資料2-2

xSIRTの概況について

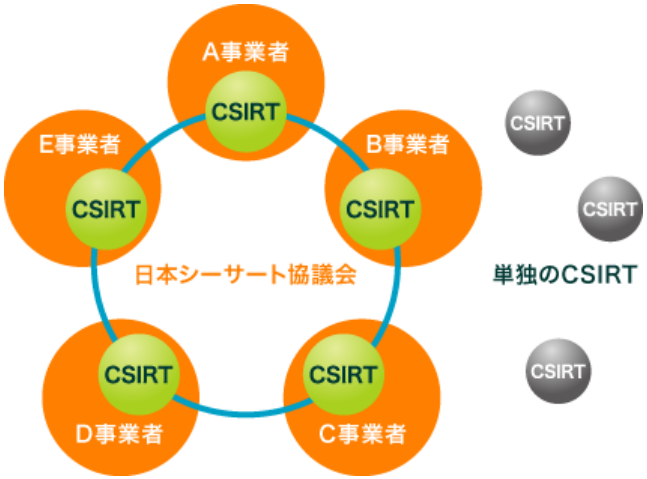
令和2年７月

内閣サイバーセキュリティセンター（ NISC ）
基本戦略第1グループ

CSIRTについて

- CSIRT（シーサート）とは（日本シーサート協議会ホームページより引用）
  - CSIRT（Computer Security Incident Response Team）とは、**コンピュータセキュリティにかかるインシデントに対処するための組織の総称**です。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をします。

- 日本シーサート協議会（NCA）
  - 同じような状況や課題を持つCSIRT同士による緊密な連携を目的に設立
  - 日本シーサート協議会
    - ✓ 名称：日本コンピュータセキュリティインシデント対応チーム協議会
    - ✓ 略称：日本シーサート協議会（NCA）
    - ✓ 設立年月日：2007年３月28日
    - ✓ 会員数：394チーム（2020年５月１日時点）
    - ✓ ホームページURL：　https://www.nca.gr.jp/



（出典）日本シーサート協議会とは
日本シーサート協議会、ホームページ（https://www.nca.gr.jp/outline/index.html）より

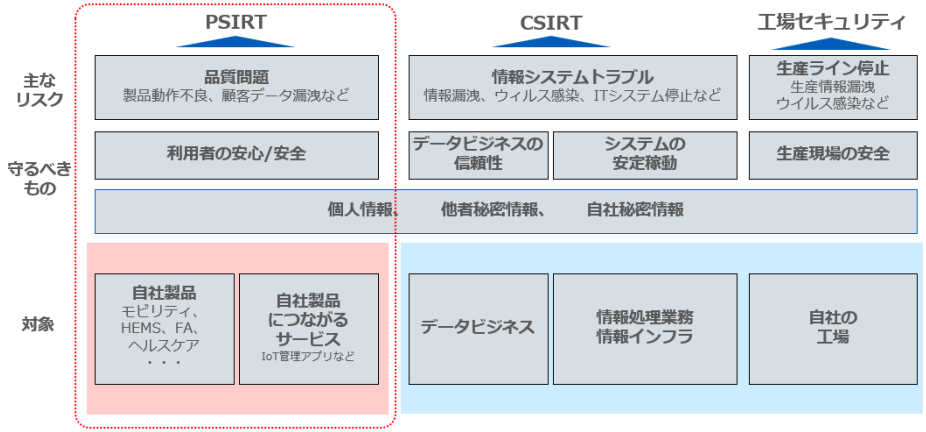
xSIRTについて

- CSIRTは、通常、企業等において自社の情報やシステムを守る組織と理解されることが多いが、2019年のシンクタンク＊の整理によれば、 セキュリティ組織であるxSIRTは、CSIRTだけでなく守るべき対象に応じて、**自社製品を対象とするPSIRT (Product SIRT)**、**工場・生産ラインを対象とするFSIRT (Factory SIRT)**、**自社サービスを対象とするDSIRT/SSIRT (Digital Service SIRT)**等の種類があるとされる。

（＊：ＮＲＩセキュアテクノロジーズ株式会社）

xSIRT	設置部署	対象	守るべきもの	活動
CSIRT	ガバナンス部門・IT部門	全般	自社で取り扱う機密情報・個人情報	セキュリティ活動全般 各xSIRT活動の支援 組織間のハブ・ファシリテータ
PSIRT	製品開発・品質保証部門	製品	自社製品を利用する顧客の安全・機密情報	製品開発ライフサイクルにおける脆弱性リスクマネジメント
FSIRT	生産管理部門	工場・生産ライン	生産ラインの安定稼動	サイバー攻撃からの工場設備の保護活動
DSIRT /SSIRT	サービス開発・品質保証部門	サービス	自社サービスを利用する顧客の安全・機密情報 自社サービスの継続的な提供	サービス開発ライフサイクルにおけるリスクマネジメント

（出典）「【次世代セキュリティ組織】CSIRTと協調する新たなセキュリティ組織xSIRTとは」（2019年7月9日）
ＮＲＩセキュアテクノロジーズ株式会社



（出典）ＮＲＩセキュアテクノロジーズ株式会社、
ホームページ（ https://www.nri-secure.co.jp/service/consulting/psirt）より

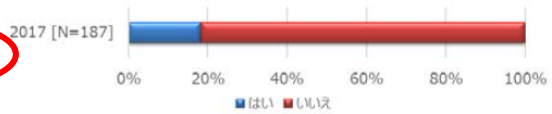
PSIRTの設置状況

- 日本シーサート協議会の2017年のアンケートによれば、**PSIRT機能**を有していると回答した組織は**18%程度（34組織）**
- PSIRT機能を有している組織のうち、半数程度は CSIRT に PSIRT の機能を持たせており、CSIRT から独立した部署として PSIRT が存在する組織は 30%程度（全体の6%弱）

日本シーサート協議会（NCA）加盟組織（262組織：2017年10月30日時点）に対し
JPCERT/CCがアンケートを実施（2017年10月～11月）、187組織から得た回答を集計

2.3. 自社で製造・出荷している製品の脆弱性を取り扱う PSIRT(Product Security Incident Response Team)機能を有しているか

#	項目	回答数
a	はい	34
b	いいえ	153



（複数回答なし 2017 [N = 187]）

2.5. PSIRT の位置付け

#	項目	回答数
a	CSIRT は、組織 CSIRT、PSIRT などを包含している	18
b	CSIRT は、PSIRT 機能のみを有する	0
c	CSIRT と PSIRT は、それぞれが独立した部署が存在しており、連携している	11
d	その他	5

（複数回答なし 2017 [N = 34]）

（出典）「2017年度CSIRT構築および運用における実態調査」（2018年12月18日）
JPCERT C／C、https://www.jpcert.or.jp/research/20181218_CSIRT-survey2017.pdf

xSIRTの設置状況

- x SIRTを設置している組織の概況は以下のとおり。必ずしも多くない状況。

日本シーサート協議会	名称	組織名	設置の有無				備考
			CSIRT	PSIRT	FSIRT	DSIRT/SSIRT	
初期会員	HIRT	株式会社日立製作所	○（1998年4月1日）	○（2002年）	○	○	製品ベンダ IRT の立上げ（2002 年 ～）：製品開発部門を中心に、社内セキュリティ有識者、社内インフラ提供部門、製品開発部門、品質保証部門等と共に、日立版 CSIRT としての本格活動に向け、関連事業所との体制整備を開始しました。
初期会員	IIJ-SECT	株式会社 インターネットイニシアティブ	○（2001年5月16日）	－	－	－	IIJ-SECT は、1997 年に開始された IIJ のセキュリティを向上するための社内活動の延長として、特に IIJ の設備や顧客が巻き込まれた事件に対応するための組織として、2001 年に結成されました。
初期会員	JPCERT/CC	一般社団法人JPCERTコーディネーションセンター	○（1996年10月1日）	－	－	－	活動は、1992 年ころに始まった、ボランティアによるインシデントの報告対応業務まで遡ります。1996 年 10 月に JIPDEC（現在は日本情報経済社会推進協会に改称）の一部署として定常業務を開始し、2003 年には有限責任中間法人として独立、現在は一般社団法人として活動しています。
初期会員	JSOC（LACERT）	株式会社ラック	○（2000年）	－	－	－	2000 年にセキュリティ監視センターが設立。更に、2016年8月、当社におけるインシデント対応機能強化を目的に組織内CSIRTを仮想チームとして設置。2018年に「LACERT」に改称し、国内外の関連組織等との情報共有や連携を強化しています。
初期会員	NTT-CERT	日本電信電話株式会社	○（2003年7月1日）	－	－	－	2003 年ごろ、NTT 情報流通プラットフォーム研究所（当時）で活動開始。2004 年 1 月、「先端セキュリティセンター」 がオーソライズされた組織として結成されました。同年のうちに 「NTT-CERT」 と名前を改め、NTT グループの代表 CSIRT として活動するようになっています。
初期会員	SBCSIRT	ソフトバンク株式会社 Wireless City Planning株式会社	○（2004年9月1日）	－	－	－	SoftBank CSIRT の前々身である SBB-SIRT は 2004 年 9 月に設立されました。2015年9月1日に名称をSoftBank CSIRTに変更しました。開発したシステムのセキュリティチェックなどは SoftBank CSIRT の活動には含まれず、別のセキュリティ担当が実施しています。
会員	ABJ-PSIRT	ABB日本ベーレー株式会社	○	○（2018年4月1日）	－	－	ABB日本ベーレー株式会社がお客様に提供する製品、サービス、および制御システムを利用されているプラントのサイバーセキュリティの普及とサイバーレジリエンス向上に貢献します。
会員	ASY-CSIRT	ANAシステムズ株式会社	○（2013年9月20日）	－	－	－	ANA システムズ株式会社（http://www.anasystems.co.jp/）によって運営されている CSIRT 。ANA システムズ株式会社のセキュリティ専門部署に所属するメンバーで構成されている仮想的なチーム。
会員	TOSHIBA-SIRT	株式会社東芝	○（2012年4月1日）	○（2017年10月以前）	－	－	2017年10月からは製品セキュリティを担当するPSIRTとの連携強化およびCSIRT、PSIRT双方のサイバーセキュリティリスクへの対応力強化を図るため、CSIRTとPSIRTを一体化し、TOSHIBA-SIRTに改めました。
会員	NEC-CSIRT	日本電気株式会社	○（2002年7月1日）	○（2004年）	－	○	NEC-CSIRT は脆弱性情報を CERT/CC とハンドリングする目的で、2002 年 7 月 1 日に活動を開始しました。SI・サービス技術（PSIRT がコアチーム）は脆弱性情報のハンドリングの中核となっています。
会員	MELCO-CSIRT	三菱電機株式会社	○（2012年10月1日）	○（2019年4月1日）	－	－	広報発表あり。事業部門毎に担当者を配置し、本社組織と連携。
会員	Panasonic CSIRT	パナソニック株式会社	○（2014年1月1日）	○（2010年）	○	－	Panasonic CSIRT、PSIRT、FSIRTあり。
会員	RichosPSIRT	株式会社リコー	○（2013年11月15日）	－（2004年1月1日）	－	－	Richos US として First（Forum of Incident Response and Security Teams）に登録あり。RICHOレビューの2015年版に2016年にPSIRTと連携強化の記述あり。FIRSTの記載は、2004年1月1日。

日本シーサート協議会の会員、およびFIRST＊の国内参加組織についてそれぞれのホームページ情報をもとに事務局作成
（参考）https://www.nca.gr.jp/member/index.html

＊：FIRST（ Forum of Incident Response and Security Teams ）
CSIRT同士が国際的に相互の情報交換やインシデント対応に関する協力関係を構築する目的で1990年に設立されたフォーラム

PSIRT設置にあたっての課題

2017年のシンクタンク*のレポートにおいて、以下が課題として指摘されている。

（＊：ＮＲＩセキュアテクノロジーズ株式会社）

- PSIRTとして製品セキュリティを確保するためには、**セキュリティ全般の知識**および**製品知識**の両方を備えた人員がその活動をハンドリングすることが理想である。しかしながら現実論として、その**両方を備えた人員は極めて少なく、確保は困難**である。

- 現実的には片方の知識を有する担当者が相互に補完する（ただし、密なコミュニケーションを通じて相互理解を深め、共に脅威に向き合うことが重要）。
- （または）解決策（短期的）としては、セキュリティの専門能力を有する外部パートナーの活用が有効。

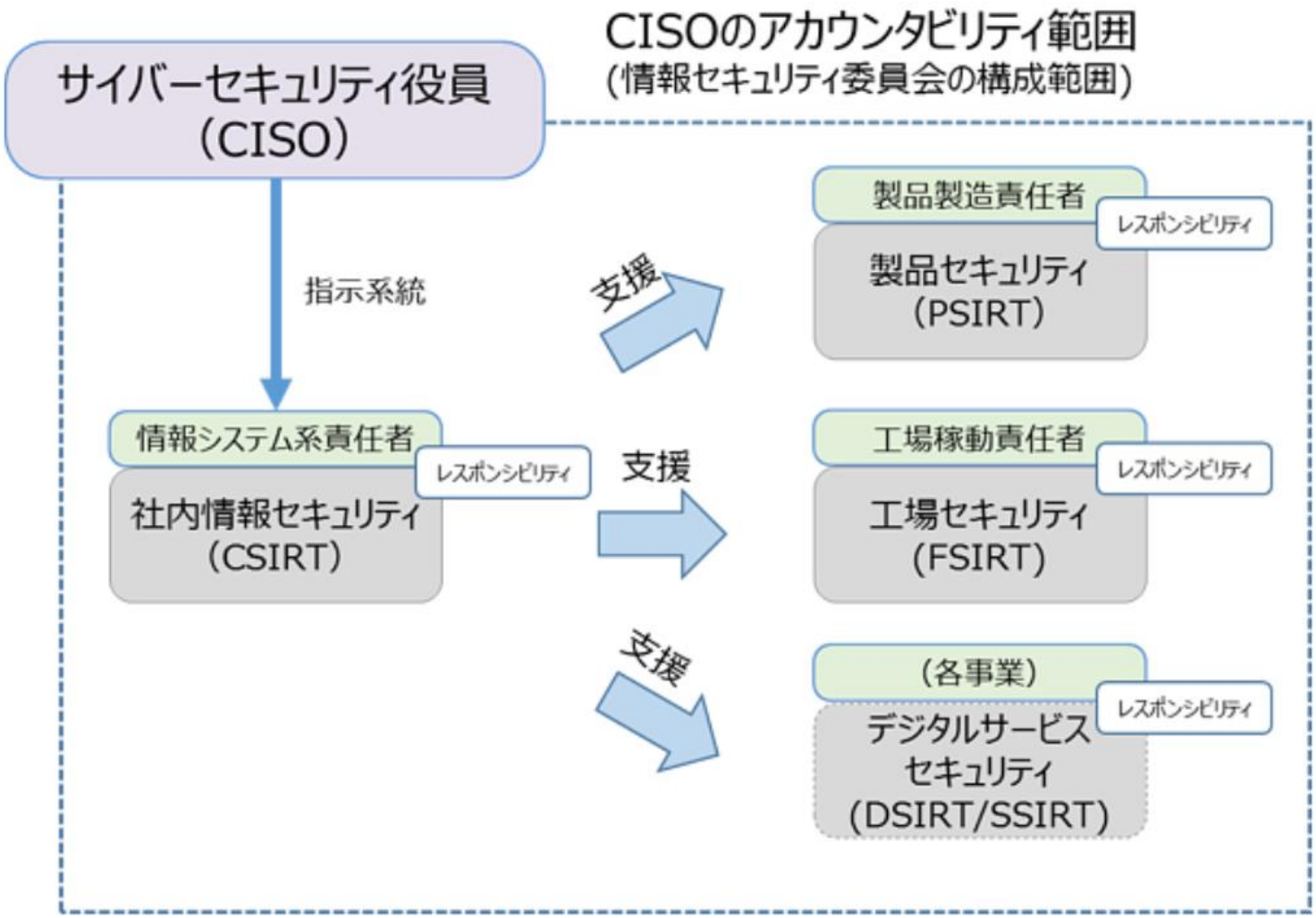
（出典）「トピックス IoTの普及に伴うPSIRTの必要性」（2017月10月）
ＮＲＩセキュアテクノロジーズ株式会社、
https://www.nri.com/-/media/Corporate/jp/Files/PDF/knowledge/publication/it_solution/2017/10/ITSF171006.pdf

概況

- デジタル化は企業にとって新たな価値を生み出す機会を与える一方、企業を狙う悪意者に対しても同様に新たな攻撃の機会/対象を与える。
- しかし、企業等において自社の情報やシステムを守っているCSIRTが、デジタル化された全ての自社製品・自社業務・自社サービスの本質を理解し、適切なセキュリティ対応を行うのは現実的に無理がある。
- そこで、**CSIRTだけでなく、例えば事業部側にxSIRT（PSIRT、FSIRT、DSIRT/SSIRT等）と呼ばれるセキュリティ組織を構築**し、一部のセキュリティ関連業務を任せる取組が始まっている。

参考資料：企業におけるガバナンスの一例

- CSIRTはCISOの指示のもとｘSIRT(PSIRT、FSIRT、DSIRT/SSIRT）を支援



（出典）「【次世代セキュリティ組織】CSIRTと協調する新たなセキュリティ組織xSIRTとは」（2019年7月9日）
ＮＲＩセキュアテクノロジーズ株式会社

参考資料：PSIRTについて・組織モデル

- PSIRTサービスのフレームワークについての解説書である「PSIRT Services Framework Version 1.0 日本語版」（JPCERT/CC）において、「PSIRTの組織構造は、守る製品が多種多様であるのと同じように様々な形がある。現在構築・運用されているPSIRTのほとんどは、分散モデル、集中モデル、ハイブリッドモデルという 3つのモデルのいずれかにあてはまるだろう。」と記述されている

➢ ①分散モデル
- ✓ PSIRTは小規模、製品開発チームと連携して対処
- ✓ 組織の規模が大きく、多様な製品ポートフォリオを持つ組織に適合

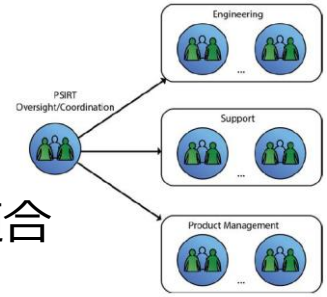


Figure 2: Distributed Model

➢ ②集中モデル
- ✓ 各部門から選抜されたスタッフが組織の製品セキュリティを担当
- ✓ 小さい組織や同種の製品ポートフォリオを持つ組織に適合

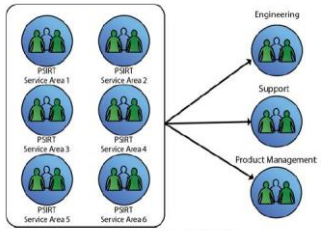


Figure 3: Centralized Model

➢ ③ハイブリッドモデル（①と②のミックス）

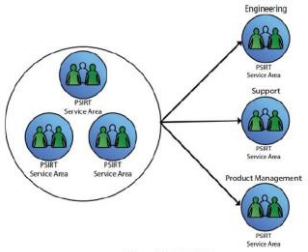
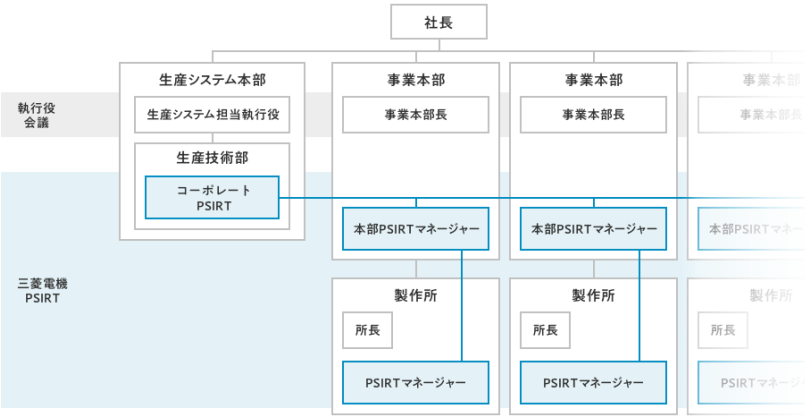


Figure 4: Hybrid Model

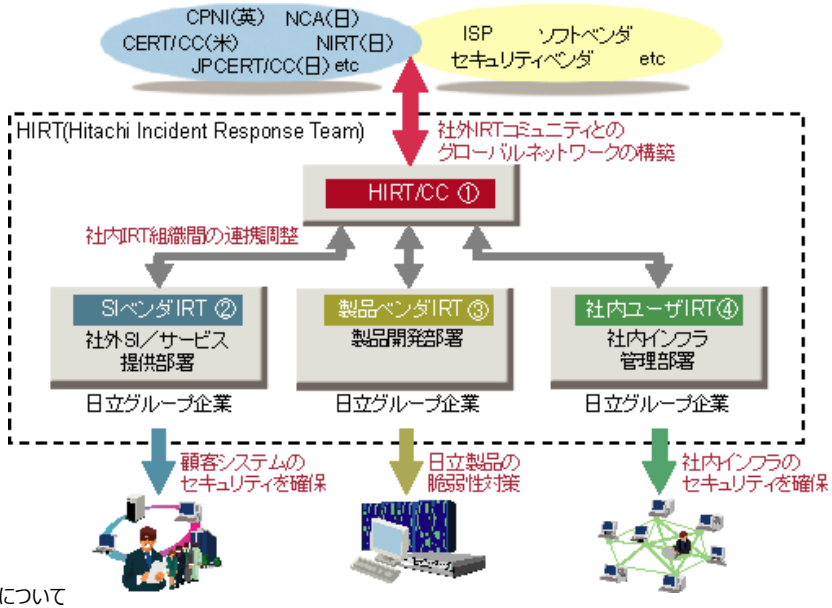
（出典）「PSIRT Services Framework Version 1.0 日本語版」（2019月11月13日）
JPCERT/CC、https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.0_jp.pdf
元となる文書「PSIRT Services Framework Version 1.0」(Summer 2018)
FIRST*、https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.0.pdf
＊：FIRST（ Forum of Incident Response and Security Teams ）
CSIRT同士が国際的に相互の情報交換やインシデント対応に関する協力関係を構築する目的で1990年に設立されたフォーラム

参考資料：PSIRTについて・国内の事例①

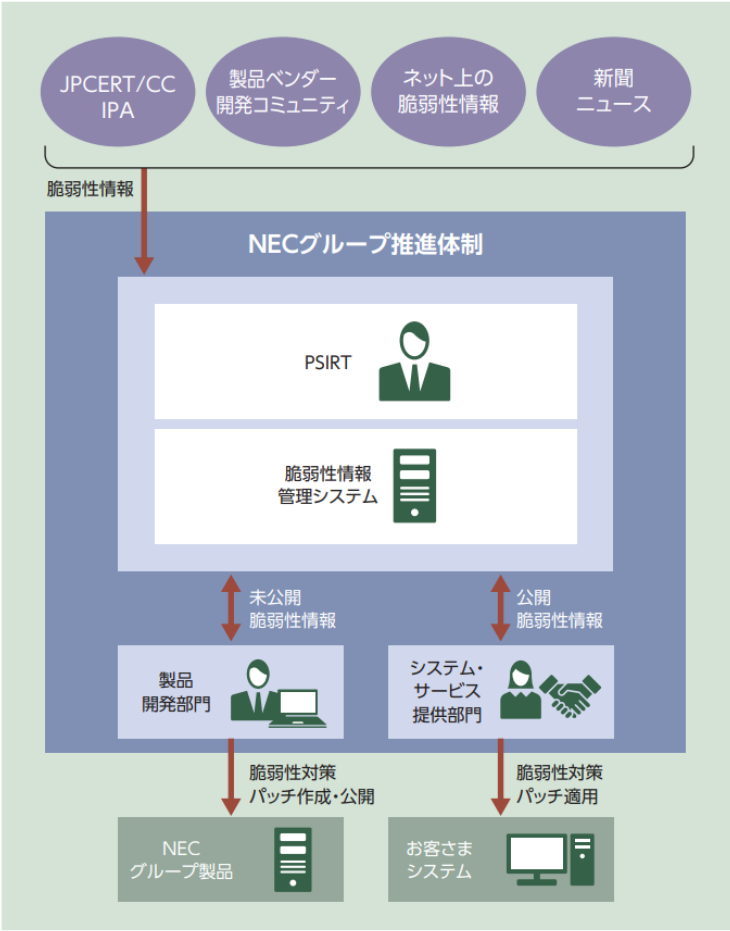
- メーカにより体制に違いがある
  （三菱電機株式会社、株式会社日立製作所、日本電気株式会社）



（出典）製品セキュリティー対応体制
三菱電機株式会社、
ホームページ（https://www.mitsubishielectric.co.jp/psirt/framework/index.html）より



（出典）HIRTについて
株式会社日立製作所、ホームページ（https://www.hitachi.co.jp/hirt/about/index.html）より



脆弱性対応推進体制

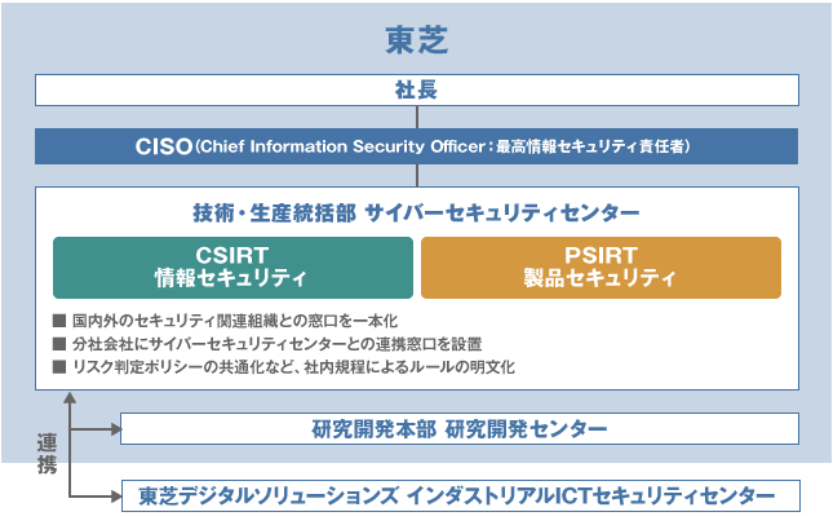
（出典）「情報セキュリティ報告書2019」（2019年７月）
日本電気株式会社、https://jpn.nec.com/csr/ja/pdf/isr2019j.pdf

参考資料：PSIRTについて・国内の事例②

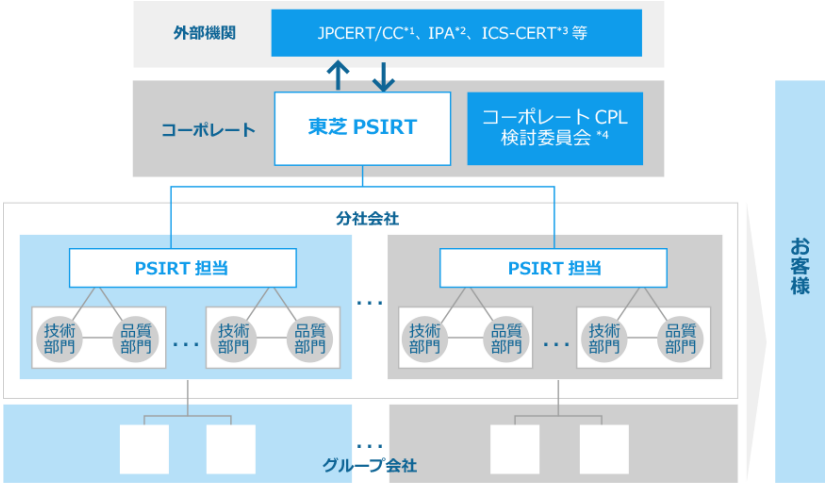
- メーカにより体制に違いがある（株式会社東芝）

図1 東芝のサイバーセキュリティセンター

サイバーセキュリティに対するガバナンスの強化と経営体制の強化を図るため、CISOとサイバーセキュリティセンターを設置しました。
情報システムと、製品やサービスに対するセキュリティ施策を集約し、東芝グループとして一貫したセキュリティ対策を推進しています。



CSIRT：Computer Security Incident Response Team
PSIRT：Product Security Incident Response Team



*1:Japan Computer Emergency Response Team / Coordination Center
*2:Information-technology Promotion Agency Japan
*3:Industrial Control Systems Cyber Emergency Response Team
*4:CPL:CL（契約に基づく品質保証責任）とPL（製造物責任）を合わせた略称

（出典）東芝の「サイバーセキュリティセンター」
株式会社東芝、
ホームページ（ https://www.toshiba-sol.co.jp/articles/tsoul/25/002.htm ）より

（出典）東芝 PSIRT
株式会社東芝、
ホームページ（ https://www.toshiba.co.jp/security/psirt ）より

参考資料：PSIRTについて・国内の事例③

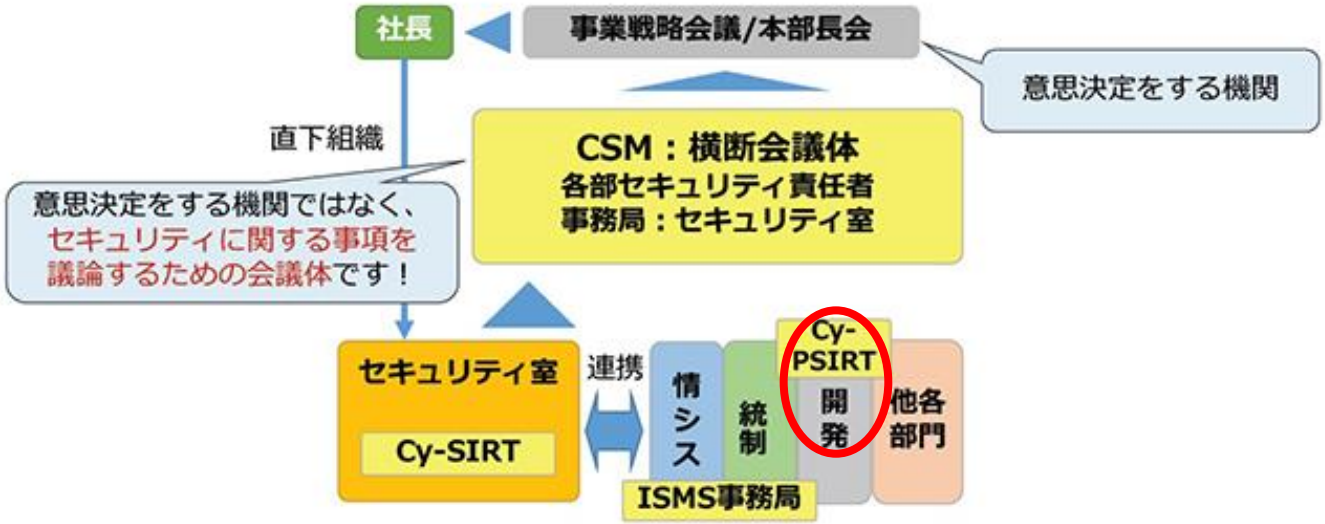
- IT企業のサイボウズ社では、一般的なセキュリティ対応を分離させてCSIRT（Cy-SIRT）を設置、PSIRTは製品（サービス、ソフトウェア）のセキュリティに集中できる体制
  - サイボウズ社は、クラウドベースのグループウェアサービスを中心に提供、導入企業は 85,000社超
- 現在は集中モデル、将来的には分散モデルへの移行も考えている模様

✓ 開発・テスト段階でセキュリティ検査を強化し、リリース前の早い段階で問題を見つけ出し、対処するプロセス作りを進めてきた。いわゆる**「セキュア・バイ・デザイン」**や「シフトレフト」といった取組み

✓ 将来的に、各プロダクトの開発チーム内にセキュリティに強いエンジニアを少なくとも1人以上配置することを考えているという。

（出典）いち早くPSIRT整備を進め、製品のセキュリティ向上に取り組んできたサイボウズがゲヒルンを信頼するワケ
ゲヒルン株式会社、ホームページ（ https://www.gehirn.co.jp/services/interview/cybozu/ ）より

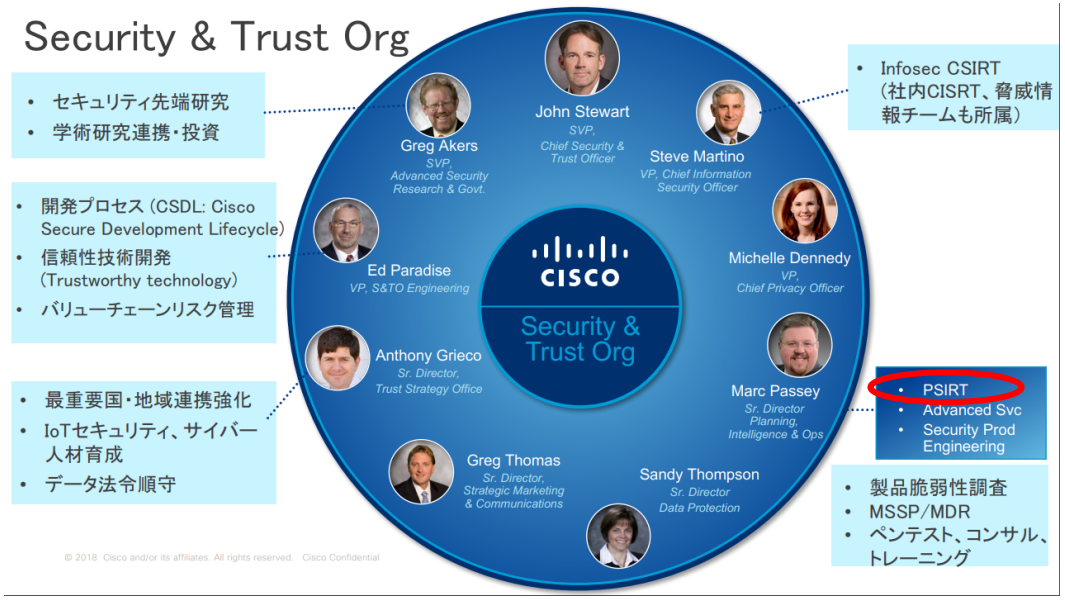
サイボウズのセキュリティ体制



（出典）「「セキュリティ室」新設から見えたサイボウズ流セキュリティマネジメントとは？」（2017年4月26日）
情シス Navi. 、ホームページ（https://josys-navi.hiblead.co.jp/%E3%80%8C%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E5%AE%A4%E3%80%8D%E6%96%B0%E8%A8%AD%E3%81%8B%E3%82%89%E8%A6%8B%E3%81%88%E3%81%9F%E3%82%B5%E3%82%A4%E3%83%9C%E3%82%A6%E3%82%BA%E6%B5%81）より

参考資料：PSIRTについて・海外の事例

- CISCO PSIRT
  - ➢ 20年以上の歴史を有し、グローバルに24時間365日対応可能
  - ➢ サイバーセキュリティ インテリジェンス＆リサーチ グループ「Cisco Talos」と連携してセキュリティインシデントに対処する体制
    - ✓ 270 人を超えるフルタイム脅威研究者を擁する
  - ➢ 体制としてはハイブリッドモデル



（出典）「シスコのサイバーセキュリティへの取組み」（2018年５月16日）
シスコシステムズ合同会社、
https://www.cisco.com/c/dam/global/ja_jp/partners/cpcp/data/p2-ciscocybersecurityforum-ciscosecurity-ho.pdf

参考資料：PSIRT支援サービス

- 企業PSIRTの構築から運用までを支援するサービスを以下のような会社が提供している
  - ➢ NRIセキュアテクノロジーズ株式会社
    - ✓ 組織内PSIRT向け支援サービス
      https://www.nri-secure.co.jp/service/consulting/psirt
  - ➢ PwCコンサルティング合同会社
    - ✓ 製品セキュリティインシデント対応体制（PSIRT）構築支援
      https://www.pwc.com/jp/ja/services/digital-trust/cyber-security-consulting/product-cs/psirt.html
  - ➢ テュフ ラインランド ジャパン
    - ✓ PSIRT構築支援サービス
      https://insights.tuv.com/jpblog/psirt

NRIセキュアテクノロジーズ株式会社の事例

（出典）ＮＲＩセキュアテクノロジーズ株式会社、
ホームページ（ https://www.nri-secure.co.jp/service/consulting/psirt ）より

参考資料：海外企業におけるPSIRT

- IBM Security Vulnerability Management (PSIRT)
  アメリカに本社をもつ、コンピュータ関連製品およびサービスの提供企業のPSIRT
  https://www.ibm.com/security/secure-engineering/process.html

- Ericsson PSIRT
  スウェーデンに本社をもつ、通信機器（移動体通信の地上固定設備等）のメーカーのPSIRT
  https://www.ericsson.com/en/about-us/enterprise-security/psirt

- The Bosch Product Security Incident Response Team (PSIRT)
  ドイツに本社をもつ、総合自動車部品及び電動工具メーカーのPSIRT
  https://psirt.bosch.com/

- NVIDIA PSIRT
  米国に本社をもつ、半導体（GPU、AI用アクセラレータ等）メーカーのPSIRT
  https://www.nvidia.com/en-us/security/

- SAS Product Security
  米国に本社を持つ、統計分析のソフトウェアおよびサービスの提供企業のPSIRT
  https://support.sas.com/en/security-bulletins.html

- CISCO Product Security Incident Response Team
  米国に本社を持つ、コンピュータネットワーク機器、サービスの提供企業のPSIRT
  https://tools.cisco.com/security/center/home.x