Hitachi Solutions
［日立ソリューションズ情報誌］
Hitachi Solutions Information magazine

REVIEW

HITACHI
Inspire the Next

2011
vol. 2

［特集］
情報セキュリティー

株式会社 日立ソリューションズ

［特集］情報セキュリティー

情報システムは、常にデータの盗難、不正アクセス、改ざん、漏えい、破壊などさまざまな脅威にさらされている。新しい情報技術が現れると同時に、新たなセキュリティーの脅威も生まれる。

すべての脅威を完璧に防御することは困難だが、新たな脅威が発生した時に、迅速に対応し、被害の拡散を抑止する対策をシステム的に構築することは不可能ではない。これまで以上に安心・安全が求められる時代。

本号の特集では、情報セキュリティーについての基本的な対策と、日立ソリューションズが提供するセキュリティソリューションの全体像を紹介する。

Special Interview
Kuniyoshi Shirai

企業はセキュリティー・リスクにどう立ち向かうべきか

白井 邦芳 氏
ACEコンサルティング株式会社
エグゼクティブ・アドバイザー　危機管理コンサルタント
リスクマネジメント協会評議員　日本法科学技術学会正会員

安心・安全が今ほど重要視される時代はない。さまざまな危機の前に、企業のセキュリティー・マネジメントも絶えず見直しが必要だ。個人情報漏えい対策などに詳しい、危機管理コンサルタント・白井邦芳氏に、これからの時代のセキュリティー対策の基本について伺った。

ソーシャル・ネットワークが新たな漏えいルートに

個人情報の漏えいや、企業内の不祥事などに対して、基本的にはどういう考え方で取り組めばよいのかを伺っていきます。まず、企業のセキュリティーを巡る状況について、最近注目されていることは何かありますか。

最近感じるのは、SNSやTwitterなどネットワーク・メディアが新たな情報漏えいのルートになってきたということですね。「アルバイトをしているお店に今日、こんな有名人が来店したよ」と気軽にツィートしてしまう。そのツィートは誰もが見られる状態にあることを、つい失念してしまうのです。会社の機密情報やお客様の個人情報が、こうしたルートから漏れていくということに注意を促したいと思います。

もう一方で、クレジットカードの番号の規則性を悪用し、カード番号にある計算を加えて他人のカード番号を割り出す「クレジットマスター」という手口が、最近再び目立っています。

クレジットマスターにはPCや高度なITは必要ない。コンピューターの技術やネットワークの技術を利用するのではなく、企業の機密情報などを物理的あるいは心理的な手段で獲得することを、ソーシャル・エンジニアリングと言いますが、こうした昔からの犯罪もいまだ根絶していないということにも注意を喚起しておきたいと思います。

物理的・心理的な方法で言えば、会社の中にお客様のフリをして侵入して、会議を盗み聴きするとか、会議の後の資料を奪うとか、通常では考えられない様なケースも実際に起こっています。

100人入る会議室があって、そこに２つの入り口があったとします。ドアが１つであれば入退室をチェックできるのですが、２カ所だとそれが難しい。実際にその部屋に外部の人間が侵入して、配布資料が持ち出され、マスコミに漏れたケースがあります。

あるいは企業で重大な不祥事が起きると対策本部が出来ます。その本部が誰もが聞き耳を立てれば中の物音が聞こえる様な部屋にあったとすれば、そこで大きな声で怒鳴り合ったりすると、それ自体が新たな不安材料として外部に漏れるかもしれません。

重要会議を行う会議室の場所一つ取っても、実は慎重に設定しなければならないのです。誰もがその前を通れる様な所で、重要な会議を開くべきではありません。あるいは対面にビルがあって

そこが見通せるような窓がある部屋も要注意。望遠カメラで撮影されてしまう可能性も皆無ではありませんから。こうした会議では、会議資料も高度な機密情報になりますから、基本的にはその場でシュレッダーにかけて廃棄すべきでしょう。機密情報の扱いには、このくらい神経質にならないといけない訳です。

ホームページやインターネット上のデータ・ストレージサービスにも盲点

機密情報が漏れるケースでは、組織内の人物の関与を疑わざるをえない場合も多いですね。

組織内の人物が犯人である場合、一般的にはデータにアクセスしてPCにダウンロードする訳ですが、そのとき自分のPCなんて絶対に使わないですよね。すぐばれてしまいますから。そこで、他人のPC、他人のパスワードでダウンロードする。

ダウンロードボタンを押した瞬間に、室内の警備カメラが押した人の写真を撮り、それとアクセス権限者を照合するというぐらいの高度なセキュリティーシステムを導入しない限り、現行犯逮捕は難しいでしょうね。

ソーシャル・エンジニアリングの話がありましたが、IT分野でのセキュリティー状況はいかがでしょうか。

例えばホームページ上でユーザーに会員登録をしてもらい、そのデータを個人情報として保管している企業は多いと思うのですが、そのセキュリティーも盲点の一つになっています。登録された情報を本来はすぐに完全に外と切り離したサーバーに入れ直して、ホームページ上の情報を消去すべきですが、それができていない。外から閲覧できる状態のままになっている。こうしたホームページ上のセキュリティーについては、経済産業省などでもかなり危機感を持っています。海外のハッカーたちに狙われているというんですね。

また、いま一時的なデータの保管場所として便利に使われている、インターネット上のデータ・ストレージサービス。これも、情報漏えいのルートになる可能性があります。USBによる持ち出しについてはかなり厳しくなりましたが、こうしたデータ・ストレージサービスの利用については、まだ十分な対策が取られているとはいえません。昔なら数ギガバイト単位でしたけれど、今は100ギガバイト以上保存できる様なサービスも多いですから、持ち出されるデータ量もそれだけ増えています。

メールの扱いがずさんであったため、そこから重要データが漏れるという事もよくあります。たくさんの人に、CCやBCCで送信するときに、関係のない人を間違って追加してしまい、そこが漏えいルートになるケースとかですね。添付ファイルの扱いにも無頓着な企業はまだ多いですよ。

事実確認、原因究明の「初動」に失敗すると命取り

こうしたもろもろのリスクに対して、企業の対応は進んでいますか。

個人情報、機密情報が漏えいしましたよということを、犯人がわざわざ言ってくれるはずもありません。問題なのは、漏えいした事実を企業が知らないままで過ごし、被害者など外部からの指摘で初めて気づくケースです。これが意外と多いのです。

企業が被害に早く気づけば、原因の特定も早くなり、被害が大きくなる前に食い止めることができます。しかし漏えい事実の認知に手間取ると、それだけ被害も拡大してしまいます。

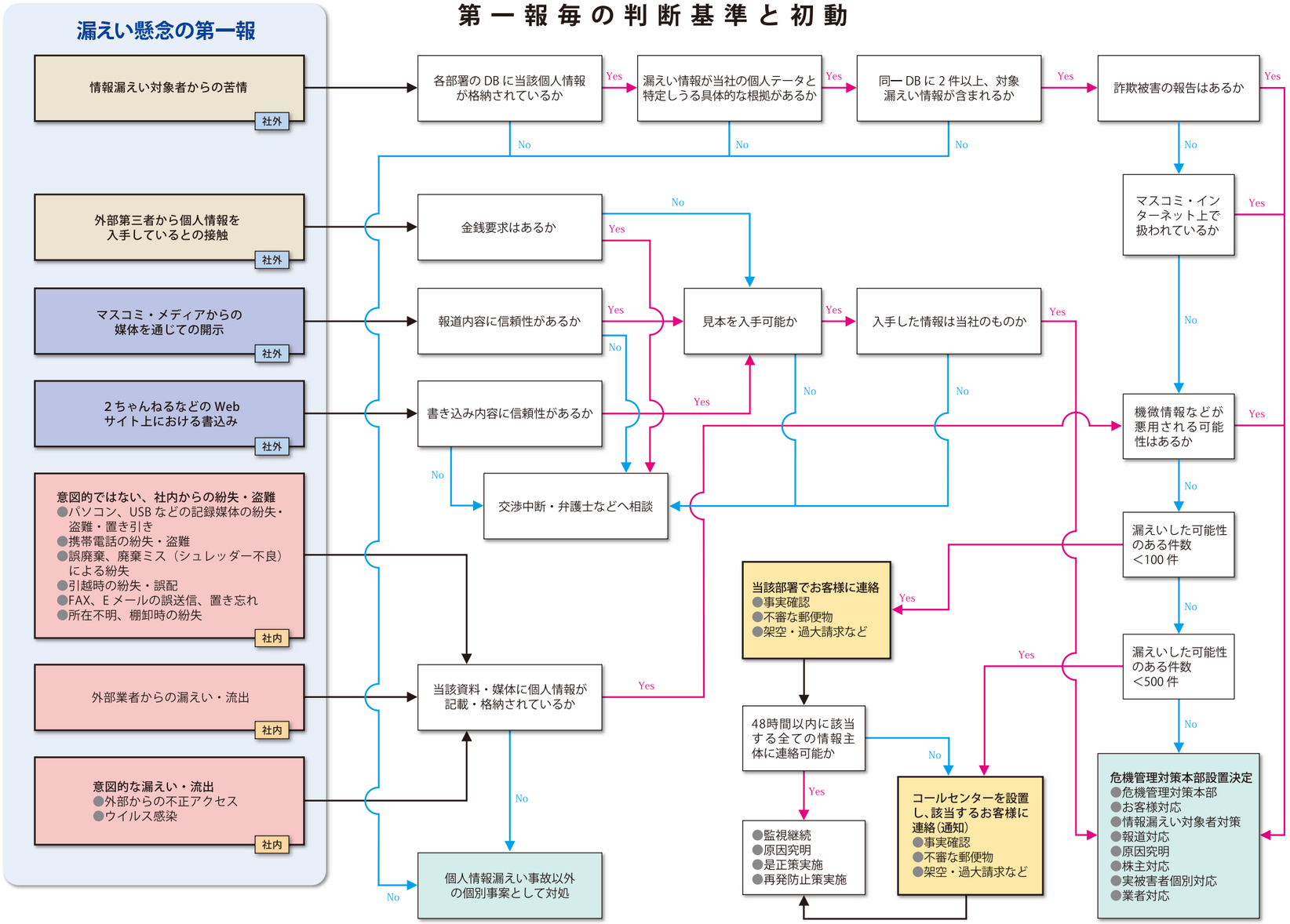
原因がわからないまま、例えば100人以上の人間を社内外で捕まえてきて、一人ひとりにインタビューを３回も４回もやって、結局わかりませんでしたというのでは、社内の人間関係もずたずたになってしまいますね。犯罪者は中にいたかもしれないし、外部かも知れない。こうした疑心暗鬼のままに業務を継続するのでは、ステークホルダーの信頼も失ってしまいます。

いくら個人情報保護法や不正競争防止法に則って「私たち頑張ってました」と言ったところで、被害が広がれば、最終的には「やっていなかったから、こういう事が起きたんでしょう」ということになってしまい、最悪の場合、行政から改善命令が出てしまいます。やはり、いかに早く事象を認知するか、原因を特定するかが重要になります。

原因の特定や被害の広がりの想定ができていないまま「現時点ではこのレベルですよ」と軽く発表したところ、後で被害が２次、３次と広がってしまって取り返しがつかなくなったケースもあります。

ただ、発表しなかったと後で言われるよりも、とりあえず発表することの方が良いというような考え方もありますね。

発表の仕方が重要です。漏えい事実の発表の第一報は、一般的に72時間以内がベターだといわれています。そこでまずどういう情報が漏えいしたのかを言わなくてはいけない。社内なのか社外なのか、原因究明中なのか、わからないことは調査していると言えばよい訳です。その上で、漏えいは最大どの位の件数になる可能性があるかを表明する。まず確認できた件数と最大の予想件数を並べて発表するという事が、個人情報漏えい事件の企業広報では重要で、それが定番となっています。



一般に漏えい事件の危機管理対策としては、事実確認、原因究明、責任の表明、是正、さらに再発防止策の策定、その監査があって、最終的には安全宣言という流れになります。これを順番に行い、それぞれのステージごとにHPなどでも随時状況を開示し、途中では専門家も入れてプロセスをきちんと実行することが重要です。

漏えい対策はステークホルダーマネジメントが基本ですから、法務部門やお客様相談室や広報部門だけに対応を任せるのではなく、経営企画もシステム部も、ありとあらゆる所が全部動くということが大切です。問題が同時多発的に発生すると、こういった流れが全部必要になってくるんですね。

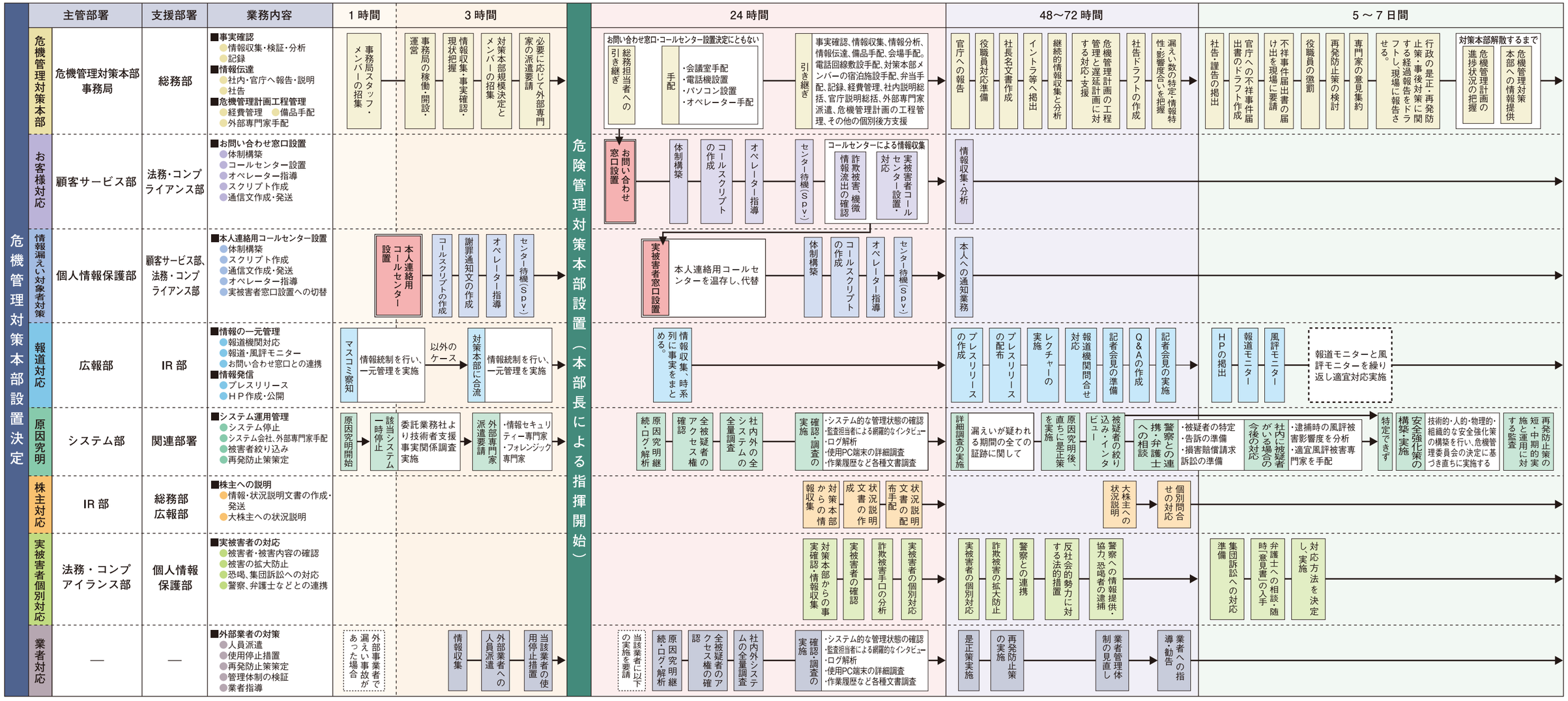
情報漏えい事件は過去においてもそうだったのですが、発生してから安全宣言までに最短で２カ月。大抵はその処理に６カ月かかります。逆に言えば、半年かかっても安全宣言を出せなければ、その会社は問題だということになるのです。最悪の場合、事業を停止せざるをえなくなったり、経営者が退陣に追い込まれたりするなど、膨大な損害を被る事になります。

災害訓練と同様に、個人情報漏えいでも、日頃から被害をシミュレーションして、それに対応する訓練を行う必要がありますね。

シミュレーションと訓練は極めて重要です。わたしたちでもそのためのトレーニング・マニュアルを作成して、企業にコンサルティングをしていますが、対応の手順は１から40ぐらいまであります。大量の個人情報を抱える企業の中には、少なくとも年に１回程度はこうしたトレーニングを実施しているところが最近は増えてきました。

個人情報漏えいでは、実際のところ、原因がなかなか究明できない事が多いのです。いつ頃どのぐらいの情報をど

情報漏えい事件におけるＢＣＰ展開図



ういう形で盗まれたかというのは、専門業者の助けを借りないとなかなか確定できません。これが確定して初めて、今後の対策が打てる訳ですが、大切なのはまずは情報主体、情報の対象者にお詫びすることです。

次に、その情報がどんな二次被害をもたらすかということを予想して、それに対応したチームを組織することが必要です。個人情報漏えいが怖いのは、それが複数の犯罪集団の間でやりとりされ、そこから詐欺などの新しい被害が発生することです。

その対策チームには、社会に対してリスクを告知しお詫びする担当と、実際の二次被害のクレームに対してきちんと対応する担当を置かなければなりません。時には損害賠償など法的な対応が必要になることもありうるので、弁護士などの専門家を参加させるべきでしょう。

こうした体制づくりは事件が発生してから準備しても遅い訳です。マスコミ対応なども含めて日頃から準備し、事故発生を想定した訓練を重ねておかないと、とっさのときに動けなくなります。

セキュリティー強化と業務効率化を両立するツールが必要

セキュリティーホールを突く手法は時々刻々と新手のものが登場しています。事態に絶えず対応していくことが欠かせませんね。

セキュリティーというのは絶対に大丈夫ということがありえない世界です。ですから、事象が発生したことをどれだけ早く認知するか、認知した後、どういうふうにそれを対応するかがやはり重要なポイントです。早急な認知のためには、何らかのツールが必要です。

特にIDS（侵入検知システム）の様なものは当然必要でしょうね。また、メールの使用にあたっては、特定の情報量以上のサイズのデータは原則として外側へ配信してはならない、という仕掛けなども場合によっては必要でしょう。もちろん、そんなことをしたら業務が止まってしまうという会社もあるでしょうから、仕事の効率とセキュリティー強化のバランスをどう担保するか、そのためにも、ITの力が必要になると思います。

事業継続的な観点からの震災対策、震災から情報を守るためには

先般の大震災のことですが、企業のリスクマネジメントの観点からはどのようにお感じですか。

今回の震災のような未曾有の災害を、BCP（事業継続計画）の観点から見ると、事業を一時停止して撤退することも選択肢の一つとして考えなければなりません。ただ、従業員を緊急に避難させる場合でも、セキュリティー機能が止まることを前提にして、データを持ち出しておくなどの対策を取る必要があります。

事態が安定してオフィスに戻ったら、情報を盗み出されていた場合には、被害も大きくなりかねない上、企業としての管理のあり方を厳しく問われることになります。

Kuniyoshi Shirai

【プロフィール】**しらい くによし**

危機管理コンサルタント。リスクマネジメント協会評議員、日本法科学技術学会正会員、経営戦略研究所外部専門委員。ACE Consulting Inc. エグゼクティブ・アドバイザー。数度の米国駐在を経て、企業不祥事、役員訴訟、異物混入、情報漏えい、テロなどの危機管理コンサルティングに多数かかわる。これまでに手がけた事例は2350件以上にのぼり、その分野は危機管理、リスクマネジメント、コンプライアンス、内部統制、事業継続、企業再生・価値向上などの専門家として広い分野で活躍の場を広げている。著書には『ケーススタディ企業の危機管理コンサルティング』『循環取引対策マニュアル』（いずれも中央経済社）などがあり、企業の危機・戦略・CSR関連で幅広い執筆活動を行う。

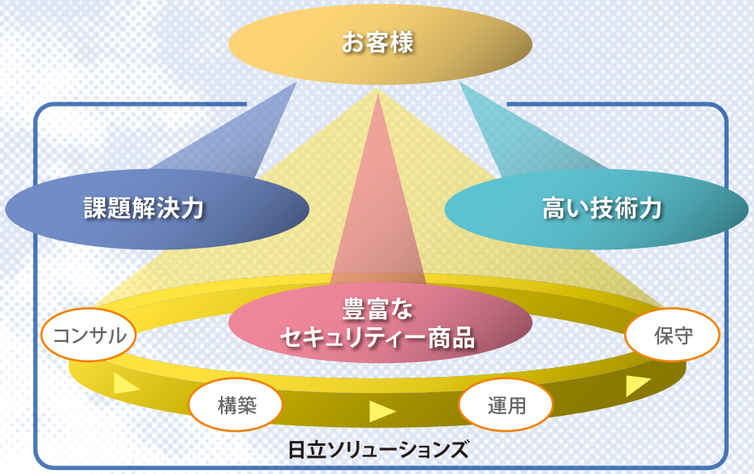
ACEコンサルティング株式会社
http://www.acec.co.jp/

『ケーススタディ 企業の危機管理コンサルティング』
白井邦芳・著
中央経済社・発行
定価:3,150円

［注目ソリューション］
セキュリティソリューション

ネットワーク・情報セキュリティーの課題を技術力とコンサルティング力で解決

セキュリティソリューションイメージ図



2010年10月に日立ソフトと日立システムが合併して日立ソリューションズが誕生して半年、互いの強みを活かし補完することで、新たな価値を創造しうる組織づくりが完了した。

セキュリティー分野では、2011年４月に発足した「システムプラットフォーム事業部」がそれにあたる。

異なる強みが合わさることで生まれるシナジー効果

この４月に誕生した「システムプラットフォーム事業部」は部員数約500名、パートナー会社をいれると約1,000名の体制で、情報セキュリティーやネットワークセキュリティーといった「セキュリティソリューション」を中心に展開している。社会環境の変化から、お客様の課題を探し出し、そのニーズに合ったプロダクト・パッケージおよびソリューションを提供していく。

旧日立ソフトと旧日立システムが、それぞれ培ってきたプロダクトやソリューションの強みが、一つにまとまることでの相乗効果が大いに期待されているところだ。

「日立ソフトと日立システムは互いに独自のカラー、ビジネスモデルを持っていたと思うのです」と語るのはプラットフォームプロダクト本部長の臼杵誠剛。

臼杵によれば日立ソフトは自社製品にこだわるモノづくりの会社。世の中の状況、市場動向をとらえシーズをもとに他社に先駆けてプロダクトを先行開発し、それをお客様に合ったソリューションという形にして販売していくというビジネスモデルだと言う。

一方、日立システムはお客様が何を欲しているかというニーズをとらえ、その要望を満たす製品やソリューションを提供するというビジネスモデルを持つ企業だったというのが臼杵の見解だ。

「つまり異なる持ち味、強みを持つ両者が一緒になり、豊富なシーズとニーズをとらえる強い力が結びついて、1＋1=2ではなく、1＋1=3以上にしていける。そんな日立ソリューションズの方向性がはっきり表れているのが『セキュリティソリューション』ではないかと思います」と臼杵は力強く語る。

情報漏えいにも外からの攻撃にも対処できるプロダクトライン

クライアントPCなどのセキュリティーで強みを発揮するのは、自社開発の製品群だ。持ち出し・印刷制御、イントラネットの情報漏えい防止、不正ユーザーのネットワーク遮断などさまざまなリスクに対応する情報漏えい防止ソリューション『秘文』。指静脈認証による厳密な本人認証を実現したシステム『静紋』や情報の持ち出し先での閲覧制限などドキュメントの統制と活用が可能な『活文』などがそれだ。

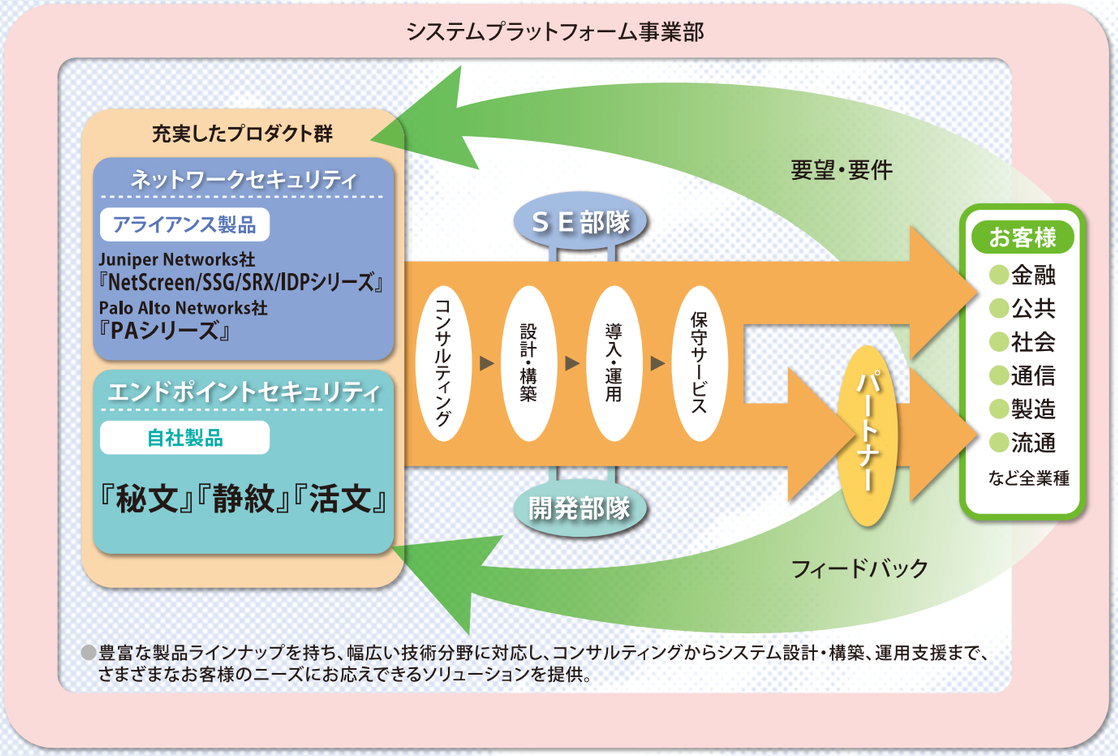
『秘文』は、国内企業5,700社605万ライセンスの導入実績を誇り(2011年３月末時点)、持ち出し制御やファイル暗号化ソフトウェアで国内シェア１位(2010年度富士キメラ総研調べ)に輝いている。

ネットワークセキュリティで力を発揮するのは、当社が国内のディストリビューターとしてNo.1売上を誇っているJuniper Networks社の『NetScreen/SSG/SRX/IDPシリーズ』やPalo Alto Networks社の『PAシリーズ』といったハードウェアを含めたアライアンス製品だ。『NetScreen/SSG/SRX/IDPシリーズ』は、UTM(統合型脅威管理)、IDS/IPS(不正侵入検知／防御)機能などを擁するファイアウォール、トラフィック制御機能などを擁するインターネットセキュリティー機器のシリーズだ。

このようにセキュリティーにおける新事業部のプロダクトの守備範囲は大きく広がっている。内部からの漏えいを防ぐセキュリティーと外部の攻撃から守るセキュリティーを合わせることで、十二分に対応できる。

「充実した多様なプロダクトの特長をとらえ、最適なソリューションを提供していける体制になりました」と語るのはセキュリティソリューション部長の宇佐見憲司郎だ。

セキュリティソリューション展開図



拡充されたソリューション部隊がニーズを広げる

これまでも、コンサルティングや設計、導入、運用・保守に至るまでのシステムインテグレーションに強みを発揮してきたが、今回の新事業部発足によって開発部隊、SE部隊ともに強化され、より充実したソリューションを実現できる体制が整った。

つまり要件分析・定義、仕様決定から始まり、製品導入、保守サービスまでを一貫したワンストップソリューションが提供できるというわけだ。

「お客様側からするとセキュリティー対策といっても、何をすべきかは必ずしも明確ではありません。情報漏えいを防止したい場合も、メールから漏れることを避けたいのか、媒体からは絶対に漏れないようにしたいのかが、はっきりしない場合も多いのです。そこでお客様に話しを伺い、本来のニーズを理解した上で、それぞれのケースにあったソリューションを展開していきたいですね」と宇佐見は抱負を語る。

臼杵も拡充されたソリューション部門による効果に期待を寄せる。

「『セキュリティソリューション』はお客様の状況をヒアリングしながら確認し、それに合わせて提案していくものなので、SEが数多く揃っていること自体が強みになります。コンサルティングから始まり、システム構築するSEがいて、初めて成り立つ。お客様にわかりやすくソリューションを提案していくSEの役割が特に重要ですね」

自社製品の強みである情報漏えい防止を中心としたプロダクトとアライアンス製品である外部からの攻撃に対処するセキュリティーを中心としたプロダクトの2つをコアに、拡充した開発部隊とSE部隊によるソリューションを合わせてシステムプラットフォームの事業は展開していくことになる。

CISSP(情報セキュリティ・プロフェッショナル認証資格)、CISA(公認情報システム監査人)技術者も有している。

ワンストップサービスを展開する６つのテクニカルソリューション

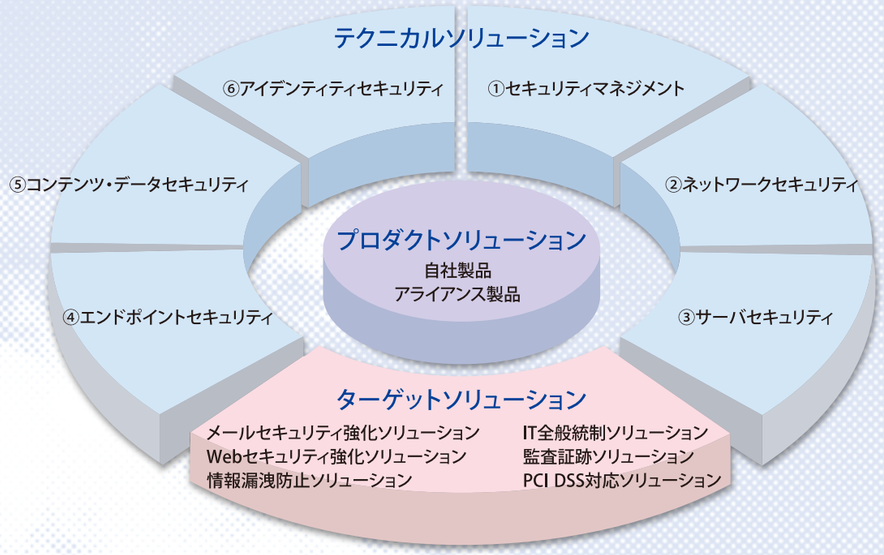
「セキュリティソリューション」を展開するのは、６項目にカテゴライズされたテクニカルソリューションだ。

①情報セキュリティーのコンサルティングやマネジメントサービスを行う「セキュリティマネジメント」
②攻撃者からサーバーやネットワークを守る「ネットワークセキュリティ」
③サーバーへの不正アクセスなどを防ぎ業務システムのセキュリティー強化を行う「サーバセキュリティ」
④PCの不正操作抑止やウイルス対策などエンドポイントを取り巻く問題を解決する「エンドポイントセキュリティ」
⑤社内の重要データの不正持ち出しといった情報漏えいを防ぐ「コンテンツ・データセキュリティ」
⑥統合認証基盤システムを提供する「アイデンティティセキュリティ」だ。

それぞれの項目ごとにコンサルティングから設計、導入、運用などセキュリティー対策に関するサービスメニューを揃えている。

「プラットフォームプロダクト本部でコアとなるプロダクトをより充実させて中心部の円を大きくし、プラットフォームソリューション本部でソリューション展開を進めて外側の円を大きくしていく。これがシステムプラットフォーム事業部が目指すことと言えるでしょう」と臼杵は語る。

システムプラットフォーム事業部が展開するソリューション



コンテンツの承認機能でビジネスの現場のニーズに対応

合併によるシナジー効果を活かしながらシステムプラットフォーム事業部は今後、具体的にはどんな分野に注目しセキュリティービジネスを展開していくのだろうか。

プロダクトで最近ニーズが高まっているのが社外に持ち出すデータに対して重要度に応じた持ち出し制御機能を提供する新DLP（Data Loss Prevention）という概念だ。

「ウィキリークス事件をはじめ、内部の人間による情報漏えいが増えてきた中で、セキュリティーの重要性は広く認識され、セキュリティー対策もごく一般的に取られるようになってきました。しかしセキュリティーが厳重だと、現場の業務の効率が落ちるというトレードオフも問題になりつつあります」と臼杵はセキュリティーへの企業側のニーズの変化を語る。

例えば製品紹介資料のように外に出ても問題のない文書を持ち出す際にも、いちいち上長の許可をもらって、コピーしてとなると、現場にはかなりの負荷が掛かってしまう。ビジネスの効率も大幅に落ちる。そこで、セキュリティーを守りつつも、データを重要度に応じランク分けして、社外への持ち出しに対してより柔軟な運用を可能にするのが新DLPなのだという。それを実現するプロダクト群の一つに『ContentsGate』がある。

『ContentsGate』はすべてのファイル種別について持ち出し可否の制御ができる。非常に重要なコンテンツは上長がその場で承認しない限り取り出すことはできないが、一方重要度の低いコンテンツの場合は本人の判断で外に持ち出すことが可能だ。ただし上長に通報が入り、履歴が残るので、社員側もコンテンツの外部への持ち出しに対しては自然と慎重になる。また、社員本人の判断での持ち出し可能なコンテンツであっても会社指定の安全なUSBメモリしか使用できないなど、それぞれの状況に応じた細かな設定ができるのが特長だ。

「セキュリティーへの対応が広がるにつれ、これからはそれぞれの会社が必要とするレベルに応じたセキュリティー機能が求められてきています。コンテンツの重要度に合わせて柔軟に運用できるといった仕組みへのニーズは今後さらに高まっていくと考えられます」（臼杵）。

クレジットカードの基準PCI DSSに向けたソリューション

2010年、最新バージョンが公表され、ソリューションの面でニーズが高まっているのはPCI DSS対応関連だ。PCI DSSとは国際クレジットカードブランド数社が協同で設けたセキュリティーのための基準で、現在、国際カードブランド会社が期限を切って加盟店に対し準拠することを求めている。このため、大手加盟店や決済代行会社が本格的に対応準備を進めている状況だ。

PCI DSSの規格は12要件にわたる。"カード会員データを保護するために、ファイアウォールをインストールして構成を維持すること""オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化すること"など、その内容は非常に細かく規定されている。

「実装面も指定されており、PCI DSSに対応するためには複数のプロダクトを組み合わせていく必要があります。私たちはコンサルテイングから始まって実際の設計、構築、導入までの一貫したソリューションをご提供できるのが強みですね」と宇佐見は語る。

また「アイデンティティセキュリティ」の分野では複数のシステムに散在するIDやアクセス権限やパスワードを一元化するといったID管理や高いセキュリティーを追求した認証強化など、ビジネスにおける利便性とセキュリティーを両立させるようなシステムのニーズが高まっていると言う。

プロダクト，SE技術者のグローバル展開も

さらに今後のビジネスでは、グローバル展開も視野に入れていくと言う。

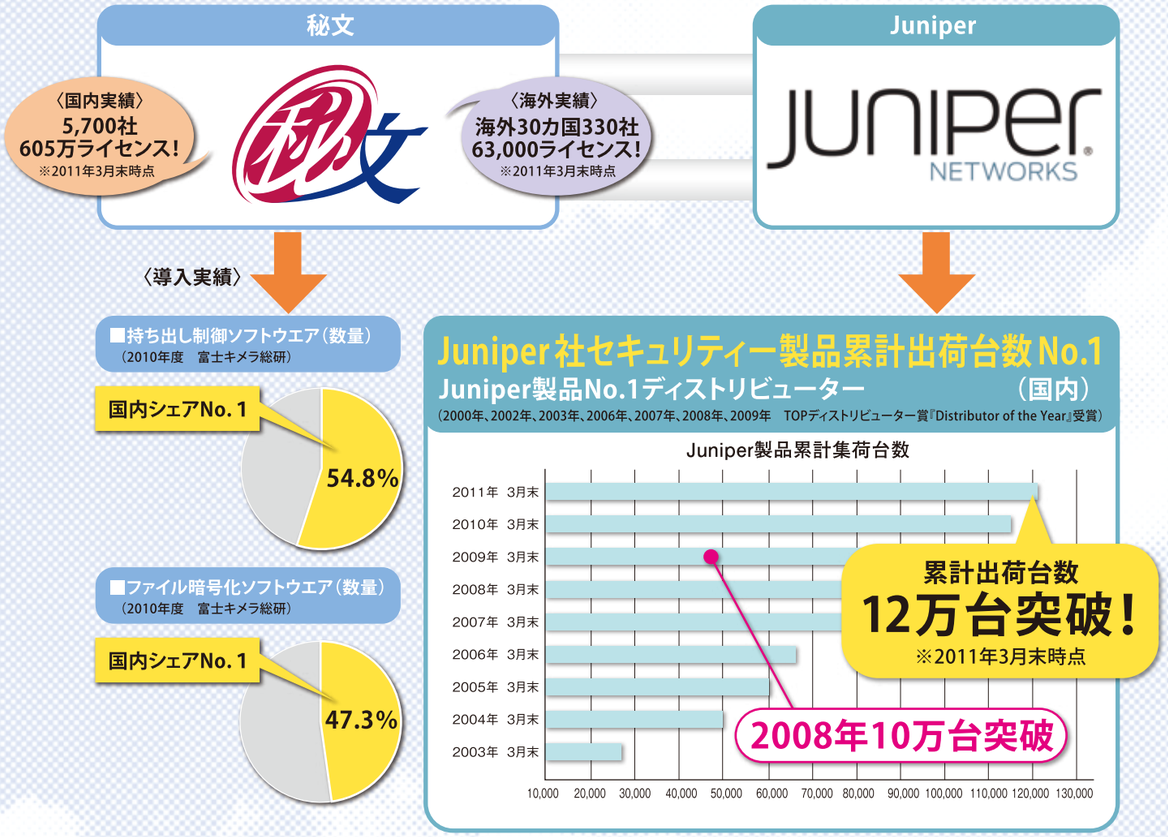
「すでに自社製品のプロダクトを海外でも販売していますが、今後はグローバルを念頭に置いたプロダクトを開発し、市場規模の大きな北米市場にまずは投入していく計画です。ただ日本製品が一番売れるのは東南アジアであるだろうと想定はしています。北米で海外ベンダーと競い合って、鍛えられながら東南アジアに向かっていくという戦略です」（臼杵）

海外で日立ソリューションズのソフトウェアが利用されるようになれば、当然各国のパートナーの支援も必要となり、将来はプロダクトと共に同社のSE技術者も海外に出ていくことになるだろうと言う。

グローバル化が進む日本の産業界だが、日本製のソフトウェア・プロダクトや日本人のSE技術者が本格的に海を渡る日も、すぐそこに迫っているのかもしれない。

旧日立ソフト、旧日立システムの異なった強味が融合したシステムプラットフォーム事業部。自社製品とアライアンス製品、ソフトウェアとハードウェア、内側からと外側からのセキュリティーが融合した広範囲な「セキュリティソリューション」を、グローバルに展開していく。

システムプラットフォーム事業部の主力製品『秘文』『Juniper』



システムプラットフォーム事業部
プラットフォームプロダクト本部
本部長
臼杵誠剛
Seigo Usuki

システムプラットフォーム事業部
プラットフォームソリューション本部
セキュリティソリューション部
部長
宇佐見憲司郎
Kenshiro Usami

CaseStudy　株式会社三菱東京UFJ銀行

『SenSage』導入によりセキュリティーの強化とともにログ収集・分析作業時間の短縮も実現

企業の情報セキュリティー意識は高まっているが、社内データへのアクセスログーつとっても、収集はしているが分析・解析まで手が回らないという企業は少なくない。日立ソリューションズの統合ログ管理ソリューション『SenSage』を例に、企業セキュリティーの最前線をみる。

サーバーごとに分散されていたログを『SenSage』で集約し一括管理・分析

個人情報保護法、金融商品取引法、新会社法の施行などに伴い、企業のセキュリティー対策、コンプライアンスへの対応は意識の高まりとともに対策の導入が進んでいる。その中で内部犯行による情報漏えい、巧妙化する不正アクセスにどう対応するかも大きなテーマだ。企業の内部統制を実効性のあるものにするため、ログデータを収集、分析、保管するソリューションが求められている。『SenSage』はその強力なアーキテクチャーにより、ログの監視、ライフサイクル管理を低コストで実現するソリューションだ。

『SenSage』は200種類のログフォーマット対応、独自の圧縮機能によるテラバイトクラスのログデータの長期保管、150種類以上のレポートテンプレートを備えたログ管理製品。ネットワーク機器のみならず、サーバーのOSログ、DBログなど多様なログを収集することができる。

すでに金融機関など大手企業での導入実績があるが、その一つが三菱東京UFJ銀行の法人企画部 法人基盤企画室だ。同室が『SenSage』の導入を行ったのは、2011年２月のこと。同室が管理するデータは主に法人顧客の格付・貸付・財務情報などで個人情報は少ないものの、中には企業経営者個人にかかわる情報も含まれている。個人情報保護法が求める要件を満たしたログ管理は必須の課題だった。

『SenSage』の導入以前から、データベースなどのログ管理を専用のログ管理ソフトで行っており、88台あるサーバーそれぞれにログを収集・蓄積してきた。情報漏えいが起きた時には、そのログから情報が漏えいした経路を追跡できるようにもなっていた。

「ただ、誰がいつ重要情報にアクセスしたか、業務時間外にアクセスした人物は誰かなど、アクセスログを分析するまでには至っていませんでした。今回『SenSage』の導入により、それが簡単にできるようになったことが、最大のメリットです」と、語るのは法人企画部 法人基盤企画室の小川祐司調査役だ。

情報セキュリティー管理者であっても情報漏えいを起こすという考え

これまでの常識で考えれば、個人情報にアクセスできる権限を少人数に限り、さらにそのIDとパスワードを管理し、ログを集積しておけば、それ以上の問題に発展する可能性は小さかった。しかし、最近はそこで安心することはできない。

「情報セキュリティーを管理すべき立場の人間が情報漏えいを起こす事件が起きている昨今、管理者がチェックしていればよいという発想には限界がある」と、小川氏は言う。

誰がどの重要情報に対して、いつアクセスしているのか、そのアクセスする根拠となる申請書は出ているのか、申請書の承認は然るべき人物が行っているか、アクセスは必要な作業だったのか――ここまで監視していかないと、情報漏えいを根本的に防ぐことはできないと言うのだ。

「誰でも漏えいの可能性はある」という考えに基づいた合理的・客観的なログ管理。『SenSage』にはそうした思想が色濃く流れている。

当初導入の目的にしたログ分析やレポート機能も、期待以上に使いやすいという。

「分析の観点は今大きく２つあります。時間帯に限らず、格付や貸付金額、住所氏名といった情報が格納されている重要テーブルに対してアクセスした人物やアクセスした情報を特定できるよう、日次でレポートを出すようにしています。もう一つは、休日などの業務時間外にアクセスした人物を特定し、時間外アクセスの傾向を分析できるようにしました」

同室の情報取り扱い・運用ルールには、事前に申請書を起こして、承認が下りて初めてデータベースにアクセスできるというものがある。

「当然レポートに名前があがってきたら、この運用ルールに則って申請書は出ているかを、まずチェックします。次に、申請書にはどのテーブルにアクセスするかを書かせているので、申請書のテーブル名とログ管理レポートのテーブル名を突き合わせる。もしも、申請書に書いていないテーブルにアクセスしていたら、なぜアクセスしたのか、その理由を個別に追及できるようにしました」（小川氏）

こうした運用ルールの厳格化で、各担当者が申請書を気をつけて丁寧に書くようになったという効果も表れている。ただ、現在は申請書との照合作業は手作業で行われている。申請ワークフローのログを『SenSage』に取り込むことによって、相関分析を自動化することが次のシステム的な課題だ。

今回の導入では、『SenSage』の基本機能であるログの収集・分析に加え、サーバーのエラー監視機能も盛り込んだ。

「せっかく統合ログ管理ツールを導入するのなら、これでサーバーのエラーもチェックできないかと思っていました。これまでは、夜間のジョブでサーバーにエラーが無かったかどうかを、毎朝８時から１時間半～２時間かけてログの記録を見ながら、数名の担当者が手作業で行っていました。これだけでも膨大な手間だったのです。それが『SenSage』のサーバーのエラー確認監視機能で自動化が可能だという。セキュリティーだけでなくシステム的な不安も解消されるので、我々としては一挙両得です」と小川氏。

エラー監視機能によりこれまでのチェック業務にかける時間が、約半分に短縮されたという。

膨大なデータも高圧縮できるので５年間の保管義務も難なくクリア

『SenSage』によるログ管理では、システムが吐き出すアクセスログの生データは、1日約20ギガバイト、ピーク時には40ギガバイトにも及ぶ。これらが積み重なると、すぐにテラバイトクラスの大規模なログデータになってしまう。法律上ではそれらのログを5年間にわたって保管しなければならない。当然、ログを保管するストレージの容量やそのコストを考えざるを得ない。

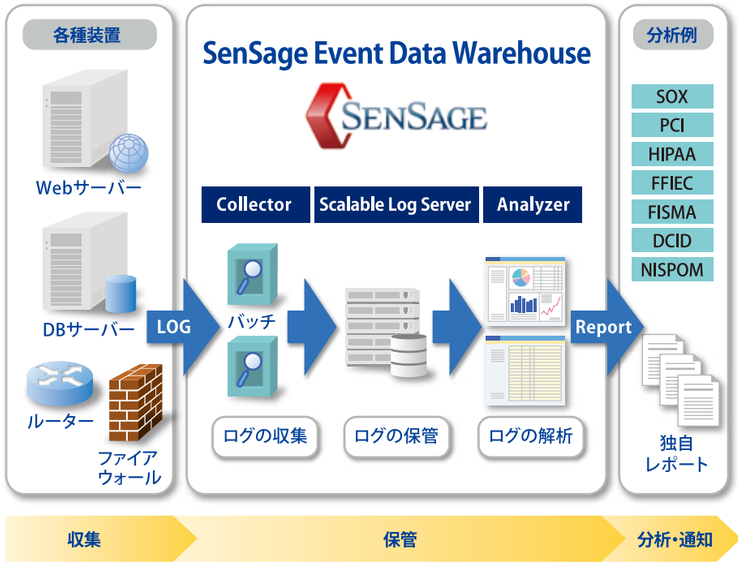
この点、『SenSage』に備わるログの高圧縮機能は大きな効果をもたらす。アクセスログに特化した独自の圧縮技術により、収集したログを約10分の1に圧縮し保存することができる。さらに、圧縮され保存されたログに対して、解凍することなく高速に検索・レポート作成が可能だ。

「当初はログのピーク容量を20ギガバイトと見込んでいましたが、それを超える時もありました。データが大きくなると、レポート作成時間内にログの収集が収まらなくて、ジョブが異常終了し、結果的にレポートが出力できないという事態もテスト段階では生じました。その部分を調整したのは、日立ソリューションズ。本稼働以降は大きな問題は発生しておらず、万一問題が発生してもそれを解消する作業手順が定められてるので、不安は感じていません」

と、小川氏は統合ログ管理ツールの意義を高く評価している。

SenSage Event Data Warehouse 概要

ログ長期保管・分析ツール『SenSage Event Data Warehouse』により、ネットワーク機器のみならず、サーバーのOSログ、DBログなど多様なログを収集し、相関分析、長期保管を実現します。



Yuji Ogawa

三菱東京UFJ銀行 法人企画部
法人基盤企画室
調査役
小川祐司氏

三菱東京UFJ銀行プロフィール

株式会社三菱東京UFJ銀行は、2006年1月1日、東京三菱銀行とUFJ銀行が合併して誕生した。三菱UFJフィナンシャル・グループ傘下の都市銀行。法人向け業務をバックアップする法人企画部では部署の情報共有（ナレッジマネジメント）システムの構築など、IT導入にあたっていくつかの先駆的事例を持っている。

導入ソリューション概要

［ジャンル］
統合ログ管理
［業種］
金融機関
［製品名］
統合ログ管理ソリューション
『SenSage Event Data Warehouse』
［ユーザー数］約3,000名

CaseStudy　独立行政法人 理化学研究所

シングルサインオンの導入で業務システムの利用率が向上

コンプライアンス、内部統制、リスク管理など、企業に求められる責任は重い。その一方で、IT環境の複雑化によりセキュリティー強度や管理ポリシー設計を統一することが難しくなっている。この対策として、認証やアクセス制御の統合・強化を実現するシングルサインオンによる統合認証基盤の重要性が高まっている。

Satoshi Tashiro

独立行政法人 理化学研究所
総務部　次長
事務情報化推進室長

田代　聡氏

Hiroshi Momose

独立行政法人 理化学研究所
総務部
事務情報化推進室

百瀬　浩氏

Masashi Murata

独立行政法人 理化学研究所
総務部
事務情報化推進室

村田雅史氏

理化学研究所プロフィール

1917年に創設された物理学、化学、工学、生物学、医科学など基礎研究から応用研究まで行う日本で唯一の自然科学の総合研究所。これまで、本多光太郎、寺田寅彦、仁科芳雄、朝永振一郎、湯川秀樹などノーベル賞受賞者を含む著名な科学者が籍をおいていた。本所は埼玉県和光市にあり、和光、筑波、播磨、横浜、神戸、さらに欧米にも研究センターを展開する。

導入ソリューション概要

［ジャンル］
認証・アクセス管理

［業種］
研究機関

［製品名］
リバースプロキシ型
Webシングルサインオンソリューション
『HP IceWall SSO』

［ユーザー数］
約10,000名

SSOはセキュリティー強度の保持とユーザーの利便性を同時に実現

独立行政法人 理化学研究所（理研）は大正年間に「科学者たちの自由な楽園」を標榜して設立された長い歴史を持つ。研究者の情報アクセスの自由を保つことは研究所の運営において絶対的な条件だ。一方、研究が高度であればあるほど、情報漏えいに神経質にならざるをえない。自由度とセキュリティーの両立が大きな課題だった。

ネットワーク環境で作業を行う際には、セキュリティーの観点からID・パスワードによる認証は欠かせない。端末起動時、LAN・サーバー接続時、Webアプリケーション利用時など、日に何度も入力するのは、かなり煩雑だ。そこで、セキュリティーを保ちながら利便性を損なうことなく、すべてのユーザー認証を一度でできる機能が必要とされている。その機能がシングルサインオン(SSO)だ。

理研では、2007年にSSO実現のために、日本ヒューレット・パッカード社(日本HP社)の『HP IceWall SSO』を導入した。

理研ではこの10年ほどの間に、業務システムを従来のクライアント・サーバー型から、Webに統合化する流れがあった。その背景には、理研ならではの事情もある。事務職に関してはWindowsが推奨OSだが、研究者の中ではMacintoshやLinuxもかなり使われており、それらのマシンで業務アプリケーションにアクセスすることになる。こうしたマルチOS環境の場合、Webシステム化の流れは当然とも言える。

その結果、理研では勤怠管理に始まり、会議用資料ダウンロードシステム、グループウェアなどの業務システムをWebアプリケーション化し、簡便に使えるようにする動きが進んでいた。しかし、SSO導入以前は、各業務システムごとにユーザーIDとパスワードを発行していたため、その管理がネックになっていた。

今後も業務システムのWeb化を強める意向を持っていた事務情報化推進室では、それらを統合的に管理する認証基盤を必要としていた。

「研究所のセキュリティールールとしてはパスワードを全部個別に設定する、定期的にパスワードを変える、ある一定以上の長さのパスワードを使うなどのルールがありますが、それをすべてのシステムに求めるのは、困難な課題でした。

セキュリティーの強度を求めつつ、利便性を高めるのにSSOというツールは強力です。1個のパスワードを覚えて、その管理をしっかりしておけば、高いセキュリティーが保てるからです。その代わり、パスワードの管理ルールは徹底するようにしています」と、実際のSSO導入にあたった総務部事務情報化推進室の百瀬浩氏は語る。

業務アプリケーションの変更もなくSSOを実現するリバースプロキシ方式

事務情報化推進室が求める仕様はWebアプリケーション対応で、稼働中の業務アプリケーション・サーバーへの改変が少ないことが条件。

Webシステム対象のSSOには、リバースプロキシ方式とエージェント方式がある。すでに安定稼働中のシステムにSSOを導入するには、アプリケーション・サーバーと利用者端末の間に認証サーバーを立ててSSOを実現する「リバースプロキシ方式」が適当と判断した。『HP IceWall SSO』はリバースプロキシ方式の代表的な製品であり、理研の求める仕様をすべて満たすことができた。導入にあたっては豊富な構築実績を持ち、利用実態に応じたカスタマイズ能力に優れているSIベンダーの役割が重要になった。

「既存の業務アプリケーションの仕組みの中にSSOを導入するにあたって、日立ソリューションズは豊富にノウハウを持つ企業。その手順や構築にあたって予想される懸念事項を前もって説明してもらえるので、安心感があります」と、事務情報化推進室の村田雅史氏は、日立ソリューションズへの信頼について話す。

例えば、パスワードを何度か間違えるとロックされるのは管理上やむを得ないが、ロック解除をしなければ業務が進まない。そのジレンマを解決するための解除機能を、日立ソリューションズが理研向きにカスタマイズすることで、利便性の向上も図っている。

『HP IceWall SSO』は数少ない国産SSO製品。日立ソリューションズと日本HP社の強力な協業体制も、ユーザーにとって強い安心感となった。後に、理研では併用することでより高いレベルでID・アクセス管理を実現できる『HP IceWall Identity Manager』と『HP IceWall SSO Dynamic Menu Portal』も導入している。

こうして『HP IceWall SSO』によるSSO認証基盤ができることで、新たな業務アプリケーションの導入もスムーズに行われるようになった。現在はWebテレビ会議、人事評価、eラーニングなど、13の業務システムがWeb上で稼働している。ユーザー数も当初の事業部門から徐々に増加し、研究部門まで拡大している。自分たちの研究成果を所内で共有するための仕組みが稼働し、研究活動の活性化に向けた情報共有も始まっている。

目指すは理研で働く人全員を一元管理するための認証の器

「理研の施設は国内・海外に多数存在し、さまざまな研究分野・研究室があります。それらに関わる人の身分は多種多様で流動性が激しい。このあたりが一般企業と違うところです」と、理研組織の特殊性を指摘するのは、事務情報化推進室長の田代聡氏だ。

研究所のネットワーク・セキュリティーを高めるためには、施設内にいま誰がいるのかを把握し、そのアカウントを一元管理するシステムが不可欠だ。そのため理研では、データへのアクセス権限をチェックする認証基盤システムを構築し、そこにユーザーアカウントを集約するという方針をとっている。

「『HP IceWall SSO』によってSSOは実現しましたが、私たちがもともと目指したのは理研で働く人全員を一元管理する認証の器を作ることでした。今後は認証基盤をセキュリティーの核として、既存の入退場管理などとも連携させていきたい」と、百瀬氏はこれからのセキュリティーへの取り組みを語っている。

これまではSSOの対象範囲を、社内Webシステムに限る企業がほとんどだったが、今後は、クラウドで提供される各種Webサービスの活用にも対象を広げる流れがある。例えばGoogleAppsなどを利用する際に、社内システムと外部サービスへのアクセスをシームレスにSSOで管理しようというものだ。『HP IceWall SSO』はこうしたクラウドサービスとの接続や仮想化環境での動作などの新しい機能を次々に追加している。

アクセス先が組織内・組織外であるかを問わず、サービス活用の利便性とセキュリティーを同時に担保するソリューションとして、あらためてその存在価値が高まっている。

CaseStudy　西日本システム建設株式会社

次世代型ファイアウォールでミッションクリティカルな画像転送システムの高可用性を実現

Web上のアプリケーションの利用が増大する中、企業の情報セキュリティーは、インターネット上の個々のアプリケーションを識別し、制御する時代へ突入しつつある。しかも業務の効率は落とさないことが企業にとって大きな課題だ。セキュリティーと高性能なソリューションの実現を目指した取り組みを紹介する。

セキュリティーには アプリケーション制御が不可欠

近年、アプリケーションの利用形態は大きく変化した。中でもWeb上の多種多様なアプリケーションの利用が増加している。Winnyに代表されるP2Pソフトは、ネットワークへ影響を与えるうえ、セキュリティー上の懸念もあり、使用を禁止している企業が多い。一方で、TwitterやYouTubeの普及により、そうしたアプリケーションを業務で活用する企業も増えている。こうした中、企業ではアプリケーションの使用を管理し、同時に業務効率の維持を実現するかが課題となっている。

画像転送システムの高可用性を 実現できるファイアウォールを求めて

西日本システム建設では、2010年11月にアプリケーション制御ファイアウォール『Palo Alto Networks PA-2050』を導入した。

国内外の情報通信インフラの構築に携わり、通信系，土木系の建設を行っている西日本システム建設では、施工現場の画像を携帯電話のiアプリを利用して撮影し、社内サーバーに転送し、社内の検査員が確認を行うという「施工現場確認システム」を導入している。これは、現場の施工状況を、検査員がチェックして工事の完了や作業の追加などを指示するものであり、リアルタイムでの確認が求められるミッションクリティカルなシステムだ。

同社が、『Palo Alto Networks PA-2050』導入以前に利用していたファイアウォールではポート単位の制御ができなかったため、ネットワーク全体に負荷がかかっていたことや、ファイアウォールを制御するソフトウェアを、最新の状態に更新するごとにシステムの再起動が必要であったことなどから現場確認を行う業務でダウンタイムが発生していた。

「リアルタイム性が大変重要な施工現場確認システムにおいて、ダウンタイムの発生は解決が急がれる大きな課題でした」と業務改善部 担当課長の中村一美氏は語る。

同社ではURLフィルタリングによるインターネットへのアクセス管理についても課題を抱えていた。アクセス解析用ログがテキストベースで大量に出力されるため、解析が追いつかず、従業員がアクセスしているサイトや、トラフィック特性の把握が現実的には不可能だったのだ。

さらにファイアウォールやアンチウイルス製品を併用することがボトルネックとなり、ネットワークシステムのパフォーマンスが低下するという事態も生じていた。

これらの対策として、WAN回線を1Gクラスにまで増強していたが、現場担当者からは「施工現場確認システムの画像転送に時間がかかる」との不満の声も上がっていたのである。

次世代型ファイアウォールの導入で 課題をまとめて解決

「画像転送システムのダウンタイム解消」「煩雑なアクセスログ解析の改善」「ネットワークシステムの性能向上」……これら３つの課題をすべて解決するファイアウォールがPalo Alto社の『Palo Alto Networks PA-2050』だった。

本製品は、アプリケーションの識別により、ネットワーク上で利用されているアプリケーションが誰によって、どのように利用されているかを把握する「アプリケーションの可視化」と、その利用の可否を管理する「アプリケーションの制御」ができる画期的なファイアウォールとして登場した。サイトの閲覧は可能だが、書き込みはできないようにするといったようにアプリケーションの機能ごとの制御もでき、部署や役職など社員の属性によって使用できるアプリケーションを変えるといった複雑な制御も可能だ。

さらにアンチウイルスやIPS（不正侵入防御）、URLフィルタリング機能を利用しても、従来のファイアウォールに比べ、高いパフォーマンスのソリューションを維持出来るという特長も持つ。

「なによりも重要だったのはアプリケーション制御のためのシグネチャ更新時に再起動する必要がないため、ダウンタイムが生じないという点でした。総合的に考え、『Palo Alto Networks PA-2050』はミッションクリティカルなシステムに耐えうるファイアウォールであると判断しました」と中村氏は導入の理由を語る。

こうしてシステムのダウンタイムが解消されたのと同時に、増強した広帯域WAN回線が有効に活用できるようになったため、導入直後から「施工現場確認システム」を利用している従業員からは画像の転送速度が向上したと報告が上がってきたという。

また、操作性の高いログ解析機能や充実したレポート機能で、個別のアプリケーションの使用状況の把握やトラフィックの推移把握が簡単に出来るようになった。

「それぞれのアプリケーションの使用状況を把握でき、画像転送の遅延原因を明らかにする上でも非常に有効でした」(中村氏)

加えてネットワークを流れるアプリケーションや脆弱性を可視化できるACC（Application Command Center）機能を活用することで、許可していないアプリケーションの使用がないか、ネットワーク上にウイルスや不正な攻撃が流れていないかをリアルタイムで確認できるようになり、セキュリティーが大幅に向上。操作・解析が容易なため管理工数の削減も実現した。

「『Palo Alto Networks PA-2050』は、画像転送システムの高性能を維持しながらセキュリティーを保持するという私たちが求めていた要件にマッチする唯一といってもよいファイアウォールでした」と中村氏は評価する。

現在は本社エリアのみでの導入だが、今後はミッションクリティカルなシステムが求められる別拠点への『Palo Alto Networks PA-2050』の導入も検討中だ。

また、アプリケーション制御について、現在のところP2Pの使用防止のみ実施しているが、今後は施工現場確認システムやその他のアプリケーションについてもACC機能を使い、同社のセキュリティーポリシーに従って不適切なアプリケーションの遮断を実施していくことも考えているという。また、『Palo Alto Networks PA-2050』に装備されているQoS機能にも注目している。

「重要なアプリケーションに帯域を割り当て、それ以外のアプリケーションの帯域を絞り込むQoS機能で施工現場確認システムの帯域を確保し、さらなるレスポンスの向上にも期待したいですね」（中村氏）

Kazumi Nakamura

西日本システム建設株式会社
業務改善部　担当課長

中村一美氏

西日本システム建設プロフィール

1954年創業。半世紀にわたり国内外の情報通信インフラの構築に携わる。本格的ユビキタス社会の実現に向けてNGN（次世代ネットワーク）や光アクセス網、高速無線通信網などのフルIPネットワーク基盤を活用した高度情報通信社会に向け、長年培ってきた先端技術やノウハウを駆使した総合エンジニアリング企業を目指している。

導入ソリューション概要

［ジャンル］
ネットワークセキュリティー

［業種］
情報通信設備建設等

［製品名］
アプリケーション制御ファイアウォール
『Palo Alto Networks PA-2050』

［従業員数］
859名（連結、2011年3月末現在）

イージーオーダーソリューション『快作スタイル』で、中小企業のニーズに応える

日立ソリューションズグループの中で、日立ビジネスソリューション(日立ビジネス)は、特にSMB市場（中堅・中小企業のお客様）向けの事業に積極的に取り組んでいる。同社が提供するパッケージ製品には、新聞販売店向けや司法書士向けの業務パッケージ、各種モバイルセキュリティソリューション、さらには汎用知的音声合成システム、給食・栄養管理システムなどユニークなものが数多くある。今回紹介するのは、2011年３月８日から販売を開始した『快作スタイル』だ。

「個別のお客様用に構築したアプリケーションではなく、イージーオーダーソリューション用として、必要となる機能を絞って一から開発したアプリケーションを利用していただき、必要に応じてお客様の業務に合った形でカスタマイズするというスタイルを取っています。言わば幾つかの型紙を基に、少し手直しして仕立てていく洋服のイージーオーダーのイメージですね」と営業企画本部長の西野敏行は『快作スタイル』のコンセプトを語る。

自社開発の『快作ベース』を基盤にしたソリューション

『快作スタイル』には『快作ベース』『どこでも快作』『快作コンシェルジェ』の３つの柱がある。

『快作ベース』はイージーオーダー型のソリューションを実現するための基盤の役割を果たす。「販売管理」「購買管理」「在庫管理」といったビジネス・テンプレート集で、日立ビジネスの開発ノウハウや業務ノウハウを結集して作り上げた。完全Web対応化に加え、クラウド対応、仮想化対応など、今後の主流となる最新アーキテクチャーに標準で対応している。

「『快作ベース』のテンプレートはシンプルに本当に必要な機能だけを抽出して作り込んでいるのが特長です。さらに必要があればお客様の業務に合わせてアドオンとして作り込んでいきます」（西野）。

この結果、スクラッチ開発よりも比較的短納期・低コストで、ERPの導入が実現できる。

モバイル端末で業務ソフトが活用できる『どこでも快作』

『どこでも快作』は『快作ベース』による業務向けアプリケーションをスマートフォンやiPadなどのタブレットでも活用できる機能だ。オフィスのPCだけでなく、モバイル端末で社外で業務画面を見たり、業務画面への入力を行うことが可能になる。

同社はモバイル端末で効率よくITを活用する『ケータイ快作!』といったアプリケーションの開発に力を入れてきた。そこで培われたノウハウを十二分に生かし、PCに比べ画面が小さく、処理速度が遅く、キーボードが無いモバイル端末での業務アプリケーションの活用が可能になった。例えば一画面では見づらい場合は複数画面に分ける、手で操作するスマートフォンやタブレット向けに文字の大きさを変えるといった細かいノウハウが生かされている。

「PCでデモ画面をお見せしながらiPad版、さらにスマートフォン版の同じ画面をお見せすると皆さん驚かれますね（笑）」とプロダクトシステム事業部基盤開発センタ長の坂本英昭は語る。

気になるのはセキュリティーの問題だが、『ケータイ快作!』はセキュリティーを強化するため、各モバイル端末専用に履歴が残らないブラウザを開発して組み込んでいる。また、モバイル機器を紛失した場合、管理機能からモバイル端末の画面表示をロックすることで、情報漏えいを防ぐことができる。『どこでも快作』でも、この機能を使用することが可能になっている。

「スマートフォンやタブレットの浸透状況を考慮すると、モバイル端末での業務用アプリケーションの利用は今後一般化し、またオフィス内での業務もPCからタブレットにある程度移行するのではないかと予測しています」と坂本。同社のモバイル関連のノウハウが生かされる機会は今後さらに増えそうだ。

『快作コンシェルジェ』で中小企業をワンストップでサポート

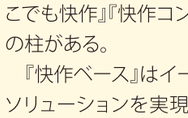
『快作コンシェルジェ』は『快作スタイル』を導入前から運用まで一貫してサポートするサービスだ。

中小企業ではIT部門のスタッフがいないケースも多く、現在のシステムの状況がどうなっているのかを把握していないことも珍しくない。

「まずは現状の整理から始まり、お客様の経営方針に従い，そもそもどのようなITシステムを導入すべきかといったことから一緒に考えていきます。『快作スタイル』の導入にあたっては、実際にどの様に使って、経営にどの様に生かすかといった具体的なご提案もしています」と語るのはITコンサルティングセンタ　主任技師の曽根国男だ。日立ビジネスでは以前からSMB市場向けのコンサルティングに力を入れ、ITコーディネータの有資格者約50名を擁している。2007年には、ITコンサルティングセンタを立ち上げ、IT導入支援を展開している。『快作スタイル』では曽根を始めとする経験豊かなITコーディネータがサポートにあたる。

「独自のビジネスを展開している中小企業はその独自な業務の部分にマッチするERPシステムを持つべきだと考えてご提案をさせていただいております」（曽根）。

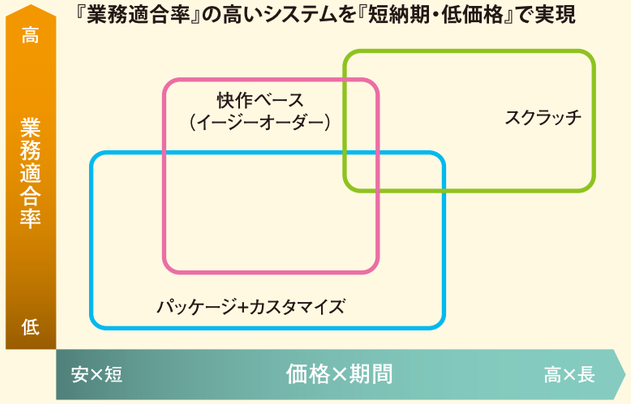
今後は業種ごとのテンプレートを増やし「イージーオーダー」の選択肢を増やすなどソリューションに厚みを持たせながら、独自のビジネスを展開する中小企業をシステム面からサポートすることを目指していく。



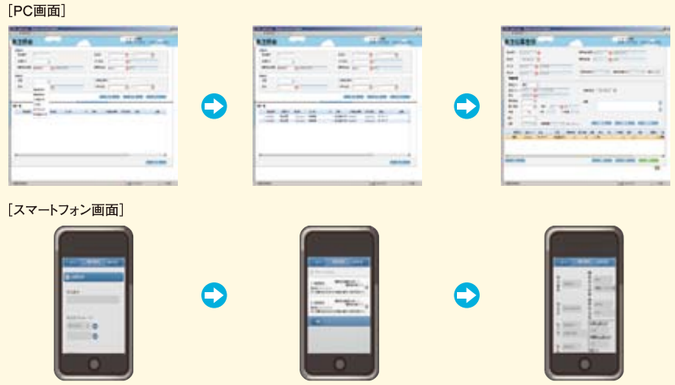
日立ビジネスソリューション株式会社
営業企画本部長
兼 開発基盤拡販推進センタ長
西野敏行
Toshiyuki Nishino

日立ビジネスソリューション株式会社
プロダクトシステム事業部
基盤開発センタ長
兼 開発基盤拡販推進センタ　部長代理
坂本英昭
Hideaki Sakamoto

日立ビジネスソリューション株式会社
ITコンサルティングセンタ　主任技師
兼 開発基盤拡販推進センタ　部長代理
曽根国男
Kunio Sone



快作スタイル-サンプル画面（伝票検索→検索結果リスト→伝票詳細表示）



日立ビジネスの主な提供製品

製品名	内　容
A³ BROWSER Xstyle	携帯電話等を活用した高度な業務システムを短期間・高品質に構築できるモバイルミドルウェア
DoMobile CSE	外出先や自宅（在宅勤務など）から自社内のPC環境へリモートアクセスできるソフトウェア
ケータイ快作!	モバイル端末で手軽に業務報告書を作成できるソフトウェア
レンタルマイスター	超小型の無線ICタグを使用して物品の登録／破棄・利用（持出／返却）といった管理業務を効率よく行えるシステム
グリーンプリント	プリンターの設定を意識することなく、トナー・インクや印刷用紙を節減するソフト
ボイスソムリエ ネオ	テキストを入力するだけで高品位な音声を作成できる音声合成システム

日立ビジネス「快作スタイル」のお問い合わせ先
日立ビジネスソリューション株式会社　営業企画本部
TEL:045-224-6754　FAX:045-224-6719　E-mail: event@hitachi-business.com

日立ビジネスソリューション株式会社
（略称：日立ビジネス）
Hitachi Business Solution Co.,Ltd.

■設立　1976年（昭和51年）4月
■本社　〒231-0062
横浜市中区桜木町一丁目1番地8（日石横浜ビル）
TEL.(045)224-6111（大代表）
FAX.(045)224-6119
■資本金　35億6千万円
■事業内容　・パッケージソリューション
・システム構築&サービス
・ソフトウエア開発
■証券コード　4738（東京証券取引所市場第1部）

Hitachi Solutions
REVIEW
［日立ソリューションズ情報誌］
Hitachi Solutions Information magazine
2011.vol.2

［編集後記］

このたびの東日本大震災で被災されたすべての方々に、心よりお見舞い申し上げます。一日も早い復興がなされますことをお祈り申し上げます。

第２号となる今回は「情報セキュリティー」に焦点をあてました。企業は常にデータの盗難、不正アクセス、改ざん、漏えいなど、さまざまな脅威さらされています。また、企業の情報セキュリティー対策への取り組みは、自社ばかりでなくビジネスアライアンスを結ぶパートナーにまで影響を及ぼすほど、企業活動にとって重要なものとの認識が高まっています。当社は、社内外からの情報漏えいに対しコンサルティングからシステム設計・構築までのソリューションとして情報セキュリティー対策を支援して参ります。これからの日立ソリューションズに是非ご期待ください。

［スタッフ］

発行元 ● 株式会社 日立ソリューションズ
編集長 ● 竹橋 徹
編　集 ● 廣納 守・柴田康平・槇田理恵
制作・印刷 ● トッパン・フォームズ（株）西尾理恵子
クリエイティブディレクター ● 本田正毅・リセット
アートディレクター ● 工藤こうきち
エディトリアルディレクター ● 弘中ミエ子
コピーライター ● 広重隆樹・原 智子
フォトグラファー ● 相沢邦広・伊藤睦美・佐藤可進
イラストレーター ● 磯 良一（表紙イラスト）

お問い合わせ先／日立ソリューションズ広報・宣伝部
E-mail:review@hitachi-solutions.com

日立ソリューションズ

株式会社 日立ソリューションズ

本　　社　〒140-0002 東京都品川区東品川四丁目12番7号
本社別館　〒108-8250 東京都港区港南二丁目18番1号
http://www.hitachi-solutions.co.jp/