7E-03

製品開発プロセスにおけるセキュリティ確認の組込

佐田　康文†　梅崎　一也†　宮崎　剛†　山本　健児†　清水　良昭†

富士電機株式会社†

1　はじめに

近年，IoT やデジタルトランスフォーメーションの活用の進展に伴い，サイバー攻撃の脅威が増加している．なかでも，企業が使用している IT/IoT 製品の脆弱性に起因するインシデントが発生している[1]．そのため，米国の NIST Cyber Security Framework(CSF)[2]などのセキュリティのガイドラインが制定されており，サプライチェーンリスクマネジメントが求められるようになっている．サプライチェーンのセキュリティの弱い部分がサイバー攻撃の標的となるため，ベンダとしては製品のセキュリティを確保に向けて，製品ライフサイクルの各段階でセキュリティ対策を確実に実施する必要がある．

富士電機では製品開発の最初からセキュリティ対策を実施する(セキュア・バイ・デザイン)ために，製品開発のプロセス管理を行う設計審査(以下 DR)へのセキュリティ確認の組込とセキュリティ検証技術の開発を行った．本稿では，その取り組みを紹介する．

2　セキュリティ確保に向けた課題

富士電機は，発電プラント，パワエレ エネルギー，パワエレ インダストリー，情報システム，食品流通，半導体といった分野で事業を展開している．

各事業分野で表 1 のような，システム・コンポーネントの製品群が存在する．

表 1　富士電機の製品(一部)

事業分野	システム	コンポーネント
発電プラント	地熱発電・火力発電	タービン
パワエレ エネルギー	エネルギーマネジメントシステム	UPS，スマートメータ
パワエレ インダストリー	プラントシステム，情報システム	インバータ，PLC
食品流通	店舗管理システム	自動販売機・ショーケース
半導体	-	パワー半導体

Implementation of security checks in the product development process

Yasufumi Sata†, Kazuya Umezaki†, Tsuyoshi Miyazaki†, Kenji Yamamoto†, Yoshiaki Shimizu†

これらの製品の多くには，ソフトウェアが実装されているため，適切なセキュリティ対策を実施する必要がある．

セキュリティ対策を実施するにあたって，以下の課題が存在する．

① 多岐にわたる事業分野に起因する，製品ごとに異なるセキュリティ要件への対応
② NIST CSF などの新しいガイドラインへの準拠
③ セキュリティ対策が有効に機能し，脆弱性が生じていないことの検証

3　セキュリティ確保に向けた対策

3.1　製品開発におけるセキュリティ確認

開発の各フェーズでセキュリティ対策が確実に実施されるように，DR でセキュリティ確認を行うためのセキュリティ確認チェックリスト（以下チェックリスト)を作成した．開発のフェーズは図 1 のようになる．

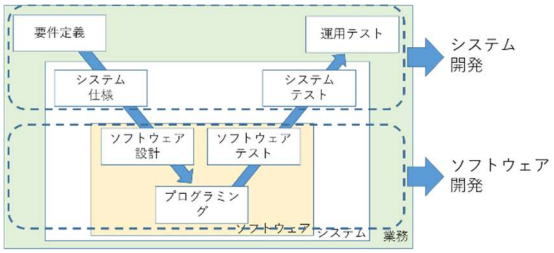

図 1　開発フェーズ

開発フェーズはシステム開発である要件定義・システム仕様・システムテスト・運用テストのフェーズと，サーバやコンポーネントのソフトウェア開発であるソフトウェア設計・プログラミング・ソフトウェアテストのフェーズに分けられる．

チェック項目の考え方としては，システム開発フェーズと，ソフトウェア開発フェーズで観点を分けて作成した．システム開発フェーズでは，セキュリティ要件の確認や脅威分析を踏まえたソフトウェア開発におけるセキュリティ対策の決定など，プロセスの確認を主なチェック項目としている．ソフトウェア開発フェーズでは，システム仕様に基づくソフトウェア設計の決定などプロセスの確認に加え，技術的対策(暗号

化，ユーザ認証など)をチェック項目としている．
また，セキュリティ対策の実施だけでなく，検証の実施もチェック項目としている．
チェックリストの作成に当たっては，NIST CSF などの既存のガイドラインから，製品開発の際に対応必要な項目を抽出してチェック項目を作成した．
チェックリストの概要を表 2，表 3 に示す．

表 2　システム開発のチェックリスト概要

開発フェーズ	チェック項目
要件定義	・セキュリティ要件の有無 ・脅威分析の実施
システム仕様	・セキュリティ要件に基づくシステム仕様の決定 ・脅威分析を踏まえたセキュリティ対策の具体化
システムテスト	・システム仕様への準拠 ・脆弱性対策の完了
運用テスト	・セキュリティ要件の準拠

表 3　ソフトウェア開発のチェックリスト概要

開発フェーズ	チェック項目
ソフトウェア設計	・システム仕様に基づくソフトウェア設計の決定 ・構成管理の実施 ・ソフトウェア開発の委託先のセキュリティ対策 ・開発環境のセキュリティ対策 ・通信・データの暗号化 ・ユーザ・デバイスの認証 ・セキュリティパッチの適用
プログラミング	・ソフトウェアの脆弱性防止
ソフトウェアテスト	・ソフトウェア設計への準拠

3.2　セキュリティ検証技術

3.1 節のチェックリストでチェックをするためには，セキュリティ検証技術を利用することが必要であり，下記の技術を開発した．

(1) ソフトウェアの脆弱性防止

プログラミングのフェーズのチェック項目である「ソフトウェアの脆弱性防止」の確認のために以下の 2 つの技術を開発した．

・セキュアコーディングルール

実装したソフトウェアについては，脆弱性を作り込まないようにすることが重要である．そこで CERT(Computer Emergency Response Team)の C 言語のセキュアコーディングルールの適用計画，診断ツールによるソースコードのルール適合性チェック，準拠報告書の作成などの適用手順や文書テンプレートを作成した．

・OSS(Open Source Software)脆弱性診断

製品で使用する OSS に脆弱性があるとサイバー攻撃を受ける可能性があるため，OSS の脆弱性有無を確認することが重要である．そこで，OSS の脆弱性診断ツールを評価・選定し，適用を開始した．

(2) 脆弱性対策の完了

システムテストのフェーズのチェック項目である「脆弱性対策の完了」の確認のために，以下の技術を開発した．

・Web サーバの脆弱性確認

インターネットに接続された Web サーバは，サイバー攻撃の標的となる可能性があるため，脆弱性を解消しておく必要がある．そこで，Web アプリケーションやプラットフォームの脆弱性診断ツールや第三者の診断サービスについての評価・選定を実施し，適用を開始した．

3.3　効果

製品ごとに異なるセキュリティ要件に対応するチェックリストを作成し，セキュリティの検証技術を開発した．これを各事業分野の製品開発に適用することで，製品毎に要件やシステム構成が異なっても，共通の考え方に基づいてのセキュリティ対策の実施が可能となる．

4　まとめ

本稿では当社の製品のセキュリティ確保のために DR で適用するチェックリストと，セキュリティ検証技術について説明した．

このチェックリストと，セキュリティ検証技術を適用することによって，当社の製品のセキュリティ対策の強化をはかっていく．

参考文献

[1] 情報処理推進機構.情報セキュリティ 10 大脅威 2021.2021-03.月.https://www.ipa.go.jp/security/vuln/10threats2021.html
[2] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018-04.