

データファイル自動暗号化システム 設計構築業務仕様書

新潟県長岡市総務部情報システム管理課

平成 28 年 月

目次

1	調達件名	1
2	概要	1
3	基本的な考え方	1
4	業務範囲について	2
5	スケジュールについて	3
6	契約期間	3
7	作業内容	3
8	納品物	6

1 調達件名

データファイル自動暗号化システム設計構築業務

2 概要

標的型攻撃による公的機関等の個人情報大量漏えい事故の発生及び平成29年7月より開始される情報提供ネットワークを介した特定個人情報の地方自治体と国の機関との連携開始などを受け、各自治体での情報セキュリティの強化が喫緊の課題となっている。

昨今の標的型攻撃の傾向を鑑みると、マルウェアなどを侵入させない入口対策や C&C サーバへのアクセスを拒否する出口対策などもさることながら、万が一、未知のマルウェアに感染し、組織内で保有するデータが、意図せず外部の第三者の手に渡る事態も想定せざるを得ない状況である。

長岡市（以下、「本市」という。）では、この事態に対応するため、データファイルを暗号化しておくことが望ましいと考えている。

その手法について、機密性、可用性を保持しつつ、利用者の負担の軽減、管理・運用の容易性などを総合的に考慮した上で最適と思われるシステムを構築し、データファイル暗号化を行う。

なお、現在のファイルサーバの利用形態及び本事業終了時点のデータファイルの自動暗号化のイメージについては別紙1「長岡市ネットワーク概略図及び自動暗号化イメージ」を参照すること。

3 基本的な考え方

以下の機能を充足するシステムの設計及び構築を行うこととする。

- (1) ユーザーがデータファイルを暗号化する上で、意識して暗号化操作を行うのではなく、ファイルサーバ上の特定のフォルダにファイルを作成、移動、コピー等を行った段階で、自動的に且つ即時的に暗号化される方式とする。
- (2) (1)記載の手法の他に、各利用者が任意のファイルを簡易な操作でファイルを暗号化できること。
- (3) 暗号化されたファイルは、フォルダ間の移動やコピー、名前変更などを行っても引き続き暗号化されていること。
- (4) 暗号化されたファイルを利用者が操作する場合、意識的に復号化操作を行うことなく、拡張子に関連付けされたアプリケーションで直接開くことができることとする。また、当該データファイルの操作を終了し、ファイルを閉じた後も自動で暗号化されていること。
- (5) 暗号化されたファイルを開くことができるのは、庁内で運用している既

存の ActiveDirectory サーバでの認証を経たユーザーや特定のエージェントソフトをインストールした端末などに限定することとし、仮に暗号化されたデータファイルを持ち出した上で、組織外の端末上で当該データファイルを操作した場合でも、通常の操作ではファイルの内容を参照できないこととする。

- (6) 業務上やむを得ず、外部の端末に暗号化されたファイルをメール等で送信する場合想定される。その際各利用者が個人の権限で簡易な操作を行うことによりファイルを復号化（平文化）できる機能を有することとする。また、その復号化操作のログについて管理者が確認できることとする。
- (7) システムの構築に当たっては既設のサーバ（ファイルサーバ、ActiveDirectory サーバなど）を可能な限り活用すること。

4 業務範囲について

- (1) 対象業務及び本案件の契約に含む費用について

本業務を遂行するため、以下の業務を行うことを基本とする。

- ア 各種設計業務に関する費用
- イ 物品調達支援作業（構築に必要なハードウェア、ソフトウェア、ライセンス等の選定及び入札仕様作成補助 等）に関する費用
- ウ 新たに調達する機器及びシステムの構築作業に関する費用
- エ 既設サーバ機器への新規ソフトウェア導入に関する費用
- オ 利用者教育支援対応に関する費用
- カ 運用者教育支援対応に関する費用
- キ システム稼働開始直後のサポート
- ク 平成 28 年度分の運用サポート
- ケ 打合せ等に必要な交通費、宿泊費等
- コ 上記のほか、システムを構築し安定稼働させるために必要となる作業及びその関連費用

- (2) 対象外業務及び本案件の契約に含まない費用について

以下の項目については本市側で実施及び調達するため、本案件の契約に含まれないものとする。

- ア 構築に必要なハードウェア、ソフトウェア、ライセンス、保守パック等の物品に関する調達費用
(本市側で別途入札により調達した物品を引き渡すこととする。)
- イ 既設端末にエージェントソフト等の資産配布が必要な場合の作業費
(本市保有の資産管理ソフトを使用して配布する。ただし、その配布準備

に係るサポート等は対象業務とする)
ウ 既設ネットワーク機器の設定変更作業費

5 スケジュールについて

現在予定しているスケジュールについては、別紙2「スケジュール案」を参照のこと。

6 契約期間

契約締結日～平成29年3月31日

※ 次年度以降についてもサポート契約等の継続が必要となる場合は平成29年度予算にて別途契約するものとする。

7 作業内容

本業務の委託契約を締結した事業者は、以下の作業を実施すること。

(1) 各種設計作業

ア 既設のサーバの稼働形態、端末性能などを考慮し、利用者の視点のみならず、運用担当者の視点からも利便性や運用の容易性を極力損なうことなく、費用対効果を最大化できるよう、最適なシステム構成を検討すること。なお、既設サーバや端末等の基礎情報については別紙3「基礎情報一覧」を参照すること。

イ 必要に応じて現地での調査や打合せを行い、設計に反映させること。

ウ 既設機器を極力活用するようにシステム設計を行うこと。

エ 設計した内容については必ず本市側の承認を得ること。

(2) 物品調達支援作業

本業務を完遂するにあたり、必要となる物品等については本市側で別途入札による調達を行うが、その入札準備行為に必要な調達仕様書を作成するにあたり、情報提供や記載内容と調達予定物品の仕様に問題がないかなどの確認を実施すること。

また、調達形態は5年間（平成28年10月1日～平成33年9月30日を予定）の長期継続契約（リース契約）となる点に留意すること。

(3) 新たに調達する機器及びシステムの構築作業

ア 機器及びシステム設定作業

（ア） 設計内容を元に、新規調達機器及びシステムの設定作業を実施するこ

と。

- (イ) 現在稼働している機器及びシステムへの影響が及ばない範囲で設定作業を行うこと。なお、設定作業において、既設システムや既設ネットワークに何らかの影響が及ぶ可能性がある場合はあらかじめ本市と対応方針について協議すること。
- (ウ) 新規調達機器を、本市が指定するデータセンター（所在地：長岡市内）内の 19 インチラックに搭載、設置すること。なお、19 インチラック仕様については下記のとおりとする。

ラックサイズ	42U
ラックサイズ（外寸）	縦：2,000mm 横：600mm 奥行：1,000mm
機器搭載許容重量	1,000kg/m ²
電源	100V/20A

イ テスト稼働対応

- (ア) 一部端末及び部署においてテスト稼働を行うこと。なお、テスト稼働の規模等については事前に本市と協議を行う決定すること。
- (イ) テストが必要となる項目についてチェックシート形式で明示し、本市側に提示すること。
- (ウ) テスト稼働時に想定外の挙動を検知した際はその発生状況を確認し、システムの設定調整等を行うこと。

ウ 既設機器の設定変更指示

既設サーバ機器等において設定変更が必要となる場合、設定変更の具体的な指示を記載した指示書を作成すること。

(4) 既設サーバ機器への新規ソフトウェア導入に関するインストール

既設のファイルサーバ及び ActiveDirectory サーバ等に対してソフトウェアのインストールが必要となる場合は、その作業を実施すること。

なお、現行機器の設定パラメータの提供や技術的な支援が必要な場合は本市側の協力を仰ぐこととする。

(5) 利用者教育支援対応

利用者に対するシステムの概要説明会で用いる資料作成補助及び操作説明会等で用いる操作マニュアルの作成を行うこと。

(6) 運用担当者教育支援対応

- ア 運用担当者が平常時の際に必要なオペレーションマニュアルを作成すること。特に年度が切り替わる際に発生する大規模な人事異動の際に対応できるようにバッチファイルやツールの提供やそれに特化した手順書等が必要となる場合は提供すること。
- イ 運用担当者が障害と思われる事象を検知した際の切り分け手順及び対応手順をまとめた障害時対応マニュアルを作成すること。

(7) システム稼働開始直後のサポート

システム稼働の直後は、利用者より様々な問合せが寄せられることが想定されるため、安定稼働後のサポート体制時よりも細やかな対応が求められる。そのため、必要に応じて現地立会いも想定したサポート体制をとること。

(8) 当年度中の運用サポート

当年度中にシステムを運用する中でのサポートを以下の内容で行うこと。

- ・システムを運用している中で、設定の調整や不具合時の対応方法、その他問合せが発生した場合に調査及び回答を行うこと。
- ・対応方法については、メール、電話で受け付けること。
- ・受付時間はメールでの受け付けは 24 時間 365 日、電話での受け付けは開庁日の 8:30~17:15 とすること。ただし、全庁的にシステムが全く利用できないなどの大規模な障害が発生した場合には上記の限りではなく電話等での問合せに適宜対応すること。

(9) 上記の(1)～(8)のほか、システムを安定稼働させるために必要となる作業を実施すること。

8 納品物

以下に示す現時点で必須と想定する納品物を納品すること。各ドキュメントの記載事項や納入期限等については、本市の承認を得ること。

すべてドキュメントを紙に出力したもの及びデータファイルを格納した電子媒体（DVD-R など）を各 2 部、本市に納品すること。

作業内容	納品物	備考
導入作業	プロジェクト計画書	
	実施スケジュール表	
	プロジェクト進捗管理表	
	基本設計書	ネットワーク構成図、ハードウェア構成図、ラック搭載図、物理配線図、論理配線図、ソフトウェア構成図等を含むこと。
	詳細設計書	各サーバ、ソフトウェア、システムの設定情報を含むこと
各種テスト	テスト計画書	
	テスト実施結果報告書	
利用者教育	操作マニュアル	利用者及び運用担当者がシステムを利用する手順書を画面の画像等を用いて作成すること。
	運用保守マニュアル	運用担当者が平時の運用としてオペレーションが必要となる作業をまとめた資料を作成すること。
	障害時対応マニュアル	運用担当者が障害と思われる事象が発生した場合に事象の切り分けや復旧方法などの実施すべきオペレーションをまとめた資料を作成すること。
共通	会議議事録	本市が指示する形式で、必要部数を納品すること。