Nomura Research Institute Group

NEWS RELEASE

2019 年 8 月 8 日

NRI セキュアテクノロジーズ株式会社

NRI セキュア、デジタルサービスの潜在リスクを複合的に分析し、対策を支援するサービスを提供開始

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、社長：小田島 潤、以下「NRI セキュア」）は、デジタルサービスの開始を検討している企業向けに、情報セキュリティに関わる潜在的なリスクを洗い出し、その対策の立案を支援する「デジタルサービス向けリスク分析支援」（以下「本サービス」）を、本日から提供します。

デジタルトランスフォーメーション（DX）の進展を受けて、企業はデジタル技術[1]を活用して自社のコアビジネスをデジタル化することで、競争力を高めようとする動きが加速しています。そうして生み出されるデジタルサービスのビジネスモデルや業務プロセスには、下記のような特徴があります。

・新しい技術やソフトウェアを採用していることが多い
・社内外の Web サービスやシステムとつながることが多い
・提供形態やビジネスモデルは多種多様、かつ関係するステークホルダーが多い

このようにデジタルサービスは複雑な構造になりがちなため、サービスを構成する要素にセキュリティの脆弱性が潜んでいても、見落とされやすくなります。また、それを突くサイバー攻撃や不正利用が起きた場合に、利用者の安全を脅かしたり資産を毀損したりするほか、ビジネスそのものに負の影響をもたらす可能性もあります。

デジタルサービスを安全かつスピーディに提供するためには、より早い段階でのリスク分析が有効です。具体的には、サービスの企画・要件定義の段階でリスク評価を行い、想定される脅威を洗い出した上で、それに対応するセキュリティ要件をサービスの仕様として組み込んだシステムを設計することが推奨されます（文末の「ご参考」を参照）。

また、セキュリティの対象領域は広がっており、プライバシーや身体の安全の担保、提供サービスに対する利用者の信頼性確保などの観点からも考慮することが、求められるようになってきています[2]。

本サービスは、企業がデジタルサービスを企画・要件定義する段階から関わり、ビジネスモデルとユー

スケース（ユーザーの利用事例）の観点から、デジタルサービスの脅威となりうるリスクを網羅的に洗い出し、適切なセキュリティ対策を提示するものです。具体的には、以下の 3 つの機能から構成されます。

1. サービス仕様・ビジネスモデルの把握と脅威の洗い出し

対象となるデジタルサービスのビジネスモデルや仕様、外部との提携先も含めた全体像を把握します。その上で、悪意者がどのような目的や手法でサービスを悪用しようとするのかを洗い出し、それらの行為の難易度や類似の事例を踏まえて、様々な悪用の形態を「脅威シナリオ」としてまとめ、各シナリオが当該デジタルサービスに対してどれほどのインパクトを持つかを評価します。

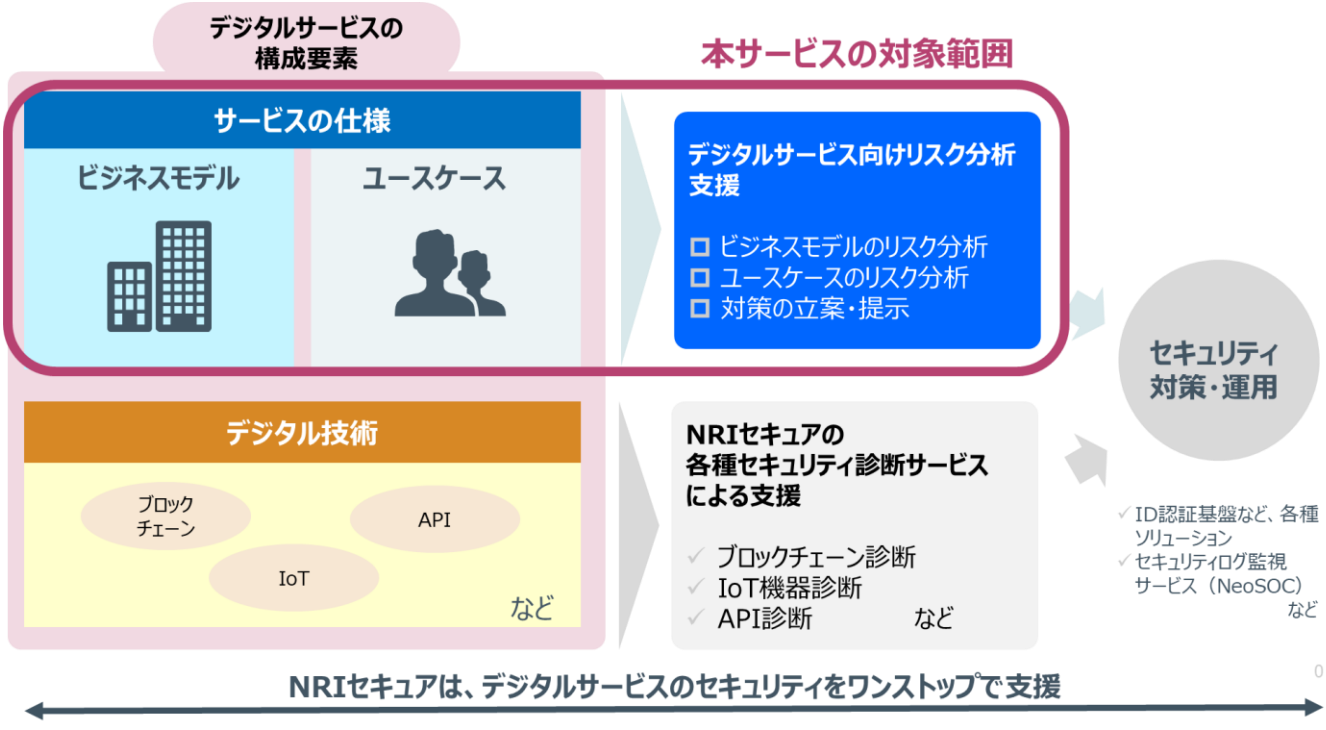
2. ユースケース（ユーザーの利用事例）に基づく脅威の洗い出し

分析対象となるデジタルサービスが持つ特有のユースケースに重点をおいて、悪用された場合のあらゆるリスクを洗い出します。その中から、実際に起きる可能性の高いリスクのメカニズムを分析し、当該リスクと現在の対策とのギャップを評価します。

3. 脅威シナリオに対する対応策の立案・提示

作成した脅威シナリオをもとに、デジタルサービスの仕様にセキュリティ対策として組み込むべき事項を、対応方針として提示します。また、各対応方針について、脅威の「予防」「検知」「抑止」「低減」等の採るべき具体策を提示します。

図：デジタルサービスが抱えるリスクに対する、NRI セキュアのソリューションの全体像



※本サービスは、システム開発における RFI や RFP 等で定義される「サービス仕様」に対するリスク分析を対象とします。アプリケーションや基盤といったシステムの脆弱性に対する評価は、NRI セキュアで提供している診断サービスの対象分野となります。

企業は本サービスを用いることで、自社だけでは見落としてしまう可能性のある脆弱性に気づいたり、より適切なサービス設計やシステムの実装を図ったりすることができます[3]。また、企業がデジタルサービスをサービスインするか否かを意思決定する際の判断材料としても、活用できます。

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・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] デジタル技術：IoT（Internet of Things）、AI（人工知能）、API（Application Programming Interface）、ブロックチェーンやクラウドなどの分野で使われる技術。これらの技術によって、xxTech（例：Fintech）や XaaS（例：“サービスとしてのモビリティ”の略である MaaS）などのデジタルサービスが誕生しています。

[2] 従来のセキュリティ概念は、情報システムの「機密性」「完全性」「可用性」を担保するものとして考えられてきました。これらに加えて、DX の時代では次の 3 つの観点も、セキュリティの概念上、重要とされています。（1）プライバシー、（2）安全性（AI を活用した車の自動運転における事故防止等、身体上の安全性も含みます）、（3）信頼性（ここでは本人認証とは異なり、利用者のサービス上の行動履歴や身分証の提示状況などから、より良いサービスを提供する相手かどうかを判断することも含みます）

[3] 企画や要件定義の段階で、デジタルサービスに潜む脆弱性が明らかになるため、企業は自社の開発部門や委託先となる開発ベンダーなどに、よりセキュアな設計・実装を促すことや変更・修正の依頼に繋げることができます。

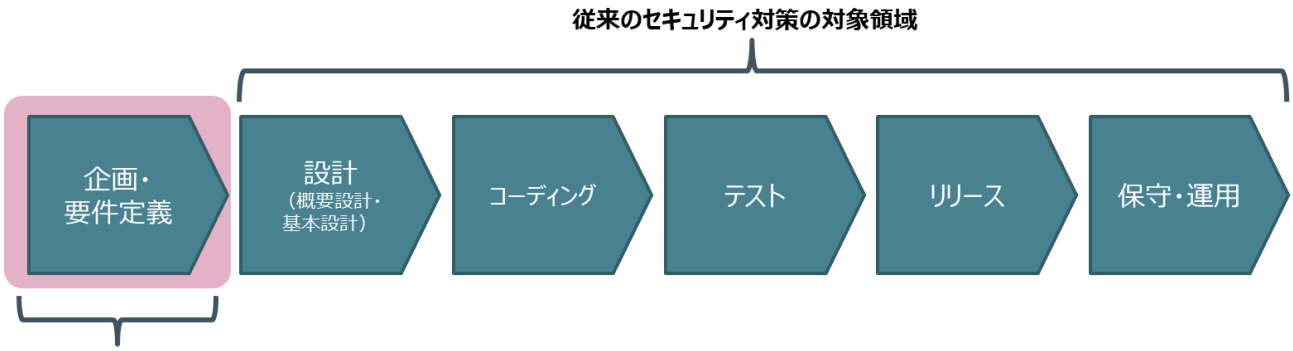
【ニュースリリースに関するお問い合わせ先】

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】

■ システム開発の一連の工程における、デジタルサービスのリスク分析の位置づけ



デジタルサービスでは、はじめの工程でリスク分析を実施することが重要。

例えば、ビジネスモデルが脆弱だったり、プライバシー情報が不適切に取り扱われたなど、サービス仕様に根差すリスクが存在した場合、後工程での対処は困難。