A10

Always Secure. Always Available.

DDoS攻撃対策をアップデートしませんか？

A10ネットワークス株式会社

2022年6月

内容

- DDoS 攻撃の現状
- DDoS 攻撃対策
  - A10 の基盤技術
  - ゼロデイ攻撃対策
  - 脅威インテリジェンスによる先回り防御
  - DNS への攻撃対策
- ユースケース
- DDoS 攻撃対応製品ラインナップ

DDoS攻撃の状況

規模とターゲット

攻撃規模が増大

今や**テラビット級**の攻撃も：

- Microsoft への攻撃
  - 3.47 Tbps の攻撃（2021年11月）
  - 2.5 Tbps を超える攻撃 2 件（2021年12月）
- AWS への攻撃
  - 2.3 Tbps（2020年2月）

出典：
- https://azure.microsoft.com/ja-jp/blog/azure-ddos-protection-2021-q3-and-q4-ddos-attack-trends/
- https://aws.amazon.com/jp/blogs/news/aws-shield-threat-landscape-report-now-available/

Cloudflare、1秒に2600万件の過去最大級DDoS攻撃に対処

- わずか5067台のデバイスで構成された、小規模だがパワフルなボットネットによって実行され、ピーク時のリクエスト件数は 1秒あたり2600万件に達した
- 攻撃トラフィックがクラウドプロバイダーのインフラから発生している点から見て、より帯域幅の大きな仮想マシンやサーバーが乗っ取られたと考えられるとしている

出典：ZDNet Japan
https://japan.zdnet.com/article/35189024/

IoT機器への攻撃も、多く観測

国内で観測されたパケットの宛先ポート番号

［表1：宛先ポート番号トップ5］

順位	宛先ポート番号	前四半期の順位
1	6379/TCP（redis）	1
2	23/TCP（telnet）	2
3	123/UDP（ntp）	6
4	22/TCP（ssh）	3
5	445/TCP（microsoft-ds）	4

23/TCPは、短期間での増減が複数回発生

この背景には、**IoT機器等をマルウェアに感染させようとする攻撃**が何度か行われ、その度に23/TCP宛のパケットの観測数が増加したのではないかと推測

出典：JPCERT/CC, インターネット定点観測レポート（2022年 1～3月）
https://www.jpcert.or.jp/tsubame/report/report202201-03.html

攻撃手法

マルチベクトル攻撃が増加

Comcast Business, 2021年に 24,845のマルチベクタDDoS攻撃に対応

- 2020年に比べて **47%増加**
- Layer 3、4、7 が標的
- ほとんどの顧客が単一ベクトル攻撃を経験した2020年とは対照的に、2021年は、**55%がマルチベクタ攻撃** の標的
- マルチベクタ攻撃の 73%は、COVID-19のパンデミックによって引き起こされた脆弱性が原因と推測。教育、金融、政府、および医療セクタを標的に

出典：Comcast Business 2021 DDoS Threat Report: DDoS Becomes a Bigger Priority as Multi-vector Attacks are on the Rise（2022年4月）

https://business.comcast.com/about-us/press-releases/2022/2021-ddos-threat-report-ddos-becomes-a-bigger-priority-as-multi-vector-attacks-are-on-the-rise

多様な攻撃検知方法が必要

フローベースの検知装置だけでは
高レイヤの攻撃を検知するのは困難

- 低レイヤのボリューム型攻撃

フローコレクタやクラウド型防御で検知可能

- 日々進化する高度な攻撃
- マイクロバースト攻撃
- ネットワークプロトコル攻撃
- アプリケーションレイヤ攻撃
- スロー攻撃

フローコレクタやクラウド型防御では検知が難しい攻撃

攻撃対応の課題

- 保護対象のリソースを検索し、手動で設定
- 攻撃検知のための閾値を設定
- 通信状況を監視

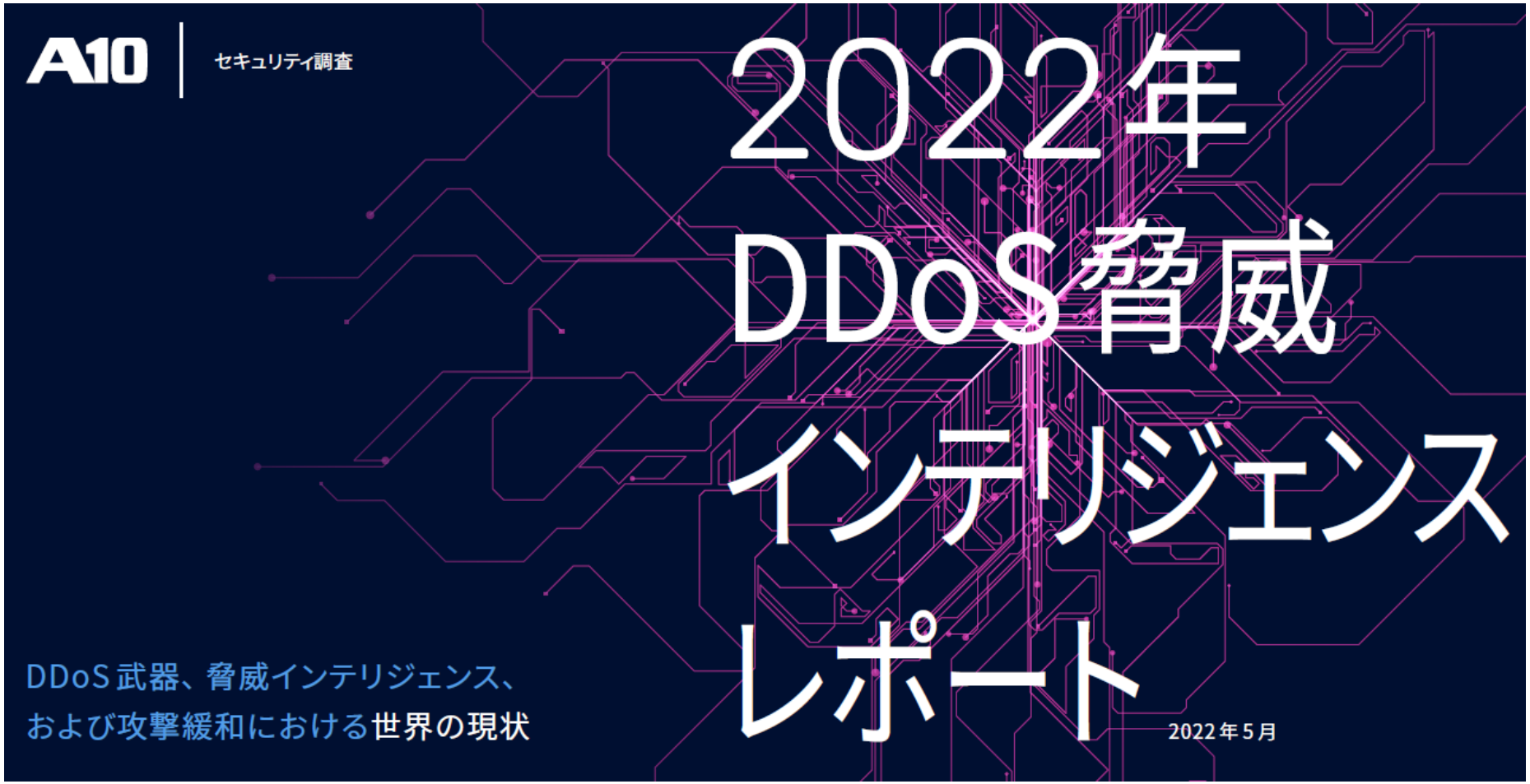
- 閾値を超えたトラフィックが発生
- 攻撃の内容を調査。緩和処置を適用

- 緩和処置を継続
- 状況によって緩和処置の内容を変更

- 攻撃の鎮静化を確認
- 攻撃終了後はレポート作成等

- **どのフェイズも備えが必要**
- **備えと対応には、専門的な知識と経験が必要**
- **手作業で毎回行うのは非常に大変**

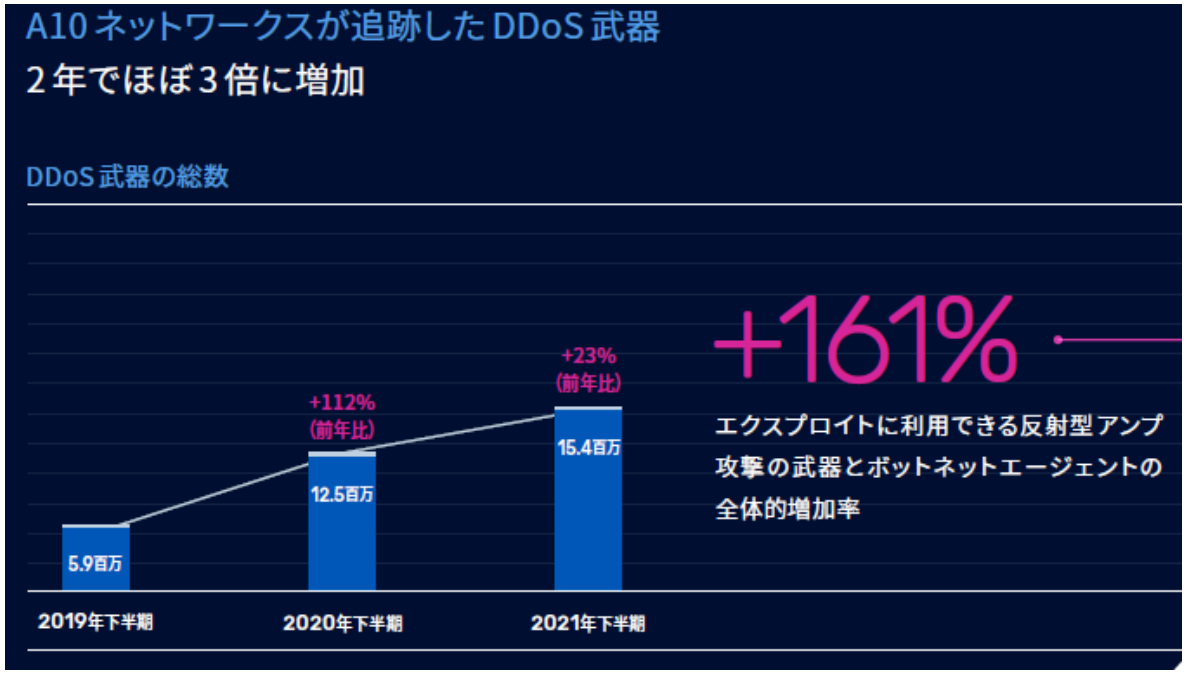
A10 DDoS脅威レポート



2022年5月発行

https://www.a10networks.com/resources/reports/2022-ddos-threat-report/

A10 DDoS脅威レポート



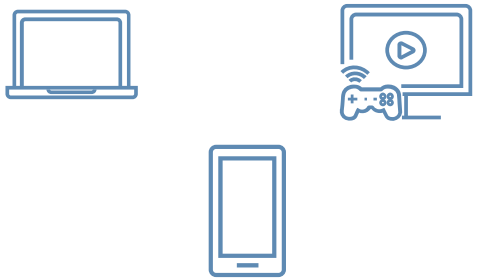
https://www.a10networks.com/resources/reports/2022-ddos-threat-report/

新たなDDoS攻撃対象

5G 環境下の様々なデバイスがDDoS攻撃を助長する可能性

高速大容量
(enhanced Mobile Broadband: eMBB)

高速インターネット
固定無線



超高信頼低遅延
(Ultra-Reliable and Low Latency Communications: URLLC)

拡張現実
バーチャルリアリティ
遠隔手術
コネクテッドカー

Massive IoT
(massive Machine Type Communication: mMTC)

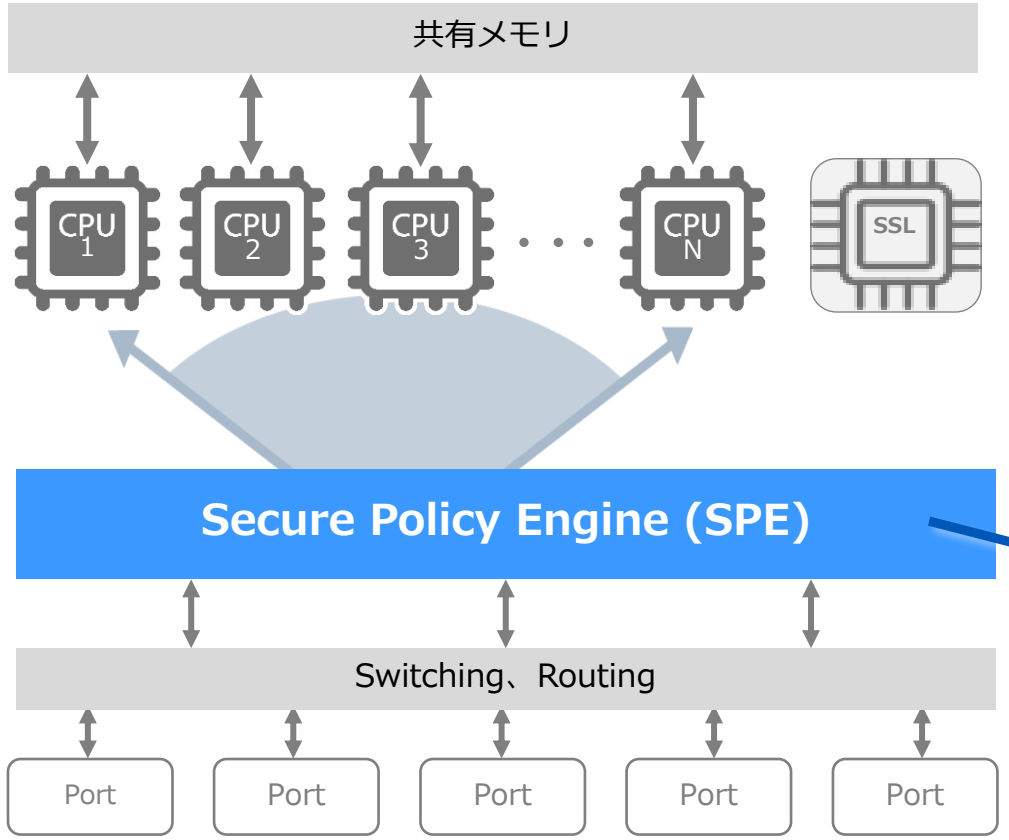
スマートホーム
スマートシティ

DDoS 攻撃対策
- A10の基盤技術 -

ACOS（Advanced Core Operating System）

HW性能を最大限に引き出す A10独自OS

ACOS 基本アーキテクチャ



- マルチコアCPU による完全並列処理
- 共有メモリアーキテクチャにより大量セッションを制御可能
- コントロールプレーンとデータプレーンの分離
- 高い拡張性。汎用CPUの使用など、機能修正や機能追加が容易

Security Policy Engine (SPE)

- セキュリティ機能の高速化を担う A10独自の HW
- 攻撃対処時の CPU 負荷を大幅に削減
- IPアノマリフィルタ
- 等々

Thunder TPS シリーズ

物理・仮想環境でハイパフォーマンスな防御環境を構築

Thunder 7655S TPS
TPSシリーズのフラッグシップモデル

380 Gbps：スループット（ソフトウェアスクラビング）
1.2 Tbps：ハードウェアブロッキング

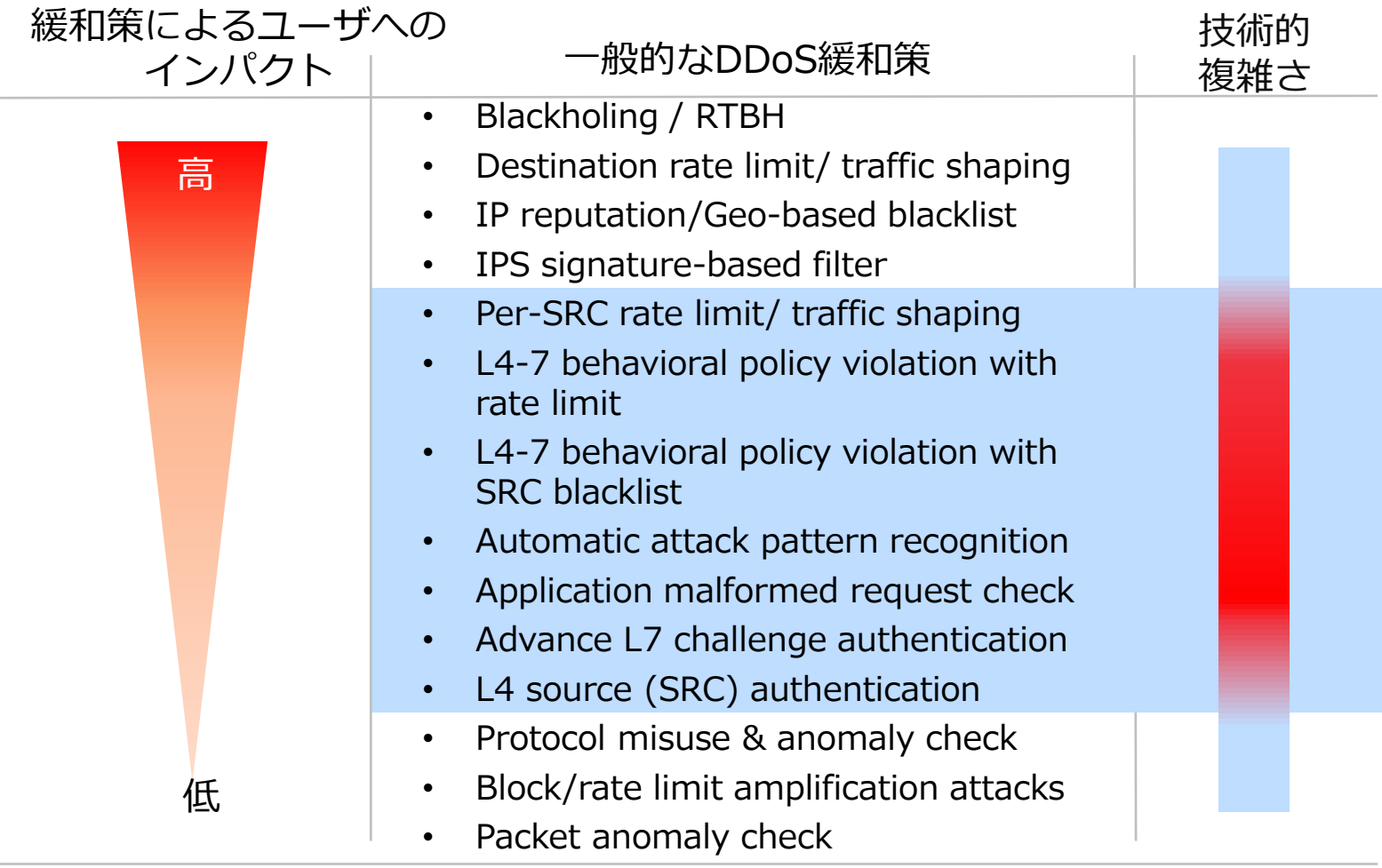
- 1.5Uの筐体
- ビルトインTLS/SSL高速化ハードウェア（Intel社QAT）搭載
- ハードウェアアクセラレーション（SPE: Security and Policy Engine）搭載
- QUICプロトコルのDDoS防御に対応

Thunder TPS シリーズ

- 大手サービスプロバイダやオンラインゲーム会社で多くの実績を持つ**DDoS攻撃対策ソリューション**
- **AI/機械学習を活用**し、DDoS攻撃を検知・緩和することで、ネットワークを大規模なDDoS攻撃から保護
- 様々なプラットフォーム
  - ✓ ハードウェアアプライアンス
  - ✓ 仮想アプライアンス
  - ✓ クラウドインスタンス（Microsoft Azure）

DDoS緩和手法とA10の優位点

技術的に複雑な箇所にも緩和手法を提供



A10ネットワークスの優位点

高精度なアノマリ検知

脅威インテリジェンス

広範囲で先進的な*L4-L7*の緩和策
- ユーザーと攻撃者を判別
- アプリケーションやプロトコルの振る舞いを検証
- 攻撃トラフィックのみを制限
- QUICによる攻撃も防御

機械学習によるパターン認識 *(ZAPR)*
- ゼロデイ攻撃のパターン認識と自動フィルタ生成
- 攻撃緩和の精度を向上

*5*段階での適応的な防御
- 複数段階のルール設定と自動エスカレーション
- 基本的な防御からアグレッシブな緩和策への段階的適用による誤検知の最小化