2W-07

セキュリティインシデント事例から見た必要なスキルセットに関する考察

内藤　美保†　　角田　裕太‡　　八代　哲‡　　細谷　竜平‡　　齋藤　孝道†

明治大学†　　明治大学大学院‡

1　はじめに

従業員が仕事を遂行するために必要なスキルを洗い出し，従業員一人ひとりの持っているスキルを一覧にしたスキルマップがある．これは業務の効率化や計画的な人材育成を図るために活用される．セキュリティ分野では JNSA が作成したセキュリティ知識分野（SecBoK）人材スキルマップ（以降，SecBoK と呼ぶ）[1] などがある．他方，本論文では，国内で発生したセキュリティインシデント（以降，インシデントと呼ぶ）を調査した．過去 14 年間のメディアでのインシデントの報告を調べた結果，個人情報の流出による被害が 756 件報告されており，そのうち約 57.6%は人的ミスが原因であった．セキュリティ対策に必要なスキルセットを特定すべく，インシデントの事例と Secbok との紐付けを行った．その結果，人的ミスに対処するためのスキルとして，「ITSS レベル 2 程度の基礎的な IT リテラシー」及び「新たに出現したセキュリティ問題，リスク及び脆弱性に関する知識」が該当することが確認された．

2　SecBoK

SecBoK[1] とは，情報セキュリティ人材としての役割を CISO やフォレンジックエンジニアなど 16 項目に分類し，それぞれに対して必要とされている能力をまとめたスキルマップである．SecBoK を利用することにより，人材の育成に必要なスキルを明確にしたり，情報処理技術者試験等の試験と結びつけてスキルを分類したりできるメリットがある．

3　インシデントの分析

本論文では，2004 年 8 月～2017 年 11 月に報道されたインシデント 3,532 件を Web サイトから収集し分析した．参照サイトは，IPA が出しているサイバー攻撃被害一覧 [2]，iid,inc. が運営する ScanNetSecurity[3]，ニュースガイア株式会社が運営する Security NEXT[4]，株式会社シーズクリエイトが運営するサイバーセキュリティ.com[5]，株式会社日経 BP が運営する ITpro[6]，アイティメディア株式会社が運営する ITmedia[7]，piyolog[8]，JP ドメイン Web 改竄情報 [9]，フィッシング対策協議会 [10] などである．本論文では特に「企業規模別の被害件数」及び「年別のインシデントの発生原因」の 2 つの観点からインシデントの分析を行い，その結果を示す．その他の結果に関しては，我々が運営している Web サイト [11] に掲載予定（執筆時）である．

3.1　企業規模別の被害件数

図 1 に企業規模別の被害件数を分析した結果を示す．本論文では，企業規模を計る指標として従業員数を用いる．図 1 から, 大企業のみならず，中小企業においてもインシデントが一定数発生することが推察される．

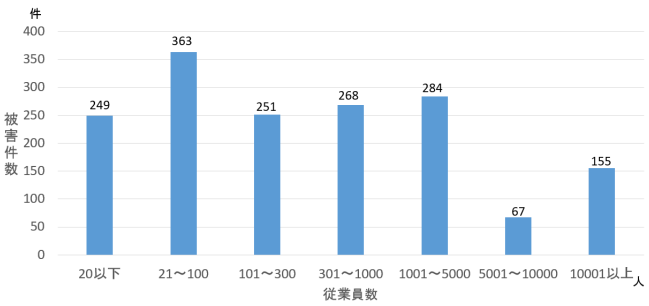

図 1: 企業規模別の被害件数

3.2　年別のインシデントの発生原因

図 2 に年別のインシデントの発生原因の上位 5 位を示す．不正アクセスによりインシデントが発生した事例に関しては，不正アクセスの具体的な手法がわからないので，分析の対象外としている．被害件数のうち，2016 年では 67.9%，2017 年では 57.5%が USB の紛失やメールの誤送信などの人的ミスが原因で発生したものであり，半数を超える企業が内的要因で被害を受けていることがわかる．したがって，FW 導入などの高度な対策だけでなく，社内教育などの基本的な対策も効果的と言える．

3.3　インシデント報告対応レポートとの比較

本節では JPCERT/CC のインシデント報告対応レポート [12] と，インシデントの事例調査の結果との比較を行う．JPCERT/CC のインシデント報告対応レポートによると，JPCERT/CC へのインシデント報告件数は 2013 年度から 2016 年度まで減少傾向にあるが，今回の調査での被害件数は図 2 のように 2013 年から 2016 年まで

Consideration on required skill set based on Security Incidents
†Miho NAITO　‡Yuta TSUNODA　‡Satoshi YASHIRO
‡Ryohei HOSOYA　†Takamichi SAITO
†Meiji University
‡Graduate School of Meiji University

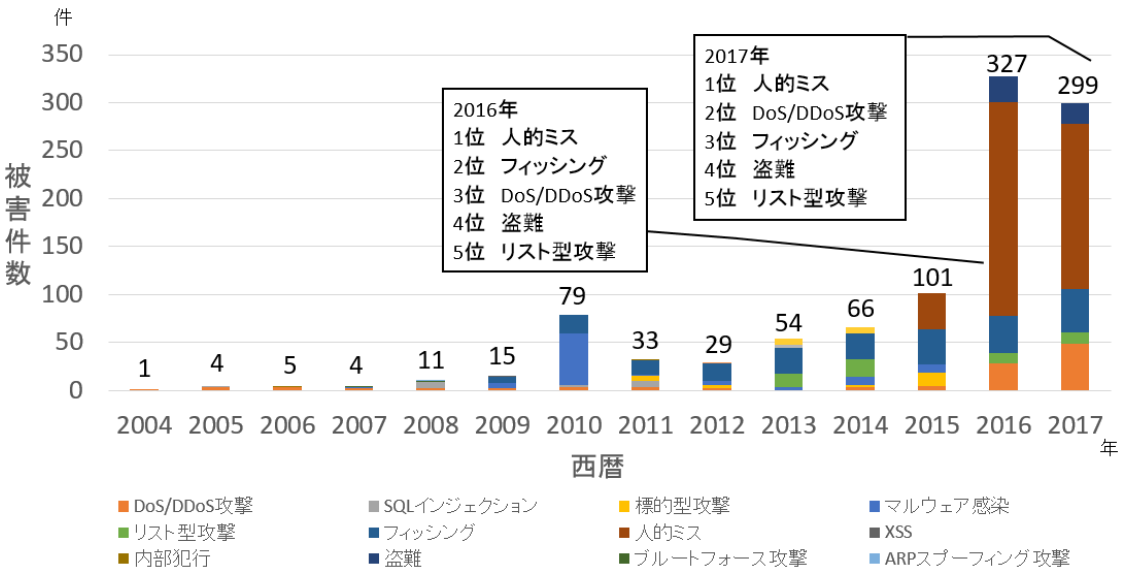

図 2: 年別の国内インシデント発生原因

増加傾向にある．これは，サイバーセキュリティに注目が集まり，報道が増えたことが原因として考えられる．

4 セキュリティ対策に必要なスキルセット

本章では調査したインシデントの事例と SecBok の紐づけを行う．3.2 節よりインシデントの発生原因は人的ミスなどの内的要因が半数を超えていることがわかっている．よって，現状のインシデントへの対策としては，セキュリティにおける高度な専門的スキルより，一般的な IT リテラシーが必要であると考えられる．たとえば，2016 年 1 月に起こった東京電力株式会社の事件では，USB の紛失という人的ミスから約 81 万軒の個人情報の紛失に繋がった．当事者には USB の紛失による被害インパクトが予見できなかった可能性もある．すなわち，人的ミスを防ぐために人的ミスによる企業などへのリスクを理解する必要があると考えられる．人的ミスへの対策に必要なスキルと SecBok との対応を見ると，基礎分野の ICT 基礎（大項目）の「ITSS レベル 2 程度の基礎的な IT リテラシー」やセキュリティ基礎分野の総論（大項目）の「新たに出現したセキュリティ問題，リスク及び脆弱性に関する知識」が該当した．「ITSS レベル 2」は，情報処理技術者試験の基礎試験に合格する程度のスキルを有しているということである．よって，これらの知識の理解とその水準を保つことが，人的ミスのリスクの理解に繋がり，現状のインシデントへの対策になると期待できる．

5 まとめ

本論文では，報道をもとに国内で発生したインシデントを収集し，「企業規模別の被害件数」及び「年別のインシデントの発生原因」の 2 つの観点から分析を行った．また，セキュリティ対策に必要なスキルを明確にするためにインシデントの事例と SecBoK の紐づけを行った．調査の結果，インシデントの被害件数は一部の例外を除き，企業規模による大きな偏りはないことがわかった．また，2016 年及び 2017 年に発生したインシデントの事例のうち，半数以上が人的ミスなどの内的要因により発生していることがわかった．人的ミスへの対策に必要なスキルについて SecBok との紐付けを行った結果から，実務などの経験から得られる高度な専門的スキルだけでなく，社内教育などで得ることができる IT リテラシーもインシデント対策に有効だと言える．

参考文献

[1] http://www.jnsa.org/result/2017/skillmap/
[2] https://www.ipa.go.jp/files/000056149.xlsx
[3] https://scan.netsecurity.ne.jp/
[4] http://www.security-next.com/
[5] https://cybersecurity-jp.com/news
[6] http://itpro.nikkeibp.co.jp/
[7] http://www.itmedia.co.jp/
[8] http://d.hatena.ne.jp/Kango/
[9] http://izumino.jp/Security/def_jp.html
[10] https://www.antiphishing.jp/
[11] https://www.saitolab.org/ipsj80/incident_report.html
[12] https://www.jpcert.or.jp/pr/2017/IR_Report20170413.pdf