# 平成27年度 情報工学コース卒業研究報告要旨

| 高田・本田 研究室 | 氏　　名 | 青 木 克 憲 |
|---|---|---|
| 卒業研究題目 | Ethernet AVB のセキュリティ分析と対策 | |

Ethernet AVB（Audio Video Bridging．以降，AVB と呼ぶ）は元々マルチメディア向けのプロトコルであるが，リアルタイム性や帯域保証ができる特徴を活かし，自動車制御システムなどのセーフティ・クリティカルシステムで使用されることが検討されている．セーフティ・クリティカルシステムでは故障や障害によって人命や人への深刻な被害を出さないことが求められる．現時点での Ethernet AVB 仕様ではセキュリティが考慮されていないので，セーフティ・クリティカルシステムの基盤ネットワークとして使用された場合，セキュリティの脅威によって，セキュリティ・インシデントを引き起こす可能性がある．AVB に関わるのは Talker，Listener，スイッチと呼ばれる 3 つの主体である．Talker から Listener への定常的なデータ（パケット）の流れをストリームと呼び，スイッチはストリームの中継をする．AVB では，通信相手のなりすましや，ストリームの意図しない切断は考慮されていない．これらの潜在的な脅威を洗い出し，それに対策した上でセキュリティ・クリティカルシステムへ導入すべきと考える．本研究では，Ethernet AVB のセーフティ・クリティカルシステムでの利用を見据え，システムの安全性や可用性の侵害につながる，AVB の特徴を悪用した攻撃方法を明らかにするためにセキュリティ分析を実施し，セキュリティの攻撃のリスクを低減する対策を提案する．

セキュリティ分析では，まずガイドワードを用いた分析を行った．あるパケットのフィールドやプロトコルの仕様にガイドワードの動作を適用すると，発生しうる影響や攻撃を発想することができる．次に，Attack Tree のアタックゴール（攻撃者の最終目標）を実現する具体的な攻撃手法をガイドワードによる分析結果を用いて導出して Attack Tree を作成した．作成した Attack Tree からストリームや帯域保証といった AVB の特徴を悪用した攻撃を選定し，それらのシステムの可用性・安全性に関わる影響を考察した．

次に，選定した攻撃を実証した上で，それぞれの脅威の発生を防止する対策を検討した．実証環境は Open-AVB をベースとしたシンプルな AVB ネットワークである．複雑なネットワーク構成における解析は今後の課題とする．実証実験により，「Talker のなりすまし」「ストリームの不当な切断」「Jamming による通信の妨害」の 3 つが明らかになった．Talker のなりすましでは，第三者によって正当な Talker になりすましたパケットを流し Listener に処理させることができた．この脅威の対策として，Talker からのストリームにメッセージ認証コードをつけることを提案する．また実装によってはこのペイロードによって脆弱性が突かれたり，不具合を引き起こしたりする．開発の設計段階で脅威分析を実施し，なるべく早い段階で，できる限り脆弱性をなくす開発プロセスを導入することを提案する．ストリームの不当な切断では，第三者によって勝手にストリームを切断できることを示した．この脅威の対策として，Listener からのストリームの開始・終了に関わるメッセージにメッセージ認証コードを適用することを提案する．Jamming による特定条件でのスイッチへの干渉では，Jamming による通信の妨害では，スイッチにおいて，特定の優先度をもつパケットを優先的に転送するよう設定されていると，その優先度以上の優先度をもつ無意味なパケットを大量に送信することで，正常なパケットの応答時間を遅延させることができることを確認した．スイッチの送信ポートの設定において，複数の受信ポートから，送信パケットを順番に選択するよう設定することで，この攻撃の影響を小さく抑えることができることを明らかにした．今後は，さらに多くの攻撃方法を試し，適切なスイッチ設定を多面的に評価したいと考えている．