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.86
2016

巻頭インタビュー

元 東京都交通局長（株）はとバス元社長

宮端 清次氏

倒産寸前のはとバスを
1年たらずでよみがえらせた
経営者の習慣とは?

第2特集

パートナー様の売上をアップするビジネスチャンス満載!

企業をめぐる法改正から考える新たなビジネスチャンス

CAD情報

「ONE TEAM Extension - Japan」レポート

これからの市場をリードするのは、
安定した収益をもたらすサブスクリプションモデル

Navi Value

PC修理の延長保証サービス「BPワランティ」

安心の修理サービスを提供する延長保証サービスに
ご要望の多いタブレット対応プランがついに登場!

メーカーズボイス

エレコム株式会社

キヤノンマーケティングジャパン株式会社

巻頭特集

サンドボックスと
クラウドバックアップが効果的

標的型攻撃と ランサムウェアの最新対策

Presented by Otsuka Corporation

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35回

宮端 清次氏

元 東京都交通局長
(株)はとバス元社長

倒産寸前のはとバスを1年たらずでよみがえらせた経営者の習慣とは?

東京の定期観光バスの代名詞として知らない人はいない「はとバス」。今から20年近く前、深刻な経営危機に陥っていたことはご存じだろうか？　その再建請負人として、わずか9カ月で奇跡の黒字化を果たし、V字回復に導いたのが今回インタビューする宮端清次氏だ。給与カットをはじめとする「徹底した合理化」と「サービスの向上」という相反する目標を達成し、瀕死のはとバスを再び大空に羽ばたかせた原動力は何だったのか？　その秘密に迫る。

もう1年赤字なら潰れたも同然 断腸の思いで給与をカット

BP：倒産の危機に瀕したはとバスの再建を託されたのは1998年、宮端さんが63歳のときだったそうですね。

宮端清次氏（以下、宮端氏）：まさに青天の霹靂でした。当時、わたしは東京都地下鉄建設株式会社で2年半後に開業を控えた都営12号線（現・都営大江戸線）の建設に携わっていました。

東京都庁に35年間勤め、交通局長などを経て退職した後、最後のご奉公のつもりで働いていたのです。

このまま無事“定年”を迎えるのかなと思っていたら、ある日突然、当時の青島幸男都知事に呼び出され、副都事から「はとバスを建て直してほしい」と言われ、「いったいどうなっているんだ?」と、ただ驚き、困惑するばかりでした。

BP：当時のはとバスの経営は、かなり深刻な状況だったと聞いています。

宮端氏：財務諸表を見て驚きました。何しろ4年連続で赤字を計上しており、売上高130億円に対して借入金が70億円にも達していたのですから。

しかも年間7回もの借り換え融資を受けており、借り入れが一度でもストップしたら、すぐにでも倒産してしまいかねない状況でした。

1998年と言えば、北海道拓殖銀行や山一証券といった大手金融機関が次々と経営破たんしたバブル崩壊後の金融危機の最悪期です。金融機関そのものが多額の不良債権処理に苦しんでいたのですから、いつまでも借り入れ融資を継続してもらえるとは限りません。

東京都は、現在と同じように当時もはとバスの筆頭株主でしたが、だからと言って民間企業を都民の血税で救うわけにはいきません。そこで何とか自力で生き延びさせようと、長年交通行政にかかわってきたわたしに白羽の矢を立てたのです。

皮肉なことに1998年は、はとバス開業50周年の節目の年でした。せっかく築き上げてきた伝統を絶やすまいと、必死に再建に取り組みました。

BP：かなり厳しいコストカットを断行されたようですね。

宮端氏：はとバスの社長に就任したのは1998年9月28日ですが、2カ月ほど前に内示を受けてから、すぐに緊急の合理化策を練り上げました。

その骨子は、1. 過去2年間赤字だった路線や事業の廃止、2. 運転手の乗務手当を拘束時間からハンドル時間（実際にハンドルを握った時間）に短縮、3. 55歳役職定年とし、管理職を調査役にして給与を引き下げる、といったものです。

このほかにも無駄なコストは徹底的に省き、出るおカネをとことん減らすことにしました。

もちろん、一方で入るおカネも増やしていかなければなりませんから、「徹底した合理化」とともに、「サービスの向上」にも努めることにしました。

しかし、これらの合理化策を推し進めたとしても、その効果は半年から1年後にならないと表れないことがわかったのです。

わたしが社長に就任した1998年9月末から、期末の翌99年6月まで、残された時間は実質わずか9カ月しかありませんでした。もし、この期も赤字になったら5年連続です。赤字が5年も続くような会社は潰れたに等しいと言えますから、何としても残りの9カ月間で合理化を果たし、黒字を達成しなければと焦りました。

そこで、社員の皆さんの猛反発を受けることは重々覚悟のうえで、即効性のある合理化策として給与カットに踏み切ったのです。まさに断腸の思いでした。社長であるわたしが3割、役員が2割、社員が1割の給与カットを実施した結果、その年は約5億円の人件費を抑えることができ、3億6千万円余の黒字となりました。

おかげでどうにか、5年連続赤字を免れることができたのです。

経費は削減しても サービスの質は落とさない

BP：とはいえ、給与カットで得られる増益効果は1回限り。その後、V字回復を果たすことができた原動力は何だったのでしょうか？ 給与カットで現場のモチベーションは下がらなかったのでしょうか?

宮端氏：正直に申し上げると、当初、現場の経営に対する怒りは相当なものでした。わたしは社長になった直後から、社員の皆さんを集めて説明会を何度も開き、「徹底的な合理化」と「サービスの向上」という2つのテーマを積極的に推し進めていきたい、という考えを丁寧に説明しました。

しかし、ある会で説明を聞いていた運転手の方から、「われわれはこの4年間、経営側が言うとおりに頑張って働いてきた。それなのになぜ給与をカットされなければならないのか？　経営の失敗の責任を、われわれに押し付けているのではないのか？」という強いお叱りをいただいたのです。

本音を言えば、失敗したのは前の経営陣なので、わたしが責任を問われる筋合いではないのですが、もちろんそんなことは言えません。ただ平身低頭、謝るしかありませんでした。

もちろん、社員の方々がそんな気分のままで業務に臨んだとしても、サービスが向上するわけがありません。

そこで気付いたのです。それまでわたしが訴えてきた「合理化」や「サービスの向上」というのは、ただ言葉を発していただけにすぎない。まったく実が伴っていないじゃないか、ということに。これでは、社員の皆さんがしらけてしまうのも無理はありません。

そもそもわたしは、都の命令を受けて天下ってきた人間です。ただでさえ社員の皆さんのほうを向いていないと思われても不思議ではない立場なのですから、わたしのほうから社員の皆さんにしっかりと向き合い、たんなる言葉としてではなく、「合理化」と「サービス向上」の何たるかを有言実行していかなければならないと考えたのです。

BP：具体的には、どのような取り組みをされたのでしょうか？

宮端氏：まず、社長室をなくして大部屋に移り、社員の皆さんを名前で呼ぶようにしました。とにかく、皆さんと顔を突き合わせて、日ごろからコミュニケーションを交わすことが大事だと考えたのです。さらに、社長専用車を共用車にして、電車とバスで通勤し、率先して合理化に努めました。

また、社員の皆さんと本音で語り合うために、「お帰り箱」という目安箱のようなものも設置し、社員の直訴に必ず返事しました。

給与カットによって、「会社はそこまで危機に陥っているのか？」と不安を抱く社員の方もいましたが、会社に不安や不満を持っているようでは、いいサービスなど到底できませんし、会社そのものが成り立ちません。「何でもいいから積極的に直訴しなさい」と呼び掛けて、不安や不満を1つひとつ潰していきました。

BP：合理化については、行き過ぎに対する反省もされたそうですね。

宮端氏：社員の皆さんに対する経営方針説明会の中で、ある女性ガイドの方から、「バスの中で提供するお茶の葉の質が下がってしまって、お客さまに申し訳ない」という意見が出たんですね。

はとバスは、何度もご利用いただいているお客さまが多く、そうした常連のお客さまほど、サービスのちょっとした変化にも敏感にお気づきになられるものです。そのガイドさんの意見を聞いて、わたしは「社長失格だ」と強く反省しました。

会社が危機に瀕しているので、「何でもいいから、とにかく経費を節減しなさい」と伝えたのは事実です。

しかし、本社や間接部門の経費は節

減しても、お客さまへのサービスの質に直接影響するものは、絶対に削ってはならない。そのことを言い忘れていました。社員の皆さんに教えられながら、わたし自身、何度も軌道修正を図りつつ、「合理化」と「サービスの向上」という一見相反する目標を1つひとつ一緒にクリアしていったのです。

自ら客として「はとバス」に乗りサービスの何たるかを知る

BP：サービス向上のため、社長でありながら自らも乗客の1人として、何度もはとバスに乗られたそうですね。

宮端氏：わたしが社長になってから、はとバスの新しい経営方針として「お客さま第一主義」「現場重点主義」「収益確保至上主義」の3つを掲げました。

このうちの「お客さま第一主義」について、社員の皆さんとの会合でわたしの考えを伝えたのですが、どうも反応がよくない。そこで「わたしの言っていることがわからない人は手を挙げて」と問い掛けたところ、3割ぐらいの方が手を挙げたのです。

3割が手を挙げるということは、実際には半分以上の人がわかっていないはず。そして、わかってもらえないのは問い掛けている自分自身が「お客さま第一主義」の何たるかを身をもって体験していないからではないか、ということに気付いたのです。

そこで、「わからない人は休みの日に自腹を切って、はとバスに乗ってみてください。わたしもこれから月3回、妻と一緒にはとバスに乗ります」と宣言してしまったんです。

言ってしまった手前、やらざるを得なくなりましたが、嫌がる妻を連れて月に3回もバスに乗るのは、決してラクなことではありませんでした。1回当たりの運賃は8000円、夫婦2人で1万6000円ですから、おカネもばかになりません。

でもそのおかげで、お客さまがはとバスのツアーに何を期待しておられるのか、どんな点に不満を抱いておられるのかというのがよくわかりました。

自分が客の立場になってみれば、サービスの良し悪しを身をもって感じることができますし、同乗するお客さまからのさまざまな声も聞こえてきます。

そうした体験を重ねることによって、「サービス向上」のための提案にも説得力が増しただけでなく、経営者自らが率先して「サービス向上」のために努力しようとしている姿を見て、社員の皆さんも何かを感じ取ってくださったのではないかと思います。

BP：そうした努力によって、経営者と社員の心がひとつになったことが、はとバスの再生に結び付いたのですね。

宮端氏：いまでも「なぜ、経営の危機に瀕したはとバスをよみがえらせることができたのですか?」と何度も尋ねられますが、それは、現場の皆さんが「お客さま第一主義」に徹する意識を持って、実行してくれたからです。まさに再建の立役者は社員だったのです。

これが実現できたのは、お客さまに直接接する現場の皆さんこそが、はとバスの“顔”であり、“代表”なのだということを自覚していただけたからです。

それに気づいてもらうために、わたしは会社の組織図も大きく見直しました。以前の組織図は、上から経営者、役員、現場の社員という正三角形でしたが、これではお客さまがその下になってしまいます。本当はお客さまがいちばん上にいらっしゃって、その下に社員、役員、経営者が並ぶという逆三角形であるべきではないか。そう考えて、組織図をひっくり返したのです。

かつての組織図では社員の方々が“末端”のように扱われていましたが、じつは、お客さまに近い現場の社員の方々こそが、会社にとっての“先端”なのです。これは、はとバスに限らず、あらゆる会社に言えることではないかと思います。“先端”で活躍する社員の皆さんに、社を代表するという誇りを持って生き生きと働いていただくこと。それを支えるのが“末端”である経営者の務めではないでしょうか。BP

元 東京都交通局長　（株）はとバス 元社長

宮 端 清 次 氏

Miyabata Kiyotsugu

◎ Profile

1935 年、大阪市出身。1959 年、中央大学大学院法学研究科修了後、東京都庁入庁。総務局災害対策部長、交通局長を経て、平成6年東京都地下鉄建設株式会社代表取締役専務、平成10年株式会社はとバス代表取締役社長に就任。当時、倒産寸前であったはとバスにて、コスト改革・意識改革を断行し、同社を再建。短期間で復配に漕ぎつけた手腕は「経営幹部の行動学の鑑」とビジネス各紙で話題となる。その後、東京都交通局経営アドバイザリー委員や大阪市交通局市バスのあり方検討委員会委員などを歴任し、現在は、研修講師として活躍中。

巻頭特集

サンドボックスとクラウドバックアップが効果的

標的型攻撃とランサムウェア最新対策

標的型攻撃は、フィッシングメール（偽装メール）と
不正プログラムを組み合わせて行う方式が一般的。
また、ハードディスクの中のファイルを暗号化し、
解除する代わりに金品を要求するランサムウェア。
似て非なる攻撃ではあるものの、
中堅・中小企業が標的とされる理由には、
セキュリティ対策の甘さがある。
パートナー様には、これらの点を踏まえたうえで、
エンドユーザー様へ情報を提供しつつ、
弱点を補強するようなご提案が求められる。

進化する標的型攻撃 求められる多重防御という考え方

実は国内企業の1/4はマルウェアに感染している!?

昨年1年間に発覚した標的型攻撃による企業・各種機関の被害件数は23件。流出情報は、公表分だけで110万件近くに及ぶ。注目したいのは、そのうち18件が外部からの指摘で初めて被害に気づいたという事実である。

トレンドマイクロの報告によると、同社が依頼を受けて行った調査でマルウェア感染が発覚した事例の多くは、調査依頼の5カ月以上前に最初の侵入を許していたという。また、全調査事例の約1/4で標的型攻撃の痕跡が発見されている。自主的な調査依頼という点で多少割り引いて考える必要はあるが、現時点においてすでにマルウェア侵入を許しているエンドユーザー様も少なくないはずだ。

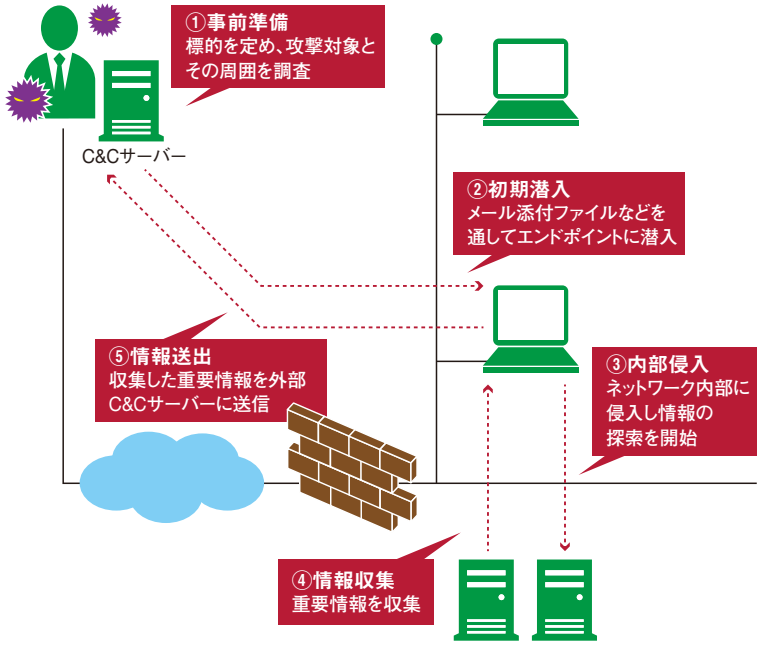
標的型攻撃が増え続ける背後には、データを人質に身代金を得るランサムウェアの登場によって、攻撃者が金銭的利益を得やすくなったという現実がある。ランサムウェアとは、感染PCをロックしたり、ネットワーク内のファイルを暗号化し使用不能にしたうえで、元に戻すことと引き換えに身代金を求める不正ソフトの総称。企業経営者などの身代金目的の誘拐が日常化する中南米を中心に、被害額が年間十数億ドルに及ぶ一大産業に成長しているという。

標的型攻撃対策として、ぜひ提案したいのが多重防御という考え方だ。セキュリティ対策としてエンドポイントへのアンチウイルス導入が広く普及しているが、それだけでは標的型攻撃を防ぐことは難しい。アンチウイルスによる防御は既に検知されたマルウェア情報に基づいて行われるが、標的型攻撃の場合、新たなマルウェアを生成したうえで攻撃を開始することが一般的だからだ。標的型攻撃は、①事前準備、②メール添付ファイル等によるネットワークへの侵入、③さらなる内部侵入、④重要情報の収集、⑤重要情報の外部への送信というプロセスで行われることが一般的である。その対策としては、①入口対策、②内部対策、③出口対策、④データ保全という四つのフェーズで行うことが効果的だ。

■多重防御の考え方

入口対策	防御力を向上し、やられないようにする	サンドボックス 不正侵入／防御システム（IDS／IPS） ゲートウェイ型アンチウイルス
内部対策	やられていることをすぐに検知できるようにする	セキュリティスイッチ 操作ログ管理
出口対策	やられていても被害を少なくする	URLフィルタリング 個人情報検知ツール
データの保全	やられた後でもデータを保護する	データバックアップ

■標的型攻撃の基本パターン



マルウェアをネットワークの入口でブロックし、大切な情報を守る

入口防御は、マルウェア対策の基本

入口対策とは、インターネットと社内ネットワークの境界やエンドポイントにおいてメール送受信やWebアクセス通信をチェックし、ネットワーク内部を守る仕組みの総称。インターネットとの境界に設置されたファイアウォールがその名のとおり塀とするなら、入口対策は塀を守る警備員や監視カメラと考えることができる。

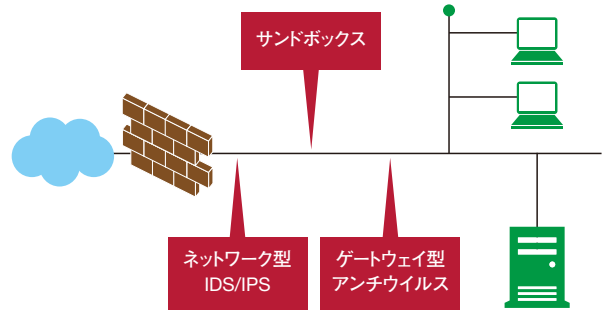
入口対策においてまず注目したいのが、受信メールに添付されたファイルを仮想環境で実行し、そのふるまいを見極めることでマルウェアを検知する「サンドボックス」と呼ばれる仕組みだ。サンドボックス（Sandbox）とは、子供たちの遊び場である砂場を意味する言葉。システムから隔離された環境を用意し、そこでファイルを自由にふるまわせることからこの名が付けられたといわれる。

サンドボックスは未知のマルウェア検知が可能だが、残念ながら万能というわけではない。分析に一定の時間が必要であり、業務に支障を生じさせないためにもファイルのコピーを分析対象にすることが一般的だからだ。つまりマルウェアを検知したときには、すでにオリジナルはエンドポイントに到達しているのだ。サンドボックスは、ネットワーク内部へのマルウェア侵入をいち早く知ることができる優れた仕組みだが、それだけでは情報を確実に守ることはできない。また、仮想環境では挙動を変えるという進化したマルウェアの登場も報告されているため、内部・出口対策を合わせて行うことが大切になる。

入口対策にはそのほかに、不正侵入検知／防御システム（IDS／IPS）、ゲートウェイ型アンチウイルス、Windows 10にも実装される未知のプログラムの実行制御などがある。

エンドポイント型アンチウイルスは軽快な動作性との両立が求められるため、セキュリティ機能のみを追求するのは難しい。ゲートウェイ型であれば動作の軽快性を考慮することなく最高水準のセキュリティ機能を提供できることから、導入を進めるエンドユーザー様も少なくない。エンドポイントとゲートウェイに異なる製品を導入することで、二重チェックが可能になるというメリットも備えている。

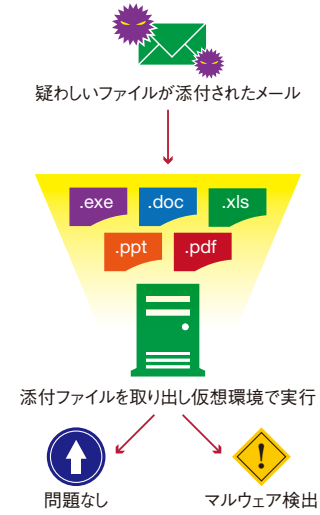
■入口対策のイメージ



■入口対策の具体例

サンドボックス	仮想環境下でファイルを実行させることでマルウェアを検知。未知の脅威にも対応可能だが、基本的にファイルのコピーを分析対象にするため、内部への侵入を完全に防ぐことは難しい。
不正侵入検知／防御システム（IDS／IPS）	あらかじめ登録されたシグネチャと呼ばれる侵入手口のパターンや、通常とは異なるふるまいを通して攻撃を検知。IPSが防御措置まで行うのに対し、IDSは防御措置を行わない。リアルタイムの防御が可能。
ゲートウェイ型アンチウイルス	メールの送受信やWeb閲覧時の通信を監視。パターンファイルと照合し、マルウェアの検知・削除を行う。マルウェアを検知すると、メッセージ全体を削除したり、マルウェアのみ削除し、ユーザーにメッセージを送るなどの対応を行う。

■サンドボックスの運用概念



[営業提案 2]
内部対策

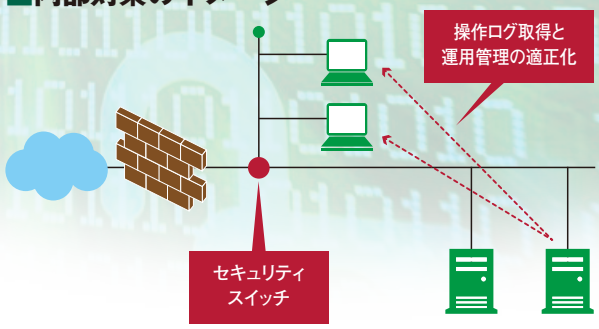
エンドポイントに到達したマルウェアのふるまいを検知し、確実に封じ込める

システム内の不審な動きを検知し、マルウェアを隔離

監視の目をくぐり抜け、エンドポイントに到達したマルウェアは、その端末を拠点としてシステム内部への侵入を開始する。マルウェアはその際、ファイルサーバーにアクセスして情報を収集するだけでなく、Active Directoryサーバーに侵入することで、より上位のアクセス権限を取得し、さらにシステムの奥深くへと侵入するという動きをとることも珍しくない。ネットワーク内部を監視し、こうした不審なふるまいを検知することが内部対策の主な役割になる。

内部対策としてまず注目したいのが、マルウェアに感染したエンドポイントを自動的に隔離するセキュリティスイッチである。従来の検疫ネットワーク（NAC）製品との最大の違いは、NACがネットワークに接続する端末のウイルス対策が最新の状態でない場合に通信を遮断するのに対し、セキュリティスイッチは、サーバーへの執拗な攻撃など、不自然なふるまいを通してマルウェアに感染した端末を検知し、通信を遮断する点にある。ふるまいを前提にすることで、既知・未知を問わず、あらゆるマルウェアへの対応が可能になる。また、ネットワーク内の端末を中継するL2スイッチの位置に配置するため、ネットワークに大きな手を加えることなく容易に導入できる点もその特長の一つである。

■内部対策のイメージ



内部対策では「いつ」「誰が」「何をしたか」を把握するログ管理、ポリシーを逸脱した不適切な操作の制限なども重要になる。標的型攻撃というテーマからは離れるが、操作ログ収集や操作画面の取得は、従業員による不正への大きな抑止力として働く。こうした対策はIT資産管理ツールを使って行うことが一般的だが、マイナンバーをはじめとする重要情報の内部からの漏えいを防止するうえで必須の仕組みといえるだろう。

なお、Windows更新プログラムをはじめとするセキュリティパッチの適用は、全てのセキュリティ対策の基本になる。ネットワークにアクセスする全端末のセキュリティパッチ適用を確実に行うには、IT資産管理ツールやモバイルデバイス管理ツールが不可欠だ。未導入のエンドユーザー様には、標的型攻撃対策という観点からあらためて積極的なご提案を行いたい。

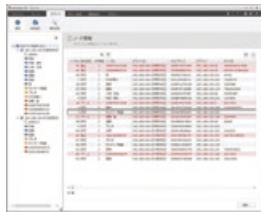
■内部対策の具体例

セキュリティスイッチ	ネットワーク内の通信をリアルタイムで監視し、不審なふるまいを検知し、マルウェア感染した端末を自動的に遮断。入口対策との連携によって、より大きな効果を発揮する。
操作ログ管理	「いつ」「誰が」「何をしたか」を可視化することで、不審な動きの検知が可能になる。標的型攻撃への対策だけでなく、不正な操作による情報漏えいを抑止する効果もある。

■SKYSEA Client View

大きなアイコンや機能ガイドで、目的の機能がひと目で分かるよう構成された管理画面。また、複数台のマスターサーバーで運用する場合でも、連動して検索したり、過去の操作ログもリストア（復元）せずに利用できるなど、「使いやすさ」にこだわった設計が特徴的だ。

■LanScope Cat



社内にあるネットワーク機器を自動検知・情報収集し、管理対象とすべきIT資産を把握できる。また、社員の持ち込みPCなども検知・遮断し、管理者に通知することでウイルス感染などの脅威からネットワークを守ってくれる。

URLフィルタリングによって社外へのデータ流出を水際で阻止

全ての送信をチェックし、水際で漏えいをブロックする

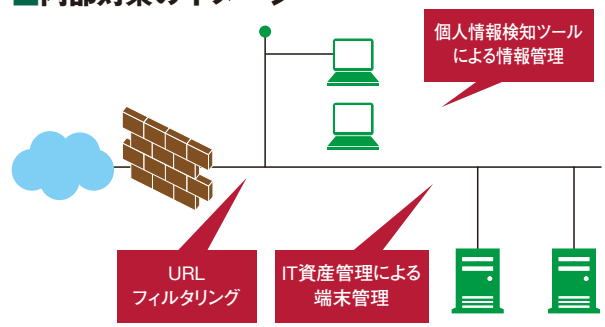
情報の取得を目的とした攻撃の場合、ネットワーク内部への侵入を許したマルウェアが入手したファイルは、最終的にメールを装う形で攻撃側サーバーに送信されることが一般的だ。その被害を食い止める最後の防衛線になるのが出口対策である。その主力として機能するのが、問題がある送信先へのデータ送信をブロックするURLフィルタリングという仕組みである。

マルウェアはデータを外部に送信するだけでなく、随時外部サーバーから指示を得て動いていることも珍しくない。これらの目的のために攻撃者が立てたサーバーは、C&Cサーバー（Command and Control Server）と呼ばれる。既知のマルウェア解析などを通してリスト化されたC&CサーバーのIPアドレスとURLデータベースにもとづき、不審な通信をシャットアウトすることがURLフィルタリングの基本的な考え方になる。

標的型攻撃の被害が海外で急増していることもあり、我々はC&Cサーバーの設置先も海外が多いと考えがちだ。しかしセキュリティ企業の米FireEyeによると、意外にもそのうちの相当数は日本国内に設置されているという。これは日本企業を直接的に狙ったものというよりもむしろ、「日本国内のサーバーであれば安心」という国際的な信用を逆手に取った攻撃側の戦略とみられるが、サーバー設置国を問わず、あらゆる通信に脅威が潜んでいる点には注目が必要だろう。

なおURLフィルタリングは、アンチウイルスと同じようにリスト化された既知の危機にしか対応できないという弱点がある。この補完には個人情報検知ツールの併用が効果的だ。個人情報検知ツールとは、ファイル内に名前や住所、電話番号、メールアドレス、マイナンバーなどの個人情報が含まれているか否かを高速でチェックするツール。ネットワーク内に分散して保管される個人情報の発見とその集約化が主な目的だが、IT資産管理ツールなどとの連携により、エンドポイントで発見された個人情報を含むファイルの自動削除など、個人情報漏えい防止にも活用できる。その機能を使うことで、マルウェアがC&Cサーバーに送り出そうとする個人情報を水際でブロックすることが可能になる。同様の理由から、個人情報検知ツールはUSBメモリーなどを媒介した情報漏えいにも有意である。

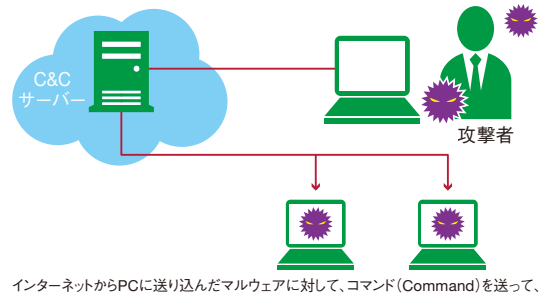
■内部対策のイメージ



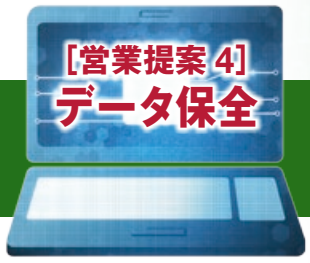
■出口対策の具体例

URLフィルタリング	マルウェア分析などを通してリスト化されたC&Cサーバー情報にもとづき不審な通信をシャットアウトし、情報流出を防ぐ。
個人情報検知ツール	マイナンバーをはじめとするネットワーク内部の個人情報を自動収集するツール。IT資産管理との併用によって、漏えい対策にも活用できる。
IT資産管理	個人情報を含む情報の送信をエンドポイントで阻止。内部からの意図的な情報漏えいに対しても効果的だ。

■C&C（Command and Control）サーバーとは？



インターネットからPCに送り込んだマルウェアに対して、コマンド（Command）を送って、遠隔からコントロール（Control）するサーバーのことを、「C&Cサーバー」や「指令サーバー」と表現する。これらのサーバーは、外部から侵入して乗っ取ったコンピューターを利用することが常套手段となっている。



ランサムウェア対策には クラウドによるバックアップが有効

端末をロックしたり、データを暗号化し身代金を要求するランサムウェアの場合、入口対策を突破された時点で被害が生じる危険性がある。だがその被害は、ネットワークと切り離されたメディアによるバックアップを定期的に行うことで回避することが可能だ。具体的には、世代管理まで含め、テープバックアップを確実に行うことがその解決策になる。

だが、テープバックアップ装置を導入するエンドユーザー様の実情を見る限り、世代管理まで含めたバックアップが行われているケースは決して多くはない。手間を考えると、世代管理まで含めたバックアップをクラウドで行うことも有意な選択肢になる。例えば、Microsoftのクラウドサービス Azureであれば、バックアップデータはフォルダ単位で5世代前まで保存され、本番運用サイトにトラブルが生じた際は必要に応じて世代をさかのぼり、リストアすることが可能だ。

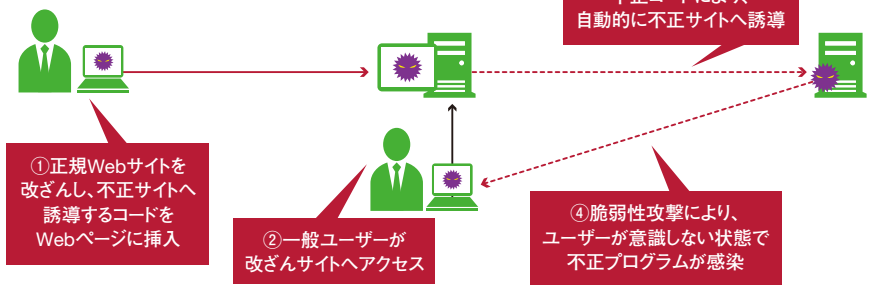
■クラウドバックアップのイメージ

データ漏えいと共に注意を促したい Webサイト乗っ取りリスク

サンラムウェアとともに注意を促したいのが、Webサイト改ざんリスクである。現実問題として、正規Webサイトの表示をいたずら的メッセージや攻撃者の主義主張に沿った内容に改ざんする愉快犯だけでなく、そこにアクセスした利用者を不正サイトに誘導することで、不正プログラムを拡散するという事例もすでに現れはじめている。企業等が管理するWebサイトが改ざんされた場合、今後管理責任を問われることも十分考えられる。

攻撃手法は大きく、①Webサイトの脆弱性攻撃、②Webサーバーへのアクセス権限を持つアカウント情報の盗み取りの二つに分けられる。Webサーバーをクラウドで運用する場合、脆弱性への対応を委託することで前者のリスクはある程度軽減可能だ。問題は一見すると正規の方法で改ざんが行われる後者である。対策としては、Webサーバー管理アカウント管理の徹底化、システム改変監視、各種ログ取得、ログ監視強化によるWebサーバー監視体制強化が重要になる。

■Web 改ざんによる不正プログラム拡散



第２特集 パートナー様の売上をアップする
ビジネスチャンス満載!

企業をめぐる法改正から考える 新たなビジネスチャンス!!

マイナンバー制度、個人情報保護法の改正、
e-文書法の改正、ストレスチェックの義務化など、
企業を取り巻く状況は法制度の面でも大きく変わろうとしている。
そこで、2015年以降の法改正のポイントを再確認。
新たなビジネスのきっかけとして、
パートナー様の売上アップにつながるようなご提案を紹介する。

改正された法律の内容を理解し、業務の効率化、コストの削減を提案!

【営業提案1】マイナンバー対策

法令対応だけにとどまらない有意かつ攻撃的なIT投資を提案

新入社員の社会保険手続きや退職者の源泉徴収票など、一部では既にマイナンバー利用はスタートしている。しかし、その本格的な利用がはじまるのは2016年1月からの給与・支払に関する源泉徴収票・支払調書からになるため、現時点でも本格的なマイナンバー対応を終えていない企業は多い。2016年の源泉徴収票の提出期限である2017年1月末から逆算すると、遅くとも2016年10月にはマイナンバー対策を終えておく必要がある。これから夏にかけてが、マイナンバー商戦の最終ステージになるだろう。

ポイント

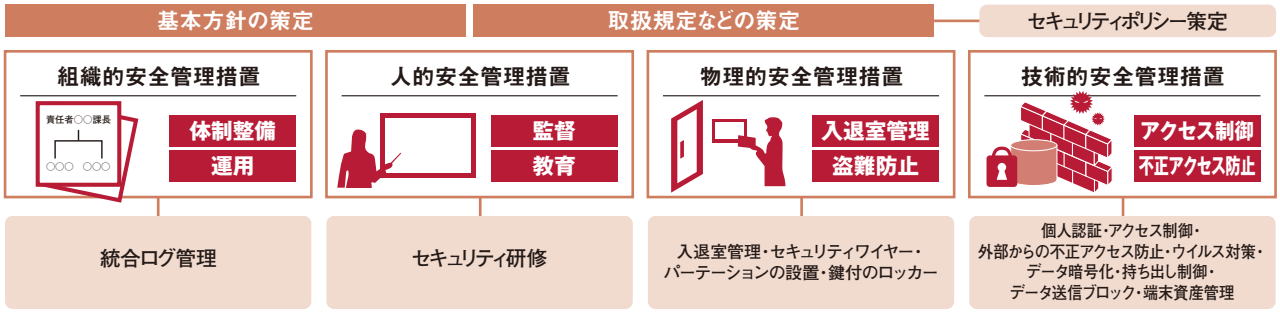
マイナンバー対応は、経営資源の強化にはつながらないと、エンドユーザー様の大部分はそう考えているはずだ。だがマイナンバー対策とは、運用ルールの策定や組織体制の整備を除けば、物理的・技術的という二つの側面からのセキュリティ対策にほかならない。企業を成長させていくうえで、より安全で使いやすいIT基盤の構築は避けて通れない課題だ。マイナンバー対策を単なる法令対応に終わらせるのではなく、むしろこの機会を利用し、求められるIT基盤の構築を図ることがエンドユーザー様にとって有意な投資になることは間違いない。こうした観点から、より積極的な提案を行いたい。

具体案

マイナンバー対策における安全管理措置は大きく、(a)物理的安全管理措置、(b)技術的安全管理措置の二つの方向から考えることができる。(a)物理的安全管理措置は特定個人情報(マイナンバー)を扱う区域を明確化し、その管理を行うサーバールームの入退室管理、マイナンバーを取り扱う事務を行う取扱区域を間仕切りで囲むなどの安全管理措置になる。サーバールームを持たない場合は、特定個人情報を管理するPCをセキュリティワイヤーで固定するか施錠できる場所に収納する必要がある。

(b)技術的安全管理措置においてまず求められるのは、電子データとして保管されるマイナンバーへのアクセス制御である。人事給与パッケージシステムの場合、マイナンバーへのアクセス権設定が機能に含まれることが一般的であるため、その利用によって最低限の対策をとることが可能だ。だがアクセスログ管理まで視野を広げるなら、Active Directoryによるドメイン環境のユーザー管理は有意義な提案になる。さらにネットワークの入口・内部・出口対策もあわせて提案することで、法令対応にとどまらないマイナンバー対策が可能になる。

ガイドラインが定める安全管理措置と具体的対策の関連



【営業提案2】e-文書法改正

3万円未満の要件緩和で現実的になった領収書の電子保管

紙による原本保持が義務づけられてきた文書や帳票の電子保管を容認する「e-文書法(電子帳簿保存法)」の施行は2005年4月のこと。これにより契約書から旅費・経費清算の領収書に至るオフィスの帳票類を電子保管することが可能になったが、数々の制約が課されたことで普及には至らなかった。特に電子保管が認められる領収書が3万円未満のものに限られたことは、大きな障壁になったに違いない。この制約により、領収書の電子保管に取り組もうとするエンドユーザー様は、領収額に応じ、2通りの業務フローを用意することが求められたからだ。

こうした状況を受け、2015年9月電子帳簿保存法が改正された。そのポイントは、①3万円未満という金額基準の廃止、②所轄税務署長の承認が不要に、③入力者の電子署名が不要に、④データサイズ等に関する規定の見直しの4点。金額基準の廃止が普及のスプリングボードになることは間違いないが、それと共に注目したいのが④データサイズ等の要件の見直しだ。これまで電子保管はフラットヘッドスキャナーによる読み取りが必須だったが、この要件が撤廃されたことで、スマートフォンで撮影したデータであっても必要な要件をそろえれば、電子保管データとして認められるようになった。

ポイント

電子保管の第一のメリットは、原本の輸送・保管コストが不要になる点にある。文書・帳票の保存に社外倉庫を利用するエンドユーザー様も少なくない。電子保管への移行によって、社外倉庫への原本の輸送費用が不要になるだけでなく、倉庫費用の減額が可能になる。二つ目は業務効率の向上である。社会人であれば、だれもが一度は経費精算時の領収書糊付けなどの手間に閉口した経験を持つはずだが、電子保管はその手間を不要にする。さらにスマートフォンによる撮影が認められたことで、領収書を随時破棄することも可能になった。もちろん管理部門によるデータ付け合わせの手間の大幅軽減もそのメリットの一つである。

具体案

領収書電子保管システムの実現には、電子承認システム、真正性を担保する電子スタンプ、文書管理システム、会計システムのe-文書対応を図ることが求められる。トータルソリューションの利用のほか、エンドユーザー様の既存環境をベースに不足する要素の補完によって対応することも可能だ。ワークフローツールを導入していないエンドユーザー様は、中小企業を中心に今も多い。領収書電子保管をテコとしてワークフローツールの導入まで含めた提案を行いたい。

電子帳簿保存法改正のポイント

	2015年9月30日までの施行規則	2015年9月30日以降の施行規則(要件緩和のポイント)
(1)対象書類の見直し	領収書や契約書のうち、額面が3万円未満のスキャナー保存が可能	金額基準を廃止 (領収書、契約書の全てをスキャナー保存の対象にすることができる) (内部統制を担保するための社内規定整備と適切な事務処理が必要)
(2)業務処理後に保存を行う場合の要件の見直し	関連帳簿の所轄税務署長による電子帳簿保存法の承認が必要	関連帳簿の電子帳簿保存法の承認は不要
(3)電子署名要件	・入力者の電子署名法に規定された電子署名が必要 ・タイムスタンプが必要	・入力者に関する情報の保存が必要 (ユーザーID等。電子署名法で規定された電子署名は不要) ・タイムスタンプは必要
(4)大きさ情報・カラー保存要件の見直し	・大きさ情報の保存が必要 ・カラー画像での保存が必要	・大きさ情報の保存不要 ・カラーもしくはグレースケール

表:電子帳簿保存法の新施行規則で示されたe-文書法規制緩和のポイント(2015年3月31日官報)

【営業提案 3】ストレスチェックの義務化

コンサルティングからデバイス販売まで ビジネスチャンスは幅広い

労働安全衛生法の改正により、2015年12月以降、従業員50名以上の事業所では年1回ストレスチェックを実施することが義務づけられた。ストレスチェックとは、一口で言うなら従業員が自分のストレスの状態を知るための制度。ストレスが高い場合、医師との面談や、会社に仕事の軽減などの措置を実施してもらうことで、メンタルヘルス不調を未然に防ぐことがその目的になる。具体的にはストレスに関する質問票への回答にもとづき、医師などの実施者がストレスの程度をチェックする。

ポイント

注目を促したいのは、ストレスチェック結果は従業員のプライバシーに関する情報と位置づけられる点だ。ストレスチェック結果は実施者（医師）から従業員に直接伝えられるが、そのプロセスにおいて企業が情報を保管する必要が生じることは否めない。法律では、事業者が従業員のストレスチェック結果を不正に入手することを禁じると共に、ストレスチェック・面接指導に関わった者には守秘義務が課され、違反した場合は刑罰の対象になる。さらに面接指導を実施した場合、その記録は事業所で5年間保存することが求められるため、「ストレスチェック結果の管理はマイナンバー以上に難しい」という声もあがっている。

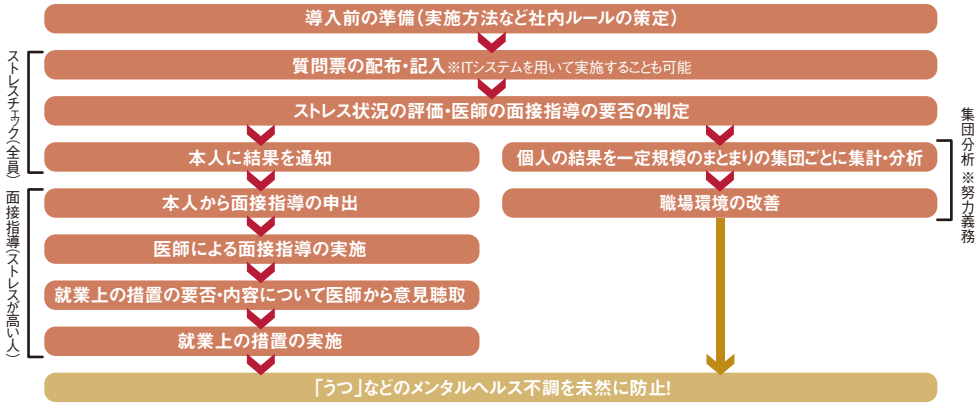
具体案

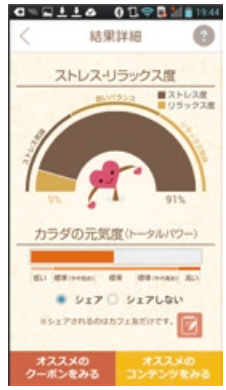
ストレスチェックは、ITシステムによって行うことも認められている。厚生労働省が無料で公開する「ストレスチェック実施プログラム」を利用すれば、ネットワーク上で行うことが可能だ。だがこの場合も、そこで得られた情報をどう管理していくかという部分で知恵が必要になる。ストレスチェック商戦の第一の商機は、こうした部分におけるコンサルティングということができるだろう。

なお質問とその回答を管理するシステムは、そのままeラーニングシステムに転用することも可能だ。実際、ASP型ストレスチェックサービスの利用事例の中には、その仕組みを双方向型の従業員教育に活用するエンドユーザー様も目立つ。ストレスチェック義務化は、eラーニングニーズの掘り起こしにも利用できるだろう。

メンタルヘルスへの関心の高まりを機器販売につなげるという方向性も考えられる。例えば指先の心電と脈波を同時に計測・解析し、疲労・ストレスの度合いを計測するデバイスは、ストレスチェックを補完するものになる。医療・介護業界など、職員・従業員のメンタルヘルス管理に積極的なエンドユーザー様にはこれらのツールも積極的に提案していきたい。

ストレスチェック制度の実施手順





ストレスを数値化するアプリ・デバイスも多数登場している。写真はスマホのカメラに指を置くだけでストレスを計測するアプリ「COCOLOLO」。

IT Keyword
最新ITキーワード

電力自由化
【The liberalization of electricity retail sales】

2016年4月から、いよいよ始まった電力小売の全面自由化。電力自由化で新たに約8兆円という市場が開放された。大手企業のみならず、中小企業や異業種、そしてITベンダーにも参入のチャンスが拡がっている。

これまで家庭や商店向けの電気は、地域の電力会社（東京電力、関西電力等）だけが販売していた。2016年4月1日以降は、電気の小売業への参入が全面自由化されることにより、消費者が電力会社や料金メニューを自由に選択できるようになった。そしてこの電力自由化が大きなビジネスチャンスだと言われている。巨大なマーケットの門戸が一気に開かれたからだ。低圧部門（一般家庭、小規模事業者）の電力小売だけで約8兆円であり、既に自由化されている特別高圧・高圧部門（工場、商業施設など）も含めると約15兆円に上る。その上、電力の需要がなくなることはなく、一度契約すれば長期に渡って売上を見込むことができる分野だ。

電力小売には現在までに279事業者（2016年4月7日時点）が登録しており、今後も増えていくことが予想される。参入事業者が増えることで競争が活性化し、様々な料金メニュー・サービスが期待されている。例えば電気とガス、電気と携帯電話などの組み合わせによるセット割引やポイントサービス、さらには家庭の省エネ診断サービスなどだ。

新規参入の戦略は2つある。ひとつは「創意工夫で徹底的に電気料金を下げる」こと。電力会社からのまとめ買いで安く電力を調達し、工場の余剰電力なども活用して電力を安価に販売する。そうやって得た資金を使って、太陽光や風力、水力、地熱、バイオマスなどの再生可能エネルギーの発電設備を整備することも可能だ。しかし競争は激しく、新規参入会社が電力単体で採算を上げることは並大抵のことではない。

そこで「自社のコアビジネスに電力小売事業を組み込んで、価格競争に陥りにくい付加価値サービスを創造する」という第2の戦略が考えられる。例えば、自治体やクレジットカード会社、ケーブルテレビ会社など、一般家庭の口座情報を持つ事業者が既存商品と一緒に電力も売るケースや、ドラックストア、コンビニ、家電量販店、カーディーラーなど、一般家庭に直接販売する事業者がコア商品とセットで電力を売るというケースがある。同時契約であれば割引やクーポンを発行するなど、インセンティブを付ける戦略も考えられるだろう。その他にも、HEMS※の電力使用データを使った高齢者見守りやホームセキュリティ、家電メンテナンスなどのサービスで市場参入することもできる。そうした事業者にビジネスアイデアを提供するコンサルも成り立つ。可能性は無限にあり、企業規模を問わずビジネスチャンスが生まれている。

ユニークな具体例を挙げると、地方の複数の中小スーパーと提携して、スーパーの顧客向けに電力を小売する会社がある。スーパーの買い物に使えるポイントが電力料金に応じて付与される。スーパーにとっては代理店手数料をもらえると同時に、ポイントによって顧客を囲い込めるというメリットがある。

こうした新電力参入の拡がりは、ITベンダーにとっても大きなチャンスだ。現行制度では事業者は供給先の需要にあわせて、電力供給量を30分単位で一致させなければならない。供給先の電力の使い方や、天候・時間による需要の変化を正確に見極めることが事業収益を左右するため、需給管理が大切だ。これに加え、顧客情報の管理、多様なメニューに合わせた料金計算や請求書発行、スマートメーターの情報収集・管理、顧客ポータルやコールセンターまで、事業者の参入を手助けするITプラットフォームサービスの市場はますます活性化していくだろう。そのIT投資規模は1,000億円とも言われている。電力自由化は始まったばかりだ。軌道に乗るまで様子見をしている事業者は多い。そこにビジネスチャンスが拡がっている。BP

※Home Energy Management System：ホーム エネルギー マネジメント システム