SOTI

第 10 巻、第 6 号

10 YEARS
OF SECURITY INSIGHT

ヘルスケアに関する詳細な調査

アプリケーションと API に特化した攻撃

Akamai

インターネットの現状／セキュリティ

目次

脆弱性から可視化まで、ヘルスケアにおけるサイバーセキュリティの状況を解き明かす

ヘルスケア業界の状況は、「脆弱」の一言に尽きます。この状況を打破するために、ヘルスケア業界は「可視化」を 2024 年のメインテーマにするべきです。プラットフォーム、サードパーティソフトウェア、広範囲にわたるデータ交換が増加し、可視化が不可欠となっています。しかし、ヘルスケア組織では、技術の最新化が急速に進んでいるため、エコシステム全体を見渡す真の可視性の確保に多くの組織が苦心しています。事態をさらに複雑化しているのが、コンプライアンス対策です。厳格な統制の下でさらなる共有が必要になります。これは、データの「堀」を撤廃し、ネットワークの独占を排除するための論理的な次なるステップですが、トップ企業を除く業界の大半の企業にとっては、現状のセキュリティ機能では対処できない高度な技術的要素が必要になります。

脅威アクターはチャンスを見逃しません。ヘルスケアの各分野は、社会において最も機微な情報を交換するために自社システムをオープン化していますが、私たちは数十年を経たレガシーインフラに、新たなシステムと新たな基準を組み合わせようとしているのです。このレガシーインフラは、膨大な技術的負債をもたらす可能性がある一方で、悪意を持つアクターにとっても暗躍のための最適な環境になります。

残念ながら、ヘルスケア業界でサイバーセキュリティ攻撃がかつてない勢いで増加しているのは当然と言えます。特に、米国の多くのヘルスケア組織では、サイバーセキュリティ対策を、長年にわたり、提案依頼書やベンダー評価の際には、形式的な作業として扱ってきました。組織は、社内で専門知識を構築するのではなく、HITRUST、HIPAA 準拠の SOC 2 認定ベンダーを単純に求め、ビジネスアソシエイト契約を通じてそうしたベンダーにリスクを転嫁することが多いのです。スタートはまずまずでしたが、メディアの見出しを飾るのは、大規模な財務問題や業務の混乱のニュースばかりです。さらに悪いことに、ヘルスケア業界における患者の安全に対する脅威も指摘されています。現時点はわずかな影響にとどまっていますが、上位 1,000 社のうち 4 分の 1 から 2 分の 1 の病院やヘルスケア機関が同じスプレッドシートによるセキュリティチェックリストを使用してベンダーの承認・採用を行うようになると、問題が生じるでしょう。

保険会社は、コンプライアンス上の理由により、これまでのオンプレミスのバッチ型システムから脱却し、最新のエコシステムである API ベースのデータ要件を満たす必要があるため、かつてないほど脅威にさらされています。この最新化により、保険会社が長年求めてきた臨床データへのアクセスが可能になりますが、オープンなデータ交換は新たなリスクを伴う新たなビジネス手法となり得ます。財務データと臨床データを保有することになる保険会社は、インフラのセキュリティを確保し、セキュリティ体制を徹底的にレベルアップし、新たなコンプライアンス対策に準拠しなければなりません。

結論としては、こうした市場変化は今後も続きます。ヘルスケア業界は、API やクラウド要件から後戻りすることはありません。変化に伴うセキュリティの懸念は想定内ですが、オープンなデータ交換を推進するという判断は、これまでデータサイロに悩まされてきた業界に大きな進歩をもたらします。

Neil Jennings 氏
Vice President、Untangle Health

Chris Notaro 氏
CEO、Untangle Health

はじめに

ヘルスケア業界は、サイバーセキュリティについて独自の課題をいくつか抱えています。

- サイバーセキュリティが生死を左右する状況も考えられます。
- 情報の価値は、あらゆる業界の中でも最高レベルです。
- インフラには、レガシーシステムと医療分野の IoT（IoMT）デバイスが混在しています。
- システムは連携し、多くの場合、互いに依存しています。
- コンプライアンス要件は最も厳格なレベルです。

このインターネットの現状（SOTI）レポートでは、ヘルスケアエコシステムのリスクに関する脅威データとトレンドを分析しています。業界に最も大きな影響を与えている 2 つの脅威は、Web アプリケーションおよび API 攻撃と、分散型サービス妨害（DDoS）攻撃です。

ヘルスケアエコシステムを構成する組織（保険会社、ヘルスケア機関、製薬会社およびライフサイエンス企業）も、それぞれがセキュリティ戦略を左右する独自の課題を抱えています。

保険会社は、適用資格、 補償範囲、保険金支払いを判断するために、臨床データと財務データに確実にアクセスでき、業界全体でのデータ共有のハブとなる存在です。

製薬企業やライフサイエンス企業は、彼らが無数のアプリケーションで人口知能や機械学習を駆使して行っている、大規模なデータセット分析などのイノベーションに、脅威アクターがフォーカスしていることをに気付いており、イノベーションとリスクの間で岐路に立たされています。

ヘルスケア機関は、遠隔医療や急増する IoMT など、臨床的なイノベーションへの投資を重視しているため、組織的な回復力を大きく左右するサイバーセキュリティアプローチを発展させるなどの、より従来的な機能への投資は手薄になっています。

相互運用性を高めることにより、患者の転帰と財務上の成果を向上させることができますが、Web アプリケーションおよび API 攻撃という形でリスクも生じます。

歴史的に見ると、脅威アクターはヘルスケアエコシステムを長年標的にしてきました。2024 年、ヘルスケア業界は、13 年連続で全業種中最も高いデータ漏えいの被害額を記録し、平均被害額の 977 万ドルは、2 位の金融サービス業界の 608 万ドルを大きく上回っています。

API は、ヘルスケア業界に属するすべての業種に影響する主要なテクノロジーの 1 つです。API を使用すると、ヘルスケア機関、保険会社、患者、その他のサードパーティ（電子カルテシステム、医療機器会社、医療情報交換など）の間でデータを共有できます。相互運用性を高めることにより、患者と財務上の成果を向上させることができますが、Web アプリケーションおよび API 攻撃という形でリスクも生じます。

アプリケーションレイヤーに対するもう 1 つの脅威が DDoS 攻撃です。現在は、ヨーロッパ、中東、アフリカ地域（EMEA）で盛んに使用されていますが、これは同地域の地政学的状況や親ロシア派のハクティビストグループが原因と思われます。しかし、攻撃を受けない国や地域は存在しません。DDoS 攻撃を利用するグループの数やその戦術、テクニック、手順は絶えず変化しているからです。

重要な知見

41%

保険組織をターゲットとしたヘルスケアエコシステムにおける API 攻撃の割合

API 攻撃は、ヘルスケアエコシステムで確実に増加しています。特に保険組織や保険会社をターゲットとした攻撃が増えています。これは、保護医療情報（PHI）、保険金請求データ、財務情報など、こうした組織が保有している豊富な情報が原因と考えられます。

API の無秩序な拡大がデータの不正アクセスなどの大きなリスクを招いている

API の無秩序な拡大、または組織内での API の無秩序な普及により、可視性が失われ、セキュリティ制御の及ばない外部で増殖し、大きなセキュリティギャップが生じています。その結果、組織のアタックサーフェスが拡大し、機微な情報への不正アクセスなどのリスクを招くことになります。

88%

EMEA の製薬組織に対するレイヤー 7 DDoS 攻撃の割合

レイヤー 7 DDoS 攻撃の件数は、EMEA 地域の製薬会社が最も多く、北米とアジア太平洋・日本（APJ）地域がそれに続いています。2024 年上半期のデータを詳しく検証すると、EMEA および北米に対する攻撃数は、2023 年の各地域の合計数を超える勢いです。

21 MILLION

ヘルスケア機関に対する Web アプリケーションおよび API 攻撃の月間平均件数

データの相互運用性とその他のコンプライアンス要件を受けて、Web アプリケーションおよび API の利用が増加した結果、ヘルスケア機関と患者の両方にセキュリティリスクが生じています。

415 MILLION

ヘルスケア機関に対するレイヤー 7 DDoS 攻撃の月間平均件数

ヘルスケア業界では DDoS 攻撃が増加しており、ハクティビズムと現在の地政学的状況がこの動きに拍車をかけています。こうした攻撃は、サービスの中断や混乱を生じさせ、患者にとって結果的に脅威となります。2023 年、Killnet は大規模な DDoS キャンペーンを立ち上げて、主にヘルスケア機関に打撃を与えました。

保険会社では API が悪用されるリスクが高まっている

保険会社は、API を多用し、ヘルスケアエコシステム全体でデータを収集・処理して大きなメリットを得ていますが、特にコンプライアンス要件の増殖やセキュリティリスクの拡大など、トレードオフも発生しています。サイバー犯罪者とアグリゲーターがこれらの機能を攻撃して悪用しており、それによって安全性とプライバシーの両方の問題が生じる可能性があります。

また、API への攻撃はサービスの中断を招く可能性があり、それによって健康保険の申し込みや請求処理に影響が生じ、ダウンタイムに伴う多大なコストが発生し、企業のブランドが損なわれます。最近の被害の大きな例としては、2024 年 2 月に米国全土の薬局の支払い処理を窮地に陥れた組織的攻撃があります。

API 攻撃の傾向

Akamai の調査によると、2023 年 1 月から 2024 年 6 月の間に発生した、ヘルスケアエコシステムを標的とした API 攻撃の 41% が、保険会社に対するものでした。つまり、保険会社は攻撃によって API が悪用されるリスクが非常に高いことがわかります。2022 年時点で米国の合計ヘルスケア支出の約 67% が保険会社を経由していることからも、ヘルスケアシステムの運用維持において保険会社が重要な役割を果たしていることは明白です。

他の規制の厳しい業界（特に決済システムを扱う業界）でも、同様の傾向が見られます。たとえば、金融業界はデジタルトランスフォーメーションがさらに進んでおり、より統合された API をビジネスモデルの一部としてすでに使用しています。オープンバンキングでは API の使用が推進されており、セキュリティリスクが増大しています。そのため、API セキュリティ SOTI レポートでも報告しているように、API を狙った攻撃は金融セクターに集中しています。

Akamai の研究者が保険会社への API 攻撃のデータを詳細に調査したところ、2023 年 1 月から 2024 年 6 月の 18 か月間、特に四半期ごとに活動に変化が見られました。各四半期の全体的な増加傾向は、四半期末に予測値と実測値の帳尻を合わせるためのシステム間の同期が影響している可能性があります。しかし、2023 年第 4 四半期の全体的な増加は、攻撃者が健康保険の申し込み期間を標的として事業を妨害しようとしたことが原因と考えられます（図 1 を参照）。

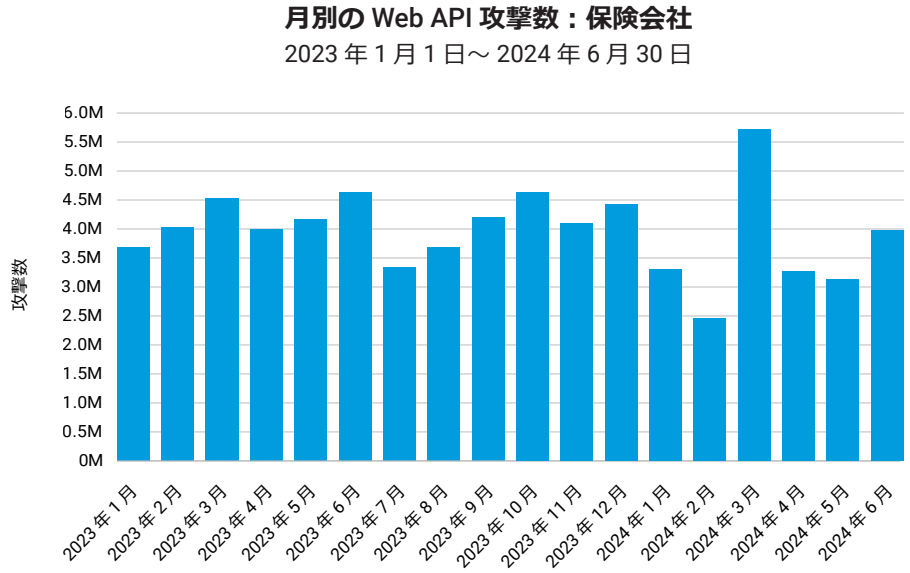


図 1：API に対する Web 攻撃は各四半期で増加傾向にあり、2023 年第 4 四半期は全体的に増加している

あらゆる業界で見られる API の悪用と重大なセキュリティ課題

多くの API セキュリティ課題はヘルスケア固有のものですが、API の基本はすべての業界で共通です。あらゆる業界で緩和すべき技術的リスクを確認しておくと効果的でしょう。第一に、OWASP API Security Top 10 で挙げられているリスクに注力すべきです。一方で、ポスチャに関する課題やランタイムの課題として分類している一般的な脆弱性を開発者や IT スタッフが理解することも重要です。

- **ポスチャの課題**は、企業の API 実装の欠陥に関するものです。ポスチャに関する問題点を警告するアラートにより、セキュリティチームは、優先度の高い脆弱性を攻撃者に悪用される前に特定して対処できます。一般的なポスチャに関する課題には、シャドウエンドポイントや URL に含まれる機微な情報などがあります。
- **ランタイムの課題**とは、緊急対応を要するアクティブな脅威やふるまいのことです。こうした重要なアラートは（より明確なインフラ侵害の試みとは異なり）API の悪用という形を取るため、その他のセキュリティアラートよりも繊細な内容になります。一般的なランタイムの課題には、不正なリソースアクセスの試みやデータスクレイピングなどがあります。

さらに、いったん立ち戻って API の 3 つの一般的な課題を検証し、セキュリティプログラムが API の悪用に対して効果を発揮していることを確認することも重要です。

1. **可視性**：すべての API をプログラムで確実に保護するためのプロセスと技術的な制御を備えていますか？これは重要な問題です。なぜなら、API はしばしば、デジタル・トランスフォーメーションや新製品の一部として組み込まれるため、その多くは従来の Web プレゼンスと同じレベルの管理、保護、検証体制を維持できないからです。

2. **脆弱性**：API は開発のベストプラクティスに従っていますか？ OWASP の最も一般的なコーディング不良の問題を回避していますか？さらに、脆弱性を追跡／確認していますか？

3. **ビジネスロジックの悪用**：望ましいトラフィックのベースラインを有していますか？疑わしい行為と判断する要素を特定していますか？

こうした質問の答えが、チームが理解すべき情報の土台となります。全体的な目標としては、API の可視性を確保し、調査を実施できる体制を整えて、脅威を速やかに緩和するためのプロセスを確立することを目指します。これについては、患者向けの API でも社内 API でも同様です。

パフォーマンスの向上がリスクの増大につながる可能性

患者はすべてのアプリケーションに同じレベルのユーザー体験を求めているため、パフォーマンスはますます大きな懸念事項となっています。つまり、ヘルスケアエコシステムをサービス妨害攻撃から保護するとともに、API を悪用する攻撃からも保護する必要があります。さらに、ヘルスケア機関には透明性を求める規制が課せられており、タイムリーな情報アクセスのニーズがさらに高まっています。

API の無秩序な拡大（API スプロール）は、可視性の低下につながり、アタックサーフェスの拡大に応じてさらなる混乱を招きます。API は複雑なデジタル・トランスフォーメーション・プロジェクトの一部であることが多いため、ヘルスケア機関は API に注目していない場合があります。セキュリティプログラムはなおさら注目されていません。

日々のビジネス活動に関わるさまざまな種類のデータ（医療データと財務データの両方）は、厳しく規制されているだけでなく、サイバー犯罪者の標的になりやすいため、保険会社にとっての問題が複雑化しています。

API は複雑なデジタル・トランスフォーメーション・プロジェクトの一部であることが多いため、ヘルスケア機関は API に注目していない場合があります。セキュリティプログラムはなおさら注目されていません。

ライフサイエンス組織に対する DDoS 攻撃の数は増加の一途を辿る

製薬業界におけるサイバーセキュリティは、コロナ禍に大きな注目を集めました。ワクチン開発研究、臨床試験データ、生産、供給が脅威アクターにとって格好の標的となったためです。現在、ヘルスケアは米国の重要なインフラに指定され、超党派の新たな基金により、重要と見なされる分野全体の回復力要件が引き上げられています。その理由は明白です。

- 国際的な緊張も世界的に引き続き高まっています。PwC の 25 回目となる Annual Global CEO Survey に回答した経営幹部も地政学的状況を重視しています。回答者の約 3 分の 1 は、地政学的な混乱が自社の成長の脅威だと答えており、3 分の 2 以上は、サプライチェーンの混乱を招くだろうと回答しています。
- 調達のローカライズやブロックチェーンテクノロジーの使用強化などのアプローチは、製薬会社の回復力を強化し、臨床およびビジネス面での影響を改善する効果があります。
- Akamai のライフサイエンス業界に関するグローバルデータによると、DDoS 攻撃（および DDoS 攻撃を実行するグループの数）は増加の一途をたどっており、回復力はこの業界で必須の要素となっています。

アプリケーションレイヤー DDoS 攻撃の標的となる EMEA の製薬組織

Akamai の調査によると、2023 年 1 月から 2024 年 6 月にかけて、EMEA 地域は、製薬組織を標的とするすべてのアプリケーションレイヤー（レイヤー 7）DDoS 攻撃の 88% を占めています。これに対して、北米と APJ はそれぞれ 7% と 5% にとどまります。2024 年上半期のデータを見ると、EMEA と北米への攻撃集中がさらに顕著になり、2023 年の各地域の合計数を超える勢いです（図 2 を参照）。

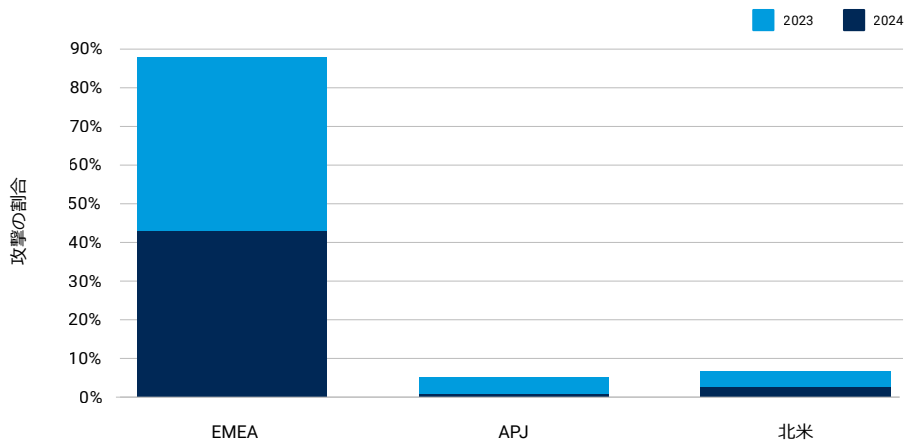


図 2：レイヤー 7 DDoS 攻撃は 2023 年から 2024 年にかけて EMEA 諸国に集中し、2024 年上半期には急増している一方で、北米での攻撃数も増加している

従来のレイヤー 3 およびレイヤー 4 DDoS 攻撃は、ネットワークやトランスポート・レイヤー・インフラに過度な負荷をかけることが狙いでしたが、レイヤー 7 DDoS 攻撃は、特定のアプリケーション機能やアプリケーションサーバー自体を標的にします。比較的な少量の悪性トラフィックでも、大きな損害を与える能力を持っています。

レイヤー 7 DDoS 攻撃は、CPU やメモリーなど、アプリケーションレベルのリソースを標的にします。攻撃を受けたアプリケーションやサービスは、ネットワークを利用できたとしても速度が低下するか、完全に無反応になります。

ヘルスケアおよびライフサイエンス業界に対する DDoS 攻撃が EU で増加

ENISA 2023 Threat Landscape: Health Sector レポートでは、EU のヘルスケアおよびライフサイエンス業界に対する DDoS 攻撃数の増加を指摘しています。興味深いことに、レポートでサイバーインシデントの「ホットスポット」として挙げられている国（特にフランス、ドイツ、オランダ）と、2022 年度の EU 上位 1,000 社にランク入りしている製薬会社やバイオテック会社が集中している地域との間に正の相関が認められます。

ENISA（欧州ネットワーク・情報セキュリティ機関）は、DDoS 攻撃増加の理由として、地政学的状況と親ロシア派のハクティビストグループ（Killnet など）の存在を挙げています。

米国のライフサイエンス組織が次の標的になる

Killnet の以前の標的はヨーロッパの病院でしたが、現在の標的は米国のほぼ全州の病院に移行しています。こうした病院に対するサイバー攻撃はニュースでも大きく報じられましたが、2023 年 4 月の米国保健社会福祉省（HHS）の報告では、Killnet の DDoS 攻撃の標的になった組織の割合は製薬会社やバイオテクノロジー企業が最も高かったと指摘しています。

米国のライフサイエンスにおける世界市場シェア（50%）は EMEA（34%）より高いという事実からも、米国の製薬会社に対する DDoS 攻撃の脅威は今後さらに高まることが十分に予想されます。

しかし、この脅威と無縁の国や地域は存在しません。インドは、世界有数のジェネリック医薬品の生産・輸出国ですが、昨年は 17 TB の企業データが流出したデータ漏えいインシデントが発生し、多大な被害を受けました。ランサムウェアギャングとして攻撃を仕掛ける ALPHV/BlackCat は、ベンダー、顧客、1,500 人の米国従業員のドキュメントに関する機密情報を含む別のランサムウェア攻撃への関与を表明しています。

どの攻撃者がどの戦術を使用しているのか？

ENISA の報告では、ALPHV/BlackCat を EMEA におけるライフサイエンスに対する主な攻撃グループと指摘しています。このグループは今年に入ってからも米国サプライチェーンを攻撃しています。

Killnet とともに、Anonymous Sudan も政治的な動機を持つグループとして名前が挙がっています。この犯罪組織の当初の標的はヘルスケア機関でしたが、現在はヘルスケアエコシステムの他の分野にもその範囲を広げています。

この拡大に伴い、Anonymous Sudan は最近の OpenAI に対する DDoS 攻撃への関与も表明しており、懸念が高まっています。同グループは声明で Skynet ボットネットを利用したと明かしています。これは、アプリケーションを混乱させ、エラーを生成するレイヤー 7 DDoS 攻撃をサポートするボットネットです。

重大なリスクには保守的なアプローチが必要

製薬会社は、長年にわたり、ヘルスケア業界の中で率先して人工知能（AI）、特に機械学習（ML）を導入し、AI を利用して無数のアプリケーションの大規模なデータセットを分析してきました。そのメリットとしては、疾病の早期発見、迅速な創薬プロセス、製薬プロセスの改善などがあります。しかし、デジタルトランスフォーメーションを推進してきた他の業界（金融サービスなど）と同様に、ライフサイエンス業界もイノベーションとリスクの岐路に立たされています。

Killnet の DDoS 攻撃の標的になった組織の割合は、製薬会社やバイオテクノロジー企業が最も高いという結果が出ています。

製薬会社の立場は明らかです。他の規制対象業界がレイヤー 7 DDoS 攻撃にどのように対処しているかについて Akamai 研究者が調査した結果、「拒否」と「アラート」のアクションの割合について、製薬会社は異常な活動を高い割合で「拒否」する保守的なポリシーを適用していることがわかりました（図 3）。

業界別のレイヤー 7 DDoS に適用されたアクション

2023 年 1 月 1 日～ 2024 年 6 月 30 日

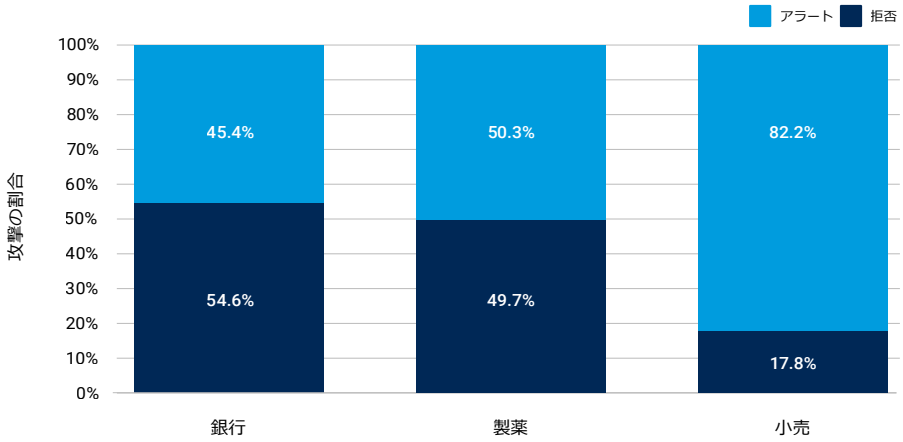


図 3：製薬会社とライフサイエンス企業は高い確率でアラートではなく拒否アクションを取っている

この拒否／アラート統計データ（2023 年 1 月から 2024 年 3 月）の初回報告後、これらの比率は 4% 以上上昇しています。拒否アクションは実に 45.5% から 49.7% となり、短期間での急上昇と言えます。

金融サービスや銀行業などの他の業界も、同様に保守的なポリシーを導入しています。特に、銀行業とライフサイエンスはいずれも重要なインフラとして厳格な規制が適用されており、多くの共通点が見られます。

さらに、製薬組織の場合は、DDoS 攻撃をまともに受けると深刻な影響につながり、救命措置が遅れることで、人命が危険にさらされる可能性もあります。まず拒否アクションを発動し、活動を検証するという流れになるのも当然と言えます。

一方、小売業界は、それほど積極的なスタンスではなく、アクションを取る前に、アラートを受信して異常な活動を評価する余裕があります。しかし、特に AI ／ ML の使用について新たな規制が登場した場合、小売業界も拒否アクションを取る頻度が高まる可能性があります。

Akamai 研究者が調査した結果、「拒否」と「アラート」のアクションの割合について、製薬会社は異常な活動を高い割合で「拒否」する保守的なポリシーを適用していることがわかりました。

ヘルスケア機関は包囲されている

HHS が 2023 年 12 月に公開したデータ漏えいに関する分析によると、健康情報共有および分析センターの最高セキュリティ責任者は、1 時間に平均 3,604 件の患者記録が漏えいしていると HHS に報告しています。

ヘルスケア機関と病院に対するサイバー攻撃の数は引き続き急増しています。Web アプリケーションと API の常用により、接続性と相互運用性が高まり、ヘルスケア機関と患者をリスクにさらしています。パッチ未適用の脆弱性とレガシーテクノロジーの技術的負債は、コストのかかる課題であると同時に、ランサムウェアグループに攻撃の糸口を与えています。

ハクティビストによる病院に対する DDoS 攻撃の継続的な脅威と地政学的な情勢は、いずれも患者の治療を混乱させています。こうしたすべての要素が PHI のデータ漏えいにつながり、患者の治療にネガティブな影響を与え、患者の安全性の問題に発展する場合もあります。

攻撃がヘルスケア組織に打撃を与えている

Akamai の調査によると、2023 年 1 月から 2024 年 6 月の 18 か月間において、ヘルスケア組織に対する Web アプリケーションおよび API 攻撃は一定のペースで継続しています（図 4）。この傾向は今後も変動しながら拡大する見込みです。サイバー犯罪者は、進化する治療モデル、実践方法、革新的なシステムに伴う新たな脆弱性と実証済みの脆弱性を利用して攻撃を仕掛け、Web アプリと API を悪用します。

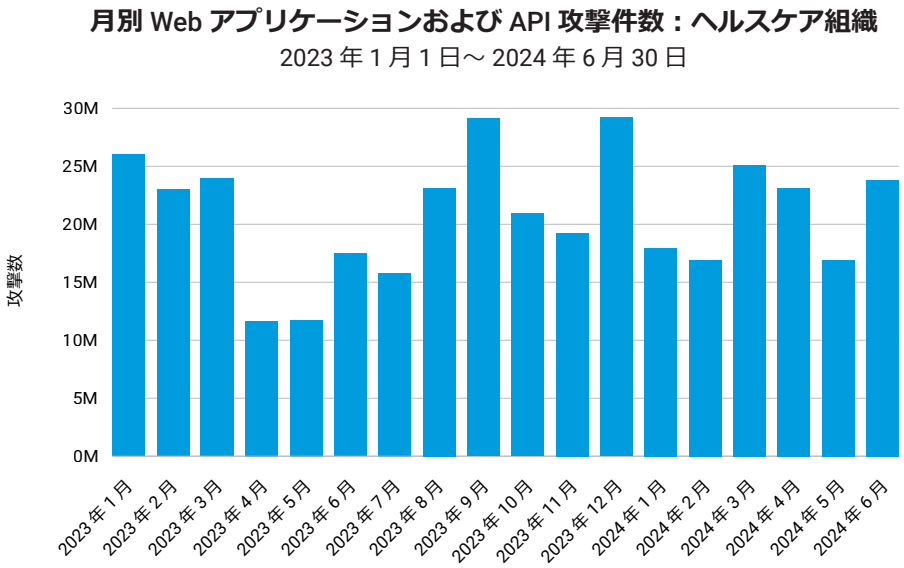
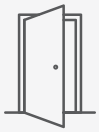


図 4：ヘルスケア組織に対する月別の Web アプリケーションおよび API 攻撃件数は全世界平均で 2,100 万件に達している（注：分布から大きく逸脱した 1 社の顧客については対象外としました）



パッチ未適用の脆弱性とレガシーテクノロジーの技術的負債は、コストのかかる課題であると同時に、ランサムウェアグループに攻撃の糸口を与えています。

Web アプリと API を使用することで、データ共有と相互運用性が実現します。その結果、医療連携を強化して、医療上および財務上の結果を改善できます。一方で、ヘルスケア業界に大きなリスクをもたらしています。これは API のセキュリティへの影響をまだ完全には把握できていないためです。

最適な医療連携と脆弱性によるリスクのバランスを取る

膨大な数の患者記録とシステム接続ポイントにより、ヘルスケア機関は医療連携を最適化するとともに、制御を通じて可視性をもたらし、脆弱性によるリスクを先読みして緩和する必要があります。多くの場合、API を始めとする新たなテクノロジーやインフラを展開する際、このバランスを取るのは容易ではありません。

Akamai の調査によると、2023 年 1 月から 2024 年 6 月の 18 か月間において、ヘルスケア組織に対するレイヤー 7 DDoS 攻撃は、2023 年 1 月以降、一定のペースで継続しています（図 5）。その原因の一部としては、親ロシア派のハクティビストグループである Killnet によるヘルスケアを標的としたグローバルな DDoS キャンペーンが考えられます。このキャンペーンでは、米国のヘルスケア組織が重点的に狙われました。この期間中、サイバー犯罪者はアプリケーションの機能やアプリケーション自体を標的として DDoS 攻撃を何度も仕掛け、患者の治療にリスクをもたらしています。

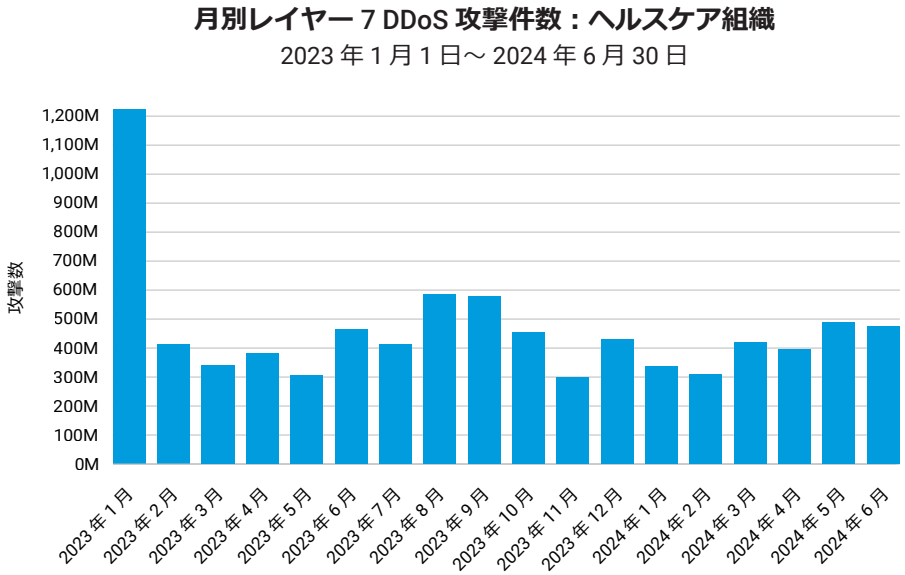


図 5：1 月の独立した急増を除き、ヘルスケア組織に対する月別の DDoS レイヤー 7 攻撃件数は世界平均で 4 億 1,500 万件に達した

ヘルスケアに対する DDoS 攻撃は規模的にも速度的にも新記録を更新している

地政学的状況とハクティビストグループによる DDoS 活動の増加により、業務の停滞が発生し、患者の転帰を妨げています。ヘルスケアエコシステム全体が影響を受けています。ヘルスケア組織は、Killnet による 2023 年の大規模 DDoS 攻撃で最も頻繁に標的になりました。HC3 の警告によると、ヘルスケアサービスが数時間停滞しただけで、ルーティーン的なものから重大なものまで、あらゆる日常業務が影響を受け、深刻な結果をもたらす可能性もあります。

アプリを介したヘルスケアのやり取りが増えるにつれて、情報や治療をタイムリーに提供することが患者体験にとって重要となります。そのため、保護とプロセスを導入することも同様に重要になります。

多方面からの攻撃が医療連携を阻害する

ヘルスケア機関は、DDoS だけでなく、別の一般的な攻撃タイプにも直面しています。ランサムウェア攻撃は、医療記録へのアクセスを制限し、救急車を混乱させます。医療履歴にアクセスできなければ、各ヘルスケア機関は連携できないという事実を浮き彫りにします。紙の記録に戻ると、患者の治療追跡や主要部署とのやり取りが混乱し、すべての発注サービスが停滞します。

機微な情報が影響を受けると、ヘルスケア組織もデータ漏えいの影響を被ることになります。一般的なソフトウェアツールの脆弱性を悪用することで、攻撃者は、PHI から健康保険、医療情報まで、データの宝庫にアクセスできるようになります。

患者の保護にはデータの保護が不可欠

患者の治療には、患者データの保護とアクセス管理が含まれます。伝統的に、ヘルスケアのサイバーセキュリティ予算とチーム体制は十分ではなく、データ保護が困難でした。しかし、ヘルスケア機関に対するサイバー攻撃が続々と報じられる中、ヘルスケア機関はアウトソースの保護パートナーシップを継続的に強化し、サイバー保険の適用範囲を拡大し続けています。

重大なインフラ分野の回復力を強化する米国政府のポリシー更新に伴い、ヘルスケア機関が保護を強化する機運は今後も高まり続けると考えられます。

ヘルスケア組織は、Killnet による 2023 年の大規模 DDoS 攻撃で最も頻繁に標的になりました。

コンプライアンスの考慮事項

規制環境はさらなる透明性を求めており、API の利用に拍車をかけています。コンプライアンス上の理由により、ヘルスケア機関と保険会社は幅広いデータ共有要件に対応しなければなりません。このデータ共有は、医療データと財務データの相互交流を意図しています。これまではそうした相互交流は困難でしたが、バリューベースケア（VBC）の効果的な実践のためには不可欠となります。

VBC への移行、つまりコストを考慮して治療を提供するようになると、膨大な量の多種多様な情報を共有しなければなりません。保険会社は長きにわたって、患者やヘルスケア機関の財務データへのアクセス権を保持しています。しかし、VBC データポイント（服薬遵守や入院など）が増えると、イノベーションだけでなく、相互運用性も求められるようになり、そのデータを共有する方法も必要になります。このようなデータ共有を可能にするのが API です。

最近の CMS Interoperability and Patient Access Final Rule では、保険会社が次の 3 種類の API を通じて、保険会社、ヘルスケア機関、患者の間で情報を効率よくやり取りできる状態を保つように求めています。

1. 患者アクセス API：保険加入者が自身の医療データにアクセスしやすくなり、保険加入者の満足度が向上する可能性があります

2. ヘルスケア機関ディレクトリー API：保険加入者は地理的位置や医療専門分野に基づいてヘルスケア機関や施設を検索できるため、医療へのアクセスが向上します

3. 保険会社とヘルスケア機関の間の API、および保険会社間の API：医療格差に対処してそれを減らすために役立ち、サービスの重複やコストの削減につながる可能性があります

さらに、まもなく公開される CMS Interoperability and Prior Authorization Final Rule により、対象の保険会社は追加の事前認証 API の導入を求められます。

また、コンプライアンス対策として、Fast Healthcare Interoperability Resources（FHIR）規格でも API のフォーマットが規定されています。これらの要件と規格により、システム間の相互運用性をシンプル化および合理化し、セキュリティを強化できます。FHIR では、セキュリティプログラムを導入し、そのプログラムに Web アプリケーションファイアウォール、認証、暗号化、プライバシー、マイクロセグメンテーションなどの基本的な機能を盛り込むように求めています。

ヘルスケア機関は以前より多くのデータを共有するように求められ、標準的な形式で（患者が使用する）患者のヘルスアプリケーションにタイムリーに接続できるように環境を整備する必要がありますが、FHIR 規格の意図は、管理負担を軽減し、透明性を高めることにあります。そのため、患者はサービスレベルの改善を期待できます。

さらに、データ交換で遅延が発生すると、情報ブロッキングによる罰金の対象になるなど、医療に悪い（そして多くの場合、高コストにつながる）影響が出る可能性があります。したがって、最近になってクラウドに移行したヘルスケア機関は、新フォーマットの外部向け API を展開することで、こうした新しいコンプライアンス対策に準拠しています。

API を標的とした攻撃のリスクに加えて、DDoS やランサムウェアなど、可用性を妨げる攻撃は、今後もあらゆる業界に影響を及ぼし、ヘルスケア業界は大きな影響を受ける業界の 1 つと言えます。こうした攻撃に対処するための規制は、回復力を重視する傾向があります。たとえば、米国では、HHS が Healthcare Sector DDoS Guide を公開しました。さらに、NPO の Healthcare Information Sharing and Analysis Center は、Resilience is in our DNA というヘルスケア分野における回復力の問題についてまとめたホワイトペーパーを発行しました。

対策の実施：推奨される緩和対策

API セキュリティは、リスク管理とコンプライアンスの観点から、かつてないほど重要になっています。しかし、API の無秩序な拡大が原因で、ヘルスケア API の特定、カタログ化、保護がますます困難になっています。さらに、ヘルスケア組織は、サービスの可用性を妨げる DDoS 攻撃を防ぐ必要があります。

攻撃を防ぐためには、まず攻撃を把握しなければなりません。そのためには、最初にすべてのアセットを把握し、セキュリティプログラムの対象とする必要があります。次に、どのような脆弱性が存在するのか、また、パフォーマンスとセキュリティの両面において、何が起きているのかを認識しなければなりません。最後に、自動型および従来型のペネレーションテストを通じて、システムのセキュリティを検証する必要があります。

以下で解説する API および DDoS 保護戦略のマイルストーンを達成することで、強固なセキュリティプログラムを導入できます。

API 保護戦略の 5 つのマイルストーン

強固な API セキュリティプログラムを導入することで、すべての API に対する可視性が改善され、リスクの状況の理解を深めて、保護体制を強化できます。

1. 野良 API またはシャドウ API を徹底的に探索することによってインフラの盲点を取り除き、そのような API が廃止されるか、API セキュリティ制御に組み込まれるようにします。

2. よくあるアラートの種類の分析、API コードの欠陥の修正、誤設定の問題への対処、教訓に基づいて将来の脆弱性を防止するプロセスの実行により、リスクへの対策を確立し、強化します。

3. 正常なふるまいを把握し、API セキュリティアラートの急増に基づいて悪用の可能性を見極めることで、脅威検知と対応を強化します。その後、適切に定義された対応手順を実施して、リスクとアラートの量を通常レベルまで引き下げます。

4. トレーニングと専門知識を提供するベンダーと提携します。プロジェクトベースのサポートから、複雑な統合型のサイバーセキュリティソリューションを適切に構成して管理できるフルマネージド型のサービスまで、幅広いサービスを提供できるベンダーを選びましょう。

強固な API セキュリティプログラムを導入することで、すべての API に対する可視性が改善され、リスクの状況の理解を深めて、保護体制を強化できます。

5. 後手に回る前に潜在的な脅威を特定することを目的とした正式な API 脅威ハンティングの統制を確立することで、オフェンス体制を強化します。

DDoS 保護戦略の 4 つのマイルストーン

レイヤー 7 Web ページおよび API、レイヤー 3 および 4 インフラ、DNS システムに対する DDoS 攻撃が記録的な水準にまで急増する中、サービスと機能の可用性を確保することが重要になっています。そのためには、最新の攻撃の規模、範囲、速度に対応できるだけのアクティブな保護が必要です。

1. 攻撃に対する可視性と速やかな対応をもたらすシステムを導入します。レイヤー 7、レイヤー 3 および 4、DNS インフラを保護できるシステムが必要です。

2. オンプレミス DDoS 保護に加えて、ハイブリッド DDoS 緩和プラットフォームを導入して、オンプレミスアプリケーションを過負荷状態にする攻撃から防御します。

3. ヘルスケア機関を関与させるか、ポリシーと IP 許可リストを簡単に管理して維持できるシステムを使用します。このシステムにより、実用的な分析をリアルタイムで獲得し、事前対応型のセキュリティ体制を導入できるようになります。

4. テストを介してアラート、保護機能、危機管理プロセスを検証し、すべてのインフラが適切に保護されるように体制を整えます。

詳細については、最新の調査をご覧いただくか、Akamai のブログをお読みください。

レイヤー 7 Web ページおよび API、レイヤー 3 および 4 インフラ、DNS システムに対する DDoS 攻撃が記録的な水準にまで急増する中、サービスと機能の可用性を確保することが重要になっています。

手法

Web アプリケーションおよびレイヤー 7 DDoS 攻撃

このデータは、Akamai の Web アプリケーションファイアウォール（WAF）を通じて観測されたアプリケーションレイヤーのアラートです。保護されている Web サイト、アプリケーション、API へのリクエスト内に悪性のペイロードを検知した場合に、Web アプリケーション攻撃アラートが作動します。レイヤー 7 DDoS のアラートは、保護対象の Web サイト、アプリケーション、API に対するリクエストの数に異常を検知した際に発せられます。このアラートは、悪性のリクエストと良性のリクエストのいずれによっても発動されます。通常、リクエスト自体は良性ですが、リクエスト数が大量になると、悪質な意図が疑われます。このアラートは、攻撃が成功したことを意味するものではありません。この製品では高度なカスタマイズが可能ですが、このレポートで提示されているデータは、保護対象のプロパティのカスタム設定を考慮せずに収集されています。

データは、Akamai Connected Cloud で検知されたセキュリティイベントを分析するための内部ツールから抽出されました。Akamai Connected Cloud とは、130 か国以上、1,300 近くのネットワーク上の 4,000 か所以上に配置された約 34 万台のサーバーからなるネットワークです。このデータは、ペタバイト／月の単位で測定され、Akamai セキュリティチームによる攻撃のリサーチ、悪性のふるまいの警告、Akamai ソリューションへのインテリジェンスの追加のために使用されます。

2023 年 1 月 1 日～ 2024 年 6 月 30 日までの 18 か月間のデータを使用しています。

データ更新について（2024 年版）

10 周年という節目を迎え、この機会に、当社のデータセットの更新について説明します。当社は、Web アプリケーションとボット攻撃のデータセットに関して、数回のアップグレードを実施してきました。それぞれの収集方法について、変更、合理化、最適化を行ってきました。知見の範囲と深さが広がりました。SSRF など、攻撃ベクトルの分類を追加してきました。API エンドポイントを標的にする攻撃の識別も各データシートに追加してきました。これらの改善点の一部は、本レポートでご紹介しました。今後もこの「SOTI ／セキュリティ」レポートを通じて、読者の方々に最新状況を引き続きお知らせしようと考えています。

クレジット

Research director
Mitch Mayne

共同執筆者
Neil Jennings
Chris Notaro
Charlotte Pelliccia
Badette Tribbey
Maria Vlasak
Steve Winterfeld

校閲およびテーマ別寄稿者
Claire Broome
Shane Keats

データ分析
Chelsea Tuttle

販促資料
Barney Beal

マーケティング・出版
Georgina Morales Hampe
Emily Spinks

その他の「インターネットの現状／セキュリティ」レポート

高い評価を受けている Akamai の「インターネットの現状／セキュリティ」レポートのバックナンバーおよび今後のリリースについては、**akamai.com/soti** をご覧ください。

その他の Akamai の脅威リサーチ

akamai.com/security-research では、最新の脅威インテリジェンス分析、セキュリティレポート、サイバーセキュリティリサーチを通じ、常に最新情報を把握できます。

このレポートに掲載されているデータ

このレポートに引用されているグラフや図のハイクオリティバージョンを以下のリンクからご覧いただけます。これらの画像は、出典元として Akamai を明記し、Akamai のロゴをそのまま残すことを条件に、利用および引用が可能です：**akamai.com/sotidata**

Akamai ソリューションの詳細

ヘルスケア業界を標的とする脅威に対する Akamai のソリューションについて、詳しくは**ヘルスケアおよびライフサイエンスのページ**をご覧ください。

Akamai のセキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。当社のグローバルプラットフォームの規模と脅威に対する可視性を活用して、お客様と Akamai が提携し、脅威を防止、検知、緩和することで、ブランドの信頼を構築し、ビジョンを実現できます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、X（旧 Twitter）と LinkedIn で Akamai Technologies をフォローしてください。公開日：2024 年 10 月。