2018 年 6 月 11 日
損害保険ジャパン日本興亜株式会社
SOMPOリスケアマネジメント株式会社
株式会社日立製作所

セキュリティインシデントの発生率と損害額を定量化するサイバーリスク診断手法の開発
～産業・重要インフラ分野における適切なセキュリティ投資判断を支援～

損害保険ジャパン日本興亜株式会社（本社：東京都新宿区、社長：西澤敬二、以下「損保ジャパン日本興亜」）とSOMPOリスケアマネジメント株式会社（本社：東京都新宿区、社長：布施康、以下「SOMPOリスケア」）、株式会社日立製作所（本社：東京都千代田区、執行役社長兼CEO：東原 敏昭、以下「日立」）は、産業・重要インフラ分野における適切なセキュリティ投資判断の支援を目的に、セキュリティインシデントの発生率と損害額を定量化する共同研究を実施し、「セキュリティ診断システム」と「損害発生モデルシミュレータ」の開発および技術検証を行いました。

今後、3 社は、新たな保険商品やセキュリティサービスの開発も視野に入れ、今回開発した定量的診断手法のさらなる高度化に取り組んでいきます。

1. 背景

近年、サイバー攻撃の脅威は深刻化しており、その対象は工場・プラントなどの産業設備だけでなく、エネルギー、交通、金融といった社会を支える重要インフラ*1 にも拡がるなど、さまざまな分野でサイバーセキュリティ対応の重要性が増しています。一方、セキュリティインシデントは発生リスクや投資対効果（ROSI*2）の定量的な算出が困難なため、事業者においてはどこまでコストをかけて対策をとるべきかの判断が難しいと言われています。

このような背景をふまえ、損保ジャパン日本興亜とSOMPOリスケア、日立の３社は、日本の産業・重要インフラにおけるサイバーセキュリティ対応の促進を目的に共同研究を実施しました。

2. 共同研究の概要・成果

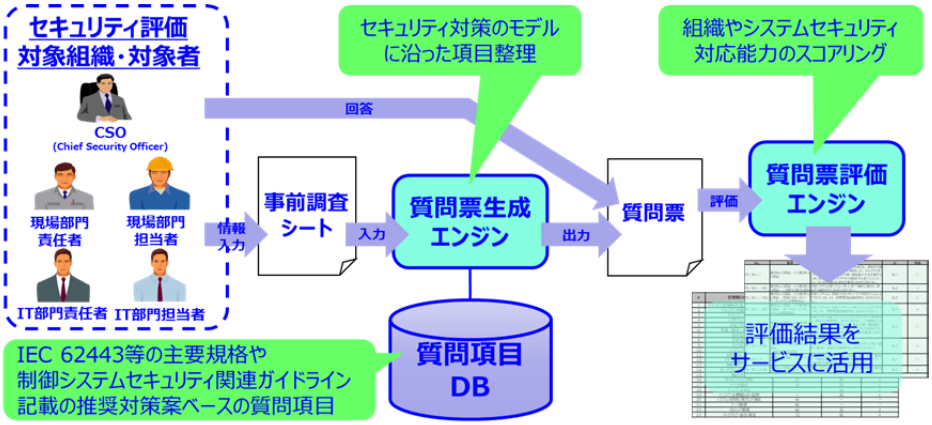
今回の共同研究では、損保ジャパン日本興亜およびSOMPOリスケアが損害保険事業で培ったリスク評価技術と、日立が産業・重要インフラ分野のシステム構築で培ったセキュリティ対策技術や脆弱性リスクの評価手法を組み合わせ、サイバーリスクの総合的な定量的診断手法の開発を行いました。具体的には、企業のセキュリティ対策状況を診断するための各種規格に対応した「セキュリティ診断システム」と、システム構成や対策状況に応じたサイバーリスクを損害額として定量的にシミュレーションできる「損害発生モデルシミュレータ」の開発および技術検証を実施しました。

（1）セキュリティ診断システム

組織の経営層・システム管理者・現場担当者それぞれに対する質問項目を生成し、その回答に基づいたセキュリティ対策レベルを評価・スコア化するシステムのプロトタイプを開発しました。

NIST Cybersecurity Framework(CSF)[*3]や IEC 62443[*4]など各種セキュリティ標準規格で求められている項目をデータベース化するとともに、事前調査に基づいて生成される質問票では対象者ごとに回答いただく質問を再構成します。

本システムにより、企業における自社のセキュリティ対策レベルの確認作業が容易になるほか、各種規格を網羅した質問に対し適切な対象者に回答いただくため、より正確に対策レベルを評価することが可能となります。

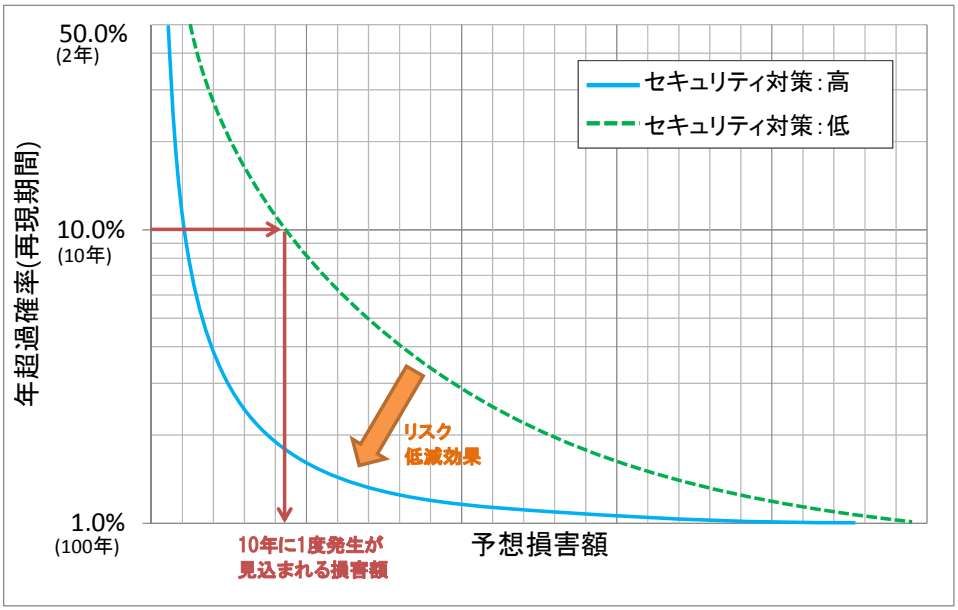


［セキュリティ診断システムの利用イメージ］

(2)損害発生モデルシミュレータ

本共同研究では、大規模生産工場を想定し、サイバー攻撃による損害発生リスクをシミュレーションで定量化する検証を行った結果、システム構成やセキュリティ対策状況に応じたサイバーリスクを、セキュリティインシデントの発生率と損害額として算出できることを実証しました。

本シミュレータとセキュリティ診断システムを組み合わせて活用することで、対策レベルにより損害発生リスクがどれだけ変動するかを可視化することも可能となります。



［予想損害額と1年間に予想損害額を超過してしまう確率の関係を示す曲線］

3. 今回開発した定量的診断手法の活用例

（1）サイバーセキュリティ対策の費用対効果の可視化

セキュリティ対策への投資を検討する際に、対策の必要性ならびにその費用対効果、対策導入の優先順位に関する判断材料を提供することで、適切なセキュリティ投資をサポートします。これにより、適時適切なセキュリティ対策の打ち手を検討する一助となります。

（2）サイバーセキュリティに対するリスクファイナンスの最適化

従来、サイバー保険検討の際の適切な保険金額の設定は、同種同規模の企業における罹災（りさい）事例の情報や取り扱う個人情報件数などから検討されることが一般的ですが、本技術により、現行のシステムをもとにした定量的なリスク評価を実施することで、各企業の実情に合わせた適切な保険金額の検討が可能となり、保険手配の最適化を図ることができます。

4. 今後について

今後 3 社は、新サービスの開発など新たな協創ビジネスも視野に入れ、セキュリティ診断システムの共同利用や損害発生モデルシミュレータの適用分野拡大など、今回開発した定量的診断手法のさらなる高度化に取り組んでいきます。

また、今回の成果は、3 社それぞれの事業領域でも活用していきます。

損保ジャパン日本興亜は、サイバーリスク定量化手法を活用し、新しいサービスや保険商品を検討していきます。また、SOMPOリスケアは、2018年1月から開始したサイバーセキュリティ事業において、サイバーリスク定量化手法を活用したコンサルティングサービスを提供していきます。

日立は、本成果を活用し、セキュリティ投資対効果を考慮した適切なセキュリティソリューションを提供するとともに、今後もさまざまなステークホルダーとのオープンな協創関係を通じて、サイバーセキュリティ強化に取り組んでいきます。

*1 NISC（内閣サイバーセキュリティセンター）が「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」において定めている分野であり、「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」および「石油」の 13 分野。

*2 ROSI：Return on Security Investment

*3 NIST Cybersecurity Framework：米国国立標準技術研究所（National Institute of Standards and Technology）「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」

*4 IEC 62443：国際電気標準会議（International Electrotechnical Commission）の制御システムセキュリティ基準

以上