ゼロトラスト・保護サーフェスの定義

CSAJC cloud security alliance SM Japan Chapter

CSA cloud security alliance ®

Zero Trust Research Working Groupの恒久的かつ公式な場所は以下になります。
https://cloudsecurityalliance.org/research/working-groups/zero-trust。

謝辞

CSA Zero Trust Research Working Group

ゼロトラストの研究とガイダンスの範囲は、必然的にクラウドとオンプレミス環境、モバイルエンドポイントを含み、モノのインターネット（IoT）と運用技術（OT）に適用されます。CSA Zero Trust (ZT) Working Groupの目標は以下のとおりです。

- 情報セキュリティ（InfoSec）に対する現代的で必要かつクラウドに適したアプローチとして、ゼロトラストのベストプラクティスを共同で開発し、認知度を高めます。
- ソートリーダーシップを発揮し、さまざまなZTアプローチの長所と短所について業界を啓蒙することで、組織がそれぞれのニーズと優先事項に基づいて十分な情報に基づいた意思決定を行えるようにします。
- 成熟したゼロトラスト実装のためのアーキテクチャと実装アプローチについて、意図的に製品およびベンダーに中立的なアプローチをとります。
- 製品およびベンダーに中立的でありながら、ゼロトラストに関して技術的に健全な立場をとり、擁護可能な提案を行います。
- 作業部会は、ゼロトラスト成熟度モデルとアーキテクチャの柱に沿った9つの異なる作業の流れで構成されています。
- この文書のリードワークストリームは**ZT7 - Pillar: Data**です： Shruti Kulkarni、Krishna Narayanaswamy、Alex Kaluzaがリーダーを務めています。

主執筆者

Shruti Kulkarni
Michael Roza

投稿者

Krishna Narayanaswamy
Shamik Kacker
Erik Johnson

CSAスタッフ

Erik Johnson
Alex Kaluza
Claire Lehnert
Stephen Lumpe

レビュアー

John Kindervag
Jason Garbis
Chandra Rajagopalan
Bernard Coetzee
Hani Raouda
Heinrich Smit
Jennifer Minella
Steve Guilford
Paul Simmonds
Ivan Djordjevic
Anand Kumar Jha
Gopi Ramamoorthy

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・保護サーフェスの定義」は、Cloud Security Alliance (CSA)が公開している「Defining the Zero Trust Protect Surface」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
2024年4月15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・保護サーフェスの定義」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）

石井　英男
井上　尚人
納本　健太
諸角　昌宏

目次

要旨 8
対象とする読者 8
ゼロトラスト入門 8
文書の範囲 9
ビジネス資産の概要 9
ゼロトラスト導入プロセス 11
保護サーフェスの概要 12
5-ステッププロセスの反復実行の優先順位付け 16
目的が不明確なDAAS要素に関する注意 17
保護サーフェスを構成するDAAS要素 17
データ 18
アプリケーションとワークロード 19
資産: システムとデバイス 20
サービス 21
NSTAC、CISA成熟度モデルと保護サーフェス 22
保護サーフェスの侵害がもたらすリスクと影響 24
データ分類の適用 27
攻撃サーフェスと保護サーフェス 28
保護サーフェスが定義された後の展望 29
結論 31
参考文献 32

要旨

この文書の目的は、John Kindervag が最初に策定し社会化したNSTAC Report to the President onZero Trust and Trusted Identity Managementに記載されている 5 つのステップのゼロトラスト実装プロセスの第 1 ステップを反復的に実行するためのガイダンスを提供することです。5 つのステップのそれぞれについて詳細なガイダンスを作成するために、別の CSA リサーチ文書が作成されているところです。

この重要な最初のステップである「保護サーフェス の定義」では、組織のデータ、アプリケーション、資産、サービス（DAAS）の要素を特定し、ビジネスリスクと現在のセキュリティ成熟度の評価を行い、実装の優先順位付けを行います。本稿では、DAAS 要素を保護サーフェスにグループ化するなど、このプロセスの背後にある方法論に焦点を当てます。
ビジネス情報システムを構成する攻撃サーフェスと保護サーフェスの相互関係や、CISA Zero Trust Maturity Model V2実装の優先順位付けに活用する方法など、重要な検討事項と概念について説明します。このガイダンスは、組織がゼロトラスト実装の複雑さを乗り越えるための反復可能なプロセスを採用することを支援します。

対象とする読者

- **主な対象**者： ゼロトラストアーキテクトおよび実装チーム、最高情報セキュリティ責任者、情報セキュリティ管理者、ITセキュリティアナリスト
- **第二の対象**者： CxO（CEO、CISO、CFO、CTO、CIO）、プライバシー・コンプライアンス・オフィサー、IT監査・評価者、ソフトウェア開発者、ネットワーク・セキュリティ・エンジニア

ゼロトラスト入門

National Security Telecommunications Advisory Committee (NSTAC) Report to the Presidenton Zero Trust and Trusted Identity Managementは、ゼロトラスト（ZT） を *「サイバーセキュリティ戦略とは、どのようなユーザーや資産も暗黙のうちに信頼されるべきではないという考えを前提としたものです。この戦略では、情報漏洩がすでに発生しているか、または今後発生する可能性があることを前提としているため、企業の境界で行われる1回の検証によって機密情報へのアクセスが許可されるべきではありません。その代わり、各ユーザー、デバイス、アプリケーション、トランザクションは継続的に検証されなければなりません。」と定義しています。*

従来の中央集権的な信頼ベースの「城と堀」の物理ネットワーク境界セキュリティアーキテクチャは、実際にはほとんどの組織の資産やユーザーが「城」の中には存在していない、分散型クラウドコンピューティングとリモートワークフォースの時代には効果がありません。

インターネット接続を多用する現代の高度に分散した企業ネットワークにおいて、露出した技術的または人的な脆弱性を悪用することに、洗練された脅威主体はますます習熟しています。サイバー攻撃は一般的に、何らかの形で信頼を悪用します。そのため、「信頼」はリスク軽減と管理がされるべき、危険な脆弱性となっています。ゼロトラストでは、全てのネットワーク接続とパケットは信頼されず、システムを流れる他のすべてのパケットと同じように扱われます。信頼レベルがゼロと定義されるため、ゼロトラストと呼ばれます。

ゼロトラストは、クラウド／マルチクラウド（すべてのサービスモデル）、オンプレミス／ハイブリッド・システム、内部および外部のパートナー／利害関係者のユーザーの（組織管理およびBYODの）エンドポイントを包含し、運用技術（OT）、産業制御システム（ICS）、IoTを含む、包括的な全社的セキュリティ戦略です。その結果として、ゼロトラストは、一歩ずつ登っていかなければならない山に、すなわち段階的に、できればリスクベースの方法で実装されなければならないと、例えられてきました。これらの原則は、CSAのZTガイダンスに共通するテーマです。

ゼロトラストの企業導入は広範に広がり、拡大しています。Venture Beatによると、クラウドに移行する企業の90%がゼロトラスト戦略を採用しており[1]、Gartnerは、2026年までに大企業の10%が成熟した測定可能なゼロトラストプログラムを導入すると予測しています[2]。

文書の範囲

この文書の目的は、John Kindervag が最初に策定し社会化したNSTAC Report to the President on Zero Trust and Trusted Identity Managementに記載されている 5 つのステップのゼロトラスト実装プロセスの第 1 ステップを反復的に実行するためのガイダンスを提供することです。本書は、ゼロトラスト実装の複雑さを段階的にナビゲートするためのガイドです。本書は、組織のビジネス資産をしっかりと理解した上で、強靭なサイバーセキュリティを実装するための基本的なステップである「保護サーフェスの定義」から始めます。組織のデータ、アプリケーション、資産、サービス（DAAS要素）に関連するリスクとセキュリティ成熟度を特定、分類、評価する方法について説明し、リスクベースの優先順位付けのための明確な基準を確立します。このガイドでは、「保護サーフェス（Protect Surface）」と「攻撃サーフェス（Attack Surface）」の区別など、重要な考慮事項について説明しています。本書は、システムがどのように機能しているかを理解することに焦点を当てた第2ステップ「トランザクションフローのマッピング」についての重要な洞察で締めくくられています。

ビジネス資産の概要

ゼロトラストの認識と採用は、企業が複雑なデータセキュリティの課題に直面しているのと同時に起こっています。企業はITの変革に取り組んでおり、データはプライベートデータセンターの枠を出て、直接管理下には全くないクラウドホスト環境に移行しています。こうした変化において、企業は重要なビジネス資産とデータを特定し、保護することが不可欠となっています。

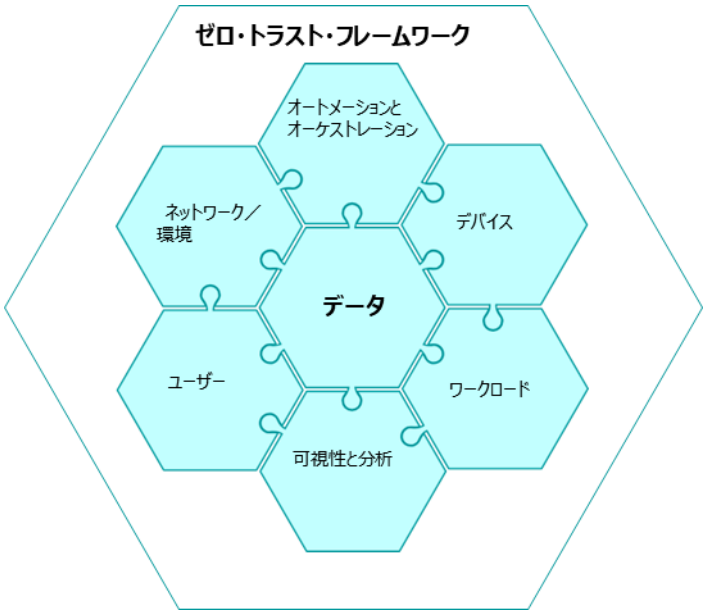
また、ビジネス資産とデータ、及びそれらの機密性は、組織の状況に応じて相対的なものであることに留意することも重要です。たとえば、金融サービス業界は、カード会員データ、銀行口座データ、および金融取引を含むように機密資産を定義することができます。アイデンティティプロバイダーは、そのストアに保持されるアイデンティティという観点でデータを定義することができます。ソフトウェア製品会社は、コードリポジトリー（コードベース）を重要資産／データと定義することができます。化学産業では、重要資産をプラントプロセス

[1] https://venturebeat.com/security/why-90-of-enterprises-migrating-to-the-cloud-are-adopting-zero-trust/

[2] https://www.gartner.com/en/newsroom/press-releases/2023-01-23-gartner-predicts-10-percent-of-large-enterprises-willhave-a-mature-and-measurable-zero-trust-program-in-place-by-2026

と定義することができ、それを悪用や妨害行為から保護する必要があります。

下の図は、米国国防総省のゼロトラストリファレンスアーキテクチャからの引用です。データはすべての柱にとって不可欠であるため、ゼロトラストフレームワークの中心として描かれています。しかし、ゼロトラストフレームワークは、デバイス、ワークロード、サービスをデータと要素の交差点として含んでいます（例えば、デバイスとワークロードの交差点）。



ZTの柱はZT戦略によって特定されました。

これらは、相互にリンクされた戦略的リソースのグループに関連付けられます。

データの保護はZT目標の中心であり、他のすべてのリソースの一部です。

すべてのリソースはゼロトラストフレームワークにバインドされています。

図 1.米国国防総省のゼロトラストの柱（参考：US Department of Defense (DoD) Zero Trust Reference Architecture）

ゼロトラスト導入プロセス

本文書は、「NSTAC Report to the (US) President on Zero Trust and Trusted Identity Management」に記載されている 5つのステップのゼロトラスト実装プロセスで定義されている最初のステップを完了するためのガイダ ンスを提供します。この基本となる参考文献は、CSA のゼロトラスト研究が活用し、整合させる先とするものであり、2.1.1 節で 5つのステップの方法を反復実行可能なプロセスとして描いています。

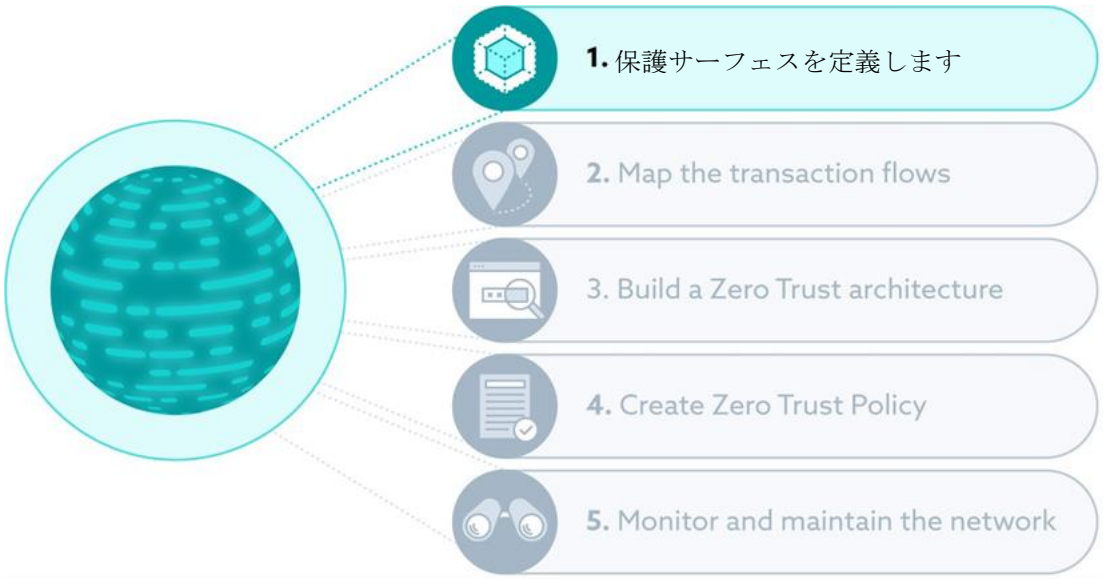


*図2. ゼロトラスト導入のための5段階プロセス　参考：*NSTAC Report to the (US) President on Zero Trust and Trusted Identity Management

保護サーフェスの概要

保護サーフェスとは、ゼロトラストポリシーの実装によって保護される組織の技術環境の領域または部分です。保護サーフェスは、データ、アプリケーション、資産、サービス（DAAS）、すなわちNSTAC reportの6ページ「表3：ゼロトラストの基礎となる主要概念と定義」に記載されている1つ以上のDAAS要素で構成されます。

データ、アプリケーション、資産、サービス (DAAS)	それぞれの保護サーフェスで使用される機微なリソース。
	• データ - 流出または悪用された場合に最大のリスクをもたらす機微データ。
	  • たとえば、ペイメントカード情報、保護された医療情報、個人を特定できる情報、知的財産などが含まれます。
	  • 政府機関では、機密情報（Classified Information）、国家安全保障情報(National Security Information)、管理された非機密情報(Controlled Unclassified Information)も含まれます。
	• アプリケーション – 機微データを使用したり、重要な資産を管理するアプリケーション。
	• 資産 - 組織の情報技術(IT)、運用技術(OT)、IoT機器などの資産。
	• サービス - 組織が最も依存しているサービス。
	  • たとえば、DNS、DHCP、ディレクトリサービス、NTP、カスタマイズされたAPIなどです。

NSTACの報告書の6ページ「表3：ゼロトラストの基礎となる主要概念と定義」には、「各保護サーフェスには、単一のデータ、アプリケーション、資産、サービス（DAAS）要素が含まれる」と記載されています。この定義は、必要以上に文字通りあるいは規定的に解釈されるべきではありません。組織のビジネス環境と要件に応じて保護対象サーフェスには、アプリケーションとそのデータのような、*ビジネス情報システム*を構成し、一体として保護されるべき関連DAASが含まれる可能性があります。我々は、ビジネス情報システムの概念は、一連の DAAS 要素、トランザクションフロー、施行ポイント、およびポリシーを整理するための概念であるべきだと考えています。各保護サーフェスに適切な粒度レベルを選択することが重要です。そうすることで、理解しやすく、関連する一連のトランザクションフロー、アーキテクチャ要素 (施行ポイント)、およびアクセスポリシーを簡単に作成できるようになります。

このことを、架空の金融サービス組織のビジネス情報システムにおける保護サーフェスを例として説明します。図3は、いくつかの保護サーフェスの例を、関連するビジネスリスク、およびゼロトラストの旅における次の行き先を決めるのに使用可能な現在のZTセキュリティ成熟度の指標とともに示しています。

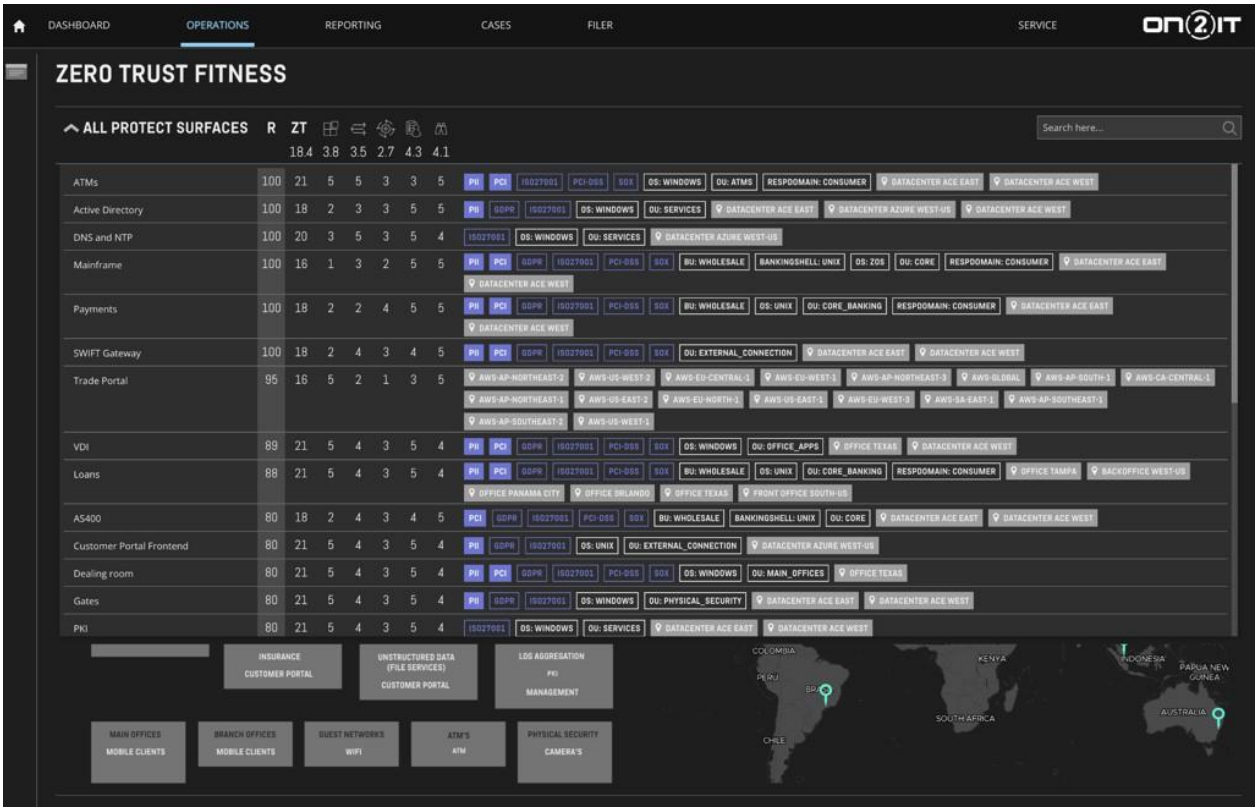


図3.ON2IT 実証システムにおける架空の金融組織の保護サーフェス。参照： CSA ZT ワークグループ 2/27/23 での[On2IT Zero Trust Implementation Methodology Presentation]

ビジネス情報システムはしばしば複数の関連するDAAS要素を含みます。ビジネスとリスクの観点からは、ある一つの要素が主要な要素とみなされることが多いです。本文書及び CSA ZT 実施ガイダンス全般の目的のため、我々はビジネス情報システムを保護サーフェスと同一視します。全てのビジネス情報システムがDAASの各要素タイプ（列）の構成要素を持つわけではありません。大規模で複雑なビジネス情報システムは、ゼロトラスト実施目的のために、系統的に関連する保護サーフェスである個別のDAAS要素で構成されるサブシステムに分割される場合もあります。これは、サブシステムが異なるリスクレベルの異種技術を含む場合に特に適用可能です。例えば、より大きなサービスモニタリング・課金業務システムの一部である OT スマートメーター測定システムは、別個のサブシステムと見なすことができます。以下の表 1 に、保護サーフェスのもう一つのサンプルを示します。

保護サーフェスのサンプル					
#	ビジネス情報システム	データ	アプリケーション	資産	サービス（サポートサービス）
1	CRMシステム	顧客データ 顧客が使用する会社の製品、サービス、連絡先、リソース、イベントに関するデータ	CRMアプリケーション（SaaS）	CRM SaaS CSPのCRMサーバー	顧客・組織のアイデンティティサービス、DNS
2	文書リポジトリ	ファイルとメタデータ	Sharepoint Online	マイクロソフトのインフラ	Identity-as-a-Service (Azure Active Directory)
3	決済システム・アプリケーション	カード会員データの取得と支払い処理のためのデータ	カード会員データを管理し、支払いを処理するウエブアプリケーション	カード会員データが保存されているデータベースをホストするサーバー	外部クレジットカード決済処理サービス、DNS
4	産業制御システム	化学プラントの化学プロセスを管理するために使用される制御、センサー、およびプロセスデータ	生産用化学プロセス制御アプリケーション	化学プラントのセンサーとPLC	暖房、換気、空調（HVAC）
5	スマートエネルギー計測・課金システム	電気消費量と顧客データ	顧客モニタリング・請求システム	エネルギー消費に関する信号を顧客モニタリングと請求システムに送るスマート メーター	スマートメーター無線ネットワーク

表1：保護サーフェスのサンプル

すべてのデータ、アプリケーション、資産、サービスを含む組織のデジタルプレゼンスとオペレーションは、プライベート、パブリック、ハイブリッド・クラウド、オンプレミス環境、またはそれらの組み合わせのいずれで配備されているかにかかわらず、潜在的な脅威から保護されるべきです。

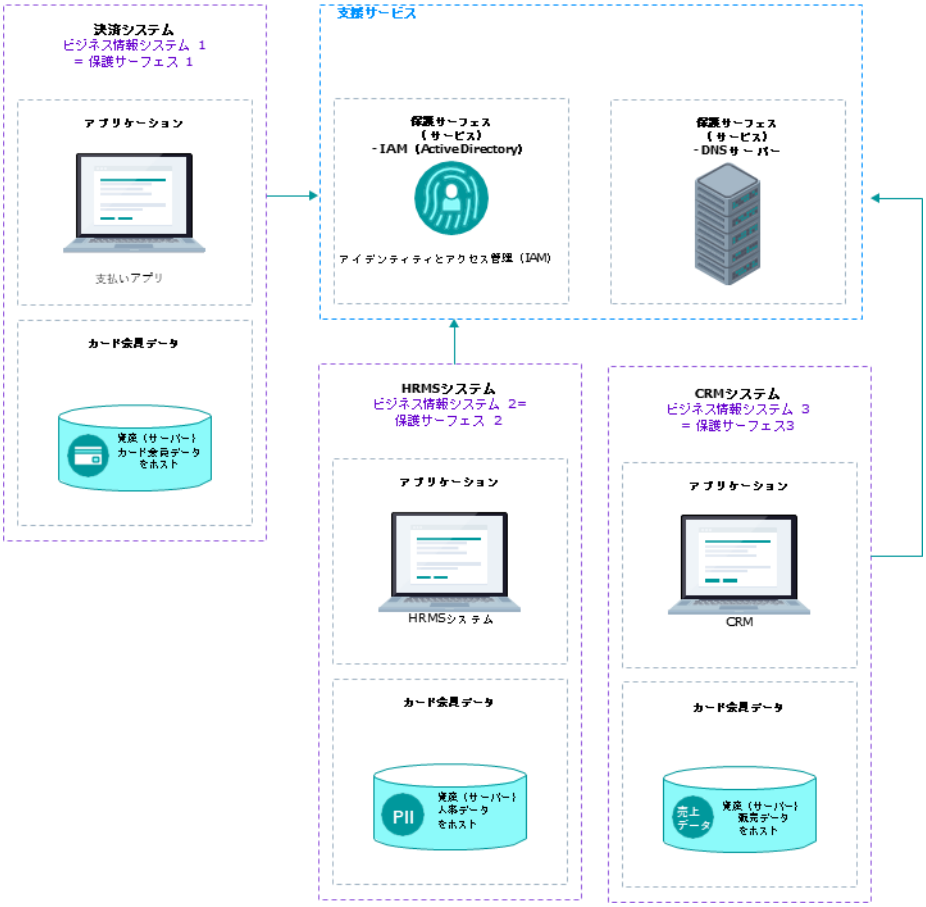


図4. 別の架空の組織の保護サーフェス

図4は、組織に対して定義された複数の保護サーフェスを示しており、すべてのサーフェスは互いにインターフェースを持っています。

- 保護サーフェス1は、カード会員データを処理するアプリケーションとデータベースで構成され、この組織の主要な高リスクのビジネス情報システムです。なぜなら、このデータが侵害されると、顧客に直接影響を与え、規制上の罰金、訴訟費用、レピュテーションの問題につながる可能性があるからです。
- 保護サーフェス2はHRMSアプリケーションで構成され、プライバシー要件がある内部向けビジネス情報システムです。
- 保護サーフェス3は、CRMで構成されています。CRMは、内部向けおよび外部向けのビジネス情報システムであり、商業的な要件を備えています。
- DNSサーバー（サポートサービス）は重要な保護対象であり、その運用が侵害された場合、サービスの停止や中断が広範囲に及ぶ可能性があります。

- アイデンティティとアクセス管理（IAM）は、重要な保護サーフェスです。そのセキュリティの侵害は、不正アクセス、データ漏洩、システムの脆弱性につながる可能性があります。

図4は、さまざまなビジネス情報システムとサポートサービスの相互関連性に起因して、保護サーフェスが互いにどのように影響しあうかを示しています。

さらに、多くの組織は、ビジネスにおいて外部データの供給に依存しています。株式市場や地理位置データなどのデータは、エンドユーザーや組織が利用するために、サプライヤーから提供されることが多いです。組織は、データの供給を確保し、指定されたサプライヤーから正しいデータが確実かつセキュアに利用するようにする責任があります。これはデータディスカバリーの一部でありトランザクションフローのマッピングとビジネス情報システムの仕組みの理解に関連します。

組織データは、給与計算サービスなど、外部のビジネスサービスプロバイダーによってホストされているデータである場合があります。このようなシナリオでは、データは引き続き組織によって所有されますが、契約・規制上の要件の範囲でデータとそのサービス (それ自体が保護サーフェスである) を保護する責任を負う外部のビジネスサービスプロバイダーの管理下にあります。契約・規制上の要件については、所有組織が引き続き責任を負います。

5-ステッププロセスの反復実行の優先順位付け

組織は、各業務情報システムに関連するリスクと組織にとっての重要度を含め、すべての保護サーフェスを包括的に特定し文書化します。組織の保護サーフェスが文書化されたら、その保護サーフェスを分析し、リスク、重要性、現在のセキュリティ成熟度に基づいて優先順位を付け、反復的に実施します。

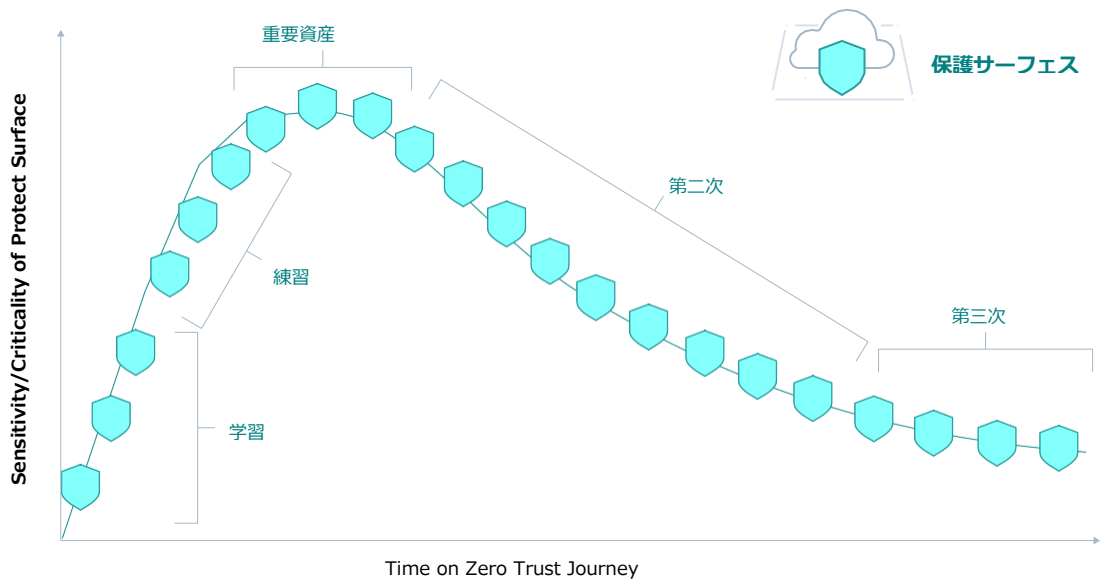


図5. The Zero Trust Learning Curve: Deploying Zero Trust One Step at a Time John Kindervag/Palo Alto

図 5 に示すように、組織は、重要な業務システムや「企業の重要資産」に対して本格的にゼロトラストを開始する前に、テストケースとして単純な保護サーフェスを1つまたは2つ実装して経験を積むという戦略を選択することができます。簡単なものから始めます。保護サーフェスを使用することで、貴重な洞察を安全に得ることができ、それをより複雑でリスクの高い保護サーフェスに適用することができます。特に、ゼロトラストの初期段階では、保護サーフェスを1つずつ実装することをお勧めします。このような反復的なアプローチにより、各保護サーフェスの実装から得られた教訓を体系的に後続の保護サーフェスに適用することができ、より十分な情報に基づいた効果的な実装が可能になります。

目的が不明確なDAAS要素に関する注意

最初のディスカバリ段階において、組織は、目的が不明確であったり、組織的な知識が不足していたり、あるいは組織目標との整合性が欠けているように見えるDAAS要素に遭遇するかもしれません。このような場合、すぐに無効にしたり削除したりする誘惑に負けないように注意することが勧められます。これらの要素は、組織の事業運営において重要な役割を果たしている可能性があり、突然削除すると混乱を引き起こす可能性があります。

その代わりに、後続のゼロトラスト導入ステップ（特に2と3）を進め、これらの疑わしい要素を注意深く評価し、その機能と影響をよりよく理解します。組織のDAASランドスケープとトランザクションフローを包括的に把握し、これらの要素の役割を検証して初めて、削除や変更に関して十分な情報に基づいた決定を下すことができます。

保護サーフェスを構成するDAAS要素

保護されるべきDAAS要素を特定し、それらのビジネス価値とリスク分類を、それらの要素が参加するトランザクションと共に理解することで、組織はゼロトラスト・保護サーフェスを定義することができます。NSTACの保護サーフェスの定義を使用すると、以下のコンポーネントがDAAS要素の一部を形成します。

- データ
- アプリケーション
- 資産
- サービス

データ

データが機微であるのは、一般に、規制上または法令上の意味を持つか、貴重な知的財産であるか、その他重要な価値を有するからです。機微データの流出や漏洩は、組織に悪影響を及ぼす可能性があります。
データは真空の中では存在できません。データには「家」が必要であり（例えば、データベースサーバー、ファイルサーバー、ワープロ、表計算ソフトなど）、その「家」（一般に資産と呼ばれる）を保護する必要があります。侵害からデータを保護することは、データをホストする資産を保護することにつながります。データだけに焦点を当てることは、データをホストする資産にズームインすることを意味しますが、これはアプリケーションやサービスを保護すべきではないという意味ではありません。もしこのようなことをすればアプリケーションが提供/利用するデータと、アプリケーションを支えるサービスとの間に断絶が生じる可能性があります。

侵害の影響：

データが漏洩または流出した場合、以下のようないくつかの影響が生じる可能性がありますが、これらに限定されるものではありません：

- 組織への直接的な影響：組織のデータが漏洩した場合、直接的に評判に影響が及びます。 規制当局の罰金、発生する弁護士費用、知的財産の損失、業務への影響など。
- サービスのエンドユーザーへの間接的な影響：しかし、実際の影響はデータが漏洩したエンドユーザーに及びます。データの種類にもよりますが、この侵害は、エンドユーザーの金銭的詐欺、デジタルアイデンティティの乗っ取り、個人的被害などをもたらす可能性があります。
- 直接的な影響と間接的な影響の間には、アイデンティティプロバイダーのストアにおけるアイデンティティの漏洩や、顧客が購入する製品への悪意のあるコードの混入など、サプライチェーンリスクの顕在化によって引き起こされる影響があり、これらは通常、外部の 保護サーフェス（APIやCI/CDパイプライン）と呼ばれます。

最初のステップとして、データが永続する場所と、関連する資産、アプリケーション、サービスを特定することが極めて重要です。

データの種類：

組織内のデータを特定するためには、組織が保有するデータの種類と、そのデータを特定する仕組みを知ることが重要です。データには以下の3種類があります。

- 構造化データ - 構造化データは特定が比較的容易です。構造化データは解析や検索が可能だからです。構造化データは通常データベースに格納されていますが、通常はアプリケーションを通じてアクセスされます。データベースやアプリケーションの管理者は、データに直接アクセスできることが多いです。
- 半構造化データ - 半構造化データの解析は比較的難しいです。しかし、これは解析はまだ可能、例えば、カンマ区切りやタブ区切りのファイル内のデータなどです。
- 非構造化データ - 非構造化データは解析が難しいです。例えば、画像やWord文書の中のデータは、もし一般的なレイアウトが分かるのであれば解析することができます。

データタイプがわかったところで、データの所在地を見つけることが不可欠です。この作業は手作業で行うことも、自動化された方法で行うこともできます。組織はこれに対し、「ビッグバン」アプローチをとることもできますし、一度に1つのデータカテゴリーを探索するようにもできます。通常、企業におけるデータの発見は膨大な労力を要するため、後者を推奨します。

非構造化データや半構造化データを発見するツールは存在します。しかし、構造化データを発見するツールは限られており、アプリケーションや資産を管理する人々にインタビューすることによって手作業で見つけることができます。

アプリケーションとワークロード

アプリケーションとワークロードは、重要なビジネス要件、機能要件、または運用要件を満たすソフトウェア、ハードウェア、およびインフラストラクチャの集合体で構成されます。アプリケーションは多くの場合APIインターフェース、CI/CDパイプライン、Webサービスなどを持つか含み、SaaSサービスとして実装されることもあれば、オンプレミスまたはクラウドのIaaS/PaaS環境でセルフホストされることもあります。これらの側面や属性はすべて、ゼロトラストの実装を目的とした保護サーフェスを特徴付けるのに役立つ重要なメタデータです。

アプリケーションは一般に、データへの直接的または間接的なインターフェースを持つか提供し、多くの場合、サポートサービスと連動します。例えば、買い物客がクレジットカード/デビットカードデータを入力/取得し、ペイメントカードサービスを使用して買い物の代金を支払うことを可能にするショッピングカート用のアプリケーションです。

- アプリケーションとワークロードは、データ取得、データ処理、データ利用、ビジネスプロセスロジックの実行、ビジネスオペレーションと資産を制御する信号の送信を通じて、データ、制御、ビジネスオペレーション、トランザクション、サービスを処理するインターフェースを提供します。データを処理するアプリケーションは、ワークロードです。データ処理の出力は、利用者が期待するもので、データ、イベント、あるいはプロセスを含みますが、これらに 限定はされません。このトランザクションの間に、悪意のある行為者がアプリケーションを侵害する可能性があります。例えば、SQLインジェクションによるデータ流出などです。したがって、アプリケーションの利用者がアプリケーションに入力するデータを保護することは、アプリケーションを SQL インジェクションから保護することを含みます。
- 今日のアプリケーションは、ライブラリ、フレームワーク、サードパーティソフトウェア、オープンソースソフトウェアで構成されることが多く、これらは独立してリスクをもたらす可能性があります。視線の可視性を維持するために、ソフトウェア部品表（SBOM）は、依存関係、ライブラリ、フレームワーク、および、その他サードパーティーコードを含む、アプリケーションで使用されるソフトウェアコンポーネントの詳細なインベントリを提供します。SBOM には、コンポーネントの名前、サプライヤー、ソフトウェアのバージョン、その他の一意の識別子などの情報が含まれます。SBOM は、組織がソフトウェアのサプライチェーンを理解し、潜在的なセキュリティリスクを特定するのに役立ちます。また、SBOM は、ソフトウェアサプライチェーンの変更と、その変更に起因する脆弱性の特定にも役立ちます。最後に、SBOM は、ソフトウェアサプライチェーンについてベンダーと議論するための共通言語を提供します。
- 組織がアプリケーションやワークロードの形で作成したり購入したりするビジネスロジック

は、多くの場合クラウドサービスとして実装され、作成、取得、処理、利用、他者への提供を行うデータを生かすことができます。このビジネスロジックは、データアクセスの認可を制御するため、データへのアクセスを安全に制御する上でも重要です。ロジックを可能な限りデータに近づけることで、きめ細かなセキュリティの実装が可能になり、ゼロトラスト保護サーフェスの1つとして扱われるようになります。

データと同様に、アプリケーションもモニタリングやスキャンツールを使って発見し、関連するメタデータを収集する必要があるかもしれません。

資産: システムとデバイス

物理資産とは、組織が保護しようとするデータをホストする、または組織が所有、使用、または企業内で重要なタスクを実行するリソースです。保護サーフェスの観点からは、資産はサーバーやワークステーションに限定されません。資産には、エンドポイントに接続されたデバイスだけでなく、IT（情報技術）、OT（運用技術）、IoT（モノのインターネット）デバイス、ICS（産業制御システム）など、環境全体のインフラストラクチャ デバイスも含まれます。資産には、以下のような、組織全体にわたる無数の物理的・仮想的デバイスが含まれます：

- IT（情報技術）、OT（運用技術）、IoT（モノのインターネット）デバイスを含む、エンドポイントに接続されたデバイスやインフラデバイス。これらの資産は、組織内のオンプレミス、リモートサイト、リモートワーカー、クラウド環境のいずれかに存在する可能性があります。
- エンドポイント接続デバイスには、ラップトップ、サーバー、スマートフォンなどのユーザーベースのプラットフォームや、医療機器、POS（販売時点情報管理）、センサー、プリンター、エレベーター、スマートビルディングテクノロジーなどの資産が含まれます。
- 製造システムは、産業用ロボット、プラント制御システム、SCADAシステムなどを含むが、これらに限定されないもうひとつの資産群を形成しています。
- インフラストラクチャ資産には、オンプレミスまたはクラウド上のネットワークインフラストラクチャーコンポーネントが含まれます。
- 運用技術（OT）は通常、環境や運用機器と相互作用するプログラム可能なシステムです。例えば、産業制御システム（ICS）、ビル管理システム（BMS）、火災制御システムなどです。これらのシステムは資産中心の保護サーフェス であり、可用性を重視し、人間の介入を最小限に抑えて使用できるように設計されています。これらのシステムは通常、これらの資産の設定や環境との相互作用の制御に役立つデータとのインターフェースを備えています。例えば、水処理システムのフッ素レベルを制御するデータなどです。OTはまた、電力網、消防署、浄水場などの重要な国家インフラ（CNI）の一部であることもあります。
- モノのインターネット（IoT）は運用技術の一種です。IoTには、スマートホームデバイス、スマートウェアラブル、またはデータや情報を交換できるネットワーク対応デバイスが含まれます。IoT デバイスは、 保護サーフェスを形成することも、その一部となることもできます。例えば、スマートテレビは、設定中や使用中にセキュリティを確保する必要があります、さもなければ悪意のある行為者の侵入口となる可能性があります。

データ同様に、資産もモニタリングやスキャンツールを使って発見し、関連するメタデータを収集する必要があるかもしれません。

サービス

サービスは通常、ビジネス情報システムをサポートする機能を提供し、またそれ自体が保護サーフェスでもあります。サービスは多くの場合、アイデンティティとネットワーク／環境の柱の一部であり、自動化、オーケストレーション、可視化、分析などの横断的な機能を提供するものとして特徴付けられます。

ビジネスと技術的な専門知識を応用することで、組織は情報とビジネスプロセスを作成、管理、最適化することができます。現代の企業では、これはSaaS（Software as a Service）のようなクラウドベースであったり、アプリケーション間やAPI（Application Program Interface）であったり、DNS（Domain Name System）のような一般的な用途であったりします。アプリケーションはサービスも提供します。例えば、DNSサービスはIPアドレスとホスト名/URL間のマッピングを提供し、これがなければエンドユーザーはURLの代わりにIPアドレスをブラウザに入力する必要があります。DNS、DHCP、SMBなどのサービスは、アプリケーションやネットワークにサービスを提供します。これらのサービスの機密性、完全性、および可用性に影響が及ぶと、結果的にこれらの柱にも影響が及ぶことになります。例えば、DNS ポイズニングはアプリケーションの利用者を悪意のあるホスト名/URL に誘導し、データ/クレデンシャルの流出につながるかもしれれません。

- ID およびアクセス管理は、人間および人間以外のエンティティが資産にアクセスし、利用者がアプリ ケーション取引を行うためのチャネルを提供します。また、アイデンティティおよびアクセス管理は、ゼロトラストのもう 1 つの機能であるアクセ スを許可する前の認証と認可も提供します。この時点で、機密性、完全性、およびある程度データの可用性が、アイデンティティおよびアクセス制御の乱用によって損なわれる可能性があることを覚えておくことが重要です。
- ネットワークの境界は、もはやオンプレミスに限定されるものではなく、クラウドサービス、ネットワークサービス、セキュアなデータや資産、アプリケーション、サービスへと拡大しています。ネットワークとネットワークデバイスは、境界セキュリティとネットワークセグメンテーションサービスを提供します。マイクロセグメンテーションとナノセグメンテーションは、ラテラルムーブメントの移動を制限・防止し、その結果、不正なアクター（人間や人間以外のエンティティ）へのアクセスを制限します。
- 自動化とオーケストレーションは、データへのアクセス権限に関するポリシーの決定を自動化し、そのポリシーの実施をリアルタイムで自動化します。
- 可視性と分析により、人間および人間以外のアイデンティティによってデータに対して行われたすべてのアクセス要求に対する洞察を提供します。デバイス、データ、ネットワーク、アイデンティティ、サービスなど、すべてのコンポーネントを発見、分析、可視化し、それらがどのようにアクセス可能で、どのようにアクセスされているかを把握することで、 保護サーフェスを定義するのに役立ちます。
- ガバナンスは、ゼロトラスト原則に対する企業のセキュリティリスクを可視化し、柱内および柱を横断するサイバーセキュリティポリシー、手順、プロセスからの支援によってリスクを管理します。

NSTAC、CISA成熟度モデルと保護サーフェス

National Security Telecommunications Advisory Committee (NSTAC) Report to the President on Zero Trust and Trusted Identity Managementでは、付録Aにゼロトラスト実装プロセスステップの成熟度の概要を示しており、成熟度が高いほど自動化レベルが高くなります。

	成熟段階	初期段階(1)	繰り返し可能 (2)	定義済 (3)	マネージド (4)	最適化 (5)
	概要と特徴	この初期段階では文書化されておらず、プロセスも定義されていないため、その場しのぎで行われます。成功は個人の努力次第です。	プロセスは文書化され、初期段階で学んだ教訓を生かして、予測可能な再現性があります。	成功のためのプロセスが定義され、文書化されています。	プロセスが監視・管理され、有効性が測定可能です。	継続的な最適化にフォーカスされています。
5ステッププロセスのステップ	**1.保護サーフェスを定義します**	DAASエレメントが不明であるか、手動で見つけます。データの分類は行われていないか、不完全です。	DAAS要素を発見し分類するための自動化ツールの使用は始まっていますが、標準化されていません。	データ分類のトレーニングとプロセスが導入され、成熟しつつあります。保護サーフェスの発見が自動化されるようになります。	新規または更新されたDAASエレメントは即座に発見され、自動化された方法で正しい保護サーフェスに割り当てられ、分類されます。	発見と分類のプロセスは完全に自動化されています。
	2.トランザクションフローのマッピング	フローはインタビューおよびワークショップに基づいて概念化されます。	従来のスキャンツールとイベントログを使用して、おおよそのフローマップを作成します。	フローマッピングプロセスが導入され、自動化されたツールが導入されてます。	自動化ツールが正確なフローマップを作成し、すべてのフローマップをシステム所有者と検証します。	トランザクションフローはリアルタイムですべての拠点に自動的にマッピングされます。

図 6.NSTACのゼロトラスト実施成熟度レベル

US Cybersecurity and Infrastructure Security Agency (CISA) は、サイバーセキュリティプログラムと能力を進化させ、運用するすることで米国行政機関を支援し、サイバーセキュリティリスクを理解、管理、削減する米国の取り組みを主導しています。*CISA のゼロトラスト（ZTMM V2）*は、急速に進化する環境と技術状況の中で、ゼロトラストに関連する継続的な近代化努力を達成するための段階的アプローチを提供します[3]。

下表は、保護サーフェス（DAAS）のエレメントに関連するCISAの柱と成熟度モデルの整合性を示しています。

3 https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

柱	サーフェス DAAS エレメント	従来	初期	高度	最適
データ	データ	データの所在に関する限られた知識	ビジネスプロセスにとって重要なデータが、サポートするシステムとともに存在する場所	ビジネスクリティカルなデータとそれをサポートするシステムの場所を把握し、手作業で保護サーフェスにマッピングします。	組織内のすべてのデータエレメントが、自動化された方法で保護サーフェスにマッピングされます。
アプリケーションとワークロード	アプリケーション	アプリケーションの機能やサポートサービスに関する限られた知識。 保護サーフェスの概念の欠如	重要なビジネスプロセスは、アプリケーション、サポートサービス、データエレメントを認識しています。	すべてのビジネスプロセスは、部門内のアプリケーション、サポートサービス、データエレメントを認識しています。保護サーフェスのマッピングは手作業です。	すべてのアプリケーション、それをサポートするサービス、およびデータエレメントは、自動化された方法で保護サーフェスにマッピングされます。
デバイス	資産	資産とその上で動作するアプリケーションに関する限られた知識。 資産に保存されたデータに関する限られた知識。	技術チームは、プロアクティブな方法で資産を管理し、アプリケーションのインベントリを維持し、永続化されたデータの分類を理解します。しかし、保護サーフェスの概念はありません。	資産とアプリケーションはインベントリ化され、資産に保存されたデータは分類されます。そして、保護サーフェスに手動でマッピングされます。	ビジネスや技術チームは、プロアクティブに、すべての資産、アプリケーション、データを、自動化された方法で保護サーフェスにマップされます。
ネットワーク	資産	大きなペリメーター／マクロセグメント	重要なワークロードの初期分離	保護サーフェスのマイクロセグメントへの手動による隔離と配置の拡大	保護サーフェスは、分散したマイクロセグメントに自動的に配置されます。

アイデンティティ	サービス	暗黙の信頼	アイデンティティとアクセス管理チームは、アプリケーション、サービス、資産の一部であるアイデンティティを認識していますが、データへのアクセスについては認識していません。	アプリケーション、サービス、資産、データの一部であり、保護サーフェスにマッピングされたアイデンティティを認識します。	保護サーフェスの継続的検証/コンテキストベースのアクセス制御。

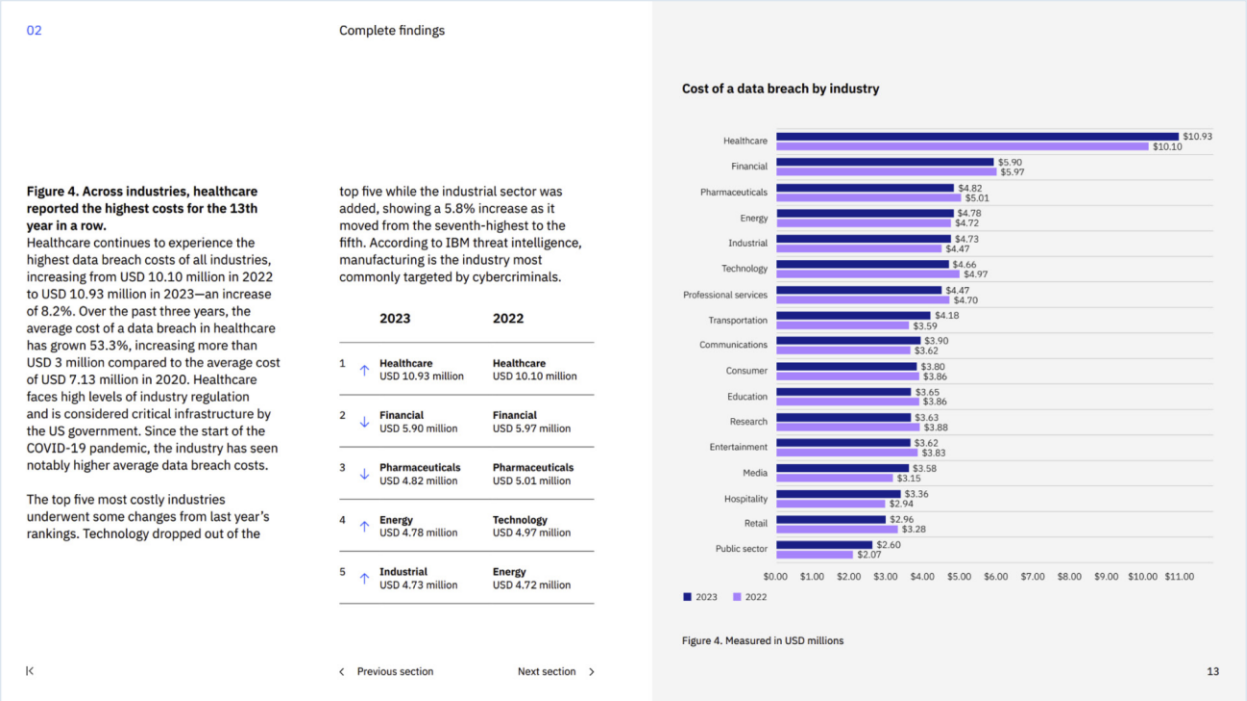
表2：ゼロトラストの柱と保護サーフェスのCISA成熟度レベルとの整合性

保護サーフェスの侵害がもたらすリスクと影響

重要なビジネス資産には様々な形態があります。多くの企業にとって、それはビジネスデータやアプリケーションでしょう。また、化学プラントや水処理プラント、医薬品の製造ラインなど、重要なインフラや運用技術も含まれます。

データと情報は様々な方法で収益化され、武器化されます。そのため、データは、流出（侵害）やランサムウェアによる暗号化など、しばしば主要な標的となります。
リスクと潜在的な影響を理解することは、ステップ1の不可欠な部分であり、ZT導入の優先順位付けに役立ちます。いくつかの例を挙げて説明しましょう。

次ページの画像は、IBMの Ponemon レポート（URL）から引用しています。このレポートは、様々な業界におけるデータ侵害のコストを記録しており、データ侵害の広がりを描いています。このような情報漏えいを確実に防ぐために、組織はデータの安全性を確保し、保護します。



02

Complete findings

Figure 4. Across industries, healthcare reported the highest costs for the 13th year in a row.
Healthcare continues to experience the highest data breach costs of all industries, increasing from USD 10.10 million in 2022 to USD 10.93 million in 2023—an increase of 8.2%. Over the past three years, the average cost of a data breach in healthcare has grown 53.3%, increasing more than USD 3 million compared to the average cost of USD 7.13 million in 2020. Healthcare faces high levels of industry regulation and is considered critical infrastructure by the US government. Since the start of the COVID-19 pandemic, the industry has seen notably higher average data breach costs.

The top five most costly industries underwent some changes from last year's rankings. Technology dropped out of the top five while the industrial sector was added, showing a 5.8% increase as it moved from the seventh-highest to the fifth. According to IBM threat intelligence, manufacturing is the industry most commonly targeted by cybercriminals.

	2023	2022
1 ↑	**Healthcare** USD 10.93 million	**Healthcare** USD 10.10 million
2 ↓	**Financial** USD 5.90 million	**Financial** USD 5.97 million
3 ↓	**Pharmaceuticals** USD 4.82 million	**Pharmaceuticals** USD 5.01 million
4 ↑	**Energy** USD 4.78 million	**Technology** USD 4.97 million
5 ↑	**Industrial** USD 4.73 million	**Energy** USD 4.72 million

Previous section Next section

Cost of a data breach by industry

Figure 4. Measured in USD millions

13

図7： Cost of a Data Breach Report 2023 - 参照：(https://www.ibm.com/reports/data-breach?)

[redacted]/BLOG-SINGLE[redacted] SLUG CROSS SITE SCRIPTING

ENTRY EDIT HISTORY DIFF JSON XML CTI

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.2	$0-$1k	0.11

Summary info edit

A vulnerability, which was classified as problematic, was found in [redacted] This affects an unknown part of the file */blog-singl[redacted]* The manipulation of the argument *slug* leads to cross site scripting. This vulnerability is uniquely identified as [redacted] It is possible to initiate the attack remotely. Furthermore, there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.

Details info edit

A vulnerability, which was classified as problematic, has been found in [redacted] Affected by this issue is an unknown functionality of the file */blog-single[redacted]* The manipulation of the argument `slug` with an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to [redacted] The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. Impacted is integrity.

The weakness was presented 07/23/2023. This vulnerability is handled as [redacted] Successful exploitation requires user interaction by the victim. Technical details as well as a exploit are known. The MITRE ATT&CK project declares the attack technique as [redacted]

It is declared as proof-of-concept. The vendor was contacted early about this disclosure but did not respond in any way. By approaching the search of inurl:blog-single[redacted] it is possible to find vulnerable targets with [redacted]

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

図8： Cost of an exploit to carry out a breach　参照：https://vuldb.com/)

上の図は、オープンソースの脆弱性管理データベースからのものです。この図は、データ流出のために悪用された脆弱性に関するものです。

上の例では、もしデータ流出が目的でなければ、クロスサイトスクリプティングは悪用の焦点ではなかったかもしれません。file/blog-singleを使用するアプリケーションは脆弱ではないでしょう。

上記の概念は、ITシステムによって生成され、ITシステムのために生成されるデータに関連するものです。しかしながら、オペレーショナルテクノロジー（OT）やモノのインターネット（IoT）もデータを生成・消費し、組織にとって重要なオペレーション機能を実行することが多いため、侵害されるとさまざまな種類の影響が生じる可能性があります。例えば、このようなシステムは兵器化される可能性があります。OT システムと IoT システムは、データがどこでどのように生成され、取得されるか、また技術がどのような機能を実行するかに関して若干異なります。個別のOTおよびIoTコンポーネントでは、データの生成／消費するエンドポイントは通常、データを取得する資産から離れた場所にあります。例えば、放射能検出器は放射性物質からの信号を検出します。検出器が危険にさらされると、放射性信号を検出できなくなり、職員が有害な放射線にさらされるという悲惨な結果につながる可能性があり、放射性物質が不注意で施設内外に放出されたり密輸されたりする可能性があります。

同様に、必要なフッ化物濃度の入力を制御するためのアプリケーションをホストしている資産に侵害が生じた場合、その場所の水が汚染される可能性があります。この例を下図に示します。

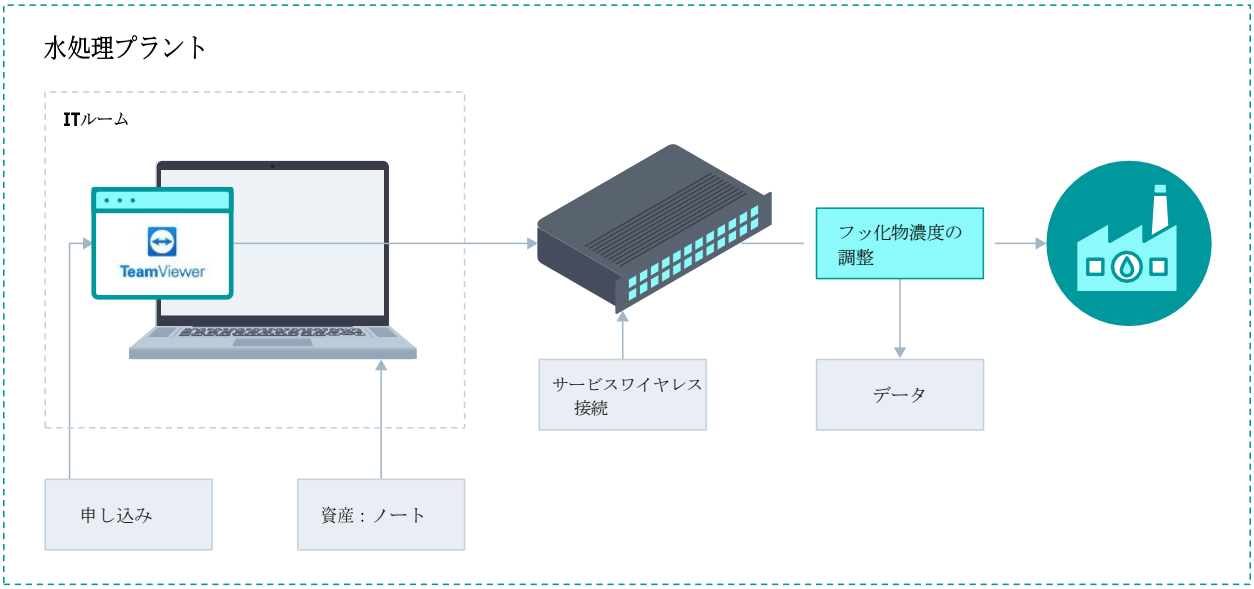


図9：浄水場の保護サーフェス

機密性、完全性、可用性に関する要件と潜在的な影響を理解することは、各保護サーフェスに関連するリスクを特定し、評価することにつながります。例えば、機密データが漏洩するリスクを考慮する必要があります。また、悪意のある行為者（ランサムウェアなど）が許可なくデータを暗号化し、可用性要件に影響を及ぼす可能性も考慮する必要があります。同様に、不正な行為者が浄水場の水のフッ化物成分を増減させた場合、完全性（製品の品質）の要件に影響を与えます。保護サーフェスに関連するリスクを特定する重要な方法は、機密性、完全性、および可用性の要件と、さまざまな潜在的な侵害や停止による潜在的な影響を考慮することです。

データ分類の適用

データは多くの保護サーフェスにとって中心的なものであるため、保護サーフェスに対応するリスクは潜在的なデータ侵害の影響によって異なります。リスクの特定と分類に一貫したアプローチを確実に適用するために、データは、財務上の損失、レピュテーションの損失、あるいはその他様々な潜在的な影響の観点で影響を表すカテゴリに分類することができます。以下にデータ分類の例を示します。

規制および安全要件に基づくデータ分類：

a. 例1
    1. 放射性
    2. 毒性
    3. 未分類
b. 例2
    1. 危険
        i. 公共の人的財産の安全
    2. 機微
        i. 知的財産、企業秘密
    3. 規制下
        i. 通信、テレメトリ、個人識別可能情報(PII)、カード決済情報(PCI)、保護対象保健情報(PHI)
    4. 事業成果や価値に基づく目的別の分類
        i. 知的財産

データが分類された後、ゼロトラストの旅がどうなるかは、該当する保護サーフェスの重要性を組織がどのように評価し、ゼロトラストの実装において対応するリスクにどのように対処するかによって決まります。NIST SP 800-60は、情報の分類と関連するリスクの特定に関する有用なガイダンスを提供しています。

攻撃サーフェスと保護サーフェス

NISTは攻撃サーフェスを「攻撃者がシステム、システム要素、または環境に侵入したり、影響を与えたり、そこからデータを取り出したりすることができる、システム、システム要素、または環境の境界上の点の集合」と定義しています。

保護サーフェスは有形であり、明確な境界を持つのに対し、攻撃サーフェスは無形であり、BYODや新しいサービスの導入などでの継続的な変化に起因して動く標的です。保護サーフェスと攻撃サーフェスの違いは、保護サーフェスは変化しない、または資産の追加による最小限の変化のみが発生するのに対し、攻撃サーフェスは新しい脆弱性や攻撃ベクトルが出現するなどして頻繁に変化することです。

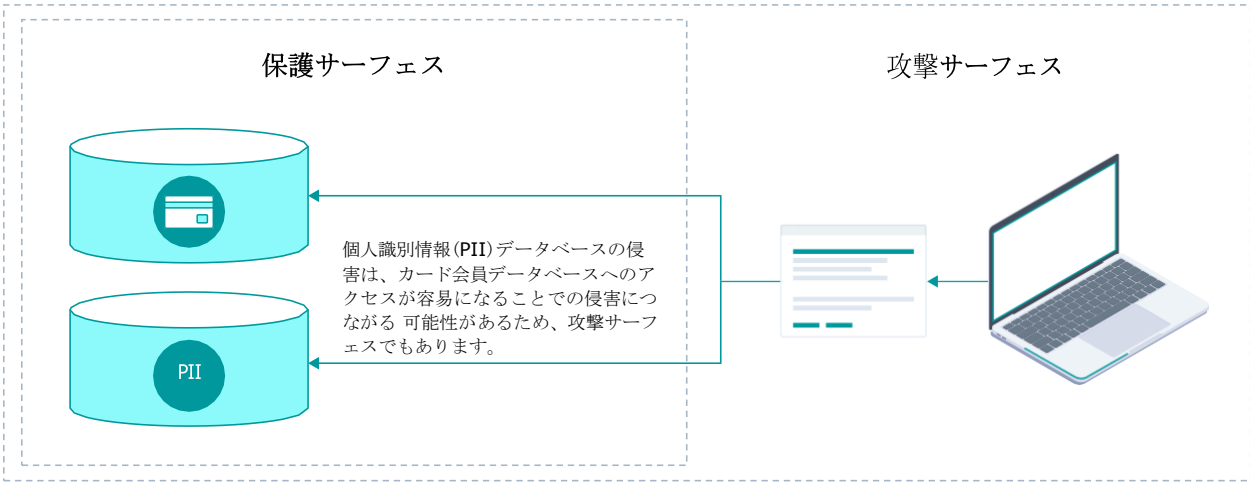


図10：攻撃サーフェスから見た保護サーフェス

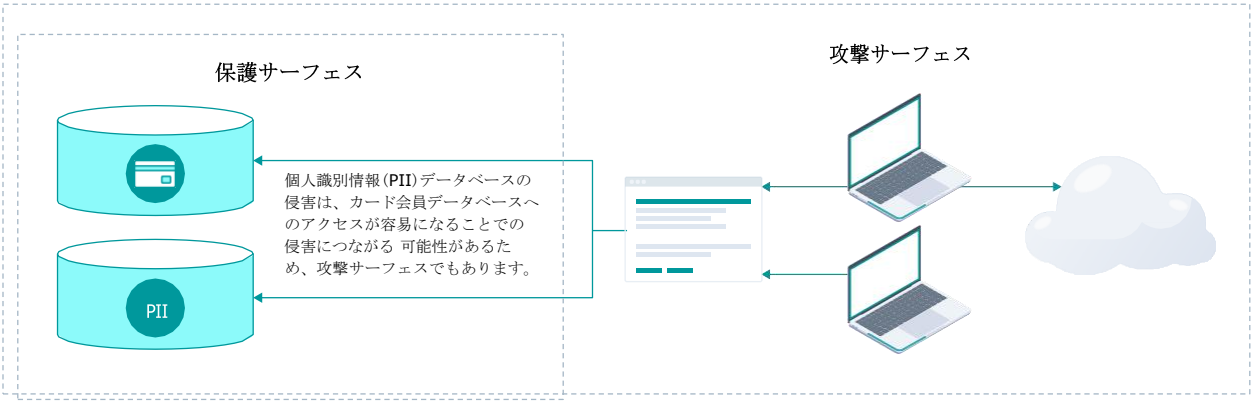


図11：攻撃サーフェスに追加された資産では、保護サーフェスは変更されない

保護サーフェスはシステムのインサイドアウトの視点となるもので、攻撃サーフェスはシステムのアウトサイドインの視点となるものです。

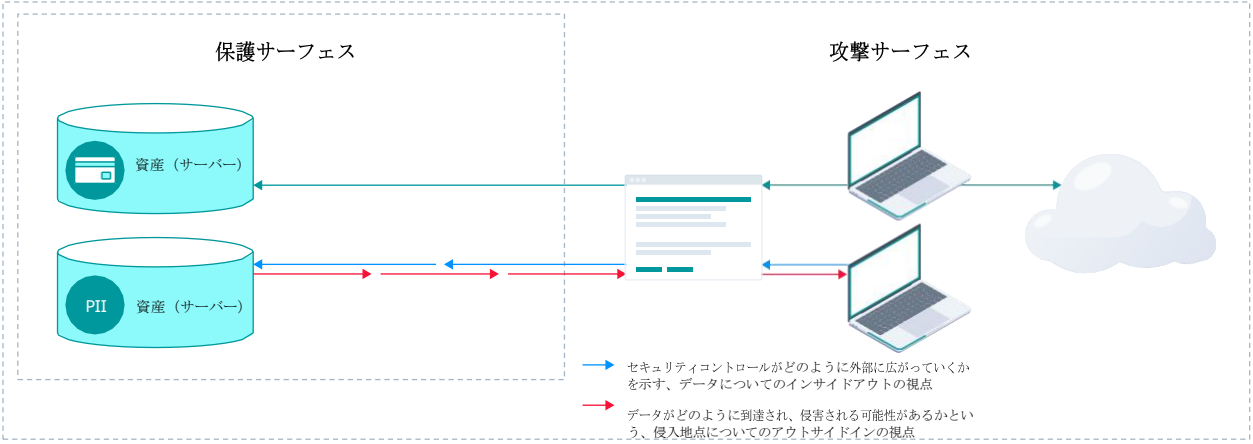


図12：「保護サーフェス」と「攻撃サーフェス」は互いに補完・追加し合う

保護サーフェスと攻撃サーフェスは互いに補完し合うものです。保護サーフェスが保護すべきものを特定するのに役立つ一方、攻撃サーフェスは、保護サーフェスがどのように侵害される可能性があるか、攻撃がどのように実行される可能性があるかを特定し、組織の保護サーフェスを最適に保護するのに役立ちます。

保護サーフェスが定義された後の展望

保護サーフェスが定義され次第、ゼロトラストの第2ステップにおいて、関連するトランザクションフローが保護サーフェスの中及びその出入りにマッピングされなければなりません。これには様々なDAASの要素が、その他のネットワーク上のリソースとどのように相互作用するかの理解形成を含みます。保護サーフェスは、1つまたは複数のビジネスプロセスと連携します。許可されたユーザーは、ビジネスプロセスを利用、実行、管理し、これは各保護サーフェスに関連するメタデータとして識別され、文書化される必要があります。ゼロトラストの第2ステップ「トランザクションフローのマッピング」では、ユーザー数とデータアクセス情報が必要です。トランザクションフローをマッピングすることで、ビジネスの情報システムがどのように動作するかを理解できます。(NSTAC Report to the President on Zero Trust and Trusted Identity Management）。マッピングはまた、第3および第4ステップで必要なコントロールをどこに配置するかを直接示します。

トランザクションはアプリケーション、サービス、またはこれら双方を通じてデータへのインターフェースを提供します。トランザクションには、データの取得、処理、およびデータの永続化が含まれます（ただし、これらに限定されません）。

アクセスを必要とするデータ処理には、以下の例のようなタスクが含まれます：

- 消費者がアプリケーションにデータを入力して買い物をします、消費者が保険商品の見積を取得します
- 当局が銀行金利に変更を加えます

- 財務チームが請求書に応じてサプライヤーに支払いを行います
- アプリケーションがアプリケーション内で行われたトランザクションに応じたイベントを生成します

以下にトランザクションフローの例を2つ示します：

> - データを使って行われるトランザクション：
>   - データの取得、処理、永続化を行うトランザクションの実行を支援する、データとのインターフェースを提供するアプリケーション。
>   - データ（移動）を取得し、そのデータをアラートに変換するモーションディテクターなどのOT。
>   - 脈拍数をカウントし、一定時間内の消費カロリーに換算する健康アプリ。
> - データをサポートするために保護サーフェス間で行われるトランザクション：
>   - データを永続化するためのアプリケーションサービスによるDNSサーバーを使用したデータベースサーバーの検出。
>   - IDおよびアクセス管理システムを使用して、データを管理するためにデータベースサーバーにログインするデータベース管理者。
>   - IoTベースのデスク監視システムの管理コンソールにログインし、使用中のデスクを報告する管理者。
>   - アプリケーションが、トランザクションを要求通りに動作させるためにサービスのサポートを要求します。例えば、DNSサーバーを介したアプリケーションの検出、可視性、トラブルシューティングや調査のための分析など。

Zero Trust Network Working Group EnvironmentとApplications/Workloads Working Groupは、共同で「Step 2, Mapping the Transaction Flows」を詳しく説明する文書を作成し、公表する予定です。

全体として、組織内の保護サーフェスを理解し文書化するには、保護サーフェス間の関係、各保護サーフェスの役割、および組織にとっての重要性を確立した上で、適切なセキュリティ対策を実装し、脅威や攻撃を監視し、インシデントに迅速かつ効果的に対応するという包括的なアプローチが必要です。

結論

保護サーフェスを定義することは、ゼロトラストの旅の第一歩に過ぎませんが、そこからビジネス上のメリットが生まれ始めます：

- 可視性の向上：組織において保護サーフェスの定義の旅に出ることは、組織にとって重要なデータ、アプリケーション、資産、およびサービスを発見することにつながります。組織は目に見えるものだけを保護することができ、DAASの要素を見つける旅に出ることは、この可視性の第一ステップを提供します。
- セキュリティの向上：保護サーフェスの定義により、トランザクション、データ、資産、アプリケーション、およびサービスを保護することで、セキュリティ管理をビジネス資産に近づけることができます。
- コンプライアンスの向上：多くの規制や標準（HIPAAや一般データ保護規則（GDPR）など）は、機微データを保護するために強力なセキュリティ管理を実装することを組織に求めています。保護サーフェスを定義することで、組織はこれらの要件に準拠していることを、データを保護するために実装されたセキュリティコントロールによって証明できます。
- コストの削減：組織の重要な保護サーフェスをすべて定義し、必要なセキュリティコントロールを実装することで、組織はデータ漏洩を減らすことができます。これにより、情報漏えいの一次的または二次的なコストを削減することができます。
- ビジネスレジリエンスの向上：ビジネスオペレーションに求められる重要な保護サーフェスを理解することで、焦点の明確化、取り組みへの専念、および障害時の強固なサポートが可能になり、全体的なビジネスレジリエンスが強化されます。

本書では、保護サーフェスを定義し、その構成要素（情報システムとそれらがサポートするビジネスプロセスを構成するDAAS要素）を明確にしました。また、ゼロトラスト実装プロセスの開始、サーフェスの定義と保護に関する重要な側面、およびその後のステップでそれらを保護するための知見を提供しています。さらに、その議論はDAAS要素、成熟度モデルの適用、およびゼロトラストの実装と運用に至るまでのトランザクションフローのマッピングに対応しています。本書では、ITシステムのみならず、OTやIoTを包含する保護サーフェスの広範な適用について強調しています。読者にとって、ゼロトラストの旅を開始し、遂行するための貴重なガイダンスとなるでしょう。

参考文献

NSTAC Report to the President on Zero Trust and Trusted Identity Management

- Definition of Protect Surface: Refer to Page 6
- Definition of Attack Surface: Refer to Page 16
- Appendix A for Protect Surface Maturity Model

CSA Zero Trust Advancement Center

- CSA Zero Trust Advancement Center

John Kindervag Presentation recordings & blogs

- ZT Implementation and Guiding Principles Briefing by John Kindervag
  Passcode: ZTimplement101!
- ZT Data Protection and Privacy Briefing by John Kindervag
  Passcode: DataPillar7!
- Palo Alto Blog with "The Zero Trust Learning Curve"

CISA Maturity Model V2

- CISA Zero Trust Maturity Model V2

US DoD Reference Architecture & Strategy

- Department of Defence Zero Trust Reference Architecture
- Department of Defence Zero Trust Strategy

NIST Special Publications

- NIST SP 800-207, Zero Trust Architecture
- A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments
- Implementing a Zero Trust Architecture figure 1 page 54, 2nd preliminary draft
- Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-60r2 initial working draft, Guide for Mapping Types of Information and Information Systems to Security Categories (enhanced draft)

IBM Ponemon Report

- IBM Ponemon Report

Venturebeat

- Venturebeat's report on clouds adopting Zero Trust

Vulnerability Database owned by Pyxyp @https://pyxyp.com/

- Vulnerability Database (vulnDB)

Gartner

- Gartner Report on Zero Trust

DHS LinkedIn Article

- Importance of defining a Protect Surface