制御システム製品のセキュリティへの取り組み

Security Efforts of System Products

高松 家廣 *1　加藤 毅 *1　真壁 浩之 *2
Katsuhiro Takamatsu　Tsuyoshi Katou　Hiroyuki Makabe

製品のセキュリティを確保するためには，製品に必要なセキュリティ機能を実装することはもとより，開発プロセスの各フェーズにおけるセキュリティを確保するための取り組みも重要である。本稿では，まずシステム製品を開発するうえで取り組んでいる開発フェーズごとのセキュリティの取り組みとして，セキュア開発ライフサイクルを紹介する。次に，制御システム製品に必要なセキュリティ機能の実装例として，OS の要塞化やアンチウイルスソフトの最適化，オープンなネットワーク環境でも安全に制御ネットワークを維持するために実装した Vnet/IP のセキュリティ対策について紹介する。

このようなセキュリティに対する取り組みは，近年整備されつつある認証プログラムにも取り込まれており，なかでも ISASecure 認証プログラムは IEC の標準を目指した活動をしており，今後注目されると考えられる。システム製品もこの流れに追従すべく，主力製品である CENTUM VP と ProSafe-RS で本認証を取得したことを紹介する。

To ensure the security of products, it is important to take measures in each phase of their development and also to implement security functions in the products themselves. This paper introduces the security development lifecycle that Yokogawa applies to each development phase of its system products. This paper also describes examples of security functions implemented in control systems. These are OS hardening, optimization of antivirus software, and security measures implemented in Vnet/IP to maintain the security of control networks even in an open network environment.

Security is also being enhanced in recent security certification programs. In particular, the ISASecure certification program aims to become an IEC standard and it is attracting attention. In an effort to keep up with this trend, Yokogawa has acquired the certifications of this program for its core products, CENTUM VP and ProSafe-RS.

1. はじめに

制御システムにセキュリティが求められるようになって久しい。横河電機はこれまでもセキュリティに取り組んできたが，効果が見えやすく，即効性のあるセキュリティ機能の実装やサードパーティ製品との連携が中心であった。一方，セキュリティの脅威にいち早くさらされてきた情報システムに目を向けると，製品の弱点を利用した攻撃にさらされてきた。

攻撃に利用される可能性がある弱点は脆弱性と呼ばれ，広く公開されるに至っている。昨今，この波は制御システムにも押し寄せており，制御システム製品の脆弱性が公開される例も増えてきた。

製品のセキュリティを考えるうえで，脆弱性を作りこまない活動はセキュリティ機能の実装に並んで重要な活動であるが，効果が見えにくい上，時間がかかるため，これまで敬遠されがちであった。

横河電機は市場の動向を踏まえ，よりセキュアな製品を提供するため，コントローラを中心に脆弱性を作りこまない活動にも着手した。本稿ではまず脆弱性を作りこまない活動として，セキュア開発ライフサイクルを紹介し，次にセキュリティ機能面での活動例として，製品が動作するインフラのセキュリティ対策として OS の要塞

*1 IA プラットフォーム事業本部グローバル開発センター
システムインテグレーション技術部
*2 IA プラットフォーム事業本部グローバル開発センター
デジタルハードウェア技術部

化（IT セキュリティツール），アンチウイルスソフトの最適化，そして製品のセキュリティとしてリアルタイム・プラント・ネットワークシステム Vnet/IP のセキュリティ対策について紹介する。そして最後に，これらの活動の結果として ISASecure EDSA 認証を取得したことを紹介する。

2. 脆弱性を作りこまない取り組み

2.1 セキュア開発ライフサイクルの概要

脆弱性を作りこまないためには，組織がセキュア開発ライフサイクルを導入し，開発者自身がスキルを身に着ける必要がある。セキュア開発ライフサイクルとは，開発プロセスの各フェーズでセキュリティ対策を行うという考え方である。これは各フェーズのアウトプットに作りこまれる脆弱性を最小限にすることと，開発フェーズの早い段階で脆弱性を見つけることを目的としている。

開発プロセスには様々な手法があるが，本項では**図 1** の開発フェーズをベースに，セキュアライフサイクルの取り組み方法について説明する。

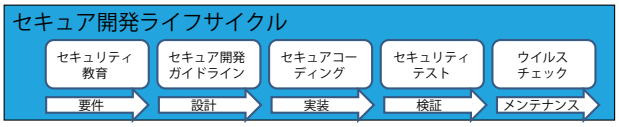

図 1 セキュア開発ライフサイクル概要

2.2 要件フェーズ

本フェーズの主な目的の 1 つは，開発者が脆弱性とはどのようなものか，どのように作りこまれていくのか，そしてどのような対策があるのか，などを理解することである。そのため，開発体制構築の際，アサインした開発者にはセキュリティ教育を実施している。もう 1 つの目的は開発プロセスにセキュリティが盛り込まれていることを確実にチェックするために，セキュリティを監査する第三者を開発体制に組み込むことである。そのため，開発とは独立したセキュリティエキスパートを 1 名アサインし，各フェーズにおけるセキュリティレビューを行うなど，プロジェクトが終わるまで，第三者が，セキュリティが守られているかをチェックしている。

2.3 設計フェーズ

本フェーズの主な目的は，設計時に作りこまれる脆弱性をできる限り排除することである。そのため，設計時に気を付けなければならないセキュリティ視点をまとめてセキュア開発ガイドラインを作成し，開発時には本ガイドに従うことをルールとした。また，開発する機能を設計した段階で脅威分析を行い，各モジュール間のインターフェース，特にネットワークやファイル I/O など，外部との接点となるインターフェースを洗い出し，どのような脅威があるかを分析している。脅威の洗い出しには，STRIDE モデル [1] を用いた。STRIDE モデルは，脅威を 6 つに分類し，それぞれの脅威がないかを検討することで網羅性を高めている。また，洗い出されたすべての脅威に対して DREAD モデル [1] により評価点をつけ，外部との接点となるインターフェースに対しては製品ごとに決めた評価点以上のすべての脅威に対して対策を盛り込むことにしている。DREAD モデルは 5 つの視点で評価点を算出するため，評価者による評価点のばらつきを少なくすることができる。

2.4 実装フェーズ

本フェーズの主な目的は , 実装時に作りこまれる脆弱性をできる限り排除することである。そのため，コーディング時に気を付けなければならないセキュリティ視点をまとめたコーディングガイドを作成し，使用してはいけない API なども定義している。また実装が完了したコードは別の開発者によるコードレビューと静的コード解析ツールによる機械的なチェックを行い，問題が見つかれば修正する。

2.5 検証フェーズ

本フェーズの主な目的は，製品に既知の脆弱性がないことや検討したセキュリティ対策の有効性を確認することである。そのため，脅威分析で想定した攻撃を実際に行い，対策が有効であることを確認している。また，今回の開発で脆弱性が作りこまれていないことを確認するために TCP や Ethernet フレームの異常パケットを作成し，流す（Fuzzing と呼ばれる）などを行っている。既知の脆弱性が存在しないことを確認するために，脆弱性スキャナである Nessus のすべてのプラグインを利用して，テストを実施している。

2.6 メンテナンスフェーズ

本フェーズの主な目的は , 出荷時にウイルスが混入していないことの確認と，出荷後に見つかった脆弱性に対する対応方針や体制を準備することである。そのため，出荷時には開発したモジュールに署名をつけ，不正なプログラムではなく，横河電機が作成したプログラムであることを確認できるようにし，最終ソースコードと出荷用のマスタメディアに対して 3 種類のウイルスチェックソフトを使ってウイルスチェックを行っている。また，JPCERT/CC（一般社団法人　JPCERT コーディネーションセンター）から情報を入手し、独自の調査を実施する体制を構築することで，市場で見つかった脆弱性を監視するとともに，脆弱性の報告を受け付ける窓口を設置し，新たに Web から投稿できるようにした。市場で見つかった脆弱性については脅威分析で定義した評価点に基づき

対応方針を決めている。

3. セキュリティ機能面での取り組み

3.1 概要

昨今は製品単体の機能だけではなく，製品が動作するインフラのセキュリティ機能（OS のセキュリティ機能やサードパーティ製のセキュリティソフトの利用）も活用し，システム全体のセキュリティを高める活動が求められている。本項ではインフラのセキュリティ実装例として OS の要塞化（IT セキュリティツール），McAfee 社のアンチウイルスソフトの最適化を紹介し，製品のセキュリティ実装例としてコントローラのセキュリティ上，最も重要な役割を担う Vnet/IP のセキュリティについて紹介する。

3.2 IT セキュリティツール

Windows OS には様々な機能があり，システム製品が使用しない機能を停止することでその機能が持つ脆弱性をふさぐことができる。また，OS のセキュリティ機能を適切に設定することでシステム製品の動作に影響を与えず，システムを堅牢にすることができる。これら OS の設定はツールを開発するまでもなく，OS 上の設定画面で設定することが可能だが，設定項目が多岐にわたるため，手順が煩雑になり，設定ミスなども起きやすい。

IT セキュリティツールは，顧客ごとの運用に合わせてセキュリティ強度を３つ用意した。互換性を重視するモデルを「従来」，必要最低限多くのユーザ環境で適用しても問題ないセキュリティ項目を設定する「標準」，ユーザ環境に応じて選択が必要なセキュリティ項目（例えばログオンに一定回数失敗したらログオン禁止にするなど）が含まれる「強固」である。ユーザはセキュリティモデルを選択するだけで OS のセキュリティ設定が行われる。

また，共通定義により，セキュリティ強度をいったん強固にしてから，各製品で必要な項目をゆるめる方式を採用することで，複数のシステム製品を 1 台の PC にインストールする場合でも，セキュリティの問題で動作しないことがないように工夫している。

このようなツールの提供は設定ミスなどの人為的なミスを軽減し，それにより生じる脆弱性を防止できる。

3.3 アンチウイルスソフトの最適化

これまでもアンチウイルスソフトの利用は可能であったが，システム製品がインストールされているフォルダの多くをアンチウイルスソフトのスキャン対象から除外するように設定していた。その理由は大きく２つある。１つは誤検知によるシステム停止が許容できないこと。２つ目はウイルススキャンの負荷によるパフォーマンスの劣化が許容できないことである。しかし，除外しているためにシステム製品のフォルダ内にウイルスが紛れ込んでも検知できないため，除外設定の撤廃を望む声は大きい。誤検知やパフォーマンスのリスクがある以上，完全に除外を撤廃することはできないが，McAfee 社とパートナーシップ契約を締結し，感染のリスクを下げるために行った取り組みを紹介する。本取り組みは順次システム製品へ展開していく予定である。

3.3.1 パフォーマンスへの対策

McAfee 社のアンチウイルスソフトにも様々な機能があり，中には制御システムには不要な機能やパフォーマンスを著しく劣化させるものもある。これらの機能を制御システムの特性に合わせるため，各パラメータを最適な値に設定した。また，パフォーマンスの検証を行い，パフォーマンスの劣化が発生するプロセスを特定し，該当プロセスに特別なスキャン定義を行うことで，除外対象をフォルダから実行ファイルに変更することができ，パフォーマンスを確保することができた。

3.3.2 誤検知への対策

システム製品が動作しても変更されない静的なファイルへの誤検知対策は，McAfee 社がパターンファイルをリリースする前に検証し，誤検知を削減するサービスで対応することができた。しかし，システム製品が動作した時に変更される動的なファイルは，McAfee 社の検証の後変更されるため，本サービスでは対応できない。そこで，システム製品が動的に変更する可能性があるファイルの拡張子を登録することで除外対象をフォルダから一部の拡張子のファイルへと変更することができ，誤検知のリスクを削減することができた。

3.4 Vnet/IP のセキュリティ

横河電機の生産制御システムおよび安全計装システムで使用されている Vnet/IP は，イーサネット技術を使用した制御ネットワークである。一般的に使用されるオープンなプロトコルを用いることで市販の Layer 2 Switch や Layer 3 Switch を使用して低コストで拡張性の高いシステムを構築できる。しかし，その反面，広く認知されたイーサネットのインターフェースを持つことによって，ネットワークを介した外部からの悪質な攻撃の対象となりやすい。多種多様なセキュリティ脅威の中でもコントローラに対して与える影響が大きいものとして，なりすまし／改ざんと DoS 攻撃がある。

なりすまし／改ざんは，攻撃者が本来の利用者になりすまして不正な操作を行う攻撃であり，ユーザが期待する制御とは別の制御が実行されてしまう危険がある。本攻撃への一般的な対策としてセキュリティ認証がある。セキュリティ認証では，送信局と受信局との間で定期的に鍵交換を実施して送信局と受信局のみが知っている鍵を共有する。この鍵と通信データから計算される認証コードをパケットに付加し，攻撃者による不正なパケットを識別する。しかし，鍵交換を終えて通信を開始するま

でに一定の時間を要するため，一般的なセキュリティ技術では，定期的に実施する鍵交換の度に通信ができない時間帯が生じる。この結果，定期的に応答時間が延び，リアルタイム性が損なわれてしまう。そこで Vnet/IP では，定期的に発生する鍵の更新処理中もセキュアな通信を継続できるような鍵交換方式を採用している。また，冗長化されたコントローラの制御側が故障して待機側コントローラへ制御権を切り替える際や通信経路が切断されて冗長化されたもう片方の経路へ切り替える際，切り替え後に鍵交換を開始していては通信を速やかに再開できない。そこで Vnet/IP では，冗長化されたコントローラの全ポートに個別の IP アドレスを持たせ，それぞれのポートで常時独立して鍵交換を実施することで，コントローラまたは通信経路が冗長化側へ切り替わったのち，瞬時に通信を開始できるようにしている。

DoS 攻撃は，アクセスを一度に集中させて正常動作を阻害する攻撃であり，コントローラが過負荷状態に陥り，期待通りにプラント制御処理が実行できなくなってしまう。本攻撃への一般的な対策として外付け機器による防御やアプリケーション層でのパケット破棄がある。しかし，外付け機器を使用した場合には機器の遅延により，アプリケーション層でパケットを破棄した場合には CPU 負荷上昇により，リアルタイム性が低下する。そこで Vnet/IP では，制御と通信を別々の CPU で処理することで通信層での負荷が制御処理に影響を与えないようにしている。また，通信階層の下位レベルで不要なパケットを破棄し，処理負荷を低減させる仕組みや，冗長化した経路の一方で規定量以上のパケットを受信した場合に，一定時間当該経路での受信を停止して別の経路で通信を継続する仕組みを実装している。

4. ISASecure EDSA 認証の取得

4.1 EDSA 認証の概要

EDSA 認証は ISA/IEC62443 標準のフレームワークを使った組み込みコントローラ向けのセキュリティ保障に関する認証制度である。組み込みコントローラがセキュリティを確保できているかを第３者機関が以下の３つの視点で評価する。

- 開発プロセスでセキュリティが考慮されているか
  （SDSA : Software Development Security Assessment）
- 必要なセキュリティ機能が実装されているか
  （FSA : Functional Security Assessment）
- 通信の堅牢性が確保されているか
  （CRT : Communication Robustness Testing）

さらに，それぞれの視点にはセキュリティ強度に合わせて３つのレベルがあり，レベルが高くなるにつれて満たさなければならない項目が多くなる。ただし、CRT はレベルに関係なくすべての要件を満たす必要がある。

4.2 EDSA 認証における横河電機の取り組み

EDSA 認証を取得するためには評価機関の審査と CRT を含む実機を使ったテストをクリアする必要がある。SDSA ではレベル 1 で 130 もの要求項目があり，開発プロセスに必要な要求項目がすべて含まれているかという点と，その開発プロセスに沿って開発されているか（レビューの議事録などのエビデンスが残されているか）という点が審査される。FSA も SDSA と同じく，仕様書や設計書などから要求項目にある機能が実装されていることが審査され，さらに一部機能は実機を使い，機能を確認される。CRT は取得する認証レベルに関係なく，すべての項目がテストされ，テスト中やテスト後にコントローラの出力が不適切な値にならないことが要求される。

前項で紹介したセキュリティの取り組みは EDSA 認証取得に際しても有効であった。SDSA にはセキュア開発ライフサイクルで，FSA にはセキュリティ機能面での取り組み（その他，今回紹介していない機能も含む）で，CRT には Vnet/IP のセキュリティで対応している。

4.3 EDSA 認証取得製品

横河電機は生産制御システムと安全計装システムの２つのコントローラで本認証を取得した。取得製品の詳細を**表 2** に示す。

表 2 EDSA 認証取得製品一覧

製品名	バージョン	セキュリティレベル
CENTUM VP	R5.03.00	EDSA 2010.1 Level1
ProSafe-RS	R3.02.10	EDSA 2010.1 Level1

5. おわりに

本稿では脆弱性を作りこまないための取り組みを述べ，セキュリティ機能面での取り組みも述べた。また，それらの取り組みは横河電機独自の考えではなく，市場で認知されている考えであることの一例として ISASecure EDSA 認証を取得していることを紹介した。

横河電機は日々変化するセキュリティの脅威に対抗するため，システム視点に立ったセキュリティ対策を継続的に提供する。

参考文献

(1) Michael Howard, David LeBlanc, Writing Secure Code, Second Edition, Microsoft Press, 2002