参考資料2

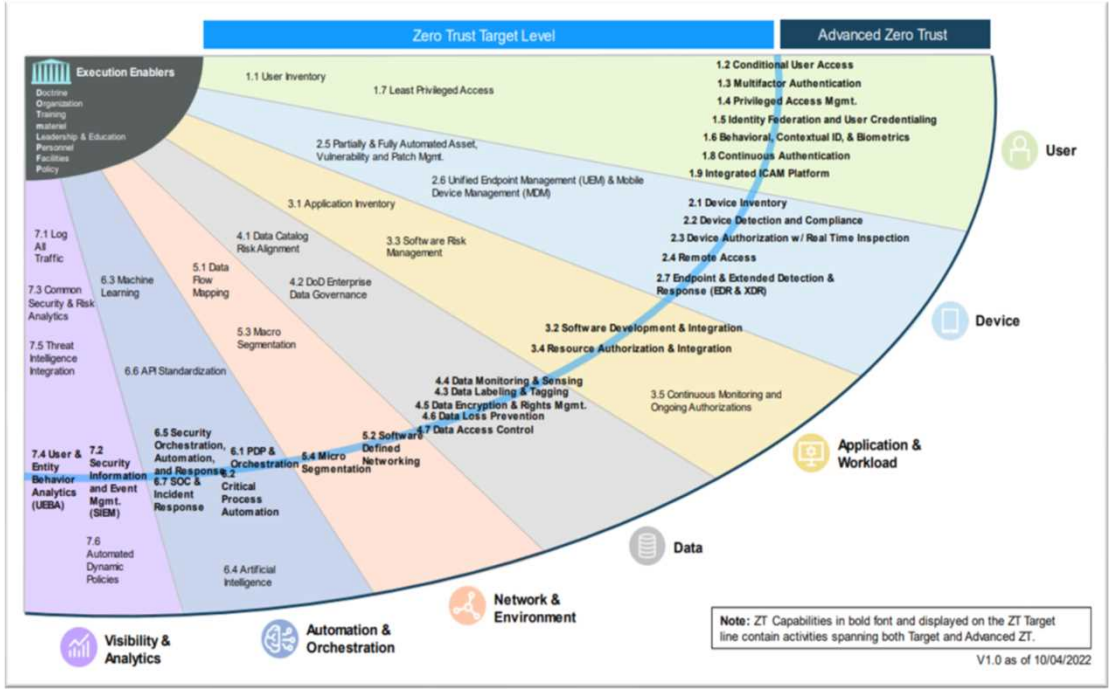
（参考資料２）海外の中央政府におけるゼロトラスト取組事例

（参考）ゼロトラストの進行状況　アメリカ国防総省

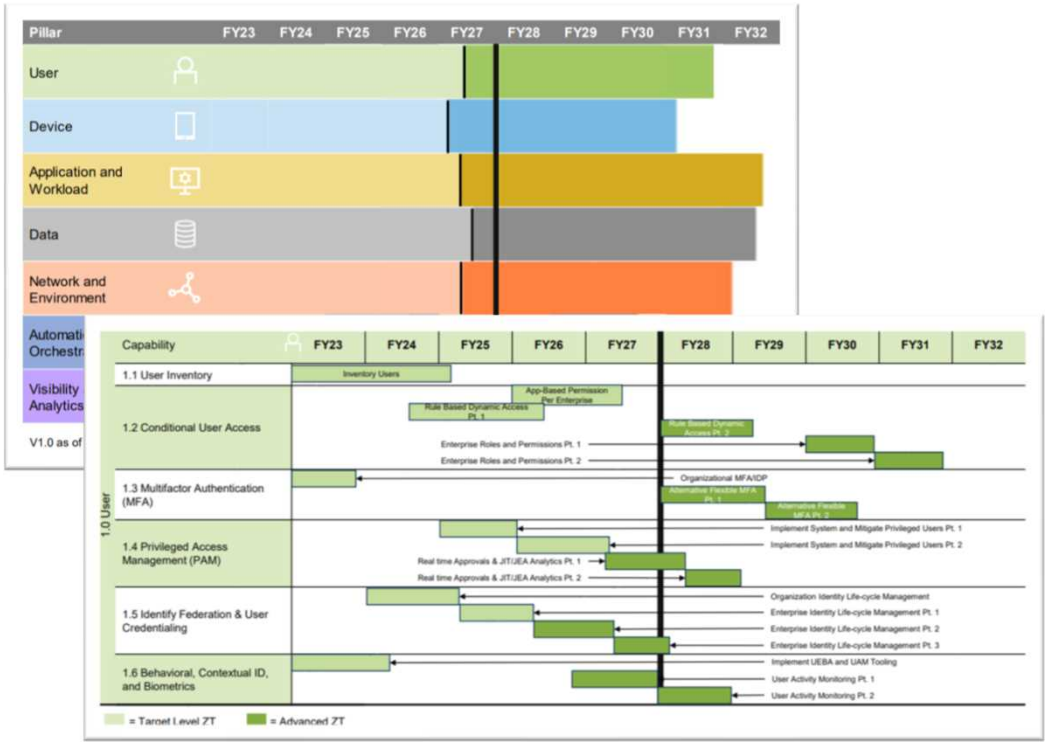
参考資料2

ゼロトラストアーキテクチャ実現において、最低限達成すべき項目（ベースライン）と、より高度な項目を分類し、FY27 （2028年9月） 年までにベースラインを達成し、FY32 （ 2033年9月）までに高度なゼロトラストアーキテクチャを実現するロードマップを作成。

■ ベースラインと高度な項目の分類
ゼロトラスト実現に必要な各項目において、FY27までに達成すべきベースとなる項目と、それ以降に実施すべき高度な項目を整理している。



■ 具体的な実施スケジュールの設計
左図において分類した各項目について、各項目ごとに具体的な実装スケジュールを策定している。



出典：DOD ZT Capability Execution Roadmap (defense.gov)

参考資料2

アメリカ国防総省のゼロトラスト実装におけるアクティビティ

凡例
■：第一に実施すべき事項
■：FY27までに達成すべきベースライン
■：高度なゼロトラストアーキテクチャ

アメリカ国防総省のゼロトラスト実装スケジュールからアクティビティ、実施時期を整理し、
FY23から優先的に実施すべき事項、FY27までに達成すべきベースライン、高度なゼロトラストアーキテクチャに分類した。

No.	大項目	小項目	アクティビティ	開始予定時期	完了予定時期
1	ユーザ	1.1 ユーザーインベントリ	ユーザーインベントリの作成	FY23	FY25
2		1.2 条件付きアクセス	事業ごとのアプリへのアクセス許可	FY26	FY27
3			ルールベースの動的アクセス1	FY24	FY26
4			ルールベースの動的アクセス2	FY28	FY29
5			事業の役割と権限1	FY30	FY30
6			事業の役割と権限2	FY31	FY31
7		1.3 多要素認証	組織的なMFA/IDPの導入	FY23	FY23
8			フレキシブルな代替MFA1	FY28	FY29
9			フレキシブルな代替MFA2	FY29	FY30
10		1.4 特権アクセス管理	システム導入と特権ユーザーの削減1	FY25	FY26
11			システム導入と特権ユーザーの削減2	FY26	FY27
12			リアルタイム承認とJIT/JEA※1分析1	FY27	FY28
13			リアルタイム承認とJIT/JEA分析2	FY28	FY29
14		1.5 IDフェデレーションとユーザー認証	組織IDのライフサイクル管理	FY24	FY25
15			事業IDのライフサイクル管理1	FY25	FY26
16			事業IDのライフサイクル管理2	FY26	FY27
17			事業IDのライフサイクル管理3	FY27	FY28

アメリカ国防総省のゼロトラスト実装におけるアクティビティ

参考資料2

（続き）

凡例
■：第一に実施すべき事項
■：FY27までに達成すべきベースライン
■：高度なゼロトラストアーキテクチャ

No.	大項目	小項目	アクティビティ	開始予定時期	完了予定時期
18	ユーザー	1.6 振舞い、コンテキストID、生体認証	UEBA※2およびUAM※3ツールの導入	FY23	FY24
19			ユーザーの活動監視1	FY26	FY27
20			ユーザーの活動監視2	FY28	FY28
21		1.7 最小限の特権アクセス	既定のポリシーによるアクセス拒否	FY23	FY24
22		1.8 連続認証	シングルサインオンの導入	FY23	FY24
23			定期的な認証	FY24	FY26
24			連続認証1	FY28	FY29
25			連続認証2	FY29	FY30
26		1.9 ICAM※統合プラットフォーム	事業のPKI/IDP1	FY24	FY24
27			事業のPKI/IDP2	FY26	FY28
28			事業のPKI/IDP3	FY28	FY30
29	デバイス	2.1 デバイスインベントリ	デバイスヘルスツールによるギャップ分析	FY23	FY23
30			管理下のNPE※4/PKIデバイス	FY24	FY26
31			事業のIDP1	FY25	FY26
32			事業のIDP2	FY29	FY29

アメリカ国防総省のゼロトラスト実装におけるアクティビティ

参考資料2

（続き）

凡例
- ■：第一に実施すべき事項
- ■：FY27までに達成すべきベースライン
- ■：高度なゼロトラストアーキテクチャ

No.	大項目	小項目	アクティビティ	開始予定時期	完了予定時期
33	デバイス	2.2 デバイスの検出とコンプライアンス	C2C(Comply-to-Connect)※5とコンプライアンスに基づくネットワーク認証の導入1	FY26	FY27
34			C2C(Comply-to-Connect)とコンプライアンスに基づくネットワーク認証の導入2	FY28	FY29
35		2.3 リアルタイムの検査とデバイス認証	次世代アンチウイルスとC2C(Comply-to-Connect)の統合	FY23	FY24
36			アプリケーションコントロールとFIMツールの導入	FY25	FY26
37			エンティティの活動監視1	FY26	FY28
38			エンティティの活動監視2	FY28	FY29
39			セキュリティスタックとC2Cの統合	FY27	FY28
40			事業のPKI1	FY28	FY29
41			事業のPKI2	FY30	FY30
42		2.4 リモートアクセス	既定のポリシーによるデバイスの拒否	FY26	FY27
43			一部の管理されたBYODとIoTサポート	FY23	FY26
44			全ての管理されたBYODとIoTサポート1	FY27	FY29
45			全ての管理されたBYODとIoTサポート2	FY29	FY31
46		2.5資産、脆弱性、パッチ管理の自動化	資産、脆弱性、パッチ管理ツールの導入	FY24	FY25

アメリカ国防総省のゼロトラスト実装におけるアクティビティ

参考資料2

（続き）

凡例
■：第一に実施すべき事項
■：FY27までに達成すべきベースライン
■：高度なゼロトラストアーキテクチャ

No.	大項目	小項目	アクティビティ	開始予定時期	完了予定時期
47	デバイス	2.6 UEMとMDM	UEDMまたは同等ツールの導入	FY24	FY25
48			業務デバイス管理1	FY23	FY24
49			業務デバイス管理2	FY24	FY25
50		2.7 EDRとXDR	EDRの導入とC2Cとの統合	FY24	FY25
51			XDRの導入とC2Cとの統合1	FY25	FY27
52			XDRの導入とC2Cとの統合2	FY27	FY28
53	アプリケーションとワークロード	3.1 アプリケーションインベントリ	アプリケーションとコードの識別	FY24	FY25
54			リソースの認証1	FY24	FY25
55			リソースの認証2	FY25	FY27
56		3.2 セキュアなソフトウェアの開発と統合	DevSecOpsのソフトウェアファクトリー構築1	FY24	FY25
57			DevSecOpsのソフトウェアファクトリー構築2	FY25	FY26
58			アプリケーションのセキュリティとコード修復の自動化1	FY27	FY28
59			アプリケーションのセキュリティとコード修復の自動化2	FY28	FY29
60		3.3 ソフトウェアリスク管理	承認済みバイナリ/コード	FY23	FY25
61			脆弱性管理プログラム1	FY23	FY23
62			脆弱性管理プログラム2	FY23	FY24
63			継続的な検証	FY25	FY25

アメリカ国防総省のゼロトラスト実装におけるアクティビティ

参考資料2

（続き）

凡例
■：第一に実施すべき事項
■：FY27までに達成すべきベースライン
■：高度なゼロトラストアーキテクチャ

No.	大項目	小項目	アクティビティ	開始予定時期	完了予定時期
64	アプリケーションとワークロード	3.4 リソースの認証と統合	SDC※6リソースの認証1	FY23	FY25
65			SDCリソースの認証2	FY25	FY27
66			リソース認可のための属性の強化1	FY29	FY31
67			リソース認可のための属性の強化2	FY31	FY32
68			REST APIのマイクロセグメンテーション	FY28	FY30
69		3.5 継続的なモニタリングと認可	継続的な使用認可1	FY26	FY27
70			継続的な使用認可2	FY27	FY29
71	データ	4.1 データカタログのリスクアラインメント	データ分析	FY23	FY24
72		4.2 国防総省のデータガバナンス	データのタグ付け標準の定義	FY23	FY24
73			相互運用規格の策定	FY23	FY24
74			ソフトウェア定義ストレージ（SDS）ポリシーの策定	FY23	FY23
75		4.3 データのラベリングとタグ付け	データのタグ付けと分類ツールの導入	FY24	FY25
76			手動によるデータのタグ付け1	FY24	FY25
77			手動によるデータのタグ付け2	FY27	FY28
78			自動的なデータのタグ付けとサポート1	FY27	FY28
79			自動的なデータのタグ付けとサポート2	FY28	FY31

アメリカ国防総省のゼロトラスト実装におけるアクティビティ

参考資料2

（続き）

凡例
■：第一に実施すべき事項
■：FY27までに達成すべきベースライン
■：高度なゼロトラストアーキテクチャ

No.	大項目	小項目	アクティビティ	開始予定時期	完了予定時期
80	データ	4.4 データ監視とセンシング	DLP※7実施ポイントの記録と分析	FY23	FY23
81			DRM※8実施ポイントの記録と分析	FY23	FY23
82			ファイルアクティビティの監視1	FY24	FY25
83			ファイルアクティビティの監視2	FY25	FY26
84			データベースアクティビティの監視	FY27	FY28
85			包括的なデータアクティビティ監視	FY28	FY30
86		4.5 データ暗号化と著作権管理	DRMと保護ツールの導入1	FY24	FY25
87			DRMと保護ツールの導入2	FY25	FY27
88			データタグとアナリティクスによるDRMの実施1	FY25	FY27
89			データタグとアナリティクスによるDRMの実施2	FY27	FY29
90			データタグとアナリティクスによるDRMの実施3	FY29	FY31
91		4.6 データ損失防止	実施ポイントの導入	FY25	FY27
92			データタグと分析によるDLPの実施1	FY25	FY27
93			データタグと分析によるDLPの実施2	FY27	FY29
94			データタグと分析によるDLPの実施3	FY29	FY32

アメリカ国防総省のゼロトラスト実装におけるアクティビティ

参考資料2

（続き）

凡例
■：第一に実施すべき事項
■：FY27までに達成すべきベースライン
■：高度なゼロトラストアーキテクチャ

No.	大項目	小項目	アクティビティ	開始予定時期	完了予定時期
95	データ	4.7 データアクセス制御	DAASアクセスとSDSポリシーの統合1	FY23	FY25
96			DAASアクセスとSDSポリシーの統合2	FY28	FY29
97			DAASアクセスとSDSポリシーの統合3	FY29	FY30
98			SDSソリューションとポリシーのIDPへの統合1	FY26	FY27
99			SDSソリューションとポリシーのIDPへの統合2	FY27	FY27
100			SDSツールの導入およびDRMツールとの統合1	FY27	FY28
101			SDSツールの導入およびDRMツールとの統合2	FY28	FY29
102	ネットワークと環境	5.1 データフローマッピング	詳細なアクセスルールとポリシーの定義1	FY23	FY23
103			詳細なアクセスルールとポリシーの定義2	FY23	FY24
104		5.2 SDN(Software Defined Networking)	SDNのAPI定義	FY23	FY24
105			SDNのプログラマブルなインフラストラクチャの導入	FY24	FY27
106			制御、管理、データプレーンへのセグメントフロー	FY24	FY25
107			ネットワーク資産の検出と最適化	FY27	FY29
108			リアルタイムのアクセス判断	FY30	FY32
109		5.3 マクロセグメンテーション	データセンターのマクロセグメンテーション	FY23	FY24
110			B/C/P/Sマクロ・セグメンテーション	FY25	FY26

アメリカ国防総省のゼロトラスト実装におけるアクティビティ

参考資料2

（続き）

凡例
■：第一に実施すべき事項
■：FY27までに達成すべきベースライン
■：高度なゼロトラストアーキテクチャ

No.	大項目	小項目	アクティビティ	開始予定時期	完了予定時期
111	ネットワークと環境	5.4 マイクロセグメンテーション	マイクロセグメンテーションの導入	FY24	FY25
112			アプリケーションとデバイスのマイクロセグメンテーション	FY25	FY27
113			プロセスのマイクロセグメンテーション	FY27	FY29
114			転送中データの保護	FY26	FY26
115	自動化とオーケストレーション	6.1 PDP※9とポリシーオーケストレーション	ポリシーインベントリの作成	FY23	FY23
116			組織のアクセスプロファイル	FY24	FY25
117			事業のセキュリティプロファイル1	FY25	FY26
118			事業のセキュリティプロファイル2	FY26	FY27
119		6.2 クリティカルプロセスの自動化	タスク自動化の分析	FY23	FY23
120			事業統合とワークフローの提供1	FY24	FY26
121			事業統合とワークフローの提供2	FY26	FY27
122		6.3 機械学習	データのタグ付けと分類のMLツール導入	FY24	FY25
123		6.4 AI	AI自動化ツールの導入	FY26	FY28
124			AI分析による自動化・オーケストレーションの修正	FY27	FY30
125		6.5 SOAR	レスポンス自動化の分析	FY23	FY23
126			SOARツールの導入	FY24	FY25
127			手順書作成	FY28	FY29

アメリカ国防総省のゼロトラスト実装におけるアクティビティ

参考資料2

（続き）

凡例
■：第一に実施すべき事項
■：FY27までに達成すべきベースライン
■：高度なゼロトラストアーキテクチャ

No.	大項目	小項目	アクティビティ	開始予定時期	完了予定時期
128	自動化とオーケストレーション	6.6 APIの標準化	ツールのコンプライアンス分析	FY23	FY23
129			APIの標準化1	FY23	FY24
130			APIの標準化2	FY24	FY25
131		6.7 SOCとIR※10	ワークフローの強化1	FY23	FY23
132			ワークフローの強化2	FY23	FY24
134			ワークフローの強化3	FY28	FY28
135			ワークフロー自動化	FY29	FY30
136	可視性と分析	7.1 全トラフィックのログ記録	規模に関する検討	FY23	FY23
137			ログ構造化	FY24	FY24
138			ログ解析	FY25	FY25
139		7.2SIEM	ID・相関情報の資産化	FY24	FY25
140			脅威に対するアラート1	FY24	FY24
141			脅威に対するアラート2	FY24	FY26
142			脅威に対するアラート3	FY28	FY29
143			ユーザ・デバイスのベースライン策定	FY25	FY26
144		7.3一般的セキュリティ・リスク分析	分析ツール導入	FY24	FY25
145			ユーザの行動指針策定	FY26	FY26

アメリカ国防総省のゼロトラスト実装におけるアクティビティ

参考資料2

（続き）

凡例
■：第一に実施すべき事項
■：FY27までに達成すべきベースライン
■：高度なゼロトラストアーキテクチャ

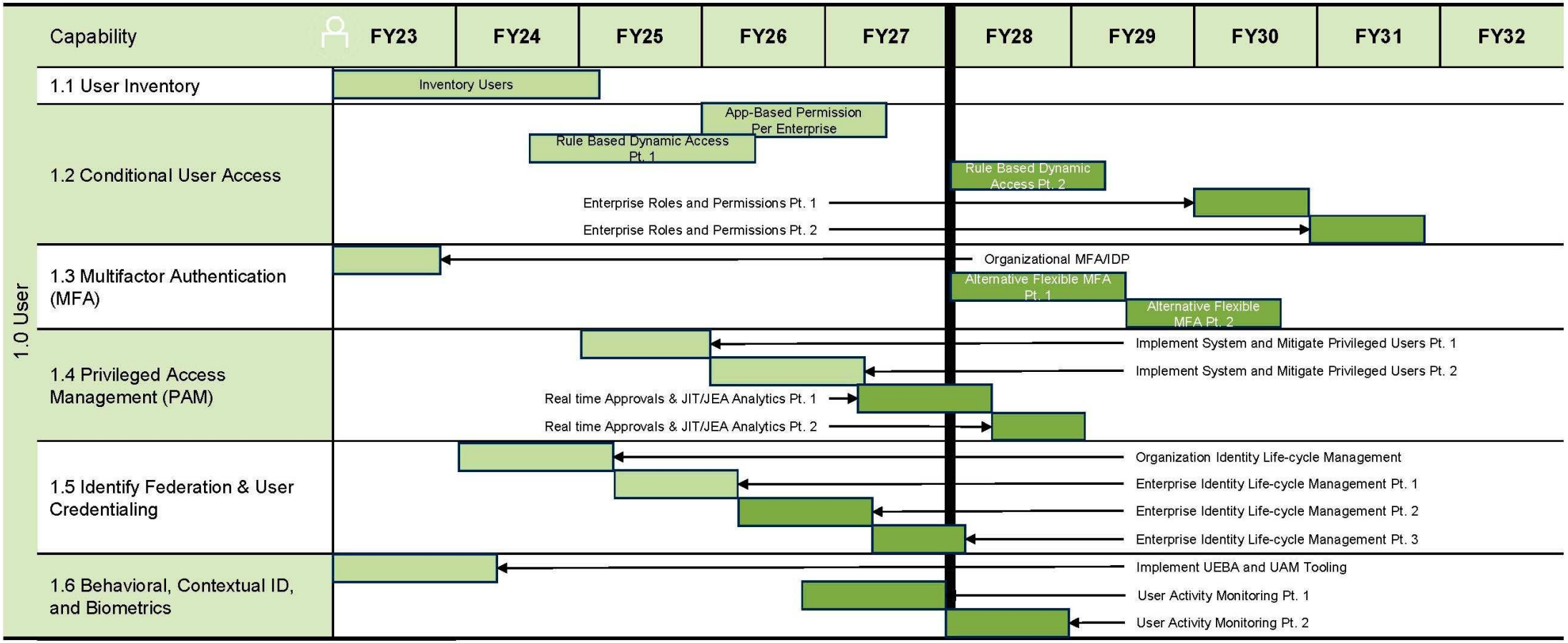
No.	大項目	小項目	アクティビティ	開始予定時期	完了予定時期
146	可視性と分析	7.4UEBA	ベースライン検討とプロファイリング1	FY26	FY26
145			ベースライン検討とプロファイリング1	FY27	FY28
147			ベースライン策定支援	FY27	FY27
148			ベースライン策定支援	FY27	FY27
149		7.5脅威インテグレーション統合	サイバー脅威インテリジェンスプログラム1	FY24	FY24
150			サイバー脅威インテリジェンスプログラム2	FY25	FY26
151		7.6動的ポリシーの自動化	AIによるネットワークアクセス制御	FY28	FY30
152			AIによる動的ポリシー制御	FY30	FY32

※1 JIT/JEA(Just-In-Time/Just-Enough-Access)・・・アクセス権限を決められた期間、必要最低限に制限して付与すること。
※2 UEBA(User and Entity Behavior Analytics)・・・ユーザ及びエンティティの行動分析を行い、不正な行動、リスクを早期に検知する技術。SIEMがセキュリティアナリスト向けのデータ整理に長ける一方で、UEBAはデータの分析に長ける。
※3 UAM(User Access Management)・・・システム内のユーザーが、適切なタイミングで必要なツールにアクセスできるように管理すること。IAMと同義。
※4 NPE(Non-Person Entity)・・・IDを持って行動する、人間以外のエンティティ。組織、デバイス、アプリケーション、情報成果物などが含まれる。
※5 C2C(Comply-to-Connect)・・・国防総省の運用環境でサイバーセキュリティの効率を高めるために設計されたフレームワーク。「デバイスの可視化・分類」、「デバイスの冗長な管理と制御」、「セキュリティとネットワーク管理のオーケストレーション」、「継続的監視と自動修復」の4つの特徴を持つ。
※6 SDC(Software Defined Compute)・・・CPUやGPU、メモリなどのコンピューターが計算するために必要とする資源を、必要な時に必要な量だけソフトウエアによって動的に確保して利用する技術やそのアーキテクチャ。
※7 DLP(Data Loss Prevention)・・・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。
※8 DRM(Digital Rights Management)・・・デジタルコンテンツの著作権を保護・管理する技術。
※9 PDP(Policy Decision Point)・・・アクセス制御に必要とされる論理コンポーネントの一つ。ユーザーIDを認証し、アクセスを許可するセキュリティチェックポイント。
※10 IR(Incident Response)・・・サイバー攻撃などのセキュリティインシデントが発生した際の対応。

アメリカ国防総省のゼロトラスト実装スケジュール – ユーザー (1/2)

参考資料2

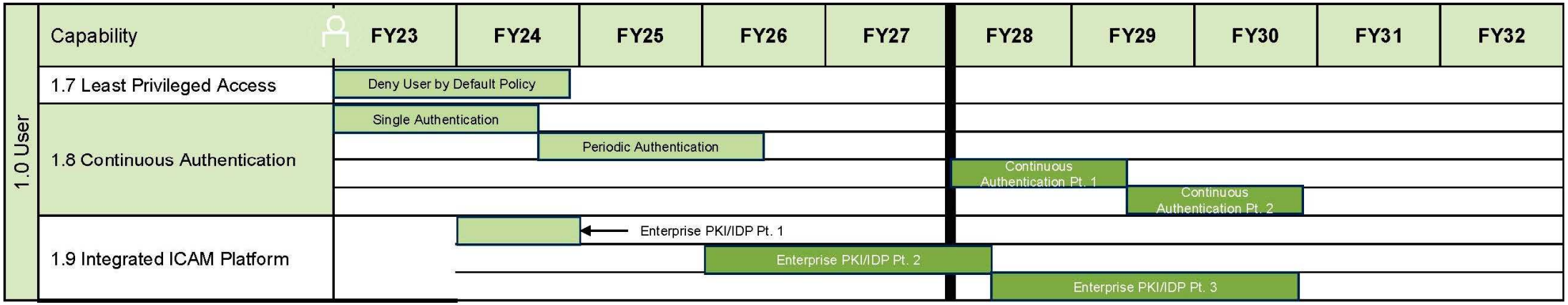
アメリカ国防総省のゼロトラスト実装スケジュール は以下の通り。



アメリカ国防総省のゼロトラスト実装スケジュール – ユーザー (2/2)

参考資料2

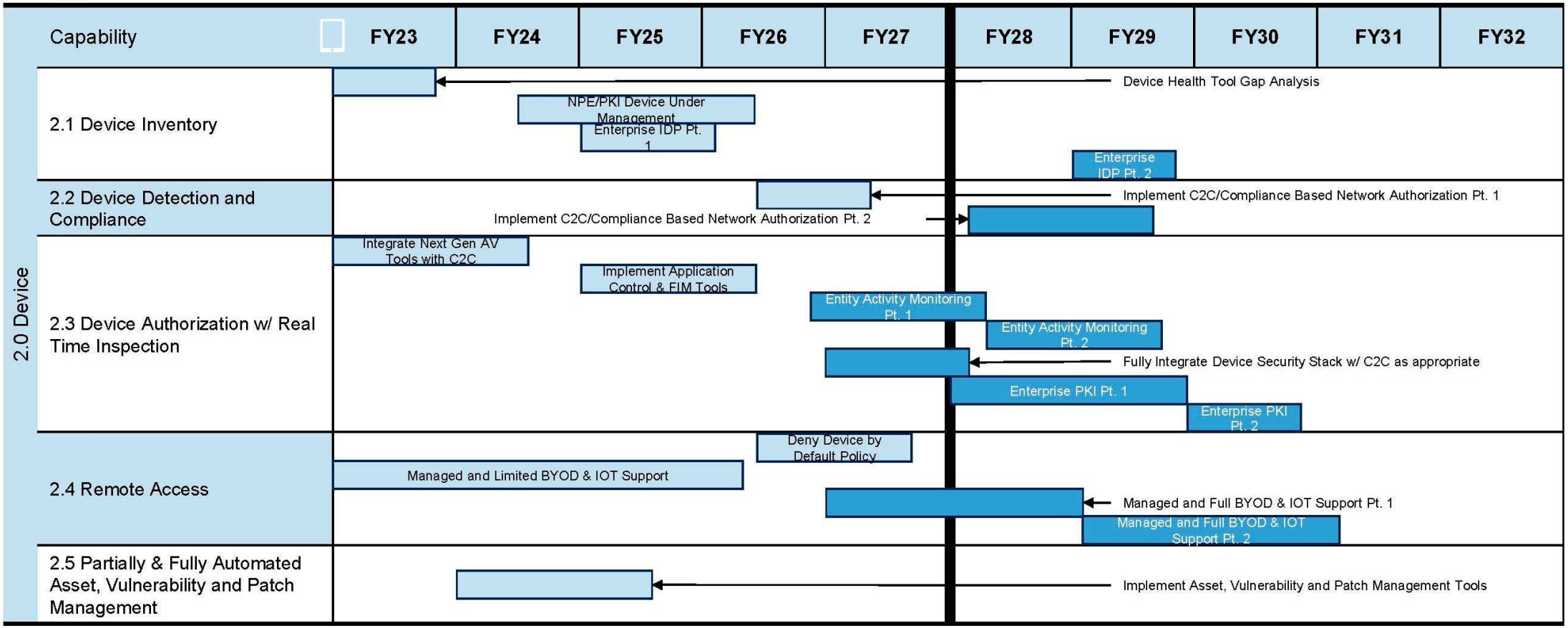
アメリカ国防総省のゼロトラスト実装スケジュール は以下の通り。



アメリカ国防総省のゼロトラスト実装スケジュール – デバイス (1/2)

参考資料2

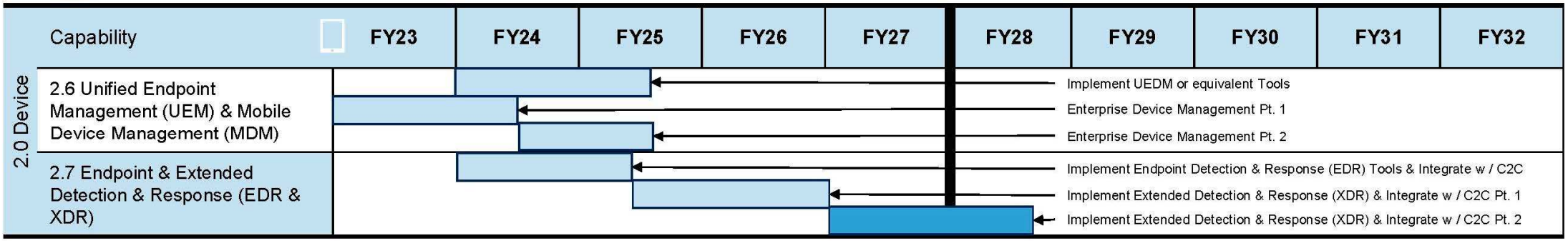
アメリカ国防総省のゼロトラスト実装スケジュール は以下の通り。



アメリカ国防総省のゼロトラスト実装スケジュール – デバイス (2/2)

参考資料2

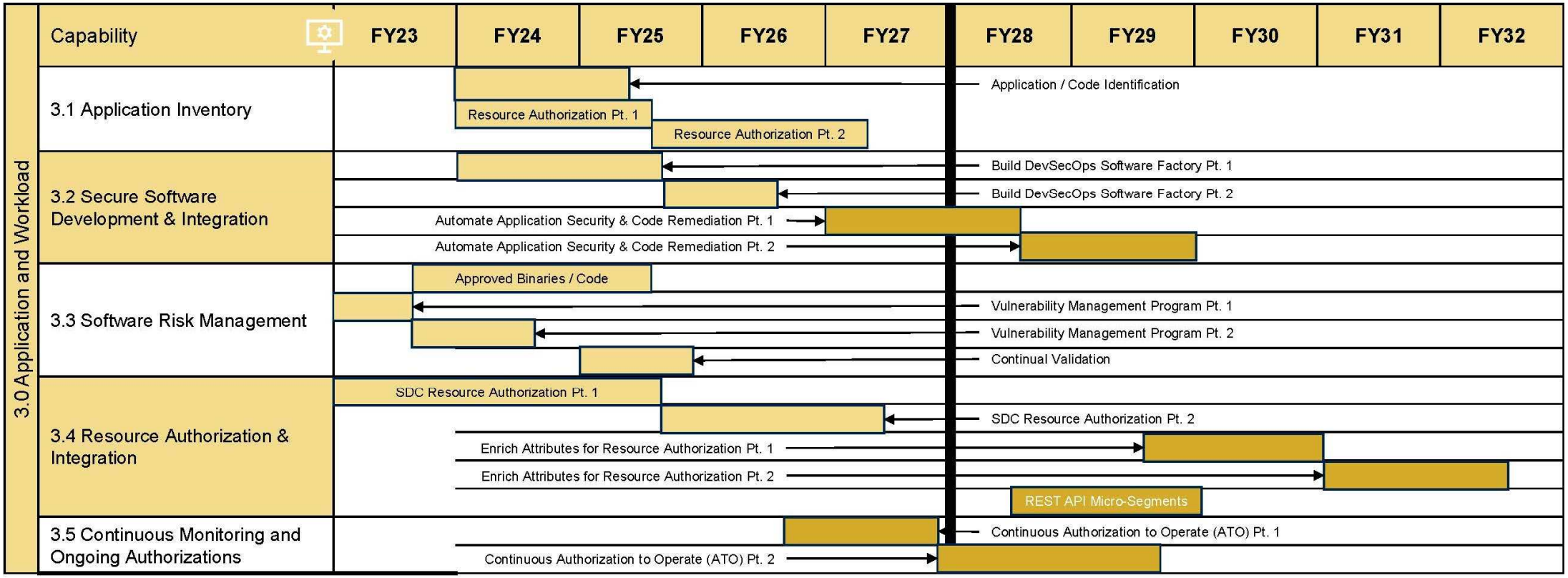
アメリカ国防総省のゼロトラスト実装スケジュール は以下の通り。



アメリカ国防総省のゼロトラスト実装スケジュール – アプリケーションとワークロード

参考資料2

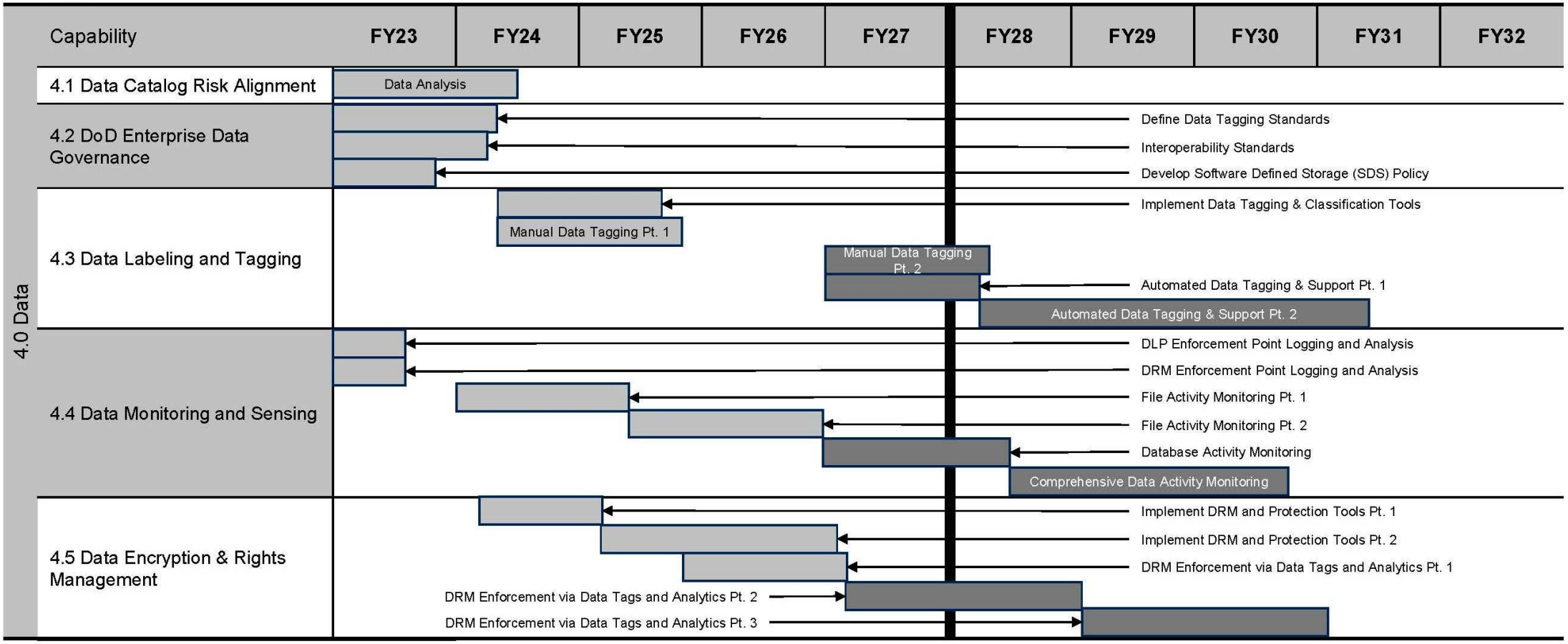
アメリカ国防総省のゼロトラスト実装スケジュール は以下の通り。



アメリカ国防総省のゼロトラスト実装スケジュール – データ (1/2)

参考資料2

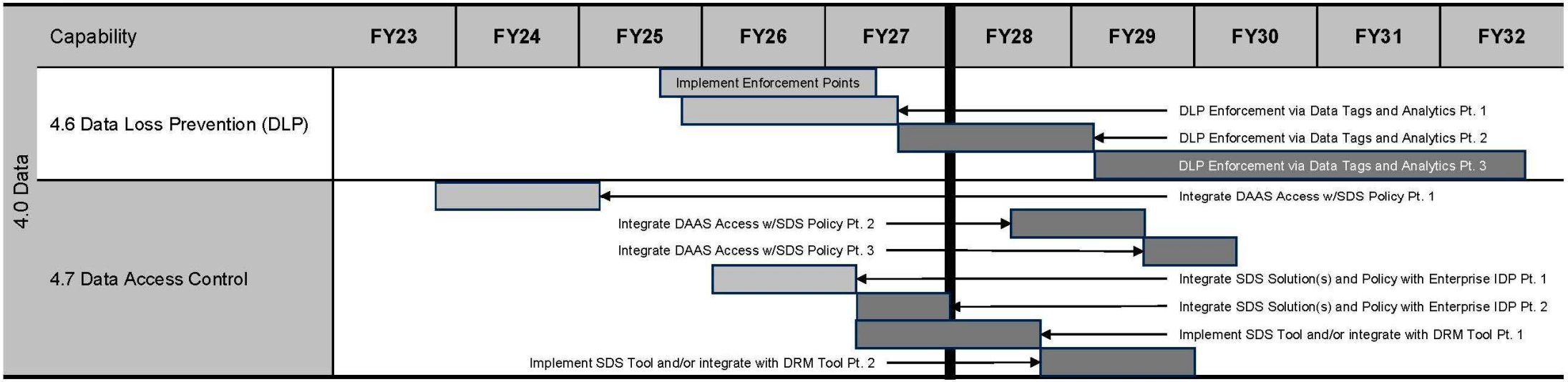
アメリカ国防総省のゼロトラスト実装スケジュール は以下の通り。



アメリカ国防総省のゼロトラスト実装スケジュール – データ (2/2)

参考資料2

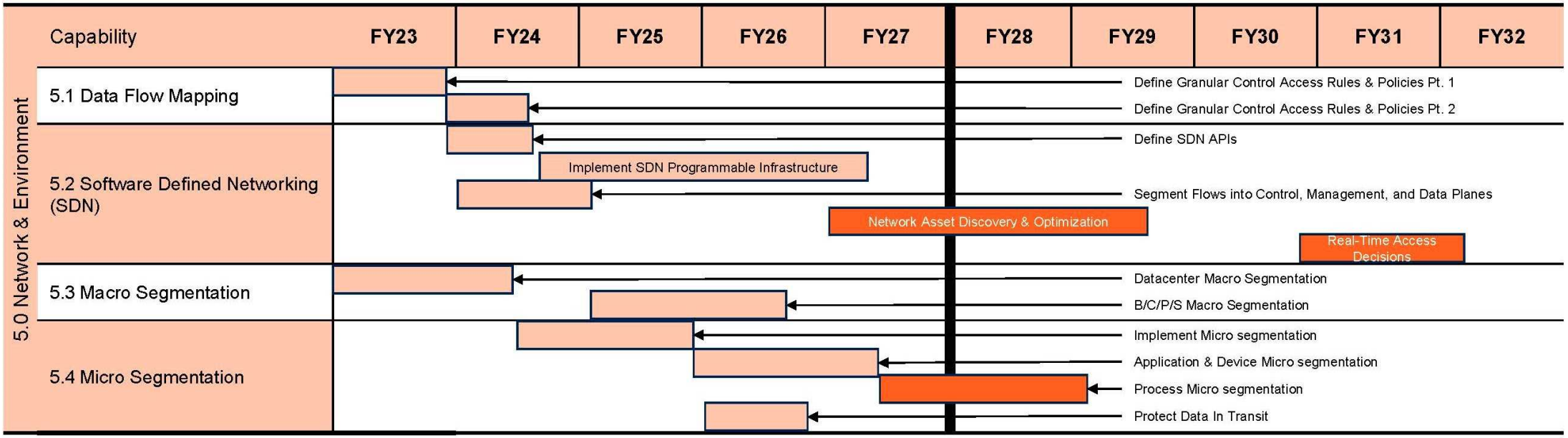
アメリカ国防総省のゼロトラスト実装スケジュール は以下の通り。



アメリカ国防総省のゼロトラスト実装スケジュール – ネットワークと環境

参考資料2

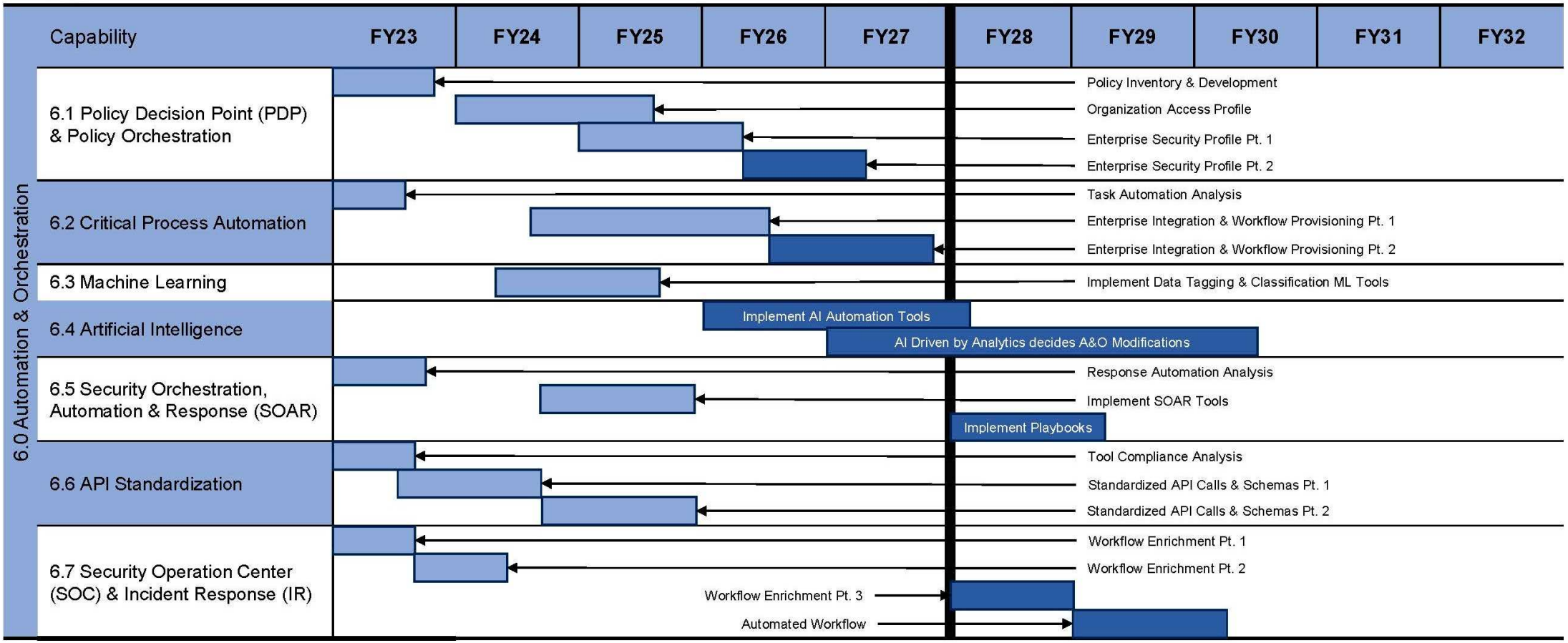
アメリカ国防総省のゼロトラスト実装スケジュール は以下の通り。



アメリカ国防総省のゼロトラスト実装スケジュール – 自動化とオーケストレーション

参考資料2

アメリカ国防総省のゼロトラスト実装スケジュール は以下の通り。



アメリカ国防総省のゼロトラスト実装スケジュール – 可視性と分析

参考資料2

アメリカ国防総省のゼロトラスト実装スケジュール は以下の通り。