NRI グループからのお知らせ

Notification from NRI Group

Nomura Research Institute Group

2019 年 12 月 18 日

NRI セキュアテクノロジーズ株式会社

# NRI セキュア、「API セキュリティ診断」サービスを刷新

## ～ OAuth2.0、OpenID Connect、FAPI などの標準フレームワークに対応 ～

NRI セキュアテクノロジーズ株式会社（以下「NRI セキュア」）は、企業の情報システムやクラウドサービスなどで急速に普及しつつある API（Application Programming Interface）[1]について、情報セキュリティの一層の確保を図るため、このたび「API セキュリティ診断」サービス（以下「本サービス」）を刷新し、提供内容を拡充します。

デジタルビジネスを推進するにあたり、企業が API を利用して、自社の Web サービスの機能を外部に公開したり、他システムと連携させたりすることで、自社サービスの価値向上や提供範囲の拡大を図る動きが増えています。

一方で、API は従来の Web アプリケーションとは異なり、画面上の挙動だけではなく、背後で動く API の要素技術や仕組みを把握した上で、セキュリティ対策を行うことが求められます。また、API を外部に公開する場合は、API の利用を他者に認可するフローに不備があると、気づかないうちにセキュリティ上の問題が発生していることもあります。

NRI セキュアは、2016 年より本サービスを開始し、様々なシーンで利用されている API について、セキュリティ診断と対策の実行を数多く支援してきました。そのため、API で用いられる技術を実装レベルで熟知した技術者が、API の利用例や連携先の外部サービスなど、案件ごとの特性を踏まえて、セキュリティ上の問題点を洗い出したり有効な対策を推奨したりすることが可能です。

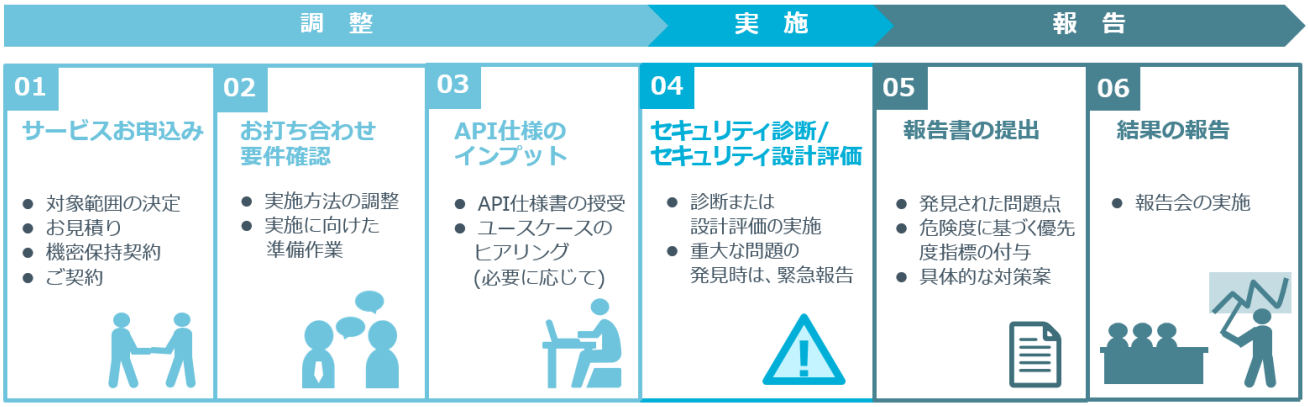
今回、API 仕様書やシステム構成図を元に、机上で評価する「API セキュリティ設計レビュー」を新たに加え、疑似攻撃を通じてセキュリティ上の問題点を洗い出す「API セキュリティ診断」とあわせて、2 つのメニューを用意しました。

本サービスでは、認可・ID 連携の標準フレームワークである「OAuth2.0」[2]と「OpenID Connect」[3]に、NRI セキュア独自の観点を加えた診断項目を基に評価します。「REST」[4]、「GraphQL」[5]といった API 特有

の仕様を採用している場合や、サーバレス[6]及びマイクロサービス[7]などの実行環境を用いる場合も、診断が可能です。

また、金融システム向けの API セキュリティ要件である、FAPI（Financial-grade API）[8]で定められた要件に基づき、診断対象となる API のセキュリティプロファイルを評価する、「FAPI セキュリティプロファイル評価オプション」[9]を提供します。

図：サービスご提供フロー




本サービスの詳細は、下記の Web サイトからご覧いただけます。

https://www.nri-secure.co.jp/service/assessment/api

NRI セキュアは、今後も企業・組織の情報セキュリティ対策を支援するさまざまな製品・サービスを提供し、社会における安全・安心なデジタルトランスフォーメーション（DX）の推進に貢献していきます。

---

[1] API（Application Programming Interface）：

プログラムの特定の機能を、その他のプログラムでも利用できるようにしたもの。

[2] OAuth2.0：

OAuth とは、Web サービスの連携において、外部からのデータやサービスに対するアクセスを、利用者の同意に基づいて認可するためのフレームワークであり、2.0 が最新バージョン（2019 年 12 月時点）。OAuth に対応したサービス間の連携では、利用者が外部サービスに ID やパスワードを漏らすことなく、必要最低限のアクセス権限のみを委譲することができる。

[3] OpenID Connect：

Web サービスサイト間で、ユーザの同意に基づき、ID 情報を流通させるための標準フレームワーク。ユーザは OpenID Connect 対応サイトに登録した ID 情報を使って、他の OpenID Connect 対応サイトにログインすることが可能となる。

[4] REST：

外部から特定のプログラムを呼び出す際に使われる、API の規格の一つ。

[5] GraphQL：

サーバからデータを取り出すための API 用言語。

[6] サーバレス：

クラウドサービスを利用しているシステムにおいて、クラウド事業者が、事前にサーバリソースを割り当てることなく、任意のイベントをトリガーにリソースを割り当て、コード実行を行うこと。

[7] マイクロサービス：

アプリケーションをサービスや機能などで細かく分割して開発する手法のこと。

[8] FAPI（Financial-grade API）：

米国 OpenID Foundation の FAPI Working Group により検討されている金融機関向けの API 要件のこと。現時点では、まだドラフトの段階で完成はしていないものの、OAuth2.0 の拡張仕様の策定を牽引している OpenID Foundation が推進していることもあり、今後の金融業界における API のセキュリティ要件のスタンダードとなる可能性が高い。金融機関は、自社の API に FAPI の要求仕様を採り入れることで、より高度なセキュリティを確保できるとともに、金融業界の API エコシステムに適合しやすい仕様になることが期待できる。

[9] 「FAPI セキュリティプロファイル評価オプション」：

NRI セキュアのこのオプションでは、FAPI Part1（Read Only API）、FAPI Part2（Read & Write API）の観点からの診断のほか、認可フローに CIBA（OpenID Connect Client Initiated Backchannel Authentication Flow）を利用したプロファイルの評価にも対応している。

**【お知らせに関するお問い合わせ先】**

NRI セキュアテクノロジーズ株式会社　広報担当

TEL：03-6706-0622　E-mail：info@nri-secure.co.jp

## 【ご参考】

NRI セキュアの API 関連サービス一覧（点線で囲んだ部分が、今回拡充したサービスの範囲）