秘匿・匿名通信の分類に関する研究

川瀬 拓哉 (0810016)

北陸先端科学技術大学院大学 情報科学研究科

2012 年 2 月 6 日

キーワード: 秘匿通信, 匿名通信, 分類, 暗号, プロキシ, オニオンルーティング.

インターネット上で金銭に関わるやりとり等の重要な通信を安全に行うため、通信内容や情報の発信者を隠蔽する技術が利用されている。この技術により、インターネット上で秘匿性や匿名性を確保した通信を行うことが可能となっている。しかし、この秘匿性や匿名性を悪用して、ファイル共有ソフトによる著作権の侵害、掲示板への誹謗中傷の書き込みといった行為が行われ問題となっている。そのため、これらの通信を制御・監視する技術の研究開発が行われ利用されている。両技術の関係はどちらか一方が強い状況になると、悪用が横行したり、安全を確保したサービスの提供が出来なくなる可能性がある。そこで、両技術が対等な関係を維持し続けるため、両技術の関係を明らかにする手法が必要となる。本研究の目的は、数多く存在する秘匿・匿名通信の技術を比較し、制御・監視する者にとって脅威となり得る技術を洗い出す手法の提案である。

本研究では、秘匿・匿名通信を「なんらかの情報を隠蔽する通信」と定義し、この通信を実現する技術を秘匿・匿名技術と呼ぶ。秘匿・匿名通信が隠蔽する情報として、「通信内容・種類」「通信経路」「通信した事実」がある。一般的な定義では、秘匿通信が「通信内容・種類を隠蔽した通信」、匿名通信が「通信経路を隠蔽した通信」に当てはまる。秘匿通信の代表的な技術には、共通鍵方式の AES(Advanced Encryption Standard)、公開鍵方式の RSA 暗号等がある。匿名通信の代表的な技術には、プロキシ, Tor, I2P, Freenet 等がある。3 つ目の「通信した事実の隠蔽」には、ランダムな通信を行って目的の通信を隠蔽する技術や、ステガノグラフィ技術を応用して他の通信に見せかける方法等がある。匿名通信が匿名化のため、秘匿通信の暗号化を行って通信内容・種類の隠蔽もしている場合があるように、多くの秘匿・匿名技術は上記 3 つの情報を隠蔽する技術に排他的に分類することは出来ない。また、ある 2 つの技術が同じ技術に該当したとしても、同じ機能を持っているとは限らず、その特徴を比較するのに使うことは出来ない。

本研究では、情報を隠蔽する行為が「”ある情報”が”ある相手”に対して隠蔽される」という形であることに着目し、”隠蔽する情報 (隠蔽情報)” と”隠蔽する相手 (隠蔽相手)” にあてはまる項目の検討を行った。隠蔽情報と隠蔽相手の項目を検討する上で、TCP/IP におけるアプリケーション層・トランスポート層・ネットワーク層の 3 層に分けることとし、

各層において、隠蔽される可能性のある情報と相手の洗い出しを行った。その結果、隠蔽情報と隠蔽相手の 2 軸を持った表を用いて、各秘匿・匿名技術を比較する方法を提案した。秘匿・匿名技術に提案する表を適用して得られた表は、その技術によって隠蔽可能となる情報と相手を表す。この表を複数の技術間で比べることで、各秘匿・匿名技術の違いを表すことが出来る。

提案した手法の有用性を確認するため、秘匿・匿名技術として HTTP(HyperText Transport Protocol),HTTPS(HyperText Transport Protocol over Secure Socket Layer), プロキシ (Proxy), オニオンルーティング (Tor) を挙げて適用し考察を行った。その結果、各技術間の隠蔽可能とする情報と相手の違いを表すことが出来た。また、技術の組み合わせによって隠蔽可能となる情報を正しく表すことが出来た。しかし、技術によって組み合わせ可能な場合と不可能な場合があり、組み合わせの可否を判断する手法を別に検討する必要がある。また、隠蔽情報と隠蔽相手の洗い出した項目には、まだ考慮しなければならない要素があることが分かった。ただし、この問題に関しては、更に多くの秘匿・匿名技術に適用することで選別を進めることが可能であると考えられる。この手法を用いることで、制御・監視する者にとって脅威となる秘匿・匿名技術を提示することができる。また、新たな秘匿・匿名技術を研究開発する場合にも、既存の技術との関係を明らかにする手段として利用することができる。これらのことから、秘匿・匿名技術と制御・監視技術の対等な関係を維持するために有効な手法であると考える。