仮　訳

保険監督者国際機構

保険セクターにおける

サイバーリスクに関する論点書

２０１６年８月

IAIS について

保険監督者国際機構（IAIS）は、およそ 140 カ国の 200 を超える管轄区域からの保険監督者および規制者である任意の会員からなる組織である。IAIS の使命は、保険契約者の利益と保護のために、公正、安全かつ安定した保険市場を発展させかつ維持すべく、効果的でグローバルに整合的な保険市場の監督を促すこと、およびグローバルな金融安定に貢献することである。

IAIS は 1994 年に設立され、保険セクターの監督のための原則、基準および他の支援する資料の策定、ならびに、それらの実施を支援する責任を有する国際的な基準設定主体である。また、IAIS はメンバーに対して、保険監督および保険市場に関するメンバーの経験および見解を共有するための議論の場を提供する。

IAIS は、他の国際的な金融政策立案者および監督者または規制者の協会と自身の取組みを調整しており、また、世界的な金融システムの形成を支援している。特に、IAIS は、金融安定理事会（FSB）のメンバーであり、国際会計基準審議会（IASB）の基準諮問会議のメンバーであり、および保険へのアクセスに関するイニシアティブ（A2ii）のパートナーである。また、その結集された専門知識が認められ、IAIS は、G20 のリーダーおよび他の国際的な基準設定主体から、保険の論点のみならずグローバルな金融セクターの規制および監督に関する論点について、定期的にインプットを求められている。

論点書は、特定のトピックについての背景を提示し、特定のトピックに関する現在の実務、実際の事例またはケース・スタディを示し、ならびに／または、関係する規制上および監督上の論点および課題を特定する。論点書は主として説明的であり、監督上の資料を監督者がどのように導入するべきかの期待を生むことを意図してはいない。論点書は、基準策定の準備作業の一部となることが多く、IAIS による今後の取組みへの提言を含む可能性がある。

本文書は、金融犯罪タスクフォース（ＦＣＴＦ）が作成した。

本出版物は IAIS のウェブサイト(www.iaisweb.org)上で入手可能。

保険セクターにおける
サイバーリスクに関する論点書

目次

1. はじめに

1. サイバーリスクの高まりおよびサイバー犯罪の顕著な高度化を受け、サイバーセキュリティにまつわる懸念は、グローバル経済のすべてのセクターにおいて高まっている。保険会社としては、サイバーセキュリティインシデントの発生は、事業の継続を毀損し、営業上の機密および個人情報の保護に支障をきたし、さらには、保険セクター全体に対する信頼を損なう恐れがある。IAISは、サイバー脅威および保険セクターにおけるサイバーセキュリティについての認識の度合およびリスク対策への監督アプローチは、管轄区域ごとに様々であることを認識した。

2. こういった状況が、サイバーリスクの評価および軽減の推進における保険監督者の関与を含め、保険セクターにおけるサイバーセキュリティの問題を検討するよう、IAISを促した。

3. 消費者の情報に関わる、最も広く知られているサイバーセキュリティインシデントの多くは、小売業者に影響を及ぼすものであるが、保険会社を含む金融サービス分野の企業も被害を受けている。

4. すべての保険会社は、規模、業務の複雑性もしくは事業の種目を問わず、膨大な個人情報、取り扱いに注意すべき健康状態に関わる情報を含む保険契約者の機密情報を収集、保管し、また多様な第三者（例えば、各種サービス提供会社、仲介人、再保険会社）との間で共有する。保険会社が保有するデータの機密性、完全性および利用可能性の保護は、根幹的に重要である。サイバー犯罪を通じ保険会社から得られた情報は、金銭を得る目的のゆすり、なりすまし、知的財産の侵害、またはその他の犯罪活動に使用される可能性がある。過失または故意による機密データの流出は、保険セクター関係者に風評被害をもたらし得るのみならず、保険契約者に長期にわたる深刻な影響を及ぼし得る。同様に、保険会社の重要なシステムに対する悪質なサイバー攻撃は、事業の継続を妨げる可能性がある。

5. 2015年、IAISは、保険業界のサイバーリスク、サイバー脅威対策のメンバーの取組み、また現在用いられているもしくは検討段階のサイバーセキュリティに対する監督上のアプローチについて、メンバーの認識についてアンケート調査を実施した。メンバー当局によるアンケート調査への回答は、本論点書の作成において参考とされた。その他にも、本文書において参照されている文書ならびに、メンバー当局、保険会社、サイバーセキュリティの専門家およびその他の有識者との意見交換の結果が含まれている。その他の参照資料は付属書3に示されている。

6. 本論点書の目的は、サイバーリスクに対処するために現在実施されているおよび検討されている監督上のアプローチを含め、サイバーリスクが引き起こす諸課題への保険会社および監督者の意識を高めることである。本文書は、論点書として、背景情報をまとめ、現在の実際の取組みについて説明し、事例を特定し、関連する規制・監督上の諸課題について考察する。本文書は、保険セクターに対するサイバーリスクおよびそのようなリスクの軽減に焦点を当てる。本文書は、より広いＩＴセキュリティ、サイバー保険（保

険会社による当該種類の保険商品の販売または引受）または監督者が巻き込まれるサイバーセキュリティインシデントのリスクには触れておらず、これらは重要なトピックだが本論点書の射程に含まれない。

7. 本文書は、主に説明を意図しており、監督上の期待を形成することは意図していない。しかし、サイバーリスクへの対処において監督者を支援するための、より具体的なIAIS文書の作成の必要性が明らかにされるかもしれない。

2. サイバーリスクの概要

8. 「サイバーリスク」という用語の標準化された定義はない。CROフォーラムは、「サイバーリスク」の意味するところについて、「インターネットおよび電気通信ネットワークのようなテクノロジー・ツールを含む、電子データの利用およびその伝送によって生じるあらゆるリスク。それはまた、サイバーセキュリティインシデント、データの不正利用により行われた詐欺、データの保存によって発生するあらゆる法的責任、ならびに、個人に関するもの、企業に関するものあるいは政府に関するものであれ、電子的情報の利用可能性、完全性および機密性から発生しうる物理的被害も含む。[1]」として幅広く説明している。証券監督者国際機構の決済・市場インフラ委員会のワーキング・グループは、サイバーリスクを「組織の情報資産、コンピュータおよびコミュニケーションの領域内で発生し得る事象の可能性、ならびにその事象により組織に対して生じる結果との組み合わせ。」と説明する。[2]

9. サイバーリスクから生じる有害事象を記述するものとして、多様な用語が使用されている。そういった用語には、米国連邦金融機関検査協議会（FFIEC）が、「コンピュータ、コンピュータ・システム、または電気通信ネットワークに損害を与える、妨害する、またはそれらへの不正アクセスを得る試み。コンピュータ環境またはインフラを妨害、無効化、破壊、または悪意を持って制御すること、もしくは、データの完全性を破壊すること、または統制された管理下の情報を盗み出すことを目的として、企業によるサイバースペースの利用を標的とした、サイバー空間を介した攻撃」[3]と定義する「サイバー攻撃」が含まれる。関連して「サイバーインシデント」は、FFIECによれば「情報システムまたはその中に存在する情報への実際のまたは潜在的な負の影響に結びつく、コンピュータ・ネットワークの利用を通じて行われた行動」と定義されている。

10. 本文書では、「サイバーセキュリティインシデント」という用語は、サイバー攻撃およびサイバーインシデントの両方の意味を含んだ広い意味で使用されている。

11 世界経済フォーラムは、グローバルリスクレポート2015において、グローバル経済が直面している10大リスクの一つとして、データ詐欺、サイバーセキュリティインシデントまたはインフラの機能停止等の形態で現れるテクノロジーの進展に係るリスクを挙げている[4]。サイバーリスクは、各業界が認識するリスクに関する2015年のレポートにおいて、調査対象とされた保険会社からは第4位（米国および英国の保険会社においては第1位）に挙げられている[5]。

---

[1] CRO フォーラム 「サイバーリスクの課題と保険の役割」パラグラフ 3（2014 年 12 月）、
http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/で参照可能。
[2]証券監督者国際機構の決済・市場インフラ委員会, 市中協議文書「金融市場インフラにおけるサイバー攻撃耐性に関する指針」（2016 年 6 月）https://www.bis.org/cpmi/publ/d146.htm で参照可能。
[3] 米国連邦金融機関検査協議会（FFIEC） 「サイバーセキュリティ評価ツール用語集」（2015 年 6 月）、
http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_C_Glossary_June_2015_PDF5.pdf で参照可能。
[4] 世界経済フォーラム「グローバルリスク 2015」（2015 年）、
http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf で参照可能。
[5] PWC および CSFI（フィナンシャルイノベーション研究センター）、「インシュランス・バナナ・スキン 2015：保険会社が直面するリスクに関する CSFI 調査」パラグラフ 1（2015 年 6 月）
http://static1.squarespace.com/static/54d620fce4b049bf4cd5be9b/t/55dde0fce4b0dff05004146c/1440604412304/2015+Insurance+Banana+Skins+FINAL.pdf.で利用可能。

12. アリアンツ社は、サイバーリスクの概要として下記の主要な傾向を挙げている[6]。
- 相互関連性の高まりおよびサイバー犯罪の「商業化」により、データ侵害を含め、インシデントの頻度および深刻性が増大している。
- データ保護に関する法令は、グローバルに厳格化が進むだろう。将来的には、さらなる通知の発出およびデータ侵害への巨額の罰金の設定が想定される。
- 事業の中断（BI）、知的財産の窃取やサイバー恐喝のリスクが高まっている。BIコストは、データ侵害による損失に等しいか、または上回るかもしれない。
- 業界の統制システムにおける脆弱性は、重大な脅威を引き起こす。

13. こういった脈絡において、本論点書中の本項目のこれ以降の部分では、最近のサイバーセキュリティインシデントの類型、頻度、深刻性およびコストに関するデータを概観する。

サイバーセキュリティインシデントの類型

14. サイバーセキュリティインシデントは、様々な形で発生しており[7]、このことは、サイバーセキュリティインシデントの中で最も多く報告されているデータ侵害の類型が、様々な発生形態を取ることから確認できる。ベライゾンは、2015年のレポートで[8]、データ侵害の大部分が以下の原因の１つ以上から生じていると結論づけた：販売時の侵入、クライムウェア（犯罪目的で使用されるマルウェアの形式）、サイバースパイ、内部関係者による悪用およびWebアプリケーションによる攻撃。その他の類型のサイバーセキュリティインシデントは、様々な過失、物理的な盗難や紛失、支払時のクレジットカードのスキミング、もしくはサービス妨害攻撃（DDoS）から発生している。これらのサイバーセキュリティインシデントは、多くの場合、データ侵害に関連する形で他の形態での損失を招くことがある（例えば、知的財産の盗難）。

15. 大抵の場合に「ランサムウェア」として知られるクライムウェアの形態で実行されるサイバーを利用したゆすりは、ハッカーが事業用または個人用のコンピュータに侵入してデータを勝手に暗号化し、それを復元するための身代金を要求するというもので、顕著に見られるサイバーセキュリティインシデントである[9]。特定の種類のランサムウェアは、実に巧妙に機能し、被害者は、ランサムウェアの攻撃対象とされなかった機器上にデータのバックアップコピーを作成していない限り、身代金を支払わなければデータを復元することができない[10]。

サイバーセキュリティインシデントの頻度、被害状況、およびコスト

16. サイバーセキュリティインシデントの発生頻度は高まっている。2014年秋、プライス

---

[6] アリアンツグローバルコーポレート&スペシャルティ、「サイバーリスクに関するガイド」（2015 年 9 月）
[7] データ侵害は「許可されていない個人によって、高度にもしくは厳しく保護されたデータがコピー、転送、閲覧、盗用されるセキュリティ濫用」のことである。米国保健福祉省児童家庭局、「情報に関する覚書 ACYF-CB-IM-15-04」（2015 年 6 月）を参照 http://www.acf.hhs.gov/programs/cb/resource/im1504.で利用可能。
[8] ベライゾン、「データ侵害調査レポート」（2015 年） p 32。
[9] デブリン・バーレット、「吹っ掛けるハッカーへの身代金の支払い」ウォールストリートジャーナル（2015 年 11 月）
[10] 同上

ウォーターハウスクーパース（PwC）による、企業幹部を対象にして9700名が参加した年次情報セキュリティ調査は、前年に検出されたサイバーセキュリティインシデントが約4300万件すなわち一日当たりおよそ10万件の攻撃となり、2013年度の調査で報告された発生件数を48%上回っていると報告した[11]。2015年のPwC調査に報告されたサイバーセキュリティインシデントの数は、年度比でさらに38%増加した[12]。さらに、報告されていないかまたは検出されていないサイバーセキュリティインシデントは、はるかに多く存在すると見込まれる[13]。マルウェアを通じた攻撃は、ますます広がっている。すべてが目論見を達成する訳ではないが、世界中の機関において、日々毎秒5つのマルウェア攻撃が発生している。[14]

17. サイバーセキュリティインシデントは、あらゆる規模の企業で発生するが、中小企業は、特に脆弱である可能性がある。 NetDiligenceによる2015年の調査では、例えば、売上高が5000万ドル未満の企業で、最も多くのインシデント（全体の29パーセント）が発生し、次点で売上高20億ドル未満の企業での発生が続く（全体の25パーセント）とされる。[15]

18. 最も多く報告されているサイバーセキュリティインシデントの形態であるデータ侵害の深刻度は、管轄区域によって異なっている。Ponemon研究所（Ponemon）のレポートが対象とした国・機関では、データ侵害により喪失もしくは窃取されたデータの平均件数は約1.9万件から3万件であり、米国、インドそしてアラブ諸国で最も高い平均値を示した[16]。

19. サイバーセキュリティインシデントは、高いコスト負担を生じさせる。例えば、戦略国際研究センターとMcAfeeは、サイバー犯罪が世界経済に年間4000億ドル以上のコストを発生させていると試算している[17]。

20. 最近、ロイズとケンブリッジ大学リスク研究センターは、米国の送電網を標的とする仮想のサイバー攻撃に伴う経済的損失を分析するレポート発表した。同報告書は、停電

---

[11] PwC、「つながった世界におけるサイバーリスク管理：2015 グローバル情報セキュリティ調査から得られた重要な知見」パラグラフ 7（2014 年 9 月）、 http://www.pwccn.com/home/eng/rcs_info_security_2015.html で利用可能。

[12] PwC、「サイバーセキュリティにおける転換と変革：2016 グローバル情報セキュリティ調査から得られた重要な知見」パラグラフ 2（2015 年 9 月） *available at* http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.で利用可能。

[13] 「マルウェアは、事情を理解した上での所有者による同意（informed consent）なくコンピュータ・システムに秘密裏にアクセスするために設計されている。この表現は、悪意ある、侵入する、または不快なソフトウェアまたはプログラム・コードを意味して用いられる一般的な用語（悪意のあるソフトウェア（malicious software）の省略）である。マルウェアは、コンピュータ・ウイルス、ワーム、トロイの木馬、スパイウェア、不正なアドウェア、ランサムウェア、クライムウェア、多くのルートキット、および他の悪意ある、望まれないソフトウェアまたはプログラムを含む。 FFIEC、「サイバーセキュリティ評価ツール用語集 」

[14] ベライゾン、「データ侵害レポート 2015」 p 21　ベライゾンの報告書によると、無数のマルウェア攻撃がファイアウォール、検出システム（IDS）防御システム（IPS）、スパムフィルター等の統制によって阻止された。

[15] Net Diligence、「サイバー犯罪スタディ」 p 22（2015 年）

[16] Ponemon 研究所、「 データ侵害によるコストの研究：グローバル分析」p8（2015 年 5 月）
11 カ国（米国、英国、ドイツ、オーストラリア、フランス、ブラジル、日本、イタリア、インド、アラブ首長国連邦、サウジアラビア、およびカナダ）を代表する 350 の企業が参加。
参加団体は、少ないケースで 2200 件から多い場合で 101000 件ものデータ侵害を経験していた。次のセクションで説明するように、データ侵害への対応に掛るコストも国によって異なっている。

[17]戦略国際研究センターと McAfee、ネットの損失:サイバー犯罪におけるコストのグロール試算（2014 年 6 月）
http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.で利用可能。

被害の状況により、全体として2430億ドルから1兆ドル（内214億から711億ドルが保険引受け損失）以上の損失を予測した[18]。

21. Ponemonは、データ一件当たりの喪失および盗難による世界平均コストは154ドルで、2014年のデータ侵害による世界平均コストは379万ドルであったとまとめた。発生したこれらのコストは、地域により異なる。インドでは、一件当たり平均56ドルであったのに対し、米国では一件当たり平均217ドルであった。コストは業界別でも異なっており、医療関係企業（一件当たり平均363ドル）、教育関係企業（一件当たり平均300ドル）、製薬企業（一件当たり平均220ドル）、金融関係企業（一件当たり平均215ドル）が、データ侵害に関連して最も高いコストを負担した。小売業における侵害による一件当たりの平均コストは、2014年の一件当たり平均105ドルから2015年には一件当たり平均165ドルと、昨年に比べ、劇的に増額した[19]。

22. Ponemonによれば、これらのコストは、次の４つのカテゴリーの一つに入ると考えられる：（ｉ）検出と拡大、（ii）通知、（iii）発生事後対応および（iv）事業喪失である。2013年、2014年、および2015年において、事業喪失（予想外の客離れ、風評被害および信用低下を含む）は、データ侵害に関係した最大のコスト要因だった[20]。

[18] ロンドン・ロイズ、新興リスク：ビジネスブラックアウト—米国発電所におけるサイバー攻撃（2015 年 6 月）https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf. で利用可能。
レポートは（米国対テロ保険法は発動されないと想定する）、保険引受損失は様々な業種に及び 50 億ドル以上（リスクカバー費用や財産等）と試算。
[19] Ponemon 研究所、「 データ侵害によるコストの研究：グローバル分析」p1、2、9（2015 年 5 月）。これらの結果は、Penemon 研究所がおよそ 10 万件を下回るデータ侵害を経験した会社を対象に実施した調査を基にする。
[20] Ponemon 研究所、「 データ侵害によるコストの研究：グローバル分析」パラグラフ 17（2015 年 5 月）

3. 保険セクターに対するサイバー脅威

23. 一般論として、保険セクターは、内部ソースおよび第三者を含む外部ソースからのサイバーリスクに直面している。保険会社は、個人が特定可能な情報を含む膨大な量のデータを収集、処理および保管する。保険会社は、投資、資金調達、および債券発行業務を含む複数のチャネルを介して、他の金融機関と関係している。保険会社は、サイバーセキュリティに影響する可能性のある合併・買収または企業構造の変更を実施する。保険会社は、多岐にわたる業務を外部に委託し、これによりサイバーリスクが増大し、または時にはこれが減少する。

近時IAISメンバーによって確認された保険会社に関わるサイバーセキュリティの事例

ITの全体状況を把握していないことまたは十分に把握できていないこと

すべての保険会社がIT機器および使用を許可されているソフトウェアの目録を備えるべきであるが、現行の記録方法においては、ITシステム、アプリケーションおよびその機器間におけるデータフローは認識されていないだろう。データフローが、保護レベルの高いシステムとセキュリティレベルの低い保護のシステムの間に存在する場合は、サイバー犯罪者は、安全性が高い方のシステムへもアクセスを得ることができる可能性がある。

ユーザー権限についての不十分な統制プロセス

ユーザーIDの管理に関し、2つの典型的な事例がある：（1）ユーザー権限付与手続きにおける統制の失敗（即ち、ユーザーに対し、必要とされているよりも強いシステム権限を持たせてしまう）、(2) アカウントがもはや特定のシステム権限を必要としなくなる時期の見極めの失敗。どちらの失敗も、内部関係者による濫用およびサイバーリスクにつながりうる。自動的にID認証管理をチェックすることができる市販のソフトウェアがある。

管理ユーザーのアカウントへの不正アクセス

十分な統制を講じずに、「管理ユーザー」アカウント（他の大多数のユーザーに与えられている権限を超える権限を有するアカウント）に対して、従業員による直接のアクセスを認めることは、保険会社にリスクをもたらす。まず一つには、ハッカーが管理ユーザーへのアクセス権限を持つ従業員のアカウントへのアクセス権限を取得した場合、ハッカーは、管理ユーザーアカウントを通じて、システム全体を巧みに制御することができる（それには、データの書き換え、ログファイルの削除、または検出機能を無効化することによる、犯罪行為の隠ぺいを含む）。次に、管理ユーザーアカウントを広く使用することにより、システム全体に影響を与える想定外のエラーを招く可能性がある。

24. 保険セクターのサイバーセキュリティインシデントから生じ得る有害な結果には、例えば、機密または機微な、事業、消費者または第三者のデータの逸失または改変、物理的逸失（例えば機器の損傷）、財産上の損害および風評被害が含まれる。これらの一部を以下で取り上げる。

機密データの喪失

25. 保険会社によって収集および保管された、保険契約者や、ある場合には第三者の個人的な健康情報を含む個人を特定できる情報には、名前、生年月日、社会保障番号、住所およびメールアドレス、医療識別番号ならびに収入といったような雇用に関するデータを含む可能性がある。個人の健康に関する記録は、保険会社に対するゆすり、詐欺およびなりすましのためのツールとして、闇市場においてとりわけ高い価値を持ち、こうした情報を収集する保険会社は犯罪者に狙われやすくなる。

26. 事業保険契約者にとっては、保険会社は、外国からの産業スパイにとって価値のある情報を収集する可能性がある。サイバー保険商品を例にとると、保険会社は、ハッカーやその他のサイバー犯罪者にとって価値のある保険契約者のネットワークセキュリティに関する制御および他のサイバー攻撃耐性に関わる情報を保持するだろう。また、機密情報の喪失は、保険契約者の貴重な知的財産権を侵害し得る。

事業の中断

27. すべてのサイバーセキュリティインシデントが、データ侵害を伴う訳ではなく、通常の事業運営の中断を招き得るサイバー攻撃もある。例えば、ソニー・ピクチャーズが見舞われたサイバーセキュリティインシデントでは、電子メール、電話帳、ボイスメール、およびコントラクトのひな型等の業務上の記録を含む社内ネットワーク全体が破壊されたと報告された[21]。保険会社に対するそうした悪意ある攻撃は、甚大な被害および莫大な復旧コストを必要とする。

風評被害

28. 保険事業の基盤は、保険会社が収集した情報が保護されるという信用、あるいは支払い請求が適宜適切に支払われるという信用といった契約者からの信用である。保険会社が契約者に係る機密情報を漏えいさせるデータ侵害に見舞われた場合、そういった信用は揺らぐだろう。同様に、保険会社が時宜にかなった支払いを不能にするもしくは事業運営を中断させられる攻撃に見舞われた場合にも、信用は揺らぐだろう。風評リスクは、保険セクター全体に波及し、消費者、契約者、投資家、格付け機関およびビジネスパートナーからの信頼を損なう可能性がある。

[21] アマンダ・ヘス、「ソニー事件の裏側」Slate 紙（2015 年 11 月 22 日）
http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html で利用可能。

4. 保険セクターにおけるサイバーセキュリティインシデントの事例

29. 保険セクターは近年、複数の米国医療保険会社における広く知られたデータ侵害を含む、多種にわたるサイバーセキュリティインシデントを経験している。これらサイバーセキュリティインシデントの事例を以下に挙げる。

30. 2015年、アンセムブルークロスブルーシールドとプリメーラブルークロスは、データ侵害に遭い、クレジットカード情報や、医療情報を含む個人を特定可能な情報が危険に晒された[22]。このデータ侵害は、米国人口の四分の一に相当する最大9100万人の契約者情報を流出させた可能性がある[23]。これらの保険会社は、風評被害および訴訟費用を低減するために迅速に対応せねばならなかったが、今回のデータ侵害によって最終的に保険会社がどれほどの損害を負担することになるかは現在も不明である。

31. もう一つの米国での事例では、ノースダコタ州によって運営されるデータサーバが危険に晒され、雇用主および被雇用者がオンライン上で作成していた4.3万件の事故報告書および1.3万件の給与報告書を含む労働者の補償請求に係る多岐にわたる個人情報が流出した可能性がある。報告によれば、医療情報および請求文書は流出していなかったが、個人の氏名、社会保障番号、生年月日、傷害の詳細、事故の詳細、雇用主の氏名および雇用主の住所に流出の恐れがあったとされる[24]。

32.「DD4BC」として知られているサイバーを利用したゆすりのグループは、ヨーロッパ、オーストラリア、カナダ、米国の金融機関を含む様々な企業をサービス妨害（DDoS）攻撃による脅迫の標的として、金銭をゆすり取ろうとしていた[25]。DD4BCは、標的が指定された期限までに身代金を支払わない限り、DDoS攻撃を発動すると脅し、ビットコイン（暗号通貨）で支払われる様々な額の身代金を要求した。二つのドイツの保険グループは、2015年半ばにこの種の攻撃を経験し、40ビットコインを支払わない限り、企業のWebサーバ上でDDoS攻撃を行うとの脅しを受けたという。保険会社は、今回の事例におけるゆすりによる被害が軽微にとどまると評価し、要求を拒否したが、攻撃がもっと重要なシステムに集中していた場合、これらのインシデントは、はるかに深刻だった可能性がある。

33. 2015年、フランスの保険会社の内部監査チームによる侵入テストにおいて、会計ツールへの不正アクセスが発生していたことが見つかった。この事例ではそれ以上の影響は

---

[22] アンセム、「対アンセムサイバー攻撃関連文書」
https://www.anthem.com/health-insurance/about-us/pressreleasedetails/WI/2015/1813/statement-regarding-cyber-attack-against-anthem で利用可能。プリメーラブルークロス、「サイバー攻撃の標的となったプリメーラ」（2015 年 3 月 17 日）https://www.premera.com/wa/visitor/about-the-cyberattack/?WT.z_redirect=www.premera.com/cyberattack/.で利用可能。

[23] NAIC, *Cybersecurity Breach Response HQ*, *available at* http://www.naic.org/index_security_breach.htm.

[24] ノースダコタ・ワークフォース・セーフティ&インシュランス、「州政府のサーバに対するサイバー攻撃—WSI 広報 5 月の衝撃」
https://www.workforcesafety.com/news/news-item/cyber-attack-on-state-server-may-impact-wsi-information.で参照可能。

[25] サービス妨害（DDoS）攻撃では、敵はそれによってマルウェアにそれらを感染させることによって、複数のシステムの制御を奪い、狙ったユーザーへのリソースを使用不能にする。対象のコンピュータやネットワークを占有するために非合法なサービス要求の大量の要求を送りつける。決済・市場インフラ委員会, 市中協議文書「金融市場インフラにおけるサイバー攻撃耐性に関する指針」http://www.bis.org/cpmi/publ/d122.pdf.で参照可能。

なかったものの、このサイバーセキュリティインシデントは、当該企業だけでなくパートナー、サービス提供会社および保険契約者に重大な影響を与えていた可能性がある。

34. サイバーセキュリティインシデントはまた、内部関係者による行為を含みうることを忘れてはならず、2012年にフランスの相互保険会社で内部不正行為が確認された。この不正行為は、機密顧客情報を含む複製環境上で起きた社内でのデータ盗難から生じており、なりすましや不正請求につながった。

35. オランダでは、ある保険会社が、「CEOハック」と通称される特定のフィッシングサイバー攻撃の対象となった[26]。犯人は、保険会社の主要な、よく知られている顧客事業者の最高経営責任者（CEO）を装い、特定の口座に送金するよう保険会社の従業員の説得を試みた。犯人は、明らかに保険会社の特定の業務の詳細を調べ上げていた。

36. PwCによるレポートは、個人、旅行、医療および海上保険事業に対する攻撃を含む複数の管轄区域で保険会社が経験したいくつかの追加のサイバーセキュリティインシデントを特定した[27]。

[26] このタイプのサイバー攻撃は新たに現れる脅威として観察された。例、米国連邦捜査局「事業用メールの侵害：新興するグローバルな脅威」（2015 年 8 月 28 日）
https://www.fbi.gov/news/stories/2015/august/business-e-mail-compromise/business-e-mail-compromise.で参照可能
[27] PwC、「アンダーレンズ：保険セクターにおける脅威」（2015 年 11 月）

5. 保険会社のサイバー攻撃耐性

37. サイバーリスクによってもたらされる様々な課題は、保険会社による幅広い対応で克服されるべきである。効果的なガバナンス構造によりサイバーセキュリティインシデントを理解、防止、検出、対応および対処することができるよう、適切なハイレベルな経営陣の注意が必要である。また、サイバー攻撃耐性のベストプラクティスと整合するよく機能するリスク管理プログラムが備えられるべきであり、監督上のレビューを通じて検証されるべきである。以下に記述されるように、このレベルの対応は、保険基本原則（ICP）でも求められている。

38. サイバーセキュリティが効果的であるためには、その機関のすべてのレベルにおいておよびあらゆる外部関係者との取引に際してサイバーセキュリティへの対処がなされる必要がある。一般的に、実効的なサイバーリスク管理プログラムは、継続的なプロセスと統制の改善、災害への対策および復旧などのインシデント管理手順、適切なネットワーク方針と手続き、ユーザー権限の厳格な管理および制御、構成指針の厳秘、適切なマルウェア防護手順、リムーバブルメディアの使用状況の一貫した管理、モバイルおよびホーム作業手順のモニタリングおよび全従業員のための継続的な啓発・教育活動、を含む。

39. 例えば、一般的に、サイバー攻撃耐性のためのベストプラクティスには、以下が含まれると認識されている：[28]

- ガバナンス

  取締役会および上級管理職の関与と責任と併せ、適切なサイバー攻撃耐性の枠組みは、サイバーリスクの軽減に資する。例えば、上級管理職には、サイバー耐性の枠組みを開発、導入する責任を負い、取締役会に対する報告権限を持つ者が置かれるべきである。

- 特定

  特定は、侵入から保護されるべき事業能力と手続きを特定することを意味する。（機微個人情報を含む）情報資産および関連するシステムへのアクセスは、特定プロセスの対象であるべきである。サイバーリスクは常に進化しており、また「隠れたリスク」が出現する可能性があるため、定期的なレビューと更新は重要な要素である。関連する法人は、全体像の一部であり、そこからもたらされるリスクの重要度は、提供されている特定のサービスの重要度に必ずしも比例しない。例えば、小売業者のターゲットに対するよく知られたサイバー攻撃は、空調サービス提供会社を経由して侵入した[29]。

- 防衛

  耐性は、設計によって備えることができる。総合的な防衛には、相互接続および内

[28]アメリカ国立標準技術研究（NIST), 重要なサイバーセキュリティ推進のためのフレームワーク（2014 年 2 月）http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf で参照可能。; FFIEC, サイバーセキュリティ評価ツール（2015 年 6 月）https://www.ffiec.gov/cyberassessmenttool.htm で参照可能。；決済および市場インフラ（CPMI）委員会および証券監督者国際機構、「金融市場インフラにおけるサイバー攻撃耐性に関する指針」（2016 年 6 月） http://www.bis.org/cpmi/publ/ d146.htm で参照可能。

[29] SANS 研究所、「ケース・スタディ：ターゲットの流出を防げた重要な統制」（2014 年 8 月）http://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.で参照可能。

部および外部の脅威からの当該機関に対するその他のアクセス手段を防衛することを必要とする。防衛策を設計する場合、「人為的要因」を考慮すべきである。そのため、訓練は、サイバーリスクに対するセーフティネットの不可欠な部分となる。強力なIT統制が保護に役立つことから、統制は、最先端の技術基準を踏まえているべきである。

・検出

発生し得るサイバーインシデントの検出には、継続的かつ総合的なサイバーセキュリティの監視が不可欠である。セキュリティの実効性分析もまた、サイバーインシデントを検出および軽減するのに役立つ。

・対応および復旧

最善の手続きが用意されていても、発生前にサイバーインシデントを検出または防止することは必ずしも可能でない。こうした理由から、インシデント対応計画は非常に重要である。サービス（妨害が発生した場合）の再開は、事件の影響やサービスの重要度に応じて、合理的な期間内になされるべきである。（また、データ共有契約があった場合）緊急時対応計画、設計、業務統一性だけでなく、データの完全性は、早期再開のための重要な要素である。緊急時対応計画を効果的にするためには、定期検査の対象とすべきである。感染を防止するための手順により、さらにリスクを軽減することができる。情報開示方針は、危機における情報通信を強化するために、整備されるべきである。最後に、証拠準備も緻密な調査のために不可欠である。事業継続計画は、これらの要素を考慮すべきである。

・テスト

テストプログラム、脆弱性評価、シナリオベースのテスト、侵入テスト、およびレッドチームテストは、テスト段階における要である。サイバーセキュリティテストは、システムの指定、開発、および統合に際し、組み込まれるべきである。

・状況把握

把握は、サイバー脅威の特定に貢献する。したがって、危険な兆候に関する情報収集プロセスの確立が、サイバーリスクを軽減するのに役立つ。この関連で、保険会社は、確立された情報共有の取組みへの参画を検討すべきである。

・学習および向上

保険会社は、継続的にサイバーセキュリティ管理の有効性を再評価すべきである。サイバーに係る事件とサイバーインシデントから得られた教訓は、改善計画に寄与する。新たな技術的進歩は、モニタリングされるべきである。

6. サイバーセキュリティへのICP適用可能性

40. 保険コア・プリンシプル（ICP）は、サイバーリスクやサイバー攻撃耐性には具体的には対応していないが、重大なリスク管理および関連する内部統制の要件を求めることによって、サイバーリスクおよびサイバー攻撃耐性に関して保険セクターの対処を行う監督当局者へ、一般的な基礎を提供する。

41. 保険セクターにおけるサイバーリスクの監督に最も関連する可能性のある ICP には、以下がある。[30]

- ICP7（コーポレート・ガバナンス）
- ICP8（リスク管理および内部統制）
- ICP9（監督上のレビューおよび報告）
- ICP19（事業行為）
- ICP21（保険詐欺対策）

そして、特に、情報交換および監督協力については以下が関連する。

- ICP3（情報交換および守秘義務要件）
- ICP25（監督上の協力および調整）
- ICP26（危機管理における国境を越えた協力および調整）

ICP7（コーポレート・ガバナンス）

42. ICP7 は、2015 年 11 月に改訂された。本 ICP のもとで、保険会社は、システム、統制およびコーポレート・ガバナンス体制の有効性を検証する能力を持つことを期待されている。 本 ICP の指針は、「保険会社が、リスク管理および全体的な内部統制のための適切なシステムおよび機能を有することを確保すること、ならびに、それらを監視するこれらのシステムおよび機能が効果的にかつ意図したとおりに機能していることを確保するための監視を提供することが、取締役会の責任である。」と述べている。サイバーリスクを特定し対処することは、保険会社のリスク管理の不可欠な要素とされるべきである。

ICP8（リスク管理および内部統制）

43. ICP8 は、2015 年 11 月に改訂された。本 ICP は、保険会社に対し、リスク管理、コンプライアンス、保険数理上の事項および内部監査のための効果的な機能を含む、リスク管理および内部統制の効果的なシステムを全体的なコーポレート・ガバナンスの枠組み

[30] その他の ICP も、ICP16（ソルベンシー目的の全社的リスク管理）および ICP18（仲介人）もまた関係する可能性がある。

の一部として保持するよう、要求している。

44. ICP8 の指針は、リスク管理システムが対象とすべき最底限の分野を列挙している。サイバーリスクに関しては、指針は、「オペレーショナル・リスク管理」、「事業行為」および「その他のリスク軽減策」に言及している点で関連性がある。加えて、指針は、リスク管理システムが、現行および新たに発生するリスクを含む、すべての合理的に予測可能かつ関連する重要なリスクを考慮に入れるべきであるとしている。

45. 指針はまた、効果的な内部統制システムの典型的な要素について説明している。指針は、これらの要素の一つとして示される「方針およびプロセス」において、そのような内部統制システムを、「重要な IT 機能」、「（従業員による）データベースへのアクセス」および「従業員による IT システムへのアクセス」を含む「すべての事業上のプロセスおよび方針に対する適切な統制」を具備したシステムとして説明している。これは、明らかにサイバーリスクを含む。

46. また、指針は、適切な IT システムまたは管理情報システムを含む、統制機能のための十分なリソースを求めている。

47. 最後に、ICP8 の指針は、内部監査部門は、取締役会および上級管理職に対し、会計、財務およびリスクに関する報告情報をタイムリーに提供する IT システムの能力および適応性を含む事項に関して独立した保証を提供すべきであるとする。

48. 外部委託契約を締結もしくは変更する場合、取締役会および上級管理職は、保険会社のリスク・プロファイルと事業継続性が、外部委託することによってどのような影響を受けるか検討すべきである。これは、サイバーリスクの観点でも、サービス提供会社のガバナンス、リスク管理および内部統制に適用できる。

ICP9 （監督上のレビューおよび報告）

49. ICP9 は、監督上のレビューおよび報告に関して、監督者が備えるべき一般的なプロセスおよび手続について述べている。これらのプロセスは、レビューおよび報告の監督枠組みの分析を行い、保険会社によってもたらされるリスクまたは保険会社が晒されるリスクの変化する性質、規模および複雑性に注意を促すようにすることを含む。本 ICP では、監督上の枠組みは、保険会社の状況および顧客に影響を与え得るインシデントもしくは重大な変更を即座に報告するよう保険会社に要求すべきとされる。オフサイトモニタリングまたは立入検査の一部として、監督者は、保険会社とその顧客が晒されるリスクを評価および分析するのに十分な情報を得るべきであり、また保険会社のリスク管理

の有効性を確認すべきである。 ICP9 は、現在見直されている。

ICP19（事業行為）

50. 保険の事業行為の要件は、プライバシー保護に関する規定を含み、そこでは、顧客の個人情報を取得、保有、利用または、第三者に提供することが保険会社および仲介人に認められている。

51. ICP19 は、顧客に関するプライバシー情報の保護のための方針および手順を備えるよう保険会社および仲介業者に要求している。指針は、個人情報の悪用もしくは不適切な第三者への伝達の防止に重点を置き、プライバシー保護を確保しかつセキュリティ侵害を防止するための多くの措置を説明している。

ICP21（保険詐欺対策）

52. ICP21 では、監督当局は、保険会社および仲介者が保険詐欺を防止、摘発、報告および改善するために効果的な措置をとることを要求している。保険詐欺は、サイバーインシデントを介して発生する可能性がある。ICP21 は、より直接的にサイバーリスクに対処するために改訂すべきかどうかを検討することを目的の一つとして、現在見直されている。

ICP3、ICP25 および ICP26（情報共有および監督上の協力）

53. リスクの特定、管理および軽減に複数の管轄区域が巻き込まれる可能性のあるサイバーリスクの性質に照らして、ICP3（情報交換および守秘義務要件）は関連性が高い。ICP3 は、現在見直されている。

54. 他の管轄区域と情報を共有する能力は、ICP 25（監督上の協力および調整）に定められるように、サイバーインシデントがクロスボーダーな影響を生み出す可能性を踏まえ、サイバーインシデントに対応する監督者にとって重要なツールである。即座にリスクを特定、管理および軽減する監督者の能力は、情報共有の効率的な仕組みを備えることで強化されるだろう。そのような仕組みは、二国間または IAIS 多国間覚書（保険監督者間の情報共有の世界基準）のような複数者間の覚書、または監督者カレッジの関係で既に交わされているもの等の協力合意を含むだろう。加えて、本文書で言及した IAIS の調査結果は、ほとんどの管轄区域が、サイバーセキュリティに関する規制および監督上の取組み、とりわけ、サイバーに関する教育・訓練における課題、外部委託に関するサイバーリスクの取扱い等を共有することで恩恵を得る可能性を示唆している。ICP 25 は、現在見直されている。

グローバル金融セクターにおける他の規制設定機関によるサイバーセキュリティに関する取組事例

決済および市場インフラ（CPMI）委員会および証券監督者国際機構（IOSCO）

2016 年 6 月、CPMI および IOSCO よるサイバー攻撃耐性に関する共同作業部会は、「金融市場インフラのサイバー攻撃耐性に関する指針」を公表した[31]。この指針は、サイバー攻撃の防止、迅速かつ効果的な対応さらには早期かつ安全な回復という目標を達成するために、金融市場インフラ（FMIs）の能力強化を目指すものである。本指針は、既に定められている「金融市場インフラのための原則」（PMFI）を超えた FMIs に対する追加的な基準を定めるものではなく、PMFI について細部を説明することを目的とする[32]。

バーゼル銀行監督委員会（BCBS）

2014 年 10 月、BCBS は、「健全なオペレーショナル・リスク管理のための諸原則のレビュー」[33]を公表し、その中で 2011 年公表の「健全なオペレーショナル・リスク管理のための諸原則」の実施状況を評価した[34]。レポートは、60 のシステム上重要な銀行のオペレーショナル・リスク管理実務を取り上げ、いくつかの銀行においてはサイバー攻撃等の壊滅的な事態を想定したシナリオを準備していると報告している。

55. ICP26（危機管理における国境を越えた協力および調整）では、監督者は、特定の保険会社もしくはグループに係るクロスボーダーな危機を効果的に管理するために、他の関係当局と共に協力・調整する。したがって、監督者は、特定の保険会社もしくはグループに係るクロスボーダーな危機に関して他の関係当局と協力・調整することになる。（政策措置、危機対応判断および外部との折衝を含む）クロスボーダーの危機に対する迅速かつ円滑な一貫した調整と管理について予め計画しておくことは、効果的な危機管理の一つの要素である。ICP26 は、現在見直されている。

56. サイバー分野に特化したさらなる IAIS 文書があれば、監督者による一貫性がありかつ健全な監督実務の実施の支援に役立ち、また保険会社による適切なサイバーセキュリティ実務の遂行の支援にも役立つ可能性がある。

---

[31] http://www.bis.org/cpmi/publ/d146.htm.で参照可能（2016 年 6 月 29 日）。共同 WG の招待により、本指針の開発の間、FCTF の座長がオブザーバーとして参画した。

[32] CPMI and IOSCO, *Principles for Financial Market Infrastructures* (April 2012), *available at* http://www.bis.org/cpmi/publ/d101a.pdf.で参照可能。

[33] http://www.bis.org/publ/bcbs292.htm.で参照可能。

[34] http://www.bis.org/publ/bcbs195.htm.で参照可能。

7. サイバーリスクに対する監督上の対応

57. 本セクションは、監督者の役割を検討し、サイバーリスク対策に関する IAIS メンバーへの 2015 年の調査の概要を含み、そして、サイバーセキュリティの問題に対する実施中または検討中の監督上の対応の例を提示する。

58. IAIS の使命には、保険契約者の利益と保護のための、公正、安全かつ安定した保険市場の発展及び維持が含まれる。この文脈において、保険監督者は、保険市場の安全性および安定性、ならびに保険市場への信頼に脅威をもたらしうる、保険契約者を傷つけうるリスク（サイバーリスクを含む）に対応する役割を担う。

59. 監督者は、適切な規制および監督プロセスを通じて、サイバーリスクに対応することができる。サイバーリスクおよびサイバー攻撃耐性に特に関係する可能性がある監督上の領域は、以下を含む：

- 保険会社および仲介人によって保持される個人情報のセキュリティ
- サイバー上の手段を通じて行われる金融犯罪、ならびに
- 事業継続計画および災害復旧計画―個々の保険会社および仲介人、ならびに、場合によっては保険セクター全体について

60. 加えて、当問題は本質的にはグローバルなものであるため、サイバーリスクへの対応においてはクロスボーダーでセクター横断的な監督上の協力が重要となる可能性がある。

サイバーリスクおよび監督実務に関する IAIS の調査

61. 2015 年の 1 月から 2 月の間、IAIS は、サイバーリスクへの現在の監督アプローチについての見識を得るために、メンバーへの調査を実施した。具体的には、当調査は、サイバーリスクについてのメンバーの認識、サイバー脅威の対策への彼らの関与、および、この領域において利用中または開発中の監督アプローチについての FCTF の理解に貢献することを意図していた。およそ 30 のメンバーが回答した。受け取った調査への回答によれば、サイバーセキュリティに関する監督実務および見解は、IAIS のメンバーの間で大きく異なる。以下は、調査への回答において認められた、いくつかの注目すべき傾向である。調査結果の概要は、付属書 1 において示されている。

62. 多くの回答者は、サイバーセキュリティに関して、保険会社のコーポレート・ガバナンスに係る規制上または監督上の要件を設けている、または設ける予定であると示唆した。調査の回答者の多くはいまだ具体的なサイバーセキュリティの規定を置いていないものの、彼らは、保険会社がより一般的な規制上および監督上の要件のもとで（すなわち、

全社的リスク管理（ERM）活動、特にITリスクの評価を通じて）サイバーリスクに対応することになると想定している。加えて、調査の回答者の一部は、関係する基準の遵守、とりわけ、情報セキュリティ管理のISO規格[35]、およびアメリカ国立標準技術研究所（NIST）のインフラ強化のための枠組み[36]の遵守を報告した。いくつかの回答者は、金融機関に適用されるサイバーセキュリティのガイドラインを公表している。

63. とはいえ、サイバー攻撃耐性は、ほとんどの調査回答者にとって規制上の優先事項としては認識されていないようであった。理由として挙げられた中には、現在のIT化の度合い、サイバー攻撃耐性に関する具体的な規制上の要件の欠如、および保険会社の自己評価への依存が含まれる。さらに、多くの調査回答者は、サイバーセキュリティのモニタリングと監督を担当する、専門知識を持つスタッフに制約があるようであった。

64. 調査の結果は、サイバー攻撃耐性に対しては様々な監督アプローチが存在することを示していた。例えば、一部の回答者は、保険会社が直面するサイバーリスクの性質と規模を立ち入り検査によって査定する。一部の回答者は、保険会社のサイバー攻撃耐性に焦点を当てた、全体的な自己査定の実施またはテーマに沿った検査の導入を予定している。他の回答者は、サイバーリスクに明確に焦点を当ててはいないが、保険会社の事業継続計画またはリスク管理枠組みの一部としてサイバーセキュリティを査定する可能性がある。また、回答者の大多数が監督当局への通知の具体的な要件を持たない一方で、一部少数の回答者は、保険会社がその監督当局に報告する必要があるサイバーインシデントの種類または深刻さを定義し、また若干の回答者は、年次報告書を活用している。

65. 調査の回答数は限られていたものの、回答したメンバーからの答えおよび本報告書で記述されている他の情報からは、サイバーセキュリティに関する監督についてIAISのメンバー間での統一の実務が存在しないことが見て取れる。

サイバーリスクへの監督上の対応の例

66. 調査への回答に加えて、IAISの一部のメンバーは、メンバーの管轄区域において実施されているサイバーリスクに関する取組みの例（一部の場合には、官民の協力や市場全体のアプローチを含む）を提示した。これらの例は以下の通りである。

67. *フランス*　*健全性*規制・破綻処理庁（ACPR）は、サイバーリスクに関連する監督を情

[35] ISO 27000基準は、組織が情報資産の安全を確保することに役立つ。ISO/IEC 27001は、情報セキュリティ管理システムのための要件を提示する。（国際標準化機構　「ISO/IEC 27001—情報セキュリティ管理」、http://www.iso.org/iso/home/standards/management-standards/iso27001.htm で入手可能。）
[36] NIST　「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」（2014年2月12日）、http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf で入手可能。

報システム（IS）統制に分類している。ACPR は、サイバーセキュリティの監督のために、以下の 4 つの規準を策定した：(1) 機密性：情報はアクセス権限を与えられた者のみがアクセス可能であり、取得から破棄まで保護されていること、(2) 完全性：蓄積されたデータが正確かつ変更がないこと。データ記録は編集無用であること、(3) 利用可能性：情報は、権限を与えられた者により、適時に、正しくアクセス可能であること、(4) 監査可能性：IS へのアクセス、IS へのアクセス試行、または IS における行動が記録され（logged）、蓄積されること。記録されたファイルは、修正または削除されてはならない。これらの規準により、ACPR は、以下の領域を調査する：ガバナンス、IS リスクの特定および査定、IS リスクへの対応、ならびに、統制、リスク管理、ならびにフォローアップ活動の評価。

68. ***ドイツ*** サイバーリスク管理の監督上の検査は、通常、立ち入り検査によって実施される。実際の手続きは、具体的な事業体の規模およびリスク、ならびに監督者のチームの規模による。より小規模の事業体には、連邦金融監督庁（BaFin）は、リスク管理の文脈からこの側面に対応する。より大規模な事業体には、情報セキュリティの問題に焦点を当てた会議を設定することが多い。こうした会合では、チームは、サイバーセキュリティと IT リスク管理の重要性の高い側面を議論する。サイバーセキュリティのさらなる領域は、ソフトウェア開発プロセスまたはアイデンティティ管理のような、IT に関連する他の側面をより詳しく調べる際に対応される可能性がある。

69. ***欧州連合*** 連合内でのより高い共通の水準のネットワークおよび情報セキュリティを確保するための措置に関する指令の案[37]は、欧州委員会によって 2013 年に提出された。2015 年 12 月 7 日に、欧州議会および理事会は、委員会による、EU におけるオンラインのセキュリティを向上するための措置案について合意に達した。この指令は、サイバーセキュリティに関する欧州における最初の法令である。その規定は、オンライン環境をより信頼できるものにすること、そして、それにより、EU デジタル単一市場が円滑に機能することをねらいとしている。新たな規則は、(1) メンバー国におけるサイバーセキュリティ能力を改善し、(2) サイバーセキュリティに関するメンバー国の協力を深め、そして(3) エネルギー、運送、銀行および医療セクターの重要なサービスの運営者、ならびに、検索エンジンおよびクラウドコンピューティングのような主要なデジタルサービスの提供者に、適切なセキュリティ措置をとり、国家当局にインシデントを報告することを要求することになるだろう。[38]

---

[37] 連合内でのより高い共通の水準のネットワークセキュリティおよび情報を確保するための措置に関する指令の案―2013/048（SRI または NIS と呼ばれる）。

[38] 欧州委員会 「ネットワークおよび情報セキュリティ指針：共同立法者がサイバーセキュリティに関する EU の最初の法案に合意」（2015 年 12 月 9 日）、http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation で入手可能。

70. 個人データの処理に関する個人の保護についての規制案、および、こうしたデータの自由な移動に関する規制案は、2016 年 5 月 24 日付で発効し、2018 年 5 月 25 日から適用開始となる。[39]この文書は個人データに関するセキュリティインシデント通知条項を含み、多額の罰金を科す権限を各国のデータ委員会に付与する。

71. ***オランダ*** オランダの中央銀行（オランダ銀行、または DNB）によるテーマに沿った調査の成果の一つは、個々の金融機関に対し、調査結果に基づき各セクター（例えば、保険会社、銀行、および年金基金）内で自らを比較するベンチマークを提供したことである。個々の金融機関は、各セクターの平均と比べて彼らがどの位置にいるのかを理解することができる。これは、サイバーリスクの管理に当てはまる。

72. DNB はまた、他の管轄区域の監督者と合同で、大規模な国際的な保険会社も監督している。こうしたグループの監督のための多くの合同研究プロジェクトが実施されている。加えて、調査においては、異なる監督当局出身の 2 つのグループが、1 つのチームとして協働している。DNB は、こうした協力を通じて保険グループ内でのサイバーリスクの管理についての見識を得ることをねらっている。さらに、個々のグループ事業体が各管轄区域で適用される別個の金融規制の対象となる可能性があるものの、グループ内の一部のユニットは複数のグループ事業体にグループ内でサービスを提供する。DNB は、このような作業を通じて、グループ全体の観点からこのようなユニットへのより良い見識を得ることをねらっている。この種の監督上の協力の良い例として、グループ全体の資産管理および IT システムに焦点を当てた監督がある。

オランダにおける民間セクターの情報共有の取組み

オランダでは、中央銀行（オランダ銀行、または「DNB」）は、保険会社がサイバーリスクによってもたらされる危険を認識していること、および、互いに協力したいと望んでいることを承知している。オランダ保険協会は、現在、IT リスクの分野で活動している 2 つのワーキング・グループと、保険会社の IT 責任者から成る別個の協議グループを持つ。2 つのワーキング・グループはそれぞれ、情報セキュリティ（IS）と事業継続管理（BCM）に取り組む。これらの 2 つのグループにおいては、大手保険会社の専門家が、彼らの経験、彼らが何をしているか、そしてどのようにして互いから学ぶかについて情報を交換する。ワーキング・グループは、年に 3～4 回会合を持つ。DNB は双方のグループに対してプレゼンテーションを行い、情報交換プロセスは、なお改善の余地があると感じられた。例えば、保険会社に対する攻撃についての情報はより広く共有されうる。

[39] 欧州議会および欧州連合理事会、個人情報処理および個人情報の移転の自由に関する自然人保護ならびに指令 95/46/EC（データ保護一般規則）の廃止についての欧州議会・理事会 2016 年 4 月 27 日規則 2016/679http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation で入手可能。

73. ***シンガポール*** シンガポール金融管理局（MAS）は、シンガポール銀行協会と共に、サイバーセキュリティインシデントから生じる危機の影響を最小化するように、金融機関が主要な政府のパートナーとの調整を訓練し改善することを可能にするための業界全体の訓練を 3 年に一度実施する。2014 年の訓練である第 4 回ラッフルズ演習では、およそ 141 の銀行、金融会社、保険会社、資産運用会社、および証券ならびに仲介業者が、金融業界に対する大規模なサイバーセキュリティインシデントへの参加者の対応をテストした半日の演習に参加した。金融機関および市場インフラは、情報窃盗、金融機関の中核システムのへ侵害、ATM の停止・オンラインサービスの障害、ならびにウェブサイトの改変を含む、模擬サイバーセキュリティインシデントの組み合わせに直面した。模擬攻撃を受け、金融機関には、当該機関の事業に対する攻撃の影響を大きく 5 つの分類で評価することが要求された。すなわち、顧客、風評、法令・規則、財務、そして事業活動である。[40]

74. ***英国*** 英国の金融当局[41]は、サイバーリスクを理解し、その軽減に努めるために、多くのプロジェクトを実施してきた。2005 年、2007 年および 2009 年に、英国の金融当局は、英国の金融セクターの事業上の耐性をベンチマーキングするためのプロジェクトを実施した。[42]2012 年に、当局は、増加するサイバー脅威と業界からの意見に対応し、テクノロジーおよびサイバー攻撃耐性のテーマについてより深く掘り下げるために、より小規模で目標を絞った調査に集中的に取り組んだ。これは、長引く集中的なサイバー攻撃へのホールセール型銀行セクターの対応をテストするための 2013 年の机上訓練につながった。[43]

75. 金融安定政策委員会（FPC）は、英国財務省は、関連する政府当局および他の金融当局と協力して、中核的な英国の金融システムおよびそのインフラと連携し、サイバーリスクへの耐性を向上しテストするための作業プログラムを整備するべきであると提案した。これに対し、当局は英国の中核的な企業へのサイバーリスクの管理の質問票を発出し、この将来の作業の領域を特定できるよう調査のテーマが設定されている。この評価に基づけば、サイバーリスクに対応するために必要とされる能力は、3 つに分類することが有用である。すなわち、防衛能力、回復能力、および実効的なガバナンスである。最終的な作業プログラムは、4 つのテーマを中心に設定されている。すなわち、(1) 金融セクターに対する脅威についての理解の促進、(2) サイバーリスクに対するセクターの現在の耐性を評価する作業の強化、(3) セクターの耐性をテストするための計画の策定、および(4)

[40] シンガポール銀行協会 「金融セクターが第 4 次業界全体の事業継続訓練においてサイバー攻撃への対応をテスト」（2014 年 11 月 21 日）、http://abs.org.sg/docs/library/mediarelease_20141121.pdf で入手可能。
[41] 2013 年 4 月 1 日まで、金融当局はイングランド銀行、金融サービス機構、および大蔵省だった。
[42] イングランド銀行：http://www.bankofengland.co.uk/financialstability/fsc/Pages/bcinformation.aspx
[43] 同ページ。

情報の共有の向上である。

76. 2015 年 6 月に、FPC は、イングランド銀行、健全性規制機構（PRA）、および金融行為監督機構（FCA）が英国金融システムの中核にある会社と協働し、彼らが CBEST テスト（サイバー攻撃耐性をテストするための枠組み）を完了すること、および個々のサイバー攻撃耐性の行動計画を採択することを確保すべきであるとさらに提案した。イングランド銀行、PRA および FCA もまた、CBEST テストが英国の金融システムにおいて定期的なサイバー攻撃耐性の評価の一要素となる取り決めを確立すべきである。2015 年 8 月に、PRA および FCA は、保険セクターの耐性を評価するためのプロジェクトを開始した。[44]

英国における追加的な監督上の協力策

英国政府は、サイバー攻撃を、テロの脅威と並んで、国家の安全保障への最高位のリスクと捉えている。それゆえ英国政府は、以下を含む多くの、サイバー攻撃の防止に役立てるための取組みを立ち上げてきた：

- サイバー・エッセンシャルズ[45]―組織が一般的なサイバー攻撃から自らを守ることを支援するための、2014 年に開始された基本的なサイバーセキュリティ上の管理基準
- 国家犯罪対策庁内の国家サイバー犯罪ユニット
- 政府と業界のサイバー脅威についての情報交換を可能にするための、サイバー情報共有パートナーシップ[46]
- サイバーインシデントへの国家的な調整を改善するための、英国国家コンピュータ緊急対応チーム（CERT）である Action Fraud[47]を通じた、金銭的動機によるサイバー犯罪を報告する人々に向けた単一の報告システム[48]
- 組織がサイバー攻撃から回復するのを助けるための、政府通信本部における新たなサイバーインシデント対応スキーム
- 信頼性があり、かつ最新の、研究および学術的な手腕を提供するのを助けるための、英国の大学間での 2013 年のサイバーセキュリティ研究拠点のネットワーク

---

[44] 健全性規制機構、イングランド銀行：
http://www.bankofengland.co.uk/pra/Documents/about/insuranceletter100815.pdf
[45] 英国政府、ビジネス・イノベーション・技能省および内閣府 「指針―サイバー・エッセンシャルズのスキーム」（2014 年 4 月）、https://www.gov.uk/government/publications/cyber-essentials-scheme-overview で入手可能。
[46] 英国政府、内閣府、ビジネス・イノベーション・技能省、外務・英連邦省ならびに国家安全保障機関「政策文書―2010 年から 2015 年の政府方針：サイバーセキュリティ」（2013 年 2 月）
https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/establishing-a-cyber-security-information-sharing-partnership で入手可能。
[47] Action Fraud は、英国国立の、詐欺およびインターネット犯罪の報告センターである。情報は以下で参照可能：
http://www.actionfraud.police.uk/about-us
[48] CERT-UK（https://www.cert.gov.uk/）は、国家サイバーセキュリティ戦略（2011 年 11 月）（https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf で入手可能）に対応して 2014 年 3 月に組織された、英国国家コンピュータ緊急対応チームである。

77. ***米国*** 保険会社を含む金融セクターのサイバー攻撃耐性に焦点を当てた、いくつかの米国内の取組みおよびプログラムが存在する。これらには、以下等が含まれる。

78. 金融・銀行情報インフラ委員会。米国財務省は、連邦準備制度理事会および州の保険規制者を含む、18 の連邦および州の金融規制者ならびに関係する組織の委員会である、金融・銀行情報インフラ委員会（FBIIC）の議長を務めている。FBIIC は、(1) 金融規制者の間の調整およびコミュニケーションを向上させること、(2) 金融セクターの耐性を強化すること、および(3) 官民連携を強化すること、に焦点を当てるように任務を与えられている。米国財務省は、FBIIC を通じて米国金融セクターのサイバーセキュリティの取組みを調整する。その使命を果たすため、FBIIC は (1) 重要インフラ資産を、それらの場所および潜在的な脆弱性と併せて特定し、それらの米国の金融システムに対する重要性に優先順位をつけ、(2) 金融規制者の間の確実なコミュニケーション能力および緊急時のコミュニケーション協定を確立し、そして、(3) 各メンバー組織の充分なスタッフが、機密の情報を取り扱い緊急時に調整を行うための適切なセキュリティ上の許可を有することを確保する。[49]

79. 連邦の制裁権限。2015 年 4 月 1 日に、大統領は、大統領命令第 13694 号 *著しく悪意のあるサイバー利用活動に関与する特定の者の資産の凍結*に署名した。この大統領命令は、財務長官に対して、司法長官および国務長官との協議により、著しく悪意のあるサイバー利用活動に関与する個人または事業体に制裁を科す権限を与える。[50]

80. NIST の枠組み。重要インフラのサイバーセキュリティ向上のための本枠組みは、2014 年 2 月にアメリカ国立標準技術研究所より公表された。NIST の枠組みは、業界と政府の協働から生み出され、任意の、重点的な、柔軟な、反復可能な、かつ費用対効果に優れたサイバーセキュリティ管理のアプローチを定める。[51]当初、重要インフラ（つまり、米国経済、安全保障および保健を下支えする不可欠なサービス）を対象とするものとして生み出されたが、NIST 枠組みはまた、あらゆる規模ならびに業界および管轄区域の企業も利用できるよう設計されている。米国当局は、サイバーリスクの理解の拡大および集団的サイバーセキュリティの向上を目指し、NIST 枠組みの利用を通じて、基準となるサイバーセキュリティ関連のベストプラクティスの採用拡大を後押しし続けている。[52]

---

[49] 金融・銀行情報インフラ委員会：https://www.fbiic.gov/index.html
[50] 大統領府「大統領命令：著しく悪意のあるサイバー利用活動に関与する特定の者の資産の凍結」（2015 年 4 月 1 日）、https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m で参照可能。
[51] アメリカ国立標準技術研究所（NIST）、「重要インフラのサイバーセキュリティ向上の枠組み」（2014 年 2 月 12 日）http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf で参照可能
[52] ホワイトハウス、「サイバーセキュリティに係る行政の取組：2016 年の中間振り返りと 今後に向けて」（2016 年 2 月 2 日 https://www.whitehouse.gov/blog/2016/02/02/administration-efforts-cybersecurity-year-review-and-looking-forward-2016.

81. FFIEC のサイバーセキュリティ評価ツール。2015 年に、米国連邦金融機関検査協議会（FFIEC）[53]によって開発されたサイバーセキュリティ評価ツール（「評価」）は、特に銀行向けの自主的な自己査定のツールとして設計されているものの、サイバーリスクの管理への論理的なアプローチを提示しており、その視点は保険会社を含む他の金融機関も参考にできる。評価は、金融機関に対して、サイバーリスクとサイバーセキュリティの準備を組織の上級管理職および取締役会に通知するために、社内に「反復可能かつ測定可能なプロセス」を設けるように設計されている。[54]評価は以下のために用いられうる：(1) 組織に内在するリスク・プロファイル、またはその全体的なサイバーリスクに寄与する、またはそれらを決定づける要素を特定する、(2) 5 つの別個の領域において組織のサイバーセキュリティに関する習熟度、および、そのサイバーセキュリティに対する準備が組織の内在するリスクに合致しているかどうかを評価する、そして、(3) サイバーセキュリティを強化するために必要な具体的なリスク管理実務または統制を特定する。

米国における追加的な連邦監督上の協力策

*サイバーの情報共有。*2015 年の 12 月に、大統領は、民間企業がサイバーセキュリティ脅威に関する情報を連邦当局と自主的に共有するためのシステムを設立する、2015 年サイバーセキュリティ情報共有法案（CISA）に署名した。こうした情報を共有する企業は、所定の損害賠償保障を受ける。脅威に直接関係していない、個人が特定可能な情報は、データが共有される前に取り除かれなければならない。[55]

*国家サイバーセキュリティ計画。*2016 年 2 月 19 日、大統領は行政部に、サイバーセキュリティの意識および保護を強化し、プライバシーを保護し、公共の安全および経済的安全・国家の安全保障を維持し、そしてアメリカ人が彼らのデジタル・セキュリティをより良く制御する力を与えるために、短期的な措置を実施し長期的な戦略を整備する、サイバーセキュリティ国家行動計画（CNAP）を実施するように指示した。将来の活動のロードマップを策定するために国家サイバーセキュリティ強化委員会を設置することに加えて、CNAP は、医療保険会社および医療関係者に対して、彼らのデータの受託責任を強化すること、および、消費者がそのセンシティブなデータが安全かつ保護されていると信頼できることを確保するように求める。[56]

---

[53] FFIEC は、特定の米国の銀行規制者による金融機関の連邦検査のための統一の原則、基準、および報告様式を規定する権限を与えられた、複数機関で構成される米国の公式な主体である。FFIEC のウェブサイトを参照：http://www.ffiec.gov/

[54] 米国連邦金融機関検査協議会（FFIEC） 「サイバーセキュリティ評価ツール用語集」（2015 年 6 月）、https://www.ffiec.gov/cyberassessmenttool.htm.で参照可能。

[55] 統合予算法、2016, Pub. L. 114-113（2015 年 12 月 15 日）

[56] ホワイトハウス・プレスリリース 「ファクトシート：サイバーセキュリティ国家行動計画」（2016 年 2 月 9 日）、https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan で入手可能。

金融サービス情報共有分析センター。金融サービス情報共有分析センター（FS-ISAC）は、会員組織およびいくつかの公共機関からの匿名の報告を含め、脅威、脆弱性、そしてインシデントの情報を共有するために民間セクターによって設立された。FS-ISAC への加盟は、FFIEC、その会員当局、国土安全保障省、そして財務省を含むいくつかの当局により推奨されている。国土安全保障省大統領指令第 7 号（2003 年）は、除去された脅威および脆弱性に関する情報を FS-ISAC および重要インフラを運営している民間セクターの事業体に提供すること、官民連携により重要インフラの保護を支援すること、ならびに金融サービスの重要インフラに影響するインシデントへの対応に関する財務省の役割を調整する際の、連邦政府の役割を確立した。[57]加えて、金融サービスセクターにおける民間の重要インフラの企業は、インシデント対応および関連する情報の共有を含め、金融セクターの重要インフラを保護する活動を調整するため、金融サービスセクター調整評議会（FSSCC）を組織した。[58]保険会社は FS-ISAC と FSSCC の双方に関与している。

83. 全米保険監督官協会（NAIC）のサイバーの取組み。NAIC は、存在感を増しつつあるサイバー脅威に対していくつかの取組みを続けている。州の保険規制者は、FBIIC と、彼らが連邦の規制者と協働してベスト・プラクティスを開発しサイバーセキュリティ上の課題への共通のアプローチを議論する、独立した行政の規制者のためのサイバーセキュリティフォーラムにおいて一員として働く。2014 年末に、NAIC は、サイバーセキュリティの課題に対応するための保険規制者の取組みを調整するために、サイバーセキュリティ（EX）タスクフォースを組織した。その組織から間もなく、タスクフォースは、*実効的なサイバーセキュリティの保険規制指針のための 12 原則*を策定したが、これは規制者が保険会社、募集人その他の被規制事業体による消費者の情報を保護するための取組みを評価する枠組みを規定した。[59]これらの原則は、2015 年 6 月の NAIC 執行委員会／総会で改訂され、採択された。タスクフォースはその後、保険会社の財務諸表に、サイバーセキュリティの保障引き受けに係る財務成績についての情報を集めるための、*サイバーセキュリティおよびなりすましの保障に関する追加条項*を策定した。改訂された追加条項は、2015 年 8 月の NAIC 執行委員会／総会で採択され、2016 年の第一四半期に提出が開始された。[60]タスクフォースはまた、NAIC の情報テクノロジー検査ワーキング・グループおよび市場行為審査基準ワーキング・グループと協働し、サイバー脅威の発展に応じ、財務状態検査官ハンドブックおよび市場規制ハンドブックのそれぞれに指

[57] 金融サービス情報共有分析センター（https://www.fsisac.com/about）
[58] 重要インフラ保護および国土安全保障のための金融サービスセクター調整評議会（https://www.fsscc.org/ ）
[59] NAIC 「実効的なサイバーセキュリティのための原則：保険規制指針」（2015 年 4 月）、http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf で入手可能。
[60] NAIC 「サイバーセキュリティおよびなりすましの保障の保険追加条項」（2015 年 6 月）、http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_cyber_id_theft_ins_suplement.pdf で入手可能。

針として盛り込まれる更新版プロトコルを開発・更新している。金融検査の改訂は 2016 年のハンドブックに反映されており、2015 年 12 月 31 日から有効なものとして検査に用いられている。最後に、タスクフォースはまた、*消費者のサイバーセキュリティ保護のロードマップ*を策定し、保険会社、募集人、および他の事業が個人情報を収集、保管、および利用する際に消費者が受ける資格があると NAIC が考える保護を説明した。[61]ロードマップはまず 2015 年 10 月にタスクフォースによって採択され、2015 年 12 月に NAIC 執行委員会／総会で採択された。これらの保護は、関連する NAIC のモデル法およびモデル規制の更新、ならびに、2016 年 3 月に公表されその後 2016 年内に採択が検討される可能性がある、新たな「保険データセキュリティモデル法」に組み込まれるだろう。

84. 米国の州監督者の役割。一般的に、国内の保険会社において侵害が発生した場合、対応を主導する州は以下の方法でその規制権限を利用する可能性がある：(1)いつ侵害が発生したのか、このような侵害から誰が影響を受けるのか、そしてその情報から、州居住者へのこの影響についていずれの規制者が通知を受ける必要があるのか、そして、影響を受ける個人にどのように通知されることになるか（例えば、郵便、メール、新聞公告等）を判断するために保険会社との電話会議を設定すること、(2) その侵害に対して保険会社によって適切な措置が取られていることを確保する（例えばなりすまし防止等）こと、(3) 適正な場合には、州／連邦の規制者とコミュニケーションをとること、そして(4) 目標を絞った検査が必要／適切かどうかを決定し、該当する場合には以下を行うこと：サイバーセキュリティの検査を行うベンダーの選定を調整し、検査手続きの実行を調整し、適切な場合には、財務検査官ハンドブックの概念を利用して作業の範囲を決定し、検査の結果を伝達し、そして、規制上の措置が必要かどうかを決定する。関係する州の保険規制者は、保険会社のデータの侵害を受けての複数州による市場行為の検査に参加し、とりわけ、侵害の詳細、侵害に対する保険会社の対応、ならびに侵害が保険契約者および保険会社に与える財務上の影響について調査してきた。

85. ニューヨーク州金融サービス局。2015 年 11 月に、ニューヨーク州金融サービス局（DFS）は、FBIIC の会員に対し、DFS は金融機関への新たなサイバーセキュリティ規制を検討している旨、書簡を出した。書簡は、これらの規制の一部として DFS が検討している主要な規制上の提案を述べ、フィードバックを求めた。規制案は、規定の中でもとりわけ、金融機関に対して、指名された最高情報セキュリティ責任者（CISO）によって監督された、以下についての書面上のサイバーセキュリティ方針および手続きを採用することを求めるだろう：(1) 情報セキュリティ、(2) データのガバナンスおよび分類、(3) アクセス統制およびアイデンティティ管理、(4) 事業継続性計画および災害復旧計画ならびにリ

[61] NAIC 「サイバーセキュリティの消費者保護のロードマップ」（2015 年 12 月）、http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_cybersecurity_consumer_protections.pdf で入手可能。

ソース、(5) キャパシティ計画およびパフォーマンス計画、(6) システムの運営および利用可能性を巡る懸念、(7) システムおよびネットワークのセキュリティ、(8) システムおよびアプリケーションの開発ならびに品質保証、(9) 物理的セキュリティおよび環境制御、(10) 顧客のデータのプライバシー、(11) ベンダーおよび第三者のサービス提供者の管理、ならびに(12) 明確に規定された役割および意思決定権限を設定することによるものを含む、インシデント対応。さらに、第三者のサービス提供者が利用可能な、または彼らが保有する、センシティブなデータまたはシステムのセキュリティを確保するために、組織は方針および手続を実施および維持することを求められることになり、また、手続きおよび方針は、必要最低限の条件に関する情報セキュリティリスクに対応する第三者のサービス提供者との契約に含まれるように内部の要件を含めることが要求されるだろう。さらに、CISO は、DFS に対し、取締役会によって確認された、サイバーセキュリティ計画および機関へのサイバーリスクを評価する、年次報告書を提出することが求められるだろう。ニューヨーク州の取組みは、まだ草案段階にある。

8. 結論

87. サイバーリスクが保険セクターにもたらす課題はますます増大しており、監督者は、ICP のもとで当該課題への対応を義務付けられている。保険会社は、膨大な量の機密的な個人情報および商業上の情報を集め、蓄積し、管理する。これらのデータの蓄積があることから、保険会社は、ゆすり、なりすまし、または他の犯罪行為によって後に金銭上の利益のために使用可能な情報を求めるサイバー犯罪の主たる標的である。加えて、保険会社は、グローバルな金融セクターにおける大きな存在であるため、サイバーセキュリティインシデントによる保険会社のシステムの遮断は広範囲に及ぶ影響をもたらしうる。

88. 保険セクターは、内部および第三者との相互接続を通じたものを含む外部からのサイバーリスクに直面している。保険セクターのサイバーセキュリティインシデントは、影響を受けた保険契約者への深刻で長引く損害ならびに重大な法的コスト、規制上のコスト、および風評被害を含む運営上のコストに結びつくかもしれない。さらに、保険セクター全体としては、社会的な信頼の喪失により影響を受けるかもしれない。サイバーセキュリティインシデントの頻度と、全ての営利事業体にとっての重大性の高まりのために、サイバー攻撃耐性は、その規模、特質、本店所在地または地理的範囲に拘らず、全ての保険会社によって達成されなければならない。

89. サイバーリスクの規模のグローバル性が、グローバルなベースでこれらのリスクに対応する必要性に影響を与えており、これは、CPMI および IOSCO のような金融セクターの基準設定主体によるものを含む、国際的なレベルでの継続中の作業によって実証されている。実効的なクロスボーダーの協力および調整は、サイバーリスクへの監督上の対応の重要な要素である。

90. 保険監督者は、保険セクターにおけるサイバー攻撃耐性の強化にあたり重要な役割を持つ。サイバーリスクの性質は、監督者による監視の強化、および、サイバー攻撃耐性を高めるための、民間セクターと公的セクターの間の、ならびに各セクター内の協力および適切な安全策を講じた上での情報連携の強化を必要とする。

91. ICP はサイバーリスクまたはサイバー攻撃耐性に明示的には言及していないものの、その原則の文言ならびに付随する基準および指針における用語は、これらのリスクによってもたらされる課題の全てを包含する。したがって、ICP は、サイバーセキュリティに関して保険セクターの監督の一般的な基準を提供する。さらに、FCTF は、その任務に則って、2016 年から 2017 年に、ICP 21 がサイバーセキュリティの要素に特に対応するた

めに拡充されるべきか、および、もしそうであるならばどのようにして対応すべきかを調査する予定である。

92. IAIS のメンバーの間で、サイバーに関連する課題についての熟練度はさまざまである。一部の保険監督者は、彼らの管轄区域の保険会社のサイバー攻撃耐性に対応するため、有意義な措置を講じてきている。しかしながら、サイバーリスクに関する 2015 年の IAIS の調査の結果によれば、指標の中でもとりわけ、監督者がサイバーリスクを重視する度合、および、こうしたリスクに対応するために利用可能なツールは世界中で大きく異なる。

93. これまでの経験および予測される傾向をふまえると、サイバーリスク、およびサイバーインシデントの影響は大きくなり続けるだろう。監督者は、サイバーリスクへの彼らの理解、および保険セクターのサイバー攻撃耐性に関する彼らの監督上の能力を向上しようとすべきである。このような監督上の焦点は、サイバーリスクおよびサイバー攻撃耐性への保険会社の認識、ならびに、外部委託、およびサイバー攻撃耐性についての他の第三者との関係の影響を含む、サイバー攻撃耐性を高めるための保険会社の方針、手続き、および技術の開発および実施を適切に含む可能性があるが、それらに限定されるべきではない。

94. サイバーリスクに関連する取組みおよび課題が進化し続ける中で、IAIS はそれらをモニタリングするだろう。ICP に則った、サイバー攻撃耐性のベストプラクティスを取扱う追加的な IAIS の補助的資料は、監督者および保険会社に有益かもしれない。この点に関連して、FCTF は、その任務に則って、IAIS が本論点書の後に一つまたはそれ以上の適用文書によってこれらのトピックをさらに探求することを検討するように推奨する。FCTF は特に、サイバーセキュリティについての監督者のための指針が、保険セクターの(1) 監督者の検査実務、および(2) 保険会社のリスク管理実務という側面から有益だろうと認識している 。

付属書 1

IAIS の調査への回答の概要

2015 年 1 月から 2 月にかけ、FCTF は IAIS メンバーに、サイバー犯罪について調査を実施した。この調査は、リスクについてのメンバーの認識、サイバー脅威の対策への彼らの関与、および、この領域における実施中または検討中の監督アプローチについてタスクフォースが理解するのを支援することを意図していた。およそ 30 のメンバーが回答した。本セクションは、調査の主要なテーマに沿って示された、これらの回答の主要なポイントを提示する。

規制および監督上の文脈

i) サイバーリスクは、オペレーショナル・リスクの枠の中で検討され、オペレーショナル・リスクのガイドラインまたは指定された IT 基準を通じて、IT 規制の枠組みの中で対応される。一般的に、回答者は、サイバー脅威が彼らの管轄区域の中で高まっていると考えていた。しかしながら、大多数は、サイバー攻撃耐性を規制上の優先事項とは判断していなかった。サイバー攻撃耐性を優先しない要因の一部には、彼ら自身の保険セクターの現在の発展段階、規制上の枠組みの欠如、および保険会社の自己評価への依存が含まれた。

監督上の期待

ii) 一部の当局は、近い将来に更新が期待される彼らの規制上の枠組みがすでに整備されているとの仮定の上で回答した一方で、他の当局は、オペレーショナル・リスクまたは IT リスクに対応する彼らの規制上の枠組みがどのようにしてサイバーリスクに対応するかを説明した。一般的に、多くの調査回答者は、特に 3 つの防衛線との関係における役割について、彼ら自身のサイバー規制の枠組みのなかでガバナンス要件を含めることを想定する。[62] しかしながら、サイバーインシデントのモニタリングまたはスタッフの研修および認識といった他の領域での回答は、これらの領域がサイバーの規制上の枠組みの中で対応されているかどうか疑問を投げかける。

iii) 例えば、回答者の半数以上が、サイバーインシデントの根本的原因を修正するために、その成果物および行動計画を含めて、保険会社のプロジェクトをモニタリングすると述べた一方で、他の回答者は、サイバーインシデントに対応するプロジェクトをモニタリングするための特定の枠組みを持たないと述べた。一部の当局は、しかしながら、保険会社のサイバーインシデントに対応する上での何らかの脆弱性を立ち入り検査または他の機会に

[62] 健全なリスク・ガバナンスのために業界において一般的に見られる実務は、3 つの防衛線に依拠することが多い―(i) 事業種目管理、(ii) 独立した、企業におけるオペレーショナル・リスクの管理部門、および(iii) 独立した監査上のレビュー。例えば、バーゼル銀行監督委員会 「オペレーショナル・リスクの管理および監督の健全な実務」（2011 年 6 月）を参照。

認識した場合には、それらの脆弱性に対応するための保険会社のフォローアップ活動とその進展を、評価およびモニタリングするだろうと述べた。

監督上のレビューおよび評価

iv) 数名の回答者は、サイバーセキュリティの問題について継続的に研修を受ける経験豊富な IT 専門家のチームを有している一方で、ある一部の調査回答者は、サイバーセキュリティの監視に特に充てられたスタッフを持たなかった。これらの両極の間で、調査の多くの回答者は、サイバーセキュリティのモニタリングに責任を負うスタッフの数に限りがあるように思われた。

ガバナンス

v) 調査の回答者の 3 分の 2 は、取締役会および上級管理職へのサイバーリスクについての定期的な報告ならびに統制評価が行われていることを確認した。同じ割合が、監査部門によるサイバーセキュリティ枠組みの検証を確認していると報告した。半数強の回答者は、監督者が、サイバーリスク管理と組織の戦略との整合性をレビューしていると確認した。

サイバーリスク統制環境

vi) 調査の回答者の半数は、保険会社のサイバーリスク統制環境を評価するための規制上の条項および監督実務を整備しているように思われた。しかしながら、彼らの多くは、具体的なサイバーセキュリティの条項を定めておらず、むしろリスク管理活動、および特に、IT リスク評価を通じてサイバー脅威をフォローしている。数名の回答者は、保険会社のサイバーセキュリティの監視をモニタリングするための定期的な監査報告に依存している一方で、他の回答者は免許付与要件の一部にサイバーセキュリティの条項を盛り込んでいる。

脅威および脆弱性のリスク管理

vii) 回答者の 3 分の 1 は、保険会社によるソフトウェアのセキュリティ・ツールの利用を含め、保険会社によるサイバーリスクの管理を査定すると明確に示唆した。ほぼ同じ割合の回答者は、サイバーリスクの管理についての最近の進展に追いついていると述べた。このような実務に従わない者については、一部の回答者は、保険会社が主要なサイバー脅威の対象となった場合にのみ通知を受けることを想定していると述べた一方で、外部の IT 専門家からの報告に裏付けられた保険会社の内部監査報告書に依存している。

サイバーセキュリティインシデントへの対応

viii) 回答者の 3 分の 2 以上は、サイバーインシデントについて当局に通知することを求め

る具体的な要件を持たない。いくつかの当局はそれでもなお、個人情報保護または主要なオペレーショナル・リスクのインシデントに関する規制上の要件の下で、保険契約者に重大な影響を与えるあらゆるインシデントについて保険会社から通知されることを想定するか、保険会社から直接報告を受けるのではなく、情報保護一般について責任を有する他の政府当局から通知を受けることを想定する。サイバーセキュリティインシデントの件数について統計情報の収集をさらに発達させる余地が明らかに存在する。

ix) また、回答者の半数以上は、サイバーインシデントの根本的原因を修正するために、その成果物および行動計画を含めて、保険会社がどのようにしてサイバーインシデントをフォローアップするかをモニタリングすると述べた。数名の他の回答者は、保険会社がサイバーインシデントに対応する上での何らかの脆弱性を彼らが立ち入り検査を通じて認識した場合には、彼らは脆弱性に対応するための保険会社のフォローアップ活動を評価およびモニタリングするだろうと述べた。

x) さらに、サイバーインシデントに関連する事業継続に関して、回答者の大多数は、サイバーインシデントの後の保険会社の事業継続計画の実効性を評価すると述べた。アプローチは回答者の間で異なる。いくつかの回答者は、サイバー攻撃耐性が当該計画または枠組みの一部となるような、より広範な観点から、事業継続計画または危機管理枠組みを調査する。

監督上の措置

xi) 回答者の大多数は、サイバーリスクに特に対応する規制上の要件が存在しないと述べたものの、彼らの多くは、多くの監督上の措置が利用可能であると示した。これらには、警告状、追加的な報告の要求、改善計画、罰金、または業務停止が含まれた。調査の回答者の半数以上は、過去の 5 年の間に、保険会社のサイバーセキュリティ実務における脆弱性または不備に対応するための監督上の強制措置を利用していないと報告した。

サイバーリスクに対応するために監督上のアプローチおよび他の取組み

xii)他のリスク・カテゴリーと比較してサイバーセキュリティの取組みに与えられる優先順位を含め、監督アプローチは多くの理由により異なる。監督アプローチは、保険会社の IT および電気通信インフラの成熟度によっても異なる。本セクションにおいて言及されているガイドラインおよび他の文書は、詳細さおよび明確さが同等またはより高水準の他の文書も存在しうるものの、多くの管轄区域に対して有益であり得ると考えられていることに留意すべきである。これを念頭に置いて、観察されたアプローチは以下のセクションに細分化されている：

xiii）*基準の順守。*調査の結果は、多くの管轄区域がサイバーセキュリティを基準の順守と結び付けることを明確に示した。サイバーセキュリティの実務は進化し続けているものの、一部の規準は、多くの組織に関連し、適用可能である。その基準の一つは、健全な情報システムのセキュリティ管理のための要件の提示を目的とした国際的な規範である ISO 27001 である。[63]サイバーセキュリティにより具体的に関連するのは、アメリカ国立標準技術研究所（NIST）によって公表された「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」[64]であり、これはサイバーセキュリティ活動を導くために事業の推進力を利用することに焦点を当て、サイバーセキュリティのリスクを組織のリスク管理プロセスの一部として検討している。

xiv）*指針および立ち入り検査。*調査の数名の回答者は、サイバーセキュリティに特化したガイドラインを公表していると言及した。例えば、米国の NAIC は保険業界に特化した、実効的な規制上の指針のための原則を公表している。他の場合には、米国の「サイバー・エッセンシャルズ」スキームのように、ガイドラインは全ての種類の組織に適用可能であると思われている一方で、カナダにおける OSFI のサイバー自己評価ガイド、またはオーストラリアのサイバー攻撃耐性検査の場合には、金融機関に特化している。

xv）多くの管轄区域はベスト・プラクティスの文書を策定しているのみであるとは言え、数か所の管轄区域は既に、ニューヨーク州金融サービス局によって開発されているもののような、更新された検査枠組みを実施する段階にある。

[63] 国際標準化機構 「ISO/IEC 27001—情報セキュリティ管理」
[64] NIST 「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」

付属書 2

用語集

本文書において用いられている一部の主要な用語の定義は以下の通りである：[65]

サイバー攻撃	コンピュータ、コンピュータ・システム、または電気通信ネットワークを傷付ける、妨害する、またはそれらへの、無権限でのアクセスを得る試み。コンピュータ環境またはインフラを妨害、無効化、破壊、または悪意を持って制御すること、もしくは、データの完全性を破壊すること、または管理下の情報を盗み出すことを目的として、企業によるサイバースペースの利用を標的とした、サイバー空間を介した攻撃。[66]
サイバーインシデント	情報システムまたはその中に存在する情報への実際のまたは潜在的な負の影響をもたらす、コンピュータ・ネットワークの利用を通じて行われた行動。[67]
サイバーリスク	インターネットおよび電気通信ネットワークのようなテクノロジー・ツールを含む、電子データの利用およびその伝送によって生じるあらゆるリスク。それはまた、サイバーセキュリティインシデントから発生しうる物理的被害、データの不正利用により行われた詐欺、データの保存、ならびに、個人に関するもの、企業に関するものあるいは政府に関するものであれ、電子的情報の利用可能性、完全性および機密性に関して発生するあらゆる法的責任も含む。[68]
サイバー攻撃耐性	サイバー攻撃またはサイバーインシデントによって発生した妨害を、予想、吸収、適応および／または早期に回復する能力。[69]
サイバーセキュリティ	この用語は、あらゆる種類の脅威の軽減、脆弱性の軽減、抑止

[65] これらの定義の提示において、標準化が限定的であり、一部の用語については代替的な定義が他の情報源に見られる可能性があることが認識されている。
[66] 米国連邦金融機関検査協議会（FFIEC） 「サイバーセキュリティ評価ツール用語集」（2015 年 6 月）、http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_C_Glossary_June_2015_PDF5.pdf で参照可能
[67] 同ページ。
[68] CRO フォーラム 「サイバーリスクの課題と保険の役割」（2014 年 12 月）、http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/で参照可能。
[69] 決済・市場インフラ委員会および証券監督者国際機構 「金融市場インフラのサイバー攻撃耐性の指針」（2016 年 6 月）、http://www.bis.org/cpmi/publ/d146.htm で入手可能。

力、国際的な関与、インシデント対応、耐性、および回復活動、ならびに、保険会社の事業のセキュリティに関する方針を含む、戦略、方針ならびに基準を指す。[70]

サイバーセキュリティインシデント　本文書において、「サイバーセキュリティインシデント」という語句は、一般的に、サイバー攻撃とサイバーインシデントの双方を含むものとして用いられる。

サイバー脅威　意図的に、または意図せずして、システムの脆弱性を利用して、機密性、完全性、または利用可能性の喪失をもたらす可能性のある状況または事象。[71]

データの侵害　権限を与えられていない個人により、機微な、保護された、または機密のデータが、複製、伝送、閲覧、窃盗、または利用される、セキュリティ侵害。[72]

マルウェア　マルウェアは、事情を理解した上での所有者による同意（informed consent）なくコンピュータ・システムに秘密裏にアクセスするために設計されている。この表現は、悪意ある、侵入する、または迷惑なソフトウェアまたはプログラム・コードを意味して用いられる一般的な用語（悪意のあるソフトウェア（malicious software）の省略）である。マルウェアは、コンピュータ・ウイルス、ワーム、トロイの木馬、スパイウェア、不正なアドウェア、ランサムウェア、クライムウェア、多くのルートキット、および他の悪意ある、望まれないソフトウェアまたはプログラムを含む。[73]

NIST フレームワーク　アメリカ国立標準技術研究所　「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」（2014 年 2 月）[74]

---

[70] 決済・市場インフラ委員会、「金融市場インフラのサイバー耐性」（2014 年 11 月）、 http://www.bis.org/cpmi/publ/d122.pdf.で参照可能。用語集で用いられる定義と一致。
[71] 同ページ。用語集で用いられる定義と一致。
[72] 米国保健福祉省、子供およびグループのための管理「インフォメーション・メモランダム：ACYF-CB-IM-15-04」（2015 年 7 月 1 日）、http://www.acf.hhs.gov/sites/default/files/cb/im1504.pdf で参照可能。
[73] FFIEC 「サイバーセキュリティ評価ツール用語集」
[74] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf で参照可能。

参考文献

大西洋評議会およびチューリッヒ保険グループ、リスクネクサス「データの侵害を越えて：サイバーリスクのグローバルな相互関連性」（2014 年 4 月）、http://www.atlanticcouncil.org/publications/reports/beyond-data-breaches-global-interconnections-of-cyber-risk で参照可能。

大西洋評議会国際的将来に関するフレデリック・S・パーディセンターおよびチューリッヒ保険グループ、リスクネクサス「サイバーリスクに負けるのか？経済的利益および費用を交互に生じさせるサイバーの将来」（2015 年 9 月）、http://publications.atlanticcouncil.org/cyberrisks/.で入手可能

決済・市場インフラ委員会 「金融市場インフラのサイバー攻撃態勢」（2014 年 11 月）、http://www.bis.org/cpmi/publ/d122.pdf で参照可能。

決済・市場インフラ委員会および証券監督者国際機構 「金融市場インフラのための原則：重要インフラの提供者に適用可能なオーバーサイト上の期待の評価手法」（2014 年 12 月）、http://www.bis.org/cpmi/publ/d123.htm で参照可能。

欧州評議会 「サイバー犯罪に関する条約」（2001 年 11 月）、http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 で参照可能。

デボラ・ボドー、リチャード・グローバート 「サイバー攻撃耐性の評価：建築的改善を可能にする」マイター・テクニカル・レポート（2013 年 5 月）、http://www.mitre.org/publications/technical-papers/cyber-resiliency-assessment-enabling-architectural-improvement で可能。

欧州委員会「サイバーセキュリティ」スペシャル・ユーロバロメーター390（2012 年 7 月）、http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf で参照可能。

アンジェリア・ヘリン 「サイバーリスクの課題を達成する」ハーバード・ビジネス・レビュー（2012 年 11 月 27 日）、https://hbr.org/webinar/2012/12/meeting-the-cyber-risk-challen で参照可能。

国際サイバーセキュリティ保護アライアンス「プロジェクト 2020―サイバー犯罪の将来のシナリオ」、

https://www.icspa.org/wp-content/uploads/2014/12/ICSPA_Project_2020_-_Scenarios_for_the_Future_of_Cybercrime.pdf で参照可能。

国際電気通信連合、国連教育科学文化機関・デジタル開発のためのブロードバンド委員会「2012 年ブロードバンドの状況：全人類のデジタル包摂を達成する」（2012 年 9 月）、http://broadbandcommission.org/documents/bb-annualreport2012.pdf で参照可能。

国際電気通信連合 「発展途上国のためのサイバーセキュリティガイド」、http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf で参照可能。

国際標準化機構 「ISO 31000: 2009 年 リスク管理—原則およびガイドライン」（2009 年 11 月）、
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43170 で参照可能。

- 「ISO/IEC 27005: 2011 年、情報テクノロジー—セキュリティ技術—情報セキュリティリスク管理」（2011 年 6 月）、http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742 で参照可能。
- 「ISO/IEC 27032: 2012 年、情報テクノロジー—セキュリティ技術—サイバーセキュリティのガイドライン」（2012 年 7 月）、http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44375 で参照可能。
- 「ISO/IEC 27000: 2016 年、情報テクノロジー—セキュリティ技術—情報セキュリティ管理—概観および用語」（2016 年 2 月）、http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66435 で参照可能。

証券監督者国際機構 「取引所が電子取引リスクおよび事業継続計画を効果的に管理するメカニズム」（2015 年 12 月）、
http://www.iosco.org/library/pubdocs/pdf/IOSCOPD522.pdf で参照可能。

情報システムコントロール協会 「情報および関連するテクノロジーの制御目標」、http://www.isaca.org/COBIT/Pages/default.aspx で参照可能。

経済協力開発機構 「将来の世界的ショック、リスク・ガバナンスの向上」（2011 年 9 月）、

http://www.oecd.org/governance/48329024.pdf で参照可能。

- 「ターニング・ポイントにおけるサイバーセキュリティの政策決定、インターネット経済のための新世代の国家のサイバーセキュリティ戦略を分析する」（2012 年）、http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf で参照可能。
- 「進展するプライバシーの情勢： OECD プライバシーガイドラインからの 30 年」（2011 年 4 月）、http://www.oecd-ilibrary.org/science-and-technology/the-evolving-privacy-landscape-30-years-after-the-oecd-privacy-guidelines_5kgf09z90c31-en で参照可能。
- 「情報セキュリティとプライバシー」、http://www.oecd.org/sti/ieconomy/informationsecurityandprivacy.htm で参照可能。

ロニヒ・テンダルカー 「サイバー犯罪、証券市場およびシステミックリスク」*共同スタッフによる作業文書*、証券監督者国際機構、国際取引所連合、http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf で参照可能。

SANS Institute 「CIS 重要なセキュリティのコントロール―バージョン 6.0」（2013 年 1 月）、https://www.sans.org/critical-security-controls/で参照可能。

証券業金融市場協会 「実効的なサイバーセキュリティ指針の規制指針のための原則」（2014 年 10 月）、http://www.sifma.org/issues/item.aspx?id=8589951691 で参照可能。

英国国家危機対応チーム「サプライチェーンにおけるサイバーセキュリティリスク」（2015 年 2 月）、https://www.cert.gov.uk/resources/best-practices/cyber-security-risks-in-the-supply-chain/で参照可能。

国際連合 「サイバーセキュリティのグローバルな文化の確立、総会決議 57/239 号」（2003 年 1 月）、

http://www.itu.int/ITU-D/cyb/cybersecurity/_docs/UN_resolution_57_239.pdf で参照可能。

国連薬物犯罪事務所 「サイバー犯罪の問題、ならびに加盟国、国際的なコミュニティおよび民間セクターによるその対策についての包括的研究」（2013 年 2 月）、http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf で参照可能。

米国証券取引委員会　企業財務部門 「企業財務の開示指針：トピック No.2、サイバーセキュリティ」（2011 年 10 月）、
https://www.sec.gov/divisions/corpfin/cfdisclosure.shtml.で参照可能。

世界経済フォーラム 「サプライチェーンの耐性の構築」（2013 年 1 月）、http://www3.weforum.org/docs/WEF_RRN_MO_BuildingResilienceSupplyChains_Report_2013.pdf で参照可能。

- 「密接につながった世界におけるリスクと責任：グローバルなサイバー攻撃耐性への道筋」（2012 年 5 月）、http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdfで参照可能。
- 「サイバー攻撃耐性への連携―サイバー脅威の定量化に向けて」（2015 年 1 月）、http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdfで参照可能。