

Secure Coding Checker

基本操作マニュアル



株式会社ラック

Secure Coding Checker をご契約いただき、まことにありがとうございます。Secure Coding Checker をご利用いただくにあたり、様々な機能を正しくご利用いただくため、「本マニュアル」、「サービス仕様書」および「Secure Coding Checker オンラインヘルプ」を必ずお読みください。Secure Coding Checker は利用できる機能、アプリの検査項目などが、Android OS版、iOS版、オプションの契約状況により異なります。詳細は、「サービス仕様書」および「Secure Coding Checker オンラインヘルプ」にてご確認ください。

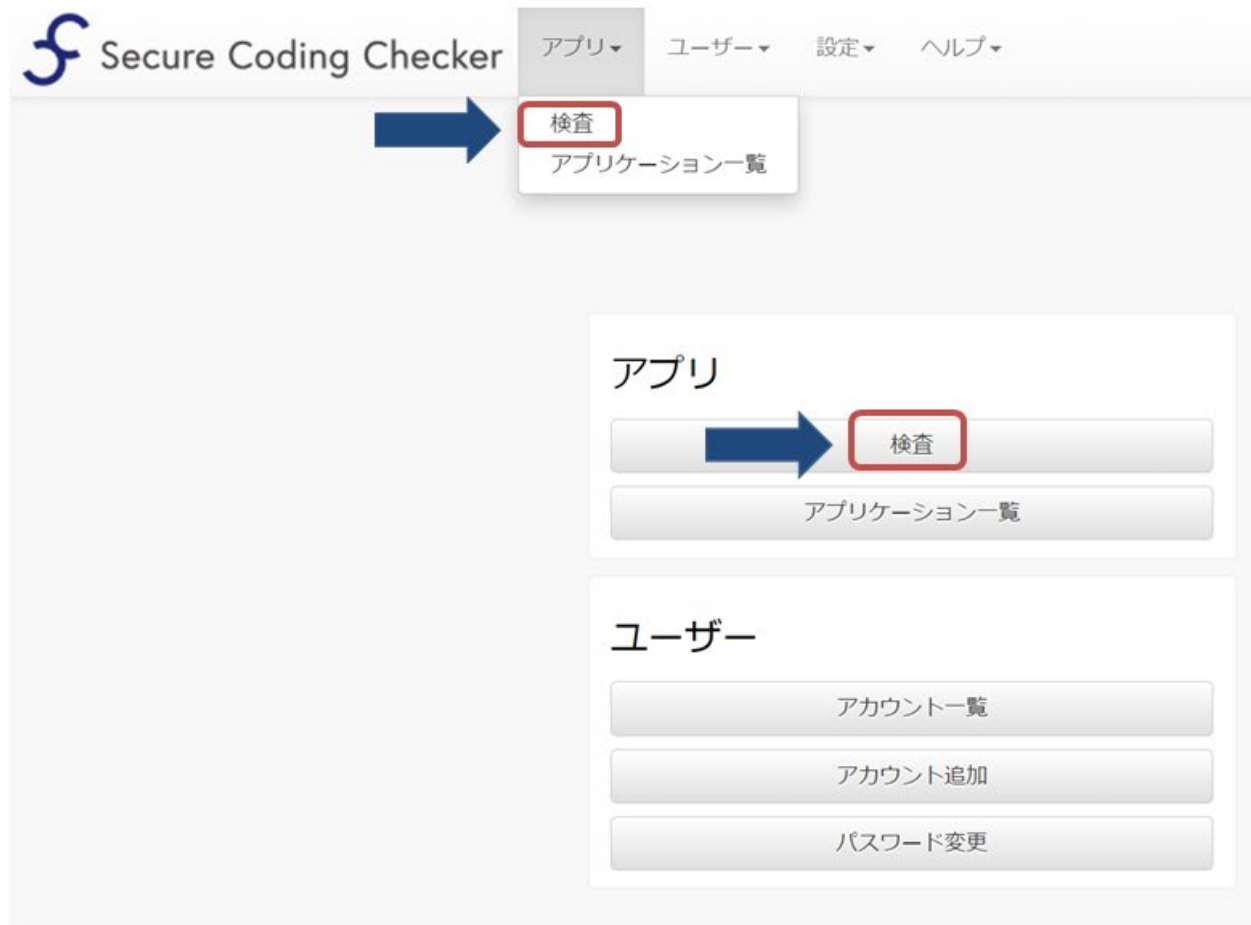
- 本書の内容の一部または全部を無断で複製・転載することはおやめください。
- 本書の内容に関しては将来予告なしに変更することがあります。
- 本書に誤り、乱丁、落丁などがありましたら弊社までご連絡ください。
- LAC、ラックは、株式会社ラックの登録商標です。
- その他、記載されている製品名、社名は各社の商標または登録商標です。

- 開発者向け機能 4ページ～
- 管理者向け機能 46ページ～
- オプション機能 58ページ～

開発者向け機能

- アプリ検査
- 質問回答
- ユーザー判断
- エビデンス出力
- JSON出力
- 検査オプション
- 差分通知
- アプリケーション一覧
- アプリ数とユーザー数の上限確認
- Cordova Android

アプリ検査



検査

APK/AAB/IPA
ファイルを選択



検査するアプリケーション

ファイルの選択

ファイルが選択されていません

検査メモ (任意)







必要に応じて、ここにメモを入力します。
メモは後で変更することもできます。

+ 検査オプション

検査

キャンセル

➤ 検査結果のアイコン種別

アイコン	意味
 違反	ガイドの（必須）項目に反している
 注意	ガイドの（推奨）項目に反している
 不明	質問に回答してください
 安全	
 安全判断	<input type="button" value="この項目を安全と判断する"/>
 リスク受容判断	<input type="button" value="この項目のリスクを受容する"/>

▶ DEMO



質問回答

➤ 検査結果に対して、データの重要性など、開発者が質問に回答することで、より踏み込んだ判定を行える。

センシティブな情報を結果情報として返しますか？

ガイド

- 未回答
- はい
- いいえ

センシティブな情報は、開発するアプリにおける「守るべき情報」（＝情報資産）を意味します。センシティブな情報を結果情報に含めるとは、本Activityが保護しているセンシティブな情報を、他アプリに対して意図して提供することを意味しています。

com.example.referenceapp.ContentProviderUserActivity

検出結果を確認し、以下の質問に回答して下さい。

この項目を安全と判断する この項目のリスクを受容する

質問事項

Activityの用途は？ ガイド

- 未回答
- 非公開
- 公開
- パートナー限定
- 自社限定

センシティブな情報を結果情報として返しますか？ ガイド

- 未回答
- はい
- いいえ

検出結果



com.example.referenceapp.ContentProviderUserActivity

安全

質問事項

Activityの用途は？ ガイド

- 未回答
- 非公開
- 公開
- パートナー限定
- 自社限定

センシティブな情報を結果情報として返しますか？ ガイド

- 未回答
- はい
- いいえ

検出結果

▶ DEMO

com.example.referenceapp.ContentProviderUserActivity

安全

または

com.example.referenceapp.ContentProviderUserActivity

違反事項があります。ガイドに従って修正して下さい。

この項目を安全と判断する この項目のリスクを受容する



センシティブな情報を結果情報として返しますか？



センシティブな情報は、開発するアプリにおける「守るべき情報」（＝情報資産）を意味します。センシティブな情報を結果情報に含めるとは、本Activityが保護しているセンシティブな情報を、他アプリに対して意図して提供することを意味しています。

ガイド

- 未回答
- はい
- いいえ

ユーザー判断

➤ 自社で修正できないライブラリ等で問題が検出されリスク受容判断する場合

安全でない暗号アルゴリズム・暗号モード・パディング方式



違反事項があります。ガイドに従って修正して下さい。

この項目を安全と判断する

この項目のリスクを受容する



この項目のリスクを受容する

「リスクを受容できる」と判断した根拠を記入して下さい。(最大2000字)

Text input area for justification.

この項目がサードパーティ製ソフトウェアに含まれていて修正できない場合、そのソフトウェアのパッケージ名を指定し、グループ管理者がサードパーティソフトウェア一覧を更新できます。

サードパーティソフトウェア

(選択してください)

(選択してください)

com.vishtekstudios.droidinsight360

OK

キャンセル

➤ リスク受容で選択できるソフトウェアは管理者が設定



- リスク受容で選択できるソフトウェアは管理者が設定

サードパーティーソフトウェア一覧

[この項目のリスクを受容する]で選択できるパッケージ名。

追加

パッケージ名

検査対象外

com.vishtekstudios.droidinsight360



変更

削除

Version: 2022.02.08 © 2022 LAC Co., Ltd.

DEMO

安全でない暗号アルゴリズム・暗号モード・パディング方式

違反事項があります。ガイドに従って修正して下さい。

この項目を安全と判断する この項目のリスクを受容する

アプリ▼ ユーザー▼ 設定▼ ヘルプ▼

- 検査
- アプリケーション一覧
- サードパーティーソフトウェア一覧**

アプリ

検査

アプリケーション一覧

サードパーティーソフトウェア一覧



サードパーティーソフトウェア一覧

[この項目のリスクを受容する]で選択できるパッケージ名。

追加

パッケージ名	検査対象外	
com.vishtekstudios.droidinsight360	<input checked="" type="checkbox"/>	変更 削除

Version: 2022.02.08 © 2022 LAC Co., Ltd.

エビデンス出力



Androidアプリケーション脆弱性検査結果

検査日時: 2022/9/1 16:08
 出力日時: 2022/9/1 16:28
 Secure Coding Checker/バージョン: 2022.02.08
 グループ名:
 グループID:

検査対象:

ファイル名:	ReferenceApp.apk
ファイルサイズ:	6,066 KB
ハッシュ値:	8608A346418EE611D04D7035958B535F336FD072F12BA760BC819CFDD183092D
パッケージ名:	com.example.referenceapp
バージョンコード:	1
バージョン名:	1.0
アプリケーション名:	ReferenceApp

検査結果

安全	3 件
安全判断	0 件
リスク受容	0 件
違反	23 件
注意	24 件
不明	78 件



検査結果

Activityを作る

安全	1 件
安全判断	0 件
リスク受容	0 件
違反	0 件
注意	8 件
不明	3 件

共通情報

uses-sdk#minSdkVersionの値	20 以下
--------------------------	-------

名前	ステータス	ユーザー判断根拠
com.example.referenceapp.MainActivity	質問未回答あり	
(質問) Activityの用途は?	公開	
(質問) センシティブな情報を結果情報として返しますか?	未回答	
(質問) 入力値の安全性を考慮して処理していますか?	未回答	
(質問) 利用元アプリの証明書を検査していますか?	-	
(質問) 本アプリ・利用元アプリを同じ鍵で署名していますか?	-	
(質問) IsValidFragment()をoverrideして、意図しないFragmentが入力されていないか確認していますか?	-	
exported	true	

DEMO

検査結果

エビデンス出力

ReferenceApp

com.example.referenceapp

検査サマリー

検査サマリー

検査結果

異常事項 27

違反: 23 注意: 24 不明: 78

安全: 3 安全判断: 0 リスク警告: 0

検査対象:

ファイル名: ReferenceApp.apk



Androidアプリケーション脆弱性検査結果

検査日時: 2022/9/1 16:08
出力日時: 2022/9/1 16:28
Secure Coding Checkerバージョン: 2022.02.08

検査対象:

ファイル名: ReferenceApp.apk
ファイルサイズ: 6,066 KB
パッケージ名: com.example.referenceapp
バージョンコード: 1
バージョン名: 1.0
アプリケーション名: ReferenceApp

検査結果

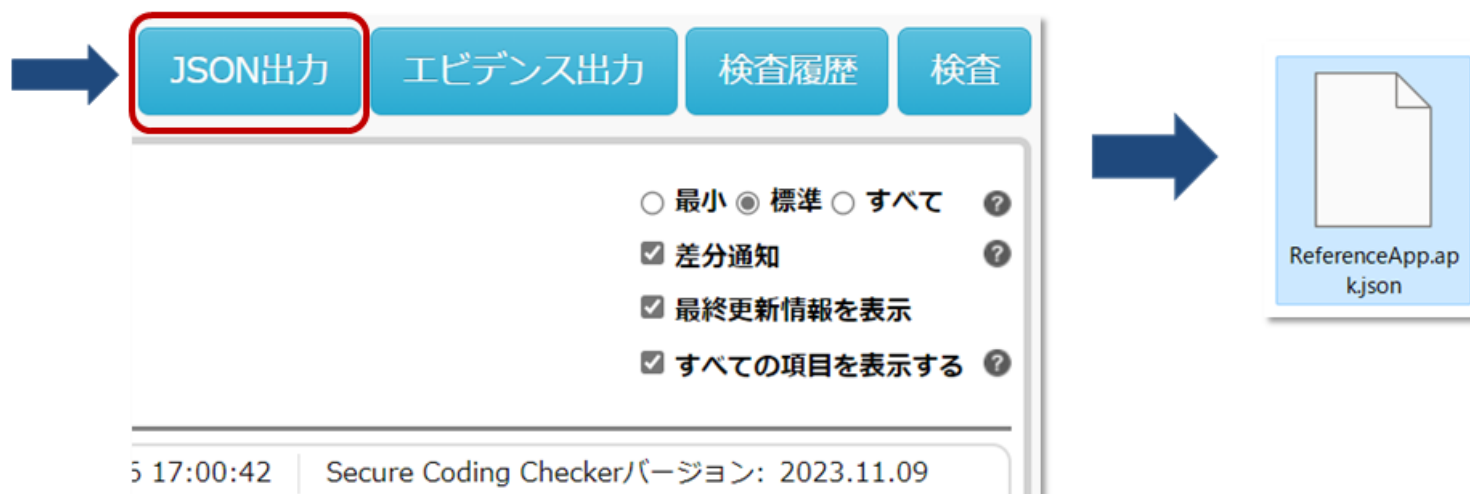
安全: 3 件
安全判断: 0 件
リスク警告: 0 件
違反: 23 件
注意: 24 件
不明: 78 件

Activityを作る

検査結果

違反	違反事項	違反内容	違反レベル	違反位置
違反	Activityを作る	Activityを作る時に、Intentのフラグを指定して渡す必要があります。	違反	com.example.referenceapp/MainActivity.java
違反	Activityを作る	Activityを作る時に、Intentのフラグを指定して渡す必要があります。	違反	com.example.referenceapp/MainActivity.java
違反	Activityを作る	Activityを作る時に、Intentのフラグを指定して渡す必要があります。	違反	com.example.referenceapp/MainActivity.java
違反	Activityを作る	Activityを作る時に、Intentのフラグを指定して渡す必要があります。	違反	com.example.referenceapp/MainActivity.java
違反	Activityを作る	Activityを作る時に、Intentのフラグを指定して渡す必要があります。	違反	com.example.referenceapp/MainActivity.java

JSON出力



ReferenceApp.apk.json ×

C: > Users > Downloads > ReferenceApp.apk.json > ...

```
1  {"Url": "https://.scc.lac.co.jp/ScanResult/Detail/158", "ScannedDateTime": "2023-11-06T08:00:42.3682287", "GroupName": "",
  "GroupId": "", "FileName": "ReferenceApp.apk", "PackageName": "com.example.referenceapp", "ApplicationName": "ReferenceApp", "Summary":
  {"Violations": {"Count": 23, "Diff": 0}, "Warnings": {"Count": 24, "Diff": 0}, "NotEvaluated": {"Count": 76, "Diff": -3}, "Safeties": {"Count": 5,
  "Diff": 3}, "JudgedSafeties": {"Count": 0, "Diff": 0}, "AcceptedRisks": {"Count": 0, "Diff": 0}}, "Details": [{"Category": "Activityを作る",
  "Violations": 0, "Warnings": 8, "NotEvaluated": 0, "Safeties": 4, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "Activityを利用する",
  "Violations": 0, "Warnings": 0, "NotEvaluated": 2, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "Broadcastを受信する",
  "Violations": 2, "Warnings": 4, "NotEvaluated": 1, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "Broadcastを送信する",
  "Violations": 0, "Warnings": 0, "NotEvaluated": 4, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "Content Providerを作る",
  "Violations": 1, "Warnings": 0, "NotEvaluated": 2, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "Content Providerを利用する",
  "Violations": 0, "Warnings": 0, "NotEvaluated": 1, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "Serviceを作る",
  "Violations": 1, "Warnings": 0, "NotEvaluated": 2, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "Serviceを利用する",
  "Violations": 0, "Warnings": 0, "NotEvaluated": 2, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "SQLiteを使う",
  "Violations": 0, "Warnings": 1, "NotEvaluated": 2, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "ファイルを扱う",
  "Violations": 0, "Warnings": 3, "NotEvaluated": 7, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "Browsable Intentを利用する",
  "Violations": 0, "Warnings": 0, "NotEvaluated": 1, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "LogCatにログ出力する",
  "Violations": 1, "Warnings": 0, "NotEvaluated": 1, "Safeties": 1, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "WebViewを使う",
  "Violations": 1, "Warnings": 0, "NotEvaluated": 3, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "Notificationを使用する",
  "Violations": 0, "Warnings": 0, "NotEvaluated": 2, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "共有メモリを使用する",
  "Violations": 1, "Warnings": 0, "NotEvaluated": 1, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "パスワード入力画面を作る",
  "Violations": 0, "Warnings": 0, "NotEvaluated": 1, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "独自Permissionを定義する",
  "Violations": 5, "Warnings": 4, "NotEvaluated": 1, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "Permissionを利用する",
  "Violations": 0, "Warnings": 0, "NotEvaluated": 22, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "Account Managerに独自アカウントを追加する",
  "Violations": 0, "Warnings": 1, "NotEvaluated": 1, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "HTTPSで通信する",
  "Violations": 5, "Warnings": 1, "NotEvaluated": 2, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "プライバシー情報を扱う",
  "Violations": 0, "Warnings": 0, "NotEvaluated": 7, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "暗号技術を利用する",
  "Violations": 5, "Warnings": 0, "NotEvaluated": 3, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "指紋認証機能を利用する",
  "Violations": 0, "Warnings": 0, "NotEvaluated": 1, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "Clipboardから情報漏洩する危険性",
  "Violations": 0, "Warnings": 0, "NotEvaluated": 2, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "Apache Cordova",
  "Violations": 0, "Warnings": 2, "NotEvaluated": 4, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}, {"Category": "その他(注意すべき実装)",
  "Violations": 1, "Warnings": 0, "NotEvaluated": 1, "Safeties": 0, "JudgedSafeties": 0, "AcceptedRisks": 0}]}
```

DEMO

検査結果

確定 JSON出力 エビデンス出力 検査履歴 検査

ReferenceApp
com.example.referenceapp

JSSEC & MASDC JSSEC MASDC

検査サマリー

検査サマリー 検査日時: 2023/11/6 17:00:42 Secure Coding Checkerバージョン: 2023.11.09

検査結果

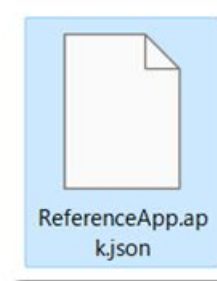
100% 94

違反: 23 注意: 24 不明: 76

安全: 5 安全判別: 0 リスク発覚判別: 0

JSSEC

Category	Count
Activity	10
Activityを利用する	2
Broadcast	2
Broadcastを受信する	2
Broadcastを送信する	4
Content Provider	3
Content Providerを作成する	3
Content Providerを利用する	1
Service	1
Serviceを利用する	2
SQLite	2
SQLiteを使う	2
ファイル	2
ファイルを開く	2
Browsable Intent	2
Browsable Intentを利用する	2
LogCat	1
LogCatにログ出力する	1
WebView	2
WebViewを使う	2
Notification	2
Notificationを使用する	2
共有メモリ	1
共有メモリを使用する	1
パスワード	1
パスワード入力画面を作成する	1
独自Permission	5
独自Permissionを定義する (Permission/Protection Level)	5
Permission	22
Permissionを利用する (Permission/Protection Level)	22
Account Manager	2
Account Managerに独自アカウントを追加する	2
HTTPS	3
HTTPSで通信する	3
プライバシー	2
プライバシー情報を扱う	2
許可技術	0
許可技術を利用する	0



```
1 [{"url":"https://www.sec.lac.co.jp/ScanResultDetail/334","scannedatetime":"2023-11-06T10:00:42.342207","orgname":"LAC","product":"Secure Coding Checker","packageName":"com.example.referenceapp","appName":"ReferenceApp","summary":["Violations":{"Count":23,"diff":0},"Warnings":{"Count":24,"diff":0},"NotValuated":{"Count":76,"diff":0},"SafeTies":{"Count":5,"diff":0},"JudgeSafeTies":{"Count":0,"diff":0},"AcceptedRisks":{"Count":0,"diff":0},"Details":{"Category":"Activityを作成する","Violations":0,"Warnings":0,"NotValuated":0,"SafeTies":4,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"Activityを利用する","Violations":2,"Warnings":0,"NotValuated":1,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"Broadcastを送信する","Violations":0,"Warnings":0,"NotValuated":4,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"Content Providerを作成する","Violations":1,"Warnings":0,"NotValuated":2,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"Content Providerを利用する","Violations":0,"Warnings":0,"NotValuated":1,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"Serviceを作成する","Violations":1,"Warnings":0,"NotValuated":2,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"Serviceを利用する","Violations":0,"Warnings":0,"NotValuated":2,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"SQLiteを使う","Violations":0,"Warnings":1,"NotValuated":2,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"ファイルを開く","Violations":0,"Warnings":0,"NotValuated":2,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"Browsable Intentを利用する","Violations":0,"Warnings":0,"NotValuated":1,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"LogCatにログ出力する","Violations":1,"Warnings":0,"NotValuated":1,"SafeTies":1,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"WebViewを使う","Violations":0,"Warnings":0,"NotValuated":2,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"Notificationを使う","Violations":0,"Warnings":0,"NotValuated":2,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"共有メモリを使う","Violations":0,"Warnings":0,"NotValuated":1,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"独自Permissionを定義する","Violations":5,"Warnings":4,"NotValuated":1,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"Permissionを利用する","Violations":0,"Warnings":0,"NotValuated":22,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"Account Managerに独自アカウントを追加する","Violations":0,"Warnings":1,"NotValuated":2,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"HTTPSで通信する","Violations":0,"Warnings":0,"NotValuated":3,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"プライバシー情報を扱う","Violations":0,"Warnings":2,"NotValuated":4,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0},"Category":"許可技術を利用する","Violations":1,"Warnings":0,"NotValuated":1,"SafeTies":0,"JudgeSafeTies":0,"AcceptedRisks":0}]}]
```

検査オプション

- 質問に対する以前の回答を引き継ぐ
- 前回の検査後にアプリのパッケージ名が変更されたので、変更前の検査結果の質問回答・ユーザー判断を引き継ぎたい。
- 「引き継ぎ元」を変更可能

検査オプション

質問に対する以前の回答を引き継ぐ

引き継ぎ元

以前に入力した回答をリセット

すべての回答を「未回答」にする

- 以前に入力した回答をリセットする
- 前回の検査結果の回答・ユーザー判断を引き継がない。

検査オプション

質問に対する以前の回答を引き継ぐ

引き継ぎ元

以前に入力した回答をリセットする

すべての回答を「未回答」にする

- すべての回答を「未回答」にする
- 前回の検査結果の回答・ユーザー判断を引き継がない。
- Secure Coding Checker の判断による初期回答も設定されない初期状態。

検査オプション

質問に対する以前の回答を引き継ぐ

引き継ぎ元

以前に入力した回答をリセットする

すべての回答を「未回答」にする

差分通知

- 差分通知
- コード上に差分が見つかった項目や、ユーザー判断済み項目の実装の変化を検知。
- 判断内容の変更、取り消しなどが必要か、再確認を促す。

The screenshot shows the application interface with the following elements:

- Navigation Bar:** Three buttons: "エビデンス出力" (Evidence Output), "検査履歴" (Inspection History), and "検査" (Inspection).
- Filter Settings:** Radio buttons for "最小" (Minimum), "標準" (Standard), and "すべて" (All). Below them are checkboxes for "差分通知" (Difference Notification) and "最終更新情報を表示" (Display Latest Update Information). A blue arrow points to the "差分通知" checkbox.
- Notification Panel:** A section titled "その他(注意すべき実装)" (Others (Implementation to be noted)) with a "質問事項" (Question Item) count of 1. It includes a "アプリ設定" (App Settings) section with a "安全" (Safety) button. A red-bordered box highlights a notification message: "質問回答時点(1回前の検査結果)からコード上に差分が見つかりました。質問回答に変更が必要無いか確認してください。" (At the time of the question answer, a difference was found in the code since the last inspection result. Please confirm if a change is necessary for the question answer.) A "確認" (Confirm) button is located to the right of the message. A blue arrow points to this notification box.

➤ DEMO

Apache Cordova

その他
(注意すべき実装) 1 ✓

補足情報



エビデンス出力 検査履歴 検査

最小 標準 すべて ?

差分通知 ?

最終更新情報を表示



+ - その他(注意すべき実装) 質問事項 1 0 0 0 1 0 0

アプリ設定

安全

質問回答時点(1回前の検査結果)からコード上に差分が見つかりました。
質問回答に変更が必要無いか確認してください。 確認



アプリケーション一覧



【履歴削除】

今月未検査のアプリは削除可能

- 検査履歴は月単位で管理しているため、検査実施月の翌月以降に削除可能です。
- 例)9月30日に検査した検査履歴は10月1日以降削除可能

最終検査日時	アプリケーション名	パッケージ名	
2022/09/12 14:50:52	ReferenceApp	com.example.referenceapp	検査履歴
2022/09/06 15:12:57	Droid Insight 360	com.vishtekstudios.droidinsight360	検査履歴

➤ 最新の検査結果を削除

ReferenceApp (com.example.referenceapp) 1 - 6 / 6

検査日時	バージョン	メモ		!	!	?	✓	✓	✓	
2022/09/05 09:50:21	1			23	24	78	3	0	0	検査結果
2022/09/05 09:41:20	1			23	24	78	3	0	0	検査結果
2022/09/02 17:20:02	1			23	24	78	3	0	0	検査結果
2022/09/01 16:08:44	1			23	24	78	3	0	0	検査結果
2022/09/01 16:07:18	1			23	24	79	2	0	0	検査結果
2022/08/31 15:21:32	1			23	24	79	2	0	0	検査結果

最新の検査結果を削除する

アプリ数とユーザー数の上限確認

- 1グループ当たりのアプリ数上限 と ユーザー数が確認できます。



プランの詳細

アプリ数上限/Gp	10
ユーザー	32
エビデンス出力	<input checked="" type="checkbox"/>
開発者がユーザー管理	<input checked="" type="checkbox"/>
グループ管理者	<input checked="" type="checkbox"/>
統計情報	<input type="checkbox"/>
アクセス制限	<input type="checkbox"/>
操作ログ	<input type="checkbox"/>
差分通知	<input checked="" type="checkbox"/>
サポート	<input type="checkbox"/>
Web API	<input checked="" type="checkbox"/>
契約失効日	< 2024-05-01 >

Cordova Android

- Cordova Androidアプリにも対応



APACHE
CORDOVATM

➤ Cordova Androidのバージョン

「Apache Cordova」に存在する脆弱性を確認、Androidアプリを簡単に改変できる恐れ

投稿日: 2015年6月5日

脅威カテゴリ: 脆弱性

執筆: Mobile Threats Analyst - Seven Shen

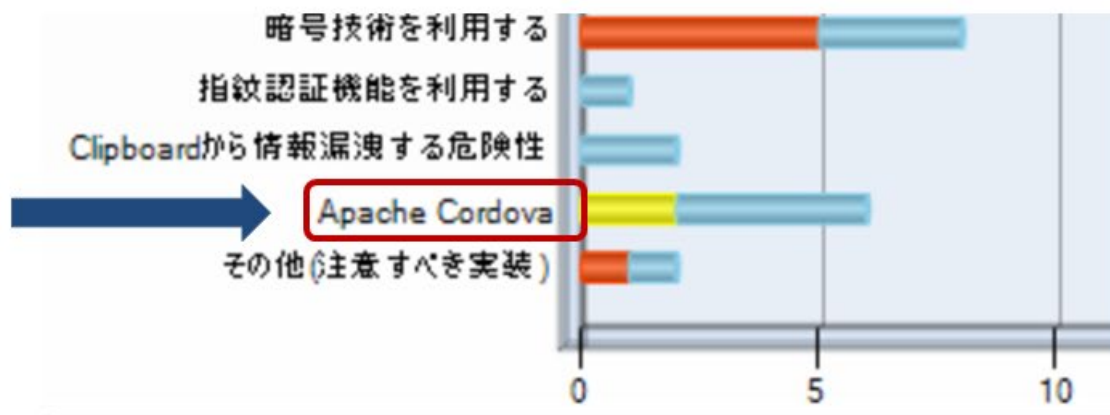
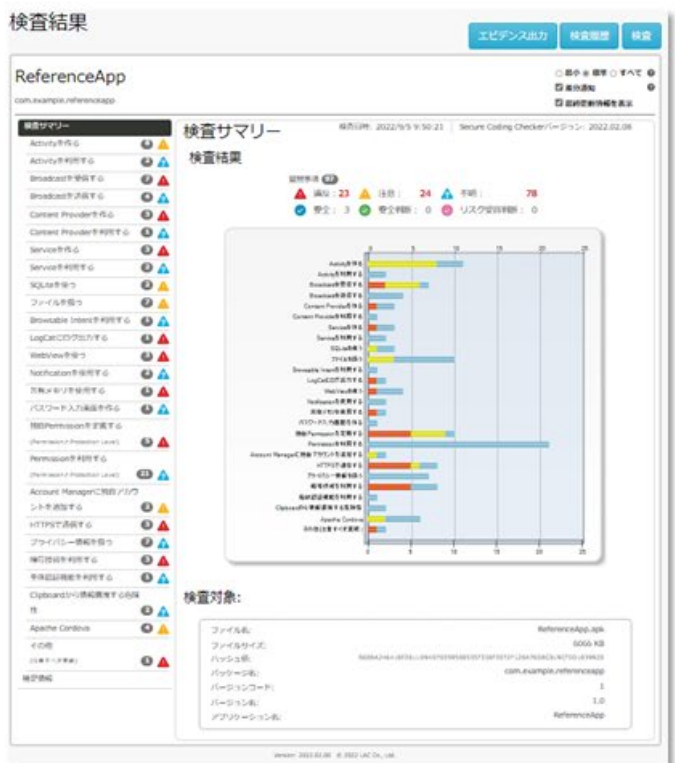
トレンドマイクロは、オープンソースモバイル開発フレームワーク「Apache Cordova」に存在する脆弱性を確認しました。攻撃者は、この脆弱性を利用することにより、被害者に攻撃コードを含んだWebページを閲覧させるだけで、アプリの動作を改変することが可能になります。この改変の範囲は、アプリのユーザを不愉快にさせるものから、アプリを完全に機能不全させるものまでに及びます。

この問題の脆弱性「CVE-2015-1835」は非常に深刻な脆弱性であり、Apache Cordova のバージョン 4.0.1.までのすべてのバージョンに影響を与えます。Apache は**セキュリティ情報**を公開して、この脆弱性を確認しました。Google の公式アプリストア「Google Play」の**全アプリの 5.6%** を占める Cordova をベースにしたアプリの大半がこの脆弱性を利用した攻撃を受ける可能性があります。

<http://blog.trendmicro.co.jp/archives/11622>

- その他のApache Cordova検査項目
 - ・ 新しいWebViewを使う
 - ・ InAppBrowserを使う
 - ・ Content Security Policy
 - ・ Whitelists - access要素
 - ・ Whitelists - allow-intent要素
 - ・ Whitelists - allow-navigation要素

▶ DEMO



管理者向け機能

- グループ管理者
- 指定ライブラリの検査対象外設定
- 二段階認証

グループ管理者

➤ 【グループ管理者】

- 自他のユーザー権限の変更や、グループ管理者の追加が可能。
- 既定では、グループの最初のユーザー。

グループ名	グループ ID	ユーザー名
プロジェクトA	A1.-_	user1

The screenshot shows a user management interface. A dropdown menu is open for the user 'user1'. The menu items are:

- グループ管理者
- アカウント管理
- 検査結果の閲覧
- 回答
- 検査
- 新規アプリ検査
- 最新検査結果の削除
- 検査履歴の削除

At the bottom of the menu is a blue button labeled '保存' (Save). To the right of the menu, a blue arrow points to a panel with three orange buttons: '削除' (Delete), 'パスワード再設定' (Reset Password), and 'ユーザー権限' (User Permissions).

▶ DEMO

ユーザー▼ 設定▼ ヘルプ▼

- グループ一覧
- グループ追加
- 開発者アカウント一覧**
- グループ・開発者アカウントアップロード
- 既定のユーザー権限

- アカウント一覧
- アカウント追加
- パスワード変更



グループ名	グループ ID	ユーザー名	サインイン	
プロジェクトA	A1.-_	user1		<ul style="list-style-type: none">削除パスワード再設定ユーザー権限



- グループ管理者
- アカウント管理
- 検査結果の閲覧
- 回答
- 検査
- 新規アプリ検査
- 最新検査結果の削除
- 検査履歴の削除

保存

指定ライブラリの検査対象外設定

- 検査結果に表示させたくない第三者ライブラリを指定する
「サードパーティソフトウェア一覧」で設定可能（管理者機能）

追加

サードパーティソフトウェアのパッケージ名

パッケージ名 androidx.appcompat.app

検査対象外

作成

追加

パッケージ名

androidx.appcompat.app

検査対象外

変更

削除

➤ [検査対象外]と指定したライブラリが検査結果に表示されなくなる

アプリに呼び出し起点が見つからないコード	Line
androidx.appcompat.app.AppCompatActivity#setDefaultNightMode(int)	559
androidx.appcompat.app.AppCompatActivity#setNightMode(int)	2420
androidx.appcompat.app.AppCompatActivity#twilightManager#getLastKnownLocationForProvider(String)	138
androidx.appcompat.widget.ResourceManagerInternal#tintDrawable(Drawable,TintInfo,int[])	453
androidx.appcompat.widget.ViewUtils#<clinit>()	50
androidx.appcompat.widget.ViewUtils#computeFitSystemWindows(View,Rect,Rect)	70
androidx.appcompat.widget.ViewUtils#makeOptionalFitsSystemWindows(View)	94
androidx.appcompat.widget.ViewUtils#makeOptionalFitsSystemWindows(View)	92
androidx.appcompat.widget.ViewUtils#makeOptionalFitsSystemWindows(View)	90
androidx.core.app.NotificationManagerCompat\$SideChannelManager#onServiceConnected(ComponentName)	548
androidx.core.app.NotificationManagerCompat\$SideChannelManager#onServiceDisconnected(ComponentName)	558
androidx.core.app.NotificationManagerCompat\$SideChannelManager#processListenerQueue(NotificationCompat\$NotificationCompatAction)	675
androidx.core.app.NotificationManagerCompat\$SideChannelManager#processListenerQueue(NotificationCompat\$NotificationCompatAction)	694
androidx.core.app.NotificationManagerCompat\$SideChannelManager#processListenerQueue(NotificationCompat\$NotificationCompatAction)	700

Total Items: 49



アプリに呼び出し起点が見つからないコード	Line
androidx.appcompat.widget.ResourceManagerInternal#tintDrawable(Drawable,TintInfo,int[])	453
androidx.appcompat.widget.ViewUtils#<clinit>()	50
androidx.appcompat.widget.ViewUtils#computeFitSystemWindows(View,Rect,Rect)	70
androidx.appcompat.widget.ViewUtils#makeOptionalFitsSystemWindows(View)	94
androidx.appcompat.widget.ViewUtils#makeOptionalFitsSystemWindows(View)	92
androidx.appcompat.widget.ViewUtils#makeOptionalFitsSystemWindows(View)	90
androidx.core.app.NotificationManagerCompat\$SideChannelManager#onServiceConnected(ComponentName)	548
androidx.core.app.NotificationManagerCompat\$SideChannelManager#onServiceDisconnected(ComponentName)	558
androidx.core.app.NotificationManagerCompat\$SideChannelManager#processListenerQueue(NotificationCompat\$NotificationCompatAction)	675
androidx.core.app.NotificationManagerCompat\$SideChannelManager#processListenerQueue(NotificationCompat\$NotificationCompatAction)	694
androidx.core.app.NotificationManagerCompat\$SideChannelManager#processListenerQueue(NotificationCompat\$NotificationCompatAction)	700
androidx.core.app.NotificationManagerCompat\$SideChannelManager#scheduleListenerRetry(NotificationCompat\$NotificationCompatAction)	663
androidx.core.app.NotificationManagerCompat\$SideChannelManager#updateListenerMap()	594
androidx.core.app.NotificationManagerCompat\$SideChannelManager#updateListenerMap()	606

Total Items: 46

▶ DEMO

アプリに呼び出し起点が見つからないコード	Line
androidx.appcompat.app.AppCompatActivity#setDefaultNightMode(int)	559
androidx.appcompat.app.AppCompatActivity#isActivityManifestHandlingUiMode()	2420
androidx.appcompat.app.AppCompatActivity#getLastKnownLocationForProvider(String)	138
androidx.appcompat.widget.ResourceManagerInternal#tintDrawable(Drawable,TintInfo,int[])	453
androidx.appcompat.widget.ViewUtils#<clinit>()	50
androidx.appcompat.widget.ViewUtils#computeFitSystemWindows(View,Rect,Rect)	70
androidx.appcompat.widget.ViewUtils#makeOptionalFitsSystemWindows(View)	94
androidx.appcompat.widget.ViewUtils#makeOptionalFitsSystemWindows(View)	92
androidx.appcompat.widget.ViewUtils#makeOptionalFitsSystemWindows(View)	90
androidx.core.app.NotificationManagerCompat\$SideChannelManager#onServiceConnected(ComponentName,String,Intent)	548
androidx.core.app.NotificationManagerCompat\$SideChannelManager#onServiceDisconnected(ComponentName,String,Intent)	558
androidx.core.app.NotificationManagerCompat\$SideChannelManager#processListenerQueue(NotificationCompat\$Notification)	675
androidx.core.app.NotificationManagerCompat\$SideChannelManager#processListenerQueue(NotificationCompat\$Notification)	694
androidx.core.app.NotificationManagerCompat\$SideChannelManager#processListenerQueue(NotificationCompat\$Notification)	700

Total Items: 49



変更

サードパーティソフトウェアのパッケージ名

パッケージ名

検査対象外

保存

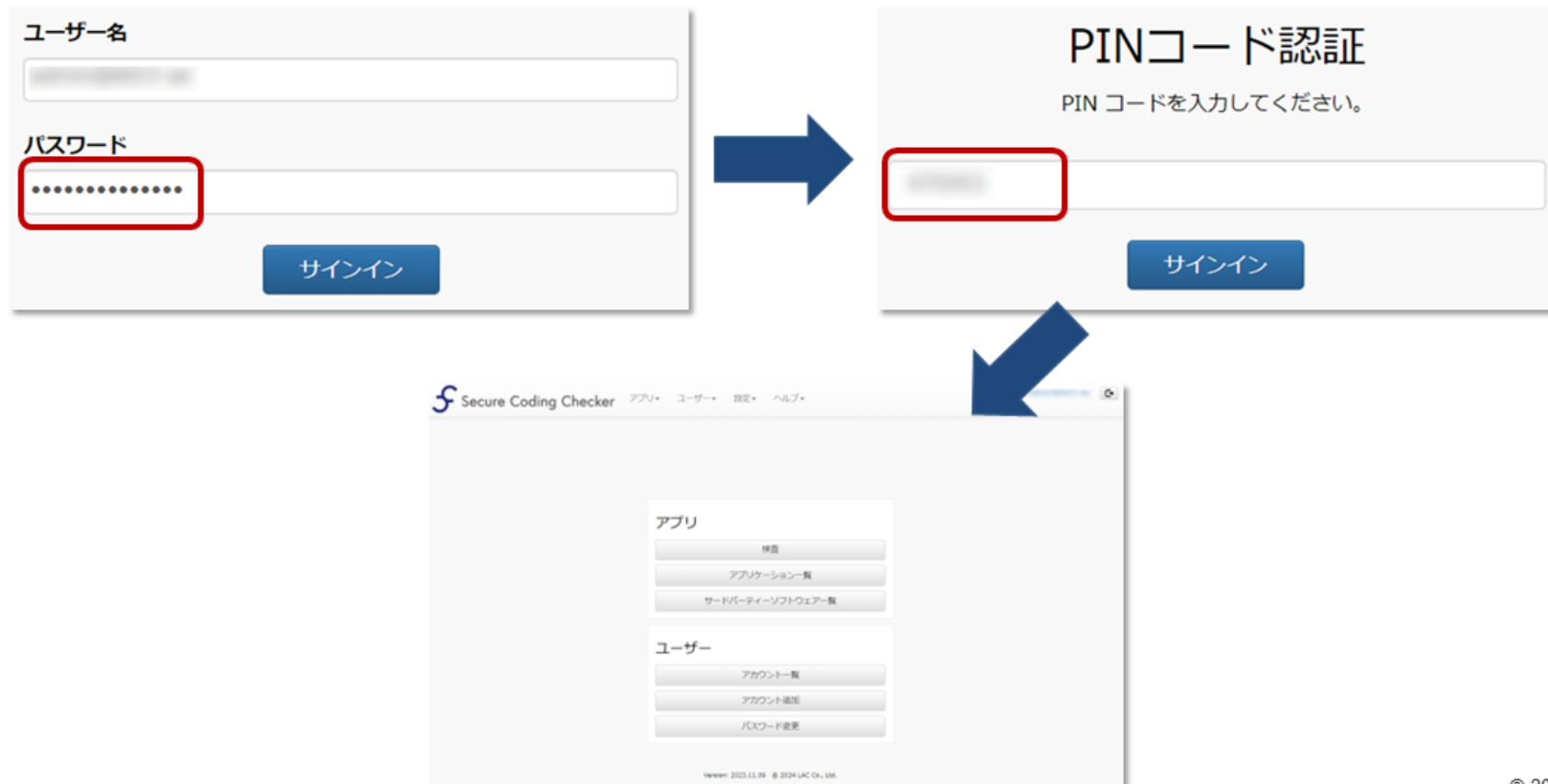


アプリに呼び出し起点が見つからないコード	Line
androidx.appcompat.widget.ResourceManagerInternal#tintDrawable(Drawable,TintInfo,int[])	453
androidx.appcompat.widget.ViewUtils#<clinit>()	50
androidx.appcompat.widget.ViewUtils#computeFitSystemWindows(View,Rect,Rect)	70
androidx.appcompat.widget.ViewUtils#makeOptionalFitsSystemWindows(View)	94
androidx.appcompat.widget.ViewUtils#makeOptionalFitsSystemWindows(View)	92
androidx.appcompat.widget.ViewUtils#makeOptionalFitsSystemWindows(View)	90
androidx.core.app.NotificationManagerCompat\$SideChannelManager#onServiceConnected(ComponentName,String,Intent)	548
androidx.core.app.NotificationManagerCompat\$SideChannelManager#onServiceDisconnected(ComponentName,String,Intent)	558
androidx.core.app.NotificationManagerCompat\$SideChannelManager#processListenerQueue(NotificationCompat\$Notification)	675
androidx.core.app.NotificationManagerCompat\$SideChannelManager#processListenerQueue(NotificationCompat\$Notification)	694
androidx.core.app.NotificationManagerCompat\$SideChannelManager#processListenerQueue(NotificationCompat\$Notification)	700
androidx.core.app.NotificationManagerCompat\$SideChannelManager#scheduleListenerRetry(NotificationCompat\$Notification)	663
androidx.core.app.NotificationManagerCompat\$SideChannelManager#updateListenerMap()	594
androidx.core.app.NotificationManagerCompat\$SideChannelManager#updateListenerMap()	606

Total Items: 46

二段階認証

➤ 二段階認証によるログイン



▶ DEMO

アカウント一覧

検索条件
検索アカウント名

ユーザー名	サインイン	操作
_apl.scc.lac.co.jp		詳細 二段階認証の有効化



.....scc.lac.co.jp の内容

選択したアカウントの二段階認証情報を有効化します。
よろしいですか？


OK キャンセル

二段階認証

認証アプリを使用して、下記のQRコードをスキャンしてください。

- お使いのスマートフォンで、AppStore もしくは Google Play で Google Authenticator アプリをインストールします。
- Google Authenticator アプリを起動し、下記 QR コードをスキャンして登録します。
- 登録が完了したら、下記の完了ボタンをクリックします。
- 認証コードの入力欄が表示されますので、Google Authenticator に表示された 6桁の数字を入力します。

※機種変更時は、管理者により二段階認証情報をリセットする必要がありますのでご注意ください。



セットアップキー:

OK

PINコード認証

PIN コードを入力してください。

サインイン

Secure Coding Checker

アプリ

- 詳細
- アプリケーション情報
- サードパーティバイナリ/ライブラリ情報

ユーザー

- アカウント情報
- アカウント検索
- パスワード管理

オプション機能

- アプリ発注先管理機能
 - 1 アカウント・複数グループ
 - 開発者グループの無効化と削除
 - 閲覧者アカウント
 - 統計情報
 - 開発者アカウントの管理（オプション）
- WebAPI機能
 - 検査Web API
- セキュリティパック
 - 操作ログ
 - IPアクセス制限（管理者・開発者）

アプリ発注先管理機能

- 複数のグループを作成でき、ユーザーは他のグループの検査結果を見られません。
- ユーザーは複数のグループに所属することが可能で、現在のグループを切り替えて使うことができます。
- 管理者はすべてのユーザーの検査結果を見ることができます。
- 管理者グループと開発者グループの両方に所属することも可能です。

[アプリ発注先管理機能]

1アカウント・複数グループ

1アカウント・複数グループ

➤ 他グループのユーザーを自分の開発者グループに参加させる

開発者ユーザー名を入力

この開発者はサインインしたままグループを切り替えて利用可能になる

管理者ユーザー名を入力

この管理者はサインインしたまま管理者・開発者を切り替えて利用可能になる

グループ情報
グループ名 プロジェクトA
グループID Lac_ex

既存アカウント
既存ユーザー名

新規アカウント
新規ユーザー名 ユーザー名にグループ名を付加
ex: user, user@Lac_ex, user@example.com

パスワード パスワード自動生成
※パスワードは8文字以上32文字以内、英数字記号(@_!)を使用してください。

パスワード (確認入力)

有効化 キャンセル

DevGroup (DevGroup1) ▾

管理者
プロジェクトA (A1.-_)
プロジェクトA (Lac_ex)
DevGroup (DevGroup1)

1アカウント・複数グループ

- 開発者に管理者権限を追加する
管理者権限を追加したい開発者ユーザー名を入力

アカウント追加

既存アカウント

既存ユーザー名

新規アカウント

新規ユーザー名

パスワード パスワード自動生成

パスワード (確認入力)

開発者を作成する

追加 キャンセル

既存の開発者を管理者としても利用可能にします。

新しく管理者を作成します。

※パスワードは8文字以上32文字以内、英数字記号(@_!)を使用してください。

この開発者はサインインしたまま管理者・開発者を切り替え利用可能に

管理者

管理者

プロジェクトA (A1.-_)

プロジェクトA (Lac_ex)

DevGroup (DevGroup1)

1アカウント・複数グループ

▶ DEMO

グループ情報
グループ名 プロジェクトA
グループID Lac_ex

既存アカウント
既存ユーザー名

新規アカウント
新規ユーザー名 ユーザー名にグループ名を付加
ex: user, user@Lac_ex, user@example.com
パスワード パスワード自動生成
※パスワードは8文字以上32文字以内、英数字記号(@_/)を使用してください。
パスワード (確認入力)

他グループのユーザーをこのグループに追加します。

アカウント追加

既存アカウント
既存ユーザー名

新規アカウント
新規ユーザー名
ex: user, user@example.com

パスワード パスワード自動生成
※パスワードは8文字以上32文字以内、英数字記号(@_/)を使用してください。

パスワード (確認入力)

隠匿者を作成する

既存の開発者を管理者としても利用可能にします。

新しく管理者を作成します。

DevGroup (DevGroup1) ▾

管理者
プロジェクトA (A1.-_)
プロジェクトA (Lac_ex)
DevGroup (DevGroup1)

管理者 ▾

管理者
プロジェクトA (A1.-_)
プロジェクトA (Lac_ex)
DevGroup (DevGroup1)

[アプリ発注先管理機能] 開発者グループの無効化と削除

➤ グループの無効化

- グループにサインインできなくなる
(所属アカウントは所属を解除される)
- 管理者向けに検査結果は残る
- 有効化で利用再開

➤ グループの削除

- 最後の検査が先月以前の無効グループ
- グループの検査結果も**削除**

グループ ID	
LAC.ex	検査履歴
	統計情報
	有効化
	削除
Lac_ex	検査履歴
	統計情報
	アカウント一覧
	アカウント追加
	無効化

➤ DEMO



グループ ID	
LAC.ex	<ul style="list-style-type: none">検査履歴統計情報有効化削除
Lac_ex	<ul style="list-style-type: none">検査履歴統計情報アカウント一覧アカウント追加無効化

[アプリ発注先管理機能] 閲覧者アカウント

➤ 閲覧者ができること

- 全グループの検査結果を閲覧
- 自分のパスワード変更

既存アカウント

既存ユーザー名

新規アカウント

新規ユーザー名

パスワード パスワード自動生成

※パスワードは8文字以上32文字以内、英数字記号(@_!)を使用してください。

パスワード (確認入力)

閲覧者を作成する

追加 キャンセル

▶ DEMO

アプリ▼ ユーザー▼ 設定▼ ヘルプ▼

- グループ一覧
- グループ追加
- 開発者アカウント一覧
- グループ・開発者アカウントアップロード
- 既定のユーザー権限
- アカウント一覧
- アカウント追加**
- パスワード変更

既存アカウント
既存ユーザー
新規アカウント
新規ユーザー



既存アカウント

既存ユーザー名

新規アカウント

新規ユーザー名

ex: user, user@example.com

パスワード パスワード自動生成

※パスワードは8文字以上32文字以内、英数字記号(@_!)を使用してください。

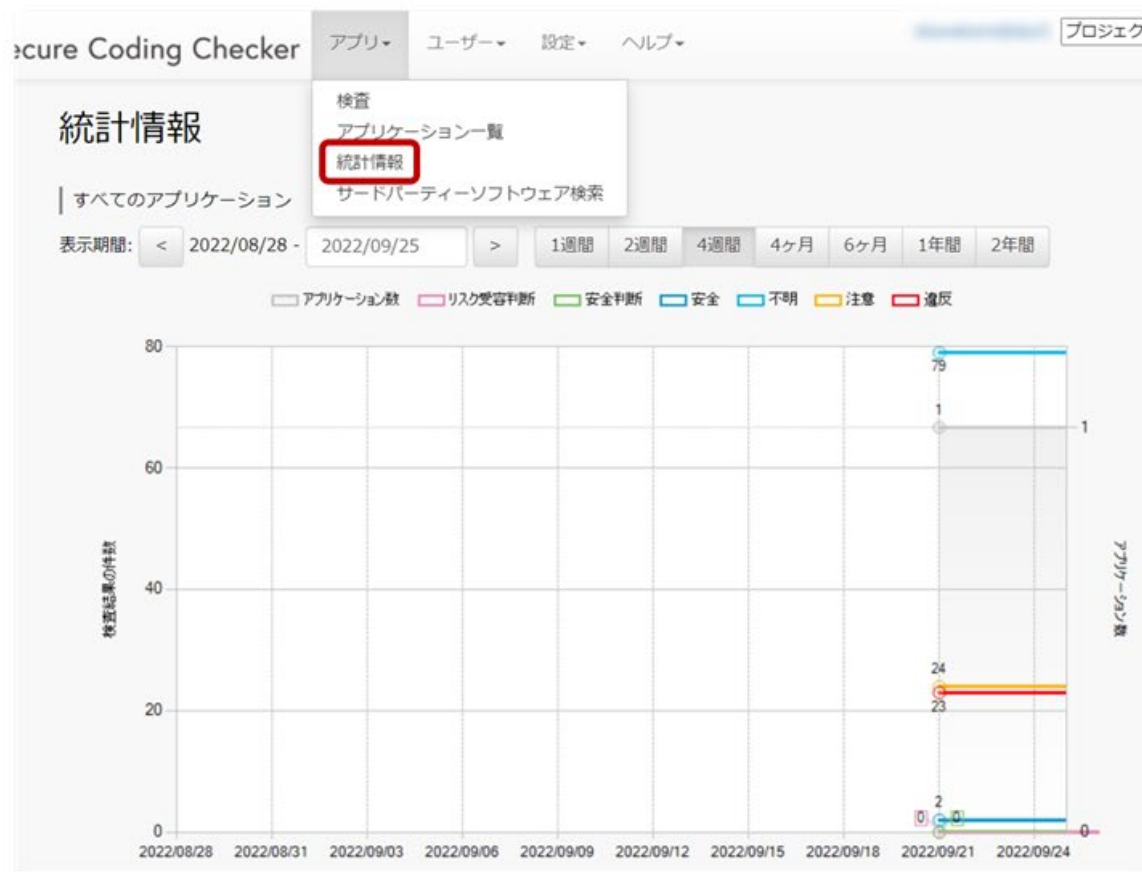
パスワード (確認入力)

閲覧者を作成する

追加 キャンセル

[アプリ発注先管理機能] 統計情報

➤ 検査結果の推移をグラフ表示する



[アプリ発注先管理機能]

開発者アカウントの管理 (オプション)

開発者アカウントの管理（オプション）

- アプリ発注先管理機能を適用したプランでは、開発者アカウントの管理を管理者が行うようにすることもできます。

グループ ID	
Lac_ex	検査履歴
	統計情報
	アカウント一覧
	アカウント追加
	無効化
A1.-_	検査履歴
	統計情報
	アカウント一覧
	アカウント追加
	無効化



グループ名	グループ ID	ユーザー名	サインイン	
プロジェクトA	A1.-_	user1		削除 パスワード再設定 ユーザー権限

➤ DEMO

ユーザー▼ 設定▼ ヘルプ▼

- グループ一覧
- グループ追加
- 開発者アカウント一覧**
- グループ・開発者アカウントアップロード
- 既定のユーザー権限

- アカウント一覧
- アカウント追加
- パスワード変更



グループ ID	
Lac_ex	<ul style="list-style-type: none"> 検査履歴 統計情報 アカウント一覧 アカウント追加 無効化
A1.-_	<ul style="list-style-type: none"> 検査履歴 統計情報 アカウント一覧 アカウント追加 無効化



グループ名	グループ ID	ユーザー名	サインイン	
プロジェクトA	A1.-_	user1		<ul style="list-style-type: none"> 削除 パスワード再設定 ユーザー権限

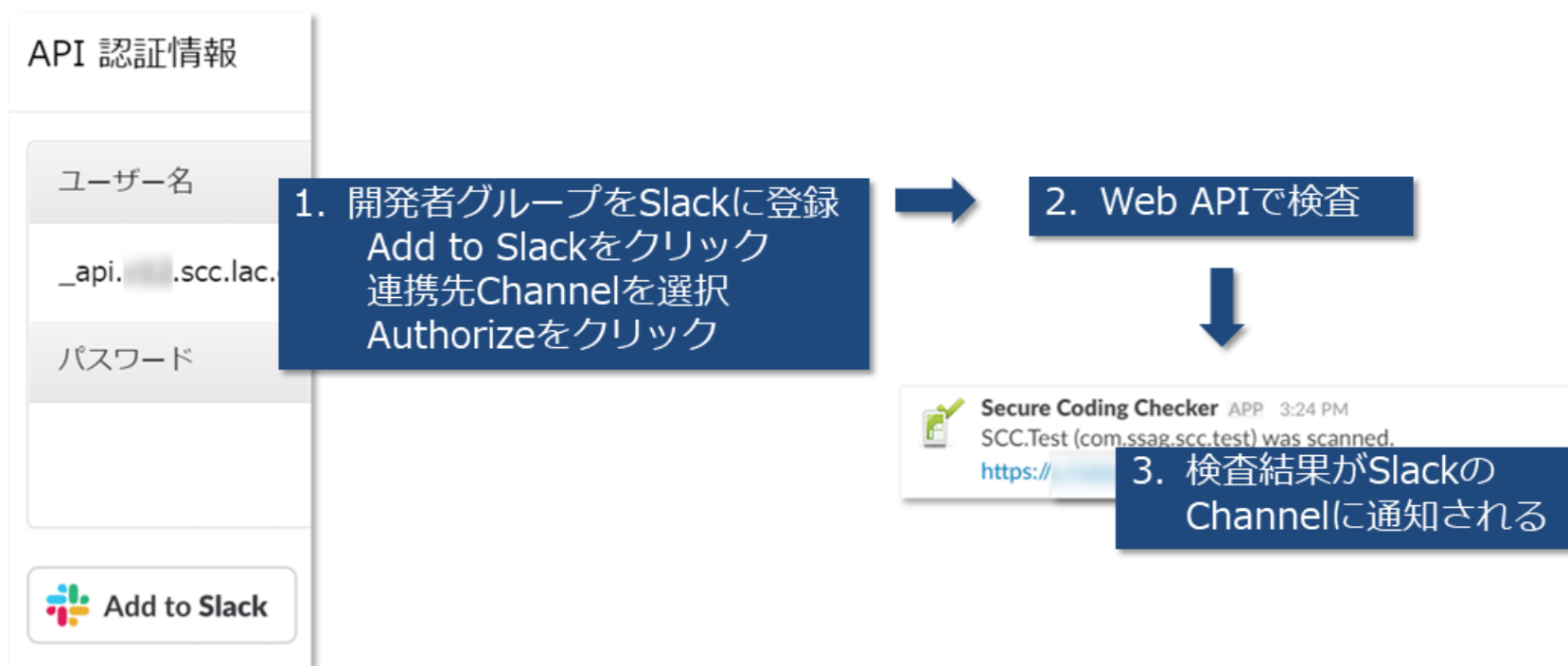
WebAPI機能

- 有効になると、ヘルプページにWeb APIの使い方が追加されます。
- APKファイルをSCCに POSTすると、検査が行われます。
- 検査履歴など、他の検査結果と同様に扱われます。

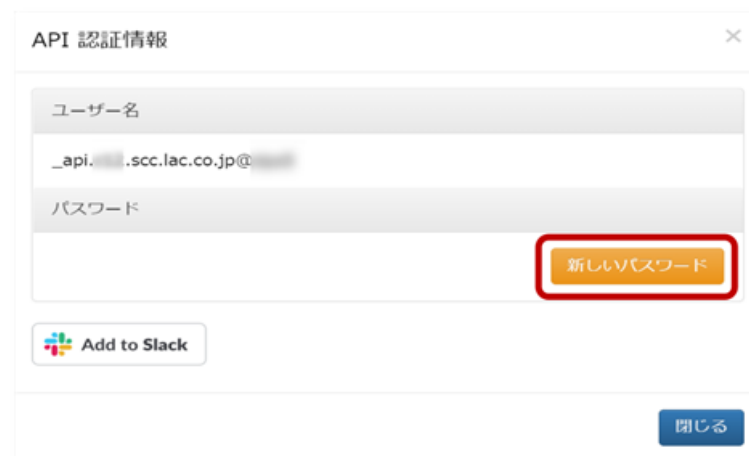
例) curlコマンド

```
curl -u "_api.xxx.scc.lac.co.jp@abc123:passw0rd." -F  
"file=@ReferenceApp.apk" -F "lang=en" https://xxx.scc.lac.co.jp/api/scan
```

- Slackと連携させることで、検査Web APIでアプリ検査時、検査結果画面の直URLをSlackに通知します。



➤ DEMO



```
C:\Users\%Users% >curl -u "_api. scc.lac.co.jp@" -F "file=@C:\Users%\Documents\ReferenceApp.apk" -F "lang=en https:// scc.lac.co.jp/api/scan"
{"Success":true,"ErrorMessage":null,"Url":"https:// scc.lac.co.jp/ScanResult/Detail/356","ScannedDateTime":"2022-09-1
```

```
{"Success":true,"ErrorMessage":null,"Url":"https:// scc.lac.co.jp/Content/icons/checkp3.png"}}, {"Detailings":0,"NotEvaluated":2,"Safeties":0,"JudgedSafeties":0,"Violations":0,"Warnings":0,"NotEvaluated":1,"Safeties":0}, {"Category":"Info Leakage from Clipboard","Violatio
```


➤ アカウント管理権限を外すと、API認証情報が表示されなくなります。



- アカウント管理者が一人しかいない場合、そのユーザーの「アカウント管理」権限を削除できません。

ユーザー権限の変更に失敗しました。

ユーザー権限を変更するとグループ管理者が存在しなくなるため、変更できません。グループ内の最低一人のユーザーにグループ管理者権限を付与してください。

OK

セキュリティパック

[セキュリティパック] 操作ログ

- 表示期間・グループ・ユーザー名・操作・操作結果・IPから、操作ログを表示させることができます。

The screenshot shows the application's navigation menu on the left with '操作ログ' highlighted in a red box. A blue arrow points to the '操作ログ' page on the right. The page features a search and filter section with the following fields:

- 表示期間: [] - []
- グループ: (すべて) [v]
- ユーザー名: (すべて) [v]
- 操作: (すべて) [v]
- IP: []

Below the filters is a pagination control showing '1 - 30 / 2540'.

日時	ユーザー名	グループID	IP アドレス	操作	操作結果
2024/01/11 17:41:13	[]	[]	[]	サインイン	OK
2024/01/11 15:54:23	[]	[]	[]	サインアウト	OK

サインイン	アプリ検査	ユーザー権限
サインアウト	パスワード変更	既存アカウント追加
アカウント登録	パスワード変更を忘れたら	既存メール付きアカウント追加
メール付きアカウント登録	パスワード再設定	グループ切り替え
開発者アカウント登録	メール確認	アカウント除外
グループ登録	メール差出人の編集	一括登録
アカウント削除	メールアドレス変更	
グループ作成	新しいメールアドレスの確認	

[セキュリティパック] IPアクセス制限(管理者・開発者)

IPアクセス制限(管理者・開発者)

アプリ ユーザー 設定 ヘルプ

ユーザー

- 管理者アクセス制限
- 開発者アクセス制限
- 日本語 (ja-JP)

開発者アカウント一覧

グループ・開発者アカウントアップロード

アカウント一覧

アカウント追加

パスワード変更

設定

- 管理者アクセス制限
- 開発者アクセス制限

管理者アクセス制限

作成

開始IPアドレス

終了IPアドレス

メモ

アクセス制限されていません。アクセスを許可するIPアドレス範囲を設定できます。

管理者アクセス制限

許可される IP アドレス範囲

開始IPアドレス

終了IPアドレス

メモ

作成

管理者アクセス制限

以下のIPアドレス範囲からアクセスできます。

作成

開始IPアドレス	終了IPアドレス	メモ		
192.168.1.1	192.168.1.255		変更	削除
192.168.1.1	192.168.1.255		変更	削除

現在のクライアントIPアドレスが含まれていない場合、エラーが表示される。

現在のクライアントIPアドレスが許可される必要があります。



※本資料は作成時点の情報に基づいており、記載内容は予告なく変更される場合があります。

※本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。

※本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。

※ LAC、ラック、Secure Coding Checkerは株式会社ラックの登録商標です。その他記載されている会社名、製品名は一般に各社の商標または登録商標です。