Check Point
SOFTWARE TECHNOLOGIES LTD

UTM

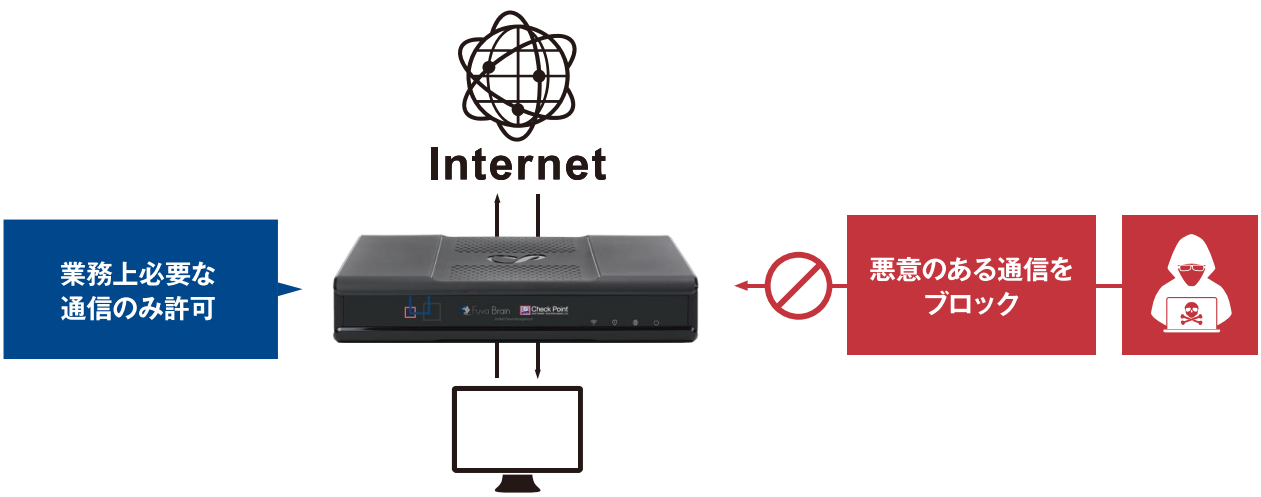
CP1500Series

セキュリティ機能詳細

1. ファイアウォール
2. IPS
3. アンチウイルス
4. スパムメールフィルタ
5. URLフィルタリング
6. アプリケーションコントロール
7. アンチボット
8. サンドボックス

ファイアウォール

ファイアウォールの草分け的な製品であるFirewall-1で培った技術と性能を有する、17万を超える企業に採用されている業界最先端のファイアウォールです。



主な機能

- アクセス制御
- ユーザ認証
- ネットワーク・アドレス変換（NAT）
- ブリッジモード

IPS

チェックポイントのUTMは、最高レベルの侵入防御システム（IPS)を備えており、従来型のスタンドアロンIPSソリューションよりも低コストで革新的なパフォーマンスを実現します。脅威の振る舞いとシグネチャに基づく、数千種類におよぶ外部からの攻撃に対する防御機能を提供します。

パソコンには、OSや、ブラウザ、Java、Flash、Adobeなど多数のアプリケーションに脆弱性が存在します。インターネットに接続する限り、常に外部からの脅威にさらされている状態です。

IPS機能により、外部からの脆弱性を突く攻撃をブロック。常に安心してインターネットをお使いいただくことが可能となります。
対応例:Internet Explorer、Windows OSの脆弱性など

特徴

- **リアルタイムでの保護**

  拡大する脅威に対する最新の防御を定期的に更新。常に先手を打ち、脆弱性が発見されたり、ハッカーに侵入される前に防御機能を提供します。

- **脆弱性への対応**

  Microsoft及びAdobe製品の脆弱性への対応実績では業界No.1！

- **SSLで暗号化されたトラフィックの検査**

  ゲートウェイを通過するSSL暗号化トラフィックをスキャンして安全性を確認できます。

主な機能

次のような悪意のある、あるいは好ましくないネットワーク・トラフィックに対する幅広い保護機能を提供します。

- マルウェアによる攻撃
- Dos/DDos(サービス妨害/分散サービス妨害)攻撃
- アプリケーションやサーバの脆弱性を狙う攻撃
- 内部からの脅威
- インスタント・メッセンジャー(IM)やP2Pなど、好ましくないアプリケーションのトラフィック

アンチウイルス

チェックポイントの ThreatCloud™ から、パターンファイルをゲートウェイへ自動配信します。ゲートウェイでマルウェア感染を阻止し、クライアントPCへの感染を防ぐことが可能です。

特徴

- サイバー犯罪阻止を目的とした業界初の協調型ネットワークを活用Dos/DDos(サービス妨害/分散サービス妨害)攻撃
- 450万件以上のマルウェアと30万件以上の不正サイトを検出
- 世界的なセンサーのネットワークと業界トップのマルウェア対策機関により攻撃情報を動的にアップデート
- マルウェアに感染したWebサイトへのアクセスを遮断
- 脅威レポートとダッシュボードを活用して、マルウェア動向の全体像を把握、対応

主な機能

- **ネットワークに対するマルウェア攻撃を遮断**

  シグネチャや振る舞い分析エンジン、レピュテーション・エンジンなど、複数のマルウェア検出方法を用いてマルウェの攻撃を遮断し、ネットワークを保護します。

- **統合されたマルウェア・レポート**

  感染状況の概要と傾向を確認し、マルウェアが組織にもたらす脅威とリスクを明確に把握することができます。

スパムメールフィルタ

メールに添付しているファイルをウイルス対策機能で精査したり、送信者情報をインターネット上にあるブラックリスト情報と付き合わせることで、危険なメールを止める（設定によっては警告を出す）機能を持っています。

メールを「ブロック」するか、件名の先頭に「SPAM」の文字例を付けて受信

特徴

- コンテンツやIPレピュテーションに基づく高度なアンチスパム機能
- リアルタイムの検出と検索エンジンの自動アップデートにより 新たに発生したスパムメールにも即座に対応

主な機能

- **IPレピュテーションによるアンチスパム**

  悪意あるIPアドレスが随時追加される動的データベースで送信者のレピュテーションをチェックすることにより、スパムやマルウェアを接続レベルでブロック

- **コンテンツ・ベースのアンチスパム**

  画像を利用したスパムや各国語のスパムなど、最新のスパムをパターン・ベースで検出

- **拒否/許可リストによるアンチスパム**

  拒否リストや許可リストを使用して、明らかなスパム送信者からのE-mailを拒否し、信頼できる送信者からのE-mailを許可

- **メールのアンチウイルス**

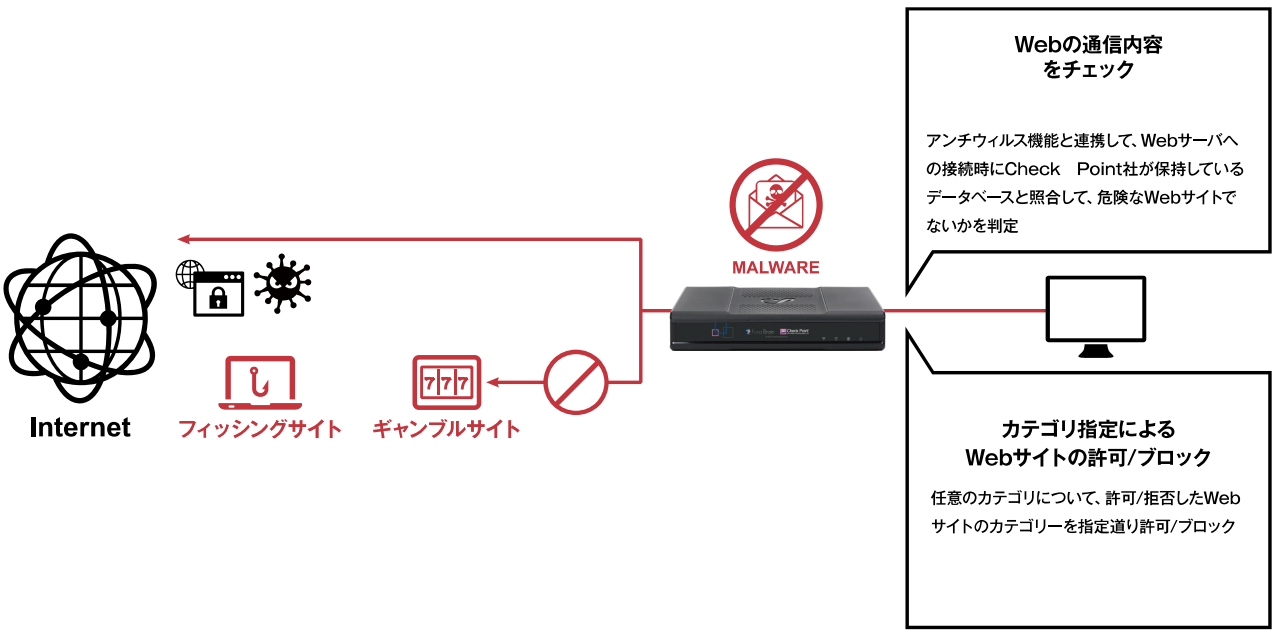
  メッセージ本文と添付ファイルのスキャンなどにより、多様なウイルスおよびマルウェアをブロック

- **ゼロアワー・アウトブレイク保護機能**

  分析エンジンの使用および配布により、新種のスパムおよびマルウェアをブロック

URLフィルタリング

UTMのアンチウイルス機能と連携し、セキュリティリスクのあるサイトへのアクセスを自動的に制限します。 また、業務に無関係なWebサイトへのアクセスを管理し、制限します。



特徴

- 幅広いURLにリアルタイムで対応
- SSLで暗号化されたトラフィックを検査、簡易HTTPSフィルタリングも可能

主な機能

- 2億以上のWebサイトへのアクセスをリアルタイムで許可、禁止、制限
- SSLで暗号化されたトラフィックを分析
- 事前設定された64種類のカテゴリに基づいてポリシー・ルールを作成
- サイト単位またはページ単位でアクセスを制御
- 特定のURLをホワイト・リストとブラック・リストに登録することでポリシーをきめ細かく調整

アプリケーションコントロール

6,000以上のWebアプリケーションや約30万のウィジェットを識別し、その利用を禁止または制限するきめ細かいポリシーを、ユーザーやグループごとに容易に作成することが可能。
対応アプリケーション数は業界ナンバー1

ソーシャル・ネットワーク・
サービス 使用禁止

Webストレージ
使用禁止

フィルタ交換ソフト
使用禁止

特徴

- きめ細やかなアプリケーション制御
- AppWikiで提供される最大規模のアプリケーション・ライブラリ

主な機能

- **アプリケーションの検出と利用の制御**

  ポートやプロトコルの種類、ネットワークをすり抜ける回避技術が使用されているかどうかに関係なく、アプリケーションのセキュリティポリシーに基づいて、Web2.0やソーシャル・ネットワーキングを含む膨大な数のアプリケーションを識別し、その利用を許可、禁止、制限します。

- **アプリケーション分類ライブラリ「AppWiki」**

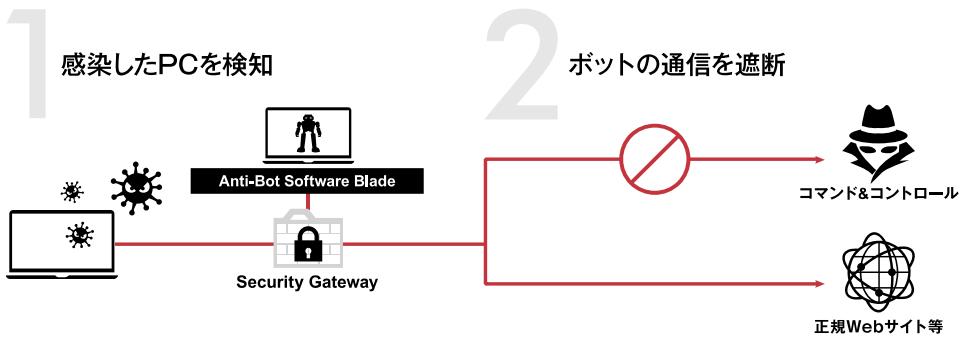
  AppWikiに基づき、6,000を超える個別アプリケーションと約30万のWeb2.0ウィジェット（インスタント・メッセージングやソーシャル・ネットワーキング、ビデオ・ストリーミング、VoIP、ゲームなど）をスキャンして検出します。

- **UserCheck**

  アプリケーションの利用制限についてリアルタイムで社員に警告し、インターネットのリスクや企業のアプリケーション利用ポリシーを周知します。特定アプリケーションの使用をポリシーで許可または禁止するだけでなく、アプリケーションの利用が業務上必要なのか、プライベートな目的なのか、ユーザに問うように設定することもできます。

アンチボット

ボットウイルス※に感染した場合、情報漏えい被害だけでなく、スパムメールの発信やDoS攻撃など、攻撃者の踏み台にクライアントPCが利用され、被害者でありながら、加害者となる危険もあります。
アンチボット機能により、感染したクライアントPCと外部の指令サーバ間の通信を検知し、不正な通信を遮断します。



特徴

- 2億5,000万を超えるアドレスを分析してボットを検出
- 世界的なセンサーのネットワークと業界トップのマルウェア対策機関により攻撃情報を動的にアップデート
- ボットに対する指令の発信元やボットネットの通信パターン、攻撃時の振る舞いに関する組み合わせを正確に検知
- ボット感染ホストと遠隔地にいるボット管理者との間の通信を遮断して、ボットによる被害を予防

主な機能

ボット検出エンジンのMulit-Tier ThreatSpect、複数の手法を組み合わせてボットの感染を検出

1. レピュテーション
   IPアドレスやURL、DNSアドレスを評価し、既知のボットネット指令（C&C)サーバ宛てのトラフィックが発生していないかどうかを調査

2. パターン
   HTTPやDNS、SMTPなど、複数のプロトコルでボットネット・ファミリー固有の通信パターンを検出
   標準的でないポートやプロトコルの使用のほか、クリック詐欺などの攻撃タイプを把握してボットの活動を抑止し、被害を予防

3. 標準的でないポートやプロトコルの使用のほか、クリック詐欺などの攻撃タイプを把握してボットの活動を抑止し、被害を予防

インラインでのボット防御・ボット感染ホストからの通信を遮断

1. ボットからC&Cサーバへの通信を遮断して被害を予防
2. ボットのトラフィックのみを遮断し、良好なトラフィックは引き続き許可して、ビジネスへの影響を阻止

※ボットウイルスとは、コンピュータウイルスの一種で、コンピュータに感染し、そのコンピュータを、ネットワーク(インターネット)を通じて外部から操ることを目的として作成されたプログラムです。 感染すると、外部からの指示を待ち、与えられた指示に従って内蔵された処理を実行します。この動作が、ロボットに似ているところから、ボットと呼ばれています。 IPA情報セキュリティより参照
https://www.ipa.go.jp/security/antivirus/bot.html

サンドボックス：Threat Emulation

チェックポイント Threat Emulationは、未知の脆弱性を狙うゼロデイ攻撃や標的型攻撃によるマルウェア感染を防止し、その被害を防ぎます。不審なファイルを発見後、直ちに仮想サンドボックス内で実行して不正活動の有無を確認し、マルウェアのネットワークへの侵入を阻止します。

特徴

- 仮想サンドボックス内でファイルを分析して、新しい脅威やゼロデイ攻撃を検出、防御
- 電子メールへの添付やダウンロードで受信する不正なファイルをブロック
- Microsoft Officeファイル、Adobe PDFファイル、EXE、ZIPに埋め込まれた脅威に対応
- SSLとTLSによる暗号化通信に潜む脅威を検出
- ボット発見を目的として分析された2億5,000万件以上のアドレスや、1,200万件以上のマルウェア・シグネチャ、100万件以上の不正サイトの情報により、保護機能が向上

主な機能

業界最高水準の仮想サンドボックス技術

Threat Emulationでは、ネットワークに送信されてきたファイルをインターセプトして無害なファイルを除外した後、不審なファイルを仮想環境で実行します。マルウェア特有の不審な活動や不正な動作を示したファイルは脅威として認識され、そのシグネチャがチェックポイント ThreatCloudに送信されます。これにより、新たに見つかったマルウェアが既知の脅威として登録され、ブロックできるようになります。

暗号化通信

多くの一般的なセキュリティ・ゲートウェイを通過するSSLやTLSトラフィックは、攻撃者にとって組織による不正ファイルの検出を回避できる有用な攻撃経路です。Threat Emulationは、SSLやTLSトンネルの内部を検査してファイルを抽出、実行し、暗号化されたトラフィックに潜む脅威を検出します。

EXEとZIPに潜む脅威を防御

Threat Emulationは、ダウンロードや電子メールへの添付で受信する可能性のあるEXEやZIP経由の感染を検出、防御します。

Microsoft OfficeファイルとAdobe PDFファイルに潜む脅威をブロック

Threat Emulationは、業界をリードする脅威エミュレーション技術でMicrosoft OfficeファイルとAdobe PDFファイルを保護します。どちらもビジネスにおいて最も多用されるファイルですが、容易に悪用可能な攻撃手段である点は見過ごされがちです。Threat Emulationは、誤検出を発生させずにセキュリティを強化できるため、業務の妨げとなるデメリットも避けられます。

※サンドボックス：Threat Emulationは、オプションになります。