要旨

１．背景

クラウドサービスが普及している。総務省の発表によれば、部分的でもクラウドのサービスを利用している企業は 2013 年末で 33.1%、2014 年末で 38.7%、2015 年末で 44.6%となっており、年々増加している。

またクラウドサービスの普及が拡大するにともない、情報漏洩のリスクも年々高まっている。

２．課題・仮説

我々は、クラウドサービスを利用することによるセキュリティリスクに対して、安全に利用するためにはどうすればよいかを知っておく必要があると考える。

クラウドサービスを利用する前に、対策を知り、実践することで、全てのクラウドリスクは対策可能であるという仮説を立て、検証を行うこととした。

３．検証

検証の項目として、技術的な範囲だけではなく、クラウドサービスのリスクを検討した結果、技術、組織、法律に分類することとした。

技術	組織	法律
1.リソースの枯渇	1.ロックイン	1.証拠提出命令と電子的証拠開示
2.不完全なデータ削除	2.ガバナンスの喪失	2.司法権の違いからくるリスク
3.クラウド内部の盗聴	3.コンプライアンスの課題	3.データ保護に関するリスク
4.従事者の不正	4.他の共同利用者の行為による信頼の喪失	4.ライセンスに関するリスク
5.クラウドと利用者間の通信データ漏えい	5.クラウドサービスの終了または障害	
6.不正な探査スキャンの実施	6.クラウドプロバイダの買収	
7.DDoS攻撃・EDoS攻撃	7.サプライチェーンにおける障害	
8.管理用インターフェイスの悪用		

技術の 1～4 については、クラウドサービス事業者に対応を求め、事前に確認する必要があり、5～8 については、クラウドサービス利用者が対応できる。

組織と法律については、クラウドサービス利用者側でできる対策はほとんどなく、クラウドサービス事業者に対して、SLA や利用規約、司法の違いを理解しておくことが必要である。

上記の結果から現時点で想定されるリスクについては、クラウドサービス事業者側での

要旨

対策（ISO27017 など）を進めること、また、利用者側で正しく選定することで、対策できると考える。しかし、今後も未知のセキュリティリスクは発生していくと考えられる。

４．今後予想されるリスク

我々は以下の 2 点に注目した。

・従量課金のクラウドユーザが今後さらに増加

・クラウドへの接続機器は多種多様・増加傾向

また事例として、米国のセキュリティインシデントでデフォルトパスワードの IoT デバイスを利用した DNS への攻撃が発生しており、今後はクラウドサービスに対しても、類似の攻撃が発生する恐れがある。

IoT が普及拡大している現時点では、ハードコード（ソース直書き）のパスワードで固定されているものや、デバイスにバックドアが存在しているものなどもあり、ユーザが簡単に変更できないものも流通しているため、攻撃者に狙われやすい状態である。

利用者は IoT デバイスを使用する前に、デバイスの選定や設定の見直しを実施する必要がある。

５．まとめ

クラウドサービスを安全に利用するために必要な要素は以下の１０点である。

【一つ】	デフォルトや類推されやすいパスワードを使用しない
【二つ】	重要データは利用者側でもバックアップを取り、極力預けない
【三つ】	ダウンロードしたアプリケーションには常に最新のパッチを適用する
【四つ】	従量課金には上限や課金状況検知の仕組みを設ける
【五つ】	サービス提供会社のデータ保護対策を確認する
【六つ】	サービス提供会社のセキュリティ対策を確認する
【七つ】	サービス提供会社の財務状況を確認する
【八つ】	突然のサービス停止に備え、類似のサービスが他にないか知っておく
【九つ】	以上をもってクラウドサービスを安全に利用するためのルールとする
【十】	みんな利用規約はちゃんと読みましょう（＾－＾）ｖ

参考資料）

・総務省：情報通信白書平成 28 年版
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/html/nc252130.html