中小企業基盤整備機構ＷＡＮシステムに係る

業務・システム最適化計画

平成２０年2月２９日
独立行政法人中小企業基盤整備機構

独立行政法人中小企業基盤整備機構（以下「中小機構」という。）は、独立行政法人等の業務・システム最適化実現方策（平成１７年６月２９日　各府省情報化統括責任者（ＣＩＯ）連絡会議決定）を踏まえ、以下のとおり中小機構ＷＡＮシステムに係る業務・システム最適化計画を定める。

第１ 業務・システムの概要

中小機構ＷＡＮシステムは、中小機構の役職員等利用者の利便性向上、業務の効率化、情報の共有化を図ることを目的に構築された情報基盤であるとともに、中小機構の業務を遂行するために整備する個別業務・システムに対し通信基盤を提供するものである。

中小機構ＷＡＮシステムは、本部に設置された基幹ＬＡＮ及び各地方拠点（支部、大学校、事務所、開発所等）に設置された構内ネットワーク（以下「拠点ＬＡＮ」という。）と、それらＬＡＮを相互に接続した広域ネットワーク（以下「ＷＡＮ」という。）、インターネット接続用の設備（Ｊ－ＮＥＴ）並びにファイル共有システムや電子メールシステム、グループウェア等の情報共有システム等から構成される。

中小機構は平成１６年に中小企業総合事業団、地域振興整備公団及び産業基盤整備基金の三つの法人が統合され、設立した。

中小機構ＷＡＮシステムは中小機構の設立に際し、それまでの三法人がそれぞれの業務・システムの目的に沿って個別最適化を行っていた情報通信基盤（情報共有システム、ＬＡＮ及びＷＡＮ）を統合し、再構築したものである。再構築の際、ＷＡＮ及びグループウェア等については中小機構として一元化が実施されてきたところであるが、効率性・合理性、安全性・信頼性、利便性維持・向上などの全体最適化の視点から整備が行われたものとはなっていないのが現状であり、特に中小機構全体としての明確なセキュリティポリシーが存在していない等の問題が顕在化している。

このため、中小機構ＷＡＮシステムについては、「電子政府構築計画」（２００４年（平成１６年）６月１４日一部改定　各府省情報化統括責任者（ＣＩＯ）連絡会議決定)、「共通システムの見直し方針」（２００４年（平成１６年）３月２５日　行政情報システム関係課長連絡会議了承)、「業務・システム最適化計画策定指針（ガイドライン）第５版」（２００６年（平成１８年）３月３１日　各府省情報化統括責任者（ＣＩＯ）連絡会議決定）を踏まえるとともに、「政府機関の情報セキュリティ対策のための統一基準」（２００５年１２月版［全体版初版］（平成１７年）１２月１３日　情報セキュリティ政策会議決定、以下、「政府機関統一基準」という。）をはじめとする各種の関連する政府方針を遵守しつつ、最適化計画を策定することとする。

中小機構ＷＡＮシステムの業務・システム最適化計画策定に当たっては、以下の事項を基本理念とする。

（１）「独立行政法人等の業務・システム最適化実現方策」に則り、経済性も考慮しつつ業務・システムの簡素化・効率化・合理化を推進する。

（２）中小機構ＷＡＮシステムのシステム面における検討については、平成１６年の３団体統合時にネットワーク・サーバ構成等の統合化等に着手し合理化されていることから、主に情報セキュリティの確保・向上、可用性・信頼性の向上、システムの高度利用の推進等について見直しを行う。

（３）その他、中小機構ＷＡＮシステムにおける情報セキュリティの確保のための規程類の整備、システム運用方法の改善及び調達方法の合理化等についても検討を行う。

第２　最適化の実施内容

１．ネットワークの信頼性向上及び合理化・効率化

（１）現状

全拠点又は多数の拠点から使用する重要システム（共済システム、指紋サーバ等）が本部に設置されているが、中小機構ＷＡＮシステムのＷＡＮ回線はルートの冗長化がされていないため、本部のＷＡＮ回線等の一箇所の障害により前述の重要システムが全拠点から利用できなくなるリスクがあり、業務に支障が出る可能性がある。

本部に設置される基幹ＬＡＮは、ルートの冗長化がされておらず、バックボーンスイッチ周辺の幹線ルートの１箇所が障害（機器障害、配線障害）になると、本部内及び本部拠点間のほぼ全ての通信が行えなくなるリスクがある。これにより、本部に設置される重要システムが利用できなくなり、業務に支障が出る可能性がある。

また、本部の基幹ＬＡＮは、ドメインの簡素化を行うために、ネットワーク構成を見直したが、調達当初の機器がそのまま利用されており、見直し後のネットワー

クに対して過剰な機能、性能の機器となっている可能性があり、コストアップの要因になっている可能性がある。
　インターネット接続用の設備（Ｊ－ＮＥＴ）については、既に機構として集約が実施されており、包括的なセキュリティ対策も実施されている。

　拠点ＬＡＮにおいては、現状、拠点側のルータ装置及びファイルサーバの監視を本部から実施しているが、拠点ルータ配下のネットワーク機器（ハブ）にネットワーク監視対応機能が具備されておらず、本部からの拠点ＬＡＮの監視が実施できていない。そのため、拠点ＬＡＮに障害が発生しても本部から状況を正確に把握することが難しく、迅速な障害対応が行えない等、利用者の利便性を損なっている可能性がある。

（２）実施内容
（ア）ＷＡＮの冗長化
　既設のＷＡＮ回線であるＩＰ－ＶＰＮ網（現用網）に加え、ブロードバンドサービスを利用した安価な閉域網を現行ＩＰ－ＶＰＮ網のバックアップ網として構築することにより、各拠点から本部までの迂回ルートを確保する。これにより、ＷＡＮ回線等の一箇所の障害により、前述の重要システムが全拠点から利用できなくなるリスクを回避する。
　また、現行ＩＰ－ＶＰＮ網に業務系の通信トラフィックを、バックアップ網にインターネットアクセス等の非業務系の通信トラフィックを負荷分散して流すことにより、ＩＰ－ＶＰＮ網に流れる通信トラフィックを軽減することで、業務系で利用可能な通信帯域の増加を図る。
　このバックアップ網の構築により、年間約２，０００万円（試算値）の経費増加が見込まれる。

（イ）本部基幹ＬＡＮの冗長化と合理化
　本部基幹ＬＡＮの構成を見直し、本部基幹ＬＡＮの主要通信ルートの冗長化を実施することにより、1箇所の障害による本部基幹ＬＡＮの全体ダウンのリスクを回避する。合わせて、構成見直し後のネットワークに必要な機能・性能に見合った適正な装置を選定することにより、現状相当以上の信頼性を維持しつつコストの適正化を行う。
　この本部基幹ＬＡＮの見直しにより、年間約９０万円（試算値）の経費削減が見込まれる。

（ウ）拠点ＬＡＮの監視強化
　拠点側ルータ装置配下のネットワーク機器として、ネットワーク監視対応機能を具備するインテリジェントスイッチを導入し、本部のネットワーク監視装置から当

該スイッチのポートを監視することにより、拠点ＬＡＮの状況を把握できるようにすることで、拠点ＬＡＮに障害等が発生した場合の障害検出、原因切分け、及びその対策の実施を迅速化する。

この拠点ＬＡＮの監視強化のために、年間約１３０万円（試算値）の経費増加が見込まれる。

（エ）ＩＰｖ６への対応

ＩＴ新改革戦略（平成１８年1月１９日　ＩＴ戦略本部）等において、ＩＰｖ６の利用を推進することは我が国の国家目標とされている。

将来的なＩＰｖ６の利用を考慮し、中小機構ＷＡＮシステムを構成する機器（ネットワーク機器、サーバ機器等）については、更改に合わせ原則としてＩＰｖ４とＩＰｖ６の両方に対応した機器を導入する。

２．共通利用システムの信頼性・安全性の向上及び合理化・効率化

（１）現状

現状、ファイル共有のためのファイルサーバが、本部及び全国の支部・大学校に設置されているが、全国の支部・大学校に設置されるファイルサーバにおいては、保存されるデータ量の増加により、搭載するバックアップ装置にて確実なバックアップが困難な状況となっている。また、運用管理を本部からの遠隔制御で行っているため、支部・大学校のファイルサーバにバックアップエラー等の障害が発生した場合には、テープ交換等の復旧作業のために現地職員によるサポートが必要となっている。

支部・大学校のファイルサーバにおいては、データの暗号化が実施されておらず、居室等に無防備な状態で設置されている等、設置環境及びバックアップテープ媒体の保管状態が適切性に欠ける。このため、機密性の高い情報が格納されたファイルサーバやバックアップテープ媒体への不正な操作が容易に行える環境であることに加え、粉塵や温度変動等によるサーバ装置の故障やテープ媒体の破損等により重要なデータの破壊・消失を引き起こす可能性がある。

現在導入されているグループウェアは、豊富な機能を持つクライアントサーバ型のパッケージソフトウェアを使用して構築されているが、メール機能を除き、掲示板機能、データベース機能等のグループウェア機能及び情報共有の高度な機能が積極的に活用されておらず、投資対効果が低い利用状況となっている。

また、各役職員のＰＣに対して、グループウェア専用のクライアントソフトウェアのインストール・環境設定作業等を実施する必要があり、Ｗｅｂアクセス型のグループウェアに比べ運用・管理の負荷が大きい。

（２）実施内容

（ア）支部・大学校のファイルサーバの信頼性、安全性の向上

支部・大学校に設置されるファイルサーバの構成を見直し、テープ媒体を複数本収容可能なテープオートローダを搭載する。これにより、データ量に応じたバックアップ容量を確保することで、安定した信頼性の高いバックアップ運用を可能とするとともに、テープ交換に要する現地職員によるサポートを不要とする。

また、支部・大学校に設置されるサーバ機器については、施錠ラック等の安全な環境に設置し、バックアップテープ媒体は施錠可能な安全な環境に保管することにより、重要なデータに対するセキュリティ上のリスクを低減するとともに、サーバ装置の故障やテープ媒体の破損等によるデータの破壊・消失を回避する。

この支部・大学校のファイルサーバの見直しにより、年間約５４０万円（試算値）の経費増加が見込まれる。

（イ）グループウェアの合理化・効率化

現状導入されているグループウェアの機能を利用し、Ｗｅｂアクセス型の利用形態に変更することにより、各役職員のＰＣに対して実施していた、グループウェア専用のクライアントソフトウェアのインストール・環境設定作業等を廃止することで運用・管理の更なる効率化を行う。合わせて、システム構成、ソフトウェアライセンス構成を見直すことにより、費用の削減を行う。

また、現状有効活用されていない掲示板機能、データベース機能等のグループウェア機能及び情報共有の高度な機能については、積極的な周知・教育活動により利用促進を行うことで費用対効果の向上を図る。利用部門でカスタマイズを行うＥＵＣ（End User Computing）については、一定の管理と統制を行うことにより、維持・管理不能なデータの蓄積を抑制することで、将来的な他のグループウェア製品への移行の可能性を担保する。

このグループウェアの合理化・効率化により、年間約３３０万円（試算値）の経費削減が見込まれる。

３．運用管理業務の合理化・効率化

（１）現状

中小機構ＷＡＮシステムの運用管理業務については、外部の専門業者への委託によって行われており、中小機構内での常駐による作業形態にて、職員との円滑なコミュニケーションが確保されている。しかしながら、運用管理業務の作業内容については、年間を通した作業計画の策定や障害分析、中小機構職員が利用するネットワーク全体の定常監視など、システムの信頼性・安全性の維持向上及び運用管理業務の効率化に向けた、いわゆるプロアクティブな運用を実現するという点で改善の余地がある。

そのため、現在委託している運用管理業務については、運用管理業者の作業実態

の見える化を促進しつつ、作業実績をＰＤＣＡの観点で継続的に見直すことが可能なしくみを確立し、作業の品質レベルとコストの妥当性の判断を容易にすることが必要である。

　また、ソフトウェア資産の管理において、各部門個別で必要なパッケージソフトウェアについては、各部門毎に購入しており、ソフトウェアライセンス等の管理が分散して行なわれていることから、将来的に中小機構全体で利用されているソフトウェア資産及びライセンスの把握が困難となる可能性がある。

（２）実施内容

（ア）運用計画の策定と作業実施報告の管理

　運用管理業務を実施するための運用計画を策定し実行することにより、システム運用の更なる安定化を図る。また、運用計画に基づく作業実施報告の実施により、作業実態の把握をより正確に行い、運用管理業務の継続的な改善を実施する。

（イ）予防保全の強化

　バックアップ作業等の不定期に実施する作業の事前訓練や、作業方法のチェック、及び障害履歴・ログ等の分析による異常傾向の事前把握等を運用管理業務の一環としてより一層充実させ、不測の事態に備えた予防保全の強化を行う。

（ウ）ネットワーク監視の高度化

　現在導入されている運用管理ツールを積極的に活用し、中小機構ＷＡＮのユーザである役職員等が利用するネットワークに関し、可能な限り広い範囲でのリアルタイム監視を実施する。

（エ）ソフトウェア構成管理の一元化

　現在導入されている資産管理ツールを有効に活用し、役職員等が利用するＰＣを中心としたソフトウェア資産の洗い出しを行い、ソフトウェア構成を把握し、ソフトウェアライセンスのより適切な管理を継続的に実施する。

４．セキュリティ対策の強化

（１）現状

　中小機構ＷＡＮシステムは、大量の顧客（団体、個人）データの管理を行う機能を有しているが、中小機構として遵守すべき情報セキュリティ管理及び個別情報システムの管理に関する規定並びに実施手順が明確に定められておらず、以下のような情報セキュリティ対策の不備により、機密情報の漏洩等の事故が発生する恐れがある。

・ 情報の重要度の判断、データの暗号化等、重要データの取扱いが個人に依存

・ 重要情報の暗号化、アクセス制御が不徹底
・ アカウントの申請、登録、削除の承認手続き、権限が不明確
・ 機構支給以外のＰＣの持込み、及びネットワークへの接続についてのポリシーが不明確
・ パスワードの定期的変更が不徹底
・ 機構が指定した以外のメールサーバやＨＴＭＬメールの利用が禁止されていない
・ 外部委託時の情報セキュリティ対策が不明確
・ 外部委託業者の入退室の他、サーバ室に対する包括的な安全対策が不十分　等

　また、中小機構においては現在もセキュリティ意識及びＩＴリテラシーの向上を目的とした教育や広報活動が実施されているが、役職員等のＩＴリテラシー及びセキュリティに関する意識は十分に上がっていないと考えられ、このため、機構役職員等のセキュリティ意識の不足による事故の発生が懸念される。

（２）実施内容

（ア）情報セキュリティポリシーの策定と運用

　「政府機関統一基準」に準拠し、中小機構として遵守すべき情報セキュリティポリシーとして「情報セキュリティ管理規程」を策定するとともに、その実施手順を策定し、経営トップからのトップダウンにより適正に運用することで、中小機構全体として安全性の確保を行う。

（イ）職員教育等によるリテラシーの向上

　上記で策定する情報セキュリティポリシーに準拠し、機構役職員等のセキュリティ意識及びＩＴリテラシーの向上を目的とした教育研修及び広報活動についてＰＤＣＡサイクルを確立することで、組織一丸となって情報セキュリティ対策強化に取組む風土を醸成する。

　また、外部リソースの有効活用等を含めた、情報システム企画・管理部門のＩＴスキルの向上により、情報システムの企画・管理力の更なる強化を行う。

（ウ）情報システムの機能によるセキュリティ面での個別対策

　上記の情報セキュリティに関する対策の他、既存の情報システムの機能の有効利用により解決が可能な以下の対策についても実施する。

① 機密性の高い情報を格納するファイルサーバにおいては、導入済みの暗号化ツールを活用し、暗号化が必要と認められた情報については暗号化を実施することで、情報漏洩のリスクを低減する。
② 利用可能な既存システムのパスワード強制変更機能を使用し、人的要因によ

るパスワード変更漏れの防止と管理部門の負荷が小さい効率的なパスワード変更を実現する。

③ 既存のＤＨＣＰサーバのＩＰアドレス予約機能を活用し、管理対象外機器のネットワーク接続を制限することにより、持込ＰＣ等による不正侵入や攻撃等のセキュリティ上の脅威を低減する。

④ 情報システム利用時の申請フローを見直し、承認権限を明確化することにより、より確実なアカウント管理を実施する。

５．調達内容の継続的改善

（１）現状

中小機構ＷＡＮシステムの調達にあたっては、政府調達の手続きに則り、一般競争入札を採用する等により適切に行なわれている。より公平性・透明性・費用対効果の高い調達を実現するには、調達後における機器及び運用の実態を踏まえた上で、より精度の高い調達仕様となるよう、継続的に改善を行なうことが必要と考えられる。

（２）実施内容

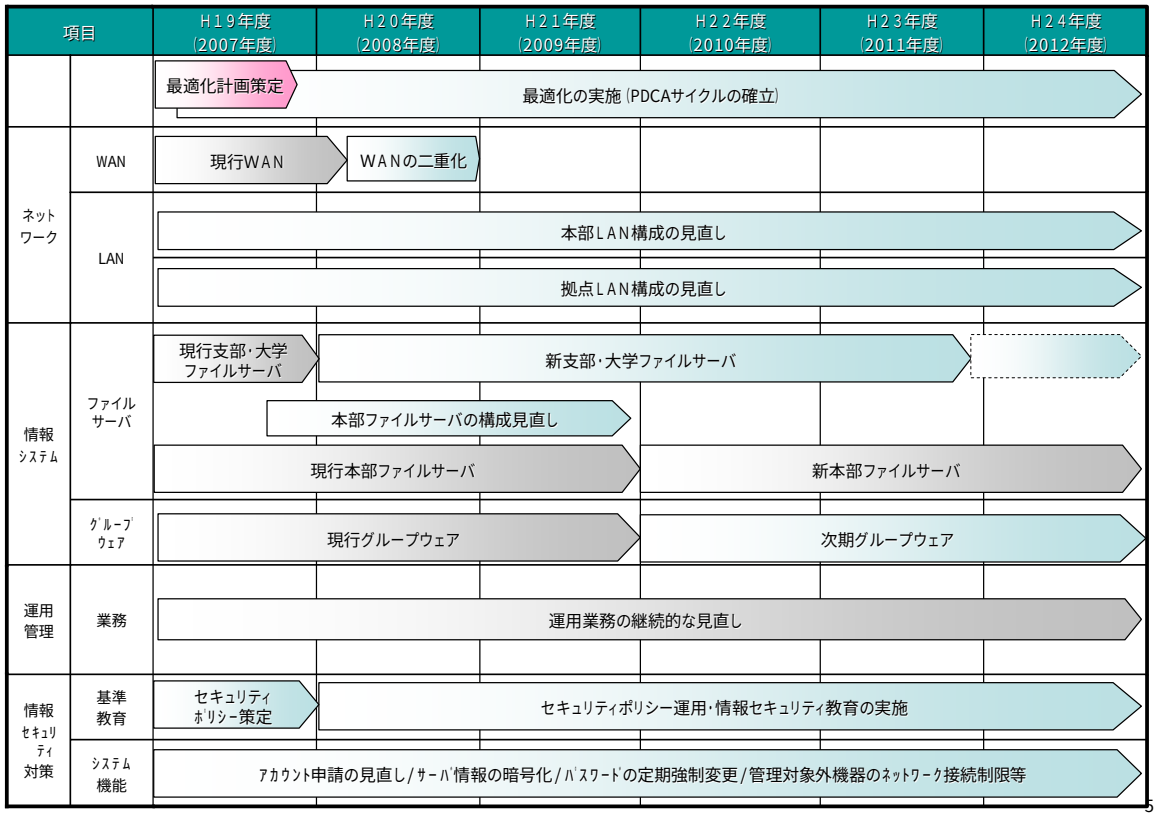
これまでに掲げた最適化施策を推進するにあたり、中小機構ＷＡＮシステムに係る調達に関しては、現状システムの実態に基づく仕様の明確化、システムに関するドキュメンテーションの徹底等により、一層の透明性・公平性の確保を図るとともに、外部委託やオープン・ソース・ソフトウェアの活用等についても積極的に検討を行い、更なるシステム運用経費の削減が可能となるよう配慮する。

第３ その他

最適化計画の実施に当たっては、最適化計画策定後の情報通信技術の進展、ネットワークサービスの多様化、製品化の動向、機構内の他の最適化計画の実施状況等を踏まえ、経費及び業務処理時間の効果を明らかにしつつ、必要に応じてネットワークの構成等を含め継続的に最適化計画の見直しを行うこととする。

第４ 最適化工程表

■ 最適化工程表



第５ 現行体系及び将来体系

別添１「現行体系」、別添２「将来体系」

第６ 今後取組むべき課題

支部・大学校のファイルサーバについては、ＷＡＮの回線帯域の制約により本最適化計画実施後も地方拠点に設置することとしているが、運用・管理の効率化、情報セキュリティ対策の徹底の視点からは、本部サーバ室に集約設置することが望ましい。現時点においては、回線帯域の増強費用、ＷＡＮ高速化装置の導入費用等の追加投資と上記本部サーバ室に集約設置した場合の費用対効果を考慮し、従来どおり地方拠点に分散配置することが最適との判断をした。一方、国内ネットワークについては、急速に回線の広帯域化、低価格化が進んでおり、支部・大学校ファイルサーバの更改タイミングにおいて、回線帯域の増強と合わせて再度本部集約設置について検討する必要がある。