ゼロトラストアーキテクチャに向けて

複雑でハイブリッドな世界のためのガイド付きアプローチ

CSAJC cloud security alliance℠ Japan Chapter

CSA cloud security alliance®

要約

企業の利害関係者は、リアルタイムシステムの複雑化、新たなサイバーセキュリティポリシーの必要性、そしてセキュアにシステムを運用するために欠かせない力強い文化的サポートといった課題を考慮する必要があります。ゼロトラストのような新たなテクノロジーソリューションやアプローチは、バイデン大統領の大統領令14028 *Improving the Nation's Cybersecurity* で定められた義務を果たすために不可欠です。本稿では、新たに登場した豊富で多様なソリューションの意味と、ゼロトラストアーキテクチャ（ZTA）を最終的に実現するための組織の能力に対する課題について検討しています。また、企業のリーダーとセキュリティ担当者がそれぞれの環境にゼロトラストを導入することを促進するために、業界が主要なステークホルダーグループ間のコラボレーションを強化する方法についても提言しています。

本稿は、Cloud Security Alliance - Washington DC Chapter (CSA-DC) Research Committee によって作成されました。
Research Committee Chair: Mari Spina

Acknowledgments

Authors:

Juanita Koilpillai
Jyoti Wadhwa
Dr. Allen Harper
Salil Parikh
Paul Deakin
Vivian Tero
Greg Bateman
Aubrey Merchant-Dest
Jay Kelley
Phyllis Thomas
Uma Rajagopal
Rebecca Choynowski

Contributors:

Jason Keplinger
Tom Stilwell
Lauren Bogoshian
Bob Klannukarn
Joe Klein
Daniele Catteddu
Nirenj George
Jagan Kolli
Andres Ruz

Special Thanks:

Bowen Close

About the CSA DC Chapter

This document was created by the DC chapter of the Cloud Security Alliance (CSA). The DC Chapter of the CSA consists of volunteers who have been at the forefront of cloud security. Visit our website at https://www.cloudsecurityalliance-dc.org/ for more information.

献辞

本稿は、突然の予期せぬ死により、サイバーセキュリティコミュニティとCSA-DC支部の友人たちにとって大きな損失となったJuanita Koilpillai氏に捧げるものです。Juanitaは、本稿および本稿を作成したCSA-DC支部のワーキンググループの主要な著者であり、貢献者でもありました。Juanitaのサイバーセキュリティへの貢献は今後も続き、世界中の組織のサイバーセキュリティ態勢を強化していくでしょう。彼女の技術的なリーダーシップとSoftware-DefinedPerimeter (SDP)技術の開発は、ゼロトラストアーキテクチャ(ZTA)の初期の基盤を形成しました。
Juanitaは、サイバーセキュリティコミュニティを明るく照らす真の光でした。真に偉大なリーダーでありエンジニアであった彼女に別れを告げるのは、非常に残念なことです。

Anil Karmel
President, CSA-DC Chapter

日本語版提供に際しての告知及び注意事項

本書「ゼロトラストアーキテクチャに向けて」は、Cloud Security Alliance (CSA)が公開している「Toward a Zero Trust Architecture」の日本語訳です。本書は、CSAジャパンが、CSAの許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSAジャパンは何らの保証をするものではありません。
この翻訳版は予告なく変更される場合があります。以下の変更履歴(日付、バージョン、変更内容)をご確認ください。

変更履歴

日付	バージョン	変更内容
2022年02月10日	日本語版1.0	初版発行

CSAジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス(CSAジャパン)は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

1.　責任の限定

CSAジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。

(1) 本書の内容の真正性、正確性、無誤謬性
(2) 本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3) 本書の内容に基づいて行われた判断や行為がもたらす結果
(4) 本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

2.　二次譲渡の制限

本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。

ただし、以下の場合は本項の例外とします。

(1) 本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2) 本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。

(3) CSA ジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4) 転載、再掲、複製の作成と配布等について、CSA ジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

3. 本書の適切な管理

(1) 本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。
(2) 本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。
(3) 本書をダウンロードした者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。
(4) 本書を印刷した者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

4. 原典がある場合の制限事項等

本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

5. その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSAジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

日本語版作成に際しての謝辞

「ゼロトラストアーキテクチャに向けて」は、CSAジャパン会員の有志により行われました。作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名を記します。（氏名あいうえお順・敬称略）

伊藤　文二
小野　貴博
小田部　悟士
塩澤　将弘
中垣　弘幸
松村　康平
諸角　昌宏

目次

1 背景

COVIDパンデミックの影響で、企業はグローバルなリモートワークをサポートするために迅速な対応を迫られています。リモートワークの拡大とクラウド技術の採用により、セキュリティ境界線の定義が拡大し、今後の仕事を守るためにゼロトラスト（ZT）戦略の採用が必要になっています。さらに、俊敏性と拡張性に優れたマルチクラウド、ハイブリッド・アーキテクチャへの移行が進んでいることもあり、情報システムのセキュリティとリスク管理を改善する必要性がかつてないほど高まっています。現在、IT組織は、自社の環境に固有のゼロトラスト・アーキテクチャ（ZTA）を定義して採用することに優先的に取り組む必要に迫られています。ZTAの採用は、国家のサイバーセキュリティの改善を義務付ける最近の大統領令[1]や、連邦ゼロトラスト戦略[2]によってさらに促進されています[2]。

境界防御や多層防御によるアプローチがこの新しいセキュリティパラダイムに取って代わられたことで、企業は、特にリモートでの生産性に必要な最新のマイクロサービス、マイクロセグメンテーション、およびソフトウェア定義のアーキテクチャを採用し始める中で、セキュリティリスクを低減することを求めています。ITベンダーから幅広い支持を得ていますが、企業はZTAアプローチのベースラインを策定し始めたばかりであり、業界は継続的な協力関係を通じてベストプラクティスや標準を形成するための洞察を求めている段階のため、ZTAの実現はまだ野心的な将来の目標です。

本稿は、サイバーセキュリティの担当者、エンジニア、設計者、ビジネスリーダー、IT関係者に情報を提供するのに役立ちます。広く役立つ内容ですが、本稿は米国政府の視点に焦点を当てています。そのため、NIST SP 800-207についての一般的な知識が必要となります。

1.1 なぜゼロトラストなのか？

情報セキュリティにおけるZTモデルは、2003年にJericho Projectが従来の境界型ネットワークのセキュリティ上の課題を認識して発表したもので、2009年にはGoogleのBeyond Corpプロジェクトが ZTを導入し（2014年に公開）、さらに2010年にはForrester Researchが続きました。ZTモデルでは、「信頼できるネットワークという概念を排除」し、「ゼロトラスト（ZT）では、すべてのネットワークトラフィックは信頼できない。したがって、セキュリティ専門

[1] Exec. Order No. 14208, 86 FR 26633 (May 12, 2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[2] U.S. Office of Management and Budget. (n.d.). *Federal Zero Trust Strategy. Cybersecurity & Infrastructure Security Agency*. Retrieved September 29, 2021, from https://zerotrust.cyber.gov/federal-zero-trust-strategy/

[3] Kindervag, J. (2010, September 17). *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*. Palo Alto Networks. https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

[4] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August 11). SP 800–207, Zero TrustArchitecture. NIST. https://csrc.nist.gov/publications/detail/sp/800-207/final

家は、すべてのリソースを検証して保護し、アクセス制御を制限して厳密に実施し、すべてのネットワークトラフィックを検査して記録しなければならない」と教えています[3]。2019年、NISTはZTのアイデアをZTAの抽象的な定義に融合し、ZTAの開発と実装のための指針を示す「Zero Trust Architecture[4]（SP 800-207）」を作成しました（図1参照）。新たなZTセキュリティ環境の導入を推進する業界のダイナミクスには、セキュリティコストの増大、5Gの普及、クラウドコンピューティング、IoT（Internet of Things）、マイクロサービス指向アーキテクチャなどがあります。これらの要因は、物理的またはソフトウェア定義による固定的なネットワーク境界の重要性を下げ、所有権の境界や使用パターンの再定義を促します。

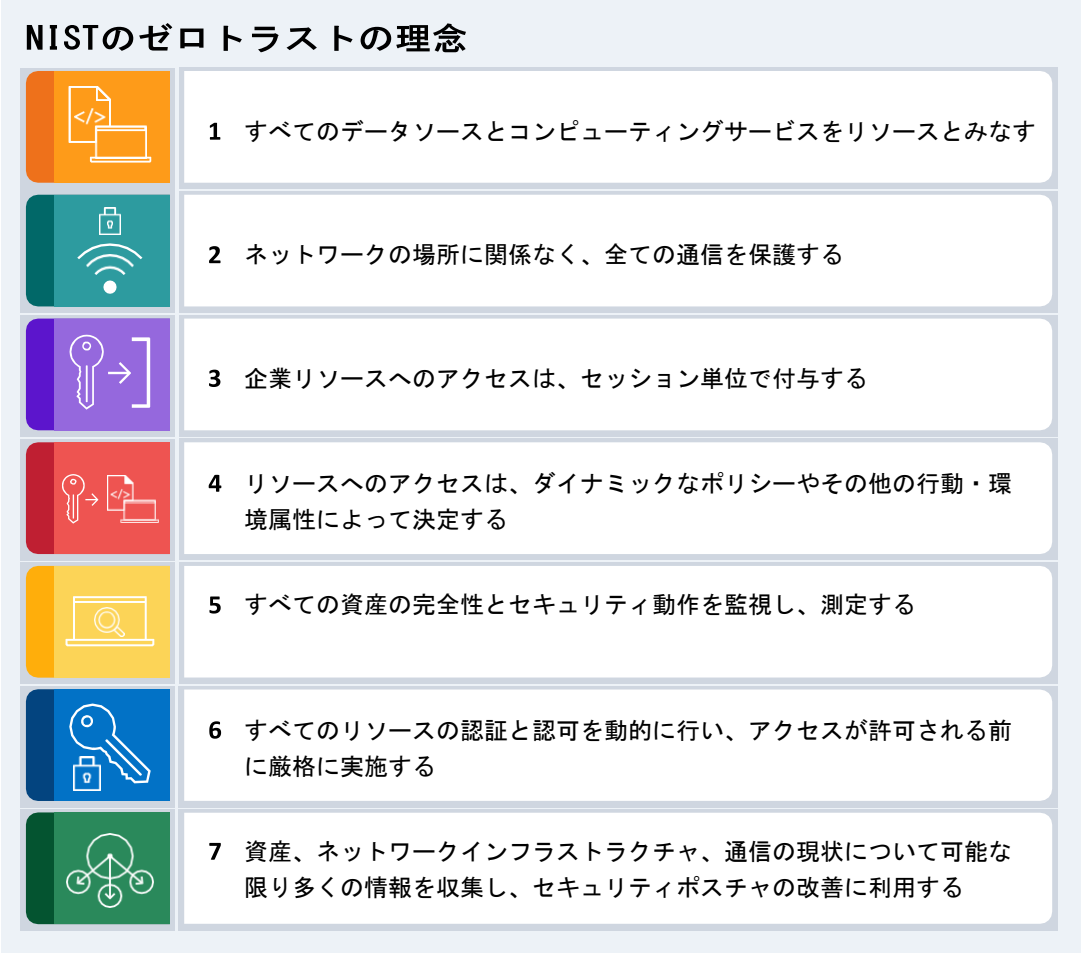

図1. ゼロトラストの理念、NIST SP 800-207

政府機関や民間企業では、ネットワークの全部または一部をクラウドに移行する動きが進んでおり、プライベートクラウド、パブリッククラウド、コミュニティクラウドのインスタンスを新たな方法で保護することが求められています。その必要性は切迫していますが、このようなセキュリティ環境の変化を実現するには時間と意思が必要です。組織は、新しい技術スタック、スキルセット、およびプロセスを用いて、クラウド上のシステムを保護する能力を向上させる必要があります。そのため、継続的な検証、マイクロセグメンテーション、SDN、継続的な監視と可視性に基づいた新しいセキュリティガバナンスとポリシーの策定が課題となっています。このような最新のポリシーを導入し、実施するためには、業界関係者は、従来のアクセス制御技術と最新のネットワーク技術の両方を複雑に組み合わせ、時間をかけて自社の環境に合わせてカスタマイズしながら設計・運用する必要があります。

常時接続のVPN接続や企業のゲートウェイを経由した全トラフィックのルーティングなど、一般的に導入されているアプローチは、コストやユーザー体験の観点から効率が悪くなり、もはや実行不可能なものになっています。さらに、サイバーセキュリティの多くはシグネチャベースの概念に基づいており、ツールは既知の悪質な行為の「シグネチャ」を探しますが、ゼロデイの脅威は、定義上、既知のシグネチャがありません。ZTAはリスクを緩和する手助けとなるシグネチャベースの技術やアノマリーベースの技術に依存しないため、この限界に対応することができます。ZTでは、セキュリティコントロールは、実際のデータや機能が実在する場所や時間に関係なく、広く行き渡り、正しい傾向を示します。しかし、組織間で近代化の速度とレベルに格差があることから、これらの最新のアーキテクチャを保護する方法に関する業界のガイダンスの速度と成熟度は遅れており、システムとそのデータを最適に保護するには、まだ十分な調整が進んでいません。

アーキテクチャや市場の複雑さを考えると、ZTソリューションやロードマップの成熟はまだ始まったばかりです。例えば、セキュリティ担当者は、リアルタイムのマルチクラウド環境でユーザーを特定し、新たなサイバー脅威を自動検知する機能を実装するという課題に直面しています。今日の高度でハイブリッドな状況を踏まえ、本稿では、ゼロトラストアーキテクチャ能力成熟度モデル（ZTA-CMM）の基本要素を提案し、ZTロードマップと関連付けています。政府と業界の対話とコラボレーションを継続することで、ZTA-CMMのベストプラクティスを開発し、現在のアーキテクチャとギャップに対処するためのZTロードマップに、ZTの原則がどのように適用されるかを評価することにより、リスク管理とサイバーレジリエンスの改善を実現します。

1.2 現在のゼロトラストの成熟度を評価

組織は、組織全体でレビューを行い、徹底的かつ効率的な分析を行うことにより、自組織における現在の ZTA の成熟度を把握する必要があります。この分析では、ZT の中核になる現在の人材、プロセス、および技術を考慮する必要があります。連邦政府機関に特化した文書ではありますが、CISA Federal Zero Trust Strategy[5] は、ZTAの導入を成功させるために不可欠なプロセスや技術を理解するためのガイドとして活用できます。米国国立標準技術研究所（NIST）およびACT-IAC[7]やForrester[8]などの業界関係者[6]によって、概念モデルやフレームワークが特定されつつあり、今後も進化していくと思われますが、現時点ではこれらのフレームワークをまとめる取り組みは行われていないことに留意する必要があります。CISA は、アイデンティティ、デバイス、ネットワーク、アプリケーション・ワークロード、データという柱で構成される ZT CMM[9] を発表しました。これらの5つのコンポー

---

[5] U.S. Office of Management and Budget. (n.d.). *Federal Zero Trust Strategy.* Cybersecurity & Infrastructure Security Agency. Retrieved September 29, 2021, from https://zerotrust.cyber.gov/federal-zero-trust-strategy/

[6] Microsoft. (n.d.). *Zero Trust Model - Modern Security Architecture.* Retrieved September 29, 2021,from https://www.microsoft.com/en-us/security/business/zero-trust

[7] American Council for Technology-Industry Advisory Council. (2019, April 18). *Zero Trust Cybersecurity Current Trends.* https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf

[8] Forrester. (n.d.). *The Zero Trust Security Playbook For 2021.* Retrieved September 29, 2021, from https://www.forrester.com/playbook/The+Zero+Trust+Security+Playbook+For+2020/-/E-PLA300

[9] Cybersecurity and Infrastructure Security Agency, Cybersecurity Division. (2021, June). *Zero Trust Maturity Model - Pre-decisional Draft, Version 1.0.* Cybersecurity and Infrastructure SecurityAgency. https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20 Maturity%20Model_Draft.pdf

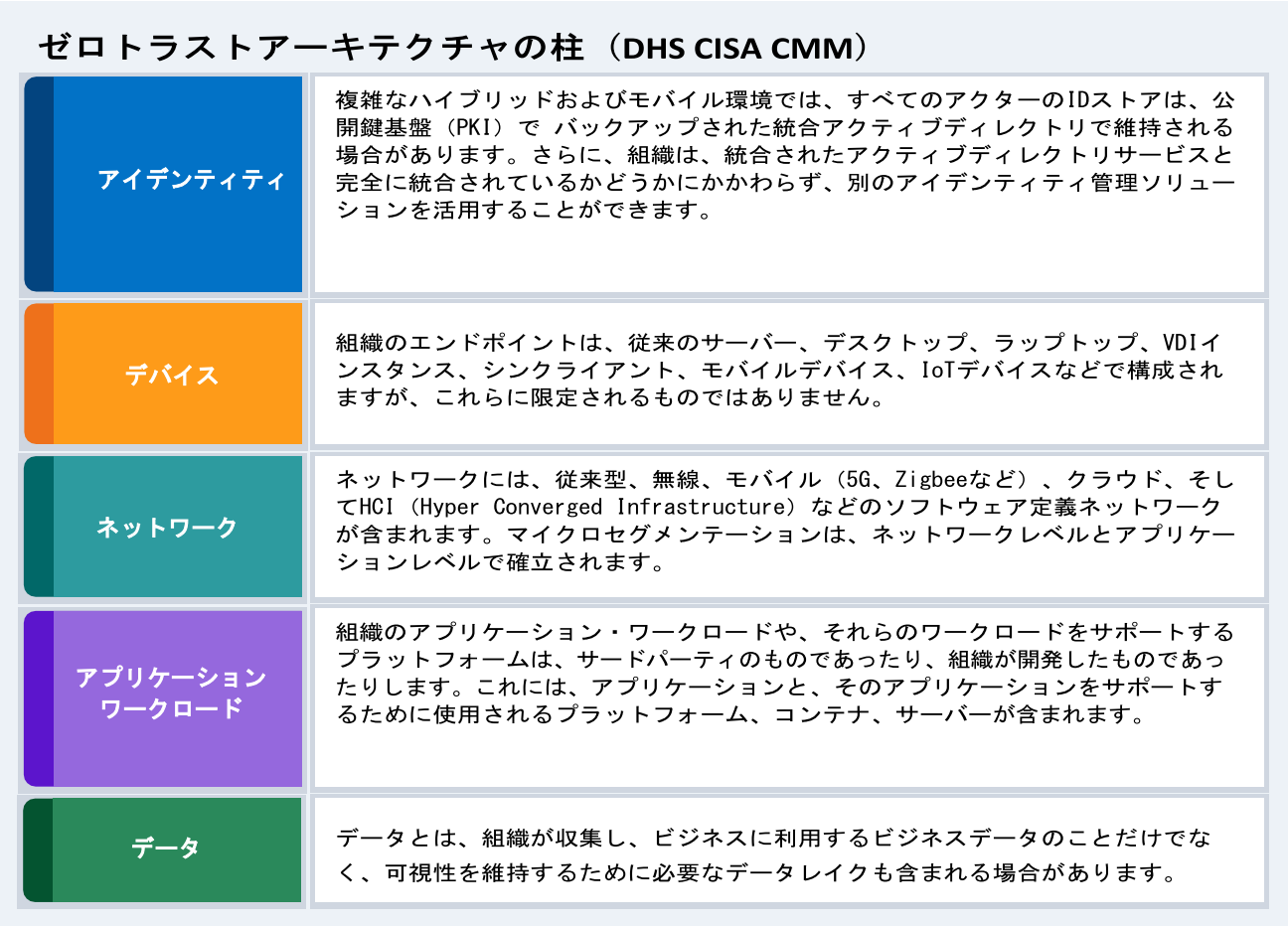

図2. ゼロトラストの柱、DHS CISA ZT-CMM

ネントを合わせることで、組織がZTAの開発に向けてリソースを適用し得るさまざまな領域について、全体的な視点が得られます。

ZTA-CMMでは、それぞれの柱の成熟度を知ることができます（図2参照）。各分野を深く理解することで、組織の利害関係者に、ZTAの導入に関する環境独自の強みとギャップを伝えることができます。現在、組織がZTAの評価に利用できる、広く受け入れたゼロトラスト成熟度モデルがありません。これは業界のガイダンスにおけるギャップであり、ZTA-CMMの順序付けやレベルによって業界のコラボレーションを促進する分野でもあります。その間、個々の組織は最初の評価を進め、その最初の評価の結果がその組織のベースライン評価となるでしょう。

1.3 ゼロトラストロードマップの策定

企業は組織のZTA成熟度レベルの現状をより深く理解することで、ギャップに対処して成熟度を高める新しいソリューションを特定し、アーキテクチャに組み込むことができます。例えば、DHS CISA ZT CMM（DHS CISA）では、図3に示すように、従来型、先進型、最適型の3つのレベルを使用しています。

図3. CISA ZT-CM, (DHS CISA)

目標とする成熟度レベルを達成するためには、組織の現在の成熟度レベルを評価し、その評価に基づいて、目標とする成熟度レベルを達成するために、定められたスケジュールで実行すべき優先分野、必要なリソース、予算配分を特定するよう利害関係者に促すことが必要です。すでに ZT アプローチを高度にアーキテクチャに反映させている先進的な環境における目標成熟度は、セキュリティとITの近代化の道を歩み始めた組織と比較して、はるかに高くなることが予想されます。ZTAロードマップの要件に対応するために、利害関係者は、目標とする成熟度の達成につながる可能性がある、進化するテクノロジーの最新の展望をより深く理解する必要があります。

これは5つの柱のそれぞれについて、組織の能力の成熟度を評価することから始まります。それぞれの柱について、いくつかの質問を作成し、関連する利害関係者が各重点分野の成熟度について総合的な評価を行います。これらの質問は、その柱におけるZTの成熟度が高まるにつれ、難易度と範囲を増やしていくことになります。質問への回答後、組織は定量化された結果を、組織の現在の ZTA 成熟度のベースライン評価として活用することができます。成熟度は、CMMC[10] が提案するアプローチと同様に、組織の方針に合わせて測定結果を数値化し、図4に例示するように組織のZT成熟度の望ましい状態または目標状態と一緒にスパイダーダイアグラムで表すことができます。

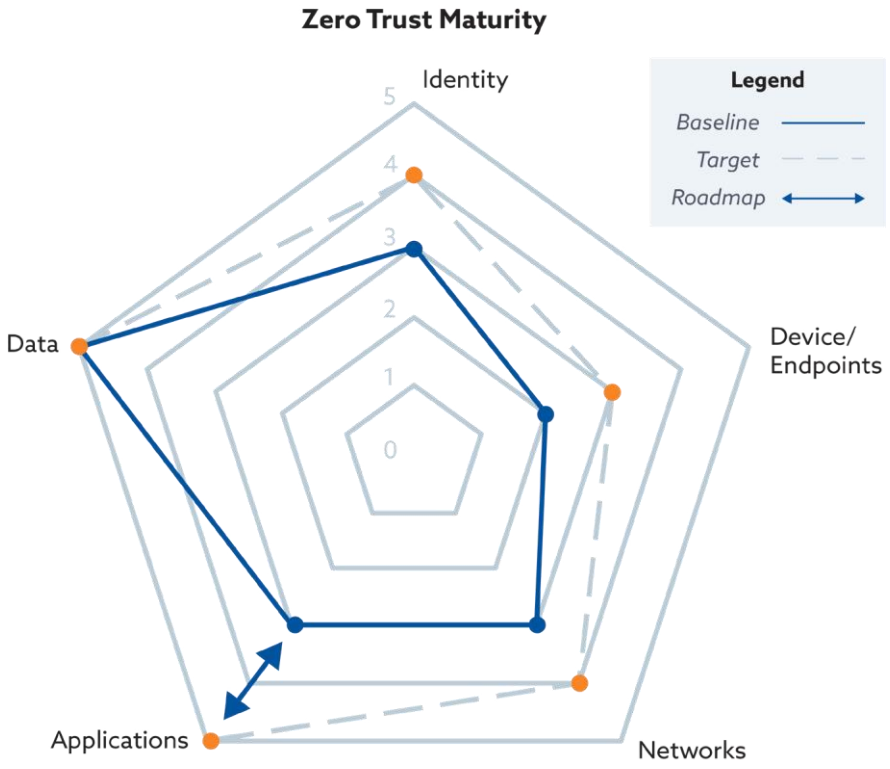

図4. ゼロトラスト成熟度・スパイダーダイアグラム（概念的）

その結果、ベースラインポイントとターゲットポイントの差がギャップ評価となります。ギャップ評価では柱ごとにZTロードマップが取り組むべき具体的な分野を設定し、1～3年かけて現状を目標状態へと段階的に改善していきます。

[10] CMMC Information Institute. (2021, August 21). *DoD/NIST SP 800–171 Basic Self Assessment Scoring Template*. https://cmmcinfo.org/cmmc-info-tools/dod-nist-sp-800-171-basic-self-assessment-scoring-template/

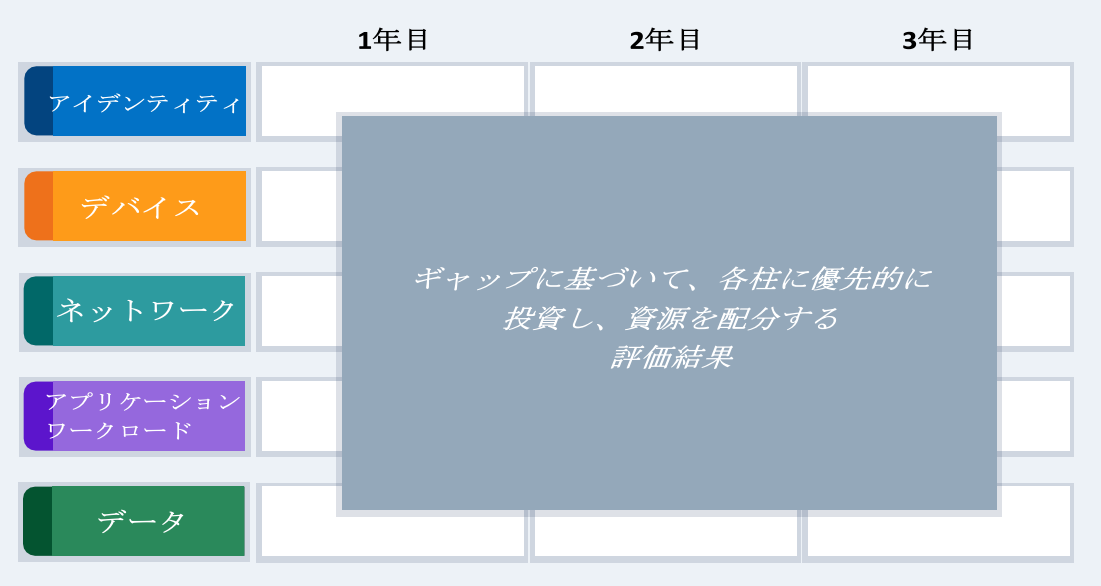

図5. ZT優先投資ロードマップ(想定)

このアプローチにより、図5に示すようなZTの優先順位付き投資ロードマップが作成されます。また、それぞれの柱に関連する、NIST Special Publication (SP) 800 シリーズ、CSA Cloud Controls Matrix (CCM)、政府の Security Technical Implementation Guides (STIG) などの業界のベストプラクティスやフレームワークの利用を取り入れる必要があります。これにより、組織が1～3年かけて望ましい成熟度を達成するために、現状では不足している詳細なプロセスや技術の要件を導き出すことができます。このアプローチは、可能性の一例として提示したものであり、各組織に合わせてカスタマイズすることが可能です。 ZTAを採用するための全体的なアプローチとして、将来のワーキンググループや組織が、能力の成熟度を評価するための標準的な質問と図表を開発するかもしれません。

2 ゼロトラスト導入時の注意点

ZTの成熟度評価とロードマップの検討に加えて、技術、組織文化、ポリシー、規制環境の4つの要素が、ZTAを開発する上で重要な検討事項となります。これらの組織の内部および外部の要素は、今日の複雑でハイブリッドな環境のZTAロードマップを理解、設計、および実装する組織の能力に影響を与えます。組織のステークホルダーが、現在のZTAの成熟度において、どの要素が重要な障壁または推進要因となっているか、また、どの要素がZTAの進展に最も役立つかを特定するのに役立ちます。

ZTAを採用する上で欠かせないのが、人、プロセス、技術、重要資産、セキュリティコントロールの棚卸しです。これは、アーキテクチャの採用を成功させるための鍵となります。NISTは、単一のプロセスから始めて、組織全体にアーキテクチャを展開していくことを推奨しています。

組織は、すぐに効果が得られる施策を盛り込み、ZTAの採用は長期的かつ戦略的な取り組みとなることを理解する必要があります。そのため、3年から5年の間、経営陣の支援とこれらすべての要素の継続的な検討が必要となります。ZT能力成熟度モデルは、適切な質問をしてその答えを求めることを通じて、既存、かつレガシーな組織の能力を理解するためのガイドとなります。例えば、以下のような質問が考えられます。

1. 組織が使用しているレガシーなテクノロジーとは？
2. どのようなデータ/サービスを利用しているのか？
3. 具体的にどのようなクラウドサービスを導入しているのか？
4. CASBソリューションが導入されているか？
5. アイデンティティはどのように管理され、どのようなツールが導入されているか？
6. 組織はクラウド導入のどの段階にいるか？

ただし、これらの質問は組織の特定の事業やミッションに合わせて行う必要があります。それぞれの質問は、組織のビジネス状況に関連するテクノロジー、組織文化、現在のポリシー、影響を受ける規制環境、組織が採用予定のクラウドセキュリティアーキテクチャなどを取り上げる必要があります。米国連邦政府機関の場合、これらはCISAのCloud Security Technical Reference Architectureに明記されています。[11]

2.1 テクノロジー

技術的な検討は非常に重要です。従来の技術的なソリューションは、境界における多層防御が中心でしたが、この境界をベースにしたアプローチでは、ITシステムに対する攻撃の多様化と攻撃の増加を抑えることはできませんでした。アプリケーションデリバリーのためのコンピューティングユニットは、集中管理された物理サーバーからクラウド全体に分散された多数の仮想化サーバーおよびサービスや、非常にきめ細かいコンテナへと移行しています。

[11] Cybersecurity and Infrastructure Security Agency. (n.d.). *Cloud Security Technical Reference Architecture*. Retrieved September 29, 2021, from https://zerotrust.cyber.gov/cloud-security-technical-reference-architecture/

機能の細分化は、ZTの適用にポータビリティの課題をもたらしますが、デジタルトランスフォーメーションの一環としてクラウドの導入が進む中、ZTは次の進化を意味し、サイバー攻撃の防止と回復のための最新のアプローチであると言えます。ICAM（Identity and Credential Access Management）、SDN（Software-Defined Network）、マイクロセグメント化された環境、IAP（Identity-Aware Proxies）、システムを継続的に監視する能力などの主要な機能を組織が使いこなすことが、ZTへの移行を促進します。組織が採用するアーキテクチャにおけるテクノロジーの状況と、市場エコシステムで利用可能なオプションを理解することが、組織の環境に適したソリューションの選択に影響します。

2.2 組織文化

組織の文化もまた、組織のすべてのステークホルダーが考慮すべき強い影響力を持っています。COVID-19の大流行は、組織を在宅勤務プログラムやセキュリティチームのZT戦略へと向かわせるきっかけとなったことが証明されています。ZT を採用するためには、組織は進んで変化に対応し、組織の再構築を通じて「誰も信用しない」アプローチを促進する必要があります。レガシーな環境ではなく、拡張性のあるクラウドやハイブリッドモデルの採用に積極的な企業は有利な状況であり、"ZTマインドセット "をより容易に採用できるでしょう。自組織の文化と変化への対応力を理解することが重要です。

2.3 ポリシー

組織文化と並んで重要なのは、組織がポリシーを更新できるかどうかという点です。最新のIT環境は、オンプレミス型とクラウド型のアーキテクチャが混在した、高度で複雑なハイブリッド型であり、組織のサイバーセキュリティコントロールのポリシー策定を困難なものにしています。ポリシーの変更による影響は、組織のインフラ、アプリケーション、およびデータ全体に及びます。ZTベースの新しいポリシーを特定し開発する能力は、重要な要素であり、組織毎に固有のものとなります。ZTAは未成熟であるため、組織がこれらのポリシーを特定し、作成し、正式に発行することは困難が伴うかもしれません。

2.4 規制環境

ZTの採用において、最後に注目すべき要素は規制環境です。米国政府は、サイバーセキュリティのコンプライアンスを推進するために、NISTが管理するRisk Management Framework（RMF）[12]とCybersecurity Framework（CSF）という2つの主要なフレームワークを用意しています。これらのフレームワークは、セキュリティの評価、導入、承認、監視に関するガイダンスを提供しています。2013年2月12日に発行された大統領令13636「*Improving Critical Infrastructure Cybersecurity*」[13]は、既存の標準、ガイドライン、慣行に基づいて、重要インフラにおけるサイバーリスクを減らすためのフレームワークを確立しました。

[12] Securicon Team. (2019, October 8). *NIST 800–53 Rev. 5: What it Is, and Why You Should Care*. Securicon. https://www.securicon.com/nist-800-53-rev-5-what-it-is-and-why-you-should-care/

[13] Exec. Order No. 13636, 78 FR 11737 (February 12, 2013). https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

このガイドラインは、2014年のサイバーセキュリティ強化法を補強するものでした[14]。これらのコンプライアンスフレームワークは柔軟性がありますが、効果的なZTAの導入を促進するための特別なものではなく、また最適化されたものではありません。2021年5月12日に発行された大統領令14028「*Improving the Nation's Cybersecurity*」[15]は、組織にサイバーセキュリティリスクの説明責任を負わせ、サプライチェーンを含む重要インフラの所有者および運営者のサイバーセキュリティへの取り組みを支援するよう行政機関に求めています。これらの取り組みは、評価され、さらなる政策立案への機運を高めています。ZTAの成熟度評価（ZTA-CMM）や、本質的なセキュリティの改善を実現するタイムラインを含むZTAロードマップの必要性と相まって、国防総省の事例など参考となるZTAが構築されています。このような規制面での取り組みは、新たなサイバー攻撃を阻止してレジリエンス（攻撃の影響を最小化し、早急に元の状態に回復する能力）を高めるために必要な変化を促すのに役立ちます。新しい規制が義務化されると、ハードウェアやソフトウェアのベンダー、システムインテグレーター、サービスプロバイダ、IT企業などの業界のプロバイダーやステークホルダーによるソリューションの展開に革新をもたらすことになります。

[14] National Institute of Standards and Technology. (2021, July 14). *Cybersecurity Framework | GettingStarted*. NIST. https://www.nist.gov/cyberframework/getting-started

[15] Exec. Order No. 14208, 86 FR 26633 (May 12, 2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

3 ゼロトラストソリューションランドスケープ

ZTの成熟度を高めるためには、適用可能な技術やソリューションを検討・特定することが不可欠です。例えば、クラウドコンピューティングの従来のインフラは進化し、現在ではコンテナやサービスメッシュなどの最新のコンポーネントが含まれており、ZTのコアコンポーネント（「ポリシーエンジン」[PE]、関連する「ポリシーアドミニストレータ」[PA]、および様々な「ポリシー実施ポイント」[PEP]）との統合が必要になります[16]。ZTAを管理するためのこの種の新しい戦略は必然的に発生するものであり、以下の技術分野および関連する例は、ZTAに向けた最新のソリューションを提供する進化したセキュリティ環境のほんの一例に過ぎません。本稿で検討した技術的アプローチと影響の例としては、Software-Defined Architectureコンポーネント、サービスメッシュ機能、エッジコンピューティングのトレンド、コードとしてのポリシー定義の可能性についてのレビューが含まれます。

3.1 Software-Defined Perimeter

Software-Defined Perimeter（SDP）とZTの原則は、セキュリティの状況における同じような圧力、認識、および変化に対応しながら、同時に進化してきたと言えるでしょう。さらに、ZT原則の動機となった懸念事項の多くをSDPコンポーネントが解決していることから、これらの概念はよく一致しています。現在、SDPは、ZT原則を実現するSoftware-Defined Architectureの明確な一部として業界で認識されており、NIST ZTA出版物では、ZTAへのアプローチとしてSDPが紹介されています。[17]

ガートナーリサーチは、SDP を「企業アプリケーションへのセキュアなアクセス」を提供する技術と位置づけ、デバイス認証とユーザー認証を「本質的な機能」とし、「多様な宛先に向けて複数の暗号化トンネルを確立する機能」を備えていると強調しています[18]。SDPは、要求システムとアプリケーションインフラストラクチャ間のリアルタイムの暗号化された接続を通じて、デバイス認証と本人確認を行った後にのみ、アプリケーションインフラストラクチャへのアクセスを提供します。2019年、ガートナーは、アプリケーションまたはアプリケーション群の周囲にアイデンティティとコンテキストベースの論理的アクセス境界を設ける「ゼロトラストネットワークアクセス（ZTNA）」モデル[19]を通じて、SDPを引き続き支持しています。アプリケーションは発見されないように隠され、アクセスは信頼されたブローカーを介

---

[16] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August 11). *SP 800–207, Zero TrustArchitecture*. NIST. https://csrc.nist.gov/publications/detail/sp/800-207/final

[17] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August 11). *SP 800–207, Zero TrustArchitecture*. NIST. https://csrc.nist.gov/publications/detail/sp/800-207/final

[18] Gartner Research. (2018, November 9). *Fact or Fiction: Are Software-Defined Perimeters Really theNext-Generation VPNs?* https://www.gartner.com/document/3892882

[19] Riley, S., MacDonald, N., & Orans, L. (2019, April 29). *Market Guide for Zero Trust Network Access*. Gartner. https://www.gartner.com/en/documents/3912802/market-guide-for-zero-trust-network-access

して一連の指定されたエンティティに制限されます。これにより、アプリケーション資産が一般の人の目に触れることがなくなり、攻撃対象面が減少します[20]。この進化は、クラウドセキュリティアライアンス（CSA）が2020年に発表したレポート「Software-*Defined Perimeter（SDP） and Zero Trust*」[21]において、SDPを"ネットワーク層のゼロトラスト"として認識することでも支持されています。

[20] Riley, S., MacDonald, N., & Orans, L. (2019, April 29). *Market Guide for Zero Trust Network Access*. Gartner. https://www.gartner.com/en/documents/3912802/market-guide-for-zero-trust-network-access

[21] Cloud Security Alliance SPD and Zero Trust Working Group. (2020, May 27). *Software-Defined Perimeter (SDP) and Zero Trust*. Cloud Security Alliance. https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-and-zero-trust/

3.2 ネットワークセグメンテーション

上述したように、SDPはZTAへのアプローチを提供しますが、SDPはセグメンテーション（ZTの文脈ではマイクロセグメンテーションと呼ばれることが多い）を活用して、default-DENYモデルにより攻撃対象面を減らし、データ侵害の特徴であるラテラルムーブメントを妨ぐ必要があります。SDPのアプローチは、アクセスを許可する前に認証と認可を実施するネットワークセグメンテーション機能の進化に由来します。共有ネットワークのリンクに暗号化を加えることで、暗号化キーによるネットワークのセグメンテーションが可能になります。もう一つのアプローチであるホストベースのセグメンテーションは、ホストのファイアウォールを制御して認可された通信チャネルを作成し、動的なポリシーとセグメンテーション制御を、大規模かつ異機種のOSコンピューティングプラットフォーム(オンプレミス、パブリックおよびプライベートクラウド、コンテナ)間で実現する機能であり、暗号化キーの使用に対してワークロードに沿ったポリシーを可能にします。

ネットワークのセグメンテーションをセキュリティに利用するには、各ゾーンのサービスタイプとその通信関係、ユーザーのアイデンティティ、データの機密性などを組み合わせて定義されたセキュリティゾーンを作成する必要があります。[22] 従来のネットワーク・セキュリティ・ゾーニング・パラダイムは、リソースのオーバーヘッド、ファイアウォール・ルールの管理の複雑さ、および統合のリスクなどの問題により、かなり広い信頼ゾーンの限られたセットになってしまいます。これは、ZTの「攻撃対象領域の削減/最小特権」という理念に反するものです。さらに、仮想マシン、コンテナ、ステートレスサーバー、コンテナ、サーバーレス、マネージドクラウドサービスなどの新技術上でワークロードを実行する最新のアプリケーションアーキテクチャを持つ組織は、これらの伝統的なパラダイムで効果的にセグメント化することに苦労するかもしれません。

一方、SDN（Software-Defined Network）は、トラフィックを管理するネットワークコントロールプレーンとフォワーディングプレーンを分離します。ネットワークコントロールは、APIを介して直接プログラム可能であり、フローのよりダイナミックな調整や、トラフィックをマイクロセグメント化するセグメンテーション制御が可能です。また、SDNによるEast-Westのセグメンテーションにより、より詳細なセキュリティゾーンの設定が可能になります。

マイクロセグメンテーションソリューションは、ワークロード、デバイス／エンドポイント、およびユーザーのアイデンティティを包括的かつ統一的に可視化する統合機能を備えている必要があります。また、セキュリティインシデントの予防と対応のために、セグメンテーションの自動化とオーケストレーションが可能であることが理想的です。ZTの機能が成熟するにつれ、メタデータ・ラベリング・ガバナンスを組み込む機能が、セグメンテーション制御の自動化とオーケストレーションをサポートするようになります。
その例を以下に示します：

[22] Riley, S., MacDonald, N., & Orans, L. (2019, April 29). *Market Guide for Zero Trust Network Access*. Gartner. https://www.gartner.com/en/documents/3912802/market-guide-for-zero-trust-network-access

- IPアドレス、新しいワークロードの検出、ユーザーやデバイスの接続などの変化に対応して、許可リストを動的に実施。
- DevSecOpsのCI/CDパイプラインとの統合により、新しいワークロードやコンテナの誕生時にセグメンテーションを提供。
- アラートとアナリティクスで、ダイナミックなポリシー管理を実現。
- 脅威の検知、監視、脆弱性スキャンとの統合により、適用可能な許可リストを自動的に再計算し、プロセスレベルのセグメンテーションをオーケストレーションする。

セグメンテーションのアプローチはすべてが同じではないため、組織は自社のクラウドインフラに最も適したアーキテクチャと配備モデルを選択する必要があります。

クラウドサービスプロバイダ（CSP）が、IT組織に安全で拡張性のある俊敏なコンピューティングとストレージのオプションを提供するという重要かつ広範な役割を果たしていることを考えると、これらのプロバイダーがZTAへのアプローチとしてSDPとSDNをユビキタスに採用していることにも注目する必要があります。CSPは現在、グローバル規模のIPv4およびIPv6ネットワークを設計、構築、運用するためのZTアプローチに不可欠なコンポーネントとしてSDNを活用しています。これにより、セキュリティの向上をサポートし、膨大な顧客ベースとパートナーエコシステムのZTコンポーネントをサポートするために利用可能なネイティブサービスを拡大しています。個々の組織は、それぞれのロードマップに沿って独自のZTAを設計・実装するために、ネイティブコンポーネントやサードパーティのプロバイダーをどのように活用するかを理解する必要があります。

3.3 サービスメッシュ

ZTAで考慮すべきもう一つの重要な技術は、集中的なポリシー管理とオーケストレーションを実現するためのコンテナベースのサービスメッシュです。コンテナは、最新のクラウドコンピューティング環境で好まれるアプリケーション構成として登場しましたが、展開の効率化が図られる一方で、ITアーキテクチャのエンドポイントの数が大幅に増加する可能性があります。サービスメッシュを使用していない場合、コンテナ環境に広くセキュリティポリシーを導入しようとすると、これが課題となります。

現在、ほとんどの新しいコンテナ環境は、Kubernetes、RedHat OpenShift、Docker Swarm、Nomadなどのコンテナプラットフォームや、AWS Elastic Container Service（ECS）などのクラウドベースのサービスによって実現されています[23]。コンテナプラットフォームは通常、コンテナ内の通信セキュリティに対応していないため、サービスメッシュソリューションは、コンテナ環境全体の通信セキュリティポリシーの管理、展開、およびリアルタイムのオーケストレーションをサポートするように進化しています。実装は、サイドカーのコンテナやプロセスを利用するアプローチが主流です。サイドカーは、ポリシー実施ポイント（PEP）として機能するように実装され、コンテナベースのワークロードに対応しています。Kubernetesクラスター内のPEPは、高性能で安全なプロキシである必要があり、ポリシーの適用だけでなく、Webアプリケーションファイアウォール（WAF）などの他のセキュリティ保護にも対応できます。セントラルオーケストレーションサービスは、アクセス制御やイベント監視などに関連するサイバーセキュリティポリシーを呼び出すためのポリシー決定ポイント（PDP）として機能します。このKubernetes内のアーキテクチャは、コントロールプレーンや企業のICAMサービスとうまく統合され、最新および従来の認証規格をサポートする必要があります。

ZTをコンテナ化されたマイクロサービスのエンドポイントに拡張する際の革新的な点は、ISTIOのようなサービスメッシュの実装です。ISTIOは、オープンソースのサービスメッシュで、組織の既存のKubernetesベースのコンテナ化されたアプリケーションの提供を透過的に行うことができます[24]。ISTIOは、米国国防総省のPlatform Oneで実証されているように、今日のDevSecOpsのパイプラインをサポートするように調整されています[25]。ISTIOのソリューションは、NIST SP 800-207の規定に沿って、組織のコンテナ環境にZTAソリューションを提供することができます。

---

[23] ClickIT. (2021, August 5). *The most popular Kubernetes alternatives and Competitors.* https://www.clickittech.com/devops/kubernetes-alternatives

[24] Istio. (n.d.). *Istio*. Retrieved September 29, 2021, from https://istio.io/

[25] Chaillan, N. (n.d.). *How did the Department of Defense move to Kubernetes and Istio?* NIST Computer Security Resource Center. Retrieved September 29, 2021, from https://csrc.nist.gov/CSRC/media/Presentations/dod-enterprise-devsecops-initiative/images-media/DoD%20Enterprise%20DevSecOps%20Initiative%20%20v2.5.pdf

3.4 エッジコンピューティング

Kubernetesをベースにした最新のアプリケーションアーキテクチャが普及し、企業がITインフラの要素として複数のクラウドプロバイダーを利用するようになると、複数の展開場所（オンプレミス、様々なクラウド、さらにはユーザーに最も近いネットワークエッジ）でZTAを管理する必要性が生じます。
「エッジ」でのコンピューティングは、ロボット工学、自律走行車、拡張現実（AR）などのコネクテッドインダストリーにとって、今後数年間でますます重要になってくる、進化し続ける検討事項です。高度に分散されたアプリケーションの世界では、最新のスタックのすべてのコンポーネントが必要になります。しかし、エッジで安全かつ透過的にユーザーに向けてコンピューティングを行うには、分散アプリケーションの「メッシュ」とそのアプリケーションのオリジン（クラウドまたはオンプレミス）の間でZTAを確立する能力など、セキュリティを強化する必要があります。このような分散型アプリケーションの概念は、「エッジ2.0」[26] と考えることができ、ローカルなテレメトリや双方向のデータ交換の要求を処理する従来のクラウドインフラの拡張が複雑になるため、より成熟したZTAの設計が必要になります。

3.5 Policy as Code (コードとしてのポリシー)

本稿の最後の技術的考察は、policy as codeの今後の意義についてです。policy as codeの目的は、様々なテクノロジー（純粋にクラウドネイティブに限らない）の間でポリシーの施行を統一することです。これは、CI/CDパイプライン内でのコンプライアンスと構成の適用を自動化し、ABACとRBACを単一の宣言型ポリシーから生成することで実現します。これにより、ZTAを成熟させようとしているハイブリッド環境やクラウド環境に最適なソリューションとなっています。

Policy as codeは、サービスのコンプライアンス検証やアクセスルールを実施する宣言型メカニズムを実装し、（企業や規制当局による）デプロイ前のチェック／テストについて、標準化された評価方法を通して、望ましい状態を定めたランタイムコントロールを適用します。これは、監査証跡を文書に残すソース管理と同じ方法でコードとして実装されるため、ZTAに含める意義のある技術アプローチです。そのため、業務上のアクセスや相互依存性のあるサービスを定義するルールを、アプリケーションおよびサービスインターフェースの厳格な要件に対してタグ付けまたはマッピングすることができます。また、クラウドネイティブなパイプライン全体で、具体的なポリシーを記述するフレームワークを提供します。

[26] Lin, G. (2021, 2月 8).*Edge 2.0 Manifesto:Redefining Edge Computing*.F5. https://www.f5.com/company/blog/edge-2-0-manifesto-redefining-edge-computing

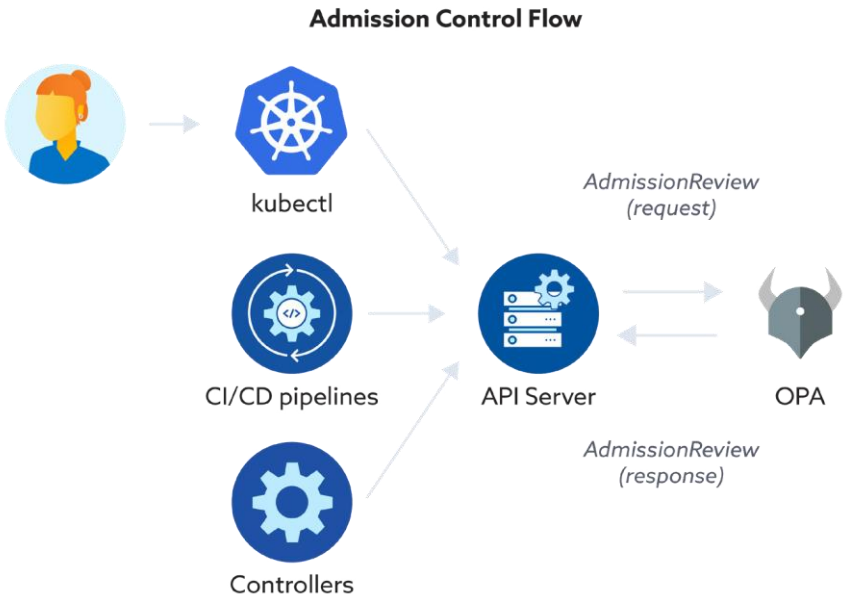

図6. OPAアドミッション・コントローラー（CNCF

Open Policy Agent（OPA）は、コードとしてのポリシーの定義と適用を支援するために、Cloud Native Computing Foundation（CNCF）[27]を通じて2018年に開始され、2021年2月に卒業したプロジェクトです。OPAは、アドミッションコントローラ、すなわちPEPとして、図6. に示すように宣言型ルールエンジンと自動化により、統合およびデプロイメントパイプラインにおいて特定の要件とチェックを実施します。

図7. OPAがサポートするZTA、OpenPolicyAgent.org

[27] Cloud Native Computing Foundation. (2021, February 4). *Cloud Native Computing Foundation Announces Open Policy Agent Graduation*. https://www.cncf.io/announcements/2021/02/04/cloud-native-computing-foundation-announces-open-policy-agent-graduation/

これは、Kubernetes、API認可、Linux PAMの各環境に統合されたライブラリまたはデーモンとして実装されています。このポリシーを実施する必要のあるアプリケーションやサービスは、APIリクエストごとにOPAに照会してPEPの決定を行います[28] 。これにより、図7.[29]に示すように、アクセスおよび構成ポリシーの一貫性を実施することで、ZTAを強化します。

3.6 Identity Aware Proxy（アイデンティティアウェアプロキシ）

コードとしてのポリシーの例として、Identity-Aware Proxy（IAP）があります。アイデンティティとコンテキストの認識は、ZTAにおけるアクセスの基本です。アイデンティティおよびコンテキストは、意図と組み合わせて、IAPの基礎でもあります。IAPは、信頼できるアイデンティティのルートを必要とし、ユーザーとそのデバイスを認証（検証）し、アクセスを許可（認可）します。これがアイデンティティを意識したアクセスです。IAPは、プロキシ・レイヤーを使用して、認証および認可された安全なアクセスを特定のリソースに提供します。このように、IAPは、企業がZTをレガシーネットワークに後付けすることを可能にし、企業のセキュリティポリシーを実施できるアプリケーションの前にインテリジェントなプロキシを置くことができます。

IAPは、アプリケーション層でのアイデンティティとアクセスに焦点を当て、ファイアウォールのルールではなく、アクセスコントロールに依存しています。設定されたポリシーには、ポートやIPアドレスではなく、ユーザーやアクセスの意図が反映されます。さらにIAPは、最小特権アクセスの原則に基づいて中央の認証層を確立し、リクエストごとにアクセスを強制することで、ZTの運用ガバナンスモデルを提供します。IAPでは、どのようなアクセスリクエストでも、終了、検査、再検査、修正、承認を行うことができます。

[28] Open Policy Agent. (n.d.). *OPA Ecosystem*. https://www.openpolicyagent.org/docs/latest/ecosystem/

[29] Open Policy Agent. (n.d.-b). *Open Policy Agent.* Retrieved September 29, 2021, from https://www.openpolicyagent.org/

4 業界への影響

このセクションでは、テクノロジー、文化、ポリシー、規制による取組といった主要な影響要因の観点から、ソリューション概況がもたらす意味合いを簡単に検討します。網羅的ではありませんが、各検討領域で業界のコラボレーションを通して、継続的に注意を払う必要がある重要な課題と機会を、業界のステークホルダーが特定するために役立ちます。

4.1 テクノロジー

豊富で多様なテクノロジーソリューションや機能が登場していることを考えると、安定したZTAへの選択肢は、複雑で、潤沢で、有望です。IT組織が、進化したこれらのソリューションをZTAの一部として取り入れるに従い、セキュリティの情勢には、従来とは異なる改善されたサイバーセキュリティへのアプローチが根本的に反映されていきます。その結果、コストカーブが変化する可能性もあります。すなわち、極めて包括的で継続的な検証が必要になることによって、攻撃者のコストを大幅に引き上げ、防御側のコストを削減できる可能性があるアプローチであるということです。ZTAの実装には初期費用がかかりますが、時間の経過とともに、他のテクノロジーは必要性が低くなり、おそらく重複するものとして完全に排除されるでしょう。ZTの標準が成熟する中で、経済やビジネスへの影響を業界の関係者が議論する必要があります。このような複雑な状況では、NISTのドラフト出版物「Planning for a Zero Trust Architecture: A Starting Guide for Administrators」[30]に見られるように、NIST Risk Management Framework（RMF）がZTAの開発と実装にどう役立つかについて、政府から継続的なガイダンスも必要です。ITおよびセキュリティの専門家が、現在利用可能な無数のZTアプローチを評価、判断、統合する方法を理解するため、追加の業界ガイダンスが依然として必要です。

例えば、SDPとSDNについては、組織の環境ごとに適切なSDPの要素を特定するという課題が残っています。例えば、SDPの境界は、データ、アプリケーション、プラットフォーム、ホストのどのレベルで制御するべきでしょうか。実際には、ハイブリッドソリューションが進化するかもしれません。このギャップを埋めるには、業界と政府がさらに協力し、環境に適した要素を選択するためのガイダンスを組織のリーダーに提供する必要があります。このような状況ですが、SDPに対する成熟度を高めることは、組織のZTAにとって不可欠です。

サービスメッシュに関しては、将来のサービスデリバリーファブリックは、さらに分散され、より細分化されるでしょう。一般的に、Kubernetesやサービスメッシュアーキテクチャはいずれも、実装コンポーネント（コンテナ、サイドカープロキシなど）に依存しませんが、今日のハイブリッド環境におけるソフトウェアおよびハードウェアコンポーネントの多様性を考慮すると、コンテナ化されたアプリケーション環境にZTAを適切に適用するには、ベストプラクティスについてある程度の業界標準が必要です。従来のハードウェアや、仮想マシンインフラ（オンプレミスまたはクラウド）で実行されるコンポーネントと、ネイティブ

[30] Rose, S. (2021, August 4). *Planning for a Zero Trust Architecture: A Starting Guide for Administrators.* NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.08042021-draft.pdf

なコンテナ環境の間に橋渡しが必要になります。業界にとっての課題は、比較的小規模なランタイムコンテナ環境（ディスクやRAMの要件など）で、ZTAの主要なコンポーネントをネイティブに常駐させることです。この開発には、CISAやサードパーティのクラウドインテグレーターによるTrusted Internet Connectionポリシー（TIC）の進化の一部として、検討やガイダンスが必要になる可能性があります。

4.2 組織文化

冒頭で述べたように、ZTの原則を業界全体で採用するには、変化への対応力が不可欠です。ビジネスとセキュリティの文化を変えるには、様々なペルソナへの理解を深める必要があります。ZTは、最初、管理者や開発者にとって威圧的に見えるかもしれませんし、彼らの仕事に必要なアクセスや能力をさらに制限するものと受け取られるかもしれません。ZTの原則を採用する利点や、環境の評価および定義したロードマップの実装に向けた動きを理解してもらうため、組織は人材やリソースを支援し、育成する必要があります。繰り返しになりますが、経営層のサポート、定義された変更管理プロセス、そして現在の予算サイクルに含まれていない可能性もありますが、ZTAの設計、評価、実装に必要な資金およびリソースの投資が必要です。

4.3 ポリシー

ポリシーの課題は、動的なクラウド環境における相互運用性と管理の問題として、引き続き残ります。ガバナンスに関する現代組織の主戦場は、可視性、コンテキスト、およびコントロールです。幸いなことに、今日のZTの原則、フレームワーク、およびアーキテクチャは、この課題に関する組織開発のガイダンスになります。まず、ZTAを実現する際、新しい役割、プロセス、およびテクノロジーを導入するため、組織全体のポリシーを改訂または開発する必要が生じる可能性があります。クラウドは組織全体で複数のテナントもサポートできるため、ポリシーに新しい課題が発生します。端的に言えば、一部のポリシーはグローバルに実装できません。さらに、アクセスポリシーとベストプラクティスの進化にともない、ポリシーロジックを保護対象のアプリケーションの外部で管理する必要がある一方、経済的な管理を実現するため、集中管理にも対応する必要があります。これまでのアプリケーション開発が、DevSecOps環境で徐々に進行する縦割りの考え方に根付いており、マルチテナント／マルチシステムを所有する環境では、考え方が複雑になります。改善され、より自動化され、効率的なポリシー管理ソリューションを、DevSecOpsプロセスの一部として開発すると、業界にとって恩恵となるでしょう。

Policy as Codeは引き続き重要性を増しており、この業界は、ソフトウェアサプライチェーン全体にZTAを実装するアプローチを開発し、採用する際、有利な立場にいる可能性があります。DevSecOpsとCI／CDパイプラインは、アプリケーションとインフラのための新しいサプライチェーンであり、コンテナ技術の活用が進んでいます。ソフトウェアサプライチェーンにおいて、CI／CDアプローチの内部および全体の実装から、ZTAを無視することはできません。最近のアプリケーションは、サードパーティーベンダーやオープンソースのコンポーネントがその一部を構成することがあり、これらは「依存関係」と呼ばれます。その結果、コンポーネントを利用する組織は、サプライヤーのサプライチェーンをほとんど把握できない可能性があり、ZTAなどの新しい枠組みを監査するためのコストが増えること

により、より多くの規制から影響を受けます。これにより、導入が遅れる可能性があります。

エッジコンピューティングにおいても、サイバーセキュリティのポリシーは、主要なOS、ネットワーク、およびクラウドサービスによって実装します。アクセス、承認、アカウンティング（AAA）の実施には、明確な説明責任が求められます。CDNやCSPなどのプロバイダーは、監査可能かつ検証可能な方法で、規制が要求するAAAを厳密に実施します。これは「責任の共有」の中核であり、エッジコンピューティング環境のZTAにおいても、説明責任モデルとして維持すべきです。この観点はベストプラクティスとして、業界から支持されています。

4.4 規制環境

セキュリティを政府当局が規制できるか定かではありませんが、政府のポリシーは、セキュリティへの関心を高め、投資の意思決定を導くことができます。最近の大統領令14028「*Improving the Nation's Cybersecurity*」[31]は、まさにこのために機能しています。しかし、政府のポリシーを確立し、サイバーセキュリティソリューションの実装に関する全体的な視点を育て、導く必要があります。アクセス、ネットワーク、およびデータにおける利用可能なセキュリティ機能を考慮せず、アプリケーションにセキュリティを組み込むことができなくなりました。ZTの原則の導入を進めるポリシーの特徴は、相互運用性と統合性です。ユーザー操作に対応するが、マシン間通信に対応していないデータフローに注目しても、長期的には不十分です。サプライチェーンにおいて技術的な縦割りを促すポリシーは、防御に穴を作るだけです。

[31] Exec. Order No. 14208, 86 FR 26633 (May 12, 2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

5 推奨事項

ZT の成熟度とロードマップのアプローチ、進化する ZT の状況、技術、文化、ポリシー、規制要因の影響などを幅広く調査することで、本稿は、ZT 採用の多様性、複雑性、初期段階のスナップショットを提供しています。多くのトピックを紹介してきましたが、このセキュリティの進化は、現在進行中の多くの業界の議論のトピックとなるでしょう。本稿の目的は業界全体のZTA導入を支援するための次のアクションを提唱し、以下の提言を行っています。

CISA ZTA能力成熟度モデル（ZTA-CMM）評価アプローチは、本書で規定されているように**採用されるべきです。**この成熟度評価を実施し、その結果をもとに、3年から5年のスケジュールで、目標とする成熟度レベルまでの具体的かつ優先度の高いZTAロードマップをどのように作成するかを利害関係者に伝える必要があります。これにより、ZTロードマップや関連する企業計画サイクルの一環として検討する必要のある必要なリソース配分や技術評価、投資についての情報が提供されることになります。組織のリーダーは、目標とする成熟度とロードマップの要件に基づいて、ロードマップの要件に「クロール・ウォーク・ラン（crawl-walk-run）」のアプローチを採用すべきです。10年経っても、ZTの技術、スキルセット、およびプロセスの革新は、すべて初期段階です。

業界と政府は、組織のロードマップ要件に最も適した**ZTソリューションを評価するための継続的なガイダンスを提供するために、今後も協力していく必要があります。**本書で既に述べたように、政府および業界の組織は、ZTの成熟度目標に最も適合するソリューションを特定するために、複雑で進化し続ける状況を探り始めたところです。これらのソリューションの多くは同時に進化し続け、評価プロセスを複雑にしています。

そのため、**主要な組織は、業界フォーラムを通じて、ソリューション評価の進捗状況を継続的に共有する必要があります。**これにより、同じような環境で機能するZTAのベストプラクティスを特定することができます。さらに、政府と産業界が継続的に協力することで、ZTAの採用を促進し、業界の標準化を進めることができます。最近では、National Cybersecurity Center of Excellence（NCCOE）が、ZTAを評価するためのラボプロジェクトを開始するなど、この取り組みが注目されています。本書で紹介したZT実装におけるRMF要件の指針となる最近の政府参考資料は、政府が業界に対応していることを示すもう一つの例です。もう一つの推奨される産業界の取り組みは、コンポーネントメーカー（ハードウェア／ソフトウェア）、システムインテグレーター、サービスプロバイダなどの豊富なエコシステムの中で、業界のステークホルダーの声を集め、まとめるためのCSA ZTワーキンググループです。

[32] National Cybersecurity Center of Excellence. (n.d.). Zero Trust Architecture. NIST NCCoE. Retrieved September 29, 2021, from https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

最後に、**ベンダーエコシステムは、ポリシーの自動化から、相互運用性、コントロール、およびコンテキストを推進するリアルテクノロジー機能まで、幅広いZTA要件に対応する能力を再評価することを**推奨します。ZTランドスケープにおける独自の役割を迅速に特定し、共有することができる透明性の高いソリューションがあれば、IT企業は早期採用者を獲得し、より安全な国家およびグローバルインフラのための能力を継続的に成熟させることができるでしょう。ソリューションプロバイダは、積極的に顧客とパートナーの関係を模索し、包括的で容易な評価サイクルを促進し、新たな効率化をサポートし、この新しい時代に消えゆくソリューションの特定を、ユーザーにとって低コストで支援する必要があります。

6 追加資料

SDNの定義： Aliyu, A. L., Aneiba, A., Patwary, M., & Bull, P. (2020).A trust management framework for Software Defined Network (SDN) controller and network applications.*Computer Networks, 181.* https://doi.org/10.1016/j.comnet.2020.107421

IaaSをベースにしたクラウドとトラスト分類学（Trust Taxonomy）の提供： Ibrahim, F. A. M., & Hemayed, E. E. (2019).Trusted Cloud Computing Architectures for infrastructure as a service: Survey and systematic literature review. *Computers & Security, 82,* 196–226. https://doi.org/10.1016/j.cose.2018.12.014

クラウドセキュリティ分類学の提供： Mthunzi, S. N., Benkhelifa, E., Bosakowski, T., Guegan, C. G.,& Barhamgi, M. (2020). Cloud computing security taxonomy: From an atomistic to a holistic view.*Future Generation Computer Systems, 107,* 620–644. https://doi.org/10.1016/j.future.2019.11.013

Ruan, Y., & Durresi, A. (2019).A trust management framework for clouds.*Computer Communications, 144,* 124-131. https://doi.org/10.1016/j.comcom.2019.05.018

Scott, B. (2018). How a zero trust approach can help to secure your AWS environment. *Network Security, 2018(3)*, 5–8. https://doi.org/10.1016/s1353-4858(18)30023-0

National Security Agency. (2021, February). *Embracing a Zero Trust Security Model.* U.S. Department of Defense. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

FedRAMP. (2017, November 15). *FedRAMP Security Assessment Framework*. https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf

National Institute of Standards and Technology. (2018, December). *NIST Special Publication 800–37 Revision 2, Risk Management Framework for Information Systems and Organizations*. NIST. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

7 参考資料

American Council for Technology-Industry Advisory Council. (2019, April 18). *Zero Trust Cybersecurity Current Trends*. https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf

Chaillan, N. (n.d.). *How did the Department of Defense move to Kubernetes and Istio?* NIST Computer Security Resource Center. Retrieved September 29, 2021, from https://csrc.nist.gov/CSRC/media/Presentations/dod-enterprise-devsecops-initiative/images-media/DoD%20Enterprise%20DevSecOps%20Initiative%20%20v2.5.pdf

ClickIT. (2021, August 5). *The most popular Kubernetes alternatives and Competitors*. https://www.clickittech.com/devops/kubernetes-alternatives/

Cloud Native Computing Foundation. (2021, February 4). *Cloud Native Computing Foundation Announces Open Policy Agent Graduation*. https://www.cncf.io/announcements/2021/02/04/cloud-native-computing-foundation-announces-open-policy-agent-graduation/

Cloud Security Alliance SPD and Zero Trust Working Group. (2020, May 27). *Software-Defined Perimeter (SDP) and Zero Trust*. Cloud Security Alliance. https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-and-zero-trust/

CMMC Information Institute. (2021, August 21). DoD/NIST SP 800–171 Basic Self Assessment Scoring Template. https://cmmcinfo.org/cmmc-info-tools/dod-nist-sp-800-171-basic-self-assessment-scoring-template/

Cybersecurity and Infrastructure Security Agency. (n.d.). *Cloud Security Technical Reference Architecture*. Retrieved September 29, 2021, from https://zerotrust.cyber.gov/cloud-security-technical-reference-architecture/

Cybersecurity and Infrastructure Security Agency, Cybersecurity Division. (2021, June). *Zero Trust Maturity Model - Pre-decisional Draft, Version 1.0*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

Exec. Order No. 13636, 78 FR 11737 (February 12, 2013). https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Exec. Order No. 14208, 86 FR 26633 (May 12, 2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Forrester. (n.d.). *The Zero Trust Security Playbook For 2021*. Retrieved September 29, 2021, from https://www.forrester.com/playbook/The+Zero+Trust+Security+Playbook+For+2020/-/E-PLA300

Gartner Research. (2018, November 9). *Fact or Fiction: Are Software-Defined Perimeters Really the Next-Generation VPNs?* https://www.gartner.com/document/3892882

Istio. (n.d.). *Istio*. Retrieved September 29, 2021, from https://istio.io/

Kindervag, J. (2010, September 17). *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*. Palo Alto Networks. https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

Lin, G. (2021, February 8). *Edge 2.0 Manifesto: Redefining Edge Computing*. F5. https://www.f5.com/company/blog/edge-2-0-manifesto-redefining-edge-computing

Microsoft. (n.d.). *Zero Trust Model - Modern Security Architecture*. Retrieved September 29, 2021, from https://www.microsoft.com/en-us/security/business/zero-trust

National Cybersecurity Center of Excellence. (n.d.). *Zero Trust Architecture*. NIST NCCoE. Retrieved September 29, 2021, from https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

National Institute of Standards and Technology. (2021, July 14). *Cybersecurity Framework | Getting Started*. NIST. https://www.nist.gov/cyberframework/getting-started

Open Policy Agent. (n.d.). *OPA Ecosystem*. https://www.openpolicyagent.org/docs/latest/ecosystem/

Open Policy Agent. (n.d.-b). *Open Policy Agent*. Retrieved September 29, 2021, from https://www.openpolicyagent.org/

Riley, S., MacDonald, N., & Orans, L. (2019, April 29). *Market Guide for Zero Trust Network Access*. Gartner. https://www.gartner.com/en/documents/3912802/market-guide-for-zero-trust-network-access

Rose, S. (2021, August 4). *Planning for a Zero Trust Architecture: A Starting Guide for Administrators.* NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.08042021-draft.pdf

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August 11). *SP 800–207, Zero Trust Architecture.* NIST. https://csrc.nist.gov/publications/detail/sp/800-207/final

Securicon Team. (2019, October 8). *NIST 800–53 Rev. 5: What it Is, and Why You Should Care.* Securicon. https://www.securicon.com/nist-800-53-rev-5-what-it-is-and-why-you-should-care/

U.S. Office of Management and Budget. (n.d.). *Federal Zero Trust Strategy.* Cybersecurity & Infrastructure Security Agency. Retrieved September 29, 2021, from https://zerotrust.cyber.gov/federal-zero-trust-strategy/

