システム運用に関する一考察

ーインシデントを収束できない場合を想定した体制を中心にー

A Study on System Operation

- Focusing on a structure assuming cases where incidents cannot be converged -

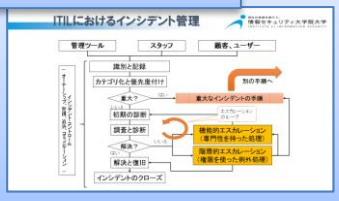
髙田英通・マネジメント分科会・情報セキュリティ大学院大学

In this study, on the premise that a cyber-attack that cannot be handled as an organization occurred to the information system, we listed what should be examined as an organization.
In the procedure of this study, we first investigated various documents such as ITIL which is the best practice of system operation and guidelines for business continuity plan related to information system. As a result, it was found out that the troubleshooting in the operation management of the information system and the security incident response of the information system are concepts having the same structure.
Next, a newly extended model (OODA three-layer model) was derived by assuming a situation that does not correspond to a cyber-incident that cannot be converged on the model of the previous research. Then, using this model, problems such as organizational structure on incidents that cannot be converged can be derived and visualized and listed. Finally, assuming reflection on future practice, we classified the problems in academic research field and practical examination field.

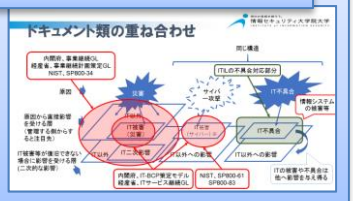
システム運用現場とセキュリティ部署との間の問題

1. 運用現場にはサイバーセキュリティの専門的な知識をもち、対応できる人員がいるとは限らない。
2. 同様にセキュリティ担当部署にはシステム固有の構造に詳しい者がいるとも限らない。
3. このような状況でお互いに調整をしながらサイバーインシデントに対応する、といっても、現実には時間的切迫など非常に難しい場合がありえる。

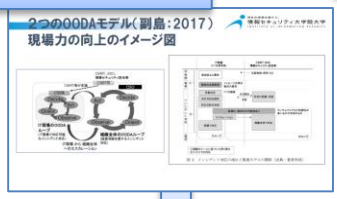
インシデント管理のフロー



IT-BCPガイドライン類との構造比較



先行研究（IT現場力向上



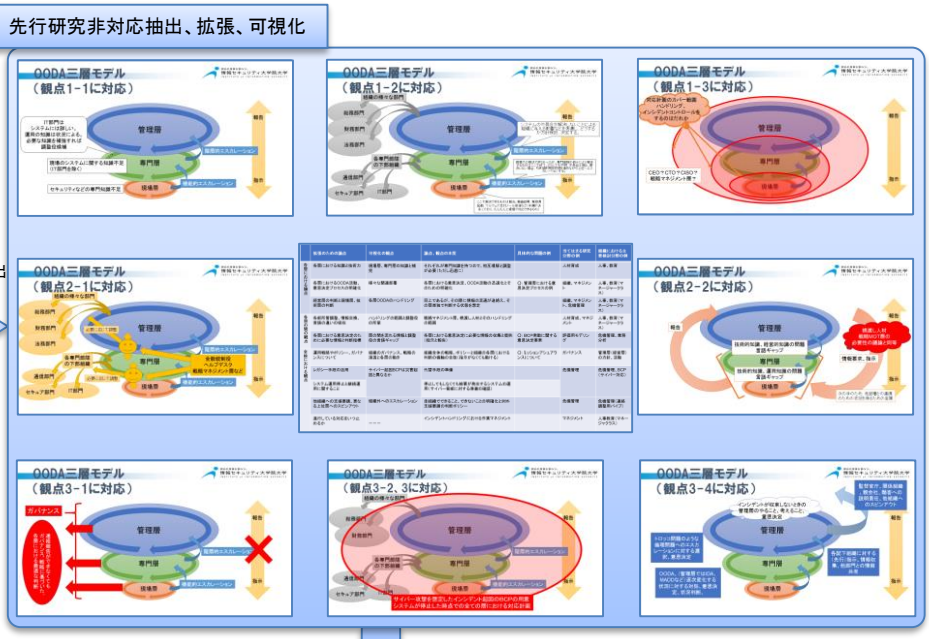
非対応部分の抽出

インシデントを収束できないという前提

先行研究拡張

拡張、可視化

先行研究非対応抽出、拡張、可視化



論点、観点と研究、検討分野の対応

	観点	当てはまる研究分野の例	組織における主要検討分野の例
各層における論点	観点1-1	人材育成	人事、教育
	観点1-2	組織、マネジメント	人事、教育（マネージャークラス）
	観点1-3	組織、マネジメント、危機管理	人事、教育（マネージャークラス）
各層の間の観点	観点2-1	人材育成、マネジメント	人事、教育（マネージャークラス）
	観点2-2	評価用モデリング	危機管理、業務分析
全般における観点	観点3-1	ガバナンス	管理層（経営層）の方針、活動
	観点3-2	危機管理	危機管理、BCP（サイバー対応）
	観点3-3		
	観点3-4	危機管理	危機管理（連絡調整用パイプ）
	観点3-5	マネジメント	人事教育（マネージャクラス）

分類、整理

今後の発展

1. 本研究が当てはまるシステムと当てはまらないシステムの切り分け
2. 当てはまるシステムの実務への具体的検討への落とし込み
3. 副島モデルで対応できないという切り口以外からの検討
4. 学術的な研究と、実務的な検討のリンクと研究の実務への利用態勢／体制の整備、検討