大学での個人情報漏えいに関する包括的セキュリティリスク算定の検討

石坂 徹

室蘭工業大学 情報メディア教育センター

ishizaka@mmm.muroran-it.ac.jp

概要：大学における ICT 活用が促進される中、情報セキュリティ対策の重要性は高まっている。さらに近年業務システムのクラウド化や仮想化によりセキュリティ対策自体の内容も変化している。しかしながら大学全体としてのセキュリティ対策費用が適切かどうかを判断するのは難しい。本研究では、保有している個人情報漏えい発生を想定したときの賠償額をリスク値とみなし、組織におけるリスク値を包括的に算出する方法を検討する。

1 はじめに

IT の活用機会が多くなっている今、各組織における情報セキュリティ対策の重要性はさらに高くなっている。大学を含む教育機関においても、学生の個人情報漏えいをはじめとした様々なセキュリティインシデントがたびたび発生している。セキュリティインシデントの低減のためには、組織における情報セキュリティ対策が必要不可欠である。2009 年の文部科学省の調査[1]によると、ほとんどの大学でコンピュータ・ネットワークに対する技術的な対策または情報セキュリティポリシーの策定・施行など運用対策のいずれかの対策を行っていることが示されている。

また、総務省の調査[2]では業種別にセキュリティ対策費用の統計が取られている。この調査における「教育（国・公立除く）、学習支援業」の業種では、資本金 10 億円超 100 億円以下の規模の組織で 600 万円以上の対策費を講じているところはなかった。これは全業種の統計と比較して低いとおもわれるが、教育関連の業種は他の業種と比べて個人情報の量が少ないわけではなく、成績などセンシティブな情報を扱うことが多いため、むしろセキュリティ対策を重視すべきと考える。しかしながら、組織全体を見渡したとき、適切な予算措置、人的リソース配分などが効果的に行われているかどうかを判断するのは難しい。中村らは情報システムに対するセキュリティ対策の選定を離散最適化問題に帰着させることで効率化を図る手法を提案している[3]。西垣らは情報システムのセキュリティ対策の選定方式として、インシデント発生時の賠償リスクを考慮した手法を提案している[4]。これら手法ではそれぞれのシステムの保有情報や脆弱性などの詳細な情報を用いている。またしかし、大学全体を考えた場合、一般的にガバナンスが企業と異なることや利用形態、保有情報の正確な把握が困難などの理由により、すべてのシステムに対して厳密なリスクアセスメントを行うことは困難である。また、日本ネットワークセキュリティ協会（JNSA）によると情報漏えいの

原因の多くは管理ミスと誤操作などのヒューマンエラーであることが報告されている[5]。

本研究ではリスクを管理ミスやヒューマンエラーを原因とするものを含む個人情報漏えい事件に限定して、組織全体のリスク値を包括的に算出する方法を提案する。この手法は組織で保有している情報システム内の個人情報漏えい発生を想定したときの賠償額をリスク値とみなすことにより、組織全体でのセキュリティ対策のための定量化された指標とすることを目的とする。

2 個人情報漏えい事故の想定損害賠償額によるリスク評価

2.1 想定損害賠償額の算出法

個人情報漏えい事故発生時の想定損害賠償額（以下、賠償額）の算定方法としては、JNSA が提唱している JO モデル（JNSA Damage Operation Model for Individual Information Leak）[6]がある。この手法は JNSA により日本の企業 1000 社に対して行ったアンケート調査、株価の影響、実被害額に基づいてモデル化を行っていることから、実情に即したモデルであると考えられる。この手法における 1 件あたりの賠償額は、以下の算出式により与えられる。

$$\begin{aligned} \text{賠償額} = & \text{基礎情報価値}[500(\text{円})] \\ & \times \text{機微情報度}[\text{Max}(10^{x-1} + 5^{y-1})] \\ & \times \text{本人特定容易度}[1,3,6] \\ & \times \text{社会的責任度}[1,2] \times \text{事後対応評価}[1,2] \end{aligned} \quad (1)$$

ここで、基礎情報価値は情報の内容に依存しない固定値(500)である。機微情報度は情報の内容によって、精神的苦痛レベル(x)と経済的損失レベル(y)に対して、図 1 の Simple-EP(Economic-Privacy)図により求められる。このほかのパラメータは以下の基準により設定される。

経済的損失レベル(y)	3	口座番号+暗号番号、クレジットカード+暗証番号など	遺言書	前科、前歴、ブラックリストなど
	2	パスポート情報、購入既読、アカウント+パスワード、口座番号のみ、など	年収、資産、所得、借金など	
	1	氏名、住所、メールアドレス、身長体重など	健康診断、病歴、国籍、人種、学歴、成績など	加盟政党、信条、思想、宗教、身体障害、知的障害、性癖など
		1	2	3

精神的苦痛レベル(x)

図1: Simple-EP図

- 本人特定容易度：
漏えいした情報から本人特定のし易さを表す。氏名および住所など、複数の情報の組み合わせで簡単に本人特定ができるものは6、情報に対してコストをかけると本人特定ができるものは3、本人特定ができないものは1である。
- 社会的責任度：
医療、金融など「個人情報の保護に関する基本方針(平成16年4月2日閣議決定)」に「適正な取り扱いを確保すべき個別分野」として挙げられている機関および公的機関は2、それ以外は1である。
- 事後対応評価：
情報漏えいの事案に対して適切な対応をした場合は1、不適切な対応をした場合は2である。なお、対応の内容が不明の場合は、不適切な対応が露見しなかったと考え1とする。

2.2 JOモデルのシステムへの応用

JOモデルによる個人情報漏えい事故の賠償額の算出方法は、事後対応評価のパラメータからわかるように、実際に個人情報漏えい事故が起きた場合の対象の個人への賠償額を算出するものである。本研究では事故において、個々の情報システム内のすべての個人情報が漏えいすること想定する。JOモデルを用いることにより、情報システム内の個人情報の価値を算出し、さらに、件数、従事者、漏えい事故の発生確率を用いた値を対象システムのリスク値とみなすことを試みる。対象システムとして、大学で運用しているAデータベースでのリスク値の計算例を示す(表1)。このシステムは利用者自身で個人の情報を入力し、そのうちいくつかの情報を外部へWebシステムとして公開するシステムである。格納されている情

表1: Aデータベースに対するJOモデルの適用とリスク値算出

機微情報度		本人特定容易度	社会的責任度	事後対応評価	賠償費/件 (C_i) 千円	件数 (I_i)	従事者数 (N_i)	総賠償額 (T_i) 千円	発生確率 (P_i)	リスク値 (R_i)
精神的苦痛Lv (x)	経済的損失Lv (y)									
2	1	3	2	1	33	360	5	11,880	2.3E-04	2,734

報は個人の氏名、職名、研究実績などである。

ここで、JOモデルにおけるパラメータ(網掛け部)はこのシステムに格納されているデータの内容から精神的苦痛レベルを2、経済的損失レベルを1とした。本人特定容易度はこのシステムには氏名が格納されているが住所等完全に個人を特定する情報は保持していないことから3としている。また、社会的責任度は大学という機関の公共性を踏まえ2とし、事後対応評価は適切な対応を行うこととして1としている。

C_i は式(1)により求められる1件あたりの賠償額である。件数(I_i)はシステムに登録されているユーザ数であり、情報漏えいが起きた場合の被害件数とみなす。従事者(N_i)は件のデータを扱うことができる人数である。この例での、 N_i の値はシステムの管理者への調査によって求めた。情報漏えいインシデントの発生確率(P_i)は、JNSAに報告された件数(教育関連:81件,2009)および2009年の文部科学省の幼稚園~大学院の教職員数(1,759,492)から一人当たりの発生確率 P_p ($=81/1759492=4.6E-5$)を求め、この値からこのシステムでは従事者の誰かがインシデントを発生させる確率

$$P_i = 1 - (1 - P_p)^{N_i} \quad (2)$$

として定義した。また、総賠償額(T_i)はユーザ全員の個人情報が漏えいしたと仮定したときの賠償額で、

$$T_i = C_i I_i \quad (3)$$

となる。本手法では、個々のシステムにおける個人情報漏えいのリスク値(R_i)として、

$$R_i = T_i P_i \quad (4)$$

を用いる。このリスク値は1年間で対象のシステムが個人情報漏えいによって支払う賠償額の期待値と考えることができる。このシステムに対して算出されたリスク値は2,734となった。

2.3 部門内のリスク値算出

ひとつの部門のリスク値の算出方法としては部門が保有するシステムすべてに対してリスク値 R_s を算出し、それらすべてを総和するのが一般的である。すなわち、

$$R_s = \sum_i R_i \quad (5)$$

となる。

ここでは、ひとつの部門としてある大学の事

事務局を例として、この部門が運用しているサーバについてシステム管理者に各システムに格納されている個人情報内容などの聞き取り調査を行い、個々のサーバのリスク値を算出して事務局全体のリスク値として算出した。それぞれのシステムでのリスク値は2.2で述べた方法により、機微情報度および本人特定容易度をそれぞれ設定して求めている。表2に聞き取り調査により求めた大学事務局で保有するシステムの一部と各システムのリスク値(R_i)および総和(R_s)を示す。

3 JOモデルを応用した包括算出法

3.1 大学における問題点

本研究では、前節で述べた手法を部門ごとの全体リスク値算出法のひとつとして提案する。しかしながら、大学という組織を踏まえた場合、以下の理由により個々のシステムすべてから大学全体のリスク計算を行うことは難しいと考えられる。

- 管理・運用上の問題**
 大学の業務システムでは、学外機関とのデータ統一やシステムの連携をおこなうため、各校一律のシステムを導入することがある。このとき、導入したシステムの運用だけに着目し、システム自体のセキュリティ要件の把握がおろそかになり、リスク評価を行うことができないことが考えられる。
- PC・ネットワークの利用内容特定**
 組織内の利用者数として最も大きく占めるのは学生である。学生によるPC・ネットワークの利用目的は学業、就職活動さらに個人的な利用などが考えられ、リス

ク算出のための情報の内容の把握は非常に困難である。

また近年、大学として設置している共用PCの数は減少傾向にあることが報告されている[1]。これはPC利用のコモディティ化が進み、大学のPCを利用するよりも個人所有のPCを利用する機会が増えているためであると考えられる。それに加え携帯端末によるネットワーク利用が増えているため、さらに個人利用の内容を特定することが困難になっている。

3.2 利用形態別包括算出法の提案と算出

そこで本研究では、部門が保有するすべての情報システムを包括してひとつの情報システムとしてみなし、これに対して2.2節で述べたリスク算出法を当てはめることにより部門全体の個人情報漏えいリスク値として算出する。この手法を包括算出法と呼ぶ。

ここでは、リスク値の算出のため、2.3と同じ事務部門をサンプルとして用いた。まず、機微情報度、本人特定容易度のパラメータを与え、JOモデルのパラメータを決定し、1件当たりの賠償額を計算した。さらに、扱う情報の件数と、情報漏えいを引き起こす原因となる従事者を用いて、(2)~(4)式を適用することにより、「事務サーバ」としてのリスク値を求めた。表3に包括算出法により最終的に求められた「事務サーバ」のリスク値を示す。

4. 考察

3.2で求めた「事務サーバ」のリスク値、2.3求めた各システムの総計と比較して約69%の値となっ

表2：大学事務局で保有するサーバリスク値

システム名	概要	個人情報内容	登録利用者数	実従事者数	リスク値 (R_i)
業務文書配布システム	学内限定の教職員間の業務メールシステムおよび教室の予約システム	氏名、E-mailアドレス	418人 (全教職員)	4人 (メディアセンター技術職員)	462
休講・呼出し等掲示	学生への休講・呼出し等の掲示システム	氏名、所属、学年	3692人 (全学生3505人+全教員187人)	5人 (メディアセンター技術職員、教務・学生課職員)	5,099
財務会計システム	予算管理、資産管理、決算処理等に関する業務	氏名、電話番号、住所、E-mailアドレス、所属、銀行口座番号、国籍、その他大学の資産情報	約8,000人	25人	828,191
物品請求システム	財務会計システムと連携と連携したWebシステム	氏名、所属、E-mailアドレス	約250人	25人	1725
:	:	:	:	:	:
総和 R_s					2,053,519

表3：事務サーバに対するJOモデルの適用とリスク値算出

機微情報度		本人 特定 容易度	社会 的 責任 度	事 後 対 応 評 価	賠償費/ 件 (C_i) 千円	件数 (I_i)	従事 者数 (N_i)	総賠償額 (T_i) 千円	発生確 率 (P_i)	リスク値 (R_i)
精神的 苦痛Lv (x)	経済的 損失Lv (y)									
2	1	3	2	1	33	1250	75	412,500	3.4E-03	1,419,000

ている。JOモデルにおける精神的苦痛レベル(x)および経済的損失レベル(y)の値は、(1)式に示すように、本来、システムが保有する情報の内容から与えうる最大の値を設定する。表2に示す「事務サーバ」中で、ひとまとめにした複数のシステムでも機微情報度の値が高いシステムがいくつか存在するが、全体のシステムの数から見ると少数である。包括算出法においてひとつのシステムとしてみなしたとき、最大の値を与えた場合、1件当たりの賠償額の値が非常に大きくなり、現実的でないリスク値が算出されてしまう。そこで本研究では、ここでは「事務サーバ」のJOモデルのパラメータとして調査したシステムのうち多くを持つ値を用いた。

本手法で用いたJOモデルおよび I_i 、 N_i のパラメータ設定によっては大きな数値の変動が考えられる。ここでは工科系学部の単科大学を例にしているため、個人情報の保有は少ないと考えるが、医系学部など特に機微情報度が高い情報を扱う部門・大学などでは、値が異なってくるのが予想される。

また、服部らによる調査[8]から、組織として導入・運用コストの低減を期待したクラウドの導入が進んでいる。本研究ではすべてローカルシステムで動作しているものでリスク値を算出したが、ローカルシステムで扱っている個人情報をそのままクラウド化した場合、パラメータに変化が無い限り、本研究で扱った個人情報のリスク値そのものに変化はない。したがって、導入・運用コスト自体は低減させることはできるが、セキュリティ対策費は削減することはできないと考えられる。

5. おわりに

本論文ではJOモデルをベースとして、システムが保有する個人情報の件数、漏えいを起こす可能性のある従事者をパラメータとしたリスク算出法を提案し、個々のシステムへの適用と総和によって一部門におけるリスク値の算出を試みた。この値は個々のシステムのリスク値によって重要度の認識や予算配分などの目安とすることができる。しかし、情報の内容、件数などのパラメータをシステムごとに与えているため、すべてのシステムの調査が必要である。この手法は、すべてのシステムを把握できる一部門など限られた組織では適用可能であると考えられるが、大学全体という大きな組織を考えた場合は現実的ではない。そこで本研究では部門で保有するシステムをひとつの情報システムとみなし、包括的にリスク値を算出す

る手法を提案した。この手法を用いて、部門全体の個人情報漏えいに対するリスク値を大まかに見ることによって、リスク対策費の配分を行う目安のひとつとすることが考えられる。さらに、大学の各部門、組織に適用することにより、大学全体のリスク対策費として利用することも考えられる。また、クラウド環境に対応したこれらセキュリティ対策選定方法に関する研究は熟成しているとはいえず、本手法も対応を検討する必要がある。

参考文献

- [1]文科省調査 2009年度 セキュリティ対策の実施状況 ,<http://www.e-stat.go.jp/SG1/estat/GL02020101.do?method=xlsDownload&fileId=000003653310&releaseCount=1> (2011/10/11 現在)
- [2]総務省調査 <http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/h21jyojitsu.html>(2011/10/11 現在)
- [3]中村 逸一 ,兵藤 敏之 ,曾我 正和 ,水野 忠則 ,西垣 正勝 ,セキュリティ対策選定の実用的な一手法の提案とその評価,情報処理学会論文誌 Vol.45, No. 8, 2022-2033, 2004
- [4]西垣 正勝, 白井 佑真, 山本 匠, 間形 文彦, 勅使河原 可海, 佐々木 良一, 賠償リスクを考慮した情報セキュリティ対策選定方式の提案と評価, 情報処理学会論文誌, Vol.52, No.3, 1173-1184, 2011
- [5]日本ネットワークセキュリティ協会「2009年度情報セキュリティインシデントに関する調査報告書 Ver.1.1,http://www.jnsa.org/result/incident/data/2009incident_survey_v1.1.pdf (2011/10/11 現在)
- [6]日本ネットワークセキュリティ協会「2003年度 情報セキュリティインシデントに関する調査報告書 , http://www.jnsa.org/active/2003/active2003_1a.html(2011/10/11 現在)
- [7]<http://www.atmarket.co.jp/fsecurity/special/50invest/invest.html> (2011/10/11 現在)
- [8]服部 真, 原田 要之助, クラウドに関する情報セキュリティの課題の整理～アンケート調査結果からの分析～, 情報処理学会研究報告, Vol.2010-CSEC-51, No.6, 2010