Presented by

Trellix ADVANCED RESEARCH CENTER

# TRELLIX HEALTHCARE CYBERSECURITY THREAT INTELLIGENCE REPORT

日本語翻訳版

Analysis Period: January 1 - December 31, 2025

Sector Focus: Global Healthcare

Classification: TLP: White

# TABLE OF CONTENTS


1. Executive Summary
   2025年のヘルスケア産業における脅威の状況

2. The Financial Reality of Care Disruption
   **ケア中断がもたらす財務的現実**
   侵害の費用と運用停止
   規制および長期的な財務的影響
   主要な財務指標

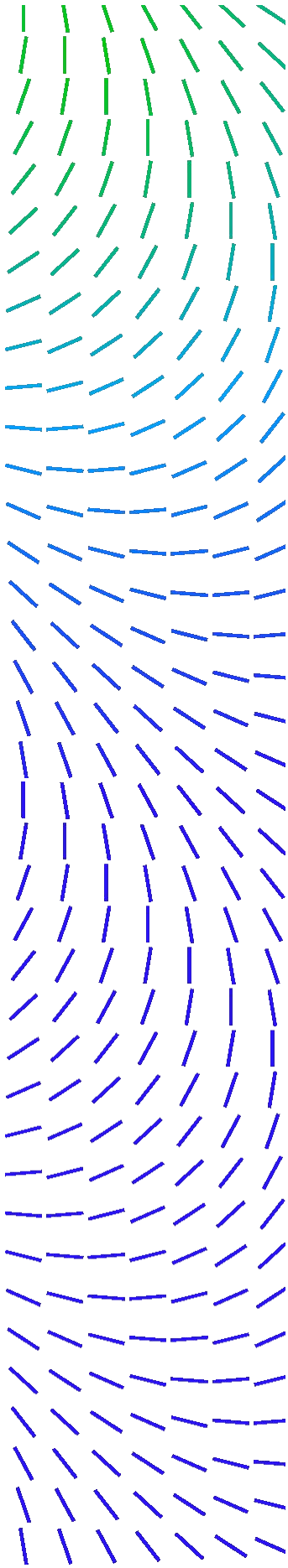
3. The 2025 Adversary Profile: From Ransomware to Patient Extortion
   **2025年の攻撃者プロファイル：ランサムウェアから患者恐喝へ**
   テレメトリーとインテリジェンスの概要
   アクティブな脅威オペレーションとキャンペーンの追跡
   脅威アクターの詳細分析
   戦略的トレンド：患者恐喝
   Ransomware-as-a-Service (RaaS) の経済的変化

4. Landmark Healthcare Cybersecurity Incidents in 2025
   **2025年の象徴的なヘルスケアサイバーセキュリティインシデント**
   侵害の傾向と影響分析
   プロバイダー対ビジネスアソシエイトのリスク
   注目すべきヘルスケア侵害

5. Tactics, Techniques, and Procedures (TTPs)
   **戦術、技術、および手順 (TTPs)**
   Initial Access Methods：初期アクセス手法
   Credential Access：認証情報へのアクセス
   Lateral Movement and Clinical Pivot：ラテラルムーブメントと臨床ピボット
   Impact and Data Destruction：影響とデータ破壊
   Command-and-Control and Technical Indicators：
   コマンド・アンド・コントロールと技術的指標

6. The Vulnerability Matrix: IoMT and OT Exposure
   **脆弱性マトリックス：IoMTおよびOTの露出**
   Medical Device Exploitation Trends：医療機器の悪用トレンド
   Critical Vulnerabilities and CVE Breakdown：重大な脆弱性とCVEの内訳
   Legacy and End-of-Life System Risk：
   レガシーシステムおよびサポート終了システムのリスク
   Operational Technology (OT) as an Attack Vector：
   オペレーショナルテクノロジー（OT）を攻撃ベクトルとして

7. Strategic Recommendations for Healthcare Security Leaders
   **ヘルスケアセキュリティリーダーへの戦略的推奨事項**
   脅威インテリジェンス主導の防御
   Eメール、ネットワーク、ID、エンドポイントセキュリティの優先事項
   脆弱性への優先順位付けとリスク軽減
   PHI保護と持ち出し防御
   SOC主導のインシデント対応とレジリエンス

## EXECUTIVE SUMMARY

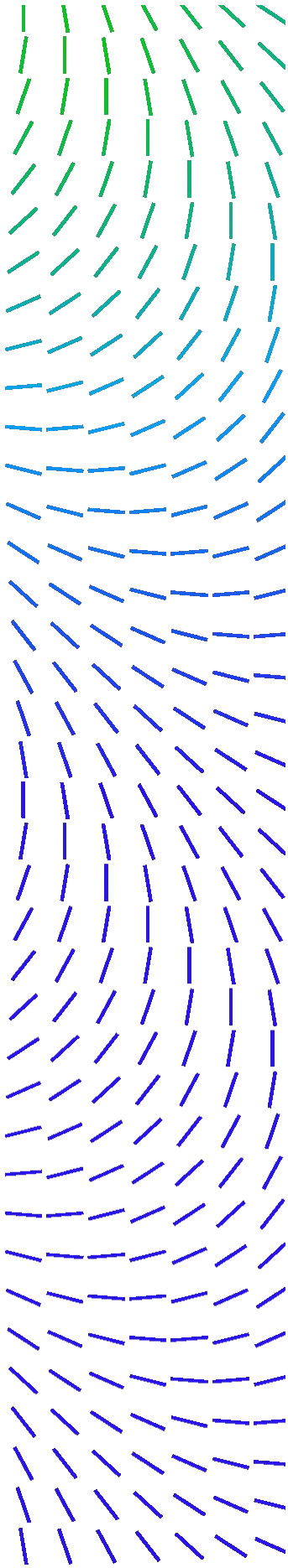
何十年もの間、病院や医療提供者は、サイバーセキュリティではなく、患者の安全を最優先に設計された、大部分が隔離された臨床システムに依存してきました。多くの医療機器は、限られた接続性と外部脅威への最小限の露出で、閉鎖された環境で運用されてきました。これは、ネットワークにさらされた患者監視システムに関するTrellixの調査を含む初期の研究にも反映されている現実です。

しかし今日、そのモデルは根本的な変化を遂げました。ヘルスケア分野は、効率性、相互運用性、ケアの質を向上させるために、クラウドプラットフォーム、リモートアクセス、そしてインターネット接続された医療機器を急速に導入しています。このイノベーションは本質的に前向きなものですが、同時に攻撃対象領域を拡大し、臨床技術を、それが耐えるように設計されていなかった脅威にさらしています。人工知能がこの分野全体のデジタルトランスフォーメーションを加速させるにつれて、接続性のペース、そしてそれに伴う患者の安全へのリスクは増大し続けるでしょう。

Trellixはヘルスケア組織の大規模な顧客基盤を維持しており、現在の脅威の状況に対する独自の視点を提供しています。2025年に、当社のテレメトリーは、ヘルスケア業界の顧客によってインストールされた複数のTrellixセキュリティ製品全体で5,470万件の検出を記録しました。これらの検出は、確認された成功した攻撃ではなく、当社のテレメトリーによってフラグが立てられた潜在的なセキュリティイベントを表していますが、ヘルスケアネットワークを通過するノイズと潜在的なリスクの膨大な量を浮き彫りにしています。注目すべきは、これらのグローバルな検出の75%が米国を拠点とする顧客からのものであり、米国のヘルスケアインフラストラクチャに対する不均衡な標的化を強調しています。

今年は、データ侵害にかかる費用が最も高いセクターとしての地位を15年連続で維持しました。世界的な侵害コストは落ち着きましたが、米国では **1件あたり1,022万ドル** という過去最高の記録を樹立しました。

2025年を決定づけるトレンドは「連鎖的影響（Cascading Effect）」でした。これは、建物のHVACなどの管理ネットワークまたは非臨床オペレーショナルテクノロジー（OT）システムへの侵害が、医療システム全体の臨床ワークフローを麻痺させる可能性があるという変化です。これらの混乱は単に財務的なものではなく、致命的でした。クラウド/アカウントの侵害、サプライチェーン攻撃、ランサムウェア攻撃、ビジネスメール詐欺（BEC）インシデントなどのサイバー攻撃の影響を受けた病院では、入院患者の死亡率が 29%増加し、近隣の病院では緊急転送により心停止の症例が 81%急増したことが、調査で確認されています。



## THE FINANCIAL REALITY OF CARE DISRUPTION
**ケア中断がもたらす財務的現実**

2025年の財務上の損失は、記録的な身代金の額だけでなく、システム的な運用停止がもたらす予測不可能な莫大なコストの結果でもありました。

IBM 2025年データ侵害のコストレポート によると、ヘルスケア侵害の平均コストは2024年の977万ドルから742万ドルに減少しました。この減少にもかかわらず、ヘルスケアは14年連続で最もコストのかかるセクターであり続けています。これは主に、HIPAAのような厳格な規制要件や、IBMが調査した業界の中で最長となる279日という検知・封じ込めサイクルの長さによるものです。

- ブラックマーケットのプレミアム：単一の電子健康記録（EHR）は現在、ダークウェブで約60ドル で売買されており、これは盗まれたクレジットカードの約20倍の価値に相当します。この高い評価が、「静かな」データ流出攻撃の増加を促進しています。このプレミアムをさらに裏付けるように、Trellixは2023年後半に、米国の医療提供者の医療記録を侵害されたアカウントあたり250ドルで提供する脅威アクターを観測しており、これは専門的な、または完全性の高い臨床データセットが、一般的なブラックマーケットの平均をはるかに超える価格をつけられることを示しています。
- コストの内訳（侵害あたりの平均）：
  - 検出とエスカレーション：147万ドル
  - ビジネス損失（ダウンタイム/評判）：138万ドル
  - 侵害後の対応（法務/通知）：120万ドル

ヘルスケアシステムにとって、「時は金なり」は文字通り、壊滅的な意味合いを帯びます。ComparitechとCensinetの業界ベンチマークが示唆するところ：

- **1分あたりのコスト：** 7,500ドルから9,000ドルの間。
- **1日あたりのコスト：** 平均190万ドルの収益損失および復旧費用。
- **継続期間の危機：** 2025年、平均的なヘルスケア組織は1回の攻撃あたり17日以上のダウンタイムに直面し、一部の主要システムでは数か月にわたる部分的停止を経験しました。大規模な攻撃からの完全な復旧には100日以上かかったと76%の組織が報告しました。

大手サードパーティのクリアリングハウス侵害（2025年初頭の報告にまで及ぶ）による財務上の波紋は、業界全体の混乱の青写真を提供しました。親会社は、その単一のインシデントの総費用が29億ドルを超える可能性が高いと報告しました。

AMAの2025年の分析 によると、診療所の80%が未払い請求による収益を失い、55%が診療費用を賄うために自己資金を使用する必要がありました。小規模な施設にとって、2025年に 4倍に増加した 20万ドルの損失は、存続と閉鎖の分かれ目となることがよくあります。

### Regulatory and Long-term Financial Impact

- 価格引き上げの影響：これらの驚異的なコストを吸収するため、侵害を受けたヘルスケア組織の ほぼ半数（48%）が、医療サービスの価格を引き上げると報告しており、中には15%以上の引き上げに達するものもあります。
- HHS-OCRによる罰則：2025年には執行が積極的に強化されました。HIPAA違反に対する連邦民事罰は、「意図的な怠慢」に対する最高ティアに達することが多くなり、未是正の違反の一部は年間150万ドルを超える費用がかかっています。

### Key Financial Metrics

- Average Cost of US Breach: 1022万ドル（2024年から9.2%増加）
- Downtime Cost: 全システム停止時、現代の病院の運用は1分あたり約9,000ドルの損失
- Detection & Escalation: これらのコストは1インシデントあたり平均 147万ドルで、複雑な臨床ネットワークで「静かな」アクターを見つけることの難しさを反映しています。

## THE 2025 ADVERSARY PROFILE: FROM RANSOMWARE TO PATIENT EXTORTION

**2025年の攻撃者プロファイル：ランサムウェアから患者恐喝へ**

2025年の脅威アクターは、単純な暗号化を超え、「三重の恐喝」、すなわちデータ窃盗、サービス妨害、そして個々の患者への嫌がらせへと移行しました。Ransomware-as-a-Service（RaaS）のエコシステムは、Change Healthcare侵害による注目度の高い余波を受けて激しい再編成を経験し、より攻撃的でアフィリエイト中心のモデルへと変化しました。

Trellixのテレメトリーと標的型キャンペーンの追跡が示すように、2025年における脅威アクターの活動規模は依然として高い水準にあります。このデータは、ヘルスケア分野特有の脆弱性に特化して調整された、持続的で大量の脅威環境を明らかにしています。

### Trellix Telemetry and Intelligence

- 総検知数:Trellixは、2025年を通じて世界中のヘルスケア関連顧客組織全体で5,470万件の検出を記録しました。
- 総検出数の85%はTrellix Email Securityによるものです
- Geographic Concentration: 米国がこの活動の主要な震源地であり続け、全ヘルスケア検出の75.14%を占めました。

## Active Threat Operations (Campaign Tracking)

- 対象のキャンペーン: 当社のAdvanced Research Centerは、2025年にヘルスケアインフラストラクチャを侵害するために特別に設計された109のユニークなキャンペーンを特定しました。
- 活動のピーク: Trellixのテレメトリーは、2025年上半期に最も多くの活動を観測し、1月と3月にはEメール検出で孤立したスパイクが見られました。

## Threat Actor Deep-Dive

Qilin：Qilinは2025年にハイテンポなオペレーションへと成熟し、月間二桁の被害者投稿に注力しました。彼らは、重要なEHRデータベースを格納するバックエンドサーバーを標的とする、洗練されたLinuxおよびESXi対応のペイロードで知られています。

- インシデントハイライト：2025年5月、米国の主要な病院システムが大規模なQilin攻撃を受け、478,188件の患者記録に影響が出ました。このグループは852GBのデータ（135万ファイル）を不正に持ち出しました。Qilinは、「患者恐喝」という戦術で悪名高く、医療提供者を介さずに患者に直接診断結果をテキストメッセージで送り、公開を防ぐための「プライバシー料金」を要求します。

INC Ransom: 2024年から2025年にかけて最も多作なヘルスケア標的型オペレーションの一つとして台頭したINC Ransomは、観測された34件の攻撃で目覚ましい一貫性を示し、全ヘルスケア攻撃の7.9%を占めました。彼らのヘルスケアへの標的化は2025年にピークを迎え、彼らの全オペレーションの大部分を占めています。

- インシデントハイライト：TrellixのEnriched Ransomlookデータセットによって追跡されたランサムウェア被害者の投稿に基づくと、2025年にINC Ransomはヘルスケアキャンペーンを実行しました。これには、北米の地域病院、国の公衆衛生システム、南半球の主要な病院などの注目度の高い標的が含まれていました。

Devman2: 2024年後半から壊滅的な効率で活動しているDevman2は、観測された26件の攻撃（全ヘルスケア攻撃の6.1%）により、国際的なヘルスケアインフラストラクチャに対する主要な脅威としての地位を確立しました。このグループは、大規模なデータ流出で悪名高く、個々のヘルスケア侵害で盗み出された患者データは一貫して1インシデントあたり200GBから300GBに及んでいます。

- インシデントハイライト：TrellixのEnriched Ransomlookデータセットによって追跡されたランサムウェア被害者の投稿に基づくと、2025年12月はDevman2の最も攻撃的なヘルスケアキャンペーンとなり、単月で23のヘルスケア被害者を主張しました。チリの主要な民間ヘルスケアネットワークへの攻撃では、250GBのデータが盗まれました。同時に、彼らはフランスの病院（221GB）と米国のプロバイダー（QuickBooksの財務ダンプを含む300GB）にも侵入しました。

Sinobi: 2025年7月という比較的最近に登場したにもかかわらず、Sinobiは観測された21件の攻撃で、全ヘルスケア攻撃の4.9%を占める重大な脅威として急速に地位を確立しました。彼らの急速な台頭と、バイオテクノロジーのような専門企業への即座の注力は、経験豊富なオペレーターが新しいブランドを立ち上げたか、洗練された初期アクセス能力を持っているかのいずれかを示唆しています。

- インシデントハイライト：TrellixのEnriched Ransomlookデータセットによって追跡されたランサムウェア被害者の投稿に基づくと、Sinobiの2025年10月の「電撃戦」により、製薬メーカーから個人の歯科医院に至るまで、単月で13のヘルスケア被害者が発生しました。そして、2026年1月にはすでに、専門的なライフサイエンス企業や高齢者向けサービス部門を標的としたオペレーションを開始しており、高価値のヘルスケアテクノロジーや専門的なケア提供者へと進化していることを示しています。

Medusa: 2024年から2025年を通じて安定したヘルスケアオペレーションを維持したMedusaは、18件の攻撃が観測され、全ヘルスケア攻撃の4.2%を占めました。このグループは、詳細なデータ定量化と、主要な製薬企業およびメンタルヘルスプロバイダーへの体系的な標的化によって際立っています。

- インシデントハイライト：TrellixのEnriched Ransomlookデータセットによって追跡されたランサムウェア被害者の投稿に基づくと、Medusaによる2025年9月の主要製薬会社への侵害は、478.2GBのデータ持ち出しを引き起こしました。これは、同年の製薬業界における最大級の侵害の1つです。HIPAAの下で最も保護された医療情報を扱う組織への標的化は、地域のメンタルヘルス当局と専門のHIV/AIDSケア提供者への攻撃によって際立っていました。

Interlock: 2024年後半に登場した Interlockは、北米のヘルスケア分野に明確に焦点を当て、重要インフラに対する高度な脅威として急速に地位を確立しました。このグループは、「珍しい」初期アクセス戦術で知られており、侵害された正規のウェブサイトでドライブバイダウンロードを頻繁に使用し、偽のブラウザアップデート（例：ChromeやEdge）やセキュリティソフトウェアパッチをプッシュして、独自のInterlock RATを展開します。彼らは二重恐喝モデルで運用し、多くの場合、特に仮想マシン（VM）環境を標的にし、AzCopyのような正規のツールを利用して、暗号化を起動する前に大量のデータセットをクラウドストレージに持ち出します。

- インシデントハイライト：2025年初頭、Interlockは腎臓透析大手を標的とし、その検査データベースから約1.5テラバイトのデータを不正に持ち出しました。この侵害は最終的に270万人に影響を与え、氏名、社会保障番号、臨床治療記録が流出しました。Interlockはまた、地域医療システムでの影響の大きい混乱にも直接関与しており、その結果生じたシステムダウンタイムは、選択的処置のキャンセルを余儀なくさせ、患者の安全に重大なリスクを生じさせました。

RansomHub: 2025年初頭、RansomHubはヘルスケア分野を標的とする最も影響力のあるグループの一つでした。その成功は、90%の手数料を提供し、アフィリエイトに身代金取引を直接扱わせるという、革新的なアフィリエイトモデルによって推進されました。これにより、ALPHV/BlackCatのような活動を停止したグループから優秀な人材が集まりました。

- インシデントハイライト：RansomHubは、大手保険会社のラテンアメリカ部門や大規模なビジネスアソシエイトを含むいくつかの大容量侵害の責任を主張し、数百万件の記録が流出する可能性をもたらしました。彼らの戦術はデータ流出のみを目的とした攻撃を好みます。これは、医療データを漏洩させると脅すことが、暗号化という技術的なハードルよりも効果的であるとグループが認識したため、2025年にはその頻度が3倍になりました。

Cl0p: 2025年後半、Cl0pランサムウェアグループは、オンプレミスのOracle E-Business Suite (EBS) システムを標的とした大規模なキャンペーンを実行しました。パッチがリリースされる数カ月前から、CVE-2025-61882とCVE-2025-61884をゼロデイとして悪用することで、彼らはヘルスケアサプライチェーンの組織を含む、約30の主要な組織を侵害しました。彼らの戦略は、個々の病院を標的とするのではなく、広く使用されているエンタープライズソフトウェアを介した「大量の被害者化」に焦点を当てています。

Rhysida: Rhysidaは依然として大きな脅威であり、年間を通じて強力なヘルスケアへの注力を維持しました。彼らは「二重の危機」アプローチで知られており、データを公開する前に、しばしば7日間の厳しい支払い 期間を使用します。

- インシデントハイライト：2025年半ば、Rhysidaは専門的な外科センターと地域の医療グループをリークサイトに追加し、SQLデータベースと保険証券の盗難を主張しました。CISAは2025年4月にRhysidaに関する#StopRansomwareアドバイザリを更新し、彼らの新しい「CleanUpLoader」と「OysterLoader」の初期アクセスツールに対応しました。

### Strategic Trend: The "Patient Extortion" Game
### 戦略的トレンド: 患者恐喝ゲーム

Health-ISAC　2025年の脅威の概観レポート によると、患者恐喝はサイバー犯罪者にとって引き続き主流の収益源となっています。

- 少額バッチ恐喝の経済性：患者一人あたりわずか50ドルから500ドルを要求することで、攻撃者は企業の保険や法務チームを迂回します。2025年には、ヘルスケア提供者に対する恐喝のみの攻撃が 全ヘルスケア攻撃の12%で観測され、2023年以降300%の増加を示しました。

### The RaaS Economic Shift

2025年の驚くべき傾向は、平均身代金支払額の減少でした。件数は高水準を維持したものの、ヘルスケア分野での平均身代金支払額は147万ドルから15万ドルに急落しました。これは、中程度の要求（100万ドル～500万ドル）が大幅に引き下げられて交渉される傾向を反映しており、2025年に支払いを選択したプロバイダーはわずか36%と過去最低を記録しました。

## LANDMARK HEALTHCARE CYBERSECURITY INCIDENTS IN 2025
**2025年の象徴的なヘルスケアサイバーセキュリティインシデント**

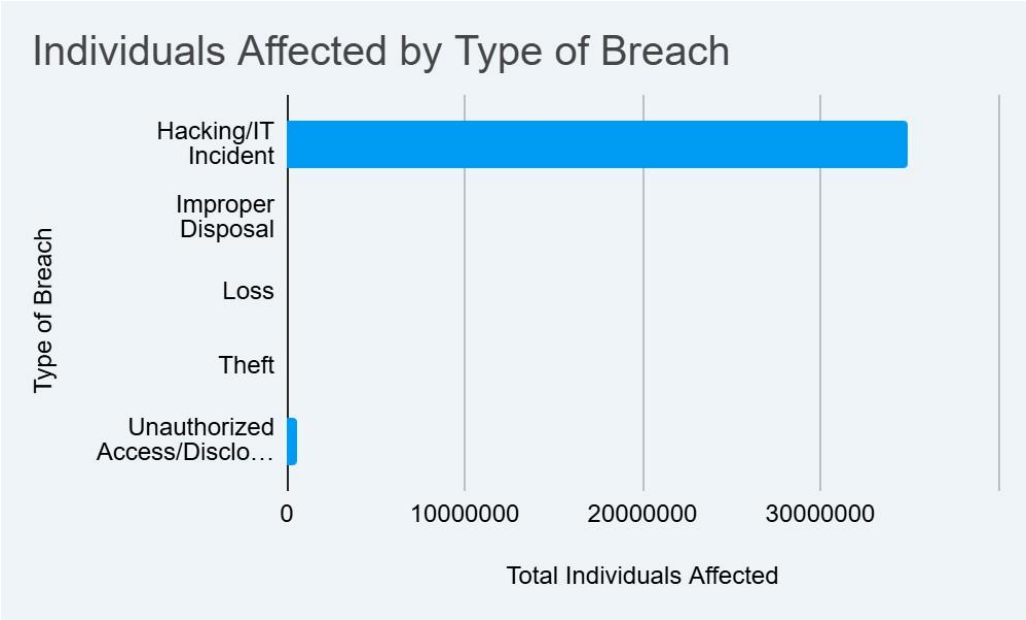
In 2025, the U.S. Department of Health and Human Services (HHS) は、約516件の侵害を公表し、3,550万人以上の個人に影響を与えました。それぞれの侵害は、スプレッドシート上の単なるデータ以上のものを意味します。それは、患者が自身のプライバシーについて不安に直面し、組織が信頼を回復するために奔走することを意味します。

### Key Takeaways from the Breach Report Data
ハッキング/ITインシデントが主要な脅威であり、影響の主な要因である。

ハッキング/ITインシデントは、データセットにおいて、発生件数と影響を受けた個人の数の両面で、圧倒的に最も頻繁で影響力の大きい種類の侵害です。

- 発生頻度の高さ：全516件のうち410件 (79%)がハッキング/ITインシデントに分類されました。
- 影響の規模：この種類の侵害は、影響を受けた全個人3,550万人のうち3,490万人（総影響の98%以上）を占めました。
- 発生場所：侵害の主な発生場所はネットワークサーバー（306件）で、次にEメール（120件）が続き、ハッキング/ITインシデントの性質と一致しています。

以下のチャートは、ハッキング /ITインシデントの影響が他のすべての種類の侵害と比較してどれほど大きいかを示しています。




Source: (U.S. Department of Health and Human Services Office for Civil Rights Breach Portal)

ヘルスケア提供者はより頻繁に侵害に遭うが、ビジネスアソシエイトの侵害は平均してより多くの人々に影響を与える

ヘルスケア提供者が最も高い頻度で侵害に遭う一方で、ビジネスアソシエイトが関わる侵害は規模が大きくなる傾向があり、侵害された個人の総数のかなりの部分に影響を与えます。

- 頻度: ヘルスケア提供者は360件の侵害を報告しており、ビジネスアソシエイトが報告した101件よりも著しく多い。
- 影響: ヘルスケア提供者が関わる侵害は、約1,910万人の個人に影響を与えたのに対し、ビジネスアソシエイトが関わる侵害は、ほぼ同等の1,540万人の個人に影響を与えた。
- 平均的規模: この頻度と総影響の差は、ビジネスアソシエイトが関わる平均的な侵害が、ヘルスケア提供者が関わる平均的な侵害よりも、より多くの個人に影響を与えることを示唆しています。

不正アクセス/開示は2番目に多い問題ですが、個人への影響ははるかに少ない

ハッキング/ITインシデントが支配的である一方で、次に最も一般的な問題は、明確な運用上またはプロセスに関連する問題、すなわち不正アクセス/開示です。

- 2番目の頻度: 不正アクセス/開示は85件で、2番目に多い種類の侵害となりました。
- 限定的な個々の影響: 発生頻度にもかかわらず、この種類の侵害による影響を受けた個人はわずか580,976人であり、ハッキング/ITインシデントによる影響を受けた個人のごく一部に過ぎません。

## Notable Incidents

### Major Academic Health System Compromise: 550万人の患者情報が流出

2025年3月、ある主要な学術医療システムがITネットワーク上で異常な活動を発見しました。これは急速に拡大し、2025年最大のヘルスケア侵害となり、550万人に影響を与えました。

- 詳細: 攻撃者は機密性の高い人口統計学的詳細と社会保障番号を不正に持ち出しました。臨床システムは無傷のままでしたが、その甚大な規模により、後に訴訟および管理費用を賄うための1,800万ドルの和解金が支払われました。

### サプライチェーンの混乱：ビジネスアソシエイト経由：540万件の記録

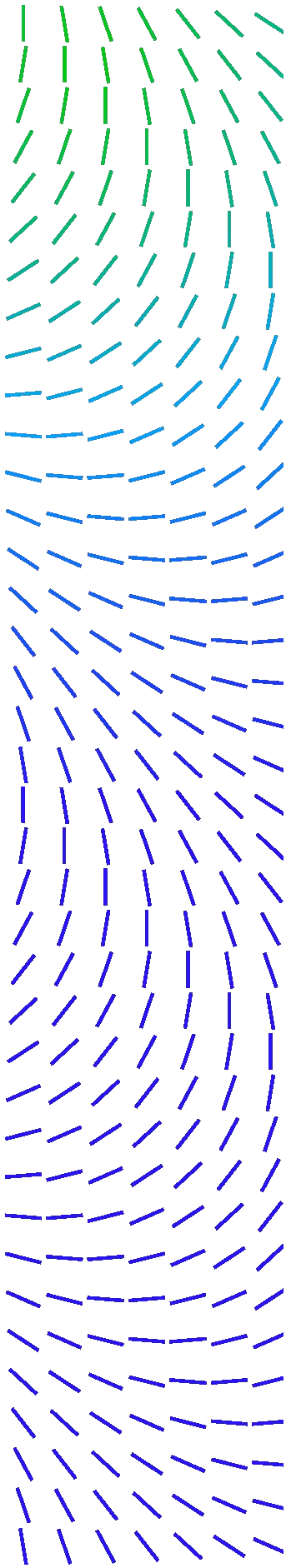
2025年1月下旬から2月上旬にかけて、大手ビジネスアソシエイトがランサムウェアによる侵入を受けました。同社は業界の巨大企業の主要パートナーであるため、この侵害により540万人の個人情報が漏洩しました。

- サプライチェーンへの影響：波及効果は甚大で、複数のパートナーが個別にインシデントを報告せざるを得ませんでした。

### ある腎臓透析大手がランサムウェアの被害に：100万人に影響

ある腎臓透析大手が2025年3月から4月の間にInterlockランサムウェアグループの犠牲となりました。

- 影響：当該グループは、医療記録と納税者番号を含む1.5テラバイトのデータを不正に持ち出しました。
- コスト：当該プロバイダーは、主に修復とシステム復元のために、SEC提出書類において1,350万ドルの直接費用を開示しました。



### 大手健康保険プランの誤設定：470万人の加入者の誤設定

2025年4月、米国の大手健康保険プラン提供者が、470万人の加入者に影響を与える重大なプライバシーインシデントを開示しました。これはハッキングではなく、広告サービスの誤設定でした。

- 詳細: 約3年間、機密性の高い加入者データ（「医師を探す」検索を含む）が広告サービスと共有されており、保護医療情報に基づいてターゲティング広告が行われる可能性がありました。

### 大手仲介業者に対するID攻撃：110万件の記録

このインシデントは、2025年初頭に開示されたもので、大手保険仲介業者に対する標的型アイデンティティ攻撃に関わるものでした。攻撃者は、たった数時間のうちに一人の従業員のコンピューターにアクセスし、その間に112万人の個人データを不正に持ち出しました。

- 詳細：これは、ID脅威検出と対応（ITDR）およびセッショントークン保護が、最新のヘルスケアセキュリティスタックの重要なコンポーネントである理由を示す好例です。

## TACTICS, TECHNIQUES, & PROCEDURES (TTPS)
**戦術、技術、および手順 (TTPs)**

外部のライフライン部門の妨害が病院の利用可能性に深刻な「波及効果」をもたらす一方で、脅威アクターは同時に「臨床ピボット」—内部の管理ネットワークから臨床環境に直接移行する方法—を完成させています。この融合は、ヘルスケアにおけるサイバーセキュリティが単なる技術的な問題ではなく、患者の安全に不可欠なものとなる根本的な変化を表しています。以下のセクションでは、より広範な重要インフラストラクチャのキャンペーンで観察されるインフラストラクチャの混乱戦略を反映し、ITと臨床の境界を悪用するために使用される特定の戦術、技術、手順（TTP）について詳述します。

### Initial Access

フィッシング (T1566.001)：依然として主要なベクトル（89%）ですが、進化しています。アクターは現在、「AIトランスフォーメーション」や「規制コンプライアンス」のテーマを利用して、管理スタッフを欺いています。

VPN悪用 (T1133)：SonicWall (CVE-2024-40766) および Fortinet デバイスの悪用は、Akiraにとって標準的な侵入ポイントとなりました。

### Credential Access

Credential Dumping (T1003.001): MimikatzとLaZagneは、看護師のワークステーションからLSASSメモリをダンプし、ドメインの認証情報を盗むために使用されます。

## Discovery & Lateral Movement

Living-off-the-Land (LotL): 攻撃者はネイティブツールを悪用して臨床ネットワークをマッピングします。

- WMI Queries: Get-WMIObject -Class Win32_NetworkAdapter は、MACアドレスベンダー（例：GE、Siemens）に基づいて医療機器を識別するために使用されます。
- PowerShell: ITネットワークと臨床ネットワークの交差点に位置することが多いPACS（画像）サーバーでリモートコマンドを実行するために使用されます。

## Impact (Data Destruction)

ESXi暗号化 (T1486)：ハイパーバイザーを標的とすることで、アクターは数百の仮想マシンを同時に暗号化できます。これは、EHR（電子健康記録）、PACS（画像アーカイブ通信システム）、およびラボシステムが同じクラスター上で仮想化されていることが多いヘルスケア分野では、特に壊滅的です。

## Technical Indicators and TTPs

コマンド・アンド・コントロール・インフラストラクチャ (Source: Campaigns + Detections)

**Domain Patterns:**

- ヘルスケアをテーマにしたドメイン: medical-update[.]com, hipaa-compliance[.]org
- タイポスクワッティング: microsft-teams[.]net, zoom-healthcare[.]com
- サブドメインの悪用: 悪意のあるサブドメインを持つ正規のヘルスケアドメイン。

**Network Indicators:**

- ビーコンパターン: 正当な医療機器の通信を模倣するための60秒間隔。
- データ持ち出し: ソフトウェアアップデートを装ったHTTPSトンネリング。
- 永続化メカニズム: WMIイベントサブスクリプション、医療プロセスにちなんで名付けられたスケジュールされたタスク。

**File-based Indicators:**

- マルウェアファミリー: Cobalt Strikeビーコン、Metasploitペイロード、カスタムPowerShellフレームワーク。
- 命名規則: 医療ソフトウェアに偽装したファイル: MedicalDeviceUpdate.exe, HIPAACompliance.pdf.exe.
- 永続化の場所: %PROGRAMFILES%¥Common Files¥Medical¥, 医療ソフトウェアに似せたレジストリキー。

## THE VULNERABILITY MATRIX: IoMT AND OT EXPOSURE

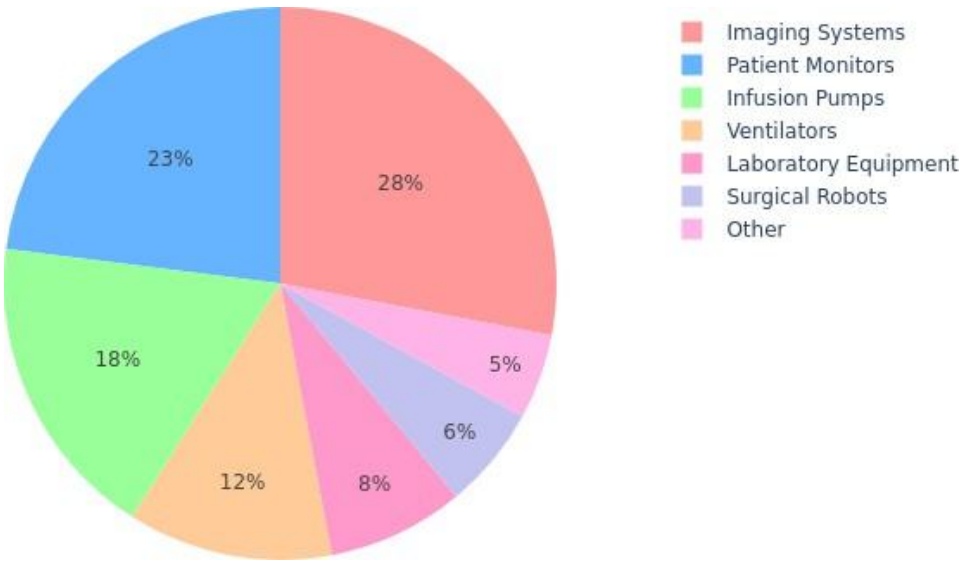
**脆弱性マトリックス：IoMTおよびOTの露出**

2025年のヘルスケアの攻撃対象領域は、ラップトップやサーバーのような従来の末端機器に限定されなくなりました。代わりに、それは医療モノのインターネット（IoMT）とオペレーショナルテクノロジー（OT）の複雑なウェブであり、現在、99%の病院が、既知の悪用可能な脆弱性（KEV）を持つデバイスを少なくとも1つ管理しています。

医療機器は、標準的なエンタープライズハードウェアと比較して、より高い密度のセキュリティ上の欠陥を抱えていることが多く、平均で1台あたり6.2件のソフトウェアバグがあります。

- 輸液ポンプ：2025年の20万台の輸液ポンプの大規模分析により、75%が1つ以上の既知のセキュリティ上の欠陥を保有していることが明らかになりました。半数以上がファームウェアの重大な2019年CVEの影響を受けやすく、多くはハードコードされたパスワードまたはデフォルトパスワードを持つレガシーファームウェアで稼働し続けており、ラテラルムーブメントの格好の標的となっています。
- 医用画像（DICOM/PACS）：CTスキャナーやMRIスキャナーを含む放射線機器は、古いオペレーティングシステムへの依存により、依然として主要な標的です。調査によると、DICOM/PACSワークステーションの32%に少なくとも1つの重大な未パッチの脆弱性があり、20%の画像システムは、主要なランサムウェア集団が積極的に悪用するKEVを抱えていました。
- 患者モニターとバイタルサインコントローラー：これらのデバイスは基本的なセキュリティ保護を欠いていることが多く、より広範なネットワークへのゲートウェイとして機能する可能性があります。Contec Health CMS8000に関する2025年の注目すべき開示では、デフォルトでプレーンテキストの患者データをハードコードされたパブリックIPアドレスに送信していたことが明らかになり、実質的にデータ漏洩のバックドアとして機能していました。

Medical Device Compromise Distribution (2025)
**医療機器の侵害分布** (2025年)




Medical Device Exploitation (Source: Detections + Underground)

## 2025 Critical Vulnerability & CVE Breakdown

以下の脆弱性は、2025年を通じてヘルスケア分野で特定または大規模に悪用され、臨床業務に重大なリスクをもたらしました:

- Contec Health CMS8000 (CVE-2025-0683): この重大な脆弱性は、患者モニターのファームウェアに 組み込まれたバックドア に関わるものです。デフォルト設定では、デバイスが プレーンテキストの患者データをハードコードされたパブリックIPアドレスに送信するため、不正なリモートアクターが個人医療情報を持ち出したり、デバイスを制御して意図しないアクションを実行したりすることが可能になります。

- Oracle E-Business Suite (CVE-2025-61882): このマルチステージの悪用チェーンは、認証のバイパスとリモートでのコード実行 を組み合わせ、ユーザー認証情報を必要とせずにOracle Concurrent Processingを侵害します。2025年10月6日、AHAはOracle EBSを使用するすべての病院に対し、直ちに対応するよう促す緊急アラートを発行しました。FBIはこれを、大規模なヘルスケアデータ窃盗における役割に注目し、「作業を止めて直ちにパッチを適用すべき」脆弱性として分類しました。Cl0pランサムウェア のような注目度の高いグループは、この欠陥を標的にして運用バックエンドをシャットダウンし、医療システムから機密性の高い従業員データや財務データを持ち出しました。英国最大の病院トラストの1つは、 Cl0pランサムウェアギャング の被害に遭い、2025年8月にこの特定のゼロデイが悪用され、財務データと患者関連の請求書データが盗まれたことを確認しました。

- Cisco Secure Email (CVE-2025-20393): この最大深刻度(CVSS 10.0)の ゼロデイ脆弱性 は、Spam Quarantine機能が有効になっている場合のAsyncOSソフトウェアに影響を与えます。2025年12月18日、NHS England Digitalは、Cisco Secure Emailアプライアンスを標的とした 進行中の悪用キャンペーン に関して、高深刻度のアラートを発行しました。

- SonicWall SMA 1000 (CVE-2025-40602): 認証チェックの不備により、Appliance Management Console (AMC) で見つかった重大なローカル権限昇格の欠陥です。2025年12月に公開されたこの脆弱性について、NHS England National CSOCは、ヘルスケアエンティティに対する将来的な悪用を「起こりうる」と評価しました。このアラートは、CVE-2025-23006と連鎖 した場合、この欠陥により認証なしでルート権限によるリモートコード実行(RCE)が可能になると警告しています。

## The "Legacy Gap": Unsupported Systems in Use

多くの病院における重大なセキュリティ上の欠陥は、セキュリティを考慮せずに設計されたレガシーデバイスへの依存です。

- End-of-Life (EoL) Dominance: 病院内の 医療機器の60%は耐用年数を過ぎており、セキュリティパッチがありません。
- Unsupported OS: 接続されている医療機器の5台に1台 がサポート対象外または耐用年数を過ぎたオペレーティングシステムで稼働しています。
- Dwell Time(滞留時間 ): パッチが適用された後でも、ヘルスケアデバイスは平均で3.2年間脆弱なままです。

## External Operational Technology (OT) Vulnerabilities and the Hospital Pivot

OT—HVAC、エレベーター、バックアップ電源、気送管を制御するシステム—は、攻撃者に何千もの侵入経路を提供します。

- Converged Risk: 2025年、Clarotyは OTシステムの65% (BMS、UPS、エレベーター)がKEVを抱え、インターネットに接続されていると評価しました。
- The Pivot Path: 攻撃者はパッチ未適用のHVACまたは電気コントローラーを侵害して足がかりを得ます。一度侵入すると、 DICOM画像ネットワークにラテラルムーブメントし、放射線科を効果的に麻痺させ、救急車の受け入れ先変更を強いる可能性があります。これらのシステムはEDRエージェントをホストすることがめったにないため、この「OTピボット」は従来のITセキュリティを回避します。
- USB Threats: OTシステムは「エアギャップ」されていることが多いですが、USB経由でパッチ適用や更新が行われたとしても、それらのOTシステムは安全ではない可能性があります。 2024年の調査 でUSBドライブ上で発見されたマルウェアの51%は、産業用および運用機器を侵害するように設計されていました。

# STRATEGIC RECOMMENDATIONS FOR HEALTHCARE SECURITY LEADERS

**ヘルスケアセキュリティリーダーへの戦略的推奨事項**

2026年のプロフェッショナル化された脅威の状況に対抗するため、ヘルスケア組織は「場当たり的な」セキュリティから、統一されたリスクベースの運用戦略へと移行しなければなりません。

この変革の要となるのは、ヘルスケアに特化した脅威インテリジェンス機能の開発です。Trellix Insights solutionとTrellix Intelligence-as-a-Service (INTaaS) サービスを通じて脅威インテリジェンスを活用することで、組織はリアクティブな防御からプロアクティブな予測へと移行し、攻撃が発生する前に特定の環境を標的とする可能性のある脅威を特定できるようになります。Trellix Insightsはさらに、リーダーシップがリアルタイムのグローバルセンサーデータに基づいてリスクに優先順位を付け、セキュリティ体制を最適化するための実行可能な修復手順を指示することを可能にします。加えて、全体的な戦略の一部として、以下が実施されるべきです。

**・高度なメール保護とフィッシング対策を実施する:**
当社の調査結果から、メールテレメトリーに起因する総検出数の85%と、初期アクセスの89%がフィッシングによって引き起こされています。組織は、認証情報の窃取やマルウェアドロッパーの配信を阻止するために、階層化されたメール制御を優先することが不可欠です。メールおよびリモートアクセスに対してフィッシング耐性のある多要素認証(MFA)を義務付け、メールフローを強化し、クレーム、コンプライアンス、AIイニシアチブなど、ヘルスケアの誘引に合わせた迅速な隔離と合理化されたユーザー報告ワークフローを備えたメールセキュリティを使用して、リンクや添付ファイルをデトネーション/検査します。

**・「連鎖的影響」と臨床ピボットを防ぐためにセグメンテーションとネットワーク検出を使用する:**

2025年が連鎖的な混乱(管理ネットワークや非臨床オペレーショナルテクノロジー(OT)(HVAC/建物システム/バックアップ電源)の侵害が臨床ワークフローを麻痺させる可能性がある)によって特徴づけられたことから、組織は、Corporate IT、Clinical IT、Internet of Medical Things (IoMT)、およびFacilities/OTにわたって、デフォルトで東西の通信を拒否するポリシーを持つ階層化されたセグメンテーションを実装すべきです。これをネットワーク検出と応答(NDR)と組み合わせて、デバイスのトラフィックを模倣したビーコン、異常なDICOM/PACS通信、「アップデート」を装ったHTTPSによる持ち出しを検出し、特にエージェントを実行できないIoMT/OT資産に対して実施します。

**・「静かな」侵害を防ぐためにアイデンティティガバナンスとセッションレベルの監視を強化する:**

持ち出しのみの攻撃、患者恐喝、およびアイデンティティ主導のインシデントの増加を考慮すると、組織はアイデンティティを主要なセキュリティ境界として扱うべきです。MFAと最小特権を標準化し、共有アカウントを排除し、電子健康記録(EHR)および画像アーカイブ通信システム(PACS)環境に触れる特権ワークフローに対して特権アクセス管理(PAM)とジャストインタイム(JIT)アクセスを実装し、トークン/セッション盗難、異常な管理者行動、およびメールボックスのルール操作に対するアイデンティティに焦点を当てた検出を追加します。

**・認証情報の窃取とLiving-off-the-Landムーブメントを阻止するためにEDRを配備する:**

当社のレポートでは、2025年の攻撃者が、認証情報のダンプ(LSASS)とLotL技術(PowerShell/WMI)を一般的に使用して臨床システムを発見し、ピボットすることが強調されています。ヘルスケア組織は、最新のエンドポイント検出と応答(EDR)を企業のエンドポイントおよびサポートされている臨床サーバー/ワークステーション全体に配備し、積極的に監視することを保証すべきです。「ブリッジ」資産(PACS/インターフェースエンジン/ジャンプホスト/仮想化管理エンドポイント)を優先し、迅速な隔離と認証情報のリセットプレイブックを実用化します。

**・悪用される可能性とヘルスケアを標的としたキャンペーンに基づいた修復を優先する:**

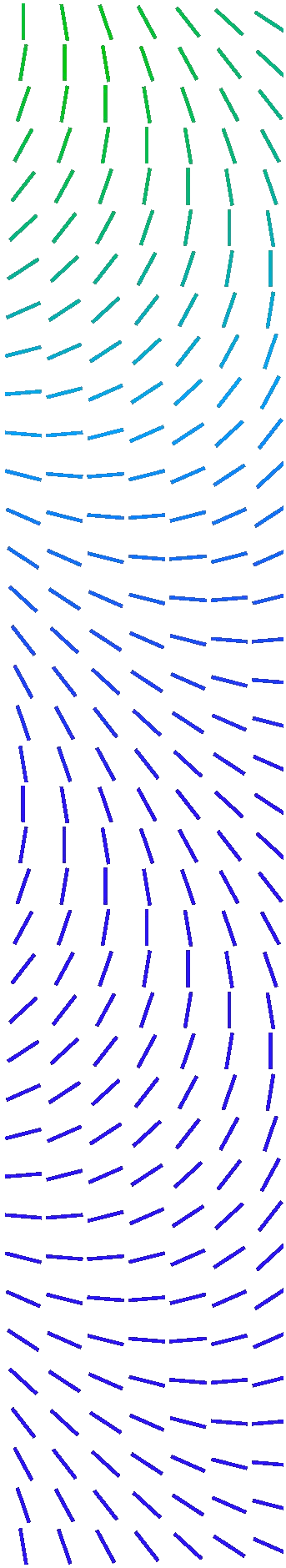
99%の病院が、既知の悪用可能な脆弱性（KEV）を持つデバイスを少なくとも1つ管理しており、レガシーデバイスの普及率が高いです。したがって、組織は悪用を重視した脆弱性プログラムを運用すべきです。KEVとインターネットに面したシステム（例：Oracle EBS、Cisco AsyncOS）を優先し、脅威インテリジェンスを使用してアクティブなキャンペーンをパッチの決定に反映させます。パッチ適用が不可能な場合は、補償的コントロール（隔離、仮想パッチ適用、認証情報の強化、プロトコル認識型監視）を適用します。

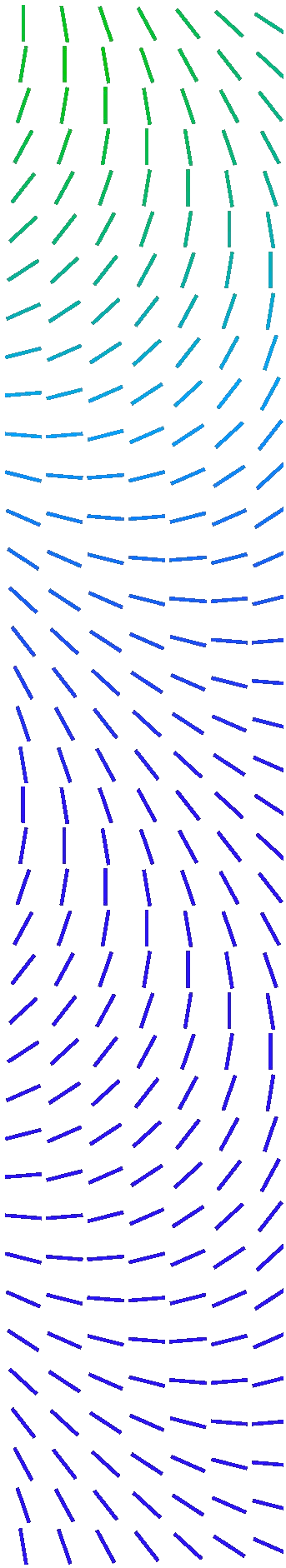
**・持ち出し優先のオペレーションと患者恐喝からPHIを保護する:**

攻撃者が三重の恐喝や患者への嫌がらせへと移行し、保護医療情報（PHI）がアンダーグラウンド市場で高値で取引されていることから、組織は強力なデータ保護および損失防止コントロールを実装すべきです。PHIリポジトリへの大量エクスポートと高リスクアクセスパスを制限し、大量アクセスと異常なアプリケーションプログラミングインターフェース（API）使用を監視し、持ち出しのみのインシデントと患者通知シナリオのために設計されたプレイブックに合わせたデータ損失防止（DLP）とエグレス監視、および転送中と保存中のPHIに対する暗号化を適用します。

**・ダウンタイムの影響を軽減するためにSOC主導のインシデント対応とレジリエンスを実用化する:**

ダウンタイムが週単位で測定され、コストが運用の中断によって引き起こされているため、組織は、メール + EDR + NDR + 脅威インテリジェンスを相関させ、ランサムウェア、持ち出しのみ、BECのための事前定義されたプレイブックに統合した検出から対応へのワークフローを運用すべきです。EHR/PACS/Labの依存関係に対する不変/オフラインバックアップと日常的な復元テストを検証し、仮想化管理を強化して、一度に数百のシステムを無効にする可能性のあるESXiの「ブラスト半径」イベントを削減します。





**See more threat reports from**

**Trellix Advanced Research Center**

This document and the information continued herein describes computer security research for educational purposes only and the convenience of Trellix customers. Trellix conducts research in accordance with its Vulnerability Reasonable Disclosure Policy I Trellix. Any attempt to recreate part or all of the activities described is solely at the user's risk, and neither Trellix nor its affiliates will bear any responsibility or liability.



Trellix