米国防総省のネットワークSaaS トランスフォーメーション

情報セキュリティを変革させた
米国防総省（DoD）の取り組み

zscaler™

背景

9.11以降、米国防総省（DoD）はサイロ化した連邦機関のネットワークが、機関間や世界中のミッションパートナーとの重要な情報の共有を妨げていることを把握しました。また、各機関が独自のネットワークやセキュリティアーキテクチャを構築、設計し続けたことでサイロ化がさらに進み、その結果、多くの重複する作業が発生し、設計全体のコストが増加の一途をたどることになりました。こうした非効率を回避するために、DoDは2012年12月に、統合情報環境（JIE：Joint Information Environment）フレームワークを開発しました。JIEは、DoDの各機関が情報テクノロジネットワークを変革するための統一された方法を構築することを目的とし、連邦機関とミッションパートナー間の安全な情報の共有、余剰人員やインフラストラクチャの継続的な支出の削減を実現しました。

「JIEは、共通化された基準と構成で構築された連合ネットワークを持ち、シンクライアント、Everything over IP、電子メール、クラウドサービスなどの共有ITインフラやエンタープライズサービスの利用を拡大する予定です。これらのサービスは、JIEのそれぞれの部分を運用して維持するとともに、共通のIT移行サービスやアプリケーションを取り入れつつ、ミッション独自の機能も提供されるようになるでしょう」

- 元国防総省最高情報責任者のTeri Takai氏（統合情報環境実現のための国防総省戦略、2013年）

JIEは野心的な目標であり、DoDに必要な進化でもありました。JIEは、公式のプログラムではなく、エンドユーザの要求から生まれ発展し、15個の星のメモにまとめられました。国防総省の最高レベルの司令部と第四階級のコミュニティがこの要求を合意し、1つのフレームワークが形成されました。このフレームワークで最も困難だった2つの技術的な課題が、**シングルセキュリティアーキテクチャ**と**クラウドコンピューティング**でした。

シングルセキュリティアーキテクチャ（SSA）

DoDの当初のJIE実装戦略には、以下のSSAの目標と利点が盛り込まれていました。

- ネットワークセキュリティの境界を破壊する
- DoDの外部の攻撃対象領域を削減する
- 管理、運用、技術的なセキュリティコントロールを標準化する

DoDは、NSA（国家安全保障局）、DISA（国防情報システム局）、DoDを構成する各機関のテクノロジや運用に関する専門知識を活用して、DoDIN（国防総省情報ネットワーク）の最適な場所に配備する標準化セキュリティスイートの設計、認証、認定を継続しています。

「最も重要な利点は積極的な防衛力であり、DoDのネットワークをサイバー防衛作戦の実行に必要な時間内に防御できることです。つまり、単一のセキュリティアーキテクチャによって、グローバルのサイバー環境の把握を現状では不可能なレベルにまで引き上げ、DoDネットワーク全体で何が起きているかを理解できるようになることです」

- DISAの元最高情報保証責任者のMark Orndorff氏（Slabodkin、2013年）

SSAの最も重要な2つのコンポーネントは、**統合地域セキュリティスタック（JRSS：Joint Regional Security Stack）**と**インターネットアクセスポイント**です。

統合地域セキュリティスタック

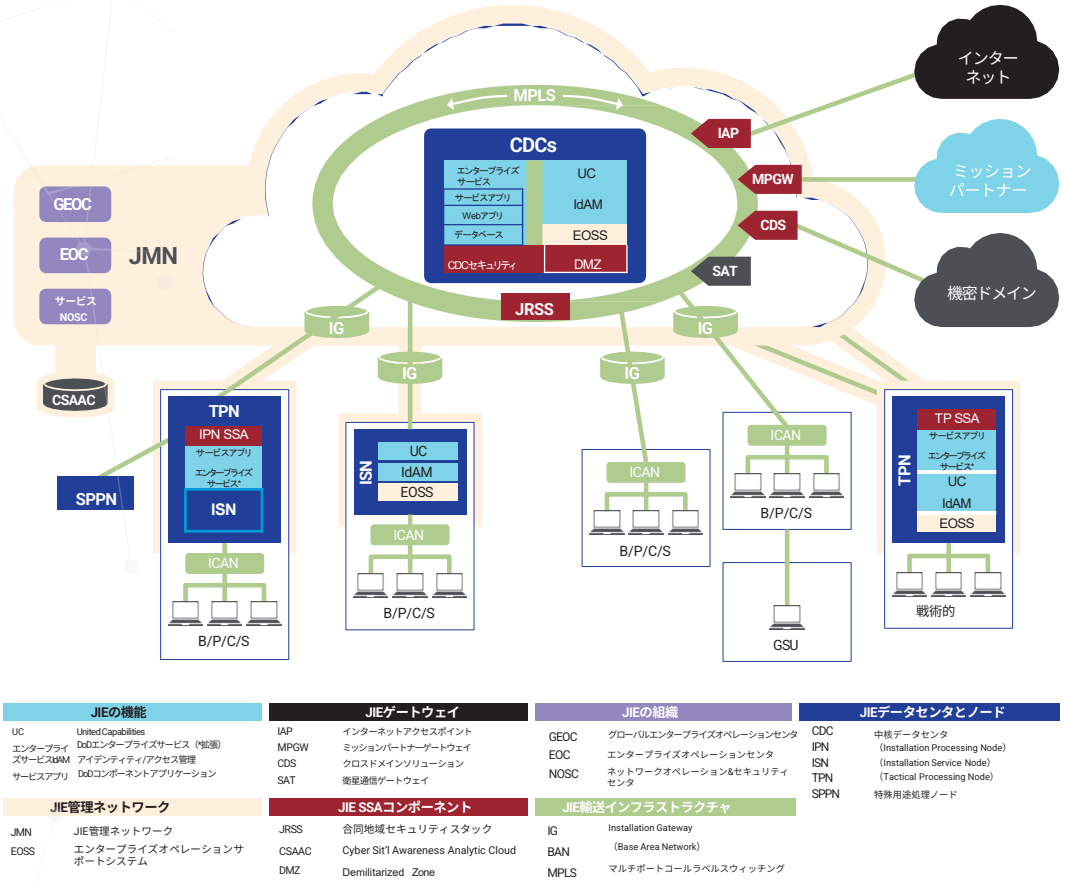
統合地域セキュリティスタック（JRSS：Joint Regional Security Stacks）戦略は、エンタープライズネットワークを保護するJIE SSAネットワークセキュリティスタックの出発点として、境界セキュリティをB/P/C/S（Base（基地）/Post（駐屯地）/Camp（キャンプ）/Station（ステーション））やICAN（Installation Campus Area Network）のテナントコミュニティに提供することになります。JIE STIGの概要によると、「JRSS（統合地域セキュリティスタック）は、IA（情報アシュアランス）の機能、スイッチ、ルーターの完全冗長化セットとして、複数のローカルのB/P/C/SとIPN（Installation Processing Node）のセキュリティスタックを単一の物理JRSSインスタンスに置き換え、地域拠点のネットワークセキュリティと可視性を提供し、CYBERCOMビジョンの実現に貢献します」（Team、2016年）

現在、米国本土（CONUS）に11か所、米国本土以外の場所（OCONUS）に11か所の計22か所にJRSSの冗長化サイトが存在します。

インターネットアクセスポイント

JIEの境界防御は、DoDINからインターネットへの安全なゲートウェイの役割を果たすセキュリティスタックであるインターネットアクセスポイントから開始します。IAPはさらに、インターネットからDoDINのNIPRNet（Non-Secure IP Router Network）への承認された接続も可能にし、エンタープライズEメールセキュリティゲートウェイ、侵入検知、ファイアウォール、アクセス制御などのエンタープライズセキュリティ機能を提供します。

JIEフレームワークの全体像は、以下の図1のとおりです。



JIEの機能

UC	United Capabilities
エンタープライズサービスIdAM	DoDエンタープライズサービス（仮設） アイデンティティ/アクセス管理
サービスアプリ	DoDコンポーネントアプリケーション

JIEゲートウェイ

IAP	インターネットアクセスポイント
MPGW	ミッションパートナーゲートウェイ
CDS	クロスドメインソリューション
SAT	衛星通信ゲートウェイ

JIEの組織

GEOC	グローバルエンタープライズオペレーションセンタ
EOC	エンタープライズオペレーションセンタ
NOSC	ネットワークオペレーション&セキュリティセンタ

JIEデータセンタとノード

CDC	中核データセンタ
IPN	(Installation Processing Node)
ISN	(Installation Service Node)
TPN	(Tactical Processing Node)
SPPN	特殊用途処理ノード

JIE管理ネットワーク

JMN	JIE管理ネットワーク
EOSS	エンタープライズオペレーションサポートシステム

JIE SSAコンポーネント

JRSS	合同地域セキュリティスタック
CSAAC	Cyber Sit'l Awareness Analytic Cloud
DMZ	Demilitarized Zone

JIE輸送インフラストラクチャ

IG	Installation Gateway
BAN	(Base Area Network)
MPLS	マルチポートコールラベルスウィッチング

クラウドコンピューティング

JIEがクラウドコンピューティングに関して早い段階から認識していた課題の1つが、SSAの一部としてのサイバーセキュリティの管理でした。この課題を解決するため、DoDは、FedRAMP（Federal Risk and Authorization Management Program）とSCCA（セキュアクラウドコンピューティングアーキテクチャ）を採用しています。DoDは、機密性が低〜中程度のデータにFedRAMPを使用し、FedRAMPによって、クラウドコンピューティングサービスのアクセスと認証の標準アプローチが確立されます。

DISAの公開サイトによると、SCCAは、エンタープライズレベルのクラウドセキュリティと管理のサービススイートで、商用クラウド環境でホストされている影響レベル4とレベル5のデータに対して、境界やアプリケーションレベルのセキュリティの標準アプローチを提供します。SCCAの目的は、DoD情報サービスネットワーク（DISN）とDoDが使用する商用クラウドサービスとの間に保護の障壁を提供しつつ、サイバーセキュリティのコストとパフォーマンスのトレードオフを最適化することです。

クラウドファーストアプローチへの進化

DoDは、インフラストラクチャビジネスから脱却し、クラウドサービスプロバイダからサービスとして提供される情報テクノロジを利用する意向を公式に表明しています。JIEは正しい方向へとその一歩を踏み出しましたが、基盤となる設計の多くは10年以上前に開発されたアーキテクチャに基づくものであったため、本番環境への展開に10年近くを要し、DoDは、大量のインフラストラクチャを利用し続けることになりました。陸軍と空軍は、商用ソリューションプロバイダのEITaaS（Enterprise IT-as-a-Service）ソリューションを採用することで、コストを削減し、敵を上回る競争力を維持しようとしており、DEOS（Defense Enterprise Office Solution）は、このクラウドアプローチへの進化の一例です。

DISAは、次のように説明しています。「DEOSは、DoDのECAPS（Enterprise Collaboration and Productivity Services）戦略をサポートするエンタープライズ商用CSO（Cloud Service Offering）であり、DoD全体で共同利用する共通のエンタープライズアプリケーション/サービスを取得して実装、クラウド採用を標準化し、地上や海上の組織を含むローカルのB/P/C/S（Base/Post/Camp/Station）レベルの部門横断コラボレーションを可能にすることで、DoDの既存のUC（Unified Capabilities）を置き換えます」（DEOS（Defense Enterprise Office Solution）、2019年）

これまでは機関ごとにMicrosoft Exchange Serverの固有のクラスタを運用していましたが、これは非常に非効率的であり、DoDは多額のメンテナンス費を強いられてきました。DISAのDefense Enterprise Emailは、DoDのすべての部門が使用し、DISAがホストと管理を担当する統合DoDエンタープライズソリューションを提供する第一歩になりました。

> 「Enterprise Email Systemは、我々が構想する統合情報環境（JIE）の実現に向けた重要な要素の中核となる基盤なのです」
>
> **- DISAの元エンタープライズアプリケーション担当責任者、John Hale氏（Crank、2013年）**

Defense Enterprise Emailは、DoDが分散型のメールソリューションから一元化されたエンタープライズサービスへの移行を可能にし、クラウドサービスプロバイダが完全にサービスとして提供するクラウドオフィスソリューションに移行する道を開拓する重要な第一歩となりました。JIEのSSAコンポーネントもこれと同様に、サービスとして提供することができます。DoDはすでに、代替クラウドアクセスポイントソリューションの検討を開始しており、そのソリューションによって、DoDの機関がIL-4/5サービスをクラウドサービスプロバイダから効率的に直接利用できるようになり、現在のJIE SSA実装に伴うボトルネックや遅延に悩まされることもなくなります。現在、世界10か所でDISAがホストおよび管理するIAPは、今後はFedRAMP IL-2セキュリティスタックアズアサービスソリューションを提供するクラウドサービスプロバイダがサービスとして提供する可能性があります。クラウドソリューションに移行することで、JRSS、IAP、CAPで重複している多くの機能が統合されるため、国防総省のユーザや戦闘員にサービスを効率的かつ合理的に利用するための最適な経路を提供できるようになります。

ネットワーク中心からリソース中心のフレームワークへの移行

現在のJIEはネットワーク中心に設計されており、ネットワークが保護されればリソースやユーザも保護されるという前提をもとに、ネットワークそのものの保護に重点が置かれています。過去の経験からこの考えが誤りであることがわかっており、保護されたネットワークを過剰に信頼してしまったために悪用されてしまった例が数多く存在します。DoDに必要なのは、

NISTによる以下の定義を満足するゼロトラストアーキテクチャを採用した最新のアプローチです。「ZT（ゼロトラスト）は、ネットワークが侵害されたとみなされる状況で、情報システムやサービスにおける正確で要求に基づくアクセス判断にあたっての不確実性を軽減する目的で設計された概念とアイデアの集りです。ZTA（ゼロトラストアーキテクチャ）とは、ゼロトラストの概念を活用し、コンポーネントの関係、ワークフローの計画、アクセスポリシーを包む、エンタープライズのサイバーセキュリティ計画です。したがって、ゼロトラストエンタープライズは、ゼロトラストアーキテクチャ計画の成果としてエンタープライズに配置されるネットワークインフラストラクチャ（物理および仮想）であり、運用ポリシーということになります」（Scott Rose氏、2020年）

NISTが定義するゼロトラストアーキテクチャの基本的な考え方は、以下のとおりです。

- すべてのデータソースとコンピューティングサービスをリソースとみなすすべての通信は、ネットワークの場所に関係なくセキュリティで保護されるべき
- 個々のエンタープライズリソースへのアクセスはセッション単位で許可される
- リソースへのアクセスは、動的ポリシーにより決定される。これには、クライアントのアイデンティティ、アプリケーション、要求するアセット（これ以外の動作属性が含まれる場合もある）の観測可能な状態が含まれる
- エンタープライズは、すべての所有するデバイスや関連するデバイスが可能な限り最も安全な状態であることを保証し、アセットを監視することでその最も安全な状態が維持されるようにする
- すべてのリソース認証と承認は動的であり、アクセスが許可される前に厳しく適用すべき
- エンタープライズは、ネットワークインフラストラクチャと通信の現在の状態に関する情報を可能な限り多く収集し、その情報を使用してセキュリティ態勢を改善する

DoDはすでにゼロトラストソリューションを検討し始めており、IAPやCAPなどのソリューションが境界を保護する一方で、ZTAはネットワーク内部からリソースを保護するための焦点になりつつあります。ZTAが実装されれば、ネットワークそのものは単なる情報伝達の手段に過ぎなくなります。

セキュリティをサービスとして提供するZscaler

Zscalerは10年以上にわたり、世界最大規模の商用企業にセキュリティをサービスとして提供してきました。当社は2018年末にクラウドベースのセキュリティソリューションとして初めて、FedRAMP認定を取得し、FedRAMP ModerateであるZscaler Internet Access™（ZIA™）とFedRAMP HighであるZscaler Private Access™（ZPA）™の2つのサービスを提供しています。

Zscaler Internet Access

Zscaler Internet Access（ZIA）は、サービスとして提供されるセキュアインターネットゲートウェイ/クラウドサービスプロバイダ（CSP）ゲートウェイです。CSPへのゲートウェイをZscalerにするだけで準備が完了し、インターネットやCSPへの安全な入り口を提供します。軍事拠点の場合は、最も近いZIA Public Service Edge（旧Zscaler Enforcement Node）にルータトンネル（IPsec）をセットアップし、さまざまな場所で働く従業員の場合は、軽量のZscaler Client Connector（旧Zscaler App）またはPACファイル経由でトラフィックを転送できます。

SSAのIAPとCAPの主な機能は、それぞれがインターネットとCSPからのDISNを保護する包括的で堅牢なセキュリティスタックを提供することです。ZIAはこれまでに、この種の保護を世界中のお客様に提供してきました。ZIAは、ユーザとインターネットまたはCSPの間で、複数のセキュリティ手法を活用し、SSLを含むすべてのトラフィックをバイト単位かつインラインで検査することで、Web、インターネット、クラウドの脅威から完全に保護します。

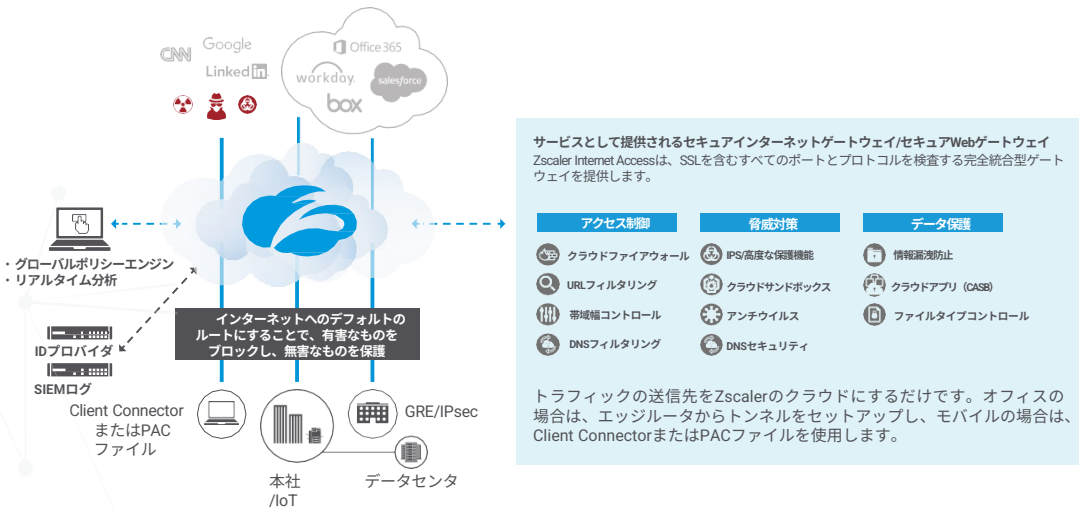


図2 - Zscaler Internet Access

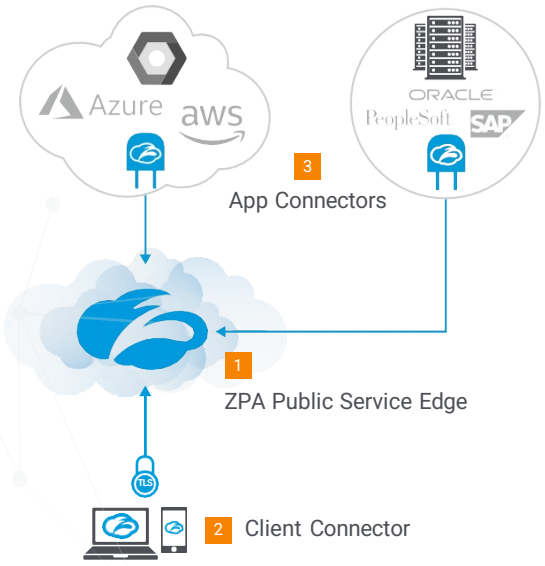
Zscaler Internet Access

ZPAは、クラウドやプライベートデータセンタで実行中の内部アプリケーションに対して、ゼロトラストで安全なリモートアクセスを提供するFedRAMP High/IL-4のクラウドサービスです。ZPAではアプリケーションやサービスが外部に公開されないため、権限のないユーザからは完全に見えなくなります。このサービスにより、ネットワークをユーザまで拡張することなく、内側から外側への接続でユーザがアプリケーションにアクセスできるようになります。

ゼロトラストアクセスは、以下の4つの主要な考え方に基づいています。

- ネットワークにアクセスしたり、VPNを使用したりすることなく、アプリケーション/サービスにアクセスする。
- 内側から外側への接続により、権限のないユーザからアプリやサービスを見えないようにする。
- ネットワークではなく、アプリケーションをセグメント化することで、ユーザを特定のアプリに接続し、水平移動を制限する。
- エンドツーエンドの暗号化されたTLSトンネルにより、ネットワーク通信を保護する。

ZPAは、シンプルで安全かつ効果的な方法で、内部サービスへのアクセスを可能にします。IT管理者がZPA Admin Portalで作成し、Zscalerのクラウドでホストされるポリシーに基づき、アクセスが許可されます。Client Connectorと呼ばれるソフトウェアがユーザのデバイスにインストールされ、ユーザが内部サービスにアクセスしようとすると、Client Connectorがユーザのデバイス態勢を確認して、Zscalerのクラウドへの安全なマイクロトンネルを拡張します。



ゼロトラストアーキテクチャ

1 ZPA Public Service Edge
- Client ConnectorとApp Connectorの間の安全な接続を仲介
- クラウドでホスト
- 認証に使用
- 管理者によるカスタマイズが可能

2 Client Connector
- デバイスにインストールするモバイルクライアント
- アプリへのアクセスを要求

3 App Connector
- AzureやAWSなどのパブリッククラウドサービス内のアプリの前面に配置
- アプリケーションへのアクセス要求を処理
- インバウンド接続なし

図3 - Zscaler Private Access

両サービスは、業界標準ベースのSAML 2.0接続を介して、DoDの既存のアイデンティティプロバイダと統合し、DoDのSIEMアーキテクチャにトランザクションログ情報をストリームする機能も備えています。これは、ZscalerがDoDの既存のサイバーセキュリティプラットフォームやビッグデータに関する取り組みと統合できることを意味します。ZIAとZPAはどちらもオンプレミスで拡張でき、効率的なトラフィックエンジニアリングを実現します。DoDINの境界でクラウドベースの保護を行うZIAと、DoDIN内の接続を保護するゼロトラストアーキテクチャを提供するZPAが、以下のようにアーキテクチャを大幅に簡素化します。

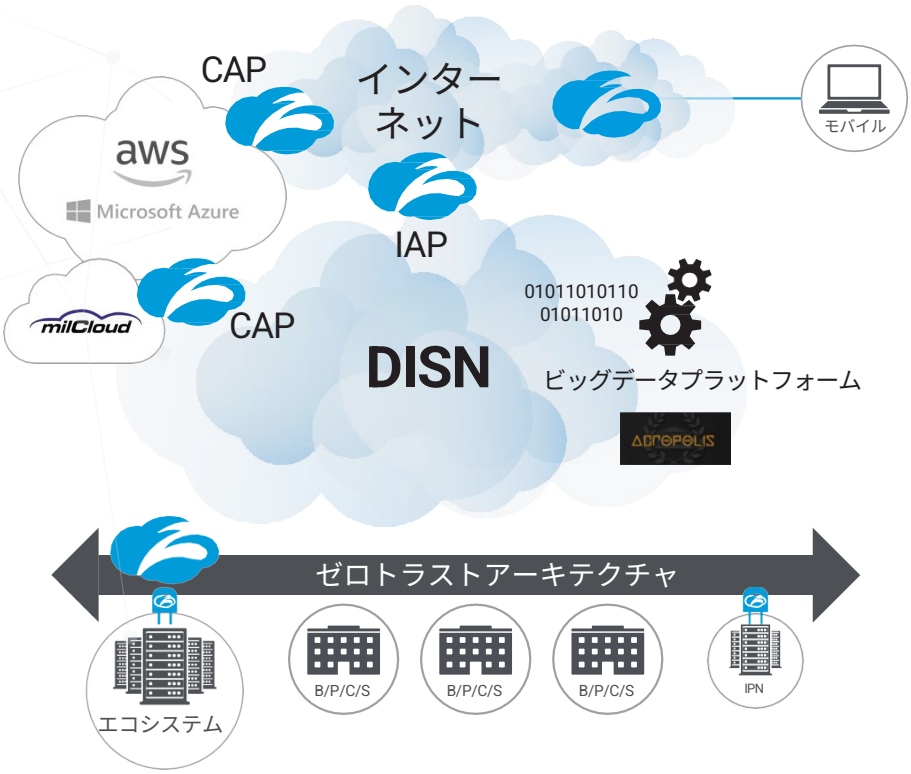


図4 - サービスとして提供されるJIE SSA

パートナーシップによる強化

Zscalerは、堅牢で完成度の高いSaaSプラットフォームを提供するだけでなく、高水準のソリューションを実現するために業界パートナーと緊密に連携することで、サービスを簡単に導入し、統合できるようにします。Zscalerは、ZPAサービスの一部として基本的なデバイス態勢を検証しますが、CrowdStrike、Carbon Black、SentinelOneなどのEDR（Endpoint Detection and Response）企業と連携することで、その機能をさらに強化します。業界をリードするパートナーと連携することで、Zscalerはユーザをリソースに接続する前に、エンドポイントでEDR機能が有効であることを確認します。ZIAとCrowdStrikeは脅威インテリジェンスをクラウド間で共有しているため、Zscalerが世界中で検知した脅威シグネチャをCrowdStrike Falconサービスを利用しているエンドポイントでも検知できます。また、Zscalerを Splunk、Elastic、ArcSightなどのSIEM（Security Information and Event Management）ベンダと統合して、これらのソリューションにZscalerのリアルタイムのストリーミングデータを簡単に取り込むこともできます。ZscalerはインラインCASB（クラウドアクセスセキュリティブローカ）機能を提供していますが、ZIAをMCAS（Microsoft Cloud App Security）やMcAfee MVISIONなどのサードパーティのCASBソリューションと統合することも可能です。

まとめ

JIEは、DoDの各機関が独自のサイバーセキュリティ戦略を管理するという、断片的でサイロ化したアーキテクチャから、「統合セキュリティアーキテクチャ」への移行を実現した革新的な概念でした。世界中のB/P/C/Sに配置されていた190以上の各機関のセキュリティスタックを、DISAが一元管理する数十のスタックに置き換えることができました。SSAのセキュアクラウドコンピュートアーキテクチャにより、商用クラウドサービスプロバイダのクラウドサービスを採用するセキュリティフレームワークが提供されました。

DoDは、統合セキュリティアーキテクチャにセキュリティを集約させる第一歩を踏み出し、アーキテクチャ自体の管理と保守から「サービスとして」の提供に移行するという、変革の次のステップに準備を進めています。Zscalerは、クラウドベースのセキュリティスタックをサービスとして提供することで、現状ではIAPとCAPが提供している境界セキュリティの役割を果たします。パフォーマンスの大きなボトルネックとなっている複雑で高価な地域別のセキュリティスタックを、EDRソリューションを搭載した当社のゼロトラストフレームワークに置き換えることができます。DoDがJIEをサービスとして提供することで、コストの削減、スケーラビリティの向上、エンドユーザや戦闘員の効率的な任務の遂行などが可能になります。そして最終的には、サイバーセキュリティの強化が実現します。

参考資料

Crank, T. M.（2013年）DISAの100万ユーザに配信されたエンタープライズEメール、DoDニュース

DEOS（Defense Enterprise Office Solution）（2019年2月）、www.disa.milから取得 Scott Rose, O. B.（2020年）、ゼロトラストアーキテクチャSlabodkin, G.（2013年7月19日）DODネットワークの単一セキュリティアーキテクチャによる防御、防御システム

Team, S. I.（2016年）JRSS（Joint Regional Security Stack）EDS（Engineering Design Specification）

（2013年）国防総省の統合情報環境（JIE）実装戦略、米国防総省

Zscalerについて

Zscalerは、世界の主要企業がモバイル/クラウドファーストの世界に対応するために、ネットワークやアプリケーションの安全な変革を実現します。Zscalerの代表的サービスであるZscaler Internet Access™およびZscaler Private Access™は、デバイス、場所、ネットワークなどに影響されることなく、ユーザとアプリケーション間の高速で安全な接続を構築します。クラウドで提供されるこれらのサービスは、従来のアプライアンスやハイブリッドソリューションとは比較にならない容易性、高度なセキュリティ、優れたユーザエクスペリエンスを提供します。185か国以上で使用されているマルチクラウド分散型セキュリティプラットフォームを運営し、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。
詳細については、zscaler.jpをご覧いただくか、Twitter（@zscaler）をフォローしてください。

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.jp