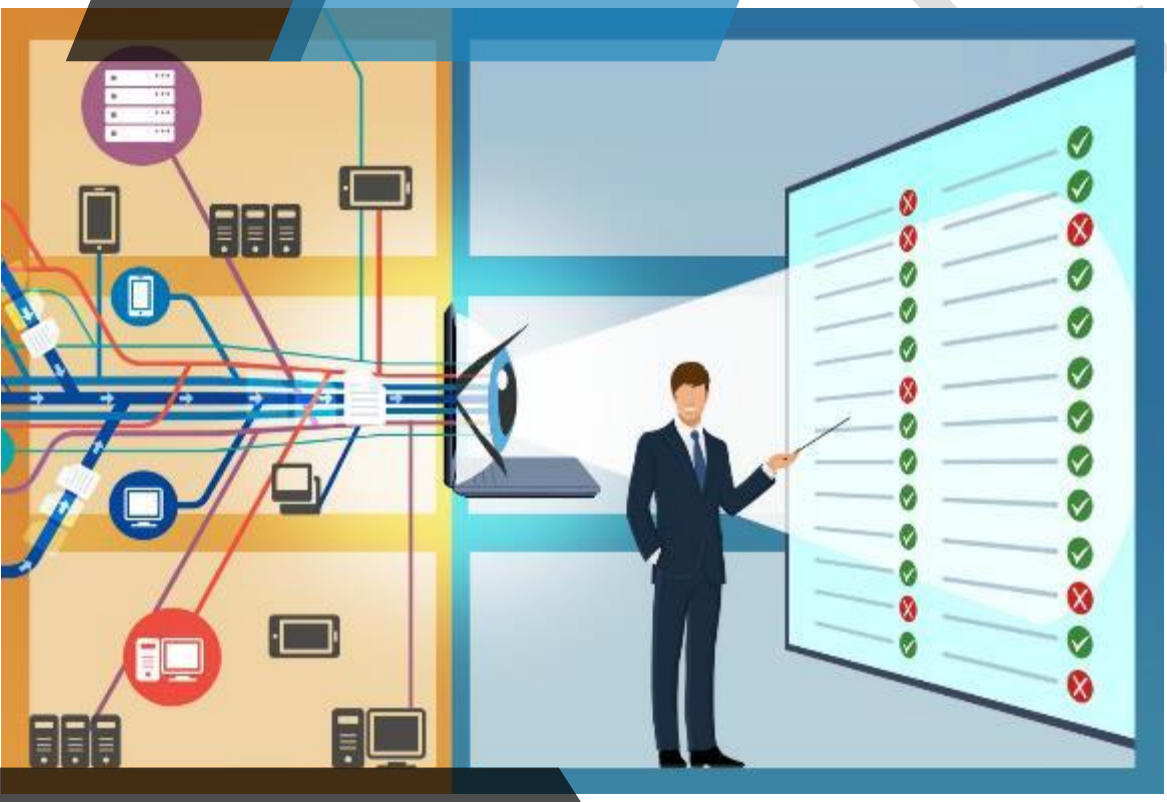
CSAT



Cloud Security Report

Contoso 株式会社様

(サンプル)

目次

1. 管理の概要

このクラウド セキュリティ レポートは、**コントソ株式会社様**向けに 2021 年 7 月に実施されたクラウド セキュリティ アセスメントの結果です。

このクラウド セキュリティ アセスメント レポートは、**コントソ株式会社様**のクラウドセキュリティプログラムと実践に関する総合的なレビューを提供することを目的としています。**コントソ株式会社様**のクラウドセキュリティの成熟度は、アンケートとセキュリティ関連データの自動スキャンによって測定されました。このレポートは、詳細な制御確認やセキュリティ監査を行うものではありません。

このアセスメントの結果は、セキュリティ改善に関する推奨事項を含めたアクションプランであり、コントソ株式会社様が総合的なクラウドセキュリティのポジションを改善する上で役立ちます。

1.1. 会社評価

コントソ株式会社様のクラウドセキュリティプログラムと実践の評価では、後で詳しく説明する CIS Controls™ (v7) アンケートをレビューした結果、アンケートの回答における成熟度スコアに基づいて「Basic Lv1」というグローバル成熟度が算出されました。

質問に対するすべての回答の平均スコアは以下の通りです。今後のセキュリティスキャンの改善状況を追跡するために使用できます。

会社のスコア

最もリスクの高い項目に対するアクションリストについては、「第 2 章: 緊急アクション項目」をご覧ください。

このグローバル評価に関連する最終的な推奨事項は、コントソ株式会社様の規模、業界、規制環境、そのほかのリスク要因によって変化することもありますが、概略レベルにおいて、コントソ株式会社様のクラウドセキュリティの位置づけは次のように推定されます。

- プログラム的な側面は、ほとんどが予防的ではなく、対処的な特徴があります。
- 組織が直面するセキュリティリスクに対する全般的な理解はありますが、こういったリスクを管理するためのプログラムが構造化されていません。
- 組織の従業員には、今日のクラウドセキュリティの脅威に関する完全な認識がなく、セキュリティとプライバシーに関する意識向上関連トレーニングが存在しません。
- クラウドへの移行に伴い、ユーザーとデータの保護の重要性がさらに増しています。

推奨事項

プライバシー、セキュリティ、および関連するサイバー脅威に関するリスクを回避するには、ISO 27001 や NIST などに基づくサイバーセキュリティプログラムを実装する、組織の積極的な行動が必要です。

コントソ株式会社様は、クラウドセキュリティプログラムの一環としてリスク管理を実装する必要があります。リスク管理は、戦略的課題であるため、上級管理者がこのプロセスの主要関係者であることが求められます。 問題が発生してから対応するリスク管理アプローチだけでなく、先を見越した積極的なリスク管理が推奨されます。 これには、アクティブユーザーアカウント数の確認やファイアウォールログの監視など、実装したセキュリティ対策の有効性を定期的に確認することが必要となります。

2.アプローチ計画 (Migration Plan)

セキュリティチームとのインタビューで収集された情報と、CSAT スキャンから得た技術的事実情報から、現在の推奨される実践に比肩するための推奨事項が導かれています。その量に圧倒されることがあります。以下のアプローチ計画は、それらに優先順位を付けるための提案です。

このアプローチは 3 段階で構成されています。最初の段階は、ラピッドサイバー攻撃に対するリスクの緩和、そして「低い位置にぶら下がっている果実」に例えられる機能（比較的に簡単に実装できるが、セキュリティインシデントを防止する上で高い効力を発揮する機能）の有効化に焦点を当てています。また、セキュリティ戦略を活性化することにも注目しています。

2 つ目の段階では、IT 環境をさらに強化し、クラウドサブスクリプションに含まれる（基本的な）ガバナンスとレポート作成機能を実装することに焦点が当てられています。3 つ目の段階では、プロセスの作成/改訂と、より長い準備時間を要するソリューションの実装を対象としています。

お客様の環境について、次のアプローチ計画を提案します。

フェーズ *1* | *0～30* 日

- 緊急対策、クイック・ウィン、ラピッドサイバー攻撃の 0～30 日緩和と言及されているリスクを緩和します。ID 保護、デバイス保護、データ保護に焦点を当てます。

フェーズ *2* | *30～90* 日

- IT セキュリティをさらに成熟させるために、推奨セキュリティ機能を引き続き実装します。

フェーズ *3* | *90* 日～

- ゼロトラストアーキテクチャの採用を強化するために、現在の ID アーキテクチャを活性化します。
- 不要なレガシーネットワークプロトコルを無効にします。

フェーズ	機能	製品/スイート	ライセンス数（所有/必要）
0～30 日	Multi-Factor Authentication セルフサービスのパスワードリセット Privileged Identity Management 条件付きアクセスベース マルチウェア対策の統合（+XDR 機能）	Azure AD P1 Azure AD P1 Azure AD P2 Azure AD P1 EMS E3（Windows E5/EMS E5）	

30～90日	リスクベースの条件付きアクセス アプリケーション/シャドー IT のポリシー適用 デバイス監視/ログファイルの一元化	Azure AD P2/EMS E3 Microsoft Cloud App Security Azure Monitoring/Security Center	
90日～	SIEM へのアラート/検出レポート	Azure Security Center/Sentinel	

3.CSAT アプローチ

このレポートは、組織の現在のサイバーセキュリティ体制をさらに理解し、検出されたリスクを緩和するための実行可能な項目を提供することを目的としています。サイバーセキュリティ評価ツール（CSAT）は、環境の技術的スキャンと広く知られている CIS コントロールに基づくインタビューで構成されています。今お読みになっているレポートには、業界の推奨事項に基づいて IT 環境を強化するための推奨事項が詰まっています。アプローチをより理解するために、CIS の簡単な説明、ゼロトラストセキュリティ、およびラピッドサイバー攻撃について説明します。

3.1. Center for Internet Security

Center for Internet Security®（CIS）は、CIS Controls® と CIS Benchmarks™ を引き受けるコミュニティ主導の非営利団体です。この組織は、IT システムとデータを保護するための世界的に認められたベストプラクティスを提供しています。IT 専門家の CIS グローバルコミュニティは、新しい脅威から積極的に保護できるよう、これらの標準を常に進化させています。

CSAT アンケートは、CIS Controls に基づいており、組織の IT プロセスについての関連性の高い情報を提供することを目的としています。また、アンケートには ISO 27001 コントロールに関連する質問も含まれています。Center for Internet Security に関する詳細は、https://cisecurity.org をご覧ください。

3.2. ゼロトラストセキュリティアーキテクチャ

ゼロトラストセキュリティアーキテクチャの原則は、ビジネス目標の達成を技術標準によって実現する「The Open Group」という世界的コンソーシアムが定義したものです。The Open Group は、カスタマー、システム・ソリューションサプライヤ、ツールベンダー、インテグレーター、学術機関、およびコンサルタントなど、複数の業界にまたがる 790 以上の組織と協力しています。様々なワーキンググループで編成されており、現在の要件と新しい要件を把握、明確化、および統合し、標準とポリシーを確立し、ベストプラクティスを共有しています。これらの標準によって、オープン性、相互運用性、およびコンセンサスが保証されています。

ゼロトラストセキュリティアーキテクチャは、現在進行中のアーキテクチャであり、多くのことが取り込まれる予定です。IBM や Microsoft といった企業は、ゼロトラストの主要原則に関するホワイトペーパーに基づいてこれらの原則をリファレンスアーキテクチャに組み込んでいるため、 組織は、認識しているソリューションと製品を ZTA パラダイムに関連付けることができます。

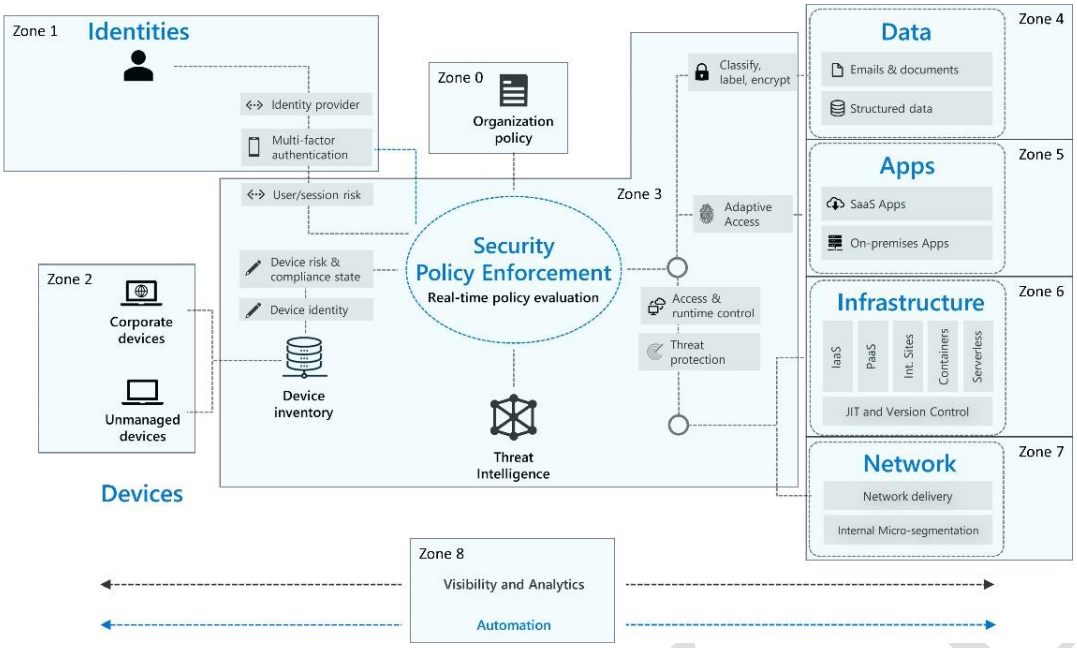
アーキテクチャの原則は製品に依存していないため、最終的にどの製品とソリューションを実装するのかは、企業の戦略によって決定します。Microsoft ベースのオンプレミスソリューションとクラウドソリューションで構成される IT 環境の評価がほとんどであるため、この推奨事項も、Microsoft が推奨する実践とゼロトラストリファレンスアーキテクチャに基づいています。

詳細については、https://theopengroup.org と https://www.microsoft.com/en/security/business/zero-trust をご覧ください。

ゼロトラスト原則は、次のとおりです。

1. 明示的に検証する
   必ず、ユーザー ID、ロケーション、デバイスの健全性、サービスまたはワークロード、データ分類、および異常といったすべての利用可能なデータポイントに基づいて認証し、承認すること。
2. 最小特権アクセスを使用する
   データと生産性の両方を確保するために、ジャストインタイムとジャストイナフアクセス（JIT/JEA）、リスクベースの順応性ポリシー、およびデータ保護を使用してユーザーアクセスを制限すること。
3. 侵害を想定する
   ネットワーク、ユーザー、デバイス、およびアプリの認識をセグメント化することで、侵害の増加を最小化し、ラテラルムーブメントを防止すること。 すべてのセッションがエンドツーエンドで暗号化されていることを確認すること。 アナリティクスを使用して、可視性を高め、脅威の検出を促進し、防御を改善すること。

ゼロトラストモデルは、企業ファイアウォールの背後にあるすべてが安全であると想定するのではなく、侵害を想定し、各リクエストがオープンネットワークから発信されているものとして検証します。リクエストの発信元やどのリソースにアクセスするのかに関係なく、ゼロトラストは「決して信用せず、常に検証する」と教えています。 すべてのアクセスリクエストは、アクセスを付与される前に、完全に認証され、承認され、暗号化されます。 ラテラルムーブメントを最小化するには、マイクロセグメンテーションと最小特権アクセスの原則が適用されます。リアルタイムで異常を検出して対応するには、リッチインテリジェンスとアナリティクスが使用されます。図で表すと、次のようになります。



上記のゾーンは、第 4 章と 5 章の表にあるそれぞれの CSAT 推奨事項と相関しており、CIS コントロールと ZTA ゾーンに関連付けられています。

3.3. ラピッドサイバー攻撃

ラピッドサイバー攻撃は一般化し、攻撃の破壊的な性質により、ますます厄介なものになっています。多くの攻撃は、エンドユーザーに、信頼できるように見えるフィッシングやスパムリンクをクリックさせるなどして、ファイアウォールと侵入検知システムをバイパスしたときに成功します。システムが最新の状態でなかったり、OS/ソフトウェアがサポート対象外である場合、パッチ適用プロセスが存在しないか遅すぎる場合などがあれば、マルウェアは数分のうちにグローバルネットワーク全体を人質に取って、ロック解除するための身代金を要求することができます。

サイバー犯罪者が最近見つけた最新の手段は、アプリケーションプロバイダからのアップデートシステムを侵害し、トロイの木馬を正当なアップデートソフトウェアに植え付ける方法です。この方法は、国家が資金援助している組織が最もよく使用する方法で、こういった組織は特定のターゲットを攻撃することを念頭としています。しかし、ターゲット以外の組織もそういったアップデートを入手すると、ほかの犯罪者もインストールされたマルウェアを使ってそういった組織を攻撃できるようになります。このような展開から、これまでになく、多層防御戦略が必要となっていることがわかります。

多くの組織がラピッドサイバー攻撃の犠牲となっていますが、それに対する防御を簡単に強化できるステップがいくつかあり、そういった攻撃が成功するのが困難になっています。これらの脅威を軽減する主なコンポーネントには、次のものがあります。

このレポートの推奨事項には、ラピッドサイバー攻撃に対抗するための主な活動の通知が含まれます。

推奨事項は、Microsoft がこれらの攻撃から得た教訓をもとに作られています[1]。

[1] 出典: https://aka.ms/rapidattack

4. クラウドセキュリティ向上のためのアクションプラン

4.1. 緊急アクションアイテム

以下は、評価で特定された緊急アクションアイテムです。これらの項目を評価し、該当する場合は最優先事項として実行することをお勧めします。

トピック	アクション	関連するソフトウェア製品
緊急		
3. 継続的脆弱性管理	脆弱性スキャンソフトウェアを実装してください。機密情報が含まれるシステムを中心に、定期的に脆弱性をスキャンしてください。	Microsoft エンドポイントマネージャー、Microsoft Defender ATP、Azure Security Center、Cloud App Security
4. 管理特権の使用の管理	管理特権を持つすべてのアカウントに対し、Azure AD PIM Access Reviews を用いた定期的な資格と承認の審査プロセスを実装してください。古い未使用のアカウントをクリーンアップしてください。	Azure Privileged Identity Management（PIM）、Azure AD Access Review
5. モバイルデバイス、ノートパソコン、ワークステーション、およびサーバー上のハードウェアとソフトウェアのセキュアな構成	構成管理ツールを実装し、最小限のセキュリティ設定について、すべてのシステムを確認できるようにしてください。	Microsoft エンドポイントマネージャー、Microsoft Defender ATP、Azure Security Center、Cloud App Security
6. メンテナンス、監視、および監査ログの分析	ロギングプラットフォームをセットアップし、境界デバイスのロギング構成を中央システムのロギングプラットフォームに指定してください。Azure Sentinel を使用してセキュリティ情報イベント管理（SIEM）ソリューションをセットアップし、オンプレミスまたはクラウドで実行してるユーザー、アプリケーション、サーバー、およびデバイスなどのすべてのソースから収集するデータを集計してください。	Azure Sentinel、Azure Security Center、Azure Advanced Threat Protection（ATP）、Microsoft Cloud App Security
10. データ復旧機能	物理的または技術的なセキュリティ対策を通じて、組織のバックアップを安全に保管してください。	Azure Backup
13. データ保護	組織の主要データソースで機密情報を識別できるようにしてください。ラベル付けと分類を適用してください。	Azure Information Protection Scanner、データ損失防止、Office 365 アドバンストデータガバナンス、Azure Information Protection P2
16. アカウントの監視と制御	すべてのアカウントにビジネスオーナーを立て、ビジネスオーナー/機能オーナーが各アカウントをチェックし、古いアカウントをクリーンアップしてください	Azure AD アクセスレビュー
AD.2. データガバナンス	ラベル付けと分類ポリシーを定義して実装してください。	Azure Information Protection Scanner、データ損失防止、Azure Information Protection P2

4.2. クイック アクション

次のアクションは、コントソ株式会社様 が実装を検討できるクイック・ウィンです。推奨されるアクションと製品は次の通りです。

トピック	アクション	関連するソフトウェア製品
クイック アクション		
Active Directory アカウント	• 古いアカウントや未使用のアカウントを無効化してください • すべてのユーザーアカウントに多要素認証（MFA）を実装してください	• Azure MFA • 条件付きアクセス
管理者	• 管理者アカウントを定期的に確認し、古いアカウントや使用されていないアカウントをクリーンアップするプロセスを実装してください	• Azure Privileged Identity Management（PIM）
オペレーティングシステム	• サポート終了（または終了間近）のオペレーティングシステムを移行してください	• Windows Server 2016 または 2019 • Windows 10
Windows の更新プログラム	• 利用可能なセキュリティパッチをすべてのエンドポイントにロールアウトしてください	• Intune • Azure Security Center
ファイアウォール	• すべてのエンドポイントにファイアウォールを有効化してください	• Windows ファイアウォール
ディスクの暗号化	• モバイルデバイスをはじめ、すべてのエンドポイントでディスク暗号化を有効化してください	• BitLocker

5.クラウドセキュリティに関する調査結果と推奨事項

1 つに纏められた総合的な組織評価より重要なのは、各 CIS Controls™（v7）コントロールと ISO/IEC 27001 フレームワークから取得したコントロールに関連する具体的な評価です。現在の状態を表す各評価には意味があり、特にコントソ株式会社様のクラウドセキュリティプログラムと実践が将来あるべき状態と比較した場合に、その重要度が増します。

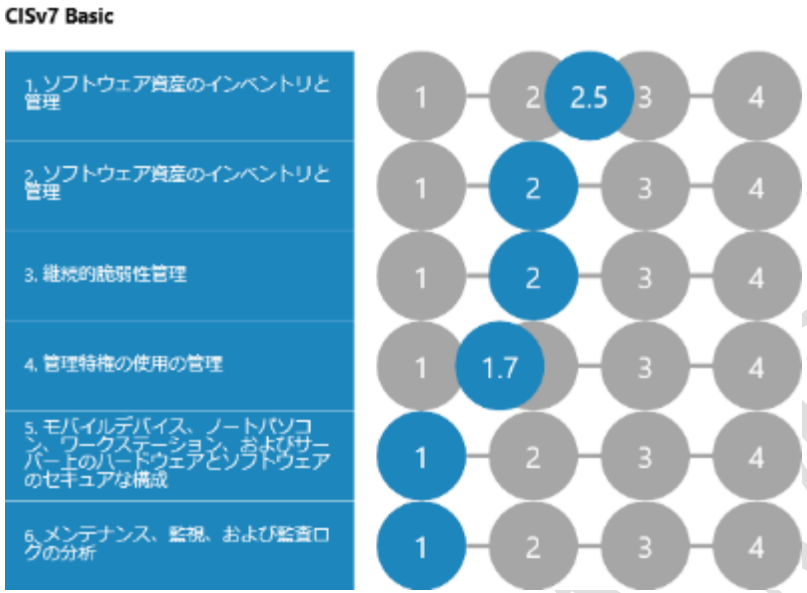
5.1. Basic CIS Controls

Basic CIS Controls は、最大限の IT 環境のインベントリ、スコーピング、および制御に関連します。Basic CIS Controls の 6 項目とその目的は、次の通りです。

トピック	目的
1. ハードウェア資産のインベントリと管理	ネットワーク上のすべてのハードウェアデバイスを積極的に管理（インベントリ、追跡、修正）することで、承認されたデバイスのみがアクセスできるようにし、検出された未承認のデバイスと非管理対象のデバイスによるアクセスを防ぎます。
2. ソフトウェア資産のインベントリと管理	ネットワーク上のすべてのソフトウェアを積極的に管理（インベントリ、追跡、修正）することで、承認されたソフトウェアのみをインストール・実行できるようにし、検出された未承認のソフトウェアと非管理対象のソフトウェアのインストールまたは実行を防ぎます。
3. 継続的脆弱性管理	新しい情報を継続的に取得し、評価した上で対応することで、脆弱性の特定、修復、攻撃者の攻撃機会の縮小化を実現します。
4. 管理特権の使用の管理	プロセスやツールを使用して、コンピュータ、ネットワーク、およびアプリケーションに対する管理特権の使用、割り当て、および構成を追跡、管理、防止、修正します。
5. モバイルデバイス、ノートパソコン、ワークステーション、およびサーバー上のハードウェアとソフトウェアのセキュアな構成	厳格な構成管理と変更管理プロセスを使用して、モバイル デバイス、ノートパソコン、サーバー、およびワークステーションのセキュリティ構成を確立、実装、および積極的に管理（追跡、レポート作成、修正）し、攻撃者が脆弱なサービスや設定を悪用するのを防ぎます。
6. メンテナンス、監視、および監査ログの分析	イベントの監査ログを収集、管理、および分析し、攻撃の検出、理解、または攻撃からの回復に役立てます。

5.1.1. Basic CIS Controls - スコアの概要

この評価は、上記に示す「Basic CIS Controls」の目的に対する測定に基づくアプローチを用い、コントソ株式会社様の現在のポジションを Basic CIS Controls の各項目ごとに示しました。



5.1.2. Basic CIS Controls - 調査結果と推奨事項

お客様からご回答いただいた質問項目および技術的調査結果に基づき、クラウドセキュリティの状態を改善するために次の項目が推奨されます。 以下に示される詳細な結果は、Basic CIS Controls の 6 つの各項目に関連付けられており、コントソ株式会社様 への推奨事項を示しています。

緊急				
トピック	**質問**	**回答**	**推奨**	**対象製品**
3. 継続的脆弱性管理	組織のインフラストラクチャにあるシステムに、ソフトウェア	Basic（1）実装されていない	脆弱性スキャンソフトウェアを実装してください。機密情報が含まれるシステムを中心に、定期的に脆弱性をスキャンしてください。	Microsoft エンドポイントマネージャー、Microsoft Defender ATP、

緊急				
	の脆弱性を特定する検出ルーツは実装されていますか？			Azure Security Center、Cloud App Security
4. 管理特権の使用の管理	すべての管理者に、通常のユーザーアカウントから分離された専用の個人管理者アカウントがありますか？組織のすべての管理アクセスに多要素認証（MFA）が実装されており、デフォルトの権限を制限する Just-in-Time アクセスルールが適用されている必要があります。	Basic（1）実装されていない	個人の管理者アカウントをセットアップし、すべての外部管理アクセスに対して多要素認証を有効化してください。	Azure AD Privileged Identity Management（PIM）、Privileged Access Management（PAM）、Azure Multi-Factor Authentication
4. 管理特権の使用の管理	組織には、サーバー、デスクトップ、およびノートパソコンで管理特権を持つ各ユーザーが上級管理者によって承認されていることを確認する、定期的な資格審査プロセスがありますか？	Basic（1）所定のプロセスはない	管理特権を持つすべてのアカウントに対し、Azure AD PIM Access Reviews を用いた定期的な資格と承認の審査プロセスを実装してください。古い未使用のアカウントをクリーンアップしてください。	Azure Privileged Identity Management（PIM）、Azure AD Access Review
5. モバイルデバイス、ノートパソコン、ワークステーション、およびサーバー上のハー	組織のインフラストラクチャに、全システムにおけるセキュリティ設定の誤構成を特定	Basic（1）実装されていない	構成管理ツールを実装し、最小限のセキュリティ設定について、すべてのシステムを確認できるようにしてください。	Microsoft エンドポイントマネージャー、Microsoft Defender ATP、Azure Security Cen

緊急				
ドウェアとソフトウェアのセキュアな構成	する検出ツールを実装していますか？			ter、Cloud App Security
6. メンテナンス、監視、および監査ログの分析	情報セキュリティ担当者またはセキュリティ専門家は、分析を実施してレポート作成を実行し、ログの異常を識別していますか？	Basic（1）所定のプロセスはない	ログの確認プロセスを実装し、重大なセキュリティ問題について定期的に確認してください。	

高				
トピック	**質問**	**回答**	**推奨**	**対象製品**
2. ソフトウェア資産のインベントリと管理	組織のすべてのシステムに、承認済みのソフトウェアプログラムのみの実行を許可するソフトウェアホワイトリストツールを実装していますか？	Basic（1）実装されていない	不要なソフトウェアや悪意のあるソフトウェアの使用を制限するホワイトリストを構成してください。	Microsoft エンドポイントマネージャー、Microsoft AppLocker、Windows Defender Application Control、Azure Security Center、Cloud App Security

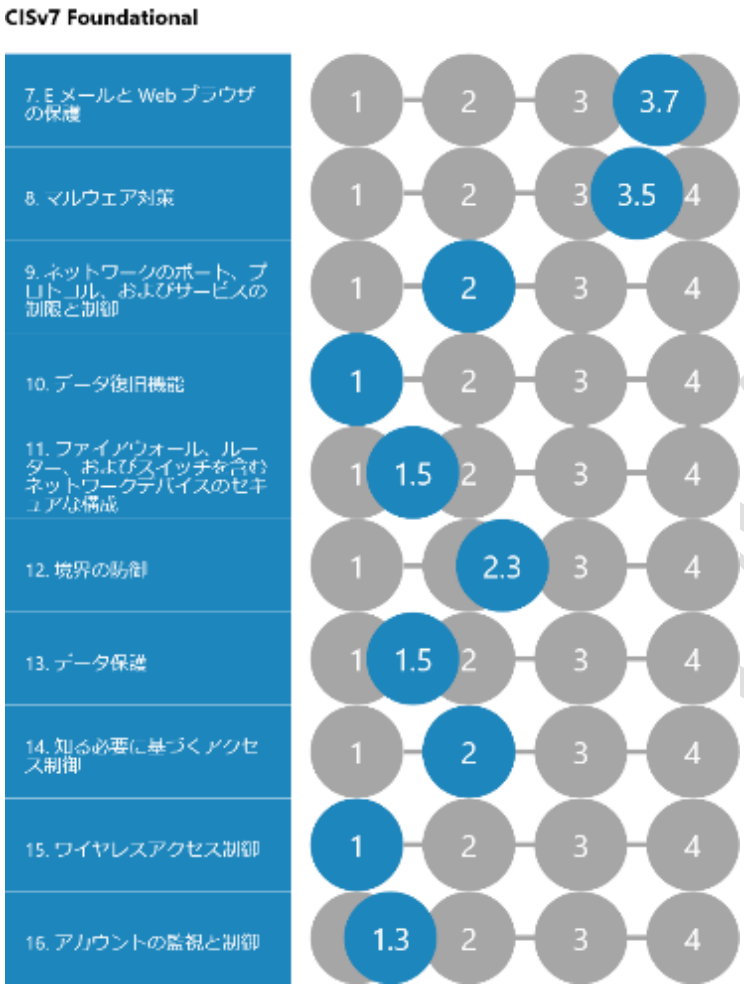
5.2. Foundational CIS Controls

Foundational CIS Controls では、IT 環境の全範囲において、主に IT 資産の安全を技術的に確保することと脅威の検出に焦点が当てられています。Foundational CIS Controls の 10 項目とその目的は、次の通りです。

トピック	目的
7. E メールと Web ブラウザの保護	Web ブラウザや E メールシステムとの対話を通じて人の行動を操作しようとする攻撃者の機会と攻撃を受ける窓口を最小化します。
8. マルウェア対策	エンタープライズの複数の箇所で悪意のあるコードのインストール、拡散、および実行を制御しながら、自動化を最適化して、対策更新、データ収集、および是正アクションを迅速に行えるようにします。
9. ネットワークのポート、プロトコル、およびサービスの制限と制御	攻撃者が利用できる脆弱性の窓口を最小化するために、ネットワーク接続されたデバイスにあるポート、プロトコル、およびサービスの継続的な運用利用を管理（追跡、制御、修正）します。
10. データ復旧機能	プロセスとツールを使用して、実績ある方法でクリティカルな情報を適切にバックアップし、適時に復旧します。
11. ファイアウォール、ルーター、およびスイッチを含むネットワークデバイスのセキュアな構成	厳格な構成管理と変更管理プロセスを使用して、ネットワークインフラストラクチャデバイスのセキュリティ構成を確立、実装、および積極的に管理（追跡、レポート作成、修正）し、攻撃者が脆弱なサービスや設定を悪用するのを防ぎます。
12. 境界の防御	セキュリティにダメージを与えるデータに焦点を当て、信用レベルの異なるネットワークを通過する情報の流れを検出、防止、修正します。
13. データ保護	データ流出を回避し、流出したデータの影響を緩和し、機密情報のプライバシーと完全性を確保するために使用されるプロセスとツールを評価します。
14. 知る必要に基づくアクセス制御	クリティカルな資産（情報、リソース、システムなど）にアクセスする必要性と権利のある人、コンピュータ、およびアプリケーションを決定する正式な分類に基づいて、クリティカルな資産への安全なアクセスを追跡、制御、防止、または修正するプロセスとツールを評価します。
15. ワイヤレスアクセス制御	ワイヤレスローカルエリアネットワーク（WLAN）、アクセスポイント、およびワイヤレスクライアントシステムの安全な使用を追跡、制御、防止、修正するために使用されるプロセスとツールを評価します。
16. アカウントの監視と制御	システムとアプリケーションアカウントのライフサイクル（作成、使用、休止、削除）を積極的に管理し、攻撃者がこれらを悪用する機会を最小限に押さえます。

5.2.1. Foundational CIS Controls - スコアの概要

この評価は、上記に示す Foundational CIS Controls の目的に基づく測定を行い、コントソ株式会社様 の現在のポジションを Foundational CIS Controls の各項目ごとに示しました。



5.2.2. Foundational CIS Controls - 調査結果と推奨事項

以下に示される詳細な結果は、Foundational CIS Controls の 10 個の各項目に関連付けられており、コントソ株式会社様 への推奨事項を示しています。

緊急				
トピック	**質問**	**回答**	**推奨**	**対象製品**
10. データ復旧機能	バックアップを保存する場合、さらにネットワーク間で移動する必要がある場合、物理的なセキュリティや暗号化によってバックアップの安全を保護していますか？	Basic（1）実装されていない	物理的または技術的なセキュリティ対策を通じて、組織のバックアップを安全に保管してください。	Azure Backup
13. データ保護	暗号化と完全性制御の適用が必要な機密情報を識別するために、データに評価を実施していますか？また、すべての機密文書に対して、ラベル付けと分類を実行していますか？	Basic（1）実装されていない	組織の主要データソースで機密情報を識別できるようにしてください。ラベル付けと分類を適用してください。	Azure Information Protection Scanner、データ損失防止、Office 365 アドバンストデータガバナンス、Azure Information Protection P2
14. 知る必要に基づくアクセス制御	ネットワークセグメンテーションは、サーバーに保存されている情報のラベルまたは分類レベルに基づいて適用されていますか？	Basic（1） ネットワークセグメンテーションは適用されていない	組織の主要データソースに対してネットワークセグメンテーションを適用してください。	

緊急				
16. アカウントの監視と制御	一元化された認証プラットフォームがあり、すべてのアプリケーション、デバイス、およびクラウドに使用されていますか？	Basic（1）実装されていない	一元管理された認証プラットフォームを確立してください。	Azure AD
16. アカウントの監視と制御	アカウント管理は、各アカウントのビジネスオーナーによって実施されており、一定期間が経過した後に休止アカウントを無効にし、自動的に期限切れとなるようにセットアップされていますか？	Basic（1） アカウントの管理がないか、IT によって、適宜、実施されている	すべてのアカウントにビジネスオーナーを立て、ビジネスオーナー/機能オーナーが各アカウントをチェックし、古いアカウントをクリーンアップしてください	Azure AD アクセスレビュー

高				
トピック	**質問**	**回答**	**推奨**	**対象製品**
10. データ復旧機能	組織には、各システムが自動的にバックアップされ、四半期に 1 回は、リストアが検証・確認されるような所定のバックアッププロセスはありますか？バックアップは、災害復旧用に別のサイトまたは場所に保管されている必要があります。	Standardized（2） 主要システムのバックアップは実装されとり、リストアは付随的に検証されている	すべてのシステムを含むようにバックアッププロセスを拡張し、リストアの検証スケジュールを設定してください。	Azure Backup and Site Recovery

高				
12. 境界の防御	ネットワークセグメンテーションは、異なるロールと制限レベルでシステムを分離するように適用していますか？	Standardized（2） サーバーとエンドポイントのみを分離している	ロールと制限レベルに基づき、システムを分離してください。	
13. データ保護	機密データを保持するモバイルデバイスと全システムに、デバイスとディスク暗号化ソフトウェアを適用していますか？	Standardized（2） 機密データを含む一部のシステムに対して実装されている	組織のすべてのデータソースで暗号化を有効化してください。	BitLocker、Microsoft エンドポイントマネージャー

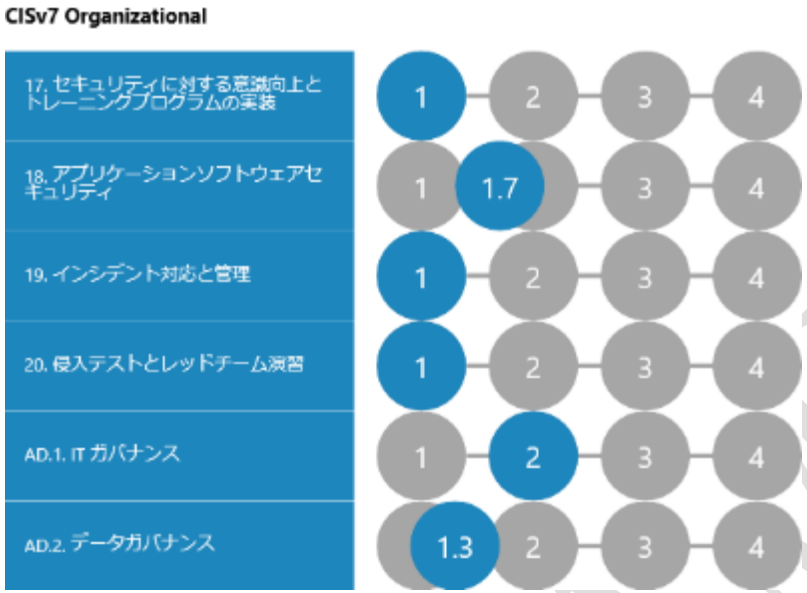
5.3. Organizational CIS Controls

Organizational CIS Controls は、組織のプロセスと手続きに関連しています。Organizational CIS Controls には、ISO/IEC 27001:2013 フレームワークの補足項目「AD.1」と「AD.2」の高レベルコントロールが伴います。補足質問は、IT およびデータガバナンスに関連しており、ポリシー、コンプライアンス、リスク管理、およびプライバシーの分野がカバーされています。Organizational CIS Controls の 4 つの項目と Addendum Controls の 2 つの項目、そしてその目的は、次のとおりです。

トピック	目的
17. セキュリティに対する意識向上とトレーニングプログラムの実装	組織内のすべての機能ロール（ビジネスとセキュリティに対してミッションクリティカルなロールを優先）において、エンタープライズの防御をサポートするために必要な具体的な知識、スキル、および能力を特定し、ギャップを評価して識別し、ポリシー、組織的プランニング、トレーニング、意識向上プログラムを通じて修正するための統合プランを開発・実行します。
18. アプリケーションソフトウェアセキュリティ	社内で開発されたソフトウェアと取得したソフトウェアのセキュリティライフサイクルを管理し、セキュリティの弱点を防止、検出、修正します。
19. インシデント対応と管理	攻撃の素早い検出、被害の効果的な封じ込め、攻撃者の存在の撲滅、およびネットワークとシステムの完全性の復旧を行うインシデント対応インフラストラクチャ（プラン、定義されたロール、トレーニング、通信、管理監督など）を確立し、組織の情報だけでなく評判も保護します。
20. 侵入テストとレッドチーム演習	攻撃者の目的とアクションをシミュレートすることで、組織の全体的な防衛強度（技術、プロセス、人員）を検査します。
AD.1. IT ガバナンス	組織に適用される規制と法的要件に準拠するセキュリティとプライバシーのポリシーフレームワークを確立することで、組織の透明性と整合性を作り出します。
AD.2. データガバナンス	リスクベースのアプローチにより、個人を識別できる情報（PII）に注目し、プライバシーに関する規制要件を調整して採用します。

5.3.1. Organizational CIS Controls - スコアの概要

この評価は、上記に示す Organizational CIS Controls と Addendum Controls AD.1 と AD.2 の目的に基づく測定を行い、コントソ株式会社様 の現在のポジションを Organizational CIS Controls の各項目ごとに示しました。



5.3.2. Organizational CIS Controls - 調査結果と推奨事項

以下に示される詳細な結果は、Organizational CIS Controls の各 4 項目と Addendum Controls の各 2 項目に関連付けられており、コントソ株式会社様 への推奨事項を示しています。

緊急				
トピック	**質問**	**回答**	**推奨**	**対象製品**
17. セキュリティに対する意識向上とトレーニングプログラムの実装	セキュリティとプライバシープログラムは確立されていますか？	Basic（1） セキュリティとプライバシーの意識向上プロ	セキュリティとプライバシーの意識向上プログラムを確立してください。	

緊急				
		グラムは用意されていない		
19. インシデント対応と管理	適切なレポート作成、データ収集、管理責任、法的プロトコル、およびコミュニケーション戦略が含まれた所定のインシデント対応手続きがありますか？	Basic（1） 所定の手続きはない	最も一般的なシナリオを網羅する基本的なインシデント対応手続きを実装し、それを実践してください。	Office 365 Advanced Compliance: Advanced eDiscovery
AD.2. データガバナンス	全組織において、すべての文書に対するデータ分類とラベル付けを自動化して実施していますか？	Basic（1） データの分類やラベル付けは適用されていない。	ラベル付けと分類ポリシーを定義して実装してください。	Azure Information Protection Scanner、データ損失防止、Azure Information Protection P2

高				
トピック	**質問**	**回答**	**推奨**	**対象製品**
AD.2. データガバナンス	組織内にある個人を特定できる情報（PII）が識別されており、担当者は PII に関する規則や規制について把握していますか？	Standardized （2） 中核ビジネスシステムのデータ管理実践は、個人を特定できる情報（PII）の識別に焦点を当てている。	PII レジスタを改善し、組織のあらゆる場所で利用可能な PII データを管理してください。	Azure Information Protection Scanner、データ損失防止、Office 365 アドバンストデータガバナンス、Azure Information Protection P2

6.技術データと分析

これは、コントソ株式会社様 の IT 環境をスキャンして得た事実に基づく（セキュリティ）データの要約です。

この情報は、Cyber Security Assessment Tool（CSAT）によって収集されました。

6.1.1.CIS Control 1: ハードウェア資産のインベントリと管理

CSAT では技術データは収集されません。推奨事項は、「Basic CIS Controls - 検出結果および推奨事項」に示されます。

6.1.2.CIS Control 2: ソフトウェア資産のインベントリと管理

CSAT 出力 - バージョン管理ステータス

ENDPOINT OPERATING SYSTEMS

No Data	948
Microsoft Windows 10 Enterprise	2
Microsoft Windows 10 Pro	151
Microsoft Windows 10 Pro for Workstations	4
Microsoft Windows 2000 Server	1
Microsoft Windows 7 Professional	63
Microsoft Windows Server 2008 R2 Standard	2
Microsoft Windows Server 2012 R2 Standard	3
Microsoft Windows Server 2012 Standard	12
Microsoft Windows Server 2019 Standard	9
Microsoft Windows XP Professional	48
Microsoft(R) Windows(R) Server 2003 Standard x64 Edition	1
Microsoft(R) Windows(R) Server 2003, Standard Edition	4
Microsoft® Windows Server® 2008 Standard	1
Microsoft® Windows Vista™ Business	3

CSAT 出力 - AD コンピュータアカウントの概要

AD コンピューターアカウント (有効なコンピューターアカウント)

有効アカウント	2405
無効アカウント	27
過去30日間アクティブなクライアント OS	1831
過去30日間アクティブなサーバー OS	71
30日以上アクティブでないクライアントOS	499
30日以上アクティブでないサーバーOS	4

CSAT 出力 - ライセンスのステータス

Consumed	Consumed	Prepaid	Available	Capability Status
DESKLESSPACK	2	2	0	Enabled
EMSPREMIUM	5	500	495	Enabled
O365_BUSINESS_ESSENTIALS	1	1	0	Enabled
POWER_BI_STANDARD	20	500	480	Enabled
RMSBASIC	0	1	1	Enabled
WINDOWS_STORE	0	25	25	Enabled

ソフトウェア資産のインベントリと管理に関する推奨

Windows オペレーティングシステム（OS）

サポート終了（間近の）OS Windows XP、Windows Vista、Windows 7、Windows Server 2003、Windows Server 2008 が検出されました。これらのオペレーティングシステム（OS）の段階的廃止計画を作成してください。Windows Server 2008 のOS を Azure に移動すると拡張セキュリティ サポートが受けられます。

レガシー製品およびサポート終了（間近の）製品が存在する場合、運用リスクと脅威に対する感度が高くなります。サポート終了となった製品は、サポートされていないため、脅威や脆弱性に対する更新やホットフィックスが提供されません。
Azure に移行すると、セキュリティが強化され、従来の IT 環境を維持するよりも柔軟性、信頼性、および拡張性が高くなります。サポート終了（間近の）ソフトウェア製品のアップグレードを開始してください。**付録 B - サポート終了製品** をご覧ください。

常に、サポートされている、最も安定したリリースでクライアントが実行していることを確認してください。**Microsoft Defender ATP** や **Azure Security Center** などのソフトウェアツールを使用すると、エンドポイントにインストール済みのアプリケーションを把握しやすくなります。**Cloud App Security** などのツールは、シャドー IT クラウドアプリケーションの使用を検出する上で役立ちます。

AppLocker や Azure Security Center の Windows アプリケーション制御、および Cloud App Security（クラウド用）を使用することで、企業インフラストラクチャにインストールできるアプリケーションを定義することができます。

6.1.3. CIS Control 3: 継続的脆弱性管理

CSAT 出力 - 更新ステータス

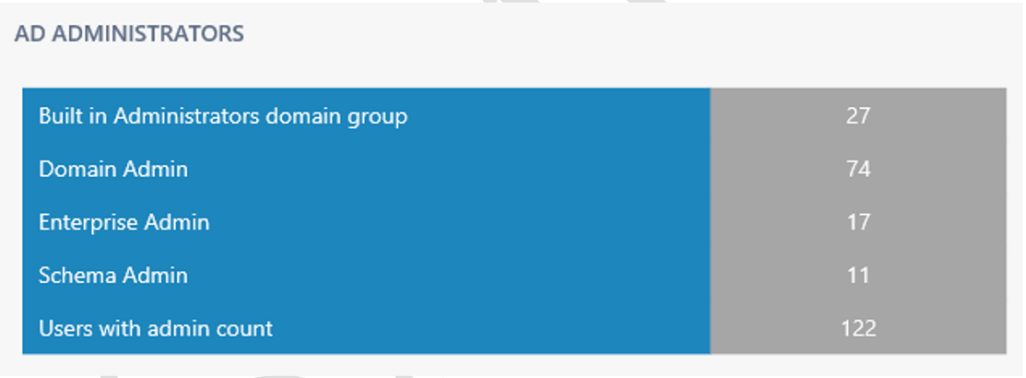
EndpointName	Critical	Important	Moderate	Low	Other
SrvWin2008	4	25	0	0	148
SrvWin2012	2	16	0	0	84
PCWin10	0	0	0	0	21
PCWin7	0	0	0	0	1

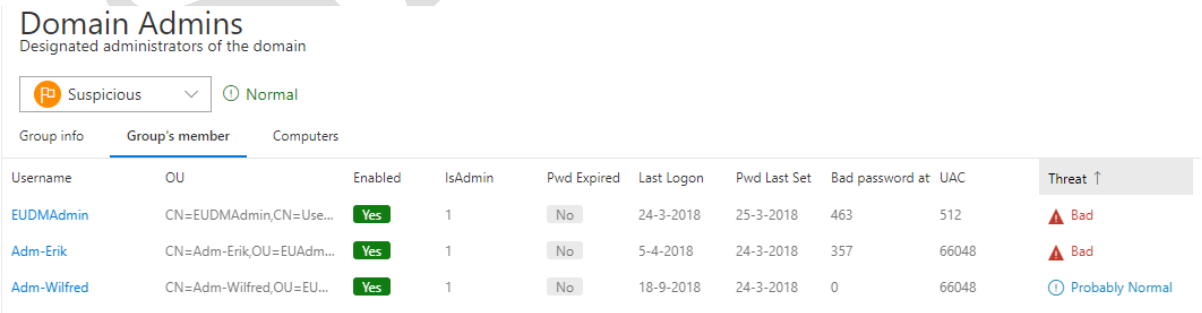
Windows 更新プログラムの状況に関する推奨

- 重大なセキュリティ修正プログラムが適用されていないエンドポイントが **46** 個検出されました。できるだけ早くセキュリティ修正プログラムをロールアウトしてください。

6.1.4. CIS Control 4: 管理権限の使用の管理

CSAT 出力 - *Active Directory* 管理グループ





CSAT 出力 - Azure Active Directory のロール

Inventory	Group name	Count
Office 365/Azure roles	Global Administrator	5
	Billing Administrator	2
	Security Administrator	5
Administrator accounts that use MFA for access	MFA enabled	0
	MFA not enabled	12

管理特権のステータスに関する推奨

Active Directory 管理者

- **ビルトイン管理者ドメイングループ**に多数の管理者が検出されました。このグループのメンバーには、ドメインコントローラーのフルコントロールが与えられているため、メンバー数は可能な限り制限する必要があります。これらのアカウントを確認し、古いアカウントや未使用のアカウントを削除してください。
- **多数のドメイン管理者が検出されました。**このグループのメンバーには、ドメインのフルコントロールが与えられているため、メンバー数は可能な限り制限する必要があります。これらのアカウントを確認し、古いアカウントや未使用のアカウントを削除してください。

Azure Active Directory 管理者

- **会社の管理者が多数**検出されました。このロールに含めるユーザーは 5 人未満が理想的です。これらのアカウントを確認し、古いアカウントや未使用のアカウントを削除してください。
- **12 個の AAD 管理者に多要素認証が有効化されていません。**すべての AAD 管理者に Azure MFA を実装してください。

管理者アカウントは、ネットワーク、またはシステムや機密データにアクセスできるため、企業のネットワークに高いリスクをもたらします。そのため、管理者の数をできる限り制限することが推奨されます。また、特権アカウントの権限を定期的に確認するプロセスを実装することをお勧めします。

6.1.5. CIS Control 5: ハードウェアおよびソフトウェアのセキュアな構成

CSAT 出力 - エンドポイントのセキュアな構成

Endpoints with LM Compatibility lower than 5	50
Endpoints with RDP enabled without NLA	28
Endpoints with PowerShell execution set to Unrestricted	81
Endpoints with SMB V1 enabled	124

CSAT 出力 - レジストリマシン

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa	lmcompatibilitylevel		[redacted]
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManWorkstation\Parameters	RequireSecuritySignature	0	[redacted]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	AutoAdminLogon	1	[redacted]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	AutoAdminLogon		[redacted]
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters	RequireSecuritySignature	0	[redacted]

CSAT 出力 - レジストリユーザー

HKEY_CURRENT_USER\Control Panel\Desktop	ScreenSaverActive	[redacted]
HKEY_CURRENT_USER\Control Panel\Desktop	ScreenSaverIsSecure	[redacted]

ハードウェアおよびソフトウェアのセキュアな構成に関する推奨

脆弱なサービスのセキュアな構成

- **SMBv1 が無効化されていない**エンドポイントが **124** 個検出されました。セキュリティを強化するには、新しいバージョンの SMBv2 または SMBv3 を使用することをお勧めします。GPO 構成、Windows PowerShell、または Intune を使って SMBv1 を無効化することができます。
- **NLA なしで RDP が有効化**されたエンドポイントが **28** 個検出されました。必要に応じて、管理対象の RDP エンドポイントでリモートマシンの NLA を有効化するか、マシンの RDP を無効化してください。

CSAT は、一連のマシンとユーザーレジストリキーを検査します。収集されたデータを確認するには、次のキーを変更することをお勧めしま

- LMCompatibilityLevel を、サーバーでは 4 または 5 に、ワークステーションでは 2 または 3 に変更してください。
  - NTLM バージョン（0～5）を上げて、セキュリティを改善します。
- RequireSecuritySignature を 1 に変更してください。
  - クライアントポリシーを常にパケットに署名するように設定します。
- LimitBlankPasswordUse を 1 に変更してください。
  - パスワードが空になっているアカウントをシステムで作成・維持することはできません。
- ScreenSaverActive と ScreenSaverIsSecure を 1 に変更してください。
  - 使用中でないシステムをロックします。スクリーンセーバーを一定期間後にパスワード保護が起動するように設定することで、コンピュータに物理的にアクセスできる未承認の人員にクリティカルな機密データが漏洩しないように保護することができます

6.1.6. CIS Control 6: メンテナンス、監視、および監査ログの分析

CSAT 出力 - AD の不正なパスワード試行

AD BAD PASSWORD ATTEMPTS (ENABLED ACCOUNTS, TOP 5) -

S-1-5-21-2324591617-2130959701-1352041874-1332	246246
S-1-5-21-2324591617-2130959701-1352041874-1254	85363
S-1-5-21-2324591617-2130959701-1352041874-2640	76857
S-1-5-21-2324591617-2130959701-1352041874-1666	36246
S-1-5-21-2324591617-2130959701-1352041874-500	6432

メンテナンス、監視、および監査ログの分析に関する推奨

- 不正なパスワードで何度も試行されていることが検出されました。つまり、アカウントは攻撃の標的になっている可能性があります。アカウントを確認することをお勧めします。

ハッキングのリスクを緩和するために、不審なログオンを監視する必要があります。潜在的な攻撃に関する早期警告を得るには、**Azure ATP** または **Advanced Threat Analytics（ATA）**を実装することをお勧めします。こういったセキュリティソリューションを使用すれば、さまざまな (AD) 攻撃に対する監視が可能になります。Cloud ユーザーの場合は、**Azure AD Identity Protection** を併用してください。

6.1.7. CIS Control 7: E メールおよび Web ブラウザの保護

CSAT 出力 - E メールの DNS

Inventory	Used	Notes
SPF record	v=spf1 include:spf.protection.outlook.com -all	
DKIM record	Not found	
DMARC record	Not found	

6.1.8. CIS Control 8: マルウェア対策

CSAT 出力 - ウイルス対策の概要

Windows Defenderを持たないサーバーエンドポイント	56
ウイルス対策を使用しないクライアントエンドポイント	0
古いウイルス定義のエンドポイント	1

Flag	Machine/IP	Operating system	AV Name	AV Type	AV Status	AV Definition
	WinVistaPC 172.20.100.168	Microsoft® Windows Vista™ Ultimate Version: 6.0.6002		NONE	OFF	UNKNOWN
	VMEU-WIN7-01 172.16.1.7	Microsoft Windows 7 Enterprise N Version: 6.1.7601		NONE	UNKNOWN	UNKNOWN
	Win2008PC 172.20.100.150	Microsoft Windows Server 2008 R2 Star Version: 6.1.7601	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN
	Win7PC 172.20.100.147	Microsoft Windows 7 Professional Version: 6.1.7601	Microsoft Security Es...	AUTOUPDATE_SE...	ON	UP_TO_DATE
	VMEU-WIN7-02 172.16.1.8	Microsoft Windows 7 Enterprise N Version: 6.1.7601		NONE	OFF	UNKNOWN
	VMEU-Win10-06 172.20.100.126	Microsoft Windows 10 Enterprise N Version: 10.0.17134	Windows Defender	AUTOUPDATE_SE...	SNOOZED	UP_TO_DATE
	WIN-RF4JEBCAUJ5 172.20.100.151	Microsoft Windows Server 2016 Standa Version: 10.0.14393	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN
	Win10PC 172.20.100.167	Microsoft Windows 10 Enterprise Version: 10.0.15063	Windows Defender	AUTOUPDATE_SE...	SNOOZED	UP_TO_DATE
	Win2012PC 172.20.101.63	Microsoft Windows Server 2012 R2 Star Version: 6.3.9600	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN
	Win8PC 172.20.101.96	Microsoft Windows 8.1 Enterprise Version: 6.3.9600	Windows Defender	AUTOUPDATE_SE...	SNOOZED	UP_TO_DATE
	VMEU-DCCore1 172.16.5.101	Microsoft Windows Server 2016 Datace Version: 10.0.14393	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN
	VMEU-DC2 172.16.5.102	Microsoft Windows Server 2016 Datace Version: 10.0.14393	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN
	VMEU-MGMT01 172.16.5.110	Microsoft Windows Server 2016 Datace Version: 10.0.14393	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN
	VMEU-Win10-01 172.16.1.6	Microsoft Windows 10 Pro Version: 10.0.16299	Windows Defender	AUTOUPDATE_SE...	SNOOZED	UP_TO_DATE

CSAT 出力 - 無効化されたウイルス対策

EndpointName	AvName	AvStatus	AvType
Srv01	*No AV API*	OFF	NONE
Srv02	*No AV API*	OFF	NONE
SQLDB03	*No AV API*	OFF	NONE
SQLDB99	*No AV API*	OFF	NONE
Web05	*No AV API*	OFF	NONE

マルウェア対策に関する推奨

- ウイルス対策が無効化されているか、使用されていないエンドポイントが **5** 個検出されました。これらのマシンのウイルス対策を有効化してください。

ウイルス対策のステータスを定期的にチェックし、すべてのマシンで最新のウイルス対策が実行していることを確認することをお勧めします。
ウイルス対策の使用は、ご利用の環境から攻撃とウイルスを排除する最もコスト効率の良い方法の 1 つです。

6.1.9. CIS Control 9: ネットワークのポート、プロトコル、およびサービスの制限と制御

CSAT 出力 - ファイアウォールのステータス

FQDN	# IN	# OUT	Domain	Public	Private	Threat ↑
Win2016_Clean 192.168.150.21	129	81	E B N	D B N	E B N	Bad
Win7_Pro_X64_EN 192.168.150.51	178	131	D B N	E B N	D B N	Bad

ファイアウォールに関する推奨

- 1 つ以上の Windows ファイアウォールが無効化されているエンドポイントが **518** 個検出されました。該当マシンのファイアウォールを有効化することをお勧めします。

Windows ファイアウォールは、未承諾の着信トラフィックを通じて拡散するトロイの木馬攻撃、ワーム、またはその他の悪意のあるプログラムなど、境界ネットワークを通過するまたは組織内で発生するネットワーク攻撃からエンドポイントを保護します。 感染したマシンが企業イントラネットにアクセスすると、Windows サービスまたはサードパーティアプリケーションの脆弱性を利用して保護されていないエンドポイントまたはサーバーに接続し、改ざんする可能性があります。

6.1.10. CIS Control 10: データ復旧機能

CSAT では技術データは収集されません。推奨事項は、「Foundational CIS Controls - 検出結果および推奨事項」に示されます。

6.1.11. CIS Control 11: ネットワークデバイスのセキュアな構成

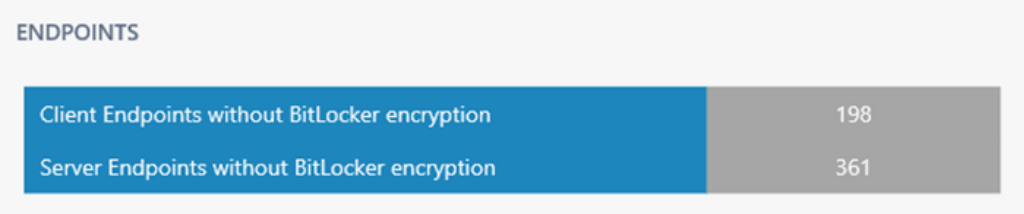
CSAT では技術データは収集されません。推奨事項は、「Foundational CIS Controls - 検出結果および推奨事項」に示されます。

6.1.12. CIS Control 12: 境界の防御

CSAT では技術データは収集されません。推奨事項は、「Foundational CIS Controls - 検出結果および推奨事項」に示されます。

6.1.13. CIS Control 13: データ保護

CSAT 出力 - BitLocker 暗号化のステータス



Machine/IP	Operating system	AV Name	AV Type	AV Status	AV Definition	BitLocker	Threat ↑
WinVistaPC 172.20.100.168	Microsoft® Windows Vista™ Ultimate Version: 6.0.6002		NONE	OFF	UNKNOWN	No	Suspicious
VMEU-WIN7-01 172.16.1.7	Microsoft Windows 7 Enterprise N Version: 6.1.7601		NONE	UNKNOWN	UNKNOWN	No	Unknown
Win7PC 172.20.100.147	Microsoft Windows 7 Professional Version: 6.1.7601	Microsoft Security Es...	AUTOUPDATE_SE...	ON	UP_TO_DATE	No	Probably Normal
VMEU-WIN7-02 172.16.1.8	Microsoft Windows 7 Enterprise N Version: 6.1.7601		NONE	OFF	UNKNOWN	No	Probably Normal
VMEU-Win10-06 172.20.100.126	Microsoft Windows 10 Enterprise N Version: 10.0.17134	Windows Defender	AUTOUPDATE_SE...	SNOOZED	UP_TO_DATE	No	Normal
VMEU-DCCore1 172.16.5.101	Microsoft Windows Server 2016 Datace Version: 10.0.14393	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN	Yes	Normal
VMEU-DC2 172.16.5.102	Microsoft Windows Server 2016 Datace Version: 10.0.14393	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN	Yes	Normal
VMEU-MGMT01 172.16.5.110	Microsoft Windows Server 2016 Datace Version: 10.0.14393	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN	No	Normal
VMEU-Win10-01 172.16.1.6	Microsoft Windows 10 Pro Version: 10.0.16299	Windows Defender	AUTOUPDATE_SE...	SNOOZED	UP_TO_DATE	No	Normal

CSAT 出力 - Office 365 の概要

データ保護に関する推奨

BitLocker 暗号化

- BitLocker 暗号化が有効でないクライアントエンドポイントが **198** 個検出されました。
- BitLocker 暗号化が有効でないサーバーエンドポイントが **361** 個検出されました。

暗号化されていないハードドライブには、デバイス/システム、特にノートパソコンを紛失した場合や盗難にあった場合に、データを紛失するリスクがあります。 BitLocker でハードドライブの暗号化を適用することで、紛失または盗難デバイスのデータをコスト効率良く保護することができます。 ディスク暗号化は、データストレージへの不正アクセスの防止に最適です。 PCI-DSS や GDPR などの一部の規制では、データ暗号化の使用が要求されています。 機密データを保持するエンドポイントで BitLocker を有効化してください。**Intune** と統合すると、回復キーを一元管理できるほか、暗号化ステータスの洞察を得られるようになります。

6.1.14. CIS Control 14: 知る必要に基づくアクセス制御

CSAT 出力 - エンドポイント共有

Path	Sharename	Servername	Description	Type	BitLocker	Threat ↑
C:\Users	Users	VMEU-WIN7-02		Disk Drive	No	Probably Normal
C:\Windows	ADMIN$	WinVistaPC	Remote Admin	Disk Drive Admin	No	Normal
C:\	C$	WinVistaPC	Default share	Disk Drive Admin	No	Normal
E:\	E$	WinVistaPC	Default share	Disk Drive Admin	No	Normal
C:\Windows	ADMIN$	VMEU-Win10-06	Remote Admin	Disk Drive Admin	No	Normal

知る必要に基づくアクセス制御に関する推奨

エンドポイント共有

共有には機密データが含まれる場合があります。 ユーザー権限を証明し、その作業にオーナーを割り当てるための手続きの作成をお勧めします。 これを定期的に実施すると、ユーザーに必要な権限が与えられているか、ユーザーが閲覧すべきでないデータが表示されないようになっているかを確認できます。

6.1.15. CIS Control 15: ワイヤレスアクセス制御

CSAT では技術データは収集されません。推奨事項は、「Foundational CIS Controls - 検出結果および推奨事項」に示されます。

6.1.16. CIS Control 16: アカウントの監視と制御

CSAT 出力 - AD アカウントのステータス

AD ACCOUNTS

Enabled Accounts	2578
Disabled Accounts	521
Enabled Accounts no login more than 30 days	447
Enabled Accounts no login more than 90 days	318
Enabled Accounts never logged in	472
Accounts flagged as bad	0

CSAT 出力 - AD ユーザーアカウント制御フラグ（有効アカウント）

AD UAC DETAILS ENABLED ACCOUNTS

Cannot Change Password	13
Don't Require PreAuth	12
Password not Required	256
Password not going to expire	542
Reversible Text Password	13
Smartcard Required	12
Use DES Key Only	7

CSAT 出力 - AD パスワードポリシー

PASSWORD POLICY

Max Password Age	10675199
Min Password Age	0
Lockout Duration in Minutes	30
Complex password required	true
Lockout Threshold	0
Password History	0
Min Password Length	0

CSAT 出力 - *AAD* 外部ユーザー

○	Chakir.Borsboom_outlook.com#EXT#@expanded.onmicrosoft.com	Chakir.Borsboom@outlook.com	Yes
○	Doeke.Moerman_outlook.com#EXT#@expanded.onmicrosoft.com	Doeke.Moerman@outlook.com	Yes
○	eriko_qssolutions.nl#EXT#@expanded.onmicrosoft.com	eriko@qssolutions.nl	Yes
○	Peggy.van.Amelsvoort_outlook.com#EXT#@expanded.onmicrosoft.c...	Peggy.van.Amelsvoort@outlook.com	Yes
○	Renee.Towell_outlook.com#EXT#@expanded.onmicrosoft.com	Renee.Towell@outlook.com	Yes
○	wilfredh_qssolutions.nl#EXT#@expanded.onmicrosoft.com	wilfredh@qssolutions.nl	Yes

アカウントの監視と制御に関する推奨

Active Directory アカウント

- **90 日を超えてログオンしていない**アカウントが **318** 個検出されました。これらのアカウントを確認し、未使用のアカウントを無効化してください。
- **521** 個のアカウントが**無効化**されています。これらのアカウントをクリーンアップしてください。
- **256** 個のアカウントで、「**Password Not Required（パスワードは必要ありません）**」設定が有効化されています。このフラグがある場合、パスワードを空欄にしたままアカウントにログオンすることができます。これらのアカウントを確認し、可能な場合はこの設定は削除してください。この設定の変更には、IT 管理者が PowerShell を使用する必要があります。

すべてのアカウント、特に特権アカウントに対し、**Azure MFA** を使用して**多要素認証（MFA）**を実装することをお勧めします。MFA は、アカウントにログインするためにユーザー名とパスワードに加え、もう 1 つの承認を必要とする機能で、ランダムに生成される SMS コード、電話、スマートカード（仮想または物理）、または生体認証デバイスなどが使用されます。MFA が有効化になっている場合、フィッシングメールやブルートフォース攻撃などでアカウントのユーザー名とパスワードが侵害された場合でも、攻撃者は 2 つ目の認証を完了できないため、そのアカウントにアクセスすることができません。

AD パスワード ポリシー

パスワードポリシーを次のような推奨される実践に合わせて構成することをお勧めします。

1. パスワードの有効期間: **60** 日 または **90** 日
2. パスワードの変更禁止期間: **1** 日、**3** 日、または **7** 日
3. ロックアウト期間: **30** 分または **60** 分
4. 複雑さの要件を満たす必要があるパスワード: **有効**（**true**）
5. アカウントのロックアウトのしきい値: **4** 回または **5** 回の無効なログイン試行
6. パスワード履歴: **10** 個または **24**個パスワード
7. パスワードの最小文字数: **8** 文字または **12** 文字

アカウントを保護するには、強力で複雑なパスワードを使用することが前提ですが、 さらに、多要素認証を使用することで、2 つ目の防衛線を引くことができます。

6.1.17. CIS Control 17: セキュリティに対する意識向上とトレーニングプログラムの実装

CSAT では技術データは収集されません。推奨事項は、「Organizational CIS Controls - 検出結果および推奨事項」に示されます。

6.1.18. CIS Control 18: アプリケーションソフトウェアセキュリティ

CSAT では技術データは収集されません。推奨事項は、「Organizational CIS Controls - 検出結果および推奨事項」に示されます。

6.1.19. CIS Control 19: インシデント対応と管理

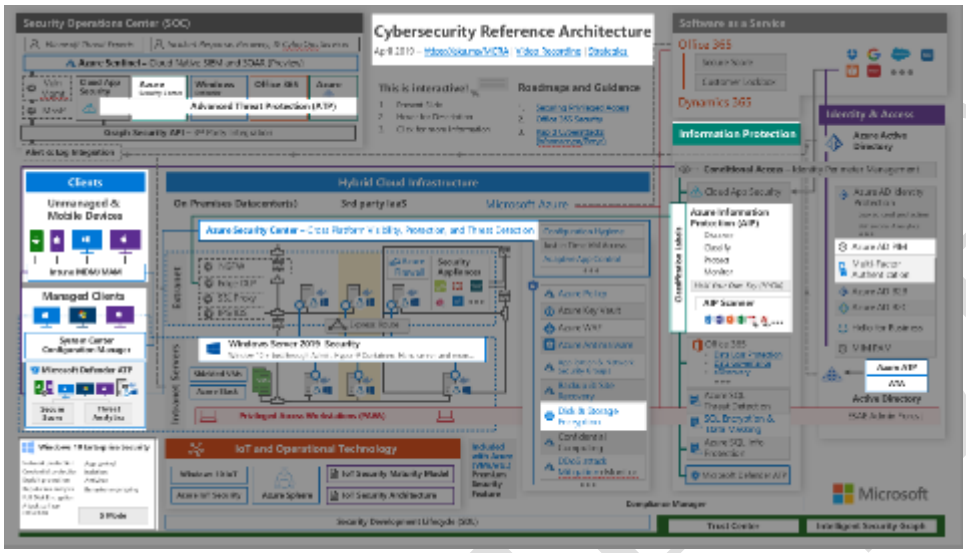
CSAT では技術データは収集されません。推奨事項は、「Organizational CIS Controls - 検出結果および推奨事項」に示されます。

6.1.20. CIS Control 20: 侵入テストとレッドチーム演習

CSAT では技術データは収集されません。推奨事項は、「Organizational CIS Controls - 検出結果および推奨事項」に示されます。

7. 付録 A - 推奨するセキュリティソフトウェア製品の概要

このレポートには、この評価で検出されたセキュリティの問題の解決に役立てられる Microsoft 製品が 1 つ以上あります。対象製品の概要については、Microsoft が配布する以下の「**サイバーセキュリティ リファレンス アーキテクチャ**」をご覧ください。強調して表示されている項目は、このレポートで推奨されている製品です。



出典: https://aka.ms/mcra

このレポートには、クラウドセキュリティの状態を改善するために推奨される製品が複数含まれています。Microsoft Cloud には、さまざまなライセンスで使用できる広範なクラウドセキュリティソリューションが提供されています。

8.付録 B - サポート終了製品

次のサポート終了製品が検出されました。

サポート終了の製品	
WINDOWS 10 1703	

次のサポート終了間近の製品が検出されました。

サポート終了間近の製品	
WINDOWS 10 1903	
WINDOWS 10 PRO 1809	
WINDOWS 8.1	

9. 付録 D - 評価の範囲

9.1. クラウドセキュリティ評価の目標

多数の組織と同様に、コントソ株式会社様は、モバイルデバイスの急増、組織運営に対するソーシャルネットワークの影響、構造化されていないデータの急速な増大、クラウドとプライバシー規制の迅速な導入など、IT 分野が今日直面している主なトレンドに取り組んでいます。こういったすべての分野は、脅威の移り変わりに影響を受けており、セキュリティプログラムと実践が全社的に大きな影響を与えています。

Center for Internet Security® が公開している CIS Controls™ バージョン 7 フレームワークの 3 つの領域（Basic、Foundational、Organizational）に含まれるセキュリティコントロールに基づいて実施される Cybersecurity Solution Assessment により、コントソ株式会社様のセキュリティプログラムの成熟度に関する概略的レビューを作成します。

クラウドセキュリティ評価の目標は、次のとおりです。

- 包括的に統合された方法で、IT 資産を保護し、最新のクラウドセキュリティ実践するための基盤の構築に着手すること。
- クラウドセキュリティの基盤として高く評価された既知のセキュリティフレームワークが示すセキュリティの「推奨される実践」に合わせて調整すること。
- 認証、権限、およびデータ保護などの分野における内部コントロールがよりクリティカルとなるクラウドについて、セキュリティ面でのそれへの移行経路を計画すること。
- IT 環境に関するインタービューとそのスキャン中に検出された事実を基に推奨事項を提供すること。
- クラウドセキュリティに関連する重大な問題を明白にすること。
- 調査結果の重要度に基づいて優先順位付けされたアクションリストを、組織のクラウドセキュリティプログラムにおいて短期的なロードマップとしても使用できるリストとして作成すること。

9.2. インベントリツール

コントソ株式会社様 の IT インフラストラクチャのインベントリ調査（技術的なトピック）を実施する上で、評価、分析、レポートの情報として使用する IT 資産と現在の状況を判定するために、Cyber Security Assessment Tool（CSAT）が使用されました。

9.3. Cyber Security Assessment Tool

Cyber Security Assessment Tool（CSAT）は、経験豊かなセキュリティエキスパートによって開発されたソフトウェア製品で、組織のセキュリティの現状を素早く評価し、事実に基づく改善事項を推奨することを目的としています。

このツールは、IT 環境に含まれるエンドポイント、Active Directory、および SharePoint Online などをスキャンし、関連するデータを収集します。また、アンケートを使用して、ポリシーやその他の主な指標に関するデータも収集しています。

組織は、セキュリティのステータスを単純に素早く確認する方法を求めています。社内の IT インフラストラクチャや Office 365 から得られるデータを基に、脆弱性を把握したいと考えています。QS solutions の Cyber Security Assessment Tool（CSAT）では、自動スキャンと分析によって、これらの情報を提供し、さらにその結果を利用して、組織がセキュリティを改善するための推奨事項と短期的なアクションプランをまとめたレポートを作成することができます。セキュリティを最大限に強化し、セキュリティに対する組織の真剣な取り組みを示す上で最適な方法です。GDPR と AVG の規制の観点からも、この取り組みの重要性は高まっています。

10. 付録 E - 評価の背景

10.1.はじめに

従来のオンプレミス型 IT インフラストラクチャとクラウドプラットフォームを統合したハイブリッド IT 戦略は、多くの組織において標準的な戦略となりました。これにより、クラウドセキュリティの実践の範囲も拡大しています。IT セキュリティに対する従来の考え方は、本質的に最小限で静的であることがほとんどですが、非常に速い速度で脅威の領域が拡大、移行、そして進化するようなクラウドの時代においては、もはや十分とは言えません。企業の資産を保護するには、セキュリティのビジネスオーナー、および必要なセキュリティに要求されるレベルについての明確な指示が重要な鍵となります。

セキュリティの範囲の拡張に伴い、過去数年において以下のように大きな変化を遂げた今日の脅威とリスクに合わせ、確固たるクラウドセキュリティプログラムと実践を確立することが求められています。

従来の IT 環境	最新の IT 環境
「スクリプトキディ」とサイバー犯罪	サイバースパイ、サイバー戦争
個人のサイバー犯罪者	大規模なハッカー集団による、ほぼ無制限のリソースを駆使した（海外）スポンサー付きの活動
フォーチュン *500* 社や多国籍企業への攻撃	中小企業も含む、あらゆる産業セクターを標的
企業所有の、厳重に管理されたデバイス	（非）管理対象の BYOD（Bring Your Own Device）や CYOD（Choose Your Own Device）ポリシー
ビジネス/商業中心の戦略要求	プライバシー中心戦略は必須
IT 資産を保護するためのセキュリティ実践	プライバシーを確保するためのデータ保護

エンドユーザーの要求は急速に変化しており、人々が働く方法も、組織ではなく、各ユーザーの日常のクラウドサービスの使用経験とそのサービスによって尽きることのない可能性に基づくユーザーの意思によって決定されています。データもまた、さまざまな場所に保存されるようになり、ユーザーは、いつでもどこからでも、あらゆるデバイスから企業のデータとアプリケーションにアクセスできることを期待しています。この状況において、組織の IT 環境のほぼあらゆる部分が公開されるようになったため、新たなセキュリティリスクが生まれています。

セキュリティは、組織が直面する脅威とリスクに相対しています。つまり、絶対的なセキュリティは存在しないのです。ある組織とって良いと言えることは、別の組織では過度なこととなる場合もあり、あらゆる組織に適用できるセキュリティプログラムは存在しません。こういった、セキュリティの脅威と IT リスク管理における格差に対応するには、成熟度に基づくアプローチが役立ちます。

測定可能なセキュリティフレームワークを確立するには、セキュリティの「推奨される実践」に関するしっかりとした基盤が必要です。このため、クラウドセキュリティ評価には、**Center for Internet Security®**（CIS）（http://www.cisecurity.org）が公開している **CIS Controls™ (v7)** セキュリティフレームワークが使用されています。参考: **付録 E - 評価の背景**

クラウドセキュリティ評価では、アンケートにお答えいただくことで、コントソ株式会社様 のクラウドセキュリティ実践レベルが測定されています。この測定は、「Basic」、「Foundational」、および「Organizational」という、CIS Control™ (v7) セキュリティフレームワークのコントロールドメインにおける実践を対象に実施されています。

アンケートを通じた測定のほか、コントソ株式会社様 の IT 環境から、関連性のあるセキュリティ関連データも収集されています。この、アンケートを通じた測定結果、ならびに収集したデータの分析により、コントソ株式会社様 のクラウドセキュリティプログラムと実践の改善を図るための調査結果、推奨事項、アクションアイテム、およびコンパイルされた短期ロードマップが提供されています。

10.2.コントロールフレームワークの背景（CIS）

このセキュリティフレームワークは、**3** つの領域で構成されています。CIS Controls™ (v7) は、実装と実装後の運用に渡るアライメントと指導を提供するために領域別に分けられています。 実装範囲を定義してその基準を設定する「**Basic**」コントロールから始まり、IT 資産を保護する上で不可欠かつ重要な対策をカバーする「**Foundational**」コントロールが続きます。さらに、「**Organizational**」コントロールでは、組織をクラウド脅威から保護するために、積極的で緩和的なコントロールを用いたプロセスと手続きに関する指導が提供されます。

CIS Controls™ (v7) は、リスク評価の概念に（企業型アプローチに相反する）コミュニティ型アプローチを採用しています。CIS Controls™ (v7) は、機関や施設などの特定のエンタープライズの観点からではなく、コンセンサス方式のリスク評価を使用して作成されており、 大企業でよく見られる広汎性の脅威と脆弱性に対して、政府、業界、および学界から集まった大規模な専門家グループが出した判断を統合するものです。

CIS Controls™ (v7) は、最も一般的な攻撃パターンに基づいており、政府と業界の非常に幅広いコミュニティによって精査され、非常に固い統一見解によって生み出されています。そのため、有用性の非常に高いアクションの揺るぎない基盤としてみなされています。このフレームワークは、包括的な IT およびセキュリティリスク管理フレームワークに置き換わるものではなく、 CIS Controls™ (v7) では、高いレバレッジと見返りが伴う、少数の実行可能なコントロールに焦点を絞り、それらを優先しています。

クラウドセキュリティ評価では、Organizational Control 領域の補足として、ISO/IEC 27001:2013 フレームから精選された概略レベルのコントロールを含めるように CIS Controls™ (v7) を技術的に拡張

しています。そこで問われる質問は IT やデータガバナンスに関連しており、ポリシー、コンプライアンス、リスク管理、およびプライバシーの分野がカバーされています。

10.3.SOM モデル

この目標を達成するために、クラウドセキュリティ評価は、成熟度モデルを使用して、検出結果や推奨事項を提供します。Microsoft（Security Maturity Model v1）が開発した同様のモデルに基づき、Software Optimization Model（SOM）と一貫する成熟度モデルを使用しています。以下の図は、その成熟度レベルを説明しています。

会社の完全なスコアは、組織の最低スコアによって決まります。ほとんどのプロセスがレベル 3 であっても、1 つのプロセスがレベル 1 である場合、組織全体の評価はレベル 1 になります。