セキュリティTFについて

2021.11.4

1．デジタル庁技術検討会議セキュリティTFの設置

- デジタル・ガバメント推進標準ガイドライン等を作成していたデジタル庁技術検討会議の下部組織として、セキュリティに関連するガイドライン等を作成する「セキュリティTF」を設置する。
- 具体的な検討事項として、 **①統一基準群を踏まえた整備方針及び具体的な技術ガイダンスの作成**、**②パブリッククラウド利用を前提とした統一基準群の改定案の整理**などを想定。
- セキュリティTFで作成したガイドラインは、NISCと連携をとりながら、**デジタル社会推進会議幹事会と必要に応じてサイバーセキュリティ対策推進会議（CISO等連絡会議）共同で決定**をする。

セキュリティTFの主要な活動

①統一基準群を踏まえた具体的な技術ガイダンスの作成

統一基準群は、府省庁自らがセキュリティ対策を講じていく原則の下で、各組織の取組水準を向上させるための統一的な枠組みとして基本的な考え方（遵守事項）と実践のポイントを取りまとめたもの。

- 各府省の理解や体制が十分でない場合、実務で十分なセキュリティ対応がなされないおそれ

▼

- 統一基準群で示された考え方に基づき、これを実務で即活用できる実践的な技術ガイダンスを作成。

②パブリッククラウド利用を前提とした統一基準群の改定案の整理

統一基準群は特定のシステム像を想定したものではないが、現状政府情報システムで中核であるオンプレ型基幹システムに必要なセキュリティ対策の考え方は相対的に充実している

- R3改定でクラウドについて記載の充実がされたが、クラウドについては不足部分があるのではないか。

▼

- パブリッククラウド利用を前提として今後の統一基準群に盛り込むべき事項や章立てのあり方を整理し、R5年度改定案（R4秋に検討）の検討に提案。

検討内容を②にもフィードバック

① 統一基準群を踏まえた整備方針及び具体的な技術ガイダンスの作成

- **①検査関係、②クラウド関係、③ゼロトラスト関係**等をテーマとしながら、統一基準群を具体化した**技術ガイダンス**を作成。（デジタル庁「標準ガイドライン群」及びNISC「統一基準群」の一部に、これら技術ガイダンスを位置付ける）
- R3年12月までに整備方針を策定し、重点計画に反映。R4年6月までに詳細化し、出来上がったものから順次、デジタル社会推進会議幹事会・サイバーセキュリティ対策推進会議（CISO等連絡会議）で共同決定する。

技術ガイダンスのテーマ（例）

1．検査関係

a. 脆弱性診断

b. システム検証

c. バックドア検証と検証事業者

2．クラウド関係

a. クラウド利活用の検討
   - クラウドのPF上にアプリを作る場合のSecurity By Designをイメージ。ISMAPの活用方法を含む。

b. 影響度に応じたコントロールのベースライン
   - 現状のISMAP管理策は、影響度が中程度に応じたコントロールになっているので、その他影響度のコントロールのベースラインを整理する。

c. 調達時に求めるセキュリティ要件

3．ゼロトラスト関係

a. ゼロトラストアーキテクチャ
   - 各府省におけるガバナンス、職員管理・組織管理、IT資産管理（CDM（※））の在り方

※Continuous Diagnostics and Mitigation

①統一基準群を踏まえた整備方針及び具体的な技術ガイダンスの作成

庁内実施体制（案）

※必要に応じて外部有識者の参加も検討。

1．検査

a. 脆弱性診断
b. システム検証
c. バックドア検証と検証事業者

2．クラウド

a. クラウド利活用の検討
b. 影響度に応じたコントロールのベースライン
c. 調達時に求めるセキュリティ要件

3．ゼロトラスト

a. ゼロトラストアーキテクチャ（必要に応じて複数のガイダンスを作成予定。）

テーマ選定の注意点

- 想定するターゲット
  - デジタル庁各プロジェクトに加え、IT・セキュリティ態勢を十分に充実できない中規模の組織を対象にする。政府職員や受託事業者候補であるSIerへの教育プログラムと連携することが重要。
- 進め方
  - テーマ設定およびガイドラインの内容（仕様書への記載文言、チェック表の必要性等）の検討にあたっては、ニーズのヒアリングを実施する。
  - 技術ガイダンスのテーマに関しては、（全てを一度に作成せず）まずテーマの全体像と作成予定を示す。

②パブリッククラウド利用を前提とした統一基準群の改定案の整理

- **パブリッククラウド利用を前提として今後の統一基準群に盛り込むべき事項や章立てのあり方に関して整理**し、NISCに改定案を提案する。
- 検討に際しては、**クラウドTに提案の原案策定を依頼**し、セキュリティTFの一つのテーマとして、セキュリティTの観点でブラッシュアップする。
- 本年秋から検討を開始し、R4年夏までにデジタル庁の考え方を整理。内容は、**R5年度版の統一基準案（R4年秋に検討）の検討に提案**。

論点（案）

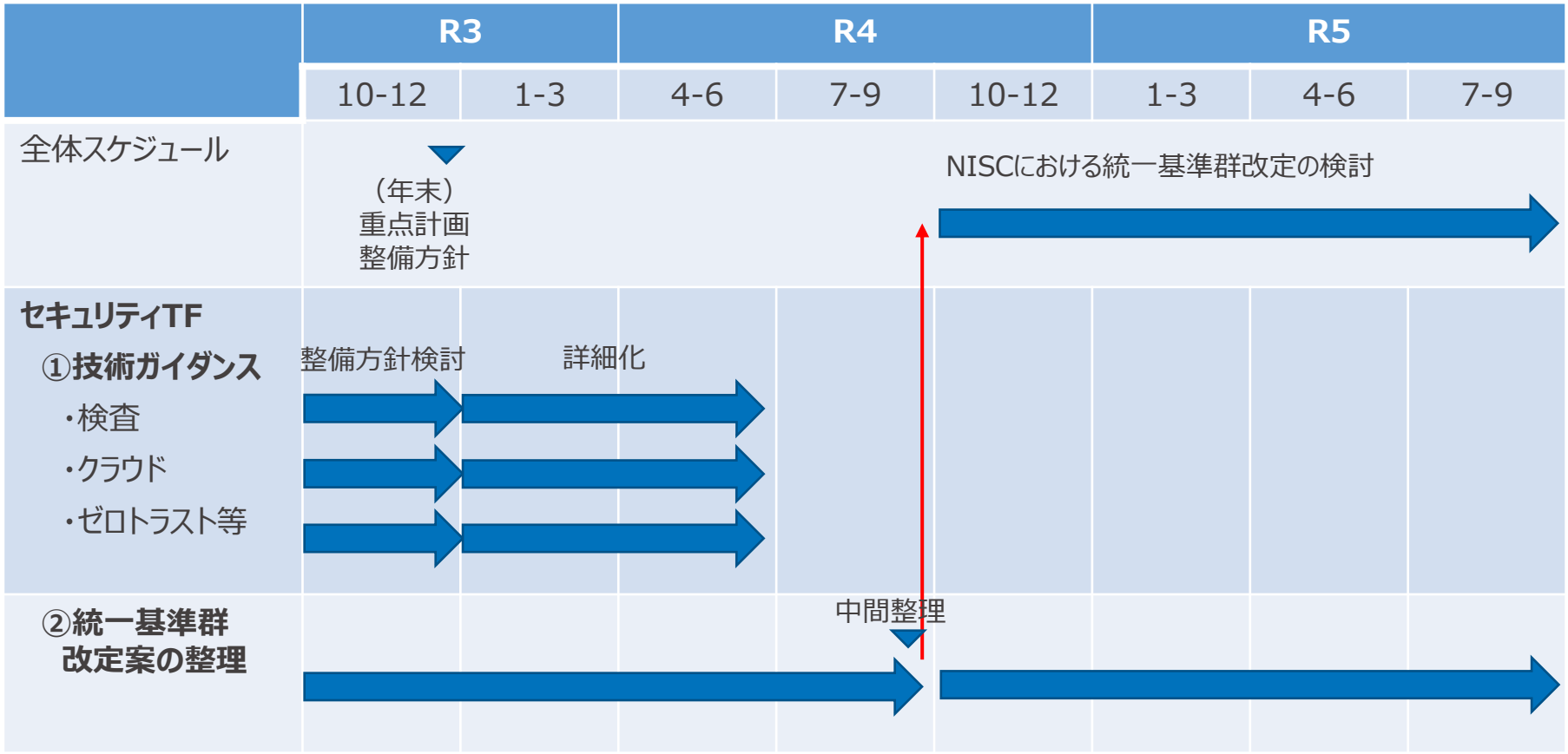
- 自動監査による統一基準への準拠性の自動確認
- ・・・
- ・・・（要検討）

スケジュール

- R3年秋　：検討開始
  （年末の重点計画・整備方針で論点提示）
- R4年夏　：中間整理
- R４年秋　：NISCのR5年度版統一基準案の検討に提案。

※追加の整理が必要であれば、R4年秋にNISCと一緒に対応。

2．スケジュール


R3
R4
R5
10-12
1-3
4-6
7-9
10-12
1-3
4-6
7-9
全体スケジュール
（年末）
重点計画
整備方針
NISCにおける統一基準群改定の検討
セキュリティTF
①技術ガイダンス
・検査
・クラウド
・ゼロトラスト等
整備方針検討
詳細化
②統一基準群
改定案の整理
中間整理