シスコ ゼロトラスト アドバイザリ サービスのご紹介

シスコシステムズ合同会社
カスタマー エクスペリエンス（CX）

ゼロトラストの展開に向けて

ゼロトラストって？

何をすればいいんだろう？

何をしたらゼロトラストを実現できたといえるの？

ゼロトラストは概念であり、
実現のために特定のソリューション・製品
を使わなければならないといった制約はない

シスココンサルティングサービスが、
ゼロトラスト実現に向けたの計画化をサポート

サービス内容

- 本サービスの位置付け
- アドバイザリ サービス概要
- 評価基準
- 評価方法
- プロジェクトの進め方
- スケジュールと役割分担
- 評価報告書

CX セキュリティ サービス ポートフォリオ

MDR

BCS

Talos IRR

Customer Success

Talos IRR

マイグレーション
サポート

ゼロトラスト
アドバイザリ

ペネトレーション
テスト

標的型攻撃耐性評価
サービス

IoT/OTセキュリティ
アセスメント

セキュア デベロップ
メント ライフサイクル

設計 / 構築サービス

ゼロトラスト アドバイザリ サービス概要

❖ ライトプラン

現状のセキュリティ 状況をアセスメントにより点検し、今後、お客様がゼロトラストの検討を進める判断材料をご提供。
今現在のセキュリティ対応状況とゼロトラストへの準備状況の確認を目的とする。

❖ スタンダートプラン

上記のアセスメントに加え、目指すべき姿をヒアリングした上で、ゼロトラスト実現に向け、どのようにアプローチしていけばよいのか、その計画化も目的とする。お客様要件も踏まえたアセスメントとロードマップの策定を実施。

		ライトプラン	スタンダードプラン
ご提供サービス	アセスメント	○	○
	要件ヒアリング (目指すべき姿の確認)		○
	定例会実施	最大3回	最大4回
成果物内容	アセスメント (現状評価とギャップ分析結果)	○	○
	課題と推奨	○	○(お客様要件を考慮)
	ロードマップ		○
その他	想定サービスご提供期間*	5～7週	8～10週

*ご提供期間は、サービスご提供前にお客様と合意の上確定するため、目安となる。

本サービスの位置付け

アドバイザリ サービスとは

本サービスは、ゼロトラストの導入に向け、設計や実装のインプットとなる計画、および要件整理のフェーズに該当します。以下のような課題や期待をお持ちのお客様を対象とした、コンサルティング サービスです。

対象

計画
課題・要件整理

アーキテクチャ
設計

構築
テスト

運用保守

最適化

- ゼロトラスト導入を検討しているが、何をしてよいか、何から実施すればよいかわからない
- ゼロトラストの導入を効率的に実施したい
- グローバル基準と照らし合わせ、自社のセキュリティ対応状況を可視化し、把握したい
- 働き方改革でリモートワークを導入するがセキュリティ対策に不安がある
- 中長期計画を立案しており、そのインプットとして活用したい

ゼロトラストアドバイザリサービス概要

スタンダードプランのみ対応

目標	目指すべき姿	対応状況確認	計画化 ロードマップ策定
サービス概要	現状評価	ギャップ分析 課題と対応方針	ロードマップ 実施タスクと計画 アーキテクチャ
納品物	ゼロトラストアセスメント報告書 分析と評価結果		ロードマップ

ゼロトラスト アドバイザリ サービス概要 (スタンダードプラン)

目標

1. ゼロトラストへの対応状況の確認
2. ゼロトラスト導入計画化 (ロードマップ策定)
   - 目指すべき姿の検討
   - 目指すべき姿の実現に向け、どのような課題があり、それに対しどのように対応するのか、ゼロトラストの展開を計画化し、迅速な導入へのインプットとする。

サービス概要

1. 現状評価
   NIST、およびシスコ独自 Zero Trust Architecture のフレームワークを活用したゼロトラストへの対応状況を確認
2. ギャップ分析
   お客様要件も含め、そのギャップを分析し、レーティングの実施および課題を明確化
3. ロードマップ
   実施すべきタスクの洗い出しとその優先付けをおこない、ゼロトラストの展開を計画

納品物

ゼロトラスト アセスメント報告書
- アセスメント結果
- ロードマップ

サービス対象

アセスメント範囲

部分的な 確認ではなく、システム全体を確認対象とするため、広範囲に自社のセキュリティ対応状況が把握できます。

- リソースにアクセスするユーザ / デバイス、すべてを識別することは可能ですか？
- いつ、誰が、どのようにアクセスしたか分かりますか？
- アプリケーションの異常を検知して、分析できますか？
- マルウェア感染がリソースにアクセスできますか？

評価基準

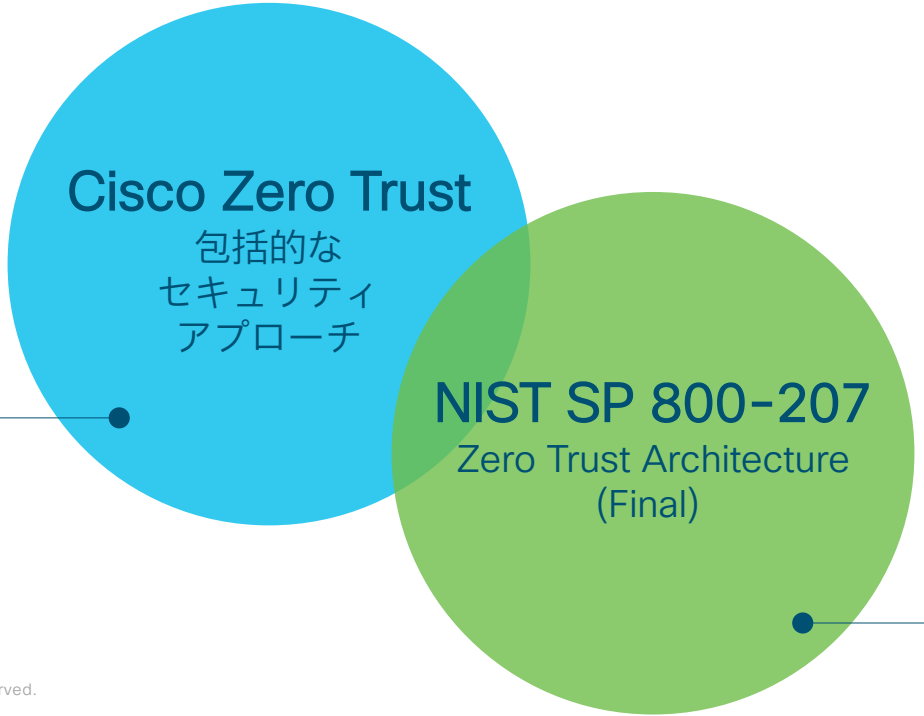
シスコ ゼロトラストと NIST 標準の考え方を取り入れて評価を実施

- シスコ ゼロトラストは、エンドポイント、ネットワーク、データセンタやクラウドなど、セキュリティ対策において必要な領域をカバーした包括的なアプローチです。これにワールドワイドにサービスを展開するシスコ カスタマー エクスペリエンスのコンサルティング経験から得られた知見も加味して評価を実施します。
- NIST の定義するゼロトラスト アーキテクチャ (SP800-207) の考え方を取り入れて、現状評価およびギャップ分析を進めていきます。NIST を参照する主な理由は、以下の通りです。
  - NIST SP 800-207では、ゼロトラストへの対策状況をハイレベルな観点で定義しており、本サービス提供の目標にも合致している。
  - 国際標準として認知されており、グローバルの多くの企業が取り入れている業界基準となるガイドラインである。

補足資料：なぜ NIST、他社と何が違うのか？

第三者視点としてのグローバルスタンダードとなるNIST Zero Trust Architectureのガイドラインを参照し、シスコの包括的な視点 (ワークフォース・ワークロード・ワークプレイス) を掛け合わせ、独自のアセスメントフレームワークを作成し、幅広い視点で現在のセキュリティ対応状況を確認できる。

- エンタープライズアーキテクチャを対象とした**包括的な**アプローチ
- 特にネットワークに強み
- 社内への展開実績より、NIST の抽象的なところをカバーできる



- ゼロトラストを**第三者機関**が定義している唯一に近いガイドライン
- NISTは**グローバルスタンダード**で強い影響力がある
- 認証のみならず、ネットワークに関する詳細化がされている

評価指標と仕組み

シスコベストプラクティスとNIST SP800-207をインプットとし、評価項目を作成します。

トラストを確保すべき対象 (セキュリティ ドメイン)

1 ユーザとデバイス

- ✔ 認証済みユーザは本当に正しいか？
- ✔ 安全な状態のデバイスでアクセスしているか？
- ✔ 信頼されたデバイスでアプリにアクセスしているか？

2 アプリケーション

- ✔ 組織に必要なアプリなのか、何が稼働しているのか？ (閲覧 / 可視化)
- ✔ すべてのアプリケーションに適切なポリシーが適用されているか？

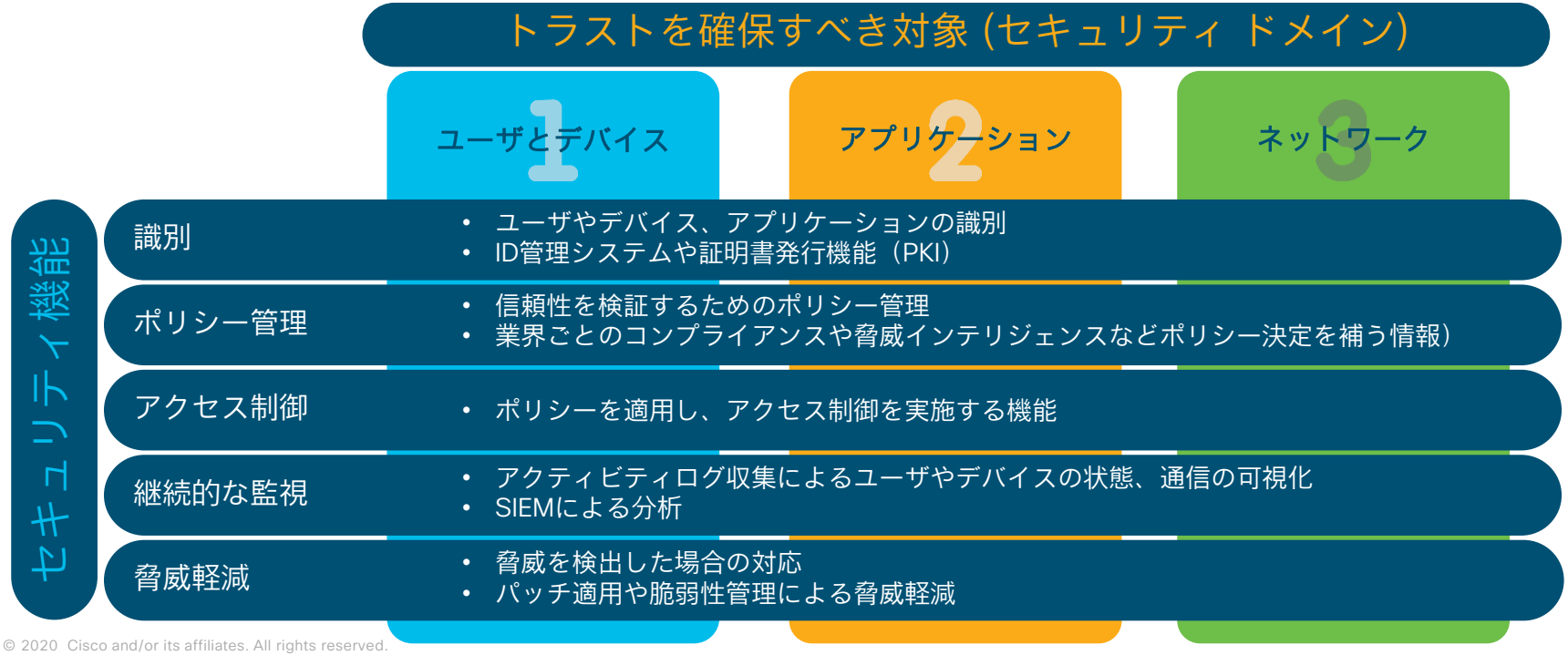
3 ネットワーク

- ✔ ユーザ/デバイスは、正しいレベルで認証され、ネットワークにアクセスしているか？
- ✔ ポリシーに基づき、ネットワークが適切に分離 / アクセス制限されているか？

セキュリティ論理ドメインとセキュリティ機能

評価指標と仕組み

シスコベストプラクティスとNIST SP800-207をインプットとし、70 近い評価項目を確認し、アセスメントを実施する 。



プロジェクトの進め方 (スタンダードプラン)

① 現状把握

お客様情報

以下の情報提供のご依頼。

1) セキュリティポリシー
2) セキュリティの実装
3) システム情報
4) ネットワーク構成

Webフォーム入力

アセスメントに関する調査項目をウェブによるアンケート形式にてご提供。お客様にて回答を入力頂く。

Web調査

② 調査・分析

ワークショップ実施

ご提供頂いたお客様情報と入力頂いた回答をもとに、弊社コンサルタントが分析を進め、目指すべき姿のヒアリング含め、ワークショップを実施。

第１回目
テーマ：ユーザとデバイス

第２回目
テーマ：アプリケーション

第3回目
テーマ：ネットワーク

インプット

ゼロトラストの考え方

Cisco Zero Trust や NIST 標準(800-207)など

③ 報告

中間報告

アセスメント結果から見えた課題と対応方針の確認、および実施すべきタスクの優先度等を確認し、計画化。

第4回目
テーマ：ロードマップ策定に向け

最終報告

中間報告の内容をインプットとし、最終報告書を作成し、ご提示。ロードマップの策定を含む。

最終報告書

プロジェクトの進め方 (ライトプラン)

① 現状把握

お客様情報

以下の情報提供のご依頼
1) セキュリティポリシー
2) セキュリティの実装
3) システム情報
4) ネットワーク構成

Webフォーム入力

アセスメントに関する調査項目をウェブによるアンケート形式にてご提供。お客様にて回答を入力頂く。

Web調査

② 調査・分析

ワークショップ実施

ご提供頂いたお客様情報と入力頂いた回答をもとに、弊社コンサルタントが分析を進め、ワークショップを実施。

第１回目
テーマ：ユーザとデバイス

第２回目
テーマ：アプリケーション

第3回目
テーマ：ネットワーク

インプット

ゼロトラストの考え方

Cisco Zero Trust や NIST 標準(800-207)など

③ 報告

最終報告

ワークショップの情報をインプットとし、最終報告書を作成、ご提示。

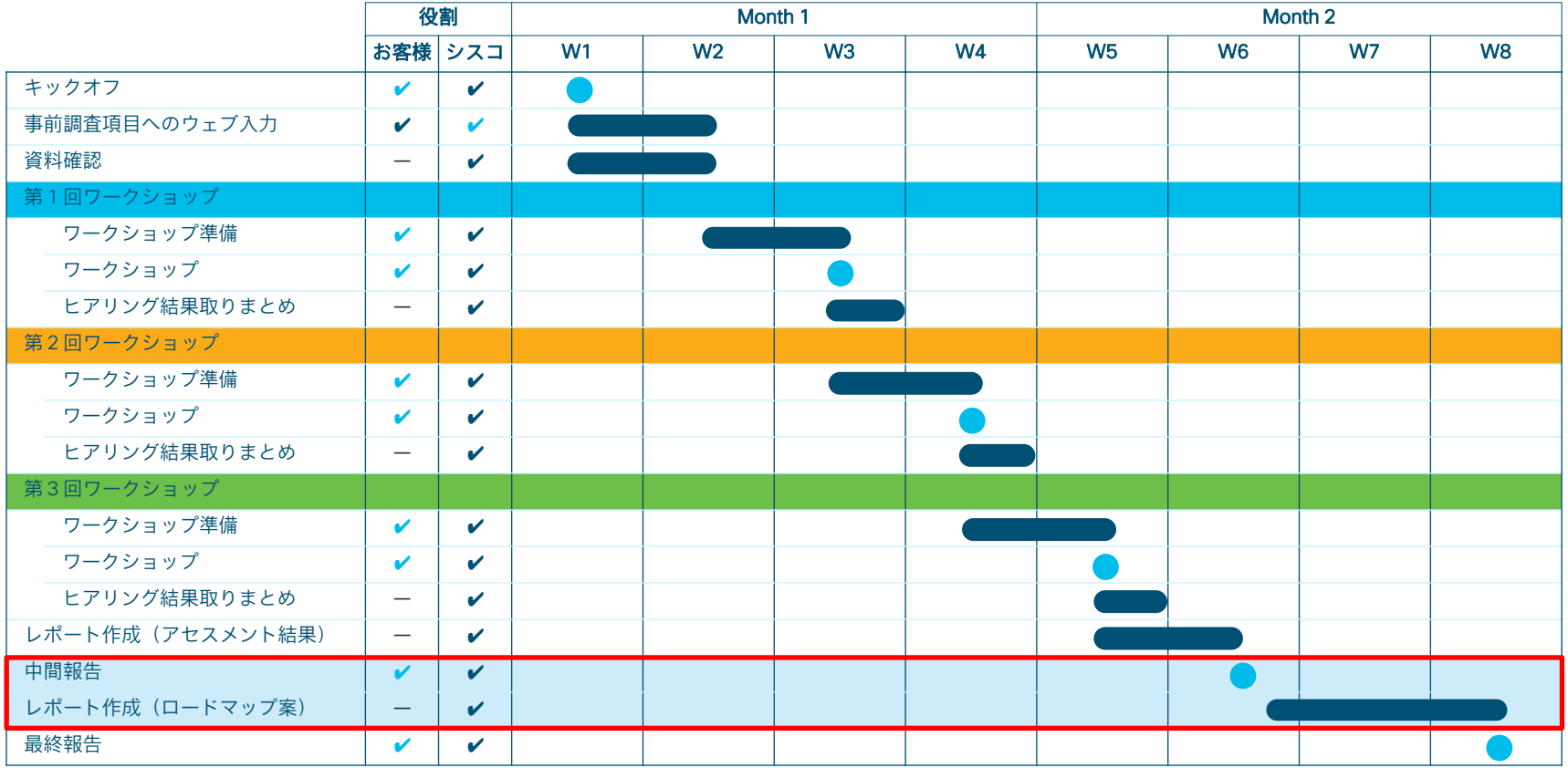
最終報告書

スケジュールと役割分担（案）

✔：作業主体　✔：作業支援

※ ワークショップは 1 回あたり最大 2 時間を想定

スタンダードプランのみ対応



	役割		Month 1				Month 2			
	お客様	シスコ	W1	W2	W3	W4	W5	W6	W7	W8
キックオフ	✔	✔								
事前調査項目へのウェブ入力	✔	✔								
資料確認	—	✔								
第 1 回ワークショップ										
ワークショップ準備	✔	✔								
ワークショップ	✔	✔								
ヒアリング結果取りまとめ	—	✔								
第 2 回ワークショップ										
ワークショップ準備	✔	✔								
ワークショップ	✔	✔								
ヒアリング結果取りまとめ	—	✔								
第 3 回ワークショップ										
ワークショップ準備	✔	✔								
ワークショップ	✔	✔								
ヒアリング結果取りまとめ	—	✔								
レポート作成（アセスメント結果）	—	✔								
中間報告	✔	✔								
レポート作成（ロードマップ案）	—	✔								
最終報告	✔	✔								

評価報告書

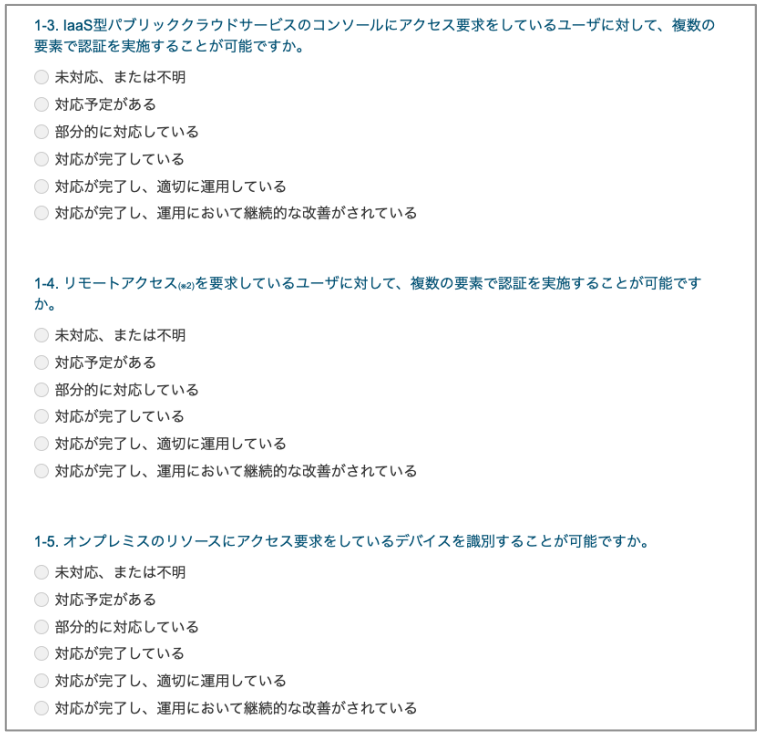
目次

1. エグゼクティブ サマリ
2. プロジェクト概要
3. ゼロトラスト評価結果
4. 課題と推奨
5. ロードマップ スタンダードプランのみ
6. ソリューション提案

※目次構成や表記は変更される可能性があります。

Webを活用したアセスメント (イメージ)

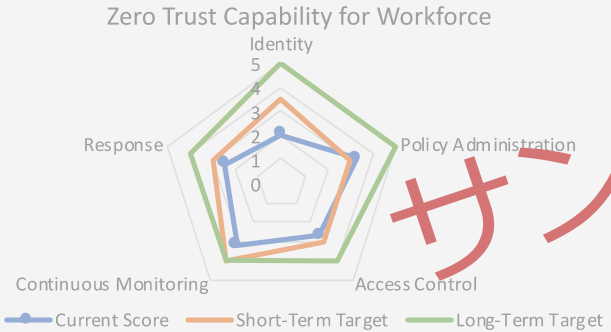
ゼロトラストアセスメントフレームワークをウェブによるアンケート形式でご提供し、事前にと回答頂き、プロジェクトの効率化も可能とする。



評価報告書イメージ (サマリー)

ワークフォースに対する評価結果サマリ

ワークフォースに対するゼロトラスト対応状況について評価した結果を以下に記載する。



セキュリティ機能	現在のスコア	短期的な目標	長期的な目標
特定	2	3.5	5
ポリシー管理	3.3	3	5
アクセス制御	2.7	3	4
継続的な監視	3.2	4	4
対応	2.5	3	4

※目標値については、4章に記載の推奨事項を実施した場合の想定値

総評
5つのセキュリティ機能のうち「特定」に関する機能が一番低いスコアを示している。これは現状クラウドサービスへのログインには多要素認証が実装されているもののオンプレミスのリソースに対するアクセスについて態（OSやパッチ適用状況など）を識別する機能が不足していること ソースへのログイン時にロールベースのアクセス制御が実施されて いるが、ユーザのアクティビティを分析する機能については不足し ている一方、モバイルデバイス紛失時に当該端末からのアクセス

評価基準

5段階の評価は以下を基準に実施する
0 - 不明・非該当
1 - 対応する機能がない初期状態
2 - 対応する機能を部分的に具備している状態
3 - 対応する機能を標準的に具備しているが、課題や制約が存在する状態
4 - 対応する機能を標準的に具備しており、運用において管理されている状態
5 - 対応する機能を標準的に具備しており、継続的な改善がされ、最適化されている状態

評価報告書イメージ (セキュリティ機能/特定)

ワークフォースに対する評価結果（特定）

セキュリティ機能「特定」における評価項目と現状を分析した結果を以下に記載する。

評価項目		
ID	評価項目	スコア
WF.ID-1	オンプレミスのリソースにアクセス要求をしているユーザに対して、複数の要素で認証を実施することが可能か	2
WF.ID-2	クラウドのリソースにアクセス要求をしているユーザに対して、複数の要素で認証を実施することが可能か	
WF.ID-3	オンプレミスのリソースにアクセス要求をしているデバイスを識別することが可能か	
WF.ID-4	クラウドのリソースにアクセス要求をしているデバイスを識別することが可能か	

現状分析		
	分析と考察	関連する評価項目
良かった点	[WF.S01]リモートアクセスを実施する際のユーザ認証やクラウドサービスへのアクセスでは多要素認証が実施されている	WF.ID-1
	[WF.S02]クラウドサービスへのログインには多要素認証が実施されている	WF.ID-2
課題	[WF.W01]オンプレミスの社内Webサーバへのアクセスはパスワード認証のみとなっているため内部ネットワークからの不正アクセス対策の検討が必要	WF.ID-1
	[WF.W02]オンプレミスのリソースにアクセスする場合も、クラウドのリソースにアクセスする場合にもデバイスのOSバージョンやパッチ適用状況を確認する機能は具備していない	WF.ID-3, WF-ID-4

評価報告書イメージ (ロードマップ)

ゼロトラスト施策の導入ロードマップ（案）

ゼロトラスト施策の導入ロードマップ（案）を以下に記載する。

お客様ビジネスを加速

ライフサイクル全体のサポート

戦略的なロードマップの展開が、IT およびビジネス課題を解決します。複雑化するシステムの設計・導入・運用、ライフサイクル全体において、継続的にご支援させて頂きます。

運用

定量的で計測可能なKPIを定義し、システム品質確保と活用

- カスタマーサクセスチーム
- 最適化
- 収集 / 分析 レスポンス

計画

実点可能な戦略的ロードマップ

- アドバイザリ
- アセスメント

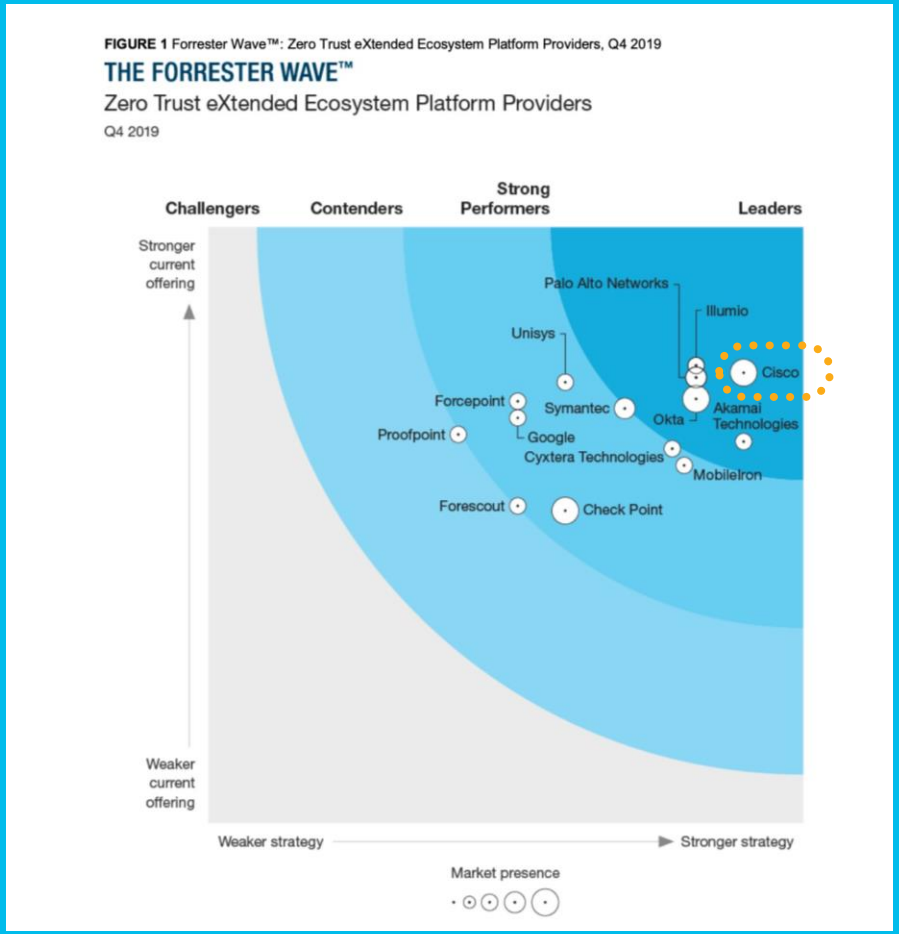
導入

安全で効率的な展開と運用の定着、および最適化

- 設計 / 導入支援
- トレーニング

シスコの優位性

ForresterWave にて、14 社中トップの評価



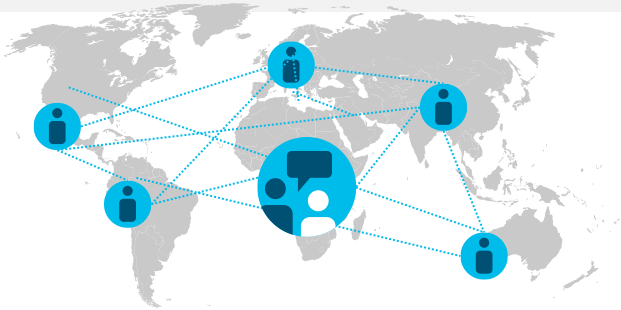
シスコ サービスの特徴と提供体制

サービスの特徴

- 製造、金融、官公庁他、多くの業種に渡る、世界各国で蓄積した経験とノウハウ
- 開発メーカならではの最新技術動向を踏まえた提案やコンサルティング力
- 成功事例に基づく知見を”シスコ ベストプラクティス”としてデータベース化
- 先進的なツール、手法、ノウハウを活用したサービス

サービス提供能力・体制

- 全世界 180ヵ国で、12,000 名のプロフェッショナルがサービスを提供
- CCIE、CCNP、PMPなど、保持資格数は25,000以上
- 国や地域を超えた情報連携、プロジェクト実施体制
- 世界最大規模の商用セキュリティ研究機関「Talos」にて全世界からの脅威情報をリアルタイムで分析
- 11 年連続で J.D. Power がテクノロジーサービスとサポート分野で「優れた会社」と認定



シスコ CX の優位性

シスコ カスタマー エクスペリエンス(CX)では、12,000人以上のプロフェッショナルが世界各地のお客様にサービスを提供し、高い評価を頂いています。

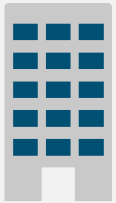
グローバルの規模と実績

エンジニアの稼働

12千 エンジニア、アーキテクト、コンサルタント数

11年 J.D. Power がテクノロジーサービスとサポート分野で優れた会社と認定

テクノロジービジョナリー



Fortune 1000の 3/4 が採用

#1 ネットワーク技術

年間 R&D 投資額 >$60億

ネットワークにおけるリーダー

有資格技術者数

導入済みネットワーク数 >5千万

180+国 17言語 でサポートを提供


CISCO