G-02

生成 AI を用いたインシデント対応の CISO への報告書作成システムの開発

近藤 銀音†　　川橋 裕‡
Kondo Ginto　　Yutaka Kawahashi

1. はじめに

近年，サイバー攻撃が増加傾向にあることや，セキュリティ人材が不足していることから，企業はインシデントへ対応するリソースもひっ迫している状況であるといえる．インシデント対応チームの作業の中でも，報告書の作成は負担の大きい作業の一つである．特筆すべきは，インシデント対応を完了し，振り返りや，知識の蓄積のために作成する技術報告書の内容と，組織の CISO(Chief Information Security Officer，最高情報セキュリティ責任者)に報告するために作成する報告書の内容との間には，文書作成の内容に差異が生じている点である．そのため，インシデント対応チームは，別個の報告書を作成しなければならない状況となっている．

そこで本研究では，インシデント対応中に担当者が作成している，インシデントの対応手順や対応タイムラインを記載したメモから，LLM を用いて，CISO へ報告するための報告書を作成するシステムを開発する．システムの使用によって，報告書作成作業の時間短縮を図り，作業担当者の負担軽減を目指す．加えて，メモ作成の担当者および報告書作成の担当者が誰であろうと，インシデント報告書の内容に一定の質を確保することを目指す．

2. 関連研究・関連システム

2.1　関連研究

介護業務におけるヒヤリハット報告書作成支援システム[1]では，メモと報告書の作成を音声入力によって行うシステムを構築している．多くの介護事業所では，不安全な行動や状態に気づいた場合に，ヒヤリハット報告書とメモを作成している．研究では，事例の発生時に録音アプリケーションを使用し，事例の情報を録音することで，メモと報告書作成の効率化を実現した．実験では，システム利用によって，メモと報告書作成の時間を短縮したことを示した．

サイバーセキュリティのインシデント報告書には，プログラム等も数多く記載される．数字と英単語が多く使われており，音声で入力するのは難しい．よって，部分的な活用の余地はあるものの，インシデント報告書の全文に 対しては，音声入力のシステムの利用は困難である．

2.2　関連システム

Waroom[2]は，株式会社 Topotal が提供しているインシデントマネジメントサービスである．Slack を利用したインシデント対応の仕組みとなっている．機能の一つとして，AI を使用した文書作成が用意されている．インシデント対応中の Slack 上のやり取りの内容を基に，文書を自動で作成する．

Waroom は，Slack でインシデント対応を行うことを前提としている．そのため，Slack を使用していない組織はサービスを利用することができない．加えて，作成した文書は Waroom のシステム内に出力される．そのため，文書を扱いやすいデータフォーマットで受け取ることができない．

3. 提案手法

本研究で使用する LLM には，OpenAI が提供する GPT-4 Turbo[3]を使用する．GPT-4 Turbo は，GPT-4 よりも高機能なモデルとなっている．なお，システム構築時では，GPT-4 Turbo の安定版は提供されていなかったため，プレビュー版(gpt-4-1106-preview)を使用している．ユーザが使用するツールには，Excel を使用する．

報告書の作成は，組織の上層部や他組織への報告など，社内および社外とのやり取りを行っており，事務職員が担当することも多い．そのため，広く普及しており，事務職員が普段の業務から使用している可能性が高い Excel を入力ツールとして採用した．さらに，Excel は文書の印刷と親和性が高いツールであることも利点として挙げられる．

作成する報告書は，図 1 のような書式で作成する．書式は，私立大学情報教育協会が公開している情報セキュリティ事故発生報告書[4]を参考として，独自に作成した．

インシデント報告書

インシデントの発生日時		2024/1/1 18:07
インシデントの種類		☐ システム障害
		☑ 外部からの攻撃
		☐ 情報漏えい
インシデントの概要		弊社ホームページが不正なページにリダイレクトされる障害が発生。原因はVictorサーバのhttpd.confが不正に書き換えられたことによる。
被害サーバ・機器		Victorサーバ
想定される原因		BF攻撃による[redacted]ユーザの不正ログイン、sudoの脆弱性(CVE-2019-18634)を利用した特権昇格、httpd.confの不正なリダイレクト設定追加。
初期対応	暫定措置	httpd.confから不正なリダイレクト設定を削除し、apacheを再起動。[redacted]ユーザのパスワード変更。/etc/sudoersからpwfeedbackをコメントアウトし、sudoの脆弱性を対処。
	現在の状況	httpd.confの修正とapacheの再起動により、ホームページの正常な閲覧が可能に。sudoの脆弱性対策を実施し、攻撃経路を遮断。
復旧時期の見込み		2024-01-01 18:46に問題解決を報告。

図 1 : システムを使用して作成した報告書の例

3.1　システム構成

本研究で作成したシステムのシステム構成図を図 2 に示す．

†和歌山大学大学院 システム工学研究科 川橋研究室

‡ 和歌山大学学術情報センター

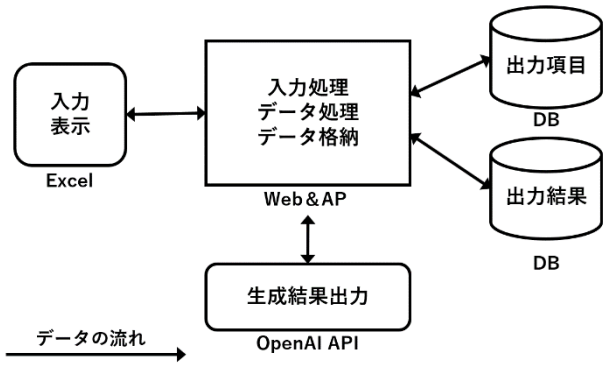

図 2 : システム構成図

Web&アプリケーションサーバは，Excel や OpenAI API とのやり取りにおけるデータ処理，データベースへのデータ格納を行う．Web&アプリケーションサーバと Excel とのやり取りには，API を使用している．データベースは，出力項目の保管用と出力結果の保管用の 2 種類を用意している．

4. 実験

システムの有用性を評価するために，報告書の正確さを測る評価基準を表 1 のように作成した．

表 1 : 評価基準表

項目	評価基準
インシデントの発生日時	正確な日時であるか
インシデントの種類	インシデントの種類(システム障害・外部からの攻撃・情報漏えいから選択，複数可) が正確であるか
被害サーバ・機器	正確なサーバ名・機器名であるか
インシデントの概要	発生したインシデントを簡潔に要約できており，必要な情報を迅速に把握できるか
想定される原因	攻撃手法や悪用された脆弱性，エラーなどが記載されており，原因を把握できるか
一次対応 (暫定措置)	実施した具体的な対応策，修正箇所を把握できるか
一次対応 (現在の状況)	継続中の対応策とその進行状況を把握できるか
復旧時期の見込み	復旧計画とそのスケジュールを把握できるか 復旧済みの場合は，復旧した日時が正確であるか

評価基準は，一般的なインシデント報告として必要な内容を基準としており，報告書の各項目で「〇」と「×」で評価する．

システムに入力する，インシデントに関して記載されたメモには，情報機器管理コンテストにて実施した 3 つのインシデントシナリオから作成されたものを使用する．情報機器管理コンテストとは，和歌山大学が運営を担当している情報セキュリティに関するチーム対抗のコンテストのことである．使用するインシデントシナリオを下記に示す．

1. Sudo の脆弱性によって特権昇格を行い，Web サーバソフトの設定ファイルが改ざんされるインシデント
2. ネットワーク機器の設定不備によって正常通信が途絶されるインシデント
3. ユーザの Web ページの設定ファイルが改ざんされるインシデント

インシデントに関して記載されたメモは，2 種類用意する．1 つ目は，評価基準をすべて満たすように独自に作成したメモである．1 つのインシデントシナリオにつき，1 つ作成する．2 つ目は，コンテストにてコンテスト参加者が作成するトラブルチケットである．トラブルチケットとは，コンテストの参加チームがインシデントの対応を記録として残したものである．1 つのインシデントシナリオにつき，4 チーム分のトラブルチケットをシステムに入力するメモをして使用する．

5. 実験結果・考察

各シナリオの平均所要時間と平均所要費用について表 2 に示す．

表 2 : 平均所要時間・平均所要費用

	シナリオ 1	シナリオ 2	シナリオ 3
平均所要時間	23.2 秒	34.5 秒	32.56 秒
平均所要費用	$0.033	$0.029	$0.030

平均所要時間と平均所要費用のどちらとも，シナリオごとに 5 回計測し，それらの平均を算出している．平均所要時間は全シナリオで 30 秒程度であり，手作業で報告書を作成するよりも時間短縮となるのは明らかといえる．平均所要費用は全シナリオで$0.03 程度であり，使用する組織にとって大きな負担とならない．

システムを使用して作成した報告書を評価した結果は，各シナリオで独自に作成したメモはほぼ「〇」評価となった．ただ，想定される原因という項目においては，シナリオ 2 で「×」評価となった．これは，インシデントを引き起こす原因となった機器の設定となってしまった背景が生成 AI によって簡略化して記載されたからである．このようなインシデントの原因となった情報は，CISO に正確に伝えるべきである．

トラブルチケットをメモとして使用した場合は，「〇」評価が多くなる場合と，「×」評価が多くなる場合が報告書ごとに分かれた．「×」評価の多い報告書では，メモに報告書の項目に必要な内容が記載されていなかった．実験結果より，GPT-4 Turbo は報告書作成に十分な性能を有していることが示された．さらに，作成者が異なっていても，報告書に記載したい内容が十分に記載されているメモであれば，良い評価となった．ゆえに，システムを使用することによって，報告書の均一性が確保できているといえる．逆に，報告書に記載したい内容がメモに記載されていなければ，報告書に正確な内容が記載されないことも示された．良質な報告書を作成するためには，報告書に必要な要素を考慮しながらメモを作成しなければならない．

5. 今後の課題

今後の課題として，今回の実験では 3 種類のシナリオでしか検証できなかったため，他のインシデントでも良質な報告書を作成できるのかを検証し，LLM にとっての得意なインシデントと不得意なインシデントを明らかにしたい．さらに，記載したい事項がメモで言及されていない場合は，報告書作成の段階で，ユーザとシステム間の対話によって，不足分の内容を補完する機能の追加をしたい．

参考文献

[1] 藤井勝央, 井口信和：介護業務におけるヒヤリハット報告書作成支援システム
情報処理学会第 83 回全国大会講演論文集, No1, pp.451-452 (2021).
[2] 株式会社 Topotal：Waroom
https://waroom.com/，(参照 2024-07-18)
[3] OpenAI：GPT-4 Turbo
https://help.openai.com/en/articles/8555510-gpt-4-turbo，(参照 2024-07-18)
[4] 私立大学情報教育協会：情報セキュリティ事故発生報告書
https://www.juce.jp/secslide/2016/s320.pdf，(参照 2024-07-18)