企業の業務に活用されるコンシューマーIT

小林賢治

スマートフォン（多機能な携帯電話端末）や個人向けのクラウドコンピューティングサービスなどを企業の業務に導入し、パフォーマンスの向上やITコスト削減を図ろうという動きが進展している。その一方で、セキュリティへの懸念から、導入に消極的ないしは様子を見たいという企業も多い。個人利用を前提とした機器やサービスを企業の業務に導入する際には、管理可能な環境での段階的導入が有効である。また、コンテンツの機密度によって伝送を制限する機能や、モバイル端末のリモート管理機能など、セキュリティを強化する仕組みも検討すべきである。

加速するコンシューマーITの業務利用

Google Apps（グーグルアップス：オンライン・オフィスアプリケーションソフト）、Evernote（エバーノート：オンライン・メモサービス）、Dropbox（ドロップボックス：オンライン・ストレージサービス）といった個人向けクラウドコンピューティング（以下、クラウド）サービスが人気を集めている。

これらのサービスを利用すると、インターネットに接続したPC（パソコン）などから自分の電子メールやファイルにアクセスでき、他のユーザーと文書や写真などを手軽に共有できることから、利用者数が急激に伸びている。クラウドサービスはスマートフォンやタブレット端末（平板型端末）にも対応しているため、外出先で利用できる便利さもある。

本稿では、個人の私的利用を主な目的とする機器やサービスを「コンシューマーIT」と呼ぶことにする。上述のサービスも、もともと個人向けサービスとしてスタートした。

コンシューマーITは、機器の機能やサービス環境などが充実してきたことにより、業務シーンでも十分に活用できるものになっている。たとえば、業務で作成したオフィス文書を外出前にクラウドサービスにアップロードしておき、その文書を外出先からスマートフォンで参照するといった使い方である。Microsoft Office（マイクロソフト・オフィス）など市販のオフィスアプリケーションソフトをインストールしていないPCでも、Google Appsを利用すればオフィス文書にアクセスして編集することができるため、オフィスアプリケーションソフトの代替として使うことも可能である。

上述のサービスは、基本は無料で保存容量に限りがあるが、使用可能容量を有料で増やせるエンタープライズ版が用意されている。表1にコンシューマーITの全体像をまとめる。

コンシューマーITの業務利用のニーズは高まってきており、実際に業務に導入されるケースも増えている。スマートフォンのような多機能で利便性の高いモバイル端末が普及したことに加え、クラウドサービスが浸透してきたことがその背景にあると考えられる。

一方で、コンシューマーITの業務利用は情報漏えいのリスクを増大させる。アクセス制限があるにせよ、上述のサービスはいずれも情報共有を容易にすることを意図しており、ファイル公開がワンクリックで可能になっている。機密文書をうっかり公開してしまう危険性は否定できない。そのため

情報保護の観点から、コンシューマーITの業務利用を問題視する情報システム部門は多い。

一方で、うまく使いこなすことができれば業務利用効果が大きいと考える情報システム部門もある。少なくとも、コンシューマーITは情報システム部門の管轄外と切り捨てるべきではない。業務利用での利便性の高さや導入効果を考えれば、コンシューマーITへの何らかの対応は急務であるといえよう。

新たな「シャドーIT」問題の発生

企業のコンシューマーITへの対応はまちまちである。クラウドサービスやスマートフォンを正式に導入している企業もあれば、明示的に利用を禁止・制限している企業もある。問題となるのは、ルールを設けずに情報システム部門の管轄外として放置し、黙認をしているケースである。このような正式に認められていないITは「シャドーIT」（見えないIT）と呼ばれ、その取り扱いは従来から課題とされてきた。コンシューマーITの業務利用は、情報システム部門にとって新たなシャドーIT問題といえる。

ただし、コンシューマーITは、これまでユーザー部門が独自に導入を進めてきたシャドーITとは異なる特徴を持つ。基本機能は無料で、ユーザーが普段から使い慣れているツールであるため、導入のハードルがきわめて低い。そのため、ユーザーの一部の有志が率先して導入するケースも考えられる。無料で利用できることから社内の決裁を通さないことが多く、情報システム部門が管理しきれない面がある。禁止してしまうと、今度は利便性を感じているユーザーからの反発を買う。このように、コンシューマーITは従来のシャドーITとは異なる問題と捉えるべきである。

コンサルティングの現場でもこうした相談が増えている。ユーザーがクラウドサービスや個人所有のPC・スマートフォンを無断で業務に利用してしまい、情報システム部門としてどうルールを決めたらよいのか、どういう仕組みで統制すべきかという相談である。

コンシューマーITのメリットとデメリット

コンシューマーITの利用形態は、「企業外のクラウドサービス

表1　コンシューマーITの全体像

分類	主なサービス・製品	業務シーンでの用途
クラウド型ストレージサービス	Dropbox、Evernote、Giga（ギガ）CC	外出先からのファイル参照、社内・チームでのファイル共有、社外関係者へのファイル転送
クラウド型アプリケーションソフトサービス	Google Apps、Microsoft Office 365、Zoho（ゾーホー）	外出先からの電子メール利用・スケジュール共有、モバイル環境、ドキュメント作成
SNS（ソーシャル・ネットワーキング・サービス）	Facebook（フェイスブック）、Salesforce Chatter（セールスフォース･チャッター）、youRoom（ユールーム）	プロジェクトチームでの情報共有、同報メールの代替としての利用、ノウハウの共有
モバイル端末	ノートPC、スマートフォン、タブレット端末	外出先からのメール閲覧、外出先からのファイル共有、営業担当者の商品説明
BYOD（個人所有デバイスの業務利用）	PC、スマートフォン、タブレット端末	自宅勤務の端末としての利用、パンデミック・災害時の非常用端末、パートナー社員の業務端末

表2　コンシューマーITのメリットとデメリット

メリットと効果	デメリットとリスク
クラウドサービスはインストールの必要がなく、簡単にすぐに使い始めることができる。基本機能は無料で利用できる	利用に当たってコンプライアンス（法令遵守）上問題がないかどうかは、ユーザー個人の判断に委ねられる
エンタープライズ版の有料機能は、ユーザー当たりの年額利用料で使用できる	ユーザーが増えるとコスト効果が出ない
PCやスマートフォン、タブレット端末など、デバイスを問わず情報にアクセスできる	ユーザーが外部への情報漏えいリスクに無頓着になりやすい。業務用PCだけでなく個人所有のデバイスにまで管理範囲を広げる必要がある
数GB（ギガバイト）～数十GBクラスの大容量に対応している	大量の機密情報が一度に漏えいするリスクがある
デジタルネイティブ世代にとっては使い慣れたツールを業務利用でき、生産性が高まる	タグ方式の採用など、従来とは異なる使い勝手の面もあり、全社展開が困難である

をネットワークを介してPCやスマートフォンなどから利用する」というものである。ユーザーはいつでもどこでも必要な情報にアクセスできる点に利便性を感じている。一方で、企業情報が社外に蓄積され、セキュリティが十分でないスマートフォンや個人所有のPCからもアクセスが可能になる。そこで情報漏えいや企業情報保護への対策が重要な課題になる。

表２にコンシューマーITのメリットと効果、デメリットとリスクをまとめる。情報漏えいなどのリスクを考えてコンシューマーITの導入に消極的な企業は多い。しかし、今回の東日本大震災を契機に考え方を変える企業も多くなっている。災害に強いというクラウドサービスの利点を重視して、業務継続の観点からこれを積極的に利用しようというのである。

コンシューマーIT導入のポイント

このように、現在のところコンシューマーITの取り扱い方は企業では一定していない。いずれにせよ、メリットとデメリットのバランスを見極めながら、自社の業務内容に合った選択をすることが現実的な対応であろう。

では、実際にどのような取り組みが考えられるのだろうか。利便性がいかに高くても、情報保護は企業にとって最優先事項である。そのためリスクのあるコンシューマーITの利用を一律に禁止することも選択肢の一つであり、現時点ではそのように対応している企業が多い。

しかし、実態としてはどの企業でも、情報システム部門が把握していないコンシューマーITの利用は進んでいると見るべきである。

たとえば、クラウドサービスを利用できないようにネットワークに制限をかけていた企業から、個人所有のスマートフォンを使ってクラウドサービスを利用し、スケジュールや情報をチームで共有していた件で相談を受けたことがある。本人たちは気づいていなかったが、スケジュールには顧客の氏名や連絡先といった個人情報が書き込まれており、これが誤操作によって一般に公開される状態になっていた。

コンシューマーITの利用が意図せずに進んでしまっているという現実は、コンシューマーITが情報システム部門が提供している環境以上に便利で効果的だということでもある。したがって、情報保護だけを優先して業務利用を一律に禁止するよりも、利便性とセキュリティのバランスを考慮した効果的、かつ安全な仕組みづくりに取り組むべきであろう。仮に利用を禁止しても、導入のハードルがきわめて低いコンシューマー

ITの「勝手利用」は、意図するにせよしないにせよ、いずれ進行してしまうのは間違いない。情報システム部門が管理可能な環境を用意し、そこにユーザーを「囲い込む」ほうが安全であり効果的である。

具体的には、以下のように4つの段階で導入を進めることが望ましい。

①コンシューマーIT利用の実態把握

第1に実態を把握すべきである。その際、コンシューマーITの潜在ニーズや効果的な使い方を把握すると同時に、情報保護の観点でリスクを把握する必要がある。導入に否定的な考えを持っている、または禁止を前提に検討している企業においても、実態把握はすべきである。

②エンタープライズ版サービスの選定

次に、利用実態やニーズに基づいて具体的な導入ポリシーを定め、サービスやツールを選定する。その際に重要になるのが、セキュリティポリシーに合致するサービスやツールの見極めである。

クラウドサービスの場合、管理者機能の有無や、情報保護・プライバシー保護に関する第三者機関の認定の有無がポイントとなる。企業で必要となる管理者機能やセキュリティ機能を備えたサービスは、有料のエンタープライズ版のなかから選定することになろう。

③段階的な導入拡大

利用開始に当たっては、一度に全体に対して導入するのではなく、ITリテラシー（活用能力）やセキュリティ意識が比較的高い部門から段階的に導入していく。一部で試験的に運用しながら、利用形態やITリテラシーに課題がないかを確認し、セキュリティ強化のためのインフラがどの程度必要であるかについても見極める。

④導入拡大に合わせたセキュリティ強化

全社展開時に重要となるのはITリテラシー教育である。これはセキュリティとともに操作性に関しても必要である。一般的にクラウドサービスには「フォルダ」という概念はなく、「タグ」と呼ばれるキーワードでファイルを整理するため、新しい操作性についての教育・サポートが必要になる。

さらに、導入の拡大に当たってはセキュリティをより強化することも必要となる。たとえば、コンテンツ（情報の中身）の機密度によって伝送を制限する機能や、モバイル端末の紛失時には工場出荷時の状態に戻して重要なデータの流出を防ぐリモートワイプ機能など、セキュリティを強化する仕組みも検討すべきである。

『ITソリューションフロンティア』2011年11月号より転載

小林賢治（こばやしけんじ）
ITアーキテクチャーコンサルティング部グループマネージャー