National center of Incident readiness and Strategy for Cybersecurity

SBDマニュアル

～活用事例の紹介～

2015年5月21日

内閣サイバーセキュリティセンター(NISC)

活用例

①行政情報提供システム
（行政情報（機密性１）をウェブページに公開）

②国民参加型政策立案システム
（国民からインターネットで意見を公募）

③電子申請・届出システム
（インターネットを介して国民からの各種申請・届出手続きを処理）

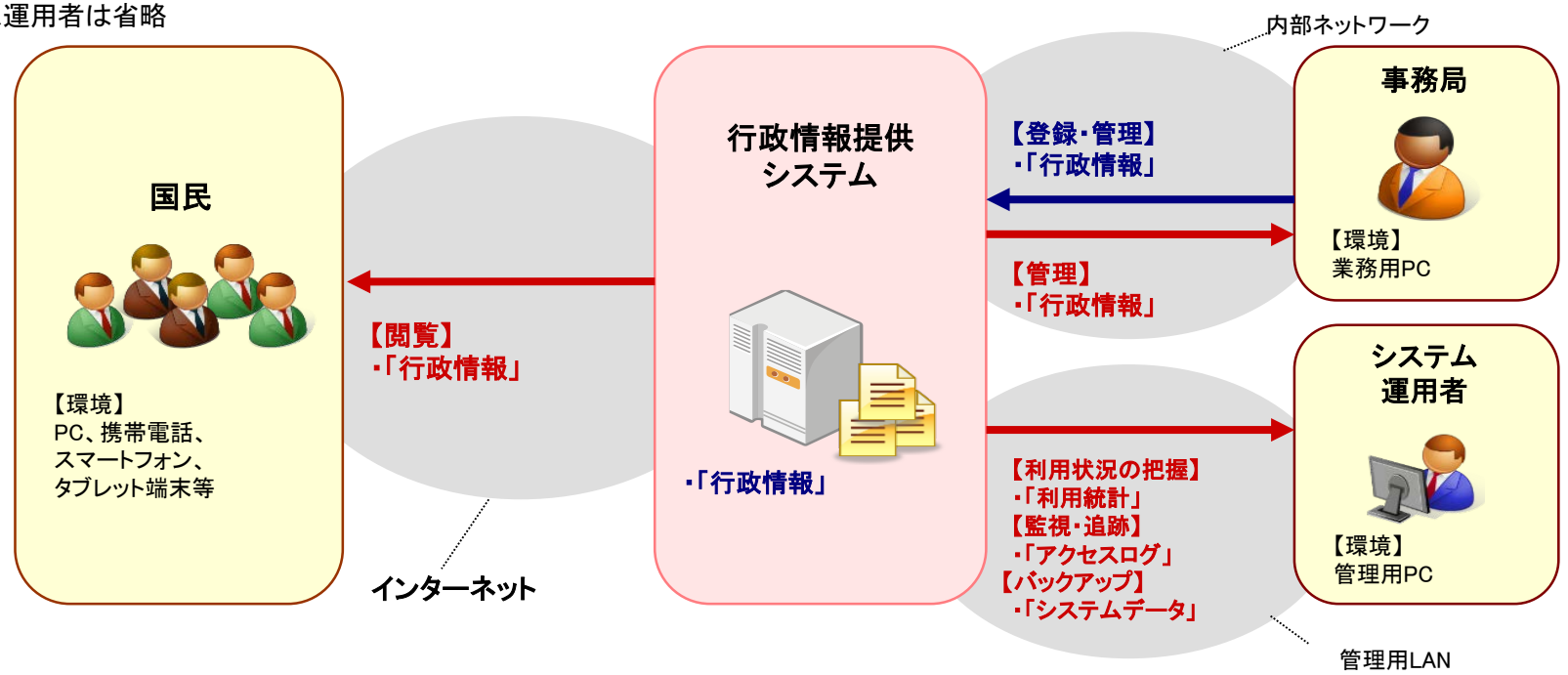
④省内イントラネットシステム（省内掲示板システム）
（機密性の高くない情報を省内限定で利用）

活用例①行政情報提供システム：ステップ1～4

- **行政情報（機密性1）をウェブページに公開する、一般的な行政情報提供のためのWEBページシステムを想定する。**

主体	業務	業務（細分化後）の概要	情報	利用環境・手段
国民	行政情報の閲覧	行政情報を表示し、内容を確認する。	「行政情報」	インターネット、PC、携帯電話、スマートフォン、タブレット端末
事務局	行政情報の登録	サーバにコンテンツ（行政情報）を登録する。	「行政情報」	内部ネットワーク、業務用PC
		サーバに登録済みのコンテンツ（行政情報）を更新及び削除する。	「行政情報」	

※システム運用者は省略



活用例①行政情報提供システム：ステップ5　判断条件による検討

- **整理した業務要件や判断条件の解説等を参考に、6つの設問に「○」「×」の二択で回答する**

名称	観点分類	判断条件	判断結果	判断結果の解説
A. 外部アクセスの有無	利用環境・手段	インターネット等の通信回線を介して（情報の管理ポリシが異なる）外部から情報システムにアクセスしてサービスの利用、業務の遂行、情報システムの管理等を行うか。	○	インターネットを介して情報システムにアクセスされる
B. 情報の重要度	情報	漏えいした場合や正常にアクセスできない場合に、深刻な損害を被る可能性がある重要性の高い情報を取り扱うか。	×	扱う情報は公開情報（機密性1）であり、重要性の高い情報は取り扱わない
C. 情報保存時の安全性	情報	入退室管理等の物理対策だけでなく、情報システムが保存する情報についてより一層の安全を期すために追加的対策をさらに行うべきと考えるか。	×	情報の重要性は低く、サーバ上での保存のみ（モバイルPCによる情報処理等なし）のため、不要
D. 利用者の限定要否	主体	情報システムにアクセスする主体は、利用資格のある者、職員、グループのメンバー等の特定の者に限定されるか。	×	システムへアクセスする利用者（国民）※は特定の者に限定されない
E. アカウントの多様性	主体	利用者によって利用可能なサービスや業務が異なる等、利用者の特徴にバリエーションがあるか。	×	想定されない
F. 複数部局による利用	主体	情報の取り扱い方や利用目的等が異なる複数の部局等の間で共用されるか。	×	想定されない

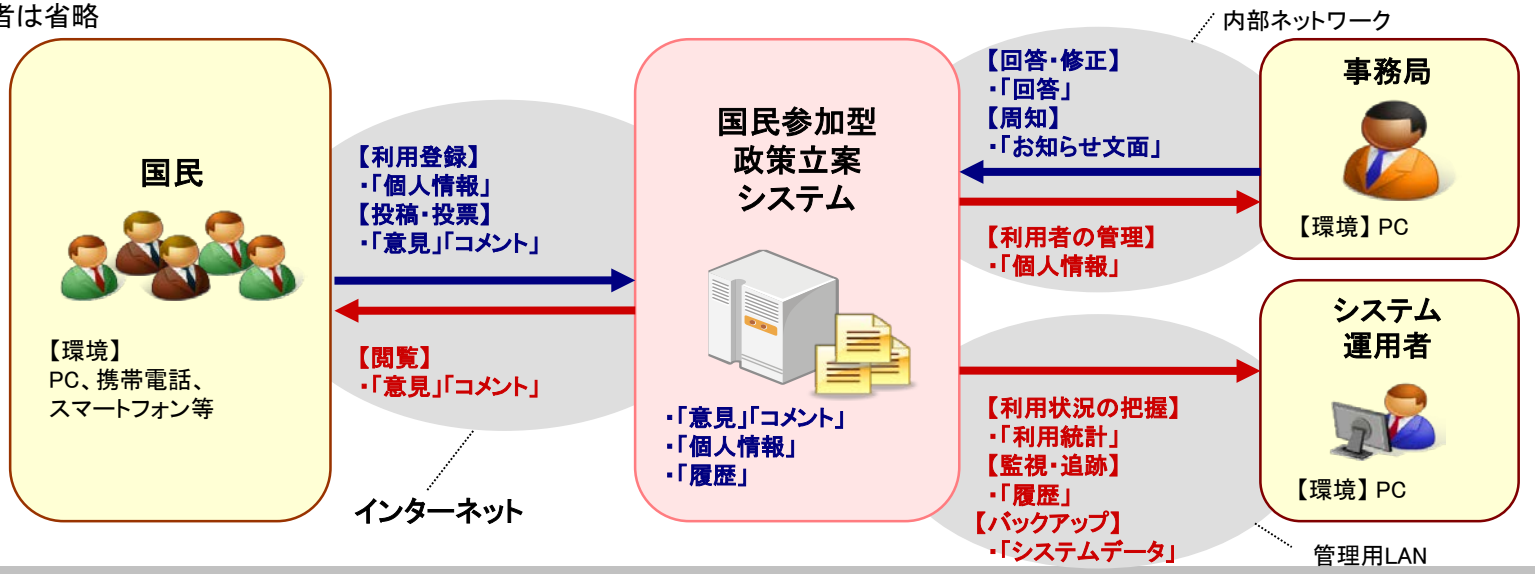
※管理者は除く
（管理者権限の保護対策は必ず要件に含まれる）

活用例②国民参加型政策立案システム　ステップ1～4

- 国民からインターネットで政策に関する意見を公募するような、国民参加型政策立案システムを想定する。

主体	業務	業務（細分化後）の概要	情報	利用環境・手段
国民	政策に関する意見・コメントの投稿	個人情報を登録して、サービスの利用資格を得る。	「個人情報」（氏名、ニックネーム、性別、年齢、職種、連絡先等）	PC、携帯電話、スマートフォン、インターネット
		新規の意見や他者の意見に対するコメントの投稿及び投票を行う。	「意見」「コメント」（タイトル、本文、投稿者名、投稿日時等）	
		意見やコメントを検索し、閲覧する。	「意見」「コメント」（タイトル、本文、投稿者名、投稿日時等）	
事務局	政策に関する情報提供及び利用者の管理	意見に対する事務局回答の投稿及び不適切な意見の削除を行う。	「回答」（本文、投稿者名、投稿日時等）	PC、内部ネットワーク
		サービス停止や注意事項等の利用者に対する周知を行う。	「お知らせ文面」	
		利用者の登録情報の確認、修正、等の管理業務を行う。	「個人情報」（氏名、ニックネーム、性別、年齢、職種、連絡先等）	

※システム運用者は省略



活用例②国民参加型政策立案システム：ステップ5　判断条件による検討

- **整理した業務要件や判断条件の解説等を参考に、6つの設問に「○」「×」の二択で回答する**

名称	観点分類	判断条件	判断結果	判断結果の解説
A. 外部アクセスの有無	利用環境・手段	インターネット等の通信回線を介して（情報の管理ポリシが異なる）外部から情報システムにアクセスしてサービスの利用、業務の遂行、情報システムの管理等を行うか。	○	インターネットを介して情報システムにアクセスされる
B. 情報の重要度	情報	漏えいした場合や正常にアクセスできない場合に、深刻な損害を被る可能性がある重要性の高い情報を取り扱うか。	○	個人情報（匿名性あり）等を取り扱う
C. 情報保存時の安全性	情報	入退室管理等の物理対策だけでなく、情報システムが保存する情報についてより一層の安全を期すために追加的対策をさらに行うべきと考えるか。	×	サーバ上での保存のみ（モバイルPCによる情報処理等なし）のため、不要
D. 利用者の限定要否	主体	情報システムにアクセスする主体は、利用資格のある者、職員、グループのメンバー等の特定の者に限定されるか。	○	IDを発行した（利用資格のある）国民に限定
E. アカウントの多様性	主体	利用者によって利用可能なサービスや業務が異なる等、利用者の特徴にバリエーションがあるか。	×	想定されない
F. 複数部局による利用	主体	情報の取り扱い方や利用目的等が異なる複数の部局等の間で共用されるか。	×	想定されない

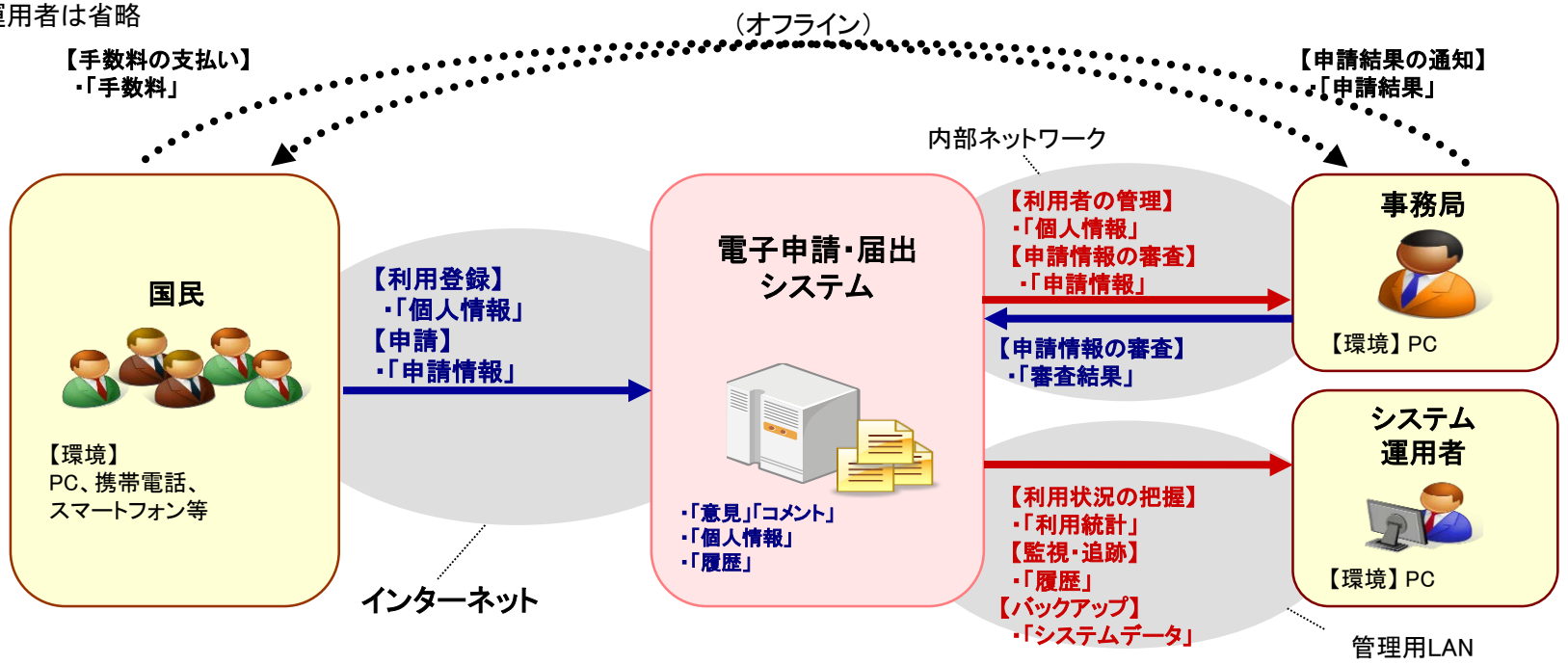
※管理者は除く
（管理者権限の保護対策は必ず要件に含まれる）

活用例③電子申請・届出システム　ステップ1～4

- インターネットを介して国民からの各種申請・届出手続きの処理を行う、電子申請・届出システムを想定する。

主体	業務	業務（細分化後）の概要	情報	利用環境・手段
国民	申請を行う	個人情報を登録して、サービス利用資格を得る	「個人情報」	PC、携帯電話、スマートフォン、インターネット
		申請情報を入力して提出する	「申請情報」	
		申請等に必要な手数料を支払う	「手数料」	オフラインでの実施
事務局	申請	システムの利用者を追加、修正、削除する	「個人情報」	PC、内部ネットワーク
		申請情報の正当性を確認して審査を行う	「申請情報」 「審査結果」	
		申請に応じた事務処理を行い、結果を通知する	「申請結果」	オフラインでの実施

※システム運用者は省略



活用例③電子申請・届出システム：ステップ5　判断条件による検討

- **整理した業務要件や判断条件の解説等を参考に、6つの設問に「○」「×」の二択で回答する**

名称	観点分類	判断条件	判断結果	判断結果の解説
A. 外部アクセスの有無	利用環境・手段	インターネット等の通信回線を介して（情報の管理ポリシが異なる）外部から情報システムにアクセスしてサービスの利用、業務の遂行、情報システムの管理等を行うか。	○	インターネットを介して情報システムにアクセスされる
B. 情報の重要度	情報	漏えいした場合や正常にアクセスできない場合に、深刻な損害を被る可能性がある重要性の高い情報を取り扱うか。	○	重要性の高い情報（申請情報や個人情報）を取り扱う
C. 情報保存時の安全性	情報	入退室管理等の物理対策だけでなく、情報システムが保存する情報についてより一層の安全を期すために追加的対策をさらに行うべきと考えるか。	○	申請情報や個人情報（匿名性なし）を取り扱うため、追加的対策を行う
D. 利用者の限定要否	主体	情報システムにアクセスする主体は、利用資格のある者、職員、グループのメンバー等の特定の者に限定されるか。	○	IDを発行した（利用資格のある）国民に限定
E. アカウントの多様性	主体	利用者によって利用可能なサービスや業務が異なる等、利用者の特徴にバリエーションがあるか。	×	想定されない
F. 複数部局による利用	主体	情報の取り扱い方や利用目的等が異なる複数の部局等の間で共用されるか。	×	想定されない

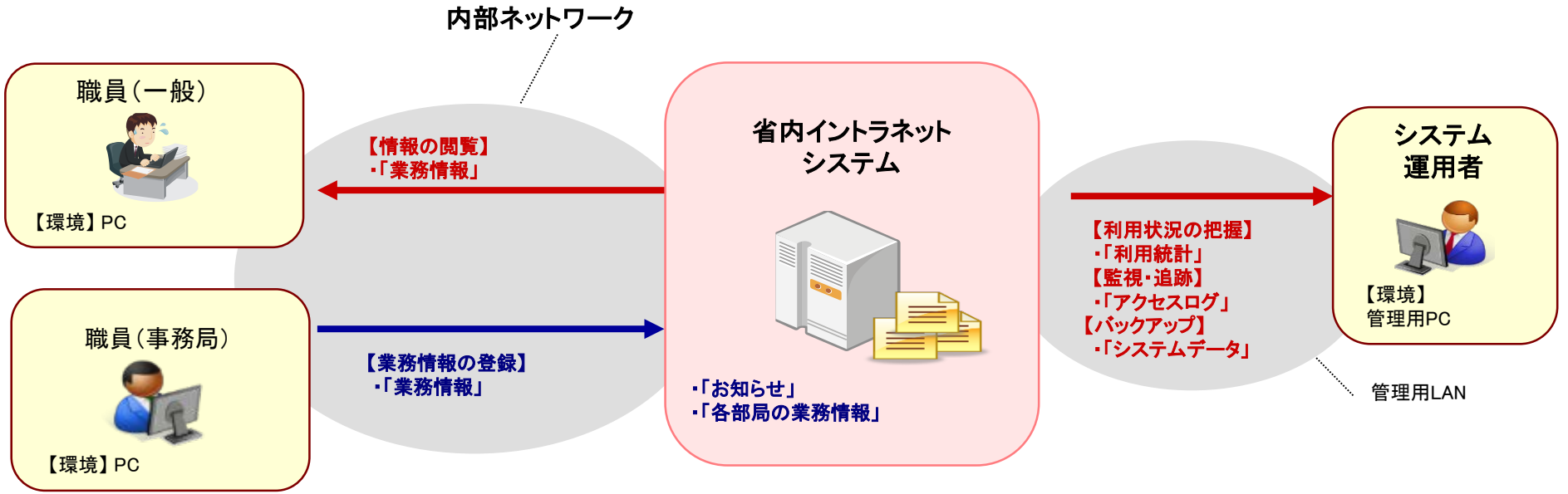
※管理者は除く
（管理者権限の保護対策は必ず要件に含まれる）

活用例④省内イントラネットシステム（省内掲示板システム）

- 機密性の高くない情報を省内限定で周知・閲覧するための、省内イントラネットシステム（掲示板システム）を想定する。

主体	業務	業務（細分化後）の概要	情報	利用環境・手段
職員（一般）	情報を閲覧する	イントラネットに掲載された情報を閲覧し、必要に応じダウンロードする	「業務情報」	PC
職員（事務局）	情報を登録する	各部局からのお知らせや規程、業務情報等をイントラネットに登録する	「業務情報」	PC

※システム運用者は省略



活用例④省内イントラネットシステム：ステップ5　判断条件による検討

- **整理した業務要件や判断条件の解説等を参考に、6つの設問に「○」「×」の二択で回答する**

名称	観点分類	判断条件	判断結果	判断結果の解説
A. 外部アクセスの有無	利用環境・手段	インターネット等の通信回線を介して（情報の管理ポリシが異なる）外部から情報システムにアクセスしてサービスの利用、業務の遂行、情報システムの管理等を行うか。	×	インターネットや自省以外の外部から情報システムにアクセスすることはない
B. 情報の重要度	情報	漏えいした場合や正常にアクセスできない場合に、深刻な損害を被る可能性がある重要性の高い情報を取り扱うか。	×	取り扱う情報の重要性は高くない
C. 情報保存時の安全性	情報	入退室管理等の物理対策だけでなく、情報システムが保存する情報についてより一層の安全を期すために追加的対策をさらに行うべきと考えるか。	×	保存する情報の重要性は高くない
D. 利用者の限定要否	主体	情報システムにアクセスする主体は、利用資格のある者、職員、グループのメンバー等の特定の者に限定されるか。	×	職員は誰でもアクセス可能（ID等の利用資格の制限なし）
E. アカウントの多様性	主体	利用者によって利用可能なサービスや業務が異なる等、利用者の特徴にバリエーションがあるか。	×	想定されない
F. 複数部局による利用	主体	情報の取り扱い方や利用目的等が異なる複数の部局等の間で共用されるか。	×	想定されない

※管理者は除く
（管理者権限の保護対策は必ず要件に含まれる）

留意事項

- 本資料はあくまでも事例であり、各情報システムの構成、設置環境、運用保守条件等を勘案した上で、各省においてSBDマニュアル（ワークシート）を利用して実施してください。各情報システムの業務特性・性質を考えた上で、セキュリティ要件を策定することが重要です。