



# FORTIFY® 導入事例レポート

横河電機株式会社 様

## 総合的な品質向上とセキュリティ強化のために

計測機器などのハードウェアから、それらを統合して管理するソフトウェアまで、プラントの稼働に必要なトータルソリューションを提供している横河電機株式会社。1年間の試験導入を終え、2010年7月からFORTIFYの本格的な運用を開始した。分散制御システムをはじめとした自社ソフトウェア製品の品質・セキュリティ管理を担当する新井氏に、導入の経緯や今後の展開について伺った。

### Chapter 1

### FORTIFY SOURCE CODE ANALYSIS SUITE

## 重要インフラを支えるための安定性・信頼性

### 適用業務

現在弊社では、主力商品である分散制御システム（生産プラントの頭脳にあたる装置）のソフトウェア品質管理にFORTIFYを用いる予定で準備を進めています。ソースコードの不具合を検出するのが目的なので、製造から単体試験のフェーズで使用することになります。導入先には、工場・上下水道・発電所・製油所などの重要インフラも含まれるので、信頼性が何よりも重要だと考えています。

### 導入までの経緯

導入の最大の目的は、ソースコードの品質向上です。FORTIFYを導入する以前から、コーディングルールの遵守、ソースコードウォークスルーや大がかりな動作検証の実施など、品質向上のための取り組みを行ってきましたが、やはり人の手や目だけでは限界があります。お客様により安心して製品をご利用いただくために、FORTIFYのような高機能ソフトウェアによるソースコード検査が必要だと考えました。



横河電機株式会社 ソフトウェア技術部  
新井 貴之氏

また、ソースコードの品質向上はセキュリティ面の強化にもつながっており、その点も導入を決定づけた大きな要因でした。IT分野では、セキュアコーディングなどのセキュリティ対策が注目を集めています。生産制御システムにおいても古くから機密保持などのセキュリティ対策が行なわれていますが、従来は外部と隔離されたネットワークで運用されるシステムが多かったため、外部からの攻撃に対する対策についてはあまり優先度が高い事項ではありませんでした。しかし、近年では、生産制御システムへのIT技術導入や広域ネットワーク対応が進んでおり、より高度なセキュリティ対策が求められるようになってきました。重要インフラをサポートする立場として安定性・信頼性の高い製品を提供するためにも、FORTIFYを導入する必要があるのです。

### 導入の決め手となったFORTIFYの機能

大きく2点、決め手となった機能要素があります。1点目、これが最大の決め手となった要素ですが、C#もカバーする対応言語の豊富さです。他社の競合製品ではC#に対応しているものはほとんどありませんでした。2点目は、CUIからの実行が可能だったことです。これにより、夜間や休日にバッチを実行し、人手を介さずに膨大な量のソースコードを検査することが可能になります。まだ試験的な導入の段階ではありますが、本運用での工数の削減に期待しています。

## 試験導入での評価は高いものの、本運用へ向けて必要な取り組みも見えてきた

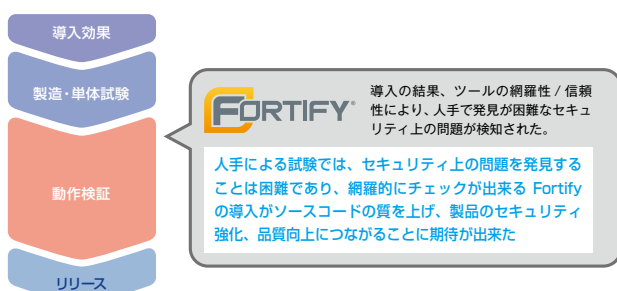
### 導入効果

動作検証に協力してくれるプロジェクトを募るところから、FORTIFY の試験運用は始まりました。はじめのうちはモジュール単位でFORTIFY による検査をし、その後開発者と検査結果のチェックを行うことで、検知ロジックの妥当性・有用性を評価しました。開発者が気づかなかった観点で不具合を検知してくれる点が大変好評で、検知結果を以降のコーディングにフィードバックできるのが大きな魅力です。ミスを引きやすい関数の使用や記法も検知されるため、開発者のコーディングスタイルの向上にも役立つと期待しています。

また、試験導入の早い段階でよい反響があったため、FORTIFY の結果を用いたセキュアコーディングの研修も実施したところ、そちらもやはり好評でした。ただのツールとしてではなく、開発者の品質やセキュリティへの意識も高めてくれるため、結果的に製品の安定性・信頼性を総合的に向上できました。

### 試験運用時

#### TEST INSTALLATION



### 本運用時

#### OFFICIAL OPERATION



### 今後必要な取り組み

今後、FORTIFY の運用をスムーズに進めていくためには、膨大な件数の検知結果を効率よく処理する方法の確立が必要不可欠だと考えています。たとえば、ソースコードの中のコメントや関数に "Password" という文字列が入っていると、パスワードがハードコードされている恐れがあるため検知されるのですが、ハードコードの恐れが無いとわかっている場合には、この検知は不要です。これに関しては、FORTIFY の機能でクレンジングルールを追加して、解消していくことが可能です。

また、試験運用では開発者に検査結果を渡す前に、「種別（セキュリティに関するものか、品質に関するものか）」「重要度（早急に改修が必要か、そうでないか）」「工数（改修は関数単位か、数行単位か、仕様変更が必要か）」という基準で項目に優先順位付けをしていましたが、こちらに関してもさらなるブラッシュアップが必要です。これら 2 つの作業を効率的に行うための仕組みが整えば、工数削減という面でも FORTIFY は大きな効果を発揮してくれると思っています。

## Chapter 3

### FORTIFY SOURCE CODE ANALYSIS SUITE

## 今後の本運用に向けて、いかに人手運用部分を減らすかが鍵

### 本運用に向けて

人の目での検出が困難なソースコードの不具合を、開発段階で発見して対策をすることが可能になるため、さらなる品質の向上とセキュリティ面の強化に、大きな手応えを感じています。加えて、開発コストの削減を実現するために、先ほどお話しした検知結果の効率的な処理ルールも、運用しながら整えていく必要があります。

FORTIFY を導入することで、弊社製品の安定性・信頼性をさらに向上させ、これからも産業界に貢献していきたいと考えています。

### Company Profile

商号	横河電機株式会社
英文商号	Yokogawa Electric Corporation
代表取締役社長	海堀 周造
創立	1915年9月1日
設立	1920年12月1日
資本金	434億100万円(2010年3月末現在)
本社所在地	東京都武蔵野市中町2-9-32



#### 担当者プロフィール

新井 貴之 氏  
IA 事業部 システム事業センター  
ソフトウェア技術部

入社 15 年目。近年は技術開発本部に所属し、ネットワークセキュリティやマルウェア対策関連の研究に従事。一昨年末に IA 事業部に転属後、自身の研究成果を生かして社内製品のセキュリティに関する業務を担当。

●お問い合わせ先