「2010年度重要インフラの共通脅威分析に関する調査」の結果について

2011年3月25日

内閣官房情報セキュリティセンター（NISC）

1. 本分析におけるクラウドコンピューティングの対象範囲

■調査を通じて、重要インフラにおける「クラウド」の定義が分野毎に大きく異なることを把握した。

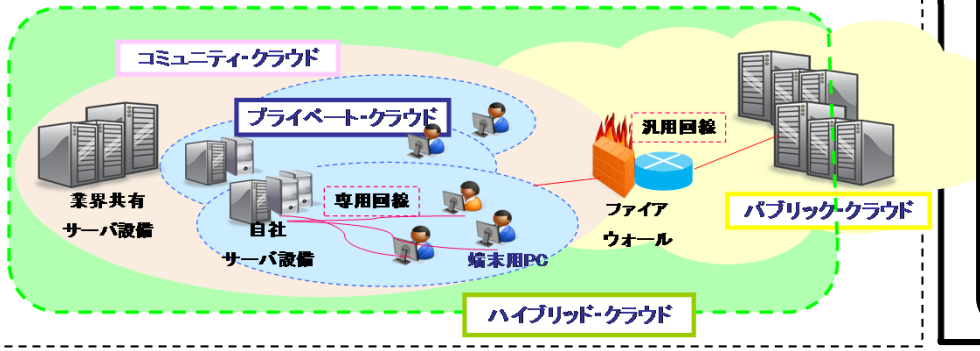
■重要インフラ共通脅威分析において主に取り上げるべきクラウドが具備する本質的な性質として、「外部性の存在」と「リソースの共有」を抽出し、これら両者を満たすことで定義した。

■一般的なクラウドの定義

展開モデル	
パブリック・クラウド	電子メールやグループウェアなど、不特定多数の利用者が計算機リソースを共有。
プライベート・クラウド	個別の企業の中で計算機リソースを共有
ハイブリッド・クラウド	複合的なアプリケーションをパブリック/プライベートの双方の特長を生かして実現。
コミュニティ・クラウド	複数企業が同じ計算機リソースを共有。

サービスモデル

SaaS　PaaS　IaaS



■重要インフラ共通脅威分析におけるクラウドの定義

共通脅威分析において本質的なクラウドの性質として

① 「外部性の存在」： 重要インフラ事業者自身が管理できない要素が存在すること。

② 「リソースの共有」： 仮想化技術を利用して、柔軟な計算機リソースの共有を実現。クラウド技術の本質から重要な性質。共有する者は問わない。

の両者を満たすこと。

■よく用いられる概念との関係

- パブリッククラウド： 共通脅威分析におけるクラウドに含まれる。
- プライベートクラウド： 外部組織（情報子会社・委託先等）が運用する場合に限り、共通脅威分析におけるクラウドに含まれる。
- ASPサービス： ASPが提供するSaaSのサービスモデルのうち、仮想化技術を用いて計算機リソースを共有しているものに限り、共通脅威分析におけるクラウドに含まれる。
- オンプレミス： 共通脅威分析におけるクラウドには含まれない

※ASP（ApplicationServiceProvider）

2. クラウド導入に際しての具体的な共通脅威

■重要インフラ分野の多くが認識した代表的な共通脅威とその対応策を整理した。

共通脅威の視点	脅威の種類	対応策
外部からの脅威	マルチテナント（共同利用型）システムにおける、共同利用者の不正行為や意図せざる影響	・テナント間のデータ等の完全な分離 ・正確なプロビジョニングの実施
システム自体が抱える脅威	クラウドサービスの認証システムの機能不足・脆弱性への不安	・社内ディレクトリシステムとの統合 ・ID管理ツールの利用
運用・管理体制における脅威	クラウド事業者都合（経営破たん、買収等）によるクラウドサービスの終了	・契約による一定の対策（限度あり） ・クラウドサービスの予期せぬ終了が、自組織にとって大きな問題となる業務委託の見合わせ
	クラウド事業者の情報セキュリティ管理体制の不備	・第三者評価制度の利用 ・クラウド利用者のための情報セキュリティマネジメントガイドライン（経済産業省）の活用
	事故発生時の対応への不安	・契約やSLA等で、事故発生時の対応についてクラウド事業者との事前合意
	特定のクラウド事業者への囲い込み（ロックイン）	・標準化された技術の利用 ・移行可能性についての事前の検証

3. クラウド導入に際しての考慮点等

■重要インフラにおけるクラウド導入に際して制度的に考慮すべき点や、アンケート等でニーズが高かった認証基準について整理した。

■重要インフラにおけるクラウド導入と制度的な考慮点について

◆クラウド導入を考える際に、分野共通で準拠すべきものは、**「個人情報保護法」**であった。

◆特定分野に影響のある制度として、ヒアリングを通じて以下のようなものが挙げられた。

- ✓ 住民基本台帳法、戸籍法　⇒　政府・行政サービス分野
- ✓ 薬事法　⇒　医療分野
- ✓ 外為法　⇒　電力分野
- ✓ WTO政府調達協定　⇒　政府・行政サービス分野、鉄道分野（一部）、通信分野（一部）、金融分野（一部）
- ✓ 金融商品取引法　⇒　金融分野

■クラウドベンダーに対する認証基準について

◆ クラウドベンダー対する基準として、以下の認証の取得や基準などが参考とされている。

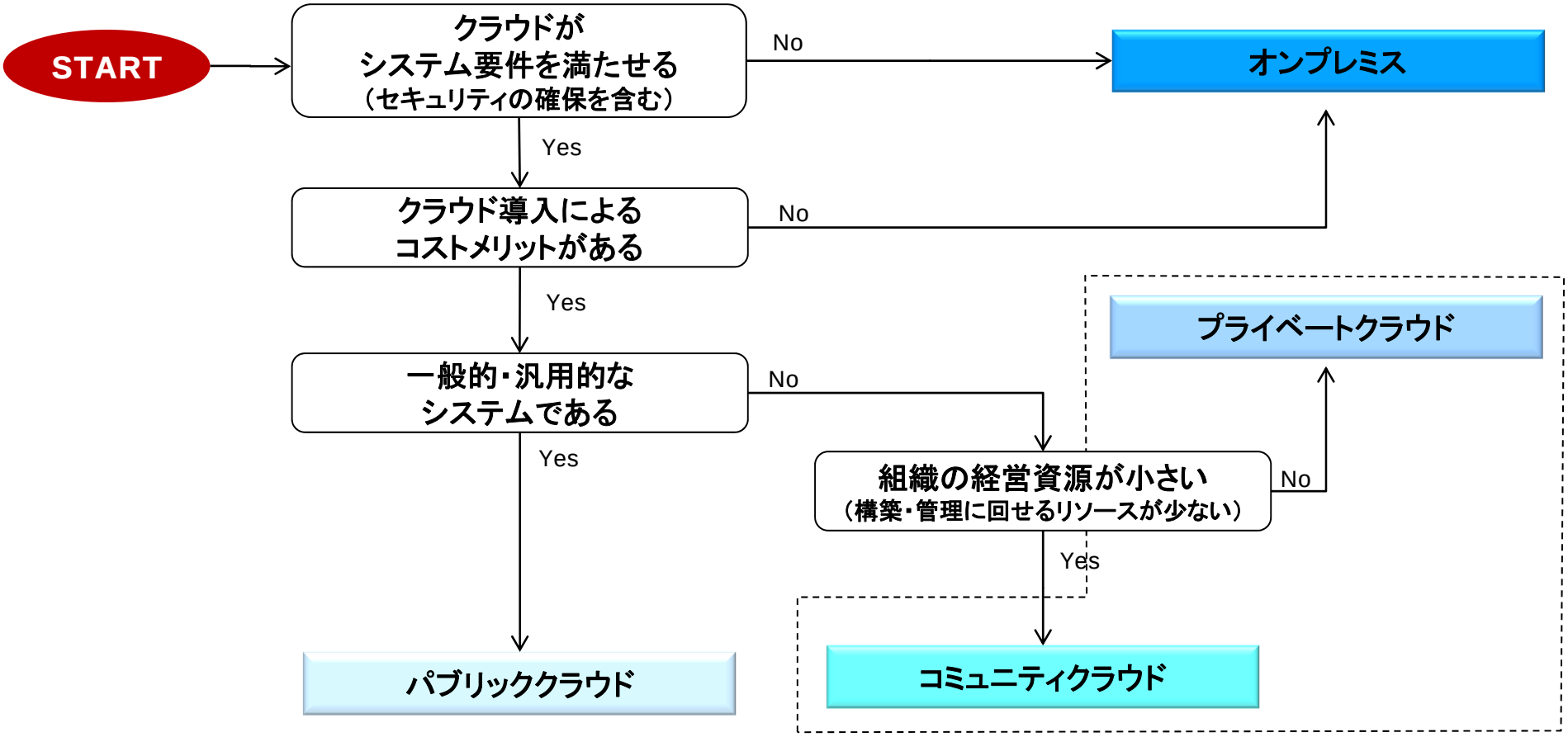
- ✓ 総務省「ASP・SaaS における 情報セキュリティ対策ガイドライン」
- ✓ 経済産業省「クラウドサービスの利用のための情報セキュリティマネジメントガイドライン（案）」
- ✓ ISMS（ISO/IEC　27001：2005）
- ✓ PCI　DSS認証
- ✓ SAS70
- ✓ 日本データセンター協会「データセンターファシリティスタンダード」
- ✓ 財団法人マルチメディア振興センター「ASP・SaaS安全・信頼性に係る情報開示制度認定制度」

◆ クラウドのセキュリティ基準として国際的に認められた基準は今のところなく、各国とも手探りの状況である。

◆ 米国では、政府調達のためのクラウドの認証制度「FedRAMP　(Federal Risk and Authorization Management Program)」を作ろうとする動きもある。

4. 重要インフラにおけるクラウド導入形態等に関する判別のモデル化

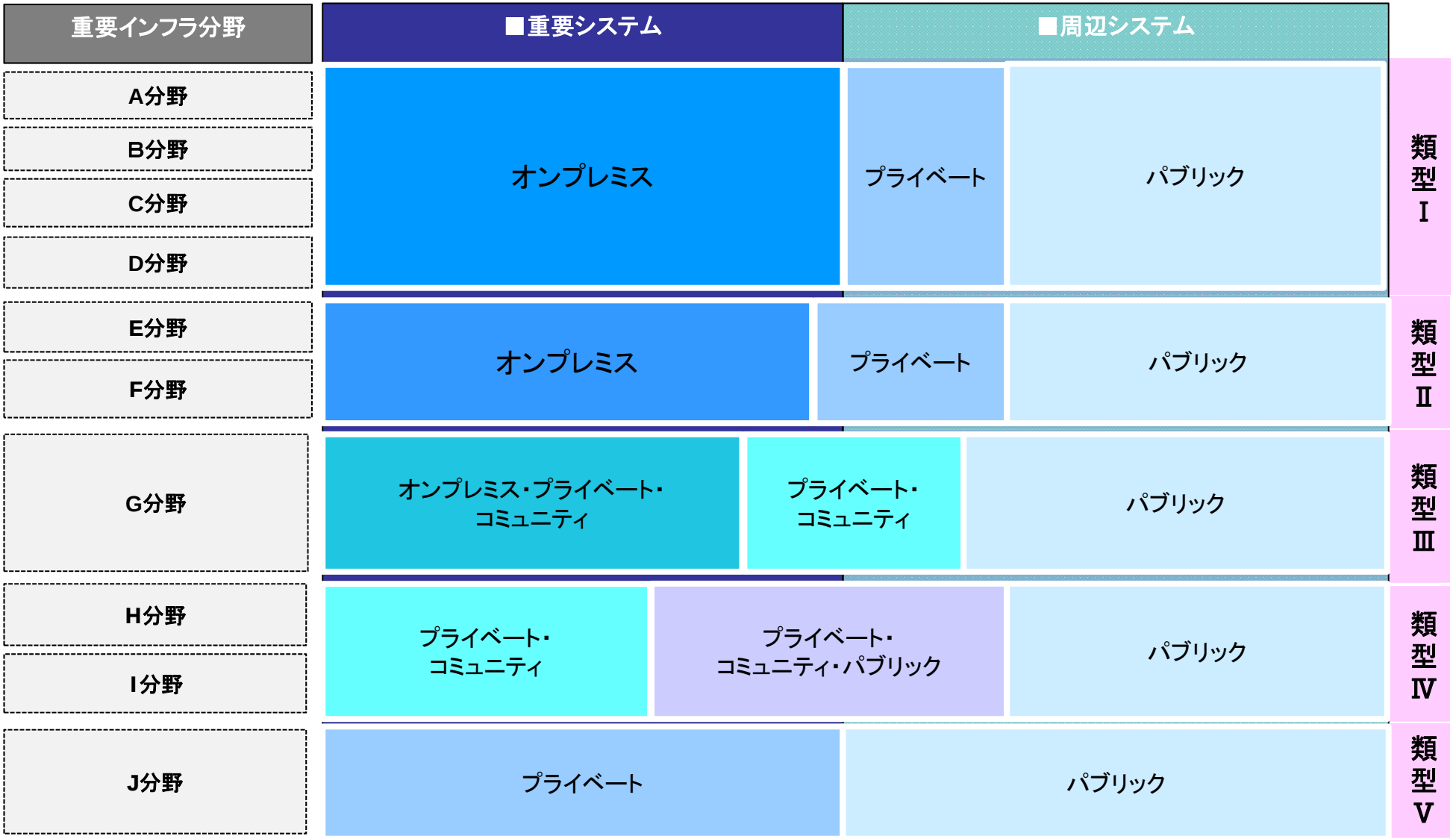
■「システム要件への適合性」「コストメリットの有無」「一般性・汎用性の有無」「組織の経営資源の大小」を判断の要素として、重要インフラにおけるクラウド導入の可否と導入形態について、**「判別のモデル」**化を試みた。



・クラウドがシステム要件を満たせる：技術的要件（例えばリアルタイム性やネットワーク非依存性）や、運用上の要件（セキュリティも含む）を満たすことが出来る
・クラウド導入によるコストメリットがある：　クラウド移行に伴うコスト（金銭的・時間的）に比較し、得られるメリット（コスト削減効果・業務効率化等）が大きい

5.「判別のモデル」から得られた類型（1）

重要インフラに関し、クラウドコンピューティングの導入又は導入可能性の観点から、5つに類型化した。



※　本整理（分析）は将来の理想的な条件下を想定したものとする。

5.「判別のモデル」から得られた類型（2）

- 周辺システムについては、分野共通的にクラウドコンピューティングへ移行可能なシステムとして認識され、一部分野では既に活用している。
- 重要システムへのクラウド導入の観点から、5つの類型については概ね以下のとおり整理できる。

類型	説明
類型Ⅰ	重要システムに関しては、重要インフラ事業者としての業務の特異性、或いは、リアルタイム性や信頼性など、クラウドコンピューティングではシステム要件を満たすことができないため、今後もオンプレミスとして運用される。
類型Ⅱ	類型Ⅰと同様、制御系などがオンプレミスとして存続する一方、重要システムに含まれる予約システムの一部などが将来的にはプライベートクラウドへ移行する可能性がある。
類型Ⅲ	リアルタイム性が必要なシステムを除けば、技術的な観点からは重要システムへのクラウドコンピューティングの導入に支障はないと考えられる。ただし、厳格な情報管理を求められる分野のため、導入に際しては、プライベートクラウド、或いは、コミュニティクラウドとなる。
類型Ⅳ	重要システムについても中小規模の組織から順次、プライベートクラウド、或いは、コミュニティクラウド、さらに一部パブリッククラウドへの移行が予測される。ただし、制度的要件を満たすために、導入可能なクラウドの展開モデルには制約がある。
類型Ⅴ	一部の事業者においては、重要システム・周辺システムともに、クラウドコンピューティングへの移行が始まっており、クラウドコンピューティング利活用の拡大が見込まれる。

6. 諸外国との比較と分析（1）　（米国に関するヒアリング）

■IT-ISAC（米国）

- ✓ クラウドの重大なリスクとしては、クラウドに対するコントロールの制約と、クラウドDDoS攻撃などの脅威を主として想定。
- ✓ IT-ISACにおいても、クラウドは近年もっともよく取り上げられるトピックとなっており、クラウドを対象としたDDoS攻撃などが主要なリスクとして認識されている。また、2011年にクラウドを対象とした攻撃が増加すると予想している。
- ✓ 米国重要インフラにおいてクラウドが使われているかについては、「重要インフラ」の定義による。例えば、公益企業（電気、ガス、水道）などは、自社の重要システムをクラウドに移行する動きはない。一方で、人事システムやERPシステムなどについては、重要インフラを含むますます多くの企業がクラウドに移行している。
- ✓ 保険について、（クラウドに限定されたものではないが）サイバーリスク保険がここ10年ほどで普及してきた。一般企業及びサービス提供事業者の双方に対して、サイバー攻撃等による損失について保証するもの。
- ✓ クラウドをBCPに活用するという方向として、テープバックアップの代わりにクラウドを利用する動きがある。

6. 諸外国との比較と分析（2）　（欧州に関するヒアリング）

■ENISA（欧州）

- ✓ ENISAは、クラウドコンピューティングを利用する際の利点・不利益点を明らかにし、リスクを最小限にすることで市場を正常にする手助けをしている。重要インフラとクラウドという観点では、将来的にENISAがクラウドコンピューティングと重要インフラを結びつけた話題を取り扱う可能性はあるものの、現状では具体的な取り組みはない。
- ✓ 重要インフラへのクラウドコンピューティングに関するリスクはさまざまなものがあるが、ひとつ挙げるとすれば国境を超えたシステムであることと認識している。
- ✓ 重要インフラ保護に関する主導権はEuropean Commission (EC) と各国政府が持っている。
- ✓ ECでは重要インフラと認定されているインフラは運輸とエネルギーであり情報通信は入っていない。いっぽう、それぞれの国は重要インフラを独自に指定しており、それらは自国の範囲におさまるものと、他国にも影響が出るものとが含まれている。そこで後者については、インフラを相互に依存していることから、ECでも重要インフラと指定している。
- ✓ ENISAは近年では加盟国間で重要インフラ保護向けの情報共有システムをつくった。このシステムは環欧州演習でも使用される。これまでは各国でセキュリティや技術のレベルに差があるだけでなく、法的な枠組みや信頼性に関する問題もあった。その後ある程度の信頼性を確保し、脅威情報などを共有するようになった。
- ✓ 欧州サイバー演習（Cyber　Europe）を2010年12月に実施した。EC加盟国の27カ国とアイスランド、ノルウェー、リヒテンシュタインを加えた30カ国で環欧州演習を初めて行った。その目的は参加国の間での情報共有に関してどれだけの量の情報を共有し、連携することができるかを確かめることである。演習に参加する国は重要インフラを共有している。例えばひとつの企業によって複数の国の重要インフラを運用している場合がある。なお、詳細レポートは公開されていない。

7. 2010年度共通脅威分析のまとめ

分析	分析の結果
本分析におけるクラウドコンピューティングの対象範囲	■重要インフラ共通脅威分析において主に取り上げるべきクラウドが具備する本質的な性質として、「外部性の存在」と「リソースの共有」を抽出し、これら両者を満たすことで定義した。
クラウド導入に際しての共通脅威と対応方策	■アンケート調査に基づき、重要インフラにおいて重視されている分野共通で起こり得る脅威の傾向を洗い出し、代表的な共通脅威とその対応策を整理した。
判別のモデル化	■「システム要件への適合性」「コストメリットの有無」「一般性・汎用性の有無」「組織の経営資源の大小」を判断の要素として、重要インフラにおけるクラウド導入の可否と導入形態について、「判別のモデル」化を試みた。
重要インフラにおけるクラウド導入の可能性と形態等に関する分析	■重要インフラ10分野について、各分野の重要システム及び周辺システムへのクラウドコンピューティングの導入又は導入可能性の観点から、5つに類型化できた。
諸外国との比較と分析	■IT-ISAC（米国）及びENISA（欧州）の動向調査の結果、重要インフラにおけるクラウドという観点からの分析は欧米でもそれほどなされていないのが現状であるが、今後注目すべき動向として認識されている。