

デジタル庁の行うサイバーセキュリティ対策

～重要基盤システムの構築運用を担う Government as a Service として、強靱なデジタル基盤を構築・運用～

○ デジタル社会の基盤となるデジタル庁システム・ネットワークのセキュアな構築と運用確保

（デジタル庁システムの意義）

- ・ 各府省が共通で利用するシステム
- ・ 各府省が情報システムを整備する上で基盤となるシステム
- ・ 他の情報システムとの連携によりセキュリティ面や業務効率性に効果がある情報システム
- ・ 緊急性が高く、かつ、政策的に重要なものとしてデジタル庁が整備・運用すべき情報システム

（デジタル庁システムの例）

- ・ ガバメント・クラウド
- ・ ガバメント・ソリューション・サービス（GSS）
- ・ 政府機関用ネットワーク（G-Net）
- ・ ID/認証などのトラスト基盤
- ・ 構築・運用・監視に加え、ポリシーの策定と運用、情報の収集・分析・共有、リスク評価、脆弱性チェック、教育・演習・訓練、検証・監査、インシデント対応（CSIRT業務）等を実施。

○ 政府全体のシステムのセキュリティ確保への支援

- 「デジタル社会の実現に向けた重点計画」（2022年6月閣議決定）では「サイバーセキュリティ等の安全・安心の確保」を規定。
- 「情報システムの整備及び管理の基本的な方針」（2021年12月デジタル大臣決定）において「政府情報システムの管理等に係るサイバーセキュリティについての基本的な方針」を策定
- 情報システムのセキュリティ確保のための各種ガイドライン等の作成・メンテナンス
（例：セキュリティ・バイ・デザイン、ゼロトラスト導入、脆弱性診断等）
- セキュリティ確保のための研究
（例：常時診断・対応型のセキュリティアーキテクチャ（CRSA）について検証中）
- セキュリティの担保されたシステムの導入支援
（例：クラウドサービスについての認定制度であるISMAPを関係府省と連携して推進）

デジタル庁設立1年の活動報告 (2022年9月1日)

設立1年の総括 | サービス提供

公共サービスの提供とインフラ整備を推進

“Government as a Startup” “Government as a Service”

1 生活者、事業者、職員に やさしい公共サービスの提供

- ・マイナンバーカードの普及
- ・マイナポータルの改善
- ・新型コロナワクチン接種証明書アプリの提供
- ・事業者向けサービス・認証基盤の提供
- ・府省庁向けオンライン行政サービス
- ・キャッシュレス法の成立
- ・地方自治体のシステム標準化の推進

2 デジタル基盤の整備による 成長戦略の推進

- ・デジタル臨時行政調査会の推進
- ・データ戦略
- ・医療DXの推進
- ・教育分野のデジタル化
- ・こどものデータ基盤整備
- ・デジタルインボイスの普及定着
- ・デジタル田園都市国家構想の推進
- ・デジタル改革共創プラットフォームの活用
- ・デジタルの日の実施

3 安全安心で強靱な デジタル基盤の実現

- ・ガバメントクラウドの整備
- ・ガバメントソリューションサービス
- ・DFFTの推進

デジタル社会の実現に向けた重点計画の概要（2022年6月版）

- デジタル社会の形成のために政府が迅速かつ重点的に実施すべき施策等を定めるもの。（デジタル社会形成基本法37②等）
- デジタル社会の実現の司令塔であるデジタル庁のみならず各省庁の取組も含め工程表などスケジュールとあわせて明らかにするもの。

我が国が目指すデジタル社会「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」

デジタル社会で
目指す6つの姿

※進捗把握指標の設定

① デジタル化による成長戦略

④ 誰一人取り残されないデジタル社会

② 医療・教育・防災・こども等の準公共分野のデジタル化

⑤ デジタル人材の育成・確保

③ デジタル化による地域の活性化

⑥ DFFTの推進を始めとする国際戦略

→Data Free Flow with Trust

具体策を考える上で前提となる理念・原則

誰一人取り残されないデジタル社会の実現 ※デジタル推進委員の全国展開
→誰もが、いつでも、どこでもデジタルの恩恵を享受

デジタル社会形成のための基本原則

→10原則（デジタル改革基本方針）

①オープン・透明②公平・倫理③安全・安心④継続・安定・強靱⑤社会課題の解決⑥迅速・柔軟⑦包摂・多様性⑧浸透⑨新たな価値の創造⑩飛躍・国際貢献

BPRと規制改革の必要性

→Business Process Reengineering

→デジタル3原則（国の行政手続オンライン化原則）
デジタルファースト/
ワンズオンリー/
コネクテッド・ワンストップ

クラウド・バイ・デフォルト原則

目指す姿を実現する上で有効な戦略的な取組（基本戦略）

デジタル臨時行政調査会

デジタル・規制・行政改革に通底する構造改革のためのデジタル原則※に沿って4万以上の法令等の適合を目指す

デジタル田園都市国家構想実現会議

デジタル原則の遵守やデータ基盤の活用等を前提に、各地域の社会的課題の解決などに向けて様々な取組を支援

国際戦略の推進

DFFT/諸外国デジタル政策関連機関との連携強化

サイバーセキュリティ等の安全・安心の確保

国際情勢の変化等へ対応/国家安全保障上のリスクへの対応としてのサイバーセキュリティの確保/個人情報保護

包括的データ戦略の推進 ※トラスト基盤構築を推進

トラスト/ベース・レジストリ/オープンデータ

デジタル産業の育成

クラウドサービス産業・ITスタートアップの育成

Web3.0の推進

ブロックチェーン技術を基盤とするNFTの利用等の環境整備

※①デジタル完結・自動化原則 ②アジャイルガバナンス原則 ③官民連携原則 ④相互運用性確保原則
⑤共通基盤利用原則

デジタル社会の実現に向けた基本的な施策

国民に対する行政サービスのデジタル化

- ・ 国・地方公共団体・民間を通じたトータルデザイン（アーキテクチャの将来像整理）
- ・ 新型コロナウイルス感染症対策など緊急時の行政サービスのデジタル化（ワクチン接種証明書のスマホ搭載の推進/公金受取口座登録推進及び行政機関による利用）
- ・ マイナンバー制度の利活用の推進（情報連携の拡大/各種免許等のデジタル化）
- ・ マイナンバーカードの普及及び利用の推進（オンライン市役所サービス/市民カード化/民間利用推進/健康保険証利用/運転免許証と一体化/市町村や業界に働きかけ）
- ・ 公共フロントサービスの提供等（ワンストップサービスの推進）

暮らしのデジタル化

- ・ 準公共分野のデジタル化の推進等（健康・医療・介護（PHR/オンライン診療）/
→ Personal Health Record
教育（校務のデジタル化/教育データ利活用）/
防災/こども/モビリティ/取引）

産業のデジタル化

- ・ 事業者向け行政サービスの質の向上に向けた取組（電子署名/電子委任状/商業登記電子証明書/
GビズID/e-Gov）
- ・ 中小企業のデジタル化の支援（IT専門家派遣/
IT導入補助金/サイバーセキュリティ対策支援）
- ・ 産業全体のデジタルトランスフォーメーション（DX認定制度/DX銘柄/DX投資促進税制/
サイバーセキュリティ強化）

デジタル社会を支えるシステム・技術

- ・ 国の情報システムの刷新（重要システム開発体制整備/ガバメントクラウドの整備/ネットワークの整備/政府調達）
- ・ 地方の情報システムの刷新（標準化基本方針の策定等）
- ・ デジタル化を支えるインフラの整備（光ファイバ/5G/半導体/データセンター/海底ケーブル）
- ・ デジタル社会に必要な技術の研究開発・実証の推進（情報通信・コンピューティング・セキュリティ技術高度化/スーパーコンピュータ整備）

デジタル社会のライフスタイル・人材

- ・ ポストコロナも見据えた新たなライフスタイルへの転換（テレワーク/シェアエコ）
- ・ デジタル人材の育成・確保（プログラミング必修化/リカレント教育/女性人材）

今後の推進体制（政府のデジタル改革推進体制強化）

サイバーセキュリティ等の安全・安心の確保

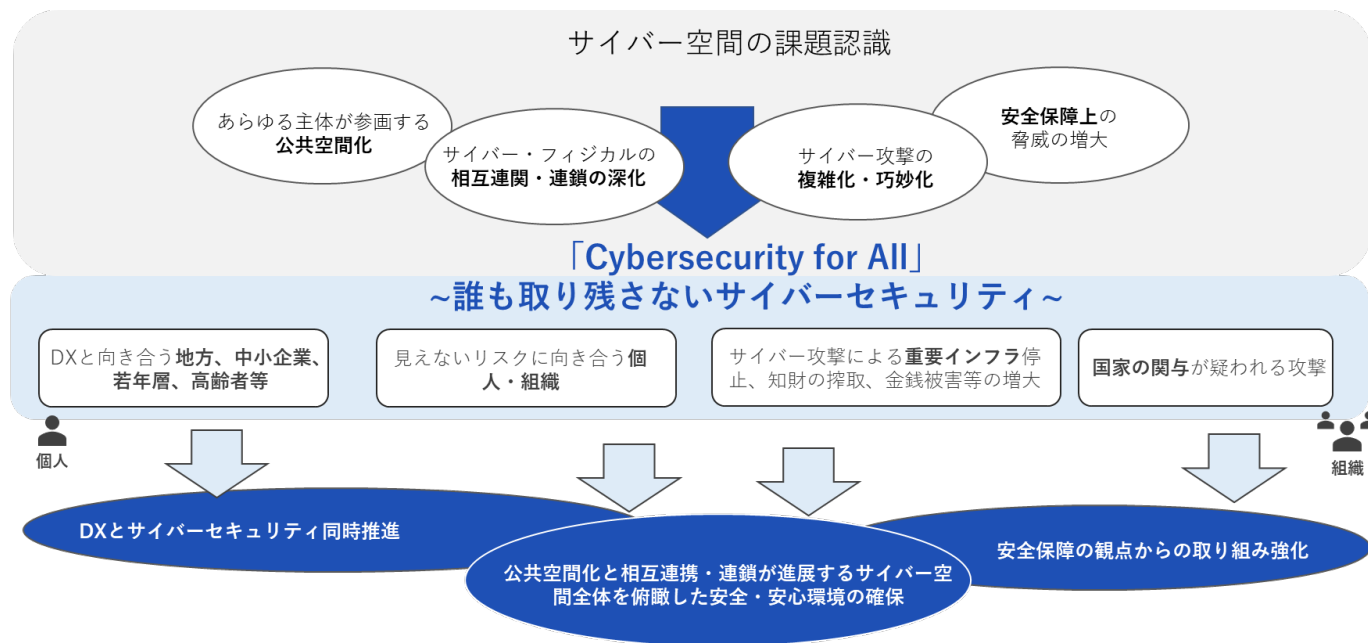
- 【目指す姿】

- 利便性の向上とサイバーセキュリティの確保を両立させる。そのため、クラウドサービスの利用拡大とともに、常時診断・対応型セキュリティアーキテクチャの実装を見据えた対応等を進めていく。政府の情報システム整備における、サイバーセキュリティについての基本的な方針を示し、この方針等に基づいて、サイバーセキュリティ対策の強化を図っていく。
- あわせて、個人情報の保護について、改正法の周知を始め制度の情報提供に積極的に取り組んでいく。さらに、情報通信技術を用いた犯罪の防止や、高度情報通信ネットワークの災害対策に引き続き取り組むことにより、安全・安心なデジタル社会の構築を図る。
- 国家安全保障上の課題へと発展していく可能性のある国際情勢の変化や世界規模の感染症の蔓延(まん)延など、デジタル社会を取り巻く環境は目まぐるしく変化しており、今後とも変化し得るものである。また、大規模地震災害を始めとする自然災害により、国民の生命・身体・財産に重大な被害が生じ、又は生ずるおそれがある事態を想定して、あらかじめデジタル社会の強靱(じん)性を確保しておくことも課題となっている。こうした状況への対応として、国民の生命や財産を守り、国民生活を維持することのできる安全・安心なデジタル社会を構築するため、官民の緊密な連携を図りつつ、次のような取組を推進する。

デジタル社会の実現に向けた重点計画（「安全・安心の確保」関係） （2022年6月）

「利便性とサイバーセキュリティの確保」を目指す姿とする。

目指す姿の実現に向けて基本方針を示し、この方針に基づいたサイバーセキュリティ対策の強化を図る。



基本方針の提示

- 政府情報システムの整備・運用

セキュリティ・バイ・デザイン、DevSecOpsを含めたセキュリティ対策の実施

安定的・継続的な稼働の確保等の観点から検証・監査の実施体制の構築

- デジタル庁システム
- デジタル庁・各府省共同のシステム

レジリエンスの向上を目的としたリアルタイムな監視と順守状況の確認

- インシデントの早期発見
- 被害の最小化
- 回復の迅速化
- リソース確保
- ルール・体制の構築

高度セキュリティ技術の研究開発

情報管理手法やシステムの挙動・ソフトウェアの状況をリアルタイムに監視するための常時診断・対応型のアーキテクチャ

政府情報システムの管理等に係る サイバーセキュリティについての基本的な方針

- 政府情報システムのサイバーセキュリティ対策については、全ての政府機関等において共通的に必要とされるセキュリティ対策である統一基準群を前提のものとして引き続き実施、推進しつつ、デジタル庁の整備する情報システム（整備をデジタル庁が各府省と共同で推進し、運用を各府省が担当する情報システムを含む。）の対策については以下の基本的な方針に従って整備を進めるとともに、デジタル庁は、NISC と連携してこれらを実践するための参考となるガイドラインや技術レポート等の策定を検討する。また、デジタル庁以外の府省が整備・運用する情報システムについても、この基本的な方針や前述のガイドライン等を参考にしつつ、必要な対策に取り組むものとする。
- 1. 共通機能等を前提とした常時診断・対応型のセキュリティアーキテクチャの実装の推進
- 2. サイバーレジリエンスを高めるためのセキュリティ対策の導入
- 3. セキュリティポリシー及びセキュリティ対策の構造化及び追跡性の確保

セキュリティ関連技術ガイドライン群と各ドキュメントにおける概要

https://www.digital.go.jp/resources/standard_guidelines/

統一基準群で示されるセキュリティ対策に係る基本的な考え方と実践のポイントをふまえ、下記の4テーマについて統一基準群を具体化した技術ガイダンスを策定。Informativeな文書として位置づける。なお、将来的には内容を改訂し、各府省庁への適用することを視野にしている。

ゼロトラストアーキテクチャ適用方針

informative

概要

政府機関では業務環境の変化に伴い、イントラネットの外側で情報システムを利用するケースが増大している。このような従来の境界型のセキュリティモデルとは前提が異なる環境で、情報セキュリティを確保するためには、境界型のセキュリティから大幅に拡張した考え方が求められる。本書は拡張の実態となる「ゼロトラストアーキテクチャ」の適用方針を説明する。

常時リスク診断・対処(CRSA)システムアーキテクチャ

informative

概要

ゼロトラストの環境下において安定かつ安全なサービス提供を実現するためには、政府全体のサイバーセキュリティリスクを早期に検知し、これを低減することが必要となる。本書は、この活動を継続的に実施するための、情報収集・分析を目的としたプラットフォームのアーキテクチャについて説明する。

政府情報システムのセキュリティ・バイ・デザインガイドライン

informative

概要

情報システムに対し効率的にセキュリティを確保するため、企画から運用まで一貫したセキュリティ対策を実施する「セキュリティ・バイ・デザイン」の必要性が高まっている。本書ではシステムライフサイクルにおけるセキュリティ対策を俯瞰的に捉えるため、各工程での実施内容を記載すると共に関係者の役割についても定義する。

政府情報システムにおける脆弱性診断ガイドライン

informative

概要

政府機関では従来においても情報セキュリティリスクの低減を目的として脆弱性診断を活用してきたが、導入方法に係る明確な基準や指針は十分整備されていない。本書は、政府情報システムの関係者が最適な脆弱性診断を選定、調達できるようにするための基準及び指針を提供する。

