特集記事
システム運用における最適なネットワーク アプリケーション制御

FUJITSU Network IPCOM EX シリーズ　ビジュアライザと次世代ファイアーウォール

目次

目次

1	**多様化するネットワークアプリケーション**	**3**
2	**ネットワークアプリケーションを制御するには**	**5**
2.1	ビジュアライザ機能の特徴	5
2.2	アプリケーション・ファイアーウォール機能の特徴	6
2.3	アプリケーション辞書の特徴	7
3	**適切なシステム運用を行うために**	**8**
3.1	「①運用状態の可視化」フェーズ	9
3.2	「②運用状態の分析」フェーズ	10
3.3	「③運用ポリシーの変更、適用」フェーズ	10
3.4	「④運用ポリシーの評価」フェーズ	10

多様化するネットワークアプリケーション

1　多様化するネットワークアプリケーション

ｅ－ｍａｉｌやＷｅｂページからはじまったインターネットは、Ｆａｃｅｂｏｏｋ、Ｔｗｉｔｔｅｒ、ＬＩＮＥ等に代表されるソーシャル・ネットワーキング・サービス（ＳＮＳ）やｇｏｏｇｌｅなどの検索サービス、動画配信サービス、クラウド・コンピューティングをベースとしたさまざまなアプリケーション・サービスなどへ進化し、現在もその速度は衰えることなく、進化し続けています。

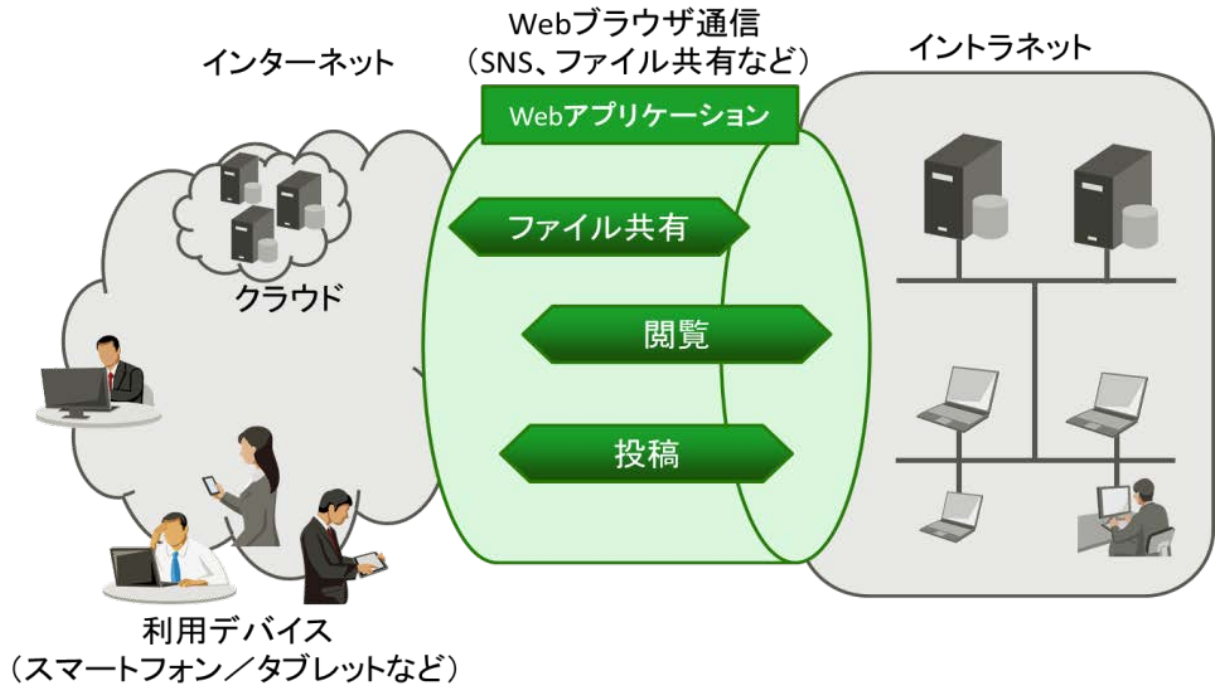

図１．多様化するネットワークアプリケーション

ＳＮＳやクラウド・コンピューティングベースの多様なアプリケーションが個人や企業へ浸透している現在、悪意の第三者からの攻撃以外に、とくにＷｅｂベースのアプリケーションに対する不適切なアクセスによって、企業内の機密情報漏えいや、企業の信頼およびイメージの低下といったリスクを招く危険性が高まっています。
このような事態を未然に防ぐために、多様化するネットワークアプリケーションを適切に制御することが必要です。

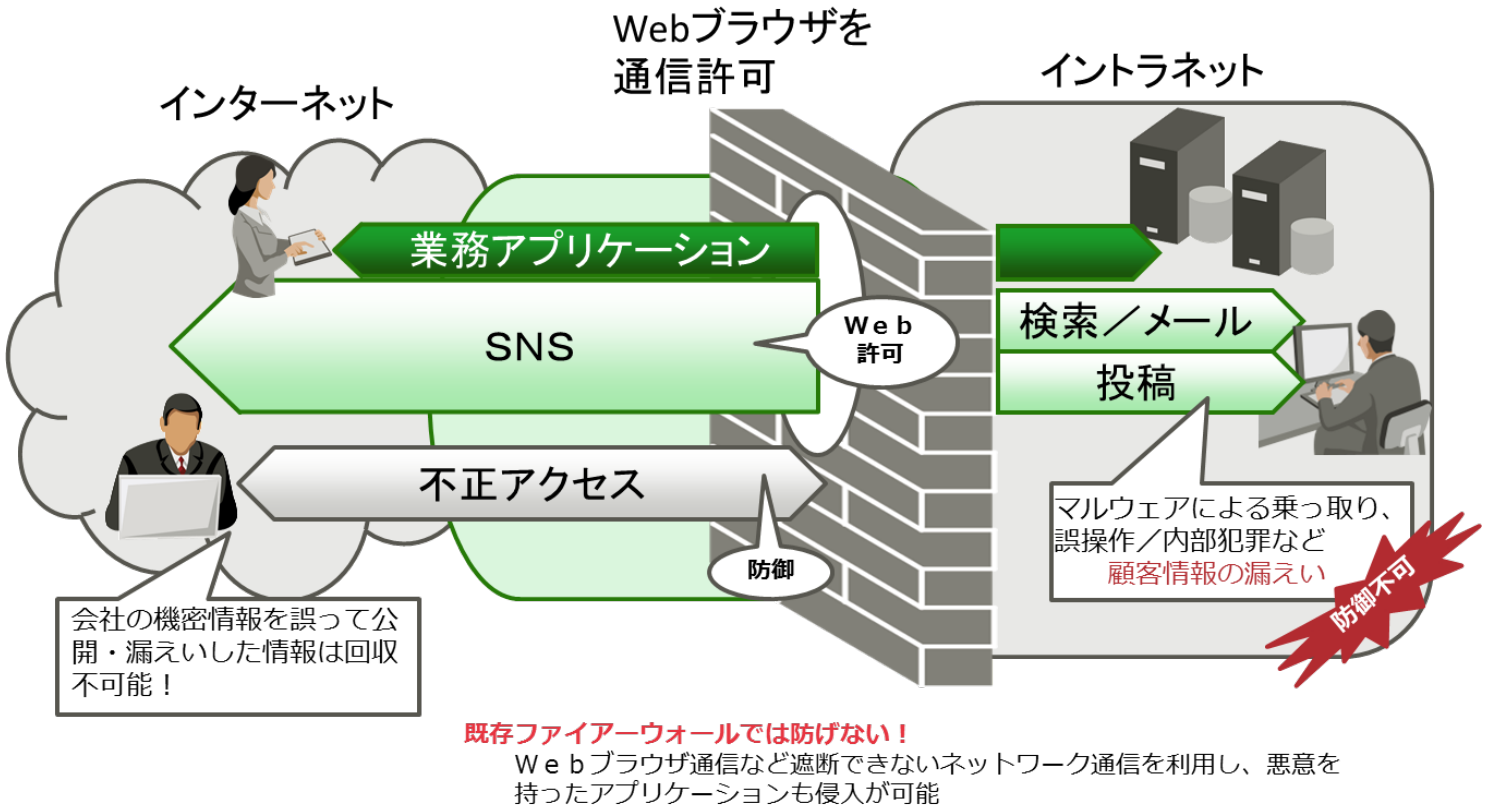

図２．情報漏えいのリスク

ネットワークアプリケーションを制御するには

2　ネットワークアプリケーションを制御するには

多様化するネットワークアプリケーション（特にＷｅｂをベースとしたアプリケーション）は既存のファイアーウォール機能では制御することができません。このようなネットワークアプリケーションを適切に利用するには、アプリケーションを可視化することでアプリケーションの識別を容易にし、制御する次世代ファイアーウォールとよばれるアプリケーション・ファイアーウォール機能が各社から提供されています。
IPCOM EX シリーズではアプリケーション辞書を利用し、アプリケーションを可視化するビジュアライザ機能とアプリケーションを制御するアプリケーション・ファイアーウォール機能を提供しています。

2.1　ビジュアライザ機能の特徴

ビジュアライザ機能は、装置を通過するネットワーク・トラフィック（サービス，アプリケーション）を収集して、さまざまな統計情報を円グラフ、棒グラフ、折れ線グラフ、表などで可視化することができます。管理者は、視覚的に装置の運用状況を把握でき、運用ポリシー（FW ポリシー，QoS ポリシーなど）の適用状況を検証、評価することを可能としています。
また、ビジュアライザ機能は、採取した統計情報を PC 上のハードディスクに蓄積しておくことができます。管理者は、ネットワークの利用傾向やサービス品質の傾向を把握でき、ネットワーク帯域の増強などのキャパシティ・プランニングを行うことができます。

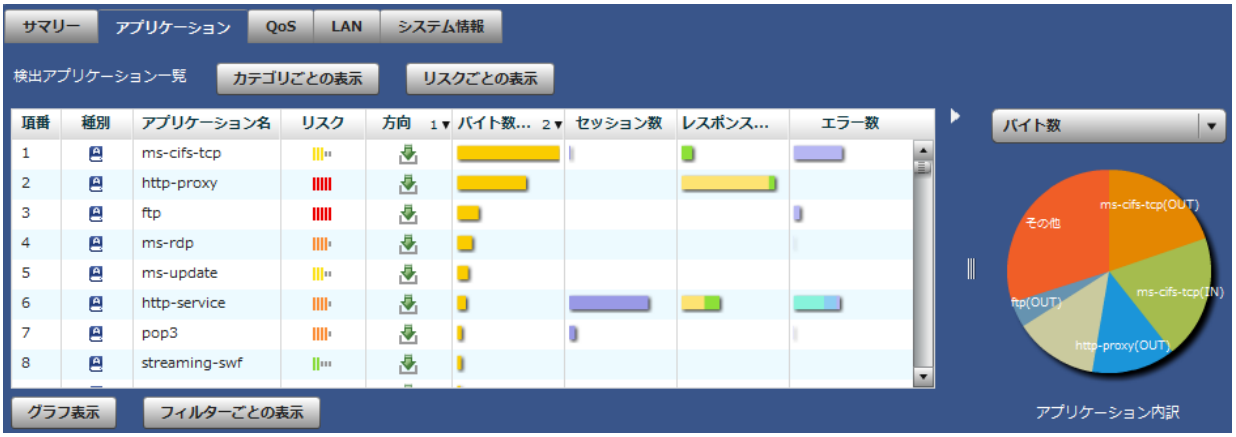

図４．ビジュアライザ

2.2 アプリケーション・ファイアーウォール機能の特徴

アプリケーション・ファイアーウォール機能は、アプリケーションの名前（または識別番号）を定義するだけで簡単に多種多様なアプリケーションを制御することができます。この制御には、制御対象となるアプリケーションの情報をアプリケーション辞書という形式で組み込み、ファイアーウォール機能と連携することで実現しています。

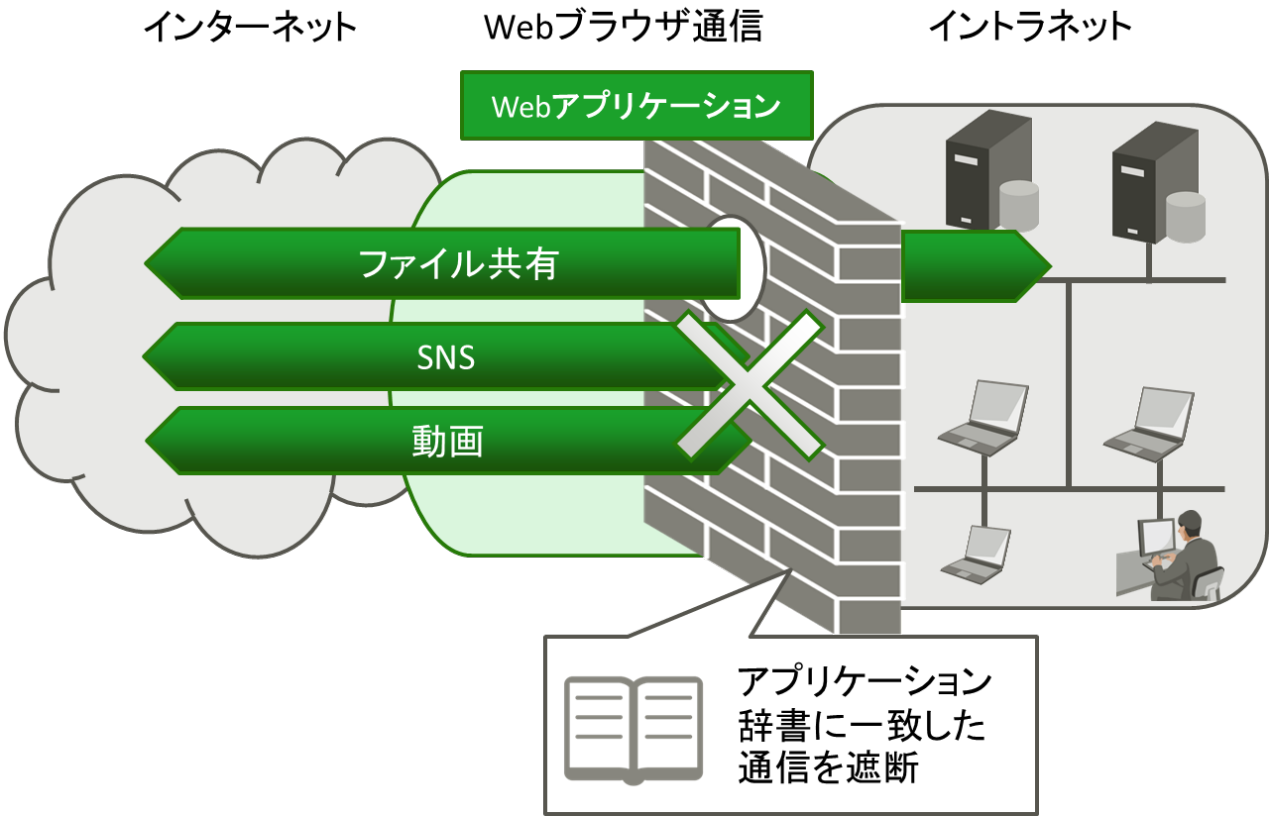

図３．アプリケーション・ファイアーウォール

アプリケーション・ファイアーウォール機能を利用することで、これまで、URL やプロトコルなど制御対象のアプリケーションを識別するための複数の条件を管理者自身が専門的な知識を駆使して作成していましたが、アプリケーション辞書の採用によりアプリケーション名を選択することで条件作成の労力を完全に排除することができ、管理者の運用負荷を抑えることができます。

2.3 アプリケーション辞書の特徴

アプリケーション辞書は、プロトコルやアプリケーションの名前とそれらを識別するための各種情報で構成されたデータベースです。アプリケーション辞書には、各種通信プロトコルやポート番号ベースのアプリケーションに加え、HTTP プロトコルベースの Web 2.0 技術が採用された、SNS、メディア共有サービス、ブログ、掲示板、オンラインストレージサービス、チャットやメッセンジャー、P2P、ファイル共有アプリケーション、リモートコントロールアプリケーションなどが 2800 種類以上のアプリケーションが登録されています。
また、各アプリケーションには、リスクレベルが設定され、アプリケーションを利用する際の危険度を示しており、リスクレベルは、アプリケーションの特性（セキュリティ回避能力、情報漏えいの危険性、ファイル転送能力、リモートコントロール能力、既知の脆弱性の有無、多くの帯域を消費する可能性、知名度や公衆性）とセキュリティ脅威（情報漏えい、データ改ざん、踏み台、マルウェア感染、DoS 攻撃や不正アクセスに利用される可能性）の観点から，総合的に評価して独自に決定しています。
アプリケーション辞書には、アプリケーションごとに、詳細情報を記載したヘルプファイルを提供しています。管理者は、ヘルプファイルを参照することで、組織のセキュリティ・ポリシーに照らし合わせて、アプリケーションをどのように制御すべきかの判断材料として利用できます。

アプリケーション情報

facebook　　Print　Close

識別番号	50801100
概略	Facebook Social Networking Service
説明	Facebook(フェイスブック)は、Facebook, Inc.が運営・提供する、世界最大のソーシャルネットワーキングサービス(SNS)です。Facebookは、2004年に米国の学生向けにサービスが開始されました。当初は学生だけに限定していましたが、2006年9月から一般にも開放されました。日本語版は、2008年5月に公開されました。Facebookの大きな特徴として、実名登録制があります。顔写真やプロフィールもリアルなものを公開しているユーザーが多く、情報の発信者も受信者も全員が実名でリアルティを追求したサービスになっています。プロフィールの名前登録もメールアドレスなどの情報に基づいた本人確認をスタッフ側で行うなど、実名制の促進に力を入れています。Facebookは、メール、カレンダー共有、写真・動画共有、アプリゲーム、ブックマーク共有、ノート共有、チャット、グループ、メールアドレス取得など、非常に豊富な機能、サービスを提供しています。Facebookは、標準で、TCPポート番号80(HTTP)と443(HTTPS)を使用します。
ヘルプバージョン	1.0.0
最終更新年月日	2012/05/07

リスク	4(大きい)
グループ	General Internet
カテゴリ	social-networking
種類および通信技術	web-service
プロトコル番号	TCP(6)
標準TCPポート番号	80,443
標準UDPポート番号	-
規格ドキュメント	-

特性	セキュリティ回避能力	なし
	機密情報漏えいの危険性	あり
	ファイル転送能力	あり
	リモート・コントロール能力	なし
	既知の脆弱性の有無	あり
	多くの帯域を消費する可能性	なし
	知名度、公衆性	あり

競合情報	-

必要なアプリケーション識別条件 (fixup protocol) アプリケーション識別条件...	サービス名	プロトコル	代表的なポート番号
	http	tcp	80
			8080
	https	tcp	443

関連アプリケーション	ファイアーウォール、帯域制御(QoS)などで本アプリケーションより**低優先**で設定が必要なもの
	http-service(10000260),https-service(10000270),http-proxy(10400900)
	ファイアーウォール、帯域制御(QoS)などで本アプリケーションより**高優先**で設定が必要なもの
	facebook-webmail(50201350),facebook-webchat(50301600),facebook-post(50801101),facebook-video(60000750),facebook-video-upload(60000751),facebook-photo(60300280),facebook-photo-upload(60300281)

図５．アプリケーション辞書

最新のネットワークアプリケーションは、改善などの変更が行われることで、それまでの通信方法と異なる通信方法が利用されるなど、激しく変化します。そのためアプリケーション・ファイアーウォール機能やビジュアライザの機能を有効に利用するためには、見知らぬネットワークアプリケーションをカスタム辞書へ登録するなど、適切な運用サイクルで最大限の効果を引き出すよう運用していただく必要があります。

適切なシステム運用を行うために

3　適切なシステム運用を行うために

ネットワークアプリケーションを利用して得られる効果を最大限に引き出す運用を維持していくためには、企業内での利用状況の推移を監視することが重要です。そのための運用手順を説明します。

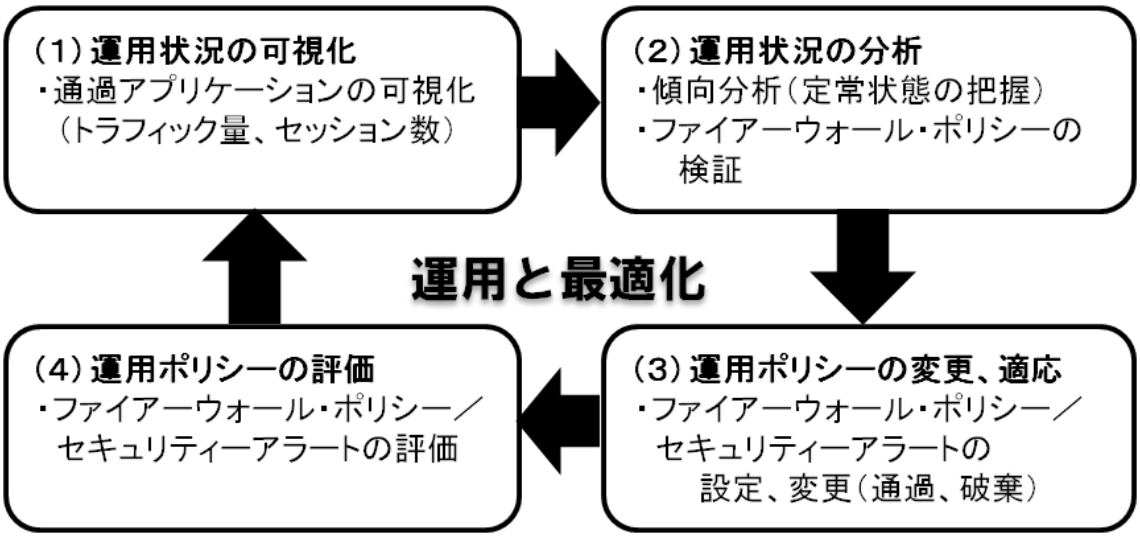

図６．適切な運用サイクル

3.1 「①運用状態の可視化」フェーズ

アプリケーションの多様化が進んだ現在、ファイアーウォールや帯域制御などを組織のネットワーク環境に導入し利用状況にあった運用ポリシーを設計するためには、どのようなアプリケーションがどの程度利用されているのかを把握することが重要です。従来は高度な専門知識を持った技術者が、採取したデータを解析するために多くの時間が必要としていました。
IPCOM EX シリーズではビジュアライザ機能を利用することで、ネットワークアプリケーションを可視化し、 P2P アプリケーション、オンラインストレージなど情報漏えいの引き金となるアプリケーションや、企業活動に直接関係ないと考えられるゲームなど想定外のアプリケーションの使用などネットワークアプリケーションの利用頻度を把握し、提供するアプリケーションヘルプを参照しながら、ファイアーウォール・ポリシーの設計を行います。

図７．アプリケーションヘルプ

3.2 「②運用状態の分析」フェーズ

使用されているアプリケーションが判明したあとは、1 日、1 週間、1 カ月といった単位でネットワークの利用特性を把握し、ネットワーク利用者が快適にアプリケーションを使えるように考慮することが重要です。従来はネットワークキャプチャー装置を使用し大量のデータを保存して解析しなければならず、データを保存する場所の確保や、データ解析のための人員確保が必要としていました。

IPCOM EX シリーズのビジュアライザ機能を利用することで、ネットワークデータを保存する時点で解析に必要なデータが分類され、必要なデータだけを長期間データ保存するとともに、蓄積されたデータからネットワークの使用傾向を把握します。

3.3 「③運用ポリシーの変更、適用」フェーズ

アプリケーションの可視化や把握したネットワークの使用状況をもとに運用ポリシーを設計／設定後は、設計に基づいた運用ポリシーとなっているかを確認することが重要です。遮断すべきアプリケーション通信が FW を通過していたり、通過すべきアプリケーション通信が遮断されたりしていると、業務の円滑な運営やビジネス機会の損失、さらには企業イメージの低下を引き起こすおそれもあります。

IPCOM EX シリーズではビジュアライザ機能の監視機能を利用することで、運用ポリシーが適切かを簡単に検証し、監視結果に基づいて運用ポリシーをより適切に変更します。

3.4 「④運用ポリシーの評価」フェーズ

アプリケーションの可視化やネットワークの利用特性に基づいて設計した運用ポリシーであっても、社会や組織の状況変化に伴って運用ポリシーを適宜評価し、追随することが重要です。その運用を実現するためには、常にネットワークの利用状況を監視し運用ポリシーから逸脱していないことを確認しなければならず、管理者の負荷が増大していました。
IPCOM EX シリーズではビジュアライザ機能が提供するモニタ・コンソールを利用することで計測結果を定期的に評価します。

この運用サイクルを日ごろから、４つのフェーズを実践することで、適切なシステムの運用を維持・継続することが大切です。

IPCOM EX シリーズが提供するアプリケーション・ファイアーウォール機能やビジュアライザ機能は、ネットワークアプリケーションの制御に効果を発揮し、安全で安定したネットワーク運用を実現することで、これまで高度な専門知識を持った技術者による分析や解析を代行し、管理者の負担軽減が実現できます。

本書でご紹介した機能は以下の IPCOM EX シリーズでご利用いただけます（2015 年 9 月）。

◎アプリケーション・ファイアーウォール機能利用可能なシリーズ

FUJITSU Network IPCOM EX1100SC
FUJITSU Network IPCOM EX1300SC
FUJITSU Network IPCOM EX2300SC
FUJITSU Network IPCOM EX2500SC
FUJITSU Network IPCOM EX2700SC

FUJITSU Network IPCOM EX1100NW
FUJITSU Network IPCOM EX1300NW
FUJITSU Network IPCOM EX2300NW
FUJITSU Network IPCOM EX2500NW
FUJITSU Network IPCOM EX2700NW

FUJITSU Network IPCOM EX2300IN
FUJITSU Network IPCOM EX2500IN
FUJITSU Network IPCOM EX2700IN

◎ビジュアライザ機能利用可能なシリーズ

FUJITSU Network IPCOM EX1100LB
FUJITSU Network IPCOM EX1300LB
FUJITSU Network IPCOM EX2300LB
FUJITSU Network IPCOM EX2500LB
FUJITSU Network IPCOM EX2700LB

FUJITSU Network IPCOM EX1100NW
FUJITSU Network IPCOM EX1300NW
FUJITSU Network IPCOM EX2300NW
FUJITSU Network IPCOM EX2500NW
FUJITSU Network IPCOM EX2700NW

FUJITSU Network IPCOM EX1100SC
FUJITSU Network IPCOM EX1300SC
FUJITSU Network IPCOM EX2300SC
FUJITSU Network IPCOM EX2500SC
FUJITSU Network IPCOM EX2700SC

FUJITSU Network IPCOM EX2300IN
FUJITSU Network IPCOM EX2500IN
FUJITSU Network IPCOM EX2700IN

お問い合わせ
FUJITSU LIMITED
Web サイト: jp.fujitsu.com
2015 年 9 月

© Copyright Fujitsu Limited All rights reserved