



Check Point®

SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



White Paper

安全なリモート・アクセス環境の構築

あらゆるリモート・アクセス環境に最適なセキュリティ機能と
管理機能を統合したチェック・ポイントのソリューション



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

はじめに	3
ビジネス環境の分散傾向とテレワーカーの増加	3
リモート・アクセス環境を安全に	3
統合されたセキュリティであらゆるリモート・アクセス環境から情報にアクセス	4
多様なリモート・アクセス・ユーザへの対応	4
エンドポイント・セキュリティの統合	5
侵入防御機能の統合	5
リモート・アクセス管理機能の統合	6
リモート・アクセス、エンドポイント・セキュリティ、 侵入防御統一管理を統合するチェック・ポイントのアプローチ	6
高度なセキュリティと柔軟性を備えたチェック・ポイントのソリューション	7
まとめ	11
付録：安全なリモート・アクセスを実現するチェック・ポイントのソリューション	12

概要

多くの企業では、分散した業務形態の環境において、リモート・アクセスを利用した企業ネットワークへのアクセスを許可しています。このような、リモート・アクセスを利用して仕事を行う社員（テレワーカー）のリモート・アクセスに対する要求はさまざまです。時折自宅から企業ネットワークにアクセスできればよいというケースもあれば、毎回異なるさまざまな場所から接続する必要があるというケースもありますが、特に後者の「毎回異なるさまざまな場所から接続する」ケースは、無線LANが普及したことを主な理由として特に増加傾向にあります。さらに、携帯電話などPC以外のデバイスを利用してリモート・アクセスを行い、昼夜やアクセスする場所を問わずに常時接続を行うケースもあります。こうした状況を受けて、社内情報の機密性、完全性、および可用性の重要性も増してきています。そのため企業は、リモート・アクセス・ソリューションを導入する一方で、社内情報リソースを保護・管理するための統一された手段を必要としています。

はじめに

リモート・アクセスを行なうリモート・ユーザ（テレワーカー）に対し、社内情報リソースに簡単にアクセスできる手段を安全に提供することは、多くの企業が抱える課題です。この課題の解決が特に難しいのは、リモート・アクセスを行なうユーザが、空港などのインターネット・キオスクやWi-Fiホットスポット、さらには知人のコンピュータなど、最近増えている一時的な作業環境を含め、社外のあらゆる場所からリモート・アクセスを行う可能性があるからです。リモート・アクセス環境が特定できない場合には、そうした場所から社内情報リソースへ攻撃が行われる可能性についても考慮することが必要になります。すなわち、どこからでもリモート・アクセスを行える利便性を提供しつつ、すべてのリモート・アクセス環境で安全に利用できるセキュリティを提供することが課題となっています。現在、米国および西欧諸国において、安全なリモート・アクセスの手段を必要としているテレワーカーの数は8,200万人にも上ります。安全なリモート・アクセス手段に対するニーズは、テレワーカーの数が増加するにつれてさらに増大すると予想されます。この問題を解決するためには、エンドポイントがネットワーク・アクセスを行なうネットワーク環境の種類を問わず、あらゆるテレワーカーに対応できるだけの柔軟性とセキュリティ性を兼ね備えた、安全なリモート・アクセス・ソリューションが必要です。この技術白書では、セキュリティ機能と管理機能が統合された安全な環境を実現する方法について解説します。

ビジネス環境の分散傾向とテレワーカーの増加

最近の調査によれば、週に1日以上オフィス以外の場所で仕事をするという人は、米国および西欧諸国では8,220万人にも上ります。2005年のAmerican Interactive Consumer Survey (AICS) では、米国在住者のうち週に1日以上自宅で仕事をするのは4,510万人、最近のGartner Groupの調査では、西欧諸国における2005年のテレワーカーの数は3,700万人とされています。この数字以上に興味深いのは、これらのテレワーカーがリモート・アクセスを行っている場所です。これらの調査では、2,430万人が外出先の顧客企業から、1,630万人が休暇中に、そして1,510万人が屋外からと回答しています。また一般的なテレワーカーがリモート・アクセスを行う場所の数は、平均3.4箇所となっています（AICSの調査結果より）。

リモート・アクセス環境を安全に

このようにリモート・アクセス・ユーザが増加していることは、それ自体興味深いことである一方、企業のセキュリティや、そうしたユーザにどの範囲までアクセスを許可するかという問題に直接的な影響を及ぼします。実際、テレワーカーが増加し、リモート・アクセス環境が一様ではなくなったことによって、リモート・アクセスを行うエンドポイントの種類が多様化してきています。例えば、自社やパートナー企業の従業員は、企業の管理下にあるPCからだけでなく、自宅のPCからも社内データにアクセスするようになってきました。また出張中や休暇中には、インターネット・キオスクや知人のPCなどからアクセスすることもあります。PC以外にも、PDAや携帯電話が使用されることもあるでしょう。こうしたデバイスのセキュリティ・レベルは、最新のパッチやセキュリティ・ソフトウェアがすべて適用されたPCから、全くセキュリティ対策が施されていない研究用PCまでさまざまです。このように、リモート・アクセスするエンドポイントの種類が多様化するということは、機密性の高い企業情報を保護する必要のある状況がますます増加することを意味します。

以前は、社外にいる従業員が社内の情報にリモート・アクセスする場合、VPNクライアント・ソフトウェアがインストールされた、企業の管理下にあるPCを利用するのが一般的でした。そのため、これらのPCとその中の情報は、VPNクライアント・ソフトウェアにバンドルされているパーソナル・ファイアウォールとポリシー検証ソフトウェアによって保護されていました。しかし現在では、リモート・アクセスの手段はクライアントPCにエージェント・ソフトをインストールする必要が無いクライアント・レスのSSL VPNが主流となっており、IT管理者はエンドポイントを直接管理することができず、またパーソナル・ファイアウォールなどのセキュリティ・ソフトウェアがインストールされていない可能性もあり、エンドポイントのセキュリティが低下してしまっています。事態をさらに深刻にしているのは、SSL VPNが普及し始めた時期が、キー・ストローク・ロガーやトロイの木馬、クライムウェアなどのスパイウェアが急増した時期と重なっていたことです(クライムウェアとはスパイウェアの新しいカテゴリで、Wikipediaでは「金融犯罪を自動で行うことを目的とする、単独または一連のコンピュータ・プログラム」と定義されています)。一般的に、この種のスパイウェアはいずれも企業の機密情報に対する脅威となります。特に、サイバー犯罪者はクライムウェアを使用して特定の企業を標的とし、システムのパスワードや、テレワーカーがリモート・エンドポイントにダウンロードした情報を盗み出そうとします。

統合されたセキュリティであらゆるリモート・アクセス環境から情報にアクセス

リモート・アクセスの安全性に関する問題の解決策を検討するにあたっては、実装に関係する複数の要素を考慮する必要があります。どのような解決策であっても、(1) 最低限、リモート・アクセス・ユーザがさまざまな環境から社内の情報にアクセスできる、(2) 情報の機密性を保護するためのエンドポイント・セキュリティ制御機能が統合されている、(3) 攻撃者やマルウェアの侵入に対してシステムの完全性を維持することができる、(4) 企業全体の管理ポリシーおよび管理プロセスに組み込むことができる、という4つの条件を満たすものでなければなりません。

多様なリモート・アクセス・ユーザへの対応

単独であらゆる要件を満たすことのできるリモート・アクセス技術は存在しません。どの技術が最適であるかは、リモート・アクセスの方法やパフォーマンス要件、組織の規模によって異なります。したがって、リモート・アクセス環境の基盤となる技術は、分散しているビジネス環境におけるアクセス要件に最適なものを選択することが重要です。リモート・アクセス技術には、次のような種類があります。

- サイト間IPSec VPN：オフィス間接続、およびオフィスへのリモート・アクセスを行う場合に適しています。リモート・ユーザは、メイン・オフィス(本社など)にいるのと全く同じようにネットワーク内のリソースにアクセスできます。
- リモート・アクセスIPSec VPN：ユーザが、企業の管理下にあるPCからネットワーク内のリソースにアクセスする場合に最適です。幅広いアプリケーションがサポートされるため、オフィス内にいるような感覚のリモート・アクセスが提供されます。
- リモート・アクセスSSL VPN：ユーザが、ネットワーク内のリソースに常時アクセスする必要はない場合、または自宅のPCなどネットワーク管理者の管理権限外のPCからアクセスする場合に適しています。ほとんどの一般的なビジネス・アプリケーションから、特別な設定なしでリモート・アクセスすることができます。またエクストラネット・アクセスにも最適です。

エンドポイント・セキュリティの統合

リモート・アクセス・ソリューションを選定する際は、情報の機密性を保護するエンドポイント・セキュリティ機能の利用を検討することが非常に重要です。安全なリモート・アクセス・ソリューションの実現には、エンドポイント・セキュリティ機能が統合されている必要があります。ソリューションに十分なエンドポイント・セキュリティ機能が備わっている場合、リモート・アクセス技術の種類を問わず、次のことが可能になります。

●**ポリシーの実施：** リモート・アクセスVPNでは、リモート・アクセス・ポリシーを実施する際、エンドポイントの状態を検査し、その結果情報を利用できる必要があります。これにより、エンドポイントの信頼レベルに基づいて、許可するアクセス・レベルを決定することが可能になります。ポリシー実施機能では、アンチウイルスやファイアウォールなどのセキュリティ・ソフトウェアがエンドポイントにインストールされ、正しく実施されているかを確認できることが必要です。IPSec VPNとSSL VPNでは、次の方法でこの機能を実現することができます。

- クライアント・ベースのIPSec VPN：VPNパッケージの一部としてエンドポイント・セキュリティ機能を提供し、パーソナル・ファイアウォールを提供します。あるいは、パーソナル・ファイアウォールがインストールされているかどうかを確認し、設定を検証します。
- クライアントレスのSSL VPN：オンデマンドのActiveXコントロールまたはJavaコントロールを使用してエンドポイント・セキュリティ機能を提供し、ホスト・チェック機能（後述）およびスパイウェア検出機能を提供します。

●**ゲスト・コンピュータのセキュリティ：** これは、SSL VPNにおいて特に懸念される点であり、エンドポイントのセキュリティを維持するために特別な対策が必要になります。リモート・アクセス・ソリューションでは、ユーザが共用PCを使用している場合でも安全に情報にアクセスできるようにすると共に、セッション終了時にPC上の情報を明示的に消去する必要があります。具体的なアプローチとしては、主に次の3つがあります。

- マルウェアのチェック：悪意あるソフトウェア（キーロガー、トロイの木馬、クライムウェアなど）がPCにインストールされていないかどうかを確認します。
- セッションの暗号化：ハード・ディスク上のセッション情報を暗号化することで、共有PCを使い終わった後、あるいはPCが盗まれるなどした場合に、PC上に残された機密情報が他人に読み取られないようにします。
- キャッシュの消去：SSL VPNのセキュリティにとって、キャッシュの消去は非常に重要なことです。ただし、これによってすべてのキャッシュ・データが消去され、すべてのキャッシュ・ディレクトリが空になると保証されるわけではありません。セキュリティを最大限に高めるには、暗号化と併用する必要があります。

●**リアルタイムのセキュリティ：** エンドポイントを最新の脅威から保護するために、新しいセキュリティ対策が公開され次第、新しいマルウェア定義ファイルをエンドポイントに適用します。

侵入防御機能の統合

エンドポイント・セキュリティと同じように重要なのが、リモート・アクセス・ポイント経由でネットワークに侵入する可能性のある悪意あるソフトウェアから、情報システムの完全性を守る事です。侵入防御機能が統合されているリモート・アクセス・ソリューションでは、プロアクティブ（事前対応的）なセキュリティ対策を実施することができます。こうしたセキュリティ・ソリューションは、悪意ある攻撃がネットワークに侵入しようとする試みを受動的に受け止めるのではなく、これらの攻撃がVPN経由で侵入しようとする試みを能動的にブロックします。このような防御を可能にするためには、リモート・アクセス・ソリューションで、悪意あるソフトウェアや攻撃がアプリケーション層またはネットワーク・レベルのトンネリングを介してリモート・エンドポイントから侵入してこないように対策を行う必要性があります。また、最新の脅威に対応したセキュリティ・アップデートや新しい防御機能がリアルタイムでリモート・アクセス・ソリューションに提供されることも必要です。

リモート・アクセス管理機能の統合

SSL VPNの統合セキュリティ機能において最も重要性が高いと考えられるのは、リモート・アクセス・ソリューションの管理機能です。リモート・アクセス・ソリューションに一貫性のある管理システムが用意されていれば、管理機能を最大限に活用すると共に、運用の負担を最小限に抑えることが可能になります。一貫性のある管理システムでは、次のことが可能になります。

- 設定方法および保守の統一化：多くの企業では、全体的なポリシーおよびリスク管理に関するセキュリティ・ポリシーを策定していますが、優れたリモート・アクセス・ソリューションは、これらのポリシーを系統的に実施可能なポリシーへ簡単に定義することのできる機能を備えています。このような機能が用意されていない場合、個々のシステムを個別に管理しなければならない、設定漏れや設定ミスが生じる可能性が高くなるほか、システム全体の構成を把握することが困難になります。しかし、複数のリモート・アクセス・ソリューションの設定と保守を統一的行うインフラストラクチャが用意されていれば、ソリューション全体の一貫性を保ち、その設定を確実に把握することが可能になります。さらに、システムの導入と保守に要する時間も短縮されます。
- 統一されたレポートングおよび監査：リモート・アクセス・ソリューションの運用状況およびイベントの監査履歴を残しておくことは、セキュリティ対策として推奨されることであり、またいくつかの法規制で規定されていることでもあります。これには、セキュリティ上の脅威を把握するために必要な重要情報を確保できる、キャパシティおよびパフォーマンス・プランニングに役立つ、という2つのメリットがあります。優れたリモート・アクセス・ソリューションでは、システム全体のデータを収集および保存を行うことが可能で、またシステムの状態を継続的に監視することのできるレポートング・インフラストラクチャが提供されます。
- セキュリティ分析の統合：ネットワーク型の攻撃は複雑さを増す一方であり、複数の脅威を組み合わせた攻撃も増えてきています。ハッカーはリモート・アクセス・ソリューションを区別して攻撃することはしませんが、セキュリティ・ソリューションの側でも製品ごとに区別して分析を行うべきではありません。リモート・アクセス・ソリューションでは、すべての製品およびソリューションにまたがってセキュリティ・イベントを相関分析し、攻撃の可能性を持ったイベントを素早く特定することが必要です。例えば、異なるロケーションからIPSec VPNとSSL VPNにログインしようとしているユーザを検出することができれば、不正なログイン行為を見つけやすくなります。

リモート・アクセス、エンドポイント・セキュリティ、侵入防御、統一管理を統合するチェック・ポイントのアプローチ

ここまで、安全なリモート・アクセス・ソリューションに求められる各種の条件について説明してきました。これ以降は、それらの条件をクリアするための具体的な手段について説明します。業界で最大規模の独立系セキュリティ・ベンダーであるチェック・ポイントは、セキュリティを専業とし、顧客が必要とするセキュリティを顧客が望む方法で実現するさまざまな製品を提供しています。

チェック・ポイントのリモート・アクセス・ソリューション製品群は、IPSec、SSL/TLS、L2TPなど幅広い技術をサポートしています。これらのリモート・アクセス・ソリューションは、サイト間VPNおよびリモート・アクセスIPSec/SSL VPNのアクセス管理に対応しており(この機能は、チェック・ポイントのすべてのVPN製品に中心的機能として搭載されています)、リモート・ユーザに対する権限付与とそのアクセス権を制限、制御、および管理することができます。通信時におけるセキュリティは、VPN-1®、Connectra™、およびSSL Network Extender™が提供します。強力な認証ソリューションが必要な場合は、チェック・ポイントのOPSECパートナーが提供する各種製品を使用することにより、リモート・アクセス環境を問わず、誰が社内の情報にアクセスしているのかを把握することが可能になります。

エンドポイント・セキュリティを統合するための製品としては、すべてのリモート・アクセスVPN製品に対するオプションとして、Integrity™ SecureClient™ (クライアント・ベースのVPN用) と Integrity Clientless Security™ (ブラウザ・ベースのVPN用) が用意されています。このオプションを使用することで、リモート・アクセス環境で使用されるさまざまな形態のエンドポイントのセキュリティと機密性を管理し、悪意あるソフトウェアから組織を保護することが可能になります。エンドポイント・セキュリティとして提供される機能には、パーソナル・ファイアウォール、アンチウイルス、アプリケーション制御、およびアンチスパイウェアがあります。IPSec VPNクライアントでは、これらすべてが提供されます。クライアントレスSSL VPNでは、スパイウェア検出機能とエンドポイントのポリシー・チェック機能も提供されます。これにより、多様なエンドポイントに対応しながら、それらのセキュリティを維持することが可能になります。

侵入防御機能の統合に関しては、各ソリューション製品に統合可能なオプションとして、Application Intelligence™技術とWeb Intelligence™技術が提供されています。これらの技術は、リモート・アクセス技術で接続されている各システムの完全性を保護します。これらのオプションとリモート・アクセス・ソリューションを組み合わせると、VPNにおいて、先進の侵入検知および侵入防御の機能を利用できるようになります。これにより、ネットワーク・レベルまたはアプリケーション・レベルの攻撃がVPN経由でネットワークに侵入されることをブロックします。

集中管理による統一された管理環境を実現する製品としては、一つの管理コンソールからリモート・アクセス・インフラストラクチャのポリシー管理を一元的に行うためのSmartCenter™製品群が用意されています。チェック・ポイントは、この分野では業界のリーダー的存在であり、継続的な技術革新に取り組んでいます。SmartCenterは、サイト間IPSec VPN環境からエンドユーザのSSL VPN環境に至るまで、さまざまなリモート・アクセス環境を包括的にサポートすると同時に、ポリシーの一貫性を強化することで矛盾の無いセキュリティの実施、セキュリティ・レベルの向上、そしてセキュリティ管理コストの低減を両立します。チェック・ポイントの管理ソリューションのひとつである、Eventia™ Reporter™は、VPNソリューションのログを統合し分析します。Eventia ReporterをEventia Analyzer™と組み合わせると、複数のベンダーの製品にまたがるセキュリティの監査とイベントの相関分析、およびインシデント処理の支援を行うことが可能になります。これらの製品を組み合わせることで、シンプルでシームレスな管理環境が実現されます。

高度なセキュリティと柔軟性を備えたチェック・ポイントのソリューション

チェック・ポイントは、社内の情報を外部から安全に利用できるようにしたいというお客様の多様なニーズを満たすための、さまざまなリモート・アクセス・ソリューションを提供しています。以下の表の「リモート・アクセスのタイプ」欄より、お客様の環境に最も近いものをお選びください。「チェック・ポイントのソリューション」欄で、選択した環境に最も適したチェック・ポイントのソリューションをご確認いただけます。

リモート・アクセスのタイプ	接続に関する要件	セキュリティ上の課題	チェック・ポイントのソリューション
本社などの主要なオフィス	広帯域幅での接続、多様なアプリケーション、多数のサブネットワークから多数のユーザが接続	インターネットを経由する通信のセキュリティ ネットワーク全体にまたがるアクセス制御 可用性の保証 完全なネットワーク保護	チェック・ポイントのサイト間IPSec VPN対応製品 ・ VPN-1 UTM™ ・ VPN-1 Power™

リモート・アクセスのタイプ	接続に関する要件	セキュリティ上の課題	チェック・ポイントのソリューション
支社・支店などの ブランチ・オフィス環境	中～広帯域幅での接続、 多様なアプリケーション、 数人のユーザ／数箇所の サブネット、場合によっては 本社あるいは他の支社・ 支店とフルメッシュ接続	インターネットを経由する 通信のセキュリティ 組織全体にまたがるアク セス制御 可用性の保証 支社・支店経由でコア・ ネットワークに侵入するワ ームからの完全なネットワー ク保護	チェック・ポイントのサイト 間IPSec VPN対応製品 ・ VPN-1 UTM™ ・ VPN-1 UTM Edge™
テレワーカー、在宅勤務 (常時接続)	ある程度の帯域幅での接 続、主要なネットワーク・ アプリケーション、個人 ユーザまたは小規模LAN	インターネットを経由する 通信のセキュリティ 組織全体にまたがるアク セス制御 可用性の保証 リモート・エンドポイント 経由でコア・ネットワーク に侵入するワームからの 完全なネットワーク保護 エンドポイント・セキュリ ティ(企業の管理下にある PCのワームおよびマルウェア への感染防止 ワームおよびマルウェアの コア・ネットワークへの侵入 防御)	チェック・ポイントのサイト間 IPSec VPN対応製品 ・ VPN-1 UTM Edge™ チェック・ポイントのリモート・ アクセス対応製品 ・ IPSec VPN™ ・ Integrity SecureClient

リモート・アクセスのタイプ	接続に関する要件	セキュリティ上の課題	チェック・ポイントのソリューション
営業担当者など	不定期のアクセス、さまざまな帯域幅での接続、少数のアプリケーション、多数のネットワーク・アクセス・オプション	<p>インターネットを経由する通信のセキュリティ</p> <p>組織全体にまたがるアクセス制御</p> <p>可用性の保証、リモート・エンドポイント経由でコア・ネットワークに侵入するワームからの完全なネットワーク保護</p> <p>エンドポイント・セキュリティ (企業の管理下にあるPCのワームおよびマルウェアへの感染防止)</p> <p>ワームおよびマルウェアのコア・ネットワークへの侵入防御)</p>	<p>チェック・ポイントのリモート・アクセスIPSec VPN対応製品</p> <ul style="list-style-type: none"> • Integrity SecureClient <p>チェック・ポイントのリモート・アクセスSSL VPN対応製品</p> <ul style="list-style-type: none"> • Connectra • SSL Network Extender for VPN-1
テレワーカー (一時的)	不定期のアクセス、さまざまな帯域幅での接続、少数のアプリケーション、自宅からのネットワーク・アクセス	<p>インターネットを経由する通信のセキュリティ</p> <p>組織全体にまたがるアクセス制御</p> <p>可用性の保証</p> <p>リモート・エンドポイント経由でコア・ネットワークに侵入するワームの完全なネットワーク保護</p> <p>エンドポイント・セキュリティ (企業の管理下にあるPCのワームおよびマルウェアへの感染防止)</p> <p>ワームおよびマルウェアのコア・ネットワークへの侵入防御)</p>	<p>チェック・ポイントのリモート・アクセスSSL VPN対応製品</p> <ul style="list-style-type: none"> • Connectra™ • SSL Network Extender™ for VPN-1

リモート・アクセスのタイプ	接続に関する要件	セキュリティ上の課題	チェック・ポイントのソリューション
週末、勤務時間後のみの使用	まれに使用、自宅から電子メール／ファイル／イントラネットに短時間アクセス	<p>インターネットを経由する通信のセキュリティ</p> <p>組織全体にまたがるアクセス制御</p> <p>可用性の保証</p> <p>リモート・エンドポイント経由でコア・ネットワークに侵入するワームからの完全なネットワーク保護</p> <p>マルウェアがインストールされていないか／企業のセキュリティ要件を満たしているかをログイン前にエンドポイントで検査 (NAC)</p> <p>機密性の保護</p>	<p>チェック・ポイントのリモート・アクセスSSL VPN対応製品</p> <ul style="list-style-type: none"> • Connectra
エクストラネット・パートナー (パートナー企業)	帯域幅に関する要件はさまざま、ソフトウェアのインストールに関する知識は組織によってさまざま	<p>インターネットを経由する通信のセキュリティ</p> <p>組織全体にまたがるアクセス制御</p> <p>可用性の保証</p> <p>リモート・エンドポイント経由でコア・ネットワークに侵入するワームからの完全なネットワーク保護</p> <p>マルウェアがインストールされていないか／企業のセキュリティ要件を満たしているかをログイン前にエンドポイントで検査 (NAC)</p> <p>機密性の保護</p>	<p>チェック・ポイントのリモート・アクセスSSL VPN対応製品</p> <ul style="list-style-type: none"> • Connectra <p>チェック・ポイントのサイト間IPSec VPN対応製品</p> <ul style="list-style-type: none"> • VPN-1 UTM™ • VPN-1 UTM Edge™

まとめ

オフィス環境やネットワーク環境が分散している企業は、ユーザが必要なときに必要な場所から安全に社内のネットワーク・リソースにアクセスすることができる柔軟なリモート・アクセス・ソリューションを必要としています。このリモート・アクセス・ソリューションには、情報の機密性を確実に保護することが可能なセキュリティ機能が備わっている必要があります。また、その管理および監査のためのインフラストラクチャは、企業の業務形態に適したものであることが求められます。リモート・アクセスの安全性に関する問題を解決するためのソリューションに必要なのは、エンドポイント・セキュリティ、侵入防御、および管理の各機能が統合され、ポリシーの管理とリモート・アクセスの監査および分析が効率的に実行可能であることです。つまり組織には、情報、システム、およびユーザに対して包括的なセキュリティを提供し、あらゆるユーザのリモート・アクセス権限を集中管理することのできるリモート・アクセス・ソリューションが必要であるということです。チェック・ポイントのソリューションは、これらすべてを実現することを念頭において開発されています。チェック・ポイントが提供するプラットフォームとリモート・アクセスVPN技術は、リモートアクセスを必要とするネットワーク環境における各企業固有のニーズを満たします。

付録：安全なリモート・アクセスを実現するチェック・ポイントのソリューション

サイト間IPSec VPN

VPN-1 UTM

限られたリソースで、増え続ける一方のセキュリティ上の脅威に対処するために、最高レベルのセキュリティを提供するシンプルなオールインワン・ソリューションが求められています。VPN-1 UTMは、あらゆる規模の企業に対応するスケーラビリティを備えた統合脅威管理ソリューションです。実績ある各種のセキュリティ機能を単一のソリューションとして提供することにより、高度なセキュリティを容易に導入することを可能にします。VPN-1 UTMでは、ファイアウォール、侵入防御、アンチウイルス、アンチスパイウェア、Webアプリケーション・ファイアウォール、IPSec VPNおよびSSL VPNの各機能が、容易に管理可能な1つのソリューションに完全に統合されています。

VPN-1 Power

インターネットには、企業のネットワーク・リソースに対する、常に変化し続ける脅威が潜んでいます。ハッカーたちは、企業アプリケーションを攻撃するために、常に新たな方法を模索しています。同時に、企業アプリケーションに対する要件は複雑化する一方であり、特にパフォーマンスについては厳しい要件が課せられるようになっていきます。インターネットを最大限に活用するためには、ミッション・クリティカルなアプリケーションが抱える可用性、パフォーマンス、スケーラビリティの課題に対応しながら、ビジネス・コミュニケーションの機密性と社内ネットワーク・リソースの安全性を確実に維持できるようにする必要があります。VPN-1 Powerは、ファイアウォール、VPN、および侵入防御の各技術が緊密に統合されたゲートウェイであり、企業で利用するアプリケーションおよびネットワーク・リソースに対する包括的で高パフォーマンスなセキュリティ機能と安全なリモート接続機能を提供します。VPN-1 Powerでは、業界で最もインテリジェントなセキュリティ検査技術であるステートフル・インスペクションとApplication Intelligenceがさらに強化されており、ネットワークの通信速度を犠牲にすることなく、ネットワーク層への攻撃とアプリケーション層への攻撃の両方を事前対応的にブロックすることが可能になっています。

VPN-1 UTM Edge

今日の企業は、インターネットを利用して支社・支店などのリモート・オフィスを接続し、アプリケーションや情報などの企業リソースを共有できるようにしています。このため企業では、数十台、数百台、場合によっては数千台ものVPNゲートウェイを、限られたITスタッフで効率的に導入および管理する必要に迫られています。こうした企業には、既存のインフラストラクチャと緊密に統合することができ、複雑化する一方のインターネット上の攻撃に対処することのできる、低コストで信頼性の高いセキュリティ・ゲートウェイが必要です。VPN-1 UTM Edgeは、リモート・サイトに対して安全な接続機能を提供するセキュリティ・アプライアンスです。VPN-1 UTM Edgeは、チェック・ポイントのファイアウォール、VPN、侵入防御、およびアンチウイルスの各技術を単一のソリューションとして提供することにより、リモート・サイトで本社などのメイン・サイトと同じレベルのセキュリティを実現します。またチェック・ポイントのSMART管理ソリューション群により、IT管理者は、メイン・サイトの管理に使用しているのと同じツールを使用して、すべてのリモート・サイトに一貫したセキュリティ・ポリシーを適用することが可能です。

リモート・アクセスIPSec VPN

Integrity SecureClient

Integrity SecureClient for VPN-1は、より簡単かつ確実に安全なリモート・アクセスを行えるようにするためのクライアント用のソリューションです。SecureClientとIntegrityの先進機能を併せ持つIntegrity SecureClientは、高度なリモート・アクセス接続機能、エンドポイント保護機能、およびネットワーク・アクセス・ポリシーの実施機能を兼ね備えています。複数の防御機能が単一のパッケージとして提供されることにより、エンドポイントのセキュリティに関するこれら重要な機能の導入および管理が容易に行えるようになります。また、これらの機能は他のチェック・ポイント製品と同じ統一セキュリティ・プラットフォームから管理できるため、企業のネットワークおよびデータを保護するための総コストを削減することも可能になります。Integrity SecureClientはVPN-1 UTMとVPN-1 Powerでサポートされます。

リモート・アクセスSSL VPN

Connectra

現代のビジネスでは、必要ときに必要な情報にアクセスできることが極めて重要です。社員やビジネス・パートナーは、いつでもどこからでも情報にアクセスできることを強く求めるようになっていきます。必要ときに必要な情報を共有可能であることは、企業としての競争力、パートナーシップの効果、および従業員の生産性を向上させることにつながります。つまり企業は、ITリソースの完全性と機密性を維持しながら、どこからでも簡単に社内の情報にアクセスできる環境を提供する必要があります。Connectraは、SSL VPNアクセス機能を単一の統合ソリューションとして提供する包括的なWebセキュリティ・ゲートウェイです。SSL VPNの接続機能とセキュリティ機能を単一のソリューションとして提供するConnectraは、SSL VPNの導入・管理を容易にすると共に、企業として成功を収めるために不可欠な情報の機密性と完全性を確実に維持できるようにします。

SSL Network Extender for VPN-1

モバイル環境の整備が進んだことに伴い、社員は、さまざまなロケーションやネットワーク環境から企業アプリケーションにアクセスするようになっていきます。これら多様な要件に対応するにあたっては、リモート・アプリケーション・アクセスの導入およびサポートに伴う複雑さを最小限に抑える必要があります。そして最も重要なことは、リモート・アクセスの種類を問わず、ネットワークのセキュリティを確実に維持することです。SSL Network Extenderは、Web未対応のネットワーク・アプリケーションにWebベースで接続できるようにすることで、リモート・アクセスの複雑さを軽減します。このWebブラウザ・プラグインにより、従業員やビジネス・パートナーは、SSL VPNを介して容易かつ安全に企業ネットワークに接続できるようになります。

統合されたエンドポイント・セキュリティ

Integrity SecureClient

前掲の「リモート・アクセスIPSec VPN」内の「Integrity SecureClient」を参照してください。

Integrity Clientless Security

Integrity Clientless Securityは、企業のWebベースのネットワーク・アクセス・ポイントに接続してくる共用PCやゲストPC上の脅威から企業ネットワークを保護します。クライアント・ソフトウェアをインストールする必要がないため、マルウェアなどがインストールされている可能性のある、企業の管理下でないPCで企業ネットワークにアクセスする場合でも、ログインID/パスワードが盗まれたり機密情報が漏洩したりするなどの被害が発生するのを防ぐことができます。Integrity Clientless Securityは、「オンデマンド・セキュリティ」に求められる3つの条件、すなわち、ネットワークへのアクセスを許可する前に、スパイウェアを無効にする、セッションの機密性を確保する、セキュリティ・ポリシーを遵守させる、のすべてを満たす業界唯一の製品です。クライアント・ベースのソリューションであるIntegrityと併用することにより、あらゆるロケーションから企業ネットワークに接続する社員やゲストに対してTotal Access Protection (総合的なアクセス保護)を実現することが可能になります。

侵入防御機能の統合

Application Intelligence

Application Intelligenceは、アプリケーション・レベルの攻撃を検出およびブロックするための先進の機能群です。Application Intelligenceにより、ネットワーク・レベルでの防御機能とアプリケーション・レベルでの防御機能がチェック・ポイント製品に統合されるため、包括的な攻撃防御およびネットワーク・セキュリティ環境が実現されます。Application Intelligenceの防御機能は、SmartDefenseサービスに対応しています。SmartDefenseサービスは、変化し続ける脅威と次々に発見される脆弱性に対する最新の防御機能およびアップデートを提供するセキュリティ・サービスです。

Web Intelligence

Web環境は、ネットワーク、OS、Webサーバ、およびバックエンド・システムで構成されています。Webに対応したソフトウェア・アプリケーションの多くは、セキュリティを重視した設計になっていないため、Webアプリケーションには、Unicodeのデコードに関するものから各種のバッファ・オーバーフローに至るまで、何らかのセキュリティ上の欠陥が含まれていることが少なくありません。ハッカーは、Web環境の脆弱性を攻撃するための新たな方法を常に模索しています。そのためWebアプリケーションは、普及が進むにつれ、こうしたハッカーによる攻撃のメイン・ターゲットになっています。Web Intelligenceは、Web環境全体に対する包括な防御機能を提供する、業界唯一のWebアプリケーション・ファイアウォール技術です。VPN-1 Power、VPN-1 UTM、Connectraなど、Web Intelligence技術を搭載するチェック・ポイントのゲートウェイ製品は、この技術を通じて、ネットワーク、OS、Webサーバ、およびバックエンド・システムのためのマルチレイヤの防御機能を提供しています。

管理、監視、レポートニングの統合

SmartCenter

複数のサイトおよび複数のプラットフォームのセキュリティを常に最新の状態で維持することは、リソースの限られたIT部門にとっては大きな課題です。そのためセキュリティ管理ソリューションは、セキュリティ対策の実効性の監視、フォレンジック調査のための詳細な情報の入手、一貫性のあるセキュリティ・ポリシーの実施、および組織全体にわたる事前対応的なアップデートを行えるものでなければなりません。SmartCenterソリューション群は、チェック・ポイントの複数のゲートウェイおよびセキュリティ実施ポイントを一元的に設定、管理、および監視するためのツールです。SmartCenterソリューション群は、チェック・ポイントの統一セキュリティ・アーキテクチャに基づいており、単一の統合管理インタフェースからあらゆるセキュリティ管理作業を行えるようにします。この包括的なアプローチにより、効率的なセキュリティ管理と、ネットワーク・セキュリティに関するTCOの大幅な削減が実現されます。

Eventia Reporter

ネットワーク管理者やセキュリティ担当者は、ネットワークを効率的に管理し、セキュリティ・ポリシーやセキュリティ対策の実効性を検証するために、ネットワークの使用状況を素早く包括的に把握できる手段を必要としています。また、セキュリティ要件を監査したりセキュリティ投資の効果をチェックしたりする必要のある関係者に、重要なセキュリティ情報を簡単に提供することのできる手段も求めています。ログ・ファイルには膨大な量のデータが記録されるため、そのログを手動で調べて長期にわたるネットワーク・アクティビティおよびセキュリティ・アクティビティの傾向を追跡することは容易ではなく、また時間もかかります。Eventia Reporterは、ネットワーク・トラフィックを追跡および監査するための使いやすいログ分析ツールです。セキュリティ担当者は、この集中レポートニング・システムを利用することで、チェック・ポイントの境界、内部、Web、およびエンドポイントのセキュリティ・ゲートウェイより収集された大量のデータから、必要なものだけを素早く抽出することができます。またネットワーク管理者は、セキュリティまたはネットワークの統計データをより簡単により高次のレベルで取得できるため、これらのデータに基づいて、リソースの割り当てやセキュリティの最適化、法規制の遵守に関する重要な判断を下すことができます。

Eventia Analyzer

今日のセキュリティ・アーキテクチャは、ネットワーク上で動作するサーバ、ホスト、およびアプリケーションを悪意あるアクティビティから保護するために、数多くのデバイスで構成されています。これらのデバイスが出力するログは膨大な量になるため、これを分析することは、時間のかかる困難な作業となります。そのため企業は、各種のネットワーク・デバイスやセキュリティ・デバイスが生成する大量のデータの中から、価値のある重要なものだけを抽出することのできる手段を必要としています。Eventia Analyzerは、何らかの判断が求められる重要なイベントだけを優先的に自動抽出する包括的なセキュリティ・イベント管理ソリューションです。Eventia Analyzerは、チェック・ポイントの境界、内部、Web、およびエンドポイントのセキュリティ・デバイスのログ・データ、さらにはサードパーティ製セキュリティ・デバイスのログ・データに対し、一元的なイベント相関分析をリアルタイムで実行するための手段を提供します。

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トップ企業として、特に企業向けファイアウォール、コンシューマ向けインターネット・セキュリティ、およびVPNの世界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、遠隔勤務者、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・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 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、今日業界で最も高い評価を得ており、世界中で何百万人ものユーザをハッカー、スパイウェア、ウイルス、および個人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、数百社におよぶ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、世界中の数千社ものパートナー・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。

©2003-2006 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, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity SecureClient, Integrity Clientless Security, InterSpect, IQ Engine, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecuRemote, SecurePlatform, SecurePlatform Pro, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, 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, 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。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。

Secure Remote Access for the Distributed Business

P/N:502244-J 2006.10

※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 Tel: 03 (5367) 2500