



ブロックするべきか、しないべきか — それは問題か？

2009 年 12 月

Palo Alto Networks
232 East Java Dr.
Sunnyvale, CA 94089, USA
Sales: 866.207.0077
www.paloaltonetworks.com

目次

概要	3
Enterprise 2.0 アプリケーション.....	3
Enterprise 2.0 の 3 つの特性.....	6
その役割は賢明なポリシーによる安全な導入を行うこと.....	8
Enterprise 2.0 を安全に導入するのに必要なツール	9
従業員の管理	9
デスクトップの管理	10
ネットワークの管理.....	10
Palo Alto Networks の次世代ファイアウォールの使用.....	11
Enterprise 2.0 アプリケーションの識別.....	11
Enterprise 2.0 アプリケーションへの積極的な管理 (ファイアウォール) ポリシーの適用.....	13
展開の柔軟性	14
結論	14
Palo Alto Networks について.....	15

Copyright c 2009, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, "the Network Security Company," PAN-OS, FlashMatch, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. in the United States. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

概要

今日の企業ネットワークには、重大な問題があります。それは、ユーザーが主導権を握っていることです。

皮膚にも同じようにこの問題の根底をなす IT 担当者たちは、その原因が、ユーザーを管理できていないことにあると信じています。ユーザーは、それでもなお新しい Web ベースのアプリケーションを使用し、その結果としてネットワークを未知の脅威にさらし、サポートするように設計されていないタスクを実行します。この点では明らかにユーザーが間違っているため、トラフィックに関するこの問題に対する答えは簡単です。つまり、*ブロックする必要があります*。

ユーザーは、彼らが業務を遂行できるように IT 担当者がネットワークを設計しなかったことに原因があると信じています。ユーザーは、会社の外で消費者として使用しているアプリケーションを使用したいと考えています。これらのアプリケーションは使いやすいからです。これらのアプリケーションが厄介でありながら意義があるとみなされるのは、コラボレーションを重視した「常時接続」という性質があるためです。オープンで使いやすく、常に世界中に接続されている。これこそが従来の企業アプリケーションに欠けている要素なのです。この点では明らかに IT 部門が間違っているため、この問題に対する答えは簡単です。つまり、*ブロックしてはなりません*。

選択を迫られる場面に直面すると、人間の心は極端な結論に偏る傾向があります。白か黒かの選択ができるのなら、灰色を選択することもできるのではないのでしょうか。言うまでもありませんが、今日の企業ネットワークの問題に対する答えは、ブロックすべきかどうかという単純な選択によって出せるものではありません。本当の答えを出すには、現状を正確に見極めて、やや灰色な選択をしながら正しい答えを見つけ出すことができなければなりません。

このホワイトペーパーでは、Enterprise 2.0 アプリケーションの安全な導入を可能にするポリシーを作成し実施する方法を明らかにすることにより、Enterprise 2.0 アプリケーションに適切に対処する方法（および、そもそも Enterprise 2.0 アプリケーションとは何なのか）について実践的に解説します。このホワイトペーパーで使用するデータは、2009 年の 6 か月間に収集された世界中の 200 を超える組織のアプリケーションとネットワークトラフィックに基づきます。¹

Enterprise 2.0 アプリケーション

わずか数年前、まだ世界は球形だと考えられていました。国、都市、企業の周囲には境界が存在していました。その中には、法律によって施行されている架空の境界と、機械によって施行されている物理的な境界がありました。企業ネットワークへの「境界線」となっていたのは、ファイアウォールです。「パスポート」を持っていなければ、中に入ることも外に出ることもできませんでした。ほんのわずかな既知のトラフィックだけが許可され、他のトラフィックはすべてアクセスを拒否されていました。世界はシンプルでした。

今日では、世界には境界はなく、平坦な形をしていると認識されています。私たちは、境界がまだ存在していると考えたり、そうであることを望んだりしていますが、実際には、ほぼすべての境界が危ういものになっています。企業ネットワークにおいては、従来のファイアウォールは、かなり以前からその意義を失っています。問題を解決するために投入されたテクノロジーが確実に広がっていたにもかかわらず、従来の境界を危ういものにした新世代のアプリケーション、テクノロジー、および技術が台頭してきました。言い換えれば、開発者は、「フェンスを飛び越える」ための回避策、トンネルなどの方法を考え出すことによって、境界を回避する方法を見つけたのです。さらに、ユーザーコミュニティでもこれらの方法が見付け出されるようになりました。開発者やユーザーは、URL がブロックされたり、アプリケーションによる企業ネットワーク内外への通信が拒否されたことに気付くと、www.proxy.org などのサイトからその回避方法を探し出します。[合衆国権利章典](#)の第 4 および第 5 修正条項または国連

¹ [アプリケーション使用およびそのリスクに関する報告書](#) (Fall Edition, 2009)、Palo Alto Networks

の[世界人権宣言](#)の第 12 条の旗の下に、このような事例はますます増加しています。これはもはや単なる IT ポリシーに関する問題ではなく、消費者の基本的な権利の 1 つに関する問題となっているのです。

Enterprise 2.0 アプリケーションは、平坦な世界のシンボリックな存在です。「*拡大した企業において迅速かつ機敏なコラボレーション、情報共有、参入、および統合機能を提供する Web ベースのテクノロジーのシステム*²」と定義された Enterprise 2.0 アプリケーションは、世界を席巻しました。初めは主に検索、リンク、タグ付けに焦点を絞ったアプリケーションでしたが、その後、オーサリング、ネットワーキング、および共有を可能にするアプリケーションへと急速に変化しました。

第 1 世代の Enterprise 2.0 アプリケーションの例を次に示します。

- Socialtext などのウィキ
- Blogger などのブログ作成ツール
- NewsGator などの RSS ツール
- Cogenz などの企業ブックマークツールおよびタグ付けツール
- AOL Instant Messenger (AIM) などのメッセージングツール

第 2 世代の Enterprise 2.0 アプリケーションの例を次に示します。

- SharePoint などのコンテンツ管理ツール
- MegaUpload.com などのブラウザベースのファイル共有ツール
- Facebook などの複雑なソーシャルネットワーク
- YouTube などの公開ツール
- Skype などのユニファイドメッセージングツール
- Twitter などの投稿ツール

企業内で使われている Enterprise 2.0 アプリケーションのディレクトリを構築するために多くの試みが行われてきましたが、完全な一覧を作り出すには至っていません。そのような試みの 1 つとして、{app}gap によって公開されている Appopedia³ があります。

Palo Alto Networks が行った 2 つの試みでは、利用可能なアプリケーションの一覧と、企業におけるこれらのアプリケーションの採用状況に関する調査結果が得られました。

1. 半年ごとに公開される[アプリケーション使用およびそのリスクに関する報告書](#)には、世界中の数百に及ぶ組織から収集されたアプリケーションの採用と使用に関するデータが含まれています。
2. [Applipedia](#) には、Palo Alto Networks が管理できる 900 を超えるアプリケーションの詳細情報が含まれています。これには、200 を超える Enterprise 2.0 アプリケーションが含まれていません。

² Wikipedia「[Enterprise Social Software](#)」

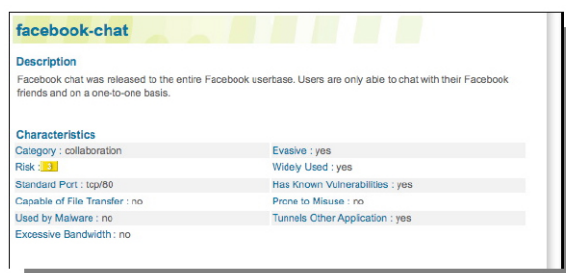
³ {app}gap の [Appopedia](#)



Category	Subcategory	Technology	Risk	Characteristic
167 business-systems	27 audio-streaming	322 browser-based	249 1	360 Evasive
246 collaboration	10 auth-service	310 client-server	151 2	272 Excessive Bandwidth
112 general-internet	16 database	177 network-protocol	226 3	217 Prone to Misuse
123 media	47 email	98 peer-to-peer	181 4	455 Transfers Files
259 networking	22 encrypted-tunnel		100 5	196 Tunnels Other Apps
	15 erp-crm			199 Used by Malware
	84 file-sharing			487 Vulnerabilities
	26 gaming			580 Widely Used

図 1: Applipedia (Palo Alto Networks のオンラインアプリケーション事典)

Facebook などのアプリケーションは、実際は複合的なアプリケーションです。Facebook が 2004 年 2 月 4 日に導入されたときは、単一の目的だけを果たす制限の多いアプリケーションでした。しかし、この数年の間に採用と使用が爆発的に増加して、今日では、世界中で 3 億人以上に使用されるようになっています。これはアメリカ合衆国の全人口を超えています。その間、Facebook には Facebook フォトなどの新しいアプリケーションが導入され、2008 年 4 月には Facebook チャットが導入されました。以前はシンプルなアプリケーションでしたが、現在ではアプリケーションのネットワークへと変貌しました。しかし、それで終わりではありませんでした。Facebook は [アプリケーションプラットフォーム](#) へと変貌し、今日では Facebook という世界の一部として [何万ものアプリケーション](#) が開発されています。同時に、Facebook では多様なハッキング、エクスプロイト、および脆弱性が生じやすくなっています。



Characteristics	
Category : collaboration	Evasive : yes
Risk : 3	Widely Used : yes
Standard Port : tcp/80	Has Known Vulnerabilities : yes
Capable of File Transfer : no	Prone to Misuse : no
Used by Malware : no	Tunnels Other Application : yes
Excessive Bandwidth : no	

図 2: Applipedia からの Facebook チャットに関する情報

さらに懸念されているのは、Enterprise 2.0 アプリケーションがネットワークに「浸透」する方法です。今までで初めて、これらのアプリケーションを IT 部門の関与なく採用できるようにする 2 つの大きな動向が同時にやってきたのです。

1 つ目の動向は、90 年代の初頭にさかのぼります。このとき、Visual Basic などのテクノロジーが出現し、誰もが IT 部門の支援を受けることなくシンプルなアプリケーションを開発できるようになりました。これらのアプリケーションは机の下に置かれたサーバーで実行され、ユーザーは業務を遂行できるようになったことで純粋に満足していました。以前は IT の消費者だったユーザーが生産者になったのです。これらのアプリケーションの大部分は、組織にセキュリティ上のリスクをもたらすものではありませんでしたが、情報管理とコンプライアンスの観点から IT 部門にとっては悩みの種となりました。

第 2 の動向は、2000 年代の初頭に、シンプルなコラボレーション機能を持つ Web ベースのアプリケーションが出現したときに始まりました。状況はまったく異なるものになりました。これらのアプリケーションは、その性質上、企業ネットワークの境界を完全に越えてしまったからです。90 年代には Web ベースのアプリケーションは主に電子商取引と電子メールに使用されていましたが、今ではこれらのアプリケーションをどこからでも起動してアクセスできるようになり、情報の消費者を生産者へと変貌させました。この動向は、最初は消費者の世界で始まり、その後、ビジネスの世界でも急速

に広まりました。多くの IT 専門家がさらに驚きと懸念を感じていることは、技術革新と採用サイクルが速度を増していることです。

次に例を挙げます。

- 2008 年 4 月に開始されて以来 18 か月未満で、Facebook チャットの企業内での使用率は Yahoo! IM および AIM を上回りました。
- 企業における Google ドキュメントの浸透率は、2009 年 3 月から 2009 年 9 月の間に 33% から 82% に増加しました。
- これと同期間に、企業での Twitter の使用率は、セッション数では 252%、帯域幅では 775% 増加しました。

すでに述べたように、Enterprise 2.0 アプリケーションは多面的かつ多機能です。機能の一部は非常に明白ですが、多くの機能は「舞台裏」で利用されます。たとえば、これらのアプリケーションの 70% はファイルを転送できます。つまり、表向きの使用目的は Voice-over-IP (VoIP) またはインスタントメッセージングでも、同じアプリケーションを使用してファイルの転送が行えるのです。このような機能の例として、Skype および IBM/Lotus Sametime があります。複雑さが増加するもう 1 つの原因として、アプリケーションを使用して多数のコンテンツを共有できることがあります。この例としては WebEx があります。このアプリケーションを使うと、デスクトップのコンテンツを多数の閲覧者と共有できます。多くの場合、PowerPoint プレゼンテーションを共有しても害はありませんが、WebEx デスクトップ共有機能を通じてデスクトップを共有すると、セキュリティとコンプライアンスに関する深刻な問題が生じます。

また、多くの Enterprise 2.0 アプリケーションは、品質面であまり優れているとは言えません。そのように作られている場合もありますが、多くの場合は、企業クラスの品質とセキュリティ要件を満たすように構築されていないことが原因です。そのため、これらのアプリケーションの 28% はマルウェアを広めることができ、64% もが既知の脆弱性を持っています。このような性質があるため、IT 部門の心配は深まり、ネットワーク上での使用を許可するか許可しないかという問題になると、非常に二者択一的な態度を取ることになります。しかし、多くの IT 専門家は、これらをブロックすることは、サーバーの電源をオフにしたり、URL やポートをブロックしたりするほど簡単ではないということに気付いています。従来の知識や技術では、もはや通用しないのです。

多くの Enterprise 2.0 アプリケーションはクラウドベースであり、ブラウザを使用してアクセスします。しかし、同様に短期間に採用が進んだ SharePoint などのアプリケーションは、多くの場合、オンプレミスで展開されるにもかかわらず、リスクをもたらしています。Gartner などの調査会社は、SharePoint は 90 年代における Visual Basic に非常に似ていると考えています。つまり、控えめに見積もっても実装の 3 分の 1 には不具合があるということです⁴。実質上、大多数の Enterprise 2.0 アプリケーションは、IT 部門の介入を得ることなく企業に侵入します。Andrew McAfee や Dion Hinchcliffe など、この分野における思想的指導者たちは、非公式なユーザー主導のキャンペーンと強力な機能管理サポートを積極的に広めています。テクノロジーの実現者としての役割以外の IT 部門の役割については詳しく述べていません。厳密な構造と監視がないことは、企業内の非常に多くのユーザーがこれらの新しいアプリケーションを採用するきっかけとなり、業務の遂行のためにこれらのアプリケーションを使用する権利があると信じさせる結果となったのです。

Enterprise 2.0 の 3 つの特性

最初に、開発者とその役割に注目しましょう。Enterprise 2.0 アプリケーションを開発する際にほとんどの開発者が悪意を持っていると考えるのは、明らかに間違っています。しかし、現実には、そのようなことが完全にはないとは言いきれません。開発者は従来のほとんどのセキュリティインフラストラクチャによって自分が開発したアプリケーションがブロックされることを知っているため、それを通過する方

⁴ Gartner のアナリスト Neil MacDonald による記事、2009 年 3 月 24 日

法を探します。つまり、通過する方法が見つかるまで、アプリケーションをポートからポートにホップさせたり、または許可されたトラフィックを通じてトンネリングさせたりします。多くの場合、その動機は感染または汚染させることではなく、目的地に到達して機能を果たすことです。しかし、その過程において、本来の意図と悪意の境界線が急速にあいまいになってきました。暗号化についても同じことが言えます。ほとんどの場合、開発者は純粋にユーザーとデータを保護していますが、隠蔽や混乱を目的として暗号化が使用されることも多くなっています。

開発者によってもたらされた共通の問題は、「すべて共有する」というアプローチです。言い換えると、共有によるメリットを得たいなら、他のユーザーが自分との共有によってメリットを得られるようにするということです。多くの場合、この考え方はソフトウェアに直接的に反映されています。つまり、インストール時にデフォルト設定（多くの場合、ソフトウェアの非常に見つけにくい場所に隠されている）によって、ユーザーのファイルがネットワーク上で共有されます。繰り返しますが、ファイル共有は良い例です。Nullsoft、Napster、および KaZaA として始まった技術は、ピアツーピア (P2P) アプリケーション、プロトコル、およびテクノロジーの膨大なコレクションへと進化し、オープンな世界 (LimeWire など) と闇の世界の両方に存在するようになっています。これらのすべてのアプリケーションでは、状況や合法性に関係なく、共有に関して同じ原則が適用されるため、ユーザーの無知が原因で重大な問題が引き起こされています。

率直に言うと、開発者の意図にかかわらず、Enterprise 2.0 アプリケーションにはセキュリティとコンプライアンスに関する明らかな問題があることは明白です。BusinessWeek⁵ の技術レポーターである Steve Hamm は、「レストランで裏口のドアを開けておくと、虫がたくさん入ってくるようなものだ。」と表現しています。

多くの記事や本⁶ に、企業内でユーザーがコラボレーション対応のアプリケーションを使用する動機は何かについて書かれています。その答えは簡単に説明できます。つまり、仕事を終わらせて早く帰宅したいのです。これは非常にありふれたことのように思えます。しかし、生産性に関する議論は動機となるだけでなく、実際の効果を分析することにより証明も可能であるということも、世界中の研究者が認めています。McKinsey は最近、このトピックに関する最も詳細と思われる世界的な研究⁷ を実施しました。この研究では、回答者の 69 パーセントが、製品やサービスの革新、より効果的なマーケティングの実現、知識へのアクセスの改善、業務コストの削減、収益の上昇など、測定可能な事業上のメリットが企業にもたらされたと報告していることがわかりました。この結果によると、テクノロジーを最大限に利用した企業は、さらに大きなメリットを報告しています。成功した企業は、Enterprise 2.0 テクノロジーを従業員のワークフローに緊密に統合するだけでなく、これらのアプリケーションを使用することで、企業を顧客やサプライヤーと結び付ける「ネットワーク化された企業」を作り出しています。

これらの結果は、Enterprise 2.0 アプリケーションの使用についてしばしば論じられる非生産性に関する議論に真っ向から逆らうものです。Enterprise 2.0 アプリケーションを使用することで、セキュリティ、プライバシー、コンプライアンス、および評判に対する本質的なリスクが生じることは明白ですが、従業員が雇用者の時間とリソースを浪費するリスクがあまり大きくないことも明らかになっています。

Enterprise 2.0 アプリケーションは人々の働き方を変化させるだけでなく、コストと時間を削減しながら生産性を向上しており、これに関する圧倒的な証拠に反論するのは困難です。このため、Association for Information and Image Management (AIIM) による最近の研究⁸ において、半数以上の組織が企業目標と成功のために Enterprise 2.0 が「重要」または「非常に重要」と考えていることは驚くに値しません。しかし、リスクがあることは明白であり、安全に導入することが最も重要です。

⁵ BusinessWeek のレポーターである Steve Hamm による[記事](#)、2009 年 11 月 24 日。

⁶ 例は Andrew McAfee 著「[Enterprise 2.0](#)」、Clara Shih 著「[The Facebook Era](#)」より

⁷ McKinsey による[世界的調査](#)、2009 年 9 月

⁸ [AIIM Industry Watch Collaboration and Enterprise 2.0](#)、2009 年 6 月

ここで IT 部門の登場となります。多くの人々は、今日の Enterprise 2.0 に対する IT 部門の影響および介入は最小限に抑えられている、または最小限に抑える必要があると主張しています。この他に、IT 部門は概して Enterprise 2.0 などユーザー主導の動向には無関係であるという意見もあれば、IT 部門はより大きな役割を果たすべきであるという意見もあります。多くの意見がありますが、その理由が述べられることはほとんどありません。

多くの場合、IT 担当者は、他の従業員と同じように Enterprise 2.0 に参加しています。結局のところ、IT 担当者も他の従業員と同様に、業務を遂行することが動機となっています。さらに、IT 担当者は、Enterprise 2.0 アプリケーションに関する問題について、率先的に、あるいは要求に応じてユーザーに対する支援を行うことを求められます。IT 部門は SharePoint などのサーバーベースのインストールを必要とする特定のアプリケーションの導入を依頼されることが一般的ですが、一方で、認可されていないアプリケーションによる不正なサーバーを密かに使用している例も無数にあります。

しかし、ほとんどの場合、IT 部門は、採用後に Enterprise 2.0 に関連する問題に気がきます。IT 部門のヘルプデスクへの問い合わせは、「Facebook のパスワードを忘れました」という無害なものから、2009 年に 100 万台近くのコンピュータに感染した Koobface⁹ のようなエクスプロイトに完全に汚染されるなど、ネットワークとセキュリティに関する重大な問題という極端なケースまで、多岐に及びます。

その役割は賢明なポリシーによる安全な導入を行うこと

Enterprise 2.0 に関する議論と動向において IT 部門がその役割を果たすときがやってきました。IT 部門の最も基本的な役割は、導入、統制、および管理の 3 つです。

導入は、何よりもまず教育に関係しています。Enterprise 2.0 アプリケーションの場合、長い間、ユーザーがそのメリットを判断してきました。しかし、業務に最も適したアプリケーションを選択するための教育を行う機会は今後もあります。IT 部門にはアドバイザーおよびメンターとしての役割があります。つまり、どのアプリケーションが要件を解決するのに最適かをユーザーに示し、選択後にはアプリケーションを活用する方法を示します。一方、導入においては、アプリケーションに関連するリスクに気付かせる役割もあります。そのため、IT 担当者は、一般的に使われている意味とは違う意味で、真のスーパーユーザーになる必要があります。Enterprise 2.0 のスーパーユーザーとは、アプリケーション内部で「生きて」いて、これに依存して主な作業を行う人のことです。IT 部門がその役割を果たすには、偏見を持つことなく本腰を入れて Enterprise 2.0 の採用に取り組む必要があります。これを達成することにより、IT 部門は、Enterprise 2.0 アプリケーションの使用に関連するあらゆるリスクについて、それらを使用することによる社会的な影響および評判への影響に関する事柄も含めて、ユーザーを適切に教育できます。

統制を効果的に行うには、賢明なポリシーを定義する際に IT 部門が重要な役割を果たす必要があります。しかし、IT 部門が、これらのポリシーの唯一の所有者にならないことが重要です。これらのポリシーの有効性と適合性は、IT 部門の昔ながらの考え方の量に反比例するためです。これについては意見が分かれる可能性があります。Enterprise 2.0 アプリケーションは「禁断の果実」になる傾向があります。「聖牛」を殺すこと、つまりポリシーに違反することが、「最高のハンバーガー¹⁰」の材料になるのです。また、ほとんどの場合 Enterprise 2.0 の採用はボトムアップで開始されますが、経営幹部の後援と支援なくして採用はあまり進みません。これが意味しているのは、IT 部門が Enterprise 2.0 アプリケーションの使用を妨げようとしても、採用が成功してしまえば、経営幹部の支援を頼りに禁止することはできないということです。

統制に関する議論では、多くの場合、ソーシャルメディアなど特定のタイプの Enterprise 2.0 アプリケーションを使用するときにユーザーが犯した誤りが例として取り上げられます。これについて議論することは IT 部門にとって簡単なことです。しかし、「ソーシャルメディアでの失敗は避けられない。結

⁹ Wikipedia:Koobface フォーム

¹⁰ 1997 年に出版された Kriegel の有名な本から引用

局のところ、あなたは関係を築いているのであり、完璧な関係など存在しない。¹¹」という理由から、最終的には IT 部門がこの議論の敗者となります。また、Enterprise 2.0 アプリケーションの使用を統制する法律自体が存在しないため、IT 部門がコンプライアンスに基づいて議論を押し進めるのは良い考えとは言えません。結局のところ、業務に適したツールを使用して、それに習熟するしかないので、たとえば、株式取引など厳しく規制された環境では、インスタントメッセージングを使用することは、保持と監査可能性に関する規則の対象となる可能性があります。IT 部門の役割は、各ツールが及ぼす影響についてトレーダーを教育し、使用ポリシーの決定に参加し、使用状況を監視して徹底することです。この例では、ポリシーによってトレーダーがインスタントメッセージングに Facebook チャットを使用するのを防ぎ、一方でその用途に MSN を使用することを許可します。

統制と管理のポリシーは、IT 部門、人事部門、経営管理者、およびユーザーという Enterprise 2.0 を取り巻く 4 つの主な利害関係者によって開発された一連の賢明な企業ポリシーに基づいていけば、非常に適切に機能します。IT 部門に果たすべき役割があるのは明らかですが、多くの場合に見られる二元的な役割であったり、実現者や統制者としての役割があいまいであったりしてはなりません。

Enterprise 2.0 を安全に導入するのに必要なツール

アプリケーション管理を実装して実施します。これは、企業の包括的なセキュリティポリシーに含まれている必要があります。アプリケーション管理ポリシーを実装するプロセスにおいて、IT 部門は Enterprise 2.0 アプリケーションに関して学習するために協調努力する必要があります。これには、すべての使用目的についてこれらのアプリケーションの使用を許可し、必要ならば、アプリケーションの動作を確認するために、ラボ環境において率先してインストールまたは導入することが含まれます。仲間と話し合いを行い、他の IT 専門家に情報を求めるのも効果があります。当然、この情報は意見（数多くの意見があります）ではなく事実に基づいている必要があります。もう 1 つの優れた情報源として、Enterprise 2.0 に焦点を当てた Web サイト、伝言ボード、ブログ、および開発者コミュニティが挙げられます。

問題を無視したり、問題の存在を認めていても「何かが起こる」まで何もしなければ、経験不足に陥る可能性があります。

従業員の管理

Enterprise 2.0 アプリケーションの使用に関するポリシーのガイドラインを策定することは、困難が伴う場合があります。その理由は、使用可能な多くの例があるにもかかわらず、リスクと恩恵の間に大きな葛藤があり、意見が二極化するためです。問題の核心となるのは、IT と人事という、通常は関与している 2 つの組織が、実際には採用に関与していないことです。採用が行われた後に安全に使用するためのポリシーを構築することは、途方もない作業になります。

ポリシーには、非常にシンプルなものから非常に複雑なものまで、数多くの例があります。シンプルな例としては、Microsoft の「Be Smart (賢くなる)」に勝るものはないでしょう。IBM¹² や Intel¹³ などの企業ではより完全なポリシーが使われています。ほとんどの場合、Enterprise 2.0 に関するガイドラインは、全体的な行動準則および個人情報保護方針に含まれています。

どのようなポリシーを策定するにしても、以下に示すいくつかの重要な要素を示す必要があります。

- 「悪質な」アプリケーションが増加しているため、許可されているアプリケーションと禁止されているアプリケーションを従業員はどのように区別するか

¹¹ [Charlene Li](#) (Altimeter Group の設立者で Enterprise 2.0 の専門家)

¹² [IBM Social Computing Guidelines](#)

¹³ [Intel Social Media Guidelines](#)

- 承認されていないアプリケーションの一覧をどのように更新するか、および一覧が変更されたことを従業員に対してどのように周知するか
- 何がポリシー違反になるか
- ポリシー違反に対する処分（解雇または戒告）

数多くの Enterprise 2.0 アプリケーションが、管理可能な企業ネットワークやデバイスだけでなく、従業員のモバイルデバイスにも見られるため、文書化された従業員ポリシーを Enterprise 2.0 の管理の重要な要素にする必要があります。しかし、従業員の管理を Enterprise 2.0 アプリケーションの安全な導入のための単独の管理メカニズムとしても、ほとんど効果がありません。

デスクトップの管理

デスクトップの管理は、以前から IT 部門に大きな課題を提示してきました。デスクトップ管理の細かさと同様に、企業において Enterprise 2.0 アプリケーションを安全に導入するための要素の 1 つです。しかし、Enterprise 2.0 アプリケーションの 72% はブラウザベースであるため、デスクトップ管理の効果は限定されたものになります。

デスクトップ上で実行される 28% のアプリケーションに対してさえ、デスクトップのロックという思い切った措置を取ってユーザーが自身のアプリケーションをインストールすることを防ぐのは、口で言うほど簡単な作業ではありません。

- ラップトップのリモート接続、インターネットからのダウンロード、USB ドライブ、および電子メールはすべて、承認されているアプリケーション、または承認されていないアプリケーションをインストールする手段となります。
- 当然のことながら管理者権限を完全に奪い取るのは困難であり、場合によってはエンドユーザーの機能を制限することにもなります。
- 今では USB ドライブでアプリケーションの実行も可能なため、事実上、ネットワーク権限が与えられていれば Enterprise 2.0 アプリケーションにアクセスできます。

デスクトップの管理は、Enterprise 2.0 アプリケーションを安全に導入するためのやや制限的な手段として、文書化された従業員ポリシーを補足できます。

ネットワークの管理

ネットワークレベルで必要とされるのは、Enterprise 2.0 アプリケーションを識別して、ブロックまたは管理する手段です。ネットワークレベルの管理を実装することによって、IT 部門は、Enterprise 2.0 アプリケーションの使用によって脅威と混乱が生じる可能性を最小限に減らすことができます。ネットワークレベルでは複数の管理メカニズムを使用できますが、いずれのメカニズムも有効性の低下につながる欠点を持っています。

- ステートフルファイアウォールを防御の最前線として使用することにより、トラフィックを大まかにフィルタリングし、パスワードで保護された異なるゾーンにネットワークをセグメント化することができます。ステートフルファイアウォールの短所の 1 つは、ネットワークに出入りするデータを識別して管理するためにプロトコルとポートを使用することです。このポート中心の設計は、ネットワークに対して開かれた接続を見つけるまでポートからポートにホップする Enterprise 2.0 アプリケーションに対処するときは、あまり効果がありません。
- ファイアウォールの展開に IPS を加えると、トラフィックのサブセットを監視し、既知の脅

威または悪質なアプリケーションをブロックできるため、ネットワークの脅威を予防する機能が向上します。IPS 製品にはアプリケーションに関する理解、およびすべてのポートのすべてのトラフィックを監視するのに必要なパフォーマンスが不足しているため、完全な解決策と見なすことはできません。

- IPS テクノロジは、一般的にパフォーマンス低下を防止するためにトラフィックの一部だけを監視するように設計されているため、今日の企業で必要とされる幅広いアプリケーションをカバーすることはできません。また、ファイアウォールと IPS を組み合わせて管理することは、通常は手間のかかる作業であり、個別のポリシーテーブルを参照する異なる管理インターフェースが必要になります。簡単に言うと、現在のお手軽なソリューションには、今日のアプリケーションの可視性と管理の要件を解決するための精度、ポリシー、またはパフォーマンスが欠けています。
- プロキシによるソリューションはトラフィック管理の手段の 1 つですが、一部のアプリケーションまたはプロトコルしか監視しないため、監視を必要とするトラフィックの一部しか監視されません。このため、Enterprise 2.0 アプリケーションは、プロキシによってブロックされたポートを見つけると、開いている次のポートにホップします。設計上、プロキシは管理対象となるアプリケーションを模倣する必要があるため、既存のアプリケーションのアップデートと新しいアプリケーション用のプロキシの開発には苦勞が伴います。他にも、プロキシによるソリューションによって生じる問題として、プロキシがどのようにアプリケーションを終了させ、その後、どのように宛先に転送するかによってスループット性能が決まる場合があります。

これらのネットワーク管理の課題は、Enterprise 2.0 アプリケーションを識別する機能を持っていないこと、トラフィックの一部しか監視しないこと、およびパフォーマンスに問題があることです。

Palo Alto Networks の次世代ファイアウォールの使用

Palo Alto Networks は、トラフィックの分類にアプリケーション中心のアプローチを取り入れた高性能ファイアウォールを提供し、使用するポート、プロトコル、SSL 暗号化、または回避策に関係なくネットワークを通過するすべてのアプリケーションを正確に識別することによって、既存のネットワーク管理ソリューションで発生する問題の多くを回避します。Palo Alto Networks では、App-ID™ という新しいトラフィック分類テクノロジーを使って今日の多くの新しいアプリケーションで一般的に使用されているセキュリティ回避策に対応することによって、IT 部門がネットワークレベルで Enterprise 2.0 アプリケーションに対する管理能力を回復するのを支援し、デスクトップおよび従業員の既存の管理メカニズムを補足します。

App-ID™ は、ネットワークを出入りする 900 を超えるアプリケーションを正確に識別します。その中には、200 を超える Enterprise 2.0 アプリケーションも含まれます。Palo Alto Networks ファイアウォールを通過するすべてのトラフィックは App-ID™ によって処理され、Enterprise 2.0 アプリケーションまたはそれ以外のアプリケーションの ID が一般的なアプリケーション名を使用して管理インターフェースに表示されます。その後、アプリケーションの ID は、アクセス制御、ユーザー権限、脅威予防など、すべてのファイアウォールのセキュリティポリシーの基礎として使用されます。

Enterprise 2.0 アプリケーションの識別

Palo Alto Networks の App-ID™ では、連携して動作する複数のトラフィック分類メカニズムを使用して、どのアプリケーションがネットワークを通過しているかを正確に判断します。App-ID™ では、使用されている既知のポートのサブセットだけではなく、すべてのポートを通過するトラフィックを確認するため、アプリケーションを検出する確率が高くなります。Palo Alto Networks では、トラフィックの分類にアプリケーション中心のアプローチを取り入れることによって、既存のファイアウォールをバイパスするための非標準ポートの使用、ポートおよびプロトコルの動的な変更、他のアプリケーションのエミュレーション、およびトンネリングなど、Enterprise 2.0 アプリケーションによって使用されるセキュリ

ティ回避策に対処します。結果として、App-ID™ は 200 を超えるさまざまな Enterprise 2.0 アプリケーションを識別できます。

トラフィックがネットワークを通過するとき、App-ID™ はアプリケーションのセッションを確立してセッションの状態を維持します。このとき、追加のアプリケーション識別メカニズムがトラフィックをより正確に分類し、管理します。App-ID™ には 4 つのトラフィック分類メカニズムがあります。その中で Enterprise 2.0 を識別するために使用されるのは、アプリケーションデコーダとアプリケーションシグネチャという 2 つのメカニズムです。

- アプリケーションデコーダ: App-ID™ によるアプリケーションのデコードには 2 つの目的があります。第 1 に、Skype など、より複雑で回避機能を持つアプリケーションを識別することです。また、アプリケーションシグネチャを適用する機能を持っているだけでなく、トラフィックに対して、より複雑なパターンマッチング処理を実行できます。第 2 に、連続的なアプリケーションのデコードに使用することにより、セッションを通して脅威検出を実行し、このプロセスの実行中にアプリケーションの異常と変更を探すことができます。
- アプリケーションシグネチャ: 特定のアプリケーションを識別することに焦点を合わせたコンテキストベースのシグネチャで、一意のアプリケーション特性と関連する情報交換を探すことにより、トラフィックを正確に識別します。アプリケーションシグネチャでは、非標準のポートをトンネリングしたり、HTTP などのキャリアアプリケーションを模倣している場合でも、広範に及ぶアプリケーションを識別できます。

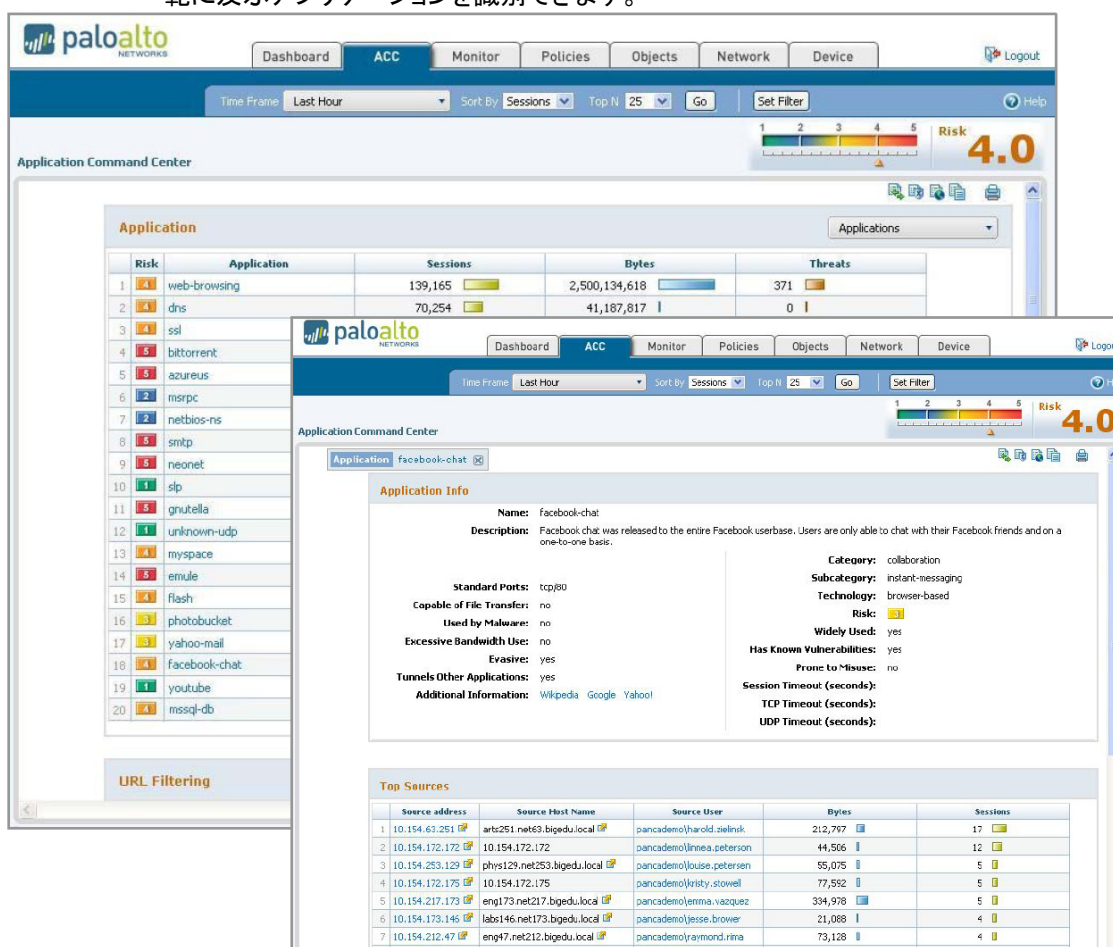


図 3: Application Command Center (背後の画面) には、アプリケーションの活動に関する現在のビューが表示され、Facebook チャットなど特定のアプリケーションの詳細がドリルダウンして表示されます (前面の画面)。

App-ID™ によって Enterprise 2.0 アプリケーションが識別されると、管理者は、アプリケーション名とともに、セッション、バイト、脅威、送信元/送信先の IP アドレス、および時間によって分類されたマイクロレベルまたマクロレベルのデータを使用して、どのアプリケーションがネットワーク上で実行されているかをすばやく正確に確認できます。Enterprise 2.0 アプリケーションの Facebook チャットをクリックすると、管理者は、アプリケーション、そのために生じる脅威、それを使用しているユーザー、および消費している帯域幅に関する詳細をドリルダウンできます。

さらに管理者は、IP アドレスに基づいて、または Active Directory プロファイルの特定のユーザーおよびグループに基づいて、だれがアプリケーションを使用しているかを確認できます。さらに、送信元および送信先となる上位 10 か国が含まれているため、管理者はトラフィックがどこに流れているかを確認することができます。Enterprise 2.0 アプリケーションがネットワークを通過している状態を可視化できるため、管理者は、従来のファイアウォールに似たポリシーエディタからセキュリティポリシーを実装できます。

Enterprise 2.0 アプリケーションへの積極的な管理 (ファイアウォール) ポリシーの適用

管理者は、Enterprise 2.0 アプリケーションを識別した後、ルールベースのエディタを使用して、Facebook チャットのようなアプリケーションに対するアプリケーション使用管理ポリシーを作成できます。または、安全性を高め、対象範囲を広げるために、インスタントメッセージンググループに対するポリシーを設定し、現在識別されているインスタントメッセージングアプリケーションをすべてカバーできます。ポリシーエディタでインスタントメッセージンググループを選択する利点は、現在のアプリケーションだけでなく、将来的に追加されるアプリケーションもすべて検出できることです。Palo Alto Networks の開発チームが新しいアプリケーションを追加すると、追加されたアプリケーションは、Palo Alto Networks の動的アップデートサービスによって自動的にカバーされます。



図 4: インスタントメッセージングアプリケーションに対する個人のポリシー

管理者はインスタントメッセージングアプリケーションをすべてブロックしたい場合もあれば、企業が顧客と連絡を取るために Facebook チャットを使用する場合など、重要な個人に限って Facebook チャットの使用を許可する特別なルールを実施したい場合もあります。このような場合には、Facebook チャットなどのアプリケーションを選択し、その後に Active Directory の情報に基づいて Facebook チャットの使用が許可されている特定のユーザーを選択できます。



Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	Options
1 Control IM	trust	untrust	any	pancademo/remote desktop users pancademo/remote web workplace users	any	Instant_messaging	any	allow		
2 Monitor ALL	tapzone	tapzone	any	any	any	any	any	deny		
3 Block P2P	trust	untrust	any	any	any	P2P Filesharing	any	deny	none	
4 Webmail - No Attachments	trust	untrust	any	any	any	Webmail Group	any	deny		
5 CEO Apps	trust	untrust	any	pancademo/harold.melak	any	CEO Apps	any	allow		
6 Block High Risk Media	trust	untrust	any	any	any	High Risk Media	any	deny	none	
7 Allow IT Remote Access	trust	untrust	any	pancademo/administrators	any	IT Remote Access	any	allow		
8 CFO Wirecraft	trust	untrust	any	pancademo/julia.stiller	any	worldofwirecraft	any	allow	none	
9 Block Remote Access	trust	untrust	any	any	any	Remote Access	any	deny	none	
10 Control Finance Web Posting	trust	untrust	any	pancademo/finance	any	Web Posting	any	deny	none	
11 General Web	trust	untrust	any	any	any	web-browsing	any	allow		
12 Inbound SMTP	untrust	trust	any	any	10.0.0.250	smtp	application-default	allow		
13 Corp Webserver	untrust	trust	any	any	10.0.0.249	web-browsing	application-default	allow		
14 SSL Web access	untrust	untrust	any	any	any	any	any	allow		

図 5: インスタントメッセージングアプリケーションに対するグループポリシー

展開の柔軟性

Palo Alto Networks は、Enterprise 2.0 アプリケーションを管理する最も適切な場所は、すべてのトラフィックが通過するネットワーク内の戦略ポイント、つまりファイアウォールであると考えています。Virtual Wire モード（周囲のデバイスに対して完全に透過的）、レイヤー 2、またはレイヤー 3 モードを含む堅牢なネットワーク基盤によって柔軟な展開が可能になるため、以下に示す 3 つのモードのいずれかでインストールできます。

- **タップモード:** Palo Alto Networks の次世代ファイアウォールを SPAN ポート経由でネットワークに接続すると、IT 部門はトラフィックをリアルタイムに監視でき、既存のインフラストラクチャを混乱させることなく、どのアプリケーションがネットワークを通過しているかを正確に示すデータが IT 部門に提供されます。
- **インラインの透過モード:** Palo Alto Networks の次世代ファイアウォールは、Virtual Wire モードを使用して、既存のセキュリティインフラストラクチャに対してインラインで補足的かつ完全に透過的に展開されるため、IT 部門は必要に応じてアプリケーションの管理を開始できます。
- **プライマリファイアウォール:** Palo Alto Networks の次世代ファイアウォールは、従来のファイアウォールアプリケーション、プロトコル、およびアクセス制御機能を完全にサポートすることで、既存のファイアウォールと同じ許可/拒否機能を実行できるため、プライマリファイアウォールソリューションとして利用できます。

結論

Palo Alto Networks は、Enterprise 2.0 アプリケーションの管理に最も適した場所は、すべてのトラフィックが通過するネットワーク内の戦略ポイント、つまりファイアウォールであると考えています。問題は、ブロックするべきか、ブロックしないべきかということではありません。Enterprise 2.0 を採用することで生産性とコストにメリットがあるという証拠は世界中に数多くあります。問題は、企業が賢明かつ安全な導入を実現するポリシーをどのように定義して実施するかということです。

Palo Alto Networks について

Palo Alto Networks™ はネットワークセキュリティ会社です。Palo Alto Networks の次世代ファイアウォールは、アプリケーションとコンテンツの他に例を見ない可視性と高度なポリシー制御を可能にし、それらを IP アドレスだけでなくユーザーベースで、パフォーマンスを低下させることなく、最大 10 Gbps で実現します。特許出願中の App-ID テクノロジーを基礎とする、Palo Alto Networks のファイアウォール製品群は、ポート、プロトコル、回避策や SSL 暗号化にかかわらず、アプリケーションを正確に識別および制御し、コンテンツをスキャンすることで脅威を抑制し、データの漏洩を防ぎます。企業は、デバイス統合によって総所有コストを大幅に削減することができるうえ、Web 2.0 を初めて採用することによって、完全な可視性と管理を維持することができます。詳細は、<http://www.paloaltonetworks.com> を参照してください。