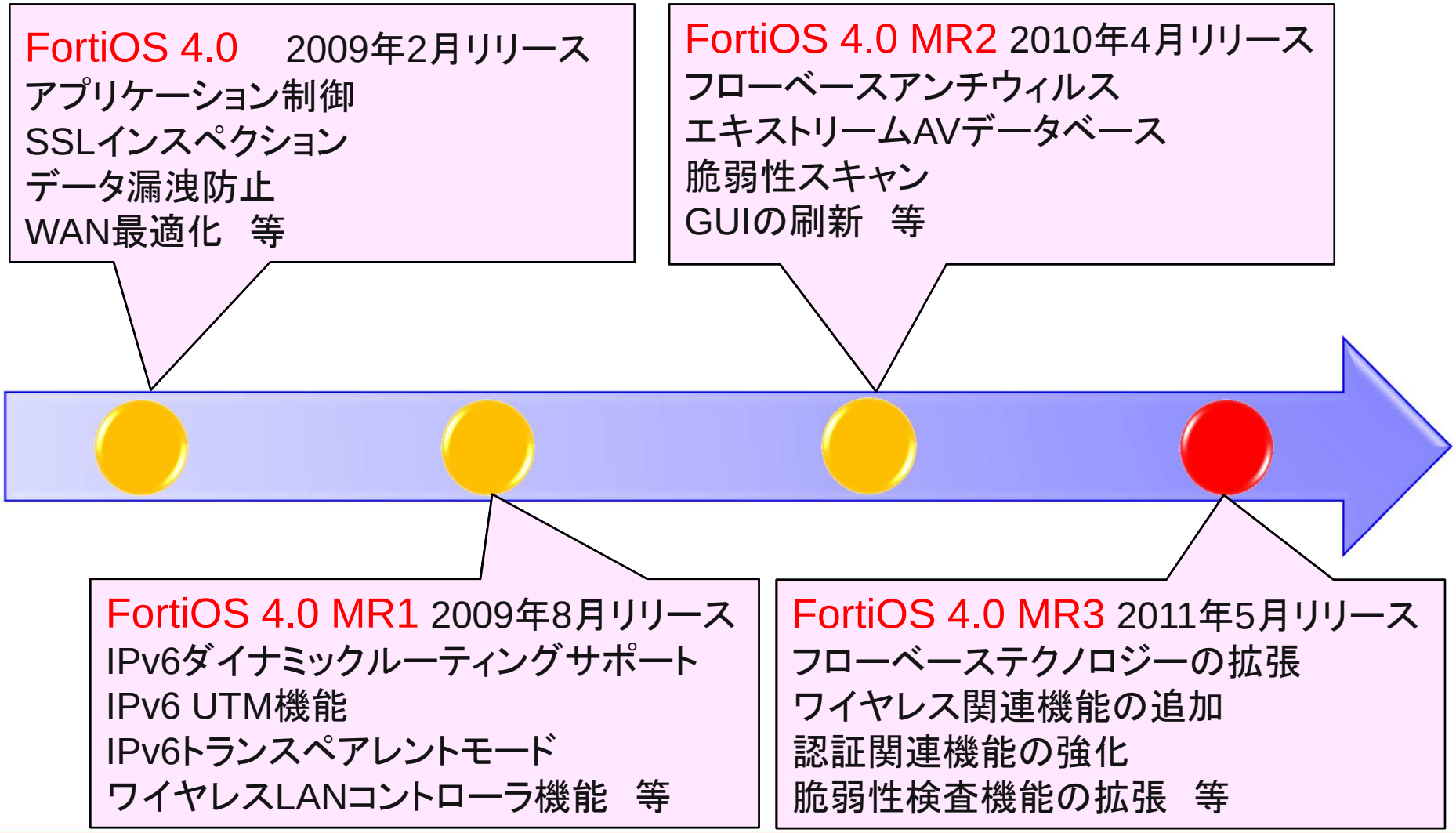
FortiOS 4.0 MR3のご紹介

フォーティネットジャパン株式会社

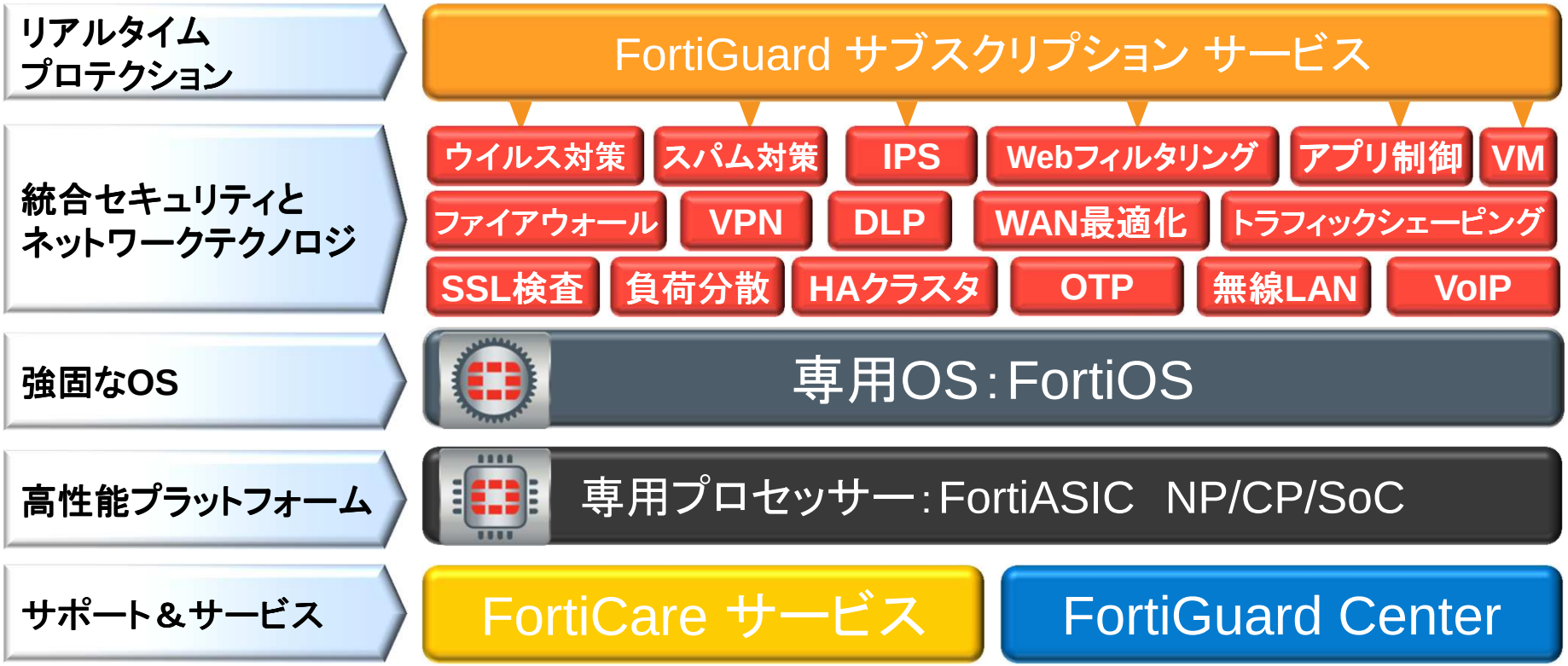
www.fortinet.co.jp

FortiOS 4.0の変遷



FortiGate 統合セキュリティプラットフォーム

- ハードウェア、ソフトウェア、サービスを全て自社開発し提供
- アプライアンスかつ、セキュリティ機能選択による容易な導入・運用
- ユーザ無制限ライセンス （アンチウイルス、アンチスパムなど）でコスト削減



FortiOS 4.0 MR3 ハイライト

ユーザーインターフェイスの充実

- ネットワークステータス（リアルタイム／ヒストリカル）の視覚化向上
- 大規模かつ複雑な案件の設定簡素化
- レポート機能の統合と簡素化

ハードウェア機能の向上

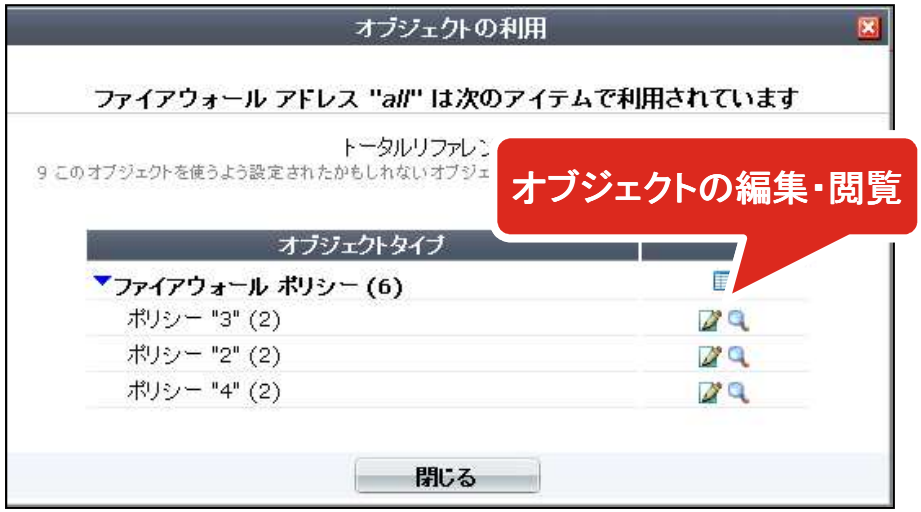
- フローベースUTM機能の向上
- ワイヤレスコントローラー機能のサポート　他

セキュリティ機能の拡張

- より強固な認証機能対応（二要素認証＆IEEE802.1x）
- SSL-VPN ポートフォワーディング方式サポート　他

オブジェクト利用状況の可視化

- 設定変更をより簡単に
  - 管理者は、利用されているオブジェクトの設定を編集するページへ、ダイレクトにアクセスする事が可能。（アイコンをクリックするだけで自動的にナビゲート）



	アドレス名	アドレス/FQDN	インタフェース	タイプ	Ref.
	all	0.0.0.0/0.0.0.0	すべて	サブネット	6
	SSLVPN_TUNNEL_ADDR1	192.168.1.[70-77]	すべて	IP範囲	2

オブジェクト利用
状況確認カウンター

セッションテーブルの機能拡張

NATされたIP
とポート番号

IPv4・IPv6 どちらの
トラフィックもサポート

Refresh　Filter Settings　　IPv4 IPv6 Both

#	Protocol	Src Address	Src Port	Src NAT IP	Src NAT Port	Dst Address	Dst Port	Policy ID	Expiry (sec)	Duration (sec)
1	udp	76.221.203.137	36592	10.85.1.2	56639	61.14.69.98	56639	12	29	153
2	udp	10.85.88.102	9664	61.14.69.99	58804	116.19.120.213	14758	15	24	156
3	udp	10.85.1.2	57151	61.14.69.98	57151	91.90.238.11	41024	22	70	110
4	udp	10.1.1.65	54372	58.185.99.220	34018	83.215.165.202	57429	13	63	117
5	udp	10.85.1.2	1093	61.14.69.98	1093	80.85.69.41	53	22	84	335
6	udp	10.85.1.2	1093	61.14.69.98	1093	80.85.69.40	53	22	84	335
7	udp	10.85.1.2	1093	61.14.69.98	1093	80.85.69.38	53	22	84	335
8	udp	10.85.1.2	1093	61.14.69.98	1093	80.85.69.37	53	22	84	335
9	udp	10.85.1.2	38207	61.14.69.98	38207	188.124.120.127	19280	22	178	2
10	udp	10.85.88.103	29773	115.42.140.114	58425	217.79.201.27	34164	16	99	80
11	udp	76.221.203.137	36592	10.85.1.2	57159	61.14.69.98	57159			
12	udp	76.221.203.137	36592	10.85.1.2	57155	61.14.69.98	57155			
13	udp	76.221.203.137	36592	10.85.1.2	57151	61.14.69.98	57151			
14	udp	10.85.1.2	56127	61.14.69.98	56127	142.68.146.71	60663			
15	tcp	10.85.88.103	50593	115.42.140.114	33749	61.59.236.224	6522	16		82
16	udp	10.85.1.2	40767	61.14.69.98	40767	202.88.81.85	59991	22	17	162
17	udp	10.85.1.2	39231	61.14.69.98	392					
18	tcp	10.85.88.102	54984	61.14.69.99	452					
19	udp	10.85.1.2	56639	61.14.69.98	566					
20	udp	10.85.88.102	9664	61.14.69.99	485					
				61.14.69.98	595					
				61.14.69.98	392					
				61.14.69.99	529					
				61.14.69.98	49471	118.168.96.84	52939	22	28	157
				61.14.69.98	55615	129.64.145.110	65319	22	74	106
	udp			61.14.69.98	53567	187.158.44.52	10357	22	69	111
27	tcp	222.253.1.	44108	10.85.1.2	42059	61.14.69.98	42059	12	116	12

改良されたセッションフィルター

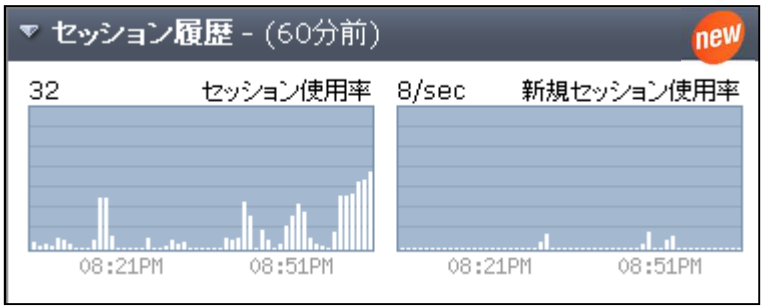
Filters:
Protocol:
Value: tcp
Add new filter ...
Clear all filters
OK　Apply　Cancel

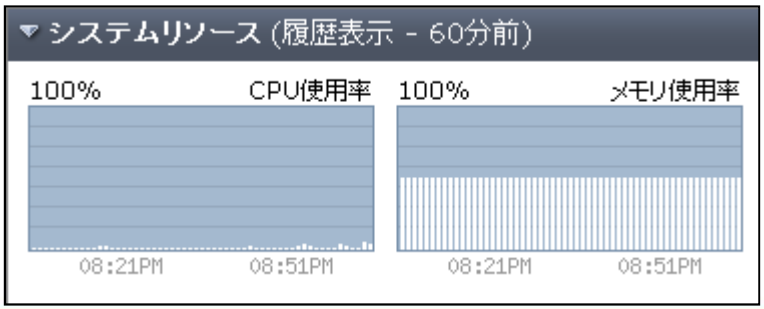
同時セッション・新規セッション
性能値（Session/Sec）

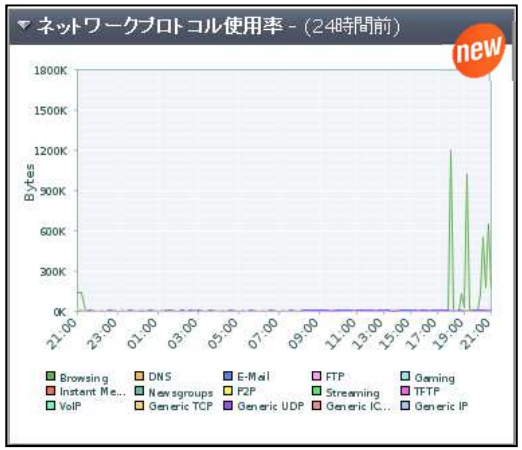
Total Concurrent Sessions: 2375 / New Sessions per Second: 17　　1 / 48　Total: 2365

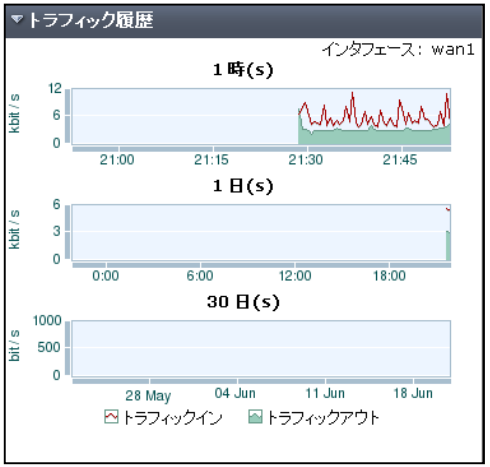
ダッシュボードのウィジェット追加

- ウィジェット追加により、ネットワークやデバイスステータスのリアルタイムでの可視化
- 毎秒の新規・同時セッション数
- ネットワークプロトコル使用率
- ストレージステータス









新しいモニターカテゴリー

システム
DHCPモニター

ルーター
ルーティングモニター

ファイアーウォール
セッションモニター
ポリシーモニター
負荷分散モニター
帯域制御モニター

UTM
AVモニター
IPSモニター
ウェブモニター
Eメールモニター
アーカイブ&DLPモニター
アプリケーションモニター
FortiGuardクォータ

VPN
IPSecモニター
SSL-VPNモニター

ユーザー
ファイアーウォールモニター
禁止ユーザーモニター

エンドポイントセキュリティ
エンドポイントモニター

Wifiコントローラー
クライアントモニター
不正アクセスポイントモニター

ログ&レポート
ログモニター

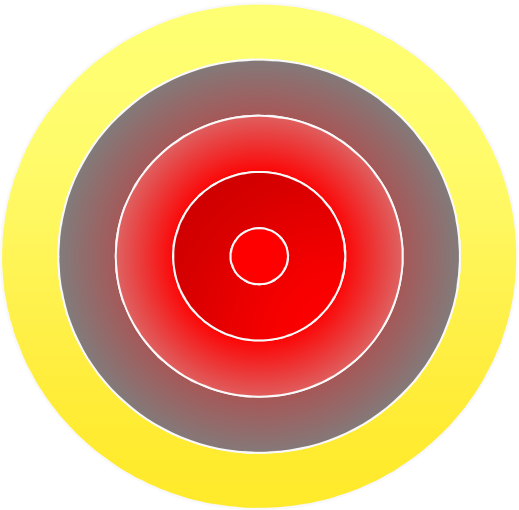
セキュアなワイヤレスLANソリューションの提供

FortiAP

セキュアワイヤレス
アクセスポイント

FortiGate

ワイヤレスコントローラー
機能を統合した複合脅威
FortiGateアプライアンス



強固に防御された
ワイヤレスネットワーク

日本国設定後の自動チャンネル選択、電波出力

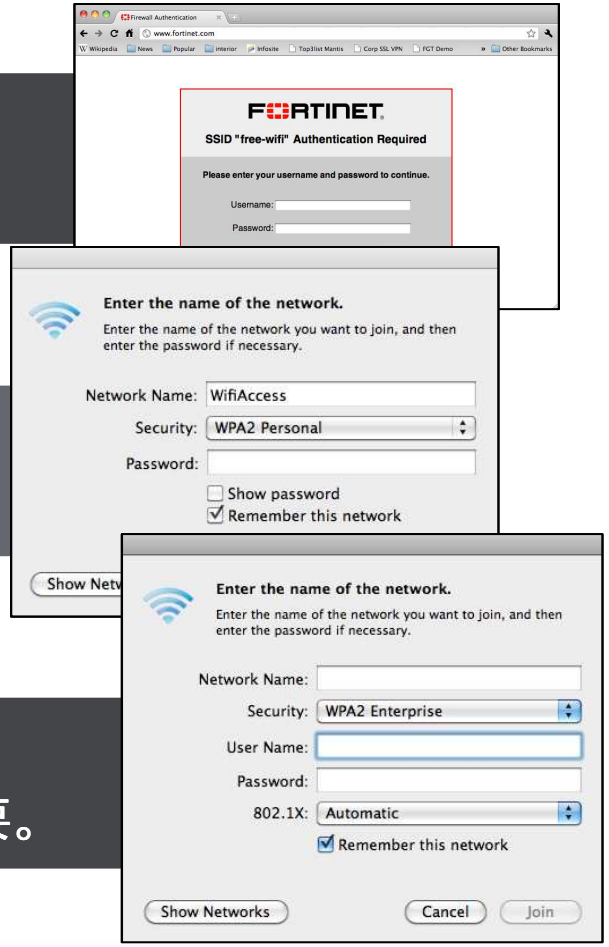
ワイヤレス認証方法

- FortiGate ワイヤレスコントローラーがサポートする認証方法

Captive Portal new
- Webブラウザでユーザー ID/パスワードの認証。

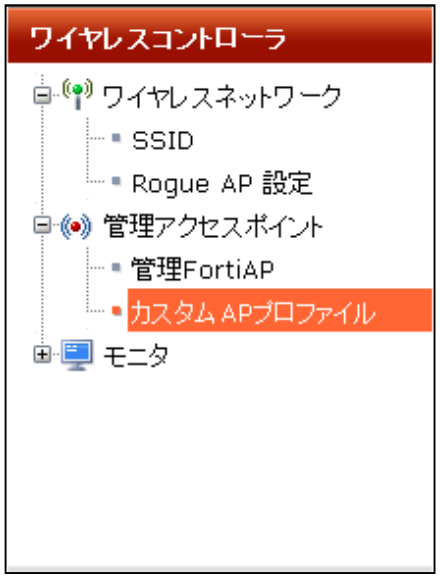
WPA Personal (PSK)
- PSK(=Pre Shared Key)を使ったワイヤレスアクセス。

WPA-Enterprise (802.1x) new
- 更に強固なセキュリティを利用。アクセス前に認証が必要。



Automatic Radio Resource Provisioning

- FortiAP自身がチャネルの選択を行うため、他アクセスポイントのチャネル相互干渉が起こりにくくなります
- DARRP機能により、各FortiAPは最適なWifiチャネルを選択します
  - ≫FortiGateワイヤレスコントローラーの負荷を軽減
  - ≫チャネルの選択は5分ごとに評価
  - ≫クライアントは自動的に新しいチャネルへ接続



不正アクセスポイント検知＆レポーティング

- 不正アクセスポイントの識別は、無線・有線上のスキャンで行います
- 未知のアクセスポイントと不正アクセスポイントは自動的に検知されます
- 不正アクセスポイントの検知時には、イベントログが生成されます

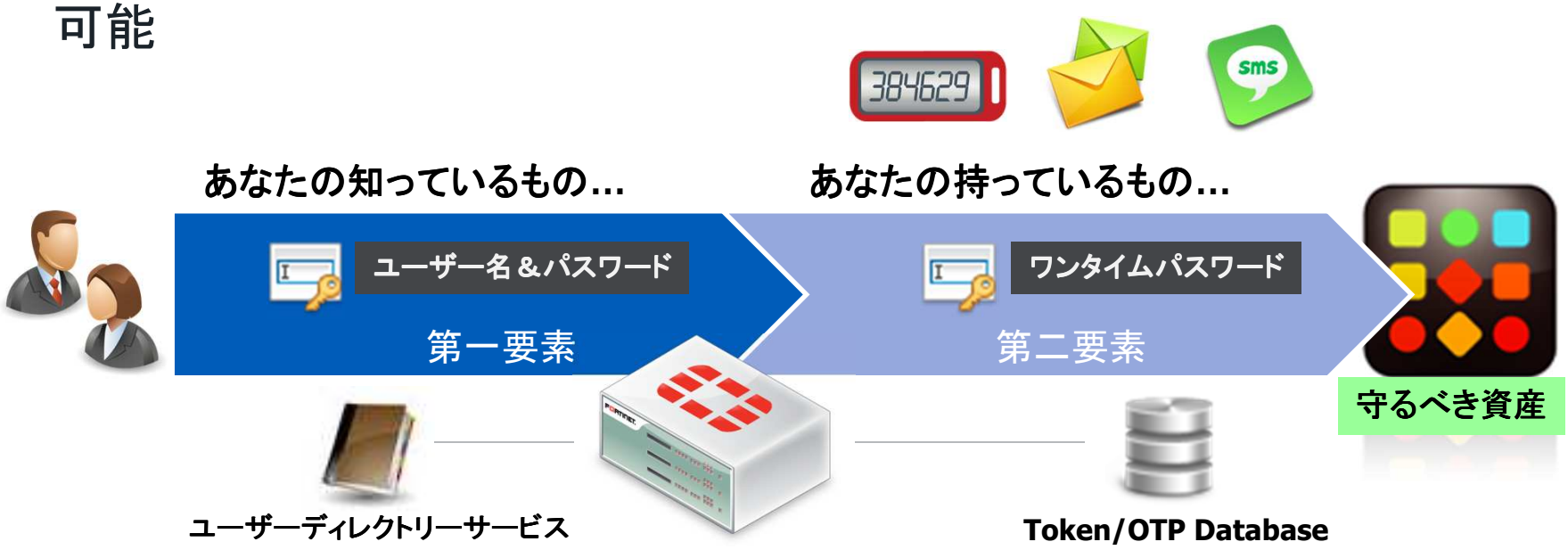
状態	オンラインの状態	SSID	セキュリティタイプ	チャネル	MACアドレス	ベンダー情報	シグナルの強度	検知済	有線上
			WPA	1	00:13:92:25:0b:8f	RuckusWire		OFFICE-AP (1)	
		2WIRE070	WEP	11	00:24:56:31:55:49	2wire		OFFICE-AP (1)	
		2WIRE402	WEP	6	00:1b:5b:31:63:f1	2wire		OFFICE-AP (1)	
		2WIRE613	WEP	6	00:1f:b3:61:91:f1	2wire		OFFICE-AP (1)	
		3AC	WPA Auto	1	00:1d:46:7e:03:00	Cisco		OFFICE-AP (1)	
		3AC BB	WPA2	1	00:1d:46:7e:03:02	Cisco		OFFICE-AP (1)	
		3ACGuest	OPEN	1	00:1d:46:7e:03:01	Cisco		OFFICE-AP (1)	
		aastar	WEP	11	00:18:39:34:34:ae	Cisco-Link		OFFICE-AP (1)	
		ACI_1	WPA2	1	00:23:69:d5:64:ed	Cisco-Link		OFFICE-AP (1)	
		AP1	OPEN	11	00:09:0f:e6:a7:a9	Fortinet		OFFICE-AP (1)	
		AP1	OPEN	6	00:09:0f:e6:a8:b9	Fortinet		OFFICE-AP (1)	
		AP2	WPA Auto	11	0a:09:0f:e6:a7:a9	Fortinet		OFFICE-AP (1)	
		AP2	WPA Auto	6	0a:09:0f:e6:a8:b9	Fortinet		OFFICE-AP (1)	
		box	WPA	11	00:90:4c:91:00:01	Epigram		OFFICE-AP (1)	
		chemie	WPA	6	00:0b:86:a8:b4:10	ArubaNetwo		OFFICE-AP (1)	
		cyndi	WPA	10	00:26:75:03:84:4c	AztechElec		OFFICE-AP (1)	
		fjsem-sin	WEP	6	00:16:b6:c5:4b:87	Cisco-Link		OFFICE-AP (1)	

不正アクセスポイントの抑制

- ワイヤレスコントローラー不正アクセスポイント抑制機能
- 不正アクセスポイントに対してリセットパケットを送り、クライアント接続の抑制を行うことで、ユーザを不正なネットワークから保護します
  - » クライアントが不正アクセスポイントに接続しない場合、ワイヤレスコントローラーはクライアントに対して認証解除（DeAuthentication）メッセージを送ります

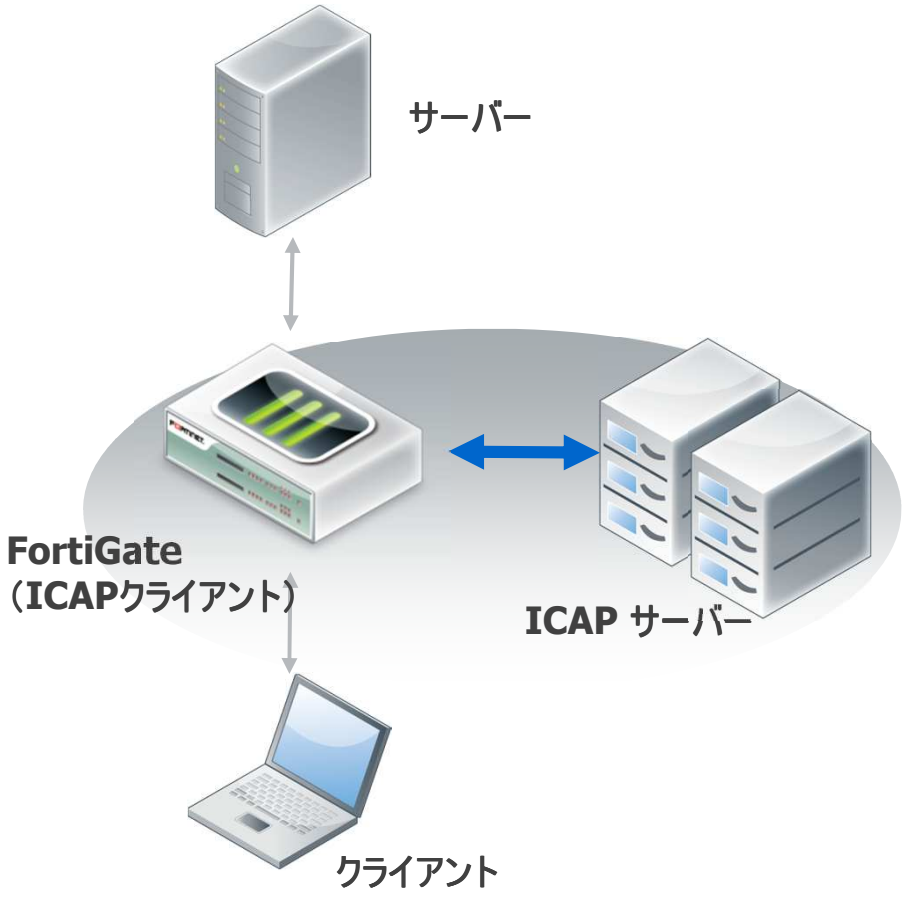
ワンタイムパスワード(OTP)／ 二要素認証

- パスワードは信頼出来ないかも知れない。
  - ≫例：盗難、ハッキング、共有
- ワンタイムパスワード(OTP)を追加する事で、より強固な認証が実現される
- FortiGate OTP サーバーは、FortiToken、VPN等のサービスとの連携が可能



ICAP サポート

- ユーザーはFortiGateがフィルタリング用途で利用出来そうなICAPサーバーのリストの編集が可能
- HTTP(S)トラフィックのオフロード
- 既存の構成にFortiGateを置き代えた後も、そのまま運用が可能
- トランスペアレントモードをサポート
- リクエストディフィケーションモード、レスポンスディフィケーションモード、どちらもサポート



ICAP=Internet Content Adaptation Protocol（RFC3507）
定義「HTTPのコンテンツに対して、何らかの処理を施すプロトコル」

SSL VPN アクセスモード

ウェブアプリケーションモード

- Javaアプレット経由でのサポート
- アプリケーションの制限あり。サポート対象は、HTTP/HTTPS, FTP, SMB/CIFS, TELNET, SSH, VNC, RDP。
- 使いやすい

トンネルモード

- SSL-VPNクライアント経由でのサポート（クライアントソフトのダウンロードが必要）
- アプリケーションの制限はなし

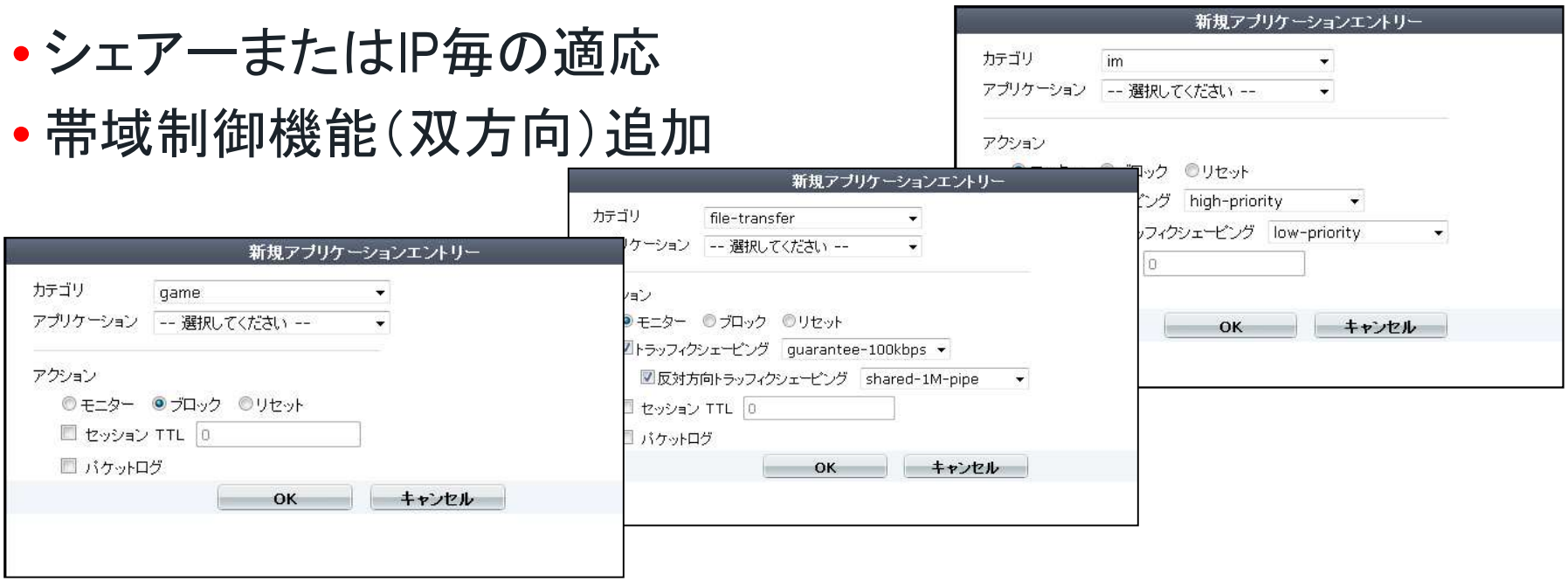
ポートフォワードモード

new

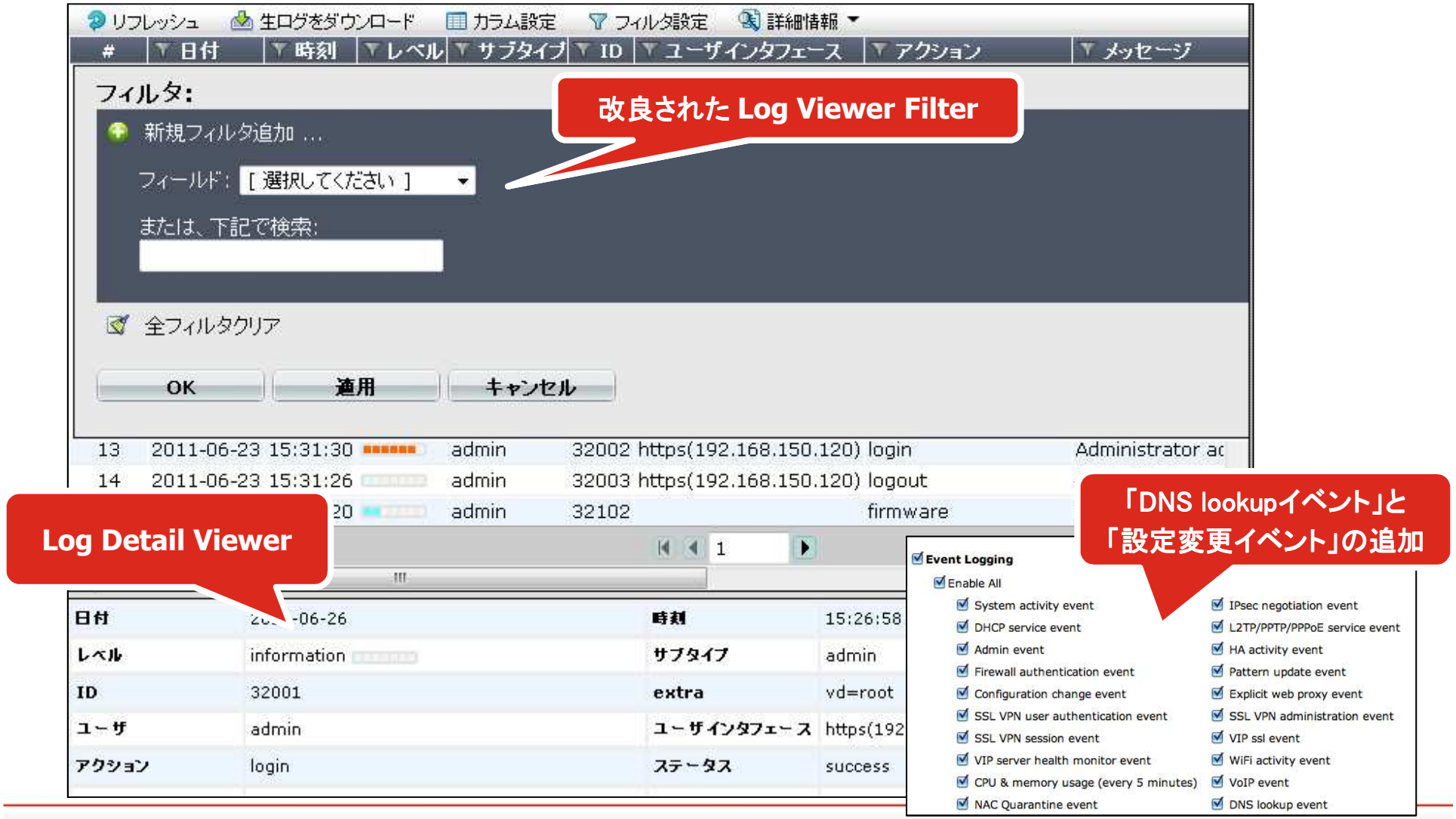
- Javaアプレット経由でのサポート
- 任意のアプリケーションの通信をHTTPSのポート番号に変換し、FWを通過させSSL-VPNを実現
- ウェブアプリケーションモードで利用出来るアプリケーションの拡張

アプリケーションコントロール

- 約1500のシグネチャーに対応
- IMの利用制御
- Facebook をアプリケーションコントロール
- アプリケーションフィルター毎のQoS制御。
- シェアーまたはIP毎の適応
- 帯域制御機能（双方向）追加

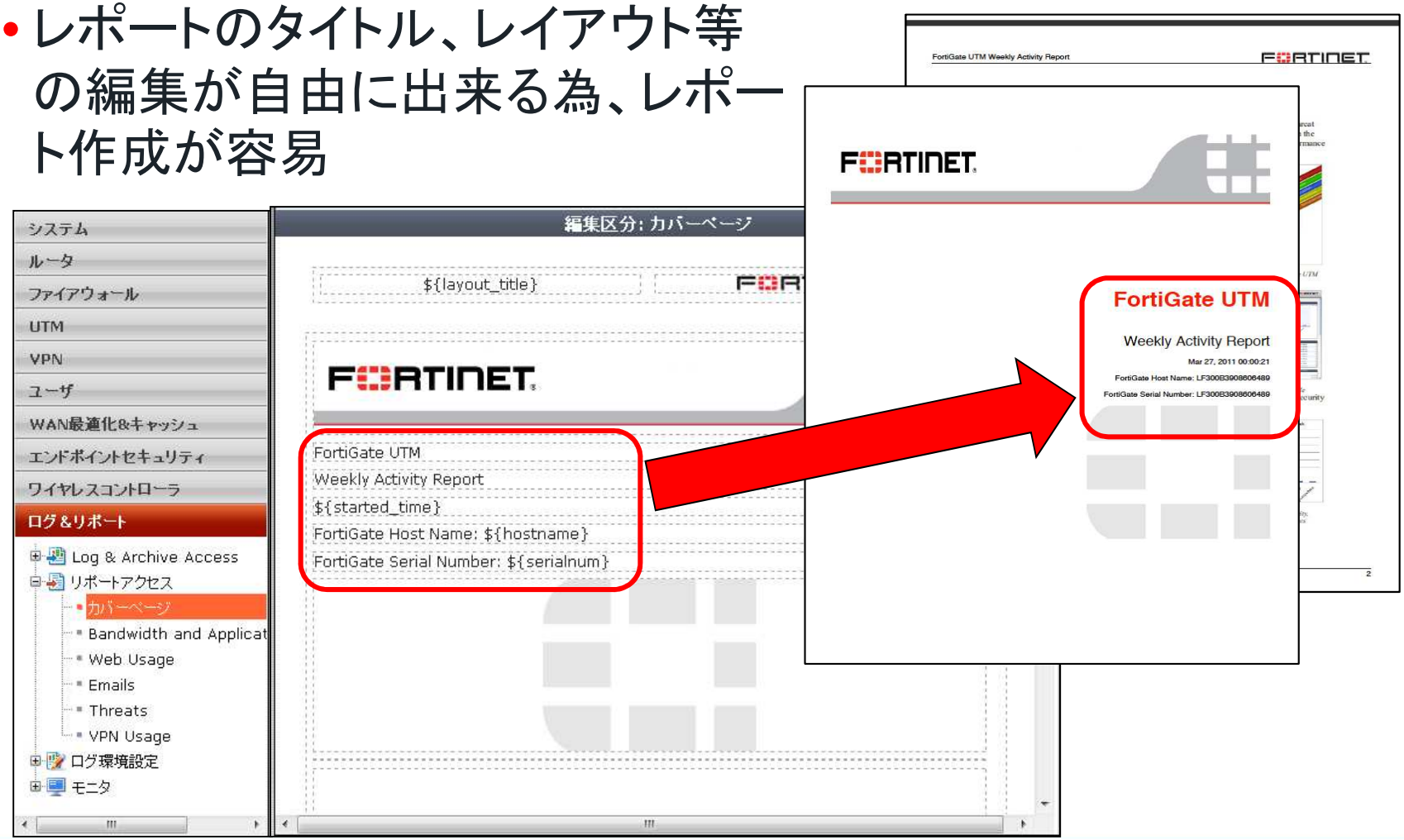


ログ機能の拡張


リフレッシュ
生ログをダウンロード
カラム設定
フィルタ設定
詳細情報
日付 時刻 レベル サブタイプ ID ユーザインタフェース アクション メッセージ
フィルタ:
新規フィルタ追加 ...
フィールド: [選択してください]
または、下記で検索:
全フィルタクリア
OK
適用
キャンセル
改良された Log Viewer Filter
13 2011-06-23 15:31:30 admin 32002 https(192.168.150.120) login Administrator ac
14 2011-06-23 15:31:26 admin 32003 https(192.168.150.120) logout
admin 32102 firmware
1
Log Detail Viewer
日付 -06-26 時刻 15:26:58
レベル information サブタイプ admin
ID 32001 extra vd=root
ユーザ admin ユーザインタフェース https(192
アクション login ステータス success
「DNS lookupイベント」と
「設定変更イベント」の追加
Event Logging
Enable All
System activity event
DHCP service event
Admin event
Firewall authentication event
Configuration change event
SSL VPN user authentication event
SSL VPN session event
VIP server health monitor event
CPU & memory usage (every 5 minutes)
NAC Quarantine event
IPsec negotiation event
L2TP/PPTP/PPPoE service event
HA activity event
Pattern update event
Explicit web proxy event
SSL VPN administration event
VIP ssl event
WiFi activity event
VoIP event
DNS lookup event

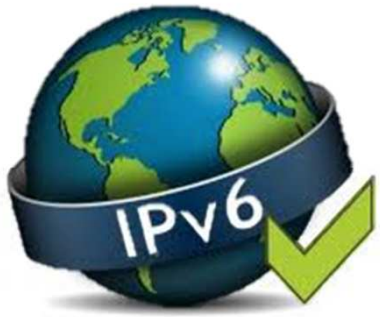
レポート機能の簡易化

- レポートのタイトル、レイアウト等の編集が自由に出来る為、レポート作成が容易



IPv6 サポート

- IPv6機能サポートの拡張



DHCP
DHCPv6

SNMP
IPv6 SNMP support

ASIC
IPv6 firewall acceleration using SP chip

Auth
IPv6 Firewall Authentication

Session
IPv6 Session table and widget

SSL-VPN
SSL-VPN Web Mode over IPv6

www.fortinet.co.jp