または、過失により情報漏洩の危険を作出した場合において、これを止める手段を構築している。今後も、人的セキュリティにつき、物理的セキュリティによるカバーを図りつつ、拡充を図られたい。

【意見】佐世保市に対する外部からの情報漏洩を企図する者としては、上記の情報セキュリティの脅威１０大類型の内、「④　サプライチェーンによる被害」、「⑤　内部不正による情報漏洩」等を絡めた方式（情報が紙媒体中心の時代のころの情報漏洩に回帰する。）によることが予測される。また、電子情報の場合、これを取り扱っている者が、指示されている操作の内容、仕組みを理解していないという場合がある。本件のアンケートを基に、監査人及び監査人補助員ＳＥにて、佐世保市からの情報漏洩を探る手段を模擬したが、その手段として、情報機器につき専門的知識まで有していない職員、佐世保市との取引業者等を道具として、情報漏洩をさせる道具として用いる手段が考えられた。

今回のアンケートについては、その詳細な結果を別途佐世保市にて把握できる状態にあるが、その内容から、情報セキュリティの１０大脅威について特に留意等していない部署とその傾向、また、各部署からの佐世保市への要請等が具体的に判明すると思われる。今回のアンケート結果につき、人的セキュリティの拡充に役立てていただきたい。

第８章　佐世保市庁舎内の情報セキュリティの現状３（技術的セキュリティ）

第１　佐世保市における技術的セキュリティ体制

日々進化を続ける情報社会において地方自治体の情報管理は益々複雑化を強いられ、現状の課題であった加速する業務のシステム化の必要性、インフラの現状に伴う高速化、安定性、可用性のリクエスト、そして高い

テクノロジーを有した最適なコストで運用できる体制の構築を求められている。この条件を満たすことを軸に、佐世保市は、提案した「仕様書」(注7)に沿って情報管理セキュリティシステムの構築を行っている。

また令和元年１０月に運用を開始した佐世保市庁内情報システムは総務部情報政策課によって統括管理され、ハードウェア及びソフトウェアの運用・保守を一手に担っている。併せて外部委託システム導入業者の担当技術者の庁舎内常駐による監視・管理・保守により事故・トラブルへの即時対応が可能となっている。

さらに各部局（支所等も含む）へ配布された３０００台強の端末機器の管理も庁舎内の種々当該サーバーシステムにより一括管理を可能としている。

今回の外部監査において、先述のとおり、佐世保市の情報管理のコアな部分を司る言わば心臓部である種々のサーバ類につき、許可を得て視察を行ったが、その際、物理的セキュリティの現状確認のみならず、その運用実態の見極めを行い、技術的セキュリティの検証を行った。

第２　設計と機器調達について

佐世保市は情報システムの導入にあたり、大規模ＩＴシステム構築とインフラ整備が予想されたため、全体のプロジェクトを統括する業者選定のため、信頼できる地元企業に委託し、そこから各分野においての役割分担化を行ったということである。その詳細は、以下のとおりである。

１　全体マネジメント（設計・構築・運用サポート）

株式会社日本ビジネスソフト

２　地域イントラネットワーク、仮想サーバ及び一人１台パソコンの基本設

（注7）　第９章第２の３で示された仕様を基準とした調達仕様書

計

株式会社富士通エフサス

3　一人１台パソコンの設計導入

エコー電子工業株式会社

4　仮装サーバ設計、導入

扇精光ソリューションズ株式会社

第３　佐世保市総務部情報政策課が接続管理する地域イントラネットの主な接続施設

北　部			
消防局	相浦支所	小佐々支所	鹿町支所
江迎支所	吉井支所	世知原支所	大野支所
南　部			
日宇支所	早岐支所	環境センター	
離島地区			
黒島地区		高島地区	
本庁管理			
すこやかプラザ	水道局	総合教育センター 宇久行政センター	

※【北部】、【南部】、【本庁管理】は光ファイバ回線による有線通信、【離島地区】は大潟ポンプ場からの無線による通信方式

1　上記各施設に配置される端末機情報は有線・無線回線を通して本庁舎サーバ類に集約されリアルタイムにて情報の動向を記録する仕組みとなって

いる。監査人は、この情報管理につき、様々な高度ＩＴ技術が取り入れられていることを確認した。この技術は比較的新しいものも率先して導入されており昨今の企業データの漏洩や内部流出等の重大なインシデント(注8)に対応すべく仕様の中に盛り込まれていたものである。

2　外部からのサイバー攻撃(注9)からの防御については、通常はソフトウェアによる対処がセオリーであるが、佐世保市は特殊な脅威保護機器を設置し、かつ、アップデートを常時行うという防御方式でサイバー攻撃に備えている（統合型次世代ファイアウォールＵＴＭ)。これは、最近のサイバー攻撃が、間断なく進化、変化を続けている現在において、対処方法としては、最新の技術を導入していると評価できる。

3　前２の統合型次世代ファイアウォールのみならず、各部局端末においても、漏れなくアンチウィルスソフト（監査人補助員ＳＥにて性能を確認済み）がインストールされており、ネットワーク以外からの脅威の侵入（外部ＵＳＢ接続等）に対しても個別に対応が可能となっている。またパターンファイル及びプログラムのアップデートはサーバからの配信による仕組みとなっており、常に最新版によって新たな脅威に備えている。

4　ネットワークの不正接続の防御（ダイナミック認証ＶＬＡＮ）(注10)として佐世保市庁舎及び関連機関のネットワークについては、その外部からの侵入に備えて、非常に強力な認証システムを装備し事前に登録された利用者以外の不正なアクセス接続を防止している。

第４　職員に対する制約

（注8）一般的に事故を意味する。情報セキュリティにおいてはコンピュータもしくはネットワークに対して脅威となる事象を意味する。　例：不正アクセスやサーバへの攻撃等

（注9）サーバやパソコンのシステムに対して、ネットワークを介してデータの破壊や改ざん、窃取等を行う攻撃をいう

（注10）端末がネットワークに接続する際に特定の条件を含む認証（MACアドレス・クライアント証明書等）を行い正しい属性情報を確認後に目的のネットワークに接続できる認証方式

佐世保市の技術的な情報セキュリティに関する内規は、情報資産管理要綱に詳細が規定されている。その内容は、先述した「第５章　佐世保市内での情報施策に関する内規」、「第２　佐世保市情報資産取扱要綱」の８のとおりである。

第５　セキュリティレベルの確認と見直し

佐世保市は毎年１回設定したセキュリティレベルを佐世保市情報セキュリティ監査実施要領に基づき実態を監査している。情報セキュリティ統括監理者は監査結果を踏まえた上で課題及び問題点を確認し情報セキュリティポリシー及びその対策を見直す（添付資料Ｑ＆Ａ別紙２１参照）

【評価】技術的セキュリティについては、監査人補助員ＳＥによると、上記のとおり、現在の情報技術上、佐世保市のリクエストにつき、最新で高い技術が用いられており、早急に改善を要する部分は見当たらないということであった。

第９章　佐世保市庁舎内の情報セキュリティの現状４（運用面のセキュリティ）

第１　佐世保市における運用面のセキュリティ体制

これまで、佐世保市の情報セキュリティにつき、物理的セキュリティ、人的セキュリティ、技術的のセキュリティについて検証したが、最後に、運用面のセキュリティについて、各セキュリティの主体的な担当者とその運営状況について調査する。

佐世保市の情報セキュリティの担当部局は、本報告書第１７９ページの「情報セキュリティの運営監督責任」のとおりであるが、その中でも、電子情報の管理について、重要な業務を行う部署は、総務部情報政策課であ

る。そこで、以下、同課に佐世保市における情報セキュリティの運用面について報告を求めた結果につき呈示し、検証する。

第２　情報管理システム導入の具体的な内容

１　情報管理システム導入の経緯

佐世保市における情報管理システムは現在、市独自に制定された情報セキュリティポリシー（注 11）に基づいて運用されている。情報を取り扱う上で必須事項である『データを守る』という点において、例外なく佐世保市もその取り組みが行われていることを確認したことは、これまでの報告のとおりである。以下、一部重複する部分もあるが呈示する。

（１）情報管理の担当部局：総務部情報政策課

（２）情報を守る仕組み（情報セキュリティ）として

ア　情報の機密性（注 12）

イ　情報の完全性（注 13）

ウ　情報の可用性（注 14）

を十分な体制で運用、実現されているかの確認が必要である。

２　令和元年１０月からの新システム構築・運用について

佐世保市は令和元年９月まで使用していた「平成２６年構築の庁舎内情報管理システム全体」を、機器の老朽化と時代のニーズに伴いシステムの再構築を行った。その際にこれまでの運用状況と問題点、また近未来の情報活用（スマート化（注 15））やデータ解析による市民生活への活用等）を生かすべく長期間に渡り慎重なシステム仕様（ハード・ソフト共に）を作成

（注 11）　企業や組織において実施する情報セキュリティ対策の方針や行動指針のこと

（注 12）　情報が漏れないように管理することで ID やパスワードの設定や不正アクセスなどの防止等の対策を行う

（注 13）　管理している情報が正確で最新の情報であること。古いシステムなどでデータが陳腐化しないようにする

（注 14）　管理している情報をいつでも使用できる状態であることを示す。具体的にはデータの破損や消失を防ぐためにバックアップを行うことも可用性対策のひとつである

（注 15）　IT(ICT・IOT)におけるスマート化とは、状況に応じて蓄積されたデータを最適に運用し、人やモノ、施設等がネットワーク（主にインターネット）によって繋がり自治体全体がスムーズなサービスを受けられるデジタル社会を構築すること

し公募をかけたということである。監査人は、この時の公募の際、入札業者のプロポーザル資料を確認した。以下、この資料を基に述べる。

3　佐世保市が公募にあたり必要とした主な仕様

（1）市庁舎内イントラネット(注16)（全庁ＬＡＮ）をフル活用し、職員一人ひとりに端末が準備され目的とする業務をスムーズに展開し、市民への行政サービスを滞らせないシステム

（2）佐世保市情報セキュリティポリシーに基づいた機密性の高いセキュリティ対策システムの導入

（3）３６５日原則無停止で運用が可能な安定性と信頼性を備えた管理システム

（4）情報の質（種類）の変更に伴い新たな方式にも対応できるような柔軟性をもった環境を構築

（5）コストパフォーマンス(注17)に優れ、運用管理等において安定したランニングコストとトータルコストが低廉であること。

（6）機器及びシステム全般において３６５日の保守体制がとれるサービスを伴うこと。

4　導入された情報管理システムの詳細

佐世保市は、上記の仕様を基盤に、過去の経験値を基にした改善点と現状の課題を盛り込んだ観点から、公募のプロポーザル資料を判定し、業者を選定した。その結果、令和元年１０月に新たな情報管理システムが稼働した。

5　新情報管理システムの内部情報漏洩を防ぐ方策

（1）ＩＴ資産管理ソフトウェアを利用した内部情報管理（クライアント運

（注16）　組織単位で構成されるプライベートなネットワークで主に企業や組織内だけの情報を当該ネットワークで取り扱う仕組み

（注17）　ある事業に対しそれにあたっての費用（コスト）とその効果（パフォーマンス）を比較したもの。一般的に投じた費用に対しその効果や性能が期待を上回っているときは『コストパフォーマンスが高い』と評価される

用管理ソフトウェア／製品内容につき監査人補助員ＳＥにて性能を確認済み）を行っており、本庁舎のみならず各地域自治体の端末における情報管理も可能にしている。この仕組みを導入した目的として、各部局に配置された端末（クライアントＰＣ）及びそれを管理するサーバの情報（ハードウェア及びソフトウェア）や接続周辺機器（プリンター等）の動向を自動で収集し全市庁のＩＴ資産の運用を最適化する。

この内部情報管理により収集する情報の項目は、以下のとおりである。

ア　ハードウェア（代表的なもの）

（ア）端末機番号

（イ）コンピューター名

（ウ）ドメイン名（ワークグループ名）

（エ）システムモデル

（オ）システムシリアル

イ　ソフトウェア（代表的なもの）

（ア）ＯＳ[注18]インストール状況

（イ）アプリケーションインストール状況

（ウ）Ｏｆｆｉｃｅインストール状況

（エ）ウイルス対策ソフトウェアインストール状況

（オ）Ｗｉｎｄｏｗｓ更新プログラムインストール状況

上記の収集した各種情報により、各部局における運用状況をリアルタイムで把握が可能になり且つこの管理を一元化することにより管理部門（総務部情報政策課）の業務の効率化により業務負担の軽減化と省人化への効果も期待できる。

（２）端末機の挙動管理（ログ）による情報漏洩リスクへの対応

（注18）　オペレーティングシステム（Operating System）の略称でコンピュータのオペレーション（操作・運用・運転）を司るシステムソフトウェア Microsoft Windows、MacOS、Linux等

日々のクライアント端末パソコンの操作やネットワーク上での通信状況、または、ファイルやフォルダ、他のデバイスへのアクセス状況等を端末パソコンごとに、その挙動をログとして記録を行うことで、「いつ、誰が、どのような操作を、どの環境で行った」などの情報を正確に抽出することできる。その結果、内外部からの情報漏洩リスクへの対応を素早く行うことが可能になる。この佐世保市におけるログの取得・保存機能を検証するため、監査人補助員ＳＥにて、実際に、総務部情報政策課の協力の下、新情報管理システムの同機能を確認してみたところ、その一例として、以下のサンプルを採取した。

ア　市民生活部の戸籍住民窓口課の管理係Ａのクライアント ＰＣが　令和２年１２月１日ＡＭ１０：３０にサーバからＸという住民戸籍データを閲覧した。

イ　土木部道路整備課の工事事務所係のＢ担当者のクライアントＰＣからＹ土木建築会社のＫ氏宛に令和３年１月２０日ＰＭ１：３５に添付ファイル付きのＥメールが送信された。

ウ　サーバに保管されている観光商工部観光課の資料画像「＊＊＊．ｊｐｇ」が令和３年２月１０日ＰＭ５：１３に「Ｘ＊Ｘ．ｊｐｇ」にファイル名が変更された。

なお、このようなログは出先施設等の情報収集も同様に行われており、膨大なログデータが本庁の専用サーバで一元管理されている。更に外部からの攻撃等による障害発生時の調査用の備えとして、ログデータの長期バックアップの体制も整えられていた。

第３　ＩＴ資産管理ソフトウェアの運用

１　ＩＴ資産管理ソフトウェア導入

佐世保市は、上記新情報管理システムの一環として、情報資産管理ソフ

トウェアを導入した。

２　ＩＴ資産管理ソフトウェア視察

このソフトウェアにつき、監査人及び監査人補助員ＳＥは、総務部情報政策課の協力の下、管理モニター作動環境を仮設した状況を閲覧し、その仕様と実務性、リアルタイムな監視モニター等を確認した。このシステムの主な導入目的は、佐世保市が管理する３０００台強の端末機器に対し本庁の一元管理が可能とすることである。代表的な機能は以下のとおりである。

（１）ソフトウェアライセンス状況やＩＰアドレス、シリアル番号等の資産情報の収集

（２）端末機器の利用ログ（記録）の収集

（３）ＵＳＢ等の外部記憶媒体等の管理（利用制限）

（４）セキュリティ管理（ソフトウェア、ネットワーク等）

（５）管理者によるリモート接続メンテナンス（操作や説明等）

（６）ソフトウェア及び最新ドライバ等の一斉配信、自動インストール

（７）Ｗｉｎｄｏｗｓ１０の更新管理

（８）利用データの暗号化（情報持ち出し時のセキュリティ）

【評価】

１　特に今回の視察で、上記（３）の外部記憶媒体使用時の挙動検知に注目した。日々業務を行う中で必ず利用されるであろうＵＳＢメモリ等のデバイス(注19)やメディア（ＣＤやＤＶＤ等）であるが、管理者による使用制限の設定により読み取り専用、書き込み禁止はもちろん印刷を禁止する設定も可能となっていた。このことにより、部外への不要

（注19）　広義の意味でパソコンやタブレットやスマートフォン等の総称であるが、ここではそれらの機器に接続する周辺機器（外部記憶装置含む）を指す

なデータの持ち出しを抑制し、組織の運用に則した取扱いが可能となっていた。

2　また上記第３の２（１）（２）のような個別の端末装置のリアルタイムな運用状況（リモートによる画面確認可能）を監視し、かつ、必要な情報の取得、記録を可能にしている。このことで、端末の利用者の利用意識の有無に関わらず管理者は必要な時、個別に状況をモニターできようになり、業務外の不必要なアプリケーションの利用や不適切なサイト閲覧の抑止に役立っている。これらの機能は、内部セキュリティの脅威の原因となるウイルスや攻撃型マルウェアの侵入の危険性を低下させ、安全な業務体制を確立するという観点からは、高評価である。

3　そして端末全体の管理がなされているため、同時にソフトウェアの現在状況の確認が行えるためバージョンアップやセキュリティの最新パッチ（注 20）等の一斉配布によりシステムが常に最新状態を保つことができる。その結果、各部署は、情報セキュリティ責任者または担当者の手を煩わせることなく業務に集中できることとなる。

4　このように、ＩＴ資産管理ソフトウェア導入は、佐世保市全体で蓄積される情報全体に対し本庁にて一元集中管理することによって細部に渡り情報の漏洩の危険を回避しつつ、同時に、長期間積み重ねられている膨大な各部局の情報資産を守る有力な手段となっている。監査人補助員ＳＥの視点からも、このシステムの導入は佐世保市の思惑をしっかりとサポートしているとの評価であった。

第４　外部接続媒体の管理

１　外部接続媒体を管理する必要性

（注 20）　インストールされているアプリケーションのバグや機能の変更を行うためプログラムの一部を変更するための修正プログラムのこと

佐世保市において、適切な物理的セキュリティを導入し、また、情報機器とネットワークの実用時の管理体制を整えているとしても、職員による外部媒体の接続につき、その入口時点での情報漏洩リスク発生を予防する必要がある。特に、最新の外部接続媒体は、小型化が進み手軽に持ち運びが可能な上、大容量のデータ保存を可能にしているため、紛失等で機密情報が漏洩する確率も高くなっている。

対象として考え得る媒体は、以下のとおりである。

（１）対応可能なデバイス（パソコンに内蔵されるものも含める）

ア　ＵＳＢメモリ

イ　ＵＳＢハードディスク

ウ　カードリーダー／ライター

エ　ＣＤ／ＤＶＤ／ブルーレイディスクドライブ

オ　イメージスキャナー・デジタルカメラ

カ　モバイル端末

キ　ｅＳＡＴＡ接続ハードディスク（注 21）

ク　フロッピーディスク

（２）対応可能なメディア

ア　ＳＤカード

イ　ＤＶＤ－ＲＡＭ

ウ　ＭＯディスク

エ　コンパクトフラッシュ

オ　メモリスティック

カ　ｘＤピクチャーカード

キ　スマートメディア

（注 21）　内蔵ハードディスクのデータ転送速度が速い SATA（シリアル ATA）規格をそのまま外付けハードディスク向けに最適化した規格のこと

ク　マルチメディアカード

2　外部接続媒体の使用制限

佐世保市は、外部接続媒体に関する危険性を、新情報管理システムの管理機能によりデバイスごとに使用制限を設定することで万が一の漏洩事故に対処している。その例は、以下のとおりである。

（1）デバイス1台ごとに使用制限（部署ごとに「読み取り専用」や「使用不可」）設定を施し、目的と運用に応じた管理を可能にする。

（2）異なったネットワーク（セグメント）(注22) ごとに使用制限を設定し使用範囲を限定することによって不要な持ち出しの抑止を可能にする。

3　外部接続媒体の端末接続時の管理

外部接続媒体の接続状況は、佐世保市総務部情報政策課により管理されるパソコンによってリアルタイムに閲覧が可能となっている。システムの最新情報を把握できるためＯＳやアプリケーションのライセンス情報も確認し、常に最新のアップデートを行いながらセキュア (注23) な環境で業務を遂行できるようになっている。

第5　職員に対する制約

先述した「第5章　佐世保市内での情報施策に関する内規」、「第2　佐世保市情報資産取扱要綱」の9のとおりである。上述の新情報管理システムやＩＴ資産情報管理ソフトウェアによる総務部情報政策課主導の情報機器・ネットワーク管理、情報資産保全につき、各部署にて阻害する行為に及ばないことを主軸とする内容となっている。以下、総務部情報政策課による管理と職員への制約につき特筆すべきものを挙げる。

（注22）　ＩＴでは「区分」の意味を持ち、ネットワークにおけるセグメントとは、192.168.1.0/24、192.168.2.0/24などと分けられた各ネットワークのことを指す

（注23）　一般的には単なる「安全」なことを指すがＩＴではシステムやネットワークが保護されて「安全な状態」であることを意味する

1　組織が許可をしていないアプリケーション(注24)のインストールは禁止されている。これに反してのインストールは、新情報管理システムにより覚知され、無断にて端末パソコンに組み込まれることを予防している。

2　業務に関係のないＷｅｂサイト(注25)の閲覧や書き込みは禁止される。指定されたサイトのみの閲覧を許可される。

3　総務部情報政策課にて指定したフォルダへのアクセスがあった場合、それを検知し、総務部情報政策課にアラート(注26)通知される。

4　管理者が事前に設定したキーワードを含むファイルやフォルダが扱われた場合、それを検知し、総務部情報政策課に通知される。

5　業務時間外や休日等にクライアントパソコンが操作された場合、それを検知し、総務部情報政策課に通知される。

6　あらかじめ使用許可を受けたＵＳＢデバイス(ハードディスク、メモリ)やＣＤ、ＤＶＤ等のメディア以外の使用を禁止する。

7　許可されたメールアドレス以外のメール送信を禁止する。

8　許可されたサイト以外のデータのアップロード(注27)を禁止する

9　パソコン画面の保存（スクリーンキャプチャ）を禁止する。

第１０章　情報漏洩事故発生時の対処

第１　前論

監査人は、第９章まで、佐世保市の情報管理に関して、その担当部局、法令、各種セキュリティの現状等を精査した。特に、物理的セキュリティ、

(注24)　アプリケーションプログラムの略称で使用する業務に応じて作成されたプログラムのこと

(注25)　ここではインターネットなどで企業や組織が自身を紹介するために構築したウエブページの集まりのことを指す。ホームページとも呼ばれている

(注26)　システムがユーザーに対し誤った操作や禁止事項があった場合注意を促すために発する警告のこと指す

(注27)　ここではネットワーク上（インターネット含む）で自パソコンから相手側ホストコンピュータにデータを送ることを指す

技術的セキュリティは、電子自治体政策による国からの助成金等をもあり、良質なレベルを導入しており、また、その運営についても、新情報管理システムやＩＴ資産管理ソフトウェア等の基盤を備えたうえで、リスクを低減する方策を備えていたことを確認した。

もっとも、内部者による故意の情報流出や外部からのサイバー攻撃は、巧妙化し続けており、物理的・技術的な防御を突破する事態は皆無ではない。また、電子メールの誤送信やホームページ誤記等のヒューマンエラーによるリスクについては、従来の人的セキュリティに依存するところであり、過失によるものである以上、そのリスクは常に存在する。

そこで、佐世保市における情報管理につき、最後に、情報漏洩発生時の対処について検証する。

第２　情報漏洩時の基本的な対処

電子情報事故が発生した場合、佐世保市では、その対処として、発見者は、速やかに各部署の情報セキュリティ責任者、総務部情報政策課に報告する義務を負う。そして、その事故につき、佐世保市ＣＳＩＲＴが集中的に対処する。

情報漏洩の場合、漏洩により発生する損害の内容、漏洩の範囲を確認し、漏洩した情報の回収、被害者への報告と警戒依頼等のうえで、被害を抑制できない場合の事故情報の公開判断、さらに、再発防止策検討と実行という過程を踏むのが一般的である。これらの過程について、佐世保市は、佐世保市ＣＳＩＲＴ行動要領を定め、初動対応、復旧措置、報告・公表等に関する詳細を定めている。

第３　佐世保市における情報漏洩発生時の公開判断

１　公開判断の基準

監査人にて、佐世保市総務部情報政策課に対し、情報漏洩発生時の事故情報公開の基準を照会したところ、佐世保市ＣＳＩＲＴ行動要領にて、例外的に公表をしなくともよい場合を定めており、それ以外、原則的に公表するということであった。その基準は、以下のとおりである。なお、いずれの場合も、「公表しないことにより隠蔽等を疑われ、市の信頼を低下させることがないよう、適切な説明に努めるものとする。」との制約が課されている。

（１）個人情報の漏洩事故等であり、第三者に閲覧されることなく速やかに情報資産を回収した場合

（２）個人情報の漏洩事故等で、情報資産に対して高度な暗号化等の秘匿化がされている場合

（３）個人情報の漏洩事故等で、情報資産が漏洩等をした事業者以外では内容を識別することができない場合であって被害が生じるおそれがない場合

（４）個人情報の漏洩事故等で、漏洩等事案の影響を受ける可能性のある者全てに連絡がついた場合

（５）サイバー攻撃による事故等で、公表することでかえって被害の拡大につながる可能性がある場合

（６）その他最高情報セキュリティ責任者（ＣＩＳＯ／佐世保市長）が公表不要と判断する場合

２　上記規定の趣旨

上記規定は、事故情報につき原則公開としつつも、①初動措置や被害者の同意等により、実害発生を実質的に防いだり、損害について抑制した場合、もしくは、②損害発生につき防止に至らなかったが、さらなる損害拡大が予測される場合において、公開を行って得られる利益と公開を行わないことによる利益を比較衡量し、後者が上回る場合における非

公開を定めるものである。

ところで、上記の例外的な非公開事由については、その判断者が一見して不明であるのみならず、（６）が包括的な非公開事由となっており、構造上、非公開が例外的ではなく原則的となり得る構成となる可能性がある。

そこで、監査人は、佐世保市へ、上記規定につき添付資料Ｑ＆Ａ３４のとおり照会し、回答を受けた。結論として、情報漏洩事故を発生させた課のみの判断ではなく、総務部情報政策課長、総務部長、市長、副市長等の判断を交えることで、その恣意的判断を回避するとのことであった。

【意見】上記の非公開事由については、（６）により、佐世保市長の判断のみをもって、情報漏洩事故を非公開とする措置が可能となる。これについての制約は、「公表しないことにより隠蔽等を疑われ、市の信頼を低下させることがないよう、適切な説明に努めるものとする。」という文言と、佐世保市長以外の判断者の意見になるが、これらが佐世保市長の非公開判断に対して、いかなる影響力を与えるのかは全く不明であり、恣意的判断防止のための手続的な保障があるとは評価できない。上記規定の構造では、第２部の佐世保市の情報公開にて述べた情報公開制度の自己統治機能（国民主権、民主政、住民自治の達成、向上を目的とする機能）に強く反するものと評価されるおそれがある。実際に、情報漏洩が発生した場合、その事故情報の公開により、漏洩内容に関わる事実が表面化する以上、非公開により得られる利益がゼロという事例は稀有であり、これを過大評価して非公開決定を行う、または、部分的な公開が可能であるにも関わらず全面的非公開を行うという懸念は常に残る。加えて、例えば、情報漏洩が発生した際、あらゆる事情を斟酌した上で、上記（６）

による非公開決定とした場合、その決定が実際妥当であるとしても、上記規定の構造ゆえ、佐世保市長の恣意的判断によるものであるとの疑念が付きまとうという問題もある。

なお、かかる恣意的判断の懸念については、上記（２）の「高度な暗号化等の秘匿化がされている場合」、上記（３）の「事業者以外では内容を識別することができない場合」、上記（５）の「公表することでかえって被害の拡大につながる可能性がある場合」についても同様である。

そこで、上記規定については、以下のとおり改正することを検討されたい。

１　上記（６）の包括的規定については、上記（１）ないし（５）をもって十分ではないかを検討し、不要である場合には、端的に削除する。

２　仮に、上記（６）について存続させる場合、その余の上記（１）ないし（５）と併せて、①各非公開事項の具体例を定めておき、情報公開請求の対象となり得る形式（上記規定以外の別の内規等）にて定める。また、②各非公開事項に該当すると決定した場合、事後的に、情報公開審査及び個人情報保護審議会へその妥当性につき諮問するものとし、同審議会が非公開決定につき、全部または一部を取り消すべきとの結論を出した場合には、再度公開手続を行う等の手続保障を上記規定へ含める。

第１１章　佐世保市の情報管理の現状に関する総合的な評価及び意見等

第１　評価

佐世保市の電子情報セキュリティについては、上記のとおり、内規の整備、高品質の物理的セキュリティ及び技術的セキュリティ、これらのセキュリティにつき総務部情報政策課にて統括する運用体制を基盤とし、日常の公務に従事する職員が人的セキュリティを遵守するという方式である

ことが判明した。各部局へのアンケート結果のとおり、ハードウェアやソフトウェアの脆弱性を理由とする情報事故は発生していないことから、引き続き、ヒューマンエラーへの注意と将来のサイバー攻撃の進化への対応を維持されたい。

雑感としては、地方自治体において、情報漏洩が発生した場合、それは、ヒューマンエラーが原因であるものが大部分であるが、佐世保市以外の地方自治体にて実際に情報漏洩が発生した事例を思い起こすと、その報道後の一般人の印象として、地方自治体が膨大な重要情報を収集しているにも関わらず、これを脆弱なハードウェアやソフトウェアにて運用しているため漏洩したという印象に基づく意見が頻出していたように思われる。佐世保市としては、物理的セキュリティ及び技術的セキュリティの強化に努めていることについては、佐世保市民からの信頼獲得のためにも適宜説明することも必要であろう。

【評価】佐世保市の物理的セキュリティ、人的セキュリティ、技術的セキュリティ、運用上のセキュリティは、総じて適切と評価できる。物理的セキュリティ及び技術的セキュリティを強化していることについては、適宜、佐世保市民あての広報も必要と思われる。

第２　意見

上記各章にて個別に述べた意見以外のものとして、以下のとおり述べる。

今回の佐世保市の情報管理に関しての監査で自治体の様々な情報やデータを管理する仕組みについて、監査人は、適切な機器と技術を用いて構築していることを理解することができた。そして、この技術は佐世保市のような大規模な自治体をセキュアに管理・運営するための緻密に構築されたものであった。特に、情報資産の運用から管理までを統合型システムと

して構築している点は、民間企業においては珍しいと思われる。この点、情報管理セキュリティの重要性については、民間企業や組織においても、軽視してはならないものである。すなわち、情報漏えいの危険性や機器の不具合をいち早く察知し如何に業務停止時間を短縮できるかの問題は、人的、物理的コストを削減し、かつ、セキュアな環境で毎日の業務遂行実現のための不可欠な要素となっている。佐世保市において、高度に実現している

①　日々のネットワーク端末の挙動管理（ログ）

②　組織内部でのネットワークの通信状況の管理

③　メール経由の情報漏洩防止

④　各種メディアやデバイスの情報管理

については、民間企業においても当てはまる重要な管理要素となっているはずである。

※情報セキュリティ１０大脅威２０２０

順位	組織内でのセキュリティ脅威	前年順位
1位	標的型攻撃による機密情報の窃取	1位
2位	内部不正による情報漏えい	5位
3位	ビジネスメール詐欺による金銭被害	2位
4位	サプライチェーンの弱点を悪用した攻撃	4位
5位	ランサムウェアによる被害	3位
6位	予期せぬIT基盤の障害に伴う業務停止	16位
7位	不注意による情報漏えい（規則は遵守）	10位
8位	インターネット上のサービスからの個人情報の窃取	7位

9位	IoT機器の不正利用	8位
10位	サービス妨害攻撃によるサービスの停止	6位

（資料　ＩＰＡ情報処理推進機構）

上記の情報処理推進機構（ＩＰＡ）[注28]の令和２年の情報セキュリティ脅威ランキングでも分かるように組織内の「内部不正による情報漏えい」が前年順位５位から２位に一気に浮上している現実から、内部関係者による情報の持ち出し、またはパソコンの誤操作や誤送信等で重大な「情報漏えい」事故を起こす頻度も高くなっている。

これへの対処として、人的セキュリティの一環として、組織のセキュリティルールをがんじがらめに設定し、事故発生時の罰則を重くするという流れがある。これは、民間企業において、物理的セキュリティや技術的セキュリティへ投資する余力が無いこと、また、経営権者の情報基礎リテラシーが欠如していること等が原因であるが、かかる方策に頼った結果、従業員の情報基礎リテラシーの停滞（情報基礎リテラシーが高い従業員または向上を希望する従業員は、物理的セキュリティ等を向上させない企業への帰属を希望しない。）とその結果による事故発生リスクの増大、そして、事故発生時の被害拡大を生み出す原因にもなりかねない。その対策として上記①に代表されるログを管理することによる抑止対策が大きな効果を発揮する力となり得る。

管理体制で大切なことは、不審な動きが発生した際の「リアルタイム」な警告と「操作ログ検索条件の充実」である。ただし、ログ項目の保存条件によっては莫大なデータを蓄積することになるためハイスペックな機器購入が必然となる。その上で費用対効果を十分に精査し当該組織に於いて

（注28）　独立行政法人情報処理推進機構（Information-technology Promotion Agency Japan）の略称で国家戦略としてITの技術面、人材面から日本を支えるために設立された独立行政法人

最適なプランを構築する経験値を高めていく必要がある。これにつき、佐世保市は、電子情報セキュリティの目的設定から、これを充足するシステム導入にあたっての公募、そして、導入後の運用を適切に行った。その結果、がんじがらめの人的セキュリティ設定という事態の回避に成功しており上記評価どおりの成果を得ているといえる。これは、民間企業においては、容易に入手、達成できない経験値である。

第２部の情報公開にて述べたとおり、佐世保市は、産業の停滞、市民の可処分収入の減退という事情があり、市内の商業活動において、情報化社会の間断無き進化に伴う情報セキュリティへの対応を必要としながら、物理的セキュリティや技術的セキュリティに投資する余力が十分ではない業者が少なくないと推測できる。佐世保市の情報セキュリティに関する経験値については、そのままの状態で、即座に大企業、中小企業、個人も参考にできるとは限らず、また、セキュリティという性格上、その経験や実績を容易に公表できるものではない。それゆえ、佐世保市にて蓄積している情報セキュリティの経験値を詳細に民間に示すことは不可能と思われるが、本報告書で記載している事実の範囲で、佐世保市が、情報セキュリティを重視していること及びその理由並びに佐世保市として上記①ないし④を達成していることについて、佐世保市民や企業向けに示し、民間における情報セキュリティへの関心を啓発していくことは有益であると思われる。

また、監査人は、本監査の過程で、将来の佐世保市の政策として、小中学生へのパソコン配布やリモート授業の強化が検討されていると聞いているが、未成年の学生に対して、情報セキュリティの問題を入口とする情報基礎リテラシーの教育、さらに、この部分からセンシティブな情報に関する教育へと繋げるという手法も考えられるだろう（例えば、児童ポルノやリベンジポルノの問題についても情報基礎リテラシーの著しい欠如が原因の一部を占めていると思われる。違法または不適切な写真画像等の作成自

体無論大問題であるが、かかる事案は、加害者も被害者も情報基礎リテラシーがほとんど無いという特徴があるのではないだろうか。)。その際、佐世保市が行っている情報セキュリティについては、実際に運用されていることから、これも本報告書記載のレベルであれば、具体的かつ分かりやすい教材となり得ると思われる。

【意見】

佐世保市の情報セキュリティ構築にあたり、本報告書にて評価とした部分についての実績に基づき、その経験値を活用するため、佐世保市民及び佐世保市内の民間企業に対して、情報セキュリティ、情報基礎リテラシーの重要性を啓発し、また、未成年者への教育のサンプルにする等して、総務部情報政策課にて学校への出前授業を推進する等していただきたい。

第１２章　第２部及び第３部を通じての監査人の感想等

第１　情報公開と情報管理

監査人にて今回行った情報公開と情報管理は、いずれも佐世保市が管理する情報資産に関わる手続である。この内、情報公開は、法律、条例の存在を重要な要件としつつ、さらには、その考察にあたっては、日本国憲法の表現の自由（知る権利）に及ぶ必要があり、実際の手続も、もっぱら情報の公開請求者と実施機関の担当者という人による判断と作業により大部分占められるものである。他方、情報管理は、各端末とネットワーク網に止まらず、新情報管理システム等の高度の統括用機器やソフトウェアの導入により、情報技術の高速の進化に対応した機器と技術が、佐世保市内で比重を大きくしている電子情報管理を支えている。

情報の作成、収集、保管及び廃棄という管理の過程では、今後も間断無

い進化を続ける情報技術（この分野は、監査人として、つとに法律の分野による規制等が現実に追いつかない部分があると思われる。）により支えられるところと予測されるが、他方で、情報の使用の一場面である情報公開の分野では、将来的には、ＡＩ導入による情報公開のシステム化が図られるかもしれないが、その実現性は全く不明である（注29）。それゆえ、当面は、情報公開は、人手に頼る部分が続くと予測できる。

情報公開と情報管理を同時に監査した結果、佐世保市は、主に、紙媒体の文書を総務部総務課、電子情報を総務部情報政策課へ担当させ、さらに、その事務処理につき紙媒体の文書管理に類する情報公開制度を総務部総務課の統轄とすることで、事務処理の効率化と重複防止を達成している。監査の過程で、両課の適切な協同も確認することがあった。両課には、本報告書の意見につき活用するとともに、例えば、情報管理につき事故発生時の公開判断については、情報公開にて述べた情報公開制度の自己統治の理念が関係していること等、両分野につき「情報」という媒体の共通性から、相互に留意すべきものがあることについても記憶に留めていただきたい。

第２　意見及び評価等

情報公開及び情報管理につき、広く条例、内規を調査し、過去の事例や事務処理の現状について確認した結果、

１　情報公開につき、２６件の意見及び５件の評価

２　情報管理につき、８件の意見及び９件の評価

を呈示した。法令に抵触しているとの判断に至るものはなく、意見につい

（注29）もっとも、ＡＩ開発は、訴訟活動や行政活動にも広く研究が進められており、裁判においては訴状等の作成、行政活動においては、情報開示についてもＡＩ導入による自動化研究が進んでいるとのことである

ても、概ねさらなる改良を求めるものが少なくなかったが、特に、情報公開については、佐世保市において、自己統治という本来の機能が果たされておらず形骸化していると評価されかねないという根本的問題、情報管理については、情報漏洩事故発生時の非公開決定判断について、その内容によっては、法令抵触を指摘される懸念もあるところである。監査人としては、これらについては、特に、佐世保市にて真摯に改善検討を求めるところである。

評価として示した佐世保市のこれまでの努力により得た成果のうえに、さらなる佐世保市の住民自治の発展と佐世保市民の主権者としての意思向上、そして、情報管理事故の防止強化へ繋がるように、本報告書の結果を役立てていただければ幸甚である。

【添付資料】

佐世保市情報セキュリティポリシー

（目的）

第１条　このポリシーは、市において作成し、又は収受した情報に対し、情報セキュリティを適切に維持するための基本方針並びに管理及び運用方針を定めることにより、情報の適正な管理及び円滑な運用を図ることを目的とする。

（定義）

第２条　このポリシーにおいて、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

⑴　実施機関　市長、教育委員会（小・中学校を除く。）、選挙管理委員会、農業委員会、公平委員会、監査委員、市議会及び固定資産評価審査委員会並びに消防長及び公営企業管理者をいう。

⑵　情報　佐世保市情報公開条例（平成１３年条例第４号）第２条第２項及び佐世保市議会情報公開条例（平成１３年条例第３５号）第２条第１項に規定する情報をいう。

⑶　情報セキュリティ　情報資産の機密性、完全性及び可用性を維持することをいう。

⑷　機密性　情報の利用及び閲覧（以下「利用等」という。）を行うことを許可された者だけが利用等をできることをいう。

⑸　完全性　情報の処理方法が正確かつ安全であることをいう。

⑹　可用性　許可された者が必要なときに情報の利用等をできることをいう。

⑺　サーバ　ネットワークを利用することで、端末機等へ業務システムが保有する機能やデータを提供するコンピュータをいう。

⑻　端末機　コンピュータとデータの収受を行うパーソナル・コンピュータをいう。

⑼　文書情報　情報のうち紙媒体で作られるものをいう。

⑽　電子情報　情報のうち電子的方式で作られるものであって、サーバ及び端末機等による情報処理の用に供されるものをいう。

⑾　ネットワーク　サーバ及びコンピュータ等間でのデータ収受を行う基盤をいう。

⑿　情報システム　サーバ、ネットワーク及びコンピュータ等を利用し業務を処理するための仕組みをいう。

⒀　情報資産　次に掲げるものをいう。

ア　ネットワーク、情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

ウ　情報システムの仕様書及びネットワーク図等のシステム関連文書

エ　実施機関の職員が作成し、又は取得した文書情報であって当該実施機関が組織的に用いるものとして保有しているもの

⒁　情報系端末　佐世保市行政情報ネットワークに接続するため、情報政策課により配付される端末機をいう。

⒂　各課端末　各課かいが所管し、庁舎内で使用する目的で導入される端末機をいう。

⒃　モバイル端末　各課かいが所管し、庁舎外に持ち出して使用する目的で導入される端末機をいう。

⒄　端末機等　情報系端末、各課端末及びモバイル端末の総称をいう。

（情報資産に対するリスク）

第３条　情報資産に対するリスクを最小限に留めるために、次に掲げる事項か

ら情報資産を守らなければならない。

⑴　権限のない者による情報資産の破壊、盗難若しくは不正アクセス又は不正操作による情報資産の破壊、改ざん、消去等

⑵　権限のある者による情報資産の無断持出、誤操作、認証情報の不適切な管理若しくは不正行為又は事故による情報資産の破壊、改ざん、消去、漏えい等

⑶　コンピュータウイルス、地震、落雷、火災、停電若しくはそ害等の災害又は事故による業務の停止

（適用範囲）

第４条　このポリシーは、実施機関のすべての職員（特別職を含む。以下「職員等」という。）及び実施機関が保有する情報に適用する。

（職員等の責務）

第５条　職員等は、情報の取扱いに関して、不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）、著作権法（昭和４５年法律第４８号）、佐世保市個人情報保護条例、佐世保市特定個人情報の保護等に関する条例等の関係法令（平成２７年条例第３５号）等を遵守しなければならない。

２　職員等は、情報セキュリティの重要性について共通の認識を持つとともに、情報の適正な管理に努めなければならない。

３　職員等は、情報の秘密を保持するとともに、情報を業務目的以外で収集し、又は使用してはならない。

４　職員等による不正行為が明らかになった場合は、当該職員等を地方公務員法等の関係法令又は本市例規に基づいて処分する場合がある。

（組織）

第６条　市において作成し、又は収受する情報資産について、情報セキュリティの適正な管理及び円滑な運用を推進するための組織を設置する。

（情報資産の分類と管理）

第７条　実施機関は、保有する情報資産について、機密性、完全性及び可用性に応じて分類し、その重要度に応じた情報セキュリティ対策を行わなければならない。

（情報セキュリティ対策）

第８条　実施機関は、第３条各号に規定する脅威から情報資産を保護するために、次の各号に掲げる情報セキュリティ対策を講ずるものとする。

⑴　物理的セキュリティ対策　情報システムを設置する施設、通信回線及び職員等の端末機等の管理について、物理的な対策を講ずる。

⑵　人的セキュリティ対策　情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、情報資産を利用する全ての者に情報セキュリティポリシーの内容を周知徹底するための教育及び啓発を行う等の人的な対策を講じる。

⑶　技術的セキュリティ対策　端末機等の管理、アクセス制御、不正プログラム対策、不正アクセス対策、通信環境の分割等の技術的対策を講じる。

⑷　運用面のセキュリティ対策　情報セキュリティポリシーの実行性を確保するため、情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等の運用面の対策を講じる。

（情報セキュリティ監査及び自己点検の実施）

第９条　ポリシーの遵守状況を検証するため、定期的に情報セキュリティ監査及び自己点検を実施する。

（ポリシーの見直し）

第１０条　情報セキュリティ監査及び自己点検の結果、ポリシーの見直しが必要となった場合又は情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、ポリシーを見直すものとする。

（教育）

第１１条　情報の取扱いに関する教育・研修の実施を計画し、その結果を情報

セキュリティ委員会に報告する。

（委任）

第１２条　このポリシーの目的を達成するために必要な具体的な遵守事項及び判断基準等は、別に定める。

附　則

このポリシーは、平成１６年　６月　１日から施行する。

附　則

このポリシーは、平成１６年１０月　１日から施行する。

附　則

このポリシーは、平成１７年　４月　１日から施行する。

附　則

このポリシーは、平成１８年　８月２４日から施行する。

附　則

このポリシーは、平成１９年　４月　１日から施行する。

附　則

このポリシーは、平成２０年　７月　１日から施行する。

附　則

このポリシーは、平成２１年　６月　１日から施行する。

附　則

このポリシーは、平成２８年　１月　１日から施行する。

附　則

このポリシーは、平成３１年　４月　１日から施行する。

【添付資料】監査人からの佐世保市各部署への人的セキュリティに関するアンケート質問事項

※便宜上、質問事項が始まる「第２」からの番号となる。

第２　貴部署での情報管理について

１　貴部署で管理する情報の内、その余の情報と区別された、「強度のセキュリティを要すると特別の重要情報」が存在しますか。そのような情報がある場合、差支えが無ければその種類を教えて下さい。

２　日常の情報セキュリティにつき、高度情報ネットワーク（ＩＴ）技術の進化は、日進月歩であり、ある技術やその知識が短期間で旧式化してしまうことがあります。貴部署において、情報セキュリティの知識につき、有識者の確保等に問題を感じることはありますか。

３　貴部署において、情報セキュリティ上の問題が発生したことはありますか。時期、それに対する対処状況等含め、ご教示下さい。

第３　情報セキュリティガイドブックについて

１　貴部署内における情報セキュリティガイドブックの活用状況を教えて下さい。

２　実際に、貴部署内にて、情報セキュリティガイドブックが利用されている頻度を教えて下さい。

３　情報セキュリティブックについて、貴部署において、希望等あれば教えて下さい。

第４　佐世保市の情報セキュリティに関して

１　佐世保市における電子情報管理等情報セキュリティにつき、貴部署にて、

佐世保市に対するリクエスト、提案等があればご教示下さい。

2　その他、佐世保市における電子情報管理等情報セキュリティに関して、貴部署にて、気づき、懸念等ありましたらご教示下さい。

第５　情報漏えいに対する質問

以下の情報セキュリティ上の脅威の類型につき、貴部署が注目ないし留意しているものがありましたら、教えて下さい。

①　標的型攻撃による被害

特定の組織内の情報を狙って、ウイルス添付電子メールを送信する等して行われるサーバ攻撃

②　ビジネスメール詐欺による被害

国内外の企業や組織の上位者を装い、情報開示や金銭支払いを求める偽メール等

③　ランサムウェアによる被害

感染したパソコン等をロックまたは情報暗号化を強行し、身代金を要求

④　サプライチェーンの弱点を悪用した攻撃

製品やサービス提供の一連のビジネス上の流れにおいて、比較的セキュリティが強固な上位組織を目標として、セキュリティが手薄な取引先や関連団体への攻撃をしかけ、そこを踏み台にして上位組織を狙う攻撃

⑤　内部不正による情報漏えい

団体の内部の者が利益取得や団体への反意等により管理情報を漏えい

⑥　サービス妨害攻撃によるサービスの停止

大量のデータ送信やアクセス等によるサーバ過負荷を実現し、相手方のインターネットを利用したサービスを使用不能にさせる

⑦　インターネットサービスからの個人情報の窃取

　個人情報等をホームページより閲覧できる状態にし、誤って電子メールにて送信等する管理ミスにより個人情報を窃取される

⑧　ＩｏＴ機器の脆弱性の顕在化

　ＩｏＴ機器（インターネットと接続された家電等）がセキュリティ能力につき劣ることを狙い、遠隔操作が可能となるマルウェアに感染させ、踏み台と二次被害を発生させる

⑨　脆弱性対策情報の公開に伴う悪用増加

　ソフトウェアの脆弱性への警告や対処依頼のため公開されることにより、その脆弱性対策を行っていないシステムへの公開情報を悪用した攻撃が行われる

⑩　不注意による情報漏えい

　情報取扱者の不注意による情報漏えいと二次被害等

以上

添付資料　　情報管理に関してのＱ＆Ａ（全 55 項目）

Q1
情報管理について（ア.担当部局）
A1
別紙 1-5 の(2)-ア　総務部情報政策課が管理している
Q2
情報管理について（イ.貴庁内での情報セキュリティのため行っている活動）
A2
別紙 1-5 の(2)-イ以下を参照
Q3-Q5
情報管理について（ウ.情報セキュリティにつき外部業者への委託を行っている場合にはその契約内容） 1.佐世保市が保有する電子情報管理について 2(1)佐世保市の情報セキュリティ対策に係る業務委託 2(2)佐世保市が情報セキュリティ対策策定及び実施の全部または大部分を外部業者に委託しているパターンについて
A3-A5
別紙 1-5 の(2)-ウ以下を参照

Q6
総合行政ネットワークはいつからあるのか
A6
別紙 6-8　2-①を参照
Q7
ファイルサーバの全保存領域と使用量はどのくらいか
A7
別紙 6-8 2-②を参照
Q8
事故件数はどのくらいあるのか
A8
別紙 6-8　2-③を参照
Q9
庁舎全体の情報の流れを把握で図（業務フロー図）の入手
A9
別紙 9①～9②フロー図サンプルを参照
Q10
フロー図に基づくデジタルデータの取り扱い部分と、それを管理するデバイスの名称
A10
別紙 9①～9②フロー図サンプルを参照

Q11
庁内データベースを管理する機器の詳細情報
A11
別紙 11　2 のデータベースを管理する機器の詳細情報を参照
Q12
情報管理（個人情報とそれ以外）に使用する主な業務システムとアプリケーション及びネットワーク方式
A12
別紙 12　4.情報管理（個人情報とそれ以外）に～を参照
Q13
各部署で使用している現行セキュリティソフトウエア又はハードウエアセキュリティの名称
A13
別紙 13　5.各部署で利用している～の機種名欄を参照
Q14
A13 における導入当初の初期費用額（イニシャルコスト）また保守費用（ライセンス料等）を含めた年間維持費額（ランニングコスト）
A14
別紙 13　5.各部署で利用している～の各費用欄を参照

Q15
情報管理機器及びソフトウエアを含む各システムの購入先（ベンダー名、代理店名）
A15
別紙 15　7.情報資産管理機器～を参照
Q16
A15 におけるシステムの稼働率と評価（満足度及び不足点） （例）省人化の目的への達成率等
A16
別紙 16　8.7.におけるシステムの稼働率と評価～を参照
Q17
現稼働システムにおける直接運用スタッフのシステム内容の認知度と操作における教育内容の充実度（マニュアル作成等）
A17
別紙 17-1、2 9.現稼働システムにおける～を参照
Q18
庁内管理情報における情報漏洩発生防止の対策と漏洩発生時の対応 （情報漏洩インシデント対応策）
A18
別紙 18 抜粋 10.庁内管理情報における情報漏洩発生防止の対策を参照

Q19
令和2年度より始まる佐世保市ＩＣＴ戦略案について、情報セキュリティに関して特別に留意している事項があればご教示ください
A19
別紙19抜粋　佐世保市ＩＣＴ戦略令和2年4月版を参照
Q20
佐世保市情報セキュリティポリシー第9条について 情報セキュリティ監査及び自己点検を「定期的に」実施するとありますが、どの程度の間隔で情報セキュリティ監査及び自己点検をしているか、また、いかなる監査及び自己点検を行っているのかについて、過去の実施日及び結果を教えて下さい。
A20
（情報セキュリティポリシー） 第9条　ポリシーの遵守状況を検証するため、定期的に情報セキュリティ監査及び自己点検を実施する。 （情報資産取扱要綱） 第109条　電子情報セキュリティ監理者及び情報セキュリティ責任者は、所管するネットワーク及び情報システムについて、定期的に自己点検を実施しなければならない。 情報セキュリティ責任者は、所管する課かいにおける情報セキュリティポリシーに沿った情報セキュリティ対策状況について、情報セキュリティ取組状況確認表（様式1）を用いて、定期的（年4回）に自己点検を行わなければならない。

(1)自己点検について

①実施方法

・情報セキュリティ取り組み状況確認表のとおり

②実施頻度

・年4回実施（4半期に一度）するものとしております

(2)情報セキュリティ監査について

（情報資産取扱要綱）

第101条　設定したセキュリティレベル並びにセキュリティレベルに対応した各課かいの管理及び運用について、定期的（年1回）に、佐世保市情報セキュリティ監査実施要領（平成17年9月1日施行）に基づき実態を監査しなければならない。

①実施方法

ａ．共同監査・内部監査

・共同監査の説明資料（別紙20-2）

・情報セキュリティ監査チェックリスト（別紙20-3）

・情報セキュリティ発見事項報告書兼是正処置計画報告書

②過去の実施日および実施結果

・情報セキュリティ監査の実施一覧表

・情報セキュリティ監査に係る内容別指摘事項一覧表

Q21
佐世保市情報セキュリティポリシー第１０条について 平成 16 年 6 月 1 日、同年 10 月 1 日、平成 17 年 4 月 1 日、平成 18 年 8 月 24 日、平成 19 年 4 月 1 日、平成 20 年 7 月 1 日、平成 21 年 6 月 1 日、平成 28 年 1 月 1 日及び平成 31 年 4 月 1 日のポリシー変更施行につき、「ポリシーの見直し及び情報セキュリティに関する新たな対策が必要となった事情」及び「実際に見直したポリシーの内容」についてご教示下さい。
A21
（情報セキュリティポリシー） 第 10 条　情報セキュリティ監査及び自己点検の結果、ポリシーの見直しが必要となった場合又は情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、ポリシーを見直すものとする。 情報セキュリティポリシーの見直し時期および内容については、別紙のとおりです。別紙 21 参照
Q22
佐世保市情報セキュリティポリシー第 11 条について これまで実行した情報の取扱いに関する教育・研修の実施状況につき、情報セキュリティ委員会への報告結果を教えて下さい。
A22
（情報セキュリティポリシー） 第 11 条　情報の取扱いに関する教育・研修の実施を計画し、その結果を情報セキュリティ委員会に報告する。

(1)教育・研修の実施状況について

「別紙 22-1」のとおりです。

(2)情報セキュリティ委員会への報告結果について

「別紙 22-2」のとおりです。

Q23

情報資産取扱要綱第 20 条(1)について

電子情報につき、定期的にバックアップデータを作成しなければならないとされていますが、バックアップデータ作成の方式とその媒体種類、フォーマット等を教えて下さい。

Q23

（情報資産取扱要綱）

第 20 条　情報セキュリティ責任者は、情報資産の分類に従って、情報資産を適切に管理しなければならない。セキュリティレベルがⅠ・Ⅱ類については、以下の管理を行わなければならない。

電子情報については､定期的にバックアップデータを作成しなければならない。

(1)外部民間データセンター利用等（住民情報等）

データセンター内に複数筐体（ディスク）へのバックアップをリアルタイムに実施しています。(別紙 23-1 参照)

さらに、遠隔地バックアップとして、別データセンターおよび非常時対応用として、本市サーバ室内にバックアップ設備を配置しています。

Q24
情報資産取扱要綱第 23 条第 3 項について 住民に公開する情報資産について、完全性を確保しなければならないとされていますが、ここで謳われている「完全性」の定義について教えて下さい。また、この完全性確保のための具体的施策を教えて下さい。
A24
（情報資産取扱要綱） 第 23 条　セキュリティレベルⅡ以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない 情報セキュリティ責任者は、住民に公開する情報資産について、完全性を確保しなければならない。 (1)完全性の定義について 佐世保市情報セキュリティポリシー第 2 条(5)において、「情報の処理方法が正確かつ安全であることをいう。」と定義しております。 これは「情報が破壊、改ざん または 消去されていない状態を確保すること」ものと考えており、正確（間違っていない）で完全（不足のない）であることを保持するものです。 (2)完全性を確保するための具体的施策について 本市では、主に以下の対策を実施しております。 ①アクセス権管理（改ざん・消去） ユーザーおよびコンピュータ単位にアクセス権を付与しており、権限のないデータ等へのアクセスを技術的に禁止しております。 ②データの整合性チェック（バックアップ・破壊・消去） システムの完全二重化により、万一データが削除された場合に

おいても、14日前までのデータを保持しております。破壊・削除があった場合においても、瞬時に復旧が可能なものとしております。また、バックアップデータについては、正⇔バックアップに誤りがないか、ログなどにて確認できる状態としております（異常があれば、管理者へ通知を発します）

③アクセスログ管理（改ざん）

庁内のネットワークに接続されている端末は、全て操作ログを取得し、保持しております。これにより、改ざん等があった場合によっても、発生源等の特定を迅速に行える状態としております。また、これらの管理については、専門的な技術を保有するシステム運用管理事業者と連携し実施しております。

④マルウェア対策（改ざん）

庁内ナットワーク接続されているパソコン等は、全てにマルウェア対策ソフトウェア（統合型ウィルス対策ソフト）を導入しております。これにより、外部からのマルウェア侵入を未然に防ぐ等の対策をしております。

Q25
情報資産取扱要綱第65条について 無線LAN（アクセスポイント）を設置している部署と無線規格の種類を教えて下さい。
A25
（情報資産取扱要綱） 第65条　電子情報セキュリティ監理者及び情報セキュリティ責任者は、無線ＬＡＮの利用を認める場合、解読が困難な暗号化及び認証技術

の使用を義務づけなければならない。電子情報セキュリティ監理者及び情報セキュリティ責任者は、機密性の高い情報を扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

※本項については、その他、佐世保市より回答を受けた部分があるが、情報セキュリティ上秘匿するべき内容となっていたため、本報告書では省略する。

Q26

情報資産取扱要綱第 72 条第 3 項について

情報セキュリティ責任者が、業務上庁舎外に持ち出すモバイル端末を導入する際、使用許可された者以外の者が電子情報を参照できない仕組みを構築しなければならないとされていますが、現時点でどのような仕組みが構築されているかをご教示下さい。

A26

（情報資産取扱要綱）

第 72 条　電子情報セキュリティ監理者は、情報系端末の技術的管理において、次に掲げる業務を行わなければならない。

情報セキュリティ責任者は、業務上庁舎外に持ち出すモバイル端末を導入しようとするときは、暗号化やパスワード等により、当該モバイル端末の使用を許可された者以外が電子情報の参照等をできない仕組みを構築しなければならない。

(1)使用許可された者以外の者が電子情報を参照できない仕組みについて

個人情報や業務情報の持ち出しはしておらず、外部でのセミナー実施等での利用が主な用途となります。セキュリティへの対応としては、ＩＤやパスワードによるログイン管理および、端末の暗号化による保護を実施しており、第三者が容易に内容を閲覧できないよう対策しています。また、本対策は、持ち出しパソコンに限らず、庁舎内で利用するパソコンも同様に適用しております。
Q27
セキュリティガイドブックに関する質問 1 「2-1-4　情報を保管する」 電子情報のバックアップにつき、保管方法（場所、媒体、バックアップ方法、頻度設定）が適切になされているかの確認をどのように行っているかを教えて下さい。
A27
(1)電子情報のバックアップ状況の確認について 「自己点検」および「情報セキュリティ監査」の実査により確認を行っております。 ・情報セキュリティ取組状況確認表「項.データ管理」（別紙 27 参照） ・監査チェックシートの「No.4-1-1」別紙 27 参照

Q28
セキュリティガイドブックに関する質問 2 「3-3　情報を守る（バックアップ)」 　全庁ファイルサーバ等の活用に関して、「B 環境 0 ドライブ」とはいかなるものかを教えて下さい。
A28
(1)自治体情報セキュリティ強化対策事業の概要について 　佐世保市では自治体情報セキュリティ強化対策事業により、平成 29 年 1 月から庁内のネットワーク環境を、マイナンバー系(A 環境)、LGWAN 系(B 環境)、インターネット系(C 環境)の 3 つに分割しております。別紙 28-1 参照 (2)B 環境 0 ドライブについて 　各職員毎に LAWAN 系(B 環境)に割り振られているデータの保存領域のことです。
Q29
セキュリティガイドブックに関する質問 3 「3-4　情報を守る（ウイルス対策)」 　ウイルスが見つかったときの一般的な対処方法に関して、「1.LAN ケーブルを抜きネットワークから切断し、情報政策課に報告を行う」とされています。Wi-Fi 利用のデバイス（PC、タブレット、その他モバイル端末）に対しての対策について、ご教示下さい。

A29
(1)Wi-Fi 利用デバイスのセキュリティ対策について 庁内の Wi-Fi については、一部試行的に導入を行っております。庁内 Wi-Fi 専用の管理システムを導入しており、管理者から一元的にネットワークへの接続状態を確認できるようになっております。 よって、情報政策課に報告があった際は、情報政策課にてネットワークからの切断作業を行うようにしております。 また、ウィルス対策ソフトウェアについては、検知と同時に管理者へメール発報がされる仕組みとなっているため、連携して迅速な対応が取れるような体制となっています。(別紙 29-1 参照)
Q30
別紙 11 では、仮想サーバ 20 台となっているが、別紙 15・3 ページの D 項目-1 ハイパーバイザーソフトウェア（Vmware 社　扇精光ソリューションズ納入）では数量が 27 となっています。庁舎内で構築されているサーバの台数及び仮想サーバのトータルの数量と情管 15 の情報に差異がある理由を教えて下さい。
A30
(1)ハイパーバイザーソフトウェアの数量の差異について ハイパーバイザーソフトウェアについては、購入するライセンス形態が利用ユーザーライセンス方式（ユーザーCAL：クライアントアクセスライセンス）となっております。 本ソフトウェアは、数量 1 式あたり 100 ユーザーが利用可能なものであることから、全職員等を対象とし、100 ユーザー×27 式＝計 2,700 ユーザーライセンスとして購入を行っているものです。

よって、「サーバ台数：20 台」と「ハイパーバイザーソフトウェア数：27 式（2,700 ユーザー)」に差異が生じております。

Q31

別紙 12・3 ページ第 29 項の市民アンケートシステム（個別開発）につき、「個別」とは誰が開発したのかを教えて下さい。

A31

(1)市民アンケートシステム（個別開発）の開発者について

本システムの開発は、株式会社日本ビジネスソフト社（佐世保市三川内新町）が開発したソフトウェアとなります。

(2)市民アンケートシステムの概要について

本システムは、市民へのアンケートを実施する際、宛名ラベルを作成するシステムです。一定の条件（年齢・性別等）からランダムに抽出し、一覧表を作成します。

Q32

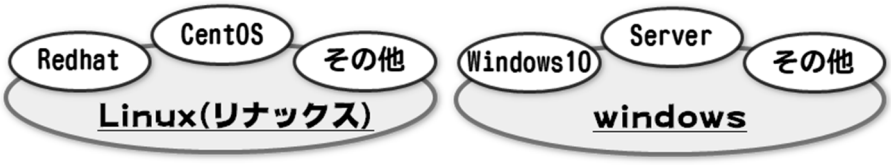
別紙 15・3 ページ D 項の Redhat システムは Linux サーバシステムと認識してよいのか、それとも単なる OS であるのかを教えて下さい。

A32

(1)Redhat システムについて

Redhat システムは、LinuxOS（オペレーティングシステム）の一つとなります。

イメージ図



Q33

別紙15・4ページのウイルス対策ソフトの数量は3,118となっていますが、別紙11のサーバ、仮想サーバ、クライアントのトータルは2,340とカウントできます。この数値の差異について教えて下さい。

A33

（１）ウイルス対策ソフトウェアの数量の差異について

ウイルス対策ソフトウェアの導入状況は、以下のとおりです。

項	種類	導入台数
1	仮想サーバ（情報政策課）	128台
2	クライアント［デスクトップ］（情報政策課）	2,340台
3	クライアント［ノートパソコン］（情報政策課）	70台
4	クライアント（各課購入）※予備含む	572台
5	計	3,118台

Q34

佐世保市CSIRT行動要領（別紙18-2について）

３ページの報告・公表の（ハ）につき、公表しないことができるパターンとして、(1)ないし(6)が定められています。これらについては、貴庁にて情報流出等事故が発生した場合においても、具体的被害が発生しないと判断される場合、公表をしなくともよいという内容になっています。条文としては、公表しない場合を例外的とするように努めているようにも読み取れますが、(1)ないし(5)について、その判断者が何人であるかが不明であり、また、その判断者の判断の公正及び適正を担保する制度の存否が不明です。そして、(6)については、最高情報セキュリティ責任者(CISO)が公表不要と判断する場合とされており、包括的に公表不要の判断がされる懸念があります。すなわ

ち、本条については、その規定の構造上、事故の公表につき例外的とする運用が可能となり、住民の人権保障に反するとも考えられます。たとえば、(1)ないし(6)の判断につき、貴庁の情報公開及び個人情報保護審議会に諮問する等の公正等担保の運用はされているのでしょうか。本条につき、事故情報の公表が例外的とされる運用の懸念について、貴庁の見解をご教示下さい。

A34

佐世保市 CSIRT 行動要領)［抜粋］

第 6 条 事故発生時の対応は、別図に示す流れにより、次のとおり行う。

⑹報告・公表

ハ　事故については、事故が発生した情報資産を所管する課かいが報道機関等への公表を行う。ただし、次に掲げる場合においては公表しないことができるものとする。この場合においては、公表しないことにより隠蔽等を疑われ、市の信頼を低下させることがないよう、適切な説明に努めるものとする。

⑴個人情報の漏えい事故等で、第三者に閲覧されることなく速やかに情報資産を回収した場合

⑵個人情報の漏えい事故等で、情報資産に対して高度な暗号化等の秘匿化がされている場合

⑶個人情報の漏えい事故等で、情報資産が漏えい等をした事業者以外では内容を識別することができない場合であって被害が生じるおそれがない場合

⑷個人情報の漏えい事故等で、漏えい等事案の影響を受ける可能性のある者全てに連絡がついた場合

⑸サイバー攻撃による事故等で、公表することでかえって被害の拡大につながる可能性がある場合

⑹その他最高情報セキュリティ責任者(CISO)が公表不要と判断する場合

情報セキュリティ事故が発生した場合は、まず内部統制担当(総務部総務課)へ事故の報告を行い、文書情報については総務部総務課、電子情報については総務部情報政策課へ併せて報告を行うこととなります。

条文上は、「公表しないことができる」となっておりますが、事故発生時は、事故を起こした課のみで公表の可否を判断することはなく、内部統制担当や情報政策課、部長、副市長、市長(CISO)等の中で判断するものと考えています。

Q35

貴庁のサーバ、電子決裁、オンライン申請等

貴庁のサーバ室構築に関連して、貴庁における紙媒体ベース情報からデジタルデータへの移行方法とその経緯を教えて下さい。

※回答例１　「紙ベース⇒デジタルデータへの移管」につき、「スキャンまたはデータ引力（パンチ引力作業)」を外部委託している。

※回答例２　デジタルデータ資産の運用につきAI等を利用したビッグデータの解析・運用を行っている。または、予定している。

A35

(1)戸籍の電算化について（委託事業者：日立製作所）

平成16年2月に戸籍を電算化（データ化）しております。

電算化（データ化）は、「現在戸籍」を事業者に委託し、パンチ入力でデータ化しております。また、「改正原戸籍(紙の戸籍)」については、スキャンにてPDF化を行い、戸籍システムに取り込んでおります。改正原戸籍の原本(紙)については、地下書庫に保存しております。

(2)AI-OCRについて

【これまでの取り組み】(トライアル実施事業者:ソフトバンク社)AI、RPA等による業務効率化を推進していく過程で、業務の起点となるデータ作成（パンチ作業）に多くの時間を要していることがわかり、その解決策としてAI-OCR導入について検討をしております。令和2年7月にAI-OCRのトライアルを実施し、庁内の紙文書を大量に扱っている業務を対象に検証を実施しました。

検証の結果、職員がパンチ作業を行う場合とAI-OCRの利用料を比較した場合、AI-OCRを導入することで十分な効果が見込めることがわかった。

■検証結果（対象26帳票）

項	実施方法	要した時間(時間)	要した費用(円)
1	職員がパンチ作業を実施した場合	21,508時間	90,332,000円
2	AI-OCRで処理した場合	3,291時間	18,416,000円
3	効果等	▲18,217時間	▲71,916,000円

【これからの取り組み】

今年度製品選定を行い、令和3年1月ごろよりAI-OCRの試行導入を

開始し、対象業務を見極め、令和 4 年度から本格導入を予定しています。

Q36

貴庁のサーバ、電子決裁、オンライン申請等について

菅新内閣が発足し、各省庁において伝達事項及び回覧承認案件について、実押印が廃止の方向に向かっていますが、貴庁内においては、現在、どのような承認プロセスが遂行されていますか。

また、その承認プロセスについて、具体的なシステム（電子押印等）の存否、不存在の場合の今後の予定を教えて下さい。

※ご参考　「佐世保市 ICT 戦略 R2/4 発行」の 10 ページ第 1 章にて、電子決済・文書管理が「見送り」となっているようです。

A36

(1)現在の承認プロセスについて

承認プロセス（決裁）については、起案書等により行っております。

通常の承認プロセスにおいては、「担当者（起案者)」→「文責者」→「係長」→「課長補佐」→「課長」→「副部長（次長)」→「部長」→「副市長」→「市長（決裁者)」となります。

また、「決裁者」は、「佐世保市事務処理規定」により、内容によりそれぞれ「市長」～「課長」まで専決者区分を定めております。

(2)承認プロセスにおける具体的なシステム（電子押印等）の存否

承認プロセス（決裁）において、「電子決裁システム」等は、現在導入しておりません。

(3)今後の予定

「電子決裁・文書管理システム」については、令和５年度当初に稼働

すべく、調査・検討を進めております。

Q37

貴庁のサーバ、電子決裁、オンライン申請等について

「佐世保市 ICT 戦略 R2/4 発行」の 14 ページ「第 3 章　行政デジタル変革」の「2.現状と問題点」、「(1)紙・対面を前提とした行政手続の補足 12」にて、「平成 30 年 4 月に庁内で実施した調査によると、本市で実施している全手続き 1,995 件のうち、オンライン申請に対応しているものは 14 件に留まる（オンライン申請対応率：0.71%)」となっています。この利用率の低さについて、貴庁の見解をご教示下さい。

※回答例　アナウンスが不足している。オンライン申請手続自体につき、庁内の情報不足のまま運用されている等。

A37

現在、棚卸を進めており、最新のオンライン申請率の調査結果におきましては、[現状（令和 2 年 9 月時点)]

項	オンライン化実施済	全手続数	対応率
手続数	36	2,039	1.76%
件数	354,158	1,445,000	24.50%

オンライン化が進まない理由の多くが「対面が必要（本人確認や支払い等)」「書類の原本確認が必要」「押印が必要」となっております。

国におきましても、急速にオンライン化への取り組みを進めていることから、本市においても遅滞なく推進できるよう体制を整え、推進しております。

ICT 戦略において、「オンライン申請の推進」につきましては、令和 5 年度までに、年間 100 件以上の件数がある手続きの内、約半数をオンライン化すべく、推進しております。

［令和 5 年度の目標］　※年間 100 件以上の件数がある手続きを対象

項	オンライン化実施数	全手続数	対応率
手続数	216	2,039	10.60%
件数	889,360	1,445,000	61.15%

Q38

貴庁のサーバ、電子決裁、オンライン申請等について

サーバ類接触の顔認証及び入室キーシステムに関する機器の詳細（メーカー、商品名等）を教えて下さい。

A38

(1)サーバ類接触の顔認証および入室キーシステムの機器詳細について

［機器メーカー等］※本報告書での表記を省略する。

［商品名］※本報告書での表記を省略する。

［台数］4 台

(2)監視カメラシステムの機器詳細について

［機器メーカー等］キヤノン株式会社 製

［商品名］※本報告書での表記を省略する。

［台数］計 6 台(3)

別紙 38　参照

Q39
情報セキュリティ推進支援業務委託について、受託事業者に対し資格要件は設けているか。どのような資格を要件としているのか
A39
事業者の公募時に以下の資格要件を設けて選定しております。 ・調達時の資格要件 以下の資格要件のうち1つ以上を保有している要員1名以上を、業務の主担当者として従事させること (1)経済産業省が認定するシステム監査技術者（AU）の資格を取得した後、2 年以上のシステム監査、またはセキュリティ監査の実務経験を有している者 (2)特定非営利活動法人日本セキュリティ監査協会（JASA）が認定する公認情報セキュリティ主任監査人（CAIS-Lead Auditor）または公認情報セキュリティ監査人（CAIS-Auditor） (3)情報システムコントロール協会（ISACA）が認定する公認情報システム監査人（CISA）または公認情報セキュリティマネージャー（CISM） (4)一般財団法人日本規格協会（JRCA）が認定するエキスパート審査員または主任審査員 現在の委託事業者については、(3)の公認情報システム監査人(CISA)を保有している者が主担当として、委託業務に従事しております。

Q40
貴庁が策定した情報セキュリティポリシー及び情報セキュリティガイドブックにつき、その運用を含め、継続的な取組みがなされていることが分かりました。つきましては、貴庁の各部署における情報管理（特に電子情報）につき、情報セキュリティガイドブックの運用等を含め、現場の声を伺いたいと考えています。お手数ですが、別紙「佐世保市各部署あての照会」につき、貴庁の各部署の情報セキュリティ責任者及び同担当者の方にご一読いただき、回答をお願い致します。
A40
各部局へのアンケートによる回答確認済み
Q41
前回全体会議（令和 2 年 10 月 27 日）に回答していただいた「情管 34」につき、情報漏洩事故の公表等に関して、貴庁にて参照している Q&A 集がある旨伺いました。この Q&A 集につき、開示していただきたくお願い致します。
A41
別紙『「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関する Q&A』のとおり、提出いたします。別紙 41 抜粋を参照

Q42
総務部情報政策課様に所属されている職員のご芳名、ご役職名、年齢、同課配属年を教えて下さい。IPA（独立行政法人情報処理推進機構）の情報処理技術者試験や情報セキュリティマネジメント試験等のITマネージャーや情報セキュリティ知識に関する資格をお持ちである場合には、追記をお願い致します。
A42
以下、1名の資格保有者がおります。 ・氏名　：　※個人名であるため本報告書では省略する。 ・役職　：　主任主事 ・年齢　：　36歳 ・情報政策課配属年　：　2020年（1年目） ・保有資格　：　基本情報技術者（2009年取得） （同試験要綱、別紙42抜粋を参照）
Q43
【Q40】において、情報セキュリティに関する研修への要望が多いようだが、検討しているものはありますか。
A43
令和2年度に株式会社サンパートナーズ様による全職員対象の研修を実施しています。

Q44
貴庁あての情報公開及び情報管理に関する質問 庁舎内向けIT関連納品物（ソフトウェア・ハードウェア共に）は導入手段として、①一般競争入札、②指名競争入札、③随意契約、④その他の方法（プロポーザル等）が考えられますが、貴庁においては、④その他の方法として「公募型プロポーザル」が用いられているということでよいでしょうか。
A44
庁舎内向けIT関連納品物につきましては、「公募型プロポーザル方式」を利用し、調達を行っております。
Q45
貴庁あての情報公開及び情報管理に関する質問 仮に、貴庁において公募型プロポーサルが用いられている場合、プロポーザルの流れとして、 (1)ステップ1：公告 (2)ステップ2：説明会 (3)ステップ3：参加申請 (4)ステップ4：質問受付・回答 (5)ステップ5：企画提案書等提出書類の作成 (6)ステップ6：企画提案書の提出 (7)ステップ7：結果通知 (8)ステップ8：プレゼンテーション になると聞いています。貴庁において、納入案採用を決定するにあたり、上記(1)ないし(8)の各事項並びに貴庁に決定の過程について、その

正当性担保のため、佐世保市民にて公開を受ける方法はありますか。
A45
「情報公開請求」により、公開を受けることができます。 ただし、(2)～(8)項においては、市内部のセキュリティ情報を含んでいること、また提案者の創意工夫や独自性ともいえる企画提案書類が公開されると、競合関係にある同種事業者が、企画内容に係る情報に加工・改善を加え、そのアイデア・ノウハウを模倣・流用する恐れがあり、公開された事業者の利益が侵害される可能性が高いことから「非公開」としております。 （情報の公開義務及び公開しない情報） 第 10 条　実施機関は、公開請求があったときは、公開請求に係る情報に次の各号に掲げる情報（以下「適用除外情報」という。）のいずれかが記録されている場合を除き、公開請求者に対し、当該情報を公開しなければならない。 (3)　法人その他の団体（国及び地方公共団体を除く。以下「法人等」という。）に関する情報又は事業を営む個人の当該事業に関する情報であって、公開することにより、当該法人等又は当該個人の競争上の地位その他正当な利益が著しく損なわれることが明らかな情報。ただし、次に掲げる情報を除く。 ア．人の生命又は身体の安全、健康の保持若しくは財産又は環境の保全に影響を及ぼすおそれがある情報 イ．違法又は著しく不当な事業活動に関する情報 ウ．消費生活その他他人の生活に重大な影響を及ぼすおそれがある情報

Q46
貴庁あての情報公開及び情報管理に関する質問 貴庁のIT連納品契約及びＩＴ関連サービス契約については、①株式会社ビズテック、②株式会社日本ビジネスソフト、③エコー電子工業株式会社、④扇精光ソリューションズ株式会社であると聞いています。各社につき、現在有効である貴庁との契約書及び貴庁の公募に際して提出した企画提案書の閲覧および写しの交付をお願い致します。
A46
「仕様書」、「提案書」、「契約書」が発行されていますが、A45の理由に基づき情報は、「非公開」となります。
Q47
貴庁あての情報公開及び情報管理に関する質問 令和元年、神奈川県庁で利用されていたハードディスクの転売・情報流出事件が起きました。貴庁において、ハードディスクやその他の記憶媒体並びにこれらを内蔵する端末等を廃棄またはリース期間終了による返却等する場合、情報流出に備え、如何なる対処が行われているかにつき、ご教示願います。
A47
佐世保市におきまして、情報を含む記憶媒体（ハードディスクなど）を廃棄または返却する際は、庁舎内（職員自身 または 職員立会いの下）においてデータを完全消去することをルール化しております。 これにより、万一、運搬事業者の搬送中の紛失や事業者による消去漏れが発生した場合も、データ漏えいが起こらないように配慮しているものです。また、廃棄事業者に依頼する際におきましても、「データ消去（ま

たは破壊）証明書」の提出を求めており、再度完全にデータ消去（または破壊）されたことを確認しております。 別紙 47 抜粋　使用済みパソコンの処分に係る手順参照
Q48
貴庁の情報管理に関する実際の運営の検証依頼 これまでの調査の結果、貴庁における外部に対するセキュリティは、ソフトウエア及びハードウェア共現時点において、堅牢に準備されているものと評価可能です。その上で、現代社会における情報漏洩の発生内容において内部からの不正流出のパターンも少なくないことに鑑み、貴庁において、内部流出防止策についての実例を、実際の貴庁内における現場（その内情が理解できる部署を選定していただけると助かります。）にて見分させていただきたくお願い致します。なお、適宜書面による回答で代替していただいても問題ありません。
A48
別途、設備等を用い、情報流出防止策等についてご説明いたします。 「情報資産管理システム」により、全パソコンを制御（利用制限等）を実施するとともに、操作ログ等を取得し、漏えいした際の追跡も可能な状態としております。 （別日にて情報資産管理システムを実演視察）

Q49
貴庁の情報管理に関する実際の運営の検証依頼 佐世保市役所では庁舎内部からの情報流出防止策に関して、現時点で導入されている手法（別紙 20-1）の項目について、現在適切に行われているかを確認させていただきたくお願い致します。
A49
別途、設備等を用い、情報流出防止策等についてご説明いたします。 （別日にて実演視察）
Q50
貴庁の情報管理に関する実際の運営の検証依頼 貴庁内にて、業務に使用しているデバイス（USB メモリ、SD カード、ポータブル HDD 若しくは SSD 等）についても現物を拝見させて下さい。
A50
別途、設備等を用い、情報流出防止策等についてご説明いたします。 （別日にて実演視察）
Q51
貴庁の情報管理に関する実際の運営の検証依頼 パスワード設定について、セキュリティガイドブック【4-1ID・パスワードを管理する】に習い適正に生成、登録しているかを現場見学させて下さい。なお、そもそもパスワード管理は個人に任せているのか、管理者はパスワード発行の部分には関与していないのかにつきご教示下さい。（別紙 51 を参照）

A51
本市のパスワード管理については、個人管理となっております。 最長 90 日間を有効期間としており（漏えい対策)、90 日を経過するとパソコン等にログインできない等（放置対策）の対策をしております。
Q52
現在画面転送（主に VDI 環境）において、主に使われているアプリケーションとその使用目的がどのようなものかをご教示ください。
A52
［主に使用しているアプリケーション］ ・インターネットエクスプローラー ・Office365（Word、Excel、PowerPoint 等） ［主な使用な使用目的］ ・インターネットの閲覧 ・財務会計システム、庶務事務システム、例規システム ・業務文書等の作成
Q53
地域イントラネット概略構成図(P73)に示されているネットワーク構成図において、北部リングの光ファイバの芯数が支所によって違うのは何か理由がおありでしょうか。
A53
地域イントラネットの整備については、総務省「地域イントラネット基盤整備補助事業」を活用しております。 平成 18 年度に「南部リング」を整備する際は、同補助事業の対象範囲

として、現用 4 心＋予備 4 心が整備対象であったため、8 心構成を基本として整備しております。平成 21 年度に整備した「北部リング」については、補助事業の対象要件が変わり、現用 2 心＋予備 2 心が補助対象範囲と変更になったため、整備心線数を変更しております。 これにより、整備地区ごとに心線数の差異があるものです。また、心線数は少なくなっていますが、1 心あたり 10Gbps まで拡張可能（現用：1Gbps）であるため、心線数の減少による業務等への支障はありません。
Q54
仮想サーバのリソース状況表を拝見させていただき、サーバシステムのほとんどが Windows Server2008 若しくは 2008 R2 となっています。 この OS については、2020 年 1 月に Microsoft のサポートが終了している事実があります。一部のブロック(B 環境 Remoteteapp セッションホスト系)は移行又は新設の対象としてフラグがありますが、その他のブロック（業務システム A～O 等）については現時点で特段問題は出てないでしょうか。また今後の予定はありますか。
A54
業務システム（A～O）については、令和元年～2 年度にかけて、Windows2016 サーバ OS 等への移行作業を実施し、完了しております。 ［補足］本資料（仮想サーバリソース状況表）にある「移行対象」とは、本委託受託事業者（日本ビジネスソフト社）に求める委託業務対象範囲を示しており、記載がないものについては、各業務システム運用事業者にて移行作業等を実施しております。

Q55
ネットワークセキュリティの穴を狙って以下の様な仕組みを考えた人がいる場合、現状のセキュリティ環境でこの不正に対してアラート又は防止することが可能でしょうか（一部セキュリティ上の関係からマスキングする)。 ・ロッカーに[redacted]を用意 ・[redacted]を持ち込む ・[redacted]を無理やり有線にして[redacted] につなぐ ・[redacted]を立て、[redacted]に繋がるようにする ・[redacted]との接続を行う 尚この方式のソースはインターネット上の掲示板等に記載されている模様で、誰でも閲覧可能なものです。このような悪用を検知できる環境にあるかどうかの確認です。
A55
※佐世保市より詳細な回答を得たが、セキュリティに関わる内容であるため、本報告書では省略する。なお、回答内容は、監査人補助員ＳＥにて検証した結果、対処可能と評価してより回答であった。

別紙１－５

令和２年度包括外部監査
～佐世保市の情報公開および情報管理について～

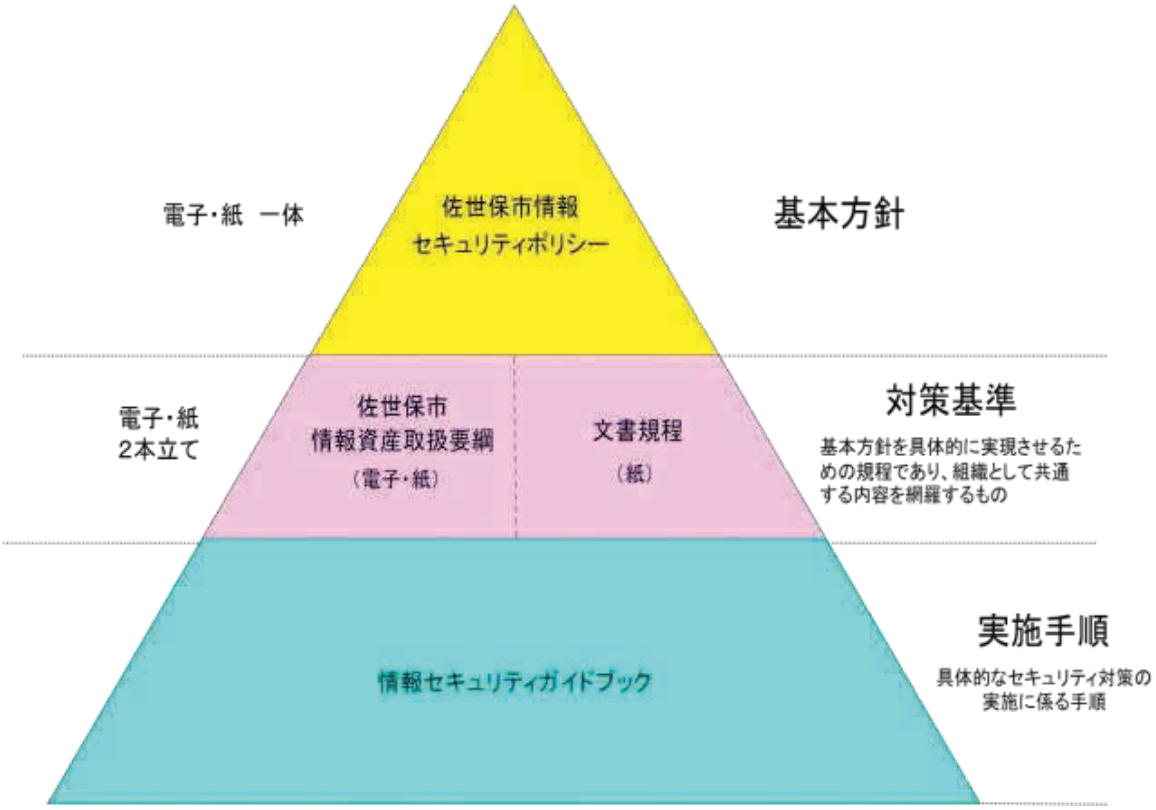
(2) 情報管理について

ア　担当部局・・・総務部情報政策課

イ　貴庁内での情報セキュリティ（情報機密性・完全性・可用性確保）のため行っている活動

佐世保市の情報セキュリティ規定類の体系は以下の図のとおりとなっており、各種規定類に基づき情報の管理を行っております。

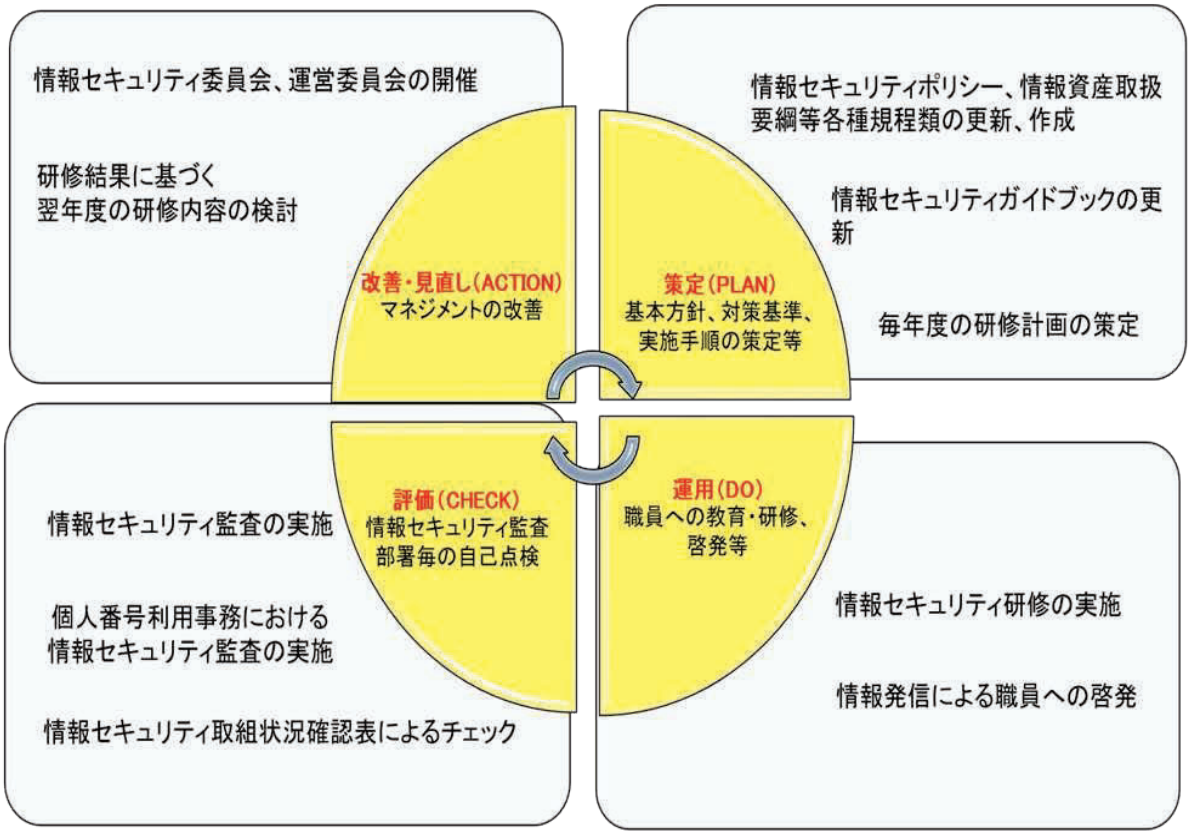
佐世保市の情報セキュリティ規定類の体系



別紙１－５

佐世保市では、佐世保市情報セキュリティポリシーに基づき、以下の PDCA サイクルで、情報資産のセキュリティ(機密性、完全性、可用性)確保のための活動を行っております。

佐世保市における情報セキュリティのPDCAサイクル



ウ　情報セキュリティにつき外部業者への委託を行っている場合にはその契約内容

1　佐世保市が保有する電子情報の管理について

佐世保市が保有する電子情報については、主にファイルサーバに保管しております。ファイルサーバについては、情報政策課が所管するサーバ室内に構築しております。

2（1）佐世保市の情報セキュリティ対策に係る業務委託ついて

別紙１－５

佐世保市の情報セキュリティ対策に係る業務委託の状況は、以下の表のとおりです。

	内容	実施主体	対象	委託内容等について
1	ネット環境構築	情報政策課	庁内ネットワーク機器等	庁内ネットワーク機器、パソコン等の構築、設定、セキュリティパッチの適用、ヘルプデスク対応等について委託を行っている。
2	端末のウイルス対策	情報政策課	情報政策課配布の端末	ウイルス対策ソフトを、情報政策課にて必要ライセンス数購入し、各端末にインストールしている。 ウイルス感染時の調査等は庁内ネットワークの保守委託に含めている。
		各課	各課調達の端末	
3	サーバ設置・維持管理	情報政策課	庁内ネットワークサーバ	サーバの障害対応、セキュリティパッチの適用、ヘルプデスク対応等について委託を行っている。
		各課	各課調達サーバ	各課において委託等の対応を行っている。
4	端末・サーバの廃棄	端末、サーバの所管課	廃棄端末、サーバ	データ消去ソフトによる消去又は HDD の物理的破壊をした後破棄等を行っている。 業者にデータ消去、物理的破壊を行わせる場合は、データ消去証明書、破壊証明書を提出させるようにしている。

２（２）佐世保市が情報セキュリティ対策策定及び実施の全部または大部分を外部業者に委託しているパターンについて

佐世保市においては、お尋ねの事項について外部業者に業務委託はしておりません。

別紙６－８

R02.07.07 包括外部監査ヒアリング　総務部

包括外部監査ヒアリング（R02.06.26）時の質問に対する回答

１．情報公開関係

①審査請求の取り下げの内容について

３件（請求日：平成 29 年 10 月 6 日、取下日：平成 29 年 10 月 27 日）
（請求日：平成 30 年 12 月 5 日、取下日：平成 31 年 1 月 7 日）
（請求日：令和 2 年 2 月 25 日、取下日：令和 2 年 3 月 27 日）
※詳細については、別添「審査請求綴（３冊）」のとおり

②非開示の理由について

令和元年度分
非公開　1 件・・・条例第 10 条第 1 項第 4 号（意思形成過程に関する情報）
部分公開　689 件（以下、主な理由）
・条例第 10 条第 1 項第 2 号（個人に関する情報）住所、氏名、携帯番号、印影等
・　第 3 号（法人その他の団体に関する情報）印影、口座情報等
・　第 5 号（行政運営情報）代価表、特殊単価以外の単価並びにそれらを類推できる金額等

２．情報管理関係

①総合行政ネットワークへの接続時期について

国・・・平成１３年度から運用開始
佐世保市・・・平成１５年度から参加

②ファイルサーバの全保存領域と使用量について

全保存領域・・・４２．０ＴＢ
使　用　量・・・　９．２ＴＢ

③情報セキュリティの事故件数について

別添資料のとおり

別紙６－８

R02.07.07包括外部監査　総務課

情報セキュリティ事故件数推移（平成29年度～令和元年度）

（単位：件）

項　　目		令和元年度	平成30年度	平成29年度
電子情報関係		2	3	7
	システム構築のミス	1	1	1
	システム障害	1	0	1
	ホームページの不具合	0	0	2
	USBの紛失	0	1	0
	ICカードの紛失	0	0	1
	情報漏えい	0	1	0
	メール送信方法の誤り	0	0	2
文書情報関係		6	4	6
	誤送付	1	3	3
	誤った情報の送付	2	0	0
	書類の紛失	2	1	2
	情報漏えい	1	0	1
計		8	7	13

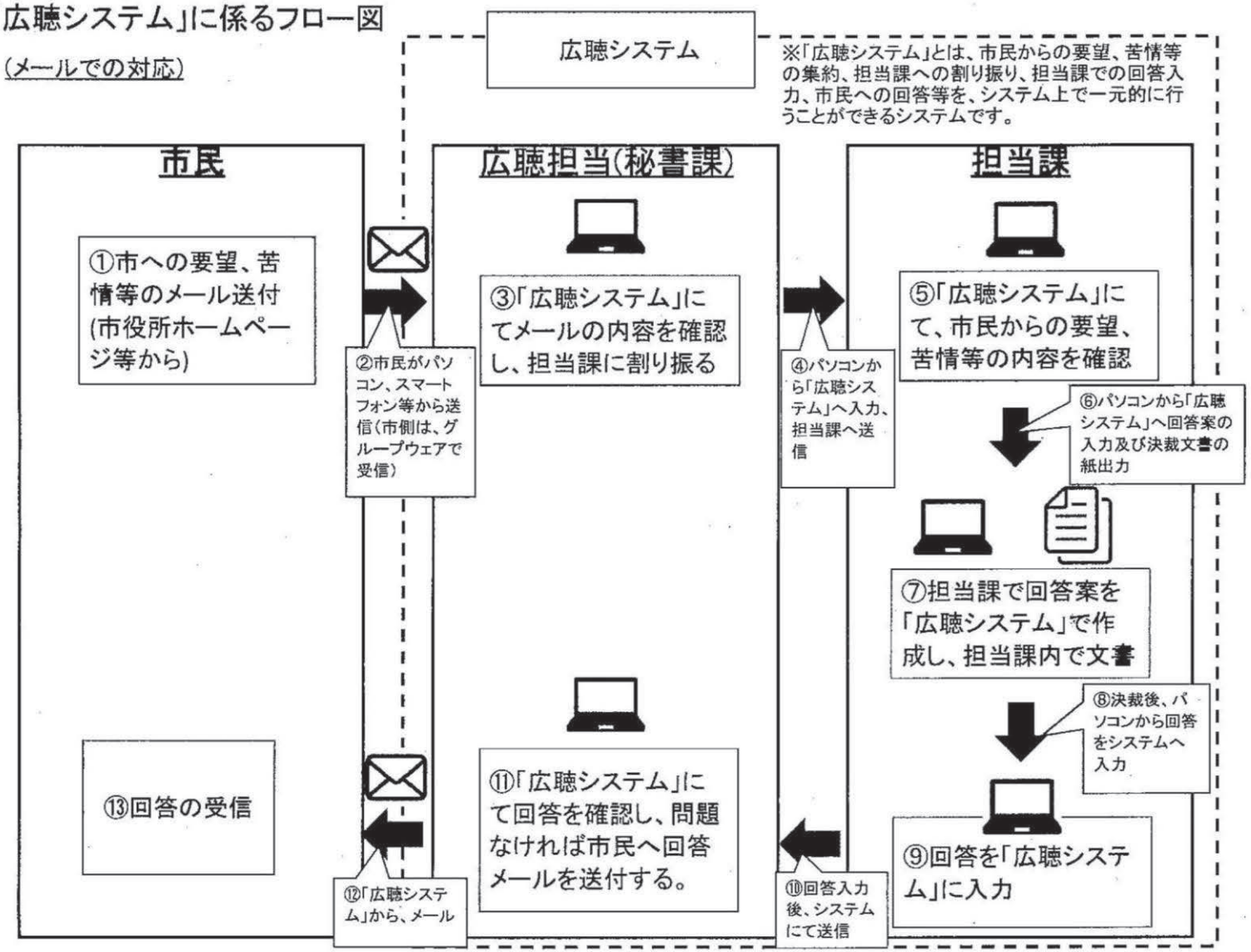
※本市以外の他の要因による事故は除く。

2. フロー図に基づきデジタルデータの取り扱い部分と、それを管理するデバイスの名称と種類

別紙９①

○「広聴システム」に係るフロー図

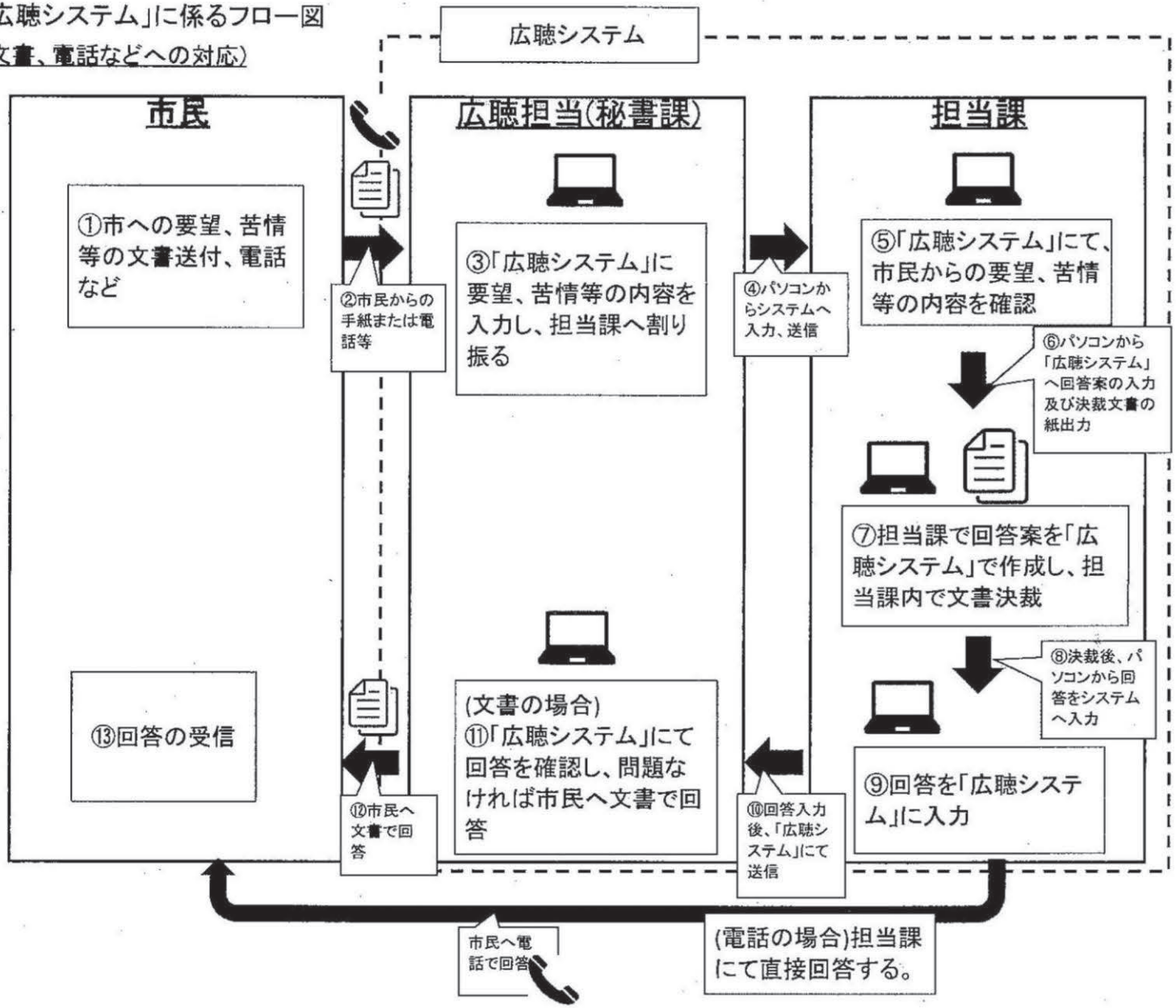
（メールでの対応）



2. フロー図に基づきデジタルデータの取り扱い部分と、それを管理するデバイスの名称と種類　別紙９②

○「広聴システム」に係るフロー図

（文書、電話などへの対応）



２のデータベースを管理する機器の詳細情報

使用データベース管理機器内訳表　　（台）

項		全台数	対象部署	内訳
1	サーバ	26台	防災危機管理局	1
2			総務部_情報政策課	1
3			財務部_納税課／保健福祉部_保険料課	1
4			土木部_土木政策・管理課	1
5			港湾部_みなと振興・管理課	1
6			市民生活部_戸籍住民窓口課	2
7			保健福祉部_看護専門学校	1
8			保健福祉部_長寿社会課	1
9			保健福祉部_生活福祉課	1
10			保健福祉部_健康づくり課	1
11			保健福祉部_生活衛生課	1
12			子ども未来部_子ども発達センター	1
13			子ども未来部_子ども保健課／保健福祉部_健康づくり課	1
14			環境部_環境保全課	2
15			環境部_廃棄物減量推進課	1
16			消防局_指令課	1
17			水道局_水道維持課	1
18			水道局_下水道事業課	3
19			教育委員会_教育総務部総務課	2
20			教育委員会_学校教育課	1
21			選挙管理委員会事務局	1
22	仮想サーバ	20台	契約管理室_技術監理課	1
23			総務部_職員課	1
24			総務部_情報政策課	2
25			財務部_財政課	1
26			財務部_資産経営課	2
27			財務部_資産税課	1
28			都市整備部_まち整備課	1
29			保健福祉部_保健福祉政策課	1
30			保健福祉部_生活福祉課	1
31			保健福祉部_生活衛生課	2
32			保健福祉部_保険料課	1
33			子ども未来部_子ども支援課	1
34			水道局_財務課	1
35			水道局_営業課	1
36			水道局_水道施設課	1
37			水道局_下水道事業課	1
38			教育委員会_教育センター	1

２のデータベースを管理する機器の詳細情報

使用データベース管理機器内訳表　　（台）

項		全台数	対象部署	内訳
39	クライアント	2294台	基地政策局	10
40	バックアップ		行財政改革推進局	6
41			企業立地推進局	9
42			防災危機管理局	12
43			契約監理室_契約課	9
44			契約監理室_技術監理課	7
45			企画部_政策経営課	31
46			企画部_地域政策課	9
47			企画部_地域交通課	9
48			企画部_文化振興課	5
49			企画部_国際政策課	8
50			企画部_島瀬美術センター	5
51			企画部_宇久行政センター産業建設課	10
52			企画部_宇久行政センター住民課	10
53			企画部_宇久家畜診療所	3
54			総務部_総務課	12
55			総務部_職員課	29
56			総務部_秘書課	12
57			総務部_情報政策課	18
58			総務部_東京事務所	4
59			財務部_財政課	13
60			財務部_資産経営課	35
61			財務部_市民税課	34
62			財務部_資産税課	49
63			財務部_納税課	40
64			財務部_債権管理対策室	3
65			観光商工部_商工物産課	20
66			観光商工部_観光課	20
67			観光商工部_ふるさと納税推進課	15
68			観光商工部_競輪事務所	5
69			農林水産部_農業畜産課	21
70			農林水産部_有害鳥獣対策室	6
71			農林水産部_卸売市場管理事務所	4
72			農林水産部_農林整備課	23
73			農林水産部_水産課	17
74			農林水産部_水産センター	8
75			都市整備部_都市政策課	14
76			都市整備部_住宅課	13
77			都市整備部_まち整備課	11
78			都市整備部_公園緑地課	24
79			都市整備部_建築指導課	33
80			都市整備部_営繕課	27
81			都市整備部_地籍調査課	8
82			土木部_土木政策・管理課	41

２のデータベースを管理する機器の詳細情報

使用データベース管理機器内訳表　　（台）

項		全台数	対象部署	内訳
83			土木部_道路整備課	28
84			土木部_道路維持課	23
85			土木部_河川課	12
86			港湾部_みなと振興・管理課	19
87			港湾部_みなと整備課	17
88			市民生活部_コミュニティ・協働推進課	23
89			市民生活部_市民安全安心課	17
90			市民生活部_人権男女共同参画課	12
91			市民生活部_人権男女共同参画課(スピカ)	6
92			市民生活部_戸籍住民窓口課	40
93			市民生活部_早岐支所	9
94			市民生活部_相浦支所	8
95			市民生活部_日宇支所	7
96			市民生活部_大野支所	4
97			市民生活部_中里皆瀬支所	3
98			市民生活部_柚木支所	3
99			市民生活部_黒島支所	3
100			市民生活部_江上支所	3
101			市民生活部_三川内支所	3
102			市民生活部_針尾支所	3
103			市民生活部_宮支所	3
104			市民生活部_吉井支所	6
105			市民生活部_世知原支所	4
106			市民生活部_小佐々支所	7
107			市民生活部_江迎支所	6
108			市民生活部_鹿町支所	4
109			保健福祉部_保険福祉政策課	27
110			保健福祉部_宇久保健福祉センター	3
111			保健福祉部_医療政策課	7
112			保健福祉部_長寿社会課	38
113			保健福祉部_障がい福祉課	33
114			保健福祉部_生活福祉課	88
115			保健福祉部_健康づくり課	32
116			保健福祉部_試験検査課	13
117			保健福祉部_生活衛生課	26
118			保健福祉部_生活衛生課（西部芳世苑）	2
119			保健福祉部_食肉衛生検査所	16
120			保健福祉部_急病診療所	5
121			保健福祉部_医療保険課A	20
122			保健福祉部_医療保険課B	22
123			保健福祉部_保険料課	40
124			保健福祉部_指導監査課	10
125			保健福祉部_看護専門学校	20
126			子ども未来部_子ども政策課	9

２のデータベースを管理する機器の詳細情報

使用データベース管理機器内訳表　　（台）

項		全台数	対象部署	内訳
127			子ども未来部_子ども支援課	36
128			子ども未来部_子ども育成課	10
129			子ども未来部_子ども育成課 北部子育て支援センター（上相浦保育所）	8
130			子ども未来部_子ども育成課 中部子育て支援センター（大黒保育所）	9
131			子ども未来部_子ども育成課 東部子育て支援センター（早岐保育所）	7
132			子ども未来部_子ども育成課 幼児教育センター	8
133			子ども未来部_子ども育成課 白南風幼稚園	9
134			子ども未来部_子ども育成課 天神幼稚園	4
135			子ども未来部_子ども育成課 すぎのこ園	7
136			子ども未来部_子ども保健課	18
137			子ども未来部_子ども子育て応援センター	18
138			子ども未来部_子ども発達センター	18
139			環境部_環境政策課	16
140			環境部_環境保全課	14
141			環境部_廃棄物減量推進課	14
142			環境部_廃棄物指導課	14
143			環境部_クリーン推進課	4
144			環境部_施設課	13
145			環境部_宇久環境センター	4
146			環境部_クリーンピュアとどろき	4
147			環境部_東部クリーンセンター	7
148			環境部_西部クリーンセンター	14
149			会計管理室	9
150			消防局_総務課	15
151			消防局_警防課	9
152			消防局_指令課	10
153			消防局_予防課	9
154			消防局_消防訓練所	2
155			消防局_中央消防署	18
156			消防局_中央消防署_日宇出張所	3
157			消防局_中央消防署_干尽出張所	3
158			消防局_中央消防署_春日出張所	3
159			消防局_東消防署	13
160			消防局_西消防署	14
161			消防局_西消防署_祝橋出張所	3
162			消防局_西消防署_江迎・鹿町出張所	3
163			消防局_西消防署_宇久出張所	2
164			水道局_水道局総務課	18
165			水道局_水道局財務課	8
166			水道局_水源対策・企画課	13
167			水道局_水道維持課	44
168			水道局_水道維持課 東部管理係	9
169			水道局_水道整備課	25
170			水道局_水道施設課	25

２のデータベースを管理する機器の詳細情報

使用データベース管理機器内訳表

（台）

項		全台数	対象部署	内訳
171			水道局_水道施設課 山の田浄水場	11
172			水道局_北部管理事務所	13
173			水道局_水道局宇久営業所	2
174			水道局_下水道事業課	48
175			水道局_下水道施設課	13
176			水道局_水質管理センター	10
177			総合医療センター	16
178			教育委員会_教育委員会総務課	24
179			教育委員会_学校教育課	19
180			教育委員会_学校保健課	13
181			教育委員会_社会教育課	17
182			教育委員会_文化財課	13
183			教育委員会_スポーツ振興課	10
184			教育委員会_総合教育センター課（少年科学館、清水地区公民館含む）	13
185			教育委員会_新しい学校推進室	3
186			教育委員会_教育センター	11
187			教育委員会_図書館	16
188			教育委員会_青少年教育センター	15
189			教育委員会_中央公民館	3
190			教育委員会_南地区公民館	2
191			教育委員会_山澄地区公民館	2
192			教育委員会_中部地区公民館	2
193			教育委員会_大野地区公民館	3
194			教育委員会_柚木地区公民館	2
195			教育委員会_愛宕地区公民館	2
196			教育委員会_西地区公民館	2
197			教育委員会_相浦地区公民館	3
198			教育委員会_北地区公民館	2
199			教育委員会_中里皆瀬地区公民館	2
200			教育委員会_九十九地区公民館	2
201			教育委員会_崎辺地区公民館	2
202			教育委員会_佐世保市学校給食センター	6
203			教育委員会_日宇地区公民館	3
204			教育委員会_世知原地区公民館	4
205			教育委員会_吉井地区公民館	4
206			教育委員会_広田地区公民館	2
207			教育委員会_三川内地区公民館	2
208			教育委員会_鹿町地区公民館	3
209			教育委員会_江迎地区公民館	3
210			教育委員会_針尾地区公民館	2
211			教育委員会_江上地区公民館	2
212			教育委員会_宮地区公民館	2
213			教育委員会_早岐地区公民館	3
214			教育委員会_小佐々地区公民館	3

２のデータベースを管理する機器の詳細情報

使用データベース管理機器内訳表　　（台）

項		全台数	対象部署	内訳
215			教育委員会_宇久地区公民館	4
216			教育委員会_黒島地区公民館	1
217			議会事務局_議会運営課	14
218			選挙管理委員会_選挙管理委員会事務局	9
219			監査事務局	11
220			農業委員会_農業委員会事務局	20

4. 情報管理（個人情報とそれ以外）に使用する主な業務システムとアプリケーション及びネットワーク方式（総務部）

項	システム管理責任者	情報管理責任者	システム名	アプリケーション名	OS（サーバー）	OS（クライアント）
1	情報政策課長	情報を掲載している課かいの長	グループウェア	AbleOffice	WindowsServer2016	Windows 10 pro
2	情報政策課長	情報を掲載している課かいの長	佐世保市役所ホームページコンテンツ管理システム	CMS-8341（やさしい）	－	Windows 10 pro
3	情報政策課長	情報を掲載している課かいの長	統合型地理情報システム	PasCAL for LGWAN	WindowsServer2016	Windows 10 pro
4	情報政策課長	情報を掲載している課かいの長	公共施設予約管理システム	eG-Reserve	－	Windows 10 pro
5	情報政策課長	情報を掲載している課かいの長	広聴・FAQシステム	FastAnswer/FastHelp	－	Windows 10 pro
6	情報政策課長	情報を掲載している課かいの長	住民公開型WebGIS	させぼ街ナビ	－	Windows 10 pro
7	情報政策課長	情報を掲載している課かいの長	情報資産管理システム	情報資産管理システム	WindowsServer2016	Windows 10 pro
8	情報政策課長	戸籍住民窓口課長	住民記録システム	総合行政システム	－	Windows 10 pro
9	情報政策課長	戸籍住民窓口課長	印鑑登録システム	総合行政システム	－	Windows 10 pro
10	情報政策課長	戸籍住民窓口課長	外国人登録システム	総合行政システム	－	Windows 10 pro
11	情報政策課長	市民税課長	宛名管理システム	総合行政システム	－	Windows 10 pro
12	情報政策課長	選挙管理委員会事務局長	選挙システム	総合行政システム	－	Windows 10 pro

4. 情報管理（個人情報とそれ以外）に使用する主な業務システムとアプリケーション及びネットワーク方式（総務部）

項	システム管理責任者	情報管理責任者	システム名	アプリケーション名	OS（サーバー）	OS（クライアント）
13	情報政策課長	教育委員会学校教育課長	教育委員会業務システム	総合行政システム	－	Windows 10 pro
14	情報政策課長	資産税課長	固定資産税システム	総合行政システム	－	Windows 10 pro
15	情報政策課長	資産税課長	軽自動車税システム	総合行政システム	－	Windows 10 pro
16	情報政策課長	市民税課長	市県民税システム	総合行政システム	－	Windows 10 pro
17	情報政策課長	医療保険課長（資格・給付） 保険料課長（賦課）	国民健康保険システム	総合行政システム	－	Windows 10 pro
18	情報政策課長	納税課長 保険料課長	収納消込みシステム	総合行政システム	－	Windows 10 pro
19	情報政策課長	市民税課長	法人市民税システム	総合行政システム	－	Windows 10 pro
20	情報政策課長	市民税課長	税証明システム	総合行政システム	－	Windows 10 pro
21	情報政策課長	保険料課長 医療保険課長	後期高齢者医療保険料徴収システム	総合行政システム	－	Windows 10 pro
22	情報政策課長	医療保険課長	国民年金システム	総合行政システム	－	Windows 10 pro
23	情報政策課長	住宅課長	住宅駐車場使用料システム	総合行政システム	－	Windows 10 pro
24	情報政策課長	会計管理室長	歳入システム	総合行政システム	－	Windows 10 pro

4. 情報管理（個人情報とそれ以外）に使用する主な業務システムとアプリケーション及びネットワーク方式（総務部）

項	システム管理責任者	情報管理責任者	システム名	アプリケーション名	OS（サーバー）	OS（クライアント）
25	情報政策課長	政策経営課長	統計調査システム	総合行政システム	－	Windows 10 pro
26	情報政策課長	情報政策課長	運用管理システム	総合行政システム	－	Windows 10 pro
27	総務課長	総務課長	例規集データベースシステム	例規システム	－	Windows 10 pro
28	職員課長	職員課長	人事情報システム（人事給与・福利厚生・臨時職員・庶務事務）	人事給与システム LAPiS	Windows Server2016	Windows 10 pro
29	情報政策課長	情報を利用している課かいの長	市民アンケートシステム	（個別開発）	－	Windows 10 pro
30	情報政策課長	情報政策課長	テレビ会議システム	Webex Meetings	－	Windows 10 pro
31	総務課長	総務課長	郵便料金管理システム	－	－	Windows 10 pro
32	情報政策課長	医療保険課長	福祉年金システム	総合行政システム	－	Windows 10 pro
33	情報政策課長	医療保険課長	年金生活者支援給付金システム	総合行政システム	－	Windows 10 pro
34	情報政策課長	戸籍住民窓口課長	住基ネット連携システム	総合行政システム	－	Windows 10 pro

別紙１３

5．各部署で利用している現行セキュリティソフトウェアまたはハードウェアセキュリティの名称
5における導入当初の初期費用額（イニシャルコスト）また保守費用（ライセンス料等）を含めた年間維持費額（ランニングコスト）

●セキュリティソフトウェア【全庁共通】　（円）　（円／年）

項	機種名	導入年度	初期費用	年間維持費用	備考
1	※各クライアントパソコンに導入し、マルウェア対策等を行う	令和元年度	9,842,500	0	６年間
2	※インターネット、メール等をフィルタリングし、有害サイトや標的型メール等の検知を行う	平成２５年度	2,220,750	700,000	

●ハードウェア【全庁共通】　（円）　（円／年）

項	機種名	導入年度	初期費用	年間維持費用	備考
3	［統合型脅威管理装置］	令和元年度	3,807,000	1,757,700	

※主にインターネット等の外部と市の内部ネットワークを切り分ける接続点に配置するものであり、外部からの不正なアクセスから内部システムを防御するとともに、アンチマルウェア対策・IPS（不正侵入検知）、DMZ環境の構築や通信制御（ルーティング）等を行う機器

別紙15

7．情報資産管理機器及びソフトウェアを含む各システムの購入先（ベンダー名、代理店名）

項		納入機器名	メーカ名	代理店	数量	ﾊｰﾄﾞｳｪｱ・ｿﾌﾄｳｪｱの別
大	小					
D	8	ウィルス対策ソフトウェア		扇精光ソリューションズ（株）佐世保支店	3,118	ソフト

別紙１６

８．７．におけるシステムの稼働率と評価（満足度及び不足点）

【満足度】

令和元年度に庁内情報システム基盤機器等を更改し、ネットワーク、仮想サーバ、一人１台パソコンとも停止することなく安定的に稼働しています。

セキュリティ対策についても、セキュリティ対策ソフト　　を各端末に導入しており、常に最新のセキュリティ状態を保つことができています。

システムの稼働率は１００％であり、高い満足度になっております。

【不足点】

社会のデジタル化に対応した業務・システムの変革が課題です。例えば、仮想サーバ基盤のクラウド化など各課導入システムのクラウド化の推進、テレワーク導入に向けた個人情報等のセキュリティへの対応、行政手続きのオンライン化、職員間コミュニケーションツールの展開による庁内のデジタル化などが課題として挙げられます。

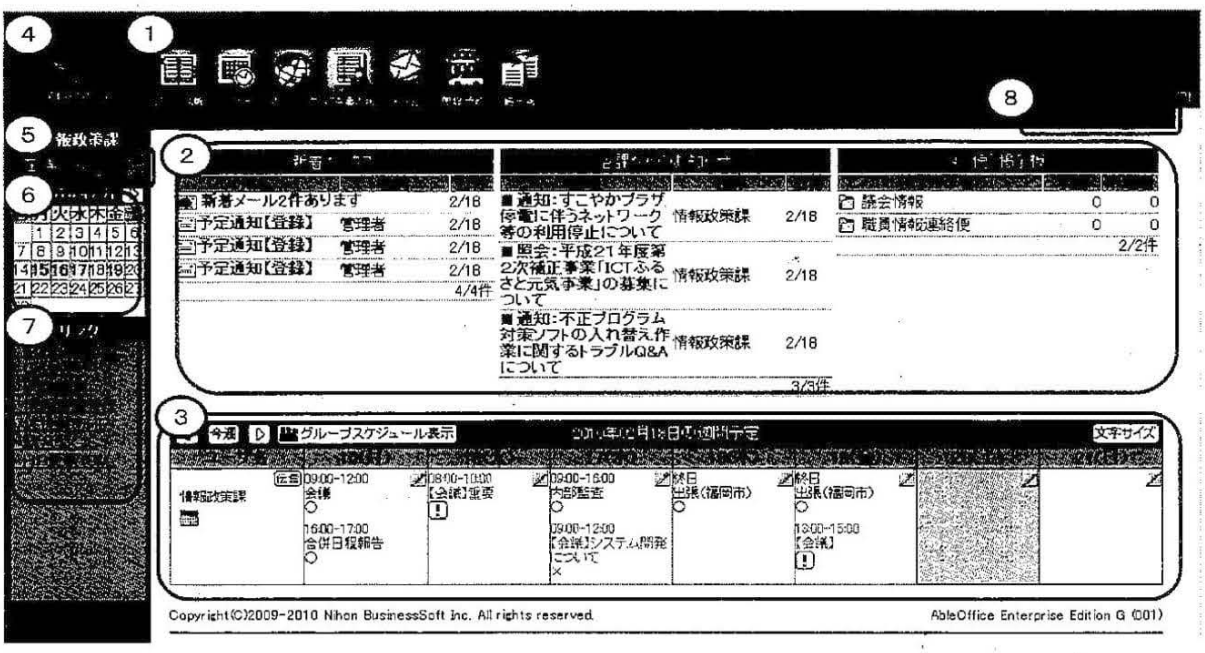
以　上

別紙１７

別紙17-1

９．現稼働システムにおける直接運用スタッフのシステム内容の認知度と操作における教育内容の充実度（マニュアル作成等）

○全庁・全職員が利用する「グループウェアシステム」の例



１．グループウェアの初期画面の紹介

グループウェアにログインした直後の画面です。
この画面から、未読のメール・各課からのお知らせ等を確認できます。
また、個人スケジュールについては、この画面から予定の管理（承認・拒否）などが行えます。

①グループウェアの各機能ボタン
　グループウェアが備えている各機能を起動します。
　　アドレス帳・・・個人アドレス帳や共有アドレス帳などの機能
　　スケジュール・・三役、所属、グループ、個人のスケジュール管理機能
　　マイリンク・・・よく使うウェブサイトを登録する機能
　　行先案内板・・・不在表示をしているユーザの状況の一覧機能
　　施設予約・・会議室、設備、公用車などの予約管理機能
　　メール・・・庁内及び外部へのメールの送受信
　　掲示板・・・各課からのお知らせ、部内掲示板など
②新着ボックス、各課からのお知らせ、よく使う掲示板
　　新着ボックス・・・メールやスケジュールが登録・変更された場合にお知らせされます。
　　各課からのお知らせ・・・各課からのお知らせに投稿された場合に更新されます。
　　　　タイトル部分を押すと、掲示板機能へ切り替わります。
　　よく使う掲示板・・・投稿・更新された場合に知らせてほしい掲示板を表示できます。
③週間スケジュール
　　１週間の個人予定が表示されます。各課かいの全職員の予定表示に切り替えることも可能です。
④トップページ表示のロゴ
　　このボタンを押すと、どの画面からでも、トップページを表示できます。
⑤在席表示
　　在席／不在の表示機能です。不在の際は行先案内板に表示され、他人からも分かります。

佐世保市広聴･FAQシステム マニュアル

1

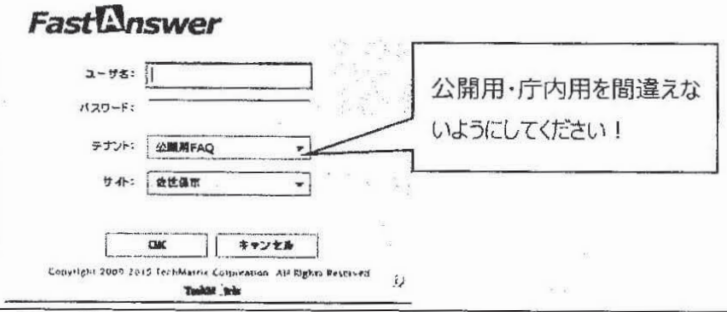
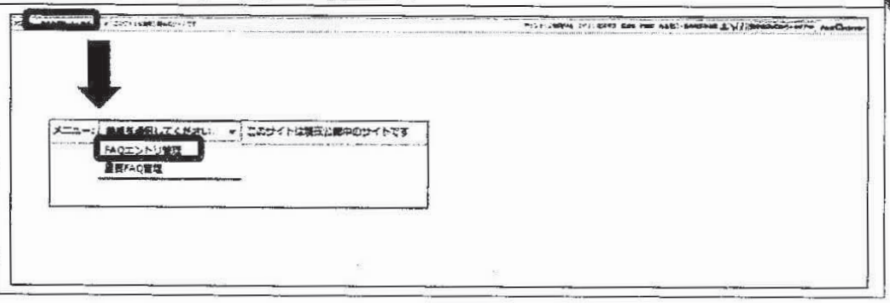
FastAnswer

<FAQ更新･削除編>

1、ログイン画面・メニュー選択	2
2、更新したいFAQの検索	3
3、FAQエントリ詳細画面の入力項目について	4
4、回答の作成について	5
5、Edit画面の解説（リンクの設定方法）	6
6、関連するFAQを表示させたい場合	9
7、外部URLを表示させたい場合	10
8、スマートフォン用ページへの反映について	11
9、添付ファイルの設定について	12
１０、カテゴリの設定について	12
１１、FAQの保存とプレビュー	12
１２、承認依頼	13
１３、内容の不備等で承認却下となった場合	14
１４、FAQの削除について	15

別紙17-2

1、ログイン画面・メニュー選択【必須】

ユーザ ID、パスワードを入力。 変更するテナント（公開用 FAQ・庁内用 FAQ）を選択します。	
画面左上の「メニュー」から「FAQ エントリ管理」を選択してください。