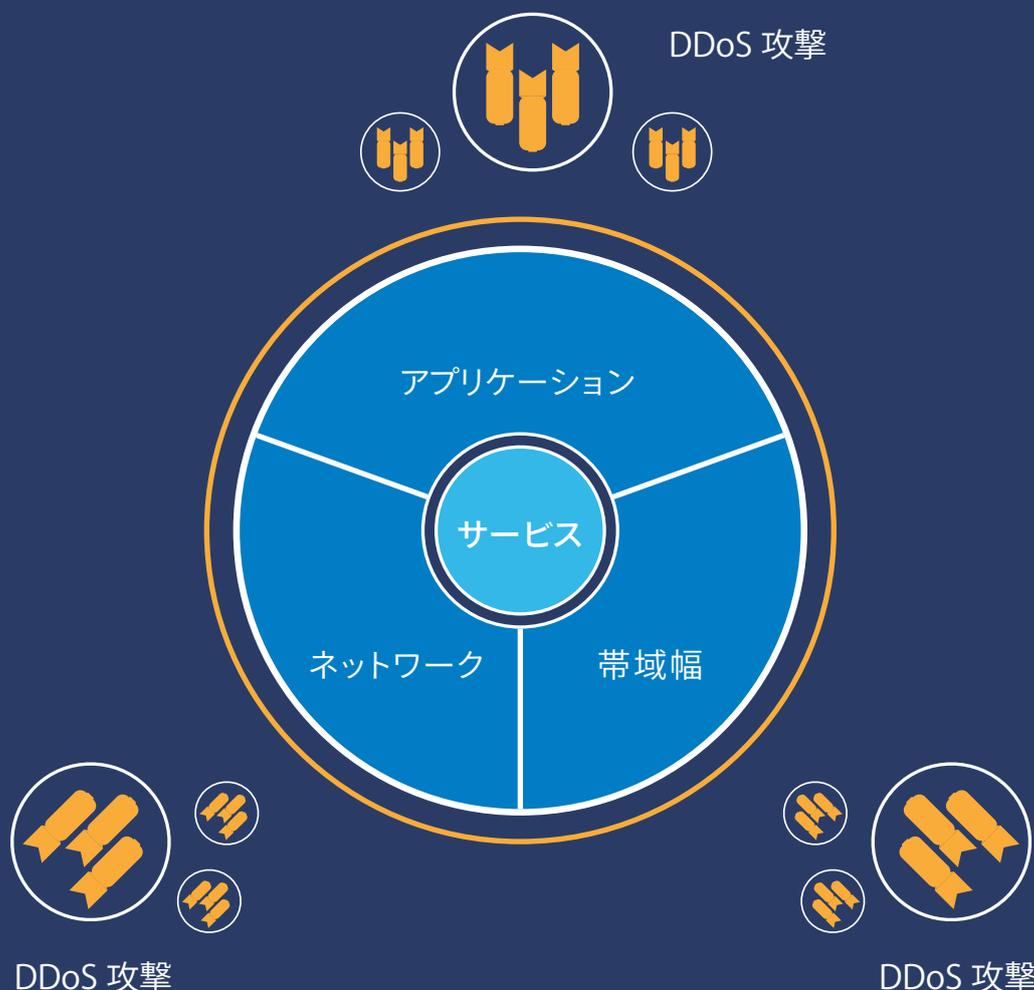


マルチベクトル型 DDoS 攻撃の 実態

1日に3,700件以上のDDoS攻撃が発生しています⁽¹⁾。そして、それらの攻撃の75%はマルチベクトル型DDoS攻撃となっています⁽²⁾。マルチベクトル型DDoS攻撃は、平均して1時間あたり最大30万ドルものビジネス損失を与えます⁽³⁾。

マルチベクトル型 DDoS 攻撃とは？

マルチベクトル型 DDoS 攻撃は単一ベクトル型の DDoS 攻撃とは異なり、**帯域幅、ネットワーク、およびアプリケーション層**に同時に攻撃をしかける連携型の DDoS 攻撃のことです。企業に対するマルチベクトル型 DDoS 攻撃は、最も脆弱なリンクを見つけて Web サイトやオンラインサービスがダウンするまで続き、その結果、サイトやサービスの利用者にも影響を与えることになります。



マルチベクトル型 DDoS 攻撃の急増



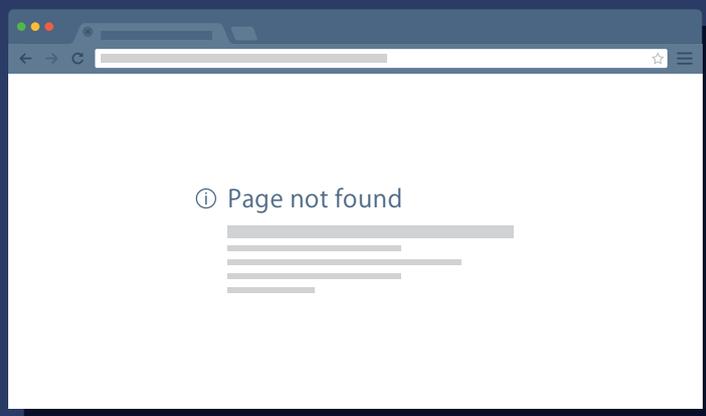
2015 年の第 2 四半期は、2014 年の同期間と比較して、攻撃が

132.43% 増加⁽⁶⁾。

大規模化かつ巧妙、そして甚大な被害をもたらす マルチベクトル型 DDoS 攻撃

2015 年の第 2 四半期時点で、アプリケーションレイヤーに対する DDoS 攻撃は 122% 増加し、ネットワークレイヤーに対する攻撃は 134% 増加⁽⁴⁾。

また、同期間において 1,000 Gbps 以上の攻撃規模を記録した攻撃は 12 件⁽⁵⁾。



ビジネスセクター別のマルチベクトル型 DDoS 攻撃

攻撃対象の 35.2% はゲーム関連企業ですが⁽⁷⁾、以下に示す通り、ダウンタイムが許されない非常に重要なサービスを運用するビジネスセクターも攻撃の標的となっています。



ゲーム関連企業 (35.2%)



ソフトウェア/技術関連企業
(27.7%)



インターネット/通信関連企業
(12.9%)



金融サービス関連企業
(8.1%)

世界的な危機

79か国で、マルチベクトル型DDoS攻撃の被害が発生
(2015年の第3四半期)⁽⁸⁾



標的上位 3か国



中国 (35.5%)



米国 (29.9%)



韓国 (17.7%)

最近ニュースになった攻撃事例：

2013年8月：BTCチャイナ、ビットコイン取引市場
(ボリューム型攻撃)⁽⁹⁾

2015年10月：TalkTalk、イギリスの電話とブロードバンドの
プロバイダー (ボリューム型およびアプリケーションレイ
ヤー攻撃)⁽⁹⁾

2015年10月：UltraDNS、米国サンフランシスコを拠点と
するWebコンテンツ配信サービス (ボリューム型攻撃)⁽⁹⁾

2015年11月：ProtonMail、スイスの暗号化された
Webメールサービスプロバイダー (ボリューム型攻撃)⁽⁹⁾

2015年11月：サンノゼ市 (米国カリフォルニア州)、
情報テクノロジーセンター (ボリューム型攻撃)⁽⁹⁾

さまざまな攻撃元から、常にマルチベクトル型 DDoS 攻撃が仕掛けられる可能性がある



サイバー犯罪者



政府のスパイ



ハクティビスト



いたずら

DDoS攻撃用ツールはオンライン上で容易かつ
安価に入手でき、現在はスマートフォンからの
攻撃も可能。



マルチベクトル型 DDoS 攻撃による莫大な損失

DDoS 攻撃が原因によるダウンタイム1分間
当たりの平均被害額は 22,000 ドル⁽¹⁰⁾。



2015 年度の調査によると、マルチベクトル型
DDoS がもたらす最も重大な損失は、
社会的信用の失墜⁽¹¹⁾。



マルチベクトル型 DDoS 攻撃に対する適切な防御



A10 Thunder TPS (脅威防御システム)

を利用すると、マルチベクトル型 DDoS 攻撃の被害が発生する前に先行してブロックすることが可能です。
A10 Thunder TPS は、大規模なマルチベクトル型 DDoS 攻撃に対して常時防御する機能を備えています。
また、数百万ものデバイスから情報や知見の収集が可能なほか、正確で最新の不正な IP アドレスリストの表示、
および強力なバックアップサポートを受けることもできます。

A10 Thunder TPS の詳細は、
Web サイト (a10networks.co.jp/tps) をご覧ください



- (1) <http://www.business.att.com/content/infographic/DDoS-Attacks-Infographic.pdf>
- (2) BT, 2015年
- (3) <http://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/>
- (4) <https://www.akamai.com/us/en/our-thinking/state-of-the-internet-report/>
- (5) <http://fossbytes.com/ddos-attacks-are-now-stronger-than-ever-mega-attacks/>
- (6) <https://blogs.akamai.com/2015/08/q2-2015-state-of-the-internet-security-report-released.html>
- (7) <http://www.4-traders.com/AKAMAI-TECHNOLOGY-INC-8303/news/Akamai-Technologies-India-Is-4th-Largest-Victim-Of-DDoS-Attacks-Web-Application-Gaming-Favorite-20897389/>
- (8) <https://securelist.com/analysis/quarterly-malware-reports/72560/kaspersky-ddos-intelligence-report-q3-2015/>
- (9) 2015年10月: TalkTalk、イギリスの電話とブロードバンドのプロバイダー (ボリウム型およびアプリケーションレイヤー攻撃)
<http://www.computerweekly.com/news/4500256046/TalkTalk-warns-customers-about-personal-data-breach>
<http://www.node4.co.uk/blog/talktalk-data-breached-by-two-pronged-ddos-attacks/>
- 2015年11月: ProtonMail、スイスの暗号化Webメールプロバイダー (ボリウム型攻撃)
<http://techcrunch.com/2015/11/07/protonmail-on-battling-a-sustained-ddos-attack/>
http://www.newsfactor.com/story.xhtml?story_id=0230024432Y4
- 2015年11月: サンノゼ市 (米国カリフォルニア州)、情報テクノロジーセンター (ボリウム型攻撃)⁽⁹⁾
<http://www.govtech.com/security/San-Jose-Calif-IT-Systems-Target-of-DDoS-Attack.html>
- 2015年10月: UltraDNS、米国サンフランシスコを拠点とするWebコンテンツ配信サービス (ボリウム型攻撃)
http://www.nytimes.com/2015/10/16/technology/ultradns-server-problem-pulls-down-websites-including-netflix-for-90-minutes.html?_r=0
<http://digital-era.net/ultradns-dealing-with-ddos-attack/>
- 2013年8月: BTCチャイナ、ビットコイン取引市場 (ボリウム型攻撃)
http://www.wired.com/2013/11/ddos_bitcoin/
- (10) http://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf
- (11) <https://www.stateoftheinternet.com/resources-web-security-white-paper-2015-ponemon-institute-the-cost-of-ddos-attacks.html>

