【講演レポート】ISMS・ITSMSウェビナー

ディスカッション「ITサービスの効果的な運用とその実践」

株式会社WellGo　代表取締役 兼 CTO　楠本　拓矢氏
ＳＯＭＰＯシステムズ株式会社　ITサービス本部シニアアドバイザー　岸　正之氏
ISMS専門部会　主査、ITSMS専門部会　委員
株式会社アズジェント セキュリティ・プラス ラボ　シニアフェロー　駒瀬　彰彦氏
ITSMS専門部会　副主査
株式会社ヒルアビット　代表取締役　黒崎 寛之　氏
JIPDECセキュリティマネジメント推進室　室長　成田　康正

2021年3月10日に開催されたISMS・ITSMSウェビナー「効果的なITサービスの設計から運用の仕組み～安全で安定したITサービス運用のために～」では、ISMSクラウドセキュリティ認証取得の取組みについて、株式会社WellGo　代表取締役 兼 CTO　楠本　拓矢氏、ITSMS認証の効果的な運用についてＳＯＭＰＯシステムズ株式会社　ITサービス本部　シニアアドバイザー　岸　正之氏にそれぞれ講演いただいた後、ISMS専門部会主査　駒瀬　彰彦氏、ITSMS専門部会　副主査　黒崎　寛之氏を交えたディスカッションで、企業が抱える課題や効果的な認証運用方法等についてお話を伺いました。

本レポートでは、JIPDEC事務局が要約した当日のディスカッション内容をご紹介します。
（当日の全プログラムの内容はこちらをご覧ください）

ISMSクラウドセキュリティ認証とは

ISMSクラウドセキュリティ認証は、JIS Q 27001および27017に基づく、クラウドサービスを扱う事業者に対するISMS認証です。ISMSの認証取得が前提となっており、ISO/IEC 27017はガイドラインという位置づけになります。

認証を受けるにあたっては、まずクラウドセキュリティの適用範囲を決め、次にクラウド固有のリスクを特定して、評価・対策を行います。この時に、リスク対策としてISO/IEC　27017を用いることになります。詳細については、「ISMSユーザーズガイド追補」（発行：JIPDEC）で解説していますので、ぜひご参照ください。

認証の対象となるのは、クラウドサービスプロバイダー（CSP）、クラウドサービスカスタマー（CSC）双方で、どちらか一方、または両方の立場で認証を取得することができます。また、CSPが認証取

得する場合はISMS認証と異なり、拠点ごとではなくサービス（提供形態）ごとに取得することになります。現在、認定機関である(一社)情報マネジメントシステム認定センター（ISMS-AC）の認定を受けたISMSクラウドセキュリティ認証機関は13組織、実際の認証取得組織は215です。

なお、ISMSクラウドセキュリティ認証の他には、ISO/IEC 27701に基づくプライバシーマネジメントに関する認証（ISMS-PIMS認証）が2020年より開始されています。こちらも、ISMS認証を取得していることが前提となります。

ディスカッション

ITSMS、ISMS導入・運用のポイント

Q:マネジメントシステムを導入・運用しようとしても、トップマネジメントの関与が希薄で、推進力を失ってしまうという声はたびたび聞かれます。経営層を巻き込んで、ITSMS、ISMSを効果的に導入・運用していくためのポイントはどのようなことでしょうか？

A: SOMPOシステムズの場合、トップマネジメント層の意識が非常に高く、自社の社会的使命とITSMSを同じレベルで位置付けて構築することができています。また、教育の機会においても、経営層がメンバーに語る場面を作ることで、メンバーの意識向上、活動の活性化につながっています。

経営層を巻き込むためには、見せ方の工夫も必要だと思います。ISO/IEC 20000は、サービス品質やコスト等、経営層がコミットメントしているものを取り込むことができます。経営層の関心事とリンクさせることによりISO/IEC 20000が企業経営に貢献するものとして理解・認識され、積極的に関与せざるを得ない状況を作ることもできます。

A:WellGoは、スタートアップ企業なので、不祥事・情報流出等が起こればビジネス自体が頓挫してしまうという強い危機意識を持っています。このため、単にISMSを構築するだけでなくしっかりと運用していかなければ会社の存亡に関わるということを、経営者が自ら発信し全社で危機意識を共有しています。ISMSを業務システムの中にしっかりと組み込んでいくためには、経営層の力が必要となるので、現場からも経営層と危機意識を共有できるようなアピールが必要だと思います。

Service Level Objective（SLO）による取組み

Q:今回取り組み事例の中でSLA、SLOの活用といった点もお話いただきました。ISMSご担当者には、SLOになじみがない方もいらっしゃると思いますが、部門管理目標を策定、部門間の役割分掌の明確化といったものととらえてください。その上で、各部門においてマネジメントシステムが形骸化しないような試みもされているというお話でしたが、具体的にはどのような指標を作り、どのように測定しているのでしょうか？

A:SLAは賠償等法的な部分に関わってくるのでどうしても安全な数値になりがちになることから、SOMPOシステムズでは、よりチャレンジングに取り組むため「事業会社の業務を止めない」という大前提の中でSLOの数値を設定しています。例えば、あるオンラインサービスの可用性が99.9とすると、1年間に停止できるのは10数時間となります。この10数時間を、そのサービスが持つリスクの低減策を明確にし、緊急対応可能な体制を組み、要員のスキルを向上させることで、ギリギリのところまで削減し、99.99に近づけようと取り組むことができる、これがSLOの長所であると思っています。

A:WellGOでも、SLAは遵守できない場合に法的リスクがあるため、SLOを選択しています。SLOの数値は過去の実績に基づいて算出しています。１年目はバッファを持った数値としていましたが、その後毎年取組みと見直しにより、より目標を高い数値にしています。お客様から要請があった場合は実現可能性を検討した上で、すべてのお客様に適用するようにしています。

Q:SLOを設定しても、測定頻度が少ないと形骸化してしまうことも考えられます。実際にSLOの測定頻度はどの程度としているのでしょうか？

A:SOMPOシステムズでは、毎月お客様との間で開催するITサービス委員会においてSLO、KGI、KPIも含む重要指標の結果を報告しています。また、その場でお客様とコミュニケーションを取り、需要予測や今後のイベント等の情報を得て次のサービスにつなげる取組みをすることで、サービス形骸化を防止しています。

A:WellGoでは、自発的に見直すのはISMS認証の更新時期が一番大きなタイミングとなります。その他に、特に大口のお客様と契約する場合などは、お客様がすでに持っている指標にどこまで合わせられるかを検討して指標を見直す場合もあります。

DXに向けて

Q:今後DXを進めつつ、従業員の満足度を高めていくためにどのようなことが考えられますか？

A:ISO/IEC 20000の活動の中にDXの取組みを取り込んでいくことができると考えています。データやデジタル技術を活用し新たなビジネスモデルが作られる時、そこには必ず顧客がいる、つまりサービスができるということです。ISO/IEC 20000はレガシーシステムを管理するものではなく、サービスを管理するためのものなので、十分に活用することができると考えています。

A:WellGoで社員に配布しているセキュリティハンドブックにはペーパーレス化への取組みも含まれています。セキュアな方向へ進もうとするとき、紙をなくしデジタル管理をしっかり行うことがセキュリティ水準を向上させるキーだと考えています。セキュリティを向上させようとすれば、ペーパーレス化は進み、デジタル化することで業務効率も上がり、結果としてDXにつながります。ISMSの取組みを通じて、古い体制・非効率な業務を刷新していかないとセキュリティは担保できないとアピールしながら社内変革を進めていきたいと思います。

以上

株式会社WellGo　代表取締役 兼 CTO　楠本　拓矢氏

大阪大学大学院基礎工学研究科修了。日本アイ・ビー・エム株式会社を経て、2006年野村證券株式会社に入社。金融工学研究センターにてマーケット・マイクロストラクチャーに携わる。2009年よりエグゼキューション・サービス部にてアルゴリズム取引システムの設計・開発、データ分析、AIプロジェクトに従事。2017年に社内ビジネスコンテストに入賞し、2019年に株式会社WellGoとして独立。

ＳＯＭＰＯシステムズ株式会社
ITサービス本部　シニアアドバイザー　岸　正之氏

ＳＯＭＰＯホールディングス・損害保険ジャパン社のＩＴ戦略会社であるSOMPOシステムズ社のITサービス本部に在職し、主に損害保険ジャパン社のITガバナンス、ITサービスマネジメントシステムにおけるサービス管理責任者として企画・統制、さらに部門の風土改革・人材育成の推進役として各種施策の企画・立案・推進を担当。現職のITサービスマネジメント／風土改革・人材育成のほか、経営企画・人事部門を歴任するなど、幅広い経歴を持つ。

ISMS専門部会　主査、ITSMS専門部会　委員
株式会社アズジェント　セキュリティ・プラス ラボ　シニアフェロー
駒瀬　彰彦氏

暗号技術を用いた個人情報・機密情報保護、認証システムの設計、開発などを経て、主にネットワーク・セキュリティに関連するコンサルティング、情報セキュリティ主任監査人としてセキュリティ監査業務、ERMアドバイザーとしての業務に従事。
現在、シニアフェローとして、情報セキュリ ティ管理、クラウドセキュリティ、ITサービス管理、事業継続管理等、リスクマネジメントの専門家として、関連する各団体の運営委員、主査、作業部員として、基準やガイドラインの策定に参画し、組織の取組むリスクマネジメントのレベルの向上・改善活動の支援を行っている。

【主な著書/共著】
•クラウドサービスを取り巻く環境の変化と情報セキュリティについて
（日本規格協会　標準化と品質管理　2020年9月　Vol.73）
•新ISMS規格を有効に活用するために （アイソス　2017年10月~2018年3月号）
~リスク対応の基礎からクラウド・個人情報保護マネジメントまで~
デジタルトランスフォーメーション時代を生き抜くために
•個人情報保護の運用と対策（オーム社）
•情報セキュリティガバナンス 経済産業省情報セキュ リティ政策室 編
•連載 1 ～10 情報セキュリティマネジメントシステム基 礎講座（@IT）
参照： http://www.atmarkit.co.jp/fsecurity/ rensai/guide01/guide01.html
【主な資格】
•公認情報セキュリティ主任監査人（CAIS）
•CISSP
【主なプロジェクト活動】
•セキュリティマネジメント推進会議委員(JIPDEC)
•ISMS技術専門部会　主査(JIPDEC)
•ITSMS技術専門部会　委員(JIPDEC)
•クラウドサービスのセキュリティ対策に係る管理基準に関するWG 委員(IPA)
•草の根サイバーセキュリティ運動全国連絡会(Grafsec)

ITSMS専門部会　副主査
株式会社ヒルアビット　代表取締役　黒崎 寛之　氏

某SIerにてデータセンター運営、ITアウトソーシング事業の責任者を経験。「要点解説ITILがわかる」、　「要点解説ITサービスマネジメント」（共に技術評論社）の著者であり、現在は各種プロジェクトマネジメント対応、運用業務の改善・組織変革の支援・ITIL®実装・ITSMS、BCMS、ISMS及びクラウドセキュリティ等認証取得に関するチーフコンサルタント、関連教育コースの講師など、幅広く活動するとともに、JIPDEC ITSMS技術専門部会のメンバーとしてISO/IEC 20000の普及・利用促進のための活動も行っている。

■資格
itSMF認定 ISO/IEC20000 コンサルタント/itSMF認定 ISO/IEC20000 審査員/PeopleCert認定 ITIL 講師/EXIN認定 ISO/IEC20000 講師/BSIグループジャパン認定 ISO/IEC20000 講師/IRCA認定 ITSMS審査員／QMS審査員/ITIL Managing Professional/ITIL Expert/ITI

L Practioner/ITSM Specialist/ITSM Professional Support Certificate of IT Service Management/According to ISO/IEC20000

本内容は、2021年3月10日に開催されたISMS・ITSMSウェビナー「効果的なITサービスの設計から運用の仕組み～安全で安定したITサービス運用のために～」でのディスカッション内容を取りまとめたものです。