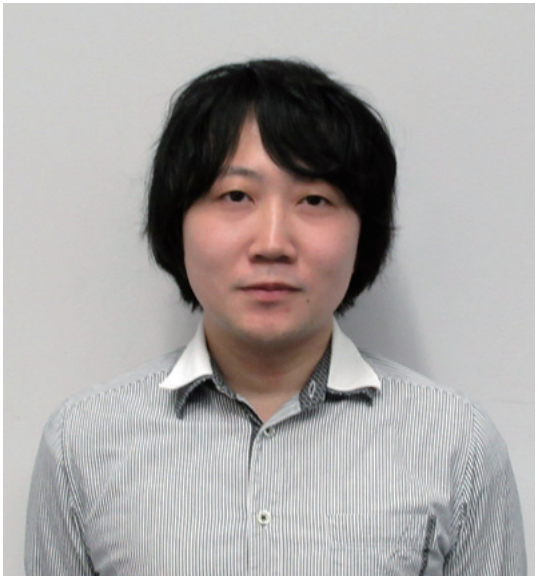
主役登場

サイバー攻撃の先を行くために



渡邉　卓弥
NTTセキュアプラットフォーム研究所
社員

私の頭の中にある一番古い記憶は，幼稚園のときに大流行していたゲームで家族と対戦する光景です．小さな子どもがゲームで遊ぶことは当時すでに珍しくなく，友人の家にもコントローラーを持ち寄りよく遊んだことを覚えています．私はその中でもとにかく「やりこむ」タイプで，自分より強い相手を探しては，勝つまで執念深く対策を重ねていました．この姿勢は年月を経ても変わらず，解決しがたい問題に直面するたび，寝ても覚めても研究のことを考えてしまいます．「相手を上回るように，行動を予測して戦略を練る」．サイバーセキュリティと対戦ゲームはとてもよく似ています．これは数あるコンピュータサイエンス分野の中でも，打ち負かすべき相手と対峙するサイバーセキュリティだけが持つ特別な性質であり，私がやりがいを持って研究に臨める大きな理由だと考えています．

サイバー攻撃がときに会社業績や人命にまで影響を及ぼす以上，私たちは相手を上回るためのより良い方法論を考え詰め，実行しなくてはなりません．一度発生した攻撃を二度と受けないようにすることも非常に大切です．NTTでは，改ざんサイトを巡回し挙動を記録するハニーポットや，マルウェア感染端末を解析するフォレンジックなどによって攻撃の特徴をとらえることで，防御のためのインテリジェンスを創出しています．しかし，皆様にとって究極の理想は，攻撃が一度も発生せずに通用しなくなることではないでしょうか．このような思いから，私たちは攻撃者の視点に立ち新たな脅威を実証するというアプローチによって，サイバー攻撃に先回りして対策を講じる「脅威実証研究」を立ち上げました．

脅威実証研究の難しさの１つに，プログラムの欠陥を闇雲に探していてはきりがないという点があります．私たちは特定のプログラムのバグだけではなく，一般的な機能に潜在する問題を見つけ出すことで，影響範囲の広い脅威からユーザを保護することをめざしています．もう１つの難しさは，発見した脅威を隠しておけば気付かないうちに攻撃が発生する可能性があり，公開すれば悪意ある人物に模倣されるかもしれないというジレンマです．私たちは，情報を一般公開する前に事業会社や公的機関と連携することであらかじめ対策を施し，適切なタイミングになったらマスメディアなどを介して広く周知し，多くの方が脅威と対策を認識できるよう心掛けています．

脅威実証研究は，世界的なトレンドにもなりつつあります．2018年の初頭に業界を騒がせたSpectreやMeltdown，そして私たちが発見したSilhouette．いずれも研究者が発見した脅威でありながら，製品やサービスに新たなセキュリティ機構を組み込ませ，早期に攻撃の芽を摘み取ることに成功しました．私はこの取り組みに強い手ごたえを感じていますが，脅威の発見が研究者の経験や技量に依存するという課題もあります．今後，私たちは新しい脅威を発見し対策するための属人的でない研究サイクルを模索し，安全なインターネット環境を持続的に提供できるよう努めていきます．