IoT対応の制御システムにおける内部犯行対策に関する考察

A study of internal crime measures in the control system for IoT

中島佳奈 ・ マネジメント分科会 ・ 情報セキュリティ大学院大学

In late years, with the development of the IT technique and the development of the robot technology, the concept called the control system for IoT was devised. This concept is a key to fourth industry revolution concept. However, a security risk occurs when various systems are connected to the factory. Therefore, in this report, I consider internal crime measures in the control system for IoT.

IoT対応の制御システムの概要

近年，IT技術の発展に伴い，ロボット技術も発展している．この技術とロボット技術の発展に製造業が結びつき，IoT対応の制御システムが普及しはじめている

①IoTの発展 様々な事業・情報がデー タ化・ネットワークを用いて，自由にやりとり可能に	②ビッグデータの発展 大量のデータの分析・解析を行うことが可能に
③AI（人工知能）の発展 機械が自ら学習し，高度な判断が可能に	④ロボットの発展 多様かつ複雑な作業の自動化が可能に

IoT対応の制御システムの普及

例：スマート工場，スマートファクトリー，つながる工場

独国	2011年	Industry4.0
米国	2014年	Industrial Internet
日本	2015年	第四次産業革命
中国	2015年	中国製造2025

IoT対応の制御システムの動向	
日立製作所	共生自律分散制御システム
富士通	スマートなものづくり
三菱電機	e-F@ctory
日本電気	次世代ものづくりソリューショ ン NEC Industrial IoT
東芝	次世代ものづくりソリューショ ン Meister

内部犯行の概要

IPA「内部不正による情報セキュリティインシデント実態調査」（2016年）

内部者の定義
役員，従業員（契約社員を含む），派遣社員等の従業員に準ずる者，元役職員であった者のうち，以下の2点のどちらかを満たした者
①組織の情報システムや情報（ネットワーク，システム，データ）に対して，直接又はネットワークを介したアクセス権限を有する者
②物理的にアクセスしうる職務の者（清掃員や警備員等を除く）

内部犯行の分類	
分類	内部犯行の例
システム破壊	システムの破壊や改ざん
知的財産の窃盗	顧客情報等の職務で得た情報の持ち出し
システム悪用	情報売買等，職務で得た情報の目的外利用
意図しない不正	ミスや不注意によるルールや規則の違反
その他	上記以外のルールや規則の違反

IPA「組織における内部不正防止ガイドライン」（2017年）

内部不正防止の基本原則	
基本原則	対策
犯行を難しくする	対策を強化する
捕まるリスクを高める	管理や監視を強化する
犯行の見返りを減らす	標的を隠す，排除，利益を得にくくする
犯行の誘因を減らす	犯罪を行う気持ちにさせない
犯罪の弁明をさせない	自らの行為の正当化理由を排除

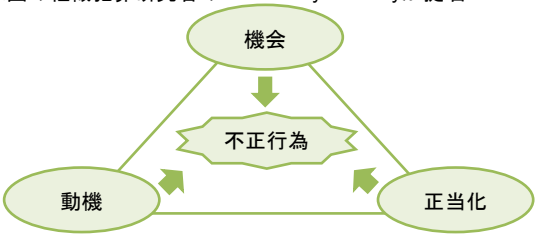
IoT対応の制御システムにおける内部犯行対策では，内部犯行者の定義及び内部犯行の分類や対策が変わる

内部者はアクセス権限を持つ場合が多く，アクセス制限等の技術的対策だけでは限界がある為，心理学に着目をして考察

犯罪心理学

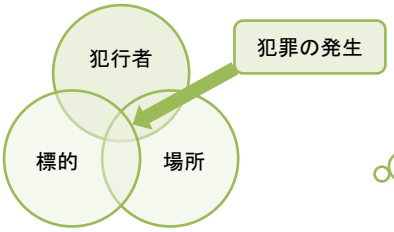
①不正のトライアングル

米国の組織犯罪研究者のDonald Ray Cresseyが提唱



②日常活動理論（Routine Activity Theory）

Marcus FelsonとLaurence Jonathan Cohenが提唱



IoT対応の制御システムの発展に伴い，従来の内部者，外部者の概念に加えて，中部者の様な内部者でも外部者でもない概念が必要になると考える

今後の研究方針

①研究対象範囲を絞る，②研究目標を定め実験を行う，③IoT対応の制御システムの発展に貢献する研究を行い，安心安全で便利な社会を目指す