

進化したメッセージング・セキュリティ

マルチレイヤのアプローチで最新の脅威をブロック

多くの企業におけるE-mail環境は、他のIT環境と同様、以前にもましてさまざまな攻撃のターゲットとなっており、多くの組織にとって、メッセージング・セキュリティを確立することは大きな課題となっています。出現当初のスパム・メールは、ネットワーク帯域を浪費し、エンドユーザに不快感を与えるというだけの存在でしたが、それでも多くの組織は、その影響を軽減するために何らかのアンチスパム・ソリューションを導入することを余儀なくされました。しかしその後、スパム送信の手法が非常に洗練されていき、現在のスパム・メールは、旧来型アンチスパム・ソリューションの多くをすり抜けることができるようになってきました。さらに悪いことに、スパム・メールは不愉快でネットワーク帯域を浪費するというだけでなく、マルウェアの主要な媒介として利用されるようになり、企業ネットワークに多数の脅威が侵入する原因にもなっています。例えばある調査では、昨年、E-mail経由でマルウェアに侵入され、ネットワークに悪影響が生じたと回答した企業は、調査対象の84パーセントにも上っています^{注1}。また、フィッシング詐欺を始めとする、E-mailを利用した不正行為も巧妙化・多様化が進む一方であり、多くの企業は、これらの攻撃から顧客を安全に守るために多大な苦勞を強いられています。こうしたことから、今日のメッセージング・セキュリティ・ソリューションには、画像などを利用する最新スパムだけでなく、これまでなかったようなE-mailベースの攻撃やメッセージング・インフラストラクチャ自体への攻撃にも対処することが求められていると言えます。

包括的なメッセージング・セキュリティ環境を構築するための要件

メッセージング環境を包括的に保護するには、メッセージング・セキュリティ・ソリューションが次の3つの主要な脅威に対応している必要があります。

最新のスパム/フィッシング

スパム・メールは驚異的なペースで増加しており、ある調査によれば、現在インターネット上で送信されている全E-mailに占めるスパム・メールの割合は80パーセント以上にも上ります^{注2}。また、最近のスパム・メールはますます洗練されてきており、画像や複数の文字形式を使用するなどさまざまなテクニックを駆使することで、本文の内容に基づいてスパム・メールを識別する古いタイプのスパム検出技術をすり抜けようとしています。そのため、スパム対策として数年前に導入されたソリューションの多くは、これらのアプローチを採用したスパム・メールに対応できなくなっています。今日のメッセージング・セキュリティ・ソリューションは、少なくとも95パーセント以上の検出率でこれら最新のスパムを検出し、それと同時に、誤検知を最小限に抑えることができなければなりません。

マルウェア/ウイルス

ウイルスなどのマルウェアからネットワークやシステムを保護することは、メッセージング・セキュリティ・ソリューションにとって、言うまでもなく非常に重要なことです。これらのソリューションはまず、高い精度で既知の脅威に対処することのできるシグネチャ・ベースの検出機能を備えている必要があります。また、シグネチャ・ベースのエンジンによる検出を免れることのできる未知の脅威（ゼロアワーの脅威）を検出および遮断する機能も備えていなければなりません。このマルチレイヤのアプローチにより、ウイルスなどの各種マルウェアに対する広範かつ確実な防御が可能になります。

注1. 注2. Osterman Researchの調査による

主な利点

- E-mail侵入防御機能により、メッセージング・インフラストラクチャへの攻撃を確実に遮断
- 検出率97パーセント以上、誤検知も最小限のアンチスパム機能
- E-mailのメッセージ内容に依存せずスパムをブロックするパターン・ベースの検出機能
- 悪質なメール送信者を事前にブラックリスト化するIPレピュテーション・サービス
- シグネチャ・ベースのアンチウイルス機能とチェック・ポイント独自のゼロアワー・アウトブレイク保護機能の組み合わせにより、既知と未知の両方の攻撃をブロック



NGXプラットフォームによりチェック・ポイントの統一されたセキュリティ・アーキテクチャを実現します。

メッセージング・インフラストラクチャに対する攻撃

メール・サーバに対する攻撃においても、旧来とは異なる新たな手法が用いられるようになってきました。かつてよく見られた、メール・サーバを勝手に中継し無断使用されるという問題は、すでにほぼ解決されていますが、その一方で、メール・サーバやクライアントがマルウェアに乗っ取られ、スパム・メールやその他のE-mailベースの脅威を大量にまき散らすボットネットとして悪用されるというケースが増えています。今日では、遵守すべきさまざまな法令や規制が増加していることに加え、データ・セキュリティ・リスクも高まっていることから、この問題に対処することは非常に重要と言えます。また、メッセージングに特化した侵入防御機能も、メッセージング・セキュリティを高めるうえで必要不可欠となっています。

チェック・ポイントのトータル・セキュリティ・ソリューション

チェック・ポイントのUTM-1™ Total Security™アプライアンスは、包括的で高性能なネットワーク・セキュリティ機能を、導入しやすさと管理性、コスト・パフォーマンスに優れた統合プラットフォーム上で、包括的かつ高性能なネットワーク・セキュリティ機能を提供するセキュリティ・ゲートウェイです。Fortune 100企業で採用されているチェック・ポイントの技術をベースとするUTM-1 Total Securityアプライアンスは、メッセージング・セキュリティを構成する6つの機能を始めとする、包括的なセキュリティ機能を備えています。これにより、最新のスパムやゼロアワーの脅威といったマルウェア、メッセージング・インフラストラクチャへの攻撃などに対する包括的な防御が実現されます。

メッセージング・セキュリティを構成する6つの機能

UTM-1 Total Securityは、メッセージング・セキュリティを構成する6つの機能を備えています。これにより、97パーセント以上のスパム・メールを効果的にブロックし、既知と未知の両方のマルウェアを遮断すると共に、さまざまな攻撃からメッセージング・インフラストラクチャを保護します。

1. IPレピュテーション・サービス: チェック・ポイント独自のIPレピュテーション・サービスは、E-mailの接続リクエストをIPアドレスの総合データベースと照合し、その送信者が正規の送信者であるか、あるいはスパムやマルウェアの既知の送信者であるかを判別します。ここで望ましくない送信者であると判定された場合、UTM-1 Total Securityは、メッセージを受け付ける前にその接続を切断します。自社宛てに送信されたスパム・メールやマルウェアが添付されたメールの80パーセント以上は、それ以上の検査を行うことなく、このレイヤでブロックすることができます。動的なIPアドレス・データベースは定期的に更新されるため、悪意ある振る舞いをしなくなったIPアドレスがいつまでもブロックされることはありません。

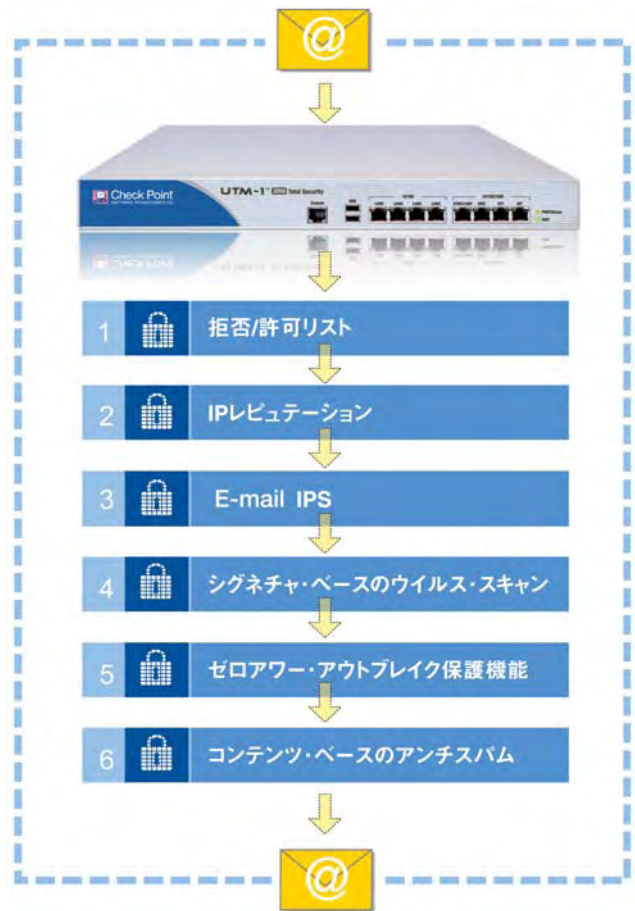
The screenshot displays the 'Messaging Security Overview' interface. At the top, there are sections for 'Enforcing Gateways' (with 'Anti Virus' and 'Anti Spam' buttons) and 'Database Updates' (with an 'Enable automatic updates' checkbox and a 'Configure' button). Below this is a table of security features, each with a status indicator, a brief description, a 'Settings' link, a 'View Logs' link, a protection level indicator, and a list of key metrics or actions.

Feature	Description	Protection Level	Key Metrics/Actions
Content based Anti Spam	E-mails finger print is sent for validation	High protection	<ul style="list-style-type: none"> Filter spam Filter suspected spam A false positive rate of 1 in a 100,000 Expected performance: 350-500 emails/sec Protects against all types of spam
IP Reputation Anti Spam	Filter spam from known spammers	High protection	<ul style="list-style-type: none"> Filter spam Filter suspected spam Expected performance: 1000-1500 emails/sec Saves Bandwidth, Enhancing Performance
Block List Anti Spam	User defined IPs and addresses blocking	Block	<ul style="list-style-type: none"> Block senders by IP Block senders by address 2 IPs will be blocked 4 Senders/Domains will be blocked
Mail Anti Virus	Scan and filter mail for malware	Block	<ul style="list-style-type: none"> Block Expected performance: 1000-1500 emails/sec Saves Bandwidth, Enhancing Performance
Zero hour malware protection	Filter mail using rapid response signatures	Block	<ul style="list-style-type: none"> Block Immediate proactive malware protection Expected performance: 350-500 emails/sec
SmartDefense	Email IPS protections	Go to SmartDefense Tab to manage	<ul style="list-style-type: none"> 2 POP3 servers defined 2 SMTP servers defined 2 IMAP servers defined

UTM-1 Total Securityが提供する6つのメッセージング・セキュリティ機能は、単一の管理コンソールから全ての機能をかたんにすばやく設定することが可能です。

- 2 **パターン・ベースのアンチスパム**：パターン・ベースのアンチスパム機能は、独自のアルゴリズムを用いて、E-mailメッセージの指紋とも言うべきシグネチャを作成します。E-mailを受信すると、そのパターンがオンザフライで計算されてこのシグネチャ・データベースと照合されます。そして、そのパターンが既知のE-mailパターンと一致するかどうかが判定されます。このアプローチは、メッセージの内容に依存しないため、実際のメッセージ本文を一切チェックすることなくスパム・メールを効果的にブロックすることができます。これにより、複数の言語や複雑な画像、画像の断片を使用する最新のスパムも高い確率でブロックすることが可能となっています。
- 3 **拒否/許可リスト**：この機能を使用して、常に拒否あるいは許可するIPアドレスまたはドメインのリストを簡単に作成できます。この機能は追加のフィルタリング・レイヤとしての役割を果たし、信頼できる送信元からのアクセスを明示的に許可し、望ましくない送信元からのアクセスを明示的に拒否できるようにします。ブロックしているIPアドレスおよびドメインの数は、[Messaging Security management] タブにある拒否/許可リストの概要セクションで確認できます。
- 4 **シグネチャ・ベースのアンチウイルス**：UTM-1 Total Securityは、送信者レベルで多くの攻撃をブロックするほか、定評あるアンチウイルス・エンジンを用いて各種メール・プロトコル (POP3、SMTP、IMAP) の検査を行います。この保護レイヤは、アプライアンスにおけるウイルス対策の中核となる機能であり、既知のウイルスやマルウェアによるさまざまな攻撃をブロックします。
- 5 **ゼロワー・アウトブレイク保護機能**：発生直後の攻撃に対処するため、UTM-1 Total Securityアプライアンスには、チェック・ポイント独自のゼロワー・アウトブレイク保護機能が搭載されています。この機能では、インターネット全体で流通している膨大な量のメッセージを分析し、新しい攻撃の出現を把握すると共に、そのメッセージ・パターンを特定してこれに「悪意あるメッセージである」というフラグを付けます。UTM-1 Total Securityアプライアンスは、このフラグを通じて、あらゆる攻撃についての最新情報を入手します。新たに出現した攻撃は、この情報に基づいて即座に (およそ0.5秒～2秒) ブロック可能となるため、シグネチャが実際に提供されるまでの非常に危険な時間帯もネットワークを保護することができます。
- 6 **SmartDefenseによるE-mail IPS**：UTM-1 Total Securityは、チェック・ポイントの先進のファイアウォールおよび侵入防御技術をベースとする、SmartDefense™によるE-mail IPSを搭載しており、メッセージング・インフラストラクチャに対する攻撃を確実に遮断します。メッセージング・インフラストラクチャに対しては、保護されたネットワークに不正アクセスしてシステムの一部を停止させる、および、新たな攻撃を仕掛けるためのリソースとしてシステムを不正利用する、といった攻撃が行われる可能性があります。UTM-1 Total Securityは、サービス妨害 (DoS) 攻撃やバッファ・オーバーフロー攻撃などの各種攻撃からメッセージング・インフラストラクチャを保護します。

メッセージング・セキュリティを構成する6つの機能



短時間で導入可能なセキュリティ・ソリューション

UTM-1 Total Securityアプライアンスは、わずか10分ほどでセットアップ可能で、IT管理者が少ない環境においても容易に導入できるシンプルさを実現しています。導入時には、初期設定ウィザードを使用することで、セキュリティ専任の管理者でなくても簡単にアプライアンスの初期セットアップや構成を行うことができます。セットアップ完了後は、業界標準であるチェック・ポイントの管理フレームワークを利用して、リモートからUTM-1 Total Securityアプライアンスを管理および更新を行えるようになります。ネットワーク中に複数のゲートウェイが存在する場合でも、セキュリティ・ポリシーやゲートウェイの設定などを一括で集約的に管理することができ、各サイトやゲートウェイを個別に管理する必要がありません。そのため、管理者の負担を軽減し、設定ミスが起きる可能性を低く抑えると同時に、ネットワーク全体にわたって一貫したセキュリティを適用することが可能になります。

ネットワークを保護するために必要なすべての機能およびサービスを一括で最大3年間提供するUTM-1 Total Securityアプライアンスは、セキュリティ機器の調達プロセスと導入プロセスの両方を簡素化します。3年が経過した後も、トータル・セキュリティ・サブスクリプション契約を更新するだけでアップデート・サービスをさらに延長できます。すべてのセキュリティ機能、アップデート・サービス、およびハードウェア保証を単一のデバイスとして提供するUTM-1 Total Securityアプライアンスは、セキュリティ環境の大幅な簡素化を実現すると同時に、セキュリティ機能の日常的な管理およびアップデート作業を効率化するというさらなるメリットを提供します。

まとめ

UTM-1 Total Securityアプライアンスは、メッセージング関連の攻撃からネットワーク・インフラストラクチャを包括的に保護するために必要なすべての機能およびサービスを提供します。メッセージング・セキュリティを構成する6つの機能を備えるUTM-1 Total Securityアプライアンスは、メッセージング関連の3大攻撃経路、すなわち最新のスパムおよびフィッシング、ウイルスなどのマルウェア、そしてメッセージング・インフラストラクチャへの攻撃に対処します。また、これらのメッセージング・セキュリティ機能に加え、ファイアウォール、VPN、侵入防御、アンチウイルス/アンチスパム、Webフィルタリング、インスタント・メッセージ/P2Pアプリケーションのブロック、VoIP保護機能などの一連のセキュリティ機能も備えています。

UTM-1 TOTAL SECURITYの主な機能

 <p>先進のファイアウォール</p> <ul style="list-style-type: none"> ● VoIP ● インスタント・メッセージ ● P2P 	<p>業界最高レベルの実績を誇るファイアウォールにより、VoIP、インスタント・メッセージ、ピアツーピア・アプリケーションを含む、数百種類のアプリケーションおよびプロトコルを保護</p>
 <p>VPN (サイト間接続およびリモート・アクセス接続)</p>	<p>多機能かつ容易に設定可能なIPSec VPN機能</p>
 <p>ゲートウェイ・アンチウイルス/アンチスパイウェア</p>	<p>シグネチャ・ベースのアンチウイルス/アンチスパイウェア機能</p>
 <p>侵入防御</p>	<p>シグネチャ・ベースの検知とプロトコル・アノーマリ(プロトコル異常)・ベースの検知の両方に対応した高性能IPS</p>
 <p>SSL VPN</p>	<p>SSL VPN機能を統合。導入後即使用可</p>
 <p>Webフィルタリング</p>	<p>2,000万以上のサイトをカバーする先進のWebフィルタリング機能</p>
 <p>メッセージング・セキュリティ</p>	<p>6つの機能で構成される包括的なセキュリティ機能により、メール・インフラストラクチャを保護し、スパムおよびマルウェアを排除</p>

製品に関するお問い合わせ

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

©2003-2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Express, Check Point Express CI, Check Pointのロゴ, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, 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, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, puresecurityのlogo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, 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, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, 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, 5,987,611, 6,496,935, 6,873,988, 6,850,943, および7,165,076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。

P/N 502772-J 2008.01 ※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。

