



製造業におけるIT環境と、 ミッション・クリティカルなネットワークの保護

安定性が最重視される環境に対するセキュリティの導入

Contents

本書の内容

| | |
|---|---|
| はじめに | 3 |
| 典型的なネットワーク・シナリオ | 4 |
| 製造施設における課題 | 5 |
| 信頼性とセキュリティ | 5 |
| コスト・パフォーマンスと管理性 | 6 |
| 製造環境に導入するセキュリティ・ソリューションに求められる機能要件 | 7 |
| 妥協のない高い信頼性 | 7 |
| 包括的なセキュリティ | 7 |
| 効率的で効果的な管理 | 8 |
| 幅広い互換性 | 9 |
| まとめ | 9 |

はじめに

世界では、さまざまな企業が製造施設を保有して、自動車や医療機器、化学製品、各種装置などの生産を行っています。現在こうした企業の多くが、自社のネットワーク環境を製造現場にまで拡張するようになっています。これにより、職人や技師、現場監督など、現場に携わるすべての関係者が、製造に関する重要な情報やアプリケーションにアクセスできるようになりました。またこのような拡張により、IP対応の工程管理のための機器などを接続できるようになり、製造工程をリモートから監視・制御することも可能になりました。

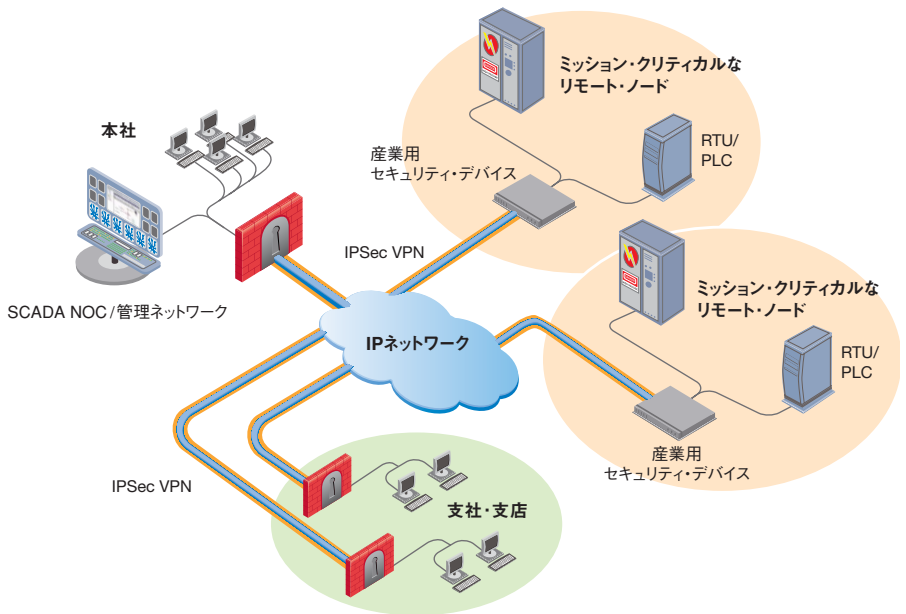
SCADA (Supervisory Control and Data Acquisition) システムや工程管理システムといった従来型の産業用コンピュータ・ネットワークは、最大限の信頼性を確保したうえで管理および制御の機能を提供できるように設計されていました。しかしながら、これらのシステムは、外部ネットワークまたは内部ネットワークから出現する最新のセキュリティ上の脅威に対処できるように設計されていないため、従来の産業用システムとIPベースのシステムを統合するにあたっては、各種要件の厳しい製造環境固有のニーズに対応可能な専用設計のネットワーク・セキュリティ・ソリューションを導入する必要があります。また、製造環境に導入するセキュリティ・ソリューションは、激しい温度変化やほこり、振動などに関する物理的な障害に耐えられる堅牢性を備えるだけでなく、さまざまな入力電圧やマウント方法に柔軟に対応できなければなりません。

製造施設へのコンピューティング環境の導入は慎重に行う必要があります。十分な注意を払わなかった場合、施設の運転が停止するリスクが高まるなど、有害無益の結果となるおそれもあります。このため、コンピューティング環境を製造施設に導入する際には、新しいタイプのセキュリティ・ソリューション、すなわち製造環境固有の要件を満たすソリューションを同時に導入する必要があるということを認識する必要があります。この技術白書では、以上のことに加えて、製造環境にネットワーク・セキュリティ・ソリューションを導入する際の課題と、それらのソリューションに求められる要件について説明します。

典型的なネットワーク・シナリオ

今日の製造業企業が直面しているセキュリティ上の課題を考察する前に、多くのネットワーク環境に共通する物理的なネットワーク構成を確認しておきます。製造業のネットワーク環境における一般的なネットワーク構成は、次に説明する2つのシナリオに大別できます。

1つ目のシナリオは、製造施設が、営業や物流、設計、管理といった諸部門の施設を含む複合施設の一部になっているケースです。このシナリオの場合、各施設にはインターネット/WAN回線などのネットワーク環境が存在するのが一般的です。



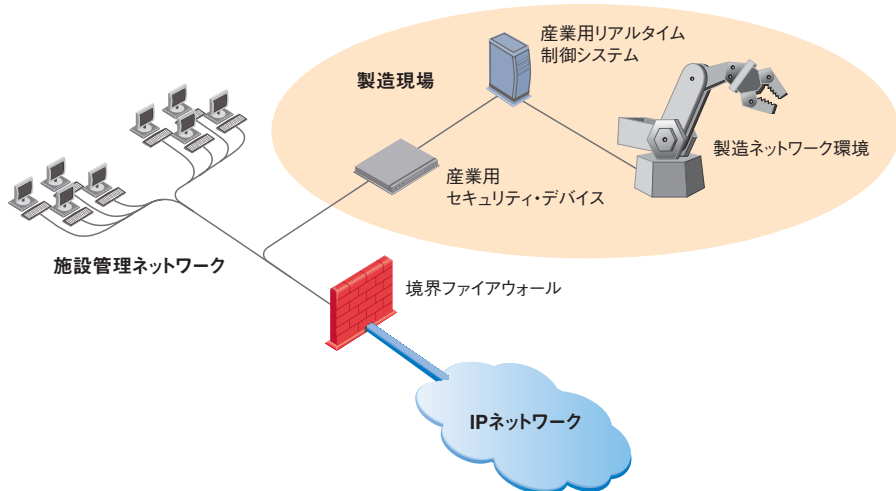
分散ネットワークにおける制御と監視

製造/組立施設のネットワークは、実質的に、コンピューティング・インフラストラクチャ全体の内部サブネットワークとなります。したがって、内部ネットワークおよび外部ネットワークより行われる攻撃から保護する必要があります。

対照的に、2つ目のシナリオでは、サイトは製造施設のみで構成され、それ以外の部門の施設は基本的には含まれません。したがって、コンピューティング・インフラストラクチャを構成する要素は最小限で、単一のネットワークに集約されています。サブネットは存在せず、1つのインターネット/WAN回線、いくつかのワークステーション、そして製造現場内部のネットワークがあるだけです。またIT担当者は常駐しておらず、ほとんどのデータおよびアプリケーションは地域データ・センターに置かれています。

このシナリオでは、実装および管理をリモートから容易に行うことのできる境界セキュリティ・ソリューションの導入が必要となります。

この2つのシナリオが示しているのは、同じ製造施設でも、ネットワーク構成が異なれば別のソリューションが必要になるということです。1つ目のシナリオでは、メインとなるネットワークに存在する脅威から製造施設のネットワークを保護する必要があります。したがって、ネットワーク間にファイアウォール、アンチウイルス、および侵入防御の機能を導入することが重要となります。一方、2つ目のシナリオでは、1つのデバイスがすべてのセキュリティ機能を担います。このデバイスは、先の境界セキュリティ機能に加えて、バーチャル・プライベート・ネットワーク (VPN) とWebフィルタリングの機能を備えている必要があります。こちらのシナリオでは、セキュリティ・デバイスをリモートから容易に実装および管理可能であることがより重要となります。



製造施設のためのネットワーク

製造施設用のセキュリティ・ソリューションは通常、さまざまなネットワーク構成をサポートしています。このため、施設ごとに異なるソリューションを導入するという高コストな方法を採用する必要がありません。

製造施設における課題

製造環境をネットワーク接続する企業がネットワーク・アーキテクチャの他に考慮する必要があるのは、100パーセントの信頼性を確保することと、内部および外部の脅威からネットワークを保護することです。これを実現するためには、堅牢なセキュリティと優れたコスト・パフォーマンス、高い管理性が不可欠となります。

信頼性とセキュリティ

職場環境の安全性維持を除けば、ほとんどの製造施設にとって最も重要なことは生産量を維持・拡大することになります。生産量が上がれば収益も増えるため、何よりもまず製造工程を停止させないことが優先されます。休止時間をゼロにすることが求められるのは、製造業だけでなく、他の産業も同様です。サービス・プロバイダの場合、生産量を最大化することはそれほど重要ではないかもしれませんが（例えば、トラフィック制御に生産性はあまり関係ありません）、サービスの可用性を100パーセント維持することが重要なのは同じです。

産業の種類を問わず、機器、特にコンピュータ・システムの信頼性は重要です。ミッション・クリティカルなネットワークの信頼性を高めるうえでポイントとなるのは、ネットワーク自体の堅牢性とセキュリティの高さです。システムは、過酷な製造環境に耐えられるだけでなく、その完全性と可用性を損なう可能性のあるサイバー攻撃からも保護されなければなりません。

例えば製造施設では、ネットワークを周囲から実質的に隔離して、マルウェアや不正ユーザが製造システムにアクセスできないようにする必要があります。脅威がネットワークにアクセスできる状態にあり、万が一セキュリティ上の問題が発生すると、物理的、金銭的に重大な被害が発生するおそれがあります。いったん製造工程が中断した場合、単に工程を再開すればそれで済むということは通常ありません。多くの場合、製造途中だった生産物は破棄することを余儀なくされ、また膨大な項目数のチェックリストを確認して、生産ライン全体を初期状態に戻さなければなりません。さらに、不正アクセスが発生した場合には、安全性に問題が生じたり、設備に甚大な不具合が発生したり、さらには生産品に微細な瑕疵が生じたりする可能性もあります。

しかし残念ながら、ネットワークに対する脅威からの実質的な隔離と保護を実現することは、次の理由により容易ではありません。

- **IPはオープンで普及した技術である**：これまで、SCADAなどの産業用システムでは、システムまたはベンダー独自の通信プロトコルを使用するのが一般的であり、その技術仕様が明らかでないことが一種のセキュリティとなっていました。しかし今日のほとんどのシステムは、オープン標準であるInternet Protocol (IP)を使用しており、以前よりも攻撃を受けやすい状況となっています。
- **密閉性の低下**：リアルタイムでの監視や制御が求められるようになったことから、製造現場がWANに接続されることが多くなってきています。
- **古い機器の使用**：産業用システムの多くは長年にわたって使用されており、旧型のオペレーティング・システムが稼働しています。このため、セキュリティ・ソフトウェアの導入やパッチの適用が困難です。
- **セキュリティを考慮した設計がなされていない**：産業用オートメーション/制御システムのほとんどはネットワーク・セキュリティを考慮した設計になっておらず、せいぜいアクセス制御機能程度の機能しか備えていません。

製造環境に導入するセキュリティ・ソリューションは、これらの課題を克服することに加えて、次の比較的新しいセキュリティ問題にも対処しなければなりません。

- **日進月歩で進化する脅威**：重要なインフラにサイバー・テロを仕掛けるため、あるいは金銭的利益を得るために、ハッカーは次々と新しい脅威を作り出しています。新たな脅威が登場するペースは年々加速しており、脆弱性の存在が明らかになってからそれを悪用する脅威が出現するまでの時間も非常に短くなっています。
- **潜在化する脅威**：複数の攻撃メカニズム、ペイロード、拡散手段を巧みに組み合わせる複合化が進んだことなどにより、脅威の存在が見えにくくなってきています。またその一方で、ネットワーク層の脆弱性を狙うのではなく、アプリケーション・サービスやアプリケーション・ロジック、データなどを悪用して攻撃を行う脅威も増加しています。
- **インターネットから内部ネットワークへの接続ニーズの増大**：ノートPCやPDAなどのモバイル・ソリューション、あるいは無線LANなどの導入が進み、従来型の境界セキュリティを迂回して内部ネットワーク環境に直接侵入する経路およびベクトルが増えたことにより、企業ネットワークが攻撃を受ける可能性はますます高まってきています。

これらのことからいえるのは、既知の脅威だけを対象とするセキュリティ対策では、もはや不十分であるということです。またセキュリティ・ソリューションは、多層セキュリティを提供することができなければなりません。つまり、受動的に脅威に対処する基本的なアンチウイルスおよびファイアウォール機能に加えて、複数の防御メカニズムを提供し、巧妙な脅威にも確実に対処できる包括的な防御態勢を築く必要があるのです。

コスト・パフォーマンスと管理性

製造施設において稼働の次に重要な課題は、コストを最小限に抑えるということです。コストの課題は、セキュリティにも影響します。IT/セキュリティ管理者の年間給与は平均8万5千ドルと、すべての拠点に管理者を配置することはできないほど高コストであるからです。これは特に、拠点が1箇所ではなく複数ある企業や、ネットワークがユーザ数5~25人程度の小規模なものである企業において特に深刻な問題となります。このことは、IT/セキュリティ・ソリューションを選定するにあたって考慮すべきいくつかのポイントを示しています。

まず、導入時に作業を担当するのは必然的に各拠点にいるスタッフになるということです。ほとんどの場合、これらのスタッフはネットワークやセキュリティについて特別な知識を有していません。したがって、導入が容易で、ポリシーが事前設定されているソリューションが望ましいということになります。

次に、運用管理をリモートから効率的に実施可能であることが必要になります。同時にリモート管理できるデバイスが1台のみというのでは、特定デバイスのトラブルシューティングといった特殊な状況を除いてあまり意味がありません。複数のデバイスをリモートから同時に管理することのできる包括的な集中管理機能が必要です。これは、複数の製造施設が分散配置されている企業には不可欠の機能です。

集中管理機能は、コスト削減の他にもいくつかの重要なメリットをもたらします。例えば、複数のデバイスの設定を統一することで、複数のデバイスの管理を手動で繰り返し行う中で発生しがちな設定ミスを少なくするといったことが可能になります。また、特定の設定を変更するのに要する時間も大幅に短縮することができます。これは、緊急に対策を講じる必要のある脅威が出現したというような場合に大きな効果を発揮します。素早く対策を講じることで、脆弱性が存在する時間をできる限り短くし、ポリシーや各種規制をより適切に遵守することが可能になります。さらに、イベントの管理や分析を複数のデバイスにまたがって行える、複数のデバイスのレポートを1つにまとめることができるといったメリットもあります。

最後のポイントは、複数のセキュリティ機能を備えたオールインワン型のセキュリティ・ソリューションが望ましいということです。オールインワン型のソリューションであれば、単一機能のデバイスを複数導入することによるハードウェア・コストおよび運用コストが増大するのを回避できます。

製造環境に導入するセキュリティ・ソリューションに求められる機能要件

製造施設のネットワーク環境を保護するための基本要件は、実際にはそれほど簡単に満たせるものではありません。特に、保護の対象となるのが製造現場に直結しているネットワークであることを考えると、「堅牢で耐久性があり、管理性とコスト・パフォーマンスに優れ、なおかつ過酷な製造環境においても高い信頼性を発揮する」という要件は極めてハードルの高いものであるといえます。したがって、どのようなソリューションであれば、この技術白書で説明されている課題に適切に対処できるのかを判断することが必要になります。この節では、課題をいくつかに分類し、製造環境で使用するセキュリティ・ソリューションの具体的な選定基準を示します。

妥協のない高い信頼性

製造環境の特性から、セキュリティ・デバイスには、堅牢性を考慮した機械設計になっていることが求められます。物理的な耐久性を高めるために、激しい温度/湿度変化や埃、振動に耐えうる産業仕様になっている必要があります。また、平均故障間隔 (MTBF) が長く、可動部品 (ファンやハードディスクなど) の数が最小限であることも重要になります。

物理的な信頼性だけでなく、ネットワークの観点から見た信頼性も重要です。したがって、次の高可用性機能および冗長機能をサポートしていることが求められます。

- セカンダリ・デバイスへのアクティブ/アクティブまたはアクティブ/パッシブのフェイルオーバー
- メインで利用するWANアクセスがダウンした場合に別の通信経路を確立するためのダイナミック・ルーティング、ダイヤルアップ・バックアップ、冗長WANインタフェース

包括的なセキュリティ

脅威が至るところに存在すること、および製造現場やミッション・クリティカルな分散ネットワークがビジネスにとって極めて重要な存在であることを考慮すると、包括的なセキュリティ機能を備えたソリューションを選択することが必要になります。すべてのセキュリティ機能が単一のデバイスで提供されることが望ましいのはいうまでもありませんが、そのためにクオリティが犠牲になっては意味がありません。各セキュリティ機能は、それぞれのカテゴリで最高レベルのものである必要があります。また、複数の機能が同時に動作している場合や、マルウェアやポリシー違反を含むトラフィックを処理する際に、デバイスのスループットが低下するようなこともあってはなりません。以上のことを踏まえると、次のセキュリティ機能を搭載していることが必要になります。

- **マルチレイヤに対応するステートフル・インスペクション・ファイアウォール**: 攻撃を含むトラフィックをブロックするには、ネットワーク/トランスポート層でアドレス、ポート、およびプロトコルに基づくアクセス制御を行うだけでは不十分です。今日のファイアウォールには、プロトコルを認識してアプリケーション層を検査する機能(例えば、Webアプリケーションにおける特定のやり取りを認識する機能)がもはや不可欠となっています。また、トラフィックを深いレベルで検査するだけでなく、インターネットで使用されている幅広いプロトコルに対応していることも重要です。例えば、インスタント・メッセージやVoIP、Webサービスといったポピュラーなアプリケーションで使用されているプロトコルに対応している必要があります。
- **明示的な攻撃防御**: ホワइटリストに基づいて機能するファイアウォールは非常に効果的ではありますが、当然のことながら一部のトラフィックはファイアウォールを通過します。最善の対策を施すには、通過したトラフィックをさらに検査して、悪意あるコンテンツが含まれていないかどうかを確認する必要があります。これは、明示的な攻撃防御あるいは侵入検出/侵入防御と呼ばれ、産業用セキュリティ・デバイスに最適な機能です。また、類似の機能として、分散サービス妨害(DDoS)攻撃をブロックする機能も備えている必要があります。
- **高度なコンテンツ・フィルタリング**: インターネットに直接アクセスすることのできる製造施設では、ゲートウェイ・ベースのアンチウイルス/アンチスパイウェア機能も必須といえます。これらの機能は、ワームの拡散を防ぐだけでなく、機密情報の漏洩を防止するためにも重要です。インターネットに直接アクセスできない環境の場合、この機能は必ずしも必要ではありませんが、多層防御戦略の強化に役立つという意味では有効であるため、少なくともオプションとして必要ときに導入できるよう拡張性を備えている必要があります。
- **VPN**: セキュリティ・ソリューションでは、不正アクセスを防止しつつ、管理者がリモートから安全にネットワークの管理および監視を行えるようにする必要があります。そのため、IPSecなど標準のプロトコルを採用したVPN機能を備え、標準の暗号化アルゴリズム(3DESまたはAES)と認証メカニズム(RADIUSやX.509証明書など)をサポートしていることが理想となります。

効率的で効果的な管理

優れた管理機能が用意されていなければ、包括的なセキュリティ機能を有効に活用することはできません。その場合、管理業務が複雑化し、設定の一貫性を保つことが困難になり、結果として組織のセキュリティに隙が生まれて、重要な製造設備がさまざまな脅威にさらされることになります。また、必要以上の複雑さは、運用コストにも大きく影響します。したがって、少なくとも集中管理はサポートされていなければならないということになります。ただし、それだけでは十分ではありません。使いやすさも重要なポイントです。効率的かつ効果的にセキュリティ管理を行うためには、直感的に操作できる洗練されたインターフェースが必要になります。また集中管理ソリューションは、次のことにも対応していなければなりません。

- **リアルタイムの監視とトラブルシューティング**: 各デバイスのステータスを個々に、あるいはまとめて確認できる必要があります。またアラートは、電子メール、テキスト・メッセージ、管理コンソール、SNMPコンソールなど、さまざまな形態で受信できる必要があります。
- **包括的なログおよびレポート**: セキュリティ・デバイスは、幅広い事前定義済みレポートとカスタム・レポートによるレポート作成の柔軟性と、詳細なログを生成できることが理想です。これらのレポートは、定期的に、または必要に応じて生成できる必要があります。
- **ローカル用とリモート用の管理インターフェース**: 単一のセキュリティ・デバイスをオンサイトとリモートの両方で完全に管理できる必要があります。また、プライマリ接続が失われた場合でもデバイスを管理できるように、あるいはサービス・プロバイダの管理システムからも管理できるように、バックアップ回線経由でアクセスが可能な管理インターフェース(Webインターフェースまたはシリアル・ポート経由のCLI)を備えている必要があります。さらに、単一の画面からマウス操作だけでネットワーク全体を管理できることも重要です。
- **統合管理ソリューション**: 製造現場ネットワークと通常の企業ネットワークの両方でセキュリティ・デバイスを使用する場合、使用する管理ツールと管理方法は、デバイスの設置場所や管理を行う場所(リモートまたはローカル)に関係なく、共通のものでなければなりません。
- **ソフトウェアとシグネチャのアップデート**: ハードウェア自体を入れ替えることなく、ソフトウェアをアップグレードすることのできるアーキテクチャが採用されている必要があります。またアップデートは、自動配信だけでなく手動でも配信できる必要があります。

幅広い互換性

最後の機能要件は互換性です。互換性についても、十分な考慮が必要になります。製造施設向けのセキュリティ・ソリューションは、既存のインフラストラクチャに変更を加えることなく、あらゆる論理的・物理的構成のネットワークにも導入できなければなりません。

ネットワークの観点からすると、これは、複数の導入モード（ブリッジ・モードや完全なルーティング・モードなど）に対応し、VLANベースのデバイスのように既存のトラフィック・セグメンテーション・スキームを維持できる必要があるということを意味します。

物理的な観点では、製造現場で一般的なあらゆるマウント方法（DINレール、ラック・マウント、ウォール・マウントなど）に柔軟に対応し、設置スペースに制約のあるエンクロージャにコンパクトに収納できる必要があるということです。また、幅広い電圧と直流および交流の両方に対応する電源を備えていることも重要になります。

まとめ

今日、製造/組立施設など重要性の高い産業施設を保有する企業の多くが、ビジネス上のさまざまな理由により、自社のネットワーク環境を製造現場にまで拡張するようになっています。その結果、高レベルでのネットワーク・アーキテクチャに関係なく、ビジネスにとって重要性の高いインフラストラクチャは、ネットワーク接続されたコンピューティング・システムに対するさまざまな脅威（ウイルス、ワーム、サービス妨害攻撃など）の影響を受けやすい状態となっています。このため、最高レベルのセキュリティ機能を用いて対策を施すことが必須となっています。こうした環境に導入するセキュリティ・ソリューションは、製造施設固有の考え方や物理的環境を考慮に入れたものであることが理想的です。さらにこれらのソリューションが提供する機能は、高い効率性とコスト・パフォーマンスを実現するものでなければならず、またこのような環境で利用されるソリューションは、製造施設固有の過酷な環境に耐えることのできる堅牢なハードウェア設計になっている必要があります。

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。

Protecting Industrial IT Environments and Mission Critical Networks

P/N:502473-J 2007.05

※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