第三者機関によるネットワーク・フォレンジックシステムの提案

Proposal of Network Forensic System for Third-Party Certification

情報セキュリティ大学院大学
金　東佑

＜要旨＞

企業や組織が考えるべき情報セキュリティ対策の中で情報セキュリティインシデントが発生した場合，法的問題への対応に必要なデジタルデータの証拠を確保する技術であるデジタル・フォレンジックが注目されてきている．

デジタル・フォレンジックの証拠性を考慮した際には，正確な時刻，原本性証明，第三者への証明という三つの要素が求められる．これにより，デジタル・フォレンジックの機能としては，ある時刻に確かにデータが存在し，かつ改ざんがされていないことを第三者へ証明できることが必要である．

本研究では，インシデント・レスポンスの事後対応で使われるデジタル・フォレンジックの中で特にネットワーク・フォレンジック技術に着目して，それに時刻認証技術を組み合わせることで，従来のネットワーク．フォレンジックシステムでは実現できなかった高い証拠生を持つ新たなネットワーク・フォレンジックシステムについて提案する．

＜Abstract＞

Recently, much attention has been paid to digital forensic system, as one of the useful security measures for enterprises and organizations. The digital forensic system is expected to collect and save digital proof believed to be helpful for handling legal problems after security incidents. The digital forensic system is required to assure the following three factors; time accuracy, originality, and objectivity, to the third party. By satisfying the above three factors, the digital forensic system can prove the fact that the concerned data actually existed at a specified time and has not been falsified.

This study highlights network forensic technology gathering digital communication data on line. By using the time authentication technique, it especially proposes a method to authenticate the time accuracy of communication data, which remarkably improves proving ability of conventional digital forensic system.