お客様とBBSをつなぐコミュニケーションツール

BBS GROUP NEWS

BUSINESS BRAIN SHOWA-OTA GROUP NEWS

Vol.49 【JULY·2015】

特 集

マイナンバー制度に対する正しい理解と対応

サービス紹介

財務経理業務のBPOサービス

グローバルに展開する組織全体の業務標準化を支援

情報セキュリティ強化支援サービス

情報セキュリティの現状を3つの調査·アセスメントで可視化

Topics

「PLMconsole®」新バージョンをリリース

特集

マイナンバー制度に対する正しい理解と対応

2015年10月5日に「行政手続における特定の個人を識別するための番号の利用等に関する法律（以下マイナンバー法）」が全施行されます。2016年1月からのマイナンバー制度の開始を控え、企業や団体にさまざまな対応が求められています。今回の特集では、企業・団体がマイナンバーを取り扱う際のリスクと対策について説明します。

2016年1月の制度スタートに向けて迫られる企業の対応

マイナンバー制度は、住民基本台帳に記載され、日本に居住するすべての人々に唯一無二のマイナンバー（12桁の個人番号）を付番し、複数の行政機関が個々に保有している個人情報を提供連携することで、“縦割り行政”と言われていた壁を取り払い、真の電子政府を実現する鍵となる制度です。これにより、公平で公正な税の負担や社会保障の提供、行政手続きの効率化や国民の利便性向上、災害被災者への迅速な支援などが期待されます。

マイナンバーの通知は2015年10月に開始され、2016年1月以降は税分野（源泉徴収や確定申告など）、社会保障分野（年金や医療／雇用保険、福祉給付金など）、災害分野（被災者生活再建支援など）の各手続きで、マイナンバーの記載が求められます。このため企業・団体にかかわらず、税や社会保障の手続きのためにアルバイトやパートを含む全社員や職員からマイナンバーを取得・収集する必要があります。

マイナンバー法では、マイナンバーおよびそれを含む個人情報を「特定個人情報」と呼び、厳格な保護を求めています。マイナンバーのライフサイクルは「取得・収集」「保存・保管」「利用・提供」「削除・廃棄」に分けられ、それぞれの場面で安全管理措置の実行が厳格に定められています。また、罰則には個人罰も含まれるなど、非常に厳しくなっています。

しかし現状は、企業・団体の対応は人事や給与システムの対応レベルに留まり、残念ながら安全管理措置実施の必要性に関しては、認知も認識も低い状況です。

マイナンバー制度のポイント

POINT 1 マイナンバーを含む情報は、一般の個人情報とは異なる**「特定個人情報」**として扱われます。

管轄法

従来の個人情報 →	個人情報法保護法
特定個人情報 →	**マイナンバー法**

POINT 2 特定個人情報を保護するため、漏えいなどに対する**罰則が強化**されました。

個人情報保護義務違反 →	事業者のみが罰則対象
特定個人情報保護義務違反 →	**事務の従事者個人も罰則対象**

POINT 3 扱う情報が**1件でも対象事業者に。**

個人情報保護法の改正により、例外規定（5,000件以下の場合は対象外）が撤廃
2017年6月までの間のいずれかの日で施行

マイナンバー法が企業や団体にもたらすリスクと責任

最近発生した個人情報の大量漏えい事故も含め、個人情報の漏えい事故が後を絶たない現状に、社会の不安は高まっています。マイナンバーは、税や社会保障に加え、預貯金口座へのマイナンバー登録も検討されています。これは個人の財産情報と結び付くことになり、より慎重で厳重な取扱いが求められることになります。そこで、企業や団体に対して、マイナンバーの取得・収集から削除・廃棄のすべての場面で「特定個人情報」を保護するための安全管理措置が求められています。

ポイントは「管理区域（サーバ室など）」と「取扱い区域（執務室など）」、および「取扱い者（マイナンバーに関わる業務処理をする者）」を明確に定め、それぞれに対する安全管理措置を実行することです。

マイナンバーはハイセンシティブな情報と位置づけられます。

株式会社ビジネスブレイン太田昭和
情報セキュリティ研究所
所長
小田部 昭

株式会社ビジネスブレイン太田昭和
執行役員
コンサルティング統括本部
コンサルティング事業開発部長
相原 秀明

マイナンバーを含む特定個人情報の取扱いを誤り、漏えいすることがあれば、企業や団体の社会的信頼が根底から揺るぎかねない事態になります。経営者は、マイナンバーの安全管理を存続に関わる重要課題と捉え、適切に実行する必要があります。

また、不適切な取扱いがあった際の罰則も強化されており、企業や団体と取扱い者の双方に、重い罰則（刑事罰など）が科されることになっています。このため、マイナンバーの取扱い者は精神的な負担とリスクを負うことになります。経営者には、社員や職員を保護するという面でも、適切な安全管理措置を実行する責任があるのです。

マイナンバーを取り扱う上での主な対策

取得・収集	・利用目的の明示 ・本人確認の徹底
保存・保管／利用・提供	・委託先・再委託先も含めた安全管理措置 ・従業員の教育・監督 ・管理区域・取扱い区域に対する安全管理措置
削除・廃棄	・所管法令などで定められた期間を過ぎたものは速やかに削除または廃棄 ・削除・廃棄したものはその記録を残す

マイナンバー法の安全管理の効率的対応を提案するBBSのサービス

マイナンバーの取扱いにあたっては、4つの安全管理措置が求められていますが、ハード／ソフトの両面から幅広い対応が必要で、短期間ですべてを実行するのは困難です。

経営者にとって重要なのは、何が「特定個人情報」に当たるのかをしっかりと理解した上で、それを「個人情報」と明確に分け、厳重な安全管理のもとで必要な処理が行える環境を整備することです。これにより、マイナンバーに関する安全管理コストと漏えいリスクを最少化することができます。

BBSは、マイナンバー法における安全管理措置の内容を精査し、マイナンバーの取得・収集／本人確認から管理区域／取扱い区域／取扱い者に対する安全管理策として、BPO（Business Process Outsourcing）をはじめとして、安全管理に関わる研修やコンサルティング、必要な安全管理措置を、的確かつ段階的に導入できるアプライアンス型のパッケージなど、多様なメニューを用意しており、お客様ごとにベストプラクティスを提供します。これから本格的なマイナンバー法対応を始めたい、コストを抑えて効率的に進めたい、というお客様は、ぜひ、お問い合わせください。

企業に求められる安全管理措置

「基本方針」および「取扱規程」の策定

・基本方針：取り組み方針や法令遵守・安全管理・問い合わせ・苦情相談などに関する方針
・取扱規程：特定個人情報などを取り扱う際のルールや事務フローなどを示した文書

組織的安全管理措置	人的安全管理措置	物理的安全管理措置	技術的安全管理措置
マイナンバーを取り扱う管理体制整備、実施策の承認、情報漏えいなどの事案発生時の連絡体制などを整備すること。	マイナンバーを取り扱う事務取扱い担当者の教育・監督、従業員に対する必要な教育を実施すること。	管理区域と取扱い区域を明確に定め、「特定個人情報」の漏えい／滅失／き損／改ざんの防止対策を実施すること。壁や間仕切りの設置、印刷物も含め覗き見できない環境への変更、鍵付きキャビネットの設置など。	システムへのアクセス制御や、ウィルス対策ソフトの導入、不正アクセス対策、ログ監視など、技術的なセキュリティ対策を実施すること。

お問い合わせ先　株式会社ビジネスブレイン太田昭和　コンサルティング統括本部　担当：相原 秀明　TEL：03-3507-1313

グローバルに展開する組織全体の業務標準化を支援

日系企業の海外進出において大きな課題となるのが、進出先の国の法制度・会計制度・行政手続きに適応した事務・会計業務プロセスの構築です。国内と海外で業務プロセスに差異が生じ、財務会計情報の収集が妨げられる例もあります。BBSでは、こうした課題を抱えるお客様に、組織全体の財務会計業務プロセスの標準化を支援するサービスを提供しています。

法制度・会計制度の差異が海外進出の“落とし穴”に

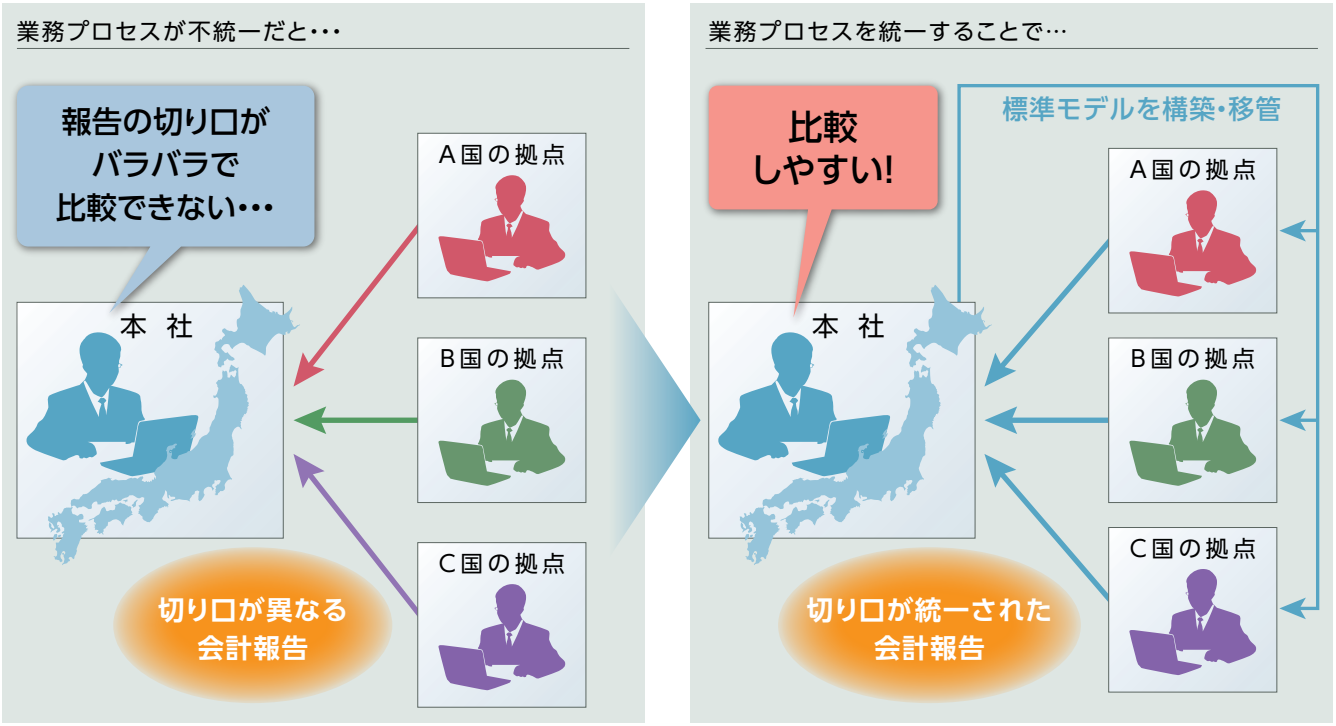
日本政府は成長戦略の1つとして、2020年までに中堅・中小企業などの輸出額を2010年比で2倍にするという成果目標を掲げ、企業の海外進出を積極的に支援しています。また、少子高齢化に伴う国内市場の縮小を背景として、日系企業が海外ビジネスを検討するケースも増加しています。その一方で、海外に進出した企業の約4割は、海外からの撤退または撤退を検討した経験があるとされます※。

撤退の主な理由としては「資金回収」「現地従業員の処遇」「法制度・会計制度・行政手続き」などの困難さが挙げられており、生産や販売、サービスの提供といった本業面よりも、その基盤である事務・管理業務面で課題に直面していることが浮き彫りになっています。加えて、その傾向は、コスト低減を狙う日系企業が海外進出の重要拠点と捉えているアジア諸国（中国、タイ、ベトナム、インドネシア）において、より顕著に見られます。つまり、進出国の法制度・会計制度・行政手続きについて、事前に十分な調査ができず、進出先で事務・管理業務の課題に直面する企業が多いのが現状です。

こうした課題の背景には、アジア諸国の法制度・会計制度自体が不安定であることや、進出先の国の制度について調査を行うためのリソースが企業に蓄積されていないことがあります。制度を事前に把握できずに進出した結果、国内外の事務・管理業務プロセスを統一できず、企業内の情報管理を一体化できない、という事態に陥っているのです。特に、経営判断の重要な材料となる財務会計情報が効率的に収集できない状況は、海外進出後の企業経営に直接影響を与える懸念材料となっています。

※（株）帝国データバンク 2014年10月15日発行 “海外進出に関する意識調査”

プロセスを標準化することのメリット



本社が求める情報を確実に取得できる業務プロセスの構築を支援

このような現状への打開策として、BBSでは、海外支社などの財務経理業務プロセスの標準モデルの構築支援サービスと、財務経理業務プロセスの受託サービスを提供しています。支援にあたっては、財務経理業務プロセスに精通したコンサルタントが、お客様にとって「最適の業務プロセス」(＝標準モデル)を検討します。

例えば、日本に本社を置き、世界20カ国に支店等の拠点を構えるA社様では、各支社の財務情報を本社が求める切り口で取得できず、各支社の財務情報が不透明となっていました。そこでBBSは、まず本社としてどのような財務情報を収集するべきかという本社財務経理部の要件をインタビューし、その上で要件確定の支援を実施、標準モデル作成に取り組みました。

業務の標準化において陥りやすい間違いの1つが、海外支店などの財務経理プロセスの現状確認から手をつけてしまうことです。しかし、時間とコストをかけて海外支社の現状の業務をヒアリングし、その支社に最適な業務を考えたとしても、結果的には部分最適に終わってしまい、本社が本来得たい情報が全く得られないという結果になりがちです。

しかし上記のアプローチであれば、その後の世界各国の支社での業務要件の確認時に無用な再定義が必要なくるため、A社様では外部委託(BPO)化のスムーズな実現が可能となりました。

標準化から移管までを一貫して支援「短期」「ローコスト」の実現へ

BBSの特徴は、財務経理の現場の現金管理業務、支払、決算、給与計算、資金管理などの各プロセスにおける業務標準化を幅広くカバーし、移管・運用までを一貫してサポートできることにあります。

これを活かして、業務の移管時には、ブラックボックス化している海外支店の財務経理業務を可視化し、標準モデルとの差異を分析します。その上で、標準モデルが適用できず海外の支店のローカルルールや会計制度に従うべきプロセスがあれば、標準モデルの種類を追加し、あくまで組織横断的な標準モデルとして扱うようにしています。

また、業務の標準モデルの定着化は、組織横断的になればなるほど時間を要します。BBSでは、すべての標準モデルの定着化を待つのではなく、標準化されたものから順次外部への移管を始めるアプローチをとることによって、より短期間、かつ、業界平均より低コストでの業務移管を可能としています。

これに加えて、BBSのBPOセンターでは、英語や中国語、その他言語に対応可能な体制を整えており、財務経理業務プロセスのアウトソーシングに広範囲に対応するなど、高品質のサービスを提供しています。

Message

ハイブリッドモデル活用による業務の平準化、品質の安定化の実現を支援

当社は、お客様の状況に応じて、日本と海外においてBPOサービスを提供する「ハイブリッドモデル」を提唱しています。業務の平準化・品質の安定化を実現するために、日本と海外BPOの特徴を活かして、お客様の戦略を支える、最適なアウトソーシングサービスの提供に努めています。

グローバル・シェアード・サービス事業部
マネージャー
山本 拓郎

お問い合わせ先

株式会社ビジネスブレイン太田昭和
グローバル・シェアード・サービス事業部
〒105-0003
東京都港区西新橋1-2-9 日比谷セントラルビル22F
TEL：03-3507-1313　FAX：03-3507-1311
コーポレートサイト：http://www.bbs.co.jp
サービスサイト：http://www.bbs.co.jp/service/consulting/global/gss.html

情報セキュリティの現状を3つの調査・アセスメントで可視化

企業に潜むセキュリティリスク、あるいは企業の外から迫るセキュリティリスクは、「現状を調査する」ことで可視化できます。グローバルセキュリティエキスパート株式会社（GSX）では、3つの現状調査を通じて、セキュリティの強化をサポートしています。

セキュリティリスクへの適切な対応が企業の生命線に

今や情報セキュリティインシデントは経営リスクに直結し、対策は企業にとっての生命線と言えます。しかし、内部不正による「内部脅威」、不正アクセスや標的型攻撃などの「外部脅威」ともに増加しています。IPA（独立行政法人情報処理推進機構）が2015年2月に発表した「情報セキュリティ10大脅威 2015」においても、「内部不正による情報漏えい」や「標的型攻撃による諜報活動」が上位にランクインしました。

こうした脅威に対しては、「現状を調査する」ことでリスクを可視化し、結果を踏まえて対策を実施することが最適解と言えます。

❶ 情報セキュリティレベル現状調査

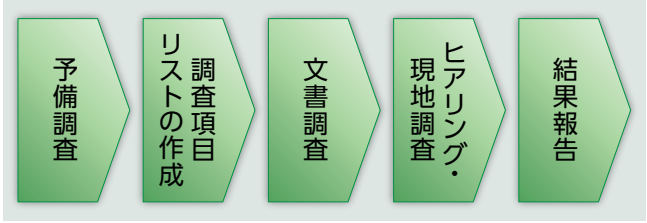
社員による情報の持ち出しや管理ルールの不徹底といった内部の脅威は、単一の対策ソリューション導入だけでは防ぎきれません。物理面／運用管理面／技術面を含めた総合的な対策と、継続的にPDCAサイクルを回すことが必要です。まずは現状のセキュリティ対策について総合的に調査・確認し、「どこに注力すべきか」「守るべき情報資産は何か」を明らかにした上で、効率的かつ効果的なセキュリティ対策をマクロ視点で実施していくことが望まれます。

GSXでは、専門コンサルタントが、既存の規程類の調査や拠点へのヒアリング、現場視察・実機確認などを実施し、お客様の物理面／運用管理面／技術面のセキュリティの現状を網羅的に調査・評価します。

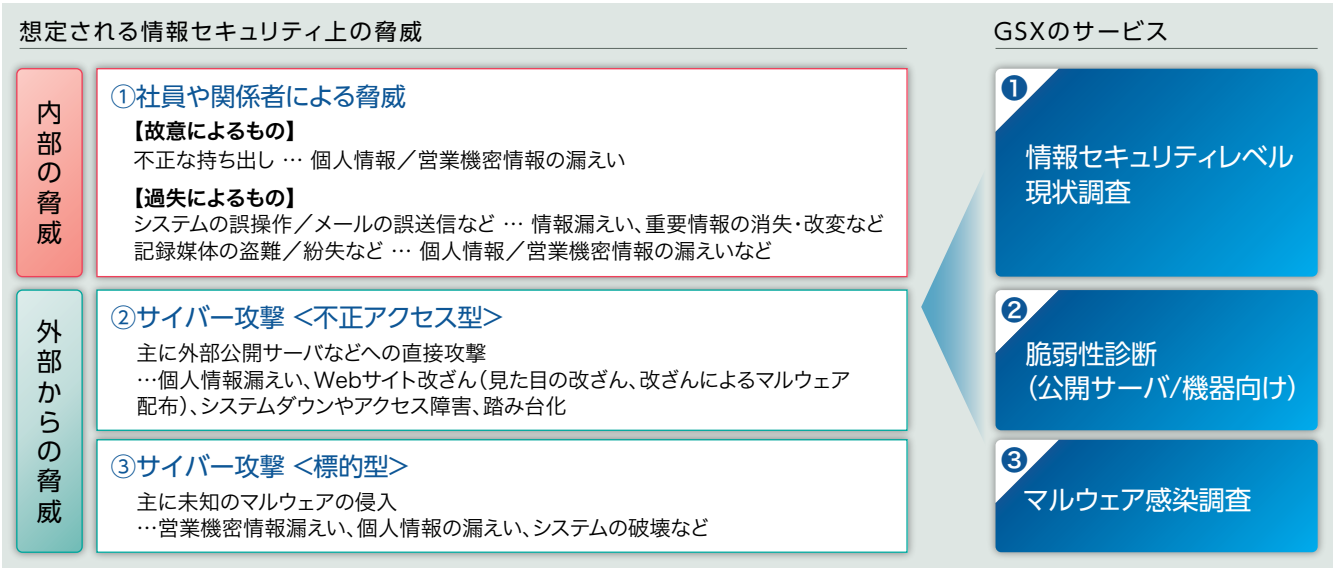
調査後は、「総合コメント」「情報セキュリティレベル」「分野別コメント」を記載した報告書を作成し、想定されるリスクの影響の大小、対応の優先順位などを報告するとともに、改善案などを提言します。

また、お客様のセキュリティの現状を業界水準やあるべき望ましい水準と比較し、その結果を、レーダーチャートを用いて、可視化して報告します。

情報セキュリティレベル現状調査 実施フロー



情報セキュリティ上の脅威とGSXのサービス



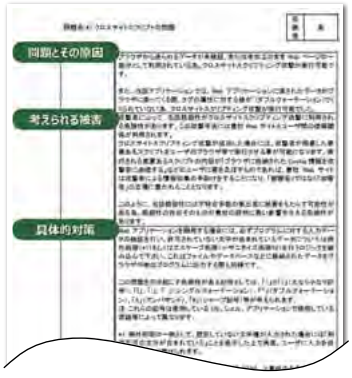
❷ 脆弱性診断（公開サーバ／機器向け）

外部に公開されるWebサーバなどへの不正アクセス（直接攻撃）は、報道発表されるセキュリティ事件のなかでも最多のものです。個人情報保護の観点から対策が必要なのはもちろんですが、昨今では個人情報が保管されていないWebサーバなどが改ざんされ、アクセス者がマルウェア配布などの被害を受ける事件も多発しています。

こうした事件・事故は、不正アクセスによる攻撃（脅威）が潜在するセキュリティホール（脆弱性）を突くことで発生します。潜在する脆弱性を検出し、対策措置を実施することができれば、事件・事故が発生する可能性や発生時の被害を極小化することが可能です。これを目的として実施するのが脆弱性診断です。

GSXでは、公開サーバ・ネットワーク機器を擬似ハッキングすることで、潜在的なセキュリティホール（脆弱性）を検出するとともに、その具体的な対策を提案します。具体的にはGSXのホワイトハッカー（セキュリティコンサルタント）が、お客様のWebサーバ（Webアプリケーションを含む）や公開されているネットワーク機器／サーバに対して擬似攻撃を実施し、検出した脆弱性への対応策を報告します。

脆弱性診断 報告書イメージ



❸ マルウェア感染調査

メールサーバのウイルス対策やスパムフィルタリング、またはエンドポイントのウイルス対策などについてはすでに大半の企業が取り組んでいると思われますが、未知のマルウェアが送りつけられるケースの多い標的型攻撃では、アンチウイルスソフトの導入に代表される従来型の技術対策だけですべてを防ぎきることは現実的に困難です。

標的型攻撃への対策、特に技術対策においては、一般的にはネットワークへのアプライアンスの導入や全クライアントへのソフトウェア導入などが必要です。GSXではこの足がかりとして、

マルウェア感染調査 サマリイメージ


2.1. 結果サマリ

調査の結果、Webブラウザの脆弱性を突く攻撃が1件と、マルウェアのダウンロードが6件検出されました。

No.	通信種別	通信内容	通信方向	危険度	検出件数	検出日
1	Malware Callback	クライアント端末がマルウェアに感染し、C&Cサーバへのコールバック通信が発生しています。	内→外	重	0	-
2	Web Infection	クライアント端末がマルウェアによりWebブラウザ経由で攻撃を受けている可能性があります。	外→内	中	1	2014/XX/XX
3	Malware Object	クライアント端末がマルウェアをダウンロードした可能性があります。	外→内	中	6	2014/XX/20
4	Domain Match	クライアント端末が、既に活動を停止したC&Cサーバにアクセスしています。	内→外	重	0	-
5	Infection Match	クライアント端末が、不審なサイトへアクセスしています。	外→内	重	0	-

・通信方向が内→外である№1 Malware CallBack 及び№4 Domain Match を検出した場合、貴社内のいずれかの端末がマルウェアに感染しているものと考えられます。
・通信方向が外→内である№2 Web Infection №3 Malware Object 、№5 Infection Match を検出した場合は、検査期間内に貴社内の端末へマルウェアが侵入した可能性があるものと考えられます。

現状のマルウェア感染の有無を調査し、対策実施の優先度や重要度を改めて確認していただく「マルウェア感染調査」サービスを提供しています。

このサービスでは、ネットワーク・ゲートウェイに専用の調査機器（アプライアンス）を設置し、マルウェアへの感染状況を調査します。その後、「①侵入してきたマルウェアや未知の脆弱性を突く攻撃の有無」「②すでにマルウェアに感染している端末の有無（攻撃者サーバへの通信＝コールバック通信の有無）」についてレポートを作成、報告会を開催します。

また、技術対策のみならず、従業員へのセキュリティ教育も必須です。例えば、日本年金機構がサイバー攻撃を受け、約125万件の年金情報が流出した問題でも、不自然なメールをそれと見分けられるような教育の必要性が改めて論じられることとなりました。

そこでGSXでは、マルウェア感染調査のオプションとして、標的型メール訓練サービスをご提供しています。本サービスでは、標的型攻撃メールを模した「訓練メール」を対象者に送信し、どの程度のユーザが攻撃メールを開封してしまうかのみならず、感染時の初動対応を徹底し、被害を最小化できるかどうかなども含めて、現状のセキュリティレベルを調査します。

お問い合わせ先

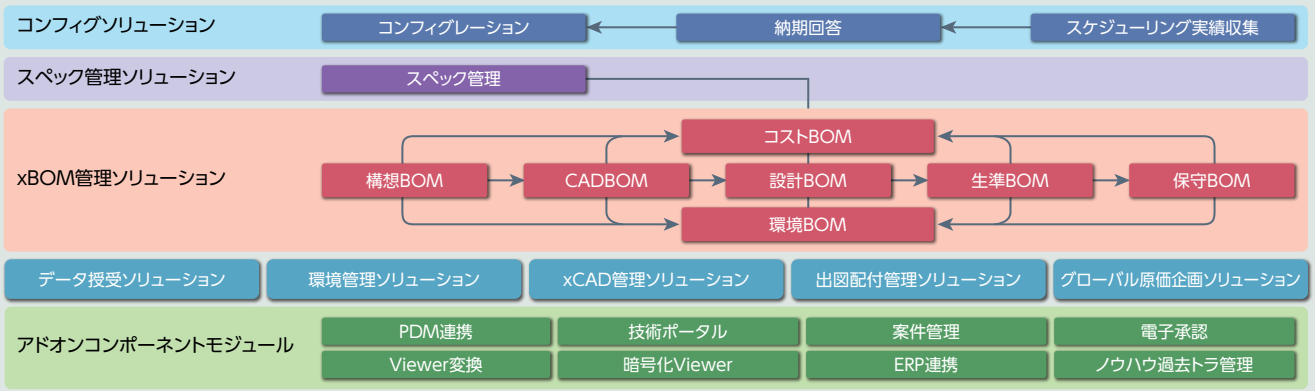
グローバルセキュリティエキスパート株式会社
事業開発部 マーケティング室
〒105-0004 東京都港区新橋1-18-16 日本生命新橋ビル 3F
TEL：03-3507-1360　FAX：03-3507-1361
コーポレートサイト：http://www.gsx.co.jp
サービスサイト：http://www.tiger1997.jp

「PLMconsole®」新バージョンをリリース

製品の機能・コスト・品質の80%は、ライフサイクルの上流工程（開発・設計段階）において決定されるといわれ、上流工程での作り込みが鍵となります。PLMジャパンが提供する純国産PLMソリューション「PLM*console*®」は、専業ベンダーとしての30年以上にわたる経験と実績を活かし、ライフサイクル全体にわたる製品情報の最適管理を支援します。2015年7月にリリースしたVer.2015では、自動車、家電、製造装置業界での実績をもとに、中堅組立製造業向けのテンプレートを追加。PLMのクイックスタートをサポートしています。

お問い合わせ先
株式会社PLMジャパン 営業本部
E-mail：sales_group@plmj.jp
TEL：（東　京）03-3507-1340
（名古屋）052-220-5215
（大　阪）06-6940-0081
コーポレートサイト：http://www.plmj.jp

ソリューション構成

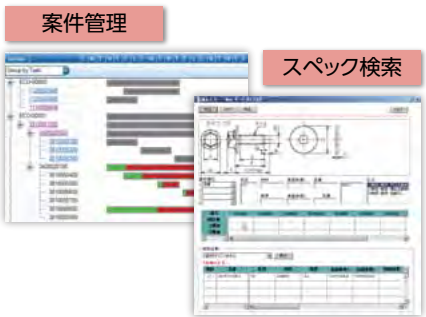


PLMconsole® Ver.2015 新機能

受注設計生産型テンプレート

受注設計生産型企業向けPLMクイックスタートテンプレート。利益を生む製品開発を支援する全体最適ソリューション。

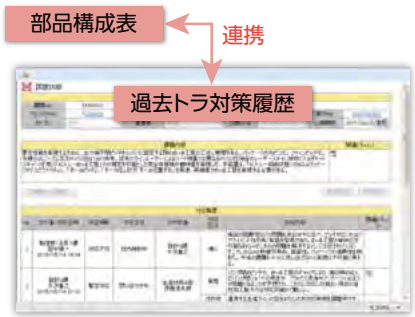
- ■製番・案件管理
- ■モジュール化・スペック管理
- ■CAD管理
- ■BOM管理
- ■ワークフロー
- ■生産システム連携



ノウハウ過去トラ管理

「同じ失敗を繰り返す事なかれ！」――「個人知」を「組織知」へ。ノウハウやトラブルとその対策履歴を品番と紐付けて管理。結果だけでなく経過情報を確認させ、実効的な知識を定着。

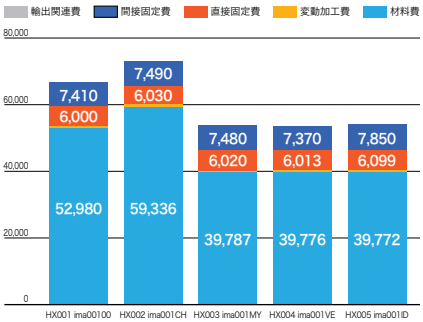
■記録→保管→伝達→共有→分析→蓄積



グローバル原価管理

グローバルな製造オペレーションの拠点原価、連結原価を見える化し、意思決定を支援。

- ■多通貨での拠点原価の可視化
- ■内部利益を控除した連結原価の集計
- ■製造拠点の原価比較



編集後記

「思考」と「志向」。この2つの言葉について、興味深い考察を読みました。ものごとの上達のためには「マイナス思考」×「ポジティブ志向」が重要だというのです。これは、厳しい現実から目を背けず、現在できていないことを素直に認めて前向きに取り組むということ。それによって自己肯定感が生まれるという内容でした。そして「プラス思考」とは実は、都合の良い部分しか見ないことであると。「プラス」という言葉を「マイナス」のイメージで捉える筆者の視点に新鮮な驚きを覚えました。

BBS Management Innovation
株式会社ビジネスブレイン太田昭和
発行：**BBS GROUP NEWS 編集室**
〒105-0003 東京都港区西新橋1-2-9 日比谷セントラルビル21F
TEL：03-3507-1300　FAX：03-3507-1301
URL：http://www.bbs.co.jp

本誌に対するご意見ご要望を編集室までお寄せください。