Analysis Report

SECURITY REPORT

2023

NOV

ガートナー(Gartner)の2023年セキュリティ運用ハイプ・サイクル

CyberFortress

このレポートは、株式会社サイバーフォートレスの独自の調査にて収集されたデータに基づき作成しています。

Analysis Report.

ガートナー(Gartner)の2023年セキュリティ運用ハイプ・サイクル

01. ガートナーのハイプ・サイクルについて

世界的なリサーチ機関であるガートナー（Gartner）が毎年発表するハイプ・サイクル（Hype Cycle）モデルを活用したレポートは、IT分野に在職している全ての人々にとって注目すべき対象である。組織や企業は、単にベンダー（Vendor）や業者の意見だけを聞いて意思決定を行うべきではない。自社のソリューションやサービスのデメリットを率直に語ることは難しく、期待することもできない。そのため、企業や組織は特定のベンダーやソリューションに偏らず、中立的な立場からメリットとデメリットを把握するためにコンサルティング企業の資料を参考にする場合がある。

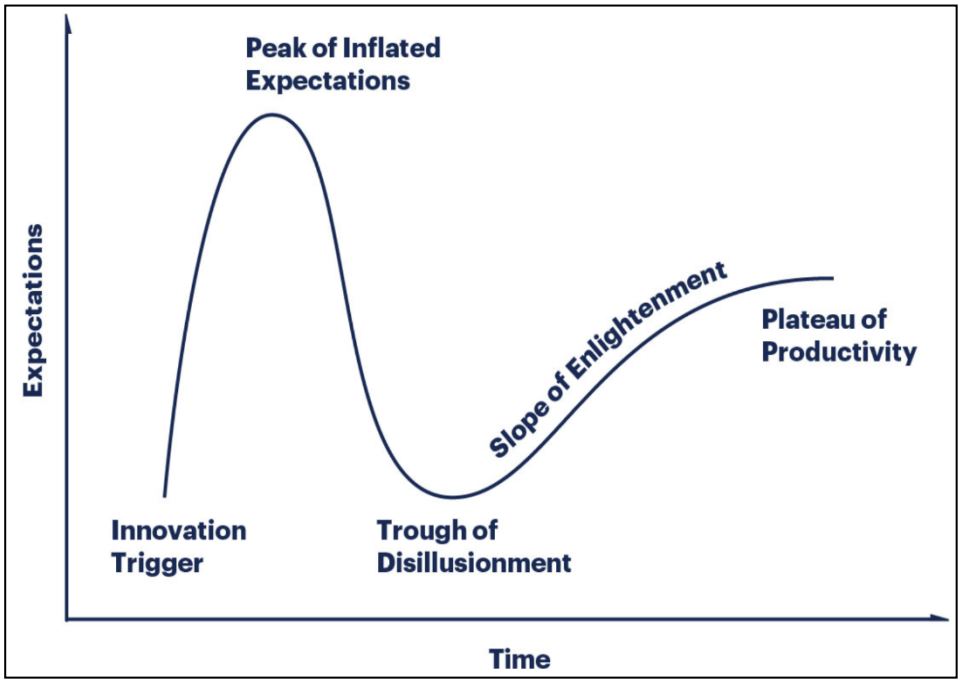
企業と組織の意思決定に役立つグローバルコンサルティング企業としては、代表的にデロイト（Deloitte）、マッキンゼー・アンド・カンパニー（McKinsey & Company）、ボストンコンサルティンググループ（Boston Consulting Group）などがある。これらの企業は研究諮問とコンサルティングなどのサービスを提供しているが、IT分野では特にガートナーの方法論を多様な技術に対する未来予測の根拠として活用している。

ガートナーが提供する代表的な方法論には、ハイプ・サイクル（Hype Cycle）、マジック・クアドラント（Magic Quadrant）、新技術ロードマップ（Emerging Technology Roadmap, ETR）などがある。その中で、ハイプ・サイクルは1995年にガートナーが最初に導入した概念で、技術に焦点を当てた方法論である。これは市場の興味度の変化を視覚的に示すツールであり、過去と比較して技術の進化や退化を予測し、現在において注目すべき技術を選択または集中するのに役立つ。

ガートナーが提供する代表的な3つの方法論	
ハイプ・サイクル (Hype Cycle)	・新たな技術が登場する時点から安定期に到達するまで時間によって5段階に分けて、時間の変化による期待値をハイプ・サイクルと言うパターンでン表現した方法論
マジック・クアドラント (Magic Quadrant)	・市場(Market)に焦点を合わせた方法論で、技術に対してどのベンダーがあるソリューションを持って市場のどの位置にあるかを検討したりレビューする際に役立つ方法論
新技術ロードマップ (Emerging Technology Roadmap)	・企業に焦点を合わせた方法論で上にある2つの方法論(ハイプ・サイクル、マジック・クアドラント)を経って最終的に技術領域全般から企業が投資の優先順位を決定する際に活用する方法論

【▲表①　ガートナーが提供する代表的な3つの方法論 (参考：イグルーコーポレーション)】

ガートナーのハイプ・サイクルモデルを整理すると、新技術の登場とそれを開発する技術業者の大げさな宣伝、メディアの興味、そして大衆の過剰な期待が組み合わさり、初めから期待を大きく上回る幻想が形成されることが一般的である。その後、失望感によってメディアと大衆の興味が減少し、一定の市場が形成されると再び興味が湧き、本格的にその技術が市場に普及する過程を示すモデルである。
ハイプ・サイクルの「ハイプ（Hype）」は「誇張」「誇大」「ごまかし」といった意味で、ハイプ・サイクルは「誇張周期」ぐらいの意味です。ハイプ・サイクルの要素の中で、横軸（Time）は技術の成熟度を示す「時間」を意味し、縦軸（Expectations）は市場が技術に対して抱く「期待値」を表す。
そして、ハイプ・サイクルの曲線は新技術に対する市場の期待と技術が成熟していく過程を表し、ガートナーはこれを5つの段階に区分している。最初は新技術が浮かび上がる段階（黎明期、Innovation Trigger）、次に新技術に対する期待が爆発的に成長して頂点に達する段階（流行期、Peak of Inflated Expectations）、その後に新技術に対する興味が頂点を達した後、大衆の興味が減少する段階（幻滅期、Trough of Disillusionment）、生き残った一部の技術だけが成熟段階に入り（回復期、Slope of Enlightenment）、最終的に回復期を超えて生き残った技術が大衆に普及する段階（安定期、Plateau of Productivity）を経るとガートナーが説明している。



【▲図①　ハイプ・サイクル(Hype Cycle)の構成要素 (参考：Gartner)】

ハイプサイクル(Hype Cycle)の5つの段階	
黎明期 (Innovation Trigger)	**新技術が浮かび上がる段階** • 一段階の黎明期（Innovation Trigger）」は、潜在的な技術が注目される時期で、初期の概念証明やその概念がメディアの関心を引く段階を指す。この段階では、まだ商用化された商品は存在せず、商用的な価値も証明されていない状態である。言い換えれば、新技術がメディアによって「世界を変える」と言われ、大衆が興味を持つ段階で、市場の期待は過度に高まるが、実際にはまだ商品やサービスとして利用可能な段階ではない。
流行期 (Peak of Inflated Expectations)	**新技術に対する期待が爆発的に成長して頂点に達する段階** • 二段階の流行期（Peak of Inflated Expectations）」では、初期のメディア報道により、成功事例と多くの失敗事例が注目され、大衆の期待が非常に高まる時期を指す。この段階では、一部の企業は新技術を実際の事業に取り入れようと試みるが、革新の限界に達することで失敗する例が増え、多くの企業は状況を慎重に見守る時期に入る。この段階では、大衆の期待が実際の成果よりも過度に膨らんでいることが一般的で、実現可能な成功事例は限られている。
幻滅期 (Through of Disillusionment)	**新技術に対する興味が頂点を達した後、大衆の興味がなくなる段階** • 三段階の幻滅期（Trough of Disillusionment）」では、多くの実験や具現化が失敗し、期待に応えられない状況により興味が急速に失われる時期を指す。この段階で、製品化を試みた主体は大きな見直しを行うか、失敗することがあり、生き残った主体が消費者を満足させるために製品の向上を成功させた場合にのみ、投資が持続される。
回復期 (Slope of Enlightenment)	**生き残った一部の技術のみ成熟段階に進入する段階** • 四段階回復期（Slope of Enlightenment）において、技術が企業にどのように利益をもたらすかについての具体的な事例が広がり、幅広い理解が進展する。この段階では、2-3世代の製品がリリースされ、多くの企業が事業に投資する一方で、保守的な企業は依然として慎重なスタンスを維持している。
安定期 (Plateau of Productivity)	**回復期を超えて生き残った技術が大衆的に拡散される段階** • 五段階の安定期（Plateau of Productivity）では、技術の実際の利点が立証され、市場の主要な位置を確立し、その技術を導入する組織の数が急増する。また、事業者の生存可能性を評価するための基準が確立され、技術の幅広い市場適用性と関連性が明確になる。

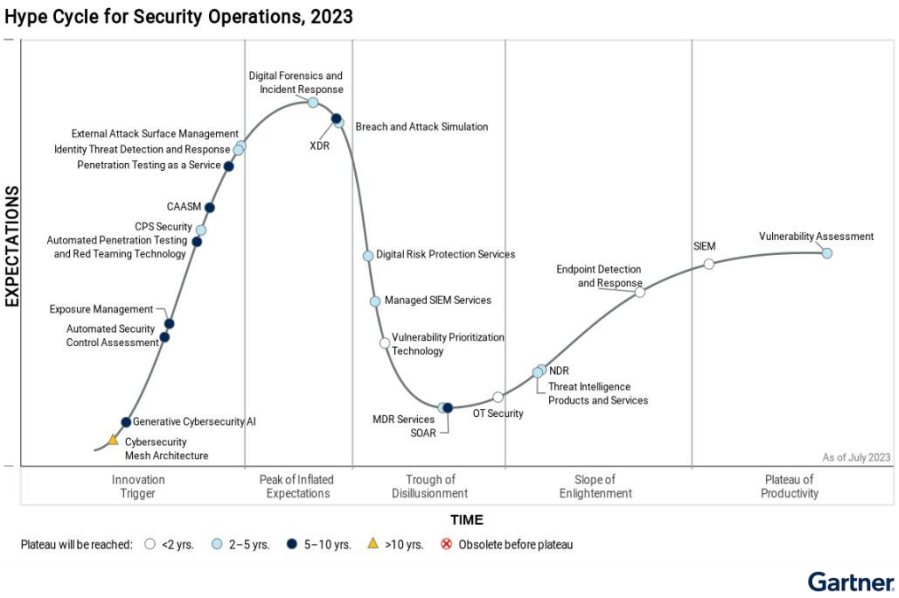
【▲表② ハイプサイクル(Hype Cycle)の5つの段階 (参考：Gartner、再構成：イグルーコーポレーション)】

ガートナーのハイプサイクルは、新技術の発展段階を分析し、それらが市場での成熟段階や安定期に到達するまでの過程を示すモデルである。このモデルは、組織や企業が将来の技術選択や戦略を計画する際に役立つ。各分野の新技術がハイプサイクル内で適切な位置に配置され、安定期に到達するまでの所要時間が示されることで、これらの技術の採用と投資戦略を理解し、計画するのに役立つ。

【▲図② 安定期段階に到達するまで所要される時間(Plateau will be reached) (参考：Gartner)】

02. 2023年セキュリティ運用ハイプサイクル

このようなハイプサイクルモデルを基にした、ガートナーは7月20日に「2023年セキュリティ運用ハイプサイクル（Hype Cycle for Security Operations, 2023）」を発表し、その中には24のサイバーセキュリティ分野の技術が含まれている。



【▲図③ Hype Cycle for Security Operations, 2023 (参考：Gartner)】

ガートナーはセキュリティ運用ハイプサイクルレポートで一番先にセキュリティ及び危険管理(Security and Risk Management, SRM)リーダーが変化するセキュリティ環境に対応するためにハイプサイクルに含まれている技術を基にビジネス危険に重点を置いた戦略(ロードマップ)の開発が必要だと伝え、次の4つの要素を含ませるべきだと強調した。

SRMリーダー開発すべきの戦略の重要要素	
1	• 持続的な脅威露出管理(Continuous Threat Exposure Management, CTEM) 概念の実現が必要
2	• ビジネスに関するアクセス方法を提供して検知及び対応の範囲と関連性を改善
3	• リスポンスタイムの短縮のための自動化の極大化
4	• 運用効率性向上及び技術強化のために生成型サイバーセキュリティAIを活用

【▲表③ SRMリーダーが開発すべきの戦略の重要要素 (参考：Gartner、再構成：イグルーコーポレーション】

02-1. 2023年セキュリティ運用ハイプサイクルに含まれている

そして、ガートナーは2023年セキュリティ運用ハイプサイクルに選定された技術（セキュリティ運用技術及びサービス）が増加した攻撃面における脅威と脆弱性の識別に役立ち、IT/OTシステム、クラウドワークロード、アプリケーション、およびその他の資産をサイバー攻撃から保護できることを伝えた。同時に、セキュリティリスク管理（SRM）のリーダーは選定された技術を活用してセキュリティ運用（SecOps）の機能を強化し、提供できることを強調した。

○ 黎明期(Innovation Trigger)段階に含まれている技術(10個)

区分	内容
Cybersecurity Mesh Architecture (CSMA)	• サイバーセキュリティメッシュアーキテクチャ（CSMA）は、全般的なセキュリティの効率性を向上させるための新しいアプローチで、構成可能な分散型セキュリティ制御を設計することを目指している。このアプローチは、構成可能で独立したセキュリティモニタリング、予測分析、および先制的な実施を提供し、中央集中型のインテリジェンスとガバナンスを強調し、共通のIDとパブリックを活用した安全な中央集中型セキュリティ運用と監視を可能にするものである。
Generative Cybersecurity AI	• 生成型サイバーセキュリティAI（Generative Cybersecurity AI）は、パブリックまたはプライベートホスティングクラウドサービスで提供したり、セキュリティ管理インターフェースと統合したり、SWエージェントと統合してセキュリティ対策を実施したりすることができる。生成型サイバーセキュリティAIを活用することで、既存のワークフローを改善し、組織のセキュリティ構成や実際の攻撃データの生成などを行い、高いレベルのセキュリティを構築することが可能である。
Automated Security Control Assessment (ASCA)	• 自動化セキュリティ制御評価（ASCA）プロセスおよびテクノロジーは、セキュリティ制御（例：エンドポイントの保護、ネットワークファイアウォール、ID、メールセキュリティ、セキュリティ情報およびイベント管理）の誤った設定の分析および修正に焦点を当て、企業のセキュリティ状態を改善する。 • ASCAは、独立した実行ツールであるか、ファイアウォール、ID脅威検知と対応、ネットワークセキュリティポリシー管理、クラウドインフラの資格管理など、他のセキュリティ製品の機能を備えている場合もある。
Exposure Management (EM)	• 露出管理（EM）は、組織が持続的かつ一貫した可視性を評価し、組織のデジタル資産のアクセス性と脆弱性を確認できるようにするための一連のプロセスとテクノロジーを含む。 • EMは、急速に拡大する攻撃面に対応する既存の脆弱性管理だけでは不十分な組織において、脅威の露出をリストアップし、優先順位をつけ、検証するなどを通じて問題を軽減する役割を果たす。
Automated Penetration Testing and Red Teaming Technology	• ガートナーは、自動化ペネトレーションテストおよびレッドチームの構成が、組織の能力を強調して、露出と攻撃表面を検証する際に重要な役割を果たすことを強調している。 • 多くの組織は、規制遵守要件を満たす必要がある場合にのみこれらのテストを実施している。 • 自動化が増加すると、より信頼性の高い評価が迅速に行われ、必要な時間が短縮され、高い効率性と信頼性のある結果を生み出すことが可能となる。

CPS Security (Cyber-Physical Systems)	• サイバー物理システム（CPS）セキュリティは、物理的な世界と相互作用し、検出、計算、制御、ネットワーキング、および分析を調整するエンジニアリングされたシステムである。 • CPSには、産業制御システム（ICS）/監視制御およびデータ収集（SCADA）、運用技術（OT）、インターネット・オブ・シングス（IoT）などが含まれる。 • CPSセキュリティは、ますます増加する脅威に直面し、CPSが安全かつ安定しており、かつ復元力を維持するように保障する包括的な規制である。
Cyber Asset Attack Surface Management (CAASM)	• サイバー資産攻撃表面管理（CAASM）は、セキュリティチームが資産の可視性と露出の問題を解決できるように焦点を当てている。 • CAASMは、エンドポイント、サーバー、およびその他の資産を含む資産のコレクションを行う製品で、資産の可視性を集計する。 • これに基づいて、セキュリティチームはすべてのデジタル資産からセキュリティ制御の不足、セキュリティポストチャー、および資産の露出などを検出し、セキュリティ状態を改善できるように取り組む。
Penetration Testing as a Service (PTaaS)	• サービス型ペネトレーションテスト（PTaaS）サービスは、セキュリティ脆弱性を発見し、修正するためのサブスクリプションモデルを用いたペネトレーションテストである。 • PTaaSは脆弱性検出とアプリケーションセキュリティテストを補完し、テスト結果のコスト効率化と品質向上、および脆弱性の状態検証を提供する。これにより、組織はセキュリティポストチャーの持続的な向上を実現できる。
Identity Threat Detection and Response (ITDR)	• IDインフラを保護することは非常に重要である。アカウントが侵害されたり、権限が誤って設定されたり、IDインフラが損傷されると、攻撃者がシステムを制御できる可能性がある。 • 身元脅威検知および対応（ITDR）は、IDインフラ自体を攻撃から保護するツールやベストプラクティスなどを含む分野である。これにより、脅威を遮断および検出し、管理者の状態を確認し、さまざまな種類の攻撃に対応し、必要に応じて正常な運用を回復させることが可能となる。
External Attack Surface Management (EASM)	• 外部攻撃表面管理（EASM）は、インターネットに接続されている企業の資産とシステム、およびそれに関連する露出を調査および記録するために実施されるプロセス、技術、および管理サービスを指す。 • EASMは、インターネットに接続されている資産を識別するだけでなく、発見された脆弱性とそれに関連する脅威の優先順位を設定するのに役立ち、脅威アクターに露出している公開ドメインのデジタル資産および関連する危険情報を提供する。

【▲表④ 黎明期段階に含まれている技術（参考：ガートナー、再構成：イグルーコーポレーション）】

○ 流行期(Peak of Inflated Expectations)に含まれている技術(3個)

区分	内容
Digital Forensics and Incident Response (DFIR)	• デジタルフォレンジック及びインシデント対応（DFIR）は、顧客が潜在的なセキュリティ被害に対処できるように、多角的にサービスを提供する。 • DFIRサービスは、規制に課せられた罰金、法的費用、訴訟、ブランド評判の悪化、お客様の離脱などの要因から、組織のインシデント対応能力を予防的かつ事後対応的に強化する戦略的な投資です。DFIRは、組織のインシデント対応（Incident Response, IR）計画にますます重要性を持つようになっている。
Extended Detection and Response (XDR)	• 拡張された検知及び対応（XDR）は、統合されたセキュリティインシデント検出および自動化された対応機能を提供している。 • XDRは、内部技術の必要性を減らし、複雑なソリューションを運用するために必要なスタッフの数を削減でき、単一の中央集中型の調査および対応システムを通じて、セキュリティ運用に関連する時間と複雑性を削減するのに役立つ。
Breach and Attack Simulation (BAS)	• 違反及び攻撃シミュレーション（BAS）技術を使用して、組織は側面移動やデータ漏洩などの脅威ベクターに対する持続的なテストを自動化し、セキュリティ態勢の脆弱点を把握できる。 • BASの評価により、組織は構成ミスによるセキュリティ状態の違いを検出し、また要諦されているセキュリティへの投資の優先順位を再評価できるようになる。

【▲表⑤ 流行期段階に含まれている技術（参考：ガートナー、再構成：イグルーコーポレーション）】

○ 幻滅期(Trough of Disillusionment)段階に含まれている技術(6個)

区分	内容
Digital Risk Protection Services (DRPS)	• デジタル危険保護サービス(DRPS)はブランド保護、第3者危険評価及び外部脅威が発見できるようにして識別された脅威に対する技術的対応を提供する一連の技術主導サービス • このようなソリューションは表面ウェブ(Web)、ダークウェブ(Dark Web)、ディープウェブ(Deep Web)、SNSなどに対する可視性を提供して重要な資産に対する潜在的な脅威を識別し、脅威行為者、悪意的な活動を実施する戦術及びプロセスに対する状況情報を適用
Managed SIEM Services	• 管理型セキュリティ情報及びイベント管理(Managed SIEM)サービスはクライアント所有SIEMソリューションのリモート管理及びモニタリング機能などを提供 • 様々な組織からSIEMを導入しているが、これを効果的に運用することに困っている場合がある • Managed SIEMは検知コンテンツ/レポートの作成及び調整、メンテナンス、セキュリティ問題に対する簡単な調査のように見逃しやすい領域に価値を提供
Vulnerability Prioritization Technology (VPT)	• 脆弱性優先順位指定技術(VPT)はインテリジェンスソース、分析及び視覚化を使用して多様な脆弱性リモート側的ソースを単一位置に簡素化して重要な修正/緩和活動で一番良く実施する方法に対する優先順位が指定されている実用的な推奨事項を効率的に提供 • セキュリティインシデント及び違反が増加することによって多くの組織から功利的な脆弱性管理プログラムを実現するためにVPTソリューションを採択中
MDR Services (Managed Detection and Response)	• ほとんどの組織は自体的にセキュリティ運用センター(SOC)機能を構築し、実行するためのリソース、予算または欲求が不足 • このような顧客のために管理型検知及び対応(MDR)サービスはセキュリティ運用センター(SOC)機能をリモートで提供 • これで組織は脅威中断及び抑制で迅速に検知、分析、調査し、能動的に対応可能
SOAR (Security Orchestration, Automation and Response)	• ガートナーはセキュリティ脅威対応自動化ソリューション(SOAR)をインシデント対応、オーケストレーション及び自動化、脅威インテリジェンス(TI)管理機能を単一ソリューションに結合したソリューションで定義 • SOARツールは柔軟で多様なセキュリティ運用センター(SOC)及び広範囲なセキュリティ運用(SecOps)使用事例に適用でき、SOARを活用したインシデント管理事例は持続的に登場している
OT Security (Operation Technology)	• 運用技術(OT)には産業用装備、資産、プロセス及びインベントを直接モニタリングまたは制御して変化を検知するHW及びSWが含まれる • OT環境を狙うサイバー脅威とセキュリティソリューションが増加することによって一時期ネットワーク中心のツールが大体だった一般的なOTセキュリティカテゴリーが現在は多様なカテゴリーに進化中 ※ガートナーはOTセキュリティがCPSセキュリティのカテゴリーに含まれていると説明

【▲表⑥ 幻滅期段階に含まれている技術 (参考：ガートナー、再構成：イグルーコーポレーション)】

○ 回復期(Slope of Enlightenment)段階に含まれている技術(3個)

区分	内容
Threat Intelligence Products and Services	• 脅威インテリジェンス（TI）製品およびサービスは、組織がサイバー脅威と脅威行為者をプロファイリングし、自身のTIを収集、キュレーションし、運用し、潜在的な外部エンティティと共有できるようにサポートするツールを提供する。 • TIは、組織が脅威環境に対する可視性を維持し、脅威が組織に影響を与える前、中、後に適用できるよう、適切で正確で実行可能な洞察力を構築できる手段を提供する。
Network Detection and Response (NDR)	• ネットワーク検知及び対応（NDR）ソリューションは、ネットワークトラフィックに対して行動分析を適用し、異常なシステムの挙動を検出する。NDRの中核となる機械学習アルゴリズムは、他の検出技術から逃れる可能性のあるネットワークトラフィックの異常を発見および特定するのに役立つ。 • NDRは、ハードウェア、ソフトウェア、またはSaaS管理コンソールで提供でき、組織はNDRを使用してランサムウェアや内部者の悪意のある活動などの侵害活動を検出し、制御することができる。
Endpoint Detection and Response (EDR)	• エンドポイント検知及び対応（EDR）ソリューションは、システム、プロセス、およびユーザーの活動を分析してセキュリティ脅威を検出する。 • EDR機能は、エンドポイント保護プラットフォーム（Endpoint Protection Platform, EPP）に組み込まれて中央集中型クラウドベースのセキュリティ分析および管理ソフトウェアとして提供される場合もある。 • EDRは、既知のマルウェア（Malware）やランサムウェア（Ransomware）を検出するだけでなく、未知の脅威を発見し、対処するのに役立ちます。

【▲表⑦ 回復期段階に含まれている技術 (参考：ガートナー、再構成：イグルーコーポレーション)】

○ 安定期(Plateau of Productivity)段階に含まれている技術(2個)

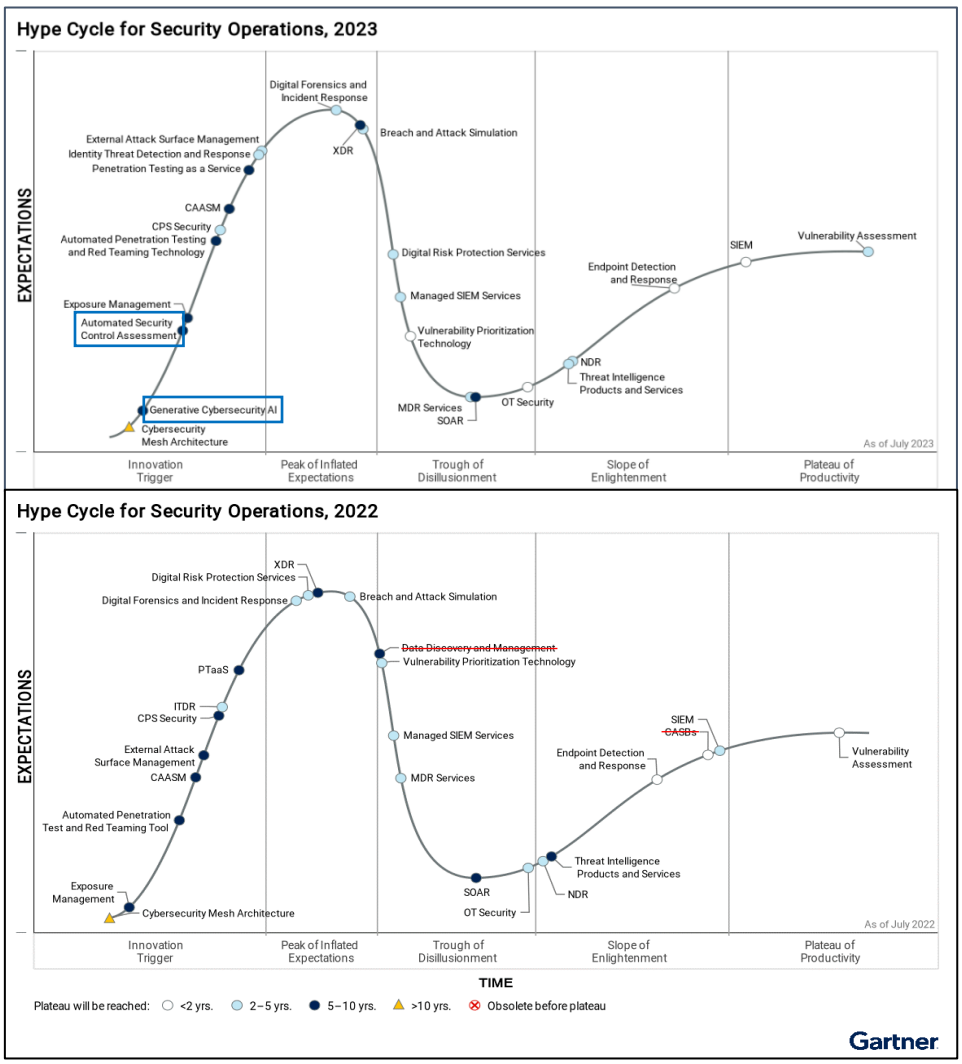
区分	内容
Security Information and Event Management (SIEM)	• セキュリティ情報及びイベント管理（SIEM）は、オンプレミス（On-Premise）およびクラウド環境からセキュリティイベントデータを収集し、分析するセキュリティシステムである。 • SIEMは組織による損害を軽減し、規制遵守と報告要件を満たすための対策をサポートします。多様な環境からデータを収集し、中央集中化して可視性を高めることは、効果的なセキュリティプログラムの重要な要素である。 • SIEMはセキュリティイベントを識別し、優先順位を付け、調査し、また現在および過去のセキュリティイベントに対する報告を支援する組織の機能をサポートしている。
Vulnerability Assessment (VA)	• 脆弱性評価（VA）ツールは、オンプレミス（On-Premise）、クラウド、および仮想環境で動作し、データ漏洩を防ぐのに役立ち、コンプライアンス報告、制御フレームワーク、危険評価、優先順位付け、改善活動をサポートする。 • VAは、脆弱性管理（Vulnerability Management, VM）プロセスの基本的な構成要素であり、インフラストラクチャの強化、セキュリティ態勢の管理、事前予防的な脅威防止、規制要件および規制遵守体系をサポートし、デジタル資産とそれに関連するセキュリティの脆弱性を検出および列挙するための基本プロセスである。

【▲表⑧ 安定期段階に含まれている技術 (参考：ガートナー、再構成：イグルーコーポレーション)】

02-2. セキュリティ運用ハイプサイクルの変化(2022年 → 2023年)

○ セキュリティ運用ハイプサイクルの技術変化

2023年のセキュリティ運用ハイプサイクルを確認すると、新たな技術の追加が確認されます。今年、セキュリティ運用ハイプサイクルには「生成型AIサイバーセキュリティ（Generative Cybersecurity AI）」および「セキュリティ制御評価自動化（Automated Security Control Assessment, ASCA）」の2つの技術が新たに追加された。中でも、「生成型AIサイバーセキュリティ」のような生成型AIがサイバーセキュリティ分野に導入され、自動化されたワークフローの改善など、セキュリティ分野で潜在的な可能性を持っていると判断され、セキュリティ運用ハイプサイクルに初登場した。



【▲図④ セキュリティ運用ハイプサイクルの変化(2022年 → 2023年) (参考：ガートナー、再構成：イグルーコーポレーション)】

そして、去年のセキュリティ運用ハイプサイクルに含まれていた「データディスカバリー及び管理（Data Discovery and Management）」および「クラウドアクセスセキュリティブローカー（Cloud Access Security Broker, CASBs）」の2つの技術は、今年のサイクルから削除されたことが確認できる。特にCASBsについて、ガートナーは「CASBsはセキュリティウェブゲートウェイ（Secure Web Gateway, SWG）およびゼロトラストネットワークアーキテクチャ（Zero Trust Network Architecture, ZTNA）と統合されてセキュリティサービスエッジ（Security Service Edge, SSE）の機能として提供されるため、今回セキュリティ運用ハイプサイクルから除外された」と説明した。

○ 発生期(Innovation Trigger)段階の技術増加

2023年のセキュリティ運用ハイプサイクルにはもう一つ大きな変化が発生した。それは、発生期（Innovation Trigger）段階に含まれている技術の数が増加したことである。発生期段階に含まれる技術は、去年の8個から今年は10個に増えた。この増加は、市場の要求に応えて攻撃表面（Attack Surface）の複雑性を克服しようとする動きを示している。

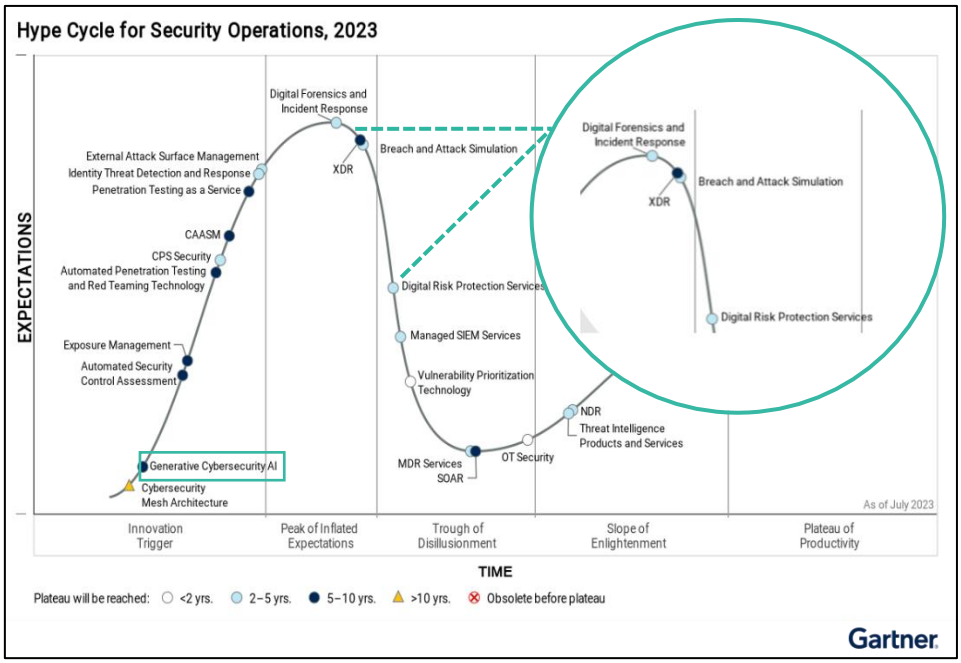
具体的に、漏洩管理（Exposure Management, EM）、外部攻撃表面管理（External Attack Surface Management, EASM）、サービス型ペネトレーションテスト（Penetration Testing as a Service, PTaaS）、自動化ペネトレーションテストおよびレッドチーム構成（Automated Penetration Testing and Red Teaming Technology）、自動化セキュリティ制御評価（Automated Security Control Assessment, ASCA）、身元脅威検知および対応（Identity Threat Detection and Response, ITDR）などの技術が、デジタル資産全体から攻撃表面の露出を持続的に発見し、評価し、最終的には組織の攻撃表面の露出を減少させるのに役立つと説明された。

発生期(Innovation Trigger)段階の技術増加	
2022年(8個)	**2023年(10個)**
• Cybersecurity Mesh Architecture(CSMA) • Exposure Management • Automated Penetration Test and Red Teaming Tool • CAASM • External Attack Surface Management • CPS Security • ITDR • PTaaS	• Cybersecurity Mesh Architecture(CSMA) • Generative Cybersecurity AI • Automated Security Control Assessment (ASCA) • Exposure Management • Automated Penetration Testing and Red Teaming Technology • CPS Security • CAASM • Penetration Testing as a Service(PTaaS) • Identity Threat Detection and Response(ITDR) • External Attack Surface Management(EASM)

【▲表⑨ 発生期(Innovation Trigger)段階の技術増加 (参考：ガートナー、再構成：イグルーコーポレーション)】

○ 今年サイバーセキュリティ分野で一番注目される技術

ガートナーは、サイバーセキュリティ分野の多様な技術の中で、今年注目されているものとして「違反及び攻撃シミュレーション（Breach and Attack Simulation, BAS）」や「デジタル危険保護サービス（Digital Risk Protection Services, DRPS）」などを挙げている。これらの技術は、内部および外部からの持続的な脅威評価と脅威識別を提供することを目的としている。さらに、「拡張検知及び対応（Extended Detection and Response, XDR）」や「デジタルフォレンジック及びインシデント対応（Digital Forensic and Incident Response, DFIR）」が2023年のセキュリティ運用ハイプサイクルの流行期（Peak of Inflated Expectations）段階に含まれている。ガートナーはこれを、脅威検知及び対応に対する市場の需要が増加していることを示すものとして説明している。また、生成型サイバーセキュリティAI（Generative Cybersecurity AI）がセキュリティ運用ハイプサイクルに初めて登場したことは、市場から多くの注目を集めていることを意味する。ガートナーによれば、まだほとんどの生成型サイバーセキュリティAIがテスト（実験）機能として提供されていると述べているが、一部の機能（脅威検知及び対応、脅威インテリジェンス、漏洩管理など）は既にテストが終了しているとの報告がある。そして、このような技術を実現しようとするSRMリーダー（Security and Risk Management Leaders）は、組織内でこれらの機能をどのように消費し、構築するかについて考慮し、メカニズムで活用率を監視する必要があると説明している。



【▲図⑤ 今年サイバーセキュリティ分野で一番注目される技術（参考：ガートナー、再構成：イグルーコーポレーション）】

02-３. 2023年セキュリティ運用ハイプサイクルの優先順位マトリックス

ガートナーは、ビジネス現場で最速で活用可能かつ最も役立つ技術を特定するための優先順位マトリックス（Priority Matrix）を提供している。このマトリックスは、技術の採用が市場で主流になるまでに必要な時間を示す横軸と、技術が提供するベネフィットを示す縦軸を組み合わせている。横軸では、技術の主流採用までにかかる時間が分かれており、△2年未満、△2～5年、△5～10年、△10年以上のカテゴリに分類されている。縦軸は技術のベネフィットを示し、△転換、△高、△普通、△低のカテゴリに分かれています。この優先順位マトリックスを使用することで、組織や企業はセキュリティ運用サービスや機能に投資する前に、どの分野に焦点を当てるべきか、どれくらいの予算を割り当てる必要があるかを簡単に識別できる。ただし、ガートナーは強調しているが、セキュリティ運用に適した技術やサービスが組織や企業に即時の利益をもたらすことはほとんどないという点を理解する必要があり、これらを効果的に活用するためには組織に合ったプロセスの構築が不可欠であると指摘している。

Benefit	Years to Mainstream Adoption	
	Less Than 2 Years	2 - 5 Years
Transformational		
High	• Endpoint Detection and Response(EDR) • OT Security • Vulnerability Prioritization Technology	• Breach and Attack Simulation(BAS) • CPS Security • Identity Threat Detection and Response(ITDR) • MDR Services • Threat Intelligence Products and Services • Vulnerability Assessment
Moderate	• SIEM	• Digital Forensics and Incident Response(DFIR) • Digital Risk Protection Services(DRPS) • External Attack Surface Management(EASM) • NDR
	5 - 10 Years	More Than 10 Years
Transformational	• Exposure Management • Generative Cybersecurity AI	• Cybersecurity Mesh Architecture(CSMA)
High	• SOAR • XDR	
Moderate	• Automated Penetration Testing and Red Teaming Technology • Automated Security Control Assessment(ASCA) • CAASM • Penetration Testing as a Service(PTaaS)	

【▲表⑩ 2023年セキュリティ運用ハイプサイクルの優先順位マトリックス (参考：ガートナー、再構成：イグルーコーポレーション)】

03. 最後に

今回の記事では、ガートナー（Gartner）のハイプサイクル（Hype Cycle）モデルと「2023年セキュリティ運用ハイプサイクル（Hype Cycle for Security Operations, 2023）」に含まれる技術について調査した。ガートナーは、黎明期（Innovation Trigger）段階に含まれる技術が増加していることを説明し、これは日々増加する攻撃表面（Attack Surface）に対応するための市場需要が増加したことを反映しており、攻撃表面に対処する技術に焦点を当てている。

ガートナーは、増加する攻撃表面に対処するために、セキュリティおよびリスク管理（Security and Risk Management, SRM）のリーダーがデジタルフォレンジックおよびインシデント対応（Digital Forensics and Incident Response, DFIR）、拡張された検知および対応（Extended Detection and Response, XDR）、違反および攻撃シミュレーション（Breach and Attack Simulation, BAS）、デジタルリスク保護サービス（Digital Risk Protection Services, DRPS）などの技術に焦点を当て、セキュリティ運用（SecOps）機能を戦略的に強化すべきだと強調している。ただし、これらの技術は実際にはセキュリティ運用ハイプサイクルの頂点である「期待の過剰なピーク（Peak of Inflated Expectations）」に位置していることが確認された。さらに、多くの国内および国際的なサイバーセキュリティベンダーが今年の攻撃表面の急激な増加を最大のセキュリティ課題の一つと位置づけ、迅速な対応が必要であると強調している。

もちろん、ガートナーのセキュリティ運用ハイプサイクルだけでは、増加している攻撃表面に対処するための正確なソリューションがどれであるかを特定することは難しい。ただし、これを活用して、個別の組織が将来増加する攻撃表面に対処できるプロセスを構築するために、どの分野にどれだけの予算を投資するかについて洞察を得ることができるだろう。