Security White Paper 2023

ゼロトラストのはじめ方

段階的な移行を成功させる３つの要素

DX が進みハイブリッドワークが浸透するなど、多様化するビジネス環境において、安全かつ高い自由度で、組織内の重要データを活用することが求められています。そうした中、避けては通れないテーマが、ゼロトラストセキュリティへの移行です。しかし、どこから着手すべきか、頭を悩ませる企業も多いのではないでしょうか。本書では何を優先して移行を進めていくべきか、国産セキュリティベンダーの視点で、実装例とともに解説します。

2023 / 10

サイバー空間におけるリスク環境は、近年劇的に変化しています。組織内部では、DX（デジタルトランスフォーメーション）が確実に進み、ハイブリッドワークが浸透することで、これまでとは異なる働く環境が形成されつつあり、組織内の重要データへのアクセスも多様化しています。一方、侵入型ランサムウェアなど外部からの脅威が頻発し、組織の存続を脅かす事態も発生しています。

このような多様化するビジネス環境において、安全かつ高い自由度で、組織内の重要データを活用することが求められる中、避けては通れないテーマが、ゼロトラストセキュリティへの移行です。しかし、どこから着手すべきか、頭を悩ませる企業も多いのではないでしょうか。

本書では何を優先して移行を進めていくべきか、国産セキュリティベンダーの視点で、実装例とともに解説します。

ゼロトラストの段階的な導入

ゼロトラストを実現するソリューションは多岐にわたります。認証・認可から自動化まで、様々な側面からゼロトラストを実現していくことになりますが、すなわち、色々な側面で検討しなければばらないということにつながります。

ゼロトラスト構成要素	ソリューション例
認証・認可	IAM（Identity and Access Management） IDaaS（Identity as a Service）
ネットワーク	SASE（Secure Access Service Edge） SDP（Software Defined Perimeter） SWG（Secure Web Gateway）
デバイス	EMM（Enterprise Mobility Management） EDR（Endpoint Detection and Response）
クラウド	CSPM（Cloud Security Posture Management） CWPP（Cloud Workload Protection Platforms）
可視化	CASB（Cloud Access Security Broker） SIEM（Security Information and Event Management）
自動化	SOAR（Security Orchestration and Automation Response）

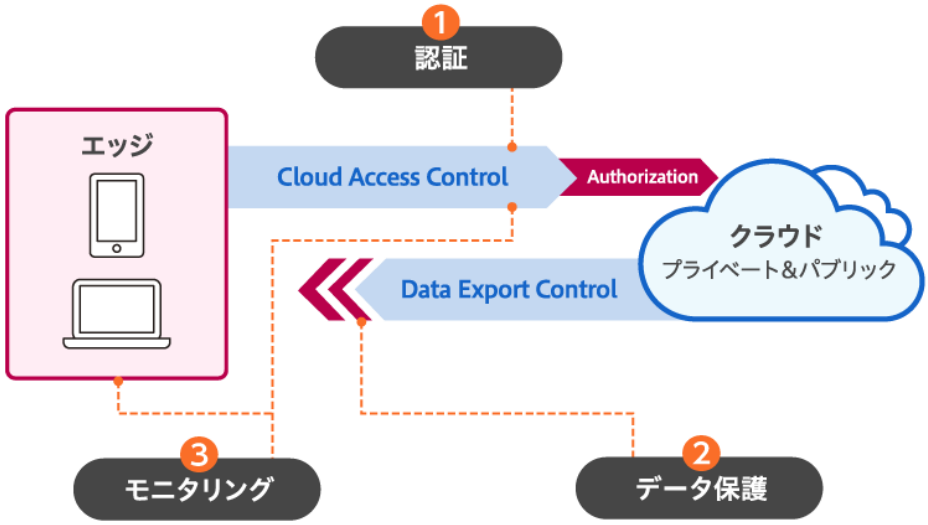
NIST（米国国立標準技術研究所）発行の「SP800-207：ゼロトラスト・アーキテクチャ」では、一気にゼロトラストに刷新することは難しいケースがあることを予見しており、ゼロトラストについて、**段階的に導入することを目指すべきであり、ゼロトラストと境界防御モデルのハイブリッド運用が継続されることを想定**しています。

つまり、検討・設計する上では、マイルストーンをおいて段階的に導入していくということと、これまで長年かけて実装してきた境界防御モデルとの併用を前提にすることの 2 点がポイントとなります。一部の解釈では、ゼロトラストは従来の境界防御モデルに代わるもの、と表現していることもありますが、共存・併用することが現実解となるわけです。

シンプルなアーキテクチャで考える

ゼロトラスト・アーキテクチャの採用を検討する場合、既存の境界モデルとの併用をしてもコストがかかりすぎないかなどを考えていくことになり、複雑あるいは二重コストになることを恐れる方もいるかと思います。そのため、できるだけシンプルなアーキテクチャで考えることをおすすめします。

ここでは、企業の重要データにアクセスする PC やスマートデバイスなどの「エッジ」と、データが保管されている「クラウド」の 2 つの括りを軸として、解決すべき課題をシンプルにした上で、『認証』『データ保護』『モニタリング』の 3 つの基本要素から優先して取り組む手法を解説します。

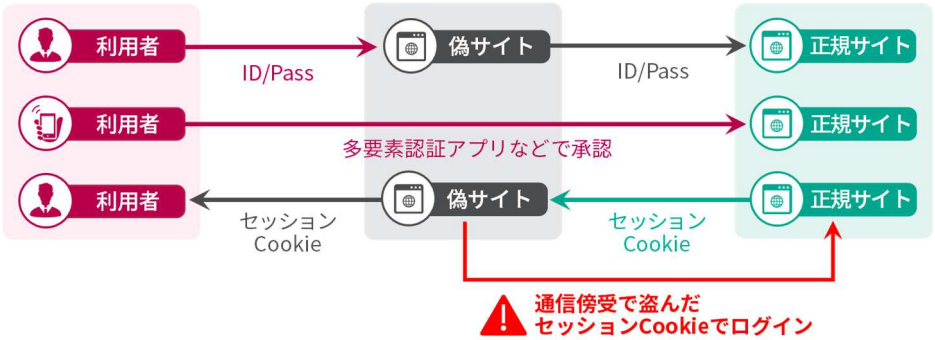


① 認証 … 多要素認証を突破する攻撃を防御

ゼロトラストでは“Untrust”が大前提で、すべてのアクセスを都度検証すべきという考え方に立っています。つまり、脅威の侵入が想定される経路における認証が対策の根幹となります。昨今のランサムウェア被害を見ても、ID・パスワードが詐取されて侵入を許してしまうケースも多いため、多要素認証（MFA）による対策の必要性が強調されており、実際、さまざまなサービスにおいて、多要素認証が日常的に使われ始めています。

ただ今日では、多要素認証を突破する攻撃が台頭しています。フィッシングサイトにターゲットユーザーを巧みに誘導して認証情報を入力させ、その情報を悪用して正規サイトへのセッション Cookie を盗み、認証情報を入力せずとも正規サイトにログインしてしまう AiTM 攻撃（Adversary in The Middle）という手法等がこれにあたります。

AiTM 攻撃のイメージ



この AiTM 攻撃のリスクを受け、これに対抗できる「フィッシング耐性がある多要素認証」として、デジタル証明書や FIDO2（公開鍵暗号を利用して認証を行う規格）が推奨されるようになりました。デジタル証明書は通信確立時に認証する手法のため、攻撃者は認証画面にたどり着けず、AiTM も成立しません。フィッシング耐性のほか、認証デ

バイス紛失時の対応や利用用途、対応 OS、またコストにおいても優位点があり、デジタル証明書は、企業・組織にとって採用しやすい多要素認証といえます。

	デジタル証明書	他の多要素認証（所有、生体）
攻撃耐性	攻撃者はログイン画面まで到達できない	攻撃者はログイン画面まで到達できる場合が多い ※
紛失時の対応	当該証明書をセンター側で失効し、新しい端末へ証明書の再発行する	緊急時の代替認証の手順を整備しておく。 物理デバイスの場合は代替機へ交換する。
利用用途	VPN、無線 Wi-Fi、クラウドサービスなど、様々な認証に利用できる	無線 Wi-Fi 認証に利用できないなど、用途が限られる
対応 OS	PKI 技術は実績豊富で信頼性が高く、マルチ OS で動作。	OS 毎に利用可能な認証要素が異なる場合がある

※FIDO2 や PIV スマートカードはフィッシング耐性有

大手鉄道会社様のゼロトラスト実装例

建設工事で利用するデータの共有のため、自社および協力会社からのクラウドサービスへのログイン認証に、デジタル証明書による多要素認証とシングルサインオンを適用し、安全性と利便性を両立されています。IT を専門としない建設工事部門の方が運用されていますが、『安心して展開でき、現場で困ることはない。管理者負担もかからず、管理画面も直観的で分かりやすい』と現場主導の DX 推進に成功されています。

② データ保護 … クラウドからデータを出さない方法

強固な認証で不正アクセスを排除した後は、クラウドに保存される情報資産、つまりデータ保護をどうするかということを考えることになります。データ保護には DLP（Data Loss Prevention）と呼ばれる、機密情報や重要データを自動的に特定し、データを常に監視、保護する機能が思い浮かぶかと思います。

フェーズ	Item	概要	問題点
導入段階	機密情報の分類	✓ 該当するキーワードで分類 例）機密・社外秘・住所・電話番号・クレジットカード・会計用語・電話番号	適切なキーワード設定が可能か？ 定期的に見直す必要があるか？
	データの保管ポリシー	✓ 機密情報を保管する場所を特定 例）機密情報という名前のフォルダ、特定のクラウドストレージ	組織全体で同一ポリシーによる運用を徹底できるか？
運用	流出経路の監視	✓ メール、チャット、外部ストレージ、USB メモリ、クラウドストレージ	シャドークラウド対策を考慮する必要はないか？
	データスキャン （定期／リアルタイム）	✓ ストレージ領域の定期スキャン ✓ データ操作のリアルタイム把握	現実的に可能か？ データ操作はどこまで追う必要があるか？

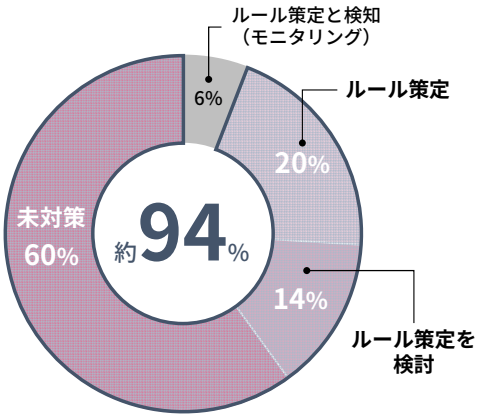
DLP : Data Loss Prevention の概要

最近は AI などを活用して楽にはなってきてはいるものの、導入段階でも運用段階でも考慮しなくてはならないことが多く、ある程度成熟した組織でなければ、DLP を精度高く運用することは難しいといった課題があります。

この課題の解決策として、クラウドからデータを出さないアプローチがあります。例えば、データ持ち出しを禁止する設定にした VDI（仮想デスクトップ）やリモートデスクトップ、セキュアコンテナやセキュアブラウザなどの手法です。既にある技術ですので、業務環境に合わせて最適なものを選択するだけで良いのですが、近年ではブラウザで完結する業務も増えているため、コストを抑えつつ実現する方式として、端末内仮想化の導入も浸透しています。

③ モニタリング … 業務の可視化と最適化

ゼロトラストにおいて、モニタリングが重要とされている理由の一つが「シャドークラウド」のリスクです。業務で指定されたクラウドサービスだけでなく、個人でもファイル送信や翻訳など広くクラウドサービスが利用されるようになってきました。正規ユーザーが、悪意というよりも過失に近い形で情報漏えいを発生させてしまうケースも増えており、IPA の調査では「シャドークラウドを把握する対策を導入していない」が約 94%と心配な状況が見て取れます。

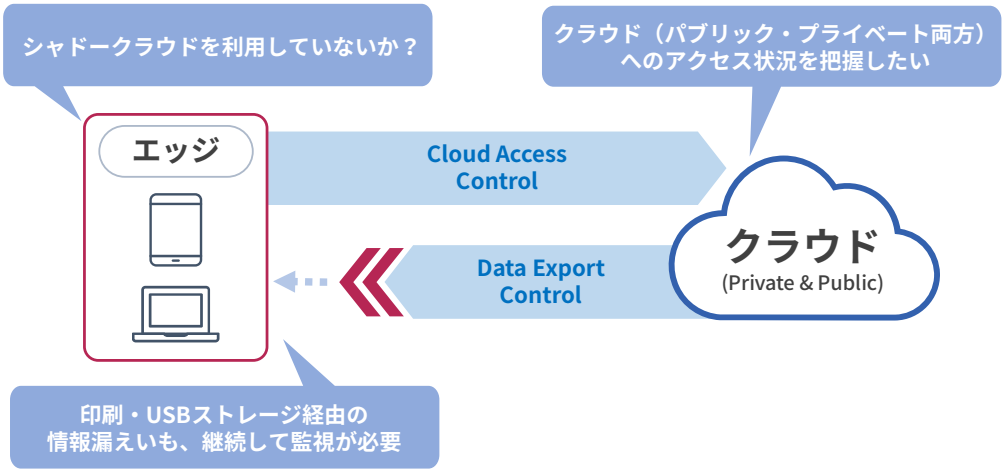


約94%が
シャドークラウドを
把握する対策を導入
していない

シャドークラウド
「組織のセキュリティ担当者が把握していない、
個人や部署が勝手に利用しているような
クラウドサービス」（IPA調査での定義）

IPA 「企業における営業秘密管理に関する実態調査2020」を元に弊社にて抜粋・編集
https://www.ipa.go.jp/security/fy2020/reports/ts_kanri/index.html

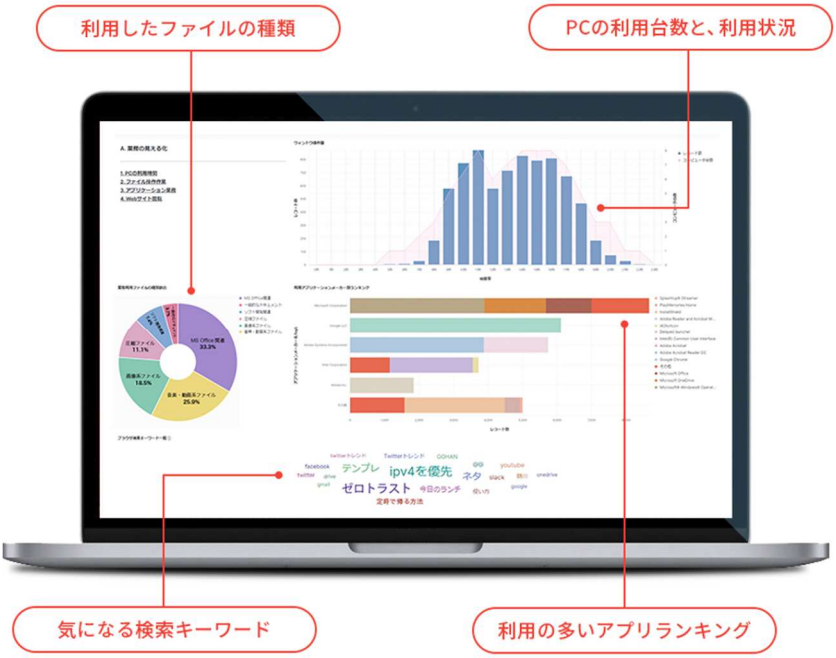
ハイブリッドワーク時代においては、シャドークラウドの監視だけでなく、もともとやってきていた印刷や USB ストレージの監視は必要ですし、クラウドに置かれた正規の IT へのアクセスに関しても把握する必要があり、モニタリングしなければならない範囲は拡がります。



準大手ゼネコン様のゼロトラスト実装例

建設現場では数多くのアプリケーションが利用されており、一昨年の試算では、全社員で年間 424 万回ものログイン操作が発生していました。一般的にも大企業では、200 近くのアプリケーションを利用しているケースも珍しくなく、ビデオ会議や E-mail の利用状況を確認するだけでは、業務実態を把握することが難しいのが実情です。

当該ゼネコン様では MFA と SSO の実施に加え、全社の PC 操作ログを取得しグラフィカルに可視化する、モニタリングサービスを利用することで、長時間労働対策（残業の多い部門の確認や、残業の業務の中身、どのアプリケーションやファイルを扱っていたかの把握等）やシャドークラウドを含めたクラウドストレージの利用状況把握（誰がどの端末でどのファイルをクラウドストレージにアップロードしたか等）を実施されています。



DX 戦略室様では、各部署からのリクエストに応じて業務分析レポートを提出し、働き方改革や業務改革につながる新たな気づきにもつなげられています。

さいごに

クラウドシフトやハイブリッドワークなどへの対応を考えると、ゼロトラストセキュリティの検討は必須となりますが、その導入は、費用対効果をみながら慎重に検討する必要があります。ゼロトラストは、段階的に最低限必要な部分からはじめて、リプレイスではなくアップデートできる形で進めていくことをお勧めします。

本書では、ゼロトラストへの移行を成功させる 3 つの基本要素を解説しました。従来の境界防御モデルとゼロトラストモデルが混在したハイブリッド環境であっても、この基本要素が大きく変わることはありません。シンプル化して考えることで、基本から足場を固め、激しい環境の変化にも柔軟に対応するゼロトラストセキュリティを実現していくことができます。

「ソリトンワンゲート」サイトでは、導入事例やデモ動画、ご利用用途に応じた各種設定ガイドを公開しています。ぜひ、アクセスしてみて下さい。

Security White Paper 2023

ゼロトラストのはじめ方　- 段階的な移行を成功させる３つの要素 -

SOGWP2310-A
発行　　2023 年 10 月
発行所　　株式会社ソリトンシステムズ
お問合せ先　　netsales@soliton.co.jp