導入事例

株式会社セブン&アイ・ホールディングス様

株式会社セブン&アイ・ホールディングス
グループDX本部　グループセキュリティ統括部
サービスセキュリティ推進Unit　シニアオフィサー
鈴木 恭敬氏

※インタビュー実施（2025年9月11日）時点

株式会社セブン&アイ・ホールディングスは、顧客の情報を守り安心・安全なサービスを提供するため、グループ共通のベースラインを定め、企画・設計段階からセキュリティレビューを実施してシステム開発を進める体制を整えてきた。MBSDはその考え方に賛同し、約5年にわたって共にセキュリティレビューやセキュリティ診断を支援している。

導入サービス

- **コンサルティングサービス**
  20年の豊富な経験と実績があり、
  お客様のコストに見合ったソリューションや体制を立案
- **Webアプリケーション診断**
  保有するWebアプリケーションシステムに対して、疑似攻撃を行い、
  Webアプリケーションシステムに存在する情報漏えいや改ざんといった
  様々なリスクを調査するサービス

プロジェクトの企画・設計段階でシステムのセキュリティに関する問題点を明らかにし、リスクを極小化するとともに、システムオーナー（＝リスクオーナー）に残存リスクを認識してもらう取り組みを、グループ内に浸透させることに成功

背景と課題

企画・設計段階からセキュリティレビューを実施

株式会社セブン&アイ・ホールディングスは、サイバー攻撃の増加により消費者の目が厳しさを増す中、セキュリティインシデントを未然に防ぐため、グループセキュリティ統括部が主導して、グループのセキュリティ管理体制を整備してきた。

グループ共通の「セキュリティ管理要領」を整備し、全体の底上げを図る。加えて、事業部や事業会社が新たなサービスやアプリを提供する際には、リリース前にセキュリティ診断をするだけでなく、企画・設計段階からシステムやサービスのセキュリティを評価するセキュリティレビューを実施している。

「ベースラインを定めるだけでなく、その順守状況とリスクベースの確認結果を併せた、必要な対策を依頼することで、リスクを極小化したシステムやサービスのリリースが出来るよう日々対応をしています。対応が難しい残存リスクには、事業部や事業会社と協議し、ビジネスとバランスを取りながら進めています」（鈴木氏）

導入のきっかけ

先進的な取り組みを支援できる数少ない企業だったMBSD

現在では、リリース前のセキュリティ診断で発見された問題を修正するより、企画・設計段階からセキュリティを意識して開発を進める「シフトレフト」の方が、セキュリティ品質とコストともに効率が良いという考え方が広まっている。鈴木氏らが着手した当時は、事業部や事業会社はもちろん、セキュリティ業界でも先進的な取り組みだった。

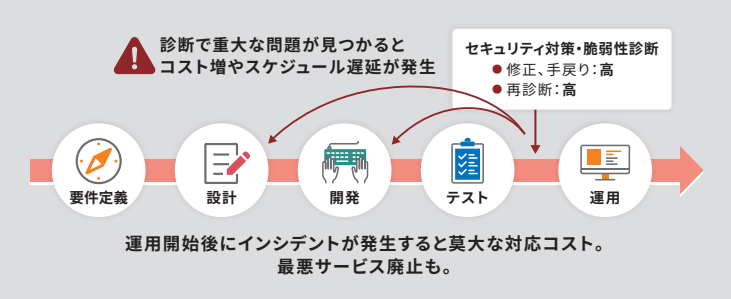
「当時は、こうした支援ができる企業は少なく、その中の企業の一つがMBSDでした」（鈴木氏）

長くセキュリティ診断サービスを提供した実績に加え、セキュアな設計に関する知見・経験が豊富であることも評価し、年間数百件に上るセキュリティレビューに関する支援を依頼した。

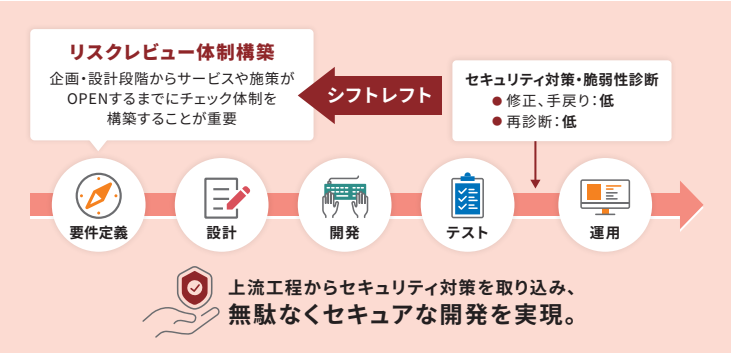
セキュリティレビューの対象は、主にお客様情報を扱うサービスやシステムだ。さらにインターネットに公開するシステムなど一定の条件に該当する場合は、リリース前のセキュリティ診断を実施する。新規サービスを企画する際はセキュリティレビューを実施する。セキュリティレビューでは、ベースラインと照合し対策を確認するとともに、リスクベースでも評価する。企画・設計段階では、どのようなセキュリティ機能や要件が必要かを伝え、安心・安全なシステム開発を推進する。セキュリティ診断が必要な場合は、スケジュールとスコープを調整し診断を実施する。

MBSDは、この一連のプロセスを5年以上にわたってセブン&アイ・ホールディングスと一体となって支援してきた。

■従来のシステム開発



■シフトレフトを導入したこれからのセキュア開発



成果

セキュリティ品質の底上げと強化

セキュリティレビューの対象は、PoC（概念実証）からグループ共通基盤のように大規模なものまで多種多様だ。しかも、一日に複数のレビュー依頼が寄せられる。

「大規模なプロジェクトにおいても、隅々までしっかりとベースラインの順守状況を確認いただいています。また、質疑をテンプレート化することにより品質を保った上で、過去の経験や知見に基づいたリスクを指摘いただき助かっています」（鈴木氏）

一方でPoCなどは、セキュリティ要件を厳しくしすぎると本来の目的が達成できなくなる恐れもある。ビジネス上の挑戦を理解し、寄り添いながら、業界標準で求められるセキュリティ水準と照らし合わせてリスクを指摘する、絶妙なバランス感覚が求められる。

「セキュリティの専門家として客観的にリスクを評価するのはもちろんですが、上からものを言って終わりではなく事業に寄り添い、背景を踏まえた適切なアドバイスをいただいています」（鈴木氏）

セキュリティ診断は対象となるシステムが多く、複数の企業が支援しているが、品質と価格を評価し、最も多い件数をMBSDが実施している。急に診断が必要になる場合においても、柔軟に診断員のリソースを割り当てられる契約形態を取っており、臨機応変に対応できる点も評価しているという。

「セキュリティレビュー対象となるシステムが非常に多い中で品質を維持していくには、我々だけの力では回りません。また、小売を本業とする我々が優秀なセキュリティエンジニアを確保し続けることも困難です。専門的な知識を踏まえ、客観的に、指摘すべきことを指摘してもらえるMBSDに支援いただけているから、業務が回っていると感じています」（鈴木氏）

約5年にわたる取り組みを経て、企画段階からセキュリティを意識することの重要性が事業部や事業会社にも浸透している。セキュリティに関する項目が記載されるなどドキュメント品質が向上したのはもちろん、レビュー時の指摘事項も徐々に減少している。また、セキュリティ診断では検出される脆弱性が減少しただけでなく、その修正も早くなった。

「MBSDの支援により、グループ全体のセキュリティ対策は確実に向上しています。今後も、セキュリティとビジネスの両立を目指し、MBSDとともに安心・安全なサービス提供に努めます」（鈴木氏）

開発元

三井物産セキュアディレクション株式会社
〒103-0013
東京都中央区日本橋人形町1-14-8
JP水天宮前ビル 6階
TEL: 03-5649-1961
Mail: sales-info@mbsd.jp

製品に関する最新情報はこちらから ⟶ www.mbsd.jp

お問い合わせ

CS21-1001-2510