社員間の利用を考慮した情報セキュリティ管理支援アプリケーションの再構築

Reconstruction for the Information Security Management Application Considering Employees Communication Uses

1641059　清水 大輔
Daisuke SHIMIZU

指導教員　秋葉 知昭

In this study, I proposed a web application considering employees communication uses to supporting company information security management. I have added in this system to responsible person for information security management support application, and added bulletin board system, comparison with past data, login history system.

1．緒　言

近年，企業が有する個人情報や重要な技術情報などを窃取したり，企業のシステムを停止させたりするサイバー攻撃の件数は増加傾向にある．2017 年の企業の CISO や CSIRT に関する実態調査[1]によると，約 4 割の企業がサイバー攻撃を受けた経験があるとされている．

企業を取り巻くサイバー攻撃への脅威が増す一方，多くの企業が十分な対策を取れているとは言いがたい．こうした原因の一つに，セキュリティ対策に対して経営者が十分なリーダーシップを発揮していないことが挙げられる．

そこで本研究は，先行研究[2]で構築した企業情報セキュリティ管理支援システムに対して社員間の利用を考慮した改良を行い，より管理支援能力の高いシステムの構築を目指す．

2．管理運用手法

本研究は，情報セキュリティ管理システム(ISMS:Information Security Management System)の標準である ISO27000 シリーズから，ISO27001 及び ISO27002 を使用する．先行研究[3][4]では，ISO27001 の附属書 A に加えて MDM を要件として組み込んだ附属書 B を作成している．このシステムに先行研究[2]では，機械学習及び Web クローリング・スクレイピングを利用したアドバイスを行う機能を導入した．本研究では，このシステムに新たに責任者の追加と，過去データとの比較機能，ログイン履歴機能，掲示板の追加を行う．

3．先行研究

図 1 に先行研究[2]のシステム概要図を示す．このシステムでは，機能としてアカウント編集機能，閲覧要件・用語検索機能，チェック機能，報告機能の 4 機能が実装されている．また，利用するユーザは，一般ユーザ，担当者，管理者の 3 種類になる．

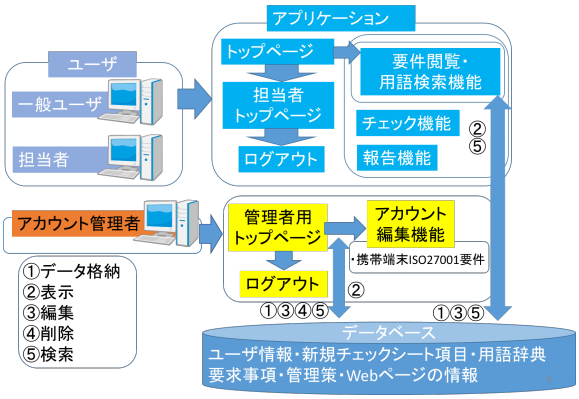


図 1 システム概要図

基本的な動きとしては，企業の情報セキュリティ部門の人が，管理者として管理者用ページで各部署数人へチェック項目の振り分けをする．そして，項目を振り分けられた人が担当者として担当者用ページでチェック判定を行い，その判定結果から改善項目，管理策と表示された後に報告書のページへと移動する．最後に報告書を管理者へ送ることで企業の情報セキュリティ対策の現状を知ることができる．また，報告書ではチェックシートの入力情報から企業の情報セキュリティについての現状を判定し，判定結果に対応した Web ページの URL と本文をアドバイスとして表示している．

4．本研究のシステム設計

本研究で構築するシステムについての説明する．本研究では，先行研究[2]のシステムに新たに責任者による再確認機能，過去データとの比較機能，ログイン履歴機能，掲示板の 4 機能を追加し，社員間での利用と，経営者による社内の情報セキュリティを確認できるシステムの構築を行った．

本システムの遷移図を図 2 に示す．

千葉工業大学　社会システム科学部　経営情報科学科
2019 年度卒業研究概要

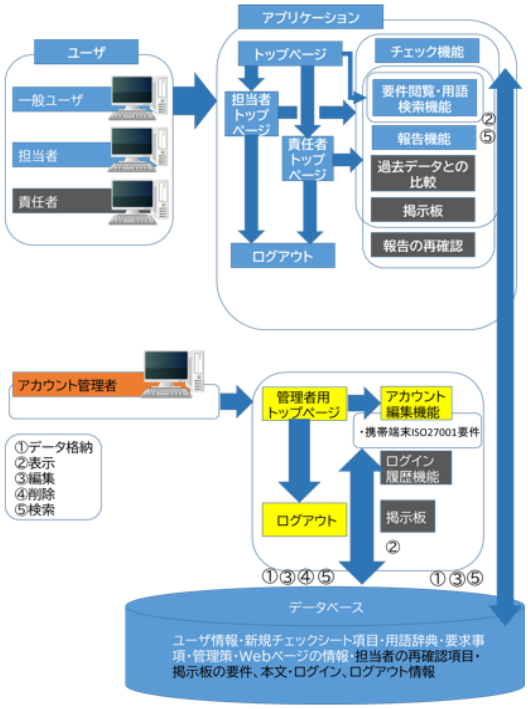
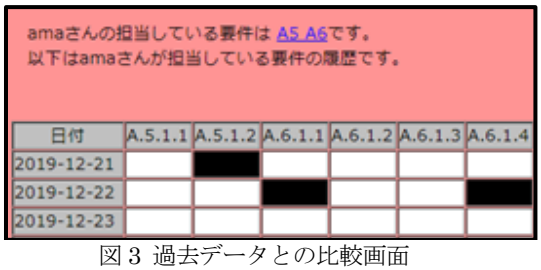


図 2 本研究のシステム遷移図

はじめに責任者の追加について説明する．本研究では，一般ユーザ，担当者，管理者の他に新たに経営者に見立てた責任者を追加した．責任者を追加した理由は，先行研究[2]ではチェックシートの利用ユーザが担当者のみであり，経営者には自社の情報セキュリティ対策の進捗の確認，および何処に不備があるかが確認できずにいた．企業が情報セキュリティ管理を怠ることで経営者が法的・道義的責任を問われることがあるため，担当者に自社の情報セキュリティ対策を任せるのではなく，経営者が自社の情報セキュリティ対策を把握し，自ら実行していくために，利用ユーザに責任者を追加した．

次に，過去データとの比較機能について説明する．先行研究では新しいチェック項目を入力した場合，過去のデータを上書きしており，直前のデータ以外は保存できていない．そのため，いつにどのように対策して改善を行ったのかが分からない仕組みだった．そこで，チェックシートの項目を判定した際にデータとチェック日とコメントを確認できるように追加した．これにより，図 3 のように自社の情報セキュリティ対策がどのように改善されたかが分かりやすくなる．

次に，ログイン履歴機能について説明する．本機能は管理者に利用者のログイン情報が確認できるようになっている．本機能で誰が頻繁にログインしているか，不適切なログインをしているか等が分かる．


amaさんの担当している要件は A5 A6です。
以下はamaさんが担当している要件の履歴です。

日付	A.5.1.1	A.5.1.2	A.6.1.1	A.6.1.2	A.6.1.3	A.6.1.4
2019-12-21						
2019-12-22						
2019-12-23						

図 3 過去データとの比較画面

最後に，掲示板について説明する．本機能は ISO27000 シリーズの更新により，データベースに変更があった際に，社員に知らせることを目的とする．また，責任者，担当者間でチェック項目の確認が完了した際に，連絡を取り合える意味もある．掲示板の投稿機能は担当者，責任者，管理者に追加しており，削除機能は悪用を防ぐために管理者のみに実装した．

5. 結　言

本研究で新たに経営者を見立てた責任者を追加したことにより，社内全体で情報セキュリティ対策を行うことを可能とした．そして，掲示板と過去データとの比較機能を利用して担当者と責任者で連携を取り合うことにより，経営者が社内の情報セキュリティ対策を自ら確認し，自ら実行していくことを可能とした．

しかし，本システムには幾つか問題点が存在する．1 つ目は，責任者(経営者)にとって ISO27000 シリーズの要求事項は IT の専門用語が多く，意味が理解しづらい．そのため，管理策を見直し，更に簡略化することでより確実な再確認ができると考える．2 つ目は，構築したシステムは IPA の「中小企業の情報セキュリティ対策ガイドライン」の内容を基に改良を行ったため，実在の企業の意見がない．そのため，実際に企業の社員から利用した感想により，更なる改善が見込めると考える．

文　献

[1] IPA 情報処理推進機構：企業の CISO や CSIRT に関する実態調査 2017 –調査報告書-(2017 年 4 月 13 日公開) https://www.ipa.go.jp/files/000058850.pdf
[2]大木秀人：機械学習を導入した情報セキュリティ管理支援アプリケーションの構築，千葉工業大学社会システム科学部経営情報科学科 2018 年度卒業研究(2019)
[3]中丸裕二郎：携帯端末を考慮した企業情報セキュリティ管理支援アプリケーションの構築，千葉工業大学 社会システム科学部経営情報科学科 2013 年度卒業研究(2014)
[4]千葉俊輔：企業情報セキュリティ管理システムの改良～知識ベースの導入～，千葉工業大学社会システム科学部経営情報科学科 2015 年度卒業研究(2016)