# IoT時代におけるセキュリティ対応態勢のありかた
# シフトレフトする攻撃に生き残れ！

一般社団法人コンピュータソフトウェア協会
Software ISAC

# 登壇者のご紹介

- サイボウズ株式会社 セキュリティ室室長　明尾洋一さん
- マイクロソフトコーポレーション
  セキュリティプログラムマネージャー　垣内由梨香さん
- 株式会社LAC 理事・シニアコンサルタント　加藤智巳さん
- アップデートテクノロジー株式会社
  代表取締役社長　板東直樹

# IoT時代の攻撃と防御、PSIRTの重要性が問われるいま！

- **IoT時代のゼロディ攻撃と防御　受け入れ必至 “Zero Trust” とは**
  - 株式会社ラック 仲上 竜太氏
    - 開発環境とオープンソースリポジトリ汚染
    - 開発プロセス・サプライチェーンの統制
    - ソフトウェアサプライチェーンリスクに備える
      ゼロトラストセキュリティ

- **IoT時代に必要なPSIRTとその役割**
  - グローバルセキュリティエキスパート株式会社 萩原 健太 氏
    - ライフサイクルまたはどの階層でリスクが潜む可能性があるのか？
    - 組織内のステークホルダーは把握できているか？
    - PSIRTは事業継続マネジメントの一環

# CSIRT, PSIRT, F/MSIRT

| | CSIRT | PSIRT | FSIRT (MSIRT) |
|---|---|---|---|
| 名称 | Computer(Cyber) Security Incident Response(Readiness) Team | Product Security Incident Response(Readiness) Team | Factory (Manufacture) Security Incident Response(Readiness) Team |
| 概要 | 主に組織内または提供するサービスのインフラなどを対象としたセキュリティチーム | 組織が提供する製品やサービスに特化したセキュリティチーム | 工場内のセキュリティに焦点を当てたセキュリティチーム |
| 主管部門 | 情報システム部門 | 品質保証・開発部門 | 生産部門・工場 |
| 保護対象(例) | • 従業員や顧客の個人情報<br>• 事業に必要なインフラ | • 製品自体の安全性<br>• 製品ブランド | • 生産ライン<br>• 工場内の設備 |

# PSIRT を始めたいが…

- どうしてよいか分からない
- 経営層、現場ともに社内の理解がない
- 適切な人材がいない
- ステークホルダー（通報者）との関係はどうあるべき？
- セキュリティ品質ってどう決めるの？
- コンポーネント管理なんてできない、棚卸が大変だ
- 企業規模が小さく一人PSIRTになってしまう
- ファジングツールなどは、高くてコストが見合わない
- ガイドラインは読んだけど、今ひとつピンとこない

# 本日のテーマ

# インシデントに強いPSIRTの作り方

# CSAJ/SoftwareISAC のご紹介

# Cy-PSIRT の活動

社外の組織・専門家と協力して**製品のインシデント発生の予防**、早期検知、早期解決、被害が発生した場合の最小化を主眼とした活動をする

- 脆弱性診断
- 脆弱性情報収集・連絡
- 外部機関との連携
- 報奨金制度運営

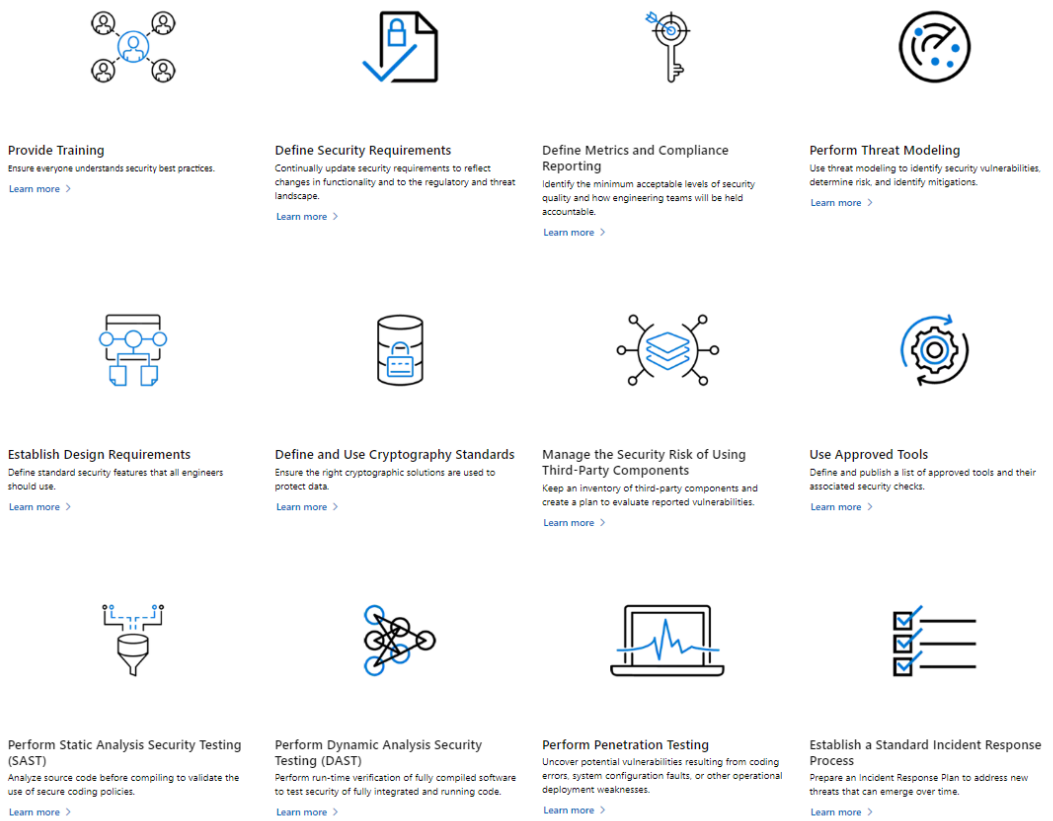
cybozu Bug Bounty

# 安全な開発・運用のために

マイクロソフトが実際に利用しているベストプラクティスを公開

- **Security Development Lifecycle (SDL)**
  - 安全な製品を開発するための ベストプラクティス、ツール
  - 「簡易版」エクセル形式のチェックリスト
- **Operational Security Assurance (OSA)**
  - クラウド環境における運用セキュリティ
- **Open Source Security**
  - オープンソースを利用する際の リスク管理手法

[マイクロソフト セキュリティ エンジニアリング](https://www.microsoft.com/securityengineering)
https://www.microsoft.com/securityengineering




© Microsoft Corporation

# 現存するPSIRT の課題や共通点：商品が多種多様であり、部門間(事業部間)調整に苦労

| | PSIRT の考え方 | PSIRTで優先すること | (意識の高い)課題 | サプライチェーンリスク |
|---|---|---|---|---|
| A社 | • 品質マネジメントシステム (SDL) の中で製品セキュリティを管理 | ・固有にSDLを構築<br>・教育や啓発活動を活性<br>・脆弱性インシデント情報共有<br>・サプライアに対しても遵守 | • 国内と海外のギャップ<br>• サプライアへの遵守は段階的に進めざるを得ない<br>• 開発側をセキュアにしたいがバランスを重視 | • 脆弱性対応の状況の確認を重視し、有事はソースコード共有も含め共同で対処 |
| B社 | • グループSIRTの下にPSIRTとCSIRTを設置し統括 | • PSIRTリソース不足を埋める手段としてまずは情報共有を重視<br>• 発見者側の視点で対応を心がける<br>• 社会的影響、損害、リスクを考慮<br>• ステークホルダの意識が重要 | • ベストプラクティスが適用しにくい<br>• 検証が難しい(顧客都合、環境等) | • サプライアに対するガイドラインの策定と遵守を進めている |
| C社 | • PSIRTとCSIRTは各々に成熟させてきたが将来的には統合 | • 横断的対処や、専門性が問われるところでPSIRTが機能<br>• 固有のSDLを構築<br>• 製品出荷前にセキュリティ対策が大前提→脆弱性診断を自前で検証 | • グループ内組織改革頻度が高い。<br>• 事業部側か発見者(ユーザ)？仕様か脆弱性か？<br>• 開発側をセキュアにしたいがバランスを重視 | • 最低限の責任を認識し合い、有事にはソースコード共有<br>• SBOMを利用 |
| D社 | • PSIRTは完全分散型を追求し、情報共有の品質を重視 | • OSS脆弱性情報の共有を重視<br>• 情報セキュリティに関する報告書を共有 | • PSIRTは事業部毎に重要度が異なり、スキルも疎ら。<br>• “適切なPSIRT支援とは”を追求 | • ガイドラインや脆弱性の対応基準を今後決めていく |

# PSIRT を始めたいが…

- どうしてよいか分からない
- 経営層、現場ともに社内の理解がない
- 適切な人材がいない
- ステークホルダー（通報者）との関係はどうあるべき？
- セキュリティ品質ってどう決めるの？
- コンポーネント管理なんてできない、棚卸が大変だ
- 企業規模が小さく一人PSIRTになってしまう
- ファジングツールなどは、高くてコストが見合わない
- ガイドラインは読んだけど、今ひとつピンとこない

# PSIRT Services Framework Ver 1.0 Draft に基づくプロダクト脆弱性対策・対応成熟度シート

*1.1* 内部のステークホルダ管理

目的： 脆弱性管理に関わる内部のステークホルダによるエコシステムマネジメントを確立するため、PSIRT と内部のステークホルダとの関わり合いや関連するプロセスを定義し、インシデント時の認識や支援について PSIRT の役割を明確に伝え、インシデント時の対応力を向上させる。

| レベル 0 | レベル 1 | レベル 2 | レベル 3 | レベル 4 | レベル 5 |
|---|---|---|---|---|---|
| 脆弱性に関する管理の柱として PSIRT は必要とされていない。又は、必要と認識しながらも経営者は組織内にその機能を持つ為のリソースを提供していない。 | 一部の担当者は脆弱性管理の必要性を感じており、業務で顕在化した脆弱性情報に関して限られた相手に情報共有し、業務範囲や既存の業務分掌を超えたなかで対処している。<br>製品の脆弱性に関してはCDLへの移行がセキュリティライフサイクルの要点であることには気が付いていない。 | PSIRTと内部ステークホルダとのコミュニケーションの重要性に気がつきはじめ、インシデント対応 プロセスは徐々にパターン化している。経営者とも 意識を合わせ、製品は顧客が利用することで初めて 価値が生み出されると感じている。 | [1.1.1] PSIRTが組織として、その責任者や機能、役割が文書化され周知されている。内部ステークホルダとしては、広報・CC、法務部、開発部門、営業が定義されている。<br>[1.1.3.1] インシデント事後対応プロセスの構築は成熟しているが、開発の不具合をレビューするプロセスまでは確立していない。 | PSIRT の機能と内部のステークホルダのマネジメ ントについて向上させるには、<br>[1.1.1.3] 社内ビジネスユニット・ラインとの交流、<br>[1.1.1.4] 内部開発・エンジニアリングとの交流、<br>[1.1.1.5] ステークホルダに対応するサポートチームとの交流、<br>[1.1.1.6] 内部ワーキンググループへ参加が必要であると認識され始めた。 | 以下のようなSDL のメンテナンスに繋がる具体的な活動が充実してきた。<br>[1.1.3.2] プロセスの不具合を追跡し教訓を招請し重要なステークホルダの問題を定期的にレビューする。<br>[1.1.3.4] 人目をひくインシデントの対応から組織としての教訓を整理し報告データを提供する。<br>[1.1.3.5] 事後対応プロセスで特定された内部プロセスの再調整を支援し改善の進捗状況を追跡する。 |

# PSIRT Services Framework Ver 1.0 Draft に基づくプロダクト脆弱性対策・対応成熟度シート

CSAJ 脆弱性対策

- **https://www.csaj.jp/NEWS/committee/security/190408.html**

# PSIRT を始めたいが…

- どうしてよいか分からない
- 経営層、現場ともに社内の理解がない
- 適切な人材がいない
- ステークホルダー（通報者）との関係はどうあるべき？
- セキュリティ品質ってどう決めるの？
- コンポーネント管理なんてできない、棚卸が大変だ
- 企業規模が小さく一人PSIRTになってしまう
- ファジングツールなどは、高くてコストが見合わない
- ガイドラインは読んだけど、今ひとつピンとこない

# CSAJ/Software ISAC

- **活動内容**
  - OSS脆弱性データベースの構築
    - 機械システム振興協会イノベーション戦略策定事業
      OSSの脆弱性情報管理に関する戦略策定
  - 脆弱性検証センターの構築・運用

  - PSIRT推進WG
  - セキュア開発WG

  - 経産省モデル契約 セキュリティガイドライン 策定

# PSIRT推進WG の活動

- **趣旨**
  - Software ISAC 加盟企業のPSIRT活動を支援する
    - PSIRTの立ち上げ支援
    - PSIRTメンバーのスキル向上支援
    - PSIRT間の情報交換

- **過去の活動**
  - 脆弱性対応組織成熟度シートの説明、測定実施
  - OSS 脆弱性管理ツール の勉強会

# セキュア開発WG

- **OSSやマイクロソフト関連のソフトウェアなど、セキュア開発につながる情報連携や勉強会などの実施**
  - Spring Frameworkのセキュアコーディング
  - .NET Framework のセキュアコーディング
  - クラウド上での安全な開発環境

# 経産省モデル契約 セキュリティガイドライン 策定

- **IPA社会基盤センター モデル取引・契約書見直し検討部会**
  - 民法改正対応モデル契約見直し検討WG
    - セキュリティ検討プロジェクトチーム