Securiy セキュリー

01 医療機関（病院・クリニック）・全13ページ

業種別 検証シーン集

病院・クリニック向け検証シーン集

患者向けWebの本人以外への到達・院内AIツールからの持ち出し・誤記録・電子カルテ連携・委託先経由の変更を検証する

USE CASES ／ FOR HOSPITALS & CLINICS

FOR HOSPITALS & CLINICS

攻撃者が AI で自動化する「権限の抜け探し」を、先に試して直す。

攻撃者は AI を使い、公開 API・画面の通信・JavaScript から操作を洗い出し、ID やロールを組み合わせて自動で試します。狙われるのは、スキャナーが拾いにくい「権限の抜け」です。 この冊子は、医療機関（病院・クリニック）の3シーン（患者向けWebの本人以外への到達・院内AIツールからの持ち出し・誤記録・電子カルテ連携・委託先経由の変更）について、原因・自社での確かめ方・修正の方向まで掘り下げたものです。

「AIを使った攻撃」で想定する2つ

1

攻撃者が AI で自動化する、権限の抜け探し

他社・他人のデータに届く経路、承認を迂回する経路、上限を超える経路を、AI が組み合わせで試す。

2

貴院の AI 機能への誘導と乗っ取り

チャット・エージェント・RAG に仕込んだ指示で、本人の権限を超えた回答や操作をさせる。

こんな兆候があれば、対象です

Web予約・問診・オンライン診療を外部サービスで導入したが、設定は提供事業者に任せている

予約番号やIDを変えると他の患者さんの情報が見えないか、誰も試していない。

カルテ要約・音声入力・文書作成にAIを使い始めた

他の患者さんの情報が混ざって出てこないか、誤った内容が記録に入らないかを確認する手順がない。

近隣の医療機関のサイバー被害を聞いて、理事会や監査で対策を聞かれた

ガイドラインのチェックリストはあるが、実際に試した結果を示せない。

対象: 病院・クリニックの院長・事務長・医療情報（システム）担当の方へ

MAP

3シーンの RULE を、貴院の条件に置き換えて読む

どのシーンも、RULE（守るべき条件）／CHECK（試す操作）／EVIDENCE（記録するもの）の同じ枠です。CHECK の操作を貴院の画面・APIに当てはめてください。

シーン	RULE ／ 守るべき条件	CHECK ／ 試す操作	EVIDENCE ／ 記録するもの	ページ
01 **患者向けWebの本人以外への到達**	患者は本人の、職員は担当範囲の情報だけを扱える	IDの差し替え、URLの推測、受付・一括表示の悪用	到達の可否、再現手順、修正後に拒否されること	P.05
02 **院内AIツールからの持ち出し・誤記録**	AIの回答・入力は、操作する職員の権限と承認の範囲に限る	誘導文の注入、参照文書の汚染、自動入力の乗っ取り	漏えい・越権の可否、モデル別の結果、未実施の経路	P.07
03 **電子カルテ連携・委託先経由の変更**	記録の変更は承認を経た操作だけが通り、閲覧は記録される	連携APIの直接呼び出し、保守用IDの悪用、ログ回避	改ざん・閲覧の可否と、通常の診療業務が止まらないこと	P.09

初回スコープ　1アプリ・1検証環境・2操作、準備完了後10営業日。1操作は、1つの業務操作（例: 返金、ロール変更）と、それにつながる API・画面の一式です。 どの2操作から始めるかは P.11 へ。

WITH YOUR CURRENT STACK

WAF と診断が通す「正しい形式の不正な要求」を、業務ロジックの層で止める

WAF・診断で既に見ている範囲は対象から外します。下の表の右列だけが、共同検証で追加する範囲です。



既存の対策	担う範囲	共同検証で足すもの
ネットワーク分離・端末管理・バックアップ	接続元・端末の制限と、被害時の復旧	接続できる人（患者・職員・提供事業者）の中での越権・越境（他の患者の情報、確定後の変更）が成立しないことの検証
医療情報システムの安全管理に関するガイドラインのチェックリスト	要件の整理と自己点検	項目ごとに「試した記録」を添えられる状態にすること
提供事業者が行う脆弱性診断	決めた期間に広い範囲を調べ、指摘を出す	指摘の修正案づくりと再検証、患者・職員権限の業務ルールの検証、再実行できるテストの作成

SCENE 01 ／ 患者向けWebの本人以外への到達 ／ OWASP API1 BOLA

予約・問診・結果照会で、他の患者さんの情報に届かないか。

RULE 「患者は本人の、職員は担当範囲の情報だけを扱える」

VERIFICATION LOG ／ PATIENT DATA / ACCESS CONTROL　SAMPLE

時刻	操作者	対象	経路	修正前	修正後
10:02	**患者本人**	自分の予約・結果	通常の取得	許可	許可
10:05	**患者本人**	他の患者の情報	IDの差し替え	拒否	拒否
10:11	**患者本人（別端末）**	他の患者の情報	URLの推測	到達	拒否
10:18	**外部連携（APIキー）**	他の患者の情報	受付・一括表示の悪用	到達	拒否
10:24	**患者本人**	他の患者の情報	IDの差し替え	到達	拒否

他の患者さんの情報へ、アクセスできないことを確認。

想定リスク

患者・家族・受付それぞれの立場で、予約番号やIDの差し替え、問診票や検査結果のURLの推測、受付画面からの一括表示を試し、本人以外の情報に到達できないことを確認します。

CHECK ／ 試す操作

- IDの差し替え
- URLの推測
- 受付・一括表示の悪用

EVIDENCE ／ 記録するもの

- 到達の可否
- 再現手順
- 修正後に拒否されること

SCENE 01 ／ 患者向けWebの本人以外への到達

予約番号・患者IDを、本人のログインと照合していない

相談の前にここまで確かめておくと、初回の2操作がすぐ決まります。手順は検証環境・テストアカウントで行ってください。

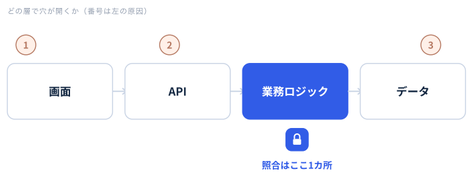
No.	自社で確かめる手順（検証環境で）	期待する結果	自社の結果
1	テスト患者を2人作り、Aでログインしたまま予約番号をBのものに変えて開く	拒否される	☐ 到達　☐ 拒否
2	問診票・結果のURLの末尾を1つ変えて開けないか試す	開けない	☐ 到達　☐ 拒否
3	受付アカウントで、担当外の日付・診療科の患者一覧が出ないか確認する	担当範囲だけ表示される	☐ 到達　☐ 拒否

よくある原因

① 予約番号や患者IDをURLやリクエストで受け取り、ログイン中の本人と照合していない

② 問診票・検査結果のURLが推測しやすく、ログインなしで開ける

③ 受付画面の一覧・検索・印刷機能が、担当範囲を超えて全患者を表示できる



修正の方向

予約番号・患者IDは、ログイン中の本人（家族の代理は同意・期限つき）とサーバー側で照合してから使う。URLは推測不能にし、ログインを必須にする。受付の一覧・印刷も同じ共通層を通す。

共同検証では、患者・家族・受付の組み合わせを AI で洗い出し、予約・問診・結果照会・印刷の全経路で到達を試します。修正は提供事業者と範囲を合意して進めます。

SCENE 02 ／ 院内AIツールからの持ち出し・誤記録 ／ OWASP LLM01 ／ LLM02 ／ LLM06

AIが、他の患者さんの情報を出したり、記録に混ぜたりしないか。

RULE 「AIの回答・入力は、操作する職員の権限と承認の範囲に限る」



想定リスク

カルテ要約・音声入力・文書作成に使うAIに対し、誘導文の注入や参照文書の汚染を試し、他の患者さんの情報を回答しないか、権限や承認を超えた記録の自動入力が起きないかを複数モデル・手順で確認します。

CHECK ／ 試す操作

- 誘導文の注入
- 参照文書の汚染
- 自動入力の乗っ取り

EVIDENCE ／ 記録するもの

- 漏えい・越権の可否
- モデル別の結果
- 未実施の経路

SCENE 02 ／ 院内AIツールからの持ち出し・誤記録

AIが院内全体の記録を参照し、確認なしに入力している

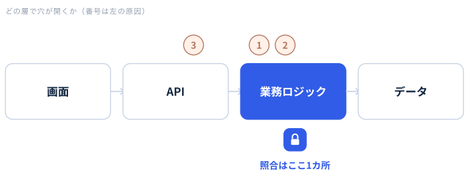
No.	自社で確かめる手順（検証環境で）	期待する結果	自社の結果
1	他の患者の記録に固有の文字列を入れ、担当患者の質問でその文字列が回答に出ないことを確かめる	文字列が一切出ない	☐ 到達 ☐ 拒否
2	AIの自動入力が確認なしに確定するか試す	職員の確認を経てから確定する	☐ 到達 ☐ 拒否
3	自由記述欄に指示文を入れて挙動を見る	実行されない	☐ 到達 ☐ 拒否

よくある原因

① AIが院内全体の記録を参照でき、操作中の職員が閲覧を許されていない患者の情報を回答・入力する

② AIの要約・自動入力に、職員の確認・承認のステップが無い

③ 問診の自由記述や外部文書に仕込まれた指示をAIが実行する



修正の方向

AI が参照できるのは、操作中の職員が閲覧を許された患者の記録だけにする。入力は職員の確認を経て確定する。

共同検証では、複数のモデル・手順で誘導文を試し、どの経路で何が出たかをモデル別に記録します。

SCENE 03 ／ 電子カルテ連携・委託先経由の変更 ／ OWASP API5 BFLA ／ API6

連携システムや保守用の経路から、記録を変更・閲覧できないか。

RULE 「記録の変更は承認を経た操作だけが通り、閲覧は記録される」

APPROVAL MATCH ／ RECORD INTEGRITY / VENDOR ACCESS

SAMPLE

承認画面

申請者	起票者
要求	連携先からの変更
対象	承認時の内容
承認者	権限のある担当者

承認

照合

EXECUTE REQUEST ／ diff

承認ID: #A-1042

要求: 連携先からの変更

- 対象: 承認時の内容

+ 対象: 承認後に書き換え

× 不一致 → 実行しない

一致した要求だけが実行される: 承認済みの変更

承認のない変更は、実行しない。閲覧は記録する

想定リスク

予約・検査・会計システムと電子カルテの連携API、保守用の接続を対象に、確定済み記録の書き換え、閲覧ログを残さない取得、連携先IDを使った越権を試し、承認と記録が迂回されないかを確認します。

CHECK ／ 試す操作

- 連携APIの直接呼び出し
- 保守用IDの悪用
- ログ回避

EVIDENCE ／ 記録するもの

- 改ざん・閲覧の可否と
- 通常の診療業務が止まらないこと

SCENE 03 ／ 電子カルテ連携・委託先経由の変更

連携・保守の経路に、権限と履歴の制約が無い

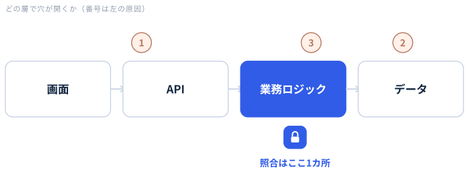
No.	自社で確かめる手順（検証環境で）	期待する結果	自社の結果
1	連携用の資格情報で、確定済みの記録を更新できるか試す	拒否される	☐ 到達　☐ 拒否
2	保守用IDでの操作が、個人を特定できる形でログに残るか確認する	操作者・日時が残る	☐ 到達　☐ 拒否
3	他部門の記録を開いた操作がログに残るか見る	ログに残る	☐ 到達　☐ 拒否

よくある原因

① 予約・検査・会計システムとの連携APIが、ステータスと権限を確認せず記録を変更できる

② 保守用のIDが共用で、誰が操作したか残らない

③ 閲覧ログが無く、権限外の閲覧に気づけない



修正の方向

連携APIは変更できる項目と状態を限定し、確定後の訂正は承認付きの経路に限る。保守用IDは個人ごとに分け、訂正前の値・訂正者・日時を消せない形で残す（真正性）。〔要確認: 提供事業者の保守契約と合わせる〕

共同検証では、連携先・保守経路ごとに誰が何をできるかを表にし、経路を横断して試します。

FIRST 2 OPERATIONS

初回の2操作は、影響の広さと、10営業日で一巡できるかで選ぶ

当社が推奨する順です。順番は相談で入れ替えられます。1操作は、1つの業務操作（例: 返金、ロール変更）と、それにつながる API・画面の一式です。



1

患者向けWebの本人以外への到達

患者向けWebは外から誰でも触れる経路で、影響が最も大きい。予約番号・IDの照合は経路が少なく、10営業日で一巡できる

2

電子カルテ連携・委託先経由の変更

連携・保守経路からの変更は発覚が遅れ、診療と請求の両方に影響する。確定後の変更経路は数が少ない

次回以降

院内AIツールからの持ち出し・誤記録 — 院内AIツールは、導入済みなら2操作目と入れ替えられます。

CHECK SHEET

6つの欄を埋めれば、初回の2操作はほぼ決まる

印をつけた状態でご相談いただくと、30分で初回スコープと費用の出し方まで決められます。

Q1

守りたいデータ

☐ 患者さんの個人情報・診療情報
☐ Web予約・問診・オンライン診療
☐ 院内で使うAIツール
☐ その他（　　）

Q2

気になる操作

☐ IDの差し替え
☐ URLの推測
☐ 誘導文の注入
☐ 参照文書の汚染
☐ その他（　　）

Q3

権限の種類

☐ 患者・家族
☐ 受付・事務
☐ 医師・看護師
☐ 医療情報担当
☐ 提供事業者（保守）
☐ その他（　　）

Q4

既存の対策

☐ ネットワーク分離・端末管理・バックアップ
☐ 医療情報システムの安全管理に関するガイドラインのチェックリスト
☐ 提供事業者が行う脆弱性診断
☐ その他（　　）

Q5

検証環境の有無

☐ 検証環境がある
☐ これから用意する
☐ その他（　　）

Q6

提出先・期限

提出先: _____　期限: ____／____

チェックシートに印をつけて、30分の無料相談へ。

守りたいデータと気になる操作が分かれば、初回に検証する2操作と環境を一緒に決められます。本番の認証情報や実データは不要です。

Securiy は Tempura technologies株式会社のセキュリティ事業です。

記載の検証シーンは共同検証のテーマ例で、業界別の導入実績・認証取得を示すものではありません。対象は、検証と修正を行える自社アプリ・独自APIです。

FREE CONSULTATION

30分無料相談を予約する

チェックシート（P.12）の内容をもとに、初回スコープと費用の出し方をご説明します。

予約ページへ →

SET

02 プログラムのご案内 ／ 03 検証記録の作り方

対象・期間・費用・体制は 02、記録の残し方と提出先への説明は 03 へ。