

UNIRITA

Magazine

08-09

2016

ユニリタマガジン

特集

"攻めのIT"の最大の推進力となる APIマネジメント

～次世代システムの構築に向けたアプローチ～

ユニリタ新ビジネスコラム

デジタルトランスフォーメーションに 必要な技術とは? Vol. 2

～セキュリティも「まことに日に新たなり」～

製品&サービス最新トピック

デジタルビジネスで勝ち抜くための
システム運営ライフサイクルの実現

ITサービスマネジメントの プロセス改革(BPR) サービス

システム管理者の会

「第10回システム管理者感謝の日イベント」
開催報告

UNIRITAユーザ会

研究グループ合同合宿開催!
全国で222名が参加!開催報告

パートナー様ご紹介

日本ビジネスシステムズ株式会社様

ユニリタ
イメージキャラクター
ホラン千秋



"攻めのIT"の最大の推進力となる APIマネジメント

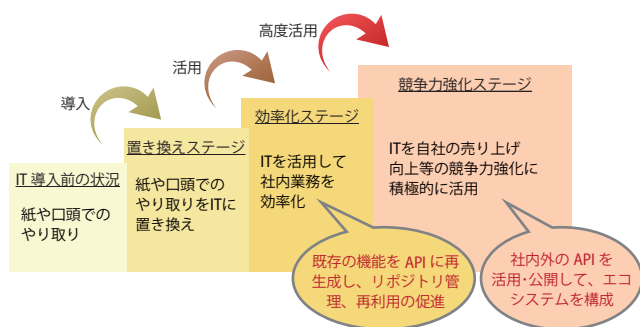
～次世代システムの構築に向けたアプローチ～



スマートフォンの爆発的普及により、スマートデバイスを活用したサービス提供やシステム構築が一気に加速しています。特に情報収集・コミュニケーションのための利用時間は、これまで首位を保っていたPCのブラウザ操作時間と逆転し、スマートデバイスが第一の情報操作窓口となっています。そのため、スマートデバイスを生かした便利で魅力的なサービスを発想・企画するスキルと、そのサービスをスピーディに提供可能とする仕組みが求められています。

効率的かつ迅速にサービスを立ち上げるには、「部品=API」を組み合わせ、作り込みを減らすことが有効です。本記事では、このAPIを管理・有効活用する「APIマネジメント」が、「攻めのIT※」を実現する1つのアプローチとなることを説明していきたいと思ひます。
※IT活用により、ビジネスに新しい価値を創出する、または市場競争力を強化すること

図1: "攻めのIT"とAPIマネジメント



求められる変化への対応力

情報端末の主流がスマートデバイスへと移り変わっているなかで、ビジネスを支えるITシステムが新しいデバイスへの対応を求められることは必然とも言えます。近年では、メールでのコミュニケーションに代わり、スマートデバイスによるSNSを使ったコミュニケーションが当たり前に行われています。つまり、利用者側はすでに新しいITとの関わり方を身に付けていると考えます。

ビジネスにおいても、このようなテクノロジーの変化の先を読み、提供するサービスをデバイスや利用用途・利用者にあわせて変化させていく必要があります。今まさに変化への対応力(柔軟性、迅速性)がITシステムに求められています。

目指すべき姿

顧客ニーズの変化に対応し、いち早く最適なサービスを提供していくには、顧客と接し、その変化を見ていることで現場から上がるアイデアとニーズを拾い上げ、企画・実現していく決断力と実行力が必要となります。

さまざまな選択肢のなかから、確実に顧客の心を捉え、ビジネスの成功に結び付く正解を探し当てることは非常に困難、かつ、勇気を伴います。まずは始めてみて、ユーザのニーズを取り入れながら、つど軌道修正を行い、正解へ近づけていくクリーンなアプローチも必要です。そのために、APIとUI/UXを明確に分離し、スピードや柔軟性が求められるUI/UXの開発に注力するアプローチが必要です。

APIマネジメントとは

自社のITシステムの持つ機能やデータをAPI (Application Programming Interface) として外部に公開し、社外からの利用を可能にすることで新たなビジネスチャンスや顧客(ユーザ)との接点を創出する取り組みが増えています。

Webサービス用のWeb APIとして公開し、利用を容易にするとともに、セキュリティやサービスレベルなどを管理し、サポートすることが「APIマネジメント」です。

表1: APIマネジメントの機能

機能概要	説明
API開発	既存社内資源を活用、再生成してAPI機能を提供するノンコーディングの開発環境
資源管理 (リポジトリ)	自社開発のAPIのみならず、外部提供のAPIも資源として均一な品質で一元管理し、利活用(再利用)を支援する
開発者ポータル	社外のAPI利用者へ利活用を促進するためAPI検索、ドキュメント、テスト環境を提供する
セキュリティ	API利用の認証、開発者の管理(制限)、外部からの攻撃への防御
モニタリング	利用実績、稼働状況、SLAに対する推移、課金機能など、分析に必要な情報の収集と可視化

図2: APIマネジメントと消費者

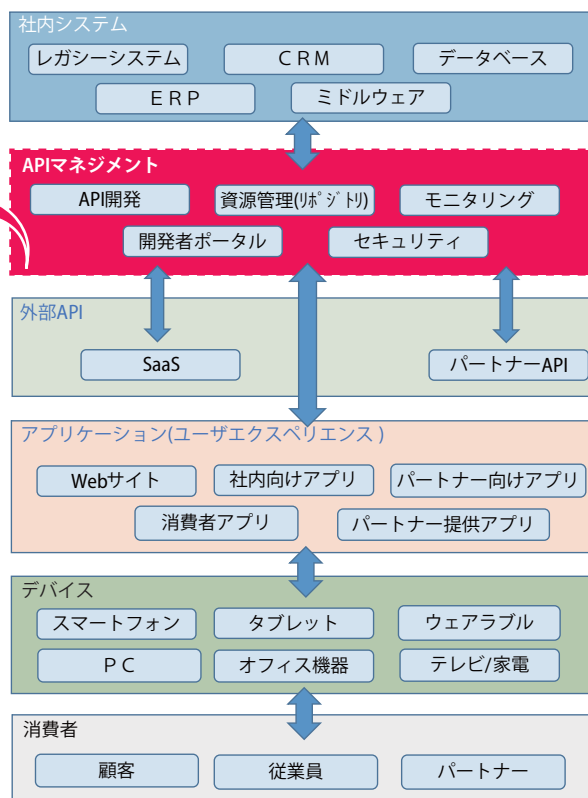
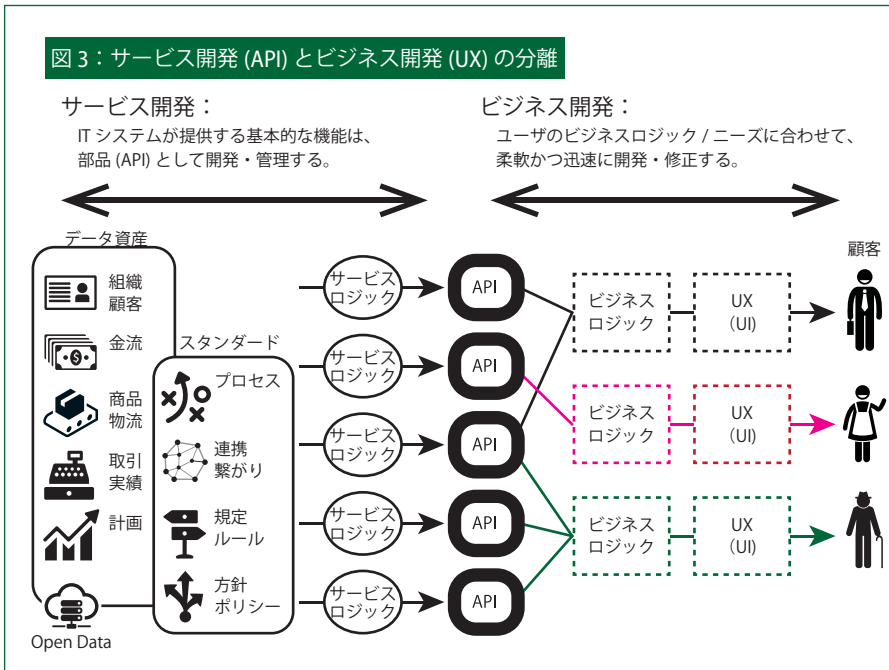


図3：サービス開発 (API) とビジネス開発 (UX) の分離



ビジネスモデル、ワークスタイルの変革へ

顧客体験向上、業務プロセスの自動化の2つ切り口で「APIマネジメント」がもたらす変革の事例を見てみましょう。

・顧客体験向上

スマートデバイスは、企業と顧客のエンゲージメント (絆・愛着) を築ききっかけとなります。スマートデバイスを通じて顧客に新しい体験 (便利、喜び、感動) を与えることで、顧客は有用性の高い情報を提供してくれます。例えば家計簿アプリを使うユーザは、すでに購買履歴、サービス消費の動向情報を家計簿サービスに蓄積しています。この情報を企業が入手することができれば、今までに無い試みができるようになります。

- ・顧客の詳細な購買動向を自社の製品・サービス改善のための研究資料とする
- ・顧客の位置情報やプロフィール情報と照らしあわせて、新商品/サービス、クーポン、キャンペーン、店舗などの情報を提案する

また、APIは、自社の情報を活用するだけでなく、パートナーとの情報授受やソーシャルな情報・機能の活用も行っていくことが肝要です。そのため、外部から提供されているサービスについても、データの意味や仕様を精査し、社内提供のAPIとあわせて、リポジトリで一元管理します。リポジトリで管理される資源は、必要に応じて社外公開も行います。

表2：API カテゴリ

カテゴリ	説明
社内サービス (自社が公開する API)	社内のデータや機能を社内外から呼び出し、活用、連携することを目的に自社のユーザやパートナーへ限定公開する API
パートナー提供サービス (パートナーが公開する API)	協業企業、SaaS と連携するためにパートナー向けに限定公開される API
ソーシャルサービス (公共事業などが公開する API)	郵便番号や地図情報に代表される公共性の高い情報の提供を目的に広く一般的に公開されている API

こういったAPIベースでの開発アプローチが、エンタープライズでは主流になってきます。APIは、セキュリティが保たれた状態であることは当然のことながら、いつ、どこから、どれだけの利用がされているのか利用状況もモニタリングできることが重要です。

図4：モニタリング

顧客	PC	Webサイト	API①
従業員	スマホ	社内アプリ	API②
	タブレット	消費者アプリ	API③
パートナー	ウェアラブル	パートナーアプリ	API④
⋮	⋮	⋮	⋮



モニタリング結果の情報を活用し、「いつ」、「どこで」、「誰が」、「どれだけ利用している/利用していない」を分析・評価します。次に提供するサービス、ビジネスロジック、UXに対する改善を実施します。

このように企業と顧客が双方向で協力することで新しい顧客体験を演出し、ビジネスの機会を創出できるようになります。これを支えるのがAPIマネジメントとなります。社内の商品情報、イベント情報などの既存データを外部連携するとともに、外部からAPIを通して提供される情報と組み合わせることで新しい価値を創出します。

・業務プロセスの自動化

営業マンや現地保守要員など、社外での活動を主としている担当者はスマートデバイスが主な操作端末となります。しかし、社内システムの業務情報は直接閲覧・操作できないため、ノート PC から VPN で接続、確認するなど、煩わしい対応を強いられています。

そんな時、API マネジメントを活用することで、

- ・スマートデバイスの持つ位置情報
- ・クラウド上のスケジュール情報
- ・社内システム上の顧客情報や拠点情報

などの情報を入手することができ、次の訪問先までの経路、目的地周辺の情報、ついでに顧客の購買履歴や、近隣の訪問候補リストまで見ることができます。社内システムで管理するデータや機能の重要性を鑑みれば、このように API をマッシュアップすることで、業務プロセスの劇的な変化を創出することも可能です。

ユニリタの提供する「APIマネジメント」は、『開発』『資源管理』『公開』『セキュリティ』『モニタリング』の5つの柱でしっかりと構築することで運用を支え、多様化する顧客ニーズに迅速に応えるとともに“攻めのIT”を強力に推進します。

担当者紹介



営業本部
ビジネスイノベーショングループ
セールスエンジニア
海老原 剛

メインフレームのオペレータから始まり、ITシステム運用のさまざまな現場業務を通じ、特に物流業務と帳票製品に関わる設計、開発、サポート、運用に永く従事してきました。これからもお客様のビジネス変革に寄与する提案をさせていただきます。

デジタルトランスフォーメーションに必要な技術とは? Vol. 2

～セキュリティも「まことに日に新たなり」～



前回のコラム「デジタルトランスフォーメーションに必要な技術とは? Vol. 1 ～クラウドサービスはまことに日に新たなり～」では、クラウドサービスは常に改善を繰り返す開発方法が必要であるという話をしました。今回は、おそらく皆さまが最も心配している「セキュリティ」の話です。

セキュリティを脅かす脅威といっても、幾つかの手口があります。「サイバー攻撃」、「標的型攻撃」、「リスト型攻撃」などです。「サイバー攻撃」とは、ネットワークで到達可能なサーバを攻撃して、システムダウンや改ざんを目的とする攻撃を言います。DoS攻撃などはこれにあたります。「標的型攻撃」は、特定の会社の内部情報を盗むために、コンピュータウイルスをメールなどで送り込み、ウイルスを使って内部情報を盗み出す方法です。最近では、比較的セキュリティの弱いと思われる子会社にウイルスを送り込み、さらにその子会社から親会社にメールを送り込むことで、グループ間のメールを装って安心させてからウイルスを送り込むといった手の込んだものがある様です。

今回テーマとしたいのは、「リスト型攻撃」です。ID/パスワードのコンビネーションを盗むことで、さまざまなシステムを乗っ取るやり方です。特に、情報システムではシステム毎に個別のセキュリティの仕組みを持つことが多いため、ID/パスワードが分散されてしまいます。この分散にセキュリティのリスクが内在しているため、気を付けなければなりません。

社内のセキュリティポリシー

皆さんは普段どれだけのシステムを利用しているでしょうか?メールや業務システム、ワークフローなど数えるときりがありませんが、すぐには思いつかない仕組みもあります。例えば、年に数回のリハールと広域災害が発生した場合にのみ利用される安否確認のシステムです。

皆さんの会社では、ISMSやPマークなどの個人情報についての認定を受けていると思います。その認定取得のために、システムのセキュリティとして、「パスワードは8桁で英数字と特殊文字を使ったコンビネーションにすること」や「パスワードは3ヶ月に1回変更すること」などのルールが決められているかと思います。では、安否確認のシステムもそのポリシーに従っているでしょうか? 私の知る限り、安否確認のパスワードを3ヶ月に1回変更している会社はごく僅かです。また、クラウドサービスの事業者を利用しているため、パスワードの桁数なども自社のポリシーに従っているのではなく、事業者のセキュリティポリシーに依存していることが多くなります。そのため、パスワードの桁数や変更に関するポリシーに従うか従わないかは個人のセキュリティに対する感受性に頼っているのが現状です。

この様な話に対して、「安否確認の仕組みは破られてもたいした影響は無い」と判断されるシステム担当者も中にはいらっしゃるかと思います。しかし、リスト型攻撃の恐ろしさは「そこ」にあります。



リスト型攻撃はなぜ問題なのか?

皆さんが使っているシステムのほとんどは、IDとしてメールアドレスまたは社員番号を利用していると思います。また、パスワードもおそらく同じ物を使いまわしていることでしょう。ある調査会社による

と、9割の人は同じパスワードを使いまわしていると言われています。

それでは、パスワードの使い回しを禁止するのか?もし禁止すると、

- 1) ノートにメモをする
- 2) パスワードの下桁桁かあるルールに従って変更する
- 3) 思い出しやすいパスワードを採用する

などの対応をします。メモすることは特に危険ですのでやめましょう。手帳が盗まれたり、落としたりした場合に、面倒なことになります。財布を落として、クレジットカード会社に電話をかけた経験のある人は、容易に想像することができるでしょう。

2)のパスワードの下桁桁かを変えるルールですが、自分も思い出せないダメなので、そのルールはある意味ロジカルなものになってしまいます。それが本当に安全かどうかは疑問です。

さて、先ほどの安否確認のシステムに戻りますが、確かに安否確認のシステムは破られてもたいした影響はないかもしれませんが、しかし、その部分のセキュリティ強度が弱いために、社員番号・メールアドレス・パスワードが全てハッキングされてしまったらどうなりますか? 社員全員のID/パスワードのリストが闇取引されてしまうかもしれません。そして、そのIDとパスワードは、他の非常に重要なシステムのID/パスワードのコンビネーションでもあります。IDがメールアドレスであれば、その会社のメールサーバにアクセスを試みて、リストの上から順番にログインを試みます。先ほどの統計でいくと、1000人の従業員のリストが漏れると、900名のメールアドレスが乗っ取られることとなります。



意外と怖いリスト型攻撃

リスト型攻撃はコンピュータプログラムでパスワードを組み立ててログインするのとは異なり、通常のWebサイトから人間のオペレー

担当者
紹介



成 亥 稔

執行役員
プロダクト事業本部
Be.Cloud グループ長

クラウド事業を担当している野球とゴルフ好きの2児の父親です。ゴルフのスコアはあまり良くなりませんが、最近飛距離が伸びました。iPhoneは2008年の3G発売以降、ずっと使っているガジェット好きの技術者です。

ションでログインされます。コンピュータプログラムにより、ハッキングされる場合は、ある特徴が浮かび上がります。例えば、「同一IPから1秒間に数千回以上のアクセスが発生する」や「昨日はロサンゼルスからログインしていたのに、今日は東京からログインしている」などです。この場合はハッキングが試みられていると気づくことができます。現在では人工知能（AI）が普及してきているため、AIにその判断を任せられることができるかもしれません。しかし、通常のアプローチでログインされると、ハッキング行為に気づきません。つまり、知らない間にメールを読まれていて、長い間その状況に気づかない場合があります。人手でやっているからたいした被害は無いであろうと思われやすいリスト型攻撃は、他の方法よりもむしろ危険であることが多いのです。

リスト型攻撃の対策1: 認証の分散を避ける

リスト型攻撃はID/パスワードのコンビネーションが盗まれることで、あたかも本人がログインしているかの様にシステムを利用します。これは、社内システムを利用する際、認識するサーバが多いこと（分散）が問題です。この問題は、認証を1箇所にすることで避けることができます。メールシステムや安否確認システム、受発注システムも1箇所で認証して利用することができれば、その1箇所の認証を強化することで問題のほとんどは解決します。IDとパスワードのコンビネーションをあちこちに分散してしまうと、一番セキュリティの弱いところが破られて、その影響が多くのシステムに及びます。お分かりになりましたでしょうか？これが「安否確認ぐらいはいいじゃないか？」が危険だということです。



リスト型攻撃の対策2: 認証サーバのセキュリティを高める

認証サーバを1箇所にすると、シングルポイントオブフェイラーが発生するのでは？という課題がでてきます。シングルポイントオブフェイラーとは、1箇所の障害で、多くの仕組みに影響を及ぼすことをいいます。「認証サーバがダウンすると、すべてのシステムが使えなくなる」や「認証サーバが破られるとすべてのシステムが利用されてしまう」などの問題です。もちろんそのリスクは否めませんが、逆に1箇所のセキュリティを高めることで、すべてのシステムが保証されます。認証サーバに何か問題がありそうなアクセスが来れば、止めてしまえば影響を及ぼしません。認証サーバにアクセスできる端末は社内の端末しかアクセスできない（グローバルIPで制限するなど）ようにすれば、それ以外の端末からはログインすらできないため、システムを乗っ取られることはありません。

最近では2段階認証の仕組みを利用しているところが大変多くなりました。例えば、ある端末からログインを試みると、その端末は登録されていないため、スマートフォンの電話番号にSMSで6桁の数字を送ります。この数字は10秒とか30秒とかで切れるワンタイムのPINコードであるため、その場ですぐに入力しなければ無効になります。SMSは自分の携帯やスマホなどで利用できますので、携帯やスマホが盗まれない限りは安全です。携帯やスマホが盗まれた場合は通常気がつくので、管理者に話してアカウントを一時的に利用できないようにしてもらえば、誰かにアカウントを乗っ取られることはありません。この端末は一度認証されると、次回からはこの処

理を行わなくてもいいので、利用上はそんなに不便になることもありません。普段利用する端末は数台ですので、その数台さえPINコードで認証をしておけば、全く問題なく利用することができます。

このようにして、1度認証サーバを1つにしてしまえば、その認証サーバのセキュリティを向上する手段はたくさんあります。2段階認証だけではなく、生体認証を使ったりすることも可能です。

お客様に安心してもらえるシステムの構築

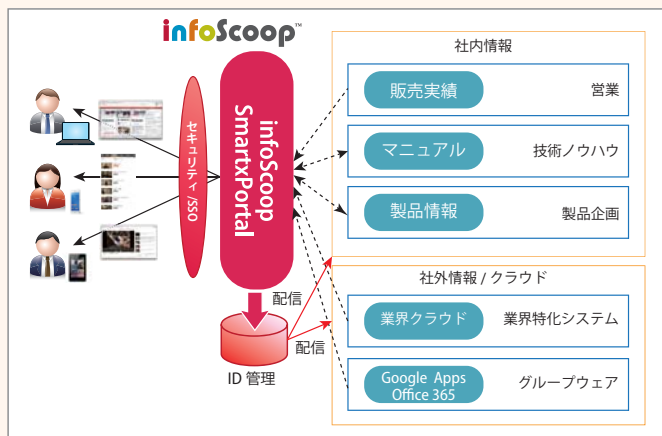
デジタルビジネスにおいては、お客様とのやりとりでシステムが必要になることが多くなるでしょう。この場合、お客様の認証を安全に進めることはお客様サービス向上につながります。もちろん、個人情報保護の観点でも重要です。認証の強度が高いかどうかは、その企業のブランド力にもなります。一度大きな問題を起こしたことがある企業は容易に信頼を取り戻すことができません。したがって、セキュリティは一度構築すればそれで終わりではなく、継続的に向上させる必要があります。前回のコラムでもご紹介した、「まことに日に新たなり」が必要となります。

リスト型攻撃の対策に効く！ infoScoopのセキュリティ関連ソリューション

セキュリティと一言でいっても単一の製品で全てを守れるものではありません。例えば、シングルサインオンの仕組みを利用しても、それは認証を1箇所にまとめることだけを意味しており、それぞれのシステムでの権限の管理やそのシステムでのアクセス許可を得るための認可についても検討する必要があります。権限管理においては、特に人事異動や退職に伴うセキュリティについて悩まれているお客様も多いかと思います。そんな時は、「infoScoop」のID管理を使って、分散されたシステムの組織や権限の情報を更新することができます。

クラウドを利用する場合、業界標準の認証プロトコルであるSAML、OpenID Connectや認可プロトコルであるOAuthを利用することでシングルサインオンを容易に実現することができますが、クラウドでも、標準プロトコルをサポートしていない事業者が多々見受けられます。この場合は、「infoScoop」のリバースプロキシによる代行ログインや、代行ログイン機能をもったポータル製品を使うことで、利用者に不便をかけずにセキュリティを確保することが可能です。

「infoScoop」のセキュリティソリューションは、ポータル、シングルサインオン（SAML / 代行ログイン）、ID管理をトータルで提供できることが特徴です。



● 詳しくは WEB ページへ！

infoScoop

検索

デジタルビジネスで勝ち抜くためのシステム運営ライフサイクルの実現 ITサービスマネジメントのプロセス改革(BPR)サービス

デジタルビジネスへの取り組みが進んでいますが、事業が成長すればするほど、システム運営の負荷が増大し、大きな課題となることが判明しています。



課題の例：

- ・システムの複雑化と運用負荷の増大により案件ごとに運用業務が属人化し、効率が低下する
- ・IT資産の全体が把握できなくなり、肥大化に気づかず、余計なコストを払ってしまう
- ・事業側とIT側の役割分担が上手くできず、ミスや取りこぼしが定期的にかかるようになる

上記課題の解決には、ITサービスマネジメントを取り入れ、正しいシステム運営方法へとプロセスの改革・標準化を行うことが有効です。「ITサービスマネジメントのプロセス改革(BPR)サービス」では、ITIL®の知見とプロセス改革の成功ノウハウを組み合わせて、実務への定着化まで支援します。

BPR効果例：

- ・デジタルビジネスのサービス品質向上
- ・ITコスト最適化、利益率の向上
- ・システム運営の効率化、工数削減

ITサービスマネジメントの専門性

業界標準「ITIL®」の豊富な活用実績

ITSMツールの提供
標準プロセス、
管理項目テンプレート

マネジメントレポート
分析と改善推進

ITサービスマネジメント

プロセス改革(BPR)

業務を改革し、
成果を出すノウハウ

ビジネス分析と、
ITSM方針の策定

現状業務の分析、
全体最適のプロセス設計

ステークホルダー
マネジメント、
チェンジマネジメント

成果の可視化、
新プロセスの定着化

サービス提供イメージ

Phase1 現状調査、要件定義、プロセス設計

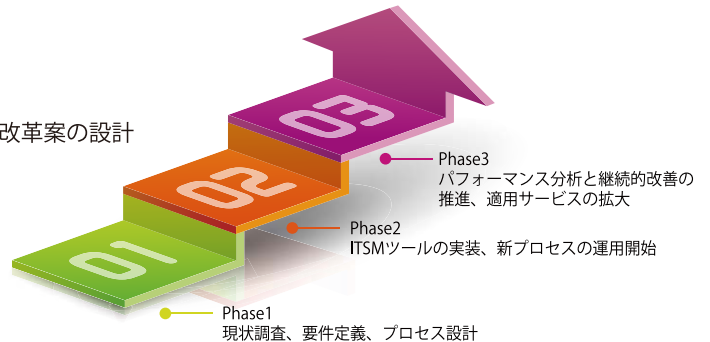
ITIL®トレーニング、ビジネス分析、関係者インタビュー
(業務プロセス・ルール・ツールの確認、問題点の洗い出し)、
ワークショップの開催(問題点レビュー、適用方針の検討)、プロセス改革案の設計

Phase2 ITSM ツールの実装、新プロセスの運用開始

ITSM ツールの実装支援(プロジェクトマネジメント、
詳細設計レビュー、要件の変更管理など)

Phase3 パフォーマンス分析と継続的改善の推進、適用サービスの拡大

実績データ分析、改善ポイント抽出、改善施策の実行と評価



- ・詳しくは、「UNIRITA ホームページ」をご覧ください。

ITSM BPR

検索

予告

IT部門の変革をリードする特設ウェブサイト 「it's YOUR turn!」を9月公開予定

ビジネスのスピードはどんどん速くなり、社会インフラとなったITのパラダイムシフトがビジネス環境を一遍させています。既存の延長ではなくなったビジネス環境では、新しいテクノロジーを学び、ビジネスを変革しなければなりません。

インフラであるITをもとに変革を進めるには、IT部門の力が必要です。ユニリタでは、このIT部門の変革に必要な情報を集めた特設ウェブサイト「it's YOUR turn!」(IT部門の出番です)を立ち上げます。

●掲載予定コンテンツ

- ✓ ホラン千秋さんが聞く! IT部門の変革って? (仮)
- ✓ 変革に役立つ eBook などの資料ダウンロード
- ✓ 関連セミナー、イベント予定、開催レポートなど



～ホラン千秋さんも登場!～



- ・ユニリタ特設 Web サイト「it's YOUR turn!」は 9 月公開予定です。ご期待ください。

400名超が参加！充実の講演内容に日常にはない刺激を得る

●「第10回システム管理者感謝の日イベント」開催報告

「デジタル変革」をテーマに、3つの講演と展示コーナーおよび情報交換会と、さまざまな企画のイベントを開催しました。当日は小雨が降る中、419名の皆さまにご参加いただき、誠にありがとうございました。来年も「ビジネスを支えるシステムを提供している」皆さまに感謝すると共に、新たな取り組みを後押しするイベントを開催いたしますので、ぜひご参加ください。

■講演ダイジェスト

●基調講演「デジタル変革時代に求められるシステム管理者の役割」

株式会社アイ・ティ・アール 生熊 清司氏

従来の企業ITの進展は成熟段階に向かっており、今後は社会・産業のデジタル化が急速に進化する時代において、「システム管理業務は従来の社内システムを安定稼働させるだけでなく、ユーザのニーズに沿い、システムの統合と再構築に対するリーダーシップを発揮し、競争力の高いIT基盤を供給する社内サービスプロバイダーへの転換が求められる。」という提言をいただきました。



●セッション1「VRは本当にくるのか」

株式会社シーエスレポーターズ 三上 昌史氏

VR制作実績で得た気づきとして、「ツールや環境によるVR体験レベルの存在と、それに伴って感想の違いがある」「VR技術はゲーム以外にも適し、疑似体験をどう生かすのかが重要である」「映像データ容量は大きく、今後益々インフラが整うことが、VR事業が発展する鍵となる」ということをお話いただきました。



●セッション2「コンテンツの変化はITの変化～バンダイナムコエンターテインメントにおけるデジタル変革～」

株式会社バンダイナムコエンターテインメント 仁木 貴之氏

ソーシャルゲームの事例をもとに、新しいビジネスモデルに対応したITサービス提供体験談をお話いただきました。失敗体験を経て得られた「時には勇気をもって、今までやってきたことが通用しなくなったと認めることも必要」、「常にアンテナを張り、変革が必要になった時のための地力をつけておく」といった言葉は来場者アンケートにも書かれるほど共感を頂きました。



●詳しくは、「システム管理者の会ポータルサイト」をご覧ください。

システム管理者の会

検索

研究グループ合同合宿開催！全国で222名が参加！

今年度のユーザ会は全国で30の研究グループが発足され、5月から活動を始めています。そんな中、全国で合同合宿が開催しました。

合宿は、長時間集中して議論していただき、研究を深めることを目的に、業務から離れた環境にて一泊で開催されます。今年度は東日本情報活用研究会、東日本システム運用研究会がそれぞれ合同という形で、中部と西日本はそれぞれ情報活用とシステム運用の垣根を越えて合同で合宿を開催しました。合宿を研究グループ間で開催することで、他のグループの活動状況を知ることができ、グループ間で刺激になり、グループ間で切磋琢磨する土壌の醸成に繋がります。

各グループとも、合宿での議論を通して研究とメンバ同士の絆を深めることができましたと思います。

東日本情報活用研究会合同合宿 7/15-16 石和温泉 華やぎの章甲斐路

東日本システム運用研究会合同合宿 7/15-16 鬼怒川 ホテル三日月

西日本合同合宿 7/8-9 京都 お宿いしちょう

中部合同合宿 7/8-9 三河 民宿鈴音館



参加者の声

久しぶりに腹を割った本音の話し合いができました。自分たちのグループがどうありたいかや研究テーマへの根本的な問い直しなど、全員が主役となり議論し、チームとしての一体感を深めることができました。また、他の研究メンバとも交流でき皆同じような悩み、想いを持っているのだと共感や刺激を受けました。

合同合宿は、自分のチームだけでなく、他のチームと交流を深めたり、意見を聞くチャンスでもありました。私達はこのチャンスを逃す手はないと事前にアンケートを作成し、お酒を飲みながら交流を図り、皆さんの意見をお聞きする事ができました。有意義な時間を過ごす事ができましたし、忘れられない思い出になったと思います。

研究活動開始直後は「合宿では何をやるのだろうか」とドキドキしていましたが、合宿の目標がはっきりすると、合宿が楽しみになっていました。2日間の合宿はあっという間で、討議も充実していましたが、なによりも、全員でよく話し、同じ時間を共有できたことで、メンバのチームワークが強くなった感じがしています。

ファシリテーターとしてメンバの表情などを見て全員が納得の上で会議を進められているか、本当に意見を言えているか確認する必要があります。しかし、私は進行で手一杯でそこまで気が回りませんでした。その事に身を持って気がつくことができてもとても勉強になりました。引き続き経験を積み3月の発表に向けてメンバーをまとめていきたいと思っています。

加速するクラウド化が起こす運用現場のカオスから ITシステム運用管理者を救済

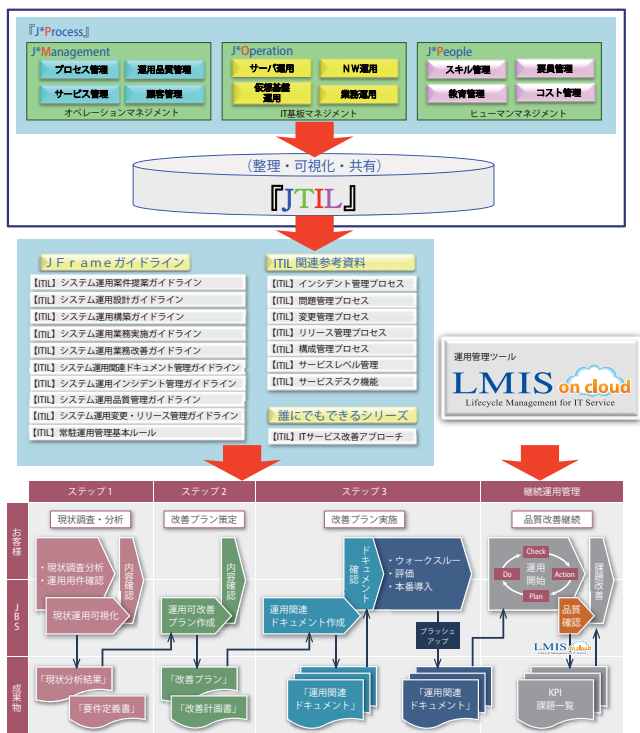
日本ビジネスシステムズ株式会社 (JBS) の提供する「ITシステム運用改善支援サービス」は、ITシステムの運用品質を可視化・分析して課題点・問題点を抽出し、お客さまの運用環境に最適な改善プランを策定、運用の改善を積極的にご支援いたします。JBSは、「すべてのリソースはお客さまのご満足のために」という「Customer First」の基本的な考え方に基づいて、情報系インフラの構築から、アプリケーション開発、システム保守、運用までをワンストップで提供しています。

ユニリタとの「LMIS on cloud」販売パートナーシップによる効果

JBSの提供する「ITシステム運用改善支援サービス」では、お客様の運用環境に合わせてITシステム運用の最適化を実現することを心がけています。サービスを提供する際は弊社運用フレームワーク「JTIL」(JBS Technology Infrastructure Library)の基本概念であるITシステム運用関連情報の「整理」、「可視化」、「共有」をどのように実現するかが重要なポイントになります。

この3つの要素を各運用プロセスで容易に実現できる「LMIS on cloud」を提案できることは、JBS企業理念「Customer First」の実現に向けて非常に心強い武器の一つになっています。

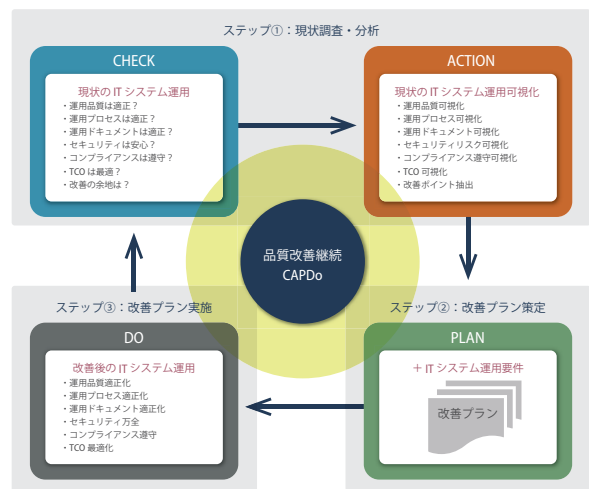
「JTIL」イメージ



JBSの「ITシステム運用改善支援サービス」とは

ITシステム運用の要件に従い、現状調査・分析を実施し、JBSの豊富な経験とナレッジを効果的に活用し、最適なITシステム運用改善の実現に向けて、プロセス整備、ドキュメント化などの各種作業をご支援いたします。

提供イメージ



JBSの強み

- ITシステム運用に関わる多彩なナレッジ、SierとしてITシステムに関わる技術力**
蓄積されたナレッジと「ITIL」、「ISO20000」、「ISMS」を融合したJBS独自ITシステム運用フレームワーク(JTIL)と経験豊かなコンサルタントによりITシステム運用要件に即したオンデマンドのいいとこ取りの対応が可能です。
- JBSの豊富なメニューとの連携**
JBSの各種サービスのミックスバリューの提供が可能です。

問い合わせ

日本ビジネスシステムズ株式会社
システムインテグレーション統括本部 マネージドサービス本部
運用企画部
〒105-6316 東京都港区虎ノ門1-23-1 虎ノ門ヒルズ森タワー16F
Tel: 03-6772-4000 Fax: 03-6772-4001
<http://www.jbs.co.jp/>

株式会社ユニリタ www.unirita.co.jp



本社	〒108-6029 東京都港区港南2-15-1 品川インターシティA棟	TEL 03-5463-6383
大阪事業所	〒541-0059 大阪市中央区博労町3-6-1 御堂筋エスジービル	TEL 06-6245-4595
名古屋事業所	〒451-0045 名古屋市中区名駅3-9-37 合人社名駅3ビル(旧48KTビル)	TEL 052-561-6808
福岡事業所	〒812-0013 福岡市博多区博多駅前2-2-2 博多東ハニービル	TEL 092-437-3200

ユニリタグループ 株式会社アスペックス / 株式会社ビーティス / 株式会社データ総研
備美必(上海)軟件科技有限公司 / 株式会社ビーエスピーソリューションズ
株式会社ユニトラント

※ 本誌掲載の会社名、製品名は各社の登録商標または商標です。

※ 掲載されている内容については、改善などのため予告なく変更する場合がありますので、ご了承ください。