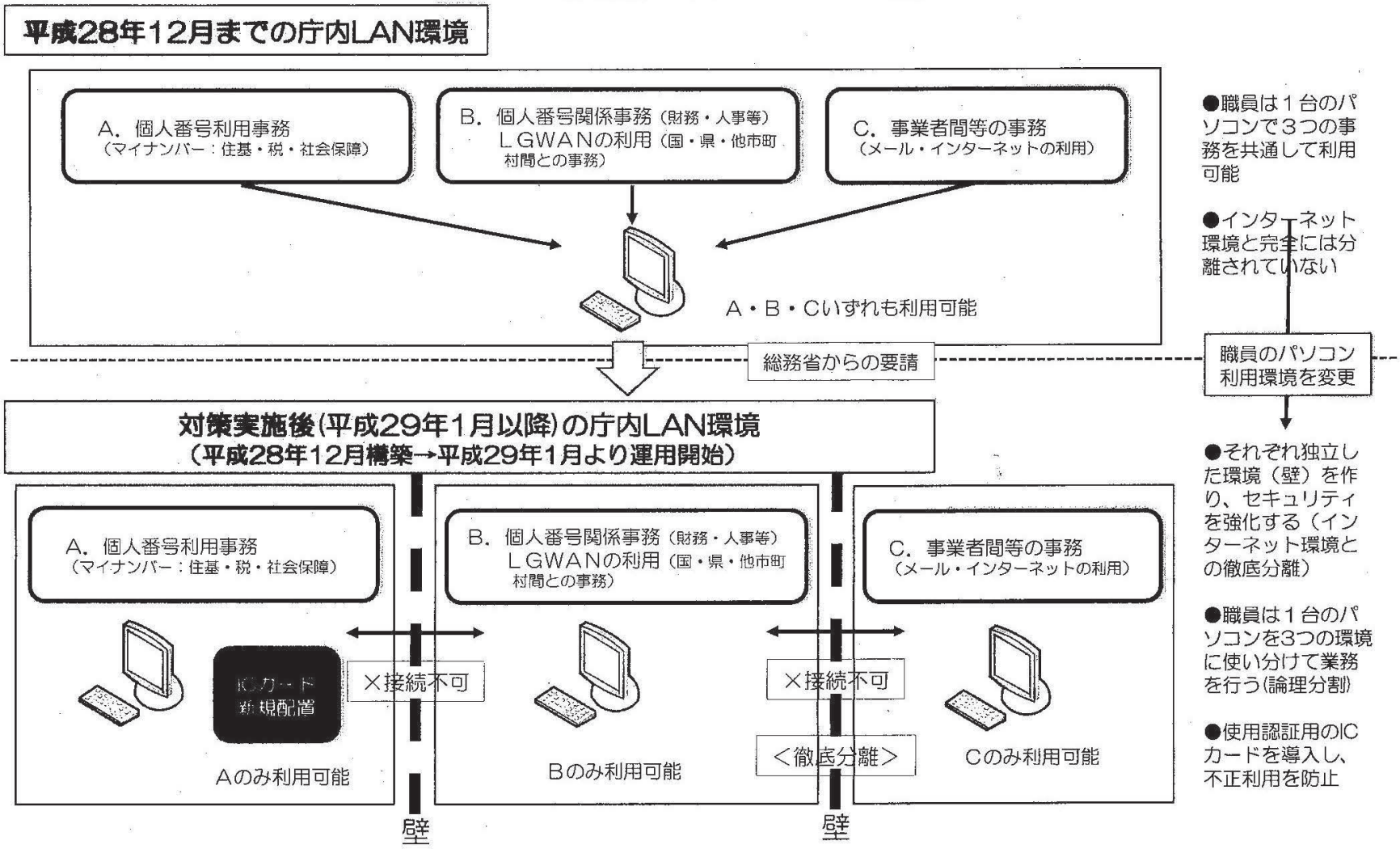
10. 庁内管理情報における情報漏洩発生防止の対策

◎自治体情報セキュリティ強化対策事業の概要

別紙18-1



別紙１９　抜粋

佐世保市 ICT 戦略

令和２年４月

佐世保市

別紙１９　抜粋

目次

別紙１９　抜粋

1 はじめに

本市では、平成 12 年度に「佐世保市地域情報化基本計画」を策定し、それ以降、情報化の取組や ICT（情報通信技術）の利活用を推進してきました。その間、AI（人工知能）をはじめとする先進技術を含め、ICT の技術は急速に進展しており、今やあらゆるサービスや組織、そして社会全体を変革する可能性を秘めたものとして、その重要性や役割が拡大しています。

このような中、本市では令和 2 年度から第 7 次総合計画をスタートします。
人口減少や少子高齢化の進展等、今後、様々な社会課題に直面することとなりますが、「海風 薫り 世界へはばたく “キラっ都” SASEBO」というコンセプトの下、着実に本市のまちづくりを推進していかなければなりません。

そのためには、ICT を「まちづくりの原動力」として位置付け、データを新たな資源として最大限に活用するとともに、官民連携・協働によるイノベーション[1]の創出が必要不可欠です。また、まちづくりの一端を担う行政の分野においても、これまでのあり方に捉われることなく、「行政のデジタル変革」に取り組んでいく必要があります。

ついては、本市における今後の ICT 活用の方向性・方針を明確化し、その取組を加速させることを目的として、ここに本戦略を策定します。

なお、本戦略の構成は次のとおりです。

まず、第 1 章では戦略策定の背景として、本市を取り巻く社会環境の変化、デジタル社会の進展、そして本市のこれまでの情報化の取組状況について整理を行いました。
次に、第 2 章では第 1 章の整理を前提として、本市が今後、ICT を「まちづくりの原動力」と位置付け、積極的に活用していくという大きな方向性を示すとともに、その方向性に基づき、各部局が連携して取組を進めるための 3 つの基本方針を定めました。
最後に、第 3 章ではまちづくりの一端を担う行政の分野において、デジタル化で目指す姿を「市民中心の行政サービスの実現」と定義し、本市の現状と比較することによって、そのギャップを問題点として抽出しました。さらに、その問題点を解決するため、「行政のデジタル変革」という視点から、本戦略で取り組むべき 4 つの課題と、課題に対する具体的な取組の方向性を示す 8 つの重点取組方針を定めました。

---

[1] 技術革新。従来のものとは異なる工夫や方法。新しい工夫。

別紙１９　抜粋

2 位置付け

本戦略は、佐世保市第 7 次総合計画を情報政策の面から補完するものであり、本市の情報政策における最上位の戦略として位置付けるものです。

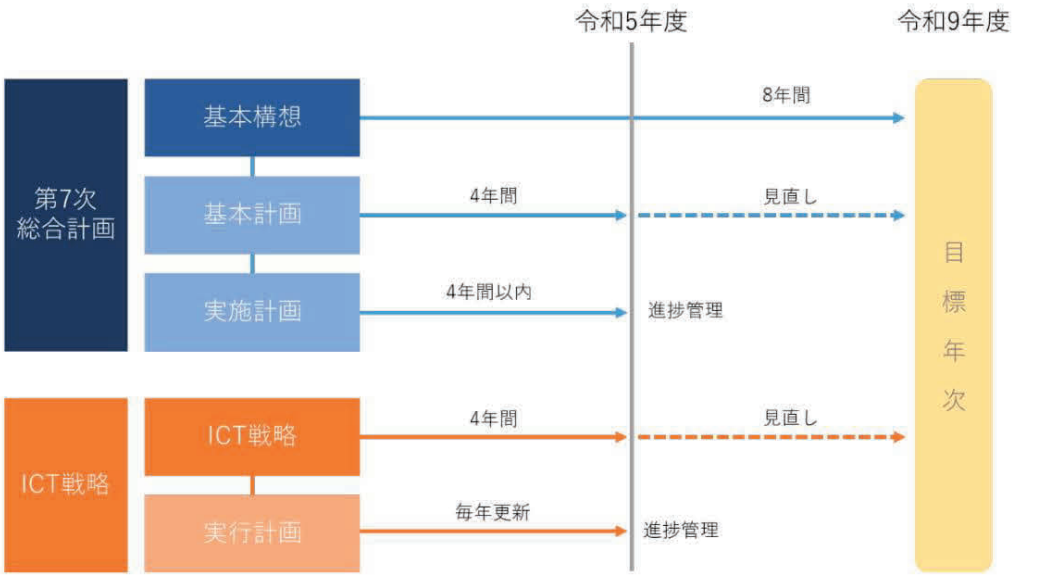
また、官民データ活用推進基本法（平成 28 年法律第 103 号）第 9 条第 3 項に基づく、佐世保市版の「市町村官民データ活用推進計画」としても位置付け、その趣旨に沿って、国、県の施策との整合性を確保しながら、各取組を推進していきます。

3 期間

本戦略の期間は、佐世保市第 7 次総合計画（基本計画）の実施期間に合わせ、令和 2 年度から令和 5 年度までの 4 年間とします。ただし、個別施策・事業について、更に長い期間を設定することが適当な場合はこの限りではありません。

なお、本戦略は、各施策の取組状況や社会情勢の変化、技術革新等の動向を踏まえつつ、必要に応じて内容の見直し、改定を行います。また、期間終了後の取り扱いについては、次期戦略の策定を前提としつつ、本市の情報化に関する意思決定機関である地域情報化推進本部（事務局：総務部情報政策課）において、各取組の進捗状況の把握及び次期戦略の方向性についての検討を行うこととします。

図表 0-3-1　第 7 次総合計画との関連性及び期間



情報セキュリティ監査の内容

別紙２０－２

（1）監査の目的 （情報セキュリティ監査実施要領）

情報セキュリティ対策について、実施状況を点検評価し、問題点の確認、改善方法等の検討、助言、指導、提案を行うことにより、情報セキュリティ対策の維持・向上につなげます。
※助言型監査

（2）監査実施期間
①共同監査　例年８月頃実施
②内部監査　例年８月頃実施

（3）監査形態
①共同監査・・・公的資格者（委託事業者）、情報政策課
②内部監査・・・情報政策課、各部局から選出された情報セキュリティ担当者

（4）被監査部署
①共同監査　例年2部署程度実施
②内部監査　例年8部署程度実施

別紙２０

別紙２０－２

監査後の流れ

①発見事項報告書【監査チーム⇒被監査部署】

・監査で指摘した事項の通知

②処置報告書の提出【被監査部署⇒監査チーム】

・指摘事項に対する処置内容の報告

③フォローアップ監査

・処置内容の確認（処置済・処置中を判断）

・例年１１月頃実施

④処置確認書の提出【監査チーム⇒被監査部署】

・フォローアップ監査で確認した結果の通知

⑤監査完了

・全ての指摘事項が処置済であることを確認

令和2年度　情報セキュリティ監査チェックリスト

監査実施	被監査部署・ﾒﾝﾊﾞｰ：	監査ﾁｰﾑ・ﾒﾝﾊﾞｰ・
		別紙２０－３

要：佐世保市情報資産取扱要綱　　メ：佐世保市電子メール取扱要綱　　接：佐世保市地域イントラネットワーク接続端末等の運用管理要綱　特要：佐世保市特定個人情報取扱要綱

確認すべき事項		項番	重点項目	実地確認事項	自己点検	質問内容	検証ﾋｱﾘﾝｸﾞ事実（文書記録等）	評価	確認すべき文書・記録等	該当条項
1．情報セキュリティ管理・運用体制										
(1)	情報セキュリティに関する取組みを実施する体制を確立している。	1-1-1	○	情報セキュリティに関する体制を整備しているか。（認識されているか。） ・情報セキュリティ責任者を認識しているか。 ・情報セキュリティ担当者を指名しているか。 ・情報管理責任者を認識しているか。 ・情報管理担当者を指名しているか。					組織図、情報セキュリティ管理体制図	要　第７条　各課かい長を、情報セキュリティ責任者とする。 ２ 情報セキュリティ責任者はその所管する課かい等の情報セキュリティ対策に関する権限及び責任を有する。 ３ 情報セキュリティ責任者は、その所掌する課室等において、情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、文書情報セキュリティ監理者、電子情報セキュリティ監理者及び情報セキュリティ統括者へ速やかに報告を行い、必要に応じて情報の取扱いに関する事故等の状況報告書（様式１）を文書情報セキュリティ監理者又は電子情報セキュリティ監理者へ提出しなければならない。 要　第８条　情報セキュリティ担当者は、課かい長が指名した職員を持って充て、次に掲げる事項を行わなければならない。 (1) 情報セキュリティの適正な管理及び円滑な運用を行うため、情報セキュリティ責任者を補佐するものとする。 (2) 情報セキュリティ責任者の指示等に従い、システムの開発、設定の変更、運用、更新等の作業を行うものとする。

別紙２１

情管２１

１．ご依頼事項

第１ 佐世保市情報セキュリティポリシーに関する質問

２ 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。

２．ご回答

（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。

以 上

別紙２１

情管２１

項	実施時期	必要となった事情など	実際に見直したポリシーの内容
1	平成 16 年 6 月 1 日	・自治体が管理している情報の重要性、業務の電子化の進展によるリスクの拡大や情報を取り巻く事件・事故等への対応が必要となったため	・庁内で取り扱う情報について、情報セキュリティを適切に維持するための基本方針、管理・運用方針について制定
2	平成 16 年 10 月 1 日	・指定管理者との契約時に係る規程が無かったため	・指定管理者との契約時の遵守事項等について追加
3	平成 17 年 4 月 1 日	・機構改革を行ったため	・機構改革に伴う、情報セキュリティ委員の役職名の変更
4	平成 18 年 8 月 2 日	・助役が退任したため	・助役退任に伴う、情報セキュリティ委員の役職名の削除
5	平成 19 年 4 月 1 日	・地方自治法の改正に伴い、助役が副市長に変更となったため ・機構改革を行ったため	・助役→副市長への役職名変更 ・機構改革に伴う情報セキュリティ委員の役職名の変更
6	平成 20 年 7 月 1 日	・情報セキュリティポリシー等規定類に基づく情報セキュリティ対策の運用について、制定当初（平成１６年度）から３年が経過し、その間、以下のような課題が発生したため。 ①情報技術の進展等により、規定で記載している事項と実際の運用レベルでの対策内容が一部乖離した状態になっていること ②監査結果に基づく改善事項を規則化し、全庁的な	・情報セキュリティ管理基準を規定　・非常勤及び臨時職員へのポリシー周知徹底 ・外部委託先の選定時及び運用時の基準項目の追加 ・外部委託先との契約書に明記すべき項目の追加 ・情報セキュリティ責任者による情報セキュリティ自己点検実施の明記

別紙２１

		対策の裏づけとする必要があること ③平成１８年度において「地方公共団体における情報セキュリティに関するガイドライン」が全部改正され、必要事項の規則化を検討する必要があること	
7	平成 21 年 6 月 1 日	・機構改革を行ったため	・機構改革に伴う情報セキュリティ委員の役職名の変更
8	平成 28 年 1 月 1 日	・番号法の運用開始に伴い、市の情報セキュリティ対策の拡充と、効果的かつ継続的な推進を図る必要があったため	・情報資産取扱要綱へ条文の移動等
9	平成 31 年 4 月 1 日	・総務省の自治体情報セキュリティ強靭化に伴い、庁内のネットワーク環境を３つに分けたため	・セキュリティ強靭化に伴う、ネットワークの分割について追加

以 上

◎情報セキュリティ職員研修の実施状況

別紙２２－１

No.	研修内容		対象区分	実施年度及び受講者数															
				H16	H17	H18	H19	H20	H21	H22	H23	H24	H25	H26	H27	H28	H29	H30	R1	計（延人数）
1	ポリシー等規定類の解説		全職員	1,342																1,342
2	ポリシーの運用等に関する説明（具体的な実施手順の説明）		各課情報セキュリティ責任者							150						168				318
			各課情報セキュリティ 担当者		105													170		275
			各課情報システム責任者・担当者								48									48
3	ポリシー等規定類の改正内容説明		全職員					1,581												1,581
			各課担当者												94		95			189
4	本市の情報セキュリティに関する取組内容説明		旧合併町職員	135	169				104											408
			新規採用職員			71	54	63	51	66	73	110	94	72	52	80	93	69	56	1,004
5	監査に関する講義・実習		情報セキュリティ内部監査員			30	10	13	20	14	17	10	9	11	12		14	14	8	182
6	e-ラーニング	情報セキュリティ内部監査員・希望者	情報セキュリティ内部監査員・希望者							32										32
		情報セキュリティWeb研修	メールアドレス配布対象者（正職員のみ）											1,851						1,851

◎情報セキュリティ職員研修の実施状況

別紙２２－１

No.	研修内容	対象区分	実施年度及び受講者数															
			H16	H17	H18	H19	H20	H21	H22	H23	H24	H25	H26	H27	H28	H29	H30	R1	計（延人数）
		メールアドレス配布対象者（嘱託職員含む）												1,996	2,008	2,070	2,014	2,072	10,160
7	特定個人情報取扱担当者向け研修	特定個人情報事務取扱担当者															500		500
8	標的型メール攻撃訓練　連続開封者研修	訓練メールの開封者等															28	19	47
9	経営層向け研修	三役、部局長																28	28
計（延べ人数）			1,477	274	101	64	1,657	175	262	138	120	103	1,934	2,154	2,256	2,272	2,795	2,183	17,965
参考	番号制度の概要（e-ラーニング）	全職員												2,150					2,150
		マイナンバー取扱事務担当者													84	102	128	84	398
計（延べ人数）			0	0	0	0	0	0	0	0	0	0	0	2,150	84	102	128	84	2,548

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**

Ⅴ　情報セキュリティ研修（令和元年度）について

研修結果等について報告するものです。

別紙２２－２

研修内容

1. 情報セキュリティ新人研修

実施日時：令和元年5月8日（水）　14:00～15:30
場所：すこやかプラザ8階　講堂

概要：

○平成31年度採用の新入職員（58名）を対象とした研修。

○職員課が主催する「新入職員等・基礎研修B（文書事務等）」の中で実施。

○セキュリティ委託事業者である、㈱サン・パートナーズを講師として、新入職員として覚えるべき情報セキュリティの基礎的事項に関して講義を行った。
講義後は小テスト、解説を実施し、講義に対する理解度を深めた。

情報を守る（バックアップ）

最初に

日常業務で作成したデータを、ルールに基づき適切なフォルダに保存いただいても、様々な理由でそのデータが破損・損失する可能性があります。人的なミスに始まりシステム障害、落雷による停電障害等々、いろいろな原因がありますが、残念ながらそれらを100%防ぐことはできません。そこで必要になってくるのが、情報を守るための手段・バックアップです。

ここではバックアップの基本的なルールについて確認しておきましょう。

関係要綱等：「情報資産取扱要綱第14条、第20条第1号、第52条」

原則

- 職員は**必要なファイルをサーバ等に保存**すること
- サーバ以外の媒体でデータ保存している場合は、**当該媒体とは別の媒体で行う**こと
- **保管期間に基づき実施**し、**期間終了後は適切に破棄**すること

全庁ファイルサーバ等の活用

- **全庁ファイルサーバ**（課内共有等）は、**毎日バックアップを取得**していますので、重要なデータは全庁ファイルサーバに保存するようにして下さい。

  ※Cドライブ、デスクトップ等はバックアップは保存していませんので、削除された場合は復元することはできません。

- 職員ごとに割り当てられている、**B環境のOドライブ**も活用して下さい。

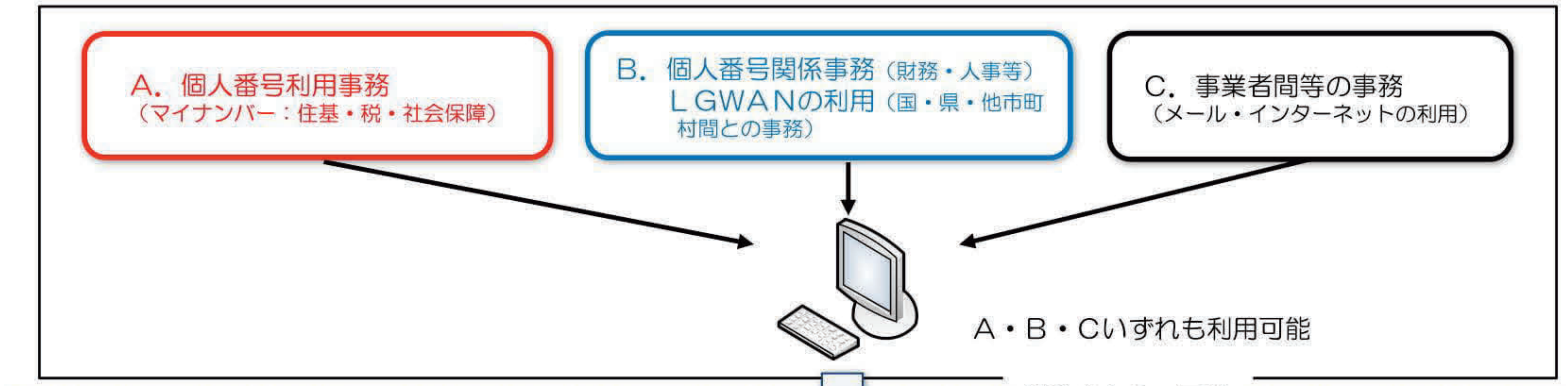
要：佐世保市情報資産取扱要綱　　メ：佐世保市電子メール取扱要綱　　接：佐世保市地域イントラネットワーク接続端末等の運用管理要綱　特要：佐世保市特定個人情報取扱要綱

確認すべき事項		項番	重点項目	実地確認事項	自己点検	質問内容	検証ﾋｱﾘﾝｸﾞ事実（文書記録等）	評価	確認すべき文書・記録等	該当条項
⑷	業務上必要がない電子情報等を庁舎外から持ち込んでいない。	4-4-1	○	業務上必要がない電子情報等を庁舎外から持ち込んでいないか。	評価 改善すべき問題点・課題					
		4-4-2	○	情報管理責任者（課長）の承認を受けて、庁舎外から持ち込んだ電子情報等の内容、使用目的、持込み方法及び管理方法等の履歴管理を行っているか。						

◎自治体情報セキュリティ強化対策事業の概要

別紙２８-1

平成28年12月までの庁内LAN環境



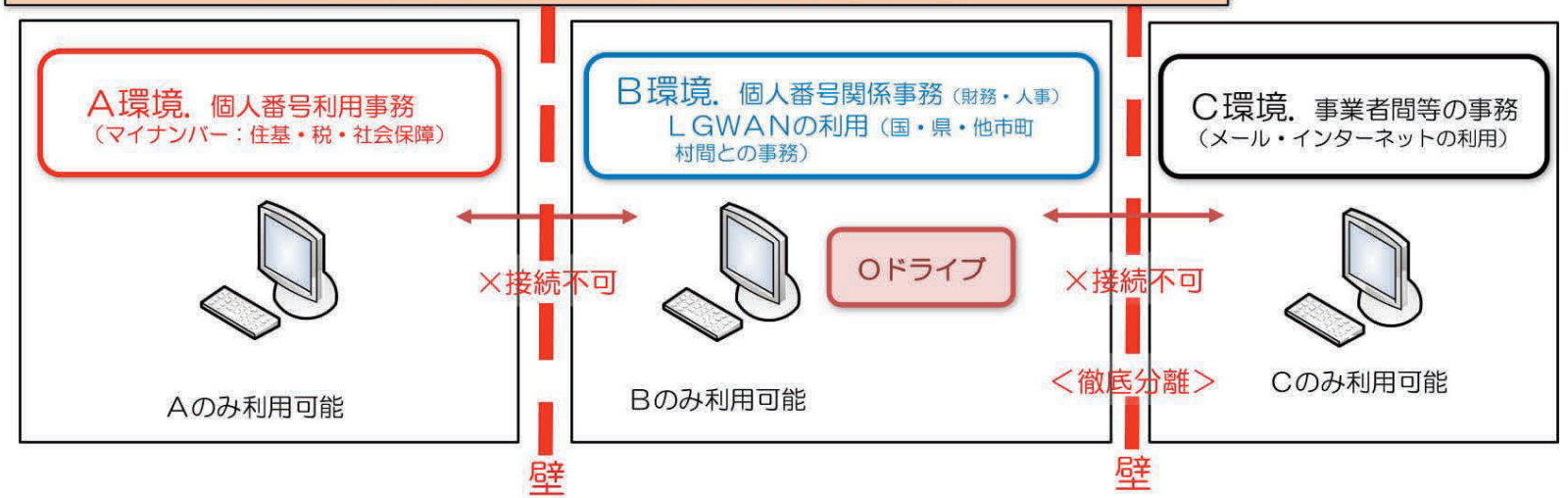
●職員は１台のパソコンで３つの事務を共通して利用可能

●インターネット環境と完全には分離されていない

総務省からの要請

職員のパソコン利用環境を変更

対策実施後(平成29年1月以降)の庁内LAN環境
（平成28年12月構築→平成29年1月より運用開始）



●それぞれ独立した環境（壁）を作り、セキュリティを強化する（インターネット環境との徹底分離）

●職員は１台のパソコンを3つの環境に使い分けて業務を行う(論理分割)

●使用認証用のICカードを導入し、不正利用を防止

情報を守る（ウイルス対策）

最初に

ファイルが添付された電子メールや業務上閲覧するウェブサイト。業務上必要なファイルやウェブサイトの閲覧から、思いがけずウイルスに感染してしまう可能性があります。昨今のウイルスは感染していることが分かり辛く、気付いた時には手の施しようもないほど被害が広がっているケースも多々あります。

職員にとっては市民の方とのやりとりも多く、またそこにはマイナンバーを含む重要な情報も含まれていることが多いため、万が一漏えいした場合、その社会的影響は甚大です。

そこで必要になるのがウイルス対策等の不正プログラム対策です。原則はウイルス対策ソフトのインストールですが、定期的な更新も重要です。

関係要綱等：「佐世保市情報資産取扱要綱（第 67 条第 8、9 項、第 71、82、83 条）」

原則（各課導入パソコン）※1 人 1 台パソコンは情報政策課にてウイルス対策を行っています

- ウイルス対策ソフトは**正常稼働していることを常時確認**すること
- ウイルス対策ソフトよるフルスキャンを、**月次で実施**すること
- ウイルス対策ソフトの定義ファイルは**常に最新の状態**を保っておくこと
- 情報政策課が発する**ウイルス等に関する情報に注意**する

注意事項

- ウイルス対策ソフトのインストール、更新等が確認できない PC 等のイントラネットワークや外部のインターネットに接続、USB 等の電子媒体によるデータのやり取りはしない
- ウイルス対策ソフトの設定は変更しない（定義ファイルのアップデートは行うこと）
- インターネットの利用は最小限とし、業務上関係の無いホームページ、業務上関係があっても、信頼のできないホームページは閲覧しない
- 見覚えのない差出人から出されたメール、本文の内容が不自然なメール等不審なメールを受信した場合は、本文中のリンク、添付ファイル等を開かずに削除する（判断できない場合は、情報政策課に連絡する）

ウイルス対策ソフトウェアを利用するケース（例）

- 外部からデータ及びソフトウェアを取り入れるとき
- メールに添付されたファイル

別紙２９

ウイルス見つかったときの一般的な対処方法

ウイルス感染と思われる症状が発生した場合には、下記の順で対応を行ってください。

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

2. 情報政策課の指示のもと、ウイルススキャンを実施し、ウイルスの感染有無を確認及びウイルス駆除方法を確認し、ウイルスを駆除する

   その後の処理については情報政策課と相談の上、適切に行ってください。

なお下記のようなケースはウイルス感染の可能性があります。

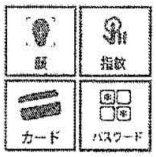
- パソコンの動作が突然重くなった
- パソコンのフリーズや強制終了が増えた
- パソコンが再起動を繰り返す
- 身に覚えのないアプリケーションがインストールされている（デスクトップにショートカットがあある）
- インターネットの接続が不安定である（重い、接続・切断を繰り返す　等）
- 身に覚えのない広告やメッセージ等がデスクトップに表示される
- 特定のサイト（特にセキュリティ関係や Microsoft 等）にアクセスできない
- ウイルス対策ソフトの更新が適切にされなくなった
- Windows Update が実施できない
- フォルダ内のデータが消えている
- フォルダ内のデータ名や拡張子が勝手に変更されている、または開くことができない
- 見覚えがない添付ファイル付きのメールが勝手に送信されていた
- 見覚えのない大量の不達メール（エラーメール）を受信した　　等

今のウイルスは「見つからないように」工夫されていることがほとんどです。（自身が被害者になるだけではなく、自信が“踏み台”になり、加害者になりえる可能性もあります）少しでも「おかしいな」と感じたら、**速やかに情報政策課に相談**をしてください。

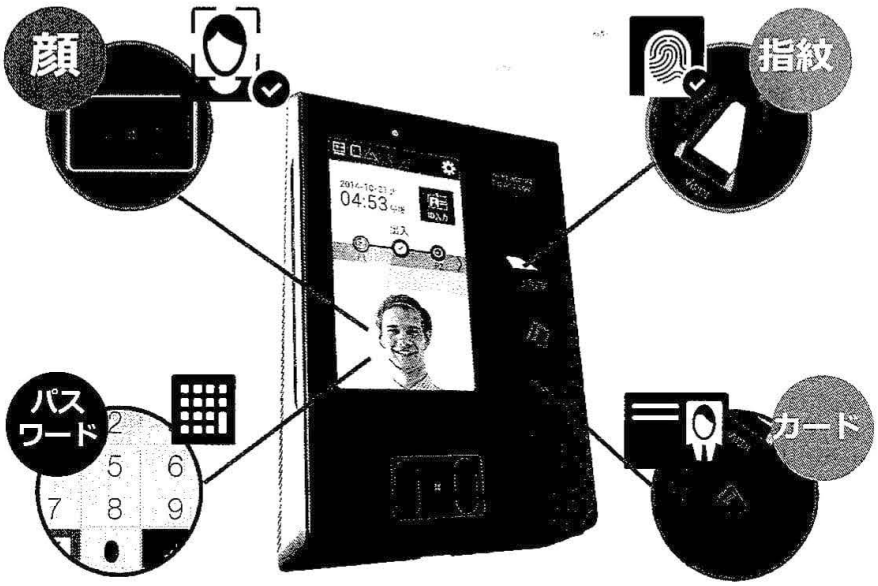
別紙３８

顔認証で入退出セキュリティを強化！

顔認証ドア開閉ユニット



ドアホン型の形状で、単体動作可能な、ドア開閉に特化したコンパクトなシステム。
顔認証に加え、指紋／カード／パスワード認証にも対応。



Powered by
NeoFace
NEC's Face Recognition Technology

ご利用シーン

■ 顔や指紋による生体認証、あるいは、複数の認証要素を組み合わせた多要素認証により、オフィスや機密エリア、重要施設等への入退室セキュリティ強化にご利用頂けます

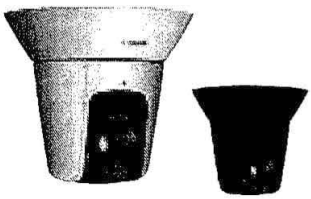
- オフィス
- 機密書類等の保管室
- マイナンバー等重要情報を取り扱う業務エリア
- 食品工場等の生産ライン（フードディフェンスなど）
- 福祉・介護施設
- 病院などの薬品保管ルーム
- 建設現場
- 学習塾、大学や企業の研究棟
- データセンターやサーバルーム　等

※「顔認証ドア開閉ユニット(AC-7000 NeoFace)」は京栄社株式会社がNEC製顔認証エンジン「NeoFace」を用いて企画・開発した製品です。

別紙３８

あらゆるモニタリングに貢献する スタンダードモデル。

屋内モデル　**スタンダード**



VB-H43
H43B

〈9902B001〉シルバー
〈9902B002〉ブラック
希望小売価格
各258,000円（税別）

【商品構成】本体、CD-ROM、電源用コネクター、設置ガイド、録画ソフトRM-Lite

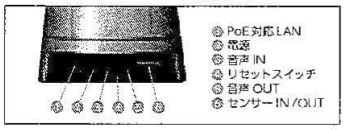
PTZ　光学ズーム 20x　FULL HD

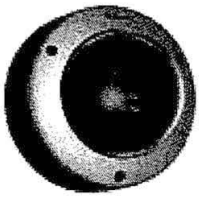
VB-M42
M42B

〈9906B001〉シルバー
〈9906B002〉ブラック
希望小売価格
各218,000円（税別）

【商品構成】本体、CD-ROM、電源用コネクター、設置ガイド、録画ソフトRM-Lite

PTZ　光学ズーム 20x　1.3 MEGA　RoHS（VB-M42B）





【商品構成】本体、CD-ROM、電源用コネクター、落下防止用ワイヤー、音声インターフェースケーブル、型紙、設置ガイド、録画ソフトRM-Lite

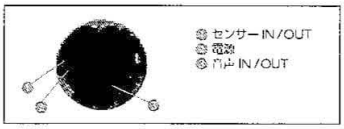
光学ズーム 3x　FULL HD

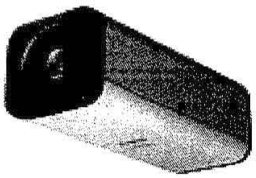
VB-M620D

〈9908B001〉
希望小売価格
118,000円（税別）

【商品構成】本体、CD-ROM、電源用コネクター、落下防止用ワイヤー、音声インターフェースケーブル、型紙、設置ガイド、録画ソフトRM-Lite

光学ズーム 3x　1.3 MEGA





VB-H730F

〈9905B001〉
希望小売価格
158,000円（税別）

【商品構成】本体、CD-ROM、電源用コネクター、設置ガイド、録画ソフトRM-Lite

光学ズーム 3x　FULL HD

VB-M720F

〈9909B001〉
希望小売価格
118,000円（税別）

【商品構成】本体、CD-ROM、電源用コネクター、設置ガイド、録画ソフトRM-Lite

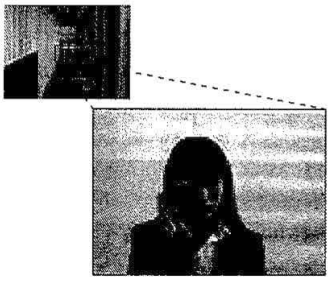
光学ズーム 3x　1.3 MEGA　RoHS

スタンダードモデルの主な特長

光学20倍ズームレンズと ワイドな視野のパンチルト

※VB-H43/VB-M42

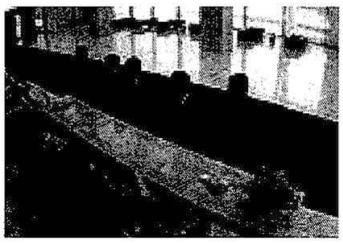
キヤノンが培ってきたレンズ技術、ビデオ技術の集積から、高精細・高解像度を保ちながら光学20倍かつワイド端での画角の広さを両立。オフィスや工場、デパート、展示場など、広大なエリアをカバーします。



広角100°超の光学3倍 ズームレンズを搭載

※ドーム・ボックス型モデル共通

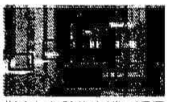
F1.2の明るいレンズで、鮮明なモニタリングを実現。狭いスペースも広く撮影でき、オフィスや店舗などさまざまな場所に設置できます。



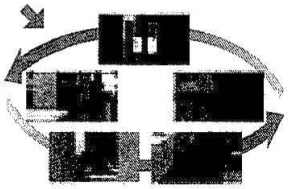
※ズーム機能は設置時のみの利用を想定。

デジタルPTZ機能

広角100°超のレンズが捉えた映像から任意エリアだけを切り出し、PTZモデルのように配信してプリセット巡回も可能。広いエリアを少ないカメラ台数でモニタリングできます。



指定した映像を巡回配信



別紙４１　抜粋

「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

平成 29 年２月 16 日
（平成 30 年７月 20 日更新）
個人情報保護委員会

別紙４１　抜粋

「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

目次

別紙４１　抜粋

１　ガイドライン（通則編）

１-１ 定義

（個人情報）

Ｑ１－１　「特定の個人を識別することができる」とは、どのような意味ですか。

Ａ１－１　「特定の個人を識別することができる」とは、社会通念上、一般人の判断力や理解力をもって、生存する具体的な人物と情報との間に同一性を認めるに至ることができることをいいます。

（個人情報）

Ｑ１－２　ガイドライン（通則編）では、氏名のみでも個人情報に該当するとされていますが、同姓同名の人もあり、他の情報がなく氏名だけのデータでも個人情報といえますか。

Ａ１－２　本人と同姓同名の人が存在する可能性もありますが、氏名のみであっても、社会通念上、特定の個人を識別することができるものと考えられますので、個人情報に該当すると考えられます。

（個人情報）

Ｑ１－３　住所や電話番号だけで個人情報に該当しますか。

Ａ１－３　個別の事例ごとに判断することになりますが、他の情報と容易に照合することにより特定の個人を識別することができる場合、当該情報とあわせて全体として個人情報に該当することがあります。

（個人情報）

Ｑ１－４　メールアドレスだけでも個人情報に該当しますか。

Ａ１－４　メールアドレスのユーザー名及びドメイン名から特定の個人を識別することができる場合（例：kojin_ichiro@example.com）、当該メールアドレスは、それ自体が単独で、個人情報に該当します。

　これ以外の場合、個別の事例ごとに判断することになりますが、他の情報と容易に照合することにより特定の個人を識別することができる場合、当該情報とあわせて全体として個人情報に該当することがあります。

（個人情報）

Ｑ１－５　新聞やインターネットなどで既に公表されている個人情報は、個人情報保護法で保護されるのですか。

Ａ１－５　公知の情報であっても、その利用目的や他の個人情報との照合など取扱いの態様によっては個人の権利利益の侵害につながるおそれがあることから、個人情報保護法では、既に公表されている情報も他の個人情報と区別せず、保護の対象としています。

別紙 42 抜粋

情報処理技術者試験
情報処理安全確保支援士試験

試験要綱

Ver.4.6

2021 年 4 月の試験から適用

IPA 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

別紙 42　抜粋

1. 実施する試験区分

次の図に示すとおり，情報処理技術者試験及び情報処理安全確保支援士試験を実施する。

情報処理技術者試験は，IT パスポート試験，情報セキュリティマネジメント試験，基本情報技術者試験，応用情報技術者試験及び高度試験（IT ストラテジスト試験，システムアーキテクト試験，プロジェクトマネージャ試験，ネットワークスペシャリスト試験，データベーススペシャリスト試験，エンベデッドシステムスペシャリスト試験，IT サービスマネージャ試験及びシステム監査技術者試験）で構成する。

別紙４７　抜粋

事　務　連　絡
令和元年 12 月 11 日

各課かい長 様

情報政策課長

パソコン等の廃棄処分時の対応について（通知）

パソコンやハードディスク等、情報を記録できる電子媒体（以下、パソコン等）を廃棄処分する場合は、情報の流出・漏えいを未然に防止するため、パソコン等の内部に保存されたデータを完全に消去の上、廃棄する必要があります。

ニュース等でも報道されておりますが、先般他の自治体において、データ消去が不十分な状態のハードディスクが第三者の手にわたり、個人情報を含む行政文書が漏洩した事故が発生しております。

パソコン等を廃棄する場合は、下記の要領にて必ず取り扱うよう、貴課かい職員に周知・徹底くださいますようお願いいたします。

記

１．パソコン等を廃棄する際のデータ消去方法について

廃棄前に必ず以下の方法にてデータの消去作業を実施してください。

※詳細は、廃棄手順を含め庁内用 FAQ「パソコン廃棄手順書（ID：2980)」にも記載しておりますので、あわせて参照してください。

[データ消去方法①]職員が実施する場合

情報政策課で貸出している「データ消去ソフトウェア」を用いて、各課にてデータ消去作業を実施してください。

※特殊な構成を組んでいるサーバ等（業務システム）は、サーバの構築事業者でなければ消去作業が実施できない場合がありますので、構築事業者へお尋ねください。

[データ消去方法②]事業者へ委託する場合

各システム等の構築・保守事業者等へデータの消去作業を委託する場合、次の点に注意して委託契約を行ってください。

＜委託作業時の注意点＞

・作業実施場所は、原則、市の施設内としてください。
・委託先事業者から「データ消去証明書」を必ず取得してください。

以 上

担当：前田か・竹野・峯
内線：2704、2703、2701

使用済みパソコンの処分に係る手順

令和元年１２月更新
佐世保市総務部情報政策課

佐世保市においては、平成28年1月に策定した佐世保市情報セキュリティポリシー、並びに佐世保市情報資産取扱要綱に基づき、情報セキュリティに万全を期しながら、資源有効利用促進法の資源の有効な利用の趣旨を踏まえ、使用済みパソコン等の処分について以下のとおり手順としてまとめる。

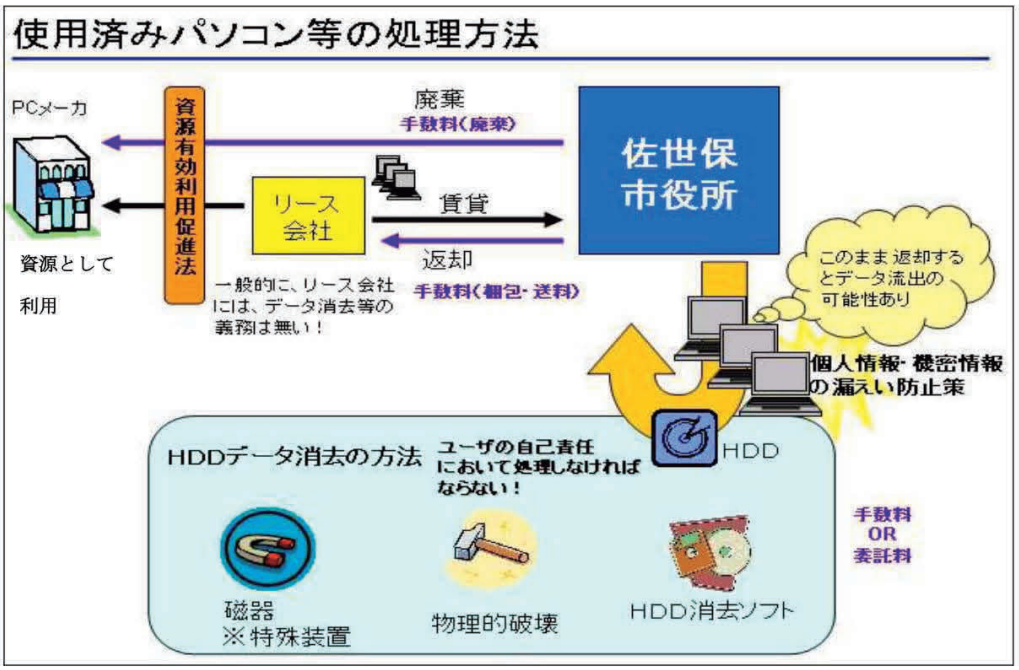
※一般社団法人パソコン3R推進協議会のホームページ（http://www.pc3r.jp/office/index.html）も参考にすること。

【用語の定義】
○パソコン等･･･パソコンやサーバ、ハードディスク等、情報を記録できる電子媒体

Ⅰ．実施の手順

使用済みパソコン等の処理については、「買取り（又は譲渡）」により取得している場合、「リース（賃借）」により使用している場合がある。また、数が多くパソコンのメーカ・機種が複数混在する場合があることから、これらの諸事情を勘案して、使用済みパソコン等を所有している課かいが、それぞれ最も遂行可能な方法により、廃棄処理を行うことを基本とする。

［図1：使用済みパソコン等の処理方法］



抜粋（参考資料）

（HDD物理破壊後）※1～50

（HDD物理破壊後拡大）※1～50

エコー電子工業株式会社
富士通九州リサイクルセンター

ID・パスワードを管理する

最初に

情報セキュリティにおいて、パスワードの重要性を疑う方は少なくないでしょう。今では、個人所有のスマートフォンへのログインパスワードから始まり、ありとあらゆるウェブサービス等でも複数のパスワードを当然のように運用されていると思います。

本市の業務においては、個人貸与のパソコンでのログイン時だけではなく、様々なシステムにアクセスする際のパスワード、その他複数の職員で共同利用しているIDへのパスワード等、職種や職位によって複数のパスワードを利用している方も少なくないと思われます。

日々の業務をよりセキュアな環境にするために、ここでは業務における適切なパスワード及びIDの管理について改めて確認しましょう。

関係要綱等:「佐世保市情報資産取扱要綱(第38条、50条、73条)

パスワード設定および運用の原則

- 他人に教えないこと
- 他人の目に触れさせないこと(付箋等でPC等に貼り付けるのはNG)
- パソコンに記憶させないこと
- 同じパスワードを使いまわさないこと

共同利用IDのパスワードの設定および運用の原則

上記「パスワード設定および運用の原則」以外にも下記の観点での注意が必要です。

- 利用者以外にパスワードが漏れないようにする
- 業務上の必要がなくなった場合は利用者登録の抹消申請を行う

※臨時職員等の ID で必要が無くなったものは、ユーザ削除依頼書（FAQ ID 3300）を情報政策課に提出してください。

・共同利用 ID の利用者の異動及び退職等が生じた場合はパスワードの変更を行う

添付資料【佐世保市の情報セキュリティに関する各役職の権限・義務等の図／監査人試作】