（議決事項）

統合ネットワークの調達について

区　分	議　決	対象範囲	法人全体

エグゼクティブサマリー

現行システムの運用保守期間満了に伴う新システムの調達について議決をお願いするもの。

バックグランド

第10回経営委員会にて報告のシステム更改に係る基本方針に基づき新システムの調達を実施する。更改案の内部説明会を実施後、要望等を収集し、調達仕様書案等を作成。情報システム委員会にて審議了承された。

戦略プラン

当初方針に基づき、NWシステムの運用保守期間を延長（契約済）し、GPDRシステムと一体的に更改する。2019年4月に契約手続きを完了させ、直ちに設計・構築を開始し、2020年1月の本番稼働を目指す。完全物理分離環境に伴う課題を解消し、業務の非効率性を極力解消するとともに、統合により生じるセキュリティリスクを回避する追加的なセキュリティ対策を実装する。

予算及び予算計画への影響

当中期計画におけるシステム関連予算の残額約41億円に対し、設計構築及び初期運用保守経費に係る費用として41億円程度と想定。加えて次期中期計画において、総額14億円程度の予算措置を要する。

便益及びリスク

【期待効果】
・機能間の連携強化（ファイル共有機能と、電子会議システム及びEメール機能等のシームレスな連携等）
・1端末で全機能の利用が可能
・ハードウェア等のリソース共有可能
・リモート接続機能により、執務室内外で同等の環境利用が可能
・一貫したシステム運用、セキュリティ管理が可能

【発生する可能性があるリスク】
・認証情報漏えい等による機密情報保存領域への不正アクセス
・ハードウェア障害時の影響範囲拡大
・ファイル転送機能を利用した内部ネットワークへのマルウェア感染
・端末の紛失・盗難による情報漏えい

【リスクへの対応】
・二要素認証(パスワード＋証明書)による不正ID利用防止
・正副二系統構成による耐障害性の向上
・マルウェアによるインターネット上の悪意あるホストとの通信を阻止
・内部にデータを保持しないシンクライアント端末を導入

〇完全物理分離により実現不可能であった機能を実現し、業務の非効率性を極力解消
⇒【インターネットに接続する外部ネットワーク】であるＮＷシステムと、【機密情報を扱う内部ネットワーク】であるＧＰＤＲシステムを【統合ネットワーク】として再構築。

〇統合により高まる可能性のあるセキュリティリスクを回避すべく、従来のセキュリティ対策に加え新たな対策を導入

	解消する課題及び実現を図る要望等	統合による期待効果	新たに発生する可能性のあるリスク	リスクへの対応
1	異なる環境上で提供される機能間での連携ができない。 （例）メールで受信した機密情報の保存には手動でのファイル転送が必要。	全ての機能を単一環境に集約することにより、機能間の連携を容易にする。	機能間の連携やファイル転送経路を利用し、内部ネットワークにマルウェア等が侵入するリスク。	内部ネットワークにインターネット経由のデータを格納する際は、安全性検証後に転送。仮にマルウェアに感染した場合も、インターネット上の悪意あるホストとの通信阻止により、情報漏洩を防止。
2	ファイルの転送に外部媒体を介す必要がある。	オンラインでのファイル転送が可能となる。	ファイルの転送経路を利用し、内部ネットワークにマルウェア等が侵入するリスク。	内外ネットワークを直接接続せずファイル転送可能な仕組みを導入し、外部ネットワークに侵入したマルウェアの、内部ネットワークへの拡散を防止。
3	利用する機能により、端末（ネットワーク）の切替が必要。	１つの端末(ネットワーク)で全ての機能が利用可能。	クライアント端末障害時、全ての機能が利用不可となるリスク。	端末上にデータを残さないシンクライアント端末の導入により、どの端末でも同一のデスクトップ環境にアクセスすることを可能とする。
4	ハードウェア及びソフトウェアのリソース共有が出来ない。	単一環境に統合することでハードウェア及びソフトウェアのリソースが共有可能。	ハードウェア障害による影響が広範に及ぶリスク。	冗長化構成により耐障害性の向上を図る。
5	ネットワーク毎にID及びパスワード管理が必要となる。	統合により、内外共通のID利用が可能となる。	ユーザーのID及びパスワード等認証情報が漏洩した場合、機密情報を有する内部ネットワークへ不正アクセスされるリスク。	不正端末接続防止機能、リモート接続時の二要素認証等、複数の機能により不正ID利用を防止。
6	インターネットを介したリモート接続では機密情報利用環境へのアクセスが不能なため、将来的なテレワークを含む働き方改革に対応できない。	リモート接続機能により、執務室内と同等の利用環境が提供可能となる。	リモート接続に利用する回線経由での不正アクセス等のリスク。 端末紛失等による機密情報の漏洩リスク。	アクセス回線を外部ネットワークに設け、画面転送により内部ネットワークの機能を利用することで、不正アクセスから内部ネットワークを保護。 内部に情報を保持しないシンクライアント端末の導入により、端末からの情報漏洩リスクを排除。
7	内部ネットワークに通信機能がなく、職員間であっても、機密情報の送受信には外部ネットワークのメール機能を利用する必要がある。	全ての機能を内部ネットワークに集約することにより、メール及びチャット機能上で機密情報の利用が可能。	-	-
8	完全物理分離により、セキュリティ管理が二重管理され、セキュリティ管理負荷が高い。	統合により、セキュリティ管理も統合され、より一体的なセキュリティ管理が可能となる。	-	-
9	重要情報を格納するファイルサーバのバックアップサイトがないため、業務継続性に係る課題がある。	環境毎にバックアップサイトを構築する必要がなくなるため、センター運用の効率性を損なうことなく業務継続性を確保可能。	業務継続計画の見直し等、バックアップサイトに求める要件の変更に迅速に対応できないリスク。	バックアップサイトにクラウド環境を利用することにより、対象業務、利用機能及びユーザー数等の要件変更にも柔軟、迅速に対応可能な構成とする。
10	iPadとWindows端末を使い分ける必要があるため、機能や操作方法に差分が生じ、混乱を招く。	ノート型Windows端末に一元化することにより、常に同一の機能を同一の操作により利用可能。	-	-

年金積立金管理運用独立行政法人
統合ネットワークシステムの調達について

年金積立金管理運用独立行政法人

統合ネットワークシステムの概要

01
統合ネットワークシステムの概要

■システム統合

【インターネットに接続する外部ネットワーク】であるＮＷシステムと、【機密情報を扱う内部ネットワーク】であるＧＰＤＲシステムを、その位置付けを維持したまま内包する【統合ネットワーク】として再構築。

なお、ＧＰＤＲデータベース及びアプリケーションは変更を加えず、統合ネットワーク上で継続利用。

■統合によるユーザビリティの向上とこれに伴うセキュリティ対策の強化

- 統合により、内外端末の切り替えをすることなく、全サービス1台の端末からの利用が可能。
- ファイルサーバ、メール及びグループウェア等、機密情報を含むファイル・データを保持するサービスを内部ネットワークに集約。これにより、各サービス間の連携が強化されるとともに、ユーザーが意識することなくインターネット上の脅威から機密情報を保護。
- 内外ネットワーク間のファイル転送のため、両ネットワークが同時かつ直接接続されないセキュアファイル交換機能を介した自動転送機能を実装。これにより、ユーザーの利便性を損なうことなく、内部ネットワークとインターネット上の悪意あるホストとのセッション確立を阻止し、マルウェア感染時も情報漏洩を阻止。
- 受信メールは外部ネットワークで検証し、安全が確認されたメールのみ内部ネットワークへ転送。これにより、標的型攻撃等の脅威から内部ネットワークを保護。

現在、経営委員においてはＮＷシステムにて提供するサービスのみ利用可能ですが、本対応により、利用可能サービスの役職員との差分は解消されます。
同一のセキュリティ対策が実装された環境にて、より緊密な情報共有が可能となります。

01
統合ネットワークシステムの概要

■その他改善ポイント

- クライアントＯＳの仮想化により、端末とユーザーの関連性を排除。これにより、どのユーザーがどの端末を使用しても、常に同一のデスクトップ環境を利用可能。また、端末でデータを保持しないため、端末の紛失・盗難による情報漏洩の可能性を排除。

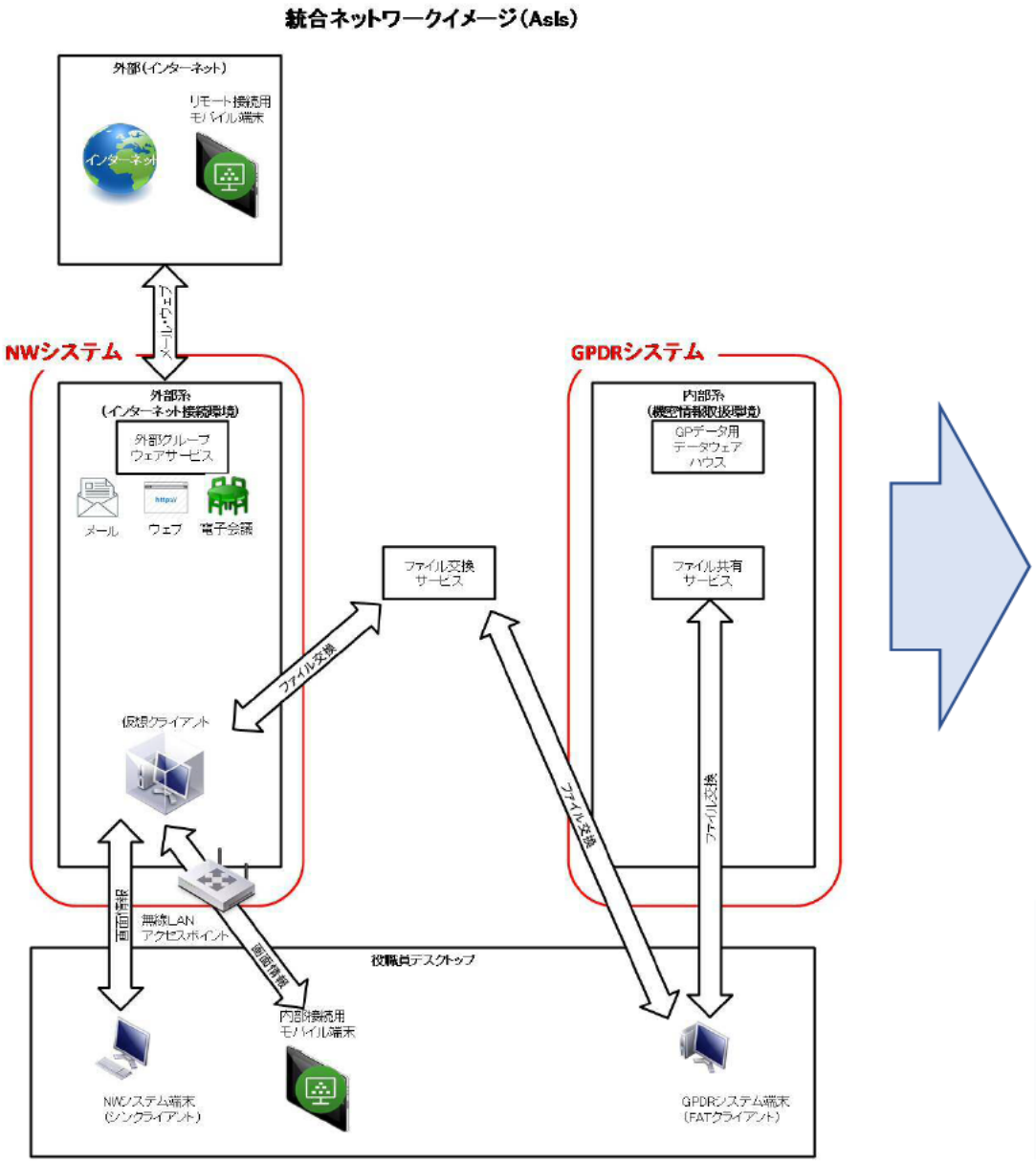
  仮想ＯＳへ接続する端末は、軽量ノート型シンクライアント端末となります。接続先は事務処理用ＰＣとして一般的に利用されるWindows環境のため、日本語入力を含め、違和感なく利用頂けます。また、データは全てサーバ側で保持するため、法人事務所来訪時は、貸与端末を持ち込むことなく、事務所側で準備する端末を利用可能です。

- 内部ネットワークに無線アクセスポイントを設けることにより、オフィス全域でのシステム利用が可能。
- インターネットを介したリモート接続に対応。端末認証・暗号化通信により、オフィス外からも安全にシステム利用が可能。

  オフィス内外を問わず、役職員と同一の環境にアクセス可能です。

- バックアップサイトとしてクラウド環境を活用。コスト削減を図りつつ、被災時等における縮退業務環境立ち上げの迅速性を確保。また、業務継続計画及びこれに基づく情報システム運用継続計画の変更にも、柔軟に対応可能。
- 次世代ファイアーウォール、ＩＰＳ及びＳＯＣサービス、ＳＩＥＭ機能、アンチウィルス等による多層防御環境を構築。法人の情報資産に対するリスクを可能な限り低減させます。

02
ネットワーク現新比較



個別機能詳細

統合ネットワークシステム個別機能詳細

インターネットに接続する「外部ネットワーク」と機密情報を扱う「内部ネットワーク」という位置づけを維持したまま、NWシステムとGPDRシステムの機能を統合。

- GPDRシステム、文書管理システムアプリケーションには変更を加えず、内部ネットワーク上で利用。
- ファイルサーバを内部ネットワークに一元化。
- メールとグループウエアをファイルサーバが有る内部ネットワークで運用
- 内部ネットワークと外部ネットワーク間のファイル転送を自動化

統合ネットワーク全体図

１．統合ネットワークのデスクトップ端末利用イメージ

ノート型シンクライアント端末1台とする（NWシステム端末とGPDRシステム端末の統合）。
画面切替ではなく、内部ネットワークのデスクトップ上のウィンドウに、外部ネットワークのアプリケーションを表示する（アプリケーションの統合）。
大型サブディスプレイ1台を配備し、作業領域を拡張する（事務処理の効率化）。
従来利用しているタブレット端末は、当面の間ペーパーレス会議システムで利用継続する（既存機器の有効利用）。

2．統合ネットワークにおける内外分離の考え方

統合ネットワークではインターネットに接続された「外部ネットワーク」と、機密情報を取り扱う業務システムネットワーク「内部ネットワーク」とを物理的に分離する構成とする。

インターネット

画面転送プロトコルのみ許可

外部ネットワークと内部ネットワークは物理的に接続されていない
設定したタイミングでスイッチされファイル交換される

専用線

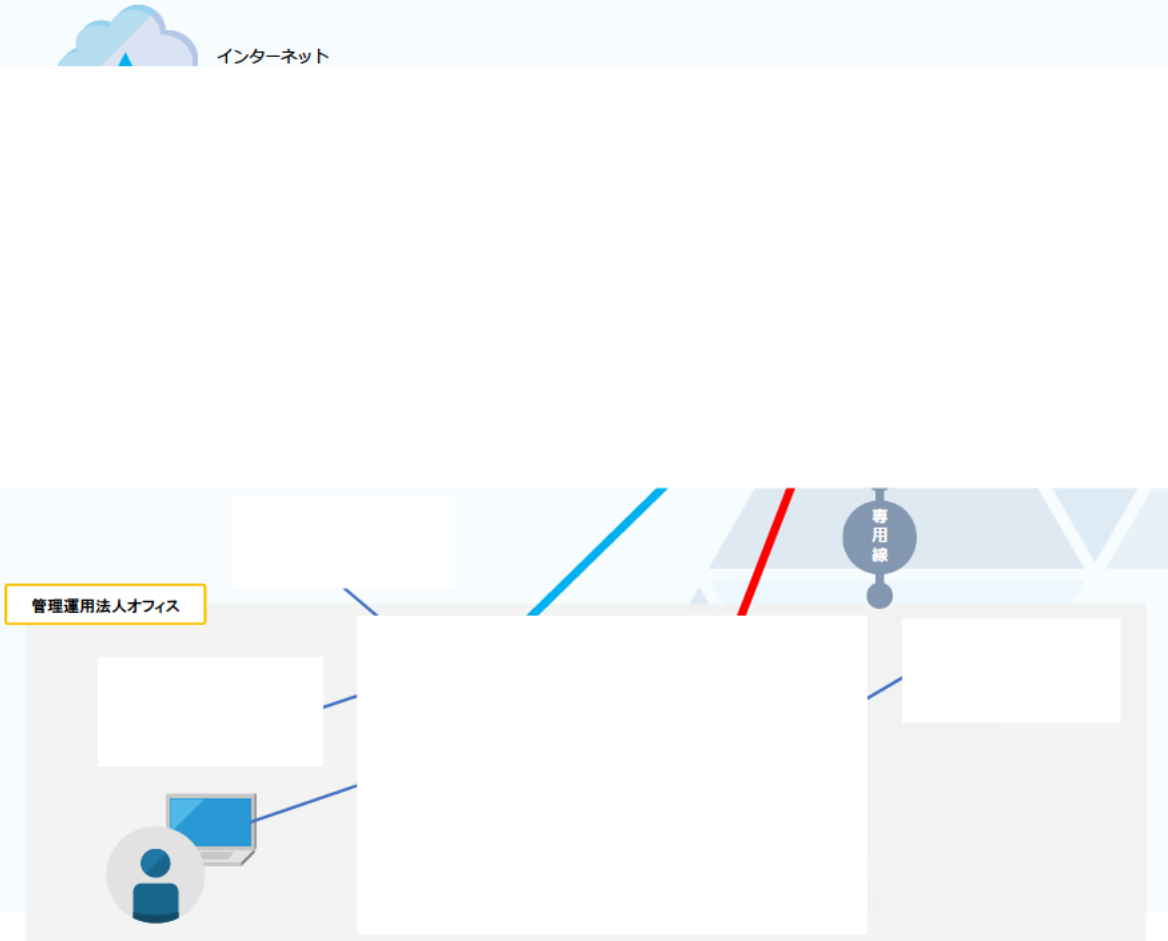
管理運用法人オフィス

インターネット接続の流れ

メール等、ファイルの流れ

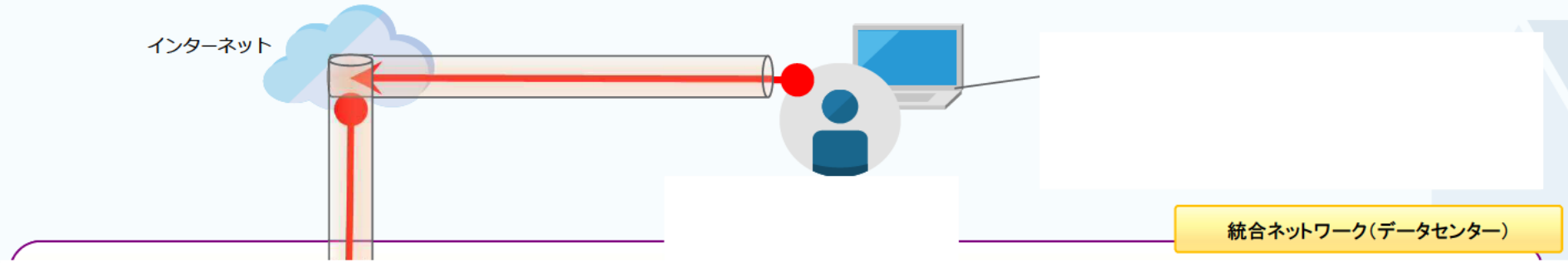
3．仮想デスクトップ構成

統合ネットワークでは「外部ネットワーク」と「内部ネットワーク」の分離を行っている。セキュリティを担保しつつ、ユーザの利便性を確保するために以下の施策を導入する。
業務に必要な機能は内部ネットワークに実装し、外部ネットワークに実装する機能はインターネットアクセス（Web閲覧）のみとすることで、内部ネットワークのセキュリティを確保する。外部ネットワーク上のインターネットアクセス（Web閲覧）は、内部ネットワークのデスクトップ上に画面情報のみを表示する。

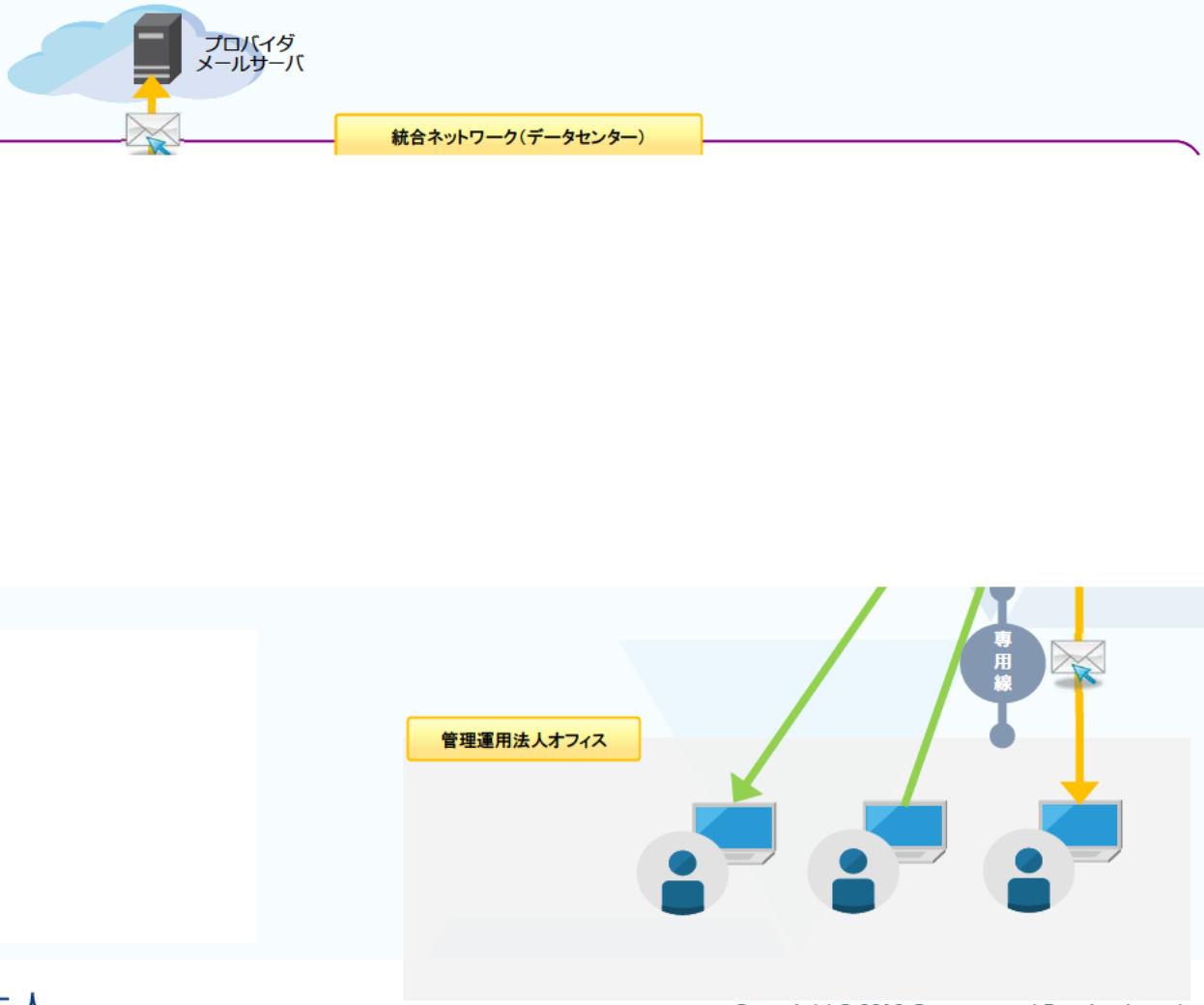


４．リモートアクセスVPN

統合ネットワークでは、管理運用法人オフィスにおいても管理運用法人オフィス外においても、可能な限り同様な執務環境を提供するために、仮想デスクトップを導入する。
業務に必要な機能は内部ネットワークに実装する為、セキュリティを確保した上で内部ネットワークへアクセスする必要があり、アクセス方法は「リモートアクセス[redacted]」を想定している。



5．メール構成



６．バックアップ

統合ネットワーク上で取得されたバックアップデータ[redacted]は、クラウド環境へ保管する。

【クラウド化の期待効果】

- 環境構築が早い。
- 環境拡張性が高い。
- 災害発生時等の復旧が早い。
- オンプレミスに比べ導入費用、運用費用を抑えることができる。

７．リカバリ

統合ネットワークが何らかの外的要因により利用できなくなった場合に、クラウド環境上で最小限業務が行えるように、クラウド環境をバックアップデータセンターとして構成する。

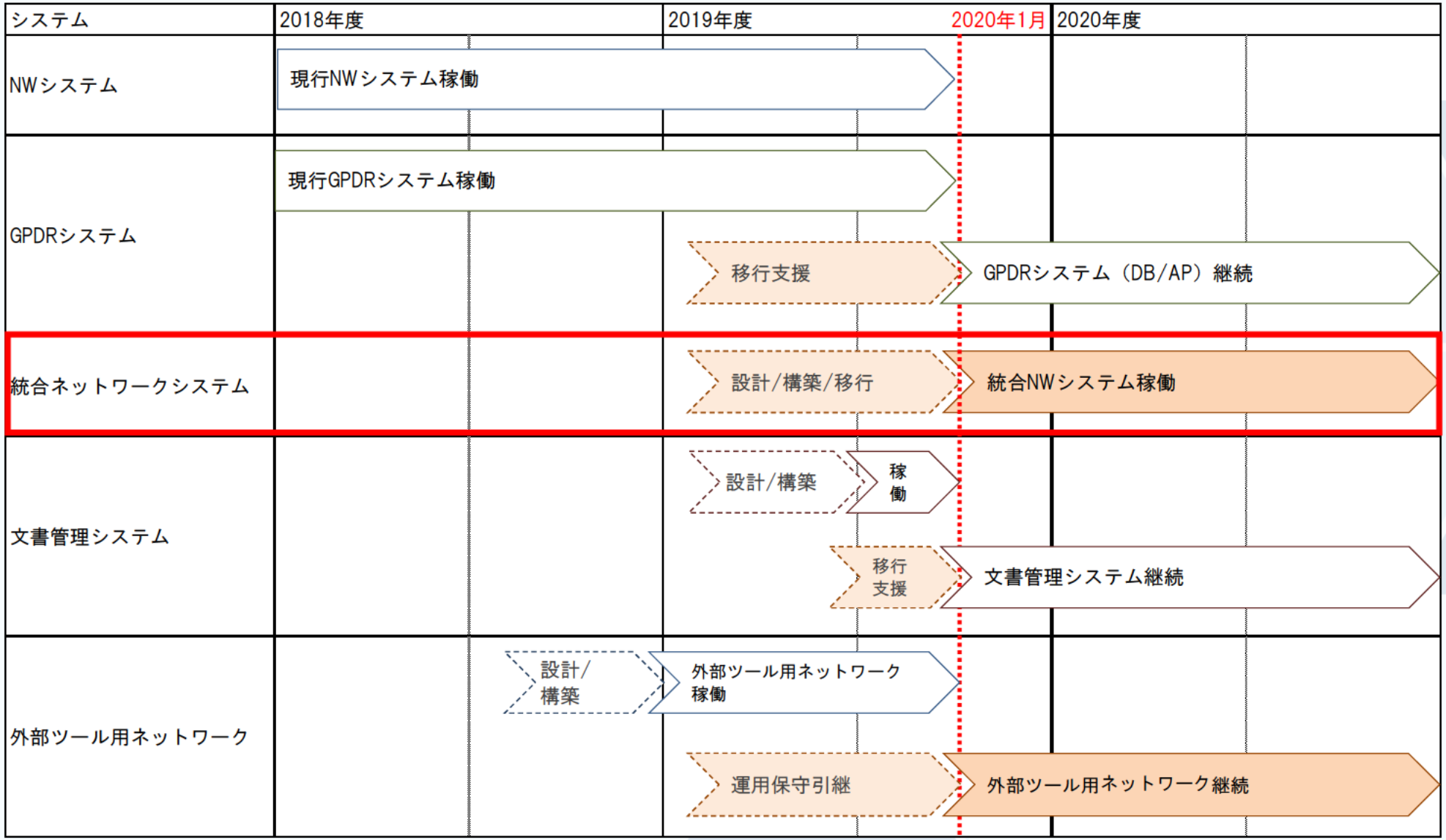
８．セキュリティについて

[redacted]

また一つのセキュリティ機器で不正通信の全てを検知することに限界があることを想定し、多層防御の観点を取り入れた複数のセキュリティ機器構成による対策を講じる。

９．スケジュール

物品調達、構築業務については、契約締結日から2019年12月末日まで、運用保守、ネットワーク回線サービス、ハウジング及び運用サービス、その他業務については、2020年1月から2025年3月31日までとする。



参考：概算所要額

（参考）

概算所要額

プロジェクト推進のための支援業務委託先であるＴＩＳ株式会社の支援により試算した、現時点で想定する概算所要額は以下のとおり。なお、最終的な契約額は一般競争入札(総合評価落札方式)により確定する。

(単位：百万円)

	2019年度		次期中期目標期間	調達期間総額
	設計構築	初期保守		
ハードウェア				
ソフトウェア				
回線				
設計構築等役務				
運用保守等役務				
合計	3,655	61	1,213	4,928
税込み（10%）	4,020	67	1,334	5,421
	4,087			

※ハードウェア及びソフトウェアには保守費用を含む。