情報システムの脆弱性に対する客観的評価手法の提案

Proposal of objective assessment approach to vulnerability of information systems

亀谷 直希

Naoki Kamegai

＜要旨＞

昨今，セキュリティに関するインシデントが数多く報告されており，自組織で管理している情報システムのインシデントが発生しないように脆弱性評価を行うことが必要不可欠であるといえる．情報システムの環境に応じた脆弱性に対する影響を評価する場合に，一般的に使用される手法として，CVSS（共通脆弱性評価システム）がある．CVSS には，基本評価基準，現状評価基準，環境評価基準があり，情報システムの環境に対する脆弱性評価を実施する場合，現状評価基準や環境評価基準を用いるが，主観的要素が含まれるため，評価者によって結果が異なる可能性がある．本研究では，基本評価基準と，脆弱性検査結果得られる攻撃成功時間を用いて，客観的に評価値を算出する方法を提案する．従来手法と提案法を比較した実験を行って提案手法が有効であるという見通しを得た．

<Abstract>

It is essential for every organization to perform vulnerability assessment to avoid the security incidents of own system because a lot of security incidents have been reported recently. In case of evaluating the vulnerability impact, CVSS (common vulnerability assessment system) is often used. CVSS includes three metrics; base metrics, temporal metrics, and environment metrics. When the vulnerability assessment is performed about the actual environment of the information system, temporal metrics and environment metrics are employed conventionally. However, these two metrics have a defect that their evaluation results depend on the evaluators because these metrics use subjective scores of the evaluators. We therefore discuss how to evaluate vulnerability of the actual environment objectively, and develop a new metric called actual metric. Here, this actual metric is given as the base metrics normalized by the attack time, which is the duration of an attack until the attack finishes successfully and measured by a vulnerability assessment tool. Based on comparative experiments between the conventional and proposed actual metric, we found that the actual metric could evaluate reasonably and replace the conventional metric.