デジタルフォレンジック

JJ1SXA/池

デジタルフォレンジックなる言葉を聞いて、これは何ぞや？と疑問を持ち一寸調べてみました、デジタルフォレンジックとは、犯罪捜査や法的紛争などで、コンピュータなどの電子機器に残る記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称で、「forensics」には「法医学」「科学捜査」「鑑識」といった意味があり、分かりやすく意訳すれば「デジタル鑑識」ということのようだ。

対象となるのはパソコンやサーバ、ネットワーク機器、携帯電話、情報家電など、デジタルデータを扱う機器全般、事件の関係先の機器を押収して記憶装置から証拠となるデータを抽出したり、サーバや通信機器などに蓄積された通信記録から違法行為の証拠となる活動記録を割り出したり、破壊・消去された記憶装置を復元して証拠となるデータを割り出したりといった技術・活動が該当する。

また、コピーや消去、改ざんが容易であるというデジタルデータの性質に対応して、データが捏造されたものかどうかを検証する技術や、記録の段階でデータが改ざんできないよう工夫したり、ハッシュ値やデジタル署名などで同一性を保全する技術なども含まれる。

不正アクセスや機密情報漏洩など、コンピュータや通信ネットワークに直接関係する犯罪における捜査手法として注目されたが、社会への IT の普及・浸透に伴って、一般の刑事事件などでも捜査や立証に活用されるようになってきている。

ここに、「ハッシュ値…hash value」なる用語がでてきたが、ハッシュ値とは、元になるデータから一定の計算手順により求められた固定長の値、その性質から暗号や認証、データ構造などに応用されている。

ハッシュ値を求めるための計算手順のことをハッシュ関数、要約関数、メッセージダイジェスト関数などというようだ。

デジタル署名とは、送信されてきたデータが間違いなく本人のものであるのかを証明するのための技術、 デジタル署名はデータの送信者を証明できるので、データの改ざんが行われていないことを確認できます。

デジタル署名は公開鍵暗号を応用した技術でもあり、デジタル署名の仕組みのなかで公開鍵と秘密鍵も 登場します。ハッシュも使用しています。デジタル署名を実現できる方式には RSA や DSA などがあります。

デジタル署名では、データだけでなく、データをハッシュ値にしてからこれを署名として受信者に送信します、受信者は、受信したデータからハッシュ値を算出し、署名として受け取ったハッシュ値と比較することにより データが改ざんされていないことを確認できますとのこと、また、第三者が知ることができない秘密鍵でハッシュ値を暗号化して送信するため、データとハッシュ値の両方が改ざんされたものを受信しても改ざんを検知できますとのこと。

（2022 年 9 月記）