グループ企業におけるセキュリティアーキテクチャ実装状況に関する可視化手法の提案

佐藤　雄二†　大久保　隆夫†

†情報セキュリティ大学院大学
221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1

mgs145501@iisec.ac.jp takao.okubo@iisec.ac.jp

Proposal of visualization on security architecture implementation in Group Company

Yuji Sato†　Takao Okubo†

†Institute of Information Security.
2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama, Kanagawa 221-0835, JAPAN

mgs145501@iisec.ac.jp takao.okubo@iisec.ac.jp

要旨　各企業は継続的な成長を遂げる為、これまでに増してビジネス環境の急速な変化に対応する必要性がある。また、グループ企業においては、内部での情報連携を密に行う要求が高まるにつれ、全体として実効性のあるセキュリティ対策を整備することが重要となってきている。そこで本稿では「グループ企業として整合性のあるセキュリティ対策の実装」を実現するための前段階として、グループ企業内の関係者が、現在のセキュリティ対策状況に関して、共通の認識を持つための、セキュリティアーキテクチャ実装状況に関する可視化手法を提案する。

Abstract

The company adapts to a rapid change of the business environment, and it is necessary to do continuous growth. As the need of the information sharing in group companies increases, it is important how to build a security defense with the consistency as a whole. In this paper, "1st step to build a security defense that is consistent as a whole group company", we propose a method for visualizing the implementation status of security architecture to promote common understanding about the current security situation for stakeholders in the group companies.

1. 社会的背景と課題

ビジネス環境の急速な変化に伴い、その規模や業態を問わず企業は、これまでにまして迅速に適合し、継続的な成長を遂げる必要性に迫られている。しかし、その一方で企業を取り巻く情報セキュリティに関する脅威は、ビジネス規模の拡大、テクノロジーの進化と共に、高度化、複雑化傾向にある。こうした状況に対し、各社情報システム部門の担当者は、自社が管理している保護資産を顕在、潜在的な脅威から防御すべく、様々な対策を講じてはいるものの、主に対策コスト面における制約から、全ての脅威に対して、

タイムリーに防御策を講じられているとは言い難い。また、ある時点で過不足のない対策を講じても、その状態を維持するのに、多くの労力を費やす傾向にあるといった課題も別に存在する。それらはグループ企業においても同様であり、特に情報化が進み、グループ企業内での情報連携を密に行う必要性が高まるにつれ、いかにグループ全体として実効性のある情報セキュリティ対策を統一的に実装するか、といった点が重要視されている。

2. 最適なセキュリティ対策実現に向けた取り組み

前項にて言及した複雑、多様化傾向にある各種脅威に対し、最適なセキュリティ対策を導出すべく、様々な観点での考察が行われている。本項では先行企業による取り組み、および関連する先行研究について紹介する。

2-1. 先行企業による取り組み

リコーグループでは、図 1[1]のように、グループ各社の情報セキュリティレベルを一定水準以上に保つべく『共通化』を推進している。共通化の推進にあたっては、情報資産の種類別に、その取り扱いの基準を定め、業務上の重要性に応じ、『必要対策』、『推奨対策』の 2 段階のチェック項目を定めている。この内、『必要対策』は、グループとして必ず順守すべき事項としている一方、『推奨対策』に関しては、各社の業務特性によって、それぞれ任意に選択させている。その結果、必要、推奨対策を組み合わせることを通じ、グループ全体としての最適化を図り、また、共通化したセキュリティレベルについては継続的にスパイラルアップさせるといった取り組みも並行して実施している。

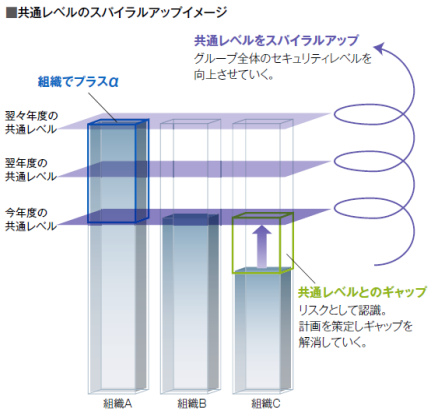

図 1 共通レベルのスパイラルアップイメージ
出典[1]

2-2. 関連先行研究

グループ企業全体を考慮したセキュリティ対策導出に関する先行研究として、長内[長内, 2014 年] [2]らによる検討が挙げられる。そこでは、図 2 に示したような企業間における ICT チェーン内において機密情報や情報システムを共有する場合、委託元から委託先へ情報セキュリティ基準を提示し、基準の順守を要求するのは通常である。しかし、図 3 にあるような ICT チェーンの規模によっては、末端委託先のセキュリティ基準が、委託元が要求するレベルよりも低くなる傾向にある状況をふまえ、ICT チェーンを構成する企業間で情報セキュリティ基準を共有し、評価を可能にする情報セキュリティアーキテクチャを提案した。ここで提案されたアーキテクチャは、情報セキュリティ標準規格を適用することで企業間の情報セキュリティ基準の指標値を統一化し、企業間でセキュリティ情報の共有や分析の自動化・継続的モニタリングする方式を採用しており、その結果、日々増加する IT 機器や脆弱性などのセキュリティ情報に対する分析を自動化し、システム管理者の負荷を軽減させることができるとしている。

表 1　ICT チェーンを構成する企業関係

No.	企業関係	例
1	グループ企業	親会社/子会社/関連会社
2	外部委託	アウトソーシング/ 海外オフショア
3	外部サービス	クラウドサービス利用/ 企業間システム連携
4	共同事業	共同研究/ ジョイントベンチャー

図 2. ICT チェーンを構成する企業関係
出典[長内, 2014 年] [2]

図 3. ICT チェーンの規模と統制強度
出典[長内, 2014 年] [2]

2-3. 考察

最適なセキュリティ対策を導出する上では、リスク分析項目の詳細化といった観点、並びに脅威分析及び対策検討の管理工数削減、プロセス継続性のバランスをとるべく、リスク分析の自動化（システム化）といった動きが主に検討されている。また、グループ企業全体、そして委託元と委託先という関係性において、セキュリティレベルを維持・管理していく為には、様々な観点での『共通化』が必要とされ、そこから継続的な改善活動へと繋げる必要性があることが確認できた。

3. 研究スコープ

グループ企業におけるセキュリティ対策実装にあたっては、極力統一的な対策を施すことが望ましいものの、その規模や環境は会社毎に異なることより、同じ対策を一律に適用することは実質的には困難である。その為、原則各社は各々の判断に基づき対策を行わざるを得ず、結果として、グループ全体として統制がとれていないケースが散見される。また、各社のマネジメントが自社システム環境に対する脅威を十分に理解していないことにより、各社の情報システム部門が導入を提案したセキュリティ対策が支持されず、結果として適切な対策を施せないことが、グループ企業のセキュリティレベル不整合に拍車をかける一因となっていると考えた。そこで、本研究では、グループ企業を対象とし、「全体として整合性のあるセキュリティ対策の実装」を実現するための前段階として、主にマネジメント向けに、現在のセキュリティ対策状況に関して、共通の認識を持つための、セキュリティアーキテクチャ実装状況の可視化手法について提案する。当該可視化手法の検討により、自社グループにおける情報資産が、どこから、どのようにアクセスされており、かつ、それらの情報は、どの程度重要な情報であるか、といった点について、大局的な観点から認知することができ、また、それら情報資産を侵害しうる各種攻撃に対して、現状どのような防御策がとられているかといった点についても、大枠をつかむことができるといった状態を目指す。

4. 情報可視化

4-1. 先行研究

情報可視化に関する先行研究として、金岡[金岡,2013 年][3]らは、リスクに対する可視化手法の分類と、可視化された手法やツールに求められるユーザ知識レベルについて 4 段階の定義付けを行い、それぞれの手法を、分類と知識レベルに合わせ、マッピングを行った。尚、マッピング時においてユーザ知識レベルに関し考慮した点について、以下のように述べている。

『ユーザ知識レベルのマッピングに関しては、そもそもの可視化対象が必要とする技術的な知識の深さは考慮に入れず、単に可視化された結果を扱うことや可視化情報をもとに物事を判断するためにはどの程度の知識が必要かという点

を第 1 に捉え、知識のレベルを踏まえ、可視化自体がその知識レベルの引き下げに貢献しているかを考慮した。』[金岡,2013 年][3] より引用

今回、当該先行研究にて調査・分類された計 72 ケの論文の内、本稿での情報可視化対象ユーザとして想定としているグループ企業のマネジメント層に該当すると思われる知識レベル（知識がない。または経験がない利用者）のユーザ向けに検討された、計 7 ケの論文を調査した。尚、ユーザ知識レベルの分類は、表 1 のとおり、Lv1 から Lv4 までが定義され、レベルが上がるにつれ、高い専門知識を有するユーザに対する可視化手法であることを示唆している。

分類	知識レベル
Lv 1	知識がない。または経験がない利用者
Lv 2	ある程度の知識を持った利用者 専門ではないが、ある程度の技術を持っている
Lv 3	十分な知識を持った利用者 実務に従事している技術者など
Lv 4	高い知識を持った利用者 実務を通じ高い実戦経験を持つエキスパート

表 1:ユーザ知識レベル　引用[金岡,2013 年][3]

今回調査したユーザ知識レベルの情報可視化論文内において、Raja [Raja,2011 年][4]らは、パーソナルファイアウォールの機能が有する警告に関し、物理的なセキュリティのメタファーに基づき可視化するブラウザ表示の検討を行っている。当該検討を行うに至った背景として、パーソナルファイアウォールが、専門的知識を有さない一般ユーザにより利用されるケースが増加傾向にあること、そして一般ユーザは、機器から発信される警告に対する知識レベルの低さ故、警告を全く認知しない、もしくは反応しない傾向にある点を挙げている。そこで、一般ユーザでも機器が発する情報に基づき意思決定を行うことができるよう、その時々におけるリスク度合いを可視化できるような設計を検討すべきといった考えに至った。尚、検討にあたっては、情報を受け取る側のメンタルモデルを考慮したうえで、図 4 のように、既存のパーソナルファイアウォールのブラウザ画面内の色と、描かれている物理セキュリティに関連する絵の内容を通じ、リスク度合いを判別可能としている。

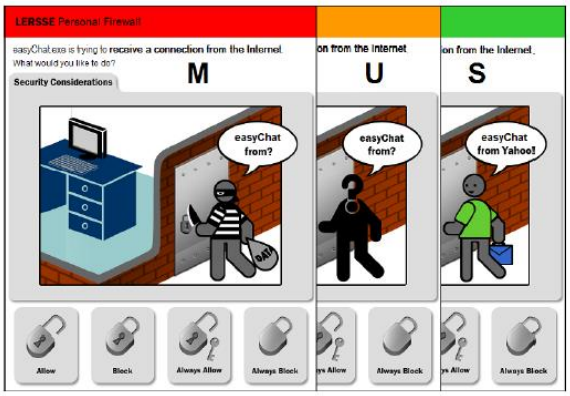

図 4:物理セキュリティのメタファーに基づく警告画面　出典[Raja,2011 年][4]

4-2. セキュリティ対策ベンチマーク

セキュリティ対策状況に関する情報可視化の例として、IPA にて作成されているセキュリティ対策ベンチマーク[5]が挙げられる。これは、Web ページにある質問に答えることを通じ、各組織の情報セキュリティマネジメントシステムの実施状況の充足度を自己評価することを可能とするものである。図 5 は、その診断結果として出力されるレーダーチャートであり、そこでは、以下の項目が主な診断結果として表示される。

- 情報セキュリティリスク指標に応じたグループ別のスコアの比較
- 企業規模別によるスコアの比較
- 業種別によるスコアの比較
- 自組織の最新スコアと過去 2 回分までのスコアの比較

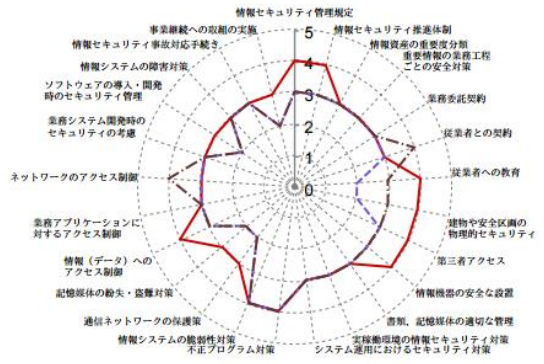

図 5:対策状況の診断結果（サンプル）出典[5]

また、その他にも当該ベンチマークの利活用を促進すべく、具体的な利用ケースを提示した活用集を作成している。[6]そのケースの 1 つに、グループ企業における情報セキュリティ対策の実装状況に関する事例が紹介されている。

その事例では、本社の情報セキュリティ対策は進んでいるものの、グループ子会社の情報セキュリティ対策状況の実態が把握できていない為、その不足箇所について改善を促したいが、調査時における対応負荷、コスト面での負担、そして診断基準が定まっていないといった課題を乗り越えるべく、ベンチマークを利用するといった具体性のあるストーリーとなっている。

4-3. 考察

情報可視化にあたっては、情報可視化対象者の知識レベルを十分考慮することが重要であると考えられ、例えば、知識レベルが低いユーザに対しリスク度合いを評価する為の理解を促進させる為には、専門家に対するアプローチとは異なり、当該ユーザが日常的に理解しうる知識対象を想起させるような形で、リスクを認識させる手法等が有効と考える。

一方、セキュリティ対策ベンチマークは、セキュリティ対策実施状況に関し、極力工数をかけずその実態を把握するといった観点では非常に有用であり、それは当該ベンチマークの利用企業数からも、ある種実証されていると思われる。但し、当該ベンチマークによるチェックがあくまで自己評価にとどまること、活用集での記述では、ベンチマークテスト前後に、文書での裏付けや、ヒアリング、実態調査等を行うことで信頼性を確保するとされているが、その場合、各社での手続如何によっては、当初想定していた作業負荷の軽減、コスト面でのメリットが享受できないものと考えた。その為、各評価項目に対する自己点検によるチェックのみならず、各企業におけるセキュリティ対策状況を各関係者が理解できるような形で可視化し、そこにセキュリティとして検討すべき事項をマッピングした方が、結果に対する信頼性（透明性）と、チェックプロセス全体で必要となる作業負荷、コスト面でのメリットが享受できるものと思われる。

4-4. 検討アプローチ

本検討を行うにあたっては、その前提となる定義を明確に行った上で、詳細を詰めていくこととする。尚、知識レベルの低いユーザ対し、リスク度合いを理解させるうえでの手法については、情報可視化の先行研究としてあった、可視化対象者の既存知識に基づくイメージを想起させるようなアプローチを検討する。

5. 定義

5-1.グループ企業

『グループ企業』に対する、セキュリティ対策実装時のガバナンス体系は一律ではないことより、本稿にて想定するガバナンス体系について、事前に定義付けを行う必要性がある。この点、企業グループにおける情報セキュリティガバナンスモデルに関する分類体系として、リーダー企業に権限を集中したモデル、グループ各社に権限を委譲したモデル、グループ各社に権限の一部を委譲したモデルの 3 ケが挙げられている。[7]本稿においては、中央集権的、な意思決定のもと、グループ全社的な対策を積極的に推進することが比較的実現しやすいモデルよりも、情報可視化による恩恵が期待できる、『グループ各社に権限の一部を委譲したモデル』（図 6）

を念頭におき、検討をすすめていくこととする。

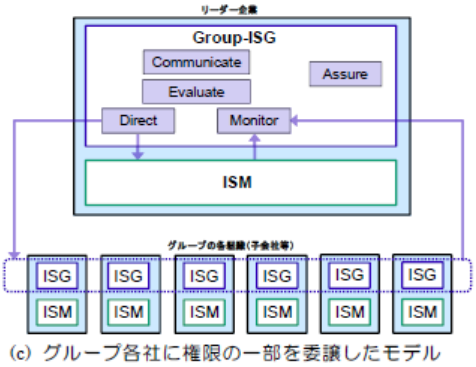

図 6 グループ各社に権限の一部を委譲したモデル　出典[7]

『本モデルは、グループの情報セキュリティに関する権限はリーダー企業(親会社)が管理するが、その一部についてはグループ各社(子会社)に委譲し、それぞれが自らの統制構造を有するモデルであり、各社は自らの組織について一定の範囲で意思決定し統制する裁量が与えられているが、グループ全体としての意思統一が必要なレベルの決定事項については、リーダー企業がグループ各社に方針を示す([7]より引用)』と定義されている。

尚、今回検討するグループ企業の範囲としては、資本関係に基づく企業関係を対象とし、外部委託先等は含めず、また想定する業界、業態についても、特段定めないこととする。

5-2. セキュリティアーキテクチャ

情報可視化(モデル)を行う上で、必要となるセキュリティアーキテクチャに関連する用語について、参考文献[8]の記載に則り、定義付けを行う。

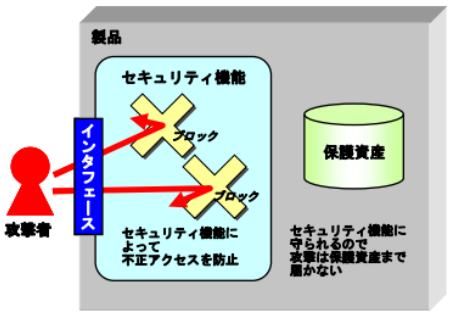

図 7.セキュリティ機能によって、保護資産が守られるイメージ　出典[8]

図 7 に記載のある『セキュリティ機能』は、『利用者の重要データなど保護すべき資産を不正なアクセスから守るための機能や、組織のセキュリティ方針を実現するための機能』を意図する。また、『セキュリティアーキテクチャ』とは、『製品に備わるセキュリティ機能自体が攻撃されたとしても、そのセキュリティ機能を守り正しく働けるようにするための仕組み』と定義されている。そして、セキュリティアーキテクチャが有効に機能することを通じ、攻撃者による保護資産への攻撃を防御することが可能となる。

6. 情報可視化 (モデル)

情報可視化(モデル)の検討にあたっては、ITの専門家でない人でも全体を容易に把握できるよう、既存知識に親和性の高いもので代替できないか検討した結果、『大型商業施設』が適当と考えた。表 2 は、大型商業施設と全体可視化(モデル)の適合例である。

大型商業施設	情報可視化(モデル)
大型商業施設	グループ企業(全体)
テナント	グループ企業(個別)
商品	データ
フロア階層	セキュリティレベル
エレベータ	アクセスレベル

表 2:大型商業施設との適合例

7. 全体まとめ

グループ企業の関係者に対し、セキュリティ対策状況をタイムリーに共有、認識させ、継続的な

見直しサイクルを効率的に回すべく、様々な方策がとられているものの、現時点において最適な手段は見いだせていない状況にあると思われる。そうした中、知識レベルの異なる対象に理解を促す手段として、情報可視化手法が、一定の効果があることが先行研究から確認できた。しかし、情報可視化手法を用いたとしても、単にデータの見える化だけでは不十分であるといえ、対象者の知識レベルと可視化要件を十分考慮したうえで提示されることを通じ、はじめて有効に機能するものと考えられる。

8. 今後の検討内容及び課題

今回提案した情報法可視化（モデル）をベースに検討を行う予定であるが、今後詳細を詰めていく上で、下記 2 点について特に留意する。

第 1 に、情報可視化（モデル）に対して反映する各種情報に関し、どの程度の粒度の情報を盛り込むべきかといった点がある。この点、情報可視化を行うメリットとして、大量の情報を認知させやすくするといった側面はあるが、それも一定の範囲を超えると、逆に理解を阻害する要因となってしまうことより、必要十分といえる範囲を考慮すべきと考える。第 2 に、単純に情報可視化（モデル）の作成のみでは、ユーザ利活用といった観点では不十分であることより、利活用ガイドラインの作成が別途必要と考える。その中には、現状把握から、リスク認識といった一連のプロセスの中で、対象ユーザがどのような点を認知、興味を抱くかといった点について、網羅的に纏められたものを検討している。

参考文献

[1]リコーグループ共通基準
http://jp.ricoh.com/security/management/activity/standard.html
[2] 長内 仁、後藤 厚宏
『企業間における情報セキュリティ連携アーキテクチャの検討』 SCIS2014
[3]金岡 晃、石川 尚樹、緒方 悠人、北島 暢曜、韓 海燕 利用者の知識レベルに応じたリスクの可視化に関する構築 DICOMO2013
[4] Fahimeh Raja、Kirstie Hawkey、Steven Hsu、Kai-Le Clement Wang、Konstantin Beznosov、2011 A Brick Wall, a Locked Door, and a Bandit: A Physical Security Metaphor For Firewall Warnings. In Proceedings of the Seventh Symposium on Usable Privacy and Security（SOUPS'11）、ACM、New York、NY、USA、2011
[5]情報セキュリティ対策ベンチマークの概要
http://www.ipa.go.jp/security/benchmark/benchmark-gaiyou.html
[6]情報セキュリティ対策ベンチマーク活用集
http://www.ipa.go.jp/security/benchmark/benchmark-katsuyou.html
[7] 情報セキュリティガバナンス導入ガイダンス補足編～ 企業グループにおける情報セキュリティガバナンスモデル ～
http://www.meti.go.jp/policy/netsecurity/docs/secgov/2010_IoformationSecurityGovernanceModel.pdf
[8] IPA 技術本部セキュリティセンター
『開発者のためのセキュリティアーキテクチャ解説』
http://www.ipa.go.jp/files/000014502.pdf