『ゼロトラスト360』整備支援

日本企業は、従業員の多様化（非正規社員、転職者、多国籍、他）による価値観の変化をはじめ、新型コロナウイルス感染症対策のリモートワークやBYOD（Bring Your Own Device）の急増により、従来よりも強固なセキュリティが求められています。その実現のためには、社員への信頼を前提とした発想から脱却し、内部犯行を仮定したセキュリティ施策（『ゼロトラスト』の発想）を採り、自社のファシリティ、ITリテラシー、運用負荷、組織構造、業務プロセス等を多面的に考慮することが必要です。KPMGは、企業の状況を360°の方向から検討し、ゼロトラストのアーキテクチャの提供と、コンサルティングファームならではの情報セキュリティ環境の整備を総合的に支援します。

『ゼロトラスト』の概念と現状

これまでの企業の情報セキュリティは、戦国時代の城設計に例えるならば、城内に住む住人を信じて、外敵からの攻撃・侵入を防ぐための城壁や堀を幾重にも強化する設計ポリシーによって実装されてきました。しかし、内部のわずかな反乱によって城主が倒される史実もあるとおり、城壁を固めるだけの企業の情報セキュリティアーキテクチャのみでは限界が生じています。

働き方の多様化によって高まる内部犯行の脅威と『ゼロトラスト』の概念

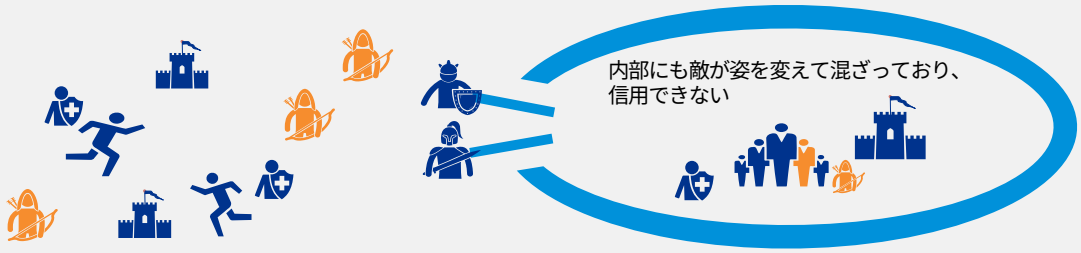
従来の情報セキュリティの守り方

幾重にも城壁（ファイアウォール）を強化し、外部の攻撃から内部を守る

『ゼロトラスト』に基づく情報セキュリティの守り方

内外からの攻撃を意識して、“守るべき対象”と“利用する人”を守るとともに監視をおこなう

※クラウド化・リモートワーク化の推進による守るべき対象の分散化



日本ではビジネス環境の変化だけでなく、派遣制度や転職を前提とした働き方の多様化によって人材の移動が流動化し、内部起因の情報セキュリティリスクが高まっています。このような内部犯行が発生しうる可能性に基づいてセキュリティを見直す思想が『ゼロトラスト（だれも信用しない）』です。しかし、城壁（ファイアウォール）に加えて、内部からの攻撃にも対応できる武器（ふるまい検知等のテクノロジー）や傭兵（モニタリング／相関分析テクノロジー／怪しい端末の隔離等）を単純に増強することは、コスト増加だけでなく無尽蔵に労力を消費する結果となり、必ずしも効率的とはいえません。確実なセキュリティの実現には、単発的なテクノロジー施策にとどまらないルールや要員育成、城構造再設計（IT設備、ファシリティ）などの組織横断的な施策の検討と実行が重要です。

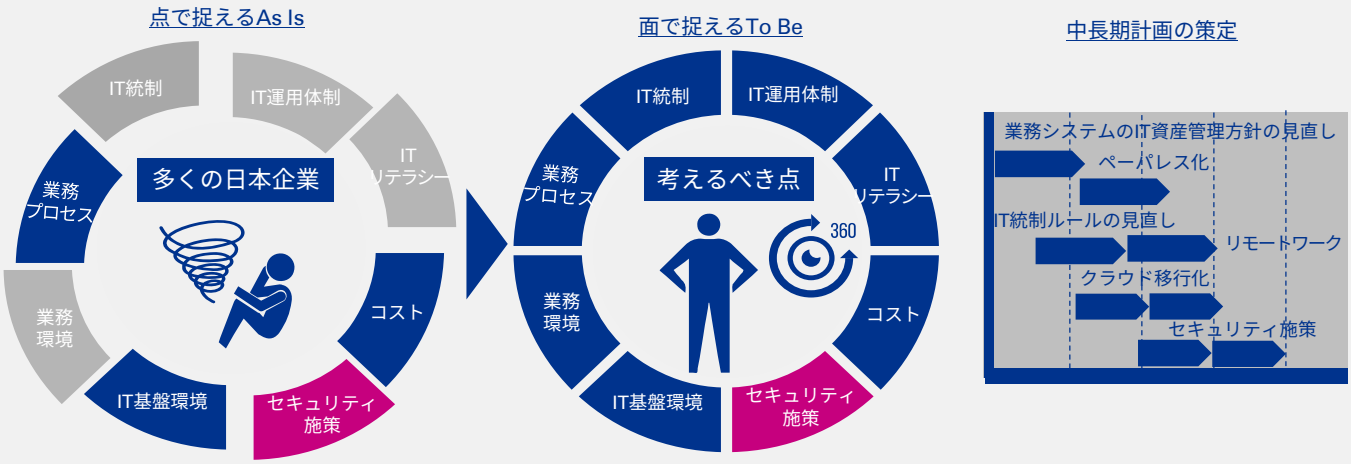
ゼロトラストの概念に基づく360°対策の進め方

ゼロトラスト・モデルによる設計思想は、十数年前より提唱されているものの、これまでは広く認知されていませんでした。昨今、政府をはじめ市場がその考え方を強く意識するようなった背景は、在宅ワークやクラウドの活用などによりビジネス環境が複雑化し、守るべき領域の境界が曖昧になってきたことに起因します。現在のビジネス環境に対して、事業部やシステム毎に個別に予算を計上してセキュリティ製品を導入することは、内部の管理・運用工数の増加リスクを孕みます。そのため、自社の業務プロセスやIT運用体制など、これまでは各部門が個別に対応していたものを、組織横断的視点（360°視点）で経営層が正しく現状把握・チェックする必要があります。それらを全社的な命題として、 IT部門・事業部門・管理部門が一体となり、情報セキュリティ施策と各部門の施策の関係性を考慮しながら、戦略的に中長期計画（ロードマップ）を策定することが不可欠です。

■ 経営層による組織横断的なトップダウン体制の構築

組織横断的な対応を行うためには、各事業部に任せていた事業システムの企画段階から、情報システム部門が情報セキュリティの観点をもって参画するなどといった、制度面の変更へとメスを入れることが求められます。トップダウンで情報システム部門が旗振り役を担って推進することができる組織体制と、役割に応じた権限の付与が必要です。

IT部門×事業部門×管理部門が三位一体となった体制によるゼロトラスト推進



■ ゼロトラストの検討対象領域

非ITインフラ領域を含めてやみくもにゼロトラスト化の検討を開始しても、範囲が広すぎるため、どこから手を付けるべきか容易に判断できません。効率的に推進するためには、下図のように検討観点をフレームワークを用いて可視化し、個々の領域にかかわるステークホルダーを明確化します。これにより、検討領域の位置づけと目的に関して、ステークホルダーと同じ目線で協議を行いながら施策を策定できます。またそうして協議を重ねることで、ステークホルダーとのリレーションシップを強めながら、情報システム部門がリーダーシップをとってゼロトラスト化を推進する土台を築くことが可能となります。

ゼロトラストにかかわる検討対象領域フレームワーク例

非ITインフラ環境領域	ゼロトラスト化に伴うITインフラ環境検討領域				ファシリティ領域
業務システムを含めたプロセス	端末環境		デスクトップ		オンプレアプリ基盤	クラウド基盤	オフィス環境
顧客、取引先とのリレーション維持	BYOD	会社貸与	非VDI	VDI	業務アプリ	SaaS	
IT組織／ガバナンス体制					グループウェア	PaaS	
社内規程／労務規程などのルール					メール、Web会議等	IaaS	
利用者のITリテラシー向上対応	統合認証基盤						
	通信インフラ環境（LAN、WAN、リモート4G/5G、Wi-Fi等）						
	情報セキュリティ対応・検知・対応機能						
	外部攻撃対策	統合認証、アクセス制御	情報漏えい、端末防御				
	EDR機能（Endpoint Detection and Response）		ログ相関分析機能				
	インシデント検知・分析・封じ込めサポート（SOC/CSIRT）						
	インシデント検知・受付	被害分析	封じ込め	リカバリ			
	セキュリティサポートデスク						
	ITサポート／ヘルプデスク						
	オンラインサポート	ITインフラリソース監視、管理	端末管理				
	ITサポートデスク（ヘルプデスク）機能						

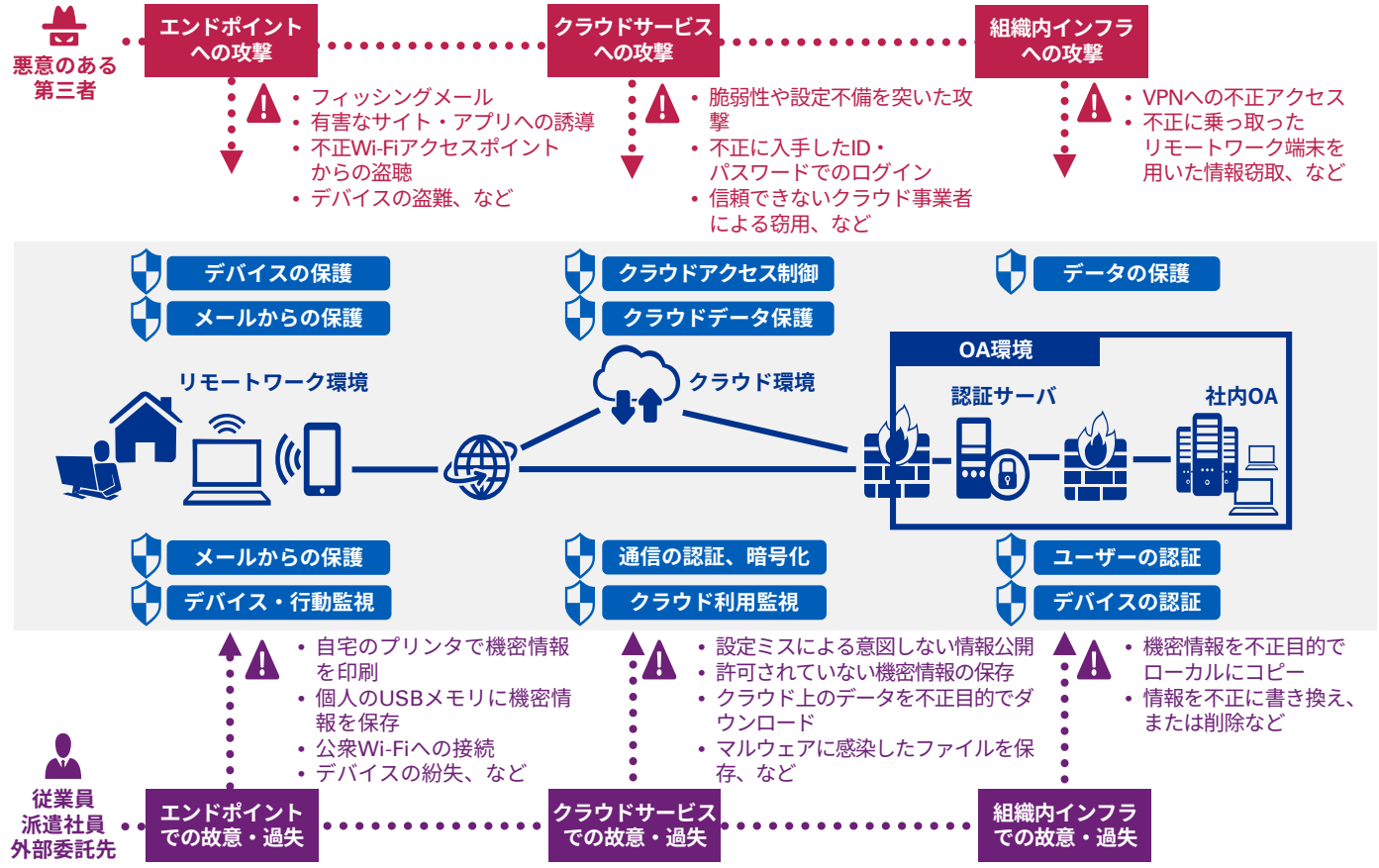
■ ゼロトラストセキュリティ対策の多層防御とは

ゼロトラストを実現する総合的なセキュリティ環境を実現するためには、既存のセキュリティ対策だけでなく、内部犯行を前提とした「多層防御」が重要です。多層といえば、ファイアウォールを重ねることや、ネットワーク、認証、データ暗号化などの施策（下図、セキュリティ対策例を参照）を多重に実装して守るイメージですが、現状のITアーキテクチャのまま実装すると、複雑性が増すばかりで運用が破綻するおそれがあるため、企業の現行構成や守るべき資産等の配置を考慮した適切な設計が必要となります。

対象	ゼロトラストセキュリティの考え方	対象セキュリテソリューション例
デバイス	• デバイスはオフィス内部に限らず社外のあらゆる環境で利用される（主にインターネット網を介した利用） • デバイスの認証を常に実施する • 全てのデバイスの保護を徹底する	• EDR（Endpoint Detection and Response）／EPP（Endpoint Protection Platform） • コンプライアンスチェック、可視化ツール • MDM（Mobile Device Management）
ID・ユーザー	• 内部・外部を問わず、ID・ユーザーを必ず検証する • ユーザーIDを多要素認証で検証する	• IAM（Identity and Access Management） • 生体認証、ワンタイムパスワード
アプリケーション	• 内部・外部を問わず、アプリケーションへのアクセスを制限し、不正操作を監視する	• 標的型メール対策 • WAF（Web Application Firewall） • UTM（Unified Threat Management）
通信	• 内部の通信も厳密に制限する • 内部・外部を問わず、送信元の検証、通信の真正性を確保する	• マイクロセグメンテーション • SDP（Software Defined Perimeter） • 通信の認証、VPN（Virtual Private Network）
データ	• 情報資産はクラウドなどの外部にも存在する • データが改ざんされないように保護する • データが漏えいしないように保護する	• データの暗号化 • DLP（Data Loss Prevention）
監視・ログ	• 内部・外部を問わず、脅威に対する監視・ログ分析によってITプロセスを可視化する • セキュリティ対応を自動化する	• CASB（Cloud Access Security Broker） • SIEM（Security Information and Event Management）／UEBA（User and Entity Behavior Analytics） • SOAR（Security Orchestration, Automation and Response）

■ ゼロトラストアーキテクチャの概念構成

実効性、運用効率性の高いゼロトラストアーキテクチャの設計には、各ソリューションを効率的に配したモデルを設計し、そのセキュリティチェックポイントに対する運用効率と、検知・対応の迅速性を最大化することが重要となります。すなわち、悪意のある第三者の攻撃を防ぐソリューションだけでなく、内部関係者（従業員、派遣社員、外部委託先等）のミスや不正の可能性も見越した、利用シーンに応じた漏れと無駄のない多面的なアーキテクチャ（ソリューション実装と監視運用）の設計が重要です。これにより余分な投資も運用負荷も極小化されたゼロトラスト環境が整備されます。



KPMGによるゼロトラストセキュリティ対策支援

■ IT投資計画（中期計画）／ロードマップ策定支援

IT中期計画策定支援

ゼロトラストセキュリティは、自社の業務環境と今後のIT・デジタル戦略およびテレワーク、クラウドなどの環境を十分に考慮し、多面的な施策の連携をもって適切なゴールを設定することが重要です。システムおよびガバナンスの観点から、企業が目指すあるべき姿の定義および実現プランの策定を支援します。

	フェーズ 1. ゼロトラスト化を考慮したあるべき姿の導出		フェーズ 2. ロードマップ策定	
作業内容	現状の可視化、ゼロトラスト化課題の導出	あるべき姿のデザイン	複数年計画策定	短期計画策定
	企業別フレームワークを策定し、領域別の課題をステークホルダと協議しながら定義	課題に対する施策を導出し、総合的に最適な施策を組み合わせた領域別のあるべき姿を策定	中長期的な目標と、それを達成するための道筋を策定	短期的な目標を達成するための具体的計画を策定
	部門横断調査を行い、社内での協力体制を確立し、将来像をステークホルダーで合意するためのプロセス		各事業部門の事情（システムの更改時期など）を考慮した無理のない組織横断的な工程の策定	

セキュリティ管理体制整備支援

セキュリティにかかる脅威およびリスク、それらに対するコントロールについて、公的ガイドラインを参考に既存の状況を評価し、不足している統制を整理します。その後、情報セキュリティ関連規程類や体制の整備・見直し、執行までを支援します。

■ テクノロジー領域にかかるゼロトラスト化セキュリティ実装支援

ゼロトラスト化ソリューションの実装に向けて、アーキテクチャ設計、ソリューション選定、実装、稼動にいたるまで、KPMGが包括的に支援します。

		エンドポイント	クラウド環境	OA環境
Strategy & Governance 戦略・ガバナンス		中期計画策定支援	クラウドトランスフォーメーション支援	リモートワーク最適化支援
		セキュリティ管理体制整備支援	セキュリティガイドライン整備支援	
Technical 技術的対策		多層防御最適化支援	セキュリティ運用・監視高度化・自動化支援	脅威ベースのペネトレーションテスト（TLPT）
		脆弱性診断（エンドポイント）	クラウドセキュリティソリューション評価支援	ID管理構想策定支援
		エンドポイント監視体制構築支援	クラウドアーキテクチャ設計支援	特権ID管理構想策定支援
		EDR導入支援	CASB導入支援	DLP導入支援

KPMGコンサルティング株式会社

T：03-3548-5111
E：kc@jp.kpmg.com

home.kpmg/jp/kc