一般口演
# 一般口演4
# 情報セキュリティとプライバシー・ネットワーク
2018年11月23日(金) 10:15 〜 11:45 H会場 (福岡サンパレスHパレスホール)

[2-H-1-4] 医療機関におけるセキュリティインシデントの事例調査
○今井 哲郎[1], 豊増 佳子[1], 川口 孝泰[1], 布広 永示[2] （1.東京情報大学 看護学部 遠隔看護実践研究センター, 2.東京情報大学 総合情報学部）

医療機関におけるセキュリティインシデントの事例分析についてはこれまでに，アメリカ保健福祉省の Webサイトにリスト化されている事故事例を収集し，発生要因別に分類した報告がある．日本においても調査報告があるが，これらの研究の多くは，報道機関からの情報や医療機関が自ら公表した情報に基づくものであった．そのため公表された情報は，実際に発生しているセキュリティインシデントに対する氷山の一角である可能性がある．本研究では，日本の医療機関におけるセキュリティインシデントの真の実態を明らかにすることを目的として， Web上の調査と併せて特定機能病院に対するアンケート調査を実施し，これらの各事例を分析した．その結果 Web情報調査では，3つのサイトから2005年〜2017年に発生した100件のインシデントが抽出された．全般に紛失などの人的要因によるインシデントが多いこと，また大学系・公共系・民間の病院の各カテゴリでインシデントの発生要因比率には差があることなどが確認された．例えば，システム化が発展している大学系病院ではシステム的要因の割合が多く，民間病院では盗難等の外的要因の発生割合が多かった．特定機能病院へのアンケート調査では，回答が得られたのは84機関（85病院）のうち12機関（約14.3%）に留まった．各病院のセキュリティインシデントの共有化に対する意識の低さがアンケートの回答率として表れることとなった．「セキュリティインシデントに遭遇した経験がある」と回答したのは8つの機関であり，要因としては置き忘れ・紛失などの人的要因によるものが多いが，ランサムウェア等のウィルス感染・ホームページサーバへの DDOS攻撃等の不正アクセス事例の報告も確認された．今後はさらに調査を継続して行うことによって，より明確な実態調査と経時的観測を図る予定である．

©一般社団法人 日本医療情報学会

医療機関におけるセキュリティインシデントの事例調査

今井哲郎[*1], 豊増佳子[*1], 川口孝泰[*1], 布広永示[*2]
*1 東京情報大学 看護学部 遠隔看護実践研究センター, *2 東京情報大学 総合情報学部

A Case Study of Security Incidents in Medical Institutions

Tetsuo Imai[*1], Keiko Toyomasu[*1], Takayasu Kawaguchi[*1], Eiji Nunohiro[*2]
*1 Telenursing Research Center, Faculty of Nursing, Tokyo University of Information Sciences,
*2 Faculty of Informatics, Tokyo University of Information Sciences

Regarding case analyses of security incidents in medical institutions, there is a report that incident cases listed on the website of the U.S. Department of Health and Human Services were classified by occurrence factors. There are already some reports about security incidents in Japan, although they are based on newspaper reports or press releases from medical institutions themselves. Published information may be only the tip of the iceberg of actual security incidents. In order to clarify the true state of security incidents in medical institutions in Japan, this study conducted questionnaire surveys in advanced-treatment hospitals along with web surveys, and categorized cases by occurrence factors. In the web survey, 99 incidents that occurred from 2005 to 2017 in three sites were extracted and analyzed. It was confirmed that many incidents are generally human-related, and that incident occurrence factor ratios are different between university-affiliated, public, and private hospitals. For example, university-affiliated hospitals, which are highly systematized, have a high proportion of factors related to electronic systems, while private hospitals have a high proportion of external factors such as theft. Although the questionnaire was administered at 85 advanced treatment hospitals, responses were obtained from only 12 organizations (about 14.3%) out of 84 organizations (85 hospitals). The low answer rate seems to be due to low consciousness in communicating security incidences, in addition to preserving the confidentiality of medical information. Eight organizations answered that they have already experienced security incidents and that many incidents are caused by human factors, such as misplacement or loss. Reports of cases of unauthorized access, such as Ransomware virus infection and DDOS attack to the website server, were also confirmed. In the future, we plan to conduct additional surveys to clarify more real situations and observations over time.

Keywords: security incidents, medical institutions, Web survey, personal health information, case study

1. はじめに

アメリカの医療機関におけるセキュリティインシデントについては，これまでにアメリカ合衆国保健福祉省のウェブサイトにリスト化されている 2013 年 1 月～2015 年 12 月の 3 年間に報告された医療機関や医師などの「医療提供者(Healthcare Provider)」による事故事例を収集し，タイプ別に分類した報告がある [1]. アメリカの医療機関では，2009 年の「経済的および臨床的健全性のための医療情報技術に関する法律(Health Information Technology for Economic and Clinical Health Act; HITECH 法)」によって，保険福祉省に対する報告義務を強化している [2]. そのため，報告されたセキュリティインシデントは相当程度の妥当性があると考えて良い.

日本においても，医療機関におけるセキュリティインシデントについて調査した報告がある. しかしながらこれらの研究の多くは，報道機関からの情報 [3-6]や医療機関が自ら公表した情報 [7]に基づくものであった. 日本においては，個人情報保護法違反に対する罰則はあるものの，具体的なルールや事故発生の際の報告や公表等についてはガイドラインの規定に委ねられるのみであり，アメリカと比較するとその法的強制力は低い [2]. そのため公表された情報は，実際に発生しているセキュリティインシデントに対する氷山の一角である可能性がある.

そこで本研究では，日本の医療機関におけるセキュリティインシデントの真の実態を明らかにすることを目的とし，Web 上の調査と併せて，特定機能病院に対するアンケートを実施した.

2. 方法

2.1 インシデントタイプと要因

本研究では品川・橋本 [7]の報告に基づき，セキュリティインシデントを 14 のタイプに分類した. さらにそれらを人的要因，システム的要因，外的要因の 3 つの要因に分類した. それらの分類を表 1 の左側に示す.

2.2 Web 情報に基づく調査

本研究の第一の調査として，セキュリティインシデントに関する Web 上の情報を検索によって収集した. 検索に用いた主なサイトは，以下の 3 つである.

- Security NEXT : http://www.security-next.com/
- Medtec Japan Online : http://www.medtecjapan.com/
- ITmedia : http://www.itmedia.co.jp/

2.3 特定機能病院へのアンケート調査

第二の調査として，日本全国の特定機能病院に対するアンケート調査を実施し，各医療機関がこれまでに遭遇したセキュリティインシデントについて情報を収集した. アンケート調査に用いた調査票を付録に示す. 調査期間は 2018 年 2 月 9 日～2 月 28 日とした. ただし，3 月半ばまで追加回答を受け付けた.

3. 結果

3.1 Web 情報に基づく調査

調査の結果，日本国内で発生した医療分野におけるセキ

ュリティインシデントのうち，2005 年から 2017 年に発生した 99 件のインシデントが抽出された．これらのインシデントについて，発生場所に関する 3 つのカテゴリ「大学附属病院」「公立・公的病院」「民間病院」についてその特徴の違いを評価し，次のような特徴が確認された．

- 大学附属病院では，システム的要因の発生割合，特にマルウェア感染の割合が多い．これは，公立・公的病院や民間病院と比較してシステム化による外部接続が進んでいることが影響していると考えられる．
- 公立・公的病院では，人的要因の発生割合，特に資料やUSBメモリなどの紛失の割合が多い．ここではシステム化は進んでいるが，情報管理は人手による移動が可能な USB メモリなどの記憶媒体が中心であると見られる．
- 民間病院では，外的要因の発生割合，特に盗難の割合が多い．ここでは，大学附属病院や公立・公的病院と比較してセキュリティ対策が遅れていると見られる．
- 大学附属病院，公立・公的病院共に，記録媒体の紛失などの人的要因の割合が多い．ここでは情報管理への意識が不足しているものと見られる．

3.2 特定機能病院へのアンケート調査

特定機能病院へのアンケートは，84 機関(85 病院)のうち回答期間中に 11 機関，追加回答受付期間中に 1 機関，合計 12 機関から回答が得られた．回答率は約 14.3%であった．アンケート調査に対する回答率が低い値に留まったことは，医療情報の守秘性に加え，各病院のセキュリティインシデントの共有化に対する意識の低さを表していると考えられる．回答が得られた 12 機関のうち「セキュリティインシデントに遭遇した経験がある」と回答したのは，9 つの機関(75.0%)であった[a]．これらから，合計 28 件のインシデント事例が報告された．表 1 右側に，各発生インシデントのタイプ別報告数を示す．

3.3 調査結果の比較

今回の両調査の結果および 2014 年に公表された品川・橋本による Web 情報を基にした調査 [5]による結果をまとめたものが図 1 である．図 1(a)は，各発生インシデントのタイプ別構成比率を，図 1(b)では各発生インシデントの要因別構成比率を示す．品川・橋本の 2014 年の調査は，2002 年から 2013 年までのセキュリティインシデントの事例を Web 上の情報に基づいて調査・集計したものである．図 1 は，本研究で用いるタイプと要因に合わせて再整理して結果を示した．

4. 考察

図 1(b)に示すインシデント要因の構成比率に関しては，いずれの調査においても，人的要因が最も多く 60%前後，システム的要因が 10%前後，残りが外的要因となっている．一方で，アンケート調査においては他の調査と比べて人的要因の比率が大きく，逆に外的要因の比率が小さくなっている．これは，調査方法による違いに起因している可能性がある．すなわち，前述の通り日本では事故発生の際の公表に関する法的拘束力が弱く，品川・橋本の調査や Web 調査による事例は，医療機関が自ら公表した報告が基になっている．外的要因によるインシデントよりも，主に組織内部の人間に起因するものが多い人的要因によるインシデントは「公表しづらい」事例であり，自発的な報告がされにくい環境があると考えられる．そのために，品川・橋本の調査や本研究の Web 調査では，アンケート調査による事例よりも人的要因によるインシデントが少なく報告された可能性がある．このことは，セキュリティインシデントの実態を明らかにするためには，本研究のような調査を全医療機関規模で実施し，再発防止に向けた分析の必要性を示唆するものである．

図 1(a)に示すインシデントタイプの構成比率に関しても，いずれの調査も全体的な傾向に大きな差はなかった．異なる点として注目すべきは，今回の両調査において，2014 年の品川・橋本の調査においては報告されていなかった不正アクセス(クラッキング・ハッキング)がある程度の割合で報告されている点である[b]．このことは，セキュリティの脅威としてクラッキング・ハッキングによる不正アクセスという手法が近年になって新たに顕在化してきたことを示唆している．

4. おわりに

本研究は，日本の医療機関におけるセキュリティインシデントの真の実態を明らかにすることを目的として，Web 上の調査と併せて特定機能病院に対するアンケートを実施し，これらの各事例を既存研究に基づきタイプと要因について分類した．今回の調査結果では，全般に人的要因によるインシデントが多いこと，また大学附属病院・公立・公的病院・民間病院の各カテゴリごとにインシデントの要因比率には差があることなどが確認された．またアンケート調査では，9 つの機関から 28 件のインシデントが報告された．アンケート調査結果では，他の調査結果と比べ外的要因の比率が低く，人的要因の比率が高かった．これは，医療機関による自主的公表に基づく調査においては人的要因による事例が比較的少なく報告されやすいことが一因として考えられる．

Web 調査における発生場所のカテゴリに関する結果の違いは，各医療機関における情報管理のシステム化状況が影響していると考えられる．システム化状況は年々変化していくものであるから，今後調査件数を増やしインシデント発生状況の時系列変化を調査していくことが必要である．また併せて海外の状況についても調査を進め，比較することが必要である．また今回のアンケート調査の限界として，回答率が約 14.3%と低く，セキュリティインシデントの発生実態をどの程度反映しているかについて，十分な妥当性が確保されていないことが挙げられる．今後アンケート調査を継続するにあたり，本研究で得られた結果を対象医療機関に送付し，セキュリティインシデントの共有化に対する意識を高める働きかけを行うなど，回答率向上の取り組みを行う予定である．またアンケート調査についても Web 調査と同様，継続調査による時系列変化の調査が重要である．

倫理的配慮について

本研究は，東京情報大学「人を対象とする実験・調査等に関する倫理委員会」の承認を受けたものである．

謝辞

本研究は JSPS 科研費 16H02693 の助成を受けたものであ

[a] 正確には「セキュリティインシデントに遭遇した経験がある」と回答したのは 8 機関であったが，「セキュリティインシデントに遭遇した経験がない」と回答しながら事例について報告をしている機関が 1 機関あった．

[b] ただし，2014 年の調査の時点において品川・橋本はクラッキング・ハッキングによる不正アクセスをインシデントのタイプとして分類しておらず，原因不明・その他として分類されている可能性がある．

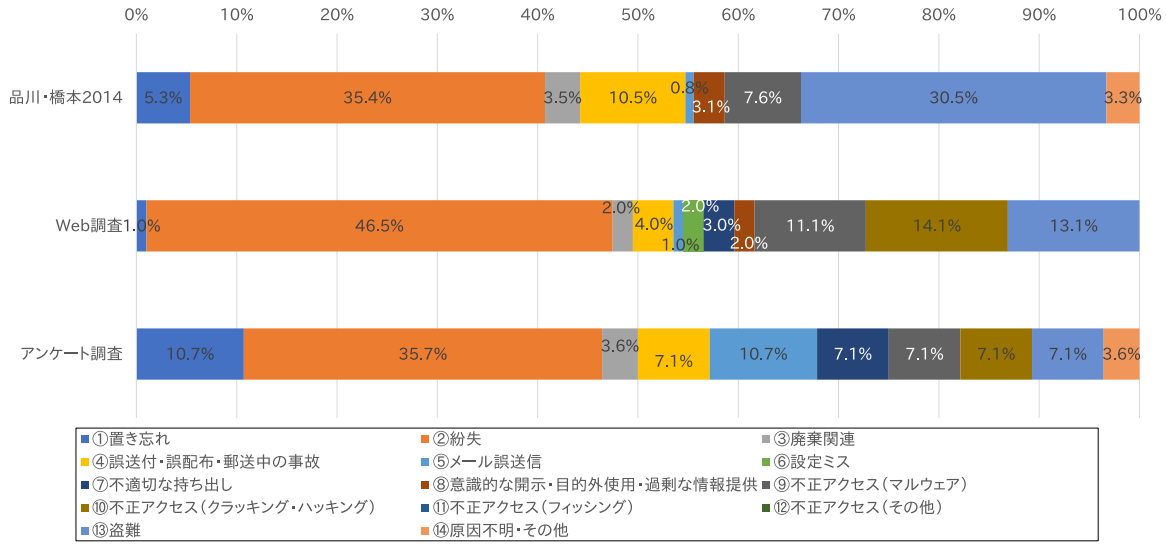
る.

参考文献

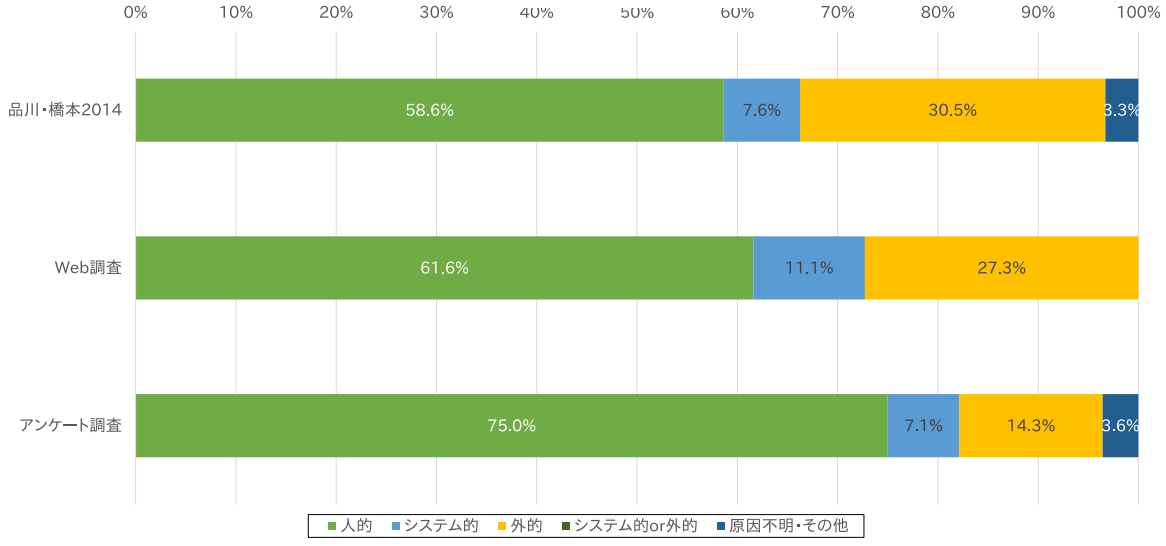
1) 品川佳満, 橋本勇人. アメリカで発生した医療提供者による個人情報に関する事故原因の図式化. 川崎医療福祉学会誌 2017；28,6：264-272.
2) 湯淺墾道. アメリカにおける個人データ漏洩通知法制. 日本セキュリティ・マネジメント学会誌 2012；26,2：24-34.
3) 相澤直行. 個人情報の事故事例から見た医療情報の安全管理. 新医療 2008；35,6：121-124.
4) 品川佳満, 橋本勇人. 医療機関における患者の個人情報に関する事故の現状－電子媒体が関係したケースの分析－. 医療情報学 2013；33,6：311-319.
5) 品川佳満, 橋本勇人. 医療機関における患者情報の取り扱い事故に関する経年変化－個人情報保護法制定後 10 年間の分析－. 川崎医療福祉学会誌 2014；24,1：103-109.
6) 品川佳満, 橋本勇人. 患者の個人情報取扱い事故のパターンと違反したルールに関する分析. 川崎医療福祉学会誌 2015；24,2：221-227.
7) 相澤直行. 医療情報の利活用と公認医療情報システム監査人. 新医療 2012；39,8：109-111.

表 1　アンケート調査におけるセキュリティインシデント報告事例

インシデント種別	要因分類	件数	報告率
①置き忘れ	人的	3	25.0%
②紛失	人的	10	83.3%
③廃棄関連	人的	1	8.3%
④誤送付・誤配布・郵送中の事故	人的	2	16.7%
⑤メール誤送信	人的	3	25.0%
⑥設定ミス	人的	0	0.0%
⑦不適切な持ち出し	人的	2	16.7%
⑧意識的な開示・目的外使用・過剰な情報提供	人的	0	0.0%
⑨不正アクセス（マルウェア）	システム的	2	16.7%
⑩不正アクセス（クラッキング・ハッキング）	外的	2	16.7%
⑪不正アクセス（フィッシング）	外的	0	0.0%
⑫不正アクセス（その他）	システム的or外的	0	0.0%
⑬盗難	外的	2	16.7%
⑭原因不明・その他	−	1	8.3%



(a) タイプの内訳



(b) 要因の内訳

図 1 セキュリティインシデントタイプおよび要因の内訳

付録

「医療分野における情報セキュリティインシデントの潜在的な問題抽出と防衛策」に関する調査

以下のアンケート項目について、ご回答をお願いいたします。（ご回答が難しい項目は無記入のままで結構です）

Ⅰ. 貴施設の情報とセキュリティ体制について

Q1. 情報セキュリティ対策を行っている専従職員の方はいますか。

1. 専従職員がいる
　　人
2. 専従職員はいない

Q2. 情報セキュリティインシデントに対する対策委員会や対策会議は、組織上に位置づいていますか。

1. 位置づいている
2. 位置づいていない

Q3. セキュリティインシデントに遭遇した際の報告・連絡等の対処マニュアルはありますか。

1. ある
2. ない

Q4. 情報セキュリティの教育や研修等を行っていますか。

1. 行っている→教育や研修等の内容をお教えください。（対象者、頻度、内容など）
2. 行っていない

Q5. 貴施設では、これまでに情報セキュリティインシデントに遭遇したことがありますか。

1. ある
2. ない→アンケートは終了です。ありがとうございました。

Ⅱ. 貴施設で起こった個人情報に関するインシデント事例について

Q6. 発生したインシデントの種類について

「有」の場合、発生したインシデント事例の情報を別シート①～⑭にご記入ください。

①置き忘れ
②紛失
③廃棄関連
④誤送付・誤配布・郵送中の事故
⑤メール誤送信
⑥設定ミス
⑦不適切な持ち出し
⑧意識的な開示・目的外使用・過剰な情報提供
⑨不正アクセス（マルウェア）
⑩不正アクセス（クラッキング・ハッキング）
⑪不正アクセス（フィッシング）
⑫不正アクセス（その他）
⑬盗難
⑭原因不明・その他

アンケートは終了です。ありがとうございました。

〔不正アクセス(⑨～⑫)以外〕

Q7 発生したインシデントの主な事例を下記にご記入ください。

1. インシデント名をご記入ください。
2. 発見の経緯や対応について概要をご記入ください。
3. インシデントの発生した日付をご記入ください。
　　西暦　年　月　日
4. インシデントの発生場所をご記入ください。
5. 影響を受けた個人情報の数をご記入ください。
　　人分

〔不正アクセス(⑨～⑫)〕

Q7 発生したインシデントの主な事例を下記にご記入ください。

1. インシデント名をご記入ください。
2. 発見の経緯や対応について概要をご記入ください。

3. インシデントの発生した日付をご記入ください。
　西暦　年　月　日
4. インシデントの発生場所をご記入ください。
5. 影響を受けた個人情報の数をご記入ください。
　人分
6. 不正アクセスの「被害者の概要」をご記入ください。
7. 不正アクセスの「加害者の概要」をご記入ください。
8. 被害を受けたシステムの構成をご記入ください。（機器・OS・アプリなど）
9. 被害を受けたシステムの形態はどれになりますか。
　1. 院内に閉じたシステム　2. 院内外でネットワーク接続されているシステム
10. 被害の内容について
　1. システム（医療機器を含む）ダウン　2. 個人情報流出　3. その他
11. サイバー攻撃（不正アクセス）の種類について
　1. Dos 攻撃／DDoS 攻撃　2. SQL インジェクション　3. クロスサイトスクリプティング　4. バッファオーバーフロー（BOF）攻撃　5. OS インジェクション　6. その他
12. マルウェアの種類について
　1. ワーム　2. トロイの木馬　3. バックドア　4. ランサムウェア　5. その他