研究エッセイ
ESSAY

WWWのセキュリティ

木下　宏揚（神奈川大学大学院工学研究科・教授）

1 まえがき

WWWが研究者の道具から一般の人々の情報伝達手段として用いられるようになり、セキュリティに関する様々な問題が発生している。ひとつは、情報の保護や通信相手の確認など技術的なセキュリティの問題、もう一つは、発信する情報の著作権など法的あるいは倫理的な問題すなわちコンテンツの問題である。以下これらのセキュリティの問題について解説する。

2 WWWの技術的セキュリティ

①サーバのセキュリティ

不特定多数にWWWコンテンツを公開するということは、WWWサーバが不特定多数からの攻撃にさらされることを意味する。クラッカー（不正侵入者、悪意を持った攻撃者）はオペレーティングシステムやサーバのソフトウェアのセキュリティ上の欠陥（セキュリティホール）を利用して侵入し、コンテンツの書き替え、消去、非公開情報の入手などを行ったり、他のサーバへの攻撃の足掛かり（踏み台攻撃）にしたりする。

防止策としては、CERT（http://www.cert.org）などのセキュリティ情報に気を配り、ソフトウェアを安全な状態に保つことが重要である。また、セキュリティ対策に必要なコストと人員を確保できない場合には、信用のできる組織にサーバの管理を委託する（ホスティングサービス）ことも有効である。

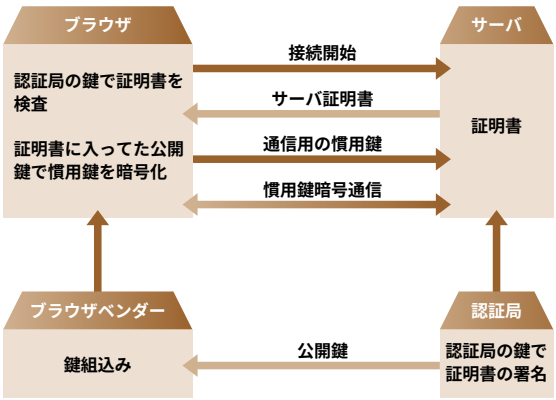
②情報の保護と相手の確認

現在のインターネットは、特別に対策をとらない限りは暗号化されていない生の情報が流れている。しかも、インターネットの盗聴は電話など他の通信手段と比較して容易であるため、個人情報やクレジットカード番号など重要な情報を取り扱う場合、暗号化などの対策が必要となる。

インターネットによる通信の場合、通信相手が本物かどうか確認することも重要である。クライアントとサーバがお互い相手を確認することを認証という。

現在用いられている認証には、証明書、パスワード、

■WWWサーバの認証と暗号化



クッキー、クライアントのアドレス（またはドメイン名）がある。

証明書はサーバの提示するサーバ証明書とクライアントが提示するクライアント証明書がある。証明書は公開鍵暗号を用いたデジタル署名に基づいている。証明書は相手の公開鍵と認証局のデジタル署名などから構成されている。公開鍵は証明書のデジタル署名を確認するとともにセッション鍵（通信用の慣用鍵暗号の鍵）の暗号化に用いられる。次に、提示された公開鍵と相手の結び付きを保証するために認証局のデジタル署名が確認される。主要な認証局（日本ではセコムなど）の公開鍵は予めブラウザに組み込まれており認証局の署名を確認出来るようになっている。図に示すような、サーバ証明書の提示と確認と通信用の暗号化鍵の交換が終了すると、サーバが本物であることと通信路の安全性が保証される。

パスワードは、サーバがクライアントを認証するときに用いられる。サーバが証明書を提示して、暗号化が行われていない状態ではパスワードが生の状態でネットワークを流れるため注意が必要となる。サーバは接続を許可するクライアントをIPアドレスやドメイン名（hertz.ee.kanagawa-u.ac.jpなど）で指定することもできる。

クッキーは、クライアントの身元を保証するものでは

ないが、サーバがクライアントの同一性を確認するものである。例えば、オンラインショッピングで、商品の選択、支払い方法の指定、配送先の指定など一連のセッションの間、あるいは後日再びセッションを開始したときに同じクライアントであることを識別する。サーバにセキュリティホールがある場合クッキーが第三者に掠め取られる危険性があるため注意が必要である。

③WWWのコンテンツの問題

①著作権など

WWWは世界規模で不特定多数の者に情報を提供可能なメディアであり、個人的なコンテンツであったとしても著作権は出版物や放送などと同等に扱われる。コンテンツで問題となるのは、他人が著作権を保有している情報を意図的あるいは無意識にコンテンツに含めてしまうことである。著作権法では、これは複製に該当するが、個人的あるいは家庭など小さな規模のグループ内での使用に限り複製は認められる。したがって、パスワード認証やIPアドレスでの認証を適切に行えば、この範囲内になる場合もあるが、個別の事例により微妙な判断が要求されるので、十分注意が必要である。また自分で撮影したものであっても被写体によっては肖像権（主に一般人）やパブリシティ権（有名人）の侵害になる可能性がある。自分で撮影した建築物の写真は一般には著作権の対象にはならないが、テーマパーク内の建物など建物自体に高度の芸術性、創造性、商品価値がある場合には注意が必要である。国により異なるが、日本では著作権は権利者の死後50年で消滅し、これ以降許可なく情報を利用できるが、対象物の著作権が消滅していても書籍など出版物から転載する場合には著作隣接権（演奏者やメディアの制作者の権利）が存在している場合がある。また、個々のデータが著作権をクリアしていたとしても、これらを体系立てて収集し、データベース化した場合、データベースに著作権が発生する。

②リンク

WWWの特徴としてリンクが挙げられる。リンクにより世界中の情報が有機的に結合され、紙の情報では得られない効率で情報収集することが可能となっている。リンクの問題としては、他サイトへのリンクを張る場合の許諾、リンク先のコンテンツの責任、リンクの方法に分類できる。

他サイトへリンクは、著作権法上は引用に該当すると考えられるので、法的には相手に許可を求める必要はない。しかし、倫理的な問題は別であり、次のように考えればトラブルとなる可能性は低いと考えられる。リンク先のページにリンクにたいする指示がある場合は原則としてそれに従う。大企業や大学全体のサイトなど規模が大きく公共性が高いと考えられるサイトに対しては管理者の手間も考慮すると許可を求める必要はない。個人や研究室単位など比較的小規模のサイトの場合は許可を求めた方が無難である。

リンク先のコンテンツには一般的には責任は生じないと考えられるが、リンクの説明内容によっては問題が発生する場合がある。同一組織内へのリンクの場合、リンクの有無に関わらず、その組織に管理責任が生じる。ただし、基本的にはコンテンツの責任はその作者が負うべきであり、所属組織は作者に対して利用規定やガイドラインの意味を理解させる努力を行う義務が生じる。

リンクの方法は、情報がサーバ上にあるのでなく、リンクであることが読者に明確にわかる形で行う必要がある。読者が錯誤するような形のリンクでは著作権法上の引用に該当しない可能性が発生する。

③電子透かし

現在のWWWのシステム（httpの範囲内）では、情報転送後の複製を制御することは困難である。そこで画像や音声などの著作権者が誰であるか明確に示すために、電子透かしが用いられる。電子透かしは人間の視覚、聴覚では知覚できないような形で、著作権を示すような視覚的パターンもしくは文字データなどを保護したい対象の情報に埋め込む者である。電子透かしは透かしの情報を故意に除去しようとすると、保護対象の品質が著しく劣化するような形式で埋め込まれており、一定の処理を行うと透かし情報を取り出して、著作権情報を確認することが可能である。