（参考）ゼロトラストアーキテクチャのソリューション例

参考資料２

「ゼロトラストアーキテクチャ適用方針(令和4年6月30日)」におけるゼロトラストアーキテクチャの6つ適用方針に対応したゼロトラストアーキテクチャ機能のマッピングを下記の通り実施した。

No	適用方針	内容	機能	機能概要
1	リソースを識別し、特定できる状態にする。	リソースを正確に特定できる状態でなければ、アクセス制御ポリシーの評価対象とすることはできないため、リソースが識別できる状態で登録されていることが重要である。	EMM(MDM)	スマートフォンやタブレット等のモバイル端末を総合的に管理するツール。
2	主体の身元確認・当人認証を実施する	利用者および端末などの物理的な主体は、システムを利用する際にはデジタルなリソースとして活動しなければならないため、身元確認及び当人認証によって確認しなければならない。	IAM (認証機能)	パスワード認証、セキュリティトークンによる認証、生体認証等、一般的な認証方式にて身元確認・当人認証が可能。
3	ネットワークを保護する	ゼロトラストアーキテクチャは、イントラネットを含めたネットワークを暗黙的に安全であるという前提を信用しないため、ネットワークは通信経路の適切な暗号化によって安全性を確保しなければならない。	FWaaS	クラウドサービスとして提供されるファイアウォール機能のこと。FWaaSはリモートやモバイルなど物理的な拠点外からの通信、契約したクラウドサービスと外部との通信、私物持ち込み端末（BYOD）など、ありとあらゆる場所や形態の通信を同じセキュリティ設定に基づいて保護することができる。
			SWG	外部への WEB アクセス等を安全に行うためのクラウド型プロキシのことで、アクセス先の URLやIPアドレスから安全性を確認・評価し、安全でないと評価された場合はアクセスを遮断する。
			SD-WAN	拠点間やクラウドとのネットワークをソフトウェアで制御する機能で、柔軟なネットワーク構成やトラフィックコントロールなどを実現する。
4	リソースの状態を確認する	適切に運用・保守されなければ、時間の経過とともに脆弱性が増えるもしくは、設定ミス・構成の不備により脆弱性が生まれることも考えられるため、各種リソースの状態や構成が安全か確認する必要がある。	EPP	エンドポイント（パソコン・サーバ・スマートデバイス等）の監視を行い，マルウェアやランサムウェアなどの侵入を防止する。
			EDR	エンドポイント（パソコン・サーバ・スマートデバイス等）の操作や動作の監視を行い，サイバー攻撃を受けたことを発見し次第対処する。
			CASB	複数のSaaSの利用状況が可視化でき、ツールや機能のアクセス制御、データごとの持ち出し制御、コンプライアンス違反の監視、マルウェアなどの脅威検知などが実現できる。
			CSPM	パブリッククラウド（IaaS,PaaS）に対して、セキュアな設定がなされていることを継続的に評価し、適切な設定への修正を支援する。
			CWPP	クラウドサービス上のサーバや仮想マシン、動作しているソフトウェアといったワークロードに対して監視と保護のセキュリティソリューションを指す。
5	アクセス制御ポリシーで評価し、アクセス管理をする	各種リソース同士でアクセスを確立する際に、その可否を事前に定めたアクセス制御ポリシーを基にアクセス制御管理機能が評価し、その結果を施行できるようにしなければならない。	IAM(IDaaS)	アプリケーションやクラウドサービスなど、利用するシステムごとに設定された複数のIDを統合管理し、同時にアクセス権限の適切な管理を行う。
			SDP	アクセスの境界線（Perimeter）をソフトウェア上で構築，集中的に制御し、アクセス制御に関わる設定を柔軟に動的に変更することにより安全にデータを転送する。
6	リソースとアクセスを観測する	運用・保守をし、システムの信頼性を高めるうえで、リソースとアクセスのログの取得、アラートの通知など、政府情報システムを観測することが重要である。	SOC	サイバー攻撃の検知や分析を行い、その対策を講じることなどを専門とする組織のこと。 各種セキュリティ装置やネットワーク機器、サーバーの監視やログの分析、サイバー攻撃を受けた場合の影響範囲の特定、サイバー攻撃を阻止するためのセキュリティ対策の立案などを行う。
			SOAR	脅威と脆弱性の管理、セキュリティ運用の自動化、セキュリティ・インシデント対応を行うサービスのこと。
			SIEM	エンタープライズシステムやその他のセキュリティツールと連動して企業全体のセキュリティログとイベントをすべて収集し、これらのイベントを分析してセキュリティチーム向けのアラートを生成する。

※上記マッピングは整理の一例であり、今後の検討においてゼロトラストアーキテクチャ機能について詳細な調査・検討を行う。