# 安全・安心な製品・サービスをご提供するための取り組み　～セキュア開発・運用～

石原 潤二　中村 匡秀　妹脊 敦子　大澤 公美子　林 秀房

**要 旨**

社会やビジネスがデジタルの世界へ大きくシフトし、インターネットに接続されるモノすべてがサイバー攻撃の対象とされる時代が到来しています。このような状況のなか、NECグループでは、お客様のビジネスを支える安全・安心な製品やサービスの提供を目指し、「セキュリティ・バイ・デザイン」の考え方に基づいたセキュア開発・運用に取り組んでいます。お客様のシステムの特徴に応じたリスクアセスメントや、管理システムを用いた効率的な脆弱性対応などにより、セキュリティ品質を担保できるようにしています。本稿では、このようなセキュア開発・運用の具体的な取り組みや今後の展望について紹介します。

KeyWords　セキュリティ・バイ・デザイン／セキュア開発・運用／リスクアセスメント／脆弱性診断／脆弱性管理

## 1. はじめに

サイバー攻撃は年々増加し、世界中で被害が拡大しています。サイバー攻撃は巧妙化、高度化し続けていますが、既知の脆弱性を悪用したものも多くあります。システムの脆弱性を放置することは、その大小に関わらず攻撃者に狙われるリスクとなり、結果として、組織活動の遅延や停滞、機密情報の流出、経済的損失、企業ブランドイメージの失墜などを招く恐れがあります。攻撃者にシステムの脆弱性を悪用されるリスクを低減するためには、そもそもシステムに脆弱性を作り込まないことと、新たに発見された脅威に対して、弱点となる部分がないかをつど調査し、対処していくことがポイントとなります。

システムに脆弱性を作り込まないためには、「どのような脅威が想定されるか」「どのように対処できるのか」などを考慮しながら設計・実装を行う必要があります。こうしたセキュリティを設計段階から考慮する考え方は「セキュリティ・バイ・デザイン」と言われ、内閣サイバーセキュリティセンター（NISC）も推奨しています[1)]。優先度の高いセキュリティ対策を含めてシステムを設計しておけば、対策の抜けもれ、あるいは過剰な対策を防止することができ、最適なシステム構成にすることができます。また脅威は継続的に発見されるため、システムの出荷時点では脆弱性対処が万全であっても、運用していくなかで不十分になる可能性があります。よってシステム運用段階において、継続的に脆弱性情報を収集し、対処していくことが必要です。

NECグループでは、システムの開発・運用において、セキュリティを確保するような取り組みを実施しており、第2章以降では、その内容について、より詳細に解説します。

## 2. NECにおけるセキュア開発・運用

NECグループで推進しているセキュア開発・運用とは、要件定義から運用・保守の各プロセスにおいてセキュリティを十分に考慮した開発・運用を実施することです。その大きな目的は、脆弱性の作り込みをなくすことと、出荷後に新たに発見される脆弱性へ対処することです。セキュア開発・運用を各部門が適切に行えるよう、これらのプロセスにおいて実施すべき事項（以下、セキュリティタスク）をNECグループの全社標準である日本電気工業標準（NEC Corporation Industrial Standards：NIS）の1つ、「セキュア開発・運用管理規程」のなかに定めています。具体的には、開発・運用プロセスを（1）企画・要件定義、（2）設計・実装・テスト、（3）運用・保守の3パートに分け、お

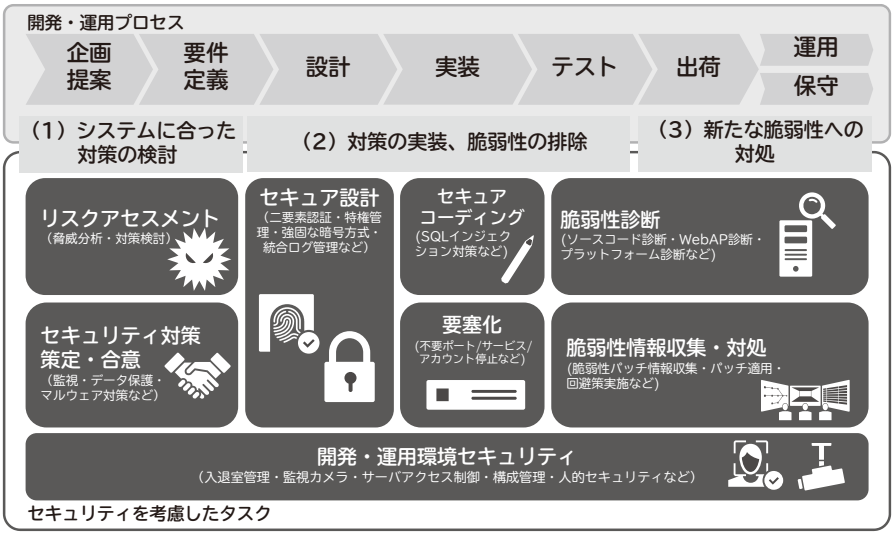



図1　セキュリティタスク一覧

客様のシステムに応じたセキュリティの検討・対策を行うために、各パートでタスクを実行しています（**図1**）。（1）では、システムへの脅威とその影響度を考慮したセキュリティ対策を検討するためのタスクを実行します。（2）では、（1）で検討した対策を実装し、出荷時点での最新の脅威に対抗するためのタスクを実行します。（3）では、出荷後に発見される新たな脆弱性に対抗するためのタスクを実行します。

セキュリティタスクのなかで特に重要となるのが、リスクアセスメントと脆弱性への対処です。セキュリティ対策は1つ実施すれば良いというわけではなく、またすべてを実施する必要があるわけでもありません。システムの脅威とその影響度に応じて最適な対策を実装するためには、リスクアセスメントをシステムのアーキテクチャや運用など全体像を考える段階で、実施することが重要です。また、システムのバグは一度対処すれば終わりですが、脆弱性は一度対処すれば終わりではなく新たに発見され続けます。そのため、それらに対して継続的に対処していくことが大切です。

## 3. リスクアセスメント

### 3.1 リスクアセスメントの概要

本稿におけるリスクとは、ビジネスにおいて企業などが損失を被る危険性のことを指します。リスクアセスメントはこのリスクを管理するために必要なタスクであり、リスク特定、リスク分析、リスク評価を含むプロセス全体を指します。

リスク特定では、お客様の守るべき情報資産を洗い出したうえで、どのようなリスクが存在するかを特定します。リスク分析では、リスク特定にて洗い出されたリスクの発生可能性、リスクが顕在化したときの影響度を算出し、リスクの大きさを数値化します。リスク評価では、リスク分析にて得られたリスクの大きさをもとに、対応の必要性や優先度を判断します。

リスクアセスメントを上流プロセスで実施しておくことで、お客様の状況に応じたセキュリティ対策を選定できるとともに、システムの機密性、完全性、可用性、あるいは管理統制や利便性などのバランスを保つことができます。

お客様のシステムに精通している担当の開発者やSEがリスクアセスメントを実施することをNECグループでは推奨しており、一般的なリスクや対策を検討するだけでなく、お客様のシステムの特性や運用を考慮したリスク、及び対策を検討しています。

### 3.2 リスクアセスメント手法

NECグループにおけるリスク分析のプロセスでは、国際規格の要求事項を採用し、対象となるシステムのセキュリティレベルが国際規格の標準に達しているかを評価します。ただし、業界や業務によってリスクが大きく異なることや、高度なセキュリティ対策が要求される場合もあり、国際規格の要求事項のみでは評価が不十分になる可能性があります。そこでお客様の重要な情報資産については、適宜詳細

なリスク分析を組み合わせることを、NECグループでは開発者・SEに推奨しています。詳細リスク分析では、情報資産に対し資産価値、脅威、脆弱性やセキュリティ要件を識別し評価しており、こうした分析手法を組み合わせることで、より精度の高い分析を実施することが可能になります。また、すべての情報資産に対して詳細なリスク分析を実施するよりも、時間や費用を削減することができます。

### 3.3 組込み、制御システムへの応用

近年、IoT機器や組込み機器を踏み台にした大規模サイバー攻撃の増加など脅威が高まっていることを踏まえ、2016年度にこれらの脅威の洗い出しと対策の検討に取り組みました。セキュリティの有識者に加えて、利用シーンを理解し設計している組込み機器の製品担当者が参加することで、機能だけでなく運用シーンも想定して脅威の洗い出しを行いました。例えば、ハンディターミナルであれば、汎用のPCやサーバよりCPUやメモリなどのリソースが限られていることや、機器が小型のため持ち出しによる不正操作の可能性があることなどが特性として挙げられます。それらを考慮した実現可能な対策や運用対策での代替案をまとめ、開発現場で活用できるチェックリストに仕立ててNECグループ全体に公開しています。本チェックリストは、IoT機器、組込み機器の開発部門を中心に開発基準に取り込み活用されています。

また、ICTシステムの分野で培ったセキュア開発のノウハウを応用し、制御システムに対しての安全性を高めるためのご提案を行った事例もあります。重要インフラの領域では各業界団体が制定しているセキュリティガイドラインが法令基準となっているため、これに準じた対策が必須の場合があります。そこで、お客様の既存のシステムがガイドラインに準拠した対策となっているかをリスクアセスメントによって確認し、脅威の洗い出しと対策の提案を行いました。これにより、お客様の次期システムにおいてのマイルストーン制定のご支援ができ、またお客様からのセキュリティ意識向上にもつながったと評価をいただきました。

### 3.4 リスクアセスメントの普及

NECは、お客様のシステムや業務を理解したうえでセキュリティを検討できるようにするために、各業種のシステムに精通している開発者・SEがセキュリティの知識も高めていくための活動に注力しています。開発者・SEが研修やOJTなどを通じてセキュリティの考え方、リスクアセスメントやセキュリティ技術の知識、テスト技法などを学び、システムの特性や運用を考慮してお客様に最適な対策の提案、設計・開発を行っています。各事業部でリスクアセスメントを行う際には各業種の動向や法令・ガイドラインなども踏まえつつ、最新の脅威やインシデント事例も取り込むことで、お客様システムを安全・安心なものにできるよう努めています。

## 4. 脆弱性への対処

### 4.1 脆弱性対応の概要

脆弱性の対応は、出荷前に既知の脆弱性をなくすこと、出荷後に発見された脆弱性に速やかに対処すること、この2点が重要です。

そのためNECでは、脆弱性に対処するためにテスト、出荷、運用、保守プロセスで行うべきセキュリティタスクとして、脆弱性診断、脆弱性情報収集・対処を定義しています（図1）。脆弱性診断を行うことで、作り込んでしまった脆弱性を検出し、出荷前に対処します。また、製品・システムで使用しているOS、ミドルウェア、フレームワークなどに脆弱性がないか日々情報を収集し、影響を受ける脆弱性に対処することで、製品・システムをセキュアに保ちます。

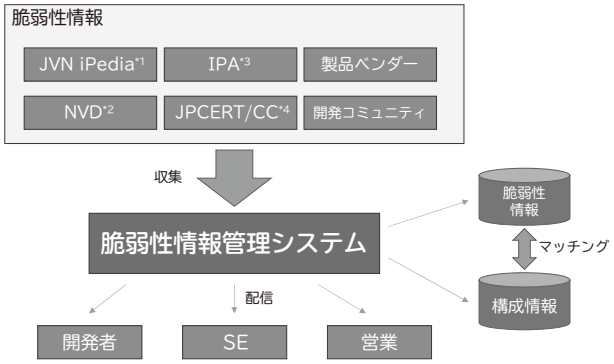
### 4.2 脆弱性診断

脆弱性診断とは、ソースコードを論理的に解析したり、実際に動作させて解析したりすることにより製品・システムに存在する脆弱性を検出するものです。脆弱性診断には静的診断と動的診断があります（**表**）。

静的診断（ソースコード診断）は、開発環境のなかで自動的に実施できるような仕組みを構築しており、多くのプロジェクトで利用しています。動的診断（Webアプリケー

表　脆弱性診断の種類

| 種類 | 特徴 |
|---|---|
| 静的診断<br>・ソースコード診断 | ・脆弱性の根本的原因を把握可能<br>・製品・システムの開発段階から実施可能 |
| 動的診断<br>・Webアプリケーション診断<br>・プラットフォーム診断 | ・製品・システムの実行環境まで含めた脆弱性を検出可能<br>・脆弱性が悪用された場合の具体的な動作や被害を特定可能 |




*1 JVN iPedia（脆弱性対策情報データベース） http://jvndb.jvn.jp/
*2 NVD (National Vulnerability Database) https://nvd.nist.gov/
*3 IPA（独立行政法人 情報処理推進機構）
*4 JPCERT/CC（一般社団法人 JPCERTコーディネーションセンター）

図２　脆弱性情報管理システム

ション診断、プラットフォーム診断）は、各プロジェクトのメンバーが診断ツールのハンズオントレーニングを受講したうえで実施しています。

### 4.3 脆弱性情報収集・対処

脆弱性情報は日々公開されています。これらの情報は製品ベンダーや開発コミュニティなどさまざまなところから発信されており、網羅的に収集するのは非常に手間がかかります。

脆弱性情報を効率的に収集し、影響のあるプロジェクトに適切な情報を配信して、速やかに対処を行うため、NECでは独自の脆弱性情報管理システムを構築しています。定期的にインプットされる脆弱性情報とあらかじめ入力しているお客様システムのソフトウェアの構成情報とのマッチングを行い、対象ソフトウェアの脆弱性情報が見つかると、その情報を担当者にメール配信します（**図2**）。情報を受け取ったら対策を検討し、お客様システムに対して修正パッチを適用する、セキュリティ機器を使用して回避する、と言った対策を実施します。

このようにして、NECグループ全体で脆弱性情報の共有を行っています。また、特に影響範囲が広く危険度の高い脆弱性に関しては、より広範囲に周知徹底するために注意喚起を行い、即時対応する体制を構築しています。

## 5. むすび

本稿では、お客様に安全・安心なシステム・サービスを提供するための「セキュリティ・バイ・デザイン」に基づくセキュア開発・運用の取り組みについて紹介しました。リスクアセスメントの実施、出荷前の脆弱性診断及び出荷後に新たに発見される脆弱性に対する対処を含む総合的な取り組みにより、お客様のシステムの安全性を確保しています。

ICTシステムに対しては、セキュア開発・運用が定着しつつありますが、IoT、制御機器などのデバイスを用いたシステムへの攻撃が社会問題になっているため、今後はこれらに対してもセキュア開発・運用を実施することが必須となります。NECでは、IoT、制御機器に対するセキュア開発・運用として脆弱性情報の収集から取り組み始めています。

NECは今後もお客様のビジネスを止めないために、システムを安全に保つための活動とその改善を継続的に実施していきます。

### 参考文献

1）内閣サイバーセキュリティセンター（NISC）：情報セキュリティの観点から見た行政情報システムの望ましいあり方」と「行政情報システムの企画・設計段階からのセキュリティ確保に向けた取組み（セキュリティ・バイ・デザイン［SBD］）」について，情報セキュリティ政策会議（平成19年）第15回会合，2007.12
http://www.nisc.go.jp/conference/seisaku/dai15/pdf/15siryou02.pdf

### 執筆者プロフィール

**石原 潤二**
サイバーセキュリティ戦略本部
セキュリティ技術センター
マネージャー

**中村 匡秀**
サイバーセキュリティ戦略本部
セキュリティ技術センター
エキスパート

**妹脊 敦子**
サイバーセキュリティ戦略本部
セキュリティ技術センター
主任

**大澤 公美子**
サイバーセキュリティ戦略本部

**林 秀房**
サイバーセキュリティ戦略本部
セキュリティ技術センター
主任

# NEC 技報のご案内

NEC 技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

## Vol.70 No.2　ビジネスの安全・安心を支えるサイバーセキュリティ特集
～Futureproof Security　安心の先へ。～

ビジネスの安全・安心を支えるサイバーセキュリティ特集によせて
増大するサイバー犯罪の根源的な解決へ～“産学官”のオールジャパンで立ち向かう第三者機関の姿とは？～
サイバーセキュリティを取り巻く社会動向とNECの取り組み

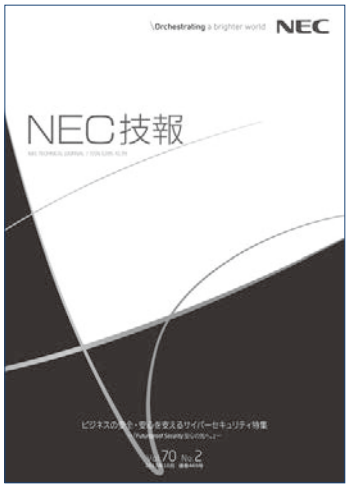
### ◇ 特集論文

**社会の動向とNECの取り組み**
重要インフラに対するサイバー攻撃の実態と分析
2017 サイバー攻撃最新動向 NEC Cyber Threat Intelligence活用モデル
サイバーセキュリティ対策の社内事例

**サイバーセキュリティソリューション**
複雑化 / 高度化するサイバー脅威に対抗するSOCとセキュリティ監視サービス
攻撃被害を極小化するためのインシデント対応支援ソリューション
サイバー演習によるインシデントハンドリング能力の強化
セキュリティ統合管理・対処ソリューション「NEC Cyber Security Platform」
クラウド型ファイル暗号化サービス －ActSecureクラウドセキュアファイルサービス－
セキュリティLCMサービス
EMMを活用したセキュアなモバイルワークソリューション
IoT 時代の経営を支援するサイバーセキュリティコンサルティング

**サイバーセキュリティへのAI技術の活用**
AI（人工知能）を活用した未知のサイバー攻撃対策
採るべき対策の「なぜ？」に答えるAIの可能性
オープンソースインテリジェンスを活用したサイバー脅威の検出と自動分析
犯罪捜査支援のためのサイバー・フィジカル統合分析技術

**お客様に安全・安心を届けるための社内の取り組み**
安全・安心な製品・サービスをご提供するための取り組み ～セキュア開発・運用～
サイバーセキュリティ人材のタレントマネジメント




Vol.70 No.2
（2017年10月）

特集TOP