資料１

技術検討会議

2022年3月15日（火）

デジタル庁

ゼロトラスト・アーキテクチャ適用方針について

1. 技術検討会でのご意見を踏まえたガイドライン対応方針
2. ゼロトラスト・アーキテクチャ適用方針（素案）ドラフトについて
3. ご意見いただきたい論点

ゼロトラスト適用原則（素案）について

ゼロトラストアーキテクチャ適用方針のガイドラインを策定するにあたり、
諸外国のフレームワークから導出された適用原則を主軸とした構成を予定している

ゼロトラスト目次案

本ガイドラインは概念と考え方を中心とした記載とし、適用に係る具体的な方針については別添、または留意事項として補記する程度を予定

ゼロトラストを適用するための基本的な原則を大項目として構成する（詳細は次ページ以降に記載）

4

ゼロトラスト適用原則（素案）について

ゼロトラスト・アーキテクチャ適用方針のガイドラインを策定するにあたり、
諸外国のフレームワークから導出された適用原則を主軸とした構成を予定している

ゼロトラスト目次案

ゼロトラスト・アーキテクチャを適用するための大前提となる綱領(心構え)を記載

ゼロトラスト・アーキテクチャを適用するための基本的な原則を記載

5

１．技術検討会でのご意見を踏まえたガイドライン対応方針
有識者の皆様からのご意見に関する対応方針をまとめました

No	章立て	ご意見	対応方針
1	はじめに	ゼロトラストの**メリット**を前面に出すだけではなく、**デメリット**の記載も必要	導入負荷、運用負荷、エンティティの複雑性の増大等を主にデメリットとして記載予定
2	はじめに	インターネット接続を前提としないシステムや境界型防御で成り立っているシステム、安定稼働を求められる重要インフラシステム等、ゼロトラストの**適用範囲**を明確にする必要がある	対象外システムを明記する予定はないものの、重要インフラ等はタイムラインを意識して適切に対応するような記載を予定
3	原則5	モニタリングが重要となるものの、運用を外注できる組織ばかりではないため、**運用負荷増**を考慮する必要がある	モニタリングに係る運用負荷については原則の中に記載予定 ※政府全体での運用負荷軽減に寄与するアーキテクチャ、仕掛けの検討も別途必要な認識
4	はじめに	ゼロトラストは一足飛びでたどり着くものではなく、予めスコープ外とされるようなシステムもあり、**当面はTrustedな環境やシステムが残る**	ゼロトラストという方向性を見定めつつ、既存の環境やシステムを改善していかなければならない事を踏まえ、目指すべき考え方、目的などを記載する
5	はじめに	「ゼロトラストを導入するには何を買えばいいのか」という質問がでるくらいにユーザ側には**イメージがつかめていない**現状がある。事例等を含め、導入プロセス等を手厚く記する事が望まれる	ゼロトラストは概念、考え方であり、目的（例えばリモートワーク等）を達成するための目標・手段である事を記載する

１．技術検討会でのご意見を踏まえたガイドライン対応方針
有識者の皆様からのご意見に関する対応方針をまとめました

No	章立て	ご意見	対応方針
6	はじめに	**運用ができない**組織が多い事が課題である	ゼロトラストに資するソリューションは導入して完了ではなく、モニタリングを含む運用が肝心であり、インソース・アウトソースを含めた運用方針も念頭に置く必要があることを記載する
7	参考	Amazon、Microsoft、Google、Ciscoなどを中心に「OpenID Continuous Access Evaluation Profile 1.0」「OpenID Shared Signals and Events Framework Specification 1.0」等ゼロトラストに役立つ内容を推進している。参考にしてもらえればと思う。	常時診断に活用する仕様・事例として、コラムへの記載を検討する（Microsoftやgoogleなど）
8	はじめに	NIST SP800-207をまとめた時の冒頭にはガバナンスの欠如に対するチャレンジというのがあり、**ゼロトラストで情報を保護ができるわけではない**ため、目的を明確にしてから対象範囲を明確にしていく必要がある	ゼロトラストの導入が目的とならないように目的や範囲を明確にする事を記載する
9	はじめに 具体方針	**境界防御vs ゼロトラスト**という構図も今後変わってくる可能性があるので、強調しなくてもいいのではないか	従来の境界型セキュリティ、境界型セキュリティとゼロトラストのハイブリッド、全面的なゼロトラスト化などのパターンの例示を予定。加えて境界型セキュリティを継続する場合のリスクを計り、報告する事等、共存を示唆する記載を検討する
10	はじめに 原則7 具体方針	7章の記載では、ゼロトラストはキーワードだけになる場合が多いので、**何をチェックすべきなのか**というが具体的な内容があるといい。	ゼロトラストは概念、考え方であり、目的（例えばリモートワーク等）を達成するための目標・手段である事を記載する。また、ユースケース等を踏まえて具体化を予定

１．技術検討会でのご意見を踏まえたガイドライン対応方針
有識者の皆様からのご意見に関する対応方針をまとめました

No	章立て	ご意見	対応方針
11	はじめに	実装が難しい。構築して満足してしまう組織も多く存在する。**構築してからがゼロトラストの始まり**である。そういったポイントも明記しておくとよい	ゼロトラストに資するソリューションは導入して完了、終わりではなく、モニタリングを含む運用が肝心であり、インソース・アウトソースを含めた運用方針も念頭に置く必要があることを記載
12	原則3 原則4	米国の民間企業の事例ではゼロトラスト環境を構築した後、実際にゼロトラストでアクセスした後、6時間等そのまま継続してアクセスをしている間にマルウェアに感染するといったケースがあるため、**常時アセスメントの必要**がある	常時診断の必要性を示すコラムとしての記載を検討
13	はじめに 原則7 具体方針	**ゼロトラストと境界型の混在環境が現在のスタンダード**である。最近はゼロトラストというよりも、コロナによるリモートワークのセキュアのためにゼロトラストが必要という意識になっている。混在環境と移行に関する示唆があるとユーザ側としてはヒントになるのではないか	従来の境界型セキュリティ、境界型セキュリティとゼロトラストのハイブリッド、全面的なゼロトラスト化などのパターンの例示を予定
14	原則7	ネットワークを使ったゼロトラストについて、NIST SP800-207の3.1章にネットワークマイクロセグメンテーションやSDN、IBNといったと**ネットワークを使ったコントロール**も含まれるので、これらの内容もガイドラインにて触れてもらいたい	ゼロトラストを適用するためのソリューション例としてどこまでを記載するかを検討
15	全体	**ユーザの利便性についても負荷が上がる。**ユーザ側ではどういう取り組みになるのか、どういう取り組みをすれば軽減できるのかについても触れるとよい	多要素認証やデバイスのセキュリティ維持等、今までよりひと手間かかるといった内容での記載を検討

１．技術検討会でのご意見を踏まえたガイドライン対応方針
有識者の皆様からのご意見に関する対応方針をまとめました

No	章立て	ご意見	対応方針
16	原則7	ゼロトラストの背景について、**ソリューションの議論**がある前提	ゼロトラストを実現する為の具体的なソリューションについてユースケース等を踏まえて記載を予定
17	原則7	適用原則はきれいごとになりやすい。**ソリューションやコストなどの具体的な例**が必要	ゼロトラストを実現する為の具体的なソリューションについてユースケース等を踏まえて記載を予定
18	原則1	アセット管理は現状でもしっかりと出来ていないところが多く、**どうやって管理を徹底していくのか**というところが困難であり、覚悟が必要だと思う。	ゼロトラストを実現する為には必要不可欠かつ重要な要素のため、何故アセット管理が必要なのかという根本的な部分からの記載を予定
19	原則2	アイデンティティ管理は重要と考えるが、**JOB型雇用**になっていない環境でアイデンティティの管理をどうやるのか、**セキュリティクリアランス**ができている環境が整う必要もあると考える	既存のID管理を刷新するだけではなく、ゼロトラストに適用するために可能な範囲で拡張していくといった記載を予定
20	原則2	JNSAのIDワーキンググループがある。具体的な検討をしているチームの為、話をきくのもよいと考える	ヒアリングも検討したい

１．技術検討会でのご意見を踏まえたガイドライン対応方針
有識者の皆様からのご意見に関する対応方針をまとめました

No	章立て	ご意見	対応方針
21	全体	**具体的な成功例**を持ち込む事で具体的なイメージを持たせることができると思う	主な成功事例としてGoogleなどがあるものの、国内、特に政府に適した事例があれば記載を検討したい
22	原則3 原則4	サイバーリスクを発見できる前提となっているが、常時権限を確認する、認証と認可をデバイスや認証に対して実施するなどで**潜在化したリスクを見つける観点**での言及も必要	ゼロトラストの要でもあり、準拠すべきポリシー、資産の状態確認で記載を予定
23	はじめに	ゼロトラスト適用に伴い、既存業務への影響が大きくなり、意識改革や取り組むための**覚悟が必要**	ゼロトラストを適用する事によって発生するメリット・デメリットで記載を予定
24	原則1	アセット、ネットワークアカウント、ワークフロー、データ等の**守るべき対象**はサイバーセキュリティ戦略で明確に定められている	齟齬のないように記載に留意する ＊利用者、デバイス、サービス、データ
25	原則3 原則4 原則5	監視強化では入口出口だけではなく、**オペレーショナルフローのような一連の流れ、サービス**も含めて監視、保護すべき。CPT2.0などが参考になる。	準拠すべきポリシー、資産の状態確認、監視強化などの項目で記載方法を検討する

１．技術検討会でのご意見を踏まえたガイドライン対応方針
有識者の皆様からのご意見に関する対応方針をまとめました

No	章立て	ご意見	対応方針
26	原則4	役割ベースから属性ベースにシフトする前に、何故シフトする必要があるのか、多要素認証等の追加認証が何故必要なのかなどのゼロトラストの概要を**丁寧に説明する**必要がある	Shoudだけでなく、Whyを記載する事で原則の持つ意味を分かりやすく記載する
27	原則3 原則4	リスクベースという観点ではIoCベースの**脅威インテリジェンスは必要な観点**であり、インテリジェンスのポリシーエンジンが重要となる。また民間の事例も合わせて紹介するのがよい	脅威インテリジェンスについても原則の中で記載する
28	原則5	モニタリングは米国のeDiscoveryに基づき、**各アクティビティに対して時間軸での保存と迅速な閲覧**が可能な事としている	各アクティビティに対するモニタリングの基準として記載を検討する
29	全体	**成熟度が重要**となる。SP800-171やRisk Management Frameworkなどをみても、ガイドラインは理想論であり、チャレンジングな内容となる。例えばAPIの暗号化など、証明書の管理等が発生する事を踏まえると事実上困難であり、**相当な覚悟**を持って取り組む必要がある	関連するフレームワーク等を踏まえた記載を検討するとともに、理想論と実現性も踏まえた形で記載方法を検討する

１．技術検討会でのご意見を踏まえたガイドライン対応方針
ゼロトラスト適用における心構えと覚悟を綱領として記載する

No	綱領	概要	詳細
1	**ZTAは中長期的な改善を要する**	**複数サービスの組み合わせで成り立つ**	・多数のソリューションやサービスの組合せにより成り立つ ・中長期にわたる計画の策定が求められる
		セキュリティクリアランスの確保が求められる	・機密情報の利用範囲が広がる ・ユーザによる機密情報のセキュリティに関する高い意識が求められる
2	**時間経過による適時見直しを要する**	**ZTA適用できるか判断が必要**	・対象となる全てのシステムで適用を検討する ・ゼロトラストがすべてではなく、境界型セキュリティとの共存もある ・境界型の残存箇所についても、将来的なZTA化の検討を行う
		組織ごとにZTAの形がある	・目的に応じたZTAを検討する ・ZTAのあるべき姿は組織の置かれた環境や状況、立場によって異なる
3	**運用・保守の強化を要する**	**常時モニタリングの重要が重要**	・関連するサービス・ソリューションの導入ではZTAは完成しない ・常時モニタリングすることで、有事において可及的速やかな対応が可能となり、それがZTAの本質である
		ゼロトラストは運用が重要	・ZTA適用後は運用の負荷が上がることが懸念される ・専門性の高いスキルの習得や体制の拡充をするなど、運用負荷の増大をあらかじめ予測し対処する必要がある

1. 技術検討会でのご意見を踏まえたガイドライン対応方針
2. **ゼロトラスト・アーキテクチャ適用方針（素案）ドラフトについて**
3. ご意見いただきたい論点

別紙

資料２ ゼロトラスト・アーキテクチャ 適用方針（案）

1. 技術検討会でのご意見を踏まえたガイドライン対応方針
2. ゼロトラストアーキテクチャ適用方針のガイドライン（素案）ドラフトについて
3. **ご意見いただきたい論点**

３．ご意見頂きたい論点

- **ゼロトラスト・アーキテクチャ適用方針（素案）について**

  諸外国のフレームワークの活用、網羅性、政府・府省への適切性、盛り込むべき要素等