情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

修士論文審査　2023年8月18日

リモートワーク環境における
ゼロトラスト導入ステップの検討および考察

大久保研究室
M2　岡本　優
2023/8/8(予行)

目次

1. 背景・研究目的

背景・研究目的

■背景

クラウドシフトによる従来の境界防御の考え方ではセキュリティ対応できなくなってきている。そこで注目され始めたのが「ゼロトラスト」の考え方である。
市場調査結果から国内企業において「ゼロトラスト」ソリューションの検討は行うが導入は進んでいない。

■研究目的

導入の進まない背景・課題の掘り下げ、最新のゼロトラストに関する技術・導入手法を調査・研究を進めることより、企業がリモートワーク環境におけるゼロトラスト導入を推進しやすくするための新たな導入ステップの検討・評価を行う。

2. ゼロトラストとは

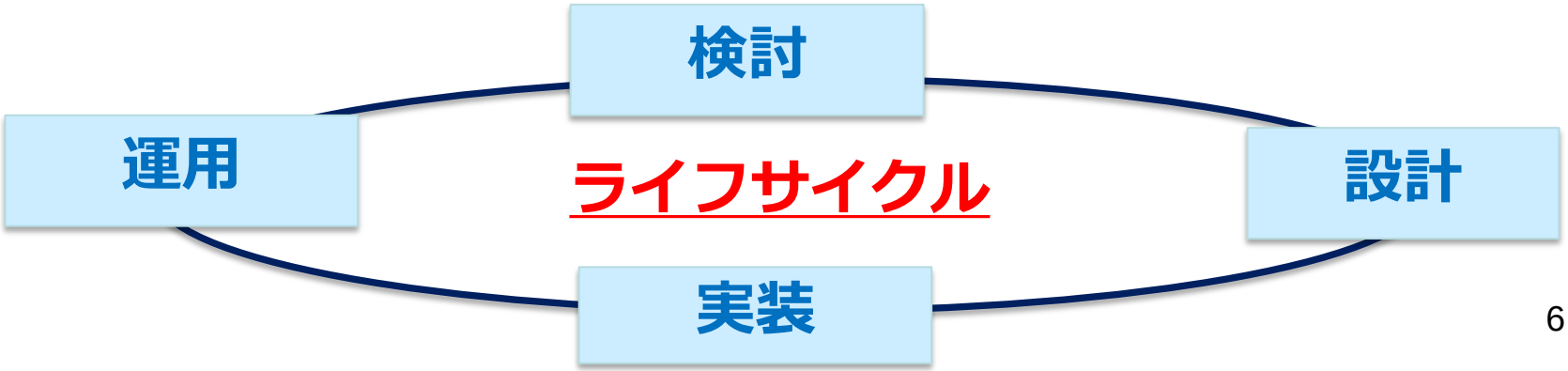
ゼロトラストとは

■ゼロトラストの定義

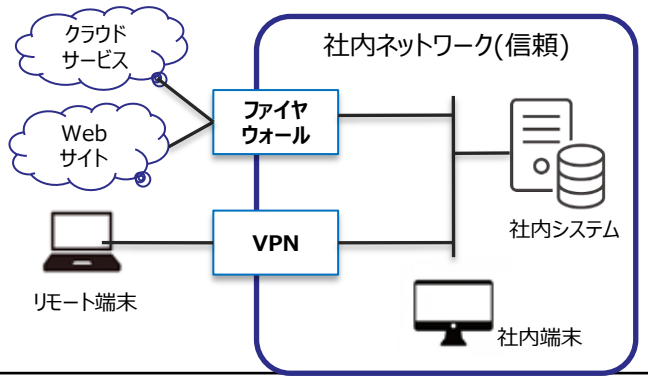
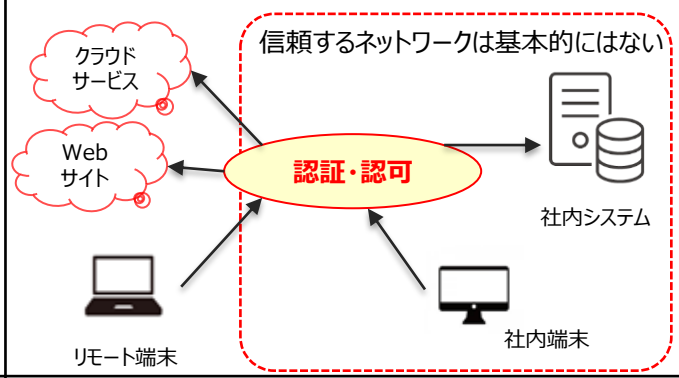
全ユーザやデバイス、接続先のロケーションを“信頼できない”という前提で、“信頼できない“ものが、重要な情報資産やシステムへのアクセスする際、要求に対して適切かつ最小限の権限を与え、その正当性や安全性を検証し、セキュリティの脅威を防ぐことを目的とした概念・考え方

■ゼロトラスト・アーキテクチャの定義

ゼロトラストの概念を利用したセキュリティ対策の考え方であり、ライフサイクル全体に適用されるものである



境界型モデルとゼロトラストモデルの違い

	境界型セキュリティ	ゼロトラスト
ネットワーク 構成イメージ		
信頼する ネットワーク	社内ネットワーク ※ファイヤウォールの内側	なし
情報資産の場所	信頼できるネットワーク内部	場所に依存しない
端末の 種類・場所	社内に設置した自社の端末 外部からはVPN等で接続	場所や端末に依存しない
セキュリティ対策 の考え方	境界での入口対策・出口対策に内部を加えた多層防御	社内リソースへのアクセスの信頼性を常に評価
侵害時の拡散の 懸念	内部の端末やITシステムへの拡散の懸念がある	認証認可を行うため拡散リスクは低い

出展：ゼロトラストの現状調査と事例分析に関する 調査報告書　2021/3/31 PwC あらた有限責任監査法人

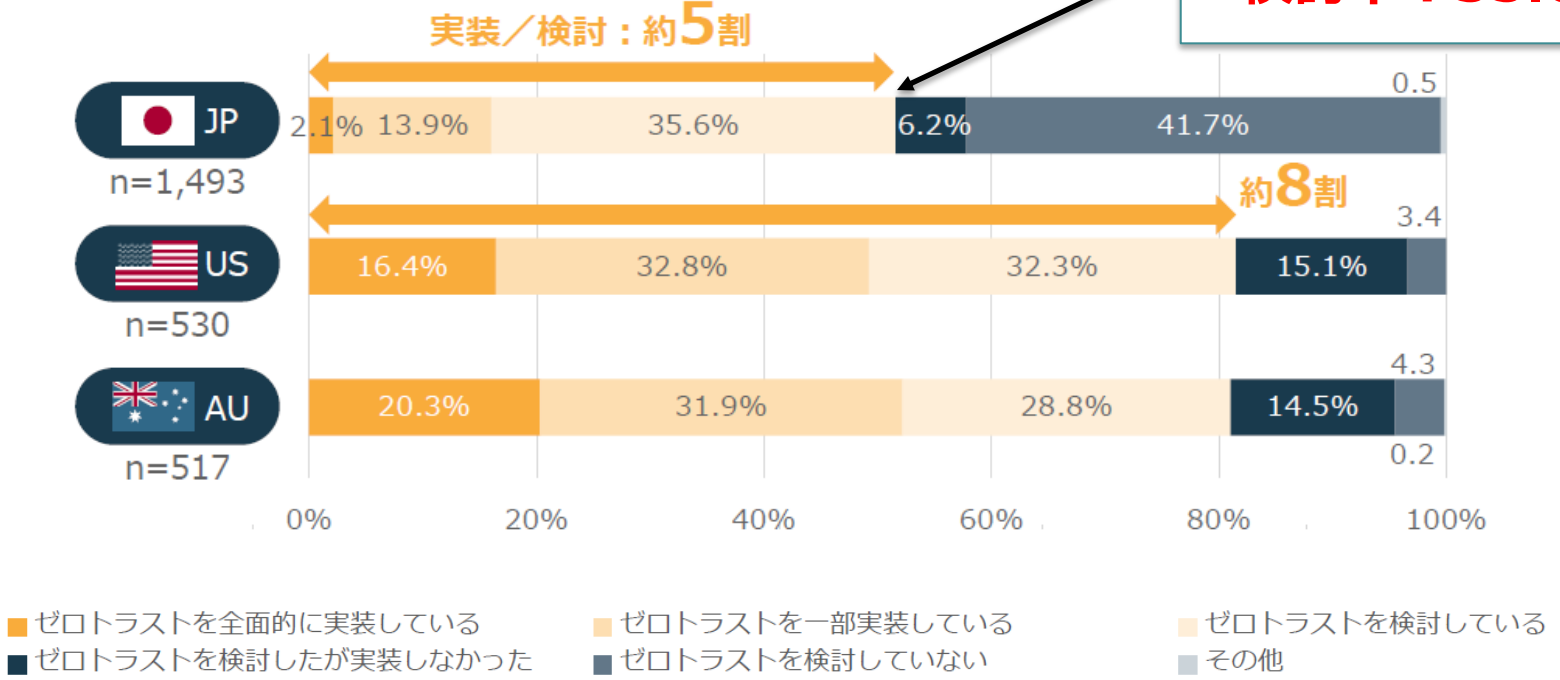
3. 関連研究

市場動向調査

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ ゼロトラストの導入状況（日本・アメリカ・オーストラリアの比較）

実装済：16.0%
検討中：35.6%



出典：NRISecure Insight 2022 企業における情報セキュリティ実態調査　NRIセキュアテクノロジーズ株式会社

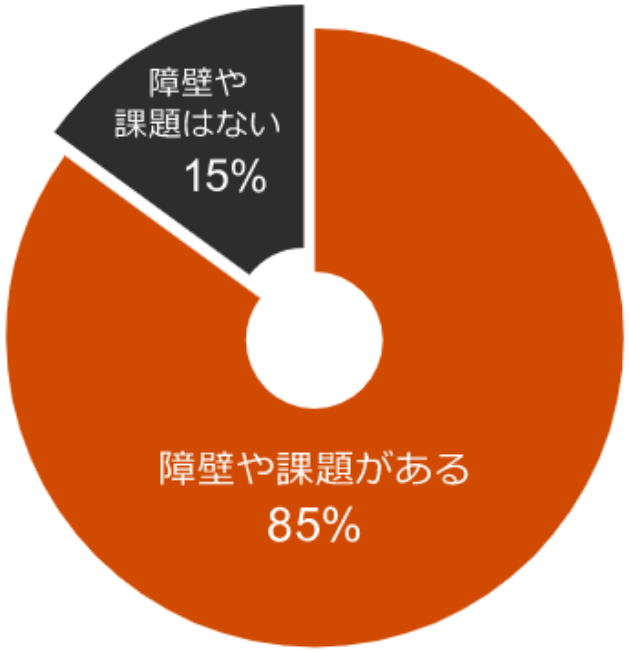
米・豪に比べて日本の実装／検討企業が少ないのは、既存の業務環境でも企業活動が継続できている上、その投資対効果が過少に見積もられており、必要性・緊急性が十分に理解されていないことが原因と推察される。

市場動向調査

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ゼロトラスト実装にあたっての障壁や課題

実装にあたる障壁や課題の経験有無
（単一回答 ｜n =338）



実装に取り組む際に障壁となった課題
（複数回答 ｜n =287）

課題	割合
実装にコスト(時間・人・予算)がかかりすぎる、不足している	**68.6%**
期待する効果が得られない（セキュリティリスク・生産性）	**36.2%**
現状把握（システム・ユーザニーズ）ができていない	**25.1%**
どこから取り組むべきか分からない	**20.2%**
経営層が協力的でない	**16.0%**
法規制遵守が難しくなる	**14.6%**
その他	**1.0%**

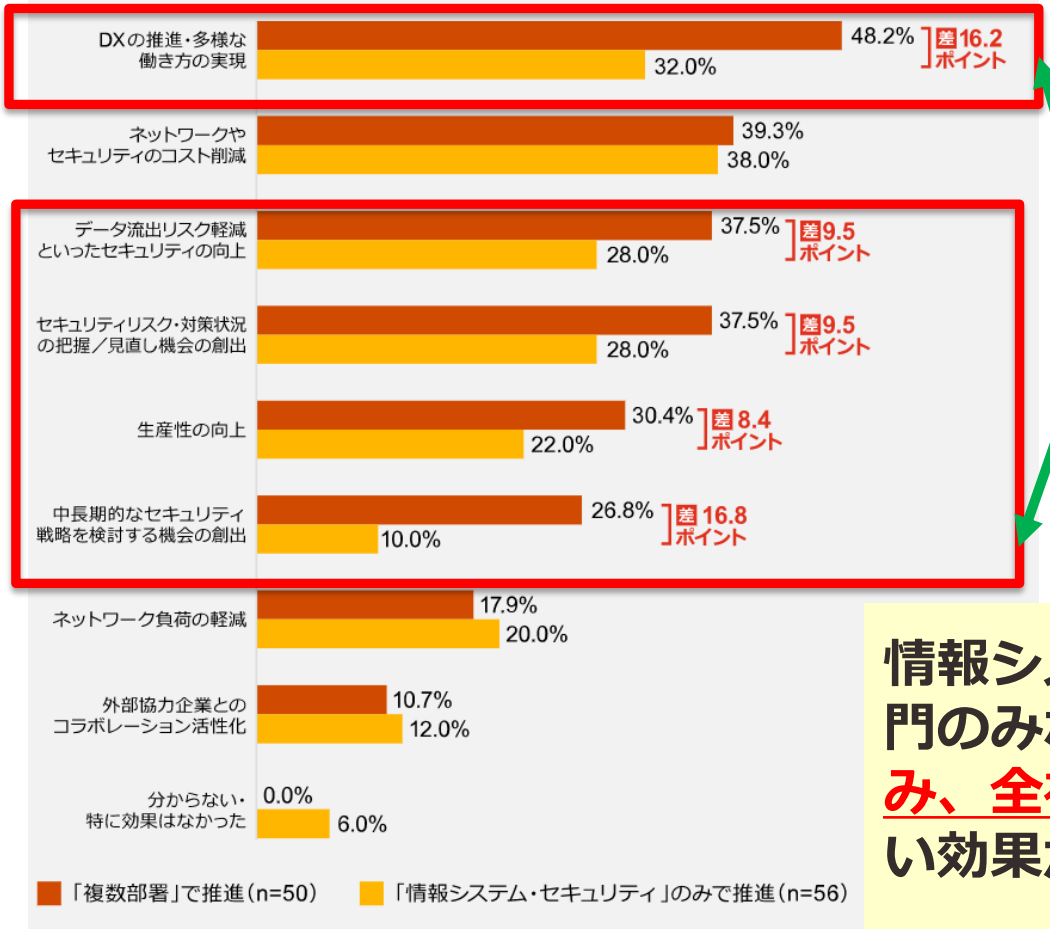
コストの課題に加え、導入効果の有無や現状を把握できていないことも導入の障壁となっている。また、経営層が協力的でないことも考えられる。

出典：国内企業における「ゼロトラスト・アーキテクチャ」の実態調査2021　PwCコンサルティング合同会社
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/zero-trust-architecture-survey2021.html

市場動向調査

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ ゼロトラスト実装済み企業における導入効果
⇒「部門横断的に推進する企業」の導入効果が高い



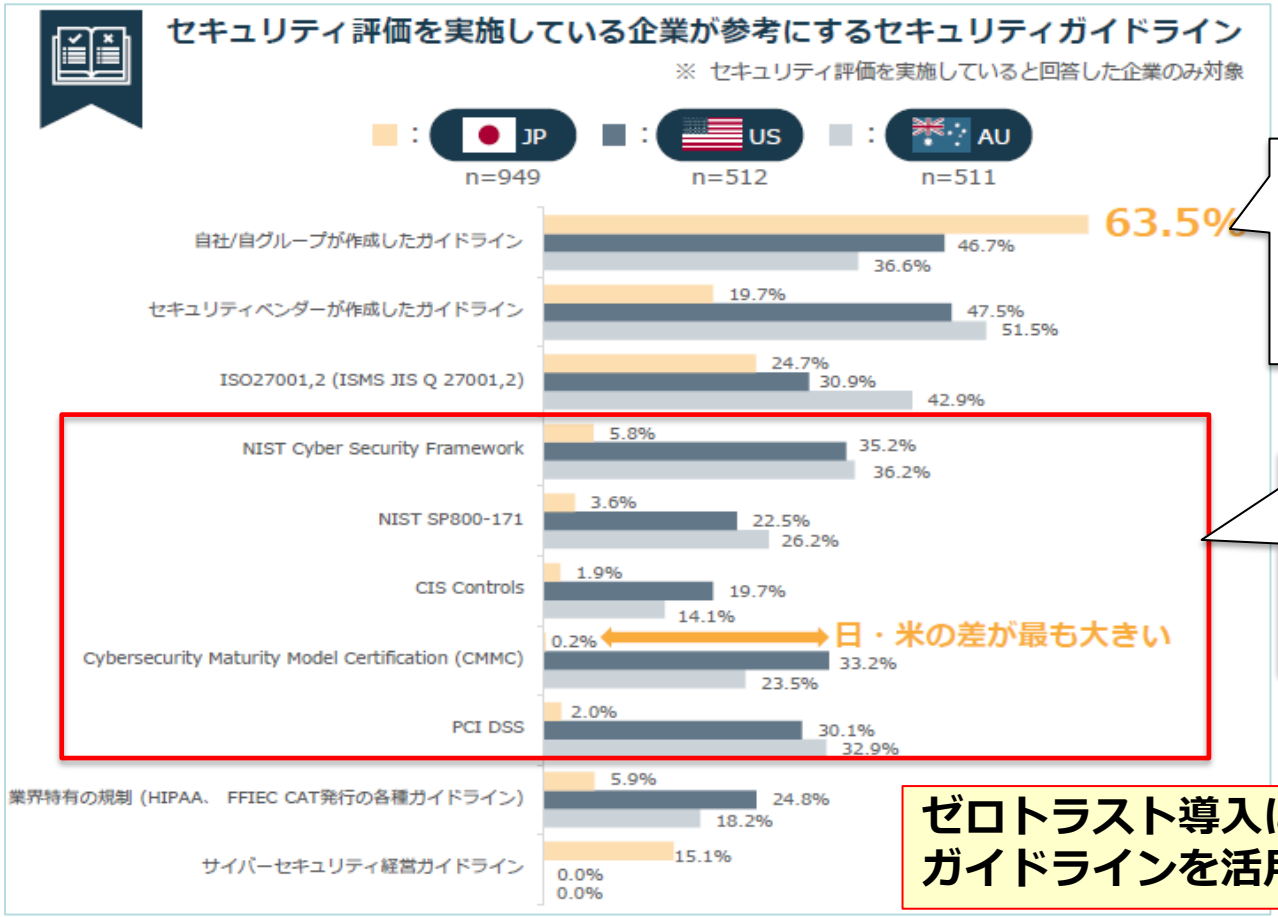
複数部門での推進体制でより多くの効果を得られた

情報システム部門やセキュリティ部門のみならず、経営層なども巻き込み、全社的に施策を推進により、高い効果が得られる

出典：国内企業における「ゼロトラスト・アーキテクチャ」の実態調査2021　PwCコンサルティング合同会社
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/zero-trust-architecture-survey2021.html

市場動向調査

■ セキュリティ評価を実施している企業が参考にするセキュリティガイドライン



日本では自組織作成ガイドラインの活用による自社の実態に即した評価

導入の進む海外では既存のガイドライン・フレームワークを活用

ゼロトラスト導入において、ガイドラインを活用することも視野に入れる

出典：NRISecure Insight 2022 企業における情報セキュリティ実態調査　NRIセキュアテクノロジーズ株式会社

市場動向調査（まとめ）

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ゼロトラスト導入における課題

- 各企業は検討含めた導入は5割程度
- 障壁・課題
  「コスト面への不安」「見えない導入効果」「経営層の協力が必要」
- ゼロトラスト推進に向けてステークホルダーとの合意形成の必要性
- 目的と効果を照らし合わせたゼロトラスト推進の必要性
- 自社独自のセキュリティガイドライン利用による事業環境の変化や脅威への対応に伴う対応負荷

■ゼロトラスト導入の課題に対する対策案

- **導入に関わるプロセスの見直し・整備**
- 各ステークホルダーとの合意形成を得やすくする仕組み
- 既存の公的機関のガイドライン活用による評価の効率化・標準化
- 各企業のビジネスとゼロトラスト導入による効果の見える化

「実装コストがかかること」・「どこから取り組むべきかわからない」

既存の導入ステップ見直し・検討必要

4. ゼロトラスト導入ステップの検討

各文献調査および検討

- ゼロトラスト導入ステップについて
  既存文献を調査・比較・分析を実施

- 課題への対策および企業のステークホルダーの
  目線を考慮した、導入ステップおよびライフサ
  イクルの検討

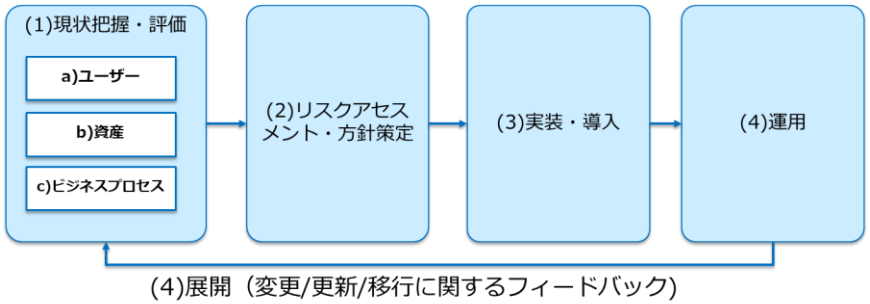
【各文献】

1．NIST SP 800-207
2．ゼロトラストアーキテクチャ適用方針(デジタル庁)
3．ゼロトラスト移行のすゝめ(IPA)
4．ゼロトラストネットワーク実践入門(NRIセキュアテクノロジー社)

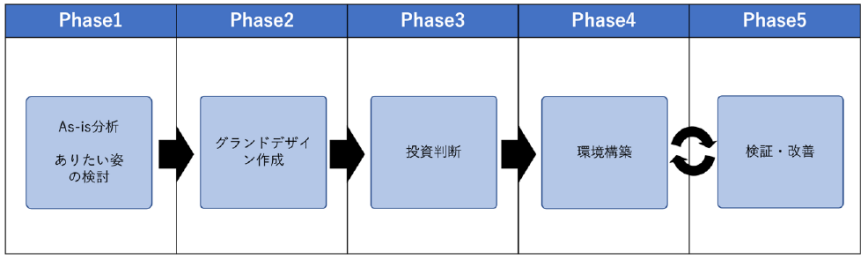
導入ステップの比較・検討

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

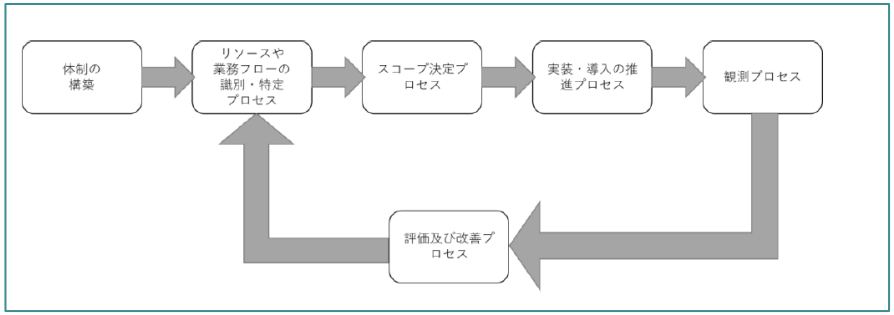
文献1



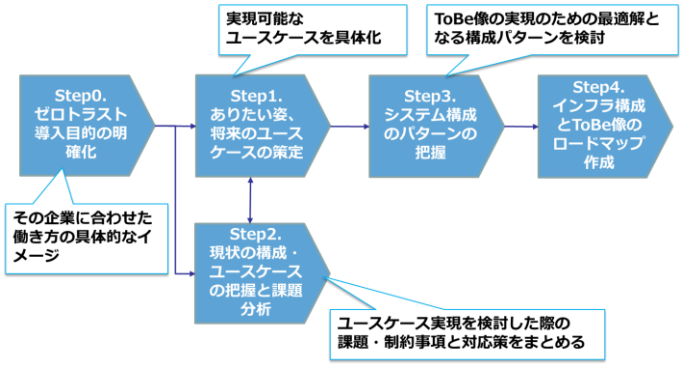
文献3.



文献2.



文献4.



- ステップなど統一性がなく、実施項目の抽出が必要
- 運用段階で見直し・改善・変更を実施している

導入ステップの比較・検討

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 各文献からの分析・フェーズ分け

文献	導入検討	設計	実装	運用・改善
1.	• 現状把握・評価 • リスクアセスメント	• 方針策定 • リスクアセスメント	• 実装・導入 • リスクアセスメント	• 運用・展開 • リスクアセスメント
2.	• 体制の構築 • リソースや業務フローの特定・識別	• スコープ決定プロセス	• 実装・導入の推進プロセス	• 観測のプロセス • 評価・改善のプロセス
3.	• As Is分析 • ありたい姿の検討	• グランドデザイン作成 • 投資判断	• 環境構築	• 検証・改善
4.	• 目的の明確化 • ありたい姿、将来のユースケースの策定 • 現状の構成、ユースケースの把握と課題分析	• システム構成パターンの把握 • インフラ構成のToBe像(あるべき姿)とロードマップ作製	• ー	• ー

実施項目をフェーズごとに振り分け、位置づけを明確化
各ステークホルダーが認知・理解できるようにする

新導入ステップ策定

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

ゼロトラスト導入ステップ

①導入検討フェーズ

1．ゼロトラスト化の体制構築
2．目的の明確化
3．既存IT環境・業務フローのAs-Is分析・ありたい姿の検討
4．導入実施案検討

②設計フェーズ

1．具体的な実装検討
2．ソリューション選定・To-Be像の策定
3．実装・運用時の実コスト検討・承認

③実装フェーズ

1．ソリューション実装・導入
2．既存・ゼロトラストの混在による段階的導入
3．定常的な運用・改善検討の体制確立

④運用・改善フェーズ

1．導入後の運用・監視
2．各ステークホルダーによる改善検討

改善、運用状況によりソリューションの追加導入・変更する場合は「導入検討」フェーズで検討し実施する

ステークホルダ

各フェーズへの積極的関与
ステークホルダー同士のコミュニケーション

セキュリティ リスクマネジメント

フレームワークに基づいた標準的なセキュリティマネジメントを実施

策定のポイント

- ステークホルダーや企業へシステムを提供する立場などが、システムのライフサイクルの形式を踏襲し**フェーズごとの実施項目を明記**することで、検討の煩雑さを緩和する
- **ステークホルダー間で積極的なコミュニケーション**を取りながら導入を促進させ、かつ経営層の理解を得やすくする
- **共通的なフレームワークの活用および継続的なセキュリティリスクマネジメント**を実施することにより、セキュリティリスクを低減させ、セキュアなリモートワーク環境を確保することが可能となる
- **企業のあるべき姿を目指す**ためにステップを参考にし、**組織横断的な体制を構築**することで導入のスピードを高めることが可能となる.

導入検討フェーズ

■ 求められる要件

ゼロトラストの導入おける具体的な目的および導入における
企業のありたい姿へ近づけるためステークホルダー間で検討

・導入の目的および企業のありたい姿が明確化
・各ステークホルダーにより認知・共有
・後続フェーズを効率よく進めゼロトラスト化推進の方向性を示す

■ 実施内容

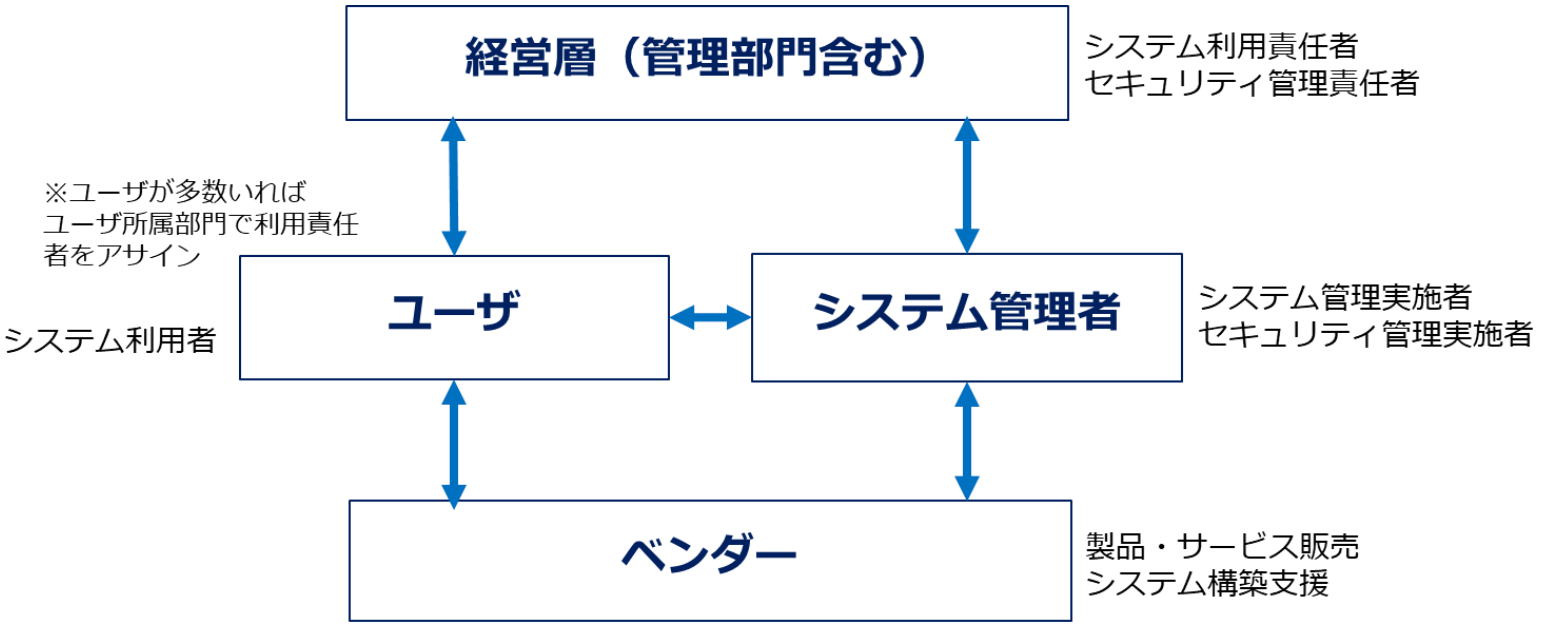
・ゼロトラスト化の体制構築
・目的の明確化
・既存IT環境・業務フローのAs-Is分析・ありたい姿の検討
・導入実施案検討

導入検討フェーズ

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■導入体制構築

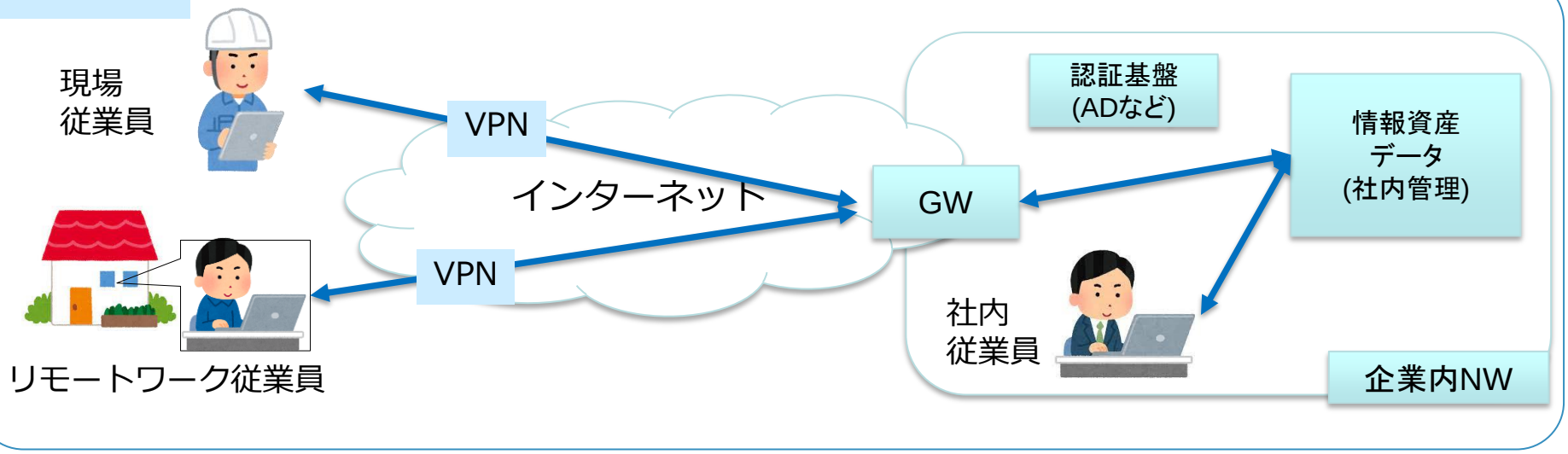
最初にステークホルダーをアサインし,各フェーズでのステークホルダーの役割分担・責任範囲を明確にする.



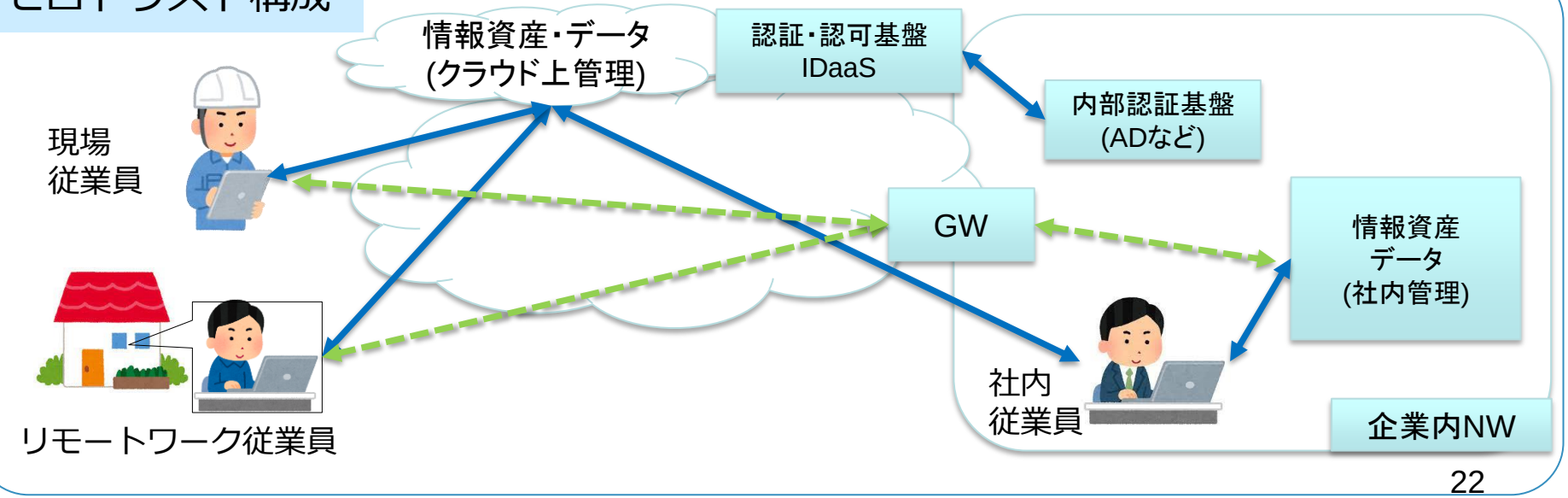
経営層の理解, 組織横断での検討および継続的な議論を
各フェーズで行える環境にする
⇒ゼロトラストへの移行による効果が高まる

導入検討フェーズ（ありたい姿）

既存構成



ゼロトラスト構成



導入検討フェーズ

As-Is 分析

- ユーザ・資産・組織の抱えている課題を可視化
- セキュリティの課題および懸念の洗い出し

リモートワーク環境におけるありたい姿を経営層へ十分に理解してもらい組織に対してゼロトラストの適用につなげる

項目	具体的例	現状の管理・運用	課題
システム	ID管理方法	社内の従業員・協働者DB 管理部門にて登録・変更・削除申請	協働者の契約満了後の削除漏れなどが発生する
	認証認可システム	ADサーバを利用	従業員DBと連携している
	利用アプリケーション	Webアプリ・会社固有のアプリを使用	会社固有のアプリは持ち出し端末にインストールできず使用できない
	端末上のセキュリティ	ウィルス対策ソフト	持ち出し端末を定期的にセキュリティパッチの適用が施されていない
	システム構成	社内ネットワークからのみインターネットアクセスやクラウドサービスへの接続が可能	VPNへの接続が集中したときにボトルネックになり業務効率が落ちる可能性がある。
ユーザビリティ	アクセス方法	VPNソフトを起動し社内VPNゲートウェイへ接続し、社内ネットワークへ接続	インターネットアクセスもVPN経由でありボトルネックとなっている
	端末利用時	持ち出し端末は共通のパスワードが設定されている	紛失時の第三者利用
	アプリケーション利用時の認証方法	社内システムのアプリには、従事者DBに登録されたユーザ名・パスワードを利用	定期的なパスワード更新があり接続できない場合にサポートデスクに問い合わせるなどの対応が必要
運用	リモートワーク時に持ち出す端末	社外で使用するために持ち出す際には部門の管理者の許可を得る	貸し出し管理・返却管理が必要
	社内端末	従業員は帰宅時に各自のロッカーに保管	持ち出し端末と社内端末は分けられていて従業員の利便性を欠く場合がある

導入検討フェーズ

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

フレームワークの活用によるリスク分析

NIST Cyber Security Framework(NIST CSF) 1.1の活用
カテゴリに対応する機能やソリューションを検討

機能	カテゴリー	サブカテゴリー	対応する製品名(※)	製品説明
識別(ID)	**資産管理 (ID.AM)** 自組織が事業目的を達成することを可能にするデータ、人員、デバイス、システム、施設が、識別され、組織の目的と自組織のリスク戦略における相対的な重要性に応じて管理されている	**ID.AM-1**：自組織内の物理デバイスとシステムが、目録作成されている	製品A-1 (資産管理ツール)	システムからハードウェアおよびソフトウェアの仕様の一覧を入手し、OS のバージョン、ハードウェアの詳細、IP アドレス、 ハードウェアのドメインなどの目録を作成. この情報を報告し、システムアセットの監査に活用できるようにする
		ID.AM-2：自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている	製品A-2 (CASB)	ファイアウォールやプロキシサーバーなどの企業セキュリ ティデバイスと統合し、シャドー IT を検知
			製品A-3 (資産管理ツール)	デスクトップ、サーバー、アプリケーションなど、従業員が使用する資産の詳細アクティビティログを提供。こういった情報は ID 管理や資産管理システムのレポートや補足情報から収集可能。さらに PDF レポートが提供されるため、自社事業に特有のリスクや該当するリスクの特定や対処に活用可能

引用：proofpoint NIST サイバーセキュリティガイドラインへの準拠　(※一部抜粋, 製品名は省略)

出典：重要インフラのサイバーセキュリティを改善するためのフレームワーク
https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000071204.pdf

導入検討フェーズ

導入実施案策定・スコープ決定

導入に向けたスコープ決定
As-Is分析・リスク分析より具体的な導入実施案を策定する

As-Is 分析　　**リスク分析**

実施項目	詳細
概算コスト算出・承認	導入時の人稼働、システム変更構築費用、運用稼働あるべき姿と経営方針と照らし合わせ、段階的導入の検討も実施
導入優先度の選択	利用者のニーズ、コスト、リスクなどをもとにソリューション導入優先度を検討
導入スケジュール・ロードマップの策定	いつまでにゼロトラスト化（一部・全部）するか示す
スコープ・タスク一覧を策定	各ステークホルダごとの実施スコープ タスク一覧を作成・共有する
環境・情勢変化・課題に対する対応案を策定	（例）企業の経営状況・方針が変わり、ゼロトラスト化のさらなる推進

設計フェーズ

■ 求められる要件

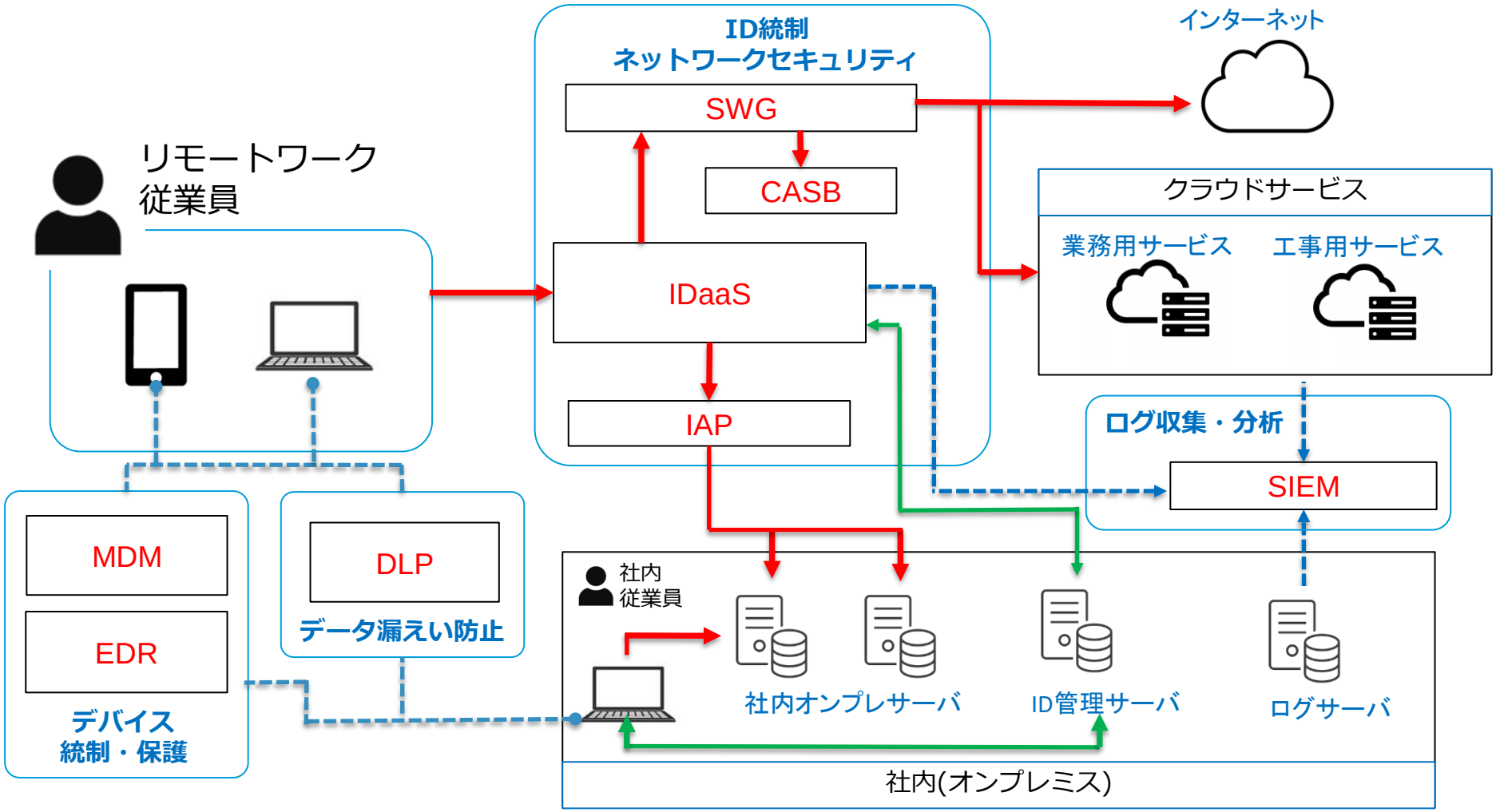
ゼロトラストの製品・サービスを組み合わせた実装、および運用に関わるコスト、運用体制などの検討を実施する.
ゼロトラスト導入による具体的なコスト・リスク分析・導入効果などをもとに総合的に導入決定を判断する

■ 実施項目

- 具体的な実装検討
- ソリューション選定・To-Be像の策定
- 実装・運用時の実コスト検討・承認

設計フェーズ

ソリューション選定・To-Be像の策定



実装フェーズ

■ 求められる要件

設計フェーズで決定したソリューション実装導入を行うことにより、各ステークホルダーがゼロトラスト化された状況を認知し、 利用・管理することにより動的に関与させ、以降のフェーズで継続的に運用・改善を繰り返し行える状態にする

■ 実施項目

・ソリューション実装・導入
・既存・ゼロトラストの混在による段階的導入
・定常的な運用・改善検討の体制確立

実装フェーズ

ゼロトラストの段階的導入

ありたい姿から、あるべき姿への実現可能にするため
段階的導入を進める前提

■段階的導入を進める為に実施する事

・次の段階（新たなソリューション導入など）への基準を設定
・運用・改善フェーズでモニタリング実施

■モニタリング実施項目（例）

・ゼロトラスト・アーキテクチャに関連する問い合わせ件数
・業務上必要な認証・認可の拒否件数
・開発・運用部門の負荷、ユーザの声などのフィードバック
・運用コスト

参考文献：ゼロトラストの現状調査と事例分析に関する調査報告書　**PwC**あらた有限責任監査法人 2021

運用・改善フェーズ

■ 求められる要件

導入実装されたゼロトラストのシステムに対して,各ステークホルダーが能動的にかつ継続的に運用および改善の検討を実施する

■ 実施項目

- 定常的な運用および各ステークホルダーによる改善検討
  ⇒システムがセキュアな状態で継続的に利用される状態
- 現場利用状況のモニタリング
  管理者が能動的に現場で業務を行う利用者へ
  システム利用状況や利用における改善点, 利便性向上に
  対する意見・提案を集約する機会を設ける取り組み
- 社内からの要望や改善に対して実装済みのシステムの
  構成変更がある場合は新たな施策として導入検討フェーズ
  にて再検討を開始

5. 検討における評価・考察

検討結果

■ 関連研究

1．市場動向調査
　導入が進まない課題への対策案を検討
2．導入ステップの比較検討
　各文献の共通項目の抽出による新たな導入ステップ策定

■ 新たな導入ステップの策定

・対策案の盛り込み、各文献の共通事項を抽出、用語の定義
・導入ステップのフェーズ分けおよび実施事項の明記
・ステークホルダーの関与およびフレームワーク活用を明記
・段階的導入を前提とした運用時のモニタリングの必要性
・能動的な改善検討によるセキュアな環境の維持
　および新たなソリューション導入の継続的な検討

考察

- 各フェーズで期待される効果
  ⇒継続的なライフサイクルの運用
  　セキュアな環境を確保

- ステークホルダー同士の共通認識・合意形成
  ⇒新たな導入ステップを活用による導入が促進

- 各企業が簡素化された導入ステップでの検討可能

6. まとめ・今後の課題

まとめ・今後の課題

- ゼロトラストの導入が進まない背景や課題を掘り下げ、導入を促進するための対策を検討

- 様々な文献における導入ステップの比較・検討を実施
  共通要素の抽出やフレームワーク活用
  ⇒新たなゼロトラスト導入ステップを提示

- ゼロトラスト導入に関わるステークホルダーの目線、ソリューションを提供するベンダー目線を合わせた導入ステップへ改善

- 今後は各業種ごとに業務分析、課題分析を行い、それぞれの導入ステップを検討実施