（別紙 1）

2022 年度産業保安システム更改に係る

要件定義書

令和 5 年 1 月

経済産業省産業保安グループ

産業保安企画室

目次

用語集

用語	定義
保安ネット	産業保安・製品安全関連法令に係る諸手続の電子申請システムを指す。 令和２年１月より運用を開始しているシステムを「現行保安ネット」とする。 本要件定義書の対象であり、令和 6 年 4 月の運用開始を予定しているシステムを「次期保安ネット」とする。
保安ネットポータル	産業保安・製品安全関連法令に関する申請手続を窓口まで行かなくても、オンラインで記入・申請・審査状況の確認、交付される通知文書の確認が行えるシステムを指す。 なお、地方自治体向け保安ネットにおけるポータルについても同様の呼称とする。
法令	電気、製品安全、液化石油ガス、火薬、鉱山、ガス、熱供給分野の各法令に係る該当手続及びマスタに対し、行政機関が設けた規則や省令を指す。
手続	届出：行政庁に対し、(申請に該当するものを除いた)一定の事項の通知をする行為を指す。 申請：法令に基づき、行政庁の許可、認可、免許その他自己に対し、何らか利益を付与する処分を求める行為を指す。
様式	管轄の行政機関に対し、届出並びに申請書類を提出する際のフォーマットを指す。
業務フロー	保安ネット上で行う業務プロセスの可視化、明文化を図ることを目的として、用いるフロー図を指す。
審査フロー	審査者が手続を審査する一連のプロセスの可視化、明文化を図ることを目的として、用いるフロー図を指す。
汎用申請機能	本申請機能と比べて一定の機能制約があるものの、より簡易に手続のオンライン化を実現する機能を指す。 画面レイアウトや審査プロセスを設定シート(エクセル等)にて定義を行い、保安ネットへ読み込ませることで、ノーコードで手続の受付・審査等に係る画面・機能・データを保安ネットへ具備する機能である。
簡易申請機能	申請書を添付する形で提出することができる簡易な申請機能を指す。
集中入力センター	産業保安監督部/経済産業局の依頼を受けて、申請者より紙の様式で提出された手続内容を、保安ネットに入力する組織。
Ｇビズ ID	デジタル庁が整備・運用を行っている、法人・個人事業主向け共通認証システムである。
gBizINFO	経済産業省が整備・運用を行っている、国内法人情報を集約しているデータベースである。
ガバメントクラウド	デジタル庁が整備・運用する政府共通のクラウドサービスの利用環境であり、マルチクラウドサービスに対応するものである。
GIMA	Government Identity Management for Authentication の略称を指す。 デジタル庁が整備・運用しているシステムであり、政府職員の ID(ユニバーサル ID)を統合管理し、府省共通業務アプリケーション及び個別業務アプリケーションに対し、利用者認証情報・機能を一元的に提供するための基盤である。
GSS	ガバメントソリューションサービス(GSS)の略称を指す。 デジタル庁が整備・運用するゼロトラストを基礎とした、政府共通の標準的な業務実施環境(パーソナルコンピュータやネットワーク環境)である。
政府共通 NW	デジタル庁が整備・運用する政府機関等(地方自治体含む)のＬＡＮを相互に接続する、政府内専用の通信ネットワークシステムである。 なお、地方自治体間の相互接続ネットワークである LGWAN(総合行政ネットワーク)と相互接続可能である。
LGWAN	Local Government Wide Area Network の略称を指す。 地方公共団体の組織内ネットワーク(「庁内 LAN」)を相互に接続し、地方自治体間のコミュニケーションの円滑化、情報の共有による情報の高度利用を図ることを目的とした高度なセキュリティを維持した行政専用ネットワークである。

用語	定義
電子決裁システム(EASY)	府省共通で利用される、行政文書ファイルの管理(受付、起案・決裁/供覧、登録・保存)を行うシステムである。一元的文書管理システムの後継として、経済産業省では 2022 年 12 月から利用されている。
GPKI 電子署名サーバ	デジタル庁が整備・運用する政府認証基盤(GPKI)において電子決裁システム(EASY)に格納する公文書に対してリモート署名を行うためのシステムを指す(現在は企画段階であり未整備。)。
マイナポータル	デジタル庁が整備・運用する行政手続のオンライン窓口(ポータル)サービスで、オンライン申請のほか、行政機関等が保有する利用者情報の確認等のサービスを提供している。
e-Gov(REPS 連携基盤)	e-Gov とはデジタル庁が整備・運用する、政府全体の法人及び個人事業者等向けの行政手続のポータルサイトであり、ほかに法令検索やパブリックコメント募集等の機能を有する。 e-Gov(REPS 連携基盤)とは、e-Gov の機能を拡張し行政手続の一部種類である手数料の納付及び登録免許税の納付をオンライン(キャッシュレス)で可能とするため、令和６年度に当該機能の整備が予定されている基盤である。

第1章 はじめに

1. 背景

経済産業省では、産業保安及び製品安全の維持・向上のため、電気事業法、鉱山保安法、ガス事業法、液化石油ガス保安法[1]、製品安全４法[2]等に基づく許認可・承認・届出等の年間約 27 万件の手続業務を実施している。従前では紙を主体とした行政手続が行われていたため、産業保安監督部等の審査業務の煩雑化、事業者の申請・届出手続に係るコスト増大にもつながっていた。そこで、産業保安の強化に資することを目的として、産業保安・製品安全関連法令に係る諸手続の電子申請システム(以下、保安ネットと言う。)を構築し、令和２年１月から運用を開始している。

現在、保安ネットを用いて、電気、LP ガス、都市ガス等の産業保安法令及び製品安全法令に基づく年間約 27 万件の申請手続のうち、約 17 万件が電子申請で行われている。他方、保安ネットでは、これまで申請件数の多い申請・届出を中心に電子化を進めており、法令に基づく全ての申請・届出手続きを網羅的に電子化するに至っていない。さらに、都道府県等に事務委任している行政手続もあり、保安ネットにおいて電子化対象手続を拡張することで事業者・行政機関双方の大幅な業務の効率化・合理化が図られることも期待される。

また、事業者情報・事故情報等のビッグデータ分析によるリスクの高い事業者対する早期かつ有効な立入検査を実施したり、リスクアセスメントの結果を新たな制度の創設につなげたりするなど、法令手続データ等の利活用・オープンデータ化による産業保安・製品安全行政の高度化についても求められている。

次期保安ネットは、現行保安ネットの実装範囲を継承することを前提としつつ、①利便性の一層の向上、②行政手続の電子化範囲の拡大、③事故情報データベースとの連携等による産業保安・製品安全行政の高度化、を実現するものであり、令和６年４月の運用開始を予定している。

2. 次期システム導入の目的

(1) 産業保安・製品安全分野におけるすべての行政手続のオンライン化

業務効率化やデータ収集・分析等の観点でオンライン化による恩恵を最大限に高めるため、産業保安・製品安全分野におけるすべての行政手続のオンライン化を実現する。

なお、オンライン化実現範囲には、地方自治体の行政手続も含める。

(2) 利便性の一層の向上

現行保安ネットに対する利用者の意見・要望を取り入れたシステムを実現する事で、官民双方の業務コストを削減できるよう利便性の一層の向上を図る。

---

[1] 液化石油ガスの保安の確保及び取引の適正化に関する法律のことを言う。

[2] 消費生活用製品安全法、電気用品安全法、ガス事業法、液化石油ガスの保安の確保及び取引の適正化に関する法律のことを言う。

(3) 事故情報データベースとの連携等による産業保安行政の高度化

保安ネットで収集したデータや他システムとの連携等により得られるデータを活用することで、データ駆動型の保安実現により行政監督体制の高度化を図る。

第2章 業務要件の定義

1. 手続の類型化

現行保安ネットにてオンライン化が実現できていない残り約 1,000 手続の効率的なオンライン化に向けて、汎用申請機能の導入に加えて手続様式や業務フローが類似する手続を一纏め(類型化)にすることで、要件定義及び設計構築の効率化を図る。手続の類型化は、「様式」「業務フロー」「審査フロー」の 3 つの観点において行う。

手続の様式とは、法令や行政で定められた提出書類に求められる記載事項やその書式を指す。

手続の業務フローとは、行政手続に係る一連の業務プロセスをフローにして可視化したものを指す。

手続の審査フローとは、業務フローの内、手続受付から受理、施行完了までの間のフローを指す。

なお、現行保安ネットにおいてオンライン化済みの手続及び複雑な要件のため類型化が困難な手続は、類型化を行わずに手続ごとに要件定義及び設計構築を実施すること。

各手続の類型は「別紙 2-1 手続一覧」に示す。

(1) 様式での類型化

項目及びレイアウトを観点とし、様式の類型化を行う。様式類型の一覧を以下に示す。

表 2-1 様式類型の観点

観点	概要
項目	マスタ管理が想定される項目の更新等が必要になる手続は、対象となるマスタごとに分類
レイアウト	様式に表形式の項目があるかで分類 (汎用申請機能に表形式の要件はないため、リスト形式の入力フォームで実現すること)

表 2-2 様式類型一覧

類型観点			様式類型		
法令	更新対象マスタ	表有無	#	類型 ID	類型名
電気	事業場	あり	1	ELE-JIGYO-1	事業場・電気工作物情報関連手続
	主任技術者(資格・合格科目・認定校)	なし	2	ELE-SYUGI-1	主任技術者情報関連手続
	資格者(電気工事士法)	なし	3	ELE-KOJISHI-2	電気工事士資格認定関連手続(表形式なし)
	事業者 (電気工事業法)	あり	4	ELE-KOHJIGYO-1	電気工事業情報関連手続(表形式あり)
		なし	5	ELE-KOHJIGYO-2	電気工事業情報関連手続(表形式なし)
ガス	事業者	あり	6	GAS-JIGYOSHA-1	都市ガス事業者情報関連手続(表形式あり)
		なし	7	GAS-JIGYOSHA-2	都市ガス事業者情報関連手続(表形式なし)
	ガス工作物	あり	8	GAS-KOSAKU-1	都市ガス工作物情報関連手続(表形式あり)
		なし	9	GAS-KOSAKU-2	都市ガス工作物情報関連手続(表形式なし)
	主任技術者	あり	10	GAS-SHUNIN-1	都市ガス主任技術者情報関連手続(表形式あり)
	ガス消費機器資格者	あり	11	GAS-SHOHIKIKI-1	ガス消費機器資格情報関連手続(表形式あり)

類型観点			様式類型		
法令	更新対象マスタ	表有無	#	類型 ID	類型名
		なし	12	GAS-SHOHIKIKI-2	ガス消費機器資格情報関連手続(表形式なし)
液石	事業者	あり	13	LIQ-JIGYO-1	液化石油ガス販売事業者情報関連手続(表形式あり)
		なし	14	LIQ-JIGYO-2	液化石油ガス販売事業者情報関連手続(表形式なし)
	保安機関	あり	15	LIQ-HOAN-1	液化石油ガス保安機関情報関連手続(表形式あり)
		なし	16	LIQ-HOAN-2	液化石油ガス保安機関情報関連手続(表形式なし)
製 品安全	事業者	あり	17	PRD-JIGYOSHA-1	製品安全 4 法事業者情報関連手続(表形式あり)
		なし	18	PRD-JIGYOSHA-2	製品安全 4 法事業者情報関連手続(表形式なし)
高圧ガス	事業者	あり	19	HPG-JIGYOSHA-1	高圧ガス事業者情報関連手続(表形式あり)
		なし	20	HPG-JIGYOSHA-2	高圧ガス事業者情報関連手続(表形式なし)
共通	- (マスタ管理不要)	あり	21	COM-YOUSIKI-1	マスタとの紐づけ不要手続(表形式あり)
		なし	22	COM-YOUSIKI-2	マスタとの紐づけ不要手続(表形式なし)
		なし (添付のみ)	23	COM-YOUSIKI-3	マスタとの紐づけ不要手続(電子フォーム化対象項目なし)

(2) 業務フローでの類型化

手続種別と業務内容を観点とし、業務フローの類型化を行う。業務フロー類型の一覧を以下に示す。

表 2-3 業務フロー類型一覧

類型観点				業務フロー類型		
手続種別	業務内容			#	類型 ID	類型名
	マスタ参照	マスタ更新	手数料			
申請	○	×	×	1	Apply01	マスタ参照必須申請
	○	○	×	2	Apply02	マスタ参照/更新必須申請
	○	○	○	3	Apply03	手数料納入・マスタ参照/更新必須申請
	○	×	○	4	Apply04	手数料納入・マスタ参照必須申請
	×	×	×	5	Apply05	手数料納入・マスタ参照/更新不要申請
	×	×	○	6	Apply06	手数料納入必須申請
届出	○	○	×	7	Nortif01	マスタ参照/更新必須届出
	×	×	×	8	Nortif02	手数料納入・マスタ更新不要届出
	○	○	○	9	Nortif03	手数料納入・マスタ参照/更新必須届出

(1) 審査フローでの類型化

手続種別に加え、決裁の有無や決裁者の所属部署を観点とし、審査フローの類型化を行う。審査フロー類型の一覧を以下に示す。

表 2-4 審査フロー類型一覧

類型観点								審査フロー類型		
手続種別	手続主体	本省宛	部署内承認	他部署承認				#	類型 ID	類型名
			保安ネット利用内決裁	保安ネット利用者外	経 済 産業省外	電子決済システム利用者外	他部署名			
共通	民間	-	-	-	-	-	-	1	CommonA	-
申請	民間	×	○	×	-	-	-	2	ApplyA	保安ネット完結型申請
届出	民間	×	○	×	-	-	-	3	NotifyD	保安ネット完結型届出
届出	民間	×	×	×	-	-	-	4	NotifyA	保安ネット完結型届出
申請	民間	×	○	○	×	-	経済産業省・大臣官房・会計課	5	ApplyB	会計課決裁対象申請
届出	民間	×	×	○	×	-	経済産業省・大臣官房室・会計課	6	-	会計課決裁対象届出
申請	民間	×	○	○	×	-	経済産業省・大臣官房・技術総括/保安審議官	7	ApplyC	グループ長決裁対象申請
届出	民間	×	×	○	×	-	経済産業省・大臣官房・技術総括/保安審議官	8	NotifyB	グループ長決裁対象届出
申請	民間	×	○	○	×	-	経済産業省・大臣官房・総務課・文書室	9	ApplyD	総務課文書室決裁対象申請
届出	民間	×	×	○	×	-	経済産業省・大臣官房室・総務課	10	-	総務課文書室決裁対象届出
申請	民間	×	○	○	×	-	経済産業省・大臣官房・技術総括/保安審議官及び大臣官房室・総務課	11	ApplyF	総務課文書室及びグループ長決裁対象申請
届出	民間	×	×	○	×	-	経済産業省・大臣官房・技術総括/保安審議官及び大臣官房室・総務課	12	NotifyC	総務課文書室及びグループ長決裁対象申請
申請	民間	×	○	○	○	不明	資源エネルギー庁・ガス市場整備室	13	ApplyE	資源エネルギー庁決裁対象手続
届出	民間	×	×	○	○	不明	資源エネルギー庁・ガス市場整備室	14	-	資源エネルギー庁決裁対象届出

2. 業務実施手順

経済産業省では、産業保安・製品安全分野の維持・向上のため、電気事業法、鉱山保安法、ガス事業法、液化石油ガス保安法、製品安全４法等に基づく許認可・承認・届出等の年間約 27 万件の手続業務を実施している。

また、事業者の自主保安体制の徹底・定着の促進や、必要に応じて立入検査等を行うことにより、法律の遵守状況や技術基準の適合状況を確認し、検査結果が不敵な場合には改善指示等を行うなど、公共の安全維持に務めている。

(1) 業務の範囲(業務機能とその階層)

産業保安・製品安全行政に係る業務の範囲について「別紙 2-2　業務の範囲」に示す。

(2) 業務フロー

産業保安・製品安全行政に係る届出・申請手続の業務フローを「別紙 2-3　業務フロー」に示す。

(3) 業務の実施に必要な体制

産業保安・製品安全行政に係る業務の実施に必要な体制を以下に示す。

表 2-5 業務の実施に必要な体制一覧

実施体制			組織概要	補足
申請者			本省/産業保安監督部/経済産業局に対して届出/申請を行う(法人、団体、個人、等)。	申請者から委任を受けた代行申請者を含む。
審査者	経済産業省 産業保安グループ	産業保安企画室	法令共通で本省宛ての手続の内容確認・審査等を実施する。また、お知らせの管理等のシステム管理業務を実施する。	-
		ガス安全室	ガス事業法・液化石油ガス保安法等に係る本省宛ての手続の内容確認・審査等を実施する。	-
		高圧ガス保安室	高圧ガス保安法等に係る本省宛ての手続の内容確認・審査等を実施する。	-
		電力安全課	電気事業法等に係る本省宛ての手続の内容確認・審査等を実施する。	-
		鉱山・火薬類監理官付	鉱山保安法・火薬取締法等に係る本省宛ての手続の内容確認・審査等を実施する。	-
		製品安全課	製品安全 4 法等に係る本省宛ての手続の内容確認・審査等を実施する。	-

実施体制		組織概要	補足
	経済産業局	各地方に拠点があり、製品安全 4 法に係る手続の内容確認・審査を実施する。	各地方拠点は下記の通り。 ・北海道経済産業局 ・東北経済産業局 ・関東経済産業局 ・中部経済産業局 ・近畿経済産業局 ・中国経済産業局 ・四国経済産業局 ・九州経済産業局 ・沖縄総合事務所
	産業保安監督部	各地方に拠点があり、電気事業法・液化石油ガス法・ガス事業法・鉱山保安法・火薬取締法等に係る手続の内容確認・審査を実施する。	各地方拠点は下記の通り。 ・北海道産業保安監督部 ・関東東北産業保安監督部東北支部 ・関東東北産業保安監督部 ・中部近畿産業保安監督部 ・北陸産業保安監督署 ・中部近畿産業保安監督部近畿支部 ・中国四国産業保安監督部 ・中国四国産業保安監督部四国支部 ・九州産業保安監督部 ・那覇産業保安監督事務所
	地方自治体	地方自治体宛の手続の内容確認・審査を実施する。	-

(4) 入出力情報及び取扱量

産業保安・製品安全行政に係る業務で使用する主たる入出力情報及び取扱量を以下に示す。

表 2-6 入出力情報及び取扱量一覧

業務処理	入出力情報名	入出力の区分	主な入出力情報項目	取扱量	取得元/提供元
届出・申請情報入力	申請者情報 手続情報	入力	申請者名、法人名、住所 提出日、対象法令、手続名、届出・申請情報、審査フロー、審査情報	580,000 件/年	申請者
事前相談内容入力	事前相談履歴情報	入力	事前相談年月日、事前相談対象項目、相談内容	120,000 件/年	申請者
問合せ・資料差替依頼	問合せ履歴情報	入力	問合せ年月日、問合せ対象項目問合せ内容	46,000 件/年	審査者

結果通知	届出・申請結果	出力	受理年月日、審査結果	580,000 件/年	審査者
通知文書作成	処分通知	出力	処分年月日、申請者名、法人名、住所、提出日、対象法令、手続名、通知内容	460,000 件/年	審査者
承認書・免状等交付	承認書・免状	出力	交付年月日、申請者名、法人名、住所、提出日、対象法令、手続名	3,200 件/年	審査者

(5) 管理対象情報一覧

入出力情報のうち、管理すべき主たる情報を以下に示す。

表 2-7 管理対象情報一覧

管理対象情報名	管理単位	主たる用途	主な属性	補足
提出者情報	管理番号	申請者の情報を持つ。	氏名、電話番号、アカウント種別 等	初回ログイン時に付番
手続情報	手続 ID	提出された届出・申請内容の情報を持つ。	手続名、法令 等	手続提出時に付番
事前相談履歴情報	手続番号	手続ごとの事前相談の履歴の情報を持つ。	事前相談実施日、提出者名、提出者メールアドレス 等	-
問合せ履歴情報	手続番号	手続ごとの問合せの履歴の情報を持つ。	提出日、お問合せ種別、提出者メールアドレス 等	-
事業者情報(法令ごと)	事業者番号	法令ごとの事業者の情報を持つ。	法人/個人名称、代表者氏名、郵便番号(ハイフンなし) 等	初回登録時に付番
事業場情報(法令ごと)	事業場番号	法令ごとの事業場に関する情報を持つ。	管区、事業場名、郵便番号(ハイフンなし) 等	初回登録時に付番
発電所情報	発電所番号	電気事業法に係る発電所の情報を持つ。	常用/非常用の別、発電所・蓄電所名称、出力 等	初回登録時に付番
主任技術者情報	交付番号	電気事業法に係る主任技術者の情報を持つ。	免状種別、交付番号、姓、名 等	初回登録時に付番(一括登録含む)
管理技術者情報	管理技術者番号	電気事業法に係る管理技術者の情報を持つ。	氏名、生年月日、資格取得年月日 等	初回登録時に付番
電気工事業者情報	電気工事業者番号	電気事業法に係る電気工事事業者の情報を持つ。	管区、法人/個人名称、電気工事業者種別 等	初回登録時に付番
鉱山情報	鉱山番号	鉱山保安法に係る鉱山の情報を持つ。	鉱山名、鉱種、等	初回登録時に付番
事故情報(法令ごと)	事故番号	法令ごとの事故の情報を持つ。	事故発生日、製品名、機種・型式等 等	初回登録時に付番
リコール情報	リコール番号	製品安全 4 法に係るリコールの情報を持つ。	リコール開始年月日、製品名、対象台数 等	初回登録時に付番

3. 規模

(1) サービスの利用者数及び情報システムの利用者数

保安ネットのサービス利用者及び情報システム利用者を以下に示す(国及び地方自治体受付の手続がオンライン化された場合)。

表 2-8 サービスの利用者数及び情報システムの利用者数一覧

利用者			利用者の種類		主な利用拠点	サービス提供時間帯	利用者数
			サービス利用者	情報システムの利用者			
申請者			○	○	全国	24 時間	約 1,460 人(月平均)
審査者	経済産業省産業保安グループ	産業保安企画室	–	○	本省	24 時間	約５人
		ガス安全室	-	○	本省	24 時間	約５人
		高圧ガス保安室	-	○	本省	24 時間	約１０人
		電力安全課	–	○	本省	24 時間	約２０人
		鉱山・火薬類監理官	–	○	本省	24 時間	約１０人
		製品安全課	–	○	本省	24 時間	約３０人
	経済産業局	北海道経済産業局	–	○	北海道経済産業局	24 時間	約５人
		東北経済産業局	–	○	東北経済産業局	24 時間	約５人
		関東経済産業局	–	○	関東経済産業局	24 時間	約２０人
		中部経済産業局	–	○	中部経済産業局	24 時間	約５人
		近畿経済産業局	–	○	近畿経済産業局	24 時間	約１０人
		中国経済産業局	–	○	中国経済産業局	24 時間	約１０人
		四国経済産業局	–	○	四国経済産業局	24 時間	約５人
		九州経済産業局	–	○	九州経済産業局	24 時間	約５人
		沖縄総合事務所	–	○	沖縄総合事務所	24 時間	約５人
		北海道産業保安監督部	–	○	北海道産業保安監督部	24 時間	約４０人

利用者			利用者の種類		主な利用拠点	サービス提供時間帯	利用者数
			サービス利用者	情報システムの利用者			
	産業保安監督部	関東東北産業保安監督部東北支部	–	○	関東東北産業保安監督部東北支部	24 時間	約５０人
		関東東北産業保安監督部	–	○	関東東北産業保安監督部	24 時間	約６０人
		中部近畿産業保安監督部	–	○	中部近畿産業保安監督部	24 時間	約４０人
		北陸産業保安監督署	–	○	北陸産業保安監督署	24 時間	約１０人
		中部近畿産業保安監督部近畿支部	–	○	中部近畿産業保安監督部近畿支部	24 時間	約４０人
		中国四国産業保安監督部	–	○	中国四国産業保安監督部	24 時間	約３０人
		中国四国産業保安監督部四国支部	–	○	中国四国産業保安監督部四国支部	24 時間	約３０人
		九州産業保安監督部	–	○	九州産業保安監督部	24 時間	約５０人
		那覇産業保安監督事務所	–	○	那覇産業保安監督事務所	24 時間	約１５人
	地方自治体		–	○	各地域拠点	24 時間	約１０人

(2) 処理件数

産業保安・製品安全行政に係る業務において処理される件数を以下に示す(国及び地方自治体受付の手続がオンライン化された場合)。

表 2-9 処理件数一覧

項目	処理件数		補足
	定常時	ピークの特性	
届出・申請手続	約 48,000 件/月	約 77,000 件/月	ピークは 4 月を想定。
立入検査結果の入力	約 63 件/月	-	-
統計資料(年報等)の作成	2~12 件/年	-	-

4. 時期・時間

(1) 業務の時期・時間

産業保安・製品安全行政に係る業務の実施時期・時間を以下に示す。

表 2-10 業務時期・時間一覧

業務	実施時期・期間	実施・提供時間	補足
届出・申請手続	通年	・申請者：原則 24 時間(オンライン) ・審査者：原則 24 時間(オンライン)	郵送・窓口での受付は各庁舎の開庁時間のみ。
立入検査結果の入力	通年	・申請者：- ・審査者：開庁時間のみ	-
統計資料(年報等)の作成	都度	・申請者：- ・審査者：開庁時間のみ	-

5. 場所等

(1) 業務の実施場所

産業保安・製品安全行政に係る業務の実施場所を以下に示す。

表 2-11 業務の実施場所一覧

場所名	実施体制	実施業務	所在地	補足
オフィス・事業場等	申請者	保安ネットにて手続の提出を行う。	全国	各オフィス・事業場等における端末で業務を行う想定。
オフィス等	経済産業省産業保安グループ	保安ネットにて、本省宛て又は複数の管区にまたがる手続の審査を行う。	東京都千代田区霞が関 1-3-1	-
	北海道経済産業局	保安ネットにて、管轄する申請者からの手続の審査を行う。	北海道札幌市北区北 8 条西 2 丁目 札幌第 1 合同庁舎 4･5 階	-
	東北経済産業局		宮城県仙台市青葉区本町 3-3-1	-
	関東経済産業局		埼玉県さいたま市中央区新都心 1 番地 1 さいたま新都心合同庁舎 1 号館	-
	中部経済産業局		愛知県名古屋市中区三の丸二丁目五番二号	-
	近畿経済産業局		大阪府大阪市中央区大手前 1-5-44 大阪合同庁舎 1 号館 2,3,5 階	-
	中国経済産業局		広島県広島市中区上八丁堀 6 番 30 号	-
	四国経済産業局		香川県高松市サンポート 3-33	-
	九州経済産業局		福岡県福岡市博多区博多駅東 2 丁目 11 番 1 号 福岡合同庁舎本館(6 階、7 階)	-
	沖縄総合事務所		沖縄県那覇市おもろまち 2 丁目 1 番 1 号 那覇第 2 地方合同庁舎 2 号館	-
	北海道産業保安監督部	保安ネットにて、管轄する申請者からの手続の審査を行う。	北海道札幌市北区北 8 条西 2 丁目 1-1 札幌第 1 合同庁舎 6 階南	-
	関東東北産業保安監督部東北支部		宮城県仙台市青葉区本町 3 丁目 2-23 仙台第 2 合同庁舎 9 階	-

場所名	実施体制	実施業務	所在地	補足
	関東東北産業保安監督部		埼玉県さいたま市中央区新都心 1 番地 1 さいたま新都心合同庁舎 1 号館 11 階	-
	中部近畿産業保安監督部		愛知県名古屋市中区三の丸 2 丁目 5-2 中部経済産業局総合庁舎 3 階	-
	北陸産業保安監督署		富山県富山市牛島審町 11 番 7 号 富山地方合同庁舎 3 階	-
	中部近畿産業保安監督部近畿支部		大阪府大阪市中央区大手前 1 丁目 5-44 大阪合同庁舎 1 号館 本館 2 階、3 階	-
	中国四国産業保安監督部		広島県広島市中区上八丁堀 6-30 広島合同庁舎 2 号館 4 階	-
	中国四国産業保安監督部四国支部		香川県高松市サンポート 3 番 33 号 高松サンポート合同庁舎 5 階	-
	九州産業保安監督部		福岡県福岡市博多区博多駅東 2 丁目 11-1 福岡第 1 合同庁舎 8 階	-
	那覇産業保安監督事務所		沖縄県那覇市おもろまち 2 丁目 1-1 那覇第 2 地方合同庁舎 4 階	-
	地方自治体	保安ネットにて、管轄する申請者からの手続の審査を行う。	各地方自治体拠点	-

(2) 諸設備、物品等

産業保安・製品安全行政に係る業務で使用する諸設備・物品等を以下に示す。

表 2-12 諸設備・物品一覧

種類	量	補足
PC	-	申請者：各事業者が業務に利用している端末を使用する。 経済産業省：経済産業省が支給するセキュア PC、定められた NW を使用する。 地方自治体：各自治体の基準に従った端末、定められた NW を使用する。

6. 管理すべき指標

(1) 管理すべき指標

次期保安ネットを用いたサービス・業務の運営上管理すべき指標を以下に示す。

表 2-13 管理すべき指標一覧

指標の種類	指標名	計算式	目標値	計測方法
プロジェクト成果目標	オンライン利用率	電子申請件数/(電子申請件数+紙申請件数)×100	87%	オンライン化済み手続で 1 か月の間に提出された手続件数の内、電子申請件数の割合を算出する。 法令ごと、地域ごとに算出する。
	オンライン化率	電子フォーム化されている手続数/オンライン化対象手続数×100	100%	すべてのオンライン化対象手続の内、すでにオンライン化されている手続の割合を算出する。 法令ごとに算出する。

7. 情報システム化の範囲

(1) 情報システムの機能

産業保安・製品安全行政に係る業務の情報システム化の範囲を以下に示す。

表 2-14 情報システムの機能一覧

情報システム機能		対応する処理 ※「別紙 2-2. 業務の範囲」の処理 ID
届出・申請情報入力	• 提出対象の法令・手続を選定する。 • 手続に応じた届出・申請項目の入力を行う。 • 手続に必要な添付書類のアップロードを行う。	1-1-6
マスタ参照(提出者)	• 提出者が過去に入力・提出した手続を検索・確認する。	1-1-7
提出内容確認	• 入力した提出内容を確認する。	1-1-8
申請情報事前確認	• 手数料情報など、審査者に確認すべき事項がある場合に事前確認をする。	1-2-1
手数料設定	• 手続ごとに手数料を設定する。	1-2-2
手数料納入情報確認	• 審査者が手数料納入情報を確認する。	1-2-3
手数料納入(電子)	• 提出者が手数料をオンラインで納入する。	1-2-4
担当者確認	• 提出者から提出された手続の内容を確認する。	1-3-1
マスタ参照(審査者)	• 審査者が過去に入力・提出された手続を検索・確認する。	1-3-3
届出・申請取下げ	• 届出・申請中の手続を取下げる。	1-3-4
問合せ・資料差替依頼	• 手続内容について提出者に確認すべき事項がある場合に、提出者に問合せ・資料差替依頼を行う。	1-3-5
問合せ回答	• 提出者が問合せ内容に回答する。	1-4-2
問合せ回答内容確認	• 審査者が問合せへの回答内容を確認する。	1-4-3
起案	• 審査が完了した案件を起案する。	1-5-1
上長決裁(複数ステップ)	• 提出者から提出された手続の決裁をする。	1-5-2
差し戻し	• 申請情報や審査内容に誤りがある場合などに、起案者へ差し戻しを行う。 • 不備解消後決裁を再開する。	1-5-3
結果通知	• 審査結果を提出者に通知する。	1-6-2
通知文書作成	• 処分通知を作成する。	1-6-1
承認書・免状等交付	• 承認書・免状等を交付する。	1-6-5
文書保存	• 行政文書として保存する(電子決裁システム(EASY)との連携等)。	1-7-2
マスタ管理	• 各種マスタデータ(手続情報、法令ごとの事業者情報や事業場情報等)を登録・更新・削除する。 • 各種マスタデータを検索する。 • 各種マスタデータの検索結果を CSV 出力する。	1-7-3
新規受付手続追加	• 新しくオンラインで受付する手続の電子申請フォームを作成する。	1-7-4
検査対象選定	• 手続きや違反情報などを基に検査対象を選定する。	2-1-2
検査実施	• 立入検査を実施する。	2-2-3

情報システム機能		対応する処理 ※「別紙 2-2. 業務の範囲」の処理 ID
検査結果管理	• 立入検査結果を登録・更新・削除等する。	2-2-4
組織間情報連携	• 事故や災害発生時に各組織間で情報連携する。	3-1-1
リスク分析	• 事故・違反情報等の情報から、事業者ごとの事故のリスクを分析・評価・可視化する。	3-2-1
マスタデータ集計・可視化	• 手続情報や事故・違反情報等を所定の項目で集計し、CSV 等で出力、もしくは BI ツールで可視化する。	4-1-1
マスタデータ連携	• 公表データを他システムに連携、もしくは他システムから参照できるようにする。	4-1-2
アクセス	• 提出者は gBizID やマイナポータルを利用しアクセスする。 • 審査者は GIMA で認証してアクセスする(地方自治体は LGWAN 接続系を利用してアクセスする)。 • 運用者は ID と Password でアクセスする。	-
アカウント管理	• アカウント情報を登録・更新・削除等する。 • 権限を設定する。	-
トップページ	• ログイン後トップページに重要なお知らせ、よくある質問、各種リンク等を表示する。 • 利用規約・プライバシーポリシーを表示する。	-
メニュー表示	• トップページメニューに新規手続、要対応手続一覧、データ管理、アカウント管理等のメニューを表示する。	-
掲載情報管理	• お知らせ情報を登録・更新・削除等する。 • 登録されているお知らせ情報を一覧表示する。 • よくある質問を登録・更新・削除等する。 • 登録されているよくある質問情報を一覧表示する。 • はじめにお読みくださいを登録・更新・削除等する。 • 登録されているはじめにお読みくださいを表示する。	-
システム管理	• コードを登録・更新・削除等する。 • 各種ログを記録する。	-
ヘルプデスク	• 提出者がヘルプデスクに問合せを行う。 • ヘルプデスクが提出者の問合せに回答する。	-
利用状況確認	• 電子・紙申請それぞれの手続提出件数、オンライン利用率等を集計・確認する。	-
メール配信機能	• 手続受付時やリマインド等の各種メールを配信する。	-

8. 業務の継続の方針等

(1) 目標復旧時間及び目標復旧時点

産業保安・製品安全行政に係る業務を継続して実施するための目標復旧時間及び目標復旧時点を以下に示す(各法令に係る申請の標準処理期間を参考にしながら、業務要件とシステム要件が乖離しないように設定)。

表 2-15 目標復旧時間及び目標復旧時点

目標復旧時間	目標復旧時点
12 時間以内	障害発生時点(日次バックアップ＋アーカイブからの復旧)

9. 情報セキュリティ

(1) 情報セキュリティ対策の基本的な考え方

情報セキュリティ対策の基本的な考え方を以下に示す。ただし、自治体のセキュリティポリシーについては、各自治体の方針に従うこと。

表 2-16 情報の格付け一覧

主な情報	情報の機密性	
	特徴	格付の区分
提出者情報	個人情報が含まれる。	機密性 2 情報
手続	-	同上
事前相談履歴情報	-	同上
問合せ履歴情報	-	同上
事業者情報(法令ごと)	個人情報が含まれる。	同上
事業場情報(法令ごと)	個人情報が含まれる。	同上
発電所情報	-	同上
主任技術者情報	個人情報が含まれる。	同上
管理技術者情報	個人情報が含まれる。	同上
電気工事業者情報	-	同上
鉱山情報	-	同上
事故情報(法令ごと)	個人情報が含まれる。	同上
リコール情報	-	同上

第3章　機能要件の定義

1．機能に関する事項

(1) 機能一覧

次期保安ネットに求められる機能の一覧について「別紙 3-1　機能一覧」に示す。

(2) 次期保安ネット機能概要

次期保安ネットにおける基本機能及び届出・申請(受付、起案・決裁、施行、保存・保管)機能の全体像を以下に示す。次期保安ネットは現行保安ネットにおける機能要件の更改及び新規追加の機能要件をもとに構築すること。

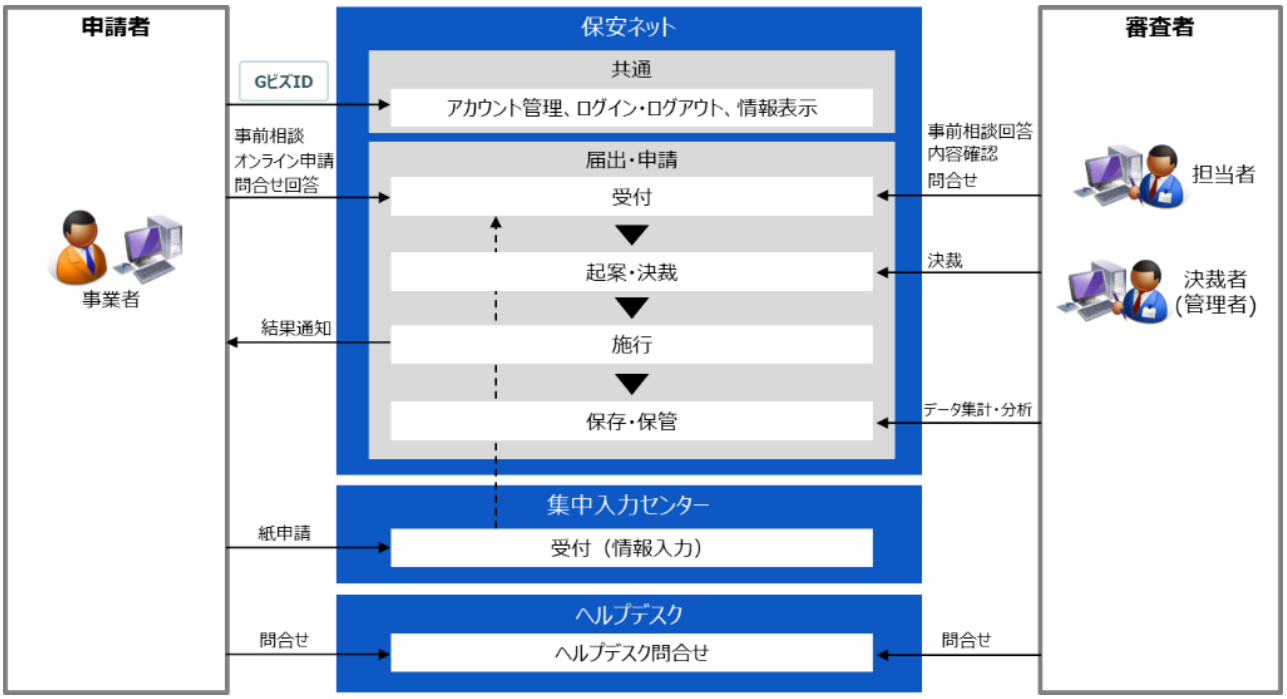

図 3-1　次期保安ネットの概要図

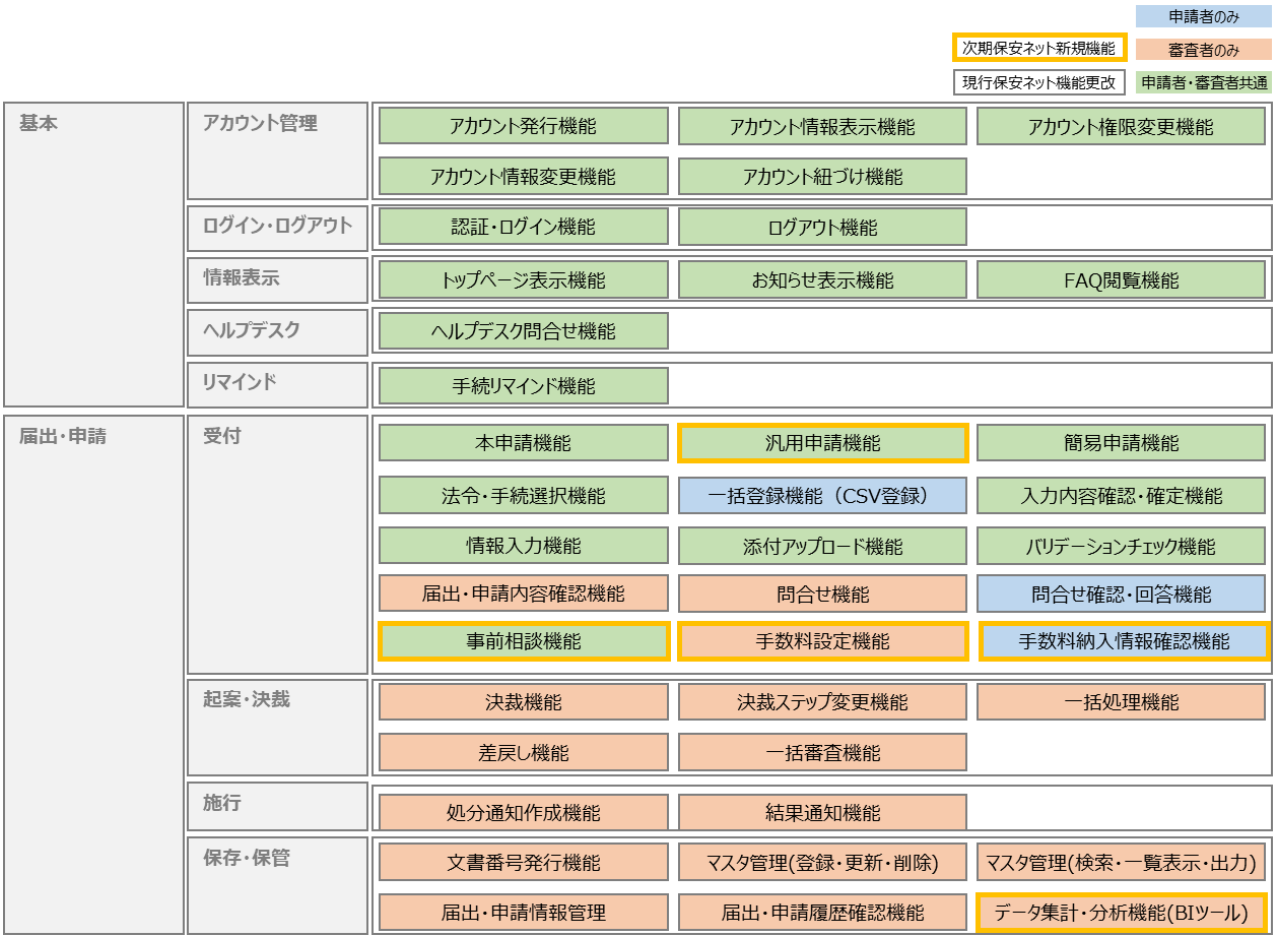

図 3-2　次期保安ネットの機能

次期保安ネットの機能のうち、汎用申請機能及びデータ集計・分析機能(BI ツール)に関する要件を以下に示す。

ア. 汎用申請機能概要

現行保安ネットは申請件数の多い手続を中心にオンライン化を進めてきた。現行保安ネットにおける届出・申請(受付、起案・決裁、施行、保存・保管)の機能は、設計構築事業者や運用保守事業者によって手続ごとに画面や機能、データに係る設計構築及び改修を実施することで実装された機能(以下「本申請機能」という。)である。一方で、現行保安ネットでは、法令に基づくすべての手続の網羅的なオンライン化には至っていない。オンライン化対象となっているが現行保安ネットにてオンライン化が実現できていない手続は残り約 1,000 手続あり、より効率的にオンライン化を実装する方策が必要である。

そこで、次期保安ネットでは、本申請機能によるオンライン化に加えて、本申請機能と比べて一定の機能制約があるものの、より簡易に手続のオンライン化を実現する機能(以下「汎用申請機能」という。)を実装すること。汎用申請機能は、画面レイアウトや審査プロセスについて、あらかじめ手続の類型ごとに設定のテンプレートを準備しておき、テンプレートに対して各手続に応じたカスタマイズ設定をすることでオンライン化を実現する機能とすること。現行保安ネットにおいて本申請方式にてオンライン化を実現している手続は、次期保安ネットにおいても本申請

方式を採用すること。

なお、現行保安ネットは本申請機能以外に、手続内容を記入した様式ファイルをアップロードすることで提出可能な簡易申請機能も有する。簡易申請機能は次期保安ネットにおいても実装すること。

(ア) 汎用申請機能の要件

① 画面項目のカスタマイズ設定

法令毎に共通的な項目の他に、手続ごとに固有の項目を任意に設定可能とすること。また、設定可能な項目は運用期間中においても変更可能とすること。

② 審査プロセスのカスタマイズ設定

手続ごと、または同一手続においても監督部・経産局等ごとに審査担当者や審査フロー等を設定可能とすること。また、設定可能な項目は運用期間中においても変更可能とすること。

③ 手続新規追加・変更

類型ごとに作成したテンプレート及び手続ごとに定義した画面項目をもとに設定シート(Excel、等)を自動作成できること。

自動作成された設定シートを経済産業省職員にて内容の確認・修正を行い、記載内容を基に設計構築事業者や運用保守事業者にてシステムへ取り込むためのデータシート(CSV、等)を自動作成できること。

データシートを保安ネットへ取り込むことで、手続を汎用申請機能で追加・変更することを可能とすること。

(イ) 汎用申請機能として具備すべき機能一覧

表 3-1 汎用申請機能として具備すべき機能一覧

対象機能		次期保安ネット機能要件概要	
		本申請機能	汎用申請での実装要否
受付	法令・手続選択	• 新規提出対象の手続を選択できること。	要
	情報入力	• 提出者情報欄に提出者の情報を初期表示すること。 • 詳細情報を入力できること。 • 表形式の入力ができること。詳細情報入力時にマスタを参照できること。 • 過去に提出を実施した手続情報を新たに提出する手続の画面上に反映が可能であること。 • 紙申請による手続についても入力できること。	要
		• 入力された項目の値に応じて、他の項目の表示、非表示を制御できること。 • 入力された項目に対して任意処理を実施し、他項目に自動入力できること。 • 入力された項目のコピーを行い、他項目への反映が可能であること。	不要
	一括登録(CSV 登録)	• 複数の手続情報を入力した CSV をアップロードして一括登録できること。	不要
	添付アップロード	• 添付ファイルをアップロードできること。	要

対象機能		次期保安ネット機能要件概要	
		本申請機能	汎用申請での実装要否
	入力内容確認・確定	• 入力内容の確認を行い問題なければ提出ができること。	要
	バリデーションチェック	• 必須・型・桁のチェックができること。 • 提出先が正しいかチェックできること。	要
		• 手続固有のチェックができること。	不要
	届出・申請内容確認	• 審査者は提出された届出・申請情報を確認できること。	要
	事前相談	• 申請者は入力した届出・申請情報について事前相談が実施できること。	要
	手数料納入	• 申請者は手数料納入情報を確認できること。	要
	問合せ	• 審査者は手続内容について申請者に確認すべき事項がある場合は、問合せできること。	要
	問合せ確認・回答	• 申請者は問合せ内容を確認して回答できること。	要
起案・決裁	決裁	• 審査者は提出された届出・申請を決裁することができること。	要
	差戻し	• 審査フローにおいて、前の決裁者にプロセスを戻すことができること。	要
	審査フロースキップ	• 審査フローにおいて、後の決裁者のスキップができること。	要
	一括審査	• 電子申請・紙申請で提出された手続を一括で審査できること。	不要
	一括処理	• 上長確認、課長決裁・施行を一覧で処理できること。	不要
施行	処分通知作成	• 手続内容を基に処分通知を作成できること。	要
	結果通知	• 審査が完了した段階で申請者へ結果通知を送付すること。	要
保存・保管	文書番号発行	• 手続の受理・審査完了後に、文書番号を発行できること。	要
	マスタ管理	• 届出・申請情報に応じて各種マスタに登録・更新・削除できること。	要
出力	CSV 出力	• すべての手続の提出内容を CSV 形式で出力できること	要

初期構築時及び運用開始後の汎用申請機能の利用イメージを以下に示す。

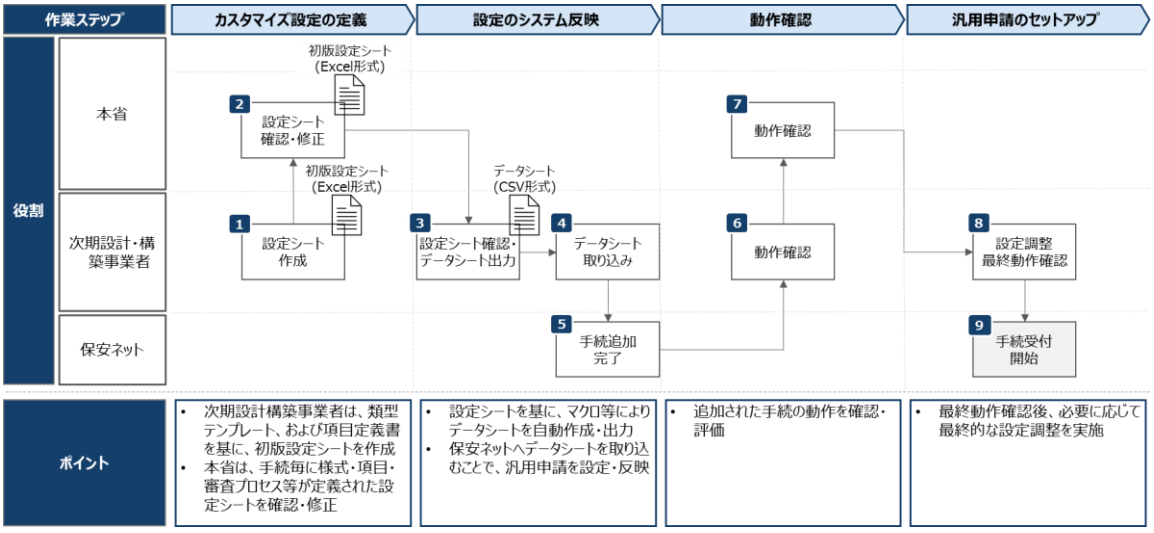

図 3-3　初期構築時の汎用申請機能利用イメージ

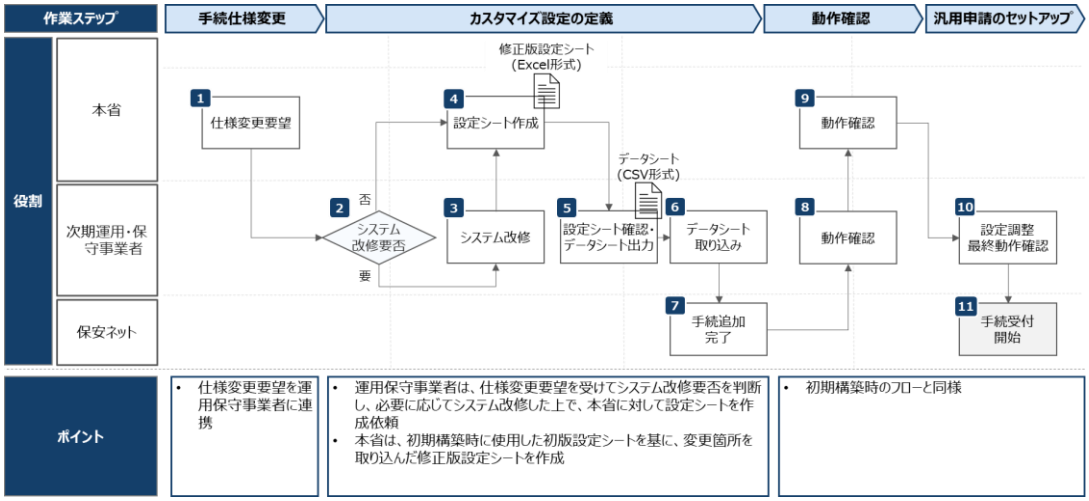

図 3-4　運用開始後の汎用申請機能利用イメージ

イ. データ集計・分析機能(BI ツール)概要

次期保安ネットにおいては、行政手続のオンライン申請率向上に加え、蓄積した情報を利活用(データ集計・分析の自動化及びグラフ等可視化)することで、審査業務のみならず、調査・報告業務の効率化、さらには産業保安・製品安全行政の高度化につなげていくことが重要である。そのため、BI ツール(Business Intelligence ツール)を導入し、保安ネットとデータ連携して政策判断の基礎的情報となる事故や法令違反等の情報を目的応じた観点にて集計を行い出力・可視化を実現すること。

BI ツールの導入によって、例えば、各法令等で作成・公表することが定められている報告書や審議会等の資料を効率的かつ正確に作成すること可能となる。さらに、分析結果から事故リスクの高い事業者を予見し、先行して立入検査等を実施することにより、事故発生の防止につなげることなどが期待される。

(ア) データ集計・分析機能(BI ツール)の要件

法令ごとに定められた集計・分析機能を BI ツールで実現できること。また、その他定型業務やデータ利活用等に鑑みて必要と想定されるものについては随時追加検討すること。また、BI ツールに係る要件詳細については、「令和 4 年度経済産業省デジタルプラットフォーム構築事業(産業保安システムにおけるデータ収集・分析の自動化及びグラフ等可視化に関する実証調査)」の調査報告書も参照すること。

(3)　詳細業務フロー

産業保安・製品安全行政に係る届出・申請手続の業務フローを「別紙 2-3　業務フロー」に示す。

2. 画面に関する事項

(1) 画面一覧

画面一覧を「別紙 3-2 画面一覧」に示す。

(2) 画面イメージ

基本的・代表的な画面イメージを「別紙 3-3 画面イメージ」に示す。設計構築事業者は画面設計ポリシーを考慮し作成すること。

(3) 画面遷移の基本的考え方

保安ネットに係る画面遷移の基本的な考え方について、代表的な画面を用いて下記に示す。

- 次期保安ネット全体の画面遷移、画面表示及び画面構成に統一性を持たせること。
- 画面を一度閉じたり、メニュー画面に遡ったりすることなく、連続的な操作を可能とすること。
- ポップアップ表示による子画面を除き、各画面の上部に統一的な操作メニューを表示し、他の画面への遷移を可能とすること。
- ポップアップ表示による子画面を除き、現在の画面のメニュー体系における位置を階層的に表示し、他の画面への遷移を可能とすること。

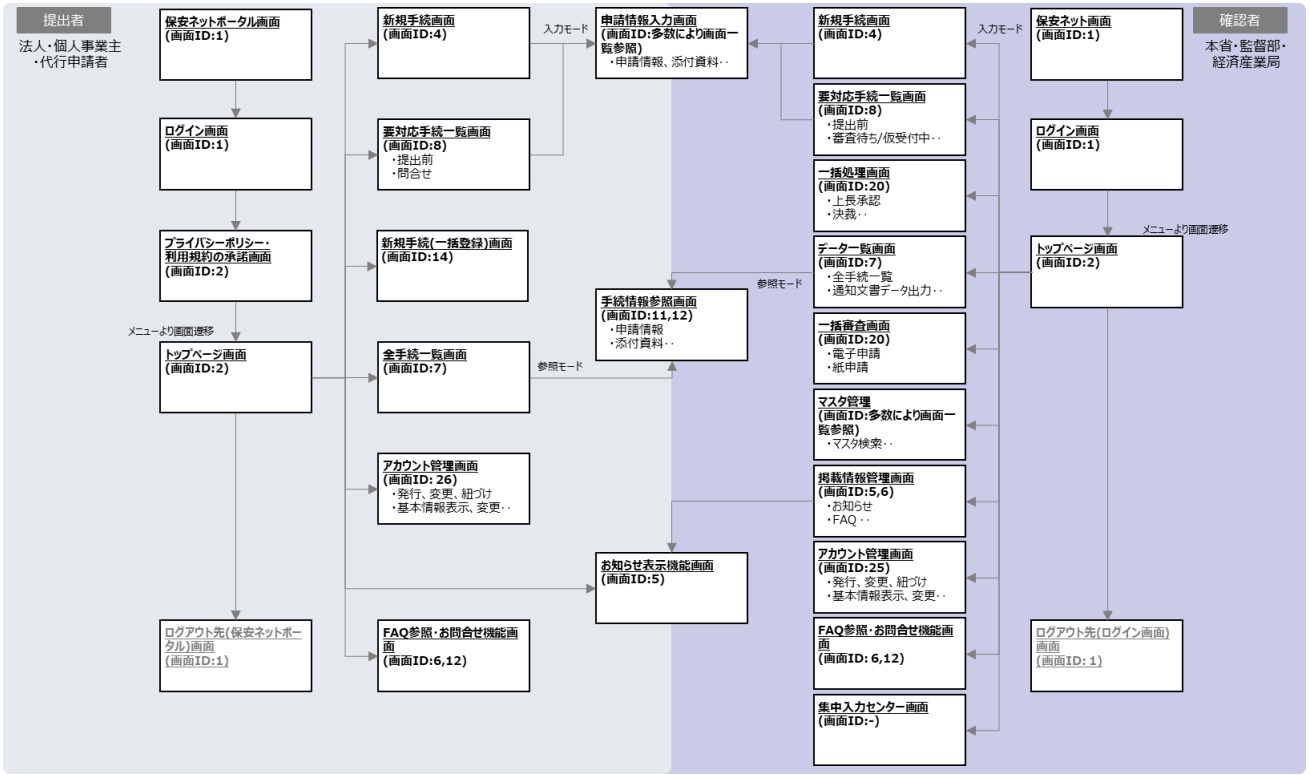

図 3-5 画面遷移の基本的は考え方

(4) 画面設計ポリシー

「第 4 章 非機能要件定義　1．ユーザビリティ及びアクセシビリティに関する事項」を参照すること。

3. 帳票に関する事項

(1) 帳票一覧

帳票一覧を「別紙 3-4　帳票一覧」に示す。

(2) 帳票イメージ

代表的な帳票のイメージを「別紙　3-5　帳票イメージ」に示す。設計構築事業者は別紙を参照の上、帳票設計ポリシー等を考慮し各手続の処分通知等の帳票レイアウトを作成すること。

(3) 帳票設計ポリシー

出力する帳票について、設計時に考慮すべき基本的な要件を以下に示す。

- 出力用紙は、日本工業規格(JIS)による A4 とすること。
- Excel 形式又は PDF 形式で出力される帳票の文字は、タイトル文字・内容文字等に区別して、それぞれフォント及びサイズを規定することとすること。
- CSV 形式で出力される帳票の特定のフィールドに、必ず見出しを付けること。
- Excel 形式又は PDF 形式で出力される帳票の特定のフィールドに、必ず見出し、ページ番号を付けること。
- Excel 形式又は PDF 形式で出力される帳票において、文字列の値は常に左揃えにすること。
- Excel 形式又は PDF 形式で出力される帳票において、数値は常に右揃えにすること。
- 帳票間での表示内容及び出力項目を見直し、統一化すること。
- 帳票上に表示する日付項目は、西暦・和暦を見直し、統一化すること。
- 本申請の処分通知については、既存の紙媒体の様式に従って設計構築すること。

4. データに関する事項

(1) データモデル

データモデルを「別紙 3-6　データモデル」に示す。

(2) データ一覧

データ一覧を「別紙 3-7　データ一覧」に示す。

(1) データ定義

データ定義を「別紙 3-8　データ定義」に示す。

(2) CRUD マトリクス

保安ネットで扱うデータのアクセス権限を「別紙 3-9　CRUD マトリクス」に示す。

(3) コード一覧

コード一覧を「別紙 3-10　コード一覧」に示す。

(4) コード内容定義

コード内容定義を「別紙 3-11　コード内容定義」に示す。

(5) オープンデータ一覧

保安ネットで扱うオープンデータを以下に示す。なお、扱うデータは今後対象が拡大する可能性がある。

表 3-2 オープンデータ一覧

データ ID	データ名	概要	利用者	公開範囲	利用目的	利用頻度・特徴	実装方式	処理方式
DT-68	公表情報管理	製品事故の公表情報を管理する。	職員・一般市民	制限なし	製品事故の情報を社会全体で共有することで、再発防止に取り組むため。	アクセス数約 50 件/日 ピーク時アクセス数約 500 件/日 ピークは情報公開時を想定している。	HTML	リアルタイム型

5. 外部インタフェースに関する事項

(1) 外部インタフェース一覧

保安ネットと他システムとの連携(外部インタフェース)について「別紙 3-12　外部インタフェース一覧」に示す。

第4章 非機能要件の定義

1. ユーザビリティ及びアクセシビリティに関する事項

次期保安ネットのユーザビリティ及びアクセシビリティに関する要件は、現行保安ネットと同等となることを前提とする。必要に応じて、経済産業省が閲覧に供する現行保安ネットの設計書等を参照すること。なお、ユーザビリティ要件は、設計構築フェーズをもって実装完了とするものではなく、運用開始後も、サービス品質の向上を目的に、アクセス解析等のツールを用いて継続的に改善すること。

(1) 情報システムの利用者の種類、特性

次期保安ネットの利用者の種類及び特性を以下に示す。

表 4-1 情報システムの利用者の種類・特性一覧

<table>
<tr><th colspan="3">利用者種類</th><th>利用者役割</th><th>特性</th></tr>
<tr><td colspan="3">申請者</td><td>本省/産業保安監督部/経済産業局/地方自治体に対して届出/申請を行う(法人、団体、個人、等)。</td><td>・ 対象手続の追加に伴い、次期システムからの新規利用者の増加が想定される。
・ 現行システムの利用に慣れている。
・ IT リテラシーにばらつきがある。</td></tr>
<tr><td rowspan="8">審査者</td><td rowspan="6">経済産業省
産業保安グループ</td><td>産業保安企画室</td><td>法令共通で本省宛ての手続の内容確認・審査等を実施する。また、お知らせの管理等の、システム管理業務を実施する。</td><td rowspan="8">・ 対象手続に関する知識レベルが高い。
・ 現行システムの利用に慣れている。</td></tr>
<tr><td>ガス安全室</td><td>ガス事業法・液化石油ガス保安法等に係る本省宛ての手続の内容確認・審査等を実施する。</td></tr>
<tr><td>高圧ガス保安室</td><td>高圧ガス保安法等に係る本省宛ての手続の内容確認・審査等を実施する。</td></tr>
<tr><td>電力安全課</td><td>電気事業法等に係る本省宛ての手続の内容確認・審査等を実施する。</td></tr>
<tr><td>鉱山・火薬類監理官</td><td>鉱山保安法・火薬取締法等に係る本省宛ての手続の内容確認・審査等を実施する。</td></tr>
<tr><td>製品安全課</td><td>製品安全 4 法等に係る本省宛ての手続の内容確認・審査等を実施する。</td></tr>
<tr><td colspan="2">経済産業局</td><td>各地方に拠点があり、製品安全 4 法に係る手続の内容確認・審査を実施する。</td></tr>
<tr><td colspan="2">産業保安監督部</td><td>各地方に拠点があり、電気事業法・液化石油ガス法・ガス事業法・鉱山保安法・火薬取締法等に係る手続の内容確認・審査を実施する。</td></tr>
</table>

	地方自治体	地方自治体宛の手続の内容確認・審査を実施する。	・ 対象手続に関する知識レベルが高い。 ・ 次期システムからの新規利用者である。 ・ 自治体によっては、システムにアクセス可能な端末が限られる可能性あり。

(2) ユーザビリティ要件

画面の構成やデザイン及び操作方法について、基本的には現行システムと同等の要件とする。以下に、詳細のユーザビリティに係る要件を示す。

表 4-2 ユーザビリティ要件一覧

ユーザビリティ要件分類	ユーザビリティ要件
画面の構成	• 統一感があり、利用者が直感的に操作内容を理解できるような画面構成にすること。 • 無駄な情報、デザイン及び機能を排し、利用者にとって簡潔で分かりやすい画面にすること。 • 画面ウィンドウに縦スクロールを使用する場合には、作成更新処理を実行するためのボタンと、その他の常に画面に表示されている必要のあるボタンを精査し、固定して表示する場所(フッタ部等)に配置するなど、利用者の利便性に配慮した構成(スクロールの手間がかからない画面構成)とすること。 • 不要な画面遷移をせず、画面遷移の数は最小限に抑えること(検索条件の入力と検索結果の表示とが単一の画面で行える等)。 • 確認画面等を設け、利用者が行った操作、入力の取消し、修正、その他操作が容易にできるようにすること。 • ユーザの意思で前の画面に自由に戻ることができ、入力内容を修正することができること。 • 作業中断しても、随時再開できるように操作を一時的に保存できる機能を有することとし、作業を随時保存し、途中断面で適切に再開できること。 • 効率よく作業を行うことが可能な分かりやすい画面構成とすること。 • 十分な視認性のあるフォント及び文字サイズを用いること(文字サイズを拡大したとしても破綻しないこと)。 • スマートフォン、PC、タブレットなどマルチデバイスに対応した画面を設計すること。 • ユーザの使用環境に応じて、画面の大きさや位置の変更が適切かつ容易にできること。 • その他機能については、主管課と相談の上決定すること。
操作方法の分かりやすさ	• 無駄な手順を省き、最小限の操作、入力などで利用者が作業できるようにすること。 • 画面上の入出力項目値の再利用を容易にするため、各入出力項目のコピー・貼付けができるようにすること。 • 操作効率と操作柔軟性の向上のため、複数の操作手段・入力手段(ショートカット、アクセラレータキー、マウス、キーボード等)を用意すること。 • 業務の効率化を図る観点から、操作の容易性と誤操作の防止に配慮すること。 • 用語、指示及びデザイン(ページ、ボタン等)には、サービス全体で一貫性を持たせること。 • 操作の指示、説明、メニュー等には、利用者が正確にその内容を理解できる用語を使用すること利便性に影響を与える機能の開発・改修を行う場合、開発期間中においては思考発話法を用いてユーザビリティテスト(プロトタイプを利用者に操作してもらう)を実施し、その場で得られたユーザの意見を分析し優先順位を付け開発に取り込むこと。リリース後においては、アクセス解析を行いユーザの行動を分析し A/B テストもしくは多変量テストを継続的に実施し、より効果が得られる手段を採用し続けること。 • 継続的な改善を行えるよう、アクセス解析、テスト、ユーザ行動分析などが実施できる環境を採用すること。 • ユーザの行動(閲覧、入力、ページ遷移、ページ滞留時間など)を計測できること。
指示や状態の分かりやすさ	• 必須入力項目と任意入力項目の表示方法を変える等、各項目の重要度を利用者が認識できるようにすること。 • ユーザの操作に応じて、入力項目の追加、入力条件(必須⇔任意)が動的に行われる場合は、遅滞なくユーザが認識・操作できるように支援すること。 • 利用者の誤操作を防ぐため、また、利用者の円滑な操作を補助するため、適宜、適切なエリアにメッセージを

ユーザビリティ要件分類	ユーザビリティ要件
	表示すること(メッセージの内容は、指摘内容、指摘の理由(参照箇所など含む)、対応方法などをわかりやすく表示すること)。 • 入力や各種操作について、問題があればエラーを検出し、適宜エラーメッセージを表示すること。 • システムが処理を行っている間、ブラウザの機能等を用いることで、処理の経過状況について利用者が直ちに分かるようにすること。 • ユーザが複数の画面を経て操作を行う場合、全体としていくつの画面が存在するのか分かるようにすること。また、直前・直後の操作に何が有るのかについてユーザが理解できるようにすること。
エラーの防止と処理	• 利用者の誤操作及び誤入力を防止するような仕組み又は案内を提供すること。 • ユーザ自身の操作を円滑に進めるため入力補助機能及び入力漏れ/間違いのチェック機能を有すること。 • 入力内容の形式に問題がある項目については、それを強調表示する等、利用者がその都度、該当項目を容易に見つけられるようにすること。 • 重要な処理については事前に注意表示を行い、利用者の確認を促すこと。 • エラーが発生した際は、利用者が容易に問題を解決できるよう、エラーメッセージ、修正方法等について、分かりやすく十分な情報提供をすること。 • 入力内容の形式に問題がある項目については、それを強調表示する等、利用者がその都度その該当項目を容易に見つけられるようにすること。 • 他のコンテンツで入力項目、テキストなどを隠さないこと。
ヘルプ	• ヘルプ情報、マニュアル、その他利用者を補助する情報等を参照できるようにすること。

(3) アクセシビリティ要件

次期保安ネットのアクセシビリティは、日本産業規格 JIS X8341 の適合レベル AA 及び経済産業省ウェブアクセシビリティ指針等を考慮したうえで、現行保安ネットと同等の要件とする。以下に、詳細のアクセシビリティに係る要件を示す。

- 画面の設計構築時は、日本産業規格 JIS X8341 の適合レベル AA、経済産業省ウェブアクセシビリティ指針等を考慮すること。
- データ設計は共通語彙基盤を参照して行うこと。
- 共通語彙基盤に定義されていない項目については自由に設計が可能であるが、データの構造化を行い再利用しやすいデータとすること。
- 十分な視認性のあるフォントと文字サイズを用いること。
- 文字サイズを変更できること。
- ユーザへの情報伝達や操作指示を促す手段はメッセージを表示する等とし、可能な限り色のみで判断するようなものは用いないこと。

2. システム方式に関する事項

次期保安ネットはクラウド・バイ・デフォルト原則にのっとり、クラウドサービスの利用を原則とすること。なお、合理的な理由のない限りマネージドサービスを活用し、インフラ・アプリのモダン化に努めること。

また、次期保安ネットの開発は可能な限りノーコード/ローコードによる開発が可能なソフトウェア製品を活用すること。

(1) 情報システムの構成に関する全体の方針

表 4-3 情報システムの構成に関する全体の方針一覧

全体方針の分類	全体方針
システムアーキテクチャ	• システムのシステムアーキテクチャは、Web サーバ型とすること。 • 利用者の端末に追加でソフトウェアのインストール等を行うことなく、一般に利用されている Web ブラウザで処理を行うものとすること。 • クラウドサービスの利用によるコスト削減や継続的な運用改善等の効果を高めるために、可能な限りモダンな技術を用いてアプリケーション開発を行うこと。なお、本項でいう「モダンな技術」の具体的な内容については「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針（案）令和 4 年 9 月 30 日公開版」を参照すること。
アプリケーションプログラムの設計方針	• システムを構成する各コンポーネント(ソフトウェアの機能を特定単位で分割したまとまり)間の疎結合、再利用性の確保を基本とすること。 • Web アプリケーションの開発は、原則として HTML5 や CSS3 などの Web 標準技術を使用し、特定のブラウザに依存する技術(ActiveX や Flash などプラグインを用いた技術や、Internet Explorer 独自に定められたタグ等)は極力利用しないこと。 • 特定 の入力情報に起因し処理がエラーとなって場合においても、正常な他の入力情報に係る処理は継続可能となること(例：特定の事業者から提出された調査票の内容に不備がありエラーとなった場合も、別の事業者から提出された同一種別の正常な調査票は処理可能である等)。
文字コード及び文字の符号化形式の方針	• 取り扱う日本語文字集合の範囲は、JIS X 0213 とすること。 • 文字コードは、ISO/IEC 10646 とすること。 • 文字の符号化形式は、UTF-8 とすること。 • JIS X 0213:2012 の範囲外の文字の入力はエラーとし、代替文字で入力するように案内すること。 • 代替文字は、国税庁の法人番号サイトで提供する文字とし、JIS X 0213 の範囲外であるが、代替文字のない法人名については、当該部分をカタカナで記載すること。 • 氏名で取り扱う日本語文字集合の範囲は文字情報基盤とし、外字の作成は行わない • システム処理で氏名を扱う必要がある場合には、代替文字の入力を戸籍文字に合わせて行うこと。 • 利用者との入出力以外は代替文字で処理を行い、できる限り戸籍文字での運用範囲を限定すること
基本的なデータの記述形式の方針	• 日付時刻、住所、郵便番号、電話番号については、行政基本情報データ連携モデルを参照すること。 • 氏名データは、「氏」と「名」を別データ項目で設定すること。 • 氏名データはフリガナデータを持つこと。 • データの記述方式は現行システムからの移行容易性を鑑み、現行システムのデータ設計を参考とすること。
データベースの設計方針	• データの構造化に対応すること。 • 可能な限り schema.org に対応すること。

全体方針の分類	全体方針
	• データベースの設計は現行システムからの移行容易性を鑑み、現行システムのデータ設計を参考とすること。
ソフトウェア製品の活用方針	• 広く市場に流通し、利用実績を十分に有するソフトウェア製品を活用すること。 • アプリケーションプログラムの動作、性能等に支障を来さない範囲において、可能な限りオープンソースソフトウェア(以下「OSS」という。)製品(ソースコードが無償で公開され、改良や再配布を行うことが誰に対しても許可されているソフトウェア製品)の活用を図ること。ただし、受託者は、利用するソフトウェアはサポート期間を考慮して選定し、ソフトウェアベンダによるサポート又は他の事業者によるサポートサービスを必ず受けること。 • 特に OSS 製品を利用しない場合(商用／独自フレームワークを利用する場合など)は、第三者がソフトウェアの構造や仕様を理解できるよう、十分な情報(製品の情報や拡張機能に関する情報等)提供を行うなど、配慮すること。 • ノンプログラミングによる画面生成等プロトタイピング用のツール等を利用することにより、システムライフサイクルコストの削減等が見込める場合には、積極的に採用を検討すること。
システム基盤の方針	• クラウド・バイ・デフォルト原則にのっとり、クラウドサービスの利用を原則とすること。また、クラウドサービスの利用に当たってはクラウドスマートを検討すること。その他クラウドサービスの利用に関しては「政府情報システムにおけるクラウドサービスの利用に係る基本方針(2022 年 9 月 30 日)」の記載内容に従うこと。 • 構成等については、業務要件及び非機能要件を踏まえ、受託者において適切なものを提案すること。 • 採用するクラウドサービスの選定に当たっては、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」(2021 年(令和 3 年)3 月 30 日各府省情報化統括責任者(CIO)連絡会議決定)の記載内容に従うこと。 • システムの設計構築に係るコストを低減させるため、可能な限り環境プロビジョニングサービス(Infrastructure as Code の概念に基づいて、環境構築用のテンプレートに各種パラメータ情報を入力し、テンプレートを実行することで環境構築に係る作業を自動化するサービス)を利用すること。 • 将来的な電子化対象となる手続の追加を見据え、申請書・ワークフロー等の機能追加やデータ量増加に係る拡張が容易なクラウドサービスの利用を検討すること。

(2) システム全体構成

次期保安ネットのシステム構成概要図を以下に示す。

下図は国向けの「次期保安ネット」のシステム構成を示しているが、地方自治体向けの次期保安ネットもほぼ同様(ただし、「他政府システム連携」及び「決済」を除く。)のシステム構成の想定である。そのため、地方自治体向け次期保安ネットのシステム構成については、国向けの次期保安ネットのシステム構成をベースとし、設計構築工程にて主管課と協議のうえ基本設計(方式設計等)としてまとめること。

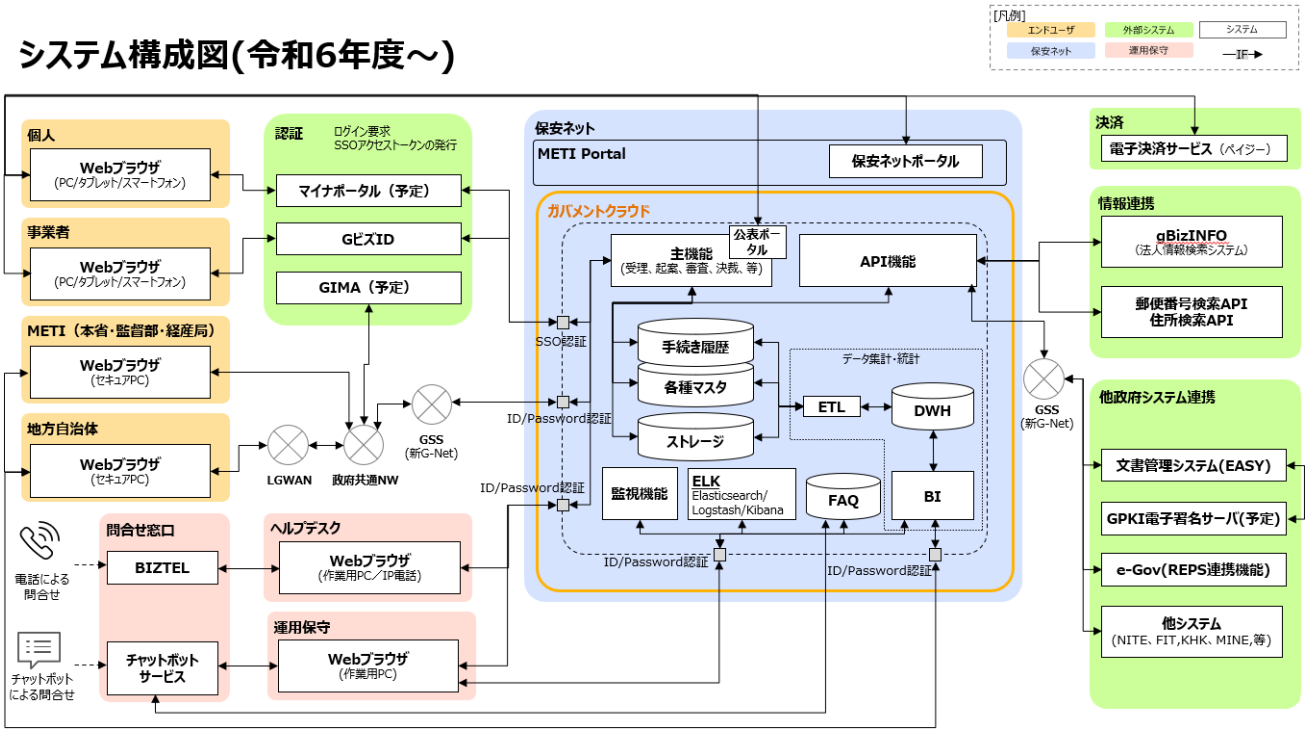

図 4-1　次期保安ネットシステム構成概要図

(3) 開発方式及び開発手法

次期保安ネットの開発は可能な限り、ノーコード/ローコードによる開発が可能なソフトウェア製品を活用すること。また、クラウドサービスから提供される機能等を活用することにより、システムライフサイクルコストの削減等が見込める場合には、積極的に採用を検討すること。なお、活用する機能等は、以下の要件を充足するものであること。また、クラウドサービスから提供される機能を利用するにあたり、可能な限り、主管課にて利用実績が確認できる手法を積極的に採用すること。

- 活用する機能は、本書に記載されている要件を満たしたものであること。
- 受託者が、クラウドサービスや活用するクラウドサービスの機能について習熟していること。

システムの開発手法はウォータフォール型を想定しているが、実現機能の一部について、プロトタイプ開発(システムのモックアップや簡単な試作品(プロトタイプ)を行い、ユーザによるプロトタイプの評価が行われてから本格的な設計を開始する開発手法)を併用することを妨げない。なお、開発における受託者の責任に係る要件を以下に示す。

- 受託者は設計構築の管理主体者として設計構築管理を実施すると共にその結果と品質に責任を負うこと。
- 開発を行うにあたり、受託者の体制並びにメンバーの責任及び役割を明確にすること。
- 開発環境は、受託者の負担と責任において確保すること。

3. 規模に関する事項

(1) 機器数及び設置場所

次期保安ネットの構築環境はクラウド利用を想定しているため、サーバ等の機器は不要。次期保安ネットの利用に必要な機器を以下に示す。

表 4-4 機器数及び設置場所一覧

機器の区分	機器の用途	機器数	設置場所	補足
PC	保安ネットの利用	-	-	経済産業省が支給するセキュア PC を使用する。 地方自治体は各自治体の基準に従った端末を使用する。

(2) データ量

現行保安ネットにおける各種データ容量から概算で見積もった次期保安ネットのデータ容量を以下に示す。

表 4-5 データ量一覧

データ区分	最大のデータ蓄積量(想定)	補足
届出・申請データ	240GB	永久保存
添付ファイルデータ	120GB	永久保存
各種マスタデータ	100GB	永久保存
ログデータ	50GB	30 日分保存

(3) 処理件数

現行保安ネットにおける各種処理件数から概算で見積もった次期保安ネットの処理件数を以下に示す。

表 4-6 処理件数一覧

項目	処理件数
届出・申請手続	定常時：48,000 件/月 ピーク時：77,000 件/月 ピーク特性：ピークは 4 月を想定。
立入検査結果の入力	定常時：63 件/月 ピーク時：-
統計資料(年報等)の作成	定常時：2~12 件/月 ピーク時：- ピーク特性：-

(4) 利用者数

「第 2 章 業務要件定義　3. 規模」を参照すること。

4. 性能に関する事項

(1) 応答時間

次期保安ネットのオンライン処理及びバッチ処理の目標応答時間を以下に示す。

表 4-7 目標応答時間一覧

設定対象		指標名	目標値	応答時間達成率
オンライン処理	画面遷移	レスポンスタイム	• 定常時： 1 秒以内 • ピーク時：3 秒以内	平均を目標値とする。
	検索処理	レスポンスタイム	• 定常時：3 秒以内 • ピーク時：5 秒以内	平均を目標値とする。
	データ処理	レスポンスタイム	• 定常時：3 秒以内 • ピーク時：5 秒以内	平均を目標値とする。
	ファイルアップロード/ダウンロード	レスポンスタイム	• 定常時：30 秒以内 • ピーク時：60 秒以内	平均を目標値とする。
バッチ処理	データ処理	レスポンスタイム	• 全ての夜間バッチ処理が翌開庁時間までに終了すること。 • 再実行の余裕が確保できる範囲であること。	平均を目標値とする。

(2) スループット

スループットの目標値については、設計構築時に設定を行う方針とする。

5. 信頼性に関する事項

(1) 可用性要件

次期保安ネットは広域災害を想定しデータを遠隔保管(他リージョン保管)することで広域災害時もデータを保護できコスト効果の高い構成とすること。また、通常時の負荷分散及び障害発生時の縮退運転を可能とすること。可用性に係る指標及び目標を以下に示す。

表 4-8 可用性要件一覧

設定対象	指標名	目標値	補足
保安ネット	サービス時間	24 時間 365 日	計画停止／定期保守を除く。
	計画停止予定通知	5 日前に保安ネットポータルで通知	-
	稼働率	99.8%	-
	ディザスタリカバリ	有	他リージョンで保管した定期バックアップデータによる復帰。

(2) 完全性要件

次期保安ネットの可用性に係る要件を以下に示す。

- クラウドサービスのリージョン障害に起因するデータの消失や破損を防止すること。
- 異常な入力や処理を検出し、データの滅失や改変を防止すること。
- 処理の結果を検証可能とするため、ログ等の証跡を残すこと。
- データの複製や移動を行う際に、データが毀損しないよう、保護すること。
- データの複製や移動を行う際にその内容が毀損した場合でも、毀損したデータ及び毀損していないデータを特定できること。
- システム運用・保守担当者及び業務運用担当者が誤操作を行った場合にも、容易にデータが消去されることのないようにすること。
- データの送受信が確実に実行できるようにすること。また、実行されなかった場合、その結果が確実に検知できるようにすること。

6. 拡張性に関する事項

(1) 性能の拡張性

「3. 規模に関する事項」に示した次期保安ネットの業務量及び処理件数について、法令改正や制度変更に伴う、業務の追加・変更によって業務量及び処理件数の増加する可能性がある。そのため、業務量及び処理件数増加に伴う拡張性を考慮し、必要に応じて性能の拡張が可能であるように、以下の対応を実施すること。なお、「3. 規模に関する事項」に示した次期保安ネットの業務量、処理件数を超過する事象によるリソース不足が発生した場合に備え拡張性を確保すること。

- 将来の法令改正や制度変更に伴う業務の追加・変更等に対する拡張性を考慮し、必要に応じて性能の拡張が可能であるように柔軟性を持たせること。
- 利用者の増加、アクセスの増加、データ量の増加等に対して、サーバやディスクの増強、負荷分散等が容易に対応可能な拡張性と柔軟性を確保すること。

(2) 機能の拡張性

法令改正や制度変更に伴う業務や機能の追加・変更に対する拡張性を考慮し、必要に応じて機能拡張が可能であるように、以下の対応を実施すること。

- 利用者ニーズ及び業務環境の変化等に最小コストで対応可能とするため、システムを構成する各コンポーネント(ソフトウェアの機能を特定単位で分割したまとまり)の再利用性を確保すること。
- 機能、画面、帳票等において固有の ID・項目名等を付する際には、中長期的な重複等を避けつつ可読性を担保するため、あらかじめ系統だった命名ポリシーを策定すること。その際、一見して意味が通じない命名はしないこととし、同種の項目を複数設定する必要がある場合には各項目の性質の違いが分かるように留意すること。
- 将来の制度の変更、対象業務の追加等の変化に対する拡張性を考慮し、必要に応じて機能の拡張が可能であるように柔軟性を持たせること。

7. 上位互換性に関する事項

(1) 上位互換性に関する要件

次期保安ネットにおける、上位互換性に係る要件を以下に示す。上位互換性要件を遵守し、製品を選定すること。

- サーバ OS は特定バージョンに依存する機能がない限り最新バージョンを導入すること。
- サーバ OS のバージョンアップに備え、OS の特定バージョンに依存する機能が判明している場合は、その利用を最低限とすること。
- 特定の Web ブラウザに依存する機能が判明している場合は、その利用を最低限とすること。また、主な利用環境として想定する Web ブラウザを一定の範囲に限る場合でも、対象ブラウザのバージョンアップに備え、対象ブラウザの特定バージョンに依存する機能が判明している場合は、その利用を最低限とすること。
- Web ブラウザ及び実行環境等のバージョンアップの際、必要な調査及び作業を実施することで、バージョンアップに対応可能なシステムとすること。
- OS・ミドルウェア等の選定に当たっては、各製品のバージョンアップのポリシーにも留意し、バージョンアップが頻繁に行われる製品を選定する際には、バージョンアップ時のテスト内容の簡略化等を検討すること。
- 次期バージョンで互換性を持たないことが発表されているソフトウェアは次期保安ネットで導入しないこと。

8. 中立性に関する事項

(1) 中立性に関する要件

次期保安ネットにおける、中立性に係る要件を以下に示す。受託者は、中立性要件を遵守し、製品を選定すること。

- プログラミング言語については、市場における技術者の確保の容易性に留意しつつ、ISO/IEC 等の国際規格として整備されているものの採用を考慮すること。
- 導入するソフトウェア等の構成要素は、標準化団体(ＩＳＯ、ＩＥＴＦ、ＩＥＥＥ、ＩＴＵ、ＪＩＳＣ等)が規定又は推奨する各種業界標準に準拠すること。
- ノンプログラミングによる画面生成等プロトタイピング用のツール等を採用する場合には、当該ツールは中立性の観点から問題ないものを選定すること。
- 次期システム更改の際に、移行の妨げや特定の装置や情報システムに依存することを防止するため、原則としてシステム内のデータ形式は XML、CSV 等の標準的な形式で取り出すことができるものとすること。
- 特定の事業者や製品に依存することなく、他の事業者がシステムの運用・保守作業やシステムの更改作業を引き継ぎ、実施することが可能なシステム構成であること。

9. 継続性に関する事項

(1) 継続性に係る目標値

次期保安ネットの目標復旧時間及び目標復旧時点を以下に示す。

表 4-9 継続性に係る目標値一覧

目標復旧時間	目標復旧時点
12 時間以内	障害発生時点(日次バックアップ＋アーカイブからの復旧)

(2) 継続性に係る対策

次期保安ネットのバックアップ及びリカバリに係る要件を以下に示す。なお、開発時において以下の要件について実現性等で困難な場合は、主管課と協議の上、対応を決定すること。

表 4-10 継続性要件一覧

要件分類	継続性に係る要件
バックアップ、リカバリに係る要件	• データベースは日次でオンラインバックアップを取得し、制御ファイル及び変更ログはリアルタイムでバックアップを取得すること。 • データベースに障害が発生した場合は、日次バックアップデータ及び制御ファイル、変更ログをもちいて障害発生時点にリカバリすること。 • システムバックアップは、パッチ適用等システム構成変更作業前後に取得し、2 世代管理とすること。 • pdf 等の文書ファイルは日次で災対環境へバックアップを取得すること。 • システムに係るデータはすべてバックアップ対象とし、災対環境へ遠隔地保管及び災対環境内のシステムで使用可能な状態にすること。 • 誤操作又は障害によるデータの改変、減失の発生等に使用するリカバリ手順書を整備すること。 • データベースのデータの保持期間は無期限とし、pdf 等のファイルデータ、ログデータに係るバックアップデータの保持期間は標準文書保存期間基準に準ずること。 • オペレーションミスを防ぐためバックアップは自動取得を基本とすること。ただし、開発時バージョン管理や運用中のバッチ適用前取得等のため、手動取得も行えるようにもすること。 • バックアップの取得については、クラウドサービスプロバイダから提供されるバックアップサービスを利用して差し支えない。ただし、利用するサービスの種類、同時被災しないことを前提としたバックアップサイトの場所、バックアップデータの取得時期及び保持期間(世代管理を含む)、自動化の程度等については、対象とするデータの性質等に応じて、業務に影響を与えず、かつコスト最適となるものを選定すること。
大規模災害等に係る業務継続計画に関する要件	• 大規模災害時のサービス継続性の確保のため、通常時稼働しているメインサイトの他に地理的に離れた地点に災対環境を設置し、メインサイトが被災した際にはメインサイトから災対環境への切替えを想定している。災対環境の構成については、継続性に関する要件を満たし、コストが最低限となる構成とすること。 • 災対環境で業務を再開するまでの間は、代替業務として旧来通りの紙を用いた申請及び処理を行えること。

10. 情報セキュリティに関する事項

「経済産業省情報セキュリティ管理規程」、「経済産業省情報セキュリティ対策基準」、「政府機関等の情報セキュリティ対策のための統一基準群」、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」に準拠した情報セキュリティ対策を講ずること。

(1) 情報セキュリティ対策要件

次期保安ネットにおける情報セキュリティ対策も概要を以下に示す。

- システムへのアクセスを業務上必要な者に限るための機能を具体化し、実装すること。
- 「安全なウェブサイトの作り方(改訂第 7 版)」に準拠し、実装すること。
- システムに対する不正アクセス、ウイルス・不正プログラム感染等、インターネットを経由する攻撃、不正等への対策機能を具体化し、実装すること。
- システムにおける事故及び不正の原因を事後に追跡するための機能(システムに含まれる構成要素(サーバ装置・端末等)のうち、時刻設定が可能なものについては、システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定すること)を具体化し、実装すること。
- システムがスパムメールの標的とならないような処置を行うこと

情報セキュリティ対策に係る要件を以下に示す。

表 4-11 情報セキュリティ対策要件一覧

情報セキュリティ対策	対策に係る要件
通信回線対策の実施	• 不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離すること。 • 通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。 • 情報システムのなりすましを防止するために、サーバの正当性を確認できる機能を備えること。 • 情報システムで取り扱う通信について、通信内容の秘匿性を確保するため、暗号化プロトコルとして TLS1.2 のみ通信可能な設定とすること。 • 「TLS 暗号設定ガイドライン(第 3.0.1 版)」に準拠すること。 • サービスの継続性を確保するため、構成機器が備えるサービス停止の脅威の軽減に有効な機能を活用して情報システムを構築すること。 • 職員が利用するシステムは IP アドレスによるアクセス制御を実装すること。なお、アクセス許可を行う IP アドレスについて、主管課庁へ確認を行うこと。
不正プログラム対策の実施	• 不正プログラム(ウイルス、ワーム、ボット等)による脅威に備えるため、想定される不正プログラムの感染経路のすべてにおいて感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。 • 不正プログラム対策として、事業者から提出された文書データ(添付書類や報告に係る CSV ファイル)に対してリアルタイムスキャンを行い、週に 1 度システム全体のファイルに対してフルスキャンを実行すること。

情報セキュリティ対策	対策に係る要件
	• システム全体として不正プログラムの感染防止機能を確実に動作させるため、当該機能の動作状況及び更新状況を一元管理する機能を備えること。
脆弱性対策の実施	• 第三者による脆弱性検査を実施し、その結果を担当課室に書面にて報告すること。 • 確認された脆弱性情報について、対処の要否、可否を判断すること。対処したものに関して対処方法、対処しなかったものに関してその理由、代替措置及び影響を報告すること。決定した対処又は代替措置を実施すること。
ログ管理の実施	• 情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関するログを蓄積し、１年間以上(※1)の期間保管するとともに、不正の検知、原因特定に有効な管理機能(ログの検索機能、ログの蓄積不能時の対処機能等)を備えること。 ※1:内閣官房内閣サイバーセキュリティセンターの「政府機関等の対策基準策定のためのガイドライン（令和３年度版）」に記載の推奨期間(１年以上)に可能な限り準拠すること。 • ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能を備えるとともに、ログのアーカイブデータの保護(消失及び破壊や改ざん等の脅威の軽減)のための措置を含む設計とすること。 • 利用記録には、アクセス日時、アクセスしたユーザ、アクセス元、アクセス先を収集できること。 • 利用記録は、標準的な形式で保存すること(製品依存の独自形式でないこと)。または、平易にCSV 形式等の標準的な形式に変換できること。 • 内部からの不正操作、ユーザの誤操作等による情報セキュリティ上の脅威に対応するため、管理者権限操作を含めた証跡を取得すること。 • 具体的な収集情報・保管期間については主管課と協議の上、決定すること。
不正監視の実施	• 不正行為に迅速に対処するため、通信回線を介して所属する府省庁外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知及び通知する機能を備えること。 • サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバや通信回線等の過負荷状態を検知する機能を備えること。
主体認証の実施	• 情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体のうち申請者認証(事業者)を行う機能として、Ｇビズ ID と API 連携し、認証を行うこと。 • 情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体のうち申請者認証(個人)を行う機能として、マイナポータルと API 連携し、認証を行うこと。 • 情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体のうち担当課室職員においては、閉域ネットワーク(新 G-Net)から職員認証サービス(GIMA)を利用した認証を行うこと。 • 情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体のうち地方自治体においては、システム独自の認証機能を実装すること。また、認証機能についてはセキュリティの観点から多要素認証の方式を採用すること。 • 情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体のうち運用・保守業務担当者においては、システム独自の認証機能を実装すること。また、認証機能についてはセキュリティの観点から多要素認証の方式を採用すること。
機密性・完全性の確保の実施	• 通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信回線を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。 • 情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機

情報セキュリティ対策	対策に係る要件
	能を備えること。また、保護すべき情報を利用者が直接アクセス可能な機器に保存しないことに加えて、保存された情報を暗号化する機能を備えること。 • 暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。 • 情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。
構成管理の実施	• 情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成(仮想サーバ、ソフトウェア及びサービス構成に関する詳細情報)が記載された文書を提出するとともに文書どおりの構成とし、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。
情報セキュリティが侵害された場合の対処	• 情報セキュリティが侵害又はそのおそれがある場合には、速やかに担当課室に報告すること。これに該当する場合には、以下の事象を含む。 ➢ 受託者に提供し、又は受託者によるアクセスを認める担当課室の情報の外部への漏えい及び目的外利用 ➢ 受託者による担当課室以外の情報へのアクセス
製品サポート期間の確認	• システムの構築等又は運用・保守・点検の際に導入する製品(ソフトウェア)については、システムのライフサイクル(システム利用期間の終了まで)におけるサポート(セキュリティパッチの提供等)が継続される製品を導入すること。なお、システムの契約期間は 1 年を想定している。具体的な製品・技術の選定に当たっては、「政府情報システムにおけるサポート終了等技術への対応に関する技術レポート」(2021 年(令和 3 年)8 月 31 日 内閣官房情報通信技術(IT)総合戦略室)等を参照すること。また、システム更改の設計構築期間を含めライフサイクルは 5 年を想定している。
情報セキュリティ対策の履行状況の報告	• 情報セキュリティ対策の履行状況について、担当課室から以下の報告を求めた場合には速やかに提出すること。 ➢ 本調達仕様において求める情報セキュリティ対策の実績
情報セキュリティ監査への対応	• 主管課が別途実施する第三者による情報セキュリティ監査に対応すること。
情報セキュリティ対策の履行が不十分な場合の対処	• 本調達に係る業務の遂行において、受託者における情報セキュリティ対策の履行が不十分であると認められる場合には、受注者は、主管課と協議を行い、合意した対応を実施すること。
IT セキュリティ評価及び認証制度に基づく認証取得製品の採用	• システムを構成するソフトウェア、機器等について、IT セキュリティ評価及び認証制度に基づく認証を取得している製品を積極的に採用すること。 • 採用に当たっては、以下の資料を参照すること。 ➢ 「 IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック（平成 30 年 2 月 独立行政法人情報処理推進機構）」 ➢ 「IT 製品の調達におけるセキュリティ要件リスト（平成 30 年 2 月 28 日 経済産業省）」
クラウドサービス利用時の取扱い	• 情報セキュリティ対策の実施に当たっては、適宜クラウドサービスプロバイダから提供されるサービスを利用すること。
セキュリティ診断	• ネットワーク診断及び Web 診断、DB 診断の実施及びセキュリティリスクが存在しないことの確認を行う。セキュリティリスクが存在する際は、対応期限及び対応方法を提示し、主管課と合意を得ること。
システム上の対策における操作制限度	• ソフトウェアのインストールや利用制限等、必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可すること。

情報セキュリティ対策	対策に係る要件
アクセス制御・権限管理	• ユーザアカウントは次期保安ネットにおける作業者の役割毎(各種システム操作を含む)に作成し、作業に必要な権限のみの付与等、目的に応じた適切なアクセス制限、権限管理及び設定を行うこと。 • 審査・承認者側システムのアクセスは経済産業省が認めたものに限り、アクセス元の IP アドレスを限定すること。 • 申請者(事業者)の権限は Ｇビジネス ID に準拠するものとするが、特定のグループ化などの権限管理も可能とすること。 • 審査者の権限は階層にて管理し、アクセス可能なデータ範囲の設定を可能とすること。
その他セキュリティ要件	• インターネット接続回線を含む次期保安ネットを攻撃目標とした分散サービス不能攻撃に対し、可能な限り防御するための対策を実施すること。 • 次期保安ネットの機器が踏み台として使われることを防止するための措置を可能な限り講ずること。 • メールサーバが不正に利用されないよう、不正中継を防止する設定、メールクライアントの主体認証、なりすましの防止、不正プログラムの実行防止等の措置を講ずること。

11. 情報システム稼働環境に関する事項

(1) 情報システム稼働環境に関する要件

次期保安ネットはクラウド・バイ・デフォルト原則にのっとり、クラウドサービスの利用を原則とすること。クラウドサービスの構成に係る要件を以下に示す。

- 次期保安ネットの稼働環境(本番環境、検証環境、含む)をガバメントクラウド若しくは「政府情報システムのためのセキュリティ評価制度(ISMAP)」において登録されたクラウドサービスを利用すること。なお、ガバメントクラウドを利用する場合は「2. システム化方針に関する事項 (1) 情報システムの構成に関する全体の方針」に示すアプリケーションのモダン化は必須となることに留意すること。
- 次期保安ネットに求められる要件(機能要件、非機能要件)に応じたクラウドサービスを活用すること。
- クラウドサービスの構成については主管課へ提案、承認を得たうえで構築すること。
- システム監視のクラウドサービスを活用すること。
- 契約終了時に、すべての情報を復元できないように抹消すること。なお、受注者は取り扱われた情報が確実に抹消されたことを確認すること。
- マルチテナントアーキテクチャを採用している場合には、データの保護やリソースの管理等、十分な対策が行われていること。
- 利用するクラウドサービスで提供される仮想サーバ等の可用性に係る SLA に留意し、各構成要素について適切に冗長化等を行うこと。ただし業務に係る仮想サーバ等の冗長化を行い、業務に係らない仮想サーバ等は適宜冗長化を行わないこと。
- バックアップの取得については、クラウドサービスプロバイダから提供されるバックアップサービスを利用して差し支えない。ただし、適用するサービスの種類、同時被災しないことを前提としたバックアップサイトの場所、バックアップデータの取得時期及び保持期間(世代管理を含む)、自動化の程度等については、対象とするデータの性質等に応じて、業務に影響を与えず、かつコスト対効果が高いものを適宜選定すること。

12. テストに関する事項

(1) テストに関する要件

受託者は各種要件に対する十分なテストの実施を行うこと。なお、経済産業省が設定するマイルストンにおいて設計構築等業務に関する品質状況を報告し、適切な品質が担保されていることを確認できるようにすること。

なお、当該マイルストンにおいて十分な品質を確保していないと経済産業省が判断した場合、受注者がコンティンジェンシー計画書において予め定めたとおり、進捗・品質状況を改善するための是正を行うことや、受注者にて用意した、現行システムの本番環境と同等な環境、アプリケーションを移行したり、または、現行システムの稼働延長を現行システム事業者に依頼したりすること等、設計構築等の進捗に拘わらず確実に保安ネットのサービスを継続させるためのコンティンジェンシー計画を発動すること。

表 4-12 テストの種類(案)

テストの種類	テストの目的、内容	テスト環境	テストデータ
単体テスト 結合テスト 総合テスト	• テストの目的、スケジュール及び環境要件を設定するとともに、作業手順や成果物の作成標準を規定し、テストの品質を確保すること。 • テストの妥当性を定量的に検証するためのテスト項目数等の指標を策定し、主管課の承認を得ること。 • 設計書等の記述内容を網羅的に確認できるテスト項目を作成すること。 • テスト項目は、品質を確保するために十分なケースが定義されており、計画時に策定した指標が満たされることを検証すること。 • テスト実施後は、計画時に策定した指標とテスト結果を用いて、品質が確保されていることの確認を行うこと。 • テストデータ、テスト用プログラム及び各テスト項目に対する想定結果等を作成し、テスト開始前までに必要十分な準備を行っておくこと。 • 非機能要件テストに必要なツールやシステムを構築すること。 • 性能要件を満たしていることをパフォーマンス検証により確認すること	テスト環境は受注者にて準備すること。	原則として設計構築事業者が擬似データを作成して用いること。ただし、外部の連携情報システムとの調整を踏まえて作成分担を決定すること。
受入テスト	• 主管課が受入テストを行うに当たって必要な支援を行うこと。 • 主管課が各種要件の確認を行うための確認手順書を作成すること。	受入テストは本番環境にて行うため、システムを稼働させるための各種移行作業を本番環境に対し実施すること。	受け入れテストのテストデータは主管課と協議の上で必要に応じて準備すること。

13. 移行に関する事項

保安ネットは申請者(事業者)からの申請・届出を 24 時間 365 日受け付けているシステムであり、現行保安ネットから次期保安ネットへ移行するにあたっても、業務の継続性を担保し、利用者への影響を最小限とする必要がある。

(1) 移行に係る作業区分

移行に係る作業区分を以下に示す。以下の区分に則して移行計画の策定及び移行手順の検討を実施すること。

表 4-13 移行作業区分

作業区分	作業概要
データ移行	現行保安ネットにて管理されているデータ、及び各課室が独自に管理しているデータを次期保安ネットで利用可能にするための一連の作業。 次期保安ネットの機能要件に即して既存データを加工する作業を含める。
業務移行	次期保安ネット稼働後に、保安ネット利用者が申請・届出等の業務を実施可能にするための一連の作業。
システム移行(切替)	サーバ、ネットワーク、アプリケーション等を次期保安ネットで利用可能にするための一連の作業。 現行保安ネットを停止し、データ移行・業務移行以外に必要となるすべての作業を実施した上で、次期保安ネットを稼働するための一連の作業を本区分の範囲とする。

(2) 移行計画書の作成

次期保安ネットへの移行にあたり、設計構築事業者は業務開始後 1 か月以内の早期に移行計画書を作成し、主管課の承認を得た上で関係部署・機関との調整を開始すること。なお、移行計画書には、移行概要、移行対象、スケジュール、外部システムを含めた作業体制、利用する環境、移行方法及び使用するドキュメントとその定義を含めること。

また、万一次期保安ネットへの移行に失敗した場合においても、事前に計画しておいた「コンティンジェンシー計画」を発動することで、現行保安ネットと同等の業務の継続を可能とすること。

移行計画書を作成するにあたっての要件を以下に示す。

ア. 計画書作成要件

(ア) 共通

- 技術、外部要因、組織またはプロジェクトマネジメント等の複数の観点で、本件と類似する案件で発生した問題等から、移行計画策定時点から移行実施までの間において、想定リスクを識別し、抽出すること。
- 抽出されたリスクについて定性的、または定量的な分析を行った上で、回避、転嫁、軽減及び受容等の対応計画を作成すること。
- リスクが顕在化した場合に備え、現行保安ネットを継続して稼働させること等によって業務の継続を担保す

るためのコンティンジェンシー計画書を作成すること。

(イ) データ移行

- 「別紙 4-1　移行対象データ一覧」に示すデータを次期保安ネットへ移行する作業について検討し、計画書へ含めること。
- 現行保安ネットが保有するデータ等については、原則、すべてのデータを次期保安ネットへ移行させること。
- 現行保安ネットでは管理していないが、各課室が独自に管理しているデータのうち、次期保安ネットでは管理対象となるデータを次期保安ネットへ移行させること。
- 現行保安ネットにおける各種ログデータについては、参照可能なファイル形式で次期保安ネット、もしくは外部記録メディア等に保管すること。
- 運用・保守業務の業務継続性を確保するに当たり、インシデント対応状況や作業依頼対応状況等、保安ネットにおいて必要となる運用・保守作業を行うためのデータについて、現行保安ネットの運用・保守事業者と協議の上、データ移行の対象とすること。

(ウ) 業務移行

- 次期保安ネットの業務要件及び機能要件を次期保安ネットにおいて実現するために必要となる作業を検討し、計画書に含めること。
- 保安ネットポータル内の掲載情報の移行について移行計画書に含めること。
- 移行のために利用者(申請者、審査者)が行う作業は、当事者以外では実施不可能であると主管課が判断したもののみとすること。また、これに該当する作業が必要となる場合、特段の専門的知識を必要とすることなく実施可能な作業説明書等を作成するとともに、十分な説明を行うことを移行計画書に含めること。
- 利用者(特に、申請者)への周知すべき事項、周知方法、周知スケジュール、等について移行計画書に含めること。

(エ) システム移行

- 次期保安ネットは、ガバメントクラウド若しくは「政府情報システムのためのセキュリティ評価制度(ISMAP)」において登録されたクラウド上に環境を構築する想定であることを留意すること。
- 連携先の外部システムとの安全かつ確実な移行を実現するため、移行時の作業内容、外部システムに対する影響点や依頼事項、作業スケジュール、連絡体制等を移行計画書に含めること。
- 外部システムとの調整については、本件業務開始後の早期に着手し、外部システム運営主体と密に連絡・調整を図ること。

(3) 移行手順書の作成

移行の事前に実施する準備作業、移行中の作業及び事後に実施する検証作業等を対象とし、移行に係るすべての関係者が個々に利用できる移行手順書を作成し、主管課の承認を得ること。

移行手順書を作成するにあたっての要件を以下に示す。

ア. 手順書作成要件

(ア) 共通

- 移行手順書の作成にあたり、設計構築事業者は、事業開始後の可能な限り早いタイミングで、移行対象データの全量を受領し、移行対象データに含まれるバリエーションを整理した上で、移行プログラムの要件、データクレンジングの実施要否・実施方針を整理するとともに、移行データの確定(断面凍結)のタイミングを主管課と認識合わせすること。
- 移行作業実施に当たり、保安ネットで取り扱うデータは主管課が許可した拠点・環境外への持出しを行わないこと。
- 移行作業の手順に、各作業が正しく行われていることの検証作業も含めること。
- 移行作業中に発生が想定されるトラブル等のリスクを識別し、当該リスクが顕在化した場合に、切り戻しを行う必要性があるか検討の上、必要に応じて、コンティンジェンシー計画を改版し、主管課の承認を得ること。
- コンティンジェンシー計画に定義した、リスク顕在化時の対応計画を実施するための作業手順について、移行手順書に含めること。
- バックアップ等準備作業、移行作業及び事後作業等を対象とし、移行の関係者全体で情報共有できるタイムチャートを作成すること。
- 各課室担当者、外部システムの運営主体、ベンダ等の関係者を含む作業体制図、連絡先一覧を作成すること。
- 正確性及び効率性を考慮し、必要に応じて移行プログラムを作成すること。
- 移行後の検証作業についても、可能な限りプログラムによる自動化を図ること。

(イ) データ移行

- 移行対象データ、移行方式、移行環境、移行後の品質保証方法等の移行設計を行うこと。
- データ移行にあたり、既存データを加工する必要があるデータについては対象データ、データ量、作業手順を整理すること。

(ウ) 業務移行

- 移行対象業務、移行方式、移行環境、移行後の品質保証方法等の移行設計を行うこと。
- 各課室担当者への影響点及びその影響点に対する対応内容の妥当性について、該当担当者の確認を得ること。

(エ) システム移行

- 次期保安ネット及び外部システムにおいて対象となる環境設定、移行方式、移行後の品質保証方法等の移行設計を行うこと。
- なお、保安ネットへアクセスするための URL は現行保安ネットと同一のものを利用する想定であるため、DNS 等の設定変更をする際は留意すること。
- 外部システムに対する影響点及び依頼事項については、外部システムごとに明確化し、外部システムからの確認を得ること。
- ガバメントクラウド若しくは「政府情報システムのためのセキュリティ評価制度(ISMAP)」において登録されたクラウド環境を構築するための手順書を別途作成すること。

(オ) ガバメントクラウド若しくは「政府情報システムのためのセキュリティ評価制度(ISMAP)」において登録されたクラウド環境構築手順書の作成

- ガバメントクラウド若しくは「政府情報システムのためのセキュリティ評価制度(ISMAP)」において登録されたクラウド上に環境を構築するにあたり、作業スケジュール、作業内容、手続等を整理した手順書を作成し、主管課の承認を得ること。
- ガバメントクラウド若しくは「政府情報システムのためのセキュリティ評価制度(ISMAP)」において登録されたクラウド環境単体での基本動作の確認を初期動作確認手順として含めること。
- 作成した手順書について、ガバメントクラウドを管理・運用する部署に確認を依頼し、必要に応じて修正すること。

イ. 手順書の妥当性確認

- 移行手順書(タイムチャート、作業体制図、連絡先一覧等を含む)が妥当であることを関係者との読み合わせ等の実施により確認すること。
- 確認結果の分析を行い、必要に応じて移行手順書を修正すること。
- 移行プログラムが仕様どおりに動作することを設計構築事業者の開発環境にて確認すること。
- 移行プログラム確認結果の分析を行い、必要に応じて、移行プログラムを修正すること。

ウ. 移行リハーサルの実施

- 本番の移行作業を模した条件において、移行リハーサルを実施すること。
- 移行リハーサルの実施結果について、結果分析を行い、必要に応じて移行手順書及び移行プログラムを修正すること。
- 移行手順書及び移行プログラムの最終版について主管課の承認を得ること。

(4) 移行の実施・移行結果報告書の作成

移行に伴う保安ネットの計画停止期間を主管課と協議の上で決定し、移行作業を実施すること。

また、本番移行の実施結果について作業完了後 1 週間以内に、移行計画書に記載された内容に基づいた移行結果報告書を作成し、主管課の承認を得ること。

移行作業の実施及び移行計画報告書作成にあたっての要件を以下に示す。

ア. 作業実施、報告書作成要件

(ア) 共通

- 移行手順書に基づいて作業を実施すること。

(イ) データ移行

- 現行保安ネットからのデータ抽出作業は、現行保安ネット運用・保守事業者が実施すること。
- 抽出したデータを次期保安ネットで利用可能にするために、次期保安ネットのデータベースやファイルシステムに投入すること。
- データ移行作業が完了した後、次期保安ネットのデータベースにおけるデータ件数を確認することや次期保安ネットの主要機能を各課室担当者が動作確認すること等をもって、データ移行が正常に完了したことを確認すること。

(ウ) 業務移行

- データ移行、システム移行のすべての作業が完了した後、主要な機能を対象に動作確認することで、作業が正常に完了したことを確認すること。
- 動作確認の対象とする機能の範囲については、主管課の承認を得ること。

(エ) システム移行

- ガバメントクラウド若しくは「政府情報システムのためのセキュリティ評価制度(ISMAP)」において登録されたクラウド環境構築手順書に基づいて作業を実施すること。
- 作成した初期動作確認手順に基づき、クラウドの初期動作確認を実施すること。
- クラウドの初期動作確認終了後、結果をとりまとめた「クラウド構築結果報告書」を作成、主管課に提出し承認を得ること。
- 移行手順書に基づいてシステム移行作業を実施すること。
- 現行保安ネットの停止は現行保安ネットの運用・保守事業者にて実施すること。
- 移行計画書と移行手順書に則して現行保安ネットの運用・保守事業者に対して現行保安ネット停止を予め依頼しておくこと。
- 現行保安ネットの停止後、保安ネットと外部システムとの接続について、現行保安ネットから次期保安ネットへの移行を行い、次期保安ネットでのサービスを開始すること。
- 次期保安ネットの最終動作確認を行い、移行作業が正常に完了したことを確認すること。

(5) 初期稼働の支援

次期保安ネット公開直後は、通常時と比べて多くのトラブルや問い合わせが発生する可能性があることから、初期稼働期間として作業支援を行うこと。設計構築事業者は、作業支援を行うために十分な次期保安ネットの構成や調整の経緯を熟知した要員、対応時間を確保すること。

また、初期稼働支援の作業内容は、「保守に関する事項」の定義に基づくものとするが障害等発生時において迅速な復旧が可能となる体制を整備すること。初期稼働期間は、主管課と協議し決定すること。

14. 引継ぎに関する事項

(1) 引継ぎ事項

本業務の契約履行期間の満了、全部若しくは一部の解除、またはその他契約の終了事由の如何を問わず、本業務が終了となる場合には、受注者は、経済産業省が継続して本業務を遂行できるよう必要な措置を講じ、他社に移行する作業の支援や引継を行うこと。

設計構築時完了時時の引継ぎ事項について以下に示す。

表 4-14 設計構築完了時の引継ぎ

引継ぎ発生時	引継ぎ元	引継ぎ先	引継ぎ内容	引継ぎ手順
運用開始時	設計構築事業者	運用・保守事業者	設計書 作業経緯 残存課題	• 設計構築事業者は、引継ぎ書を作成し、主管課の承認を受けること。 • 引継ぎ書に基づき、運用・保守事業者に対して確実な引継ぎを行うこと。 • 運用・保守事業者は、引継ぎ業務報告書を作成し、主管課に報告すること。

15. 教育に関する事項

(1) 教育対象者の範囲、教育の方法

業務の手順や次期保安ネットの操作方法について、特に更改に際しての現行保安ネットからの変更点を中心として、システム利用時の手順等を示した手順書を利用者の役割ごとに作成し、必要に応じて利用への教育を行うこと。

表 4-15 教育対象者の範囲、教育の方法(想定)

教育対象者の範囲	教育の内容	教育の実施時期	教育の方法	教材	教育対象者数
• 産業保安グループ保安課 • 経済産業局 • 産業保安監督部 • 地方自治体	保安ネット操作方法	運用開始前準備時	集合研修及びオンライン研修(録画を実施し、不参加者へ展開すること)。	• 操作手順書 • システム管理者用操作手順書	約 500 人

表 4-16 教材の種類(想定)

教材	教材の概要	対象者
操作手順書	• 利用者区分ごとに操作手順書の内容を分割するなど、利用しやすいように工夫すること。 • 個々の業務に沿った画面の流れを中心に作成すること。	• 産業保安グループ保安課 • 経済産業局 • 産業保安監督部 • 地方自治体
システム管理者用操作手順書	• 管理者権限のみが操作可能な機能に特化したシステム管理用操作手順書を作成すること。	• 産業保安グループ保安課(システム管理者)

16. 運用に関する事項

(1) 運用に関する要件

ア. 運用設計

次期保安ネットの安定稼働を確保するために必要となる具体的な監視項目や作業項目、作業スケジュール等運用設計を行い、主管課の承認を受けること。設計に当たっては、以下の点について考慮すること。

- システム運用設計を行い、契約期間中のシステムの日々の安定稼働を確保するために必要となる具体的な監視項目や作業項目、作業体制、作業スケジュール、整備対象の文書、成果物、形態や環境等の運用の定常的な計画等を取りまとめた運用計画書を作成し、主管課の承認を受けること。
- 「別紙 4-2　運用管理項目一覧」に示す運用項目を含めること。なお、受注者が提案する構成により当該運用管理項目に過不足が生じた場合は、必要に応じて修正を行うこと。
- リアルタイム監視を行い、障害につながる可能性の検出及びその対応を行う。
- 受注者は、業務影響を考慮し、24 時間 365 日対応を行う。

イ. 運用スケジュール

次期保安ネットは、開庁日及び非開庁日ともに全日オンライン・サービスが提供されること。

ウ. 集中入力センター

申請者(事業者)より紙の様式で提出された申請内容を保安ネットに登録すること。

エ. 掲載情報管理

ヘルプデスク等の頻発問合せ等を踏まえ、「よくある質問」の情報を更新する。必要に応じて、「お知らせ」を掲載すること。

オ. ヘルプデスク

開庁日の 9:00～18:00 の間は、システムの操作方法、処理結果、処理機能に関する利用者からの質問等への回答、対応等を迅速に行う体制を確保すること。問合せの内容によっては主管課へのエスカレーションを行うこと。なお、運用場所は受注者にて準備すること。

- サービスの停止等、利用者に影響するインシデントが発生した際には、当該事象に対する問合せに対応すること。なお、インシデント発生時にシステムに関連するベンダと回答内容については事前に協議し、正確な情報を回答すること。また、問合せ内容により当該インシデントに対する新たな事象等が判明した場合は、速やかに主管課にエスカレーションすること。
- 利用者からの問合せ及び対応に関する情報(対応状況、回答内容、対応時間、担当者、主管課へのエスカレーション要否等)を一元管理し、主管課と共有できる仕組みを講ずること。また、問合せ内容の分析を定

期的に行い、件数の多い問合せについては主管課と協議の上、FAQ への反映等を行うことにより、当該作業の効率化及び品質の向上を図ること。

・ 職員からの依頼による次期保安ネットの職員アカウントの発行及び削除等の作業を行うこと。なお、職員用アカウントについては、年 1 回の棚卸しを実施するため、各組織別のアカウント一覧を主管課に提供すること。

カ. バックアップ・リカバリ管理

バックアップ方針及びリカバリ方針を満たすために必要な運用設計を行うこと。

キ. ジョブ管理

オンラインの起動・終了及びバッチ処理やバックアップ処理の起動・停止等、システム運用については、事前にスケジュール登録を行い、基本的には自動で実行されるようにすること。また、受託者はジョブの管理に当たり、以下の要件を満たした製品を提案の上、新規に導入すること。

なお、システム全体構成を設計する際にジョブ管理が不要の際には、本検討を考慮外とすること。

・ ジョブ運行制御の一元管理が可能であること。
・ ジョブの実行状況、実行履歴はログ情報として記録可能であること。
・ ジョブの実行状況がモニタリング可能であること。
・ ジョブの実行が失敗した場合、アラート通知機能を有していること。また、アラートが発生したジョブ及び後続ジョブの停止機能を有していること。

ク. ログ管理

以下の通り、様々な情報解析に向けてログ管理をすること。

表 4-17 情報解析内容

情報解析分類	解析内容
エラー・障害検知	死活監視、状態異常監視、ジョブ監視、リソース監視でエラー、障害の検知に使用する。
原因解析	システム管理者がエラー、障害時の原因解析情報として使用する。
リカバリ	システム管理者がエラー、障害時のリカバリ作業に使用する。
監査・セキュリティ	システムへのリクエストや処理内容を記録し、監査の証跡として使用する。セキュリティ違反の検知や処理内容把握、経路追跡のために使用する。
可用性管理(稼働率等)	稼働率、障害回復時間の非遵守回数等を計算するためのデータとして使用する。
性能管理(応答時間等)	処理の応答時間遵守率を計算するためのデータとして使用する。
ジョブ管理(ジョブ稼働状況等)	ジョブが正常に動作しなかった件数の取得のためのデータとして使用する。
稼働統計情報	CPU、メモリ、ディスク、データベース、ネットワーク等の稼働統計情報。サーバ等のリソース管理を行うためのデータとして使用する。
機能ごとの処理件数	機能(オンライン処理、バッチ処理)ごとの処理件数。将来のシステム改善・刷新等の際に使用するためのデータとして使用する。
アクセス解析に係る情報	オンライン利用率の改善に資する情報を収集するために、画面遷移の離脱率並びに入力項

	目ごとの離脱数、未入力数及びエラー数等の解析の結果を収集すること。

ケ. 監視

次期保安ネットの構成を踏まえ、監視対象となる機器について、事前に主管課と調整の上、サーバ等システムリソース及びサービスの動作状況を監視し、異常発生時には検知可能な仕組みを有すること。

監視に係る要件を以下に示す。

- 監視項目には、死活監視、性能監視、ネットワーク監視、リソース監視、バックアップの実行結果監視、ジョブの監視を含み、システムの稼動状況及びサーバ、ネットワーク等システムリソースの稼動状況をモニタリング可能な仕組みを有すること。
- サービス停止につながる異常に対するリアルタイム通知機能を有すること。
- サービス停止を検知した場合、迅速に主管課に連絡できる体制を確保すること。
- データベースが正しく機能しているかデータベースの監視を行うこと。
- アイドル時間や IOPS 等ストレージの監視で必要な項目の監視を行うこと。
- 端末は既存で使用している端末を使用するため監視対象外とすること。
- ネットワーク機器はクラウドサービスの利用を想定しているため監視対象外とする。
- ネットワークパケットレベルの監視は、申請及び処理に係るネットワークに対して行うこと。
- 主管課と協議の上、リモート監視及び異常事態時の対応を行う執務場所を決定すること。
- システムのリソース利用率及びアラート検知の閾値を以下に示す。
  - CPU：50%以上 80%未満、 アラート発砲：80%以上
  - メモリ：50%以上 80%未満、 アラート発砲：80%以上
  - ディスク：50%以上 80%未満、 アラート発砲：80%以上

コ. 運用作業に関する要件

運用計画書に基づいて運用作業を実施すること。

サ. 運用実績の評価と改善

必要に応じて運用作業の作業効率及び運用管理項目の過不足を評価・検証すること。また、評価・検証の結果、作業効率の問題及び運用管理項目の過不足がある場合には見直しを検討すること。

17. 保守に関する事項

(1) 保守に関する要件

ア. 保守設計

受注者は保守設計を行い、契約期間中に計画的に発生する作業内容やその想定される時期等、システムの日々の安定稼働を確保するために必要となる具体的な作業項目や作業体制、作業スケジュール、整備対象の文書、成果物、形態や環境等の保守の定常的な計画等を取りまとめた保守計画書を作成し、主管課の承認を受けること。設計に当たっては、以下の点について考慮すること。

- 受注者は、保守計画書に基づいてシステムにおける保守作業を実施すること。
- 受注者は、導入した仮想サーバ・ソフトウェアについて、第三者製品であっても責任をもって保守を行うこと。
- 受注者は、契約期間中(運用開始前も含む。)におけるソフトウェアの製造元等のサポート(バグ修正パッチやセキュリティパッチも含む。)の期限及びバージョンアップに関する情報について、製造元等から公表または提供された情報を主管課へ速やかに報告すること。製造元等から追加の費用なく提供される等、バージョンアップが図れるものについて、主管課の求めに応じてバージョンアップ作業を行うこと。
- 契約期間中において、提供する製品の保守期限が切れる場合は、無償にて当該物品と同等以上の物品に交換すること。
- 受注者は、製造元から提供されるパッチ等の情報収集に努めるとともに、対策を講ずること。
- 受注者は、定期的にパッチ適用、バージョンアップ作業、設定変更作業等を実施すること。ただし、緊急性のあるものは随時とすること。その際、更新ファイルの配布は自動化し、更新処理は手動実行とする。更新を行う方法(手順等)を備えること。また、端末への更新ファイル配布機能は実装しないこと。
- 受注者は、定期的なパッチリリース情報を提供すること。その際推奨パッチを中心に適用後の影響を踏まえて、適用可否判断を行うこと。
- 定期保守時にパッチ適用を行うことを基本とするが、緊急パッチや重大パッチがリリースされた際は、定期保守を待たず適用可否を主管課と協議すること。
- パッチリリース情報提供やパッチ適用、監視状況、リソース使用状況等を定期的(月次を想定)に報告すること。
- 調査及びパッチ適用前のバックアップは取得するが、パッチ検証は行わない。
- 冗長構成を想定しているため、縮退運転を行うことで業務を停止させず、一部のソフトウェア(ミドルウェアやアプリケーションを想定)の活性保守を行うこと。ただし、OS は範囲外とする。また、ハードウェア活性保守はクラウド想定のため考慮しない。
- パッチ適用に当たっては、適用前と同等以上の機能・性能を満たすこと。また、パッチ適用後の動作確認については、主管課と十分調整を行った上で実施すること。
- 受注者は、導入したソフトウェアの販売が終了することが判明した場合、速やかに主管課に当該製品等の報告を行うとともに、その後の保守可能期間についても報告すること。
- 受注者は、導入したソフトウェアの運用・保守に必要となるドキュメント、メディアその必要な媒体を常に利用

可能な状態で保管・管理すること。

- 受注者は、運用・保守において、導入したソフトウェアの運用・保守に必要となるドキュメントに変更が発生する場合、更新(最新化)の上、改訂履歴とともに主管課に提示すること。また、改訂を行った際には、その履歴を管理すること。
- 受注者は、主管課の求めに応じて、技術的なサポートを行うこと。
- 受注者は、導入したソフトウェアについて、移設、外部システム機器との接続、別途ソフトウェアを追加インストールする等の要件が生じた場合、主管課に協力すること。
- 受注者は、システムの構成について、常に把握しておくこと。受注者は、異動等によって担当者が変更となる場合、システムの構成に関する説明を行うこと。
- 受注者は、障害に備えたシステムに関する保守部品及び予備機を確保することは行わないこと。
- クラウド想定のためハードウェアに係る保守契約は行わないが、システムを構成するために必要なすべてのソフトウェアに係る保守契約は行うこと。
- 導入後の実業務において挙動の確認も含め導入サポートを行うこと。また、期間は 1 か月とすること。
- インシデント管理、問題管理、構成管理、変更管理、リリース管理等 IT サービスを管理していく中で IT サービスマネジメントを参考に SMO(Service Management Office)の設置を検討すること。

イ. 保守作業に関する要件

受注者は、保守計画書に基づいて保守作業を実施すること。

ウ. 保守実績の評価と改善

受注者は、必要に応じて情報システムの安定的な運用の維持と継続的な改善のために必要となる保守実績の評価、改善活動を行うこと。

また、受注者は、必要に応じて保守作業の作業効率及び作業項目の過不足を評価・検証すること。評価・検証の結果、作業効率の問題及び作業項目の過不足がある場合には見直しを検討すること。

エ. 障害対応及び対策

以下に示す作業は開庁日の 9:00-18:00 に実施すること。ただし、サービスが停止するような障害に係る対応についてはこの限りではない。また、受注者は、障害に伴う復旧作業が開庁日の 9:00-18:00 に完了しない場合においても、必要に応じて復旧作業を継続すること。

- ソフトウェア障害、通信障害及び主要なファイル障害が発生した場合、迅速に解決できる体制を確保するとともに復旧作業を実施すること。
- サービス継続ができない障害が発生したと判断した場合、一次対応を迅速に行うこと。本番環境については、発生した障害がソフトウェアに起因する場合は、即時、復旧作業を開始すること。また、速やかに主管課へ事象を報告し、復旧後においては、原因及び対策を記載した報告書を作成すること。
- 障害のあった箇所について、製造元に問合せを行う等、障害原因を特定し、同様の事象を発生させないた

めの措置を講ずること。また、ログの取得等が必要な場合は、作業に必要な機器等を用意して対応すること。

- セキュリティ問題や不具合等により、ソフトウェアの変更やバージョンアップが必要な場合、無償にて行うこと。
- 主管課は、システムに関連するシステム障害が発生した場合において、受注者に対して故障切り分け等の作業を依頼することがあるため、受注者は、積極的に対応すること。

(2) 保守項目一覧

次期保安ネットで必要な保守項目について以下に示す。

表 4-20 保守項目一覧

保守項目	概要
障害対応	障害や不具合を検知時、暫定対応を実施する。原因を調査し、恒久対応を実施する。
作業依頼対応	本省より依頼された作業依頼を確認し、影響調査を行う。影響調査結果を踏まえて、本省に実施要否を判断いただき、要実施のものの対応を行う。
バックログ対応	利用者より受領した改修要望の対応を行う。
問合せ対応	利用者より受領した問い合わせの対応を行う。

以上