

# Integrity

## トータル・アクセス・プロテクション

### 製品の特徴

- ・プロアクティブなエンドポイント・セキュリティ
- ・確実なアクセス・ポリシーの実施
- ・簡単で柔軟な集中管理
- ・トータル・アクセス・プロテクション

### 製品の利点

- ・内部・外部における未知の脅威からの防御
- ・LANに接続されるPCの安全性を確保
- ・導入と管理が簡単
- ・あらゆるネットワーク環境での保護を実現

### 課題

企業ネットワークにつながるすべてのPCは、増殖が急速なワーム、侵入型の攻撃、トロイの木馬、スパイウェアなどによる攻撃の対象となります。もはやリアクティブ(事後対処型)、即ちアンチウイルスや侵入検知などのシグニチャに依存する従来の技術では、これら脅威の最新亜種に対して確実な防御を実現することはできません。

### 解決策

Integrity™は、ネットワークの各エンドポイントにおけるプロアクティブ(事前予防型)な防御とポリシーの集中管理および実施とを組み合わせ、悪意のあるコードによる企業ネットワークへの侵入や攻撃からの防御を実現します。トータル・アクセス・プロテクションのための最高のエンドポイント・セキュリティを簡単に構築・管理・実施し、ITやエンドユーザの生産性を犠牲にすることなく、企業データやクリティカルなシステムの機密性、整合性、可用性を回復し、ビジネスの成長と収益の達成を支えます。

### プロアクティブなエンドポイント・セキュリティ

企業におけるデスクトップのデータ・セキュリティのために毎年多額な経費が費やされてきました。Integrityにより、様々な攻撃の対象となることを防ぎます。

### プロアクティブな防御

Integrityのステートフル・ファイアウォールは、PCをハッカーから完全に見えなくするステルス技術により、すべての未承認インバウンドトラフィックをブロックします。ポリシー機能により、セキュリティ・ポリシーで明示していない限り、すべてのネットワーク・トラフィックとアプリケーションを信頼できないものとして処理し優れた防御を可能とします。管理者は短時間で基本となるセキュリティ・ポリシーを定義してPCに配備することができます。簡単な設定のみで直ちに企業のエンドポイントのファイアウォール保護を実現します。

Integrityはさらに、各企業独自の必要性やその変化に対応し、ポリシーの微調整にも優れた制御能力を発揮します。管理者はPCが通信を行う方法、時間、およびリソースを、3つのネットワーク・ゾーンにより管理することができます。ブロック・ゾーンでは、指定したネットワーク・アドレス以外とのすべての通信を停止します。トラスト・ゾーンでは、既知の信頼に値するトラフィック宛先を含みます。インターネット・ゾーンでは、トラスト・ゾーンとブロック・ゾーンのどちらでもない境界ファイアウォールの内外にあるすべてのトラフィックを含みます。また、従来のファイアウォール・ルールを使用し、企業ネットワーク内にカスタム・ゾーンを作成して、それぞれに異なるレベルのセキュリティを適用することもできます。このネットワーク・セグメンテーションは、ワームが発生する危険性をはらみ最低の権限のみを与えられたアプリケーションのネットワーク・リソースへのアクセスを可能にします。

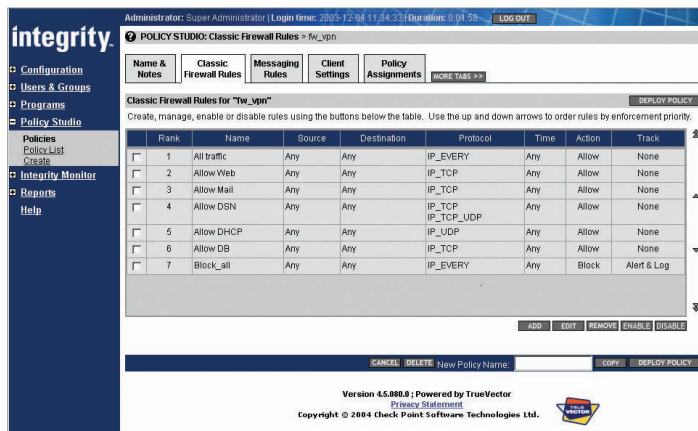
### アプリケーション権限の制御

Integrityは、企業の機密データが悪意のあるコードにより破壊されるのを防ぎます。管理者はネットワーク・アクセスを許可/禁止するPCアプリケーションを指定し、未認識プログラムの処理方法を指定します。これによりIntegrityのプログラム監視機能が、ネットワーク・アクセスを試みるPCアプリケーションのリストを自動的に作成するため、潜在的なネットワーク脆弱性をすばやく効率的に確認して防御することができます。

アプリケーション制御は、ファイアウォール・ルールまたはアプリケーション権限ルールを実施することで実現可能です。Integrityのファイアウォール・ルールにより、管理者はトラスト・ゾーンとインターネット・ゾーンに別々のアプリケーション権限を適用することができます。例えば、トラスト・ゾーンではあらゆるアプリケーションからの接続を許可し、インターネット・ゾーンでは禁止するよう設定できます。



Intelligent Security



Integrityは、従来のファイアウォール・ルールを使用したセキュリティ・ポリシーの微調整などの柔軟な管理を実現します。

## 電子メールとインスタント・メッセージの防御

Integrityは、ハッカーの攻撃やマルウェアに対して特に脆弱な電子メールとインスタント・メッセージ(IM)両方の、脆弱性に対する自動防御機能を備えています。IntegrityのMailSafe機能は、POPサーバまたはIMAPサーバから取得する個人の電子メール・メッセージを監視し、企業のアンチウィルス・メカニズムでは防ぎきれない45種類以上の危険性のある添付を検査することができます。これにより、アンチウィルスがアップデートされるより早く電子メールからのウィルスをブロックし、アドレス帳の奪取により自己繁殖するのを未然に防ぎます。

IMは、現在もっとも人気の高いインターネット通信手段です。IntegrityのオプションであるIMセキュリティモジュールは、従業員がネイティブまたはサードパーティ・クライアントを使用してIMサービスにアクセスした場合に、メッセージの暗号化、コンテンツ・フィルタリングなどの制御を提供し、IM通信の利便性と管理者のセキュリティ・リスク軽減を同時にサポートします。

## 確実なアクセス・ポリシーの実施

Integrityは、ネットワーク・アクセスの条件としてすべてのネットワークPCに包括的なセキュリティ・ポリシーを実施することにより、セキュリティとビジネスの継続を損なう危険性のある攻撃に対する効果的な防御を実現します。PCがネットワークへのアクセス権を得る前に、アンチウィルスを実行していること、重要なパッチおよびサービス・パックをインストールしていること、ブラウザやVPNクライアントなどのアプリケーションが最新バージョンであること、その他の信頼性に関する条件が整っていることなどを検証します。

ネットワーク・アクセスを制御するには、協調施行(Cooperative Enforcement)技術により、Integrityと広範なVPN、スイッチ、無線アクセス・ポイントなどを統合して、ネットワーク・アクセスを制御します。さらに柔軟性を高めるため、業界標準の802.1x EAP (Extensible Authentication Protocol) をサポートしています。これにより、どのようなネットワーク機器を使用する場合も企業全体で同一のポリシーを実施することが可能です。

## クライアント・ソフトウェアを使用しないポリシーの実施

企業ネットワークにアクセスを許すことで発生するリスクは、最近まで軽減が困難でした。

Integrity Clientless Securityは、基本となるセキュリティ要件を実施し、この問題を解決し企業におけるWebベースのゲートウェイおよびアプリケーションにアクセスしようとするゲストと従業員の両方のエンドポイントで、セッションの機密性を確保し、スパイウェアを無効にしています。これにより、IT管理者はIntegrityのクライアント・ベースのソリューションで実施された同じネットワーク・アクセス・ルールを、クライアント・ソフトウェアをインストールすることなく実施できるようになりました。Integrityのクライアント・オプションおよびクライアントレス・オプションにより、企業のすべてのネットワークにおいて、エンドポイントがアクセス要件を満たしていることを

確実にし、トータル・アクセス・プロテクションを実現します。

## 簡単に柔軟な管理

Integrityは、ビジネスが円滑、安全かつ効率的に継続できるよう、セキュリティ・ポリシーの配備と管理に必要な時間と作業を最小限に抑えます。

## 迅速な設定と配備

Integrityは、エンドユーザの作業を軽減することが可能です。管理者はダウンロード可能な設定済みソフトウェア・パッケージを作成し、すばやく簡単に新しいアップグレード済みのIntegrityクライアント・ソフトウェアをインストールできます。インストール後、Integrityクライアントは管理サーバに接続して基本となるポリシーを受け取ります。管理者は、定義済みの便利なポリシー・テンプレートを使用してすばやく簡単に、初期セキュリティ・ポリシーを設定することができます。さらに柔軟性の高いIntegrity Flexクライアント・オプションにより、ユーザは企業ネットワークに接続中は企業のポリシーに従い、接続していないときは独自のセキュリティ設定を制御することができます。

全てのIntegrityクライアントは、トータル・クライアント・ロックダウン (Total Client Lockdown) 機能を備えています。この機能により、ローカル管理権限を持つエンドユーザが、PCのセキュリティとポリシーの実施を、変更したり無効とすることを制限します。

## 簡単なポリシー管理

Integrityにより、管理者は再利用可能なポリシー要素を1回作成し、複数のポリシーに割り当てることができます。ポリシー要素を変更すると、関連するすべてのポリシーが自動更新され、関連するクライアントに瞬時に送信されます。

管理者は、別のポリシーを定義して、エンドポイントがネットワーク間、ロケーション間、ユーザ間で移動する際に自動的に適用するよう設定することもできます。ユーザのIP接続アドレス、ユーザ・グループやロール、ゲートウェイの種類(VPN、スイッチ、無線アクセス・ポイントなど)、またはこれらの条件の組み合わせに基づいて、ポリシーを動的に割り当てることが可能です。すべてのエンドポイントの防御を確

実にするため、未認識ユーザには基本的なデフォルト・ポリシーを割り当てます。Integrityでは、いくつかの管理レベルを用意しています。例えば、未認識ポリシーの決定をせずにエンドポイントの問題をトラブルシューティングするための、読み取り専用ロールなどがあります。さらにサーバ・フェイルオーバーのサポートにより、ビジネス継続のためのハイ・アベイラビリティ機能も実現します。

### 動的な監視とレポート

Integrityのレポート機能は、エンドポイントのイベントに対する広範で詳細な分析を提供します。管理者は、フィルタリング可能な様々なアクティビティ・レポートを閲覧できます。これにより、アプリケーションの使用状況、セキュリティ警告やポリシー違反の多いユーザなどの情報をグラフや詳細レポートで確認することができます。

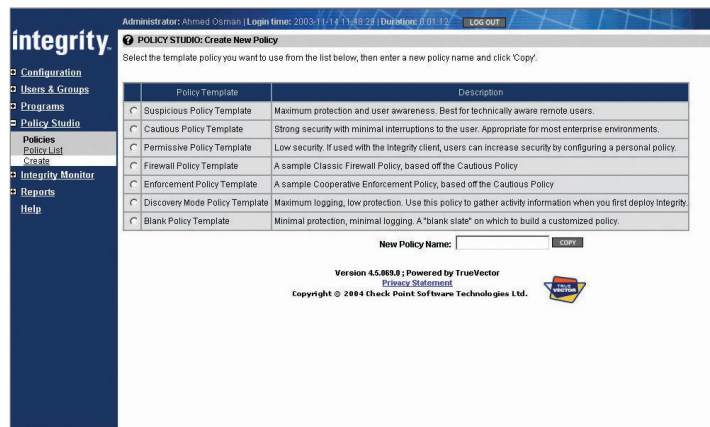
### 集中管理と個別管理

Integrityクライアントには、企業のための多様で柔軟なエンドポイントのセキュリティ管理オプションがあります。相互に互換性があるため、同一企業内で各ユーザのニーズに合わせて使い分け、共存することが可能です。

**Integrity Agent**：エンドユーザにとって完全に透過的なエンドポイント・セキュリティ・ポリシーを最大規模で集中IT管理することが可能です。技術的でないユーザが多い企業で一貫したセキュリティ・ポリシーを適用したい場合に最適です。Integrity AgentはIntegrity Server管理コンソールから集中管理できます。管理者は、Integrity Agentポリシーの実施を、PCが企業ネットワークに接続されている場合のみ、または常時のいずれかに設定できます。

**Integrity Flex**：Integrity Agentが持つすべての機能のほか、エンドユーザが企業ネットワークに接続していないときに独自にセキュリティ・ポリシーを管理できる機能を提供します。ユーザが企業に接続しているときは、Integrity Agentと同様、管理者が定義したポリシーが透過的に実施されます。企業ネットワークに接続していない社外にいる従業員が、客先のLANまたは自宅などのネットワークへのアクセスが必要となった場合は、Integrityの直感的なGUIを使用して、PCのセキュリティを維持しながら他のネットワークを使用するために必要な調整を簡単に行うことができます。

**Integrity Desktop**：集中、スタンドアロン・ソリューションです。エンドユーザが自身のPCセキュリティ環境を設定することが可能です。技術レベルが高く、自身のセキュリティ・ポリシーを決定する能力を持つエンドユーザに最適です。また、IT部門のリソースが不足していたり、エンドポイントの集中管理が困難な場合もこのソリューションが適しています。一貫した基本となるセキュリティをエンドユーザが変更できないように、Integrity Desktopおよびセキュリティ・ポリシーをロック・ダウンすることができます。



定義済みポリシー・テンプレートにより、数回のクリックで直ちに企業全体のエンドポイントの防御を実現します。

機能	Integrity Agent	Integrity Flex	Integrity Desktop
エンドポイントのプロアクティブなセキュリティ。ステルス、ステートフル・ファイアウォール、高度なアプリケーション制御、オプションのインスタント・メッセージ・セキュリティを含む。	✓	✓	✓
Integrityクライアントの非実行時リモート・アクセス拒否	✓	✓	✓
最新のアンチウィルス、パッチ、その他のポリシー要件のLANおよびリモートでの実施	✓	✓	
企業ポリシーのGUIによる集中管理および監視	✓	✓	
拡張性、可用性の高い管理サーバ	✓	✓	
コマンド・ライン設定ツール			✓
エンドユーザのGUIヘルプ・リソース		✓	✓
ネットワーク接続時、非接続時のセキュリティ・ポリシー		✓	

## TCOの削減

Integrityは広範なネットワーク・ハードウェアとソフトウェアとの統合により、既に導入済みの技術と合わせ、投資回収率を高めます。さらに、優れたゲートウェイとの統合性に加え、ディレクトリからインポートされたグループ構造や様々な認証システムと自動的に同期をとることで、スタッフがグループ管理に費やす時間を削減することができます。また、一般的なデータベース管理システムとの統合も可能です。

Integrityは、先進のアンチウイルス製品とも親和性を持ち、常に最新のポリシー実施ルールを実行します。リファレンスPCからアップデート情報を収集し、直ちにエンドユーザに対してインストールを要求する新しいポリシーを配備します。これにより、手作業でポリシー・データを収集してアップデートする管理作業に費やす時間を削減します。

各Integrity Serverは5,000までの同時接続ユーザをサポートしています。より小規模な実装には、Integrity Server Workgroup Editionが最適です。組み込みデータベース内で1,000人までのユーザをサポートし、サードパーティ・データベースや統合コストは不要のため、よりシンプルで高速、低コストの配備を可能にします。

### INTEGRITY SERVER

#### ハードウェア要件

- Intel Pentium III (600 MHz) 以上のプロセッサ
- 256色以上のビデオアダプタ

#### オペレーティングシステム

- Windows 2000 Server (SP4) および Advanced Server (SP4)
- Windows Server 2003

#### ブラウザ

- Internet Explorer 6 以上
- Netscape Navigator 7 以上

#### データベース管理システム

- Oracle 9iR2、Oracle Thin JDBC driver version 1.2
- Microsoft SQL Server 2000 (SP3)、Microsoft SQL Server 2000 Driver for JDBC SP1

### INTEGRITY AGENT と INTEGRITY FLEX

#### ハードウェア要件

Intel Pentium III (450 MHz) 以上のプロセッサ

#### オペレーティングシステム

以下のMicrosoft Windowsプラットフォーム

- XP Professional, 2000 Professional SP4
- NT 4.0 Workstation SP6a, 98 SE, 95 OSR2\*

\*Internet Explorer 5 かそれ以降のバージョンが必要

Check Point



We Secure the Internet.

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@checkpoint.co.jp Tel: 03 (5367) 2500

※記載された製品仕様は予告無く変更される場合があります。

©2005 Check Point Software Technologies Ltd. All rights reserved.

Check Point, Application Intelligence, Check Point Express, Check Pointのロゴ, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMSecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecurRemote, SecurServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, TrueVector, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecurRemote, VPN-1 SecureServer, VPN-1 VSX, Web Intelligence, ZoneAlarm, Zone Alarm Pro, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd. およびその関連会社の商標、サービス・マーク又は登録商標です。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。本書に記載された製品は米国の特許No.5,606,668、5,835,726および6,496,935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。