Vol.2020-CSEC-91 No.14
Vol.2020-SPT-40 No.14
Vol.2020-EIP-90 No.14
2020/11/25

組織の情報セキュリティインシデント対処を振返ると、

鳥居悟 [1]

概要：昨今，特定の組織を対象としたサイバー攻撃の被害事例が多数公表されている．一方で，これまで，組織が保有する情報資産をさまざまな脅威から守るため，多くの研究開発が行われてきている．このような行きつ戻りつの関係は，利用環境の変化と攻撃手口の巧妙化に伴い，長期に渡って繰り広げられている．
特に，APT(Advanced Persistent Threat)と呼ばれる特定組織や個人に対する標的型攻撃は，長期に渡って侵入した組織の内部ネットワークに潜伏し活動を続ける点で，これまでの攻撃手口とは顕著な違いがある．すなわち，守りを固める既存の要塞型セキュリティ対策だけでは対応が困難であり，すでに侵入されていることを前提として，出来る限り早期に検知し被害を最小限に抑えることが求められる．特に，組織内においてこのような不審な挙動を監視するには，正常な業務通信を不正な攻撃通信と見誤らないようにすることが求められる．
本発表では，まず，組織における脅威の変遷を整理する．次に，これまで筆者が取り組んできた，内部ネットワークに侵入したマルウェアの挙動に着目してラテラルムーブメントを検知する技術，外部との通信セッションの特徴に着目して制御サーバとの通信を検知する技術などを紹介する．最後に，これらの対策においては多種多様な監視ログを適切に分析することが重要との観点から，これらログ分析に関する取り組みを紹介する．

キーワード：APT，内部対策，ラテラルムーブメント，C&C 通信，行動特性，データサイエンス

Historical Study on Response of Security Incidents in Organizations

Satoru TORII [†1]

1 株式会社富士通研究所
FUJITSU LABORATORIES LTD.