フリガナ	アブドラ　アルムバラク
氏　名　（　本　籍　）	Abdullah Almubark　　（サウジアラビア）
学　籍　番　号	H14001
学位（専攻分野の名称）	博士　（総合情報学）
学　位　記　番　号	第 H10010 号
学位授与の日付	平成　29　年　3　月　25　日
学位授与の要件	学位規則第４条第１項該当
学位論文題目	Identifying the Mechanisms of Information Security Incidents 情報セキュリティインシデントのメカニズムの明確化

論文審査委員	主査	畠中 伸敏 教授
	副査	浅沼 市男 教授
	副査	櫻井 尚子 教授
	副査	綾野 克俊 教授

論文内容の要旨

セキュリティ特性の時代的変化に対して，企業や機関は，柔軟に組織の体質を変化し，組織改善を図る必要があるが，セキュリティホールや脆弱性を放置し，外部からの攻撃を受けて，初めて，情報セキュリティ上に欠陥があることに気付く場合が多い．例えば，ソニー・コンピュータエンタテイメントのゲーム機 PSⅢのサービスサイトの１億人の個人情報の漏えいの事件の例では，open SSH 4.4 の古いバージョンのソフトを使用していたために，ハッカー集団からの侵入を容易にした．また，ハッカー集団による SQL インジェクションによる攻撃も行われ，Web 画面の脆弱性対策を怠っていた．このように，コンピュータシステムそのものに依存する脆弱性と，組織内部の人間に起因する組織上の欠陥を放置することは，経営者の責任である．

ところで，バーナードは，利益優先，効率重視，成果主義の結果として，組織要員の正当なる評価が歪められ，特定の人物による地位の独占を強められることを示した．また，賃金，名誉，威信が地位により，配分の差異があることを示した．これらが階層組織の逆機能として働く結果，不祥事や事故が発生するとした．さらに，企業の生産活動の根幹となるテイラリズムでは，“能率”は，投入と産出の関係で決まるとしたが，サイモンは，組織の目標に企業活動の社会的価値が加えられてこそ，企業活動は意義あることで，組織目標と“社会的価値”の不協和により，社会的不祥事や事故

が発生することを示した.

大日本印刷から個人情報 863 万件の漏えい事件，ベネッセコーポレーションの 2,300 万件の顧客データの漏えい事件は，いずれも，組織目標と社会的価値の不協和と，委託先の従業者により個人情報が漏えいする組織構造の中で発生している．これは，下請負契約者が，一次，二次から五次請まであり，最後は一人親方の構造となる建築土木業界と似た構造がある．この構造的欠陥が階層組織の逆機能となって，情報セキュリティインシデントの発生を助長している.

本研究の先行研究としては，一橋大学の星野崇宏教授を中心とするグループが，企業不祥事の組織要因として，43 の要因を挙げ，共分散構造分析を適用して，主要な組織要因を 11 項目に絞り込んだ．また，北海道大学の眞野脩教授は，“対等の立場において個々の人々や団体が，自己の個人的目的達成のために自主的に結んだ協定の結果生み出された組織（側生組織）”の存在を主張した. ベネッセコーポレーションの 2,300 万件の顧客データの漏えい事件は，委託先の従業者による個人情報の漏えいである．これは，眞野脩教授の主張した側生組織の負のメカニズムが出現した例である.

本研究では，星野崇宏教授のアプローチを，インシデント（事件）が発生した組織に適用し，主要な組織要因 11 個を同様に導き出した.

次に，主要な組織要因 11 個をもとに，2006 年から 2015 年までの過去約 10 年間に事件が発生した 186 企業に対して，Correspondence method を用いて，累積寄与率 56.8%で，組織帰属性，プロ意識，内部統制の軸を抽出した．この分析軸をもとに，得られた各企業のサンプルスコアに対して，階層型クラスタ分析を行い，事件が発生した企業の組織上の特徴を分類及び事件発生のメカニズムを明確にした．得られた企業グループは，自己自滅型組織，非帰属型組織，カモフラジュ型組織，無防備型組織，アウトロー型組織の 5 つである.

一方，ISO/IEC27001:2013(情報セキュリティマネジメントシステムの国際規格)の項番 5.3 には組織の役割，責任及び権限が規定され，同 6.1.1a)及び b)には，“意図した成果を達成できることを確実にする”，“望ましくない影響を防止又は低減する”とある．また，情報セキュリティの事件・事故の対策として，付属書 A には，114 の管理策と 35 の管理目的を掲げている.

本研究では，さらに，抽出した組織タイプで，それぞれ異なる組織要因により事件が発生していることから，個人情報保護マネジメントシステム、及び環境マネジメントシステムで適用されている局面と影響の関係を明確にする方法を、5 プロセスとして考案した.

事件が発生するアスペクト（欠陥のある組織活動）とインパクト（欠陥が情報セキュリティ上の事件に及ぼす影響）との関係を，それぞれに抽出した組織タイプごとに明確にし，それぞれの組織改善策を導き出し，日本のサウジアラビア大使館 IT 部門，及び，サウジアラビア大学イマム校アラビア語研究所で，５プロセスの有効性を検証した。

Abstract

Security characteristics have changed, and as a result, companies need to changes their structures in order to promote flexibility and organizational improvement. In many cases, companies neglect security holes and vulnerabilities, realizing information security deficiencies only after they are attacked. For example, Sony Computer Entertainment leaked the personal information of 100 million people through its PS3 game console service site by using an old software version of Open SSH 4.4; which made it easy for hacker groups to invade the site. Because Sony failed to implement vulnerability countermeasures on its website, hacker groups were able to carry out an SQL injection attack. Clearly, it was the responsibility of Sony management to ensure that the organization properly addressed vulnerabilities directly derived from its computer systems; management also needed to concentrate on the organizational deficiencies caused by its people.

Barnard (1938) shows the result of a profit-first, efficiency-oriented and results-based has led to the corruption of the legitimate evaluation of the organizational members, and strongly enabling certain people to monopolize positions. Furthermore, differences in position caused several disparities in people's wages, reputations, and dignity. As a result of these acting as an inverse function of the hierarchical organization, scandals and accidents occurred. Furthermore, efficiency was determined by the relationship between investment and production in Taylorism, a doctrine that constitutes the basis of the production activities of companies. Simon (1997) shows that corporate activities are significant and meaningful only when their social value is adding to organizational objectives and that social scandals and accidents occurred due to disharmony between organizational objectives and social value.

In both cases of Dai Nippon Printing Co. leakage incidents of 8.63 million personal information, and Benesse Corp. leakage incidents of 23 million customer data, the information security incidents occurred due to disharmony between organizational objectives and social values in an organizational structure, which allowed subcontractor's employees to steal personal information. This structure is similar to that of the construction and civil engineering industry in which there are multiple layers of subcontractors, namely Tier 1, Tier 2 to Tier 5 and the bottom layer is comprised of self-employed craftsmen. This structural flaw constitutes an inverse function of hierarchical organization, which triggers information security incidents.

A previous study of this research in which 43 organizational factors of corporate scandals were conducted by a group led by Prof. Takahiro Hoshino (2008) of Hitotsubashi University. the number of organizational factors were narrowed down to

the main 11 factors using a covariance structure analysis. In addition, Prof. Osamu Mano (1989) of Hokkaido University has insisted the existence of lateral organizations which are “a result of voluntary agreements between persons or groups of equal positions for the purpose of achieving their individual goals” (p.2). The incident at Benesse Corporation in which the data of 23 million customers was leaked by subcontractor’s employees. This is an example of the negative mechanism of the lateral organizations that insisted by Prof. Osamu Mano.

In this research, applied Prof. Hoshino's approach to organizations in which incidents have occurred and similarly induced the 11 main organizational factors.

Based on the 11 main organizational factors, applied a correspondence method to 186 organizational samples in which incidents had occurred within approximately the last 10 years, between 2006 and 2015. With a cumulative proportion of 56.8%, three axes were derived and named as organizational attribution, professional consciousness and power of internal control. Based on the three derived axes, hierarchical cluster analysis was applied for the sample score obtained for each organization. Then classified the organizational characteristics of companies with incidents and identified the mechanism behind the occurrence of the incidents. The result was five groups of bureaucratic self-destructive organizations, none-belonging organizations, purpose camouflage organizations, unguarded organizations and outlaw organizations.

On the other hand, the organizational roles, responsibilities and authorities are defined in Clause 5.3, and Clauses 6.1.1.a) and b) of ISO/IEC 27001:2013 stipulate “ensure the information security management system can achieve its intended outcome(s)” and “prevent, or reduce, undesired effects”. In addition, as measures of information security incidents, 114 management measures and 35 control objectives are listed in Annex A of ISO/IEC 27001:2013.

This research proposes a five-process method for identifying the relationship between aspects and impacts applied to PII (Personally Identifiable Information) protection management systems and environment management systems. This method is based on incidents resulting from different organizational factors specific to selected organization types.

For each type of organization, the research identified the relationship between the aspect (defective organizational activity) where the incident occurred and its impact (the effects of defects on information security incidents). Their respective organizational improvement measures then were induced. Finally, the effectiveness of the five-process method was verified, both for the IT department at the Saudi Arabian Embassy in Japan and the Arabic Institute at IMAM Branch of Saudi Arabian University.