



2018 年 3 月 2 日 金曜日

## SEC 道後 2018 学生研究賞受賞研究発表会

森井先生から研究賞の趣旨が述べられたあと小林実行委員長から表彰状が以下の 4 名の方に授与された。最優秀賞は投票によりシンポジウムの最後に発表される。

(1) 研究題目：「BGP 経路情報の変更データ観測による Mis-Origination 発生可能性分析」

発表者：安藤 正仁 (東邦大)

発表内容：BGP の経路情報において乗っ取り (Mis-Origination) が行われる可能性がある。乗っ取りが行われているかどうか観測する手法を提案した。

(2) 研究題目：「指向性スピーカを用いた音声認識装置への攻撃と評価」

発表者：飯島 涼 (早稲田大)

発表内容：指向性スピーカを使えば音声認識可能なスマートデバイスを遠隔操作できるかを検証し、ある条件で攻撃が成功することを示した。

(3) 研究題目：「ブロック暗号へのプロービング攻撃における鍵復元効率の正確な評価モデル」

発表者：庄司 奈津 (電通大)

発表内容：物理攻撃の一つでデバイスに穴をあけて暗号鍵を導出するプロービング攻撃について鍵導出までに必要なプロービング回数を正確に求める式を導出した。

(4) 研究題目：「Research on Integrated Authentication Using Passwordless Authentication Method」

発表者：森井理智 (徳島大)

発表内容：大学では多くのサービスがあり複数のログイン処理が必要になる。大学のパスワード管理を容易にするために、Shibboleth に FIDO を導入した認証システムの実現方法を示し、セキュリティリスクを検証した。



安藤 正仁 (東邦大)



飯島 涼 (早稲田大)

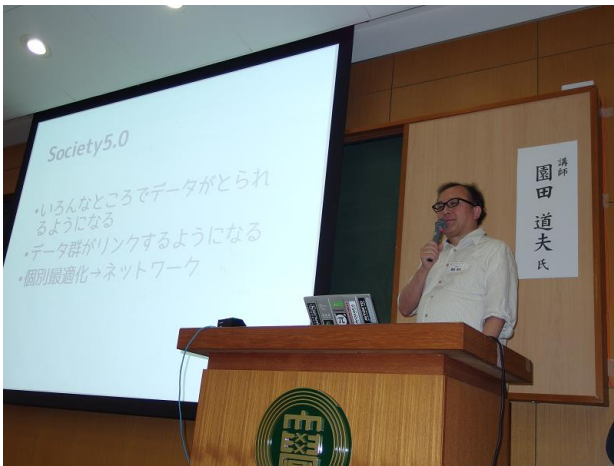


庄司 奈津 (電通大)



森井理智 (徳島大)

## 講演(3)



国立研究開発法人情報通信研究機構ナショナルサイバートレーニングセンター センター長 園田道夫氏により「Society5.0時代のセキュリティ」というテーマで講演が行われた。Society5.0では収集されたデータを分析することで便利な社会の実現が期待できるが、データ収集においてデータの汚染を完全に防ぐことは難しい。攻撃者にとって有用な結果を導く

ようなノイズの混入やデータの学習機械をだます研究も進んでいる。このような攻撃に対応するために、モデルを抽象化・ネットワーク化した設計が有効かもしれない。また、データによる学習のために、変化の急激なデータに対して良い具合のデータセットの開発・実装が必要である。

CTF、ハッカソンやセキュリティキャンプなどの活動により、セキュリティをもの作りで何とかしたいと考えている。良いものを作って、攻撃コストを上げることを目指している。