

IoT時代の攻撃と防御、PSIRTの重要性が問われるいま！

「IoT時代に必要なPSIRTとその役割」

2019年10月17日

グローバルセキュリティエキスパート株式会社
事業戦略室 CSO兼CSRO

萩原 健太

ISACとは

• Information Security and Analysis Center

- 業界固有の問題に対して、業界内でより密な連携を行うことによって、防御力の向上や効率化などを図る枠組み
- ICT、金融、電力、交通（航空・鉄道・物流）、J-Auto（自動車）、ソフトウェアなどのISACがある

言うまでもなく…



ソフトウェアに支配される時代

ソフトウェア支配時代の課題

- ・ソフトウェア開発に欠かせないもの…

Open Source Software

サプライチェーンとは何か？

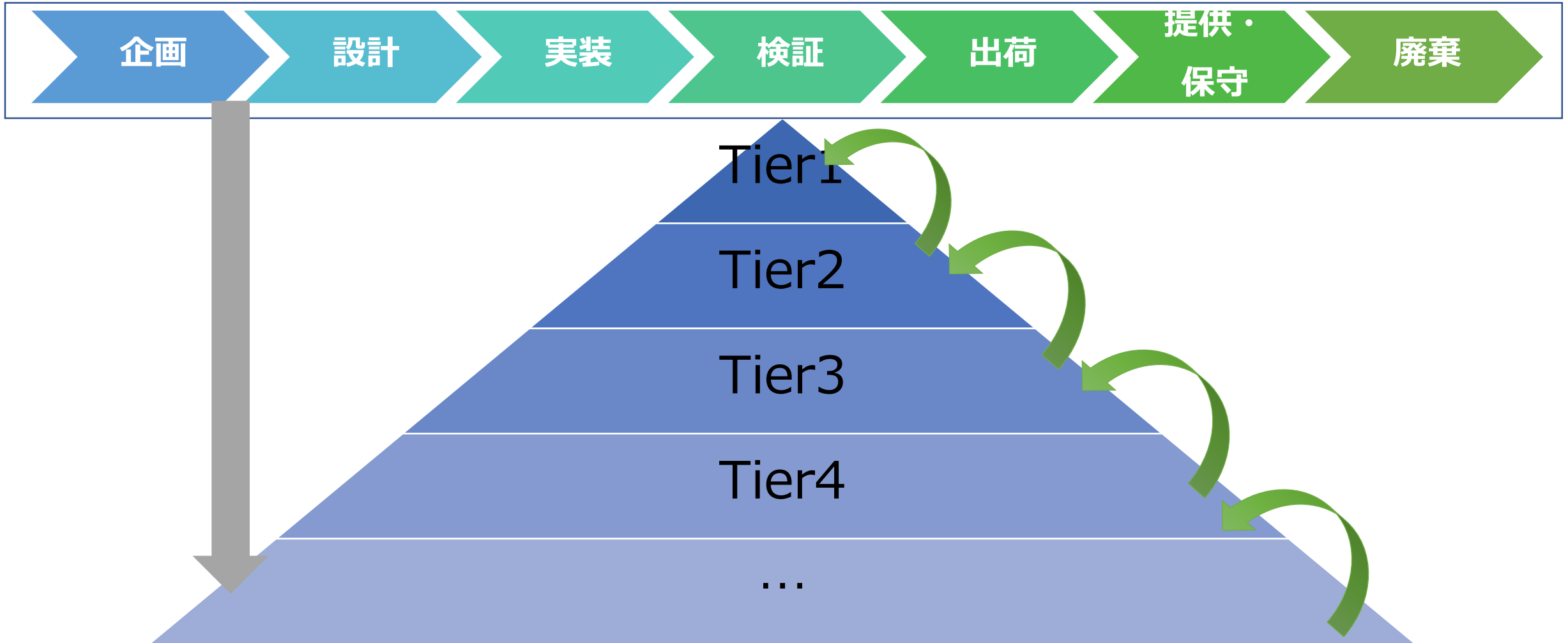
- ・ 個々の企業の役割分担にかかわらず、原料の段階から製品やサービスが消費者の手に届くまでの全プロセスの繋がり。

引用元：ASCII.jpデジタル用語辞典

【セキュア開発ライフサイクル】



複雑な構造、、、



「IoT 製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」

(独立行政法人情報処理推進機構)

<https://www.ipa.go.jp/files/000065094.pdf>

そのような中迫る…

攻撃の シフトレフト？

そのような中迫る…

データ取り扱いの 重要性

営業秘密・限定提供データ

【営業秘密の3要件】

- ①秘密管理性（秘密として管理されていること）
- ②有用性（有用な営業上又は技術上の情報であること）
- ③非公知性（公然と知られていないこと）

【限定提供データの3要件】

①限定提供性（業として特定の者に提供する）

→反復継続的に提供している場合／一定の条件の下でデータ提供を受ける者

②相当蓄積性（電磁的方法により相当量蓄積）

→社会通念上、電磁的方法による蓄積によって価値を有する

③電磁的管理性（電磁的方法による管理）

→特定の者に対しての提供、また管理する保有者の意思が、外部に対して明確化されている

そのような中迫る…

民法改正

瑕疵担保責任 → 契約不適合

• 瑕疵担保責任

- 発注側の想定(期待)した成果物の状態に達していない（性能がない）時に生じる責任

• 契約不適合

- 目的物が種類又は品質に関して契約の内容に適合しない

「契約不適合」の課題：期間

- **引き渡した時から1年**
→不具合を知った時から1年以内
- **請求権（いわゆる知った時期）は5年**
- **消滅時効は10年**（10年間は無償で修補を求められる？）

インシデント対応体制の確保

**Computer (Cyber)
Security
Incident
Response (Readiness)
Team**



組織のサイバー空間上に
おける対応の中心

**Emergency Readiness
(事前準備)**

と

**Incident Response
(事後対応)**

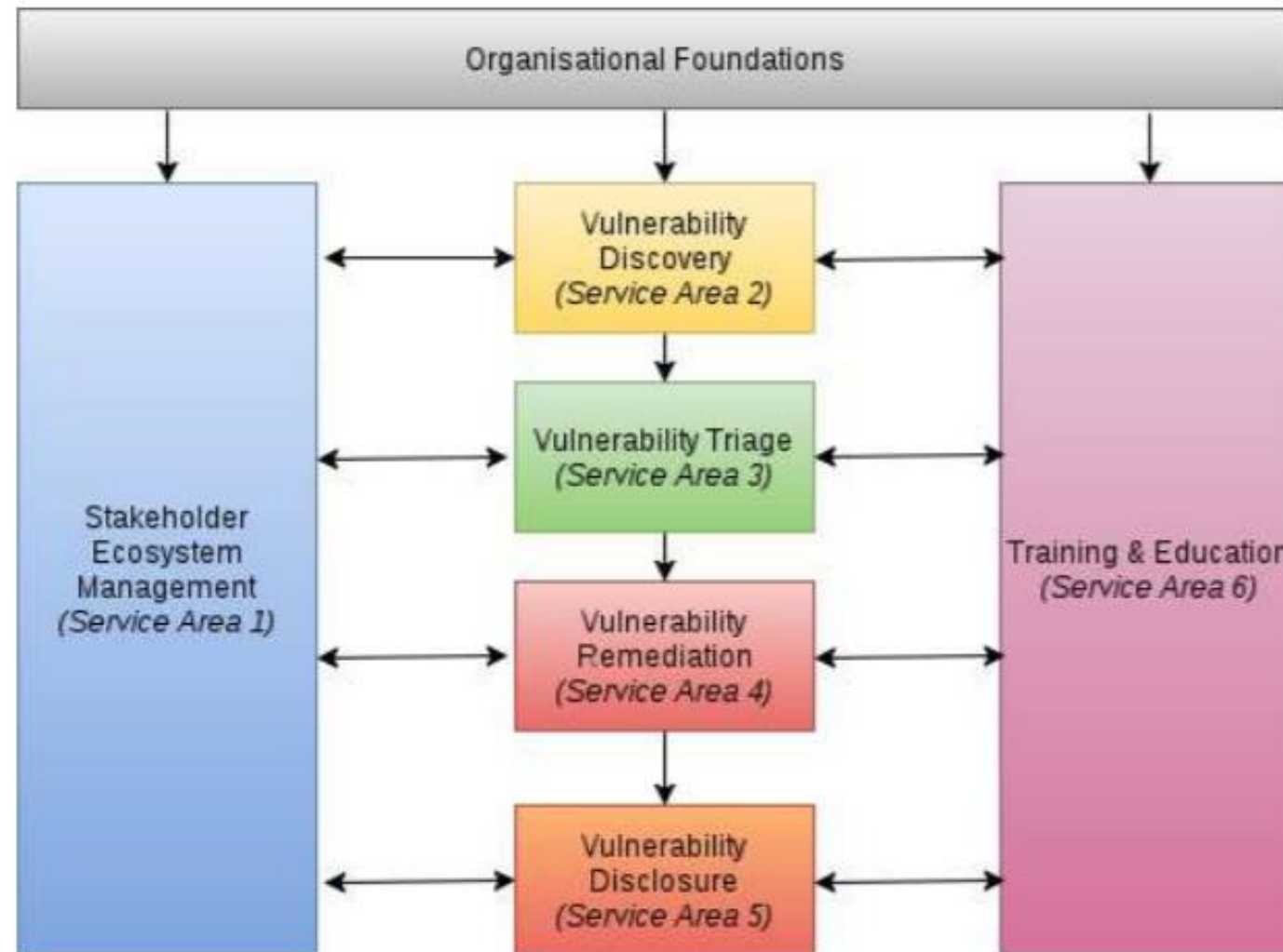
を担うチーム (**能力**)

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 - 事業に必要なインフラ	- 製品自体の安全性 - 製品ブランド	- 生産ライン - 工場内の設備

製品・サービスを提供するための体制

- PSIRT (Product Security Incident Response Team)



FIRST 「PSIRT Service Framework」

Stakeholder Ecosystem Management

Service Area 1

ステークホルダーを…

- 把握する
- 理解する
- 指標を定める
- 会話する
 - 報告のレベル等の確認含む

Discovery

Service Area 2

- **Point of Contact**
- **情報の取り扱い体制・ルール**
- **自ら未報告の脆弱性を探しに…**

コンポーネント・脆弱性を管理する：分類

1. 製品固有のソースコード内の脆弱性
2. 製品開発者の組織内リソースによってメンテナンスされるコンポーネントの脆弱性
3. 製品開発者の外部リソース（サードパーティ）によってメンテナンスされるコンポーネントの脆弱性

- **Software Bill of Materials
(ソフトウェア部品表)**

- アプリケーションに組み込まれているすべてのコンポーネント

作成できるのか？活用できるのか？

Triage

Service Area 3

判断するための体制

- 認定基準
- 再現させるための環境整備
- 発見者との関係構築

Remediation

Service Area 4

- ・製品開発・管理プロセスの構築と運用
- ・脆弱性の分析・緩和策／対策の検討
- ・修正プログラムの提供
- ・インシデントハンドリング

Discloser

Service Area 5

- ステークホルダーへの通知、調整
- 開示
 - プレス
 - リリースノート
 - 記事

Training and Education

Service Area 6

トレーニング

1. PSIRT トレーニング

1. 法律やコミュニケーション、開発などさまざまなトレーニング

2. 開発(内部エンジニアリングと開発)

1. 開発者は高度に熟練され、スキルに重点を置いているため、焦点を絞ったトレーニングが必要

3. 製品検証（内部エンジニアリングと開発）

1. 診断担当者は、リリース前に脆弱性を発見するため、最新のツール・ペンテスト・脆弱性スキャン・初期設計のレビューのテクニックに精通するためのトレーニングが必要である

4. 他のすべてのステークホルダ

1. ステークホルダは、セキュアな製品の開発・検証・出荷に関する基礎を理解すると同時に出荷された製品に脆弱性がある場合の対応に関するトレーニングが必要である

Software ISACの取り組み

- **目的**：ソフトウェアのよりセキュアな開発や更新等が行えるように、「Software ISAC」を構築し、
ソフトウェア開発や脆弱性管理等の工数最適化や、さらには日本のより安全・安心な社会への貢献を図る。
- **実施概要**
 - 国内ソフトウェア産業に必要な脆弱性・脅威情報等の集約、分析、展開
 - 開発の上流工程からのセキュリティ組み込み（シフトレフト）
 - 開発ソフトウェアに係る外部連携の支援
 - 脅威情報の早期把握と発見
- **活動**
 - OSS脆弱性データベースや脆弱性検証センターの構築・運用
 - ワーキンググループ
 - PSIRT推進/実践WG
 - セキュア開発WG
 - 強靱化WG
 - 他団体との連携

最後に

- 攻撃もシフトレフト？
- 複雑になる技術＋レギュレーション
- 本来はCSIRT（さらに本来はBCNの一環で）対応
- PSIRTのサービスの6つのサービスの実装検討
- 大切なことは「コミュニケーション」