情報通信審議会 情報通信技術分科会 ＩＰネットワーク設備委員会

電気通信事業におけるパブリッククラウドシステム利用に関する検討作業班（第１回）

1. 日時

令和７年７月２８日（月）15時00分～16時50分

2. 場所

Web開催

3. 出席者

（１）構成員

内田主任（早稲田大学）

矢入主任代理（上智大学）

田中構成員（明治大学）

長谷川構成員（東北大学）

堀越構成員（株式会社日経ＢＰ）

宮田構成員（東京科学大学）

吉田構成員（国立情報学研究所）

（２）発表者

田部井氏（富士通株式会社）

山本氏（デジタル庁）

（３）総務省

湯本総合通信基盤局長

吉田電気通信事業部長

飯嶋料金サービス課長

【事務局】

枡浦電気通信技術システム課長

由本電気通信技術システム課課長補佐

（４）オブザーバー

NTT東日本株式会社

NTT西日本株式会社

株式会社NTTドコモ

楽天モバイル株式会社

KDDI株式会社

株式会社インターネットイニシアティブ

ソフトバンク株式会社

グーグル・クラウド・ジャパン合同会社

富士通株式会社

アマゾン ウェブ サービス ジャパン合同会社

さくらインターネット株式会社

日本電気株式会社

ノキアソリューションズ＆ネットワークス合同会社

エリクソン・ジャパン株式会社

日本クラウド産業協会

4. 議事

(1) 本作業班の進め方

事務局（由本課長補佐）より、資料１－１に基づき、説明が行われた。主な質疑応答は以下のとおり。

【田中構成員】

現在、クラウドだけではなくＡＩサービスがオンライン、クラウド上から使えるようになったため、データ保護の管理の在り方、そしてセキュリティの在り方について、また、通信との接続の在り方についても非常にタイムリーで重要な会議だと感じております。

【内田主任】

御指摘のように様々な角度でクラウドというのは非常に注目を浴びているところでご

ざいますので、丁寧な議論をしていきたいなと思います。

そのほか、いかがでしょうか。私としましても、この本作業班の進め方という形で今、御説明いただいた内容に関しましては特段気になるところはなくて、御提案いただいたような形で進めていければと考えております。

こういった非常に難しい問題である一方、電気通信事業者さんとクラウド事業者さんとのお話をしっかり聞きながら検討を進めていかなければ、健全な協力関係や、いい技術基準というものは設定できないと考えておりますので、その辺は主任としましても留意をしながら進めていきたいところでございます

(2)　クラウド環境に関する技術の事例

富士通株式会社（田部井氏）より、資料１－２に基づき、説明が行われた。主な質疑応答は以下のとおり。

【長谷川構成員】

技術的なところは、決して専門家ではございませんので分からないところがあるので、その上でお聞きいただければと思うのですが、この手のシステム、絶対にセキュリティの事故が起こりうると思う。どれだけシステムをちゃんとつくっても、どこかに事故の要因となるところというのはあると思いますが、その場合どうするか気になります。

特に途中で出てきたアテステーションサービスというようなサービスを使うようなところだとプレーヤーが増えて、こういう事故のリスクが増えそうな点についてお聞かせ願えればと思います。

【富士通株式会社（田部井氏）】

非常に難しい問題かと思います。もちろんヒューマンエラーみたいなところもある中で、このアテステーションについても世界の各機関で懸念があり、誰が認証機関を立ち上げて、どのように承認していくかの社会実装のスキームは結論が出ていないところがあると認識しております。

それぞれの使い方に合わせて、クローズにする部分、オープンにする部分であるとか、そこは適宜、使うワークロードや、ユースケースに応じた形が出てくるのかなと思います。あとは全般的には脅威モデルに対しての対策は、ある程度、網羅的に議論しながら対応し

ていく必要があると思います。

【堀越構成員】

１点目、CPUとかＶＭでやる方式というのを御説明いただきましたが、このサービスとかハードごとの相互接続性について、もう少し教えていただけないでしょうか。CPUがトラストの肝となりますとCPUベンダごとにロックインされそうな気がしましたので、ぜひこの辺りの状況を教えてください。

２点目、このConfidential Computingサービスについて各国の法規制、例えばＧＤＰＲとかにはもう対応済みみたいな情報が出ていますか。

また、Confidential Computingみたいな仕組みに対して通信の秘密の要件は担保される可能性はあると見ていいのでしょうか。可能性を含めて教えてください。

【富士通株式会社（田部井氏）】

サービス自体はそれぞれ、既にAMD、Intelベースに対応したConfidential Computingサービスが提供されているという理解をしています。

各社のサービスとハードとの連携に関しては、根本的なConfidential Computingサービスとしてはそれぞれ独立して提供されており、その上でお客様がＶＭを使うことを想定しているのが基本的な今々のユースケースかなと思います。

あとは、アテステーションについては、先ほど言及がありましたが、ここも別サービスとして立ち上げて提供されているので、例えば恐らくなんですけれども他社クラウドでのConfidential Computingサービスを使って、アテステーションはまた別のクラウド事業者のサービスを使うケースも可能であると思います。

【由本課長補佐】

今般ご紹介いただいたConfidential Computingについて、通信の秘密の保護をしっかり担保できるような技術なのか、ないしは、この技術自体の普及状況なども踏まえつつ技術基準として位置づけることが適当なのかどうかといった観点は、今後の作業班での議論の中でも深めていけたらありがたいと考えております。

【堀越構成員】

各国の法規制の状況も同じような形でしょうか。

【由本課長補佐】

各国がConfidential Computing技術を技術基準に適用して扱っているかどうかまで、総務省でもまだ把握し切れておりませんが、必要なタイミングで関連情報をフィードバックしたいと考えています

【内田主任】

今の通信の秘密のところに関しましては私も気になっておりまして、この通信の秘密とConfidential Computingの整合性などについては今後、議論が必要になってくるだろうなと思います。

このConfidential Computingを活用するということで、クラウド上でも通信の秘密が実質的に担保できるのかどうかということ､技術的にはそうだと言えるのかもしれませんが、制度や基準の上で、それが十分に認定できるのか、評価できるのかというところ、そこら辺は今、そこから議論しなくてはいけないと理解しましたので、今後議論を深めていければなと思ったところでございます。

【宮田構成員】

重要な情報をこれからきちんと守りながら通信していく意味では、こういうような技術ってすごく大事と感じまして、さらに今回の御発表の内容というのは日本国内で設計しているというお話もありましたので、重要な情をしっかり守っていく意味でも、とても使える技術なのかなと思いました。

一方でお聞きしたいことが、これからの技術という説明に関してです。これから開発していく技術であるため、国際関係も含めて、標準化の動向もいろいろコミットしているというお話ですが、今の標準化の動向で、もし説明できるところがあれば教えていただきたいです。

【富士通株式会社（田部井氏)】

ご意見ありがとうございます。基本的にはConfidential Computingのベース機能仕様はフィックスされており、あとはそこをどう実装していくかというところで各社のハードへ

の適用など様々な動きがあります。また、さらにフィックスといっても例えば、 アクセラレーターなどのデバイス間への適用も含めて活用していく等、Confidential Computingの機能を拡張していくという動きはございます。そういったところは、また新たな仕様の中で、Confidential Computingコンソーシアムや各種コミュニティが中心に仕様を含めた議論が進んでいる状況です。

したがって、上記の動きに対して、基本的には富士通としてはArmチップでの実装を検討しており、各社Intel、AMD含めて、サービス提供しながら、標準化を見据えた仕様検討を進めているところありますので、そういった状況になります。

【宮田構成員】

日本国内で設計していくところと、最終的には標準化も含めた世界動向も見据えながらつくっていくというところが、大事かなと思いますので、その辺りも議論できれば思いました。

あと１点コメントですが、先ほど内田先生などからもありましたように通信の秘密が気になりまして、今回のこの技術が通信の秘密に関してうまく担保できるものなのかどうかというところも議論していけるといいかなと思います。

【富士通株式会社（吉田）】

少し補足の説明をいたします。通信の秘密について、我々富士通のコンピューティングチームはまだ通信全体をシステム全体として把握できないところが正直なところでございます。ただ、キーとなるのはメモリ上のデータが今まで暗号化ができてなかったところが、新しくできてくることが一つの大きな課題の解決になるものだと思っています。

今後議論させていただくところで、通信の秘密の観点では全体のシステムとして、そこに穴がないかがポイントになると思っています。それがハードウェアと、それ上でのソフトウェアをいかにオープンな形、スタンダードでやっていくかというところが課題と認識しておりますので、今後議論させていただければと思います。

【田中構成員】

７ページのアプリケーションの修正とあるのは、これ、バイオスレベルで修正するとチップのところまで暗号化できるというチップですよという理解でいいのでしょうか。そう

すると、そこまで修正しちゃうと外部から介入できなさそうだなとか、もしそれが本当であるならば、仮想的なローカル環境というものがいよいよ完成するというのは、とても重要な技術進化だなと思います。そうすると日本のチップメーカーさんも対応しようとしているということはとても重要だと感じています。

質問について、このチップレベルでConfidential Computingが対応すると、今までの一般的な共用の仮想マシンというのはアプリケーション修正、バイオスを修正しないような理解でいいのでしょうか。

２つ目についてパイロットプロジェクトに参加する企業が出てきているということですけれども、既にそういった企業さんの特徴など出てきていますでしょうか。

【富士通株式会社（田部井氏）】

１点目について、直接アプリの修正を行う点の前提として、まず基本的にはアプリケーションというのはＯＳ上で動くソフトウェアであり、ＯＳからプロセスとして見えます。バイオスのレイヤーのことではないです。ただ、アプリケーションについて、ＯＳ上で動くソフトの一部の中身を変えないと、そのプロセスごとの粒度でメモリ暗号化の保護を実現できないというのが、Intel社のＳＧＸになります。ＶＭ方式は、基本的にはＶＭが使うメモリを丸ごと暗号化するということです。

【田中構成員】

ということは、チップの挙動を処理する、設定するもののアプリケーションが、それは結構新しいものとして出てきたという理解でよろしいですか。

【富士通株式会社（田部井氏）】

既存のアプリケーションを修正するというイメージです。

【田中構成員】

何か仮想マシンとかで入れたりセキュリティを設定したりというのは、うっすらレンタルサーバーとかでやったことはありますが、そのチップレベルでエンドユーザーだと触れないので、じゃあ、具体的にどんな場面だろうと思いました。

参加企業さんに既に特徴とか、こういった企業が参加しているのが目につきますとか、そ

ういう情報はお持ちですか。

【富士通株式会社（田部井氏）】

既にクラウドベンダが機密ＶＭのようなサービスの提供を開始していると認識はしております。したがって、ユーザーから見ると単純に自分が動かすＶＭ環境が、もう既にメモリ暗号化された状態で使えるところがまず一つあります。

他に具体的には、マルチクリーンルームなど、金融機関等でまだ詳細を把握していないところですが、ユースケースとしての事例はお客様から聞くということはあります。

【田中構成員】

大学で、あと今、ノートブックのＬＬＭとかを使おう思いますが、成績とか入試とかこれから機微な用途というものもあるかと思います。今、ノートブックＬＬＭは個人だと触れないので、どうしても情報がないなというところです。

【富士通株式会社（田部井氏）】

ＡＩに関しては、特にユースケースとして一番多く議論されている部分なので、その辺は既に海外各社、メジャーな企業ではもう活用され始めているという認識を持っています。

【富士通株式会社（吉田）】

補足させていただきます。まず、最初の質問、アプリケーションの変更という点では、IntelのＳＧＸという実行環境のメモリを暗号化する意味では、このIntelの２つ、ＳＧＸとＴＤＸという同じテクノロジー、同じ目的なのですが、ＳＧＸに関しては暗号化できるメモリの容量の制約があるなど幾つかの制約がございまして、ＳＧＸに関しては既存のアプリはどんなものでもよいわけではなくて、ＳＧＸの暗号化に対応できるようなアプリの変更が必要になります。

一方で、インテルTDX、AMDのSEV、ArmのConfidential Computingアーキテクチャの CCAの３つに関しては既存のＶＭ環境、いわゆる仮想環境、丸ごと、そのままで変更なしで、Confidential Computing設定でＶＭのデータがユーザーには見えるが管理者から急にハードウェアに鍵がかかって見えなくなるという、見え方になります。補足になればと思いました。

あともう一つ、パイロットプランのところに関しましては、こちら、金融やヘルスケアで扱う個人情報など機微度の高いものに対してConfidential Computingを使いたいという要望のお客様というのはいらっしゃいます。ただ、それがまだ全面的にどこまで使えるのかというところ、手探りで見ているというのが今の状況です。

もう一方､違う見方ですとクラウドベンダはお客様のデータを見たくないですけれども、現在のコンピュータアーキテクチャというのは管理権限があるとユーザーのデータは見えてしまうというアーキテクチャ上のセキュリティ欠点がございます。管理者が見たくもないのに見えてしまうところがクラウド業者としても課題認識がありまして、そこがハードウェアに鍵をかけることによって、管理権限者あるいは管理権限のソフトが侵入されて見えてしまうリスクを抑えるために、あえてハードウェアによる暗号化をしてお客様の情報を見ないようにしたい要望があります。金融などのユーザーだけではなくて管理者も必要性を感じてConfidential Computingに取り組んでいるのが今の実態です。

これが今後２７年から以降はかなり広がると考えております。そこにFUJITSU-MONAKAを提供していくことで、あとは鍵をかけるのがハードウェアですので、ここはどこのベンダが鍵をかけるか、ハードウェア設計をしているかが重要ではないかというのが富士通の今の考え方になります。

【田中構成員】

ハードウェアに鍵をかけると、鍵のかかった金庫を誰に開けるか問題が出てくると思いますけれども、そういった点についても追々また、お聞きしていければと思います。

【矢入主任代理】

パブリッククラウドを利用して通信ネットワークサービスを実現する際には、クラウドに関する業界標準や国際認証に準拠するだけでなく、総務省の定める電気通信事業法に基づく要件が重要になると思いますが、電気通信事業法の基本的な部分に関する基準に関して富士通様はどのようなお考えや御要望があるか、お聞きしてもよろしいでしょうか。

例えば事故や災害などによる電気通信設備の損壊、または故障による著しい支障等が起きないようにするのを止めるとか、防止するとか、電気通信役務の品質の確保、その他の接続電気通信事業者様との責任分界、事故が起こった際とかにどういうふうに責任分解しますでしょうか。

【富士通株式会社（田部井氏)】

その点に関しては我々、今回はコンピューティングの技術ということの御紹介から入っておりまして、電気通信の領域、また、あるいは我々としてのクラウド事業との関わりというところに関しては今後のお話として我々も調べて、議論させていただきたいというところでございます。

【由本課長補佐】

矢入主任代理からの御質問に関連して補足いたしますと、今後クラウド事業者へのヒアリングを予定しておりますが、先ほどおっしゃっていただいたような点についても、改めて質問するタイミングがあるかと思います。

【吉田構成員】

御発表どうもありがとうございました。大変参考になりました。

それで幾つかお伺いしたいのですけれど、まず、先ほどＶＭとコンテナという話を伺いましたけれども、こういった仮想環境が前提になるのでしょうか。つまりベアメタルを提供するサービスもあるかと思うのですが、そういうものも対象になるのでしょうか。

それからもう一つ、仮想化基盤というといろいろな種類のものが世の中にはあり、クラウドにおいてもVMWareを使っているところもあるし、KVMなどもあるかと思うのですが、そういった仮想化基盤には依存しないのでしょうか。

それから、今どきですからGPUは必ず使うことになると思っており、先ほどNVIDIAにも対応されているとお伺いしましたけれども、そのNVIDIA対応について、アプリケーションからはGPU自体は透過的に見えるものでしょうか。ご教示をお願いいたします。

【富士通株式会社（田部井氏)】

まずは、仮想環境についてですが、現在も我々、KVMをベースに対応をしていきます。基本、VMWareを扱われているお客様が非常に多いかなと思うのですけれども、ここについても、Confidential Computingへの対応をしていくという動きは聞いております。我々の場合だと、Arm上についてはKVMを対応していくというところです。

ベアメタルについても、メモリ暗号化という意味では対応しています。ここも

Confidential Computingと呼んでいいかというところがありますけれども、基本的にはメモリの暗号化については、ベアメタルでも対応というのはできています。仮想化ベースでないと、このConfidential Computingという定義をカバーできないのではないかという理解ではおります。

【富士通株式会社（平井氏）】

富士通の平井と申します。GPUについては、基本的にはこの機能自体がCPUとか、プロセッサベースの暗号化になりますので、GPUに載っているプロセッサのConfidential Computingというか機密機能、これに基づいて暗号化されます。ですので、ホスト上のCPUとGPU上の暗号化というのは違うプロセッサ上で暗号化されますので、ここについては、お互いに逆に見えなかったり、見えたりするようにするためにはお互い何か鍵を共有するなりという、また別の仕組みになってくるという理解をしています。

【富士通株式会社（田部井氏）】

そうですね。先ほど言ったデバイスアサインメントという機能が今、出てきているというところで、CPU、GPU間、含めたところのConfidential Computingのところというのは、これから普及してくる、仕様含めて議論されて普及してくるような状況です。

(3)　政府が活用するクラウド環境の状況　（非公開）

デジタル庁（山本氏）より、資料１－３に基づき、説明および質疑応答が行われた。

(4)　その他

事務局より、電気通信事業におけるパブリッククラウドシステム利用に関する検討作業班の第２回目については、別途連絡する旨説明が行われた。

以上