YOKOGAWA グループの製品セキュリティへの取り組みと脆弱性対応

Yokogawa's Approach to Enhancing Security of its Products and Handling of their Vulnerability

辻 宏隆 *1
Hirotaka Tsuji

今日，情報システムだけでなく制御システムにおいてもサイバー攻撃のリスクが認識され，YOKOGAWA グループの事業においてもセキュリティがお客様の重要な要件となってきている。YOKOGAWA グループは，企業理念であるお客様満足を実現していくため，製品とサービスを通してお客様環境のセキュリティを確保していくことに，これまで以上に取り組んで行かなければならない状況にある。2014 年，YOKOGAWA グループは統合生産制御システム CENTUM CS 3000 の脆弱性を公開するという事案を経験した。この事案は YOKOGAWA グループにとって初めてユーザー以外へ脆弱性情報を公開した事例であり，対応過程においていくつかの課題が見つかった。脆弱性情報社内連絡体制事務局 YPOC (YOKOGAWA Point of Contact) は，今回の脆弱性対応を契機に，脆弱性対応基準と体制について，グループ規程としての発行を視野に入れた見直しを行った。本稿ではこの脆弱性対応基準と脆弱性対応体制について報告する。

These days, the risk of a cyber-attack is recognized on not only information systems but also industrial control systems, and for Yokogawa's business, security has become an important requirement for our customers. Customer satisfaction is inherent in Yokogawa's corporate philosophy and to achieve it Yokogawa needs to work harder, through its products and services, to ensure the security of customers' environments. In 2014, Yokogawa disclosed a vulnerability in the CENTUM CS 3000 integrated production control system. This is the first time that Yokogawa disclosed a vulnerability to people other than users, and several problems were found while responding to these. Taking this opportunity, Yokogawa Point of Contact (YPOC) revised the vulnerability handling standards and system with a view to issueing them as rules for the entire Yokogawa Group. This paper describes these standards and system.

1. はじめに

従来，制御システムは独自のアーキテクチャや独自プロトコルで構成された独立したシステムであり，ビジネスネットワークとも分離されていたことから，セキュリティについてあまり考慮されていなかった。一方 IT 技術の発展とコストダウンによりコモディティ化した技術が制御システムに採用されるようになった。さらに利便性や経営情報など他の情報との連携を理由として，制御システムがビジネスネットワークと接続されるようになってきた。その結果，情報システムにおけるセキュリティの脅威が制御システムにおいても顕在化し始めており，制御システムのセキュリティ対策への関心が高まっている。

*1 IA プラットフォーム事業本部共通技術開発センター
技術推進部

2. 製品セキュリティへの取り組みの必要性

2.1 制御システムセキュリティの現状

2010 年，制御システムを攻撃対象とする初のマルウェアと言われる Stuxnet(1) の出現以来，制御システムのセキュリティを取り巻く状況は急速に変化している。

1) サイバー攻撃の多様化

近年のサイバー攻撃は，犯罪者集団による金銭目的のフィッシング詐欺や共通思想集団による自己主張のための Dos 攻撃，軍事組織による情報搾取など多種に及んでいる。攻撃手法においてもやり取り型攻撃や水飲み場型攻撃など新しい攻撃手法が現れている。

2) サイバー攻撃の容易性

インターネット上では攻撃用のツールや情報が簡単に手に入る状況にあり，攻撃にかかるコストは下がってい

ることから，攻撃に関する技術的，経済的障壁は下がってきている。

3) 制御システムのオープン化

制御システムに汎用技術が適用されるようになった。ビジネスネットワークと接続される事が増えた。

4) 制御システムセキュリティに関する研究・調査

制御システムセキュリティに関する研究や調査が行われ，制御システムを構成するソフトウエア製品や機器の脆弱性レポートがイベントや Web で公開されている。これら公開される情報には検証用ツールとして攻撃ツールが含まれている場合もある。

5) 製品ベンダーの責務

製品を供給するベンダーは，セキュアな製品の供給に努めることはもちろんのこと，自身の製品の脆弱性に関して，対策情報を含む脆弱性情報をユーザーに提供しなければならない。このような認識が IT 製品を扱うベンダーに限らず制御システムのベンダーに対しても求められるようになった。

このように，制御システムのセキュリティを取り巻く状況は大きく変わってきている。しかし制御システムの可用性重視の運用状況は変わっておらず，一旦稼働を始めると簡単に止めることができない。また制御システムの寿命は数十年に及ぶなど長期間使用されることが多い。そのため多様化したサイバー攻撃への対策がタイムリーに行えないケースや最新のセキュリティ対策が適用できないケースなどお客様環境のリスクは年々増大している。

2.2 YOKOGAWA グループにおける製品とサービスのセキュリティ向上の取り組み

YOKOGAWA グループは，これまで品質改善活動による製品やサービスの品質向上や秘密情報管理，危機管理によるリスクマネジメントに積極的に取り組むことで，製品とサービスのセキュリティ向上に取り組んできた。YOKOGAWA グループの製品とサービスのセキュリティ向上への取り組みを概念的に**図 1** に示す。

品質改善活動により，製品品質が改善されれば，製品の脆弱性は減少し，セキュリティ品質も改善される。秘密情報管理により製品の設計情報や脆弱性情報が適切に管理されることで，攻撃に利用できる情報が安易に攻撃者に渡ることは無くなる。YOKOGAWA 製品へのサイバー攻撃が原因でお客様に甚大な損害あるいは人命にかかわるような事故が発生した場合，それは危機管理に該当し，危機管理規程に沿って対応されなければならない。しかし，お客様環境のセキュリティを確保し，向上していくためには品質改善や秘密情報管理，危機管理に取り組むだけでは十分でない。それらに加えサイバー脅威へ対応していかなければならない。セキュアな製品の提供や脆弱性対応に取り組むことが今まで以上に重要になっている。

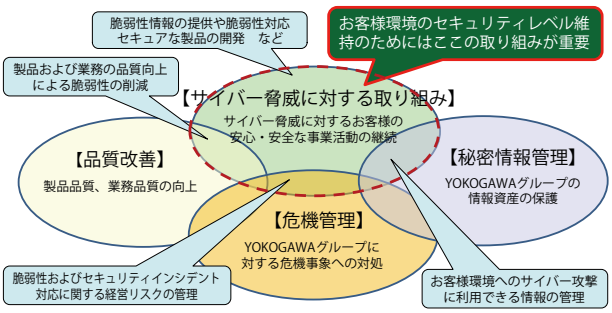

図 1 YOKOGAWA グループにおける製品とサービスのセキュリティ向上の取り組み

2013 年まで YOKOGAWA グループの製品で脆弱性情報が一般公開された製品はなかった。2014 年 3 月，セキュリティベンダーから米国の脆弱性情報調整機関である CERT/CC (Computer Emergency Response Team/Coordination Center) への通報がきっかけで，統合生産制御システム CENTUM CS 3000 の脆弱性情報を公開するに至った。CENTUM CS 3000 の脆弱性の公開に当たり，組織をまたぐ対応が必要となり，そこに統一された基準や手順の必要性がグループ内で認識された。YOKOGAWA グループは，お客様満足を理念に掲げ，品質改善や秘密情報管理に取り組むことで製品・サービスセキュリティに取り組んできた。近年の制御システムを取り巻く状況の変化に対応し，お客様満足の理念を実現するため，脆弱性対応をはじめとする製品・サービスのセキュリティに対して更なる取り組みを進めていく。

3. 脆弱性対応

3.1 脆弱性とは

脆弱性について，経済産業省告示第二百三十五号「ソフトウエア等脆弱性関連情報取扱基準」[2] では

- ソフトウエア等において，コンピュータウイルス，コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所

と定義されている。また，同告示においてソフトウエア製品は以下のように定義されている。

- ソフトウエア又はそれを組み込んだハードウエアであって，汎用性を有する製品

脆弱性とソフトウエアの不具合は混同されることが多く，実際，脆弱性の原因となるのは不具合であることが多い。しかしお客様の通常の使用状態でシステムのハングアップなどを引き起こす不具合と異なる。脆弱性はお客様の通常の使用環境においてはリスクが潜在している状態であり，攻撃によって初めてシステムのハングアップなどのインシデントへ移行する。脆弱性対応は，セキュリティインシデント発生の予防の観点から，潜在的リスクの状態での対応が必要である。

3.2 日本における脆弱性情報取り扱い体制

平成 16 年，経済産業省告示第二百三十五号「ソフトウエア等脆弱性関連情報取扱基準」が告示された。これを契機に脆弱性情報取扱い体制が構築された（**図 2**）。脆弱性情報の受付を独立行政法人 情報処理推進機構（IPA）が行い，脆弱性対応の調整を一般社団法人 JPCERT コーディネーションセンター（Japan Computer Emergency Response Team Coordination Center）が行っている。この体制は情報セキュリティ早期警戒パートナーシップガイドライン [3] に沿って運用されており，国内においてコンピュータ不正アクセスやコンピュータウイルスなどによる被害発生を抑制することを目的としている。このガイドラインの 2014 年版ではソフトウエア製品の補足説明に制御システムの説明が追加され，脆弱性取扱いの対象が IT 製品だけでなく制御システムおよびそれらを構成する製品も含まれることが明示された。

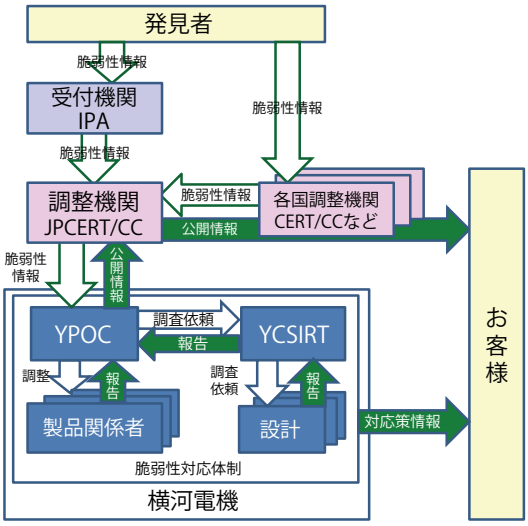

図 2 横河電機の脆弱性対応体制

3.3 脆弱性対応実施規程

市場やお客様により，期待される脆弱性への対応はそれぞれ異なる。横河電機では，脆弱性への対応はお客様の要件の一つとして事業ごとあるいは組織ごとに対応してきた。今回の CENTUM CS 3000 の脆弱性対応において，他の製品への影響が及んだことにより，YOKOGAWA グループとしての対応基準と対応体制の必要性が認識された。現在 YPOC (Yokogawa Point of Contact) が中心となり，脆弱性対応規程を策定している。この規程は YPOC 管理文書として，YPOC が脆弱性情報をハンドリングする場合の業務基準，手順として運用していく。現在，YPOC ではこの脆弱性対応規程をグループ規程として発行するための作業を進めている。その概要をここで解説する。

1) お客様環境のリスク軽減の取り組み

お客様環境のリスク軽減のため，以下に取り組むことを明記している。

- ■ 最新の脆弱性情報の収集に努める。
- ■ 製品への脆弱性の作り込みおよび混入の防止に努める。
- ■ 脆弱性情報およびセキュリティ情報の適切な管理を行う。
- ■ 脆弱性発見時には，お客様への速やかな情報提供および回避策，対策の提供を行う。

横河電機は，最新の脆弱性情報を把握することに努め，それを業務にフィードバックし，開発プロセスの改善や業務の基準・手順の見直しを行う。セキュアな製品をお客様へお届けすることはもとより，最新情報に基づき脆弱性対策・回避策をお客様へ提供するなどの支援に取り組む。また変化する状況へも対応して行く。

2) 脆弱性発見時の責務

製品に脆弱性が発見された場合の対応を，情報の受付から公表まで脆弱性ハンドリングフローに沿って，業務ごとに責務を定め，各業務で行うことを明確にしている（**図 3**）。この体制を運用していくことで，横河電機は入手した脆弱性情報を迅速にお客様へお伝えし，お客様のリスクを増大させないよう取り組んで行く。

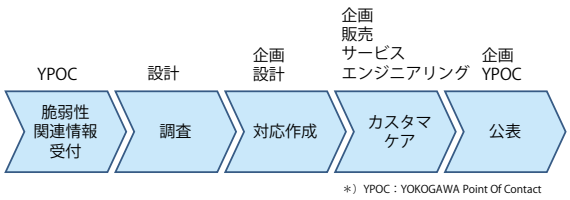

図 3 脆弱性情報ハンドリングフローと業務の責務

3) 脆弱性発見時の対応基準

脆弱性対応を行うに当たり，以下の項目などについて対応基準を明記している。

- ■ 脆弱性対応責任
- ■ 脆弱性情報の提供方法
- ■ 脆弱性情報の提供時期
- ■ 提供する脆弱性情報の内容
- ■ 対策・回避策提供

横河電機として対応の基本方針を定め，現場においてお客様に信頼していただけるよう取り組んで行く。

3.4 横河電機の脆弱性対応体制

1) 社外機関との連携

横河電機は 2005 年より，情報セキュリティ早期警戒パートナーシップガイドラインに則り，調整機関 JPCERT コーディネーションセンターとの窓口である YPOC を設置し，脆弱性に関する最新情報の収集と対応にあたっている。またこれら社外機関と連携すると共に海外 CERT 機関とも連携して取り組んでいる。

2) 社内体制

社内においてはYPOCを中心とし，製品群ごとに担当者を配置した脆弱性情報社内連絡体制：YCSIRT (Yokogawa Computer Security Incident Response Team) を組織し，脆弱性情報の迅速な社内展開と影響調査を行っている（**図 2**）。

YPOCでは影響調査結果を基に，脆弱性対応において，対応方針の策定からお客様への連絡情報の作成，Webによるお客様への通知など，脆弱性影響製品担当部署の作業をサポートし，脆弱性対応全体の調整を行っている。

このように横河電機では脆弱性に対応するための体制を構築しており，お客様に提供する製品に脆弱性が確認された場合，脆弱性対応実施規程に沿って対応している。お客様のリスクを増大させないよう，お客様へ正確な情報の速やかな伝達に努めている。

4. おわりに

制御システムのセキュリティはお客様の重要な要件の一つであり，今後その重要性は増していくと思われる。YOKOGAWA グループは，制御システムのセキュリティ実現に取り組んでいくが，お客様環境のセキュリティレベルの維持は，YOKOGAWA グループ内部での取り組みだけでは実現できるものではない。YOKOGAWA グループの取り組みをお客様に説明し，ご理解いただいた上で，共に取り組んでいくことが不可欠である。

YOKOGAWA グループは，お客様が行う生産環境のセキュリティレベル維持の取り組みを，製品とサービスを通して支援していく。この支援を継続的に行っていく上で，世の中の状況や技術的な変化にも追従していかなければならない。そのためにも社外組織，機関とも協力して製品・サービスのセキュリティ実現に取り組んで行く。

参考文献

(1) 小熊信孝，“Stuxnet- 制御システムを狙った初のマルウェア –”，JPCERT/CC，2011-03-02，
https://www.jpcert.or.jp/ics/2011/20110210-oguma.pdf
(2) 経済産業大臣，“告示第百十号「ソフトウエア等脆弱性関連情報取扱基準」”，経済産業省，2014-05-14，
http://www.meti.go.jp/policy/netsecurity/downloadfiles/140514kaiseikokuji.pdf
(3) 情報システム等の脆弱性情報の取り扱いに関する研究会，“情報セキュリティ早期警戒パートナーシップガイドライン ”，独立行政法人 情報処理推進機構，改訂第 8 版，2014-05-30，
http://www.ipa.go.jp/files/000039236.pdf