



Check Point®

SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



White Paper

# Total Access Protection

ネットワーク保護のためのより効果的なアプローチ



Intelligent Security

チェック・ポイントは、境界、内部、WEBなど、ネットワークのあらゆる局面に対するセキュリティ・ソリューションを提供します。これにより、企業はネットワークや、ネットワーク・リソース等を安全に保護しながら、高い接続性を実現するリモート・アクセスを提供し、簡単に管理することができます。

# Contents

本書の内容

---

概要	3
セキュリティ・レベルの低下	3
より効果的なアプローチ	4
ネットワーク保護のためのより効果的なアプローチ	5
総合的なアクセス保護を実現するTotal Access Protection	6
他社のアクセス制御技術	6
ネットワーク・アクセス・ポリシー実施の将来	7
まとめ	7

## 概要

ネットワーク、およびネットワークに接続されるエンドポイントPCを保護することは、近年ますます困難になっています。エンドポイント脆弱性の数やエンドポイントに対する攻撃が急増したことに加え、エンドポイントのアクセス方法が多様化している状況に、従来の防御方法では対応できなくなっているためです。現在では、エンドポイントを経由した攻撃が企業に甚大な被害をもたらしています。さらに、今やネットワークのセキュリティと有効性に対する主要な脅威となったスパイウェアが、この状況を深刻化させています。こうしたセキュリティ・レベルの低下は、企業で利用されるほぼすべてのPCにアンチウイルス・ソフトウェアが導入されているにもかかわらず起きています。

このような問題を解決するのが、チェック・ポイントのTotal Access Protection (総合的なアクセス保護:TAP) 戦略です。Total Access Protectionとは、すべてのPCに対し、ネットワークへの接続前に確実にセキュリティを適用することによって、企業ネットワークを保護するという考え方です。Total Access Protection戦略は、次の3つの基本原則に基づいています。

- ・ ネットワークに接続するすべてのPCは、企業ネットワーク・アクセスのためのセキュリティ・ポリシー要件 (アンチウイルス/アンチスパイウェア・ソフトウェアの定義ファイルやパーソナル・ファイアウォールのルールが最新かどうか、最新のパッチが適用されているかどうかなど) を順守していなければならない。
- ・ TAPは、シングルベンダー環境でもマルチベンダー環境でも実現できなければならない (場合によっては、ネットワーク機器やオペレーティング・システムのアップグレードを必要)。
- ・ 最良のエンドポイント・セキュリティと、広範なネットワーク・ゲートウェイ製品を統合可能にすることによって、最も柔軟性が高く、最もコスト・パフォーマンスの高いアクセス・コントロール・ソリューションが実現される。

チェック・ポイントのエンドポイント・セキュリティ製品、Check Point Integrity™は、このTAPを実現するソリューションです。Integrityは、多くのアンチウイルス製品が提供する、シグネチャベースの事後対応的なセキュリティ対策をすり抜ける攻撃も事前予防的にブロックします。さらに、エンドポイントの安全性やセキュリティ・ポリシー違反をチェックして、ネットワーク・アクセスに必要なセキュリティ基準を満たしていない場合、Integrityは、チェック・ポイントのセキュリティ・ゲートウェイ製品やさまざまなベンダーのVPN機器、スイッチ、ルータ、無線アクセス・ポイントと連携して、ネットワーク接続を行う際のセキュリティ・ポリシーを満たさないエンドポイントをすべて隔離します。また、こうしたセキュリティ・ポリシー違反により隔離されてしまったクライアント (エンドポイント) に対し、セキュリティ・パッチなどを適用させセキュリティ・ポリシーを満たすよう対策を行なうことを手助けし、ネットワークへ接続させるための仕組みも備えています。Integrityは、企業ネットワークに接続するあらゆるタイプのPC (社員用PC/ゲスト用PC、リモートPC/内部PC、有線LAN/無線LAN接続) を保護することにより、Total Access Protectionを実現します。エンドポイントおよびネットワークのセキュリティを維持するためのIntegrityのアプローチは、一般的に検疫と呼ばれるソリューションのように、単純にネットワーク・アクセスのコントロールを行なうだけで、セキュリティ・チェックを一切行なわない従来型検疫ソリューションの手法の弱点を補いながら、TCOも低く抑えます。

## セキュリティ・レベルの低下

最近発生した情報セキュリティに関連する被害のうち、損害の大きかった事例の多くには、パーソナル・コンピュータ、すなわちネットワークの「エンドポイント」が関わっています。一部の組織では、エンドポイントを経由した攻撃による被害が、数値上でも感覚的にも最大の財務コストとなっているほどです。BagleやBlaster、MyDoom、Nachi、Netsky、Sasserなどのワームが出現したとき、ネットワークがダウンし、重要な業務が行えなくなり、ビジネスが継続できなくなったのは、「これらのワームが極めて短時間のうちにLAN上のすべてのエンドポイントに広まったことが原因だ」と、複数のニュース記事が指摘しています。これらのワームは、電子メールの添付ファイルで広まることが多いウイルスとは異なり、多くの場合ユーザの介在を必要とせずに自らを複製し、自動的にネットワーク上の脆弱なノードに拡散していきます。

また、スパイウェアもネットワークにとって大きな問題となっています。スパイウェアは、企業のセキュリティ・インフラストラクチャに大きな穴を開けるだけでなく、ネットワーク・リソースを大量に消費するため、ネットワーク速度が遅くなったというエンド・ユーザからの問い合わせがヘルプ・デスクに殺到するという事態を招いています。このように現在では、ワームとスパイウェアの影響により、業務の継続性に大きな支障が生じることが珍しくなくなっていますが、これはエンドポイントのセキュリティが充分でないことが原因と考えられます。

このような、ネットワーク・エンドポイントのセキュリティ状態の低下は、ほとんどすべての企業PCにアンチウイルス・ソフトウェアが導入されているにもかかわらず発生しています。同じことは、侵入検知システム (IDS) を導入しているネットワーク環境でも起きています。さらに言えば、ソフトウェアの脆弱性を修正するためのパッチが、ほとんどの場合新しいタイプの攻撃が出現する前に無償でベンダーより提供されているにもかかわらず、このような状況になっています。

これらのテクノロジーが有効に機能していない理由は明らかです。すなわち、アンチウイルス製品は基本的に事後対応的であり、事前予防的ではないということです。アンチウイルス・ベンダーは、新しいワームを発見してからでなければ、対応するシグネチャを作成し、テストすることはできません。ネットワーク管理者は、メーカーがシグネチャを提供した後に、各エンドポイントにシグネチャを配布します。新しいシグネチャを配布したとしても、配布開始時に企業ネットワークに接続していなかったPCは、企業ネットワークに接続するまでの間に外部でワームに感染してしまう可能性もあり、万が一外部でワームに感染してしまっていた場合には、そのPCが次に企業ネットワークに接続したとき、ネットワーク内に存在するすべてのPCに感染を広げることになります。SlammerやWittyといったワームが、わずか数分のうちにインターネット上の脆弱なホストのほとんどに感染したときなどは、すべてのPCにシグネチャを配布するのに数時間あるいは(多くの場合) 数日かかるアンチウイルス・ソフトウェアは、そういった危機的状況の中でほとんど無力な存在と化していました。現在では、主要なワームでは新しい亜種が毎日のように出現することが珍しくなくなっており、アンチウイルスのシグネチャの更新に関する問題は、さらに難しいものとなっています。

多くのセキュリティ管理者は、利用しているソフトウェアへのパッチ適用に関する限界を身をもって理解しています。パッチは大急ぎで作成する必要があるため、ベンダーによってリリースされるものとしてはおそらく最も品質管理のなされていないソフトウェアの可能性があるといます。したがって多くの場合、企業内での検証を行ない、自社環境で問題が発生しないか確認を行ってからパッチを配布する必要があり、その間に、そのソフトウェアの脆弱性を狙った攻撃が出現してしまいます。また、Microsoftなどのベンダーから次々と容赦なく重要なパッチが公開されるため、一般的に人材不足のことが多いIT管理者グループは、他の脆弱性を放置し一部の脆弱性だけに対処せざるを得なくなっています。

## より効果的なアプローチ

Blaster、そしてSlammerにより何十億ドルという損害がもたらされたことで、PCを経由した攻撃を阻止するための新しいアプローチが必要であることが明らかとなりました。チェック・ポイントは、この問題に対する解決策として、Total Access Protection (総合的なアクセス保護:TAP) 戦略を提唱しています。Total Access Protectionとは、すべてのPCに対し、ネットワークへの接続前に確実にセキュリティを適用することによって、企業ネットワークを保護するという考え方です。そして、このTAPを実現するうえで重要な役割を担うのが、エンドポイント・セキュリティ製品のCheck Point Integrity™です。Integrityは、エンドポイントの安全性やセキュリティ・ポリシー違反をチェックし、基準が満たされていない場合には企業ネットワークへのアクセスを拒否します。この機能は、ネットワーク・アクセス制御、スキャン&ブロック、エンドポイント・ポリシー制御、最近では検疫ソリューションなどと呼ばれています。指定できるポリシー要件には、次のようなものがあります。

- 最新のアンチウイルス/アンチスパイウェア・ソフトウェアが実行されているか
- 重要なパッチおよびサービス・パックがインストールされているか
- パーソナル・ファイアウォールに最新のルールが適用されているか
- ブラウザなどのアプリケーションのバージョンは最新か
- 禁止されているソフトウェアが実行されていないか
- 特定のレジストリ・エントリがあるか/ないか

違反しているポリシー要件が1つでもあるエンドポイント、およびIntegrityソフトウェアが実行されていないエンドポイントは、ネットワークのセキュリティが損なわれないようにするためネットワークの実環境には接続できず、隔離されます。要件を満たしていないエンドポイントのために、Integrityには、問題のあるセキュリティ要件を修正するための管理者用の簡単なツールが用意されており、エンド・ユーザは、この修正リソースを使用することで、エンドポイントを容易にポリシーに従った状態にすることができます。マウスを数回クリックするだけで、最新のアンチウイルス・シグネチャをダウンロードしたりパッチをインストールしたりすることが可能で、この他に簡単な手順をいくつか実行すれば、アクセス・セキュリティ・ポリシーに従った状態になります。また管理者は、古いバージョンのファイルやア

アプリケーションを自動的に修正するよう設定することもできます。この場合には、エンド・ユーザの操作なしで、エンドポイントをポリシーに従った状態に復元することが可能です。こうしてポリシーを順守し、セキュリティが確保されたエンドポイントには、そのエンドポイントの実環境へのネットワーク・アクセス権限が付与されます。

PCへの攻撃から企業を保護するためのこの新しいアプローチは、従来型の手法の弱点をすべて解消しています。すべてのPCのアンチウイルス・ソフトウェアを最新の状態に保つことは、もはや不確実なプロセスではなくなりました。なぜならIntegrityでは、シグネチャが最新でないPCはネットワークに接続することを許可されないからです。新しいワームが発見されてからそれに対応したシグネチャが提供されるまでの間は、優秀な製品として数々の受賞歴があるIntegrityのパーソナル・ファイアウォールが、新しいワームのPCへの侵入/PCから外部へのアクセスを阻止します。シグネチャが公開され、テストおよび検証作業が終了すれば、Integrityを使用して、ネットワークに接続されているすべてのPCにシグネチャをインストールすることができます。ただしその間も、Integrityのエンドポイント・セキュリティ・メカニズムおよびアクセス制御メカニズムが、「仮想パッチ」として最新の脆弱性を突く攻撃をブロックし、感染PCをネットワークに接続させないようにします。

## ネットワーク保護のためのより効果的なアプローチ

セキュリティ・ポリシーを順守していないエンドポイントを隔離する機能は、Integrityとネットワーク・ゲートウェイとを統合することによって実現されます。この統合を利用する場合は、ネットワーク・アクセスを行おうとするすべてのエンドポイントにIntegrityソフトウェアがインストールされていることも保証されます。Integrityソフトウェアがインストールされていない自社の管理外のPC（派遣社員や一時利用者などを含むゲストPC）は、通常のLANから切り離されたゲスト・ネットワーク・ゾーンに隔離できます。これを可能にするのは、Cooperative Enforcement®（協調施行）と呼ばれるチェック・ポイント独自の統合技術です。この協調施行技術により、Integrityは、さまざまなベンダーから提供されている多種多様なVPN機器、スイッチ、ルータ、無線アクセス・ポイントと通信を行い、ネットワーク・アクセスを制御できるようになります。協調施行技術においては、ゲートウェイ・サーバはネットワーク・アクセスの関所として機能し、Integrityは、エンドポイントがポリシーを順守しているかどうかに応じて、そのアクセスを拒否するか許可するかをゲートウェイ・サーバに通知する役割を担います。Integrityとネットワーク・ゲートウェイの統合は、ネットワークにアクセスするすべてのPCでセキュリティが確保されていることを保証すると同時に、障害ポイントが増えてしまうという、企業ポリシーの実施を非統合型で行う場合の問題点を回避することにもつながります。

他に類を見ない協調施行が実現する独自の機能により、Integrityは、事実上すべてのマルチベンダー・ネットワーク環境でネットワーク・アクセスを制御することが可能になります。Integrityは、リモート・アクセス用のVPN-®、内部ネットワーク・セキュリティ用のInterSpect™、そしてSSLベースのネットワーク・アクセス用のConnectra™という、チェック・ポイントのすべてのセキュリティ・ゲートウェイ製品と密に統合できます。とりわけ、IntegrityとInterSpectの組み合わせでは、境界内部におけるワーム被害に効果的に対抗できる、最も包括的で、最も導入の容易な防御ソリューションを実現できます。また、Integrityは、ほとんどのベンダーのIPSec機器およびSSL VPN機器との組み合わせで協調施行を実現することもできます。さらに、Integrityのアーキテクチャは、認証に関するオープンな標準規格であるIEEE 802.1xをサポートしているため、主要機器メーカーが提供する802.1x互換のさまざまな内部ネットワーク・ゲートウェイと統合することが可能となっています。最良のエンドポイント・セキュリティと、さまざまなベンダーが提供する広範なネットワーク・ゲートウェイ製品とを統合可能にすることは、Total Access Protectionが掲げる基本方針の1つでもあります。

Integrityとネットワーク・ゲートウェイを直接統合することは、企業ポリシーを実施するという点において最も確実性の高い方法です。しかし、ゲートウェイとの統合が行えない環境（エンドポイントが企業ネットワークに接続されていない場合など）においても、Integrityは単独で包括的なポリシーを実施することができます。Integrityはそのために、エンドポイントがポリシーを順守していないことが判明した場合、ユーザ・アクセスを一部のネットワーク・リソースまたはIPアドレスに限定するというエンドポイント・ファイアウォール・ルールを適用します。協調施行の場合と同様、Integrityのみによるポリシー実施においても、ユーザが容易にアクセスに必要なポリシー要件を満たす状態に戻れるよう支援する修正リソースが提供されます。また、Integrityのトータル・クライアント・ロックダウン（Total Client Lockdown）機能により、エンド・ユーザやハッカーがIntegrityを無効にしたりポリシーを変更したりすることが禁止されます。このため管理者は、すべてのIntegrityクライアントで常にエンドポイント・セキュリティおよびポリシーの順守が実施されているかどうかを心配せずに済みます。

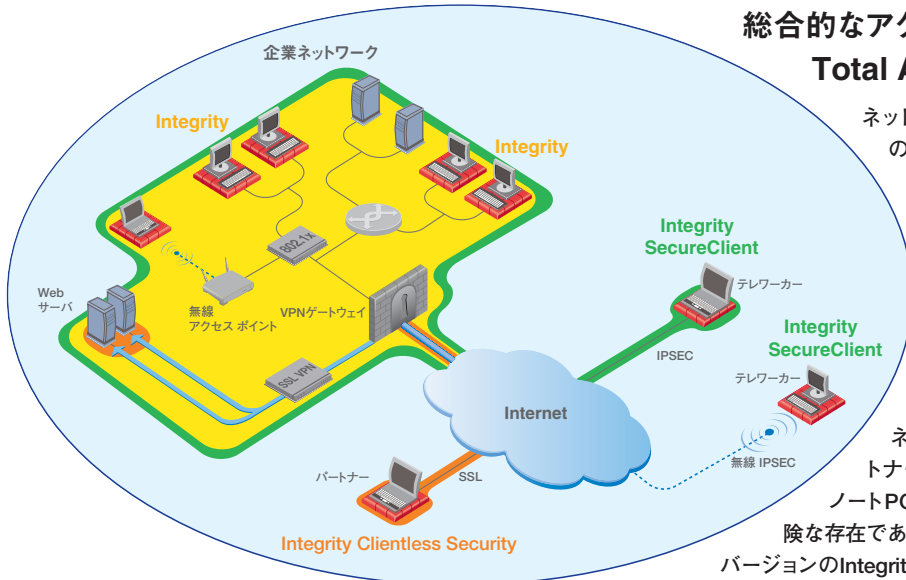
## 協調施工 (Cooperative Enforcement®) の利点

**Total Access Protection**：業界初の総合的なアクセス保護のための戦略であるTAPは、企業ネットワークに接続するすべてのPC（社員用PC/ゲスト用PC、内部PC/リモートPC、有線LAN/無線LAN接続）に対し、あらかじめ定義されたエンドポイント・セキュリティを漏れなく適用します。TAPは、すべてのエンドポイントに先進のセキュリティ技術を提供し、すべてのエンドポイントでポリシーを実施することにより、ワームやスパイウェアなどの脅威がもたらすさまざまなセキュリティ・リスク（業務の継続性に関わる問題、データ漏洩の問題など）を大幅に軽減します。

**広範なゲートウェイとの統合**：Integrityは、チェック・ポイントのすべてのゲートウェイ製品、および20社以上の主要ベンダーが提供するゲートウェイ製品と連携することで、包括的なエンドポイント・ポリシーの実施を保証します。協調施行技術により、Integrityは、エンドポイントのセキュリティ状態を検証し、主要なVPN機器および200種類以上のスイッチ、ルータ、および無線アクセス・ポイントと協調してネットワーク・アクセスをコントロールできるようになります。Integrityは、多様なマルチベンダー環境におけるネットワーク・アクセスを保護するために、広く普及している標準規格802.1xを実装した初めてのエンドポイント・セキュリティ製品です。

**トータル・クライアント・ロックダウン（Total Client Lockdown）**：クライアントのセキュリティ・ソフトウェアが変更されたり無効にされたりした場合、ネットワーク・アクセス・コントロールを実施できず、その効力を失ってしまいます。内部ゲートウェイが、ポリシー違反のあるエンドポイントを隔離することのできない環境では、管理者は、ポリシーの実施をセキュリティ・クライアント自体に頼るしかありません。Integrityに搭載されたこの高度な自己防衛メカニズムは、攻撃者やエンド・ユーザが設定を変更したり無効にしたりすることを禁止します。これにより、ゲートウェイが使用されているかどうかにかかわらず、事実上すべての環境においてネットワーク・アクセスを保護することが可能になります。

## 総合的なアクセス保護を実現する Total Access Protection



Total Access Protectionは、ネットワークへの接続前に、すべてのネットワークPCがあらかじめ定義したセキュリティ要件を満たしているかを確認し、満たしていた場合のみアクセスを可能にします。

ネットワーク・アクセス制御のためのチェック・ポイントの戦略に関して重要なポイントは、企業ネットワークに接続するあらゆるタイプのエンドポイントを制御できる点です。つまり、社員用PCとゲスト用PC、リモートPCとネットワーク内部のPC、有線LANを利用するPCと無線LANを利用するPCのすべてをコントロール可能であるということです。これは、ネットワーク・アクセス制御を行う上で非常に重要な点です。セキュリティ対策が充分でないPCで自社のWebアプリケーションにアクセスするネットワーク・ゲスト(派遣社員や顧客、ビジネス・パートナーなどを含む一時利用者)は、ワームなどに感染したノートPCを自社ネットワークに接続する社員と同じくらい危険な存在であるからです。こうした状況に対し、クライアントレス・バージョンのIntegrityでは、ブラウザのプラグインを使用することでゲスト

によるネットワーク・アクセスを制御します。あらゆるタイプのエンドポイントに対するアクセス制御と、業界で最も実績のあるエンドポイント・セキュリティを提供し、チェック・ポイント製品と多種多様なベンダーのゲートウェイ製品との統合を可能にするTAPは、企業ネットワークを保護する戦略としてまさに理想的と言えます。

### 他社のアクセス制御技術

チェック・ポイントがネットワーク・アクセス・コントロール・ソリューションを市場に投入したのは、2002年のことでした。現在これは、アクセス・ポリシー実施のアプローチとして、最も成熟し、実績のある、包括的な存在となっています。このソリューションは、すでに2,000以上もの組織に導入されており、PC経由のあらゆる攻撃からこれらの組織を保護しています。

最近では、いくつかのベンダーもネットワーク・アクセス制御に対するニーズが極めて強いことを認識し始めており、具体的ではないながらも、このようなソリューションを提供予定であることをプレス・リリースで発表しています。これらのベンダーは、ネットワーク製品およびオペレーティング・システムに内在する欠点が企業にとって大きな問題となっていることを認識しており、この欠点を解消するにはセキュリティが確保されたPCだけにネットワーク・アクセスを許可するのが最良の方策であるという、チェック・ポイントの以前からの主張に同調しています。

中でもCiscoとMicrosoftは、チェック・ポイントの既存ソリューションと同じようなアクセス・ポリシー実施の仕組みを提案しています。しかしこれは、チェック・ポイントほど包括的でもオープンでもありません。CiscoおよびMicrosoftとチェック・ポイントのアプローチの違いは、セキュリティ・レベル、インフラストラクチャの変更、そして短期的/長期的な柔軟性の獲得という点に関して、重大な問題を示しています。

- CiscoのNetwork Admission Control (NAC)とMicrosoftのNetwork Access Protection (NAP)は、各ベンダー独自に開発された技術であり、自社製品だけを使用するように顧客を囲い込むことができるものです。例えば、NACをサポートするのはCiscoの最新のスイッチ、ルータ、および無線アクセス・ポイントだけです。発表されている文書によれば、NAC発表以前のCisco製品や他ベンダーのネットワーク機器を使用してネットワーク・アクセスをコントロールすることはできません。
- NACソリューションを完全に導入するためには、ソフトウェアおよびハードウェアのすべてのレイヤをCisco製品(認証サーバのACSを含む)で統一する必要があります。また、アクセス・コントロールに使用するCiscoのネットワーク機器は、認証に関する標準規格802.1xのCisco独自実装をサポートするためにアップグレードする必要があります。同様にMicrosoftのNAPでも、同社の最新バージョンのPC製品およびサーバ製品を使用することが必要となる見込みです。
- 2005年後半の時点では、Cisco、Microsoftの両社とも、プレス・リリースで発表したソリューションを提供するには至っておらず、Microsoftは、NAPの提供は2007年以降になるとしています。いずれ2つのソリューションのすべてのコンポーネントが市場に出そろったとしても、そのときになってようやく、バージョン1.0の安定性がどの程度のものであるのか、統合に関する問題がどの程度解決されているのかが判明するのであり、それらの解決にさらに時間がかか

ることになります。

チェック・ポイントのTotal Access ProtectionとNACおよびNAPは、次の点において際だって対照的です。

- TAPは現段階で、成熟し、実績のある、包括的なネットワーク・アクセス制御を提供可能です。
- TAPは、標準規格802.1xのほとんどの実装をサポートしています。したがって、さまざまなベンダーのネットワーク製品および認証製品を組み合わせる使用することができます。またTAPは、Integrityとチェック・ポイントのゲートウェイ製品 (VPN-1、InterSpect、Connectraなど) を統合することで、容易に実装可能となっています。
- TAPは、ネットワーク・アクセス・コントロールの管理を容易にします。TAPは、企業で使用されているWindowsおよびIOSのバージョンに関係なく同じように管理できます。

チェック・ポイントは、顧客のニーズに最適なITインフラストラクチャをサポートするという哲学に基づき、チェック・ポイント製品をNACとNAPにも対応させていく予定です。それと同時に、多くの企業にとって戦略上の最良の選択肢であり続けるために、Total Access Protectionの拡張も続けていきます。チェック・ポイントは、セキュリティに特化したセキュリティ専門の企業です。顧客の保護を唯一最大の目的とするソリューションを提供できるのは、セキュリティ専門企業以外にありません。

## ネットワーク・アクセス・ポリシー実施の将来

企業の通信手段が多様化し、常時接続のPCやネットワーク・アクセス機器が急激に増加・多様化した結果、ビジネス機会と共に、セキュリティ・リスクも増大しています。チェック・ポイントには、顧客企業が、絶えず進化を遂げる脅威の一步先を行くことを可能にする、革新的な事前予防セキュリティを長きにわたり提供してきた実績があります。チェック・ポイントは、企業のコンピューティング・リソースに接続するすべてのホストが、その接続形態を問わず、セキュリティが確保され、企業ポリシーを順守した状態となるようにするための仕組みに注力しています。これは、Total Access Protectionの基本原則であり、ユーザの数、デバイスの種類、プラットフォーム、ネットワーク環境を問いません。このような柔軟性に欠けるネットワーク・アクセス制御のアプローチ (サポートするのが単一ベンダーのネットワーク機器やオペレーティング・システムのみであるなど) にメリットがあるのは、どちらかと言うと顧客ではなく、むしろベンダー自身です。同じように、802.1xなどの業界標準を独自実装するのも、顧客ではなくベンダー自身の利益のためです。ある1つのベンダーに囲い込まれたり、そのような実装を採用することでTCOが上昇したりするのは避けたいというのが、ほとんどの企業に共通する思いでしょう。

チェック・ポイントは、あらゆる環境においてオープンかつ包括的なアクセス・ポリシーの実施を可能にすることに加え、エンドポイント・セキュリティ・ソリューションの導入および管理に伴う管理者の負担を最小限に抑えるよう努力しています。標準ベースの技術を採用し、管理者の負担を軽減することは、エンドポイント・セキュリティとITインフラストラクチャ全般のTCOを最大限削減することにつながります。これらセキュリティ上、財政上のメリットを提供することにより、チェック・ポイントは、企業にとって最良のエンドポイント・セキュリティを提供し続けることを約束します。

## まとめ

Check Point Integrityは、今ある脅威、そして今後出現する脅威からエンドポイントを確実に保護する、高い機能性と柔軟性を兼ね備えた包括的なソリューションです。Integrityは、すべてのネットワーク・エンドポイントを事前予防的に保護し、ポリシー実施を一元管理することによって、悪意あるコードや個別的な攻撃から企業ネットワークを守ります。チェック・ポイントは、Integrityを通じて、Total Access Protectionの実現をサポートします。

## Check Point Software Technologies Ltd.について

チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド (www.checkpoint.com) はインターネット・セキュリティにおける世界トップ企業として、特に企業向けファイアウォール、パーソナル・ファイアウォール、およびVPNの市場においてマーケット・リーダーとして広く認められています。チェック・ポイントは、NGXプラットフォームを通じて、企業ネットワークおよびアプリケーション、支店・支社環境、およびパートナー各社のエクストラネットのビジネス通信およびリソースを保護する、広範な境界、内部、Webおよびエンドポイントに対するセキュリティ・ソリューションのための統一されたセキュリティ・アーキテクチャを提供しています。チェック・ポイントのZoneAlarm製品群は、インターネット・セキュリティの分野で高い信頼性を誇るブランドとして、数々の賞に輝くエンドポイント・セキュリティ・ソリューションを提供し、何百万台ものコンピュータをハッカーやスパイウェア、データの盗難などから保護しています。またチェック・ポイントは、350社を超える各分野のトップベンダーが提供する“ベスト・オブ・ブリード”ソリューションとの統合および相互運用性を実現するフレームワークであるOPSEC (Open Platform for Security) により、自社ソリューションの能力をさらに拡大します。現在、チェック・ポイント・ソリューションは、世界88ヶ国、2200社を超えるパートナー・ネットワークを通じて販売、導入、サービス提供されています。チェック・ポイントの顧客にはFortune 100社の全社を含む、何万ものあらゆる規模の企業や組織が含まれています。

©2003-2005 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, Eventia, Eventia Analyzer, Eventia Reporter, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, NGX, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, 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, Stateful Clustering, TrueVector, Turbocard, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, VPN-1 XL, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, 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、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。本書で記載された製品は米国の特許No.5,606,668、5,835,726、6,496,935、6,873,988、および6,850,943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。

Total Access Protection

P/N:501759-J 2005.12

※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。



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

**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\\_jp@checkpoint.com](mailto:info_jp@checkpoint.com) Tel: 03 (5367) 2500