



### 製品の概要

SmartEvent Software Blade™は、実践的な脅威情報をリアルタイムで提供する、業界初にして唯一の統合イベント解析/管理ソリューションです。

## SmartEvent Software Blade

セキュリティ情報を必要なアクションに変換

### 課題

セキュリティ・ソリューションがますます包括的でプロアクティブな機能を備える一方、企業の機密情報を狙う脅威も増し、その巧妙化が進んでいます。これら脅威による不正な活動の痕跡は、ネットワーク機器やセキュリティ・デバイスが生成し続ける膨大なログの中に瞬く間に埋没してしまうため、攻撃が開始された直後に検出して抑止する機能が非常に重要です。具体的には、大量のログの中から本当の脅威に関連する情報を抽出し、ネットワークやデータが侵害される前に攻撃をプロアクティブに阻止できる優れた可視性が不可欠となります。

### 解決策

SmartEvent Software Blade™は、チェック・ポイントのセキュリティ・ゲートウェイおよびサードパーティ・デバイスで発生したセキュリティ・イベントの相関分析および管理をリアルタイムで行い、得られた情報を基に実施すべき対応策を提示します。統合されたイベント解析機能により、膨大なデバイス・ログの中から重要なセキュリティ・イベントだけを抽出し、すべてのセキュリティ・システムにわたってイベントの相関分析を行うことができます。データの集約と相関分析が自動化されているため、ログ・データ分析に必要な時間を大幅に短縮できるほか、真のセキュリティ上の脅威を顕在化させて、その問題への対応を優先的に行うことが可能です。

セキュリティ関連部署は、SmartEvent Software Bladeを利用することで、環境内のデバイスから生成される膨大なデータを綿密に調査するという工数を削減し、ビジネスに重大な損害を与える可能性のある危険な脅威への対応にリソースを集中させることができます。

### イベント情報を基に実施すべき対応策を提示



抜群の可視性



迅速な対応



緊密な統合



簡単な運用

### 製品の特徴

- ファイアウォール、IPS、DLP、エンドポイント、サードパーティ・システムにわたってイベントを相関分析
- タイムライン、チャート、マップの各ビューを使用してリアルタイムのイベント情報や傾向を把握
- セキュリティ機能をオンザフライで追加して攻撃を阻止
- 地理情報を活用する Geo-Protection 機能を使用して、悪意のある国外からの不正トラフィックを遮断
- 組み込みのチケット作成機能により、イベントへの対応状況を追跡

### 製品の利点

- 取り扱いが難しい膨大なデバイス・ログの中からセキュリティ脅威情報をすばやく特定
- リアルタイムで提示される実施すべき対応策により、ビジネス・リスクを軽減
- 重要度を認識できるため、既存リソースに優先順位をつけ、最も危険度の高い脅威に効率的に対応可能
- 法令遵守関連のレポートを統合
- 既存のセキュリティ・システムを活用し、投資効果を最大化

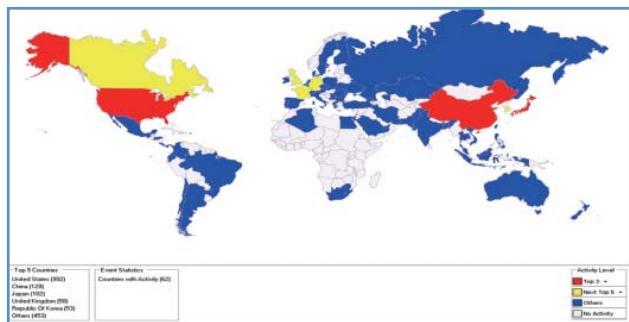


### 重要なイベントだけを監視



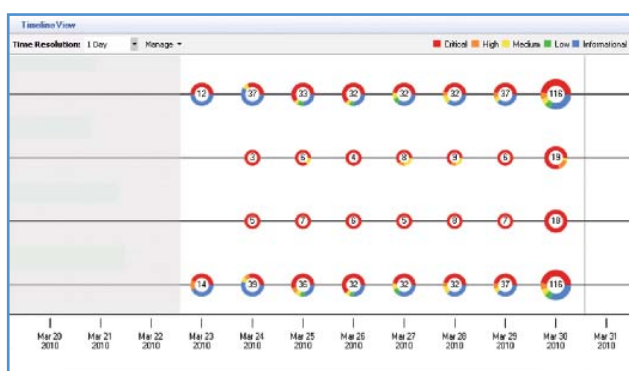
膨大な情報の中から重大なセキュリティ・イベントを素早く抽出できます。

### 脅威を発信元の国別に表示



地理情報を活用するGeo-Protection機能を使用して、悪意のある国からの不正トラフィックを遮断することができます。

### イベント分析の統合



ファイアウォール、IPS、エンドポイント、DLPなど、あらゆるセキュリティ・システムにわたってイベントを相関分析します。

### 抜群の可視性

SmartEventにはさまざまなリアルタイム・ビューが用意されており、セキュリティの状態を素早く把握して、臨機応変に対処することが可能です。タイムライン・ビューでは、攻撃の傾向や拡大状況を確認できます。チャート・ビューでは、イベントの統計を円グラフまたは棒グラフのいずれかで表示できます。またマップ・ビューでは、潜在的な脅威を国別に把握することができます。

### 迅速な対応

SmartEventには、迅速なイベント解析を可能にするさまざまなツールが用意されています。管理者は、イベントを動的にフィルタリング、検索、ソート、および分類できるため、ネットワーク・セキュリティの状態を素早く把握できます。その後、把握した内容に基づいて、イベント画面からそのまま攻撃の遮断に移ることができます。具体的には、セキュリティ機能をオンザフライで追加して攻撃を阻止したり、地理情報を活用するGeo-Protection機能を使用して、悪意のある国外からの不正トラフィックを遮断することができます。

### 単一の統合イベント管理コンソール

SmartEvent コンソールを使用して、IPSやDLP、Endpoint Securityをはじめとするすべてのチェック・ポイント製品のほか、サードパーティのセキュリティ・システムが生成するイベントを一括して相関分析および管理できます。また、共通のインターフェースを使用して監査とレポートを管理できるため、法令遵守関連のレポートも統合することができます。

### 緊密な統合

SmartEvent Software Bladeは、チェック・ポイントのセキュリティ管理機能であるSecurity Management™およびProvider-1®のログ・サーバとのインターフェースを備えているため、ログの収集や分析のために個々のデバイス・ログ・サーバを構成する必要はありません。SmartEvent サーバは、Security ManagementまたはProvider-1で定義されているすべてのオブジェクトに自動的にアクセスし、それらを使用してセキュリティ・イベント・ポリシーを定義および実施します。

### 簡単な導入

SmartEvent Software Bladeには、事前定義済みのカスタマイズ可能なセキュリティ・イベントが多数用意されており、迅速な導入が可能です。また、ウィザードを使用して独自のイベントを作成することもできるため、環境固有の要件にも簡単に対応できます。

### 拡張性に優れた分散アーキテクチャ

SmartEvent Software Bladeは拡張性のある柔軟なアーキテクチャを採用しているため、1日あたり/相関分析あたり数百万のログにも対応できます。SmartEvent Software Bladeは単一のサーバにインストールすることもできますが、分散アーキテクチャを利用して処理負荷を複数の相関分析ユニットに分散させるような柔軟な導入も可能です。




### オールインワンのイベント管理を実現する

#### Smart-1 SmartEvent アプライアンス

- あらゆるチェック・ポイント製品のイベントを管理できる短時間で導入可能なソリューション
- 拡張性に優れた Software Blade アーキテクチャをベースとするアプライアンス
- 先進のログ・ストレージと LOM (Out-of-Band Management) による高い運用性を提供



## Smart-1 SmartEvent アプライアンス

			
	Smart-1 SmartEvent 5	Smart-1 SmartEvent 25	Smart-1 SmartEvent 50
インストール済みSoftware Blade	SmartEvent、SmartReporter、ログ&ステータス		
ディスク容量	0.5TB x 1	0.5TB x 4 (RAID 10)	1TB x 4 (RAID 10)
ファイバ・チャンネルSANカード	-	-	オプション
LOM (Out-of-Band Management)	-	内蔵	内蔵
管理可能なゲートウェイ数 (推奨)	5	25	50
管理可能なゲートウェイ数 (最大)	25	50	150
ロギング容量 (推奨)	2GB/日	10GB/日	25GB/日

## SmartEvent Software Blade の仕様

機能	説明
データ・ソース	
チェック・ポイント製品	事前定義されたルールに基づくイベントの相関分析が可能
サードパーティのセキュリティ製品	複数のサードパーティ・ログ形式をサポート
グラフィカルなログ構文解析ツール	あらゆるサードパーティ・ログ・ファイルを手動で解析および調製可能
複数のログ収集手法	エージェント・ベースまたはエージェントレスのログ収集に対応
イベントの把握	
タイムライン・ビュー	リアルタイムのイベント情報、傾向、および異常をグラフィカルに表示
チャート・ビュー	イベントの統計を棒グラフまたは円グラフで表示
マップ・ビュー	イベントに関連するトラフィックの発信元/送信先IPを地図上に表示
イベントのクイック・ビュー	タイプ、関連トラフィックの発信元/送信先、ユーザ、国別にイベントを素早く分類
イベント解析	
事前定義のイベント相関分析ルール	チェック・ポイントのベスト・プラクティスに基づく、業界で一般的なセキュリティ問題に対応した事前定義のイベント相関分析ルール
セキュリティ・イベントのカスタマイズ	独自のイベント相関分析ルールを作成してあらゆるセキュリティ・イベントを監視
フォレンジック調査	タイムライン、チャート、マップの各ビューでイベントをダブルクリックし、パケット・レベルまで素早くドリルダウン
イベントの分類と検索	使いやすい検索およびデータ分類機能を使用してイベントを解析
アイデンティティの記録	Active Directoryの情報に基づき、IPアドレスをユーザ名にマッピング
ClientInfoアプリケーション	クライアント・デバイスを右クリックして重要な情報(プロセス、ホットフィックス、脆弱性)にアクセス
インテリジェントな学習モード	アクティビティを一定期間調査し通常の傾向を把握可能
脆弱性評価	セキュリティ・イベント適用の評価機能を内蔵
セキュリティ・イベントへの対応策	
イベント・チケット	チケット・ワークフローにより、管理者にイベントを割り当て
グローバルな例外とイベント固有の例外	製品、送信元、送信先、サービスごとにアラートをカスタマイズしてイベントを除外
改善オプション	イベントの解析結果に基づき、自動または手動で改善処理を適用してセキュリティ・ポリシーを変更
その他	
拡張性に優れた分散アーキテクチャ	ログ・サーバ、イベント相関分析サーバ、イベント・サーバを別々のシステムに導入可能



---

## 製品に関するお問い合わせ

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社  
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F  
<http://www.checkpoint.co.jp/> E-mail : [info\\_jp@checkpoint.com](mailto:info_jp@checkpoint.com) Tel : 03(5367)2500

---

© 2010 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express Cl, the Check Point のロゴ, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Full Disk Encryption, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity の logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, Secure-Knowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, Smart-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity の ロゴ, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express Cl, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, VSX-1, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labs のロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company. その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の特許 No.5,606,668、5,835,726、5,987,611、6,496,935、6,873,988、6,850,943、および 7,165,076 により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。