平成２９年１０月１６日

「平成29年度から平成32年度までの環境省ネットワークシステムにおけるディザスタ・リカバリサイトの構築及び運用・保守業務」
要件定義書に係る要件の補足

項番	要件定義書の記載	要件の補足
1	３．２ システム方式に関する事項 （１） 情報システムの構成に関する全体の方針 「表３－２ 情報システムの構成に係る全体方針」 No.2　ソフトウェア製品の活用方針 ② 導入予定のソフトウェアについて、環境省でライセンスを保有している場合には、既存ライセンスを有効活用すること。	「環境省でライセンスを保有している場合には、既存ライセンスを有効活用する」の記載について、DRサイトが提供する仮想デスクトップサービス上で利用する端末を含め、マイクロソフトOffice製品の利用権利は既存契約で取得済であり、新たな追加購入は必要ない。 ただし、クラウドサービス（Azure・Office365）が提供する仮想デスクトップサービス及びメールサービスを活用してDRサイトを構成する場合は、新たにライセンスが必要となる。（別紙「マイクロソフト製品ライセンスに係る参考情報」参照）
2	３．３ 規模に関する事項 （２） データ量　「表３－３－１　データ量」 No.1　共有ファイルのデータ量　50TB	「共有ファイルのデータ量　50TB」のうち、平成30年3月末までに主系サイトからDRサイトへ非常時の優先業務の遂行に必要なファイル（最大5TB）を同期し、災害訓練（平成30年8月実施予定）の実施までに残りのデータを同期すること。
3	３．１０ 情報セキュリティに関する事項 （３） 情報システムのセキュリティ要件 （イ） アクセス制御 「ファイル共有サービス」で導入されるファイル・フォルダへのアクセス制御機能を提供すること。 アクセス制御機能は必要に応じて以下に示す方式による制御が可能であること。 - DRサイト利用者やそのグループ属性に基づくアクセス制御 - 同時利用者数によるアクセス制御 - 同一IDによる複数アクセスの禁止 - IPアドレスによる端末の制限	「必要に応じて以下に示す方式による制御」とは、「DRサイト利用者やそのグループ属性に基づくアクセス制御」を行うことを必須とし、「同時利用者数によるアクセス制御」、「同一IDによる複数アクセスの禁止」、「IPアドレスによる端末の制限」を含むその他の対策は応札者の提案によるものとする。
4	３．１０ 情報セキュリティに関する事項 （３） 情報システムのセキュリティ要件 (ケ) 標的型攻撃対策 (c) 内部への侵入低減対策（入口対策） アラートやログ分析による侵入の早期検知 検知結果に対する迅速な対応	「早期検知」及び「迅速な対応」とは、24時間365日の対応を求めるものではない。
5	３．１０ 情報セキュリティに関する事項 （３）情報システムのセキュリティ要件 （ケ）標的型攻撃対策 （a）メールセキュリティ対策 ・メール本文中のURLのサイト情報から不正サイトを判断した場合、不正なメールとしての適切な処理を実施する。	「メール本文中のURLのサイト情報から不正サイトを判断した場合」における判断とは、環境省が判断を行うものである。請負者は環境省が不正なメールと判断したメールへ適切な処理を実施するものである。
6	３．１０ 情報セキュリティに関する事項 （３） 情報システムのセキュリティ要件 (ケ) 標的型攻撃対策 (e) セキュリティ監視 セキュリティインシデントを検知した場合は被疑仮想サーバ・仮想デスクトップの隔離を行うこと。	「セキュリティインシデントを検知した場合」における検知とは、発生した事象がセキュリティインシデントであると環境省が検知（判断）した場合を指し、請負者は環境省の指示により被疑仮想サーバ・仮想デスクトップの隔離を実施するものである。
7	（別紙３）機能一覧 １． 本調達範囲で実現するサービス （２） 認証サービス · 環境省ネットワークシステム（主系サイト）に接続しているクライアント端末（約3,700 台、その内シンクライアント端末は約1,100 台）がDR サイトに接続した際にも利用できるように、主系サイトにおいて認証サービスを実現するために利用しているMicrosoft社の製品Windows Server（Active Directory 機能）を採用し、主系サイトとDR サイト間で認証情報を連携すること。なお、記載した要件と製品仕様に相違がある場合は、製品仕様を優先する。	「主系サイトとDRサイト間で認証情報を連携する」に記載する認証情報の連携方式は、主系サイトとは疎結合の方式（主系サイトとDRサイトは別フォレストにする）を採用することが望ましい。