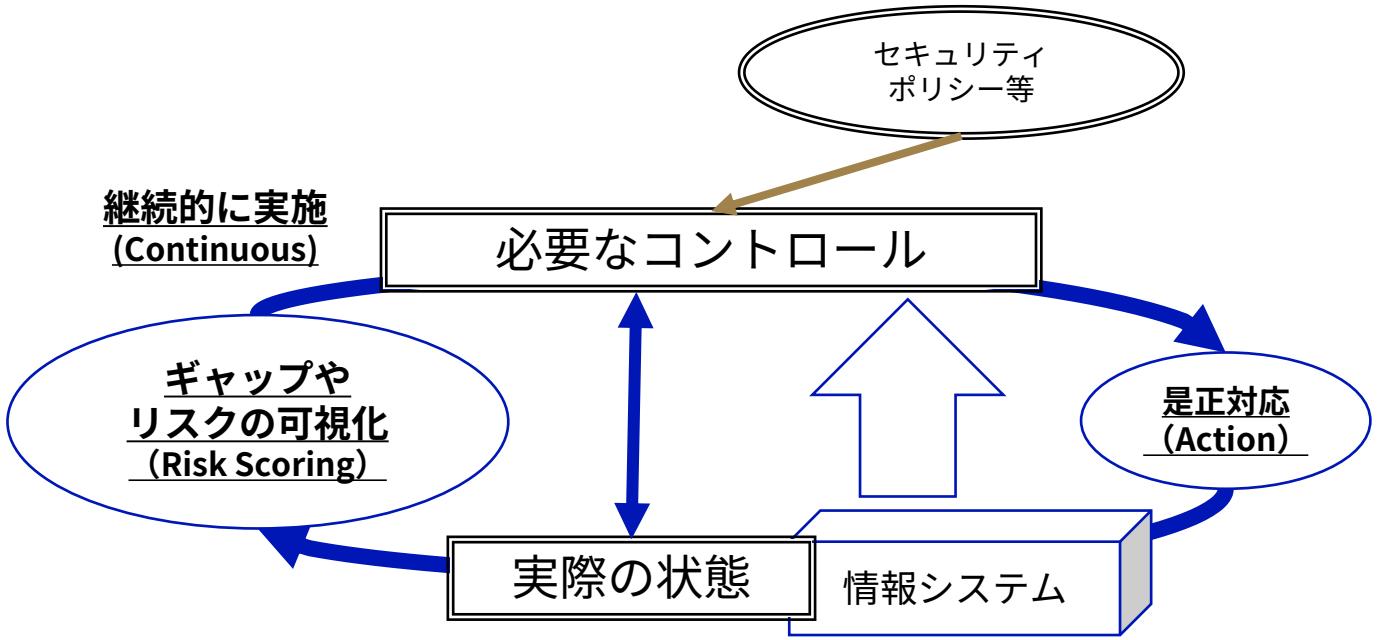
常時リスク診断・対処
（CRSA：Continuous Risk Scoring and Action）

常時リスク診断・対処（CRSA：Continuous Risk Scoring and Action）の概要

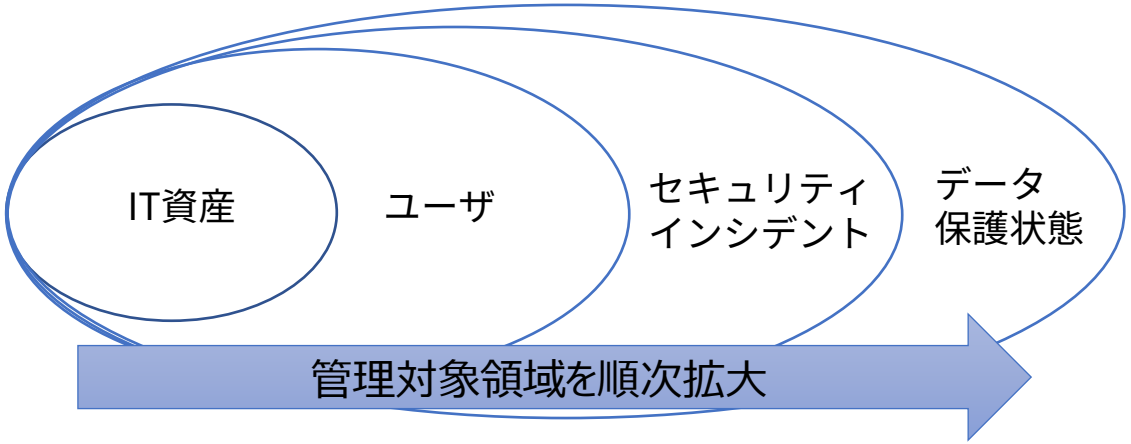
●常時リスク診断・対処

- **リスク診断**
  必要なコントロールと実際の状態の
  ギャップやリスクを可視化
- **対処**
  可視化されたギャップやリスクの
  是正対応
- **常時**
  ギャップやリスクの可視化と
  是正対応を継続的に実施

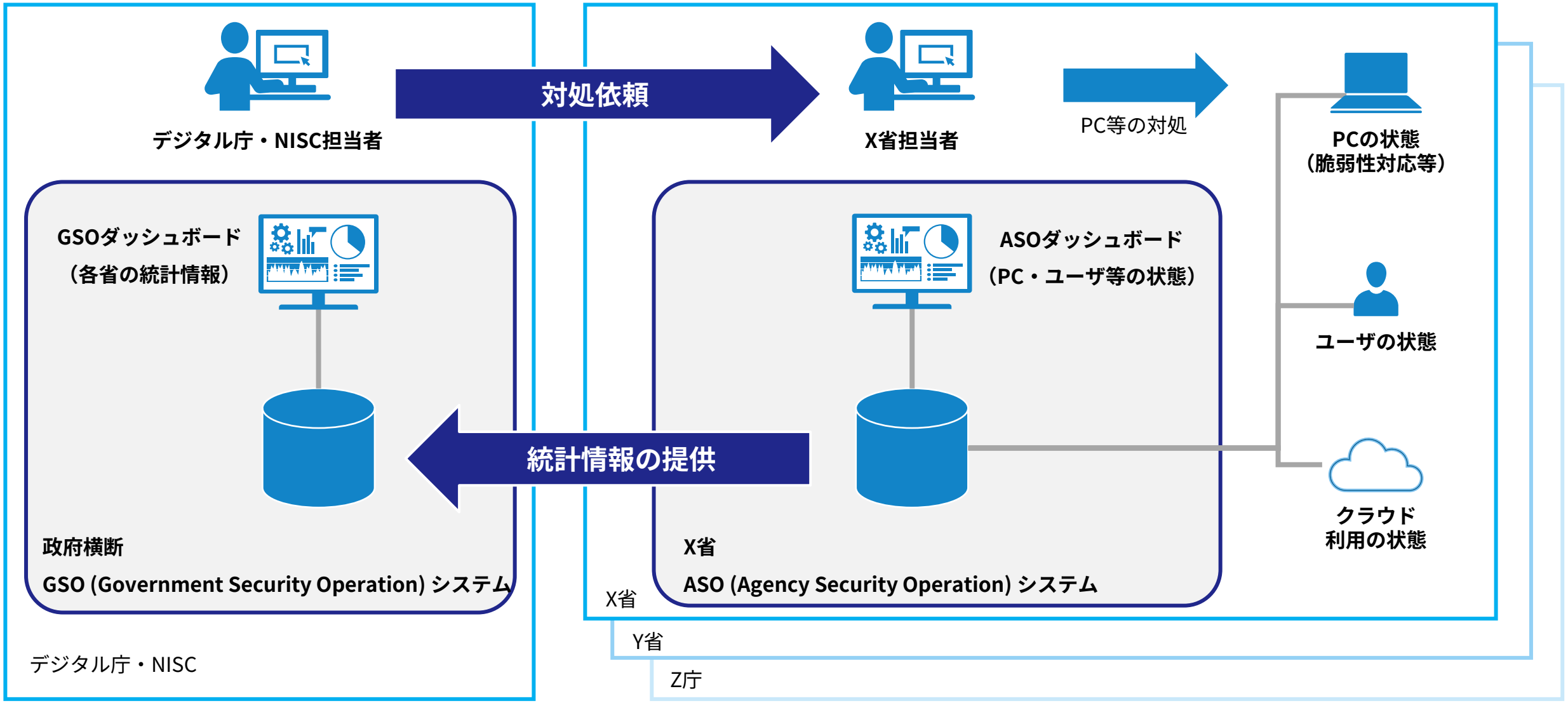


●管理対象

- **IT資産（デバイス、ソフトウェア、サービス等）、ユーザ、セキュリティインシデント、データ保護状態**を管理対象と想定
- 実装される管理対象は、順次追加



常時リスク診断・対処（CRSA）のシステム構成概要



常時リスク診断・対処（CRSA）の目的と効果

① 政府機関統一基準等に準拠したコントロール（管理策）からの逸脱の迅速な把握と是正対応

CRSAシステムは、サイバーセキュリティ対策に必要なコントロールの実施状況を継続的にモニタリングできるため、どこが不適切な状態になっているかを迅速に把握し、是正対応を実施できる。

② インシデント発生時のトリアージ等の効果的な対応

CRSAシステムは、リアルタイムに自組織の資産状況、脆弱性対応状況等を把握できるため、インシデント発生時の資産等への影響規模や対応の優先度について迅速に判断できる。

③ リアルタイムデータによるセキュリティ対策実施状況の効率的な報告

CRSAシステムを導入した組織は、リアルタイムな資産状態、アカウントの利用状況、インシデントの発生状況などを把握できる。これにより、サイバーセキュリティ対策状況を客観的かつ効率的に報告できるようになる。政府全体としては、各組織のサイバーセキュリティ対策状況を各組織に負担をかけることなく効率的に把握できるようになる。

④ 脅威やインシデントに対する政府横断的な脆弱箇所の迅速な発見と是正対応

CRSAシステムは、特定の脅威情報やインシデントに関する情報をもとに、影響のある箇所やインシデントの発生する可能性のある箇所を政府横断的に特定できるため、迅速かつ効果的に対処できる。

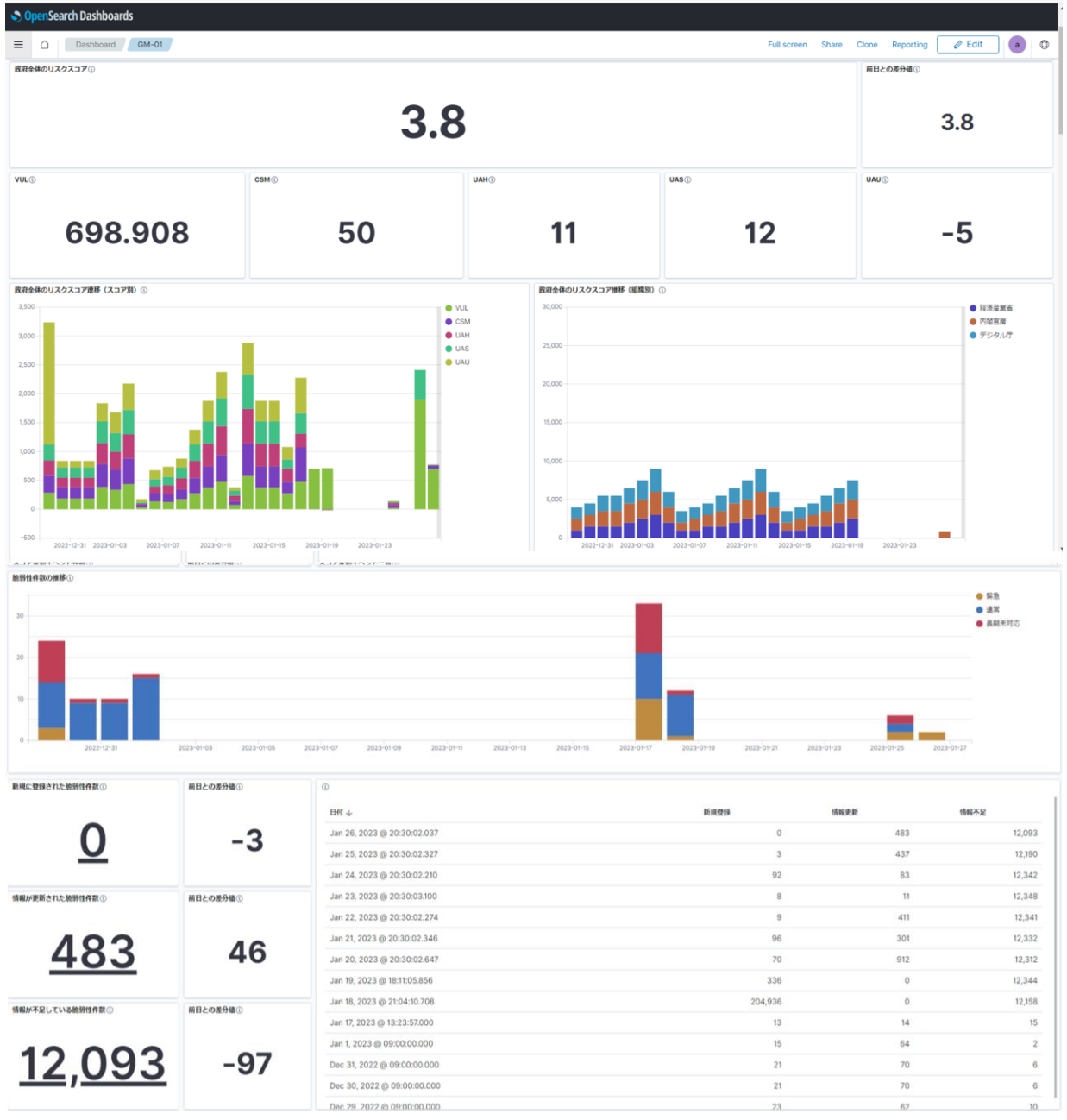
⑤ ゼロトラストアーキテクチャの運用環境を適切に維持

ゼロトラストアーキテクチャの具体的な実装・運用においては、ネットワーク上の各デバイスでの脆弱性対応状況等を把握することにより、システム全体の健全性を把握し、維持していく必要がある。CRSAシステムにおける診断結果は、ゼロトラストアーキテクチャにおけるポリシーエンジンのインプット情報としても活用していく。

リスクスコア候補とGSOダッシュボード（検討中）

- リスクスコアの候補を整理し、適用の検討中
- ダッシュボードについても検討中

CDM	対象領域 CRSA	スコア名称	評価項目	スコア概要
Area 1	端末とサーバ装置等の管理	VUL	ソフトウェア脆弱性の対応状況	デバイスにおける未対応の脆弱性をスコア化
		CSM	構成の規定準拠状況	ソフトウェアにおける構成誤りについてスコア化
		UAH	デバイスの管理状況	未承認（非管理）デバイスの存在をスコア化
		UAS	ソフトウェアの管理状況	未承認ソフトウェアの存在をスコア化
		USS	ソフトウェアの署名状況	未署名ソフトウェアの存在をスコア化
Area 2	認証・認可・特権の管理	UAU	ユーザの管理状況	未承認（非管理）ユーザの存在をスコア化
		PPS	パスワードの管理状況	パスワード強度が低いアカウントの存在をスコア化
Area 3	情報システムのライフサイクル管理	*LSS*	ログ管理の状況	不適切なログの保管状況をスコア化
		EVT	不正アクセス等の発生状況	セキュリティアラートの発生状況をスコア化
Area 4	データの保全管理	*NPF*	情報の保護状況	要保護情報が適切に保護されていない状況をスコア化
		ETS	データ暗号化の状況	暗号化されていないデータの存在をスコア化



デジタル庁

Digital Agency