サイバーリスクに関する実証分析

和泉 あゆみ† 加藤 慎也† 小松 文子† 竹村 敏彦‡

†情報処理推進機構
113-6591 東京都文京区本駒込 2 丁目 28 番 8 号

‡佐賀大学
840-8502 佐賀県佐賀市本庄町 1

あらまし 近年，サイバー攻撃や内部不正によるインシデントが複数報道されており，中には原因調査や復旧作業等に多大な費用が発生し，企業経営に影響を及ぼす事例もある．そこで本稿では，情報セキュリティが持つ相互依存性の解決策の一つとしてのサイバー保険に着目し，企業のサイバーリスクに対する体制整備や各種セキュリティ対策との関連について分析を行った．この結果，リスク分析や高度なセキュリティ対策の実施が，サイバー保険の加入に影響を与えることが確認された．

An Empirical Analysis on Cyber risk

Ayumi Izumi† Shinya Kato† Ayako Komatsu† Toshihiko Takemura‡

†Information-technology Promotion Agency (IPA),
2-28-8 Honkomagome, Bunkyo-ku, Tokyo 113-6591, JAPAN
‡Saga University
1 Honjo-machi, Saga-shi, Saga 840-8502, JAPAN

Abstract In recent years, there have been reports on information security incidents where companies suffered cyber attacks, malicious insider incidents and so on. According to the reports, investigation of the incidents or IT recovery by them sometimes resulted in huge costs and, consequently, shook them. This paper focuses on cyber insurance as a solution to interdependency of information security and analyzes a relationship between the insurance and establishment of a department to cope with cyber risk or information security measures.

1 はじめに

企業のセキュリティ対策の現状や被害状況などについて調査した「2014 年度情報セキュリティ事象被害状況調査」（情報処理推進機構（IPA））によればサイバー攻撃を受けたと回答した企業は全体の 19.3%に上り，前年より 5.5 ポイント増加したことが報告されている[1]．この報告からも分かるように，現在，多くの企業がサイバー攻撃の脅威に晒され，企業には大きな経済的損失が生じうることを意味する．

例えば NetDiligence 社 2013 年調査レポートによれば，米国におけるサイバー攻撃の事故対応費用（フォレンジック，コンサルティング，モニタリングなどの費用）として平均 95

万ドルになったと試算している[2]．また，田中たちは情報セキュリティ・インシデント被害による日本全体の経済的損失額として 46～94 億円と試算している[3]．

近年，日本企業の情報セキュリティ投資額は増加し，投資意欲は高まりつつある一方で，日本企業の情報セキュリティ投資額は世界全体平均と比べると半分の規模にとどまっていること，4 割以上がインシデントの発生要因を把握できていないことや，役員クラスの情報セキュリティリーダーが不足していることがわかり，情報セキュリティに対して日本企業の対策が十分な水準に達していないと文献は指摘している[4]．

そもそも情報セキュリティ対策には，Varian たちが指摘したように適切な対策の水準を明確化することは困難であるという特有の問題（「相互依存性（interdependency）」の存在）がある[5]．それは，例え個々の企業において適切な情報セキュリティ対策が実施されていたとしても，ネットワークでつながっている他の企業（関連企業）が対策を実施せずに何らかのインシデント被害（サイバー攻撃など）に遭遇した場合，その影響が適切な対策をしている企業にも及んでしまう．言い換えると，自らが対策をしていても他社が対策をしていなければ被害を受ける潜在的なリスク（残存リスク）が存在し続けるのである．この相互依存性に関する問題（経済学でいうところの外部不経済の問題）に対する解決策の一つとして保険（本稿における「サイバー保険」）の活用がある．

サイバー保険とはサイバー事故発生に伴う損害を企業が被った場合，包括的に補償する保険商品のことである．米国では証券取引委員会（SEC）のコンプライアンス検査局（OCIE）の指針で金融サービス企業の効果的な戦略としてサイバー保険の加入が推奨されており，多くの米国企業に理解されているようである [5]．一方，日本では，2012 年にサイバー保険が発売されて以降，各社で補償内容や付帯サービスの拡充が行われてきており，サイバー保険の普及に向けた環境は整いつつあるが，市場規模は約 90 億円に過ぎず，諸外国と比較すると，十分に浸透しているとはいえない状況である[6]．

そこで本稿では，2015 年 2 月に実施したアンケート調査結果[7]を用いて，サイバー保険と，企業のリスク管理やセキュリティマネジメントとの関連について分析し，考察を行う．

2 関連研究

ここでは，セキュリティエコノミクスにおける情報セキュリティ対策と保険に着目したいくつかの研究を紹介する．1 章でも触れたように，インターネットを企業が利用する限り，企業は相互依存性の問題に直面してしまう．Varian は，情報システム全体・インターネットを公共財としてとらえたとき，情報セキュリティ対策をせずにシステムを利用するただ乗り（free rider）の存在についていち早く指摘し，企業の情報セキュリティ対策が不十分になることを説明している[5]．また，Gordon and Loeb は脆弱性の水準と情報セキュリティ投資の水準の関係について分析を行い，中程度の脆弱性に対して重点的に情報セキュリティ投資を行うべきであるという示唆を与えている[8]．さらに，Kunreuther and Heal はゲーム理論のフレームワークを用いて，相互依存性が存在する状況下で企業が情報セキュリティ投資をする条件を求めている．これらの研究を受けて，企業に情報セキュリティ対策の動機づけを行わせる研究や相互依存性の問題に対する解決策に関する研究が行われるようになった[9]．

Kunreuther and Heal は相互依存性への対応（外部性の内部化）として保険，補助金，規制や第三者機関の検査などの可能性についての議論の中で保険が有効とならないことを指摘したが，Gordon, Loeb and Sohail は情報セキュリティ投資と保険の間にはトレードオフの関係があるものの，企業の事業活動における保険を活用したフレームワークが，他の事業リスクと同様にサイバーリスクのマネジメン

トにも有効であるとしている[10]．また，田中・松浦は情報セキュリティの相互依存性を踏まえて，保険と監査制度の活用が民間ベースでの情報セキュリティ水準を確保するための動機付けとなる可能性があることを指摘している[11]．さらに，Lelarge and Bolot は，保険料を情報セキュリティ投資水準と対応させるなどの一定の条件を設定することで，モラルハザードを発生させることなく情報セキュリティ投資および保険への加入の両方を行うインセンティブが働く可能性を示している[12]．

ここで紹介した研究はいずれも経済学から見た理論研究にとどまっている．

3　課題

サイバーリスクは，回避や低減などのいかなる対策をとっても，完全なリスクコントロールは困難であるから，リスク移転のひとつであるサイバー保険の活用が有効なリスク対応の手段である．また，保険を有効に活用することで，関係者間が相互に投資し合うインセンティブが働くエコシステムの構築も期待されている[13]．

しかし，サイバー保険がリスク対応のひとつの手段として提供されている中で，国内の企業におけるリスク管理状況，保険についての認知や加入に対する意識が明らかではない．本稿では，アンケート調査によって，保険加入率が低い状況の要因は何かを調査分析し，保険加入に影響を与える要因を明らかにする．

4　アンケート調査

4.1　アンケート概要

2015 年 2 月に実施した「民間企業のサイバー保険等についての調査」（以下，「本調査」と略す）と題した Web アンケート調査形式によって収集した個票データを用いて分析を行う．この調査形式を採用した理由として，調査環境の変化（回収率の低下や拒否率の上昇など）に加えて，情報セキュリティ特有の問題点として多くの企業が部外者にセンシティブな情報を出したくないといった理由により調査協力がそもそも得られない点をカバーし，効率よく調査対象者を抽出するためである．

本調査はサイバーセキュリティ上のリスクを含めた企業の経営リスク管理の実態や対処体制，リスク対応の一つであるサイバー保険の認知やニーズ等に関する現状把握を目的として実施したものである．本調査の対象は，企業の経営者やリスク管理・IT 担当責任者であり，また企業規模（売上高）別の相違点を調べるために企業規模による事前割付を行った．調査対象者の構成は表 1 の通りであり，計 1,773 人の有効回答数を得ている．

表 1：調査対象者の構成

企業規模	役割		
	経営者（%）	リスク管理・IT担当責任者（%）	合計（%）
大企業 （年間売上10億円以上）	240（13.5）	397（22.4）	637（35.9）
中堅企業 （年間売上1億円以上10億円未満）	177（10）	371（20.9）	548（30.9）
中小企業 （年間売上1億円未満）	322（18.2）	266（15）	588（33.2）
計	739（41.7）	1034（58.3）	1773（100）

質問項目は，組織の体制，セキュリティ対策，企業属性等である（計 48 問）．本稿で分析の対象とするアンケート項目の詳細については参考文献の[7]を参照のこと．

5　アンケート結果

本章では，サイバーセキュリティリスクに対する組織の体制や，情報セキュリティに関する事故経験の有無，サイバー保険の認知について単純集計を示す．

5.1　組織の体制

情報セキュリティおよびリスク管理に対する組織体制に関して，「経営リスク分析を行っているか」「情報セキュリティ担当役員（CISO）を任命しているか」を質問した結果が図 1 と図 2 である．

経営リスク分析を「行っていない」は 54.3%であった．CISO についても「任命していない」が 70.9%となった．このことからリスク管理体制としては，十分浸透してない

ように見受けられる.

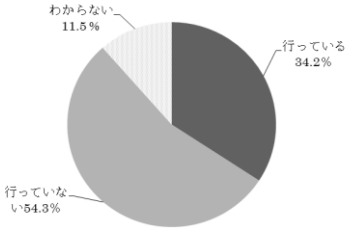

図 1: 経営リスク分析の実施状況

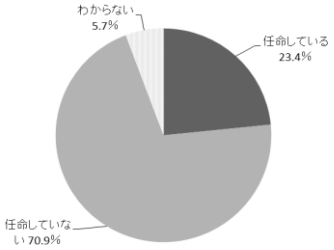

図 2: 情報セキュリティ管理の担当役員（CISO）の任命状況

5.2 情報セキュリティに関する事故経験の有無

情報セキュリティに関する事故経験の有無（図 3）と今後の情報セキュリティに関する事故の有無（図 4）について回答を求めた. 本稿では, 情報セキュリティに関する事故について 8 項目あるうち, どれか一つでもあると回答したものを「ある」としている.

情報セキュリティに関する事故経験の有無で「ある」と回答している人の割合は約 15.2%であった. また約半数以上の割合が, 今後事故にあう可能性があると考えている.

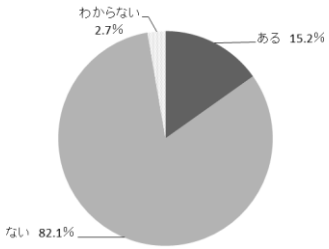

図 3: 情報セキュリティに関する事故経験の有無

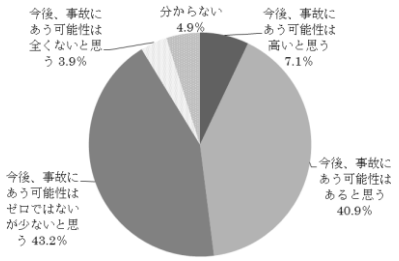

図 4: 今後の情報セキュリティに関する事故に対する認識

5.3 サイバー保険の認知度と加入

サイバー保険[1]について質問した結果は図 5 と図 6 である.

認知度については, 大まかに内容まで知っている人も含めれば, 知っていると回答した人の割合は約半数であった. サイバー保険の加入で「加入している」と回答した人の割合は 14.6%であった. この結果からサイバー保険の認知度は半数以上あるが, 実際の加入率についてはまだ少ないことが分かる.

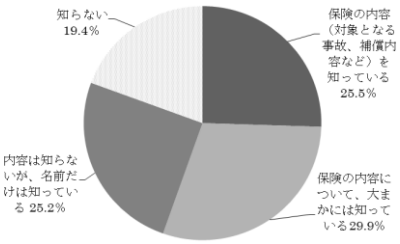

図 5: サイバー保険の認知状況

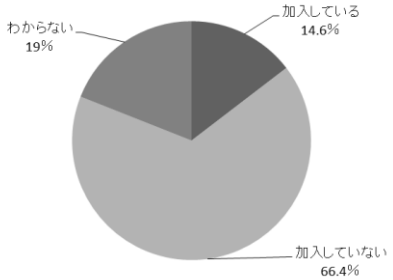

図 6: サイバー保険の加入状況

[1] 本調査では、コンピュータ故障に関する保険、情報漏えいに関する保険またはサイバー攻撃に関する保険をまとめて IT 関連保険と定義したが、本稿ではこれらをサイバー保険と呼ぶ.

6 分析

6.1 分析対象と変数

本稿では，サイバー攻撃等から保護すべき資産（個人情報，機密情報）を電子データで保有している組織を対象とし，1,443 人を抽出した．更に「分からない」という回答を除外した 772 人を分析対象としている．

サイバー保険に対する影響要因を明らかにするため，次の手順で統計分析を実施した．

① 分析対象として，組織のセキュリティ対策，懸念事項，リスクの影響度の共通因子を抽出するために因子分析を実施．

② 共通因子とリスク分析の実施，CISO の任命，業種，従業員数の変数を説明変数として，サイバー保険の加入の有無に対するロジット回帰分析を実施．

なお，本稿の分析には統計ソフトウェアとして StataSE 13 を用いた．

6.2 項目の信頼性評価

組織のセキュリティ対策，懸念事項，リスクの影響度の信頼性を確認するため，クロンバックの α 係数を求めた（表 3）．なお，質問項目の回答が 2 値となっている質問項目のみ RIDIT による重み付けを実施している[2]．Hair らによれば，クロンバックの α 係数が 0.70 以上であれば，共通因子の一貫性（信頼性）は高いと考えられている[15]．表 3 に示したいずれの共通因子の α 係数も 0.70 を上回っていることから，これら変数はある程度の妥当性を有しているといえる．

表 2：各項目のクロンバックの α

項目	クロンバックのα
セキュリティ対策	0.9687
懸念事項	0.9341
リスクの影響度	0.8809

6.3 因子分析

まず scree 法を用いて因子数を決定し，その後，プロマックス回転をさせて因子分析を実施した．scree 法の結果，因子数はそれぞれ 2 因子になると判断した．なお，共通因子を表 3 の通りに名前を付けた．共通因子が大きくなるほど，組織への影響が大きくなると解釈する．例えば「リスクの影響度の場合，共通因子の値が大きくなるほど，組織への影響が大きいことを示す．因子分析の結果については付録に添付している．

表 3：共通因子

項目	共通因子
セキュリティ対策	高度セキュリティ対策の実施の傾向 （生体認証、ISMS・Pマーク取得）
	基本セキュリティ対策の実施の傾向 （ウイルス対策、パスワード設定等）
懸念事項	情報漏えいの懸念の大きさ
	風評被害の懸念の大きさ
リスクの影響度	人為的リスクの影響の大きさ （サイバー攻撃、為替変動、リストラ）
	偶発的リスクの影響の大きさ （自然災害、交通事故等）

6.4 ロジット回帰分析

ロジット回帰分析を行った．被説明変数および説明変数は表 4 の通りである．ロジット分析の結果を表 5 に示す．1%水準で有意な係数は「リスク分析の実施の傾向」「高度セキュリティ対策の実施の傾向」，5%水準で有意な係数は「従業員数」，10%水準で有意な係数は「人為的リスクの影響度の大きさ」であった．

表 4：被説明変数と説明変数

	被説明変数	
	サイバー保険への加入	0：加入していない 1：加入している
	説明変数	
体制	リスク分析の実施の傾向	0：実施していない 1：実施している
	CISOの任命	0：任命していない 1：任命している
セキュリティ対策	高度セキュリティ対策の実施傾向 （生体認証、ISMS・Pマーク取得）	因子分析による因子 （RIDIT実施）
	基本セキュリティ対策の実施傾向 （ウイルス対策、パスワード設定等）	
懸念事項	情報漏えいの懸念の大きさ	因子分析による因子 （RIDIT実施）
	風評被害の懸念の大きさ	
リスクの影響度	人為的リスクの影響の大きさ （サイバー攻撃、為替変動、リストラ）	因子分析による因子
	偶発的リスクの影響の大きさ （自然災害、交通事故等）	
企業属性	業種	0：非製造業 1：製造業
	従業員数	1：5人未満5人未満 2：5人以上50人未満 3：50人以上300人未満 4：300人以上1,000人未満 5：1,000人以上

[2] RIDIT とは、質問項目を回答者の分布で重み付けを行い、RIDIT スコアを計算する手法である[14]．

そして，「リスク分析の実施の傾向」「高度セキュリティ対策の実施の傾向」「従業員数」の係数は正の値となっている．一方で，「人為的リスクの影響度の大きさ」の係数は負の値となっている．例えば，「高度セキュリティ対策の実施の傾向」と「人為的リスクの影響度の大きさ」を取り上げると，前者は高度な情報セキュリティ対策を実施している（ISMS や生体認証を導入している）組織ほど，サイバー保険に加入する傾向が高いことを，また後者はサイバー攻撃や内部不正による情報漏えいが経営に影響を与えないと考える組織ほど，サイバー保険に加入する傾向が高いことを，それぞれ意味している．

「CISO の任命」「基本セキュリティ対策の実施の傾向」「情報漏えいの懸念の大きさ」「風評被害の懸念の大きさ」「偶発的リスクの影響度の大きさ」および「業種」の係数は統計的に有意ではなかった．つまり，これらの要因はサイバー保険の加入の有無に影響を与えないことを意味している．

表 5：分析結果（ロジット分析）

項目	Coef.	Std. Err.	z	P>|z|
リスク分析の実施	0.794432	0.269163	2.95	0.003
CISOの任命	0.311318	0.271224	1.15	0.251
高度セキュリティ対策の実施傾向	0.54677	0.155764	3.51	0.000
基本セキュリティ対策の実施の傾向	0.252845	0.177178	1.43	0.154
情報漏えいの懸念の大きさ	0.243462	0.177944	1.37	0.171
風評被害の懸念の大きさ	−0.03246	0.160229	−0.2	0.839
人為的リスクの影響度の大きさ	−0.46624	0.269625	−1.73	0.084
偶発的リスクの影響度の大きさ	0.371312	0.283235	1.31	0.19
業種	0.201199	0.282021	0.71	0.476
従業員数	0.225587	0.104371	2.16	0.031
_cons	−3.11815	0.438274	−7.11	0
Number of obs =	LR chi2(10) =	221.11		
Prob > chi2 =	0.0 Log likelihood =	−282.04726		
Pseudo R2 =	0.2816			

7　考察

分析の結果，サイバー保険の加入に影響を与える要因として「リスク分析の実施の傾向」「高度セキュリティ対策の実施の傾向」「人為的リスクの影響度の大きさ」「従業員数」があることがわかった．これらの中で，「人為的リスクの影響度の大きさ」以外の要因についてはサイバー保険の加入に対して正の影響を与えること（サイバー保険の加入を促す要因であること）がわかった．しかしながら，「人為的リスクの影響度の大きさ」に関してはサイバー保険の加入に対して負の影響を与えるという結果が得られた．人為的なリスクについては，保険によらず，リスク回避が可能であると考えているのかもしれない．

「セキュリティ対策」において「高度セキュリティ対策の実施傾向」の係数は有意に正であるが，「基本セキュリティ対策の実施傾向」の係数は統計的に有意にはならなかった．つまり，ウイルス対策やパスワード設定などの基本的なセキュリティ対策を実施していることはサイバー保険の加入の有無には影響を与えないが，それよりも高度な対策になるとサイバー保険の加入の有無に影響を与えることが分かる．

また懸念事項について見てみると，いずれの要因も統計的に有意ではない，つまりサイバー保険の加入の有無に影響を与えないことが分かる．言い換えると，これは懸念をもつだけではサイバー保険への加入への有無に影響を与えないことを意味する．

最後に，「従業員数」の係数が有意であるのに対して，「業種」の係数が統計的に有意にならなかった．これは売上高以外ではかられる企業規模を表す従業員数が多い企業ほど，サイバー保険に加入する可能性が高いことを意味している．また，この結果は，情報セキュリティ・インシデントが企業規模にかかわらず，中堅や中小企業に対しても発生するものであることを考えると，今後中小企業に対してよりサイバー保険を含めた対策を推進してく必要があることとも読み取れる．

8 おわりに

本稿では，Web アンケートで実施した調査結果を基に分析を実施した．サイバー攻撃等の情報セキュリティ事故が依然として増えている状況では，組織に損害を及ぼす可能性が高い。したがって，サイバー脅威に対し、組織の事業戦略に沿ったリスク分析を実施し、適切にリスクをコントロールすることが重要と考える。

今回採用したインターネット調査では結果を一般化するには限界が存在する．調査の目的が個人や組織の意思決定の一つの有益な判断材料を提示することであれば，この方法を採用することに意味があると考える[16]．

9 参考文献

[1]情報処理推進機構：2014 年度情報セキュリティ事象被害状況調査（2015）(http://www.ipa.go.jp/security/fy26/reports/isec-survey/)

[2]NetDiligence: Cyber Liability & Data Breach Insurance Claims - A Study of Actual Claim Payouts (2013)

[3]田中秀幸・竹村敏彦・飯高雄希・花村憲一・小松文子：情報セキュリティ・インシデントによる経済損失の推計に関する研究」『経済政策ジャーナル』第 11 巻第 2 号，59-62（2015）

[4] プライスウォーターハウスクーパース株式会社：グローバル情報セキュリティ調査 2015（2015）（http://www.pwc.com/jp/ja/advisory/research-insights-report/assets/pdf/information-security-survey2015.pdf）

[5]Varian, H.R.: System Reliability and Free Riding, ACM Transactions on Information and System Security, Vol.5, 355-366 (2002)

[6]特定非営利活動法人日本ネットワークセキュリティ協会：2014 年度情報セキュリティ市場調査速報（2015）（http://www.jnsa.org/seminar/nsf/2015/data/B1_kishiro.pdf）

[7]情報処理推進機構：企業におけるサイバーリスク管理の実態調査 2015（2015）（https://www.ipa.go.jp/security/fy27/reports/cyber-ins/）

[8]Gordon, L.A., Loeb, M.P.: The Economics of Information Security Investment, ACM Transactions on Information and System Security, Vol.5, 4380457 (2002)

[9]Kunreuther, H., Heal, G.: Interdependent Security, The Journal of Risk and Uncertainty, Vol.26, 231-249 (2003)

[10]Gordon, L.A., M.P. Loeb and T. Sohail, Market Value of Voluntary Disclosures Concerning Information Security, MIS Quarterly, Vol. 34, No. 3, 567-594 (2010)

[11]田中秀幸，松浦幹太：情報セキュリティ・マネジメントの制度設計，Network Security Forum 2003 (2003)

[12]Lelarge, M., Bolot, J.: Cyberinsurance As An Incentive for Internet Security. In: WEIS (2008)

[13]情報処理推進機構：情報セキュリティ白書 2015（2015）

[14]Lieberthal: Hospital Quality: A PRIDIT Approach, Health Research and Educational Trust, 43(3), 988-1005 (2008)

[15]Hair, Jr, J.F., Anderson, R.E, Thatham R.L.,and Black, W.C., Multivariate Data Analysis,Upper Saddle River, NJ: Prentice-HallInternational, Inc (1998)

[16]労働政策研究・研修機構：インターネット調査は社会調査に利用できるか『労働政策研究報告書』No.17 （2005）

付録　因子分析結果

●セキュリティ対策

変数名	高度セキュリティ対策の実施傾向	基本セキュリティ対策の実施傾向	独自性
フロアや施設への入退出管理	0.425	0.2986	0.5693
機器や記録媒体の持込み・持出しの制限	0.2613	0.5117	0.5002
一般ユーザアカウントの管理ルールの策定（パスワードの設定ルール等）	−0.0059	0.7489	0.4448
Webサイト管理者権限アカウントの管理ルールの策定	0.0377	0.7437	0.4098
その他の管理者権限アカウントの管理ルールの策定	0.0659	0.7334	0.3964
一般ユーザのプログラムインストールの制限（exeファイルの実行禁止等）	0.2623	0.5161	0.4931
重要なシステム・データのバックアップ	−0.1157	0.6677	0.6388
ハードディスク等の機器廃棄時の破砕／溶融	0.1423	0.5621	0.5623
外部専門家によるセキュリティ監視サービスの活用	0.6113	0.0986	0.5401
ログやファイル情報に基づくWebコンテンツの改ざん検知	0.6271	0.2219	0.3809
IT資産構成や設定の文書化	0.5384	0.2991	0.4163
セキュリティポリシーの策定	0.4608	0.3933	0.4031
事業継続計画（BCP）の策定	0.613	0.2135	0.4125
委託先における情報セキュリティ対策実施状況の確認	0.6444	0.2075	0.372
リスク分析に基づくリスク報告書の作成	0.7466	0.1044	0.3328
情報セキュリティ監査の実施	0.698	0.1651	0.3394
情報セキュリティマネジメントシステム（ISMS）の認証取得	0.8281	−0.0325	0.3473
プライバシーマーク（Pマーク）の取得	0.7679	−0.0214	0.4308
セキュリティ教育・研修の実施	0.5373	0.2929	0.4259
アプリケーションソフト等の脆弱性に関する迅速な対応	0.3647	0.4165	0.5007
WEBサイトやネットワークなどの脆弱性診断サービスの活用	0.629	0.1911	0.4154
ネットワークサーバ（メールサーバ、Webサーバ）向けウイルス対策	−0.0478	0.6438	0.6223
ローカルサーバ（ファイルサーバ、プリントサーバ）向けウイルス対策	−0.0958	0.7269	0.5508
クライアント（パソコン）向けウイルス対策	−0.096	0.5973	0.7068
プロバイダによるウイルスチェックサービス（*1）	0.1126	0.3984	0.7716
ウェブ閲覧のフィルタリングソフトウエア	0.3328	0.4064	0.5525
メールフィルタリングソフトウェア（誤送信防止対策製品、スパムメール対策製品を含む）	0.1994	0.5059	0.5764
情報漏えい対策（DLP）製品	0.695	0.1122	0.4055
ファイアウォール	−0.0253	0.6202	0.6346
VPN	0.4324	0.3472	0.502
IDS/IPS（*2）	0.7234	0.0732	0.4042
アプリケーションファイアウォール（WAF（*3）を含む）	0.6331	0.1667	0.4374
アイデンティティ管理／ログオン管理／アクセス許可製品（SSO（*4）を含む）	0.6749	0.1612	0.3804
ワンタイムパスワード、ICカード、USBキーによる個人認証	0.7202	−0.0469	0.522
生体認証（バイオメトリクス）	0.7588	−0.163	0.5546
PKIシステムおよびそのコンポーネント（電子証明書の発行、管理、証明サービスを提供するシステム）	0.8684	−0.1344	0.3759
セキュリティ情報管理システム製品（ログ情報の統合・分析、システムのセキュリティ状態の総合的な管理機能）	0.8209	−0.0058	0.3321
クライアントPCの設定・状態・動作・ネットワーク接続等を管理する製品（検疫ネットワーク*10を含む）	0.8359	−0.0154	0.3175
デバイス制御製品（USB、スマートフォン等各種デバイスの利用管理、書き込み制御機能）	0.8632	−0.0393	0.2964
シンクライアント（*5）	0.8544	−0.1215	0.3869
暗号化製品（ディスク、ファイル、メール等）	0.6388	0.1437	0.4548
ソフトウエアライセンス管理／IT資産管理製品	0.6511	0.1287	0.4532

chi2(861) = 3.7e+04 Prob>chi2 = 0.0000

●懸念事項

変数名	情報漏えいの懸念の大きさ	風評被害の懸念の大きさ	独自性
顧客情報が盗まれる（流出する）	0.7731	−0.0362	0.4378
業務情報（機密情報等）が盗まれる（流出する）	0.8144	−0.0809	0.4168
Webサイトが改ざんされる	0.6394	0.2031	0.3793
Webサイトがサイバー攻撃の踏み台として利用される	0.6674	0.2185	0.3153
Webサイトの負荷がサイバー攻撃によって高まり利用できなくなる	0.6607	0.244	0.2924
業務サーバの内容が改ざん・破壊される	0.7244	0.1557	0.3029
業務サーバ、Webサーバがウイルスに感染する	0.684	0.0649	0.4696
経営陣による記者会見を開催する	0.1633	0.7033	0.328
インターネット上で風評被害が広がる	0.1354	0.7103	0.3509
新聞等マスコミで騒がれる	0.0018	0.8844	0.2157
被害者から集団訴訟を起こされる	0.0346	0.8259	0.2792

chi2(55) = 1.0e+04 Prob>chi2 = 0.0000

●リスクの影響度

変数名	人為的リスクの影響の大きさ	偶発的リスクの影響の大きさ	独自性
自然災害に関するリスク（例）地震、津波、台風、竜巻、噴火、干ばつ、洪水など	0.0141	0.6874	0.5135
事故に関するリスク　（例）交通事故、労災事故、航空機事故、船舶事故、コンピュータ故障など	0.0442	0.6409	0.5473
政治に関するリスク　（例）戦争、革命、動乱、貿易摩擦、外圧など	0.3918	0.3397	0.5431
経済に関するリスク　（例）金利変動、為替変動、税制改正、金融不安など	0.5274	0.1896	0.5446
社会に関するリスク　（例）企業脅迫、誘拐、企業テロ、サイバー攻撃、産業スパイ、風評リスクなど	0.62	0.2083	0.3897
法務に関するリスク　（例）製造物責任訴訟、知的財産訴訟、環境汚染責任訴訟、独占禁止法など	0.744	0.0229	0.4218
財務に関するリスク　（例）債権リスク、デリバティブ投資、不良債権、資産の陳腐化など	0.8164	−0.0385	0.3764
労務に関するリスク　（例）労働争議、役職員の不正、内部犯行による情報漏えい、求人難、リストラなど	0.6528	0.0954	0.4767

chi2(28) = 4855.91 Prob>chi2 = 0.0000