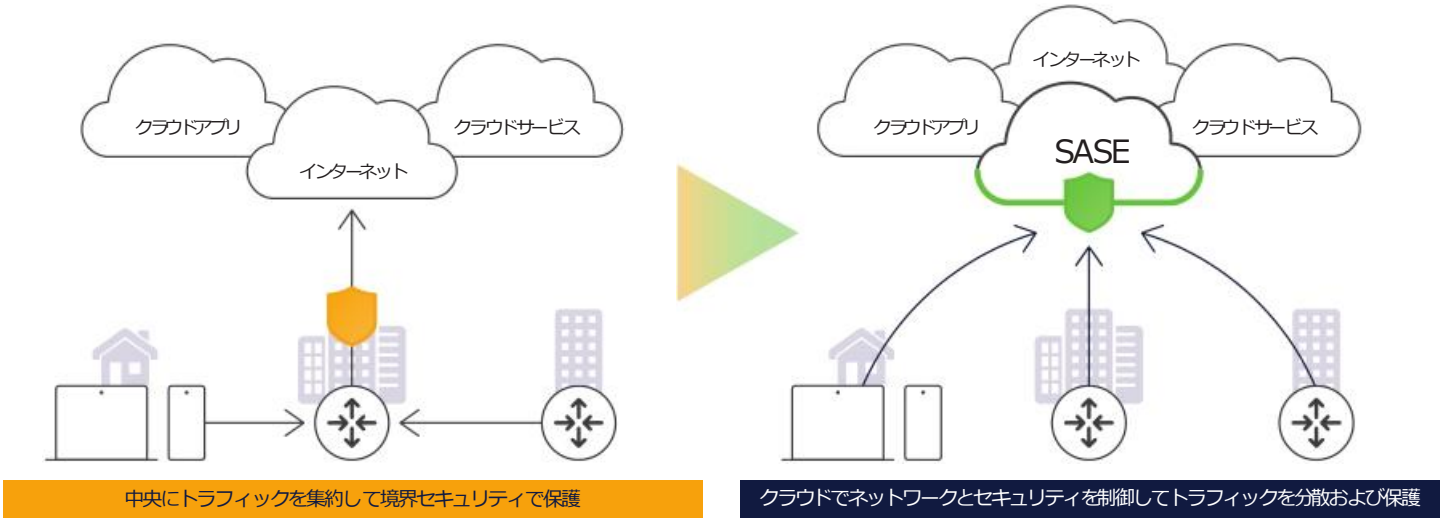
教育版ゼロトラストを実現する Cisco SASE ソリューション

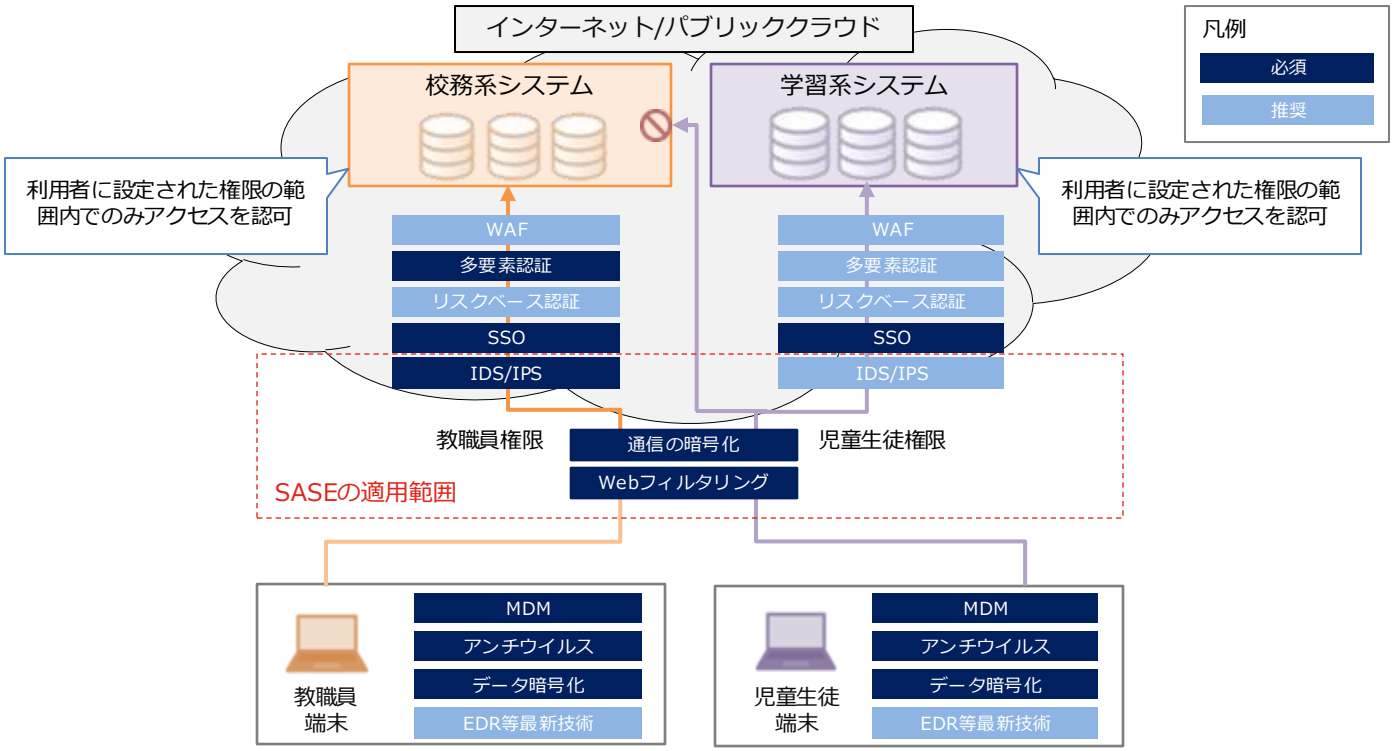
SASEとは

SASE（Secure Access Service Edge）とは、Gartner 社が「包括的な WAN 機能と包括的なネットワークセキュリティ機能を組み合わせた新しいサービス」と定義したセキュリティフレームワークです。社内外を出入りするユーザー（テレワーカー）やモバイルデバイスの増加、コワーキングスペースやタッチダウンオフィスなどの新しいオフィス環境、Microsoft 365 などのクラウドサービスの利用拡大など、新しい働き方や IT 環境に対応するために提唱されました。SASE を実現するためのインフラ構成としては、本社やデータセンターにトラフィックを集約して境界セキュリティで保護する従来のアーキテクチャから、クラウドでネットワークとセキュリティを制御してトラフィックを集約せずに分散させたまま保護するアーキテクチャへとシフトすることが基本になります。



教育版ゼロトラストにおけるSASEの適用範囲

文部科学省より要素技術の構成例として以下のように例示されていますが、インターネットに向かう通信は Web 閲覧以外にもさまざまあるため、Web フィルタリングだけでなく DNS セキュリティやクラウドファイアウォールで包括的に防御する仕組みも重要です。
加えて、クラウド利活用の一層の推進に向け、CASB によるテナントコントロールや DLP による情報漏洩対策も併せて検討することを必要です。



参考：文部科学省（2023 年 2月発行）【資料2-1】GIGAスクール構想の下での校務の情報化について(最終まとめ)【案】より
https://www.mext.go.jp/kaigisiryo/content/20230224-mxt_jogai02-000027674_22.pdf

Cisco Secure Access

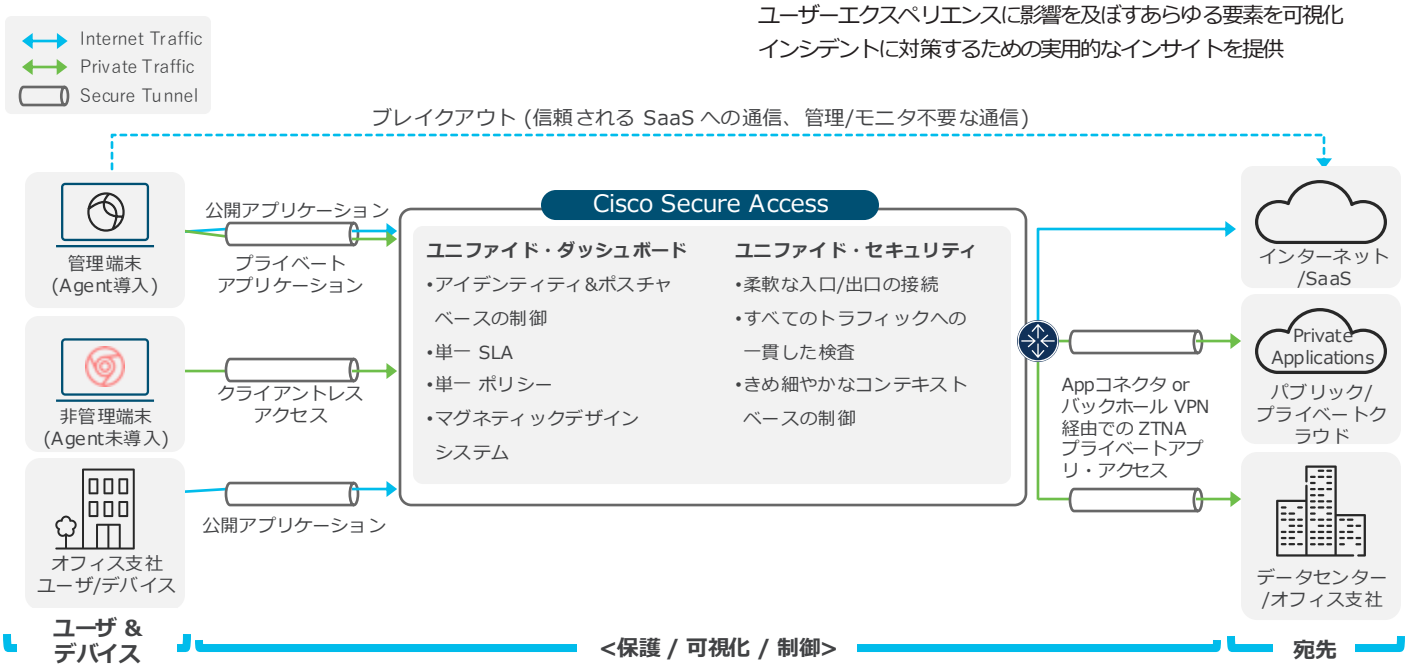
SASEの中核となるCisco Secure Access

Gartner 社は、ユーザーエクスペリエンスを損なわずに提供すべき SASE のコア機能として次の機能を挙げていますが、そのほとんどが **Cisco Secure Access** に含まれる機能です。

- ✓ DNSセキュリティ
- ✓セキュア Web ゲートウェイ（SWG）
- ✓クラウドアクセスセキュリティ制御（CASB）
- ✓クラウド提供型ファイアウォール（CDFW、FWaaS）
- ✓機密データとマルウェアの検知
- ✓リモートブラウザ分離
- ✓ゼロトラスト ネットワーク アクセス（ZTNA）

その他の機能も Cisco SASE を構成する次のコンポーネントで提供可能。

- **Cisco SD-WAN**
  あらゆるアプリやサービスへの接続を最適化
  ローカルブレイクアウトを容易に実現
- **Cisco Secure Client**
  リモートアクセス VPN クライアントをベースとした
  シスコ セキュリティの統合エンドポイントエージェント
- **Cisco Duo**
  多要素認証でゼロトラスト ネットワーク アクセスを実現
- **Cisco ThousandEyes**
  ユーザーエクスペリエンスに影響を及ぼすあらゆる要素を可視化
  インシデントに対策するための実用的なインサイトを提供



パッケージ詳細

カテゴリ	機能	Essentials	Advantage
セキュアな アクセス	セキュアインターネット アクセス (SIA) • SD-WAN DIA • ローミングセキュリティ • DNSセキュリティ、SWG、FWaaSなど Secure Internet Access (SIA)	✓	✓
	セキュアプライベート アクセス (SPA) • クライアントベースの ZTNA • クライアントレス ZTNA • 安全なリモートアクセス（VPNaaS、AutoVPN） Secure Private Access (SPA)	✓	✓
基本 セキュリティ	Web アプリおよびプライベートアプリのレイヤ 3 およびレイヤ 4 を制御するクラウド提供型ファイアウォール	✓	✓
	セキュア Web ゲートウェイ（プロキシ Web トラフィック、URL フィルタリング、コンテンツフィルタリング、高度なアプリ制御）	✓	✓
	CASB - クラウドアプリの検出、リスクスコアリング、ブロック、クラウドマルウェアの検出、テナント制御	✓	✓
	リモートブラウザ分離（Risky）	✓	✓
	安全なマルウェア分析（サンドボックス）	制限付き	無制限
高度な セキュリティ	クラウド提供型のレイヤ 7 ファイアウォール		✓
	IPS による保護		✓
	Web アプリケーションのデータ損失防止（DLP）		✓
	リモートブラウザ分離（ALL）		✓
サポート	電子メールと電話による 24 時間年中無休のシスコサポートへのアクセス	✓	✓