3Z-3

SaaS利用企業におけるSaaSに起因するビジネスリスクの影響分析

今井 和人† 大木 榮二郎‡

工学院大学大学院 工学研究科 情報学専攻† 工学院大学 情報学部‡

1. はじめに

1.1. 背景

クラウドサービスは，コスト圧縮，即時性，可用性，拡張性，効率性，弾力性があるなど様々なメリットがあり，企業や個人の利用拡大など，クラウドサービスが社会の様々なところで使われるようになってきている．[1] セキュリティ対策においても専門能力を持った事業者側のスタッフに依存することで，企業が自力で実施するよりも総合的で質の高いセキュリティ対策を実現できる可能性がある．しかしながら，利用者は企業内データをクラウド事業者に預ける必要があり，情報セキュリティに対して懸念されている．[2]

1.2. 目的

セキュリティ対策が懸念されているため，クラウドサービス利用企業は自身が使うサービスについてセキュリティ対策を考慮する必要がある．そのため，実際の SaaS に起因する問題が SaaS 利用企業にどのような影響を与えるのかを調査するため，クラウドサービスにおけるリスクについてセキュリティ対策の有効範囲を示し，リスク原因の発生場所を明らかにすることを目的とする．

1.3. クラウドサービス

一般的にクラウドコンピューティングとは情報やデータなどのリソースがネットワーク上のどこにあるか意識することなく利用するモデルである．そしてクラウドサービスとはそのクラウドコンピューティングを利用して提供されるサービスのことを示す．本研究で扱うクラウドサービスとは，上記の定義をもとに企業向けに提供されているサービスを指す．また，クラウドサービスを 3 つのサービス体系の IaaS，PaaS，SaaS に分類して検討する．

A SaaS User's Focusing on the Relationship between SaaS Service Structure and User's Busines Process

† Kazuto Imai Major of Informatics, Graduate School of Engineering, Kogakuin University

‡ Eijiroh Ohki, Faculty of Informatics, Kogakuin University

2. 検証方法

セキュリティ対策の有効範囲とリスク原因の発生場所を明らかにするためにモデル企業を設定し，それもとに検証を行う．以下に設定条件の概要を示す．

・SaaS 利用企業は SaaS を利用し EC サイト運営を行うことを想定する

・EC サイトは全般的に一般財団法人日本経済社会推進協会のセキュリティ評価基 CC(ISO15408) の EC サイトへの適応研究[3]に従う

・SaaS，PaaS，IaaS は各々別の事業者が経営している

2.1. リスクアセスメント

まず，EC サイトにおける脅威事象についてどの程度リスクがあるのか把握するため，リスクアセスメントを行った．NIST Special Publication 800-30 Revision 1 リスクアセスメントの実施の手引き[4]を参考に特別な対策を行わないという仮定のもとリスクアセスメントを行った．また，脅威事象に関しては一般財団法人日本経済社会推進協会のセキュリティ評価基 CC(ISO15408) の EC サイトへの適応研究を参考にデータの漏洩，盗用，改ざん，破壊の 4 項目を設定した．その結果を表 1 に示す．

表 1 EC サイトにおけるリスクアセスメント

脅威事象	リスクレベル
データの漏洩	中間
データの盗用	高い
データの改ざん	低い
データの破壊	中間

2.2. EC サイト対策評価

クラウドサービスを用いた EC サイト経営におけるセキュリティ対策の有効範囲を保護資産ごと対策別に主観評価で測定を行った．範囲の区分は顧客，SaaS 利用企業，SaaS，PaaS，IaaS の 5 項目とした．また，評価対象は一般財団法人日本経済社会推進協会のセキュリティ評価基 CC(ISO15408) の EC サイトへの適応研究で挙げている EC サイトにおける資産と脅威及びセキュリティ対策におけるセキュリティ対策の項目のすべてとした．また，リスクの有効範囲を把握

するには，プロセスを評価，分析する必要がある．そのため，顧客と従業員の視点からプロセスを評価，分析を行うことができる LOVEM-E(Enhanced Line of Visibility Methodology)を採用した．評価結果を表 2 に示す．SaaS 利用企業だけでは必要な対策は行えない．また，対策を行ってもその他の区分までは有効にはならないことが判明した．

表 2　EC サイトセキュリティ対策有効範囲

対策	脅威事象	有効範囲
保護資産：アプリケーション情報		
パスワード管理の厳重化	改ざん 破壊 盗用	利用企業のみ
リモートログインの禁止		利用企業のみ
実装ソフトのセキュリティホール情報の速やかなフォローアップ		SaaSのみ
物理マシンへの物理的な接近管理，制限		IaaSのみ
システム開発や導入時のプログラム管理の徹底		SaaSからIaaS
ユーザとサーバ間を秘匿通信化	漏洩 盗用	SaaSからIaaS
ユーザ各自の運用注意	盗用	顧客のみ
視覚シールド		利用企業のみ
ユーザとサーバ間の認証子や内容証明の添付	改ざん	SaaSからIaaS
保護資産：セキュリティ管理情報		
セキュリティホール対策	改ざん 破壊 盗用	PaaS
バックアップデータの管理徹底		SaaS，PaaS
管理者認証の強化(物理的・論理的)	破壊 盗用	PaaS
複数管理者による相互牽制		PaaS
セッション中の送信データの暗号化	盗用	SaaSからIaaS
試行回数管理		SaaSのみ
利用者認証の強化(物理的・倫理的)		利用企業のみ
利用者責任の明確化		利用企業のみ
店舗認証の強化(物理的・論理的)		SaaS
店舗責任の明確化		利用企業のみ
鍵管理装置の導入		SaaSのみ
運用規定の確定・要員教育		PaaSからIaaS
セッション中の送信データの正当性検証	改ざん	PaaSのみ
データの暗号化	漏洩	SaaSからIaaS
保護資産：ソフトウェア情報		
マシンへの近接制限	破壊	IaaSのみ
管理者パスワード管理強化		利用企業のみ
モラル教育		利用企業のみ
運用ルール、罰則の制定周知		利用企業のみ
ネットワーク経由ログイン禁止設定		利用企業のみ
一般利用者のリブート操作禁止設定		利用企業のみ
プログラムファイルの書込/削除権限を管理者に制限する設定		SaaSからPaaS
パブリックドメインのセキュリティホール情報を傍受、定期的なパッチ当て		PaaSのみ
ウイルスチェッカで進入を検地、削除		SaaS，PaaS

3. 検証結果と結論

本調査により，表 3 の結果が得られた．リスクアセスメントの結果からも EC サイトにおいてデータの盗用のリスクが高いことがわかった．また，EC サイトのセキュリティ対策の有効範囲の調査においても特にリスクの高いデータの盗用が SaaS 利用企業の対策だけでは補いきれず，SaaS 利用企業の対策だけでは十分とは言えないことが判明した．

4. まとめ

セキュリティ対策の有効範囲とリスク原因の発生について明らかにした．クラウドサービス環境において脅威事象の対策は一箇所だけではそれほど意味がなく，対策はクラウドサービスの各場所で必要となってくる．また，クラウドサービスにおいて脅威事象発生時に特定の場所のみならず利用企業や顧客までに及ぶ可能性が高い．したがって，SaaS 利用企業が対策できない範囲や SaaS 利用企業が対策を行っても SaaS 以下で対策が有効にはならない範囲は注意が必要である．

表 3　リスク原因の発生場所

顧客	近傍での覗き 推測可能なパスワード
SaaS利用企業	顧客メモ・会話 パスワード投入試行 店舗側のメモ・会話 管理者としてログインし，ファイルを破壊
SaaS	内部不正ログインにより，DB内容読み取り 不正プログラム動作によるデータ変更 伝送データ内容読み取り ファイル制御情報の改変 伝送データの内容変更 バックアップデータの差し替え 管理者としてログインし，ファイルを破壊 ネットワークからの進入によりデータの読み取り，変更，破壊
PaaS	内部不正ログインにより，DB内容読み取り DBスキーマ情報の改変 セキュリティホールを利用したファイルの差し替え サーバの直接操作によるパスワードの変更 バックアップデータの差し替え 管理者としてログインし，ファイルを破壊 ネットワークからの進入によりデータの読み取り，変更，破壊
IaaS	物理的な不正侵入によるデータの内容変更 物理的媒体の破壊 物理的な不正侵入によるバックアップディスク内容読み取り

5. 今後の予定

リスク原因の発生場所とセキュリティ対策の有効範囲もとにクラウドサービス各場所に対してのリスクがクラウドサービス利用企業のビジネスにどのように影響するかリスクレベルとともに調査を行う．

6. 主要参考資料

[1] 独立行政法人 情報処理推進機構，“クラウドコンピューティングのセキュリティその意味と社会的重要性の考察”，2012 年 4 月，< http://www.ipa.go.jp/files/000024751.pdf > (2013/12/20 アクセス)

[2] 経済産業省，“クラウドサービス利用のための情報セキュリティマネジメントガイドライン”<http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloud_security_guideline.pdf> (2013/12/20 アクセス)

[3] 一般財団法人日本経済社会推進協会，“セキュリティ評価基 CC(ISO15408) の EC サイトへの適応研究”<http://.jipdec.or.jp/archives/ecom/results/h12seika/h12results-08.pdf > (2013/12/20 アクセス)

[4] アメリカ国立標準技術研究所，“NIST Special Publication 800-30 Revision 1 リスクアセスメントの実施の手引き”<http://www.ipa.go.jp/files/000025325.pdf> (2013/12/20 アクセス)