会誌「情報処理」Vol.64 No.11（Nov. 2023）「デジタルプラクティスコーナー」

日立ITユーザ会論文

# 顧客向け自社運用基盤へのSOCサービス適用によるサイバーセキュリティ対策強化

土井聡弘[1]　船井裕亮[1]　市川絵里奈[1]　緒方啓大[1]

[1]（株）日立システムズ

当社では，2020年度に顧客向け自社運用基盤において不正アクセスが確認され，多くのお客さまに多大なるご心配をおかけした．お客さまへの安全なサービスの提供，当社の経営リスク回避に向け，サイバーセキュリティ対策のさらなる強化が急務となった．この状況を踏まえ，2021年4月より，顧客向け自社運用基盤のセキュリティ運用監視を目的としたSecurity Operation Center（SOC）を新規に社内に立ち上げ，高度化するサイバー攻撃へのセキュリティ対策強化を社内IT部門，セキュリティ統括部門，品質保証部門が一体となって推進した．SOCの新たな立ち上げに伴う体制や業務プロセスを整備し，インシデント発生の早期検知，初動対応の強化など有事のセキュリティ対策強化を目的に，顧客向け自社運用基盤に対して「ログ監視サービス」適用を推進した．さらに，サイバー攻撃に対する平時のセキュリティ対策強化と継続的なリスク低減を目的に，セキュリティ設計や運用業務が日立グループのセキュリティ要件や基準を満たしているかを設計書，運用エビデンスを基に精査，評価する「セキュリティ運用チェックサービス」適用を推進した．また，セキュリティリスクの低減だけでなく，SOCサービスのプロセス自動化・効率化を推進した．ログ監視サービスのインシデント対応管理基盤としてServiceNowを導入し，関連部署がインシデント対応状況をタイムリーに参照できる基盤を整備した．また，プロセスマイニングソリューションとしてCelonisを適用し，業務プロセスの課題抽出，分析，改善を行い，SOCサービスの継続的改善プロセスを確立した．その結果，顧客向け自社運用基盤の効率的なセキュリティ強化・品質向上を実現した．

※本稿は第60回記念大会日立ITユーザ会論文です．


## 1. 会社概要とSOCサービス適用の背景

（株）日立システムズは，企業理念に掲げる「真に豊かな社会の実現に貢献する」ために，日立グループの社会イノベーション事業を支える一員としてサステナビリティ経営を推進している．強みであるさまざまな業種の課題解決で培ってきたお客さまの業務知識やノウハウを持つ人財・サービスインフラを活用したデジタライゼーションサービスと，日立の先進的なデジタル技

術を活用したLumada[1]やパートナと連携した独自のサービスによりお客さまのデジタル変革を徹底的にサポート．社会課題を解決するだけでなく，社会価値，環境価値，経済価値の3つの価値向上に貢献し，人々のQuality of Lifeの向上とお客さまの価値向上を支援していく．

当社では，2020年度に，当社が提供している顧客向け自社運用基盤（お客さまに提供しているサービスのうち，運用基盤を自社で管理しているサービス）の1つであるITシステムの運用監視サービスにおいて，不正アクセスが確認され，多くのお客さまに多大なご心配をおかけした．本事案発生の反省として，お客さまへの安心安全なサービスの提供およびサイバー攻撃に対する当社の経営リスク回避に向け，セキュリティ対策のさらなる強化が急務となり，顧客向け自社運用基盤セキュリティ強化プロジェクトを立ち上げた．本プロジェクトでは，2021年4月にSecurity Operation Center（以下，SOCと略す）を新規に社内に立ち上げ，技術的な知見を持つ社内IT部門，第三者評価としてのセキュリティ統括部門，顧客向け自社運用基盤の品質管理を主管する品質保証部門が一体となって，顧客向け自社運用基盤のサイバーセキュリティ対策強化を推進した．

本稿では，顧客向け自社運用基盤へのサイバーセキュリティ対策強化の取り組みについて，有事と平時の両面からセキュリティ対策を行い，第三者的視点でリスク評価することで効果的にセキュリティ品質を確保した事例と，ServiceNow[2]やCelonis[3]を用いたSOCサービスの自動化・効率化事例を紹介する．

## 2. SOCサービス適用に向けた取り組み

### 2.1 SOCサービス概要

サイバー攻撃や不正アクセスなどの脅威をいち早く検知し対応するには，SOCサービスを導入することが一般的である．しかし，当社では過去の経験から平時より適切なセキュリティ対策を継続的に行い，有事に備えることも同じく重要であると考えている．このような観点から，有事と平時の両面から顧客向け自社運用基盤のセキュリティ強化を行うため，SOCサービスを以下2サービスの構成とした（**図1**参照）．

（1）ログ監視サービス（有事に備えたインシデントの早期検知）
（2）セキュリティ運用チェックサービス（平時のセキュリティ運用定期評価と改善依頼）

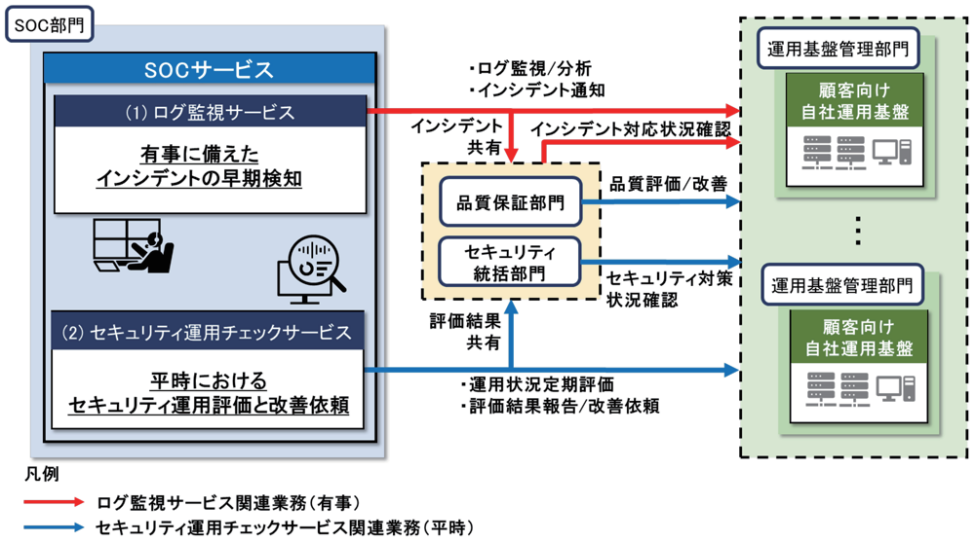


図1　SOCサービス概要

また，SOC立ち上げにあたり，日立グループのセキュリティポリシーに準拠した運用とするため，セキュリティポリシーを理解し日々実践している社内IT部門，セキュリティ統括部門，および，品質保証部門の3つの部門が一体となって推進する体制とした．SOCサービスに関連する各部門の主な役割は以下のとおりである．

・SOC部門　：社内IT部門が担当しSOCサービスを提供．セキュリティ技術面から顧客向け自社運用基盤のログ監視，分析とセキュリティ運用状況を評価
・運用基盤管理部門　：SOC部門からインシデント通知，評価結果報告を受領し改善を実施
・セキュリティ統括部門：SOC部門からの評価結果を基に，運用基盤管理部門に対しセキュリティ対策実施状況の確認を実施
・品質保証部門　：SOC部門からの評価結果を基に，運用基盤管理部門に対しサービス品質評価と改善指示を実施

これまでも当社では，顧客向け自社運用基盤に対する平時のセキュリティ運用チェックを行っていたが，運用基盤管理部門の技術者が独自で評価していた．しかし，近年のサイバー攻撃の高度化と加速的変化に加え，運用基盤管理部門と顧客間でサービス継続を重視するケースも多く，セキュリティ対応の優先度を運用基盤管理部門が独自で評価・判断することにセキュリティリスクが生じていた．そのため，当社のSOCサービスはSOC部門がログ監視サービスとセキュリティ運用チェックサービスによる有事と平時の両面でのセキュリティ評価を行っている．各サービスの詳細は「2.3　ログ監視サービス」と「2.4　セキュリティ運用チェックサービス」にて詳述する．

単なるSOC導入によるセキュリティ強化ではなく，セキュリティに関する技術的な部分をSOCが監視，分析し，その分析結果をセキュリティ統括部門や品質保証部門が評価することで，セキュリティリスクを第三者の観点から定量的かつ客観的に評価し，顧客提供サービスのセキュリティ強化対策を行っている．

## 2.2　SOCサービス推進スケジュール

SOC立ち上げからの推進スケジュールは**図2**のとおりである.

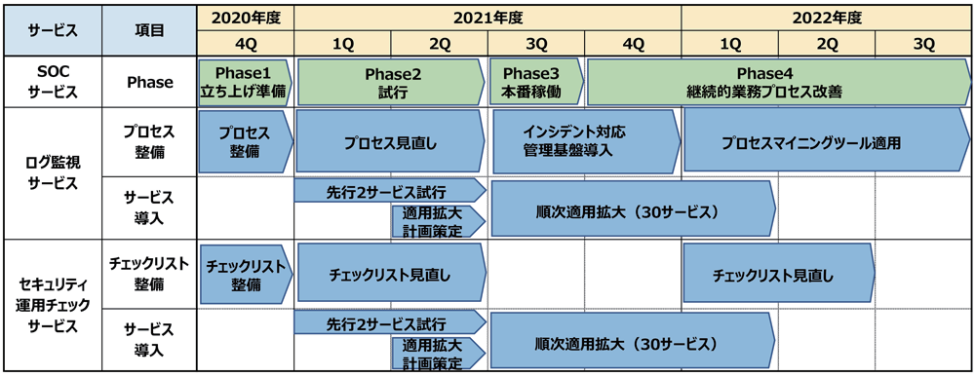


図2　推進スケジュール

Phase1では，2020年度の4QにSOC立ち上げ準備として，SOCサービスの業務設計，システム設計・構築を実施し，業務プロセスやドキュメント類の整備を実施した．Phase2として，先の当社への不正アクセス確認を受け改善対応を終えたサービス，および，特定多数のお客さまに提供しインシデントが発生した際のビジネスインパクトが大きいサービスの2サービスを試行対象として選定し，2021年4月からSOCサービスを適用させた．Phase3の本番稼働からは，当社の顧客向け自社運用基盤へ順次SOCサービスを適用し，最終的には30サービスまで適用を拡大した．Phase4ではSOCサービスの業務体制整備，および業務プロセスの評価，改善を行った．特に，ログ監視サービスにおいて，インシデント対応状況を関係者間でタイムリーに可視化するため，発生したインシデントの対応状況が，SOC部門，運用基盤管理部門だけでなく，品質保証部門，セキュリティ統括部門も把握できるよう，インシデント対応管理基盤としてServiceNowを導入する大規模な改善を加えた．また，インシデント対応管理基盤上で行われた操作ログを収集し，プロセスマイニングソリューションを適用することで，SOC業務プロセスの課題や問題点を抽出し，効率的な業務改善を継続的に行える仕組みを確立した.

## 2.3　ログ監視サービス

### 2.3.1　ログ監視サービス概要

本節では，SOCサービスを構成するサービスの1つであるログ監視サービスについて述べる．ログ監視サービスとは，顧客向け自社運用基盤の監視対象デバイス（エンドポイント，ファイアウォール，ネットワーク機器等）から出力された各種ログやアラートをモニタリングすることにより，サイバー攻撃や不正な挙動を早期に検知，分析し，その分析結果の通知と脅威への対処をサポートするサービスである.

ログ監視サービスの概要を**図3**に示す．顧客向け自社運用基盤で運用されているサーバやネットワーク機器等の監視対象デバイスから，イベントログやアクセスログ等の各種ログを継続的に収集し，リアルタイムで当該ログを監視・分析可能な環境を整備している.

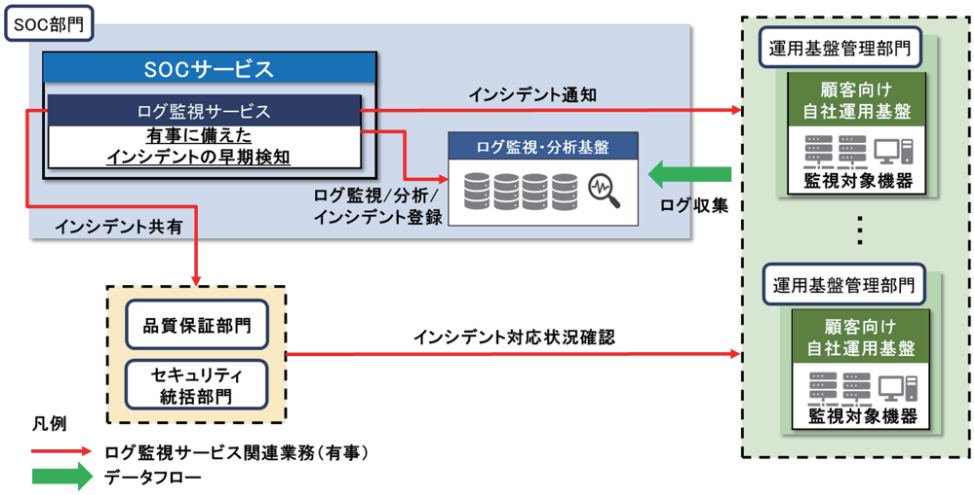


図3　ログ監視サービス概要

ログ監視サービスの業務フローを**図4**に示す．ログ監視・分析基盤にてアラートを検知した場合，まずアラートの初期分析から開始する．初期分析の結果，誤検知ではなく脅威と判断された場合，詳細分析を実施する．詳細分析では，あらかじめ定義したセベリティ（重大度）判定表に基づき，セベリティを決定する．セベリティ判定表は過去のインシデント分析の蓄積データや，監視対象デバイスの種類等に基づいて定義されており，セベリティは重大度の高い順から以下3段階で定義されている．

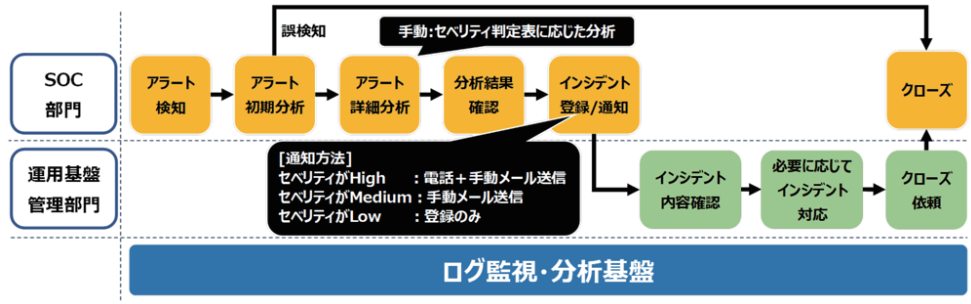


図4　ログ監視サービス業務フロー

・High（高）　：実際にセキュリティ侵害が発生している可能性が高い検知
・Medium（中）：ぜい弱性をついた攻撃等，セキュリティ侵害が発生する可能性のある攻撃検知
・Low（低）　：スキャン等偵察レベルの攻撃検知

詳細分析の結果，セベリティ・推定される影響・推奨する対応策を添え，分析内容に誤りがないことを別の担当者がクロスチェックした上で，運用基盤管理部門へインシデントとして通知する．インシデント通知においては，セベリティに応じて通知方法と通知時間（セベリティ確定からインシデント通知までの時間）が異なる．High（高）の場合，運用基盤管理部門，品質保証部門，セキュリティ統括部門へ電話連絡および手動でのメール送信を30分以内に実施，Medium（中）の場合，運用基盤管理部門へ手動でのメール送信を60分以内に実施，と定めている．イン

シデント通知後，運用基盤管理部門にてインシデントの内容確認を実施する．システムへの影響確認を実施し，必要に応じてインシデント対応を実施した上で，SOC部門にクローズ依頼を行う．SOC部門ではクローズ理由の妥当性を確認し，インシデントをクローズする．

### 2.3.2　ログ監視サービス適用推進

ログ監視サービス適用推進にあたり，まずは2020年度の4QにPhase1（立ち上げ準備）として，ログ監視サービスの業務プロセス設計，業務体制整備，セベリティ判定書・手順書等運用ドキュメント類の整備を実施し，サービスを提供するための環境を整えた．次に，Phase2（試行）として，あらかじめ選定した2サービスに対し2021年4月から試行を開始した．Phase1の立ち上げ準備に要した期間がわずか3カ月しかなく，最低限の業務体制・業務プロセス，運用ドキュメントを整備した上で試行を開始しているため，2021年10月からのPhase3（本番稼働）までに対処すべき課題の洗い出しと見直しを並行して行う必要があった．主な課題と見直し結果は**表1**のとおりである．

表1　本番稼働に向けた課題と見直し結果

| 項目 | 試行時(Phase2)の<br>運用状況 | 試行(Phase2)における課題 | 本番稼働時(Phase3)の<br>見直し結果 |
|---|---|---|---|
| サービス<br>稼働時間 | 平日のみ<br>09:00-17:00<br>(Highインシデントは<br>24時間365日対応) | 休日に発生したアラート、インシデントを<br>タイムリーに運用基盤管理部門に<br>連携できない | 平日＋休日･祝日(365日対応)<br>09:00-17:00<br>(Highインシデントは<br>24時間365日対応) |
| 業務体制 | [2021年4-5月]<br>アラート分析手順共有も兼ねて<br>全員で対応<br>[2021年6-9月]<br>4グループ編成<br>(各グループの人数は不統一) | ･あるグループで発生した例外事項の<br>引き継ぎが漏れる可能性あり<br>･業務都合でのシフト変更が<br>円滑に実施できない<br>･アラート詳細分析時の分析スキルが<br>特定のグループに偏在 | ･1グループあたり3、4名の<br>4グループに編成<br>･引き継ぎ事項を日次で共有<br>･シフト変更方法を定義<br>･グループ編成を定期的に変更し、<br>分析スキルを平準化 |
| 業務プロセス | 業務フローレベルの大まかな手順<br>に基づき業務を実施 | ･グループ間で分析結果の記述方法や<br>クロスチェックの実施方法等細かい点で<br>手順が異なっており、サービス品質にリスクあり | 業務フローレベルだけではなく、<br>手順レベルで運用手順書を整備 |

Phase3（本番稼働）として，2021年10月より表1で見直したサービス稼働時間・業務体制・業務プロセスをベースに，顧客向け自社運用基盤に対して順次ログ監視サービスを適用し，30サービスまで適用を拡大した．30サービスの選定にあたっては，セキュリティリスクやビジネスインパクトを考慮し，以下2点を条件に選定した．

- 外部公開あり（インターネットに接続されている）
- 複数（2社以上）の顧客にサービスを提供している

ログ監視サービス適用においては，インシデント通知後の運用基盤管理部門側の業務プロセスの整備・変更や，緊急対応としての体制確保などの対応も必要となり，運用しているサービスの継続性・損益管理にも影響を及ぼすこととなる．そのため，SOCサービスのサービス仕様や機能面に関することだけではなく，本取り組みの背景や重要性，効果を根気強く丁寧に説明し，ログ監視サービス導入に対し，運用基盤管理部門の協力と理解を得た上で，ログ監視サービスを適用推進した．

## 2.4　セキュリティ運用チェックサービス

### 2.4.1　セキュリティ運用チェックサービス概要

本節では，SOCサービスを構成するもう1つのサービスであるセキュリティ運用チェックサービスについて述べる．セキュリティ運用チェックサービスとは，平時のサイバーセキュリティ対策強化を目的として，顧客向け自社運用基盤のセキュリティ対策状況や運用業務が日立グループのセキュリティ要件や基準を満たしているかどうか精査し，評価するサービスである．

導入時期が古いサービス等では設計や運用プロセスが最新のセキュリティ要件を満たしていないサービスがあるため，運用基盤管理部門に代わりシステム内のネットワーク機器やサーバ，運用業務で利用するクライアント端末等の運用エビデンスを基に，第三者としてセキュリティ運用チェックを実施する．

セキュリティ運用チェックを行う前提として，対象サービスの資産を事前確認し特定する．その後，運用基盤管理部門の担当者と打合せを行い，チェック対象とする機器やそのチェックの必要性をお互いに明確にした上でチェックを実施する．

SOC部門が対象機器における運用設計および業務運用プロセスのセキュリティリスクを洗い出し，結果をレポートにまとめ，報告する．報告書に基づき運用基盤管理部門は改善を行うことで，セキュリティリスクに対する平時の強化対策と継続的なリスク低減を行うセキュリティ運用チェックプロセスを確立させた．

セキュリティ運用チェックプロセスは**図5**に示すとおり，以下の流れで定期的に実施する．

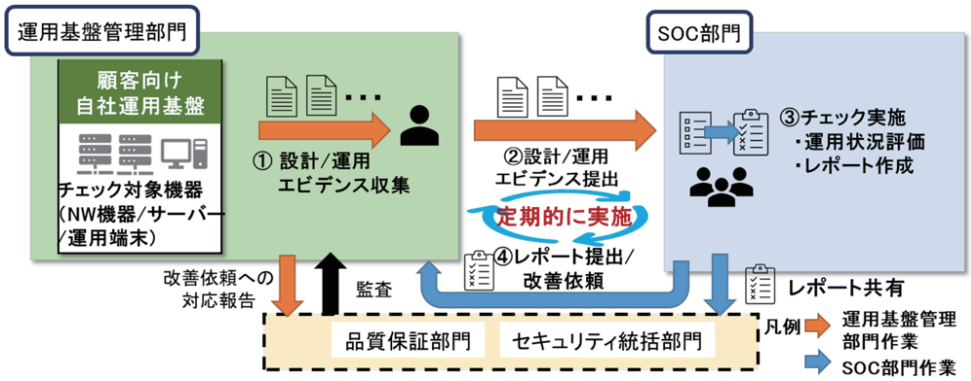


図5　セキュリティ運用チェック概要図

① 設計，運用エビデンス収集
運用基盤管理部門の担当者がセキュリティ運用チェックに関連した設計書および運用エビデンスを収集する．

② 設計，運用エビデンス提出
運用基盤管理部門の担当者がSOC部門にエビデンスを提出する．

③ チェック実施
SOC部門がセキュリティ運用チェックを行い，評価結果としてレポートを作成する．

④ レポート提出，改善依頼
SOC部門が運用基盤管理部門へレポートを提出し，是正，改善を依頼する．レポート内容については，品質保証部門やセキュリティ統括部門にも共有する．

### 2.4.2　セキュリティ運用チェックサービス適用推進

Phase1のチェックリスト整備では，セキュリティ運用チェックで利用するチェックリストの作成，および評価方法の検討を行った．チェックリストの項目は，近年のサイバーセキュリティの傾向などを加味するため，IPA（（独）情報処理推進機構）や日立製作所など，さまざまな組織，団体が発行する基準やチェックリスト等を精査，検討した．検討の結果，基本的な要件から応用的な項目まで幅広く網羅している日立製作所のセキュリティ機能要件チェックリストを主な基準として採用し，チェックリストを作成した．また，当社内で実施している社内IT機器ぜい弱性点検（PCヘルスチェック）におけるチェック項目や，過去のセキュリティインシデント事例，システム構成ごとの注意点（オンプレミス環境，クラウド環境等）などを，セキュリティ対策のチェック項目に加え，チェックリストを完成させた．

Phase2では試行対象として選定した顧客向け自社運用基盤2サービスに対してセキュリティ運用チェックサービスを先行適用した．試行の結果を受け，以下のとおり，セキュリティ運用チェックサービスにおける課題を抽出し，それぞれ対策を実施した．

【課題1】1つのチェック項目に対して複数のチェック観点が含まれていたり，チェック対象の機器が明確に定められていたりしないことで，チェックの品質にばらつきが発生した．
【対策1】チェック項目の分類やカテゴリを見直し，単独のチェック観点や対象機器ごとにチェックが行えるよう改善した（**図6**参照）．

【課題2】運用状況を確認するためのエビデンスの内容に不足が見られたり，チェックを行うSOC部門が想定するエビデンスではないものが提出されたりするなど，運用基盤管理部門とSOC部門との間に提出エビデンスに関する認識齟齬が発生した．
【対策2】全チェック項目に対して，想定する設計書や運用エビデンスを明確に記載する改善をした（**図6**参照）．

【課題3】チェックを行う担当者の前提知識やチェックにおける考え方が異なることにより，評価結果にばらつきが発生した．
【対策3】設計エビデンスと運用エビデンスの判定に明確な基準を設け，両者のチェック結果レベルを基に，「重大な指摘あり」「指摘あり」「軽微な指摘あり」「指摘なし」の4段階に分けて総合判定するように，チェック結果判定基準を改善した（**図7**参照）．

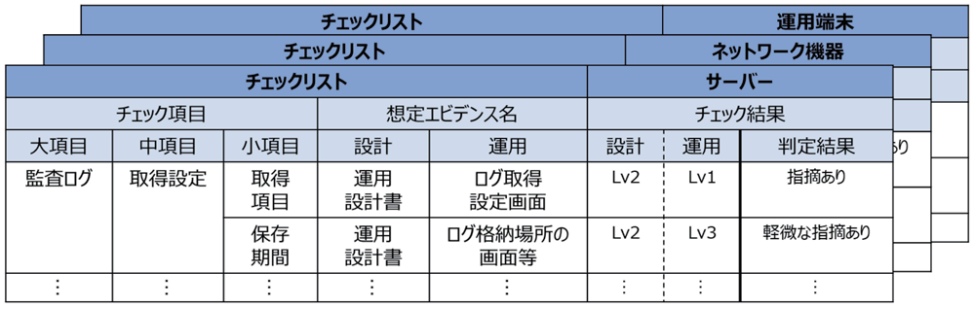


図6　セキュリティ運用チェックリスト例

**ステップ1：設計、運用エビデンスに対する判定**

| チェック結果レベル | 判定基準 | |
|---|---|---|
| | 設計エビデンス | 運用エビデンス |
| 重大 | | エビデンス内容に重大な問題がある場合<br>(未対策のサポート切れ製品が使用されている等) |
| Lv1 | エビデンス提出有無に関わらず、<br>大項目単位で設計内容確認不可 | エビデンスが提出されておらず、運用実態確認不可 |
| Lv2 | エビデンスが提出がされており、大項目単位で設計が確認できるが、小項目単位で設計確認不可 | エビデンスが提出されているが、内容に問題あり |
| Lv3 | エビデンスが提出されており、<br>小項目単位で設計が確認できる | エビデンスが提出されており、内容に問題なし |

**ステップ2：各チェック結果レベルから総合判定結果を導出**

| チェック結果レベル | | 総合判定結果 | 判定結果説明 |
|---|---|---|---|
| 設計 | 運用 | | |
| - | 重大 | 重大な指摘あり | 直ちに対策が必要な問題あり<br>(未対策のサポート切れ製品/ソフトウェアの使用等) |
| Lv1 | Lv1 | | 設計エビデンス、運用エビデンスともに確認できず、実態確認不可 |
| Lv1 | Lv2/3 | 指摘あり | 設計エビデンスに運用設計/運用方針の記載なし |
| Lv2/3 | Lv1 | | チェック項目を満たす運用エビデンスの確認不可 |
| Lv2/3 | Lv2 | | 運用エビデンスが提出されているが、内容に問題あり |
| Lv2 | Lv3 | 軽微な指摘あり | 設計エビデンスの項目不足など内容に一部問題あり |
| Lv3 | Lv3 | 指摘なし | 設計通りに運用されていることが確認できている |

図7　チェック結果判定基準の改善

これらの改善を行い，ベースとした日立製作所のセキュリティ機能要件チェックリストの更新に合わせて，2021年上期にチェックリストの改訂を実施．追加や更新内容を運用基盤管理部門へ説明し，説明会での意見や質疑の内容をさらにチェックリストへ反映した．改善を加えたセキュリティ運用チェックリストをPhase3から順次，顧客向け自社運用基盤へ適用した．

各顧客向け自社運用基盤の運用基盤管理部門へは，チェックリストのチェック結果を一覧で提出するだけではなく，結果をレポートの総評として整理し，より重要度の高い判定から適切に対応するように報告している．重大な指摘事項であれば即日対応，軽微な指摘事項であれば次回のチェック時（半年後）までに対応，など指摘レベルによって期日設定やフォローを行っている．レポートの総評例を**図8**に記載する．

**■総評例**

セキュリティ運用チェックの結果、改善が必要な指摘事項は、「指摘あり」1件と、「軽微な指摘あり」13件です。
次回チェック時までに修正を確認できるように優先度を設け、計画的に改善するよう努めてください。
以下「指摘概要」に主な指摘事項を抜粋して記載しています。詳細は、別紙チェックリストをご参照の程よろしくお願いします。

1.指摘概要
1-1.「指摘あり」指摘事項
　一部のチェック項目に対する運用エビデンスを確認できません。
　運用実態を確認できないため、運用エビデンスを取得のうえ、提出をお願いいたします。
　・ログのバックアップ取得について運用エビデンスを確認できません。
　　また、バックアップ取得対象のログについて、設計書に「対象仮想マシンのOSシステムログ、トラップログ、リソース収集データ
　　監視ログを取得する」と記載されていますが、提出されたエビデンスはOSシステムログのみであるため、他のログについても提出してください。
1-2.「軽微な指摘あり」指摘事項
　指摘事項の内容は、設計書における一部整合性誤りです。以下に一部抜粋して記載します。
　・脆弱性管理台帳の対象機器について、設計書の内容と運用エビデンスに一部不整合が見受けられます。
　　設計書の対象機器(サーバー(7台))に過不足がないかご確認をお願いします。
　・設計書へのアカウントロックアウトに関する記述が一部不足しています。運用エビデンスと整合性のある内容へ更新してください。
　・不要アカウントの棚卸について、設計書にアカウント抽出/アカウントの段階的な無効化を概要として記載されていますが、
　　詳細な実施、管理方法や実施時期について追記してください。

図8　レポートの総評例

## 2.5　SOCサービス運用における課題

ここまで，SOCサービスを構成するログ監視サービスとセキュリティ運用チェックサービスの概要，および各サービスの適用推進状況について述べてきた．本節では，2つのサービスを試行，本番稼働した結果明らかになってきたSOCサービス運用における課題について述べる．**表2**に課題と対策，対策状況を示す．

表2　SOCサービス運用における課題と対策，および対策状況

| 対象サービス | 課題 | 対策 | 対策状況 |
|---|---|---|---|
| ログ監視サービス | ・関係部門間でのタイムリーな情報共有が困難<br>・インシデントクローズ理由の妥当性を品質保証部門が確認できていない<br>・手動オペレーションが多く、サービス品質維持にリスクあり、監視対象拡大時に工数大 | インシデント関連情報の可視化による、品質保証部門、セキュリティ統括部門とのタイムリーな情報共有、また、業務自動化・効率化によるサービス品質向上を目的にインシデント対応管理基盤としてServiceNowを導入 | 実施済（22/1Q） |
| | 設計した業務フローに基づいて業務を実施しているが、各人の作業手順が異なり、業務品質がばらばら | プロセスマイニングツールを適用し、定期的に業務プロセス分析・評価・改善を実施することで、業務品質向上を図るとともに、継続的プロセス改善を確立 | 実施済（22/1Q） |
| | アラート分析やインシデント対応手順のノウハウ蓄積 | 類似アラート、インシデントを参考にした分析・対応方法を検討中 | 23年度実施予定 |
| セキュリティ運用チェックサービス | ・運用基盤管理部門へのフォロー頻度が多く、フォローメール作成に時間がかかる<br>・セキュリティ運用チェックレポート作成に時間がかかる | ServiceNow導入によるメール送信自動化、レポート作成自動化を検討中 | 22/4Q実施予定 |
| | サービス新規適用時の準備に時間がかかる | ツールでの自動化・効率化を検討中 | 22/4Q実施予定 |

ログ監視サービスでは，ログ監視・分析基盤上におけるSOC部門と管理基盤運用部門の間でのやりとりにとどまっており，関連部門含めたタイムリーな情報共有ができておらず，品質保証部門でのクローズ理由の妥当性確認等が機能していなかった．また，手動オペレーションが多いことで作業ミスが発生する可能性が高く，今後の監視対象拡大に向けて，SOCサービスの品質を維持することが難しかった．これらの課題に対策すべく，インシデント対応管理基盤としてServiceNowを導入した．アラートやインシデント情報を可視化することで，タイムリーな情報共有とアラート分析業務の自動化・効率化によるSOCサービス品質向上を図った．

また，ログ監視サービスの別の課題として，あらかじめ設計した業務プロセスに基づいて業務を実施するよう指示しているものの，各人の間でアラート分析内容や分析時間にばらつきが見られ，実際に業務プロセスにしたがって正しく運用されているか不透明な状況であった．そこで，プロセスマイニングソリューションを適用することで，定期的に業務プロセスを分析・評価・改善することで，継続的にSOCサービスの品質向上を図ることとした．

さらに，ログ監視サービスにおいて，アラート分析やインシデント対応手順のノウハウ蓄積方法に課題がある．本課題に対しては，過去の類似アラートや類似インシデントを基にした分析・対応方法について検討中である．

次に，セキュリティ運用チェックサービスでは，以下の課題が存在する．

- 運用基盤管理部門に対するエビデンス提出フォロー頻度が高く，フォローメール作成に時間がかかる
- セキュリティ運用チェック結果の集計，レポート作成に時間がかかる
- セキュリティ運用チェックサービス新規適用時の事前準備に時間がかかる

これらの課題に対しては，ログ監視サービス同様にServiceNow導入および，ツールでの自動化・効率化を図ることを検討中である．

第3章では，このうち特に，すでに対策実施済の課題として，ログ監視サービスにインシデント対応管理基盤を導入した事例と，プロセスマイニングソリューションを適用した事例を述べる．

## 3. SOCサービス改善に向けた取り組み

### 3.1 インシデント対応管理基盤導入

前節で述べたとおり，本番稼働後のログ監視サービス運用において，以下の課題があった．

- インシデントに関連する情報がタイムリーに関係部門間（SOC部門，運用基盤管理部門，品質保証部門，セキュリティ統括部門）で共有されていない
- 現状の業務プロセスや体制を踏まえると，ログ監視サービス適用対象拡大後のアラート分析やインシデント通知の作業量が膨大になり，サービス品質維持にリスクあり

そこで，インシデント関連情報の可視化，およびログ監視サービス業務の自動化・効率化を目的として，新しくインシデント対応管理基盤を導入した．

インシデント対応管理基盤として，導入の容易性およびシステム柔軟性が高いことから，ServiceNow, Inc.が提供する企業向け統合サービスマネジメントサービス（SaaS）のServiceNowソフトウェアを選定した．そのうち，今回は導入目的を考慮し，セキュリティオペレーションのセキュリティインシデントレスポンスアプリケーション（Security Operations Standard - SIR）[4]を導入した．

インシデント対応管理基盤導入後の全体概要図を**図9**に示す．ログ監視・分析基盤からインシデント対応管理基盤導入へアラート等のデータを連携し，インシデント関連データをインシデント対応管理基盤において一元的に管理することにより，SOC部門・運用基盤管理部門だけではなく，品質保証部門・セキュリティ統括部門においてもタイムリーにインシデント対応状況を参照することが可能となった．

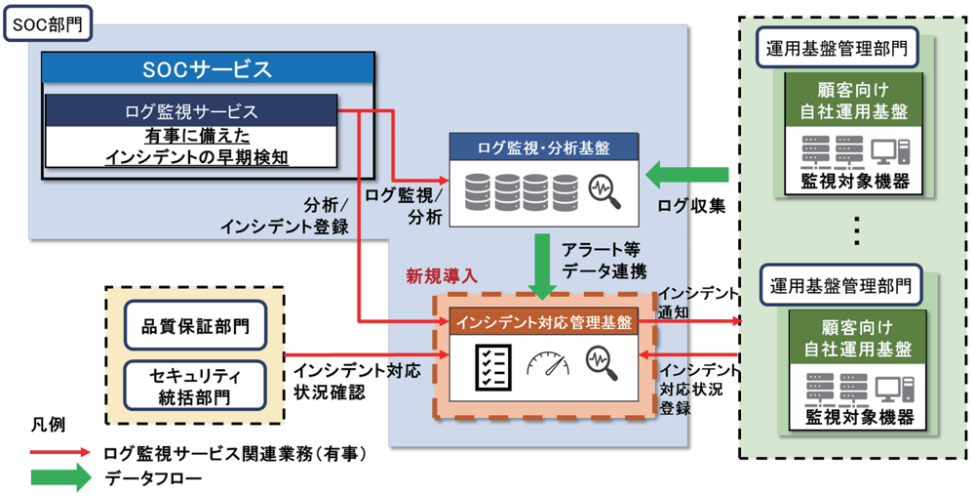


図9　インシデント対応管理基盤導入後のログ監視サービス概要

今回，インシデント対応管理基盤導入により，インシデント対応状況の可視化とログ監視サービス業務の自動化・効率化に関して改善を図った．以下，それぞれの改善について具体的に説明する．

### （1）インシデント対応状況の可視化

インシデント対応状況の可視化にあたっては，ダッシュボード機能を利用した．インシデント対応管理基盤にログインする部門の役割ごとに必要な情報が異なるため，各部門に対してダッシュボードに表示する情報をヒアリング・整理した上で，可視化する環境を整備した．

- SOC部門および運用基盤管理部門
- 未着手，仕掛中，未クローズ等の要対応インシデント情報を表示
- 品質保証部門およびセキュリティ統括部門
- オブザーバとして，インシデントの傾向把握に必要なインシデント件数推移等の情報を表示

**図10**にインシデント対応状況可視化の例を示す．

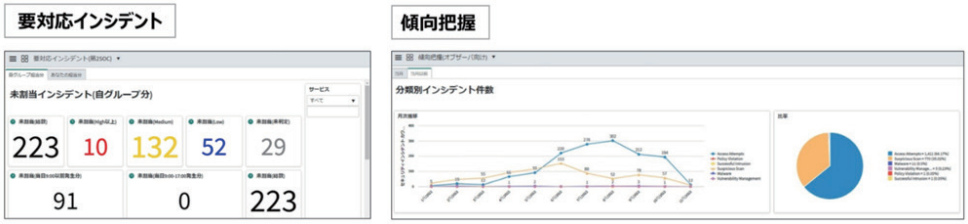


図10　インシデント対応状況可視化の例

### （2）ログ監視サービス業務の自動化・効率化

ログ監視サービス業務の自動化・効率化については，手動でのオペレーションにおいて作業ミスが発生しやすい以下3つの点に焦点を当てて，推進した．

① セベリティ判定自動化
ログ監視・分析基盤に存在するアラート等のデータをインシデント対応管理基盤へインポートした後，セベリティが自動判定される仕組みとした．これまではセベリティ判定表を利用して手動で判定していたが，ServiceNowのビジネスルールと呼ばれる機能を活用することで，セベリティ判定表の判定ロジックを組み込み，セベリティを自動判定している．

② 分析結果テンプレート取得自動化
アラートの詳細分析を行う際，これまではアラートのパターンごとにMicrosoft Excel[5]で一覧化していた分析結果テンプレートと照合してから，分析に着手していた．今回，インシデント対応管理基盤を導入したことで，アラートに対応した分析結果テンプレートを自動で取得することが可能となり，誤った分析結果テンプレートを用いて分析着手することを抑止した．

③ インシデント通知メール送信自動化
運用管理基盤部門へインシデント通知メールを送信する際，これまではMicrosoft Excelで管理していた宛先一覧を確認して，分析結果をメール本文に貼り付けた上で送信していた．今回，インシデント対応管理基盤を導入したことで，事前に登録しておいた運用管理基盤部門の宛先と，インシデント対応管理基盤に登録した分析結果をベースに，自動でメ

ール送信する仕組みとした．

**図11**に，上記3点の自動化・効率化の適用個所を図示した．インシデント管理基盤導入後のログ監視サービス業務フローを示す．

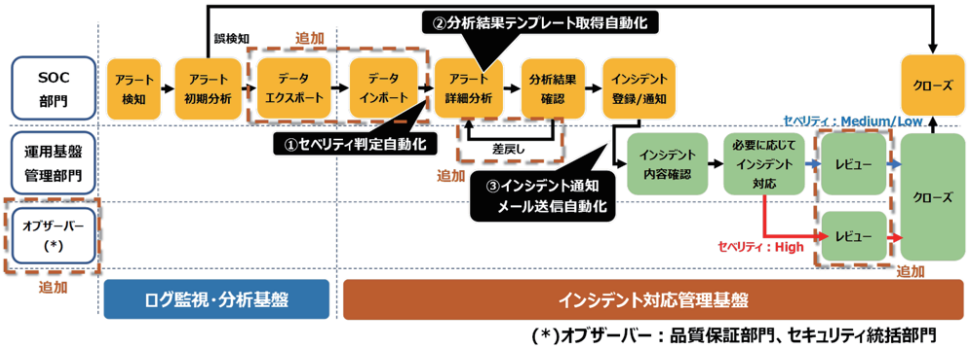


図11　インシデント管理基盤導入後のログ監視サービス業務フロー

### 3.2　プロセスマイニングによる継続的改善プロセスの確立

プロセスマイニングとは，システムからさまざまな業務活動の操作ログを継続的に収集し，業務プロセスを可視化，分析することで，プロセスの改善ポイントを抽出し，業務改善に活用する手法である．プロセスマネジメントを進めるには改善サイクルを継続的に回す必要があり，プロセスマイニングはこれに対する非常に有効な手段である．

ログ監視サービス稼働後，設計した業務フローに基づいて運用手順を整備してはいたものの，作業の手戻りや分析内容の誤りによる差し戻しが発生したり，各メンバの間で分析時間や分析内容にばらつきが生じたりしている状況であり，サービス品質維持に課題があった．そこで，設計した業務フローに対して想定外の業務フローが発生していないかどうか，業務プロセスに課題がないかどうかを明らかにするため，プロセスマイニングを適用することとした．ただし，プロセスマイニングを適用するためには，システムでの操作ログを収集できることが前提であるが，ログ監視・分析基盤では必要なログを収集することができなかった．そこで，前節で述べた，インシデント対応管理基盤導入後に，業務プロセスの標準化を目的として，ログ監視サービスにプロセスマイニングを適用した．プロセスマイニングソリューションとして，社内ですでに導入実績のある「Celonis Execution Management System（EMS）」（以下，Celonis）を採用した．**図12**にCelonis適用イメージを示す．

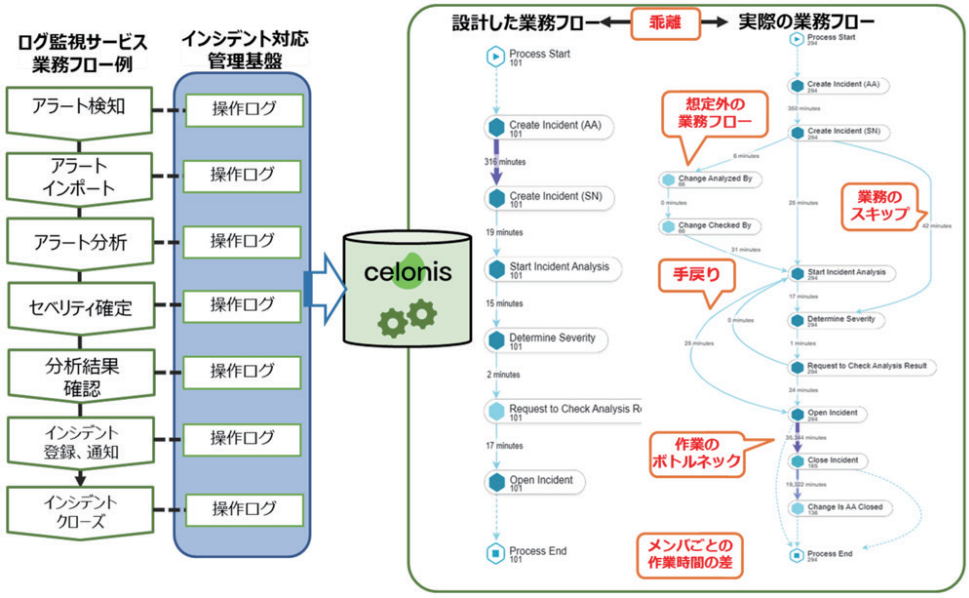


図12　Celonis適用イメージ

ログ監視サービスにプロセスマイニングを適用するにあたり，以下4つのステップで推進してきた．

**（1）KPI設計・アクティビティ定義**

ログ監視サービスの課題抽出を実施し，以下3つのカテゴリごとに，プロセスマイニングで可視化すべき数値をKPIとして設計した．

- プロセス明確化による作業ミスの解消：差し戻し件数，手戻り件数等
- 業務効率向上による工数低減　　：リードタイム（分析時間，分析結果確認時間等）
- リスク管理　　：業務プロセス適合率等

上記KPIを可視化するために必要なアクティビティ（図12のログ監視サービス業務フロー例に記載のアラート検知，アラート分析等のひとまとまりの操作単位のこと）を定義する必要がある．今回，Celonisに用意されていたServiceNow用のテンプレートを参考に一部カスタマイズを加えてアクティビティを定義した．

**（2）データ連携・アクティビティ設定・分析シート作成**

インシデント対応管理基盤で発生したログ監視サービスの操作ログをCelonisに連携する設定を実施した．CelonisではServiceNowからデータを連携するテンプレートが用意されているため，スムーズにデータ連携設定を完了することができた．また，（1）で定義したアクティビティを画面に表示するための設定を実施した．さらに，KPIと業務プロセスを可視化すべく，Celonisで分析シートを作成した．**図13**に分析シートのサンプルを示す．


図13　分析シートサンプル

### （3）分析実施・改善策検討

（2）で作成した分析シートを基に，SOC部門，および過去に社内で他業務のプロセスマイニングに携わった関係者を集めて分析ワークショップを実施し，簡易分析を実施した．その後，改善効果が高いと見込まれる業務プロセス適合率，差し戻し件数に詳細分析対象を絞り込んだ．業務プロセス適合率については逸脱パターンの上位4件の詳細分析を実施し，差し戻し件数については差し戻しによる損失時間が60分を超えていたインシデント上位10件について詳細分析を実施した．その結果，下記の分析結果を得た．

- アラート検知パターンの混在による分析着手遅延，分析漏れが発生
- 設計した業務プロセスにしたがって実行していないケースが9%発生
- 変更すべきでないタイミングで，分析結果やインシデント件名の修正が8%発生

上記分析結果を基に，再度関係者を集めて，改善策を検討するためのワークショップを実施した．その結果，インシデント対応管理基盤に対する改善策として，以下を立案した．

- インシデント対応管理基盤の仕様変更（アラート検知パターンベースでの分析自動化）
- 調査にあたってのポイントをインシデント対応管理基盤の画面に表示して注意を喚起
- 変更すべきでないタイミングと対象の項目をインシデント対応管理基盤側で制御

### （4）改善策適用・適用後評価，分析

（3）で立案した改善策をインシデント対応管理基盤に対して適用完了した．本稿執筆時点（2022年11月）現在，適用後における業務プロセスで運用中であり，改善適用効果を評価，分析中である．

## 4. SOCサービス適用・改善による成果

本章では，SOCサービス適用による成果と，インシデント対応管理基盤導入，プロセスマイニングソリューション適用によるSOCサービス改善の定量的効果・定性的効果について述べる．

### （1）定量的効果

**◆SOCサービス適用による成果**

- ログ監視サービスでのインシデント約5,900件（Medium：約2,500件，Low：3,400

件）（2022年10月末時点）の検知・通知による，インシデント早期発見とセキュリティリスク低減

**◆SOCサービス改善による成果**

- インシデント対応管理基盤導入による業務改善効果
  分析業務自動化・効率化による作業工数削減：約75%削減
- プロセスマイニング適用による業務改善効果
  ① 手戻り発生抑止によるインシデント対応時間削減：約33分／日の削減
  改善適用前：手戻り件数　1件／日，手戻りによる平均損失時間約46分／日
  改善適用後：手戻り件数0.3件／日，手戻りによる平均損失時間約13分／日
  ② 業務プロセス適合率向上：75%から90%へ増加によるサービス品質向上

### （2）定性的効果

**◆SOCサービス適用による成果**

- SOCサービスをわずか3カ月で早期に立ち上げ，顧客向け自社運用基盤30サービスへのログ監視サービス，セキュリティ運用チェックサービス適用により，有事と平時両面からのサイバーセキュリティ対策を強化
- セキュリティ運用チェックサービスでの設計・運用エビデンスに基づく定期的評価による，平時における顧客向け自社運用基盤のセキュリティリスク低減
- SOCサービス運用と併せ，計画的なセキュリティ知識習得に向けた教育計画に基づいた各種教育受講，資格取得を奨励したことによるセキュリティ人財の育成
- 顧客向け自社運用基盤のサイバーセキュリティ対策強化による当社のブランド価値の維持に貢献

**◆SOCサービス改善による成果**

- インシデント対応管理基盤導入により，品質保証部門，セキュリティ統括部門含めたインシデント情報を可視化し，タイムリーな情報共有を実現
- プロセスマイニング適用により，業務プロセスベースでの分析・可視化と，継続的業務プロセス改善のサイクルを確立し，ログ監視サービス品質維持向上の基盤を整備
- SOC部門が実施，推進してきた，ログ監視サービスのプロセスやドキュメント類の整備やServiceNow導入事例，プロセスマイニング適用事について，事業部へ随時取り組み内容をフィードバックしたことで，事業部との連携を強化

## 5. 今後の取り組み

当社でのSOCサービスに関する今後の取り組みとして，以下4点を推進予定である．

### （1）SOCサービス適用拡大

本稿執筆時点（2022年11月）現在，SOCサービスを当社顧客向け自社運用基盤30サービスへ適用済みであるが，さらなるセキュリティ強化に向け，当社内の他の顧客向け自社運用基盤への適用を継続して拡大していく．また，当社グループ全体としてのセキュリティ強化，ブランド価値の維持を目的に，2023年度以降，国内グループ会社，海外グループ会社への適用拡大を検討している．

### （2）事業貢献

顧客向け自社運用基盤に対する社内向けSOCサービスとしてのサービス評価・検証，ブラッシュアップ，標準プロセス化，業務効率化事例等ノウハウを当社内で横展開することにより，事業部との連携を引き続き強化していく．

### （3）SOCサービス業務自動化・効率化

「2.5　SOCサービス運用における課題」に記載している未対策の課題を継続して対策予定である．セキュリティ運用チェックサービスの課題については，ServiceNowへの一部業務取り込みや，その他の自動化ツールを利用することで，2022年度4Q以降対策を実施する．ログ監視サービスにおけるアラート分析やインシデント対応手順のノウハウ蓄積に関しては，2023年度以降対応実施予定である．

### （4）継続的プロセス改善

ログ監視サービスの業務プロセス改善サイクル（分析・課題抽出，改善策検討，改善適用，評価）を継続的に実施し，ログ監視サービスの品質維持向上を図っていく．

サイバーセキュリティ攻撃が日常となっている中で，当社自身も相当厳しい経験を積んできた．これまでの経験を教訓として，お客さまにサービスを提供する顧客向け自社運用基盤のセキュリティを堅固に保ち，お客さまへの影響を最小限に抑えることは，当社の非常に重要な責務である．本稿で紹介したサイバーセキュリティ対策強化は当社のブランド価値維持のために必須の取り組みであり，顧客向け自社運用基盤での監視・チェックを通じてのサービス検証，ブラッシュアップ，標準化，効率化などにも事業部との連携で事業貢献していくとともに，セキュリティ人財育成の実践の場としても効果的に活用していきたい．

### 参考文献

1）日立：Lumada（ルマーダ），https://www.hitachi.co.jp/products/it/lumada/index.html（2023年7月18日）
2）ServiceNow：ServiceNow ― ServiceNow と連携する世界，https://www.servicenow.com/jp/（2023年6月15日）
3) Celonis Japan（セロニス）：プロセスマイニング，https://www.celonis.com/jp/（2023年6月1日）
4）ServiceNow：Security Operations (SecOps) ―エンタープライズセキュリティ―，https://www.servicenow.com/jp/products/security-operations.html（2022年11月11日）
5）Microsoft 365：Microsoft Excel スプレッドシート ソフトウェア，https://www.microsoft.com/ja-jp/microsoft-365/excel（2023年7月18日）

**土井聡弘**（非会員）
（株）日立システムズ セキュリティリスクマネジメント本部 セキュリティ監視運用センタ主任技師．2009年（株）日立情報システムズに入社（現（株）日立システムズ），社内ITインフラや社内システムの設計，構築，運用として経験を積み，2022年より現職．自社サービスのセキュリティを監視するSOCの運用，プロセス改善，定着化の推進に従事．

**船井裕亮**（非会員）
（株）日立システムズ セキュリティリスクマネジメント本部 セキュリティ監視運用センタ担当．2012年（株）日立システムズに入社，フィールド・サポートサービスとして現地での拡販作業に従事，また，品質保証としてさまざまな業種のプロジェクト対応などに従事し，2022年より現職．

**市川絵里奈**（非会員）
（株）日立システムズ セキュリティリスクマネジメント本部 セキュリティ監視運用センタ担当．2016年（株）日立システムズに入社，社内システムの開発・運用を担当し，2022年より現職．自社サービスのセキュリティを監視するSOCのアナリストとして，セキュリティ分析・評価業務に従事．

**緒方啓大**（非会員）
（株）日立システムズ セキュリティリスクマネジメント本部 セキュリティ監視運用センタ担当．2018年（株）日立システムズに入社，品質保証本部で業務経験を積み，2022年より現職．自社サービスのセキュリティを監視するSOCのアナリストとして，セキュリティ分析・評価業務に従事．

採録決定：2023年7月25日
編集担当：長坂健治（キンドリルジャパン）