JPCERT CC®

参考資料
「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」

2014年8月11日

一般社団法人
JPCERTコーディネーションセンター

本資料について

2010年にStuxnetが発見されて以降、制御システムのセキュリティに対する関心が高まりを見せるなか、セキュリティの研究者らによって様々な制御システム用製品の脆弱性が発見されています。発見された制御システム用製品の脆弱性は、IT製品の脆弱性と同様、適切かつ安全に取扱われることが望まれます。

2013年度、JPCERTコーディネーションセンターでは、経済産業省の平成24年度情報セキュリティ対策推進事業（サイバー攻撃の被害拡大に対する緊急事態対策事業）として、国内の制御システム製品ベンダにご参加いただいて、「制御システムベンダにおける脆弱性取扱の社内体制整備促進検討会」を開催し、制御システム用製品を扱うベンダにおける脆弱性関連情報の取扱体制について検討を行いました。

本資料は、制御システム用製品を扱うベンダが脆弱性関連情報を取扱う場合に考えられる「必要な機能」、「機能を担う体制の在り方」等について、同検討会で交わされた議論をまとめたものです。脆弱性がもたらす事業リスクや制御システム用製品の脆弱性を取り巻く昨今の状況から説き起し、一例として仮想企業A社における対応機能・体制の在り方、外部組織を含めた脆弱性関連情報の取扱いの流れも紹介しています。

本資料を脆弱性関連情報の取扱いについて検討される際の参考資料としてご活用いただければ幸いです。なお、実際の機能・体制の整備に当たっては、自社の状況に合わせ、必要な機能・体制をご検討ください。

目次

- 脆弱性と脆弱性に関わる事業リスク
  ・・・ P3 ～ P6
- 制御システム用製品の脆弱性を巡る動向
  ・・・ P7 ～ P10
- 脆弱性関連情報の取扱社内体制について
  ・・・ P12 ～ P25
- 仮想企業A社における脆弱性関連情報の対応事例
  ・・・ P28 ～ P43

脆弱性と脆弱性に関わる事業リスク

製品の脆弱性※とは

ソフトウエア製品やウェブアプリケーション等において、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セキュリティ上の問題箇所

（経済産業省告示第110号　「ソフトウエア等脆弱性関連情報取扱基準」より）

製品の脆弱性とは

- 汎用技術を使った製品が
- 取扱説明書などから妥当と判断される運用環境下で
- 特定の攻撃行為が行われた時に
- セキュリティ上の問題を生じる

という特性である

特注品は対象としない
∵第三者の被害が無い

まだ攻撃に使われていない脆弱性も対象とする

セキュリティ上の問題とは、情報セキュリティのCIA※の侵害または他の攻撃の踏み台になること

製品の脆弱性確認では再現性が必要

※「製品の脆弱性」・・・後述する情報セキュリティ早期警戒パートナーシップの対象となる「脆弱性」を指す

※C（Confidentiality：機密性）、I（Integrity：完全性）、A（Availability：可用性）

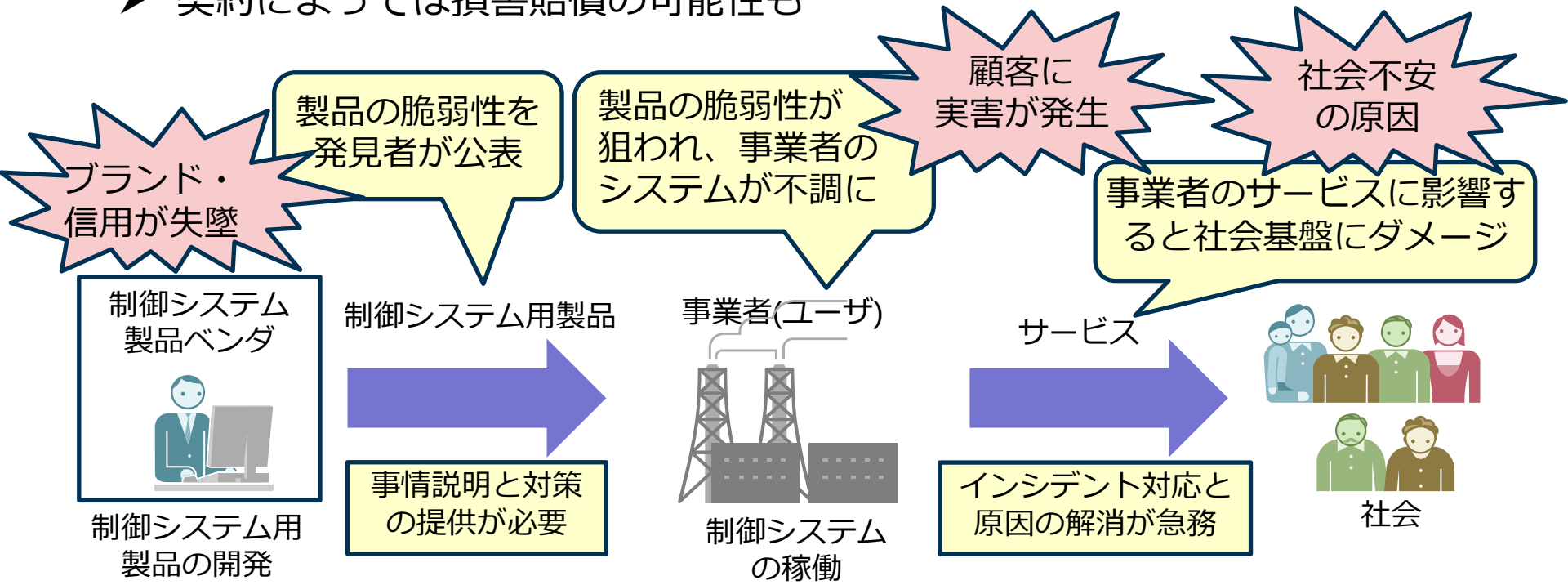
製品の脆弱性とインシデント

製品の脆弱性の例	インシデントの例
● PLC製品XYZは、500Byte以上のサイズのICMPを受信すると停止する ● PLC製品ABCは、特定の形式のIPパケットを受信するとリセットされ、パスワードがデフォルト値に戻る ● HMIソフトウェアPQRは、入力フィールドに細工した文字列を入力すると、本来はシステム管理者しかアクセスできない情報を読み出したり書き換えたりできる	● PLC製品XYZが、インターネットに接続されて、デフォルト・パスワードのまま運用され、不正操作される ● P工場で稼働中のPLC製品が、週に何回か、理由が不明な状態で警報音を発して停止する

脆弱性に関わる事業リスク

- 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
  - 世界中の顧客に文書で事情説明した事例も
- 自社製品の脆弱性が社会的経済的な混乱を引き起こすリスク
  - 脆弱性への対応の遅れにより、脆弱性が攻撃され、社会基盤を支えるシステムが不安定に
- 自社製品の脆弱性が顧客の事業に実害をもたらすことによるリスク
  - 契約によっては損害賠償の可能性も

脆弱性は経営者が配慮すべき事業リスク



制御システム用製品の脆弱性を巡る動向

制御システム用製品の脆弱性を巡る動向
①制御システム製品ベンダ以外の脆弱性の公表

セキュリティベンダによる脆弱性公表(米国)

- DigitalBond社が複数の制御システム用製品に存在する多数の脆弱性情報を同時公表し、後日検証ツールも公表 (2012年)

発見者(セキュリティベンダ等)により脆弱性が公表され、当該脆弱性をベンダが放置していたと非難されかねないことに注意する必要がある

公的調整機関による脆弱性公表

- ICS-CERTが Vulnerability Handling policyを改定(2012年)

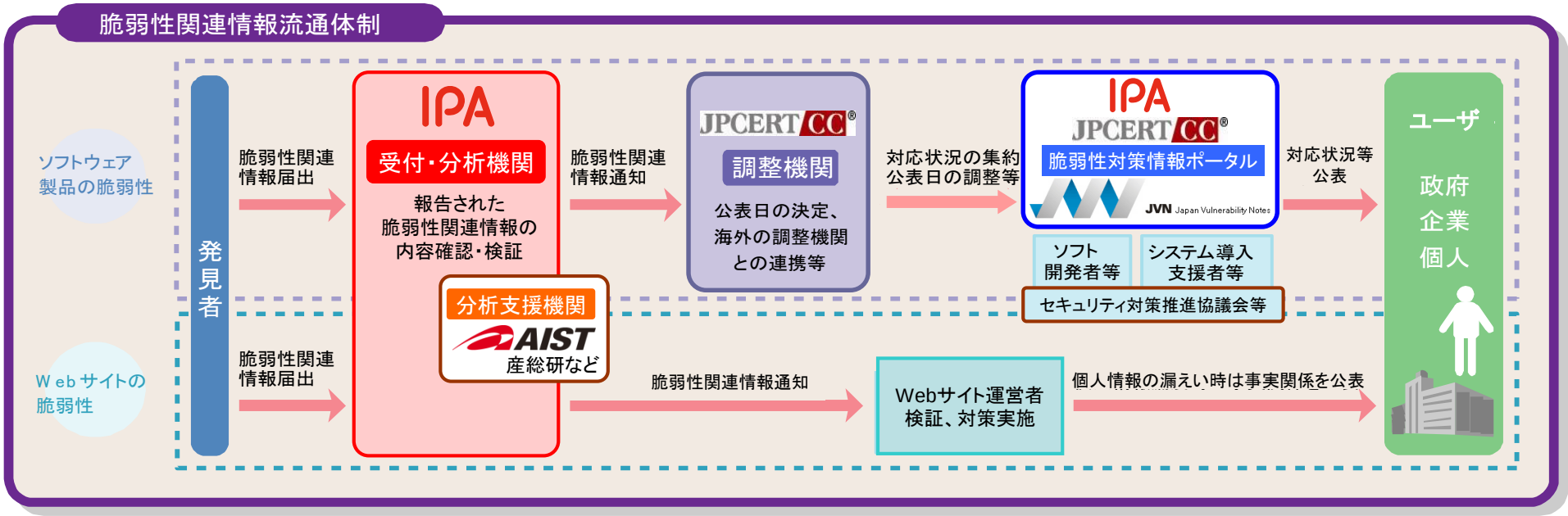
UPDATE! In cases where a vendor is unresponsive, or will not establish a reasonable timeframe for remediation, ICS-CERT may disclose vulnerabilities 45 days after the initial contact is made, regardless of the existence or availability of patches or workarounds from affected vendors.

- 日本では、IPA主催の情報システム等の脆弱性情報の取扱いに関する研究会において、制御システム用製品の脆弱性取扱いについて検討が行われ、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対象ソフトウェアに制御システム用製品を明示（2014年5月公開）

公的調整機関を含めた、発見者とのコミュニケーションを行うことで、脆弱性情報が突然公表されてしまうリスクを低減できる

（参考）情報セキュリティ早期警戒パートナーシップ

- ソフトウェア等の製品やウェブサイトで発見された脆弱性関連情報を受け付け、製品ベンダやサイト運営者に対策を促す枠組み
- 「ソフトウエア等脆弱性関連情報取扱基準」に基づく官民の連携体制として整備され、2004年7月8日に運用を開始
- 発見されたソフトウェア等の製品に対する脆弱性関連情報は、IPAが受け付け、JPCERT/CCが影響を受けるソフトウェア等の製品を特定し、製品開発者へ内容を通知し、脆弱性への対応を協議・調整する
- JVNは、対応された脆弱性の詳細と製品開発者の対応状況を公表し、利用者へ対策を周知



https://www.ipa.go.jp/security/vuln/index.html#section10

制御システム用製品の脆弱性を巡る動向
②制御システム製品ベンダの対応（情報開示等）

■ 製品脆弱性情報の開示プロセスの公表

- 日立グループでは、製品ベンダIRT（Incident Response Team）の活動として製品脆弱性情報の開示プロセスを公表（2010年）
- Siemens社は、脆弱性についての詳細な情報を含んだセキュリティアドバイザリを通じて対応が完了した脆弱性に関する情報の公表ポリシーを公開(2012年)

■ ソフトウェア製品の脆弱性に関する国際標準化

- ソフトウェア製品開発者の脆弱性開示（ISO/IEC 29147）、脆弱性情報取扱い手順（ISO/IEC 30111）の国際標準化（2013～2014年）

■ 技術研究組合制御システムセキュリティセンター(CSSC)の設立

- 制御システムのセキュリティを高める技術の研究開発、制御機器の安全性の検証、模擬プラントを使った人材育成・普及啓発(2012年)

脆弱性への真摯な姿勢を表明することで、脆弱性への対応努力について、顧客や発見者等の第三者から理解を得ることにつながる

次ページ以降、制御システム用製品およびソフトウエアを開発するベンダが自社製品の脆弱性関連情報を取り扱うための組織内基盤を整える上で、設置・整備することが望ましい機能・体制やそれら機能・体制を設置・整備する手順、脆弱性関連情報の取扱手順を例示しております。

28ページ以降は、仮想企業 A社を仮定し、A社が自社製品の脆弱性関連情報の適切な取扱いに向けて設置・整備した体制や実際の脆弱性関連情報の対応事例を記載しております。

当資料は参考資料としてご活用いただくことを想定しております。実際の機能・体制の整備に当たっては、自社の状況に合わせ、必要な機能・体制等をご検討ください。

脆弱性関連情報の取扱社内体制について

制御システム製品ベンダに期待される取組み

- 制御システム製品ベンダは脆弱性取扱に向けて以下の取組みが期待される

脆弱性取扱に関する中核機能の整備
（脆弱性POC※）

※「脆弱性POC」・・・15ページ参照

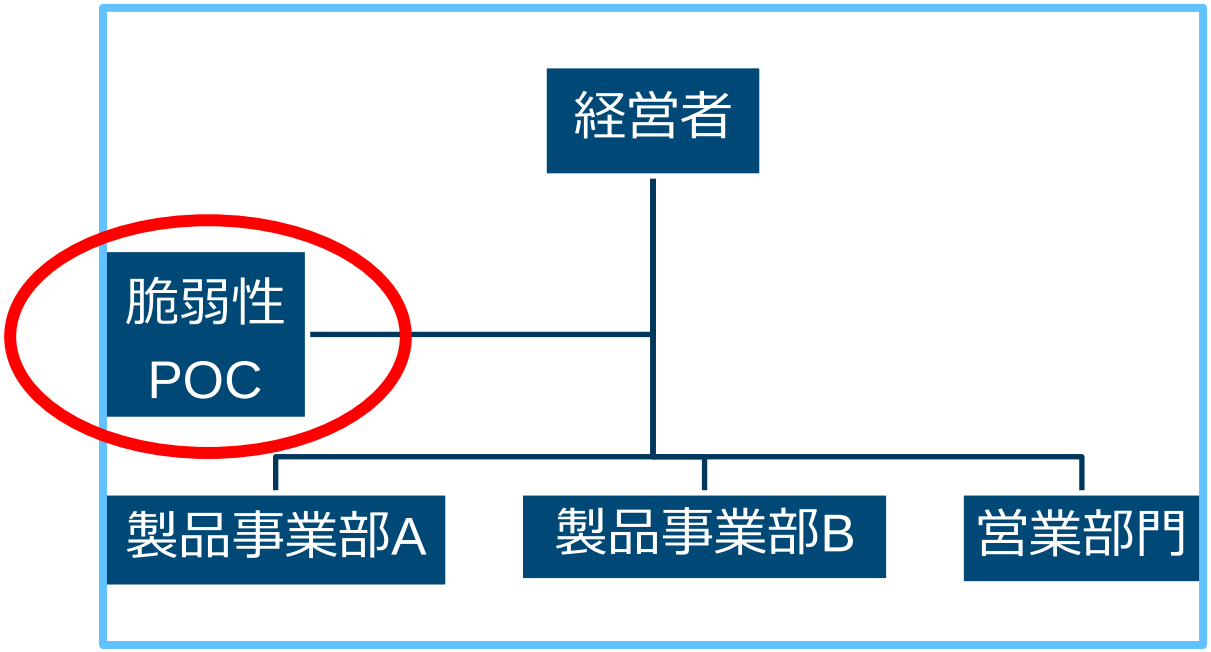
全社的なコミットメントの宣言
（脆弱性取扱ポリシー、責任者）

脆弱性取扱プロセスの整備
（体制、手順）

順番は自社の状況に応じて変更可能

脆弱性取扱に関する中核機能の整備

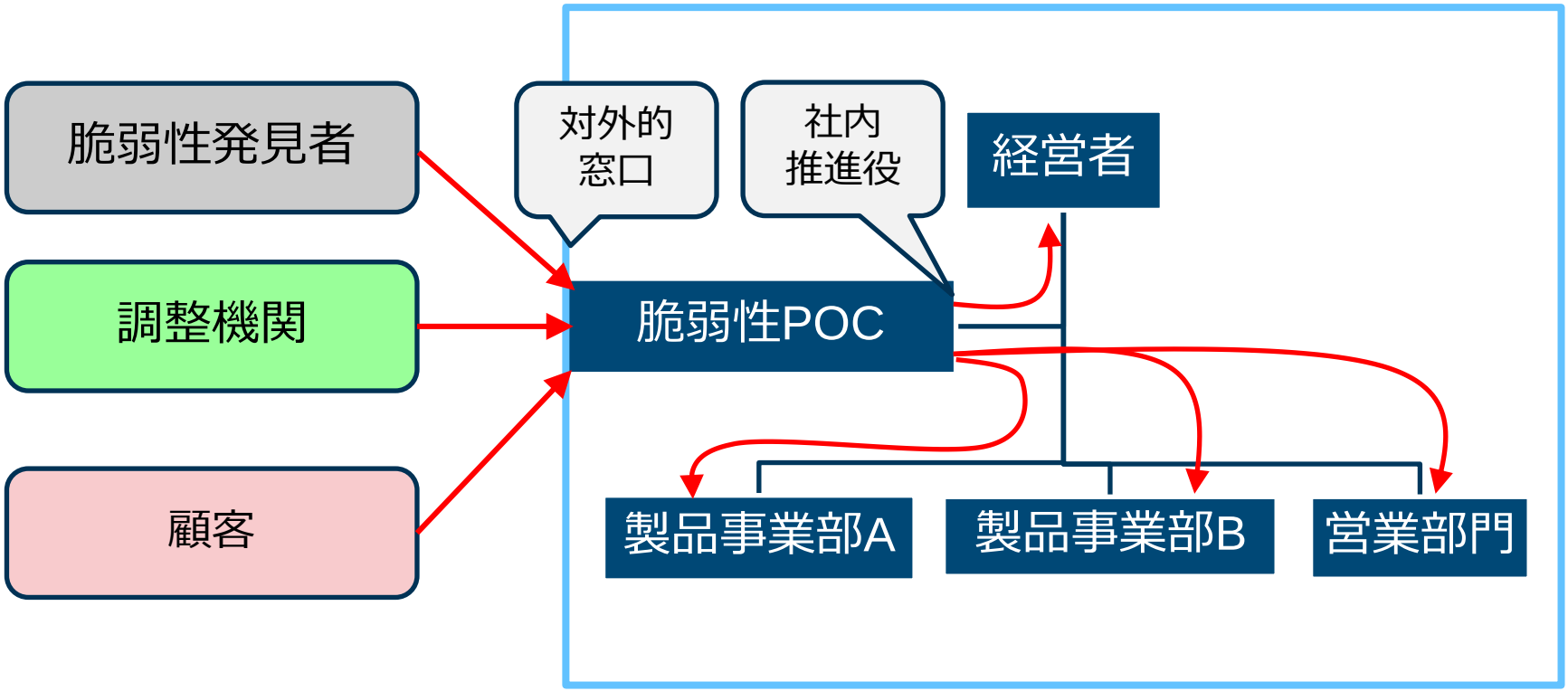
- 脆弱性取扱に関する中核機能
- 脆弱性の受付や外部組織と情報交換を行う対外窓口（脆弱性POC）を置き、ミッションと権限を定める
- 提供している様々な製品に起こりうる問題であるため、横断的な位置づけで捉えるべき



脆弱性POC（ポック）の設置

脆弱性POC（Point of Contact）は…

- 脆弱性の発見者や調整機関がコンタクトする対外的窓口
- 社内の脆弱性取扱のしくみを整備・維持・改善する推進役



脆弱性とCSIRT（シーサート）

- 製品ベンダには、3種類のCSIRT機能が存在しうる
- 自社製品の脆弱性取扱は脆弱性POCまたはPSIRTが主導する

◆ 通称(俗称)	◆ サービス対象	◆ 対応する事案
◆ 脆弱性POC ◆ PSIRT	◆ 製品事業部	◆ 社外の脆弱性発見者や調整機関と社内の製品事業との間の脆弱性情報交換を統括し円滑化する司令塔
◆ 組織内CSIRT ◆ SOC	◆ 社内の利用者 ◆ 企業ホームページ	◆ 事業活動に直接に付随して発生する(主として社内で起きる)セキュリティ事故に対応
◆ 顧客インシデント対応支援	◆ 顧客	◆ 提供製品やサービスに関連して顧客で発生したセキュリティ事故(インシデント)における顧客による対応を支援

PSIRT： Product Security Information Response Center
SOC：Security Operation Center　　POC： Point of Contact

脆弱性POC（以下POC）のイメージ①

- 要　員：ハンドリング責任者と窓口業務担当の2名以上
- スキル：ネットワークセキュリティ
  コンピュータプログラミング
  ソフトウェア製品ベンダのセキュリティアドバイザリを読んで理解できる水準
- 情　報（収集・整備することが望ましい情報等）：
  脆弱性情報データベース（JVN、NVD）
  調整機関、研究機関等の対策情報、技術情報
  自社製品の技術構成、連絡先
- 関係部署：
  - 設計部門・製品主管部門
  - 研究開発部門
  - 品質管理部門・品質保証部門
  - SI部門
  - カスタマケア部門
  - 営業部門
  - リスク管理統制部門
  - 広報部門

※ただし、組織の業態や規模によっては、独立の部門ではなく、いくつかの部門の機能を兼務している場合もある

POCのイメージ②

POCの位置づけ

- 既存の不具合対応体制の拡張（品質管理として）
- 緊急対応の一部（危機管理として）
- 企業グループ全体の窓口（グループ統制として）

POCの設置場所

脆弱性への対策を行う主担当部門とPOC機能を受持つ部門が異なる場合も、一致させる場合もある

- ケース1：大半の脆弱性が特定の研究開発部門の製品に偏っている
  → 事業部
- ケース2：事業部横断的な共通技術を担当する部門がある
  → 事業部
- ケース3：脆弱性を持つ製品が複数の部門にある → 管理部門
- ケース4：研究所が委託研究型ではなく、本社予算で動いている
  → 研究所
- ケース5：（強い権限を持つ）組織内CSIRTがある
  → 組織内CSIRT

POCのイメージ③

- POCに関する合意形成
  - 対象範囲の設定

    事業部　/　全社　/　国内外グループ会社　/　OEM委託先

    ［考え方の例］
    - 情報系と制御系のPOCを一本化するか、別々にするか
    - 開発子会社の場合、製品販売元が責任を持つ
    - OEM委託先には、自社から連絡するケースとJPCERT/CCから連絡するケースがある
  - ミッションの明確化

    ［例］
    - 脆弱性の発見者や調整機関がコンタクトする対外的窓口
    - 社内の脆弱性取扱のしくみを整備・維持・改善する推進役
  - 権限に関する社内統制
    - 所掌範囲、関係部署への指示・要請

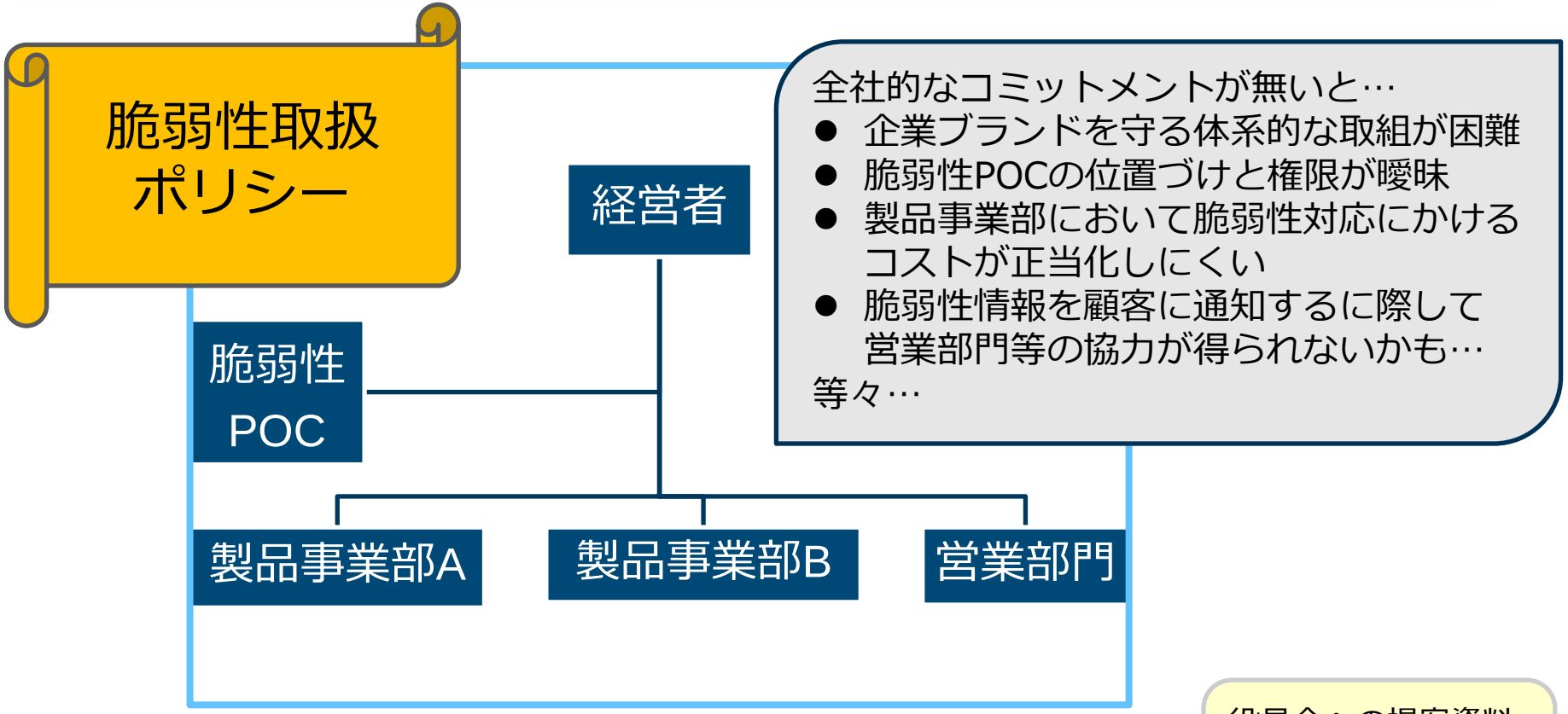
（参考）製品開発者の窓口登録について

- 脆弱性関連情報の通知を希望する製品開発者は、JPCERT/CCに製品脆弱性対策管理者の連絡窓口情報を登録する

- 登録種別には次の２種類がある
  - 一般登録
    登録者は、自らが開発した製品固有の脆弱性関連情報に限らず、製品に関係する可能性のある脆弱性関連情報を受け取り、調査を行うことができる
  - 個別登録
    登録者は、原則として、自らが開発した製品に固有の脆弱性関連情報だけを受け取り、調査を行うことができる

(https://www.jpcert.or.jp/vh/regist.html)

全社的なコミットメントの宣言



役員会への提案資料

全社ポリシー(規程)

責任者が…

- 脆弱性への対応を行う全社方針を宣言する
- 社内の対応体制を整備し権限を付与する

脆弱性取扱ポリシーの策定

脆弱性取扱ポリシーとは

- 脆弱性の取扱いに関する基本方針
- 責任者が表明する、組織としての脆弱性取扱におけるコミットメント
- 公開することで、脆弱性に対する自社の姿勢を発見者や調整機関、顧客に伝える効果
- 公開するのは概要だけでもよい

（参考）脆弱性取扱ポリシーの公開事例

＊日立グループにおける製品脆弱性情報の開示プロセス
http://www.hitachi.co.jp/hirt/publications/hirt-pub10008/index.html

＊Siemens Vulnerability Handling Version 1.3, 2014-05-07
https://www.siemens.com/innovation/pool/de/forschungsfelder/siemens_vulnerability_handling.pdf

脆弱性取扱ポリシーの内容（例）

- 望ましい連絡方法
- 予想されるやりとり
- 脆弱性の届出フォーム
- 脆弱性以外のセキュリティ問題に関する連絡先
- 届出の取扱状況に関する確認方法

脆弱性取扱プロセスの整備

- 脆弱性取扱プロセスとは
- 脆弱性取扱ポリシーに基づく、社内の脆弱性取扱の手順
- 社内の関係部門がプロセスのフレームワークを構成

- 脆弱性取扱プロセスの要件
- 脆弱性取扱に係る関係部門のミッションと権限を定める
- 脆弱性取扱の手順を定める
  - ✓ 入手した脆弱性の検証・フィードバック
  - ✓ 脆弱性対策のための計画の策定と実施
  - ✓ 脆弱性関連情報（対策、回避策等）の顧客への連絡・公表

関係部門①

- 設計部門・製品主管部門
  - 製品設計を担う立場であり、脆弱性の原因分析や対策策定において主導的役割を担う
- 研究開発部門
  - 研究開発部門が製品の脆弱性テストを担当する場合がある
- 品質管理部門・品質保証部門
  - 製品の品質保証の立場から、脆弱性やその対策について把握する
  - パッチの最終的な品質検証を担当する
  - 脆弱性をバグの一部として取り扱う場合、脆弱性対策は品質管理部門・品質保証部門が主導する形になる
- SI部門
  - 顧客のシステムを組み上げ、運用する立場であり、主に対策を適用する立場から関与する

関係部門②

- カスタマケア部門
  - SI部門と連携して、脆弱性対策の実施について通知すべき顧客のリストアップや調整を担当する
- 営業部門
  - SI部門と連携して、脆弱性対策の実施について通知すべき顧客のリストアップや調整を担当する
- リスク管理統制部門・法務部門
  - 組織のリスク管理の一環として、脆弱性やその対策について把握する
  - 法務部門は、製品の瑕疵や保守の範囲を規定する
- 広報部門
  - 脆弱性の公表に関し、内容等の調整を担当する
  - たとえば、自社発表やJVN公表の内容について調整する

脆弱性ハンドリングのフローについて

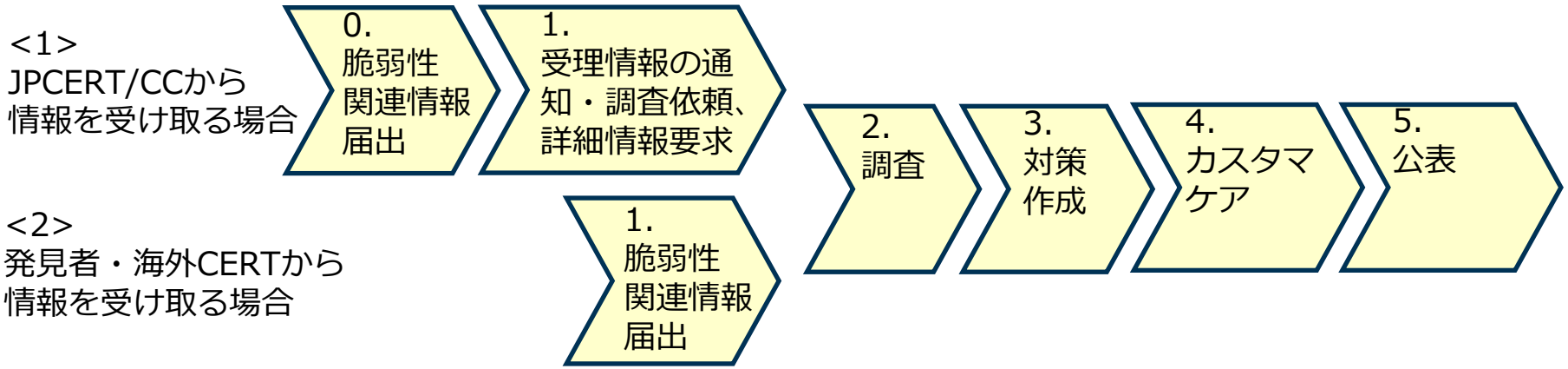
- 以降、社内における脆弱性ハンドリングの流れ（フロー）について解説する
- フローは、次の２つのケースに分けて示している

  <ケース1>

  POCが脆弱性関連情報をJPCERT/CCから受け取る場合

  <ケース2>

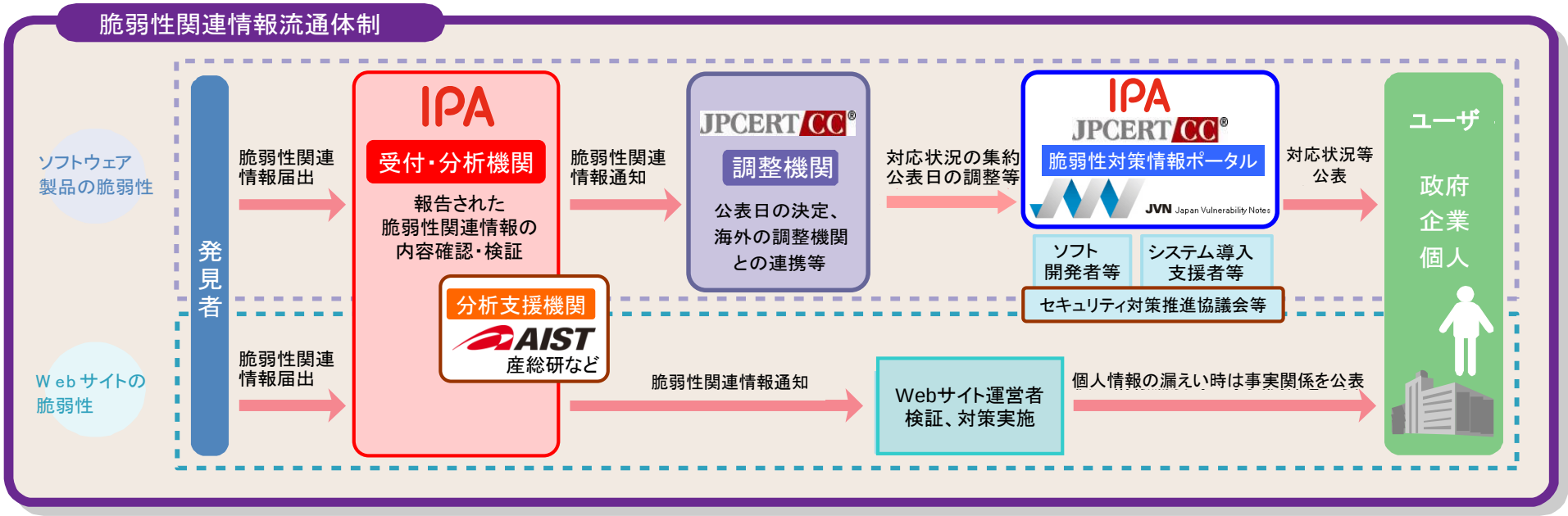
  POCが脆弱性関連情報を発見者・海外CERTから直接受け取る場合



脆弱性関連情報の届出から公表に至るまでの間、対応状況について、発見者と定期的なコミュニケーションを図り、脆弱性を放置していると誤解され、意図しない公表に繋がらないようにする

（再掲）情報セキュリティ早期警戒パートナーシップ

- ソフトウェア等の製品やウェブサイトで発見された脆弱性関連情報を受け付け、製品ベンダやサイト運営者に対策を促し、周知する枠組み
- 「ソフトウエア等脆弱性関連情報取扱基準」に基づく官民の連携体制として整備され、2004年7月8日に運用を開始
- 発見されたソフトウェア等の製品に対する脆弱性関連情報は、IPAが受け付け、JPCERT/CCが影響を受けるソフトウェア等の製品を特定し、製品開発者へ内容を通知し、脆弱性への対応を協議・調整する
- JVNは、対応された脆弱性の詳細と製品開発者の対応状況を公表し、利用者へ対策を周知

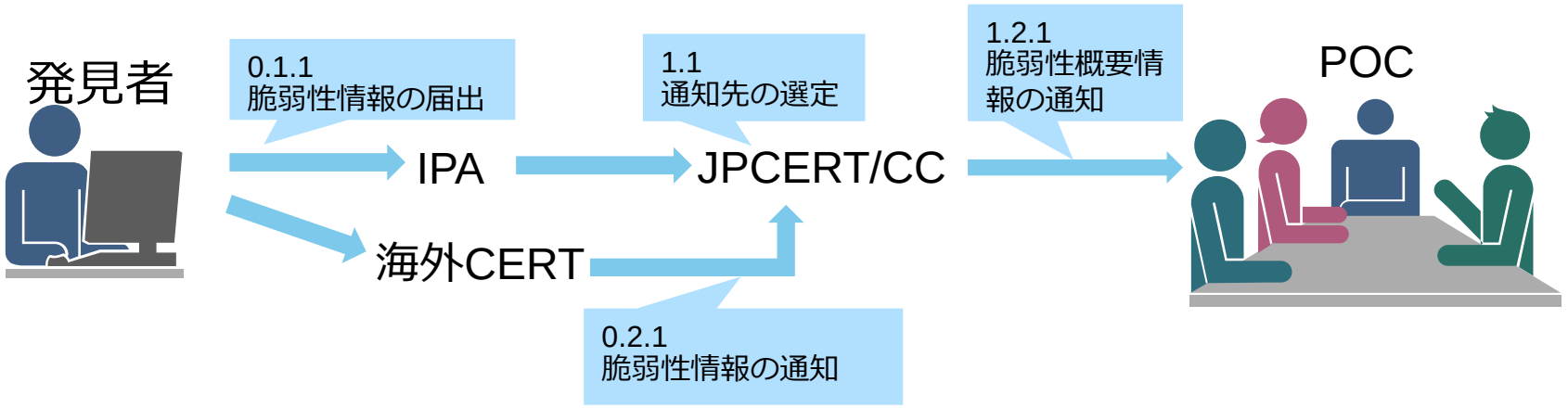


https://www.ipa.go.jp/security/vuln/index.html#section10

仮想企業A社における脆弱性関連情報の対応事例

0. 脆弱性関連情報届出
1. 受理情報の通知・調査依頼、詳細情報要求
2. 調査
3. 対策作成
4. カスタマケア
5. 公表

社内フロー図 <1>JPCERT/CC→POC
0. 脆弱性関連情報届出 ～ 1.受理情報の通知



0.1 情報届出（ケース1：発見者からIPAに届け出）

0.1.1 脆弱性情報の届出

発見者からIPAに届けられた脆弱性関連情報は、IPAで確認の上、JPCERT/CCに通知される。

0.2 情報通知（ケース2：海外CERTからJPCERT/CCに通知）

0.2.1 脆弱性情報の通知

発見者から海外CERTに届けられた脆弱性関連情報が、海外CERTからJPCERT/CCに通知される。

1.1 通知先の選定

JPCERT/CCは、当該脆弱性関連情報に関係する製品ベンダを特定する。

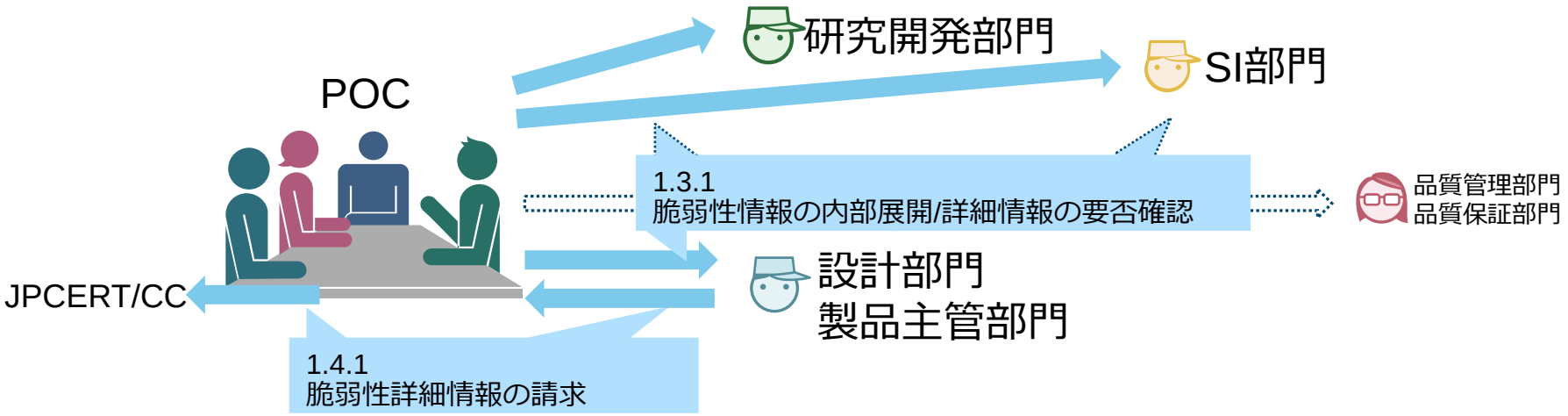
1.2 通知・調査依頼

1.2.1 脆弱性概要情報の通知

JPCERT/CCは、特定した製品ベンダのPOCに脆弱性概要情報を通知する。

※JPCERT/CCが製品ベンダへ脆弱性概要情報を通知した日を起算日とし、起算日から1年経過した時点で、発見者は情報非開示依頼（IPA・JPCERT/CCが脆弱性情報を公表するまでの間、脆弱性関連情報が第三者に漏れないよう、発見者に対する情報非開示依頼）の取り下げを求めることができる。

社内フロー図 <1>JPCERT/CC→POC
1. 受理情報の通知・調査依頼、詳細情報要求①



1.3 確認

1.3.1 脆弱性概要情報の内部展開/詳細情報の要否確認

POCは、受け取った脆弱性概要情報に関係する設計部門・製品主管部門や研究開発部門、SI部門を特定し、情報を展開する。また、社内のポリシーに則って、必要であれば品質管理部門・品質保証部門にも脆弱性関連情報を受け取ったことを報告する。

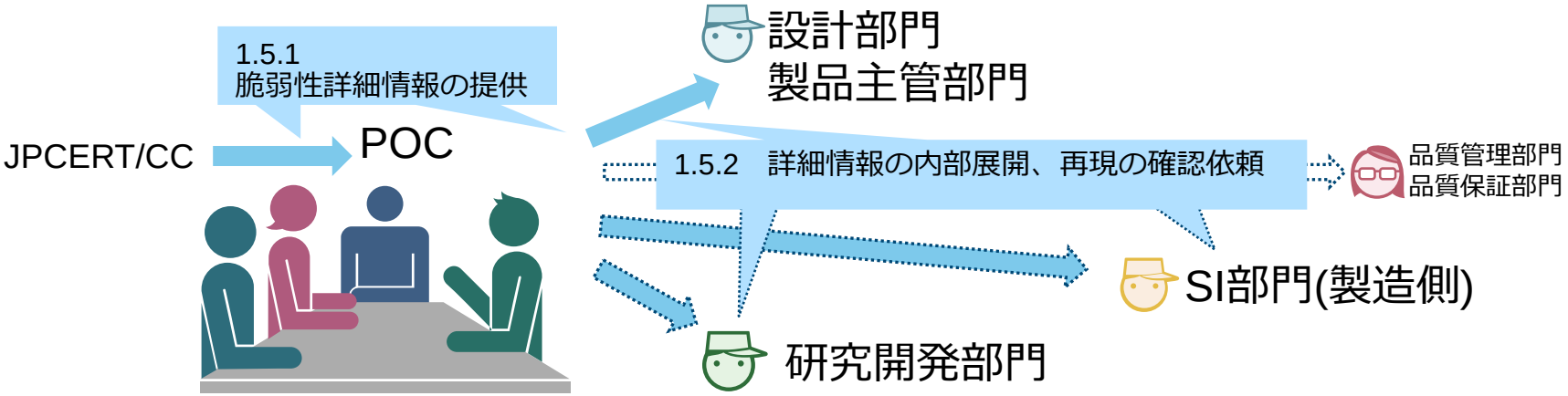
POCから通知を受けた部門（主に設計部門・製品主管部門）は、脆弱性概要情報をもとに詳細情報の要・不要を判断し、POCにその旨を伝える。その際、詳細情報をやりとりした場合には、その後の対応や公表についてJPCERT/CCに報告・調整する義務が生じることを踏まえて判断すること。

1.4 詳細情報請求

1.4.1 脆弱性詳細情報の請求

POCは、設計部門・製品主管部門から詳細情報を必要とする連絡を受けたら、JPCERT/CCへ脆弱性詳細情報の請求を行う。

社内フロー図 <1>JPCERT/CC→POC
1. 受理情報の通知・調査依頼、詳細情報要求②



1.5 詳細情報の受理

1.5.1 脆弱性詳細情報の提供

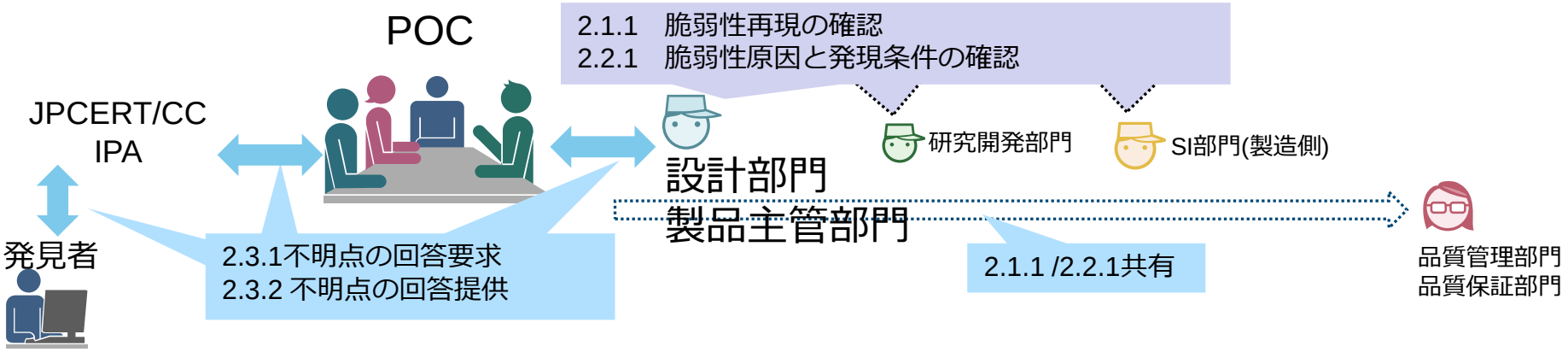
JPCERT/CCからPOCへ脆弱性詳細情報が提供される。

1.5.2 脆弱性詳細情報の内部展開・再現の確認・共有

POCは、脆弱性詳細情報を設計部門・製品主管部門へ提供し、脆弱性が再現できるか確認するよう依頼する。

また、必要であれば、研究開発部門やSI部門、品質管理部門・品質保証部門にも同様の情報を展開する。

社内フロー図 <1>JPCERT/CC→POC
2. 調査①



2.1 脆弱性再現の確認

2.1.1 脆弱性再現の確認・共有

設計部門・製品主管部門は、脆弱性詳細情報に基づき脆弱性の再現を確認する。本作業は、研究開発部門やSI部門と共同で行う場合もある。また、必要に応じて、その結果を品質管理部門・品質保証部門と共有する。

2.2 脆弱性の原因と発現条件の特定

2.2.1 脆弱性原因と発現条件の確認・共有

脆弱性が再現できた場合、設計部門・製品主管部門は脆弱性の原因と発現条件を確認する。本作業は、研究開発部門やSI部門と共同で行う場合もある。また、必要に応じて、その結果を品質管理部門・品質保証部門と共有する。

2.3 不明点を発見者に確認

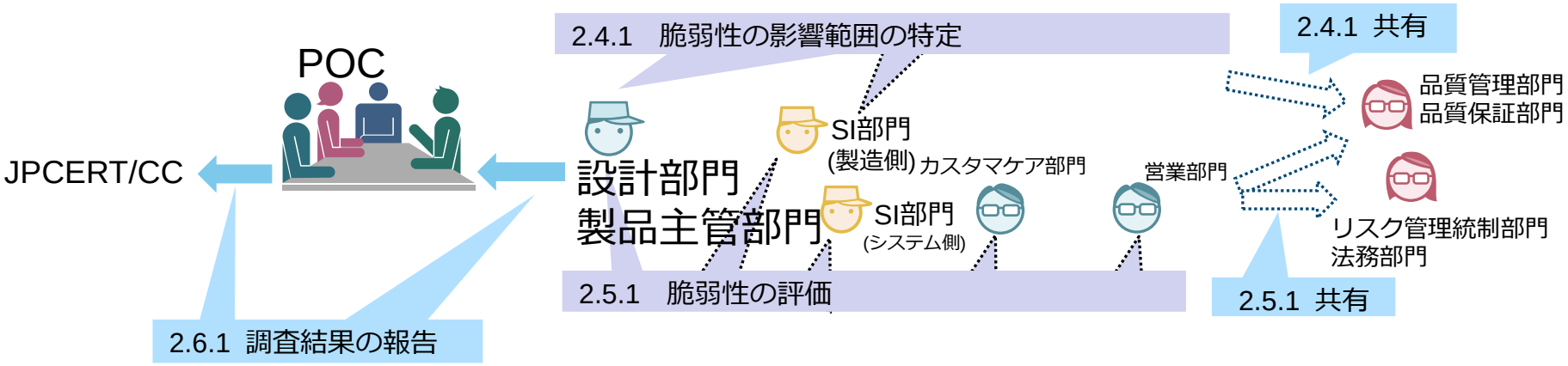
2.3.1 不明点の回答要求

設計部門・製品主管部門は、脆弱性の再現や原因、発現条件の確認に際し、必要に応じて、自社のPOC、JPCERT/CC・IPAを介して発見者へ不明点を確認することができる。

2.3.2 不明点の回答提供

IPA・JPCERT/CCは、発見者から不明点の回答を得たら、その情報をPOCへ提供する。POCは、受け取った情報を設計部門・製品主管部門へ提供する。

社内フロー図 <1>JPCERT/CC→POC
2. 調査②



2.4 対象となる自社製品の範囲の特定

2.4.1 脆弱性の影響範囲の特定・共有

設計部門・製品主管部門は、脆弱性の影響範囲を特定する。本作業は、SI部門と共同で行う場合もある。また、必要に応じて、その結果を品質管理部門・品質保証部門と共有する。

2.5 脆弱性の評価

2.5.1 脆弱性の評価・共有

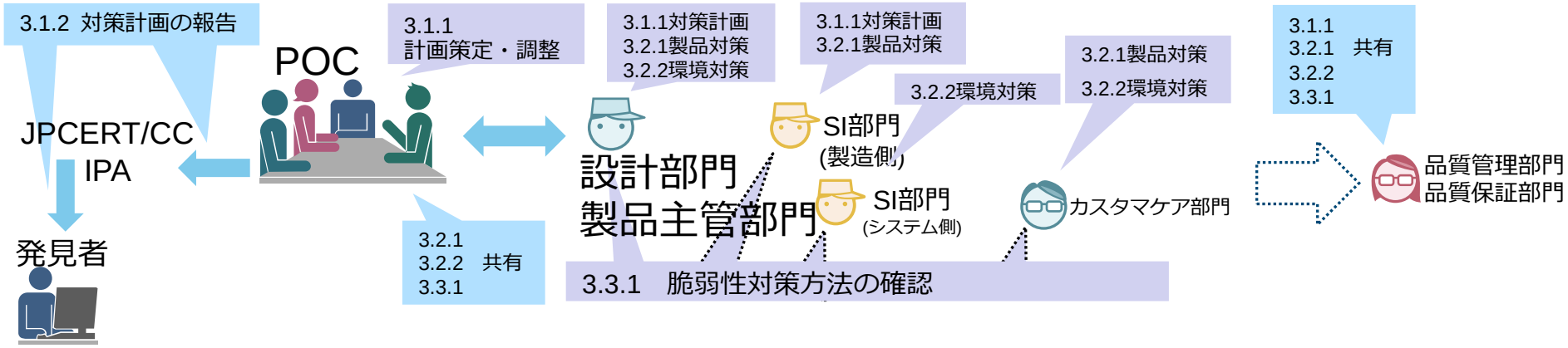
設計部門・製品主管部門は、発現条件、影響度、対策策定の難易度の観点から脆弱性を評価する。本作業は、SI部門、カスタマケア部門、営業部門と共同で行う場合もある。また、必要に応じて、その結果を品質管理部門・品質保証部門、リスク管理統制部門・法務部門と共有する。

2.6 脆弱性調査結果

2.6.1 脆弱性調査結果の報告

POCは、社内で調査した内容（再現結果、原因、評価、対応時期等）をJPCERT/CCへ報告する。

社内フロー図 <1>JPCERT/CC→POC
3. 対策作成



3.1 計画の策定・調整

3.1.1 脆弱性対策計画の策定・調整

POC、設計部門・製品主管部門、SI部門が中心となって脆弱性対策計画を策定する。また、POCは、本計画についてJPCERT/CCと調整する。さらに、必要に応じて、その計画を品質管理部門・品質保証部門と共有する。

3.1.2脆弱性対策計画の報告

IPAは、発見者から問い合わせを受けた場合、JPCERT/CCから得た情報に基づき、製品ベンダの取組方針について発見者へ報告する。

3.2 対策方法の検討

3.2.1 製品における脆弱性対策方法の検討

設計部門・製品主管部門、SI部門、カスタマケア部門が中心となり、製品における脆弱性対策方法を検討する。また、必要に応じて、その結果をPOC、品質管理部門・品質保証部門と共有する。

3.2.2 システム・環境における脆弱性対策方法の検討

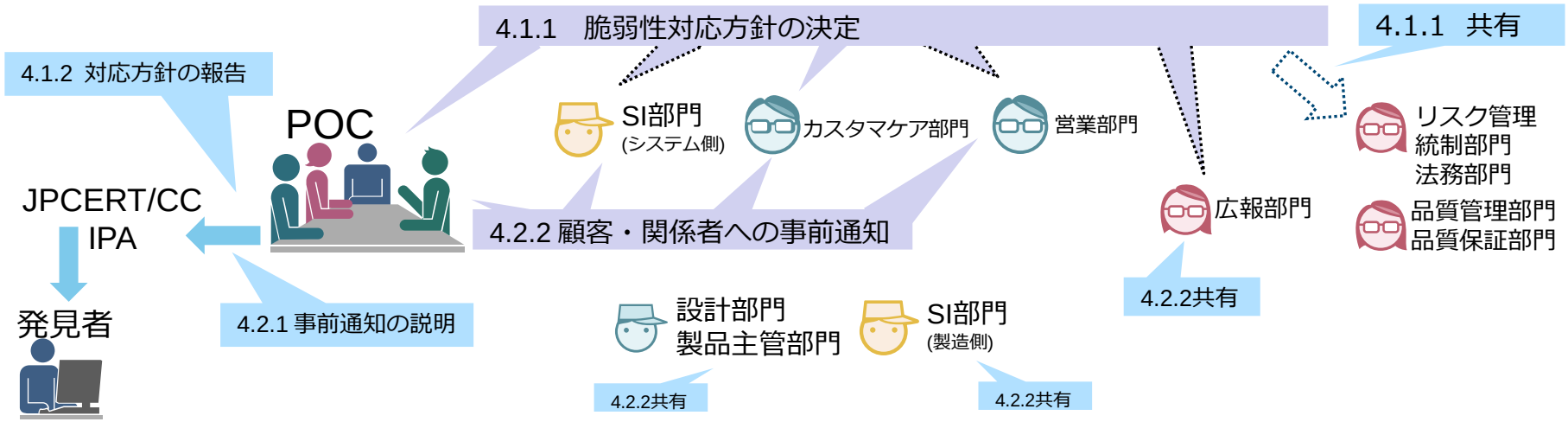
設計部門・製品主管部門、SI部門、カスタマケア部門が中心となり、システムや利用環境における脆弱性対策方法の検討を行う。また、必要に応じて、その結果をPOC、品質管理部門・品質保証部門と共有する。

3.3 対策方法の確認

3.3.1 脆弱性対策方法の確認

設計部門・製品主管部門は、3.2で検討された脆弱性対策方法に問題がないか確認する。本作業は、SI部門、カスタマケア部門と共同で行う場合もある。また、必要に応じて、その結果をPOC、品質管理部門・品質保証部門と共有する。

社内フロー図 <1>JPCERT/CC→POC
4. カスタマケア（ケース1：顧客が不特定多数）



4.1 対応方針決定

4.1.1 脆弱性対応方針の決定

POCは、カスタマケア部門とともに、顧客の状況に応じて脆弱性対応方針（どのように対策を適用するか、どのように対策を展開するか(公表の判断等)）を決定する。本作業は、SI部門、営業部門、広報部門と共同で行う場合もある。公表については、自ら公表しない場合に発見者から公表されるリスクと、自ら公表する場合の対応の負担増を勘案する必要がある。また、必要に応じて、その結果を品質管理部門・品質保証部門、リスク管理統制部門・法務部門と共有する。

4.1.2対応方針の報告

POCは、JPCERT/CCへ脆弱性対応方針を報告する。

4.2 顧客・関係者への事前通知（ケース1：顧客が不特定多数の場合）

製品ベンダは、JPCERT/CCと調整した上で、顧客やSI事業者との秘密保持契約を前提に、JVN公表前の通知を行うことができる。
※重要インフラ等に対し特に影響が大きいと推察される場合、JPCERT/CCは製品ベンダと協議の上、脆弱性情報の一般公表より前に、脆弱性情報と対策方法を、政府・行政機関や重要インフラ事業者等に対して優先的に提供する場合がある。

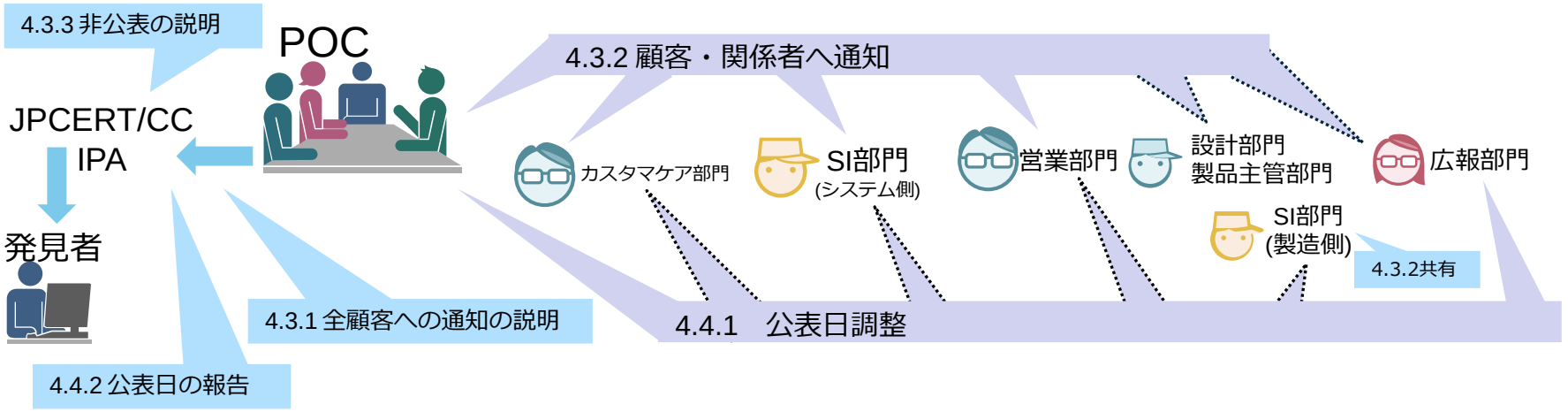
4.2.1 顧客への事前通知の説明

POCは、JPCERT/CCに対し、顧客への事前通知を行う意向を説明する。

4.2.2 顧客・関係者への事前通知

POCは、JPCERT/CCの了解を得た上で（4.2.1）、SI部門、カスタマケア部門、営業部門ともに、保守契約等を通じて連絡が可能な顧客やSI事業者へ事前通知を行う。事前通知は相手との秘密保持契約が前提となる。また、トラブル対処の可能性を踏まえ、必要に応じて、広報部門、設計部門・製品主管部門、SI部門と情報を共有する。

社内フロー図 <1>JPCERT/CC→POC
4. カスタマケア（ケース2：全顧客を把握）



4.3 顧客・関係者への通知（ケース2：全顧客を把握している場合）

製品ベンダがすべての顧客に通知する場合、JPCERT/CCと調整した上で、当該脆弱性情報をJVNの公表対象から外すことができる。

4.3.1 全顧客への通知の説明

POCは、該当製品のすべての顧客（SI事業者経由を含む）への通知が可能であり、公表が不要である旨をJPCERT/CCに説明し、合意を得る。

4.3.2 顧客・関係者への通知

POC、SI部門、カスタマケア部門、営業部門が中心となって、該当製品を利用しているすべての顧客（SI事業者経由を含む）へ脆弱性とその対策方法の通知を行う。また、トラブル対処の可能性を踏まえ、必要に応じて、広報部門、設計部門・製品主管部門、SI部門と情報を共有する。

4.3.3 非公開の説明

JPCERT/CCからの連絡を受け、 IPAは当該脆弱性関連情報の取扱いを終了する旨を発見者へ説明する。

4.4 公表日調整

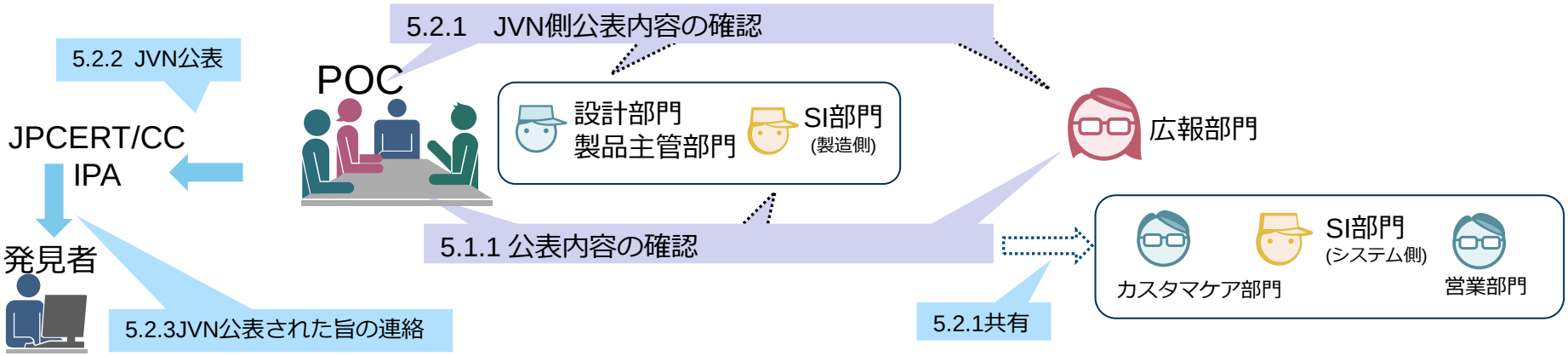
4.4.1 公表日調整

POC、広報部門が中心となって、公表日について社内をとりまとめるとともに、JPCERT/CCと調整する。本作業は、設計部門・製品主管部門、SI部門、カスタマケア部門と共同で行う場合もある。また、必要に応じて、その結果をSI部門と共有する。

4.4.2 公表日の報告

POCは、JPCERT/CCに対し、公表日を報告する。

社内フロー図 <1>JPCERT/CC→POC
5. 公表



5.1 企業側公表

5.1.1公表内容の確認・公表

POCと広報部門は、自社発表を行う内容を確認し、公表する。本作業は、設計部門・製品主管部門、SI部門と共同で行う場合もある。また、必要に応じて、顧客と接するSI部門、カスタマケア部門、営業部門と情報を共有する。

5.2 JVN側公表

5.2.1 JVN側公表内容の確認

POCは、JVNの公表内容を確認し、JPCERT/CCと調整する。本作業は、広報部門、設計部門・製品主管部門、製造部門、SI部門と共同で行う場合もある。

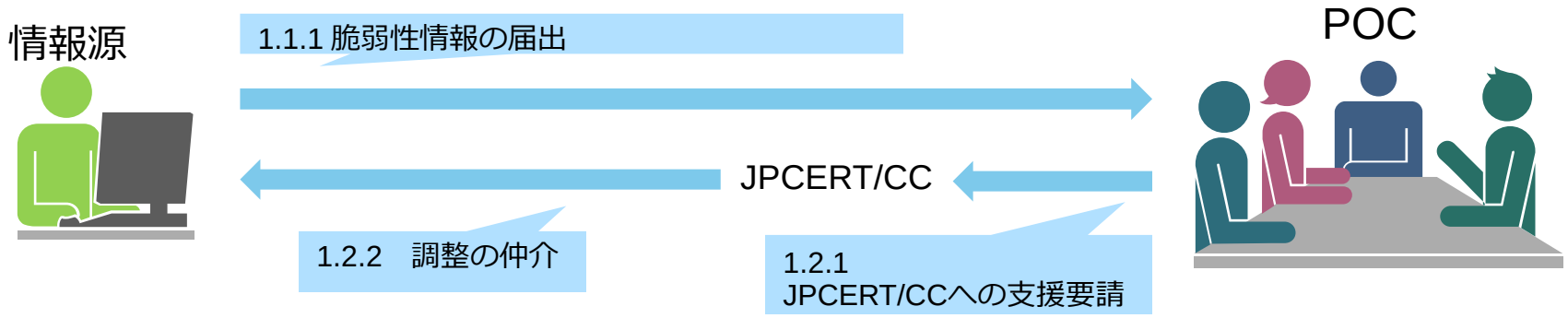
5.2.2 JVN公表

JPCERT/CCは、POCと合意が得られた内容をJVN上で公表する。

5.2.3 JVN公表された旨の連絡

IPAは、届け出られた脆弱性情報がJVN公表された旨を発見者へ連絡する。

社内フロー図 <2>情報源（発見者・海外CERT）→POC
1. 受理情報の通知（JPCERT/CCに支援を要請する場合）



1.1情報届出

1.1.1　脆弱性情報の届出

発見者、もしくは海外CERTから脆弱性情報がPOCへ直接通知される。

1.2 JPCERT/CCへの連絡

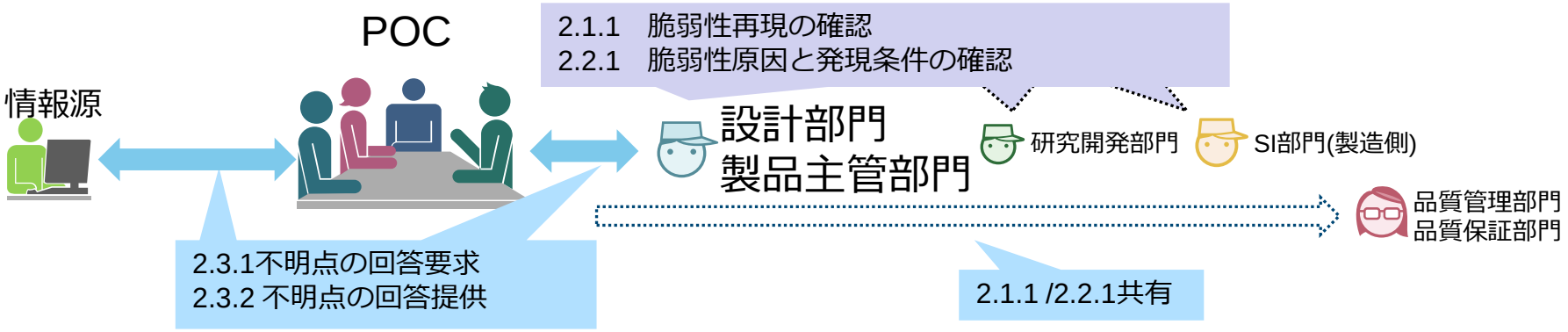
1.2.1 JPCERT/CCへの支援要請

届け出られた脆弱性情報について情報源（発見者や海外CERT）と調整する際に、JPCERT/CCの仲介が必要であると社内で判断した場合、JPCERT/CCへ支援を要請する。

1.2.2 調整の仲介

支援要請を受けたJPCERT/CCは情報源（発見者や海外CERT）が仲介を認めた場合、情報源との窓口となる。情報源がJPCERT/CCの仲介を認めない場合はPOCの後方支援に回る。

社内フロー図 <2>情報源（発見者・海外CERT）→POC
2. 調査①（JPCERT/CCに支援を要請しない場合）



2.1 脆弱性再現の確認

2.1.1 脆弱性再現の確認・共有

情報源から通知された脆弱性情報をもとに、設計部門・製品主管部門は脆弱性の再現を確認する。本作業は、研究開発部門やSI部門と共同で行う場合もある。また、必要に応じて、その結果を品質管理部門・品質保証部門と共有する。

2.2 脆弱性の原因と発現条件の特定

2.2.1 脆弱性原因と発現条件の確認・共有

脆弱性が再現できた場合、設計部門・製品主管部門は脆弱性の原因と発現条件を確認する。本作業は、研究開発部門やSI部門と共同で行う場合もある。また、必要に応じて、その結果を品質管理部門・品質保証部門と共有する。

2.3 不明点を発見者に確認

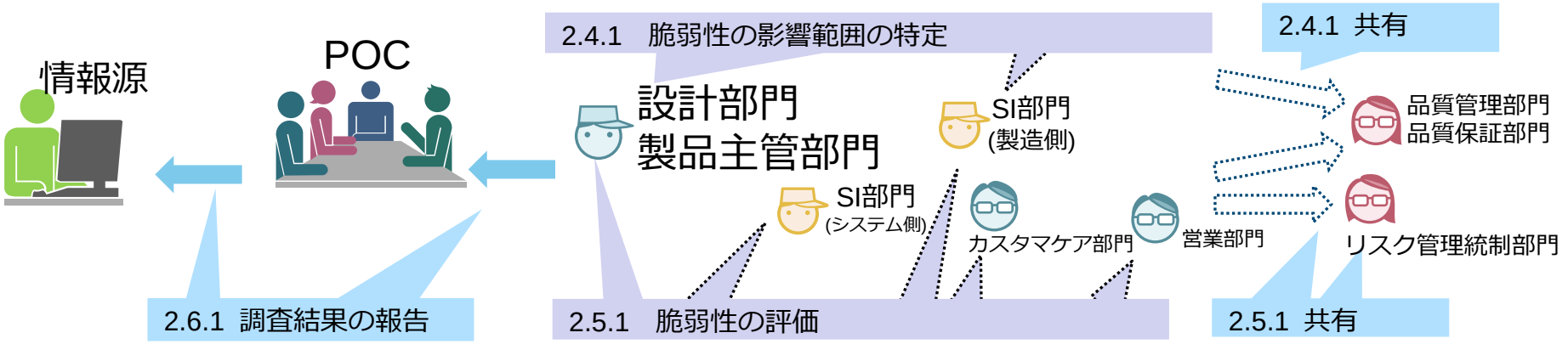
2.3.1 不明点の回答要求

設計部門・製品主管部門は、脆弱性の再現や原因、発現条件の確認に際し、必要に応じて、POCを通じて情報源へ不明点を確認する。

2.3.2 不明点の回答提供

POCは、発見者から不明点の回答を得たら、その情報を設計部門・製品主管部門へ提供する。

社内フロー図 <2>情報源（発見者・海外CERT）→POC
2. 調査②



2.4 対象となる自社製品の範囲の特定

2.4.1 脆弱性の影響範囲の特定・共有

設計部門・製品主管部門は、脆弱性の影響範囲を特定する。本作業は、SI部門と共同で行う場合もある。また、必要に応じて、その結果を品質管理部門・品質保証部門と共有する。

2.5 脆弱性の評価

2.5.1 脆弱性の評価・共有

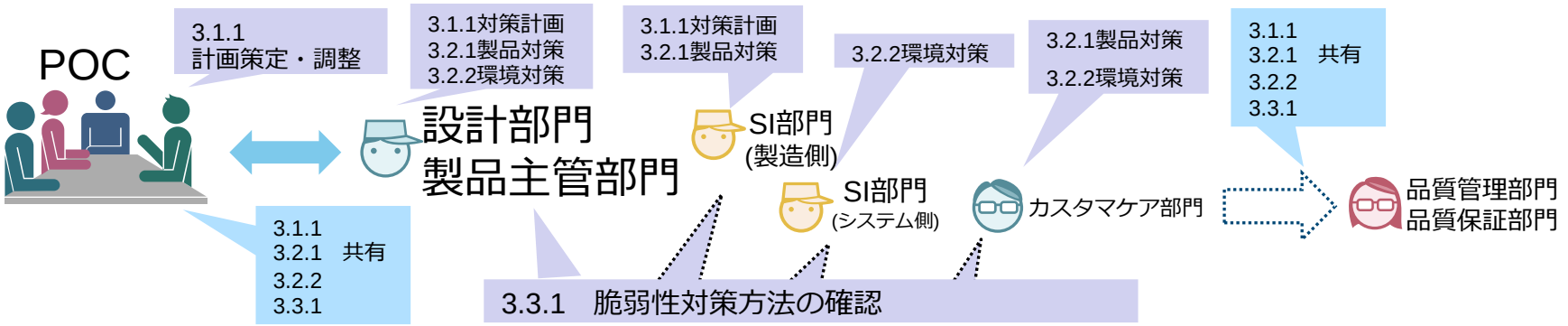
設計部門・製品主管部門は、発現条件、影響度、対策策定の難易度の観点から脆弱性を評価する。本作業は、SI部門、カスタマケア部門、営業部門と共同で行う場合もある。また、必要に応じて、その結果を品質管理部門・品質保証部門、リスク管理統制部門・法務部門と共有する。

2.6 調査結果報告

2.6.1 調査結果の報告

POCは、社内で調査した内容（再現結果、原因、評価、対応時期等）について、問い合わせを受けた場合は情報源へ報告する。

社内フロー図 <2>情報源（発見者・海外CERT）→POC
3. 対策作成



3.1 計画の策定・調整

3.1.1 脆弱性対策計画の策定・調整

設計部門・製品主管部門、SI部門が中心となり、脆弱性対策計画を策定する。必要に応じて、その計画をPOCや品質管理部門・品質保証部門と共有する。

3.2 対策方法の検討

3.2.1 製品における脆弱性対策方法の検討

設計部門・製品主管部門、SI部門、カスタマケア部門が中心となり、製品における脆弱性対策方法を検討する。また、必要に応じて、その結果をPOC、品質管理部門・品質保証部門と共有する。

3.2.2 システム・環境における脆弱性対策方法の検討

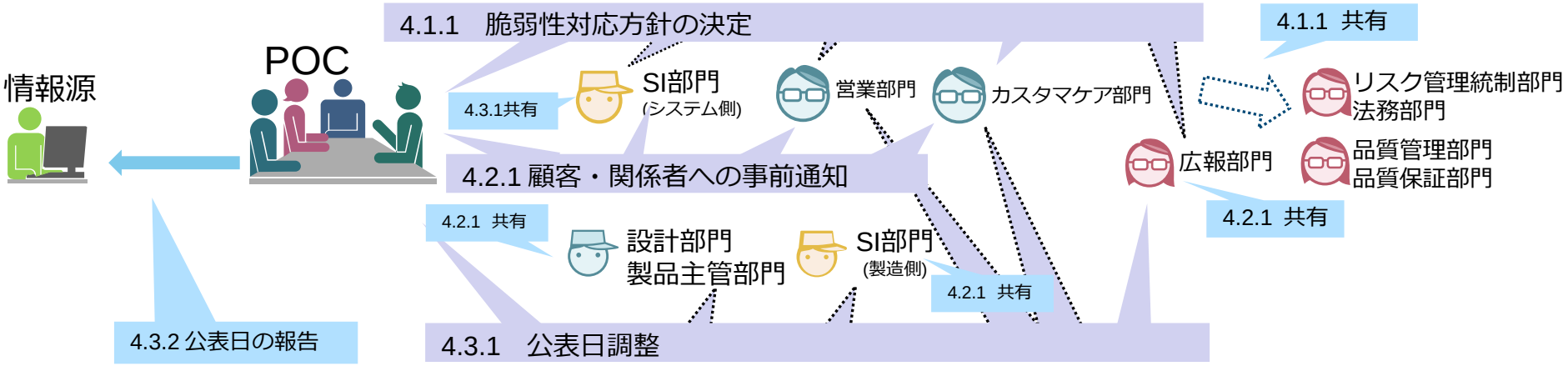
設計部門・製品主管部門、SI部門、カスタマケア部門が中心となり、システムや利用環境における脆弱性対策方法の検討を行う。また、必要に応じて、その結果をPOC、品質管理部門・品質保証部門と共有する。

3.3 対策方法の確認

3.3.1 脆弱性対策方法の確認

設計部門・製品主管部門は、3.2で検討された脆弱性対策方法に問題がないか確認する。本作業は、SI部門、カスタマケア部門と共同で行う場合もある。また、必要に応じて、その結果をPOC、品質管理部門・品質保証部門と共有する。

社内フロー図 <2>情報源（発見者・海外CERT）→POC
4. カスタマケア



4.1 対応方針決定

4.1.1 脆弱性対応方針の決定

POCは、カスタマケア部門とともに、顧客の状況に応じて脆弱性対応方針（どのように対策を適用するか、どのように対策を展開するか(公表の判断等)）を決定する。本作業は、SI部門、営業部門、広報部門と共同で行う場合もある。公表については、自ら公表しない場合に発見者から公表されるリスクと、自ら公表する場合の対応の負担増を勘案する必要がある。また、必要に応じて、その結果を品質管理部門・品質保証部門、リスク管理統制部門・法務部門と共有する。

4.2 顧客・関係者への事前通知

4.2.1 顧客・関係者への事前通知

POCは、 SI部門、カスタマケア部門、営業部門ともに、保守契約等を通じて連絡が可能な顧客やSI事業者へ事前通知を行う。また、トラブル対処の可能性を踏まえ、必要に応じて、広報部門、設計部門・製品主管部門、SI部門と情報を共有する。

4.3 公表日調整

※発見者の意向や海外CERTのポリシー等により、公表日の調整が必ずしも製品ベンダ主導で出来ない場合もある。

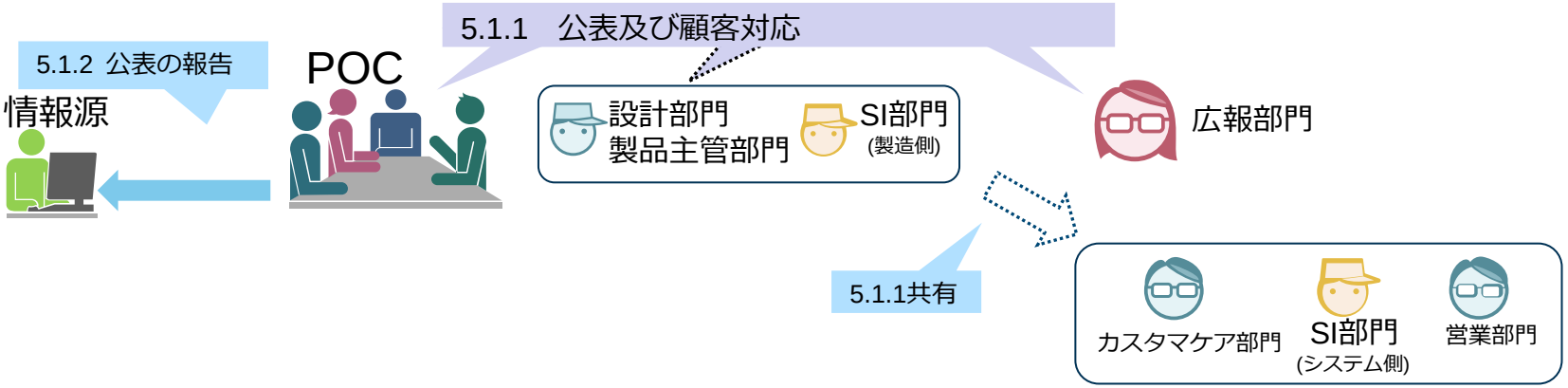
4.3.1 公表日調整

POC、広報部門が中心となって、公表日について社内をとりまとめる。本作業は、設計部門・製品主管部門、SI部門、カスタマケア部門と共同で行う場合もある。また、必要に応じて、その結果をSI部門と共有する。

4.3.2 公表日の報告

POCは、情報源から問い合わせを受けた場合、公表日について情報源へ報告する。

社内フロー図 <2>情報源（発見者・海外CERT）→POC
5. 公表



5.1 企業側公表

5.1.1公表及び顧客対応

POCと広報部門は、自社発表を行う内容を確認し、公表する。本作業は、設計部門・製品主管部門、SI部門と共同で行う場合もある。また、必要に応じて、顧客と接するSI部門、カスタマケア部門、営業部門と情報を共有する。

※JVN公表を希望する場合、IPAへ脆弱性情報を届出る。＜1＞0.1.1のフローへ移る。

5.1.2公表の報告

POCは、届出られた脆弱性情報を公表した旨を情報源へ連絡する。

参考資料

- 日立グループにおける製品脆弱性情報の開示プロセス
  http://www.hitachi.co.jp/hirt/publications/hirt-pub10008/index.html
- Siemens Vulnerability Handling Version 1.3, 2014-05-07
  https://www.siemens.com/innovation/pool/de/forschungsfelder/siemens_vulnerability_handling.pdf
- 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.ipa.go.jp/security/ciadr/partnership_guide.html
- 製品開発者登録(JPCERT/CC)
  https://www.jpcert.or.jp/vh/regist.html
- JPCERT/CC 脆弱性関連情報取扱いガイドライン
  https://www.jpcert.or.jp/vh/vul-guideline2014.pdf
- 製品開発ベンダーにおける脆弱性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（JEITA・JISAガイドライン）
  http://it.jeita.or.jp/infosys/info/0407JEITA-guideline/index.html
- ISO/IEC 29147: 2014 “Vulnerability disclosure”
- ISO/IEC 30111: 2013 “Vulnerability handling processes”
  ※一般財団法人日本規格協会（JSA）「JSA Web Store」にて、JISやISOなどの規格の購入が可能
  http://www.jsa.or.jp/