制御システムの脆弱性関連情報への対応のための組織体制構築のガイドライン（対象分野：FA システム）

2016 年 12 月 6 日

一般社団法人　日本電機工業会（JEMA）
PLC 技術専門委員会　制御システムセキュリティ WG

＜目次＞

1. はじめに

情報系の製品を製作する企業だけではなく、FA システムに使用する制御機器を製作する企業が製品の脆弱性に対応するために、IPA や JPCERT/CC などのサイバーセキュリティに関する専門機関と連携して対応して行くことが必要になる。本文書の目的は、これらの専門機関と制御機器を製作する企業が連携して、脆弱性情報に対応するための体制作りのガイドラインを提供することにある。

2014 年 5 月に経済産業省の「ソフトウエア等脆弱性関連情報取扱基準」(文献１) 告示が改正され、これを受けて IPA (注１) と JPCERT/CC (注２) （他に連名の発行者は JEITA (注３)、CSAJ (注４)、JISA (注５)、JNSA (注６)）が発行している「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」(文献 2) が改訂された。

同ガイドラインでは、制御システムを対象にしたサイバー攻撃による事故が明らかとなって来ていることや、国内の社会インフラ設備がますます IT 化されていること、産業分野で脆弱性に起因するインシデントの発生から、制御システム分野においてもセキュリティ対策の重要性が強くなっていることを受け、情報系の製品だけでなく、制御システム製品もセキュリティ対策の対象となることが明示された。

（注１）IPA ：Information-technology Promotion Agency, Japan
独立行政法人 情報処理推進機構

（注２）JPCERT/CC ：Japan Computer Emergency Response Team Coordination Center
一般社団法人 JPCERT コーディネーションセンター

（注３）JEITA ：Japan Electronics and Information Technology Industries Association
一般社団法人　電子情報技術産業協会

（注４）CSAJ ：The Computer Software Association of Japan
一般社団法人　コンピュータソフトウェア協会

（注５）JISA ：Japan Information Technology Services Industry Association
一般社団法人　情報サービス産業協会

（注６）JNSA ：Japan Network Security Association
特定非営利活動法人　日本ネットワークセキュリティ協会

図１は同ガイドラインの中で示された「脆弱性発見者」「IPA」「JPCERT/CC」「制御機器ベンダ内に設置する POC（Point of Contact、脆弱性対応窓口、以下 POC と呼ぶ)」「ユーザ」の連携方法について示す図である。

図１に実線で代表的な脆弱性情報の流れを示す。この流れは「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」で手順が示されている流れである。この場合、脆弱性の発見者が届出をするとその情報が IPA に集約される。IPA から JPCERT/CC に脆弱性関連情報の通知が行き、JPCERT/CC から制御機器ベンダである企業内に設置された POC に脆弱性関連情報を伝達する。あらかじめ JPCERT/CC と制御機器ベンダが情報セキュリティ早期警戒パートナーシップを結ぶことにより、JPCERT/CC から制御機器ベンダに製品の脆弱性情報が伝達されるようになる。

図中に点線で示すように、他に IPA や JPCERT/CC を経由しないで制御機器ベンダに脆弱性関連情報

が伝達される場合も想定される。例えば海外の発見者や CERT 機関が IPA を経由せずに、JPCERT/CC に脆弱性情報を通知する場合は、パートナーシップの中の取扱いとは違う手順で調整が進むことがある。また国内外の発見者や海外の CERT 機関が制御機器ベンダの POC に対し直接連絡する場合は、パートナーシップの取扱い範囲外となる。

制御機器ベンダは、伝達された脆弱性関連情報が、自社製品に対して脆弱性関連情報の通りの影響があるかどうかを検証する。検証した結果、製品に脆弱性を確認した場合、どのような対策方式があるかを検討する。以上の検討結果を制御機器ベンダは JPCERT/CC に報告し、関係者で協議の上、対策内容を公表する。また、単独で検証や対策が十分にできない場合は、制御機器ベンダは外部の分析機関に検証や対策方式の検討を依頼する場合がある。

制御製品の持つ脆弱性の影響の大きさと影響の範囲は、その製品の納入先や脆弱性の重要度、また、単独の製品が脆弱性を持つのか、数多くの種類の製品が脆弱性を持つのかどうか、などの条件によって様々なケースが発生することが想定される。この影響の大きさと範囲によって脆弱性をどのように公表するかを決める。

製品が一般のユーザに広く納入され、納入先が特定されない場合は、一般ユーザに脆弱性関連情報を公表する場合がある。これに対して、製品が特定の顧客にだけ納入された場合は、一般ユーザには公表せず、該当製品のユーザにだけに公表する場合がある。公表する範囲、公表する方法と内容、どの機関が公表するのかは、JPCERT/CC、企業、IPA などが協力して、公表の方法を決定する。複数の機関が同時に公表する場合もある。

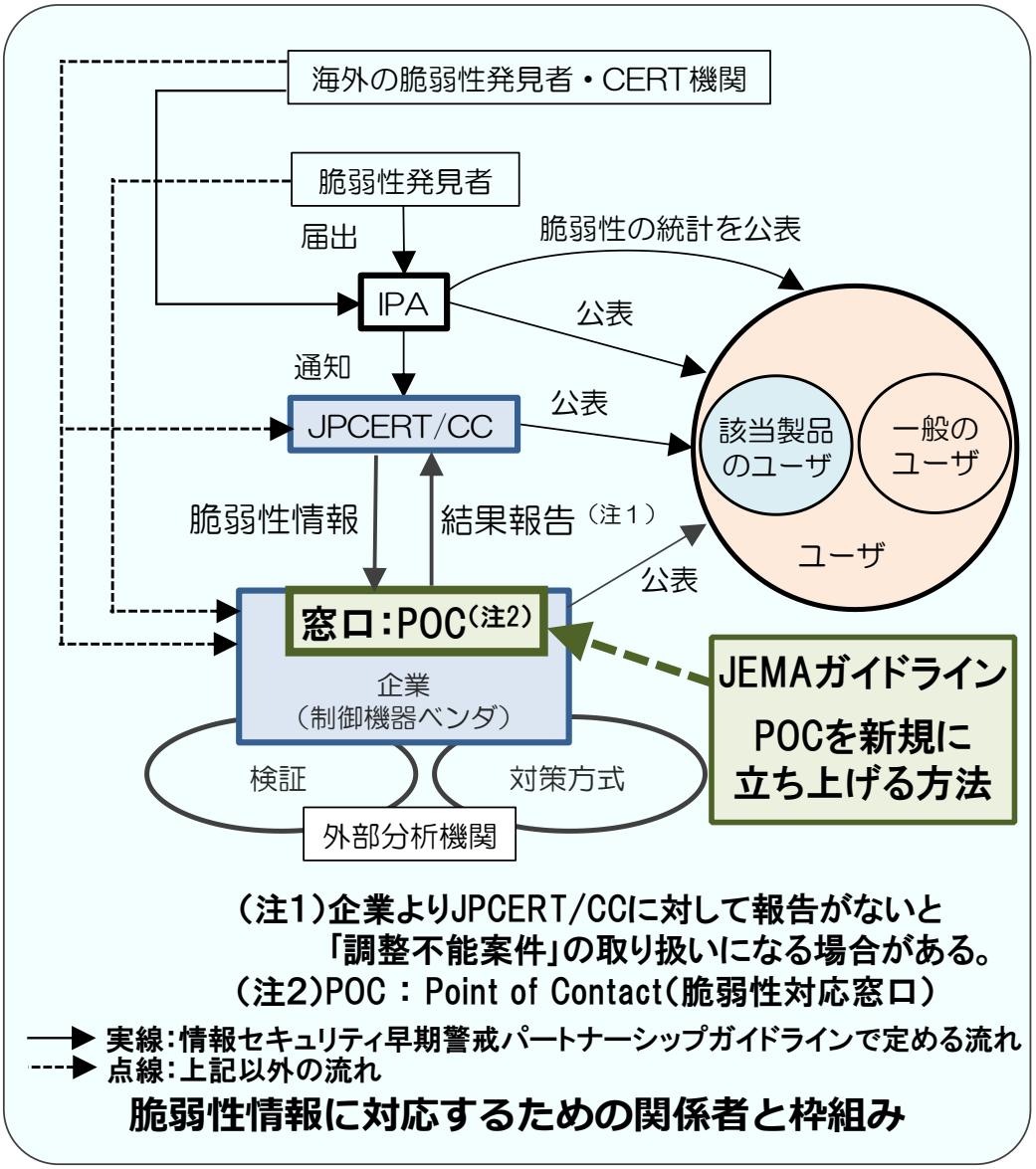


図１．　脆弱性関連情報の伝達と企業内 POC

IPA や JPCERT/CC などの専門機関と企業が連携して脆弱性に対応して行くためには、制御機器ベンダ側で、まず POC を作ることが必要である。本文書では、１章から３章では脆弱性と POC の目的について記載し、４章と５章では具体的な POC の組織を立ち上げるためのガイドラインを示す。本文書は、最初からセキュリティ対策のための機能を網羅するような組織作りを目指すのではなく、既存の開発部門や情報部門の組織をベースにしてスモールスタートを行い、企業内で速やかに機能する POC を立ち上げることを推奨する。

本文書は、対象とする読者として、制御機器ベンダ内で製品のセキュリティを担当し、JPCERT/CC のパートナーシップガイドラインに従って企業内で POC を新たに立ち上げることが必要になった責任者や担当者を想定している。ここで、本文書に取り上げる制御製品については、FA（Factory Automation）関連の産業用で使用する制御機器（主に PLC と PLC に接続される制御機器）を対象としている。

2. 脆弱性とは

本ガイドラインでは、「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」の中で定められている「製品の脆弱性」を「脆弱性」として定義する。このため、脆弱性の詳細については「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」を参照することとする。本ガイドラインの読者の理解のために、以下にその文書に示されている脆弱性の記述の概要を示す。

脆弱性とは、ソフトウェアやシステム等において、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である。

ここでセキュリティ上の機能や性能として、具体的には機密性、完全性、可用性の３つの性質を指す。機密性とは、ソフトウェアやシステムが提供する情報や機能を、認められた者にのみ提供できる状態を確保することである。完全性とは、情報や機能が破壊・改ざん・消去されていない状態を確保することである。可用性とは、ソフトウェアやシステムが提供する情報や機能を、必要とするときに中断されることなく利用できる状態を確保できることである。

例えば制御システムにおいては、システムに含まれるソフトウェアやデータの閲覧を認められていない者が読み出せる状態になった場合、機密性が失われていることになる。また、システムに含まれるソフトウェアやデータが改ざんされたり消去されたりしている場合は完全性が失われていることになる。システムを利用できない状態になった場合は可用性が失われていることになる。

脆弱性は、ソフトウェアやシステムの仕様、設計、製作の欠陥によって生じる場合もある。たとえば、本来公開すべきでないデータに対して、インターネットを通じて誰でもパスワード等の保護なしにアクセスできる状態になっている場合には、このシステムは機密性が失われる脆弱性を持っているとされる。これらのシステムは本来、データをインターネットへ公開しない、あるいは、パスワード等で保護するなどといった仕様でなければならない。

一方で、制御機器ベンダが開発したプログラムだけではなく、第三者により開発され、そのソフトウェアやシステムが使用している一般のライブラリプログラムなどから脆弱性が継承され、それが製品の発売された後に脆弱性が顕在化するケースも想定される。また、制御機器ベンダの想定とは異なる使用方法によって、脆弱性が顕在化することもある。脆弱性は、製品の欠陥や不具合とは異なり、制御機器ベンダが最大限努力していたとしても存在しうるものと考えなくてはならない。

また、近年では制御システムでのイーサーネットの技術に代表されるように情報システムと要素技術の共通化が進み、特別なハードウェアがなくともソフトウェアにより脆弱性の解析が可能になっている。インターネット上には、脆弱性関連情報や解析ツールが公表されており、解析のノウハウの入手が可能になっている。

3. 脆弱性関連情報と POC の必要性

3.1 脆弱性関連情報への対応の必要性

企業の中、あるいは脆弱性に対応するために委託している外部の組織に、POC などの脆弱性関連情報に対応する組織（または、機能）がない場合、JPCERT/CC から（あるいは、その他の組織、届出者などのその他のルートから）企業に脆弱性関連情報が伝達された場合に、事前に脆弱性情報に対応する方法に関する知識が準備されていないため、対応に時間がかかる場合がある。また、脆弱性関連情報への対応が企業内の担当者により異なってしまうことにより、不安定な対応になる場合がある。

このような場合には、企業から JPCERT/CC への応答ができないまま、時間が経過してしまう恐れがある。企業から JPCERT/CC へ応答が全くない場合には、場合によっては、「調整不能案件（連絡不能者リスト)」の取り扱いになる場合がある。

さらに企業が脆弱性を放置した場合、次の事例に挙げるように企業ブランドや信用を損なうリスクがある。これらの事例は、JPCERT/CC の発行する「制御システム用製品の開発ベンダにおける脆弱性対応について」(文献４) に記載された例である。このようなリスクを回避するため、企業は脆弱性に対応する必要がある。

＜脆弱性を放置した場合のリスク＞

- 「脆弱性を放置したとして企業ブランド・信用を損なうリスク」（対応を放置した結果、世界中の顧客に文書で事情説明することが必要になった例がある)。
- 自社製品の脆弱性が原因になり社会的、経済的な混乱を引き起こすリスク
- 契約によっては損害賠償となるリスク

企業が脆弱性に対応するためには、各方面から脆弱性関連情報を収集し、その情報が自社製品に影響するかどうかを判断する必要がある。一般の企業においては、広い範囲から脆弱性関連情報を収集し続け、その情報を的確に分析するための人員が揃っていない場合がある。さらに脆弱性関連情報においては初動の時に、ソフトウェアやセキュリティに関する知識を元にその情報の重要性を理解する必要がある。脆弱性関連情報のこのような特長のために、初動における情報収集と重要性の判断は関連機関が共同で実施することが現実的な方法である。

このような課題に対して IPA、JPCERT/CC と企業が連携するための企業側の窓口として、「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」と「制御システム用製品の開発ベンダにおける脆弱性対応について (文献 3)」を参考にして、企業内に組織（POC）を構築することを推奨する。

POC という組織はこれまで制御機器ベンダにとってなじみのない組織であるため、その概要、目的、組織の構築方法について以下に解説する。

3.2　POC の必要性

JPCERT/CC や外部組織からの脆弱性情報の受付窓口となる POC を企業内に設置しておくことにより、企業が IPA や JPCERT/CC と連携し、迅速に、かつ、脆弱性関連情報に安定して応答することができるようになると考えられる。あらかじめ POC を中心とした脆弱性対応の仕組みを作っておくことにより対処方法のノウハウを集約することができ、また、JPCERT/CC や他の CERT 機関、及び、脆弱性届出者などに対して、企業の連絡先が事前に明確になっているため、脆弱性情報の伝達に無駄な時間を費やすことが少なくなると考えられる。

４．　POC の期待される役割

4.1　POC の役割：情報伝達

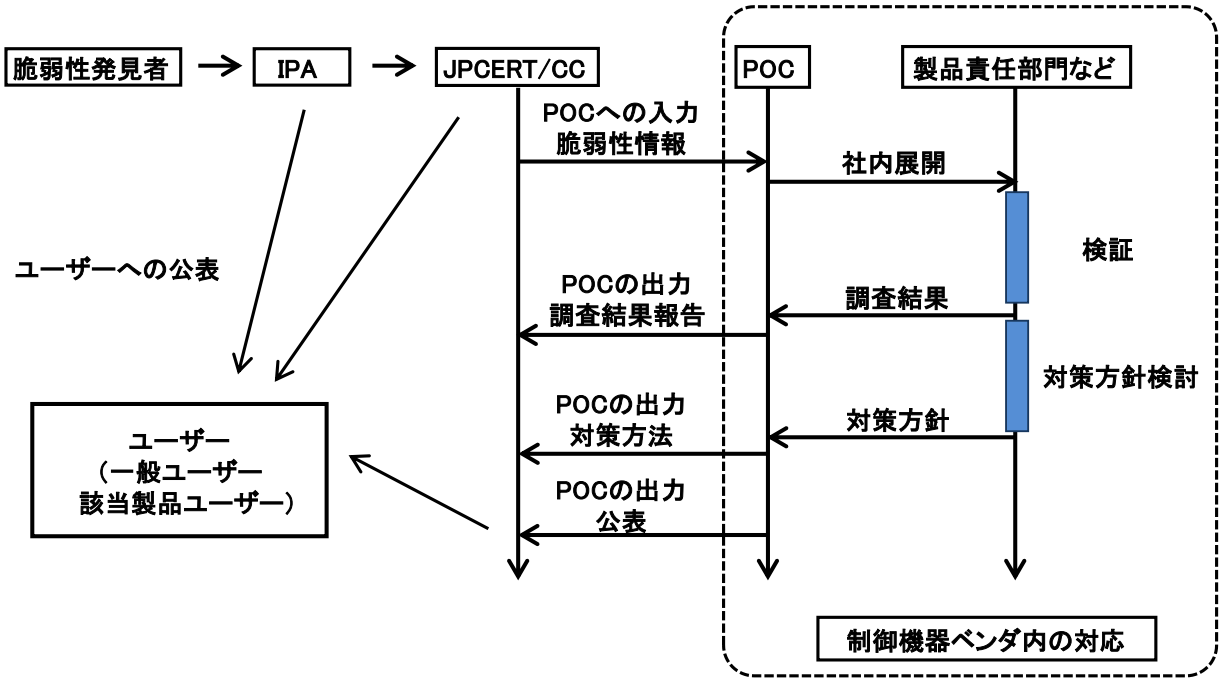


図３.POC の情報伝達機能の概略

脆弱性発見者が IPA に脆弱性関連情報を届け出た場合、IPA は脆弱性関連情報を JPCERT/CC に連絡する。JPCERT/CC はこの脆弱性関連情報の影響を受ける製品を特定し、その製品開発者の POC に対して脆弱性関連情報を通知する。POC は企業の窓口として情報を受け取る（POC への入力）。

組織内における、製品責任部門などの組織は、POC から脆弱性関連情報の展開を受けた後、通知された脆弱性関連情報が製品に該当するかを検証し、調査結果を POC を通じて JPCERT/CC に報告する（POC の出力）。

また、製品責任部門が脆弱性に対する対策方針を決定した後、POC が対策方針を JPCERT/CC に通知し（POC の出力）、IPA、JPCERT/CC、企業の３者の協議により、必要に応じてユーザに対する公表を行う（POC の出力）。

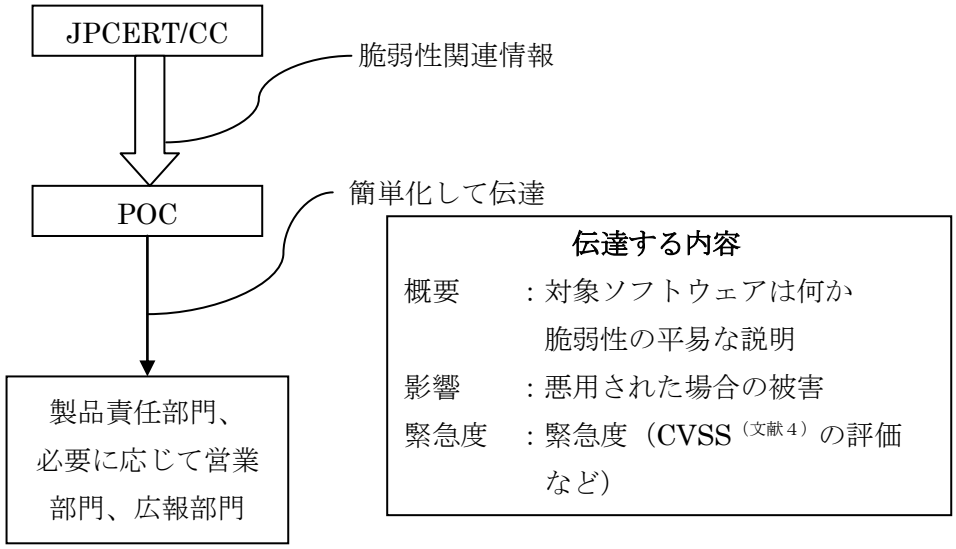


図４．　POC は JPCERT/CC からの情報を組織内に平易に伝達

POC はこの情報を組織内の関係部門に対して情報伝達する。POC は外部から報告された脆弱性関連情報をどの製品・機器・システムに関連するものであるかを判定し、その情報を適切な部門（製品責任部門をはじめ、場合によっては営業部門、広報部門等を含める）に対して伝える必要がある。また、製品責任部門の理解度に応じて、製造部門が具体的に現象を理解できる形に翻訳し、平易に伝達することが必要となる。

4.2　POC が兼務することもある役割その１：教育

以下、4.2 節から 4.4 節に POC にとって必須の役割ではないが、POC が兼務することもある役割についてまとめる。

POC には、組織内の関係部門に対する教育を行うことも期待される。ここでの教育では①制御機器の脆弱性が及ぼすリスクの大きさ②脆弱性関連情報がもたらされた場合の対応についての教育が求められる。

制御機器の脆弱性についてはこれまで取り上げられる機会が少なかったために、その影響や制御機器を製作する企業としてのリスクの大きさが良く知られておらず、結果として製品責任部門による脆弱性への対応に遅れが出ることが懸念される。

具体的には、脆弱性は製品の不具合とは異なるため、不具合対策に比べて対応の仕方が確立してなく、対応する期間が延びる場合がある。対応までに時間を要すると、その間に脆弱性を攻撃され、さらに被害の大きなトラブルが出る可能性がある、という認識を持たせる教育が必要である。対策が遅れることにより、脆弱性に対する姿勢が前向きではないと外部から評価される恐れもあり、企業イメージが悪化する恐れがある。

4.3　POC が兼務することもある役割その２：技術相談窓口

脆弱性の情報に対して、その脆弱性を再現して発現条件を調査し、原因の追究、影響の評価、対策方法の策定を行うのは POC ではなく製品責任部門の役割である。また、製品責任部門は、脆弱性を作りこまないような製品開発を行っていくことも必要である。

POC は製品責任部門に対して、外部の返答先、返答期限、返答内容等について知識を持ち、製品責任部門に必要な情報は何かを示し、必要な対応を取る相談窓口として機能する必要がある。

さらに、日頃から、POC として内外の関連部門と連携することにより、制御システムセキュリティの関連の情報を収集することが望ましい。

4.4　POC が兼務することもある役割その３：脆弱性関連情報のユーザへの伝達及び公表

製品と脆弱性関連情報との関連性が明確になった段階で、製品責任部門は脆弱性が及ぼす影響範囲、対策可否、回避策等の脆弱性関連情報をまとめる。

POC は製品責任部門、営業部門、広報部門と連携し、脆弱性関連情報への対応方法を脆弱性関連情報の報告者に回答する。その後、JPCERT/CC と協議して、脆弱性情報の公表・非公表や公表内容・公表時期などについて調整する。

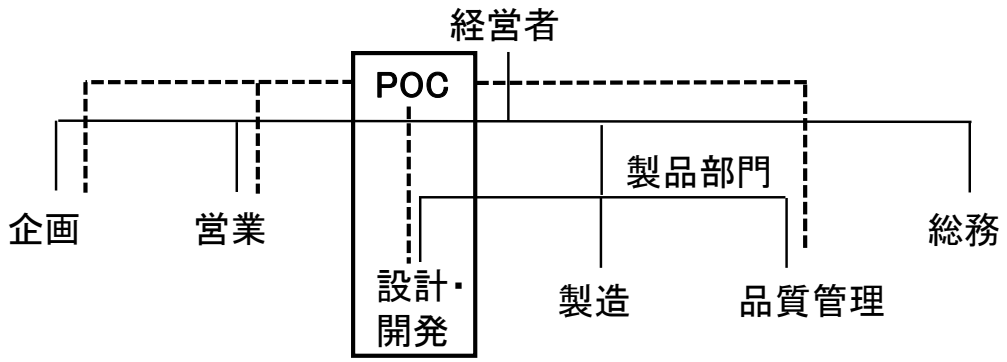
5.　POC 体制構築のガイド

5.1　POC 体制構築のためのガイドラインの考え方

本ガイドラインでは、実際に POC を構築する時の組織の参考例を示す。このような例を参考にして企業内に POC を構築することを推奨する。POC の立ち上げにあたっては、人員的・技術的・所掌的な問題から新規組織として立ち上げることが困難な場合も予想される。このような場合には既存の組織をベースに POC を立ち上げることが考えられる。POC を円滑に立ち上げるための手法として、製品部門をベースに組織する方法と、情報部門をベースに組織する方法の２つの例を示す。以下に示すような機能を備えた POC をまず立ち上げ、徐々に完全な組織体制となるよう推進して行くことを推奨する。

5.2　POC の作り方（参考例①）：組織内の製品部門をベースに組織する場合

POC は、災害に備えるための防災体制に例えられる。企業において、災害に備える体制は、一部を除いては、専任の組織体制とはなってない。日常業務の傍らにおいて、万が一災害が発生した場合に備え、いわば、仮想的な体制が組織されている（図 6. 参照)。製品責任部門の品質保証部門や設計・開発部門を中心に防火組織の例にならって POC を構築し、いざという時に機能するよう、通常から組織作りと意識作りをすることが必要である。このような例では、脆弱性関連情報の知識の分野の特性から製品の設計・開発部門が POC を担当する例が多い。



――：企業の組織体制

……：防火組織のような仮想的な体制（脆弱性情報対応の POC を中心とした体制）

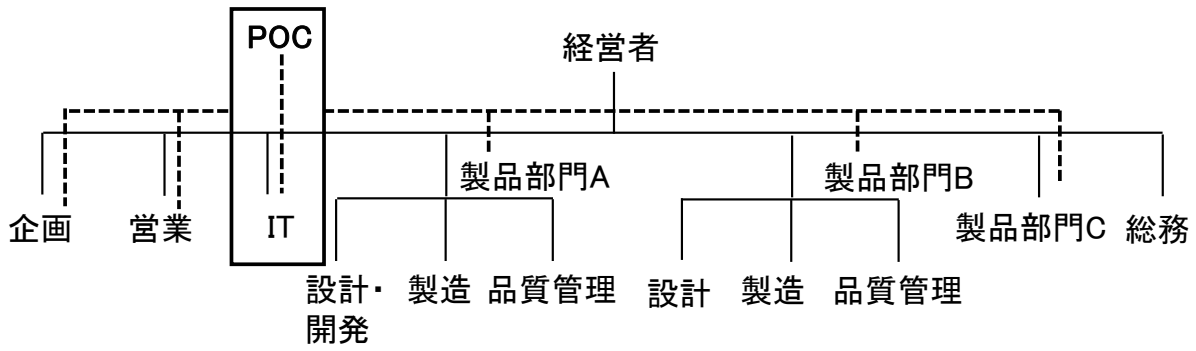
図６． 製品の種類が単一の企業の POC（設計・開発部門を POC とする体制）

5.3 POC の作り方（参考例②）：組織内情報部門をベースに組織する場合

１社で数多くの製品を製造する企業においては、個々の製品責任部門に POC を設置するのは非効率な場合がある。例えば、入手した脆弱性関連情報がオープンソフトウェアに関わる場合、当該オープンソフトウエアを搭載した製品すべてが、脆弱性への対応の候補となる。このような場合、POC には、全社の製品とその製品責任部門を包括的に把握し、入手した脆弱性関連情報を適切な製品責任部門に展開する機能が必要となる。

企業によっては、組織内の情報システムや公開ウェブなどを扱っている本社 IT 部門がある。POC 設置の一つの方法として、本社 IT 部門にて、POC を設置し脆弱性関連情報を扱う方式がある（図 7. 参照）。

制御製品や制御システムでは、現状のところ POC に定常的な負荷は少ないと予想され、独立した組織として運営することは難しい。このため、既存の組織に追加業務として POC 業務を加えた方が、POC 体制を構築するのがより容易であると考える。また、このような POC の体制により、脆弱性関連情報の窓口を一本化し、組織内、外販を問わず迅速な対応が可能となる。



――：企業の組織体制

……：本社 IT 部門に脆弱性情報対応の POC を兼務させる体制

図７． １社で数多くの製品を製造する企業（本社の IT 部門を POC とする体制）

5.4 脆弱性関連情報の秘密管理（文献５）

JPCERT/CC から受け取る脆弱性関連情報には、次のように秘密情報の内容が含まれる場合がある。脆弱性関連情報は、対策方法が明らかになるまでは、情報が漏洩しないように取り扱うことが重要である。

①一般的な IT 技術に関わる脆弱性関連情報

社内 Web や共有ドライブを使い、公開情報として扱う。

②特定の製品・システムに関わる脆弱性関連情報

特定の製品・システムに関わる担当だけが扱える秘密情報として扱う。

③緊急性を要する脆弱性関連情報

脆弱性関連情報の情報共有の仕組みについて、JEITA のガイドライン（文献6）「製品開発ベンダーにおける脆弱性関連情報取扱に関する体制と手順整備のためのガイドライン」の 4.1.4「情報共有の枠組み」に、脆弱性関連情報の管理方法が示されている。

5.5 JPCERT/CC への POC 登録

製品開発者が POC を組織した後、「JPCERT/CC 製品開発者リスト」に POC を登録して JPCERT/CC から脆弱性関連情報を入手できるようにすることを推奨する。POC の登録方法については、JPCERT/CC のサイトにその案内（文献６）があるので参照して手続きができる。

製品開発者は JPCERT/CC に窓口担当者の情報を提出し、登録手続きの後、運用を開始する。現在、JPCERT/CC は無償で脆弱性関連情報を提供している。

６． おわりに

本文書でまとめた脆弱性情報に対応する組織を参考にして検討し、制御機器を製作する各企業が対応組織を構築することを推奨する。

７． 引用文献

（１）文献１ ：P.3
脆弱性とは：引用元:経済産業省告示第 110 号 「ソフトウェア等脆弱性関連情報取扱基準
http://www.meti.go.jp/policy/netsecurity/downloadfiles/140514kaiseikokuji.pdf

（２）文献２ ：P.3
「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」
https://www.jpcert.or.jp/vh/partnership_guideline2015.pdf

（３）文献３：P.7
JPCERT/CC の発行する「制御システム用製品の開発ベンダにおける脆弱性対応について」
https://www.jpcert.or.jp/ics/information05.html

（４）文献４：P.10（図中）
CVSS による脆弱性の深刻度評価
http://www.ipa.go.jp/security/vuln/SeverityLevel2.html

（５）文献５：P.14
http://it.jeita.or.jp/infosys/info/0407JEITA-guideline/guideline-v10.pdf
「4.1.4 情報共有の枠組み」に相当する内容である。

（６）文献６：P.14
JPCERT/CC　POC の登録について　製品開発者登録の方法
https://www.jpcert.or.jp/vh/regist.html