



Nomura Research Institute Group

2020年11月26日

NRI セキュアテクノロジーズ株式会社

NRI セキュア、「セキュアアプリケーション設計レビュー」

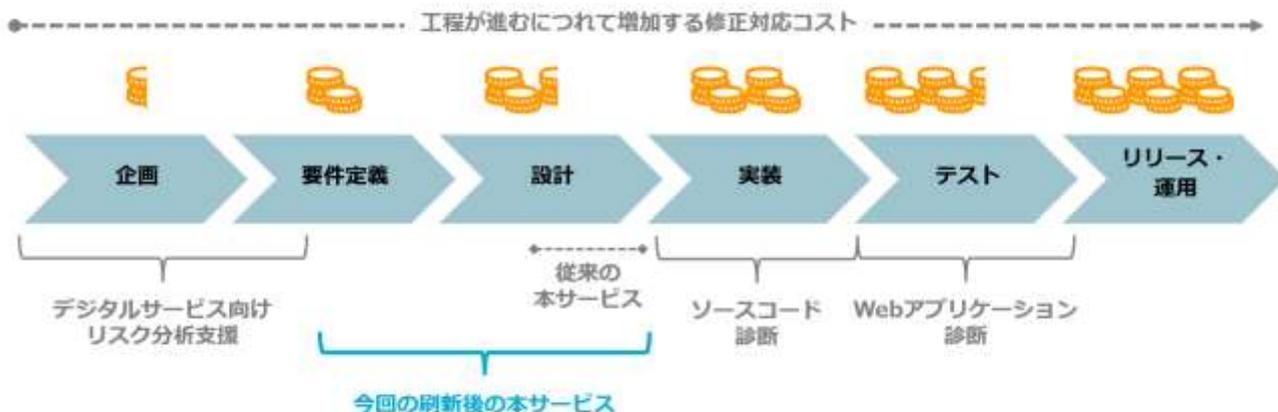
サービスを刷新し、DX のセキュリティを確保

～ 上流工程でセキュリティ要件を組み入れる「シフトレフト」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、アプリケーションをセキュリティの観点からレビューし、改善策を提案するサービス「セキュアアプリケーション設計レビュー（以下「本サービス」）」を刷新し、本日提供を開始します。

このたびの刷新では、DX（デジタルトランスフォーメーション）時代に開発される、Web アプリケーションなどのセキュリティレベル向上に主眼を置き、従来、完成した設計書に対して行っていた設計レビューを、要件定義・設計段階などの上流工程で行う「シフトレフト」¹に対応しました。セキュリティ上の問題点を早期に洗い出すことにより、リリース直前の手戻りや、サービス開始後の情報漏洩および不正アクセス等のセキュリティインシデント（事件・事案）が発生することを防止します。

図：本サービスおよび周辺サービスの対象と、手戻り発生時の修正対応コストの関係



■ 開発の上流工程におけるセキュリティ確保の重要性

DXの進展に伴い、IT（情報技術）を活用したデジタルサービスの開発が盛んになる一方で、これまでITを専門としていなかった部門がサービスを企画し、新しい要素技術²を採用したり、サービス開始を急ぐあまり開発を突貫で進めてしまったりするケースも増加しています。こういった状況では、セキュリティリスクが残ったままサービスが提供され、以下のようなインシデントやスケジュールの遅延が生じ、結果として企業のレピュテーションの低下や修正対応コストの増大を招く恐れがあるため、要件定義や設計を行う上流工程からセキュリティを考慮し、対策を行うことが一層重要となっています。

- リリース直前のテストで、要件定義・設計段階で考慮漏れとなったサービス仕様の課題や、要素技術の誤用に起因する脆弱性が見つかり、それらの修正対応のためにサービス開始を延期
- 機能追加により潜在リスクが顕在化したか、気づかないままリリースし、個人情報漏洩
- サービス仕様の隙を突いたサイバー攻撃により、サービスの不正利用などの重大事故が発生

■ 本サービスの特長

1. 要件定義・設計段階からセキュリティを考慮

本サービスでは、NRI セキュアの専門家が Web アプリケーションの設計資料を評価し、担当者へのヒアリングを実施することにより、セキュリティ上の課題を早い段階で洗い出します。これにより、サービス仕様上の問題とアプリケーションの脆弱性が重なることで、初めてリスクとして顕在化するケースなども見つけ出すことができます。

また、設計書がまだ作成されていない要件定義の段階においても、担当者へのヒアリングや設計会議への参加を通じて、セキュリティの観点からレビューを行うことが可能です。

2. 独自のヒアリングシートによる、問題抽出の網羅性・効率性の拡充

開発ベンダごとに書式や記載内容が異なる設計資料には、セキュリティ上の課題が明文化されていないものも多く、資料を確認するだけでは課題を見逃してしまう危険があります。NRI セキュアでは、これまで行ってきた数多くのセキュリティ診断や各種設計書のレビューで培った知見を集約し、独自のヒアリングシートを新たに作成しました。これを用いて、設計時に考慮すべき観点をひとつひとつ確認し、問題点を抽出します。

また、上流工程の評価では、複数回のヒアリングを行うことが一般的ですが、本サービスではセキュリティ診断の専門家が設計資料を事前に分析し、観点として抜けている部分のみ上記のシートを利用してヒアリングを行うことで、担当者の負担を低減します。

3. 最新の攻撃トレンドを加味した対応策を提案

これまで実施してきた、5,000 件以上の Web アプリケーション診断の実績に基づく評価項目をベース

に、熟練のテクニカルコンサルタントが評価を実施します。対象のシステムやお客さまの業種に即した、最新の攻撃トレンドとインシデント事例を考慮して、問題点を抽出し、最も実効性の高い対策を提案します。

本サービスの詳細については、次の Web サイトをご参照ください。

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

なお、NRI セキュアでは、Web アプリケーションだけでなく、インフラシステムやクラウド、アーキテクチャの課題に関する評価や対応策の提案も支援しています。加えて、デジタルサービスを企画・要件定義する段階でリスクを網羅的に洗い出す「デジタルサービス向けリスク分析支援」³や「ソースコード診断」⁴「Web アプリケーション診断」⁵等と、本サービスを組み合わせることで、一層高いセキュリティレベルを確保しつつ、スムーズなシステム開発・運用を行うことが可能になります。

NRI セキュアは、今後も時代のトレンドや脅威の動向を捉え、企業や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 DX の推進に貢献していきます。

1 シフトレフト：

開発ライフサイクルが短期間化し、迅速かつ頻繁にアプリケーションをリリースする傾向が社会全般で広がっていく中で、リリースのスケジュールを妨げないように、セキュリティに関わる工程を前倒しして実施するという概念です。具体的には、開発前の段階からセキュリティを考慮した設計を行ったり、開発したシステムにおけるセキュリティ診断工程を内製化・自動化したりする取り組みが行われています。

2 要素技術：

製品の開発に必要な基本技術を指します。

3 デジタルサービス向けリスク分析支援：

詳細は、2019年8月8日に発表した、「デジタルサービス向けリスク分析支援」の次の発表資料をご参照ください。
<https://www.nri-secure.co.jp/news/2019/0808>

4 ソースコード診断：

詳細は、次の Web サイトをご参照ください。https://www.nri-secure.co.jp/service/assessment/source_code

5 Web アプリケーション診断：

詳細は、次の Web サイトをご参照ください。https://www.nri-secure.co.jp/service/assessment/web_application

【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