Sec01-02-62\_各種ガイドブックの内容要約\_【参考】IT関連

ドキュメントを参照: [Sec01-02-50\_サイバーセキュリティ関連\_各種ガイドブックの内容要約.mmap](file:///D:\Cloud_Storage\OneDrive%20-%20ＮＰO知的資源イニシアティブ（ＩＲＩ）\git_repository_Duo\Sharing_Knowledge3\MindManager3\Sec01-02-50_サイバーセキュリティ関連_各種ガイドブックの内容要約.mmap)

1. （原本は「Bib10-08国の事業が実施に至るまで」）
2. IT戦略本部
3. 高度情報通信ネットワーク社会形成基本法（IT基本法）（2015年2月1日改訂施行）

ドキュメントを参照: [honbun.html](http://www.kantei.go.jp/jp/singi/it2/hourei/honbun.html)

1. 「世界最先端IT国家創造宣言」の改定（高度情報通信ネットワーク社会推進戦略本部（IT戦略本部））（2016.5.20閣議決定)

ドキュメントを参照: [siryou1.pdf](http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20160520/siryou1.pdf)

* 1. Ⅰ.世界最先端 IT 国家創造宣言に基づくこれまでの成果
     1. １. これまでの代表的な成果
        1. (１) 行政情報システム改革を通じた利用者志向の行政サービスの実現
        2. (２) マイナンバー制度を活用した国民生活の利便性の向上
        3. (３) 安全・安心なデータ流通の促進
        4. (４) 農業のIT 化による国際競争力強化
        5. (５) 世界で最も安全で環境にやさしく経済的な道路交通社会の実現
     2. ２．IT 利活用による目指すべき社会の実現に向けた今後の重点的な取組方針
  2. II. 「国から地方へ、 地方から全国へ」（IT 利活用の更なる推進のための３つの重点項目）
     1. １．[重点項目１] 国・地方のIT 化・業務改革（BPR）の推進
        1. (１) 国のIT 化・業務改革（BPR）の更なる推進
        2. (２) 地方公共団体のIT 化・業務改革（BPR）の推進
        3. (３) ガバナンス体制の強化
     2. ２．[重点項目２] 安全・安心なデータ流通と利活用のための環境の整備
        1. (１) 利用者志向のデータ流通基盤の構築
        2. (２) データ流通の円滑化と利活用の促進
        3. (３) 課題解決のためのオープンデータの「実現」（オープンデータ2.0）
     3. ３．[重点項目３] 超少子高齢社会における諸課題の解決
        1. (１) ビッグデータを活用した社会保障制度の変革
        2. (２) マイナンバー制度等を活用した子育て行政サービスの変革
        3. (３) IT 利活用による諸課題の解決に資する取組
           1. ① 産業競争力の強化
           2. ② 地方創生の実現
           3. ③ マイナンバー制度を活用した国民生活の利便性の向上
           4. ④ 安全で災害に強い社会の実現
  3. III. 推進体制等
     1. １．政府 CIO の司令塔機能の発揮
     2. ２．関係本部等との連携体制
     3. ３．進捗管理における評価指標の設定・管理
     4. ４．国際貢献及び国際競争力の強化に向けた国際展開

1. 電子行政オープンデータ戦略（2012年7月4日IT戦略本部）【再掲】

ドキュメントを参照: [denshigyousei.html](http://www.kantei.go.jp/jp/singi/it2/denshigyousei.html)

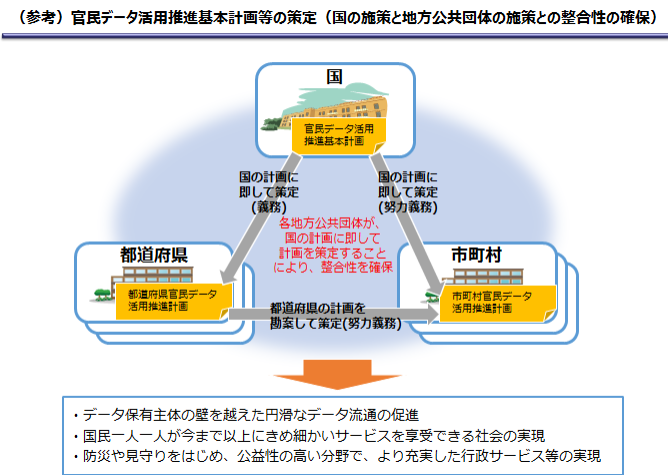
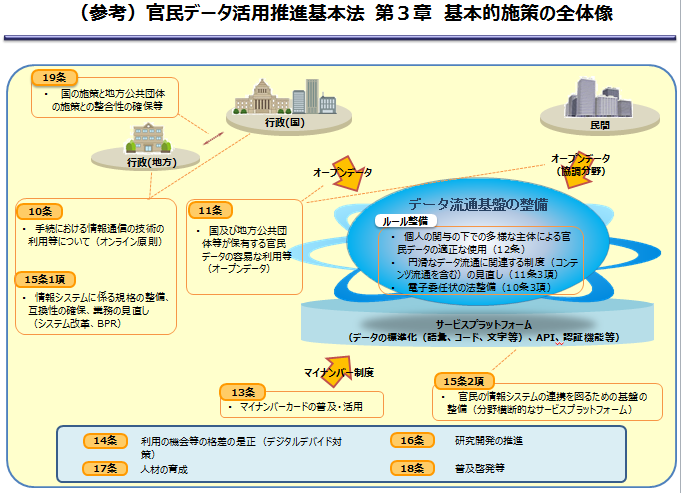
* 1. ○電子行政オープンデータ戦略の概要（抜粋）61
  2. Ⅰ．基本的方向性
     1. ＜基本原則＞
     2. － 政府自ら積極的に公共データを公開すること
     3. － 機械判読可能な形式で公開すること
     4. － 営利目的、 非営利目的を問わず活用を促進すること
     5. － 取組可能な公共データから速やかに公開等の具体的な取組に着手し、 成果を確実に蓄積していくこと
  3. Ⅱ．具体的な施策
     1. １．公共データ活用の推進
        1. ①公共データ活用ニーズの把握
        2. ②データ提供方法等に係る課題の整理、 検討
        3. ③民間サービスの開発
     2. ２．公共データ活用のための環境整備
        1. ①公共データ活用のために必要なルール等の整備
           1. 各府省におけるデータ公開時の著作権の取扱い、 利用条件、 機械からのアクセスルール、 利用者と提供者の責任分担の在り方、 機微情報の取扱いの在り方等について、 利用者の利便性と権利者の権利の保護に十分配意しつつ、 公共データ活用のために必要なルール等を整備する。
        2. ②データカタログの整備
        3. ③データ形式・構造等の標準化の推進等
        4. ④提供機関支援等についての検討

1. 電子行政オープンデータ推進のためのロードマップ（2013年6月14日IT戦略本部決定）

ドキュメントを参照: [siryou3.pdf](http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20130614/siryou3.pdf)

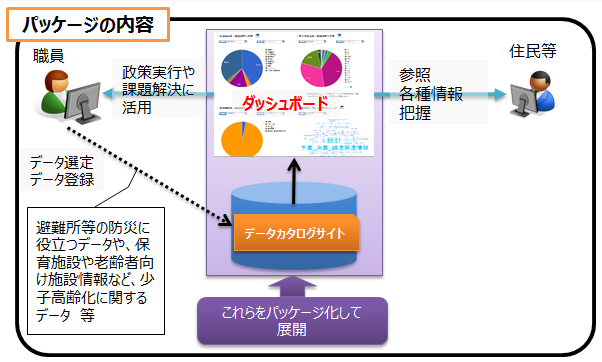
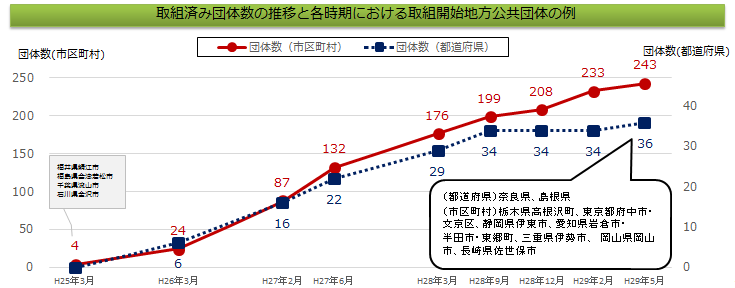
1. 官民データ活用推進基本法（平成28年法律第103号）
2. 「オープンデータ基本指針」（案）「オープンデータ基本指針」（案）【2017年5月23日官民データ活用推進基本計画実行委員会】

ドキュメントを参照: [gijisidai.html](http://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/opendata_wg_dai3/gijisidai.html)

* 1. 体制
     1. 高度情報通信ネットワーク社会推進戦略本部（IT本部）
     2. 官民データ活用推進戦略会議
        1. ＜法律（官民データ活用推進基本法）により設置（平成28年12月14日）
        2. 議　 長：内閣総理大臣 副議長：情報通信技術（IT）政策担当大臣、 内閣官房長官、 総務大臣、 経済産業大臣 議　 員：議長・副議長を除く全国務大臣、 政府CIO及び有識者
     3. 官民データ活用推進基本計画実行委員会
        1. ＜官民データ活用推進戦略会議議長決定により設置（平成29年3月31日）＞
        2. 会長：民間委員、 （委員会構成：民間委員＋各省庁局長級
  2. 概念
     1. サブトピック  
        
     2. サブトピック  
        
  3. オープンデータ基本指針（案）の概要
     1. 本基本指針の位置づけ
        1. 平成28年12月14日に公布・施行された「官民データ活用推進基本法」において、 国、 地方公共団体、 事業者が保有する官民データの容易な利用等について規定された。 本文書は、 これまでの取り組みを踏まえ、 オープンデータ・バイ・デザイン（注）の考えに基づき、 国、 地方公共団体、 事業者が公共データの公開及び活用に取り組む上での基本方針をまとめたものである。
     2. １．オープンデータの意義
        1. （１）国民参加・官民協働の推進を通じた諸課題の解決、 経済活性化
        2. （２）行政の高度化・効率化
        3. （３）透明性・信頼の向上
     3. ２．オープンデータの定義
        1. ①　営利目的、 非営利目的を問わず二次利用可能なルールが適用されたもの
        2. ②　機械判読に適したもの
        3. ③　無償で利用できるもの
     4. ３．オープンデータに関する基本的ルール
        1. （１）公開するデータの範囲
           1. ・・・各府省庁が保有するデータは、 原則オープンデータとして公開。 公開することが適当でない公共データは、 公開できない理由を原則開示するとともに、 限定的な関係者間での共有を図る「限定公開」といった手法も積極的に活用。
        2. （２）公開データの二次利用に関するルール
           1. ・・・ 原則、 政府標準利用規約を適用。
        3. （３）公開環境
           1. ・・・特にニーズが高いと想定されるデータは、 一括ダウンロードを可能とする仕組みの導入や、 APIを通じた提供を推進。
        4. （４）公開データの形式等
           1. ・・・機械判読に適した構造及びデータ形式で掲載することを原則。 法人情報を含むデータは、 法人番号を併記。
        5. （５）公開済みデータの更新
           1. ・・・可能な限り迅速に公開するとともに適時適切な更新。
     5. ４．オープンデータの公開・活用を促す仕組み
        1. （１）オープンデータ・バイ・デザインの推進
           1. ・・・行政手続き及び情報システムの企画・設計段階から必要な措置
        2. （２）利用者ニーズの反映
           1. ・・・各府省庁の保有データとその公開状況を整理したリストを公開 利用者ニーズを把握の上、 ニーズに即した形での公開
     6. ５．推進体制
        1. （１）相談窓口の設置
           1. ・・・総合的な相談窓口（内閣官房IT総合戦略室）・相談窓口（各府省庁）の設置
        2. （２）推進体制
           1. ・・・内閣官房IT総合戦略室は、 政府全体のオープンデータに関する企画立案・総合調整、 各施策のレビュー、 フォローアップを実施等
     7. ６．地方公共団体、 独法、 事業者における取組
        1. 地方公共団体
           1. ・・・官民データ法の趣旨及び本基本指針を踏まえて推進。
        2. 独立行政法人
           1. ・・・国費によって運営されていること又は実施している事業や研究があることに鑑み、 基本指針に準拠して取組を推進することが望ましい。
        3. 公益事業分野の事業者
           1. ・・・その公益性に鑑み、 本基本指針及び利用者ニーズを踏まえて推進することが望ましい。
  4. オープンデータ・バイ・デザインの推進（案）
     1. １．オープンデータ・バイ・デザインの定義
        1. 「行政が保有するデータについては、 オープンデータを前提として情報システムや業務プロセス全体の企画、 整備及び運用を行う」
     2. ２．オープンデータ・バイ・デザインの具体的な内容
        1. 行政が保有するデータを原則としてオープンデータ化するとともに、 利用者が活用しやすい形で公開するため、 行政手続及び情報システムの企画・設計段階から必要な措置を講じる。
        2. （１）一括ダウンロードやAPIを通じたデータ提供
           1. 特にニーズが高いと想定されるデータは一括ダウンロードを可能とする仕組みの導入や、 APIを通じた提供を推進する
        3. （２）メタデータの公開
           1. 公開データについて適切なメタ情報を付与し、 政府のデータカタログサイトへ漏れなく登録がされるようにする
        4. （３）機械判読に適したファイル形式およびデータ構造
           1. 公開可能なデータを抽出/出力/公開するための仕組みをシステム要件に含める
           2. 公開データがJSON・CSV等、 機械判読に適したファイル形式で公開されるようにする
           3. 各府省庁が行う委託・請負契約に当たっては、 報告書等の成果物を機械判読に適したファイル形式で納品されるようにする
        5. （４）データ構造やデータ形式の標準化
           1. 可能な限り標準化された形式やコード体系等でデータを格納・出力する法人情報を含むシステムの開発・更新に当たっては、 法人番号の併記を原則とする
        6. （５）公開済みデータの更新
           1. データ公開後も適切にデータの更新がされるように仕組みや運用体制を構築する
     3. また、 データベース構築にあたっては、 オープンデータを前提とする（非公開とすることに合理的な理由がないものについては、 予算計上を認めないこととする）。
     4. 今後オープンデータ・バイ・デザインの取組は、
        1. 「デジタル・ガバメント推進方針」の動き※と連携しながら進めていく。
           1. デジタル・ガバメント推進方針【2017年5月】
           2. デジタル・ガバメント実行計画【2017年内】
           3. 【2018年以降】

実行計画に基づく各種取組の推進

各府省における中長期的な計画の策定、 推進　等

* + - 1. 企画・設計時の具体的な実施事項については「政府情報システムの整備および管理に関する標準ガイドライン」及び同実務手引書に盛り込み、 政府情報システム全体への浸透を図ることとする。
  1. 地方公共団体の取り組み促進（案）
     1. 地方公共団体におけるオープンデータへの取組を加速する改良版パッケージの提供。
        1. オープンデータに取組む意思や必要性は感じているが、 具体的な取組方法が分からない地方公共団体を支援するため、 関係諸団体と連携し、 オープンデータのデータカタログとダッシュボードアプリケーションをパッケージ化して提供することで、 地方公共団体によるオープンデータの導入・活用を促進する。
     2. サブトピック  
        
     3. ■期待される効果
        1. ・防災関連や少子高齢化など地域課題に関係するデータの公開による、 地域課題解決の一助
        2. ・公開と活用両方の自治体展開パッケージの提供による、 地方公共団体の取組を容易化
        3. ・標準化の推進（登録データのフォーマット標準例の提供等）
        4. パッケージはオープンソースとしてGitHubで公開することにより、 他の地方公共団体に展開可能とする (※) 。
     4. ※パッケージ一式導入用：
        1. https://github.com/nes-opendata/odpkg-docker
     5. ※ダッシュボードのみ導入用：
        1. https://github.com/nes-opendata/odpkg-dashboard
     6. オープンデータに取り組む地方公共団体数
        1. サブトピック  
           
     7. 導入予定
        1. ・福岡市、 久留米市へダッシュボードを導入。 （平成29年4月公開）
        2. ・長崎県（平成29年6月公開予定）、 京都府（平成29年6月公開予定）へパッケージを導入。

1. 世界最先端ＩＴ国家創造宣言・官民データ活用推進基本計画【2017年5月30日付け閣議決定】
   1. 本文

ドキュメントを参照: [ITsengen\_honbun.pdf](https://cio.go.jp/sites/default/files/uploads/documents/ITsengen_honbun.pdf)

* + 1. 第１部 総論 . 3
       1. Ⅰ IT 戦略の新たなフェーズに向けて（「データ」がヒトを豊かにする社会の実現） 3
          1. Ⅰ－１ これまでのIT 戦略 3
          2. Ⅰ－２ IT 戦略の新たなフェーズに向けて（「データ」大流通時代の到来） 3
          3. Ⅰ－３ 「データ」の上で、 ヒト、 モノ、 カネが活いきる社会 . 5
          4. Ⅰ－４ 「データ」がヒトを豊かにする社会、 「官民データ利活用社会」のモデル構築 . 6
       2. Ⅱ 「官民データ利活用社会」のモデルの構築に向けて 8
          1. Ⅱ－１ IT をめぐる諸動向 8

Ⅱ－１－(1) 技術・サービスの動向等 . 8

Ⅱ－１－(2) データ利活用への期待の高まり . 9

* + - * 1. Ⅱ－２ 我が国の置かれた状況等 10

Ⅱ－２－(1) 急速な人口構造の変化等に伴う諸課題 10

Ⅱ－２－(2) 今の国民が生活において求めるもの（国民視点での取組の強化） 10

* + - * 1. Ⅱ－３ 「官民データ利活用社会」のモデルの構築 11

Ⅱ－３－(1) 我が国の置かれた諸状況を踏まえたデータ利活用による新たなライフスタイルの提案 . 11

Ⅱ－３－(2) 官民データの利活用に向けた環境整備 12

Ⅱ－３－(3) 我が国が目指す社会の構築等 14

* + - 1. Ⅲ 推進体制 .15
         1. Ⅲ－１ 官民データ活用推進基本計画のPDCA . 15
         2. Ⅲ－２ 他の推進本部等との連携 16
      2. Ⅳ 地方公共団体との連携・協力 .18
      3. Ⅴ 事業者等との連携・協力 .18
    1. 第２部 官民データ活用推進基本計画 . 20
       1. Ⅰ 官民データ活用推進基本計画に基づく推進の施策 .20
          1. Ⅰ－１ 官民データ活用の推進に関する施策についての基本的な方針 20

Ⅰ－１－(1) 基本計画の策定とその着実な実施 20

Ⅰ－１－(2) 重点分野の指定（分野横断的なデータ連携を見据えつつ） 21

Ⅰ－１－(3) 国と各地方公共団体の施策の整合性の確保 23

Ⅰ－１－(4) 成果の横展開 24

Ⅰ－１－(5) 官民データ活用によるEBPM の推進 . 24

* + - * 1. Ⅰ－２ 具体的施策 25
      1. Ⅱ 施策集 37
         1. Ⅱ－１

Ⅱ－１－(1) 行政手続等のオンライン化原則【基本法第10 条関係】 39

Ⅱ－１－(2) オープンデータの促進【基本法第11 条第１項及び第２項関係】、 データの円滑な流通の促進【基本法第11 条第３項関係】 44

Ⅱ－１－(3) データ利活用のルール整備【基本法第12 条関係】 52

Ⅱ－１－(4) マイナンバーカードの普及・活用【基本法第13 条関係】 56

Ⅱ－１－(5) 利用の機会等の格差の是正（デジタルデバイド対策）【基本法第14 条関係】. 61

Ⅱ－１－(6) 情報システム改革・業務の見直し【基本法第15 条第１項関係】 65

Ⅱ－１－(7) データ連携のためのプラットフォーム整備【基本法第15 条第２項関係】 70

Ⅱ－１－(8) 研究開発【基本法第16 条関係】 77

Ⅱ－１－(9) 人材育成、 普及啓発等【基本法第17 条、 第18 条関係】 . 83

Ⅱ－１－(10) 国の施策と地方の施策との整合性の確保等【基本法第19 条関係】 . 88

Ⅱ－１－(11) 国際貢献及び国際競争力の強化に向けた国際展開 89

* 1. 別表

ドキュメントを参照: [ITsengen\_beppyo.pdf](https://cio.go.jp/sites/default/files/uploads/documents/ITsengen_beppyo.pdf)

* 1. 用語集 【後日、 別シートに移行予定】

ドキュメントを参照: [ITsengen\_yougosyu.pdf](https://cio.go.jp/sites/default/files/uploads/documents/ITsengen_yougosyu.pdf)

* + 1. アクセシビリティ
       1. 情報通信分野においては、 高齢者や障害者等、 ハンディを持つ人にとって、 情報やウェブサービス、 ソフトウェア等が円滑に利用できることを意味する。
    2. アジャイル
       1. ソフトウェア開発手法の1 つで、 開発対象を多数の小さな機能に分割し、 反復(イテレーション) と呼ばれる短い開発期間単位ごとに1 つの機能を開発・ソフトウェアリリースを行う手法である。 短いサイクルで一連のPDCA を回す開発手法であり、 日々生じる変化にすばやく適応することに主眼が置かれている。
    3. 医療等ID
       1. 医療等ID は、 患者の医療情報の連携や研究利用など、 保健医療分野の情報連携を安全で効率的に行うための、 一意的な識別子のことである。 「医療等分野における番号制度の活用等に関する研究会」(平成27 年12 月報告書取りまとめ)において、 具体的な制度設計等が取りまとめられた。
    4. ウェアラブル端末
       1. 腕や頭部などの身体に装着して利用する情報端末のこと。 デバイスに搭載されたセンサーを通じて装着している人の生体情報を取得・送信し、 クラウド上で解析しフィードバックすることで、 フィットネスやヘルスケア分野などでの活用が期待されている。 また、 スマートフォンと連携してのハンズフリーでのアプリ操作や、 産業分野での作業支援などにも使われ始めている。
    5. オープンデータ
       1. 一般的には、 データは誰もが制限なしにアクセス、 再利用、 そして再配布できるように、 利用可能にすべきであるという概念のことであるが、 本戦略においては、 公的機関が保有するデータを、 民間が編集・加工等をしやすい形で、 インターネットで公開することを意味する。
    6. オープンデータ・バイ・デザイン
       1. 行政が保有するデータについて、 オープンデータを前提として情報システムや業務プロセス全体の企画、 整備及び運用を行うこと。
    7. おもてなしシステム
       1. 訪日外国人の同意の下、 属性（性別・年代・国籍等）や行動履歴（宿泊・買い物・移動等）に関するデータを事業者間で共有・活用し、 先進的かつ多様なサービス・決済環境を提供する仕組みのこと。
    8. 海事生産性革命(i-Shipping)
       1. IT を利活用して船舶の設計から建造、 運航に至る全てのフェーズにおいてイノベーションの創出・生産性向上を目指す政府の取り組みの総称。
    9. 課題解決型オープンデータ
       1. データの公開のみにとどまらず、 公開されたデータを積極的に利活用することによって様々な社会課題の解決を目指す、 オープンデータに係る取組のこと。
    10. 共通語彙基盤
        1. 氏名や住所等語彙の表記・意味・データ構造を共通化してデータの交換・活用を容易にする基盤のこと。
    11. 業務改革（BPR）
        1. BPR はBusiness Process Reengineering の略である。 既存の組織やビジネスルールを抜本的に見直し、 利用者の視点に立って、 業務プロセス全体について職務、 業務フロー、 管理機構、 情報システムを再設計すること。
    12. クラウドサービス
        1. インターネット等のブロードバンド回線を経由して、 データセンタに蓄積されたコンピュータ資源を役務（サービス）として、 第三者（利用者）に対して遠隔地から提供すること。
    13. クラウド・バイ・デフォルト
        1. システム導入に際し、 クラウドサービスの活用を前提とする考え方のこと。
    14. 公共価値
        1. 制度の不知等利用者の置かれた環境にかかわらず、 公平・公正な行政サービスを享受できること、 行政サービスの利用が簡便でメリットがあること、 また、 行政機関が保有する資産を利用することで新たなビジネスを創造できること等、 利用者たる国民等にとっての行政サービスの有用性を意味する。
    15. 公的個人認証サービス
        1. 公的個人認証サービスとは、 オンラインで（＝インターネットを通じて）申請や届出といった行政手続などやインターネットサイトにログインを行う際に、 他人による「なりすまし」やデータの改ざんを防ぐために用いられる本人確認の手段。 「電子証明書」と呼ばれるデータを外部から読み取られるおそれのないマイナンバーカード等のIC カードに記録することで利用が可能となる。
        2. 電子証明書には、 以下の２種類がある。
        3. 署名用電子証明書・・・インターネット等で電子文書を作成・送信する際に利用（例 e-Tax 等の電子申請）。 「作成・送信した電子文書が、 利用者が作成した真性なものであり、 利用者が送信したものであること」を証明する。
        4. 利用者証明用電子証明書・・・インターネットサイトやコンビニ等のキオスク端末等にログインする際に利用（例 マイナポータルへのログイン、 コンビニでの公的な証明書の交付）。 「ログインした者が、 利用者本人であること」を証明。
    16. コネクテッドカー
        1. 情報端末としての機能を有する自動車のことであり、 車両の状態や周囲の道路状況などの様々なデータをセンサーにより取得し、 ネットワークを介して集積・分析することで、 新たな価値を生み出すことが期待されている。
    17. コネクテッド・ワンストップ
        1. 民間サービスを含め、 複数の手続・サービスがどこからでも一か所で実現 することを原則とする考え方のこと。
    18. サービスデザイン思考
        1. サービスを利用する際の利用者の一連の行動に着目し、 利用者がその手続を利用しようとした背景や、 手続を利用するに至るまでの過程、 利用後の行動までを一連の流れとして捉え、 利用者の心理や行動等を含めた体験（UX：ユーザーエクスペリエンス）全体を最良とすることを目標にしてサービス全体を設計する考え方のこと。
    19. シェアリングエコノミー
        1. 個人等が保有する活用可能な資産等（スキルや時間等の無形のものを含む。 ）を、 インターネット上のマッチングプラットフォームを介して他の個人等も利用可能とする経済活性化活動のこと。
    20. 準天頂衛星
        1. 日本で常に天頂付近に１機以上の測位衛星が位置し、 複数の軌道面にそれぞれ配置された測位衛星を組合せて位置を測定する衛星及びそのシステムのこと。 全国をほぼ100%カバーする高精度の衛星測位サービスの提供が可能である。
    21. 情報銀行
        1. 情報利用信用銀行の略で、 個人とのデータ活用に関する契約等に基づき、 PDS等のシステムを活用して個人のデータを管理するとともに、 個人の指示又は予め指定した条件に基づき個人に代わり妥当性を判断の上、 データを第三者（他の事業者）に提供する事業のこと。 データの提供・活用に関する便益は、 データ受領事業者から直接的又は間接的に本人に還元される。
    22. スマートホーム
        1. IoT 技術等によって家庭内の機器をネットワークでつなぎ、 制御することで、 生活者のニーズに応じた効率的かつ快適なサービスの提供を可能とした住まいのこと。
    23. 政府共通プラットフォーム
        1. 「新たな情報通信技術戦略」(平成22 年５月IT 戦略本部決定)に基づき、 国の行政情報システム全体の運用コストの削減、 セキュリティ強化等を図ることを目的とする情報システム基盤。 クラウドコンピューティング技術を活用した本基盤（平成25 年３月から稼働）の活用により、 各府省が別々に整備・運用している行政情報システムを可能なものから統合・集約化している。
    24. 政府統計の総合窓口（e-Stat）
        1. 各府省が公表する統計データを一つにまとめ、 統計データの検索をはじめとした、 さまざまな機能を備えた政府統計のポータルサイトのこと。 各府省が公表している統計表をExcel・CSV・PDF 形式でダウンロードすることが可能。
    25. 地理空間情報（Ｇ空間情報）
        1. 地理空間上の特定の地点又は区域の位置を示す情報（位置情報）と、 これに関連付けられた様々な情報のこと。
    26. ディープラーニング
        1. ニューラルネットワーク（機械学習におけるアルゴリズムの1 つ）を用いた機械学習における技術の1 つである。 情報抽出を一層ずつ多階層にわたって行うことで、 高い抽象化を実現する。 従来の機械学習では、 学習対象となる変数（特徴量）を人が定義する必要があった。 ディープラーニングは、 予測したいものに適した特徴量そのものを大量のデータから自動的に学習することができる点に違いがある。
    27. デジタルデバイド
        1. インターネットやパソコン等の情報通信技術を利用できる者と利用できない者との間に生じる格差のこと。
    28. デジタルファースト
        1. デジタル技術を徹底的に活用し、 デジタル処理を前提としたサービス設計を行うこと。
    29. データ取引市場
        1. データ保有者と当該データの活用を希望する者を仲介し、 売買等による取引を可能とする仕組み（市場）のこと。 価格形成・提示、 需給マッチング、 取引条件の詳細化、 取引対象の標準化、 取引の信用保証等の機能を担うことが想定される。
    30. テレワーク
        1. テレワークとは、 ICT を活用し、 場所や時間を有効に活用できる柔軟な働き方のことであり、 雇用型と自営型に大別される。 雇用型テレワークとは、 ICT を活用して、 労働者が所属する事業場と異なる場所で、 所属事業場で行うことが可能な業務を行うこと（例：在宅勤務、 モバイルワーク、 サテライトオフィスでの勤務）を言い、 自営型テレワークとは、 ICT を活用して、 請負契約等に基づき、 遠隔で、 個人事業者・小規模事業者等が業務を行うこと（例：ＳＯＨＯ、 在宅ワーク、 クラウドソーシング）を言う。
    31. 電子委任状
        1. 法人の代表者から与えられている権限の範囲を表示する電磁的記録のこと。
    32. 匿名加工情報
        1. 特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、 当該個人情報を復元することができないようにしたもののこと。
        2. 匿名加工情報は、 個人情報に関するルールは適用されず、 加工基準に従った加工その他の一定のルールのもと、 本人の同意を得ることなく自由に利活用することができる。 これにより、 新事業や新サービスの創出や、 国民生活の利便性の向上に寄与することが期待される。
    33. 農地情報公開システム
        1. 農地の集積・集約化を進めるため、 各市町村の農業委員会が整備している農地台帳に基づく農地情報を電子化・地図化して公開する全国一元的なクラウドシステム（平成27 年４月稼働）のこと。
    34. バックオフィス連携
        1. 地方公共団体を含む各行政機関が保有する情報を行政機関間でやり取りすること。 行政手続の際に必要な添付書類の省略を始めとした利便性の向上等が期待される。
    35. ビッグデータ
        1. ボリュームが膨大でかつ構造が複雑であるが、 そのデータ間の関係性などを分析することで新たな価値を生み出す可能性のあるデータ群のこと。 例えば、 ソーシャルメディア内のテキストデータ・画像、 携帯電話・スマートフォンが発信する位置情報、 時々刻々と生成されるセンサデータなどがある。
    36. 府省庁連携災害情報共有方式(SIP4D)
        1. 府省庁横断で災害情報を共有する仕組みのこと。
    37. ブロックチェーン
        1. 複数のデータを塊り（ブロック）にし、 暗号化してチェーンのように繋ぎ合わせて情報を管理する仕組みのこと。 複数の端末で運用するため、 耐障害性が高く、 またデータの改竄もほぼ不可能と言われている。
    38. 法人インフォメーション
        1. 政府の許認可、 委託契約受注、 補助金交付、 表彰受賞等の法人の情報等を一括で検索、 閲覧できるWeb システムのこと。
    39. 法人番号
        1. 設立登記法人、 国の機関、 地方公共団体、 その他の法人や人格のない社団等に対し、 国税庁長官より1 法人につき1 つ指定される13 桁の番号のこと。 マイナンバーとは異なり、 自由な利活用が可能。 なお、 法人の支店や事業所、 個人事業主等には法人番号は指定されない。
    40. マイナポータル
        1. マイナンバー制度の導入に併せて新たに構築した、 国民一人ひとりがアクセスできるポータルサイトのこと。 具体的には、 自己情報表示機能、 情報提供等記録表示機能、 プッシュ型サービス、 ワンストップサービス等を提供する基盤であり、 国民一人ひとりが様々な官民のオンラインサービスを受けられるよう、 平成29 年秋頃に本格運用を開始予定である。
    41. マイナンバー（個人番号）
        1. 日本国内に住民票を有する全ての方が一人につき1 つ持つ12 桁の番号のこと。
        2. 外国籍でも住民票を有する方には住所地の市町村長から通知される。 マイナンバーは行政を効率化し、 国民の利便性を高め、 公平、 公正な社会を実現するための社会基盤。 その利用範囲は法令等で限定されており、 平成28 年1 月から順次、 社会保障、 税、 災害対策分野の行政手続で利用されている。
    42. 官民ラウンドテーブル
        1. 行政運営上の意見交換や懇談の場のことであり、 官民が我が国の向上・活性化に向けて、 持続的な対話を行っていくことを目的としている。
    43. リカレント教育
        1. 近年の技術革新の著しい進展や産業構造の変化などに対応して学校教育の終了後、 技術系人材を含む職業人を中心とした社会人に対して行われる教育のこと。
    44. レセプトデータ
        1. レセプト（保険医療機関又は保険薬局が保険者に医療費を請求する際に提出する診療報酬明細書や調剤報酬明細書）に記載されているデータのこと。
    45. レピュテーションリスク（風評リスク）
        1. 企業に関する否定的な評価・評判が世間に周知されることで企業の信用やブランド価値等が悪化し、 結果的に損失を被るリスクのこと。
    46. ワンスオンリー
        1. 一度行政機関が提出を受けた情報は、 原則再度の提出を求めない仕組みのこと。
    47. ４Ｋ
        1. 現行のハイビジョンを超える解像度の映像のこと。 水平方向の画素数が約4 千であることから、 4K と呼ばれる。 超高精細度テレビジョン放送に対応する規格として、 平成24 年にITU（国際電気通信連合）で勧告化されるなど、 国際標準化がなされている。 4K は現行ハイビジョンの4 倍の解像度となる。
    48. ５Ｇ
        1. 「超高速」だけでなく、 「多数接続」「超低遅延」といった特徴を持ち、 平成32 年の実現が期待されている次世代の移動通信システムのこと。 我が国においても産学官連携の推進団体である「第５ 世代モバイル推進フォーラム（5GMF）」の設立（平成26 年９月30 日）、 研究開発の推進、 国際連携の強化などの取組が進められている。 現行LTE と比べて100 倍の接続機器数（100 万台/km2）、 100 倍の通信速度（10Gbps）などが要求条件とされており、 ITU をはじめ、 世界各国でも実現に向けた取組が本格化している。
    49. ８Ｋ
        1. 現行のハイビジョンを超える解像度の映像のこと。 水平方向の画素数が約8 千であることから、 8K と呼ばれる。 超高精細度テレビジョン放送に対応する規格として、 平成24 年にITU（国際電気通信連合）で勧告化されるなど、 国際標準化がなされている。 8K は現行ハイビジョンの16 倍の解像度となる。
    50. 人工知能（AI）
        1. Artificial Intelligence（人工知能）の略である。 コンピュータを使って、 学習・推論・判断など人間の知能のはたらきを人工的に実現するための技術。
    51. API
        1. Application Programming Interface の略。 複数のアプリケーション等を接続（連携）するために必要なプログラムを定めた規約のこと。
    52. AR（拡張現実）
        1. Augmented Reality の略である。 現実の環境にコンピュータを用いて情報を付加することにより人工的な現実感を作り出す技術の総称。 情報を付加された環境そのものを示すこともある。
    53. CIO
        1. Chief Information Officer の略である。 日本語では「最高情報責任者」「情報システム担当役員」「情報戦略統括役員」などと訳される。 企業や行政機関等といった組織において情報化戦略を立案、 実行する責任者のこと。
    54. e-ラーニング
        1. パソコンやタブレット、 スマートフォンを使ってオンラインで学ぶ学習形態のこと。
    55. EBPM
        1. Evidence Based Policy Making の略で、 統計や業務データなどの客観的な証拠に基づく政策立案のこと。
    56. Fintech
        1. 金融（Finance）と技術（Technology）を掛け合わせた造語であり、 主に、 ITを活用した革新的な金融サービス事業を指す。
    57. HHI
        1. Herfindahl-Hirschman Index（ハーフィンダール・ハーシュマン指数）の略である。 当該市場における各事業者の有するシェアの二乗和として算出され、 市場集中度を表す指標のこと。
    58. i-Construction
        1. 調査・測量から設計、 施工、 検査、 維持管理・更新までの全ての建設生産プロセスでICT 等を活用して、 建設現場の生産性の向上を目指す。
    59. IoT
        1. Internet of Things（モノのインターネット）の略である。 自動車、 家電、 ロボット、 施設などあらゆるモノがインターネットにつながり、 情報のやり取りをすることで、 モノのデータ化やそれに基づく自動化等が進展し、 新たな付加価値を生み出すというコンセプトを表した語である。
    60. ITS
        1. Intelligent Transport Systems（高度道路交通システム）の略である。 道路交通の安全性、 輸送効率、 快適性の向上等を目的に、 最先端の情報通信技術等を用いて、 人と道路と車両とを一体のシステムとして構築する新しい道路交通システムの総称。
    61. KPI
        1. Key Performance Indicators の略で、 目標の達成度を評価するための主要な評価指標のこと。
    62. Ｌアラート（災害情報共有システム）
        1. 避難勧告・指示等といった、 安心・安全に関わる公的情報など、 住民が必要とする情報が迅速かつ正確に住民に伝えられることを目的とした情報基盤のこと。 全国の情報発信者（地方公共団体等）が発信した情報を、 地域を越えて全国の情報伝達者（メディア等）に一斉に配信できるので、 住民はテレビ、 ラジオ、 携帯電話、 ポータルサイト等の様々なメディアを通じて情報を入手することが可能となる。
    63. MVNO
        1. Mobile Virtual Network Operator の略で仮想移動体通信事業者のこと。
    64. PDS
        1. Personal Data Store の略で、 他者保有データの集約を含め、 個人が自らの意思で自らのデータを蓄積・管理するための仕組み（システム）のこと。 第三者への提供に係る制御機能（移管を含む）を有する。 運用形態としては、 個人が自ら保有する端末等でデータを蓄積・管理する（事業者は本人の同意によりデータを活用できる）分散型と、 事業者が提供するサーバ等でデータを蓄積・管理する（個人は当該事業者にデータの蓄積・管理を委託する）集中型がある。
        2. 実際にデータをやり取りする形態と、 データをやり取りせず必要な時にアクセス権（閲覧のみ可、 コピー不可など）を提供・管理する形態もある。
    65. PHR
        1. Personal Health Record の略である。 個人が自らの生活の質(QOL=Quality of Life)の維持や向上等を目的として、 自らの健康に関する情報を収集・保存・活用する仕組みのこと。
    66. SNS
        1. Social Networking Service(Site)の略である。 個人間の交流を支援するサービス（サイト）で、 参加者は共通の興味、 知人などをもとに様々な交流を図ることができる。
    67. Society5.0
        1. 狩猟社会、 農耕社会、 工業社会、 情報社会に続くような新たな社会を生み出す変革を科学技術イノベーションが先導していく、 という概念である。
    68. VR
        1. Virtual Reality の略である。 コンピュータ上に仮想的な世界を作り出し、 あたかも現実にそこにいるかの様な体験をさせる技術。 \_\_
  1. 概要

ドキュメントを参照: [ITsengen\_gaiyou.pdf](https://cio.go.jp/sites/default/files/uploads/documents/ITsengen_gaiyou.pdf)

1. 「政府情報システムの整備及び管理に関する標準ガイドライン」(2015年3月19日更新、 2014年12月3日各府省CIO連絡会議決定）および「実務手引書」

ドキュメントを参照: [infosystem-guide.html](http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/infosystem-guide.html)

* 1. http://www.soumu.go.jp/main\_sosiki/gyoukan/kanri/infosystem-guide.html

ドキュメントを参照: [infosystem-guide.html](http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/infosystem-guide.html)

* 1. 世界最先端IT国家創造宣言(2013年6月14日閣議決定。 2014年6月24日変更)に基づき、 政府におけるITガバナンス強化のため、 情報システム調達やプロジェクト管理に関する共通ルールとして策定

1. 人材育成・人材確保
   1. IT人材白書2017【2017年4月25日IPA】

ドキュメントを参照: [about.html](https://www.ipa.go.jp/jinzai/jigyou/about.html)

* + 1. デジタル大変革時代、 本番へ
       1. 時代環境が大きく変わる時、 それにそぐわないビジネスは淘汰されていく
       2. デジタル変革とも呼ぶべき第4次産業革命の入り口にいる
       3. デジタル時代にふさわしい新たなビジネスを生み出して行く必要がある
          1. 旧来の仕組みの高度化、 洗練は否定されるべきではないが
       4. デジタルトランスフォーメーション が重要
          1. 仕事の進め方や社会のあり方をゼロベースで刷新し、 時代に適合するように自らを変える
       5. それに歩みを進めるかどうか、 つまり企業の方向性を決めるのは、 言うまでもなく経営者
          1. 経営者の役割： 時代の潮流を捉え、 自社が変化の中で発展できる道を探り、 ビジョンをはっきりと示す
       6. 同時に従来から続く組織構造の破壊や再構築も必要
          1. 求められるのは、 周囲を巻き込みながら改革を進める能力やビジネスとデジタルを結び付けて全体をデザインする能力を持った新しい時代のリーダー
          2. ITエンジニアがリーダーへと成長するには挑戦する意欲を持つ
          3. さまざまな経験を積み、 多様な人と関わる環境が必要
       7. 企業が行わなければならないのは、 誰もが挑戦できる環境、 開かれた場を作ること
       8. 個々のIT人材は、 自らも デジタルトランスフォーメーション の流れの中にあることを意識
          1. その中で活躍できる人材となれるように、 自らの能力を高めていくことが重要である
          2. そのためには情報への感度を高め、 自ら挑戦する場を求める姿勢が重要になる。 普段の仕事に専念しているだけでは不十分と考えなければならない。
    2. 企業に向けたメッセージ
       1. IT企業
          1. デジタル変革が進む中では、 IT企業は デジタルトランスフォーメーション に資する技術力や提案力を磨き、 ユーザー企業のパートナーとして新たな事業価値を生み出していく役割を担う必要がある。
          2. そのためにはユーザー企業やベンチャー企業などとの「協働」関係を築くことも欠かせない。
       2. ユーザー企業（IT部門）
          1. デジタルトランスフォーメーション を推進するのか、 それとも現状維持を選択するのか。

第4次産業革命が進むにつれて、 発展するビジネスと縮小するビジネスが明確になっていく。

* + - * 1. CIOやIT部門は、 そのことを認識し、 変化を主導する側に立つ必要がある。

そのために一刻も早く現状把握を行い、 ビジョンを明確にし、 戦略を遂行しなければならない。

* + - * 1. デジタルトランスフォーメーション を実現するには、 ビジネスとデジタルのスキルを併せ持った人材が重要となる。

それがあって初めて、 イノベーティブなデジタル技術を持つ企業や、 他業種など多様な企業間での連携を進められる

その視点に立って、 人材の育成と獲得をしていく必要がある。

* + - * 1. 従来、 社内でIT業務の中核を担ってきたIT部門は今、 再び挑戦を迫られている。

デジタル変革に伴って生じる新たな事業や業務において重要な役割を担うことへの挑戦でもある。

* + 1. IT人材個人に向けたメッセージ
       1. デジタル時代は、 個々のIT人材にとって活躍の場を広げられるまたとないチャンスである。
       2. 所属する企業で新たな試みをすることもできるし、 起業のチャンスも開けている。
       3. クラウドコンピューティングやモバイルの進展で、 個人や少数のチームでできることが飛躍的に拡大している
       4. このことを認識し、 目の前の業務だけにとらわれることなく、 広く視野を持って進むべき道を探り、 学ぼう。 勉強会やコミュニティなど、 学びの場は周囲にある。 自己研鑽によって能力を高めれば高めただけ、 社会をリードする人材になっていく。
    2. 1．デジタルトランスフォーメーション時代のIT人材
       1. デジタルトランスフォーメーション とは何か
          1. ITの進展やインフラの整備によって、 ビジネスや社会のあり方が変わり始めている。

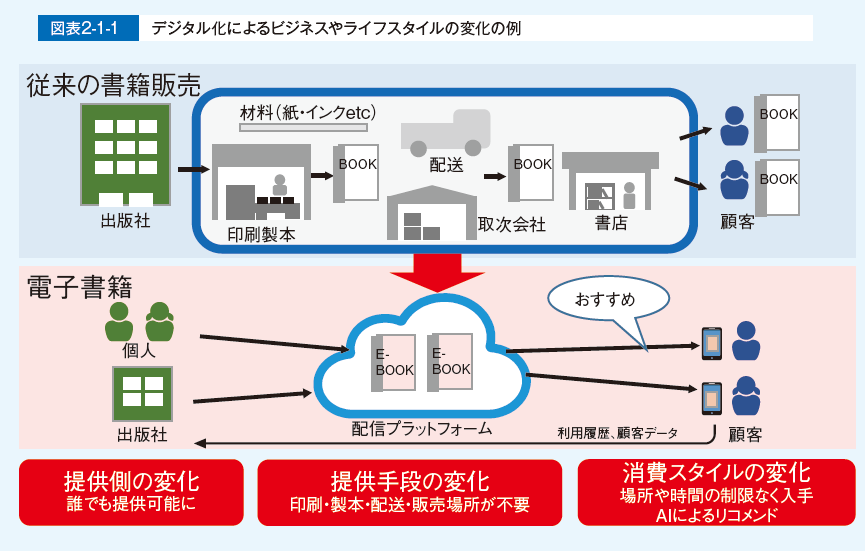
あらゆるものがインターネットに接続するIoTの拡がりや、 ビッグデータ活用、 人工知能（AI）の様々な分野への適応が始まっている。

デジタル化を進めるということは、 様々な要素（アナログデータも含む）をデジタル化、 数値化して扱うことを意味する。

共通に扱えるデータへと変換することによって、 処理や分析が可能になり、 フィードバックまで含めた一連の流れを作ることが可能になる。

デジタル化の本質は、 以上のようなデータ駆動型へのビジネスや社会の変革にある。

既存のビジネスや業務に新技術を取り入れるだけでなく、 ビジネスモデルを変え、 経済活動のみならず、 個人の生活や社会構造にまで影響が及ぶ。

* + - * 1. その変化は、 デジタルトランスフォーメーション や デジタル革命 と呼ばれている。
        2. サブトピック  
           
        3. デジタル化によって起こる変化の一例として、 紙の書籍から電子書籍へのデジタル化を図式化したものである。
      1. すでに始まっている デジタルトランスフォーメーション
         1. 「IoTやビッグデータ、 AIなど技術の進展等によって、 社会や産業、 企業、 人のあり方や働き方が大きく変化すると言われている。 この変化に対してどのように捉えているか」
         2. ネットサービス実施企業は

、 「すでに変化の中にいる」が約40%である。 インターネットを活用し、 データを扱うビジネスを実施しているという性質上、 変化に対して敏感だと言える。

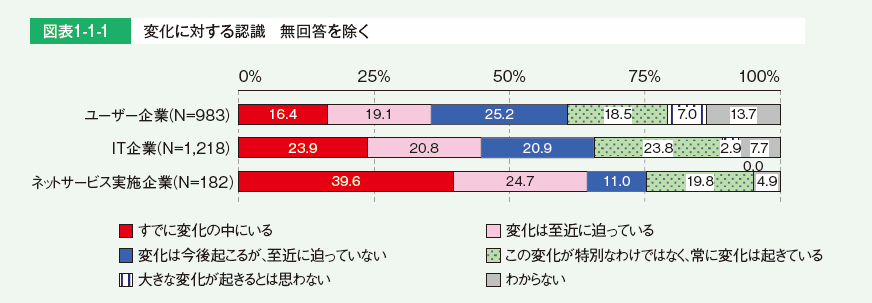
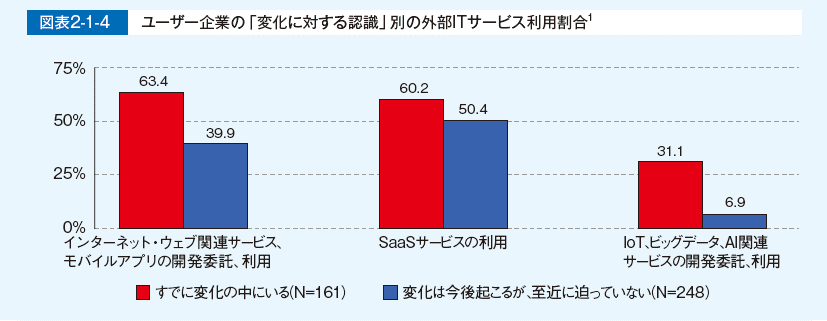
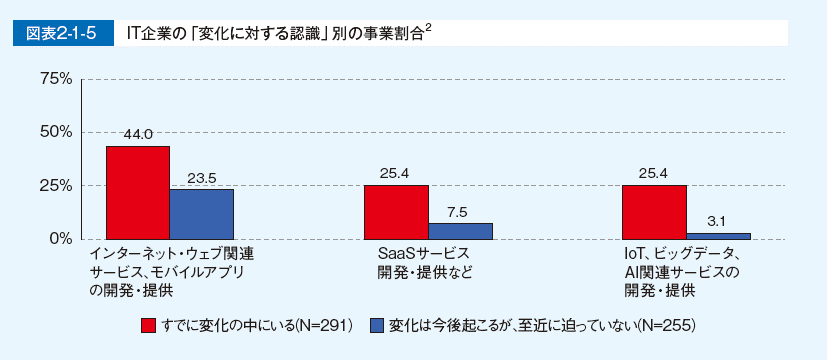
* + - * 1. 事業会社であるユーザー企業では

「変化は今後起こるが、 至近に迫っていない」という回答の割合が最も高い。

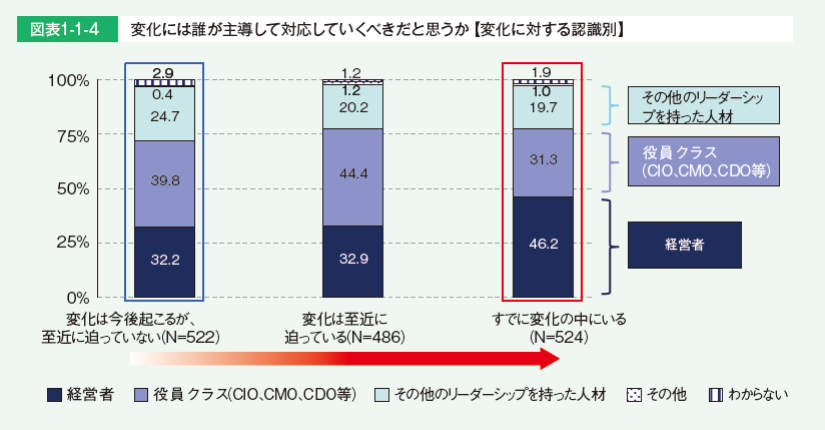
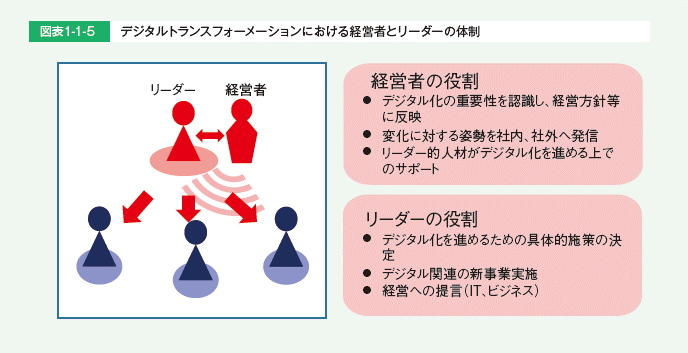
「大きな変化が起きるとは思わない」や「わからない」も他の企業区分に比較して高い割合を占めている。

* + - * 1. 一方、 IT企業では、

「すでに変化の中にいる」、 「変化は至近に迫っている」、 「変化は今後起こるが、 至近に迫っていない」、 「この変化が特別なわけではなく、 常に変化は起きている」の回答割合がほぼ同率だった。

* + - * 1. サブトピック  
           
      1. 外部ITサービス利用状況、 現在の事業【変化に対する認識別】
         1. サブトピック  
            
         2. サブトピック  
            
      2. デジタルトランスフォーメーション が進む企業では、 経営者による主導の重要性を認識
         1. デジタルトランスフォーメーションには、 大きな変化が伴うため、 業務の部分的なデジタル対応やIT導入による効率化のみでは対応できない。
         2. 変化 には誰が主導して対応していくべきか尋ねた。

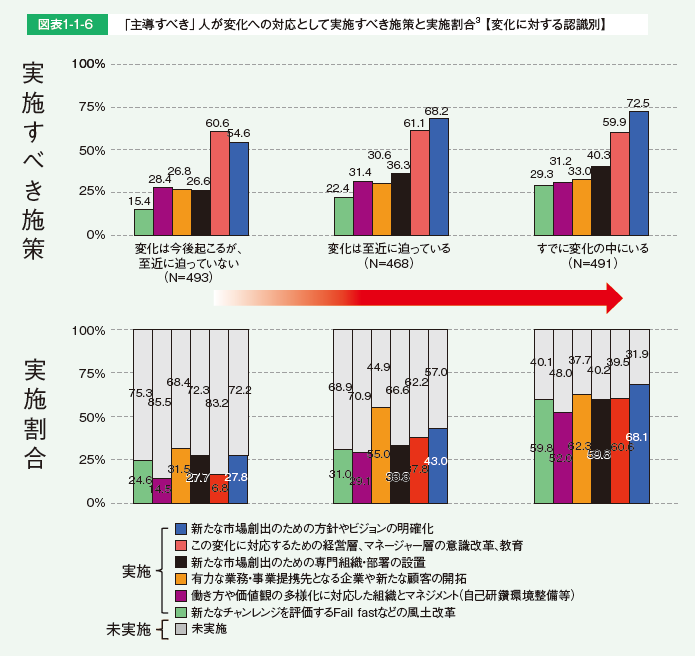
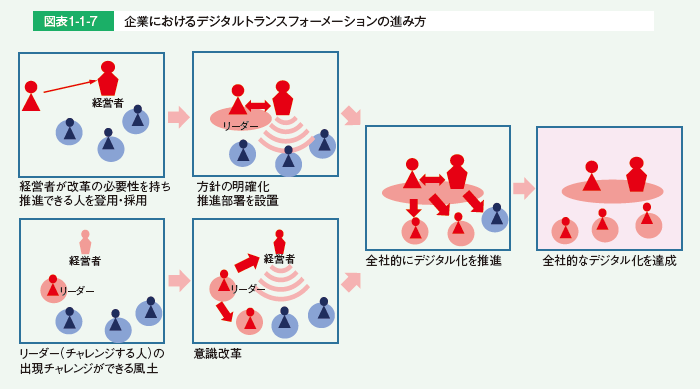
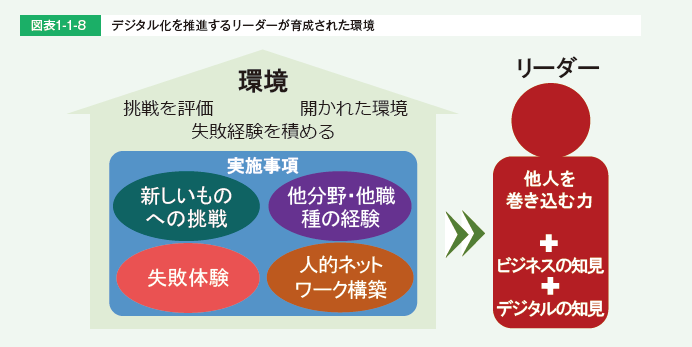
「すでに変化の中にいる」企業では、 他の認識の企業に比べて「経営者」が主導していくべきだという回答の割合が高い。

* + - * 1. サブトピック  
           
      1. デジタルトランスフォーメーション の鍵を握るリーダー的人材
         1. 全体方針を示す経営者に加え、 具体的な推進を行う人材も存在している。
         2. デジタル化の具体的な施策の決定や新事業の立ち上げなどを主導する、 リーダー的な役割を担う人材が大きな役割を果たしている。
         3. この人材は、 例えばCIOや、 デジタル推進部門、 デジタル技術を用いた新事業部門、 IT系部門などに存在し、 それぞれのデジタル化を推進している。
         4. サブトピック  
            
      2. 方針やビジョンの明確化」、 「専門組織・部署の設置」、 「Fail fastなどの風土改革」を重要視
         1. デジタル化を「主導すべき」人が実施すべき施策

「新たな市場創出のための方針やビジョンの明確化」

「新たな市場創出のための専門組織・部署の設置」

「新たなチャレンジを評価するFail fastなどの風土改革」

* + - * 1. サブトピック  
           
      1. 経営者とリーダーが周囲を巻き込み、 改革を進める
         1. リーダー的存在が企業内の複数個所に存在する場合もあるが、 経営者と現場に近いリーダーとがともに改革を進めていく大きな流れは変わらない。
         2. サブトピック  
            
      2. デジタル化の推進をリードする人材に必要な能力と環境
         1. ・デジタル化を推進するリーダーに求められるのは、 他人を巻き込む力 、 ビジネスとデジタルの知見
         2. ・デジタル化を推進するリーダーが育ってきた背景は、 多様な経験と新しいものへの挑戦 、 ネットワーク、 外部とのつながり
         3. ・デジタル化を推進するリーダーの育成に重要となる環境の整備
         4. サブトピック  
            
      3. デジタル化に携わる人材
         1. 必要な能力

もともと製品の社内開発・運用を行ってきた企業の場合、

社内に既存の技術力はあり、 加えて具体的な技術（データ解析やAI、 クラウド等）が求められている。

また、 具体的な要素技術だけでなく、 システムの構造設計を行い開発する能力（システムアーキテクト）の重要についても挙げられていた。

一方、 これまでITが深くかかわっていなかった事業がデジタル化した場合、

今までIT部門が行っていた外部企業への開発委託を事業部門が直接行うことになり、 ITを事業に適用する能力や、 機能設計や要件定義を行う能力が求められる。

* + - * 1. 人材の獲得方法と育成

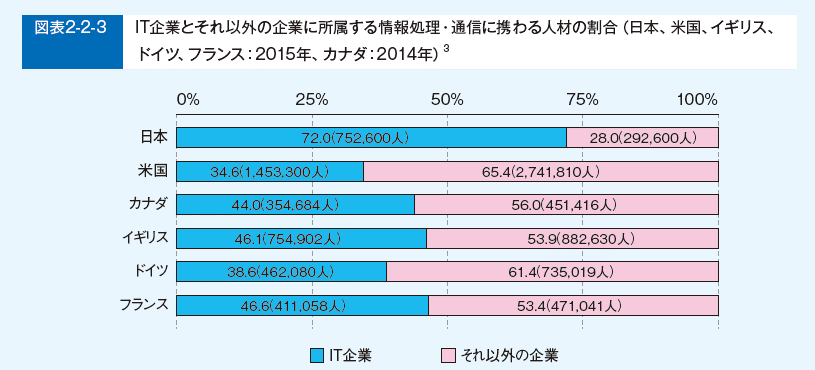
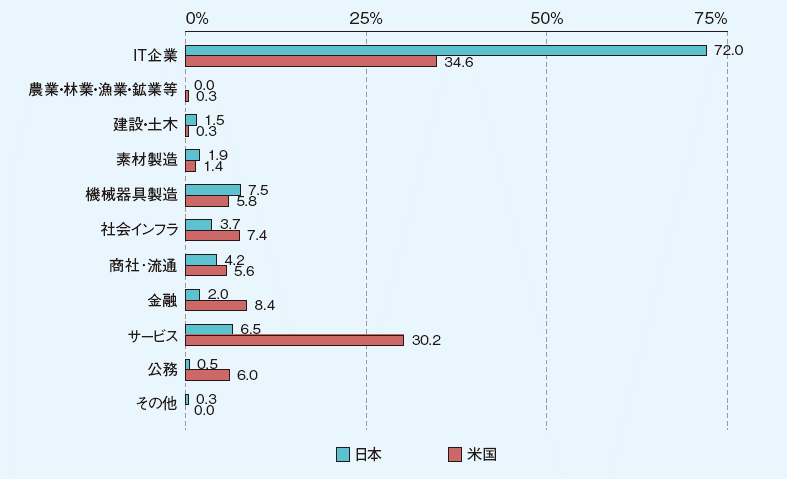
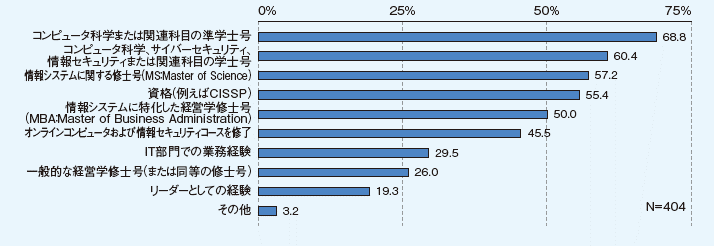
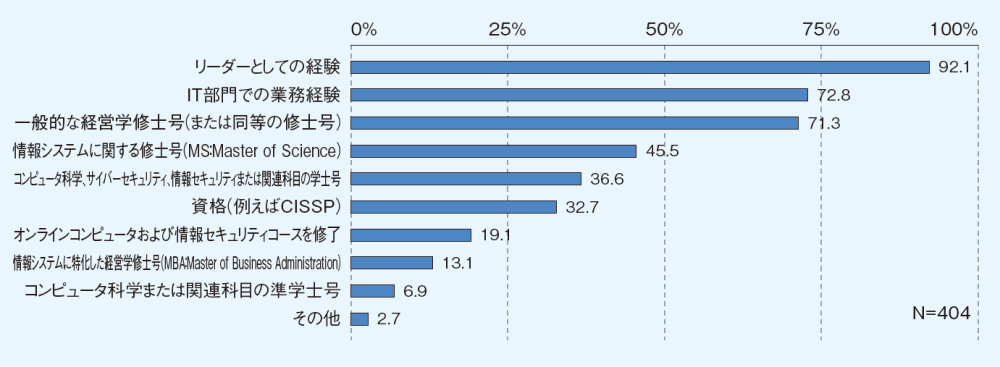
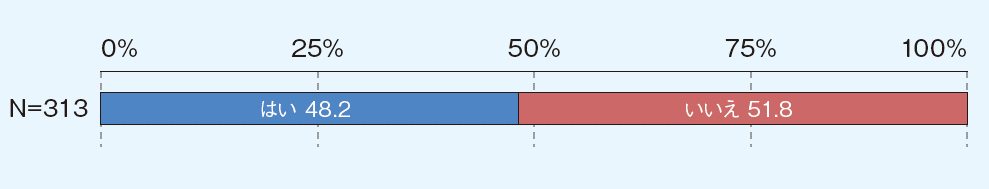
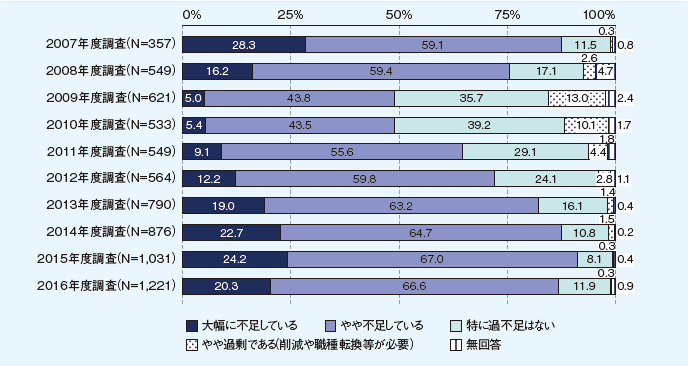
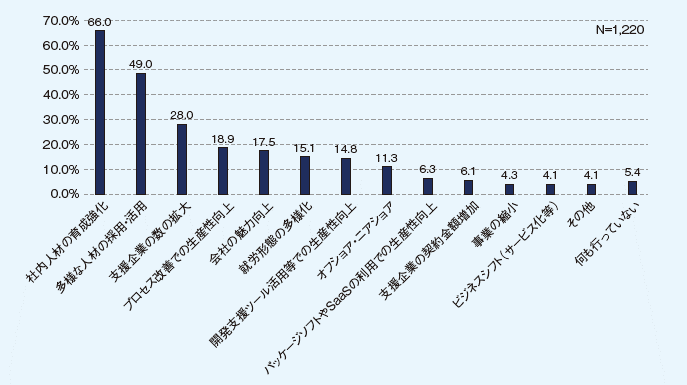
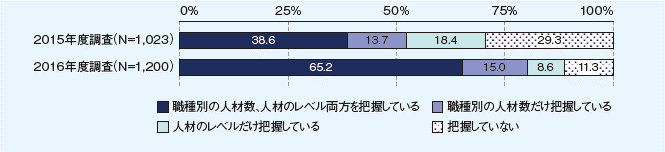
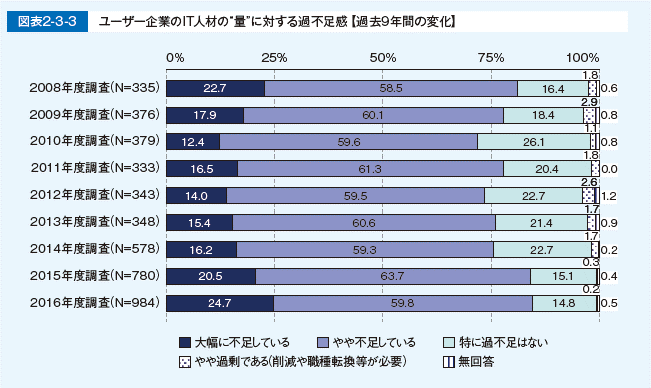
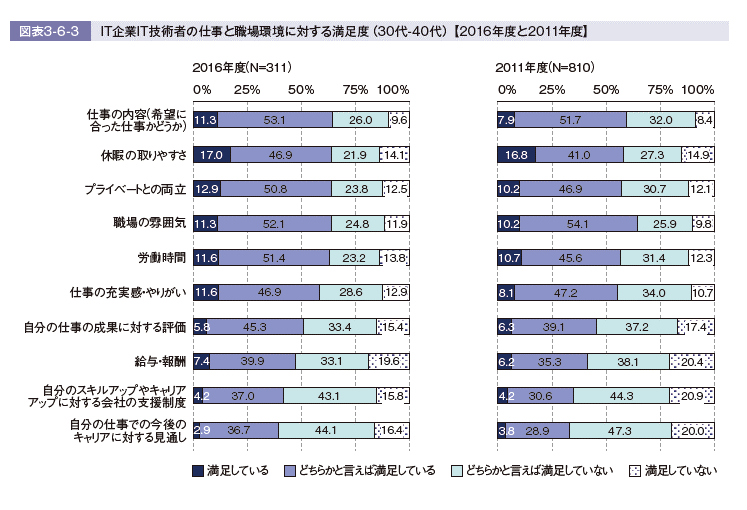
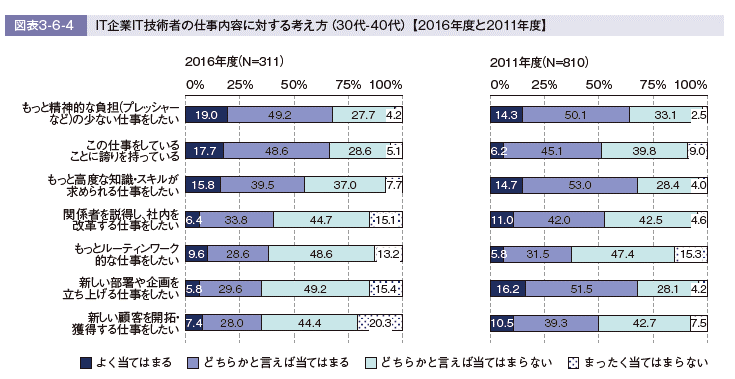
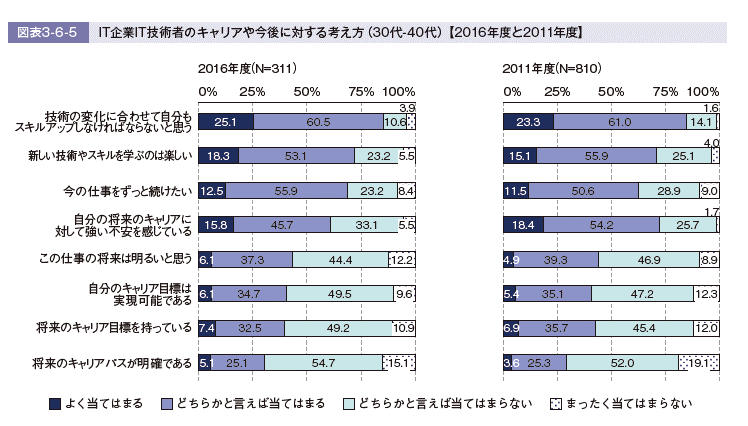
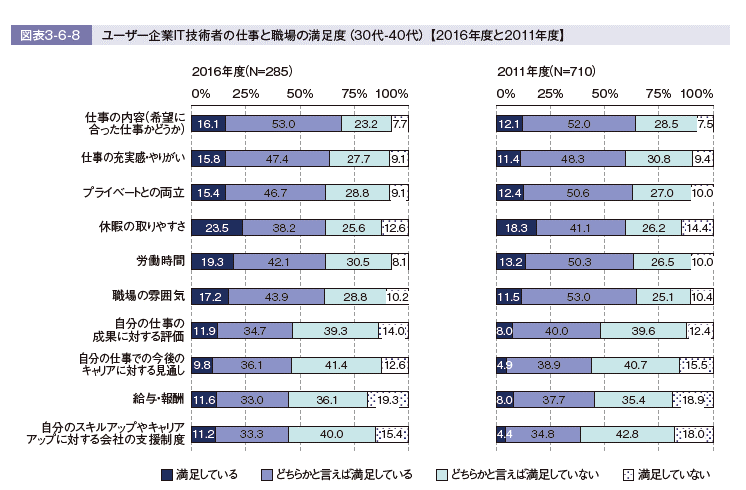
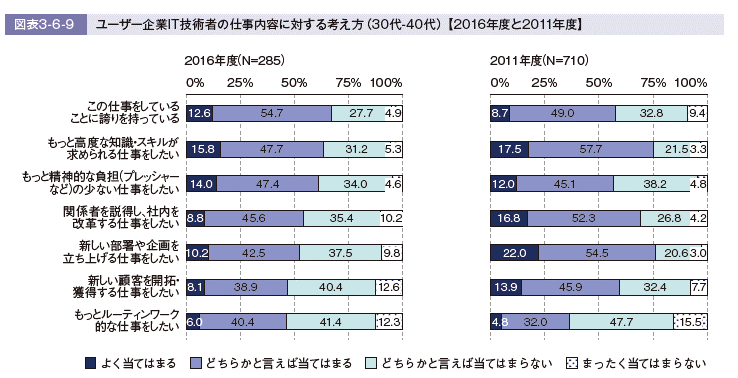
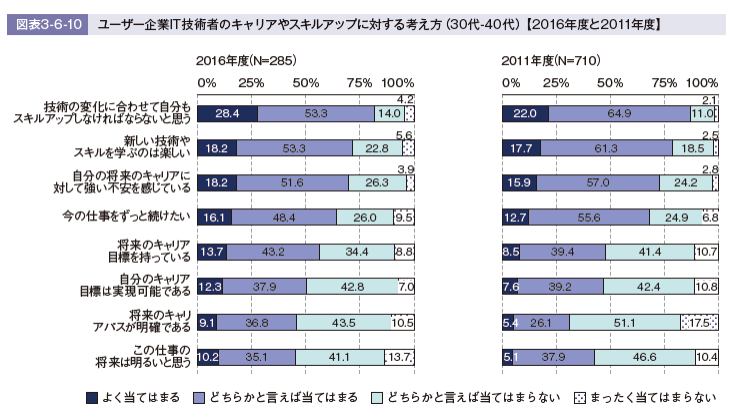
事業のデジタル化に必要なIT能力を、 既存の人材でまかなうのは難しいとの意見があった。

デジタル化した事業を行っている企業では、 ネット系の企業等でデジタルビジネスの経験がある者を中途採用し、 事業の推進を行っている例が見られる。

また、 新しい技術（データ活用やAI、 IoTなど）を持った人材に関しては、 中途採用の難しさを挙げる企業が多く、 新卒採用した人材を育成して人材確保する傾向が見られ、 新卒を採用する際に理数系人材を重視する企業もいくつかあった。

育成のスピードアップと高い技術力を持った人材の輩出につなげたい考えである。

ただし、 内部人材育成の難しさを挙げる企業もあり、 必要な技術を持った人材を中途採用できる場合は行い、 できない場合はアウトソーシングや、 外部との連携を行うことで技術を補完する場合もあった。

* + 1. 2．日本と米国の情報処理・通信に携わる人材
       1. 日米、 欧州等の情報処理・通信に携わる人材の所属企業
          1. 日本はIT企業に所属する情報処理・通信に携わる人材の割合が72%と突出して高くなっている。
          2. 一方、 日本以外の国は、 IT企業以外の割合が5割を超えており、 米国はIT企業以外に所属する情報処理・通信に携わる人材の割合が65.4%と最も高くなっている。
          3. サブトピック  
             
       2. 日米の情報処理・通信に携わる人材の業種別人材の割合
          1. 米国では、 「IT企業」に次いで「サービス」の割合が30.2%と高くなっている。
          2. 「金融」については日本の2%に対し米国では8.4%、 「公務」については日本の0.5%に対し米国が6%と、 日本より幅広い業種に情報処理・通信に携わる人材が所属していることがわかる。
          3. サブトピック  
             
       3. 米国における情報セキュリティ技術者に必要なスキルや経験
          1. 「コンピュータ科学または関連科目の準学士号」の割合が68.8%と最も高く、 「コンピュータ科学、 サイバーセキュリティ、 情報セキュリティまたは関連科目の学士号」（60.4%）、 「情報システムに関する修士号（MS（Master of Science））」（57.2%）と続き、 学歴を重視する傾向が見られる。
          2. 「資格（例えばCISSP）」が55.4%と、 資格への関心も高い。
          3. サブトピック  
             
       4. 米国の組織のCISOに必要なスキルや経験
          1. 「リーダーとしての経験」の割合が92.1%と最も高く、 「IT部門での業務経験」（72.8%）、 「一般的な経営学修士号（または同等の修士号）」（71.3%）と続いている。
          2. 情報セキュリティ技術者にとって必要なスキルや経験の調査結果とは違い、 経験を重視する傾向が見られる。
          3. サブトピック  
             
       5. 米国の組織におけるサイバーセキュリティ：トレーニングプログラム開発のための大学との連携・協業状況
          1. 約5割もの組織がサイバーセキュリティトレーニングプログラムの開発のために大学と連携・協業していることがわかる。
          2. サブトピック  
             
    2. 3．IT人材不足の動き
       1. IT人材の 量 に対する過不足感【過去10年の変化】
          1. IT企業では、 リーマンショック以来高まり続けていたIT人材の 量 に対する不足感の高まりがやや緩和した。
          2. 「大幅に不足している」と答えた割合が、 2015年度調査の24.2%から、 今年度では20.3%と減少している。
          3. また、 「特に過不足はない」は2015年度調査の8.1%から、 今年度では11.9%と増加している。
          4. サブトピック  
             
       2. 人材不足改善の取り組みのうち効果があったもの
          1. 「社内人材の育成強化」が最も多く、 66％に上っている。
          2. サブトピック  
             
       3. IT人材の「職種別の人材数」と「人材のレベル」の把握状況【経年】
          1. 計画的な人材育成には人材把握が必要となるが、 今年度調査では、 「職種別の人材数、 人材のレベル両方を把握している」割合が大きく増加していた。
          2. サブトピック  
             
       4. IT人材の 量 に対する過不足感【過去9年の変化】
          1. 2010年ごろに不足感が減少した以降、 2014年度調査までは不足感に大きな変化のなかったユーザー企業だが、 2015年度調査の結果ではIT人材の 量 について、 「大幅に不足している」「やや不足している」と回答した割合が増加した。
          2. 今年度も引き続き不足感が増す傾向にある。
          3. サブトピック  
             
    3. 4．IT人材動向（IT人材の意識の比較【2016年度と2011年度】）
       1. 仕事や職場の環境に対する満足度（30代-40代）【2016年度と2011年度】
          1. 2016年度、 2011年度共に「仕事内容（希望に合った仕事かどうか）」、 「休暇の取りやすさ」、 「プライベートとの両立」「職場の雰囲気」に対する満足度は高い。
          2. 全項目に対して微増微少はあるが、 変化は読み取れない。
          3. サブトピック  
             
       2. 仕事内容に対する考え方（30代-40代）【2016年度と2011年度】
          1. 「この仕事をしていることに誇りを持っている」では、 「よく当てはまる、 どちらかと言えば当てはまる」では2011年度の51.3％から2016年度の66.3％と増加した。
          2. 一方、 「新しい部署や企画を立ち上げる仕事をしたい」では「よく当てはまる、 どちらかと言えは当てはまる」の合計が、 2011年度の67.7％から2016年度の35.4％、 「関係者を説得し、 社内改革する仕事をしたい」も同様に2011年度53％から2016年度の40.2％と割合が低下している。
          3. サブトピック  
             
       3. キャリアやスキルアップに対する考え方（30代-40代）2016年度と2011年度】
          1. 2016年度、 2011年度共に「技術の変化に合わせて自分もスキルアップしなければならないと思う」について「よく当てはまる、 どちらかと言えは当てはまる」と回答した割合は8割台半ばであり、 「新しい技術やスキルを学ぶのは楽しい」の割合も共に7割強である。
          2. 一方、 「将来のキャリアパスが明確である」で「よく当てはまる、 どちらかと言えは当てはまる」と回答した割合は2011年度と2016年度共に約3割であり傾向に変化はない。
          3. サブトピック  
             
       4. 仕事と職場環境に対する満足度（30代-40代）【2016年度と2011年度】
          1. 全項目において「満足している」の割合が増加している。
          2. サブトピック  
             
       5. 仕事内容に対する考え方（30代-40代）【2016年度と2011年度】
          1. 「この仕事をしていることに誇りを持っている」では「当てはまる、 どちらかと言えは当てはまる」を合計した割合が2011年度の57.7％から2016年度の67.3％と増加している。
          2. 一方、 「新しい部署や企画を立ち上げる仕事をしたい」では「当てはまる、 どちらかと言えは当てはまる」の合計は、 2011年度の76.5％から2016年度の52.7％へと23.8ポイント低下した。
          3. また、 「新しい顧客を開拓・獲得する仕事をしたい」の割合も2011年度の59.8％から2016年度の47％へと低下している。
          4. サブトピック  
             
       6. キャリアやスキルアップに対する考え方（30代-40代）2016年度と2011年度】
          1. 「将来のキャリアパスが明確である」では「当てはまる、 どちらかと言えは当てはまる」を合計した割合が2011年度の31.5％から2016年度の45.9と増加し、 「将来のキャリア目標を持っている」、 「自分のキャリア目標は実現可能である」のいずれにおいても割合が増加している。
          2. しかしその一方で、 「自分の将来のキャリアに対して強い不安を感じている」に対する「よく当てはまる」の割合はやや増加しており、 キャリアは明確なったものの、 不安感は弱まってはいないように見受けられる。
          3. サブトピック  
             
  1. 情報技術者試験

ドキュメントを参照: [www.jitec.ipa.go.jp](https://www.jitec.ipa.go.jp/)

* 1. iコンピテンシディクショナリ

ドキュメントを参照: [i\_competency\_dictionary](https://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/)

1. 人材育成・人材確保【セキュリティ関連】
   1. ■ITのスキル指標を活用した情報セキュリティ人材育成ガイド【2015年5月IPA】

ドキュメントを参照: [000039528.pdf](http://www.ipa.go.jp/files/000039528.pdf)

* + 1. あなたの企業に迫る脅威～ あなたの企業は大丈夫ですか？
    2. ＜脅威１＞ 標的型攻撃・サイバー攻撃
       1. 必要な対策は実施されていますか？
          1. ウィルス対策ソフトを社内のすべてのコンピュータに導入し、 ウィルスチェックやウィルス対策ソフトの更新を頻繁に実施していますか。
          2. 社内のメール利用者に対して、 「怪しいメールは開封しない」、 「疑わしいメールのＵＲＬはクリックしない」、 「不審な添付ファイルは開かない」などの基本事項についての教育が徹底されていますか。
          3. ウィルス対策ソフトから「ウィルスに感染した」という警告メッセージが表示された場合、 まず何をすればよいか、 すべての従業員が十分に理解していますか。
          4. 標的型攻撃を防御・検知するためのシステムの監視を行っていますか。 また、 そのような機能をもったセキュリティ対策ソフトを導入していますか。
          5. ウィルス感染や情報漏えいが発覚した場合の組織としての緊急対応手順は定められていますか。 また、 その手順は関係者に周知されていますか。
       2. あなたの企業は 大丈夫？被害を防ぐためには、 こんな役割も重要です！
          1. システム運用において、 セキュリティ障害管理 （事故の検知、 初動対応、 分析、 復旧等）のタスクを実行する役割
       3. その役割を担う人材の例
          1. セキュリティ アドミニストレータ （インシデントハンドラ）

自社内のセキュリティインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧業務の実施において、 自らあるいは適切な対応者をアサインして対応にあたる役割。 被害の拡大防止のために、 適切かつ迅速な対応が求められる。

* + - * 1. ITサービスマネジメント（システム管理）

顧客の情報システムの日々の運用業務やシステム基盤の管理業務を担い、 円滑な運用を実現する役割。 運用時にセキュリティインシデントをモニタリングし、 インシデントが発生した場合には、 被害拡大防止等の初動対応を担う。

サブトピック

* + 1. ＜脅威２＞ 不正アクセス
       1. 必要な対策は実施されていますか？
          1. 123456, admin, password などの単語を避けることは当然ながら、 意味のある単語にしない、 最低８文字以上にする、 定期的に変更するなど、 パスワードに関する基本的なルールが社内で徹底されていますか。
          2. 自分の席を離れる際は、 パスワードで保護されたスクリーンセーバーでパソコンを保護することをルール化していますか。
          3. 退職した従業員の ID など、 不要な ID を放置せず、 きちんと削除していますか。
          4. ユーザーごとにアクセス権を設定し、 定期的な見直しや管理を行っていますか。
          5. 企業内のネットワークやコンピュータに、 ファイアウォールなどの外部からの不正アクセスを検知・遮断する仕組みを導入していますか。
          6. 自社が提供しているサービスについて、 不正アクセス対策を実施していますか。 （例：不正アクセス対策 http://www.ipa.go.jp/security/fusei/ciadr.html）
       2. 被害を防ぐためには、 こんな役割も重要です
          1. システム運用において、 セキュリティ管理のタスクを実行する役割
       3. その役割を担う人材の例
          1. セキュリティ アドミニストレータ （ＩＳセキュリティアドミニストレータ）

自社の情報セキュリティ対策の具体化や実施を統括する役割。 企業全体としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込み、 対策の立案や実施（指示・統括）、 その見直しなどを行う。 また、 利用者に対する教育等も実施する。

* + - * 1. ITサービスマネジメント（運用管理）

顧客の情報システムの運用管理の責任者として、 ITサービスマネジメントの統括責任を担う。 セキュリティの面では、 運用するシステムのセキュリティマネジメントに関する方針や計画を策定し、 具体的な対策の実施を統括する。

* + 1. ＜脅威３＞ エクスプイト
       1. 必要な対策は実施されていますか？
          1. 社内のコンピュータ上で利用しているソフトウェアの修正プグラム（セキュリティパッチ）が公表されたら迅速に適用していますか。 セキュリティパッチが適用されずに長期間そのまま利用されているコンピュータはありませんか。
          2. セキュリティパッチの適用状況をきちんと把握していますか。 また、 それを把握し、 管理する担当者は決められていますか。
          3. 情報システムを設計・開発する際に、 セキュリティに関する仕様や基準、 要求事項などを明確にしていますか。
          4. 開発した情報システムのテストを行う際に、 外部からの攻撃などを意識したセキュリティに関するテストも実施していますか。
          5. 現在運用している自社のWEBシステムに脆弱性がないか、 検査を行ったことはありますか。
       2. 被害を防ぐためには、 こんな役割も重要です！
          1. システム開発・構築において、 システム設計における セキュリティ面の検討や決定などのタスクを実行する役割
       3. その役割を担う人材の例
          1. システムテザイナー

自社で用いるシステムの要件定義から、 システム基盤（インフラストラクチャ）の分析・設計及び構築を担う役割。 ネットワークの構成やアプリケーション基盤の設計の際に、 セキュリティを考慮した設計を行う。

* + - * 1. ITスペシャリスト（セキュリティ）

情報システムの設計・開発・運用において、 情報セキュリティに関する高い専門性を発揮するスペシャリスト。

セキュリティインシデントが発生した際は、 高度な技術的スキルを駆使して原因の究明や復旧対応等も担う。

* + 1. ＜脅威４＞ クラウド利用におけるデータ消失・流出
       1. 必要な対策は実施されていますか？
          1. 外部のクラウドサービスを利用する際のリスク（データの消失・流出や改ざんなど）について認識していますか。
       2. 情報セキュリティ強化対応スキル指標のご紹介
          1. 自社のどのような情報がクラウドサービス上にあるか、 把握していますか。
       3. 情報セキュリティを担う人材育成のヒント
          1. クラウドサービスの利用・管理に関する責任者や実務担当者を決めていますか。
       4. 組織において求められる情報セキュリティ対策
          1. クラウドサービスを提供する事業者が実施しているセキュリティ対策の具体的な内容や水準を把握していますか。
          2. クラウドサービスを利用する際の ID やパスワードは、 適切に管理していますか。 特に「なりすまし」を防ぐために、 推測されにくいものになっていますか。
          3. クラウドサービスの停止時や障害発生時に、 情報が手元で（自社内で）利用できるような対策が取られていますか。
       5. 被害を防ぐためには、 こんな役割も重要です！
          1. ITシステム企画において、 システム化計画の具体化 （要件定義、 アーキテクチャの設計等）のタスクを実行する役割
       6. その役割を担う人材の例
          1. ＩＳアーキテクト

自社内の情報システム基盤の構築・維持・管理を主に担う役割。 自社のIT戦略に基づき、 自社システムのアーキテクチャ設計を行うほか、 基盤の整備や品質統制のための取り組みなども行う。

* + - * 1. ITアーキテクト（セキュリティアーキテクチャ）

強固なセキュリティ対策が求められる情報システムのアーキテクチャの設計を担う役割。 システムの企画・開発・構築・運用の各工程において、 情報セキュリティ対策が十分に機能し、 維持されることを担保する組織設計、 ルール設計、 プセス設計もあわせて行う。

* + 1. ＜脅威５＞ スマートデバイスからの情報漏えい
       1. 必要な対策は実施されていますか？
          1. 紛失・盗難対策として、 スマートフォンなどのモバイル機器の利用時に、 パスワード入力しなければ使えない「パスワードック」を設定していますか。
          2. ウィルス対策として、 スマートフォンなどのモバイル機器のOSを、 常に最新のバージョンにアップデートしていますか。
          3. スマートフォンのアプリは、 メーカーやキャリアのアプリケーション・ストアなど、 信頼できる場所からインストールしていますか。
          4. 業務で利用するスマートフォンなどのモバイル機器に、 業務とは関係のないアプリが数多くインストールされていませんか。
          5. 私用のモバイル機器を業務上で利用することは、 現状ではあまり推奨されませんが、 利用可とする場合は、 モバイル機器用のセキュリティソフトを導入するなど、 適切なセキュリティ対策を利用者に義務付けていますか。
       2. 被害を防ぐためには、 こんな役割も重要です
          1. 事業戦略、 経営戦略の中で情報セキュリティ戦略の策定のタスクを実行する役割
       3. その役割を担う人材の例
          1. セキュリティアドミニストレータ（情報セキュリティアドミニストレータ）

自社の情報セキュリティ戦略やポリシーの策定等を推進する役割。 戦略策定のほか、 戦略実行体制の確立や開発組織の統括も担う。 また、 企業内のセキュリティ業務全体を俯瞰し、 アウトソース等のリソース配分の判断・決定も行う。

* + - * 1. コンサルタント（情報リスクマネジメント）

ビジネス機能内で情報マネジメントが適切に実現される土台としての組織体制の整備や組織内の各種ルール整備等に関する支援を担う役割。 組織ガバナンスやリスクマネジメント、 コンプライアンス等に関する領域において、 ITソリューションを前提としたコンサルティングを行う。

* + 1. ＜脅威６＞ 内部不正・うっかりミス
       1. 必要な対策は実施されていますか？
          1. 一時的な従業員も含め、 重要な情報を扱う作業は、 管理監督者の目の届くところで行われていますか。 単独で重要な情報にアクセスしている従業員はいませんか。
          2. 社員の管理・監督権限に応じて、 適切なアクセス権限を設定していますか。 多くの従業員が、 管理者アカウントを自由に利用できるような設定になっていませんか。
          3. 重要な顧客情報などを保存しているコンピュータは、 管理者の目の届くところに置く、 別室に置いて入退室記録をつける、 部屋に鍵をかけるなどの対策を行っていますか。
          4. 個人情報などの機密情報については、 保存されているファイルにもパスワードを設定するなど、 二重三重の対策を工夫していますか。
          5. 重要な情報が保存されているコンピュータでは、 アクセスグを記録していますか。
          6. 重要な情報については、 担当者を決めて定期的にバックアップを取っていますか。
       2. 被害を防ぐためには、 こんな役割も重要です！
          1. 情報セキュリティマネジメントにおいて、 セキュリティ方針の策定、 セキュリティ基準の策定のタスクを実行する役割
       3. その役割を担う人材の例
          1. セキュリティアドミニストレータ（ＩＳｾｷｭﾘﾃｨｱﾄﾞﾐﾆｽﾄﾚｰﾀ）

情報セキュリティ戦略やポリシーを具体的なルールや計画に落とし込み、 その実行（ないしは実行の指示）のほか、 維持・管理や見直しを行う役割。 また、 インシデント対応に備えて日頃のマネジメントや教育等の実施も担当する。

* + - * 1. コンサルタント（情報リスクマネジメント）

ビジネス機能内で情報マネジメントが適切に実現される土台としての組織体制の整備や組織内の各種ルール整備等に関する支援を担う役割。 組織ガバナンスやリスクマネジメント、 コンプライアンス等に関する領域において、 ITソリューションを前提としたコンサルティングを行う。

* + 1. 情報セキュリティ強化対応スキル指標のご紹介

ドキュメントを参照: [security](http://www.ipa.go.jp/jinzai/hrd/security/)

* + - 1. 「iコンピテンシ・ディクショナリ」とは、 ITスキル標準（ITSS）や情報システムユーザースキル標準（UISS）、 組込みスキル標準（ETSS）の３つのスキル標準を包含する形で整理した、 タスクとスキルのデータのことです。 この iコンピテンシ・ディクショナリを参照することで、 ３つのスキル標準の区別を意識することなく、 スキル指標としてIT関連業務に携わる人材の役割、 タスクやスキルを確認することができます。
    1. 情報セキュリティを担う人材育成のヒント
       1. 情報セキュリティを担う人材の育成についての悩み
          1. 自社の情報セキュリティ対策

現場が情報セキュリティの重要性を理解してくれない。

セキュリティに関する事故を経験したことがあるかないかによって、 現場のセキュリティ意識は大きく異なる。 以前事故が発生したことをきっかけに、 経営者がセキュリティ対策を現場横断的な重要なテーマとして掲げ、 全社的な取り組みを始めることができた

経営層に対して、 情報セキュリティ対策の重要性を効果的に伝えられず、 企業全体としての対策が進まない。

企業にとってのセキュリティ対策は、 今や単なる事故の予防ではなく、 企業のサービスの機能・品質の向上の一環であるということを、 経営者に伝える必要がある。

経営層に対してセキュリティの重要性を伝えられる人材の有無によって、 経営層の理解が変わる。 これは、 経営とITの関係と同じであり、 経営と現場をつなぐキーマンの育成 が鍵である。

情報セキュリティ担当者のスキルアップが難しい。

ユーザー企業には、 専任の情報セキュリティ担当者は少なく、 担当者は数年で異動・交代することが一般的であるため、 限られた期間で効果的にスキルアップする必要がある。 情報セキュリティマネジメントに関する資格などの学習も効果的である。

* + - * 1. 情報セキュリティを担う専門人材の育成

専門性の高い人材の育成方法が分からない。

専門性は高いが、 スキルの幅が広がらない。

専門性は高いが、 ビジネスマインドが身につかない。

* + 1. 組織において求められる 情報セキュリティ対策のレベル
       1. 自社の属性に合った情報セキュリティ対策のレベルを見極めていく
  1. 情報処理安全確保支援士試験チェックシート
     1. 第1章　情報セキュリティ及びITの基礎
        1. 情報セキュリティの主な特性として，機密性・完全性・可用性の三つがある。 また，真正性，責任追跡性，否認防止及び信頼性を，情報セキュリティの付加的な特性とする場合がある。
        2. 情報セキュリティ対策には，抑止・抑制，予防・防止，検知・追跡，回復などの機能がある。 情報セキュリティ対策は，これらの機能のうち必ず一つ以上の機能をもっている。
        3. サイバー攻撃とは， 企業，組織，個人のコンビュータや情報システムに対し，ネットワークを介して侵入したり，不正なプグラムやコマンド，パケットを送りつけたりして，情報窃取，改ざん，破壊，サービス妨害等の攻撃や不正行為をすることである。
        4. 情報資産にアクセスする人間，プセス，プグラム等に対して，常に必要最小限の権限のみを付与するように徹底する。 これをf最小権限の原則Jという。
        5. 同ーの者に関連する複数の業務を行う権限を与えると，確認不足によるミスや不正行為などを発生させる原因となるため，業務ごとに担当を適切に分離する。 これを「責務の分離（職務分離）の原則jという。
        6. 組織内やシステムで発生する様々な事象について，それを発生させた主体（利用者，端末，プセス，プグラム等）を一意に識別・特定し追跡・検証できるようにする。
        7. 情報セキュリティマネジメントとは，「明確な方針や規定に基づいて，組織の情報資産の機密性，完全性，可用性などの特性を適切に維持・管理すること」と定義できる。
        8. 問合せ元のアドレスや問合せ対象ドメインの制限なく，名前解決要求に応じるDNSサーバ（キャッシュサーバ）は「オープンリゾルバjと呼ばれる。 オープンリゾルバはDNSキャッシュボイズニング攻撃に対して脆弱である。
        9. GETメソッドを使用したWebアフリケーションでは，URしから入力データが読み取られたり，改ざんされたりする可能性がある。 また， Referrerグから入力データが漏えいする可能性がある。
        10. POSTメソッドを使用すれば入力データがURLに含まれないため，GETメソッドよりも秘匿性が高まるが，入力データをグに記録するにはアプリケーション側で対応する必要がある。
        11. シンクライアントを実現する主な方式として，ネットワークブート方式と画面転送方式がある。 画面転送方式には，サーバベース型，プレードPC型， VDI型があり，これらの中で近年主流となっているのがユーザの利便性とコストバフォーマンスのバランスのとれたVDIである。
     2. 第2章　情報セキュリティにおける脅威
        1. ポートスキャンとはターゲツ卜となるホスト上で開いている（通信可能な状態となっている）ポートをスキャン（探査）することである。
        2. TCPハーフスキャン（ステルススキャン）はコネクションを確立しないためターゲットホストのグには記録されない。
        3. 管理者権限で実行されているサービスに対してBOF攻撃を行い，シェルなどに置き換えることに成功すれば，侵入者は管理者権限でそのホストを操作できることになる。
        4. BOF攻撃はソフトウ工アのバグが原因となっているため，その対策は， OSや使用しているソフトウェアのバージョンアップ，パッチの適用を確実に行うことで，既知のセキュリティホールを塞ぐことである。
        5. 侵入者は，所有者がrootで， setuid/setgid属性をもってプグラムを実行し，非常にサイズの大きい入力データを与えることでBOF状態を引き起こし， root権限を手に入れることができる。
        6. BOF攻撃への対策として所有者がrootで＇setuid/setgid属性をもつフグラムを探し，不要なものを削除するか， setuid/setgid属性を解除する。
        7. rootkitとは，侵入に成功した攻撃者が，その後の不正な活動を行いやすくするために自身の存在を隠ぺいすることを目的として｛吏用するソフトウェアなどをまとめたパッケージの呼称（俗称）である。
        8. パスワードクラックとは， 何通りものパスワードを繰返し試してパスワードを破る行為であり，推測によるもの，辞書ファイルを用いたもの，総当たりによるもの（ブルートフォース攻撃）などがある。
        9. ワンタイムパスワード方式，バイオメトリック認証システムなど，パスワードクラックが困難な認証システムにするのが確実な対策手段であり，従来の固定式パスワードを用いる場合にはアカウントのックアウト設定が有効な対策手段となる。
        10. TCPでは，シーケンス番号の交換によって通信の信頼性を高めているが，この仕組みを悪用し，他のホストのセッションに割り込んでシーケンス番号やIPアドレスを矛盾なく操作することができればセッションハイジャックが成立する可能性がある。
        11. UDPでは，クライアントからのリクエストに対し，正規のサーバよりも先にレスポンスを返すことでセッションハイジャックが成立する可能性がある。
        12. Webアプリケーションではセッション管理の脆弱性を攻略し，URL，クッキー， hiddenフィールド、 などlこセットされたセッション管理情報を推測／盗聴することによってセッションハイジヤックが成立する可能性がある。
        13. 攻撃者自身のMACアドレスと正規のホストのIPアドレスとを組み合わせた偽のARP応答パケットを送信することでARPキャッシュの内容を書き換え，セッションをハイジャックする手法をARPスプーフイングもしくはARPキャッシュポイズニングという。
        14. DNSサーバがゾーン転送要求に制限をかけていないと，不正なゾーン転送要求により，サイトのネットワーク構成やサーバの構成が攻撃者に推測されてしまう可能性がある。
        15. DNSキャッシュボイス・ニンク攻撃とは，DNSサーバからの名前解決要求に対して不正な名前解決情報を付加して返すことでDNSのキャッシュを汚染し，ユーザを悪意あるサイトに誘導する攻撃である。 DNSの送信元ポート番号とトランザクションIDが推測されやすいと，この攻撃による被害を受けやすい。
        16. SYNFlood攻撃とは，発信元アドレスを偽装したSYNパケットを特定のポートに大量に送りつけることで，正常なサービスの提供を妨害する行為である。
        17. コネクションレスであるUDPやICMPでは発信元アドレスの偽装が容易であるため，攻撃に悪用された場合，攻撃者を特定するのは困難である。
        18. smurf攻撃とは，ターゲヅトホストのIPアドレスに発信元アドレスを偽装したICMPecho requestを踏み台ネットワークのブードキャストアドレスに送りつけ，その応答パケットによってDoS攻撃を成立させる手法で、 ある。
        19. DDoS攻撃とはインターネット上にある多数の踏み台サイトにあらかじめ仕掛けておいた攻撃プグラムから，一斉にDos攻撃を仕掛けることで，ターゲットサイトのネットワークの帯域をあふれさせる攻撃手法である。 近年， DDoS攻撃はポットネットによって実行されるケースが大半となっている。
        20. DDoS攻撃への対策として，十分な回線帯域を確保し，十分な処理能力を有する機器を使用するとともに，負荷分散，帯域制限などによって攻撃を緩和するほか，CONサービスやCONプバイダ等が提供するDDoS攻撃対策サービスを利用することも選択肢となる。
        21. クスサイトスクリプティング（XSS）とは，ユーザの入力データを処理するWebアプリケーションや，Web ページ．を操作するJavaScript等に存在する脆弱性を悪用し，ユーザのPC上で不正なスクリプトを実行させる攻撃手法である。
        22. xssは，その仕組みにより，反射型xss，格納型XSS,DOM Based XSSの3種類に分類される。 DOMBasedxssは，スクリプ卜によるWebページ出力処理（DOM操作）に不備があることによる脆弱性である。
        23. SQLインジヱクションとは，ユーザの入力データをもとにSOL文を編集してDBにアクセスする仕組みに
        24. なっているWebアプリケーションに対して不正なSOL文を入力することで，機密情報を不正に取得したり，DBを不正に操作したりする攻撃手法である。
        25. OSコマンドインジェクションとはユーザの入力データをもとに，OSのコマンドを呼び出して処理する
        26. Webアプリケーションにおいて，不正なコマンドを入力することで，任意のファイルの読出し，変更，削除，パスワードの不正取得などを行う攻撃手法である。
        27. HTTPヘッダインジェクションとは，ユーザの入力データをもとに， HTTPメッセージのレスポンスを生成するWebアプリケーションにおいて，不正なデータを入力することで任意のヘッダフィールドやメッセージボディを追加したり複数のレスポンスに分割したりするなどの攻撃を行う手法である。
        28. メールヘッダインジェクションとはユーザがフォームに入力したデータをもとにメールを送信するWebアプリケーションにおいて，不正なメールヘッダを混入させることにより意図していないアドレスに迷惑メールを送信するなど，メール送信機能を悪用した攻撃手法である。
        29. xssやSOLインジェクションに対しては，ユーザの入力データ中にスクリプトやSQL文として特別な意味をもっメタキャラクタが存在した場合，それらをエスケープ処理することで対処する。
        30. OSコマンドインジェクションに対しては，OSコマンドの呼出しが可能な関数を極力使用しないようにすることと，使用する場合にはルールに従わないデータを無効とし，一切処理しないようにする必要がある。
        31. HTTPヘッダインジ、 エクションに対しては，HTTPレスポンスヘッダ生成に用いるユーザ入力データに改行コードが含まれていた場合には削除するほか，ヘッダ出力用のAPIやライブラリを使用するなどの対策が有効である。
        32. マルウェアへの対策は各ホストにウイルス対策ソフトを導入することに加え，ファイアウオール， IPS，サンドボックス，SMTPゲートウェイ，プキシサーバなど，通信経路上での検知・駆除対策を複合的に実施する必要がある。
        33. ボット（bot）とはワームの一種で，コンビュータに感染するだけでなく攻撃者によって遠隔地から操作ができ，機能拡張なども行うよう作られた悪質なプグラムであり，その操作にはIRC,P2Pソフトなどが悪用される。
        34. ランサムウェアとは感染したコンビュータのファイルやハードディスクを勝手に暗号化する等して正常に利用できない状態にした後それを解除するための身代金の支払いを要求するタイフのマルウェアである。
        35. 標的型攻撃とは特定の組織や団体等をターゲットとして，その取引先や関係者，公的機関などを煽ってマルウェアや不正なリンクが埋め込まれたメールを送信することで相手を編し，情報を盗もうとする手法である。
        36. 水飲み場型攻撃とは攻撃者がターゲツトとなる組織の社員／職員等が日頃頻繁に利用しているWebサイト（水飲み場）を改ざんすることで同組織のPCをマルウェアに感染させる手である。
        37. 出対策とは，マルウェアの侵入・感染を許したとしても，その拡散や，機密情報や個人情報の外部への流出などの被害を防ぐために行う対策である。
        38. マルウェアの検出手法としては，パターンマッチング法が代表的だが，パターンファイルに登録されていないものは検出できない。 既知のウイルスの亜種や，未知のウイルスなどの検出にはヒューリスティック法やビヘイビア法が有効である。
     3. 第3章　情報セキュリティにおける脆弱性
        1. 公開Webサーバと社内専用のファイルサーバなど，アクセスを許可する範囲（人，機器等）が明らかに異なるホストが同一セグメントに混在しているネットワークは脆弱であり，機密性，完全性の侵害につながるリスクが高い。
        2. 発信元IPアドレスにプライベートアドレスが設定されたインターネットからのインバウンド、 パケットなど，明らかに発信元アドレスが偽装されているパケットについては，ルータやファイアウオールによって遮断する必要がある。
        3. 広く普及しているメールサーバソフトウェアの旧バージョンでは，メールの投稿にあたってユーザを認証する仕組みがなかったため発信元メールアドレスの詐称が堂々と行われるほか，組織外の第三者から別な第三者へのメール投稿を受け付け$中継してしまう。
        4. 組織外の第三者から別の第三者へのメール投稿を受け付け，中継してしまうことを第三者中継（Third-PartyMail Relay）という。 なお，第三者中継をオープンリレー，それを行うSMTPサーバをオープンリレー(SMTP）サーバとも呼ぶ。
        5. OP25Bとは，ISPのSMTPサーバを経由せず，直接インターネットに出ていく25番ポートあてのパケットを遮断することで，スパムメールの発信を防ぐ技術である。
        6. OP25Bが設定された環境で正当なユーザがISP以外のSMTPサーバを使用してメールを発信する場合には，投稿専用のSubmissionポート（587/TCP）を使用するとともに， SMTP-AUTHによってユーサ．認証を行う。
        7. 発信元情報を偽装したメールを発見し，排除する技術として，発信元のIPアドレスやディジタル署名によってメール受信側で発信元SMTPサーバを認証する仕組み（送信ドメイン認証）が近年実用化されている。
        8. 標準的なPOP3ではUSER/PASSコマンドによってユーザ認証を行うが，その際ユーザIDとパスワードは
        9. 平文のままネットワーク中を流れていくため，経路上でのパケット盗聴により，ユーザの認証情報が盗まれてしまう可能性が高い。
        10. POP3の脆弱性への対策としては，APOP,POP3over TLS (POP3S) SSHによるポートフォワーデイングなどがある。
        11. DNSSECは，ディジタル署名を用いて応答レコードの正当性，完全性を確認する方式であり，DNSキャッシュポイズニング攻撃への有効な対策となる。
        12. UDP53番ポートを使用するDNSの通常の名前解決では，一つのパケットに格納できるデータが512オクテットに制限されているがDNSの拡張機構であるEDNSOを用いることにより，最大65,535オクテットまで拡張することができる。
        13. DNSの脆弱性への対策として， DNSサーバを，代理名前解決を行わないコンテンツサーバと，ゾーン情報をもたない代理名前解決専用のキャッシュサーバに分離し，後者を利用可能なホストの範囲を制限する方法などがある。
        14. Webアプリケーションでは， URLパラメタ，hiddenフィールド，クッキーのいずれかの手段でセッション管理を行うが，それらのうちどれを用いていたとしても，HTTPで通信していればセッション管理情報の漏えいが発生する可能性がある。
        15. クッキーの有効期限は可能な限り短く，また有効範囲は可能な限り狭くすることに加え， HTTPS(TLS）を使用しているページでは必ず、 secure属性を設定し，盗聴によってクッキーが盗まれるのを防ぐ必要がある。
        16. HttpOnly属性をクッキーに設定することにより，適用範囲をHTIP/HTIPS通信だけに限定し，xssによってクッキーが盗まれるのを防ぐことが可能となる。
        17. 重要なセッション管理情報はすべてWebサーバ側で管理し， URLパラメタ，クッキー， hiddenフィールドには，セッションの識別情報（ID）しか含めないようにする。
        18. セッションIDには十分な長さをもった乱数やハッシュ値を用いる（GETメソッドを使用している場合は特に重要）。
        19. HTTPのベーシック認証では盗聴によって認証情報が漏えいする可能性があるため，使用する場合にはHTTPSによって暗号化する。
        20. Webサーバが詳細なエラーメッセージをクライアントに返す設定になっていると機密情報の漏えいにつながる可能性があるため，必要最小限のエラーメッセージのみを返すように設定する。
        21. CSRFとは， Webアプリケーションのユーザ認証やセッション管理の不備を突いて，サイトの利用者に，Web アプリケーションに対する不正な処理要求を行わせる手法である。
     4. 第4章　情報セキュリティマネジメントの実践
        1. 情報セキュリティ対策の効果を高めるためには，リスク分析によって組織に内在する様々な情報リスクを洗い出すとともに，その影響度を分析・評価し，有効な対策を導き出す必要がある。 この一連の取組みをリスクアセスメントという。
        2. 詳細リスク分析では，分析の対象となる組織や情報システムにおける情報資産，脅威，脆弱性を洗い出し，それらの関連性からリスクを洗い出し，その大きさを評価する。
        3. リスクコントールとは，潜在的なリスクに対して，物理的対策，技術的対策，運用管理的対策によって，発生を抑止したり，損失を低減させたりすることである。
        4. リスクファイナンシングとは， リスクが顕在化して損失が発生した場合に備えて，損失の補壌や対応費用などの確保をしておくことである。
        5. 組織の重要な情報資産を適切に保護するためには，その重要度などに応じて整理・分類するとともに，取扱い方法を明確にする必要がある。
        6. 特定組織におけるCSIRTには，インシデン卜発生時にその対応を主導し，情報を集約して顧客，株主，経営者，監督官庁等に適時報告するとともに，現場組織等に適時対応を指示することなどが求められる。 また，平常時の活動として，セキュリティ情報の収集，業界団体，他のCSIRT等と連携し，インシデント発生に備えた対応を行うことなども重要な役割となる。
        7. BCMを確立するには，まずビジネスインパクト分析(BIA）を行い，重要業務の停止時に目標時間内に復旧させるための具体的な計画や手順を事業継続計画(BCP）として策定する必要がある。
     5. 第5章　情報セキュリティ対策技術
        1. (1)侵入検知・防御
           1. ホスト要塞化の主な実施項目としては，最適なパーティション設計とセキュアなファイルシステムの選択，最新バージョンのソフトウェアのインストールとパッチ適用，不要なサービスや機能の停止，アカウントの停止／削除とパスワードの強化，システムリソースに対する最小限のアクセス権の設定適切なギング設定，などがある。
           2. OS，サーバソフトウェアに対する脆弱性検査で、 は，発見された脆弱性に直ちに対処するとともに，同じ製品構成の他のホストにも同様の脆弱性が存在する可能性が高いため，それを確認し，対処する必要がある。
           3. Webアプリケーションに対する脆弱性検査では，発見された脆弱性に直ちに対処するとともに，そのページを開発したベンダが開発した他のアプリケーションにも同様な脆弱性が存在する可能性が高いため，それを確認し，対処する必要がある。
           4. パケットフィルタ型（スタティックパケットフィルタ型）ファイアウオールとは，パケットのヘッダ情報に含まれるIPアドレスポート番号などによって中継の可否を判断するもので，パケットのアプリケーション層のデータ（ぺイード）についてはチェックしない。
           5. ダイナミックパケットフィルタ型ファイアウオールとは，最初にコネクションを確立する方向のみを意識した基本的なACしを事前に登録しておき，実際に接続要求があると，個々の通信を管理テーブルに登録するとともに必要なルールが動的に作成され，フィルタリング処理を行う方式である。
           6. ファイアウオールでは，許可されたプトコルに対するポートスキャンや，BOF攻撃などOSやミドルウェアの脆弱性を突いた攻撃， SOLインジエクションなどWebアプリケーションの脆弱性を突いた攻撃，DoS系の攻撃などを防ぐことはできない。
           7. 一般的なNIDSは主に登録されたシグネチャ（攻撃パターンのデータベース）とのマッチング，異常検知（アノマリ検知）というこつの手法を用いて攻撃や不正アクセスを検知する。
           8. アノマリ検知とは取り込んだパケットをRFCのプトコル仕様など（正常なパターン）と比較し，仕様から逸脱したものを異常として検知する手法である。
           9. HIDSは監視対象となるホストに常駐し，グインの成功／失敗，特権ユーザへの昇格，システム管理者用プグラムの起動，特定のファイルへのアクセス，プグラムのインストールなどのイベントをリアルタイムに監視する。
           10. IDSの誤検知の割合を測るための指標として，フォールスポジティブとフォールスネガティブの二つがある。 前者は不正ではない事象を不正行為として検知してしまうことを指し，後者は本来検知すべき不正行為を見逃してしまうことを指す。
           11. NIDSには誤検知のほか，一部の高性能な機種を除き暗号化されたパケットを検知できない，サイト独自のアプリケーションの脆弱性を突いた攻撃を検知できない，不正アクセスを防御できない，内部犯罪の検知は困難，などの機能上の限界や運用上の課題がある。
           12. 侵入防御システム（IPS）とは，従来のNIDSをインライン接続することで＇ ，NI DSと同等の侵入検知機能と，NIDSよりも強力な防御機能を備えた製品である。 誤検知が発生しやすかったアノマリ検知機能の強化などが図られている。
           13. IPSをインライン接続することによってパケットを遮断する場合，フォールスポジティブが発生すれば正常なアクセスが遮断されてしまう。 逆に，フォールスネガティブが発生すれば攻撃を見逃してしまう。 また，誤検知ではなくとも攻撃が多発すればIPSの処理能力等の問題でネットワークのパフォーマンスやアベイラビリティを低下させてしまう可能性がある。
           14. 一般的なIPSでは，フェールオープン機能を用いることで，障害が発生した場合にはパケットをそのまま通過させ， トラフィックが遮断されないようにすることも可能である。
           15. Webアプリケーションファイアウオール（WAF）とは， XSS, SQLインジェクションなど， Webアプリケーションに対する攻撃を検知・排除する製品である。
           16. 一般的なWAFにはSSL暗号化／復号機能や負荷分散機能が内蔵されている。 そのため， SSLアクセラレータ，ードバランサを併用することなくWebサイトを運用することも可能である。
           17. リバースプキシ型のWAFを経由したリクエストは，発信元の情報がWAFに置き換えられるため， Webサーバのアクセスク上では実際の発信者を特定できなくなる。 そのため， WAFによっては実際の発信者のアドレスを引き継いで渡す機能もある。
           18. 近年普及しつつあるサンドボックスとは，実環境から隔離されたセキュアな仮想環境のことであり，当該環境でマルウェアの可能性がある不審なファイル等を実行させ，その振る舞いを観察することでマルウェアであるかどうかを判定する。
        2. (2)アクセス制御と認証
           1. ファイルやシステム資源などの所有者が，読取り，書込み，実行などのアクセス権を設定する方式を任意アクセス制御（DAC）という。 DACでは所有者の裁量次第でファイルなどへのアクセス権が決定するため，十分な機密保護を行うのは困難である。
           2. 保護する対象である情報と，それを操作するユーザなどに対してそれぞれセキュリティのレベルを付し，それを比較することによって強制的にアクセス制限を行う方式を強制アクセス制御（MAC）という。 MACでは，たとえファイルの所有者であったとしても，アクセス権を自由に決定することはできない。
           3. 認証の対象として，人の認証（本人認証），物（機器，デバイス等）の認証情報の認証（メッセージ認証）の三つがある。 また，本人認証として，バイオメトリクスによる認証，所有物による認証，記憶や秘密による認証の三つがある。
           4. 認証された利用者に対して，定められた機能などを実行するための権限を与えることを「認可(Authorization)J という。
           5. チャレンジレスポンス方式とはサーバから送られた乱数文字列である「チャレンジ」と，クライアントのパスワードである「シード」(Seed ：種）を組み合わせて計算した結果を「レスポンス」としてサーバに返し，サーバも同様の計算を行って求めたレスポンスとの比較によってユーザ を認証する方式である。
           6. ワンタイムパスワード方式は，認証のたびに毎回異なるパスワードを使用することでセキュリティを確保するが，そのためには生成するパスワードに規則性や連続性がなく（ランダムであることにユーザがパスワードを覚えなくてもよいようになっている必要がある。
           7. チャレンジレスポンス方式やS/Keyによる認証における問題として，サーバの正当性を確認する仕組みがないと通信経路上に不正なホストが存在し，それによってセッションをハイジヤックされてしまう可能性がある。 これを中間者攻撃（Man-in-the-MiddleAttack）と呼ぶ。
           8. 認証システムに対する中間者攻撃の脅威に対しては，SSL/TLSのように通信に先立ちディジタル証明書によってクライアントがサーバの正当性を確認する方式を採用することなどが対抗策となる。
           9. ICカードに対する攻撃手法は， ICチップの破壊を伴うもの（破壊攻撃）と伴わないもの（非破壊攻撃，もしくはサイドチャネル攻撃）に大別される。 前者の代表的なものとして，プービングやリバースエンジニアリングがあり，後者の代表的なものとしては， DPA,SPA，グリッチ，光照射などがある。
           10. ICチップの脆弱性評価に関する事実上の基準となっているのはJIWGである。 JIWGはICカードの評価の公平性や客観性を実現するための解釈の統ーや， ISO/IEC 15408をICカードの評価に適用する際の解釈の統一を目的としたワーキンググループである。
           11. IEEE802.1Xは，ネットワーク環境でユーザ認証を行うための規格である。 もともとは有線LAN向けの仕様として策定が進められたがその後EAPとして実装され，現在では無線LAN環境における認証システムの標準仕様として広く利用されている。
           12. IEEE802.1Xは，クライアントであるサプリカント(Supplicant）システム，アクセスポイン卜やLANスイッチなど，認証の窓となる機器である認証装置(Authenticator），認証サーバ（RADIUSサーバなど）から構成される。
           13. EAP-TLSは，サーバ・サフリカントでTLSによる相互認証を行う方式であり認証成立後にはTLSのマスタシークレットをもとにユーザごとに異なる暗号鍵を生成・配付し，定期的に変更するため，無線LANのセキュリティを高めることができる。
           14. EAP-TTLSは，TLSによるサーバ認証によってEAPトンネルを確立後，そのトンネル内で様々な方式を用いてサプリカントを認証する方式であり， EAP-TLSと閉じ仕組みにより，無線LANのセキュリティを高めることができる。
           15. PEAPは，EAP-TTLSとほぼ問機の方式だが，サプリカントの認証はEAP準拠の方式に限られる。 EAPTLS,EAP-TTLSと同じ仕組みにより，無線LANのセキュリティを高めることができる。
           16. EAP-MD5は， M05によるチャレンジレスポンス方式によってパスワードを暗号化しサプリカントの認証のみを行う方式である。 認証フセスそのものは暗号化されず，暗号鍵の生成・配付等も行わないため，無線LANでの使用には向かない（有線LAN向き）。
           17. シングルサインオン（SSO）を実現するには，各サーバ間でユーザの識別情報を交換する必要があるが，それを行うための仕組みとして，クッキーを用いる方式，リバースプキシサーバを用いる方式， SAMLを用いる方式があるo
           18. クッキーを用いたsso認証システムでは，クッキーが共有可能な範囲内（同一ドメイン内）でしか使用できない，クライアントがクッキーの使用を制限している場合には使用できない等の問題がある。 一方，リパースプキシ方式については，ネットワーク構成の制約により，複数のドメインにまたがったシステムでssoを実現するのは困難である。
           19. SAMLとは，認証情報を安全に交換するためのXML仕様であり，OASISによって策定された。 SAMLはSOAPをベースとしており同一ドメイン内や特定のベンダ製品にとどまらない大規模なサイトなどにおいて，相互運用性の高いssoの仕組みゃ，セキュアな認証情報管理を実現する技術である。
           20. SAMLでは，認証結果の伝達，属性情報の伝達，アクセス制御情報の伝達，のそれぞれにアサーションと呼ばれるセキュリティ情報を扱うほかアサーションへのリファレンス情報などからなる「Artifact」と呼ばれる情報が使用されている。
           21. SAMLでは，ldPとSP闘で要求・応答メッセージを送受信するためにHTTPやSOAP等のプトコルにマッピングする方法（バインディング方法） として，SOAP, HTTP Redirect, HTTP POST, HTTPArtifactなどの穫類がある。
           22. 一般的に，アイデンティティ管理（ID管理）は，ディレクトリ，プビジョニング，アクセス制御（管理），ワークフーなどのシステムとそれを運用管理するためのポリシ，手順，体制などによって実現される。
        3. (3)暗号
           1. AESとは，DESの後継となる米国政府標準の共通鍵暗号方式である。 NISTによる審査の結果，ベルギーのJoanDaemen氏とVincentRijmen氏が開発したfRjjndaelJ （レインダール）という方式が選ばれた。 ブック長は128ビットで＼ 使用する鍵の長さは128/192/256ビ、 ツトの中から選択できる。
           2. ブック暗号では，処理を複雑にし，暗号の強度を高める暗号化手法（暗号モード）が確立されており，CBC(Ci pher Block Chaining）やCFB(Cipher Feedback)などがある。 CBCは一つ前の平文ブックの暗号結果と次の平文ブックをXOR演算し，その結果を暗号化する方式であり，広く使用されている。
           3. ハッシュ関数とは，任意の長さの入力データをもとに，固定長のビット列（ハッシュ値メッセージダイジ、 エスト）を出力する関数であり，衝突発見困難性，第2原像計算困難性，原像計算困難性（一方向性）の三つの性質が求められる。
           4. SHA-1には，ある条件下でハッシュ値の衝突を意図的に起こすことができるという脆弱性が発見されていることから，次世代ハッシュ関数（SHA-3）が決定されるまでの措置として， SHA-2に移行することが推奨されていたが，NIST主催の次世代暗号コンペティションの結果，2012年10月にfKeccakJ がSHA-3に選出された。
           5. MAC（メッセージ認証コード）とは通信データの改ざん有無を検知し完全性を保証するために通信データから生成する固定長のコード（ビット列）である。 MACには，ブック暗号を用いたCMAC，ハッシュ関数を用いたもの（HMAC）などがある。
           6. HMACは，ハッシュ値の計算時に，通信を行う両者が共有している秘密鍵の値を加えてその通信固有のハッシュ値を求めるようにすることで通信データの改ざんを検知する仕組みである。
           7. フィンガプリントとは，ディジタル証明書や公開鍵，メールなどの電子データが改ざんされていないことを証明するために使用するデータであり，ハッシュ関数を用いて対象となる電子データから生成する。
           8. PC環境において暗号化に用いる鍵を安全に生成して格納したり，暗号化・復号処理等を実行したりするための技術として， 近年TPM(Trusted PlatformModule）が広く用いられている。 TPMは耐タンパ性に優れたセキュリティチッフであり，通常PCのマザーボードに直付けする形で搭載されている。
           9. Diffie-Hellman鍵交換アルゴリズムは，離散対数問題が困難であることを安全性の根拠にしており，安全でない通信路を使って暗号化に用いる秘密対称鍵を生成し，共有することを可能にするものである。
           10. SAとは，IPsecにおける論理的なコネクション（トンネル）であり，制御用に用いるISAKMPSAと，実際の通信データを送るために用いるIPsecSAがある。 IPsec通信を始める際には最初に制御用のISAK MPSAが作られ，次にIPsecSAが作られる。
           11. ISAKMPSAはIPsecゲートウ工イ聞で一つ（上り下り兼用）作られるが， IPsecSAは，各ホスト問において，通信の方向や使用するプトコル（AH, ESP）ごとに別々のSAが作られる。 IPsecSAの識別情報として，あて先IPアドレス，フトコル，SPIが使用される。
           12. AH（認証ヘッダ）は，主に通信データの認証（メツセージ認証）のために使用されるプトコルであり，通信データを暗号化する機能はない。
           13. ESP（暗号化ぺイード） は通信データの認証（メッセージ、 認証）と，暗号化の両方の機能を提供するプトコルである。
           14. AHではMACを用いてパケット全体のICVを作成するため，完全性チェックの精度を高めることが可能だが，その反面， NATを使用している場合には経路上でIPアドレスが変更されてしまうため完全性チェックが正常に行えなくなってしまうという問題がある。
           15. ESPもAHと同様にMACを用いてICVを生成するが，AHとは異なり，IPアドレスについては計算の対象としていないため，NATを行ってもICVは影響を受けずに済む。 ただし， NAPTについては正常に行えないため，対処が必要となる。
           16. IKEバージョン1(IKEv1）は， SAや鍵管理の仕様を規定したISAKMP/Oakleyを実装した汎用的なプトコルであり，500/UDPを使用する。 IKEv1の鍵交換方式として，ISAKMPSAの作成に使用するメインモード＼ アグレッシブモード， IPsecSAの作成に使用するクイックモードなどが、 ある。
           17. IKEでは，通信に先立って通信相手を認証する。 その方式としては，通信を行う者同士が，あらかじめ鍵を共有しておき，それによって相手を認証する［事前共有鍵認証jのほか，「ディジタル署名認証jや「公開鍵暗号認証jなどがある。
           18. メインモードで事前共有鍵認証を行う場合，通信相手を識別するIDは暗号化されるが，IDにはIPアドレスしか使用できないという制約がある。 そのため，モバイル接続のように，毎回動的にIPアドレスが、 設定される環境では使用できない。
           19. アグレッシブモードで事前共有鍵認証を行う場合，IDは暗号化されないが，最初に送信されるため，IDにFQDNなどを使用して事前共有鍵との対応付けを行うことができる。 そのためIPアドレスが動的に設定される環境でも使用することができる。
           20. クイックモードでは前フェース で確立したISAKMPSAを使用して通信が行われるためパケットのぺイード部分が暗号化される。
           21. リモートアクセス環境でのIPsec通信では，SAの作成時に端末機器を認証（デバイス認証）するだけでなく，端末の使用者も認証（ユーザ認証）する必要がある。 IPsecでは，これを行う手段として， XAUTHが広く利用されている。
           22. NAPTを使用する環境では，AH,ESPともにそのままではIPsecを使用することができないため， IPsecのパケットに新たなUDPヘッダを追加（カプセル化）することによって対応する方法が広く用いられている。
           23. SSL/TLSは， トランスポート層とアプリケーション層の間に位置付けられ，その内部は下位層のRecordプトコルと，上位層の四つのプトコル（HandshakeプトコJレ，ChangeCipher Specプトコル，Alertプトコル，ApplicationDataプトコル）から構成される。
           24. Recordプトコルは，上位層からのデータを214バイト以下のブックに分割し，圧縮，MACの生成，暗号化の処理を行って送信する。 データ受信時には，復号，MACの検証，伸張の処理を行って上位層に引き渡す。
           25. Handshakeフトコルはサーバ・クライアント間で新たにセッションを確立する，もしくは既存のセッションを再開する際に，暗号化アルゴリズム，鍵，ディジタル証明書など，通信に必要なパラメタを相手とネゴシエーションして決定する。
           26. SSL/TLSにおける「セッションjとは， Handshakeプトコルによるサーバとクライアントの鍵交換（ネゴシエーション）の結果生成された，マスタシークレツトによって特定される仮想的な概念である。 一方「コネクションJは，セッションに従属して存在する通信チャネルであり，一つのセッションには，必要に応じて複数のコネクションが存在する。
           27. HSTSは， Webサイトが， HTTPSでアクセスしたブラウザに対し，当該ドメイン（サフドメインにも適用可能）への次回以降のアクセスにおいて， max-age で指定した有効期限（秒単位）まで， HTTPSの使用を強制させる機構である。
           28. S/MIMEは不特定多数のユーザ問で安全性，信頼性の高い通信を行うことを想定しているため，利用にあたって各ユーザは公的な第三者機関が発行するディジタル証明書（S/MIME証明書）を取得することが前提となる。
           29. X.509は，ITU-Tが1988年に勧告したディジタル証明書及びCALの標準仕様でありISO/IEC 9594-8として国際規格化されている。 X.509では，ディジタル証明書の発行者が拡張フィールドに独自の情報を追加できるようになったほか， 2000年にはX.509v3の改訂が行われ，新たにAC（属性証明書），ACAL （属性証明書失効リスト）が定義された。
           30. OCSPレスポンダとは，ディジタル証明書の失効有無をリアルタイムで応答するサーバであり，CAやVAが運営する。 クライアン卜はOCSPレスポンダに問い合わせることによって自力でCRしを取得したり照合したりする手間を省くことができる。
           31. SCVPはOCSPと同様に証明書の有効性検証をリアルタイムで行う仕組みであるがOCSPではディジタル証明書の失効情報のみをチェックするのに対し，SCVPでは信頼関係（有効期限，署名など）も含めてチェックする。
           32. タイムスタンプとは，電子文書に対して，信頼される第三者機関である時刻認証局（TSA）が付す時刻情報を含んだ電子データでありその電子文書が「いつ」作成されたかということと「その時刻以降改ざんされていなしリことを保証するものである。
           33. 過去のある時点でディジタル署名が有効であったことを検証するために，当該署名に対する公開鍵証明書，当該証明書からルート証明書に至るまでのパス上のすべての公開鍵証明書， 及びそれらに関する失効情報等をすべて集め，それらに対するタイムスタンプを付したものをアーカイブタイムスタンプという。
           34. アーカイブタイムスタンプは関連する技術の危殆化によって有効性が失われてしまう前に，その時点の最新技術を用いて次のアーカイブタイムスタンプを取得する必要がある。 これは，電子文書を保存している限り，必要に応じて繰返し行っていく必要がある。
     6. 第8章　システム開発におけるセキュリティ対策
        1. システム要件や利用環境等に応じた適切なセキュリティ機構を有し，脆弱性への対処がなされたセキュアなアプリケーションを開発するためには，開発工程の初期段階からセキュリティ対策に取り組む必要がある。
        2. CIC＋＋ 言語のgets,strcpy, strcat, sprintf, scant,sscanf, fscanfなどの関数では，入力データをサイズの制限なくメモリ内の変数領域に格納してしまうため，バッファオーバフー（BOF）状態を引き起こす可能性が高い。
        3. 上記の関数への対策としては，バッファに書き込むサイズを指定できる関数（fgets, strncpy, strncat,snprintf等）で代用するか，精度を指定してバッファに書き込む最大サイズを制限することである。
        4. CIC＋＋言語をはじめ，多くのプグラム言語で，ナル文字は文字列の終端を示すものとなるため，文字列を処理する関数はナル文字を見付けると読込みなどの処理を終了する，バッファに文字列を格納する関数は，末尾にナル文字を付加する，などの処理を行う場合が多い。
        5. 末尾にナル文字を付加する関数を使用する際には，文字列を格納する先のバッファのサイズとして，格納する対象となる文字列の長さに加えナル文字分（1バイト）が必要である。 これを怠るとBOFの問題が発生する可能性が高まる。
        6. Javaで採用されているサンドボックスモデルとは，ネットワークなどを通じて外部から受け取ったプグラムを，セキュリティが確保された領域で動作させることによって，プグラムが不正な操作や動作をするのを防ぐ仕組みである。
        7. レースコンディション（競合状態）とは，並列して動作する複数のプセスやスレッドが，同一のリソース（ファイル，メモリ，デバイス等）ヘほぼ同時にアクセスしたことによって競合状態が．引き起こされ，その結果，予定外の処理結果が生じるという問題である。
        8. ECMAScriptにおいて，外部からの入力値を文字列リテラルとして扱う場合にはメタキャラクタをエスケープ処理する必要がある。 エスケープ処理が必要な文字として最低限次の四つが挙げられる。 「＼ ＼＼」「 ＼ 」「 ＼ 」「改行 ＼n」。
        9. ECMAScriptにおいて，グーバル変数は関数の外で「var」を用いて定義し ーカル変数は使用する関数の中で「var」を用いて定義する。 「var」を使用せずに定義した変数はすべてグーバル変数として解釈されるが，発見が困難なバクを作り出す大きな要因となるため，避けなければならない。
        10. Ajax(Asynchronous JavaScript + XML） とは，JavaScriptなどのスクリプト言語を使ってサーバと非同期通信を行うことで、 Webページ全体を再描画することなく，ページの必要な箇所だけを部分的に更新することを可能にする技術である。
        11. XMLHttpRequestは各種ブラウザに実装されている組込みオブジエクト（API）であり，周期通信，非同期通信の双方をサポートしている。
        12. JSON(JavaScript Object Notation）とは，ECMA-262標準第3版準拠のJavaScript(ECMAScript）をもとにした軽量のデータ記述方式である。
        13. JSONP (JSON with Padding）とは，くscript＞タグのsrc属性にはクスドメイン通信の制限がなく，別ドメインのURしを指定できることを利用することで，JavaScript (ECMAScript）とJSONを用いてクスドメイン通信を実現する技術である。
     7. 第9章　情報セキュリティに関する法制度
        1. ISO/IEC 15408は，オペレーテイングシステム，アプリケーションプグラム，通信機器，情報家電など，セキュリティ機能を備えたすべてのIT関連製品や，それらを組み合わせた一連の情報システムのセキュリティレベルを評価するための国際規格である。
        2. CMMI（能力成熟度モデル統合版）は，米国国防総省が米国カーネギーメン大学に設置したソフトウェア工学研究所で考案された能力成熟度モデルの一つであり，システム開発を行う組織がプセス改善を行うためのガイドラインとなるものである。
        3. PCIDSS (Payment Card Industry Data SecurityStandard）とは，クレジットカード情報や取引情報の保護を目的として国際ぺイメントブランド5社が共同で策定したセキュリティ基準であり，対策を実施する頻度や許容期間などが具体的に示されているのが大きな特徴となっている。
        4. ISO/IEC 20000とはIT関連サービスを提供する組織が，顧客の求める品質を確保し，維持・改善するための要求事項を規定した国際規格であり， ITサービスマネジメントにおける業務プセスや管理手法を体系的に整理した書籍群であるITILに基づいている。
        5. 行政手続における特定の個人を識別するための番号の利用等に関する法律（マイナンバー法）は，年金や納税等，異なる分野の個人情報を照合できるようにするとともに，行政の効率化や公正な給付と負担を実現し，手続の簡素化による国民の負担軽減を図ることなどを主な目的としている。
        6. サイバーセキュリティ基本法は，サイバーセキュリティに関する施策や戦略を明確に定め，総合的かつ効果的に推進することにより，経済社会の活力向上，持続的発展，国民が安全で安心して暮らせる社会の実現，国際社会の平和及び安全の確保，国の安全保障への寄与などを目的にしている。
        7. 知的財産権のうち，特許権，実用新案権，意匠権，商標権の四つを［産業財産権Jという。
        8. 産業財産権の存続期間は，特許権が出願日から20年，実用新案権が出願白から10年，意匠権が登録日から最長20年，商標権が登録日から10年（継続使用による更新可能）となっている。
        9. 著作権とは，創作された表現を保護する権利であり，著作物を創作した時点で成立し，著作者の死後， 50年を経過するまでの間，存続する。 ただし，映画の著作物の保護期間は公表後70年となっているo
        10. 不正競争防止法が保護の対象としているのは「秘密として管理されている有用な技術上又は営業上の情報であって，公然と知られていないもの」である。
        11. 内部統制とは，企業において業務が正常かつ有効に行われるよう各種の手続や仕組み，プセスを整備し，それを遂行することによって，企業の活動全般を適切にコントールすることをいう。
        12. COBIT(COBITS）は，ITガバナンス及びITマネジメントに関する実践規範であり，ガイドライン文書， フレームワーク，プセス参照モデル等からなる。