DevCentral

DevCentral™は、F5の製品をさらに有効活用していただくためのオンライン コミュニティです。

DevCentralには、ネットワーク管理者、アプリケーション開発者を中心に、全世界で162,000名以上の方にご登録され、日本のお客様にも多数ご利用いただいております。最新のテクノロジー情報、カスタマイズツール、カスタマイズ用サンプルコードなどを提供するとともに、登録ユーザ同士が情報共有を図るための場を提供しています。

ユーザ登録は無料です。ご登録いただくと、Forumへの参加などが可能となり、すでにご導入されている製品のさらなる有効活用のためのヒントをご覧いただけます。

devcentral.f5.com/

F5ネットワークスジャパン合同会社

東京本社
〒107-0052 東京都港区赤坂4-15-1 赤坂ガーデンシティ 19階
TEL 03-5114-3210　FAX 03-5114-3201

西日本支社
〒530-0012 大阪市北区芝田1-1-4 阪急ターミナルビル 16階
TEL 06-7222-3731　FAX 06-7222-3838

お問い合わせは：f5.com/jp/fc/

● お問い合わせ先

2015年10月A

F5製品&サービス総合カタログ

on TMOS® platform

ハイブリッド化するアプリケーション環境の構築ニーズに柔軟な解決策を

アプリケーションの基盤は、オンプレミスの自社データセンターに加え、
プライベート、商用のパブリッククラウドへと急速に拡大しています。
一方で、スマートフォンやタブレットなどデバイスの多様化に伴い、
ネットワークもSDNへの対応を求められると同時に、
複雑化するセキュリティ課題にも適切に対応しなくてはなりません。
さらに、クラウドとオンプレミスをビジネスニーズに応じて使い分ける時代において、
アプリケーションの活用には迅速と安全性の実現が求められています。
F5は、BIG-IPを中核としたオンプレミス対応製品群に加え、
Silverlineというクラウド基盤に対応した新たなソリューションを提供し、
ビジネスにおける多様な課題への解決策を提案します。

データセンター

ADC（アプリケーション デリバリ コントローラ）製品であるBIG-IPを中核に、ハードウェアから、仮想化モジュール、運用管理環境まで、快適なアプリケーションの活用を実現する製品群を提供します。

クラウド

パブリック クラウド サービスのマーケットプレイスからBIG-IPを。これにより、パブリック クラウド上のIT資産にも、F5ソリューションを適用できます。

コンバージド システム

F5製品は、検証済みのITインフラの統合パッケージであるコンバージドシステムにも適応しています。FlexPod、HP CloudSystem、Microsoft Cloud Platform System、Vblockなどで採用が始まっています。

As-a-Service

F5はクラウド環境をグローバル規模で独自に構築しました。この上で提供するクラウドサービスを「Silverline」というブランド名で新たに展開。DDoS対策やWAFを皮切りに、今後も様々なソリューションを展開していく予定です。

F5製品&ソリューションの特長

競合他社との差別化、迅速な新事業展開、業務プロセスのさらなる効率化――。
その成功は、アプリケーションの柔軟な対応が鍵となります。
F5は「Synthesis」というビジョンで、お客様のビジネスの成長を支援します。

アジャイル開発、DevOps、クラウド、SDDC（Software Defined Data Center）、そしてビッグデータ。ビジネスの重要な基盤の一つであるアプリケーションを取り巻く環境は、今、大きな変化の中にあります。こうした変化に対応すべく、ITシステムの現場では、アプリケーションを支えるプラットフォームの仮想化と、ネットワークのSDN化という両側面からの進化が成されています。しかし、アプリケーションの可能性を最大化するには、両者の間に進化から取り残されたギャップが存在しています。F5は「Synthesis」というビジョンのもと、このギャップに対応するための様々なソリューションを提供します。

ギャップの解消に向けたF5の「Software Defined Application Services」

F5はネットワークの視点から、アプリケーションに注目し、快適な利用環境、そして安全・安心をどうしたら効果的に実現できるか、という問いに答え続けてきました。アプリケーションが仮想化・クラウドの環境へ移行し、またネットワーク技術が仮想化（SDN化）しても、F5の基本姿勢は変わりません。「Software Defined Application Services」として位置づけたコンセプトのもと、ソリューションを従来型・クラウド・SDN上すべてで提供します。従来の物理的な操作をベースとした管理・運用ではなく、ソフトウェアをベースとした、より簡単で柔軟性に優れ、機敏な管理・運用へ。しかも、将来のテクノロジーの進化にも容易に対応できること。その具現化に向けた取り組みは、以下の3つの要素が柱になります。

■ハイパフォーマンス サービス ファブリック

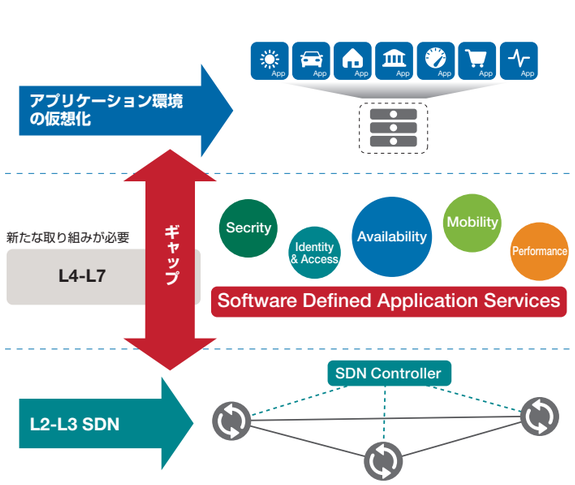
BIG-IPを中心とした多彩な製品と各種ソリューション、独自の共通プラットフォーム テクノロジーTMOS、BIG-IPアプライアンス製品や仮想化アプライアンスに加え、これらの機能をクラウドサービスとして実現したSilverlineも提供

■インテリジェント サービス オーケストレーション

調和のとれたサービスを可能にする次世代マネジメント ソリューションであるBIG-IQ

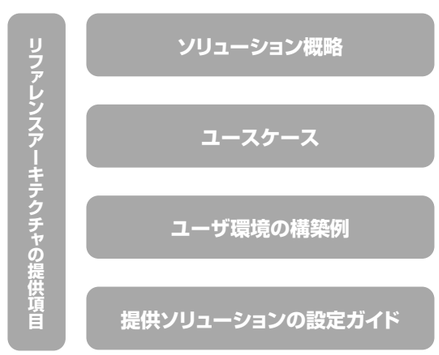
■シンプリファイド ビジネス モデル

ソリューション利用形態の多様化に応じた様々なライセンスモデル



確実に、そして迅速な導入を実現する「リファレンスアーキテクチャ」

テクノロジーの進化や利用形態の変化に応じて次々と登場してくる新たなユーザニーズ。そうした先進的な要望を確実に、そして迅速に形にできるよう、F5のワールドワイドな活動をとおして蓄積した実績をベースに、機器の推奨構成などの具体的な情報を目的や用途に応じて「リファレンスアーキテクチャ」として整備。単なるユースケース資料に留まらない、現場の実務に則した情報が入手できます。これにより、従来はイメージできなかったF5製品活用ケースの再発見、実践的な情報に基づいた迅速な現場への導入が可能になります。



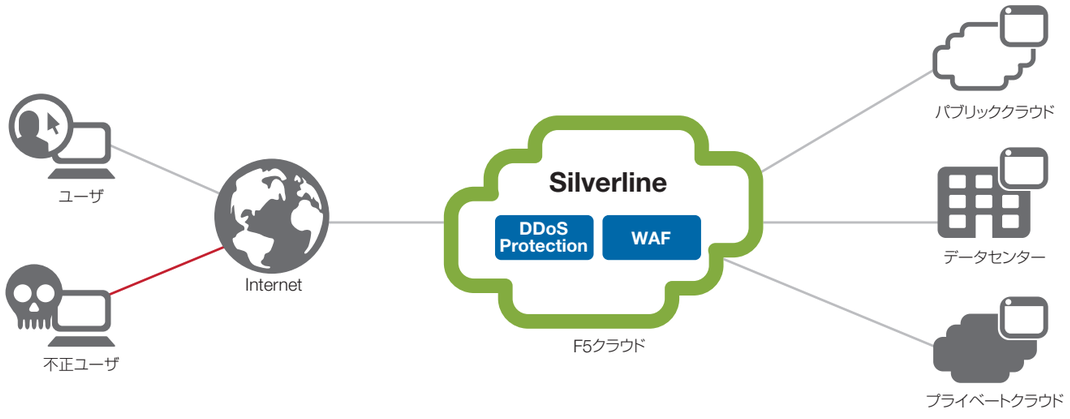
BIG-IPの優れた機能をそのままに
F5独自のデータセンター網で提供するクラウドサービス

Silverline

DDoS Protection　Silverline WAF

サブスクリプションベースの料金体系でコストダウンに貢献、導入期間の大幅短縮や容易な性能拡張も可能に

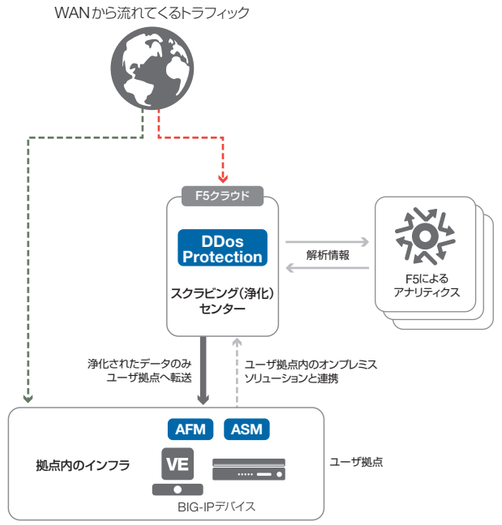
ITはハードウェアを「自社で保有」する時代から、必要な「機能を利用」する時代へ確実に変化しています。こうした動きをアプリケーションデリバリの分野に適用したのが、F5のクラウドサービス、Silverlineです。クラウドサービスならではのサブスクリプション型の料金体系により、ハードウェア保有の際に必要だった導入コストを削減。運用フェーズにおいては、F5のSecurity Operation Centerによる24時間365日の監視サービスを提供し、お客様のサイトに悪意あるトラフィックが到達する前にネットワーク上で確実なセキュリティ対策を講じます。



Silverlineの主な特長

- 資産を保有することなく、L4-L7の各種技術が利用可能に
- 設置作業も不要、簡単な設定作業だけでF5の技術を即利用可
- メンテナンスや専門エンジニアも不要に
- ネットワーク状態を容易に把握できる管理画面とレポートを提供。F5のSecurity Operation Center担当者との連携も可能
- グローバル展開するお客様を対象に、国内外の区別なく、同一技術で全拠点一貫した対応が可能

Silverline DDoS Protection　自動スクラビングでリアルタイムな防御を実現



- 常時F5クラウド経由でのトラフィック配信<Always On>とするか、有事の際のみ<Always Available>（普段は緑のルート）とするかは設定次第。
- 将来的にはオンプレミスとクラウドがシームレスに連携。設定情報、DDoS攻撃への対応状況などを包括的に管理。

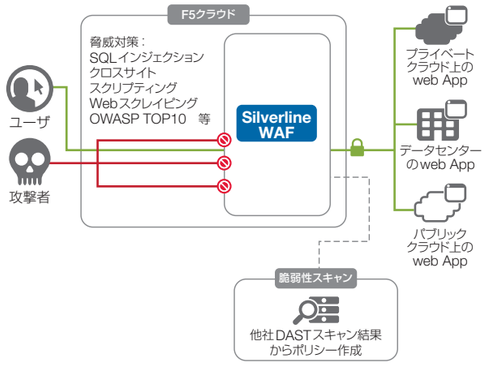
大規模DDoS攻撃などをネットワーク上でブロック

Silverline DDoS Protectionは、大量のトラフィックを集中的に送ることでオンラインサービスやウェブサイトをダウンさせる大規模DDoS（Distributed Denial of Service）攻撃などをクラウド上のスクラビング センターでフィルタリング（洗浄）。お客様サイトにクリーンなトラフィックだけを戻します。スクラビングセンターでは脅威の監視から検出、特定、制御までを完全自動化。リアルタイムな防御を実現します。

選べる2つのサービスメニュー

Silverline DDoS Protectionは、トラフィックを常時スクラビングセンター経由とする「Always On」と、DDoS攻撃を受けたときにスクラビングセンター経由に切り替える「Always Available」という2つのサービスを用意しています。お客様のニーズに応じて最適な防御形態を選択できます。

Silverline WAF　アプリケーションの場所を問わないWAF機能

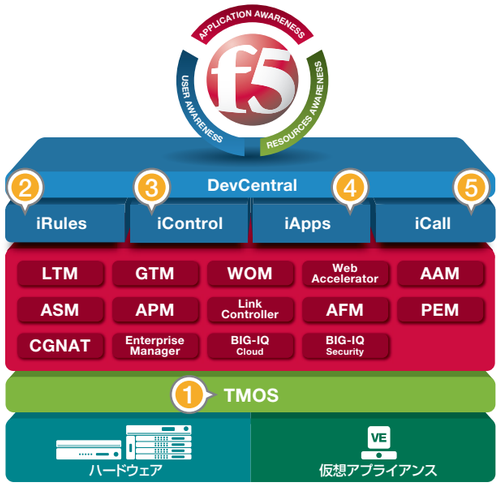


BIG-IP ASMの機能をクラウド化

Silverline WAFは、WAF黎明期から長年にわたって国内外で数多くの導入実績を積み上げてきたBIG-IP ASMをクラウドサービスとして実装。Silverline WAF、およびBIG-IP ASMという2つのソリューションにより、ユーザ企業の自社サイト上、クラウド上を問わず、柔軟な提供形態で同じ強度のアプリケーション セキュリティを実現できます。また、WAFの運用に必要な専門知識も、F5のエキスパートがユーザ要件を理解し対応し、ユーザ側の業務負担を大幅に軽減します。

BIG-IP製品群の基盤となる各種機能、アーキテクチャ

ロードバランサに始まり、市場のニーズに応え続けてきた結果、BIG-IPは高機能なアプリケーション デリバリ コントローラへと進化しました。そのすべての製品・技術を支える共通のプラットフォームテクノロジーがTMOSです。TMOSのプログラマビリティを形成する中核の機能群として、下の図で示すように、iRules、iControl、iApps、iCallの4つがあります。各機能はBIG-IPの豊かな拡張性を生み出す源泉であり、F5の開発者向けのオンラインコミュニティ「DevCentral™ Japan」上で、すべての機能に関するサンプルや導入事例などを公開・共有。ユーザ様のより実践的なF5製品活用を効果的にサポートしています。



① TMOS®

TMOSは他に類を見ない、F5 BIG-IP製品の基盤となる共通のプラットフォームです。TMOSのアプリケーション制御プレーンのアーキテクチャはスケーラビリティに富んだ、弾力的で再利用性の高いサービスプールを形成します。変化を続けるデータセンターと仮想化の状況に適応し、高速で可用性が高くセキュアなアプリケーション配信を可能にします。さらに、汎用性の高いオープンなAPIが、完全なコントロールと柔軟性をもたらします。

② iRules®

TCLベースのスクリプト言語を使って状況に応じた振り分けルールを記述できるプログラミング言語。BIG-IPを通過するパケットに対し、決められたタイミング（イベント）ごとにあらかじめ記述したスクリプト（ルール）を実行することで、トラフィック制御の効率化や、クライアントとサーバ間のセキュアな通信を実現。例えば、Cookieの暗号化やリソースクローキングなどの実用に即したルールをあらかじめ用意して利用できます。また、最新の機能であるスクリプトのプロシージャ化により、「重い処理」を外部ライブラリで処理可能。一層効率的なトラフィック処理の設計を実現します。

③ iControl®

アプリケーション デリバリ コントローラとして初めて実装されたオープンなAPIで、F5製品を統合するためのインタフェースをSOAPベース、RESTベース両方で提供します。さらに、iControlのSDK（ソフトウェア開発キット）を利用することで、サードパーティ ソリューションとF5製品を統合できます。

④ iApps™

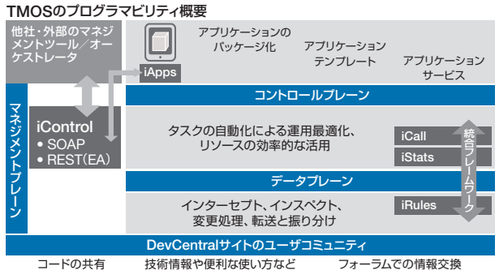
アプリケーションを中心に据えたフレームワーク（アーキテクチャ）設定投入を実現します。ネットワークの高度な専門スキルがなくても、アプリケーション デリバリのための設定やネットワークの展開が可能です。また、簡単に設定を複製できるため、類似した設定を複数ディプロイすることが多いネットワーク環境では、導入時の負荷を大幅軽減。マクロテンプレートなどの活用によりユーザの入力箇所を最小化でき、使い勝手はさらに向上しました。

⑤ iCall

あらかじめ設定したイベント（しきい値など）を状態監視し、条件にマッチした場合に設定通りのスクリプトを実行する、BIG-IPのコントロールプレーンに対する柔軟性を提供します。多様な運用プロセスの自動化を実現し、工数削減、プロセス改善などに効果を発揮します。

BIG-IPのプログラマビリティ機能群

TMOSのプログラマビリティ概要



コントロールプレーン（BIG-IPの設定情報等）の書き換えなどをスクリプトで行い、運用プロセスの自動化を目指すiCallと、データプレーン（トラフィックの転送等）を柔軟に設定できるiRulesの活用により、無限の柔軟性を提供します。また、これらを外部システムと簡単に連携させるAPIであるiControl、外部連携でも威力を発揮するアプリケーションテンプレート機能等を含めたiAppsにより、BIG-IPのプログラマビリティは構成されています。

Scale^{N}™

F5のスケーラビリティを可能にするのがScale^{N}技術。主に、以下のような機能群で構成されています。

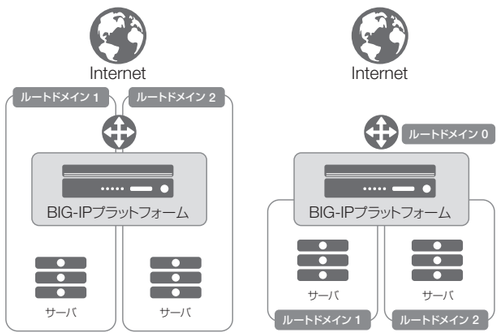
デバイス サービス クラスタリング：デバイス間の多重クラスタリングを可能にし、一般的なフェイルオーバー（アクティブ-スタンバイ構成）ではなく、アクティブ-アクティブ構成を採用。アプリケーションの負荷に応じたフェイルオーバーによって、アプリケーションサービスの中断を回避します。

vCMP™（virtual Clustered Multi Processing）：VIPRIONおよび一部のBIG-IPアプライアンスでは、単一デバイス内に複数の仮想インスタンスを設定し、専用ハイパーバイザを用いることで、リソースを独立した仮想ADCに完全分割することが可能です。CPUレベルでアイソレーションした運用を実現。マルチテナント環境でのリソース効率化を飛躍的に高めます。

オンデマンド アップグレード ライセンス：最新ハードウェアの標準モデルから強化モデルへ、ハードウェアの入れ替えなしにアップグレードできる仕組みです。BIG-IPを効率的にアップグレードでき、柔軟なインフラ計画を実現します。

ルートドメイン

複数のルーティングテーブルの保持により、分離されたIP空間で重複IPを使用できるため、1つのBIG-IPで複数の顧客、アプリケーション、セグメントを競合させずにサポートできます。

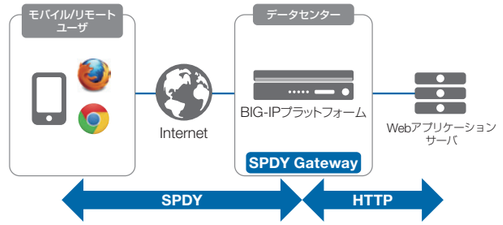


IPv6にいち早く対応

IPv4ネットワークとIPv6ネットワーク間での完全なアドレス変換とロードバランシングを実施。IPv4/IPv6が混在する環境を一元的に管理でき、費用効果の高いIPv6への移行を実現できます。

Webを加速させるSPDYゲートウェイ

最新のWeb配信プロトコルSPDYへの対応を、BIG-IPで代理することが可能です。SPDYプロトコルをBIG-IPで終端し、BIG-IPとWebサーバ間は従来通りHTTPで通信するため、サーバ側での追加投資、改修作業なしに、Web配信を高速化できます。



拠点間VPN

BIG-IPを対向設置することで、拠点間をIPsec VPNで接続できます。WAN高速化やセキュリティ機能とともに活用することで、専用線で結ぶのが難しい遠隔地のオフィスとも低コストで安全に、ネットワークを結ぶことができます。

わかりやすく高度な管理画面（GUI）

高度な管理GUIによって製品の設定が容易になり、設定や保守に要するコストを軽減します。GUIはSSLで保護されたブラウザベース インタフェースを介して提供され、オンライン ヘルプ、検索と並べ替えなど多数の機能を含み、大規模なシステムのメンテナンスに要する時間を大幅に短縮します。また、BIG-IPダッシュボードにより、システム パフォーマンスに関するリアルタイムな情報をひと目で確認できます。

ビジネス要件に合わせてITインフラ全体を最適化する
アプリケーション デリバリ コントローラ

BIG-IP®
Local Traffic Manager™ LTM

ITインフラ全体を最適化し、アプリケーション導入を成功へと導く

BIG-IP® Local Traffic Manager™（BIG-IP® LTM®）は、日々進化するビジネスアプリケーションに対応する柔軟性を備え、ITインフラ全体を最適化するアプリケーション デリバリ コントローラです。アプリケーションやサーバを理解したインテリジェントな機能により、より安全に、より高速に、より安定してアプリケーションを配信するだけでなく、アプリケーションやサーバの負荷をオフロードすることでリソースの有効活用を実現します。さらに、拡張性や管理の容易さも提供し、アプリケーション導入を成功に導きます。

課　題

- システムが突如ダウン。利用者に迷惑を掛け、会社は多大な損失を出してしまった
- 数ヶ月前にサーバを増設したばかりなのに、もう処理能力が限界になってしまった
- 単純なヘルスチェックでは最近の複雑なWebアプリケーションシステムに対応できない
- 対症療法的に設備投資を続けたせいで、システムが複雑になり運用の手間もかかって仕方がない
- システムの拡張や追加要件に対応したいが、開発する予算もスタッフも限られている
- システムやアプリケーションの高度化にともないITインフラが複雑化し、運用・管理のコストがふくらんでしまう
- サーバ集約環境にネットワークが対応しておらず、運用管理の手間が増えてしまった

解決策

- プロトコルの最適化やデータの圧縮など、負荷がかかる機能をサーバからオフロード。帯域をフル活用でき、サーバリソースもフル活用できることから、投資効果を最大化
- アプリケーションの正常性を常にチェック。万一障害が発生しても、いち早くデバイスを切り替えることで、決して止まらないWebシステムを提供
- システムを容易に拡張できるので、リソースを効率よく集約。また、必要な機能を簡単に追加拡張できる仕組みや柔軟な振り分けルールの実現により、TCO適正化をバックアップ
- ネットワークの運用支援、アプリケーション統合・導入支援を同時に提供することにより、運用管理コストを削減
- 柔軟な管理者権限設定やアクセス制御、重複IPアドレスの使用などにより、仮想化、集約化環境に対応

BIG-IP Local Traffic Managerの主な特長

- ロードバランサとしての高い基礎能力
- システムを止めない「安定稼働」
- リソースを最大限に活用した「高速配信」
- 攻撃を未然に防ぐ「安全性」

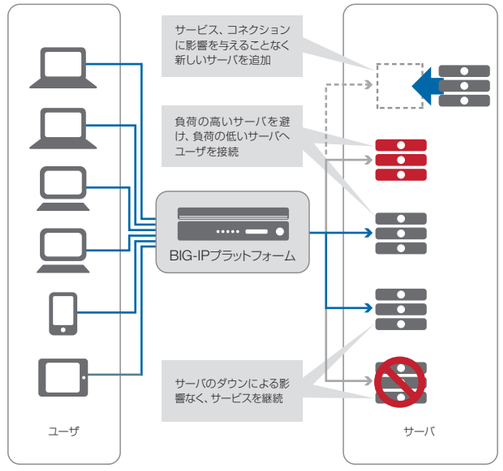
ロードバランサとしての高い基礎能力

多彩なロードバランシング ロジック

サイトに集中するアクセスを多数のサーバ群に振り分け、配信速度とサービスの安定性を向上させます。豊富なモードを備え、スタティック/ダイナミック ロードバランシングを可能にします。

- Round Robin mode
- Least Connection mode
- Observed mode
- Predictive mode
- Dynamic Ratio

ほか

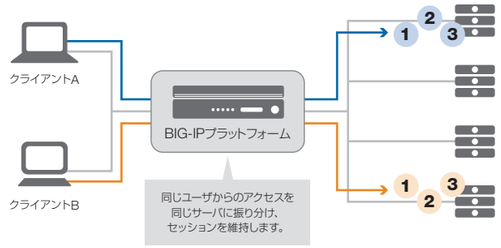


ディープ パケット インスペクション

ユニバーサル インスペクション エンジンを搭載し、パケットのヘッダだけではなくペイロードの内容まで精査するディープ パケット インスペクションを実現。高度なL7処理により適切なロードバランシングを可能にしています。

パーシステンス

セッションの整合性を維持するため、同一セッション中のクライアントを同一のサーバに振り分けるパーシステンス機能を備えています。ソースIPやCookieに基づくシンプルなパーシステンスのほか、アプリケーションの情報にもとづくユニバーサル パーシステンスが可能です。

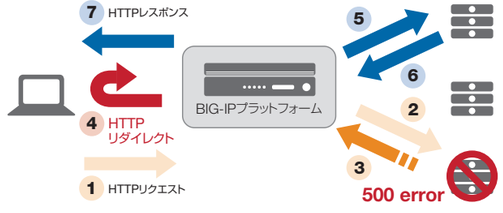


ヘルスモニタ

さまざまなアプリケーションサーバごとに、コンテンツをチェックするための独自のモニタプログラムの作成、擬似的にアプリーションを呼び出し、正常性をチェックするなど、複数のモニタの組み合せによって精度の高いヘルスチェックを行います。

応答エラー処理

トラフィックのエラーコードを見つけると、自動的に別のサーバに振り分けるため、クライアント側からはサイトが通常通り動いているように見えることから、ダウンタイムを実質ゼロにする究極のソリューションといえます。また、管理者にとっては、BIG-IPがあればサーバのヘルスチェックに要する負荷から解消されます。

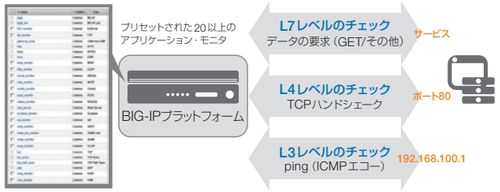


Silverline
BIG-IP
BIG-IP LTM
BIG-IP GTM
BIG-IP AAM
BIG-IP ASM
BIG-IP APM
BIG-IP AFM
BIG-IP CGNAT
BIG-IP PEM
BIG-IP LC
Enterprise Manager
BIG-IQ

システムを止めない「安定稼働」

アプリケーション モニタ

HTTP、TCPはもちろん、SIPやSNMP、SOAPなど20種類以上のアプリケーション モニタリング機を搭載。アプリケーションの稼働状態はもとよりアプリケーションの健全性を各レベルで正確に判断します。



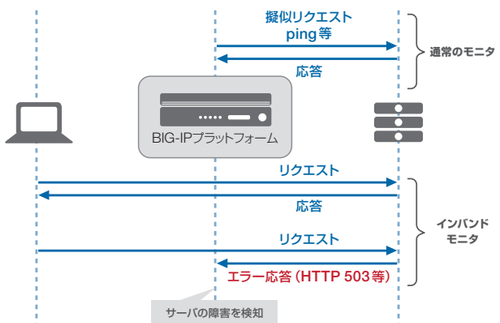
機器の稼働状態だけではなくアプリケーションの健全性を各レベルでチェックします。

高速シリアルフェイルオーバー

1秒未満で実行されるフェイルオーバー機能を搭載。ネットワーク検知機能も高速化され、ネットワーク切断にも即座に対応します。万一障害が発生しても、瞬時にデバイスやネットワークを切り替え、セッションを中断させません。

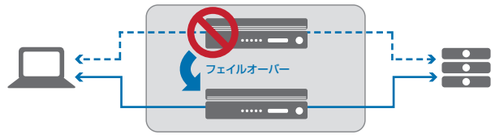
インバンド モニタ

実際にサービス提供で利用されているアプリケーショントラフィックを監視することで、サービスが提供可能な状態かどうか確認。個別に確認するトラフィックを送信する場合と比べ、BIG-IPへの負荷、アプリケーションサーバやネットワークへの負荷を軽減します。また、通常のアプリケーションモニタとの併用で、効率的なサーバのヘルスチェックが可能です。



コネクション ミラーリング

クライアントとサーバ間のセッション状態をミラーリングすることで、障害時にスタンバイユニットへ切り替わる際にもセッションを継続します。サイト利用者はサイトを継続利用できるので、BIG-IP LTMの障害がサイト利用を阻害することはありません。



セッションを維持したままフェイルオーバーするため、サイト利用者が障害に気づくことはありません。

コネクション リミット（iRules）

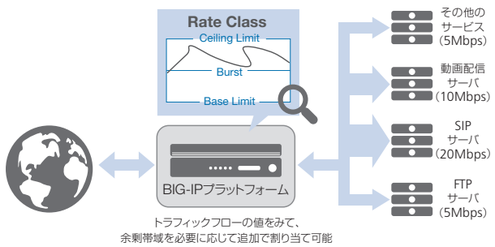
コネクション リミットは、サーバへの同時接続セッションを一定の値に制限する機能です。接続中のTCPコネクションをカウントし、あらかじめ設定しておいた数を上回った場合には新規のコネクションはリセットされます。サーバへのアクセス集中とコントロールすることで、アプリケーションの快適性を維持します。

Sorryメッセージ（iRules）

一定数以上のアクセスが集中し、アプリケーションを快適に提供できそうにない場合や、アプリケーションの健全性が保たれていない場合に、新規のコネクションをSorryサーバへと転送します。

L7レート シェイピング

基幹アプリケーションやVoIPなど、優先順位の高いアプリケーションを遅滞なく配信するよう、帯域幅を柔軟に管理。HTTPなどのバーストトラフィック発生時にも、リアルタイムアプリケーションの通信帯域を確保します。



HTTPなどのバーストトラフィック発生時にもリアルタイムアプリの通信帯域を確保。

攻撃を未然に防ぐ「安全性」

リソースクローキング

クライアントへのレスポンスに、サーバの情報や特定の文字列を含めないことで、脆弱性につながる手がかりを一切排除。悪意ある攻撃から情報資産を守ります。

Cookieの暗号化

クライアントとサーバの間でやり取りされるテキストデータであるCookieを暗号化することで、改ざんによる「なりすまし」を防ぎます。

GeoIPを使った公開地域の限定

IPアドレスと物理的な位置とを結びつけたGeoIPのリストを使い、接続元となるユーザの場所を高い精度で判断、Webサイトやアプリケーションの公開先を地理的に限定することが可能です。例えば、日本以外の地域へアプリケーションサービスを制限したい場合等に有効です。

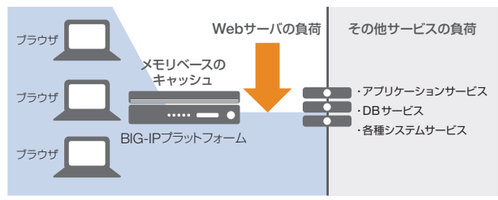
リソースを最大限に活用した「高速配信」

SSLアクセラレーション

SSL通信を開始する際の暗号化キーの生成のみならず、実際のデータを暗号化するバルク暗号処理もBIG-IP LTMが行うことで、サーバに負担をかけずに高速処理を実現します。

Fast Cache™

サーバに対し繰り返し要求される画像ファイルやスタイルシートなどのコンテンツをキャッシュの対象とすることで、サーバの負荷を軽減。圧縮済みコンテンツにも対応し、リソースを追加することなくユーザへの応答速度向上を実現します。キャッシュ対象のファイルを種類やディレクトリで指定したり、動的なコンテンツを除外するなどの設定にも対応します。



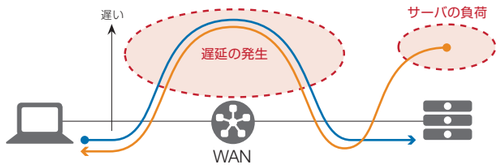
画像ファイルやスタイルシートなど、繰り返し読みだされるファイルをBIG-IP LTMから送信。サーバリソースをアプリケーション処理に集中できます。

HTTP圧縮

HTTPトラフィックを圧縮することで、データの転送速度を高速化し、帯域幅コストを削減します。圧縮効果の高いファイルのみを選択的に圧縮したり、遅延の大きい回線に対するレスポンスのみを動的に圧縮するなど、より効果的な場面のみでの圧縮利用も実現します。また圧縮処理はすべてBIG-IP LTMで行われるため、サーバの負荷はありません。

TCP Express™

TCP Expressは、TCP通信自体を最適化する機能です。RFC標準に準拠した最新のTCPスタックをBIG-IP LTMが提供することで、通信相手に特別なソフトや設定を行うことなく通信効率を向上できます。TCP通信における遅延や、通信帯域の無駄を省き、高速なレスポンスと回線帯域の有効活用を実現します。



WANを経由した通信においては、TCP通信における遅延がアプリケーション配信のボトルネックとなります。TCP ExpressはTCP通信を最適化し、帯域を有効活用します。

複数データセンターを集中管理する
アプリケーション デリバリ コントローラ

BIG-IP®
Global Traffic Manager™ GTM

リスクを低減し、アプリケーション配信を最適化しながら事業の継続性を確保

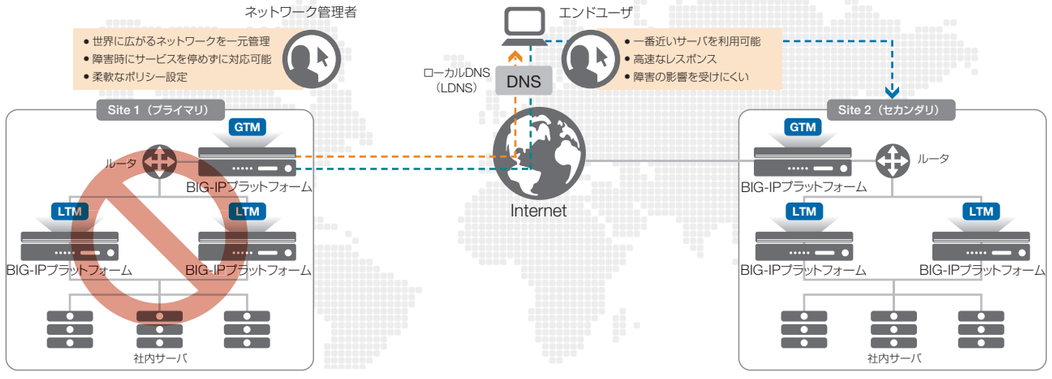
BIG-IP® Global Traffic Manager™（BIG-IP® GTM™）は、分散するデータセンター全体におけるアプリケーション配信を最適化する、アプリケーション デリバリ コントローラです。インフラとアプリケーションの状態を監視し、トラフィック管理を最適化し、事業継続性を実現します。さらに、DNSの外部脅威対策、DNSを狙ったDDoS攻撃対策としても豊富な実績を誇るDNS機能を強化、最新の脅威からサイトを守ります。DNS機能の拡張に伴い、より多くの環境で活用していただけるよう、多様な提供形態をご用意しています。

課　題

- システム障害により、サービスが停止
- 海外からのアクセスが遅くサービスが中断
- システムの停止やメンテナンス時には、手作業で対応
- 分散したデータセンターの運用管理の負荷とコスト増
- DNSの管理が複雑になり、設定と維持管理の工数大
- DNSを狙ったDDoS攻撃が増加。DNSダウンによる影響はメール、Webなど極めて甚大なのに効果的な対策が無い
- DNSサーバのパフォーマンスが低下、サービスの品質低下に繋がっている

解決策

- 複数のデータセンターを1つのドメイン名にまとめることで二重化する「広域負荷分散」を提供
- アプリケーションとネットワークの状況に応じて、最高のパフォーマンスが得られるサイトへユーザを振り分け
- サイトの稼働状況や、LANの状況、コンテンツの有効性まで判断し、システムを止めない
- すべてのリソースを視覚的に把握できる複数の管理ツールにより、複雑な分散ネットワークのシンプルかつ効率的な管理を実現
- 専用GUIにより、容易なDNS設定・管理を実現。IPv6にも対応
- 包括的なDNS外部脅威対策を実現。また、DNSのパフォーマンスを大幅に強化する事により、サービス品質の低下を防ぐだけでなく、DDoS攻撃に対する対策も実現



BIG-IP Global Traffic Managerの主な特長

GeoIPを含む多彩なメトリックで最適なルーティング

BIG-IP GTMはネットワーク メトリックに基づいて、最適なグローバルリソースへユーザをルーティングします。ラウンドロビンなど標準的なメトリックの他に、QoSや動的比率に応じたダイナミックルーティングも可能です。また地理的なルーティングにはGeoIPも使用でき、ドメイン名のみに頼るルーティングに比べ、はるかに高い精度でユーザを最適なリソースへ導けます。

- **QoSモード**
  多くのメトリック（RTT、Hop数、トポロジー情報、使用帯域など）から、ご使用の環境で重視されるメトリックを選択し、各々の重要度を相対的に勘案した上で、最適なサイトへ振り分けます。
- **動的比率モード**
  ネットワークやサーバリソースに関して取得した情報を動的な比率に変換し、その比率に基づいて対象の各々のリソースに振り分けます。
- **GeoIP**
  IPアドレスからユーザの場所を高い精度で判断、複数のデータセンターの中から物理的に近いサイトへアクセスを振り分けます。

次世代インターネットプロトコルIPv6をサポート

IPv6の需要が増大する中、多くのサイトではIPv6トラフィックの処理という新たな課題に直面しています。BIG-IP GTMは、AAAAレコードの設定など、IPv6アドレスの名前解決にも対応しています。

様々なアプリケーションをチェックする複数のモニタ

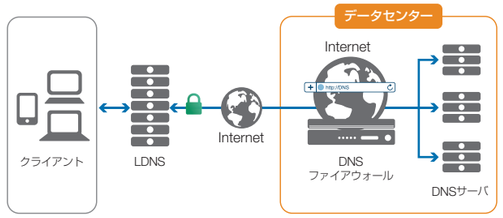
日々複雑化するアプリケーションの状態を判断するには、複数のモニタを組み合わせたヘルスチェックが必須です。複雑な構成のアプリケーションでも、迅速かつ的確に動作状況の判断を行い、ダウンタイムの軽減にも貢献します。

最新の経路制御技術IP Anycastをサポート

IP Anycastは、複数のデータセンターでサイトを運営する際、ユーザからネットワーク距離が最も近いサイトに誘導する技術です。サイトのレスポンス向上、障害時の影響の局所化が可能です。

多彩な機能を持つハイパフォーマンスでセキュアなDNSファイアウォール

BIG-IP GTMは各種のDNS機能を搭載しており、DNSファイアウォールとしても働きます。DNSの安全性を確保し、DNSクエリが確実に最適なデータセンターもしくはクラウドへとルーティングされる環境を実現します。



DNSファイアウォールとは

- マルチコアによるハイパフォーマンスDNS
- スケーラブルDNS – DNS Express機能
- 複数デバイスを活用した負荷分散– IP Anycast
- SecureなDNSクエリ – DNSSEC
- ルートベースで近いDCへ誘導 – Geolocation
- DNS iRulesによるきめ細やかなDNS管理

- **DNS Express**
  DNSクエリに対するレスポンスのパフォーマンスを劇的に向上させる機能です。DNSのクエリ返答を一部デレゲーションし、非常に高いパフォーマンスを誇るBIG-IP GTMで一部の処理を行うことによりDNSサーバのパフォーマンスを補完し、DNSレスポンス処理能力を向上させます。BIG-IP GTMに実装された、他の様々なDNS技術と併せることでDNS技術の強力な外部脅威対策、DNSを狙ったDDoS攻撃対策を実現します。
- **DNSの信頼性を確保する「DNSSEC」**
  DNS通信を公開暗号方式を使って通信することで、DNS情報の正確性を確保します。DNSに偽りの情報を書き込むことでユーザをフィッシングサイトなど悪意あるサイトに誘導するDNSキャッシュポイズニングなど、DNSがセキュリティホールとなる危険性を排除し、Webサイトとユーザを保護します。
- **DNS DoSアタックにも屈しない最大600万クエリ毎秒※の処理能力**　※VIPRIONの場合
  近年増加しているDNS DoSアタックは、DNSに対して処理能力を超える大量の不正リクエストを送信し、正規ユーザからのDNSリクエストを正常に処理できない状態に陥らせるものです。1秒間に最大600万クエリを処理可能なBIG-IP GTMはDNS DoSアタック中であっても正規のDNSリクエストに正常に対応できます。
- **DNSファイアウォール単体としても導入可能**
  複数サイト間の負荷分散要件がないネットワークにも、セキュアなDNSとしてBIG-IP GTMを導入できます。ハイパフォーマンスでスケーラブルなうえに、DNS iRulesにより柔軟性を身に着けた高機能なDNSとしてご活用ください。

クラウド時代の要求に応える
Webアプリケーション最適化ソリューション

BIG-IP®
Application Acceleration Manager™ AAM

WAN回線とWebアプリケーション配信を併せて最適化し モバイル機器からでも快適なアプリケーション利用を実現

BIG-IP® Application Acceleration Manager（BIG-IP AAM™）は、クラウド環境でのWebアプリケーション活用、モバイル端末などの多彩なデバイスからの高速アクセス、といった時代の要請に応え、WAN最適化とアプリケーション高速化を実現します。遅延の改善、ラウンドトリップ回数の低減、コンテンツの優先度管理などにより、回線品質の低いネットワークからでも快適なアプリケーション利用が可能になります。SaaSアプリケーションでは最大50倍のパフォーマンス改善が見込めます。

課　題

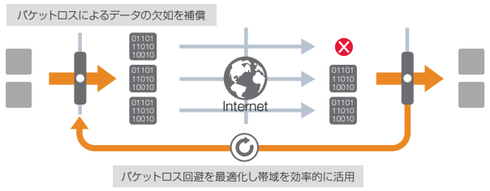
- WANを介したデータセンター間のデータレプリケーションに時間がかかりDRサイトとの同期が間に合わない
- WANを経由したデータセンターへのアクセスで高い実効速度を得られない
- 遅延の大きい国際回線を経由した海外拠点からの業務アプリケーション利用において早いレスポンスを得られない

解決策

- 配信側と拠点側に対向設置することでデータ量削減、プロトコル最適化を行い、アプリケーションを高速化
- 実際に送受信されるデータ量を削減しデータセンター間でのデータレプリケーションを高速化
- 遅延の大きいWAN回線で実効スループットを向上し、海外拠点からの業務アプリケーション利用環境を低コストで改善
- 高速化効果を可視化するダッシュボードを備え投資対効果を明確化

フォワード エラー コレクション（FEC）

FECは、高速通信インフラのない地域、あるいはクラウド環境などパケットロス率が高いネットワークにおいて、遅延の発生を改善します。データ送信の際に重複・余剰を持たせてパケットを送り出すことにより、エラーやパケットロスが起きても再送信・再受信を不要にし、通信品質の低いネットワーク環境下でも遅延の少ない通信を可能にします。



HLSビデオ配信最適化

iOS/Androidなどのスマートデバイスで採用されているHLS（HTTP live streaming）プロトコルの配信を最適化します。コンテンツの重要度（例：閲覧数の多少など）に応じたキャッシング、アクセス環境に応じたビットレート指定などを柔軟に判断し、個別の環境に適した映像配信を可能にします。

ダイナミック データ リダクション

メタデータやコメントなどの重要でないデータを削除し、データのサイズを最適化。モバイル環境などのWAN帯域やインターネットアクセスを効率化・高速化します。

F5 Application Speed Tester（FAST）

回線スピードをあらかじめ容易に検証できるよう、シミュレーション環境であるFASTを無償で提供しています。
www.f5.com/featured/performance-tools/f5-application-speed-tester/

対向設置によりWAN経由でのアクセスを高速化

アプリケーション配信側と拠点側に対向設置することで、WANを流れるデータ量の削減やプロトコルの最適化を行い、最大10～300倍もの高速化を実現します。

データセンター間の通信による帯域消費を最低限に

ディザスタリカバリや事業継続性確保ために必要なデータセンター間のデータレプリケーション。ただし、回線で遅延やパケットロスが発生するとデータ転送のパフォーマンスが極端に劣化し、データ転送時間が大幅に延びるなどの課題が顕在化します。BIG-IP AAMはデータレプリケーションに必要な帯域を削減し、遅延・パケットロスなどに起因する問題を軽減します。

BIG-IP LTMにモジュールを追加する事で2～60倍の効果

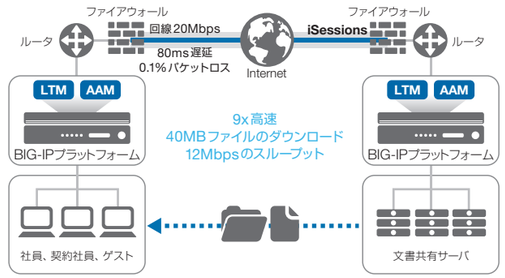
BIG-IP LTMには標準機能としてWAN最適化サービスが搭載されています。TCP通信の最適化によりアプリケーション配信を2～5倍程度高速化する機能です。BIG-IP AAMではデータの重複排除、プロトコル最適化の利用など、さらに高度な技術を投入することで、標準機能の約60倍、最大10～300倍の高速化が可能です。

効果を可視化するダッシュボード

WAN高速化の効果をリアルタイムに把握できるダッシュボード機能を搭載。BIG-IP AAMの機能による効果を体感でき、実際の費用対効果の把握にも役立ちます。

遅延の大きな回線でも帯域を有効利用できる

TCPの実行通信速度は遅延の大きさに依存するため、遠距離間の通信ではWAN帯域を使いきることができません。BIG-IP AAMは遅延による実行速度の低下を最低限に抑え、WAN回線が持つ性能を引き出します。特に国際回線のように回線コストが高い場合は、高コストな帯域増強よりBIG-IP WOMの導入が効果的です。



80msの遅延がある場合、有効スループットが2～4Mbps程度しか得られません。BIG-IP AAMを導入すれば、ネットワーク帯域を約9倍も効果的に使えます。

ダイナミック コンテンツ コントロール

ダイナミック コンテンツ コントロールは、ブラウザの挙動をコントロールして使用帯域幅を低減し、繰り返しや重複のあるデータのダウンロードを防ぎます。さらに、ブラウザの条件付きリクエストやWebアプリケーション間のデータ転送量を減らし、遅延が大きくエラーの多いWAN回線の影響を最小限にします。この機能はデータ圧縮のための標準技術で構成されており、Javaアプレットの起動要求やブラウザの設定変更が生じることもありません。ダイナミック コンテンツ コントロールには以下の機能が含まれます。

ダイナミック データ オフロード

ダイナミック データ オフロードは、同じデータへの重複したリクエストを防ぐことでサーバの負荷を軽減し、サーバが処理可能なリクエスト数を拡張します。ダイナミック データ オフロードには以下の機能が含まれます。

- SSLアクセラレーション
- ダイナミックキャッシング
- ダイナミック圧縮

検証済みポリシー内蔵で、容易な導入・設定を実現

検証済みのWeb高速化ポリシーを内蔵。迅速に設定、導入でき、すぐに最適なアプリケーション高速化を適用できます。これらのテンプレートを使用し、独自のWebアプリケーションに合わせてWebAcceleratorをカスタマイズすることも可能です。

双方向のトラフィックを監視する
アプリケーション ファイアウォール

BIG-IP®
Application Security Manager™ ASM

最も狙われやすいWebアプリケーションを保護し、ビジネスのリスクを軽減する

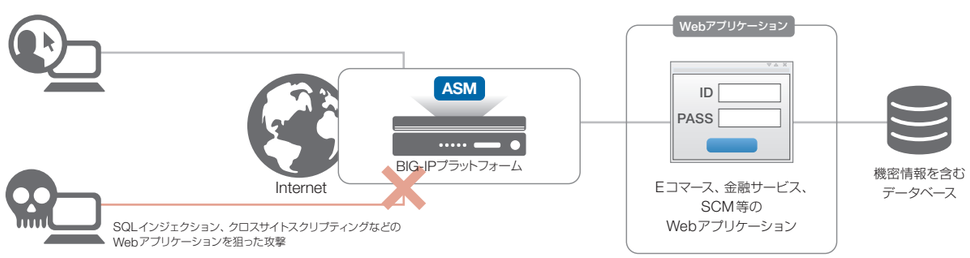
BIG-IP® Application Security Manager™（BIG-IP® ASM™）は、各種モジュールを組み合わせることによりL3からL7までのマルチレイヤ セキュリティ機能を提供するBIG-IP製品の中でWebアプリケーションの保護に特化したWebアプリケーション ファイアウォールの機能を提供します。正しいと定義されたトラフィックのみアクセスを許可するポジティブ セキュリティと、シグネチャをベースとしたネガティブ セキュリティを併用して攻撃を防御し、さらにSQLインジェクション攻撃への対応や情報のマスキングなどにより、情報漏えいリスクも軽減します。

課　題

- 外部から従来のファイアウォールでは防げない攻撃を受けている
- 高度なSQLインジェクションなど、既存のセキュリティシステム（ネットワーク型FW、IDS･IDP）では防御できない攻撃への対策
- Webアプリケーションをセキュアにプログラミングするコストが膨大になる。また、パッチをアプリケーションへ適用するまでの時間がかかる
- 誤検知のあったセキュリティポリシーの修正に手間がかかる
- WAFのポリシー作成に時間や知識が必要
- セキュリティ機能がボトルネックになり、Webアプリケーションのパフォーマンスが劣化
- PCI DSSに準拠したいが、手間やコストがかかり対応できない
- 追加でWAFアプライアンスを導入する費用がない

解決策

- レポーティング機能により、Webアプリケーションに対する攻撃を可視化
- 高度なSQLインジェクションを解析し攻撃を阻止。ポジティブセキュリティと、シグネチャをベースとしたネガティブ セキュリティの併用により、既知や未知の攻撃を防御
- シグネチャの試験的な適用により誤検知を事前に確認し、誤検知への対応コストを削減
- 事前に定義されたセキュリティポリシーを活用することでポリシーの作成時間を短縮
- 高速な処理エンジンとスケーラビリティの高いハードウェアプラットフォームにより、WAFによるパフォーマンス劣化を軽減
- PCI DSS要件6.6に対応
- BIG-IP Local Traffic ManagerにアドオンするだけでWebアプリケーションを保護



BIG-IP Application Security Managerの主な特長

きめ細やかなアクセス管理が実現する アプリケーションの外部脅威対策

BIG-IPファミリは多様な外部脅威対策を提供しますが、その中で主にL7のWebアプリケーションファイアウォール機能を提供するのがBIG-IP ASMです。TMOSやBIG-IP LTMと共に導入頂く事でL3からL7までネットワークトラフィックを包括的に理解し、30以上のDDoS攻撃を防ぐ強力なセキュリティソリューションをご提供します。BIG-IP ASMはコンテキストベースのユーザ情報などを元に管理し、豊富なログ機能と共に極めてきめ細やかなアプリケーション保護ソリューションをご提供します。アプリケーションのセッションとユーザネームを紐付けて管理するため、複雑なポリシーの実装も簡単に実現し、ユーザの行動に基づくアクセス拒否などの詳細なポリシー設定を簡単に導入でき、PCI DSSへの対応も支援します。

運用負荷を軽減するポリシーステージング機能

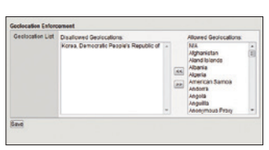
新たなシグネチャやポリシーを追加する際、適用後に誤検知が発生しないかどうかを事前に確認できます。個別のポリシー設定毎にブロックとトランスペアレントを選択できるので、既存のポリシーでWebサイトを保護しながら新たなポリシーの有効性を確認できます。シグネチャやポリシーのアップデート時に発生し得る誤検知への対応コストを削減します。

アプリケーションの可視化とレポーティングを実現

優れたレポート機能を標準で搭載。不正アクセスの検知や遮断した内容と理由、URL単位のパフォーマンス劣化が容易に判断できるレポートを提供することで、セキュリティインシデントへの迅速な対応や運用管理負荷軽減を実現します。

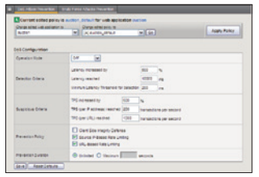
ジオロケーションブロッキング

地理情報に基づくアクセス管理をシンプルなユーザインタフェースで実現。特定地域、国単位でのアクセス拒否などを簡単に実装できます。



L7 DoS攻撃とブルートフォースアタックの防御

正確なトリガーと自動制御によりL7 DoS攻撃をブロックし、アプリケーションのパフォーマンスを改善します。この機能は、検知要素と、3種類の防御手法を次々に適用するという綿密な手段とテクニックに基づいています。さらに、失敗の多いログイン要求を絞り込むことによって、ブルートフォースアタックを検知、その危険を軽減します。サーバ応答からブルートフォースアタックを検知した場合、要求元のブラウザを低速化します。高い割合でログイン プロセスに失敗し続けているIPからのログイン要求を絞り込むこともできます。



Ajax、JSONなど最新技術に対する脅威にも対応

Web画面をリアルタイムで書き換えるAjaxにも対応。JSONのデータ形式を読み取り、Ajaxを利用した攻撃からもサイトを保護します。

Webスクレイピング攻撃からの防御

Webスクレイパーと呼ばれるWebアプリケーションに含まれる情報を自動収集するプログラムによる情報流出を防ぎます。クライアントが、自動プログラムなのか通常のユーザからのアクセスなのかを識別し、自動プログラムのアクセスをブロックします。

データガード

Webアプリケーションからクライアントへ渡る個人情報や機密情報などをマスクすることにより、クライアントのWebページへの表示を防ぎます。さらに、エラーページとアプリケーションエラー情報を隠し、攻撃の手がかりとなるようなインフラ情報をハッカーに与えません。

多様な脆弱性診断ソリューションと連携

新たに発見される脆弱性をいち早く検知し、自動的にその脆弱性に対処するポリシーを作成する連携を実装しています。これにより、作業効率の向上だけでなく緊急性が高い脆弱性対策を極めて早く対応し、実装する事が可能となります。様々な脆弱性診断ソリューションと連携し、幅広いニーズやユースケースに合った最適解をご提供可能です。

- Cenzic社 Hailstorm
- Qualys社 QualysGuard Web App. Scanning
- IBM社 IBM Rational AppScan
- WhiteHat社 WhiteHat Sentinel

アプリケーションからWeb、リモートまで
すべてのアクセスをカバーする統合アクセス ソリューション

BIG-IP®
Access Policy Manager® APM

内外双方向のユーザトラフィックをきめ細やかに監視・管理し、効率的な運用と強固なセキュリティを両立

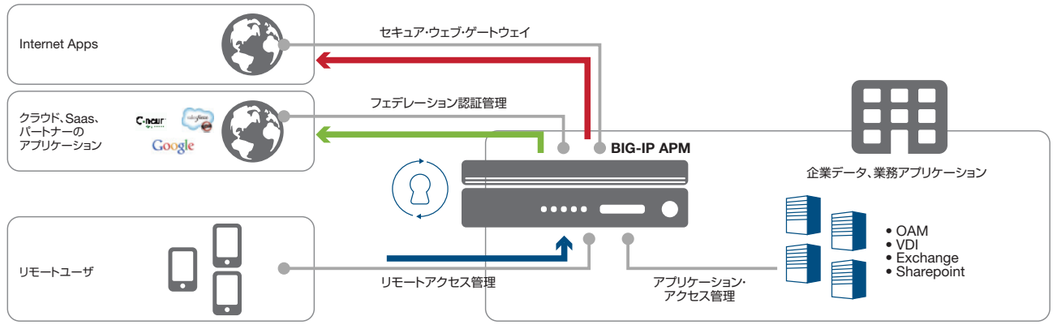
BIG-IP® Access Policy Manager®（BIG-IP® APM™）は、社外からのリモートアクセス、社内からの多様なリソースへのアクセスが求められる時代に対応した、統合アクセス ソリューションです。社内外のアプリケーションへのアクセス制御、URL単位でのフィルタリング、マルウェア対策といった万全なセキュリティ機能を提供すると同時に、複数のドメイン対応、豊富なシングルサインオン（SSO）認証など使いやすさの向上も実現。さらに、iPhone、iPad、Androidをはじめとする豊富なデバイス対応、充実したレポート機能も魅力です。

課　題

- サーバやアプリケーションの数が多く、適切なセキュリティ管理のために多大な人員と時間が必要
- ネットワーク機器、セキュリティ機器と多数の機器でシステムが複雑化し、コストも増大
- アプリケーションの数だけユーザID、パスワードを覚え、個別にログインしなくてはならない
- ネットワーク上に仕掛けられた不正プログラムがますます高度化、巧妙化し、企業システムへの感染の危険が増大
- 業務アプリケーションのモバイル対応を進めるため、エンドポイントのセキュリティ確保やモバイルユーザの権限管理が必要
- 従来のインフラはネットワーク中心で設計されており、アプリケーション中心で規定されたセキュリティポリシーを厳密に施行するのは困難

解決策

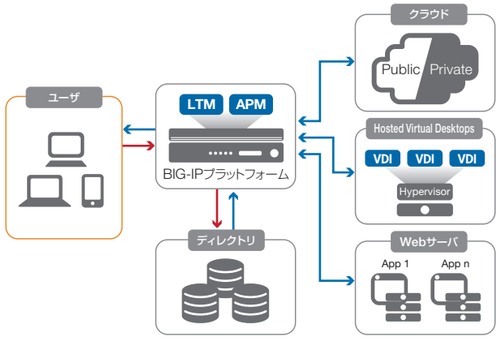
- ネットワークの要となるアプリケーション デリバリ コントローラにセキュリティ管理機能を追加することで、システムをシンプルにし、低コストですべてのアプリケーションのセキュリティを向上
- アプリケーションとの認証を代行し、シングルサインオンを実現
- 侵入を試みるマルウェアの挙動を解析し、企業システムへの感染を未然に防止
- アクセスポリシーにエンドポイントチェックを追加し、セキュリティポリシーに適合した端末からのみ接続を許可
- 高度なL7処理によりアプリケーションを中心としたセキュリティポリシーを施行可能



セキュアなリモートアクセス管理

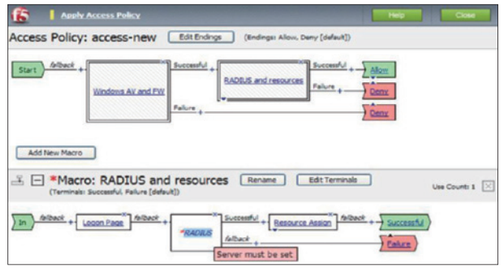
安全なリモートアクセス環境の提供

長年リモートアクセス分野に取り組んできた中で培ったノウハウを活かして、高いセキュリティを実現しながら快適でユーザフレンドリーなリモートアクセス機能を実装しました。Webベースの業務アプリケーションはもちろん、SSLトンネルを利用してすべてのTCPアプリケーションを社外から利用できます。エンドポイントのセキュリティ状態まで考慮して、アクセスしてきたユーザを適切なリソースにのみ導くことで、利便性もセキュリティも高めることができます。また、今後普及が見込まれるIPv6クライアントからのアクセスにも対応し、多様な環境への対応を進めています。



フローチャート式の「ビジュアルポリシーエディタ」

アクセスポリシーは見やすいフローチャート式で作成。グループ、ユーザ、デバイスごとの容易な管理を実現します。



大規模導入に応える最大6万同時接続のハイパフォーマンス

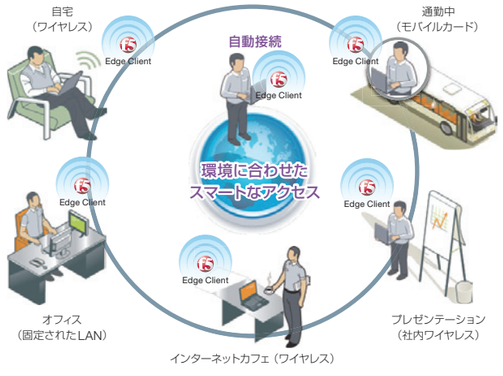
アプリケーション デリバリ コントローラとして性能の高さに定評のあるアプライアンスを採用しており、最大で6万ユーザからの同時接続に対応可能です。スケーラビリティが高く、サイトやビジネスの成長に合わせてその能力を拡張できます。

業界最高のエンドポイント セキュリティ

利用者がログオン前にセキュリティ状態をチェックする「ログオン前シーケンス」。クライアントOSの種類やIEのバージョン、パッチの適用状況だけでなく、ウイルス対策ソフトが最新の状態で稼働しているかなどのチェックを行います。また、MACアドレス、CPU情報、HDD ID情報などを検査し、煩雑なマシン証明書を使うことなく端末のハードウェア検査をする、包括的なエンドポイント セキュリティを備えています。この優れた機能はリモートアクセスはもとより、社内LANやワイヤレスLANにおいても有効です。

BIG-IP® Edge Client®

ネットワーク環境に応じて最適な接続を自動選択するクライアントPC専用のソフトウェアを標準で提供しています。接続されているネットワークをクライアントソフトウェアが自動的に社内ネットワークなのか社外ネットワークなのかを判別し、社外のネットワークに接続した場合には自動的にBIG-IP Edge Gatewayへの接続が行われます。ユーザは接続するネットワークを意識する必要がなく、ログオンに伴う作業負荷を軽減し、ユーザビリティが向上します。



最新のOS、クライアントをサポート

Windows 7（x64）、IE9、Mac OS Xなど最新のOSへの対応は勿論、iPhone iOS 6.x、Android 4.xなどの多様なモバイル端末でのポータルアクセスをサポートしています。クライアント側のインストール作業の手間を最小化し、Windowsログオンクレデンシャルの再利用が可能で、ユーザビリティを向上します。

マルチドメインでの運用も可能

BIG-IP APMは仮想化してマルチテナントで運用することもできます。それぞれのドメインには、個別のセキュリティポリシーを適用して運用できます。テナントごとに完全に独立しているため、IPアドレスの重複などの制限もありません。

きわめて高いコストパフォーマンス

アプリケーション デリバリ コントローラと統合できるため、セキュリティ専用機器に比べて格段に高いコストパフォーマンスを誇ります。既存のBIG-IPにモジュールとして導入することもできるため、新たにセキュリティ機器を導入することなく低コストでシステム全体のセキュリティを強化できます。

多様なMDMソリューションと連携

BIG-IP APMはリモートアクセス ソリューションとして様々なパートナー企業様と連携し、更なるバリューをご提供します。その中でも、スマートデバイスの急速な普及に伴い、モバイル端末を管理するニーズに対しても積極的なパートナー様との連携を開始しています。

- Mobile Iron社
- Airwatch社
- サイバートラスト社
- アイキューブドシステムズ社

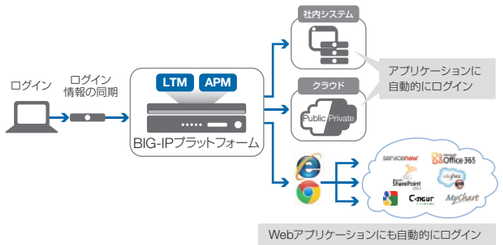
シンプルで自由自在のフェデレーション認証管理

クラウド環境のファイルにもシングルサインオン

ますます利用が広がっているクラウド環境。APMの強力なシングルサイオン機能機能により、プライベートはもちろん、パブリッククラウド上のリソースも含め、クラウド上にあるすべてのファイルへのアクセス権限を自在に設定できます。

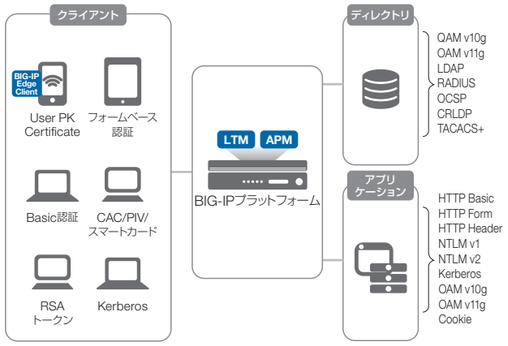
シングルサインオン機能がSAMLもサポートし、豊富なユースケースに対応

ハイブリッドクラウド環境で複数のWebアプリケーションと業務アプリへのシームレスなアクセスなどを実現する、シングルサインオンはSAMLにも対応し、快適なビジネス環境を提供します。



多彩な認証方式に対応

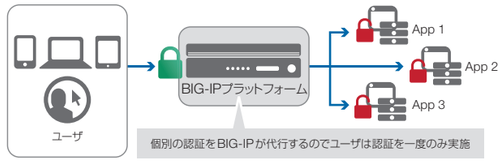
セキュリティをさらに強化するには、アクセスしてきたユーザが本人かどうかのチェックが不可欠です。BIG-IP APMでは、ワンタイムパスワードやSSLクライアント証明書を使って、ログオン時のユーザ認証を強化する各種認証ソリューションを多数用意しています。



柔軟で強固なアプリケーション アクセス管理

Webアクセスのコントロール

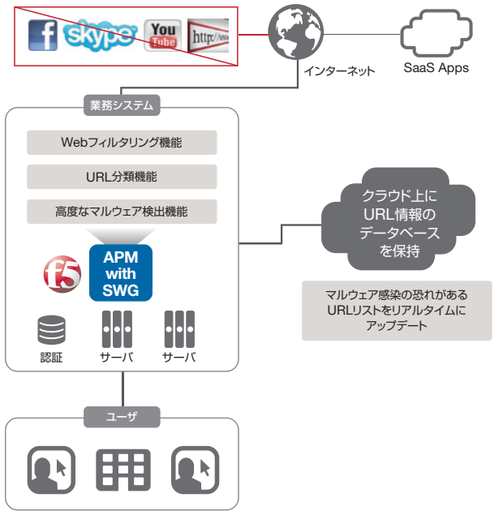
業務に多く使われているWebアプリケーションですが、そのままインターネットに向けて公開するのは危険です。BIG-IP APMがあれば、確実なセキュリティを担保した上で、正規ユーザにのみアクセスを許可できます。また、各Webアプリケーションのクレデンシャル情報を内部にキャッシュし、バックエンドのWebアプリケーションへの認証をBIG-IP APMが代行することで、ユーザはアプリケーションごとにログイン操作をすることなく、Webアプリケーションを利用できるようになります。



端末、ユーザを完全に把握可能なログ機能

アプリケーションのログインをBIG-IP APMが代行するので、アプリケーション利用ログを残すことが可能です。従来はアプリケーションごとに確認しなければならなかったログをBIG-IP APMに集約できるので、ユーザや端末を軸にした動向を把握しやすくなります。

Web利用の安全性を強化するセキュア ウェブ ゲートウェイ



URL単位でWebアクセスをフィルタリング

業務に関係のないWeb閲覧を防止、あるいはウイルス感染につながる危険なWebへのアクセスを未然に防止するため、URL単位でWebアクセスをフィルタリング。フィルタリングするURLリストも簡単に作成・管理できます。

不審な動きをキャッチしてマルウェア侵入を防止

悪意のあるWebサイトは年々増加しており、その攻撃は巧妙化、凶悪化の一途。単純にWebサイトを閲覧するだけでも各種のマルウェアに感染するリスクが高まっています。F5セキュア ウェブ ゲートウェイは社内のユーザがインターネット上のWebサイト・サービスにアクセスするトラフィックを解析し、マルウェアの社内への侵入をブロックします。悪意のあるWebサイトのリストは随時アップデートされるため、管理の負担も最小化できます。

リモートを含めたきめ細やかなユーザ管理から外部ネットワークへのアクセス管理まで包括的に提供

外部ネットワークへのアクセス制御（従来のURLフィルタリング）、マルウェア検知というセキュア ウェブ ゲートウェイの機能と、アクセス管理セキュリティ、セキュアなリモートアクセス、ハイブリッドクラウド認証連携、端末セキュリティチェックといったAPMの機能。これらを組み合わせることで、F5ならではの効率的なユーザ管理とセキュリティが実現できます。また、外部へのアクセス制御から管理対象のユーザプロファイルまでを一貫した分かりやすいGUIで一括管理できるため、運用管理性も大幅に向上します。

アプリケーション セントリックなセキュリティを実現する
ハイパフォーマンス ファイアウォール

BIG-IP®
Advanced Firewall Manager AFM

ネットワークの中核で
統合されたセキュリティを提供

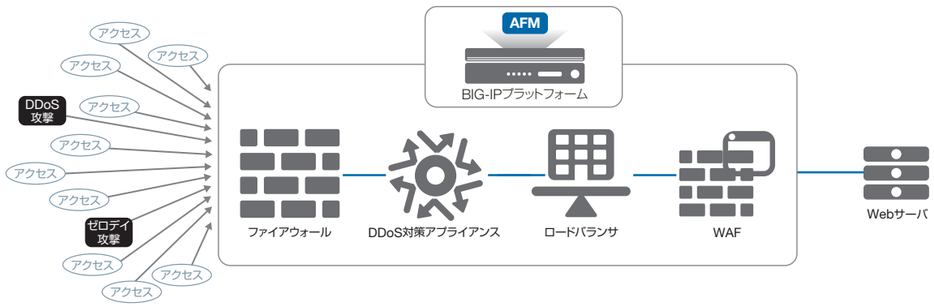
BIG-IP® Advanced Firewall Manager（BIG-IP AFM）は、ハイパフォーマンスで多彩な機能を提供する先進的なネットワーク ファイアウォールです。トラフィック処理に極めて特化したBIG-IPだからこそ実現できるその圧倒的なパフォーマンスにより、急増するトラフィックに対応することが困難になりつつある従来型ファイアウォール製品では成し得ない多くの問題点を一気に解消します。さらにその高いパフォーマンスを活かし、BIG-IPの持つ多様な技術と外部脅威対策の統合による管理性向上、コスト削減を実現します。

課　題

- リスクの多様化に応じてポリシー追加を繰り返し、管理が複雑化
- ポリシーが整理されていないため、追加・修正時にはーから作業が必要。担当者が代わると、設定内容の確認さえ困難に
- レスポンス低下の不安から取得するログの種類を制限
- 広範囲にログ取得しようとするとハイエンド機が必要。SSLやHTTPなどのログは取得そのものが困難
- DDoS攻撃元の特定や防御は人手によるため、対応が後手に
- サービス品質を維持するにはファイアウォールと別に専用ハードが必要で、高コストなうえ構成も複雑化

解決策

- 階層的なポリシー管理を実現し、ポリシーの一括適用、変更／削除が容易に。担当者異動や組織改編にも迅速な対応
- ポリシー変更時に起きがちな設定ミスを事前に予防できるポリシーステージング機能を提供
- 超高速なロギング機能により、従来より広範なログの取得が可能。エントリー機種でもレスポンス低下の不安なし
- SSL、アプリケーションレベルをはじめとしてより深いログの取得が可能
- DDoS攻撃対策作業の一部を自動化し、迅速対応。対策スタッフの作業負担は大幅に軽減
- 圧倒的なパフォーマンスでDDoS対策などの機能も統合できるため、コスト効率の良い投資を実現。ネットワーク構成もシンプルに



BIG-IP Advanced Firewall Managerの主な特長

従来型FWと比べると驚異的 ADC製品ならではのスループットとコストパフォーマンス

L3からL7のアプリケーションレイヤすら包括的に対応できる、広範囲なマルチレイヤ セキュリティを実現します。複数レイヤにまたがる確かなインスペクションにより従来では複数デバイスが必須であった環境に対して統合・コスト削減を実現します。また、驚異的な処理能力で、レスポンスを落とすことなくサイトを保護し、デバイス集約によるコスト削減、管理ポイントの低減を実現します。

多くの攻撃からサイトを確実に保護

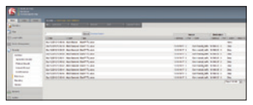
BIG-IPが持つ柔軟なトラフィックコントロール機能を使い、サイトの安全性を維持し続けます。

- **DDoS防御**
  SYNフラッド攻撃などのTCP攻撃をはじめ、IP攻撃、HTTP攻撃など30種類以上のDDoS攻撃からサイトを防御できます。
- **ゼロデイ攻撃防御**
  サーバ側での緊急対応が難しいゼロデイ攻撃にも、iRulesを駆使して対応可能です。BIG-IPで攻撃を排除することで、サーバへのパッチマネジメントの柔軟性が向上します。

ファイアウォールエンジンを統合し 管理性、パフォーマンスが向上

BIG-IP AFMでは高度に統合されたファイアウォールエンジンにより、BIG-IP LTMよりもさらに高いパフォーマンスと、L3-L7まで網羅した高い管理性を得られます。

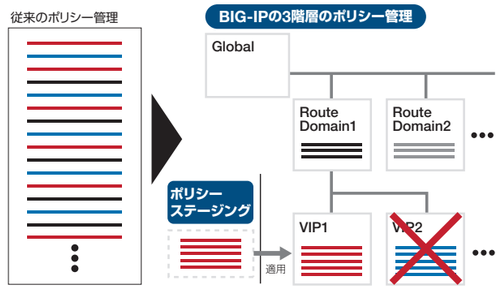
- **統合されたGUI**
  ファイアウォール機能の設定、管理がBIG-IPの管理GUIに統合され、サイトのパフォーマンスとセキュリティをひとつの設定画面で管理できます。
- **ロギング、レポーティング機能**
  パケット処理のログを詳細に記録し、抽出したログからレポートを作成。レポートフォーマットは多数用意され、ユーザによるカスタマイズも可能。

アプリ視点での3階層のポリシー管理

BIG-IP AFMは、セキュリティポリシーを3つのレイヤーで体系的に管理しています（下図参照）。このため設定内容を見通し良く把握し、設定の変更や追加、削除などを容易に行えます。例えば、サービス提供のポイントとなるVIPのポリシーを削除しても、ほかのVIP のポリシーには一切影響を与えないため、安心してポリシー変更ができます。

このようなファイアウォールポリシーをアプリケーション単位で設定していけば、ダイナミックに日々新しいアプリケーションやサービスが展開・縮退していく今日のクラウド データセンターで、ファイアウォールも迅速な設定変更が可能となり、アプリケーション環境に適した運用を実現できます。



ミスを事前に検出するポリシーステージング機能

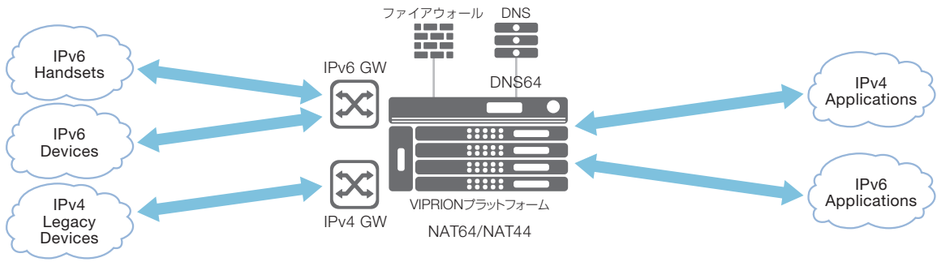
ファイアウォールのトラブルはポリシー変更後やアプリケーション追加後に発生しやすいもの。こうした事態を回避できるよう、BIG-IP AFMはポリシーステージング機能を搭載（上図参照）。事前に実運用に近い環境で実トラフィックに基づいた、「新しいポリシー適用後の動き」をシミュレーションできるため、しっかりと挙動・リスクなどを精査した上で変更作業を実行でき、深刻なトラブルの発生を防止することが可能です。

L7を理解するF5だから可能な
アプリケーション視点のキャリア向けNATソリューション

BIG-IP®
Carrier Grade NAT CGNAT

アプリケーションを
IPv4/v6のあらゆる端末へ

BIG-IP® Carrier Grade NAT（BIG-IP CGN）は、IPv4からIPv6への移行期間に混在するIPv4、IPv6アプリケーションをIPv4、IPv6のあらゆる端末に向けてサービスするための大規模NATソリューションです。高速でスケーラビリティに富むだけではなく、BIG-IPのファイアウォール機能、セキュリティ機能やポリシー管理機能との集約により、優れたコストパフォーマンスを実現します。



スケーラブルで可用性の高いNATサービス

止まってはならないネットワークの中核におけるトラフィック処理に特化して開発されたBIG-IPプラットフォームにより、膨大な端末との同時接続にも耐える高いパフォーマンスと、高い可用性を発揮。

BIG-IPファミリの幅広い
アプリケーションデリバリ技術との集約により
大きなシナジー効果を発揮

例えば、ポリシー制御、DNSサービス、キャリアグレードのファイアウォールやGiファイアウォールなど、BIG-IPが持つ様々なモジュール、機能を一台のプラットフォームに集約し、よりアプリケーションやサービス視点のソリューションをキャリアインフラにご提供します。また、機器の集約により管理ポイントの削減、運用プロセスの効率化も期待できます。

NAT64/DNS64

IPv6のみに対応する端末に向けて、IPv4のみをサポートするアプリケーションを配信する際に必要となる機能です。IPv6をゲートウェイでIPv4にNATすることで、IPv4アプリケーションへの接続を可能にします。IPv4サービスを利用する際に必要な名前解決においても、DNS64によりIPv6に変換されたアドレスで応答します。

NAT44

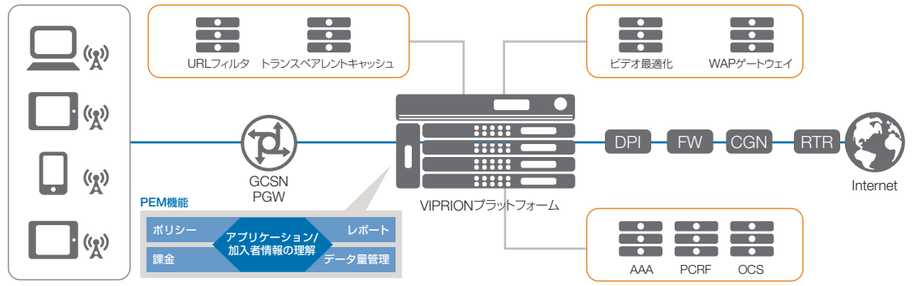
IPv4のみに対応する端末からのトラフィックをIPv4にNATすることで、限られたIPv4アドレスでより多くのIPv4端末を収容可能になります。IPv4端末が多数ある期間はNAT44として活用し、IPv6端末の増加に合わせてNAT64機能を活用することで、移行期間全体においてBIG-IP CGNを活用できます。

ユーザ、アプリケーションに応じた制御を実現する
ポリシー制御ソリューション

BIG-IP®
Policy Enforcement Manager PEM

トラフィックを可視化し
加入者ごとのプロファイル別に最適なサービス提供を効率的に実現

BIG-IP® Policy Enforcement Manager（BIG-IP PEM）は、ユーザごと、アプリケーションごとのトラフィックを可視化し、制御するトラフィックコントロールソリューションです。アプリケーションの品質を確保し、ユーザごとのトラフィック制御、個別のサービス品質の提供などのきめ細やかなトラフィック管理を実現します。トラフィックコントロールの機能をBIG-IPに統合することで、パフォーマンス拡張や新サービスを展開しやすいシンプルなネットワークが実現します。



トラフィックを可視化する
Traffic Classification

トラフィックの中身を精査し、アプリケーションやユーザごとにトラフィックを分析可能。利用状況を正確に把握することで適正な課金やアプリケーションに応じた帯域コントロールを実現できます。

- **ユーザごと、アプリケーションごとの分析**
  ユーザやプロトコルに応じたL4-L7のトラフィック分析により、ポート単位、加入者のIPアドレス単位、基地局などの単位で精細な情報を提供します。分析機能はBIG-IPに統合され、GUI画面を使って設定できます。
- **シグネチャベースの挙動分析**
  あらかじめ設定したシグネチャを使い、トラフィックの挙動分析を行います。多彩なアップデート方法を用意しており、サービス追加などに応じたシグネチャ更新にも柔軟に対応可能です。

Policy Engineによる加入者情報の管理

PCRFとのGxインターフェイスをサポートし、加入者情報に基づいて帯域利用ポリシーを適用し、ユーザやプランに応じたサービスを提供可能。

加入者情報に基づくトラフィック管理

加入者の分類、アプリケーションの種類に応じてトラフィックを制御可能。DSCPやL2 QoSのマーキング機能も持ち、ユーザやアプリケーションに応じたトラフィック品質の確保に貢献します。

詳細なレポーティング

統計情報やユーザ、アプリケーションの利用情報をレポート出力。サードパーティ製分析エンジンとの連携も可能です。

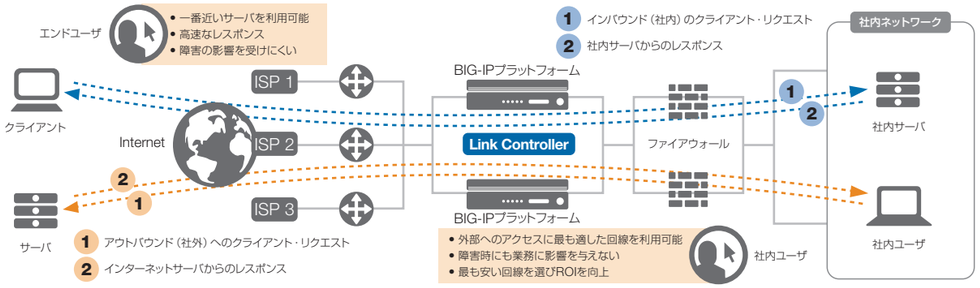
複数のWANリンク（ISP）を最適に制御する
アプリケーション デリバリ コントローラ

BIG-IP® Link Controller™

Link Controller

WANリンクを最適化しながら事業の継続性を確保

BIG-IP® Link Controller™（BIG-IP® LC™）は、ファイアウォールやインターネット回線を二重化するアプリケーション デリバリ コントローラです。複数のWANリンクのパフォーマンスや健全性をシームレスに監視し、ISP回線や接続ルータに障害が起こった場合の回線切替えはもちろん、マルチホーミング時の高度な経路制御を実現。障害時の自動切替えを備えた複数回線を使った効率的なインターネットアクセスを提供します。



回線をアクティブ/ アクティブで運用可能

リアルタイムのトラフィックフローに基づき、トラフィックをリンク全体に分散・制御できることから、回線を二重化したうえ利用可能な帯域幅が増加します。混雑していないリンクへトラフィックを移すことで、サイト全体のパフォーマンスが向上します。

高度なトラフィック分散を実現する「多様なメトリック」

複数のISP回線のアベイラビリティをチェックするだけでなく、インバウンド/アウトバウンドのそれぞれでベストなパフォーマンスを提供できるよう、さまざまなメトリックでビジネスポリシーを定義できます。

コストに基づく回線の選択

最もコストのかからないリンクにトラフィックを転送し、帯域幅に対する投資を最小限に抑えます。ISPの課金モデルなどを考慮して異なる接続によって帯域幅を最大化するので、非効率な帯域幅を抑えつつ、遅延を解消します。

リンクのパフォーマンスをアップする多彩な機能

- **WANリンクのコストを削減する「HTTP圧縮」**
  トラフィックの圧縮モジュールを使用することで、インターネットに送出するトラフィックを削減、WANリンクの必要な帯域幅を縮小します。ISPコストを引き下げると同時に、帯域幅のボトルネックを改善してアプリケーション配信の高速化を実現します。
- **トラフィックの優先順位を定義できる「帯域制御」**
  VoIPなどミッション クリティカルなアプリケーションに対して、優先的に通信帯域を確保します。また、特定のトラフィックタイプが帯域を使用しない時は、他のタイプがその帯域を流用できるよう定義づけられるので、WANリンク帯域幅の節約およびアプリケーションの応答時間が改善されます。
- **TCPプロトコルの非効率性を解消する「TCP 最適化」**
  TCP Express機能により、リンクの帯域幅利用に悪影響を及ぼし不要な遅延を引き起こすTCPプロトコルの非効率性を解消。エンドツーエンドのパフォーマンスの改善やコストの軽減にもメリットをもたらします。

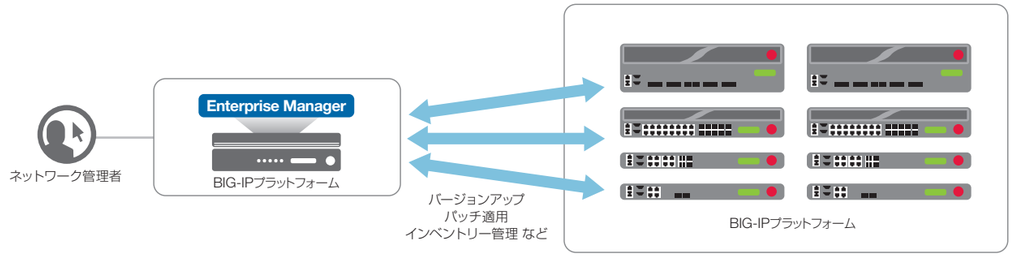
ネットワーク上のBIG-IP製品を
一元管理するソリューション

Enterprise Manager™

Enterprise Manager

複数のBIG-IPデバイス向けに低価格の中央集中管理を実現

Enterprise Manager™は、ネットワーク内に存在するすべてのBIG-IPデバイスの表示および管理を一元化するソリューションです。複数のBIG-IPデバイスの管理・運用にかかるコストを削減し、冗長構成時の設定アーカイブの作成と保全、ソフトウェア アップグレートやセキュリティパッチの迅速な展開が可能になります。環境の健全性の維持や、先見性のある警告通知も行われます。



BIG-IPのソフトウェアの中央管理

Enterprise Managerではネットワーク内の複数のBIG-IPに対して、ボタンひとつで同時に新しいソフトウェア バージョンや修正プログラムを読み込ませることが可能です。既存のデバイス設定やライセンスは新規ソフトウェアバージョンの読み込み時も完全に保持されるので、アップグレード中に重要な情報が紛失する心配はありません。インストールの正常な終了はEメールで確認できます。

BIG-IPデバイスの一覧表示と制御

すべてのBIG-IPデバイスに関するプラットフォーム情報はEnterprise Managerに保存され、簡単に探し出すことができます。各BIG-IPのソフトウェア バージョンの表示や選択が可能です。ステータスチェックに対する応答がない場合は警告が送信されます。デバイス間で設定の同期をとることも可能です。

中央集中化によるBIG-IPの設定内容のバックアップと復元

それぞれのBIG-IPに保存されている設定ファイルやライセンス情報を定期的にバックアップし、デバイスごとに複数の設定内容を保存できます。いつでも過去の設定状態に戻すことができるので、設定エラーからの回復が早く、デバイス再設定時の安全を確保できます。以前の設定にロールバックする可能性を残したまま、一時的にネットワーク設定を変更できるので、異なるネットワーク設定を試しながらトラブル シューティングも可能です。

BIG-IPにインストールされた証明書の一元管理

Enterprise Managerでは、企業内のBIG-IPデバイスにあるSSL証明書および期限の表示を一元管理できます。証明書の期限が近づくと、SNMP、Eメール、またはsyslogによる警告を発行できます。最新の証明書を保持するための対処時期および対象デバイスを常に正確に把握できます。

複数台のBIG-IPの管理工数を劇的に削減する
集中管理のための次世代マネジメント ソリューション

BIG-IQ™

BIG-IQ Device　BIG-IQ Cloud　BIG-IQ Security

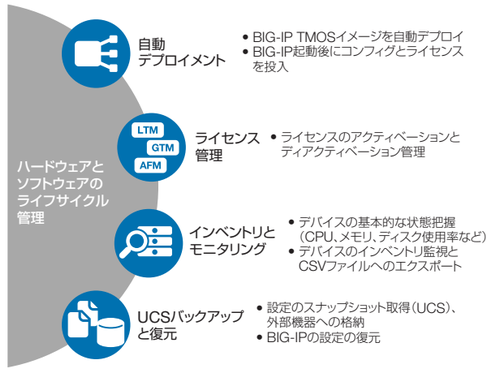
BIG-IP製品の展開にかかる時間を劇的に短縮、運用面でも様々な技術を統合し、他社製ソリューションとの連携も可能

ITインフラが大規模化、複雑化し、仮想化技術の利用も一般化している今日、ネットワークの管理工数は急激に増加。また、クラウドの活用も進むなど、ネットワークには従来とまったく発想の異なる管理手法が求められます。BIG-IQはこうしたニーズに応える次世代マネジメント製品です。ライフサイクルをカバーする効率管理、パブリッククラウドも含めた広範なオーケストレータとの連携、包括的なセキュリティ管理、直感的なスマートUIの採用などにより、複数のBIG-IPプラットフォームを一括して容易に、しかも調和的に集中管理。生産性の劇的な向上を強力に支援します。

BIG-IQの主な特長

- 拡張可能なモジュラ型のアーキテクチャ
- BIG-IQ Deviceが一貫した効率的な管理環境を提供
- BIG-IQ Cloudが柔軟で広範なオーケストレーションを実現
- BIG-IQ Securityがセキュリティ環境を包括的にコントロール

BIG-IQ Device　一貫した効率的な管理環境を提供



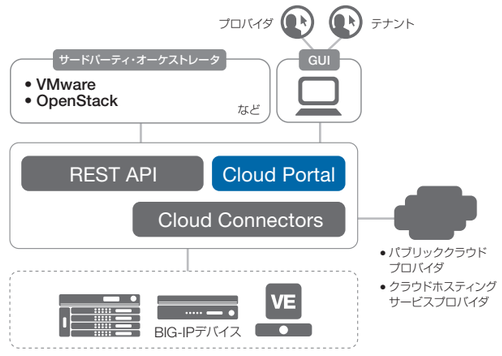
ライフサイクル全体を効率的に管理

機器の設定から必要なライセンスの管理、稼働状況の監視、設定情報のバックアップまで、BIG-IQ Deviceは複数のBIG-IPデバイスを一括管理できる統合的な環境を提供します。自動化も積極的に採用し、管理業務の大幅な効率化が可能です。

BIG-IP VEのライセンスを自在に展開・縮退

仮想版BIG-IPのプールライセンスを別途購入すれば、仮想アプライアンスを「プール化されたリソース」として、環境の変化に応じてスピンアップ／スピンダウン、再配置する事が可能になります。複数のアプリケーションやサービスが頻繁に追加･変更される環境で、仮想ADCの柔軟な配置が求められるユーザに最適なソリューションです。

BIG-IQ Cloud　柔軟で広範なオーケストレーションを実現



REST APIで他のオーケストレータと柔軟に連携

BIG-IQ Cloudは、クラウドのオーケストレーションのための技術であるREST API形式でインタフェースを公開。VMWareやOpenStackなどをはじめとするサードパーティが提供する多様なオーケストレータとの連携が可能です。利用環境に縛られない、柔軟なBIG-IPの管理を実現します。

サービスのカタログ化で作業効率が劇的に向上

ネットワークの管理工数を急増させ、デプロイメント期間の長期化にもつながる設定の複雑な作成作業や頻繁な変更作業。こうした問題をBIG-IQ Cloudはサービスのカタログ化で解消します。数クリックするだけで設定の作成や変更は即完了。BIG-IQ Cloudが、複数BIG-IPの管理業務を一新します。

BIG-IQ Security　セキュリティ環境を包括的にコントロール

複数台のBIG-IPセキュリティ製品を一括管理

BIG-IQ Securityは、ファイアウォール、WAFといったBIG-IPセキュリティ製品を一括して集中管理するためのモジュールです。ハードウェアアプライアンスに加え、バーチャルエディションのBIG-IPも管理可能。複数のセキュリティポリシーを一元的に、そして容易に管理することが可能になります。

セキュリティ管理をビジュアルに支援

スマートフォンライクなスマートUIを採用し、使いやすさを追求。加えて、収集したセキュリティ関連のログを分かりやすく表示するレポーティング機能も充実しています。