ゼロトラスト情報セキュリティーの発展動向

ゼロトラスト情報セキュリティー市場は 17.3%の複合年間成長率で急速に成長する見込みである。米国政府は関連する制度、アーキテクチャおよび推進指針を積極的に制定し、世界各国をけん引して共に活性化させようとしている。組織によるゼロトラストアーキテクチャ導入は一度の技術更新では済まず、組織文化と情報セキュリティー／IT の部門横断協力の不足、人材不足およびガバナンス能力の不足などの問題に直面する可能性がある。技術レベルではレガシーシステムの統合、マルチクラウド／マルチサプライヤー環境の同時アクセスとポリシー実行などの難題に直面し、使用と管理上の不具合を引き起こしているため、AI に頼る必要がある。ゼロトラスト情報セキュリティー資本市場は近年持続的に活性化され、大量の資金が投入され、関連のスタートアップを IPO に向かわせる動きを強めている。関連する応用分野は広範囲にわたり多様で、各垂直分野に浸透しつつある。ゼロトラストを導入する組織は段階ごとに実行ポリシーを採用し、同時に人材と自動化監視プラットフォームに投資する必要があり、それにより転向のリスクを減らし、情報セキュリティーの価値の実現を加速する。

ゼロトラストアーキテクチャ

世界のデジタル化の波が広がるにつれ、従来のサイバーセキュリティーの防御方式ではあらゆるすきを狙うサイバー攻撃を防ぐことが徐々に難しくなっている。2010 年、John Kindervag はゼロトラストアーキテクチャ（Zero Trust Architecture，ZTA）を打ち出した。「信用できるネットワーク周辺は存在しないこと」を仮説とし、すべての接続を信用しない原則を採用し、さまざまなサイバーセキュリティー保護方法を統合し、一つ一つのアクセスを検証することで、重要資産、データ、アプリケーションプログラムおよびサービスが悪意あるものに掌握されないよう適切に保護する。

その後、さまざまなゼロトラスト計画が続々と打ち出された。例えば 2014 年に Google Cloud はゼロトラストアーキテクチャ実装を実施し、2022 年には対外的に実践の成果を説明し、ソリューションの発表に努力を重ねた。クラウドセキュリティーアライアンス（Cloud Security Alliance）は 2014 年と 2019 年にそれぞれ Software Defined Perimeter（SDP）1.0 と 2.0 のアーキテクチャガイドラインを発表し、企業によるゼロトラストネットワーク設置を支援し

た。

需要の増加により、米国国立標準技術研究所（NIST）も 2020 年 8 月にゼロトラストアーキテクチャのガイドライン SP 800-207 を発表し、すべての組織が現行の情報セキュリティー防御アーキテクチャをゼロトラストアーキテクチャに転換することを促したことは図 1 に示した通りである。これはより多くの組織に転換を促し、多くの情報セキュリティー業者もこのアーキテクチャを参考にしてソリューションを発展させた。当該文書はゼロトラストの 7 原則を略述している。

1. すべてのデータソースとコンピューティングサービスはリソースとみなす。
2. ネットワークの場所に関係なく、すべての通信を保護する。
3. 単一企業のリソースへのアクセスはセッション単位で付与する。
4. リソースへのアクセスは動的ポリシーにより決定する。
5. 企業はすべての自己資産および関連資産の整合性と安全性を監視、測定する。
6. すべてのリソースの ID 認証と権限付与は動的に行われ、アクセスが許可される前に厳格に実施する。
7. 企業は関連資産、ネットワークインフラおよび通信の現状の情報を可能な限り収集し、それらの情報を利用してそのセキュリティー体制を改善する。

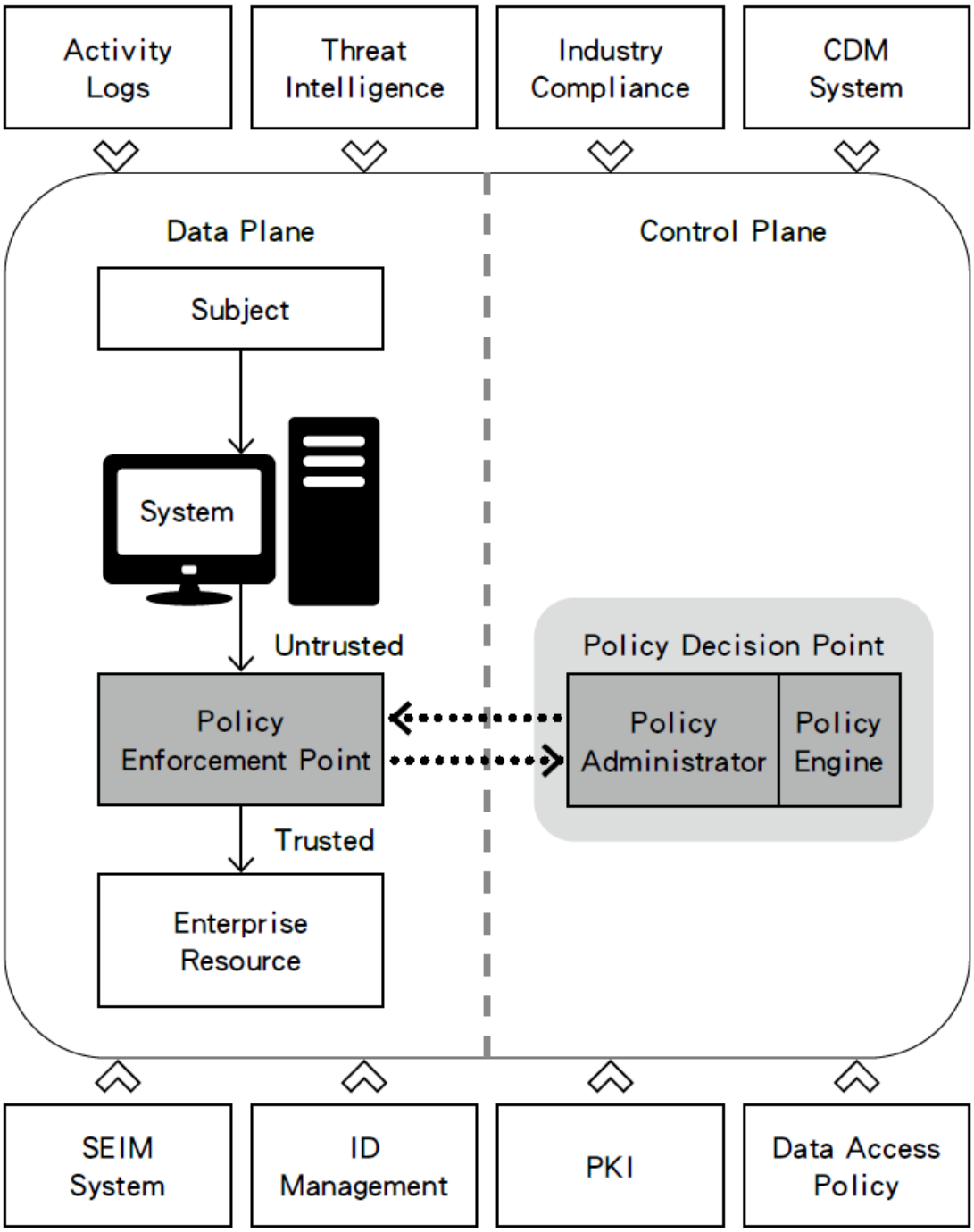

図 1　Core Zero Trust Logical Components
鋭企作成、出典：米国国立標準技術研究所

また、世界の地政学的な緊張と対立の高まりに伴い、政府の政策面における進歩は米国行政管理予算局（OMB）が 2022 年 1 月 26 日に新サイバーセキュリティーポリシーおよび M-22-09 覚書を正式に発表し、政府機関にゼロトラストアーキテクチャを実施することを求めたことからわかる。各機関は覚

書発表後 30 日以内にゼロトラスト戦略実施責任者を指定し、2024 年までに 5 項目の情報セキュリティー標準要件を満たさなければならない。ペンタゴンは 5 年以内にすべてのネットワークをゼロトラストアーキテクチャに転換することを計画している。今後ゼロトラストアーキテクチャの転換ニーズは必ずや情報セキュリティー分野の主流に躍進することが予想される。

2024 年、John Kindervag はゼロトラストの実施を 5 つの段階に分けられると説明した。Define the protect surface → Map the transaction flows → Architect a Zero Trust Environment → Create Zero Trust policy → Monitor and maintain であり、簡略化したセキュリティーフローで組織のシステムの反脆弱性（Antifragile）を確保し、情報セキュリティーが課題に直面した時の強じんさを高める。

ゼロトラスト情報セキュリティー市場の現状

リサーチ会社 Claight の報告によると、2024 年、世界のゼロトラスト情報セキュリティーの市場規模は約 316.3 億米ドルであった。今後 10 年間、市場は 17.30%の複合年間成長率で持続的に成長し、2034 年までに市場規模は 1,559.8 億米ドル前後に達する見込みである。米国はこの市場の主な推進者であり、北米市場はゼロトラスト関連産業の発展においてかなり大きなシェアを占めている。その主な原因は米国政府と公共部門のこの分野における支出が大幅に増加したこと、政策制定と産業規範を通じて日々厳格になるデータのプライバシーおよびセキュリティー標準と政策を持続的に発表したこと、またモノのインターネット（IoT）、人工知能（AI）およびデジタル技術の普及より中小企業と大企業関連の情報セキュリティーのニーズが増大したことである。それらすべてが当該地域の市場の成長を著しく促進したこと。その他の地域の主要国家も同調し続け、さまざまな組織がゼロトラストセキュリティー実施計画のソリューションに対するニーズを増加させ続け、市場全体の成長を著しく促進する見込みである。

各国のゼロトラスト推進の現状

ゼロトラストアーキテクチャは早期の概念研究から実務配置の段階に入り、米国、EU、英国、日本、韓国、オーストラリア、シンガポールなどの国が続々とゼロトラストアーキテクチャ推進政策を制定した。推進過程において、ゼロトラストアーキテクチャの導入は従来の既存の情報セキュリティーモデルと合わせて運用する必要があり、運転しながら車を改造するようなも

のである。推進時、全体のフローが 1 度の技術更新では済まないことに留意し、導入過程全体においてシステムが持続的に運用でき、情報セキュリティーの空白期間や新たな抜け穴が発生しないことを確実に保証する必要がある。次に、各国の推進方法の特徴を概説する。

米国は政策側において OMB / White House の M-22-09 をマイルストーンとし、連邦機関にゼロリスク原則を採用するよう求め、DoD および多くの連邦機関が専属ポリシーと成熟度モデルを制定した。サイバーセキュリティー・インフラセキュリティー庁（CISA）および NIST は実装と成熟度ツールを提供することで配置を支援した。2023 年 4 月、CISA はゼロトラスト成熟度モデル 2.0 バージョンを発表した。5 つの異なる支柱で漸進型実施プロセスを際立たせ、時間の推移と共に徐々に最適化することができる。この 5 つの支柱は ID（Identity）、デバイス（Devices）、ネットワーク（Networks）、アプリケーションおよびワークロード（Applications and Workloads）、データ（Data）である。各支柱は次の分野横断機能の共通点を含む。可視性および分析（Visibility and Analytics）、自動化および編成（Automation and Orchestration）、ガバナンス（Governance）である。CISA も各段階の指導標準を表 1 の通り提供し、各機関が各ゼロトラストの技術的支柱の成熟度を認識することで、成熟度モデルの整合性を確実に保証する。

表 1　ゼロトラスト成熟度の発展過程（Zero Trust Maturity Journey）

段階	中核となる特徴
従来の段階 **Traditional**	● ライフサイクルを手動で設定（確立→変更→停止） ● ID の属性、アクセス制限、ログの属性はすべて人が設定 ● セキュリティーポリシーは「静的」、多くが個別システムから独立して管理される ● 最小権限はアカウント構築時に 1 回設定し、その後の調整はない ● 情報セキュリティー技術と防御措置は「各自で行い」、多くの陣営が存在する ● インシデントの対応は人手によるフローに頼る ● ログ／遠隔測定（telemetry）はシステムを横断した関連分析を行うことができない 典型的な状態 ● 依然として従来のエッジ型情報セキュリティーを主とし、動的

	調整能力に欠ける ● 段階の特徴：低自動化、低協力、低可視性
初期段階 **Initial**	● コンポーネントの属性（ID、デバイスの健全度など）の「一部自動化設定」が始まる ● 初期に技術分野（pillars）横断統合方法を確立 ● アクセス制限は最小権限の原則における「制限付き調整を行う」 ● 外部システムと一部統合可能（IDaaS、情報セキュリティー監視など） ● 一部の情報セキュリティーインシデントに対し初期対応を行う ● 内部システムが「統合型の可視性」を具備し始める 典型的な状態 ● ZTNA、IAM、自動化政策などの導入を開始するがすべてを網羅していない ● 段階の特色：自動化、統合を開始、ただし依然として限定的
発展段階 **Advanced**	● ライフサイクルと属性の設定（ID、デバイス、リスク、ポリシー）の高度自動化 ● Zero Trust の五大支柱横断協力：ID、デバイス、ネットワーク、アプリケーションおよびデータ ● 「集中型視角管理と ID 制御」を実現 ● ポリシーとアクセス制限は支柱横断で一致して実行可能 ● 予定の緩和措置（アカウント封鎖、権限低下など）を自動実行可能 ● 最小権限をリスクレベル、ポスチャー（posture）に基づき 動的調整可能 ● 外部リソース、クラウド、マルチクラウド環境を含む企業範囲統合を目指す 典型的な状態 ● 成熟したポスチャー管理、XDR、動的ポリシー、プラットフォーム横断協力を具備 ● 段階の特色：高度自動化、集中ガバナンス、リスクガイド
最適化 **Optimal**	● ライフサイクルの全面自動化（Just-in-Time / Just-enough access） ● 全ての資産、デバイスおよび ID が「自己報告」可能な状態にあり、ポリシーを自動駆動できる ● 動的ポリシーはインシデント、アクション、リスクの検出に基

	づき自動で変動 ● 全企業一致（Enterprise-wide）の機微度およびインシデント検出能力 ● ロール、アクション、リスクに基づき動的に最小権限（JEA/JIT）を自動提供 ● 各支柱がすべてインタラクティブで「継続的な動的全域監視」を達成 ● 「完全なコンテキストアウェアネス」および環境（クラウド／外部とサプライチェーンを含む）横断防御能力 典型的な状態 ● ゼロトラストは企業運営、ポリシー、アーキテクチャに完全に浸透 ● 段階の特色：全自動化、全動的、全支柱横断、全範囲可視化

鋭企作成、出典：米国国土安全省サイバーセキュリティー・インフラセキュリティー庁

EU は一般データ保護規制（GDPR）の大きな枠組みの下、データの最小化および国境横断コンプライアンスを強調している。英国もゼロトラストを個別の構成国との重要インフラ防御要件に組み込んでいる。

アジア太平洋諸国は重要インフラを優先推進対象とし、日本とシンガポールは専門指導と試行を発表し、オーストラリアもゼロトラストとスマート国家防御を情報セキュリティー重要プロジェクトとしている。

韓国政府はゼロトラスト六大応用状態を打ち出した。企業のリモートアクセス、サードパーティ協力、組織内ネットワーク／インターネット隔離、組織内デプロイおよびクラウド統合、OT/ICS 産業制御、M2M/モノのインターネットであり、それぞれ推進目標、要件および実践の重点を立案し、産業界の導入時の参考に供する。

台湾のゼロトラスト推進状況

台湾政府は 2021 年 2 月、「第 6 回国家サイバーセキュリティー発展計画」を公布し、政府組織のゼロトラストアーキテクチャ導入を始動させた。2022 年 7 月、サイバーセキュリティー責任等級 A 級の機関のゼロトラストアーキテクチャ導入を優先的に推進することを確定し、同時に台湾国内のメーカー

がゼロトラスト情報セキュリティー産業チェーンを発展させることを推進した。関連業務は新たに成立したデジタル発展部傘下のサイバーセキュリティー署が政策計画を策定し、リソースを投入している。

そのほか、デジタル発展部は傘下の国家サイバーセキュリティー研究院の指導の下、デジタル政府司やサイバーセキュリティー署と協力して政府の情報セキュリティーの強じんさを定期的にチェックする。

政府は米国の NIST 関連文書を参考にし、「使用者の ID、使用デバイス、アクション」をデータアクセスとアプリケーションの管理の依拠とし、「ID 識別、デバイス識別、信用推定」の 3 つの中核メカニズムに対応する。2023 年、デジタル発展部は 22 の情報セキュリティーA 級機関が ID 識別を導入し、デバイス識別と信用推定メカニズムを続けて導入することを優先的に指導した。

ゼロトラスト推進時に直面する課題

ゼロトラストメカニズムは使用と管理において不具合を引き起こすことがある。例えば、組織と運営レベルにおいては組織文化と情報セキュリティー／IT の部門横断協力の不足、人材不足およびガバナンス能力の不足などに直面することがある。技術レベルではレガシーシステムの統合（OT/ICS と医療システムは典型的な難題）、マルチクラウド／マルチサプライヤー環境の同時アクセスとポリシー実行などの難題に直面することがある。

ソリューションの発展動向

今後、AI に頼って識別と管理を行い、AI を隠れたゲートキーパーとして運用しなければ、メカニズムが引き起こす不具合を効果的に減少させることはできない。サイクラフト（CyCraft Technology）は台湾の AI 情報セキュリティー技術に焦点を当てたスタートアップ企業であり、同社は 2023 台湾情報セキュリティー総会において次のように表明した。情報セキュリティー業者は政府が徐々に厳格化する法規を遵守するだけでなく、より短時間で検出→調査→処置を完了させなければならない。引き続きこれまでの方法に頼っていれば、品質の防御を犠牲にし、防御目標を達成できないため、AI などの自動化科学技術導入は必ず行わなければならず、特にインシデント発生前の検出と発生中の調査段階において支援を最大限おこなわなければならない。今後、情報セキュリティー人材は不可欠のパートナーとなる。

ゼロトラスト情報セキュリティー市場の近況

情報セキュリティー資本市場は 2024 年から 2025 年まで持続的に活性化し、SASE／ZTNA／ゼロトラスト関連メーカー Netskope、Zscaler、Palo Alto のクラウド製品は大量の資金と IPO の原動力を引き寄せている。最近資金を調達したゼロトラスト情報セキュリティースタートアップ企業数社を次の通り列挙する。

表 2　ゼロトラスト情報セキュリティースタートアップ企業の資金調達の近況

企業	主要業務／ポジション	**資金調達状況／近況**
Elisity	ID 中心（identity-centric）マイクロセグメンテーション ＋ ゼロトラストアクセス制限（IT＋OT / IoT 環境対象）	2024 年 4 月に 4,500 万米ドルのシリーズ B 資金を調達。
TXOne Networks	産業／OT／重要インフラ（ICS/SCADA）のゼロトラスト／OT セキュリティーソリューションに特化	2024 年 5 月 5,100 万米ドルのシリーズ B エクステンションラウンド資金調達完了。
NetBird	オープンソース／SNS 誘導の Zero-Trust ネットワーク overlay ソリューション	2024 年 12 月にシード資金 400 万ユーロを獲得。
Hypori	ゼロトラスト BYOD／バーチャルワークプレイス（virtual workspace）プラットフォーム提供	2025 年 1 月にシリーズ B エクステンション（1,200 万米ドル）完了。
Portnox	クラウドネイティブのアクセス管理／ネットワークアクセス制限（従来の NAC に取って代わる）	2025 年 4 月に 3,750 万米ドルのシリーズ B を取得。
Zero Networks	agentless、自動化 micro-segmentation／ゼロトラストネットワークアクセス（ZTNA）プラットフォーム提供	2025 年 6 月に 5,500 万米ドルのシリーズ C 融資を獲得。
Noma Security	ゼロトラスト ＋ データ／AI-モデルセキュリティー（AI agent、クラウド環境の威脅対象）	2025 年 7 月に私募ファンド 1 億米ドル（Series B）を発表し、累計 1.32 億米ドル達成。

鋭企作成、出典：Crunchbase

ゼロトラスト情報セキュリティーの商機

現在、ゼロトラスト情報セキュリティーは金融業を含む主要産業の応用の機会において ID と取引保護、詐欺防止を網羅している。エネルギー／公益事業は OT／ICS のネットワークセグメンテーションとプロセス保護を網羅している。通信業は地域横断認証とエッジセキュリティーサービスを網羅している。Managed Zero Trust／MSSP はゼロトラスト管理代行サービスを提供している。

上記の近年資金調達したゼロトラスト情報セキュリティースタートアップ企業の分析を通じて、次の発展動向がわかる。情報セキュリティー分野のスタートアップのグループに投資するならば、関連する商機に留意することができる。

1. 多様化した応用シナリオ：企業の IT／クラウド、ハイブリッド／マルチクラウド環境から産業 OT／ICS、IoT／エッジデバイス（TXOne 等）、BYOD、AI-agent／クラウドサービスセキュリティー（Noma Security 等）――ゼロトラストは単純な VPN に取って代わられることはなく、IT、OT、Cloud／AI／ハイブリッド環境の全面防御を貫徹することが明らかである。
2. 資金流入の力強さ：多くの企業が 2024 年から 2025 年に シリーズ B／C 資金の獲得に成功し、金額は数千万から 1 億米ドル以上まで一様ではなく、市場と投資家のゼロトラストセキュリティーソリューションに対する需要は徐々に高まっていることを示している。
3. 新技術／新モデル：一部のベンチャー企業は従来の ZTNA／マイクロセグメンテーションだけでなく、identity-first、セキュリティークラウド workspace、AI／モデル保護、agentless micro-segmentation、産業制御システム（OT）のゼロトラストの統合に焦点を当て、技術と応用レベルの刷新を展開している。
4. 市場が網羅する面の拡張：企業／クラウドから産業、OT、IoT、AI などまで、今後ゼロトラスト市場は企業 IT だけでなく、運営技術（OT）、産業マニュファクチュアリング、クラウドサービスサプライヤー、AI 研究開発機関などの多くの分野を含むことを意味し、情報セキュリティーメーカー、サービスプロバイダーは広範囲に機会があ

る。

結論

ゼロトラストアーキテクチャは政策駆動から商業化に向かいつつある。政府と企業は段階ごとに（Identity → Device → Network → Applications and Workloads → Data）実行ポリシーを採用し、同時に人材と自動監視プラットフォームに投資することでリスク転換および情報セキュリティー価値の実現を加速することを提言する。

出典

• 【ゼロトラスト理解、NIST SP 800-207 理解より着手】ゼロトラスト原則の企業のサイバーセキュリティー環境を創出。iThome, 2021

• 【台湾企業はゼロトラストに対する認識を強化すべし】ゼロトラスト時代を迎える！資産点検とデータフローから着手。iThome, 2021

• 【台湾情報セキュリティー総会を直撃】サイバーセキュリティー研究院：政府がゼロトラストアーキテクチャを推進、今年 A 級機関が ID 識別を導入、2 機関が信用推定メカニズムを先行導入。iThome, 2024

•ゼロトラストアーキテクチャ導入の 5 段階：内から外へのセキュリティーポリシー。iThome, 2024

•Zero Trust Architecture. National Institute of Standards and Technology (2020)

•Zero Trust Maturity Model. Cybersecurity and Infrastructure Security Agency (2023)

•Zero Trust Security Market Size, Share, Growth Analysis Report and Forecast Trends (2025-2034). Expert market research (2025)