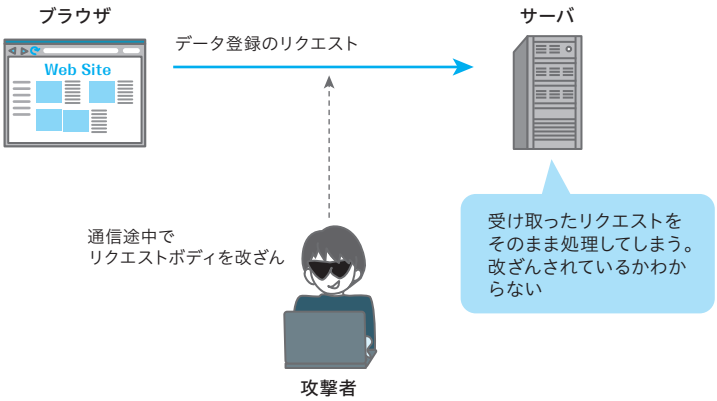
●通信内容の改ざん

通信経路の途中には、通信内容が正しいかどうかを検証する仕組みがありません。相手が送った内容と自分が受け取った内容が本当に一致するのか検証できないため、通信途中で攻撃者に内容を改ざん（書き換え）されていても知ることができません（図3-24）。

通信データの改ざんを防ぐためには、データの欠損や不整合がないことを保証する仕組みが必要です。



▶図3-24　通信途中での改ざん

3.3.2 HTTPの弱点を解決するTLS

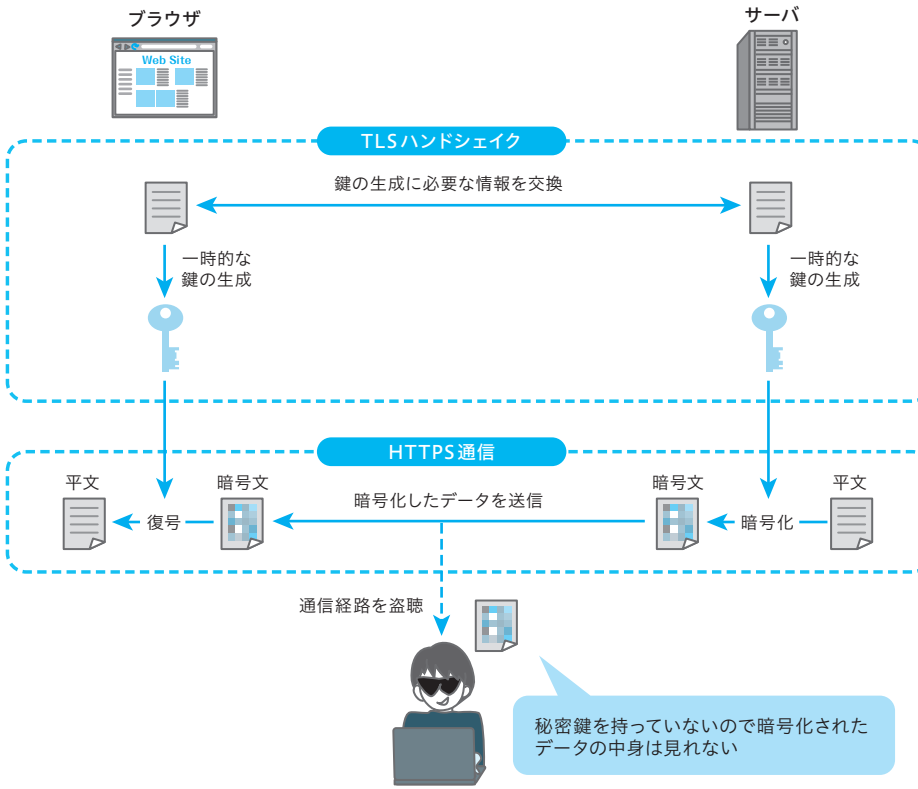
前項で説明したHTTPの弱点を解決するためには、**HTTPS**（HTTP over TLS）を用いて通信を行う必要があります。HTTPSは**TLS**という通信プロトコルを用いて、HTTPデータを暗号化して通信する仕組みです。HTTPデータのやりとりをする前にTLSハンドシェイクと呼ばれる一連の手順によって暗号通信が確立されます。

TLSを使った通信は「通信データの暗号化」「通信相手の検証」「通信データの改ざんチェック」を実現します。本書ではTLSの概要を説明しますが、詳しいTLSの通信方法については説明しません。より詳しく学びたい方は『プロフェッショナルSSL/TLS』（ラムダノート）を一読することをおすすめします。

●通信データの暗号化

TLSはデータの暗号化と改ざんから守る機能を備えています。平文データ（暗号化されていないデータ）を暗号化して相手に送信し、受け取った相手は暗号文を復号（平文へ戻すこと）することでデータの中身を見ることができます。暗号化と復号に必要な鍵は、ブラウザとサーバが情報のやりとりをして安全に共有されます。鍵を持つものだけが暗号文を復号できます。

仮に攻撃者がHTTPS通信途中で盗聴を試みたとしても、秘密鍵を持っていないのでデータの中身を見ることはできません（図3-25）。また、秘密鍵はTLSの通信ごとに作られる一時的なものです。通信が終わると廃棄されるため、仮にサーバに不正侵入することがあっても秘密鍵は盗まれません。TLSの暗号方式についての詳細は『図解即戦力 暗号と認証のしくみと理論がこれ1冊でしっかりわかる教科書』（技術評論社）をお読みください。



▶図3-25　データの暗号化の概要図

●通信相手の検証

TLSでは、電子証明書を使って通信相手が本物か確認します。電子証明書は認証局（CA）と呼ばれる社会的に信頼されている機関によって発行されます。サーバから送信された電子証明書はブラウザによって正しいかどうか検証され、あらかじめブラウザやOSの中に組み込まれている電子証明書と照合されます。もしCAから発行されていない電子証明書が使用されていると、ブラウザは警告画面を表示します。サーバは必ず信頼できるCAから発行された電子証明書を使わなければいけません（図3-26）。