

フォグコンピューティングを利用した IoTシステムのセキュリティに関する研究

Study on the IoT system using fog computing

丹羽雅哉・マネジメント分科会・情報セキュリティ大学院大学

In recent years, the number of various IoT devices has increased year by year, and investigations or developments of systems for storing, and analyzing information acquired by IoT devices are under way. For such researches and developments, it is necessary to consider security not only for individual devices but also for whole system. However, IoT devices often have limited power and limited memory, therefore, it is difficult for IoT devices alone to take adequate security countermeasures against various threats. Under such circumstances, we consider to apply Fog Computing to a system architecture for organizing the assumed threats and security requirements in the IoT system and realizing the requirements.

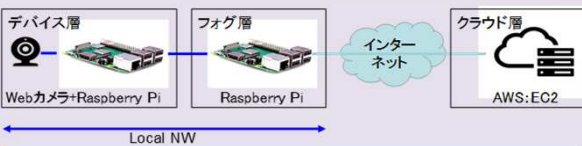
■背景

現在、様々なIoTデバイスで収集された情報を蓄積し、分析などを行うシステムの検討/開発が進められている。検討/開発が進み、複数のIoTデバイスやサーバを含むシステムをサービス化していく中で、デバイス単体だけでなく、システム全体としてセキュリティを考慮する必要がある。

■実施内容

IoTシステムの特徴や想定脅威を整理し、脅威に対するアーキテクチャとしてフォグコンピューティングを検討した。フォグコンピューティングの考え方を基に、監視カメラを想定したIoTシステムを検証環境として構築し、セキュリティ要件の実現性確認/性能測定/脆弱性診断を行った。

■検証環境



■性能測定 ※1MBの画像ファイル転送

デバイス→フォグ(ローカル) フォグ→クラウド(インターネット)

ftp	平分 1.0秒	ftp	平分 3.0秒
MQTT	平分 0.8秒	MQTT	平分 1.6秒
HTTP	平分 0.7秒	MQTT 暗号化	1.9秒

■実現性確認

ファイル改ざん監視:不正利用の監視



■脆弱性診断

OpenVASによる脆弱性診断を行い、監視ツールへのアクセスを平文で行うことの危険性や、ファイル転送時のアクセス制御、ユーザ認証を怠ると攻撃を受ける可能性があることを、再度確認した。

■課題

非力なデバイスでの検証、デバイスやフォグノードの台数を増やしたより複雑な構成での検証、スマートフォンをフォグノードとした場合の検討/検証が今後の課題と考えられる。

脅威	フォグノードで推奨される対策
不正アクセス	外部からの不正な通信を防ぐため、インバウンドを必要最低限とする。 内部からの外部への不正な通信を防ぐため、アウトバウンドを必要最低限とする。 アクセスログを管理する。
情報の改ざん なりすまし	IoTデバイスやフォグノードから送信される情報の改ざんを防ぐため、メッセージ認証を行う。 IoTデバイスやフォグノードのなりすましを防ぐため、認証を行う。
不正利用	踏み台とならないよう、不正アクセスを防ぐと共に、意図しないプロセスなどが動作していないか監視する。 IoTデバイスが不正な設定で動作しないよう、IoTデバイスを監視する。 操作ログを管理する。
情報の漏洩 盗聴	資産であるファイルや公開ディレクトリなどがある場合は、アクセス制御を行う。 TLSなどにより、通信の暗号化を行う。途中のルートが信用できない場合、エンドツーエンドの暗号化する。
ウイルス感染	予防として、不正なアクセスを防ぐ 監視を行い、通常と異なる動作を検出する。 監視で不正動作を検出した際に、場合によってはIoTデバイスを切り離したり、初期化(再起動)などのリカバリを行う。
DoS	IDS/IPSなどにより、検知/遮断する。
情報の消失、破損	定期的にデータのバックアップを行う。