ソリューション概要

サイバーセキュリティーおよびネットワーク性能監視
アプリケーションの高速化

サイバーセキュリティーおよびネットワーク監視用アプリケーションの高速化

インテル® FPGA プログラマブル・アクセラレーション・カード (インテル® FPGA PAC) 対応 Napatech Link* キャプチャー・ソフトウェアでアプリケーションの性能を向上

概 要

このソリューション概要では、インテル® FPGA プログラマブル・アクセラレーション・カード (インテル® FPGA PAC) 上で動作する Napatech の Link* キャプチャー・ソフトウェアが、主要なサイバーセキュリティーおよびネットワーキング・アプリケーションをどのように高速化できるかについて説明します。

このソリューションは、サーバーのインテル® Xeon® CPU コアから最も過酷な処理ワークロードを取り除き、重要なコンピューティング・リソースを本来の用途であるアプリケーションやサービスへと振り向けます。こうした方法を採用することで、標準的なネットワーク・インターフェイス・カード (NIC) のデプロイメントと比較して、パフォーマンス上の損失を大幅に削減できます。

ビジネス上の課題 : 性能を犠牲にすることなく標準デプロイメントのメリットを享受

クラウドサービス、5G モバイル通信、および IoT の到来は、企業によるネットワークの設計、管理、保護の方法に対して大きな影響を及ぼしています。

デプロイメント次第では、標準的な NIC を搭載した低コストのサーバーでも性能要件を十分に満たすことが可能です。しかし、多くのアプリケーションやサービスは、計算量が多く CPU リソースに大きな負担をかけるワークロードやプロセスによって定義されてしまいます。そしてこのようなデプロイメントにとって、標準的な NIC では通常不十分であり、ネットワーク・パケットの重大な損失やアプリケーションの性能の低下を招きます。

サイバーセキュリティーとネットワーク性能の監視では、このプロファイルに適合するアプリケーション・タイプとして、侵入検知システム (IDS)、侵入防止システム (IPS)、ネットワーク・フォレンジック、合法的傍受、ネットワークの記録と再生、分析と監視、テストと測定、ネットワークとアプリケーション性能の監視などに加えて、増え続ける内製の IT アプリケーションが挙げられます。すべ

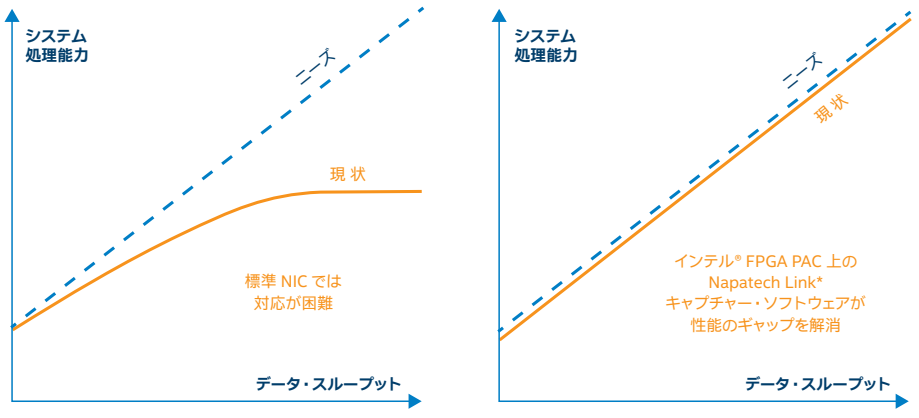

図 1. インテル® FPGA PAC で標準 NIC と Napatech Link* キャプチャー・ソフトウェアを使用したセキュリティーおよびネットワーク監視用アプリケーションに必要な CPU 処理の比較

著 者

Jarrod J.S. Siket
Napatech
Chief Marketing Officer

Sven Olav Lund
Napatech
Software & Solutions
Director, Product Management

てに共通しているのは、どんなにセッション、ユーザー、フローが多くても、すべてのサイズのパケットにおいて100%ロスのないパケット転送とキャプチャーを可能にするラインレート・ネットワーク・スループットが無条件に要求されることです。これらのアプリケーションの性質上、トラフィックが少しでも失われると、アプリケーションの価値が失われます。

制御の実現に欠かせない可視性

セキュリティー・チームにとっては、1つのパケットが失われても死角が生じて、フォレンジック調査全体が役に立たなくなる可能性があるため、すべてのネットワーク・トラフィックを完全に把握することが不可欠です。同様に、ネットワーク運用チームにとって、完全かつ信頼性の高いネットワーク・テストとトラブルシューティングを実行し、最適なサービス品質を実現し、ネットワークや機器への過負荷を回避するには、完全なキャプチャーが必須です。

企業のこうした課題克服を支援するために、Napatechは、インテル® プログラマブル・アクセラレーション・カード（インテル® Arria® 10 GX FPGA搭載版）対応のアクセラレーション・スタックとして、Link* キャプチャー・ソフトウェアを提供しています。このソリューションにより、標準的な低コストのサーバーをベースにした高性能プラットフォームの構築が可能になりました。標準的なNICでは、対象アプリケーションにおいて許容できないパケットロスに常に悩まされてきましたが、Napatechを採用することですべてのパケットサイズで、ゼロ・パケットロスのラインレート・スループットが保証されます。これはネットワーク性能、テスト、セキュリティー分析の信頼性を確保するためには不可欠です。

Napatech Link* キャプチャー・ソフトウェアは、インテル® FPGA PACに搭載された強力なインテル® Arria® 10 GX FPGAを利用して、最大40 Gbpsまでのすべてのパケットサイズでラインレートのパケット・キャプチャーとフロー対応転送を実現します。このソリューションは、最も負荷の高いネットワークおよびセキュリティー処理のワークロードから、サーバーのインテル® Xeon® CPUコアを解放して、重要なコンピューティング・リソースを本来のアプリケーションおよびサービスへと振り向けます。

ユースケース

あらゆる種類のネットワーク事業者が、ソフトウェア・ベースのネットワークおよびセキュリティー・アプリケーションを使用しています。これには、クラウド・データセンター事業者、電話会社およびケーブルのサービス・プロバイダー、Fortune 5000企業、および政府機関が含まれます。これらの業界では、Linux* ベース、サードパーティー、自社製、オープンソース、および市販のネットワーキング / セキュリティー・ソフトウェア・アプリケーションを展開しています。

ソリューションのメリット

- メリット1：すべてのサーバーにおいてアプリケーションの性能が向上します。
- メリット2：ラックスペース、電源、冷却、管理に関連する運用コストを削減しながら、目標性能を達成するために必要なサーバーの数を減らすことでシステムコスト全体を削減します。
- メリット3：SmartNICのFPGAベースのコプロセッサーの計算能力の追加により、複雑なタスクによって消費される時間を削減します。
- メリット4：可視性の欠如によって高コストになりがちなミッション・クリティカルなビジネスツールに対して、ネットワーク通信の完全な可視性により、パケットロスのないキャプチャーおよび転送を保証します。

Napatechとインテルを組み合わせたソリューションは、サイバーセキュリティー用のSuricata*、ネットワーク性能監視用のn2disk*、ネットワーク性能監視用のWireshark*、トラフィック生成用のTRexなど、いくつかの主要なサードパーティー製、市販、およびオープンソースのアプリケーションに対して測定可能で再現性のある優れたベンチマーク結果を提供します。

改善効果には2つの主な側面があります。まず、FPGAベースのハードウェアとNapatech Link* キャプチャー・ソフトウェアは、ホストCPUリソースを過度に消費する負荷の高いワークロードを軽減し、その貴重なコアを本来の目的であるアプリケーションやサービスに振り向けます。第2に、FPGAの存在により、システム内部の計算能力が向上します。こうした2方向からのコンピューティング能力の向上は、以下のベンチマークで示されるように、アプリケーションの性能を劇的に増大させます。

アプリケーション	リンク
Suricata*	https://suricata-ids.org/（英語）
Snort*	https://www.snort.org/（英語）
Bro	https://www.bro.org/（英語）
Wireshark*	https://www.wireshark.org/（英語）
TRex	https://trex-tgn.cisco.com/（英語）
ntop* nProbe* Cento	https://www.ntop.org（英語）
ntop* n2disk*	https://www.ntop.org/（英語）
内製のIT	
その他の市販アプリケーション	

表1. Napatech Link* キャプチャー・ソフトウェアでサポートされているアプリケーション

サイバーセキュリティー : Suricata* IDS

Suricata* IDS は、既知の脅威、ポリシー違反、および悪意のあるアクティビティーを検出します。しかし、Suricata* はネットワークを事後対応的には保護できますが、その効果は Suricata* の実装と比例します。すべてのネットワーク・パケットの内容を調べることは、特にマルチギガビットのトラフィック負荷の場合、非常に CPU に負荷がかかります。これによって、Suricata* の性能、つまり CPU のパケット処理能力が制限されてしまうことが少なくありません。

インテル® FPGA PAC および Napatech Link* キャプチャー・ソフトウェアによるソリューションは、Suricata* の損失を伴わないアクセラレーションに最適です。すべてのネットワーク・トラフィックをフルラインレートでキャプチャーするように最適化されており、どんなフレームサイズでもホストサーバーに CPU 負荷がほとんどかからないため、このソリューションは標準 NIC と比較して、大幅なロスレス性能という利点を Suricata* にもたらします。

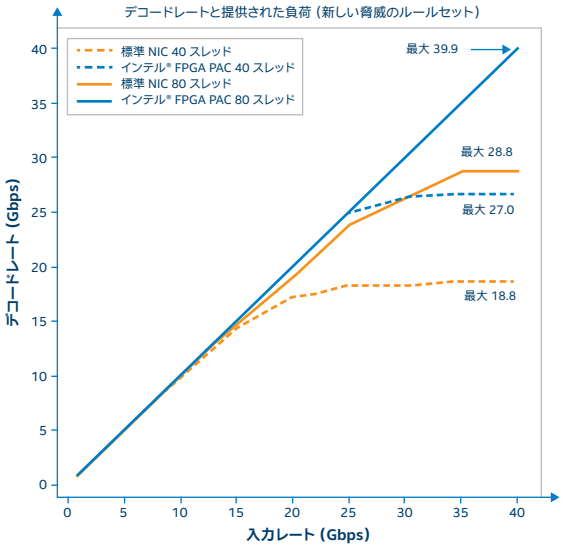

図 2. サイバーセキュリティーの最大スループットの向上

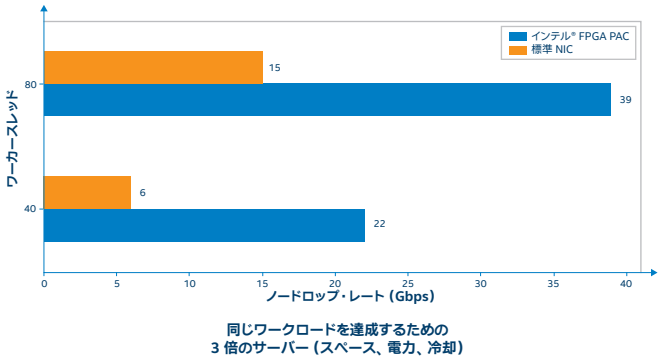

図 3. サイバーセキュリティーのロスレス・スループットの向上

ネットワーク・レコーディング : n2disk*

n2disk* は、ライブ・ネットワークからマルチギガ・ビットレートでネットワーク・パケットをキャプチャーし、保存することを可能にする強力なネットワーク・トラフィック・レコーダー・アプリケーションです。n2disk* を使用すると、セキュリティー・チームはすべてのネットワーク・データのオンデマンドでの捕捉、保存、取得が可能となり、ベクトル識別、フォレンジック分析、または運用上のトラブルシューティングのための遡及的パケット・キャプチャー (PCAP) の証拠を手に入れることができます。

n2disk* を効果的に活用するための前提条件は、すべてのネットワーク・パケットを損失ゼロでキャプチャーできることです。しかし、数ギガビットのトラフィック負荷によって、標準的なサーバーのデプロイメントでは対応が不可能となることがよくあります。

インテル® FPGA PAC と Napatech Link* キャプチャー・ソフトウェアによるソリューションは、n2disk* に極めて優れた性能上の利点をもたらします。

- 最大 3 倍のロスレスパケット - ディスク・パフォーマンス
- 最大 600 ミリ秒のパケットバーストのディスクへのキャプチャー保証

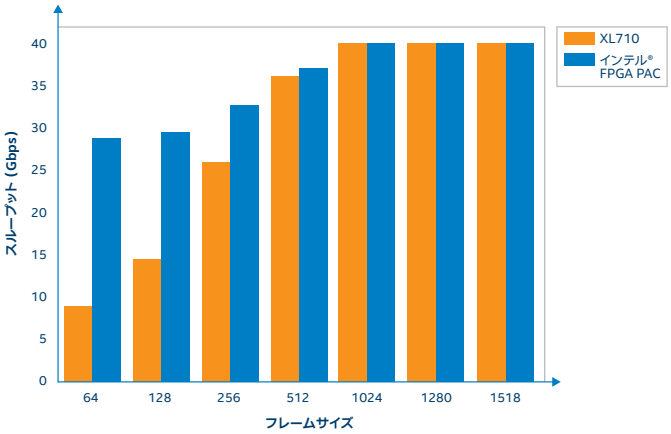

図 4. n2disk* のスループット

ネットワーク性能監視 : Wireshark*

Wireshark* は広く使用されているネットワーク・プロトコル・アナライザーで、ユーザーは自分のネットワークで何が起きているのかを詳細に確認できます。多くの民間企業および非営利組織、政府機関、教育機関などにおいて、トラブルシューティングとプロトコル分析のためのデファクト・スタンダードとなっています。

Wireshark* が効率的に動作するためには、トラフィックを損失ゼロでキャプチャーおよび分析する機能が決め手となります。すべてのトラフィックをデコードするには、Wireshark* が「すべてを見る」ことが基本的な要件です。トラフィックが見逃された場合、完全なプロトコル分析は不可能となります。また、キャプチャー・サーバーが過負荷状態となり、受信パケットレートを処理するには遅すぎる場合、パケットは破棄され、情報は永久に失われます。

インテル® FPGA と Napatech Link* キャプチャー・ソフトウェアによるソリューションはキャプチャーとプロトコル解析を劇的に向上させ、ネットワーク・エンジニアが Wireshark* の全機能を利用してネットワーク・トラフィックを理解し、異常を発見し、そしてネットワークの問題を驚異的な速度で診断できるように支援します。このソリューションは、Wireshark* にとって非常に高いロスレス性能の利点をもたらし、標準的な NIC と比較して、最大 7 倍のロスレス・キャプチャーおよびデコード性能を実現します。

トラフィック生成 : TRex

TRex は、オープンソース、低コスト、ステートフル、ステートレスのトラフィック・ジェネレーターです。他のトラフィック生成ソリューションと同様に、すべてのパケットサイズにわたってラインレートでパケットを確実に生成する TRex の能力には注意が必要です。テストのために単にパケットをブラストするか、PCAP ファイルを実行するかにかかわらず、小さいパケットのトラフィックを最大速度で送信できることが前提条件です。

トラフィックの受信も非常に重要です。テスト対象デバイス (DUT) を通過した後に生成されたトラフィックを受信する機能は、ソリューションの有効性を測定する唯一の方法です。トラフィック受信が生成能力と一致しない場合、トラフィックをドロップ (欠落) させているのが DUT なのかテスト機器自体なのかを識別できないため、テストの効果そのものが損なわれます。損失ゼロの送受信用に最適化されたインテル® FPGA PAC と Napatech Link* キャプチャー・ソフトウェアによるソリューションは、標準的な NIC と比較して、TRex の性能を大幅に向上させます。

- 2 倍のトラフィック生成性能
- 4 倍のトラフィック受信性能

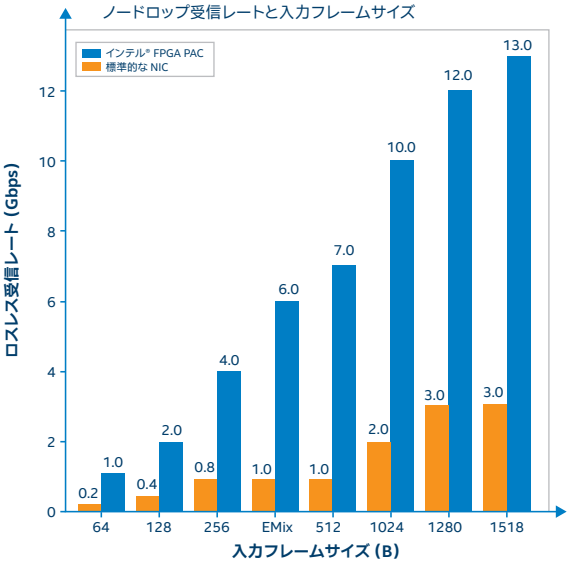

図 5. Wireshark* のロスレス・スループット

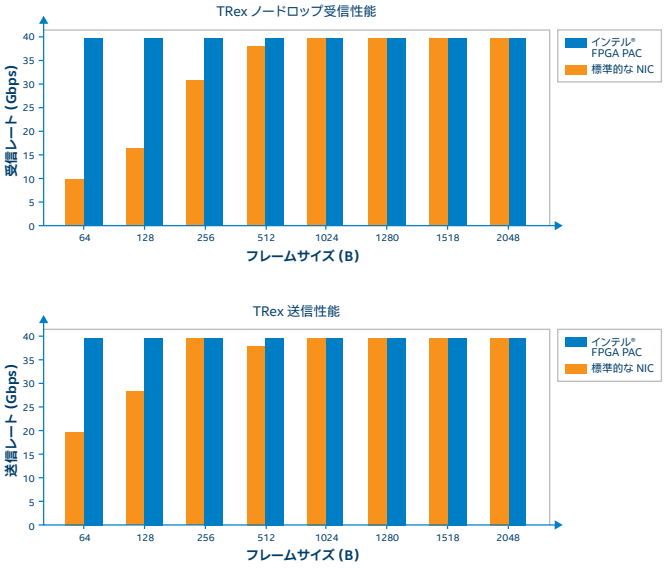

図 6. フレームサイズによる TRex ノードロップ受信性能と送信性能

お客さまの声

「インテル® FPGA PAC 用の Napatech の Link* キャプチャー・ソフトウェアは、今日の企業に見られるネットワーキングおよびセキュリティー・アプリケーションに対する大きな需要をもたらします。大手サーバーメーカーからインテル® FPGA 搭載製品が発売されるようになり、FPGA ベースのアクセラレーションが普及し、現在では主流となりました」(ntop 創設者、Luca Deri 氏)

ソリューションの価値

インテルと Napatech のソリューションによるアプリケーションの高速化は、測定可能な価値を直ちにもたらします。第 1 に、ユーザーはどんなサーバーからでも、より高いアプリケーション性能を得られます。個々のアプリケーションの改善点はさまざまですが、個々のサーバーとそのアプリケーションは、性能に関する相乗効果の恩恵を受けられます。第 2 に、事業者は、目標とする性能を達成するために使用するサーバーの数を減らすと同時に、ラックスペース、電源、冷却、管理に関連する運用コストを削減することで、システムコストを大幅に削減できます。第 3 に、FPGA ベースのコプロセッサーがもたらす計算能力により、複雑なタスクの実行にかかる時間が大幅に短縮されます。最後に、このソリューションはパケット損失ゼロのキャプチャーと転送を確実にし、可視性の欠如が致命傷となるようなミッション・クリティカルなビジネスツールが必要とするネットワーク通信に対して完全な可視性を保証します。

これらの利点は、顧客組織内の以下の主要な利害関係者にとって価値があります。

- 財務部門および CFO は、ネットワーキング、サイバーセキュリティー、規制遵守のために導入される機器の設備投資 (CAPEX) と運用コスト (OPEX) を大幅に削減し、その上、IT 予算内に収まるソリューションの選択肢を手に入れることができます。オープンかつ標準的な大容量サーバーをベースにしたこれらの新しいソリューションにより、高価で専用の垂直統合型ハードウェアをわずかなコストで置き換えることが可能なります。さらに、ソフトウェア主導でフィールド・プログラマブルであるため、固定機能のハードウェアやカスタム・ハードウェアよりも長期的な運用が可能で、常に最新のイノベーションを提供します。
- ネットワークの設計、展開、運用、管理を行うチームは、性能、機敏性、コストを比較して選択する必要がなくなります。インテルのネットワーク・ハードウェアと Napatech のソフトウェアを搭載した標準サーバー・プラットフォームは、幅広いアプリケーションに対して 1 つのプラットフォームで対応でき、あらゆる利点を提供します。
- 内製のビジネス・アプリケーションを設計するアプリケーション設計者および DevOps は、ソフトウェア・イノベーションのスピードでハードウェア性能を提供する高性能ネットワーキング・プラットフォームを利用できるようになります。

ソリューション・アーキテクチャー : インテル® FPGA PAC 上の Napatech Link* キャプチャー・ソフトウェアによるアプリケーションの高速化

完全なソリューションは、以下のコンポーネントで構成されています。

- インテル® FPGA PAC をサポートする標準的なサーバー・プラットフォーム (Dell、Fujitsu、HP プラットフォームなど)
- インテル® PAC インテル® Arria® 10 GX FPGA 搭載版
- インテル® Open Programmable Acceleration Engine (OPAE) ソフトウェア
- Napatech Link* キャプチャー・ソフトウェアおよびライセンス
- エンドカスタマーによって選択されるユースケース固有のアプリケーション・ソフトウェア

この製品は、以下のような固有の主要機能を提供します。

- すべてのパケットサイズで最大 40 Gbps の双方向の完全理論スループット
- 10 Gbps と 40 Gbps の両方の設定をサポート
- あらゆる条件下でパケット損失がゼロ
- 確定的なパフォーマンス
- すべてのパケットの正確なタイムスタンプ
- PCAP およびデータプレーン開発キット (DPDK) アプリケーション・プログラミング・インターフェイス (API) のサポート

このソリューションは 40 Gbps イーサネット (GbE) x 1 構成および 10 GbE x 4 構成をサポートし、PCAP および DPDK ホスト API に基づいて構築されているため、市販、内製、およびオープンソースのアプリケーションとの統合が簡単です。

Napatech には、インテル® FPGA PAC への移植を継続するのに理想的なソフトウェア機能とユースケースの広範なライブラリーがあり、フットプリントの拡大に向けて主要なアプリケーションに関する新しいベンチマークが定期的に公開されています。

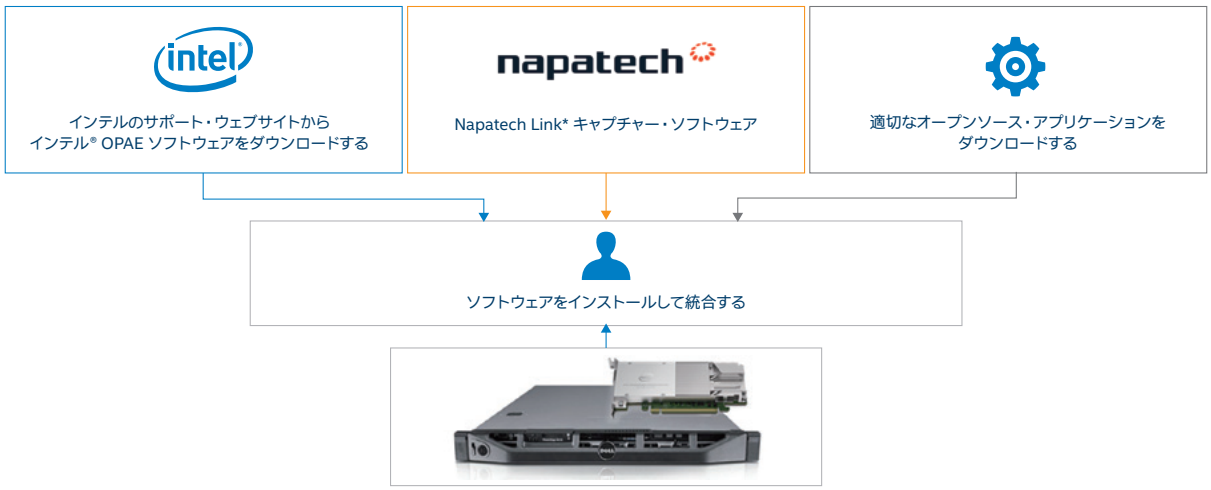

図 7. Napatech Link* キャプチャー・ソフトウェアをベースとしたソリューションの発注と導入の流れ

まとめ

汎用的なコンピューティング・アーキテクチャーはあるレベルまでのデプロイメントには十分ですが、サイバーセキュリティーおよびネットワーク監視用アプリケーションに関しては、計算量が多いワークロードによる制限が生じます。このようなデプロイメントでは、標準的なNICでは十分な効果が得られないことが多く、ネットワーク・パケットの重大な損失とアプリケーションの性能低下を招きます。

インテル® FPGA PACとNapatech Link* キャプチャー・ソフトウェアのソリューションを使用することで、こうした性能のギャップへの対処が可能になります。このソリューションにより、あらゆる規模のIT組織が標準的なサーバーにサイバーセキュリティーおよびネットワーキング・アプリケーションを展開して、カスタム・ハードウェアに比べてほんのわずかなコストで圧倒的な性能を実現できます。

さまざまなサードパーティー、市販、およびオープンソースのLinux*ベースのネットワーキングおよびサイバーセキュリティー・アプリケーションのベンチマークによって検証されたこのソリューションは、標準的なNIC構成を使用したサーバー上でのアプリケーション性能を大幅に向上させることができます。

自分たちの組織に合った適切なソリューションを見つけましょう。詳細については、インテルの担当者にお問い合わせいただくか、http://www.napatech.com/(英語)を参照してください。

ソリューション・プロバイダー

Napatechについて

Napatechは、あらゆる規模のIT組織に大規模コンピューティングのメリットをもたらすことで、ビジネスの再構築を目指す企業を支援します。Napatechは、オープンかつ標準的な仮想化サーバーを強化してイノベーションを促進し、サービスを向上させ収益を増大させる重要なコンピューティング・リソースを解放します。

NapatechのReconfigurable Computing Platform*は、幅広いFPGAハードウェア設計でサポートされている、最先端のITコンピューティング、ネットワーク、およびセキュリティー・アプリケーション向けの幅広いFPGAソフトウェアに基づいています。

詳細情報

次のリソースも参照してください。

- パートナー企業

  http://www.napatech.com/(英語)

  http://www.intel.com/content/www/us/en/programmable/solutions/partners/partner-profile/napatech.html(英語)

- 製 品

  http://www.napatech.com/products/link-capture-software-for-intel/(英語)

- その他の関連資料

  Napatech Link* キャプチャー・ソフトウェア製品概要(英語)

  Napatech Link* キャプチャー・ソフトウェア機能概要(英語)

  Suricata*のインストールと操作のアプリケーション・ノート(英語)

Napatechシステム構成:

Dell* PowerEdge* R740、インテル® Xeon® Gold 6138 CPU x 2、2GHz、20コア、40スレッド、128GB RAM(8GB RDIMM x 16、2666MT/秒)、インテル® PACインテル® Arria® 10 GX FPGA搭載版(40 GE x 1)、NIC:インテル® イーサネット・ネットワーク・アダプター XL710-QDA2(40 GE x 2)、光トランシーバー:40GBASE-SR4 QSFP + 850nm 150m MTP / MPO光トランシーバー・モジュール、Napatech Link* キャプチャー・ソフトウェアv11.1.4、Linux*:CentOS* Linux*リリース7.3 - Linux* カーネルバージョン3.10.0-957.1.3.el7.x86_64、Suricata*バージョン:4.0.5。Suricata*は侵入検知モードで使用されます。トラフィックは一方向に送信され、スループットはアプリケーションによって報告された統計情報を使用して測定されます。

テストはNapatechによって実施されました。インテルは、サードパーティーのデータについて管理や監査を行っていません。記載内容について検討し、ほかの情報も参考にしながら、本資料で参照しているデータが正しいかどうかを確認してください。

インテル® テクノロジーの機能と利点はシステム構成によって異なり、対応するハードウェアやソフトウェア、またはサービスの有効化が必要となる場合があります。実際の性能はシステム構成によって異なります。絶対的なセキュリティーを提供できるコンピューター・システムはありません。詳細については、各システムメーカーまたは販売店にお問い合わせいただくか、http://www.intel.co.jp/を参照してください。

インテルは、明示されているか否かにかかわらず、いかなる保証もいたしません。ここにいう保証には、商品適格性、特定目的への適合性、および非侵害性の黙示の保証、ならびに履行の過程、取引の過程、または取引での使用から生じるあらゆる保証を含みますが、これらに限定されるわけではありません。

Intel、インテル、Intelロゴ、Arria、Xeonは、アメリカ合衆国および/またはその他の国におけるIntel Corporationまたはその子会社の商標です。

* その他の社名、製品名などは、一般に各社の表示、商標または登録商標です。

©2019 Intel Corporation. 無断での引用、転載を禁じます。

SS-1098-1.0/JP