BP usiness artner Navigator

大塚商会の販売最前線からお届けするセールスノウハウマガジン

vol.85 2016

年頭特集

東日本大震災から5年

BCP対策の総点検 「備える」を再提案!

巻頭インタビュー

株式会社感性リサーチ 代表取締役

黒川 伊保子氏

失敗はビジネスセンスを磨くチャンス
「ラッキー」と思って、乗り越えていくことです!

第2特集

個人情報や機密情報が危ない
お客様の情報を守るのは、パートナー様の使命です!

CAD情報

Autodesk
全世界のパートナー様向けカンファレンス
「One Team Conference 2016」を盛大に開催! ほか

Navi Value

つながると見える! ひろがるビジネス。
実践ソリューションフェア2016開催!!

メーカーズボイス

株式会社富士通パーソナルズ
株式会社日本HP

Presented by Otsuka Corporation

BP usiness artner Navigator
大塚商会の販売最前線からお届けするセールスノウハウマガジン
vol.85 2016

CONTENTS

Series にっぽんの元気人

BP Top Interview

各界の最前線で活躍する
オピニオンリーダーに
IT業界復活のヒントを聞く

第34回

株式会社 感性リサーチ 代表取締役

黒川 伊保子氏

失敗はビジネスセンスを磨くチャンス「ラッキー」と思って、乗り越えていくことです！

女性にとって、男性中心のビジネス社会は完全アウェー。それだけに、似たような失敗をしても男性社員より女性社員のほうが目立ちやすく、何となく不公平にも思えてくる。しかし、「目立つからこそ、女性のほうがビジネスセンスを磨くチャンスに恵まれている」と語るのは、女性脳と男性脳の違いに関する本などを数多く執筆する感性アナリストの黒川伊保子さん。ただし、そのチャンスを活かして働く女性がもっと輝くためには、意識の変革が求められるという。

自分にスポットライトを当てると失敗するのが怖くなる

BP：安倍内閣が「女性の活躍促進」を成長戦略のひとつとして打ち出して以来、働く女性に対する世の中の期待も高まっているように感じます。しかし、黒川さんは逆にその風潮が、働く女性たちを疲弊させていると感じておられるようですね。

黒川伊保子氏（以下、黒川氏）：「女性の活躍推進」と言われて期待され、本人も素敵なキャリアウーマンになりたいと思っている女性たちがなぜ疲弊していくのかと言うと、「美しくて、若々しくて、センスがよくて、頭もよくて、英語もできる」といった世の中の理想像を目標にしているからですね。外から見た理想像ではなく、もっと自分らしさを追求してみてはどうでしょうか。

疲弊しないための方法は2つ。「自分を基準にすること」と「自分にスポットライトを当てないこと」です。

自分にスポットライトを当てる人は、誰かに叱られると「こんなに努力しているのに、認めてもらえない」と自分を責めてしまうので、とても苦しくなってしまいます。でも、自分ではなく、上司やお客さまといった相手にスポットライトを当てられる人は、叱られたり、クレームを受けたりしても、「えっ、自分は何を読み間違えたのだろう」と客観的になれるのです。

自分にスポットライトを当てがちな女性が増えているのは、時代のせいもあると思います。

わたしは感性トレンドと言って、世の中の人々の気分の変遷を研究しているのですが、1980年代ごろまでの若い人たちは、どちらかと言うと興味が外に向いていました。

ところが1990年代以降の“空気を読む”若者世代は、外よりも自分に興味があるのです。他人にどう思われているのかがすごく気になる。他人から見て素敵な人になりたいし、やさしい人になりたい。あくまでも自分が中心ですね。そういう人は、他人に何か言われたときにものすごく打たれ弱い。だから自分にスポットライトを当てないことがとても大切だと思います。

もう1つの「自分を基準にすること」は、自分にスポットライトを当てないことの裏返しだと言えます。

周りにどう思われるかを恐れるのではなく「自分はこう生きていく」と1人称で物事を考えること。上司もお客さまも、周りはつねに自分を楽しませてくれる観客だと思って、気楽に向き合うことが大事です。

もともと女性は、自分の気持ちを見つめやすい傾向があります。女性の脳は、感情をつかさどる右脳と理性をつかさどる左脳の“橋渡し役”である脳梁と呼ばれる部分が男性の脳よりも太く、感じる領域の出来事が男性の数百倍も顕在意識に伝わるので、つねに自分の気持ちを強く感じながら生きています。

なので、いい意味でも悪い意味でも、ビジネスのシーンの中で自分にスポットライトを当てやすい。だからどうしても、自分はちゃんとできているかどうかとか、人にとやかく言われるのが怖いという感情が男性よりも強く働いてしまいます。女性が社会で活躍するためには、まずそういう感情を消すこと。他人にとやかく言われるのを恐れないでと言いたいですね。

35歳までの失敗が脳のセンスを育てる

BP：小言やクレームを受けても、自分を責めすぎないことが大切ですか?

黒川氏：そもそもビジネスなんて、とやかく言われないと始まらないじゃないですか。ビジネスセンスは、小言やクレームを受けながら少しずつ身に着いていくものなのですから。

じつは、失敗こそが脳のセンスを育ててくれるので、恐れる必要はなく、むしろ積極的に受け入れたほうがいいのです。これは何歳になってもそうですが、とくに35歳までの失敗は脳にとって大変重要です。

BP：なぜ、失敗は脳のセンスを育ててくれるのでしょう。また、なぜ35歳までの失敗が大事なのでしょうか?

黒川氏：人わたしたちの脳には1000億を超えるニューロン（脳細胞）が入っていて、それが縦横無尽にネットワークされるので、その組み合わせは天文学的な数字になります。

仮にこのネットワークに等しく電気信号が流れてしまったら、人間は何の判断もできなくなってしまいます。目の前を通り過ぎる黒い影が猫だと認識するためには、猫だとわかる回路だけに電気信号が流れる必要があります。でもネズ

ミだとわかる回路や、象だとわかる回路にも信号が流れてしまうと、何が通り過ぎたのかがわからなくなって、立ちすくむしかなくなるわけです。

ところが、やがて成長するにしたがって、日常生活で象と出会うことはないという知識を積んでいくと、余分な回路が消えて、目の前を通り過ぎたのは猫だということがわかってくるようになります。わたしたちはそうした日々の経験をもとに脳の中を整理し、ブラッシュアップしています。

もちろん、失敗も大切なブラッシュアップの要素です。失敗して痛い思いをすると、人間の脳は失敗のために使われた回路のしきい値（反応に必要な刺激量）を上げて、そこに信号が行きにくくします。また逆に、成功してうれしい思いをすると、しきい値を下げて信号を受けやすくします。

それによってわたしたちの脳は、成功しやすく失敗しにくい脳に変わっていくわけです。

BP：失敗を重ねることが、知らず知らずのうちに脳に磨きを掛けるのですね。

黒川氏：ヒトは、生まれてきたその瞬間、人生最多の脳細胞を持っていると言われています。どのような環境でも生きていけるように、満載の感度で生まれてくるわけですね。

しかし、それでは、先ほど言ったように、すべての事象に反応してしまって、とっさの判断がかなわない。このため、体験による試行錯誤を繰り返し、要らない脳細胞を捨て、回路の優先順位をつけていくわけです。

脳を装置として見立てると、28歳までの脳はいちじるしい入力装置で、脳神経回路を増やす方向。他者から見て失敗と見える事象であれ、成功と見える事象であれ、そこから等しくさまざまなことを得ていきます。

このため、28歳までは、失敗を失敗とも思わないタフさがあるのです。まさに人材教育の好機ですね。

29歳からの28年間は、成功と失敗を明確に分けて、脳の優先順位をつけていく「脳の洗練期」。特に最初の7年は、失敗適齢期です。最初に要らない回路を消してしまった方が、成功回路の上書きがしやすいから、脳は先に失敗したがっているのです。というわけで、35歳までは失敗しやすく、それを脳神経回路に活かしやすい、ということになりますね。

十分に要らない回路に電気信号が行かなくなれば、当然、物忘れが始まります。物忘れは老化じゃなくて、進化。物忘れするくらいの脳じゃないと、ビジネス・センスは発揮できません。

入力期を終えた30歳の頃、世界のすべてを知ったような気になるのがヒトの脳の定番です。仕事にも慣れ、「あー、世の中こんなもん」とちょっとなめた気分にもなる。なのに、失敗適齢期を迎えた脳は、懲りたあげく失敗案件を選び取ってしまう。

そういう意味では、30代は過酷な年代ですね。周りの期待もどんどん高まるし。でも、失敗に疲弊しやすいこの年齢だからこそ、あえて失敗を恐れない人だけが抜きんでてくる。特別なひとりになりたければ、失敗を恐れないことです。

35歳を過ぎても、もちろん間に合います。年齢にかかわらず、人生は失敗の数が多いほど勝ち。わたしは50代ですが、いまでも失敗は大好物（笑）。

それによって脳に磨きがかかり、使い物になる知識や経験を手に入れられるのは、とてもありがたいことだと思っています。

いままでにやったことがないこと、失敗しそうなことに出会ったら、逆にものすごいチャンスをもらったと思ったほうがいいですね。

失敗を糧にするために守りたい“3カ条”とは？

BP：失敗を恐れないようになるための効果的な方法があれば教えてください。

株式会社 感性リサーチ　代表取締役
黒 川 伊 保 子 氏
Ihoko Kuokawa

◎ Profile

1959 年、長野県生まれ、栃木県育ち。1983 年、奈良女子大学理学部物理学科を卒業後、（株）富士通ソーシアルサイエンスラボラトリにて、14 年に亘り人工知能（AI）の研究開発に従事する。その後、コンサルタント会社勤務や民間の研究所を経て、2003 年、（株）感性リサーチを設立し代表取締役に就任。2004、脳機能論と AI の集大成による語感分析法『サブリミナル・インプレッション導出法』を発表。サービス開始と同時に化粧品、自動車、食品業界などの新商品名分析を相次いで受注し、感性分析の第一人者となる。2006 年、大前研一アタッカーズビジネススクールで、感性マーケティング講座を開講。明治大学スマートキャリア講座講師、日経 MJ セミナー講師。日本テレビ「世界一受けたい授業」やフジテレビ「ホンマでっか!?TV」などに出演。雑誌の脳トレ、恋愛特集のコメンテイターとしても幅広く活躍している。

黒川氏：そもそもビジネス社会は男性脳型ですね。

男性脳型というのは、大量の商品を、均一の質で、迅速に、しかもコストパフォーマンスよく市場に流通させていくという行為に向いています。一方、女性は1つひとつのことを丁寧にやっていく脳を持っているので、男性脳型に合わせていくのは簡単なことではありません。でも商品は1つひとつ丁寧に扱うことも大事じゃないですか。だからビジネス社会には、女性が活躍できる場もありますよね。

だけど、どうしてもビジネス社会における主流は男性。ということは、わたしたち女性はアウェーにいるわけです。そのことは覚悟したほうがいいと思います。わかってもらって、ちやほやされることなんてはなっから考えないこと。そう割り切ると意外と周りの男性がやさしく接してくれるものです。

逆に、男性にもアウェーがありますからね。それは家庭です。半径3メール以内のものに気が付かないのが男性脳なので、女性の目からは、どうしてもリビングの中で使い物にならない存在に見えています。

お互いにホームとアウェーが異なるだけで、イーブンと言えばイーブンなのですから、アウェーである会社での身の振り方、相手との接し方については覚悟を決めちゃったほうがいい。

そして、会社にいるときは、つねに自分がこの世のエンターテインメントを楽しんでいる観客だと思ってください。いやな上司や手強い顧客を見て遊んでいる観客。そのぐらい感覚で相手に接すれば、失敗を受け入れることができるはずですし、こちらが観察者の立場になるので、接していても緊張することもないと思います。

もうひとつ、これは失敗の経験を脳に最大限書き込むためにぜひ心掛けていただきたいのですが、①失敗を他人のせいにしない、②過去の失敗をくよくよ思い返さない、③まだ起こってもいない失敗に怖気づかない、という“失敗の3カ条”を守ってみてください。

失敗を他人のせいにすると、脳が自分の失敗だと認識できないので、脳神経への書き込みが行われません。せっかく痛い思いをしたのに、それがムダになってしまって、センスの向上に結び付かない。

また、過去の失敗をくよくよ思い返すと、せっかく捨てた回路を通電させてしまうので、成功回路が見つけにくくなってしまいます。

3つ目のまだ起こってもいない失敗に怖気づかないことも大切。これは、失敗を責める上司の方に気を付けていただきたいですね。「以前にも似たようなことをやって失敗しただろう」などとあげつらわず、むしろ「失敗を恐れることなく、どんどんチャレンジしてみて」と背中を押してあげることが大切だと思います。

BP：最後に頑張っている働く女性たちに応援メッセージをお願いします。

黒川氏：とにかく失敗したら「ラッキー!」と思ってどんどん経験し、乗り越えていくことです。

女性はアウェーにいるので、どうしても男性より失敗が目立ちやすくなってしまうけど、見方を変えればビジネスに必要な「勘」や「つかみ」「センス」を手に入れるチャンスに恵まれているということじゃないですか。そういうふうに発想を転換して、凛々しく頑張っていただきたいなと思います。BP

巻頭特集

東日本大震災から5年

BCP対策の総点検「備える」を再提案!

いざというときの「備え」は、
平時の準備が肝要ではあるものの、
日常の業務で多忙である
エンドユーザー様は、なかなか対策を
推し進めることが難しい。
だからこそ、パートナー様がエンドユーザー様を
サポートすることで、良好な関係を構築できると
ともに売上アップにつなげることもできるのだ。
今回の特集では、UPSやSaaS、
バックアップシステムなど、5年前に注目を浴びた
商品やサービスを点検し再提案する。

☑ 基礎編　確実なデータ保護のために

最重要の経営資源は「情報」 BCP提案はその保護を第一に行うべき

事業の中断が招く 顧客流出と企業評価の低下

今年3月、日本を揺るがした東日本大震災から5年が過ぎた。大震災を振り返る行事が各地で行われ、大災害の脅威をあらためて実感した方も多いだろう。それと共に忘れてはならないのがBCP（事業継続計画）対策の重要性である。

企業にとって業務中断は顧客の流出、マーケットシェアや企業評価の低下につながる。一方で、東日本大震災では、BCP対策への取り組みによって評価を向上させることに成功した企業も実は少なくない。データ保護をはじめ、BCP対策に関連する予算はえてして後手に回りがちだ。だが、これからも南海トラフ地震をはじめとする大地震が予測され、地域によっては水害、土砂災害などの発生が想定される中、BCP対策には「万が一の保証」という以上の意味がある。大震災から5年の節目を機に、あらためてエンドユーザー様にその意義を伝えていきたい。

BCPで大切になる ボトルネックの洗い出し

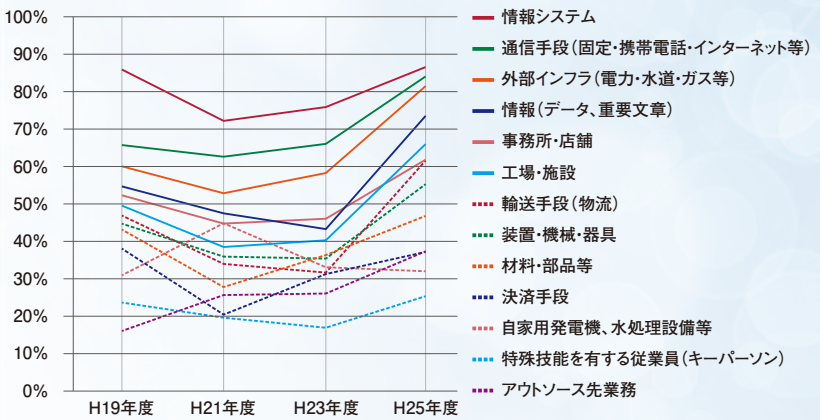
具体的な提案を検討する前に、まずはBCP対策の基本的な考え方をおさらいしておこう。BCP対策とは、事業に著しいダメージを与える重大被害を前提として、事業継続を図るための取り組みである。その際に重要になるのは、①継続すべき重要業務の絞り込み、②重要業務の継続に不可欠な要素（ボトルネック）の洗い出し、の2点。大災害後に活用できるリソースには限りがあるため、優先的に再開、復旧すべき業務の絞り込みが重要になる。その上で、事業を継続・復旧させるために欠かせない資源の確保を図ることが、その基本的な考え方になる。

では、事業を継続する上でのボトルネックとは何か。内閣府が東日本大震災後の2013年に行った調査によると、多くの企業が「情報システム」「通信手段（固定電話、携帯電話、インターネット）」「情報（データ、重要文書）」を挙げている。

これは極論になるが、「情報」さえ守ることができれば、事業の継続・復旧は比較的容易だ。事実、東日本大震災でも、取引記録や設計図、品質管理資料といった「バイタルレコード」の保護に成功した企業は、たとえ社屋が倒壊しても、代替施設を確保することですぐに業務を再開できた。エンドユーザー様への提案は、こうした背景を押さえた上で進める必要がある。

蛇足だが、非常用保存水の賞味期限は5年ということが多い。東京都が帰宅困難者対策として、企業に3日分の水・食料の備蓄を義務付けたことなどもあり、エンドユーザー様の多くは現在、社内に非常用の水や食料を備蓄している。こうした備蓄品の入れ替えが防災計画、BCP対策の見直しにつながることも十分に考えられる。エンドユーザー様のBCP対策の強化という観点からも、5年という節目の年を確実にビジネスへとつなげていきたい。

□重要な経営資源の推移（大企業）



※平成25 年度　企業の事業継続及び防災の取組に関する実態調査（内閣府）

□施設内待機のための備蓄について

3日分の備蓄量の目安

①水については、1人当たり1日3リットル、計9リットル
②主食については、1人当たり1日3食、計9食
③毛布については、1人当たり1枚
④その他の品目については、物資ごとに必要量を算定

備蓄品目の例示

①水：ペットボトル入り飲料水
②主食：アルファ化米、クラッカー、乾パン、カップ麺
※水や食料の選択に当たっては、賞味期限に留意する必要がある。
③その他の物資（特に必要性が高いもの）
毛布やそれに類する保温シート、簡易トイレ、衛生用品（トイレットペーパ等）、敷物（ビニールシート等）、携帯ラジオ、懐中電灯、乾電池、救急医療薬品類

※東京都帰宅困難者対策ハンドブック

Point.1 電源障害から機器・データを守る

UPSはシステム・データ保護の第一歩 BCP提案はバッテリー寿命の確認から

IT機器とデータを保護するうえでUPSは不可欠な装置だ。東日本大震災後にUPSへの注目が一気に高まったことは記憶に新しい。あれから5年が過ぎた今、UPSは再び忘却のかなたにある。それに伴うバッテリー交換需要の掘り起こしがBCP対策の提案の第一歩になる。

シュナイダーエレクトリック株式会社
戦略・事業開発本部 ビジネスデベロップメント マネージャー
神谷 誠氏

保守不良のUPS機器こそビジネスのチャンス!

BCP提案を考えるうえで、5年という数字には節目という以上の意味がある。BCPの主力商材の一つであるUPS(Uninterruptible Power Supply:無停電電源装置)のバッテリー寿命が長くても4～5年が一般的なことがその理由だ。

輪番停電に代表される東日本大震災後の電力供給の不安定化に伴い、電源障害から機器やデータを守るUPSに大きな注目が集まったことは記憶に新しい。APCブランドのUPS機器を手掛けるシュナイダーエレクトリック 戦略・事業開発本部 ビジネスデベロップメントマネージャーの神谷 誠氏は言う。

「縁の下の力持ちであるUPSは、普段あまり注目されることはありません。そのため大震災後に慌てて点検をしてみると、既にバッテリー交換ランプが点灯していたというケースが少なくありませんでした。またネットワーク機器の保護に目が向けられるようになったことも大震災後の変化の一つ。新たにネットワーク機器の保護を目的にUPSを導入するエンドユーザー様も多数に及びました」

5年後の今、そのときに交換されたバッテリーや新たに導入された機器のバッテリーは交換時期を迎えている。だが、電力需給の逼迫(ひっぱく)が一段落した今、専任のシステム管理者がいない中小企業などでは、「喉元過ぎれば」の例えどおり、UPS管理が大震災以前の状態に戻っていることも多いはずだ。BCP対策の提案の第一歩としてまず注目したいのが、こうした保守不良のUPSである。

日本の場合、長時間停電の発生はまれだ。だが、0.06～2秒程度の瞬時電圧低下(瞬停)は、比較的頻繁に発生しているという。その原因の多くは送電

□UPS選定の進め方

1 保護対象を決める

停止するとビジネスへの影響が大きい機器を優先的に選ぶことがポイント。また機器単体ではなく、システム全体を考慮し、検討することも大切です。接続機器数でUPS側のコンセント数が決まるため、機器数は必ず確認します。

2 消費電力と保護時間を確認する

保護対象機器のW値を調べる。W値とは、機器が実際に使用する電力(有効電力)です。通常は説明書・仕様書に記載されています。次に、シャットダウンに必要な時間を確認。一般的には10分が目安。

3 保護対象の入力電圧を調べる

国内の電気製品は大きく、電圧100Vと200Vに分けられます。対象機器のコンセントの形状を見れば入力電圧が100Vなのか200Vなのか確認できます。

上記3項目に基づき、最適なUPSを選ぶ

メーカーWebサイトなどで、出力コンセント数、容量、電圧が目的に見合う製品を探します。
容量を大きくしたり、バッテリーを増設したりすることで、より長時間の保護が可能になります。

線への落雷で、温暖化による異常気象などもあり、瞬停はむしろ増加する傾向にある。仮にUPSのバッテリーが劣化していた場合、瞬停時に機器やデータを守ることができないことも十分考えられる。エンドユーザー様のUPSの状況を確認し、必要に応じてバッテリー交換を提案することは、今すぐにでも始めたいところだ。

「バッテリーの状態は利用環境によって異なります。当社のUPS製品にはバッテリー状態のセルフチェック機能が備わっていますが、そこで表示されるランタイムがカタログ値の半分以下になっていたら交換時期と考えてください」と神谷氏は言う。

旧型機種の場合 リプレースの方がお得に

提案にあたっては、UPSの性能向上も考慮したいポイント。2012年に発売されたAPCの主力製品である「Smart-UPS」の場合、従来品に比べ消費電力が1/2になっているが、これは電気代を抑えるだけでなく、内部発熱の抑制によるバッテリー寿命の大幅な延長にもつながっている。

「2011年頃に購入されたUPSは装置交換時期をむかえることもあり、古いモデルを長くご使用いただくよりも、現行モデルにリプレースする方がメリットは大きいと考えられます」

ところで、UPS製品のバッテリーが今も鉛電池が主流であることを不思議に思う方も少なくないはずだ。その第一の理由は、低コストで機器が必要とする大量の電流を出力することが可能という点にある。充電可能回数ではリチウムイオン電池に劣るが、UPSの使われ方を考えると、実はそれも大きなデメリットではないと神谷氏は語る。

「日本の場合、UPSの第一の役割は瞬停への対応になります。この場合、バッテリーを使い切ることはまずありません。そのため、鉛電池でも十分な寿命を確保することが可能なのです」

UPSの容量は左下にまとめたとおり、保護対象機器が実際に必要とする電力であるVA値とバックアップ時間から

現行モデルのSmart-UPS SMTシリーズ。保守提供期間を6年に延長した。 製品型番:SMT750J

求めることができる。本来は安全なシャットダウンのための時間を確保することがUPSの目的だが、より大きな容量の機器を選んだり、バッテリーを増設することでバックアップ時間を数時間～1日以上延長することも可能だ。金融・証券、医療関連など、「停電中もシステムを稼働させたい」というニーズを持つエンドユーザー様も多い。バックアップ時間について、あらためてヒアリングを行ってもいいだろう。

「ビジネスを停めないという目的のために導入されたUPSですが、バッテリーが劣化していた場合には思わぬトラブルの原因にもなります。エンドユーザー様との接点であるパートナー様には、ぜひそうした啓発を進めていただきたいと考えています」

「バッテリーは消耗品! 導入後4～5年で交換提案を」

オムロン株式会社 電子機器統轄事業部 UPS事業部
営業部 営業2課 服部 貴明氏

バッテリーは消耗品のため、交換は必ず必要になります。導入後4～5年経ったUPSの場合、そろそろバッテリーが寿命を迎えることになります。当社製品の場合、4週間に一度、バッテリー自動診断を行い、バッテリー交換時期に達した場合はそのサインを表示しています。しかし急な出費を抑えるという意味でも、サインが表示される前の交換を推奨しています。また、本体の点検もご希望の場合は、UPSの設置場所にエンジニアがお伺いし、点検やバッテリーの交換などを行う「予防保守サービス(有償)」を用意しています。

なお、当社製品の場合、UPS本体の生産終了日から原則5年間の修理受付を行っています(バッテリーは本体生産終了日から原則6年間供給可能)。安心して利用し続けられるというメリットをエンドユーザー様にご提供できます。

Point.2 人的リソースの確保

大災害でオフィスを失っても Web会議システムで業務遂行が可能に

言うまでもないことだが、大災害発生後は人的リソースもボトルネックの一つになる。交通インフラのダメージによって従業員が自宅待機を余儀なくされる状況でも、Web会議システムがあればフェイストゥフェイスのコミュニケーションが可能になる。

BCP対策の一環として提案したいSaaS活用

浸水や倒壊によって社屋が使用不能になったとしても、取引記録や設計図といったバイタルレコードの保全に成功すれば、業務の再開は比較的容易だ。その際に、課題として浮上するのが、従業員間のコミュニケーション手段の確保ということになるだろう。仮に社屋が無事だった場合も、大災害発生後はしばらくの間、交通機関のマヒが続くと考えられるため、何らかの対策を考えておくことが大切だ。そうした中、注目されているのが平時からのSaaS(サービスとしてのソフトウェア)活用である。

その代表がSaaS型グループウェア。東日本大震災の際、自社のメールサーバーが浸水するなどの被害やその後の電力需給逼迫(ひっぱく)により、ビジネスの生命線とも言える通信環境の復旧に時間を要した企業も少なくなかった。しかし、従来からSaaS型グループウェアサービスを利用してきた企業の場合、こうした問題を比較的容易に乗り越えることができた。インターネットにアクセスできる環境さえ確保できれば、メール送受信や従業員間の情報共有が図れることがその理由だ。

メールサーバーを社内で運用するエンドユーザー様の場合、HDD容量の問題から、1人当たりのメール容量を厳しく制限していることも少なくない。こうした場合、"いざ"というときだけでなく、日々の業務効率向上に貢献する点でも有意な提案になるだろう。

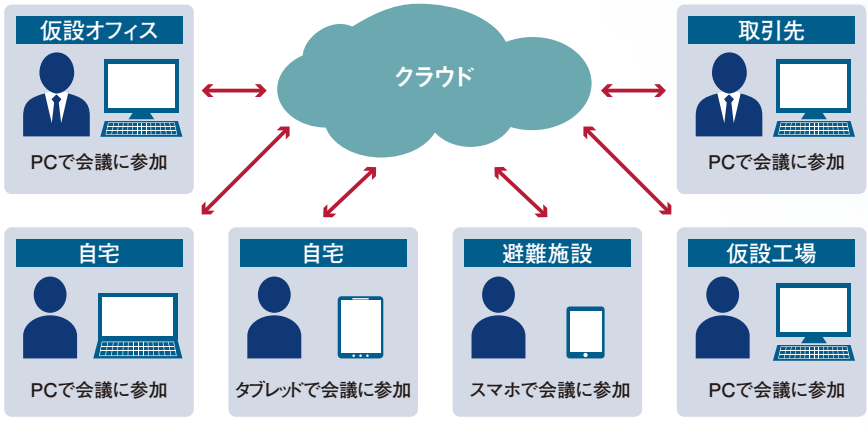
大切なのは人とデータ それがあれば仕事は動く

バイタルデータと並ぶ大災害後のボトルネックの一つが、人的リソースであることは間違いない。また、社屋が使用不能になり、複数のサテライトオフィス、代替工場に分かれて業務を行うような状況も考えられる。その際に大きな力を発揮するのが、Web会議システムである。インターネットに接続できる環境さえあれば、常にフェイストゥフェイスのコミュニケーションが可能になる。

テレビ会議システムが専用カメラや大掛かりな音響機器を必要とするのに対し、PCの組み込みカメラやイヤホン／マイクがあれば、すぐに会議に参加できることがWeb会議システムの最大の特長である。大災害に伴う交通インフラの崩壊により、従業員が自宅待機を余儀なくされる状況のほか、新型インフルエンザのまん延など、パンデミックに対応できる点もWeb会議システムのメリットと言える。

通信手段の確保という点では、スマートフォン、SIMフリータブレットの活用も注目したいポイントになる。東日本大震災が通信手段に大きなダメージを与えたことは記憶に新しい。固定電話・携帯電話共に厳しい通信制限が行われる中、携帯電話のパケット通信だけは比較的スムーズにつながった。一般的な家庭用ネットワーク機器の場合、停電中はブロードバンド回線が利用できないことを考えると、スマートフォン、タブレットからもスムーズにアクセスできるWeb会議システムの提案が望まれる。

□大災害後のWeb会議システム利用イメージ



※Web会議システムによって、インターネットに接続できる環境があれば、端末を問わず、フェイストゥフェイスのコミュニケーションが可能になる。

Point.3 確実なデータ保護のために

注目したいのはクラウドとレプリケーションの複合提案

バイタルレコードの保護にデータバックアップは欠かすことができない。だが、その確実な保護と迅速な復旧を図るうえでそれだけでは不完全である。より迅速な復旧を求めるエンドユーザー様に対しては、クラウドによるレプリケーションをぜひ提案したい。

大震災が浮き彫りにしたデータバックアップの課題

最後にBCP対策の肝とも言えるバイタルレコードの保護について考えていこう。バイタルレコードには、紙文書／電子文書を問わず、設計図や品質管理資料、取引記録など、業務継続に必要なあらゆる記録が含まれるが、ここでは便宜上、電子データを前提に話を進めたい。

データ保護はこれまで、HDDやテープ装置によるデータバックアップによって行うことが一般的だった。だが、東日本大震災を通して浮上したのは、それだけでは不完全という現実だった。大規模災害の際には、バックアップ先の装置も被害を受けることが少なくないことがその第一の理由である。エンドユーザー様の中には、テープ媒体を担当者が定期的に自宅に持ち帰ることで冗長性を担保しているケースもあるが、大規模災害時にはそれも焼け石に水にすぎない。

もう一つの理由は、バックアップを取るだけでは、復旧に長い時間が必要になる点。サーバーに障害が生じた際、サーバー再構築やデータリストアには最低でも2、3日の時間が必要になることが一般的だからだ。

BCP対策におけるデータ保護では、RTO（Recovery Time Objective:目標復旧時間）、RPO（Recovery Point Objective:目標復旧時点）という考え方が重視される。RTOは、復旧までに要する時間で、最短は遠隔地サーバーによる同期レプリケーションになる。RPOはデータ復旧ポイントの新旧を示している。毎日バックアップを取るというエンドユーザー様は多いはずだが、仮に毎日0時にバックアップを行う場合、それ以降翌日0時までに追加されたデータは全て消失することになる。

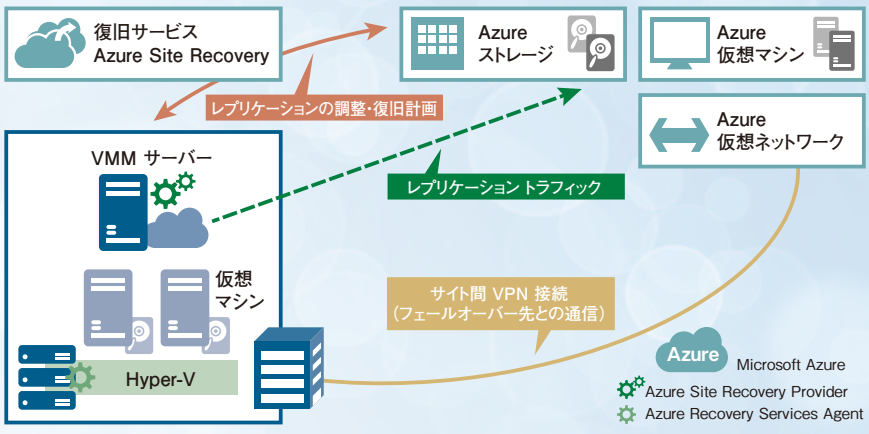
BPOの観点から考えると、「全てのデータが即座に復旧できる」ことが最も好ましいことは言うまでもない。だが、RTO、RPOが短いほど高コストが必要になることもあり、エンドユーザー様がそれぞれの考え方に従って対策を検討することが基本的な考え方と言えるだろう。

クラウドが可能にした新たなDRの選択肢

ROTの短縮には、複製（レプリカ）を別のコンピューターに構築するレプリケーションの利用が効果的だ。これまで遠隔地レプリケーションの仕組みを構築するのは、大企業や一部の業種に限られるのが現実だった。だが今日では、オンプレミスの仮想化サーバーをクラウドにレプリケーションすることで、より低コストで本格的なディザスタリカバリー（DR）環境を構築することが可能だ。大災害時のデータ保護を検討するエンドユーザー様には、こうした提案もぜひ行いたいところだ。

マイクロソフトが提供する、レプリカ先としてMicrosoft Azureを利用する「Azure Site Recovery」（ASR）はその一例である。具体的には、オンプレミス側のHyper-V環境で仮想マシンを構成し、Azureの復旧サービスを使ってMicrosoft Azureにレプリカの設定をするだけで準備が完了する。なお、レプリケーションによってデータの長期保存や世代管理を行うことはできない。人為的ミスやウイルス感染に対応するためにも、従来のデータバックアップとの併用が不可欠だ。BP

□Microsoft Azureによるレプリケーションソリューション



第２特集　個人情報や機密情報が危ない

お客様の情報を守るのは、パートナー様の使命です!

ITの進化した現代社会では、
マルウェアやランサムウェアなどが、
常にオフィスの情報を狙っている。
中堅・中小のエンドユーザー様は、
情報システムに精通した専門スタッフを配置することは難しく、
パートナー様がその役割を担うこともある。
そのため情報漏えいのリスクからエンドユーザー様の
情報を守るのは、パートナー様の責務であると言えるだろう。
ここからは、マイナンバーガイドラインが定める、
物理的・技術的安全管理措置について、具体策を紹介したい。

基礎編

マイナンバー制度のスタートは セキュリティ提案の絶好の機会!

営業提案 1

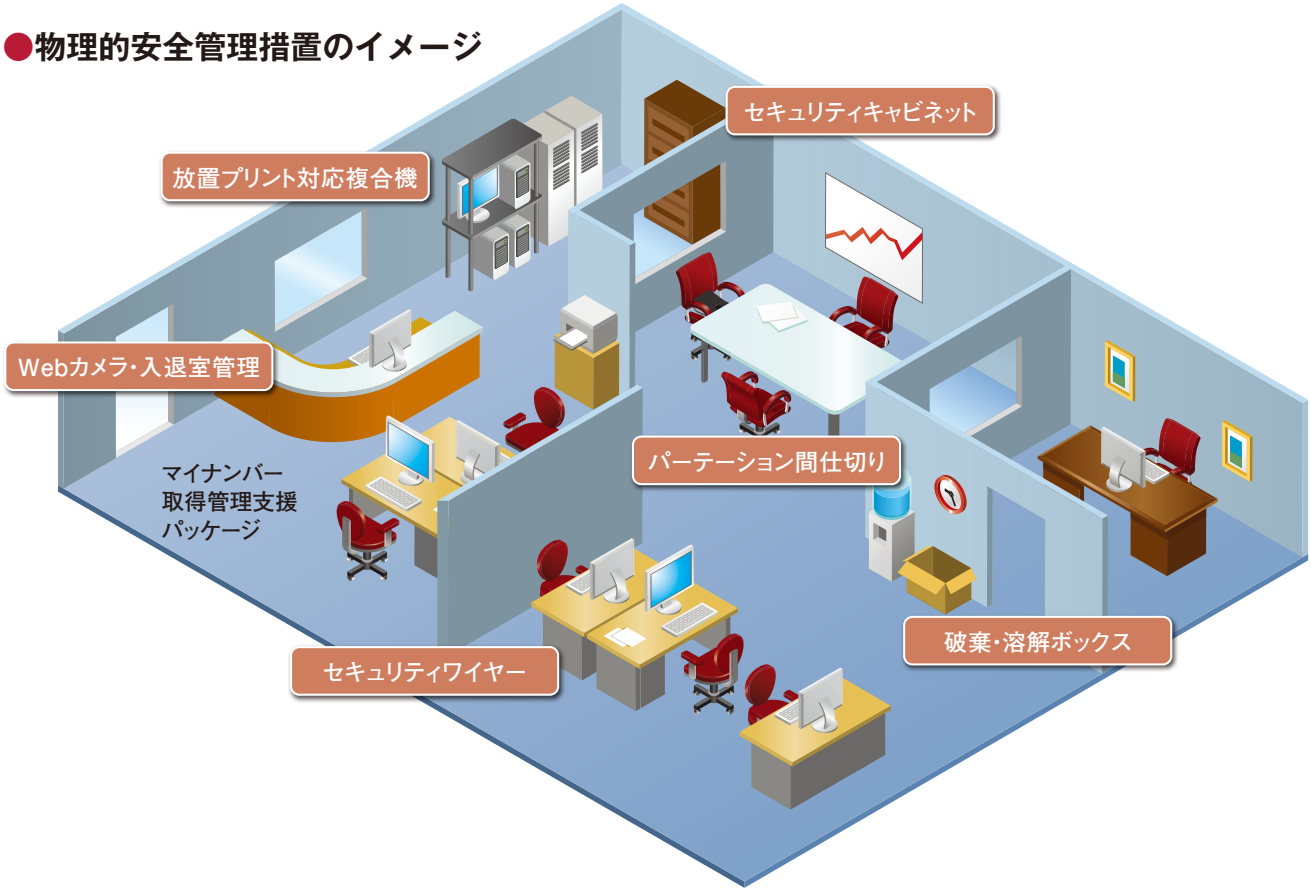
物理的安全管理措置

入退室の管理と共に注目したい 紙出力のセキュリティ管理

物理的安全管理措置は「区域」と「機器」という二方向から考える必要がある。ガイドラインではマイナンバー取扱区域の明確化を求めているが、区域のセキュリティで最も効果的なのが、入退室管理システムの導入である。だがスペースの関係上、それが難しいケースも多い。ガイドラインではパーテーションによって視線を遮るなどの工夫が紹介されているが、それらに加え、紙出力のセキュリティも注目したいポイントの一つ。マイナンバーが記載された書類を出力する機会がこれから確実に増えていく中、プリントアウトの放置対策が大きな課題になると考えられることがその理由だ。具体的には、複合機への個人認証システムや専用プリンター導入がその解決策になる。また廃棄・溶解サービスも今後さらに重要性を増すと考えられる。

他にも入退室などを監視するWebカメラの導入も効果的だ。オフィスへのWebカメラ導入に抵抗を持つ経営層も多いが、不正行為そのものを抑止する効果があることは否定できない。機器の保全では、PCなどをオフィス器具に固定するセキュリティワイヤーの導入が強く求められている。

●物理的安全管理措置のイメージ



営業提案 2

技術的安全管理措置

今後のIT基盤としてぜひとも推奨したい Active Directoryと IT資産管理ツール

厳密なアカウント管理が Active Directoryで可能に

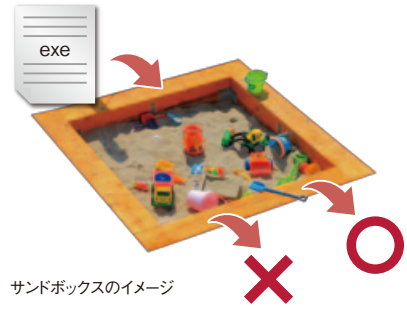
技術的安全管理措置は大きく、「アクセス権の設定による制御」「外部からの不正アクセス防止」という2方向から考えることができる。正当な権限を持つ者だけが情報にアクセス可能な状態を実現する方法としては、Active Directory（AD）によるネットワークリソースの一元管理、ファイル暗号化とパスワード設定による個別ファイルの保護などの方法が考えられる。中でもファイルへのアクセス権限を個別アカウントごとにきめ細かく設定できることに加え、グループポリシーの設定によって、企業が認めたソフトウェア以外のダウンロードを制限することなども可能になるAD導入提案は、エンドユーザー様のこれからのセキュリティ基盤を構築するうえで極めて有意である。

また、これに関連して「どのPCで」「誰が」「いつ」「どのぐらいの時間」「何をしたか」を記録する操作ログ管理機能を備えたIT資産管理ソフトの導入もぜひ提案したい。いわゆるマイナンバー法では、情報漏えいにつながる行為を故意に行った者は処罰されるが、それが故意か否かを判断する際、操作時間等も含むログの存在は大きな意味を持つ。ログ取得は、不正の抑止力になるだけでなく、情報漏えい発覚後のトラブルから従業員を守るうえでも大きな意義を持つ点を強く訴求したい。

ふるまい方でマルウェアを検知するサンドボックス

外部からの不正アクセス防止は、ファイアウォールの設置とマルウェア対策をベースに考えていくことになる。近年、標的型メール訓練サービスを利用するエンドユーザー様も多い。その結果明らかになったのは、どれだけ啓発に力を入れても、悪意ある添付ファイルの実行は決してゼロにはならないという事実だ。

拡張子を注意深く確認することで、悪意ある添付ファイルはある程度見分けることが可能だ。だが、同僚の名をかたるなど標的型攻撃がより巧妙化する中、常に注意を払い続けることは決して簡単なことではない。マルウェアの発見に大きな効果があるのが、仮想環境上で実際にファイルを実行し、そのふるまいを観察することでマルウェアを検知する「サンドボックス」と呼ばれるソリューションだ。マイナンバーを実際に運用する自治体のシステムに導入が義務付けられているサンドボックスは、SaaSとしての提供も開始されている。



サンドボックスのイメージ

なお、ローカルで実行されたマルウェアは、そこからシステムに侵入し、通信回線を経由してデータを外部に持ち出すことが一般的だ。水際対策としては、IT資産管理ソフトが備える外部との通信ログのチェックも有効だ。標的型攻撃によるデータ流出先が、海外小国のサーバーであることが多いからである。

●技術的安全管理措置の概要と具体的な対応例

対策	ガイドライン概要	具体的な対応例
アクセス制御	情報システムを使用して特定個人情報等の業務を行う場合、適切なアクセス制御を行う	・Active Directoryによるアカウント管理 ・IT資産管理ツール等による操作ログ取得 ・生体認証機能の活用 ・ファイル暗号化／パスワードの設定
アクセス者の識別・認証	特定個人情報等を扱う情報システムは、正当なアクセス権を有することを識別・認証する	
外部からの不正アクセス防止	情報システムを外部からの不正アクセス等から保護する仕組みを導入し、適切に運用する	・ファイアウォールの設置・セキュリティ対策ソフトウェアの導入 ・ログ解析による不正アクセスの検出
情報漏えいの防止	特定個人情報等を外部に送信する場合、通信経路における情報漏えい等を保護する措置を講ずる	・添付ファイルの暗号化とパスワード設定

営業提案 3

その他の注目提案

マイナンバーで紙文書管理の弊害が浮上 再注目したい電子化ソリューション

書類を作成し送信し、承認の署名を取得するプロセスが一度も紙出力することなく行える新機能「eSign」もAcrobat DCの注目点の一つだ。

セキュリティを考えるなら純正PDFツールが不可欠

ここまで電子データを前提にセキュリティを考えてきた。だが、オフィスには機密性が求められる紙文書が今も数多く存在する。紙文書をセキュアに管理するには、鍵が掛けられるロッカーなどの物理的対策が不可欠になるが、日々の運用のレベルでも課題が多いのが、文書の卓上への放置、持ち出しによる紛失である。マイナンバー対応が必要な届出書類は最終的には80種類に及ぶとも見られるため、今後、紙をベースとした運用の見直しが進むことが考えられる。こうした中、あらためて提案したいのが、PDFによる電子化・ペーパーレス化ソリューションである。アドビシステムズのPDFソリューション「Adobe Document Cloud」と、その中核を担う「Adobe Acrobat DC」であれば、単に電子化するだけでなく、暗号化しパスワードを設定し、管理することで情報漏えいリスクを大幅に軽減できることがその理由である。

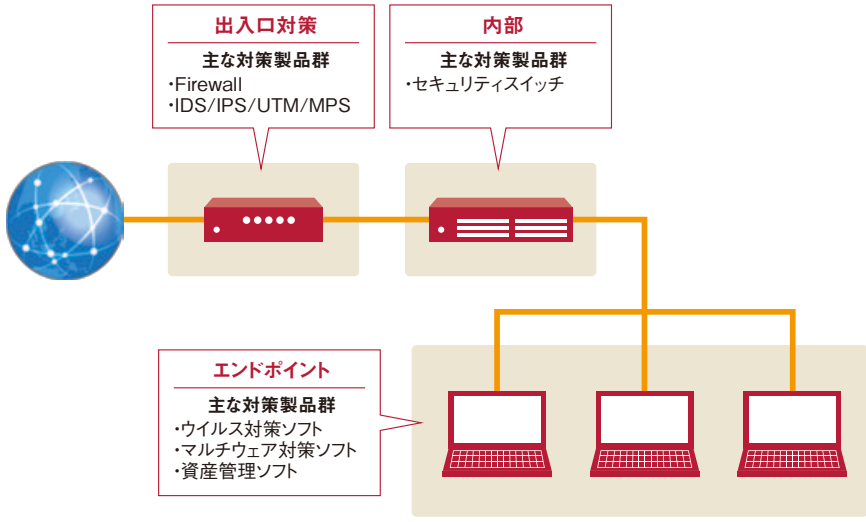
ちなみにPDFを編集・管理するツールは各社が手掛け、こうしたサードパーティー製ツールを使用するエンドユーザー様も少なくない。だがサードパーティー製ツールは、改ざんの容易さなどセキュリティ面でも課題が多いことはあまり知られていない。電子化ソリューション提案では、こうした部分の啓発も重要になるだろう。

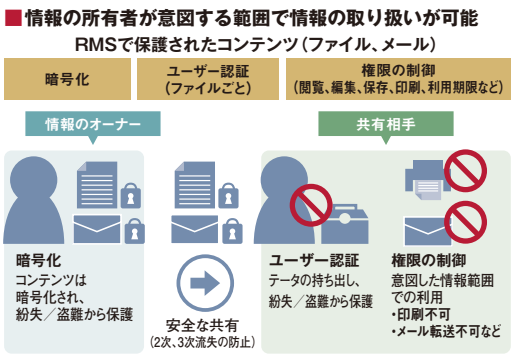
システム内でも防衛し標的型攻撃をブロック

ファイアウォールの設置をはじめとする外部からの不正アクセス防止は、既に多くのエンドユーザー様が対策を行っている。だが、メール添付ファイルや外部記憶媒体などを経由してネットワークに侵入するマルウェア対策は、それだけでは不十分だ。セキュリティ対策では「内部対策」「多重防衛」が重視されつつある。標的型攻撃では、最終目的を達するには複数の段階を経る必要がある。いずれかの段階を失敗させることで、被害を未然に防ぐことが多重防衛の基本的な考え方である。その中核を担うのが、ネットワーク内部の情報を盗み取ろうとする動きを自動的に検知、遮断する「セキュリティスイッチ」だ。また、社内ネットワークの可視化によって、どのような侵入ルートで、どのような被害が生じたか把握できるようになることもその特長である。

標的型攻撃では、知らぬ間に攻撃され、知らぬ間に情報が持ち出されていることが一般的だ。個人情報を取り扱うエンドユーザー様には、転ばぬ先の杖として、ぜひセキュリティスイッチの提案も行いたい。なお同装置は、L2スイッチ（ハブ）と交換することで、簡単に設置できる。BP

●多重防衛のイメージ





IT Keyword
最新ITキーワード

ライツマネジメント
【Rights Management】

システム単位からファイル単位へと変化するセキュリティ対策。セキュリティ対策と利便性はトレードオフの関係にあるといわれるなか、細やかなファイル認証を実現するライツマネジメントの普及が注目されている。

これまでのセキュリティ対策は、不正なアクセスを防ぐためのファイアウォールやパスワードを暗号化してやり取りするPKI（Public Key Infrastructure：公開鍵暗号方式）など、システム全体へのアクセスを保護することに重きが置かれていた。

オフィスで取り扱う個人情報や機密情報のデジタル化が進むにつれて、先に触れた仕組みでは、漏えい対策が難しくなっている。なぜなら保護されたシステムの中にあれば、安全であっても、個々のファイルをシステムの外に持ち出した後には、保護するすべがないからだ。どんなに強固な暗号化技術で保護されているデータであっても、ファイルのコピー、さらにはメールによる転送や印刷を防止することはできない。つまり、複数のユーザーで利用するデータは、情報の漏えいや改ざんを防ぐことは基本的にできないのだ。たびたび話題となる情報漏えい事件のほとんどは、単純なヒューマンエラーによる誤操作（うっかりミス）か、アクセス権限を持つユーザーの故意による犯行とされている。

そこで、注目されているのが、「Rights Management（以下RM）」というキーワードだ。直訳すると“権限の管理”というこの言葉は、次世代のセキュリティ対策の入り口かもしれない。

RMにより保護されたサービスを導入すれば、ファイル単位のアクセスコントロールを行うことができ、先に触れた課題の解決を手助けしてくれる。例えば、データの管理者（作成者）が、印刷や転送、コピーや編集、そして画面キャプチャといった操作の許可や不許可をあらかじめ設定できるので、利用者は設定された制限の中でしかファイル操作ができなくなる。設定した条件に従って、指定された利用者しか、許可された操作を実行できないので、仮にデータが誤って別の利用者に送付されてしまったり、外部に持ち出されてしまったりした場合でも、権限を与えられていないユーザーはファイルを自由に操作できないのだ。

これらRMの代表的なサービスとしては、マイクロソフトが提供する「Azure Active Directory Rights Management (Azure RMS)」などがある。

Azure RMSは、Azure Active Directoryに実装されたクラウド上の認証システムで、暗号化やID、承認のポリシーを使用して、ファイルや電子メールを保護できるサービスだ。もともと、Windows Server 2003には「Rights Management Services（RMS）」という機能があり、このシステムとMicrosoft Office製品を組み合わせることで、ファイル単位のコントロールを可能にしている。RMSで保護されたコンテンツは、「暗号化」され、利用するためには、ユーザー「認証」が必要となる。閲覧はもちろん、印刷の可不可がファイルとユーザーごとに設定されるというわけだ。このRMS が、Azure Active Directoryに対応することで、社内だけでなく、社外でもサービスが提供できるようになり、複数のデバイス（携帯電話、タブレット、および PC）でもRMのサービスを提供できるようになっている。

Office365やPDFファイルは、Azure RMSを想定したファイル形式となっているので、ネイティブでAzure RMSの保護を受けることができる。近い将来、zip形式でファイルをやり取りする感覚で、RMが利用できるようになると予測されている。

今後のセキュリティ対策としては、システム全体やデバイス単位の保護に加えて、ファイル単位といった情報の保護が重要な課題となる。同時にこれらのセキュリティ対策の変化は、パートナー様のビジネスチャンスでもあることも間違いない。BP

Possibility of IT basic technology

進化する

IT基礎技術の可能性

text by 石井英男
1970年生まれ。ハードウェアや携帯電話などのモバイル系の記事を得意とし、IT系雑誌やWebのコラムなどで活躍するフリーライター。

最大7Gbpsの超高速通信を実現する次世代無線通信規格「WiGig」

PCやスマートフォンなどに搭載されている無線通信技術の中でも、広く使われているのが無線LANである。無線LANの標準規格はIEEEによって定められており、IEEE 802.11bやIEEE 802.11gなどのように、IEEE 802.11＋英字という形になる。現在は、IEEE 802.11nやIEEE 802.11acが主流であり、前者は最大600Mbps、後者は最大1.7Gbpsでの通信に対応した製品が発売されている。最大1.7Gbpsというと、非常に高速なようだが、この値はあくまでも理論値であり、実効速度はその半分以下しか出ないのが普通だ。さらなる高速化を目指して、2013年1月に策定された規格がIEEE 802.11adである。IEEE 802.11adの最大の特徴は、利用する周波数帯にある。これまでの無線LANは、2.4GHz帯または5GHz帯を利用しているのに対し、IEEE 802.11adでは60GHz帯という非常に高い周波数帯を利用する。60GHz帯も2.4GHz帯/5GHz帯と同じく、免許不要でグローバルで使える周波数帯である。なお、60GHz帯の波長はミリメートルオーダーになるため、ミリ波と呼ばれることもある。

一般に周波数が高くなるほど広い帯域を使えるため、高速通信には有利だが、直進性が強くなり、距離による減衰も大きくなる。WiGigはこのIEEE 802.11adをベースにしており、最大7Gbpsという超高速通信を実現する。WiGigはもともと「Wireless Gigabit Alliance」という業界団体が標準化や認定プログラムの策定を行っていたのだが、2013年3月に無線LAN機器の技術策定を行う業界団体「Wi-Fi Alliance」に吸収された。業界団体が統合されたことで、Wi-Fiの認証とWiGigの認証を一緒に行うことが可能になり、WiGigの普及に弾みが付くことが予想される。前述したように、WiGigは60GHz帯という高い周波数帯を利用するため、通信範囲は約10mと現行の無線LANに比べると短い。また、人の身体などに遮られると届きにくくなるので、WiGigでは電波を特定の方向に集中的に照射する「ビームフォーミング」技術を利用している。WiGigは、主に宅内での機器や身につけるウェアラブル機器での活用を想定しており、現行の無線LANの置き換えというよりは、相互に補完する役割を果たすことになるだろう。つまり、2.4GHz帯/5GHz帯/60GHz帯のトライバンドに対応し、電波が十分に届く近距離では通信速度の速いWiGigを使い、移動するなどして電波が届きにくくなったら、Wi-Fiにシームレスに切り替えてそのまま通信できるようになるわけだ。

WiGig対応チップセットやモジュールは、Qualcomm AtherosやIntelなどからすでに出荷が開始されており、CES 2016の会場でもWiGig対応無線LANルーターの参考展示が行われていた。また、2016年2月18日～26日に成田国際空港でWiGigスポットの実証実験が実施された。成田国際空港と共同で実証実験を行ったパナソニックによると、WiGigスポットの実証実験は「世界初」とのことだ。この実験では、3つのWiGig対応モジュールを内蔵したアクセスポイントが用意され、コンテンツサーバに格納された映像コンテンツをダウンロードするというものだ。1つのアクセスポイントには最大12人の同時接続が可能で、1ユーザーあたりの実効速度は1Gps以上を実現する。この速度なら2時間の動画も10秒程度でダウンロードできることになる。2016年度中にも、WiGig対応チップセットやモジュールを搭載したノートPCやタブレット、スマートフォンが登場するとみられており、今年はWiGig市場が本格的に立ち上がる年となるだろう。古くなったPCのリプレイスで、WiGig対応PCを導入するのなら、あわせて無線LANルーターや無線LANアクセスポイントなどもWiGig対応のものへ更新することをお勧めしたい。BP

成田国際空港に設置されたWiGigスポットの様子（イメージ）