4ZD-01

幅広い事業に取り組む大企業グループにおける情報セキュリティベースライン向上策の提案

佐々木　千波留† 後藤　厚宏†
情報セキュリティ大学院大学†

1. はじめに

幅広い事業に取り組む大企業グループでは，多くのグループ企業を抱え，セキュリティインシデントの影響は個社のみならず親会社やグループ全体に及ぶ可能性が高い．

しかしながら，その事業内容の多様さから一律の情報セキュリティ対応を取ることは難しく，またその事業形態により各社に対しての強制力も様々である．

本研究では，親会社として情報セキュリティの観点でグループ全体を俯瞰し，各企業の特性からセキュリティリスク値と対策実態からベースラインを設定し，優先的に対応を行う必要がある会社・対策の抽出を行う．親会社主導で対策を推進し，情報セキュリティベースラインの引き上げと継続的な運用のための仕組みづくりの提案を行う．

2. 先行研究

鈴木[1]は「住友化学グループにおける情報セキュリティの確保に向けて」の中で，国内外に150 社近いグループ会社を抱える大企業グループである住友化学グループの情報セキュリティマネジメントの実装について以下の提案を行っている．

・ISO/IEC 27001:2005，ISO/IEC27002:2006 情報セキュリティマネジメントシステムの PDCA サイクルを親会社とグループ全体で適用するアプローチを提案
・情報セキュリティガバナンス導入ガイダンス[2]におけるベースラインアプローチとグループ企業マッピングの複合型を提案

先行研究はベースラインアプローチとグループ企業マッピングを複合する，より企業特性に合った提案である．ただし，各企業の費用対効果が大前提であり，セキュリティ対策の実施については，各社に依存しておりグループ全体での優先順位は定められていない．

3. 研究提案

先行研究を応用した本研究の提案に基づく PDCA サイクルを図 1 に，研究提案 3 点を以下に示す．

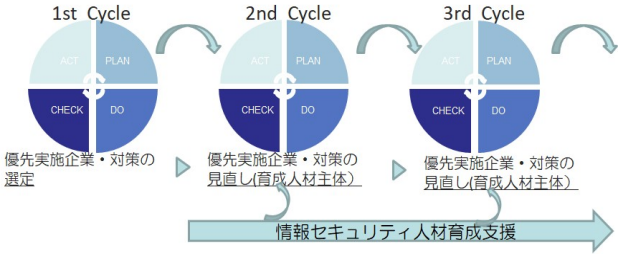

図 1. 情報セキュリティベースライン向上の PDCA サイクル

（1）研究提案 1 ：より優先的に注力する必要のある企業・対策の抽出方法の提案（PDCA 1st Cycle）

よりリスク値が高い企業・対策の洗い出しを行うことを目的として，図 2 に示す手順のとおり，①企業の特性(業種，規模等)に応じた分類→②対応するリスク値の設定→③セキュリティ対策の実態調査→④リスクと実態調査のマッピング(図 3)→⑤ベースラインの設定(図 4)を行う．

図 4 のベースラインの設定は，図 3 のマッピング結果に基づき，各企業グループにてベースライン設定を決定する．

Copyright ©2020 Information Processing Society of Japan.
All Rights Reserved.

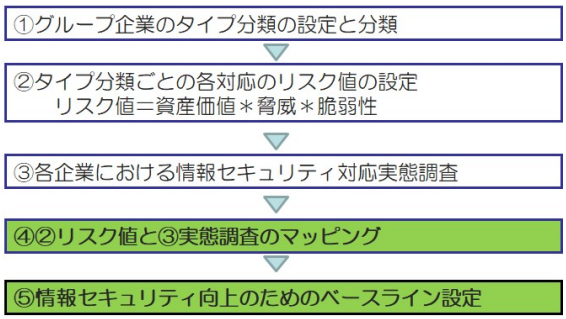

図 2. 情報セキュリティ対策優先順位付け手順

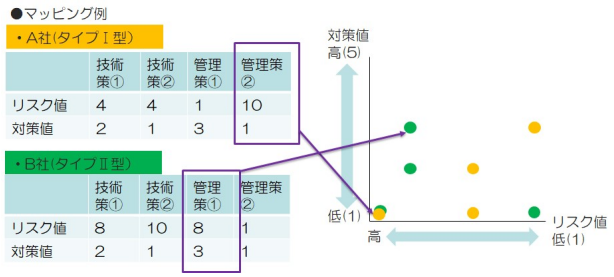

図 3. 各社のリスク値と対策値のマッピング

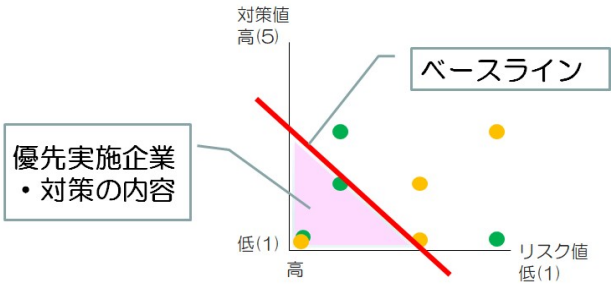

図 4. 情報セキュリティベースラインの設定

(2) 研究提案 2：再度優先的に注力する必要のある企業・対策の見直しサイクル(PDCA 2nd Cycle ～)

PDCA 1st Cycle の結果・市場動向等を鑑み，図 2 に示す手順の再見直しを実施する．変動要素として，資産価値(CIA)・脅威・脆弱性の変化などがあげられる．

(3) 研究提案 3：情報セキュリティ人材の育成支援策の提案(PDCA 2nd Cycle～)

公的機関の情報セキュリティ人材育成戦略を参考に人材育成支援策の検討を行った．情報セキュリティベースラインの引き上げのためには以下の対応が必要である．

①各グループ企業の実態に即した情報セキュリティ教育の実施

②戦略マネジメント層の育成

上記①，②の支援策として，情報セキュリティ専門部隊をもつグループ会社から教育・訓練・人材育成・コンサルティング等のメニュー化を行う．

4. まとめと今後の予定

本稿では，幅広い事業に取り組む大企業グループにおける情報セキュリティの可視化，サイクルを提案することで，ベースライン向上の可能性を示した．

今後は本提案について，複数の子会社・関連企業を持つ重要インフラに属する大企業グループ 1 社に対して行った実態調査を基に，モデルケース検証を進めていく予定である．また，グループ分けに基づく数社に対して，提案内容のヒアリングを予定している．

引用文献

[1] 鈴木龍大：住友化学グループにおける情報セキュリティの確保に向けて，住友化学 技術誌 2009-II（2009 年 11 月 30 日発行）P67～76

[2]経済産業省(平成 21 年 6 月)
情報セキュリティガバナンス導入ガイダンス
https://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf

Proposal of measures to improve information security baselines for large corporate groups engaged in a wide range businesses

†Chiharu SASAKI, Atsuhiro GOTO
†Graduate school of Information Security

Copyright ©2020 Information Processing Society of Japan.
All Rights Reserved.