

新たなITリスクに立ち向かう 連載シリーズ 第5回 インターネットビジネス

インターネットビジネスの定義はさまざまであるが、企業一個人(B to C)による電子商取引について、サービス提供の初期段階と比較すると、利用者および市場規模は拡大し、ビジネスモデルも進化している。また、インフラ面でも、モバイル端末利用の拡大といった多様化が進んでいる。

本稿では、環境が変化、拡大するインターネットビジネスをとりまくリスクへの対応について解説する。

1. 環境の変化とリスク

比較的早い段階より提供されている「パソコンでチケット予約をし、代金振り込み後に郵送で受領」というサービスと、「タブレット端末で最新刊の電子書籍を電子決済で購入し、ダウンロード」等の最近のサービスを比べると、利用者の視点ではより利便性を感じる機会が増えているが、環境面の比較では、以下のように多様化が進んでいる。

	初期のサービス	現在のサービス
利用端末	パソコン	パソコン、スマートフォン、タブレット端末、双方向テレビ等
決済手段	インターネット以外で実施 (振り込み、代金引換払い等)	インターネット上での電子決済
コンテンツ	物流を通じた現物の提供	電子書籍、音楽ファイル等 デジタルコンテンツの普及
サービス 提供形態	個別サーバで提供	クラウドサービスの普及

では、これらの環境変化がもたらす影響は、リスク対策上でどのような考慮が必要になってくるだろうか。



	環境変化に伴う影響	リスク対策上の考慮事項
利用端末の 多様化	<ul style="list-style-type: none"> ウィルス形態、攻撃手法の多様化 利用者数、利用者層の増加に伴うウィルス感染機会の拡大 各種端末を想定したサイト構築の多重化が必要となり、構築側でのセキュリティ対策漏れが発生する可能性 	不正アクセスに伴う、改ざん、情報漏えい、破壊等の脅威に晒される機会や範囲が拡大するため、多様な攻撃手法への対応が必要
決済手段の 多様化	<ul style="list-style-type: none"> 決済関連データがインターネット上で扱われることで、盗みとられる可能性の増加 	機密性の高いデータの分散管理や暗号化等、厳格な管理が必要
コンテンツの 電子化	<ul style="list-style-type: none"> サービス提供後のコンテンツに対しても配慮が必要 	不正コピー、著作権等への対応が必要
サービス 提供形態 の多様化	<ul style="list-style-type: none"> クラウドサービスの利用形態に応じて、インフラ、アプリケーション、データ等の管理主体が、サービス提供者側に移る 	委託先の適切な選定および委託内容の管理、品質評価等が必要

不正アクセスに伴う、改ざん、情報漏えい、破壊等は、以前より認識されていた脅威ではあるが、環境変化に伴い、リスクが顕在化する範囲や頻度は確実に増している。

また、決済手段が電子化されることで、扱われるデータの重要性も高まっている。サービス提供側にとって、重要な情報資産を安全に管理するという本質は変わらないが、巧妙かつ高度化されたサイバー攻撃に対して、備えるべき対策は常に進化させていく必要がある¹。

コンテンツの電子化に伴い考慮する事項は、インターネットビジネスに限らず、不正な複製品対策や知的財産管理のように、必要な対策の範囲が広がっている。クラウドサービスの利用機会増加に伴う委託先管理の重要性も、従来から外部委託時に考慮すべき事項であったが、サービスの多様化、責任分界点の複雑化等により、より深い考慮が求められている。

このように環境変化に伴う対策は、従前の延長で強化や分野の拡大が必要なもの、より深い考慮が必要なもの等、これまで認識していたリスクに対して、変化や拡大した状況を的確にとらえて対応していく必要がある。

2. さらなる対応領域と範囲の多様化

不正アクセス等については、攻撃手法が常に巧妙化、高度化しており、技術的なセキュリティ対策の強化にとどまらず、利用者への迅速な注意喚起、被害発生状況の確認等も同時に行わなければならない。

<不正アクセスの攻撃例>

- 巧妙なメールでの誘導とフィッシングサイトによる ID、パスワードの奪取
- ブラウザソフトの脆弱性を利用した遠隔操作等の不正アクセス

¹本連載シリーズ 第3回「サイバーセキュリティ攻撃者に隙を見せない態勢づくり」

<http://www.kpmg.com/jp/ja/knowledge/article/risk-advisory-thoughtleadership/Documents/it-risk-cyber-security.pdf>

また、ビジネスモデルやサービス内容に関連して、企業の責任にかかわるような事象等も発生しており、法務、品質、企業倫理等さまざまな観点からの対応が必要となっている。

<企業責任にかかわる事象例>

- オークションサイトでの違法性が疑われる商品への対応
- マッチングサービスにおける引き合わせ先のサービス提供能力と品質の確保
- 不当な商品表示や金額表示への対応

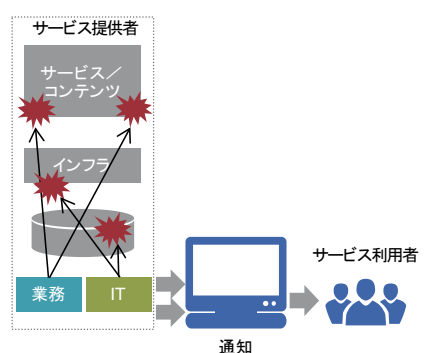
このように、日々発生するさまざまな状況に対して、影響を正確に見極め、適切な部署が漏れなく対応していく必要があるが、外部環境やビジネスモデルが変化していく状況では、セキュリティ等の技術的側面や、ビジネスモデル等の業務的な側面に起因する問題に個別に対応するだけでなく、これらが絶えず複合的に発生することを想定した備えが必要となる。

3. ビジネス全体を俯瞰したリスク管理

インターネットビジネスでは、通常のビジネスの店舗・売り場が、利用者と提供者をつなぐインターネット空間であり、売り物は、インターネット上で展開するサービスやコンテンツにあたるため、売り場と売り物が一体化しているといえる。

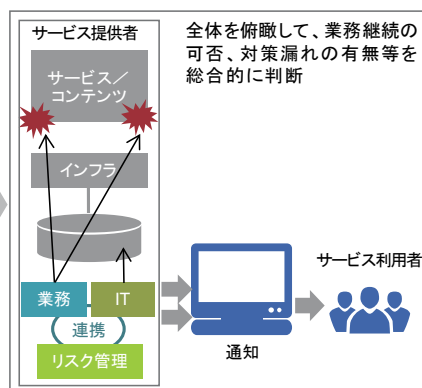
そのような状態で、技術と業務に関する複合的な問題への対応が遅れた場合、サービス提供の中断が余儀なくされ、またビジネスの継続に直接影響を与え、企業の存続にもかかわる可能性がある。そのため、技術的なセキュリティ対策や、ビジネスモデルに起因する問題等、多岐にわたる領域全体を俯瞰して、複合的な問題の対応が部分的になっていないかを確認する機能が必要である。

<従来の対応>



問題が発生する都度、担当部署が対処して、ポータルサイト、メール等を通じて利用者に通知

<全体を俯瞰した対応>



全体を俯瞰して、業務継続の可否、対策漏れの有無等を総合的に判断

リスク全般を俯瞰して、担当部署と連携

例えば、ブラウザソフトの脆弱性が確認された場合、対応としてまずは技術的なセキュリティ対策の検討に入ると考えられる。ただし、それと同時にブラウザソフトはサービス提供空間そのものであることを踏まえ、その影響を考慮した業務継続についての判断が必要となる。また、サービス利用者への案内、サービス提供に不具合が生じた場合の対応方法等、単にブラウザソフトに関する技術的な問題だけではとどまらない。

多様化する問題に対して、専門性を備えた組織がそれぞれの能力を高める一方で、リスク管理全体の視点を持った組織が、IT技術、業務継続、法務、広報等複合的な判断を行い、組織間で対応漏れのないよう、必要に応じて連携した対応が必要である。このように、総合的な対応力の向上が、常に進化し続けるインターネットビジネスのリスクに立ち向かっていく術だといえる。

KPMGビジネスアドバイザリー株式会社
ディレクター 関 克彦

KPMGビジネスアドバイザリー株式会社

東京本社
〒100-0004
東京都千代田区大手町1丁目9番7号
大手町フィナンシャルシティ サウスタワー
TEL : 03-3548-5305
FAX : 03-3548-5306

名古屋事務所
〒451-6031
名古屋市中区牛島町6番1号 名古屋ルーセントタワー
TEL : 052-571-5485

kpmg.com/jp/ba

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供できるよう努めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

©2014 KPMG Business Advisory Co., Ltd., a company established under the Japan Company Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved..

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.