スマートエ場における運用シナリオに基づく5Gの脅威分析

Takahashi Hideaki <takahashi.Hideaki.tg8@is.naist.jp>

Abstract 第5世代移動通信システム(5G)は、複数の異なる種類の技術を統合することにより、移動通信ネットワークに大きな革新をもたらすとされており、3GPPがrelease15で定義した高速大容量通信(eMBB:enhanced Mobile Broadband)、超高信頼低遅延(URLLC:Ultra-Reliable and Low Latency Communications)、及び超大量端末の接続(mMTC:massive Machine Type Communication)のシナリオ実現に向け開発されている. しかしながら、5Gの脅威分析は、5Gの大規模性やユースケースの多様性に起因して、具体的な脅威分析に至っていない. また、5Gに実装されるネットワーク機能の仮想化(NFV: Network Function Virtualization)については、基地局や5Gのパケットコア(5GC)におけるネットワーク機能を仮想化により実現する役割を有する. そのため5Gの持続的な運用の観点からNFVは、特にセキュリティが重要視される中核技術である. しかしながらNFVの脅威分析についても、5Gの具体的な脅威分析をもとに行われていないため、そのセキュリティ機構が安定した5Gの運用に寄与できるものか検討できていない. そこで本稿では、ユースケースを用いた脅威分析を実施し、5G脅威の具体化を試みることで、当脅威分析手法の有用性と将来の移動通信システムにおける脅威分析で着意すべき事項を検討する.

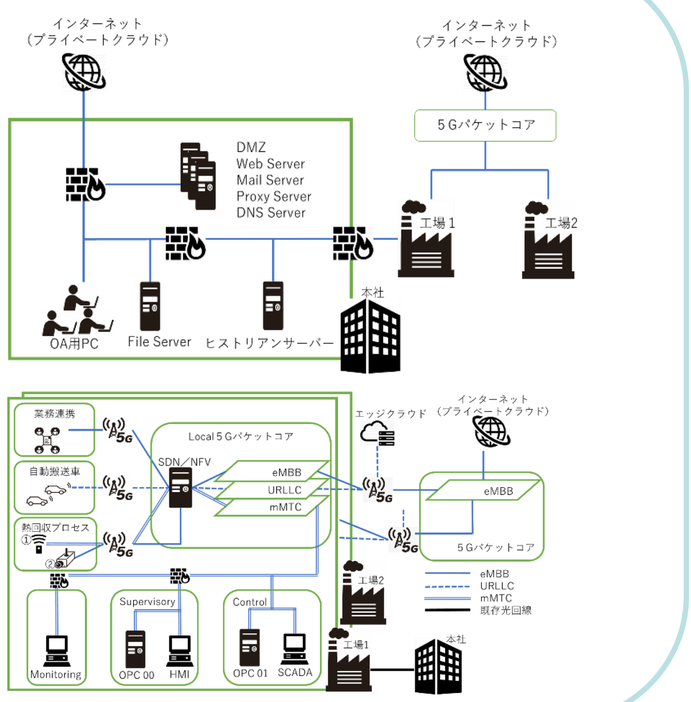
Background & Motivation

・5Gでは運用形態の柔軟性を拡充することに相まって、一般社会や重要インフラで用いられる5Gに対する依存度が高まる.
・NFVは、5Gの中核技術とされ、5Gサービスの持続的運用に供するため、特にセキュリティが求められる.
・5GにおけるNFVの有用性から、開発が近年盛んに行われている. しかしながら、これらは機能拡充が主な目的であり、5Gの脅威を考慮したものとは言えず、5Gの持続的運用に供せるものか検討できていない.

→ 5Gの持続的運用を可能としながら高度なセキュリティ機能を提供することを目的として、特定の5Gユースケースを想定し、そこに存在する利害関係者及びその役割・管理する資産を明確にするとともに、利害関係者間の責任分界点を決定する事でユースケースに応じた具体的な脅威を明らかにする必要がある.

Proposed Idea and Methodology

手順1 5Gユースケースの想定



手順2 責任分界点の明確化

分類	利害関係者	役割	責任範囲	資産	関連する形態
①	VISP	RAN領域役務提供 NFVOaaSの提供	端末-Local5Gエンドポイント間通信の24時間運用保証 NFVOテナント管理 NFVOの24時間運用保証	RAN領域設備 NFVOaaS環境 (NFVO、NFVM) NFVO加入テナントデータ	形態1及び2
	IIoT - SP	IIoT機器設定・保守	IIoT機器の24時間運用保証	IIoT機器の想定情報	形態1及び2
②	DCSP	IaaS環境の提供	プライベートクラウド環境の保証	IaaS環境	形態2
	全国MNO	5G網の保守・整備 エッジクラウドの提供	Local5Gエンドポイント-所要サービス間通信管理 エッジクラウド管理	5G通信網 5G加入者情報 エッジクラウド基盤	形態2
③	事業部	出荷管理 在庫管理	出荷・在庫データの加工と保管	データベース 加工済みデータ	形態1及び2
	製造部	生産計画調整 製造、搬送	IIoT機器運用 Rawデータの保護 DBへの転送	生産データ センシングデータ IIoT機器	形態1及び2
	情シス	Local5Gにおける端末・加入者の管理 NFVOの運用 NFVIの保守・整備 セキュリティ	端末-Local5Gエンドポイント間通信管理 テナントとしてNFVO管理 VNF管理 VIM、NFVI管理	基幹LAN Local5G加入者情報 NFV構成データ(VNFD、NSD、NST等)、VNF、VIM、NFVI	形態1及び2

手順3 脅威の優先付け・脅威の具体化

キルチェーン	キルチェーン①	キルチェーン②	キルチェーン③
攻撃概要	NW構成変更	仮想NWへの侵入	アクセスポイントの有線コネクタへの接続
目的	NFVOにおける可用性喪失(ID:T826)	Local5GNWへの侵入(ID: T883)	運用情報の盗聴(ID:T882)
偵察	ヒストリアンサーバーの侵害(ID:T810) OPCプロトコルによる情報収集(ID:T802)	ヒストリアンサーバーの侵害(ID:T810) OPCプロトコルによる情報収集(ID:T802)	アクセスポイント設置場所の確認
武器化	RATツールの準備[14]	RATツールの準備[14]	スプリッターの準備
配送	スピアフィッシングアタッチメント(ID:T865) USBを介したレプリケーション (ID:T847)	スピアフィッシングアタッチメント(ID:T865) USBを介したレプリケーション(ID:T847)	保守点検に偽装し侵入
攻撃	悪性ファイル実行	悪性ファイル実行	スプリッター及びラズパイの設置
インストール	バックドア配置	バックドア配置	外部への通信手段確保
遠隔操作	C2通信	C2通信	—
侵入拡大	NFVOアカウントの調査	NW横展開	—
目的実行	NFVOログイン NFV構成データ改ざん	SupervisorNW 侵入とデータ改ざん/搾取	NFVO認証情報 端末/加入者情報の盗聴

Result

・複数の利害関係者が介在する 5G システムにおいて、 責任分界点を明確にし、脅威分析対象の決定や脅威の 優先付け・具体化を実施できた点において、ユースケ ースを用いた脅威分析手法の有用性は示されたと考える.
・本稿では、5G における脅威の具体化という目的 から、スマート工場の責任分界に限定して脅威分析を 実施した. 一方で、5G 以降の移動通信システムは、シ ステム全体に存在する利害関係者数が増大し、システ ムの保守・運用においては利害関係者の環境整備状況 への依存度が高まることが考えられる.

考察1: VISP や全国 MNO 等の責任分界における脅威について も具体化する必要がある.
考察2: NFV などの 5G 中核 技術に関するセキュリティ対策の検討については、ユ ースケースを用いた脅威分析によって具体化された脅威を考慮するべきであり、NFVO、VNFM の NFV 管理 層や NFVI のリソース層、VNF のインスタンス層をどの責任分界において管理されるのかを検討することが 重要であると考える.
考察3: 既存のセキュリティフレームワークで対応させる場合 の解決策として、仮想化資産と仮想化していない資産 を分離して管理することが望ましいと考えられる. 仮 想化資産については、動的に変化し得る仮想化資産を 単位として管理するのではなく、ユースケースに基づ くライフサイクルを定めたルール(ポリシー)を単位 として管理する必要があると考える. また、仮想化資産に対する脅威分析については、当該ポリシーを管理 する責任分界において実施されるべきである.

Conclusion and Future Work

今後の課題としては、今回想定したスマート工場以外の利害関係者が主管する責任分解において存在する脅威を具体化する必要がある. また、FA、PA分野のみの検討であるため、他分野の検討についても、同等の検討する必要がある. この2点を実施することで、5G脅威の効果的な対策立案に寄与できると考えられる.