次期サーバ基盤構築及び納品業務

入札仕様書

第１版

栃木県農業共済組合

【版数管理】

版数	日付	備考
第 1 版	令和 6 年 2 月 9 日	

1　システム化の背景・目的

農業共済ネットワーク化情報システムは､既にその構想段階から数えると 20 余年を経過しており、その間、ＮＯＳＡＩを取り巻く状況（農政の動き、制度検討、ＮＯＳＡＩ団体運営、コンプライアンス、内部統制の状況など）は大きく変化している。

一方、ＩＴ分野においても、新しい技術の開発やネットワーク環境の進化など、急速な技術の進展・システム環境の変化を遂げており、その対応に係るシステム保守・維持のコスト削減が求められるとともに、セキュリティ強化（個人情報保護、機密保持）など、システムに対する新たな課題やその重要性が高まっている。

また、組織運営面からも業務の合理化・効率化やＴＣＯの削減が求められる一方で、内部統制や、コンプライアンス強化、事業継続の強化等が重要課題となっており、それらに対するシステム対応が必要となっている。

こうしたなか､農業共済ネットワーク化情報システムは､①ｗｅｂ化への移行が必要なこと、②既存の事業システムが完全移行するまで、既存システムを維持する必要があること、③現在導入されているハードウェアが更新時期を迎えていることなどの課題がある。

これらの課題を踏まえ、次期システムへの移行を円滑に進めるため、2023 年度中に次期システムへの移行計画を策定することが組織決定された。

栃木県農業共済組合（以下「組合」という。）では、現在運用しているシステムを 2018 年度に導入した。これらの機器の保守サービスの終了に伴うサービスの打ち切りが、2024 年 7 月に予定されている。そのため、2024 年度以降における、機器の安定した運用を確保するために、これらの機器の更新を行うものである。

なお、機器の更新に当たっては、機能配置の再考（メンテナンス性の向上）及びスケーラビリティの確保を念頭においた上で、業務規模に見合った機器に置き換えるものとする。

2　構築・運営形態

現在稼動中のシステム（基盤、アプリケーション）は、次期システムに移行することとする。システム移行を円滑に行うために検証環境を用意し、現行システムとの並行稼動期間を設け、次期システムの組合検証期間を 2024 年 6 月～2024 年 7 月､次期システムの本番運用開始を 2024 年 8 月 1 日とする。

2.1　システム形態

ＳＢＣ運用。

2.2　基盤構築時期

2024 年 6 月 30 日までに基盤構築を行う。

2.3　サーバの設置場所

組合。

2.4　端末展開

既存クライアントの接続先設定変更。

2.5　調達範囲

調達の範囲	内容
ＤＢサーバ基盤	ＤＢ基盤の構築 　既存ＤＢ（Oracle）のデータ移行 　新規 PostgreSQL の構築
ＡＰサーバ基盤	ＳＢＣ基盤の構築 既存アプリケーションの移行
ＡＤサーバ基盤	認証基盤の構築 ユーザ管理 ・ユーザメンテナンス ・アクセス権設定 ・時刻同期
管理サーバ基盤	仮想サーバ管理、運用管理クライアント
バックアップサーバ基盤	バックアップ管理・バックアップ用 NAS、LTO
ログ取得サーバ基盤	SKYSEA の移行
グループウェアサーバ基盤	Desknet’s NEO の移行
フィルタリングサーバ基盤	i-Filter、m-filter の移行
ウイルス対策サーバ基盤	APEX ONE の移行
ファイルサーバ基盤（基幹系、情報系）	共有データ、被害写真等保存用、 既存データの移行、
セキュアプリントサーバ基盤	SecurePrint
ファイアウォール基盤	アプライアンス機器
ファイル受け渡し専用サーバ基盤	Smooth File ネットワーク分離モデルの移行
ＶＰＮ基盤	外部からの接続（ＮＯＳＡＩ職員管理者メンテナンス用）
運用管理（障害対応等）	ハードウェア保守
ヘルプデスクサービス	ヘルプデスク（組合管理者からのヘルプデスク）
クライアント接続設定	既存クライアントの接続先設定
組合のネットワーク機器	ルータ、ハブ等
ＩＣカード	カードリーダー等 250 個
インターネット分離	インターネット分離サービスの利用
クライアント機器	ノート型 PC（Windows11 Pro）208 台、外部ディスプレイ 183 台

3　ソフトウェア製品の選定

3.1　事業システムの動作サーバ（ＡＰ、ＤＢサーバ）ＯＳ

Windows Server 2012（64bit）を選定。(既存のライセンス)

3.2　Office 製品

ＡＰサーバ：Microsoft Office2013（32bit）を選定。(既存のライセンス)

クライアント：Microsoft365 を選定。(既存のライセンス)

3.3　データベース製品

既存事業システム：Oracle11g R2（64bit）を選定。

新規事業システム：PostgreSQL を選定。

3.4　ODBC

ODBC バージョン 11.2.0.xx（32bit）を選定。

3.5　仮想化製品

組合で稼働するシステムを運用するために最適な製品を選定。

3.6　ログ取得製品

SKYSEA Client View を選定。現在利用している製品を使うこと。

3.7　Web・メールフィルタリング製品

i-Filter・m-Filter を選定。現在利用している製品を使うこと。

3.8　グループウェア製品

desknet's NEO を選定。移行ツールの提供あり。現在利用している製品を使うこと。

3.9　ファイル受け渡し専用製品

Smooth File ネットワーク分離モデル（仮想アプライアンス版）を選定。現在利用している製品を使うこと。

4　次期システム等の機能要件

4.1　システム機能

4.1.1 機能要件

①　既存事業システム環境

既存事業システムは、組合設置型ＳＢＣ方式を採用し、サーバ仮想化によるシステム環境を前提として、集中管理によるサーバ群の運用管理が可能なものとする。（別紙１参照）

また、農業共済事業システム及び収入保険システムとインターネットは分離すること。(別紙２「収入保険システム導入に関連する NOSAI システム環境等について」に準ずる)

4.1.2　機能条件

① 既存事業システム環境

ア.　クライアント接続

本所及び各支所からの接続は、ファットクライアントからの接続を可能とするこ

と。

イ．　ユーザレベルのアクセス制限

ユーザレベルで、利用権限の設定に基づいて、システムやファイルのアクセス制限が行えること。

ウ．　バックアップ

次期システムにおいては、バックアップ用NAS及びＬＴＯ等外部媒体へバックアップを行うこと。

エ．　稼働システム

現在稼働中の全事業システムの移行及び、情報系システム業務が支障なく運用できること。

オ．　印刷

プリンタからの印刷は、カードをかざして出力すること。現在稼働中の基幹系システム及び、情報系システムの業務が支障なく運用できること。

② 基幹系仮想デスクトップ環境

ア．　組織レベルのアクセス制限

ＯＵ（組織）レベルに属するユーザは、利用権限の設定に基づいて、システムやファイルのアクセス制限が行えること。

イ．　移動プロファイル機能

ログオンする端末を固定するのではなく、どの端末でログオンした場合においてもログオンした固有のデスクトップ環境が設定されること。

ウ．　ファイル共有機能

ログオンした組織レベルで、共有フォルダをマッピングして、特定ドライブでファイル共有ができること。

エ．　プログラム利用制限機能

ユーザレベルで、利用可能なプログラムの制限が行えること。

オ．　インターネットブラウザの設定

インターネットブラウザの設定を一元管理でき、セキュリティ設定等をユーザが設定変更できないこと。

カ．　システム設定の制限

画面設定、システム設定、コマンドプロンプト等システムに影響があるプログラムは利用できないように制限ができること。

キ．　ローカルディスクの保護

サーバのローカルディスクは隠蔽して、アクセスできないこと。

ク．　ネットワークコンピュータの表示制限

ネットワークコンピュータは隠蔽して、利用できないこと。

ケ．　冗長化機能

サーバに障害が発生し利用できない場合でも、利用可能なサーバに自動的に振り分けられること。

コ．　事業システムへの接続

事業システムを起動するためのメニューを作成すること。

サ．　収入保険システムへの接続

収入保険システムへ接続するためのメニューを作成すること。

シ．　インターネット接続

インターネット接続は不可とすること。

4.2　サーバ機能

4.2.1機能要件

① サーバの役割

ア．　ＤＢサーバ

ＤＢＭＳ（Oracle、PostgreSQL）サービスを提供するサーバ

イ．　ＡＰサーバ

アプリケーションを実行するサーバ

ウ．　ＡＤサーバ

Active Directory サービスを提供するサーバ

エ．　管理サーバ

仮想サーバ環境を管理するサーバ

オ．　バックアップサーバ

ディスク装置に保存されているデータを媒体にバックアップするサーバ

カ．　共有データファイルサーバ

共有データ等の保存場所（基幹系、情報系）

キ．　グループウェアサーバ

Desknet’s NEO が運用できるサーバ

ク．　ウイルス対策サーバ

ウイルス対策ソフトの管理コンソールが運用できるサーバ

ケ．　ログ取得サーバ

SKYSEA Client View が運用できるサーバ

コ．　ファイアウォール

ファイアウォールアプライアンス製品

サ．　ファイル受け渡し専用サーバ

Smooth File ネットワーク分離モデルが運用できるサーバ

シ．　セキュアプリントサーバ

SecurePrint が運用できるサーバ

ス．　WSUS サーバ

Microsoft の各製品の更新プログラムを管理・配信するサーバ

4.2.2　機能条件

① サーバ仮想化要件

ア．　運用管理の工数削減

・ 外部 SAN、ストレージ装置を利用せず、スケールアウトにも柔軟に対応できる

HCI で構築すること。

② 各サーバの機能要件

ア. ＤＢサーバ

・ Oracle 11g Standard Edition One が稼働すること。

・ PostgreSQL が稼働すること。

イ. ＡＰサーバ

・ NOSAI 全国より配布される全国標準システムが稼働し、ＤＢサーバとのデータ通信を行い、業務を遂行できること。

・ 収入保険システムに接続すること。

・ SBC は、RDS で実現すること。

・ 同時接続ユーザ数は、220 ユーザとする。

・ 1 台の AP サーバに接続するユーザは、25 ユーザ以下として構成すること。

・ 全ユーザは公開デスクトップを利用すること。

・ 基本的には、クライアントのローカルデバイスに保存できないようにすること。許可された場合は、保存可能とする。

・ 以下のアプリケーションをインストールすること。

Microsoft Office 2013
Adobe Reader
Oracle Client
アタッシェケース（暗号化ソフト）
Lhaplus（圧縮解凍ソフト）
一太郎ビューア
サクラエディタ
Claunch（ランチャーソフト）

ウ. ＡＤサーバ

・ Active Directory 構造は、１フォレスト１ドメイン２ＤＣで構成とする。

・ ユーザ数は最大 300 ユーザ。本支所単位のＯＵで管理すること。

エ. 管理サーバ

仮想サーバ環境の保守・メンテナンスが同一ネットワーク上の管理コンソールインストール端末より実施可能なこと。

オ. バックアップサーバ

共有ストレージのバックアップデータを媒体にバックアップが行えること。

カ. 共有データファイルサーバ（基幹系、情報系）

将来のデータ量の増加に柔軟に対応すること。
現在の NAS よりすべてのデータを移行すること。
アクセス権の設定を行う。ユーザ作業の場合は、ユーザ向け移行手順書を作成すること。

キ. グループウェアサーバ

・ 現在運用中である Desknet's NEO の最新版を利用すること。

ク. ウイルス対策サーバ

・ 現在運用中であるAPEX ONEを利用すること。

ケ. ログ取得サーバ

・ 現在運用中であるSKYSEA Client Viewの最新版を継続利用すること。

コ. WSUSサーバ

・ 最新バージョンのWSUSを利用すること。

サ. ファイアウォール

・ 専用装置を用意すること。

シ. ファイル受け渡し専用サーバ

・ Smooth Fileネットワーク分離モデルの仮想アプライアンス版を利用すること。

4.3 クライアントの機能

4.3.1 機能要件

① クライアントの役割

当該システムを利用して業務を行うために十分な性能を有するノート型パソコンを導入すること。また、23.8インチ相当の外部ディスプレイを付属すること。

ア. 既存事業システムへRDSで接続できること。

イ. インターネットへ接続できること。

ウ. グループウェアを閲覧できること。

エ. メールの送受信ができること。

4.3.2 セキュリティ要件

① ウイルス対策ソフトで、ウイルス対策を行うこと。

・ウイルス対策ソフトのインストール・不正プログラム検出用パターンファイル等の自動更新（即時適用）

・リアルタイム検索

・フルスキャン　実行するタイミングは、システムのレスポンスに影響しないよう各県の運用に合わせて検討。

・ウイルス対策ソフトの統合管理機能の導入

② 不正なソフトウェアのインストールを防ぐための利用者への権限管理や、情報漏えい防止のためのアクセス制限を実施すること。従って、ActiveDirectoryの権限管理機能などを利用し、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よう制限を行うこと。

・端末の利用者へはユーザ権限のみを付与

・ActiveDirectoryの権限管理

・クライアント運用管理ソフトウェアにより、端末にインストールされているソフトウェアの管理

③　OS、ブラウザ、ソフトウェアのアップデートを行うこと。※最低でも緊急性の高いもの（WindowsUpdate の優先度の高い更新プログラム等）の適用を月１回の頻度で行うこと。

・管理対象となる端末・ソフトウェアすべてを対象に適用
・全てのセキュリティパッチを適用・定期的な適用（運用負荷等を考慮しやむをえない場合を除き、原則、月１回の頻度）
・パッチ適用、更新状況の一元管理機能

④　インターネット分離サービスを利用すること。

ア．　インターネット分離機能

業務端末にエージェント等のソフトウェアをインストールする必要なく、サービスの利用ができること。

・HTTP/HTTPS のトラフィックが増えた場合も、管理者自身のメンテナンスが不要で自動でオートスケールする機能を SaaS サービスとして有し、システム側でリソース上限がないこと。
・Firefox、Safari、Chrome、Edge ブラウザで利用できること。
・クライアント端末の代理で Web アクセスを行い、サイト内コンテンツの取得・実行・描画を安全な環境で行った後、描画情報のみをクライアント端末に送付可能なこと。
・クライアント端末の代理で Web アクセス・サイト内コンテンツの取得・実行・描画を行う環境ではコンテナ技術が利用されており、業務端末上のブラウザを閉じる度に、利用されたコンテナとコンテナ内のコンテンツが破棄されること。
・無害化され端末のブラウザ上に表示された閲覧情報における、文字のコピー・ペーストが行えること。
・業務端末から Web サイトのフォーム画面に日本語入力することができること。
・URL フィルタリング機能を提供し、指定したカテゴリや脅威情報が確認されたサイトの閲覧を制御可能であること。
・ウェブサイト閲覧の際に読み取り専用（フォームへの文字入力を禁止）とする機能を持つこと。
・無害化機能を利用して閲覧するか，利用せずに閲覧するか，閲覧禁止するか，読み取り専用にするかを，ドメイン単位で設定できること。
・ファイルのアップロードおよびダウンロードができること。また管理画面の設定により、特定の Web サイトからのファイルのアップロードおよびダウンロードがドメイン単位で制御できること。
・Web サイトの文書ファイルを端末にダウンロードする場合は、無害な形式でダウンロードできること。
・ファイルアップロードを禁止する機能を持つこと。
・Web サイトへの書き込みやファイルのアップロードに対して、データが難読化さ

れることなく、情報漏洩対策等の検査に影響を与えないこと。

・ハッシュ値をもとにしたファイルスキャンが可能であり、有害と判定されたファイルのダウンロード/アップロードを制御できる仕組みを有すること。

・原則無害化対象とする宛先を制限されていないこと（メーカーの非推奨及び制限事項に該当するサイトを除く）

・無害化対象とする宛先を制限されていないこと。

・Web サイトの文書ファイルを端末にダウンロードすることなく、Web ブラウザで安全に閲覧できること。以下のファイルに対応しており、パスワード付きのファイルも閲覧できること。

Microsoft Office(Word, Excel PowerPoint, OneNote, Project), OpenOffice(Text, Spreadsheet, Presentaion), 一太郎, Word Perfect, PDF, XPS, リッチテキスト, CSV, Visio, AutoCAD

・パスワード付きファイルをダウンロードする場合、パスワードを入力することによってファイルハッシュ値、アンチウイルス、サンドボックスによるスキャン後にオリジナルファイルを安全にダウンロードできるオプションが用意されていること。

・99.9%以上のサービス稼働率を保証していること。

イ. 構成

・ユーザの送信元のグローバル IP アドレスをもとにした IP 認証および ID とパスワードによる認証を経て Web サイトを閲覧できる機能を持つこと。

・ユーザの送信元のグローバル IP アドレスを IP アドレス/ネットワークレンジで指定でき、アクセス制御ができること。

・SAML 連携が可能で、シングルサインオンに対応していること。

ウ. 管理者権限

・管理者にシステムの設定変更権限を開示し、管理者自身が利用者の使用状況をリアルタイムに確認でき、なおかつ設定変更できること。

・管理者にアクセスログ情報からレポートを作成でき、リアルタイム及び定期的に取得できる機能を有すること。

・Web 無害化サービスとして PAC ファイル及び PAC ファイルを提供するサーバを提供可能なこと。PAC ファイルは管理者が自身で設定、変更ができ、自由にダウンロードできる環境を提供すること。

・全ての Web サイトを無害化対象とすることを利用者自身で選択可能なこと。

・管理者(運用管理当者)が自らのパスワードを変更可能なこと。

⑤ データの外部への持ち出しが制限されていること

・承認フロー等が整備され、容易に持ち出せない運用となっていること

⑥　USB メモリ、CD/DVD 等の外部記録媒体の利用を制限すること。

・外部記録媒体の利用を許可する端末や、担当者を一部に限定
・外部記録媒体の利用を許可する端末を制限
・端末管理ソフトウェアで制限
・外部記録媒体を外部持出する場合は、紛失に備え、持ち出す情報を記録・書込み可能な個体管理、利用時の用途等の記録

⑦　不正実施の抑止のために、外部境界（外部サイトへのアクセスやメールの添付、USB メモリ等の外部記録媒体利用、プリンタなど）は追跡可能なログ取得等を行うこと。

・外部サイトへのアクセスログを、プロキシサーバで取得・メール利用に関するログを、ログ管理ソフトウェアで取得
・外部記録媒体利用に関するログを、端末管理ソフトウェアで取得・プリンタ機種固有の機能、または印刷ログ取得管理ソフトウェアで印刷ログを取得
　・取得したログを保護
　・ログのアーカイブデータの暗号化
　・ログの定期的なアーカイブ（ログのローテーション及び圧縮等を含む）
　・ログ保存メディアのライトワンス（１回書込、追記不可）メディア使用

⑧　端末利用者の主体認証を行うこと。

・クライアントへのログインユーザのパスワードが設定／管理されていること。

⑨　機器の持ち出し、盗難を防止すること

ア．持ち出し、盗難防止
・記録装置のパスワードロック、暗号化・データ消去ソフトや物理的破壊等による情報の完全廃棄

イ．不正持出、紛失対策
・管理者による持出管理
・端末に情報を保存させない仕組み
・記録装置のパスワードロック、暗号化
・MDM ソフトウェア等による GPS での位置情報監視
・MDM ソフトウェア等による遠隔データ消去による盗難・紛失対策

⑩　クライアント上での不正操作を防止するため、クライアントの操作記録機能や USB 等のデバイス制御機能を持ったクライアント運用管理ソフトウェアを導入すること

・クライアント上での画面キャプチャや画面のプリンタへの直接印刷など、サーバ側では制御不可能な不正操作を防止するため、クライアントの運用管理ソフトウェアを導入して、利用者の操作やデータ持ち出しを監視、制御すること。

5　次期システムの非機能要件

5.1　信頼性（可用性）要件

5.1.1　継続性

継続性の観点から、システムの稼働時間や停止運用については次のとおりとする。

①　通常運用時間（平日）

平日の運用時間については、夜間は殆どシステムを利用しないため夜間のシステム停止は可能とする。

但し、夜間バッチ等がある場合は上記の限りではない。

②　特定日運用時間（土休祝日）

平日と同様の運用スケジュールとする。

③　計画停止の有無

24 時間無停止での運用は必要ないため、事前に合意が取れていれば運用スケジュールの変更も可能とする。（計画停止有り）

5.1.2　業務継続性

業務継続を保証する対象業務の範囲としては、利用者が組合等及び組合内部の職員に限定されることから、基本的には組合等及び組合内部向けの業務システムの範囲に限定する。

また、ハードウェアの故障など想定できる障害により業務が停止する場合に、その対策により業務が再開するまでに要する時間（サービス切り替え期間）として許容できる範囲としては、手作業での代替運用が可能な点を考慮すると、１～２日と定める。

なお、ハードディスクやサーバの単一障害時は業務を停止させず処理を継続させることを要求するが、ネットワークや電源の故障時については状況に応じ対応する。

5.1.3　目標復旧水準

①　通常業務停止時

通常の障害発生時における目標復旧地点については、再処理による復元も可能なことから、１営業日前の時点（日次バックアップからの復旧）とする。

また、その復旧に要する時間の制限については、１～２営業日以内とし、復旧の対象業務は、農業共済ネットワーク化情報システムの全業務とする。

②　大規模災害時

大規模災害時は保管するデータからの復旧により業務システムを再開することとなり復旧までに時間を有する。また、ハードウェアの手配など、機器調達面で時間が掛かる場合を想定する必要がある。

よって、一ヶ月以内を大災害時の復旧目標とする。

5.1.4　耐障害性

①　サーバ

「5.1.2 業務継続性」の記載内容から考慮すると、サーバ本体については１台が故障しても縮退運転が可能な冗長化構成とする。

コンポーネント（構成物）については、業務システムで使用するハードディスクは最低限 RAID 構成が必要。また、電源については冗長化構成とする。

② ネットワーク機器

特に冗長化を必須としないが、サーバラック内のネットワーク機器については冗長化をする。

③ ストレージ

業務継続の要求度等から考慮すると、業務データを集約するストレージ構成については障害による停止時の業務に対する影響が大きいことからハードディスクの冗長化を行う。

④ データ

全業務システムを対象に業務処理で使用する一部（または全部）のデータのバックアップについては、システムを停止せずにバックアップを行えるオンラインバックアップとする。

5.1.5 災害対策

① システム復旧方針

大規模災害時の復旧方針として、早期に完全に近い形に復旧する必要がある場合はディザスタリカバリーサイト（ＤＲサイト：災害によるシステムの破壊、停止からデータを守り業務を継続するために構築するサイト）を用意する等の対策が必要となるが、費用対効果や業務継続の要求度を考慮すると、まずは限定された構成でシステムを再構築する方針とする。

5.1.6 回復性

障害の復旧作業は、復旧のスピードや正確性を確保するため、一部に手作業が発生したとしても、原則として自動バックアップツールを活用した復旧を必須条件とする。

なお、復旧が不可能となった場合を想定し手作業で行なうなどの代替運用を検討しておく必要がある。

5.2 性能・拡張性要件

システムリソース（サーバ台数、ＣＰＵ、メモリ、ハードディスク容量等）を決定する上で重要となる性能及び拡張性を判断するためには、事前に現行システムの通常時、繁忙期における使用リソース情報を収集し、分析した結果を踏まえてのサイジングが必要となる。

サイジングを行う上で検討が必要な性能・拡張性要件を以下に示す。

5.2.1　業務処理量

性能及び拡張性を検討するうえで考慮が必要な業務処理量について、農業共済ネットワーク化情報システムに関しては、プラットフォーム（ＯＳやミドルウェア）のライフサイクルより 2024 年度から５年間をシステムのライフサイクルと想定した場合、今後大幅な減少が見込まれる。2029 年度には、農業共済システムが、収入保険システムと同様、農業保険システム（Web システム）の基盤に統合される予定である。よって、統合後は、農業共済システム以外のファイルサーバ、グループウェア等のみを運用することになる。

システムを利用するユーザ数、同時アクセス数、オンラインリクエスト数（主に画面からの入力件数）、バッチ処理件数等については現時点の数値から変動は少ないと想定されるが、利用者の異動等を考慮し若干の増加（1.2 倍程度）を考慮する。

また、業務データ量については、歴年のデータを保存する事業も存在することから、現時点の 1.5 倍程度とする。

なお、その他のデータ量として、システム基盤が利用するデータ（ログなど）に関しても考慮が必要であるため、システムでの保管期間（最低１ヶ月）、ローテーションのタイミング等を定め、必要なデータ量の見積りを行う必要がある。Desknet’ｓの AppSuite データ保存領域は、500GB

5.2.2　大量リモート印刷時の性能要件

ＳＢＣ環境で特に注意が必要なリモート印刷について、大量帳票印刷時でも画面レスポンス等が極端に悪化しないよう、使用するプリンタードライバは印刷データ圧縮機能付きを必須条件とし、ネットワークの状況で更に対策が必要な場合は、ネットワークの帯域制御を検討する。

5.3　運用・保守要件

5.3.1　バックアップ

バックアップからの復旧対象データとして、事業システムの運用に必要なデータ（Oracle データ、ＭＤＢ、その他必要ファイル）を特定しバックアップを行なう。

バックアップは、障害時やユーザ操作ミス等からの復旧を目的とし、データの長期保存としての退避は別途検討する。よって、取得タイミングは日次を基本とし保存期間は１年未満を最低条件とする。

取得媒体は、一定間隔（月次または週次）で外部媒体（ＬＴＯ等、バックアップ用 NAS）への取得を必須とするが、運用効率を考慮すると日次バックアップについては同一サイト（サーバ）のディスク内への保存も考慮する。

5.3.2　運用監視

サーバやネットワーク機器の死活監視を行い、ログによるエラー監視、リソース監視、パフォーマンス監視は必要に応じて行うこととする。

死活監視は分間隔のリアルタイム監視とし、その他エラー監視、リソース監視、パフォーマンス監視は手動により不定期で行う監視を基本とする。

なお、監視を行うサーバ機器は最低限、時刻同期を行う必要がある。

また、バックアップの自動化を行うためバックアップジョブの監視も行う。

ハードウェアの異状発生時は、アラートを自動検出し管理者にメールによる自動通知を行う機能を設ける。

5.3.3 保守運用

① 計画停止の有無

「5.1.1 継続性」で記載のとおり、運用時間帯の計画停止（点検作業、領域拡張、デフラグ、マスターメンテナンス等によるシステム停止）は、事前に利用者に通知することで可能とする。

② 運用負荷軽減

サーバや端末ソフトウェアの更新プログラム（Windows Update 等）の自動配信（及び自動更新）機能は、対象台数が多いほど運用負荷を軽減するために有効であるため、集中化するＳＢＣ環境では導入を行う。(WSUS サーバの導入等)

③ パッチ適用方針

セキュリティパッチに関しては「5.4.2 セキュリティパッチ適用」の項でも規定しており、システム全体に対し、最低でも緊急性の高いものの適用を必須とする。適用タイミングは即時を推奨するが、運用負荷を考慮し定期的な適用も可とする。

その他のパッチについては、必要性、タイミングの検討を行う。

なお、実施に当たっては、組合職員の指示に従い作業すること。

④ 活性保守

システムを停止せずにハードウェア交換やファームウェア更新といった保守作業を実施する活性保守については、必須ではないが対象を特定して（例えば、ハードディスクのみ行う等）行うこととする。

⑤ 予防保守

システム構成部材が故障に至る前に予兆を検出し事前交換などの対応をとることとする。

5.3.4 障害時運用

① 復旧作業

障害発生時の復旧作業は、「5.1.7 回復性」で記載したとおり、復旧のスピー

ドや正確性を確保するため、自動バックアップツールを活用した復旧とする。

② システム異常検知時の対応

委託業者との保守契約に関する条件として、システムの異常を検知した場合の委託業者の対応について以下の取り決めを行う。以下はその最低条件とする。

- 対応可能時間 ： 原則 8:30 ～ 17:15
- 連絡方法 ： 第 1 報は電話が基本
  (障害終息までの中間報告はメールでも可)
- 駆けつけ到着時間 ： 異常検知から原則 2 時間以内

③ 交換用部材の確保

保守部品確保レベルとしては、保守契約にて委託業者が規定する年数での確保とする。

5.3.5 運用環境

① マニュアル準備レベル

通常運用に加え障害対応時のリカバリ作業手順などを示した保守マニュアルも要求する。

② リモートオペレーション

リモート監視やリモート操作については特に必須とはしないが、業者が遠隔操作で保守を行う必要がある場合等に必須条件とする。

但し、外部接続に伴うセキュリティ強化も必要となる。

5.3.6 サポート体制

① サポート範囲

納品物のすべてを一括でサポートすること。

製品ごとに委託（Oracle は外注する等）しないこと。

② 保守契約（ハードウェア、ソフトウェア）

導入対象のハードウェア、ソフトウェアが同一ベンダのものではない場合が多い状況で、窓口を 1 本化するためにマルチベンダのサポート契約を行う。

③ ライフサイクル

次期システムのライフサイクルを 2024 年 4 月から 2030 年 3 月末までとする。

④ 役割分担

メンテナンス作業及び問い合わせ等の一次対応は、運用負荷の軽減を考慮し、

全て委託業者対応とする。

但し、ＥＵＣ環境等、一部はユーザ作業とする部分も存在すると考えられるため費用対効果も含めて対応範囲の検討が必要。

⑤　サポート要員

サポート契約を行う場合、委託業者の常駐要員（営業時間に常時連絡が可能な人員）は最低１名以上とする。

なお、委託業者の営業時間はサポート契約での取り決めとなるが、原則 8 時 30 分から 17 時 15 分までとする。

納品物に対する電話等の質疑応答には、随時対応する。また、回数制限は設けないこととする。

⑥　定期報告会

三か月に１回の定期報告会を開催し、障害および運用状況報告に加えて改善提案も報告内容に含め、システムの安定稼動や障害回避に活用する。

⑦　サービスデスク（ヘルプデスク）

運用効率上、利用者からの問い合わせに対し単一の窓口機能の提供を受ける必要があるため、サービスデスク（ヘルプデスク）を設置する。

⑧　オプションシステムの開発

基幹システムに附随するオプションシステムの開発を実施する。（案件ごとに別途見積り）

⑨　その他の運用管理の役割分担

運用･保守に関して必要となる以下の作業について、委託業者との役割分担を検討しサポート契約の範囲を明確にする。

- インシデント管理
  何らかの原因で業務を停止させる状態（インシデント）を迅速に回復させるプロセスの実施
- 問題管理
  インシデントの根本原因を追究し、可能であれば取り除くための処置を講じるプロセスを実施
- 構成管理
  ハードウェアやソフトウェアなどのＩＴ環境の構成を適切に管理するためのプロセスを実施
- 変更管理
  ＩＴ環境に対する変更を効率的に管理するためのプロセスを実施

- リリース管理
  ソフトウェア、ハードウェア、ＩＴサービスに対する実装を管理するためのプロセスを実施

5.4　セキュリティ要件

以下に記載するセキュリティ要件は、組合のセキュリティポリシー及び情報セキュリティに関する組織規定やルール、法令、ガイドライン等への適合を確認し、適合するよう要件の追加並びに対策レベルの見直し等を行う必要があるものとする。

5.4.1　セキュリティ診断

インターネットからのアクセスがある機器に対し、ツールを利用して擬似攻撃を実施することにより脆弱性を発見する診断を実施する。

5.4.2　セキュリティパッチ適用

セキュリティパッチの適用は、システム全体に対し行う。

適用パッチの対象としては全てのセキュリティパッチを適用することを推奨するが、最低でも緊急性の高いもの（Windows Update の優先度の高い更新プログラム等）の適用を月１回の頻度で行う。

なお、適用のタイミングは、パッチ出荷時の適用を推奨するが、運用負荷等を考慮し即時適用が困難な場合は定期的(四半期に１回以上)に適用を行うこととする。

但し、ウィスル対策ソフトのパターンファイルの適用については、即時適用とする。

なお、実施に当たっては、組合職員の指示に従い作業すること。

5.4.3　アクセス・利用制限

①　認証機能

利用者（管理者、一般利用者）が農業共済ネットワーク化情報システムにアクセスするためには、二要素の認証を行うこととする。各事業システムにおいては認証機能を持たないものが存在するため、例えば、事業システムが存在するドメインへのアクセス時に、ＩＤ、パスワードによる認証を行なうなど、事前に認証を行なわなければ利用できない仕組みとすることが必要となる。

また、上記の認証については、必ず個人ごとに割り当て及び管理されたカード及びPIN コードを使用することを原則とする。

②　利用制限

不正なソフトウェアのインストールを防ぐための利用者への権限管理や、情報漏えい防止のためのアクセス制限を実施する。

従って、Active Directory の権限管理機能などを利用し、必要最小限のプロ

グラムの実行、ファイルへのアクセスのみを許可するよう制限を行う。

5.4.4　データの暗号化

通信データの暗号化までは必須とはしない。また、データベース上のデータについても標準システムでは暗号化は必須とせず、Oracle ユーザに対するパスワード設定でアクセス制限を行うまでとする。但し、状況により暗号化が必要と判断した場合は、別途、対応ソフトの導入等の検討を行う。

また、データベース等の暗号化を行う場合は、該当サーバが災害などで使用不可となった場合でも複合を可能とするよう、サーバ（暗号化ソフト）の二重化や複合キーの保管などの対策を行う必要がある。

5.4.5　不正監視

①　ログの取得

事業システムでは一部を除きログの取得を実施していないため、Windows のイベントログや Oracle の操作ログ等の取得を行う。取得内容及び取得方法については以下を検討する。

- 操作ログ取得については、現在運用中の SKYSEA Client View を継続利することとする。
- Oracle の操作ログ（トレースファイル、リスナーログ等）の取得。

なお、保存期間については最低３ヶ月とする。

②　不正監視対象（ログの取得対象）

ｉ）サーバ

サーバの不正監視（ログの取得）については、アプリケーションサーバ、データベースサーバ、ファイルサーバは必ず行うこととする。その他のサーバは必要性により判断する。

ⅱ）ネットワーク

ネットワークの不正監視については、インターネットに公開しないシステムであることから必須とはしない。但し、インターネットへの外部接続が可能な環境については不正監視（ログの取得）を行う必要がある。

ⅲ）プリンタ

情報漏洩対策として、プリンタへの出力結果に対しログの取得を可能とする。

5.4.6　ネットワークへの対策

次期システムのネットワークに対する通信制御、不正検知、サービス停止攻撃の回避などのセキュリティ対策については、インターネット接続箇所に対しファイアウォールを設置すること。

5.4.7　マルウェア対策

マルウェア（ウィルス、ワーム、ボット等）の感染を防止する対策は、全サーバに対し行うことが必要となる。

リアルタイム検索の実施も必須とし、状況に合わせてそのタイミングを検討する必要がある。

＜リアルタイム検索の例＞

・ファイルサーバへデータをコピーするタイミング

・メールサーバがメールを受信したタイミング

・ファイルへの入出力処理が実行される前

フルスキャンについては、システムのレスポンスに影響しないようそれぞれの運用に合わせての実施が必要となる。

5.4.8 不正接続対策

許可されていない端末等がネットワークに接続することを防止する対策を講ずること。

5.4.9　外部媒体保存制限

外部媒体への保存制限を行う対策を講ずること。

5.5　ネットワーク要件

5.5.1　回線種別

現在運用している「FENICS ビジネス VPN サービス」を継続利用するものとする。但し、「FENICS ビジネス VPN サービス」よりセキュリティレベルが高く、安価なサービスがあれば、提案すること。

5.5.2　ネットワークの冗長化

障害復旧時間の目安および費用対効果を考慮すると、ネットワーク回線や経路の冗長化までは必須とはしないが、安価なサービスがあれば提案すること。

5.5.3　帯域保証

ネットワークの帯域保証は必須とはしない。

5.6　外部接続要件

5.6.1　外部接続の種類

①　農林水産省（再保険システム）、金融機関への口座振込関連のシステム

VPN 回線により農林水産省経営局保険課、または、金融機関へ接続。

②　収入保険システム

農業保険システムのうち収入保険システムへの接続。公開デスクトップより、接続する。収入保険システム専用回線（DCAN）

③　帳票印刷業務委託

帳票印刷を委託している業者へインターネットディスクを介して、データの受け渡しをする。

④　インターネット

組合のフレッツ光から抜けていくこと。また、ユーザは組合のＡＰサーバにログインし、i-Filter のプロキシ機能を経由すること。また、一部ＡＰサーバを介さず、ローカル PC からインターネットへ抜ける場合もある。この場合、ＡＰサーバへの接続は不可とする。

⑤　電子カルテシステムとのデータ送受信

電子カルテシステムのサーバとデータの送受信をする。専用のルータ（アライドテレシス　CentreCOM AR415S）で、組合のフレッツ光から抜けていくこと。また、ユーザは組合のＡＰサーバにログインし、i-Filter のプロキシ機能を経由すること。

⑥　家畜個体識別情報提供システム

家畜改良センターより個体データをインターネット経由でダウンロードする。

⑦　建物再共済データ送信

建物再共済データをインターネット経由で送信する。

⑧　給与システムのリモートサポート及び各種申請提出

「給与大将」システムにおいて、マイナンバーの登録・管理をする。（ローカル PC で実施）

⑨　社会保険・税金の手続き

社会保険及び税金の手続きをインターネット経由で行う。

⑩　銀行の手続き

（ア）財形貯蓄等中央労働金庫の手続き

（イ）インターネットバンキング（電子証明書が必要）

⑪　ホームページ作成

WIX にログインし、メンテナンス等実施する。

⑫　メンテナンス等のためのリモート接続

外部よりメンテナンス等のため組合のサーバログインできること。

5.6.2　性能要件

①　農林水産省（再保険システム）、金融機関への口座振込関連のシステム

再保険システム、VPN 回線であるため、性能要件としては現行の速度を保持することを条件とする。

②　インターネット

光回線接続。ＮＴＴのフレッツ光を利用する。

③　リモート接続

外部よりＰＣ、スマートフォン、タブレットから接続を可能とする。

5.6.3　信頼性要件

冗長化は必須ではない。

5.6.4　セキュリティ要件

①　農林水産省（再保険システム）、金融機関への口座振込関連のシステム

VPN によるクローズされたネットワークへの接続のため、農業共済ネットワーク化情報システムと同様の対策とする。

②　インターネット

組合のゲートウェイには、ファイアウォール設置を必須とする。

5.6.1 のうち､インターネットを利用する処理をローカルＰＣから実施する場合、事業システムを利用するサーバには接続付加とする。

③　リモート接続

VPN 装置で IPsec または、SSL-VPN によるインターネット VPN を構築する。

6　サーバ機能構成

次期システムのサーバ機能構成を下表に示す。

なお、各ハードウェアを接続するために必要なケーブル、装置等も全て提供すること。

No.	機器	性能等
1	仮想化サーバ	最適な製品 CPU Xeon 2.4GHz 20 ｺｱ、ﾒﾓﾘ 128GB、HDD 147GB 同等又はそれ以上
2	共有ストレージ	仮想 OS 領域 7TB 以上 ｵﾝﾗｲﾝﾊﾞｯｸｱｯﾌﾟ 領域も別途確保すること
3	ＡＰサーバ	Windows Server2012 Standard CPU2GHz 10 ｺｱ、ﾒﾓﾘ 20GB、HDD 200GB と同等又はそれ以上

No.	機器	性能等
4	データベースサーバ	Oracle11g：Windows Server 2016 Standard CPU Xeon 2GHz 12ｺｱ、ﾒﾓﾘ 32GB、HDD 2TB と同等又はそれ以上 PostgeSQL：Windows Server 2022 Standard CPU Xeon 2GHz 12ｺｱ、ﾒﾓﾘ 32GB、HDD 2TB と同等又はそれ以上
5	ＡＤサーバ	Windows Server 2022 Standard CPU 2GHz 4ｺｱ、ﾒﾓﾘ 12GB、HDD 100GB と同等又はそれ以上
6	管理サーバ	Windows Server 2022 Standard CPU 3GHz 2ｺｱ、ﾒﾓﾘ 16GB、HDD 300GB と同等又はそれ以上
7	バックアップサーバ	Windows Server 2022 Standard CPU 3GHz 2ｺｱ、ﾒﾓﾘ 16GB、HDD 900GB と同等又はそれ以上
8	ファイルサーバ	基幹系領域 20TB 以上、情報系領域 20TB 以上
9	グループウェアサーバ	Windows Server 2022 Standard CPU2GHz 4ｺｱ、ﾒﾓﾘ 8GB、HDD 300GB と同等又はそれ以上
10	ウイルス対策サーバ	Windows Server 2022 Standard CPU2GHz 4ｺｱ、ﾒﾓﾘ 6GB、HDD 300GB と同等又はそれ以上
11	ログ取得サーバ	Windows Server 2022 Standard CPU2GHz 4ｺｱ、ﾒﾓﾘ 8GB、HDD 500GB と同等又はそれ以上 ※ 基幹系のﾛｸﾞ取得が可能であること
12	フィルタリングサーバ	Windows Server 2022 Standard CPU2GHz 4ｺｱ、ﾒﾓﾘ 8GB、HDD 300GB と同等又はそれ以上
14	ファイル受け渡しｻｰﾊﾞ	Windows Server 2022 Standard 2ｺｱ、ﾒﾓﾘ 2GB、HDD 7000GB と同等又はそれ以上
15	ファイアウォール	ｱﾝﾁｳｨﾙｽ、ｱﾝﾁﾏﾙｳｪｱ、ｱﾝﾁｽﾊﾟﾑ機能を有すること
16	バックアップ専用機	バックアップアプライアンス製品
17	バックアップ用 LTO ライブラリ装置	全てのメディア（Ultrium1～Ultrium8）に対応していること

7　ソフトウェア構成

ソフトウェア構成を下表に示す。

ソフトウェアは、各サーバに必要なライセンス数提供すること。また、CD-ROM 等のメディアで提供することとし、同一ソフトウェアのメディアは、可能な限り 1 組のメディア及び提供する数のライセンスで提供すること。ただし、フリーソフトウェアはこの限りではない。

No.	ソフトウェア	備考
1	Office Professional Plus 2013	既存ソフトウェア
2	Windows Server 2012 CAL (User)	既存ソフトウェア〃
3	Windows Server 2012 Remote Desktop Services CAL (User)	既存ソフトウェア

No.	ソフトウェア	備考
4	Windows Server 2012 Datacenter	既存ソフトウェア
5	Windows Server 2012 Standard	既存ソフトウェア
6	Windows Server 2022 Standard	
7	Windows Server 2022 Datacenter	
8	最適な製品	仮想化ソフトウェア関連
9	Oracle 11g Standard Edition One	データベースソフトウェア関連
10	PostgreSQL	データベースソフトウェア関連
11	Arcserve Backup 19.0 for Windows	バックアップソフトウェア関連
12	Arcserve Backup 19.0	バックアップソフトウェア関連
13	PowerChute Network Shutdown Standard	バックアップソフトウェア関連
14	Smooth File ネットワーク分離モデル	ファイル受け渡し関連
15	Desknet’s NEO V8.0	既存ソフトウェア
16	i-FILTER	既存ソフトウェア
17	m-FILTER	既存ソフトウェア
18	SKYSEA Client View Ver.19	既存ソフトウェア
19	ADManager Plus	Active Directory の管理ソフト

調達ソフトウェアは、指定要件に基づき、最新版数を用意すること。

8　プリンタ構成

8.1　以下の既存プリンタを利用すること。

	RICOH SPC841	その他機種	備考
河宇支所	2	C5580	
上都賀支所	2		
芳賀支所	3		
塩谷支所	2		
那須中央支所	2		
那須北支所	2	RISO GD7330	
那須南支所	2	RICOH MPC5530	
県南支所	3		
安足支所	2		
本所	2	RISO GD7330	
合計	22	3	

9　クライアント構成

9.1　クライアントの構成

ノート型パソコン：Windows11 Pro　CPU:Core™i5-1235U　ﾒﾓﾘ:8GB　SSD 256GB 同等又はそれ以上
テンキー付キーボード

9.2　クライアントの設定作業設定

設定作業は以下の台数分発生する。

	既存 PC	新規導入 PC	新規導入 外部ディスプレイ	備考
河　宇　支　所	7	18	17	
上都賀支所	7	20	18	
芳　賀　支　所	5	26	27	
塩　谷　支　所	6	17	7	
那須中央支所	5	16	17	
那須北支所	5	16	17	
那須南支所	4	15	12	
県　南　支　所	7	26	28	
安　足　支　所	5	14	2	
本　　所	11	40	38	
合　　計	62	208	183	

10　撤去

現行のハードウェアを一部撤去すること。テスト環境として、以下のハードウェアを残し、1本のラックに集約する。その他のサーバ、ラックは撤去すること。撤去場所は、組合倉庫とし、防塵カバーを施すこと。

11　設置

ハードウェアに示した機器を以下のとおり設置すること。

なお、機器の設置に当たっては、組合職員の指示に従い作業すること。

また、設置の際に行う工事の実施に当たっては、事前にその内容について組合担当職員と打ち合わせを行い、承認を得ることとし、工事完了後に 11.2 工事に示すドキュメントを納品すること。

11.1 設置場所

設置場所	住所	機器
栃木農業共済組合　サーバ室、事務室	宇都宮市下平出町前表 319-1	サーバ等、クライアント
河宇支所　事務室	宇都宮市平出町 936-3	クライアント、ルータ、ハブ
上都賀支所　事務室	鹿沼市御成橋町 2-2051-7	クライアント、ルータ、ハブ
芳賀地方支所　事務室	真岡市八條 678	クライアント、ルータ、ハブ
塩谷地方支所　事務室	さくら市桜野 1622-1	クライアント、ルータ、ハブ
那須中央支所　事務室	大田原市町島 666-1	クライアント、ルータ、ハブ
那須北支所　事務室	那須郡那須町高久甲 5083-2	クライアント、ルータ、ハブ
那須南支所　事務室	那須烏山市大桶 2141-2	クライアント、ルータ、ハブ
県南支所　事務室	小山市立木 567	クライアント、ルータ、ハブ
安足支所　事務室	佐野市大橋町 3232-1	クライアント、ルータ、ハブ

11.2 工事

11.2.1　電源工事

組合で手配する。

11.2.2　転倒防止工事

転倒防止として、ラックは、OA フロア下の床に固定すること。

なお、転倒防止対策を行うに当たっては、OA フロアを加工してもよい。

また、以下のドキュメントを納品物として納めること。

- 転倒防止工事完成図書（内容：工事写真(工事前及び工事後)、使用材料一覧表、等）

11.2.3　無線 LAN 配線工事

エンハンスドカテゴリー６対応以上のケーブルを用いて配線を実施し、天井に無線 LAN のアクセスポイントを設置すること。

なお、配線の際には美化を損なわないように、既存の OA フロアの下や天井裏を通して配線を行うとともに、ケーブルを識別するためのシール又はタグをつけること。

また、以下のドキュメントを納品物として納めること。

- ＬＡＮ配線図

なお、工事対象の支所は、以下の通り。

- 河宇支所、上都賀支所、芳賀支所、那須中央支所、那須北支所、那須南支所、県南支所

11.2.4　「FENICS ビジネス VPN サービス」の回線速度切り替え作業

回線速度を現在の 100MB から 1GB へ変更すること。

12 導入

システム設計、機器の設定、OS、アプリケーションのインストール等を行うこと。また、現行環境からの移行、テストを行うこと。

12.1 設計

以下に示す設計書等を作成し、組合担当職員承認の上、作業を実施すること。

12.1.1 システム構成定義書

① 各種サーバ

- ハードウェア構成
- 機器の利用目的
- 機器情報
- OS インストール情報
- ディスク情報
- パーティション情報
- パッチ情報
- ユーザアカウント情報
- イベントログの設定情報
- セキュリティの設定情報
- 導入ソフトウェア一覧及び設定情報
- その他

② ネットワーク機器

- ハードウェア構成
- 機器の利用目的
- 機器情報
- 機器の設定情報
- その他

12.1.2 機能別設計書

- 仮想化基盤
- Active Directory
- Oracle
- PostgreSQL
- グループウェア
- ウイルス管理
- ログ管理
- セキュリティ管理
- バックアップ管理

12.1.3　運用設計書

起動及び停止方法、停電時の対応方法、バックアップ及びリストア方法、ログの管理方法、リソース監視等システム運用に必要な項目をすべて列挙すること。

12.1.4　テスト仕様書

テストの目的、対象範囲、実施方法、テスト体制、テスト環境、スケジュール、合格基準等、テスト全般に関わる方針をまとめること。また、テストシナリオを作成し、シナリオごとに複数のテストケース定義し、どのようなテストで何を確認するかを定義すること。

12.2 構築

12.1 設計 で作成した、システム構成定義書、機能別設計書を基に、OS、アプリケーションのインストール、設定等を行うこと。

12.3 移行

現行環境からの移行を行うこと。

なお、移行に当たっては、別途、移行スケジュール、移行内容をまとめ、事前に組合担当職員に承認を得ること。

以下に、移行に当たっての条件を示す。

12.3.1　各種サーバ

Active Directory の移行
基幹システムの移行
共有ファイルの移行
SKYSEA Client View の移行
Desknet’s NEO の移行
i-FILTER & m-FILTER の移行
ウイルスバスターの移行
クライアントの設定変更（組合、組合）
その他必要なもの

12.3.2　ルータ

既存ルータから置き換えること。

12.4 テスト

12.1.4 テスト仕様書で作成した仕様とおりに、テストを実施すること。

テスト項目及び結果については、テスト仕様書兼成績書として提示すること。

テスト項目については、システムの導入、運用、移行について行った各種設定を確認

するために必要十分な項目であること。さらに、事前に組合担当職員に提示し承認を得ること。また、テスト項目については、運用手順書に記載した内容に促して運用が可能であることを示す項目を含むこと。

テスト結果については、テスト完了後速やかに組合担当職員に提示し、確認を得ること。

なお、テスト完了後に、バックアップソフトウェアを用いて、ハードディスクのフルバックアップを行うこと。

13 教育

システム管理者向け研修を組合担当職員と打合せの上、実施すること。

研修の内容については、システム構成定義書、運用手順書、運用に用いるソフトウェアのマニュアル等に基づいて実機を用いて行い、システム運用に必要なものすべてを含むものとし、その詳細については、事前に組合担当職員に示すこと。

なお、研修対象者は 3 名とする。また、研修スケジュールについては、研修内容の量を勘案した上で、必要な日数を組合担当職員に提示した上で、組合担当職員と調整しながら作成すること。

14 契約形態

組合は、買い取りで落札業者と契約とすること。

15 入札金額

組合の納品物一括の価格で提示すること。入札金額は、設置、導入、運用、移行、テスト、教育、保守（2030 年 3 月末までの総額）等、一切の付帯経費を含むものとする。ただし、11.2 工事については、別途見積りとする。

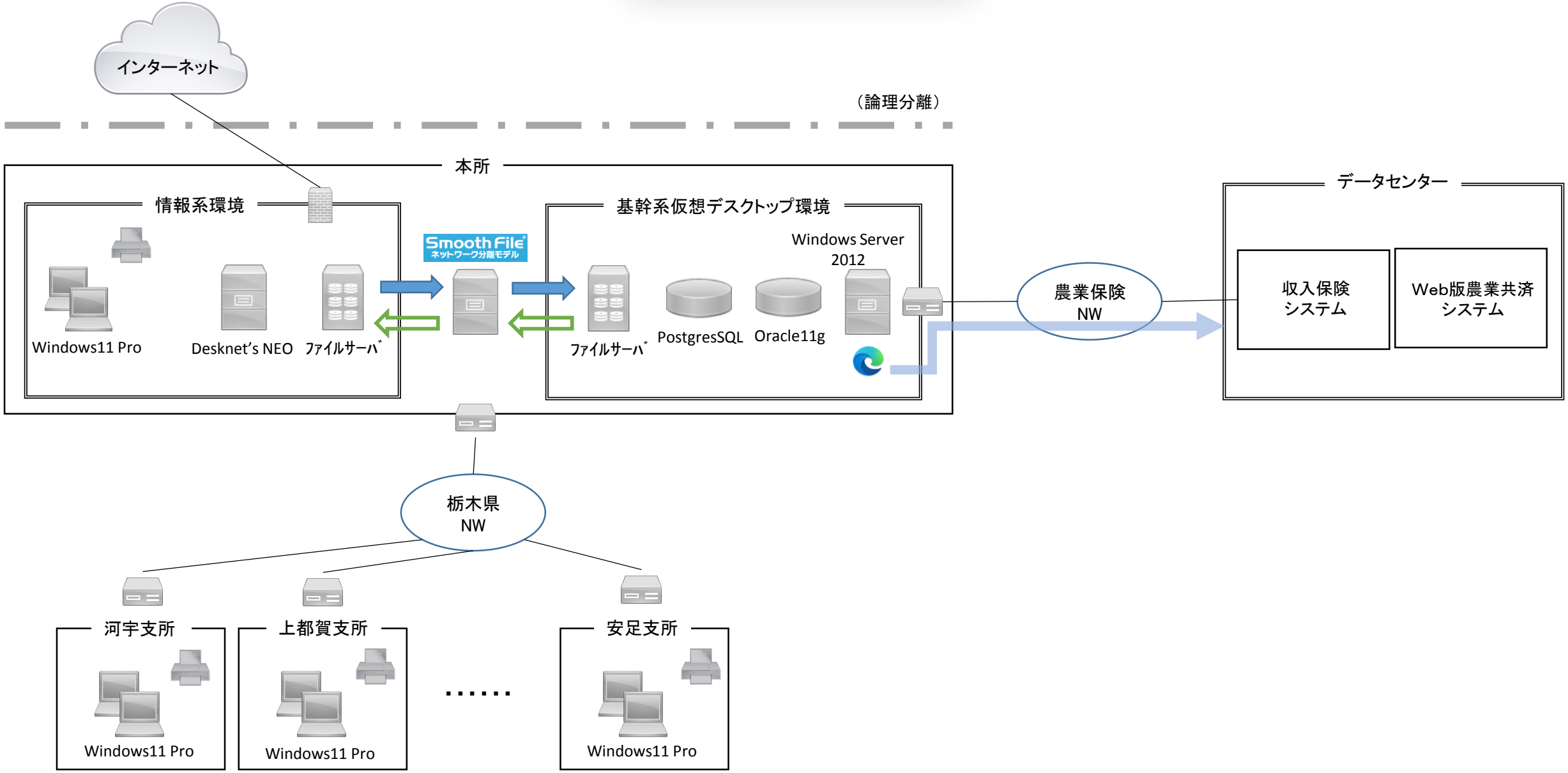
また、サポート費用については、落札業者と協議の上、別途見積りとする。

16 その他

本仕様書に明記されていない事項であっても、契約履行上必要なものは、随時組合担当職員の指示を仰ぐこととする。

【別紙1】

構成概要図


インターネット
（論理分離）
本所
情報系環境
Windows11 Pro
Desknet's NEO
ﾌｧｲﾙｻｰﾊﾞ
Smooth File
ネットワーク分離モデル
基幹系仮想デスクトップ環境
ﾌｧｲﾙｻｰﾊﾞ
PostgresSQL
Oracle11g
Windows Server
2012
農業保険
NW
データセンター
収入保険
システム
Web版農業共済
システム
栃木県
NW
河宇支所
Windows11 Pro
上都賀支所
Windows11 Pro
……
安足支所
Windows11 Pro

【別紙２】

収入保険システム導入に関連するNOSAIシステム環境等について

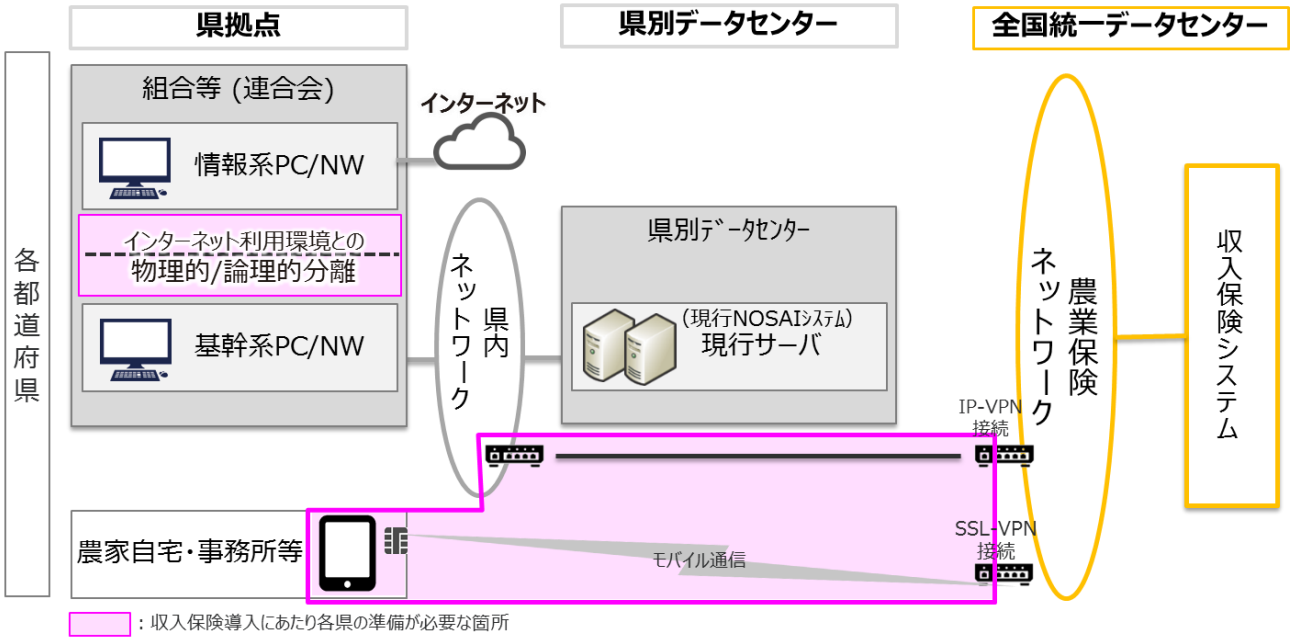
平成30年 5月24日

全国農業共済組合連合会

1．収入保険システム　全体概要

収入保険システムは、**全国統一のデータセンターでの運用**とします。
また、収入保険システムでは、取り扱うデータの性格から、NOSAIシステムよりも高いセキュリティが求められます。そのため、農業保険ネットワークに接続可能な**セキュリティポリシーとして「統一の基準」を設定**し、それを満たす環境からのみ、農業保険ネットワークへの接続を許容することとします。

システム　全体概要（NOSAI環境を含む）



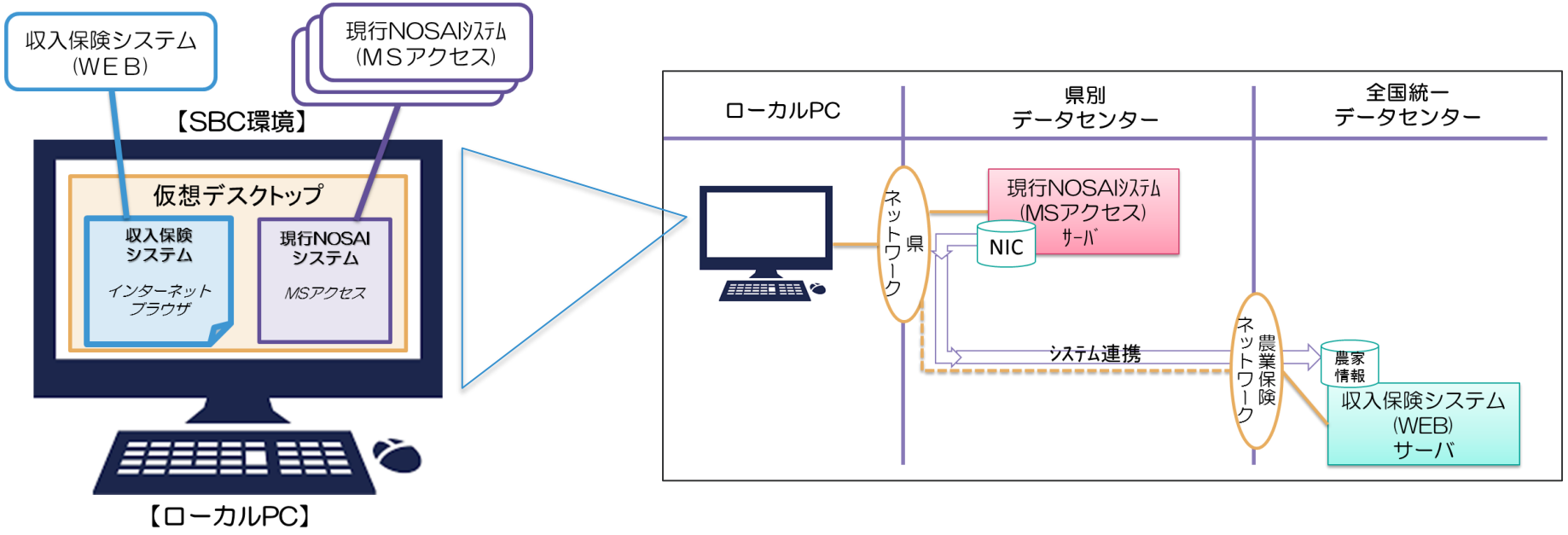
※収入保険制度開始当初は、タブレットによる申請に注力することとし、農業者によるインターネット経由の加入申請については、先送りとなっております。

NOSAIシステム環境から収入保険システム利用にあたっての統一基準

- □NOSAIシステムにおけるネットワークの要件として、外部への接続が可能な情報系のネットワークとは**物理的、または論理的に分離する**こと。（※ウイルス対策のパターンファイル取得は許可する。）
- □収入保険システムの利用は、各県の**NOSAIシステムを利用する県内ネットワーク**から、**SBC環境にて行う**、もしくは、**物理的、または論理的に外部のネットワークとは分離した環境を別途用意して行う**こと。

１．収入保険システム　全体概要

NOSAIシステムと収入保険システムの利用イメージ

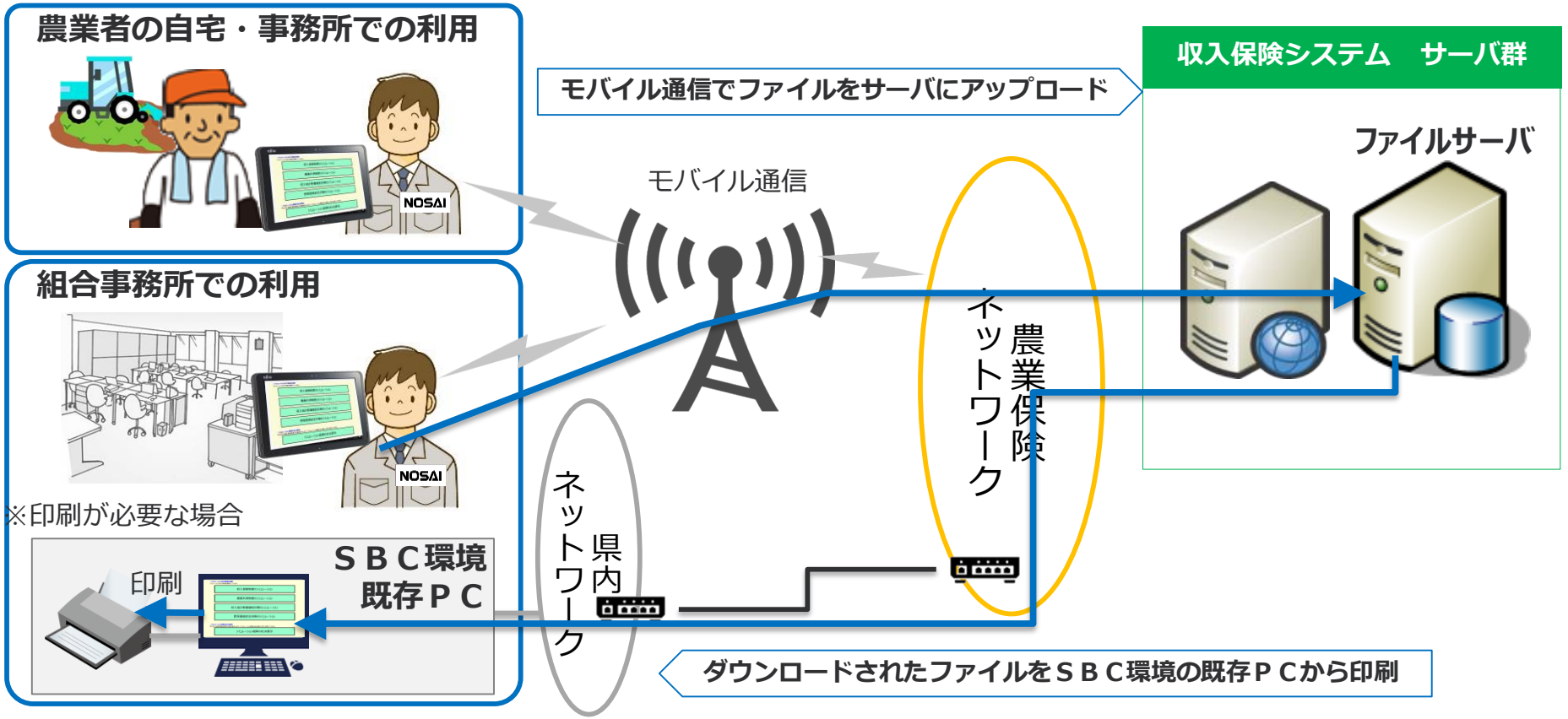


- 現行NOSAIシステム、並びに収入保険システムは、現在NOSAIでご利用のPC（ローカルPC）にあるＳＢＣ環境にて稼働が可能です。
- 両システム利用時は、ローカルPCからSBC環境にログオンします。
- 表示された仮想デスクトップ上にNOSAIシステムと収入保険システムの起動用アイコンが存在するイメージとなります。
- NOSAIのアイコンをクリックすると、従来通りNOSAIシステムが起動し、収入保険アイコンをクリックすると収入保険システムが起動されます。

- ローカルPCから収入保険システムを利用するためには、県のネットワークから農業保険ネットワークに接続する回線を用意する必要があります。（点線部）
- 現行NOSAIシステム(アクセス)は県別のシステム環境に構築されており、農業保険ネットワークを通じてNIC情報を収入保険システムに連携することを見込んでいます。（実行は任意）
- 物理的なＩＤＣ拠点は、収入保険は当初１か所を想定し、トランザクション数に合わせて拡張可能とします。

１．収入保険システム　全体概要

収入保険システムを利用するタブレットの運用方法



- □タブレットを使用する場合には、農業者宅への訪問時、組合事務所での利用ともに**モバイル通信（LTE方式）で農業保険ネットワークへ接続**する。
- □印刷が必要な場合は、タブレットで作成したファイルをファイルサーバにアップロードしたうえで、農業保険ネットワークに接続可能な**SBC環境の既存PCからダウンロードし、印刷**を行う。

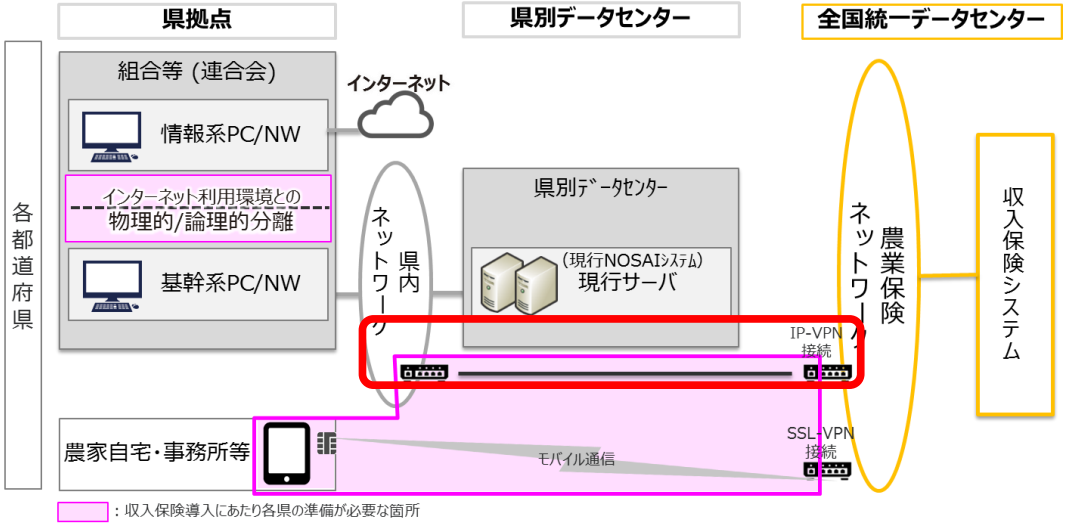
※現在、各県毎に対応中

2．ネットワーク関連

（1）各NOSAIの県内ネットワークと農業保険ネットワーク接続に関する前提条件

（ア）県内ネットワークから農業保険ネットワークに接続する際の「機能要件」

各NOSAIから収入保険システムを利用するにあたっては、既存の県内ネットワークと農業保険ネットワーク網との接続が必要となる（図中の赤枠）。その際の「機能要件」を以降に記載する。



【 機能要件】

No	要件	要求レベル	備考
1	**農業保険ネットワークに接続するための仕様に沿った回線**であること。	必須	農業保険ネットワーク全体を安定稼動させるため、収入保険システム基盤を構築するベンダーが示す「統一仕様」に基づいたネットワーク設備を用いる。
2	農業保険ネットワーク-県内ネットワーク間の**回線は2系統用意し、冗長化**すること	推奨	
3	農業保険ネットワーク-県内ネットワーク間は、**100MbpsBE以上の速度の回線**を用意すること	推奨	円滑にシステムを利用するため、100MbpsBE以上の性能を推奨する。
4	**クライアント端末（SBC環境）から収入保険システムの利用に必要な通信を可能とする**こと	必須	県内のネットワークについて、ルーティング設定、ファイアウォール設定等を変更し、クライアント端末（SBC環境）から収入保険システムへの通信を可能とすること。

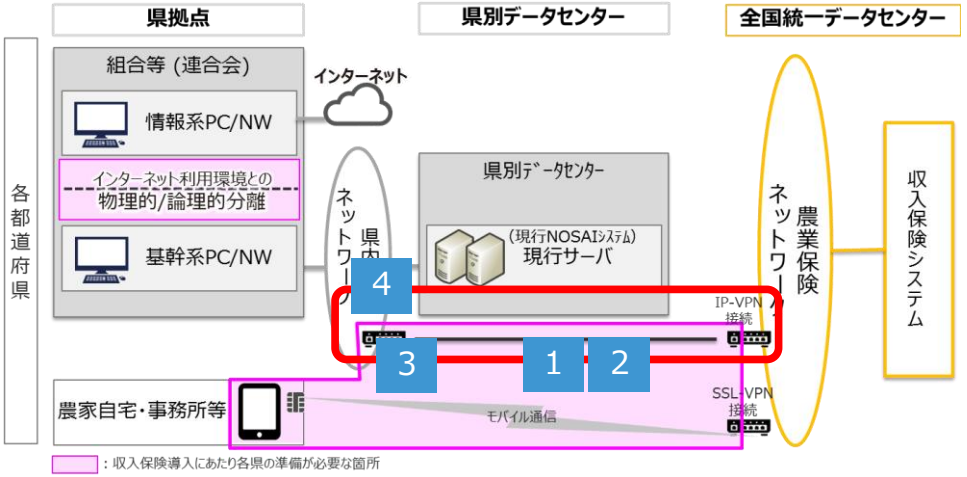
※現在、各県毎に対応中

2．ネットワーク関連

（1）各NOSAIの県内ネットワークと農業保険ネットワーク接続に関する前提条件

（イ）県内ネットワークから農業保険ネットワークに接続する際の「セキュリティ要件」

既存の県内ネットワークと農業保険ネットワーク網との接続を行う際、ネットワークに関する「セキュリティ要件」を以降に記載する。



【 セキュリティ要件】

No	要件	要求レベル	備考
1	**農業保険ネットワークに接続するための仕様に沿った回線**であること。	必須	農業保険ネットワークとの接続点で認証を行い、不正な通信が接続されることを防ぐため。
2	農業保険ネットワークに接続する回線は**専用線、または暗号化されたVPN回線とし、盗聴を防止**すること。	必須	VPN回線を利用し、閉域網接続とする。
3	農業保険ネットワークから県内ネットワークへの通信について**ファイアウォールで不要な通信をフィルタリング**すること	任意	基本的に農業保険ネットワーク側にて県内ネットワークへの不要な通信は遮断する。
4	クライアントの**セキュリティ要件を満たさない端末からは農業保険ネットワークに接続できないように設定**すること（設定方法は問わない）	必須	設定方法例：県内ネットワークにおいて 例①：ファイアウォールでの端末IPによる接続許可。 例②：収入保険接続用セグメントの追加と当該セグメントのみ許可。

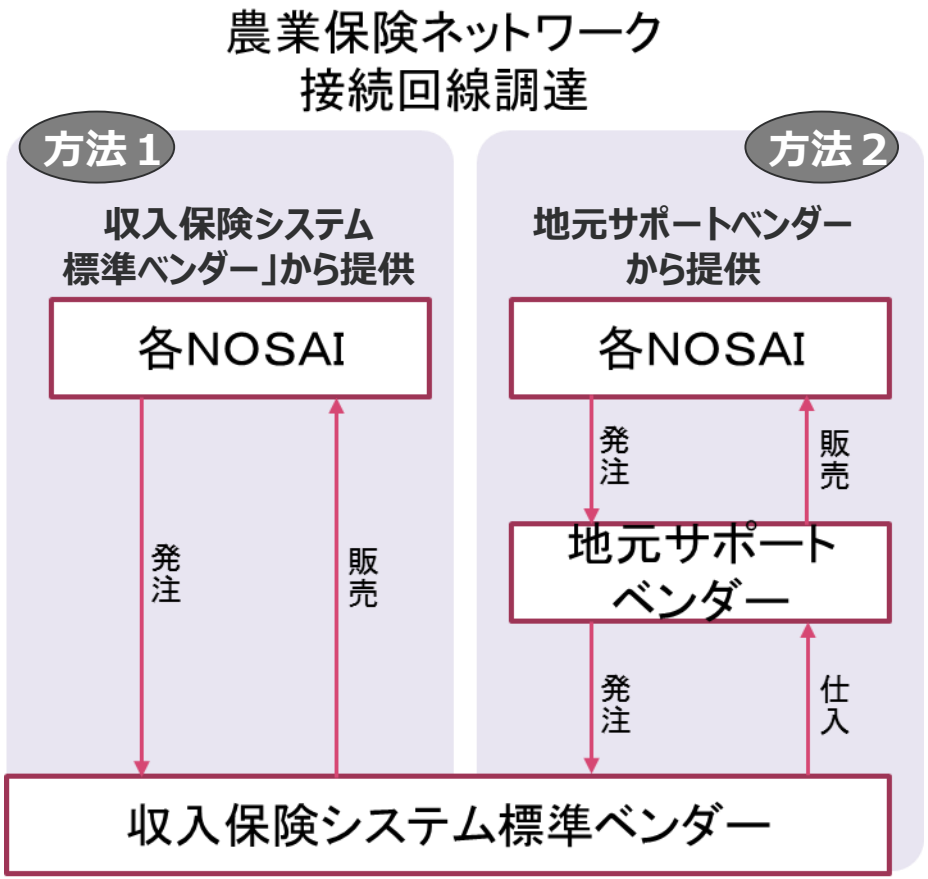
２．ネットワーク関連

※現在、各県毎に対応中

（１）各NOSAIの県内ネットワークと農業保険ネットワーク接続に関する前提条件

（ウ）各ＮＯＳＡＩにおける農業保険ネットワーク接続回線の提供について

農業保険ネットワークへの接続回線の提供は、２種類の提供方法が可能
　方法１：「収入保険システム標準ベンダー」から提供
　方法２：地元サポートベンダーから提供（収入保険システム標準ベンダーからの再販）

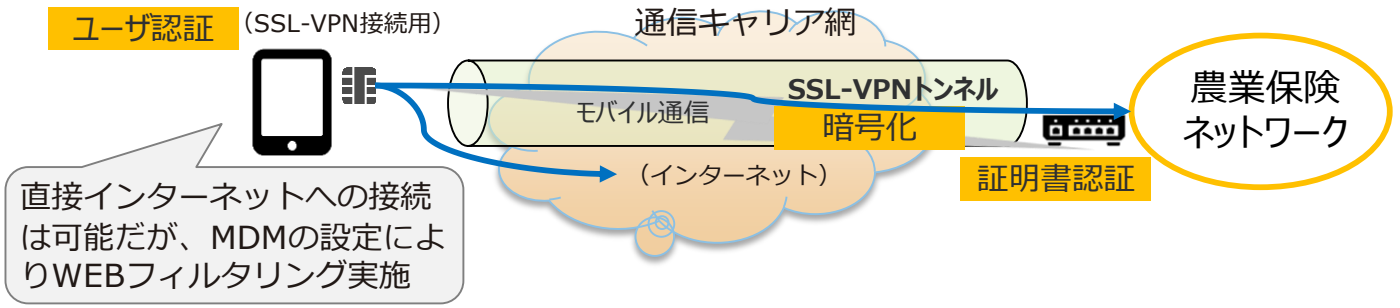


２．ネットワーク関連

（２）収入保険専用タブレットからの農業保険ネットワーク接続に関する前提条件

（ア）収入保険専用タブレットから農業保険ネットワークに接続する際の「機能要件」

収入保険専用タブレットにて収入保険システムを利用する場合は、モバイル通信による農業保険ネットワークへの接続が必要となる。その際の「機能要件」を以降に記載する。



- ✓ 通信キャリア網に接続（インターネット接続）しSSL-VPNで暗号化
- ✓ タブレットの証明書認証・ユーザ認証の2段階方式によりセキュリティ確保

【 機能要件】

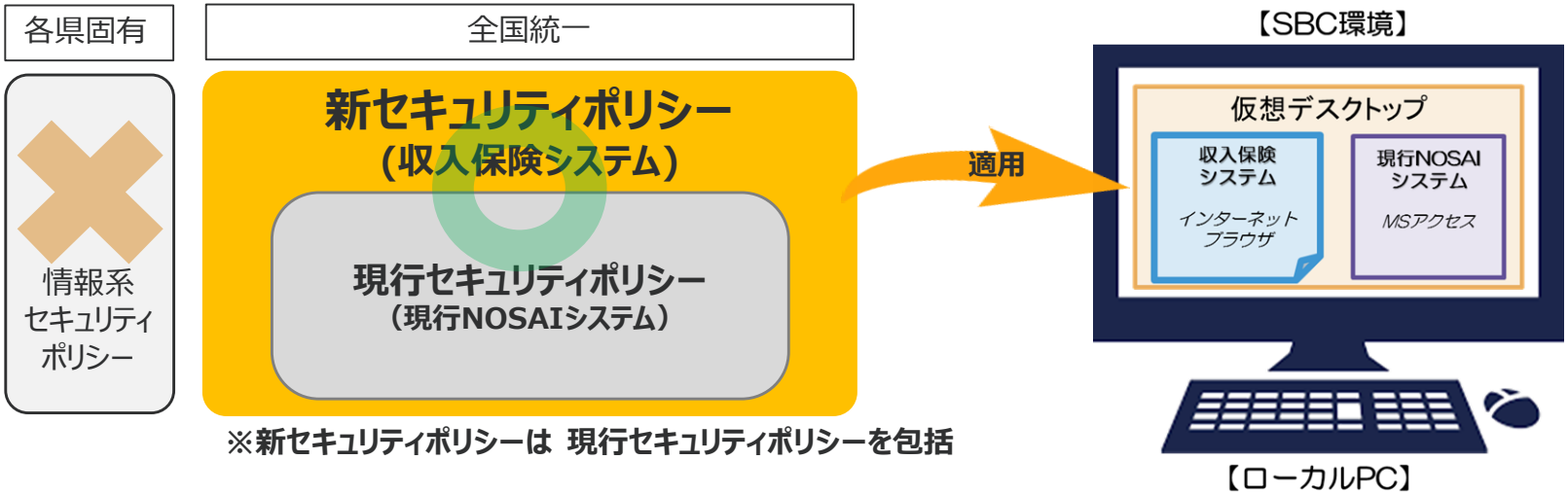
No	要件	要求レベル	備考
1	農業保険ネットワークに接続可能であること	必須	通信キャリアが提供するモバイル通信（ＬＴＥ方式）によるＳＳＬ－ＶＰＮ接続
2	農業保険ネットワークの接続について、SSL-VPN等の技術を利用して暗号化すること	必須	

3．セキュリティポリシー関連

（1） NOSAIシステム環境から収入保険システム利用する場合の考え方

収入保険システムを各県の既存PC等で利用するにあたっては、既存のNOSAIシステム用県内ネットワークと、新たな農業保険ネットワークを接続する事となる。収入保険システムは全県で利用する事から、セキュリティを担保するためのポリシーが必要となる。

- 収入保険システムに接続するローカルPCは、全国で統一された現行NOSAIシステム運用環境のセキュリティポリシー（以降、現行セキュリティポリシー）に準拠している事を前提とする。
- 現行セキュリティポリシーとは異なる、各県固有の情報系システムのセキュリティポリシー（以降、情報系セキュリティポリシー）のみに準拠したローカルPCは収入保険システムの利用は不可とする。
- また、新たに収入保険システム（WEBシステム）を前提とした新セキュリティポリシーを定める事とし、現行セキュリティポリシーを包括するものとする。
- 収入保険システムを利用するローカルPCは上記を前提とする。

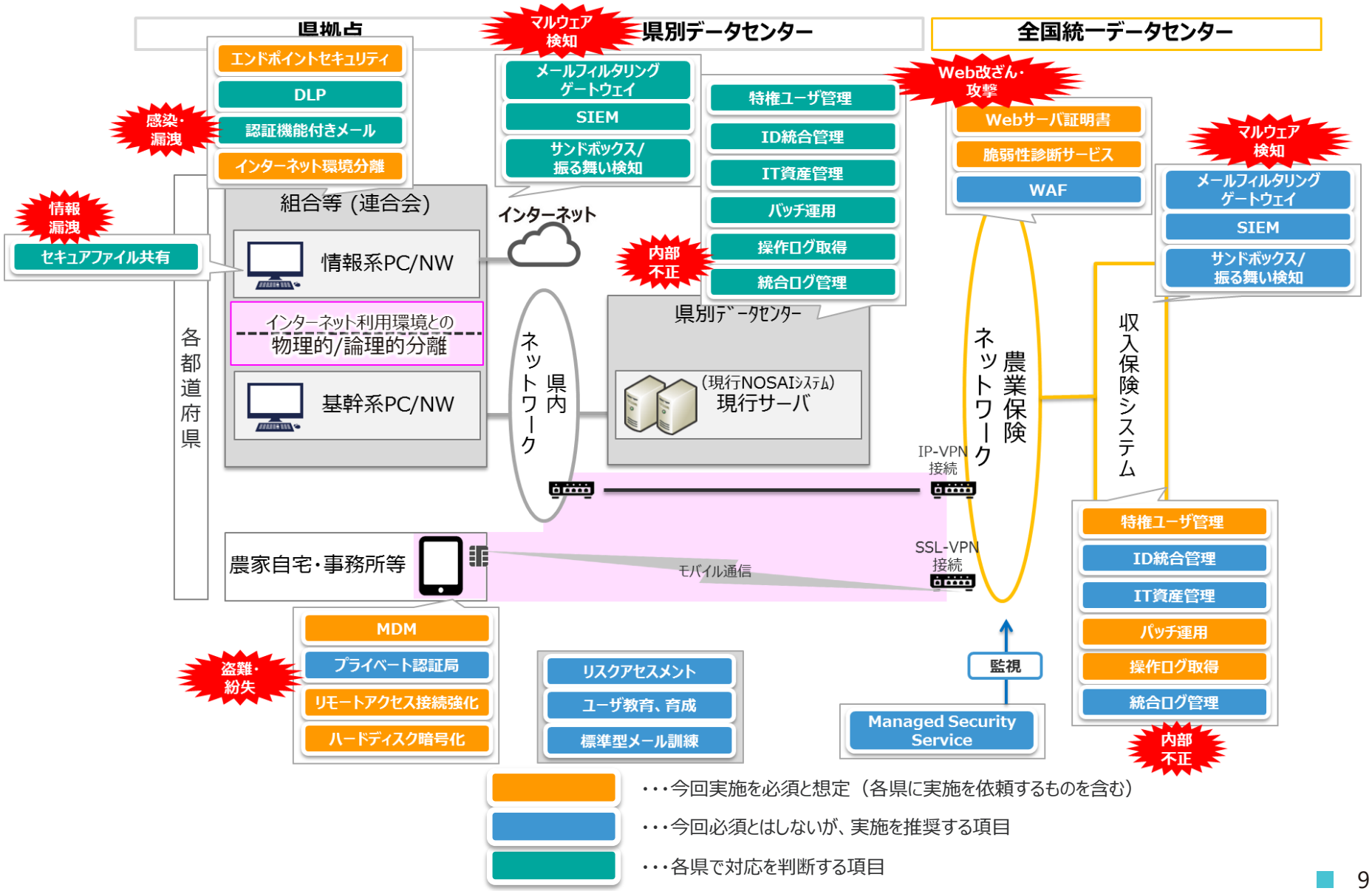


※新セキュリティポリシーは 現行セキュリティポリシーを包括

3．セキュリティポリシー関連

（2）セキュリティーポリシーの策定

（ア）各種脅威に対するセキュリティソリューション



3．セキュリティポリシー関連

（2）セキュリティーポリシーの策定

（イ）各種脅威に対するセキュリティソリューション（ソリューション概要）

それぞれのセキュリティ対策ソリューションの概要、及び収入保険システム運用に必要な対策は以下のとおり。

分類	ソリューション	ソリューション概要	必須 収入保険	必須とした理由
盗難・紛失	MDM(Mobile Device Management)	モバイル端末紛失時のロック、重要情報の遠隔消去。	○	タブレット端末を持ち出して利用する為、端末の管理は必須。
	プライベート認証局	PCやスマートデバイスの端末認証に証明書を利用、パスワード不要の管理が可能。		
	リモートアクセス接続強化	インターネット経由でのリモート接続や二要素認証などによりなりすましリスクを回避。	○	リモート接続が可能な環境を用意する為、二要素認証によりなりすましリスクを回避。
	ハードディスク暗号化	フルディスク暗号化によるPCの紛失、盗難時に情報漏洩を防ぐ。	○	タブレットの盗難・紛失に備える。
感染・漏洩	エンドポイントセキュリティ	パターンマッチング、ヒューリスティック検知などによりPCをウイルスから保護。	○	閉じられた環境下ではあるが、ウイルス対策は必須。
	DLP（情報漏洩防止ツール）	データの重要度に応じて、ユーザやファイル単位で書き込みや送信などを制限。		
	認証機能付きメール	メール送信後、認証サーバへのアクセスを必須とし相手が開封できなくなる仕組。		
	インターネット環境分離	基幹系と情報系が同一ネットワーク上にある場合、両方のネットワークを物理的、または論理的に分離し、外部サイトの閲覧が可能な情報系ネットワークにおけるマルウェアの脅威を基幹系から排除する。	○	収入保険のセキュリティポリシーとして、外部サイトへの接続がないことを必須とする。
内部不正	特権ユーザ管理	重要なシステムに対するアクセス権限強化。職務分掌、職務権限を管理、証明する。	○	全県の様々な職員がアクセスするため、個人単位でのアクセス権限管理は必須。
	ID統合管理	異動者、退職者のID削除し忘れを防ぎ、ユーザIDのアクセス権限を一元管理。		
	IT資産管理	社内にある様々なIT資産の検知、管理を行う。		
	パッチ適用	社内のIT資産に対するパッチ配布、適用を行う。	○	脆弱性対策は必須。
	操作ログ取得	ファイル操作、データベースなど重要サーバで行われた動作を取得、保管。	○	不正アクセスの抑止と把握のために必須。
	統合ログ管理	様々な製品が取得したログを一元管理、インシデントレスポンスに効果を発揮。		
組織的予防策	リスクアセスメント	企業のセキュリティに対する組織的体制、技術的体制をヒアリングし、全体の状況を可視化、対策ロードマップを提供する。		
	ユーザ教育、育成	セキュリティに関する基礎知識や専門スキルを研修や実地形式で学ぶ。		
	標的型メール訓練	疑似標的型攻撃メールを送信し開封率、開封時の初動状況チェック、教育などインシデントに備えた訓練を行う。		
マルウェア検知	SIEM	検知、対処に重きをおきクラウドデータベースと連携、標的型攻撃対策を実現する。		
	メールフィルタリングゲートウェイ	スパムメール排除、ウイルス検索、レピュテーションで怪しいメールを削除。		
	Managed Security Service	セキュリティアナリストによるネットワークの監視、アラートの通知、月次のセキュリティ報告など情報セキュリティサービス事業者によるログ分析サービス。		
	サンドボックス/振る舞い検知	仮想環境で外部から送信されたファイルやネットワーク上のパケットからマルウェアを検知したり遮断する。		
Web改ざん・攻撃	Webサーバ証明書	Webｻｲﾄ、運営組織の実在性、Webサイトとブラウザ間のSSL暗号化通信を実現。	○	キャリア網などのネットワーク経由でのアクセスがあるため、通信は暗号化を必須。
	脆弱性診断サービス	Webアプリやネットワークに脆弱性があるかをチェック、標的型攻撃に対処する。	○	閉域網での提供ではあるが、Webアプリケーションへのサイバー攻撃に備え、脆弱性診断を行う。
	WAF(Web Application Firewall)	F/W、IPSでは防げないWebサイトに対する攻撃を検知、防御する。		
情報漏洩	セキュアファイル共有	社内外の関係者間でファイルを暗号化した状態で共有、マルチデバイスで編集可能。		

これらを踏まえ、詳細は別途定める。

3．セキュリティポリシー関連

（3） NOSAIシステム環境における外部接続要件

【参考】次期農業共済ネットワーク化情報システムの開発等に関する基本設計書（第２版）より

６．外部接続要件

（１）外部接続の種類

農業共済ネットワーク化情報システムとして考慮すべき外部接続は、以下のとおりとする。

①標準システムに関連する外部接続

(ア)インターネット接続が無いネットワークへの接続

農林水産省（再保険システム）

(イ)自らのインターネット接続（別セグメントを経由する場合も含む）

Windows Updateやウィルス対策ソフトのパターンファイルの取得、NTPサーバ接続

(ウ)インターネット接続が存在するネットワークへの接続

情報系ＬＡＮ（業務系ＬＡＮとは本来切り離されるべき、グループウェア、メール、ブラウザなどを利用するＬＡＮ）などへの接続

②直接連携が無いまたは接続形態が不明な外部接続

(ア)金融機関への口座振込関連のシステム

(イ)その他、関係団体等への接続

（２）セキュリティ要件

前記(1)の①の(ア)「農林水産省（再保険システム）」については、ISDNによるクローズされたネットワークへの接続のため、不正監視は必須とはしない。

前記(1)の①の(イ)「自らのインターネット接続」の場合は、ファイアウォールによる通信制御を行い、外部からの不正アクセスを防止する必要がある。

前記(1)の①の(ウ)「情報系LAN」への接続の場合は、上記(1)の①の(イ)の対策に加え、「情報系LAN」側の端末を含めて情報漏洩対策（データの持ち出し制御やファイル操作ログ取得等）が必須となる。

なお、前記(1)の② 直接連携が無いまたは接続形態が不明な外部接続については、標準システムとの接続があり且つインターネット接続やデータ持ち出しの可能性がある場合に、上記(1)の①の(イ)の対策、上記(1)の①の(ウ)の対策が必要となる。

※「４．セキュリティ要件」「５．ネットワーク要件」もあわせてご確認ください

３．セキュリティポリシー関連

（４） NOSAIシステム環境から収入保険システム利用にあたっての前提条件の整理

NOSAIシステムにおける外部接続要件、及び、収入保険システムのセキュリティポリシーから、NOSAIシステム環境（基幹系SBC環境）で収入保険システムを利用するには、以下の通り「**基幹系SBC環境とインターネット利用環境との物理的、又は倫理的分離**」が必要となる。

① 基幹系SBC環境からのインターネット接続は、環境維持に必要な「特定のサイト」を除き利用不可であること。（「特定のサイト」とは、前頁で掲載した「Windows Updateやウィルス対策ソフトのパターンファイルの取得、NTPサーバ接続」等であり、NOSAIシステムにおける外部接続要件を満たすことが前提となる）

② 基幹系SBC環境は、以下の何れかによりインターネット利用環境（Web閲覧やメールの利用環境）と分離し、セキュリティを担保すること。

- **【物理分離】**基幹系SBC環境は、インターネット利用環境とは異なる物理的設備（ネットワーク設備、ローカルPC等）にて構築されていること。
- **【論理分離】**同一クライアントにより基幹系SBC環境、インターネット利用環境を利用する場合、(ア)サーバ環境にてネットワーク機器等により基幹系SBC環境とインターネット利用環境を分離されていること。（イ）クライアント環境では、画面転送方式によりローカルのクライアント環境と基幹系SBC環境を分離されていること。

③ 基幹系SBC環境とインターネット利用環境間でデータ授受等を行う場合は、 **無害化通信等のセキュアな仕組み**により実施すること。

④ 情報系と基幹系の端末を共有する場合は、**情報系端末を含めた情報漏洩対策を行っていること**。

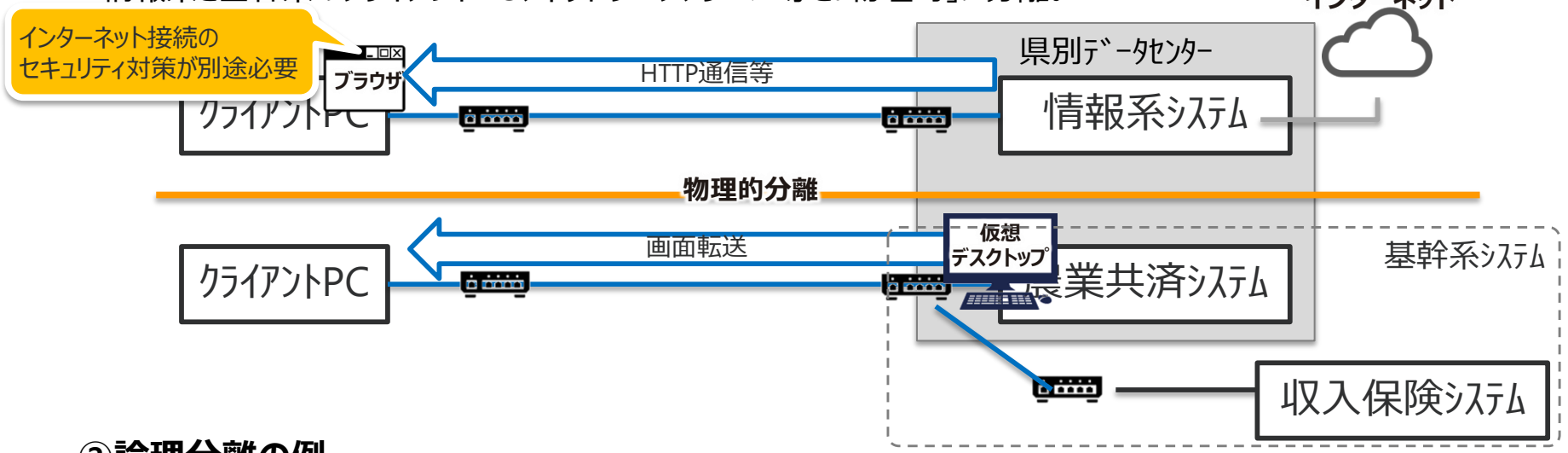
3．セキュリティポリシー関連

（4） NOSAIシステム環境から収入保険システム利用にあたっての前提条件の整理

インターネット環境の分離の方法（例）

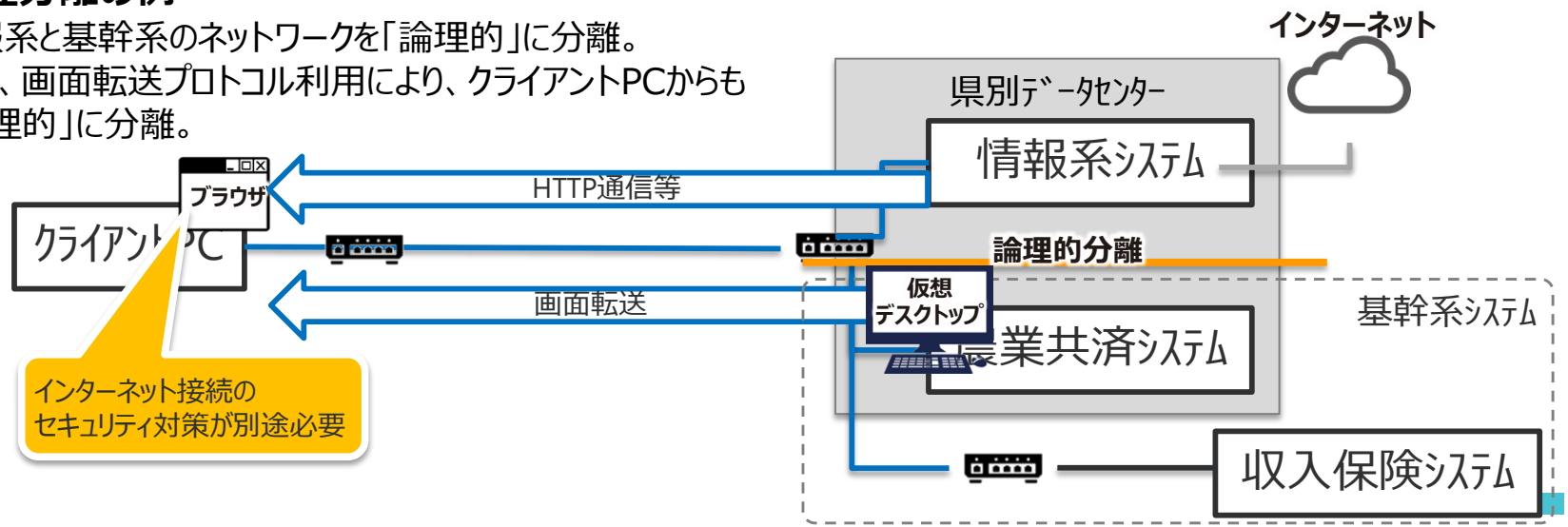
①物理分離の例

情報系と基幹系のクライアントPC、ネットワーク、サーバ等を「物理的」に分離。



②論理分離の例

情報系と基幹系のネットワークを「論理的」に分離。
及び、画面転送プロトコル利用により、クライアントPCからも「論理的」に分離。



3．セキュリティポリシー関連

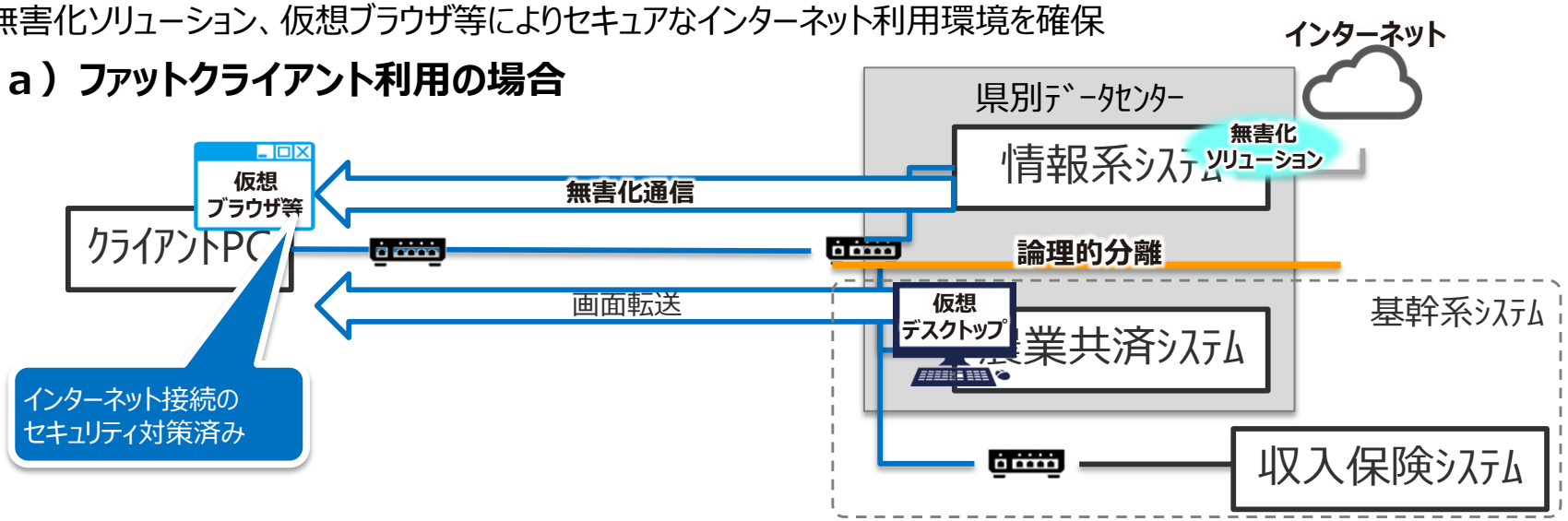
（4） NOSAIシステム環境から収入保険システム利用にあたっての前提条件の整理

インターネット環境の分離の方法（例）

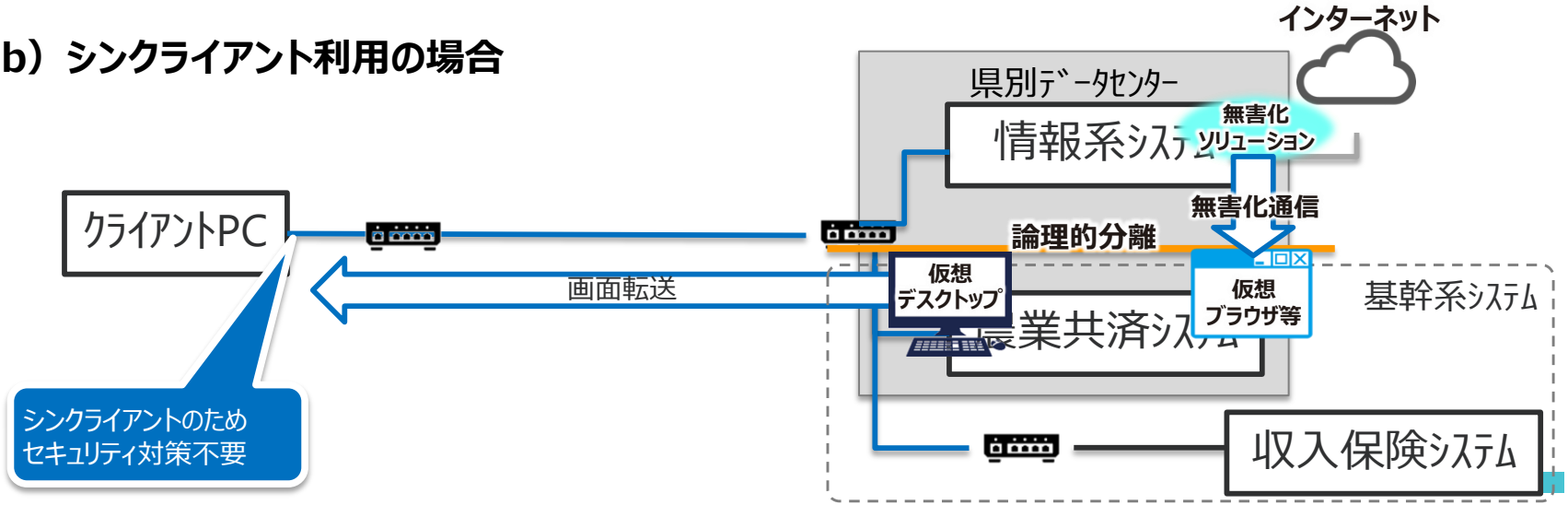
③インターネット無害化の例

無害化ソリューション、仮想ブラウザ等によりセキュアなインターネット利用環境を確保

a）ファットクライアント利用の場合



b）シンクライアント利用の場合



3．セキュリティポリシー関連
（5）セキュリティーポリシー（クライアント要件）

（ウ）収入保険システム側で求める県側のクライアント要件

1．システム要件

- ◻クライアントOS（Windows 7, 10）
  ※収入保険用タブレット以外のPCによるシステム利用は、各県のSBC環境（ Windows Server 2008 R2，2012）からの利用が前提。
- ◻ブラウザ（IE11）
- ◻PDF Viewerが利用可能であること。（動作確認はAdobe PDF Reader DCで実施）
- ◻zipファイルを解凍できること。

2．セキュリティ要件

- ◻ウィルス対策ソフトがインストールされており、マルウェア対策が行われていること。
- ◻インターネットに接続されていないこと。
- ◻OS、ブラウザ、ソフトウェアのアップデートが行われており、既知のセキュリティホールが存在しないこと。
- ◻データの外部への持ち出しが制限されていること。（システム的な制限というより運用ルールが定められているレベル）
- ◻ユーザを職員間で共用していないこと。
- ◻ユーザのパスワードが設定／管理されていること。
- ◻外部持ち出し可能な端末でないこと。（収入保険用タブレットを除く）
- ◻クライアント上での不正操作を防止するため、クライアントの操作記録機能やUSB等のデバイス制御機能を持ったクライアント運用管理ソフトウェアを導入すること。（推奨）

4．タブレット仕様

富士通　Q508/SB　OS:Windows10　（画面サイズ 10.1型）			
外形寸法(W×D)	263.4×169.1 mm	外形寸法(H)	11.3mm
質量(本体)	599g	質量(キーボード込)	989g
画面サイズ・解像度	10.1型高輝度(WUXGA)	CPU	Atom x5-Z8550(1.44GHz)/ Atom x7-Z8750(1.60GHz)
インターフェース	USB×2(Type-A×1、 Type-C(映像出力兼用)×1)/ μSD/Audio	ペン	電池不要 本体に収納可能
バッテリー駆動時間	12.0h	充電時間	4.0h
防水・防塵	IPX5/7/8、IP5X	堅牢性	76cm落下/MIL(122cm)対応 その他耐久試験(振動 etc)
外観			

用語集

1	VPN	Virtual Private Networkの略。インターネット上の拠点間を専用線のように接続して、のぞき見や改ざんなどの不正アクセスを防ぎ、安全な通信を可能にする技術。パブリックネットワークを使って、仮想的にプライベートネットワークを実現する。VPNを使えば、インターネットなどを経由しているにもかかわらず、あたかも同一ネットワーク上にいるかのような利便性と安全性が得られる。
2	SSL-VPN	Secure Sockets Layer virtual private networkの略。SSL-VPNは、リモートアクセス端末と企業イントラネット側のVPN装置間でSSL暗号通信を行うことによりVPNを構築する。SSL機能は、WEBブラウザやグループウェアにあらかじめ搭載されているため、専用ソフトのインストールの必要がなく、使用可能機器の範囲も広くなっている。また、特別な環境設定を行う必要がない。
3	LTE	Long Term Evolutionの略。携帯電話通信規格のひとつで、第3世代携帯の通信規格（3G）をさらに高速化し「長期的に進化」（Long Term Evolution）させたもので、将来的に登場する4Gへのスムーズな移行を目指すもの。そのため、一般的には「3.9G」と呼ばれている。
4	SBC	Server Based Computingの略。クライアントのアプリケーションを管理サーバーに集中させ、システム管理者が一括して管理を行う仕組みのこと。
5	Webフィルタリング	Webフィルタリング（URLフィルタリング）とは、アダルトサイトや薬物・犯罪に関するWebサイトなどのように、職務上または教育上、閲覧することが不適切なインターネット上のWebサイトをフィルタリングし、ユーザーに見せなくすること。 Webフィルタリングが世に出始めた当時は、Webフィルタリングはまだ「業務効率化のための製品」と認識されていたが、職務上不適切なWebサイト以外にも、SNSや危険性のあるWebサイトへアクセスさせなくすることで、故意や不用意な情報漏洩を防ぐ「セキュリティ製品」としてWebフィルタリングは進化している。
6	MDM	Mobile Device Managementの略。統一したポリシーの下に遠隔から複数の端末を一元管理する。搭載する機能は「（1）紛失・盗難時の情報漏えい対策、（2）不正利用の防止、（3）端末情報の収集とポリシー一斉適用等による管理の効率化」の3つに分けることができる。
7	マルウェア	悪意のあるソフトウェアをマルウェア（malware＝malicious【悪意がある】とsoftware【ソフトウェア】を組み合わせた造語）と呼ぶ。ウイルスもマルウェアの一種である。
8	セキュリティホール	コンピュータのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のこと。セキュリティホールが残された状態でコンピュータを利用していると、ハッキングに利用されたり、ウイルスに感染したりする危険性がある。
9	リモートロック	携帯電話やスマートフォンなどのモバイル端末を通信回線を用いて遠隔操作し、端末が不正な操作を受け付けないように設定できる機能やサービスのこと。端末を紛失したり盗難に遭った場合などに、他人に端末を操作されることを防ぐ目的で用いられる。
10	リモートワイプ	携帯電話やスマートフォンなどのモバイル端末を遠隔地から操作し、端末に保存されているデータを削除する機能およびサービスのこと。リモートワイプを実行すると、モバイル端末に保存されたデータは消去され、端末を操作しても情報を得ることができなくなる。
11	100MbpsBE	BEはベストエフォートのこと。ベストエフォートとは、性能に関して明示的な保証をせずに、最大限（ベスト）の努力（エフォート）サービスを提供するという形態。 100MbpsBEであれば、1秒当たり100Mbitのデータ量を通信できるように最大限の努力サービスを提供するということ。
12	ルーティング	経路制御（けいろせいぎょ）。データを目的地まで送信するために、コンピュータネットワーク上のデータ配送経路を決定する制御の事。
13	IDC	Internet Data Centerの略。データセンターとは、企業からデータやサーバーを預かり管理・運用などを行う拠点のこと。安全な環境のもとで管理することで、企業はシステムを安定的に運用し続けることができる。
14	セグメント	セグメントとは、もともとは「全体を分割したうちのひとつ」といった意味合いを持つ英語。LANのネットワークを構成する範囲の単位で、リピータハブやスイッチングハブで区切られる範囲を指している。
15	証明書認証	システムやサービス、メールを利用するユーザのデバイスに証明書をインストールし、そのユーザが正規の利用者であることを認証する仕組み。
16	閉域網	閉域網とは、インターネットなどに直接は繋がれておらず、限られた利用者や地点の間のみを接続する広域通信ネットワークのこと。 通信事業者の内部ネットワークなどとして構築されるもので、事業者自身の通信需要のために利用されるほか、VPNサービスなどの形で企業内ネットワークの拠点間接続などに用いられる。
17	SIM	スマートフォンや携帯電話、タブレットなどのモバイル端末でデータ通信や音声通話などを行うために必要なICチップカードのこと。3GやLTEといった電波を使ってデータ通信や音声通話するには、このSIMカードがなくてはならない。SIMカードには電話番号など契約者情報が記録されており、利用者を特定する役割も果たしている。
18	閉域SIM	インターネットではなく閉域ネットワークに接続する SIM のソリューション。閉域 SIMを使用することで、インターネットを介さずに業務システム等に安全に接続することができる。