機２：関係者限り

２．共通ネットワークシステム

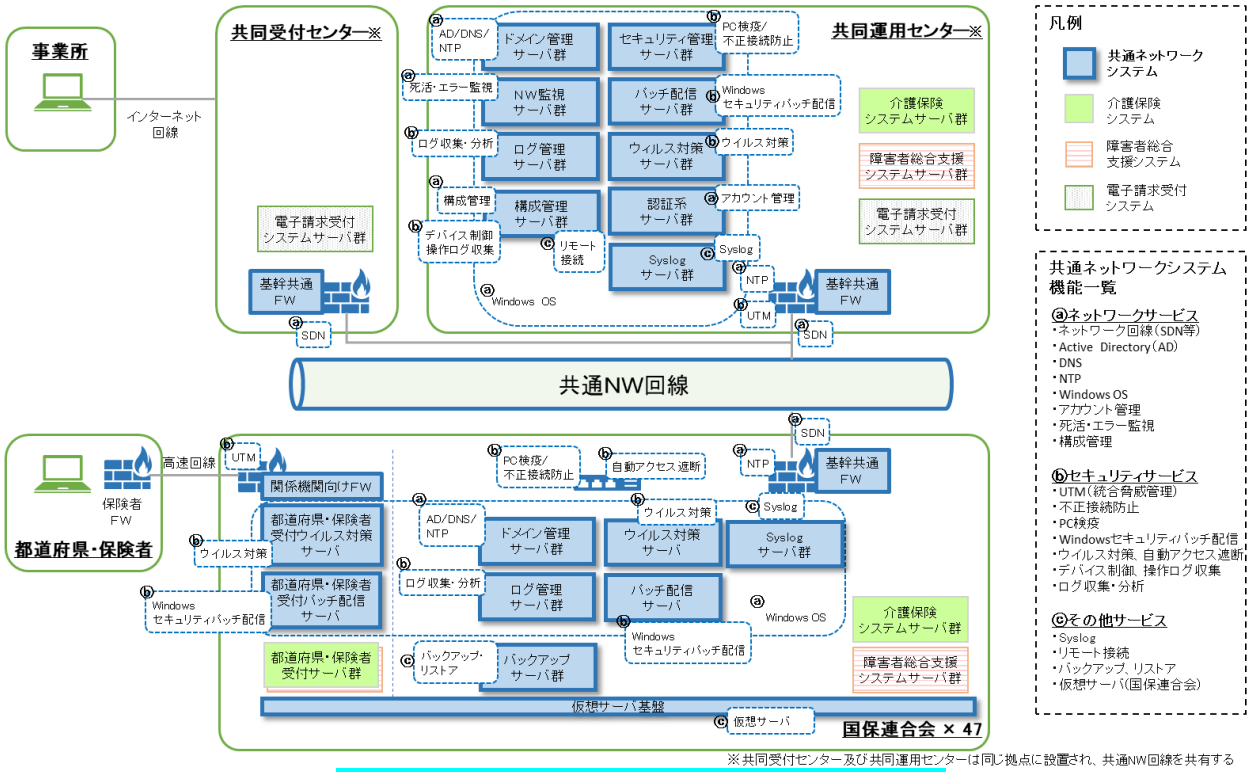
2. 共通ネットワークシステム

2.1. 共通ネットワークシステム提供サービス

2.1.1. システム全体構成

（1） 全体構成概要

共通ネットワークシステムは、介護保険システムと障害者総合支援システム及び電子請求受付システムを結ぶネットワーク基盤として、ネットワークサービス、セキュリティサービスを提供する。また、Syslog 等のその他サービスも併せて提供する。



※共同受付センター及び共同運用センターは同じ拠点に設置され、共通NW回線を共有する

図 2-1 共通ネットワークシステム全体構成イメージ

(2) 提供機能一覧

共通ネットワークシステムで提供する機能を以下に示す。

表 2-1 共通ネットワークシステム提供機能一覧

No.	提供機能	機能分類※	機能概要
1	L3SW	a	共通ネットワークシステム内の通信を異なるネットワークへ中継する機能を提供する。
2	L2SW	a	共通ネットワークシステム内の各システムの機器を収容し、各機器間でネットワーク接続機能を提供する。
3	ルータ制御	a	共通ネットワーク回線を収容する基幹共通ルータで WAN 経路制御及び QoS による優先制御機能を提供する。
4	UTM/ファイアウォール	b	UTM/ファイアウォールで拠点内部のシステム間及び拠点内外の通信制御、並びにセキュリティ対策機能を提供する。共同運用センター、共同受付センター、国保連合会に UTM/ファイアウォールを設置する。
5	自動アクセス遮断	b	クライアント L2SW や運用管理クライアント L2SW とウイルス対策機能を連携させることで、ウイルス/不正プログラムに感染したクライアント PC の通信を自動遮断する機能を提供する。
6	Windows OS	a	共通ネットワークシステムの提供サーバでは Windows Server 2016（64bit 版）を用い、ストレージ、ネットワーク、セキュリティ機能に特化したオペレーティングシステム環境を提供する。なお、介護保険、障害者総合支援システムのサーバも Windows Server 2016(64bit 版)となる。介護保険、障害者総合支援システムの Windows OS 機能は介護保険、障害者総合支援システムが提供する。
7	Active Directory （以下、「AD」という。）	a	マイクロソフト社の AD の機能を用いて、共同運用センター、全国の国保連合会、国保中央会のクライアント PC、Windows サーバで利用するユーザオブジェクト、コンピュータオブジェクト、グループポリシー(セキュリティポリシー)の一元管理機能を提供する。
8	アカウント管理	a	Web インタフェースで Windows ユーザアカウントの登録・更新・削除を行うための申請ワークフロー機能を提供する。
9	DNS	a	共同運用センター、全国の国保連合会及び国保中央会のクライアント PC、サーバに対し効率的な名前解決機能を提供する。
10	NTP	a	共同運用センター、国保連合会、国保中央会のドメイン環境のクライアント及びネットワーク機器等に対して、時刻同期機能(NTP)のサービスを提供する。
11	死活・エラー監視	a	共通ネットワークシステムに接続するネットワーク機器、サーバ、ストレージ機器を監視する。なお、国保連合会内で発生したアラート一覧を国保連合会が確認できる管理画面の機能も提供する。
12	Syslog	c	共通ネットワークシステムで導入するネットワーク機器の Syslog を収集する機能を提供する。
13	構成管理	a	管理対象機器にインストールしてあるミドルウェアの情報を収集し、各ミドルウェアの導入状況やライセンスの割り当て状況を一元的に管理する機能を提供する。

表 2-1 共通ネットワークシステム提供機能一覧

No.	提供機能	機能分類※	機能概要
14	デバイス制御	b	管理対象機器で利用する内蔵・外付け CD/DVD ドライブや USB デバイスに対する利用制限や利用状況管理、利用不可能なデバイス接続時のアラート等の機能を提供する。
15	リモート接続	c	専用の管理コンソールを用い、管理対象の Windows 機器に対するリモート接続機能を提供する。
16	不正接続防止	b	国保連合会内のクライアントPC 及びプリンタ等の IP アドレスとMAC アドレスを許可登録し、許可登録されていない不正に接続された機器をネットワークから遮断する機能を提供する。
17	PC 検疫	b	国保連合会内のクライアント PC で検疫ポリシーの適合状態を検査し、問題ないと判断されたクライアント PC のみネットワークへの接続を許可し、不適合となったクライアント PC は検疫ネットワークに隔離する機能を提供する。
18	Windows セキュリティパッチ配信	b	Microsoft 社製のサーバ OS、クライアント OS、Office 製品に対してセキュリティ更新プログラムの配信、管理機能を提供する。
19	ウイルス対策	b	管理対象機器に対して定期的にウイルスパターンファイル及び検索エンジンを配布し、定期的または手動による不正プログラムの検索、駆除/隔離を実行する機能を提供する。
20	ログ収集・分析	b	共同運用センター、国保中央会、国保連合会に設置されている特定個人情報・個人情報に係る機器から発生する各種ログの収集と分析を行う機能を提供する。
21	操作ログ収集	b	管理対象機器内においてユーザが操作した内容(起動/終了、アプリケーション利用、ファイルアクセス等)に関する操作ログを収集して保管する機能を提供する。
22	バックアップ/リストア	c	国保連合会内のWindows サーバのオペレーティングシステム及びデータに対するバックアップ／リストアの機能を提供する。
23	メール	ー	監視、セキュリティアラート及びアカウント管理の通知用にのみメール機能を提供する。国保連合会への共通ネットワークとしてのメール機能の提供は行わない。(現行システムで利用していたキャビネット及びメール連絡(事務連絡、リリース媒体の配布、ログ及び簡易的な連絡)での利用も廃止となり、国保連合会にメールサーバは設置しない。)
24	仮想サーバ	c	国保連合会で各システムの仮想サーバを集約する仮想サーバ基盤機能を提供する。

※「機能分類」は「図 2-1 共通ネットワークシステム全体構成イメージ」に示した「共通ネットワークシステム機能一覧」に対応する。

（3） 提供機能利用条件

共通ネットワークシステムで提供する機能の利用条件を以下に示す。

運用フローに準じた運用が開始されるのはいずれも連合会運用試験以降となる。

なお、独自処理システムへの機能提供は国保連合会で任意の時期に導入するため、以下の利用条件には従わない。

表 2-2 共通ネットワークシステム提供機能利用条件一覧

No.	提供機能	利用条件 ※「共通ネットワーク回線の開通」、「連合会 HW 受託者による機器設置及び配線」の完了が前提条件となる。
1	L3SW/L2SW /ルータ制御	・L3SW、L2SW、ルータ制御機能は前提条件が満たされることで利用可能(通信が可能及び国保連合会で設定追加が可能な状態)となる。
2	UTM/ ファイア ウォール	・UTM/ファイアウォール機能は前提条件が満たされることで利用可能(通信が可能及び国保連合会で設定追加が可能な状態)となる。 ・UTM/ファイアウォール機能の通信制御(ファイアウォールポリシー)は各システムの導入作業完了後、必要な通信の許可、不要な通信の遮断を開始する。また、仮移行、本移行時には作業に必要な通信の許可設定の追加が発生する。 ・UTM/ファイアウォール機能によるセキュリティ対策(不正接続防止、ウイルス対策)は前提条件が満たされることで利用可能となる。
3	自動アクセス 遮断	・自動アクセス遮断機能は以下条件を満たすことで利用可能となる。 1. 国保連合会による「連合会ウイルス対策サーバ#1」のシステム導入完了 2. 国保連合会によるクライアント PC へのウイルス対策ソフトの導入完了 3. 「連合会クライアント L2SW#1～#4」または「連合会運用クライアント L2SW#1～#4」にクライアント PC の接続完了
4	Windows OS	・Windows OS 機能は前提条件を満たすことで利用可能(共通ネットワークシステムのサーバ導入ができる状態)となる。
5	AD/DNS/NTP	・AD、DNS、NTP 機能は以下条件を満たすことで利用可能となる。 1. 国保連合会による「連合会 AD サーバ#1」のシステム導入完了
6	アカウント管理	・アカウント管理機能は以下条件を満たすことで利用可能(申請ワークフローを用いた Windows ユーザアカウントの登録・更新・削除)となる。 1. 国保連合会による「連合会 AD サーバ#1」のシステム導入完了
7	死活・エラー監視	・死活・エラー監視機能は以下条件を満たすことで利用可能となる。 1. 国保連合会による「連合会監視サーバ#1」のシステム導入完了 2. 国保連合会による共通ネットワークシステムのサーバ導入完了(監視エージェントの導入完了) 3. 国保連合会による運用管理クライアントへの「JP1/Intergrated Management(View ソフト)」導入完了 4. 国保連合会による介護保険、障害者総合支援システムのサーバ導入完了(監視エージェントの導入完了) 5. 国保連合会による共通ネットワーク、介護保険、障害者総合支援システムのサーバの監視設定完了
8	Syslog	・Syslog 機能は以下条件を満たすことで利用可能となる。 1. 国保連合会による「連合会 Syslog サーバ#1」のシステム導入完了

表 2-2 共通ネットワークシステム提供機能利用条件一覧

No.	提供機能	利用条件 ※「共通ネットワーク回線の開通」、「連合会 HW 受託者による機器設置及び配線」の完了が前提条件となる。
9	構成管理 /デバイス制御 /リモート接続 /操作ログ収取	・構成管理、デバイス制御、リモート接続及び操作ログ収集機能は以下条件を満たすことで利用可能となる。 1. 国保連合会による共通ネットワークシステムのサーバ導入完了(SKYSEA 端末機の導入完了) 2. 国保連合会によるクライアント PC への「SKYSEA 端末機」または「SKYSEA 管理機」の導入完了 3. 共通ネットワークシステム受託者による「SKYSEA 管理機」への操作範囲設定の完了 4. 国保連合会による介護保険、障害者総合支援システムのサーバ導入完了(SKYSEA 端末機の導入完了)
10	不正接続防止	・不正接続防止機能は前提条件を満たすことで利用可能となる。 なお、仮移行や本移行等の別フェーズ作業の妨げになる可能性があるため、本移行完了まではモニタモード(接続機器の遮断をしないモード)で運用する。本稼働開始に合わせて不正接続機器の遮断を開始する。
11	PC 検疫	・PC 検疫機能は以下条件を満たすことで利用可能となる。 なお、仮移行や本移行等の別フェーズ作業の妨げになる可能性があるため、本移行完了までは接続機器の検疫条件を緩和して運用する。本稼働開始に合わせて PC 検疫を開始する。 1. 国保連合会によるクライアント PC への PC 検疫エージェントの導入完了
12	Windows セキュリティパッチ配信	・Windows セキュリティパッチ配信機能による国保連合会サーバへのパッチ適用は以下条件を満たすことで利用可能となる。 ただし、サーバへのセキュリティパッチ適用は各システムの導入手順書に従い行うものとする。 1. 国保連合会による「連合会セキュリティパッチ配信サーバ#1」のシステム導入完了 2. 国保連合会による共通ネットワークシステム、介護保険システム及び障害者総合支援システムのシステム導入作業完了 ・Windows セキュリティパッチ配信機能による国保連合会設置のクライアント PC のパッチ適用は以下条件を満たすことで利用可能となる。 1. 国保連合会による「連合会セキュリティパッチ配信サーバ#1」のシステム導入完了 2. 国保連合会によるクライアント PC への共通ネットワーク提供サービスの導入(各エージェント導入)完了 ・Windows セキュリティパッチ配信機能による都道府県・保険者のクライアント PC(伝送クライアント)のパッチ適用は以下条件を満たすことで利用可能となる。 1. 国保連合会による「連合会都道府県・保険者セキュリティパッチ配信サーバ#1」のシステム導入完了 2. 都道府県・保険者回線の切替え(本移行後) ※仮移行、連合会運用試験における都道府県・保険者回線の切替え時は、切戻し作業の影響が大きいため Windows セキュリティパッチの適用は行わない。

表 2-2 共通ネットワークシステム提供機能利用条件一覧

No.	提供機能	利用条件 ※「共通ネットワーク回線の開通」、「連合会 HW 受託者による機器設置及び配線」の完了が前提条件となる。
13	ウイルス対策	・ウイルス対策機能による国保連合会サーバ及びクライアント PC のウイルス対策は以下条件を満たすことで利用可能となる。 1. 国保連合会による「連合会ウイルス対策サーバ#1」のシステム導入完了 2. 国保連合会による共通ネットワークシステムのサーバ導入完了(ウイルス対策エージェントの導入完了) 3. 国保連合会によるクライアント PC へのウイルス対策エージェント導入完了 4. 国保連合会による介護保険システム及び障害者総合支援システムのシステム導入(ウイルス対策エージェント導入)作業完了 ・ウイルス対策機能による都道府県・保険者のクライアント PC(伝送クライアント)のウイルス対策は以下条件を満たすことで利用可能となる。 1. 国保連合会による「連合会都道府県・保険者ウイルス対策サーバ#1」のシステム導入完了 2. 都道府県・保険者回線の切替え(本移行後)
14	ログ収集・分析	・ログ収集・分析機能は以下条件を満たすことで利用可能となる。 1. 国保連合会による「連合会ログ管理サーバ#1」のシステム導入完了 2. 国保連合会による共通ネットワークシステムのサーバ導入完了(ログ収集・分析エージェントの導入完了) 3. 国保連合会によるクライアント PC へのログ収集・分析エージェント導入完了 4. 国保連合会による介護保険、障害者総合支援システムのサーバ導入完了(ログ収集・分析エージェントの導入完了)
15	バックアップ/リストア	・バックアップ/リストア機能は以下条件を満たすことで利用可能となる。 1. 国保連合会による「連合会バックアップアプライアンス#1、#2」のシステム導入完了 2. 国保連合会による共通ネットワークシステムのサーバ導入完了(バックアップエージェントの導入完了) 3. 国保連合会による介護保険、障害者総合支援システムのサーバ導入完了(バックアップエージェントの導入完了) 4. 国保連合会による共通ネットワーク、介護保険、障害者総合支援システムのサーバのバックアップ設定完了
16	仮想サーバ	・仮想サーバ機能は前提条件を満たすことで利用可能となる。

2.1.2. 提供サービス詳細

（1） ネットワークサービス

① ネットワーク回線

(a) 概要

共同運用センターと国保連合会を接続する WAN 回線は正回線、副回線の 2 回線から構成し、共通ネットワーク回線 1(正回線)は帯域保証のサービス、共通ネットワーク回線 2(副回線)はベストエフォートのサービスを利用する。

(b) 機能イメージ

ネットワーク回線の機能イメージを以下に示す。

（連合会①、連合会②は別の連合会を示す）

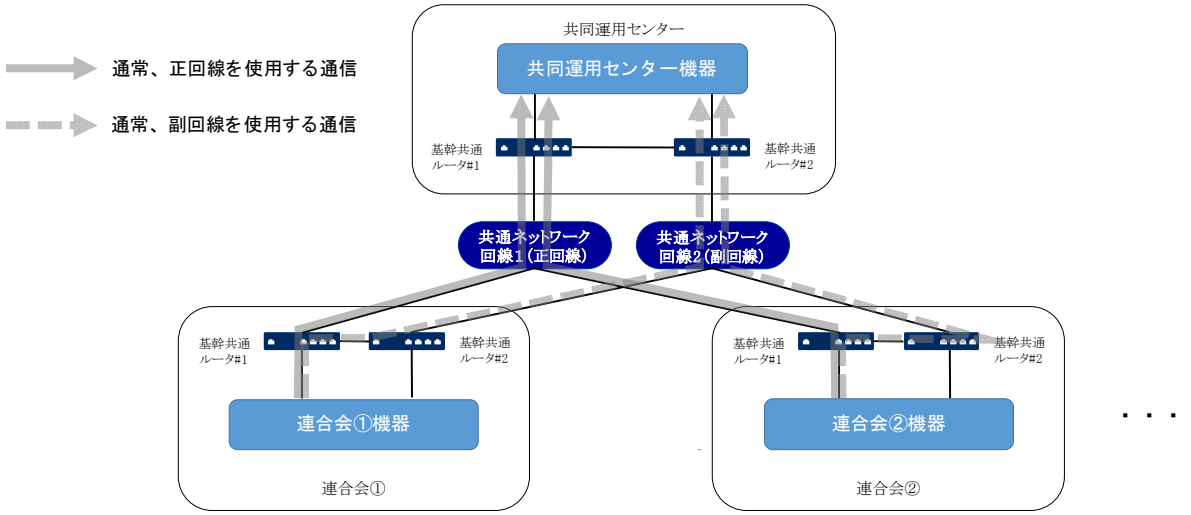


図 2-2 回線利用イメージ（通常時）

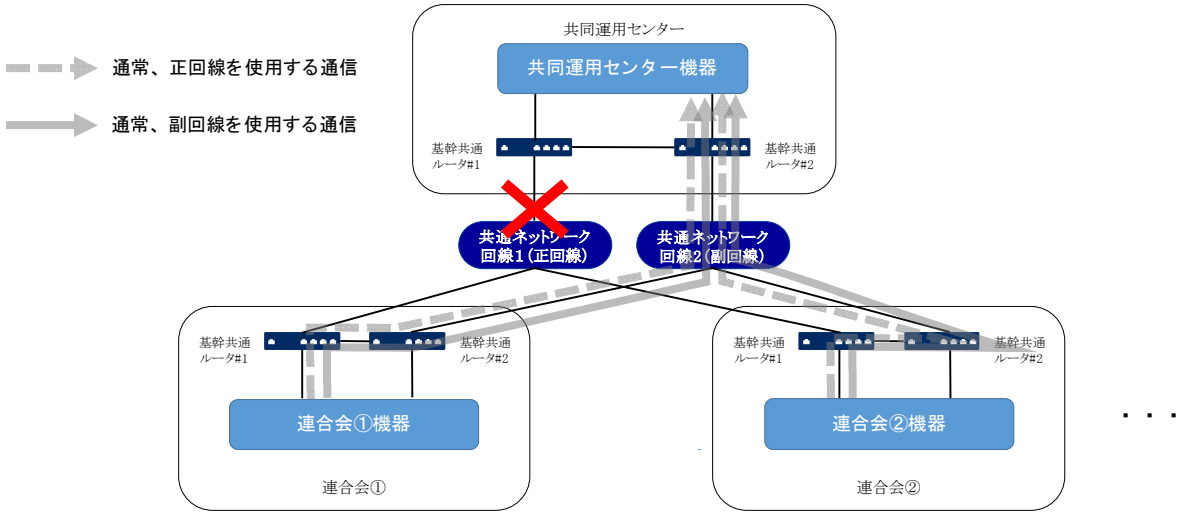


図 2-3 回線利用イメージ（正回線障害時）

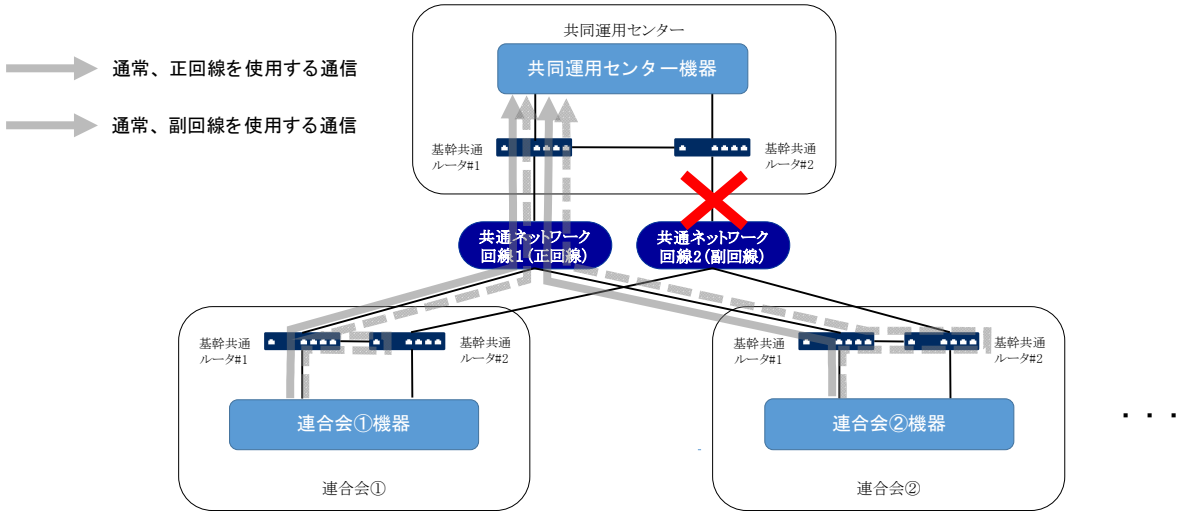


図 2-4 回線利用イメージ（副回線障害時）

(c) 提供機能

ネットワーク回線で提供する機能を以下に示す。

表 2-3 ネットワーク回線機能一覧

No.	機能	説明
1	WAN 回線	共同運用センター、国保連合会を接続する共通 NW を提供する。
2	回線冗長化	いずれかの回線に異常があった場合も、相互に機能を補完し、通信断となることを回避する。

(d) 運用項目

国保連合会でネットワーク回線機能の運用項目はない。

(e) 留意事項

・ 国保連合会に設置する独自処理システムに導入するSKYSEAは、共同運用センター設置のSKYSEAの管理サーバと通信する。そのため、国保連合会が「2.2.2 提供ドキュメント」に記載の手順書を参照して、SKYSEAの通信ポートの許可を連合会独自向けFW（仮想）に設定する必要がある。

② ネットワーク機器(L2/L3/ルータ)

(a) 概要

国保連合会内の各システムの機器を収容し、各機器間でのネットワーク接続機能を提供する。

ア. L2SW

国保連合会内の各システムの機器を収容し、各機器間で IPv4 のネットワークを提供する。

ウイルス対策機能を持つ L2SW はウイルス対策サーバと連携して、感染したクライアント PC の通信を遮断する。(「2.1.2. (2)②自動アクセス遮断」を参照。)

表 2-4 L2SW 一覧

No.	L2SW 名	説明
1	連合会サーバ L2SW#1～#2	主に国保連合会設置のサーバを収容する。 システム構成により独自処理システムの機器を接続する。
2	連合会 DMZL2SW#1～#2	主に国保連合会設置の都道府県・保険者向けサーバを収容する。 システム構成により独自処理システムの機器を接続する。
3	連合会関係機関 L2SW#1～#2	主に都道府県・保険者向け高速回線用ネットワーク機器を収容する。
4	連合会クライアント L2SW#1～#4	主に国保連合会設置のクライアント PC を収容する。(運用管理クライアント PC の収容も可能) 基本的な構成は 2 台の冗長構成であるが、国保連合会の規模に応じて#3、#4 を追加する。 システム構成により独自処理システムの機器を接続する。
5	連合会運用クライアント L2SW#1～#2	主に国保連合会設置の運用管理クライアント PC を収容する。(業務クライアント PC の収容も可能) システム構成により独自処理システムの機器を接続する。

イ．L3SW

国保連合会内の異なるネットワークセグメント間を中継する機能を提供する。

表 2-5 L3SW 一覧

No.	L3SW 名	説明
1	連合会基幹共通 L3SW#1～#2	国保連合会設置のネットワーク機器を収容し通信の中継を行う。

ウ．ルータ

共通ネットワーク回線と国保連合会のネットワークを中継する機能を提供する。

表 2-6 ルーター覧

No.	ルータ名	説明
1	連合会基幹共通ルータ#1～#2	共通ネットワーク回線と連合会基幹共通 L3SW#1～#2 を収容し、共同運用センターとの通信の中継を行う。

(b) 機能イメージ

機能イメージは「2.2.1.(2)①　システム構成」に示す。

(c) 提供機能

ネットワーク機器(L2/L3/ルータ)は以下の機能を提供する。

ア. L2SW

表 2-7 L2SW 機能一覧

No.	機能	説明
1	レイヤ 2 通信制御	国保連合会内の通信を同一ネットワーク間で中継する。 必要に応じて、VLAN 機能による仮想ネットワークの分割を行う。

イ. L3SW

表 2-8 L3SW 機能一覧

No.	機能	説明
1	ルーティング	国保連合会内の通信を異なるネットワークセグメント間で中継する。
2	レイヤ 2 通信制御	国保連合会内の通信を同一ネットワーク間で中継する。 必要に応じて、VLAN 機能による仮想ネットワークの分割を行う。

ウ．ルータ

表 2-9 ルータ機能一覧

No.	機能	説明
1	スタティックルーティング	国保連合会と共通ネットワーク回線の間で通信を中継する。
2	ネットワーク冗長化	正回線、副回線の死活監視を行い、片系の回線障害時に正常な回線を利用して通信を継続する機能を提供する。
3	ポリシーベースルーティング	パケットの転送を「送信元アドレス」、「プロトコル」、「ポート番号」の情報に基づきルーティングを行う。 あらかじめ設定したポリシーに従い、正回線、副回線に通信を分散させる制御を行う。
4	VPN	共通ネットワーク回線上に流れるパケットの暗号化を行う。
5	QoS	送信データに優先順位を付加する機能。 優先順位の高いデータから先に通信させることで、低速なネットワーク回線を効率的に利用する。

(d) 運用項目

ネットワーク機器(L2/L3/ルータ)の運用項目を以下に示す。

表 2-10 ネットワーク機器 運用項目一覧

No.	運用項目	頻度	説明	運用者
1	L2SW の設定変更	機器構成変更時	独自処理システムの追加、削除を行う際に、接続ポートの設定変更を行う。	国保連合会

(e) 留意事項

・ 「表 2-9 ルータ機能一覧」の No4「VPN」機能は連合会運用試験で実施の可否を判断する予定であり、試験結果により停止する可能性がある。

③ AD/DNS/NTP

(a) 概要

AD/DNS/NTP 機能は、Windows Server 2016 のバンドル機能を用いて実現する。

ア. AD 機能

・アカウント情報（ユーザ認証）の管理機能及びグループポリシー（セキュリティポリシー）の適用機能を提供する。

・次期システムでは、シングルドメイン構成とする。（都道府県のアルファベット名 3 文字は利用せず、「kokuho.pr」とする）

・共同運用センターの被災時を考慮し、国保連合会に AD のサーバを導入する。

イ. DNS 機能

名前解決機能を提供する。

ウ. NTP 機能

サーバ及びクライアントの時刻を日本標準時(JST)に同期する機能を提供する。

表 2-11 AD/DNS/NTP コンポーネント一覧

No.	コンポーネント	説明
1	センター統合 AD 管理サーバ#1～#2	AD 機能を一元管理する。 NTP 機能では、共同運用センター提供の時刻同期装置と時刻同期し、日本標準時間(JST)を全国のサーバに配信する機能を提供する。
2	センターAD 管理サーバ#1～#3	AD 機能において、共同運用センターに設置された各システムの Windows サーバ/Windows クライアントに対し、ユーザ認証、グループポリシーの配信機能を提供する。 DNS 機能では、共同運用センターの各機器に対して名前解決機能を提供する。
3	連合会 AD 管理サーバ#1	AD 機能において、国保連合会に設置された各システムのサーバ/クライアントに対し、ユーザ認証、グループポリシーの配信機能を提供する。 DNS 機能では、国保連合会の各機器に対して優先的な接続先として名前解決機能を提供する。 NTP 機能では、国保連合会の各機器に対して時刻配信の機能を提供する。
4	連合会セキュリティパッチ配信サーバ#1	DNS 機能では、国保連合会の各機器に対して代替の接続先として名前解決機能を提供する。

(b) 機能イメージ

AD の機能イメージを以下に示す。

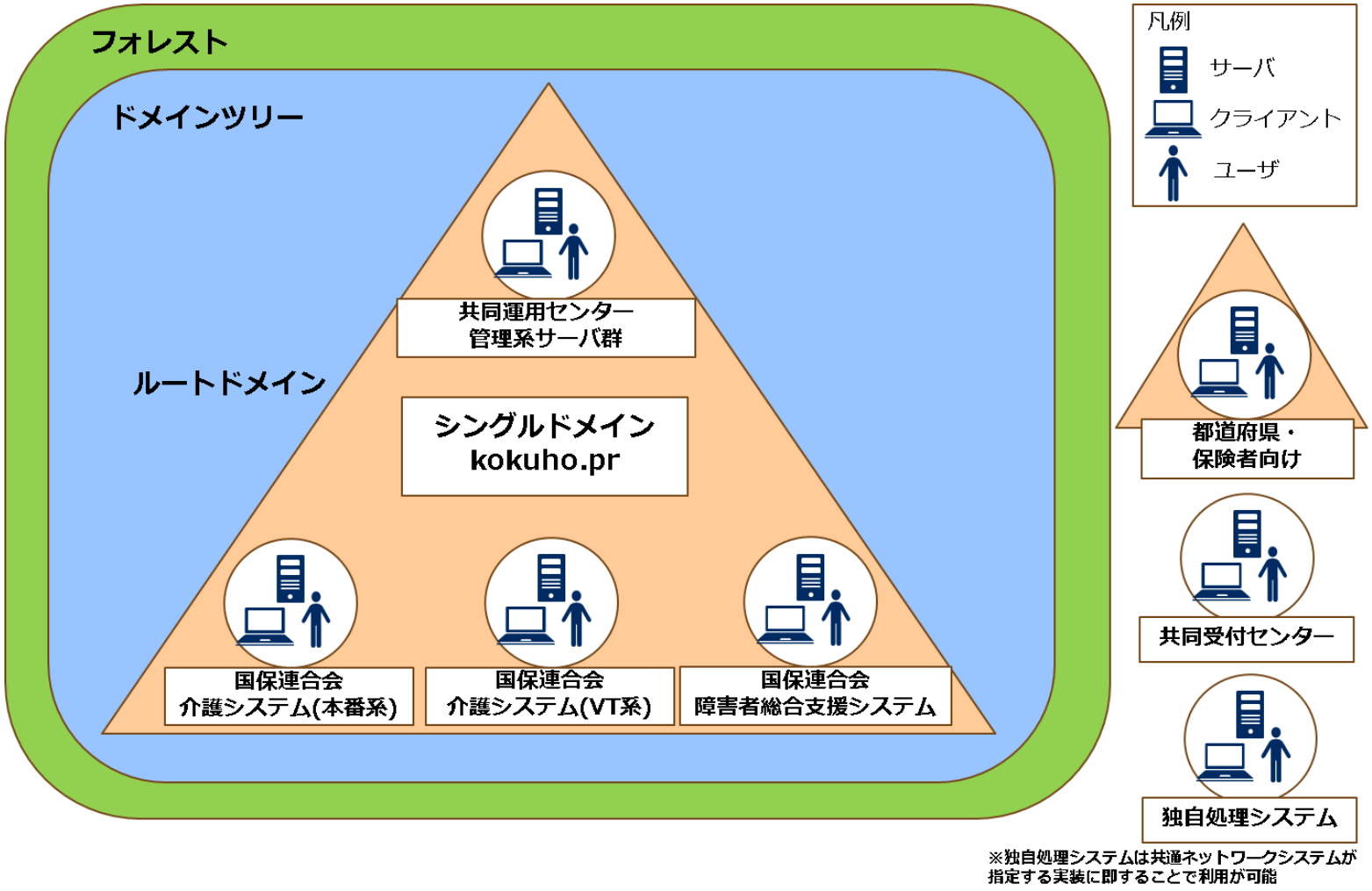


図 2-5 AD の機能イメージ

(c) 提供機能

AD/DNS/NTP で提供する機能を以下に示す。

表 2-12 AD 機能一覧

No.	機能	説明
1	アカウント情報管理機能	クライアント及びサーバのアカウント情報（氏名、ログイン名、パスワード、所属等）を管理し、ユーザ認証を行う機能を提供する。次項のアカウント管理機能を用いてアカウントの登録・変更・削除を行う。
2	コンピュータオブジェクト管理機能	コンピュータオブジェクトの一元管理機能を提供する。 国保連合会で PC を新規設置・撤去する場合、コンピュータオブジェクトの登録・削除が必要なため、共通ネットワークシステム運用に申請する。
3	グループポリシー適用機能	ユーザやコンピュータに対し、パスワードポリシー、Internet Explorer 等を自動で設定するグループポリシー機能を提供する。

表 2-13 DNS 機能一覧

No.	機能	説明
1	名前解決機能	FQDN の名前解決機能を提供する。

表 2-14 NTP 機能一覧

No.	機能	説明
1	時刻同期機能	サーバ及びクライアントの時刻を日本標準時(JST)に同期する機能を提供する。

(d) 運用項目

AD 機能の運用項目を以下に示す。

DNS/NTP 機能に関しては機能提供のみとなり、国保連合会で DNS/NTP に関する運用項目はない。

表 2-15 AD 機能 運用項目一覧

No.	運用項目	頻度	説明	運用者
1	コンピュータオブジェクトの追加・削除申請	随時	PC の新規設置・撤去時に、共通ネットワークシステム運用へ申請する。 共通ネットワークシステム運用は申請内容に基づきコンピュータオブジェクトの登録・削除を行い、申請者に結果報告する。	・国保連合会 ・共通ネットワークシステム運用
2	グループポリシー(PSO)の変更申請	随時	グループポリシーでパスワードの有効期限の延長が必要な場合、共通ネットワークシステム運用へ申請する。 共通ネットワークシステム運用は申請内容に基づきグループポリシー(PSO)の変更を行い、申請者に結果報告する。	
3	アカウントロック解除	随時	アカウントのロック解除が必要な場合、アカウントの利用者が共通ネットワークシステム運用に申請する。 共通ネットワークシステム運用は申請内容に基づきアカウントロック解除を行い、申請者に解除した旨を連絡する。	
4	未ログインユーザの抽出	月次	共通ネットワークシステム運用が半年間ログインを行っていないユーザを抽出し、当該のユーザが所属する国保連合会に連絡する。 国保連合会は、ユーザの必要・不要を決定し、不要なユーザである場合はアカウント管理システムで削除申請する。	
5	DNS レコードの追加	随時	独自処理システムの機器追加等で DNS のレコードが必要な場合、共通ネットワークシステム運用に申請する。 共通ネットワークシステム運用は申請内容に基づき DNS レコードの追加を行い、結果報告する。	

(e) 留意事項

・現行システムの AD ユーザの移行はしないのでアカウント管理を利用して新規登録を行うこと。

・独自処理システムは、AD の参加を任意とする。

・ログインで利用するパスワードは、原則として有効期限を 90 日とし、以下のパスワードポリシーを満たすものとする。

1) パスワードの長さ:8 文字以上

2) パスワードの変更禁止期間:1 日

3) アカウント名に 3 文字以上連続する文字列を使用しない

4) 4 つのカテゴリ内(大文字、英小文字、数字、アルファベット以外の文字)から、3 つを選択し使用する

・アカウント管理機能で利用する共同運用センターに設置されたサーバに障害が発生した場合、アカウント管理機能が利用できなくなる。アカウント管理機能が復旧するまでは利用者からのアカウント登録・変更・削除依頼の情報をとりまとめ、共通ネットワークシステム運用が手動により AD でアカウント登録・変更・削除を行う運用を実施する。

・都道府県保険者(伝送クライアント)に対する機能提供について

1) AD 機能は、都道府県・保険者(伝送クライアント)に対して機能提供をしない。

2) DNS 機能は、介護保険システムが都道府県・保険者(伝送クライアント)に対して機能提供を行う。

3) NTP 機能は、都道府県・保険者(伝送クライアント)に対して機能提供をしない。

・独自処理システムに対する機能提供について

1) AD 機能は、独自処理システムに対して機能提供を行う。

独自処理システムで利用するクライアント及びサーバは、AD 機能の利用を任意とする。

(AD 機能を利用する場合は DNS 機能の利用は必須とする)

AD 機能が利用可能なオペレーティングシステムのバージョン：

Microsoft Windows 10 Enterprise 2016 LTSB (64BitOS)

Microsoft Windows Server 2016

2) DNS 機能は、独自処理システムに対して機能提供を行う。

独自処理システムで利用するクライアント及びサーバは、DNS 機能の利用を任意とする。

DNS 機能を利用する機器のオペレーティングシステムやバージョンに関して指定はない。

独自処理システムの DNS 機能接続先を以下に記載する。

優先 DNS：連合会 AD 管理サーバ#1

代替 DNS：連合会セキュリティパッチ配信サーバ#1

3) NTP 機能は、独自処理システムに対して機能提供を行う。

独自処理システムで利用するクライアント及びサーバは、NTP 機能の利用を必須とする。

NTP 機能を利用する機器のオペレーティングシステムやバージョンに関して指定はない。

独自処理システムの NTP 機能接続先を以下に記載する。

NTP プライマリ：連合会 AD 管理サーバ#1

NTP セカンダリ：連合会基幹共通 FW

④ アカウント管理

(a) 概要

アカウント管理機能は共同運用センターに設置するサーバに NEC 社 SECUREMASTER / EnterpriseIdentityManager を導入することで実現する。
アカウント管理機能では Web インタフェースによる申請ワークフロー機能を提供する。
また、AD と二要素認証機能へのアカウント配信を自動的に行うことで、アカウントの一元管理機能も提供する。
なお、現行システムの申請対象である以下①～③のアカウントのうち、次期システムでは「①Windows ユーザアカウント」の申請のみ対象とする。

[現行システムの申請対象アカウント]
①Windows ユーザアカウント
②StarOffice のユーザアカウント
③業務支援システムのユーザアカウント

※補足事項
・StarOffice のユーザアカウント　：StarOffice の対象範囲縮小に伴い、StarOffice のユーザアカウントの追加・削除申請は不要となる。
・業務支援システムのユーザアカウント ：申請先が共通ネットワーク運用から介護保険システムの運用へ変更となるが、現行システムと同様の運用でユーザアカウントの申請を行う。

(b) 機能イメージ

アカウント管理の機能イメージを以下に示す。

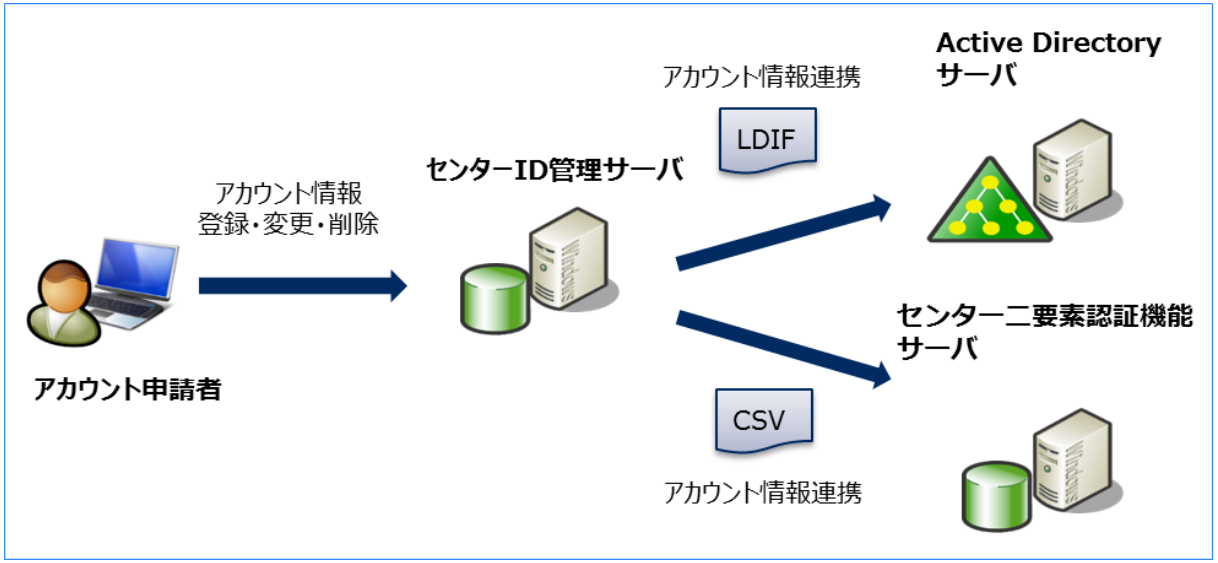


図 2-6 アカウント管理の機能イメージ

(c) 提供機能

アカウント管理機能で提供する機能を以下に示す。

表 2-16 アカウント管理機能一覧

No.	機能	説明
1	申請ワークフロー機能	WEB ブラウザで申請画面を表示し、申請処理や承認処理を実施する。 [補足：ワークフロー処理の背後で実施される機能] ①メール送信機能：申請承認依頼や初期パスワード変更に関するメールを送信 ②AD 連携機能：ユーザ情報の登録・更新・削除が発生した際に AD にユーザ情報を配信 ③セルフメンテナンス機能：パスワード変更及びパスワードリマインダの機能

(d) 運用項目

アカウント管理機能の運用項目を以下に示す。

表 2-17 アカウント管理機能　運用項目一覧

No.	運用項目	頻度	説明	運用者
1	Windows ユーザアカウントの登録	随時	Windows ユーザアカウントの登録を行う。	国保連合会 共通ネットワークシステム運用
2	Windows ユーザアカウントの変更	随時	Windows ユーザアカウントの変更を行う。	
3	Windows ユーザアカウントの削除	随時	Windows ユーザアカウントの削除を行う。	
4	管理者アカウントの登録	随時	管理者アカウントの登録を行う。	
5	管理者アカウントの変更	随時	管理者アカウントの変更を行う。	
6	管理者アカウントの削除	随時	管理者アカウントの削除を行う。	
7	パスワードリセット	随時	Windows ユーザアカウントや管理者アカウントのパスワードをリセットする。	国保連合会
8	ユーザ検索	随時	Windows ユーザアカウントや管理者アカウントを検索する。	
9	申請書検索	随時	申請書を検索する。	

※アカウント種別について

・Windows ユーザアカウント ： Windows にログオンするためのアカウント

・管理者アカウント　　： アカウント管理機能で申請・承認を行うためのアカウント

（e）留意事項

・ 現行システムではExcelファイルの台帳を基にした申請運用となっているが、次期システムではWEBブラウザ画面を利用した申請運用となるため運用手順が大きく異なる。

・ アカウント管理機能で利用する共同運用センターに設置されたサーバに障害が発生した場合、アカウント管理機能が利用できなくなる。アカウント管理機能が復旧するまでは利用者からのアカウント登録・変更・削除依頼の情報をとりまとめ、共通ネットワークシステム運用が手動によりADでアカウント登録・変更・削除を行う運用を実施する。

・ 国保連合会の Windows ユーザアカウントと管理者アカウント登録時の初期パスワードの通知はメール機能(StarOffice X)の利用範囲縮小に伴い、情報系端末のメール（Outlook 等）で国保連合会担当者宛に送付する。そのため、国保連合会ではアカウント申請時に初期パスワードを受信する担当者を選出する必要がある。（パスワードの通知のため、メーリングリスト宛ての送付は不可とする。）
なお、初期パスワード通知の契機は以下となる。
–ユーザ作成申請の完了時
–パスワードリセット申請の完了時
(セルフパスワード変更/パスワードリマインダによるパスワード変更はメール送信は発生しない)

・ アカウント管理機能は独自処理システムに対する機能提供をしない。

・ アカウント管理機能は都道府県・保険者(伝送クライアント)に対する機能提供をしない。

⑤ 死活・エラー監視

(a) 概要

共通ネットワークに接続する機器（NW 機器、連合会仮想基盤、バックアップサーバ）を監視する。

監視機能を実現するミドルウェアを以下に示す。

表 2-18 死活・エラー監視機能 実装ミドルウェア一覧

No.	機能	説明
1	JP1/Integrated Management	監視対象機器を監視するための管理コンソール。通知されたエラーメッセージを一覧表示する。
2	WebSAM SystemManager G	サーバを監視するミドルウェア。死活監視、プロセス監視、ログ監視、リソース監視、ハードウェア基盤監視をする。
3	WebSAM NetvisorPRO V	ネットワーク機器を監視するミドルウェア。死活監視、SNMP トラップ監視、リソース監視をする。

(b) 機能イメージ

死活・エラー監視の機能イメージを以下に示す。

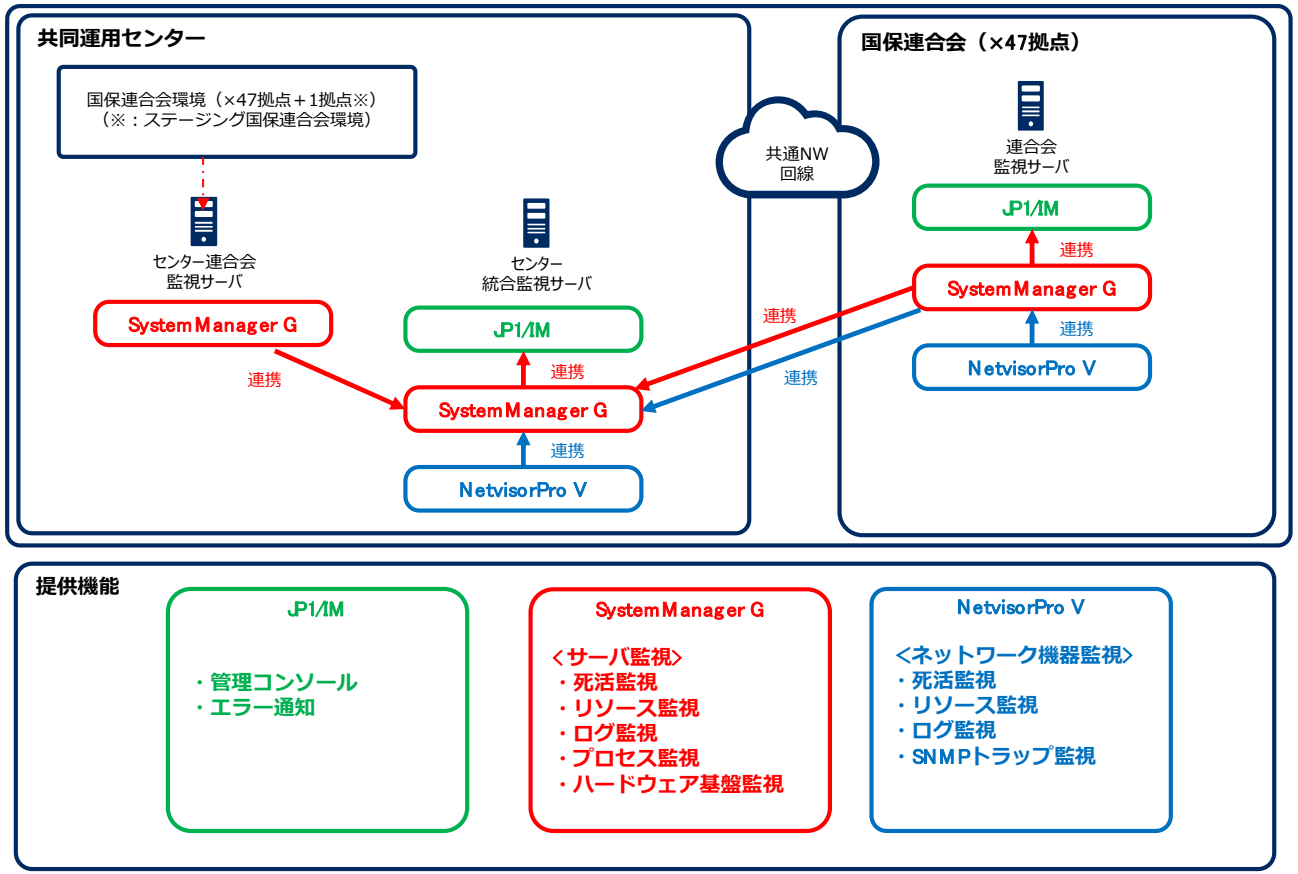


図 2-7 死活・エラー監視機能イメージ

（c） 提供機能

死活・エラー監視で提供するサーバ監視機能及びネットワーク機器監視機能を以下に示す。

表 2-19 死活・エラー監視機能 サーバ監視機能一覧

No.	機能	説明
1	死活監視	サーバの死活状態を監視し、サーバの停止時にエラーを通知する。
2	リソース監視	サーバのリソースを閾値監視し、リソースが閾値を超過した場合、エラーを通知する。
3	ログ監視	サーバのシステムログとアプリケーションログを監視し、異常メッセージ出力時にエラーを通知する。
4	プロセス監視	サーバのプロセスとサービスの起動状態を監視し、異常検知時にエラーを通知する。
5	ハードウェア基盤監視	仮想化基盤の稼働状態を監視し、異常検知時にエラーを通知する。

表 2-20 死活・エラー監視機能 ネットワーク機器監視機能一覧

No.	機能	説明
1	死活監視	ネットワーク機器を ICMP、SNMP 要求により監視し、異常検知時にエラーを通知する。
2	リソース監視	ネットワーク機器のリソースを閾値監視し、リソースが閾値を超過した場合、エラーを通知する。
3	ログ監視	ネットワーク機器のから送信される Syslog を監視し、異常メッセージ出力時にエラーを通知する。
4	SNMP トラップ監視	ネットワーク機器から送信される SNMP トラップを監視し、異常メッセージ出力時にエラーを通知する。

(d) 運用項目

死活・エラー監視の運用項目を以下に示す。

表 2-21 死活・エラー監視機能 運用項目一覧

No.	運用項目	頻度	説明	運用者
1	アラート監視	随時	サーバ及びネットワーク機器からのアラート発生を監視する。	国保連合会 共通ネットワークシステム運用
2	レポート作業	月次	国保中央会への運用報告で提出するレポートを作成する。	共通ネットワークシステム運用
3	構成変更	随時	サーバ及びネットワーク機器の構成変更時に伴う設定作業を行う。	国保連合会 共通ネットワークシステム運用 共通ネットワークシステム保守

(e) 留意事項

・死活・エラー監視機能は独自処理システムで導入する機器及び分散配置用スイッチに対する機能提供をしない。

・死活・エラー監視機能は都道府県・保険者(伝送クライアント)に対する機能提供をしない。

⑥ 構成管理

(a) 概要

構成管理機能は SKY 社の SKYSEA Client View により実現する。

構成管理機能では管理対象機器にインストールしているミドルウェアのバージョン、インストール日付、有効期限等の情報を定期的に自動収集する。

収集した資産情報を一元的に管理することで、ミドルウェアの導入状況を把握する。

なお、構成管理機能、デバイス制御機能、リモート接続機能及び操作ログ収集機能は1つのミドルウェアで統合管理する。

国保連合会に導入するコンポーネントを以下に示す。

表 2-22 SKYSEA コンポーネント一覧

No.	コンポーネント	説明
1	管理コンソール(管理機)	国保連合会設置の運用管理クライアントに導入する。 国保連合会内の資産情報の閲覧を可能とする。
2	エージェント(端末機)	国保連合会設置のサーバ及びクライアントに導入する。 起動時または定期的に資産情報の自動収集が行われる。

(b) 機能イメージ

構成管理の機能イメージを以下に示す。

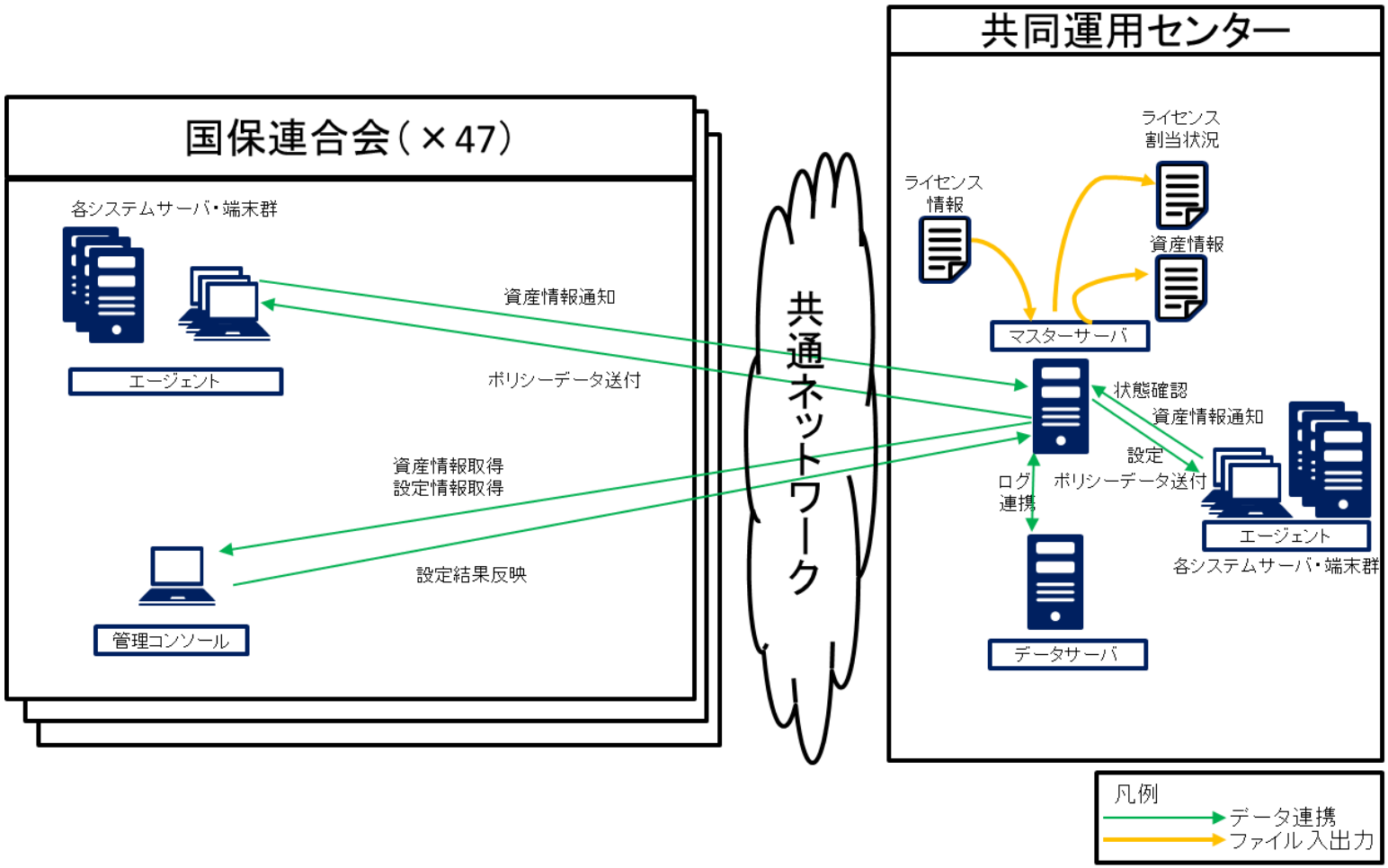


図 2-8 構成管理機能イメージ

(c) 提供機能

国保連合会に提供する構成管理機能を以下に示す。

表2-23 構成管理機能一覧

No.	機能	説明
1	資産情報収集	各システムサーバ・端末群にインストールしているミドルウェアのバージョン、インストール日付、有効期限等の情報を定期的に自動収集する。また、手動による収集も可能とする。
2	資産情報の閲覧	各システムサーバ・端末群から収集した資産情報を管理コンソールから閲覧することを可能とする。

(d) 運用項目

国保連合会内の資産情報の閲覧は可能であるが、国保連合会で実施する運用項目はない。

(e) 留意事項

・ 構成管理機能が利用可能なオペレーティングシステムのバージョン：
Microsoft Windows 10 Enterprise 2016 LTSB (64BitOS)
Microsoft Windows Server 2016

・ 構成管理機能を提供するソフトウェアが現行システムから変更となる。そのため、資産情報の閲覧手順が変更となる。

・ 管理コンソールの起動パスワードは拠点の担当者が決定し、国保連合会で管理する。

・ 構成管理の運用は共通ネットワークシステム運用で、ライセンス管理等を実施する。
ライセンス管理対象は以下とする。

表 2-24 ライセンス管理対象

No.	ソフトウェア
1	ウイルスバスター コーポレートエディション クライアント
2	SKYSEA Client View 端末機
3	InfoCage PC 検疫(InfoCage シリーズ検疫エージェント)
4	NeoFace Monitor V3 クライアント用-i
5	JP1/Automatic Job Management System - View

・ 構成管理機能は国保連合会に閲覧機能のみ提供を行うが、共通ネットワークシステム運用で資産情報を収集することを目的とする。
・ 構成管理機能は都道府県・保険者(伝送クライアント)に対する機能提供をしない。
・ 構成管理機能は独自処理システムに対して機能提供を行う。
ただし、独自処理システムで個別に調達した SKYSEA を導入している場合、機能提供の対象外とする。

(2)　セキュリティサービス

①　UTM(統合脅威管理)/FW(ファイアウォール)

(a) 概要

国保連合会内のシステム間及び国保連合会外との通信制御を行う。また、都道府県・保険者向けには、ウイルス対策や不正接続防止も行う。

表 2-25 UTM(統合脅威管理)/FW(ファイアウォール) 一覧

No.	UTM(統合脅威管理) /ファイアウォール(FW) 名	説明
1	連合会 FW#1～#2	2つの仮想 FW(連合会基幹共通 FW、連合会独自向け FW)が稼働する。 連合会 FW#1 と#2 で、冗長構成とする。
2	連合会基幹共通 FW (仮想)	国保連合会内の各システム間及び共通ネットワーク回線向けの通信の制御を行う。
3	連合会独自向け FW (仮想)	国保連合会の独自処理システム向け通信の制御を行う。
4	連合会関係機関向け FW#1～#2	都道府県・保険者との通信制御を行う。 連合会関係機関向け FW#1 と#2 で、冗長構成とする。 都道府県・保険者向けの独自処理システムを通信制御する。

(b) 機能イメージ

UTM(統合脅威管理) /FW(ファイアウォール)の機能イメージを以下に示す。

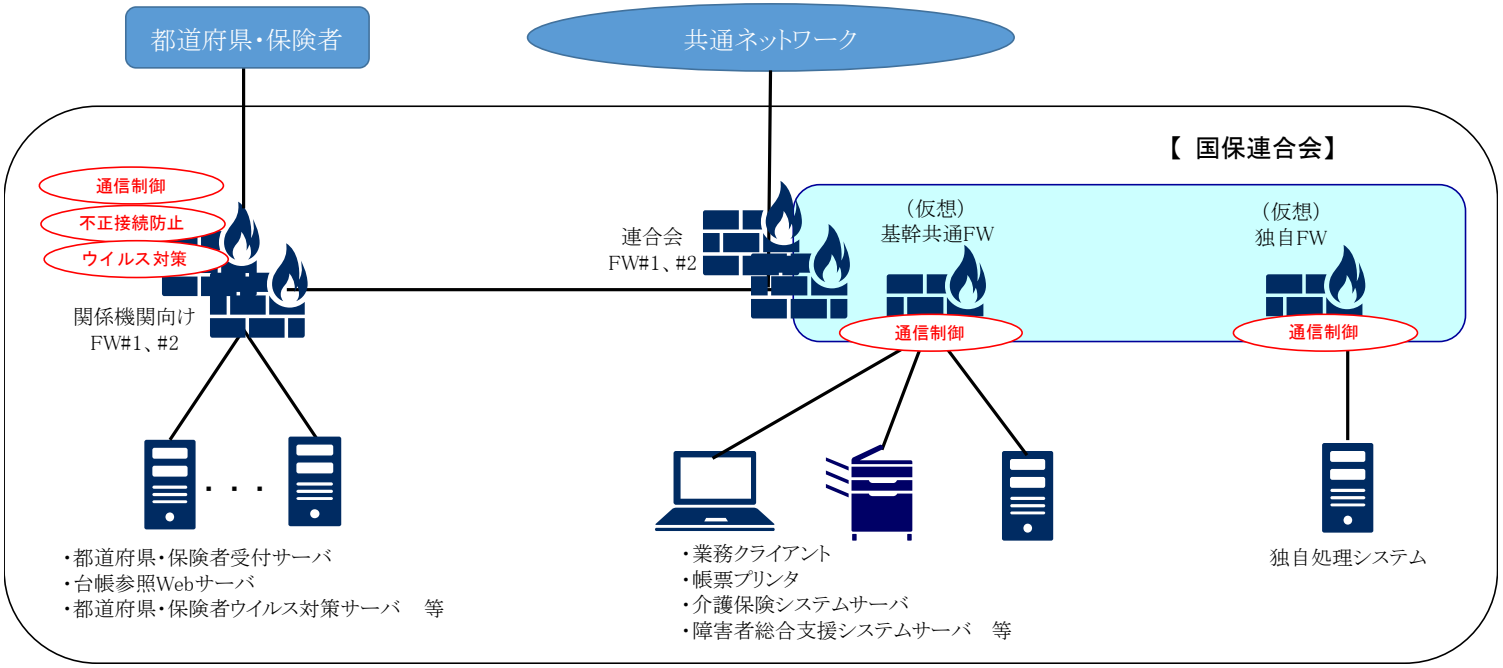


図 2-9 UTM/FW 機能イメージ

(c) 提供機能

UTM(統合脅威管理) / FW(ファイアウォール)の機能を以下に示す。

表 2-26 UTM(統合脅威管理) /FW(ファイアウォール)機能一覧

No.	機能	説明
1	ファイアウォール	ネットワークセグメント間を許可された通信のみを通し、不許可な通信をブロックする制御機能。 通信制御の結果を記録し、Syslog サーバに送信する。
2	仮想ファイアウォール	物理的なファイアウォール上に仮想的に複数のファイアウォールを構築する機能。 仮想ファイアウォールは、それぞれ異なる設定で動作させることが可能。 連合会 FW#1、#2 で、基幹共通 FW と独自向け FW を仮想 FW として構築する。
3	不正接続防止	通信を監視し、シグネチャにマッチングした攻撃を検知した場合、通信を遮断する。 不正接続防止は、都道府県・保険者との接続部分である関係機関向け FW で利用する。
4	ウイルス対策	シグネチャにマッチングしたウイルスファイルを検知した場合、ファイルを削除する。 ウイルス対策は、都道府県・保険者との接続部分である関係機関向け FW で利用する。

(d) 運用項目

UTM(統合脅威管理) /FW(ファイアウォール)の運用項目を以下に示す。

表 2-27 ネットワーク機器 運用項目一覧

No.	運用項目	頻度	説明	運用者
1	独自処理システム変更時に伴う通信ポリシー変更	随時	システム構成変更時等に通信ポリシーの変更を行う	国保連合会

(e) 留意事項

・ 連合会独自向け FW(仮想)の初期設定は全ての通信を遮断する設定となっている。そのため、国保連合会が「2.2.2 提供ドキュメント」に記載の「独自処理システム向けファイアウォール操作手順書」を参照して、独自処理システムで必要な通信ポートの許可を連合会独自向け FW(仮想)に設定する必要がある。

② 自動アクセス遮断

(a) 概要

自動アクセス遮断は、トレンドマイクロ社の Trend Micro Policy Manager（TMPM）を用いて実現する。L2SW とウイルス対策機能が連携し、クライアント PC でウイルス検知した時に、クライアント PC の通信を自動遮断し、ウイルス感染の拡大防止措置を自動化する。

表 2-28 自動アクセス遮断コンポーネント一覧

No.	コンポーネント	説明
1	センターウイルス対策連携装置#1	連合会ウイルス対策サーバから受信した感染クライアント PC の IP アドレスを、センターSDN コントローラ装置#1～#2 に連携する。
2	センターSDN コントローラ装置#1～#2	センターウイルス対策連携装置#1 から連携された情報を元に、クライアント L2SW を制御する。
3	連合会ウイルス対策サーバ#1	国保連合会設置のサーバ及びクライアント PC のウイルス対策機能を管理する。。
4	連合会クライアント L2SW#1～#4	センターSDN コントローラ装置からの制御を受け感染クライアント PC の通信を遮断する。（連合会クライアント L2SW の台数は国保連合会ごとに変動）
5	連合会運用クライアント L2SW#1～#2	
6	クライアント PC	ウイルス対策エージェント（CorpCL）がインストールされたクライアント PC で、No4-No5 の L2SW に接続しているクライアント PC が制御対象となる。

(b) 機能イメージ

自動アクセス遮断の機能イメージを以下に示す。

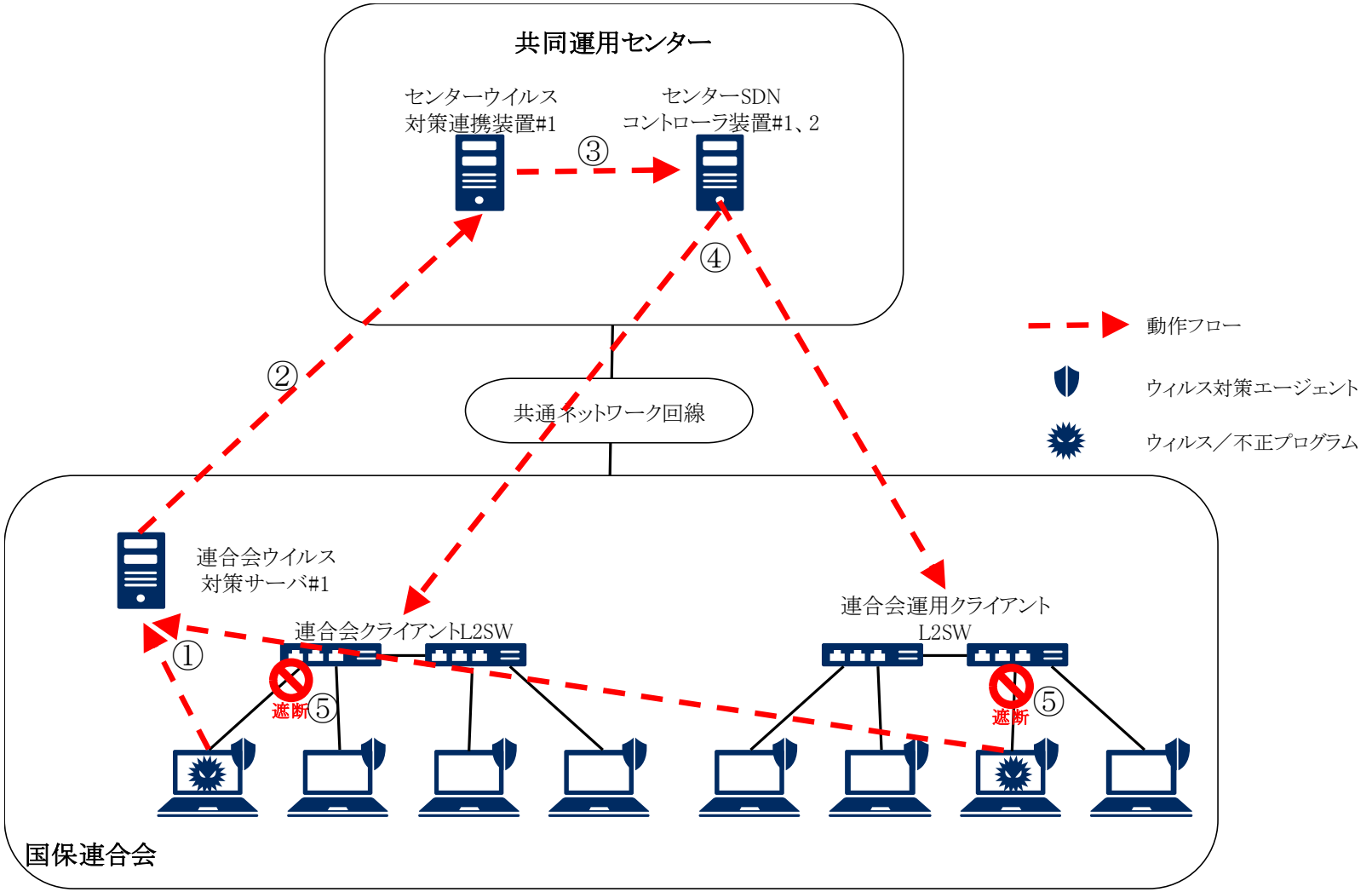


図 2-10 自動アクセス遮断 機能イメージ

表 2-29 自動アクセス遮断フロー

No.	機能	説明
①	感染検知	クライアントPCに導入したウイルス対策機能のエージェントでウイルス/不正プログラムの感染を検知し、連合会ウイルス対策サーバ#1に通知する。
②	感染情報通知	連合会ウイルス対策サーバ#1からセンターウイルス対策連携装置#1にクライアントPCの感染情報を通知する。
③	遮断連携	センターウイルス対策連携装置#1からセンターSDNコントローラ装置#1、#2に感染クライアントPCのIPアドレスを連携する。
④	遮断制御	センターSDNコントローラ装置#1、#2からクライアントL2SWを感染クライアントPCからの通信を遮断するよう制御する。
⑤	遮断	感染クライアントPCの通信をクライアントL2SWと接続されたポートで遮断する。

(c) 提供機能

自動アクセス遮断の提供機能は「2.1.2. (2)②(b)機能イメージ」に示す。

(d) 運用項目

遮断に関しては自動で実施するため、国保連合会で自動アクセス遮断に関する運用項目はない。

(e) 留意事項

- 自動アクセス遮断機能は独自処理システムに対する機能提供をしない。
- 自動アクセス遮断機能は都道府県・保険者(伝送クライアント)に対する機能提供をしない。

③ デバイス制御

(a) 概要

デバイス制御機能は SKY 社の SKYSEA Client View により実現する。
デバイス制御機能は管理対象機器で利用する内蔵・外付け CD/DVD ドライブや USB デバイスに対する利用制限を行う。
また、利用状況管理や利用が許可されていないデバイスの接続時にアラートを通報する機能を提供する。
デバイス制御機能の運用は国保連合会内の情報セキュリティ担当者と情報セキュリティ管理者により行う。
なお、構成管理機能、デバイス制御機能、リモート接続機能及び操作ログ収集機能は1つのミドルウェアで統合管理する。

国保連合会に導入するコンポーネントを以下に示す。

表 2-30 SKYSEA コンポーネント一覧

No.	コンポーネント	説明
1	管理コンソール(管理機)	国保連合会設置の業務クライアントに導入し、国保連合会の情報セキュリティ担当者のみが利用する。 国保連合会の情報セキュリティ担当者は利用者からのデバイス申請の受付け及び許可を実施する。
2	エージェント(端末機)	国保連合会設置のサーバ及びクライアントに導入する。 デバイス制御を行い、許可されたデバイスのみ利用可能とする。

(b) 機能イメージ

デバイス制御の機能イメージを以下に示す。

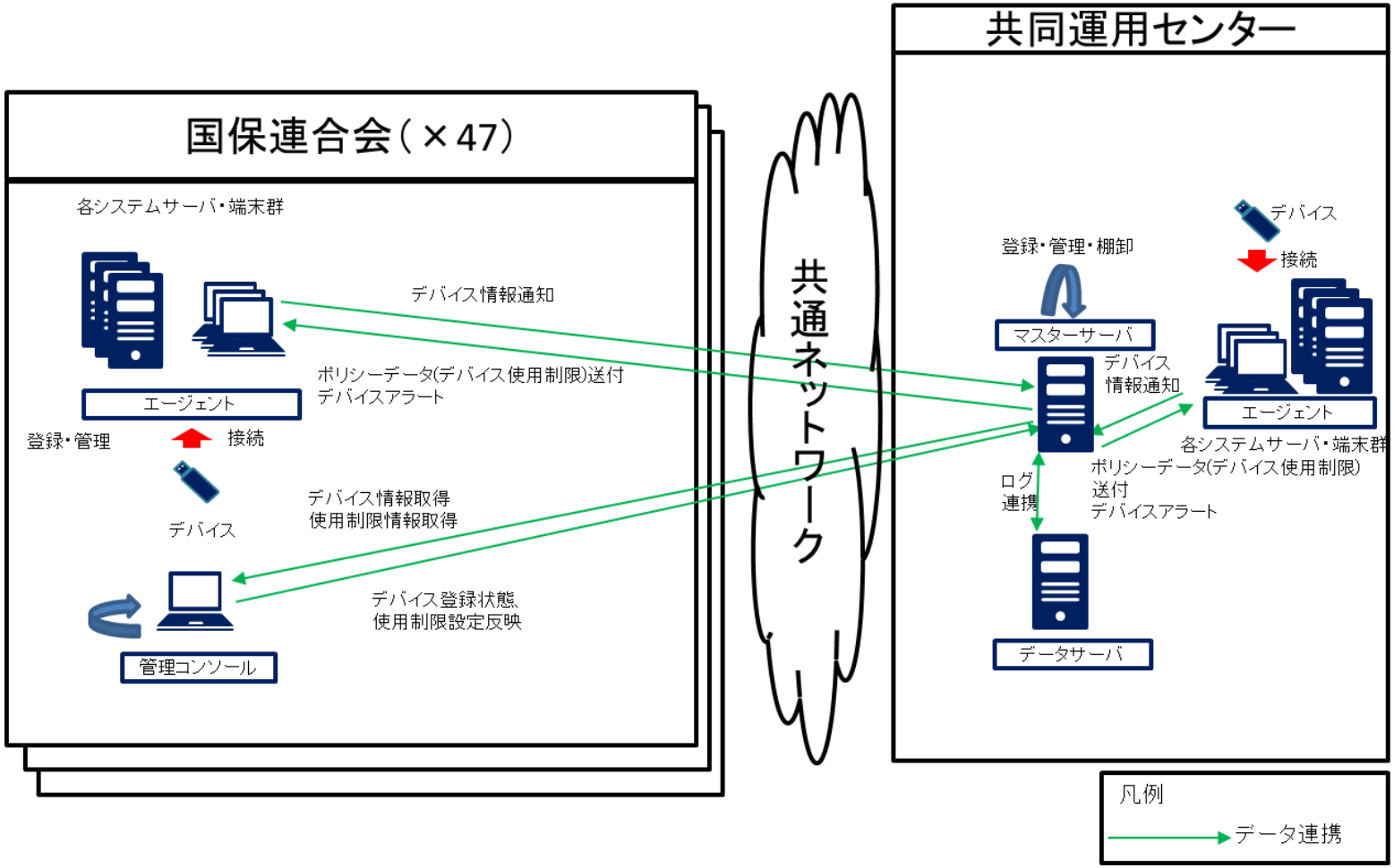


図 2-11 デバイス制御機能イメージ

（c） 提供機能

国保連合会に提供するデバイス制御機能を以下に示す。

表 2-31 デバイス制御機能一覧

No.	機能	説明
1	登録・管理・棚卸	管理コンソールからデバイスの登録、登録されているデバイス情報の確認、利用状況の確認を可能とする。登録したデバイス情報は共同運用センターで一元管理される。また、利用可否の変更やデバイス情報の削除も可能とする。
2	利用制限	内蔵・外付け CD/DVD ドライブ、SD カード及び USB デバイスを、デバイスごとに利用不可能や読み取り専用の設定を行う。Bluetooth デバイスや無線 LAN 機能の利用は禁止とする。
3		あらかじめ台帳に登録したデバイスのみ利用可能とする。
4		デバイス制御機能の利用制限はマスターサーバが停止状態でもエージェントに配布されたデバイス制御ポリシーに基づき動作する。
5	デバイス検知／登録確認	各システムサーバ・端末群においてデバイス接続を検知し、登録済みデバイスであるか確認する。 登録済みの場合、デバイスの利用が可能となる。未登録の場合、アラートを通知する。

(d) 運用項目

デバイス制御機能の運用項目を以下に示す。

情報セキュリティ担当者が利用する管理コンソールは、任意の業務クライアントに導入する。

表 2-32 デバイス制御機能 運用項目一覧

No.	運用項目		頻度	説明	運用者
1	USB デバイス(内蔵・外付け CD/DVD ドライブ含む)	利用申請	申請時	利用者は利用するデバイスの種別と接続するクライアント PC を情報セキュリティ担当者に申請する。	国保連合会
				情報セキュリティ担当者は利用者からのデバイスの利用申請/削除申請の内容を確認し、情報セキュリティ管理者に提出する。 利用者が内蔵・外付け CD/DVD ドライブの利用を希望し、かつ書き込みも希望する場合、書き込み理由を利用者に確認する。	情報セキュリティ担当者
				情報セキュリティ管理者は、申請書を確認の上、承認／却下を情報セキュリティ担当者に通知する。	情報セキュリティ管理者
				情報セキュリティ担当者は承認／却下の結果を利用者へ通知する。承認された場合、デバイス登録設定を行い、利用者に設定完了を通知する。	情報セキュリティ担当者
2		削除申請	申請時	情報セキュリティ担当者は、利用者から連絡をうけた管理対象デバイスについて、登録削除の対応を実施する。	情報セキュリティ担当者
3		台帳の棚卸し	3 か月ごと	管理コンソールから登録された承認済みデバイスの利用状況を確認する。一定期間利用していないデバイスは利用者に今後の利用有無を確認する。利用予定がないデバイスは登録削除を行う。	情報セキュリティ担当者

（e） 留意事項

- デバイス制御機能が利用可能なオペレーティングシステムのバージョン：
  Microsoft Windows 10 Enterprise 2016 LTSB (64BitOS)
  Microsoft Windows Server 2016
- デバイス制御機能一元化に伴い、現行システムでは国保連合会に設置されていたマスターサーバを共同運用センターに設置する。
  参照範囲は国保連合会ごとに制御する。
- 現行システムで運用しているデバイス登録用端末を廃止するため、申請手順及び申請フォーマットが変更となる。
- 構成管理、操作ログ収集、リモート接続するために SKYSEA の管理コンソールを運用管理クライアントに導入するが、権限のない運用者が不正にデバイスの許可申請を行うことを防ぐため、デバイス制御機能は利用不可設定とする。
- デバイス制御機能を利用可能とする管理コンソール(以降「管理機(SC)」と記載)は情報セキュリティ担当者が任意のクライアント(システムの推奨としては業務クライアント)に導入する。管理機(SC)は国保連合会内で最低１台は指定すること。管理機(SC)はデバイス制御の申請、許可のみ可能とする。(構成管理機能、操作ログ収集機能、リモート接続機能は利用不可設定とする。)
  そのため、情報セキュリティ担当者は管理機(SC)のパスワード管理を適切に行うこと。
  なお、上記情報セキュリティ担当者用の業務クライアントについては、2018 年 9 月末時点で想定しているものであり、今後の検討及び調整により変更となる可能性がある。
- 管理コンソールの起動パスワードは拠点の担当者が決定し、国保連合会で管理する。
- 共同運用センター設置のマスターサーバと通信できない状況では、登録済みのデバイスであっても一度も利用実績がない場合、当該デバイスは利用できない。
- デバイス制御機能は都道府県・保険者(伝送クライアント)に対する機能提供をしない。
- デバイス制御機能は独自処理システムに対して機能提供を行う。
  ただし、独自処理システムで個別に調達した SKYSEA を導入している場合、機能提供の対象外とする。
- 仮想サーバへの USB デバイス制御機能は対象外とする。

・　制御対象デバイス種別ごとの基本設定および申請により可能な個別設定を以下に示す。

表 2-33 制御対象デバイス種別

No.	デバイス種別	説明
1	USB メモリ/USB ハードディスク	利用禁止設定とし、申請で登録したデバイスは読み書き可能とする。
2	内蔵・外付け CD/DVD ドライブ	読み取り専用設定とし、書き込みが必要な場合、申請の上、書き込み許可設定を行う。
3	フロッピーディスクドライブ	読み取り専用設定とし、書き込みが必要な場合、申請の上、書き込み許可設定を行う。
4	カードリーダー/ライター	利用禁止設定とし、申請で登録したデバイスは読み書き可能とする。
5	カードメディア	利用禁止設定とし、申請で登録したデバイスは読み書き可能とする。
6	イメージスキャナ	利用禁止設定とし、申請で登録したデバイスは利用可能とする。

・　利用禁止デバイスを以下に示す。利用禁止デバイスは申請による利用も不可とする。

表 2-34 利用禁止デバイス

No.	デバイス種別
1	Bluetooth デバイス
2	無線 LAN デバイス
3	デジタルカメラ等
4	eSATA 接続ハードディスク
5	テープドライブ、スマートカードリーダー
6	モバイル端末

・　デバイスアラートは以下の場合に出力する。

表 2-35 デバイスアラート

No.	デバイス種別
1	台帳登録外デバイス接続時
2	禁止デバイス利用時
3	記憶媒体/メディア書き込み時

④ 操作ログ収集

(a) 概要

操作ログ収集機能は SKY 社の SKYSEA Client View により実現する。

操作ログ収集機能は管理対象機器内においてユーザが操作した内容(起動/終了、アプリケーション利用、ファイルアクセス等)に関する操作ログを収集、保管する機能を提供する。

なお、構成管理機能、デバイス制御機能、リモート接続機能及び操作ログ収集機能は1つのミドルウェアで統合管理する。

国保連合会に導入するコンポーネントを以下に示す。

表 2-36 SKYSEA コンポーネント一覧

No.	コンポーネント	説明
1	管理コンソール(管理機)	国保連合会設置の運用管理クライアントに導入する。 国保連合会内の収集した操作ログの閲覧を可能とする。
2	エージェント(端末機)	国保連合会設置のサーバ及びクライアントに導入する。 リアルタイムで操作ログの自動収集が行われる。

(b) 機能イメージ

操作ログ収集の機能イメージを以下に示す。

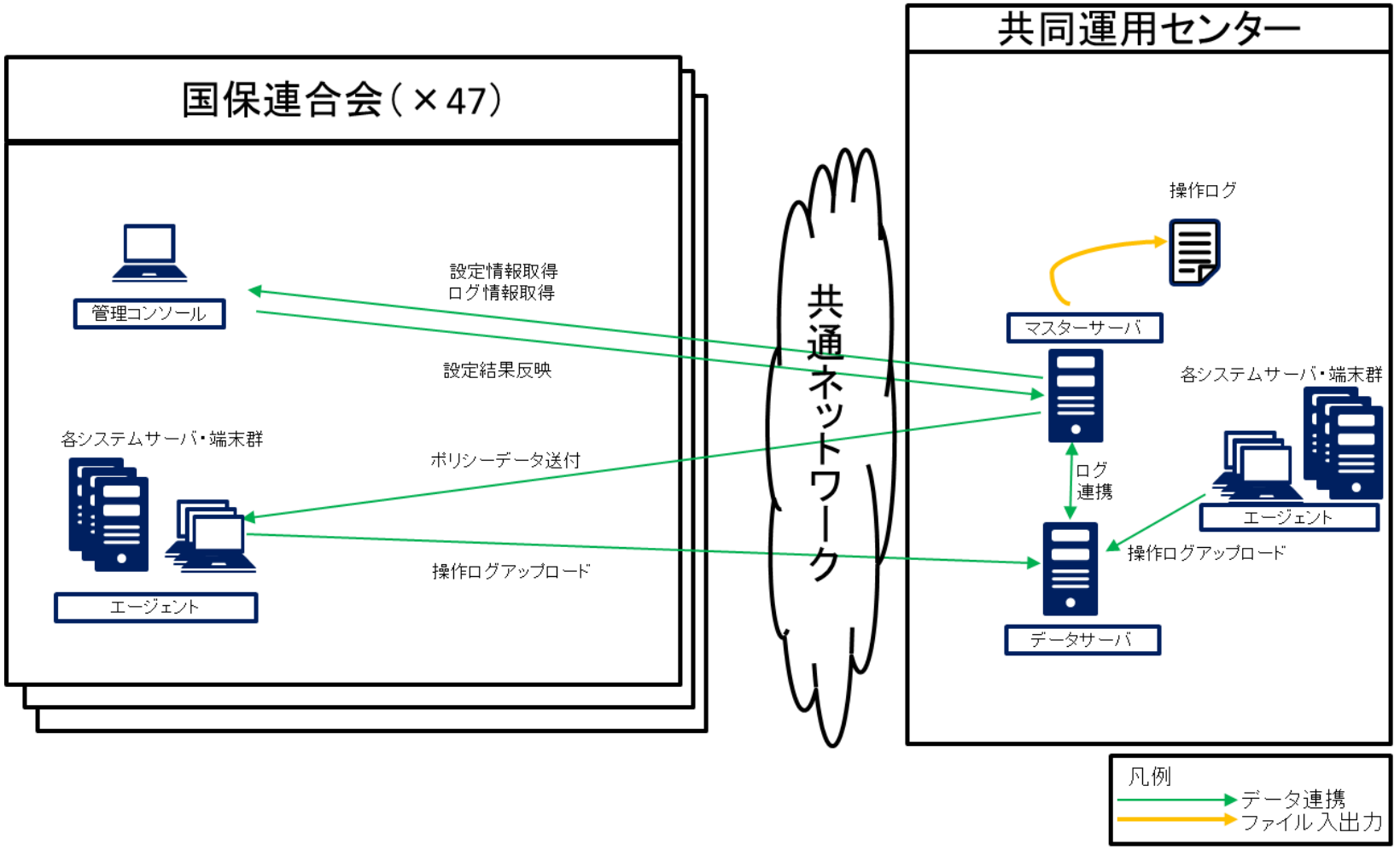


図 2-12 操作ログ収集機能イメージ

(c) 提供機能

国保連合会に提供する操作ログ収集機能を以下に示す。

表 2-37 操作ログ収集機能一覧

No.	機能	説明
1	操作ログ収集	各システムサーバ・端末群から操作ログをリアルタイムに収集し、共同運用センター設置のマスターサーバに転送する。
2	操作ログ閲覧	各システムサーバ・端末群から収集した操作ログを管理コンソールから条件を指定して、閲覧可能とする。

(d) 運用項目

国保連合会内の操作ログ収集情報の閲覧は可能であるが、操作ログ収集機能の運用項目はない。

(e) 留意事項

- 操作ログ収集機能が利用可能なオペレーティングシステムのバージョン：
  Microsoft Windows 10 Enterprise 2016 LTSB (64BitOS)
  Microsoft Windows Server 2016
- 管理コンソールの起動パスワードは拠点の担当者が決定し、国保連合会で管理する。
- 操作ログ収集機能は都道府県・保険者(伝送クライアント)に対する機能提供をしない。
- 操作ログ収集機能は独自処理システムに対する機能提供をしない。

⑤ 不正接続防止

(a) 概要

国保連合会内のクライアントPC及びプリンタ等のIPアドレスとMACアドレスを許可登録し、許可登録されていない不正に接続された機器をネットワークから遮断する機能を提供する。

表 2-38 不正接続防止 コンポーネント一覧

No.	コンポーネント	説明
1	センター不正接続防止管理サーバ#1～#2	全国の国保連合会に設置された不正接続防止装置を一元管理する。
2	連合会不正接続防止装置#1	ネットワークに接続された機器のデータを収集し、不正に接続された機器をネットワークから遮断する。

(b) 機能イメージ

不正接続防止の機能イメージを以下に示す。

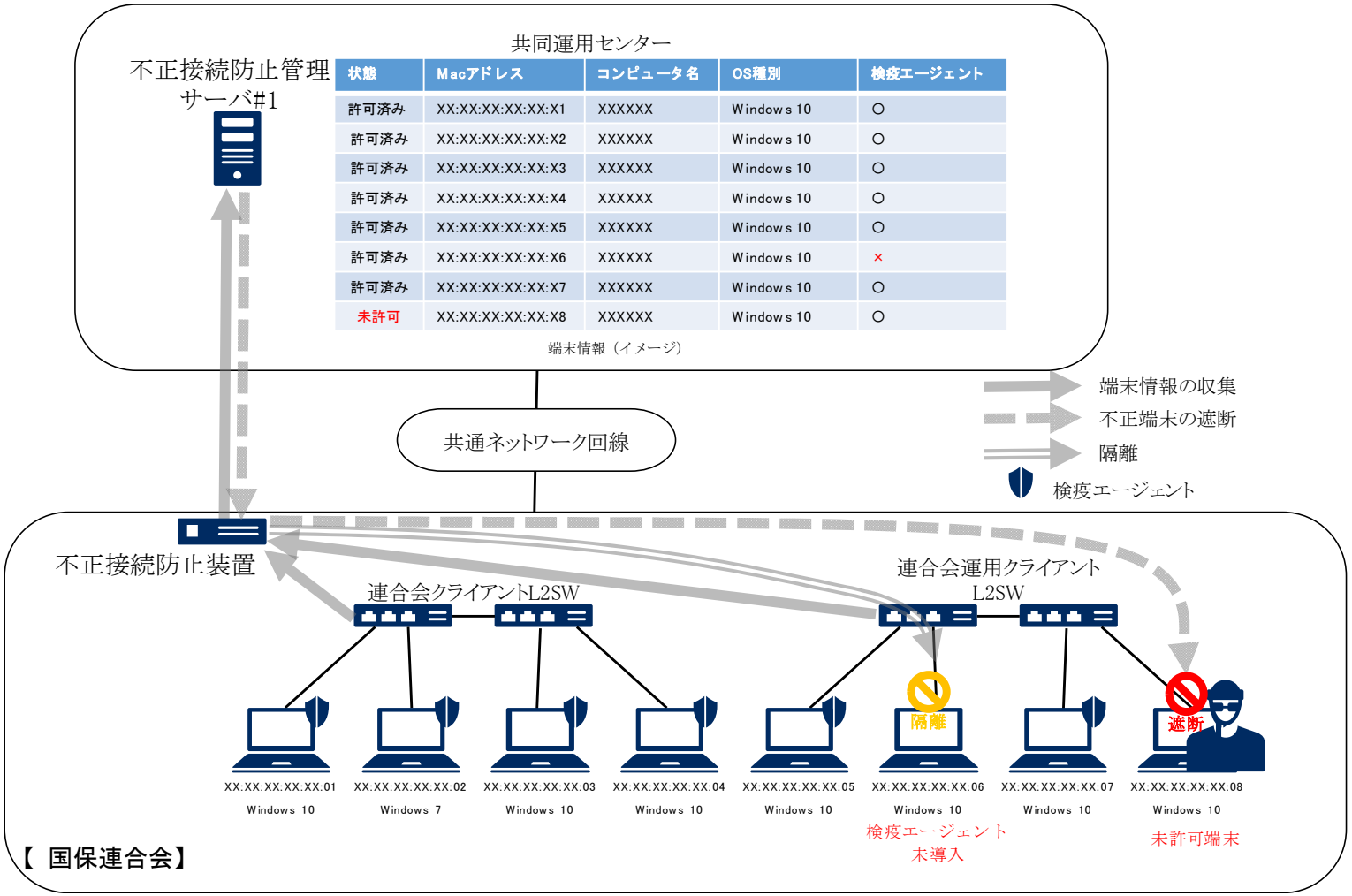


図 2-13 不正接続防止の機能イメージ

(c) 提供機能

不正接続防止で提供する機能を以下に示す。

表 2-39 不正接続防止機能一覧

No.	機能	説明
1	端末情報収集	国保連合会に設置された不正接続防止装置がクライアント PC 及びプリンタから IP アドレス、MAC アドレス、OS 種別等の機器情報を収集する。 共同運用センターに設置された不正接続防止管理サーバが収集した端末情報を集中管理する。
2	不正接続防止	不正接続防止機能は、クライアント PC 及びプリンタを接続するセグメント単位で MAC アドレス及び IP アドレスをキーとして監視する。 不正接続の発見時に、不正接続機器の遮断と、不正接続防止管理サーバにアラートを通知する。 共通ネットワークシステム運用が不正接続防止管理サーバから接続を許可する MAC アドレス及び IP アドレスの設定を実施する。(新規クライアント PC 及びプリンタの導入時)
3	PC 検疫連携	不正接続防止装置で検疫エージェントが導入されていないクライアント PC の接続を遮断する。 クライアント PC に検疫エージェントが導入された後は、自動的にクライアント PC の遮断は解除される。

(d) 運用項目

不正接続防止機能の運用項目を以下に示す。

表 2-40 不正接続防止機能　運用項目一覧

No.	運用項目	頻度	説明	運用者
1	MAC アドレス情報収集と通知	随時	クライアントPC 及びプリンタの増設・交換の際に、接続を許可するため該当機器の MAC アドレス情報を確認し、共通ネットワークシステム運用に申請を行う。	国保連合会 共通ネットワークシステム運用

(e) 留意事項

- 不正接続防止機能は独自処理システムに対する機能提供をしない。
- 不正接続防止機能は都道府県・保険者(伝送クライアント)に対する機能提供をしない。

⑥ PC 検疫

(a) 概要

国保連合会内のクライアントPC で検疫ポリシーの適合状態を検査し、問題ないと判断されたクライアントPC のみネットワークへの接続を許可し、不適合となったクライアントPC は検疫ネットワークに隔離する機能を提供する。

表 2-41 PC 検疫コンポーネント一覧

No.	コンポーネント	説明
1	センター検疫管理サーバ#1～#2	検疫エージェントが導入されたクライアントPC を一元管理する。
2	検疫エージェント	各クライアントPC のポリシー適合状況の確認及び最新ポリシーのアップデートを行う。

(b) 機能イメージ

PC 検疫の機能イメージを以下に示す。

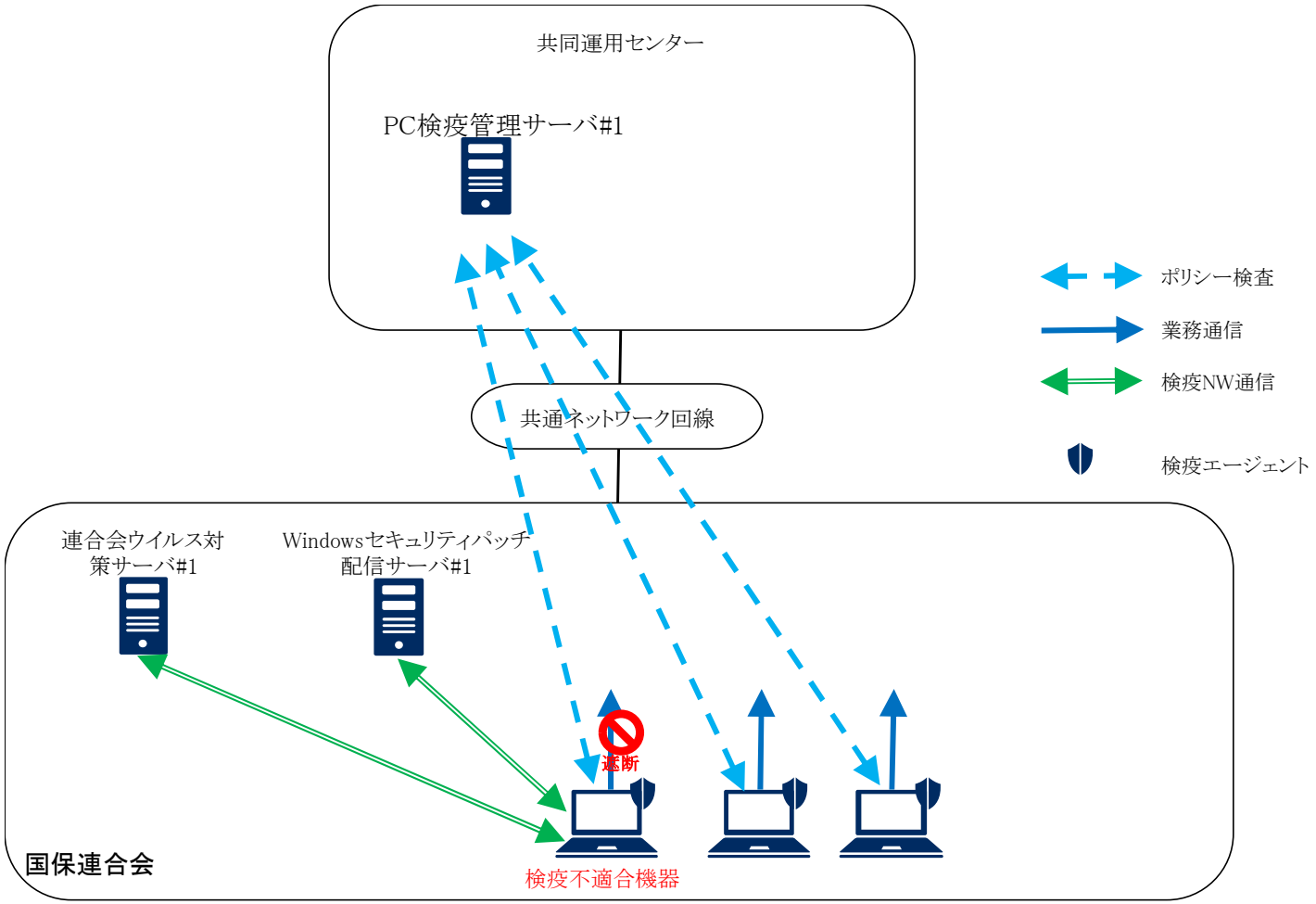


図 2-14 PC 検疫機能イメージ

(c) 提供機能

PC 検疫で提供する機能を以下に示す。

表 2-42 PC 検疫機能一覧

No.	機能	説明
1	ポリシー検査機能	定期的に PC 検疫管理サーバと検疫エージェント間で通信し、クライアント PC を検査する。 検疫エージェントが未導入の場合、不正接続防止機能によりクライアント PC の接続を遮断する。 ポリシー検査機能による自動検査は、クライアント PC の起動直後と、起動後 3 時間ごとに動作する。 検査項目は「表 2-43 PC 検疫検査項目一覧」に示す。
2	適合結果通知機能	ポリシー検査機能の結果を「適合/不適合」で検疫エージェントに通知する。
3	隔離機能	適合結果通知機能で「不適合」の結果を受け取った場合、クライアント PC を検疫ネットワークへ隔離する。 検疫ネットワークに隔離された場合、ウイルス対策機能及び Windows セキュリティパッチ配信機能以外への通信を遮断する。 セキュリティ確保のため、PC 検疫管理サーバと検疫エージェントが 5 分間通信不能となった場合にも、クライアント PC を検疫ネットワークに隔離する。
4	解除機能	隔離機能で隔離されていたクライアント PC が適合結果通知機能から「適合」の結果を受け取った場合、クライアント PC の隔離を解除する。

表 2-43 PC 検疫検査項目一覧

No.	検査項目	概要
1	クライアント OS	WindowsOS のバージョンを検査する。 Windows10 以外のクライアント PC は検査不適合とする。
2	検疫エージェントの導入有無	不正接続防止機能で検疫エージェントの導入有無を検査する。 検疫エージェントが導入されていないクライアント PC の接続を遮断する。
3	Windows セキュリティパッチの適用有無	Windows セキュリティパッチ配信機能から配信される Windows セキュリティパッチの導入状況を検査する。 Windows セキュリティパッチ配信サーバから配信されてから 3 日を適用猶予とし、猶予を超えて未適用の場合、検査不適合とする。
4	ウイルス対策パターンファイルの適用有無	ウイルス対策パターンファイルの適用状況を検査する。 PC 検疫管理サーバが保持するウイルス対策パターンファイルのバージョン情報と、クライアント PC に適用されているバージョン情報を比較することで検査を実施する。 ウイルス対策サーバから 2 日を適用猶予とし、猶予を超えて未適用の場合、検査不適合とする。
5	SKYSEA エージェントの導入有無	SKYSEA エージェントの導入有無を検査する。 未導入のクライアント PC は検査不適合とする。
6	Splunk エージェントの導入有無	Splunk エージェントの導入有無を検査する。 未導入のクライアント PC は検査不適合とする。

(d) 運用項目

隔離／解除は自動で実施するため、国保連合会で PC 検疫に関する運用項目はない。

(e) 留意事項

- PC 検疫機能は独自処理システムに対する機能提供をしない。
- PC 検疫機能は都道府県・保険者(伝送クライアント)に対する機能提供をしない。

⑦ Windows セキュリティパッチ配信

(a) 概要

Windows セキュリティパッチ配信機能は、Windows Server 2016 のバンドル機能（WSUS）を用いて実現する。

クライアント及び Windows サーバに対し、Windows 及び Office のセキュリティパッチを配信する機能を提供する。

表 2-44 Windows セキュリティパッチ配信 コンポーネント一覧

No.	コンポーネント	説明
1	センターセキュリティパッチ管理サーバ#1	全国の連合会セキュリティパッチ配信サーバ#1 に対し、セキュリティパッチを配信する。
2	連合会セキュリティパッチ配信サーバ#1	国保連合会のクライアント及び Windows サーバに対しセキュリティパッチを配信する。 都道府県保険者セキュリティパッチ配信サーバ#1 に対し、セキュリティパッチを配信する。
3	都道府県保険者セキュリティパッチ配信サーバ#1	都道府県・保険者向け伝送クライアントに対し、セキュリティパッチを配信する。

(b) 機能イメージ

Windows セキュリティパッチ配信の機能イメージを以下に示す。

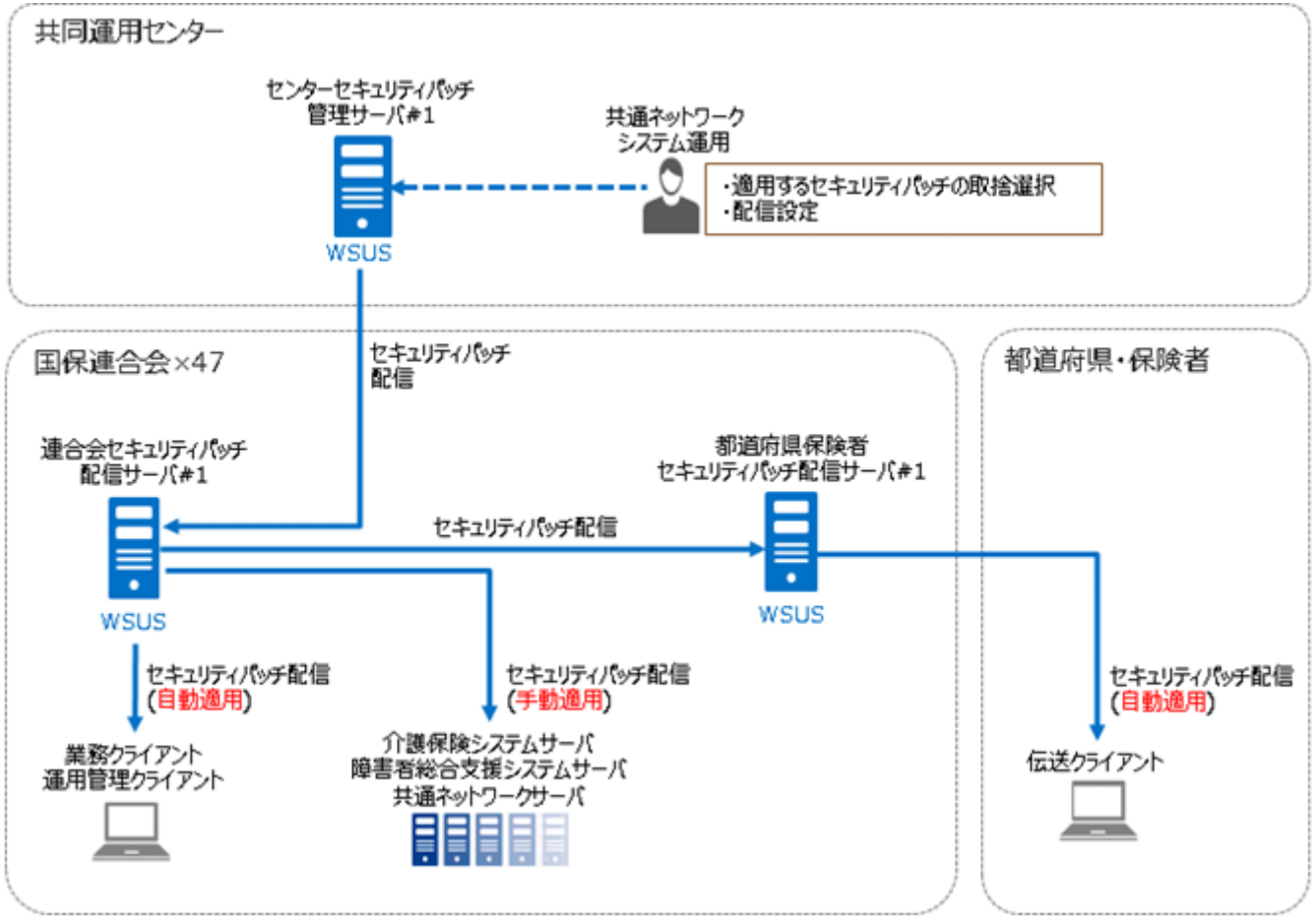


図 2-15 Windows セキュリティパッチ配信の機能イメージ

(c) 提供機能

Windows セキュリティパッチ配信で提供する機能を以下に示す。

表 2-45 Windows セキュリティパッチ配信機能一覧

No.	機能	説明
1	セキュリティパッチ配信機能(クライアント)	国保連合会のクライアントに対し、Windows 及び Office のセキュリティパッチを毎月自動で配信する機能を提供する。 都道府県・保険者向け伝送クライアントに対し、Windows 及び Office のセキュリティパッチを毎月自動で配信する機能を提供する。
2	セキュリティパッチ配信機能(Windows サーバ)	国保連合会の Windows サーバに対し、Windows 及び Office のセキュリティパッチを配信する機能を提供する。定期的な配信は行わず、必要に応じて配信し、保守業者が手動で適用する。

(d) 運用項目

Windows セキュリティパッチ配信機能の運用項目を以下に示す。

表 2-46 Windows セキュリティパッチ配信機能 運用項目一覧

No.	運用項目	頻度	説明	運用者
1	全国へセキュリティパッチの配信	毎月	全国の国保連合会に対してセキュリティパッチの配信を行う。	共通ネットワークシステム運用
2	セキュリティパッチ適用後の再起動(クライアント)	毎月	クライアントに対して、毎月、セキュリティパッチが自動で適用される。必要に応じてセキュリティパッチ適用後のクライアント再起動を行う。	国保連合会 都道府県・保険者
3	セキュリティパッチ適用及びセキュリティパッチ適用後の再起動(Windows サーバ)	随時	Windows サーバに対して、必要に応じてセキュリティパッチの配信・適用を行う。また、セキュリティパッチ適用後のサーバ再起動を行う。	共通ネットワークシステム運用 各システム保守業者

(e) 留意事項

・Windows セキュリティパッチ配信の対象製品は、Windows10 Enterprise 2016 LTSB、Windows 8.1 Pro、Windows Server 2016、Microsoft Office 2013/2016 を対象とする。

・配信は「セキュリティ問題の修正プログラム」のみ対象とする。

・Windows 8.1 Pro、Microsoft Office 2013 は伝送クライアントのみ対象とする。

・Windows10 Enterprise 2016 LTSB、Windows 8.1 Pro、Microsoft Office 2013/2016 のセキュリティパッチは毎月自動で配信し、配信日の 11:00 以降に自動適用を行う。

・Windows Server 2016 のセキュリティパッチは自動で配信せず、保守業者がアップデートを手動で行う運用とし、定期アップデートの対象外とする。

・都道府県・保険者（伝送クライアント）に対する機能提供について

Windows セキュリティパッチ配信機能は、都道府県・保険者（伝送クライアント）に対する機能提供を行う。

対象とするオペレーティングシステム及び Microsoft Office のバージョンは、伝送クライアントの必要要件に準ずる。

都道府県・保険者（伝送クライアント）の Windows セキュリティパッチ配信機能接続先を以下に記載する。

Windows セキュリティパッチ配信機能接続先：連合会都道府県保険者セキュリティパッチ配信サーバ#1

・都道府県・保険者の伝送クライアントのみ Windows10 Enterprise 2019 LTSC を 2020 年 5 月より提供する。

・独自処理システムに対する機能提供について

Windows セキュリティパッチ配信機能は、独自処理システムで利用するサーバに対して機能提供の対象外とする。

Windows セキュリティパッチ配信機能は、独自処理システムで利用するクライアントに対して機能提供を行う。

対象とするオペレーティングシステム及び Microsoft Office のバージョン：

Microsoft Windows 10 Enterprise 2016 LTSB (64BitOS)

Microsoft Office 2016

独自処理システムで利用するクライアントの Windows セキュリティパッチ配信機能接続先を以下に記載する。

Windows セキュリティパッチ配信機能接続先：連合会セキュリティパッチ配信サーバ#1

⑧ ウイルス対策

(a) 概要

ウイルス対策機能はトレンドマイクロ社のウイルスバスターコーポレートエディションにより実現する。

ウイルス対策機能では管理対象機器に対して定期的にウイルスパターンファイル及び検索エンジンを配布し、定期スキャン、手動スキャン及びリアルタイムスキャンによる不正プログラムの検索/処理を実行する機能を提供する。

国保連合会に導入するコンポーネントを以下に示す。

表 2-47 ウイルス対策コンポーネント一覧

No.	コンポーネント	説明
1	連合会ウイルス対策サーバ#1	国保連合会設置のサーバ及びクライアントのウイルス対策機能を管理する。
2	都道府県・保険者ウイルス対策サーバ#1	都道府県・保険者の伝送クライアントのウイルス対策機能を管理する。
3	ウイルス対策エージェント	国保連合会設置のサーバ及びクライアント PC に導入する。

(b) 機能イメージ

ウイルス対策の機能イメージを以下に示す。

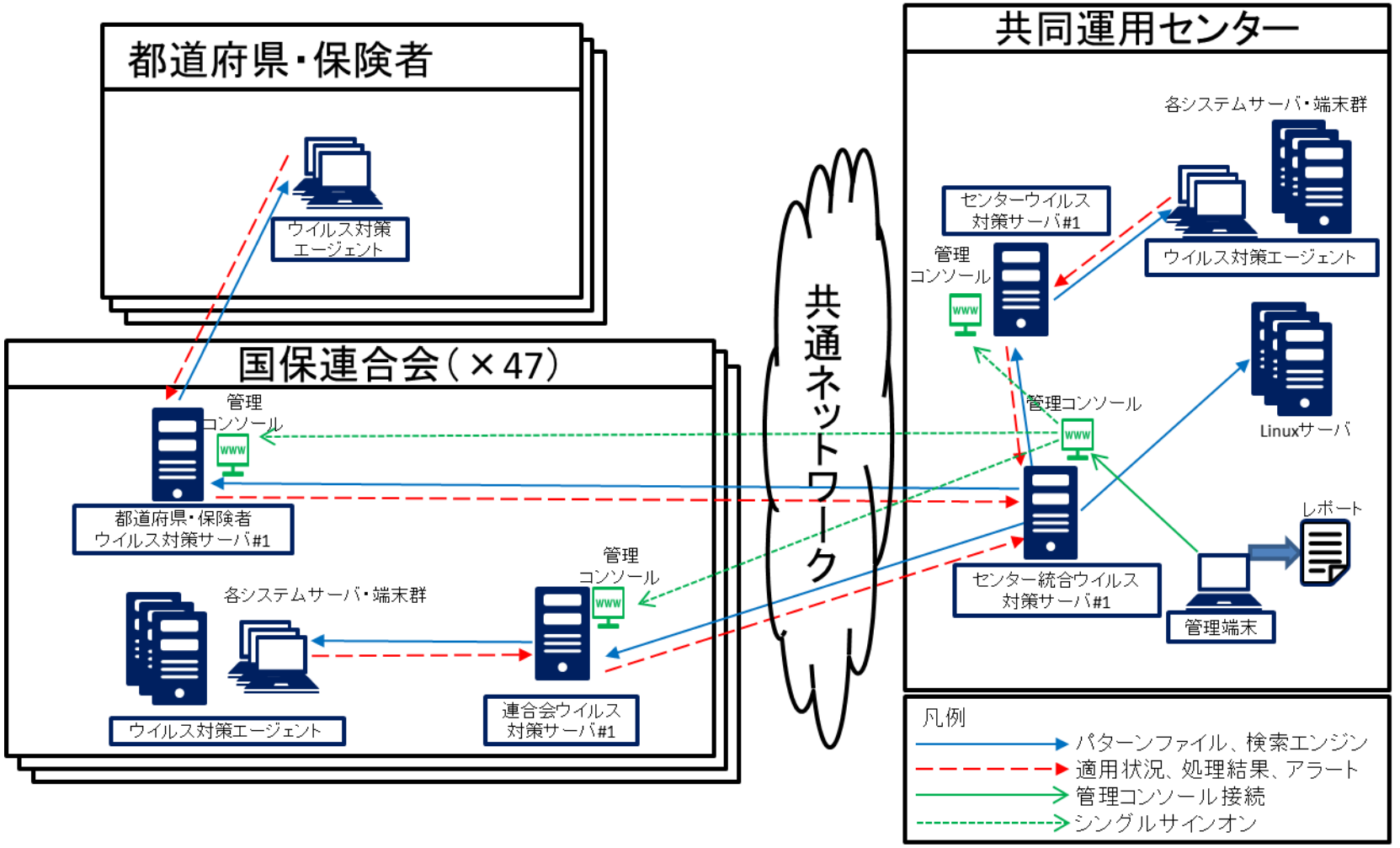


図 2-16 ウイルス対策機能イメージ

（c）提供機能

国保連合会に提供するウイルス対策機能を以下に示す。

表 2-48 ウイルス対策機能一覧

No.	機能	説明
1	配信対応	ウイルス対策サーバ、ウイルス対策対象機器にパターンファイル・検索エンジンを配布する。
2	リアルタイムスキャン	パターンファイルを基にリアルタイムで不正プログラムの検索/処理を実行する。 リアルタイムスキャンは基本有効とする。ただし、レスポンス遅延等が発生する場合、対象のフォルダを除外する。 また、他のソフトウェアの処理停止等が発生し、やむを得ない場合に限りリアルタイムスキャンを無効化する。
3	手動スキャン	パターンファイルを基に手動で指定フォルダの不正プログラムの検索/処理を実行する。 手動スキャンを行う場合、業務影響を考慮した上で実行する。
4	定時スキャン	パターンファイルを基に定時に指定フォルダの不正プログラムの検索/処理を自動で実行する。 サーバに対するフルスキャンを毎月１回実行する。

(d) 運用項目

ウイルス対策機能の運用項目を以下に示す。

表 2-49 ウイルス対策機能 運用項目一覧

No.	運用項目	頻度	説明	運用者
1	パターンファイル配信対応	日次１回 (共通ネットワークシステム運用の業務日)	共通ネットワークシステム運用はパターンファイルを取得し、共同運用センター設置のウイルス対策機能統合管理サーバに格納する。 その後、連合会ウイルス対策サーバ及び都道府県・保険者ウイルス対策サーバに自動で配布する。	共通ネットワークシステム運用
2	検索エンジン配信対応	検索エンジン更新時	共通ネットワークシステム運用は検索エンジンを取得し、共同運用センター設置のウイルス対策機能統合管理サーバに格納する。 その後、連合会ウイルス対策サーバ及び都道府県・保険者ウイルス対策サーバに手動で配布する。	共通ネットワークシステム運用
3	不正プログラム検知時対応	不正プログラム検知時	共通ネットワークシステム運用/国保連合会担当者は不正プログラム検知時、メールの通知、自動遮断の状況、イベントログによる通知状況の確認を行い、検知のあった対象機器で手動スキャンを実施する。	国保連合会 共通ネットワークシステム運用
4	管理対象機器追加、削除対応	管理対象機器追加、削除時	国保連合会担当者は管理対象機器が追加、削除された際に申請を行い、共通ネットワークシステム運用が連合会ウイルス対策サーバで追加、削除対応を実施する。	国保連合会 共通ネットワークシステム運用

（e）留意事項

- ウイルス対策機能が利用可能なオペレーティングシステムのバージョン：
  Microsoft Windows 10 Enterprise 2016 LTSB (64BitOS)
  Microsoft Windows Server 2016
  Microsoft Windows 8.1 Pro Update(64BitOS)　※都道府県・保険者(伝送クライアント)のみ
- パターンファイルの配布は日次で行う。国保連合会設置のウイルス対策サーバに対しては 20:00～23:00 の間で分散して配信する。
  ウイルス対策エージェントには、起動時または 12:00 に配信される。
- ウイルス対策エージェントのアンインストールはパスワードによる制限を行う。
- 不正プログラム検知時に自動遮断が失敗した場合、共通ネットワークシステム運用から国保連合会で感染端末の LAN ケーブルの抜線を依頼する連絡を行う。
- 定時スキャン設定は連合会運用試験の期間で設定の調整及び変更を国保連合会で実施する予定となる。
- ウイルス対策機能は都道府県・保険者(伝送クライアント)に対する機能提供をする。
  なお、ウイルス対策機能を都道府県・保険者(伝送クライアント)に導入する場合、必要なライセンスを調達する必要がある。
  ただし、都道府県・保険者(伝送クライアント)で個別に調達したウイルス対策製品を導入している場合、機能提供の対象外とする。
- ウイルス対策機能は独自処理システムに対して機能提供を行う。
  ただし、独自処理システムで個別に調達したウイルス対策製品を導入している場合、機能提供の対象外とする。

⑨ ログ収集・分析

共同運用センター、国保中央会、国保連合会に設置されている特定個人情報・個人情報に係る機器から発生する各種ログの収集と分析を行う機能を提供する。

(a) ログ収集

ア. 概要

Splunk 社の Splunk を導入し、国保連合会設置のサーバ及びクライアント PC の操作ログ、OS ログ、ネットワークログ、DB ログ等を収集し一元管理する。収集対象の機器には Splunk のエージェント機能である Universal Forwarder を導入しログ収集の機能を提供する。

イ. 機能イメージ

ログ収集の機能イメージを以下に示す。

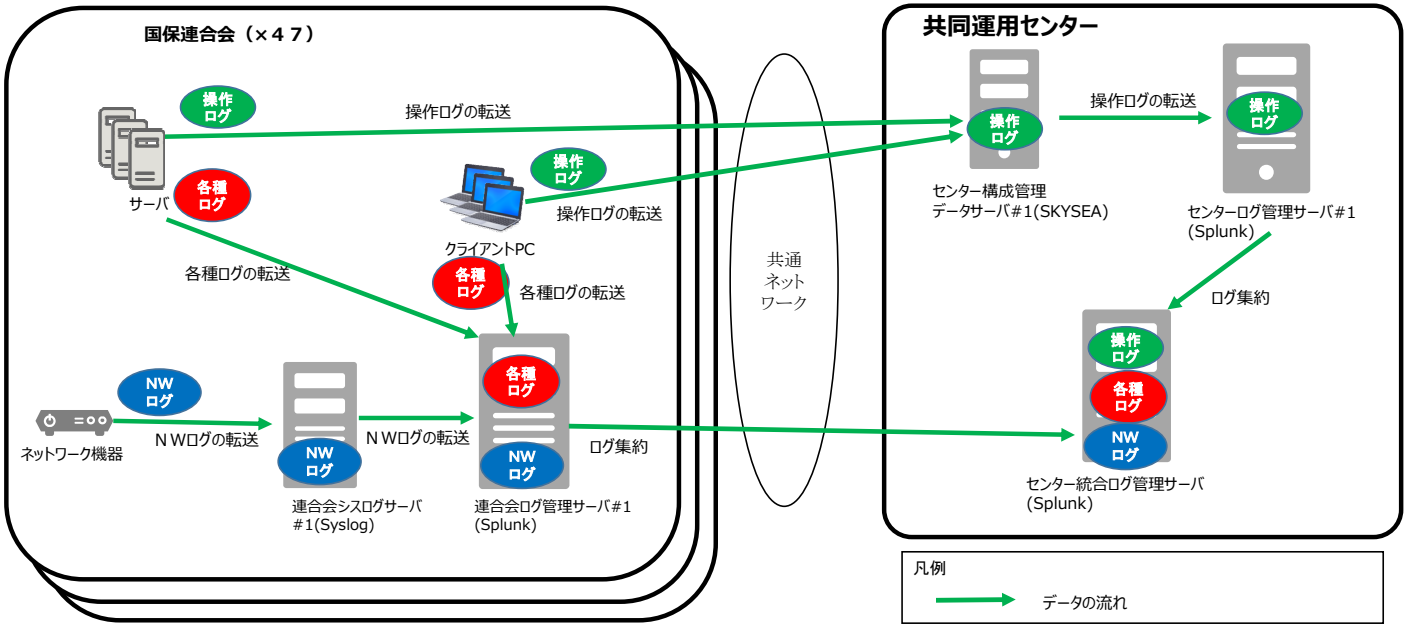


図 2-17 ログ収集機能イメージ

ウ. 提供機能

ログ収集で提供する機能を以下に示す。

表 2-50 ログ収集機能一覧

No.	機能	説明
1	ログ収集	個人番号に対するセキュリティ分析、運用保守の監査、内部不正操作等の監査を行う目的で、操作ログ、OSログ、データベースの監査ログ、ミドルウェアログ、ネットワークログを収集する。 OS ログには、セキュリティ分析の強化に伴い、「プロセス追跡の監査ログ」「システムモニタログ」を追加で収集する。

エ. 運用項目

ログ収集機能は共通ネットワークシステム運用での運用となるため、国保連合会の運用項目はない。

オ. 留意事項

・　ログの保管期限は現行システムから以下のように変更となる。

表 2-51 ログの保管期限

No.	現行システム	次期システム
1	個人番号に関するログ：7 年保管	変更なし
2	個人情報に関するログ：1年保管	3 年保管に拡大

・　ログ収集機能は、独自処理システムに対する機能提供をしない。

・　ログ収集機能は、都道府県・保険者(伝送クライアント)に対する機能提供をしない。

(b) ログ分析

ア. 概要

現行システムと同様に「個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」に従い、個人番号が適切に取り扱われていることを国保連合会の監査報告として都道府県・保険者（市町村）に説明するために、監査報告レポートを作成する。

個人番号にかかわるアクセスはすべてログとして記録されるが、監査報告レポートはアクセス記録すべてを出力するのではなく、通常業務と異なるアクセスと判断したものに限定して作成する。

イ．機能イメージ

ログ分析の機能イメージとして特定個人情報の監査報告レポートの運用フローを以下に示す。

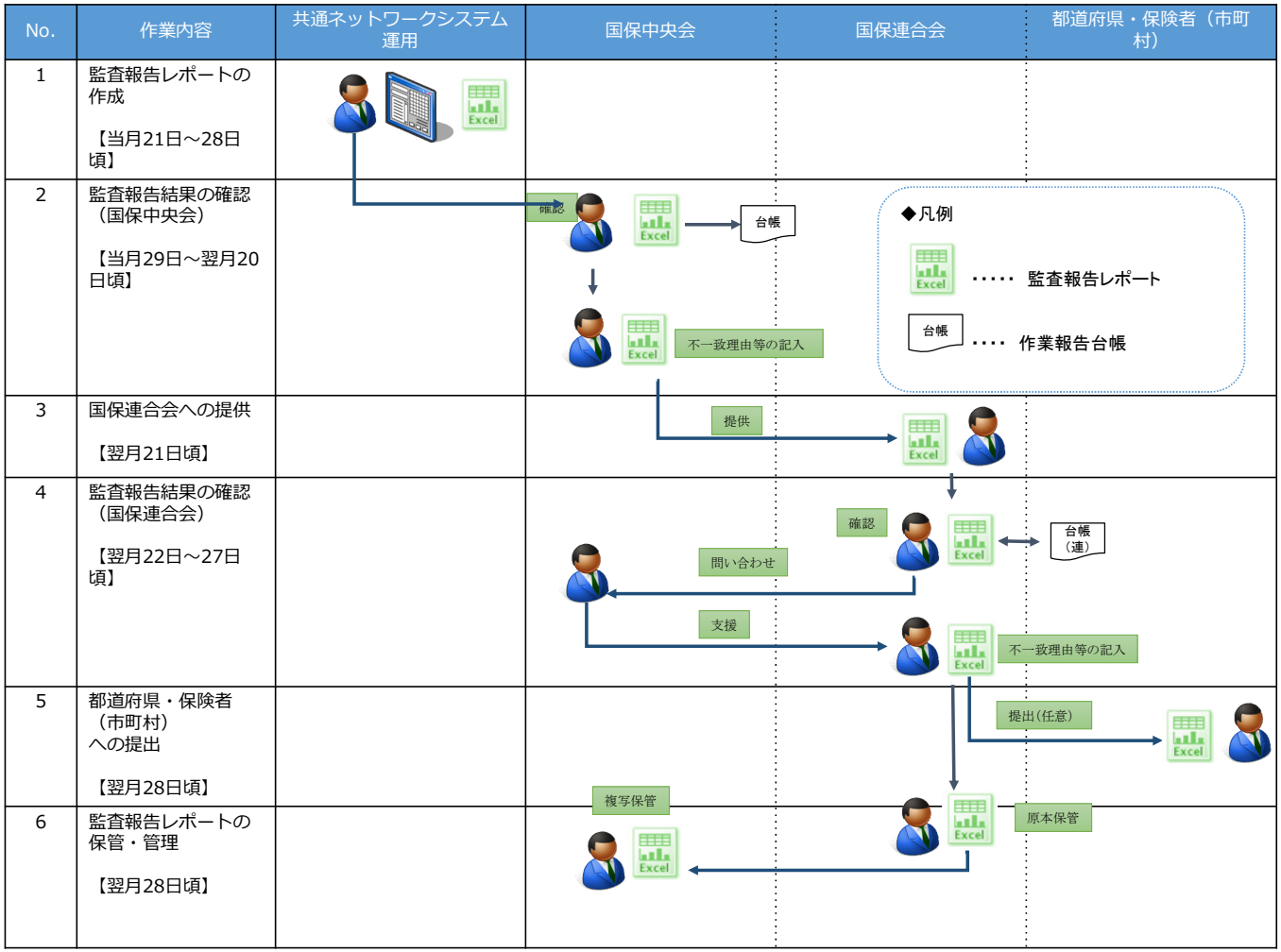


図 2-18 ログ分析機能（特定個人情報の監査報告レポート）の運用イメージ

ウ. 提供機能

ログ分析で提供する機能を以下に示す。

表 2-52 ログ分析機能一覧

No.	機能	説明
1	特定個人情報の監査報告レポート作成	DB アクセスレポート 個人番号データベースへ、アプリケーション以外からアクセスをした記録。 国保中央会の計画作業と合致する場合、作業申請時の管理番号を付与する。
2		ファイル持出しレポート 個人番号を含むファイルを、アプリケーション以外から持出した記録。 国保中央会の計画作業と合致する場合、作業申請時の管理番号を付与する。

エ．運用項目

ログ分析の特定個人情報の監査報告レポートの運用項目一覧を以下に示す。

表 2-53 ログ分析機能(特定個人情報の監査報告レポート) 運用項目一覧

No.	運用項目	頻度	説明	運用者
1	監査報告レポートの作成	月次 (当月 21 日～28 日)	共通ネットワークシステム運用は、監査報告レポートを作成する。	共通ネットワークシステム運用
2	監査報告結果の確認 (国保中央会)	月次 (当月 29 日～翌月 20 日)	国保中央会は、監査報告レポートを確認する。 国保中央会の実施作業について、国保中央会の作業報告台帳と突合せ、差異がないことを確認する。 突合せの結果、監査報告レポートと、作業報告台帳に不一致があった場合、不一致理由を記入する。	国保中央会
3	国保連合会への提供	月次 (翌月 21 日)	国保中央会で確認済みの監査報告レポートを国保連合会へ提出する。	国保中央会
4	監査報告結果の確認 (国保連合会)	月次 (翌月 22 日～27 日)	国保連合会は、監査報告レポートを確認する。 監査報告レポートに不明点等がある場合、必要に応じて、業務支援システムで問合わせる。	国保連合会
5	都道府県・保険者(市町村)への提出	月次 (翌月 28 日)	国保連合会は、監査報告レポートの確認結果を都道府県・保険者(市町村)へ提示する。なお、提示の有無や頻度、方法等は国保連合会の任意とする。	国保連合会
6	監査報告レポートの保管・管理	月次 (翌月 28 日)	国保連合会が確認済みの監査報告レポートを、国保中央会に送付する。 国保連合会が確認済みの監査報告レポートの原本は、国保連合会が保管・管理する。	国保連合会
7			国保中央会は、国保連合会から受領した監査報告レポートを複写として保管・管理する。	国保中央会

オ．留意事項

- ログ分析機能は、都道府県・保険者(伝送クライアント)に対する機能提供をしない。
- ログ分析機能は、独自処理システムに対する機能提供をしない。

(3)　その他サービス

①　Syslog

(a) 概要

共通ネットワークシステムで導入するネットワーク機器から Syslog を収集する。

表 2-54 Syslog コンポーネント一覧

No.	コンポーネント	説明
1	連合会シスログサーバ#1	Syslog を収集する。マスターサーバ。
2	センターシスログバックアップサーバ#1	Syslog の欠損を補うため、バックアップ用として Syslog を収集する。
3	収集対象機（ネットワーク機器）	マスターサーバ及びバックアップサーバに Syslog を転送する。

(b) 機能イメージ

Syslog の機能イメージを以下に示す。

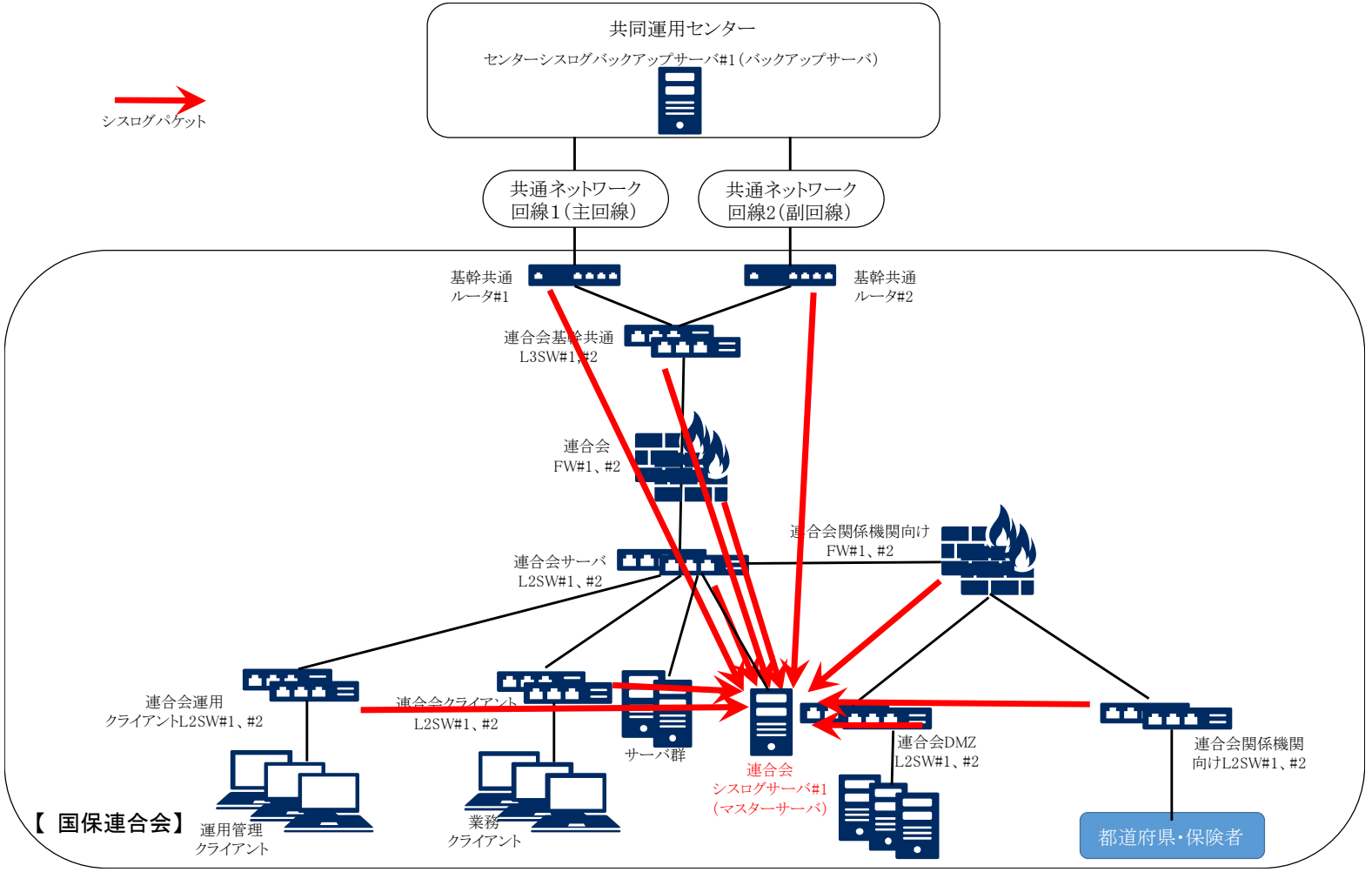


図 2-19 Syslog 機能イメージ（マスターサーバ向け）

機２：関係者限り

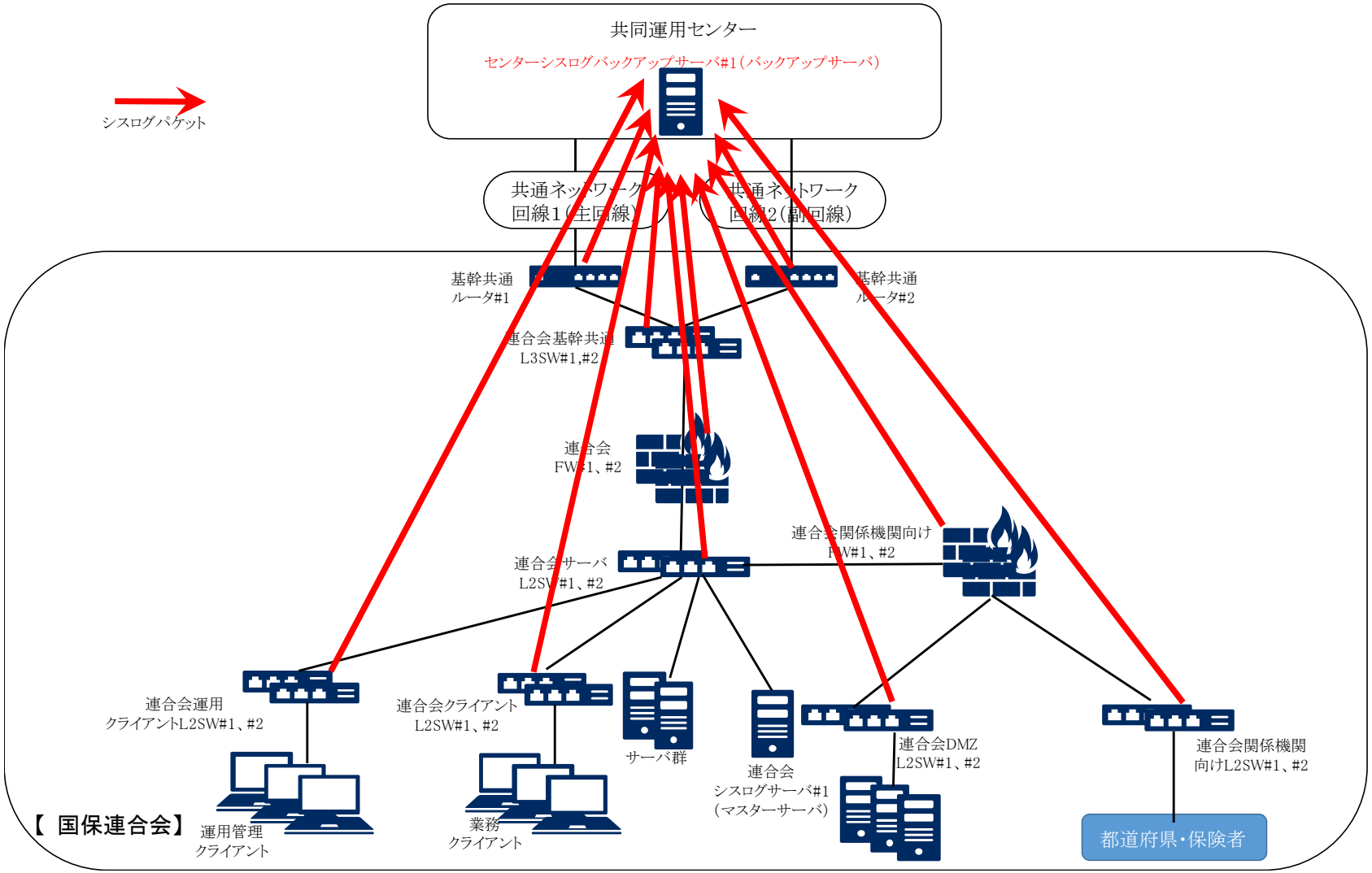


図 2-20 Syslog 機能イメージ（バックアップサーバ向け）

(c) 提供機能

Syslog 機能で提供する機能を以下に示す。

表 2-55 Syslog 機能一覧

No.	機能	説明
1	Syslog 収集機能	ネットワーク機器が送信する Syslog を受信し保存する。

(d) 運用項目

国保連合会で Syslog 機能の運用項目はない。

(a) 留意事項

・ Syslog 機能は独自処理システムに対する機能提供をしない。

② リモート接続

(a) 概要

リモート接続機能は SKY 社の SKYSEA Client View により実現する。

リモート接続は専用の管理コンソールから管理対象の Windows 機器に対するリモート接続機能を提供する。

なお、構成管理機能、デバイス制御機能、リモート接続機能及び操作ログ収集機能は1つのミドルウェアで統合管理する。

国保連合会に導入するコンポーネントを以下に示す。

表 2-56 SKYSEA コンポーネント一覧

No.	コンポーネント	説明
1	管理コンソール(管理機)	国保連合会設置の運用管理クライアントに導入する。 管理コンソールから国保連合会内のサーバにリモート接続を可能とする。
2	エージェント(端末機)	国保連合会設置のサーバ及びクライアントに導入する。 管理コンソールからリモート接続を受付ける。

(b) 機能イメージ

リモート接続の機能イメージを以下に示す。

【リモート接続のシーケンス】
①接続元（管理コンソールまたはマスターサーバ）はマスターサーバへ接続先のエージェント情報を要求する。
②マスターサーバは接続元にエージェント情報を返す。
③接続元から接続先のエージェントに対してリモート接続を要求する。
④エージェントは接続元からのリモート接続を受け付け、自身のデスクトップを画面転送する。

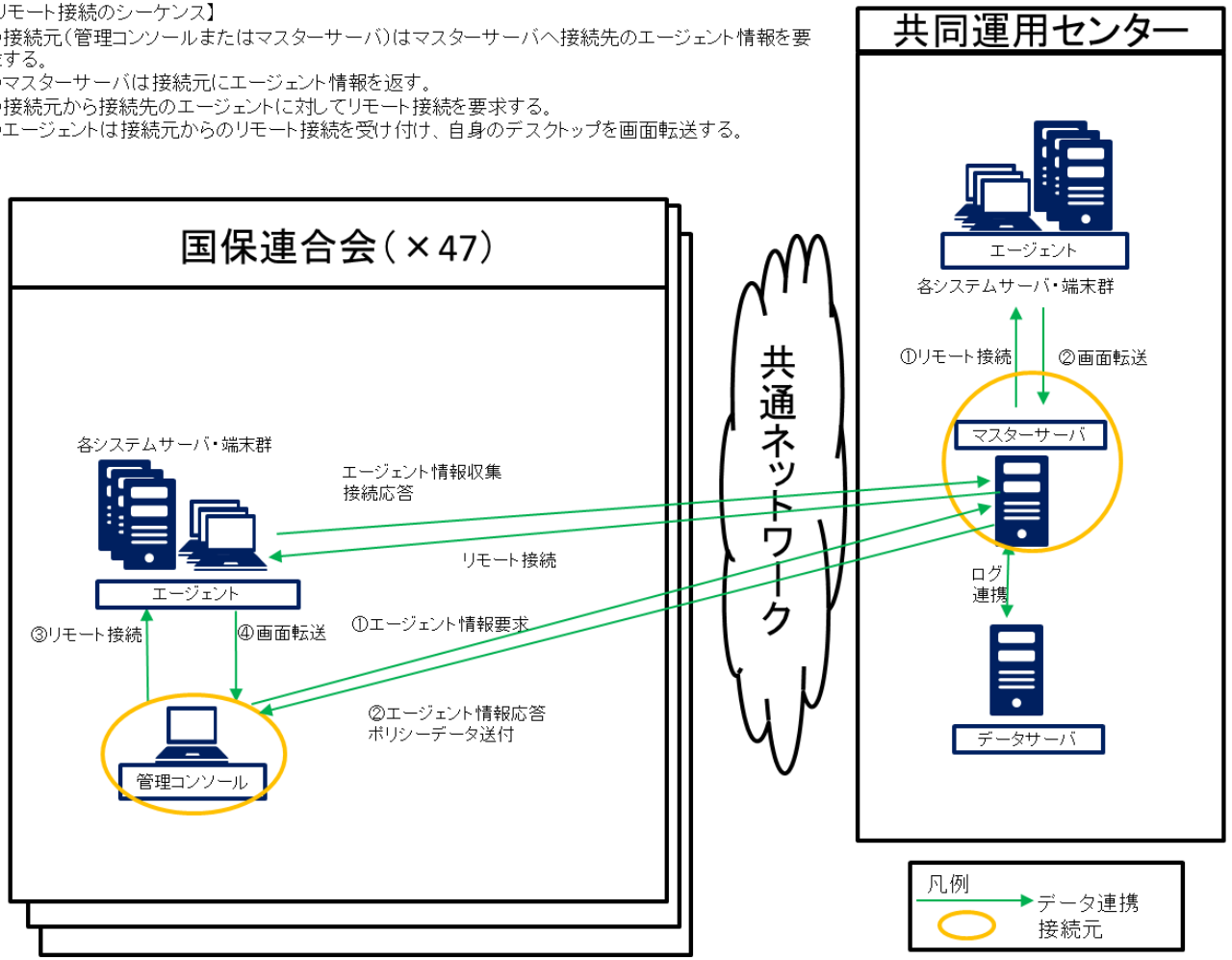


図 2-21 リモート接続機能イメージ

(c) 提供機能

国保連合会に提供するリモート接続機能を以下に示す。

表 2-57 リモート接続機能一覧

No.	機能	説明
1	管理コンソール	管理コンソールからマスターサーバに登録された各システムサーバの情報を参照する。 マスターサーバから各システムサーバ・端末群へリモート接続する機能を提供する。
2	リモート接続	各システムサーバはマスターサーバからの接続要求を受け、リモート接続を実施する。

(d) 運用項目

リモート接続機能の運用項目はない。

(e) 留意事項

- リモート接続機能が利用可能なオペレーティングシステムのバージョン：
  Microsoft Windows 10 Enterprise 2016 LTSB (64BitOS)
  Microsoft Windows Server 2016
- 現行システムとリモート接続機能を提供するソフトウェアが異なるため、操作手順が変更となる。
- リモート接続は運用管理クライアントからのみ可能とする。
- リモート接続機能は都道府県・保険者(伝送クライアント)に対する機能提供をしない。
- リモート接続機能は独自処理システムに対する機能提供をしない。
- 独自処理システムに対するリモート接続は不可とする。
- 共同運用センター設置のマスターサーバと通信ができない場合、各システムサーバに対してリモート接続が不可となる。ただし、既にリモート接続済みの状態でマスターサーバと通信ができない状況が発生した場合についてリモート接続機能は継続して利用可能となる。
- Windows 標準のリモートデスクトップの利用は原則禁止とするため、各サーバのサービス(Remote Desktop Services)を停止する。
- 管理コンソールの起動パスワードは拠点の担当者が決定し、国保連合会で管理する。

・　仮想化基盤機能を用いたリモート接続は以下の場合のみ利用可能とする。

1. マスターサーバ障害発生時
2. リモート接続機能の障害発生時
3. 業務、運用上必要な場合

・　運用管理クライアントは用途によって、以下の 3 種類の区別がある。

・運用管理クライアント(共用)

・運用管理クライアント(介護)　※VT系を含む

・運用管理クライアント(障総)

なお、運用管理クライアント(共用)の有無で各運用管理クライアントの操作範囲が異なるため、以降に記載する。

運用管理クライアント(共用)が有る場合

運用管理クライアント(介護)、運用管理クライアント(障総)に導入する管理コンソールの操作範囲は以下とする。

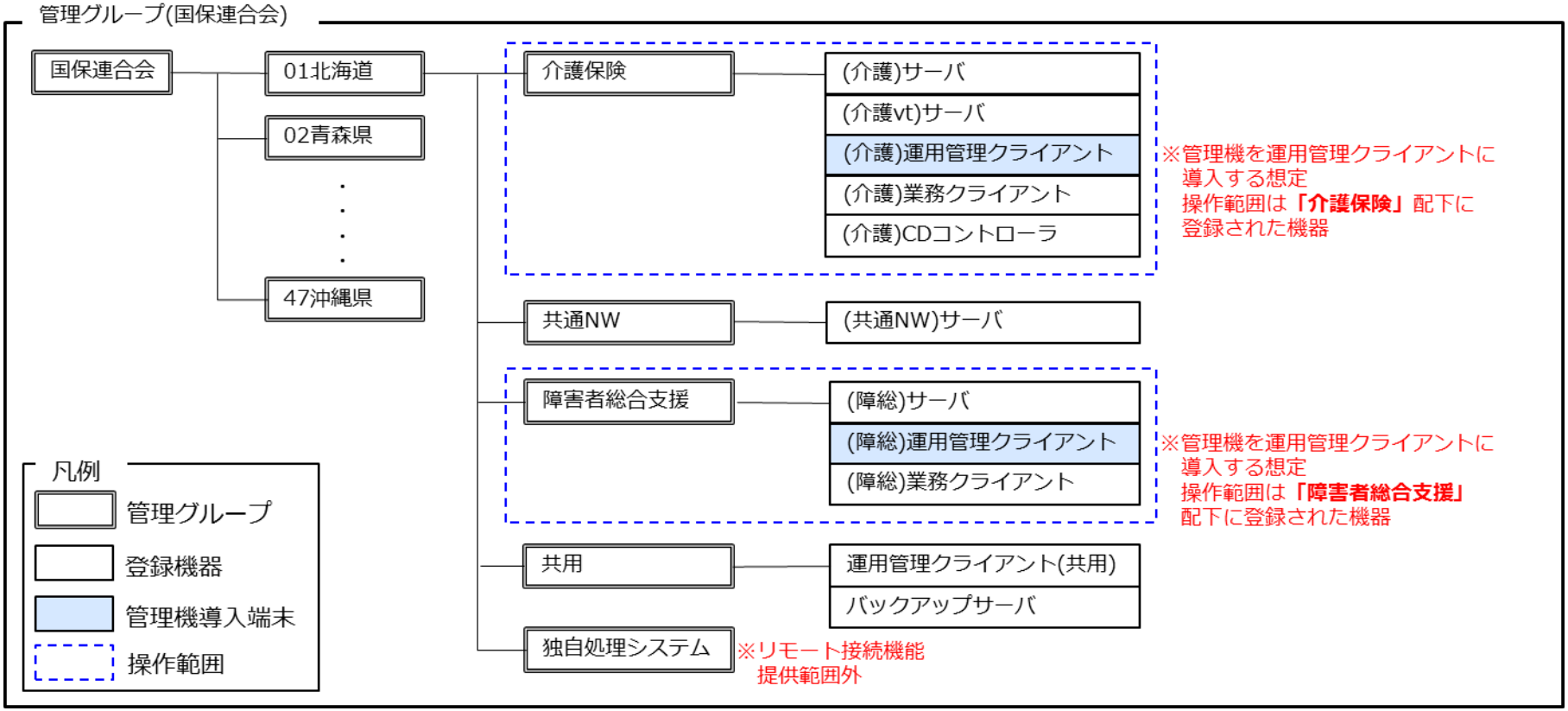


図 2-22 介護保険システム・障害者総合支援システムに関する運用管理クライアントのアクセス範囲

運用管理クライアント(共用)に導入する管理コンソールの操作範囲は以下とする。
運用管理クライアント(共用)に管理コンソールを導入した際、デフォルトの操作範囲は管理グループ「共用」のみとなるため
共通ネットワークシステム運用が管理グループ「介護保険」「共通 NW」「障害者総合支援」「独自処理システム」の操作範囲を追加する。
なお、管理グループ「独自処理システム」に対するリモート接続機能は提供範囲外となるが、構成管理機能およびデバイス制御機能のために
操作範囲を追加する。(独自処理システムに対するリモート接続は不可)

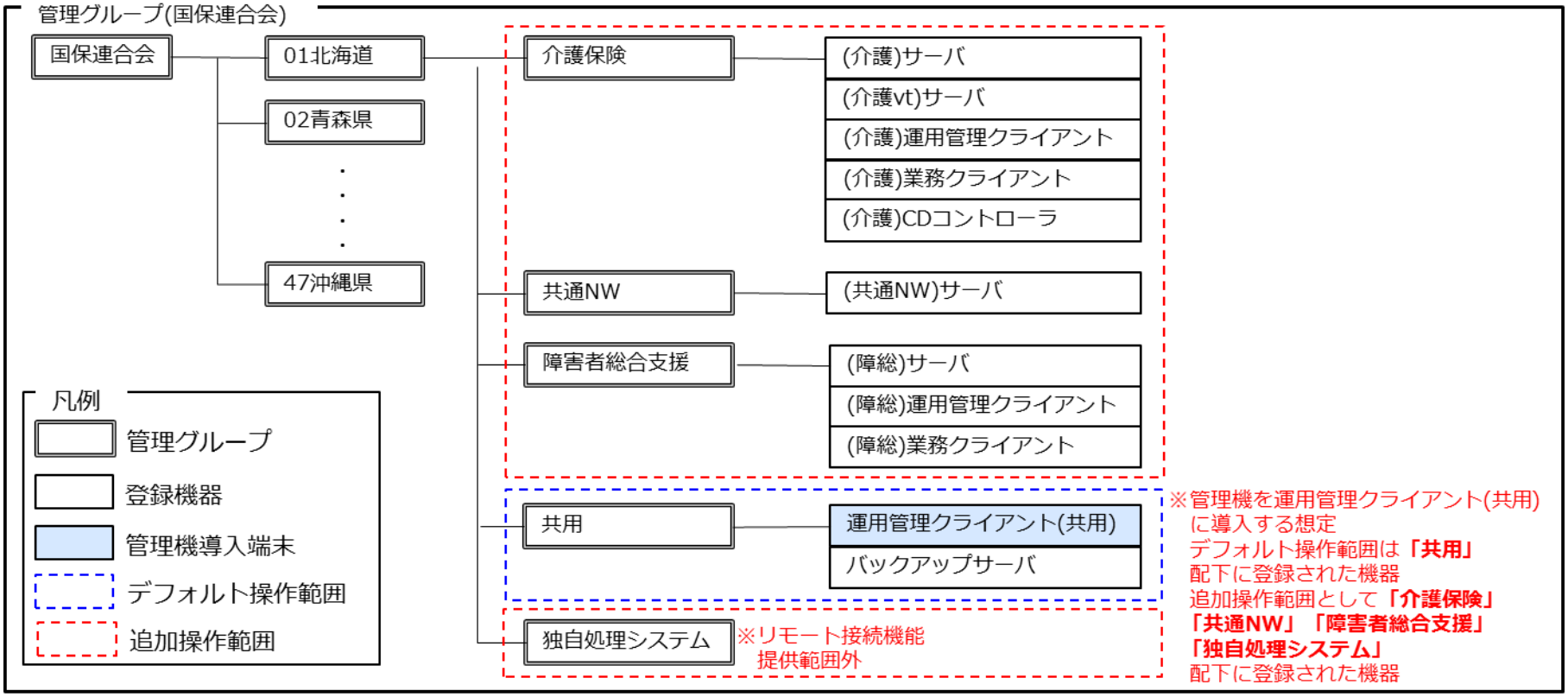


図 2-23 共用の運用管理クライアントのアクセス範囲

運用管理クライアント(共用)が無い場合

運用管理クライアント(介護) に導入する管理コンソールの操作範囲は以下とする。

運用管理クライアント(介護)に管理コンソールを導入した際、デフォルトの操作範囲は管理グループ「介護保険」のみとなるため、

共通ネットワークシステム運用が管理グループ「共通 NW」「共用」「独自処理システム」の操作範囲を追加する。

なお、管理グループ「独自処理システム」に対するリモート接続機能は提供範囲外となるが、構成管理機能およびデバイス制御機能のために操作範囲を追加する。(独自処理システムに対するリモート接続は不可)

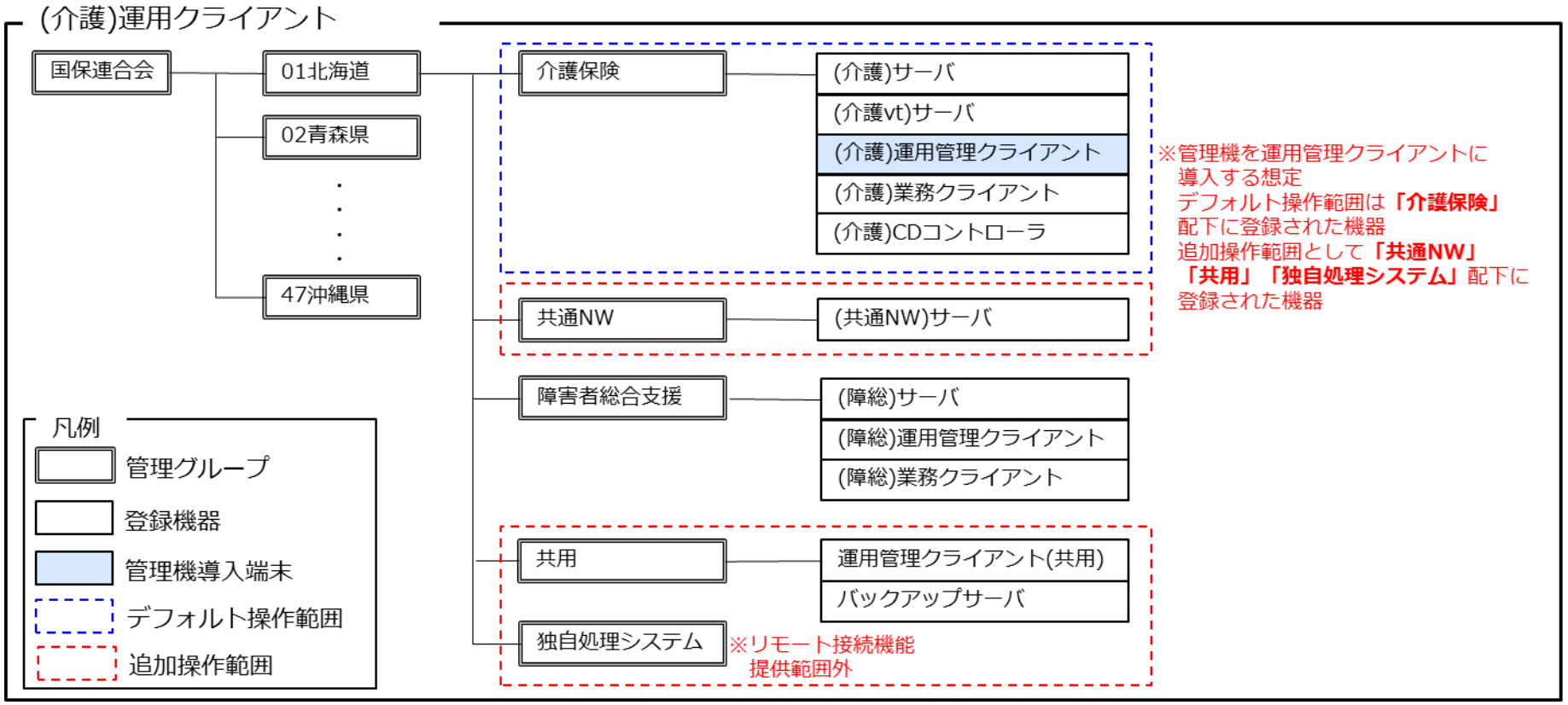


図 2-24 介護保険システムに関する運用管理クライアントのアクセス範囲

運用管理クライアント(障総)に導入する管理コンソールの操作範囲は以下とする。
運用管理クライアント(障総)に管理コンソールを導入した際、デフォルトの操作範囲は管理グループ「障害者総合支援」のみとなるため、共通ネットワークシステム運用が管理グループ「共通 NW」「共用」「独自処理システム」の操作範囲を追加する。
なお、管理グループ「独自処理システム」に対するリモート接続機能は提供範囲外となるが、構成管理機能およびデバイス制御機能のために操作範囲を追加する。(独自処理システムに対するリモート接続は不可)

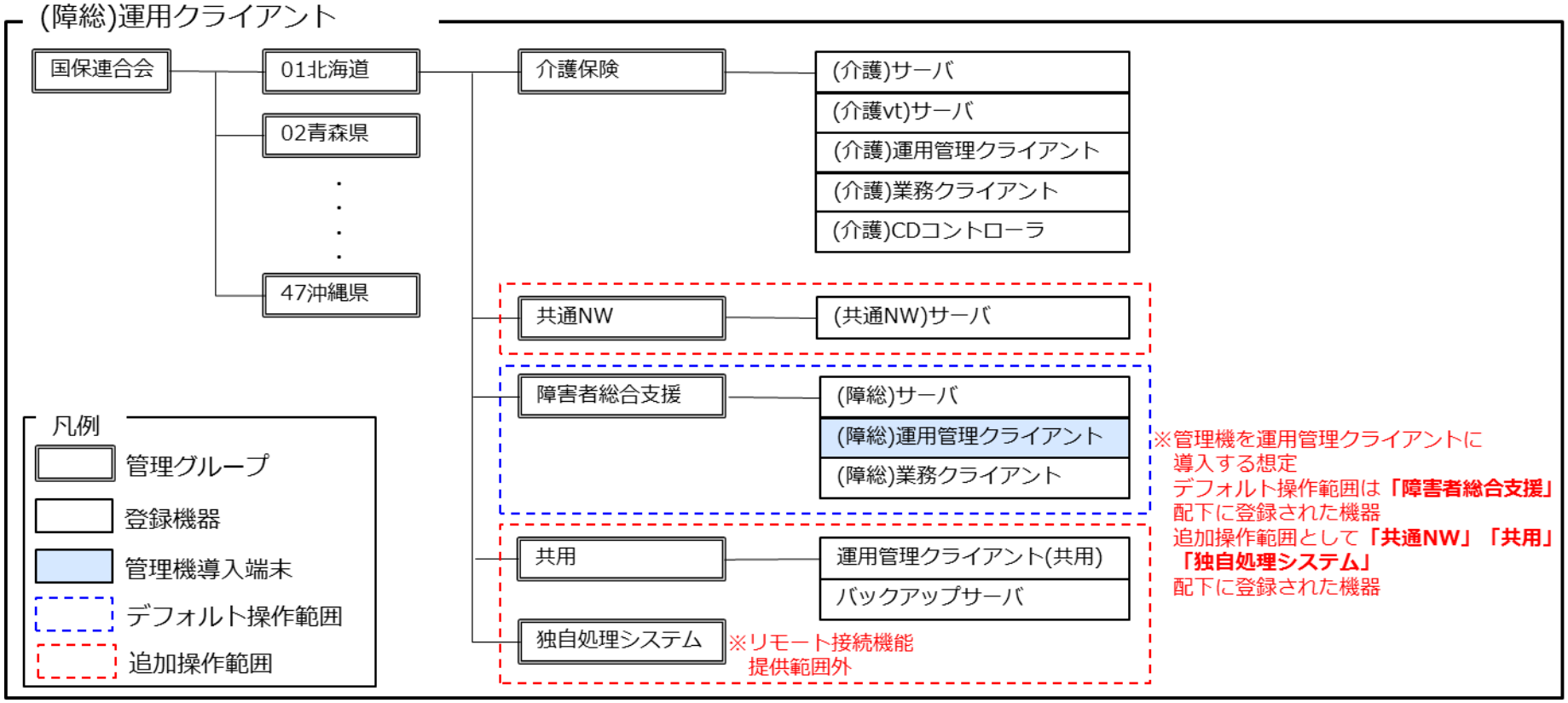


図 2-25 介護保険システム・障害者総合支援システムに関する運用管理クライアントのアクセス範囲

③ メール

(a) 概要

現行システムでは、全国の国保連合会に設置したメールサーバ（連合会連携サーバ）にメールを保持し、国保連合会のメールアカウントを保持しているユーザが全国の国保連合会、国保中央会及び各システム運用等とメールの送受信を行っているが、次期システムではメール機能を提供しない。

メール（事務連絡、モジュールリリース、簡易連絡等）は、国保連合会の情報系端末のメール機能（Outlook 等）による送受信とする。

(b) 留意事項

- 現行システムで保存しているメールデータの移行は行わない。
- メール機能は都道府県・保険者（伝送クライアント）に対する機能提供をしない。
- メール機能は独自処理システムに対する機能提供をしない。

④ バックアップリストア

(a) 概要

バックアップ・リストア機能は、バックアップアプライアンス(Arcserve UDP Appliance)を用いて実現する。

バックアップ・リストアは、共通ネットワークシステム、介護保険システム、障害者総合支援システムの各サーバを対象とする。

表 2-58 バックアップリストア機能　運用項目一覧

No.	コンポーネント	説明
1	バックアップアプライアンス#1	サーバのバックアップ・リストア機能を提供する。 共通ネットワークシステム及び障害者総合支援システムのサーバを対象とする。
2	バックアップアプライアンス#2	サーバのバックアップ・リストア機能を提供する。 介護保険システムのサーバを対象とする。

(b) 機能イメージ

バックアップ・リストアの機能イメージを以下に示す。

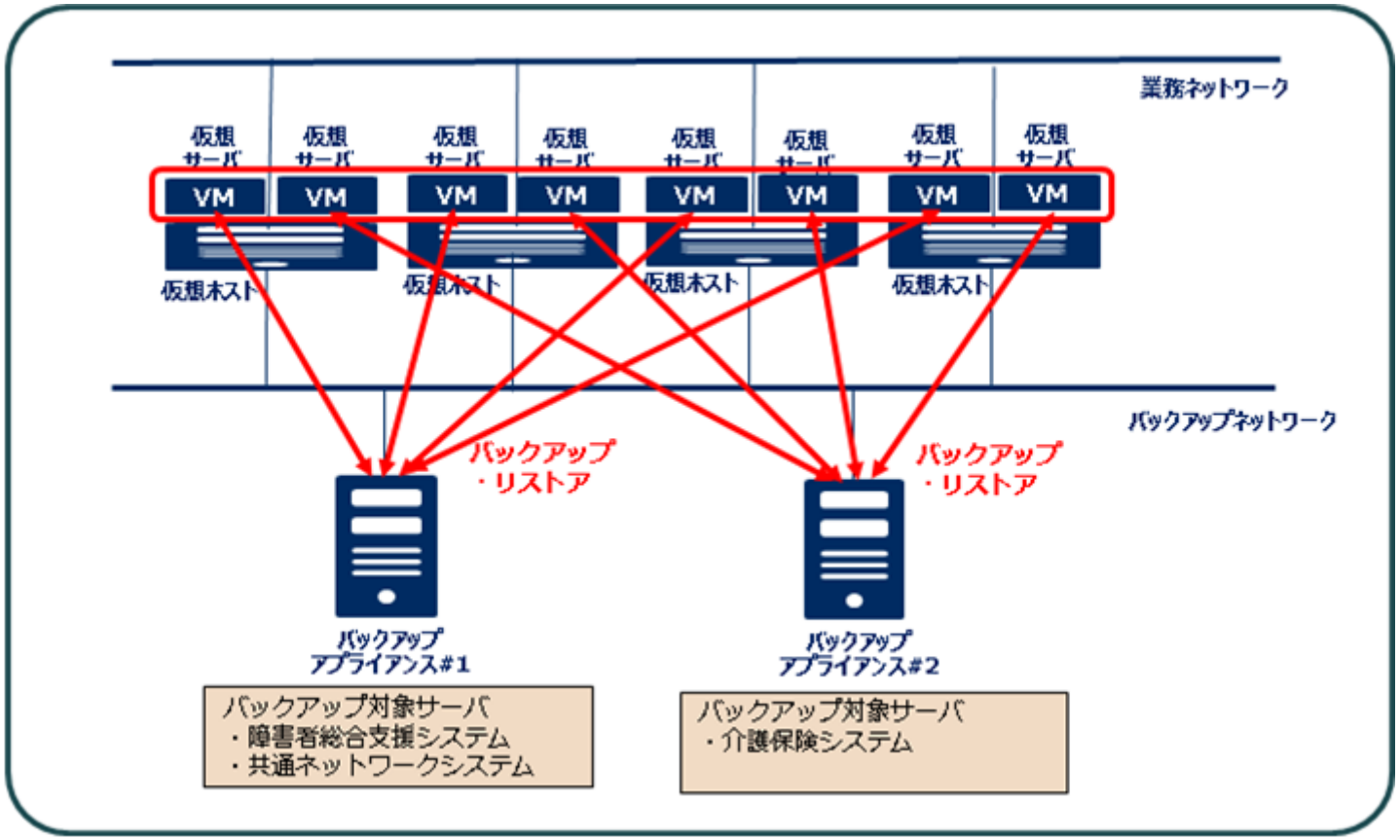


図 2-26 バックアップ・リストアの機能イメージ

(c) 提供機能

バックアップ・リストアで提供する機能を以下に示す。

表 2-59 バックアップ・リストア機能一覧

No.	機能	説明
1	バックアップ機能 (バックアップアプライアンス#1)	バックアップ製品(Arcserve UDP)を用いて、仮想サーバのバックアップ機能を提供する。 仮想サーバ機能(VMware)と連携して、サーバのシステムバックアップ機能(VADP)を実装する。 バックアップ製品のエージェントを用いて、サーバのドライブ単位バックアップ機能を実装する。
2	バックアップ機能 (バックアップアプライアンス#2)	バックアップ製品(Arcserve Backup)を用いて、仮想サーバのバックアップ機能を提供する。 仮想サーバ機能(VMware)と連携して、サーバのシステムバックアップ機能(VADP)を実装する。 バックアップ製品のエージェントを用いて、サーバのドライブ単位バックアップ機能を実装する。
3	リストア機能	サーバに障害が発生した場合、復旧する手段としてサーバ全体及びファイル単位のリストア機能を提供する。

(d) 運用項目

バックアップ機能に関しては機能提供のみとなり、国保連合会でバックアップ機能に関する運用項目はない。

(e) 留意事項

- バックアップ・リストア機能は都道府県・保険者(伝送クライアント)に対する機能提供をしない。
- バックアップ・リストア機能は独自処理システムに対する機能提供をしない。

⑤ 仮想サーバ

(a) 概要

仮想サーバ機能は、VMware 及びハイパーコンバージド・インフラストラクチャ（HCI）を用いて実現する。

ハイパーコンバージド・インフラストラクチャ（HCI）の特徴として、ノードの増設によりスケールアウトが容易に行うことができる。

表 2-60 仮想サーバ機能 コンポーネント一覧

No.	コンポーネント	説明
1	連合会仮想化基盤#1～#4	介護保険システム、障害者総合支援システム、共通ネットワークシステムの各仮想サーバが動作する環境を提供する。
2	連合会仮想基盤管理サーバ#1	連合会仮想化基盤の管理機能及び連合会仮想化基盤上で動作する仮想サーバをWeb 画面で操作する機能を提供する。

(b) 機能イメージ

仮想サーバの機能イメージ（従来の仮想化基盤とHCIの相違）を以下に示す。

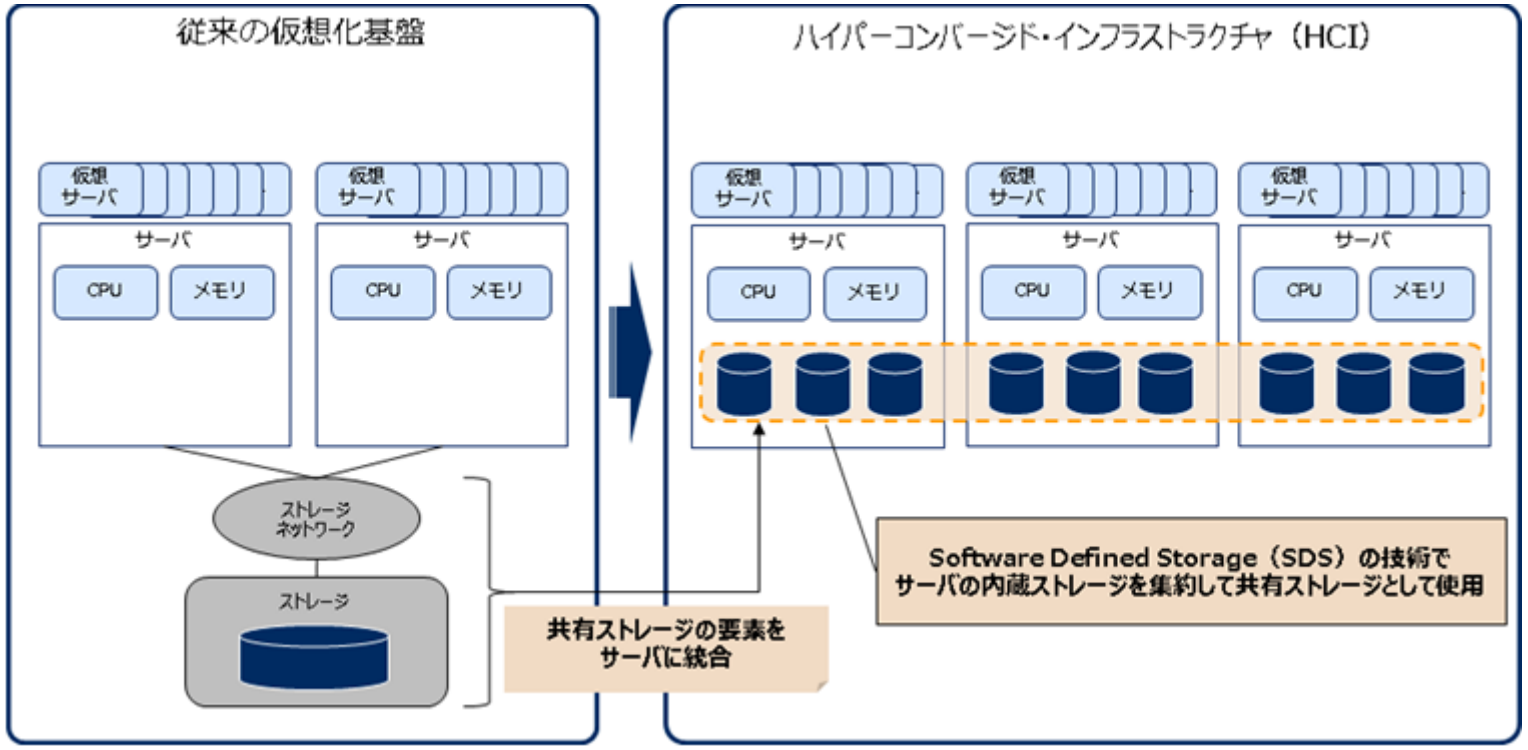


図 2-27 仮想サーバの機能イメージ

(c) 提供機能

仮想サーバで提供する機能を以下に示す。

表 2-61 仮想サーバ機能 コンポーネント一覧

No.	機能	説明
1	仮想サーバ機能 (VMware ESXi)	サーバを仮想化し、1台の物理サーバ上で複数の仮想サーバを稼働させる機能を提供する。
2	仮想サーバ管理機能 (VMware vCenter Server)	クライアントから Web ブラウザで管理コンソールに接続し、仮想サーバのデスクトップを操作する機能を提供する。
3	仮想ストレージ機能 (VMware vSAN)	連合会仮想化基盤#1～#4 のハードディスクを集約し、1 つの大きな仮想ストレージ領域として認識させる機能を提供する。

(d) 運用項目

仮想サーバ機能の運用項目を以下に示す。

表 2-62 仮想サーバ機能 運用項目一覧

No.	運用項目	頻度	説明	運用者
1	仮想サーバ及び仮想化基盤の停止・起動作業	計画停止	計画停止が行われる際、事前に仮想サーバ及び仮想化基盤の停止を行う。 また、計画停止終了後に、仮想サーバ及び仮想化基盤の起動ならびに正常性確認を行う。	国保連合会

(e) 留意事項

- 仮想サーバ機能は都道府県・保険者（伝送クライアント）に対する機能提供をしない。
- 仮想サーバ機能は独自処理システムに対する機能提供をしない。

2.2. システム導入

本節では、国保連合会設置機器の共通ネットワークシステム範囲の作業概要について説明する。

2.2.1. 作業内容

(1) 作業概要

次期システム機器（サーバ、クライアント PC 等）の搬入・設置にあたり、国保連合会は機器設置場所の確保及び設置場所に関する情報を提供する。
また、必要に応じて電源、空調設備、LAN 配線等の工事を実施し、機器の搬入・設置に備える。
機器の搬入・設置が完了した後、国保連合会は国保中央会から提供される導入手順書に従い、機器の構築、設定及び動作確認を行う。
また、次期システム機器の環境構築に伴い、都道府県・保険者ファイアウォール（都道府県・保険者設置の機器）の設定変更等（※1）を行う。

※1 国保連合会設置の関係機関向けファイアウォールや都道府県・保険者受付サーバ等は現行システムの IP アドレス体系を引き継ぐ予定だが、都道府県・保険者向けの新システム（障害者総合支援システム台帳参照 Web サーバ）が追加となるため、都道府県・保険者ファイアウォールの設定変更が必要となる。
また、都道府県・保険者ファイアウォールのバージョンにより、ファームウェアのアップグレード作業が必要となる可能性がある。（作業有無については現在評価中となる）

機２：関係者限り

システム導入の作業内容を以下に示す。

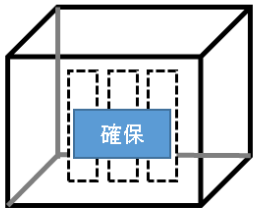
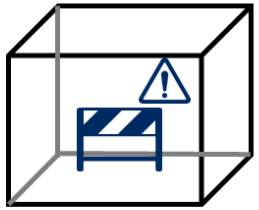
場所	国保連合会		連合会HW受託業者 構築場所	国保連合会		
区分	システム導入事前作業					システム導入 その他
作業	環境調査 /設置・作業場所準備	導入手順書確認	ハードウェア初期設定	工事	ハードウェアの搬入・設置	
作業イメージ	設置・作業場所準備 	導入手順書確認 	HW初期設定 /OS、一部ミドルウェア導入 	電源、回線等の工事 	ハードウェア等の搬入・設置 	システム導入、報告等 
作業内容	・環境調査票の修正、提出 ・機器設置場所の確保 ・導入作業場所の確保	・導入手順書の事前確認/問合せ	・導入機器の初期設定、OSや一部ミドルウェアの導入	・電源、空調設備、フロア間LAN配線、共通NW回線等の工事	・ハードウェアの搬入・設置 ・搬入、設置立会い	・機器の構築、設定、動作確認 ・機器のバックアップ ・次期システムと分散配置回線の接続作業 ・問合せ対応 ・作業報告
作業担当者	国保連合会	国保連合会	連合会HW受託業者	国保連合会 回線業者	連合会HW受託業者 国保連合会	国保連合会 システム開発業者 国保中央会(事務局) 連合会ヘルプデスク

図 2-28 共通ネットワークシステム作業概要

(2)　システム導入対象

①　システム構成

国保連合会のシステム構成を以下に示す。なお、「表 2-63 **導入機器・仮想サーバー覧**」の「機器・仮想サーバ名称」に記載した名称の接頭辞としてある「連合会」はシステム構成図上、割愛する。

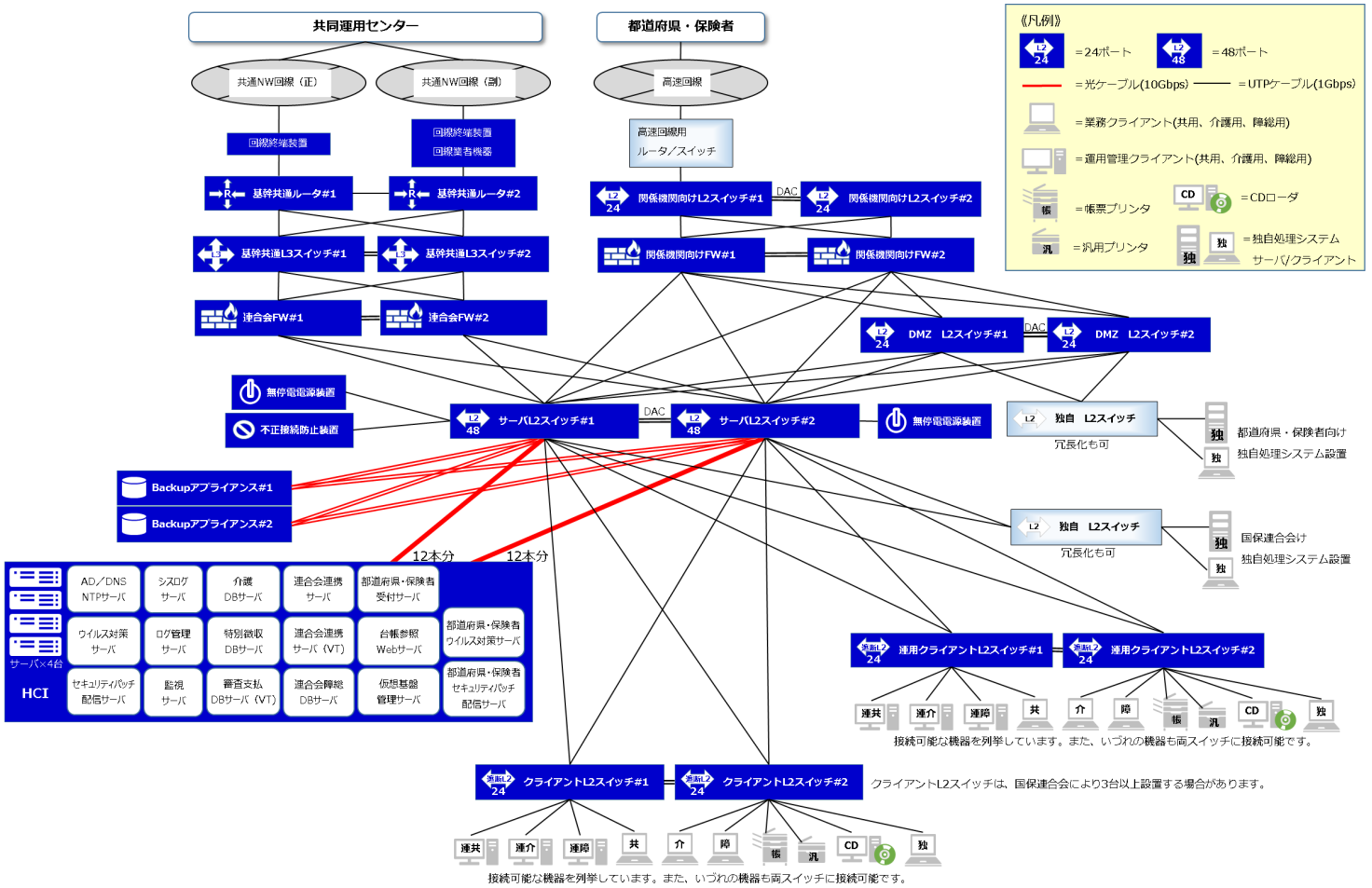


図 2-29 国保連合会システム構成(標準構成)

機２：関係者限り

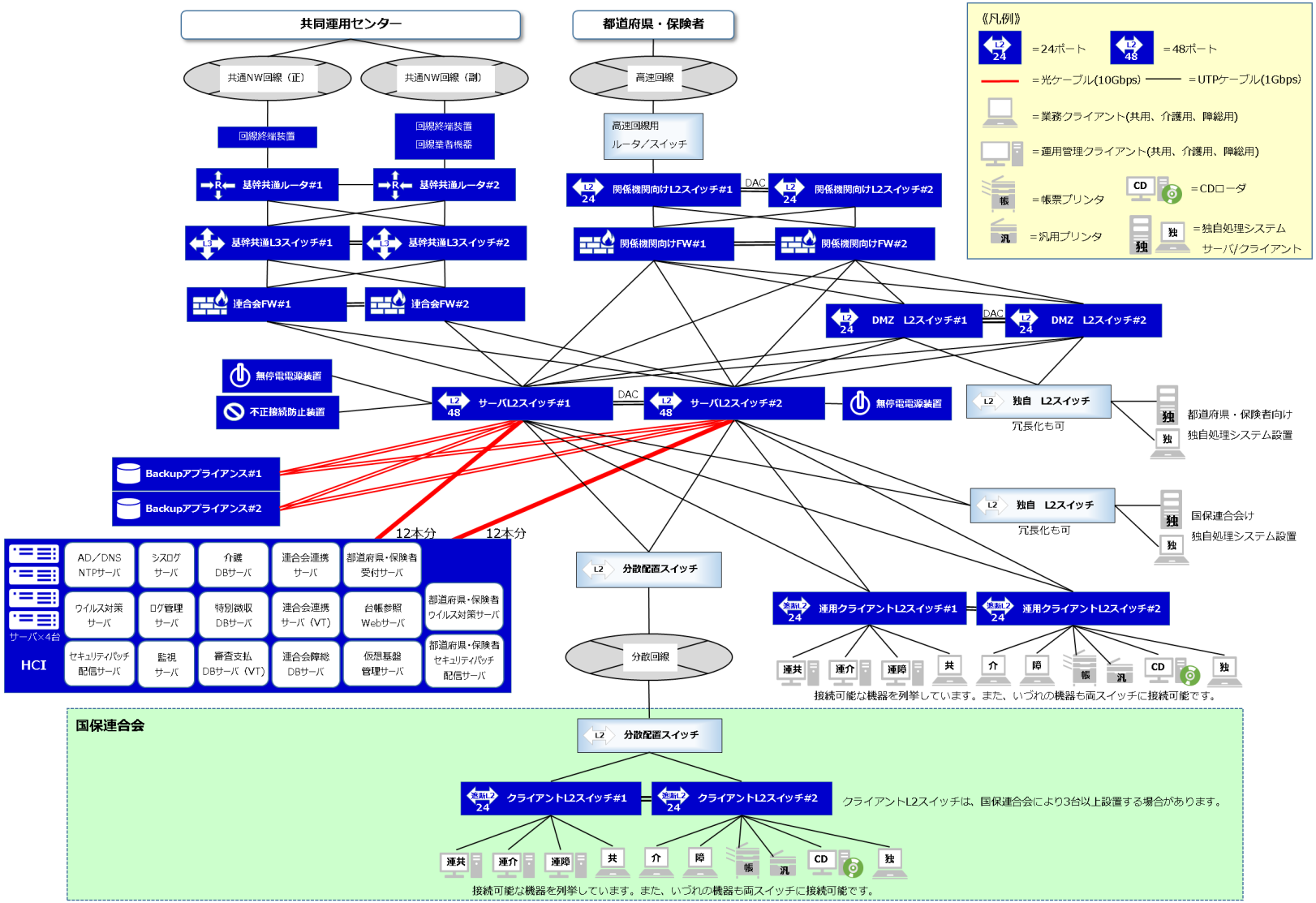


図 2-30 国保連合会システム構成(分散配置構成例)

② 導入機器・仮想サーバ

国保連合会設置の共通ネットワークシステムを提供するために必要な機器、仮想サーバを以下に示す。

表 2-63 導入機器・仮想サーバ一覧

No.	機器・仮想サーバ名称	数量	提供機能	種別	機器調達担当	構築担当
1	連合会基幹共通 ルータ#1～#2	2	ルータ制御	NW 機器	SDN 機器受託業者	連合会 HW 受託業者
2	連合会 FW#1～#2	2	UTM/ ファイアウォール	NW 機器	連合会 HW 受託業者	連合会 HW 受託業者
3	連合会基幹共通 FW	1	UTM/ ファイアウォール	NW 機器(仮想)	―	連合会 HW 受託業者
4	連合会独自向け FW	1	UTM/ ファイアウォール	NW 機器(仮想)	―	連合会 HW 受託業者 国保連合会(※2)
5	連合会基幹共通 L3SW#1～#2	2	L3SW	NW 機器	SDN 機器受託業者	連合会 HW 受託業者
6	連合会サーバ L2SW#1～#2	2	L2SW	NW 機器	連合会 HW 受託業者	連合会 HW 受託業者
7	連合会クライアント L2SW#1～#4	4(※1)	L2SW	NW 機器	SDN 機器受託業者	連合会 HW 受託業者
8	連合会運用クライアント L2SW#1～#2	2	L2SW	NW 機器	SDN 機器受託業者	連合会 HW 受託業者
9	連合会関係機関向け FW#1～#2	2	UTM/ ファイアウォール	NW 機器	連合会 HW 受託業者	連合会 HW 受託業者 国保連合会(※2)
10	連合会 DMZL2SW#1～#2	2	L2SW	NW 機器	連合会 HW 受託業者	連合会 HW 受託業者
11	連合会関係機関 L2SW#1～#2	2	L2SW	NW 機器	連合会 HW 受託業者	連合会 HW 受託業者
12	連合会不正接続 防止装置#1	1	不正接続防止	NW 機器	SDN 機器受託業者	連合会 HW 受託業者
13	連合会 AD サーバ#1	1	AD/DNS/NTP	仮想サーバ	―	連合会 HW 受託業者 国保連合会(※3)

表 2-63 導入機器・仮想サーバ一覧

No.	機器・仮想サーバ名称	数量	提供機能	種別	機器調達担当	構築担当
14	連合会セキュリティパッチ配信サーバ#1	1	Windows セキュリティパッチ配信/DNS	仮想サーバ	—	連合会 HW 受託業者 国保連合会(※3)
15	連合会ログ管理サーバ#1	1	ログ収集・分析	仮想サーバ	—	連合会 HW 受託業者 国保連合会 共通ネットワークシステム受託者(※3)(※4)
16	連合会ウイルス対策サーバ#1	1	ウイルス対策	仮想サーバ	—	連合会 HW 受託業者 国保連合会(※3)
17	連合会バックアップアプライアンス#1～2	2	バックアップ/リストア	アプライアンスサーバ	—	連合会 HW 受託業者 国保連合会(※3)
18	連合会監視サーバ#1	1	死活・エラー監視	仮想サーバ	—	連合会 HW 受託業者 国保連合会(※3)
19	連合会シスログサーバ#1	1	Syslog	仮想サーバ	—	連合会 HW 受託業者 国保連合会(※3)
20	連合会都道府県・保険者セキュリティパッチ配信サーバ#1	1	Windows セキュリティパッチ配信	仮想サーバ	—	連合会 HW 受託業者 国保連合会(※3)
21	連合会都道府県・保険者ウイルス対策サーバ#1	1	ウイルス対策	仮想サーバ	—	連合会 HW 受託業者 国保連合会(※3)
22	連合会仮想基盤管理サーバ#1	1	仮想サーバ	仮想サーバ	—	連合会 HW 受託業者
23	連合会仮想基盤	4	仮想サーバ	仮想化基盤	連合会 HW 受託業者	連合会 HW 受託業者

※1 国保連合会によって 2 台～4 台で台数が異なる。

※2 FW の構築は連合会 HW 受託業者が実施する。ただし、国保連合会は独自処理システムの FW ポリシーの設定を行う。

※3 OS の初期導入までは連合会 HW 受託業者が実施する。国保連合会は OS 設定以降の作業を行う。

※4 ログ収集・分析機能の主要機能構築は共通ネットワークシステム受託者が行う。

③ ソフトウェア構成

共通ネットワークシステムを提供するために必要なソフトウェア構成を以下に示す。

表 2-64 作業対象ソフトウェア一覧

No.	ミドルウェア名称	提供機能	サーバ導入有無	クライアント PC 導入有無
1	Microsoft Windows Server 2016 Standard Edition	Windows OS	有	無
2	WebSAM NetvisorPro V	死活・エラー監視	有	無
3	WebSAM SystemManager G	死活・エラー監視	有	無
4	JP1/Integrated Management	死活・エラー監視	有	有
5	JP1/Base	死活・エラー監視	有	無
6	Splunk	ログ収集・分析	有	有
7	SKYSEA Client View	構成管理/デバイス制御/リモート接続/操作ログ収集	有	有
8	InfoCage PC 検疫	PC 検疫	無	有
9	ウイルスバスター コーポレートエディション	ウイルス対策	有	有
10	Kiwi Syslog Server	Syslog	有	無
11	NeoFaceMonitor	アカウント管理	有	無
12	VMware vCenter Server (※1)	仮想サーバ	有	無
13	Arcserve UDP Backup	バックアップ/リストア	有	無

※1 連合会 HW 受託業者が導入を行うソフトウェア。

(3) 作業詳細・分担

システム導入等の作業内容及び役割分担を以下に示す。

表 2-65 構築作業役割分担

No.	作業区分	作業名	役割分担	備考
1	システム導入事前作業	環境調査	国保連合会	
2		設置・作業場所準備	国保連合会	
3		導入手順書確認	国保連合会	
4		ハードウェア初期設定	連合会 HW 受託業者	
5		工事（電源、回線等）	国保連合会 回線業者	
6		ハードウェアの搬入・設置	連合会 HW 受託業者：搬入・設置 国保連合会：立ち合い	
7	システム導入	分散配置 SW 設定 分散配置 SW に接続する標準 L2SW の設定	国保連合会	分散配置構成の国保連合会のみ
8		国保連合会導入作業(サーバ)	国保連合会：サーバ導入作業 共通ネットワークシステム受託者：一部機能の導入作業	共同運用センター導入作業含む
9		国保連合会導入作業(クライアント PC)	国保連合会	
10		動作確認・バックアップ	国保連合会	
11		作業報告	国保連合会	
12	その他	問合わせ対応	国保連合会：問合わせ、情報採取、回答指示対応 連合会ヘルプデスク：問合わせ受付、回答 共通ネットワークシステム受託者：調査、回答作成	
13		システム導入作業指揮	国保中央会(事務局)	
14		独自処理システム向け作業	国保連合会	独自処理システムを設置する国保連合会が対象

表 2-65 構築作業役割分担

No.	作業区分	作業名	役割分担	備考
15		都道府県・保険者向け回線高速化作業	国保連合会	拡張構成の国保連合会が対象
16		都道府県・保険者の遠隔接続保守	国保連合会：遠隔接続保守用のクライアント PC の準備 連合会 HW 受託業者：遠隔接続保守の利用が可能な設定	

① システム導入事前作業

(a) 環境調査・設置・作業場所準備

国保連合会の次期システムの環境調査を実施する。国保連合会は国保中央会から提示される環境調査票の各様式に従い回答を作成する。
また、国保連合会で次期システム機器の設置場所及び連合会 HW 受託業者のシステム導入の作業場所確保も行う。

表 2-66 環境調査・設置作業場所準備の役割分担

No.	作業区分	作業名	作業詳細	役割分担	備考
1	システム導入事前作業	環境調査	環境調査票様式提供	国保中央会	
2			環境調査票作成	国保連合会	
3			環境調査票確認	国保中央会	
4		設置・作業場所準備	設置・作業場所準備	国保連合会	
5			現地調査	連合会 HW 受託業者 SDN 機器受託業者	

(b) 導入手順書確認

国保中央会から提供される暫定版の導入手順書の確認を国保連合会で行う。
不明点、質問等がある場合、現行システムの業務支援システムを利用して問合せを行う。
改版が必要な問合せは導入手順書に反映を行い、システム導入作業前に正式版を国保中央会より発出する。

表 2-67 導入手順書確認の役割分担

No.	作業区分	作業名	作業詳細	役割分担	備考
1	システム導入事前作業	導入手順書確認	導入手順書の提供	国保中央会	
2			導入手順書の確認	国保連合会	
3			問合せ対応	共通ネットワークシステム受託者	

（c）ハードウェア初期設定

連合会 HW 受託業者がハードウェアの初期設定を行う。

表 2-68 ハードウェア初期設定の役割分担

No.	作業区分	作業名	作業詳細	役割分担	備考
1	システム導入事前作業	ハードウェア初期設定	NW 機器構築(設定、試験)	連合会 HW 受託業者	
2			仮想化基盤構築(設定、試験)		
3			仮想サーバ構築(OS 初期導入まで)		
4			アプライアンスサーバ構築(初期設定まで)		

（d） 工事(電源、回線等)

次期システム機器の導入に向けて、連合会 HW 受託業者から提供された情報を基に国保連合会で電源、空調設備、フロア間 LAN 配線、共通 NW 回線等の工事を行う。

表 2-69 工事の役割分担

No.	作業区分	作業名	作業詳細	役割分担	備考
1	システム導入事前作業	工事（電源、回線等）	HW 情報提供(電気容量、コンセント形状等)	連合会 HW 受託業者	
2			NW 情報提供(回線、ONU 設置等)	共通ネットワークシステム回線業者	
3			工事対応(ラック、電源拡張等)	国保連合会	
4			次期システム用分散配置 SW の設定	国保連合会	

（e）ハードウェアの搬入・設置

HW 受託者が初期設定を完了させた機器を国保連合会に搬入する。

搬入後、ラックマウント・配線を連合会 HW 受託業者、国保連合会で行う。

なお、ハードウェアの搬入・設置期間中に、共通ネットワーク回線を開通するよう調整すること。

表 2-70 ハードウェアの搬入・設置の役割分担

No.	作業区分	作業名	作業詳細	役割分担	備考
1	システム導入事前作業	ハードウェアの搬入・設置	搬入	連合会 HW 受託業者 SDN 機器受託業者	
2			ラックマウント、電源接続	連合会 HW 受託業者 SDN 機器受託業者	
3			配線(次期システム機器間)	連合会 HW 受託業者	
4			配線(連合会基幹共通ルータ～ONU)	連合会 HW 受託業者	
5			配線(次期システム機器、分散配置スイッチ)	連合会 HW 受託業者	
6			配線(連合会関係機関 L2、高速回線ルータ)	国保連合会	
7			配線(連合会クライアント L2SW、クライアント PC)	国保連合会	
8			搬入・設置作業立ち合い	国保連合会	

② システム導入

共通ネットワークが提供する範囲のシステム導入は国保中央会が提供する導入手順書に従い、国保連合会でシステム導入を行う。なお、導入の過程で共同運用センター側で共通ネットワークシステム受託者の作業も発生するため、現行システムの業務支援システムを経由して連携を行う。

表 2-71 システム導入の役割分担

No.	作業区分	作業名	作業詳細	役割分担	備考
1	システム導入	分散配置 SW 設定 分散配置 SW に接続する標準 L2SW の設定	次期システム用分散配置 SW の設定(※1) 分散配置 SW と接続する標準 L2SW の設定（※2）	国保連合会	
2		国保連合会導入作業(サーバ)	導入手順書を利用した導入作業	国保連合会：サーバ導入作業 共通ネットワークシステム受託者：一部機能の導入作業	共同運用センター導入作業含む
3		国保連合会導入作業(クライアント PC)	導入手順書を利用した導入作業	国保連合会	
4		動作確認・バックアップ	共通ネットワークシステムの動作確認・バックアップ	国保連合会	
5		作業報告	システム導入作業結果の報告	国保連合会	

※1 分散配置する国保連合会は、現行システムで利用している分散配置回線及び分散配置 SW を次期システムでも流用する場合、次期システム向けの作業が必要となる。

※2 分散配置を行う国保連合会は、分散配置 SW に接続するために標準システムの L2SW の設定変更を行う必要がある。

標準システムの L2SW の設定変更は以下ドキュメントを参照して国保連合会が行う。

・分散配置 SW 接続用クライアント L2 操作手順書

・連合会サーバ L2SW 操作手順書（連合会 HW 受託業者から提供）

・連合会 DMZL2SW 操作手順書（連合会 HW 受託業者から提供）

・インタフェース一覧

共通ネットワークのシステム導入作業の流れを以下に示す。

また、「介護保険システム・障害者総合支援システム提供機能導入」は各システムの提供ドキュメントを参照して行う。

なお、共通ネットワークシステムのシステム導入作業完了後はサーバを起動した状態にする。

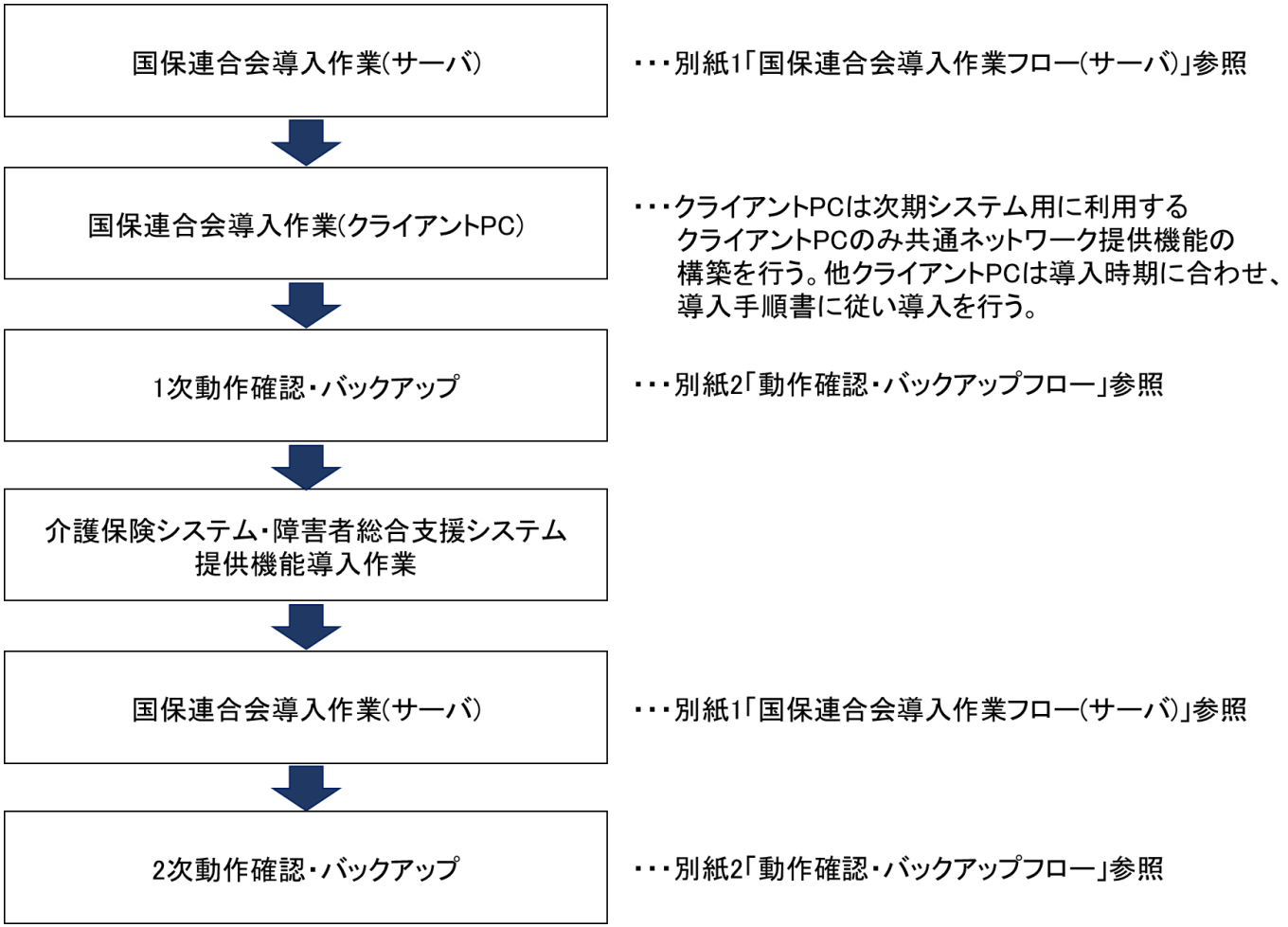


図 2-31 共通ネットワークシステム全体システム導入フロー

(a)　国保連合会導入作業(サーバ)

サーバ導入作業のフローを別紙 1「国保連合会導入作業フロー(サーバ)」に、作業項目及び作業内容を以下に示す。

導入作業は連合会 AD サーバ#1 の構築から開始すること。

連合会 AD サーバ#1 の「サーバ個別設定」が完了後、連合会 AD サーバ#1 以外のサーバの構築は並行に実施することが可能。

表 2-72 国保連合会導入作業詳細(サーバ)

No.	作業項目	作業内容
1	作業概要の確認	対象マシン、作業予定時間、準備物、前提条件、注意事項等を確認する。
2	作業開始連絡	国保連合会は、現行システムの業務支援システムを利用して国保中央会へ作業開始連絡を行う。「作業開始連絡」が完了した後、後続作業の「構築用端末の設定」を行う。
3	作業開始連絡受領	国保中央会は、業務支援システムを経由して国保連合会から作業開始連絡を受領する。
4	構築用端末の設定	HCI 上の共通ネットワークシステムの仮想マシンのシステム導入を行うために、構築用端末に IP アドレスの設定や仮想マシンで利用するツールのインストール等を行い、連合会運用クライアント L2SW または連合会クライアント L2SW に接続する。
5	対象機器に接続	仮想マシンには構築用端末から vSphere Web Client で、アプライアンス機器(連合会バックアップアプライアンス#1、連合会バックアップアプライアンス#2)にはコンソールで接続する。
6	事前作業	構築作業で利用するツールのコピー等を行う。
7	サーバ共通設定	各サーバで共通的な Windows OS の設定を行う。
8	サーバ設定	アプライアンス機器(連合会バックアップアプライアンス#1、連合会バックアップアプライアンス#2)の OS 設定を行う。
9	サーバ個別設定	各サーバのメイン機能を構築する。連合会 AD サーバ#1 の「サーバ個別設定」完了後、他のサーバの「ドメイン参加」が実施可能となる。ただし、連合会バックアップアプライアンス#1 及び連合会バックアップアプライアンス#2 の「ドメイン参加」は不要。
10	ドメイン参加	対象サーバをドメインへ参加させる。
11	サーバ個別設定作業依頼	連合会ログ管理サーバ#1 の「サーバ個別設定」は共通ネットワークシステムが行う。そのため、国保連合会は、現行システムの業務支援システムを利用して国保中央会へサーバ個別設定作業依頼を行う。
12	サーバ個別設定作業依頼受領	国保中央会は、現行システムの業務支援システムを経由して国保連合会から連合会ログ管理サーバ#1 のサーバ個別設定作業依頼を受領する。
13	サーバ個別設定作業完了報告	国保中央会は、NO11「サーバ個別設定作業依頼」で受けた業務支援システムの回答で国保連合会へ連合会ログ管理サーバ#1 のサーバ個別設定作業完了報告を行う。
14	サーバ個別作業完了報告受領	国保連合会は、現行システムの業務支援システムを経由して国保中央会から作業完了報告を受領する。

表 2-72 国保連合会導入作業詳細(サーバ)

No.	作業項目	作業内容
15	各サーバの「サーバ個別設定」が完了するまで作業を中断する。	後続の「エージェント導入」を開始するためには、各サーバの「サーバ個別設定」が完了している必要がある。そのため、各サーバの「サーバ個別設定」が完了するまで作業を中断する。各サーバの「サーバ個別設定」が完了した後、後続の「エージェント導入」を開始する。なお、「エージェント導入」以降の作業は各サーバ同時に進めてもよい。
16	エージェント導入	以下のエージェントを導入する。ただし、導入するエージェントはサーバごとに異なる。 ・Splunk Universal Forwarder ・WebSAM SystemManagemer G Agent ・NeoFaceMonitorAD モジュール ・Arcserve エージェント ・ウイルスバスターCorp クライアント ・SKYSEA 端末機
17	Windows パッチ適用	各サーバに Windows セキュリティモジュールパッチを適用する。ただし、連合会バックアップアプライアンス#1 及び連合会バックアップアプライアンス#2 の「Windows パッチ適用」は不要。
18	1 次作業完了報告	国保連合会は、現行システムの業務支援システムを利用して国保中央会へ 1 次作業完了報告を行う。1 次作業完了報告後は次期システム用に利用するクライアント PC の共通ネットワーク提供機能の導入作業を実施する。 他クライアント PC は導入時期に合わせ、導入手順書に従い導入を行う。
19	1 次動作確認・バックアップ	別紙 2「動作確認・バックアップフロー」に従い、共通ネットワークシステム提供機能の動作確認・バックアップを実施する。
20	介護保険システム・ 障害者総合支援システム 提供機能導入	共通ネットワークが提供する範囲のクライント PC のシステム導入が完了後、 介護保険システム、障害者総合支援システムの各導入手順書に従い、サーバ及びクライアント PC の導入作業を実施する。
21	サーバ個別設定	介護保険システム、障害者総合支援システムのシステム導入の完了後に実施可能になる、共通ネットワークシステムのサーバでの設定作業を実施する。
22	事後作業	構築作業で利用したツールの削除等を行う。
23	対象機器から切断	仮想マシンは vSphere Web Client から、物理マシン(連合会バックアップアプライアンス#1、連合会バックアップアプライアンス#2)はコンソールから切断する。
24	作業完了報告	国保連合会は、現行システムの業務支援システムを利用して国保中央会へ作業完了報告を行う。
25	作業完了報告受領	国保中央会は、現行システムの業務支援システムを経由して国保連合会から作業完了報告を受領する。

(b)　国保連合会導入作業(クライアント PC)

クライアント PC は次期システム用に利用するクライアント PC のみ共通ネットワーク提供機能の構築を行う。他クライアント PC は導入時期に合わせ、導入手順書に従い導入を行う。

(c)　動作確認・バックアップ

動作確認・バックアップのフローを別紙 2「動作確認・バックアップフロー」に、作業項目及び作業内容を以下に示す。

また、共通ネットワークシステムのサーバ及び次期システムで利用する構築用端末に共通ネットワークシステム提供機能を導入完了した後に行う動作確認・バックアップを「1 次動作確認・バックアップ」とし、介護保険、障害者総合支援システムの導入完了後に行う動作確認・バックアップを「2 次動作確認・バックアップ」とする。

なお、1 次動作確認では共通ネットワークシステムに閉じた動作確認を行い、2 次動作確認では介護保険、障害者総合支援システム導入完了後に実施可能な動作確認を行う。

表 2-73　1 次動作確認・バックアップ作業詳細

No.	作業項目	作業内容
1	動作確認	次期システムで利用する構築端末の共通ネットワークサービス提供機能の導入が完了後、開始する。国保連合会が作業チェックシートを参照して動作確認を行う。
3	バックアップ実行	国保連合会が作業チェックシートを参照してバックアップを行う。
4	バックアップ完了報告	国保連合会が現行システムの業務支援システムを利用して国保中央会へ完了報告を行う。
5	バックアップ完了報告受領	国保中央会は、現行システムの業務支援システムを経由して国保連合会から作業完了報告を受領する。

表 2-74　2 次動作確認・バックアップ作業詳細

No.	作業項目	作業内容
1	作業開始連絡	国保中央会から「表 2-72　国保連合会導入作業詳細(サーバ)」の NO25「作業完了報告受領」で受けた業務支援システムの回答で動作確認・バックアップ作業の開始連絡を行う。 ※「国保連合会導入作業フロー(サーバ)」の作業完了後、共通ネットワークシステムで導入完了したサーバの秘匿化作業を行う。共通ネットワークシステムでの秘匿化作業完了後に開始連絡を行う。
2	動作確認	国保連合会が作業チェックシートを参照して動作確認を行う。
3	バックアップ実行	国保連合会が作業チェックシートを参照してバックアップを行う。
4	バックアップ完了報告	国保連合会が現行システムの業務支援システムを利用して国保中央会へ完了報告を行う。
5	バックアップ完了報告受領	国保中央会は、現行システムの業務支援システムを経由して国保連合会から作業完了報告を受領する。

③ その他

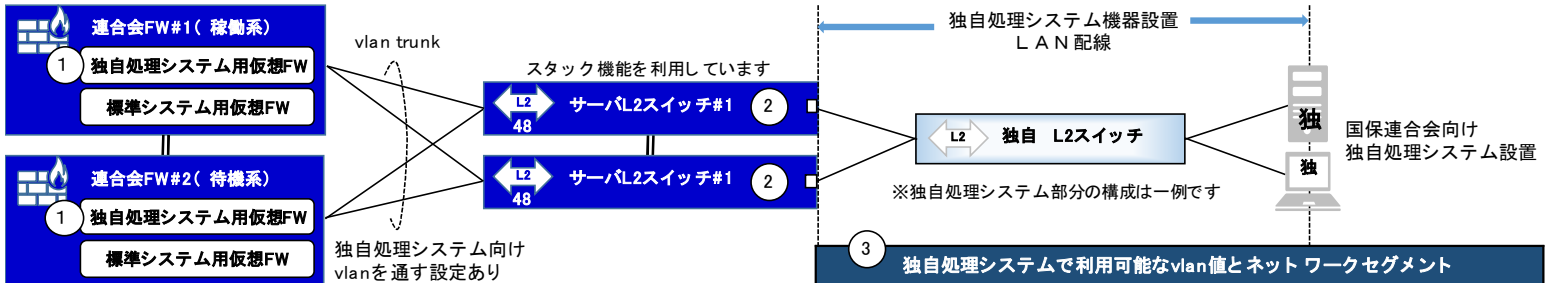
システム導入作業に関するその他作業を以下に示す。

表 2-75 その他作業の役割分担

No.	作業区分	作業名	作業詳細	役割分担	備考
1	その他	問合わせ対応	システム導入時の問合わせ対応	国保連合会	国保連合会：問合わせ、情報採取、回答指示対応 連合会ヘルプデスク：問合わせ受付、回答 共通ネットワークシステム受託者：調査、回答作成
2		システム導入指揮	システム導入作業指揮	国保中央会(事務局)	
3		独自処理システム向け導入作業	独自処理システムを導入する際のネットワーク機器設定変更	国保連合会	独自処理システムを設置する国保連合会が対象
4		都道府県・保険者向け回線高速化作業	都道府県・保険者向け高速回線を次期システムに切り替えるためのネットワーク機器設定変更	国保連合会	都道府県・保険者回線の高速化を拡張構成で導入した国保連合会が対象
5		都道府県・保険者の遠隔接続保守	遠隔接続保守用のクライアントPCの準備	国保連合会	都道府県・保険者に設置したネットワーク機器を遠隔接続保守する国保連合会が対象

(a) 国保連合会向け独自処理システムの導入作業

次期システムにおける国保連合会向けの独自処理システムについて、ネットワーク構成概要とネットワーク機器の設定変更概要を説明する。



3 独自処理システムで利用可能なvlan値とネット ワークセグメント

vlan値	ネット ワークセグメント （ ○○＝都道府県番号）
1828	10.○○.82.0/24
1868	10.○○.86.0/24
1888	10.○○.88.0/24
128	10.○○.182.0/24

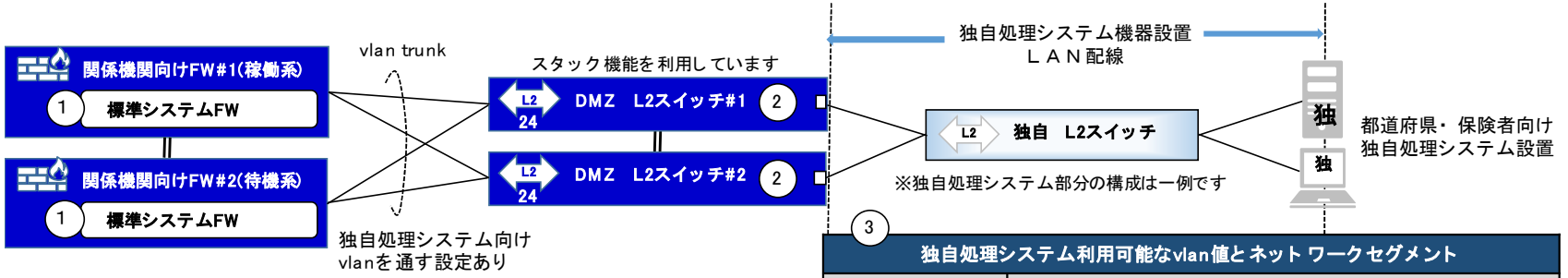
図 2-32ネットワーク構成概要図（国保連合会向け独自処理システム）

表 2-76 ネットワーク設定変更概要（国保連合会向け独自処理システム）

図内番号	図内番号説明	国保連合会で実施する設定変更概要	備考
①	国保連合会向け独自処理システムは、連合会 FW に設定済みの専用仮想 FW で通信制御を行う。	国保連合会向け独自処理システムを導入する際は、独自処理システム用仮想 FW のポリシーを設定し、必要な通信を許可する。	ポリシーの初期値は、全ての通信が拒否状態である。
②	次期システムでは、サーバ L2 スイッチに国保連合会向け独自処理システムを接続する。	国保連合会向け独自処理システムを接続するためのスイッチポートを設定する。	国保連合会向け独自処理システムの接続要件に合わせて設定すること。
③	国保連合会向け独自処理システムで利用するvlan値とネットワークセグメントである。 なお、ネットワークセグメントは全て 24 ビットマスクである。	国保連合会向け独自処理システムを現行システムから移行する場合、基本的に同一のネットワークセグメントを利用する。	現行システムの vlan 値と異なるネットワークセグメントに注意すること。なお、新規に独自処理システムを導入する場合、国保中央会から利用セグメントを割り当てる。

(b) 都道府県・保険者向け独自処理システムの導入作業

次期システムにおける都道府県・保険者向け独自処理システムについて、ネットワーク構成概要とネットワーク機器の設定変更概要を説明する。



独自処理システム利用可能なvlan値とネットワークセグメント

vlan値	ネットワークセグメント （ ○○＝都道府県番号）
48	10.○○.84.0/24 もしくは 10.○○.84.0/25
148	10.○○.184.0/24 もしくは 10.○○.184.0/25
168	10.○○.186.0/24

図 2-33 ネットワーク構成概要図（都道府県・保険者向け独自処理システム）

表 2-77 ネットワーク設定変更概要（都道府県・保険者向け独自処理システム）

図内番号	図内番号説明	国保連合会で実施する設定変更概要	備考
①	都道府県・保険者向け独自処理システムは、現行システムと同様に、関係機関向け FW で通信制御を行う。	都道府県・保険者向け独自処理システムを導入する際は、関係機関向け FW のポリシーを設定し必要な通信を許可する。	ポリシーの初期値は、全ての通信が拒否状態である。
②	次期システムでは、DMZ L2 スイッチに都道府県・保険者向け独自処理システムを接続する。	都道府県・保険者向け独自処理システムを接続するためのスイッチポートを設定する。	都道府県・保険者向け独自処理システムの接続要件に合わせて設定すること。
③	都道府県・保険者向け独自処理システムで利用する vlan 値とネットワークセグメントである。	都道府県・保険者向け独自処理システムを現行システムから移行する場合、基本的に同一のネットワークセグメントを利用する。	現行システムの vlan 値と異なるネットワークセグメントに注意すること。なお、新規に独自処理システムを導入する場合、国保中央会から利用セグメントを割り当てる。

(c) 都道府県・保険者の遠隔接続保守

標準構成で都道府県・保険者回線高速化を実施している場合、都道府県・保険者に設置されている機器（都道府県・保険者ファイアウォール（保険者）及び都道府県・保険者ルータ/スイッチ（保険者））に対し、遠隔接続保守が可能となる。

遠隔接続保守の使用有無については、各国保連合会の判断によるが、標準構成向け遠隔接続保守用の設定を次期システムで導入する標準機器に連合会 HW 受託者が設定を行う。

ア．目的

- 都道府県・保険者に設置されている機器の設定変更（ファイアウォールのポリシー変更対応等）
- 通信障害時の原因の切り分け

イ．概要

- 国保連合会の DMZ L2 スイッチ#1 に遠隔接続保守用のクライアント PC を接続し、都道府県・保険者に設置されたファイアウォール及びルータ/スイッチに遠隔接続する。
- 遠隔接続は、暗号化された通信プロトコルのみを許可する。
- 遠隔接続は関係機関向けファイアウォールで通信制御し、都道府県・保険者ファイアウォール（保険者）及び都道府県・保険者ルータ/スイッチ（保険者））以外の都道府県・保険者機器へのアクセスを不可とする。

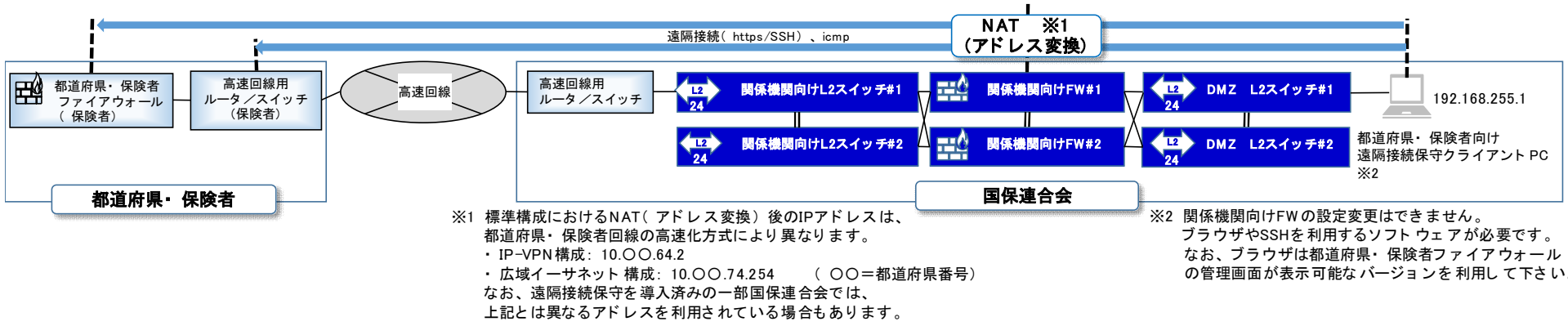


図 2-34 都道府県・保険者の遠隔接続保守概要図

2.2.2. 提供ドキュメント

システム導入に必要となる手順書等、提供を予定しているドキュメントについて以下に示す。

表 2-78 提供予定ドキュメント

No.	ドキュメント名称	内容	先行連合会 提供予定時期	全国連合会 提供予定時期
1	導入手順書	・国保連合会導入作業フロー(サーバ) ・動作確認・バックアップフロー ・連合会 AD サーバ#1 ・連合会セキュリティパッチ配信サーバ#1 ・連合会ログ管理サーバ#1 ・連合会ウイルス対策サーバ#1 ・連合会バックアップアプライアンス#1 ・連合会バックアップアプライアンス#2 ・連合会監視サーバ#1 ・連合会シスログサーバ#1 ・連合会都道府県・保険者セキュリティパッチ配信サーバ#1 ・連合会都道府県・保険者ウイルス対策サーバ#1 ・分散配置 SW 接続用クライアント L2 操作手順書 ・連合会サーバ L2SW 操作手順書(連合会 HW 受託業者から提供) ・連合会 DMZL2SW 操作手順書(連合会 HW 受託業者から提供) ・独自処理システム向けファイアウォール操作手順書 ・関係機関向けファイアウォール操作手順書 ・インタフェース一覧	暫定版 2019 年 4 月上旬 正式版 2019 年 4 月下旬	暫定版 2019 年 4 月上旬 正式版 2019 年 5 月下旬
2	導入作業実績報告書	作業チェックシート兼作業報告書	2019 年 4 月下旬	2019 年 5 月下旬
3	構築用アカウント一覧	構築時に必要となるアカウント一覧	2019 年 4 月下旬	2019 年 5 月下旬
4	構築用媒体	構築時に必要となる作業媒体。DVD での提供を予定。	2019 年 4 月下旬	2019 年 5 月下旬

なお、上記提示物は、今後の検討及び調整により変更となる可能性がある。

2.2.3. スケジュール

先行連合会及び全国連合会での導入するスケジュールを以下に示す。

なお、スケジュールは、今後の検討及び調整により変更となる可能性がある。

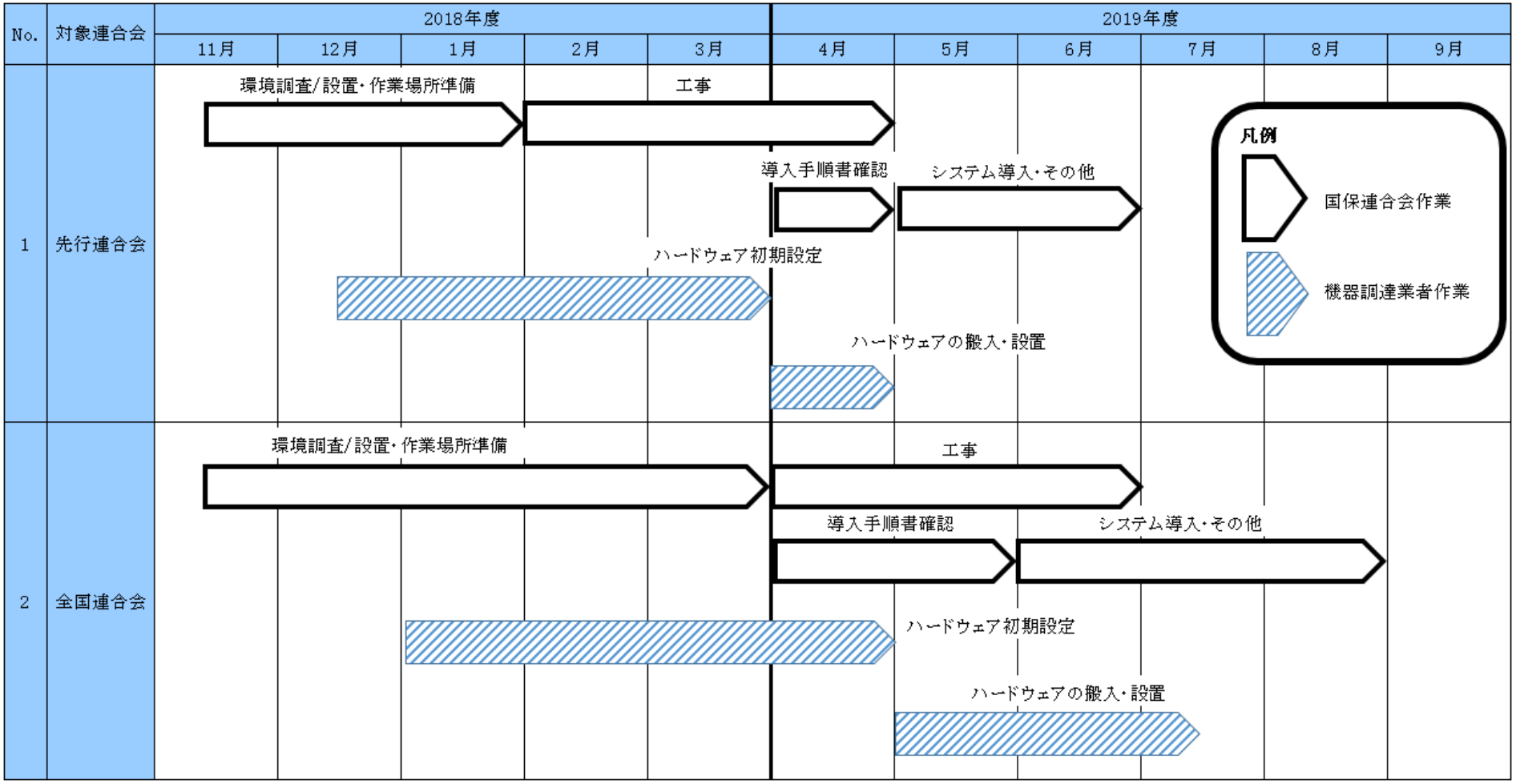


図 2-35 導入スケジュール

2.2.4. 留意点・依頼事項

- 構築用端末は次期システムで使用するクライアントPCを利用して行う。
  なお、構築用端末は以下の仕様を満たすこと。
  Microsoft Windows 10 Enterprise 2016 LTSB (64BitOS)
  Microsoft Internet Explorer 11
- システム導入作業(導入手順書を利用して行う作業)は共通ネットワーク回線の開通後に行う。
- 「表 2-63 導入機器・仮想サーバ一覧」のNO13～21の機器は介護保険、障害者総合支援システムのサーバより先にシステム導入を行う。

別紙1
国保連合会導入作業フロー
(サーバ)

機2：関係者限り

フロー名称： 国保連合会導入作業フロー(サーバ)

凡例：
- ○：開始・再開（○内の数字は作業順番）
- ◉：終了
- ◇：分岐
- →：流れ
- ▭：作業項目
- ：備考
- ：備考（複数）

国保連合会

連合会ADサーバ#1 導入手順書	連合会ログ管理サーバ#1 導入手順書	連合会セキュリティパッチ配信サーバ#1 導入手順書	連合会都道府県・保険者セキュリティパッチ配信サーバ#1 導入手順書	連合会ウイルス対策サーバ#1 導入手順書	連合会都道府県・保険者ウイルス対策サーバ#1 導入手順書	連合会監視サーバ#1 導入手順書	連合会シスログサーバ#1 導入手順書	連合会バックアップアプライアンス#1 導入手順書	連合会バックアップアプライアンス#2 導入手順書	国保中央会（共通ネットワークシステム）

連合会ADサーバ#1を最初に構築する。
連合会ADサーバ#1の「作業概要の確認」～「サーバ個別設定」までを実施する。

連合会ADサーバ#1の「サーバ個別設定」が完了していることを確認する。
②～⑩の作業は並行に実施することが可能。

① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩

作業概要の確認

作業開始連絡

業務支援システム

「作業開始連絡」完了後、「構築用端末の設定」へ進む。

作業開始連絡受領

構築用端末の設定

対象機器に接続

事前作業

サーバ共通設定

サーバ設定

サーバ個別設定

連合会ADサーバ#1の「サーバ個別設定」完了後、他のサーバの「ドメイン参加」が実施可能となる。
ただし、連合会バックアップアプライアンス#1および連合会バックアップアプライアンス#2は除く。

ドメイン参加

連合会ログ管理サーバ#1の「サーバ個別設定」は共通ネットワークシステムで実施するため、作業依頼を行う。

サーバ個別設定作業依頼

サーバ個別設定作業依頼受領

連合会ログ管理サーバ#1の「作業概要の確認」へ進む。

サーバ個別設定

サーバ個別設定作業完了報告

サーバ個別設定作業依頼」で受けた業務支援システムの回答で国保連合会へ完了報告を行う。

各サーバの「サーバ個別設定」が完了するまで作業を中断する。
各サーバの「サーバ個別設定」完了後、⑪の作業を開始する。
なお、⑪～⑳の作業は並行に実施することが可能。

⑪ ⑫ ⑬ ⑭ ⑮ ⑯ ⑰ ⑱ ⑲ ⑳

エージェント導入

Windowsパッチ適用

1次作業完了報告

1次作業完了報告受領

各サーバの1次作業完了報告を行うまで作業を中断する。
各サーバの1次作業完了報告後、**別紙「国保連合会導入作業フロー(クライアントPC)」**に従い、**クライアントPC**の導入作業を実施する。

各サーバの1次動作確認及びバックアップを別紙2「動作確認・バックアップフロー」)に従い行う。

介護保険システム・障害者総合支援システム提供機能導入
共通ネットワークが提供する範囲のクライントPCのシステム導入が完了後、
介護保険システム、障害者総合支援システムの各導入手順書に従い、サーバ及びクライアントPCの導入作業を実施する。

事後作業

対象機器から切断

作業完了報告

作業完了報告受領