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

株式会社WellGo – 会社概要

設立

2019年1月

野村HD 社内ベンチャー1期生

SaaS型顧客数/BaaS型顧客数(1)

69社/685社

エンジニア比率

56%(役職者除く)

総データ人数(2)

392,633名

(1)(2) 2020年度ベース＋2021年の4月までにWellGoのデータベースに保存予定の人数データ

人生100年時代　WellGoが目指す姿

人生100年時代、有形資産や無形資産を全く気にすることなく、一人ひとりが健やかに暮らせる社会インフラを構築します

有形資産

価値測定**可能**なもの

貯蓄

不動産

有価証券

有形＋無形資産のバランス

有形＋無形資産
ポートフォリオマネジメント
が重要

「ウェルビーイングな人生の提供」

無形資産

価値測定**不可能**なもの

家族

友人

スキル・知識

肉体的・
精神的健康

株式会社WellGo - サービス概要

職域向け統合型クラウド健康経営サービス

- **統計分析機能**
  - ・勤怠統計、定期健診・問診統計、医療費統計、ライフログ統計など
- **運動促進動機付け機能**
  - ・スマホによる運動・食事・睡眠・体温記録
  - ・インセンティブポイント付与・交換
  - ・イベント機能
  - ・ゲーミフィケーション機能（開発中）
- **カスタムレポート**
  - （健康経営度調査票に必要な統計情報出力機能）

健保向け統合型クラウド保健事業サービス

- **ハイリスク・アプローチ機能**
  - ・特定保健指導やがん健診管理機能
  - ・本人介入機能
  - ・オンライン特定保健指導（開発中）
- **ポピュレーション・アプローチ機能**
  - ・スマホによる運動・食事・睡眠・体温記録
  - ・インセンティブポイント付与・交換
  - ・イベント機能、クイズ
  - ・ゲーミフィケーション機能（開発中）
- **統計分析機能**
  - （データヘルス計画に必要な統計情報出力機能）

職域向け統合型クラウド産業保健向けサービス

- **産業保健機能**
  - ・健診事後措置
  - ・事後介入機能（２次健診介入）
  - ・保健指導履歴・産業医意見書各種
- **ストレスチェック機能**
  - ・ストレスチェックアンケート57問・80問
  - ・集団分析結果と保健師サポート※
  - （※別途、提携先の（株）ドクタートラストに依頼）
- **各種アンケート機能**
  - ・健康意識調査、プレゼンティーズム入力
  - ・各種カスタマイズアンケート、クイズ

ヘルスケア業務を幅広くカバーする
オールインワンヘルスケアプラットフォーム

SaaS

株式会社WellGo – [沿革] 野村ビジネスコンテスト

年1回の社内ビジネスコンテストに応募し入賞

※野村HD及び野村総合研究所 共同で実施

ビジコンから生まれたチーム

CTO 楠本　拓矢
TAKUYA KUSUMOTO

【ビジコン当時の業務】
機関投資家向け
アルゴリズム取引システム/AI
設計・開発

CEO 原田　大資
DAISUKE HARADA

【ビジコン当時の業務】
機関投資家向け
アルゴリズム取引システム/AI
企画

2年以上のサービス社内開発＆PoCの後、
平成31年1月17日　株式会社WellGo として独立

独立直後の社会的信頼獲得のためのマーケティングマテリアル

- 野村證券から独立という背景
- アジアで初めてディープラーニングモデルをアルゴリズム取引で実用化した技術力
- セキュリティの厳しい証券グループでPoCを行い、成功を収める
- アドバイザーが石川善樹先生
- FISC安全対策基準・解説書への対応
  - 第三者による認証は存在せず、対応状況は自己申告
- 3省4ガイドライン（現：医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン）への対応
  - 第三者による認証は存在せず、対応状況は自己申告

ISMSやISO/IEC27017などの認証は一切未取得

委託先の要求事項の現実

サービスの販売活動を進めるうち、様々な会社から委託先審査を受けたが．．．

- 企業の沿革や背景、出資者などはほとんど考慮されない
- FISCなどの一部の業種以外には広く知られていないものはほとんど評価されない
- ISMS、ISMSクラウドセキュリティ、Pマークなどのセキュリティ認証を取得しているかどうかが、委託先の前提となっていることが多い
- セキュリティ認証のない企業は取引先の候補に入らない

BtoBのSaaSビジネスにおいて
ISMS / ISO/IEC27017 取得は必須

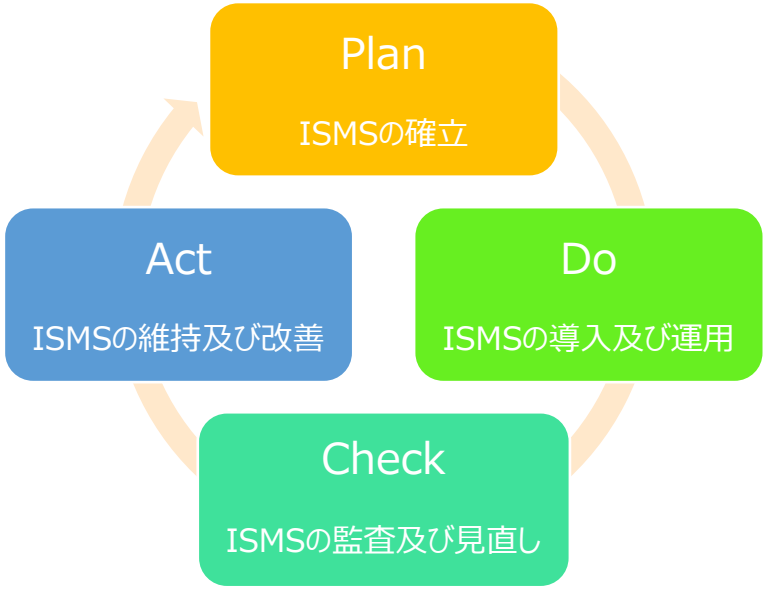
ISMS（情報セキュリティマネジメントシステム）って何？

■ 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

- システムという名前で勘違いしやすいが、特定の情報システムや特定のツールを導入するわけではない
- 管理体制の整備（リスク、情報資産、委託先、組織、ネットワーク、インシデントなど）
- 情報の公開、責任範囲の明確化、顧客への通知方法などの取り決め

■ 確立、導入・運用、監査・見直し、維持・改善というPDCAを回す

- リスクの洗い出し、定量評価（発生確率x影響度）、対策
- 法令対応
- 内部監査、マネジメントレビュー



■ ISMSクラウドセキュリティはクラウド用の規格をISMSに補足したもの

■ セキュリティ認証審査は上記が正しくできているかがチェックされる

セキュリティ認証のよくある勘違い

■ サービスを提供しているシステムの使用技術は問われない

- ロジックや使用している技術の評価は要求事項や審査内容に入っていない

■ システムそのものの脆弱性を審査するものではない

- 具体的なシステムの脆弱性チェックは審査項目にほとんど入っていない
- ファイヤウォール、暗号化、ウイルス対策、ペネトレーションテスト、IDS、IPSなどのキーワードも
  要求事項にはほとんど記載されていない（要塞化、ポートを閉じるなどの抽象的な内容)

■ 具体的なISMSの確立方法が案内されているわけではない

- ISMSの規格は雛形や見本を示してくれるわけではない（管理されるべき項目、網羅すべき事項などが記載されている）
- 具体的にどうやってISMSを作るかは自分たちで考える
- マネジメントシステムが正しく機能しているかのプロセスと結果が審査される

認証取得計画 (2019年10月頃)

ISMS (ISO27001)

- Pマーク同様、広く知られた情報セキュリティ認証

ISMSクラウドセキュリティ (ISO/IEC27017)

- クラウドの利用及び提供に関するセキュリティ認証
  （WellGoの場合はCSC: AWS, CSP: WellGo）
- SaaS企業が取得しているケースが多い

ISO/IEC27018

- 個人情報の保護に関するセキュリティ認証
- 当時Pマークの代わりに取得するケースを聞いていたが、日本では公式認証は存在しなかった
- 当時発行が計画段階だったISO/IEC27701規格の認証とどちらが良いか迷っていた

認証の種類

公式認証

- ISMS-ACによって統一された基準によって審査され、認証される公式な認証
- ISMS-ACに認定された審査会社を通して認証を取得する必要がある

プライベート認証

- 各審査会社の裁量によって審査され、審査会社の名前で認証が出される
- ISMS-ACの認定の有無にかかわらず、任意の審査会社が認証を出せる

認証取得までの流れ

各種ドキュメントやシステムの整備、ルールの徹底を行い、
ISMSの確立を行う

↓

ISMSを適切に運用（PDCAを適切に回す）

↓

審査会社を選択し、審査を受ける

↓

認証取得

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を強制的に適用）	独立後 （セキュリティポリシの強制適用がない）	
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	誤送信するリスク
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	顧客情報を どこかに公開してしまうリスク
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	P2Pなど不正なソフトウェアを 導入してしまうリスク
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	アップデート未適用による 最新マルウェア感染リスク
電話	部署によっては通話記録など	制限なし	内部情報や顧客情報を 話してしまうリスク
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	セキュリティの担保に 必要な管理ができないリスク

**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**

**意識してポリシを守る必要がある
→ ISMSでリスク管理**

WellGoのISMS確立例1 (ISMS / ISO/IEC 27017)

1. ISMS

a. 文書

情報セキュリティ方針（Web公開）、MSマニュアル、情報セキュリティマニュアル、セキュリティハンドブック（社員用）、適用宣言書

b. 台帳

文書管理台帳、フロア図、ネットワーク図、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、セキュリティに関するアンケート（委託先へのアンケート）

c. 内部監査/審査

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

d. 会社組織

組織図、入社時における誓約書、入社退職時チェックリスト、退職時における誓約書

2. ISMSクラウドセキュリティ

ベースライン管理表、WellGoセキュリティホワイトペーパー（Web公開）

WellGoのISMS確立例2 (ISMS / ISO/IEC 27017)

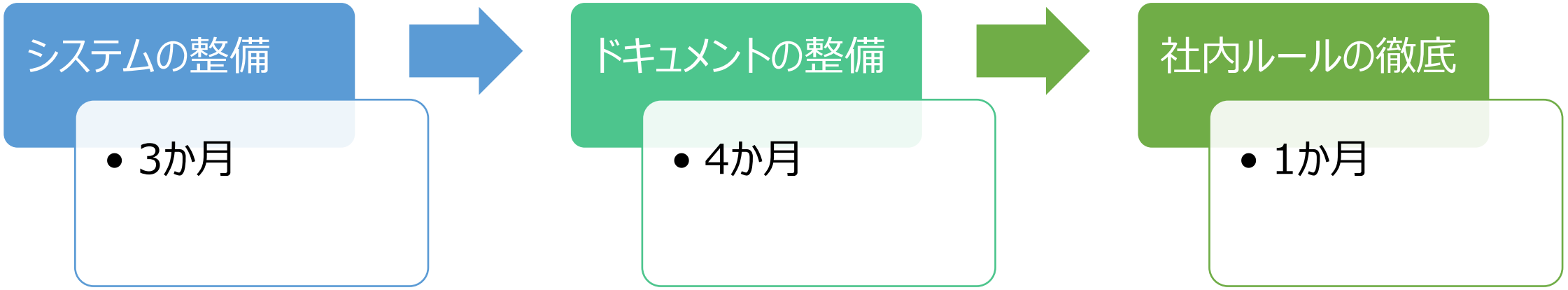
3. 各種管理システムの整備

- Redmine（課題管理、インシデント管理）
- Seculio（e-ラーニング、社員のセキュリティアンケート、法令管理）
- G Suite / Box (メール、スケジュール、ドキュメント管理)

4. 要求事項ではないが合わせて見直したもの

- SLO (サービスレベル目標)
- プライバシーポリシ
- 契約書

ISMS確立にかかった時間 (通常業務と並行して)



ISMSの基盤がない状態から取得を考える場合、
コンサルティング会社に委託する選択肢もある

実際に認証取得してみて感じたこと1

1．最新のシステム技術の追求とISMSの確立は異なる

- 業務システムが最新技術を使用しているからといってISMSが確立できているとは限らない
- 重要なことは、組織が適切に情報セキュリティを管理する体制ができているかどうかということ
  （セキュリティに対する意識と行動が重要）

2．認証取得を通じて見直した部分が少なからずあった

- 建前としては、既存のISMSを審査してもうらうもの
- しかし実際は、認証取得のためにISMSを見直した部分が少なからずあった
  （順序が逆であり、管理が十分ではなかったことを認識）
- 具体的にはリスクの定量評価、法令の適切な管理、社員教育の整備など

実際に認証取得してみて感じたこと2

3．自社のセキュリティレベルについて自信がつく

- 時間と労力をかけてしっかりと確立したものなので、社内外に「適切に管理している」と自信を持って言えるようになった

4．SaaS企業にとってセキュリティ認証は必須

- セキュリティ認証はBtoBでは委託先選定条件のデファクトスタンダード
- 持っていないSaaS企業はそもそも取引先候補にも入れてもらえない

5．脆弱性、法令、セキュリティの最新動向に敏感になった

- 必須項目を管理するうちに、知識レベルが向上し、最新情報への感度が高くなった


WellGo