2024

セキュリティ業務の自動化推進レポート

独立行政法人情報処理推進機構　産業サイバーセキュリティセンター
中核人材育成プログラム 7 期生　セキュリティ業務自動化推進プロジェクト

概要

近年、企業のセキュリティ部署では、サイバー攻撃の頻発に伴いセキュリティインシデント対応の回数が増加しており、侵入後の展開速度も上がっている。また、デジタルトランスフォーメーション（DX）の推進による IT 資産の拡大により、脆弱性対応件数も増えている。これら 2 つの要因が相まって、セキュリティ部門の業務負荷は重くなる一方である。業務負荷が増加することにより、重大アラートの見落としや人材の離職が予想される。

セキュリティ部署における担当者の業務負荷を軽減するため、本プロジェクトでは自動化ツールによるセキュリティ業務の自動化に着目し、その活用を検討した。また、ツールの活用検討や文献調査、有識者へのヒアリングを踏まえて、自動化を進める上で必要になる戦略面での考慮事項などについてもまとめた。セキュリティ業務を自動化することは、工数を削減できるだけでなく、対応速度の向上や人的ミスの削減などのメリットがある。

本書の前半（第 2 章）では、セキュリティ業務の自動化を検討するにあたり、自動化のメリットを改めて考察し、自動化推進のプロセス全体を中長期的な視点および短期的な視点のもとに整理した。また、自動化推進プロセスの各フェーズにおいて注意すべき考慮事項について考察した。

本書の後半（第 3 章）では、企業におけるセキュリティインシデント対応業務を例に自動化を実践し検証した。効果の検証に当たっては、工数削減といった定量的効果や、副次的な定性的効果を検証した。1 か月あたり 50 件のアラートが発生する前提条件では、アラート 1 件あたり約 7.7 分、年間で約 100 時間の工数削減ができるとわかった。

著者らは実際にセキュリティ部署で働く運用担当者であり、現場担当者として業務負荷増によるリソース不足や定型業務の退屈さを日々痛感している。本プロジェクトはそのような問題を自動化によって解決したいと考え発足した。本書にまとめた戦略的知見や実践例を、自部署のセキュリティ業務の自動化推進における具体的な指針としてぜひ活用されたい。

目次

概要 1
目次 2
第 1 章　序言 4
1.1　背景 4
1.2　目的 4
1.3　スコープ 5
1.3.1　想定する企業 5
1.3.2　効果検証の対象セキュリティ業務 5
1.4　本書の活用方法（誰が、いつ、どう読むべきか） 6
1.5　免責事項 6
第 2 章　業務自動化推進における戦略 8
2.1　なぜ自動化するのか 8
2.1.1　業務負荷軽減のメリット 9
2.1.2　業務負荷軽減以外のメリット 9
2.1.3　業務量とコストの比較（費用対効果） 10
2.2　原則 11
2.3　標準的な流れ（プロセス） 12
2.3.1　考え方 12
2.3.2　具体的なプロセス 13
2.4　考慮事項 15
2.4.1　計画における考慮事項 15
2.4.2　業務調査／整理における考慮事項 15
2.4.3　自動化導入検討における考慮事項 16
2.4.4　自動化すべき業務の判断 16
2.4.5　自動化の方向性定義における考慮事項 19

2.4.6　自動化の設計／実装における考慮事項 21
2.4.7　自動化の運用における考慮事項 21
2.4.8　自動化の評価における考慮事項 21
第 3 章　業務自動化の実践例 23
3.1　検証の前提条件 23
3.2　検証環境の構成 23
3.3　自動化するセキュリティ業務の選出 25
3.3.1　全体業務の調査と自動化対象業務の選出 25
3.3.2　今回想定する初動調査について 25
3.4　ツールを使った自動化の実装 26
3.5　効果測定の方法と結果 28
3.5.1　測定方法 28
3.5.2　算出方法 29
3.5.3　測定結果 29
3.5.4　定性効果 30
3.5.5　削減した工数の活用 31
第 4 章　まとめ 32
付録 A　専門用語集 33
付録 B　参考文献 36
謝辞 37

第1章　序言

1.1　背景

近年、企業のサイバーセキュリティ部署は業務負荷が増加傾向にある。大きな原因は 2 つあると考えられる。ひとつはサイバー攻撃の増加である。総務省のホームページではサイバー攻撃関連の通信が 2015 年から 2022 年の 7 年で 8.3 倍に増加したという調査結果が示されている（図 1-1）。もうひとつは脆弱性件数の増加である。図 1-2 にある通り、年々報告される脆弱性の数は増えており、企業内の DX 推進等で IT 資産も増加しているため、企業が対応すべき脆弱性も増加している。新しいシステムの導入や通信の増加により、サイバーセキュリティの守備範囲は広がっている。膨大な脆弱性対応・アラート処理にリソースの大半を消費し、さらにそれを改善する時間も割けずに、サイバーセキュリティの現場は疲弊していくことが想像される。

セキュリティ担当者の業務負荷増と、それに起因するアラートの見落としや人材離職を防ぐには、彼らの業務負荷の軽減が重要な課題である。そこで我々は自動化ツールを活用した業務の自動化を推進することで業務負荷軽減に繋がると考えた。

しかし市場には様々な自動化ツール・業務改善ツールがあるにも関わらず、セキュリティ業務の現場の自動化は未だ進んでいるとは言えない。文献調査を行った結果によると、セキュリティ業務自動化には「どこから手を付ければよいか分からない」「必要な DevOps スキルがチームにない」「自動化の予算がない」などといった課題があることが分かった。

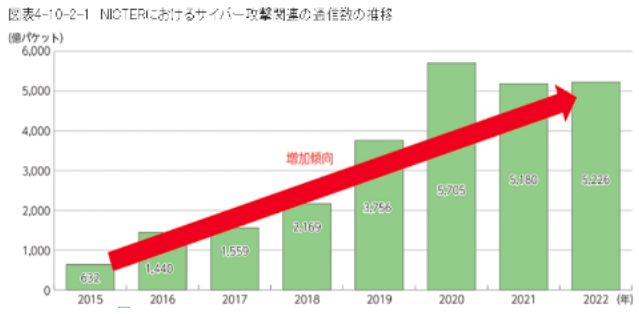
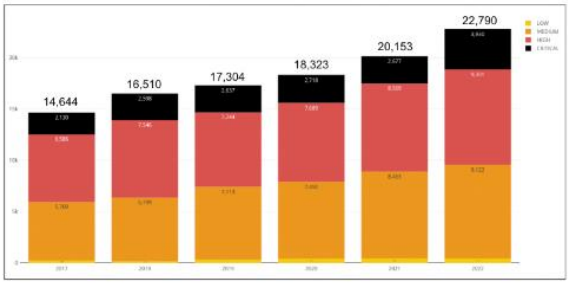


図 1-1　サイバー攻撃の増加

（情報通信白書 令和 5 年版「第 2 部　情報通信分野の現状と課題」，https://www.soumu.go.jp/johotsusintokei/whitepaper/r05.html ）



2017 年から今年までの脆弱性数の推移（CVSS v3）

図 1-2　脆弱性数の推移

(yamoryBlog. 2022 年脆弱性セキュリティレポート https://yamory.io/blog/2022-security-report/)

1.2　目的

本プロジェクトはセキュリティ担当者の負荷軽減を目的として、セキュリティ業務の自動化における主要な課題に対する解決アプローチを提案する。

企業のセキュリティ業務自動化には前節で挙げた 3 つの課題があり、本書では、その解決アプローチとして、「どこから手を付ければよいか分からない」に対しては 1. 自動化推進における実施順序と考慮事項の提供、「必要な DevOps スキルがチームにない」に対しては 2. 自動化に活用できる

ツールを調査・整理、「自動化の予算がない」に対しては 3. 低コストで活用できるツールの検証結果の提供 という 3 つをまとめた。

また、実際に検証環境を用意し、課題解決に適したツールの検証を行い、導入時の注意点や有用性などの所感についても記載した。本書が、セキュリティ業務の自動化を推進したいが課題を感じて足踏みしている読者の、自動化を推進するための参考になれば幸いである。

1.3 スコープ

1.3.1 想定する企業

セキュリティ業務自動化において、企業ごとの規模感や体制によってどういったアプローチが有効かは大きく変わってくる。そこで表 1-1 のように我々の派遣元企業をベースに想定した企業ペルソナを設定し、自動化推進の議論を展開する。

表 1-1 本書で対象とする企業ペルソナ

企業概要	製造系の IT 子会社
事業内容	親会社の IT 管理および外販
従業員数	1000 人規模
資本金	100 億円規模
生産拠点	東京、神奈川、兵庫、他グループ会社（国内）
情報システム要員	50 人規模
セキュリティ方針	クラウド活用、自動化推進
セキュリティ成熟度（AsIs）	防御、検知のためのツールは存在
	RSS や Python を使って個人が自動化している業務は一部存在
	クラウド等による組織レベルの自動化はない
セキュリティ組織体制	SOC、CSIRT、リスク統括管理部門（情シスは別に存在）
セキュリティ要員	6～10 人規模
セキュリティ自動化予算	100～300 万（初期コスト含む）

1.3.2 効果検証の対象セキュリティ業務

一言で「セキュリティ業務」と言っても、インシデント対応、セキュリティ製品の導入、社員のセキュリティ教育など、多岐にわたる作業がある。一般的なセキュリティ業務は、日本セキュリティオペレーション事業者協議会（ISOG-J）によると、大きく 9 つのカテゴリに分類され、全 64 種類の業務がある（図 1-3）。

本プロジェクトの実証は、この内の「D. インシデント対応」(=IR) に焦点を当てて行ったので、注意されたい。自動化の効果が高い業務としてインシデント対応業務を選択したが、選択までの過程は後述する。

カテゴリー	関連作業
A. CDCの戦略マネジメント	13 種類
B. 即時分析	4 種類
C. 深掘分析	4 種類
D. インシデント対応	7 種類
E. 診断と評価	9 種類
F. 脅威情報の収集および分析と評価	5 種類
G. CDCプラットフォームの開発/保守	13 種類
H. 内部不正対応支援	2 種類
I. 外部組織との積極的連携	7 種類
9 カテゴリー	**64 種類**

図 1-3 セキュリティ業務の種類とカテゴリ

ISOG-J.セキュリティ対応組織の教科書　第 3 版, 2023 年.

https://isog-j.org/output/2023/Textbook_soc-csirt_v3.1.pdf

1.4　本書の活用方法（誰が、いつ、どう読むべきか）

本書は、インシデント対応に従事するサイバーセキュリティ担当者を対象とし、日々のセキュリティ業務を自動化ツールへ置き換える際の参考資料とすることを想定している。

技術的提案については、第 2 章でセキュリティ業務の自動化を組織で行う上での基本戦略や実施順序をまとめ、第 3 章で自動化に活用できるツールの実装と、効果検証を行った。必要に応じて下記のユースケースも参考にしながら、本書を読み進めることを推奨する。

表 1-2　ユースケースと該当する見出しの一覧

ユースケース	該当する見出し
業務が本書の対象か知りたい	1.3 スコープ
業務自動化のメリットを確認したい	2.1 なぜ自動化するのか
自動化の具体的な推進手順を知りたい	2.3 標準的な流れ（プロセス）
自動化する作業の判断基準を知りたい	2.4.4 自動化すべき業務の判断
実装する際の注意点や所感が知りたい	第 4 章まとめ

1.5　免責事項

- 本書は単に情報として提供され、内容は予告なしに変更される場合がある。
- 本書に誤りがないことの保証や、商品性または特定目的への適合性の黙示的な保証や条件を含め明示的または黙示的な保証や条件は一切ないものとする。
- 本書に記載の内容は、独立行政法人 情報処理推進機構および産業サイバーセキュリティセンターの意見を代表するものではなく、著者の見解に基づいている。
- 本書の利用によるトラブルに対し、本書著者ならびに監修者は一切の責任を負わないものとする。

- 本書の有効期限は、発行日から 2 年間とする。

第2章　業務自動化推進における戦略

1.1 の自動化推進の課題には、「どこから手を付けていいかわからない」というものがあった。これを解消するために、我々は自動化推進の基本的な戦略（自動化をどのように推進すべきか）をまとめることにした。

本章では、はじめにセキュリティ業務をなぜ自動化するのか（自動化のメリット）を考える。メリットを理解して自動化を推進することに納得した上で、基本戦略（自動化をどのように推進すべきか）の言及に移る。本章のメインとなる基本戦略だが、今回は下記のように整理した。

- ✓ 原則
- ✓ 標準的な流れ（プロセス）
- ✓ 考慮すべき考慮事項

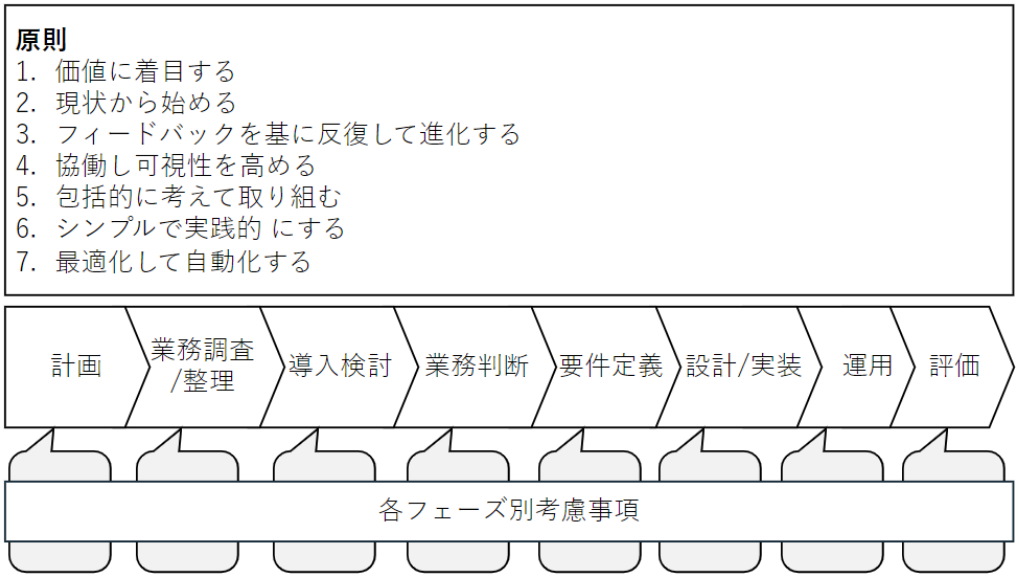


図 2-1　本章の基本戦略についての構成イメージ

本章を書くにあたっては、「外部組織へのヒアリング」や第 3 章で後述する「ツール検証のフィードバック」から得た知見を、書籍やウェブ情報から得たフレームワークを使って整理した。業務自動化は目的ベースで進めることが重要だが、セキュリティ要員は自動化スキルが少なく目的がブレやすい。そのため、業務自動化を目的ベースで進めるにあたって拠り所になる考え方をまとめたいと思い本章を作成した。

2.1　なぜ自動化するのか

1.2 節でも述べたように、本書のテーマは業務上の手作業を減らし、年々増加するセキュリティ担当者の業務負荷を軽減することである。よって、本書が自動化を目指す理由は「担当者の業務負荷軽減」である。ここでは、業務負荷軽減を軸にしつつ、より幅広い視点で業務自動化の重要性を理解してほしい。

2.1.1　業務負荷軽減のメリット

自動化における業務負荷軽減は、業務量（業務時間）の軽減と言ってもよい。自動処理が、業務担当者の手作業の業務を肩代わりすることで、担当者の業務量は減り、下記のような効果が得られる。

1. **リソースの再割り当て：**
   自動化で空いたセキュリティ担当者の人的・時間的リソースを、セキュリティ業務の更なる効率化や高度化、もしくは教育等に割り振れる。
   これにより、組織全体のセキュリティレベル向上にもつながる。
2. **人材の満足度向上：**
   単調で退屈な作業の削減は、セキュリティ人材のモチベーション低下や離職の抑止に繋がる。
   また、1. リソースの再割り当てで述べたリソースを高度な業務や教育に充てることは、担当者のスキルアップとキャリア成長にも寄与し、長期的な満足度向上を実現する。

その一方で、手動業務を自動化しても、状況次第で業務量は軽減されず、増加するかもしれないということに思い当たる読者もいると思う。例えば、下記のようなことが起こり得る。

- ✓ 自動化の導入時に、セキュリティ担当者のリソースが少なからず奪われる
- ✓ 自動化の運用初期に、意図しないエラーや慣れないツール保守に悩まされる

しかし、この見方は短期的な視点であるということを強調したい。つまり、長期的な視点で見ると、

- ✓ 対応件数が多い作業であれば、件数が積もった結果として、業務負荷軽減となる
- ✓ 業務負荷軽減以外のメリットが付加価値となり、セキュリティ業務がより高度化される。

ここで「業務負荷軽減以外のメリット」が登場したので、次項でそれらのメリットについて述べる。

2.1.2　業務負荷軽減以外のメリット

業務自動化では、業務負荷軽減以外にも、様々なメリットが得られる。

3. **業務プロセスを改善する機会の創出：**
   業務自動化を行う前には、業務プロセスの可視化や、場合によっては見直しが必要なため、業務プロセス改善のよい機会が生まれる。
4. **操作・確認ミスの削減：**
   手作業では操作・確認ミスが発生しやすいので、業務を自動化するとそれらミスの削減となる。業務負荷が高い場合には、特にそれが顕著だと予想される。また、単調かつ頻度の多い作業ほどミスが発生しやすいが、単調かつ頻度の多い作業は自動化に向いている点も強調したい。
5. **対応速度の向上**：
   業務量軽減に似ているが、こちらは対応時間の短縮に注目した利点である。迅速さが重

要な業務において、自動化による対応時間の短縮は重要さを増す。例えば、インシデント対応業務の自動化では、インシデント発生時の対応時間の短縮により、事態の深刻化を早い段階で食い止めることができ、セキュリティ侵害が重大化するリスクを低減できる。

これらのメリットは、大まかに言うと「組織のセキュリティ体制強化」に繋がっていく。

業務負荷軽減を中心に考える場合でも、それ以外のメリットにも着目し、総合的に自動化推進の理由を考えるべきである。セキュリティ業務自動化にメリットがあることは、ほとんどの組織が理解していると思うが、総合的な観点を忘れないようにしたい。

2.1.3　業務量とコストの比較（費用対効果）

業務量軽減の効果を考える場合には、基本的にコストとの比較で行う。つまり、費用対効果を考え、コストの見合わない自動化は避けるべきである。但し、上述したように、それがすべてではないので注意されたい。

損益分岐点を考える

業務を自動化すると、それ以前の手作業と比べ、運用費用の削減となる。しかし、初期費用（例：自動化ツールのライセンス費用[i]、導入の人件費）がかかる。そのトレードオフを考えるために、損益分岐点を考えるグラフを描く。すると、一般に図 2-2 のようなグラフとなると思われる。

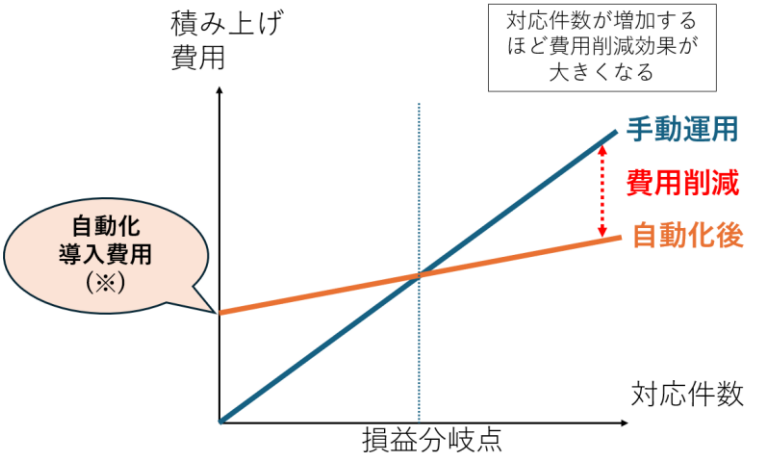


図 2-2　自動化の損益分岐点

この図が示す要点は２つある。

① 元の手動運用費用に対して自動化導入費用が相対的に高価だと、対応件数が非常に多くなければ投資回収できない。

② 業務における対応件数（対応頻度）が非常に少ないと、自動化導入費用が安くても、現実的な期間で投資回収できない。

但し、実用上は、対応件数や運用費に変動があることにも注意したい（下記参照）。

---

[i] サブスクリプションライセンスのような場合には本来運用費扱いとなるが、簡単化のため初期費用扱いとした。

- ✓ 対応件数：一定ではないため、自動化を数年運用する場合、対応件数増減の見込みをある程度考慮すべき。
- ✓ ライセンス費用：特に海外製品のライセンス費用は増減が激しいので、為替変動・直近の値上げ等を加味して考える。また、適宜契約先に確認する等も行う。

費用対効果が十分でない場合

費用対効果が十分でない場合でも、操作・確認ミス防止など、その他のメリットが十分に見込めるなら、自動化を推進すべきかもしれない。ただ、費用対効果が悪いと、その分高度化や教育に使えるコストを不要に圧迫するため注意が必要である。

2.2 原則

セキュリティ業務自動化の原則について述べる。本書では「セキュリティ業務自動化の 7 つの原則」を提示することにした。これは、ITIL[ii]の「7 つの原則」を参考に作成している。「7 つの原則」は、組織の指針として環境や戦略が変わっても活用できる原則を表し、業務自動化のような不安定な環境においても不変の指針となる。

1. **価値に着目する：**
   - 目的ベースで自動化を行う
   - 組織の方針を確認する
2. **現状から始める：**
   - 現状分析を行う（OODA ループの活用 ※後述）
   - 既存ツールの活用を検討する
3. **フィードバックを基に反復して進化する：**
   - スモールスタートで始め、調整・改善を柔軟に行う
4. **協働し可視性を高める：**
   - 自動化の取り組み内容を適切に報告する
   - 部・チーム間で取り組み内容を共有し知見を交換する
5. **包括的に考えて取り組む：**
   - 推進体制（ワーキンググループ）を構築し、全体最適で自動化を検討する
6. **シンプルかつ実践的にする：**
   - 目標を細かく分解し、必要最低限のタスクで実施する
7. **最適化して自動化する：**
   - 業務プロセスの見直しを行う
   - プロセス上の判断基準を明確化する

[ii] Information Technology Infrastructure Library。IT 活用のナレッジをフレームワーク化したもの。業務自動化に関する考え方も記載されている。

2.3　標準的な流れ（プロセス）

本項では、セキュリティ業務の自動化推進プロセス（どのような順序で行うか）を記載する。いきなり具体的な自動化推進方法を述べるのではなく、どのような考え方（フレームワーク）に基づいて自動化推進を考えるべきかを述べることにする。

2.3.1　考え方

まず基本となる考え方を述べる。セキュリティ業務の自動化を進めていく上では、下記の２つの考え方が重要となる。

スモールスタート

業務自動化を進める上ではスモールスタートで考えることが望ましい。スモールスタートとは、案件を小規模化して、小さいスコープ・コストで素早くスタートすることを指す。

スモールスタートを推奨する理由は下記の通りである。

- ✓ セキュリティ専門性と高い業務自動化スキルを両立する人材は比較的希少であるため、組織・チームとして知見やスキルが少ない状態から業務自動化を始める場合が多い。
- ✓ 業務自動化は、想定外の事象が発生するなどして思惑通りに進むことは少ない。

スモールスタートにより、シンプルさと柔軟性を確保し、断念する場合も影響の少ない規模感で進めることが重要である。

2 つの周期

説明すべきは「業務自動化の推進」の方法だが、自動化が軌道に載った後まで考慮すると「業務自動化の段階向上」の方法も重要となる。両者を下記にて説明する。

- ✓ **業務自動化の推進**
  - ➢ 実施内容：業務自動化を導入し、導入した自動処理を徐々に改善。
  - ➢ ポイント：いきなりの明確なゴール設定は困難。
  - ➢ 実施周期：少しずつ実施（数週間～数か月。短期的)。
- ✓ **業務自動化の段階向上**
  - ➢ 実施内容：現在の自動化の成熟度評価を行い、次の成熟度の段階へ進む計画を立案。
  - ➢ ポイント：一般的な自動化成熟度に照らし合わせて、目標達成を評価。
  - ➢ 実施周期：まとめて、定期的に実施（半年や１年程度。中長期的)。

両者の共通点は、改善を繰り返す点であるが、期待される実施周期が異なる。

さて、改善のフレームワークとなると、おそらく最も有名なのは PDCA サイクルだが、ここでは同系統として OODA ループ[iii]を紹介する。OODA ループは、下記ステップを周期的に実施するフレームワークである。

1. 【Observe：観察】現状を観察して必要なデータを収集
2. 【Orient：方向づけ】収集したデータから取るべき行動を検討

[iii] アメリカ空軍のジョン・ボイド氏が提唱した意思決定手法。

3. 【Decide：意思決定】検討結果に基づき、具体的な実施事項や優先度を決定
4. 【Act：行動】優先度に沿って実施事項を実行

今回は、PDCA サイクルと OODA ループの両方を使用する。両者の比較を、以下の図 2-3 に示す。

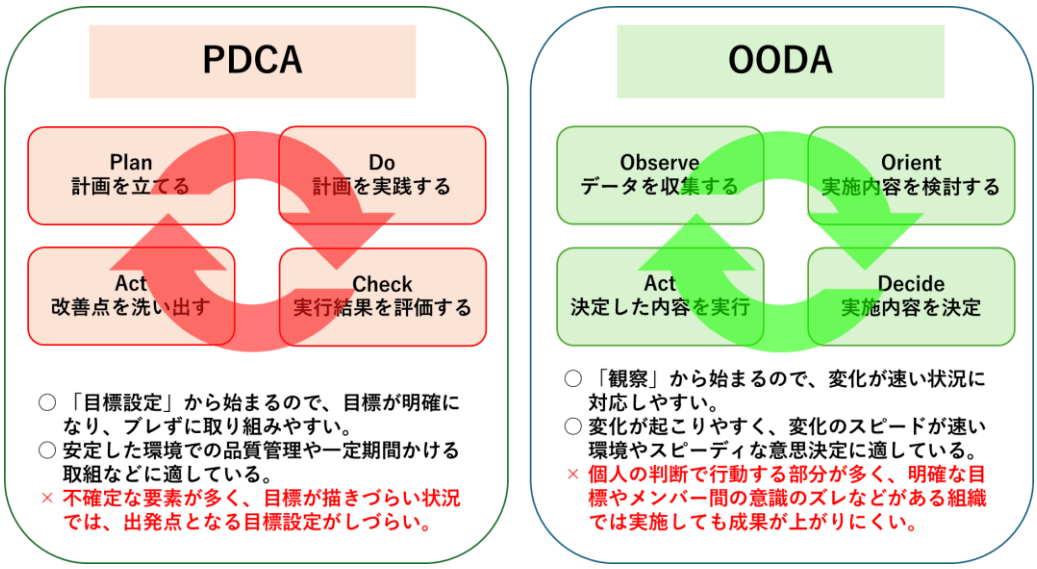


図 2-3 PDCA サイクルと OODA ループの比較

PDCA サイクルと OODA ループに関して、大雑把に言えば次のことが言える。

- PDCA サイクル：明確なゴールに向かう場合に適し、ゴールに対する評価と改善を提示してくれる。一方、明確なゴール設定が難しい案件に適さない。
- OODA ループ：現状分析から開始できてスピード感が速い。一方で、ゴールに対する評価が組み込まれていない。

上記のような特徴から、利用するフレームワークを下記のように規定すると、自動化業務を効率よく推進できると考えるに至った。

- **業務自動化の推進（短期）**
  - ➢ 利用フレームワーク：OODA ループ
- **業務自動化の段階向上（中長期）**
  - ➢ 利用フレームワーク：PDCA サイクル

2.3.2 具体的なプロセス

業務自動化推進の開始点をスモールスタートとしたが、今度は、その改善をどう繰り返していくべきかについて説明する。

以下に推奨する改善ループを提示する。まず中長期的には PDCA サイクルを回す。

1. 【Plan】中長期サイクルの初めに、自動化の戦略目標・計画を立てる
2. 【Do】短期の自動化推進ループ（OODA ループ）を繰り返す
3. 【Check】現在の自動化の成熟度評価を、年単位等でまとめて実施
4. 【Act】必要に応じて戦略目標・計画を修正し、より高度な自動化に取り組む

PDCA サイクルの Do の中で、短期的に下記の OODA ループを実施する。

1. 【Observe：観察】
   - 自動化担当者の決定
   - 部・チーム全体の業務把握と業務整理
   - 各業務の負荷の割出し（記録データやヒアリングから）
     ※可能ならば原因も考察。
   - 自動化に活用できそうなツールの調査（現在所有中のもの、市場のもの）
2. 【Orient：方向づけ】
   - 「1.の業務負荷」から自動化を行うべき業務を選出する。
   - 自動化できそうな業務を見込みで選択し、利用するツールを「1.のツール調査」から選択し、（トライアル期間利用などで）検証。
     （判断後はすみやかに「意思決定」へ）
3. 【Decide：意思決定】
   - 2.の 2 点から、自動化可否を判断する。
   - 自動化可能な業務の中で優先度を決める。
     （決定後はすみやかに「行動」へ）
4. 【Act：行動】
   - 3.で決定した優先度に従い、業務自動化実装を行う。

業務自動化の計画を立てる上では、現在の自動化がどの段階にあるのかの評価（成熟度評価）に応じて、段階的に高度な自動化に取り組む必要がある。しかし、この評価に難しさがある。ここでは「業務自動化における段階的な成熟度モデル」を利用することを提案する。これは、ITIL の「インシデント管理の段階的な高度化」を参考に作成したものである。以下に高度化モデルとその例を示す。

<u>業務自動化における段階的な成熟度モデル</u> ※数値が大きいほど成熟

Lv.1【情報の一元化】: 情報の一元的な集約、共通プラットフォームができている
Lv.2【ツール間連携】: ツール間の情報のやり取りが自動で処理できている
Lv.3【スクリプト実行】: 自動化に適した業務がツールで自動処理できている
Lv.4【高度な自動化】: AIOps による分析、要約などの自動処理ができている

<u>インシデント対応の自動処理におけるモデル例</u> ※数値が大きいほど成熟

Lv.1【情報の一元化】: インシデント情報等の重複記録の廃止、手順やルールの標準化
Lv.2【ツール間連携】: チケット自動起票・更新・クローズ、インシデント通知・連携
Lv.3【スクリプト実行】: インシデント対応のプロセスの自動化
Lv.4【高度な自動化】: AIOps を活用したインシデント解析、推奨対応の提案

2.4　考慮事項

セキュリティ業務自動化は、セキュリティ担当部署の通常業務とは勝手が異なる。通常業務は、予め作られた年間計画やルール・手順に従えばよいので進めやすい。その一方で、セキュリティ業務自動化はこれまでの運用を改善する取り組みであり、セキュリティ業務自動化では通常業務の計画・ルール・手順に頼ることができない。また、業務に必要となるメンバーの専門知識も、既存業務と比較すると十分には醸成されていない可能性が高い。

これらを踏まえると、業務自動化は通常業務に加えて考慮すべき事項があると著者らは考える。本節では業務自動化を進める上で活用できる考慮事項について述べる。

2.4.1　計画における考慮事項

目的の設定

目的の設定では、様々なメリット（2.1 参照）の内、何を目指して自動化を実施するのかを決定する。

2.4.2　業務調査／整理における考慮事項

業務調査

予め、部・チームにどのような業務が存在するのかを自動化担当者が把握しておく必要がある。通常自動化担当者は全体の業務を把握していないため、管理職から自動化担当者に対してどのような業務が存在しているのかを連携し、業務調査における考慮漏れがないようにしておくことが重要となる。

業務プロセスの標準化／整理

予め、自動化を行う業務プロセスを標準化しておく必要がある。この標準化は、個人で業務プロセスの手順を作成することではなく、関係者にプロセスの意図までを含めた手順を展開し、関係者全員が同プロセスを理解することを指す。

また、整理する上では「モデル化」「不要業務の排除」を意識するとよい。ここでのモデル化とは、業務を一般化し無駄を排除したモデルを用意し、類似の業務をそのモデルと一致するように整理するアプローチを表す。

業務量の可視化／定量化

自動化を行う前に、部・チーム内に存在する業務を把握し、各業務の業務量を把握する必要がある。業務量は、[作業時間(人時/件)]×[作業頻度]で算出する。

作業実績（これから作業頻度を割り出す）や作業時間を記録する際には、可能なら、チケット管理ツール等を使用するのが望ましい。ただし、作業時間記録の方は、不正確な場合もある。なぜなら、手動記録の場合には、記録の手間が無視できないし、自動記録でも、他作業との並行作業の場合などは正確な作業単位での記録が得られないからである。そのため作業時間の検討については担

当者数人で集まり、記録データを見ながら各作業目安時間を割り出すとよい。

情報の一元化

情報は、重複保存を避けて 1 箇所に集約する。そうすることで、自動化時の不要な連携やプロセスの複雑化を回避できる。例えばインシデント対応業務の場合、インシデント情報を登録・管理するチケット管理システム上に手順書も保管したり、同システム上の Wiki を利用したりすることで、プロセスを単純化できる。

条件分岐の判断基準の決定

業務プロセス上に条件分岐がある場合には、どのような閾値/選択肢で分岐するのかの判断基準の決定が重要となる。閾値/選択肢設定のないプロセスは、個人が都度判断していることになるため自動処理が困難となる。閾値/選択肢は複数の観点が含まれていることも多いため、都度人間で考慮する必要のある観点がないかについても検討が必要である。

2.4.3 自動化導入検討における考慮事項

推進体制（ワーキンググループ）の構築

部・チームとして自動化ワーキンググループを構築する。

ほとんどの組織・担当者は、業務自動化の意欲を持っているものの、リソース的には既存業務で余裕がなく、業務自動化に手を付けられない状態に陥っているものと思われる。しかしこのような状況では、定型作業に疲弊した個人が、個人の業務範囲で自動化を行うのみとなり、全体最適な自動化につながりにくい。また、個人による実装であるため属人化のリスクも高い。そこで、部・チームとして自動化ワーキンググループを構築することで、業務自動化自体を組織のタスクリストに追加して時間を確保することが重要となる。組織で検討・実装することで属人化リスクも低減できる。

また、ワーキンググループは異なる業務担当者で構成することが望ましい。これは特定の業務担当者を集めた場合、思考にバイアスがかかり、自身の担当業務の負荷を多く見積もったり、優先順位を自分優位にしたりする可能性があるためである。異なる業務担当者同士で検討することで多角的な視点から自動化後のリスク分析ができる。

ツール検証の実施

自動化に使用するツール調査では、ネット調査、製品比較、ベンダーからの情報入手だけでなく、実際にツール検証を行うことが望ましい。実際の使用でしか分からないことが多く存在する。

使用しにくいツールは運用担当者に受け入れられず使われない可能性がある。使用者の UX（User Experience）を十分踏まえた検討をすべきである。

2.4.4 自動化すべき業務の判断

ここでは、自動化すべき業務を選定する際の判断基準をまとめる。後述する複数の判断基準を全

体的に考慮し、全体最適を意識した検討が望ましい。但し、やむを得ない都合で考慮できない判断基準も出てくると思われるため、必要に応じて例外を許容することが重要になる。

業務ごとの自動化判断基準の概要

ある業務を自動化すべきか否か判断する基準は、大きく 3 つあると考えられる。

① **現場における自動化需要：**業務が高負荷か
② **業務種類：**業務が定型的か、低リスクか
③ **自動化の実用性：**その業務が自動化された際に、工数削減効果は十分か、属人性を十分に低減できるか

以下に更に判断基準を詳細化する。

基準 A：業務が高負荷か

高負荷の業務ほど、自動化効果を期待できる。負荷を定量化するためには、各業務の作業量を算出する（3.2.2 の「業務量の定量化/可視化」項目参照)。また、作業量算出は、担当業務の被らない複数人の担当者で実施することが望ましいため、3.2.2 の「自動化ワーキンググループの構築」項目を参照し、体制検討を進めることが推奨される。

基準 B：業務が定型的か

以下のような条件に当てはまる業務は定型的である。

① マニュアル化されていること
② フローが条件分岐しない又は分岐条件の基準に明確な閾値があること

反対に、都度判断をしながら思考力を駆使して対処するような業務は非定型的であるといえる。非定型的な業務の例を以下に示す。

1. 承認プロセス（遮断作業の承認、クローズの判断など）
2. インシデント対応者の厳密な判断を要するもの（過検知の判断など）
3. 関連部門との連携、相談（都度やり取りの内容が変わるものなど）
4. 高度な知識を要するもの（フォレンジックでの詳細調査など）

承認プロセスについては、チェックリスト化できるような確認作業であれば定型的な業務にできる。また、厳密な判断を要するものであっても、一部が閾値などで判定しているものであれば部分的に自動化することができる。

基準 C：業務が低リスクか

ここでいうリスクとは、自動処理が意図しない動作をした時に生じる業務への影響度を指す。リスクの例は以下の通りである。

1. 自動処理が意図しない結果（例えば API のエラーレスポンス）を返す
2. 自動処理が停止する
3. 自動処理に使っていたサービスが終了する

自動処理の実行で意図しない動作が発生した際、なるべく影響を受けない業務のほうが、自動化に適している。例えばチケットクローズのチーム内連携の自動処理が停止してもインシデントが無害化されたことの気づきが遅れる程度だが、端末隔離の自動処理が誤動作して正常な端末をネット

ワークから切り離してしまった場合は組織において重要な事業活動や取引に影響が生じる可能性がある。自動化検証段階でエラーを 100%対策できることは基本的にないと考えるべきである。自動化のメリットの 1 つに操作ミス防止があるが、その一方で、自動処理の意図しない動作は、手動処理における操作ミスよりも、異常に気づきにくく、原因が分かりにくいことが多い。

リスクに関しては、低リスクの業務についてもリスク低減策を取ることが望ましい。

1. 自動化実装でエラーが出た時に記録・通知する設定をしておく。また、利用ツール上で想定しない異常動作が生じた場合、エラーは出ていないが意図しない出力が生じる場合もある。そのため、出力がパターン化されるような処理はパターン外の出力がないか確認する等、意図しない動作を検知できるような仕組みが必要となる。
2. 自動化対象業務の作業を細かく分解し、分解した単位ごとに自動化を行う。自動化実装を細かく分けることで特定の実装箇所が停止した場合の影響を最小化し、かつ原因の特定をしやすくすることができる。
3. 自動化実装が停止した時のための復旧マニュアルを作成しておく。また、自動化実装が長期間停止した場合、手動で同じ処理を実施できるようマニュアル整備や訓練を実施しておくことが推奨される。

基準 D：自動化による工数削減効果（費用対効果）が十分か

A. 費用削減効果があるかを検討する。
方法は 2.1.3 参照。

B. 費用対効果が十分でなくても、自動化を推進すべき場合もある。2.1.3 参照。

基準 E：自動化後の属人性が十分に軽減できるか

自動化を行う上で避けるべき状況の 1 つが、導入・運用の属人化である。そのデメリットを以下に例示する。

1. 実装した自動化処理に異常が生じた場合、特定人物以外に復旧できなくなること
2. 自動化処理の実装が共有されず、全体最適や効率的な実装ができないこと
3. 自動化効果の評価ができず、OODA や PDCA が回せなくなること

属人性の軽減をどこまで行うかは組織の方針などにより差異があるが、属人性を十分に軽減した上で、受容できるレベルか判断する必要がある。基本的に特定人物がいなければ成立しないような状況は避ける必要がある。

主な属人化の軽減策は以下の通りである。

1. プロコード[iv]とローコード&ノーコードを使い分ける
   簡単かつ独立した業務の自動化であれば、プロコードのほうが、ツール独自の操作などを覚える必要がなく、デバッグしやすい分、適していると思われる。複雑または複数業務を連続的に自動化したい業務はローコードやノーコードのほうが直感的に実装できる分適していると思われる。上記バランスについては部・チーム内のプロコードのスキル感を見ながら適した手段を使うことが望ましい。
2. マニュアルや運用ナレッジを記録・共有する
   定型的またはシンプルな業務はマニュアルを作成し、自分以外の担当者がいれば担

[iv] プログラム言語を用いてソースコードを記述し、開発する手法。

当者間の人間は誰でもわかるように整備しておくことが望ましい。また、自動化実装の設計/運用上で得られたナレッジについても適宜記録し、関係者間に共有しておくことが重要になる。このような知見については検索性が重要になるため、チケット管理ツールの Wiki 機能等を利用し、一元的に管理することが望ましい。

3. 担当者スキルを管理・リスキルする

3.2.2 の「自動化スキルマップの作成/リスキル」項目の通り、部・チームの要員の誰がどの程度のスキルを所有しているか把握し、全体でスキルアップできる仕組みを構築しておくことが重要である。

スキル感を把握した後は担当者のリスキルを行う必要があるが、自動化に際しては外部研修などで学習した内容だけで十分なスキルを獲得することは難しいため、2.4.3 の「推進体制（ワーキンググループ）の構築」の通り、ワーキンググループで知見を交換・共有しながらスキル向上に取り組むことが望ましい。

4. 変更履歴を管理する

自動化実装やマニュアル、運用ナレッジを変更するときは記録・承認が取られるようにし、意図しない変更を防ぐことが望ましい。自動化処理については設定変更のログを取得しておくことも対策になる。

判断時の具体的な手順

業務自動化の対応優先度を決める方法を記載する。

検討する全業務を列挙したうえで、各業務に対し判断基準それぞれを＜高・中・低＞などで評価する。さらにそのうえで、下記のように判断を行うことが望ましい。

- ✓ 自動化を行うか否か：業務全体の中で閾値を決める
- ✓ 対応順序：業務全体の中で評価値の高いものから優先して行う

ここでは、スコアカードで評価する方法を紹介する。但し、前提として、スコアカードの値のみで自動化対象業務を決定するのではなく、値はあくまで参考情報であることに注意されたい。スコアカードによる評価方法は以下の手順で行う。

1. 各業務に対し、以下の指標でそれぞれの数値を選択する。
   ① 作業量　１：低い　２：普通　３：高い
   ② 定型的　１：都度判断が必要　２：時々例外が存在　３：同様の処理の繰り返し
   ③ 低リスク（自動化処理が意図しない動作を起こした時のリスク）：
   　　１：影響が大きい　２：影響はあるが緊急性は少ない　３：影響が殆どない
2. 各業務で、1.の数値を掛け合わせてスコアを決定する
3. 算出したスコアは、自動化対象業務の選定時に、合わせて管理職の確認をとる

2.4.5　自動化の方向性定義における考慮事項

セキュリティ要件の設定

自動化に使用するツールのセキュリティリスクを検討し、要件を設定する必要がある。セキュリ

ティ業務では機微情報が多く、機微情報を保管している環境ではインターネット接続が制限されることが多い。また、ISMS 等の認証を受けている組織の場合、使用するツールのセキュリティ要件が厳格に定められることが大半である。そのため、事前にネットワーク同士の接続性や組織のセキュリティルールを確認し、要件に合うツールを選定・実装する必要がある。

以下は、特に注意すべきセキュリティリスクの例を示す。

- 脆弱性の存在

  ツールに脆弱性があり、攻撃者がそれを悪用することでシステムを侵害される恐れがある。対策としては脆弱性情報を定期的に確認し、リスクの大きい脆弱性が報告された場合はパッチやアップデート適用をして脆弱性を取り除く必要がある。

- マルウェア感染

  ダウンロードしたツールにマルウェアが含まれていないか注意する必要がある。特に OSS などのフリーソフトはインストール時にユーザーが意図しないマルウェアやアドウェアがインストールされる場合があるため、正規のダウンロードサイトからダウンロードするなどの注意が必要となる。

- ツールのサポート体制

  今回の実装で利用した自動化ツールは OSS が主流となっている。OSS ツールを利用する場合、開発やサポートの状況にも注意が必要である。

  そのツールが活発に開発されていない場合、脆弱性に対するパッチ配信が適切なタイミングでされない恐れがある。

  その場合はツールを安全に利用できなくなってしまうので、公式サポートやコミュニティの存在、脆弱性やバグの報告先は用意されているかなどは利用前に確認したい。

自動化スキルマップの作成／リスキル

自動化実装の前に、導入・運用に必要なスキルを調査し、自動化スキルマップを作成しておくべきである。これを使えば、部・チームの要員の誰がどの程度のスキルを所有しているか把握できる。スキル醸成には時間を要するため、スキルマップ作成は事前に行い、スキル学習も早めに行う。

作成は、（自動化に限らず）セキュリティ部署に担当者のスキル管理表のようなものが既にある場合、そこに自動化実装の必要スキルを追加する対応でも問題ない。

他のチームのスキルを借りることは一時的な対策にはなるが、恒久化すると歪な運用や他チームの負荷となるため、恒久的には自チームのスキルを醸成させることが必要になる。

スキル感を把握した後は担当者のリスキルを行う必要があるが、自動化に際しては外部研修などで学習した内容だけで十分なスキルを獲得することは難しいため、2.4.3 の「推進体制（ワーキンググループ）の構築」の通り、ワーキンググループで知見を交換・共有しながらスキル向上に取り組むことが望ましい。業務自動化への課題感が強い部・チームについては、追加人員を補填する際に、自動化やツール開発のスキルを持つ人員を優先的に登用することでリスキルにかかるリソースを軽減することができる。

スキルギャップの大きい自動化実装をする場合は、リスキルで無視できないコスト（外部研修等）

が生じる可能性があるが、スキルマップを作成すれば、スキルギャップが激しい手段を避けることもできる。

2.4.6　自動化の設計／実装における考慮事項

自動処理への入力データの品質

入力データの品質が求められる。品質が低い場合、自動処理が正常に動作しないなど、自動化の効果が減る可能性がある。

入力データの品質は以下が満たされていることが望ましい。

- データの正確性：誤った入力はプロセス誤作動につながる
- データの完全性：必要なデータが揃っているか。欠損がないか
- データの一貫性：連携システム間で矛盾がないか
- データの信頼性：データソースが信頼できるか
- データの最新性：最新のデータが用いられているか

これらを満たすために、データの重複やエラー排除、フォーマット統一などの事前処理が必要となる場合もある。

自動処理の動作監視

自動処理が正しく動作しているかを監視する。自動処理停止時に管理者へ自動通知される状態が望ましい。

自動処理に関するログ取得

自動処理の実行ログや、自動処理ロジックの編集ログなどを記録する。

自動処理の実行ログは自動処理停止時の原因確認に役立つ。自動処理ロジックの編集ログは自動処理に異常が出た際にロジックが編集されたことによるものかの切り分けに利用できる。

2.4.7　自動化の運用における考慮事項

従業員への情報共有と教育

従業員が自動化後の業務に順応できるように、情報共有や教育・トレーニングを実施する必要がある。自動化によって新たに生じる業務や、自動処理停止時の手作業を理解してもらう必要がある。

特に自動処理停止時の手作業は定期的に訓練をし、手順を作成するだけでなく実際にオペレーションできるか確認しておく必要がある。

2.4.8　自動化の評価における考慮事項

自動処理の短期&中長期的評価

自動処理の実装において、OODA ループを何度か繰り返した後は、セキュリティ業務の自動化がどこまで進んでいるか評価するべきである。評価をする上では、自動処理が正常に動作しているか、

工数削減効果などを確認する。長期的には自動化の成熟度の両方を評価することが望ましい。長期的な評価の具体的な手法としては 2.3.2「具体的なプロセス」等を参照すると良い。

第3章　業務自動化の実践例

本プロジェクトでは、模擬的に、企業におけるセキュリティ業務自動化を実施し、自動化の効果を検証した。この効果検証の最大の目的は、ツールを実際に試用して自動化を実施することで、調査だけではわからない知見を得ることである。本章では検証の内容および結果を、検証の実施順に従って説明する。

なお、本章における検証は、前章の戦略面での考察を行う前に実施しており、前章で紹介した業務自動化における実施順序や判断基準などは踏まえていないことに注意されたい。

検証実施順は、表 3-1 の列「本プロジェクトの検証ステップ」に示す。

表 3-1　効果検証の流れと本章の構成

本プロジェクトの検証ステップ	節	説明内容
検証環境の構築	3.2	・検証環境の構成
自動化するセキュリティ業務の選出	3.3	・セキュリティ業務の分類 ・仮想のインシデント対応フローの定義
ツールを使った自動化の実装	3.4	・仮想対応フローの各業務に対して、 何のツールをどのように適用したか
自動化による効果の検証	3.5	・効果検証方法 ・検証結果

3.1　検証の前提条件

検証における業務ネットワーク環境前提を述べる。下記を満たす業務ネットワーク環境を使用しているものとする。

- ✓ クラウド接続環境がある[i]
- ✓ SIEM が導入されている
- ✓ メールやチャットなどのコミュニケーションツールを使用している

3.2　検証環境の構成

本プロジェクトのセキュリティ業務自動化に使用した環境を図 3-1 に示す。企業の社内ネットワークを模した構成としているが、実際に構築するリソースは検証に必要最低限のみとした。

[i] なお、今回自動化に使用するツールにはオンプレミス版が存在するものが多いため、検証としての一般性を失わないと考えられる。

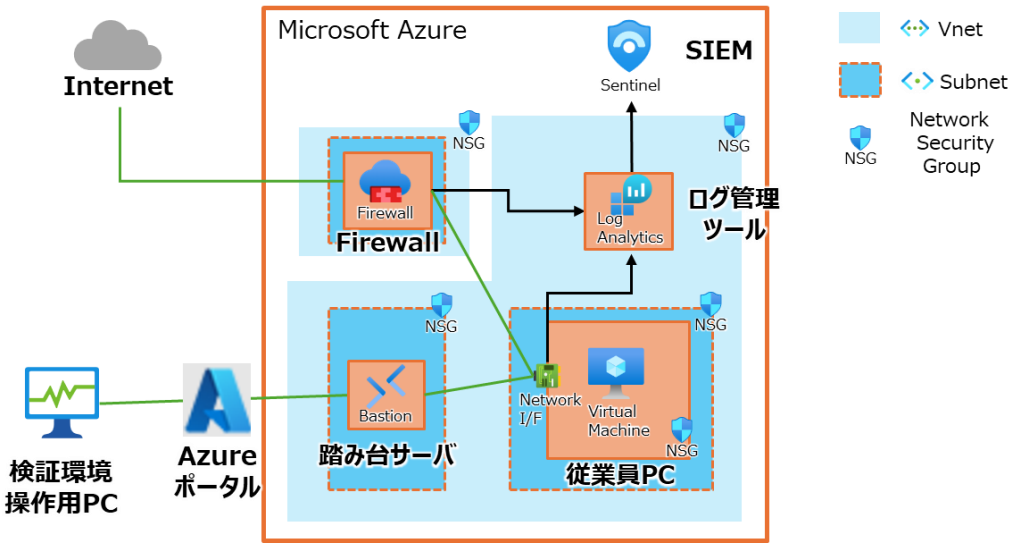


図 3-1　検証環境

環境はクラウド（Microsoft Azure）上に構築した。クラウドとしたのは、検証のしやすさを重視したためである。

従業員 PC

各従業員用の PC として Virtual Machine を用意する（検証に複数台は不要なため 1 台のみ）。社内からは Firewall 経由でインターネットに接続可能としている。

ログの収集

Log Analytics を使用し、従業員 PC と Firewall のログ収集を実施する。Log Analytics はエージェントによるログ収集機能、クエリ（検索）機能、分析機能を持つサービスである。今回、クエリ・分析機能の実行は、SIEM である Sentinel が行う。

アラート設定

SIEM のアラート設定は、従業員 PC から不審な通信先へ通信が発生した際にアラートを発報するルールを設定した。

検証環境操作用 PC から Azure へのリモート接続

検証上、Azure 外の検証操作用 PC から Azure 環境にリモートデスクトップ接続する必要がある。その接続は、踏み台サーバ（Bastion）を経由して行う。踏み台サーバーを使用するのは、外部からの環境内部のリソースへの直接参照を避けるためである。また、リソースにグローバル IP アドレスを付与する必要もなくなる。

3.3　自動化するセキュリティ業務の選出

3.3.1　全体業務の調査と自動化対象業務の選出

まず全体業務調査だが、今回は疑似的な自動化のため、ISOG-J の資料を使い、一般的な業務をすべて洗い出した。

これらの分類を基に、実際のセキュリティ業務の内容、手順、および自動化推進状況を知るために、企業へのヒアリングを行った。ヒアリング先は、製造・IT 企業 3 社で、対象部門は情報システム部門および SOC/CSIRT 部門とし、そこに従事する担当者に回答を依頼した。すると、3 社とも「D. インシデント対応」が業務負荷の面で課題を抱えており、業務自動化への期待度が高いと回答した。

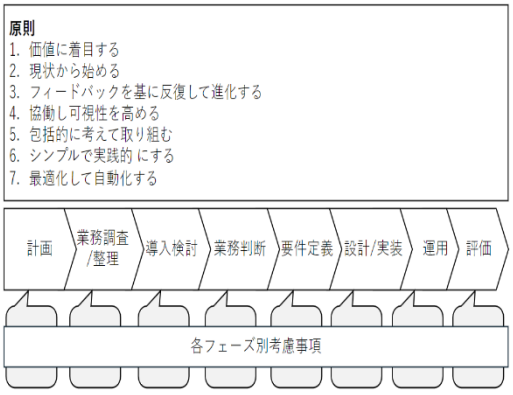


図 3-2 セキュリティ業務の種類とカテゴリ

理由は大きく 2 つあると我々は推測した。1 つは単純作業であること。また、もう 1 つは高負荷であることが挙げられる。1.1 で述べたように企業のセキュリティリスクは年々上がっており、その分セキュリティ担当者の作業も増えている。逆に言えば、インシデント対応業務の改善が、彼らの業務負荷軽減に最も効果的であると言える。以上から我々はインシデント対応に焦点を当てて自動化を進めていくことにした。

また、今回はスモールスタートの観点や実装に使える時間的制限も踏まえ、比較的業務が定期的で自動化しやすいであろう検知システム（SIEM）のアラートの発出から過検知判断までを自動化実装のスコープとした。一連の業務を「初動調査」と定義し、次節では初動調査の流れについて説明する。

3.3.2　今回想定する初動調査について

インシデント対応の自動化を進めるため、初動調査の例を挙げ、作業単位に詳細化していく（図 3-3)。初動調査は、現場からの問い合わせ、または SIEM のアラートをトリガーとして始まる。検知したアラートは担当者によってタスク管理ツールに登録され、その後の進捗管理が行われる。この作業は IT 業界においてはチケット管理ツールを利用することが多いため、本書ではチケット発行として進めるものとする。担当者名の登録など必要な情報をチケット管理ツールに入力し、チケットを発行後、チーム内へ共有するためインシデント通知をメール送信する。その後はトリアージの判断をするため、脅威調査と過去事例の確認を並行して進めていく。脅威調査では外部脅威 DB サイトや社内脅威 DB を活用し、問題の起きているファイルのスキャンや、危険な IP アドレス・URL、マルウェア検体のハッシュ値を検索して、詳細情報を収集する。それが危険であると判断された情報であり、社内脅威 DB に未登録の新情報であれば登録も必要となる。別途必要に応じてユーザヒアリングを行う。

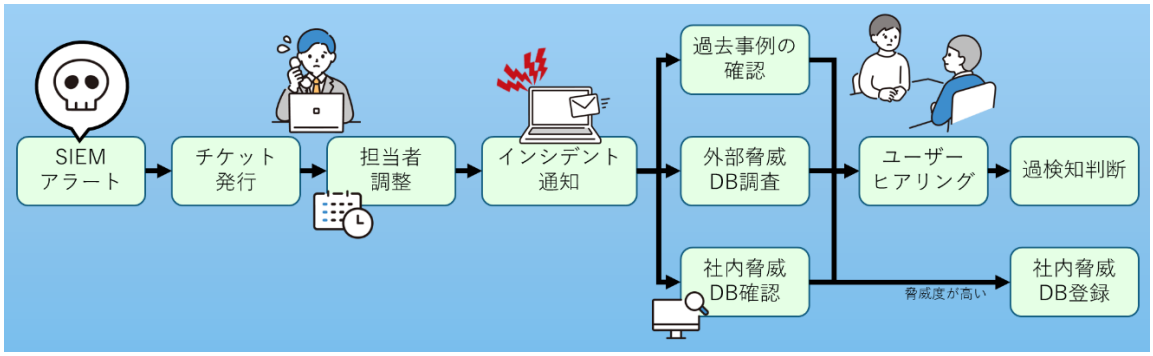


図 3-3　本書が想定するインシデント対応の初動調査フロー例

本書が対象とする業務範囲は検知アラートをトリガーとし、検知アラート発生前に想定される、SIEM の導入、検知閾値の設定といった業務は今回の自動化対象外作業とする。また、同様にインシデントレスポンスにおけるユーザヒアリングと社内脅威 DB への登録までを自動化の対象とし、その後の過検知判断や詳細分析は対象外とする。

3.4　ツールを使った自動化の実装

ここでは、当プロジェクトで実装した内容を説明する。また、本節に登場するツールおよびその用途は以下の通りである。

- ✓ **SIEM**：収集した通信ログから不審な通信を検知しアラートを発報する
- ✓ **チケット管理ツール**：インシデント情報の管理、情報の一元化的を行う
- ✓ **チャットツール**：セキュリティ部署メンバー間での情報連携をする
- ✓ **SOAR**：自動処理のためのシステム間連携等を行う
- ✓ **社内脅威 DB**：IR 時に集約した脅威情報を記録し活用している
- ✓ **評価サイト**：IP アドレスやドメインの悪用情報を確認する

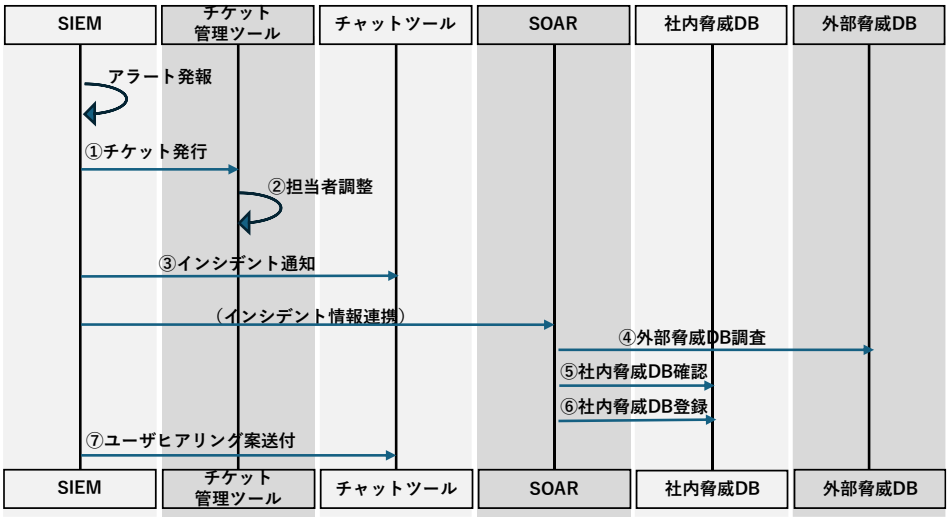


図 3-4 のシーケンス図は、各種ツールのブロック間でどのような自動処理が行われているかを表

している。

上部にある四角で囲まれた部分が各ツールを表しており、各ツールから伸びる縦線間をつなぐ矢印

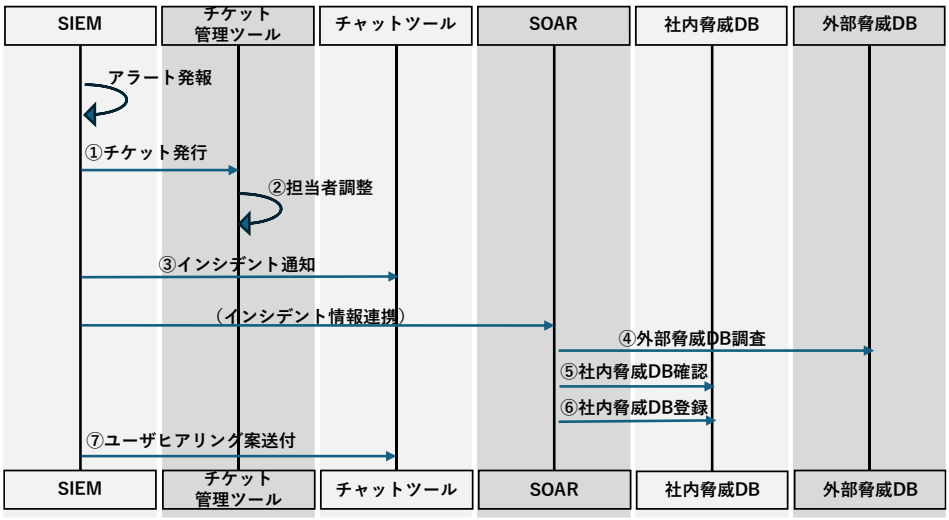


図 3-4 各種ツールのブロック間での自動処理内容

でツール間の連携と作業内容を簡潔に示した。例えば、SIEM からチケット管理ツールに伸びる横線に「①検知チケット発行」とあるが、これは SIEM からチケット管理ツール上に検知チケットが発行されたことを示す。また、「②担当アサイン」はチケット管理ツールの縦線から出てその場でループするような記載になっているが、これはチケット管理ツール内で処理が完了することを示す。

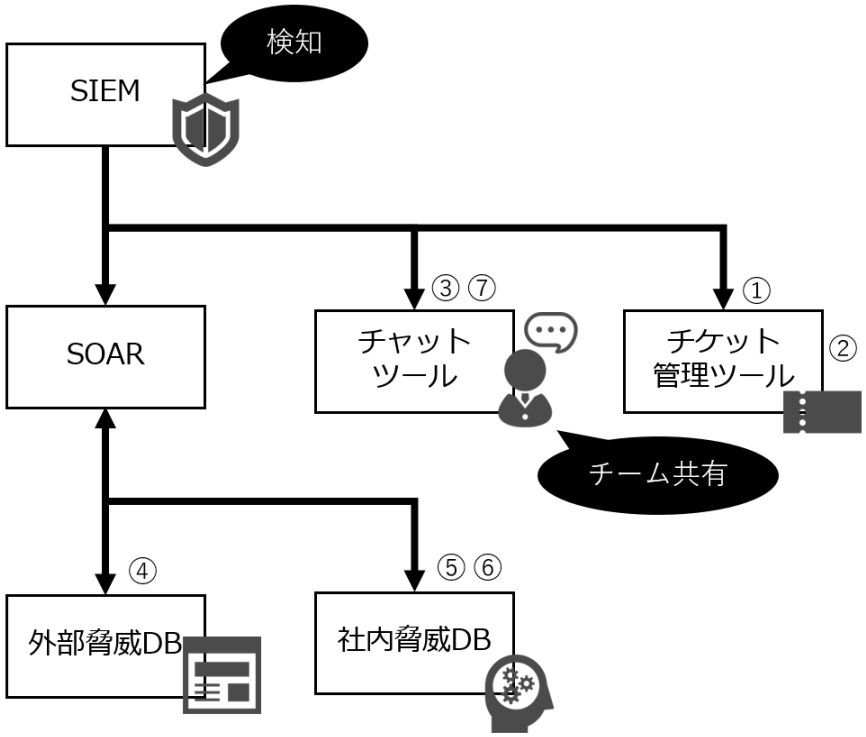


図 3-5　各ツール間の連携

図 3-5　各ツール間の連携は各ツール間連携と自動化した処理を図にしたもので、図内の①などの番号は図 3-4 各種ツールのブロック間での自動処理内容と対応している。

ここから、上記の図と対応した各アクションの説明に移る。

① 検知チケット発行
この作業は SIEM で検知が上がった際に SIEM 上で自動化ロジックが起動しチケット管理ツールのインシデント管理 DB に新規チケットが発行され、検知内容が自動で反映される。

② 担当アサイン
この作業はチケット管理ツール内に組み込まれたロジックによるもので、チケット発行日をもとに内部に組み込まれたシフト表を参照し、担当者をチケット内に自動記入する。

③ インシデント通知
SIEM で検知した内容をチャットツールに投稿し、インシデント発生を通知する。
インシデント通知には不審な通信先などが含まれる。

④ 社外脅威 DB 確認
SIEM の検知内容の中から IoC 情報を取得し、外部の脅威 DB サイトに自動連携し、評価結果を確認する。

⑤ 社内脅威 DB 確認
社内脅威 DB を参照し、過去に脅威 DB として登録されたことがあるかを確認する。

⑥ 社内脅威 DB 登録
④の評価の判定結果が指定した閾値以上の場合、社内脅威 DB に以下情報を記録する。
・IoC 情報(ドメインや IP アドレスなど)
・評価スコア
・評価ページのリンク

⑦ ユーザヒアリング案送付
SIEM から受け取ったインシデント情報をもとに、ユーザヒアリングの文案を作成しチャットツールに文案を投稿する。

3.5 効果測定の方法と結果

3.5.1 測定方法

次に自動化ツールを使ってセキュリティ業務を自動化した際にユーザーが得られる効果について記載する。今回我々は工数削減効果の定量評価と、副次的効果の定性評価を行った。

定量効果測定として、自動化前の手動運用における作業時間と、ツールを使った自動化後の作業時間を比較した。今回ツールを導入したのは、検知→通知→初動脅威調査→内部脅威 DB 検索→調

査結果報告→クローズ の大きく分けて 6 フェーズの作業となる。手動運用の方は SIEM で発生したアラートを担当者が目視で発見してから、チケット管理ツールによるチケット発行処理、チャットツールやメールでの通知文の作成、社外脅威 DB での初動調査などをすべて手作業で行い、トリアージの判断とインシデントのクローズ通知文の作成・送信するまでの時間を測定した。

3.5.2 算出方法

手動運用はチームメンバーの 5 人がそれぞれ 1 件のインシデント対応を実施し、かかった時間の平均値を結果とした。インシデント 1 件あたりの削減時間は

削減時間［秒/件］＝ 手動運用の計測時間［秒/件］― 自動化後の計測時間［秒/件］

として算出している。また、参考として年間削減工数を算出するため、1 か月あたり 50 件のインシデント（過検知を含む）が発生すると仮定し、

年間削減時間［時間/年］＝ 削減時間［秒/件］× 50［件/月］× 12［月/年］÷ 3600

と算出した。

また、作業の中の初動脅威調査に関しては、1 インシデントで IP アドレスや URL、ファイルハッシュ値などの IoC 情報が複数出ることもあると仮定し、アラート 1 件に対し 3 回作業するものとして計算されている。そのため、年間の工数削減効果の計算の計算時は初動脅威調査による工数削減効果のみ

年間削減時間［時間/年］＝ 削減時間［秒/件］× 150［件/月］× 12［月/年］÷ 3600

として計算されている。

3.5.3 測定結果

測定の結果、インシデント 1 件あたり約 7.7 分、年間で約 100 時間の工数削減ができるとわかった。詳細結果については表 3-2 に示す。

表 3-2 業務量削減効果の測定結果

	自動化前 工数[秒/件] ※	自動化後 工数[秒/件]	自動化前後 の工数差[秒/件]	削減率[%]
検知	127.0	5.7	121.3	95.5%
調査開始通知	141.8	5.5	136.3	96.1%
初動脅威調査	83.0	16	67.0	80.7%
内部DB検索	21.0	20	1.0	4.8%
調査結果報告	98.3	30.6	67.7	68.9%
クローズ通知	137.8	70.1	67.7	49.1%
合計［1 件あたり］	608.8	147.9	**460.9［秒/件］**	**75.7%**
合計［年間］			**99.5［時/年］**	

3.3.2 で説明したインシデント対応の初動調査について、平均 1 件 30 分程度の時間がかかっていると見込んだ場合、年間でかかっている初動調査の時間は以下の通り計算される。

300[時/年] ＝ 30[分/件] × 50［件/月］× 12［月/年］÷ 3600

上記の内容を踏まえると、初動調査 300[時/年]中のうち 100[時/年]を削減できたことから、３分の１の工数を削減できた。今回自動化していない業務はより高度な自動化を要するものや人間が思考して行うべき業務であるため、スモールスタートとして自動化しやすい業務を自動化した時の効果の参考として見ていただきたい。

また、今回は 50 [件/月]と仮定したが、発生頻度が増加した場合はより大きな削減効果が得られる（表 3-3）。にある通り、発生頻度が 100[件/月]の場合は 199.0[時/年]、200[件/月]の場合は 398.0[時/年]の削減効果が得られる。

表 3-3 発生頻度ごとの削減効果

発生頻度(件/月)	削減効果(時/年)
50	99.5
100	199.0
150	298.5
200	398.0

自動化における効果が特に高かったのは、検知および調査開始通知の業務である。

検知業務はインシデント情報のチケット管理ツールへの登録や、担当者を決めるために担当者負荷や割り振りルールを確認する工程があり、人手による確認作業に時間がかかっていた。今回は API 連携による情報のコピーが自動的に行われることで、重複する内容確認作業を省くことができ、かつ担当振り分けもルールに沿って自動的に実施するため、判断する手間や時間を省くことができた。

調査開始通知業務は、コミュニケーションツールを使った作業にマンパワーを要していた。手動運用の場合は仮にテンプレートの通知文が用意されていても、いちいち内容を確認して書き写す作業が発生していた。情報をそのままコピーするだけであれば SOAR - インシデント管理ツール間の連携により、一瞬でインシデント管理ツール内に通知文章を作成することができる。

3.5.4 定性効果

自動化では、定量的な工数削減効果以外に、以下のような定性効果も見込める。( ) 内は対応する 2.1「なぜ自動化するのか」で述べたメリットである。

- マンパワーの節約（1. リソースの再割り当て）
- 単調作業削減によるモチベーションの上昇（2. 人材の満足度向上）
- 業務プロセスの見直し（3. 業務プロセスを改善する機会の創出）
- 人的ミスの軽減（4. 操作・確認ミスの削減）
- 即時対応（5. 対応速度の向上）

今まで人手で行っていた作業をシステムに置き換えることで、手の空いた担当者を人手の判断が必要な作業に回すことができる。昨今不足している貴重なセキュリティ人材のリソースを節約することは本 PJ が解決したかった背景課題へのアプローチとなる。

担当者の精神面でのメリットも定性的ではあるが効果が大きい。折角セキュリティ人材を増やしても単純作業ばかりさせていてはリソースがもったいない上に、モチベーションの低下や離職に繋がる可能性もある。

自動化ツールの導入は、セキュリティ業務のプロセスを見直す機会にもなる。今回の効果測定シナリオの作成に向け、我々は企業ペルソナの策定と仮想の業務フローを作成した。セキュリティ業務の現場では属人化した業務の引継ぎが横行しており、業務フローが文書として存在しないケースも多い。自動化ツールを活用するために自社の状況を整理することで、無駄の多い連絡経路や社内規定と実運用の乖離など、業務負荷以外の課題の可視化につながる。

人のやることにミスはつきものである。今回のシナリオの中でも単純な通知文の作成やチケット情報の入力作業があったが、URL の貼り忘れやメール宛先の間違いなどが度々発生していた。セキュリティ作業のシステム化は人的ミスをなくすことで、情報漏洩等のリスク低減および手戻りの削減にも繋がることが実感できた。

自動化前は簡単な判断も人が考えて行っていたが、自動化すれば閾値に従って即時判断できる。自動化する作業（フロー）を増やすほど、インシデント対応全体のリードタイムはどんどん短縮され、より早期の対策立案が可能となる。

また、実際に自動化ツール導入を経験することで得た知見として

・対応履歴の自動記録

の効果もあった。対応履歴を自動で取得することで、記録漏れがなくなり、問題が発生した際には誰がどのような対応手順を取ったかを確認できる。

3.5.5　削減した工数の活用

自動化によって空いたリソースについて、どのように活用するかを考えておくことも自動化では重要になる。今回の自動化実装・検証はスモールスタートの観点から業務のスコープを絞って自動化実装を行っているが、検証で得られた経験やスキルを他の業務の自動化に活かせば更にセキュリティ業務の自動化を推進することができるほか、自動化が進んで空いたリソースが増えれば脅威ハンティング等より高度なセキュリティ業務にリソースを回すことができる。このようにしてセキュリティ部署の状況を、業務負荷が増大してますます自動化に使えるリソースが減少していく「守りのネガティブスパイラル」から、業務自動化を進めてセキュリティ業務の自動化・高度化を広げていく「攻めのポジティブスパイラル」に変えていくことが重要となる。

第4章　まとめ

本書では、セキュリティ業務自動化の推進における重要な戦略的視点と技術的なアプローチ例をまとめた。業務自動化は最初からスムーズに進むわけではなく、現実的には数々の課題に直面しながら、その都度考え方やアプローチを改善して取り組んでいくことになる。課題に直面した時には、本書を活用して自部署の状況を確認し、本書の推奨事項と比較することで、解決策を見つけるための一助となれば幸いである。

セキュリティ部署の業務自動化は、戦略面と技術面の両方で考える必要がある。戦略面だけでは検証してみないと分からないことがあり、技術面だけではツールベースの考え方になり課題や目的に沿った自動化にならない。

業務自動化の戦略は「基本的なプロセス（実施順序）」と「戦略的な考慮事項」を考慮することが重要である。定例的な運用業務とは異なり、セキュリティ担当者のスキルが少ないため、適切な実施順序や考慮すべき点を理解して進めることが自動化推進の鍵となる。

セキュリティ部署の業務負荷は年々増加しており、業務自動化の重要度はますます高まっている。自動化の推進は工数短縮だけでなく、運用の最適化や高度化にも寄与する。そのため、自動化の重要性を十分に理解し、優先度を上げて取り組むことが求められる。

本書は様々な企業・個人へのヒアリングおよび技術検証をもとに作成したが、内容はプロジェクトメンバーで考察したものであり、ヒアリングにご協力いただいた企業・個人の主張とは異なる点がある。そのため、本書の内容は一つの参考であり、企業においては自社の状況に応じて柔軟に活用することが求められる。

なお、本書は 2024 年 6 月時点の情報をもとに作成しており、技術の進展を考慮すると、本書の内容が有効である期間は 2 年程度と考えられる。業務環境や技術は日々変化しているため、常に最新の情報と技術を取り入れることで効果的な業務自動化を推進してほしい。

付録 A　専門用語集

用語	意味・解説
AIOps	機械学習を利用してアプリケーションのデータを分析し、IT 運用を簡素化するとともに問題解決を自動化する手法
API	あるソフトウェアの機能を別のソフトウェアから呼び出す仕組み
CSIRT	セキュリティインシデントへ迅速、かつ適切に対処するために設置されるセキュリティ分野の専門チームまたは組織
DevOps	開発担当と運用担当が連携・協力し、フレキシブルかつスピーディーに開発するソフトウェアの開発手法
IR	インシデントレスポンスの略称であり、セキュリティ上の脅威となる事件やトラブルに対する活動全般を指す
ISMS	情報セキュリティマネジメントシステムが、リスクアセスメントにより、必要なセキュリティレベルを決めてシステム運用するための仕組み。ISO27001 に準拠していることを証明する認証がある。
ITIL	IT サービスマネジメントの成功事例をまとめ、体系化したガイドラインのこと
MISP	オープンソースの脅威インテリジェンスプラットフォーム
OODA	観察・判断・決定・行動の 4 ステップによる意思決定プロセスで、迅速な意思決定が求められる場に使われる
OSS	オープンソースソフトウェアの略であり、利用者の目的を問わずソースコードを使用、調査、再利用、修正、拡張、再配布が可能なソフトウェアの総称
PDCA	計画・実行・評価・改善の 4 ステップによる意思決定プロセスで、目標に沿った意思決定を行いやすい
PoC	新しいアイデアや技術の実現可能性を確認するための試験的な検証のこと
SIEM	ネットワークの監視、サイバー攻撃やマルウェア感染などのインシデント分析・検知を目的としたツール
SOAR	セキュリティ運用業務の効率化や自動化を実現するための技術またはソリューション
SOC	ネットワークやデバイスを監視し、サイバー攻撃の検出や分析、対応策のアドバイスを行う組織
UX(UsereXperience)	ユーザーが製品やサービスの利用で得られる体験を表す言葉
VirusTotal	ファイルやウェブサイトの悪性検査を行うウェブサイト

Wiki	PoC ブラウザーを使って、手軽にウェブページを作成・編集できるシステム
アーティファクト	（フォレンジック・アーティファクト）フォレンジックを行う際に証拠として収集される、価値のあるデータ
アドウェア	宣伝や広告を目的とした様々な動作を行うプログラムの総称
エージェント	クライアント端末にインストールされ、特定のタスクを実行するためのソフトウェア
オンプレミス	システムの稼働やインフラの構築に必要となるサーバーやネットワーク機器、あるいはソフトウェアなどを自社で保有し運用するシステムの利用形態
クライアント	ユーザーが直接操作するデバイス サーバーが提供したサービスを受け取るコンピューター
クラウド	インターネットなどのネットワーク上でサービスとして提供されている、ハードウェアやソフトウェアを用いたコンピューターの利用形態
サーバー	サービスや機能を提供するコンピューター
脆弱性スキャン	ソフトウェアのセキュリティ脆弱性を検出する操作のこと
セキュリティインシデント	セキュリティ上の脅威となる事件やトラブル(不正アクセス、データ漏洩など)のこと
デバッグ	プログラムや関数における「バグ」と呼ばれる間違いを発見し、不具合の原因を特定・修正する作業
トリアージ	セキュリティインシデントが起きた際に、複数インシデントの優先順位を迅速に判断・分類すること
ノーコード	ソースコードのコーディングを行わずに開発を行うことが可能な開発手法
ハッシュ値	データに対して不可逆的な変換を行って生成される値のこと。データの整合性確認等に利用される。
フォレンジック	セキュリティインシデントが起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにすること
マルウェア	悪意のあるソフトウェア全般を示す
リポジトリ	データを保存、管理する場所のこと
ローコード	0 からコーディングを行うよりも少ないプログラムコードで開発ができるという開発手法
脅威ハンティング	自組織に既に脅威が存在することを前提として、アナリストの知識やセキュリティログを活用して潜在的な脅威や侵害を洗い出す手法・活動

脆弱性	コンピューターや OS などのハードウェア・ソフトウェアなどにおいて、設計上のミスやプログラムの不具合(バグ)などが原因で発生する、セキュリティ上の欠陥のこと
属人化	業務が特定の個人に依存している状態のこと
レピュテーション	対象のファイルやサーバーの過去の実績や現在の利用状況などから評価を行い、それに基づいて悪質なファイル／サーバーであるかどうかを判断する仕組み

付録 B　参考文献

1. ISOG-J.
   セキュリティ対応組織の教科書　第 3 版, 2023 年.
   https://isog-j.org/output/2023/Textbook_soc-csirt_v3.1.pdf

2. Jeffery D. Smith. システム運用アンチパターン（田中 裕一 訳）, 2022 年, 352 ページ

3. 経済産業省.
   DX レポート～IT システム「2025 年の壁」の克服と DX の本格的な展開～, 2018 年,
   https://www.meti.go.jp/shingikai/mono_info_service/digital_transformation/pdf/20180907_03.pdf

4. 中 寛之. 【ITIL4 公認】ITIL 4 の基本 図解と実践. 日経 BP, 2022 年, 400 ページ

5. 日本シーサート協議会. CSIRT 構築から運用まで, NTT 出版, 2016, 182 ページ

6. パロアルトネットワークス株式会社.
   AI によるセキュリティの自動化は本当に有効？調査で見えた実態, 2024 年,
   https://wp.techtarget.itmedia.co.jp/contents/81958

7. 総務省.
   情報通信白書 令和 5 年版 「第 2 部　情報通信分野の現状と課題」, 2023 年,
   https://www.soumu.go.jp/johotsusintokei/whitepaper/r05.html

8. yamoryBlog.
   2022 年脆弱性セキュリティレポート 増加する脆弱性とソフトウェア管理の重要性, 2022 年,
   https://yamory.io/blog/2022-security-report/

謝辞

本書の執筆にあたり、貢献いただいたすべての人への感謝を表明します。

奈良先端科学技術大学院大学 門林 雄基 教授には、本書の査読と講評をいただきました。また、プロジェクト全体の進め方へのアドバイス、タスクの適切性についてもご指導いただき、プロジェクト目標をより明確かつ洗練することができました。

東洋大学 満永 拓邦　准教授にも、本書の査読と講評をいただきました。読み手にインパクトを与える資料作りや伝え方についてのアドバイスに加え、執筆用の環境整備にもご尽力いただき、効率的に検証・執筆活動を進めることができました。

AWS 松本様には、さまざまな自動化ツールをご紹介いただきました。ツールそのもののご紹介だけでなく、事前の運用設計の重要性や法的な観点など、我々の調査だけでは得られなかった自動化の知見もいただき、感銘を受けました。

isog-j の皆様には豊富な実践経験から、セキュリティ業務自動化を進めるにあたって前提となるペルソナの重要性や、そもそもセキュリティ業務とはどんなものか、という PJ の根幹となる知見をいただきました。また、参考文献にもあります「セキュリティ対応組織の教科書」は文字通り本 PJ における教科書となりました。

Colorkrew の皆様には実際に行っている自動化の実装方法や、など経験と実績に基づいた自動化のナレッジをご教示いただき、アプローチ方法に困っていた我々を助けていただきました。

独立行政法人 情報処理推進機構 産業サイバーセキュリティセンターの職員の方々には、遅くまで執筆・検証作業のために施設をお借りし、事務的な面でたくさんの助力をいただきました。何より中核人材育成プロジェクトの、セキュリティの基礎知識、実践的な演習やプロジェクトマネジメントなど、さまざまな講義の経験全てが本プロジェクトにつながっています。

チームメンバー派遣元企業の方々には、本プロジェクトにおける活動へのご理解ご協力、ひいてはこのような経験の場を用意していただけたことに、心からの感謝を申し上げます。

本書の読者の皆様には最後まで読んでいただけたこと、心より感謝いたします。我々ICSCoE7 期卒業 PJ セキュリティ業務自動化推進チームは、このレポートがあなたにとって少しでも助けになることを祈っております。

最後に、本プロジェクトおよび本書の作成をともに実施した、下記メンバーの皆様に感謝を伝えたいと思います。

【リーダー】
上田　貴大
【サブリーダー】
橘田　渉
皆吉　遥
【メンバー】
兼子　翔伍
長嶋　秀孝
安田　卓磨