環境変化に対応できる情報セキュリティ組織の機能と構造 -CSIRTに着目した考察-

The function and structure on information security organization that respond to environmental change -A study focused on the CSIRT -

副島恵子・システム分科会・情報セキュリティ大学院大学

The information security activities of the organization based on ISMS is a top-down approach based on the PDCA cycle. While cyber attacks such as APTs (Advanced Persistent Threats) are diversifying and sophisticated, the organization is required to respond promptly to environmental changes such as information security incidents. On the other hand, CSIRT has attracted attention, as a specialized unit handling information security incidents in cooperation with local staff.

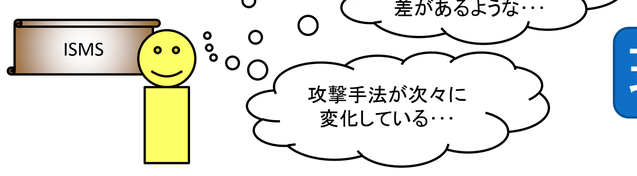
In this study, focusing on the function of CSIRT, the function and structure on information security organization are examined to activate the information security activities of the organization.

背景

- 大規模な個人情報漏洩事件などが頻発
- サイバー攻撃は悪質化・巧妙化
- 組織の信頼度低下を防ぐため，インシデント発生時は早期の段階での対応が重要

従来の情報セキュリティの取り組みの問題

- PDCAサイクルではインシデント対応に限界
  - 環境変化に対応しきれない
  - PDCAは組織をクローズドシステムと捉えている ⇔ 情報セキュリティはオープンシステム
  - PDCAは計画と執行が分離
- 現場との距離感
  - ISMS特有の取り組み
  - 現場が関与せず対策決定
- サイバー攻撃などは動的リスク ⇔ ISMSは静的リスクを扱う



PDCAサイクルによらない仕組みが必要

- OODAループによる動的プロセス連携の考え方
- 現場に権限を集中させ被害を最小化するICSの考え方

現場に権限を持たせるボトムアップの取り組みが必要

現場主体型の課題

- 現場のモチベーションをどうするか
- 現場の情報セキュリティ意識を高める必要がある
- 情報セキュリティの専門知識や技術が十分とは限らない

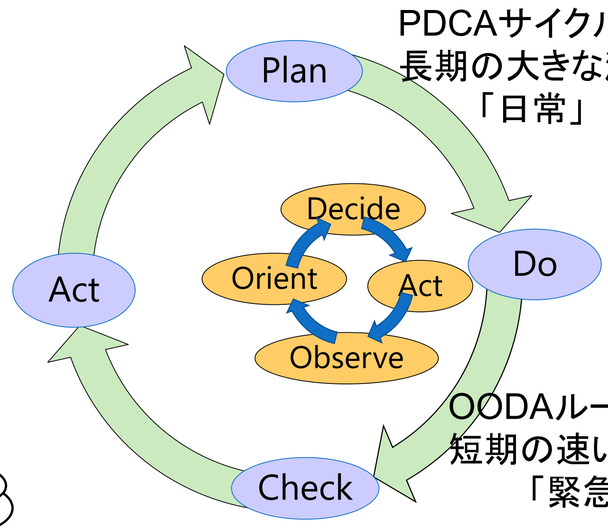
CSIRTの活動が現場主体型を助ける

- CSIRT：インシデント対応を専門に行うチーム
- インシデント時は、現場、CSIRT、関係箇所が連携
- 平常時には、CSIRTは教育・啓発活動などを行っている

現場主体型のボトムアップの取り組みで組織の情報セキュリティを向上させる

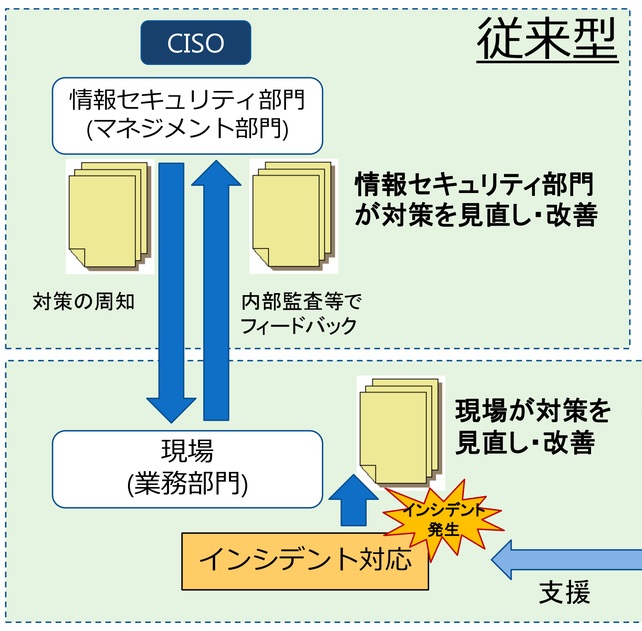
- ◆現場が当事者意識を持って情報セキュリティに取り組む
- ◆環境変化に対応可能な情報セキュリティ組織を実現

トップダウンとボトムアップの融合



PDCAとOODAの組み合わせで組織の情報セキュリティを向上させる

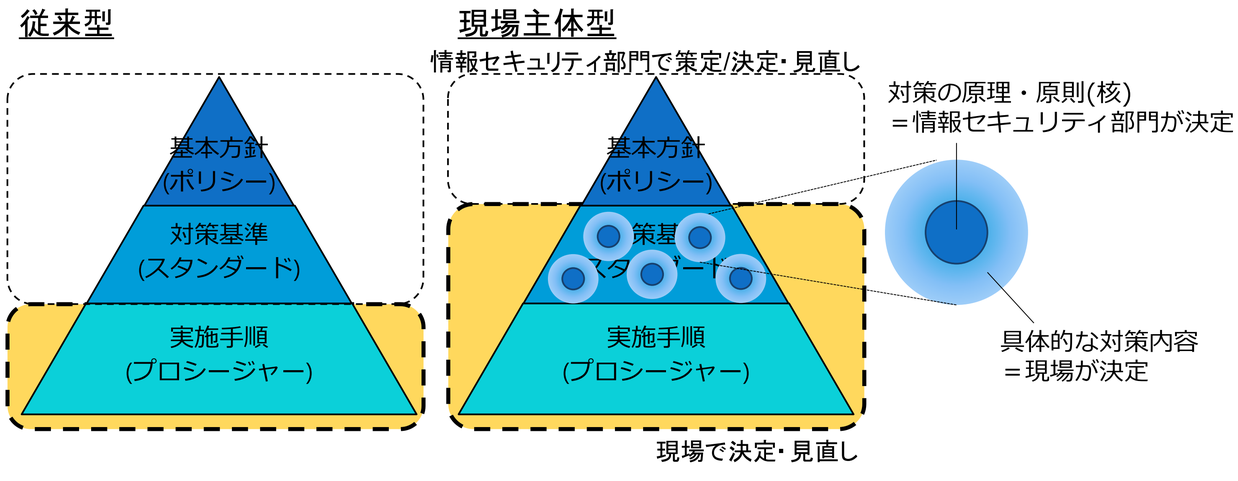
現場主体型の情報セキュリティの提案



現場主体型とは

- 現場が対策を決定・見直し
- 緊急時の迅速な改善が可能
  - ◆ボトムアップ
  - ◆リアルタイムの改善
  - ◆環境変化に対応

- ルール
  - 基本となる決まり
  - 組織全体の取り組みを統一、共通認識
  - 対策の指針・原則
- 対策
  - 実現の手段・手続き
  - 技術・文書などのツールで実現
  - 具体的な手順・行動



現場主体型は環境変化に柔軟に対応できる