「第8回 情報セキュリティマネージャーISACAカンファレンス in Tokyo」
「進化する技術と攻撃に対するこれからのサイバーセキュリティマネジメントとは」

多様化するＩＴ社会において情報セキュリティマネージャーが取るべき戦略

ーそれは「IT」の仕組みを元にした「人」における取り組みですー

2020年2月15日（土曜日）
一橋大学　一橋講堂

印藤　晃

本日皆様と過ごすストーリーを考えました

- まず、想定される聴講者をCISM有資格者を中心にいたしました
- 次に、なぜ小職がここに立つのかの自己紹介をさせてください
- そして、10大脅威で上位にランクインされる事象について考えます
- そこで、脅威を隔てるネットワーク分離を極めることのお話しをします
- 次は、官でのシステム調達の基本事項についてお話しします
- すると、システムとセキュリティの要件定義での空洞を認識します
- 今度は、そこにクラウドサービスで安全性評価制度が出来ます
- 本日は、2020年1月30日迄の情報で、方向性をお伝えします

必ずしも全てのご聴講者の皆様に適した内容では無いかもしれません、またあまりにも基本的なお話もさせていただきますが、お許しください。
本日はCISM＝情報セキュリティマネージャーとして初めて実務でのご担当をされる方々も意識しての内容となります。何卒ご理解とご了解をいただけますようお願いたします。

目次

- 本講演の概要・概念と自己紹介　【04～13】(10ページ)
  - CISMライセンス保有者を意識した内容 ・・・・・・・・・・・・・・・・・ イントロ
- 最近の脅威情報から紐解いた考察　【14～36】(23ページ)
  - 実際に発生した情報セキュリティインシデント事案と、その対応事例から見えるもの (情報セキュリティ10大脅威2019(IPA)を起点)
    - 5位　内部不正による情報漏洩 ・・・・・・・・・・・・・・・・・・・・・・・ 内部不正
    - 4位　サプライチェーンの弱点を悪用した攻撃の高まり ・・・・・・・・ サプライチェーン
    - 1位　標的型攻撃による被害 ・・・・・・・・・・・・・・・・・・・・・・・・ 標的型攻撃
- 具体的対策例　【37～43】(7ページ)
  - ネットワーク分離と利便性の確保による、セキュリティ確保と業務効率の向上 ・・・・・・・ 分離と利便性
- 正しい検討と実装における注意点　【44～66】(23ページ)
  - システム調達におけるセキュリティ要件の正しい検討と実装における注意点 ・・・・・・・ システム調達

本講演の概要・概念と自己紹介

イントロ

この講演タイトルのことばの示すもの

- 多様化するIT社会とは
  - DX、AI、IoT、自動運転、５G、
  - サイバー攻撃、Emotet
  - RPA、ブロックチェーン、ビックデータ、VDI、働き方改革
  - クラウド利用、クラウド・バイ・デフォルト
  - ・・・　等々
- 情報セキュリティマネージャーとは
  - 企業または官公庁の事業体でシステムの安全管理を行うこと
  - 事業体の全体最適化を考えリスクを管理すること
  - 規程、基準を精査して正しい運用の環境整備をおこなうこと
  - ・・・　等々

ことばの示すものは多々あります。上記を一例として上げさせていただきましたが、

本日はサイバー攻撃　→　分離　→　セキュリティ確保されたシステム調達　→　＋
クラウドサービス　と言う方向性でお話を進めさせていただきます。

どのような方々をお話の中心とするか

- 今日はISACAのCISM委員会を中心としたカンファレンスです
  - CISM資格の認定を保持されている方も本日多くおられると考えます
- お話の前提として、例えば
  - 何となくシステムのセキュリティを見る事になった方
  - リスク管理室等で仕事をする事になった方
  - 理科系出身ではないが文科系の自分がセキュリティに関与する事になった方
  - 自部門でシステムを調達する事になった方(必ずしも専門家でない)
    - このような方を想定してお話をまとめてみました
- お話しの推移はどちらかと言うと官の色が濃いかもしれませんが
- 情報セキュリティとか調達では考慮点としては同じと考えます
  - 官で有っても民で有っても参考にしていただけると幸いです

情報セキュリティマネージャーとは

- 情報セキュリティマネージャーの立場として取るべき方向性
  - 理科系的対応
    - インシデントにおける現場対応
    - 技術の深さにより他の専門家の登用でも良いのでは
      - 情報セキュリティ対応技術の全てを自ら保持するものではありません
  - 文科系的対応
    - 規程、基準、ガイドライン、手順書等の整備
    - 現場業務を認識した管理・運用が分かること
      - 業務運用を理解したユーザの立場を理解して対応が出来ること

事業体の現場で業務をされる方々及びSI専門家と共に、問題解決を管理する立場であることです

情報システム・情報セキュリティと言うことは

例えば

- 組織における位置づけでは
  - 情報システム部、リスク管理室
  - システム担当、セキュリティ担当
  - 情報システム委員会、情報セキュリティ委員会

- 調達における役割及び牽制の範囲
  - 業務要件
    - 機能要件
  - システム要件、セキュリティ要件
    - 非機能要件

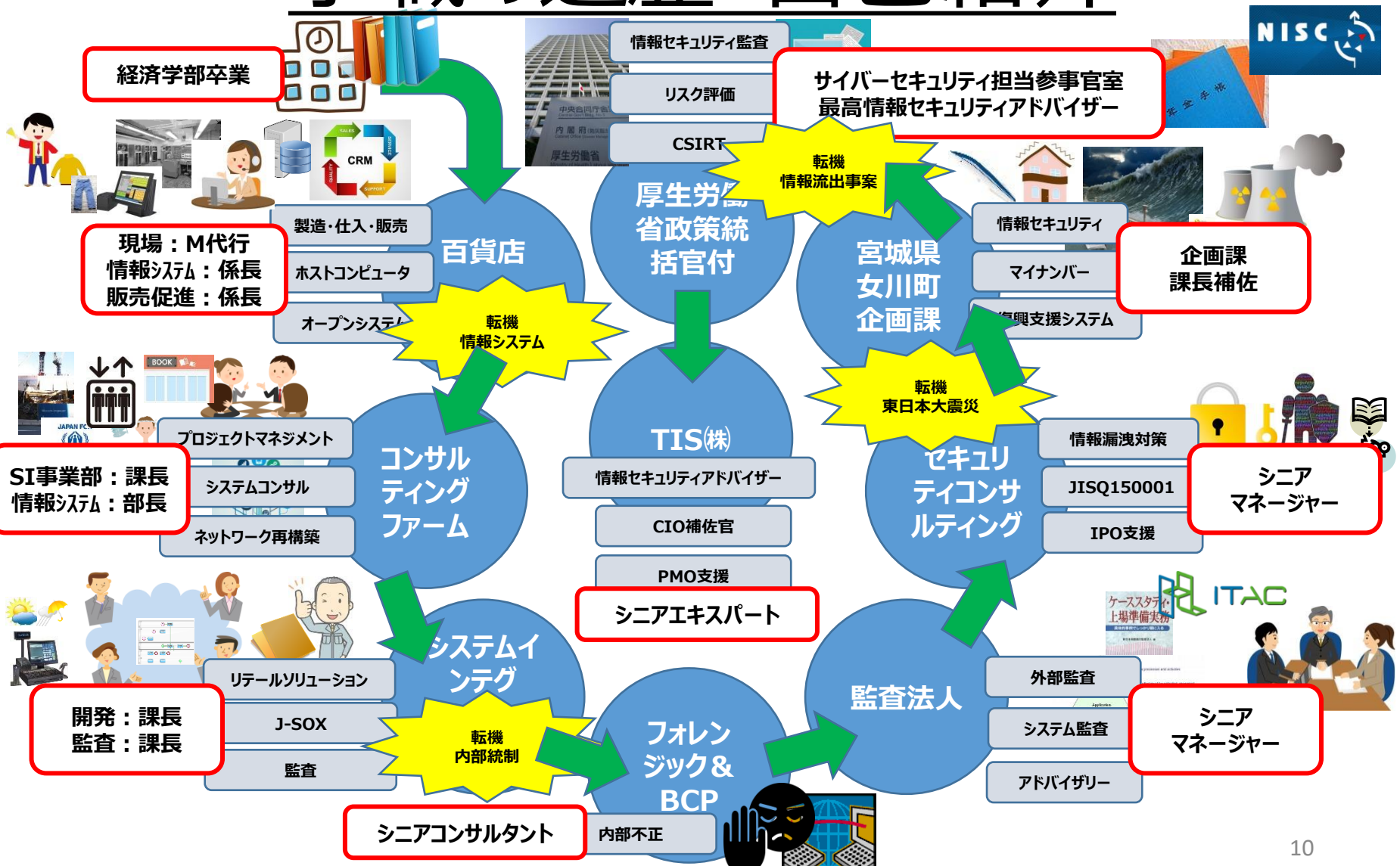
システムとセキュリティは別々では無く一緒に考えなくてはいけないのではないでしょうか

情報セキュリティマネージャーで大切な事

- ユーザの目線として業務を知り理解すること（業務要件）
- ユーザ、事業体含めた情報システム部の運用を理解すること(運用)
- 各々の事業体組織における情報システムを知る（事業計画）
- 時間軸・粒度・優先度・予算等の認識と全体の整合性確保(全体)
- ユーザにとって、運用者にとっての予算配分の適正化（実施計画）
- 業務要件の実装を第三者的に考えてみる（中立的）
- 事業体の対外的影響度でのセキュリティ対策の重要性（粒度）
- 各々の事業体での、万一のシステム障害時対応を考慮（文書化）
- ステークフォルダーの立場からの上記対応策（末端の利用者）
- インシデント対応想定し、発生時の対応訓練を実施（予防的）
- 事業体全体にわたるGRCを継続的に行う事（継続）

理屈に溺れない・最悪の事態をイメージ対応すること・
ガバナンス/リスクマネージメント/コンプライアンスの三つを意識すること

小職の遍歴・自己紹介


経済学部卒業
現場：M代行
情報ｼｽﾃﾑ：係長
販売促進：係長
製造・仕入・販売
ホストコンピュータ
オープンシステム
百貨店
転機
情報システム
情報セキュリティ監査
リスク評価
CSIRT
厚生労働省
政策統括官付
転機
情報流出事案
サイバーセキュリティ担当参事官室
最高情報セキュリティアドバイザー
NISC
宮城県
女川町
企画課
情報セキュリティ
マイナンバー
復興支援システム
企画課
課長補佐
転機
東日本大震災
SI事業部：課長
情報ｼｽﾃﾑ：部長
プロジェクトマネジメント
システムコンサル
ネットワーク再構築
コンサルティングファーム
TIS㈱
情報セキュリティアドバイザー
CIO補佐官
PMO支援
シニアエキスパート
セキュリティコンサルティング
情報漏洩対策
JISQ150001
IPO支援
シニア
マネージャー
開発：課長
監査：課長
リテールソリューション
J-SOX
監査
システムインテグ
転機
内部統制
フォレンジック&BCP
シニアコンサルタント
内部不正
監査法人
外部監査
システム監査
アドバイザリー
ITAC
シニア
マネージャー

業務経験で学べたこと

① 現場経験と情報処理部門双方のかかわりの重要性(現状認識)
② 理論と実践の架け橋となること（実現可能性）
③ ITによる統制と内部統制の融合（全てがITではない）
④ 現実的な企業内IT利用における様々な事情を考慮(優先順位)
⑤ 第三者的に見るIT及び内部統制から分かること(リスク認識)
⑥ 現実的な情報漏洩対応の終わりなき到達点(備えの充実)
⑦ 現実的なIT活用と地方自治の現状(中央と地方格差の認識)
⑧ 社会的影響のある情報流出事案以降での官の取り組みと方向性(粒度)
⑨ 官に指針を受けた現実的な対応と向かう方向(事業体での認識)

現場に出て人と語る事
策に溺れないで、現実的な運用面を重視して、穏便な対応を行うこと
システムとセキュリティはガバナンス/リスクマネジメント/コンプライアンスにて守られること

現在の小職の立ち位置

- 現職はTIS㈱のセキュリティコンサル(シニアエキスパート)
  - 準委任にて複数の独立行政法人と契約
    - 最高情報セキュリティアドバイザー
    - CIO補佐官
    - CSIRT実施責任者
    - PMO支援実施責任者　等
  - セキュリティ研修講師
    - 複数の公共事業体にて情報セキュリティ研修を実施
- NPOでの情報セキュリティアドバイザー
  - 規程類整備、情報セキュリティ研修、自己点検の運用支援　等
- 独立行政法人情報処理推進機構IPA
  - 情報処理技術者試験委員/情報処理安全確保支援士試験委員
- ISACA東京支部
  - 前調査研究員会副委員長
  - ISACA保有資格　CISA、CRISC

監査する側のCISA、その情報システム環境をリスクを意識して整えるCRISC、
その二つの異なる立場でシステムやセキュリティをとらえるのは極めて有効です

情報セキュリティ10大脅威2019

昨年順位	個人	順位	組織	昨年順位
1位 (*1)	クレジットカード情報の不正利用	1位	標的型攻撃による被害	1位
1位	フィッシングによる個人情報等の詐取	2位	ビジネスメール詐欺による被害	3位
4位	不正アプリによるスマートフォン利用者への被害	3位	ランサムウェアによる被害	2位
NEW	メール等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
3位	ネット上の誹謗・中傷・デマ	5位	内部不正による情報漏えい	8位
10位	偽警告によるインターネット詐欺	6位	サービス妨害攻撃によるサービスの停止	9位
1位	インターネットバンキングの不正利用	7位	インターネットサービスからの個人情報の窃取	6位
5位	インターネットサービスへの不正ログイン	8位	IoT機器の脆弱性の顕在化	7位
2位	ランサムウェアによる被害	9位	脆弱性対策情報の公開に伴う悪用増加	4位
9位	IoT 機器の不適切な管理	10位	不注意による情報漏えい	12位

31頁～36頁

20頁～30頁

14頁～19頁

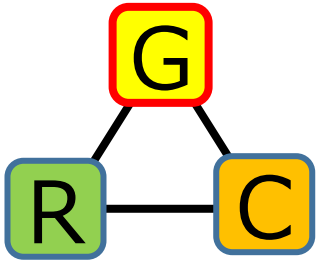
出典：独立行政法人情報処理推進機構

おなじみの「標的型攻撃による被害」が上位、「サプライチェーンリスク」が躍進して4位
「内部不正」も順位を上げています。今日はこの3つに関連したお話しといたしましょう

内部不正からの教訓　＝　ガバナンス (Governance)

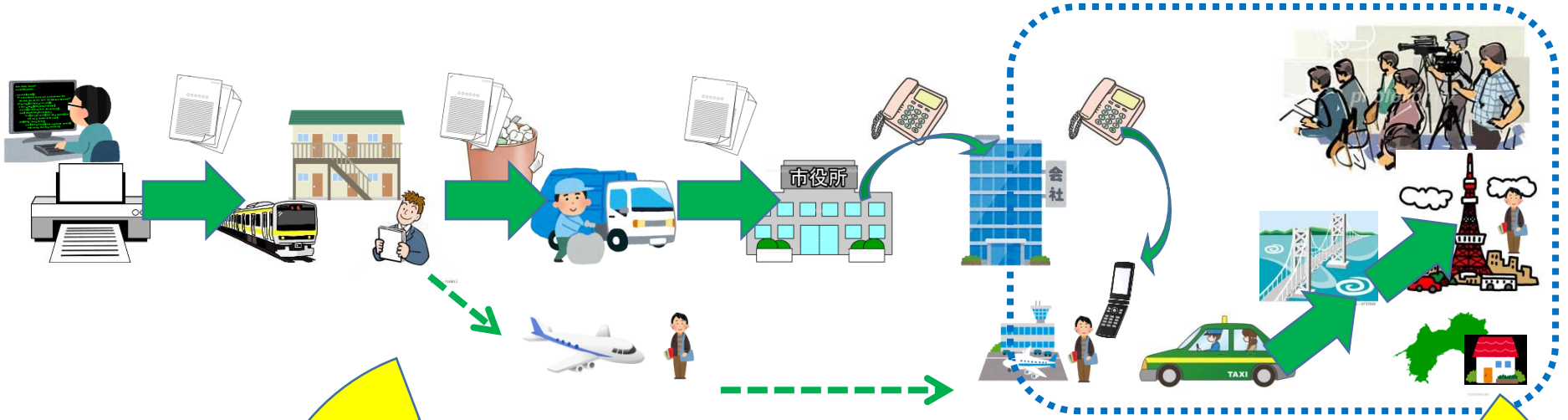
内部不正

リスク管理手法　Governance　Risk Management　Compliance　・・・　GRC



不注意による情報漏洩

1990年代



教訓として同社にて残されているものと、継続して守られているもの

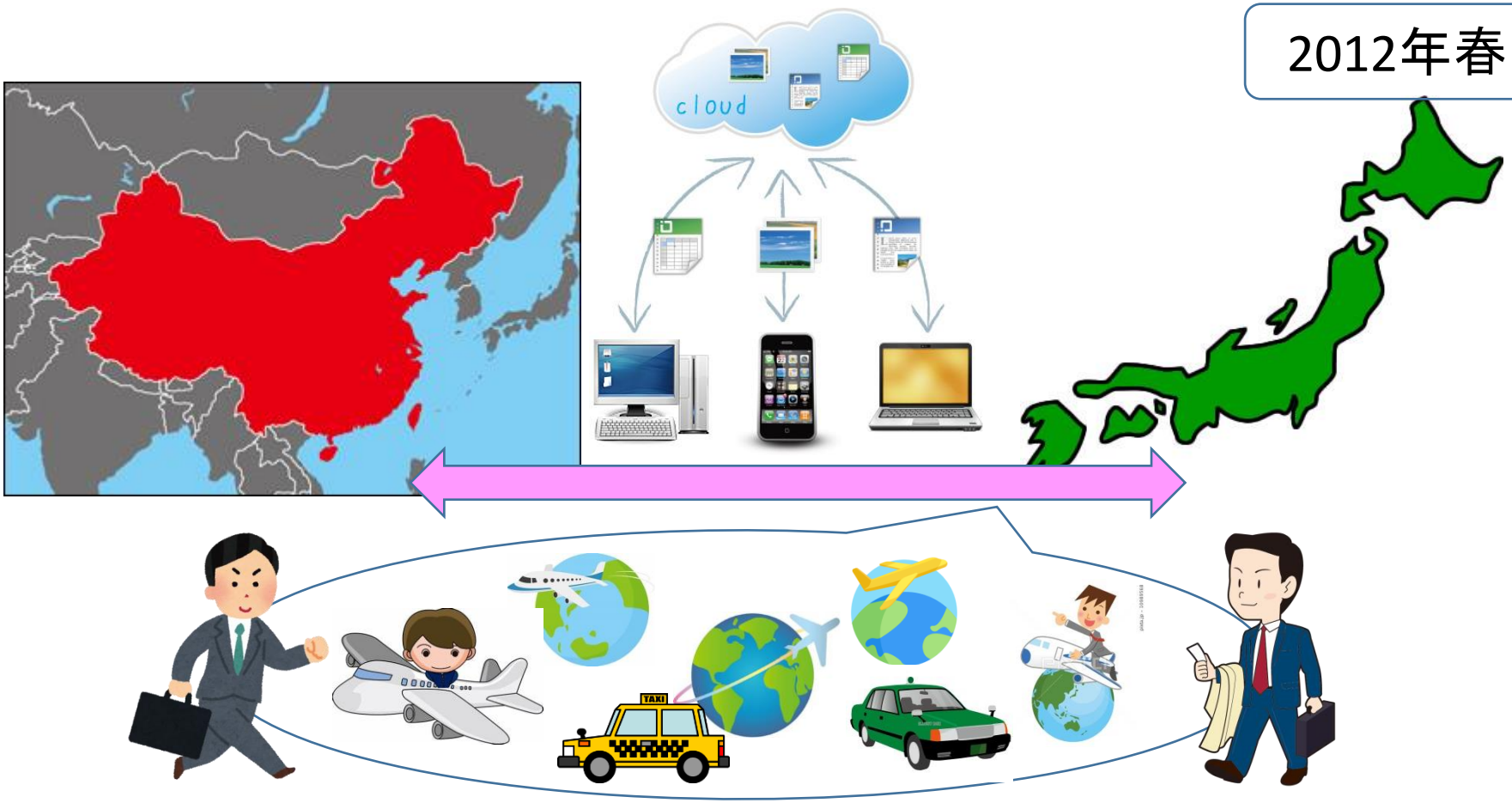
非買冊子

社内掲示

初動が早く的確であった

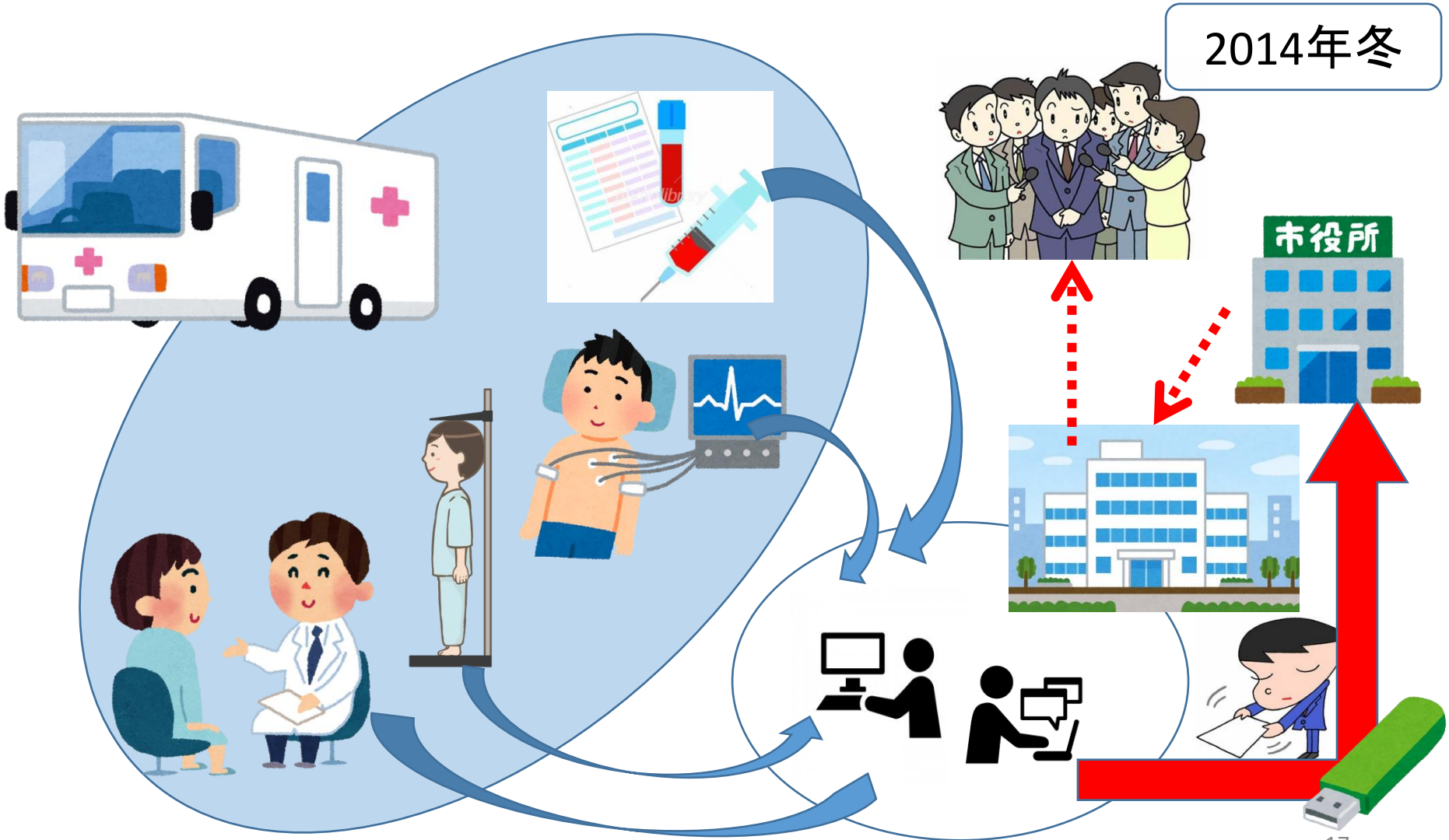
オンラインストレージを利用した内部不正

2012年春



ガバナンスを強化して、オンラインストレージの使用禁止、
必要に応じて約款による外部サービスの利用手続

悪意ある退職者による個人情報漏洩



内部不正により受ける事業体への影響

組織内部の従業員や元従業員により、私怨や金銭目的等個人的な利益享受のために組織の情報が持ち出され、公開・売買することで組織が損害を被ることがあります。また、組織の情報持ち出しのルールを守らずに不正に持ち出し、その情報を紛失することで情報漏洩等につながってしまいます。

これら内部不正が発覚すると、社会的な信用失墜につながり、組織は大きな損害を被ることとなります。

◆対策

資産の把握、重要情報の管理・保護（アクセス制御、暗号化等）、アカウント／権限の管理・定期監査等が挙げられます。

◆想定されるリスク

内部不正による犯行は何処の組織においても起こりうるものです。職員の不満や人間関係の問題が大きくなると発生リスクは高まります。上記技術的対策に加え、職員の不満を溜めない環境づくり等の予防対策についての検討も有用です。

情報セキュリティ10大脅威2019の解説

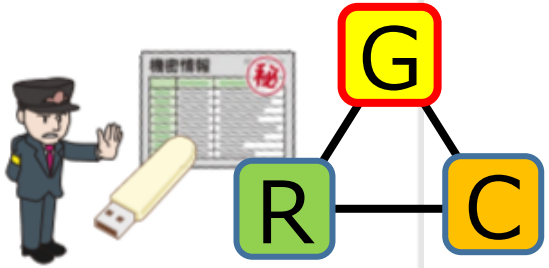
【5位】内部不正による情報漏えい

～不正を許さない管理・監視体制を～

IPA

- **対策**
  - **経営者、管理者**
    - ・被害の予防
      - －基本方針の策定
      - －情報資産の把握、体制の整備
      - －重要情報の管理、保護
    - ・情報モラルの向上
      - －人的管理、コンプライアンス教育徹底
    - ・被害の早期検知
      - －システム操作履歴の監視
    - ・被害を受けた後の対応
      - －CSIRT、警察等への連絡
      - －影響調査および原因の追究、対策の強化
      - －内部不正者に対する適切な処罰実施

この部分は追記です



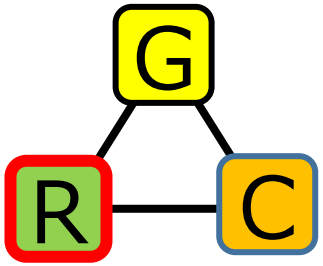
ガバナンス
Governance

出典：独立行政法人情報処理推進機構

サプライチェーンリスク ＝ リスクマネジメント (Risk Management)

サプライチェーン

リスク管理手法 Governance Risk Management Compliance ・・・ GRC



サプライチェーン：業務の一部を系列企業やビジネスパートナー等へ外部委託することは一般的となっていて、このような外部委託者が関与する供給の連鎖を「サプライチェーン」と言います。

リスク：委託先で発生する情報セキュリティに関するリスクの管理、委託元から要求される情報セキュリティに関するリスクを言います。

委託先情報セキュリティインシデント事例

委託先での情報漏えいの事件・事故の事例として、2018年3月に公表された「日本年金機構」の事例

1.インシデント概要

2017年８月、日本年金機構が情報処理会社に委託した約500万人分の個人情報データの入力業務について、情報処理会社は再委託を禁じられているのにも関わらず、中国の業者にデータの一部を渡して入力業務の再委託を行っていました。

委託作業（入力業務）に誤りが多く、2018年2月の年金支給において必要な手続きをしたのに控除を受けられなかった受給者が約6万7千人発生しました。日本年金機構は2018年2月13日付で「平成30年2月の老齢年金定時支払における源泉徴収税額について」という文書を発表し、一部の年金受給者の源泉徴収税額に誤りがあったことを認め、委託業者の入力内容については全件を点検・精査するとしており、調査の中で、再委託の実態が分かりました。

2.情報漏洩の恐れがある情報

(1) 対象　2017年(平成29年)8月 扶養親族等申告書・個人番号申出書提出者
(2) 流出の可能性のある人数　約500万人
(3) 流出の可能性のある情報　氏名、マイナンバー、配偶者の年間所得額

3.本事案を踏まえた必要な対応

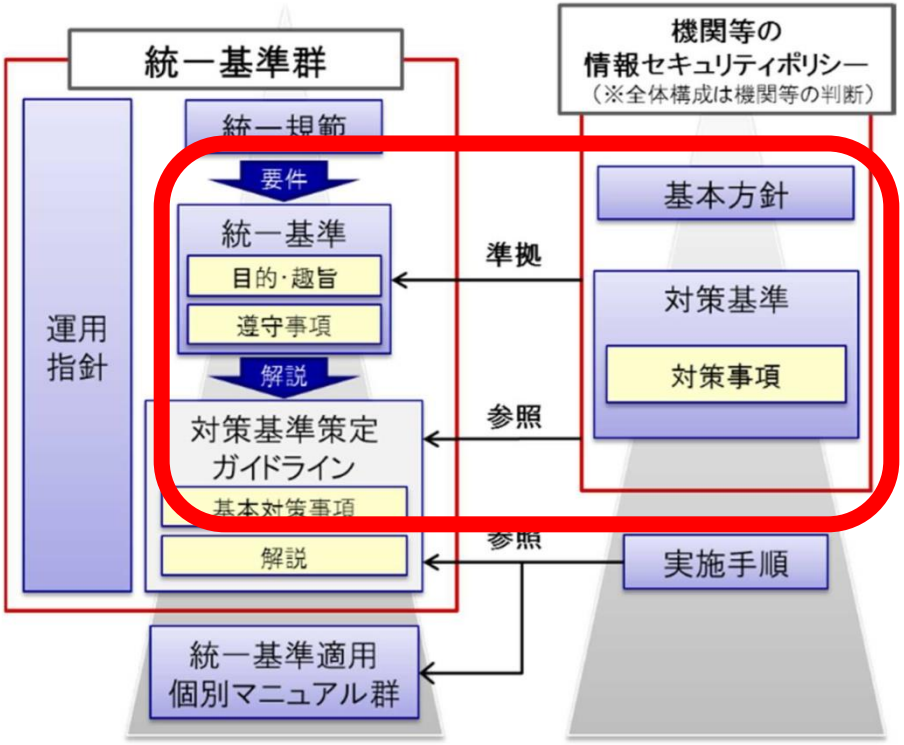
上記は、委託先からの再委託(再々委託)を禁じる契約書を締結していたにも関わらず、再委託が発生した事例です。違反行為の早期発見や、是正措置を行うため、情報セキュリティ上の要求事項を定めるだけでなく、要求事項が正しく遵守されているかの確認を定期的に行うことが必要です。

外部委託の情報セキュリティ確保の規程

政府機関等の対策基準策定のためのガイドライン（平成30 年度版）によると、「国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）は、「政府機関等の情報セキュリティ対策のための統一基準」（以下、「統一基準」という。）に定める遵守事項等の規定を満たすよう、具体的な対策事項を対策基準に規定する必要がある。」と記載されており、この要求に従い各事業体の情報セキュリティに関する規程は、統一基準に準拠する形で定められています。

外部委託時における対策については、統一基準内の「第4部 外部委託」に定められているため、これに沿ったセキュリティ対策基準を定める必要があります。

各事業体においては、外部委託時における対策が情報セキュリティポリシーに規定として定められている必要が有ります。



「政府機関等の情報セキュリティ対策のための統一基準」は
45ﾍﾟｰｼﾞ **システム調達** にてふれさせていただきます

出典：内閣サイバーセキュリティセンター(NISC) 政府機関等の対策基準策定のためのガイドライン（平成30 年度版）

委託先での情報セキュリティ確保の方法

情報処理業務を外部委託により行う場合には、以下の流れでセキュリティの確保が行われます。

(1) 外部委託の可否の判断

- 対象情報処理業務について、外部委託により行うことの可否を判断する

(2) 委託先の選定

- 調達において事業の安定性・情報セキュリティ対策の遂行能力から委託先を選定する

(3) 実施する情報セキュリティ対策に関する合意

- 外部委託先が実施すべき情報セキュリティ対策に関し合意し、契約に含める

(4) 情報セキュリティ対策の実施

- 委託先が合意した情報セキュリティ対策を実施する

(5) 情報セキュリティ対策の履行状況の確認

- 委託先における情報セキュリティ対策の履行状況について確認を行う

(6) 是正措置

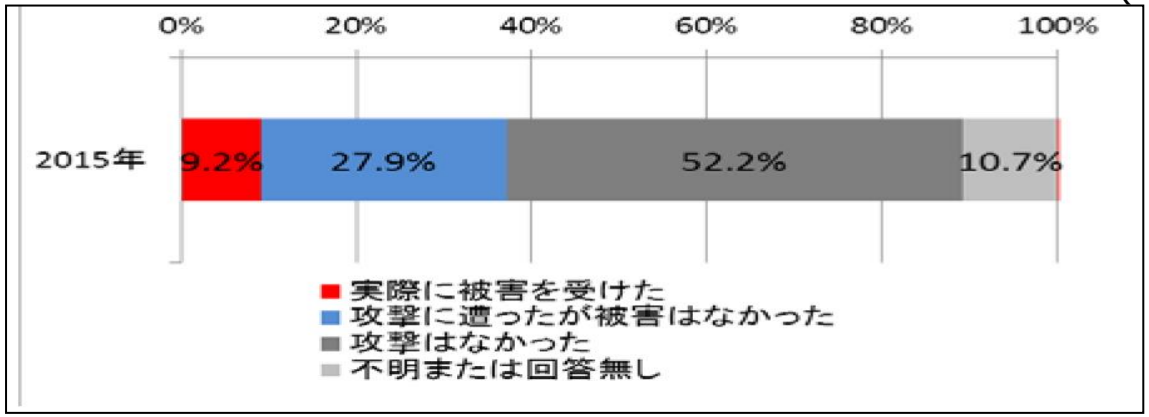
- 履行状況の確認の結果、必要であればこれを是正する

出典：内閣サイバーセキュリティセンター(NISC) 外部委託における情報セキュリティ対策に関する評価手法の利用の手引

Ver 2.0 実践のためのプラクティス集

サイバーセキュリティ経営ガイドラインとは

様々なビジネスの現場において、IT利活用は企業の収益性向上に不可欠なものとなっている一方で、企業が保有する顧客の個人情報や重要な技術情報等を狙うサイバー攻撃は増加傾向にあります。その攻撃手口も年々巧妙化しており、約４割の企業がサイバー攻撃を受けた経験があるという結果になっています。(下図)



サイバー攻撃（ウイルス以外）被害を受けた企業の割合

経済産業省とIPAにより
平成27年12月に策定
平成29年11月に改訂

想定読者
経営者・CISO・
CSIRT・セキュリティ担当者等

このようにサイバー攻撃への脅威が増す一方、多くの企業が十分な対策を取れているとは言えない状況です。
原因の一つに、セキュリティ対策に対して経営者が十分なリーダーシップを発揮していないことが挙げられます。
サイバー攻撃の脅威は、業務停止や情報漏洩等、企業・組織活動への影響が甚大となる可能性が高く、経営課題として経営層が率先して取り組む必要があります。つまり、**サイバーセキュリティの確保は、経営者が果たすべき責任のひとつであり、経営者自らがリーダーシップをとってサイバーセキュリティ対策を講じなければなりません。**

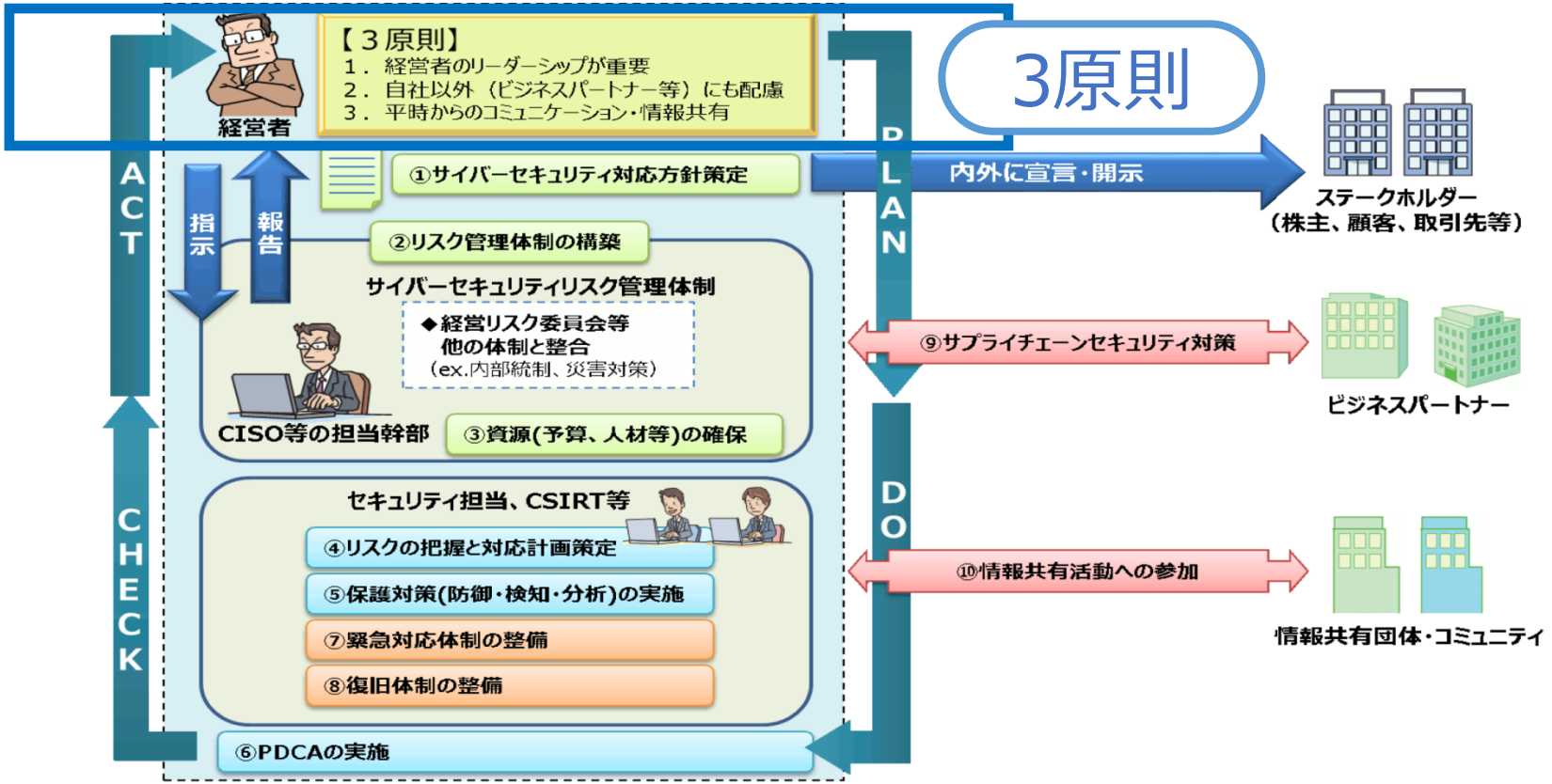
そこで、ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である経営者を対象に、**経営者が認識すべきサイバーセキュリティに関する原則や、経営者のリーダーシップによってサイバーセキュリティ対策を推進するため**に、経済産業省が独立行政法人情報処理推進機構（IPA）と協力して**策定されたものが、サイバーセキュリティ経営ガイドライン**となります。

出典：独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン」Ver 2.0

サイバーセキュリティ経営ガイドライン

経営者が認識すべき3原則と指示すべき「重要10項目」

サイバーセキュリティ経営ガイドラインでは、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3原則」と、**経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO等）に指示すべき「重要10項目(下図①～⑩)」がまとめられています。**この「重要10項目」を経営者はCISO等に対して、着実に実施させるとともに、実施内容についてCISO等から定期的に報告を受けることが必要となります。自組織での対応が困難な項目については、外部委託によって実施することも検討しなければなりません。



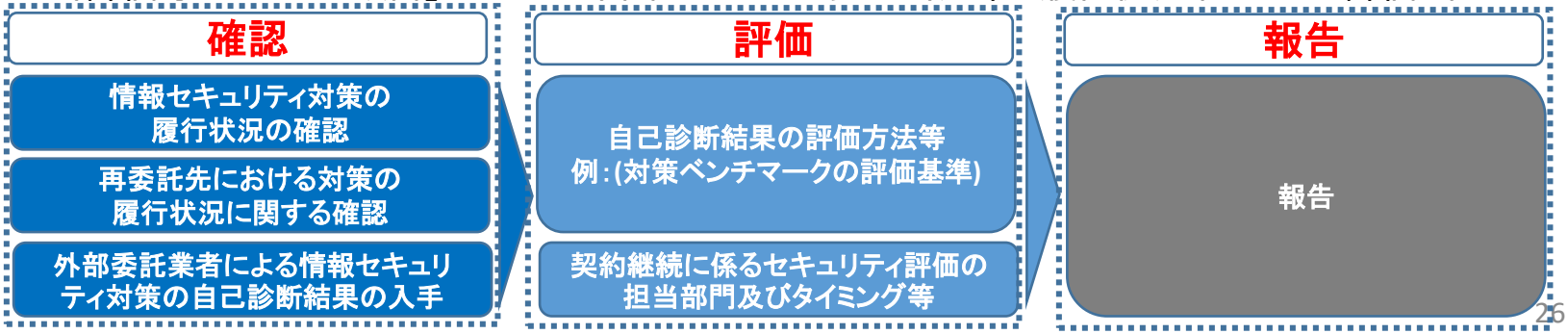
出典：独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドラインの概要」

サイバーセキュリティ経営ガイドライン

例、「重要10項目」の⑨サプライチェーンセキュリティ対策

	サイバーセキュリティ経営の「重要10項目」	政府統一基準　該当箇所	昨年度の事業体での取組
⑨	**ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握** ●サイバーセキュリティリスクのある委託先の特定 ●サイバーセキュリティ対策状況の把握 ➢系列企業、サプライチェーンのビジネスパートナーやシステム管理の委託先等のサイバーセキュリティ対策状況（監査を含む）の報告を受け、把握する。もしくは自ら定期的に確認する。	第4部 外部委託 4.1.1　(3) 外部委託における対策の実施 ➢契約に基づき、委託先における情報セキュリティ対策の履行状況を確認すること。	・外部受託業者等のセキュリティ管理および評価の実施（20nn年nn月～nn月）

重要情報を預ける委託先等においては、事業体と同等以上のセキュリティ対策を行ってもらう必要があります。
もし、委託先企業において適切なセキュリティ対策が行われていない場合、これらの企業等から、預託している重要情報が漏洩するなどの被害が発生することがあります。
事業体では、対策として契約前の委託先選定時におけるセキュリティ対策状況の評価と、契約期間中におけるセキュリティ対策の履行状況の確認を行います。契約期間中のセキュリティ対策の履行状況の確認については、「運用受託機関等のセキュリティ評価等に関する手順書」に基づき、下図のように、セキュリティ対策の履行状況確認及び、評価を行います。



外部委託において利用できる評価手法

① 情報セキュリティマネジメントシステム(ISMS)に関する適合性評価制度

・委託する業務で必要とされる情報セキュリティ対策の遂行能力が、要求する水準に到達していることを確認する。「委託先の選定」においては、委託先候補が情報セキュリティマネジメントシステムに関する適合性評価制度に基づく認証を取得していることを、選定における評価の要素に含めるなどで活用できる。

② 情報セキュリティ対策ベンチマーク

・委託先組織の情報セキュリティ対策の取組状況を把握するための評価手法(JIS Q 27001:2014 の付属書Aの管理目的及び管理策に基づいた評価項目)であり、情報セキュリティ対策を履行しているかどうかを確認する。基本的にはセルフチェック(自己申告)による評価であり、他の手法に比較して簡便に確認することが可能だが、虚偽の情報を受けとる可能性など、評価の精度が低い。（「対策ベンチマークチェックリスト」等を利用します）

③ 情報セキュリティ監査

・委託先の情報セキュリティ管理体制や管理策が要求事項を満たしていることや、情報セキュリティ対策を履行しているかどうかを、情報セキュリティ監査の手法を用いて確認する。

情報セキュリティ対策の履行状況の確認においては、業務における定常的な確認に加えて、委託先における当該情報処理業務を対象にした上記3つの何れかの方法により、情報セキュリティの確認を行います。

出典：内閣サイバーセキュリティセンター(NISC) 外部委託における情報セキュリティ対策に関する評価手法の利用の手引

委託先での情報セキュリティ対策の確認

各事業体では、システム運用やデータ取り扱いに関する業務について外部委託を行っています。世間では委託先での情報漏えいの事件・事故が多く発生しており、委託先監査の重要性が日々高まっています。また、情報漏えい等のインシデントの影響は、直接の被害組織だけでなく、複数の関係者や組織に影響を及ぼす可能性があり、看過できない課題となっています。

その為、委託を行う側の組織はこのような状況に対処するために、重要情報を取り扱う業務を外部委託で行う場合には、実施する情報セキュリティ対策に関する合意状況や、合意した情報セキュリティ対策の実施状況、さらに委託先における情報セキュリティ対策の履行状況などの確認を行い、各状況に対して情報セキュリティの確保が図られているかなどの評価を実施し、結果が不十分である場合は、速やかに是正させるといった対策を取ることが必要となります。

【ポイント】

情報セキュリティ対策においては、選定した委託先に対して、情報セキュリティ対策の履行状況などの評価基準に適合しているか定期的に見直しを行い不具合があれば是正処置を施すことが重要です。

サプライチェーンの弱点を悪用した攻撃の高まり

多くの組織で行われているウェブサイトや情報システムの運用には設備や人材が必要であり、外部の業者に委託することもありますが、このような環境で、委託先組織がセキュリティ対策を適切に実施していないと、攻撃者に狙われ、被害が発生することがあります。

例えば、委託先組織に個人情報等の重要情報を扱うウェブサイトの運用管理を委託している場合、委託先のサーバに個人情報等の重要情報が存在することとなります。この場合、委託先のサーバに不正アクセスを受けると、個人情報等の重要情報が搾取される恐れがあります。

◆対策

業務委託や情報管理における規則の徹底、信頼できる委託先組織の選定を行うことが挙げられます。

※ **「サイバーセキュリティ経営ガイドライン V2.0」**でも 経営者が認識する必要のある「3原則」および経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部に指示すべき「重要10項目」に サプライチェーンセキュリティ対策の推進が記載されております。

◆想定されるリスク

各事業体では多くの業務を外部委託している場合もあります。委託にあたっては業者選定の際の評価のみならず、契約期中のセキュリティ対策状況の確認も必要です。委託先による情報管理不備による情報漏えいを防ぐための管理を継続・改善して行く事が重要です。

情報セキュリティ10大脅威2019の解説

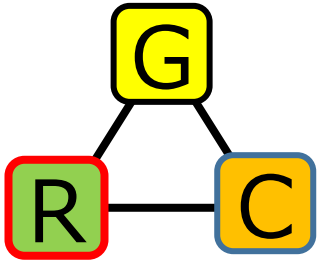
【4位】サプライチェーンの弱点を悪用した攻撃の高まり

IPA

～業務委託先にも適切なセキュリティ管理を要求～

- **対策**
  - **委託元組織**
    - ・被害の予防
      - –業務委託や情報管理における規則の徹底
      - –信頼できる委託先組織の選定
      - –委託先からの納品物の検証
      - –契約内容の確認
      - –委託先組織の管理
    - ・被害を受けた後の対応
      - –影響調査および原因の追究、対策の強化
      - –被害への補償

この部分は追記です



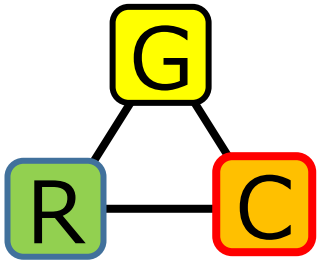
リスクマネジメント
Risc Management

出典：独立行政法人情報処理推進機構

標的型メール攻撃　＝　コンプライアンス（Compliance）

標的型攻撃

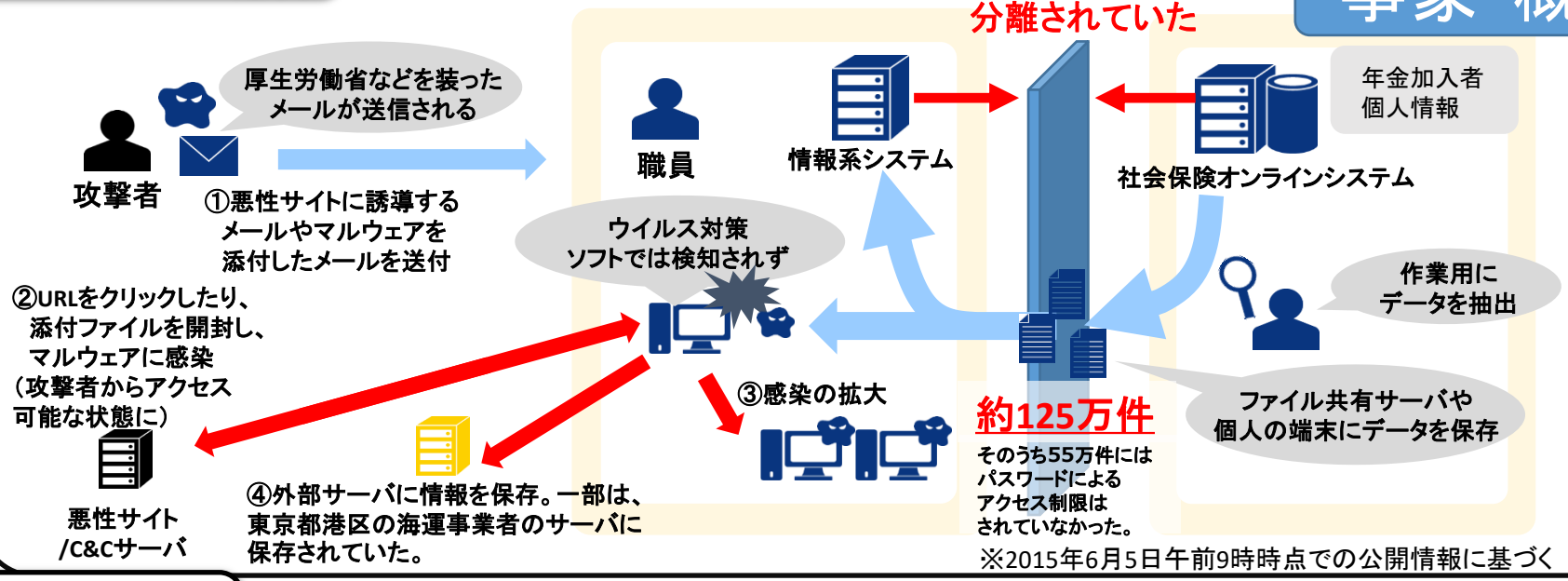
リスク管理手法　Governance　Risk Management　Compliance　・・・　GRC



日本年金機構における情報流出事案

インシデントの経緯

事象・概要



※2015年6月5日午前9時時点での公開情報に基づく

概要

外部からの不正アクセスにより、日本年金機構の年金情報管理システムサーバから個人情報が流出。大量に送信された悪意あるメールの添付ファイルまた外部リンクを日本年金機構の職員が開き、マルウェアに感染した。感染端末は、個人情報を含むサーバーに接続されていたもの。およそ125万件の個人情報が流出しました。

問題点

①マネジメントをはじめとする組織全体の**危機意識が欠けて**おりセキュリティの徹底が図られていませんでした
②職員による不審メール開封の問題が適切に**エスカレーションされなかった**ため、被害が拡大しました
③個人情報を**暗号化せずに**保管していました、**多くの職員のコンプライアンス違反が問題点です。**

日本年金機構における情報流出事案 発生・経緯

年金情報管理システムにおける125万件の個人情報流出事案

「標的型メール」での攻撃

・2015年(平成27年)5月8日　：「厚生年金基金制度の見直しについて（試案）に関する意見」
　⇒端末1台が不正プログラムに感染、不審な通信が発生、約4時間後に端末の通信ケーブルを抜線、その後不審な通信は有りません
　この時点で「個人の業務用メールアドレス一覧が漏洩」しています

・5月18日　・・・・・・・・・・・・・　：「給付研究委員会オープンセミナーのご案内」
　⇒端末3台が不正プログラム感染、不審な通信が発生したが接続先への通信は失敗
　「担当部署の実在者名がメール本文中に記載」されています

・5月18日～19日　・・・・・・・・　：「厚生年金徴収関係研修資料」
　⇒不審な通信は発生しない

・5月20日　・・・・・・・・・・・・・　：「医療費通知」
　⇒20日午後、端末1台が不正プログラムに感染、不審な通信が発生。数時間以内に他の6台の端末からも不審な通信が発生。21日～23日にかけて合計21台の端末から国内他のサーバへ多数の通信が発生。「未開封者の端末へ感染拡大」

・5月21日　⇒「年金情報管理システムにおける125万件の個人情報流出」が始まる

・5月23日　⇒「ネットワークの遮断実施」

出典：「不正アクセスによる情報流出事案に関する調査結果報告」

この時、既にネットワークは分断され、ルール上インターネットセグメントに必要に応じてデータを置くときは、暗号化して保存することが義務付けられていました

日本年金機構における情報流出事案 調査・勧告

事案発生から厚生労働省に対するNISCからの「勧告」

「内閣での対応」

・2015年(平成27年)8月20日
　機構不正アクセスによる情報流出事案に関する調査委員会が
　⇒「不正アクセスによる情報流出事案に関する調査結果報告」

・同日
　サイバーセキュリティ戦略本部が
　⇒「日本年金機構における個人情報流出事案に関する原因究明調査結果」

・8月21日
　日本年金機構における不正アクセスによる情報流出事案検証委員会が
　⇒「検証報告書」

・9月4日
　閣議決定
　⇒「サイバーセキュリティ基本法」
　(平成26年法律第104号)第12条第1項の規定に基づくサイバーセキュリティ戦略

・9月11日
　菅官房長官（戦略本部長）が
　⇒厚生労働大臣に対して、戦略本部の原因調査結果等を踏まえた「勧告」

10月1日に日本年金機構においては理事長を本部長とする「日本年金機構再生本部」「情報管理対策本部」を設置、12月9日に「日本年金機構業務改善計画」を公表しました

日本年金機構における情報流出事案 対策・取組

「厚生労働省での対応」

「勧告」に対する厚生労働省における取組

・2015年(平成27年)9月25日
　厚生労働大臣から日本年金機構理事長に対する業務改善命令
・2016年(平成28年)6月21日
　サイバーセキュリティ・情報化審議官を設置
　サイバーセキュリティ担当参事官室及び情報システム管理室を設置
　⇒厚生労働省及び独立法人等で発生した情報セキュリティインシデントに対応して、情報セキュリティ対策に関する省全体の司令塔の機能を担うことになります
・ 8月26日
　厚生労働省と日本年金機構が連携して、日本年金機構における情報セキュリティ対策を恒久的に推進するため、「情報セキュリティ対策連絡会議」に「情報セキュリティ対策連絡会議ワーキンググループ」を設置、厚生労働省と日本年金機構双方の最高情報セキュリティアドバイザーを含めた会議体を設置しました
　⇒以降、具体的対策がこれまでより円滑に進むよう体制が見直されました！！
・8月30日
　「平成28年から31年度厚生労働省セキュリティ・IT人材確保・育成計画」策定
・10月21日
　厚生労働省情報セキュリティポリシーと関係規程を見直し、所管法人に対し情報共有
　⇒「厚生労働省所管法人における情報セキュリティ対策推進会議」で厚労審より

厚生労働省における日本年金機構及び独立法人に対する取組を実施しました

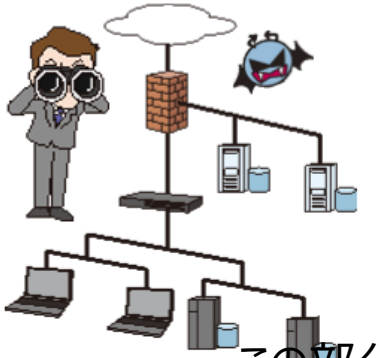
情報セキュリティ10大脅威2019の解説

【1位】標的型攻撃による被害

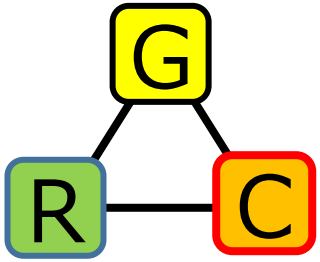
～標的型攻撃メールの多くはOffice文書ファイルを悪用～

IPA

- 対策
  - システム管理者
    - ・被害の予防
      - –セキュアなシステム設計
      - –アクセス制御・データの暗号化
      - –ネットワーク分離
    - ・被害の早期検知
      - –ネットワーク監視・防御
      - –エンドポイントの監視・防御
  - 従業員、職員
    - ・情報リテラシーの向上
      - –セキュリティ教育の受講
    - ・被害を受けた後の対応
      - –CSIRTへ連絡



この部分は追記です



コンプライアンス
Compliance

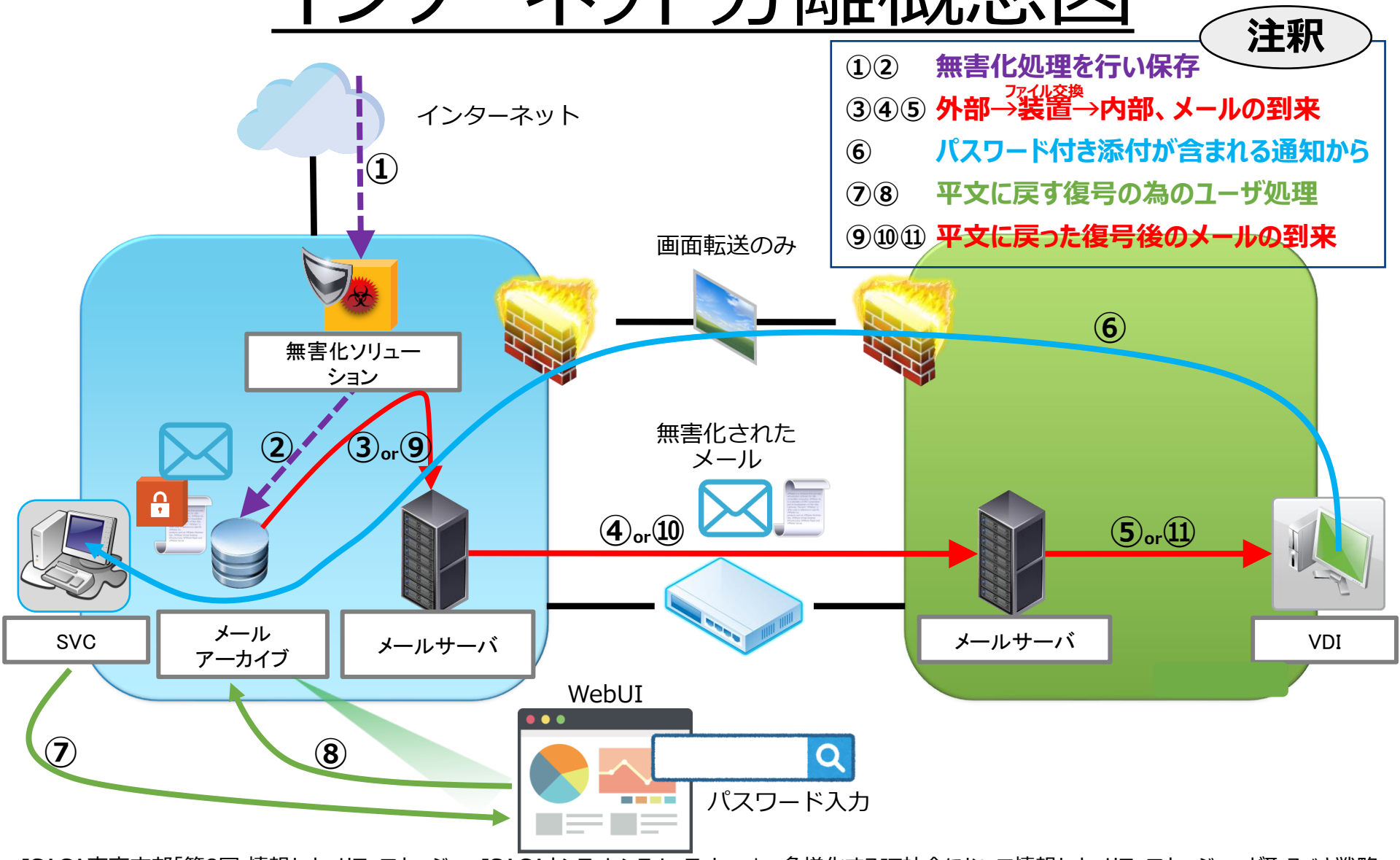
出典：独立行政法人情報処理推進機構

ネットワーク分離と利便性の共存

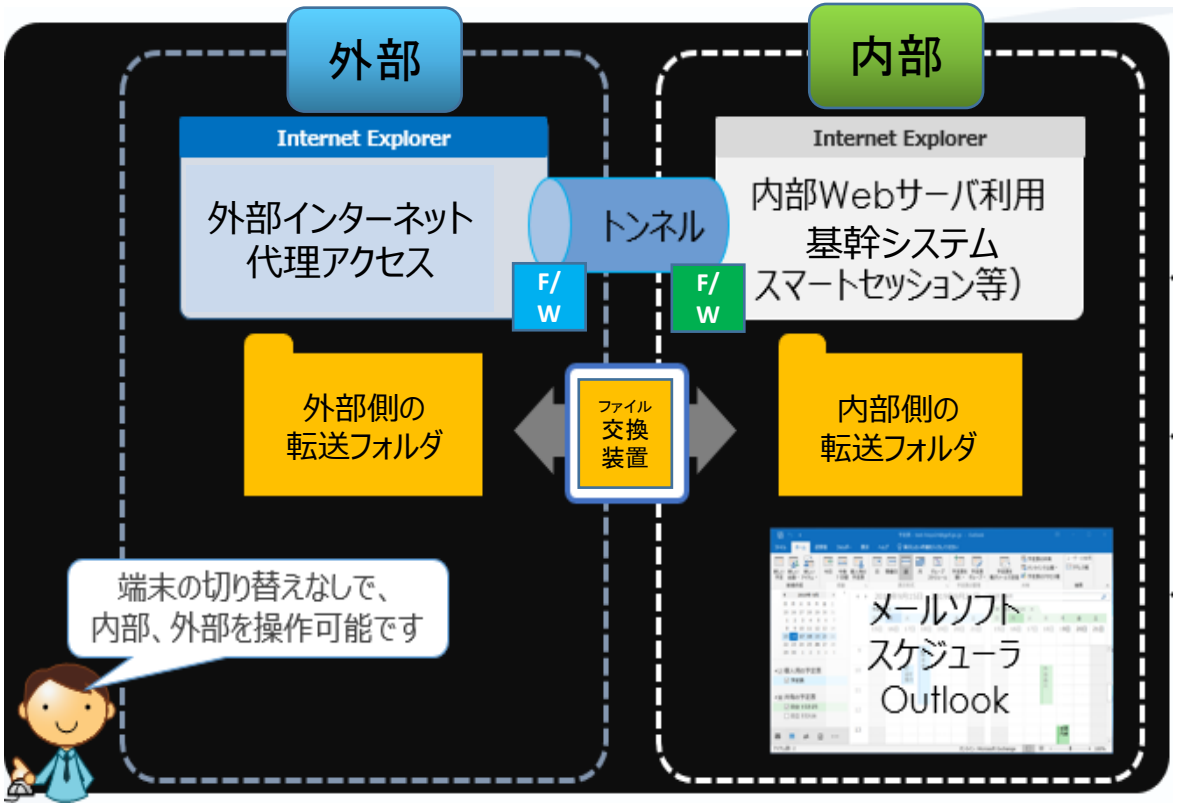
分離と利便性

- 標的対象端末でメールを取り扱わない
  - メール・基幹業務・ファイルサーバは同時に利用したい
  - 一元的に使いたい
    - 自動検疫を行い、内部セグメントでメールを取り扱う
    - 外部URL接続は外部環境を画面転送で内部で見る
    - ・・・

インターネット分離概念図



仮想化端末での画面表示イメージ図



←外部のインターネット閲覧は
ビューアーにより画面データの
み転送され表示されています

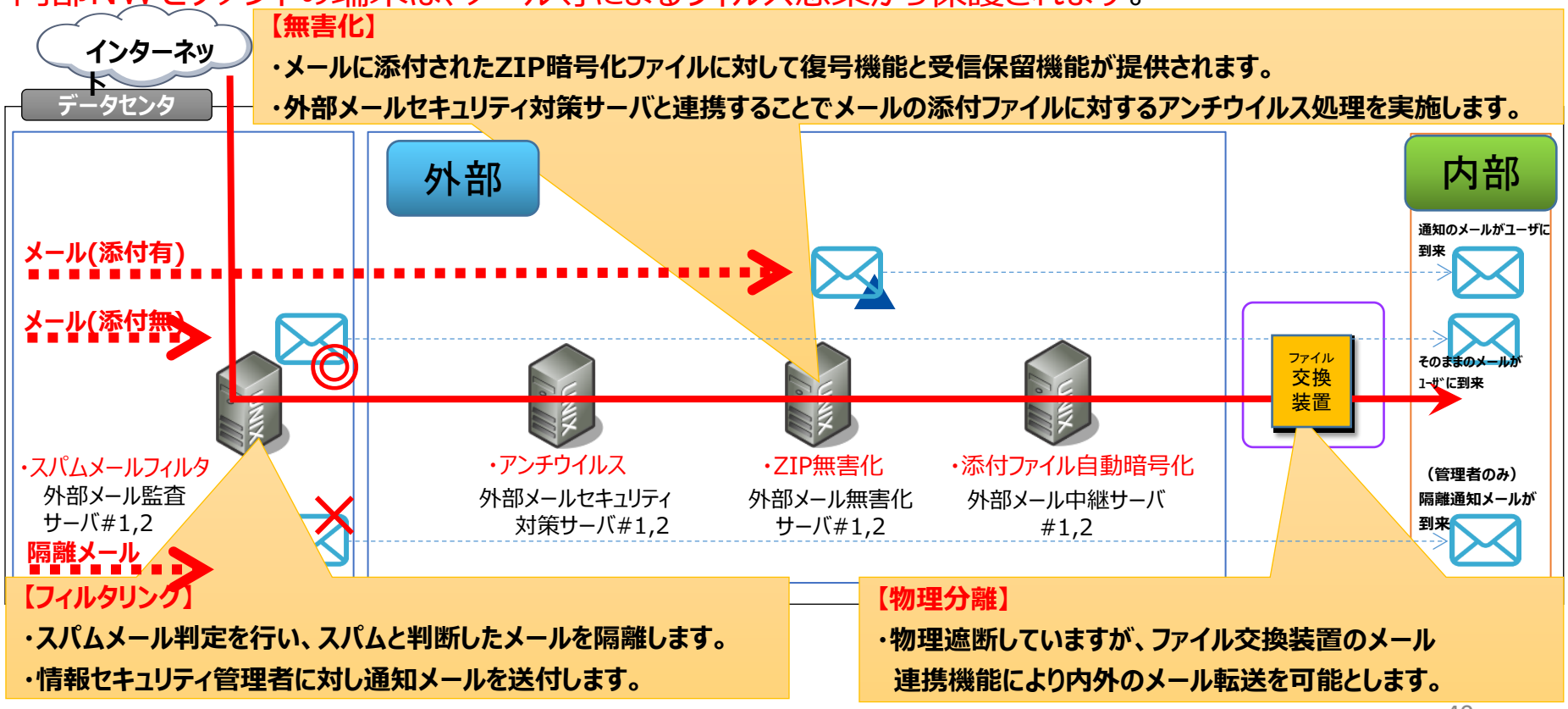
←添付ファイルを含めてメールは全て
必ずファイル交換装置を経由します。

←内部だけで利用され外部から
直接見えません。

トンネルはビュアーだけが通過し、データ伝送は行えない設定です
ファイル交換装置は、瞬間的に内部又は外部何れにしか接続されません(HTTPは切れています)

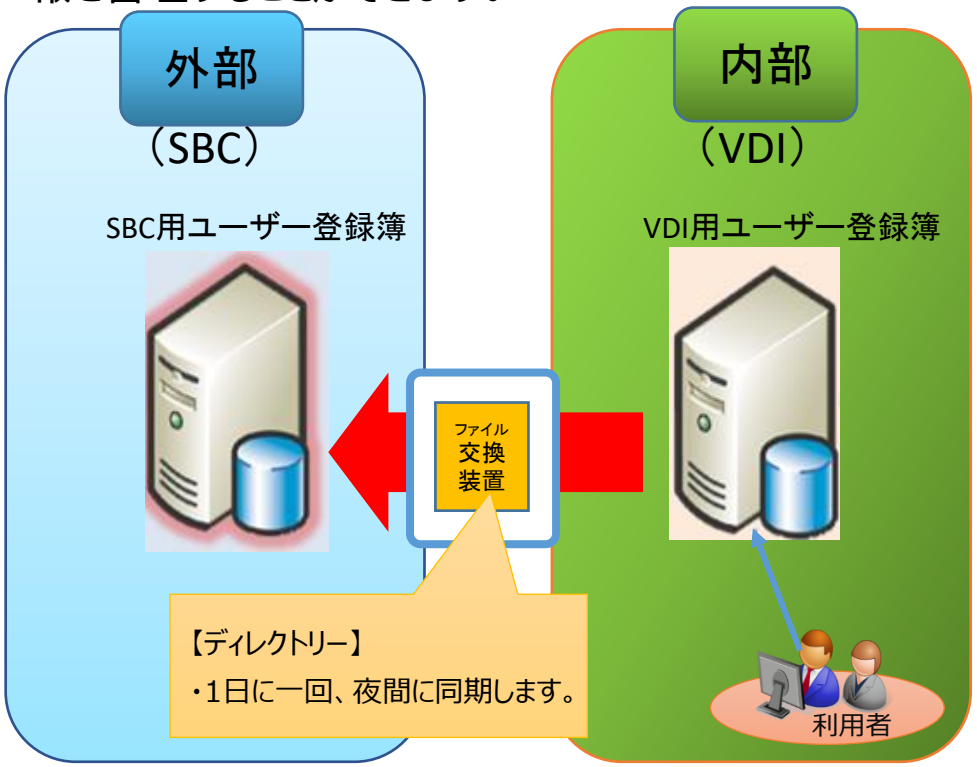
受信メールが保留隔離された場合の対応

前頁のインターネット分離概念図の手法により、外部と内部のネットワークの完全分離が実施されています。
ウイルス感染メールやなりすまし等の怪しいメールは利用者に到達前に外部NWセグメントで検疫されます。
外部NWセグメントで検査され安全性が確認されたメールのみファイル交換装置経由で内部NWセグメントの利用者へ到達します。
内部NWセグメントの端末は、メール等によるウィルス感染から保護されます。



統合ユーザ管理と利用時の対応

外部LDAPマネージャ/LDAPデータベース機能は、ファイル交換装置の転送スケジュールに従い、内部ネットワークユーザ情報(LDIFファイル)を取得します。取得したユーザ情報を外部LDAPデータベースサーバと外部LDAPマネージャサーバを経由し、外部ディレクトリサーバに連携することで、内部ネットワークと同一のユーザ情報を管理することができます。



【内外PWがリアルタイム連携しない理由】

キーワード

- ユーザは内外のPW変更を一回で行いたい
- ディレクトリーは内外個別に保持しています
- 特殊なファイル構造をファイル交換装置にて渡されます
- 関連するサーバに若干のディレイが発生します
- 業務中に外部にPWが反映されるタイミングにおける混乱を避けます
- 外部への変更タイミングを夜間一回として整合性を保つこととします

ユーザのアクセス権管理情報を一元管理することにより、絶えず正しい情報が保持されます。
運用の利便性を高めて、常に正しい人員情報を元にセキュリティが保たれた運用が実現できます

端末を持出しして外部で使用する場合

端末持出しには利用申請書による持出し申請が必要となります。
端末の種類が例えば以下のような場合の手続きは個別に異なります。

①持出し用FAT端末 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・**主として機内でのオフラインにおける報告書作成等**

SIMカード実装

【外部利用のルーター】
・自宅のルーター・WiFiスポット・ホテルWiFiの利用は禁止とします。

②自席シンクライアント端末 **・・・主としてテレワーク等**

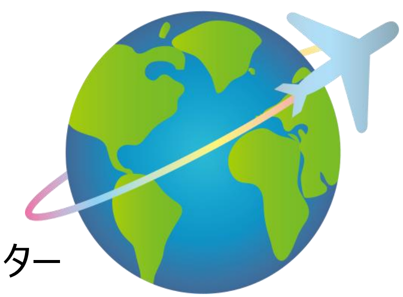
＋ **国内用** モバイルルーター

③持出し用シンクライアント端末

SIMカード実装

国内利用 ／ 海外利用

＋ **海外用** モバイルルーター



海外での利用については、海外出張時の所定の手続きに従い、海外用モバイルルーターを空港でレンタルして使用します。

・必ず事業体が配布したモバイルルータを利用します。配布したモバイルルータ以外利用してはいけません。
・万一の紛失時には、利用者が速やかにリモートワイプの手続きを行います。（FAT端末の場合のみ）

分離・統合ユーザ管理・持出での残存リスク

強固な多層防御

仮想化の技術を利用すると内外のネットワークを分離して、更に

①メールは検疫されて、しかも外部に接続されていない環境で運用することが出来ます。

②内部で見ているメールに外部URLが有るときは、外部ブラウザが起動し外部で取り扱います。

ネットワークを介した感染で一番多い①と②に対して、多層防御が施されます。

残存リスク

運用上の利便性を加味して、

③ユーザの使い勝手の良さを考慮して一部の添付ファイルの運用をユーザに委ねる場合が有ります。

その手順をルール通りに全てのユーザが守り、正しい手順で運用を行う事が何よりも重要です。

④ルータの利用は貸与及び海外出張での利用については、事業体が事前に手配しているルーターを国内で受取、出先の海外で使用する事を定めます。

⑤VPNでも完全なセキュリティ確保が保たれる保証はありません。信頼できるキャリア及びVPNの利用に努めます。(自宅のルーター・WiFiスポット・ホテルWiFiの利用は禁止といたします。)

全体への影響

一人又は一台の端末のウイルス感染は、ネットワーク全体に及びます。ルールを厳守した運用を心がけることが必要です。感染抑止及び感染範囲の最小化のための仕組みは出来ますが、ユーザがルールを逸脱した運用を行った場合の感染は発生します。

システム調達におけるセキュリティ要件

システム調達

- 官と民の調達方法の違い
  - 民は官とは異なる方法です
  - 官は手続きが多い
    - 限られた予算において執行する必要があります
    - 但し、ブランド・メーカー指定はできません
    - 競争の原則が過剰装備になります
    - ・・・

以下Ⓐ～Ⓜの表記は参考文書（文末にURLを表記しています）

A「政府機関等の情報セキュリティ対策のための統一基準」

22ﾍﾟｰｼﾞでも記載 サプライチェーン

国の行政機関及び独立行政法人等は、統一規範及びその実施のための要件である統一基準に準拠するとともに、ガイドラインを参照しつつ、組織及び取り扱う情報の特性等を踏まえて情報セキュリティポリシーを策定します

サイバーセキュリティ基本法（平成26年法律第104号）（抜粋）

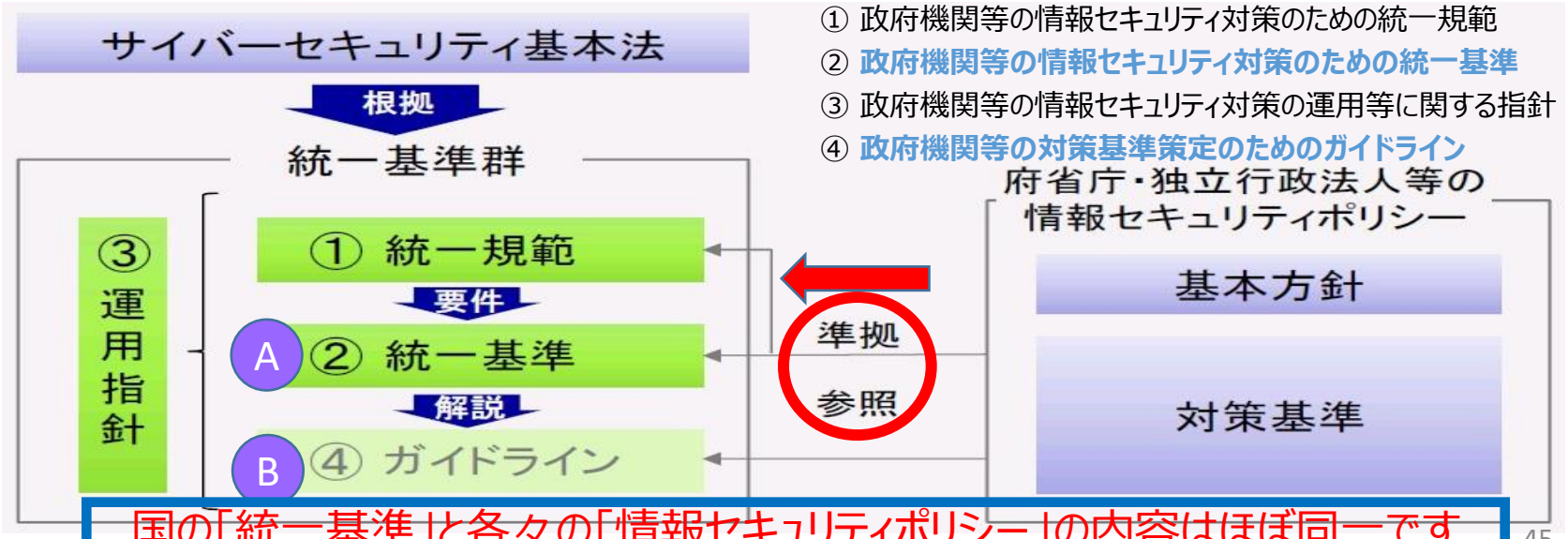
第二十五条サイバーセキュリティ戦略本部は、次に掲げる事務をつかさどる

二　国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること

政府機関等の情報セキュリティのための統一規範（抜粋）

第四条機関等は、自組織の特性を踏まえ、基本方針及び対策基準を定めなければならない

3　対策基準は、別に定める政府機関等の情報セキュリティ対策のための統一基準と同等以上の情報セキュリティ対策が可能となるように定めなければならない



国の「統一基準」と各々の「情報セキュリティポリシー」の内容はほぼ同一です

B「政府機関等の対策基準策定のためのガイドライン」

- 第1部　総則
  - 用語の定義等
- 第2部　情報セキュリティ対策の基本的枠組み
  - 組織・体制・規定・例外措置・教育・インシデント・点検
- 第3部　情報の取扱い
  - 格付・区域・バックアップ
- 第4部　外部委託
  - 外部委託・約款による外部サービスの利用・クラウドサービスの利用
    - SaaSは約款による外部サービス、IaaS,PaaSはクラウドサービス(セキュリティ要件を調達者が決める)
- 第5部　情報システムのライフサイクル
  - 企画・要件定義・調達・構築・運用・保守・更改・廃棄・運用継続計画
- 第6部　情報システムのセキュリティ要件
  - 認証・アクセス制御・権限・ログ・脅威（脆弱性、不正プログラム、攻撃）
- 第7部　情報システムの構成要素
  - 端末・サーバ・電子メール・ウエブ・DNS・通信回線（リモート、無線含）
- 第8部　情報システムの利用
  - 利用に係る規定の整備・暗号・感染防止・支給以外の端末利用

1部～4部は組織に対して1個、5部～8部はシステム単位で複数で対策を策定します

「IT調達に係る国の物品等又は役務の調達方針及び調達手続きに関する申合せ」

C

- 発行元、発行日
  - NISC、2018年(平成30年)12月10日
- 目的
  - 政府の重要業務に係る情報システム、機器、役務等の調達に置けるサイバーセキュリティ上の深刻な悪影響を軽減するための新たな取組が必要
- 対象とする調達
  - より一層サプライチェーン・リスクに対応することが必要であると判断されるもの
- 参照すべき基準等

A

  - 平成30年度版の「政府機関等の情報セキュリティ対策のための統一基準」
    - 2018年(平成30年)7月25日サイバーセキュリティ戦略本部決定
      - 同基準「第4部　外部委託」
      - 同基準「第5部　情報セキュリティのライフサイクル
    - 情報セキュリティ対策の内容は「政府機関の情報セキュリティ対策のための統一基準」に、各府省庁が守る最低限の対策水準を定めるが、セキュリティ要件を調達仕様に具体的かつ適切に組み込むための手法を記載しているわけではありません
- 調達するシステムがクラウドサービスを含む調達の場合

J

  - 2018年(平成30年)6月7日各府省情報化統括責任者(CIO)連絡会議決定「政府情報システムにおけるクラウドサービスの利用に係る基本方針」を考慮

「情報セキュリティを企画・設計段階から確保するための方策に係る検討会報告書」

D

- 検討の背景
  - 上流工程で決 めなければならない事項が複雑化かつ増加してきています
  - E 平成15年には「電子政府 構築計画」を策定
  - 平成18年には業務・システムのその時点におけるあるべき姿への 到達を計画的に推進するための指針として「業務・システム最適化指針（ガイドライン）」を策定 F
  - G 平成19年には、「情報システムに係る政府調達の基本指針」が策定
  - 非機能要件のうち特にセキュリティ要件は曖昧、過不足な調達となることが多い
  - 結果としてシステムの実態によらず全網羅的な過剰なセキュリティ対策や設計・開発工程での 手戻り、運用開始後のセキュリティ事故等の問題を生じさせる可能性があります
  - 企画段階から情報セキュリティ対策を考慮し、セキュリティ要件を適切に組み込むことが必要不可欠です
  - H 「情報セキュリティを企画・ 設計段階から確保するための方策（SBD: Security By Design）に係る検討会」において、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」等 がとりまとまりました

政府機関の情報システム調達に係る課題抽出

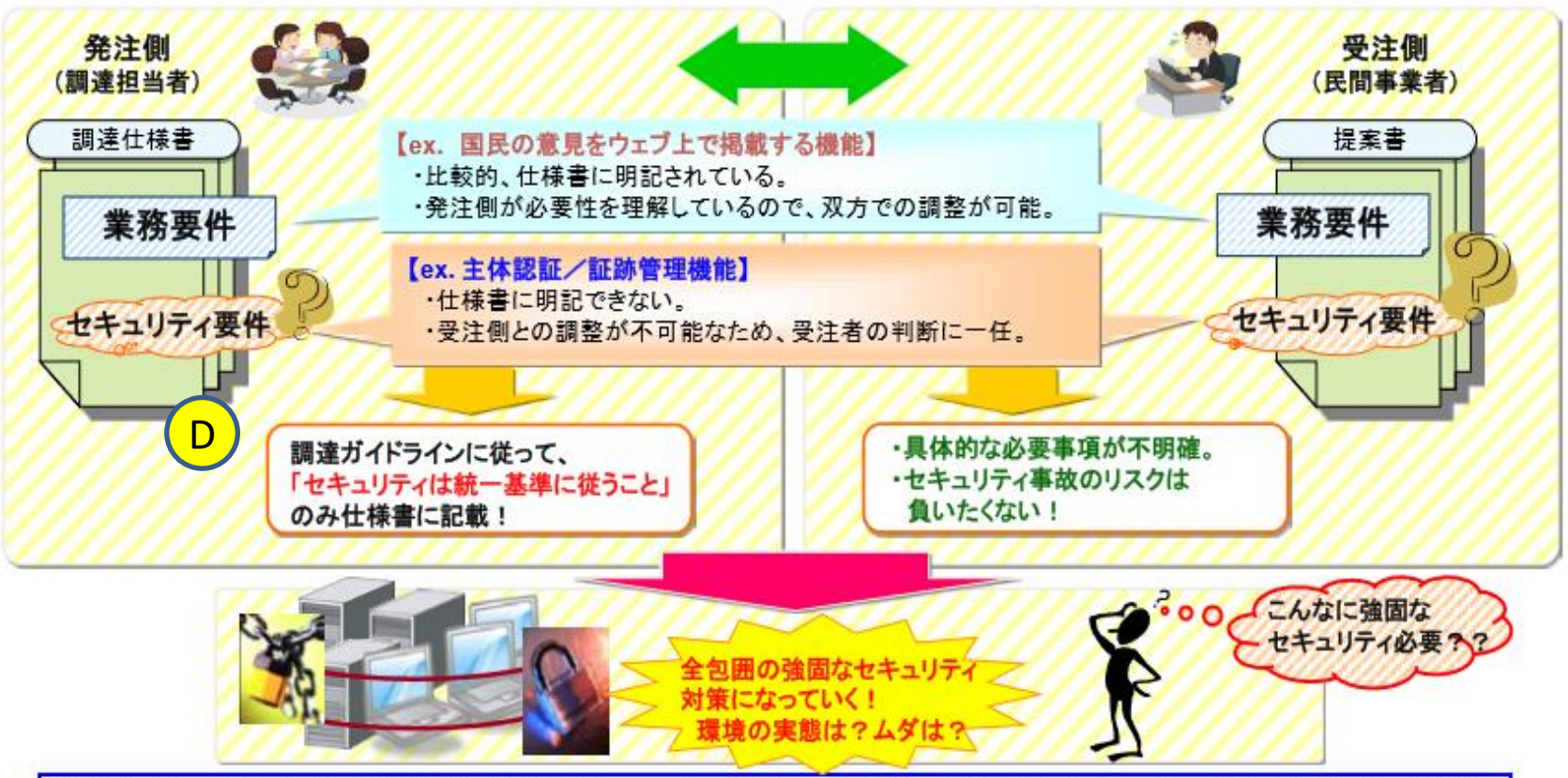
- 情報システムの発注側である政府機関及び受注側である民間事業者の双方で３つの現状が明確となった
  - 発注側の政府機関の政府職員（調達担当者）は必ずしも情報システムの専門家 ではない
  - その結果、情報システムの調達、工程管理、運用などを自立して行うことが困難になる（情報セキュリティにおいても想定される脅威に対応した具体的かつ適切なセキュリティ要件策定が困難になる）
  - 一方で、受注側としてシステムを供給する民間事業者は、調達仕様が不明確であるため、適確な実装方法の提案が困難であり、また、要件解釈のばらつきから公平な競争の妨げにもつながる
- 曖昧な調達仕様を是正すること
- 情報システムの特性に応じて無駄がなくかつ現実の脅威に 効果的な情報セキュリティ要件を策定する必要があります
- 相互に不利益が生じた事例につい ては、「情報システム・ソフトウェア取引トラブル事例集」（2010 年 3 月経済産業省 委託事業）
- システムの特性に応じたリスク分析を不十分にし、セキュリティ事故発生時の責任回避の観点のみが重視され、全網羅的かつ過剰なセキュリティ対策や調達費用の増加を招く可能性があります

H

適切なセキュリティ要件定義が困難

課題

発注側の業務上に必要な機能（業務要件）は明快で、受注側との理解も比較的行いやすいが、
セキュリティ要件は理解・判断が困難。したがって、セキュリティ要件は曖昧な状態となることが多い。



適切なセキュリティ要件を仕様書上に明確化していないため、全網羅的で不明確なセキュリティ対策となる傾向があり、結果として調達費用の増加となる傾向に。

出典：内閣官房情報セキュリティセンター

H「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」

- マニュアルの概要 SBD:Security by design
  - 発注側の調達担当者が調達仕様書にセキュリティ要件を記載するための手順を定めます
  - 想定読者は、情報システムの調達を担当 する調達担当者及び情報システムを供給する事業者です
  - 調達仕様書に対する適切なセキュリティ要件の組み込み手法を確立します
    - 調達仕様書に記載すべきセキュリティ要件を調達担当者が自ら決定可能とする手法を検討することとしました

これが情報システムに係る政府調達におけるセキュリティ要件策定マニュアル＝SBDマニュアルです

H

SBDマニュアルの使い方

- SBDマニュアルの使い方
  - このマニュアルは、情報システムの調達プロセスにおける発注側の調達担当者が、調達仕様書にセキュリティ要件を記載するための手順を定め、作業を支援するものです
  - 標準ガイドラインは、調達仕様書の作成にあたって留意すべき事項として「事業者が提案内容を検討するために不可欠な情報が網羅される」ことを求めています
  - 調達担当者は、情報システムのセキュリティ要件に関しても同様の点に留意し、各府省庁の情報セキュリティポリシーに準ずるとともに、セキュリティ機能の提案に不可欠な情報を曖昧性がない形で調達仕様書に記載する必要があります
  - SBDマニュアルはこのような場面での活用を想定しています

H

情報セキュリティの設計段階からの確保

情報セキュリティを企画・設計段階から確保するための方策（SBD(Security by Design)）

NISC

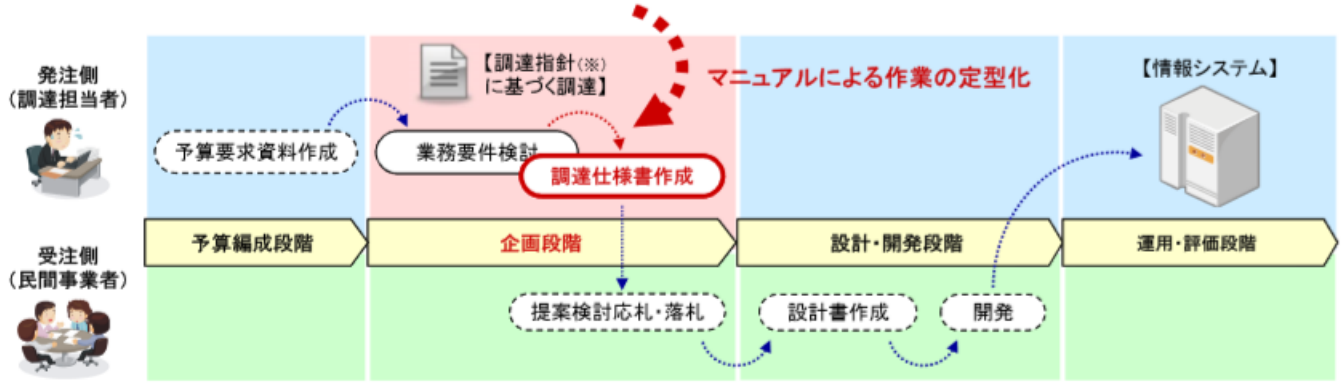
問題認識： 行政情報システムの企画・設計段階から情報セキュリティ対策を考慮すべき

SBD検討会構成員
（座長）東工大 山岡准教授
（委員）大手ベンダー、システム関連事業者関連団体、府省庁CIO補佐官 等
（オブザーバ）関連府省庁 等

『情報セキュリティを企画・設計段階から確保するための方策に係る検討会（SBD検討会）』を設置
- 検討課題
  - ✓ 調達仕様書の「**情報セキュリティ要件の不明瞭さ**」から、調達者と供給者の合意形成に支障を来す。
  - ✓ 結果として、「**不公平な調達**」、「**過度なセキュリティ対策**」、運用開始後の「**セキュリティ事故**」を招くおそれ。
- 解決方針
  - ✓ 調達担当者が調達仕様書作成時に「**情報セキュリティに係る仕様**」を適切に組み込める方法を確立する。

検討成果

『情報システムに係る政府調達におけるセキュリティ要件策定マニュアル』
- 調達担当者がシステム特性に応じて「**調達仕様書にセキュリティ要件を記載する方法**」を解説
- 「**対策要件集**」及び「**対策要件選定作業の定型化**」等のツールによる調達担当者の支援



※ 調達指針：情報システムに係る政府調達の基本指針（H19.3.1 CIO 連絡会議決定）

出典：内閣官房情報セキュリティセンター

H

SBDマニュアルによる作業の定型化

『情報システムに係る政府調達におけるセキュリティ要件策定マニュアル』による作業の定型化

NISC

【マニュアル利用場面】 調達指針に基づく調達において、調達仕様書に盛り込むべきセキュリティ要件を検討する際に以下の作業を行う。

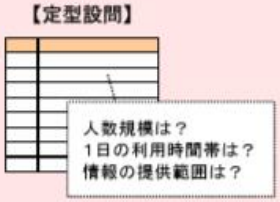
■ 業務要件の検討 （対象業務をシステム概要図にまとめ、定型設問に回答する）【※ 他の方法による代替可】

ステップ1
目的及び業務を洗い出す

ステップ2
業務の特徴を3つの観点から整理する

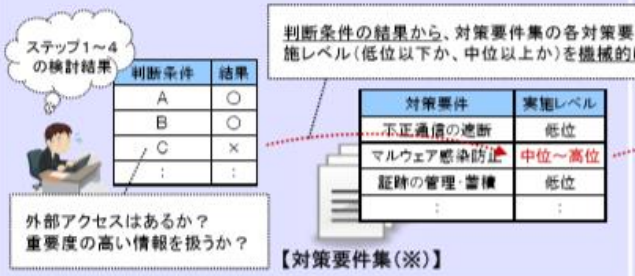
ステップ3
システム概要図を表記ルールに基づいて作成し、要件を俯瞰する

ステップ4
定型設問により業務要件を詳細化する

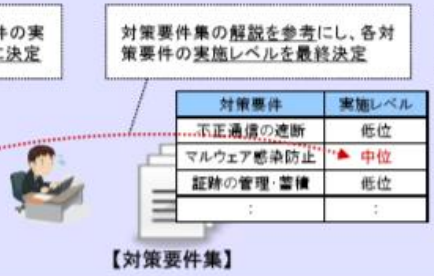


■ セキュリティ要件の策定 （業務要件を判断条件にあてはめ対策要件を決定する）

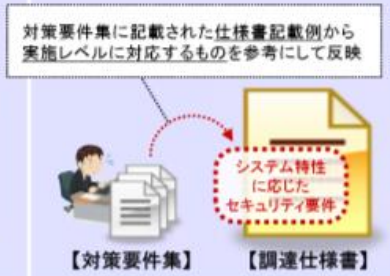
ステップ5
判断条件を判定し、対策要件ごとの実施レベルを検討する



ステップ6
実施レベルを確定し、対策要件を決定する



ステップ7
調達仕様書に反映する



（※）侵害対策、不正監視等の24種類の対策要件、3段階の実施レベル（対策の強度）に応じた仕様書記載例に関する解説

出典：内閣官房情報セキュリティセンター

J「デジタル・ガバメント推進標準ガイドライン」（第1章～第10章迄）

- キーワード
  - サービス改革、業務改革、ＢＰＲ、政府情報システム、ＩＴガバナンス（組織体制、計画管 理、ＩＴ人材管理、予算管理、執行管理、情報資産管理、ドメイン管理、システム監査管理、プロジェクト検証等）、ＩＴマネジメント（プロジェクト管理、予算、要件定義、調達、設計・開発、業務運営・改善、運用、保守、システム監査等）、情報システムの経費区分
- 概要
  - サービス・業務改革並びにこれらに伴う政府情報システムの整備及び管理に関して、その手続・手順に関する基本的な方針及び事項並びに政府内の各組織の役割等を定める体系的な政府の共通ルール

デジタル・ガバメント推進標準ガイドライン実践ガイドブック (第3編第6章　調達)

- 入札の決まりごと
  - 調達は、契約方式や金額等に応じて調達手続や公示期間等が定められています
  - 調達の準備を開始しようとした時点で、当初想定していたよりも時間がなかったことに気が付くことが少なくありません
  - 調達の準備の時間が十分に取れないと、資料の準備不足や説明会等の不足から事業者への十分な理解が得られず、入札の不調や不落となりかねません
  - このような不測の事態を防ぐために、プロジェクト計画の段階で調達に係るルールを理解し、調達に必要な期間を踏まえて準備を行えるように調達の計画をたてることが重要です
- 調達の基本的ルール
  - 調達に関する期間等のルールは、政府調達に関する協定や会計法等で調達手順や期間等が定められています
  - 標準ガイドライン解説書「第６章１．　調達の計画」に記載しているルールを確認して、計画を立てます
  - 予定価格や案件の規模等により、必要な期間が異なるので、余裕を持った計画を立てるようします

K「政府情報システムにおけるクラウドサービスの利用に係る基本方針」

- キーワード
  - 2018年(平成30年)6月7日の各府省情報化統括責任者（ＣＩＯ）連絡会議で決定
  - 従来の政府方針から、全く異なる指針
  - クラウドサービスの採用をデフォルト（第一候補）
  - 標準ガイドライン附属文書
  - 正しい選択を行えば政府情報システムにおいても、クラウドサービスを利用することで様々な課題が解決されることが期待される
  - ・・・・・・・

L 「公共機関のクラウド・バイ・デフォルトと法人デジタルプラットフォームでの活用」

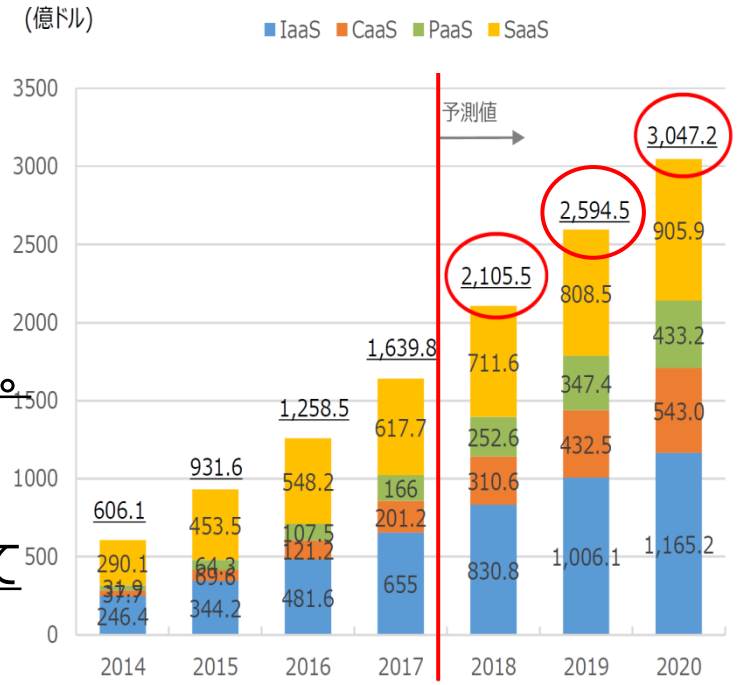
- デジタルガバメント実行計画
  - デジタル・ガバメント実行計画には、オンライン原則を徹底する「デジタルファースト」、添付書類を撤廃する「ワンスオンリー」、民間サービスとの連携を含めた「ワンストップ」を3本柱とする、省庁横断の行政サービス改革も明記されています
  - そのため、システム改革が、今後、クラウドを中心に進むことが想定されます
  - クラウドの「安全性評価」は、具体的には米国政府が調達するクラウドサービスの基準のFedRAMP（フェドランプ）などを参考に策定される基準に基づいて、監査人が各サービスを監査し、“技術”・“オペレーション”・“組織”の各基準を満たすサービスを登録して公開されます

クラウドサービス市場規模の推移

世界におけるクラウドサービスの市場規模は年々拡大しており、(下図参照) 世界の潮流として、海外の政府調達の多くがクラウドバイデフォルト、すなわちクラウドサービスの利用を第一候補とし、クラウドの評価制度が決められています。

日本でもクラウドバイデフォルトの考え方により、クラウド化が推進されているが、クラウドサービスの安全な利用のため、クラウドサービスの安全性評価の統一的な基準や制度が必要となってきています。

現在、クラウドサービスに関する様々な方針やガイドライン等が存在しますが、各政府機関等が独自に運用しており、非効率な状態となっています。
その為、経産省はクラウドサービスに関する統一的なセキュリティ基準を明確化し、実効性・効率性・網羅性のある安全性評価制度の制定を進めています。



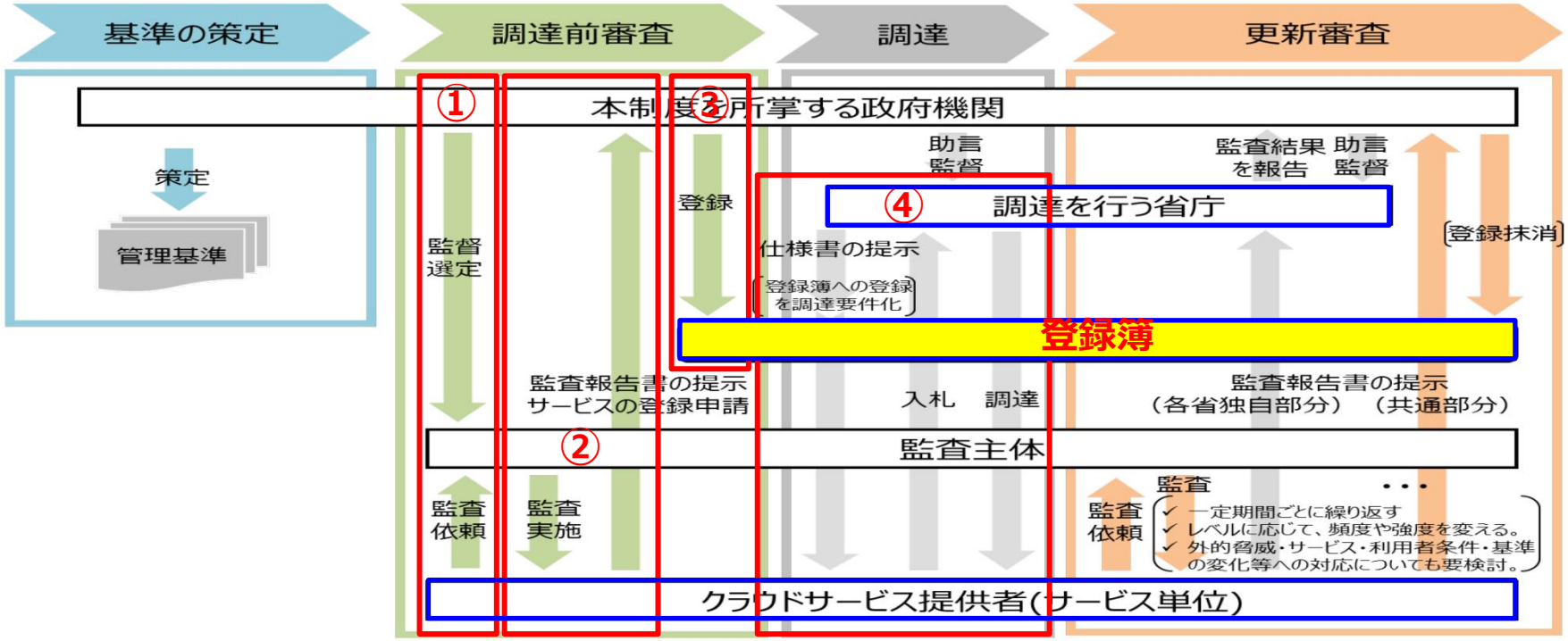
出典：平成30年版情報通信白書

M

クラウドサービスの安全性評価業務フロー

現在検討が進められているクラウドサービスの安全性評価では、特定の政府機関が各種基準の随時改訂、監査主体の選定、登録簿の管理を行い、下図の評価フローにて運用することが検討されています。

①政府機関が監査主体を選定、クラウドサービス提供者は監査主体に対し監査の依頼を行います。
②監査主体は依頼に基づき監査を実施。クラウドサービス提供者は実施後登録申請を行います。
③政府機関は監査内容を確認し、基準を満たしている場合、**登録簿**に登録されます。
④調達を行う省庁は**登録簿**への登録を調達要件化することにより安全なクラウドサービスのみ調達することができます。



出典：経済産業省　クラウドサービスの安全性評価に関する検討会（令和2年1月）

M

クラウドサービスの安全性評価利用メリット

安全性評価が行われた登録簿に登録されているサービスを利用することで、調達を行う省庁等とクラウドサービス提供者のメリットは以下のとおりになります。

【調達を行う省庁等】

・**登録簿**に登録されているということは、安全性評価が実施済みであり、一定のセキュリティ基準を満たすクラウドサービスということとなります。このため、**登録簿**から選定することにより安全性の高いサービスが利用可能となります。また、調達を行う省庁等は**登録簿**への登録を調達要件化することで、仕様書には追加的な要件のみを記載するだけで良いこととなります。

【クラウドサービスの提供者】

・**登録簿**に登録されることは、一定のセキュリティ基準を満たす安全性の高いサービスである事となる為、質の高いサービスを提供していることが保証されます。

安全性評価制度活用についてのスケジュールについては以下のとおりと進んでいます。

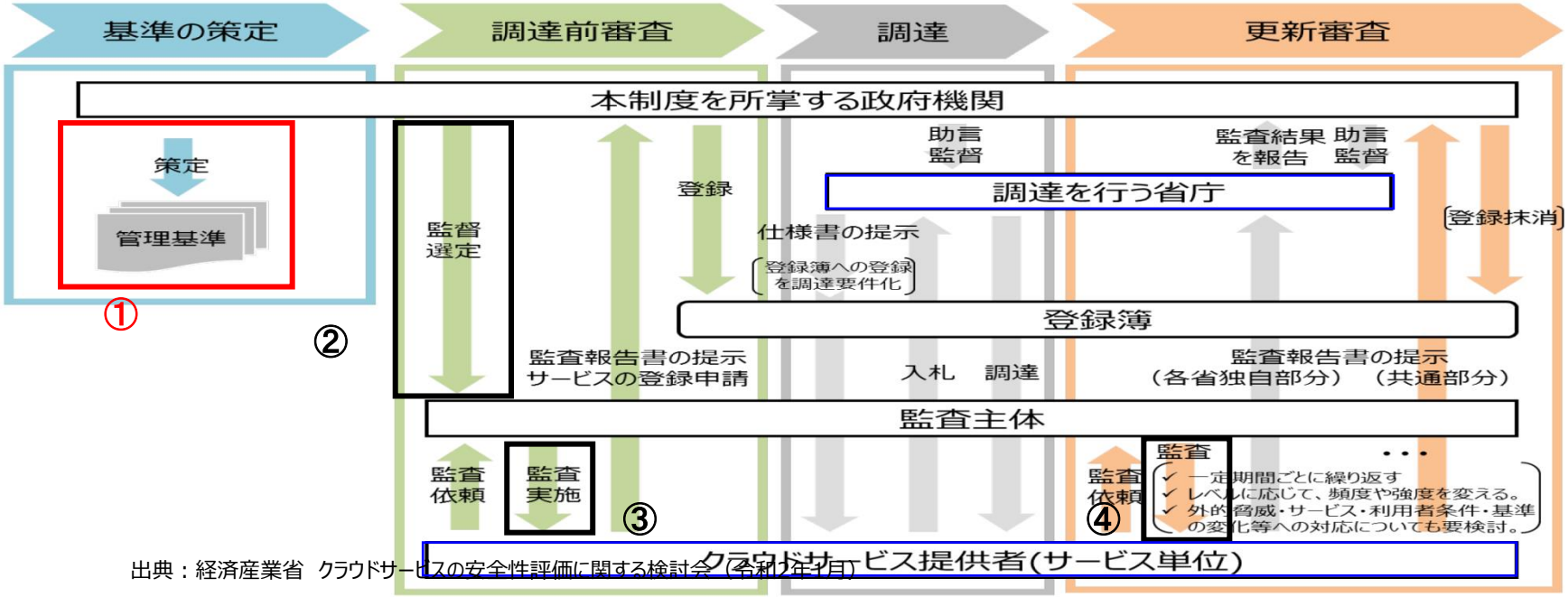
- ●2019年夏　各種基準の素案策定・制度の試行実施、基準の意見募集
- ●2019年内　制度の立ち上げ
- ○2020年夏　クラウドサービスの監査・登録作業等
- ○2020年秋　全政府機関等での制度活用開始

M

安全性評価に必要な基準

評価フローに従って安全性評価を行うために必要な基準について、現在整備・策定が進んでいる各基準等の概要は以下の通りとなります。

① **管理基準** ⇒ 政府が調達にあたりクラウドサービス提供者に求めるセキュリティ基準
② 監査主体の選定基準⇒ 政府が監査主体を選定する際の基準
③ 監査基準 ⇒ 監査主体が監査を実施する際の規範
④ 標準監査手続 ⇒ 監査手法及び監査手順を踏まえた監査の手続



出典：経済産業省　クラウドサービスの安全性評価に関する検討会（令和2年1月）

出典：経済産業省　クラウドサービスの安全性評価に関する検討会（令和2年1月）

M

クラウドサービスの安全性評価管理基準

◆**管理基準**の検討

政府が調達にあたりクラウドサービス提供者に求めるセキュリティ基準について、国際規格をベースとしながら、統一基準及びSP800-53から国際規格に不足していると考えられる項目のうち、政府として必要と考えられる項目を追加する形で**管理基準**が作成されます。

① **国際規格**について

JIS Q 27001/JIS Q 27002/JIS Q 27017に準拠して編成された「クラウド情報セキュリティ管理基準(平成28年度版)」を参考とし検討を行っています。

② **統一基準**について

①で含まれず、かつ「CSPが実施しなければ、調達者/利用者側が統一基準を満たすことに支障を来たす内容か否か」の観点からCSPに求めるべき内容であると判断されるものについて、追加を行います。

③ **SP800-53**について

海外の基準の中で、運用実績が長く、複数回の基準更新が行われてきたものとしてJIS Q 27001では対応がとれないとされている項目について追加要否を検討されます。

出典：経済産業省　クラウドサービスの安全性評価に関する検討会（令和2年1月）

M

調達者利用制度の考え方

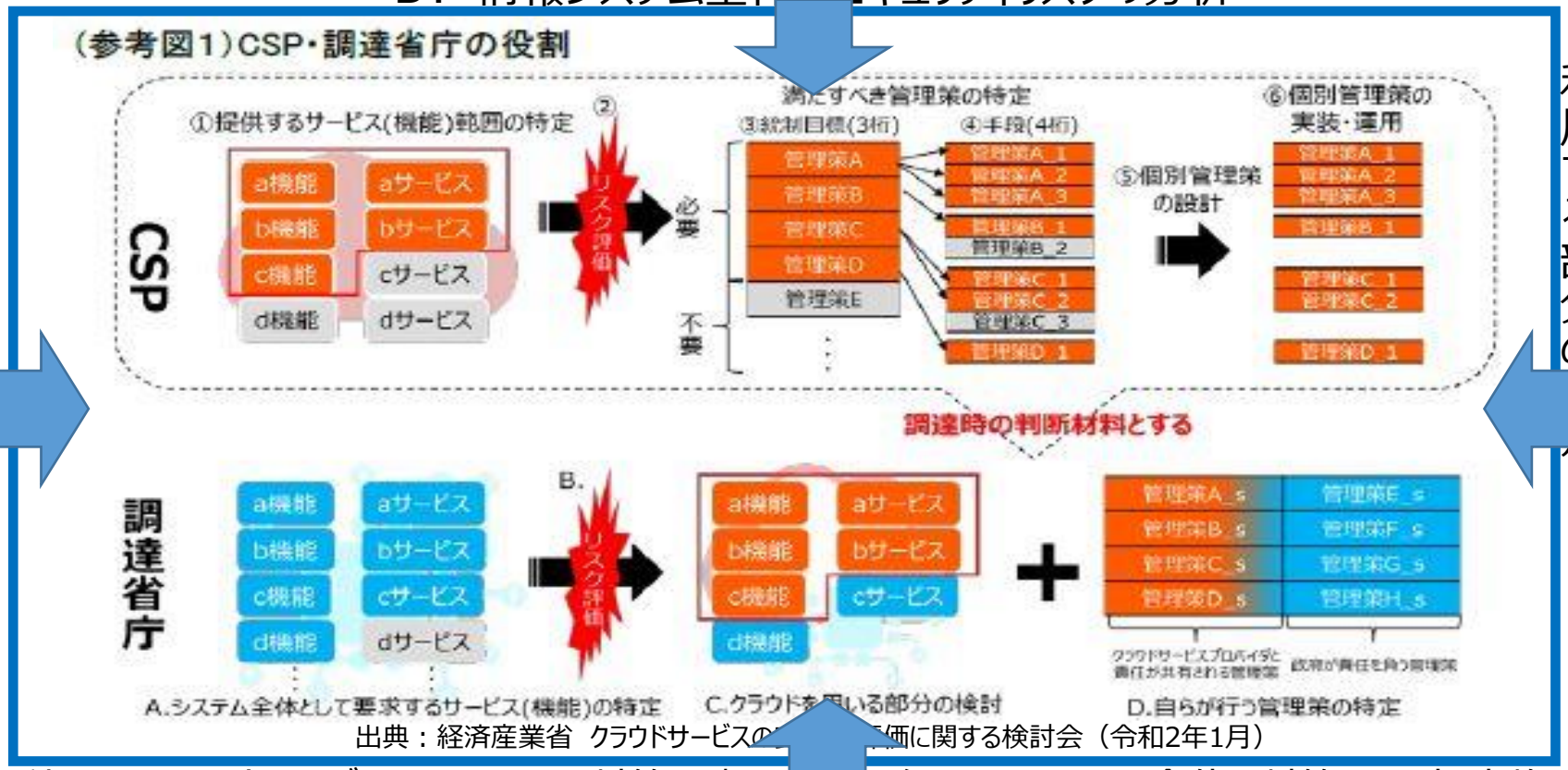
◆調達者の制度利用の考え方

情報システムを調達する政府機関等においては、調達にあたり通常以下のプロセスによって具体的な情報システムの内容とセキュリティ対策を決定・実施することが想定されます。

B．情報システム全体のセキュリティリスクの分析

A．情報システム全体の機能の特定

C．全体機能のうちクラウドサービスを利用する部分の特定



出典：経済産業省　クラウドサービスの[illegible]価に関する検討会（令和2年1月）

D．利用するクラウドサービスのセキュリティ対策を踏まえた自ら行うべきシステム全体の対策の設計・実施

調達者/利用者が留意すべき点

◆情報システムの調達者/利用者が留意すべき点

情報システムのセキュリティ確保の責任は、一義的に当該システムの調達者/利用者が負うものであります。本制度において登録されたクラウドサービスを利用していたとしても、単にそのサービスを利用するだけでは情報システム全体のセキュリティが十分に確保されることにはなりません。

自身が利用するクラウドサービスについて、ユーザーとして適切な設定を行うことが当然に求められることに加えて、情報システム全体について、そのセキュリティリスクを分析し、適切な対策を行うことが求められます。

本制度に登録されているクラウドサービスを利用するにあたっては、当該サービスが組み込まれる情報システムのセキュリティリスクを適切に把握した上で、当該サービスが提供するセキュリティ機能やセキュリティに係る提供情報を踏まえ、情報システム全体のセキュリティ対策を実施するとともに、セキュリティ確保についての最終的な責任を負わなければなりません。

他方で、本制度を運営する立場においても、政府機関等が適切な判断を行うことに資する情報を、適切に提供できるよう努めることが必要となります。

参考URL一覧

A 「政府機関等の情報セキュリティ対策のための統一基準」
- https://www.nisc.go.jp › active › general › pdf › kijyun30

B 「政府機関等の対策基準策定のためのガイドライン」
- https://www.nisc.go.jp › active › general › pdf › guide30

C 「IT調達に係る国の物品等又は役務の調達方針及び調達手続きに関する申合せ」
- https://www.nisc.go.jp › active › general › pdf › chotatsu_moshiawase

D 「情報セキュリティを企画・設計段階から確保するための方策に係る検討会報告書」
- https://www.nisc.go.jp › active › general › pdf › SBD_report

E 「電子政府 構築計画」
- https://www.kantei.go.jp › singi › cio › dai4

F 「業務・システム最適化指針（ガイドライン）」
- https://www.kantei.go.jp › singi › cio › dai19

G 「情報システムに係る政府調達の基本指針」
- www.soumu.go.jp › main_content

H 「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」
- https://www.nisc.go.jp › active › general › pdf › SBD_manual

I 「情報システム・ソフトウェア取引トラブル事例集」
- https://www.meti.go.jp › policy › it_policy › softseibi

J 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」
- https://cio.go.jp › sites › default › files › uploads › documents

K 「デジタル・ガバメント推進標準ガイドライン」
- https://www.kantei.go.jp › singi › cio › kettei

L 「公共機関のクラウド・バイ・デフォルトと法人デジタルプラットフォームでの活用」
- https://www.sbbit.jp/article/bitsp/36613

M 「クラウドサービスの安全性に関する検討会
- hhttps://www.meti.go.jp/shingikai/mono_info_service/cloud_services/20200130_report.html

本日の講演で参照している文書のURLです、実務でご活用下さい