1｜まず、何が起きた設定か読む

会社・人物・時刻・対応経過はすべて架空です。自社の連絡先と権限に置き換えて使用してください。

一度で全部埋める必要はありません。この3ページは、異変→第一報→記録交代を具体例でつなぐ教材です。

会社と画面の設定

従業員8人の受注会社。専任IT担当はいません。顧客管理サービスに、顧客の氏名・連絡先・受注内容を保存しています。発見者Cは通常業務で画面を閲覧できます。操作履歴のアカウント欄には「受注担当用」と表示されています。画面の時刻は日本時間（JST）という設定です。

役割は、この教材で決めた設定

発見・最初の記録：C	見えた事実と自分の操作を記録し、社長Aへ伝える。
決める人：社長A	この例では対応範囲・業務制限・外部依頼を決める権限を事前に指定。実際の会社で肩書きから権限を推測しない。
技術確認先：保守会社B／担当D	ログ保全・技術確認の対応可否を確認する窓口。受付だけでは、調査や操作の実施済みを意味しない。
記録を引き継ぐ人：E	17:25にCから記録を受け取り、未完了作業と回答を追記する。決定権や操作権限は引き継がない。
Aが不在のときの代行者	未定。実際の会社では平時に経営者と決め、権限・代行条件・連絡先を記入する。

17:10にCが見たこと・したこと

画面で見えた異変	操作履歴に17:04「ログイン成功」、17:05「データ出力」。Cには見慣れない記録だった。
まだ分からないこと	操作した人物、出力された内容、外部流出の有無、影響人数。社内の正規操作かどうかも未確認。
Cが行った操作	17:10に表示画面を保存。設定変更・ログ削除・再起動はしていない。
保存先も架空の設定	社内のアクセス制限付き記録フォルダ「訓練用事案01」に「証跡01_操作履歴画面」を保存。実在フォルダではない。

最初の連絡は4点だけ

「17:10／顧客管理画面／見慣れない成功ログインとデータ出力／画面を保存、設定変更なし」。まずこれをAへ伝え、残りは未確認で構いません。連絡先は役名だけの架空設定です。実際に使う前に、確認済みの連絡方法を用意します。

2｜第一報の「どこに何を書くか」

会社・人物・時刻・対応経過はすべて架空です。自社の連絡先と権限に置き換えて使用してください。

初動対応マニュアルPDFの3ページの9欄に対応する記入見本です。上から完成させてから連絡する必要はありません。下の時刻・依頼・受領も、すべて架空の設定です。

件名

【訓練用・状況確認依頼】顧客管理画面の見慣れないログイン・データ出力

発見日時・タイムゾーン／発見者・折り返し先

訓練日 17:10 JST（日本時間）。発見者C。折り返し先：Cの社内連絡先（役名のみの設定）。

対象の端末・アカウント・サービス・URL

対象：顧客管理サービスの操作履歴画面。記録上のアカウント：受注担当用。実際の操作者は未確認。端末・URLは設定なし。

確認した事実

17:10、Cが操作履歴を確認。17:04「ログイン成功」、17:05「データ出力」の表示を発見。Cには見慣れない記録だった。不正操作と断定していない。

根拠となる画面・通知・ログの保管先

証跡01：17:10に保存した操作履歴画面。保管先：アクセス制限付き「訓練用事案01」。原ログは未取得。

実施済みの操作・実施者・時刻

C：17:10に画面を保存。設定変更・ログ削除・再起動なし。17:11に社内連絡でAへ状況確認を依頼した設定。

現在の業務影響

この時点では業務への影響は未確認。サービス停止・制限は実施していない。業務を続けて安全かどうかも未確認。

まだ分からないこと／依頼したい対応

未確認：操作者、出力内容、外部流出、人数。Aへ：対応方針と保守会社Bへの確認依頼を判断してほしい。

受領した責任者・受領時刻／次の状況確認時刻

Aが17:12に受領した設定。17:30に状況共有を希望。作業完了・回答時刻の確約ではない。実際の次回確認時刻は相手と調整して記録。

> **迷ったら「見たこと」と「推測」を分ける**
>
> 見たこと＝画面の表示とCの操作。分からないこと＝操作者・出力内容・外部流出・人数。未確認の欄を空欄にせず「未確認」と書けば、次に調べる対象が残ります。

3｜技術確認と、記録の引き継ぎを分ける

会社・人物・時刻・対応経過はすべて架空です。自社の連絡先と権限に置き換えて使用してください。

追加の架空設定：AがBへ確認を依頼し、担当Dが17:18に受付。調査・設定変更等の操作はまだ実施されていません。17:25にCからEへ記録を交代します。

> **Dには技術確認を頼む。Eには記録の続きを渡す**
>
> 同じ「引き継ぎ」でも目的が違います。D＝ログ保全・技術確認の対応可否を回答する人。E＝事実・未確認事項・担当・回答状況の記録を続ける人。A＝判断を担う人。

事案の名称・管理番号／引き継ぎ日時・時差

訓練用事案01：顧客管理画面の見慣れない操作記録。記録交代：訓練日17:25 JST。

前任者・後任者／安全な連絡方法

前任C→記録担当E。社内の確認済み連絡先を使う設定。連絡先の実値は設定なし。

確認済みの事実と根拠

17:04ログイン成功・17:05データ出力の表示をCが17:10に確認。証跡01は「訓練用事案01」。Dは17:18受付、操作は未実施。

不明点と次に必要な確認

操作者・出力内容・外部流出・人数は未確認。Dがログ保全と調査の対応可否を確認、Aが業務制限・依頼範囲を判断、Eが回答を追記する設定。

隔離・停止・制限中の対象／継続業務・代替手段

隔離・停止・制限は未実施。継続可能な業務と代替手段も未確認。Aの判断待ち。

実施済み操作と結果／記録の保管先

Cが17:10画面保存。設定変更なし。17:11 Aへ依頼、17:12 A受領。事案記録と証跡01を同じ制限付きフォルダでEへ渡す設定。

外部連絡・法定報告・本人通知・公表の状況と期限

B／Dへ技術確認を依頼し受付済み。法定報告・本人通知・公表の要否と期限は未判断。Aが事実を集め、必要な相談先と確認する未完了作業。

再開の判断者・確認条件／再停止する条件

再開判断は未実施。停止もまだない。判断者はこの設定ではA。確認条件・制限条件はDの技術回答等を受けて決める。安全と断定しない。

受領確認／次の状況確認時刻・連絡方法

Eが17:25に記録を受領する設定。次は17:30の状況共有を希望（完了確約ではない）。A・Dへ社内連絡／保守窓口で調整し、確定後に追記。

> **平時に決めることは、まず3つ**
>
> ①判断する人と不在時の代行条件 ②使える技術窓口と連絡方法 ③記録の保存先と交代する人。未定のものは「未定」と残して経営者と決めます。まずは、この3点について自社の決定事項と未定事項を確認してください。