SANS

Analyst Program

ホワイトペーパー

SANS 2021レポート：可視性を定義して測定するために

執筆：Barbara Filkins、John Pescatore

2021年6月

ExtraHop

©2021 SANS™ Institute

可視性の定義

2020年にSANSが実施した調査では、結果の至るところであるテーマが何度も現れていました。それは、「セキュリティのあらゆる側面で可視性を改善する必要がある」というものです。可視性（もしくは可視性の欠如）という概念はほとんどの人が容易に理解できるものですが、この言葉は依然として主観的であり、関係者の役割によって認識が大きく異なる場合があります。

企業の取締役会はサイバーセキュリティとビジネスの健全性との間に強い相関を認め始めており、セキュリティ・マネージャーに対して、戦略の策定や、堅牢なサイバーセキュリティのプロセスと管理策への投資提言を期待しています。Security Boulevardの報告[1]にあるように、サイバーセキュリティの戦略的な重要性は取締役会の構成からも明らかです。Gartner社の調査によると、現在少なくとも40%の取締役会がサイバーセキュリティの専門知識を持つ役員を置いています。[2]取締役会のメンバーは、ビジネスに不可欠なセキュリティ・メトリクスのために、動的でリアルタイム、かつ一元化された重要データとその可視化を求めています。このようなセキュリティ・メトリクスは、取締役会や経営陣がビジネス・ガバナンスとリスク管理のパフォーマンスを評価し、戦略的な意思決定を行うために欠かせません。

可視性には明確な定義がなく、見る人によって意味が異なります。それでも組織は、将来に向けた改善のためにどこにリソースを割くべきかを評価するために、自らのセキュリティ・プロファイルを補完する可視化戦略を定める必要があります。

そのためには、SANSが今回の報告の中で行ったように、学際的なアプローチをとることが不可欠です。私たちは、カリキュラム・リーダー、インストラクター、アナリストなど、SANS内の主要な人材の見識を集めました。そこから見えてきた共通のメッセージは、「優れた可視性は、人、プロセス、テクノロジーの3つの要素からなる」というものでした。これは、組織のさまざまな目的、経営目標と技術目標、さらにはビジネス目標とセキュリティ目標をこえたコミュニケーションの手段となるものです。本稿では、そこに至るためには何が必要かに焦点を当てます。これにより、関係者はそれぞれの役割にとって最も重要な要素に注力しながら、組織のセキュリティの全体像を詳細に把握できるようになります。

出発点：実用的な定義

サイバーセキュリティの専門家は一貫して、数あるニーズの中で「可視性」を最重要視しています。しかし、「セキュリティの可視性」とはいったい何を意味しているのでしょうか。可視性に期待するものが関係者によって異なるため、定義は1つには定まりません（サイドバー「役割に応じた関係者の期待」参照）。とはいえ、いずれの関係者も単独で動くことはありません。それぞれの役割の間には接点があります。**したがって、セキュリティの可視性を組織として確保するには、異なる目標と見なされがちな事柄を整理する必要があります。**

役割に応じた関係者の期待

関係者が可視性に何を期待するかは、以下のように、それぞれが自分の役割にとって重要な問いにどう答えるかによって変わってきます。

- **経営陣**は、現在の状況とトレンドの両方について、脅威とリスクに対する簡潔な視点を必要としています。
  - この業界のセキュリティ・リスクは高まっているか？
  - 組織は検知、保護、防御の準備がどの程度できているか？
  - 組織のリスクは増加（または減少）しているか？

  また、以下のような従来の問いにも答えなければなりません。
  - 組織の支出は適切か？
  - 組織は昨年の同時期よりも良い状態か？
- **運用セキュリティ・チーム**は、脆弱性、イベント、脅威に対するハイレベルな（ほぼリアルタイムの）視点に加えて、すべての詳細を迅速に確認する能力を必要としています。ここでのニーズと問いは以下のようなものです。
  - システム内にマルウェアの兆候はないか？
  - 従業員がアクセス権を乱用していないかどうかを検知できるか？
  - PCIコンプライアンスに準拠できそうか？
- **アナリスト**は、正常な行動と考えられるベースラインに集中します。これには通常、ビジネス分析で使用されるものと同様の手法が採用されます。ここでの問いは以下のとおりです。
  - どのデバイスが既知の悪意のあるWebサイトと通信しようとしているのか？
  - どのようなシステムがネットワークを探ってきているのか？
  - ［最新の脅威名］の兆候は見られるか？

[1] 「The Importance of Board Members in Building a Cybersecurity Strategy（サイバーセキュリティ戦略の策定における役員の重要性）」、https://securityboulevard.com/2021/05/the-importance-of-board-members-in-building-a-cybersecurity-strategy

[2] www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-

セキュリティの可視性が有効であるためには、組織の使命と人口統計（業種、従業員規模、役割、場所など）の両方を考慮した上で、人、プロセス、テクノロジーの要素を含めることが欠かせません。これらの人口統計上の特性は、どのようなメトリクスまたはパフォーマンス指標が最も重要かを左右する、一連の独立変数と見なすことができます。

組織におけるセキュリティの可視性を実用的に定義することは、組織全体のさまざまなセキュリティ概念を統合することから始まります。この体制を構築するために、SANSは安全管理で規範とされる概念に着目し、安全管理システムの4つの柱[3]の定義を採用して、「方針」、「リスク管理」、「保証」、「推進」[4]の領域を構成しました。これらの領域を図1に示します。なお、各領域の内容はサイバーセキュリティを取り巻く概念に合わせて変更されています。

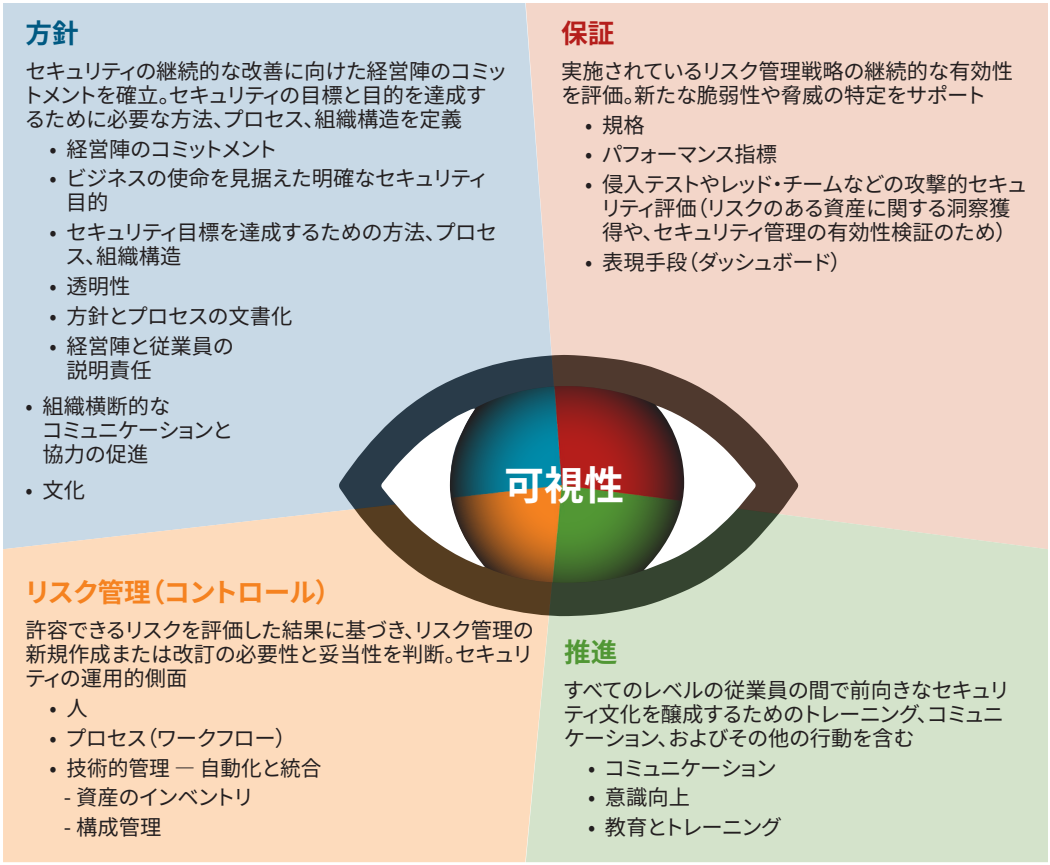

図1：セキュリティの可視性を実用的に定義するための要素

可視性の第一歩となるのは組織（ドメイン）の知識です。知識は分析と結果の目的を設定して維持し、可視化される対象に意味を与えます。どのような可視性が有効であるかは組織によって異なるものの、定義の策定プロセスは一貫したロードマップに従うことができます。これは、SANSが本稿で採用しているアプローチに他なりません。

課題の理解

4つのコア領域がそれぞれ独自のものであるため、可視性のための体系的なアプローチを開発することは困難を伴います。ここからは、各領域に固有の課題について説明します。

- **方針** —最初の大きな課題は、規制で要求されているものと、ビジネスを保護して守るために必要なものの両方の点で、セキュリティに対する組織のコミットメントを確立することです。強固なセキュリティ文化を醸成することは、企業全体のセキュリティ・リスクを理解することから始まります。そのためには、経営陣のコミットメントから資産管理、運用セキュリティに至るまでの各要素がどのように組み合わされ、リスクを許容範囲内に抑えているのかを知る必要があります。組織間のコミュニケーションと協力を促進するには、すべてのレベルの関係者が（アナリストも経営陣も同様に）、自分が見ているものを自らの役割に照らして理解することが求められます。また、なぜ特定のデータを保護すべきなのか、あるいはなぜ特定の活動を記録して監視すべきなのかといった適切な問いを投げかけ、かつそれに答えることも必要です。

[3] www.faa.gov/about/initiatives/sms/explained

[4] www.faa.gov/about/initiatives/sms/explained/components

- **リスク管理** — リスクを効果的に見積もって伝えるためには、問いに答えるために必要となる情報の完全性、正確性、関連性が欠かせません。資産のインベントリと管理は、特に2020年のリモートワークへの移行に伴い、依然として多くの組織の課題となっています。「SANS 2021 Endpoint Monitoring in a Dispersed Workforce Survey（SANS 2021 分散型労働環境におけるエンドポイント監視に関する調査）」では、クラウドまたはDMZベースのサーバを備えたエンドポント監視ソリューション（組織のネットワーク外のデバイスからもデータをキャプチャする場合に必要）を利用していると回答したのは、調査回答者のわずか25%でした。[5] このことは、組織がエンドポイントの可視性をどのように維持できるかに大きく影響しています。中央集中型の管理では、企業ネットワークの内部にしか対処できません。
- **保証** — 導入済みの管理策を監視して評価することは、リスクへの暴露を軽減する取り組みの中で、その管理策が期待どおり機能しているかどうか（準備が整っているか、適切に設計されているか、効果的に運用されているか、定期的に監視されているかなど）を確かめるために不可欠です。ここでの課題は、導入済みの管理策の有効性を、しばしば人為的に作り出される規制遵守の監視要件と分けて考えることです。例を挙げましょう。ある組織は、PCIの認定審査機関（QSA）からPCI準拠と認められたにもかかわらず、PCI関連のインシデントに苦しんでいました。[6]
- **推進** — トレーニング、コミュニケーション、およびその他の行動を含む戦略を策定し、すべてのレベルの従業員の間で前向きなセキュリティ文化を醸成すること（人的要素）は、ネットワークの構築のように単純ではありません。航空業界では、人間の能力や信頼性に関するデータは多くの技術専門家から「ソフト」なものと見なされており、技術的なデータほど注目されていません。セキュリティの専門家である私たちも、数値やハード・データの方が扱いやすいという偏見を持ちがちです。しかし、セキュリティには主観的な側面があります。これらの側面は多岐にわたり、しばしば測定可能な要素を欠いているため、可視性の向上によるリスクの軽減予測には役立ちません。

「SANS Securing the Human」のディレクターであるLance Spitznerは、次のように述べています。「可視性という言葉は［人的側面に対しては］あまり使われませんが、本来はそうあるべきです。［その場合］、可視性は以下の2つの問いに対する洞察をもたらします。

- 組織の最大の人的リスクは何か？
- これらの人的リスクを管理（低減）する組織の能力はどの程度か？」

ここでの課題は、これらの問いにどう答えるのがベストかということです。指標やメトリクスは、技術的な問いに答えるときほど客観性を持つとは限りません。

スタートガイド：組織の可視化戦略の策定

可視性は、組織が脆弱性に対処し、インシデントに対応するための能力を知る手掛かりとなります。各コア領域で何が必要かを検討する出発点として、以下の問いを考えてみましょう。

- **方針**
  - 組織の検知、保護、防御の能力のうち、死角はどこにあるか？
  - トレンドは改善に向かっているか、それとも悪化しているか？
- **リスク管理**
  - 現在の（および潜在的な）攻撃対象領域はどこか？
  - コードやランタイムなどに含まれる既知または潜在的な脆弱性は何か？
- **保証**
  - 組織はコンプライアンスやプライバシー法を正しく遵守しているか？
  - 最近実施した攻撃的セキュリティ評価（侵入テストやレッド・チーム演習など）の結果では、何が組織の脆弱性とされているか？
- **推進**
  - フィッシング演習の結果は、ユーザの継続的な意識向上に何が必要と示しているか？
  - 過去6〜12か月の間に、セキュリティに関するリカレント・トレーニングについての組織のニーズは変化したか？
  - 組織は過去に学んだセキュリティの教訓を従業員に伝え、組織の文化を高めることに積極的か？

[5] 「SANS 2021 Endpoint Monitoring in a Dispersed Workforce Survey（SANS 2021 分散型労働環境におけるエンドポイント監視に関する調査）」、2021年3月、www.sans.org/reading-room/whitepapers/analyst/2021-endpoint-monitoring-dispersed-workforce-survey-40200、p. 6

[6] 「Compliant but not Secure: Why PCI-Certified Companies Are Being Breached（準拠は安全確保にあらず：PCI認定企業が侵害されている理由）」、www.csiac.org/journal-article/compliant-but-not-secure-why-pci-certified-companies-are-being-breached

可視性の意味を知ることの重要性

SolarWinds[7] に対する攻撃やExchangeサーバの侵害[8] など、最近発生したいくつかの大規模なイベントは、事後対応を超えた可視化の必要性を示しています。図2のタイムラインに注目すると、以下のことがわかります。

- SolarWindsの高い市場シェア、大量の採用実績、機密性の高い社内ネットワークへの導入事例、および企業システム全体にわたる広範なリーチを早期に可視化していれば、攻撃者の標的になる可能性が高いことがわかっていたかもしれません。企業はプロアクティブな行動プロファイリングと異常監視を優先できたはずです。
- **攻撃者はSolarWindsのシステムを侵害した後、SolarWindsが悪意のあるコードが仕込まれたOrionアップデートをリリースする3か月前から活動していました。**SolarWindsが攻撃の原因となった脆弱性をプロアクティブに可視化していれば、または内部リソースを走査する攻撃者の行動をリアクティブに可視化さえしていれば、アップデートが侵害されている可能性に気づき、リリースには至らなかったでしょう。
- **侵害されたアップデートは企業ネットワークにインストールされてから最大10か月間機能しており、侵害されたソフトウェアは、以前のバージョンでは一切見られなかったさまざまな動作を行っていました。**事後の調査により、侵害されたSolarWinds Orionに起因する異常な活動や潜在的に悪意のある活動に関しては、被害企業がそれらを迅速に検知するチャンスが十分にあったことがわかりました。

セキュリティの状態

- **リアクティブ** — 過去と現在の脅威に対応します。将来の危険は予測しません。インシデントから得た教訓に基づいて行動することは、リアクティブなセキュリティの一例です。
- **プロアクティブ** — 重大なインシデントを未然に防ぎます。インフラストラクチャの脆弱性を把握して対処し、既知の脅威から守ることは、プロアクティブなセキュリティの一例です。
- **プレディクティブ** — 高度なコンテキスト分析（および人工知能や機械学習などの手法）を用いて、潜在的な脅威をインシデントへの発展前に特定します。これにより、多大な損失やその他の悪影響を回避するための予防措置が実現できます。

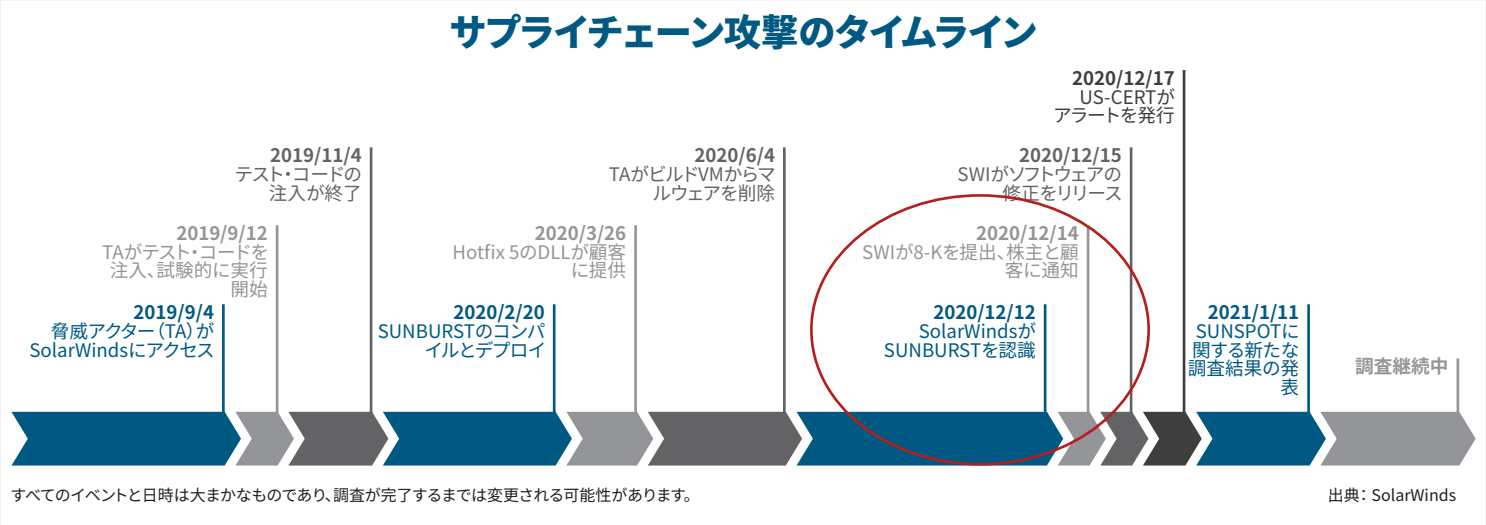

図2：SolarWindsのサプライチェーン：攻撃タイムライン[9]

[7] www.cisecurity.org/solarwinds

[8] www.csoonline.com/article/3616699/the-microsoft-exchange-server-hack-a-timeline.html

[9] 「New Findings From Our Investigation of SUNBURST（SUNBURSTの調査から得られた新たな知見）」、https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst

可視性の具体化

従来、可視性はテクノロジー（デバイス、アプリケーション、エンドポイント、ネットワークなど）の状態と構成を対象としていました。SANSのフェローであり、「SANS Cybersecurity Leadership」と「SANS Cloud Security」の両カリキュラムの責任者でもあるFrank Kimは、次のように述べています。「ユーザ（アイデンティティ、アクセス、リスク・プロファイル）や主要なビジネス・プロセス（M&A、新市場への参入）、テクノロジー・プロセス（DevSecOps）についても可視性が必要です。」

この発言は「Effectively Addressing Advanced Threats（高度な脅威への効果的な対処）」の結果からも裏付けられています。この結果では、インフラストラクチャの可視性のギャップとして、データやアクセスに関するものが上位を占めています。詳細を表1に示します。[10]

表1：可視性のギャップ（SANSの調査による）

順位	可視性のギャップ
1.	インフラストラクチャ内で処理されているデータの種類と場所に対する可視性の欠如
2.	管理対象外の安全でないデバイスによる機密情報へのアクセス
3.	組織の内部関係者による乱用
4.	機密データの地理的な位置または保存先に対する正確な理解の欠如
5.	個人による機密データへの不正アクセス
6.	ユーザ・アクセスに対する監査能力の欠如
7.	インフラストラクチャ横断のインシデントに対する対応力の欠如
8.	インターフェース（APIなど）の構成またはセキュリティの不備
9.	短時間で起動するアプリケーション・コンポーネント（コンテナなど）の構成とセキュリティの不備
10.	マルウェアによる侵入
11.	アプリケーションによる機密データへの不正アクセス
12.	部外者によるインフラストラクチャへの不正アクセス
13.	ハイパーバイザやその他の仮想化管理ソフトウェアの構成不備または脆弱性
14.	アプリケーションのダウンタイムまたは非可用性をその都度認識

クラウドへの移行に伴い、総合的な可視化の必要性が高まっています。2021年のカスタム調査「Network Security in the Cloud（クラウドのネットワーク・セキュリティ）」（本稿執筆時点では未公開）では、回答者の68%がクラウド・サービスを自社ネットワークの中心に据えており、66%が新型コロナウイルス感染症のパンデミック以降でクラウドの利用が拡大していると回答しています。また、回答者の約50%は、組織がよりリモートなモデルへ移行するにつれ、パブリック・クラウドで処理されるデータの可視性の欠如がより顕著になっていると述べています。「SANS 2021 Cloud Security Survey（SANS 2021 クラウド・セキュリティに関する調査）」では、回答者がインシデント対応とフォレンジック分析をクラウドに適応させる際に直面する最大の課題は、インシデントに関わるイベントとコミュニケーションに対するリアルタイムの可視性の欠如であるとされています。[11]

可視性は、組織の主要な問いを1つの（または一連の）結果や答えに結び付け、意思決定を裏付けたり行動を促進したりするコミュニケーションの手段として捉えるのが最も良いでしょう。リスクと可視性の関係については、リスク判断に必要な状況認識の観点では以下のようにまとめられます。

リスク + 可視性 = 洞察と対応力

vs.

リスク + 可視性の欠如 = 対応なし、または間違った対応

[10] 「Effectively Addressing Advanced Threats（高度な脅威への効果的な対処）」、2019年7月、www.sans.org/reading-room/whitepapers/analyst/effectively-addressing-advanced-threats-39105、p. 4

[11] 「SANS 2021 Cloud Security Survey（SANS 2021 クラウド・セキュリティに関する調査）」、2021年4月、www.sans.org/reading-room/whitepapers/analyst/2021-cloud-security-survey-40225、p. 10

図3：可視性ロードマップにおける関係性

図3は、可視性の実現に向けたロードマップを構成する一連のステップをまとめたものです。

以下でそれぞれのステップについて説明していきます。ただし、多くのステップはデータ・サイエンスと分析のベスト・プラクティスに依拠していることに注意してください。なお、本稿では関連する項目を説明しますが、あまり詳細には立ち入りません。

ソース：見えないものに対する考慮

ITの専門家もセキュリティの専門家も、組織のインフラストラクチャに何があるかを知ることの重要性を理解しています。「2020 SANS Network Visibility and Threat Detection Survey（2020 SANS ネットワークの可視性と脅威検知に関する調査）」に回答した専門家のほとんどが、ネットワーク上のデバイスに対する可視性の欠如が、高いリスクをもたらすと感じています。[12] さらに、最近の調査結果では、資産を可視化できていない組織の80%近くが約3倍のインシデントを報告しています。[13]

組織のインフラストラクチャ上に存在するものと、組織が管理しているものとの対比を可視化することは、2つの主要な観点から非常に重要です。まず、インフラストラクチャに何が接続されているかを知ることで、組織（または組織のSOC）がセキュリティで保護すべきものの全体像や、どのような問題が起こり得るのかが明らかになります。つまり、どのような脆弱性が考えられるのか、そしてどのような潜在的な問題があれば攻撃者に脆弱性を利用されるのかが把握できます。ここで、攻撃的なセキュリティ・ソリューションを使用して組織の攻撃対象領域を評価することが、すべての資産の中から実際の攻撃のリスクにさらされている資産を区別するために重要な意味を持つ場合があります。侵入テストやレッド・チーム演習などの活動は、目に見えない（ただし攻撃者からは見えている）現実の問題を明らかにできます。

[12] 「2020 SANS Network Visibility and Threat Detection Survey（2020 SANS ネットワークの可視性と脅威検知に関する調査）」、2020年3月、www.sans.org/reading-room/whitepapers/analyst/2020-network-visibility-threat-detection-survey-39490、p. 5

[13] 「Study Shows 79% of Organizations Acknowledge an Asset Visibility Gap, Leading to 3X More Incidents（79%の組織が資産の可視性ギャップを認識、インシデント件数は3倍に ― 米調査結果）」、www.bloomberg.com/press-releases/2021-04-27/study-shows-79-of-organizations-acknowledge-an-asset-visibility-gap-leading-to-3x-more-incidents

インフラストラクチャを理解する2つ目の重要な理由は、信頼できるデータをもたらして現状把握を可能にしてくれるソースを把握し、かつ信用する必要があるためです。可視化のために収集しようとしているデータのソースには、ギャップが存在しないでしょうか。可視化の要件として、新たなデバイスを導入する必要があるでしょうか。

信頼できない不正なデバイスを検知して特徴付けるには、通常、複数の可視化手法を使用する必要があります。不正なデバイスは協調的なホストベースのセキュリティ・エージェントを持つことがめったになく、多くの場合、単純なネットワーク・スキャンには応答しません。DNSレコードやネットワーク・アクセス制御（NAC）のシステム・ログを使用すれば、不正な要素に対する可視性が向上する可能性があります。

これから説明するCIS Controlsは、ソース管理に対するプロアクティブなアプローチの出発点となります。特に実施すべきCIS Controlファミリーは以下のとおりです。

- **CIS Control 1：企業資産のインベントリ作成と管理**
  このコントロール・ファミリーは、物理的、仮想的、リモート、およびクラウド環境内のインフラストラクチャに接続されているすべての企業資産（ポータブル機器やモバイルを含むエンドユーザ・デバイス、ネットワーク・デバイス、非コンピューティング/IoTデバイス、サーバ）を能動的に管理（インベントリ作成、追跡、修正）し、企業内で監視して保護すべき資産の全体像を正確に把握します。また、未認可で管理されていない資産を特定し、削除または修復することもサポートします。[14]
- **CIS Control 2：ソフトウェア資産のインベントリ作成と管理**
  このコントロールは、ネットワーク上のすべてのソフトウェア（OSとアプリケーション）を能動的に管理（インベントリ作成、追跡、修正）し、認可されたソフトウェアのみをインストールして実行できるようにすると同時に、未認可で管理されていないソフトウェアを特定してインストールや実行を防止します。[15]
- **CIS Control 4：企業の資産とソフトウェアの安全な構成**
  このコントロールは、企業の資産（ポータブル機器やモバイルを含むエンドユーザ・デバイス、ネットワーク・デバイス、非コンピューティング/IoTデバイス、サーバ）とソフトウェア（OSとアプリケーション）の安全な構成を確立して維持します。[16]
- **CIS Control 5：アカウント管理**
  このコントロールは、プロセスとツールを使用して、企業の資産とソフトウェアへの認可をユーザ・アカウント（管理者アカウントやサービス・アカウントを含む）の認証情報に割り当てて管理します。[17] このコントロールはCIS Control 6と連携します。
- **CIS Control 6：アクセス制御管理**
  このコントロールは、プロセスとツールを使用して、組織の資産とソフトウェアへのアクセス認証情報と権限を、ユーザ、管理者、サービス・アカウントに対して作成、割り当て、管理、および無効化します。[18]

> 「基本的には、どのような資産がインフラストラクチャに接続され、どう構成されているのか、それらは管理されているのか、そして誰からアクセスされるのかを知りたいものです。もちろんすべての点で100%を目指したいところですが、常にそうできるとは限りません。
>
> 私がよく使うもう1つのメトリクスは『管理が行き届いているか、手付かずかの割合』です。ほとんどのネットワークには、管理されていないデバイスが存在するでしょう。ネットワーク上で確認されている資産と、完全なサイバーセキュリティ機能が備わったと自分たちが考えている資産との割合を明らかにしたいのです。」
>
> — Chris Crowley、シニア・インストラクター兼SOCコース開発者、SANS

[14] www.cisecurity.org/controls/inventory-and-control-of-enterprise-assets
[15] www.cisecurity.org/controls/inventory-and-control-of-software-assets
[16] www.cisecurity.org/controls/secure-configuration-of-enterprise-assets-and-software
[17] www.cisecurity.org/controls/account-management
[18] www.cisecurity.org/controls/access-control-management

データ、どこでもデータ

とりわけクラウド・コンピューティングの世界では、セキュリティの可視性はデータ駆動であり、さまざまなソースからの主観的および客観的なデータ収集に依存しています。可視性に関連するデータは、大きく分けてエンドポイント（モバイル・デバイス、ワークステーション、サーバ、仮想デバイス、IoTなど）とネットワークの2つのカテゴリに分類できます。

エンドポイントのデータには通常、OSとバージョン、実行中のアプリケーションとプロセスに関する情報、ユーザ・コンテキスト、およびポートの利用状況と確立済みの接続などのネットワーク・データが含まれます。「SANS 2021 Endpoint Monitoring in a Dispersed Workforce Survey（SANS 2021分散型労働環境におけるエンドポイント監視に関する調査）」[19]の回答者は、エンドポイント、メモリベースのアーティファクト、およびマシン間接続で保存または使用されている機密データ（個人の健康情報や企業の占有情報など）についても可視性を高めたいと答えています。

しかし、ネットワークに関しては共通項が少ないままです。表2は、「2020 SANS Network Visibility and Threat Detection Survey（2020 SANSネットワークの可視性と脅威検知に関する調査）」[20]の結果に基づき、現在ネットワークから収集されているデータを示しています。

2021年のSANS調査[22]の結果（本稿執筆時点では未公開）では、**回答者の50%がパブリック・クラウド内の脅威の予防、検知、または対応のためにネットワークのメタデータを積極的に使用しています。そのうちの81%が従来のL2-L4ネットワーク（NetFlow）のデータ、75%がアプリケーションレベルのメタデータを使用して、**以下の内容を正しく識別できるようにしています。

- ネットワーク通信の行動パターン
- 高度な戦術、技術、手順（TTP）
- 不正な資産とサービス

「可視性を評価するための唯一にして最良のメトリクスは、企業内をくまなく捜索する能力です。これは時間ベースのメトリクスでもあり、品質（完了率）のメトリクスでもあります。測定基準は、特定の侵入の痕跡（ファイル、ファイルのハッシュ、ミューテックス、ホスト名、IPアドレス、ユーザ・アカウントなど。ただし、必ずしもこれらに限定されない）に対して、現在管理している資産の80%、90%、100%を評価するためにどの程度の時間がかかるか、といったものです。この資産は、サーバ、ワークステーション、モバイル・デバイス、またはその他の適切なカテゴリへとさらに細分化できます。」

— Chris Crowley、シニア・インストラクター兼SOCコース開発者、SANS

表2：収集されたネットワーク・データ[21]

データの種類	収集した回答者の割合
Active Directory/LDAPのログイン試行	89.2%
DNSトランザクション	71.4%
DHCPトランザクション	64.0%
HTTPペイロード	62.1%
IPFIX/NetFlow/ホスト間接続データ	60.1%
証明書のメタデータ	43.8%
SMB/CIFSのメソッド	41.9%
データベースのメソッド	40.4%
その他	2.0%

暗号化されたトラフィック：ネットワークの可視性を阻害する要因

クラウド・インシデント対応に関する2020年の調査[23]では、回答者の約3分の1（32%）が、組織における効果的なクラウド・インシデント対応を阻害する要因として、暗号化されたネットワーク・トラフィックの可視性が不十分であることを挙げています。

「2020 SANS Network Visibility and Threat Detection Survey（2020 SANS ネットワークの可視性と脅威検知に関する調査）」では、回答者の約40%が社内ネットワークのトラフィックの50～74%が暗号化されていると答えており、ほとんどの回答者がトラフィックの暗号化によってネットワーク上の脅威に対する可視性が損なわれることを懸念していました。[24] しかし、SANSによる2019年のSOC調査から判断すると、大半の場合はTLSインターセプトが一切利用されていません。たとえ技術が導入されていたとしてもです。

こうして見ると、なぜ組織は可視性を実現するために復号を*用いないのか*という疑問が湧いてきます。プライバシーの懸念からでしょうか。それとも、復号処理によるパフォーマンス上の制約など、より技術的な理由からでしょうか。

[19]「SANS 2021 Endpoint Monitoring in a Dispersed Workforce Survey（SANS 2021分散型労働環境におけるエンドポイント監視に関する調査）」、2021年3月、www.sans.org/reading-room/whitepapers/analyst/2021-endpoint-monitoring-dispersed-workforce-survey-40200（注：このデータは報告書には含まれていない調査結果によるものです。）

[20]「2020 SANS Network Visibility and Threat Detection Survey（2020 SANSネットワークの可視性と脅威検知に関する調査）」、2020年4月、www.sans.org/reading-room/whitepapers/detection/paper/39490、p. 4

[21] www.sans.org/reading-room/whitepapers/analyst/2020-network-visibility-threat-detection-survey-39490、p. 8

[22]「A SANS Survey: Network Security in the Cloud（SANS調査：クラウドのネットワーク・セキュリティ）」、2021年6月公開予定、www.sans.org/reading-room/whitepapers/analyst

[23]「2020 SANS Enterprise Cloud Incident Response Survey（2020 SANS企業におけるクラウド・インシデント対応に関する調査）」、2020年9月、www.sans.org/reading-room/whitepapers/cloud/paper/39805、p. 6

[24]「2020 SANS Network Visibility and Threat Detection Survey（2020 SANSネットワークの可視性と脅威検知に関する調査）」、2020年4月、www.sans.org/reading-room/whitepapers/analyst/2020-network-visibility-threat-detection-survey-39490、p. 7

- コマンドアンドコントロール（C2）トラフィック
- 特定のネットワークIoC（侵入の痕跡）

図4に示すように、データ収集には特有の問いとメトリクスがあります。

適合性	どのデータが非標準形式で保存されているか？
一貫性	どのデータ値が矛盾した情報を与えているか？
正確性	どのデータが間違っている、または古くなっているか？
重複性	どのデータ・レコードまたは属性が繰り返されているか？
完全性	どのデータが欠けている、または参照されていないか？

図4：データ品質のメトリクス[25]

情報への注力

ソース・データをキャプチャして正しく情報に変換することは、測定と保証に向けた次なるステップとして欠かせません。分析アルゴリズム（ルールベースまたはAI/機械学習ベース）でデータを分類し、実用的な情報（メトリクスとKPI）に変換します。

メトリクスと測定

メトリクスとは、最も単純な形では、ビジネス活動のある側面を追跡して活動実績の成否を測定するために記録された値に過ぎません。メトリクスは定量化できるため、組織は結果を具体的に説明し、掲げた目標に対して実際の活動がどの程度うまくいっているかを示すことができます。

ここで難しいのは、主要なメトリクスを選択して有効性を判断することです（使用されないメトリクスには価値がないため）。有効なメトリクスを開発することは、口で言うほど簡単ではありません。図5を用いて説明します。

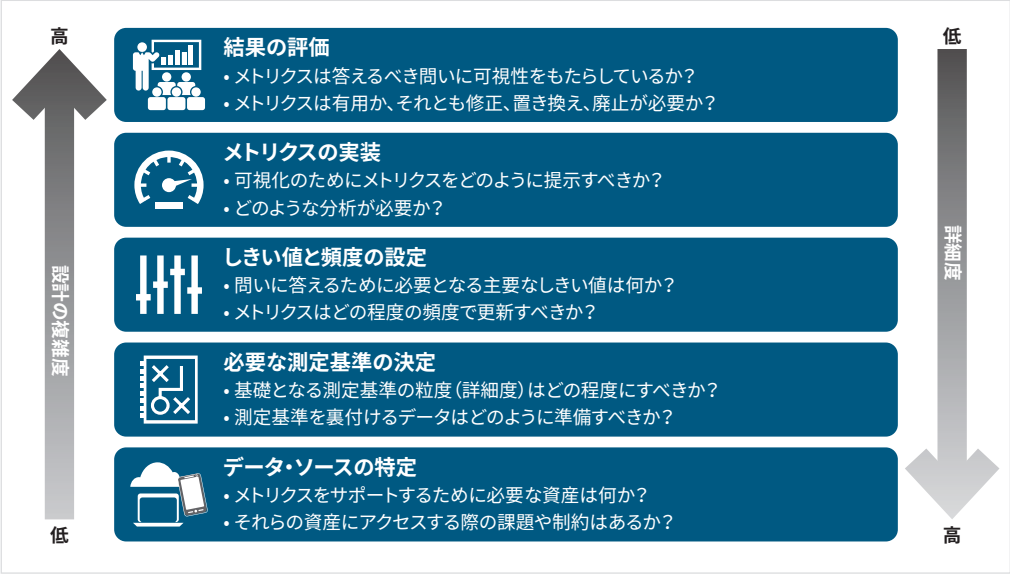

図5：データからの情報取得：メトリクスの構築[26]

設計の複雑度が最も低いとき、詳細度が最も高くなり、さまざまなエンドポイントから収集されるデータ要素の量が最も多くなります。設計の複雑度が増すにつれて詳細度は低下し、最終的にはこれらのデータが集約され、情報の塊にまとめられて関係者に提示されます。

ビジネスの測定：セキュリティ・パフォーマンス指標

セキュリティ上のビジネス目標を達成するにあたり、組織がどの程度の効果を上げているかを可視化するにはどうすればよいでしょうか。パフォーマンス指標が役に立ちます。メトリクスが特定のビジネス・プロセスの状態を追跡するのに対し、パフォーマンス指標は組織がビジネス目標/目的を達成したかどうかを追跡します。

> 「これらすべての領域でメトリクスを定義するのに役立つ、業界標準の測定フレームワークは存在しません。たしかに、MITRE ATT&CK™ などは検知の領域で素晴らしい成果を挙げています。しかし、たとえば識別と保護については包括的なフレームワークがありません。セキュリティ・チームがサポートする必要のある主要なビジネス・プロセスについても同様です。」
>
> — Frank Kim、フェロー、SANS

[25] https://datacadamia.com/data/quality/metric

[26] 「Improving the Bottom Line with Effective Security Metrics: A SANS Survey（効果的なセキュリティ・メトリクスによる収益改善：SANS調査）」、2020年8月、www.sans.org/reading-room/whitepapers/analyst/improving-bottom-line-effective-security-metrics-survey-39720、p. 11

メトリクスとパフォーマンス指標の違いを示す簡単な例を以下に示します。

- **メトリクス（準備の度合い。ただし、ビジネス目標に関わるビジネス上の文脈は考慮しない）** — 完全にパッチ適用されて最新状態になっているネットワーク上のデバイスの数
- **ビジネス目標** — ネットワーク上のデバイスの少なくとも80%が、完全にパッチ適用されて最新状態になっていること
- **パフォーマンス指標** — ネットワーク上の既知のデバイス数に対する、完全にパッチ適用されて最新状態になっているデバイス数の割合は80%未満

簡単に言えば、すべてのパフォーマンス指標はメトリクスになりますが、メトリクスのすべてがパフォーマンス指標になるとは限りません。決定的な違いは、パフォーマンス指標では組織がセキュリティにどのようにアプローチし、そのアプローチがどの程度成功し得るかを測定する点です。セキュリティ・パフォーマンス指標は、改善のための行動が必要な場所を可視化できますが、必ずしもその行動の内容を示すものではありません。

別の視点から見ると、パフォーマンス指標は、脅威の悪用可能性や深刻度に関するメトリクスを策定済みのビジネス目標（たとえば、対応する管理策の実際のコスト）と相関させることができます。経営陣はこのパフォーマンス指標を使用して、リスクを軽減するためのコストと、リスクが実現した場合の実際の影響とを比較して評価できます。

セキュリティの伝達（可視化）

最後のステップは可視性を伝えることです。絶えず変化する脅威環境、広がり続ける脅威の対象領域、および新たな脅威ベクトルに対しては、スタンドアロンのスプレッドシート、レポート、モジュラー式のガバナンス・ツールなど、従来の静的な表現手段は不十分であり、効率も悪くなる場合があります。関係者が求めているのは、動的でリアルタイム、かつ実用的な洞察です。

ただし、静的なレポートがもはや意味をなさないというわけではありません。それらは特にレトロスペクティブ（時間的/事後対応的な遡及分析）やフォレンジックの目的では重要です。しかし、プロアクティブまたはプレディクティブ（予測的）なセキュリティ態勢へ移行する場合、組織のサイバーセキュリティの状態をリアルタイムに示す実用的な情報（メトリクスとパフォーマンス指標）を、理解しやすく、かつ行動につなげやすい形で提示することが課題となります。主要なサイバーセキュリティ管理からのデータを組み合わせ、実用的な単一ダッシュボードにまとめる一元的な視点が必要なのです。これにより、組織のサイバーセキュリティ態勢に関する明快な洞察がもたらされます。

可視化技術は理解を容易にし、検知、予測、予防に関する実用的な意志決定をサポートします。自動化と分析により、リアルタイムの表示（すなわち可視化）と連携し、検知、予測、予防に関する懸念に対処できます。

「ダッシュボードとは、1つまたは複数の目的を達成するために欠かせない重要情報を視覚的に表示したものです。情報を一目で確認できるように、1つの画面に集約して配置されています。」

— Stephen Few、創設者兼代表、Perceptual Edge[27]

[27]「Dashboard Confusion Revisited（続・ダッシュボードにまつわる混乱）」、http://perceptualedge.com/articles/visual_business_intelligence/dboard_confusion_revisited.pdf、p. 1

可視化やその他の手法の詳細な説明は本稿の範囲外ですが、以下の点には留意しておきましょう。[28]

- 重要な側面に集中し、ダッシュボードへの詰め込みを避けること。すべてが重要なものとして扱われると、本当に重要なものがわからなくなります。
- 視覚、聴覚、触覚を駆使して重要なメッセージを明らかにし、整った環境の中でもそれらのメッセージが目立つようにすること。ここではKISSの原則が当てはまります。
- あちこち見回して時間を無駄にしないこと。計器飛行では走査することが重要ですが、ここでも同じことが言えます。
- 表示媒体（紙、タブレット、オーバーヘッド・スクリーンなど）に留意すること。
- 3次元を避けること。紙やディスプレイ画面は2次元であるため、結果を提示する際にはこの点に注意しましょう。

ダッシュボードはリアルタイムの情報を提示するのに最適なツールです。適切に設計された効果的なサイバーセキュリティ・ダッシュボードは、実用的な洞察をもたらすことで、優れた意思決定を促進します。その方法の1つは、入り組んだ主要リスク指標と複雑な視覚情報の詳細を単純化し、最も重要な情報を伝えることです。優れたダッシュボードは、さまざまなサイバーセキュリティ管理からのデータに基づく一元的かつ総合的な視点をもたらすことで、サイバーセキュリティのサイロを解消するのに役立ちます。

ダッシュボードの概念は特に新しくはないものの、数年ごとにより革新的なものへと再発明されているように思われます。ただ、素晴らしいツールではあるのですが、開発には労力とリソースを要します。メトリクスに関する2020年のSANS調査において、パフォーマンス・メトリクスを完全かつ継続的に可視化できる統合ダッシュボードでメトリクスを追跡、分析、報告しているとの回答がわずか5%しかなかったのは、これが理由の1つかもしれません。[29] 恐れずにダッシュボードを採用してみましょう。

真の目標は、最も重要な情報を正確に（そして魅力的に）伝えるタイムリーな方法を見つけ出すことです。関係者は、組織の現在のセキュリティ態勢に関する全貌を可視化して概念化するために、こうした情報を必要としています。

可視化の成功パターン

組織におけるセキュリティの可視性をどのように定義するかを決定したら、次のステップは前述のギャップ分析です。組織は現在どのような状態にあり、そして本来はどうあるべきなのでしょうか。前者は比較的容易に把握できますが、後者は特定のビジネス、テクノロジー、および組織が直面している脅威環境に大きく依存します。後者をうまく行うためには、セキュリティの可視性を構築または向上するためのすべての取り組みに対し、最終的な可視性の目標と、目標の達成に必要となる戦略を定義する必要があります。

[28] Rudis、Bob、Jay Jacobs、*Data-Driven Security: Analysis, Visualization and Dashboards（データ駆動型セキュリティ：分析、可視化、ダッシュボード）*、.Wiley、2014年

[29] 「Improving the Bottom Line with Effective Security Metrics: A SANS Survey（効果的なセキュリティ・メトリクスによる収益改善：SANS調査）」、2020年8月、www.sans.org/reading-room/whitepapers/analyst/improving-bottom-line-effective-security-metrics-survey-39720、p. 16

1つの方法は成熟度モデル[30]のアプローチに基づくことです。このアプローチでは、より高い成熟度の可視性がビジネス上の利益につながります。これは、組織が成熟度モデルのアプローチ[31]をIT運用やサイバーセキュリティ・プログラムの全体ですでに使用している場合に最も効果的です。しかし、正式な成熟度モデルは取締役会や経営陣とのコミュニケーションには威力を発揮する一方で、維持と追跡のオーバーヘッドが増します。

組織が成熟度モデルを使用していない場合の別のアプローチとして、可視化の有効性についての一般的なパターンを調べて、組織が現在どのような状況にあり、どのようにすればより高いパフォーマンスとビジネス上の利益が得られるかを明確化する方法があります（図6参照）。

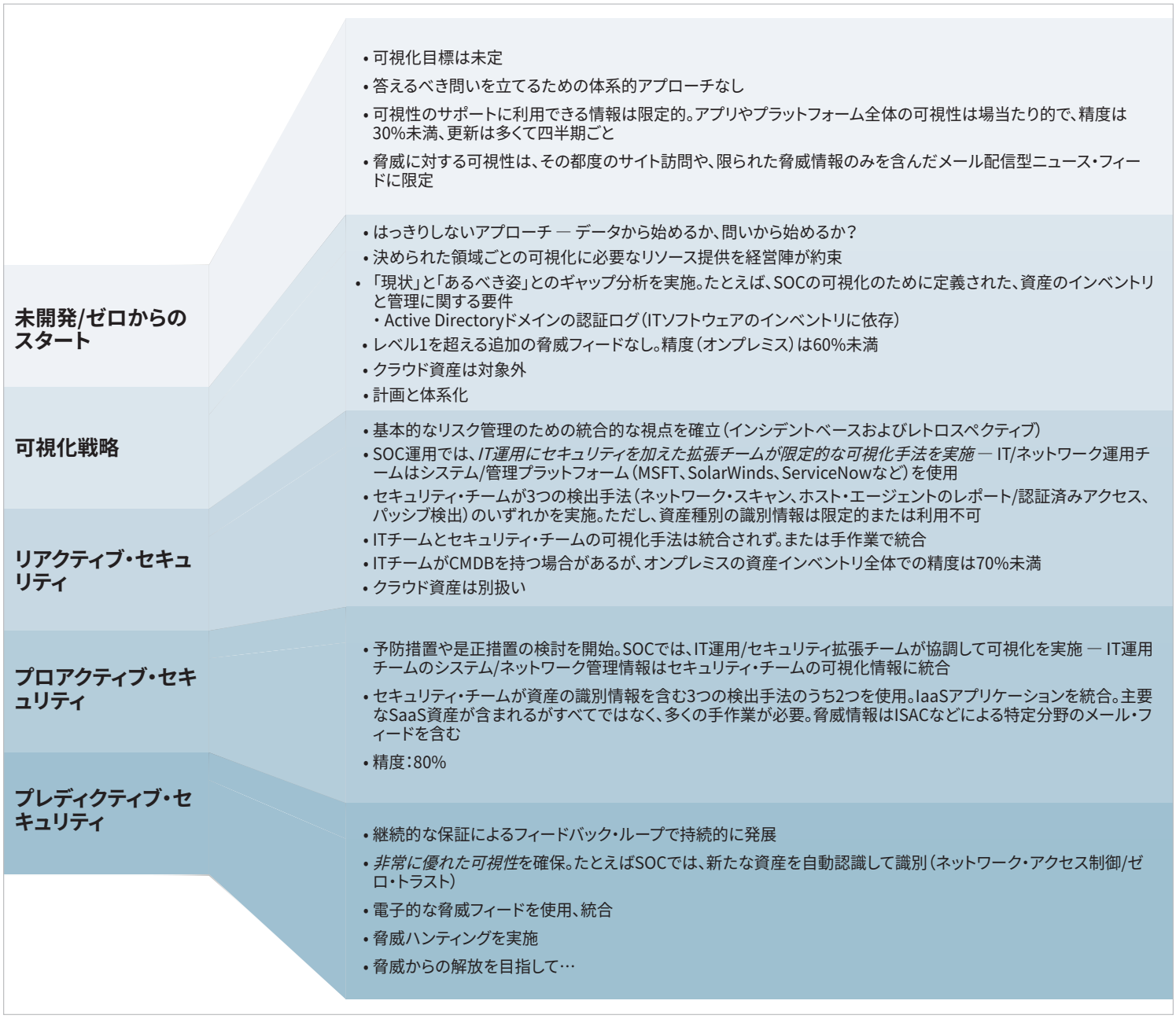

図6：可視化の成功パターン

[30]「Cybersecurity Capability Maturity Model（サイバーセキュリティ能力成熟度モデル）」、米国エネルギー省、2014年2月、http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

[31]「Improving Detection, Prevention and Response with Security Maturity Modeling（セキュリティ成熟度モデリングによる検知、予防、対応の改善）」、2015年5月、www.sans.org/reading-room/whitepapers/analyst/improving-detection-prevention-response-security-maturity-modeling-35985

改善への道のり

可視性は主観的なトピックであり、関係者によって意味が異なります。そのため、オンプレミスのセキュリティ、クラウド、またはサプライチェーンのいずれに関しても、可視化戦略を策定する上でのギャップが数多く存在します。認知された（または実際の）ギャップの多くは、セキュリティの専門家が技術的な考え方とビジネスの理解を橋渡しできていないために生じています。もう一度Frank Kimの言葉を借りれば、「ビジネス・プロセス、メトリクスの分析、データを洞察に変えること、[これらは]リスクが実際にどこにあるかを示すものです。障壁となるのは、ビジネス・ドライバーの理解の欠如です。」

また、人的要因にも対処する必要があります。Lance Spitznerによると、組織は最上位の人的リスクに対する可視性と、それらの人的リスクを管理する能力を大きく改善する必要があります。奇妙なことに、最大の障壁となるのは、セキュリティ・チームが人的セキュリティを真剣に受け止めず、自分たちの仕事とさえ認めていない場合が多いという事実です。セキュリティ意識はしばしば「娯楽」と捉えられ、セキュリティのテーマを実質的に矮小化しています。これは実際、人を守るためだけでなく、組織全体のリスクを管理するために意識の向上が欠かせないような場合にさえ起こっています。しかしSpitznerによれば、幸いにもこのような認識は変化し始めています。

クラウド・コンピューティングによって、世の中はソフトウェアとデータの両方を駆使したものに変わりつつあります。こうした中では、開発と運用のサイロを越えて可視性を向上させる必要があります。これには、コードの内容、変更されるコードと変更の頻度、変更の権限を持つユーザ、さらにはビルド、テスト、デプロイの方法など、実際のコードに対する可視性も含まれます。

組織においては、経営陣とセキュリティ・チームが協力し、トップダウンであると同時にボトムアップでもある強固なセキュリティ文化を醸成する必要があります。そのためには、組織内で共通の「セキュリティ上のビジネス言語」を作り上げることが欠かせません。セキュリティ・チームがビジネス目標に取り組むことができない場合、特にチームの影響力が限られている領域では、経営陣と協力してビジネスのリスクを大きく軽減する効果はほとんど期待できません。

まとめ

可視性には主観的な性質があるとはいえ、組織はそれを定義して測定するための手段を講じることができます。本稿でSANSは、組織が戦略を策定するのに役立つ目的志向のアプローチ（ロードマップ）を提示しました。サイバー世界における可視性が依然としてデータ駆動であることを考えると、さらなる発展に向けた基本的なアドバイスは以下のようになります。

- 目的と前提/制約条件を明示すること。
  - 目的を定めましょう。どのような問いに答える必要があるでしょうか。どのようなプロセスを監視すべきでしょうか。どのトレンドを追跡したいでしょうか。
  - 各自の役割を理解すること。経営陣がSOCのディレクターやアナリストと同じ問題意識（または注意力）を持つとは限りません。
- 目的を果たすために何が必要かを明らかにすること。プロセスの監視やトレンドの追跡のためには、どのようなソースやデータが必要でしょうか。
- 問いが客観的な答えを持つように、結果を体系化すること。物事がどれだけうまくいっているかを測定し、重要なトレンドを特定するために使用できる、意味のあるメトリクスを確立しましょう。ただし、期待バイアスに注意する必要があります。
- 分析や表現/可視化の「アート」に陥らないこと。データと情報そのものに任せましょう。

そして何よりも、組織が可視性を欠いた状態からリアクティブ、プロアクティブ、そして最終的にプレディクティブなセキュリティ慣行へ移行していく際には、可視化の成功パターンを常に意識しておきましょう。

「ソフトウェア開発とコーディングに対する可視性は、開発/運用チームが構成をコードとして扱っている場合、つまり、コード内で実行時の構成をモデル化し、実行時のスタックに構成変更を加えている場合には特に重要です。なぜなら、このコードはインフラストラクチャの攻撃対象領域をとらえて描写しており、攻撃対象領域の変化をよりわかりやすく、追跡しやすく、そしてテストしやすくするからです。

また、SolarWindsに対するSUNBURSTの脆弱性で見られたように、コードのビルド・ツールチェインとワークフローの可視性は、組織を攻撃から守るために欠かせません。ビルド・パイプラインに対する攻撃は、理論上のものからすでに現実のものへと変化しているのですから。」

— Jim Bird、アナリスト、SANS

著者について

Barbara FilkinsはSANSのリサーチ・ディレクターです。GSEC、GCIH、GCPM、GLEG、GICSPなどさまざまなSANS認証、およびCISSPを保有し、SANS Technology Instituteで情報セキュリティ管理の修士号を取得しています。システム・エンジニアリングやインフラストラクチャ設計のコンサルタントとして、システムの調達、ベンダの選定、ベンダとの交渉などを幅広く手がけてきました。Barbaraは特に保健福祉業界において、自動化に関わる問題（プライバシー、個人情報の盗難、詐欺への暴露）や、今日のモバイルとクラウドの環境で情報セキュリティを実施する際の法的側面に注力しています。連邦政府機関から地方自治体、商業企業に至るまで、幅広い顧客を抱えています。

John Pescatoreは2013年1月にエマージング・セキュリティ・トレンド担当ディレクターとしてSANSに加わりました。以前の経歴には、Gartner社での主席セキュリティ・アナリストとしての13年以上の経験、Trusted Information Systems社とEntrust社でのコンサルティング・グループの運営経験、GTE社での11年の勤務経験があるほか、米国家安全保障局ではセキュアな音声システムを設計し、米国シークレット・サービスではセキュアな通信および監視システムや「臨時弾道装甲設備」を開発していました。Johnは米議会でのサイバーセキュリティに関する証言経験を持ち、2008年にはセキュリティ分野で最も影響力のある15人の1人に選ばれています。また、NSA認定の暗号技術者でもあります。

スポンサー

SANSは本稿のスポンサーに感謝いたします。

ExtraHop