＜SecurityGate case study 資料＞

株式会社テリロジー

ケーススタディ

Chevron がアセスメント作業工数を 57%削減した事例

～OTサイバーセキュリティリスクプラットフォームの進化～

Chevron とは

Chevron は世界中に石油と天然ガスの探査、燃料の精製と販売、何千もの製品を生産するための化学物質の生産、そして新しい革新的なエネルギー源の開発に特化した施設をグローバルに有している世界で最大のエネルギー企業である。

Chevron でのリスク管理とサイバーセキュリティの課題

Chevron のサイバーセキュリティ脅威は、IT および OT の幅広い範囲にわたって、多くの国々、多様言語、異文化にまたがる信じられないほど大規模で多種多様な運用エコシステムが稼働している。同社のリスクマネジメントとサイバーセキュリティのプロジェクトチームは、運用システムの安全性を脅かすリスクがどこにあるかを把握するだけでなく、サイバーセキュリティの監査レポートと改善対策の標準化、作業コストとその効率化、一貫性をもたらす手法を見出すという課題に直面している。何年にもわたる手動プロセスの後、同社はグローバルなサイバーセキュリティプログラムにスケーラビリティと効率性をもたらす対策にフォーカスした。

◆課題

Chevron は以下に示す課題解決をサポートしてくれるパートナーとして SecurityGate を選択した：

- 監査レポートおよびリスクマネジメントの不整合を取り除く。
- セキュリティアセスメントに関連する作業時間とそのコストを削減する。
- 現場オペレーションでの生産性インパクトを最小化する。
- 一貫した成熟度モデルの向上を可能にするスケーラブルなプロセスを実装する。

（注）成熟度モデル(Maturity Model)とは、対象の業務プロセスを分析し、そのプロセス改善の成熟度レベルついてアセスメントし、目指すべきプロセスレベルを明確にする。

Chevron は、DX 化の波に乗って、サイバーセキュリティの取り組みを分散化し、世界中の各施設のアセット管理者がサイバーセキュリティプログラムを実行出来るようになった。全ての取組みが同じプラットフォーム内で管理され、同じスケーラブルなプロセスを使用していたため、Chevron はこのプロジェクトの標準化に成功した。

◆重要インフラ成熟度モデルのレビュー

サイバーセキュリティプログラムの成功と効率は、主に、現場の管理者自身がどのような状況にあるのか、そしてどこまでのレベルを監視できるかにかかっている。重要インフラ成熟度モデル（CIMM:参照 1）は、この重要な課題にフォーカスする。

◆SecurityGate がこれらの課題に答える

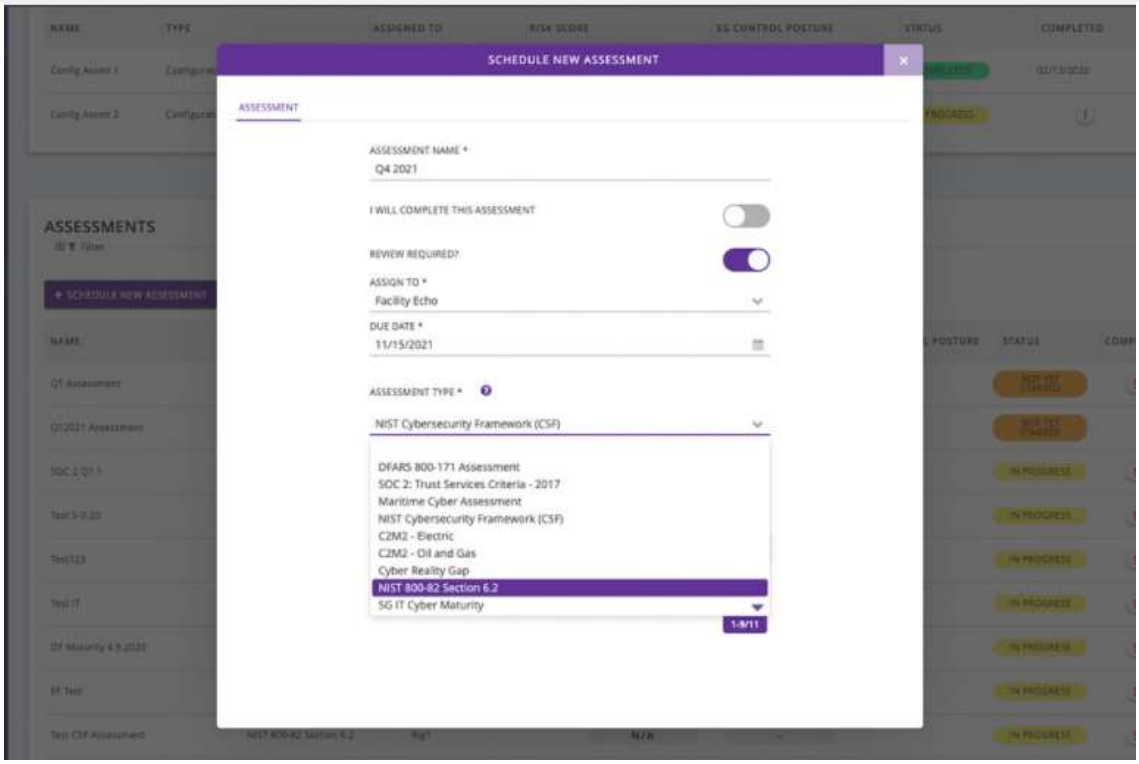
SecurityGate プラットフォームが最適だった。Chevron は、デジタルトランスフォーメーション(DX)の波に乗って、サイバーセキュリ取り組みを分散化し、世界中の各施設の管理者がこの

ソフトウエアを実行出来るようにした。Chevron は、すべての取り組みが同じプラットフォーム内で管理され、同じスケーラブルなプロセスを使用していたため、以下を実現出来た：

- レポートの標準化とアセスメントの自動化されたプロセスにより、結果に一貫性がもたらされ、成熟度の向上をより簡単に測定出来るようになった。
- リスクを理解し、システムの有効性を高レベルのビューで測定できること、および各施設の詳細ビューにズームイン出来ることの利点を含む、すべての利害関係者に対する会社間の可視性を実現。
- アセスメント時間が大幅に短縮– 57%削減。
- アセスメントロジスティクスと関連する活動のコストと複雑さが軽減された。
- サイバーセキュリティアセスメントによるチームへの影響は大幅に狭められた。OT チームは、サイバーセキュリティチームとのミーティングを回避し、自分のペースとスケジュールでアセスメントの質問を完了することが出来た。

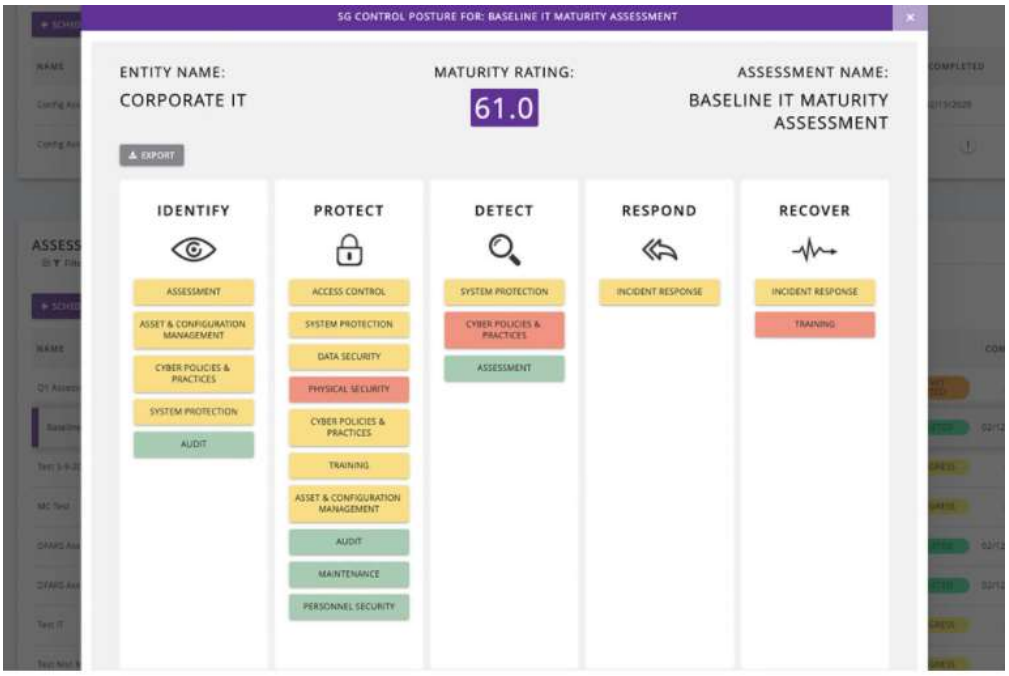
●標準化

同社プロジェクトチームは、アセスメントレポートを標準化し、これら作業プロセスを自動化することで、一貫性を持たせ、成熟度レベルの向上をより簡単に達成できるようになった。



●企業グループ間の見える化

すべての利害関係者(Stakeholders)が、リスク把握を共有し、システムの有効性を高レベルのビューで測定できること、および各施設の詳細ビューにズームインできるという利点が含まれる。



●チームインパクトの削減

サイバーセキュリティアセスメントによるプロジェクトチームのビューは大幅に狭められた。OT チームは、サイバーセキュリティチームとのミーティング時間を回避し、独自のペースとスケジュールでアセスメント指標に関する様々な質問をカバーすることができた。

企業経営者は、優れたサイバーセキュリティフレームワークを導入することにより、企業全体のセキュリティ体制を維持できると確信した。サイバーセキュリティフレームワークを構築および運用する場合、企業が直面する固有のサイバー脅威、事業環境、対処する業務フローなど、一貫した対策が必要である。但し、これらの対策が、企業全体の目標と十分に一致していない場合、サイバー攻撃のリスクを排除することは出来ない。

一般に、全ての事業体においては、IT 環境に存在する無数のリスクを管理するために“更新された”サイバーセキュリティプログラムまたはフレームワークを導入する必要があるとSecurityGate は指摘する。規制遵守、各組織のセキュリティ成熟度(Maturity) レベルなどに焦点を当てたサイバーセキュリティフレームワークは、依然として定期的に多大なサイバーリスクにさらされることを注意する必要がある。

◆Chevron は、SecurityGate が十分に機能していることをどのように評価しているか？

前に述べたように、Chevron のリスク管理チームとサイバーセキュリティチームは、さまざまな方法で SecurityGate がグローバルなサイバーセキュリティにスケーラビリティと効率をもたらすことに成功したことを高く評価している。この新たに見出された効率の結果として、Chevron はアセスメント作業時間をなんと 57%短縮することができた。

●Less time running assessments

最終的に、Chevron の最終的な成功の尺度は、意思決定に必要な正しい情報を受け取るだけでなく、最も重要なことに、同社のプロジェクトチームの迅速なレスポンス対応によって信頼のアセスメントデータが示されていることである。

◆SecurityGate とのパートナーシップの価値証明

COVID-19 が 2020 年の初めに予期せず世界を混乱させたが、Chevron は SecurityGate プラットフォームのデプロイメントによって完璧なユースケースを証明した。スケーラブルなプロセスとリモートでのサイバーセキュリティアセスメント運用で、SecurityGate に活用して Chevron はサイバー攻撃が急速に増加している中で、その打開策を実現した。

＜参考１＞

CIMM とは：

能力成熟度モデル統合（Capability Maturity Model Integration, CMMI）で、企業組織がプロセスをより適切に管理できるようになることを目的として遵守するべき指針を体系化したものである。平易な言い方をすると、ソフトウェア開発組織及びプロジェクトのプロセスを改善する

ために、その組織の成熟度レベルを段階的に定義したものである。CMMI は、もともとは能力成熟度モデル（CMM; Capability Maturity Model）として開発された。

＜参考２＞

OT/ICS 向けリスクアセスメントとは

国内でサービス提供している各社は基本的に、IPA セキュリティセンターが作成の、重要インフラや産業システムの制御システムのセキュリティリスク分析ガイドをベースに展開している。その手法手順は以下の通りである：

（1）**資産ベースのリスク分析**

保護すべきシステムを構成する各資産を対象に、その重要度（価値）、想定される脅威の発生可能性、脅威に対する脆弱性の 3 つを評価指標として、リスクを評価する分析手法。

（2）**事業被害ベースのリスク分析（攻撃シナリオと攻撃ツリーによる分析）**

システムで実現している事業やサービスに対して、事業被害とそのレベル、事業被害を引き起こす攻撃ツリーの発生可能性、攻撃に対する脆弱性の 3 つを評価指標として、リスクを評価する分析手法。

＜参考３＞

ES-C2M2 とは：

ES-C2M2 は米国エネルギー省（DoE）が、米国内電力会社のセキュリティマネジメントを自己評価するために発行したもので、サイバーセキュリティ成熟度モデル（Cybersecurity Capability Maturity Model：C2M2）のひとつで広く用いられている。ES-C2M2 とほぼ同じ内容の ONG-C2M2（Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model）もあり、石油・ガス業界でも活用されている。

＜参考４＞

NIST CSF とは：

NIST（National Institute of Standards and Technology：アメリカ国立標準技術研究所）が定めるサイバーセキュリティフレームワーク（以下、NIST CSF）。日本国内でもさまざまな企業や公的機関がこのフレームワークを採用するに至っている。

１）フレームワークコア（Framework Core）

業種や重要インフラとは関係なく、共通となる具体的なサイバーセキュリティ対策を示したものである。必要なセキュリティ対策を検討する際に、自社に足りないセキュリティ対策を明確にし、必要なツールを導入するための指針となる。「識別（Identify）」、「防御（Protec

t）」、「検知（Detect）」、「対応（Respond）」、「復旧（Recover）」という 5 つのコア機能と、23 のカテゴリーで構成されている。

2）インプリメンテーションティア（Implementation Tier）

自社のセキュリティ対策のレベルがどの程度にあるのか、客観的な判断が必要になることもある。NIST CSF の 2 つ目の要素であるインプリメンテーションティアは、組織のサイバーセキュリティ対策がどの段階にあるのかを評価する基準を示すものとなっている。「ティア 1（部分的である）」から、「ティア 4（適応している）」の 4 段階に分かれており、現状が低いレベルにある場合は、より高いレベルを目指すことが推奨される。必ずしも上のレベルに到達することが求められているわけではなく、組織が置かれている状況や費用対効果から総合的に判断すべきとしている。

3）フレームワークプロファイル（Framework Profile）

自社の置かれた経営環境やリスク許容度、割り当て可能なリソースに基づき、サイバーセキュリティ対策の現状と、あるべき姿を記述するために利用する。「現状（As-Is）」と「あるべき姿（To-Be）」を記述し、そのギャップを明確にすることで、企業はセキュリティ対策の改善計画を策定できるようになる。なお、NIST CSF においては、組織ごとの環境や特性、戦略が異なるという観点からプロファイルのひな型は準備されていない。