中小企業向けゼロトラストガイダンス

CSAJC cloud security alliance SM Japan Chapter

Softchoice

CSA cloud security alliance®

The permanent and official location for the CSA Zero Trust Working Group is
https://cloudsecurityalliance.org/research/working-groups/zero-trust/

日本語版提供に際しての告知及び注意事項

本書「中小企業向けゼロトラストガイダンス」は、Cloud Security Alliance (CSA)が公開している「Zero Trust Guidance for Small and Medium-Sized Businesses (SMBs)」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
2025年02月01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

「中小企業向けゼロトラストガイダンス」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）

井上　尚人
笠松　隆幸
諸角　昌宏
山下　亮一

謝辞

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ゼロトラスト（ZT）ワーキンググループの目標は以下の通りです：

- 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。
- 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を得た上で意思決定できるよう、さまざまなZTアプローチの長所と短所について、ソートリーダーシップを発揮し、業界を啓発します。
- 成熟したゼロトラスト実装のアーキテクチャと実装アプローチに関して、意図的に製品およびベンダーに中立的なアプローチを取ります。

本ワーキンググループは、ゼロトラストの柱に沿った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、 Frank DePaola、Joy Williams、Maureen Rosadoが率いるZT1&2、 Zero Trust as a Philosophy & Guiding Principle, Organizational Strategy & Governance です（訳注： https://cloudsecurityalliance.org/research/working-groups/zero-trustを参照）。

Lead Author(s)

Frank DePaola
Mark Fishburn
Larry Kinkaid
Andrea Knoblauch
Aaron Robel
Alex Sharpe
Michael Theriault

Contributors

Sam Aiello
Sue
Bergamo
Dr.Chase Cunningham
Kevin Dillaway
Alice Murr

Reviewers

Akintayo Ajayi
Sami Al-Shaher
Srija Allam
Reddy Deepak
Antiya Richard
Baker Daniel
Balmer Songbo
Bu Jonathan
Flack Aditya
Garg Iftikhar
Javed Shamik
Kacker Rahul
Kalva
Chad Kliewer
Kimberley Laris
Steven Lorenz
Dr.Ron Martin
Sonia Mishra
Prateek Mittal

Denis Nwanshi
Meghana Parwate
Mithilesh Ramaswamy
Maureen Rosado
Michael Roza
Naveen Rudraradhya Kumar
Yeliyyur
Osama Saleh
Paul Simmonds
Amit Singh
Nelson Spessard
Bryant Tow

CSA Staff

Erik Johnson
Stephen Lumpe
Stephen Smith

スポンサーについて

当社はソフトウェアとクラウドに特化したITソリューションプロバイダーであり、組織が俊敏で革新的であり、人々が仕事に従事し、つながり、創造的になれるよう支援します。私たちは、高度なソフトウェア資産管理手法と能力によってサポートされた、セキュアでAIを活用したクラウドおよびデジタルワークプレイスソリューションを提供することで、これを実現します。カスタマーサクセスフレームワークを通じて、IT支出を削減し、テクノロジーを最適化し、顧客をサポートすることで、顧客の価値を創造します。

ビジネス主導のイノベーション。私たちは、歓迎され、包括的で、考え方も経験も多様な、非常に意欲的でパフォーマンスの高いチームであり、カナダと米国のGreat Place to Work®に認定されています。私たちの詳細については、www.softchoice.comを参照してください。

目次

要旨

この文書の目的は、中小企業（SMB）が組織を保護するためにゼロトラスト戦略の実施を通じて特定されたリスクを管理するアプローチを評価する際の、基礎となるガイダンスを提供することです。このガイダンスは、ジョン・キンダーバーグ（John Kindervag）が最初に策定し広めたNSTAC Report to the President of the United States on Zero Trust and Trusted Identity Management [1] に記載されている 5 段階のゼロトラスト実装プロセスに沿ったものです。Cloud Security Alliance（CSA）は、ゼロトラストアーキテクチャを構築し、成熟させるための、より高度なコンセプトとガイダンスを含む追加の研究文書を作成しており、今後もニーズの優先事項に応じて開発を継続する予定です。

これらの進化する原則を詳述した基本ガイダンスは、中小企業がゼロトラストを中核的なサイバーセキュリティ戦略として採用する際の指針となります。中小企業特有の課題について議論し、ゼロトラストアーキテクチャを評価、実装、そこから恩恵を得るためのロードマップを提供します。CSA Zero Trust Guiding Principles[2]の基本ガイダンスの中小企業向けの先駆けとして、この文書では、5 段階の方法論にわたって中小企業に合わせた関連する文脈と実践的なステップを提供しています。

想定読者

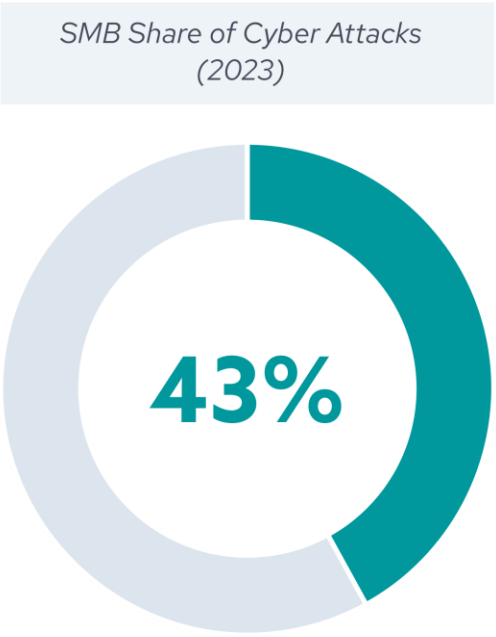
- 主な対象者：SMBオーナー、IT/セキュリティチーム、vCISO、アウトソーシング/マネージドITおよびセキュリティサービスのバイヤーおよびプロバイダー、マネージドサービスプロバイダー
- 第二の対象者：ビジネスマネージャー、中小企業の経営陣／リーダーシップチーム、オフィスマネージャー、事務スタッフ、中小企業の従業員、外部IT監査人および評価者

なぜ中小企業はセキュリティに関心を持つべきか？

中小企業は世界の売上高の約40%に貢献していますが[3]、効果的なサイバーセキュリティ対策を確立する上で、しばしば大きな障害に遭遇します。障害には、ビジネスリスク許容度に対する理解の浅さ、サイバーセキュリティのための限られたリソース、競合するビジネスの優先事項、熟練した従業員の育成と維持、有能なテクノロジーパートナーとの既存の関係、急速に進化するサイバー脅威の状況に適応する能力などがあります。中小企業の経営者の多くは、サイバー犯罪者は大企業だけをターゲットにしており、自分たちは小さすぎてターゲットにならないと考えています。しかし、この誤解は中小企業にとっ

[1] NSTAC Report, page 7
[2] CSA Zero Trust Guiding Principles
[3] What are SMBs?

て壊滅的な結果をもたらす可能性があります。



中小企業に対するサイバー攻撃の影響は、経済的にも評判的にも壊滅的なものになる可能性があります。最近の研究では、以下のことが明らかになっています。

- 昨年のサイバー攻撃の43%が中小企業を標的としており、その平均コストは331万米ドルでした[4]。
- 2023年には中小企業の41%が事件の被害者となり、2022年から3%増加しました[5]。
- 中小企業の60%は、直接サイバー攻撃を受けた後、6ヶ月以内に廃業しています[6]。

中小企業は、知的財産の損失、顧客の信頼低下、手頃な保険や資金調達、融資枠の確保といった、サイバーインシデントによる間接的ではあるが重大な影響に直面しています。これらは、企業規模に関係なく、強固なサイバーセキュリティ対策が不可欠であることを強調しています。

サイバー犯罪者は、攻撃の規模や到達可能性を拡大する手段として中小企業を攻撃することがよくあります。現実の顕著な例として、2013年に発生したアメリカの大手小売業者の情報漏洩事件があります。攻撃者は空調設備業者を経由してアクセスし、4,000万件以上のクレジットカードとデビットカードのアカウントが侵害されました。同様に、あまり公表されていませんが、インターネットに接続された脆弱な水槽を通じてカジノがハッキングされた事件もあります。中小企業の保護は、規制当局、立法者、標準化団体にとって優先事項であると広く認識されています。

中小企業に対する攻撃には、しばしば以下のようなものがあります。

- ランサムウェア：データを暗号化し、復号の代金を要求
- データ侵害（別名：Exfiiltration）：顧客記録や財務記録などの機密情報への不正アクセスや盗難
- 知的財産（IP）の損失：独自のデータ、設計、または営業秘密を盗み、企業の競争優位性を損なう可能性
- アイデンティティ情報の盗難：クレデンシャルを悪用してシステムにアクセスし、情報を盗む
- 経済的損失：ビジネス電子メール詐欺（BEC）に関わる事件など、不正な電信送金や盗難。
- 運用停止：顧客へのサービス提供を妨げる。
- 金融犯罪：不正行為やマネーロンダリングのために侵害されたシステムを活用。

[4] SMB Budget for Cybersecurity
[5] Despite Awareness SMBs Still Highly Vulnerable to Cyber Attacks
[6] 60% of Hacked SMBs are Out of Business 6 Months Later

- 人的要因とその結果：サイバー攻撃は約39秒ごとに発生しており、侵害の95%近くは人為的ミスに起因する。

2025年までに、サイバー犯罪に関連する被害額は全世界で10兆5000億ドルに達すると予測されており、強固なセキュリティ対策の緊急性が浮き彫りになっています[7]。

中小企業には独自の特徴と、サイバーセキュリティのニーズがある

中小企業の価値は、彼らの技術に集中することと結びついています。中小企業は、官僚主義が少ない分、機敏さと革新性から利益を得ます。中小企業は、多くの場合、アウトソーシングされた IT マネージドサービスプロバイダ（MSP）に強く依存しており、マネージドセキュリティサービスプロバイダ（MSSP）や、少数またはリモートの仮想 CISO（vCISO）のためのコンサルタントなど、柔軟な外部セキュリティリソースを活用しています。

中小企業はサイバーリスクの影響を非常に受けやすく、インシデントが発生した場合、その影響は企業の存亡に関わる可能性があります。中小企業庁（SBA）の報告によると、中小企業の50%が少なくとも1回はサイバー攻撃の被害にあっており、攻撃を受けた企業の60%以上が廃業に追い込まれています[8]。

中小企業は、サードパーティのリソースによってもたらされるセキュリティポスチャーのリスクに対して責任を負い続けるため、プロバイダーを賢く選択する必要があります。中小企業とそのプロバイダーとの間でセキュリティ責任を明確に定義し、調整することで、ストレス下でコストのかかるセキュリティエラーを減らすことができます。例えば、リスクの高いデータを扱う産業では、コミュニティへの被害を最小限に抑えるため、迅速なインシデント対応が義務付けられています。しかし、その効果は、ベンダーやサービスプロバイダーとの意図的な連携に依存しており、このような分野の中小企業にとって連携は不可欠です。

基本を忘れずに

ゼロトラスト戦略の一環として、まずは特定の基本的なセキュリティ対策を実施することが推奨されます。これらの要素をすべて盛り込むことよりも、前進させることが重要なのです。これらは確固とした前提条件ではありませんが、しばしば健全なゼロトラスト戦略を効果的に構築するための基礎となる構成要素として機能します。以下の推奨事項はすべてを網羅しているわけではありませんが、中小企業がセキュリティアーキテクチャの一部として考慮すべき最低限の基準のリストです。これらの

[7] Cybersecurity Statistics 2024
[8] The Impact of Cybersecurity on Small Business

対策は、中小企業が直面する5つの主要な制約を背景に書かれています。

- 自社にとっての真の脅威に対する認識が低い
- サイバーセキュリティ対策への投資の重要性を過小評価しがちです
- 技術的専門知識の欠如
- 適切な資金の不足
- 競合するビジネスの優先事項がサイバーセキュリティの取り組みよりも優先されることが多い

中小企業が事業を開始する前に考慮すべき基本的な推奨基準は以下の通りです。

- **エンドポイント保護ソフトウェアをデプロイする：**すべてのクライアントおよびサーバーシステムは、最新のウイルス対策ソフトウェアまたは Endpoint Detection and Response（EDR）ソフトウェアを使用する必要があります。さらに、ソフトウェアに自動更新機能が含まれていることを確認し、メンテナンスを簡素化し、人による見落としのリスクを減らします。
- **システムやソフトウェアアプリケーションに定期的にパッチを当てる：**ほとんどのオペレーティングシステムとソフトウェアアプリケーションは、自動アップデート機能を提供しています。もしそうでなければ、中小企業は重要なアップデートやパッチをインストールするための定期的なプロセスを確立すべきです。IT環境をスキャンして脆弱性を特定し、是正措置を講じるツールやサービスの活用を強く推奨します。さらに、ベンダーのサポートが終了したオペレーティングシステムやアプリケーションは、可能な限りサポートされたバージョンにアップグレードしてリスクを軽減すべきです。サポートされているバージョンの維持やアップデートのインストールを怠ると、侵害の可能性が著しく高まります。
- **従業員にセキュリティ意識向上トレーニングを実施する：**人間の行動は、依然としてサイバーセキュリティにおける最大の脆弱性の一つです。2024 Verizon Data Breach Investigations Report（DBIR）によると、データ侵害の68%に人的要因が関与していることが浮き彫りになっています[9]。万全を期すことはできませんが、中小企業にとっては、セキュリティを意識する企業文化を醸成するためだけでも、ある程度のレベルの継続的なセキュリティ意識向上トレーニングを実施することが重要です。中小企業を標的とする脅威が進化し続ける中、リモートブラウザ分離のような技術的コントロールは、より効果的な予防策を提供します。成熟度の低い組織では、トレーニングはエンドユーザーが被害に遭うリスクを最小限に抑える仕組みとして役立ちます。予算に見合ったセキュリティ意識向上トレーニングソリューションは数多く存在します。
- **重要なシステムとデータのバックアップを定期的に実行する：**データと重要なシステムの可用性は、あらゆるビジネスが機能するために不可欠です。サポート可能な頻度で、データとシステムのバックアップを定期的に実行することが重要です。また、バックアッププロセスが、バックアップを狙うことが多いランサムウェアの脅威に対して耐性があることを確認することも重要です。中小企業は、バックアップを復元できるかどうかもテストする必要があります。

[9] Verizon DBIR 2024, page 8

- **機密データへのアクセスを制限し、適切に保護する：**さまざまな業種の中小企業は、知的財産（IP）、財務情報、個人情報（PII）、ソフトウェアコードなど、特定の機密データを持っている可能性があります。これらのデータへのアクセスは積極的に管理し、必要な場合にのみ許可し、必要なくなったら取り消す必要があります。機密データは、保存時にも暗号化する必要があります。社内のITチームやMSPは、中小企業がこれらのベストプラクティスをサポートできるように、管理可能なプロセスを提供する必要があります。
- **パスワードレスを優先し、強力なパスワードポリシーを実装する：**パスワードは歴史的に、アカウントや機密情報をセキュアにするための第一の防御線でした。中小企業は、CISA（Cybersecurity and Infrastructure Security Agency）が推奨するベストプラクティスに準拠した強力なパスワードポリシーを導入する必要があります[10]。
- **可能な限り多要素認証（MFA）を利用する：**MFAは、アカウントの乗っ取りを防ぎ、不正アクセスのリスクを最小化するための極めて効果的なコントロールです。
  さらに、MFAは中小企業のゼロトラストアーキテクチャにおいて、非常に重要なビルディングブロックとして機能します。MFA は、認証されたアクセスが重要なビジネスシステムや機密性の高い組織データに提供される場合、どこでも採用されるべきです。MFA プロンプトを使用して定期的に再認証を行い、その効果を高めます。SMS ベースの MFA は、漏洩する可能性があるため、使用すべきではありません。フィッシングに強い MFAを可能な限り使用すべきです。
- **仮想プライベートネットワーク（VPN）ソリューションを使用したセキュアなリモートアクセス：**オンプレミスのリソースへのリモートアクセスを許可する必要がある中小企業では、VPNソリューションを活用する必要があります。VPNは、中小企業が、内部ネットワーク全体ではなく、必要な資源へのアクセスを明示的に許可するなど、ゼロトラストの原則に沿ったリモートアクセスソリューションで必要性を代替できるようになるまでの一時的なソリューションであるべきであることに注意することが重要です。ゼロトラストネットワークアクセス（ZTNA）ソリューションは、これらの機能を提供します。

より詳細なガイダンスを提供するリソースへのリンクについては、Appendixを参照してください。

[10] CISA Password Guidance

ゼロトラスト入門

ゼロトラストは、情報セキュリティ（InfoSec）に対するシンプルなアプローチですが、しばしば誤解されやすく、複雑すぎると思われがちです。ゼロトラストの哲学と戦略を正しく理解すれば、組織はセキュリティの強化、レジリエンスの向上、デジタルトランスフォーメーションの指針として利用できる貴重なツールとなります。これらのツールは、相互に有益な方法でAIに適用することもできます：AIはゼロトラスト戦略の実施を支援することができます。

ゼロトラストは、2023年バイデン大統領令[11]によって米国のすべての連邦機関に義務付けられており、欧州連合（EU）のデジタルオペレーションレジリエンス法（Digital Operational Resilience Act（DORA））やNetwork and Information Security（NIS2）指令などの取組みを通じて、世界的に採用されています。

歴史的に、情報セキュリティは技術的コントロールに大きく依存しており、セキュリティモデルは資産を収集し、コントロールされた物理的境界内に囲い込む能力に基づいていましたが、もはやそうではありません。特に、在宅勤務やWi-Fiの普及、クラウド技術の利用拡大が当たり前の世界ではなおさらです。このシフトにより、セキュリティは境界からデータそのものへと移行し、これはほぼすべてのアプリケーションがインターネット経由で接続されているため不可欠です。

これまでユーザーは、組織の境界内の場所に基づいて「信頼されている」とみなされてきました。ゼロトラストは、資産へのアクセスを許可する前およびその後も継続的に、場所に関係なく検証を要求することで、この概念を覆します。

ゼロトラストは、「決して信用せず、常に検証する」といった長年の原則、最小特権の概念、セグメンテーションの実践を活用し、サイバーハイジーンを向上させ、インシデントによるコストと損害を削減し、迅速な復旧を促進します。

既存のセキュリティ対策をゼロトラストの原則で補強することで、組織は複雑で分散した環境で資産を保護するための強固な基盤を確立することができます。このプロアクティブなアプローチは、セキュリティポスチャーを強化し、進化する脅威の状況に関連する潜在的なリスクを最小限に抑えます。

ゼロトラストはまた、侵害が起こることも認識しています。レジリエンスを高めるために、ゼロトラストは「影響範囲」を抑制し、侵害の影響を軽減しながら、迅速な復旧を促進する手段を提供します。これらの同じテクニックは、悪意のあるアクターが必要とする作業と投資を増加させ、インシデントの可能性をさらに低下させます。

[11] Executive Order on Improving the Nation's Cybersecurity

CSAのゼロトラスト指針となる原則[12]は、ゼロトラストの根底にあるテーマをマッピングした優れたリソースです。読者は、より深い理解のために確認し、以下のような提案を見直すことを強くお勧めします：

- 結果を念頭に置いて始める（ビジネス／ミッションの目的）
- 複雑にしすぎない
- 製品が優先事項ではない
- アクセスは意図的な行為である
- アウトサイドインではなくインサイドアウト
- 侵害は起こる
- 組織のリスク選好度を理解する
- トップの姿勢を保証する
- ゼロトラスト文化を浸透させる
- 小さく始めて、すぐに効果がでることに集中する
- 継続的に監視する

最後に、すべての強力なゼロトラスト戦略には、反復の理解が組み込まれています。中小企業は、成功の鍵はコントロール体制の反復的な強化にあることを認識すべきです。中小企業はこのことを予期し、継続的な改善に備えるべきです。完璧は進歩の敵であることを忘れてはなりません[13]。

[12] CSA Zero Trust Guiding Principles
ゼロトラスト指針となる原則

[13] Winston Churchill - Where Ideas, Experiences, and Lessons Learned Intersect

ゼロトラスト実施プロセス - 5つのステップ

ステップ 1 -資産の目録と評価

ゼロトラスト導入のための5つのステップのプロセスというより広い文脈では、**ステップ1は「Defining Your Protect Surfaces」**と呼ばれています。プロテクトサーフェスとは、重要なデータ、アプリケーション、資産、サービス（DAAS）で構成されるビジネスシステムのことで、事業運営にとって重要であったり、サイバー脅威の影響を受けやすかったりするため、その保護が必要となります。このプロセスは、中小企業が取り組みの優先順位をつけ、最も重要な分野にリソースを集中させるために役立ちます。このテーマについては、幅広い民間組織および公的機関向けの詳細なガイダンスが存在します。本書では、中小企業に関連する主要な側面と活動に焦点を当てますが、より複雑なシナリオについては、詳細なガイダンスが役に立つかもしれません。

プロテクトサーフェスを定義するプロセスの中心は、さまざまな種類の技術資産をインベントリ化し、分類することです。重要なビジネスシステムとサービスを最初に特定します。次に、組織にとっての最も重

要度が高く、現在のセキュリティ成熟度が最も低い順に、リストの優先順位をつけます。プロセスの次のステップは、各ビジネスシステムを構成するDAAS要素を特定することです。

DAASの要素には、機密性の高い価格情報（データ）、ビジネスを推進する物理的インフラストラクチャー（資産）、重要なビジネスアプリケーション（アプリケーション）、アイデンティティとアクセス管理などの主要な技術サービス（サービス）など、さまざまなリソースが含まれます。侵害された場合、事業運営に支障をきたす資産を特定することが重要です。資産のインベントリと評価では、保護すべき資産の優先順位を決定するためのインプットとして、自社が責任を負い、依存している資産、それらが侵害された場合のビジネスへの影響、現在のセキュリティ成熟度を知ることです。重要なシステムはサイバー犯罪者の標的となることが多いため、組織のリスクを効果的に管理するためには、その保護を継続的に再評価する必要があります。

各デバイスの脆弱性と機密情報へのアクセスレベルを理解することは非常に重要です。さらに、DNSやディレクトリサービスなど、組織のアプリケーションや資産が依存する重要なサービスについても概要を説明すべきです。これらのサービスの中断は、業務に重大な影響を及ぼす可能性があることを認識してください。中小企業はまず、以下の基準を満たす資産に焦点を当てるべきです。

- 重要度：在庫管理、ERP、CRMソフトウェアなど、日常業務に不可欠なシステム、および収益の向上に関与するシステム
- 機微性：顧客情報、知的財産、財務記録、その他機密性の高い組織データを含むデータリポジトリ
- 脆弱性：既知のセキュリティ課題または外部への露出があるシステム

中小企業はリソースが限られていることが多いため、効率を高めるために推奨される戦略は、関連するDAASの要素をグループ化し、それらを1つのユニットとしてセキュアにすることに重点を置くことで、プロテクトサーフェスをさらに細分化することです。例えば、CRMシステムとそれに関連する顧客データをひとつの保護対象として考えてみましょう。

優先順位をつけることも中小企業にとっては重要です。顧客データや金融取引システムなど、最も機密性の高い、あるいは最もリスクの高い要素を優先すべきです。財務上の損失を回復するためのサードパーティサポートコスト、風評被害、規制上の罰則などの要因を考慮し、各プロテクトサーフェスが侵害された場合の潜在的なリスクとビジネスへの影響を評価します。このアセスメントにより、早急な対応が必要なプロテクトサーフェスの優先順位が決まります。

中小企業のITチームやそのMSPは、このプロセスを反復的に実施し、まずは試験的なプロテクトサーフェスから始めて経験を積むべきです。これには、変更管理プロセスに適切に対処しつつ、プロセスを検証するために、それほど重要でないシステムを含む可能性があります。スコープは、資源の利用可能性、予算、優先順位、望ましいリスク削減に基づいて、徐々に拡大することができます。中小企業は現在の状態から始めて、自由に使える資源を活用すべきです。大規模な投資は必要なく、むしろ既存のツールやテクノロジーへの投資を活用すべきです。

DAASのインベントリを維持するプロセスは、これらの要素が絶えず変化する可能性があるため、継続的に見直す必要があります。中小企業のリーダーシップチームは、そのプロセスを通じて教育を受け、最新の情報を得るべきです。スタッフは、ゼロトラストの原則を認識し、プロテクトサーフェスの重要性を理解し、自分の行動がセキュリティ全体にどのような影響を及ぼすかを認識すべきです。

最後に、中小企業は拡張性を計画すべきです。中小企業が成長したり縮小したりした場合、ゼロトラストのプロテクトサーフェス戦略は、それに応じて適応できるように柔軟でなければなりません。プロテクトサーフェスは、ビジネス環境の変化や新たなセキュリティ脅威に対応できるよう、定期的に見直し、更新する必要があります。この方法論に基づいたアプローチにより、中小企業は実用的かつ手頃な価格でゼロトラストプロテクトサーフェス戦略を確立することができ、過度に複雑で高価なソリューションを必要とすることなく、重要な資産を効果的に保護することができます。

資産管理とプロテクトサーフェスの定義という重要な仕事には、経営陣の賛同と全体的な優先順位付けされたアプローチが必要です。そのため、MSPを活用することで、中小企業の能力と専門知識を拡張することができます。中小企業は小さく始めて、進歩に向けて管理しやすいステップを踏むべきです。これらのステップを踏み、文書化することで、他の組織に製品やサービスを提供する際に、競争上の優位性としてデューデリジェンスを証明することができます。

ステップ 2 -テクノロジーがビジネスを推進する理解

ゼロトラスト実装の5つのステッププロセスのより広いコンテキストとして、**ステップ2の** タイトルは「Mapping the Transaction Flows」と呼ばれます。これは、システム、データ、資源間の依存関係と相互作用をマッピングする事からなります。これは非常に重要なステップであり、その結果、テクノロジー依存とコアビジネスプロセスの両方を深く理解することになります。
トランザクションフローをマッピングするために、中小企業は、ステップ 1 で特定したプロテクトサーフェスの優先順位リストを再検討する必要があります。これらのプロテクトサーフェスは、組織のオペレーションにとって重要なDAASが含まれます。分析する重要な業務システムを選択することから始めます。たとえば、住宅建設サービスを提供する中小企業であれば、WebサイトのWebホスティングプラットフォーム、会計ソフトウェア、CADソフトなどのコンポーネントを、その保護対象として特定します。中小企業やそのMSPが、相互作用の分析に優先順位をつけ、理解することに時間をかければかけるほど、各サブシステムに対するゼロトラストコントロールの策定がより効果的になります。

中小企業がプロテクトサーフェスを定義したら、他のビジネス利害関係者と深く繋がり、すべての要素が考慮されていることを確認し、その結果を検証する必要があります。この協力的なアプローチにより、重要な要素が見落とされることなく、サイバーセキュリティへの取り組みがビジネスのニーズや優先順位と一致するようになります。これらの要素には、製品設計などのデータ、CADアプリケーション

などのアプリケーション、アプリケーションをホストするサーバーなどの資産、クレジットカード決済アプリケーションなどのデータが含まれる場合があります。

中小企業は、プロテクトサーフェスと相互に作用するユーザーを特定します。これには、社内従業員、社外顧客、パートナー、第三者サービスプロバイダーなど、社内外のすべての利害関係者を理解することが含まれます。アイデンティティ管理システム、顧客データベース、さらには人事（HR）チームやビジネス機能リーダーとの話し合いなどのリソースを利用して、さまざまなユーザータイプを特定し、関連するユーザー交流情報を収集します。

次に、プロテクトサーフェス領域内外との依存関係や相互作用を特定します。これには、相互接続されたシステム、バックエンドデータベース、ネットワークインフラストラクチャー、および特定のワークフローへの依存関係の分析が含まれます。例えば、地方銀行では外部の金融機関、外部の監査人やコンサルタント、そしてActive Directoryのような内部システムとやり取りをする場合があります。これらのシステムがどのようにデータを交換し、または共有資源に依存しているかを文書化します。この手順は、プロテクトサーフェス領域との全ての相互作用を特定するのに役立ちます。現実的なアプローチとしては、ネットワーク図、アーキテクチャ図、データフロー図などの利用可能なリソースを使用することです。中小企業とそのMSPは、ネットワークトポロジー、ソフトウェアシステム構造、データフローを視覚化する必要があります。これは、トランザクションを処理する入口と出口、サービス、およびプロセスを特定するのに役立ちます。さらに、スキャンツールとモニタリングツールを活用することで、トランザクションの流れをリアルタイムで把握することができます。

これらの情報をすべて収集したら、さまざまな関連ソースからのデータを関連付けて詳細なトランザクションフローをマッピングし、理解を深めるための視覚的な表現を作成し、ビジネス内の関連する関係者とこれらのフローをレビューして明確さと正確性を高めます。

最後に、ドキュメンテーションマップに基づいてプロテクトサーフェスを検証し、再調整します。このマッピングを使用して、各プロテクトサーフェスのリスクとセキュリティの成熟度を評価します。リスクと成熟度を理解し関連付けることで、より効果的に優先順位をつけることができます。規制遵守要件や中小企業のリスク許容度などの要素を考慮します。プロテクトサーフェスの定義と保護を強化し、十分に包括的で、進化する脅威に適応できるように調整します。このステップは、ゼロトラストアーキテクチャを微調整し、中小企業からの真の関連性とビジネスコンテキストを含めるのに役立ちます。

ステップ3 - ゼロトラストアプローチの設計

ゼロトラスト実装の5つのステップのプロセスのより広いコンテキストとして、**ステップ3は、**「Build a Zero Trust Architecture」と呼ばれます。このステップでは、中小企業とそのMSPは、ゼロトラストア

ーキテクチャの設計を正式に開始します。これには、ステップ1と2の要素、その過程で収集されたビジネスコンテキストのほか、本書で前述した「基本を忘れずに」のセクションで説明した基本的なセキュリティ対策が組み込まれます。

実施する設計のスコープは、経営陣のコミットメントと、組織の目標に合致したセキュリティポリシーを包含するものにすべきです。セキュリティ目標が組織のビジネス目標と合致していれば、ゼロトラスト戦略を支えるために必要な投資に対し、必要な支持を集めることがはるかに容易になります。そのスコープには、人事、営業、マーケティング、顧客サービス、財務、法務など、中小企業のあらゆる職務のコンテキストも含まれていなければなりません。さらに、機密性の高いビジネスデータやシステムにアクセスできる外部の関係者、請負業者、コンサルタントも設計スコープに組み込む必要があります。ゼロトラストは重要なDAASを保護することなので、中小企業の従業員だけでなく、すべての関係者にとってゼロトラスト戦略のリスクとメリットを考慮することが重要です。

ゼロ トラストアプローチの開発を開始する際には、ゼロトラストアーキテクチャは製品に依存しないことを理解することが重要です。つまり、適切に実装されたゼロトラストアーキテクチャは、コントロールの要件に適合する限り、どのようなテクノロジーでも使用できるはずであり、適切に実装されていれば、将来的にベンダー／テクノロジーの変更が可能なほど柔軟であるべきです。

中小企業の目標は、ステップ2で定義したスコープと目標に基づいてゼロトラストアーキテクチャを設計することです。中小企業は、自社の環境にゼロトラストの原則とコンポーネントを実装することを可能にする適切なテクノロジー、ソリューション、ベンダーを特定し、選択する必要があります。中小企業はまた、ユーザー、デバイス、アプリケーションの動作と相互作用を管理するポリシー、ルール、ワークフローを定義し、文書化する必要があります。

重要な考慮点は、中小企業が事業を開始する際に法外な金額を費やすことに重点を置くのではなく、既存のテクノロジーへの投資を十分に活用することに重点を置くべきだということです。さらに、ゼロトラスト以外のテクノロジーやビジネスイニシアチブを検討し、それらを連携させることが戦略的に有益かどうかを判断することが推奨されます。

まず開始するには、中小企業またはそのMSPは、以下の質問を検討する必要があります。

- ゼロトラストアーキテクチャの中核となるコンポーネントと機能（アイデンティティとアクセス管理、デバイス管理、ネットワークセグメンテーション、データ保護、脅威の検知と対応など）は何ですか？
- 組織の要件（クラウドベース、オンプレミス、ハイブリッドなど）との整合性を確保するために、どのようにそれらを実装し、環境に統合しますか？
- ゼロトラストアーキテクチャのセキュリティ、信頼性、相互運用性（暗号化、認証、認可、ロギング、モニタリングなど）を確保するために従うベストプラクティスと標準は何ですか？
- ユーザー、デバイス、アプリケーションのアクセスやパーミッションを強制するコントロール機

能は何ですか？また、それらを設計のどこに配置しますか（例えば、最小特権、ロールベースのアクセスコントロール、属性ベースのアクセスコントロール、コンテキストアウェア、動的）？
- ゼロトラストアーキテクチャ（ユーザー／デバイス／アプリケーションのプロビジョニング、無効化、監査、更新など）を管理・維持するために実装するワークフローとプロセスは何ですか？

多くの場合、中小企業がすでに多要素認証（MFA）などのテクノロジーに投資している場合、重要なDaaSにアクセスする全てのシステムにMFAを拡張することは、ZTのユースケースを実現するための非常に基礎的な構成要素として機能することがよくあります。MFAプラットフォームの中には、より動的な性質に拡張できるものもあり、中小企業が組織内にMFAをデプロイする際に確立したプロセスを成熟させるために利用できます。
中小企業は、アーキテクチャ図、ユースケース、ユーザーストーリー、テストケースなどのツールや手法を使用して、中小企業がゼロトラストアーキテクチャを設計するのを支援することができます。米国Critical & Infrastructure Security Agency（CISA）の「ゼロトラスト成熟度モデル」（Zero Trust Maturity Model）の出版物[14]も、ゼロトラスト成熟度レベルを評価し、改善するための実用的なフレームワークとして活用できます。

もうひとつの有用なリソースは、米国 NIST SP 1800-35[15]です。この出版物では、ゼロトラストアーキテクチャを実装するために使用可能なアーキテクチャとテクノロジーについて深く掘り下げています。本書はどちらかといえば企業向けですが、中小企業でも採用できるさまざまなアーキテクチャの可能性の基礎について、包括的なガイダンスを提供しています。

ステップ4 - 設計の実装

ゼロトラスト実装の5つのステップのプロセスのより広いコンテキストとして、**ステップ4は、「Create Zero Trust Policies」**と呼ばれます。前のステップでゼロトラストプロセスを設計したら、次のステップでは実装をデプロイすることです。このステップでは、中小企業はプロテクトサーフェス内の資源へのトラフィックアクセスを許可するきめ細かいルールを提供するポリシーの作成に重点を置く必要があります。

このステップでは、オンプレミス環境とパブリック／プライベートクラウド環境を含む中小企業の環境全体で、適切な人やリソースだけが適切なデータやサービスにアクセスできるようにするゼロトラストのセキュリティポリシーとプロセスを作成します。中小企業はスモールスタートを計画し、管理可能で迅速な成果の達成に集中すべきです。多くの中小企業は、複雑なゼロトラストの成果を達成することを考えると圧倒されてしまうかもしれませんが、本来のメリットは、スコープを必要なだけ小さくできる

[14] US Government - Cybersecurity & Infrastructure Security Agency Zero Trust Maturity Model
[15] US Government - National Institute of Standards & Technology SP 1800-35 Implementing a Zero Trust Architecture

ことです。

多くの中小企業にとって、コストと複雑さへの感度を理解することの重要性を改めて強調する必要があります。新たなZTのユースケースが達成されるにつれて、ツールやテクノロジーへの既存の投資を活用する可能性を再検討することが大いに推奨されます。中小企業が、既存のツールやテクノロジーを使いながら小さく始めるというアプローチを組み合わせることで、ZTの結果を達成することが可能になり、困難が少なくなります。

投資対効果を評価する簡単なアプローチは、ZTアーキテクチャを実装するために必要な時間と技術投資に関連するコストと、重要なDAASがサイバーセキュリティインシデントによって長期間悪影響を受けた場合の財務的なビジネスインパクトとを比較することです。このような影響を明らかにする机上演習のような演習を通じて、中小企業のビジネスリーダーを指導することは、非常にインパクトのあるものになります。

中小企業がどのようなZTの成果を優先させるかを検討し始めたら、前のステップで作成したデータを重要なインプットとして使用します。例えば、**ステップ** 1で特定した資産データを見直し、ビジネスにおける重要性を理解することは、優先順位を決定する際の重要な検討事項となります。この資産に関する知識を、**ステップ2の**トランザクションフローのマッピングによって明らかになった、ビジネスを推進する重要なプロセスの理解と組み合わせることで、中小企業がどこに重点を置くべきかを理解する上で大きな助けとなります。

上記のステップから、保護のスコープ、価値、コストを組織のセキュリティポリシーにフィードバックし、コスト、期待されるリスク削減効果、組織への影響、脅威に対する耐性に基づいて、いつ、何を保護すべきかを決定することができます。これは、各脆弱性が強化されるにつれてリスクが軽減されるように、一歩ずつ段階的に進めるアプローチを強力にサポートするものです。

この新たな認識を既存のツールやテクノロジーとマッピングすることで、すぐに着手できる「low hanging fruit（簡単に達成できるもの）」を特定するのに役立ちます。このようなプロセスを受け入れることは、中小企業にとってゼロトラストの概念を簡素化し、その成果からどのようなメリットを得ることができるかを想像し、継続的な組織的支援のための強力で明確なビジネスケースを開発するのに役立ちます。

ステップ5 - 環境の監視と改善

ゼロトラスト実装の5つのステップのプロセスのより広いコンテキストとして、ステップ5は、「Monitor and Maintain Your Environment」と呼ばれます。このステップでは、先のステップを通して定義された KPI と測定基準に基づいて、中小企業のゼロトラストアーキテクチャの監視と改善を行います。中小企業は、ゼロトラストアーキテクチャのコンポーネントと機能から得られるデータとフィードバックを収集し、分析する必要があります。また中小企業は、ゼロトラストアーキテクチャのために実装されたポリシー、ルール、ワークフローを見直し、更新する必要もあります。

このステップで考えるべき質問は、以下のようにいくつかあります。

- ゼロトラストアーキテクチャのコンポーネントと機能（ログ、アラート、レポート、ダッシュボードなど）から、どのようにデータとフィードバックを収集し、分析するか？
- ゼロトラストアーキテクチャのパフォーマンスと有効性は、以前に定義したKPIと測定基準（例えば、セキュリティインシデント、データ侵害、監査結果、ユーザー満足度）に対して、どのように測定し、評価するか？
- ゼロトラストアーキテクチャのギャップや弱点は、どのように特定され、対処されるか？（根本原因の分析、是正措置、教訓など）
- 中小企業は、組織や環境のニーズや期待の変化（フィードバックループ、継続的改善、イノベーションなど）に、どのようにゼロトラストアーキテクチャを適応させ、改善していくか？

ゼロトラストアーキテクチャの監視と改善に役立つデータ分析、フィードバック調査、パフォーマンスレビューなど、予算に応じたツールや方法が存在します。

サービスプロバイダーの関係

中小企業では、社内のリソース、経験、サイバーセキュリティの専門知識が限られているため、MSP、ソフトウェアサプライヤー、請負業者などの外部サービスプロバイダーに委任することが不可欠になっています。効果的な委任には、サプライチェーンの第三者を厳密に検証しながら責任を維持することが含まれます。CISAは、サプライヤーがセキュアな開発手法を順守していることを証明するようソフトウェア会社に要求することで、貴重なリソースを提供しています[16]。これは、すべてのソフトウェア製品とサービスの開発、運用、管理方法のセキュリティを検証するために適用されるべきゼロトラストの考え方です。

適切なMSPを選択することは、組織固有のニーズに対応する上で非常に重要です。社内の人員や能力に不足がある場合、MSPは中小企業にとって戦力となり、多額の財務投資や社内の人員を増やすことなく、セキュリティの成熟度を高めることができます。中小企業は、自社のネットワークを活用して、どのMSPにコンタクトする価値があるかを判断し、テクノロジースタックに最適なスキルセットを持ち、最適なサポート体制を整え、最も競争力のある価格設定を提供する、といった能力の適切な組み合わせを探すべきです。既存のサプライチェーンや調達プロセスが存在する場合、それらをコンサルティングサービスの調達にも適用することができます。評価すべき主な要素としては、MSPが同様の組織を扱った実績、SOC2コンプライアンスなどの認証、報告・モニタリングプロセスの透明性などがあります。

中小企業のためのサービスプロバイダーとの関係構築フレームワーク

- **デューデリジェンス：**中小企業は、外部のサービスプロバイダーを選ぶ際に、徹底的にデューデリジェンスを行う必要があります。
- **主な選考基準：**
    - **実績：**同様のニーズや課題を抱える組織を支援した実績
    - **認証：**SOC2 コンプライアンスなど、関連する業界認証の取得
    - **透明性：**報告およびモニタリングのプロセスに関するオープンで明確なコミュニケーション
- **能力：**MSPのスキルセット、サポート体制、価格設定を評価し、中小企業の具体的な要件との整合性を確認します。

[16] CISA Secure Software Development Attestation

- **調達：**一貫性のある効率的なベンダー選定のために、既存のサプライチェーンと調達プロセスを活用します。
- **ゼロトラストの原則：**セキュリティに対する責任を維持し、サプライチェーン内のサードパーティプロバイダーを厳格に検証します。MSPがゼロトラストプログラムの成熟度メトリクスに関する一貫性のあるレポートを提供するようにします。

サプライチェーン のリスクを認識

今日の相互接続されたグローバルなビジネス環境において、サプライチェーンのリスクは重大な破壊要因となっており、より高い意識と積極的な管理が求められています。組織が外部のベンダーやサプライヤーに依存するようになるにつれ、こうした第三者との関係に起因するサイバーセキュリティ上の脅威や混乱、その他のリスクにさらされる機会が増えています。

サプライチェーンリスク管理（SCRM）は、特に中小企業にとって、相互接続されたサプライチェーンへの依存度が高まり続ける中、もはやオプションではありません。ベンダーやサプライヤーのセキュリティを盲目的に信頼することは、もはや有効な戦略ではありません。中小企業は、潜在的なリスクを軽減するために、システムやネットワーク接続に関わるサードパーティとの関係を洗い出し、これらの重要な環境の強固なモニタリングを実施する必要があります。

包括的なSCRMプログラムは、かつてはそのコストと複雑性から大企業に限られていましたが、技術の進歩により、あらゆる規模の企業にとってこうした取り組みがより身近なものとなりました。今後、SCRMの方法論は、よりデータ主導で、費用対効果が高く、効率的なアプローチにシフトしていくことが予想されます。

結論

ゼロトラストアーキテクチャの採用は、世界中のあらゆる組織にとって不可欠なものとなっています。中小企業にとって、ゼロトラストアーキテクチャは、基本的なセキュリティツールのデプロイだけでは達成できない、より高度な防御を実現するためのイネーブラーとして機能するため、その重要性はますます高まっています。さらに、５ステップの方法論に従うことで、中小企業は侵害される可能性を大幅に減らし、重要なデータを適切に保護し、ユーザーアクセスを厳格にコントロールすることができます。コストを意識したアプローチをとることで、中小企業は、資金繰りに苦しむことなく、セキュリティ向上という望ましい成果を確実に達成することもできます。

この5つのステップからなる方法論は、中小企業がどの資産を優先的に保護する必要があるかを特定することから始まり、同時に現在のセキュリティポスチャーを評価します。

次に、組織はビジネスプロセスを評価し、それらを詳細にマッピングして、どのプロセスが最も重要であるかについての知識と認識を深める必要があります。中小企業はその後、ゼロトラストアーキテクチャを設計する必要がありますが、これは多くの場合、能力のあるMSSPと提携することで可能になります。MSSPはまた、ZTアーキテクチャの実装、ゼロトラスト環境のモニタリングと維持といった残りのステップに取り組むための貴重なリソースとなります。

セキュリティやレジリエンスの強化など、ゼロトラストがもたらす長期的な恩恵は、初期の努力をはるかに上回ります。ゼロトラストアーキテクチャを採用することで、中小企業は高度な脅威から業務を守り、DAASを適切に保護し、高度なビジネスレジリエンスを確立することができます。中小企業が大企業と比較して独自の課題に直面していることは事実ですが、ゼロトラストを採用することで、中小企業はビジネス目標をサポートする、より堅牢な環境を構築することができます。

Appendix

用語集

- CSA - Glossary
- CSA - SDP Glossary
- On2IT - Zero Trust Dictionary

参考文献

1. NSTAC - Report to the President on Zero Trust and Trusted Identity Management
2. CSA - Zero Trust Guiding Principles
3. What are SMBs?
4. SMB Budget for Cybersecurity
5. Despite Awareness SMBs Still Highly Vulnerable to Cyber Attacks
6. 60% of Hacked SMBs are Out of Business 6 Months Later
7. Cybersecurity Statistics 2024
8. The Impact of Cybersecurity on Small Business
9. Verizon DBIR 2024
10. CISA Password Guidance
11. Executive Order on Improving the Nation’s Cybersecurity
12. CSA Zero Trust Guiding Principles
13. Winston Churchill - Where Ideas, Experiences, and Lessons Learned Intersect
14. US Government - Cybersecurity & Infrastructure Security Agency
15. US Government - National Institute of Standards & Technology SP 1800-35 Implementing a Zero Trust Architecture
16. CISA Secure Software Development Attestation

有用なリソース

1. CSA - ZTAC Resource Hub
2. CSA - Zero Trust for Critical Infrastructure Security
3. NIST - Small Business Cybersecurity Corner
4. NIST - Small Business Information Security:The Fundamentals
5. NIST - Cybersecurity Framework 2.0, Small Business Quick-Start Guide
6. CISA - Cyber Guidance for Small Businesses
7. SBA - Strengthen Your Cybersecurity

8. FTC - Cybersecurity for Small Business
9. FCC - Cybersecurity for Small Businesses
10. CIS Center for Internet Security (cisecurity.org)
11. HBR - The Devastating Business Impacts of a Cyber Breach
12. SEC.gov - The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses
13. Verizon DBIR
14. 35 Alarming Small Business Cybersecurity Statistics for 2024

SMB(中小企業)のリソースと定義

1. Gartner - Small And Midsize Business (SMB)
2. US Dept. of State - What is a Small Business
3. Census.gov - What is a Small Business?
4. OECD - Enterprises by Business Size
5. Markaaz - SMBs are the Backbone of the Economy
6. Computer Weekly - SMBs Leaning More Heavily on MSPs
7. US Chamber of Commerce - The State of Small Business Now
8. Techround - 60% Of SMEs That Suffer a Cyber Attack Out Of Business Within Six Months
9. CISA - Securing SMB Supply Chains Resource Handbook

重要なSMBセキュリティインシデント

- Code Spaces (2014):This startup providing code hosting services went out of business after a cyberattack destroyed most of its data, including backups.
- VerticalScope (2016):A breach exposed 45 million user accounts from this network of online forums.The lack of multifactor authentication was a key issue.
- Click2Gov (2019):A breach that exposed credit card details impacted hundreds of municipalities using this web payment portal.
- Crystal Valley (2022):This agricultural co-op shut down operations for over a week due to a cyberattack on its systems.