにない言い切りを点検する
STEP 6 報告の期限を確かめる
STEP 7 速報の対象かをGeminiと考える
職場のチェック表
この演習とセキュリティの仕事
うまくいかないとき

よくある質問

01

本日のゴール

インシデントに気づいた最初の1時間でする行動と、しない行動を区別し、事実だけで第一報を組み立てられるようになります。

本日の学び

- 最初の1時間に、隔離と連絡と記録を優先し、証拠を消す行動を避ける
- 見たことと推測を分けて、時系列メモを作る
- Geminiの下書きから、メモにない言い切りを見つけて直す

作るもの

時系列メモ.txt と、経営層へ送る第一報の2つです。第一報は、Geminiの下書きを直したものを手元のメモ帳に保存します。

A社の情報システム部より、経営層の皆様へ向けたセキュリティインシデントに関する第一報をご報告いたします。

ご提示いただいた時系列メモに基づき、以下の通り状況をまとめました。メモに記載のない事項につきましては、現時点では推測で補わず「調査中」としております。

セキュリティインシデントに関する第一報

1. 攻撃の種類
- ランサムウェアによる攻撃（疑い）および不正アクセスの可能性
- （根拠：EDRによる「ランサムウェアの疑い」の警告、身代金を求める文面のファイル「README_RESTORE.txt」の確認、および予定外の保守アカウントによるVPNログインの検知）
2. 判明している範囲
- 該当端末：経理担当のパソコン（PC-KEIRI-03）にて、共有フォルダのファイル名末尾が `.locked` に変更され、暗号化されていることを確認。
- アクセス記録：共有フォルダ「顧客台帳」への読み出し記録を確認（取引先の担当者約2,300人分の氏名、電話番号、メールアドレスが含まれています）。

図1：作るもののひとつ、第一報。6項目に分かれ、分からないことは「調査中」になっていれば完成です

当日の流れ

全体で[120min]です。前半の講義で会社の対策と、これからの備え方を見てから、後半のハンズオンで初動を練習します。

枠	中身	形式	時間
S01	前回の振り返りと本日の到達点	講義	[10min]
S02	会社としての対処	講義	[25min]
S03	これからのセキュリティの考え方	講義	[25min]
S04	ハンズオン インシデントの初動と報告文	ハンズオン	[40min]
S05	持ち帰りチェックリスト	講義	[10min]
閉会	質疑応答		[10min]

進め方

- 講師が画面を共有し、同じ操作を見せながら1STEPずつ進めます。
- 質問はZOOMのチャットに、STEPの番号と、画面に出ていることを書いてください。
- 各STEPの[Nmin]は目安です。時間になったら、講師が次のSTEPへ進めます。
- Geminiに入れるのは、配布フォルダの架空の情報だけです。自分の会社や顧客の情報は入れません。
- シートとメモは提出しません。自分の業務のことをそのまま書いて構いません。書いたファイルは、社外の人に送らずに保存します。

始める前の準備

配布フォルダを開き、Geminiに文面を送れることを確かめてから演習に入ります。

配布フォルダを開く

- 1 教材サイトの「配布物」から、day3_handsonのZIPをダウンロードします。WindowsとMacで別のZIPです。
- 2 ZIPを展開し、デスクトップに置きます。
- 3 `day3_handson` フォルダを開き、中身を確認します。

	名前	サイズ	更新日
	01_シナリオ/		2026/10/27 17:20:50
	02_初動/		2026/10/27 17:21:22
	03_報告文/		2026/10/27 17:21:22
	04_持ち帰り/		2026/10/27 17:21:22
	00_コピペ用_当日使う文章.txt	1.1 kB	2026/10/27 17:20:34
	README.md	1.6 kB	2026/10/27 17:20:34

図2：展開した配布フォルダ。ブラウザで開いた画面で、Windowsのエクスプローラーでも同じ名前が並びます

Geminiに文面を送る

- 1 Chromeで `gemini.google.com` を開きます。ログインしなくても使えます。
- 2 このガイドの黒い枠の右上にある `コピー` を押します。
- 3 Geminiの入力欄に貼り付け、 `<ここに…>` の部分を配布ファイルの中身に置き換えます。
- 4 入力欄の右下にある送信ボタンを押します。



図3：ログインしていない状態のGemini。中央の入力欄に文面を貼り付け、右下のボタンで送ります

Tips： 同じ文面は、配布フォルダの `00_コピペ用_当日使う文章.txt` にも入っています。ガイドを見失ったときは、そちらからコピーしてください。

S04 インシデントの初動と報告文

[40min]

個人演習

ねらい

架空のA社で起きたランサムウェアの被害を題材に、最初の1時間にする行動と、しない行動を区別します。事実だけを並べた時系列メモから、経営層へ送る第一報を作ります。

できあがりの目安

- ☐ 最初の1時間の8つの行動を、する4つとしない4つに分けて理由を書いた
- ☐ 時系列メモで、見たことと推測を分け、分かっていないことを3つ以上並べた
- ☐ 第一報が6項目に分かれ、分かっていない項目は「調査中」になっている

記号	行動	する、しない（記入）	理由（自分の言葉で1行）
A	感染したパソコンのLANケーブルを抜き、Wi-Fiを切る	する	ほかの端末やサーバーへ広がるのを止める。警察庁もまず隔離を求めている
B	感染したパソコンの電源を切る	しない	メモリ上の記録が消える。隔離できないときだけ検討する
C	上長と情報システム部の窓口へ、電話で連絡する	する	社内のメールも攻撃者に見られている前提で、別の手段で伝える
D	画面とランサムノートをスマートフォンで撮影し、時刻を書き留める	する	あとで時系列を組み立てる材料になる
E	ランサムノートに書かれた連絡先へ、交渉のためにメールを送る	しない	攻撃者との接触は会社として判断する。個人で連絡しない
F	自分でウイルス対策ソフトを動かして、駆除を試みる	しない	調査に要る痕跡が消える
G	共有フォルダのほかのファイルを開いて、被害の範囲を確かめる	しない	被害を広げ、記録を上書きするおそれがある
H	委託先の保守アカウントを止めるよう、VPN機器の担当者に依頼する	する	侵入に使われた入口をふさぐ

図4：最初の1時間の選択肢に記入した例です。C列に判断、D列に理由が入っていれば、STEP 2までは済んでいます

使うファイルと作るファイル

区分	ファイル	使い方
使う	01_シナリオ/インシデントのシナリオ.txt	A社の月曜の朝に起きたこと
使う	01_シナリオ/検知メモ.txt	EDRの警告、ランサムノート、VPN機器の記録
作る	02_初動/最初の1時間の選択肢.xlsx	8つの行動を、するとしないに分ける
作る	02_初動/時系列メモ.txt	様式をもとに、時刻順に書く。別の名前で保存する
使う	02_初動/時系列メモ_記入例.txt	書ききれなかったときに使う

区分	ファイル	使い方
使う	03_報告文/第一報の6項目.txt	第一報に入れる6つの項目
使う	03_報告文/報告の期限早見表.txt	個人情報保護委員会への報告の期限



STEP 1

シナリオと検知メモを読む

AIを開かない

[5min]

何が起きたかを、AIを使わずにつかみます。あなたはA社の情報システム部の担当者です。

1

01_シナリオ/インシデントのシナリオ.txt を読みます。

2

検知メモ.txt で、EDRの警告、ランサムノートの要点、VPN機器の記録を確認めます。

3

共有フォルダの顧客台帳に、何人分のどんな情報が入っているかを書き留めます。

インシデントのシナリオ

会社 A社（架空・物流会社）。社員は約120人。本社のほかに倉庫が2か所ある
あなた A社の情報システム部の担当者。部の人数は3人
11月24日（月）の朝、経理担当の社員から内線が入りました。
「共有フォルダのファイルが開けない。ファイル名の最後が .locked に変わっている」という内容です。
同じころ、EDR（端末の不審な動きを見張る仕組み）の管理画面に警告が出ました。
A社は、倉庫の業務システムの保守を外部の会社に委託しています。
委託先は、VPN機器を通して社内のネットワークに入れる保守用のアカウントを持っています。
このアカウントには多要素認証を設定していませんでした。
経理担当のパソコンからは、共有フォルダ「顧客台帳」が見えます。
顧客台帳には、取引先の担当者約2,300人分の氏名、電話番号、メールアドレスが入っています。

図5：シナリオ。A社（架空・物流会社）の月曜の朝の出来事です

検知メモ

EDRの警告
時刻 11/24 08:52
端末 PC-KEIRI-03（経理担当のパソコン）
内容 ランサムウェアの疑い。短い時間に多数のファイルの書き換えを検知
関連する動き 08:31 に共有フォルダ「顧客台帳」の大量の読み出し
ランサムノート（README_RESTORE.txt）の要点
・ファイルを暗号化した
・データを持ち出した。支払わなければ公開する
・72時間以内に、書かれた連絡先へ連絡せよ
VPN機器の記録
11/24 02:14 委託先の保守アカウントでログイン（予定にない深夜の作業）

図6：検知メモ。VPN機器の記録の時刻に注目します

ここまでできたら

☐ 顧客台帳の人数と、入っている情報の種類を書き留めた

STEP 2

最初の1時間にする行動を選ぶ

AIを開かない

[7min]

8つの行動を、するとしないうちに分けます。善意の行動でも、被害を広げたり証拠を消したりするものがあります。

1

02_初動/最初の1時間の選択肢.xlsx を開きます。

2 C列で、AからHのそれぞれに **する** か **しない** を選びます。

3 D列に、理由を1行で書きます。

記号	行動	する、しない（記入）	理由（自分の言葉で1行）
A	感染したパソコンのLANケーブルを抜き、Wi-Fiを切る		
B	感染したパソコンの電源を切る		
C	上長と情報システム部の窓口へ、電話で連絡する		
D	画面とランサムノートをスマートフォンで撮影し、時刻を書き留める		
E	ランサムノートに書かれた連絡先へ、交渉のためにメールを送る		
F	自分でウイルス対策ソフトを動かして、駆除を試みる		
G	共有フォルダのほかのファイルを開いて、被害の範囲を確かめる		
H	委託先の保守アカウントを止めるよう、VPN機器の担当者に依頼する		

図7：記入する前の選択肢のシートです。8つのうち、するは4つあります

ここまでできたら

☐ 8つすべてに判断と理由が入っている

答え合わせ（判断を書き終えてから開く）

行動	判断	理由
A LANを抜きWi-Fiを切る	する	ほかの端末へ広がるのを止める。警察庁もまず隔離を求めています
B 電源を切る	しない	メモリ上の記録が消える。隔離できないときだけ検討します
C 電話で連絡する	する	社内のメールも見られている前提で、別の手段で伝えます
D 撮影して時刻を書く	する	あとで時系列を組み立てる材料になります
E 攻撃者へ連絡	しない	接触するかは会社として判断します。個人では連絡しません
F 自分で駆除	しない	調査に要る痕跡が消えます
G ほかのファイルを開く	しない	被害を広げ、記録を上書きするおそれがあります
H 保守アカウントを止める	する	侵入に使われた入口をふさぎます

STEP 3

時系列メモを作る

AIを開かない

[8min]

見たことと推測を分けて、時刻順に書きます。第一報は、このメモに書いたことだけで作ります。

- 1 時系列メモの様式.txt をメモ帳で開き、時系列メモ.txt という名前で保存します。
- 2 1行に、時刻と出来事を1つだけ書きます。推測には「推測」と付けます。
- 3 最後に「分かっていないこと」を3つ以上並べます。
- 4 書ききれなかったときは、時系列メモ_記入例.txt を使って次へ進みます。

時系列メモの様式

書き方

- ・1行に、時刻と出来事を1つだけ書きます
- ・見たことと、推測したことを分けます。推測には「推測」と付けます
- ・最後に「分かっていないこと」を並べます

11/24 (月)

⋮

分かっていないこと

図8：時系列メモの様式

時系列メモ (記入例)

11/24 (月)
02:14 VPN接続の記録に、委託先の保守アカウントでのログインが残っている(遠征で、予定にない)
08:40 経理担当のパソコン(PC-AE1312-45)で、共有フォルダのファイル名の末尾が「locked」に変わっているのに本人が気づく
08:41 デスクトップに、README.txtが置かれているのを確認(身代金を求める文面)
08:52 120が「ランサムウェアの支払い」の要求を出す(端末 PC-AE1312-45)
08:55 本人がVPNケーブルを抜き、Wi-Fiを切る。電源は入れたまま
09:00 本人が上長と情報システム部の窓口へ電話で連絡
09:20 情報システム部が、共有フォルダ「顧客台帳」への読み出しの記録を確認。取引先の担当者約2,300人分の氏名、電話番号、メールアドレスが入っている
09:30 情報システム部が、委託先の保守アカウントを停止

分かっていないこと
・顧客台帳のデータが外へ持ち出されたかどうか
・PC-AE1312-45のほかに感染した端末があるか
・攻撃者が誰か

図9：記入例。推測には「推測」と付け、分かっていないことを最後に並べています

ここまでできたら

- ☐ 分かっていないことを3つ以上書いた
- ☐ 推測の行に「推測」と付けた

STEP 4

Geminiで第一報の下書きを作る

[7min]

時系列メモだけをGeminiに渡し、経営層へ送る第一報を作らせます。項目は、配布の第一報の6項目.txtと同じ6つです。

Geminiに送る文面

コピーしてGeminiの入力欄に貼ります

あなたはA社の情報システム部の担当者です。次の時系列メモをもとに、社内の経営層へ送る第一報を作ってください。項目は、攻撃の種類、判明している範囲、影響、初動対応、外部への報告の状況、二次被害の相談先の6つです。メモに書いていないことは推測で埋めず、「調査中」と書いてください。

<ここに、自分の時系列メモか 時系列メモ_記入例.txt を貼り付けます>

- 1 文面をコピーして、Geminiの入力欄に貼ります。

2

<ここに…> の行を消し、自分の時系列メモか記入例を貼って送ります。

3

返ってきた第一報が、6項目に分かれているかを確認めます。

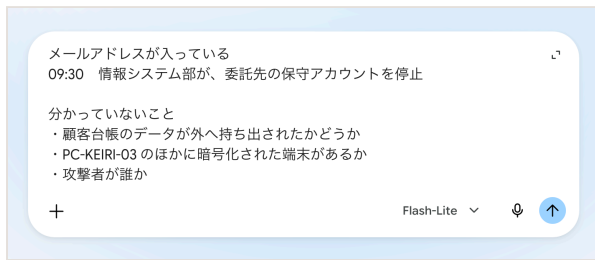


図10：文面と時系列メモを貼り付けたところ

A社の情報システム部より、経営層の皆様へ向けたセキュリティインシデントに関する第一報をご報告いたします。

ご提示いただいた時系列メモに基づき、以下の通り状況をまとめました。メモに記載のない事項につきましては、現時点では推測で補わず「調査中」としております。

セキュリティインシデントに関する第一報

1. 攻撃の種類
 - ランサムウェアによる攻撃（疑い）および不正アクセスの可能性
 - （根拠：EDRによる「ランサムウェアの疑い」の警告、身代金を求める文面のファイル「README_RESTORE.txt」の確認、および予定外の保守アカウントによるVPNログインの検知）
2. 判明している範囲
 - 該当端末：経理担当のパソコン（PC-KEIRI-03）にて、共有フォルダのファイル名末尾が「.locked」に変更され、暗号化されていることを確認。
 - アクセス記録：共有フォルダ「顧客台帳」への読み出し記録を確認（取引先の担当者約2,300人分の氏名、電話番号、メールアドレスが含まれています）。

図11：時系列メモの記入例から作られた第一報の冒頭

ここまでできたら

- ☐ 第一報が6項目に分かれている

STEP 5 メモにない言い切りを点検する

[7min]

Geminiの下書きには、メモにないことや、分かっていないのに言い切った文が混ざります。Geminiと自分の両方で点検します。

Geminiに送る文面

コピーしてGeminiの入力欄に貼ります

いま作った第一報の中で、時系列メモに書いていない内容と、メモでは分かっていないのに言い切っている文を抜き出して、一覧にしてください。あいさつの文は除いてください。なければ「なし」と書いてください。

1

同じチャットで、文面をコピーして送ります。

2

Geminiが挙げた一覧を読みます。

3

第一報を自分でも読み、時系列メモの記述と1文ずつ照らし合わせます。

4

見つけた言い切りを、「調査中」や「推測」に直します。

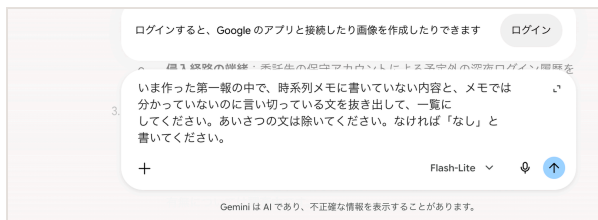


図12：STEP 4の続きのチャットに、点検の文面を貼り付けたところ

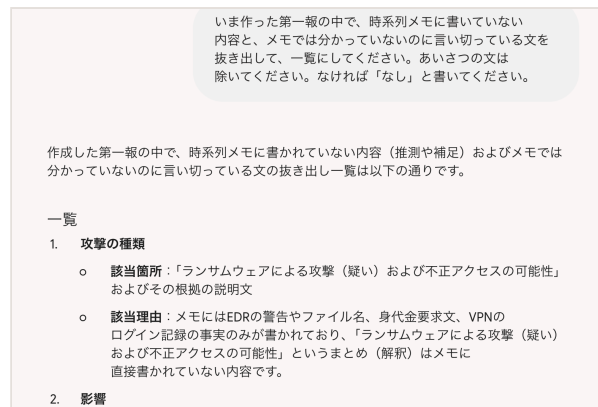


図13：Geminiが自分の下書きを点検した結果

AIの点検をすり抜けた言い切り 講師が試したとき、Geminiは「侵入経路の端緒」として委託先の保守アカウントのログインを書きました。時系列メモでは、予定にない深夜のログインがあったことしか分かっていません。この文は、Geminiの点検の一覧にも出ませんでした。

ここまでできたら

- ☐ メモにない言い切りを、自分で1つ以上見つけて直した

STEP 6 報告の期限を確かめる

[6min]

顧客台帳の個人情報が漏えいしたおそれがあるときは、個人情報保護委員会への報告が要ります。期限を公式のページで確かめます。

- 1 個人情報保護委員会の 漏えい等の対応とお役立ち資料 を開きます。
- 2 速報の期限が、気づいた時点からおおむね3～5日以内であることを確かめます。
- 3 03_報告文/報告の期限早見表.txt で、確報の期限と、報告の対象になる4つの類型を読みます。



図14：個人情報保護委員会のページ。速報は3～5日以内と案内されています

報告の期限早見表（2026年10月時点）

個人情報保護法（個人情報保護委員会への報告）

対象 次の4類型のどれかに当たる漏えい、またはそのおそれ

- ・要配慮個人情報が含まれる
- ・財産的な被害が生じるおそれがある
- ・不正の目的によるおそれがある（不正アクセスやランサムウェアはここに入る）
- ・本人の数が1,000人を超える

速報 事態を知った時点から、おおむね3～5日以内、会社のどこかの部署が知った時点から数える

確認 30日以内、不正の目的によるおそれがある事態は60日以内

出典 <https://www.ppc.go.jp/personalinfo/legal/LeakAction/>

サイバー対処能力強化法（2026年10月1日施行。基幹インフラ事業者が対象）

速報 ランサムウェアなどのサイバー攻撃は3～5日以内

確認 30日以内

出典 https://www.cyber.go.jp/pdf/press/siryou_20260930.pdf

警察への相談

最寄りの警察署か、都道府県警察のサイバー犯罪相談窓口

出典 <https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html>

図15：報告の期限早見表。確認は30日以内、不正の目的によるおそれがあれば60日以内です

ここまでできたら

- ☐ 速報と確認の期限を言える

ここまでが必須です

STEP 1～6が終わると、この演習の必須はすべて済みます。ここから先は発展で、時間が残った方と、研修のあとに続ける方が進めてください。

STEP 7 速報の対象かをGeminiと考える

発展

この事案が、個人情報保護委員会への速報の対象かを考えます。STEP 4と同じチャットで続けます。

Geminiに送る文面

コピーしてGeminiの入力欄に貼ります

この事案で、個人情報保護委員会への速報が必要かどうかを、判断の理由とともに説明してください。報告の対象になる4つの類型に当てはめて考えてください。

1 同じチャットで、文面をコピーして送ります。

2 Geminiの答えを、**報告の期限早見表.txt** の4つの類型と照らし合わせます。

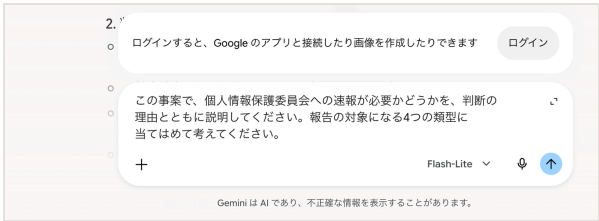


図16：続きのチャットに文面を貼り付けたところ

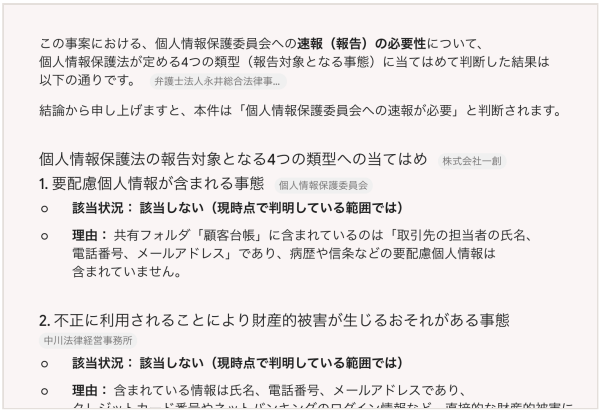


図17：Geminiは法律事務所などのサイトを根拠に挙げることがあります。最後は早見表と公式のページで確かめます

職場のチェック表

演習のあとに、自分の職場で確かめる8項目を、配布フォルダの **04_持ち帰り/職場のチェック表.xlsx** にまとめています。分からない項目を1つ選び、確かめる相手に聞いてください。危ない点に気づいたら、同じフォルダの **職場に相談するときのメモ.txt** に整理して、派遣先の指揮命令者か上長に相談します。表もメモも提出しません。

No	確かめること	状態（できている、一部、できていない、分からない）	確かめる相手	メモ
1	インターネットに出ているVPN機器などの一覧があり、更新を当てているか		情報システム部	
2	社外から入るアカウントと管理者のアカウントに、例外なく多要素認証がかかっているか		情報システム部	
3	委託先に渡しているアカウントの一覧があり、使っていないものを止めているか		情報システム部	
4	バックアップを、ネットワークから切り離れた場所にも保管しているか		情報システム部	
5	端末とネットワーク機器の記録を、1年以上残しているか		情報システム部	
6	生成AIの利用ルールがあり、使ってよいサービスが決まっているか		上長、派遣元	
7	パスワードの再設定を頼まれたときの、本人確認の手順が決まっているか		ヘルプデスク	
8	インシデントに気づいたときの連絡先を、紙でも持っているか		上長	

図18：職場のチェック表。D列に、確かめる相手を書いています

この演習とセキュリティの仕事

今日やったこと	セキュリティの現場での仕事	担う人
最初の1時間の行動を選んだ	被害の広がりを止め、証拠を残す初動を指揮する	CSIRT、インシデント対応の担当者
時系列メモを作った	記録から何がいつ起きたかを組み立て、原因を調べる	フォレンジックの調査員
第一報を作った	経営層、当局、取引先へ、事実だけを期限内に伝える	CSIRT、広報、法務

Geminiの第一報が6項目に分かれていません

続けて「6つの項目の見出しを付けて書き直してください」と送ってください。

05

よくある質問

Geminiの画面に、ログインを求める表示が出ます

ログインしなくても、入力欄に貼り付けた文面は送れます。「ログイン」のボタンは押さずに進めてください。Googleアカウントでログインしている方は、そのまま使って構いません。

Geminiの返事が、ガイドの写真と違います

Geminiの返事は、送るたびに少しずつ変わります。写真と同じ文になっているかではなく、STEPの「ここまでできたら」に書いた項目がそろっているかを見てください。

会社のパソコンでGeminiが開けません

常駐先や派遣元の設定で、生成AIのサイトが止められていることがあります。私物のパソコンかスマートフォンでGeminiを開くか、講師の画面を見ながら紙に答えを書いて進めてください。

配布フォルダのファイル名が、読めない文字になっています

WindowsとMacのZIPを取り違えています。展開したフォルダを消して、お使いのパソコンに合う方のZIPを教材サイトからダウンロードし直してください。

Excelが入っていません

配布のxlsxファイルは、GoogleスプレッドシートやNumbersでも開けます。紙に番号と答えを書いて進めても構いません。

書いたシートを講師に見てもらえますか

提出の仕組みはありません。自分のアカウントの守りのように自分だけのことなら、ZOOMのチャットで質問できます。職場の情報が入ったシートは、講師にも送らないでください。迷ったときは、派遣先の指揮命令者か上長に相談してください。

