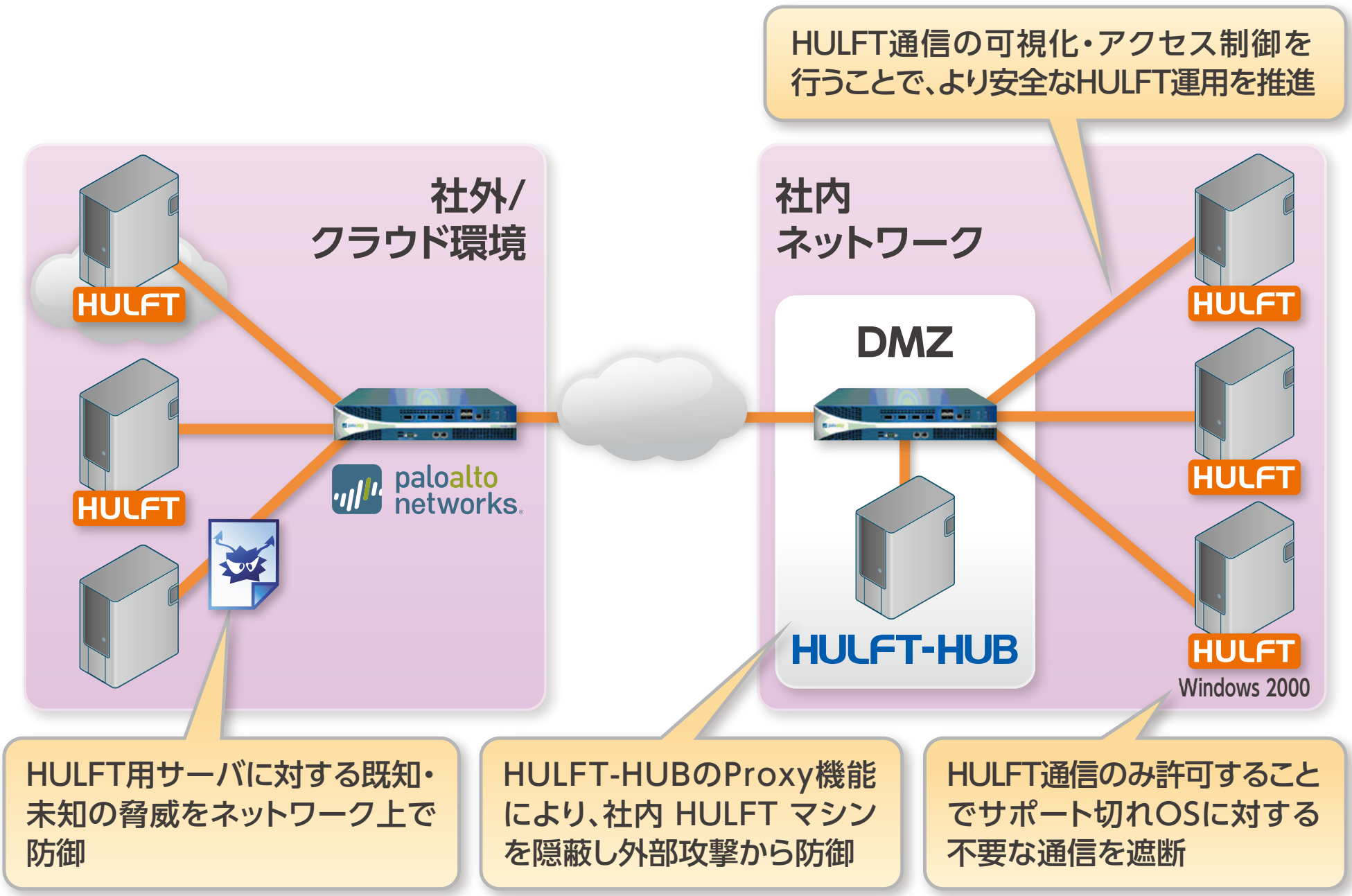
次世代ファイアウォールで HULFT通信のセキュリティ強化を実現

HULFTの企業内／企業間ファイル転送の可視化と、セキュリティ対策を
パロアルトネットワークスの次世代ファイアウォールで実現

HULFT+ 次世代ファイアウォールで実現するセキュリティ強化 4 つのポイント

- HULFT通信の可視化・アクセス制御を次世代ファイアウォールで実現
- ウイルス感染、スパイウェア感染、脆弱性攻撃、標的型攻撃など、
  HULFTサーバに対する攻撃を次世代ファイアウォールで防御
- サポート切れOS上で稼働するHULFTを継続利用したい場合に、
  次世代ファイアウォールを介して通信を限定することで安全性を強化
- 次世代ファイアウォールとHULFT-HUBのProxy機能との組合せにより
  外部からの侵入を防ぎ、より安全・安心なファイル転送基盤を実現

両製品の連携イメージ



paloalto networks

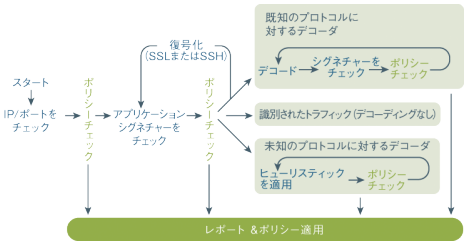
次世代ファイアウォールのテクノロジー要素

App-ID™

すべてのトラフィックの アプリケーションを自動的に識別

ファイアウォールがトラフィック ストリームを検出すると同時に複数の識別メカニズムを適用し、ネットワークを通過するアプリケーションを正確に識別します。

- ファイアウォール処理に完全統合されたアプリケーション識別エンジン
- アドレス、ポート番号、プロトコルに加えアプリケーション情報まで自動的に識別
- SSLやSSHによる暗号化通信に隠されたアプリケーションを識別可能

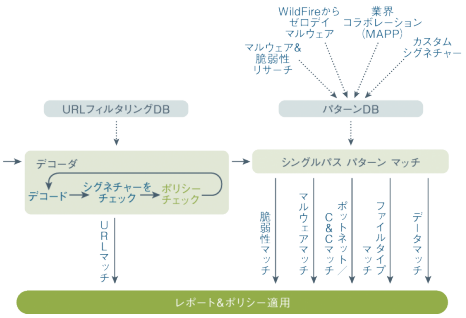


Content-ID™

さまざまな脅威を防ぐ 高速コンテンツ スキャニング

許可されたアプリケーションに対して、1つのエンジンで3つのコンテンツセキュリティ機能を提供します。

- 脅威防御：脆弱性攻撃、スパイウェア、マルウェアなどを防御
- 情報漏洩対策：ファイルタイプやデータのパターン（クレジット番号や特定文字列）によってブロック
- Webフィルタリング：URLカテゴリデータベースを基にWebアクセスを制御

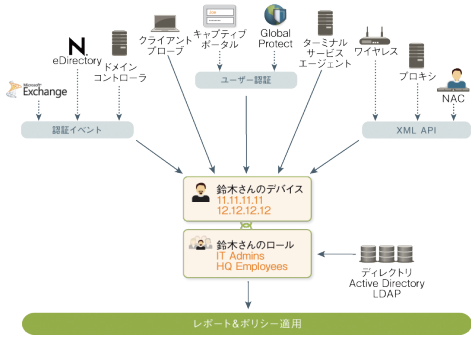


User-ID™

IPアドレスから自動的に 利用ユーザーを識別

外部のディレクトリサービスやターミナルサービスと連携して、クライアントデバイスの種類とは無関係にユーザー名やグループを識別し、ユーザー（またはグループ）にひも付いたポリシー適用を可能にします。

- Active Directory、Novell eDirectory、Microsoft Terminal Service、Citrix MetaFrame/XenApp、LDAP（Web認証＋Directory内のグループ検索）、RADIUS（Web認証のみ）に対応



ネットワークロケーション	データセンター /クラウド	エンタープライズゲートウェイ	多拠点エンタープライズ/BYOD
次世代ファイアウォール	 物理モデル: PA-200、PA-500、PA-2000 シリーズ、PA-3000 シリーズ、PA-4000シリーズ、PA-5000 シリーズ 仮想モデル: VMシリーズ		
サブスクリプションサービス	脅威防御※		
	URLフィルタリング		
	GlobalProtect™		
	WildFire™		
使用方法	次世代ファイアウォール	IDS / IPS / マルウェア対策	Webゲートウェイ / VPN
管理システム	Panorama、M-100 アプライアンス		
OS	PAN-OS™		

※アンチウイルス、アンチスパイウェア、IPS機能

paloalto networks
the enterprise security company™

パロアルトネットワークス合同会社

〒102-0094
千代田区紀尾井町4番3号 泉館紀尾井町3F
電話番号: 03-3511-4050
お問合せ: infojapan@paloaltonetworks.com