セキュリティ攻撃・防御戦略のリアルタイム意思決定モデルの提案

Real time decision making models for security attack and defense strategies

情報セキュリティ大学院大学

鈴木　亜矢子

＜要旨＞

現在広く実施されているセキュリティ対策は、インシデントの発生を未然に防ぐための事前対策が中心である。もし、事前対策を行っているにも関わらずインシデントが発生した場合、システムの管理者は攻撃に対し防御策を検討し、行動を取らなければならない。しかし、事前対策のみでは、平均的に最も大きなリスクをもたらすと想定される攻撃を推定して対策を重点化し固定的に適用するため、攻撃者が事前対策を調べあげ、想定外の攻撃をしかけた場合に即応しにくいという欠点がある。

この課題を解決する方針として、本検討では攻撃者はリスク最大化を、防御者はリスク最小化を図るよう行動すると仮定し、攻撃の進行過程において、攻撃状況から動的にリスク評価を行い、セキュリティ対策をリアルタイムに逐次意思決定することで、効果的に防御を行うための意思決定モデルを検討した。また、モデルを定式化し、適用例により検証を行った。

＜Abstract＞

Currently security measures are chosen preceding to occurrence of incidents, and static defense with them are mainly applied. This proactive and static defense has disadvantage that it cannot respond quickly to unanticipated attacks, because it is generally tuned so as to be most useful against the attacks estimated to happen with the highest probability on average. In order to solve the above problem of the conventional security defense, this study discussed real-time and dynamic decision making process including both of attacker and defender, under the game-theoretical assumption that attacker will act to maximize security risks while defender minimizes them. We developed a decision-making model corresponding to the process of attacks and defenses, where security gains and risks are assessed during the attack alternately by the attacker and the defender, and optimum attack and defense plans are sequentially determined step-by-step and put into practice in real-time. Further the proposed model was formulated and its effectiveness was examined with some application examples.