富士電機のサイバーセキュリティの取組み

Strengthening Cybersecurity of Fuji Electric

梅﨑　一也 UMEZAKI, Kazuya　　吉田　聡 YOSHIDA, Satoshi

富士電機は、IoT やデジタル技術を活用した製品・サービスの提供を通じて顧客の DX 推進に資することを目指しているが、そのためには製品・サービスがセキュアであることが前提条件として重要である。そこで、ベンダとしてのセキュリティ強化のために、セキュリティポリシーの見直し、体制整備による新たな攻撃への防御および検知対応能力の向上、ならびに開発プロセスや工場の製造環境のセキュリティ対策を行っている。さらに、製品・サービス自体のセキュリティを強化するための技術開発を進めている。

Fuji Electric aims to contribute to the promotion of customer's DX by offering products and services that use IoT and digital technologies. To achieve this goal, it is the foremost importance to ensure that our products and services are secure. To strengthen our security as a vendor, we have revised our security policy and reinforced the defense system to improve our ability to defend against and detect new attacks, as well as took security measures for our development processes and factory manufacturing systems. In addition, we are developing technologies that enhance the security of our products and services themselves.

1　まえがき

2010 年頃から、IoT（Internet of Things）や AI（Artificial Intelligence）、クラウドサービスなどのデジタル技術の活用が拡大し、お客さまや社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立する動きが強まっている[(1)]。2019 年末に始まったコロナ禍は、外出制限によりリモートワークが推奨される“ニューノーマル”の環境下で、デジタル技術の活用を加速させている[(2)]。

一方、デジタル技術の急速な利用拡大は、サイバー攻撃の急増などによるサイバーセキュリティリスクの増大も引き起こしている。

このため、DX（デジタルトランスフォーメーション：Digital Transformation）を推進していくためには、サイバーセキュリティの対策強化も併せて実施することが必須である。

本稿では、デジタル化の進展に伴うサイバーセキュリティリスクおよび国内外での対策の動向、およびそれらを踏まえた富士電機のサイバーセキュリティの取組みについて述べる。

2　サイバーセキュリティの動向

2.1　サイバー攻撃の動向[(3)(4)]

近年は、大学や企業などの組織を狙ったランサムウェアの攻撃が増加している。例えば、メールに不正なファイルを添付したり、改ざんした Web サイトに誘導したり、OS の脆弱（ぜいじゃく）性などを突いたりするなどの手法を用いてウイルスに感染させる。このウイルスを使って PC やサーバのファイルを暗号化して使用不能にし、復旧と引換えに、あるいは情報を公開すると脅迫して金銭を要求する攻撃である。工場の生産システムや石油パイプラインが停止するなど大きな被害も報告されている。

また、情報漏えいにおいては、広がるサプライチェーンを悪用し、セキュリティ対策が甘い組織（委託先、国外子会社など）が攻撃の足掛かりとして狙われるケースが増えている。このため、自組織のセキュリティ対策だけでなく、調達先や業務委託先、関連会社も含めたサプライチェーン全体でのセキュリティ対策が必要となる。

コロナ禍でリモートワークが増加した結果、VPN（Virtual Private Network）やクラウド、Web 会議などの利用が急速に拡大し、それを狙った攻撃も増加している。

2.2　セキュリティ対策の動向

このようなサイバー攻撃の状況を踏まえて、国や標準化団体などによってサイバーセキュリティ対策に関する規制や標準、ガイドラインなどの策定がなされている。

サイバーセキュリティ対策は、組織レベルの戦略的なリスクマネジメントと、情報システムのセキュリティ脅威に対するシステムレベルのリスクマネジメントとに分けられる（**図 1**）。

組織レベルでは、従来の ISMS（Information Security Management System：情報セキュリティマネジメントシステム）よりもサイバー攻撃対策を重視した新しいフレームワークとして、NIST（米国国立標準技術研究所）の CSF（Cyber Security Framework：サイバーセキュリティフレームワーク）の利用が進んでいる。

CSF は、組織が実施すべきセキュリティ対策を五つの機能（特定、防御、検知、対応、復旧）に分けて参考情報とともに列挙している。守るべき情報資産とそのリスクを

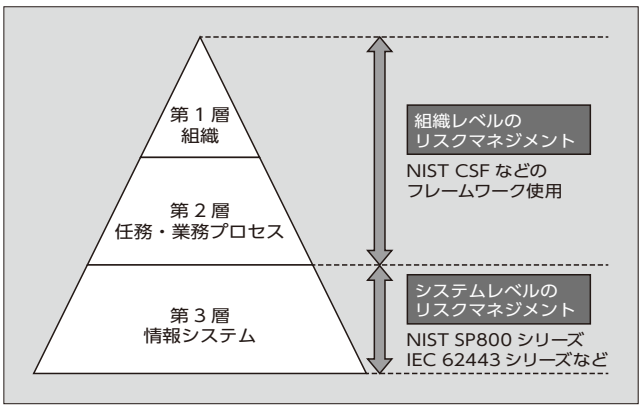

図 1　サイバーセキュリティ対策としてのリスクマネジメントアプローチ[5]

特定し、ビジネス上の要求やリスク許容度などを踏まえてセキュリティ対策（防御、検知、対応、復旧）目標を設定し、計画的に改善していくことで、組織が適切にセキュリティリスクを管理できるようにする狙いがある。CSF の特徴として次が挙げられる[6]。

⑴　防御重視から検知・対応・復旧重視へ

サイバー攻撃の手法が高度化しており、完全に防御することは不可能という前提で、いかに早く検知して被害を最小化して復旧するかを重視している。

⑵　サプライチェーンリスクマネジメント

サプライチェーン上での低品質な製造・開発により、潜在的に有害な機能を含む可能性がある製品・サービスを識別し、評価し、抑制することを目的とする。

システムレベルでは、情報システム向けに NIST の SP800 シリーズの整備が進められている。サプライチェーンにおける情報漏えいへの対策としては、NIST SP800−171（連邦政府組織と取引する企業が取るべき対策基準を示すガイドライン）が発行された[7]。制御システムでは、IEC 62443 などの標準規格の適用が進むとみられている。

自動車や鉄道、船舶などの交通系、電力や石油化学など、ドメインごとにガイドライン作成の動きがある。IoT 機器に対しては、各国で具体的なセキュリティ対策を要求する規制やガイドラインが策定されている。さらに、これらの規制や標準、ガイドラインなどへの準拠を法規制で要求したり、認証の仕組みを構築したりする動きがある。また、製品やシステム自体のセキュリティだけでなく、ベンダの開発プロセスや製造プロセスに対する要求もある。

ベンダは、これらの規制や標準、ガイドラインに準拠し、組織としてのセキュリティ対策に加えて、開発や製造環境のセキュリティ確保、製品・サービスの適切なセキュリティ対策を求められるようになってきている。

3　富士電機の取組み

2章で述べたようにベンダへのセキュリティ対応要求が強まっている状況を踏まえ、富士電機では、従来の社内の情報（IT：Infomation Technology）システムに加えて、

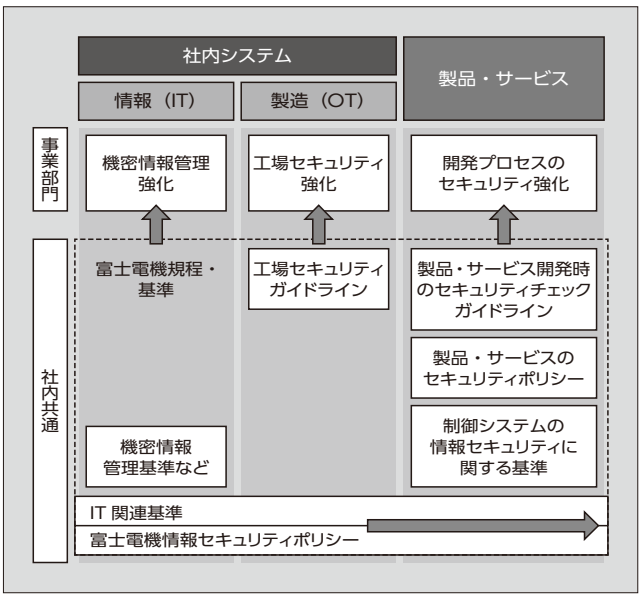

図 2　富士電機のセキュリティ強化の取組み

工場などの製造（OT：Operational Technology）システム、製品・サービスのセキュリティを強化する取組みを進めている（**図 2**）。製品・サービスについては、開発プロセスのセキュリティ強化に加えて、製品自体のセキュリティ強化のための技術開発も進めている。

3.1　組織の取組み

⑴　情報セキュリティポリシーの強化

富士電機は、サイバー攻撃の高度化、巧妙化に伴い、2019 年に新 IT 中期計画を策定し、サイバーセキュリティの強化を重点施策の一つとした。

従来の防御を主体としたセキュリティ対策では、最新の攻撃を完全に防ぐことは難しいことから、侵入されることを前提とし、新たな攻撃方法への防御を強化しつつ、侵入後の早期検知、対応の即応化、事業復旧の強化を図ることに方針を改めることとした。

そのために、情報セキュリティポリシーおよび関連する規程基準を NIST CSF と NIST SP800−171 の要求事項に準拠した見直しを行い、次のような強化を行っている。

(a)　特定・防御の強化

①機密情報の管理方法の見直しとその管理の徹底

②クラウドサービスや情報システムのセキュリティ評価、脆弱性対策、運用管理、監視の徹底

③システムやクライアントデバイスの防御、監視機能を強化し、ゼロトラストセキュリティへの対応

(b)　検知

①ネットワーク、システム、サーバ、デバイスにおける未知の攻撃や異常挙動の監視機能強化

②SOC（Security Operation Center）による監視オペレーション強化

(c)　対応

①緊急事態発生時の初期対応の即応化のため、経営層を含めた危機管理体制のサイバーインシデント対応

整備

②Fe−CSIRT（富士電機サイバーセキュリティ対応チーム）、および情報セキュリティマネジメント体制によるサイバーインシデント対応の強化

③初動対応に備えたフォレンジック（サイバー攻撃などのセキュリティ事件・事故発生時に原因究明などのためコンピュータに残された証拠を調査すること）などの技術支援や法務、広報などの対応支援を委託するため、外部専門事業者との体制整備

④サイバーリスク、脅威情報の収集の自動化、システム管理者、利用者への注意喚起の徹底

(d) 復旧・事業継続

①IT−事業継続マネジメント（BCM：Business Continuity Management）を、従来の自然災害想定のものに加え、サイバー攻撃を想定した復旧計画、手順の整備

②復旧計画の実効性を高めるための対応訓練の実施

(2) 製造セキュリティの強化

富士電機の工場では、従来、インターネットや社内の情報ネットワークからは隔離した製造系ネットワークを使って製造装置を運用していた。そのため、サイバーセキュリティリスクは小さく、例えば、USB メモリや保守用 PC を介した間接的マルウェア感染の可能性の低減など、情報システムとの接点となるデータの授受の機会を注意することで保護ができていた。

しかし、近年、工場の IoT 化、製造のデジタル化が進み、製造系ネットワークと情報系ネットワーク間の通信の必要性が増したことで、情報システムと同様のサイバー攻撃を受ける可能性が高まり、その対策が必要になっている。ただし、従来、サイバーセキュリティリスクが低かった製造現場では、サイバーセキュリティの認識は高くなく、セキュリティ技術者も不足していた。

そこで、セキュリティと実施するべき対策の必要性の理解を図るとともに、IT 部門が製造系の対策に関与する体制を敷いた。

ソフトウェアの修正プログラムやマルウェア対策ソフトウェアを適用するために、稼働中の製造装置をわざわざ停止することは難しく、稼働したまま適用すると動作に異常をきたす恐れがある。そのため、技術的な対策は情報システムとは異なる方法で行う必要がある。ただし、可能な限り情報システムと同様の対策を講じつつ、用途や通信も限られる制御装置では、サイバーセキュリティリスクとなるソフトウェアの動作や通信を最小化するなどの制限を行い、サイバー攻撃のリスクを低減する防御対策を行っている。

また、技術的な対策以外では、基本的に情報システムと同様の対策が多い。セキュリティ体制などの組織的対策、工場への入退場や工場内のセキュリティ区画などの物理的対策やその教育・周知は、従来の情報セキュリティ活動の枠組みを徹底して対応する。また、サイバー攻撃の検知や対応は、情報システムで行っている対策を拡大し、水平展開することで強化している。

復旧に関しては、工場の BCM の枠組みに、IT−BCM のサイバー攻撃想定を組み込むようにしている。

(3) 製品・サービスのセキュリティ対策

IoT の導入などによるセキュリティリスク増大に対応するため、富士電機の IoT の製品・サービスを対象にしたセキュリティポリシーを 2018 年 4 月に社内基準として発行し、セキュリティ対策の強化を進めてきた[8]。2021 年 6 月には CSF や IoT 関連ガイドラインなどで強化されたセキュリティ要求を反映した改定版を発行した。

製品・サービスのセキュリティを確保するためには、製品ライフサイクル（企画段階から開発、製造、試験、運用、破棄）の各段階でセキュリティ対策を確実に実施することが必要である。そこで、製品・サービスの各開発・ステップで実施すべきセキュリティ対策や、DR（デザインレビュー）で確認すべきセキュリティのレビュー項目を定

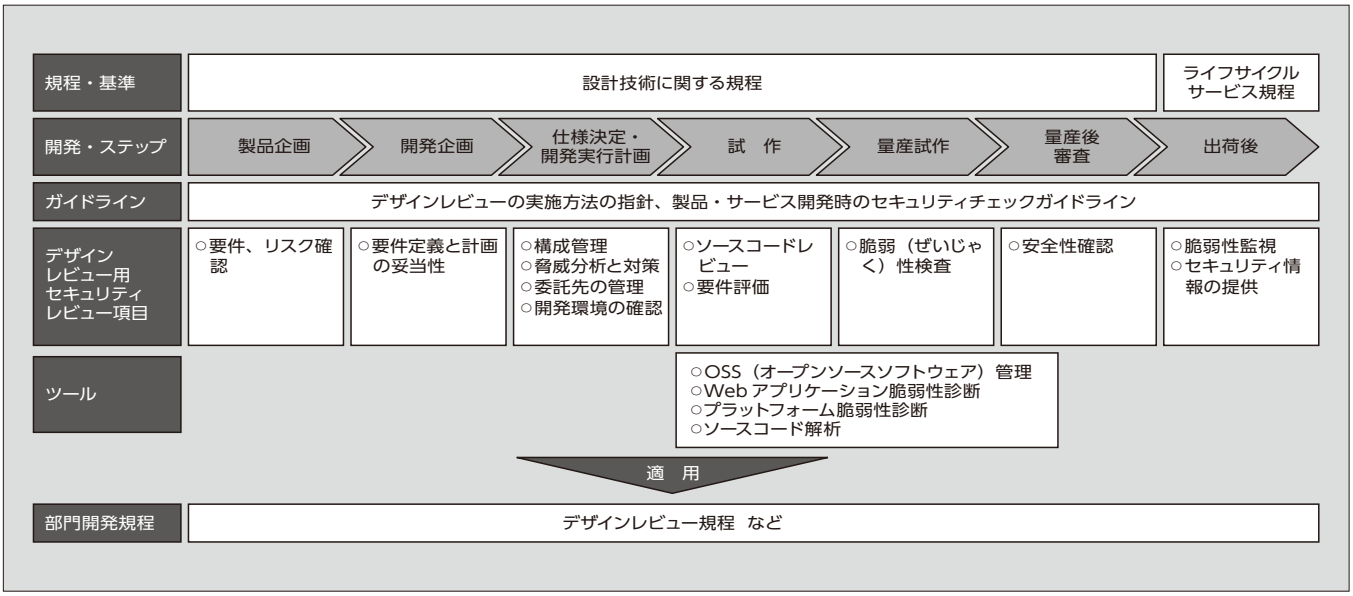

図 3　製品・サービスのデザインレビューにおけるセキュリティ対策

めたガイドラインを社内基準として策定した（**図3**）。

この社内基準では、製品企画段階で調達要件ならびに順守すべき法令やリスクなどを確認し、開発企画段階でそれらを踏まえた要件定義および開発計画の妥当性を確認することによって、対策すべきセキュリティ要件を漏れなく適切に特定することを求めている。また、仕様決定・開発実行計画段階以降では、セキュリティ要件を充足するための取組みとして、脅威分析を踏まえたセキュリティ対策の具体化や、設計・実装における脆弱性の作り込み防止、開発環境のセキュリティ確保などを求めている。サプライチェーンセキュリティ対策として、委託先の管理のほか、製品出荷後における脆弱性監視やセキュリティ情報提供のための体制やプロセスの整備を求めている。

これを各事業部門や工場のDRプロセスに反映することによって、全ての富士電機製品・サービスのセキュリティ対策の強化を図っている。

3.2　セキュリティ技術開発

製品・サービスのセキュリティを向上させるための技術開発の一部を**表1**に示す。防御のための技術に加えて、サイバー攻撃による侵入などを前提とした検知や対応、復旧のための技術開発を進めている。さらに、製品・サービス開発の各段階で必要なセキュリティ対策の技術的な手段の整備を進めている。

⑴　セキュア実行環境

インターネットなどの外部環境に接続される機器には、不正アクセスによる遠隔操作やウイルスによる情報漏えいなどのセキュリティ事故の危険がある。

そこで、セキュアブート（起動時ソフトウェア検証）や実行時データ保護を実現する技術を開発した。セキュリティ機能を内蔵したマイコンを活用しつつ、製品仕様上の制約に対応できるようにメモリ使用量の削減や処理時間の短縮を実現している[9]。

⑵　利用者認証・認可

Webサーバへの不正ログインによる情報漏えいなどの被害が増加している。

そこで、既存Webサーバ（ID・パスワードによるユーザ認証）の多要素認証対応を可能とする技術開発を進めている。既存のWebサイトに大きな変更を加えずにクライアント証明書などによる認証を追加できるようになる。

⑶　ログ監視

不正アクセスを行って情報を窃取（せっしゅ）するサイバー攻撃は高度化しており、発見までに時間がかかることが多いとされている。このため、サイバー攻撃の被害や兆候を早期に検知するための取組みが重要である。そこで、IoTシステムなどの各種ログを集約管理して効率的に監視・分析する仕組みを開発している。

この仕組みを用いて、アクセスログや操作ログなどを集約・分析することによって、認証失敗などサイバー攻撃の可能性がある事象を早期に検知できるようになる。

⑷　セキュアコーディング

製品のソフトウェアに脆弱性があると、サイバー攻撃により被害を受ける可能性が高まる。このため、ソフトウェア開発時に脆弱性を作り込まないようにすることが必要である。

そこで、CERT C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。C言語によるファームウェア開発を対象として適用していくとともに、その他のプログラミング言語でも同様の取組みを進めていく。

⑸　Webサーバ脆弱性検証

Webサーバの脆弱性を突いた不正アクセスによる情報漏えいなどの被害が増加している。

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を行うための標準的なツールの評価、選定を実施している。

表1　製品セキュリティ技術開発

技　術	説　明	防御	検知	対応	復旧
セキュア実行環境	セキュアブート、実行時データ保護	○	—	—	—
利用者認証・認可	Webサーバなどでの多要素認証	○	—	—	—
ログ監視	機器やシステムへのサイバー攻撃の兆候や被害の検知、分析	—	○	○	—
セキュアコーディング	ソフトウェア開発時の脆弱（ぜいじゃく）性作り込み防止	○	—	—	—
Webサーバ脆弱性検証	Webアプリケーションやプラットフォームの脆弱性検出	—	○	○	—
OSS（オープンソースソフトウェア）管理	ソフトウェアが依存するOSSの脆弱性やライセンス問題の検出	—	○	○	—
インシデント管理	インシデントの検知、影響分析や復旧の省力化や自動化	—	○	○	○

4　あとがき

富士電機のサイバーセキュリティの取組みについて述べた。近年、サイバー攻撃は高度化、巧妙化しており、デジタル化の利用拡大によってセキュリティ脅威も増加している。富士電機では情報セキュリティポリシーを改定し、情報だけでなく工場のセキュリティ対策強化を図っている。さらに、よりセキュアな製品・サービスの提供のために、製品・サービスを対象としたセキュリティポリシーを策定し、開発段階からセキュリティ対策を行うための体制、プロセスを整備するとともに、セキュリティ技術開発に取り組んでいる。

サイバー攻撃は日々進化しているため、セキュリティ対策は継続的な取組みが不可欠である。今後も引き続き、富士電機およびその製品・サービスのセキュリティ向上の取組みを通じて、お客さまのDX推進に貢献していく所存である。

参考文献

⑴ デジタルトランスフォーメーションを推進するためのガイドライン（DX推進ガイドライン）Ver.1.0. 経済産業省. 2018−12. https://www.meti.go.jp/press/2018/12/20181212004/20181212004−1.pdf,（参照 2021−07−28）.

⑵ 次期サイバーセキュリティ戦略（案）. 内閣サイバーセキュリティセンター. 2021−07. https://www.nisc.go.jp/active/kihon/pdf/shiryou01−2.pdf,（参照 2021−07−28）.

⑶ 情報セキュリティ10大脅威 2021. 情報処理推進機構. 2021−03. https://www.ipa.go.jp/security/vuln/10threats2021.html,（参照 2021−07−28）.

⑷ 最近のサイバー攻撃の状況を踏まえた経営者への注意喚起. 経済産業省. 2020−12. https://www.meti.go.jp/press/2020/12/20201218008/20201218008−2.pdf,（参照 2021−07−28）.

⑸ Risk Management Framework for Information Systems and Organizations：A System Life Cycle Approach for Security and Privacy, Revision 2, NIST, SP800−37, 2018−12. https://www.nist.gov/publications/risk−management−framework−information−systems−and−organizations−system−life−cycle,（参照 2021−07−28）.

⑹ Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NIST, 2018−04. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf,（参照 2021−07−28）.

⑺ Protecting Controlled Unclassified Information in Nonfederal Systems and Organization, Revision 2, NIST, SP800−171, 2020−02. https://csrc.nist.gov/publications/detail/sp/800−171/rev−2/final,（参照 2021−07−28）.

⑻ 梅﨑一也. IoTシステムのセキュリティ. 富士電機技報. 2018, vol.91, no.3, p.175−178.

⑼ 高務健二ほか. セキュリティ技術の事業への貢献における課題解決の取り組み. 情報処理学会. 第83回全国大会. 2021−03. https://www.ipsj.or.jp/event/taikai/83/ipsj_web2021/data/pdf/4D−03.html,（参照 2021−07−28）.

梅﨑　一也

IoTシステムなどに関するセキュリティ技術開発に従事。現在、富士電機株式会社技術開発本部デジタルイノベーション研究所IoTソリューションセンター主査。

吉田　　聡

社内情報システムの企画、構築に従事。現在、富士電機株式会社経営企画本部IT戦略室ITコンプライアンス部。

富士電機

Innovating Energy Technology