【副読本 資料 ⑤】

『法務、リスク管理、クラウド主権、プライバシー、行政分野 参考教材』

行政クラウド・ネットワーク

日本以外の先進国の傾向の調査

～ 日本以外の先進国の政府機関は
どのような行政クラウド・ネットワーク戦略を
策定しているのか？
EU およびヨーロッパ各国の戦略 ～

未発表のメモのため、参加者限り【再配布禁止】

2026/02/14

登 大遊

内容

第 1 節　はじめに

まだ、調査途中であるが、ヨーロッパでは、各国政府および EU の政府関係者が、米国のパブリッククラウド事業者のサービスの利用に関連し、クラウド主権の問題に関して、技術面と法制面の両面で、各国政府は、結構踏み込んだ検討、リスク分析、アクション策定を、積極的に行なっている。

特に、

「何でも外国クラウドにデータを非暗号化 (暗号鍵がクラウド事業者側に保管または送信されるものを含む) 状態で保存してしまう」

ことの問題意識が強く認識されている。

このような先進国の中では、日本政府 "だけ" が、率先して無警戒に米国クラウドをどんどん利用することを進めていることに見える。

このことから、日本は、行政のクラウド利用の方針に関して、国際的にみて相当異色なのではないかと思われる。

以下に 4 個の文献を日本語訳したものを掲載する。

第 2 節は、2021 年に公布された、EU のサイバーセキュリティ機構である ENISA (日本の内閣サイバーセキュリティセンターに相当) の公式の調査報告書・戦略提言書である。現在ヨーロッパに存在するクラウド主権問題の所在を述べ、解決のための明確な方向性を提示している。

第 3 節は、ヘルシンキ大学の学者・弁護士による 2021 年の論文であり、オラ

ンダ政府、スウェーデン政府の事例を元に、EU 裁判所のシュレムス II 判例も参照し、米国クラウドをヨーロッパ各国政府が利用する場合に実際に発生した法的問題と技術上の未解決問題について分析をしている。

第 4 節は、ZDNet の記者による 2019 年の記事であり、フランス政府、オランダ政府、ドイツ政府、スウェーデン政府が米国クラウド経由の情報漏えいリスクに対応するため、プライベートクラウドを利用していることを示すものである。ドイツの経済エネルギー大臣の「米国クラウドに代わるヨーロッパのクラウドが必要である」という発言も注目に値する。

第 5 節は、デロイト社による 2023 年の記事であり、欧州全体において機密情報に関する懸念が高まっていることを示している。その対策として、欧州委員会の委員長は、(米国の) ハイパースケーラーを複製するのは遅すぎるかも知れないが、一部の分野で技術主権を達成することは今からでも可能であると述べている。

第２節　EU 全体の方針：ENISA「Cybersecurity Research Directions for the EU's Digital Strategic Autonomy」

ENISA (欧州連合 (EU) サイバーセキュリティ機構), 2021/04/23
ISBN: 978-92-9204-458-9
https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy/

「3.1. データ・セキュリティ (抄)

データとそれを処理するアルゴリズム (注: ソフトウェアのこと) の両方をコントロールできなくなるリスクが問題である。EU は一般データ保護規則 (GDPR) により EU 市民の情報を保護しようとした。しかしながら、多くのユーザーは、データの収集と処理の両方において、GAFAM (Google, Amazon, Facebook, Apple および Microsoft) や BATX (Baidu, Alibaba, Tencent and Xiaomi) の提供するサービスに依存してしまっている。これにより、EU の一般データ保護規則による保障は、すでにある程度失われてしまっている。

問題は、大規模クラウド事業者 (Amazon, Microsoft, Google, SalesForce) が、ヨーロッパ領域外 (注: 米国のこと) に本拠地がある点にある。これにより、差し迫ったリスクが存在している。米国のクラウド法により、(米国に本拠地がある) クラウド事業者は、ヨーロッパ市民のデータを米国政府に差し出すよう強制される可能性があるのだ。この状態は、EU 市民の個人データ保護を目的とする一般データ保護規則 (GDPR) などの法令に違反する状況である。この問題を解決するために、EU および EU 加盟国は、統治のためのクラウドサービスを立ち上げる活動を主体的に開始した。ただ、現段階では、普及率とカバー範囲の両面において、その効果は限定的である。」

「3.2. 信頼できるソフトウェア・プラットフォーム (抄)

日常的に利用される大半の品目に、コンピューティングと通信機能が入り込んで

いる。これにより、ヨーロッパは、サプライチェーンの途絶に対して脆弱になる可能性がある。例えば、Google は、中国へのサービス提供を部分的に停止したし、オープンソースソフトウェアの提供をのぞき、Huawei (注: 中国企業) への供給を停止した。同様に、(米国の) 大手ソフトウェアベンダーがヨーロッパへの提供を中止すると決定した場合、ヨーロッパがどのように対応するべきかが、定かではない。このような事態に対応するに際しては、多大な犠牲を要し、多額の追加コストが発生するおそれがある。ヨーロッパに居住するソフトウェア開発者やソフトウェア企業は、相当数、存在する。だが、現在使用されているソフトウェア・コンポーネント (注: 米国クラウドサービスのソフトウェアのこと) が使用不能となった場合、必要不可欠なそれらのソフトウェアを (注: ヨーロッパで継続して利用できるものに) 置換できる保証がないのである。

今や、ソフトウェアはクラウド・サービスとして稼働されるようになってきている。しかし、前述したように、主要なクラウドプラットフォームはヨーロッパ外 (注: クラウド事業者の本拠が米国であること) にある。これは、いくつかの問題を引き起こす。第一に、そのようなベンダ (注: クラウド事業とソフトウェア開発事業の両方を行なっている Microsoft 社のような企業のこと) は、自社のソフトウェアの利用を自社のクラウド上でのみに制限する可能性があり、その結果、機能とデータの両方が、ロックインされることになる。第二に、そのようなクラウド事業者は、(注: 競争相手である) 他のソフトウェアベンダーが、当該クラウド事業者のクラウド上でネイティブなソフトウェアサービスを作成することを禁止するおそれもある。仮に、ヨーロッパがこうしたクラウドプラットフォームへのアクセスを失うことになれば、その結果、クラウドプラットフォーム専用のソフトウェアサービスへのアクセスも失うことになるのである。」

「さらに、システムやサービスは、独立したサードパーティのライブラリやサービスに依存しており、ソフトウェア開発者のコントロールの及ばないものである。一例として、SAP (注: ヨーロッパ内にあるドイツのソフトウェア企業) のような大手ソフトウェアベンダーでさえ、現在、自社製品のソースコードのごく一部しか自作しておらず、自社製品の機能の 90% 以上を、オープンソースソフトウェアに依存している。」

「ヨーロッパは、ヨーロッパ以外から供給されるソフトウェアを適切に検証する

ために、独自のソフトウェア・プラットフォームとツールを作る必要がある。同様に、ヨーロッパは、サプライチェーンが寸断された場合にも対応できるよう、商用製品に代わるオープンソース・ソフトウェアをヨーロッパ内で支援、促進、ホストすべきである。最後に、クラウドサービスの需要が高まる中、ヨーロッパはオープンで安全なヨーロッパのクラウドソフトウェアサービス市場を確実に実現する必要がある。」

「より具体的な行動項目は以下の通りである:

(1) 信頼できるオペレーティングシステム。ヨーロッパは、オペレーティングシステム開発に関する専門知識を維持することを確保すべきである。たとえ、その範囲が産業システムやセキュリティコンポーネントなど特定の環境に限定されていたとしても (ヨーロッパに専門知識が無いよりはましである)。ヨーロッパは、サーバーコンピュータ、デスクトップコンピュータ、モバイル機器のための代替オープンソース・ソフトウェアの選択肢の出現を奨励すべきである。

(2) 信頼できるミドルウェア。今日、ソフトウェアシステムは、ソフトウェア開発者のコントロールの及ばない独立したサードパーティのライブラリやサービスに依存している。ヨーロッパは、こうしたサードパーティのライブラリやサービスを検証し、それらがシステムに新たなソフトウェアの脆弱性を持ち込まないようにする必要がある。

(3) マルウェアやボットネットの検出。特に政府システムや重要インフラのような機密性の高い環境では、ヨーロッパはマルウェアや悪意のあるネットワーク活動を検知する能力 (専門知識とツールの両面) を維持する必要がある。

(4) システムと仮想化のセキュリティ。仮想環境が普及し、コモディティ化してきたことに伴い、ヨーロッパはハイパーバイザー (注: クラウド等の基盤システムの心臓部の仮想化技術のこと) の本質を理解し、サイバーセキュリティ機能を実装する能力を保持する必要がある。これは、3.7 節で述べるネットワークオペレーティングシステムとルーティング機器のサイバーセキュリティの側面と関連している。

(5) 安全なソフトウェア開発プラットフォーム。ヨーロッパは、安全なソフトウェアを開発、評価、認証する能力を維持すべきである。これには、(i) 安全なソフトウェアシステムを構築する能力と、(ii) 構築されたシステムが特定のセキュリティ

要件を満たすことを保証する能力が含まれる。これは、サードパーティのライブラリやサービスも安全であることを保証するのに役立つ、『信頼できるミドルウェア』に依存する。

(6) リスク評価プラットフォーム。複雑な ICT システムのセキュリティを確保するためには、潜在的な攻撃のリスクを評価し、設計時と実行時の両方で必要な対策を定義する必要がある。達成されたセキュリティ・レベルを測定することは、困難な作業である。この作業には、システム (ソフトウェアとハードウェアの両方) の依存関係の評価も含まれる。

(7) 信頼できるセンサー。(略)

(8) オープンなクラウド・ソフトウェア・サービス。ヨーロッパは、クラウドソフトウェアサービスのオープンな市場を創出し、異なるクラウドプロバイダー間で、同様のクラウドサービスを利用できるようにする必要がある。そうすることで、ヨーロッパのユーザーが、特定のクラウド・サービスにロックインされることを防ぐことができる。また、ヨーロッパのソフトウェア・ベンダーが、クラウド・サービスを提供できるようになる。加えて、特定のクラウドが利用できなくなった場合であっても、ヨーロッパが重要なソフトウェア・サービスへのアクセスを失うことを防ぐことができる。」

「3.7. デジタル通信セキュリティ (抄)

仮想通信環境 (クラウド・コンピューティング・インフラ、Software-Defined Network、スライシングなど) への移行は、企業も政府も同様に急速に採用している。ところが、我々は現在、多くの点で重要なサービスを、ヨーロッパ外で運用されているプラットフォームに依存している。クラウドの基本的原則は、インフラがスケーラブルであり、通信が可能であるという事実の上に成り立っている。(略)

サービスのデジタル化により、あらゆる主要分野でデジタル・インフラへの依存度が高まっている。例えば、現在では多くのサービスがクラウド・プロバイダーによって提供されている。そのサービスを利用する企業や政府にとって、利用不能、完全性の喪失、機密性の侵害は、深刻な結果をもたらすおそれがある。また、マルチテナントのクラウドストレージの利用も、セキュリティリスクをもたらすのであ

る。さらに、たとえば (注: クラウド事業者への) サービス妨害 (DoS) 攻撃などによって金融業務が停止したならば、ほとんどの国や企業の業務や経済に影響を与える可能性がある。」

第 3 節　EUの法的議論の現状と、オランダやスウェーデンの事例 ――「クラウド上の行政サービスに対する米国によるデータ監視リスクの軽減策」

Jockum Hilden 博士・弁護士, ヘルシンキ大学, フィンランド, 2021/09/30

https://policyreview.info/articles/analysis/mitigating-risk-us-surveillance-public-sector-services-cloud

「米国クラウド法は、米国に本拠がある企業に対し、令状により、(物理的にヨーロッパにある米国クラウドサービスの) サーバー上のデータを米国政府に引き渡すことを強制している。(略) これは、基本的人権の尊重に関して未解決の問題を生じさせている。そのため、スウェーデンでは、行政機関は米国企業のサービスを容易に利用できないという状況に陥っている。機密情報であるスウェーデン国民の個人データが、スウェーデンの裁判所の審査を経ることなく、米国に転送されるリスクがあり、これはスウェーデンの法律上違法である。外国の裁判所命令は、(自国における) データ転送の法的根拠にはならない。」

「オランダ政府では、Microsoft Office に関する包括的評価が行なわれた。その結果、Microsoft Office のデータやテレメトリ情報 (ソフトウェアの動作中の内部状態を集約して開発元企業に送付すること) の同社への送付は、行政機関で Office を使用する際の重大なリスクであることが発見された。Microsoft はいくつかの設定を施し、かつ、オランダ政府との契約を調整したが、未だ問題は満足に解決されていない。」

「問題は、アメリカ合衆国憲法修正第 4 条の『個人、住居、書類、所持品の安全を保障される権利』は、米国外にある外国人に対して保障されないという点にある。(略) 米国のクラウド事業者は、(クラウドの) 顧客に対して、米国政府から顧客を保護するための通知ができない。」

「結論として、基本的に、米国の SaaS ソリューションは、「シュレムス II」(欧州司法裁判所 2020/07/16 シュレムス II 判例の規範) の要件を満たしていない。なぜならば、SaaS の原理上、クラウド事業者は少なくとも一時的には暗号化キーにアクセスできる必要があるためだ。この問題を契約的、組織的、技術的に解決する方法は、(現時点では) 存在しないのである。欧州データ保護会議は、(クラウド事業者が暗号化キーにアクセスできるか否かのリスクの評価については) 「客観説」、すなわち、第三国 (クラウド事業者の本社が所在する国、すなわち米国) の法的枠組みに基づく事実上の能力により、評価されるべきである旨と定めた。(すなわち、米国の) 行政機関が、EU の法律に従わずに秘密データにアクセスする可能性が本当にあるだろうか、という主観的要因に基づくべきできないことが明確化された。この結論は、欧州委員会の示した基準 (前記の、行政機関が、EU の法律に従わずに秘密データにアクセスする可能性があるだろうか、という主観的要因を考慮すべき説 = 「主観説」) と異なる。」

「オランダ政府は、Microsoft との契約を処理するだけに、専門の "Strategic Vendor Management Microsoft" というチームを組成している。同部門が 2018 年に民間に調査委託して行なった Office 365 のデータ保護影響評価の結果レポートでは、『Office アプリの診断データとして (送信) 処理されるデータには、5 つの高レベルな機密情報侵害リスクがある』、『行政機関は、職員に Office Online およびモバイル版 Office アプリの使用を控えるべきポリシーを制定することを推奨する』と結論付けている。(略)

この問題について、2019 年、Microsoft は透明性を高めるとする新たなツールを提供し、データ収集と処理の範囲を (自主的に) 制限した。オランダ政府は新たに監査をすることができるようになった。これにより、(スタンドアロンの) Office アプリの問題は解決したが、Web 版 Office については依然として問題がある。(略)

SaaS (の Web アプリ) では、クラウド事業者を、(ユーザーの秘密データの) コンテンツから完全に隔離することは、不可能である。Microsoft 社もこれを認めている (2020 年)。ユーザーは暗号化キーを支配する必要があるが、Web アプリではユーザーが暗号化キーを支配できない。」

「スウェーデンでは、(行政機関が) 米国のクラウドサービスを利用することが機密情報の不法開示に当たるかどうかについて、行政機関、サービスプロバイダ、法律事務所それぞれによる議論がなされている。(略)

米国のクラウド事業者が (米国政府によって) 海外の顧客の情報の開示を強制される可能性があるという状態となっていれば、(スウェーデンの行政機関が) 機密情報をそのような米国のクラウド事業者のサーバーのアップロードする時点で、機密情報の違法な開示に当たる可能性があるという点が、論点である。

米国クラウド法の制定によって、スウェーデンの行政機関と既存の米国パブリッククラウド事業者との秘密保持に関する契約は無効な状態となったという主張がある。また、実際に米国政府がこの方法により (スウェーデンの秘密の) 文書にアクセスする可能性がとても低いので、(そのような低い可能性を考慮した) 法的な解釈は不合理であるという主張もある。この問題の本質は、危険の評価は法的枠組みに基づいて議論されるべきか、事実状態に基づいて議論されるか、という点にある。

確かに、米国政府がスウェーデンのある地方自治体の文書にアクセスする可能性は低い。だが、そのような事態が生じた場合は、当該地方自治体は、そのようなアクセスを止めることができないのである。この場合は、(当該地方自治体は) 機密に関する法律に違反したことになる。」

「オランダとスウェーデンの経験に基づき、次の結論が引き出せる。

第一に、(米国事業者との) クラウドサービス契約には、米国政府が米国クラウド事業者に (ユーザーデータの) 開示命令を出した場合に異議を申立てる権利を含める必要があることは、明らかなことであるが、このような (スウェーデン政府や地方自治体による) 異議申立てが、米国の裁判所で考慮される保証はない。一応は、契約上、クラウド事業者側が米国政府に自主的に従うことは防ぐことが可能である。

第二に、行政機関がすべての個人データの管理権を保持できるように、最新の注意を払って精査することが必要である。

第三に、欧州データ保護会議の定めた条件を満たすために、米国のクラウド事業者に対して、(行政機関の) コンテンツや診断データが可能な限り隔離される必要がある。これには、クラウド事業者のデータへのアクセスを制限するために、暗号化

キーをクラウド事業者に送信しないことが必要である。

第四に、第三の対策により SaaS が利用できなくなる。欧州データ保護会議の見解 (「客観説」) によると、SaaS の利用は、欧州司法裁判所シュレムス II 判例に準拠することが不可能になる。ただし、欧州委員会による「主観説」によれば、処理の性質と関係個人データのリスクを徹底的に分析すれば (SaaS 利用は) 可能であるということになる。

第五に、オランダの事例により、(Office アプリ等がテレメトリ診断データ等として) データを漏えいしていないかどうか、データフロー (送信される中身) を定期的に検査する必要がある。」

「行政機関が、EU データ保護法への準拠を唯一保証する方法は、米国クラウド事業者から (暗号化を施すことで) 非暗号データを完全に隔離することである。しかし、これにより SaaS は利用できなくなる。このジレンマの原因は、次の 5 点に集約できる。

1. 米国の最高裁は、米国領土外の外国人に基本的人権を認めておらず、今後も認めないであろう。

2. 米国政府が (米国クラウド事業者を通じた、欧州政府データの) 監視を必要かつ欧州のルールに基づいたものに (自主的に) 限定する可能性は低い。

3. (1 により) 米国が憲法上の要件を満たす形で米国市民以外に米国の司法へのアクセスを保障する可能性は低い。

4. (純粋な) データストレージではなく (SaaS 型の) 付加機能を備えたクラウドサービス (SaaS アプリ) は、クラウド事業者が、少なくとも、一時的に平文でデータにアクセスできてしまう。

5. 仮に (物理的に) 欧州にデータが置かれていたとしても、米国に本拠のある企業は米国政府の要求に従うため、(物理的なサーバーの位置は) 無意味である。」

第 4 節　フランス、オランダ、ドイツ、スウェーデンの模様 ――「EU turns from American public clouds to Nextcloud private clouds」

ZDNet, 2019/09/03

https://www.zdnet.com/article/eu-turns-from-american-public-clouds-to-nextcloud-private-clouds/

「政府を米国の大手パブリック クラウドから切り離すために、フランス内務省、オランダ教育省、ドイツ連邦政府、スウェーデン連邦政府は、プライベートクラウドを導入している。」

「スウェーデン社会保険庁は、クラウドストレージ (注: SharePoint や OneDrive のようなもの) とメッセージング (注: Teams, Slack のようなもの) をプライベートクラウド化した。Google や Microsoft の製品ほど優れていないが、完全な暗号化が実現できている。各部署の判断で、部門間でのデータ共有に利用できるようにした。」

「ドイツ連邦 Peter Altmaier 経済エネルギー大臣は、米国クラウドに代わるヨーロッパのクラウドが必要であると述べた。」

「ヨーロッパでは、データ秘匿性の需要から、クラウドリソースがローカルであることが求められるようになってきたことにより、クラウドサービスの民間競争が形成されている。」

第５節　欧州委員会の様子　――「Cloud sovereignty: Three imperatives for the European public sector」

Deloitte, 2023

https://www2.deloitte.com/xe/en/insights/technology-management/cloud-sovereignty-three-imperatives-for-the-european-public-sector.html

「欧州にとって、デジタル主権保障には二重の義務がある。第 1 に、(ヨーロッパの) ローカルなクラウド市場が、経済的繁栄と技術革新の触媒として発展し続けることを保証することである。第 2 には、特に (米国を本拠地とする) ハイパースケーラーとのパートナーシップを形成する際に、世界的なテクノロジー外交の舵取りをすることである。」

「欧州全体でクラウド導入が加速するにつれ、機密情報に関する懸念が高まっている。行政機関によって処理されるデータの量と重要性は増加しているので、情報を保護および管理するための強力な対策が必要となったためである。」

「欧州委員会の Ursula von der Leyen 委員長は、欧州向けアジェンダで上記の点について言及し、『ハイパースケーラーを複製するには遅すぎるかもしれないが、一部の重要な技術分野で技術主権を達成するには遅すぎるということはない。』と述べている。」

「Azure、AWS、Google Cloud などの一部のクラウドプロバイダーは、ロシアによるウクラロナ侵略の際、ウクライナの政府サービスの継続を確保することで同国を支援した。このことは、公的機関が外国のクラウドプロバイダーに依存しすぎることの懸念を浮き彫りにしたのである。」

「行政クラウド・ネットワーク――日本以外の先進国の傾向の調査 ～ 日本以外の先進国の政府機関はどのような行政クラウド・ネットワーク戦略を策定しているのか？ EU およびヨーロッパ各国の戦略 ～」

2024 年　登 大遊

dnobori@cs.tsukuba.ac.jp

本資料に記載されているすべての内容は、独立した研究者としての意見であり、所属組織全体の見解を示すものではありません。