■モバイルアプリケーション診断項目表

Ver1.00

概要	No	診断項目	小項目	Android					iOS					MASVS			owasp-mobile
				ツール診断	手動診断	API診断	静的解析	動的解析	ツール診断	手動診断	API診断	静的解析	動的解析	L1	L2	R	TOP10
データ・ストレージの保護	1	ローカルストレージ	外部ストレージの読み取り/書き込み権限が無効か	○	-	-	-	-	-	-	-	-	-	○	○	-	M2
	2	ローカルストレージ	データの保存に使用されるキーワードとAPI 呼び出しのソースコードが適切か（SharedPreferencesが適切か）	△	○	-	-	-	-	-	-	-	-	○	○	-	M2
	3	ローカルストレージ	データの保存に使用されるキーワードとAPI 呼び出しのソースコードが適切か（ファイルアクセスの許可が適切か）	△	○	-	-	-	-	-	-	-	-	○	○	-	M2
	4	ローカルストレージ	データの保存に使用されるキーワードとAPI 呼び出しのソースコードが適切か（外部ストレージを使用していないか）	△	○	-	-	-	-	-	-	-	-	○	○	-	M2
	5	ローカルストレージ	XORやビット反転などの単純なビット操作の暗号化を使用していないか	-	○	-	○	-	-	-	-	-	-	○	○	-	M2
	6	ローカルストレージ	Androidオンボード機能を使用せずに使用されたキーがないか	-	○	-	○	-	-	-	-	-	-	○	○	-	M2
	7	ローカルストレージ	ハードコーディングによって公開されるキーがないか	△	○	-	○	-	○	-	-	-	-	○	○	-	M2
	8	ローカルストレージ	アプリケーションによって作成された機密データを含むファイルがないか（一時ファイルの使用）	○	-	-	-	-	-	-	-	-	-	○	○	-	M2
	9	ローカルストレージ	アプリケーションによって作成された機密データを含むファイルがないか（一時ファイルの使用）	-	○	-	-	○	-	-	-	-	-	○	○	-	M2
	10	ローカルストレージ	ソリューズに含めるべきではないファイルがないか	-	○	-	-	○	-	-	-	-	-	○	○	-	M2
	11	ローカルストレージ	SQLiteデータベースに機密情報が含まれていないか	-	○	-	-	○	-	-	-	-	-	○	○	-	M2
	12	ローカルストレージ	SQLiteデータベースが暗号化されているか	△	○	-	-	○	-	-	-	-	-	○	○	-	M2
	13	ローカルストレージ	XMLファイルに保存されている共有設定に機密情報がないか	-	○	-	-	○	-	-	-	-	-	○	○	-	M2
	14	ローカルストレージ	ファイルアクセスの権限が適切か	-	○	-	-	○	-	-	-	-	-	○	○	-	M2
	15	ローカルストレージ	Firebaseリアルタイム データベースの構成が適切か	-	○	-	-	○	-	-	-	-	-	○	○	-	M2
	16	ローカルストレージ	Realmデータベースが暗号化されているか、機密情報が含まれていないか　（暗号化したrealmデータベースを使用しているか）	△	○	-	-	-	-	-	-	-	-	○	○	-	M2
	17	ローカルストレージ	機密情報をキーチェーンに適切に保存しているか（ファイルパスの管理が適切か）	-	-	-	-	-	△	○	-	○	-	○	○	-	M2
	18	ローカルストレージ	機密情報をキーチェーンに適切に保存しているか（キーチェーンを使用しているか）	○	-	-	-	-	-	○	-	○	-	○	○	-	M2
	19	ローカルストレージ	機密情報をキーチェーンに適切に保存しているか	-	-	-	-	-	-	○	-	○	-	○	○	-	M2
	20	ローカルストレージ	データをローカルに保存する際のAPIは適切か（データベースの検出）	-	-	-	-	-	△	○	-	○	-	○	○	-	M2
	21	ローカルストレージ	データをローカルに保存する際のAPIは適切か（アクセス期限が適切か）	-	-	-	-	-	△	○	-	○	-	○	○	-	M2
	22	ローカルストレージ	データをローカルに保存する際のAPIは適切か	-	-	-	-	-	-	○	-	○	-	○	○	-	M2
	23	ローカルストレージ	ネイティブiOS機能を利用していない場合に機密情報が適切に保存されているか	-	-	-	-	-	-	○	-	-	○	○	○	-	M2
	24	ローカルストレージ	アプリがダイレクトブートに対応	△	○	-	○	-	-	-	-	-	-	○	○	-	M2
	25	デバイスアクセスポリシー	ポリシーを実装するコードが適切か	-	○	-	○	-	-	-	-	-	-	-	○	-	M2
	26	デバイスアクセスポリシー	ポリシーを無効にできないか	-	○	-	-	○	-	-	-	-	-	-	○	-	M2
	27	メモリ	機密データは最小限のコンポーネントで処理されているか	-	○	-	○	-	-	○	-	○	-	-	○	-	M2
	28	メモリ	オブジェクト参照が適切に開放されているか	-	○	-	○	-	-	○	-	○	-	-	○	-	M2
	29	メモリ	参照が開放された後にガベージ コレクションが要求されているか	-	○	-	○	-	-	-	-	-	-	-	○	-	M2
	30	メモリ	機密データは不要になったらすぐに上書きしているか（非表示にしているビューはないか）	△	○	-	○	-	-	○	-	○	-	-	○	-	M2
	31	メモリ	プロセスからの参照が適切か	-	○	-	-	○	-	○	-	-	○	○	○	-	M2
	32	メモリ	機密データは不要になったらすぐに上書きしているか	-	-	-	-	-	-	○	-	○	-	-	○	-	M2
	33	メモリ	機密データを不変なデータ型で使用していないか	-	-	-	-	-	-	○	-	○	-	-	○	-	M2
	34	メモリ	非プリミティブデータ型を使用していないか	-	-	-	-	-	-	○	-	○	-	-	○	-	M2
	35	メモリ	参照を開放する前にメモリ内の値を上書きしているか	-	-	-	-	-	-	○	-	○	-	-	○	-	M2
	36	メモリ	サードパーティのコンポーネントが適切か（適切か）	-	-	-	-	-	-	○	-	○	-	-	○	-	M2
	37	サードパーティ	通知の作成に関連する関数が適切か	-	○	-	○	○	-	-	-	-	-	○	○	-	M2
	38	サードパーティ	サードパーティライブラリによって提供されるAPI 呼び出しと関数が適切か	-	○	-	○	-	-	○	-	○	-	○	○	-	M2
	39	サードパーティ	外部サービスのすべてのリクエストで機密情報が埋め込まれていないか	-	○	-	-	○	-	○	-	-	○	○	○	-	M2
	40	ログ	ログを生成するコードが適切か	-	○	-	○	-	-	○	-	○	-	○	○	-	M2
	41	ログ	システムメッセージとログファイルに機密情報がないか（ログファイルを使用しているか）	△	○	-	○	○	△	○	-	○	○	○	○	-	M2
	42	キーボード	機密情報を入力する際にキーボードキャッシュを使用していないか（キーボードキャッシュを使用していないか）	-	○	-	○	○	△	○	-	○	○	○	○	-	M2
	43	キーボード	カスタムキーボードを使用しているか※当所はMobif	-	○	-	○	-	△	○	-	○	○	○	○	-	M2
	44	バックアップ	アプリのバックアップが無効になっているか	△	○	-	○	-	-	-	-	-	-	-	○	-	M2
	45	バックアップ	クラウドに送信されるファイルが適切か	-	○	-	○	-	-	-	-	-	-	-	○	-	M2
	46	バックアップ	ファイルに機密情報が含まれていないか	-	○	-	○	○	-	-	-	-	-	-	○	-	M2
	47	バックアップ	機密情報が暗号化されているか（キーのバックアップが適切か）	-	△	○	-	○	○	○	-	○	-	-	○	-	M2
	48	機密データ利用目的への説明	プライバシーポリシーを明示しているか	-	○	-	-	○	-	○	-	-	○	○	○	-	M2
暗号化	49	暗号化標準アルゴリズムの構成の検証	getInstance へのすべての呼び出しでデフォルトプロバイダーのセキュリティサービスが使用されているか	-	○	-	○	-	-	○	-	○	-	○	○	-	M5
	50	暗号化標準アルゴリズムの構成の検証	安全でない暗号アルゴリズムや廃止された暗号アルゴリズムでないか	△	○	-	○	-	△	○	-	○	-	○	○	-	M5
	51	暗号化標準アルゴリズムの構成の検証	キーの長さが十分か	-	○	-	○	-	-	○	-	○	-	○	○	-	M5
	52	暗号化標準アルゴリズムの構成の検証	弱い擬生成関数を使用していないか	-	○	-	○	-	-	○	-	○	-	○	○	-	M5
	53	暗号化標準アルゴリズムの構成の検証	暗号化のカスタム実装を使用していないか	-	○	-	○	-	-	○	-	○	-	○	○	-	M5
	54	暗号化標準アルゴリズムの構成の検証	AES構成が適切か	-	○	-	○	-	-	○	-	○	-	○	○	-	M5
	55	暗号化標準アルゴリズムの構成の検証	弱いブロック暗号モードを使用していないか	△	○	-	○	-	△	○	-	○	-	○	○	-	M5
	56	暗号化標準アルゴリズムの構成の検証	予測可能な初期化ベクトルを使用していないか	△	○	-	○	-	-	○	-	○	-	○	○	-	M5
	57	暗号化標準アルゴリズムの構成の検証	弱いパディングまたはブロック操作の実装をしていないか	△	○	-	○	-	-	○	-	○	-	○	○	-	M5
	58	暗号化標準アルゴリズムの構成の検証	ストレージおよびメモリ内のキーの保護が適切か	-	○	-	○	-	-	○	-	○	-	○	○	-	M5
	59	暗号化標準アルゴリズムの構成の検証	キーを転送する場合の処理は適切か	-	○	-	○	-	-	○	-	○	-	○	○	-	M5
	60	乱数生成	既知の脆弱な乱数生成関数を使用していないか	△	○	-	○	-	○	-	-	-	-	○	○	-	M5
	61	乱数生成	カスタム関数を使用していないか	-	○	-	○	-	-	-	-	-	-	○	○	-	M5
	62	乱数生成	デフォルトのコンストラクターを使用しているか	-	○	-	○	-	-	-	-	-	-	○	○	-	M5
	63	乱数生成	標準の関数で乱数を生成しているか	-	-	-	-	-	-	-	-	-	-	○	○	-	M5
	64	乱数生成	ランダム性の品質がどの程度優れているか	-	○	-	-	○	-	○	-	-	○	○	○	-	M5
	65	対称暗号化	識別されたインスタンスごとに、対称キーが使用されているか	△	○	-	○	○	-	-	-	-	-	○	○	-	M5
	66	キーの目的/管理	すべてのキーは作成時に定義された目的に従って使用されているか	-	○	-	○	○	-	-	-	-	-	○	○	-	M5
	67	キーの目的/管理	非対称キーの場合、秘密鍵は署名と公開鍵の暗号化にのみ使用されているか	-	○	-	○	○	-	-	-	-	-	○	○	-	M5
	68	キーの目的/管理	一つの対称キーを複数の目的に使用されていないか	-	○	-	○	○	-	-	-	-	-	○	○	-	M5
	69	キーの目的/管理	暗号化はビジネス目的に従って使用されているか	-	○	-	○	○	-	-	-	-	-	○	○	-	M5
	70	キーの目的/管理	機密情報を保護にキーが使用されている場合、デバイス間でキーは同期していないか	-	-	-	-	-	-	-	-	○	○	○	○	-	M5
	71	キーの目的/管理	ソースコード内にキーが直接記述されていないか	-	-	-	-	-	-	-	-	○	○	○	○	-	M5
	72	キーの目的/管理	キーがデバイスの安定した機能（例：デバイスID、MACアドレスなど）から派生されていないか	-	-	-	-	-	-	-	-	○	○	○	○	-	M5
	73	キーの目的/管理	低レベル言語でキーが隠蔽されていないか	-	-	-	-	-	-	-	-	○	○	○	○	-	M5
	74	キーの目的/管理	キーが不安全な場所（例：公開されている)リポジトリ、公開APIなど）からインポートされていないか	-	-	-	-	-	-	-	-	○	○	○	○	-	M5
認証・認可	75	安全な認証および認可プロトコルを使用	Webアプリ診断に準拠	-	○	○	-	○	-	○	○	-	○	-	○	-	M4
	76	認証のテストに関する一般的なガイドライン（モバイルアプリ側）	ソーシャルメディア アプリは以下の3つの内1つを使用しているか ①基準ユーザーが知っているもの（パスワード、PIN、パターンなど） ②ユーザーが所有するもの（SIM カード、ワンタイム パスワード ジェネレーター、またはハードウェア トークン） ③ユーザーの生体認証プロパティ（指紋、網膜、音声）	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	77	認証のテストに関する一般的なガイドライン（モバイルアプリ側）	金融アプリはPCI DSS、Gramm Leach Bliley Act、Sarbanes-Oxley Act (SOX)に準拠しているか	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	78	認証のテストに関する一般的なガイドライン（モバイルアプリ側）	医療分野の会社および支払関連アプリはHIPAAに準拠しているか	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	79	ステートフル認証とステートレス認証（モバイルアプリ側）	適切なステートフル認証か	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	80	OAuth 2.0（モバイルアプリ側）	ユーザーエージェントが適切か	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	81	OAuth 2.0（モバイルアプリ側）	グラントの種類が適切か	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	82	OAuth 2.0（モバイルアプリ側）	クライアントシークレットが適切か	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	83	OAuth 2.0（モバイルアプリ側）	エンドユーザーの認証情報が適切か	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	84	OAuth 2.0（モバイルアプリ側）	トークンが適切か	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	85	ユーザーのログアウト（モバイルアプリ側）	ログアウト機能が適切か	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	86	補助認証（モバイルアプリ側）	認証スキームが適切か	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	87	二要素認証（モバイルアプリ側）	適切なSMS-OTPか	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	88	二要素認証（モバイルアプリ側）	プッシュ通知と PKI を使用したトランザクション署名が適切か	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	89	ログインアクティビティとデバイスのブロック（モバイルアプリ側）	ログイン試行が適切か	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	90	ログインアクティビティとデバイスのブロック（モバイルアプリ側）	パスワードの変更が適切か	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	91	ログインアクティビティとデバイスのブロック（モバイルアプリ側）	個人識別情報の変更（氏名、メールアドレス、電話番号等）が適切か	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	92	ログインアクティビティとデバイスのブロック（モバイルアプリ側）	機密性の高いアクティビティ（購入、重要なリソースへのアクセスなど）が適切か	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	93	ログインアクティビティとデバイスのブロック（モバイルアプリ側）	利用規約違反への措置が適切か	-	○	-	○	○	-	○	-	○	○	-	○	-	M4
	94	資格情報の機能	ロック画面が設定されているか	-	○	-	-	○	-	-	-	-	-	-	○	-	M4
	95	資格情報の機能	ユーザー認証が必要なキーが適切に作成されているか	-	○	-	-	○	-	-	-	-	-	-	○	-	M4
	96	資格情報の機能	ユーザー認証の有効期限が適切か	-	○	-	-	○	-	-	-	-	-	-	○	-	M4
	97	資格情報の機能	ロック画面で保護されたキーを使用するフローが適切に動作するか	-	○	-	-	○	-	-	-	-	-	-	○	-	M4
	98	資格情報の機能	ロック解除されたキーが適切に使用されているか	-	○	-	-	○	-	-	-	-	-	-	○	-	M4
	99	資格情報の機能	ローカル認証バイパスの脆弱性がないか	-	○	-	-	○	-	-	-	-	-	-	○	-	M4
	100	生体認証	標準の生体認証ライブラリが使用されているか	-	○	-	-	○	-	-	-	-	-	-	○	-	M4
	101	生体認証	サードパーティライブラリを使用している場合適切か	-	○	-	-	○	-	-	-	-	-	-	○	-	M4
	102	生体認証	生体認証の処理が適切か	-	○	-	-	○	-	-	-	-	-	-	○	-	M4
	103	ローカル認証	機密プロセスがキーチェーン サービス方式を使用して保護されているか	-	-	-	-	-	-	○	-	○	○	-	○	-	M4
	104	ローカル認証	アクセス制御フラグがキーチェーン項目に適切に設定されているか	-	-	-	-	-	-	○	-	○	○	-	○	-	M4
	105	ローカル認証	生体認証を使用しているか	-	-	-	-	-	△	○	-	○	○	-	○	-	M4
	106	ローカル認証	生体認証の処理が適切か	-	-	-	-	-	-	○	-	○	○	-	○	-	M4
ネットワーク通信	107	ネットワークトラフィックの保護	PFSが有効か	-	-	-	-	-	△	○	-	○	-	○	○	-	M3
	108	エンドポイント識別検証	ターゲットとなるSDKバージョンが適切か	-	○	-	-	○	-	○	-	○	-	○	○	-	M3
	109	エンドポイント識別検証	ネットワークセキュリティ構成が適切か	-	○	-	-	○	-	○	-	-	-	○	○	-	M3
	110	エンドポイント識別検証	サーバー証明書の検証が適切か（証明書を偽装する対策が適切か）	△	○	-	○	-	-	○	-	○	-	○	○	-	M3
	111	エンドポイント識別検証	WebView サーバー証明書の検証がされるか※Apache Cordova 証明書の検証を含む	△	○	-	○	-	○	-	-	-	-	○	○	-	M3
	112	エンドポイント識別検証	ホスト名の検証がされるか	△	○	-	○	-	-	○	-	○	-	○	○	-	M3
	113	SSL/TLSを適用	TLS設定が適切か（TLSのバージョンが適切か）	△	○	-	○	-	△	○	-	○	-	○	○	-	M3
	114	ネットワークとのデータ暗号化	プレーンな HTTP URL が使用されていないか（HTTPSプロコトルを使用しているか）	△	○	-	○	-	-	○	-	○	-	○	○	-	M3
	115	ネットワークとのデータ暗号化	低レベル API を使用する場合でも、安全に実装されているか	-	○	-	○	-	-	○	-	○	-	○	○	-	M3
	116	ネットワークとのデータ暗号化	クリアテキストの HTTPトフィックを許可していないか	△	○	-	○	-	△	○	-	○	○	○	○	-	M3
	117	ネットワークとのデータ暗号化	NetworkSecurityConfig 属性が適切に設定されているか	△	○	-	○	-	-	-	-	○	-	○	○	-	M3
	118	証明書ストアと証明書の設定	デバッグ証明書で署名されたアプリケーション	△	○	-	○	-	-	-	-	-	-	-	○	-	M3
	119	証明書ストアと証明書の設定	証明書のピンニングの実装は適切か	△	○	-	○	-	△	○	-	○	-	-	○	-	M3
	120	証明書ストアと証明書の設定	サードパーティライブラリを使用する場合にライブラリ証明書ピンニングは適切か	-	○	-	○	-	-	-	-	-	-	-	○	-	M3
	121	証明書ストアと証明書の設定	ハイブリッドおよびクロスプラットフォームの証明書ピンニングは適切か	-	○	-	○	-	-	-	-	-	-	-	○	-	M3
	122	証明書ストアと証明書の設定	証明書ピンニングの処理は適切か	-	○	-	-	○	-	-	-	-	-	-	○	-	M3
	123	証明書ストアと証明書の設定	アプリケーションバンドル内にサーバーの証明書が含まれているか	-	-	-	-	-	-	○	-	-	○	○	○	-	M3
	124	証明書ストアと証明書の設定	Info.plistファイル内にピンニングされたCA公開鍵が指定されているか	-	-	-	-	-	○	-	-	-	-	-	○	-	M3
	125	証明書ストアと証明書の設定	サードパーティライブラリの証明書ピンニングは適切か	△	○	-	-	-	-	○	-	○	-	○	○	-	M3
	126	証明書ストアと証明書の設定	証明書の検証が行われているか	-	-	-	-	-	-	○	-	-	-	-	○	-	M3
	127	証明書ストアと証明書の設定	カスタムピンニングの設定が適切か	-	-	-	-	-	-	○	-	○	○	-	○	-	M3
	128	セキュリティプロバイダーの更新	GmsCore_OpenSSLが最上位に存在するか	-	○	-	○	○	-	-	-	-	-	-	○	-	M3
	129	IPアドレスの開示	IPアドレスの開示をしているか	○	-	-	-	-	○	-	-	-	-	○	○	-	M3

				Android					iOS					MASVS			owasp-mobile
概要	No	診断項目	小項目	ツール診断	手動診断	API診断	静的解析	動的解析	ツール診断	手動診断	API診断	静的解析	動的解析	L1	L2	R	TOP10
プラットフォーム（OS）	130	IPCメカニズム（機能）	IPC メカニズムの使用時に機密情報が適切に扱われているか	-	○	-	○	○	-	○	-	○	○	○	○	-	M1
	131	ディープリンク	ウェブサイトの関連付けが適切か	-	○	-	○	-	-	-	-	-	-	○	○	-	M1
	132	ディープリンク	ハンドラーメソッドが適切か	-	-	-	○	○	-	○	-	-	○	○	○	-	M1
	133	ユニバーサルリンク	関連するドメインの権限が適切か	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	134	ユニバーサルリンク	Apple App Site Associationファイルが適切か	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	135	ユニバーサルリンク	リンクレシーバーメソッドが適切か	-	-	-	-	-	-	○	-	○	○	○	○	-	M1
	136	ユニバーサルリンク	データハンドラーメソッドが適切か	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	137	ユニバーサルリンク	ユニバーサルリンク経由で他のアプリを呼び出す場合に機密情報が漏洩しないか	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	138	ユニバーサルリンク	ユニバーサルリンクのトリガーが適切か	-	-	-	-	-	-	○	-	○	○	○	○	-	M1
	139	ユニバーサルリンク	許可されていないユニバーサルリンクが適切か	-	-	-	-	-	-	○	-	-	○	○	○	-	M1
	140	ユニバーサルリンク	リンクが適切に処理されているか	-	-	-	-	-	-	○	-	-	○	○	○	-	M1
	141	カスタムURLスキーム	プロトコル ハンドラーを登録しているか	-	-	-	-	-	△	○	-	○	-	○	○	-	M1
	142	カスタムURLスキーム	ターゲット アプリが利用可能するメソッドが適切か	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	143	カスタムURLスキーム	URLパスの処理が適切か（ディープリンクを使用しているか）	-	-	-	-	-	△	○	-	○	-	○	○	-	M1
	144	カスタムURLスキーム	他のアプリへのURLリクエストが適切か	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	145	カスタムURLスキーム	非推奨のメソッドがないか	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	146	カスタムURLスキーム	URLリクエストの処理が適切か	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	147	カスタムURLスキーム	URLハンドラーメソッドが適切か	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	148	カスタムURLスキーム	URLスキームの検証が適切か	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	149	カスタムURLスキーム	メモリリークが発生ないか	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	150	アプリの権限	最小限の権限のみを要求しているか	△	○	-	○	○	△	○	-	○	○	○	○	-	M1
	151	アプリの権限	カスタム権限がないか	-	○	-	○	-	-	-	-	-	-	○	○	-	M1
	152	アプリの権限	権限の要求するメソッドが適切か	-	○	-	○	-	-	-	-	-	-	○	○	-	M1
	153	アプリの権限	アクセス許可を付与した方確認するメソッドが適切か	-	○	-	-	-	-	-	-	-	-	○	○	-	M1
	154	アプリの権限	使用しているAPI、メソッドが適切か	-	-	-	-	-	-	○	-	○	○	○	○	-	M1
	155	アプリの権限	targetSdkVersionが適切か	△	○	-	○	-	-	-	-	-	-	○	○	-	M1
	156	アプリの権限	保護レベルが適切か	△	○	-	-	-	-	-	-	-	-	○	○	-	M1
	157	アプリの権限	プロバイダー接続状況が適切か	△	○	-	-	-	-	-	-	-	-	○	○	-	M1
	158	IPC メカニズム（ストレージ）	IPCにより機密情報が漏洩していないか※インテント機密情報	△	○	-	○	-	-	○	-	○	○	○	○	-	M1
	159	IPC メカニズム（ストレージ）	コンテンツプロバイダーが適切か	-	○	-	○	○	-	-	-	-	-	○	○	-	M1
	160	クリップボード	クリップボードの変更を検出する機能があるか	△	○	-	-	-	△	○	-	○	○	○	○	-	M1
	161	クリップボード	機密情報のコピーは適切か（コピー機能を使用しているか）※出所はMobsf	△	○	-	-	-	△	○	-	○	○	○	○	-	M1
	162	クリップボード	機密情報を扱う場合はシステムのペーストボードを使用していないか	-	-	-	-	-	△	-	-	○	○	○	○	-	M1
	163	クリップボード	カスタムペーストボードを使用していないか	-	-	-	-	-	-	○	-	○	○	○	○	-	M1
	164	クリップボード	プロセスが適切に使用されているか	-	-	-	-	-	-	○	-	-	○	○	○	-	M1
	165	ペンディングインテント	PendingIntentの実装が適切か	-	○	-	○	○	-	-	-	-	-	○	○	-	M1
	166	アプリ拡張機能	対応しているデータ型が適切か	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	167	アプリ拡張機能	アプリ拡張機能の使用を制限しているか	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	168	アプリ拡張機能	共有されているアイテムが適切か	-	-	-	-	-	-	○	-	-	○	○	○	-	M1
	169	アプリ拡張機能	拡張機能の処理が適切か	-	-	-	-	-	-	○	-	-	○	○	○	-	M1
	170	UIアクティビティ共有	アイテムの受け取りが適切か	-	-	-	-	-	-	○	-	○	○	○	○	-	M1
	171	UIアクティビティ共有	アイテムの送信が適切か	-	-	-	-	-	-	○	-	-	○	○	○	-	M1
	172	WebViewクリーンアップ	WebViewのデータの削除に関連するAPIのプロセスが適切か	-	○	-	-	-	-	-	-	-	-	○	○	-	M1
	173	WebViewを通して公開されるJavaオブジェクト	JavaScriptからJavaオブジェクトのアクセスは適切に実装されているか	-	○	-	○	○	-	-	-	-	-	○	○	-	M1
	174	WebViewでのJavaScriptの実行	JavaScriptの実行は適切に行われているか （JavaScriptが無効になっているか）※Mobsf	△	○	-	○	○	-	-	-	-	-	○	○	-	M1
	175	WebViewプロトコルハンドラー	WebViewがリソースにアクセスする際の実装は適切か	△	○	-	○	○	-	-	-	-	-	○	○	-	M1
	176	WebViewプロトコルハンドラー	WebViewの読み込みの処理は適切か（非推奨のメソッドを使用しているか）	-	○	-	○	-	△	○	-	○	○	○	○	-	M1
	177	WebViewプロトコルハンドラー	WebViewのファイルアクセス制御は適切か	-	-	-	-	-	-	○	-	○	○	○	○	-	M1
	178	iOS WebView	UIWebViewまたはSFSafariViewControllerを使用していないか	-	-	-	-	-	△	○	-	○	○	○	○	-	M1
	179	iOS WebView	JavaScriptが無効になっているか	-	-	-	-	-	△	○	-	○	○	○	○	-	M1
	180	iOS WebView	混在コンテンツの処理は適切か	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	181	iOS WebView	安全なコンテンツのみが許可されているか	-	-	-	-	-	-	○	-	-	○	○	○	-	M1
	182	iOS WebView	WebViewのURL操作ができないようになっているか	-	-	-	-	-	-	○	-	-	○	○	○	-	M1
	183	WebViewのネイティブメソッド	UIWebViewのJavaScriptからネイティブブリッジの実装は適切か	-	-	-	-	-	-	○	-	-	○	○	○	-	M1
	184	WebViewのネイティブメソッド	WKWebViewのJavaScriptからネイティブ ブリッジの実装は適切か	-	-	-	-	-	-	○	-	○	-	○	○	-	M1
	185	WebViewのネイティブメソッド	機密情報が公開されていないか	-	-	-	-	-	-	○	-	-	-	○	○	-	M1
	186	ユーザーインターフェイスを介した機密データの漏洩	アプリケーションが機密性の高いユーザー入力するときにマスクしているか	-	○	-	○	○	-	-	-	-	-	○	○	-	M1
	187	ユーザーインターフェイスを介した機密データの漏洩	アプリの通知の処理が適切か	-	○	-	○	○	-	-	-	-	-	○	○	-	M1
	188	ユーザーインターフェイスを介した機密データの漏洩	通知やテキストフィールドなどUIに機密情報を表示している部分がないか （テキスト入力をマスクする機能があるか）	-	-	-	-	-	○	-	-	-	○	○	○	-	M1
	189	オーバーレイ攻撃対策	オーバーレイ攻撃を防止する機能があるか（タップジャッキング防止機能の検出）	△	○	-	○	-	-	-	-	-	-	○	○	-	M1
	190	自動生成されたスクリーンショット内の機密情報の検索	アプリがバックグラウンドに移行するときに取得されるスクリーンショットを防止しているか	△	○	-	○	-	-	-	-	○	○	○	○	-	M1
クライアントコードの品質	191	アプリ内更新	アプリ内更新をサポートしているか	△	○	-	○	○	-	○	-	○	○	-	○	-	M7
	192	脆弱なサードパーティライブラリ	既知の脆弱性のあるサードパーティ製ライブラリを使用しているか	-	○	-	○	○	-	○	-	○	○	○	○	-	M7
	193	脆弱なサードパーティライブラリ	サードパーティ製ライブラリの最作権の条件を満たしているか	-	○	-	○	○	-	○	-	-	○	○	○	-	M7
	194	ローカルストレージの入力検証	データが再度読み取られると きに入力検証があるか	-	○	-	○	○	-	○	-	-	-	○	○	-	M7
	195	オブジェクトの永続性	オブジェクトの永続性を使用しているか	-	○	-	○	○	-	○	-	○	○	○	○	-	M7
	196	オブジェクトの永続性	機密情報をJSONファイルで保存していないか（Jacksonライブラリを使用していないか）	△	○	-	○	-	-	-	-	-	-	○	○	-	M7
	197	オブジェクトの永続性	ORMライブラリはデータが暗号化されたデータベースに保存されているか	-	○	-	○	-	-	-	-	-	-	○	○	-	M7
	198	オブジェクトの永続性	機密情報がインテントに保存される場合の処理は適切か	-	○	-	○	-	-	-	-	-	-	○	○	-	M7
	199	オブジェクトの永続性	オブジェクトの処理が適切か	-	○	-	-	○	-	○	-	-	○	○	○	-	M7
	200	オブジェクトの永続性	オブジェクトの永続性を使用して機密情報をデバイスに保存する場合暗号化されているか	-	-	-	-	-	-	○	-	○	-	○	○	-	M7
	201	オブジェクトの永続性	HMACメカニズムを使用しているか	-	-	-	-	-	-	○	-	○	-	○	○	-	M7
	202	オブジェクトの永続性	キーボードチェインに保存されているか	-	-	-	-	-	-	○	-	○	-	○	○	-	M7
	203	オブジェクトの永続性	逆シリアル化されたオブジェクト内のデータ検証されてから使用しているか	-	-	-	-	-	-	○	-	○	-	○	○	-	M7
	204	オブジェクトの永続性	ランダムなリファレンスを使用する永続化メカニズムを使用して、同リスクのアプリケーションでオブジェクトをシリアル化/逆シリア	-	-	-	-	-	-	○	-	○	-	○	○	-	M7
	205	オブジェクトの永続性	ミラーメソッドが適切か	-	-	-	-	-	-	○	-	○	-	○	○	-	M7
	206	インジェクションの欠陥の検査	インジェクションの対策をしているか （SQLクエリを直接実行していないか）	△	○	-	○	○	-	-	-	-	-	○	○	-	M7
	207	暗黙的なインテント	機密データが漏洩する可能性があるか	-	○	-	○	○	-	-	-	-	-	○	○	-	M7
	208	バイナリセキュリティ機能	PIE およびスタック スマッシング保護が有効になっているか	△	○	-	○	-	△	○	-	○	○	○	○	-	M7
	209	WebViewでのURL読み込み	WebView内でクリックするリンクをデフォルトのWebブラウザーで開いているか	-	○	-	○	-	-	-	-	-	-	○	○	-	M7
	210	WebViewでのURL読み込み	EnableSafeBrowsingが有効になっているか	-	○	-	○	-	-	-	-	-	-	○	○	-	M7
	211	WebViewでのURL読み込み	WebView内でリンクをクリックしたときの処理が適切か	-	○	-	-	○	-	-	-	-	-	○	○	-	M7
	212	メモリリーク	メモリリークを起こすコーディングがされているか	-	-	-	-	-	○	-	-	-	-	○	○	-	M7
	213	メモリリーク	シリアル化による脆弱性があるか	-	○	-	-	○	-	-	-	-	-	○	○	-	M7
リバースエンジニアリング	214	ルート化・脱獄の検知	バイナリの名前変更でルート検出機能を無効にできないか	-	○	-	○	○	-	-	-	-	-	-	-	○	M8
	215	ルート化・脱獄の検知	/procディレクトリをアンマウントした場合にルート検出機能を無効にできないか	-	○	-	○	○	-	-	-	-	-	-	-	○	M8
	216	ルート化・脱獄の検知	FridaやXposedでのAPIフックが使用できないか	-	○	-	○	○	-	-	-	-	-	-	-	○	M8
	217	ルート化・脱獄の検知	カーネルモジュールによる低レベルAPIのフックが使用できないか	-	○	-	○	○	-	-	-	-	-	-	-	○	M8
	218	ルート化・脱獄の検知	アプリのパッチ適用（設定ファイルやリソースファイルの変更）してルート検出機能を無効にできないか	-	○	-	○	○	-	-	-	-	-	-	-	○	M8
	219	ルート化・脱獄の検知	複数の検出メカニズムがアプリ全体に存在しているか（SafetyNet APIを使用しているか）	△	○	-	○	○	-	-	-	-	-	-	-	○	M8
	220	ルート化・脱獄の検知	複数の検出メカニズムがアプリ全体に存在しているか（ツールで検出しているか）	△	○	-	○	○	-	-	-	-	-	-	-	○	M8
	221	ルート化・脱獄の検知	複数の検出メカニズムがアプリ全体に存在しているか（ルート権限の検知を しているか）	△	○	-	○	○	-	-	-	-	-	-	-	○	M8
	222	ルート化・脱獄の検知	ルート検出メカニズムは、複数の API レイヤーで動作しているか	-	○	-	○	○	-	-	-	-	-	-	-	○	M8
	223	ルート化・脱獄の検知	ルート検出メカニズムはオリジナルのソースコードか	-	-	-	○	○	-	-	-	-	-	-	-	○	M8
	224	ルート化・脱獄の検知	ファイルベースの脱獄検出機能があるか	-	-	-	-	-	△	○	-	○	-	-	-	○	M8
	225	ルート化・脱獄の検知	その他の脱獄検出機能があるか	-	-	-	-	-	△	○	-	○	-	-	-	○	M8
	226	ルート化・脱獄の検知	脱獄検出機能を無効にできないか	-	-	-	-	-	-	○	-	○	-	-	-	○	M8
	227	シミュレータ・エミュレータの検知	build.propファイルに基づくエミュレータ検出機能があるか	-	○	-	○	○	-	-	-	-	-	-	-	○	M8
	228	シミュレータ・エミュレータの検知	TelephonyManagerを使用した エミュレータ検出機能があるか	-	○	-	○	○	-	-	-	-	-	-	-	○	M8
	229	シミュレータ・エミュレータの検知	エミュレータ検出機能があるか	-	-	-	-	-	△	○	-	○	○	-	-	○	M8
	230	シミュレータ・エミュレータの検知	他のエミュレータ検出機能があるか	△	○	-	○	○	-	○	-	○	○	-	-	○	M8
	231	シミュレータ・エミュレータの検知	エミュレータ検出機能が無効にできないか	-	○	-	○	○	-	○	-	○	-	-	-	○	M8
	232	アプリの署名	アクセス許可が適切か	△	○	-	○	○	-	○	-	○	○	-	-	○	M8,M9
	233	アプリの署名	アプリが最新のコード署名形式を使用しているか（バイナリに署名があるか）	-	-	-	-	-	○	-	-	-	-	-	-	○	M8,M9
	234	アプリの署名	アプリが最新のコード署名形式を使用しているか	-	-	-	○	-	-	-	-	-	-	-	-	○	M8,M9
	235	ファイル完全性	NOP命令でバイトコードまたはネイティブコードを置き換えを検出できるか	-	○	-	○	○	-	-	-	-	-	-	-	○	M9
	236	ファイル完全性	FridaまたはXposedを使用してファイルシステムAPIをフックして修正可能か	-	○	-	○	○	-	-	-	-	-	-	-	○	M9
	237	ファイル完全性	カーネルモジュールを使用してファイル関連のシステムコールを傍受できるか	-	○	-	○	○	-	-	-	-	-	-	-	○	M9
	238	ファイル完全性	デバイスからデータを取得して内容を変更を検出できるか	-	○	-	○	○	-	-	-	-	-	-	-	○	M9
	239	ファイル完全性	防御を無効にするためのカスタムコードの必要性と所要時間が大きいか	-	○	-	○	○	-	-	-	-	-	-	-	○	M9
	240	ファイル完全性	HMACキーまたは非対称プライベートキーの取得難易度が高いか	-	○	-	○	○	-	○	-	○	○	-	-	○	M9
	241	ファイル完全性	実行可能ファイルにパッチを適用し、署名を検出できるか（パッケージ署名を使用しているか）	△	○	○	○	○	-	○	-	-	○	-	-	○	M9
	242	ファイル完全性	アプリデータディレクトリに書き込むことのできるファイルを変更を検出できるか	-	-	-	-	-	-	○	-	-	○	-	-	○	M9
	243	ランタイム完全性	アプリはメモリ内の「脆弱性な」コードを検出できるか	-	○	-	○	○	-	-	-	-	-	-	-	○	M9
	244	デバッグシンボルの削除	静的シンボルがあるか	-	○	-	○	-	-	○	-	○	-	-	-	○	M9
	245	デバッグシンボルの削除	コンパイラに対し特定のシンボルを隠蔽しているか	-	○	-	○	-	-	-	-	-	-	-	-	○	M9
	246	デバッグシンボルの削除	ビルト設定「Strip Debug Symbols during Copy」が「YES」に設定されているか	-	-	-	-	-	-	○	-	○	○	-	-	○	M9
	247	難読化	クラス名、メソッド名、変数名などの意味のある識別子は隠蔽されているか	-	-	-	-	-	-	○	-	○	-	-	-	○	M5,M9
	248	難読化	文字列リソースとバイナリ内の文字列は暗号化されているか	-	-	-	-	-	-	○	-	○	-	-	-	○	M5,M9
	249	難読化	保護された 機能に関連するコードとデータは、難号化、パック化、またはその他の方法で隠蔽されているか	-	-	-	-	-	-	○	-	○	-	-	-	○	M5,M9
	250	難読化	クラス名、メソッド名、変数名などの意味のある識別子は隠蔽されているか	-	○	-	-	○	-	-	-	-	-	-	-	○	M5,M9
	251	難読化	文字列リソースとバイナリ内の文字列は難号化されているか	-	○	-	-	○	-	-	-	-	-	-	-	○	M5,M9
	252	難読化	保護された機能に関連するコードとデータは、難号化、パック化、またはその他の方法で隠蔽されているか	-	○	-	○	-	-	-	-	-	-	-	-	○	M5,M9
	253	コードのデバッグとエラーログ	StrictModeの設定が適切かはandroidのベストプラクティスに則っているか	-	○	-	○	-	-	-	-	-	-	-	-	○	M9
	254	コードのデバッグとエラーログ	エラーメッセージが詳細なメッセージを出していないか	-	○	-	○	-	-	-	-	-	-	-	-	○	M9
	255	コードのデバッグとエラーログ	リリースビルド時のデバッグ用コードやメソッドが無効か	-	○	-	○	-	-	-	-	-	-	-	-	○	M10
	256	コードのデバッグとエラーログ	リリースビルド時のデバッグ出力や詳細なエラーログがコンソールに表示ないか	-	-	-	-	-	-	○	-	○	○	-	-	○	M10
	257	コードのデバッグとエラーログ	リリースビルド時のログ開設がオフになっているか	-	-	-	-	-	-	○	-	○	○	-	-	○	M10
	258	リバースエンジニアリング ツールとフレームワーク検知	Xposedが検出できるか	-	○	-	○	-	-	-	-	-	-	-	-	○	M9
	259	リバースエンジニアリング ツールとフレームワーク検知	Substrate for Androidが検出できるか	-	○	-	○	-	-	-	-	-	-	-	-	○	M9
	260	リバースエンジニアリング ツールとフレームワーク検知	RootCloakが検出できるか	-	○	-	○	-	-	-	-	-	-	-	-	○	M9
	261	リバースエンジニアリング ツールとフレームワーク検知	Android SSL Trust Killerが検出できるか	-	○	-	○	-	-	-	-	-	-	-	-	○	M9
	262	リバースエンジニアリング ツールとフレームワーク検知	Fridaが検出できるか	△	○	-	○	-	△	○	-	○	-	-	-	○	M9
	263	リバースエンジニアリング ツールとフレームワーク検知	Cydia Substrateが検出できるか	-	-	-	-	-	-	○	-	○	-	-	-	○	M9
	264	リバースエンジニアリング ツールとフレームワーク検知	SSL Kill Switchが検出できるか	-	-	-	-	-	-	○	-	○	-	-	-	○	M9
	265	リバースエンジニアリング ツールとフレームワーク検知	Cycriptが検出できるか	-	-	-	-	-	-	○	-	○	-	-	-	○	M9
	266	アンチデバッグ検出	jdbtPtraceベースのデバッガの検出ができるか	-	○	-	○	-	-	-	-	-	-	-	-	○	M9
	267	アンチデバッグ検出	他のデバッグ検出機能があるか	△	○	-	○	○	-	-	-	-	-	-	-	○	M9
	268	アンチデバッグ検出	検出メソッドの分布（集中していないか）が均一か	-	○	-	○	○	-	-	-	-	-	-	-	○	M9
	269	アンチデバッグ検出	オリジナルのソースコードか	-	○	-	○	○	-	-	-	-	-	-	-	○	M9
	270	アンチデバッグ検出	単一のAPI関数のフックでアンチデバッグ機能を無効にできないか	-	○	-	○	○	-	-	-	-	-	-	-	○	M9
	271	アンチデバッグ検出	アンチデバッグコードが難読のARLレイヤーで実装されているか	-	○	-	○	○	-	-	-	-	-	-	-	○	M9
	272	アンチデバッグ検出	カスタムコードでアンチデバッグ機能を無効にできないか	-	○	-	○	○	-	-	-	-	-	-	-	○	M9
	273	アンチデバッグ検出	デバッグ検出機能があるか	-	-	-	-	-	△	○	-	○	○	-	-	○	M10
	274	アンチデバッグ検出	デバッグを試みた際に、バックエンドサーバーに通知しているか	-	-	-	-	-	-	○	-	○	○	-	-	○	M9
	275	デバッグ制御	WebViewのデバッグ機能が無効になっているか	△	○	-	○	○	-	-	-	-	-	-	-	○	M9
	276	デバッグ制御	AndroidManifest.xmlファイル内でデバッグ不可の記述があるか	△	○	-	○	○	-	-	-	-	-	-	-	○	M9
	277	デバッグ制御	テストモードでないか	△	○	-	○	○	-	-	-	-	-	-	-	○	M9
	278	デバッグ制御	エンタイトルメントのキー値がget-task-allow: falseに設定されているか	-	○	-	○	○	-	-	-	-	-	-	-	○	M9
	279	デバッグ制御	ツールを使用しデバッグ不可になっているか	△	○	-	○	○	-	-	-	-	-	-	-	○	M9
	280	デバッグ制御	デバッグツールが使用できないか	-	○	-	○	○	-	○	-	○	○	-	-	○	M9