

侵入防御システムの導入における 最も効果的な手法

Contents

本書の内容

はじめに	3
導入ニーズの把握	3
導入ポイントの選定	5
ニーズに合ったIPSの選定	6
チューニングと構成	7
防止措置の実施	8
その他の便利なヒントと方法	9
外部への通知	9
IPSへのアクセス権限	9
記録保管に関する考慮事項	10
まとめ	10

はじめに

近年、侵入防御への関心が急速に高まりました。これにはいくつかの理由がありますが、そのなかでもとりわけ「マルチ・レイヤによる防御戦略は不可欠」という考え方が根付いてきたことが挙げられます。また、法令遵守の面からも、次世代のセキュリティ・テクノロジーとして侵入防御システム(IPS)の導入を検討する企業が多くなっています。理由が何であれ、適切なテクノロジーを選択するだけでなく、それを正しく導入することが重要です。この技術白書では、IPS技術の正しい選択と正しい導入方法について、これら2つの目標を達成することを目的として、IPS導入を成功させるための条件について解説します。

まず、一般にIPSというと、ネットワーク・ベースのIPSとホスト・ベースのIPS、ファイアウォール、そして時にはスマート・スイッチまで含まれる場合があることを認識しておく必要があります。ただし、この白書では、ネットワークIPSの導入に関するベスト・プラクティスに焦点を絞って説明します。

導入ニーズの把握

IPSを導入する前に、何を保護する必要があるかを把握しなければなりません。すべてを保護する、と言うのは簡単なことです。しかし、その「すべて」には何が含まれるかを考えてみましょう。アプリケーションとサーバは間違いなく含まれるでしょう。他には、プリンタ、デスクトップ、ルータ、スイッチなど、ネットワークに接続されているデバイスも含まれるかもしれません。しかし問題は、IPSですべてを保護すると、非現実的な期待が慢心につながるおそれがある点です。

重要なポイントは、IPSの導入初期に、あまりにも意欲的な計画を立てないようにすることです。より細かいルールやコントロールは、セキュリティ管理のスキルが向上し、ネットワークやアプリケーションの機能性への理解が深まった段階でいつでも追加導入できます。一番最初にIPSを導入する場合は、FTP、電子メール、Webサービスなど、ネットワーク境界で外部に接しているサービスに集中するのが最善です。特に、Sarbanes-Oxley Act of 2002(サーベンス・オクスリー法:米国企業改革法、略称SOX法)、Gramm-Leach-Bliley Act(米国金融制度改革法)などの法令遵守規定に対応するために導入する場合、保護するサービスやリソースは、1種類の保護に依存するだけでは不十分な、ビジネスにとって最も重要性の高いプロセスに限定します。

何を保護すべきかを把握できたら、次にそれらを何から保護したいかを考えます。例えば、プロトコル・ベースの脆弱性エクスプロイトとトロイの木馬に対しては、すでにファイアウォールとアンチウイルス・ソフトウェアで2重の保護をかけているかもしれません。一方、ブルート・フォース・アタックやアプリケーション・ベースの攻撃、社内の社員による内部からの攻撃などから重要なプロセスを保護する手段は講じていないかもしれません。

IPSの導入を成功させるには、企業をどのような脅威から保護したいかを定義できなければなりません。この一見単純なことを軽視しないようにしてください。対処すべき脅威について理解することは、導入要件の決定に非常に大きな影響を及ぼします。企業のネットワーク環境に侵入する恐れのあるエクスプロイト、スパイウェア、およびマルウェアはいくつかのグループに分類できます。脅威を分類し、できる限りそれらをグループ化して効果的に対処することが重要です。脅威を個別に管理することは非常に困難です。しかし、脅威の動作や感染および伝染の方法は、さまざまなレベルで共通していることが多いのです。

脅威は、例えば以下のように分類できます。

- 認証および権限の問題。このタイプには以下が含まれます。
 - 特権的なアクセス – 適切な認証なしで管理者権限 (例えばroot) を取得する
 - ユーザ・アクセス – 適切な認証なしでユーザ権限を取得する
- マルウェア。このタイプには以下が含まれます。
 - ワーム – 既知のサービス・エクスプロイトをマッチングしたり、既知のエクスプロイトに似た動作を実行する
 - コード実行 – 標的とするシステムで任意のエクスプロイト・コードを実行し、好ましくないプログラム (キーボード・ロガーなど) をインストールする
- サービス妨害 (DoS) – サービスを正常に使用できなくします。このタイプには以下が含まれます。
 - Ping of Death
 - Sync Flood
- ベスト・プラクティス (適切な利用法) の違反 – 悪意はないが、セキュリティに関する適切な利用方法 (ベスト・プラクティス) に反するアクティビティ (例えば、パスワードなしのユーザ名入力、脆弱なソフトウェア・バージョンにリンクされたバナーなど)。このタイプには以下が含まれます。
 - セキュリティ・ポリシー違反 – 特徴的なものとしては、インスタント・メッセージ、動画のストリーミング、許可されていないサブネットからのシステムやアプリケーションへのログインなどがあります。ファイアウォールなどのセキュリティ・ポリシー実施ポイントが正しく構成されているかどうか (またはすでに攻撃を受けているかどうか) を示すトラフィックも、このグループに含めることができます。
 - パスワードの長さ、および文字と数字の適切な混合
 - 攻撃を行う為の事前の情報収集
 - データへのアクセスや、制限が施されたファイル、ディレクトリ、またはデータを移動しようとする試み
- アプリケーション・ベースの攻撃 – バッファ・オーバーフロー、インジェクション攻撃などの手段で、特定の種類のサーバの脆弱性を突く攻撃。このタイプには以下が含まれます。
 - アプリケーションのドメインの外部で情報や権限にアクセスを試みるWebベースのインジェクション攻撃
 - 一般的なアプリケーションやサービスを狙ったバッファ・オーバーフロー攻撃
 - DNSの侵害およびスプーフィング

多くの場合、上に挙げた手段が行使される前に、脅威による「偵察」活動が行われます。こうした活動は、潜在的な攻撃者が攻撃を試みようとするターゲットとしているネットワークに脆弱な部分があるかどうかを見つけるためのものです。また、これによって、特定のタイプのシステムに合わせてエクスプロイトを改造することも可能になります。多くの偵察活動は非常に綿密で、脆弱性のあるコンポーネントを利用して感染や伝染を拡大させることができるかどうか、また、別のシステムやコンポーネントを制御できるかどうかまで調べています。

IPSを固有の環境に適合させるためのチューニングには、十分な時間をかける必要があります。前述の分類のうち、認証、マルウェア、およびサービス妨害は比較的簡単に実装できます。ベスト・プラクティス違反とアプリケーション・レベルの攻撃は危険性が高いため、早い段階で捕捉することが非常に重要です。なお、これらのアプリケーションにパッチを施したり、ポリシーに変更を加えたりするたびに、IPSの設定の見直しが必要になる可能性がある点にも注意してください。

導入ポイントの選定

IPS導入を成功させる上で、センサーを配置するポイントの選定は極めて重要です。最大の効果を上げるにはIPSデバイスをどこに配置したらよいか、ということです。あらゆる箇所のネットワーク・インフラストラクチャやアプリケーションは、常に高い危険にさらされており、それらの領域が標的となりやすいのです。通常、IPSデバイスは以下の場所に導入します。

1. ファイアウォールおよびWANルータの背後
2. サーバ群またはネットワーク・リソース群の手前
3. その他のネットワーク・アクセス・ポイント

これらの重要な場所にIPSを集中し導入することで、初期導入においてより大きな効果を得ることができます。これは、ほとんどの法令遵守要件が、ネットワーク・コアの入口と出口に焦点を合わせているからです。また、ほとんどのネットワーク・トラフィックはこれらの場所で転送および有効化されるため、こうしたセキュリティを守る上で重要な箇所にIPSを導入することでセキュリティ対策の効果を最大化できます。

WANルータが設置されているポイントは、IPSを導入する場所として非常に有力な候補です。これらのポイントは、リモート・サイトからのエクスプロイトの入口になることが多い場所であるにもかかわらず、管理者として直接制御することがほとんどないためです。万が一、ルータで接続されている先のリモート・サイトやビジネス・パートナーのネットワークが感染すると、ほとんどの場合、ルータの部分でのセキュリティ対策が適切に施されていないため、すでにリモート・サイトやビジネス・パートナーの拠点で猛威をふるっている感染体に対して無防備になってしまいます。

サーバ群や何百ものアクセス・ポイントに加え、主に倉庫などで利用される無線対応のアプリケーションからの接続も別のタイプのアクセスです。簡単な例は、ブラックベリー・サーバや何百台もの無線バーコード・リーダーです。これらの新たなタイプのアクセス・クライアントは、どのようなインフラストラクチャでも特に脆弱なポイントです。これらはネットワーク内の境界をはっきり示すことが多く、他の手段では保護できないサービスやデバイスの代表例です。

これらの境界は、論理的および物理的な責任が追加されることを意味します。これらのアクセス・ポイントは、保護するのが難しいアプリケーションやサービスがあることを示します。しかし、これらも保護しなければなりません。

ニーズに合ったIPSの選定

既にIPSベンダーは無数に存在しており、すべてのベンダーのネットワークIPSが同じように作られているわけではありませんので、ニーズに合ったIPSの選定プロセスが混乱することもしばしばです。IPSを選定する際に考慮すべき主な条件を以下に示します。

- 検出の精度 – IPSを検討する際に見落とされがちなのは、本当に正しく防止できるかどうかです。検出の精度が高いことは必須条件です。注意を払うべきポイントは、検出テスト精度のスコアです。誤検出がおきても管理者が不愉快になるだけで済む侵入検知システム (IDS) とは異なり、IPSでは誤検出がビジネスに重大な影響を及ぼすおそれがあります。
- 帯域幅要件 – 速度だけにとらわれず、ネットワークの帯域幅要件も考慮する必要があります。リモート・サイトへのWAN回線が1.5Mbpsの専用線なのに、その場所にギガビット対応のIPS機器を導入しても意味がありません。ただし、公表されている帯域幅にかかわらず、パッシブな監視モードではなく、アクティブなインライン・モードで要件を満たすかどうかを必ず確認してください。
- 管理プラットフォーム – IPSを評価する場合、アプライアンスやセンサーの性能ばかりに目が向き、管理プラットフォーム全体を全く考慮しない方が多いようです。アプライアンスが複数台ネットワーク中に存在した場合でも、グループ別に効果的に管理できるかどうか、シグネチャのアップデートを自動化できるかどうか、アップグレードを導入できるかどうか、ポリシーを構成できるかどうかなどの点は、すべて評価の一部として確認する必要があります。
- チューニングの柔軟性 – IPSを柔軟にチューニングできるかどうかも重要です。特に、誤検出に関わる問題を軽減できるよう、定性的なスコアや信頼性スコアに基づいて防止およびブロックをチューニングできるかどうかを確認してください。
- ハイ・アベイラビリティ – IPSモデルにおいて、アプライアンスのハイ・アベイラビリティを検証することは必須です。万が一のハードウェア障害の発生に備え、アプライアンスは、フェイル・オープン・オプションやフェイル・クローズ・オプションを備えていなければなりません。ただし、セキュリティが非常に重要なビジネス環境では、アーキテクチャ全体におけるフェイルオーバー機能にも注意を払う必要があります。例えば、サーバ・コンポーネントがフェイルオーバー機能を提供する製品を選択してください。
- スケーラビリティ – この点は、環境の規模によってはそれほど重要ではありません。しかし、規格以上の数のセンサーを設置する場合や、導入規模をかなり拡大する予定がある場合は、アーキテクチャ全体のスケラビリティが要件に見合うかどうかを確認する必要があります。
- レポーティング – 法令遵守要件の面を考えると、既知の攻撃、保護の範囲、脆弱性などの状態に関するレポートの作成機能は不可欠です。

適切なIPSの選定に関しては、他にも多くの注意点があり、これとは別に白書としてまとめられるほどです。しかし、上に挙げた7つの主要な条件を考慮に入れば、初期導入に適切な製品を選択できるはずです。

チューニングと構成

システムをインストールしたら、使用可能な検査機能をすべて有効にしたいくなるかもしれません。しかし、これは余程のことがない限り避けてください。先の分類に基づき、最も脅威を感じているか、最も脆弱だと分かっているグループから、一度に1つずつ有効にします。次に、センサーからの警告を調べ、有効にしたグループの 익스プロイトのみを監視します。脆弱性スキャンや侵入テストを定期的の実施していたとしても、ネットワークに関してこれまでにない新たな洞察が得られるはずで

チューニング・プロセスでは、サービスやアプリケーションについて、組織内にこれまで挑戦した人がいないほどのレベルまで深く理解する必要があります。組織のアプリケーションやバックエンドの多くがいかに粗雑に記述されているかに気づき、驚くことになるかもしれません。その多くは承認済みのRFCにネットワーク・サイドで準拠しておらず、適切なプログラミング規則にさえ従っていないものもあるでしょう。バックアップ・ソフトウェア・クライアントのほとんどは、IPS/IDSセンサーを混乱させるアプリケーションの端的な例です。また、SNMPのデフォルト構成を使用しているデバイスや、感染したデスクトップに向けられている不正なメール・サーバなども見つかるかもしれません。

これらの警告を詳しく調べ、それが本当であるか誤検出であるかを検証します。誤検出だった場合は、システム全体をチューニングするか、誤検出に関係する特定のシステムのみをチューニングします。通常は、警告に関係する発信元システムと送信先システムのIPアドレスを使用してチューニングを行います。IPSの設定構成を変更することで、すべてのトラフィックを無視するようしたり、イベントを記録だけしてコンソールには報告しないようにすることもできます。また、イベントの原因となったアプリケーションを直接修正して、発信元で警告が生成されないようにすることも可能です。1つのグループについてこれらの作業を完了したら、次のグループの検査機能を有効にして同じ作業を繰り返します。

このプロセスでは、検出された特定のイベントが実際に悪意のあるものかどうかについて、その信頼性スコアも把握できなければなりません。一部の製品にはこの機能が組み込まれており、より細かいレベルまでチューニングできるようになっています。この非常に有用な機能があれば、特定のセキュリティ・イベントに関連付けられた信頼性スコアに基づいて防止のレベルを設定できるようになります。既知のシグネチャと一致する攻撃の信頼性スコアは高くなり、あいまいな性質の不審なアクティビティの信頼性スコアは低くなります。例えば、このスコアが90%以上の攻撃がブロックされるようにIPSを設定できます。これにより、重大な攻撃を確実に防止しながら、正当なトラフィックを誤ってブロックする可能性を低く抑えることができます。

初期のチューニングと細かい調整が完了したら、次のステップに進む準備ができたように感じるかもしれません。しかし、多くのアプリケーションは常に稼働しているわけではないため、IPSによる検査も時々実施されるだけです。例えばバックアップのように、多くのアプリケーションは夜中または奇数日にのみ実行されます。財務や給与計算のアプリケーションは、週次や月次でしか実行されないかもしれません。決算パッケージにいたっては、月末、四半期末、または期末にしか実行されない可能性もあります。したがって、初期段階での全体的なチューニングは完了しても、おそらくその後数日、数週間、数ヶ月にわたり、同じプロセスを繰り返してチューニングを確認する必要があります。一般的には、初期チューニングが完了した後、週末、月末、または四半期末に再度チューニングを実施します。

簡単に始められるのは、既知のマルウェアや悪意のあるコード実行の検査です。IPSの導入と同時にワームやウイルスのリスクが軽減されるため、すぐにその効果を実感することができます。もう1つ注意しなければならない重要な点は、すでにマルウェアに感染したシステムが、ネットワークの外から持ち込まれるおそれがあることです。内部の感染したリソースを特定するために、いくつか考慮すべき事項があります。

外部の脅威に対する高度なチューニングが完了したら、次は内部の感染したリソースに対処するため、IPSの規則やポリシーを作成します。ノートPCは格好の標的になります。保護された企業のネットワーク環境の外で、長期にわたって使用されることが多いからです。このようにして感染したシステムは、バックドア通信を監視することで識別できます。一部のマルウェアやスパイウェアは自身のコピーの作成複製や外部への伝達のためのコンポーネントを備えており、感染したシステムが主システムと通信しようとしたときに伝染を試みます。例えば、エクスプロイトが自身の電子メール・サーバを起動し、感染した電子メールをアドレス・ブックに登録されているすべてのアドレスに送信することも考えられます。これを検出するには、電子メール・サーバから送出される電子メール・トラフィックを監視し、企業のメール・サーバとして識別されないトラフィックを探します。これらのメールは、標準的でないメールのIPポート番号で送信されることもあります。

防止措置の実施

ここまでの時点で、かなり安心できる状態になっているはずです。IPSシステムを導入し、チューニングも完了して信頼性もかなり上がっています。受信する警告も、ほとんどが本当の攻撃を知らせるものです。ここまで来れば、新たな措置を講じることができます。

いよいよ、不愉快なトラフィックをどのようにして排除するかを決定します。予防策を講じる前に、いくつかの選択肢を検討する必要があります。選択肢は、以下の3つの手法に分類できます。

- **トラフィックを除去する** – この場合はパケットが除去されるため、当事者間でイベントを通知するためのプロトコル・ベースのハンドシェイクは行われません。この方法の利点は、攻撃がうまくいかない理由を攻撃者側から判断するのが難しい点です。この時点で、攻撃者が次に打つ手がかなり限定されます。
- **攻撃者のブラックリストを作成する** – この方法では、いったん特定できた攻撃元をリストに追加していきます。検査中にこのリストに当てはまるパケットが発見されたら、検査を中断してそのパケットを除去します。この方法の利点は、IPSシステムへの負荷が小さいことです。大量のイベントが発生した場合に、IPSシステムが正常に稼働し続けるか、サービス妨害攻撃に圧倒されてしまうかの分かれ目になる可能性があるため、システムへの負荷は非常に重要です。
- **リセット** – 攻撃者とその標的にTCPリセットを送信することで、両者に接続が切断されたことを知らせます。これは最も温和な方法で、ポリシー違反などに使用します。この方法であれば、両当事者のアプリケーションを安全に回復できます。

その他の便利なヒントと方法

ここまでで説明したポイント以外にも、覚えておくと便利なヒントや方法があります。

外部への通知

まず、外部通知機能を利用する方法があります。中小規模企業の多くでは、コンソールを常に監視する専任者を置くことは現実的ではありません。専任のセキュリティ担当者がいたとしても、その業務は多岐にわたることが多く、コンソールを常に監視するという非常に重要な任務に専念できるわけではありません。その場合は、重大な通知を外部（無線PDAや携帯電話などのモバイル・デバイス）に送信するように設定します。どの通知を外部に送信するかは、攻撃の重大度に応じて判断します。この考え方の延長として、各イベントを以下の2つのグループに分類することもできます。

- 無作為攻撃 – 攻撃者（通常は自動化されたプロセス）は、標的とするシステムのどこに脆弱性があるかを探します。通常この段階では、ワームやトロイの木馬などによって、できるだけ多くのシステムやネットワークに無作為に攻撃を仕掛けます。このグループには、検出が難しい複合型の脅威（複数のタイプの偵察、攻撃、脅威の複製を組み合わせたもの）も含まれます。
- 集中攻撃 – 標的を決めた攻撃者は、攻撃が成功するか、それ以上打つ手がなくなるまで、猛烈な攻撃を続けます。

シグネチャとポリシーが最新の状態になっていれば、ビジネス・オペレーションにとって重要な特定システムを標的にした攻撃でない限り、ほとんどの無作為攻撃は自動的に処理できます。この場合は、直接的な通知は必要ありません。しかし、集中攻撃となると話は別です。企業のセキュリティやポリシーを侵害する計画的な攻撃が行われた場合、特にそれがビジネス上重要なサーバへの攻撃であれば、すぐに通知が届くようにしておかなければなりません。

IPSへのアクセス権限

もう1つの重要なポイントは権限です。IPSは、単に悪質なトラフィックをブロックするだけのアプライアンスではなく、保護とポリシーを実施するポイントとしても機能します。すべての重要なインフラストラクチャ・コンポーネントやシステムと同様に、管理者ごとに別々の権限セットを使用してアクセスし、必要に応じてアクティビティや変更をログに記録して、それらを実施した個人まで特定できるようにしておく必要があります。多くのIPSシステムでは、管理ユーザを階層構造で簡単に管理できるようになっています。

記録保管に関する考慮事項

IPSに関する問題の中では重要度はそれほど高くありませんが、最後のポイントは警告情報の保管についてです。記録の保管期間をどのくらいに設定すべきかについては、以下の2つの情報に基づいて検討します。

- 企業の情報保管方針 – 通話記録やシステム・ログ・ファイルの保管に関する方針を参考にします。
- 業界の慣例や法令遵守要件

できる限り、実際の保管方針とバックアップ手順の間に食い違いがないようにします。

警告情報の保管手段を検討する際は、IPS/IDSの記録の状態によっては法的措置の証拠として提出することが認められない場合があることに注意する必要があります。保管スペースを節約するために圧縮したり一部を切り捨てたりすると、法的な証拠として認められない可能性があります。この点は、これらの情報を使用して個人や企業を告訴または弁護しようとしたときに問題になるおそれがあります。IPSのベンダーに、ディスク容量のプランニングについて確認することもお勧めします。

まとめ

IPSの導入を成功に導くには、次の手順に従う必要があります。

- 脅威からのリアルタイム保護のニーズを把握する
- 導入環境のニーズに合ったIPS製品を選定する
- IPSの効果的な配置場所を選定する
- 十分な時間をかけてシステムをチューニングする
- 法令遵守のためのレポート・パラメータを設定する
- IPSデータの保管およびバックアップを設定する
- システム全体を必ず定期的に評価する

IPS導入で重要なのはプランニングです。事前のプランニングに時間をかければかけるほど、その結果により満足できるはずですが、また、プランニングによって、IPSシステムが提供する保護や情報を切望している個人やグループの期待を調整することもできます。

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トップ企業として、世界中の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、データ・セキュリティおよびVPN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、ネットワーク・セキュリティ、データ・セキュリティ、およびセキュリティ管理ソリューションを含む広範囲なポートフォリオにより、ITセキュリティへのPUREなフォーカスを実現します。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、リモート・ユーザ、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に対する広範なセキュリティ保護を実現する、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。更にチェック・ポイントは、業界をリードするデータ・セキュリティ・ソリューションである、PointSec製品ラインナップを通じ、PCやモバイル端末に保存してある各種企業データや重要なデータの暗号化と保護を提供します。数々の受賞歴のあるチェック・ポイントのZoneAlarm Internet Security Suiteとその他のコンシューマ向けセキュリティ・ソリューションは、世界中で何百万にも及ぶお客様のPCをハッカー、スパイウェア、および情報窃盗から未然に保護しています。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、世界中のパートナー・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社の全社と何万ものあらゆる規模の企業や組織が含まれています。

©2003-2007 Check Point Software Technologies Ltd. All rights reserved.

Check Point, Application Intelligence, Check Point Express, Check Point Express CI, Check Pointのロゴ, AlertAdvisor, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, 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, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, 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, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, 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、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。

Best Practices for Deploying Intrusion Prevention Systems

P/N:502340-J 2007.03

*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.

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 Tel: 03 (5367) 2500