Web サービスのためのネットワーク基盤技術

Technology of Network Infrastructure for Web Service

松　尾　和　善，室　谷　亮　哉

要　約　Web サービスのネットワーク基盤に要求されることは，安全性と快適性である．安全性の観点では，Web サービスを提供する側と受ける側の二つの側面から，具体的なセキュリティの攻撃や脅威，Web サービスやシステムのトレンドとその課題などを示す．そして，その脅威や課題に対して有効なファイアウォールやプロキシサーバ等のネットワーク基盤技術での対処方法について解説する．また，快適性を実現するために性能を向上させる高速化の技術として従来から存在している Web プロキシ，SSL（Secure Socket Layer）アクセラレータ/Web アクセラレータ，CDN（Contents Delivery Network）サービスに触れる．加えて，近年導入が進んでいる WAN 高速化装置の Web サービスの高速化に特化した技術を解説する．更に，クラウドコンピューティング環境における WAN 高速化装置の対応状況とビジネスモデルの変化について言及する．今後は，スマートフォンやタブレット端末からの Web アクセスについても高速化の仕組みが実装されることが期待される．

Abstract　What is required for the Network infrastructure used in web services are the safety and comfort. As to the technology to realize the safety, the specific security threats and the recent attacks, including the trends and their issues of web services and systems, are described from both sides of the receiver and provider of web services. And how to deal with network-based technologies such as firewalls and proxy servers, which are valid for the threats and challenges, are described. As to the technology to realize the comfort, the web proxy server, SSL accelerator/web accelerator and CDN service are introduced as the traditional technology which improves the performance. After that, the technology-specific functions for Web service inside WAN accelerator actively deployed in recent years are described. In addition, the change of business model of WAN accelerator in the cloud computing environment is described. Near future, we are looking forward to being able to use the WAN acceleration feature in web access with smart phones and tablet devices.

1. は　じ　め　に

Web サービスを実現するには，Web サーバならびに Web ブラウザをインストールしたクライアント端末に加え，その間を結ぶネットワークが必要となる．Web サービスを利用するユーザは誰もが，安全にかつ快適に使いたいと思っている．本稿では，クライアント端末や Web サーバ，あるいはそれらの機器の間のネットワーク回線ではなく，その各所に設置されるネットワーク機器の中で特に今後，導入が進んでゆく技術・製品に焦点を絞り，その概要と実装を中心に述べる．また，2010 年代の大きな潮流として，クラウドコンピューティングサービスの利用が進んでいる．多くの企業は，当面の間，これまでのオンプレミスのシステムとクラウドコンピューティングサービスの二つの形態を並行して利用することになる．利用者はオンプレミスと同様にクラウドコンピューティングサービスにも安全性・快適性を求めている

が，本稿では特に断りのない限り，いずれの形態にも利用できるものとして説明する．

2. 安全に利用してもらうための技術

Webサービスに限ったことではないが，サービスやシステムを安全に使ってもらうための仕組みや取り組みは重要な要素である．とくに2005年度以降では個人情報保護の浸透や，度重なる情報漏洩問題の発生などもあり，利用者のセキュリティ意識は非常に高まっている．

2.1 Webサービスの脅威と最近の脆弱性

情報セキュリティは，ISO/IEC 27002でも定義されているように，組織の内部あるいは外部に存在する様々な脅威から情報資産を守り，情報資産が持つ機密性や完全性，可用性を維持することである．Webサービスの場合，守るべき情報資産とは，Webサーバとその上のコンテンツやプログラム，Webサーバのバックエンドにあるデータベースなどの各種データ類である．本節にて，Webサービスに対しどの様な脅威や攻撃があるのか解説する．

独立行政法人情報処理推進機構（IPA）が調査・考察し公開している情報資産への10大脅威[1]を表1に示す．Webサービス以外の脅威も含まれているが，多くはWebサービスに当てはまるものである．1位の「人が起こしてしまう情報漏えい」ではWebサービスの発達により手軽に情報発信できることも背景にあるとし，2位の「止まらない！ウェブサイトを経由した攻撃」では，ガンブラーウィルスやSQLインジェクションといった，Webサービスへの HTTPによる攻撃があげられている．

表1　2011年版　10大脅威[1]

順位	脅威
1位	「人」が起こしてしまう情報漏えい
2位	止まらない！ウェブサイトを経由した攻撃
3位	定番ソフトウェアの脆弱性を狙った攻撃
4位	狙われだしたスマートフォン
5位	複数の攻撃を組み合わせた新しいタイプの攻撃
6位	セキュリティ対策不備がもたらすトラブル
7位	携帯電話向けウェブサイトのセキュリティ
8位	攻撃に気づけない標的型攻撃
9位	クラウド・コンピューティングのセキュリティ
10位	ミニブログサービスやSNSの利用者を狙った攻撃

図1に示した一般社団法人JPCERTコーディネーションセンターの資料[2]ではWebサービスでの具体的な脆弱性の種類や脅威をIPAへの届出数でまとめており，クロスサイトスクリプティングや，SQLインジェクションといったWebサービス特有の攻撃が多いとしている．これらはWebサービスでのユーザ入力項目に対する攻撃で，攻撃者が入力項目に対し特殊なデータ，例えば，データベースをアクセスするためのコマンド文字列や，Webブラウザに表示・実行させるためのスクリプトを入力することで，Webサービスにある情報を不正に操作するものである．これらの攻撃は，次節にて説明するWAF（Web Application Firewall）やIPS（Intrusion Prevention System）などで防御することができる．

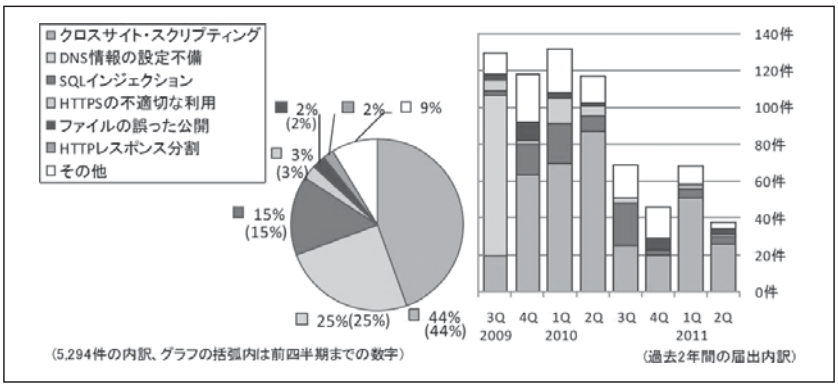

図 1　Web サービスの脆弱性の種類と届出情報[2]

2. 2　Web サービスを提供する際の安全性

前節でも述べたが，情報セキュリティは情報資産を守るための可用性，完全性，機密性の 3 要素からなる．

可用性は利用者が必要な時にいつでも情報資産にアクセスできることを指し，システムの冗長性能や復旧性能と関連づけられる．Web サービスではルータやスイッチなどのネットワーク機器を冗長構成し，また，インターネット回線や各種サーバなどは負荷分散装置で冗長化構成にすることが多い．加えて，それらを監視・運用するためのシステムも必要である．

完全性は情報資産の内容を正しい状態に保つことを指し，改ざん防止が対策となる．Web サーバへの改ざん検知システムの導入や，クライアント端末と Web サーバ間の通信の SSL（Secure Socket Layer）による暗号化，VPN によるネットワークの独立化や暗号化などの対策があげられる．またフィッシング（Phishing）[*1] 対策の一つとして DNS サーバの安全性を高

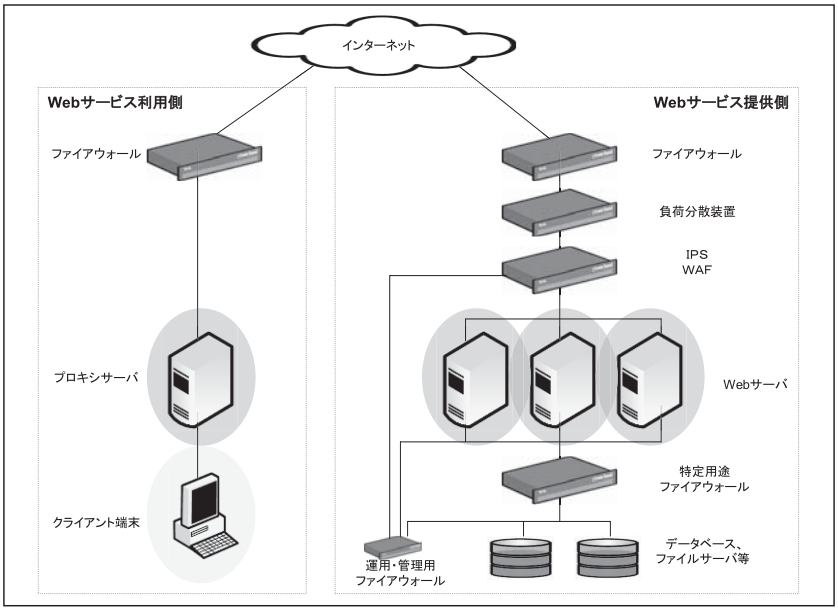

図 2　構成要素イメージ図

める必要もある．

機密性は認められた者が認められた情報資産にのみアクセスできることで，認証とアクセス制御がその中心となる．Web サービスでのアクセス制御は，インターネットからの多様な攻撃を防御するために，多層防御の手法がよく用いられる．種類や手法の違う幾つかの防御システムを階層的に組み合わせることで，より一層強固なアクセス制御を行う手法である．図 2 は Web サービスを提供する際，あるいは利用する際の，具体的な構成要素である．次々に新しく生み出される攻撃に対抗すべく，早いペースで技術革新されるアクセス制御システムについて，特徴的な機能を説明する．

2. 2. 1　ファイアウォール

ファイアウォールは Web システムへのアクセス制御のために設置する．クラアイント端末と Web サーバ間，Web サーバとデータベースやファイルサーバ間，監視・運用・保守用ネットワーク間などにファイアウォールを導入しアクセス制御を行う．アクセス制御は IP 層で行うことが多いが，最近のファイアウォールではアプリケーションの種類や取り扱うデータの種類などを指定してアクセス制御するものもある．例えば掲示板サイトの 2 ちゃんねるや YouTube 動画のアクセス禁止といったアクセス制御設定が可能である．さらにマイクロソフト Active Directory などと連携し，利用者の特定を IP アドレスではなくユーザ名（アカウント名）で行う機能もあり，誰がどの様なアプリケーションを利用しているかの「見える化」も進んでいる．他にも，ウィルスゲートウェイや IPS，URL フィルタリングなどの諸機能を組み込んだ UTM（Unified Threat Management）や，仮想サーバ間の通信をハイパーバイザ内で制御できる仮想環境に対応したファイアウォール等もある．

2. 2. 2　WAF と特定用途ファイアウォール

2. 1 節に記述したとおり Web サービスへの脅威としてクロスサイトスクリプティング攻撃や SQL インジェクション攻撃など，Web サービス特有の攻撃が多数ある．これらの攻撃は HTTP プロトコルやそれを暗号化した SSL を介して行われるが，ファイアウォールの基本機能では防御できない．Web Application Firewall（WAF）はその名の通り Web システムに特化した専用ファイアウォールで，HTTP や SSL のプロトコルの内容を検査し，攻撃を検知，防御するシステムである．以下に詳細を説明する．

1）製品の種類と構成

Web サーバにインストールするソフトウェアタイプのものもあるが，多くはゲートウェイ型で，ファイアウォールと Web サーバの間に設置する．取り扱う Web データの処理フローの観点では負荷分散装置と似た側面があり，負荷分散装置と WAF 機能が統合された製品も多くある．

2）主な機能

Web ブラウザと Web サーバ間でやり取りされる Cookie 情報や HTML のパラメータ情報を精査・監視し，これらの情報が不正改ざんされた場合や，特異な入力データがあった場合に，通信を切断するなどの制御を行う．Web サービスへのアクセスが SSL で暗号化されていると，そのままでは情報を精査できない．このため，WAF に装備されている SSL アクセラレーション機能にて復号化し，情報の精査・監視と制御を行う．

3)運用面での注意事項

攻撃の検知精度を高めるために，初期導入時だけでなく導入後のポリシーチューニングが必要な場合も多い．特にWebコンテンツを頻繁に更新する場合や，動的なコンテンツを多用するWebサービスでは，その傾向が強まる．ホワイトリストやポジティブ・セキュリティと呼ばれる正しい通信だけを定義する方式と，ブラックリストやネガティブ・セキュリティと呼ばれる違反通信を定義する方式があり，多くの製品はその両方をサポートしている．一定期間学習させることで検知精度を上げる，自動学習機能のついたものもある．

WAFはWebシステム専用のファイアウォールであるが，同じような特定システム専用のファイアウォールが他にもある．データベースを守るDBF（Database Firewall）や，ファイルサーバを守るFSF（File Server Firewall）である．Webシステムでは Webサーバのバックエンドにデータを格納したデータベースサーバやファイルサーバなどを構成していることが多い．このデータベースサーバやファイルサーバへのアクセス制御やアクセス監視，監査を行うために，DBFやFSFの利用も徐々に広がってきている．

2.2.3　IPS

IPSはIntrusion Prevention Systemとよばれる侵入検知システムで，WAFと同様，従来のファイアウォールでは止められなかった攻撃を検知し防御するものである．WAFがHTTPやSSLでの攻撃防御に特化しているのに対し，IPSはIPやTCPといった層での攻撃や，HTTPやSSL以外のプロトコルでの攻撃，Webサービスでよく使われるDNSやSMTP，管理・運用・保守のための各種通信に対する攻撃なども検知し防御することができる．

最近の製品の特徴的な機能に，ネットワーク・トラフィックの異常動作から攻撃を検知するアノマリー検知機能がある．正常状態のトラフィック変動パターンを自動測定し，逸脱したトラフィックの量や種類などから検知する．HTTPやSSLポートへのDoSアタック（Denial of Service：サービス不能攻撃）やゼロディ攻撃（脆弱点に対し有効な対処策が確立・公開される前に攻撃されること）を検知し防御することもできる．他にも仮想パッチ機能やホスト隔離機能など，システム保全に有用な機能もある．

2.3　Webサービスを利用する際の安全性

前節ではWebサービスを提供する側での安全性の取り組みについて説明したが，利用者側としても何のセキュリティ対策も必要ないというわけではない．本節ではサービスを受ける側での安全性を高めるための技術について説明する．

2.3.1　Webサービスの現状と課題

新しいシステムや技術の開発，更には社会インフラの変化とともに，利用者の利用形態やコンテンツ自身が大きく変化してきている．それにともない新たな課題が発生し，その対策が必要となっている．ここで二つの問題を例示する．

1）ソーシャルネットワークキング（SNS）の普及

mixi（ミクシィ）やTwitter（ツイッター），Facebook（フェイスブック）等のソーシャルネットワーキングサービスやブログサービスの広がりをうけ，業務での利用も広がっている．これらは，従来のセキュリティ境界の外部にもかかわらずその意識が薄く，不用意な発言の問題化や情報漏洩なども発生している．またSNSの中にも様々なカテゴリやコンテンツがあり，業務利用に適さないものもある．ウィルスやマルウェアなどが仕込まれていることすらある．これらに対してはURLフィルタリングやアプリケーション層での制御や，ウィルス対策が必要となる．

2）SSLトラフィックの増加

Webサービスでは HTTP プロトコルが使われるが，機密性や完全性の向上のため，また，ハードウェア性能が向上しSSL化にかかるコストの低下もあり，SSLを使うサービスが増えている．SSLで暗号化されてしまうと，その通信の中身を確認できない．なかには，SSLで隠蔽された望ましくないサイトやサービスもあるが，これにはSSL復号化機能を利用して対処する必要がある．

2. 3. 2　Webプロキシサーバ

Webプロキシサーバは古くから使われているWeb用のインフラ機器で，コンテンツのキャッシュ機能や，アクセス制御，監査ログの取得などに使われている．昨今ではWebサーバへのアクセスによりウィルス感染することが多くなり，前述の機能の他にウィルスチェックやURLフィルタリング機能を利用する場合も多い．Webサービスの利用者側での安全性の対策として有効なWebプロキシサーバの主な機能を以下に挙げる．

1）URLフィルタリング

URLフィルタリングはメーカが提供するURLデータベースをもとに，インターネットへのWebアクセスを制限するシステムである．多様化するWebサービスに対しフィルタリング精度を向上させるため，従来のダウンロード方式だけでなくオンデマンドによるデータベース検索や，複数カテゴリへの分類と制御機能，新規サイトの自動カテゴリ分け機能，メーカが多方面から収集し解析したレピュテーション情報，つまり「評判」をオンラインで照合する機能など，製品の機能強化が図られている．

2）アプリケーション層での制御

ファイアウォールではアプリケーション層で制御する機能が広まっているが，Webプロキシサーバにもアプリケーション層で制御する機能を持つ製品がある．この様な製品を利用すれば同一のサイトであっても特定サービスだけを許可や禁止にするなど，細かな制御が可能となる．

3）ウィルス対策

メール用のウィルスゲートウェイで，メールのトラフィックのみウィルス対策を行っているサイトが多い．しかし，昨今のウィルスやマルウェア感染経路としてはWebトラフィックが非常に多く，正規サイトでもウィルスやマルウェアが埋め込まれていることもあり，Webトラフィックに対してもゲートェイ型でのウィルス対策が望ましい．

4）SSL復号化

URLフィルタリングなどのアクセス制御を行うために，経路途中のWebプロキシサーバ

にてSSL暗号化通信を復号化する機能である．通常，SSLの暗号化通信はクライアント端末上のブラウザとWebサーバ間に開設された一つのSSLトンネルで行われる．このSSL復号化はクライアントからサーバへのSSLトンネルを，1)ブラウザとWebプロキシサーバ間，2)Webプロキシサーバと Webサーバ間の二つの独立したSSLトンネルに分けることで実現している．

一方でSSLの復号化では，クライアント端末のWebブラウザにSSL証明書が正しくない旨の警告が表示されることや，クライアント証明書を使った認証ができなくなるなどの技術的な課題がある．また，Webプロキシの管理者が，秘匿とすべき正当な暗号化通信を見ることができてしまうなど，通信の秘匿性が担保できなくなる課題もある．

3. 快適に利用させるための技術

この章では，Webサービスの快適性を実現させる，つまりネットワーク性能を向上させ，より高速に表示コンテンツを転送する為の技術について述べる．Webサービスに使用されるHTTPプロトコルは，低速，高伝送遅延環境での使用に耐えることができるように設計されている．例えばWebブラウザは，複数のHTTPセッションをWebサーバとの間に確立させ，それらを並行してデータ転送を行う．また，一度取得したコンテンツは，有効期限内であれば再読込操作をしない限り，Webクライアントのローカルディスクに保存されたデータを表示させ，余分な通信を行わないようになっている．この他に現在高速化の為に使用されている技術について整理しておく．

3.1 Webプロキシサーバ

Webプロキシサーバは，前章で述べたように主にセキュリティの確保の点で多くの企業に導入されているが，キャッシュの機能もある．企業内から外部のインターネットのコンテンツを読み出した時に一旦保存しておき，再度，企業内から同一のコンテンツへの要求があった場合，外部のインターネットにアクセスするのではなく，内部のキャッシュされたコンテンツを送信する．これにより，Webクライアントはデータ取得の時間を短縮できる．

3.2 SSLアクセラレータ/Webアクセラレータ

SSLアクセラレータは，セキュアな通信を行う為のWebプロトコルであるHTTPSのサーバ証明書をインポートして，SSLの暗号化/複合化を装置内の専用チップで処理する．これによりWebサーバ側のCPUリソースの負荷を低減させ，処理能力を向上させることができる．

また，Webサーバの処理負荷を低減し，データの通信量を抑制することでWebアクセスを高速にする為のWebアクセラレータという装置もある．これの主な機能は，1)コンテンツの圧縮，2)コンテンツの差分転送，3)重複排除（動的に見える静的コンテンツで変更内容が特定パターンの場合キャッシュする）で，通信路のWebサーバ側のみに設置する．SSLアクセラレータやWebアクセラレータの機能は，現在，市販されているハードウェア型サーバロードバランサのほとんどのモデルに実装されている．

3.3 CDNサービス

CDN（Contents Delivery Network）サービスは，Webサーバがごく短期間で大量のコンテ

ンツを送信しなくてはならない場合や，世界中どこからアクセスしても距離による転送遅延の影響を受けずにレスポンスを維持してコンテンツを提供したい場合に，Web サーバの代わりになって Web クライアントの要求に応答し，コンテンツを提供するしくみである．Web クライアントからは，別のサーバからコンテンツを転送されていることを全く意識することはない．Akamai 社が提供しているサービスが最も有名で，多くの企業や団体が利用している．全世界のインターネットのトラフィックの約 20％は，同社が提供するプラットフォームから配信されている．

3. 4　WAN 高速化装置

WAN 高速化装置[*2] は，ファイル転送（CIFS プロトコルや FTP）の高速化のみならず Web サービスに特化した機能も実装している．Web アクセスの高速化を実現する場合において最もキーとなるのはデータのキャッシュ技術である．Riverbed 社の Steelhead では，データを約 100Bytes の単位で分割して保存し，キャッシュのヒット率を上げるような工夫がされている．3. 1 節に述べた Web ブラウザや Web プロキシのファイル単位のキャッシュ方式とは異なる．Steelhead では，HTTP プロトコルによって転送されてきたデータを如何に効率的にキャッシュするかという視点で主に三つの機能が実装されており，加えて HTTPS に対する高速化の機能も実装されている．本節の各項にて説明する．

3. 4. 1　URL-Learning 機能

この機能は，Web ページ中の Object を要求する際，Object と Referer ヘッダの URL を関連付けてキャッシュしておき，次のクライアントからの Object 要求に素早く応答できるようにするものである．図 3 に示すようにクライアント側の Steelhead では，①と②のようにクライアントが要求した Web コンテンツの Object のリファレンス情報を③でグループ化し，Steelhead 内部の HTTP Database に関連ツリーとして保持する．次に別の Web クライアントから同じコンテンツの要求④を受けた場合，Steelhead 内では URL に関連づけて Object を管理している為，⑤のように要求されたツリー配下の Object を高速に提供することができる．

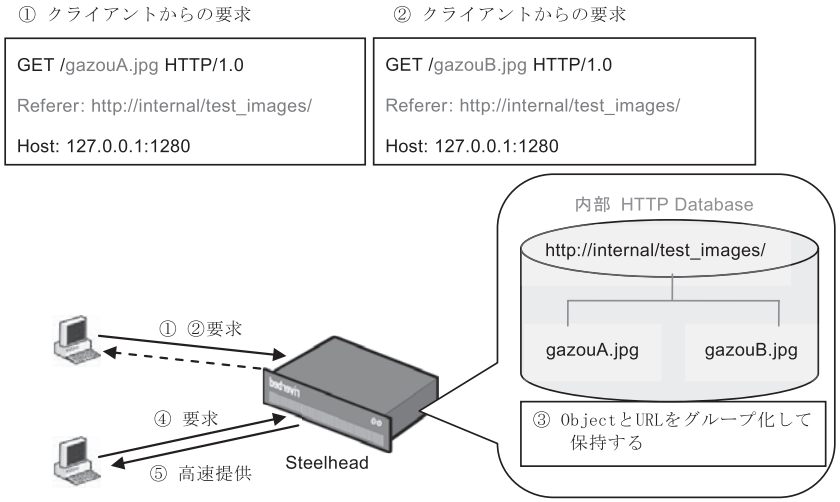

図 3　URL-Learning

3. 4. 2　Parse and Pre-fetch 機能

この機能は，クライアントが Web ページを要求した場合に Steelhead 側で構文を解析して必要な情報（js，jpg 等）を先読みすることにより高速化を実現する．図 4 に示すようにクライアント側の Steelhead は，Web クライアントからの動的な Web ページの要求を受信したらすぐに HTML ファイルの構文を解析し，そのページを表示する為に必要な情報を読み取り，先行して Web サーバに対して表示する為に必要な情報を要求する．クライアント側の Steelhead は，予めキャッシュしておくことにより高速にクライアントからの要求に応答することができる．

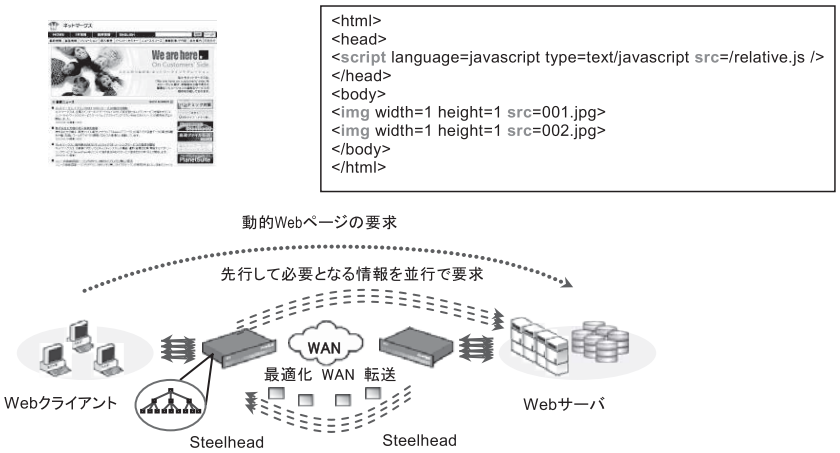

図 4　Parse and Pre-fetch

3. 4. 3　Metadata Acceleration 機能

この機能は，クライアント側 Steelhead が，クライアントからの要求に含まれるコンテンツの有効期限の IMS（If-Modified-Since）ヘッダを確認し，以下のように処理し，304 Not Modified レスポンスを代理応答することにより，WAN 経由の RTT の影響を最小化し，高速化するものである．クライアントからの要求に IMS ヘッダが含まれていれば，Steelhead 内の DB を確認し，その DB 内になければ Web サーバにアクセスする．Web サーバの応答に Last-modified ヘッダが付加されてきたら，その情報をクライアント側 Steelhead に登録する．この場合，Expire ヘッダの値もしくは，Steelhead の設定値の短い方を有効期限として登録する．他の Web クライアントより，その有効期限内に同じコンテンツに対する要求を受信した場合は，クライアント側 Steelhead は，304 Not Modified レスポンスを返し，本来 Web サーバから転送されてくる際にかかってしまう遅延を回避する．

3. 4. 4　HTTPS プロトコルへの対応

セキュアな通信である HTTPS はサーバの暗号化鍵によって通信の都度転送されるデータが暗号化される為，毎回異なるデータとなってしまう．そのため，HTTP プロトコルと同様に，転送されてきたデータを約 100Bytes 単位に分割・ストアしてもキャッシュ効果がない．Steelhead では，先に紹介した SSL アクセラレータと異なる方法で HTTPS プロトコルの高速化を実現する．図 5 に示すように予め Web サーバの証明書をサーバ側に設置されている Steel-

head にインポートしておく．クライアント側への証明書のインポートは必要ない．Web クライアントからの要求を受け付けた Web サーバ側では，暗号化されたデータをサーバ側 Steelhead が受け取ると一旦，インポートした秘密鍵を使ってデータを復号化してキャッシュに保存する．Steelhead 間は，予め Steelhead 本体に入っている公開鍵を対向先の Steelhead 同士で相互に交換しておく．サーバ側 Steelhead が生成した独自の Temporary Key で暗号化した SSL トンネルを張り，データをクライアント側 Steelhead に届ける．Web クライアントに向けてのデータ暗号化/復号化は，Temporary Key を用いて行う．各場所で使用する暗号化キーは異なるが，全ての機器の間でSSL通信を行いながら，Steelheadの特長であるキャッュのヒット率を上げ，高速化通信を実現させる．Version 5.0以降では，証明書のドメイン・ワイルドカードを使用することができ，複数の Web サーバが存在していたとしても同一ドメイン内であれば，Steelhead に対してサーバ証明書を複数インポートする必要がなくなる様な工夫がされている．

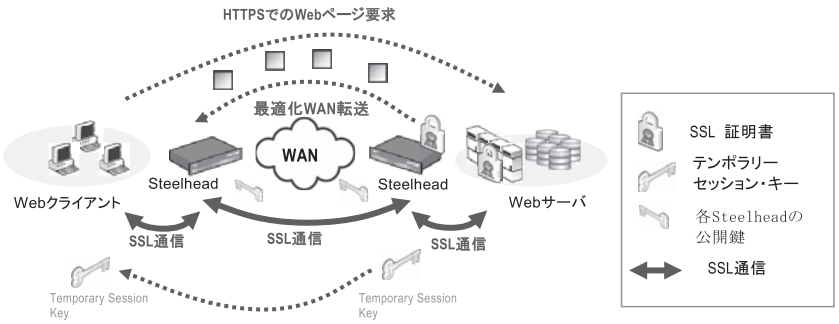

図 5　HTTPS の高速化

3. 5　クラウドコンピューティングへの対応

クラウドコンピューティングサービスの利用が進み，企業が使用する Web サーバのロケーションが変化している．自社でプライベートクラウドを構築する場合には，Web サービスを取り巻くネットワーク機器はさほど変わりはないが，今後伸びて行くであろうパブリッククラウドを利用した Web サービスの場合には，WAN 高速化装置をサーバロケーションに設置するのは困難である．WAN 高速化装置のメーカでは，パブリッククラウドサービスの環境に対応できるよう，仮想サーバ（Hypervisor）上で動作するソフトウェアをリリースし始めている．Riverbed 社でも Cloud Steelhead という商品をリリースしているが，単に Hypervisor 上で動作するソフトウェア版を販売している他のメーカと異なり，ビジネスモデルがユニークである．同社は，Amazon Web Services（AWS）等のパブリッククラウド・プロバイダと提携し，予めパブリッククラウド内 Cloud Steelhead を準備しておき，月額使用のサービス形態で WAN 高速化機能を提供している．

3. 6　今後の Web 高速化の動向

2008 年以降のモバイル端末の変化は著しく，半年毎に新しい変化が起きている．企業で使用される端末もノート PC に加えて，タブレット端末，スマートフォンが使用され始めた．当然のことながらこれらの端末でも Web ブラウザを用いて Web サービスを利用するが，ここ

にはWAN高速化の仕組みは実装されていない．いくつかのWAN高速化装置のメーカでもモバイルPC用として，高速化を実現する為のソフトウェアを既に投入している．2011年現在のモバイルPCは，十分すぎるくらいのCPU性能，メモリ，ディスク容量を搭載している為，高速化のソフトウェアにリソースを使用されても何の問題もない．一方，スマートフォンやタブレット端末は，メモリ領域をキャッシュとして使用するには，まだまだリソース不足である．また，頻繁に書き込みが発生するキャッシュ領域は，SSDの書き込み寿命を考慮すると不安が残る．これらの課題を解決し，あらゆるWeb端末からセキュアで高速なWebアクセスが実現できるようになることが，期待されている．

4. おわりに

本稿では安全性と高速性という二つの観点から，Webサービスに必要な要素技術を紹介してきた．クラウドコンピューティング環境が拡大するにつれ，システムやサーバの仮想化も進んでいる．Webサービスの要素技術も同じで，論文中ではファイアウォールの仮想環境への対応について言及した．中には，ハードウェア販売のビジネスモデルが大きく影響を受けうることから，仮想環境対応に二の足を踏んでいるメーカも見受けられるが，全般に仮想サーバ（Hypervisor）上で動作するソフトウェア版のリリースや，マルチテナント機能の拡充など仮想環境への対応がさらに進んでいくのは明確である．今後，Webサーバ自体も含め，Webサービスの各要素技術を網羅的に統合した仮想環境への対応が必要になると考えている．最後に本稿の執筆にあたり，技術トレンドや技術要素を調査・確認し解説してくださったグループメンバや，製品の最新情報を提供いただいたメーカの方々にお礼申し上げたい．

＊1　フィッシング（phishing）とは，金融機関などからの正規メールの様に装い不正サイトに利用者を誘導し，個人IDやパスワード，クレジット番号情報などを入手する行為で，「釣り」を意味するfishingと，「手の込んだ」を意味するsophisticatedから作られた造語とされている．

＊2　WAN最適化装置（WAN Optimization Controller）と呼ばれることもあるが，Webのプロトコルに対してはWAN高速化装置（WAN Accelerator）の方が適当であるので，こちらの呼称を使用する．

参考文献

［1］ 独立行政法人情報処理推進機構，「2011年版 10大脅威 進化する攻撃… その対策で十分ですか？」，2011年3月
http://www.ipa.go.jp/security/vuln/10threats2011.html

［2］ 一般社団法人JPCERTコーディネーションセンター，「ソフトウエア等の脆弱性関連情報に関する届出状況［2011年第2四半期（4月～6月）］」
http://www.jpcert.or.jp/report/press.html#year2011

［3］ ポール・S・ヘスマン著，ファサード訳「HTTP詳説」，ピアソン・エデュケーション出版，1998年

［4］ F5 networks社のホームページ
http://www.f5networks.co.jp/

［5］ akamai社のホームページ
http://www.akamai.co.jp/enja/

［6］ Riverbed社のホームページ
http://www.riverbed.com/jp/

上記参考文献のURL確認：2011. 9. 1

執筆者紹介　松　尾　和　善（Kazuyoshi Matsuo）

1998年(株)ネットマークス入社．ファイバチャネル技術をベースにSAN製品の技術を担当，2006年よりWAN高速化製品の技術サポートに携わる．2010年よりネットワーク製品全般の技術サポート業務に従事．

室　谷　亮　哉（Akiya Murotani）

1997年に住友電工システムズ(株)より(株)ネットマークスに転籍．ファイアウォールや認証システム，オープンソースでのインターネット環境のSI業務や，セキュリティ・コンサルティング業務に従事．