情報ネットワークのセキュリティ向上対策

東京電機大学　宮保憲治

要旨

本講演では、広域に分散されたクラウドのストレージリソースを超分散ネットワーク、高速ストリーム暗号、シャフリング技術、閾値秘密分散技術等を活用して、安全かつ低コストでファイルバックアップを実現し、従来技術に比べ、飛躍的にセキュリティを向上できるディザスタリカバリ技術を述べる。この技術は、企業や行政活動に対する基盤情報である重要電子データに対して、地震や火災等の自然災害やサイバー攻撃等を受けた場合でも、安全にバックアップを実現可能にする社会的要請に応え得るものである。国内外の通信環境に着目すると, 広域分散されたクラウドストレージに加え、PC、スマートフォン、NAS(Network Address Storage) 等を分散ネットワーク、高速ストリーム暗号等を活用して、ランダムに分散された断片化ファイル群を一つのファイルと見なして統合管理する技術の実現が可能である。本講演ではこれらの要素技術を用いたアーキテクチャと実用化構成例を述べる。具体的にはバッククアップサービスの提供事業者がユーザからの要望に応じ、保管対象とするファイルに対して、分割数（m）と冗長（複製）数（n）を設定する。 バックアップ用のエンジンは、分割数（m）の増減により、セキュリティレベルの高低を調整できる。この理由は元データのファイル分割後のファイルの並び替えの組み合わせ数が m! に比例するからである。また、断片ファイルの複製数（n）の増減により可用性の高低を調整でき、シャフリングと転送先のランダム選択技術を適切に組み合わせることにより、高いセキュリティと完全性（復元確率の向上）が同時に実現できる。このように本技術は、暗号化前の平文に対して、毎回、あるいは定期的に異なる乱数を用いて高速ストリーム暗号化を行った後、一体化と称する空間的な撹拌処理を行う。更にユーザの要求レベルに応じてファイルの最適分割・複製・再暗号化を行い、冗長化した断片ファイル群を作成する。本技術は HS-DRT(High Security-Distribution and Rake Technology) と呼称する。万が一のディザスター発生時には、冗長に分散保管された一連の暗号化・分割処理に使用した時系列的に用いたパラメータ（以下、メタデータと呼称）を活用して、元ファイルの復号化に必要な断片データだけを回収する。これらの一連の処理エンジンが本技術の核心であり、監視センターへのメタデータ転送を含む逐次的処理を VPN 等のセキュアーなネットワークを活用することにより、高いセキュリティのもとで重要ファイルのバックアップが可能になる。