事例８　グーグル・エルエルシーによるウィズ・インクの株式取得

第１　当事会社

グーグル・エルエルシー（本社米国。以下「グーグル」という。）は、検索エンジンサービス、動画共有プラットフォームサービス、クラウドサービス等の提供事業を営む会社である。

ウィズ・インク（本社米国。以下「ウィズ」という。）は、クラウドセキュリティサービスの提供事業を営む会社である。

以下、グーグルの親会社であるアルファベット・インクを最終親会社として既に結合関係が形成されている企業の集団を「アルファベットグループ」、ウィズを最終親会社として既に結合関係が形成されている企業の集団を「ウィズグループ」、アルファベットグループとウィズグループを併せて「当事会社グループ」という。

第２　本件の概要及び関係法条等

本件は、グーグルがウィズの株式に係る議決権の50%を超えて取得すること（以下「本件行為」という。）を計画したものである。

関係法条は、独占禁止法第10条である。

第３　本件の経緯

本件行為は独占禁止法第10条第２項に規定する届出要件を満たさないが、本件行為に係る対価の総額が400億円を超えると見込まれ、かつ、本件行為が国内の需要者に影響を与えると見込まれたことから、公正取引委員会は、「企業結合審査の手続に関する対応方針」の６(2)に基づき、当事会社グループに本件行為について説明を求め、当事会社グループから提出された本件行為に係る具体的な計画、意見、資料等を踏まえて、当委員会の職権で企業結合審査を行った。その結果、職権審査によって当委員会が把握した情報を前提とすれば、本件行為により一定の取引分野における競争を実質的に制限することとなるとはいえないと認められたことから、本件審査を終了した。

第４　本件の検討対象

アルファベットグループの商品・役務は多岐にわたるものの、本件においては、特に、当事会社グループが共に提供するセキュリティサービス（後記第５の１(1)）並びにセキュリティサービスと相互接続して利用することが可能なサービス（後記第５の１(2)）について検討を行った。

第５　一定の取引分野

１　役務の概要

(1) セキュリティサービス

ア　セキュリティサービスの概要

セキュリティサービスとは、コンピュータ、ネットワーク、システム、アプリケーション、データ等を保護するために使用されるサービスの総称である。セキュリティサービスは、サイバー攻撃からの防御や不正アクセスの防止、データの暗号化、脆弱性の検出・修正等、様々なセキュリティ上の問題に対応する機能を有し、大きく、事前予防型ツールと事後対応型ツールの二つに分類することができる。

事前予防型のセキュリティサービスは、攻撃が発生する前にこれを防止するものであり、保護対象（ユーザー側）における潜在的な脆弱性を定期的に検出することに重点を置いている。事前予防型のセキュリティサービスの例としては、サーバー、ネットワーク、クラウド等の脆弱性を特定するツール、設定ミスを検出するツール、企業のセキュリティポスチャ[1]を定期的に評価するツール等がある。

一方で、事後対応型のセキュリティサービスは、攻撃が発生した後に事後的な対応を行うものであり、攻撃や攻撃者の特定、ダメージコントロールや復旧に重点を置いている。事後対応型のセキュリティサービスの例としては、マルウェア感染後の検知・駆除サービス、インシデントレスポンスサービス、災害復旧ツール等がある。

イ　CNAPPの概要

従来、企業等は、特定の課題に対応する各セキュリティサービスを個別に導入していたところ、こうしたサービスは独立して機能することが多く、連携性に欠ける上、セキュリティの専門家向けに設計されていることがほとんどであったため、同一組織内の異なるチーム間で、意思決定の分断、方針の不一致、業務の複雑化や非効率が生じることがあった。また、マルチクラウド環境[2]の普及により、複雑化した環境におけるセキュリティ確保の必要性が生じていた。

令和３年（2021年）、世界的なリサーチ会社により、主にマルチクラウド環境向けの新しい統合型セキュリティソリューションを指すものとして「CNAPP」という用語が提唱され[3]、その後、各ベンダーがそれぞれ同様のセキュ

---

[1] 設定ミスがないか、アクセス権限が適切か、脆弱性が残っていないか、侵入された痕跡がないか、監視とログが機能しているか、セキュリティルールが守られているかなどといった点から評価される総合的な安全レベルのこと。

[2] 全てのワークロード（コンピュータシステムやサーバーに負荷を与えるタスクやアプリケーションの総称）を単一のクラウドサービスプロバイダーに集中させるのではなく、複数のクラウドサービスプロバイダーに割り当て、管理する方法のこと。

[3] CNAPPは、基本的にマルチクラウド環境を利用する需要者向けの製品であるが、シングルクラウド環境の需要者もCNAPPを利用できないということではない。ただし、シングルクラウド環境で、かつ、構造が単純なシステムを利用する需要者の場合、自社が利用しているクラウドサービスのベンダーが

リティソリューションを提供し始めた（以下、当該サービスを「CNAPP」[4]という。）。

CNAPPは、具体的には、主として事前予防型の複数のセキュリティ機能を単一のダッシュボードに統合・可視化し、継続的な脆弱性の特定、設定ミスの検出、企業のセキュリティポスチャの評価等を行うものである。

ウ　アルファベットグループが提供するセキュリティサービス

アルファベットグループは、主に事後対応型セキュリティサービスを提供しており、これに加えて事前予防型セキュリティサービスも一部提供している。このうち、事前予防型セキュリティサービスの１種類については、CNAPPに該当すると分類されることがある。

エ　ウィズグループが提供するセキュリティサービス

ウィズグループは、CNAPP及び当該サービスの機能を強化するための製品を提供している。

(2)　ウィズのCNAPPと相互接続することが想定されるサービス

一般的に、CNAPPは、複数のクラウドサービスやセキュリティ等の各種サービスとの相互接続を前提としたサービスであり、ウィズグループが提供するCNAPPも、外部のクラウドサービスや各種サービスと相互に接続することが可能である。ウィズグループのCNAPPと相互接続することが想定されるサービスは図表１のとおりである。

アルファベットグループは図表１記載の各サービスを提供している。

【図表１】CNAPPと相互接続することが想定されるサービス

相互接続の対象となるサービスの名称	左記サービスの概要及び相互接続により可能となることの概要
IaaS[5]／PaaS[6]型クラウドサービス	コンピューティング、データ保存、データ分析、機械学習等を提供するクラウド基盤サービス。 相互接続により、クラウド上のサーバー等の操作履歴

あらかじめ提供している標準的なセキュリティ機能で十分なことも多いため、マルチクラウド環境下と比較してCNAPPの必要性は相対的に低く評価される傾向にある。

[4] Cloud Native Application Protection Platformの略称。CNAPPは、クラウドネイティブ環境向けのセキュリティサービスの一種であり、複数のセキュリティ機能を統合したプラットフォームでもある。

[5] Infrastructure as a Service（インフラストラクチャアズアサービス）の略。サーバーやネットワークなどインフラそのものをクラウドで貸し出すサービス。

[6] Platform as a Service（プラットフォームアズアサービス）の略。アプリを動かすための基盤（プラットフォーム）を提供するサービス。

相互接続の対象となるサービスの名称	左記サービスの概要及び相互接続により可能となることの概要
	やログなどの情報を集め、単一の画面で管理しながら、不正アクセスや攻撃等の危険を発見することができる。
API[7]セキュリティプラットフォーム	APIを攻撃や不正利用から守るための統合型セキュリティサービス。 相互接続により、APIへの攻撃や不正利用をリアルタイムに発見し、必要に応じてブロックすることができる。
CI／CDツール[8]	開発者がコードの変更を迅速に反映できるよう支援することを目的に、ソフトウェアを作る作業（ビルド）、動作確認（テスト）及び実際の運用環境への反映（デプロイ）を自動化するツール。 相互接続により、ソフトウェアを作る作業と並行して、自動でセキュリティチェックを実行することができる。
メッセージングサービス	アプリケーション間でデータ（メッセージ）をやり取りするための基盤。 相互接続により、顧客がメッセージをレポート形式で出力できるほか、問題が発生した場合にそのセキュリティ上の通知を受け取ることができる。
コンプライアンス対応クラウドサービス	法律・規制を遵守するための機能・証明を提供するサービス。 相互接続により、ルール遵守のチェックや証跡の収集を自動化しつつ、クラウド環境のセキュリティリスクや設定不備を常時監視することができる。
DLPツール[9]	データの暗号化やアクセス制御、データの匿名化、監視等を行うサービス。 相互接続により、クラウドを利用する上でのリスクを低減し、セキュリティ対策のスピードを向上させる。
データウェアハウス	膨大なデータに対して高速にクエリ（検索）を実行し

[7] Application Programming Interfaceの略。異なるソフトウェア同士がやり取りできるようにする仕組み（インターフェース）。
[8] CIはContinuous Integration（コードを頻繁に統合して自動チェックすること）の略。また、CDはContinuous Delivery （いつでも実際の運用環境にリリースできる状態にすること）及び Continuous Deployment（自動で運用環境に反映すること）の略。
[9] Data Loss Prevention（データ損失防止）の略。

相互接続の対象となるサービスの名称	左記サービスの概要及び相互接続により可能となることの概要
	たり分析したりする基盤。 相互接続により、重要なクラウドセキュリティデータの収集及びスケジューリングの自動化が可能になる。
生成AI（LLM（基盤モデル））	大量のデータを事前学習し、自然言語処理を実行するAIモデル。 相互接続により、CNAPPが特定した問題や検出結果について、生成AIが対応の優先順位を付けたり、状況の整理等を行ったりすることができる。
事後対応型セキュリティ	上記(1)アを参照。 相互接続により、クラウドセキュリティの運用を効率化し、自動化されたインシデント対応、ワークフローの連携等可能にする。
ネットワークファイアウォール	ネットワークトラフィック（ネットワーク上における通信データの総量）を制御するためのセキュリティサービス。 相互接続により、通信の防御とクラウド全体の監視を統合することで、リアルタイムで状況を把握することができるようになり、クラウド環境の可視性と脅威検出機能を向上させることができる。
事前予防型セキュリティ	上記(1)ア参照 相互接続により、アカウント単位で脅威を可視化し、クラウド上の脅威への対応時間を短縮できるよう支援することができる。
ビジネスチャット	仕事のコミュニケーションに特化したチャットツール。 相互接続により、チャットのワークスペース内においてCNAPPから直接リアルタイムでセキュリティアラート（セキュリティに関する警告）やアップデートを受け取ることができる。

２　商品範囲

(1) CNAPPを含む各セキュリティサービス

前記１(1)アのとおり、セキュリティサービスは、事前予防型と事後予防型に大別することができ、また、目的（サイバー攻撃からの防御や不正アクセスの防止、データの暗号化、脆弱性の検出・修正等）に応じて機能が細分化され

ている。

こうした各セキュリティサービス間の代替性についてみると、例えば、需要者がサイバー攻撃からの防御を目的としたセキュリティサービスを導入したいと考えた場合、基本的にはサイバー攻撃からの防御機能を有するセキュリティサービスを選択する必要があるが、一方で、サイバー攻撃からの防御を主目的としていないセキュリティサービスであっても、その一機能として当該防御機能を持つ場合もある。また、例えばCNAPPの一種と分類される製品であっても、一般的にCNAPPに求められる全ての機能を満たしているわけではなく、CNAPPを利用したいと考えている需要者の要求に必ずしも応えるものではないという場合も存在する。

このように、セキュリティサービス間で機能が重複する場合もあれば、特定のセキュリティサービスが複数の機能を有するなど、一つの商品範囲として包括的に検討することが適切でない場合も存在する。また、CNAPP自体、新しいサービスで、技術の進歩や需要の変化に応じてサービスの変化のスピードも急速であることから、CNAPPの種類やそれに包含される機能群は、今後もその需要に応じて多様化する蓋然性が高い。このため、特定の機能を有するセキュリティサービスの価格が変化した場合における需要者の行動や他の機能を有するセキュリティサービスの供給者の行動を評価するには詳細な分析・検討が必要となる。

また、後記第６の２(1)を踏まえると、セキュリティサービスをどのように画定したとしても、当事会社グループの市場における地位は大きくないと考えられ、本件行為が競争に与える影響を検討するに当たり結論を左右するものではないと考えられる。

そこで、本件では、各セキュリティサービスの機能ごとの代替性を厳密に検討することはせず、「CNAPPを含むセキュリティサービス」及び「CNAPP」について、本件行為が競争に与える影響を検討することとした。

(2) CNAPPと相互接続することが想定されるサービス

前記１(2)のとおり、CNAPPと相互接続することが想定されるサービスは複数ある。図表１に記載のサービスのうち、セキュリティサービスについては、前記(1)と同様、セキュリティサービスの機能ごとの代替性を厳密に評価するには詳細な分析・検討が必要となる。

また、それ以外のサービスについても、種類や機能、内容等が多様であることなどから、各サービス間の需要の代替性及び供給の代替性を厳密に評価するには、詳細な分析・検討が必要となるが、後記第６の１のとおり、本件の主要な競争上の懸念は、組合せ供給による懸念や相互接続の遮断又は低下の懸念であり、CNAPPと相互接続することが想定されるサービスそれぞれについて厳密に一定の取引分野を画定しない場合であっても、これらの懸念について検討す

ることは可能と考えられる。

このため、本件では、CNAPPと相互接続することが想定される各サービスについて、機能ごとの代替性を厳密に検討することはせず、サービスごとに本件行為が競争に与える影響を検討することとした。

３　地理的範囲

(1) CNAPPを含むセキュリティサービス

セキュリティサービスは、インターネットを介して提供可能であるため、地理的な制約なくサービスを調達することが多い。一方で、大企業では先端的な知見を有する海外のセキュリティサービスを起用する傾向があるのに対し、セキュリティリスクが小さい中小企業等では日本語対応を求めて国内のセキュリティサービスを好んで選択する傾向にあるなど、顧客の属性によってサービスの購入先が異なる。

したがって、地理的範囲については、「世界全体」と「日本全国」を重層的に画定した。

(2) CNAPPと相互接続することが想定される各サービス

セキュリティサービスに関しては、前記(1)と同様である。

また、各種サービスのうち、例えばIaaS／PaaS型クラウドサービスや生成AIはインターネットを通じて提供される事業であることに加え、主たるIaaS型／PaaS型クラウドサービスや生成AIサービスは日本語に対応し、さらに、日本語によるサポート体制も整備されている場合が多いため、基本的に国内の需要者は、特に事業者の所在国を意識することなく購入していると考えられる。一方で、法規制への対応や情報管理の観点から、国内で開発された各種サービスを選択する傾向にある需要者も一定程度存在すると考えられる。

そこで、地理的範囲については、「世界全体」と「日本全国」を重層的に画定した。

第６　本件行為が競争に与える影響

１　本件行為の企業結合類型

本件行為によって生じ得る競争制限のメカニズム（セオリーオブハーム）は、おおむね以下のとおりであると考えられる[10]。

① CNAPPを含むセキュリティサービス市場又はCNAPP市場において、アルファベットグループとウィズグループの事業が統合されることにより競争を実質的に制限することとなる懸念

② 当事会社グループが、ウィズグループのCNAPPと、CNAPPと接続して利用する

[10] なお、以下のセオリーオブハームは、セキュリティサービスの機能ごとの代替性を厳密に検討しない前提で、通常考え得る市場における競争上の懸念を想定した上で検討したものである。

ことが可能なアルファベットグループのサービスとの組合せ供給（契約上の組合せ（抱き合わせ）又はバンドルディスカウント）により、これらの事業に関連する市場において閉鎖性・排他性の問題を生じさせる懸念（契約上の組合せ（抱き合わせ）又はバンドルディスカウントによる懸念）

③　当事会社グループが、当事会社グループ以外のCNAPPや、CNAPPと相互に接続して利用することが可能なサービスについて、当事会社グループのサービスとの相互接続性を遮断又は低下させることによって、これらの事業に関する市場において閉鎖性・排他性の問題を生じさせる懸念（相互接続性の遮断又は低下による懸念）

④　当事会社グループが、CNAPPを通じて競争者の秘密情報（例えば、アルファベットグループのIaaS／SaaS型クラウドサービスの競争者の秘密情報）を入手することによって、これらの事業に関する市場において閉鎖性・排他性の問題を生じさせる懸念（秘密情報の入手による懸念）

以上を踏まえると、本件行為は、上記①のセオリーオブハームに係る水平型企業結合及び上記②ないし④のセオリーオブハームに係る混合型企業結合に該当する。

２　水平型企業結合

(1)　当事会社グループ及び競争者の地位等

ア　CNAPPを含むセキュリティサービス市場

総務省の「令和７年版　情報通信白書」[11]によれば、世界におけるセキュリティサービスに関する市場シェア及び競争者は図表２のとおりであり、当事会社グループの市場シェアは不明であるものの、少なくとも上位５位までには入っていない。また、日本のセキュリティサービスに関する市場シェアは不明であるが、総務省の「令和７年度版　情報通信白書」によれば、令和５年の市場規模は5574億400万円で、外資系企業10社が日本の市場シェアの５割程度を占めるとされている。この10社の顔触れは不明であるが、ウィズの国内売上規模からすると、ウィズがこの10社に含まれているとは考えにくいことから、本件行為後の当事会社グループの市場シェアは僅かな増加にとどまると考えられる。

【図表２】セキュリティサービスの市場シェア（世界）

順位	企業名	市場シェア
1	Palo Alto Networks	9.3%
2	Fortinet	7.0%
3	Microsoft	6.0%

[11] https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/nd21a100.html

４	Cisco	5.6%
５	Crowd Strike	4.5%
	その他（当事会社グループ含む）	約70%
合計		100%

イ　CNAPP市場

セキュリティサービスのうち、CNAPPに限定した場合の市場の状況は図表３及び図表４のとおりであり、有力な事業者が複数存在する。

【図表３】CNAPPの市場シェア（世界）

順位	企業名	市場シェア
１	Ａ社	約10%
２	Ｂ社	約10%
３	Ｃ社	約10%
４	Ｄ社	約10%
５	ウィズグループ	約10%
６	Ｅ社	０～５%
不明	アルファベットグループ	０～５%
	その他	約50%
合計		100%
合算市場シェア・順位：約10%・第５位		

【図表４】CNAPPの市場シェア（日本）

順位	企業名	市場シェア
１	Ｆ社	約45%
２	Ｇ社	約10%
３	Ｈ社	約５%
４	Ｉ社	０～５%
５	Ｊ社	０～５%
６	Ｋ社	０～５%
９	ウィズグループ	０～５%
10	アルファベットグループ	０～５%
	その他	約30%
合計		100%
合算市場シェア・順位：０～５%・第９位		

(2)　小括

前記(1)を踏まえると、CNAPPを含むセキュリティサービス市場及びCNAPP市場

において、どのように市場を画定したとしても、当事会社グループが有力な地位にあるとは想定しえず、また、これらの市場には供給余力が認められる多数の有力な競争者が存在することから、競争者の牽制力が認められる。

以上のことから、当事会社グループの単独行動又は当事会社グループと競争者との協調的行動により市場における競争を実質的に制限するおそれはないと考えられる。

３　混合型企業結合

(1)　当事会社グループ及び競争者の地位等

ア　CNAPPを含むセキュリティサービス市場及びCNAPP市場

前記２(1)のとおり、当事会社グループが有力な地位にあるとは想定し得ない。

イ　CNAPPと相互接続することが想定される各サービス市場

前記第５の１(2)の図表１に記載したCNAPPと相互接続することが想定される各サービス単位で見た場合の市場の状況は図表５のとおりであり、いずれの市場においてもアルファベットグループの市場シェアは大きいとはいえない。

【図表５】CNAPPと相互接続することが想定される各サービス市場におけるアルファベットグループの市場シェア

サービス名		
市場	順位	市場シェア
IaaS／PaaS型クラウドサービス		
世界市場	第３位	約５％
日本市場	第３位	約５％
APIセキュリティプラットフォーム		
世界市場	第５位	約５％
日本市場	第３位	約10％
CI／CDツール		
世界市場	第６位以下	不明（僅少）
日本市場	第６位以下	不明（僅少）
メッセージングサービス		
世界市場	第４位	約５％
日本市場	第３位	約15％
コンプライアンス対応クラウドサービス		
世界市場	第６位以下	０～５％
日本市場	第６位以下	不明（僅少）

DLPツール		
世界市場	第６位以下	０～５％
日本市場	第６位以下	０～５％
データウェアハウス		
世界市場	第４位	０～５％
日本市場	第６位以下	０～５％
生成AI（基盤モデル）		
世界市場	第３位	約10%
日本市場	第２位	約５％
事前予防型セキュリティ・事後対応型セキュリティ		
世界市場	第３位	０～５％
日本市場	第３位	０～５％
ネットワークファイアウォール		
世界市場	第６位以下	０～５％
日本市場	第６位以下	０～５％
ビジネスチャット		
世界市場	第４位	約10%
日本市場	第３位	約15%

ウ　小括

前記ア及びイを踏まえると、CNAPPを含むセキュリティサービス市場及びCNAPP市場並びにCNAPPと相互接続されることが想定される各サービス市場において、当事会社グループは有力な地位にあるとは想定しえず、また、これらの市場には供給余力が認められる多数の有力な競争者が存在するといえる[12]。

(2) 競争制限のメカニズム（セオリーオブハーム）に関する検討

ア　契約上の組合せ(抱き合わせ)又はバンドルディスカウントによる懸念(セオリーオブハーム②)

需要者は、通常、CNAPPと相互接続することが想定される各サービスの購入を検討する際、CNAPPとの相性だけではなく、システム全体との相性や需要者が当該サービスを必要とする目的を最も達成できる製品を選定すると考えられるため、CNAPPと特定サービスの組合せが必ずしも需要者にとって魅力的なものになるとは限らない。また、前記(1)のとおり、当事会社グルー

[12] アルファベットグループはいくつかの市場において約10%～15%の市場シェアを有するが、どの市場にもアルファベットグループよりも市場シェアの高い有力な競争者がおり、それらの競争者には十分な供給余力が認められることから、仮にそれらの市場において当事会社グループが組合せ供給を行ったとしても、需要者は容易に他の取引先に切り替えることができると考えられる。

プは、CNAPPを含むセキュリティサービス市場及びCNAPP市場並びにCNAPPと相互接続することが想定される各サービス市場においていずれも有力な地位にはなく、さらに、それぞれの市場において供給余力が認められる有力な競争者が多数存在するため、仮にそうした組合せが行われたとしても、需要者は容易に他の取引先に切り替えることができると考えられる。このため、当事会社グループがCNAPPと特定のサービスを契約上組み合わせて（抱き合わせて）又はバンドルディスカウントにより販売したとしても、競争者の牽制力が弱くなる程度は大きくないと考えられる。

したがって、当事会社グループには契約上の組合せ（抱き合わせ）又はバンドルディスカウントによって混合型市場閉鎖を行う能力があるとはいえない。

イ　相互接続性の遮断又は低下による懸念（セオリーオブハーム③）

前記(1)アのとおり、当事会社グループのCNAPPを含むセキュリティサービス市場及びCNAPP市場における市場シェアは世界市場及び日本市場共に高いとはいえない。

また、前記第５の１(1)イのとおり、CNAPPは、主としてマルチクラウド環境における事前予防型のセキュリティサービスを統合する機能を有し、複数のセキュリティ機能を単一のダッシュボードに統合・可視化するものであることから、複数のクラウドサービスと接続できること及び複数のセキュリティサービスと相互接続できることを前提として提供されている製品である。また、アルファベットグループは、本件行為の目的の一つとして、自社が提供するクラウドサービスをウィズグループのCNAPPと連携させることによって、顧客が組成するマルチクラウドの中の一つとして導入されやすくすることを挙げている。

このため、仮に当事会社グループが当事会社グループ以外の製品との相互接続性を遮断又は低下させた場合、当事会社グループのCNAPPの接続先が限られてしまうこととなり、当事会社グループの製品自体の魅力や機能を損ない、かつ本件行為の目的も達成できないことになるため、相互接続性を遮断又は低下させる可能性は極めて低いと考えられる。

したがって、当事会社グループが相互接続性を遮断又は低下させることにより混合型市場閉鎖を行う能力及びインセンティブがあるとはいえない。

ウ　秘密情報の入手による懸念（セオリーオブハーム④）

CNAPPは、その性質上、顧客のクラウド環境やワークロードをスキャンし、顧客のデータを収集しながらセキュリティ機能を提供する側面を有する。そのため、本件行為後、アルファベットグループがウィズグループのCNAPPを通じて、アルファベットグループの競争者の秘密情報を入手し、当該情報を

自己に有利に用いることにより、競争者の競争力が減退し、市場の閉鎖性・排他性の問題が生じるとも考えられる。

この点、当事会社グループによれば、CNAPPにおいては一般的に、パブリックAPI[13]を利用して顧客のデータを収集しているところ、パブリックAPIは、CNAPPに限らず顧客のネットワークにアクセスする全ての第三者サービスにも広く提供されているものであり（すなわち、ウィズグループのみが顧客のデータを特別に取得できるものではない。）、そこから得られるデータには顧客のクラウド環境等の情報が含まれているものの、他のクラウドサービス自体を構築するコード等の秘密情報へのアクセス（プログラムやシステムの内部構造を閲覧するなど）はできないとされている。これは、パブリックAPIを提供する事業者が、自社に関する秘密情報を保護するため、アクセス範囲を特別に設計し、管理していることによる。

したがって、本件行為後、アルファベットグループがウィズグループのCNAPPを通じて、アルファベットグループの競争者の秘密情報を入手し、それによってクラウドサービスプロバイダー等としての競争優位性を獲得することは困難であると考えられるため、市場の閉鎖性・排他性の問題が生じるおそれはないと考えられる。

エ　小括

以上のことから、本件行為によって、市場の閉鎖性・排他性の問題を生じさせるおそれはないと考えられる。

第７　結論

本件行為により、一定の取引分野における競争を実質的に制限することとなるとはいえないと判断し、審査を終了した。

[13] 仕様が公開されており、外部の開発者や第三者が提供するサービスからも自由に利用できるＡＰＩ。