必須科目　　10時～12時30分

Ⅱ　次の２問題（Ⅱ－１，Ⅱ－２）のうち１問題を選んで解答せよ。（**解答問題番号**を明記し，答案用紙３枚以内にまとめよ。）

Ⅱ－１　資料Ａ及び資料Ｂは非常時における情報システムの対応に関する資料の一部である。これらをよく読み，情報工学の技術士の立場から次の（１）～（３）の問いにそれぞれ答案用紙１枚以内で答えよ。

（１）重要インフラ事業者の情報システム部門，及び外部組織に関わる者（以下，システム担当者）が負う責務のうち，特に重要と考えるものを１つ挙げよ。また，システム担当者が，その責務を全うするために準備すべきことを３つ，実際にプロジェクトを進めるときに行うべきことを３つ，それぞれ述べよ。

（２）システム担当者は，経営層とコミュニケーションを密にとる必要がある。そのコミュニケーションでは，具体的にどのような情報をやりとりすべきか。システム担当者から経営層へ渡される情報を１つ，経営層からシステム担当者へ渡される情報を１つ，それぞれ述べよ。また，それらの情報が受け渡される必要がある理由を述べよ。

（３）重要インフラ情報システムを開発し，その信頼性を確保し続けるために，心がけなければならないことを１つ挙げ，それが重要である根拠も述べよ。

資料Ａ：重要インフラ情報システムの信頼性向上の取組みガイドブック，
（独）情報処理推進機構ソフトウェア・エンジニアリング・センター，
2011年３月（抜粋，一部改変）

第１章　重要インフラ情報システムの信頼性の状況

１－１ 重要インフラ情報システムが置かれた状況と課題

重要インフラの中の情報システムすなわち重要インフラ情報システムは、年々その重要性を増している。
その理由は以下である。

- 既に、多くの重要インフラにおいて、人間が手動で操作・制御していたのでは間に合わない、正確かつ大量のサービスが提供されている。そこでは多種かつ大量の情報システムが重要インフラにおけるサービス（以下、「重要インフラ・サービス」）を提供する基盤（以下、「サービス提供基盤」）の中に組み入れられ、人間に代わって、あるいは人間が及ばない操作、制御を行っている。
- これら重要インフラ・サービスを利用する国民生活及び社会経済活動は、上記の重要インフラ・サービスが継続的、安定的に提供されることを期待して営まれている。
- さらに、国民生活を豊かにするため、また社会経済活動を活発にするため、日々、追加的なサービスが考案され、提供されている。その結果、サービス提供基盤の中の情報システムは年々高度化される。
- 情報システムの高度化により、提供される重要インフラ・サービスは一回り大きくなる。そして、そのサービスの利便性が国民に実感され、かつ、そのサービスが安定して提供されるようになると、さらに国民生活は、その一回り大きいサービスが継続的に提供されることを期待して営まれるようになる。

こうして、提供される重要インフラ・サービスの質・量の拡大と、その国民生活や社会経済活動への定着のループが、サービス提供基盤に置かれた情報システム、すなわち重要インフラ情報システムの重要性を増していく。

しかし、こうした重要インフラ情報システムの重要性の増加に対して、それを十分に支える管理活動が確実に実施されているかといえば、そうは言い切れない。

具体的には、情報システムに何らかの不具合が生じた結果、重要インフラ・サービスの安定供給ができなくなり、その結果、国民生活又は社会経済活動に影響が及んだトラブル事例が、頻繁とはいえないものの近年でも発生している。（図表１－１）

業　種	時　期	トラブル事例　（概要）
鉄道	2007 年 10 月	自動改札機へのデータ授受の様式誤りがきっかけとなって、自動改札機が機能しなくなった。
金融	2008 年 5 月	情報システムの更新に伴って、他行に送付した電文の形式に誤りがあり、他行ＡＴＭとの間で入送金が不能になった。
航空	2009 年 6 月	ソフトウェアの更新に伴う、旅客チェックインシステムの障害で、航空便の欠航・遅延が多数発生した。
金融	2010 年 7 月	通信用システムの不具合により、他行との間で入送金が不能になった。

図表１－１　情報システムの不具合が重要インフラ・サービスの提供に影響を与えた事例

これらトラブル事例の直接的な原因は、重要インフラ情報システムが、その製造ミス（要件定義ミスや、ソフトウェアへのバグの混入を含む）等による故障、劣化、あるいは操作ミスなどによって、その情報システムに求められた要件どおりに機能できなくなったことである。この種のトラブルは、重要インフラ・サービスの利用者からみれば、「重要インフラ・サービスの提供の信頼性の不足」と捉えられる。

重要インフラ・サービス、あるいは重要インフラ情報システムの不具合について新聞等マスメディアで報道される件数は、2000 年台前半に比べれば減少している。また、重要インフラ情報システムの信頼性もここ数年は確実に確保されていることがうかがえる調査データもある。（調査結果の１つを、１－１の後のコラムに示す。）
しかし、人やモノの移動、契約や取引、あるいは生産や販売などの活動に目立った影響が及べば、マスメディアがこれを取り上げ、また国民が関心をもつことには変わりがない。

重要インフラ事業者には、重要インフラ・サービスに関して、その質・量の拡大と、安定供給とを同時に実現する取組みが求められている。

コラム　重要インフラ情報システムの信頼性の現状

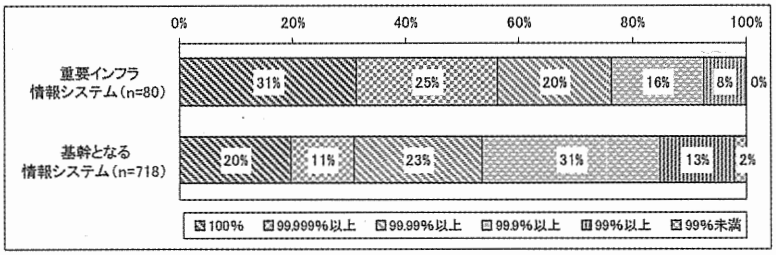
(社)日本情報システム・ユーザー協会（以下、「ＪＵＡＳ」）では、毎年、ＩＴ動向調査を実施している。ＪＵＡＳは、その 2009 年度の調査で情報システムの信頼性実績について調査を行った。内容は、情報システムの重要度と稼動率の関係などを調べたものである。結果は図Ａのとおりであり、重要インフラ情報システムについては、既に高い信頼性が確保されていることがうかがえる。

□調査結果：

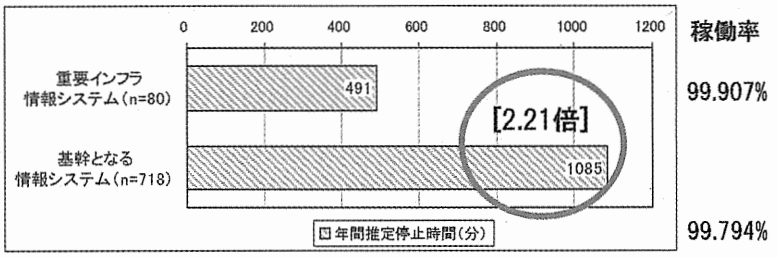
停止時間という観点だけから見れば、「重要インフラ情報システム」の信頼性は「基幹となる情報システム」より 2.21 倍高い。但し、「稼働率の目標値なしまたは不明」という企業が調査対象の 1/4 であった。

重要インフラ情報システムと基幹となるシステムの稼働率の比較

・稼働率99.999%から99.9%にかけて、年を追うごとに割合が高くなっていること、つまり情報システムの信頼性が年々高くなっていることがわかる。



重要インフラ情報システムと基幹となるシステムの稼動時間(推定)



図Ａ　企業等で使われている情報システムの稼動率の調査結果（２００９年度）

【 出典：ＪＵＡＳ　ＩＴ動向調査２００９】

1－2 重要インフラ情報システムの特徴

重要インフラ情報システムの信頼性について考える前に、そもそも重要インフラや重要インフラ情報システムとはどのようなものであるか、その特徴を整理する。

重要インフラそのものと、そこで使用されている情報システムは次のような特徴を持つ。

（1）重要インフラの特徴

1．国民生活に欠かせない社会的なサービスを長期にわたって提供している。重要インフラの種類によっては１００年を超える歴史を有している。
2．重要インフラ・サービスへのニーズは、サービス利用者である国民や企業の所在や社会様式によって変化する。
3．したがって、重要インフラ・サービスへの信頼性に関する要求（以下、「信頼性要求」）の決定には、サービスの利用者である国民との合意が重要である。重要インフラ事業者は、国民の考え、価値観を把握して、提供するサービスについての目標を検討する必要がある。

（2）重要インフラのサービス提供基盤の特徴

1．重要インフラ事業者は、サービス提供基盤にその時代で使用可能な技術を適宜採用して、その信頼性や効率性を追求してきた。サービス提供基盤への情報システムの大規模な活用はここ３０～４０年に行われたことであり、情報システムの活用拡大は今後も続くと考えられる。
2．重要インフラのサービス提供基盤の構築のための投資額は非常に大きい。また、このサービス提供基盤の運営に関係する要員、また事業者内外での利用者は多数にのぼり、サービス提供基盤を世代交代させるには、教育、訓練も必要になる。こうしたことから、一度構築されたサービス提供基盤は、大きな欠陥が顕在化しない限り、改良がされながら使い続けられる。
3．サービス提供基盤では、サービスを提供するのに必要なさまざまな仕組みが、情報システムを含む多数の構成要素を使って作られている。これらの構成要素はサービスの円滑な提供において生じた問題への対応、または新たなサービスの提供の必要に応じて、改良、更新、追加される。

（3）重要インフラ情報システムの特徴

したがって、重要インフラ情報システムとは、重要インフラのサービス提供基盤の要素として、重要インフラ・サービスの質・量の拡大と安定提供のために、他の要素との連携を変化させつつ、改良、更新、追加されながら、長期にわたって使用されている情報システムである。（図表１－２）

第2章　重要インフラ情報システムの開発・保守の管理フレーム

１章で述べた、重要インフラ情報システムの特徴、そこで必要となる信頼性を確保する事業者の活動について、重要インフラ事業者の取組みについての調査結果をもとに説明する。

2－1　開発・保守の管理フレームの全体像

重要インフラ情報システムも、情報システムの一種であるので、その信頼性確保のために行える活動は基本的に同じである。たとえば、企画・要件定義あるいは開発の工程であれば、レビュー、テストといった信頼性向上のための方策を適確に実施することである。

しかし、重要インフラ情報システムでは、以下の点が、強く求められていると考えられる。

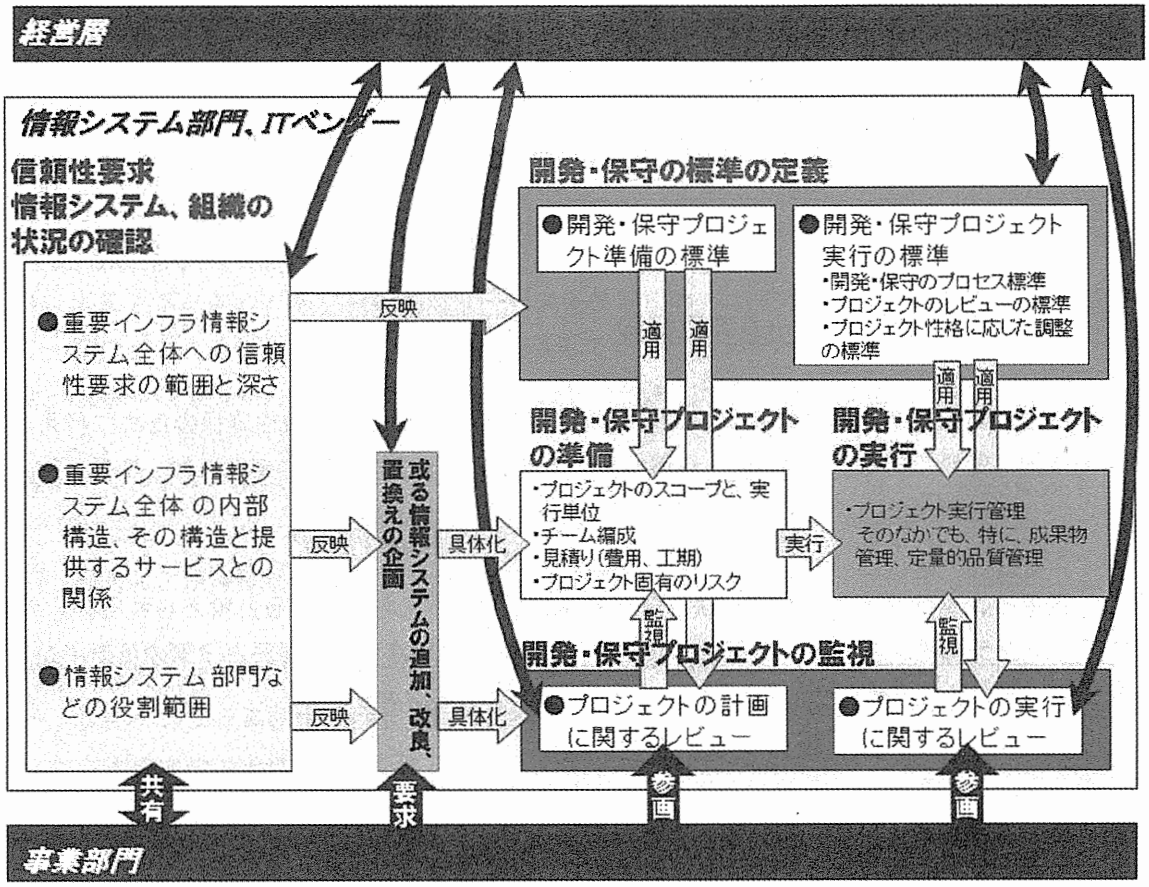
- *重要インフラ情報システムに必要な信頼性は、事業者と利用者である国民との間の重要インフラ・サービスの信頼性についての合意と結び付けて考える必要がある。*

上記を考えると、重要インフラ情報システムにおいては、一般の情報システムと同様に信頼性向上のための方策を適切に計画・実施することに留まらず、その信頼性向上の方策が事業者と利用者の合意を満たすのに有効であることの保証までされる必要がある。
保証までをするためには、以下のような目標となる「信頼性要求」を決め、その実現を確かめる活動が必要になる。

- 何についての信頼性をどの位必要とするのか、といった情報システムへの信頼性要求の明確化。さらに情報システムへの信頼性要求に影響する、情報システムの構造や、情報システム部門の役割範囲についての確認
- 情報システムへの信頼性要求を満たすための方法としての、開発・保守のプロセス標準、レビューの標準の定義
- 上項の標準を適用した、情報システムの開発・保守プロジェクトの準備
- 同じく、情報システムの開発・保守プロジェクトの実行
- 情報システムの開発・保守プロジェクトが確実に実施され、その結果、情報システムへの信頼性要求が確保されていることの監視
- 上記の活動を相互に適確に関連づけること

具体的には、図表２－１のような取組みである。
以降、この図表が示す範囲の活動を、重要インフラ情報システムの開発・運用の管理フレーム（以

下、単に「管理フレーム」と呼ぶ。）とし、以下の節でその内容を取り扱う。



図表２－１　重要インフラ情報システムの開発・運用の「管理フレーム」

2－2 管理フレームによって実現すべきこと

２－２では、重要インフラ情報システムの信頼性確保の取組みについて求められる基本的な事柄、および「管理フレーム」の意味について説明する。

2－2－1 信頼性確保の取組みの確立

２－１で、重要インフラ情報システムの強く求められている点として、次を述べた。

- *重要インフラ情報システムに必要な信頼性は、事業者と利用者である国民との間の重要インフラ・サービスの信頼性についての合意と結び付けて考える必要がある。*

ここで、各事業者は、以下のことに注意が必要である。

- 事業者と利用者である国民との間の重要インフラ・サービスの信頼性についての合意の内容は、重要インフラ・サービスによって異なっている。
- 重要インフラ・サービスの信頼性を、情報システムで支える方法には様々なものがあり、現行の方法は事業者や業種、過去の経緯により異なっている。
- 情報システムの信頼性に関わる事柄の、自社の情報システム部門、情報システム子会社、外部組織（ＩＴベンダーなど）による役割分担も、事業者によって異なる。

したがって、重要インフラ事業者は、情報システムの信頼性確保に関する他の事業者の取組みを参考にすることは出来ても、それをそのまま実施することが有効とは限らない。
各事業者は、事業内容やそこでの利用者との関係や、情報システムの位置づけや構造といった、事業者固有の状況に適した信頼性確保の取組みを確立することが必要である。
「管理フレーム」は、その信頼性確保の取組みを確立するための道具である。

2－2－2 信頼性を確保し続けること

重要インフラ情報システムは改良、更新、追加されながら数十年の長さにわたって使われる。したがって、重要インフラ情報システムの信頼性も数十年の長さで確保され続ける必要がある。
その間に、重要インフラを取り巻く環境は大きく変わっていくから、以下の３点については適宜見直しが必要である。

- 事業者と利用者（国民）との間の重要インフラ・サービスの信頼性についての合意の内容
- 重要インフラ・サービスの信頼性を、情報システムで支える方法
- 情報システムの信頼性に関わる事柄の、自社の情報システム部門、情報システム子会社、外部組織（ＩＴベンダー等）による役割分担

つまり、信頼性確保の取組みに改善サイクルを回し、「管理フレーム」の内容を描き換えていくことが必要となる。

この改善サイクルにおいて、事業者外の関係者とコミュニケーションをとることによって、その改善の有効性が更に高まることが期待される。そのコミュニケーションとは以下のようなものである。

- 利用者である国民に対する重要インフラ・サービスの信頼性についての実績値や、その改善策の概要説明、それに対する利用者の意見の収集
- 重要インフラ・サービスの信頼性を、情報システムで支える方法についての、同一業種内での知見の共有、異業種間での知見の交換
- 情報システムの信頼性確保の方法についての、外部組織（ＩＴベンダーなど）との協議

２－３ 活動フレームとステークホルダー

２－３では、重要インフラ情報システムの信頼性確保の取組みのために、その情報システムのステークホルダーに求められる役割について説明する。
２－３の内容は、重要インフラ事業者で実際行われていることをヒアリングした結果（第４章にて説明）に基づいている。

２－３－１ 重要インフラ事業者の情報システム部門、および外部組織

情報システム部門は、情報システムへの信頼性要求を把握、管理し、それを満たす開発・保守を準備、実行し、要求の実現性を確かめ、評価し、評価結果と必要なら対策を取りまとめる必要がある。具体的には、以下の役割が期待される。

期待される役割

(1) 情報システムへの信頼性要求のとりまとめ、管理
(2) 情報システム全体の構造、その提供サービスとの関係の整理
(3) 情報システム部門など情報システムの関係者の役割範囲の整理
(4) 情報システムの信頼性提供の見込みの情報システム関係者への提示
(5) 個別の開発・保守プロジェクトが、情報システムの信頼性提供の見込みを満たすようにする、準備と実行
(6) 個別の開発・保守プロジェクトが、情報システムの信頼性提供の見込みを満たしていることの監視
(7) 情報システムの信頼性の評価
(8) 情報システムの信頼性の評価結果に基づく対策の立案
(9) 情報システムの信頼性の評価結果と対策の提示
(10) 承認された対策の実施

上記は、広範にわたる上、(5)と(6)のように、同じ要員が活動することが適当でないものも含まれるので、情報システム部門の内部での適切な分担が欠かせない。

また、外部組織（ＩＴベンダーなど）には、重要インフラ事業者の情報システム部門との協議の上、以下の役割を代行することが期待される。

期待される役割

※ 以下の項番は、情報システム部門に期待される役割の項番と共通である。

(5) 個別の開発・保守プロジェクトが、情報システムの信頼性提供の見込みを満たすようにする、準備と実行

(6) 個別の開発・保守プロジェクトが、情報システムの信頼性提供の見込みを満たしていることの監視

(7) 情報システムの信頼性の評価

(8) 情報システムの信頼性の評価結果に基づく対策の立案

(9) 情報システムの信頼性の評価結果と対策の提示

(10) 承認された対策の実施

2－3－2 重要インフラ事業者の事業部門

事業者のうち、情報システムの利用者である事業部門は、主に業務要件[5]レベルで、外部環境を把握して情報システムへの信頼性要求を作り、それが実現される過程をモニターし、実際の信頼性が十分かを評価する必要がある。具体的には、以下の役割が期待される。

期待される役割

(1) 重要インフラ・サービスの信頼性について、主に業務要件レベルでの外部関係者との合意

(2) 上記のうち、情報システムに関係する部分の識別

(3) 情報システムへの、主に業務要件レベルでの信頼性要求のとりまとめ

(4) 情報システムの信頼性提供の見込みの承認

(5) 個別の開発・保守プロジェクトの承認

(6) 個別の開発・保守プロジェクトへの監視への参画

(7) 情報システムの信頼性の評価結果と対策の承認

(8) 重要インフラ・サービスの信頼性について、主に業務要件レベルでの外部関係者への説明

[5] 「業務要件」については、２－３の後の囲み記事に示す。

2－3－3 重要インフラ事業者の経営層

事業者の経営層は、事業要件[6]レベルで、外部環境を把握して情報システムへの信頼性要求を作り、それが実現される過程をモニターし、実際の信頼性が十分かを評価する必要がある。具体的には、以下の役割が期待される。

期待される役割

(1) 重要インフラ・サービスの信頼性について、事業要件レベルでの外部関係者との合意
(2) 上記のうち、情報システムに関係する部分の識別
(3) 情報システムへの、事業要件レベルでの信頼性要求のとりまとめ
(4) 情報システムの信頼性提供の見込みの承認
(5) 個別の開発・保守プロジェクトの承認
(6) 個別の開発・保守プロジェクトへの監視への参画
(7) 情報システムの信頼性の評価結果と対策の承認
(8) 重要インフラ・サービスの信頼性について、事業要件レベルでの外部関係者への説明

6 「事業要件」については２－３の後の囲み記事に示す。

資料Ｂ：早期復旧，BCPが奏功　宮城の被災中小企業，
河北新報のニュースサイト・コルネット，2011年４月３日

早期復旧、BCPが奏功　宮城の被災中小企業

震災後1週間ほどで事業を再開し、プラントの修復にも当たるオイルプラントナトリの従業員＝3月29日、名取市

東日本大震災は、沿岸部を中心に多くの中小企業にも被害を与えた。壊滅を免れた企業の中には、事業継続計画（BCP）を生かし、早期復旧を果たしたケースがある。未曽有の危機にどう対応したのか。宮城県内で取材した。

名取市のリサイクル業「オイルプラントナトリ」。海岸近くにある廃油や廃プラスチックの再処理工場は、タンク15基の3分の2が流失しプラント建屋も破壊された。

廃油回収業務は震災後約1週間で再開。3月22日には残ったタンク車と設備で工場廃水の中和処理も始めた。「ことし1月に策定したBCPが奏功した」と武田洋一社長は言う。

会社は震災直後、従業員約40人を避難させ、登記上の本社がある内陸側の民家に本社機能を移した。廃油回収の再開に当たっては、県内の同業者と連携した。

BCPには運送業者など支援を頼める協力会社を盛り込んでいた。廃水処理などを柱に売上高を5割減にとどめる想定もしていた。

武田社長は「どの設備を復旧させるかなどの手順を決めていたのが大きかった」と強調する。

仙台市若林区の建設業「皆成建設」も建物の一部に被害があったが、地震翌日の3月12日から社員約40人の半数を動員。復旧作業に向けた地域の被害調査に着手した。

昨年3月のBCP策定を受け、従業員の安否を確認するメールの自動発信システムを導入するなどしていた。南達哉社長は「建設業が被災すればインフラ復旧もままならない。初動体制の確保は社会的要請でもある」と語る。

各県によると、中小企業のBCP普及率は岩手が1割強、宮城は3割弱にとどまる。東北のある県の担当者は「被災現場はまだその段階にないが、今後の復興に合わせ、BCP策定支援を強化したい」と話す。

（斎藤秀之）

［事業継続計画］　企業が自然災害、大火災、テロなどの緊急事態に遭遇した際に、損害を抑えつつ早期復旧するための方法、手段を取り決める計画。優先する中核事業の特定、事業拠点の代替地の準備などが柱となる。

Ⅱ－２　Ｚ社は国内に10か所の拠点を持つ社員数5,000人の企業（サービス業）である。現在，自社で管理しているメールサービスを，クラウド型サービスに移行することを検討している。情報工学の技術士の立場から次の問いに答えよ。ただし，（１）については答案用紙１枚以内，（２）については答案用紙２枚以内とする。

（１）資料Ａは，クラウドコンピューティングの定義と特徴を記載したものである。この資料をよく読み，Ｚ社がメールサービスをクラウドサービスへ移行する際のメリットとデメリットを論ぜよ。

（２）資料Ｂはクラウドサービスで実際に発生した障害事例，資料Ｃは国内外のデータセンターを利用するうえでの制約に関する資料，資料Ｄはクラウドサービスレベルのチェックリストである。これらの資料から，Ｚ社がメールサービスをクラウド型サービスへ移行する際に想定されるリスクを３つ列挙し，それらを解決するための技術的方策について論ぜよ。

資料A：NISTによるクラウドの定義のIPAによる概要解説，
「クラウド・コンピューティング社会の基盤に関する研究会報告書」，
2000年３月24日，独立行政法人情報処理推進機構，による概要解説部分の抜粋。

(1) クラウドとは

「クラウド」が何を意味するかについて、合意された明確な定義はないが、広義的には、ネットワークを介して提供されるサービス全般を言及するために使われることがあるようである。

米国 NIST(National Institute of Standards and Technology：国立標準技術研究所)では、クラウドを次のように定義[1]するとともにクラウドの５つの特徴について記載している（表 1-1 参照)。

『クラウドコンピューティングとは、(ユーザにとって)最小限の管理労力、あるいはサービス提供者とのやりとりで、迅速に利用開始あるいは利用解除できる構成変更可能な計算機要素(例えば、ネットワーク、サーバ、ストレージ、アプリケーション、サービス)からなる共有資源に対して簡便かつ要求に即応できる(オンデマンド)ネットワークアクセスを可能にするモデルである。』

(バージョン 15　2009 年 10 月 7 日)

表 1-1　クラウドコンピューティングの５つの特徴　（「IPA ニューヨークだより 2009 年 9 月号」から

特徴	概要
オンデマンドかつセルフサービス	消費者（ユーザ）は、サービスプロバイダーの人的関与を必要とせず、自動的に、一方的にコンピューティング能力（サーバーやネットワーク・ストレージ）を利用できる。
幅広いネットワークアクセス	コンピューティング能力は、各種の消費者のプラットフォーム（携帯やラップトップ、PDA など）から、ネットワークを通じてサービスや資源にアクセスできる。
資源の共有	プロバイダーのコンピューティング資源は、Multiple-Tenant モデルにより、複数の消費者に提供され、その物理的・仮想的資源は消費者の需要に応じて動的に割り当てられる。その際、消費者は、一般的に、どこで計算がなされるか、管理できず、知見を有さないという点で、場所に独立的である。
迅速な拡大/縮小	コンピューティング能力は、急速かつ弾力的に、スケールイン・スケールアウトされて、提供される。消費者からみると、コンピューティング能力は、無限にあるように見え、必要な時に必要な量を購入することができる。
計測可能なサービス	クラウドシステムは、計量能力を利用することにより、サービスのレベルに応じて、資源利用の管理・最適化が自動的に行われる。資源の利用は、プロバイダー、ユーザの両方にとって、監視、制御され、透明性をもって報告される。

[1] http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

資料Ｂ－１：IPA「クラウド・コンピューティング社会の基盤に関する研究会報告書」，
2000年３月24日，独立行政法人情報処理推進機構，
クラウドサービスの実際の障害事例の表の抜粋。

（表 4-5）クラウドサービスの実際の障害事例

サービス名	提供ベンダ	サービス概要	発生時期：停止時間
Gmail (GoogleApps を含む)	Google	SaaS （メールサービス）	2008 年 06 月：12 時間 2008 年 08 月：15 時間 2009 年 09 月：6 時間
Force.com (Salesforce CRM 含む)	Salesforce	PaaS (SaaS 含む)	2005 年 12 月：5 時間 2008 年 02 月：7 時間 2010 年 01 月：1 時間
ES2/S3	Amazon	PaaS/IaaS	2008 年 02 月：3 時間 2008 年 04 月：数時間

※公開情報を元に作成

資料Ｂ－２：Scan Net Security記事，2009年10月８日，
https://www.netsecurity.ne.jp/2_14112.html より

2009年10月08日

SCAN DISPATCH：Amazon EC2へDDoS攻撃、クラウドの弱点が浮き彫り

SCAN DISPATCHは、アメリカのセキュリティ業界及ハッカーコミュニティから届いたニュースを、狭く絞り込み、深く掘り下げて掲載します。

クラウド・コンピューティングの普及と同時に、その脆弱性や弱点が指摘されているが、Amazon EC2(Amazon Elastic Compute Cloud)をホスティングに使っているbitbucket.orgが、17時間近くもダウンするという事件があった。事件自体はたいしたものではないが、クラウド・コンピューティングの弱点を浮き彫りにしている。

bitbucketはオープンソースのコード・ホスティング・サービスで、「データベース、ログファイルからユーザデータまでの全て」(bitbucket.orgのJesper Nohr氏)をAmazon Elastic Block Store (Amazon EBS)に保管している。

bitbucketが、サーバの負荷が異常に高いことに気がついたのは、10月3日の夕方。EBS volumeのiostatが高く、tps(transaction per second)が低いことが分かり、bitbucketはvolumeのリマウントを行い、xfs_checkを行い、instanceとvolumeを、us-east-1bからus-east-1aとus-east-1cに移したが、異常は解決しなかった。

bitbucketはすぐにこの異常をAmazonのサポートシステムに報告するが、なんと最初の7時間は、「異常は存在しない」「EBSは分散型ネットワーク・リソースだから、パフォーマンスは変化する」「RAID 0を使って複数のEBSにディストリビュートすると良い」といったアドバイスしかもらえなかった。Nohr氏はそのブログで、「非常に不満だった。なぜなら、(1)自分でできることが何もなかった、(2)「万事OKだ、問題ない」という答えしかもらなかった」と書いている。bitbucket側とEBS間のコネクションに必要なリソースでさえきちんと作動していないため、bitbucket側としては、対岸の自分の家の火事を見ているようなものだからだ。

bitbucketがダウンした、と、顧客の多くがTwitterでぼやく一方、Amazonと高額のサポート契約を結んでいるbitbucketの顧客らが直接Amazonlにメールを出したこともあってか、Amazon側では事態の重要性にやっと気がついたようだ。8時間後にbitbucketlは、Amazonから問題が生じていることを認識する旨の連絡を受け取り、11時間後、Amazonでは事態を非常に重く受け止め、専門家のチームを投入して解決に努めると、Amazonの重役級の人から連絡を受けてたという。

そして15時間後、問題はEC2とEBS間のネットワークに存在するということがわかり、Amazon側では問題を解決し、bitbucketlは17時間後に再びアプリケーションを作動させることができた。

bitbucketがダウンしたEC2とEBS間のネットワークの問題とは、スプーフィングされたDDoSでだったということが分かっているが、この攻撃が浮き彫りにしたクラウドの弱点はいろいろある。

まず、Amazon側が、アップストリームでUDPトラフィックをブロックするという解決方法を実施するのに17時間もかかっていること。自分(bitbucket)のリソースを管理する(Amazonの)エンジニアと即座に直接連絡がとれれば、この遅延はなかっただろう。インターネットからのトラフィックが、内部リソースであるはずのストレージをダウンさせることができることは、Amazonのインフラの構造に問題があるとしか言えない。

顧客としてはAmazon EC2の構造は単なるBlackBoxでしかなく、Nohr氏も「AmazonのCloudWatchサービスを買うことによって初めて、ネットワークの問題であるということが分かった」と書いているように、サービスをアップグレードしなければ問題の診断を行えないのも、問題点の一つと言えよう。

この事件に対する意見の多くは「クラウドだからといってダウンしないと考えてはいけない」というのが結論のようだ。

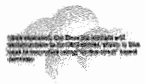
さて、10月4日に入ってからbitbucketlは、今度はTCP SYNFLOOD攻撃を受けてまたダウン。Amazonlは即座にこれに対応して全ては順調のようにみえたが、Register誌によると、1時間半にわたって、今度はAmazonのエッジ・ルーターが攻撃を受けて、bitbucketの顧客の多くが、サービスが使えなかった。

bitbucketlは、この事件の最中に他のクラウド・サービスからの営業攻勢をいくつも受けたらしい。それを受けてブログのコメントに「もしかしたら営業をかけてきた競合他社がDDoSを行った？」とあったが、さて、真相はいかに。

【執筆:米国　笠原利香】

資料Ｂ－３：ITmediaニュース，2009年12月10日
http://www.itmedia.co.jp/news/articles/0912/10/news021.html より

Amazon EC2からマルウェアを遠隔操作、クラウド利用に着目か



Amazonのクラウドサービスを使って感染PCをコントロールしているマルウェアの亜種が見つかった。

2009年12月10日 07時58分 更新

米Amazonのクラウドサービス「Amazon EC2」を使って感染PCをコントロールしているマルウェアの亜種が見つかったと、セキュリティ企業の米CAが12月9日のブログで伝えた。

このマルウェアは各国で感染を広げている「Zeus」のボット型亜種。クリスマスカードの配達通知を装ったメールで、クリスマスカードへと称する不正リンクをクリックさせようとする手口だという。

リンクをクリックすると、Zeusボット感染コードを仕掛けたWebサイトにユーザーを誘導する。感染したマシンをボット管理用のコマンド＆コントロール（C&C）サーバにアクセスさせ、ユーザーの個人情報や銀行の口座情報などを盗み出す仕掛けになっていた。

Zeusボットのコードを調べたところ、このC&CサーバとしてAmazon EC2のサービスが使われていることが分かったという。

Action	URL	Details
GET	http://ec2-[redacted]-170.compute-1.amazonaws.com/zeus/config.bin	svchost.exe (sr
POST	http://ec2-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe (sr
POST	http://ec2-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe (sr
POST	http://ec2-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe (sr
POST	http://ec2-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe (sr

記録にはAmazon AWSのドメインがある（caより）

CAでは、クラウドサービスが犯罪目的でも使われている実態が改めて浮き彫りになったと指摘。Amazonと、Zeusの不正コードが仕掛けられたWebサイトにはこの問題を伝えたとしている。

資料Ｂ－４：IT Pro，2009年３月19日
http://itpro.nikkeibp.co.jp/article/NEWS/20090319/326911/ より

Microsoftのクラウド基盤「Windows Azure」プレビュー版で障害が発生

2009/03/19
《ITpro》

米Microsoftは米国時間2009年3月18日，同社のクラウド・コンピューティング基盤「Windows Azure」のプレビュー版で同3月13日に障害が発生し，多数のサービスに影響が生じたことを明らかにした。

オペレーティング・システムの定期更新時にネットワーク関連の問題が生じたことが原因で，Windows Azureのデプロイメント・サービスのパフォーマンスが低下し，多数のサーバーでタイムアウトや障害が発生したという。この結果，単一インスタンスのみで動作するアプリケーションがサーバーとともにダウンしたほか，複数インスタンスの一部アプリケーションにも影響が出た。

また，問題が生じたアプリケーションを別のサーバーに自動移行する復旧処理の影響で，Webポータルからの管理機能も多くのアプリケーションで使えなくなった。ストレージには障害の影響はなかった。

現在はすべてのアプリケーションが正常に復旧している。米メディア（InfoWorld）の報道によると，今回の障害は，米太平洋標準時で13日午後10時30分から翌14日午後8時30分まで続いた。

同社は，障害の引き金となったネットワーク問題への対処を進めているほか，障害復旧のアルゴリズムを見直し，迅速かつ的確な対応を実現する予定だとしている。開発者に対しては，アプリケーションのデプロイメントを複数インスタンスで行うよう勧めている。今後，プロジェクトやサンプルでは2インスタンスをデフォルトにし，2つ目のインスタンスは割当数の制限から除外するという。

Windows Azureは，同社が2008年10月に発表したクラウド・コンピューティング基盤（関連記事：[PDC 2008]米マイクロソフトがクラウドOS「Windows Azure」を発表，[PDC 2008]Windows Azureとは？）。現在は，プレビュー版の「Community Technology Preview（CTP）」としてサービスを提供している。

資料Ｂ－５：「Ｇmailの障害に対するGoogle社報告」2011年２月27日，
（株）電算システムの和訳
http://web-dsknetgoogleapps.blogspot.com/2011/03/gmail2011227.html より

Google Apps Incident Report

Gmail Outage - February 27, 2011
Prepared for Google Apps for Business customers

以下は、2011 年 2 月 27 日から発生した、非常にわずかな Google Apps お客様に発生した Gmail 問題の、インシデントレポートです。その影響を受けたユーザーは、 Gmail と他の Google Apps サービスにおいて、メールボックスが空になっているか、ログイン出来ないことを報告しました。問題を解決するために、Google のエンジニアは影響を受けるユーザのためにアカウント・データとユーザーアクセスを回復しました。

この問題の間、いくつかの受信メールが自動的にバウンスされました(送付者は配信障害通知を受け取りました)。ユーザーのメールボックスからのメールのロストはありません。私たちは、このサービスの停止は、大切なお客様とそのユーザーに影響を与えたことを理解しています。また、心からお詫び申し上げます。

問題の分析と対応

注意：全ての日時は太平洋標準時で記載されています。

2 月 27 日午前 10 時頃 Google Support は最初の報告を受けました。

1) メールボックスが空になり、テーマやラベルなどの個人設定が初期状態に戻っていた。
または
2) Gmail アカウントが一時的に利用できないという、500 系のエラー状態が表示される。

問題を分析した後に、Google エンジニアは、根本的原因が Gmail ストレージソフトウェアアップデートで想定されなかったバグであることを確認しました。バグによって、影響を受けるユーザーのメッセージとアカウント設定はデータセンターから一時的に利用できなくなりました。Google エンジニアは 2 月 27 日午後 1 時 5 分に、ストレージソフトウェアアップデートを中止し、更なる展開を停止しました。

復旧プロセス

問題とその根本的原因を分析している間、Google エンジニアは、ユーザーのアカウントを回復するためのプロセスも実施していました。2 月 27 日午後 6 時に、Google エンジニアは 影響の有ったユーザーの Gmail と他の Google Apps サービスへのアクセスを一時的に無効にしました。これは、メールボックス回復プロセスの間にデータ保全の問題を防ぐ予防策でした。ユーザーが Gmail や Google Apps サービスにログインすると、「すみません、あなたのアカウントは無効にされています」と表示されました。2 月 28 日午後 1 時 30 分に、さらに分析を続け、Google エンジニアはソフトウェアのバグで影響を受けないユーザーを特定し、そのアカウントへのアクセスを回復しました。影響を受けるユーザーのために、Google エンジニアは Gmail 以外の すべての Google Apps サービスへのアクセスを回復しました。

Gmail は複数のユーザーのメッセージのコピーを、複数のデータセンターとテープバックアップで

保存します。このソフトウェア問題で、いくつかのメッセージが、オンラインで利用できなくなり、オフラインテープバックアップからの復元を必要としました。Google エンジニアはテープバックアップからユーザのデータを検索し、データをメールボックスの中に移動、データの復元を検証、全ての受信メッセージキューを配信、そして、ログインアクセスを再有効化しました。テープバックアップからユーザーのデータを取得して復元するため、長時間が必要になりました。さらに、回復時間はユーザーのメールボックスのサイズに依存しました（ユーザーのメールボックスのサイズが大きいほど、復旧時間はより長くかかりました）この間、Google Apps Directory Sync や Google Apps Provisioning API(Google Apps 管理者によって利用されたユーティリティ)によるプログラムに基づくユーザアカウントの更新は、復旧のための追加時間を必要としました。

この出来事の間、既存のメッセージも Gmail 設定もユーザーのアカウントから失われませんでした。しかしながら、2 月 27 日午後 6 時から 2 月 28 日午後 2 時の間で、新たにメールを受信できず、送信者は「配送状態通知(失敗)」のバウンス通知を受け取りました。この期間の後は、通常通りメッセージは配信され、かつてのユーザーログインが有効となりました。

Google エンジニアは、データの整合性を確保しつつ、可能な限りより早く影響のあるユーザーアカウントへのアクセス回復するために、熱心に対応しました。3 月 2 日午後 3 時 40 分までには、Gmail データとログインアクセスは Google Apps for Business ユーザーの 98%に回復されました。Google エンジニアと Google Support は、残りのユーザーに対して対応し、そして、3 月 3 日午前 11 時 30 分までには、Google Apps for Business の全てのユーザーの復旧が終了しました。

問題の伝達

この出来事の間、Google Support は定期的なアップデートを Apps Status Dashboard に掲示しました。2 月 28 日、Google エンジニアは、Gmail blog post で問題の原因の説明をリリースし、アカウントの回復プロセスの情報と、ユーザーのための、いくつかの残りの問題を報告するための電子メールアドレスを記載しました。

調整と再発防止策

Google エンジニア および Support は、内部レビューと分析を行い、問題の根本的な原因に対処するため、再発を防止するために以下のアクションを開始しています。

- テストツールの機能を拡張し、ソフトウェア開発サイクルの間、このクラスのバグをより特定しやすくする
- アラートとモニターを実装し、より早くこのタイプの問題を検出し、伝播を停止するようにする
- 影響を受けるユーザーとユーザーアカウントの無効化と再有効化のために、自動化ツールのパフォーマンスを向上させて利用することにより、メール回復プロセスを早くする
- Gmail サービスの中断中、 ユーザーが Google Apps サービスへアクセスできるツールを開発する
- サポートコミュニケーションを改良する: お客様が大規模なサービスの中断やサポート停止に関するケースを Google Enterprise Support に提出すると、自動的にメールかオンラインで状態/解決のアップデートを受けることができるようにする

私たちはこれらの改良に専念し、そのすべてが現在、進行しています。私たちはこの問題がお客様に影響を与え、失望させたことを理解しています。Google は、サービスの中断を防ぐために、継続的かつ迅速に技術と業務プロセスの改善に取り組んでいます。

資料C：経済産業省，「クラウドコンピューティングと日本の競争力に関する研究会」報告書，2010年8月16日（一部抜粋）

3.1.4. 国内外のデータセンタを利用する上での制約

クラウドコンピューティングは、サーバが設置されているデータセンタの物理的な場所に制約を受けることなくサービスを享受することが可能である。そのため、海外に設置されたサーバにデータが保存されることも当然のことながら考えられる。しかしながら、国内外のデータセンタの利用に関しては、その取扱いが現地の法令の対象になるなど、その利用に留意が必要な点がいくつかある。そこで、国境をまたぐデータの取扱いに関わる米国とEU、日本の法令の概要と制約などについてまとめる。

① 米国愛国者法（USA Patriot Act）

(ア)米国愛国者法の概要

2001年9月11日に発生した同時多発テロ事件を受け、2001年10月に成立した「Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001（以下、米国愛国者法（USA PATRIOT Act））」では、捜査機関の権限の拡大や国際マネーロンダリングの防止、国境警備、出入国管理、テロ被害者への救済などについて規定を行っている。

特に、第201条や第202条では、テロリズムやコンピュータ詐欺及びコンピュータ濫用罪に関連する有線通信や電子的通信を傍受する権限が明記されている。また、第209条では、捜査官は裁判所命令ではなく捜査令状により、電子メールやボイスメールを入手できると規定され、第213条では、捜査官は令状の通知なく家宅などを捜索できるとする規定されている。さらに、第505条では、FBIが金融機関や通信サービスプロバイダに対して顧客の個人情報の提出を求める場合に、その情報が「国際テロや秘密諜報活動の防止を目的とした正式な捜査に関連」することを明示することで足りるとしている。これは、捜査機関は、金融機関やプロバイダの同意を得さえすれば、裁判所の関与を求めることなく捜査ができるということである。

このように、米国では日本の手続きと比較して、裁判所の許可が不要など政府機関に与えられている権限が大きいため、クラウドコンピューティングなどを活用して、米国サーバへデータを保存する場合には留意が必要である。

例えば、データセンタのサービス形態によっては、仮想的に分離された環境であっても、物理的に同一のサーバ機器などを共有している場合もあり、他社に関する捜査であっても、システム停止などの影響を受けるリスクがあることを認識する必要がある。ただし、捜査手続きなどの違いを除けば、このリスクは、米国以外の国でも発生しうる。また、この問題は、クラウドコンピューティング固有の問題ではなく、どのようなシステムにおいても、データの処理・保存という観点で考慮する必要がある。

(イ)米国愛国者法の関連動向

2009年4月2日早朝、米連邦捜査局（FBI）が、米国テキサス州にある米コアIPネットワークス社のデータセンタを捜索し、捜査官が2フロア分のサーバなどのIT設備を押収したという事例がある。 その影響として、同一データセンタを利用していた約50社に上る顧客が電子メールや自社のデータにアクセスできなくなるなどの問題が発生した。

カナダでは、アウトソーシング契約を結ぶ際に参照すべきガイドライン「Taking Privacy into Account Before Making Contracting Decisions」を策定した。アウトソーシング業務の委託先が米国企業の場合、もしくはカナダの企業であっても米国に関連企業が存在する場合には、個人情報を含むデータが国境を越え、米国に置かれる可能性がでてくる。この場合、愛国者法の適用対象となることから、本人の承諾なく個人情報が米国当局に閲覧されるリスクを懸念しての措置である。このガイドラインはカナダ連邦政府予算庁が作成したもので、プライバシー法に基づき、個人情報を取り扱う業務をアウトソースする場合は、国民のプライバシーを適切に保護するため、ガイドラインで示されているアドバイスに従うよう、強く推奨している。

② EUデータ保護指令(Data Protection Directive)

EUおよび英国ではデータ保護指令（Data Protection Directive）により、EU内の住民の個人情報に関して十分なデータ保護レベルを確保していない第三国へのデータの移動を禁じている。EUのデータ保護指令が要求する十分な保護水準を確保していると認められている国・地域は、スイス、カナダ、アルゼンチン、ガンジー島、マン島、ジャージー島の６つである。

このうち、カナダは、連邦政府部門対象の法律、民間部門対象の法律、州政府対象の州法など、複数の法律を組み合わせることにより、ほぼすべての機関を対象とした法的枠組みを形成し、十分性を認められている。

米国の場合は、包括法がないため、特定の認証基準を設け、その認証を受けた企業ごとに十分性を付与するセーフハーバー協定を2000年にEUと締結している。また、米国―EU間の航空旅客情報についても認められている。なお、Google、Amazon、salesforce.com、Microsoftなど多くのサービスプロバイダはセーフハーバー協定を遵守していることから、EU内の住民の個人情報を米国で保管することが可能となっている。セーフハーバーを遵守している組織リストについては、米国商務省のウェブサイトの「Safe Harbor List[14]」を参照。一方で、2010年にドイツから、米国に個人情報を提供するに当たり、セーフハーバー協定のみでは不十分であるとの表明がなされている。このため、国によっては、より厳しい制約を要求される可能性があることに留意する必要がある。

③ 外国為替及び外国貿易法

「外国為替及び外国貿易法（以下、外為法）[15]」では、国際的な平和及び安全の維持を妨げることがないように、特定の技術を特定の外国において提供する際や特定の外国人・外国企業に提供する際には、経済産業大臣の許可が必要と定めており、第25条第３項では「特定国において受信されることを目的として行う電気通信による特定技術を内容とする情報の送信」も許可の対象として規定している。したがって、日本国内から海外の外部サーバに情報を送信する際や、当初から外国の利用者に情報を提供することを目的に自社の海外サーバに情報を送信する際、国内サーバのリソースを演算処理等のために提供してその結果を送信する際等も、許可の対象となる場合がある。

この特定技術とは、核兵器等の大量破壊兵器や通常兵器に関連した技術を指しており、例えばこの技術の中には暗号技術などの汎用的な技術も多く含まれるため、これらの情報を取り扱う際には留意が必要である。

一方、米国の「米国輸出管理規則」のように自国で開発されたソフトウェアの輸出に規制を設けている国もあるため、日本国内のクラウド事業者が他国のソフトウェアをクラウドサービスの中で提供する場合には、各国の輸出規制に準拠しているかどうかに留意する必要がある。

資料D：経済産業省，「クラウドコンピューティングと日本の競争力に関する研究会」報告書，
2010年8月16日よりクラウドサービスレベルのチェックリスト（一部抜粋）

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考
アプリケーション運用						
1	可用性	サービス時間	サービスを提供する時間帯（設備やネットワーク等の点検／保守のための計画停止時間の記述を含む）	時間帯	24時間365日 （計画停止／定期保守を除く）	計画停止時間は提供者が個々に設定
2		計画停止予定通知	定期的な保守停止に関する事前連絡確認（事前通知のタイミング／方法の記述を含む）	有無	30日前にメール／ホームページで通知	
3		サービス提供終了時の事前通知	サービス提供を終了する場合の事前連絡確認（事前通知のタイミング／方法の記述を含む）	有無	15ヶ月前にメール／ホームページで通知	
4		突然のサービス提供停止に対する対処	プログラムや、システム環境の各種設定データの預託等の措置の有無	有無	第三者へのプログラムの預託を実施	サービス提供企業が倒産等した場合にもサービスを継続できるように、プログラムを第三者に預託していることが望ましい
5		サービス稼働率	サービスを利用できる確率（（計画サービス時間－停止時間）÷計画サービス時間）	稼働率（%）	99.9%以上（基幹業務） 99%以上（基幹業務以外）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討 ※「計画サービス時間」は、サービス提供時間と計画停止時間の両方を含む。
6		ディザスタリカバリ	災害発生時のシステム復旧／サポート体制	有無	遠隔地のバックアップ用データセンタで保管している日次バックアップデータと予備システム切替時間は半日～1日	データセンタ構成、復旧までのプロセス／時間、費用負担についても明示されていることが望ましい また、適用する業務の重要性に応じた「ディザスタリカバリ」のレベルにより設定内容は変わる
7		重大障害時の代替手段	早期復旧が不可能な場合の代替措置	有無	バックアップデータの取得が可能なホームページを用意	
8		代替措置で提供するデータ形式	代替措置で提供されるデータ形式の定義を記述	有無（ファイル形式）	CSVあるいはExcelファイル	データ保護の観点からは、クラウド・コンピューティング・サービス提供者だけでなく利用者側でもバックアップを実施しておくことが望ましい また、システムの信頼性、サービス継続性の観点からは、サービス提供者は十分に対策を行っていると考えられるが、トラブル時に備えて、預託データのダウンロードが可能かどうかを確認することが望ましい
9		アップグレード方針	バージョンアップ／変更管理／パッチ管理の方針	有無	年2回の定期バージョンアップを実施	頻度、事前通知方法、履歴管理／公開、利用者の負担についても明示されていることが望ましい
10	信頼性	平均復旧時間(MTTR)	障害発生から修理完了までの平均時間（修理時間の和÷故障回数）	時間	1時間以内（基幹業務） 12時間以内（上記以外）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討
11		目標復旧時間(RTO)	障害発生後のサービス提供の再開に関して設定された目標時間	時間	3時間後 3日後	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討
12		障害発生件数	1年間に発生した障害件数／ 1年間に発生した対応に長時間（1日以上）要した障害件数	回	1回以内（基幹業務） 3回以内（上記以外）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討
13		システム監視基準	システム監視基準（監視内容／監視・通知基準）の設定に基づく監視	有無	ハードウェア／ネットワーク／パフォーマンス監視	詳細な監視項目は提供者が個々に設定
14		障害通知プロセス	障害発生時の連絡プロセス（通知先／方法／経路）	有無	指定された緊急連絡先にメール／電話で連絡し、併せてホームページで通知	初期対応後の経過報告の方法・タイミングについても明示されていることが望ましい
15		障害通知時間	異常検出後に指定された連絡先に通知するまでの時間	時間	15分以内（基幹業務） 2時間以内（上記以外）	営業時間内／外で異なる設定を行う場合がある
16		障害監視間隔	障害インシデントを収集／集計する時間間隔	時間（分）	1分以内（基幹業務） 15分（上記以外）	営業時間内／外で異なる設定を行う場合がある
17		サービス提供状況の報告方法／間隔	サービス提供状況を報告する方法／時間間隔	時間	月に一度ホームページ上で公開	報告内容／タイミング／方法は提供者が個々に設定
18		ログの取得	利用者に提供可能なログの種類（アクセスログ、操作ログ、エラーログ等）	有無	セキュリティ（不正アクセス）ログ／バックアップ取得結果ログを利用者の要望に応じて提供	提供内容／方法は提供者が個々に設定
19	性能	応答時間	処理の応答時間	時間（秒）	データセンタ内の平均応答時間3秒以内	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討
20		遅延	処理の応答時間の遅延継続時間	時間（分）	データセンタ内の応答時間が3秒以上となる遅延の継続時間が1時間以内	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討
21		バッチ処理時間	バッチ処理（一括処理）の応答時間	時間（分）	4時間以下	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討
22	拡張性	カスタマイズ性	カスタマイズ（変更）が可能な事項／範囲／仕様等の条件とカスタマイズに必要な情報	有無	利用画面上の項目配置変更や新規項目の追加が設定画面より可能	
23		外部接続性	既存システムや他のクラウド・コンピューティング・サービス等の外部のシステムとの接続仕様（API、開発言語等）	有無	API（プログラム機能を外部から利用するための手続き）を公開	APIがインターネットの標準技術で構成され、仕様が公開されており、APIの利用期限や将来の変更可能性が明記されていることが望ましい
24		同時接続利用者数	オンラインの利用者が同時に接続してサービスを利用可能なユーザ数	有無（制約条件）	50ユーザ（保証型）	同時接続の条件（保証型かベストエフォート（最善努力）型か）、最大接続時の性能について明示されていることが望ましい
25		提供リソースの上限	ディスク容量の上限／ページビューの上限	処理能力	1TB 40,000ページビュー	

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考
サポート						
26	サポート	サービス提供時間帯（障害対応）	障害対応時の問合せ受付業務を実施する時間帯	時間帯	24時間365日（電話）	受付方法（電話／メール）や営業時間外の対応は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なる
27		サービス提供時間帯（一般問合せ）	一般問合せ時の問合せ受付業務を実施する時間帯	時間帯	営業時間内（電話） （年末年始・土日・祝祭日を除 24時間365日（メール）	受付方法（電話／メール）や営業時間外の対応は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なる
データ管理						
28	データ管理	バックアップの方法	バックアップ内容（回数、復旧方法など）、データ保管場所／形式、利用者のデータへのアクセス権など、利用者に所有権のあるデータの取扱方法	有無／内容	有 （日次で、作業前後の差分のみバックアップし、週次でフルバックアップを取る。遠隔地のデータセンタにテープ形式保管。アクセス権はシステム管理者のみに制限。復旧／利用者への公開の方法は別途規定）	保証要件を設定している場合は、具体的に明示。バックアップ内容は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なる また、クラウド・コンピューティング・サービスベンダの民事再生、破産等によりサービス継続が出来ない場合についても明示されていることが望ましい
29		バックアップデータを取得するタイミング(RPO)	バックアップデータをとり、データを保証する時点	時間	前日朝6時まで ただし、災害発生時は1週間前まで	データ破損、システム障害時において、どの時点のデータを最低限保証すべきか示すこと
30		バックアップデータの保存期間	データをバックアップした媒体を保管する期限	時間	5年以上（証跡として残すべきもの、法定のもの） 3ヶ月以上（その他）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討する 証跡として残すべきだと思われるものとしては、アクセスログ等のセキュリティに関係するログ情報が挙げられる。法定のものとしては、帳票関係が挙げられる
31		データ消去の要件	サービス解約後の、データ消去の実施有無／タイミング、保管媒体の破棄の実施有無／タイミング、およびデータ移行など、利用者に所有権のあるデータの消去方法	有無	サービス解約後1ヶ月以内にデータおよび保管媒体を破棄	解約時には、CSVなどの一般的なフォーマットでデータ出力ができることが望ましい
32		バックアップ世代数	保証する世代数	世代数	3世代	ロールバックを必要と迫られた際にどの時点のバックアップデータまで遡ることが可能であるかを明確にしておくことが望ましい
33		データ保護のための暗号化要件	データを保護するにあたり、暗号化要件の有無	有無	有	個人情報や、業務において重要かつ暗号化せねば信頼性に欠けるデータを対象とする
34		マルチテナントストレージにおけるキー管理要件	マルチテナントストレージのキー管理要件の有無、内容	有無／内容	有 複数のキーを使用することで、不正アクセス等の影響範囲を限定する	マルチテナントストレージの場合のキー管理の方法について、全顧客がひとつのキーを使うのか/顧客別にひとつのキーが割り当てられるのか/顧客別に複数のキーを使えるのか明確にしておくことが望ましい
35		データ漏えい・破損時の補償／保険	データ漏えい・破損時の補償／保険の有無	有無	有	個人情報を扱う場合には、クラウド・コンピューティング・サービス提供者との間で個人情報取り扱いに関して合意を形成して契約事項の中で責任の割り当てを行っておくべきであるが、万が一の個人情報漏えいに備える意味でサービス提供者における損害賠償保険加入の有無を確認しておくことが望ましい
36		解約時のデータポータビリティ	解約時、元データが完全な形で迅速に返却される、もしくは責任を持ってデータを消去する体制を整えており、外部への漏えいの懸念のない状態が構築できていること	有無／内容	有 返却する場合は、テープ媒体にデータを保管し、提供する 消去する場合は、証明書を送付する（第三者機関発行の証明書が望ましい）	外部への漏えいをいかに防ぐ仕組みが出来ているか
37		預託データの整合性検証作業	データの整合性を検証する手法が実装され、検証報告の確認作業が行われていること	有無	有	入力データ、算出データ等がハードウェア/プラットフォーム/アプリケーションの問題や不正な操作により改ざんされていないことを検証する手法が実装され、検証報告の確認作業が行われていること
38		入力データ形式の制限機能	入力データ形式の制限機能の有無	有無	有	金額、住所、電話番号等の文字種、データ形式が制限されるフォームにおいて、想定外のデータ入力を検出し、不正なデータをデータベースに格納しないようにする仕組みを提供していること

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考
セキュリティ						
39	セキュリティ	公的認証取得の要件	JIPDECやJQA等で認定している情報処理管理に関する公的認証（ISMS、プライバシーマーク等）が取得されていること	有無	ISMS認証取得 プライバシーマーク取得	ITサービスマネジメントのベストプラクティスであるITILやJIS Q20000、JIS Q 27001:2006をベースとした情報セキュリティ監査の実施等の取得状況も確認することが望ましい
40		アプリケーションに関する第三者評価	不正な侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ていること	有無／実施状況	有 （サービス提供前に、セキュリティホールの有無等について第三者機関（又は内部機関）により検査を受け、また、検査が定期的かつ適切に行われていることを年１回、外部機関により評価を受ける。また、速やかに指摘事項に対して対策を講じる。）	セキュリティ監査、システム監査、ペネトレーションテスト等ネットワークからの攻撃に対する検証試験、ハードウェア/プラットフォーム/ウェブアプリケーションの脆弱性検査、データベースセキュリティ監査などを想定
41		情報取扱い環境	提供者側でのデータ取扱環境が適切に確保されていること	有無	有 （運用者が限定されていること）	
42		通信の暗号化レベル	システムとやりとりされる通信の暗号化強度	有無	3DES/RSA/SHA-1	SSLの場合は、SSL3.0/TLS1.0（暗号強度128ビット）以上に限定
43		会計監査報告書における情報セキュリティ関連事項の確認	会計監査報告書における情報セキュリティ関連事項の監査時に、担当者へ以下の資料を提供する旨 「最新のSAS70Type2監査報告書」 「最新の18号監査報告書」	有無	有	
44		マルチテナント下でのセキュリティ対策	異なる利用企業間の情報隔離、障害等の影響の局所化	有無	データ認証のアクセスコントロールについて明記	
45		情報取扱者の制限	利用者のデータにアクセスできる利用者が限定されていること 利用者組織にて規定しているアクセス制限と同様な制約が実現できていること	有無／設定状況	有 （利用者のデータにアクセスできる社員等はセキュリティ管理者の許可を得た者に限る）	利用者組織にて規定しているアクセス制限と同等な制約が実現できるかどうかを確認すること。クラウド・コンピューティング・サービスにおけるハードウェア/プラットフォーム/アプリケーションで用意されているロール（管理者、一般ユーザ等の役割を意味する）に制約がある場合には、ユーザを既存のロールの範囲でグルーピングする等の工夫により対応できるかどうかを確認する。クラウド・コンピューティング・サービスではマルチテナントを採用しているため、他の顧客と一つのデータベースを共有する場合があることに配慮すること
46		セキュリティインシデント発生時のトレーサビリティ	IDの付与単位、IDをログ検索に利用できるか、ログの保存期間は適切な期間が確保されており、利用者の必要に応じて、受容可能に期間内に提供されるか	設定状況	権限に沿ったID管理が行われていること（1人1ID発行）	
47		ウイルススキャン	ウイルススキャンの頻度	頻度	週次	
48		二次記憶媒体の安全性対策	バックアップメディア等では、常に暗号化した状態で保管していること、 廃棄の際にはデータの完全な抹消を実施し、また検証していること、USBポートを無効化しデータの吸い出しの制限等の対策を講じていること	有無	・権限者のみアクセス可 ・廃棄時には、データを完全に抹消する ・暗号化、認証機能を用いる ・遠地へ運ぶ際は、施錠されたトランクで運ぶこと	
49		データの外部保存方針	データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する制約条件を把握しているか	把握状況	データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する制約条件を把握している	

平成23年度技術士第二次試験問題〔情報工学部門〕

選択科目【16－1】コンピュータ工学　　1時30分～5時

Ⅰ　次の２問題（Ⅰ－１，Ⅰ－２）について解答せよ。

Ⅰ－１　次の４つの設問のうち３設問を選んで解答せよ。（設問ごとに答案用紙を替えて**解答設問番号**を明記し，それぞれ１枚以内にまとめよ。）

Ⅰ－１－１　仮想化機構により１台の物理的コンピュータで複数の論理的なコンピュータを稼働させる方法が実用化されている。次の問いに答えよ。

（１）仮想化機構の原理を簡潔に説明せよ。

（２）仮想化による情報システムのサーバが実現されているが，その目的，利点，及び技術的に注意すべき点などを説明せよ。

Ⅰ－１－２　画像に関する次の問いに答えよ。

（１）BMP（Microsoft Windows Bitmap Image）ファイル内の主要となる情報を４種類挙げ，説明せよ。

（２）GIF（Graphic Interchange Format），JPEG（Joint Photographic Experts Group），PNG（Portable Network Graphics）の中から２つを選択し，各々の特徴を説明せよ。

Ⅰ－１－３　半導体式加速度センサーに関する次の問いに答えよ。

（１）MEMS（Micro Electro Mechanical Systems）について説明せよ。

（２）MEMSを応用したセンサーから２方式を選択し，各々の原理，特徴，精度を説明せよ。

（３）MEMSを応用したセンサーの適用例を述べよ。

Ⅰ－１－４　人工知能分野の機械学習技術を応用した迷惑メールの自動振り分けシステムについて，次の問いに答えよ。

（１）単純ベイズ分類器を用いた迷惑メールの自動振り分けシステムについて，その概要を説明せよ。

（２）上記のシステムと，送信アドレスのブラックリストによる振り分け方式とを比べて利点と欠点を述べよ。

Ⅰ－２　次の２設問のうち１設問を選んで解答せよ。（答案用紙を替えて**解答設問番号**を明記し，３枚以内にまとめよ。）

Ⅰ－２－１　あなたが民生用のPC（Personal Computer）のマザーボードと同等のマザーボードを用いて産業用の製品を開発する場合を想定し，次の問いに答えよ。ただし，（１）は答案用紙１枚以内とし，（２）と（３）の解答は合わせて答案用紙２枚以内とする。

（１）民生用PCに採用されているPC/AT互換機などのマザーボードの構成要素を５つ以上挙げ，それらをブロック図として示せ。また，各々のブロックの機能を説明せよ。

（２）想定した産業用製品の概要及び目標とする項目を具体的に説明せよ。

（３）上記の産業用製品にPC/AT互換機などのマザーボードを使用する際，民生用マザーボードにおける課題を示し，その課題解決策をハードウェア，ソフトウェアの視点から述べよ。なお，解決策として筐体に関する解答を含ませてもよい。

Ⅰ－２－２　ひとり暮らしの老人の見守りサービスの一環として，浴室での事故に対応するシステムを作りたい。前提条件として，浴室内に設置したセンサーのデータから，転倒や長時間動きがないなどの異常を中継器が自動的に検出して，警備センターにおいて警告を発し，警備員が音声回線での呼びかけや現場に向かうなどの対応措置を取るものとする。また，浴室の壁には配線等の穴を開けないこととし，浴室内外の通信（数メートル以内）は無線で行う。以下の問いについて，（１）と（２）の解答を合わせて答案用紙１枚以内とし，（３）は答案用紙２枚以内とする。

（１）上記の前提条件を考慮した上で，どのようなセンサーが適しているか挙げ，その機能を説明せよ。ただし，防水・結露対策については考慮しなくてよいものとする。

（２）浴室内外の無線通信方式について，適しているものを３種類挙げ，その特徴を説明せよ。

（３）上記の異常を自動検出するシステムについて，その構成図を描き，動作を説明せよ。ただし，警備センターからの音声回線については考慮しなくてよいものとする。

選択科目【16－2】ソフトウェア工学　　1時30分～5時

Ⅰ　次の２問題（Ⅰ－１，Ⅰ－２）について解答せよ。

Ⅰ－１　次の４設問のうち３設問を選んで解答せよ。（設問ごとに答案用紙を替えて**解答設問番号**を明記し，それぞれ１枚以内にまとめよ。）

Ⅰ－１－１　システム開発プロジェクトにおいて，プロジェクトの目標に影響を与えるリスク（脅威）が想定されるならば，リスクの抽出，要因や影響範囲の明確化，対策の考案，プロジェクト計画などへの織り込みが必要である。リスクへの対策は，回避，転嫁，軽減，受容の４つに分類できる。以下の（１），（２）の問いに答えよ。

（１）回避，転嫁，軽減，受容の定義を述べよ。

（２）リスク管理が必要な具体的なシステム開発プロジェクトの例と，想定すべきリスクを記述せよ。また，情報工学の技術士の立場から，４つの対策の具体例をそれぞれ述べよ。

Ⅰ－１－２　ソフトウェア製品の開発では，あらかじめ品質の保証された成果物を再利用することは，対象とする製品の品質の安定化，生産性の向上，開発リードタイムの短縮に有効であるといわれている。以下の（１），（２）の問いに答えよ。

（１）再利用には，ホワイトボックス再利用とブラックボックス再利用がある。これら２つの再利用の方式の定義，及びそれぞれの利点と欠点を述べよ。

（２）再利用の対象として代表的なものに，ソースコード，コンポーネント，フレームワーク，プロダクトラインなどがある。この中から，再利用の対象を２つ選び，選択した対象を明記したうえで，両者を，投資コスト，粒度，再利用の容易性という観点から比較することで，それぞれの特徴を述べよ。

Ｉ－１－３　オブジェクト指向技術について，（１），（２）の問いに答えよ。

（１）以下の技術を説明せよ。

① 継承（inheritance）

② 動的結合（dynamic binding）

③ 多相性（polymorphism）

（２）オブジェクト指向技術を用いた場合，テストが困難になったり，あるいは容易になったりする。継承，多相性の技術について，テストが困難になる理由，又は容易になる理由をそれぞれ述べよ。

Ｉ－１－４　ソフトウェアにおけるさまざまな性質を計測するために多くのメトリクスが提案され，利用されてきている。それらの一部を以下に示す。

凝集度，クローン数，サイクロマティック数，バグ密度， HalsteadのSoftware Science，ファンクションポイント

これらの中から任意の３つを選び，それぞれについて（１），（２）の問いに答えよ。

（１）何を計測するメトリクスか。

（２）その値が大きいということは，どのような意味をもつか。

Ⅰ－２　以下は，あるアパレルメーカーの顧客管理サービスに関するシステムへの要求の一部である。

アパレルメーカーであるＡ社は，東京，大阪，名古屋，福岡の４都市に新規に出店することにした。新規出店に際して，購入した客に会員カードを発行し，カードによる顧客管理と顧客サービスを行うことにした。顧客サービスとして，客の購入額に応じたポイントを付与し，ポイントが一定数に達すると，店舗内で買い物ができる商品券を贈呈する。システムの稼働は出店と同時で2012年４月１日である。

店舗にて2,000円以上の商品を購入した客に対して，新規入会を勧め，同意した客にカードを発行する。カードは申し込みと同時にその場で発行する。新規入会した客は一般会員となり，購入金額に応じてポイントが付与される。一般会員に付与されるポイントは，2,000円につき１ポイントである。保有するポイントが50ポイントに達する毎に，5,000円の商品券をその場で客に渡す。その際，客の保有するポイントから50ポイントを差し引く。

ポイントの有効期限は１年間とする。ポイントが50ポイント以上になった客はプレミアム会員となり，次回から，購入額2,000円につき２ポイントが付与される。なお，前回の購入日を含む１年間，購入実績のない客は，一般会員に戻る。

会員カードは４店舗に共通で利用できる。ポイントによって贈呈した商品券は４店舗のいずれでも利用することができるが，商品券による購入ではポイントは付与されない。

なお，システムは，会員カードから顧客情報を読み取り，レジから自動的に購入金額，購入日の情報を取得し，ポイント管理処理を行う。

以下の（１），（２）の問いに答えよ。（答案用紙を替えて**問題番号**を明記し，３枚以内にまとめよ。）

ただし，ポイントの管理に関するシステムの機能を対象とし，顧客情報，購入金額，日付などのデータの入出力部分や通信については対象外とする。なお，顧客管理やポイント管理に関する実際の内容との差異については考察の対象外とする。解答に当たり，仮定が必要な場合は明記すること。

（１）上記システムの開発が進み，システムテスト工程に入ったとする。システムが正しく動作することを確認するためのシステムテストシナリオを３つ記述せよ。なお，システムテストシナリオには，シナリオ名，事前条件，システムへの操作，確認方法という４つの項目を含めること。

（2）（1）で記述したシステムテストシナリオにおいて利用するテストデータを定義せよ。なお，テストデータは，以下のディシジョンテーブルの例の解説を参照して定義すること。

ディシジョンテーブルの例

表1は国際通常郵便物の料金を示している。表1は，手紙（定形）を表1の宛先に送付する場合に，重量に応じて，料金が設定されていることを示す。表1の情報をディシジョンテーブルの形式に記述したものを表2に示す。

表1※　国際通常郵便物の料金

宛先		25ｇまで	50ｇまで
第1地帯	アジア，米国の海外領土，パラオ他	90円	160円
第2地帯	オセアニア，中近東，北米，中米，西インド諸島，ヨーロッパ	110円	190円
第3地帯	南米，アフリカ	130円	230円

※）表1の郵便料金のデータは，郵便事業株式会社（ゆうびんホームページウェブサイト http://www.post.japanpost.jp/）を参考にして作成した。

表2　国際通常郵便物の料金のディシジョンテーブル

テストデータNo. ／ 宛先／重さ		1	2	3	4	.....	N	.....
宛先	第1地帯	中国	パラオ	グアム	－		－	
	第2地帯	－	－	－	米国		－	
	第3地帯	－	－	－	－		ガーナ	
重さ	～25g	5g	－	－	25g		－	
	～50g	－	25g	－	－		50g	
	その他	－	－	51g	－		－	
料金		90円	160円	定形外	110円		230円	

選択科目【16－3】情報システム・データ工学　　1時30分～5時

Ⅰ　次の２問題（Ⅰ－１，Ⅰ－２）について解答せよ。

Ⅰ－１　次の４設問のうち３設問を選んで解答せよ。（設問ごとに答案用紙を替えて**解答設問番号**を明記し，それぞれ１枚以内にまとめよ。）

Ⅰ－１－１　社団法人 日本情報システム・ユーザ協会（JUAS）は，「ソフトウェア開発環境基準に関する調査」報告書の中でソフトウェアメトリックスについての調査を発表している。その中で「業務システム・情報システムのレベルアップは３つのステップで実現すべきである」と提言している。この３つのステップとは何か。第１ステップにおいて重視されるソフトウェア開発の３大メトリックスとは何か。また，その３大メトリックスにおいて，高い評価を得るために，技術士としてどう取り組むべきかについて述べよ。

Ⅰ－１－２　組織体の個々の部門で管理されているデータ資源を統合化し，経営的な意思決定に有効に活用するデータベース統合化を行うとき，出発点となる概念データモデリングは，管理データの項目数が大規模化するにつれて困難性を増す。そのため，一定のアプローチにしたがってモデリングを行うことが必要になる。そのアプローチの代表例として，トップダウンアプローチとボトムアップアプローチがある。それぞれのアプローチについて，その考え方と長所・短所，及び効果的な適用業務分野について述べよ。

Ⅰ－１－３　ワイヤレス技術に関する次の問いに答えよ。

（１）3.9G携帯電話システム（広域無線ブロードバンド）について説明せよ。

（２）Wi-Fi無線LAN（近距離通信）について説明せよ。

（３）上記の技術の活用について，次の①，②に答えよ。

①　スマートフォンなどのモバイル端末の活用方法としてどのようなものが考えられるか。また，課題は何か。

②　企業における情報システムで，どのような活用方法が考えられるか。また，課題は何か。

Ⅰ－１－４　グリーンITの用語について説明し，ITが環境面でどのように社会貢献できるか述べよ。

Ⅰ－２　次の２設問のうち１設問を選んで解答せよ。（答案用紙を替えて**解答設問番号**を明記し，それぞれ指定の枚数以内にまとめよ。）

Ⅰ－２－１　企業における情報システムを経営や意思決定に活用する取り組みは，例えば1960年代のマネージメントインフォメーションシステム（MIS）などから継続的に提唱され，現在もビジネスインテリジェンス（BI）などが活用されている。情報システムを経営や意思決定に活用することを使命とする情報工学部門の技術士の立場から，以下の（１），（２）の問いに答えよ。

（１）情報システムの経営への寄与に関する歴史（おおよそ50年程度）を振り返るとともに，現状と今後の展望，及び課題について述べよ。（答案用紙１枚以内に記述せよ。）

（２）BIの活用について，経営者の理解を得るための方策を述べよ。また，BIを構成するシステムやツールを３つ挙げ，それを使用するメリットや効果について述べよ。（答案用紙２枚以内に記述せよ。）

Ⅰ－２－２　社会活動のインフラとして電力の供給が大きな課題となっている。このような社会問題の解決のために，情報処理を活用して電気の供給をリアルタイムに最適化したり，企業や家庭の電気消費を効率化したりすることで，総合的に電気利用をコントロールしようとするスマートグリッドという考え方が提唱されている。米国では2009年に金融危機脱却の政策として公的資金を投入して電力インフラの整備を開始した。また，欧州では原子力や火力以外の発電能力の強化，及び電力インフラの構築が進められている。日本においても2011年３月の地震を契機に，電力の供給能力の管理や電力消費の効率化の実施が急務になってきた。このように期待されてきたスマートグリッドに関する次の問いについて述べよ。（それぞれ答案用紙１枚以内に記述せよ。）

（１）スマートグリッドとはどのような考え方か。

（２）情報アーキテクチャをスマートグリッドにどのように活用できるか，情報工学部門の技術士の立場から述べよ。

（３）日本においてスマートグリッドを推進するメリット，及び課題は何か，情報工学部門の技術士の立場から述べよ。

選択科目【16－4】情報ネットワーク　　1時30分～5時

Ⅰ　次の２問題（Ⅰ－１，Ⅰ－２）について解答せよ。

Ⅰ－１　次の５設問のうち３設問を選んで解答せよ。（設問ごとに答案用紙を替えて**解答設問番号**を明記し，それぞれ１枚以内にまとめよ。）

Ⅰ－１－１　公開鍵暗号方式を利用したセキュリティ基盤であるPKI（Public Key Infrastructure）では，公開鍵（公開鍵証明書）を第三者が保証することにより安全なやり取りを実現している。PKIにおける「認証局モデル」について述べよ。

Ⅰ－１－２　LTE（Long Term Evolution）には，３G方式と比較し以下の３つの特長がある。３つの特長から１つを選び，それを実現している通信技術について述べよ。

① 通信速度の向上

② 周波数利用効率の向上

③ マルチパスによる相互干渉の低減

Ⅰ－１－３　HTML５と並行して検討が進んでいるWebSocket（draft－ietf－hybi－thewebsocketprotocol－07）について，何故それが必要とされるのか，背景について述べよ。

Ⅰ－１－４　FCoE（Fiber Channel over Ethernet）について説明し，背景，メリット，デメリットについて述べよ。

Ⅰ－１－５　IPv６におけるPathMTU Discovery（RFC1981）について述べよ。

Ｉ－２　次の２設問のうち１設問を選んで解答せよ。（答案用紙を替えて**解答設問番号**を明記し，３枚以内にまとめよ。）

Ｉ－２－１　特定の国や地域からしか自社サービスにアクセスできないようにしようとしているインターネット上のサービスがある。例えばラジオ放送番組のインターネット向けサイマル放送サービスを日本国内で展開しているRadikoは，都道府県ごとに聴取地域を分け，既存ラジオ局の放送範囲に合わせて聴取できる放送番組を制限しようとしている。米国においてテレビ番組や映画などのストリーミング配信を行っているHuluは，提供動画を米国国内からしか視聴できないようにしようとしている。インターネット上のサービスの地域制限について，情報工学部門の技術士としての立場から下記の問いに答えよ。

（１）特に視聴環境等の違いによって，対象地域外でもアクセスできてしまうケース，対象地域内にも関わらずアクセスできないケースが発生する可能性について考慮しながら，インターネット上のサービスにおいてサービス提供地域を制限しようとする方式を設計するに際して検討すべき技術的課題について考察せよ。（答案用紙１枚以内にまとめよ。）

（２）インターネット上のサービスにおける地域制限の具体的な方式を提案せよ。提案方式が前項で検討した技術的課題をどのように解決するのか，あるいは解決できない課題が残る場合はどのような課題が残るのかについて説明せよ。さらに，提案方式の技術的実現容易性・コスト，並びに運用時の運用容易性・コストについて技術的見地から説明せよ。（答案用紙２枚以内にまとめよ。）

Ⅰ－２－２　製造業のＡ社は，自社の販売管理システムと同等のシステムを，業務提携先のＢ社に対しSaaSの形態で提供することになった。同システムの利用者はＢ社の社員，並びにＢ社の取引先社員で，プライベートネットワーク又はインターネットを経由しサーバへアクセスする。Ａ社のデータセンタのサーバは，市販のハイパーバイザ型仮想化ソフトウェアを利用し仮想化されている。Ａ社の販売管理システムも，数十台の仮想サーバ上で稼働している。

Ａ社の情報システム部は，SaaSの形態で提供するＢ社向け販売管理システムに関して次の構想をまとめた。

① Ａ社のデータセンタ内に，Ｂ社向けシステムを構築する。

② Ｂ社向けシステムと他のＡ社システムは独立で，相互のアクセスは許さない。

③ Ｂ社向けシステムは仮想サーバで稼働させ，物理サーバは他のＡ社のシステムと共有させる。

④ 現行のＡ社専用ネットワークに，Ｂ社向けネットワークを新たに追加する。

⑤ 販売管理システムはRDBMSを使って構築されており，今回アーキテクチャの見直しは行わない。

構想に基づき，Ａ社の情報システム部は情報工学部門の技術士であるあなたに，追加で構築するＢ社向けネットワークの検討を依頼してきた。以上を踏まえて下記の問いに答えよ。

（１）Ａ社のデータセンタに追加するＢ社向けネットワークの構成を考え，その概要を述べよ。概要を述べたネットワーク上において，Ａ社とＢ社の販売管理システムが同一の物理サーバを共有（構想③）しつつ，相互のアクセスを排除する（構想②）ための技術的仕組みについて説明せよ。（答案用紙１枚以内にまとめよ。）

（２）Ｂ社向けネットワークの導入，並びに運用に関して，想定される問題を複数挙げ，解決策を述べよ。（答案用紙２枚以内にまとめよ。）