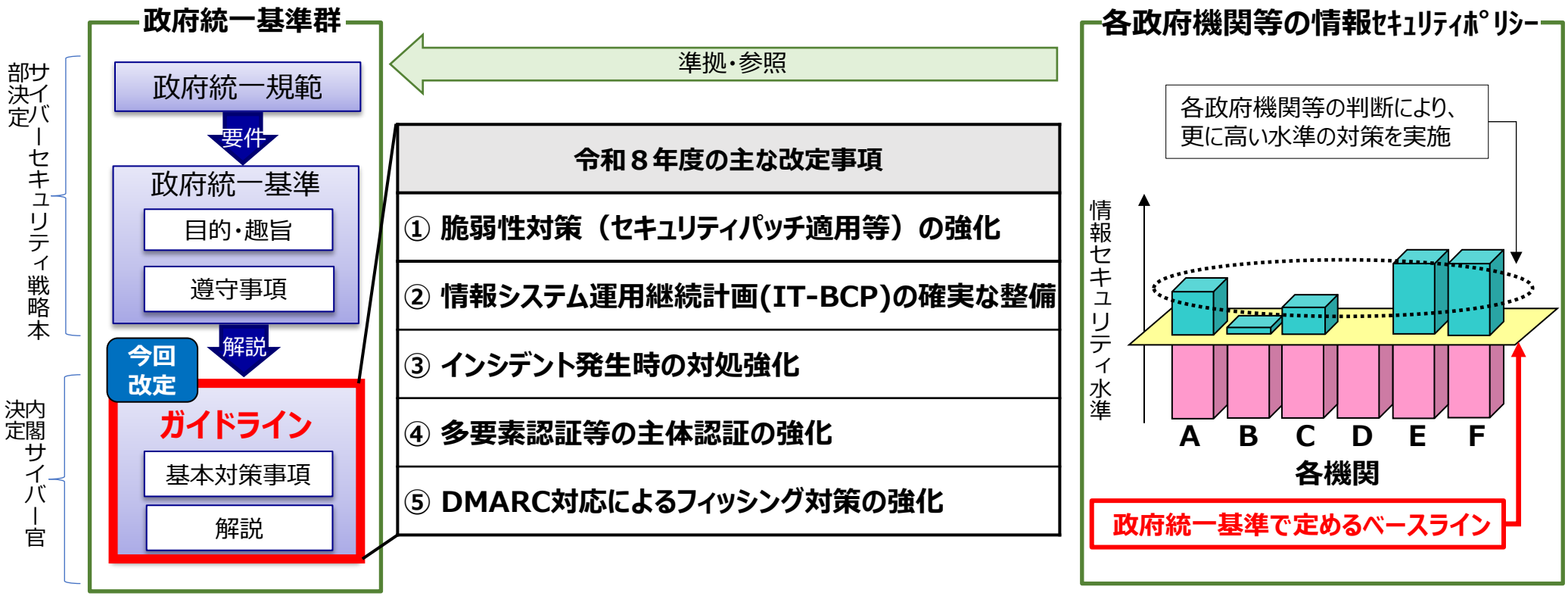
「政府機関等の対策基準策定のためのガイドライン（令和７年度版）」の一部改定（令和８年６月12日）のポイント

令和８年６月
内閣官房 国家サイバー統括室

「政府機関等の対策基準策定のためのガイドライン」の令和８年度一部改定について

- **「政府機関等の対策基準策定のためのガイドライン」**は、政府統一基準※の定めを満たすため、とるべき具体的な対策や解説を盛り込んだものであり、国家サイバー統括室において策定。
- **令和８年６月12日、最近の技術動向等を踏まえて、必要な改定を行うもの。**
- **主な改定事項は、①脆弱性対策の強化、②情報システム運用継続計画(IT-BCP)の確実な整備、③インシデント発生時の対処強化、④多要素認証等の主体認証の強化、⑤DMARC対応によるフィッシング対策強化**

※ サイバーセキュリティ基本法に基づいて、サイバーセキュリティ戦略本部が定める、政府機関等の情報セキュリティ基準。政府機関（26組織）・独立行政法人（86組織）・指定法人（10組織）が対象。



改定事項	改定の主な内容
①脆弱性対策(セキュリティパッチ適用等)の強化	・ 高性能AIの悪用などのサイバー攻撃の高度化・自動化等をふまえ、 －**全情報システムについて、セキュリティパッチの適時の適用を前提とした運用設計**(パッチマネジメント)を行う。 －**サイバー攻撃の高度化・自動化等の状況をふまえ、運用設計を見直す。** －**迅速な適用の要否を判断した上で、脆弱性対策計画を策定・実施する。** －迅速な適用が必要な場合、**情報システムの運用を一時停止することも検討**する。
②情報システム運用継続計画（IT-BCP）の確実な整備	・情報システム運用継続計画（IT-BCP）で求められるセキュリティ要件を情報システムへ確実に実装するため、機関等の各情報システムについて、 －**政府業務継続計画における非常時優先業務等を支えるシステムかを確認**する。 －**IT-BCPが整備されているかを確認**する。 －**IT-BCPの要件をふまえてセキュリティ要件を策定する。**
③インシデント発生時の対処強化 （NCOへの連絡(報告)事項の追加等）	・情報セキュリティインシデント発生時にNCOへ連絡(報告)する事項に、**サイバー脅威の分析に資する情報（IoCやログ、デジタルフォレンジック結果等）を追加**する。
④多要素認証等の主体認証強化	・基幹システム等において、情報セキュリティインシデントに繋がるおそれのある**強い権限を持つ主体には原則、多要素主体認証方式を導入**する。
⑤DMARC対応によるフィッシング対策強化 （電子メールのなりすまし対策）	・政府機関等になりすました電子メールを受信した場合、**当該受信メールが迷惑メール(quarantine)又は受信拒否 (reject)となる**よう、政府機関等側のDMARCポリシーの設定を強化する。