

【講演レポート】ISMS・ITSMSウェビナー

大手企業の社内ビジネスコンテストから独立した
SaaSスタートアップ企業のISMS/ISO/IEC 27017認証*取得事例
～ISMS/ISO/IEC 27017認証取得による社会的な信頼の獲得について～

株式会社WellGo
代表取締役 兼 CTO 楠本 拓矢氏

本日は、株式会社WellGo（以下、WellGo）立ち上げからISMS/ISO/IEC 27017の認証*に至った経緯と認証取得の過程で取り組んだことなどをご紹介します。

* ISMS（ISO/IEC 27001）/ISO/IEC 27017に基づくISMSクラウドセキュリティ認証

ISMS（情報セキュリティマネジメントシステム）とは

ISMSとは、情報セキュリティを管理するための体系化された手法、仕組みのことです。ISMSの認証基準であるISO/IEC 27001には、情報セキュリティに関するリスクや資産などを適切な体制のもと管理すること、また、確立したISMSの仕組みを運用し、継続的に維持、改善していくことが求められています。

具体的な雛形や見本は基準には規定されておらず、どのようにしてISMSを確立するかは、各企業がそれぞれの組織にあった形で考えていくこととなります。

ISMS、ISO/IEC 27017の認証取得

取得の背景（環境の変化と潜在的なリスク）

WellGoは独立前、野村ホールディングス株式会社（以下、野村HD）の社内ベンチャーとして業務を行っていました。その間は、野村HD全社で統一されたセキュリティポリシーが強制的に適用され、システム開発やウイルス対策なども常に万全な状態で業務を行うことができていました。

しかし、独立後はその高度なセキュリティポリシーの強制適用がない状態で業務を開始することになり、今まで意識せずとも担保されていたセキュリティに関して、意識して守り管理する必要に迫られました（図1）。



独立前後の環境の変化と潜在的リスク

カテゴリ	野村證券 社内環境 (全社で統一されたポリシーを強制的に適用)	独立後 (セキュリティポリシーの強制適用がない)
メール	送信時の添付ファイルのパスワードチェックなど、メーラーにポリシーが強制適用されている 送信メールは上長にBCCで転送されている	G Suiteになり、Gmailの制約以外はほとんど制限なし <small>誤送信するリスク</small>
インターネットアクセス	許可されたURL以外はProxyサーバでブロック	制限なし どのURLでもアクセス可能 <small>顧客情報をどこかに公開してしまうリスク</small>
PC	OSはWindowsのみ。全社員が同じバージョンを利用 Admin権限なし（権限が必要な場合は申請が必要）	ノートPCやOSは自由に選択可能 <small>P2Pなど不正なソフトウェアを導入してしまうリスク</small>
ウイルス対策	デフォルトでPCにインストールされている	OSデフォルトのものを使用 <small>アップデート未適用による最新マルウェア感染リスク</small>
電話	部署によっては通話記録など	制限なし <small>内部情報や顧客情報を話してしまうリスク</small>
システム開発（開発者）	変更管理/インシデント管理など、全社整備された社内システムを通じて行う	自分たちで整備 <small>セキュリティの担保に必要な管理ができないリスク</small>

知識がなくても無意識のうちに
セキュリティが担保される

意識してポリシーを守る必要がある
→ ISMSでリスク管理

図1. 独立前後の環境の変化と潜在的リスク

認証取得を意識したきっかけ

WellGoは、野村HDおよび野村総合研究所が共同で実施したビジネスコンテストでの入賞をきっかけに2年以上のサービス社内開発・PoCの後に独立した企業であり、そうした背景や保有する技術力などに対する自負もあり事業はすぐに軌道に乗ると考えていました。

しかし、実際には企業の成り立ちや出資元が考慮されることは少なく、セキュリティ認証を持っていない当社は取引先の候補にあがることも少ないというのが現実でした。

そこですぐにセキュリティ認証の取得に向けて動き始め、プライバシーマーク同様、認知度のあるISMS認証の取得が最初に決まり、同時にクラウドの利用及び提供を行っているためISMSクラウドセキュリティ認証の取得に向けても動き始めました。

認証の種類「公式認証」と「プライベート認証」

認証には、ISMS-ACの統一基準に則ったうえで、ISMS-ACの認定を受けた審査会社（認証機関）によって認証される「公式認証」と、ISMS-ACの認定の有無に関わらず各審査会社の裁量によって審査が行われ、審査会社の名前で認証が出される「プライベート認証」の2種類があります。対外的なアピール力を鑑みると「公式認証」の方が高いと考えられます。

認証取得までの流れ

ISMS認証の取得に向けては、まずは組織の中で情報セキュリティを担保できる体制・手法（ISMS）を確立させることとなります。それを適切に維持・管理するPDCAを回すことができはじめて、審査

会社の選定、審査のステップに進むことができます。ただし、本来はセキュリティ認証を取得する・しないに関わらず、セキュリティを担保する仕組みは組織内にあって然るべきもので、認証取得を目的とした取組みではないということを理解していただきたいと思ひますし、WellGo社内でも意識として徹底させました。

WellGo が構築したISMS

認証取得の際は、以下のドキュメントを作成しました。

1: ISMS

- 情報セキュリティ方針（Web公開）、情報セキュリティマニュアル等の各種マニュアル、適用宣言書等の、各種文書
- 文書管理台帳、年間実施項目管理表（PDCA管理）、情報資産管理台帳、リスク管理表、マネジメントレビュー記録、BCP試験実施記録、委託先管理台帳等、各種台帳等の、各種台帳
- 監査計画書、監査チェックリスト、監査報告書、指摘事項管理表等の、内部監査/審査資料
- 組織図、入社時・退社時における誓約書、入社退職時チェックリスト等の、会社組織に関する資料

2: ISMSクラウドセキュリティ

- ISMSの適用宣言書と対をなすベースライン管理表、対外用セキュリティホワイトペーパー

ドキュメントの運用と併せて、効率的な維持・管理という点を考慮してさまざまなツールの導入を行うなど運用面でも工夫をしました。課題管理やインシデント管理、eラーニングや法令管理のシステムのほか、クラウド上でドキュメントの安全な管理などが行えるよう環境を整え全社での利用を徹底しました。ツール自体を業務フローに組み込んでしまうことで、全社員がISMSの管理を日常的に意識することができるようになったと考えています。

ISMS確立までの時間

通常の業務と並行しながら、ISMS認証を取得する（システム整備から社内ルール徹底まで）には、約8か月を要しました。実際に認証取得を経験してみた結果、基盤のない状態からの取得には大変時間と労力とコストがかかるため、コンサルティング会社への委託も選択肢のひとつだと思います。

まとめ

最新のシステム技術の追求（攻め）と、ISMSの確立（守り）は異なるということを理解していただきたいと思ひます。

情報セキュリティを担保するシステムを導入することで、システム開発において制約が入ることも想定されますが、攻めと守りの両輪をバランスよく運用していく必要があります。認証取得に向けて、実際のPDCAを見直してみることで、そして組織として適切に情報セキュリティを管理・担保する体制を整えることが何より重要となります。

今後のSaaS企業にとって、セキュリティの認証取得は必須です。ISMSをしっかりと確立することで社外へも自信をもって示すことができるようになり、WellGoでは、セキュリティに関する社内全体の意識、知識レベルの向上が見られるなど大変よい変化が見られました。セキュリティの認証取得による社会的な信頼の獲得がビジネスを進める上で優位に働くことは間違いないと思っています。

株式会社WellGo 会社概要

2019年1月に野村HDの社内ベンチャー一期生として設立。全従業員中、エンジニアの比率が56%を占める技術者集団。SaaS型、BaaS型顧客を中心に事業を展開している。人生100年時代を見据え、有形資産に限らず無形資産、特に健康資産の最大化を目指すWebサービスとして「職域向け統合型クラウド健康経営サービス」、「職域向け統合型クラウド産業保健向けサービス」、「健保向け統合型クラウド保健事業サービス」の3つの柱を中心に幅広いヘルスケア業務をカバーするオールインワンのヘルスケアプラットフォームサービスの提供を行っている。

- ・株式会社WellGo <https://wellgo.jp/>



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年よりエグゼクティブ・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。

以上

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～」での講演内容を取りまとめたものです。