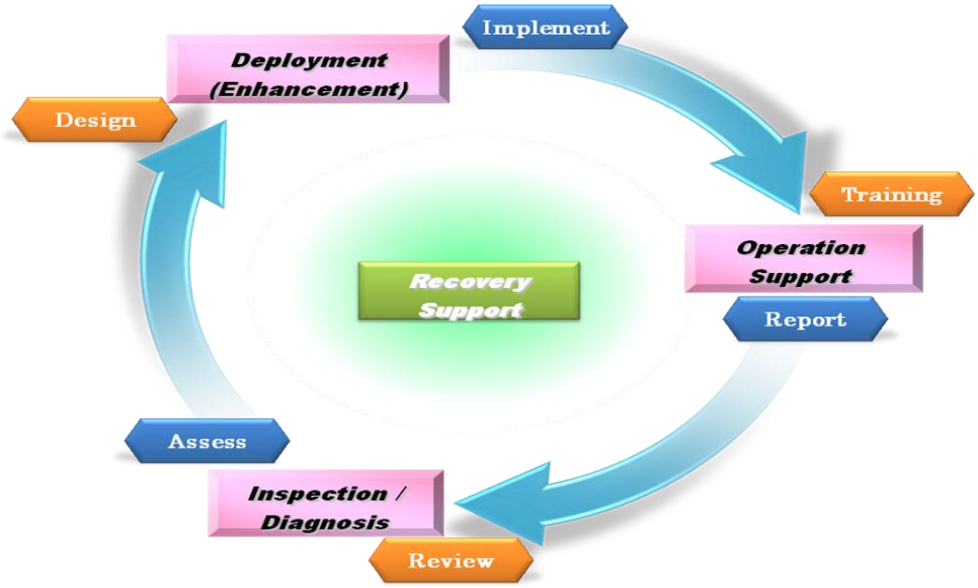
ARC 白書

ARC Advisory Group 作成

2011 年 9 月

プロセス制御システムに最適なセキュリティライフサイクル
横河電機の包括的なアプローチ



Yokogawa Security Lifecycle

Yokogawa Security Lifecycle Concept

概要

現代の生産制御システムは、高度な IT ソリューションを導入し、コスト削減、パフォーマンス改善を実現しています。また、さまざまな重要な機能を取り入れ、相互運用性も実現しています。しかし、この IT ソリューションを導入したことにより、生産制御システムはプラント内外からのセキュリティ脅威にさらされてきています。これまで、IT 業界は強力なツールと技術を開発し、こうした脅威を確実に、防止し、検出し、そして軽減してきました。しかし、工業用システムには特有の要件（例えば、連続運転や高応答性）があるため、生産制御システムにこうしたツールや技術をそのまま導入すると問題を引き起こす可能性があります。

近年のセキュリティ脅威は、生産制御システムだけでなく、生産プロセス、知的財産を危険にさらすだけでなく、作業員の健康、安全、環境にも悪影響を及ぼします。生産制御システムのユーザのみならず、システムベンダは、このような脅威に対し対策を講じていく必要があります。

近年のセキュリティ脅威は、生産制御システム、生産プロセス、知的財産を危険にさらすだけでなく、作業員の健康、安全、環境（HSE：Health、Safety、Environment）にも悪影響を及ぼします。生産制御システムのユーザのみならず、システムベンダは、このような脅威に対し対策を講じていく必要があります。

生産制御システムは、一般的な商用システムに比べてはるかに長い耐用年数を実現しなければなりません。商用システムの耐用年数は 3 年から 5 年であるのに対して、工業用システムは 15 年以上といわれています。また、システムの技術が常に進化しているのと同様に、脅威（攻撃技術）も常に進化しています。これは、セキュリティ対策を一度だけ導入すれば終わりではなく、常に対策を見直していく必要があることを意味します。したがって、制御システムベンダは、セキュリティ対策に対して、ライフサイクルアプローチを採用しなければなりません。具体的には、リスク評価、セキュリティ対策の実装、対策の有効性の監視、対策の保守に関して改善プロセスが常に必要となります。プロセスオートメーションシステムとその関連技術、そしてサービスを提供している世界のリーダ企業の一つに横河電機があります。本白書で述べているように、この横河電機は、CENTUM プロセス制御システム、ProSafe-RS 安全システム、STADROM、FAST/TOOLS SCADA システム、並びに関連する装置、ソフトウェアアプリケーションに対し、ライフサイクルアプローチを導入しています。

横河電機は、業界のセキュリティスタンダードに基づき、セキュリティライフサイクルアプローチを構築しています。これには、自社のセキュリティスタンダードとエンジニアリングスタンダードを組み込んだ独自の製品セキュリティポリシが包含されています。

はじめに

DCS、SIS、SCADA など過去の Industrial Automation（IA）システムは、独自のハードウェア、ソフトウェア、そしてプロトコルを使用していたため、クローズ型であり、他システムと接続することができませんでした。これは、他社システムとの相互運用に課題を残すものの、セキュリティの観点からは比較的安全でした。もちろん、これまでも不注意や不満を抱く従業員により、生産制御システム、会社組織あるいはその知的財産に損害を与える機会が存在していたことは言うまでもありません。

現在の生産制御システムは、一般的に利用されている高度な IT ソリューションを導入することにより、コストを削減し、パフォーマンスを向上させ、相互運用性を実現とすると共に、その他の新しい新規機能をも導入してきました。しかし、まさにこうした技術を導入したことで、現在のシステムは、工場施設の内外からの攻撃にさらされています。

ARC Advisory Group が考える現代のプロセス制御システムは、オープンであり、異なるシステムが相互に運用可能なシステムです。これを Collaborative Process Automation System (CPAS)と呼びます。そしてまさに、現在の生産制御システムは、この CPAS に近づいています。加えて、現在のシステムには、一般向けに開発され、インターネットに接続可能な IT 技術が組み込まれています。ARC は、こうした技術を Commercial Off-The-Shelf（COTS)として説明してきました。

結果的に、現在の生産制御システムは、こうした一般的に利用されている高度な IT ソリューションを導入することにより、コストを削減し、パフォーマンスを向上させ、相互運用性を実現とすると共に、その他の新しい機能をも導入してきました。しかし、まさにこうした技術を導入したことで、現在のシステムは、工場施設の内外からの攻撃にさらされています。これまで、IT 業界は強力なツールと技術を開発し、こうした侵入を防止し、検出し、そして、軽減 してきました。しかし、生産制御システムには特有の要件（例えば、連続運転や高応答性）があるため、システムにこうしたツールや技術をそのまま導入すると問題を引き起こす可能性があります。

状況を一層悪化させている問題として、ハッカーの技術がますます高度になっていることがあります。ハッカーは、さまざまなツールや手法を開発してきています。それらを用いた極めて高度な攻撃が、生産制御システムとそのネットワークに向けられている事実は、もはや無視することができません。例として Stuxnet と Night Dragon があります。Stuxnet はシーメンス社のシステムを攻撃するマルウェア[1]で、Night Dragon は、エネルギー業界を狙う攻撃のことです。これまで、産業界では多くの企業が、自社システムとネットワークは外部には知られていないため、サイバー攻撃に対して安全なものとしてきました。しかし、もはやこうした考えは時代遅れです。

[1] コンピュータウィルスの総称。コンピュータウィルスには、ワーム、ウィルス、トロイの木馬などがある

現在のセキュリティの脅威は、生産制御システム、生産プロセス、知的財産を危険にさらすだけでなく、作業員の健康、安全、そして、環境にも悪影響を及ぼします。生産制御システムのユーザだけでなく、システムベンダは、このような脅威に対して、現在だけでなく将来にわたり、対策を講じていく必要があります。

個々のユーザ、システムベンダ、業界団体、政府のみならず、IT 業界やユーザが連携し、常に進化し続ける脅威に対して、効果的な防止策と対抗策を講じる必要があります。

個々のユーザ、システムベンダ、業界団体、政府のみならず、IT 業界やユーザ団体が連携し、常に進化しつづける脅威に対して、効果的な防止策と対抗策を講じる必要があります。

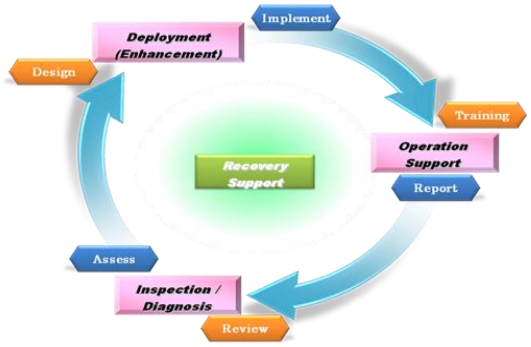
工業用プロセス制御システムは、一般的な商用システムに比べてはるかに長い耐用年数を実現しなければなりません。商用システムの耐用年数が 3 年から 5 年であるのに対して工業用システムは 15 年以上といわれています。また、システムの技術が常に進化しているのと同様に、脅威（攻撃技術）も常に進化しています。これは、セキュリティ対策を一度だけ導入すれば終わりになるのではなく、対策を常に見直していく必要があることを意味します。したがって、システムベンダは、セキュリティ対策に対し、ライフサイクルアプローチを採用しなければなりません。具体的には、リスク評価、セキュリティ対策の実装、対策の有効性の監視、対策の保守に関して改善プロセスが常に必要とされます。プロセスオートメーションシステムと関連技術、そしてサービスを提供している企業のひとつに横河電機があります。本白書でも述べているように、この横河電機は、CENTUM 生産制御システム、ProSafe-RS 安全計装システム、STADROM、FAST/TOOLS SCADA システム、並びに関連する装置、ソフトウェアアプリケーションに対し、ライフサイクルアプローチを導入しています。横河電機では、業界が作成したセキュリティスタンダードに基づき、セキュリティライフサイクルアプローチを構築しています。これには、自社のセキュリティスタンダードやエンジニアリングスタンダードを組み込んだ独自の製品セキュリティポリシが包含されています。

セキュリティライフサイクルアプローチ

サイバーセキュリティの専門家の見解は、生産制御システムであるかどうかに関わらず、十分な時間とリソースさえあれば、専門的ハッカーはどのようなシステムでも侵入できるということで一致しています。ネットワークを介して他のシステムやインターネットに接続されているシステムは、ネットワーク化されていない単体システムに比べてさらに脆弱です。また、ネットワーク経由でなくとも、ウィルスやトロイの木馬などのマルウェアがシステムに侵入する方法はいくつもあります。例えば、Stuxnet は、Windows PC の USB 経由で侵入することも可能です。

このような状況に対し、横河電機は包括的なセキュリティライフサイクルを提供しています。このセキュリティライフサイクルは、システム製品、インテグレーションサポ

ート、セキュリティ管理サポートを含み、ユーザのシステムをそのライフサイクルに渡り、サポートしています。このセキュリティライフサイクルを導入することで、システムのパフォーマンスを落とすことなく、また過度なコストを生じることなく、セキュリティの脅威をユーザが受け入れ可能な水準にまで最小化できると考えています。ユーザがシステムを安定して運用できるように、横河電機は業界が作成したセキュリティスタンダードに基づき、セキュリティライフサイクルアプローチを構築しています。さらには、自社のセキュリティスタンダードやエンジニアリングスタンダードをも包括した独自の社内製品セキュリティポリシを構築しています。



Yokogawa Security Lifecycle

横河電機は、セキュリティ分野での高度な競争力を維持するために、人材並びに技術開発への投資を行っています。また、セキュリティの国際規格策定へのサポートを行い、自社内ではエンジニアリングの標準化を進めています。システム製品、プラットフォーム及びシステムインタフェースの開発において、セキュリティの問題に十分に注意を払い、さまざまなライフサイクルサービスを提供しています。こうした取り組みは、ユーザがセキュリティの脅威を無理のない限りできるだけ低く(As Low As Reasonably Practicable; ALARP)抑えることができるようにサポートすることを目的としています。

出発点

ARC は、システムベンダとユーザが適切な業界スタンダードを最大限に遵守することを強く推奨しています。サイバーセキュリティは比較的新しい分野ですが、一般の IT 業界のみならず、基幹 IA システム分野でも多数の重要なスタンダードが国内外で策定され、それらは統合されようとしています。こうしたスタンダードでは、一般の IT セキュリティのみならず、生産制御システムに固有のセキュリティ要件(ポリシや手順、技術などを含む)をも規定しています。多くの生産制御システムは一般の IT 技術を導入していることから、IT セキュリティも生産制御システムのセキュリティに必要なものとなっています。また、問題点として、生産制御システム専門のセキュリティ専門家がいないことから、企業の IT 担当が生産制御システムのセキュリティを担当していることがあります。

横河電機が採用しているセキュリティライフサイクルアプローチは、現在までに策定されている全ての工業用セキュリティスタンダードを把握した上で作成されています。さらに、横河電機は策定中の関連するスタンダードを綿密に調査しています。

横河電機が採用しているセキュリティライフサイクルアプローチは、現在までに策定されている全ての工業用セキュリティスタンダードを把握した上で作成されています。さらに、横河電機は策定中の関連するスタンダードを綿密に調査しています。

こうしたものののなかには、ISA S99 シリーズ、ISO/IEC 27000 シリーズ、及び NIST SP 800 シリーズなどがあります。また、横河電機のセキュリティ専門家は、作業部会や技術委員会への参加を通して、積極的に主要な工業用スタンダードへの取り組みを行っています。そのなかには、ISO/IEC (JTC1/SC27、

WG3、WG4）、IEC（TC65/WG10、TCS7/WG15)並びに ISA（ISA S99、ISA Security Compliance Institute)があります。

横河製品セキュリティポリシ

横河電機は、業界のセキュリティスタンダード(ISA S99、NIST SP シリーズ等)に基づき、自社の IA 製品のセキュリティポリシを策定しています。IA 製品、システム並びにアプリケーションの機能を保全すると共に、ユーザの製造関連の情報資産の完全性を保護する安全な IA 製品を提供しています。製品セキュリティポリシは、基本セキュリティポリシと各製品に応じたセキュリティスタンダードから構成されています。さらに、このセキュリティポリシは、製品ライフサイクルでの計画、研究・開発、製造・エンジニアリング、品質保証、販売、アフターサービス等の個別フェーズ毎に規定されています。

これらは常に更新していく必要があり、横河電機内の運営委員会で定期的に見直されています。横河電機は、こうした方法により継続的にセキュリティポリシと内部スタンダードを更新し、ユーザに対して最も効果的な保護手段を明確にして提供しています。

システムセキュリティスタンダード

横河電機は、生産制御システムとアプリケーションを脅威から保護するため、セキュリティ対策のガイドラインとベストプラクティスを提供しています。これらにより、ユーザの製造関連資産へのリスクを最小限に抑えることが可能になります。システムセキュリティスタンダードは、リスクとその対策を可能な限り理解しやすい言葉で記述されたもので、業界スタンダードを参照して作成されています。

横河電機のシステムセキュリティスタンダードは、システム構成とシステム管理の課題を記載し、そして、以下の項目を記述しています。

- 生産制御システムを取り巻く**セキュリティ環境**と関連リスクの概要
- **情報セキュリティ管理システム**の体系的枠組みの策定
    - 特定の脆弱性の識別と保護対策の計画と実施
- **セキュリティ対策**の策定
    - ネットワークアーキテクチャ、ウィルス対策、パッチ管理、システムハードニング、システム及びネットワークの監視、Windows ドメイン管理、さまざまな横河電機のシステムのセキュリティ機能、並びにスタッフに対するセキュリティポリシ
- **物理セキュリティ対策**の策定

- 物理的境界の定義、リムーバブルメディアの管理、サードパーティによる保守の管理等

- **ビジネス継続プラン**を作成するためのガイドラインの策定
  - セキュリティ脅威によるリスクと損害の最小化

横河システムセキュリティスタンダードは、CENTUM VP および CENTUM CS 3000 生産制御システム、ProSafe-RS 安全計装システム、STARDOM 及び FAST/TOOLS SCADA システムをその対象製品としています。また、このスタンダードでは、横河電機の提供する多数のソフトウェアパッケージ、即ち、Exaquantum 設備傾向分析パッケージ、Exapilot 運用効率向上支援パッケージ、Exaopc 汎用 OPC サーバ、Exaplog イベント解析パッケージ等も対象製品としています。

横河システムセキュリティスタンダードは、全てのライフサイクル（開発、システムインテグレーション、サポートサービス）に渡り、主要な脅威と対策を網羅した多数の文書で構成されています。構成文書としては、以下の文書があります。

- IA システムスタンダード
- アプリケーションセキュリティ
- エンドポイントセキュリティ
- ネットワークセキュリティ
- 統合管理システム

また、システムスタンダードは、システムのハードニング、ネットワーク、ユーザ管理、監視、保守及びその他を目的として、ベストプラクティスも記載してします。

グローバルエンジニアリングスタンダード

横河電機では、グローバルエンジニアリングスタンダード(GES：Global Engineering Standard)を作成し、これを地理的に分散して配置されているリソースを活用したプロジェクトの実行に活用しています。このスタンダードは、物理セキュリティとサイバーセキュリティを含む幅広い重要分野を対象にしています。このスタンダードは、横河電機がグローバル展開している組織において、言語、文化、専門知識の多様性に対して横櫛を通す役割を担い、世界中のどこに配置されていても横河電機の IA システムに対するベストプラクティスを確実なものとします。現在までに作成されている GES を以下に示します。

- セキュリティ及び管理
- ファイアウオール
- ネットワーク管理システム
- リモートアクセス

- アンチウイルスソフトウェア
- OS パッチ管理
- Windows ドメイン管理
- バックアップ及びリカバリ

システム製品、プラットフォーム、コミュニケーションチャネル

IA システムソリューションは個々のハードウェア製品とソフトウェア製品で構成されています。これらは、共通プラットフォーム上に存在し、さらにこのプラットフォームには、システムの内部か外部かを問わず、個々の製品を接続するために、さまざまなインタフェースが存在しています。多層防御(Defense in depth)を実現するためには、まず、各システムコンポーネントとそのコミュニケーションチャネルに対して設計段階から適切にセキュリティを考慮しておくことが必要です。そして、各コンポーネントを適切に統合し、その後、運用、管理によるサポートが必要となります。また、多層防御には、プラントネットワークと外部ネットワーク間(ファイアウオールで保護された DMZ を経由)、そしてプラントネットワーク内に適切なセキュリティが必要とされ、かつ個々のワークステーションに対しても強固で十分配慮のなされたエンドポイントセキュリティを導入することが求められます。

セキュリティゾーンとコミュニケーションチャネル

セキュリティを確実なものとするには、システムベンダは、システム製品の物理的あるいは論理的グループに対して、セキュリティ保証レベル(SAL: Security Assurance Level)を満たす必要があります。この SAL は、プラントエリアやセキュリティゾーンの個々の要件に応じて設定する必要があります。セキュリティゾーンとは、共通のセキュリティ要件が適用される物理的資産、情報資産、アプリケーション資産の論理的グループのことで、ANSI/ISA S99 で定義されています。SAL とセキュリティゾーンは安全度水準(SIL:Safety Integrity Level)と似ていますが、この SIL はプロセスの保護や安全システムに適用されるもので、IEC61508 で定義されています。

横河電機のシステム製品は安全とセキュリティを確実にするために必要とされる信頼性と堅牢性を有していると、横河電機は述べています。また、横河電機では、ゾーン間(システム侵入の一次ターゲット)に適切な SAL を設定したコミュニケーションチャネルを設けています。こうしたコミュニケーションチャネルは、ゾーン間、コンポーネント間、及びインタフェース-コンポーネント間に設けられています。

個別システム製品へのセキュリティ設計

セキュリティをあとから付け足すのではなく、横河電機のライフサイクルアプローチと整合性がとれるように、システムアーキテクト、エンジニア及び製品開発の担当者は、白紙の状態からセキュリティを意識して製品設計を開始しています。

セキュリティをあとから付け足すのではなく、横河電機のライフサイクルアプローチと整合性が取れるように、システムアーキテクト、エンジニア及び製品開発の担当者は、白紙の状態からセキュリティを意識して製品設計を開始しています。また、こうすることでセキュリティを製品仕様へ反映することが可能になっています。このコンポーネント仕様レベルでセキュリティを考慮することは、システムを統合する段階で高度なセキュリティを実現することが可能となります。

製品開発の段階では、横河電機の開発エンジニアは、サードパーティ製のツールを活用し、ソフトウェア製品のソースコードを検証しています。これにより、脆弱性やその原因をあらかじめ除去しています。

商品化に先だって、横河電機のシステム製品は、自社で作成した内部スタンダードに基づいた極めて厳格な内部保証プロセスにより、認証が行われます。さらに、製品ライフサイクルの根幹の一つとして、横河電機の製品は、外部セキュリティコンサルタントにより、これまでの経験や実証済みの技術に基づいたセキュリティ評価が行われています。

また、このライフサイクルアプローチの一部として、世界中のさまざまな場所で勤務する横河電機の開発エンジニアは、最新の脅威や潜在的な脆弱性とその対策に習熟するための各種トレーニングへ参加しています。

セキュアな生産制御システムの構築

商用 IT システムのみならず生産制御システムにおいてもセキュリティの構築に向け多くの試みがなされています。横河電機は、こうした試みの成果を取り込むと共に、自社のベストプラクティス、テクニカルスタンダード、手順、並びにツールの開発を通して、より安全で確実な IA システムを提供し、ユーザの要件を満たしてきました。その結果として、横河電機の IA システム製品の各コンポーネント(I/O、コントローラー、データサーバー、アプリケーションサービス、ワークステーション、ソフトウェアアプリケーション等)は、適切に統合され、トータルシステムソリューションとしてユーザに提供されています。

システムインテグレーションの支援

セキュリティを念頭において個々の生産制御システムコンポーネントを設計し認証することは、適切で望ましことです。製造と作業員の健康や安全のために現場で配慮すべきことは、システム全体が安全かつ確実に機能するかにあります。そのために、横河電機が重点的に考えていることは、さまざまなシステムハードウェアとソフトウェアコンポーネントを単一システムへいかに統合するかということです。当然ながら、このシステムは、一日 24 時間、週 7 日間連続して稼動する基幹工業プロセスを監視、制御、そして管理を行うためものものです。

横河電機には、30 年に渡り生産制御システムをユーザに納入してきた実績があります。この間、横河電機は、セキュリティソリューションにつながるような、システムを統合するための専門知識を培ってきました。これらの専門知識は、プロジェクトを均質的に遂行するためのグローバルエンジニアリングスタンダードやその他の内部スタンダードに反映され、物理セキュリティとサイバーセキュリティに展開されています。

生産制御システムの特徴のひとつに、そのライフサイクルは他の商用システムよりはるかに長いということが挙げられます。横河電機は、技術更新に伴う潜在的な悪影響を避けるため、システムインテグレーションの視点でシステムアーキテクチャを構築してきました。さらに、IT 業界の頻繁な技術更新に対して、横河電機はシステムインテグレーションスタンダードを策定し、それらを実践することで、この重要な特徴を維持しています。

横河電機のエンジニアは、システムインテグレーションとサイバーセキュリティの両面に関する知識と技術を向上する目的で、包括的なトレーニングを受講しています。このトレーニングには、基礎、応用、実践といったコースがあり、トレーニングの有効性を確かなものにするために定期的な試験が必須となっています。

- 基礎コース– システムアーキテクチャ全般
- 応用コース– Windows ドメインとアカウント管理、オペレーティングシステムパッチ管理、ファイアウオール、レイヤー2/レイヤー3 スイッチ、リモートアクセス、アンチウイルスソフトウェア、ネットワーク管理及びバックアップリカバリ管理。
- 実践コース– 上記全般に対する実機を用いたトレーニング

横河電機では、類似のトレーニングをユーザに対しても提供しています。これは、横河電機の内部トレーニングコースに基づくもので、ユーザが自社の生産制御システムのセキュリティライフサイクルを維持・管理するのに十分なほど詳細なものです。

設計、実装、検証

横河電機のシステムインテグレーションは、三段階（設計/実装/検証）から構成されており、さらに、世界中のエンジニアリングセンターをベースとしたエンジニアのトレーニングプログラムにより補完されています。また、横河電機のグローバルエンジニアリングスタンダードとセキュリティスタンダードでは、システムインテグレーションのための設計手順を規定しています。このセキュリティスタンダードはセキュリティ技術の実装を規定し、さらに自社システム設計ツールがこれをサポートしています。システムが統合された後、横河電機は特製のツールを用いて堅牢性を確認し、横河セキュリティスタンダードに合致したものであるかを検証しています。

システムハードニングツールと検証

通常、Windows オペレーティングシステムは、家庭や会社のユーザに対して最大限の機能性と使い易さを提供することを目的として設計されています。しかし、潜在的な脆弱性や重要でない機能や使い易さといった特質に対して、工業環境では安全とセキュリティが優先されます。

通常、Windows オペレーティングシステムは、家庭や会社のユーザに対して最大限の機能性と使い易さを提供することを目的に設計されています。しかし、脆弱な機能や重要でない機能、使い易さといった特質に対して、工業環境では安全とセキュリティが優先されます。ユーザが使用するにあたり、脆弱性を最小限に抑えるため、横河電機はシステムハードニングツールを使用し、重要でない機能やセキュリティホールとなり得る潜在的な弱点を除去すると共に、オペレーティングシステム自体の信頼性を強化しています。対象となるオペレーティングシステムには、Windows XP、Windows Vista、Windows 7、Windows Server 2008、及び Windows Server 2008 R2 があります 。

このハードニングツールは、セキュリティポリシ、そしてシステムとアプリケーションの特性を考慮し、二つの異なる手順で実行され、以下を目的としています。

- サードパーティ製デバイスやネットワーク等の内部あるいは外部の攻撃から守るべく、横河電機のシステム製品が動作するオペレーティングシステムを単一のセキュリティモデルで強化すること。
- 横河電機のシステム製品と、最新かつ最適なセキュリティ対策が導入できない従来システムが連携できるようにすること。

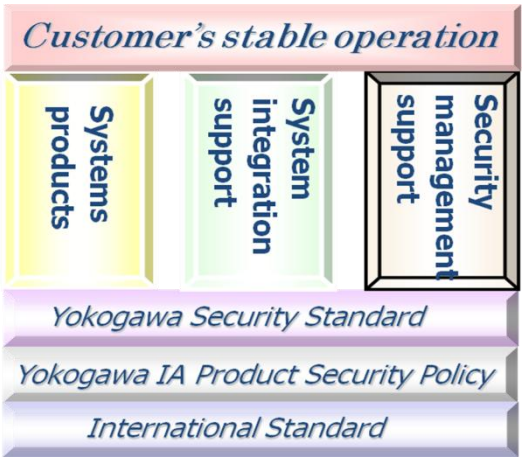
さらに、横河電機は、異なる環境に対して特定のリスクレベルに対応する必要があると判断した場合、横河電機のシステム製品に対して強化手順を追加実施しています。

セキュリティスタンダードを基本として、横河電機のエンジニアは、基本設定（レジストリ、サービスおよびローカルセキュリティポリシ）、ネットワーキング（パーソナルファイアウオール、ファイル共有、NetBIOS、DCOM などの設定）、ユーザ管理、アクセス制御、および USB の制御等すべてを安全に設定するために、自社のシステムハードニングツールを用いて PC やサーバの構成設定を行います。

横河電機は、カスタムプラグインツールを用いてシステムの堅牢性を検証することにより、安全な生産制御システムを世界中のユーザに提供しています。また、横河電機では、こうしたツールを用いることで、既存システムの堅牢性も検証しています。検証プログラムにより、ユーザは、横河電機の定める指標に基づき、自社の生産制御システムのセキュリティレベルを単一かつ包括的な視点で把握することができます。そのために、横河電機では、PARM と呼ばれる指標を開発して、ユーザがシステムのセキュリティレベルを把握できるようにしています。PARM の P はデータ保護(Data Protection)、A は可用性(Availability)、R は回復可能性(Recoverability)、そして、M は管理可能性(Manageability)を示しています。PARM は全ての ISA99 基本要件を横河電機の基準でまとめたものです。

横河電機には、システムベンダとして生産制御システムの堅牢性を検証するために必要となる専門知識、経験、およびツールがあります。加えて、横河電機は、ISA Secure などへの参加を通じて、システム製品の適切な認証を行っています。横河電機はセキュリティポリシを策定することで、システムおよび製品開発のプロセスにセキュリティ対策を導入し、ユーザのセキュリティガイドを作成し、さらには、独立した 内容領域専門家(SME: Subject Matter Expert)を有するコンサルタントのサポートを得て、ユーザのセキュリティ活動を継続的にサポートしています。

セキュリティマネージメントの支援



先に述べたように、絶え間ないセキュリティの脅威、現在の IA 技術やアプリケーションの特性により、セキュリティにはライフサイクルアプローチが求められています。横河電機は、自社が提供し、設置したシステムをユーザが確実に運用できるよう、人的かつ技術的な対応する能力を備えています。

しかし、避けがたい脆弱性やシステムの運用開始に伴うセキュリティの脅威を予測し、特定し、かつ緩和するためには、常に警戒している必要があります。残念なことに、ユーザ側には、全社的にセキュリティに対応する適切なリソースがありながらも、IT 部門がプロセス制御、プロセス保護、SCADA およびプラントレベルでのシステムやネットワークに対する運用環境やセキュリティに関して十分な理解があるとは言い難いのが現状です。その点で、生産制御システムベンダが提供しているセキュリティ管理サービス、例えば、VigilantPlant サービスとして提供しているサービスは、ユーザに大きな価値を提供することができます。横河電機のセキュリティ専門家は、最新のセキュリティ技術やツールに関する深い専門知識と経験を組み合わせるだけでなく、業界をとりまく環境を完全に理解し、さらには、横河電機の提供するシステム製品、プロセス制御ネットワーク、ソフトウェアアプリケーションに関する知識を踏まえています。横河電機の VigilantPlant サービスは、DMAIC コンセプトに基づきライフサイクルを通した継続的な改善をユーザに提供することができるものです。

アセスメントとコンサルティング

従来の生産制御システムは、セキュリティの脅威に対して特に脆弱ですが、最近に導入されたシステムでも、すぐに新たな脅威にさらされてしまいます。横河電機の VigilantPlant サービスは、セキュリティ対策のアセスメントとコンサルティングを通じて導入済のシステムに対し、ユーザが必要とする対策を講じるのをサポートするサービスです。このサービスにより、ユーザは導入済システムを診断でき、リスクを管理しビジネスの継続性を担保すると共に、システムの特定の弱点や潜在的な脆弱性を検出し特定することができます。

横河電機がこの重要なサービスで提供するものは、詳細な評価報告書と適切な対応策を示した勧告書です。また、対応策の実施サービスは、勧告書に準じて随時フォローアップされます。

対応策の実施

多くのユーザは、生産業務に対してだけでなく、作業員の健康、安全、あるいは環境に対して悪影響を及ぼすような、自社のシステムやネットワークに対する脅威に対応するためのリソースを欠いています。こうしたことへのサポートとして、横河電機では、導入済の生産制御システムに対する脅威や脆弱性に対処するための適切な対策を提供することを目的に、以下のアセスメントとコンサルティングサービスを含む VigilantPlant サービスを提供しています。

サービス内容:

- ウィルスチェック
- USB ポートロック
- セキュリティパッチ更新
- ソフトウェアのバックアップとリカバリ
- 許可されていないソフトウェアの使用制限

セキュリティの脅威が常に発生し、プラットフォーム技術が進化し続ける状況において、これらのサービスを導入することにより、運用されるライフサイクル全般にわたり、システムの堅牢性と安全性が担保されます。

メンテナンスとサポート

実施している全ての対策は、費用対効果の高い方法で維持できることが重要です。この点はライフサイクルの重要な部分をなし、生産制御システムを継続的に安全なものにするセキュリティマネージメントシステムの一部としても必須です。横河電機は、VigilantPlant サービスを通じ、メンテナンスとサポートを提供することで、展開中の対策を常に実行し、通常の運用では捕捉できない脆弱性に対しては対策の更新を行っています。横河電機は、ユーザが自社のセキュリティライフサイクルを実施できるよう、ユーザトレーニングを提供すると共に、追加のアセスメントとコンサルティングにより適宜そのフォローアップを実施しています。

横河セキュリティラボラトリ

シンガポール、東京（日本）、バンガロール（インド）、およびヒューストン（米国、テキサス）にある横河セキュリティラボラトリでは、自社のセキュリティ活動全般に対して重要な役割を果たしています。これらのラボラトリでは、横河電機のシステムエンジニアおよびセキュリティ専門家が協力して、最新のセキュリティ技術と自社のシステムとを融合させる研究を行っています。この研究成果により、常に発生し増加し続ける巧妙なセキュリティの脅威からユーザを保護することが可能となります。

セキュリティラボラトリでは、最新のセキュリティ技術と実際の生産制御システムにおけるセキュリティの実施状況を研究し、さまざまな工業分野、アプリケーションおよびシステム構成に最適な対策とソリューションを開発しています。また、これらのラボラトリでは、セキュリティサービスやその他のサービスを提供している横河電機のエンジニアとセキュリティ専門家向けに新しい手順やツールを開発・検証し、その展開を行っています。

横河電機のセキュリティラボラトリのもう一つの役割は、各種文書および作業手順を含む横河電機のセキュリティスタンダードを継続的に更新することです。

ARC Advisory Group の提言

セキュリティの専門家の見解は、十分な時間とリソースが与えられれば、セキュリティが強化され隔離された工業用生産制御システムでさえ、ハッカー、不注意な作業員、または不満を抱く従業員によって侵入されてしまうという点で一致しています。しかし、明らかに、システムの基本機能を損なうことなく、セキュリティの脅威を無理のない限りできるだけ低く（ALARP）下げる方法があります。

ARC は、横河電機が提供しているライフサイクルアプローチ（業界のセキュリティスタンダードとベストプラクティスに基づく）、セキュリティスタンダード、エンジニアリングスタンダードにより、セキュアな制御システムと安定運用を実現できると考えています。

ARC は、横河電機が提供しているライフサイクルアプローチ（業界のセキュリティスタンダードとベストプラクティスに基づく）、セキュリティスタンダード、そしてエンジニアリングスタンダードにより、セキュアな生産制御システムと安定運用が実現できると考えています。さらに、横河電機は、十分にトレーニングされた全世界に展開するサービス組織を通じて、現段階で最新のセキュリティ対策を提供しています。また、プラットフォームが進化することで発生する新たな脅威に対し、ユーザが対処できるようサポートしています。

ユーザは、いかにベンダが提供するソリューションがしっかりとしていたとしても、すべてをそれに依存してはいけないことを認識すべきです。セキュリティリスクを受け入れ可能なレベルにまで下げるには、ユーザは全社的にセキュリティ文化を育み、ANSI/ISA S99 や NIST SP 800 あるいはその他の業界スタンダードやベストプラクティスに基づき、自社のセキュリティ活動を開発・強化する必要があります。


YOKOGAWA
Security Competence Laboratory

アナリスト: バリー・ヤング、ポール・ミラー

エディタ: ディック・ヒル

略語: 工業用語の略語に関しては、以下の弊社の Web サイトを参照してください。
www.arcweb.com/Research/IndustryTerms/

API	Application Program Interface
B2B	Business-to-Business
BPM	Business Process Management
CAGR	Compound Annual Growth Rate
CAS	Collaborative Automation System
CMM	Collaborative Management Model
CPG	Consumer Packaged Goods
CPM	Collaborative Production Management
CRM	Customer Relationship Management
DCS	Distributed Control System
EAM	Enterprise Asset Management
ERP	Enterprise Resource Planning
HMI	Human Machine Interface
IOp	Interoperability
IT	Information Technology
MIS	Management Information System
OpX	Operational Excellence
PAS	Process Automation System
PLC	Programmable Logic Controller
PLM	Product Lifecycle Management
RFID	Radio Frequency Identification
ROA	Return on Assets
RPM	Real-time Performance Management
SCM	Supply Chain Management
WMS	Warehouse Management System

1986 年に設立された ARC Advisory Group は、産業界向けに調査研究・助言を行うリーダ企業で、そのカバーするテクノロジーの範囲は、ビジネスシステムから製品やアセットのライフサイクル管理、サプライチェーン管理、運用管理およびオートメーションシステムにまで及び、世界のビジネスおよび IT の経営幹部にとっては頼りになる企業です。今日、複雑な問題に直面している企業にとって、弊社のアナリストは業界の知識と直接の体験を踏まえてユーザが最善の答えを得られるよう支援いたします。

弊社のアドバイザリーサービスをご利用いただくことで、ARC の現在展開中の広汎な調査研究に加え弊社スタッフの経験をご活用いただけます。ARC の提供するアドバイザリーサービスは、特に組織の戦略と方針を策定する立場にある経営幹部の方々を対象にしたものです。お問い合わせは、電話、ファックスあるいは郵便にて下記宛てにご連絡ください。

ARC ジャパンオフィス、埼玉県所沢市くすのき台3－7－8

℡ 04－2991－1685、Fax 04－2991－1686、E-mail: sabe@arcweb.com

ウェブサイト:www.arcweb.com/Japan/

ARC Advisory Group, Three Allied Drive, Dedham, MA 02026 USA

Tel: 781-471-1000, Fax: 781-471-1100, Email: info@arcweb.com

Visit our web pages at www.arcweb.com


ARC
arcweb.com