

クラウドセキュリティアライアンス

ビッグデータワーキンググループ

ビッグデータとプライバシーの将来 に関するコメント(日本語訳)

© 2014 Cloud Security Alliance - All Rights Reserved

All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance “Comment on Big Data and the Future of Privacy” at www.cloudsecurityalliance.org/research/big-data, subject to the following: (a) the Document may be used solely for your personal, informational, non-commercial use; (b) the Document may not be modified or altered in any way; (c) the Document may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Document as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance “Comment on Big Data and the Future of Privacy” (2014).

日本語訳の提供について

「ビッグデータとプライバシーの将来に関するコメント」は、Cloud Security Alliance Big Data Working Group よりリリースされている「Comment on Big Data and the Future of Privacy」(2014年4月)の日本語訳です。このドキュメントは、ビッグデータセキュリティに関心のあるクラウドユーザーの教育・啓発を目的として、原文をそのまま翻訳したものであり、日本独自の法令や基準に関する記述は含まれておりません。

なお、日本クラウドセキュリティアライアンスに関する情報は、以下の URL より参照可能ですので、ご覧下さい。

<http://www.cloudsecurityalliance.jp/>

このドキュメントは、以下の日本クラウドセキュリティアライアンスの有志により作成されています。

日本クラウドセキュリティアライアンス・ビッグデータユーザーワーキンググループ

リーダー: 笹原 英司 (特定非営利活動法人ヘルスケアクラウド研究会 医学博士)

阿倍 克英 (特定非営利活動法人ヘルスケアクラウド研究会)

里中 慧 (特定非営利活動法人ヘルスケアクラウド研究会)

協力

イー・ガーディアン株式会社

- (1) ビッグデータの収集、保存、分析、利用に関する公共政策の導入とは何か？ 例えば、消費者のプライバシーと政府のデータ利用を保護するために、現在の米国の政策フレームワークとプライバシーに関する提言は、ビッグデータ分析により指摘された問題を適切に示しているか？

公共政策の導入は、アクセス、所有権、プライバシー、責任、そして透明性の結実である。

「リンク可能な脅威」が個人を再識別可能であることを研究者が証明するにつれて、プライバシー保護は、ビッグデータ時代のとらえどころのない目標となった。各個人のデータには極めて私的な特徴があるので、政策フレームワークは、データを保存・転送するためのベストプラクティスに誘導すべきである。既存のプラクティスは、停止中にデータを暗号化し、そのデータにアクセスする主体の適切な権限付与や認証を保証するためのインフラストラクチャを介して転送することに注力している。ビッグデータ時代の到来と共に、分析ツールは、個人だけでなく第三者組織のために価値の高い情報を生成することを目的として、ローデータへのアクセスを要求する。実際、このようなデータは、匿名化と集約のプロセスにより固有の識別子を十分取り除いた後で共有される。このプロセスは、ビッグデータのリンク可能性に基づいて再識別される事例を多く導出してきたことから、強化される必要がある。政策フレームワークは、ビッグデータの時代におけるリンク可能性の脅威を軽減し、プライバシー保護データ開示を体系化して処理する必要がある。特にこの政策フレームワークは、リンク可能なデータ全ての暗号化を強制するに至る可能性がある。その上、政策フレームワークは、データが保存される位置情報に対する懸念を処理する必要がある。透明性を強制するだけでなく、個人は、どの当事者か、どのデータへのアクセスか、どのようにして(ロー)データが利用されるのか、そしてどのようにして保護されるのかを知る権利がある。

- (2) さらなる政府のアクション、資金調達あるいは研究によって、どのようなタイプのビッグデータ利用が、計測可能な形で、アウトカムや生産性を改善させるか？

ビッグデータ利用によるアウトカム改善の例としては、以下のようなものがある。

1. 位置データと教育データをマッチングさせた仕事のデータは、雇用結果の改善につながるが見込まれる。
2. 複数企業間でサイバー脅威のインテリジェンスを共有することによって、国家のインフラストラクチャに対する潜在的なサイバー脅威の抑制につながるであろう。サイバーセキュリティにおけるビッグデータ分析技術を開発するためには、より多くの資金調達が必要である。
3. 暗号化データ上でのビッグデータ分析により、リンク可能性の脅威を抑制する。
4. 医療における改善は、より個別化された治療・処置につながる。この結果として、費用対効果の高い医療システムがもたらされるべきである。
5. よりスマートな都市や交通のインフラストラクチャになれば、より費用対効果が高く緑の多い環境や、より混雑が少なく速い通勤につながる。

どのようなタイプのビッグデータ利用が、公共政策上最も深刻な懸念を引き起こすか？

最も深刻な懸念としては、以下のようなものがある：

1. 医療、財務、人口統計、位置データなど、異なるデータの相関関係。
2. ターゲティングおよびその他の目的のために、適切な承諾を得ることなく、消費者の行動を追跡して、それを第三者と共有すること。
3. 複数の地理的境界にまたがるクラウド上でのビッグデータ保存。
4. 透明性の欠如：誰がどのデータにアクセスし、どのデータが何のために収集されるのか。

もっと政府および／若しくは公共の配慮を受ける必要がある、特定の分野や利用のタイプはあるか？

より政府／公共の配慮を受ける必要がある特定分野の例としては、医療、教育、財務的健全性、雇用、モビリティ、情報アクセスがある。

(3) どのような技術的トレンド若しくは鍵となる技術が、ビッグデータの収集、保存、分析、利用に影響を及ぼすか？

ビッグデータの収集、保存、分析、利用に影響を及ぼす技術的トレンドの例としては、予測分析、リアルタイム分析、複雑なイベント処理、ストリームコンピューティング、ハイパフォーマンスコンピューティング、クラウドコンピューティング、ディープマシンラーニングアルゴリズム、オープンソース技術、可視化、モバイルアプリケーション利用が、がある。

ビッグデータの効果的利用を可能にすると共に、プライバシーを安全に守る、有望な技術若しくは新しいプラクティスは特にあるか？

(部分)準同型暗号化や差分プライバシーは、ビッグデータの効果的利用を可能にすると共に、プライバシーを安全に守る有望な技術の例である。技術は、プライバシーを安全に守るのに重要な役割を果たすが、それ以外に、法務および経営管理の観点もアプローチに含まれるべきである。

クラウドセキュリティアライアンス(CSA)ビッグデータワーキンググループ(BDWG)は、ビッグデータのセキュリティとプライバシーを強化するために、100のベストプラクティスを提示してきた：

<https://docs.google.com/document/d/1FqeHIA53sliNS3sd3ECy2hwyJu0UJDZT71zUs-02nX4/edit#>

上位十大ベストプラクティスは以下のとおりである：

1. あらかじめ定義されたセキュリティポリシーにより、ファイルへのアクセス権限を付与する。
2. 停止中にデータを暗号化することによって、データを保護する。

3. ポリシーベースの暗号化システム(PBES)を導入する。
4. エンドポイントで、アンチウイルス/マルウェア保護システムを利用する。
5. クラスタへの異常な接続を検知するために、ビッグデータ分析を利用する。
6. プライバシー保護分析を導入する。
7. 部分準同型暗号化スキームの利用を検討する。
8. きめの細かいアクセス制御を導入する。
9. 監査情報へのタイムリーなアクセスを提供する。
10. インフラストラクチャ認証メカニズムを提供する。

(4) ビッグデータを取り扱うための政策フレームワーク若しくは規制は、政府と民間部門の間で、どのように異なるべきか？

政府の判断能力という文脈において、ビッグデータを取り扱うための政策フレームワークや規制は、政府と民間部門の間で異なる — 例えば、法の執行や政府の税金の投資において、人口統計データを管理する政策など。

(5) 現行の国際法、規制若しくは標準の妥当性など、管轄権を超えたビッグデータ利用によって、どのような問題が挙げられるか？

どこにデータが保存され、どこでデータが処理され、どこでデータ分析の結果が配布されるかという問題は、プライバシー政策や規制に関する境界/管轄権を超えて影響を及ぼす。