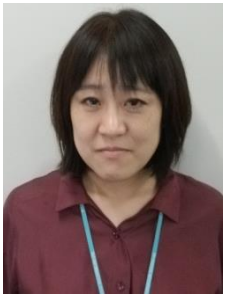
金融機関における最適なセキュリティを目指して
セキュリティフレームワークの活用

（株）Ｔ＆Ｄ情報システム

■ 執筆者Ｐｒｏｆｉｌｅ ■

執筆者




２００８年　入社
２０１９年
テクニカルサポート二部ＩＴ基盤管理二課
蘆田　昌代

２０１５年　入社
２０１８年
テクニカルサポート二部ＩＴ基盤管理二課
山中　龍太

２０１６年　入社
２０１９年
テクニカルサポート二部ＩＴ基盤管理二課
深谷　雄太

２０１７年　入社
２０１９年
テクニカルサポート二部ＩＴ基盤管理二課
中矢　竜太

■ 論文要旨 ■

Ｔ＆Ｄ情報システム株式会社は、大同生命、太陽生命、Ｔ＆Ｄフィナンシャル生命の３社を中核とするＴ＆Ｄ保険グループの情報システム会社として、グループ各社のシステム開発および運用を受託している。

生命保険会社の業務において、保険契約を締結する際にお客様よりさまざまな情報を取得する必要がある。取得する情報は、お客様の生年月日や住所、体況情報、銀行口座や過去の病歴などがあり、生命保険会社は一般的な企業と比べても非常に多くのセンシティブ情報を保有していることが特徴である。システムの運用を行っていくうえで、これらの大量の情報は安全かつユーザの利便性が高い状態での管理を求められている。

本稿では、自社のセキュリティレベルの評価と課題の抽出・対策を目的としたセキュリティフレームワークの活用と、セキュリティ評価を基に行った最適なセキュリティの維持、向上に向けた取り組みについて論述する。

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　当社の概要

Ｔ＆Ｄ情報システム株式会社（以下、当社）は、大同生命、太陽生命、Ｔ＆Ｄフィナンシャル生命の三社を中核とするＴ＆Ｄ保険グループの唯一の情報システム会社である（図１）。

業務内容は、ＩＴ戦略の立案実行をはじめ、システム開発、システム基盤の構築、システム運用とＩＴに関わる全般にわたっている。

業務を実施していくうえで、お客様の個人情報（健康に関するセンシティブ情報を含む）を収集、保管しており、これらの情報を守り、お客様に安心・安全なサービスを提供する必要がある。

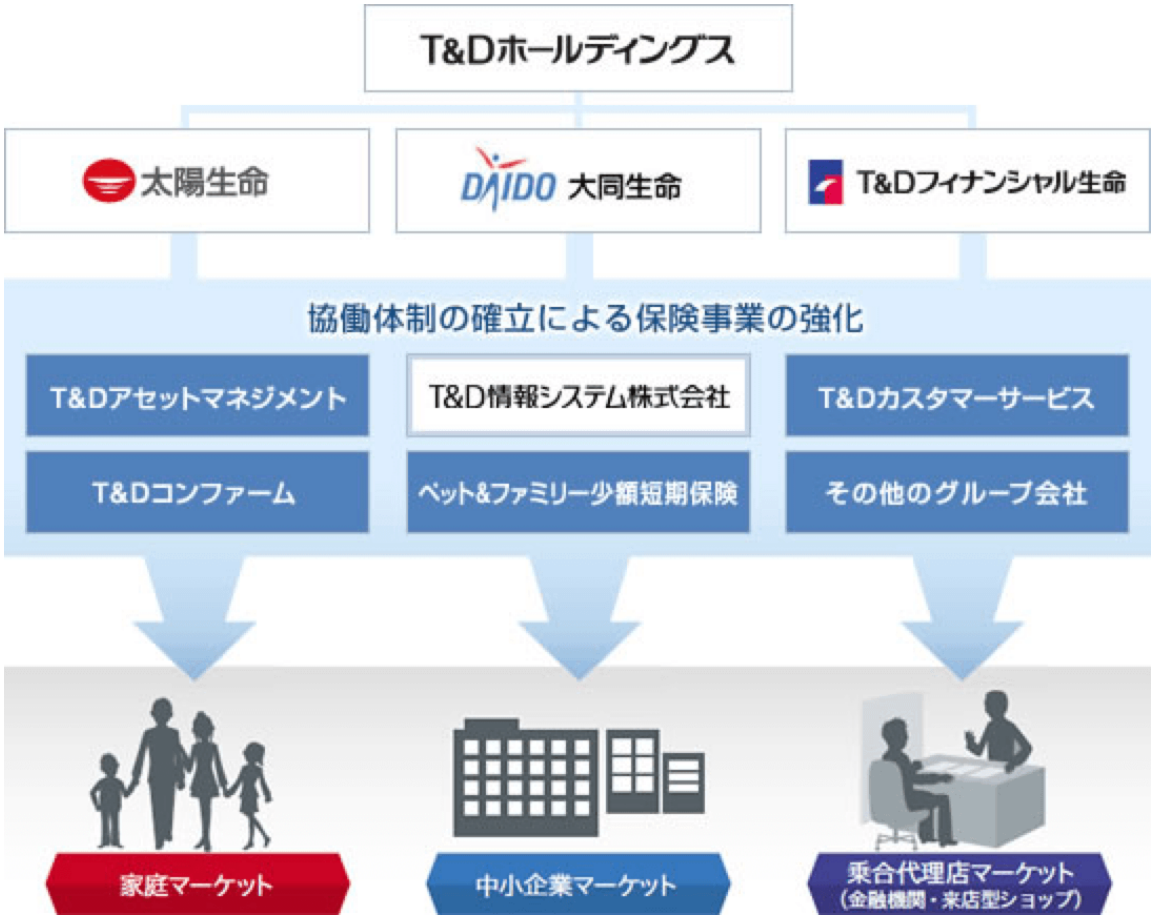


図１　Ｔ＆Ｄ保険グループの概要

１．２　当社を取り巻く環境

近年、情報セキュリティの脅威は日々高度化・複雑化を増し、その脅威に対して「切れ目なく、適切に」対応する必要がある。

セキュリティ対策を最適化していくために、まず客観的な視点から当社の脆弱な部分を理解し、現状を正確に把握し、対策を講じる必要がある。

今回、お客様に安心・安全な保険サービスを提供するために、セキュリティフレームワーク活用して、セキュリテイ対策の最適化に取り組んだ事例について、紹介する。

２．現状の分析と計画の策定

２．１　現状の分析

当社のセキュリティについて、次の３つの観点で他社等のベストプラクティスとのギャップを把握・評価した（表１）。

金融機関のガイドライン	（１）	重要インフラのサイバーセキュリティを向上させるためのフレームワーク（ＮＩＳＴフレームワーク）の活用
	（２）	金融ＩＳＡＣ等の情報をもとにした他の金融機関との比較
外部の第三者評価	（３）	外部専門機関による情報セキュリティに関するリスクアセスメント

表１　セキュリティ評価の観点

（１）　ＮＩＳＴフレームワーク※を活用した課題抽出

当フレームワークが掲げる９８項目の取組みのうち、当社がホストの運用管理の分野で認証取得しているＩＳＭＳ規格にかかる確認事項と重複しない３４項目について、自己評価を実施した結果、１９項目でベストプラクティスとのギャップを認識し、それらに関する対策を策定することとした（表２）。

※ＮＩＳＴフレームワークは、２０１４年に米国の国立標準技術研究所（ＮＩＳＴ）が発行。ＣＳＦ（Ｃｙｂｅｒ　Ｓｅｃｕｒｉｔｙ　Ｆｒａｍｅｗｏｒｋ）という略称で知られ、日本でも多くの企業・組織がサイバーセキュリティ対策を向上させるための指針として活用。

機能	カテゴリー	サブカテゴリー		
		ベストプラクティスとのギャップなし		ギャップあり【強化策の策定】
		ＩＳＭＳ認証により確認	今回確認	
特定	５カテゴリー（２４項目）	１４項目	６項目	４項目
防御	６カテゴリー（３５項目）	３０項目	０項目	５項目
検知	３カテゴリー（１８項目）	１０項目	４項目	４項目
対応	５カテゴリー（１５項目）	１０項目	２項目	３項目
復旧	３カテゴリー（　６項目）	０項目	３項目	３項目
合計	２２カテゴリー（９８項目）	６４項目／９８項目	１５項目／９８項目	１９項目／９８項目

表２　課題抽出のイメージ

（２）他の金融機関との比較

「平成２７年度金融レポート」で公表されたサイバーセキュリティ対策に関する「確認項目」「良好事例」とのギャップを把握・評価を実施した結果、全４４項目のうち、３２項目について対応済であり、取組み中の９項目および未対応の３項目について、今後の取り組みが必要であると評価した。当項目は金融ＩＳＡＣでの対応事例の情報収集等を踏まえて、対策を策定することとした。

（３）外部専門機関による情報セキュリティに関するリスクアセスメント

外部専門会社が当社の情報セキュリティ対応状況を客観的に評価し、さらに強化すべき取組み課題を検出することを目的にリスクアセスメントをした結果、リスクアセスメントの評価は、「早急な対応が必要なリスク」の検出はなく、一定水準以上のセキュリティ対策が実施されていることの確認はできた。

２．２　計画の策定

前述での現状分析の結果を踏まえ、当社のセキュリティ態勢を計画的・継続的に見直すことを目的として、「情報セキュリティ強化の取り組み計画」を策定した。取り組みに関する方針は以下のとおり。

＜取り組み方針＞

○深刻化する脅威のうち、外部環境と内部環境のそれぞれに対して対策を実施し、この分野で生命保険業界最高水準のセキュリティを確保する。
○従来からの入口・出口対策とともに、システムログ等の監視、脅威への対応手順の整備など被害軽減を目的とした内部対策を強化する。

＜取り組み施策＞

Ⅰ　組織的な安全管理措置（CSIRT 態勢の強化等）
＜到達イメージ＞
○金融 ISAC 加入で、より多くのインシデント情報が入手可能となったことから、これに迅速・適切に対応するための CSIRT の要員数を算定し、増強。
○システム情報（ログ）の相関分析ツールの導入に伴う分析可能なインシデント量の増加・金融 ISAC 活動等の他金融機関と協働した業務の増加等、東京オリンピックに向かっての他金融機関等への攻撃の増加等を見込み、要員を増強。
○CSIRT メンバーの一定割合が人事異動を実施しても、役割に応じた有用な資格保有者で構成される状態を確保。
・「情報セキュリティマネジメント」：大同生命、当社の CSIRT メンバー全員の資格保有
・「情報処理安全確保支援士」：当社の CSIRT メンバーの半数の資格保有
○既存の「標的型メール攻撃による情報漏えい発生時の対応マニュアル」に「社外 Web サイトの改ざん」「不正アクセス」「内部者による情報持ち出し」などの攻撃手法を統合した「情報漏えい発生時の対応マニュアル」を整備。
○新たに導入するセキュリティソリューションを対応マニュアルへ反映。
○マニュアルにもとづく対応訓練を定期的に実施し、対応手順の実効性を確認、マニュアルのレベルアップを図る。

Ⅱ　技術的な安全管理措置（セキュリティソリューションの導入等）
＜到達イメージ＞
○外部ベンダーで分析している通信ログに、社内システムログを加えて統合的に分析。異常発生後の検知に偏っている「不正の監視」を強化し、予兆の把握を早期化・精緻化。

３．具体的な取り組み

具体的な取り組み施策として、前述のとおり十分なセキュリティ知識・資格を保持した要員の確保やインシデント発生時の対応方針を定めたマニュアル策定といった全社的（組織的）な取り組みと、サイバー攻撃を受けた際の外部ベンダーを交えた詳細調査と迅速な対応、サイバー攻撃自体を未然に防ぐための予兆の把握等監視体制に関する技術的な取り組みの２点に整理した。

３．１　組織的な対応

取り組みのうち、インシデント発生時の各担当者の対応方針やベンダーを交えた詳細調査の手順をまとめたマニュアルの策定や対応に関わる社員の知識習得等、社内全体で行うべき対応を組織的対応と位置付けた。

３．１．１　セキュリティ人材育成計画の策定

サイバー攻撃は多様化・巧妙化の進度が極めて速く、サイバーセキュリティ対策に必要となる知識も日々変化している。そのため、最新のサイバー攻撃に適切・迅速に対応するためには新たな知識・スキルを持続的に習熟する必要がある。セキュリティ人材育成については、金融庁の「サイバーセキュリティに係る金融機関との建設的な対話と一斉把握　」でも触れており、サイバーセキュリティに係る人材の育成・拡充の重要性について述べている。これらを踏まえ、当社ではサイバー攻撃に対応可能な人材育成を目的としたセキュリティ人材の育成計画を策定した。人材育成の方針は以下のとおり。

＜人材育成の方針＞

①多様化・巧妙化の進度が著しいサイバー攻撃の対策として必要となる知識・スキルを持続的に習熟し、ＣＳＩＲＴ要員の計画的な育成・スキルの底上げを図る。

②ＣＳＩＲＴの指揮・統括とともに、経営層への報告を担う橋渡し人材を計画的に育成する。

育成計画策定に際して、金融ＩＳＡＣの「ＣＳＩＲＴの１４役割」に記載された全業務（うち特に専門性が高い項目を一部除く）について内部で対応可能とする体制構築を目標に当社の人材育成状況に照らして必要なセキュリティ要員確保を目標とした。セキュリティ人材に必要とされるスキルを習得するための具体的な育成方法として、「業務ローテーション」、「講習・資格」、「社外交流」の３点を観点として育成方法を定めた。

第一の「業務ローテーション」の具体策は次のとおり。ＣＳＩＲＴ人材は有事の際はすみやかに円滑な初動対応を行う必要があるため、複数部門間の人脈を形成して信頼関係を構築する必要がある。特に部門間を結ぶ「橋渡し人材」は他のシステム領域に関する知識・スキルの習熟が必要となるのみでなく、インシデント時におけるすみやかな経営層への対応状況の報告等、高度なコミュニケーションスキルが必要となる。これらを習得するため、キャリアパスに基づく関係部門間の人材ローテーションの実施やＩＴ関連企業、ＪＰＣＥＲＴへのトレーニー派遣を行い、実務経験によるセキュリティ関連スキルのノウハウ蓄積や関連部門間、関連他社間での人脈形成を行った。

第二の「講習・資格」の具体策は次のとおり。ＣＳＩＲＴ要員がセキュリティインシデントに対応するために必要とされる知識・スキルを習得するために、社内による講習会の実施および社外の研修（金融ＩＳＡＣ主催、ＣＹＤＥＲ等）へ参加することで該当要員の計画的なセキュリティ知識の習得を行った。また、情報セキュリティ対策に必要な「情報セキュリティマネジメント」、「情報処理安全確保支援士」等の公的資格や高度セキュリティ資格を取得し、体系的なセキュリティに関する知識・ノウハウを習得した。

第三の「社外交流」の具体策は次のとおり。情報セキュリティ対策は最新のサイバー攻撃や技術動向を把握する必要があり、最先端の技術動向および他社金融機関における対応状況等の情報収集を行うため、金融ＩＳＡＣやＮＩＳＣの共同演習等にセキュリティ要員を参画させた。

３．１．２　各種対応マニュアルの整備・運用

サイバー攻撃が発生した際に最も重要なことは、すみやかに円滑な初動対応を行い影響の拡大を防ぐことにある。これを実現させるため、外部起因のサイバー攻撃および内部起因の情報漏洩について初動対応を円滑に行うため関連部門間での連携や対応手順を記載した対応マニュアルを整備した。サイバー攻撃は多様化・巧妙化の進度が早く、その対応も一様とは限らないため、作成後の対応マニュアルは以下の観点を反映して定期的にマニュアルの実効性を評価して修正・拡充を継続的に行う運用とすることで、常にサイバー攻撃の傾向や社内環境に則したマニュアルを維持できる仕組みを整えた。

＜マニュアル修正の観点＞

①新たなサイバー攻撃手法やインシデント発生事例

②金融庁、ＮＩＳＣ、ＩＰＡ等の公的機関から提供された情報

③「金融ＩＳＡＣインシデント対応マニュアル」等の更改内容

３．１．３　サイバー攻撃を想定した社内外研修

対応方針のマニュアル化だけでなく、情報セキュリティに関する研修や難易度の高い標的型メール訓練等を社内全職員を対象に実施することでサイバー攻撃やウイルス感染、内部不正等による情報漏洩を防止するための社内ルールを組織内への周知・啓蒙を図った。

＜全職員＞

全職員に対し、定期的に標的型メール攻撃を含めたサイバー攻撃手法、内部不正防止のための社内ルール・社内システム利用方法の周知、社員のリテラシー向上を目的とした情報セキュリティ全般の知識習得をＥ－ラーニングや机上による社内研修を継続的に毎年、実施する運用とした。

標的型メール訓練は、不審メールを受信した際に事前に周知されている対応手順に沿って行動・報告が行えるかを確認する訓練を行った。この訓練では、定められた手順で不審メールの対応を行うだけでなく、不審メールかどうかを判断できているか、また対応後の報告や上位者の取りまとめがスムーズに行えているかも確認すべき観点として研修後の判定に用いた。訓練の結果を踏まえて、対応手順の再周知や不審メールの見分け方等を社内研修として実施する等の事後対応も併せて行い、組織全体に周知した。

＜ＣＳＩＲＴ＞

サイバー攻撃に対処するＣＳＩＲＴ要員には、サイバー攻撃に関する知識習得、ＣＳＩＲＴの対応能力の強化、整備された対応マニュアルの実効性の確認等を目的としたサイバー訓練を定期的に実施した。これらの訓練は、実際のサイバー攻撃を想定したシナリオに則って実施し、インシデントの詳細調査のみならず各担当者が必要や情報連携や経営層への報告を迅速に行えているかを評価項目として確認した（図２）。

＜当社におけるＣＳＩＲＴの体制＞

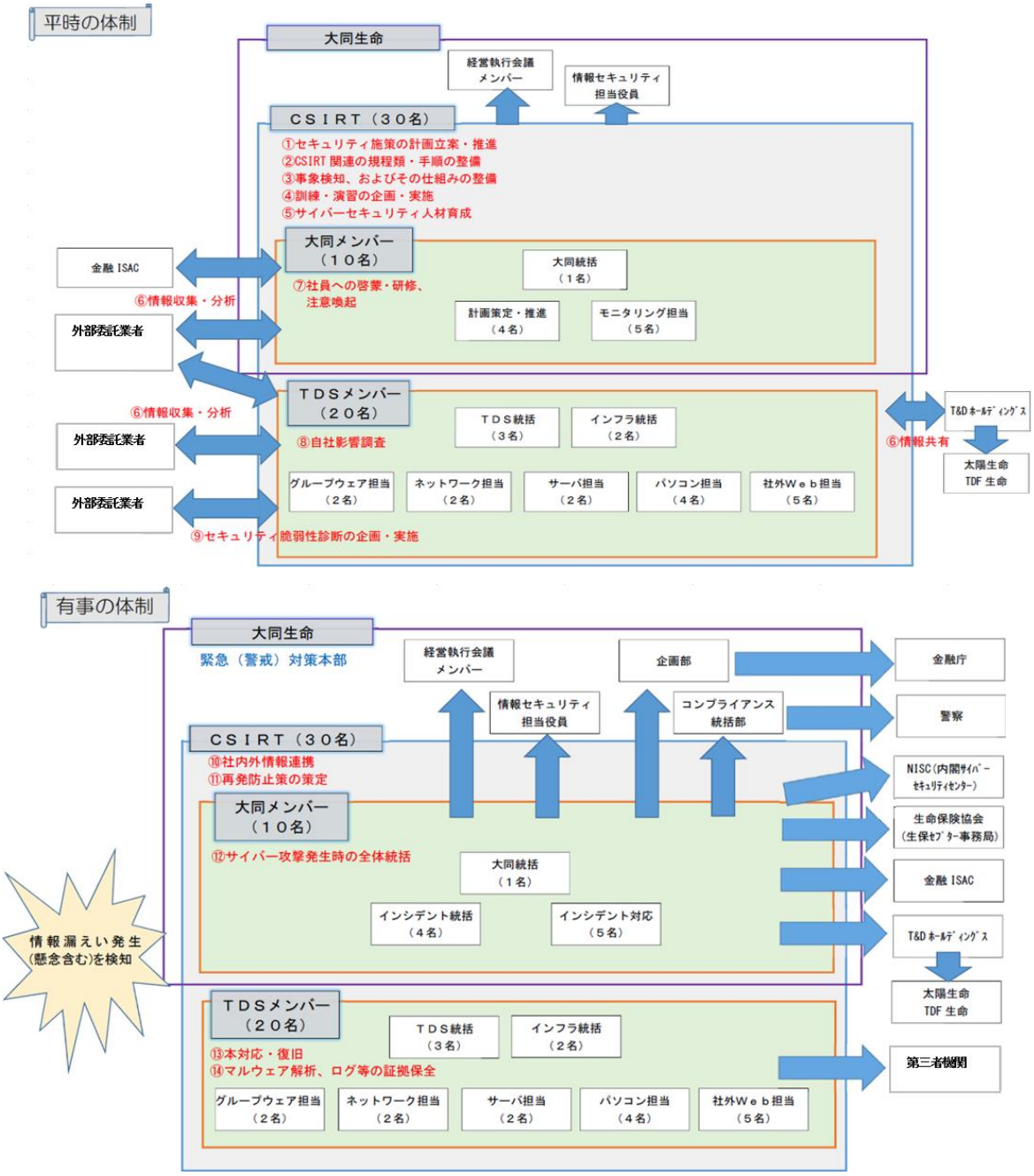


図２　当社におけるＣＳＩＲＴの体制

３．２　技術的な対応

実際にサイバー攻撃を受けた際の原因究明や調査対応、平時における監視体制に関しては技術的な取り組みと位置付けて整理した。

３．２．１　ＳＩＥＭ　導入による各種ログの監視・分析の早期化

前述のとおり、攻撃を受けた際の被害や影響を極小化させるには、インシデントの発生を速やかに検知し、原因の究明や対応を行うことが重要である。また、内部不正による情報漏洩等のリスクへの対応や日々の業務においても各種ログのモニタリングによる状況把握も必要となっている。このことは、金融庁の「サイバーセキュリティに係る金融機関との建設的な対話と一斉把握」でも触れられており、外部専門機関によるリスクアセスメントでも改善推奨項目として「ログの適切な管理・モニタリング」が挙げられている。

しかし、これらのログ分析は確認に多くの時間や要員が必要であり、ログから異常や傾向を判断するためには十分な分析知識を要することが大きな課題となっていた。この課題に対する技術的な対応として、各機器が出力するログを一元的に集中管理するとともに、複数のログを照らし合わせて相関分析やログの可視化、アラート発報等を一括して行うＳＩＥＭを導入することで課題解決を目指した。導入に際して、当時の日本では一般的なセキュリティソリューションではなかったが、フレームワークで非常に重視されており、金融 ISAC 等を通じて、一部のネット証券、ネット銀行での事例を確認できたことで導入に踏み切ることができた。ＳＩＥＭの導入により期待される効果としては、以下のとおりである。

※ＳＩＥＭ（Ｓｅｃｕｒｉｔｙ　Ｉｎｆｏｒｍａｔｉｏｎ　ａｎｄ　Ｅｖｅｎｔ　Ｍａｎａｇｅｍｅｎｔ）複数のシステムログを統合的に分析し、攻撃や攻撃予兆の検知、検知後の調査の早期化を支援するシステム

＜ＳＩＥＭ導入により期待される効果＞

①各機器が出力するログの可視化による予兆把握とログの相関分析の実現

②ログ分析およびインシデント検知時の深堀調査の早期化

(1) 段階的なＳＩＥＭ導入

ＳＩＥＭを導入するにあたり、考慮すべき点として挙げられたのはフレームワークの要求事項達成に必要な技術的機能（シナリオ）とシステム開発にあたる要員（とその工数）である。開発要員に過度な負担を掛けることなくフレームワークの要求事項を達成するため、導入は段階を踏んで行い、第一次ではＪＰＣＥＲＴ／ＣＣの「ログを活用した高度サイバー攻撃の早期発見と分析」や金融ＩＳＡＣ等で行ったヒアリングを参考に、特に優先度が高い「マルウェアによる端末乗っ取りの迅速な検知」、「内部不正による情報漏えいのモニタリング強化」等のシナリオを中心に２４のシナリオの実装を行った。

ＳＩＥＭ導入では、特定のログやログを基に行った相関分析の結果をユーザがカスタマイズした専用画面で視覚的に表示する機能（ダッシュボード）用いて、各機器のログの可視化によるログ分析の効率化を実現させた。ログのモニタリングによる予兆把握を行うため、ダッシュボードには各種システムにより出力されるログをもとに通信量や通信の発生を時間帯で表示させた。これにより、時間ごとの変化状況を可視化させることでセキュリ

ティインシデントの予兆や各機器の状況を容易に把握することが可能となった。開発画面の一例を以下（図３）に示す。

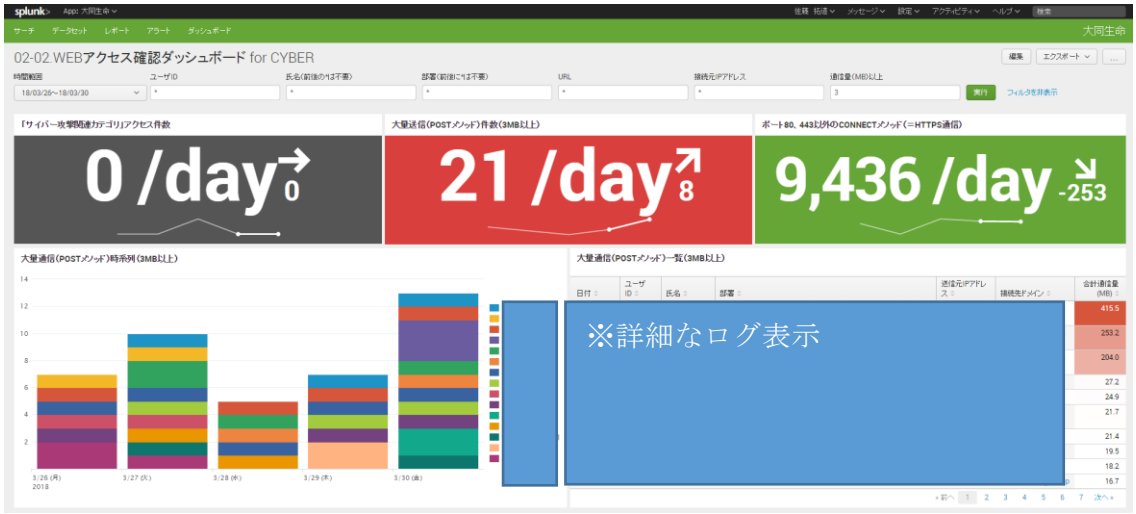


図３　開発画面の一例

(2) 第１次導入による効果

ＳＩＥＭ導入による成果として挙げられるのは、相関分析の実現である。これまでのログ分析では、個々のネットワーク機器からそれぞれログを抽出し、それらを分析することでインシデントの対応を行っていた。この方法では個々のログでしか判断ができず、複数のログを比較して調査を行う場合は多くの調査時間を要していた。ダッシュボード開発では、複数のログ情報を組み合わせて相関分析を行うことを念頭に開発を行い、ユーザ情報やＰＣ端末等の履歴情報を組み合わせることで対象ユーザによるログインや操作の妥当性の判断やユーザＩＤの不正利用監視が実現した。

ＳＩＥＭ導入によって、これまで調査に多くの時間を掛けていたログ分析はダッシュボードによる各機器のログの可視化によって大幅に時間短縮を実現することができた。これまでインシデント対応時のログ分析は対象となるログの取得に始まり、セキュリティ要員によるログの分析、金融ＩＳＡＣなどの公的機関からの提供情報との照らし合わせ、不審メールやＵＲＬへのアクセス解析等、分析・調査に多くの時間、工数が掛けられていたが、ダッシュボードによる可視化と複数のログによる相関分析によって、大幅な時間、工数の短縮が可能となった。以下にＳＩＥＭ導入前後の分析・調査時間の変化を示す（表３）。

担当部署	ＳＩＥＭ導入前	ＳＩＥＭ導入後
セキュリティ担当	**約２８時間／月**	**約５時間／月（約８３%短縮）**
インフラ担当	**約３０時間／月**	**約４時間／月（約８７%短縮）**

表３　ＳＩＥＭ導入前後でのログ分析調査にかける所要時間

インシデント検知時や日々のモニタリング監視における不審なログの深堀調査にもこれまで多くの時間が掛かっていた。理由としては、ＩＰＳ等のログは調査の度にベンダーへ調査依頼を行っており、その回答を待たなければならなかったためである。ＳＩＥＭ導入

後はこれらのログを全てダッシュボード上で確認することがで可能となり、ベンダーへの調査依頼が不要となったため深堀調査の大幅な早期化を実現することができ、インシデントへの迅速な対応が可能となった（表４）。

ＳＩＥＭ導入前	ＳＩＥＭ導入後
約５時間	**約１５分（約９５%短縮）**

表４　ＳＩＥＭ導入前後での不審ログの深堀調査にかける所要時間

(3)「アジャイル型開発手法」の適用

サイバー攻撃に対するセキュリティ対策には迅速性が求められるため、ＳＩＥＭの画面開発では従来当社で実施していた「ウォーターフォール型開発手法」ではなく、短期間で開発・修正のサイクルを繰り返す「アジャイル型開発手法」を採用し、実装後の画面イメージを先に作成し、実装後の試行期間で利用者の意見を収集し、スパイラルに修正・拡張を行った。実際に利用しなければ気づけなかった指摘や開発段階で新たに必要となった要件等を短期間で修正・拡張を繰り返すサイクルによって対応することができた。

(4) ２次導入以降のシナリオ実装

１次導入では特に優先度の高いシナリオを実装したが、サイバー攻撃が日々高度化・巧妙化する中で、新たなセキュリティ対策が必要となる要素も多々ある。２次導入では、１次導入で実装できなかったシナリオに加え、毎年更新されるセキュリティ情報や金融ＩＳＡＣから提供される脅威情報を基に新規のシナリオを作成・実装することで高度化するサイバー攻撃に対して、常に最適なセキュリティシステムの構築とその維持を実現した。

３．２．２　外部専門機関を活用したセキュリティのモニタリングと緊急時対応

ＳＩＥＭの導入によってこれまで時間が掛かっていたログのモニタリングによる予兆把握やインシデント発生時の分析・調査の負担が大幅に軽減した。しかし、サイバー攻撃の調査には高度なセキュリティ知識が必要であり、常に十分な監視要員を確保することは社員教育の面でも大きな負担となる。また、サイバー攻撃自体は２４時間常に発生する可能性があるため内部要員だけでは完全なログ監視は難しいといえる。この課題に関する解決策として、外部ベンダの活用を行うことで課題解決を図った。

外部ベンダが提供する２４時間リアルタイムで不正侵入検知・アクセス検知を監視するサービスを利用して、当社のＩＰＳ・ＷＡＦ機器（社外との通信出口に特化した監視）の監視を依頼することで当社環境と外部間で２４時間の監視体制を実現させた。当該サービスでは侵入検知に専門的な知識を持ったアナリストが常駐しており、監視を委託することで定例作業による社内のセキュリティ要員の負担を軽減させることが可能となり、システム開発等により注力する体制を整えられた。また、不審ログが発見された際はログの詳細について調査依頼を行い、内部で確認した結果と併せて統合的にログの妥当性を判断する等インシデント対応時のログ分析でも利用した。他にもセキュリティインシデント発生時にインシデントの対応ノウハウを持つアナリストに相談等を行えるなど、サイバー攻撃発生時に最新のセキュリティ知識と対応ノウハウを保有する外部ベンダを活用できる体制を整えた。

４．取り組みに対する評価と課題

当社が実施した取り組みに対して評価を実施し、課題を洗い出し、それらに対応するための新たな計画を策定した。

４．１　自己評価と外部専門機関による第三者評価

取り組み内容と対応状況をまとめ、フレームワークを用いた自己評価及び外部専門機関による第三者評価を実施し、取り組みに対する課題を洗い出した。

４．１．１　金融機関や経済産業省のガイドライン等による自己評価

取り組みに対する評価として、１章でふれたフレームワークに、サプライチェーン等に関する統制項目を追加したＮＩＳＴ「重要インフラのサイバーセキュリティを向上させるためのフレームワーク第１．１版」を活用してこれまでの取り組みに対して再度、自己評価を行った（表５）。

主な要求事項	当社の対応状況	課題と当社対応
セキュリティソリューションの定期的な棚卸により、技術的な対策を継続的に改善している。	金融ＩＳＡＣや外部ベンダーからの情報収集等を踏まえて、有用なソリューションを導入した。	高度化・巧妙化する攻撃に対応した対策が必要。 ➜情報収集を継続し、ソリューションを最新化
ＣＳＩＲＴ要員等の権限を持つユーザーの役割と責任を明確化する。	・ＣＳＩＲＴ態勢強化のため、外部の専門人材２　名をキャリア採用した。 ・２０１７　年度にＣＳＩＲＴ人材育成計画を策定し、育成を推進。	人材の確保・育成が必要。 ➜専門資格の取得、金融ＩＳＡＣ活動などを通じてＣＳＩＲＴ人材を育成。
サプライチェーンのリスクマネジメントプロセスを特定、確立、評価、管理、合意する。	関連会社のセキュリティ対策状況を一覧化。また、年１回、各社Ｗｅｂ　サイトの脆弱性チェックを実施。	関連会社への攻撃を想定した態勢強化が必要。 ➜関連会社のセキュリティ対策の強化。
役職員にセキュリティ方針・手順を周知し、訓練等を実施する。	役職員向けに不審メール開封時の個人での対応と連絡先を記載した携帯カード配布と標的型メール攻撃訓練等を実施している。	不審メール見極めと手順どおりの対応が必要。 ➜不審メールの巧妙化を踏まえた訓練のさらなる高度化。

表５　ＮＩＳＴ「重要インフラのサイバーセキュリティを向上させるためのフレームワーク第１．１　版」を活用した評価結果

また、最新版金融庁アンケート「サイバーセキュリティに係る金融機関との建設的な対話と一斉把握」では、課題事項３１事例、標準事例２０事例全て対応が完了していることを確認した。

さらに、金融ＩＳＡＣ「ベストプラクティスガイドライン」や経済産業省「サイバーセキュリティ経営ガイドライン」を用いてリスクに対する自己評価を実施し、現時点での課

題・リスクがないことを確認した。

４．１．２　外部の専門機関によるセキュリティ体制の第三者評価

また、外部の専門機関独自のフレームワークを用いたセキュリティ対策状況の評価及びリスクの可視化を依頼した。

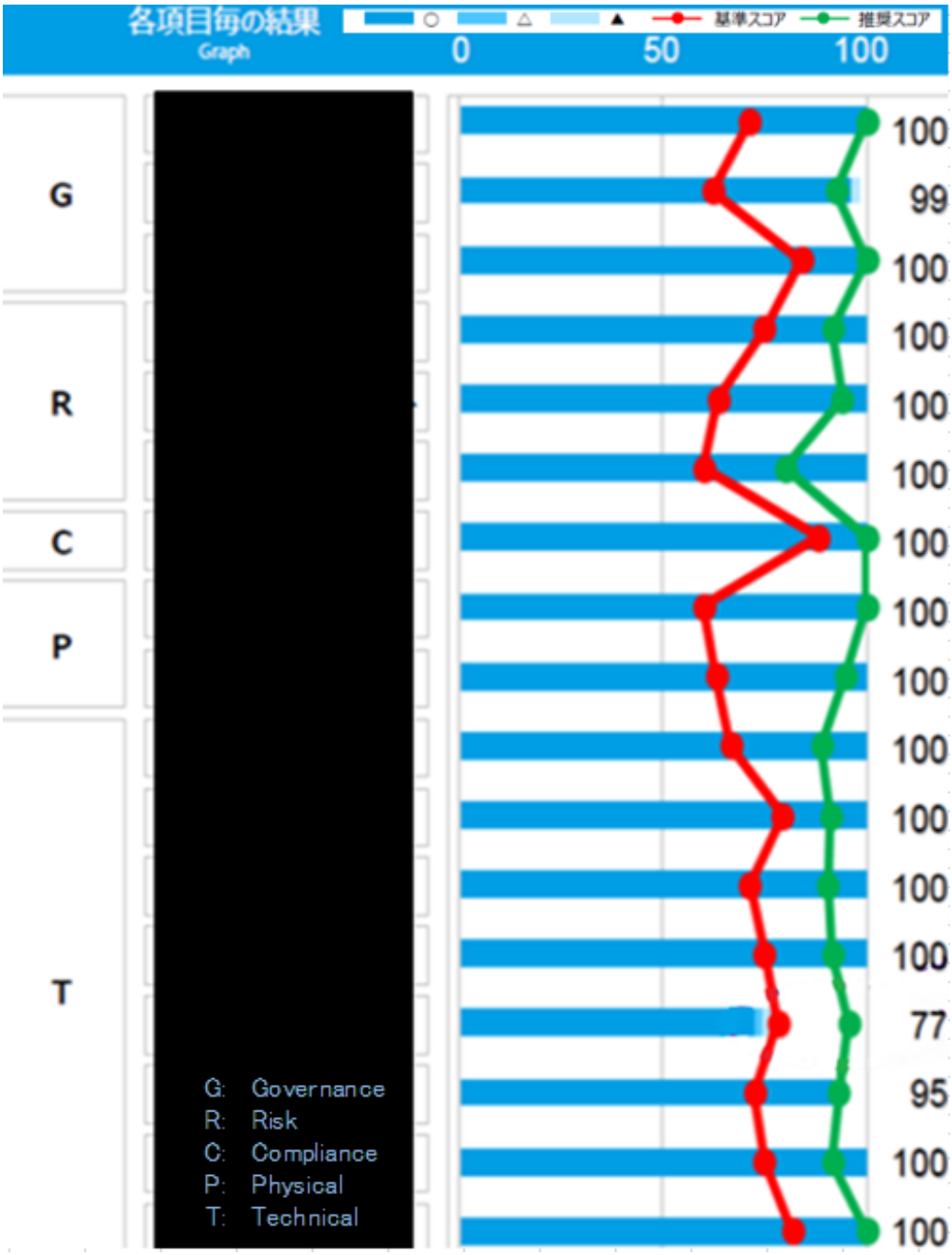


図４　第三者機関でのフレームワーク評価結果

定量・定性評価において、ほぼ全ての項目が推奨スコアを超えており、管理レベルは非常に高い結果となったが、緊急性は低いがわずかに改善点が検知された（図４）。

４．２　今後の取り組み方針

フレームワークによる自己評価および外部専門機関による第三者評価を踏まえて、今後の取り組み方針「情報セキュリティ強化の取り組み中期計画（２０１９～２０２１）」を策定した（表６）。

実施した取り組みは今後もまた、自己評価や外部機関による第三者評価を実施し、課題の検出と新たな取り組み計画を策定するといったＰＤＣＡサイクルをまわしていくことで当社のセキュリティを更に高水準に引き上げていく方針である。

主な取組み施策	内容
組織体制の強化	外部のセキュリティ専門機関による社内ネットワークへの侵入テスト（レッドチーム演習）を通じた課題の検出、改善。 〔内容〕 ・専門技術者が２～３週間にわたり、「内部への侵入」から「情報持ち出し」までのプロセスを一通り試みる。 ・ソリューションの有効性、設定不備、ＣＳＩＲＴ対応の適切性など耐性を評価、改善を提言。
内部対策の強化	緊急性の高い修正プログラムのすみやかな適用に加え、定期リリースされるプログラム適用の定例化。セキュリティソリューションの定期的な運用評価および改良対応。

表６　今後の主な取り組み施策

４．３　取り組みを振り返って

今回、活用したフレームワークは海外で作成されたものであるため、日本の金融企業への適応が困難な評価項目もあったが、金融ＩＳＡＣで収集した他社の事例を参考にすることでスムーズに評価項目を取捨選択することができた。

当社にとって最適なセキュリティ対策を目指して、セキュリティフレームワークを活用し、当社の状況を客観的な視点で把握したうえで対策を実施し、一定の効果を上げることができたと考える。金融ＩＳＡＣに参加し、セキュリティ対策は社内だけにとどまらない他社との密なコミュニケーションや定期的な運用評価と改善を継続することが重要であると実感した。

５．おわりに

今後、Ｔ＆Ｄ保険グループとして、より多くのビジネスチャンスを獲得し、多様な働き方を可能とするために「いつでも、どこでも」サービスを提供することが必要である。そのためには、クラウドや様々なデバイスの活用とそれらを安全に利用するためのセキュリティ対策が必要である。

変化し続ける環境の中で最適なサービス、最適なセキュリティを提供するために、情報収集・情報共有・評価をおこない、広い視野を持って、取り組んでいきたい。

以上