標準から学ぶ ICS セキュリティ #5

セキュアな製品開発プロセス

2023 年 9 月 14 日

一般社団法人 JPCERT コーディネーションセンター
制御システムセキュリティ対策グループ

1. はじめに

「セキュアな製品開発ライフサイクル」と題された IEC 62443-4-1 では、製品を安全に稼働させるために必要なセキュリティ対策機能が装備され、かつ脆弱性が少ない、セキュアな製品を開発するためのプロセスが論じられています。ここで言う製品には、ICS の中で使われる、コンポーネントからサブシステム、さらにはシステムまでが含まれます。多くの製品の開発は、いわゆる製品ベンダーによって行われますが、システムインテグレーターやアセットオーナーも、一部のソフトウェアや IoT 機器を開発するケースがあり、そうした場合にはセキュアな製品開発サイクルを整備しておくべきです。また、アセットオーナーがセキュアな ICS を調達する際には、調達品あるいは調達システムを構成する製品が適切なプロセスを経て開発されていることを確認しておくことが大切です。セキュアな製品開発プロセスを理解し、それを開発や調達に活用することが、製品ベンダーだけでなく、システムインテグレーターやアセットオーナーにとっても重要なのです。

2. ICS 関連製品のサイバー攻撃耐性

21 世紀に入った頃から、ICS 関連製品が設置されるネットワーク環境が大きく変化し始めます。それより前は、他のシステムから切り離された ICS ベンダー独自のネットワークの中に設置されることが多く、サイバー攻撃は理論的な可能性として考えることはできても、実際に実行するにはあまりに高い壁がありました。いわば、環境によってサイバー攻撃から ICS が守られていたわけです。ところが、その後、イーサーネットをはじめとする汎用のネットワークに移行するとともに、MES （Manufacturing Execution System）や ERP （Enterprise Resource Planning）などの IT システムとの接続も欠かせないものとなりました。それによって、ICS 関連製品にもサイバー攻撃への耐性が求められることになりました。

ICS 関連製品の提供事業者の多くは、重要インフラに関連したシステムの中で利用される製品を製造しているなどの背景から、品質を重視する社風をもち、高品質の製品を開発する手法を工夫し社内体制を整備することに努めてきました。しかしながら、2010 年前後に急に登場した「サイバー攻撃に対する耐性」という提供製品に対する新たな要求には大きな戸惑いがありました。IEC 62443-4-1 の策定は、そうした戸惑いに対する回答を提示する試みとして始まったとも言えましょう。

3. 製品開発における品質とセキュリティ

コンピューターの歴史を振り返ると、製品開発の中でソフトウェアが占める比重が高まるとともに、ソフトウェアの複雑さが急激に高まるにつれ、高い品質を維持しつつ短期間で開発するための技術が求められるようになりました。その中で誕生したのがソフトウェア工学です。初期のソフトウェア工学では、ソフトウェアを仕様から自動生成することや、仕様に適合したソフトウェアを作り出すこと、あるいは適合していることを効果的な試験により確認することが研究や企業努力の中心になっていました。その後、セキュリティ問題が大きく浮上し、ソフトウェア開発の中で作り込まれる脆弱性を減らし、開発の可能な限り早い段階で除去することが強く求められるようになりました。しかしながら、出荷される製品のセキュアさを期待される水準に近づけようとしても、古典的な品質の追求だけでは限定的な効果しかありませんでした。製品の品質を高めるための技術と製品をセキュア化するための技術の関係のイメージを図 1 に示しました。このような認識に立って、従来とは異なったセキュアな製品を開発するためのさまざまな新しい技法が提案され、それらが「セキュアな開発プロセス」などと呼ばれるようになりました。その後、ソフトウェア工学でも、サイバー攻撃への耐性など明確に文書化しがたいものを含む、さまざまな顧客ニーズへの適合を「広義の品質」と定義し直すことによって、セキュアな開発手法も含む方向に、スコープが拡大されています。

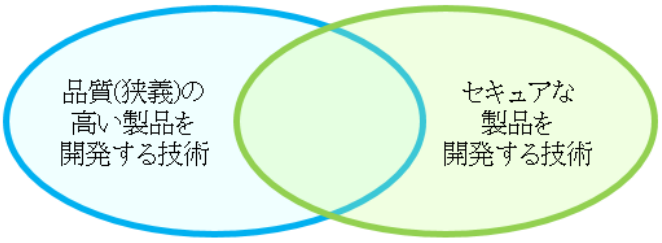

図 1. 品質の高い製品の開発技術と
セキュアな製品の開発技術との関係のイメージ

IEC 62443-4-1 では、これまでに提案され評価が定まっている「セキュアな開発プロセス」の中から、ICS を構成する製品の開発おいて実施すべき項目を選び出し、製品の開発サイクルという時間軸に沿ってまとめています。

4. 製品開発ライフサイクル

IEC 62443-4-1 では、製品開発ライフサイクルを 8 つの段階から構成されるものとしてモデル化しています。その 8 つの段階を相互関係が読み取り易いように JPCERT/CC で作図したものを図 2 に示します。

図 2.　セキュアな製品開発ライフサイクル
（作図： JPCERT/CC）

「セキュリティ管理（SM）」の段階は、開発着手前に個々の製品開発プロジェクトとは独立して、組織として実施しておくべき活動です。これ以外の 7 つの段階は、個々の製品の開発プロジェクトのライフサイクルに沿って実施される、1） 要求定義（SR）、2） 設計（SD）、3） 実現（SI）、4） 試験（SVV）、5） 不具合管理（DM）、6） 不具合改修（SUM）、7） 利用者支援（SG）です。なお、後者の 7 段階のうち、要求定義から試験までの 4 段階は、ウォーターフォール型開発モデルにおいて逐次的に行われるものであり、セキュリティ上の不具合の管理と改修、利用者支援の 3 段階は、前述の 4 段階とは別の時間軸で行われる活動と理解されます。いずれにせよ、これら 8 つの段階のそれぞれについてセキュアな製品開発に必要な数項目から 10 項目前後の要件を定めています。個々の要件については、付録の一覧表に概要をまとめていますので、必要に応じてご参照ください。

セキュリティ管理（SM）に関するものとしてカテゴライズされている要件としては、セキュアな製品開発プロセスの全体に関わる基本ルールや責任体制が定められていて、開発要員のセキュリティスキル、開発が行われる環境と開発成果物のセキュリティの担保などが掲げられています。セキュアな製品開発がルールどおりに実施されたことを検証できるような文書（証跡）の作成も求められています。また、セキュリティに関連する問題を一元的に管理し、問題が放置されたまま残っている場合には、製品が出荷されることがないような業務フローを作り込んでおく必要もあります。さらに、製品に組み込まれるコンポーネントの一部を、組織外から導入する、あるいは、外注して開発させる場合について、例えば自社以上のセキュア開発プロセスを外注先が持っていることを確認することを定めるなど、外注先企業が製品のセキュリティが担保されるような規定をあらかじめ定めておくことも求めています。これらの要件は、個々の製品開発プロジェクトに先立つ、開発組織としての準備に関するものです。

次に、個々の製品ごとに実施すべき事項について、その開発タイムラインに沿って順次述べます。

まず要求定義（SR）の段階では、製品が利用される場面の「セキュリティ文脈」と「セキュリティ脅威モデル」を文書化した上で、セキュリティ要件を文書化し、それをレビューすることを求めています。「セキュリティ文脈」には、製品が稼働する物理的およびネットワーク的な環境について想定されるセキュリティ状況や、製品にセキュリティ侵害が起きた場合に環境に及ぼす影響についての情報などが含まれます。「セキュリティ脅威モデル」は、製品を取り巻く情報の流れや、情報の処理と蓄積などの関係、信頼のおける範囲などを整理した上で、仮に悪意を持つ者がいた場合に、製品に対するどのような攻撃がありうるかをモデル化した情報です。

次の設計（SD）の段階では、製品のインタフェースを特定して、それを通じたセキュリティ侵害の可能性を検討すること、脅威モデルに基づいた多層防御を作り込むこと、セキュリティ問題の管理を伴った設計レビュー

を実施すること、セキュアな設計の方法論のベストプラクティスを文書化し適用することを求めています。製品に作り込まれた脆弱性の中でも単純な修正で取り除くことができない根深いものは、攻撃シナリオに関するものを中心とした、設計段階における考慮不足に端を発していることがしばしばです。IEC 62443-4-1 でも、設計段階におけるセキュリティの確保と多層防御の組み込みを強く謳うとともに、攻撃側の進化に対応して開発される最新の設計の方法論を採用して活用することを求めています。一方で、基本的な設計方法論について IEC 62443-4-1 では特定のものを要求または推奨しているわけではありませんが、設計段階で製品に対する攻撃シナリオの洗い出しを効果的に行うための脅威分析モデルとして広く知られているものに「STRIDE モデル」[1] があります。ちなみに、「STRIDE」は、サイバー攻撃の定石とも言える 6 つの基本的手法、なりすまし（Spoofing）と改ざん（Tampering）、否認（Repudiation）、情報開示（Information Disclosure）、サービス拒否（Denial of service）、権限昇格（Elevation of privilege）の頭文字を並べたものであり、こうした攻撃者の観点から製品の設計を見直すことを通じて、レビュー時の見落としを減らし検討の網羅度を高めています。

実現（SI）の段階では、セキュアコーディング標準に基づいた実現を行うとともに、実現に関するセキュリティレビューの実施を求めています。JPCERT/CC からも、C/C++や Java を中心にセキュアコーディングに関する資料やセキュアなソフトウェア開発関連の資料をホームページ上で公開していますので参考にしてください[2]。

さらに、試験（SVV）の段階では、製品に組み込まれたエラー処理やセキュリティ対策が正しく機能することなどを試験することに加えて、機械的にランダムに生成した多様な入力を製品に与えて異常な状態に陥らないことを確認するファジング試験などの脆弱性発見を目的とした試験や、設計や実現に関与していない要員による試験を行うように求めています。

不具合管理（DM）と不具合改修（SUM）の段階は、製品開発が完了して納入先の顧客による利用が始まった以降における、一般には「製品の保守」と呼ばれる活動の中で実施されます。

不具合管理（DM）では、組織内外から報告されるセキュリティ関連の問題を見落としなく受け取ってタイムリーな分析を行い、脆弱性であった場合には、その修正や緩和策の開発と提供、さらには利用者への通知を行うことを求めています。また、こうした不具合管理プロセスは、定期的にレビューして必要な改善が継続的に行われなければなりません。

不具合改修（SUM）の段階は、セキュリティ上の不具合を除去または緩和するための、パッチや改版などの形態によるセキュリティ更新の開発とそれに関連した活動です。この活動では、セキュリティ更新自体と添付文書の品質を確保するとともに、その提供時期を決めるためのポリシーを明らかにすることを要件として求めています。また、製品が依存している OS、ミドルウェアその他のコンポーネントにセキュリティ更新が提供された場合には、それを適用した場合に製品が受ける影響を明らかにする文書を製品利用者に提供しなければなりません。なお、製品が依存しているコンポーネントとしては、OS などのように製品の外部にあるコンポーネントばかりでなく、製品の中に組み込まれたコンポーネントもありえます。こうした依存性を製品の設計段階から一覧にして管理し、依存先のコンポーネントに関する最新のセキュリティ情報を監視するための工夫も期待されます。

さらに、出荷後における製品利用者への支援（SG）の段階では、製品出荷後を見すえて、製品自体として、および製品の設置環境として多層防御の対策を述べた文書、製品の設置時に行う堅牢化やアカウント設定に関する注意事項、製品運用中に利用者が行うべきセキュリティ管理、製品を廃棄する際の注意事項を述べた文書の作成が求められています。また、こうした文書を含む利用者マニュアルに誤りや欠落がないことを確認するレ

ビューも必要とされています。

5. IEC 62443-4-1 に基づく認証制度

事業者の製品開発プロセスが IEC 62443-4-1 の要件を満たしていることを第三者が検証して認定する制度が複数の認証団体により提供されています。例えば、ISA Security Compliance Institute （ISCI）が提供している「SDLA 認証（Security Development Lifecycle Assurance Certification）」[3]がそれです。こうした認証を製品開発事業者は、自社のセキュアな製品開発プロセスに対するいわゆるお墨付きとして利用することができます。アセットオーナーにおいては、事業者の製品開発プロセスが認証済であることを入札要件に含めることにより、一定のセキュリティ品質を持った製品の調達が可能になります。

ISCI では、コンポーネント製品やシステム製品に対するセキュリティ認証として Component Security Assurance（CSA；以前は Embedded Device Security Assurance （EDSA）と呼ばれていました）や System Security Assurance（SSA）も提供していますが、これらの認証においても、当該製品が IEC 62443-4-1 に準拠したセキュアな製品開発プロセスを経て作られたことを要件としています。

一方で、CSA 認証や SSA 認証を取得するための経費が高額で事業的に見合わないためか、これらの認証を受けた製品は種類が非常に限られています。そのために、製品の調達側から見ると、製品認証を調達要件としがたい場合が多く、また、当該製品に脆弱性が見つかってセキュリティ更新が出ると、それを適用した製品が厳密には認証を受けたものとは言えなくなるという問題も潜んでいて、製品認証の実効性が薄らいでいるように思われます。こうした状況から、製品認証に替わるものとして、製品開発事業者のセキュアな製品開発プロセス認証への期待が、製品の提供側と調達側の双方で高まっているように思われます。

6. まとめ

今回は IEC 62443-4-1 が論じるセキュアな製品開発プロセスの概略を紹介しました。これに準拠しようとすると、製品開発事業者は、出荷判定などの責任を含む業務体制や業務フローを大きく見直すことが必要になる可能性があります。それでも、セキュアな製品開発プロセスの整備は、セキュアな製品を生み出すための組織としての基本要件と言えるように思います。こうした意味合いから、セキュアな製品開発プロセスが普及することと、その認証制度の活用が一層進むことにより、ICS セキュリティの一層の強化が実現することを期待したいと思います。

参考文献

[1] OWASP： Threat Modeling Process, https://owasp.org/www-community/Threat_Modeling_Process

[2]JPCERT/CC： セキュアコーディング, https://www.jpcert.or.jp/securecoding/

[3] ISA Secure： Security Development Lifecycle Assurance （SDLA） Certification, https://isasecure.org/certification/iec-62443-sdla-certification

付録

付録 1.　セキュリティ管理（SM： Security Management）に関する要件

SM-1	開発プロセスを適切に文書化する
SM-2	各開発プロセスの責任者を決める
SM-3	開発プロセスが適用される製品を決める
SM-4	要員の専門性を担保するための教育訓練と試験制度を、開発プロセスの中で定め提供する
SM-5	製品開発プロジェクトに適用する IEC 62443-4-1 の範囲を、開発プロセスの中で定める
SM-6	製品に含まれる重要なファイルの完全性を検証する仕組みを、開発プロセスの中で提供する
SM-7	製品の開発と製造と供給の業務のセキュリティを守る対策をとる
SM-8	コード署名用の秘密鍵を守るための対策をとる
SM-9	製品に組み込むために組織外から導入した全コンポーネントについてセキュリティリスクを調べ管理する手順を用意する
SM-10	外注して開発したコンポーネントについて、セキュリティへの影響がある場合には、自社に準じたセキュア開発が外注先で実施されるようにする
SM-11	セキュリティ関連の問題の対処前に製品やパッチを出荷させない仕組みを用意する
SM-12	開発プロセスの各段階が定められた要件を満たして実施されたことを文書で記録し、要件への適合を後から検証できるようにする

付録 2.　要求定義（SR： Specification of Security Requirement）に関する要件

SR-1	製品が使われるセキュリティの文脈を文書化するプロセスがある
SR-2	製品の開発範囲に固有の脅威モデルを全製品に持たせるプロセスがある
SR-3	開発中の製品や機能に対するセキュリティ要件を文書化するプロセスがある
SR-4	コンポーネントまたはシステムの範囲ないし境界に関する情報などをセキュリティ要件に含めるプロセスがある
SR-5	セキュリティ要件をレビューするプロセスがある

付録 3.　設計（SD： Secure by Design）に関する要件

SD-1	製品のインタフェースを特定してセキュリティの観点から特徴づけするセキュア設計の開発し文書化するプロセスがある
SD-2	脅威モデルに基づくリスクベースアプローチを使って多層防御を実現するプロセスがある
SD-3	設計に大きな改版があるたびにセキュリティ関連の問題を見つけ出し特徴づけし追跡する設計レビューを行うプロセスがある
SD-4	セキュアな設計のベストプラクティスを確実に文書化し適用するプロセスがある

付録 4.　実現（SI： Secure Implementation）に関する要件

SI-1	実現に関連したセキュリティ問題に関するレビューのプロセスがある
SI-2	定期的にレビューして更新されるセキュリティコーディング標準が実現プロセスに組み込まれている

付録 5.　試験（SVV： Security Verification and Validation Testing）に関する要件

SVV-1	セキュリティ機能がセキュリティ要件に合致しており、製品がエラーや不正入力を適切に処理することを試験するプロセスがある

SVV-2	脅威モデルで見つかり検証された脅威に対する緩和策の有効性を試験するプロセスがある
SVV-3	製品中のセキュリティ脆弱性に焦点を絞った試験を実行するプロセスがある
SVV-4	製品中のセキュリティ脆弱性を攻撃して見つけ出す試験によってセキュリティに関連する問題を見つけ出すプロセスがある
SVV-5	設計や実現に関わっていない要員による試験プロセスがある

付録 6.　不具合管理（DM： Management of Security-related Issues）に関する要件

DM-1	組織内外からのセキュリティ関連の問題報告を受け取り取り扱うプロセスがある
DM-2	報告されたセキュリティ関連の問題をタイムリーに調査して影響や原因などを見極めるプロセスがある
DM-3	製品中のセキュリティ関連の問題を分析するプロセスがある
DM-4	セキュリティ関連の問題に対して修正などの対処を行い、影響評価の結果に基づいて問題を報告するか否かを判断するプロセスがある
DM-5	セキュリティ関連の問題について製品利用者に通知を行うプロセスがある
DM-6	不具合管理のプロセスを定期的にレビューするプロセスがある

付録 7.　セキュリティ更新（パッチ）管理（SUM： Security Update Management）に関する要件

SUM-1	セキュリティ更新の品質（有効であり副作用による悪影響がないこと）を検証するプロセスがある
SUM-2	セキュリティ更新に関する製品利用者への提供文書に必要な情報が含まれていることを確認するプロセスがある
SUM-3	製品が依存している OS やコンポーネントのセキュリティ更新に関する製品利用者への提供文書に必要な情報が含まれていることを確認するプロセスがある
SUM-4	脆弱性の深刻度などの状況を勘案してセキュリティ更新の提供時期を定めるポリシーを定義するプロセスがある

付録 8.　利用者支援（SG： Security Guidance）に関する要件

SG-1	製品のための多層防御戦略を述べた製品利用者向けの文書を作成するプロセスがある
SG-2	製品の稼働環境が提供すべき多層防御対策を述べた製品利用者向けの文書を作成するプロセスがある
SG-3	設定時に製品を堅牢化するガイドラインを含む製品利用者向けの文書を作成するプロセスがある
SG-4	製品を廃棄する際のガイドラインを含む製品利用者向けの文書を作成するプロセスがある
SG-5	製品の利用者の責務などを述べた製品利用者向けの文書を作成するプロセスがある
SG-6	製品上の利用者アカウントに関する要件や推奨事項を述べた製品利用者向けの文書を作成するプロセスがある
SG-7	セキュリティガイドラインを含む製品利用者マニュアルの誤りや欠落を見つけ出し対処するプロセスがある