仮　訳

保険監督者国際機構

保険会社のサイバー・セキュリティの監督に関する

適用文書

２０１８年１１月

IAIS について

保険監督者国際機構（IAIS）は、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、実効的でグローバルに整合的な保険業界の監督を促進すること、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、ならびに、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。

適用文書では、監督上の資料の実際の適用に役立つ、実例または事例研究を含む、1 つ以上の ICPs、ComFrame または G-SII 政策措置に関連する追加の資料を提供する。適用文書は、原則および基準の実際的な適用が異なりうる状況において、または、それらの解釈および実施が困難を伴いうる場合に、提供される可能性がある。適用文書は、監督上の資料がどのように実施される可能性があるかに関して、監督者にとってのさらなる助言、実例、勧告またはグッド・プラクティスの例を提供することができる。

保険監督者国際機構
国際決済銀行気付
CH-4002 バーゼル、スイス
Tel: +41 61 280 8090
Fax: +41 61 280 9151
www.iaisweb.org

本文書は、IAIS のメンバーとの協議の上、金融犯罪タスクフォースにより作成された。

本文書は IAIS のウェブサイト(www.iaisweb.org)上で入手可能。

目次

1.0　はじめにおよび経緯

1.1　本文書の目的

1. 2018 年の 1 月に、世界経済フォーラムは「サイバー・セキュリティ・リスクは、増大する金融上の影響に伴って、その発生および破壊的可能性の双方が高まっている」と言及した[1]。保険会社は、サイバー保険の引受者、および金融セクターへの参加者の双方の立場から、サイバー・セキュリティ・インシデントの破壊的可能性または金融上の影響を免れるものではない[2]。

2. 金融犯罪タスクフォースによって策定され、2016 年 8 月に公表された IAIS の『保険セクターにおけるサイバー・リスクに関する論点書』[3]に示されているように、「保険会社にとって、サイバー・セキュリティ・インシデントの発生は、事業遂行能力に支障をきたし、商業用および個人のデータの保護を脅かし、また、保険セクターへの信頼を損なうおそれがある。」

3. 論点書は、その結論の中で以下を示した：
「サイバー・リスクは、保険セクターに増大する難題を提起し、また、それは、［保険コアプリンシプル］に基づいて、監督者が対応するよう義務付けられている。保険会社は、個人および商業用の膨大な量の機密情報を収集、蓄積、および管理する。これらのデータを蓄積していることから、恐喝、個人情報の盗難、または、他の犯罪行為による金銭的利益を得るために、後日、利用可能となる情報を求めるサイバー犯罪者にとって、保険会社は第一の標的である。加えて、保険会社は、グローバルな金融セクターへの重大な貢献者であるため、サイバー・セキュリティ・インシデントに起因する保険会社のシステムの中断は、広範囲にわたる影響をもたらしうる。」

4. 重要なのは、論点書において、「IAIS メンバー間でのサイバー関連の課題についての習熟度が様々であること」を認識してはいるものの、「全ての民間企業に関するサイバー・セキュリティ・インシデントの頻度および重大性が増えていることを理由に、サイバー攻撃耐性は、規模、専門分野、本拠地、または領域に関係なく、全ての保険会社により充足されなければならない。」ことに IAIS が気付いたことである。

---

[1] 世界経済フォーラムの『グローバル・リスク報告書』（2018 年 1 月）、以下から入手可能 http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.

[2] OECD の『サイバー・リスク管理における保険の役割の強化』（2017 年 10 月）、以下から入手可能。 http://www.oecd.org/publications/enhancing-the-role-of-insurance-in-cyber-risk-management-9789264282148-en.htm.消費者および民間企業が直面するサイバーの脅威に関する議論は、例えば、RMS の『サイバー・リスクの見通し』（2018 年）、http://forms2.rms.com/CyberRiskLandscapeReport2018.html. で入手可能を参照。

[3] IAIS、『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）、以下から入手可能。 https://www.iaisweb.org/page/supervisory-material/issues-papers/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector.

5. さらに、論点書では、サイバー・リスクの特性により、監督者は、保険会社のさらなる精査を行うよう要求されると言及し、また、この点に関して、原則文書ならびに付随する基準および指針を通じて、保険コアプリンシプル（ICPs）は、サイバー・リスクにより提起された論点を網羅し、それによって、サイバー・セキュリティに関する保険セクターの監督のための一般的な基礎を提供すると結論づけた。

6. 最後に、論点書では、IAIS がサイバー・リスク、サイバー・セキュリティ、およびサイバー攻撃耐性についてさらに調査し、また、保険セクターのための監督上の実務を提案する、複数の適用文書を策定および公表するよう提言していた。

7. サイバー・セキュリティの枠組みおよび実務の発展特性を考慮して、本適用文書は、保険会社のサイバー・リスク、サイバー・セキュリティ、およびサイバー攻撃耐性を監督するためのアプローチを策定または強化しようと望む監督者にさらなるガイダンスを提供することを意図している[4]。保険会社は、自組織内で適切なサイバー・セキュリティ実務を策定および導入する際の支援として、本適用文書の提言および事例[5]を考慮するよう推奨されている。

8. 絶えず進展する脅威の特性[6]だけでなく、規制上のコンバージェンスの潜在的利益[7]を認識した上で、本文書は、概して原則ベースであり、また、金融セクターのサイバー・セキュリティに関する G7 の基礎的要素（G7FE）[8]、関連する、金融セクターのサイバー・セキュリティの実効的な評価に関する G7 の基礎的要素（G7FEA）[9]、および CPMI-IOSCO の金融市場インフラのためのサイバー攻撃耐性に係るガイダンス（CPMI-IOSCO ガイダンス）[10]を含む、複数の情報源からの枠組みおよびガイダンスを土台としている。

---

[4] 2016 年の後半に IAIS が実施した調査で、管轄区域のサイバー・セキュリティの規制上および監督上の制度は、IAIS のメンバー間で、著しく異なっていること、また、保険会社のサイバー・リスクに最も関係する分野のける更なる指針の策定をメンバーが支援したことの双方が実証された。

[5] 管轄区域の事例で使用される用語の意味は、それぞれの管轄区域で定義されている場合があり、セクション 1.2 の定義と異なる場合もあれば異なる場合もある。

[6] 例えば、以下で入手可能な CISCO の『2018 年サイバー年次報告書』を参照。
https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?.

[7] 金融安定理事会、『金融セクターのサイバー・セキュリティにおける規制、ガイダンス、および監督実務に関する報告書の概要』（2017 年 10 月）のセクション 3 の「サイバー・セキュリティに関する FSB のワークショップの概要」、以下で入手可能。http://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory- practices/.

[8] 『金融セクターにおけるサイバー・セキュリティの G7 の基礎的要素（2016 年 10 月）』以下で入手可能。
https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf?69e99441d6f2f131719a

[9] 『金融セクターにおけるサイバー・セキュリティの実効的評価を行うための G7 の基礎的要素（2017 年 10 月）』以下で入手可能。
http://www.g7italy.it//sites/default/files/documents/G7%20Fundamental%20Elements%20for%20Effective%20Assess

[10] CPMI-IOSCO の『金融市場インフラのためのサイバー攻撃耐性に係るガイダンス』（2016 年 6 月 29 日）、以下で入手可能。https://www.bis.org/cpmi/publ/d146.pdf.

9. 本文書は、保険会社のサイバー・セキュリティの監督に重点を置いている[11]。論点書に関して言えば、サイバー保険（保険会社のそのような種類の保険商品の販売または引受け、および関連市場または健全性の課題）を対象としておらず、残余リスクを軽減する際のサイバー保険の利用も対象としていない[12]。

1.2 用語

10. 2017 年 10 月の報告書で、金融安定理事会（FSB）は、FSB のメンバーから提示された、「サイバー・セキュリティ」の 6 つの異なる定義を強調した[13]。同様に、欧州ネットワーク・情報セキュリティ機関（ENISA）は、2015 年に、「サイバー・セキュリティ」という用語は、その「包絡性（enveloping nature）」から、具体的な機関に適切となる「文脈上の定義」を必要とすることを述べて、様々なステークホルダー内での、サイバーの用語の使用の差異および重複についてコメントした[14]。

11. その勧告に基づいて、および G20 の財務相・中央銀行総裁からの提言への対応として、FSB の作業グループは、2018 年 11 月のブエノス・アイレスでの G20 サミットでの配付用に「サイバー語録」の最終化を予定している[15]。全般的に、FSB が語録を策定する目的は、「実効的な実務の認識を含むサイバー・セキュリティおよびサイバー攻撃耐性に関連する」[16]基準設定主体の取組みを支援する「FSB、基準設定主体、当局および民間セクターの参加者の取組みを支援するため」である[17]。IAIS は、本 FSB プロ

---

11 監督当局自身は、サイバー・リスクの対象であることが認識されている。例えば、金融セクターのサイバー・セキュリティに関する G7 の基礎的要素では、公的企業ならびに民間企業を取り扱っている。（「それらのリスクに対処するために、以下の、拘束力のないハイレベルの基礎的要素は、民間および公的企業が、自社の具体的な運営上および脅威の見通し、セクターにおける役割、ならびに法的および規制上の要件に合わせて調整するために、金融セクター用にデザインされている。」）。しかしながら、この見方は、本適用文書の対象範囲外である。

12 金融機関にとってのリスク緩和剤としてサイバー保険を利用することに関して、例えば、米国の連邦金融機関検査協議会（2018 年 4 月 10 日付共同声明）「リスク管理プログラムにおけるサイバー保険および、その潜在的な役割」、以下で入手可能を参照。
https://www.ffiec.gov/press/pdf/FFIEC%20Joint%20Statement%20Cyber%20Insurance%20FINAL.pdf;
欧州保険年金機構の、『サイバー・リスク：一部の戦略的論点』（2016 年）、以下で入手可能。
https://eiopa.europa.eu/Publications/Stakeholder%20Opinions/IRSG%20own%20initiative%20paper%20-%20Cyber%20risk.pdf（EIOPA の保険および再保険ステークホルダー・グループが作成）、および、ジュネーブ協会の『リスク軽減戦略としてのサイバー保険』（2018 年 4 月）、以下で入手可能。https://www.genevaassociation.org/research-topics/cyber-and-innovation/cyber-insurance-risk-mitigation-strategy.

13 ボックス 1—「サイバー・セキュリティおよびサイバー攻撃耐性とは何か」、FSB の『公けに公表されたサイバー・セキュリティの規制、ガイダンスおよび監督実務の実績評価』、5 頁（2017 年 10 月）、以下で入手可能。
http://www.fsb.org/wp- content/uploads/P131017-2.pdf.

14 ENISA の『サイバー・セキュリティの定義—標準化する上での差異および重複』（基準策定機関および他の機関が検討するための多数の定義を提示）（2015 年 12 月）、以下で入手可能。
https://www.enisa.europa.eu/publications/definition-of-cybersecurity.

15 サイバー語録協議文書（2018 年 7 月 2 日）、以下で入手可能。http://www.fsb.org/2018/07/cyber-lexicon-consultative-document/

16 サイバー語録協議文書（2018 年 7 月 2 日）、以下で入手可能。http://www.fsb.org/2018/07/cyber-lexicon-consultative-document/

17 金融安定理事会、『サイバー語録に関する進捗状況の更新』（2018 年 3 月 20 日）入手可能。

ジェクトに参加している。FSB サイバー語録は、本適用文書の最終的なリソースとして公表される予定はないものの、IAIS は、サイバー語録の情報が将来の関連する研究に役立つことを期待する。

12. 本適用文書の目的上、2016 年の論点書の Annex Ⅱの用語集を参照しており[18]、その用語集は、さらに、米連邦金融機関検査協議会（FFIEC）、CRO フォーラム、決済・市場インフラ委員会（CPMI）のサイバー攻撃耐性作業グループ、および証券監督者国際機構（IOSCO）；ならびに、米国国立標準技術研究所（NIST、米国商務省）の取組みに主に基づいていた。これらおよびその他のリソースは、FSB 語録を開発してきた専門家からなる国際ワーキンググループによる基礎的な成果として役立った。

13. したがって、本文書の文脈において、「サイバー・リスク」は、「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」を意味する。「また、サイバー・リスクには、サイバー・セキュリティの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。」

14. 次に、「サイバー・セキュリティ」は、「あらゆる種類の脅威の軽減、脆弱性の軽減、抑止力、国際的な関与、インシデント対応、攻撃耐性、および回復活動、ならびに、保険会社の事業運営の安全性に関する方針を含む、戦略、方針ならびに基準を指す。」

15. 「サイバー・セキュリティ・インシデント」（またはサイバー・インシデント）は、情報が、処理、保存または送信、もしくはセキュリティポリシー、セキュリティ手順または利用規約の違反を構成するため、機密性、完全性、可用性に違反する情報システム内の悪意のあるならびに悪意のないいずれの事象も含むことを意図している[19]。

1.3 プロポーショナリティ

16. サイバー・セキュリティは、集団および個別の双方にとっての保証である。監督者は、サイバー・セキュリティが全ての保険会社にとって必要である一方で、保険会社または監督者に万能（one-size-fits-all）となる処方が存在しないことをさらに認識すべきである。本適用文書の中では、ICPs の一般的な記載を制限しようとの意図は一切ない。つ

---

http://www.fsb.org/2018/03/progress-update-on-cyber-lexicon/

[18] Annex Ⅱ－IAIS、『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）

[19] FSB サイバー語録協議文書案（2018 年 7 月 2 日）より適合され、以下にて入手可能。
http://www.fsb.org/2018/07/cyber-lexicon-consultative-document/

まり、ICPs は全ての管轄区域の保険監督に対して、その保険市場における習熟の度合および監督対象となる商品／サービスの種類に関係なく適用されるものの、それでもなお、リスクベースかつプロポーショナルな方法に実施され、適用されるべきである[20]：

- 「プロポーショナリティは、すべての ICP の基礎にある。監督者は、原則本文および基準にて規定されている結果を達成するためのそれぞれの監督要件の実施および保険監督の適用を調整する柔軟性を有する。」
- 実施―プロポーショナリティにより、ICPs は、管轄区域の監督枠組みの法的構造、市場環境および消費者に適した形で、管轄区域の監督枠組みに導入されることが可能になる。
- リスクベースの監督は、プロポーショナリティと関連するが、それとは区別される概念である。これは、監督上の措置およびリソースが、保険契約者、保険セクターまたは金融システム全体に最も大きなリスクをもたらす保険会社、保険種目および市場慣行に割かれることを意味する。

1.4　本文書の特性

17. 本文書では、保険監督者に対して（また、保険会社にとっても有用となりうる）ガイダンスを提供するが、網羅的または規範的となることは意図していない。

18. IAIS の手続きに従うと、適用文書は ICPs の実際の適用に役立つ、１以上の ICPs に関連する追加の資料を提供することができるものの、適用文書には拘束力があるわけではなく、また、基準を定めるものでもない。適用文書は、優れた実務の例を提供し、ならびに、ICPs の導入方法に関して、さらなる助言および提言を提供することができる[21]。

19. 監督者は、本適用文書を自身が監督対象としている保険仲介人のサイバー・セキュリティに関しても考慮すべきである[22]。

---

[20] ICP 改定案のイントロダクションおよび評価手法（2017 年 11 月 8 日）－プロポーショナルかつリスクベースの監督

[21] ステークホルダーとの協議方針（2015 年 2 月）の項目 2 および Annex 1、以下で入手可能。https://www.iaisweb.org/page/about-the-iais/policies-and-procedures/file/47624/policy-for-consultation-ofstakeholders.

[22] ICP 18（仲介人）

2.0　国際的、国内の、および業界のサイバー・セキュリティ基準およびガイダンス

20. 複数の国際的、国内の、および業界の機関で、公的および民間の双方のセクターは、保険監督に適合するサイバー・セキュリティの枠組みおよびガイダンスを策定した[23]。

2.1　枠組み

21. サイバー・リスクをめぐる増大する懸念への対応として、サイバー・セキュリティ・インシデントを予防し、保護し、かつ対応するための諸機関の能力向上の基礎を提供するために、様々なサイバー・セキュリティに関する枠組みが公的および民間の企業により策定されてきている。広く認められたサイバー・セキュリティの枠組みには、以下が含まれる：

(a) 情報システムコントロール協会（ISACA）－COBIT

22. COBIT（「情報および関連技術のコントロール目標」）[24]は、ISACA により作成された IT 管理および IT ガバナンスの実務の枠組みである。COBIT は、情報技術に対する実行可能な統制策を提供し、また、IT 関連のプロセスおよび IT の実現者の論理的な枠組みを中心にそれら統制策を構築する[25]。

23. 当該枠組み（最初、1996 年に公表された）では、IT 管理のための包括的なプロセス一式を、プロセスのインプットとアウトプット、主要なプロセス - 活動、プロセスの目的、実績指標、ならびに習熟度のモデルと共に各プロセスと一緒に定義している。また、COBIT では、IT と事業を一致させる目的で、情報システムおよび情報技術のガバナンスおよび統制プロセスの実務一式を提供している。COBIT は、IT のプロセスおよび関連する情報セキュリティの導入、テスト、および監査統制に使用される。

(b) 国際標準化機構（ISO）[26]

24. ISO は、160 を超える各国の標準化組織の代表者から構成される国際的（非政府）組織であり、共通基準の策定および促進に努める。ISO と国際電気標準会議（IEC）

---

[23] 金融安定理事会、『公けに公表されたサイバー・セキュリティの規制、ガイダンスおよび監督実務の実績評価』（2017 年 10 月）、32-43 頁（国際組織のガイダンスおよび他の取組みのまとめ）、以下で入手可能。http://www.fsb.org/wp-content/uploads/P131017-2.pdf

[24] 以前の、情報システムコントロール協会として知られているISACAは、情報システムのための実務の策定に携わっていた、独立、非営利のグローバルな協会である。http://www.isaca.org/aboutisaca/Pages/default.aspx

[25] また、ISACA は、サイバー・セキュリティ・リスクの軽減に特に重点を置いた、『サイバー・セキュリティ・ネクサス（CSX）』も策定した。これは、COBIT にも基づいており、以下で入手可能。https://cybersecurity.isaca.org/csx-nexus

[26] ISO/IEC 27000 ファミリー―情報セキュリティ・マネジメント・システムで、以下で入手可能。https://www.iso.org/isoiec-27001-information-security.html

は、金融セクター向けの情報セキュリティのマネジメントおよびプログラムの要素に関する提言を行う。ISO は、技術、実務、および人を含むシステムの課題として情報セキュリティを支える、実効的な全体プログラムの非常に広い構造を定義し、また、正式なセキュリティ・プログラムの必要性を記載する。ISO は、主に情報テクノロジーのガバナンス（ISO 38500）、および情報セキュリティ（ISO 27000）の管理に用いる基準のファミリー２つを作成している[27]。

(c) NIST サイバー・セキュリティ枠組み

25. 公共セクターと民間セクターの協力を受けて 2014 年に米国の商務省の米国標準技術局（NIST）により公表された、NIST サイバー・セキュリティ枠組み[28]は、組織がサイバー・セキュリティ・リスクを管理する支援となる、任意の、リスクベースの業界基準一式と最善の実務である。そもそもは、重要なインフラとして策定されたものの、サイバー・セキュリティ枠組みは、「組織がーサイバー・セキュリティ・リスクの規模、程度、またはサイバー・セキュリティの精巧度に関係なくーセキュリティと攻撃耐性を向上させるために、リスク管理の原則および最善の実務を適用できるようにする。」枠組みのコアでは、標準化されたサイバー・セキュリティ活動、望まれる結果、および適用される参考文献について定義しており、また、5 つの継続的な機能：つまり、特定、保護、発見、対応、および回復により構成されている。実際、枠組みのコアでは、実効的なサイバー・セキュリティを構成する事業プロセスの継続的なサイクルを記載している。

2.2 ガイダンス

26. 以下のパラグラフでは、最近、機関および監督者がそのサイバー・セキュリティのアプローチを向上させる際の支援とするために公表された、金融セクターのガイドラインの数セットを紹介する。

(a) FFIEC

27. サイバーによる脅威の規模と精巧度の高まりを踏まえて、米国の連邦金融機関検査協議会（FFIEC）は、機関が自身のリスクを特定し、かつ、サイバー・セキュリティへの準備について判断する支援となる、サイバー・セキュリティ・アセスメント・ツール（アセスメント）を開発した[29]。アセスメントは、金融機関が、自身のサイバー・

---

[27] ISO 27032 サイバー・セキュリティのためのガイドライン（サーバーに固有）を参照。以下で入手可能。https://www.iso.org/standard/44375.html.

[28] 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枠組み』（2018 年 4 月 16 日公表、バージョン 1.0）以下で入手可能。https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[29] 連邦金融機関検査協議会（FFIEC）の、『サイバー・セキュリティ・アセスメント・ツール』（2017 年 5 月更新）、以下で入手可能。https://www.ffiec.gov/cyberassessmenttool.htm.FFIEC は、複数の省庁間で構成される組織であり、連邦の監督対象の金融機関、その持株会社、ならびにそれらの機関および持株会社の子会社である非金融機関用の

セキュリティへの準備の経過を徐々にたどるための、繰り返し、および測定可能なプロセスを提供することを意図している。アセスメントは、内在するリスク・プロファイルとサイバー・セキュリティの習熟度の 2 つの部分から成る。内在するリスク・プロファイルでは、統制を導入する前の、機関に内在するリスクを特定する。サイバー・セキュリティの習熟度には、整備されている具体的な統制および実務を特定するための領域、評価要因、構成要素、および 5 つの習熟度内の個々の宣言文を含む。

(b) CPMI-IOSCO

28. 2016 年 6 月に、CPMI-IOSCO のサイバー攻撃耐性に関する作業グループ（WGCR）は、その CPMI-IOSCO ガイダンスを公表した[30]。IAIS は、WGCR にオブザーバー組織として参加した。CPMI-IOSCO ガイダンスは「国によって類似する、攻撃耐性を強化するため」[31]という意図で開発され、「サイバー攻撃耐性の分野での整合的かつ実効的な監視および監督を支援するための、金融市場および金融機関の分野における、国際的に合意された最初の原則一式」[32]と称されている。

29. CPMI-IOSCO ガイダンスでは、サイバーのガバナンス、対応および回復、脅威に関する情報収集、システムおよびプロセスの厳密な検証、サイバー・リスクに関する認知度に重点を置き、また、サイバー・セキュリティの体系的なアプローチについて記載している。

30. CPMI-IOSCO ガイダンスでは、ガバナンスが、サイバー攻撃耐性のある組織を構築および維持する機関の能力の中核を成すことを認識している。

31. CPMI-IOSCO ガイダンスの策定は、金融セクターのサイバー・セキュリティに関する国際的な協力の主要なマイルストーンであったし、また、以下でさらに記載しているように、本適用文書で提示しているガイダンスは、その提案から知見を得ている。

(c) 金融セクターのサイバー・セキュリティに関する G7 の基礎的要素（G7FE）

32. G7 の財務相および中央銀行の総裁は、2016 年に G7FE を公表した。G7FE は、米国財務省とイングランド銀行の共同主導の下で専門家グループにより策定され、金融セクターにおける公的企業および民間企業のためのサイバー・セキュリティの原則の簡

統一された報告制度を策定する責任を負う。https://www.ffiec.gov/about.htm を参照。

30 CPMI-IOSCO の、『金融市場インフラのためのサイバー攻撃耐性に関するガイダンス』（2016 年 6 月）、以下で入手可能。https://www.bis.org/cpmi/publ/d146.pdf.

31 BIS のプレス・リリース（2016 年 6 月 29 日）、「CPMI-IOSCO が金融市場インフラのためのサイバー攻撃耐性に関するガイダンスを公表」、以下で入手可能。https://www.bis.org/press/p160629.htm

32欧州中央銀行の理事会でのブノワ・クーレのスピーチ（2016 年 1 月 13 日）、以下で入手可能。
https://www.ecb.europa.eu/press/key/date/2016/html/sp160113_1.en.html

潔な一式である。G7FE には拘束力はないものの、企業および監督者の双方にとって有益となるよう意図されている。

33. 企業について、当該要素は、「企業が、それを元に、自社のサイバー・セキュリティ戦略および運営の枠組みを設計および導入することができ、また、リスク管理およびリスク文化のアプローチについての知見を得ることができる、基礎的要素（building blocks）として機能し」、また、「運用上のおよび脅威となる環境が徐々に生じるため」、企業のサイバー・セキュリティ・プログラムの再評価に用いることができる[33]。

34. 監督者について、G7FE では、「管轄区域の内外における公的当局は、当該要素を自身の公的政策、規制上および監督上の取組みを導くものとして同様に使用することができる」と説明している[34]。

35. G7FE では、サイバー・セキュリティの 8 つの「ハイレベルな」基礎的要素を特定しており、それらは、(1)サイバー・セキュリティの戦略および枠組み、(2)ガバナンス、(3)リスクと統制の評価、(4)モニタリング、(5)対応、(6)回復、(7)情報共有、(8)継続的学習、である[35]。これらについては、以下のセクション 3 でさらに論じている。

36. G7FE で概説されている実効的な実務を促進するために、G7 は 2017 年に『金融セクターのサイバー・セキュリティの実効的な評価に関する G7 の基礎的要素』（G7FEA）を公表した[36]。この拘束力のないガイダンスは、「望まれる結果」および「評価要素」を網羅した上で、サイバー・セキュリティに必要不可欠なリスク管理の決定に関する内部および外部での議論のガイドとなり、かつその議論を推進するツールとして役立つように意図されていた。

37. G7FEA は、G7FE で概説されている実務がどのように適切に実行されているか、および、その実績がどのように評価できるかに重点を置いている。G7FEA のパート A では、G7FE を導入している成熟した企業が達成するよう期待されるべき、望まれる結果一式、「その上、あまり成熟していない企業が目指しうる結果」を提示してい

---

33 G7FE の 1 頁、前付け。

34 G7FE の 1 頁、前付け。

35 当時最新の文献によると、2016 年の IAIS の論点書では、「一般に認識される…サイバー攻撃耐性のための最前の実務」の同様の一覧を確認している。論点書のパラグラフ 39

36 『金融セクターのサイバー・セキュリティの効果的な評価に関する G7 の基礎的要素』（2017 年 10 月）は、以下から入手可能。
http://www.g7italy.it//sites/default/files/documents/G7%20Fundamental%20Elements%20for%20Effective%20Assessment%20of%20cybersecurity%20in%20the%20financial%20sector.pdf.

る。G7FEA のパート A の要素は、G7FE の様々な要素にリンクしており、以下のセクション 3 で取り扱われている。

38. G7FEA のパート B では、企業がサイバー・セキュリティ・プログラムで望まれる結果を達成する上で、進捗状況を評価する実効的なプロセスの要素を提示している。これらは、以下のセクション 5 で論じている。

3.0　保険会社のサイバー・セキュリティ実務の監督

39. タスクフォースのサイバー・セキュリティ実務の調査では、サイバー・セキュリティに関する管轄区域内の規制上および監督上の制度の習熟度は、IAIS のメンバーの中でも大きく異なることが確認された。保険監督者は、保険会社のサイバー・セキュリティに対して行われる取組みを発展させる際には、以下で説明される実務を考慮することができる。セクター別および管轄区域のギャップの特定を支援するために、保険監督者は、自身の管轄区域における保険セクターで徐々に高まるサイバーの習熟度のレベルを、他の金融セクターと比較して考慮し、また国際的なサイバー・セキュリティ基準に関連するイニシアティブを考慮すべきである。プロポーショナリティ原則は、管轄区域または保険セクターのサイバーの習熟度のレベルに関係なく適用される。

40. 企業が自社のサイバー・セキュリティ戦略および運営の枠組みを設計および導入するための基礎的要素を提供することで、G7FE もまた保険監督者が保険セクターのサイバー・セキュリティ基準について、自身の管理および評価を構築する際の有用な出発点を提供する。したがって、本セクションでは、8 つの G7FE を保険会社のサイバー・セキュリティに関する監督上のアプローチに関する議論の骨組みを作るために使用する。当該議論はまた、適切であれば、G7FE および提案された実務がどのように既存の ICP の基準および指針に適合するかについても取扱う[37]。

41. 本適用文書は、CPMI-IOSCO　WGCR により策定されたガイダンスを含め、特に、金融セクターのサイバー・セキュリティに関する、以前の国際的な取組みを参考にしている。本適用文書のセクション 3.1 から 3.8 に示されているように、それぞれのセクション（提言）におけるパート B 内のパラグラフの多くは、WGCR ガイダンス・ペーパーに直接基づくまたは適合される。そのガイダンスは、金融市場のインフラに特別に向けられたものであったが、そのほとんどは、全ての金融機関の様々な程度で考慮することが適切である[38]。金融機関のサイバー・セキュリティのための整合的でセクターを越えたガイダンスの提供は、適切であれば、規制上のアプローチの調和に貢献しうる。

42. FSB が、その 2017 年のサイバー・セキュリティの規制、ガイダンス、および監督実務の実績評価において、メンバーである管轄区域が全て、自身のサイバー・セキュリティのための規制上のアプローチの策定の際に、「以前策定された、公的当局または

---

[37] 各 G7FE を次のセクションで ICPs に位置付けているが、（ICPs の特定の変更予定が記載されている場合を除き）2017 年の 11 月現在の ICPs に基づいている。

[38] 「本ガイダンスは、金融市場インフラのための原則（PFMI）で定義される FMIs に真っ先に向けられている、つまり、システム上重要な支払システム、中央証券預託機関（CSDs）、証券決済システム（SSSs）、清算機関（CCPs）、および取引情報蓄積機関（TRs）である。しかしながら、関連当局は、本ガイダンスを本レポートで正式にカバーされない種類のインフラに適用することを決定することができる。」CPMI-IOSCO ガイダンスの 1.31

民間組織の、国内または国際的なガイダンスまたは基準の小さな組織を参考にしている」、と報告したと気付いたことは注目に値する。FSB は、この気付きから、「管轄区域は、既存のガイダンスおよび基準が有用であり、また、金融セクターのサイバー・セキュリティの規制と監督においてある程度の国際的なコンバージェンスが存在することを発見した」と結んだ[39]。

43. 本セクションでの議論は、保険監督者に、保険セクターのサイバー・セキュリティに適用される、規制上の制度および監督実務の策定または更新の際に、有用となりうるガイダンスを提供することを意図している。特定の監督モデル、すなわち、原則ベース、ルール・ベース、直接的または間接的などに関する、好みを示してはいない。

3.1　G7FE－要素 1：サイバー・セキュリティの戦略および枠組み

44. **G7FE の 1 番目は、金融機関に対して、「国内外及び業界における標準やガイドラインを適切に踏まえ、自らが対峙するサイバー・リスクに対応したサイバー・セキュリティ・ストラテジーとフレームワークを構築・維持すること。」を求める。**

45. G7 で説明されたように、企業のサイバー・セキュリティの戦略および枠組みの目的は、「サイバー・リスクを総合的かつ包括的な方法で特定、管理および軽減する方法を規定すること」である。上のセクション 2 で記載したように、保険会社が自社のサイバー・セキュリティのアプローチを定める際に、および、監督者が保険セクターのサイバー・セキュリティに適用される、規制上の制度および実務を策定または更新する際に、ならびに、監督者が自身の管轄区域の支配下にある保険会社のサイバー・セキュリティに対する姿勢を調べる際に、国際的な、国内の、および業界の様々な基準ならびにガイドラインが、現在利用可能であり、かつ、考慮されるべきである。

A.　保険コアプリンシプルへの G7FE 要素 1 の位置付け

46. ICP 8 では、「リスク管理および統制」を扱っている。適切なリスク管理戦略およびプロセスの策定に関する ICP 8.1 および補足の指針と整合して、保険監督者は、全ての保険会社に対して、サイバー・セキュリティの戦略および枠組みを策定または採択するよう、かつ、そのような戦略および枠組みを保険会社の取締役会で監視するよう奨励すべきである。

---

[39] 金融安定理事会、『金融セクターのサイバー・セキュリティにおける規制、ガイダンス、および監督実務に関する報告書の概要』（2017 年 10 月）以下で入手可能。http://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory- practices/.

47. 企業のサイバー・セキュリティの戦略および枠組みは当該企業の性質、規模、複雑性、リスク・プロファイル、および文化に合わせて調整すべきであるとの G7FE 1 の説明は、ICPs に内在するプロポーショナリティ原則と整合している[40]。

B. 監督者へのサイバー・セキュリティの戦略およびサイバー・セキュリティの枠組みに関する提言

48. 保険会社のサイバー・セキュリティの戦略および枠組みに関して、監督実務が以下をリスクベースかつプロポーショナルな方法にて奨励または反映することが適切となりうる：

a. サイバー・セキュリティの戦略では、保険会社がサイバー・リスクをどう扱うことを意図しているかに関する原則を明確に述べるべきである。企業のサイバー・セキュリティ戦略は、サイバー・セキュリティの枠組みが当該戦略の目的を達成する能力があることを保証するために、当該企業のサイバー・セキュリティの枠組みと密接に繋がり、かつ、それを補完するものであるべきである。（C/I 2.2.1）[41]

b. 保険会社におけるサイバー・セキュリティの枠組みは、その運営上の安全性と保険契約者のデータの保護の双方を支援および促進すべきである。そのため、枠組みの目的では、保険会社が、保険会社の運営、その評判、ならびに保険会社の保険契約者および第三者のデータ機密性を損ないかねない、サイバー・セキュリティ・インシデントの可能性または影響を限定できるように、保険会社がサイバー・セキュリティ・インシデントを予測し、発見し、耐え、抑制し、かつ回復する能力の維持および促進を目指すべきである。

c. 保険会社の枠組みでは、保険会社がサイバー・セキュリティ・インシデントに実効的実効的に対応し、かつ回復するために、関連するステークホルダーと協調できるようにするために、自社のサイバー・セキュリティの目的および範囲のみならず、サイバー・リスクを管理し、かつタイムリーな連携のために必要な、人、プロセス、技術に関する要件についても、明確に定義すべきである。

d. 当該枠組みは、その実効性を最大化するために、保険会社の取締役会ならびに上級管理職[42]について明確に定義された役割および責任に裏付けられるべきであり、また、

---

[40] IAIS の保険コアプリンシプル（ICPs）の「はじめに」のパラグラフ 8 を参照。
[41] C/I の記載を含むパラグラフは、CPMI-IOSCO WGCR ガイダンスに直接基づくまたは適合される：CPMIIOSCO『金融市場インフラのためのサイバー攻撃耐性に関するガイダンス』（2016 年 6 月）https://www.bis.org/cpmi/publ/d146.pdf にて入手可能。パラグラフ 28 から 31 およびパラグラフ 41 を参照。
[42] 取締役会および上級管理職の役割および定義については、https://www.iaisweb.org/home にて入手可能な IAIS 用語集と同様に ICP 7 を参照されたい。

全役職員が保険会社のサイバー・セキュリティを確保する上で、重要な役割を担うことを認識する文化を創出することは、取締役会および経営陣に責務がある。(C/I 2.1)

e. 保険会社は、自社のサイバー・セキュリティの枠組みを自社の総合的で運用可能なリスク管理の枠組みと一致させるべきである。そのような整合性は重要であり、また、保険会社のサイバー・セキュリティの枠組みが、保険会社がこれまで他の分野のリスクを管理するために確立してきた、方針、手続き、および統制と重複する可能性があることを認識する。例えば、サイバー・リスクは、保険会社の物理的な安全枠組み（例えば、必要不可欠な ICT インフラへのアクセスを制限すること）およびその人的資源の方針（例えば、「インサイダー」の脅威を管理すること）においても、考慮事項とすべきである。(C/I 2.2.3)

f. サイバー・セキュリティの枠組みを文書化するにあたっては、保険会社が実効的自社の直面しているサイバー・リスクを実効的に特定し、自社のサイバー・セキュリティの対象、およびリスク許容度を判断し、また、サイバー・リスクを軽減および管理するために、どのように計画するか明確に述べるべきである。

g. 保険会社のサイバー・セキュリティの枠組みでは、保険会社が、保険契約者、他の保険会社、第三者であるサービス提供者（それら第三者のサービス提供者により提供されるサービスおよび商品を含む)、ならびに、その他の第三者（保険会社のサイバー・セキュリティのエコシステム）など、自社のステークホルダーから負わされ、また、それらに負わせるサイバー・リスクについて、定期的にレビューし、積極的に軽減する方法を検討すべきである。(C/I 2.2.4)

h. サイバー・リスクの管理の実効的なアプローチを維持することは、特に難題である。サイバー・リスクは急速に進展する可能性があるため、保険会社のサイバー・セキュリティの戦略および枠組みは、それらが引続き実効的であるよう確保するために、十分頻繁に見直しおよび更新がなされるべきである。

C. 現行の実務の例

49. フランス。フランスでは、健全性監督破綻処理機構(ACPR) が、サイバー攻撃耐性の監督に深く携わっている。保険会社のサイバー・セキュリティ枠組みは、IT の統制目標ならびに、リスク管理の枠組みを完全なものとすることを含めるべきである。ACPR は、2018 年 3 月 30 日に、銀行および保険セクターにおける IT リスク管理を

統制する共通の基礎を創造するための IT リスクに関するディスカッション・ペーパー[43]を公表した。ACPR は、COBIT 5、NIST、および ISO 2700x 枠組みを用いる。それらに基づき、ACPR は統制を遂行するための独自の方法論を策定した。

50. ドイツ。：ドイツ保険監督法（Versicherungsaufsichtsgesetz－VAG）のセクション 23 に従い、保険会社および年金基金は、基本要件として、自身の IT インフラの適切な管理を含む、適切な事業構造を整備するものとする。VAG のセクション 32 のとおり、それらのガバナンスに関する要件は、外部委託された機能および業務にも適用される。委託された規制（EU）2015/35（Delegierte Verordnung（EU）2015/35－DVO）の 258 条(1)lit.(j)に従い、保険会社は、問題となる情報の性質を考慮して、情報の安全性、完全性、および機密性を保護するものとする。加えて、保険会社にとって、保険契約準備金、内部モデル、および具体的なパラメーターの引受けに関するデータの質に関連し、また、データ処理に関する要件も含む、さらなる法的要件が存在する（例えば、DVO の第 231 条参照）。

51. さらに、ドイツ連邦金融監督庁（BaFin）は、サイバー・セキュリティの具体的な領域に関する詳細な要件を策定することで、ドイツ保険監督法のセクション 23 に規定される、前述の基本的要件を詳細に調べるために、IT 要件に関する回報を発行した[44]。当該回報は、保険会社に対して、少なくとも以下を含まなければならない、IT 戦略を有するよう義務付ける：

- 保険会社の組織上および運営上の IT の構築、ならびに IT サービスの外部委託についての戦略の策定；
- 保険会社がその戦略の基礎とする、確立された基準の IT 分野への配分；
- 責任、および情報セキュリティの組織内への組込み；
- IT の構成に関する戦略の策定；
- IT 問題を考慮した危機管理に関する声明；および
- 事業分野において運営および／または策定される IT システム（ハードウェアおよびソフトウェアの構成要素）に関する声明

[43] ACPR、『IT リスクに関するディスカッション・ペーパー』（2018 年 3 月）、以下で入手可能。https://acpr.banque-france.fr/node/61411

[44] 2018 年 7 月 2 日に発行した。以下で入手可能。
https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2018/meldung_180702_VAIT.html;jsessionid=87 8A1EFA012BA43394020C9F38DF4EDD.2_cid363

52. オランダ。オランダ銀行（DNB）は、情報セキュリティに関する評価枠組みを公表した[45]。当該枠組みは、保険会社が、サイバー攻撃耐性を含む、自社の情報セキュリティの習熟度を評価する際に使用できる。DNB は、当該枠組みをセクターの年次評価を行う際にも同様に使用する。当該枠組みは、オランダの金融監督法にリンクしている。さらなる情報は、セクション 4 で、事例研究と合わせて提供されている。

53. カナダのケベック州。金融市場監督局（AMF）の総合的なリスク管理ガイドライン[46]の目的の 1 つは、各保険会社内の重大なリスクについて、特定、評価、定量化、統制、軽減、および慎重にモニターするための戦略、方針および手続きにより裏付けられる、十分な管理枠組みの企業による導入である。企業の情報・通信技術に関連するサイバー・リスクは、本枠組みにおいて AMF が考慮する多くのオペレーショナル・リスクの内の 1 つである。

54. したがって、保険会社における健全かつプルーデントな経営実務を促進しようと努める監視業務の一環として、AMF はそのガイドラインで明記された原則が、各機関の具体的な特徴を考慮して、フォローされる程度を評価する。導入された戦略、方針、および手続きの有効性ならびに関連性だけでなく、取締役会および上級管理職によって遂行される監督ならびに統制の質についても評価される。

55. AMF は、認識されたサイバー関連の（NIST および COBIT などにより公表された）国際的な基準およびプロセスに基づいて、自己評価のため詳細なツールを策定した。当該ツールは、保険会社のリスク・プロファイルに基づいてサイバー・セキュリティに対する姿勢を評価するために、および AMF に報告するために保険会社によって使用される。固有の（最初の G7FE 要素への）関連性の質問の中で、当該ツールでは、機関が特定の人物に、サイバー・セキュリティの枠組み、ならびに関連する計画および戦略の策定と導入を担当するよう指名するべきであるとの AMF の期待を明確に定めている。

56. AMF はあらゆるケースにおいて、全てのガバナンスの枠組みが、保険会社の性質、規模、複雑性、およびリスク・プロファイルに基づいて策定および導入されるよう期待しており、また、保険会社が枠組みの有効性を確保するよう期待している。

---

[45] DNB、『DNB の情報セキュリティの調査に関する評価枠組み―2017』（2017 年 4 月）、以下で入手可能。
http://www.toezicht.dnb.nl/en/3/51-203304.jsp

[46] AMF、『総合的なリスク管理ガイドライン』（2015 年 5 月）、以下で入手可能。
https://lautorite.qc.ca/en/professionals/insurers/guidelines/

57. スイス。スイスの議員は、原則ベースで、リスクに由来する、保険会社の監督アプローチを制定した。

58. この点に関して、保険監督法（ISA）[47]の第 22 条では、保険会社が全ての主要なリスクを特定、統制、および制限できるよう要求している。同条に従うと、連邦委員会は、関連法令を制定し、一方、FINMA は保険会社によるリスクのモニタリングを規制する。民間保険会社の監督に関する規則[48]の第 96 条では、保険会社のリスク管理に関する要件を言明している。

59. さらに、FINMA の回報 17/2「コーポレート・ガバナンス－保険会社」[49]に規定される、保険会社用の法規定および包括的なガバナンス原則に従うと、FINMA は、保険会社に対して、実効的なガバナンスの枠組みのみならず、サイバー・セキュリティに関する適切なリスクと統制の環境を整備するよう期待している。この広範な規制は、FINMA が G7FE のその他の構成要素を同様に導入することを許可する。そのため、FINMA は、保険会社に対して、主要な基準およびガイドラインの双方、ならびにプロポーショナリティ原則を考慮する適切なサイバー・セキュリティの戦略および枠組みを維持するよう強く要請することができる。

60. 具体的な分野における監督対象の習熟度の一般的な程度をモニターするために、FINMA は通常、自己評価に基づく調査を利用する。しかしながら、特に不正の証拠が存在するケースでは、徹底した立入りでのレビューが行われる可能性がある。そのような立入りでのレビューの間に発見された事項によっては、保険会社は、規制違反を一掃する期日を含めた活動計画を策定し、FINMA に提出して承認を得るよう求められる可能性がある。FINMA は、通常、そのような活動計画の実施を綿密にモニターする。加えて、FINMA は、受任者（mandataries）として知られ、FINMA がその任務を遂行する際に支援する第三者を任命することができ、それによって、監督および強制手続きの双方において、この効率的で、資源を節約するツールの対象を絞った利用となる。

---

47 『保険監督法』、以下で入手可能。https://www.admin.ch/opc/de/classified-compilation/20022427/index.html.

48 『民間保険会社の監督に関する規則』、以下で入手可能。
https://www.admin.ch/opc/de/classified-compilation/20051132/index.html

49 FINMA、回報 17/2『コーポレート・ガバナンス－保険会社』、以下で入手可能。
https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2017-02.pdf?la=en.

61. 英国。英国の金融行動監督機構（FCA）は、過去 3 年にわたり、サイバー攻撃耐性を監督上の主要な優先事項として定めており、それを継続している。FCA ハンドブックでは、サイバー・リスクの監督に関連する、事業運営のための多くの原則を詳述している。当該原則は、英国金融規制制度に基づく、企業の基本的な義務の概論である。原則に違反すると、企業は懲戒処分を科されることになる。特にサイバー・リスクの監督に関連する原則は以下となる：

- 原則 2－技能、慎重性と勤勉性；企業は、自社の事業を適切な技能、慎重性と勤勉性をもって遂行しなければならない。
- 原則 3－管理および統制；企業は、十分なリスク管理制度を備えた上で、自社の業務を、責任をもって、かつ実効的に組織および統制するために、妥当な注意を払わなければならない。
- 原則 11－規制者との関係；企業は、自社の規制者にオープンかつ協力的な方法で対応しなければならず、また、規制者が合理的に通知を期待するであろう、企業に関するあらゆる事項について、適切に FCA に開示しなければならない。

62. これらの原則の下で、FCA は、適切な技能、慎重性と勤勉性でサイバー・リスクを管理する能力のある、相応な技能を有する上級スタッフを企業が雇用すべきであると考えており（原則 2）、企業は、リスクの変位性および複雑性を認識した上で、サイバー・リスクを適切に評価できるリスク管理制度を採用すべきであり（原則 3）、また、FCA が、サイバー・リスク管理の取決めにおいて重大な不備、またはその他の重大なサイバー事象があれば、それについて知らされていると考えている（原則 11）。

63. 米国。米国では、サイバー・セキュリティおよびデータ・セキュリティは国内の政策課題であり、連邦および州の公的セクターの企業間の調整、ならびに、公的セクターと民間セクター間の協力関係を必要とする。したがって、連邦当局は、データ・セキュリティと、データ漏えいの告示法と規制の調整を推進しながら、州の規制者と保険会社と共に、業界のサイバー・セキュリティを向上させるために取組んでいる。

64. 全米保険監督官協会（NAIC）は、2017 年に、データ・セキュリティ、捜査、および違反の通知を取扱う、保険会社、エージェント、および他の免許付与された事業体のための規則を設定する、『保険データ・セキュリティ・モデル法』[50]を採択した。これには、継続的なリスク評価に基づいて情報セキュリティ・プログラムを維持すること、第三者であるサービス提供者を監視すること、データ漏えいを捜査し、かつ規制者に「サイバー・セキュリティ事象」を通知すること、が含まれる。2019 年 1 月 1

50 『保険データ・セキュリティ・モデル法』、以下で入手可能。http://www.naic.org/store/free/MDL-668.pdf

日に施行される NAIC 保険データ・セキュリティ・モデル法について、南カリフォルニアが、米国において制定する最初の州である。

65. NAIC のメンバーは、50 の州の保険規制当局の長官で構成され、コロンビア特別区、および 5 つの米国の領域は、米国における主要な保険規制者である。NAIC の全てのモデル法と同様に、『保険データ・セキュリティ・モデル法』は、発効するためには、州レベルで立法化される必要がある。2017 年の 10 月に、米国財務省は、「データ・セキュリティ、データ漏えいの通知、および、より広範に、サイバー・セキュリティとは…国家の関心事である」と述べ、また、州による『保険データ・セキュリティ・モデル法』の迅速な採択を推奨し、また、州が「保険会社にかかるデータ漏えいの通知に関する統一法を早急に通過させるために取組む」よう推奨した[51]。

66. NAIC の『保険データ・セキュリティ・モデル法』のセクション 4A では、保険会社に対して[52]、「保険会社の規模および複雑性、保険会社の活動の性質および範囲で、第三者であるサービス提供者の利用も含み、また、当該保険会社によって利用される、もしくはその保険会社が所有、保管、または支配している、非公開情報の保護必要度に見合った」「情報セキュリティ・プログラム」の導入を要求している。

67. 加えて、NAIC の『財政状態審査官のハンドブック』（審査官のハンドブック）では、規制者が財務の審査プロセスの一環として利用するガイダンスを規定し、また、保険会社が自社のサイバー・リスクに対処しているかどうか、およびどのように対処しているかのレビューを含んでいる。『審査官のハンドブック』は、NIST の、特定、保護、発見、対応、および回復の機能を組込むように、最近更新された[53]。スコーピング・プロセスの一環として、審査官は、規制者に対して、審査の開始時に戦略および枠組みの差異、または問題について特定する機会を与えるために、通常、保険会社のサイバー・セキュリティ戦略および枠組みを含む、各保険会社の方針一式についての書類を入手する。

68. ニューヨーク州金融サービス局（NYDFS）は、金融サービス会社に関するサイバー・セキュリティ要件を定める規制である、2017 年 3 月 1 日発効の、23 NYCRR、パート 500[54]を公布した。

---

51 米国財務省、『経済的好機を生み出す金融システム：資産管理と保険』（2017 年 10 月）、以下で入手可能。
https://www.treasury.gov/press-center/press-releases/Documents/A-Financial-System-That-Creates-Economic-Opportunities-Asset_Management-Insurance.pdf

52 『保険データ・セキュリティ・モデル法』は、保険会社を含む「免許所有者」の用語を使用する。読みやすさのため、本ペーパーでは、「保険会社」の用語は、「免許所有者」に置き換えられる。

53 NIST のサイバー・セキュリティの枠組みは、上で論じられている。

54 NYDFS の『金融サービス会社に関するサイバー・セキュリティ要件』、以下で入手可能。

69. NYDFS の*『金融サービス会社に関するサイバー・セキュリティ要件』*のセクション 500.02 では、保険会社[55]は「対象とした企業の情報システムの機密性、完全性、利用可能性を保護するために設計された、サイバー・セキュリティのプログラムを維持する」ことを要求される。

D. G7FE の要素 1 の結果の評価

70. G7FEA に基づき、「実効的なサイバー・セキュリティに付随する結果」は 5 つ存在する。G7FEA の結果のどれもが各 G7FE 要素に適用できるわけではない。しかし、それらをまとめると、「望ましい 5 つの結果は、…サイバー・セキュリティについての十分に習熟した理解、受渡し、および監視を備えた金融セクターの企業が、評価者に実証することができる、広範な特性を定める。」保険会社と監督者の双方は、適切であれば、この評価ガイダンスを「規制上の審査、自己評価、および第三者による独立した審査において」活用すべきである[56]。

71. G7FE の項目 1 について、G7 により提案された、望ましい結果は以下となる：

72. **G7FEA 結果 1－基礎的要素（G7FE）が整備されている。**G7FE は、サイバー攻撃耐性を構築する初期段階にある企業と、より習熟した企業の双方に対して、サイバー・セキュリティのための基礎的要素を提供する。

73. G7FE は広範にわたり、困難な性質を反映している。実効的なサイバー・セキュリティでは、企業がサイバー・セキュリティの戦略および枠組みを維持し（要素 1）、また、自社のガバナンスのプロセスを適合させる、または強化するよう求める（要素 2）。緩和統制、および保護メカニズムの関連する一式を含む、リスクと統制の枠組み（要素 3）ならびに、実効的なモニタリング（要素 4）を求める。明確に定義され、かつ、定期的に実施される対応（要素 5）および回復（要素 6）の手続きが、破壊的なサイバー事象のケースで整備されている。最後に、情報共有（要素 7）および継続的学習（要素 8）が、各 G7FE を強化し、また、全体的なサイバー・セキュリティの増強に寄与する。

---

https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

[55] NYDFS の『金融サービス会社に関するサイバー・セキュリティ要件』では、「対象とされた企業」の用語を、対象とされた企業の定義を満たす保険会社で、パート 500.19 の規定に基づいて免除されない保険会社を含むものとして使用する。読みやすさのため、本ペーパーでは、「保険会社」の用語は、「対象とされた企業」（

[56] G7FEA の 2 頁。

74. **G7FEA 結果 2－サイバー・セキュリティは組織の意思決定に影響する。**要素 1（サイバー・セキュリティの戦略および枠組み）および 2（ガバナンス）を基礎として、企業の通常の意思決定プロセスにサイバー・セキュリティを組み込むこと、特に、サイバー・リスクの管理をそれらのプロセスの初期に含めることで、組織にわたり戦略的結果を特徴付け、また促進する。サイバー・セキュリティは、企業の中核の事業プロセスの概念、デザイン、および運営とは別物として見なされるべきではなく、新たな商品およびサービスを開発する際、および既存の技術またはインフラを活用する事業運営の有効性を評価する際の双方で、戦略上の主要な考慮事項として見なされるべきである。

75. 上級管理職または取締役会のレベルでの積極的な関与は、サイバー・セキュリティ・プログラムのデザイン、実施、および有効性の監視を示唆する。脅威、および脆弱性、ならびに企業のリスク選好に関する情報を受けて、取締役会または上級管理職は必要に応じて、リスク管理についての決定、監視、ならびに短期および長期の双方の説明責任を推進することができる。このように、取締役会および上級管理職は、サイバー・セキュリティ・プログラムを、伝統的なコンプライアンスの見方を超えて推進させるために意思決定を利用することができる[57]。

3.2 G7FE－要素 2：ガバナンス

76. **G7FE の 2 番目は、金融機関に対して「サイバー・セキュリティ・ストラテジーとフレームワークを実施し、管理し、有効性を確認する役職員の役割・責任を明確化し、これらの手順を促進することにより、アカウンタビリティを確保すること。また、当該役職員に対し、十分なリソース、適切な権限、経営陣等（例えば、企業にあっては取締役会、当局にあっては幹部）へのアクセスを付与すること。」を求める。**

77. 一般的に、「サイバーのガバナンス」とは、機関がサイバー・リスクを管理するアプローチを定め、導入し、また見直すために備えた取決めのことを言う。強固なサイバーのガバナンスは、保険会社が直面している、蔓延し、新たに発生するサイバー・リスクを管理するための、体系的かつ積極的なアプローチを維持する一助となる。また、保険会社が組織内のあらゆるレベルでのサイバー・リスクを適切に考慮し管理する一助となるだけでなく、それらのリスクに対処するための適切なリソースおよび専門知識を一貫してもたらす。(C/I 2.1)

A. 保険コアプリンシプルへの G7FE 要素 2 の位置付け

[57] G7FEA 結果 2 についての本パラグラフは、取締役会および上級管理職の間の責任の分担について定義することを意図していないという IAIS の見解を反映するために、原案から修正された。

78. 「実効的なガバナンス構造」、「説明責任」、および「責任ならびに報告系統および上程」の明確な表現のみならず、「運営ユニット、情報テクノロジー、リスク、および統制関連の活動」の中で優先事項と連携に取組むことに関する G7FE 2 の強調は、ICP 7（コーポレート・ガバナンス）と整合している。

79. ICP 7 では、「保険事業の健全でプルーデントな経営および監視を規定し、かつ、保険契約者の利益を十分に認識し保護するコーポレート・ガバナンスの枠組み」を求めている。

80. さらに、ICP 8（リスク管理）では、「その全体的なコーポレート・ガバナンスの枠組みの一部として」保険会社は、「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実効的な機能を含む、リスク管理および内部統制の実効的なシステム」を備えるよう要求する。ICP 8 の文書では、典型的なガバナンスのアプローチでは、「3 つの防衛線」モデルを組込んでいると注記している[58]。

B. 監督者へのガバナンスに関する提言

81. サイバー・セキュリティのガバナンスに関して、監督実務で以下をリスクベースかつプロポーショナルな方法にて奨励または反映することが適切となりうる。

a. 保険会社の取締役会は、上級管理職と連携して、最終的に戦略を設定する責任を負うべきであり、上級管理職に、サイバー・リスクが実効的に管理されていることを確認するよう求めるべきである。実効的取締役会は、保険会社のサイバー・セキュリティの枠組みおよび保険会社のサイバー・リスクに対する許容度を監視すべきである。

b. さらに、取締役会は、保険会社のサイバー・リスクのプロファイルについて、それが保険会社のリスク許容度のみならず、保険会社の全体的な事業目的に引続き整合していることを確保するために、定期的に知らされるべきである。上級管理職は、必要に応じて取締役会と協議し、保険会社の商品、サービス、方針または実務に加えた変更、および脅威となる状況が、保険会社のリスク・プロファイルに実質的に影響するかどうか検討すべきである。

c. 上級管理職は、保険会社のサイバー・セキュリティの枠組みの導入、およびその枠組みを支える方針手続き、ならびに統制について、入念に管理すべきである。

[58] ICP 8.2.3 および脚注 11。

d. 保険会社の取締役会および上級管理職は、サイバー・セキュリティについての認識およびそれへの関与を深めるべきである。取締役会および上級管理職は、サイバーの脅威によりもたらされるリスクに関して、監視および管理の役目に適切な技能を備えたメンバーを含めるべきである。加えて、取締役会および上級管理職は、全てのレベルの職員が保険会社のサイバー・セキュリティの確保に重要な役割を担っていること、および、規範を示して指導することを認識する（企業）文化を推進するべきである。（C/I 2.3.2, 2.3.3）

e. 保険会社は、組織内での役割および責任の定義を含む、情報セキュリティの方針、手続き、およびプロセスを備えるべきである。それらの方針、手続き、およびプロセスには、第三者であるサービス提供者の監視のみならず、サイバー・リスクの管理プロセス、ならびに優先事項、制約、引受、およびリスク許容水準の決定を含めるべきである。

f. 特に、各保険会社は、組織内のサイバー・セキュリティの枠組み全体に責任および説明責任を有する上級管理者を指名すべきである。この役割では、十分な権限、独立性、リソース、および取締役会への面会を有するべきである。この役割を遂行する上級管理者は、管理職レベルでのサイバー・セキュリティのイニシアティブを有能に計画し、かつ、実行する必要不可欠な専門技能および知識を備えるべきである。（C/I 2.3.4）

g. 保険会社は、適切であれば、および、プロポーショナリティ原則と整合して、独立した法令遵守のプログラムおよび、サイバー・セキュリティの枠組みを評価し、導入度を測定する資格を有した個人により実行された監査を通したものを含め、取締役会および上級管理職が、保険会社のサイバー・セキュリティの枠組みの十分性および有効性を評価および測定する際の一助となるよう、評価プログラムを導入すべきである。（C/I 2.2.7）

C. 現行の実務の例

82. フランス。ACPR は、サイバー・セキュリティのシステム（組織およびガバナンス）の習熟度のレベルを評価するための、および、保険会社が、ソルベンシーⅡ委任法令の第 258 条パラグラフ 1 を遵守しているか検証するための、IT 統制を遂行する。これらの統制では、ガバナンスのシステムが、サイバー・リスクをカバーするために展開されていること、および、当該リスクに関する情報が、全ての重要な管理職のレベルで共有されていることを検証するよう意図されている。

83. ドイツ。BaFin の IT 要件に関する回報によると、管理委員会は、組織上および運営上の IT 構造の規制は、IT 戦略に基づいて決定されていること、および、組織の活動およびプロセスにおけるあらゆる変更を可能な限り反映するため修正されることを確認する責任を有する。

84. 特に、保険会社は、人数および資質の双方の観点から、情報リスク管理、情報セキュリティ管理、IT 運営とアプリケーション開発に適切に職員を配置しなければならない。

85. カナダのケベック州。AMF は、健全かつプルーデントな管理実務をフォローする、金融機関の法的要件に関する期待について規定するガイドラインを定める。AMF は、ガバナンス、総合的なリスク管理およびコンプライアンス（GRC）を、健全かつプルーデントな保険会社の管理の礎石と見なしており、それゆえ、AMF により提供される健全性枠組みの基礎と見なしている。

86. AMF は、そのガバナンスのガイドラインの一部として、金融機関が、正式な運営上の枠組み、金融機関の経営を組織および監視するのを支援する、方針、手続き、ならびに情報システムを通じたモニタリングおよび説明責任を導入することで、実効的かつ効率的なガバナンスを備えていると期待する。また、AMF は、取締役会および上級管理職の役割および責任が、それらのメンバーが有能かつ独立して行動するよう確保するために、明確に定義され、かつ分離されていることを期待する。この点、AMF は、金融機関が、役割および責任を描くための信頼できる構造を示す、3 つの防衛線の採用を奨励するが、その理由は、全ての種類の機関に適切であり、また、その性質、規模、複雑性およびリスク・プロファイルに応じて適応可能なためである。

87. サイバー・セキュリティに関して、AMF は、その監督活動の一環として、IT の使用が組織の業績にプラスに貢献することを確保するために、組織への IT の健全なガバナンスの導入を推奨する。このことは、ISO および COBIT の認識された枠組み、原則およびプロセス（例えば、ISO 38500、EDM01 ガバナンス枠組みの設定および維持の確保、EDM03 リスクの最適化の確保、EDM05 ステークホルダーの透明性プロセスの確保）を用いて行われる。AMF はその活動の中で、情報・通信テクノロジーに関連するリスク（サイバー・リスクを含む）を管理するための戦略および枠組みの継続的な開発もレビューし、また、説明責任を強化するための一連の役割および責任（責任－説明責任－相談－通知のチャート）に重点を置いている[59]。

[59] AMF の『ガバナンスのガイドライン』（2016 年 9 月）、以下で入手可能。
https://lautorite.qc.ca/en/professionals/insurers/guidelines/.

88. 英国。FCA は、その監督上の戦略を英国の国家サイバー・セキュリティ・センター（NCSC）の戦略、「国家サイバー・セキュリティ戦略 2016 年－2021 年」[60]、および付随するガイダンスの公表物に合わせた。特に、FCA は、サイバーを取締役会レベルの責任と考えており、また、金融機関の取締役会が、独立した専門家にアクセスし、自身の責任を彼らに実効的に委譲できるべきであると考えている。FCA は、企業だけでなく、本文書で言及したものを含め、既存の国際的な枠組みを監督する際、NCSC の公表物「10 のステップ：取締役会レベルの責任」[61]を参照する。

89. 米国。NAIC の『保険データ・セキュリティ・モデル法』のセクション 4E では、保険会社が取締役会を設置している場合、当該取締役会に、情報セキュリティ・プログラムの監視を規定するよう要求している。取締役会は、幹部経営陣に対して、情報セキュリティ・プログラムを導入するよう要求しなければならない。また、取締役会は、幹部経営陣に対して、情報セキュリティ・プログラムの状態、保険会社の法令への遵守状況、および、「リスク査定、リスク管理・統制に関する決定、第三者サービス提供者の取決め、テスト結果、サイバー・セキュリティ事象、または違反、およびそれに対する経営陣の対応、ならびに、情報セキュリティ・プログラムにおける変更への提言」を含む、情報セキュリティ・プログラムに関連するあらゆる重大事項について、取締役会に対して書面で報告するよう要求しなければならない。

90. NAIC の『審査官のハンドブック』では、会社のガバナンス構造は、審査の間の通常分野（つまり、会社運営の全体論的視野の一部として）、最も厳重に評価される。しかしながら、『審査官のハンドブック』には、IT のガバナンス・モデルの十分性のレビューおよび評価の具体的なテスト手続きが含まれる。テストには、組織図、報告系統、主要な IT 担当役員の略歴、および、取締役会の委員会の活動のレビューを含めてもよい。『審査官のハンドブック』のガイダンスでは、取締役会／上級管理職による会社のサイバー・セキュリティ・プログラムの監視についてのレビューの重要性を強調している。

91. NYDFS の *『金融サービス会社に関するサイバー・セキュリティ要件』* のセクション 500.03 では、文書化されたサイバー・セキュリティ方針が高官または保険会社の取締役会によって承認されるよう要求している。当該方針では、保険会社の「自社の情報

---

60 FCA の『国家のサイバー・セキュリティ戦略 2016 年－2021 年』（2017 年 9 月更新）、以下で入手可能。
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

61 NCSC の『10 のステップ：取締役会レベルの責任』（2016 年 8 月更新）、以下で入手可能。
https://www.ncsc.gov.uk/guidance/10-steps-board-level-responsibility

システムおよびそれらの情報システムに蓄積される非公開情報の保護に関する方針および手続き」を規定しなければならない。セクション 500.04 では、保険会社に対して情報セキュリティ最高責任者（CISO）を指名するよう要求する。CISO は、少なくとも年に 1 度、取締役会に対して報告を行うものとする。セクション 500.17 では、保険会社の取締役会または高官に対して、規制の遵守を認証するよう要求する。

D. G7FE の要素 2 の結果の評価

92. G7FE の番目 2 について、G7 により提案された、望ましい結果は以下となる：

93. **G7FEA 結果 1－基礎的要素（G7FE）が整備されている。**上のパラグラフ 72-73 で議論されている。

94. **G7FEA 結果 2－サイバー・セキュリティは組織の意思決定に影響する。**上のパラグラフ 74-75 で議論されている。

3.3 G7FE－要素 3：リスクおよび統制の評価

95. **3 番目の基礎的要素は、金融機関に「相互接続関係や依存度、外部委託の状況も踏まえ、機能・業務・製品・サービスを特定し、それらの重要性に優先順位を付した上で、それぞれのサイバー・リスクを評価すること。経営陣によって設定された許容度の範囲内で、こうしたリスクを統御・管理するため、システム、方針、手順そして訓練を含めた管理手法を確定・実施すること。」を求める。**

96. したがって、「理想的に全社的リスク管理プログラムの一部として」、企業は、人、手続き、技術ならびに認識された各機能、活動、商品およびサービスをサポートする根本的なデータによって提示された固有のサイバー・リスク（または補償統制を欠くリスク）を評価すべきであり、そして「残りのサイバー・リスクに到着するために認識されているリスクを防ぐための制御の存在および実効性を認識および確認する。」

A. 保険コアプリンシプルに G7FE 要素 3 を位置付ける

97. G7FE 要素 3 は ICP8（リスク管理）に一致する。この基準のもとに、ICP8.1 に記されているように：「監督者は、保険会社に対し、実効的なリスク管理システムを確立し、またその下で業務を行うよう要求する。」さらに、リスク管理システムは、「保険会社のあらゆるリスクの認識、評価、モニタリング、軽減およびタイムリーな報告を可能にする。それは、リスクの蓋然性、潜在的影響および想定期間（タイムホライゾン）も考慮に入れる」べきである。

98. 論点書に要約されているように、ICP8 指針は、リスク管理システムが含むべきカテゴリーの最小のセットを記す。これらは、「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手法」を含む。加えて、ICP8 指針は、リスク管理システムは、現行および新たに発生するリスクを含む、全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するべきである、と記す。

99. ICP8 指針は、内部統制システムの典型的な構成要素についても記述する。「方針および手続き」の構成要素についての記述は、実効的な内部統制システムは「重要な IT 機能」、ならびに「従業員による IT システムへ」および「データベースへのアクセス」を含む「事業決定および取引に対する適切な統制」を含むべきであると説明する。

100. 加えて、ICP8 指針は、適切な IT／管理情報手続きを含む統制機能に十分なリソースを委ねるための保険会社への必要性に対応する。内部監査機能は、企業の経営をサポートするために保険会社の IT アーキテクチャの継続的な能力に関して、取締役会および上級管理職に独立した保証を提供すべきである、と記す。

101. また外部委託取決めは、取締役会および上級管理職が外部委託取決めを始めるまたはリバイスを行う際に、保険会社のリスク・プロファイルおよび事業継続性が熟考された取決めによって、どのような影響を受けるかという記載がなされている ICP8 指針に対応している。特に ICP8.8 は、「監督者は、保険会社に対して、外部委託されるあらゆる重要な業務または部門（統制機能など）について、少なくとも外部委託されない業務または部門に対するのと同程度の監視および責任を維持するよう要求する。」と記す。これは、サイバー・セキュリティに関するサービス提供者のガバナンス、リスク管理および内部統制に適用することができる。

102. 最後に、ICP19（事業行為）もまた G7FE3 に関連する。この基準のもとに、ICP19.12 は、「保険会社および仲介人に対し、顧客に関する情報の保護および利用に係る方針および手順を整備することを求める」ことを監督者に要求する。そのような方針および手順の例として、ICP19.12 は「サイバー攻撃のリスクなどの個人情報のプライバシーを脅かす可能性のある新しいリスクの潜在的な影響を評価し、また内部統制、技術および研修などの手段を通じ、これらの影響を軽減するための適切な措置を取る」[62]と言及する。

[62] ICP19.12.5

B. リスクおよび管理の評価に関する監督者の提言

103. 保険会社のサイバー・セキュリティ・リスクおよび管理の評価に関し、監督上の実務は、以下を促すまたは反映させることが適切だろう：

機能の認識および分類

a. 監督者は、全体としてのリスク管理システムについて機能を担うにあたり、それぞれの機能および支援手続きの重要性ならびに相互依存性を徹底的に理解していることを確保するために、ビジネス機能および支援手続きの認識ならびにリスク評価を実施する中で、十分にサイバー・リスクについて説明すべきである。認識されたビジネス機能および手続きは、保険会社の保護、探索、応答および再生努力の優先順位付けを順番に導く重要性の観点から、保険会社によって分類されるべきである。（C/I 3.2.1）

b. 実行可能な限り、保険会社は、ビジネス機能および手続きとして使用可能な資産を常時把握するために、他の内部および外部システムを伴い相互関連性を含む情報資産およびシステム構成の現状の一覧表または位置づけを、認識および維持すべきである。保険会社は、資産のリスク評価を行い、重要性という点で分類されるべきである。

c. 位置づけ手続きの一部として、保険会社はまた、例えば、第三者のサービス提供者のような、情報資産およびシステム構成を認識すべきである。

d. 一覧表は、ハードウェア、ソフトウェアのプラットフォームおよびアプリケーション、デバイス、システム、データ、職員、外部情報システム、重要なプロセスならびに期待されたデータフローに関する文書を含むべきである。

e. 保険会社は、誰が情報資産および支援システムを使用可能かということを知るために、ならびにアクセス権限が必要以上に広くないことを保証ならびに変則的な活動を認識および探索することを容易にするという両方の情報を利用するために、個人およびシステムの両方へのアクセス権限についての現状の記録を認識および維持すべきである。

f. 保険会社は、現状態、正確性、および完全性の維持が保証されるために、重要なビジネス手続き、機能、単独およびシステムの資格証明書のリストならびに情報資産の一覧表に関する規則的なレビューを促進させるために、認識する取り組みの収集および変更管理のような他の関連する手続きを調整すべきである。（C/I 3.2.3）

g. 同様に、保険会社は、サイバー・リスクによるビジネスへの影響の分析を実施すべきである（すなわち、脅威、脆弱性、類似性、影響の認識を通じたリスクの決定およびリスク対応の優先付け。）

リスク・プロファイルにおけるサイバー・リスクの保証対象

h. 保険会社のリスク・プロファイルは、内部および外部の両ソースから生じうるサイバー・リスクにさらされている主要なオペレーション分野を認識すべきである。

i. 全社的なリスク・プロファイルの発展とともに同じ取扱い規則を使用する中で、保険会社は、その会社がさらされている全てのサイバー・リスクについて記述することを目標とするだろう。リスク・プロファイルは、被害の可能性および影響の評価を含む評価プロセスを含めることにより、恩恵を受ける可能性がある。更に詳細な段階では、リスク・プロファイルは、保険会社の脆弱性調査および管理手続きを含み、またそれによって通知される場合がある。典型的な脆弱性管理システムは、脆弱性による影響の評価と同様にプラットフォーム、ソフトウェアの欠陥、および不適切な構成の列挙を含む[63]。

j. 例えば、以下のカテゴリー内では、両プロセスによる洞察が体系化される：（1）技術および接続の種類；（2）提供チャネル；（3）組織特性；（4）外部脅威[64]

- *技術および接続の種類。*特定の技術および接続の種類は、複雑性ならびに保険会社の特定の技術商品またはサービスの習熟度、接続および性質によって高いサイバー・リスクを課す場合がある。例えば、保険会社は、インターネット・サービスプロバイダー（ISP）および第三者とのシステムのホストが内部または外部委託のどちらとなっているか、安全でない接続の存在および数、無線アクセスの使用、ネットワークデバイスの容量、EOL システム、クラウドサービスの程度ならびに保険会社職員による個人的なデバイスの利用の接続の数を確認することが適切である場合がある。
- *提供チャネル。*保険会社は、一部の商品およびサービスの提供チャネルが、提供された特定の商品またはサービスによって、高度化されたサイバー・リスクを課す場合があることを認識すべきである。サイバー・リスクは、提供チャネルの種類および数の増加によって増加する。例えば、オンラインおよび可動提供チャネルは、保険会社に対しリスクの増加段階を示す場合がある。

---

63 「NIST PR.IP-12: 脆弱性管理計画は発達し、実装された」（参考情報は NIST SP 800-53 Rev.4 RA-3, 5, & SI-2 を含む）「重要なインフラサイバー・セキュリティ発展のためのフレームワーク」（2018 年 4 月 16 日に発表されたバージョン 1.1）「表 2：フレームワークコア」内の、以下で入手可能。
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

64 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」（2017 年 5 月更新）以下で入手可能。https://www.ffiec.gov/cyberassessmenttool.htm

- *組織特性。*これらの考慮すべき特性は、過去のおよび計画された合併、分裂、収集および販売、特権アクセスを有するユーザーの数、IT 環境、事業所在地、（レガシーシステムを含む）オペレーションセンターおよびデータセンターの所在地の変更、ならびにクラウドサービス提供者を含む第三者のサービス提供者に対する信頼を含む。
- *外部脅威。*外部脅威は、特に、（試みたおよび成功した）攻撃の量および種類は、保険会社のサイバー・リスク・エクスポージャーを反映し、影響を与える。保険会社は、保険会社を標的とした攻撃の量および複雑さおよび他の類似した状況の組織について考慮すべきである。

先を見越した技術および手続きの実施

k. 保険会社は、（バックアップシステムやオフラインデータストアを含む）保管中、輸送中、保管中のデータが、保持している情報の重要性と分類に見合ったときに保護するべきである。

外部委託管理

l. 多くの保険会社のシステムおよび手続きは、クラウドサービス提供および外部委託機能を有する提供者を含む多数の第三者と直接的または間接的に相互に関連付けられている。それらの法人のサイバー・セキュリティは、保険会社が直面するサイバー・リスクに著しく影響を与える場合がある[65]。保険会社は、定期的に実行されるレビューを通じ、また状況の変化を正当とし、第三者より提示されたサイバー・リスクを、先を見越して管理すべきである。

m. 保険会社は、保険会社とその顧客のデータを保険会社に期待されるものと同程度に保護および安全性を守るために、第三者であるサービス提供者が適切な管理上、技術上、および物理上の措置を講じていることを確認すべきである。

n. 保険会社は、第三者が保険会社に課す場合があるリスクの重大性が、必ずしも　保険会社のビジネスとしての関係性の重要度に比例しないことを認識すべきである。したがって保険会社は、第三者から生じ第三者に課されるサイバー・リスクを認識し、実践可能な限り、第三者は、保険会社およびその投資家の全体的な耐性を向上させる目的で独自で耐性の仕組みを設計し実施しているため、関連するステークホルダーと協調すべきである。（C/I 3.3）

---

65 例えば、Dave Shackleford の「サプライチェーンにおけるサイバー・リスクへの対抗」（2015 年 9 月 SANS Institute）を参照。以下で入手可能。https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252

状況認識の強化

o. 保険会社は、直面するサイバー・リスクについて適切な状況認識を有するべきである。保険会社は、期待されたサービスの実施または提供能力に著しく影響を与える、もしくは、機密データの保護を含む、自身の義務を果たす能力に対し重要な影響を与えるサイバー脅威を、先を見越して認識するよう努めるべきである。保険会社は、定期的にこの分析をレビューし、更新すべきである。

p. 考慮に入れられるべきサイバー脅威は、たとえそれらが起こりにくいまたは過去に一度も起きたことがないとしても、極端であるものの起こりうるサイバー事象を引き起こす脅威を含むべきである。評判に加え、保険会社は、保険会社のビジネス手続きおよび契約者データの機密性、完全性および有用性に対する脅威を考慮に入れるべきである。従業員または第三者のサービス提供者のような内部および外部のソースから生じる脅威は、個々に、考慮に入れられるべきである。（C/I 8.2.1）

C. 現行実務の例

104. ヨーロッパ連合。ヨーロッパ連合では、ソルベンシーⅡのもと、ERM 枠組み[66]は、オペレーションに関わるおよびより正確な IT リスクを含むべきである。この監督者は、特に異なるチーム同士との侵入テストおよび面接を経由して外部および内部のネットワークを標的とする。携帯電話によって持ち運ばれているアプリケーションは、データ保護の段階を管理するために一部の事例にて試されている。サイバー・リスクは、リスク管理の文書化された方針にて対応されるべきである。最初の主な目標は、ソルベンシーⅡオペレーショナル・リスクという枠組みの中で、このリスク、正確な認識および評価についての十分なレベルの理解を保証することである[67]。

105. フランス。サイバー・リスクの進行が与えるセキュリティへの影響を考慮に入れ、ACPR は、市場実務の知識を向上および企業における適切なリスク管理を発達させるために調査および分析を増やした。この観点から、ACPR は最近、保険会社のサイバー・セキュリティの習熟度の発達レベルを正確に理解するため、保険セクターにおいて特定の訪問および面接を実施した。ACPR は、リスク管理の解決策を提供する革新的な企業にも面会した。ACPR は、サイバー脅威に対する全体的な感度およびシステムの耐性を評価するため保険会社のフロントオフィスからバックオフィスシステムまで侵入テスト（ブラックボックスおよびホワイトボックステスト）を実施する。ACPR は、IT オペレーショナル・リスク管理においてサイバー・リスクが正確に理解することも保証する。

---

66 ソルベンシーⅡ規制　第 44 条

67 ソルベンシーⅡ規制　第 13 条 33 項

106. ドイツ。IT 要件に関するドイツ連邦金融監督庁の回報は、特定の情報ネットワーク、相互依存性およびインターフェースの構成についての現状の見通しを有することを保険会社に義務づける。保険会社は、内部要件、営業活動およびリスク状況について特に焦点を当てるべきである。

107. 変更された条件に対する一般的なレビューおよび調整は、リスクに基づくアプローチをもとに要求される。（ビジネス手続き、専門職務、組織構成）組織およびオペレーション構成に対する変更ならびに保険会社の IT システムは、外部の構成条件（例：法規条項、規制条件）、脅威シナリオおよびセキュリティ技術が変更されなければならないように、この手続きにおいて考慮に入れられなければならない。

108. カナダのケベック州。AMF の統合リスク管理ガイダンスの目標の一つは、それぞれの保険会社の中にある重要なリスクを認識、評価、定量化、管理、軽減、および注意してモニターするための適切な管理枠組みを実施することである。AMF は、金融機関は、リスクが個別に考えられるアプローチを取り入れるよりむしろ、統合されたリスク管理に向かって引き寄せるべきであると考える。さらに、AMF は、金融機関に内在する全ての情報およびコミュニケーションに関連するリスクの管理に対し、相互関係性および相互依存性の狭間にあるリスクを考慮に入れる総合的なアプローチを推し進める。結果として金融機関は、リスクとの繋がりを認識することができる標準化手続きおよび信頼のおける情報システムを必要とする。

109. AMF のオペレーショナル・リスク管理ガイダンスでは、AMF は、オペレーショナル・リスクを認識または確認するための特定のツールを奨励しない。しかしながら、選択されたツールおよびツール一式は、包括的なオペレーショナル・リスク・エクスポージャーの評価を達成するために、全てのビジネスセクターを通して継続的に使用されるべきである。同ガイダンスでは、AMF は、金融機関ビジネスおよび技術の変化において調整可能であるべき内部統制メカニズムが、人、手続き、システムまたは外部事象に本来備わっている金融機関のオペレーショナル・リスク・エクスポージャーを実効的に軽減することを期待する。加えて、AMF は、オペレーショナル・リスクを移転させるために保険を扱う金融機関はこのようなリスクに対し常に管理メカニズムを補完することを保証すべきであると記す。

110. またビジネス継続管理ガイダンスでは、AMF は、金融機関が重要なビジネス継続機能、単一のサイトでの集中、相互依存性および一つのサイト、従業員またはサービス提供者への依存を認識することを期待する。AMF は、金融機関がその資産、オペレ

ーションおよび環境による主たる事象の影響を確認ならびにこの評価に照らして取られる措置を決定することも期待する。

111. サイバー・リスクは、AMF によって検証されている技術が関与する多くのオペレーショナル・リスクの中の一つであると考えられる。この監督者の取り組みの中で AMF は、サイバー・セキュリティに対する姿勢を評価付け、残余のリスクレベルが会社の所定リスク選好度レベルの中に存在するか判断し、リスクを最小限に抑えるための特定の行動を計画するために、保険会社がリスクの自己評価および管理を行うよう提言する。この文脈では、AMF は保険会社に対し自己評価ツールを利用できるようにする。それは、機関によって（外部で使用されているものを含めて）使用されている全ての IT アセットの一覧表が作成されていることを保証するために、多数のサイバー事象の予防および発見手続きを特に含む。機関が全てのコミュニケーションネットワークを位置付け、本質的なサービスを維持するために要求される重要な機能、データ、相互依存性および必要性を認識することを保証する。自己評価ツールは、公表された情報および機密度の分類に基づく制度および実効的なセキュリティ措置の実施のために、重要度およびビジネスの価値に基づく全ての資産の優先順位づけについて提言する。

112. カナダ。金融監督庁（OSFI）は、多くの機関は現時点におけるサイバー・セキュリティの準備段階を評価すると認識する。OSFI は、連邦規制金融機関（FRFI）は、そのような自己評価活動に関連するガイダンスから恩恵を受けることができ、したがって、FRFI は自己評価活動を支援するテンプレートを提供した[68]。

113. FRFI は、現時点での準備段階を評価し、実効的なサイバー・セキュリティ実務の発達および維持させるために、このテンプレートまたは類似した評価ツールを使用するように促されている。

114. OSFI は、機関にテンプレートを完成するよう要望する場合があり、もし完成しない場合には監督者評価と関連してサイバー・セキュリティ実務に重点を置く。

115. さらに FRFI は、目標が全社ベースでのサイバー・セキュリティについて言及、考慮および評価するための十分な管轄区域を提供するよりむしろ評価の中でサイバー・セキュリティ実務の現状を反映させるよう促されている。

---

68 「OSFI サイバー・セキュリティ自己評価ガイダンス」（2013 年 10 月 28 日）以下で入手可能。http://www.osfi-bsif.gc.ca/Eng/fi-if/in-ai/Pages/cbrsk.aspx

116.加えて、自己評価ツールは、サイバー・リスクが機関においてリスク管理手続きの不可欠な部分であるとみなすよう提言する[69]。

117.英国。FCA は、そのようなシステムおよび管理がビジネスに適切であることと同様に、発行および維持するための十分な注意を払うために、どのようにハンドブック内の要件を満たすかについて、保険会社のためのガイダンスを含む。システムおよび管理 13.7.7（SYSC 13.7.7）に含まれている本ガイダンスは、以下について尊重すべきであると企業に通知する。

- 機密性：登録制限と同様にシステムにファイヤーウォールを要求する場合のあるような、適当な権限を有する人またはシステムにのみ利用可能であるべきであること
- 完全性：情報および手続きの正確性および完全性を保護すること
- 有用性および認証：要求および独自性が立証された際に、適切に権限が与えられた人またはシステムが情報を利用できることを保証すること
- 否認防止および説明責任：情報を処理した人またはシステムが行った動作を否定できないことを保証すること

118.これらの規則および関連したガイダンスに対するレビューは、会社のプロフィールおよび規模を考慮するようなリスクに基づいたアプローチならびに重要なサイバー攻撃の場合には、イギリスの顧客および市場に及ぼす場合がある関連する潜在的な被害に実行される。

119.米国。NAIC の『保険データ・セキュリティ・モデル法」のセクション 4C は、保険会社に進行中のリスク評価および保険会社の進行中のリスク評価に基づくリスク管理のためのセクション 4D リスト要件を実行することを要求する。保険会社が考慮すべきセキュリティの手段の例は、セクション 4D(2)に記され、以下を含む。非公開情報のアクセスを制限するために、権限を与えられた個人にのみアクセスを認証および承諾する統制の使用；情報の外部ネットワークへの移動から保護するための暗号化またはその他の適切な手段の使用；および持ち運び可能な保存デバイスへの情報の保存。

---

69 AMF の「統合リスク管理指針（2015 年 5 月）」以下で入手可能。https://lautorite.qc.ca/en/professionals/insurers/guidelines/; AMF, ビジネス継続管理指針（2010 年 4 月）以下で入手可能。https://lautorite.qc.ca/en/professionals/insurers/guidelines/; 運営リスク管理指針（2016 年 12 月）以下で入手可能。https://lautorite.qc.ca/en/professionals/insurers/guidelines/

120.加えてセクション 4F は、保険会社が、第三者のサービス提供者の選択に際しデュー・デリジェンスを行い、第三者のサービス提供者に管理上の、技術的および物理的サイバー・セキュリティ措置の実施を求める。

121.審査員のハンドブックには、企業がどのように法人のサイバー・リスクを全体として全社的リスク管理（ERM）プログラムに統合させるかを考慮するための具体的な手順が含まれる。さらに、審査員が特定のリスク・エクスポージャー（例えば、第三者によるネットワークへのアクセス）を認識するにつれて、審査員ハンドブックは、審査員がテストの適切な実施を促進させるために様々なリスクに関する記述を含む。幅広い財務審査の一部として、審査員は、企業のサイバー・セキュリティ・リスク管理の ERM プログラムへの統合も考慮に入れる。そのハンドブックはまた、審査員がサイバー・セキュリティ・エクスポージャーに関する保険会社の評価を精査する必要性を強調するための文言も含む。

122.NYDFS *『金融サービス会社に関するサイバー・セキュリティ要件』* のセクション 500.02 は、保険会社のサイバー・セキュリティのプログラムがそのリスク評価に基づくことを要求する。同様に、セクション 500.03 は、保険会社のサイバー・セキュリティ方針がリスク評価に基づくことを要求する。その規制は、以下を含めた多数のセキュリティ措置の承認を保険会社に要求する：アクセス権の制限（セクション 500.07）；マルチファクタ認証の使用（セクション 500.12）および非公開情報の暗号化（セクション 500.15）。加えて、セクション 500.11 は、保険会社に、文書化された方針および手順を「第三者のサービス提供者が利用可能な、または第三者によって保持されている、情報システムのセキュリティおよび非公開情報を保証すること」の実施を要求する。

D. G7FE 要素 3 の結果の評価

123.G7FE の 3 番について、G7 によって提案された望ましい結果は：

124.**G7FEA 結果 1－基礎的要素（G7FE）は、整備されている。**上記のパラグラフ 72-73 にて考察されている。

125.**G7FEA 結果 3－混乱が起きることについて理解されている。**要素 3（リスクおよび管理評価）探索および保護について管理を重ねることは、重要であり、類似の有用性、完全性、または機密性の欠損を減少させる。しかしながら、習熟した法人は、不具合のない環境を保証することは不可能であると認識する。オペレーション上の妨害が生

じるという考え方が身についているため、主要な意思決定者は、戦略的に調整された投資の選択は、G7FE の全ての側面において均衡を図ると理解する。

126.このコンセプトを認識できない法人は、周辺制御に過度な信頼を置き、明らかに定義され、定期的に行われる対応（要素 5）およびオペレーション再開のための実行可能かつ試験済みの緊急時の対応計画（要素 6）を犠牲にして不均衡を示す場合がある。

3.4 G7FE－要素 4：モニタリング

127.**G-7 の基礎的要素の 4 番目は、金融機関に対し、「サイバー・インシデントを速やかに検知し、ネットワークのモニタリング、テスト、監査、演習を通じて種々の管理手段の有効性を定期的に評価する、体系的なモニタリングプロセスを構築すること」を求めている。**

128.G7FE 4 で説明されているように、「実効的なモニタリングは、既設定のリスク許容度を金融機関に遵守させるとともに、既存の管理における弱点をタイムリーに強化・修正することの手助けとなる」および「テスト・監査のプロトコルは、金融機関と当局の双方に対して、基本的な保証メカニズムを提供する。」

129.本説明はまた、「テストおよび監査の機能は、サイバー・セキュリティ・プログラムの実施および管理に責任を有する人物から適切に独立すべき」と提案する。

130.個々の企業がサイバー脅威に対抗するためにどのように備えているかということと同様に、セクター全体のサイバー脅威に関する当局の理解度は、「検査、立入りおよびその他の監督メカニズム、企業のテスト結果の比較分析、および官民の演習への参加を通じて」強化される可能性がある。

A. 保険コアプリンシプルへの G7FE 要素 4 の位置付け

131.G7FE 4 で取り上げられているサイバー関連のモニタリングは、「重大なリスクに対して、時宜にかなう検討と適正な対応を可能にする早期警戒もしくはトリガーを含むべきである」という ICP 8.1 で論じられているリスク管理システムと一致する[70]。

132.「監督者は、保険会社に対し、内部統制の実効的なシステムを確立し、またその下で事業を行うよう要求する。」という ICP 8.2 にも合致している。このようなモニタリングシステムには、「内部統制システムの適切性、完全性および実効性ならびに、保

[70] ICP8.1.8

険会社の運営を統制するにあたって、取締役会および上級管理職にとってのその有用性を判断するための、（内部または外部の監査人などの客観的な当事者により実施される）定期的なテストおよび評価」が含まれる[71]。

B. モニタリングに関する監督者への提言

133. 保険会社のサイバー・セキュリティのモニタリングに関しては、監督実務が以下をリスクベースかつプロポーショナルな方法にて奨励または反映することが適切となりうる。

継続的なモニタリング

a. 保険会社は、必要に応じて情報フローの制御、境界保護、およびネットワーク分離などのネットワーク（ハードウェア、ファームウェア、およびソフトウェアのコンポーネント）の完全性を保護すべきである。

b. 例えば、保険会社は、異常な活動および事象を発見するために、リアルタイムまたはほぼリアルタイムの継続的なモニタリング機能を確立させることを検討すべきである。これを達成するために現在使用されている 1 つのプラクティスは、一般に Security Operations Center（SOC）と呼ばれる。保険会社は SOC を確立するか、または 24 時間対応のモニタリングを提供する同様の機能を開発することを検討すべきであり、そのような機能は適応的に維持され、テストされる場合がある。（C/I 5.2.1）

c. 保険会社は、潜在的なサイバー・インシデントの兆候を認識するか、または実際の違反が発生したことを発見できるべきであり、これは強力なサイバー・セキュリティにとって不可欠である。早期発見は、潜在的な違反に対して適切な対策を講じるための有益な時間的猶予を保険会社に提供し、実際の違反を積極的に封じ込めることを可能にする。後者の場合、早期の封じ込めは、侵入者による機密データへのアクセスまたはそのようなデータの漏洩を防ぐなど、攻撃の影響を実効的に緩和することができる。（C/I 5.1）

d. サイバー・セキュリティ・インシデントの隠密かつ高度な性質と、情報漏えいが起こる可能性がある複数の侵入口を考慮して、保険会社は、異常な活動を広範にモニターする実効的な機能を維持すべきである。

---

[71] ICP8.2.4

e. 保険会社は、既知の脆弱性に対するシグネチャモニタリングおよび行動ベースの発見メカニズムの組み合わせにより、脆弱性を検出するために、内部および外部の関連する活動およびイベントをモニタリングすべきである。

f. 保険会社の発見機能は、第三者であるサービスプロバイダー、保険契約者、潜在的なインサイダーの脅威、およびその他の高度な脅威活動によるアクセスの悪用にも対処すべきである。これらのプロセスは、強力なサイバー・セキュリティ情報収集プログラムによって通知され、統合されるべきである。

g. モニタリングプロセスの一環として、保険会社は最少権限および職務分掌等の原則に基づいて、情報資産への物理的、論理的、およびリモートアクセスの ID ならびに資格情報を管理すべきである。（NIST 枠組み、セクション：PR 保護）

h. 保険会社は、妥当な法的な境界の中で、企業ネットワークへのアクセス権を有する者の異常行動を捕捉して分析する手段を導入すべきである。（C/I 5.2.5）

i. 保険会社は、迅速な封じ込めおよび回復にはこの機能が不可欠であるため、早期に侵入を発見する能力を持つべきである。保険会社は、人、プロセス、および技術をカバーする複数のレイヤーから成る発見のコントロールを導入し、各レイヤーが前のレイヤーのセーフティネットとして機能するようにすることで、徹底的な防衛策を講じるべきである。

j. さらに、侵入を発見する実効的な機能は、早期修復のための防護措置の欠陥を識別する際に保険会社を支援することができる。これらの機能には、例えば、データの損失／漏えいの予防および発見、監査ログの記録および文書化、事象データの集約、相関、分析ならびに連携のみならず、ネットワーク、人材、および外部に依存する活動のモニタリングを含むことになる。

k. 保険会社は、インシデントへの対応プロセスを容易にし、フォレンジックプロセスにおける情報収集をサポートするために、モニタリングおよび発見機能を採用すべきである。（C/I 5.2.4）

テスト

l. テストは、実効的なサイバー・セキュリティの枠組みの不可欠な要素である。健全なテスト制度は、提示されたレジリエンス目標とのギャップを特定する発見をもたらし、保険会社のサイバー・リスク管理プロセスに信頼できる有意義な情報を提供す

る。テスト結果の分析は、サイバー・セキュリティへの姿勢の弱点または欠点を修正し、特定された格差を縮小または排除する方法の方向性を提供する。このようなテストには、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（攻撃を仕掛ける側）を使用したテストが含まれる。（C/I 7.1）

m. 保険会社は、サイバー・セキュリティの枠組みの全要素を厳格にテストして、保険会社内で採用される前に、またその後も定期的に全体的な有効性を判断すべきである。そのようなテストには、枠組みが正しく導入され、意図どおりに機能し、かつ望ましい結果が得られる範囲が含まれているべきである。（C/I 7.1）

n. 保険会社は、サイバー・セキュリティの枠組みをテストし、組織内で結果を伝えるべきである。例えば、保険会社はその試験方法に知見を与えるために、適切で利用可能なサイバー・セキュリティの情報を用い、彼らのサイバー・セキュリティ枠組みの全ての要素の有効性を検証するための適切な包括的なテストプログラムを確立させることを検討すべきであり、例えば、脅威となる原因が進化する可能性をシミュレートするためのテストを設計することや、極端でも起こりうるシナリオを想定すること等がある。

o. テストプログラムの結果は、サイバー・セキュリティの継続的な改善を支援するために保険会社によって使用されるべきである（G7FE の要素 8 の議論を参照）。適用可能かつ実行可能な場合、これらのテストには、事業継続性、事件・危機対応チーム、ならびに関連する外部ステークホルダーを含む事業種目の管理など、組織内の他のステークホルダーおよび部門を含めるべきである。保険会社は、取締役会および上級管理職が適切に（例えば、危機管理チームの一員として）関与し、テスト結果を通知されるための適切な手続きを備えるべきである。（C/I 7.2.1）

p. 保険会社は、利用可能な最先端のテスト手法と実務を組み合わせて使用することを検討すべきである。現在、このような最先端のテスト方法と実務には、以下の要素が含まれる（一部重複しており、統合可能）。

- 脆弱性評価（VA）。保険会社は、脆弱性評価を定期的に実施し、システムおよびプロセスのセキュリティ上の脆弱性を特定し評価すべきである。保険会社は、VA で特定された問題の優先順位をつけ、是正するためのプロセスを確立し、ギャップが完全に適時に解決されたかどうかを評価するために、その後の検証を行うべきである。（C/I 7.2.2）

- シナリオに基づくテスト。保険会社の対応、再開、および回復の計画は、定期的なレビューとテストの対象となる。テストでは、極端ではあるが確実に起こりうるサイバー・セキュリティに関する事象のシミュレーションを含む適度に広いシナリオの範囲に対処し、ガバナンスの取り決めやコミュニケーション計画などを含む対応、再開、および回復の仮定の事象に対処するように設計すべきである。保険会社は、サイバー脅威の固有の特性を真似るためにできる限りサイバーの脅威に関する情報収集およびサイバーの脅威に関するモデリング使用すべきである。また、より強固な運用上のレジリエンスを備えるため、起こりにくいシナリオに対応するスタッフおよびプロセスの能力をテストする演習も実施すべきである。（C/I 7.2.2）

- 侵入テスト。保険会社は、システム、ネットワーク、人またはプロセスに影響を及ぼす可能性のある脆弱性を特定するために、侵入テストを実施すべきである。保険会社のシステムのセキュリティの詳細な評価を提供するには、これらのテストでシステムに対する実際の攻撃をシミュレーションすべきである。インターネットに面するシステムの侵入テストは、定期的に、および更新されたシステムが展開される前に実施されるべきである。適用可能かつ実行可能な場合、テストには、事業継続に関与する人、事件・危機対応チーム、サービスプロバイダーなどの第三者といった、幅広い事業上のステークホルダーが含まれうる。（C/I 7.2.2）

- レッドチームテスト。保険会社は、制御された状況で敵対的な視点を導入するために、いわゆるレッドチームを使用することによって、自組織および外部委託者に対して攻撃することを検討すべきである。レッドチームは、脆弱性の可能性を検証し、保険会社のコントロールを軽減する有効性のテストを行うのに役立つ。レッドチームは、保険会社自身の従業員および/または外部の専門家で構成される可能性があるが、どちらの場合もテスト対象の部門から独立している。（C/I 7.2.2）

q. 保険会社は、実用的／可能な限り、その対応、再開、回復の計画およびプロセスをテストするために設計された演習を促進、設計、整理、管理すべきである。このような演習には、保険会社ならびに重要なサービスプロバイダー、および関係する保険会社（保険グループ内の関連会社など）が含まれるべきである。適切な場合には、保険会社は関係当局が主催する演習および業界全体のテストに参加すべきである。（C/I 7.3.1）

r. 保険会社および監督者は、伝統的かつ独立したテストでは、他の全てのプレーヤーが通常どおり動作することを暗示的に前提としていることに注意すべきであるが、これは非現実的な制限である。この仮説を取り除くことで、保険会社は回復計画で見過ごされていた可能性のある起こりうる複雑性、依存性、弱点を特定することができる。したがって、テストには、外部委託に影響する侵害をカバーするシナリオを含めるべきである。（C/I 7.3.1）

C. 現行の実務の例

134. 欧州連合。ソルベンシーII では、監督当局は第三者またはプロバイダーを直接監査することができる[72]。

135. フランス。ACPR は、保険会社が、情報システムのセキュリティネットワークを監督する SOC（セキュリティオペレーションセンター）などのセキュリティのモニタリングに専念する組織を、会社の規模に相応しく、それに見合うと判断された場合に展開することを奨励する。

136. ドイツ。BaFin の IT 要件に関する公開された回報では、標準的な運用からの予想外の逸脱（過失）とその原因が適切に収集、評価され、優先順位付けがされなければならず、特に結果として生じうるリスクについては、設定された規準に従うよう求めている。またフォローアップを含む処理、因果関係分析および解決策を文書化しなければならない。過失とその原因との間の考えられる相関分析のための整理されたプロセスがなければならない。評価と優先順位付けの適切性を含む、過失に関する公開報告書の処理状況はモニターされ、管理されなければならない。保険会社は、過失について取締役会に対し通知する適切な規準を設定しなければならない。

137. オランダ。DNB は、保険会社を含むオランダの金融コア・ペイメント・インフラストラクチャーを構成する機関と協力して、レッドチームテストを含む包括的な枠組みにより、高度なサイバー攻撃に対するセクターの保護をさらに改善するためのプログラムを開発した。

138. この枠組みは「脅威の情報収集に基づく倫理的レッドチーミング」（TIBER）として知られている[73]。 TIBER は、2014 年にイングランド銀行によって開始された CBEST 枠組みから学び、高度なサイバー脅威の変化する性質に適応させるためにさ

---

72 ソルベンシーⅡ規制の（37）

73 DNB の「TIBER-NL ガイドライン - TIBER-NL 試験の実施方法」（2017 年 11 月）、https://www.dnb.nl/en/news/news-and-archive/nieuws-2017/dnb365801.jsp .

らに開発された[74]。その目的は、お互いのベストプラクティスから学ぶことによって、国の中核的金融機関のサイバー攻撃耐性を強化することである。

139.TIBER テストは、実際の脅威をもたらす当事者からの潜在的なサイバー攻撃を模倣する。このテストは、高レベルの脅威集団（組織犯罪グループ／州の代理人/国家による攻撃者）だけに似ており、それによって講じられた防衛策が実効的かどうか（能力評価）をテストするが、例えば監査者および監視者による、現在の定期的な情報セキュリティの監査を補完する。このテストはまた、金融機関が実施する現在の侵入テストおよび脆弱性の精査を補完するものである。

140.オランダの保険会社は、この枠組みを使用するよう奨励されている。

141.カナダのケベック州。AMF は、事業継続管理のガイドラインにおいて、金融機関がその重要な機能を混乱させるか、遅らせるか、中断する可能性がある主要な業務上のインシデントを特定するよう期待している。

142.また、オペレーショナル・リスクマネジメントガイドラインでは、AMF は、金融機関のリスク許容度を反映したオペレーショナル・リスク報告書の作成を想定している。また、これらの報告書は、リスク・エクスポージャーの変化、そのようなリスクを管理するために整備された対策の実効性と効率性を金融機関が追跡できるようにすべきである。

143.より正確には、報告された最も重大なインシデントの分析は、取締役会および上級管理職が、軽減されていないオペレーショナル・リスクの主な原因を特定することを可能にすべきである。そのような報告書には、AMF と監査部門の両方による勧告を組み込むべきである。

144. AMF は、監督活動の一環として、認識されたサイバー関連の国際基準およびプロセス（NIST および COBIT 組織によって発行されたものなど）に基づいて詳細な自己評価ツールを開発した。このツールは、リスク・プロファイルに基づいて多くの金融機関のサイバー・セキュリティの姿勢を評価するために使用される。必要に応じて、このツールは AMF が監視する金融機関にも利用できるようになっている。とりわけ、潜在的なサイバー・セキュリティに関する事象を発見するために、ネットワークのインフラと人員、および外部のサービスプロバイダーの活動を監視することを推奨

74 イングランド銀行の「金融セクターの継続性」 https://www.bankofengland.co.uk/financialstability/financial-sector-continuity

している。攻撃ターゲットと方法を理解するため、全てのリモートアクセスの監視、発信トラフィックのモニタリングのための技術ツールの使用、およびさまざまな発生源による異常な活動とイベントの集約、相関および分析を推奨している[75]。

145. 英国。FCA は、セクターのサイバー攻撃耐性のアプローチを見直し、承認するための多層的なアプローチを運用している。これには、サイバー攻撃へのレジリエンスに対する企業の基礎的な能力を評価しようとする自己評価サイバーアンケートの発行と、重大な欠陥が発見されたリスク軽減計画の実施が含まれる。

146. FCA はまた、CBEST 設計グループの主要メンバーであり、イングランド銀行との枠組みを共同で導入している。CBEST は、制御された、特注の情報収集主導のサイバー・セキュリティテストを提供するための枠組みである。このテストでは、政府機関および商業情報機関が評価した脅威行為者の行動を、システム上重要な金融機関にとっての本物の脅威とみなして再現している。 FCA は、CBEST の範囲を広げて、より広い消費者の損害がこれらのテストの範囲の重要な考慮事項になるように、テストがシステム上重要と考えられる企業よりも広い範囲の企業に展開できるようにした。

147. FCA はまた、犯罪者にも見える脆弱性および弱点を発見するために、規制対象企業の公開されたインターフェースを受動的かつ静的に精査するための第三者のリスク評価ツールを運用している。これらの脆弱性の発見により、規制対象企業との協議が行われ、そのような問題の重大性が評価され、リスク修復計画が通知される。

148. 米国。NAIC 保険データ・セキュリティ・モデル法のセクション 4D は、「情報システムへの実際の攻撃または侵入の試み、侵入、その他のシステム障害を検出する」ために、潜在的なセキュリティ手段の中にネットワークモニタリングを含めるよう指示している。

149. さらに、セクション 4I は、保険会社が法律の情報セキュリティ・プログラム要件を遵守していることを証明する年次の供述書を監督官に提出することを保険会社に要求する。

150. さらに、セクション 7 では、州法の下ですでに規定されている権限に基づき、法律の遵守を保証するために保険会社を調査および捜査する権限を監督官に与える。

---

[75] AMF の「オペレーション・リスク・マネジメント・ガイドライン」(2016 年 12 月)、https://lautorite.qc.ca/en/professionals/insurers/guidelines/.

151.「審査官ハンドブック」には、現存する可能性のあるコントロールと実行すべきテストに関して、ネットワーク監視を見直し検討するための具体的な手順が含まれている。ハンドブックのガイダンスは、第三者の監査の見直しについての洞察も提供するが、それは行われた洞察をテスト手続きおよび実行されたフォローアップを統合するためである。

152.NYDFS の*『金融サービス会社に関するサイバー・セキュリティ要件』*のセクション 500.05 は、保険会社が、リスク評価に従って開発されたモニタリングおよびテストを実施して、年 1 回の侵入テストおよび 2 年ごとの脆弱性評価（年 1 回の侵入テストおよび 2 年ごとの脆弱性評価の要件は、継続的なモニタリングがされている場合は、適用されない）を含む、保険会社のサイバー・セキュリティの有効性を評価するよう要求する。 セクション 500.17 は、保険会社に対し、取締役会または上級役員により、監督当局に対して規制への遵守を証明するよう要求している。

D. G7FE－要素 4 の結果の評価

153.G7FE の番目 4 については、G7 提案の望ましい結果は次のとおりである。

154.**G7FEA 結果 1-基礎的要素（G7FE）が整備されている。**上記パラグラフ 72-73 で議論。

155.**G7FEA 結果 4 - 適応型サイバー・セキュリティアプローチが採択されている。**サイバー脅威および脆弱性は、引き続き出現し、進化し続けている。これに対応して、企業は自社のサイバー・セキュリティ手順が事業運営において常に変化する状況を反映するよう確保するために、順応でき、かつ、静的な「要塞」という考え方を避ける必要がある。

156.要素 5（対応）と要素 6（回復）を基にして、インシデント対応の仕組みは、企業、セクター、セクター間、国際的なレベルのいずれにおいても、経済機能が混乱またはストレスの中でも引き続き機能するように、十分にリハーサルする必要がある。混乱は予想外の方法で金融セクターに影響を与える可能性があるため、柔軟性は事後対応（reactive）において鍵となる。要素 4（モニタリング）と組み合わせて、結果に大きな影響を及ぼす混乱を迅速に特定して抑制するのが敏捷性および経験である。これに関連して、全体的な焦点は、サイバー・セキュリティ・プログラムの一環として継続的な改善と学習の環境を育むことに置かれるべきである。

3.5 G7FE－要素 5：対応

157.**G7FE の 5 番目では、金融機関が「インシデント発生時に、タイムリーに(a)サイバー・インシデントの特性、範囲、影響を評価し、(b)インシデントを封じ込め、その影響を軽減し、(c)内外の関係者（司法当局、規制当局、その他の当局に加え、必要に応じ、株主、外部委託先サービスプロバイダー、顧客）へ通知し、(d)必要に応じて、共同でインシデント対応を図るよう求めている。**

158.5 番目の G7FE は、実効的なインシデント対応を容易にするために、インシデント対応方針およびその他の統制を整備するよう企業に求め、また、「特に、これらの統制はとりわけ、意思決定の責任の所在を明確にし、エスカレーションの手順を定め、内外の関係者とのコミュニケーションプロセスを構築すべきである。」と述べている。

A. 保険コアプリンシプルへの G7FE 要素 5 の位置付け

159.G7FE 5 は、実効的なリスク管理システムのための適切なプロセスおよびツールの一部として、危機管理計画を提案する ICP 8.1.2 と一致している。そのような危機管理計画には、サイバー・インシデント後の対応および回復プロセスが含まれる。

B. 対応に関する監督者への提言

160.保険会社のサイバー・セキュリティへの対応に関して、監督実務が以下をリスクベースかつプロポーショナルな方法にて奨励または反映することが適切となりうる：

a. サイバー・セキュリティ・インシデントに先立って、保険会社は、従業員および他の人々がシステムにアクセスできるように研修を提供することで、全てのステークホルダーの意識を高めるべきである。調整された研修は、重要または繊細なデータもしくは強化されたシステム権限を利用しうる従業員にとって適切となる場合がある。また、保険会社は、サイバー・インシデントに関する対応計画（インシデントへの対応および事業継続性）および連携に関する計画も策定すべきである。これらの計画は、適宜、見直しおよび改善の対象となるべきである。

b. サイバー・セキュリティ・インシデント（または未遂）が発見された際に、保険会社は、その性質および程度ならびに生じた損害を判断するために徹底的な捜査を行うべきある。捜査が進行中の間、保険会社は、さらなる損害を防ぎ状況を抑えるために即座に行動し、対応計画に基づいて事業を回復させるための努力を開始すべきである。（C/I 6.2.1）

c. 保険会社はまた、システムをあまりにも早くバックアップしないように認識すべきであり、また別の攻撃、またはサイバー・セキュリティ・インシデント拡大の危険にさらすことのないよう注意すべきである。

d. 保険会社は、サイバー・セキュリティ・インシデントの後に安全にできるだけ早く重大な業務を再開することを計画すべきであるが、復旧の努力が継続している間は、重要な機能、取引および相互依存を分析して再開および回復活動の優先順位を決めるべきである。保険会社は、自動化されたシステムが利用できない場合には、実行可能かつ実用的であれば、人的な作業に復帰するなど、重大な人、プロセス、またはシステムがかなりの期間利用できない状況についても計画すべきである。（C/I 6.2.3）

e. 保険会社は、大規模または業界全体の事象が、そのような重要なリソースの利用可能性をすぐさま減少させる可能性があることを認識して、外部の専門家にアクセスする計画を立てるべきである。

f. 保険会社は、対応、再開、および回復計画を策定し、テストすべきである。これらの計画は、保険契約者のデータを含む資産の機密性、完全性、および資産の利用可能性を保護する目的をサポートすべきである。現在のサイバー脅威の情報収集、情報共有、以前の事象から学んだ教訓、ならびにまだ発生していない運営上および技術上起こりうるシナリオの分析に基づいて計画を積極的に更新すべきである。保険会社は、対応、再開、および回復計画の策定中に、監督当局およびその他の関係当局を含む、社内外の関連するステークホルダーと協議し調整すべきである。（C/I 6.2.4）

g. 重要な機能および運用のためのシステムとプロセスの設計ならびに制御は、インシデント対応活動を可能な限り支援すべきである。保険会社は、サイバー・インシデントの影響を制限し、契約者データのプライバシーを保護するためのシステムおよびプロセスを設計すべきである。保険会社のインシデント対応、再開、および回復のプロセスは、危機管理、事業継続、および災害回復の計画、回復作業に緊密に統合され、内外の関連するステークホルダーと調整されるべきである。（C/I 6.3.1）

h. 保険会社は、適切な準備とメッセージの一貫性を確保するために、保険契約者、ビジネスパートナー、および適切な当局を含む全てのステークホルダーとの連携のための特定のチームを設置することを検討すべきである。

i. 保険会社は、全体的なガバナンスの枠組みの一部として、および関連する法律に準拠して、リスクベースのアプローチに従って潜在的な脆弱性の責任ある開示を可能にす

る方針および手順を有すべきである。特に、保険会社は、サイバー・エコシステムとより広範な金融安定のために、ステークホルダーによる早期の対応およびリスク軽減を容易にする開示を優先すべきである。

j. 保険契約者のデータが公開される事象があった場合、保険会社は関連する全ての管轄区域の法令に定められた開示義務を満たすための方針および手続きを有すべきである。

k. 保険会社は、サイバー・インシデントのフォレンジック科学捜査を支援する、または実行する能力を有し、また、捜査プロセスを促進するための保護および発見のコントロールを持つべきである。これに関して、保険会社は、維持されるべきログのタイプおよびその保持期間を含む、関連するシステムログ記録方針を設定すべきである。フォレンジック分析は延期する必要があるかもしれず、ICT リソースは重大なシステムの回復に重点を置くことがあるものの、保険会社は、必要なシステムログおよび証拠の保存など、可能な範囲で事象後の調査を引続き実施できるよう確保すべきである。（C/I 6.4.5）

C. 現行の実務の例

161. フランス。その監督を行うために、ACPR は、インシデント、事業継続計画、および IT 管理などのさまざまなツールを活用している[76]。ソルベンシーII の枠組み[77]は、保険会社に BCP（事業継続計画）を備えるよう義務づけている。明確に指定されていない場合でも、ACPR は、これらの計画を構築するために用いられたシナリオに、サイバー脅威およびその他の情報セキュリティシナリオが含まれていることを確認する。

162. ドイツ。ドイツの法律により、BaFin は、保険会社に対して、特に危機管理計画に関する情報を提供するよう要求している。監督実務の一環として、BaFin は保険会社の危機管理計画を評価し、必要な修正を要求する場合がある。危機管理テストが保険会社によって行われている限り、BaFin は保険会社の監督者として、保険会社の前提でテストの実施に立ち会うことができる。

163. カナダのケベック州。2018 年 4 月、カナダ政府は、2018 年 11 月 1 日付けで発効する議会指令、個人情報保護および電子文書法（PIPEDA）に基づく強制的な違反通知

76 第 228 条 1 項『委任された行為および第 40 条のならびにソルベンシーⅡ規制の以下が主な強固な法的根拠を代表する.』

77 第 258 条 3 項

および記録の保管要件を公表した。一旦導入されると、これらの変更は、カナダの違反報告制度を米国と欧州連合の報告制度とより密接に整合させることになる。

164. PIPEDA の新しい規定の下で、データ侵害または「安全保護措置違反」とは、組織の安全保護措置に違反したことによる個人情報の紛失または不正なアクセスもしくは情報開示と定義される。 データ侵害を経験した組織は、カナダのプライバシー委員会（OPC）の事務所にその事件を報告し、違反が「個人に重大な損害を及ぼす本当のリスク」をもたらすと合理的に考えられる場合には、被害を受けた個人に通知しなければならない。 「重大な損害」には、とりわけ、身体的危害、屈辱、評判や関係に対する損害、金銭的損失、なりすまし、信用記録への悪影響、財産への損害または損失が含まれる。

165. ガバナンスおよびオペレーショナル・リスク管理ガイドラインで推奨されているように、AMF は、保険会社が主要な業務上のインシデント（サイバー・インシデント、システム障害等）により深刻な損害を負う可能性が高い内外のステークホルダーに速やかに通知するための必要なメカニズムを実施することにより、 開示および透明性の期待に応えることを確信する。このようなアプローチにより、AMF はステークホルダーとして、オペレーショナル・リスク管理を損なう可能性のある実務を事前に特定することが可能になる。また、AMF は、内部統制メカニズムが、重要性に応じて、人、プロセス、システム、または外部事象に内在する金融機関のオペレーショナル・リスクのエクスポージャーを効率的に軽減することを期待する。

166. さらに、AMF は現在、自身が監督する保険会社から受け取った通知の処理を標準化するための正式な通知チャネルおよびプロセスを開発中である[78]。

167. 英国。FCA は、サイバー事象への実効的な対応を可能にするための数多くの取組をサポートしている。英国の金融サービス・インシデントへの対応ガイドは、英国の金融当局および規制対象の企業のグループと共同で作成され、英国のサイバー情報共有のためのパートナーシップ（CiSP）に関して共有され、影響を受ける企業がどのように必須の報告要件を満たすべきか、および対応の支援が得られる場合について詳細に記載している。

[78] AMF の「ガバナンス・ガイドライン」（2016 年 9 月）https://lautorite.qc.ca/en/professionals/insurers/guidelines/ ；AMF の「オペレーション・リスク・マネジメント・ガイドライン」（2016 年 12 月）、https://lautorite.qc.ca/en/professionals/insurers/guidelines/

168.FCA はまた、イングランド銀行、英国財務省、国家サイバー・セキュリティセンター、国家犯罪対策庁と共に当局の対応フレームワーク（ARF）の一員でもある。ARF は、集団当局が重大なインシデントに緊密かつ協調的に対応し、全ての当事者が全ての参加者によって行われている対応活動を認識できるようにする調整と対応の仕組みを提供する。

169.FCA は、規制対象の企業の対応を定期的にレビューし、リスクに基づくアプローチを用いてこれらのレビューを実行し、損害の最も大きなリスクをもたらす企業に焦点を当てる。

170.米国。NAIC 保険データ・セキュリティ・モデル法のセクション 4H では、保険会社が定義づけられたサイバー・セキュリティ事象にどのように対応し回復するかを示す文書化された事象への対応計画を作成するよう保険会社に求めている。この計画には、定義づけられたサイバー・セキュリティ事象の発生時に必要な連携、情報システムと関連するコントロールの脆弱性の改善方法、明確な役割の定義、責任、および意思決定を行う当局のレベルに関する情報が含まれていなければならない。セクション 6 では、保険会社は、監督官（すなわち、州の保険監督者）、影響を受ける消費者、およびその他特定のステークホルダーへの通知が求められる。

171.審査官ハンドブックは、一般的に、サービスの中断をもたらす可能性のある事件に会社がどのように対応しているか（例えば、事故対応計画の見直し）をレビューし、また、重要なビジネス機能の継続性をどのように確保するか（例えば、システム回復機能のレビュー）を含む、数多くの手続きを通じてそれらの要素に対応する。

172.NYDFS の*『金融サービス会社に関するサイバー・セキュリティ要件』*のセクション 500.16 では、サイバー・セキュリティ事象に速やかに対応し、そこから回復するように設計された事象への対応計画を策定するよう保険会社に求めている。この計画には、事件の発生時に必要な連携、脆弱性の改善方法、明確な役割の定義、責任、および意思決定を行う当局のレベルに関する情報が含まれていなければならない。セクション 500.17 では、保険会社がサイバー・セキュリティ事象を監督者（すなわち、ニューヨーク州保険監督官）に報告することを要求している。

D. G7FE－要素 5 の結果の評価

173.G7FE の 5 番目については、G7 が提案する望ましい結果は以下のとおりである。

174.**G7FEA 結果 1-基礎的要素（G7FE）が整備されている。**上記パラグラフ 72-73 で議論。

175.**G7FEA 結果 3 –混乱が発生するとの理解がある。**上記パラグラフ 125-126 で議論。

176.**G7FEA 結果 4 - 適応型サイバー・セキュリティアプローチが採択されている。**上記パラグラフ 155-156 で議論。

3.6 G7FE－要素 6：回復

177.**第 6 の G7FE は、金融機関に対し、脆弱性等の改善作業を継続しつつ、速やかに業務を再開するため (a)インシデントによる有害な痕跡を除去すること、(b)システムおよびやデータを正常に復旧し、平常状態を確保すること、(c)悪用された脆弱性をすべて特定し、軽減すること(d)同様のインシデントから防御するため、脆弱性を改善すること(e)内外との適切なコミュニケーションを確保することを含め要求する。**

178.サイバー・インシデントによって中断された事業運営の回復は、「一旦事業運営の安定性と完全性が保証された時点」で行われるべきである。G7FE 6 は、「重要な機能、プロセス、および活動」が影響を受けた場合、回復は、「関連する公的当局により定められた目的に従って」行われるべきであり、また、「企業と公的当局が再開と復興の際に相互に援助する能力を持っている場合、金融セクターへの信頼と信用が大幅に向上する」と記載されている。

A. 保険コアプリンシプルへの G7FE 要素 6 の位置付け

179.前のセクションで述べたように、このことは、実効的なリスク管理システムのための適切なプロセスとツールの一部としての危機管理計画を提案する ICP 8.1.2 と一致している。そのような危機管理計画には、サイバー・インシデント後の対応および回復プロセスが含まれうる。

B. 回復に関する監督者への提言

180.サイバー・セキュリティの回復に関しては、監督実務が以下をリスクベースかつプロポーショナルな方法にて奨励または反映することが適切かもしれない。

a. 保険会社は、サイバー・セキュリティ・インシデントから回復するための計画および手続きを備えておくべきである。

b. サイバー・インシデントからの回復の取り決めは、保険契約者および事業運営者への混乱を最小限に抑えながら、保険会社が安全に業務を再開できるように設計されるべきである。

c. 保険会社は、違反の後に適時かつ正確なデータ回収を可能にするために、システムとプロセスを設計し、テストすべきである。一例として、保険会社のシステムおよびプロセスは、影響を受けるシステムおよびデータの回復に使用される重要なデータ（可能な限りアプリケーションソースコードを含む）の破損していない「ゴールデンコピー」を維持するように設計可能である。保有された情報の重要度および分類を考慮に入れると、データは、厳重な保護的および発見的コントロールによって保護されるべきである。さらに、保険会社のサイバー・セキュリティ枠組みには、そのようなデータが破損した場合に全ての保険契約者データのバックアップコピーを保持するなどのデータ回復手段が含まれているべきである。（C/I 6.3.2）

d. 保険会社の回復計画（インシデントからの回復および災害回復）は、必要に応じてレビューと改善の対象となる。

e. 保険会社のシステムおよびプロセスは、しばしば第三者のシステムおよびプロセスと相互に接続されているため、サイバー・インシデントが大規模に発生した場合、保険会社は感染リスク（すなわち、マルウェアまたはデータ破損の拡大）第三者のサービスプロバイダーまたは他の相互接続されたシステムからの感染リスクにさらされる可能性がある。保険会社は、これらの第三者と協力して、安全な方法で業務を再開すべきである。（C/I 6.4.2）

f. 保険会社は、主要なサイバー・セキュリティ・インシデントのために損害を被る可能性の高い保険契約者、内外のステークホルダー（法執行機関、規制者、およびその他の公的当局、ならびに株主および、適切であれば第三者のサービス提供者など）との連携を図る正式な計画を有すべきである。準拠法に従った連携計画は、シナリオベースの計画および分析だけでなく、事前の経験によって知見を得た適応プロセスを通じて開発されるべきである。サイバー・セキュリティ・インシデントの急速な拡大が必然となりうるため、保険会社は事前にインシデント対応および回復に関する意思決定責任を決定し、また、明確に定義された上程および意思決定手順を具備すべきである。

C. 現行の実務の例

181. フランス。サイバー攻撃または災害からの回復は、事業継続計画またはリスクとソルベンシーの自己評価（ORSA）によってカバーされることがある。

182. ドイツ。BaFin の IT 要件に関する回報では、情報セキュリティインシデントの後、情報セキュリティへの影響を分析し、適切なフォローアップ対策を準備しなければならないと求めている。

183. カナダのケベック州。AMF の事業継続管理ガイドラインでは、バーゼル銀行監督委員会、保険監督者国際機構、ジョイントフォーラムが、健全なオペレーショナル・リスク管理の実務および健全な事業継続管理の実務について公表した基本原則一式を提案している。この点を念頭に置いて、各保険会社は、主要な業務上のインシデントを処理するために最適に準備していることを確保するための、慎重に開発されたビジネス継続計画を採用することが期待されている。

184. さらに、保険会社が利用できる AMF 自己評価ツールは、全ての重要なサービスへの対応および継続計画が特にサイバー・インシデントを考慮することを推奨する。このツールは、発見された新しい脆弱性への機関のエクスポージャーを軽減するために、サイバー・インシデントと脆弱な場所を迅速に分離するための戦略とプロセスを備えることをさらに規定している。また、保険会社は、事前に定めた頻度に従って、サイバー攻撃シミュレーション演習を使用した対応および回復計画の有効性を検証すべきである[79]。

185. 英国。FCA は、企業がサイバー・インシデントの後でサービスの回復および再開を計画することを期待する。これには、必要な連携および、そのような連携の適時性および重要性を詳述するステークホルダー・マップが含まれる。 FCA は、公衆通信を要求し、レビューすることができる。英国の上場監督機関はまた、上場企業に対して主要なサイバー攻撃の後に公衆開示を行うよう要求することができる。

186. 米国。NAIC の保険データ・セキュリティ・モデル法のセクション 4H では、上記の「対応」要素に記載されているように、保険会社が定義づけられたサイバー・セキュリティ事象にどのように対応し回復するかを示す文書化されたインシデント対応計画を作成するよう保険会社に求めている。この計画には、サイバー・セキュリティ事象の発生時に必要な連携、脆弱性の改善方法、明確な役割の定義、責任、および意思決定を行う当局のレベルに関する情報が含まれていなければならない。セクション 6 で

[79] AMF の「ビジネス継続性マネジメント・ガイドライン」（2010 年 4 月）、https://lautorite.qc.ca/en/professionals/insurers/guidelines/にて入手可能

は、保険会社は、監督官（すなわち、州の保険監督者）、影響を受ける消費者、およびその他特定のステークホルダーへの通知が求められる。

187.同様に、NYDFS の*『金融サービス会社に関するサイバー・セキュリティ要件』*のセクション 500.16 では、サイバー・セキュリティ事象に速やかに対応し、そこから回復するように設計されたインシデント対応計画を策定するよう保険会社に求めている。この計画には、事件の発生時に必要な連携、脆弱性の改善方法、明確な役割の定義、責任、および意思決定を行う当局のレベルに関する情報が含まれていなければならない。セクション 500.17 は、保険会社がサイバー・セキュリティ事象を監督者（すなわち、ニューヨーク州保険監督官）に報告することを要求している。

D. G7FE－要素 6 の結果の評価

188.G7FE の 6 番については、G7 が提案する望ましい結果は以下のとおりである。

189.**G7FEA の結果 1-基礎的要素（G7FE）が整備されている。**上記パラグラフ 72-73 で議論。

190.**G7FEA 結果 3 – 混乱が発生するという理解がある。**上記パラグラフ 125-126 で議論。

191.**G7FEA 結果 4 - 適応型サイバー・セキュリティアプローチが採択されている。**上記パラグラフ 155-156 で議論。

3.7 G7FE－要素 7：情報共有

192.**G7FE の 7 番目は、企業に対して、「防御の強化や被害の最小化、状況認識の向上や広汎な知識の習得のため、脅威、脆弱性、インシデントの発生、発生時の対応に関する、信頼性の高い実践的なサイバー・セキュリティ情報を、内外の関係者（金融セクター内外の金融機関及び当局を含む）とタイムリーに共有すること。」を要求する。**

193.G7FE の 7 番目では、「テクニカルな情報 ― 脅威に関する情報や、脆弱性が悪用された際の詳細な情報等 ― を共有することにより、金融機関は自らの防御手段をアップデートし、攻撃者の最新の手口を習得することができる。」と述べている。

194.さらに、企業間、企業と公的当局間、および公的当局間での広範な見識の共有は、「重要な経済機能を混乱させ、かつ金融安定を危険にさらす可能性のある、セクター全体の脆弱性を攻撃者がどのように悪用しうるかについての集団的理解を深める。」

A. 保険コアプリンシプルへの G7FE 要素 7 の位置付け

195.保険会社にとって、G7FE 7 の勧告は、ICP 8.1.2 で取り上げられた危機管理計画の要件に位置付けることができる。

196.ICP16（ソルベンシー目的での全社的リスク管理）は、専門的情報および広範な見識の共有は、ICP16.1074 で取り扱われている、リスク対応性およびフィードバックループの一部として、実践可能であることを証明した[80]。

197.監督者間の情報共有は、一般的に ICP 3、25、および特に 26[8182]でカバーされている。これらの ICPs はクロスボーダーな危機的状況を含む情報交換と監督の協力のための枠組みおよびガイダンスを提供する。

B. 情報共有に関する監督者への提言

198.サイバー・セキュリティの情報共有に関しては、監督実務が以下をリスクベースかつプロポーショナルな方法にて奨励または反映することが適切となりうる：

a. 保険会社は、関連するサイバー脅威情報を収集し、分析するプロセスを確立すべきである。保険会社は、サイバー脅威に関連するサイバー実務、サイバー脅威、サイバー脅威に関連する早期警告指標に関する情報を収集、配付、評価するために、業界間、政府間を越え、および国境を越えたグループなど、情報共有グループおよび集団に積極的に参加することを検討すべきである。保険会社は、関連する管轄区域に設置されている場合は、インシデント対応チーム（IRT）などのシステム全体のイニシアティブに参加することもできる。

b. 保険会社が、金融サービス情報の共有・分析センター（FS-ISAC）という、サイバーおよび身に及ぶ脅威となる情報収集の分析および共有のための、認識された金融セクターへの世界的なリソースと協働することは適切となりうる[83]。FS-ISAC は 2012 年に、メンバーが情報、ベストプラクティス、および脅威情報を同業者の機関と共有することを可能にする、保険リスク審議会を設立した。

---

80 ICP 16.10 は、ICP 8.10.へ移行統合される。

81 ICP 3 (情報交換および守秘義務要件), ICP 25 (監督上の協力および調整) and ICP 26 (危機管理における国境を越えた協力および調整)。 ICP 26 は削除され ICP 12 および ICP 25 に統合される。

82 ICP 21 (保険詐欺対策)および ICP 22 (マネー･ローンダリング対策およびテロ資金供与対策)もまた、それぞれのトピックに関し監督者間の情報共有について言及している。

83 FS-ISAC に関する情報は、以下で入手可能。https://www.fsisac.com/about

c. サイバー脅威情報の保険会社による分析は、企業固有の状況を提供するために、社内外のビジネス情報およびシステム情報の他のソースと連携すべきであり、サイバー攻撃の可能性、意図、および犯罪者の決まった手口を保険会社が予測できるようにすることで、情報のタイムリーな洞察を提供し、意思決定の強化についての知見を与える役立つサイバー脅威情報収集に情報を変える。（C/I 8.2.2）

d. 実行可能であれば、保険会社のサイバー脅威情報収集の運営には、保険会社の第三者サービスプロバイダー、公共事業プロバイダーおよびその他の重要なインフラ供給者によってもたらされる、関連するサイバー脅威に関する情報を収集し解釈する機能が含まれるべきである。さらに、サイバー脅威の情報収集の運営では、この情報を、システム内で適切な保護措置を実施する目的でセキュリティ脅威および脆弱性を識別、評価、および管理する方法を理解すべきである。この状況において、関連するサイバー脅威の情報収集には、サイバー攻撃が保険会社またはその外部委託関係先のいずれかで引き起こされる可能性のある各地域での進展に関する情報を含みうる。（C/I 8.2.3）

e. 適切に情報解釈ができた場合、サイバー脅威情報により、保険会社はリソースの優先順位付け、リスク軽減戦略、研修プログラムを検証し、知見を得ることができる。したがって、保険会社は、戦略的、戦術的、および運用上のレベルでサイバー・リスクの軽減の責任を負う保険会社の適切なスタッフにサイバー脅威情報収集を可能にすべきである。サイバー脅威情報の収集は、サイバー・セキュリティ対策の実施が脅威の通知に基づくことを確実にするために、利用されるべきである。（C/I 8.2.4）

f. 大規模なサイバー・セキュリティ・インシデントへのセクター全体の対応を容易にするために、保険会社は、サイバー・セキュリティ・インシデントの間、およびサイバー・セキュリティ・インシデント後に、自らのシステムおよび他のセクターからの参加者のシステムについて、発見、対応、再開、回復を容易にする、信頼できるチャネルを通じ、タイムリーな情報を収集かつ交換する、情報共有を計画すべきである。保険会社は、対応プログラムの一環として、どのタイプの情報を誰と共有し、保険会社に提供される情報をどのように処理するかを事前に決定すべきである。報告要件および能力は、関連する法律および規制、ならびに保険会社のコミュニティおよび金融セクターにおける情報共有の取決めと整合すべきである。（C/I 8.3.1）

g. 保険会社は、第三者のサービスプロバイダーとの間でサイバー・セキュリティの枠組みに関する情報を相互に交換して、リンクまたは相互に作用するシステムを確保するお互いのアプローチについて相互の理解を促進することを検討すべきである。このよ

うな情報交換は、より優れたサイバー・セキュリティを実現するために、保険会社とそのステークホルダーのそれぞれのセキュリティ対策を適合させる取組を容易にするであろう。（C/I 8.3.2）

C. 現行の実務の例

199.欧州連合。一般データ保護規制（GDPR）[84]は、企業の機密保持のレベルに応じて、個人データの具体的な取扱いを導入している。監督者の間では、ソルベンシーII 同等性および覚書（MoU）を通じ、広範な調整が予見されている。さらなる枠組みとして、NIS 指令[85]は、保険会社が不可欠なサービスの提供者として特定されている限り関連性がある。

200.フランス。ACPR は専門家、フランスのサイバー・セキュリティ機関である ANSSI（コンピューターセキュリティのための国家機関）、およびフランス銀行の CERT（コンピュータ緊急対応チーム）と連携する。 ACPR はまた、金融セクターの会社のサイバー・セキュリティ問題に関するアプローチおよび実務の一貫性を確保するために、銀行セクターとのサイバー監視と意見交換を行っている。監督者として、ACPR はこの新しいエコシステムにおけるサイバー・リスクの監督に十分に関与している。 ACPR は、サイバー・セキュリティおよびデータ保護に関する健全かつセクター固有のアプローチを採用している。

201.この目標を達成するために、ACPR は以下の機関との複数の交流を進展させる。

- CNIL（IT および自由に関する全国委員会）
- ANSSI
- ENISA
- 国防省
- 企業およびその連盟、すなわち欧州保険協会。フランス保険協会（FFA）;フランス再保険専門家協会（APREF）;および
- アクチュアリー会

202.ACPR は、軍事計画法、GDPR、およびソルベンシーII の間の必要な円滑な連携を認め、また、サイバー・セキュリティの分析を精緻化するために監督者間の情報交換を支援する。

---

84 一般データ保護規制ポータル：https://www.eugdpr.org/ GDPR は新しい規制であり、2016 年 5 月 24 日に採択され、2018 年 5 月 25 日に施行された。

85 ネットワークおよび情報システムのセキュリティに関する指令（NIS 指令）2016/1148 は、2016 年 7 月 6 日に欧州議会で採択され、2016 年 8 月に施行された。加盟各国は、2018 年 5 月 9 日までに指令を国内において法制化し、2018 年 11 月 9 日までに必須サービスの運営者を特定する。

203. フランスでは、特定の法律がすでに GDPR の要件の一部をカバーしている[86]。この枠組みを考慮して、ACPR は、アクセス権ならびにデータの修正および削除の権利、第三者への情報の可搬性、商品ガバナンスおよび匿名性を含む、個人に対し強化された新たな権利を認めている。これらの新しく調和された原則は、保険会社のサイバー・セキュリティの監督にとって適切なものとなりうる。

204. ネットワークおよび情報セキュリティ指令の移転は、デジタルセキュリティに関する国家戦略および軍事法計画を通じてフランスでも行われている。ACPR は CNIL、ANSSI、FR-CERT と協力して、保険会社にとっての情報セキュリティと被保険者のデータ保護に関する一貫性のある適切なアプローチを開発している。

205. ドイツ。ドイツでは、「重要インフラ保護の実施計画」の略称である「UP KRITIS」と呼ばれる官民間のサイバー・セキュリティ調整フォーラムがある。 UP KRITIS は、IT セキュリティに重点を置いて、ドイツの重要なインフラを保護するために、重要インフ運営者、団体、および国家間で協力するイニシアティブである。

206. さらに、セクター固有の、特に保険セクターのワーキンググループが設立されている。これらのワーキンググループでは、対応するセクターの全てのメンバー、BSI（連邦情報セキュリティ局）および BaFin が参加し、サイバー・セキュリティに関する情報を共有する。

207. カナダのケベック州。保険会社が利用可能な AMF 自己評価ツールは、特に、役員、上級管理職、取締役会、顧客、メディア、サプライヤー、規制当局を考慮した重要なサイバー・インシデントを管理するための社内外のコミュニケーション計画を策定するよう機関に推奨する。

208. このツールはまた、保険会社が情報交換に特化したフォーラムに参加すること、および利害関係者、専門的なフォーラム、およびセキュリティ分野で著名な専門家の協会に主に頼る監視プロセスが、サイバー・セキュリティの問題および動向を検出するために整備されるよう推奨する。

209. シンガポール。シンガポールでは、シンガポール金融庁（MAS）が、IT セキュリティベンダー、法執行機関、および国際的な金融監督当局から収集された情報を通じて、新しい進化するサイバー脅威を継続的にモニタリングしている。また、MAS

[86] 「Loi pour une République numérique」 （2016 年 10 月 7 日）

は、主要な金融機関（FIs）からの毎月の IT セキュリティ脅威指標を収集することにより、シンガポールの金融セクターのサイバー脅威の状況をモニタリングする。これにより、MAS は、攻撃が成功しなかった場合でも、FI が直面しているサイバー攻撃量および主要ベクトルの幅広いシフトを把握できた。適切であれば、調査での発見事項は FIs と共有される。

210.業界と他のステークホルダーとのパートナーシップを強化するために、MAS はシンガポールの主要 FIs 間でサイバーに関する情報収集の共有を促進する安全な基盤（FINTEL）を確立した。また、シンガポールの主要な FIs は、米国金融サービス情報共有・分析センター（FS-ISAC）のメンバーとして、情報共有ネットワークを活用するために登録している。

211.FS-ISAC は、MAS の支援を受けて、シンガポールにアジア太平洋地域における業界団体の唯一のサイバー・インテリジェンス・センターを設立した。このセンターは、シンガポールの金融業界がサイバー脅威をよりよく監視し、FIs に向上した情報収集の支援を行うのに役立つ。また、シンガポールとより広範な APAC 地域のサイバー・セキュリティのコミュニティの能力を強化するのに役立つ。

212.英国。FCA は、サイバー・コーディネーション・グループ・イニシアティブを実施し、共同議長を務め、四半期ベースで約 175 の企業をまとめ、 特定のセクターに調整した。 これには、保険セクターのサイバー・コーディネーション・グループ（ISCCG）が含まれる。 これらのグループはそれぞれ約 25 の企業で構成され、また、FCA、イングランド銀行、英国財務省、国家サイバー・セキュリティセンター、国家犯罪対策庁も含まれる。グループは、サイバー・リスク、修復の取組、新しく進化する脅威、およびサイバー・インシデントについて、情報を共有できる機密度の高いフォーラムを提供する。 グループはまた、大規模なサイバー事象（例、WannaCry）後に業界の集団での対応を再検討するために会合を開いた。

213.また、FCA は、サイバー・リスク、監督実務、および検査アプローチに関する情報を共有することで、様々な重要なパートナーと双方向で協力している。これには、関連する全ての国内機関および国際的な規制に関する同業者が含まれる。

214.英国ではより広く、国家のサイバー・セキュリティ予算で資金提供され、会員の企業は無償となるサイバー・セキュリティ情報共有パートナーシップ（CiSP）を NCSC が主催している。CiSP は、機密度の高い、ダイナミックな環境で、サイバー脅威の

情報をリアルタイムで交換し、状況認識を高め、英国のビジネスへの影響を軽減するための業界と政府の共同イニシアティブである。

215.英国の企業は、FCA、PRA、および個人データが関与する場合は、GDPR に基づいて、プライバシー監視機関（ICO）に重大なサイバー事象を報告する義務がある。

216.米国。NAIC の保険データ・セキュリティ・モデル法のセクション 4D では、保険会社は、その実務の実施を決定する裁量を保険会社に与えた上で、新たに生じる脅威または脆弱性に関する情報を保険会社が常に入手するよう求めている。セクション 6 では、保険会社に対して、監督官（すなわち、州の保険監督者）、影響を受ける消費者、およびその他特定のステークホルダーにサイバー・セキュリティ事象を通知することを要求する。セクション 8 は、特定の政府系企業と NAIC 間の文書の共有を規定している。

217.審査官ハンドブックは、保険会社が他の当事者から学んだ洞察を、自社の統制に対する対応の強化にどのように組込むかを評価することに重点を置いている。リスク・プロファイルは、情報共有フォーラムおよび情報源（例えば、金融サービス情報共有・分析センター、FS-ISAC）から受け取った脅威および脆弱性情報を使用して作成される。

218.州の保険規制当局は、連邦および州の金融規制当局と定期的に調整を行う。これらの共同取組の一環として、州の保険規制当局と NAIC は、米国財務長官が議長を務める金融・銀行情報インフラ委員会（FBIIC）を通じて、金融機関とのコミュニケーションを促進し、サイバー・セキュリティのリスクを管理および評価する、規制上のアプローチを実効的に調整する方法を検討する。 FBIIC の加盟機関は、金融セクター全体のサイバー・セキュリティ事象に関するタイムリーかつ実用的な情報の共有を促進するための MoU を確立している。

219.FBIIC は、堅固で回復力のある金融サービスセクターを維持するという共通の目標に向けて、米国財務省と協力している民間セクター機関である金融セクター調整協議会（FSSCC）と定期的に協力している。FBIIC を通じて、州の保険規制当局および NAIC は、米国財務省および FSSCC と協力し、テーブルトップの演習を円滑に進め、保険業界全体にわたるサイバー・セキュリティ・インシデントへの対応および回復を探る。さらに、州の保険規制当局は、独立および行政の監督機関のサイバー・セキュリティフォーラムに参加して、米国経済のさまざまなセクター間におけるサイバ

ー・セキュリティ課題についてのベストプラクティスおよび共通の規制上のアプローチについて協議している。

220.州の保険監督当局は、情報共有の価値を認識し、新たに生じるサイバーの脅威を特定、評価およびモニターする一助となる FSISAC などの情報共有・分析機関を活用するよう保険会社に奨励する、NAIC の「実効的なサイバー・セキュリティの原則：保険規制ガイダンス」[87]で、情報共有の重要性を強調した。

221.NYDFS の*『金融サービス会社に関するサイバー・セキュリティ要件』*のセクション 500.17 では、保険会社は、サイバー・セキュリティ事象が生じたとの判断から 72 時間以内にサイバー・セキュリティ事象を監督者（すなわち、ニューヨーク州の保険監督者）に報告することを要求する。

D. G7FE－要素 7 の結果の評価

222.G7FE の 7 番目について、G7 が提案する望ましい結果は以下のとおりである。

223.**G7FEA 結果 1-基礎的要素（G7FE）が整備されている。**上記パラグラフ 72-73 で議論。

224.**G7FEA 結果 5 - 行動を促す文化がある。**要素 7（情報共有）と要素 8（継続的学習）に基づいて、実効的なサイバー・セキュリティを組織の仕組みに組み込むには、スキルと行動に継続的に焦点を当てることが不可欠である。

225.多くのサイバー・セキュリティ・インシデントでは、欠陥のある手続きまたは人的要因が重要な役割を果たす（例えば、弱いパスワード、社会工学、貧弱なセキュリティ意識などを活用する）。実効的なサイバー・セキュリティ戦略は、技術的解決策と同じ条件で人およびプロセスの側面を考慮し、これを投資判断に反映させる。研修および認識は、エンドユーザー、従業員、上級管理者を対象としており、同様に重要である。

226.人間が利便性のために機密情報を交換することが多い世界では、人間の心理の操作は、敵対者の技術的高度化と同様に関連している。それぞれの人は、彼らが果たす役割を理解している。実効的なサイバー・セキュリティは、人々の関与、教育、および情報の安全な取扱を可能にすることに依存する。サイバー・セキュリティの研修およ

---

[87] NAIC の「実効的なサイバー・セキュリティに関する原則：保険規則ガイダンス」（2015 年），http://naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf .

び認識は、技術的知識を強化するだけでなく、行動を変える機会を提供することができる。実効的な研修は、方針一式への遵守に努めるのではなく、真性かつ測定可能な変化、有意義な文化の形成を目指す。人々が最も弱いリンクと見なされるということわざが、最も価値のある資産として掲げる代わりに、覆されている。

3.8 G7FE－要素 8：継続的学習

227. **G7FE の 8 番目は、金融機関に対し、「サイバー・リスクの変化に対処し、資源を割当て、ギャップを特定・改善し、教訓を活かすため、サイバー・セキュリティ・ストラテジーとフレームワークを定期的かつ必要に応じて見直すこと（見直しに際しては、ガバナンス、リスク管理の評価、モニタリング、インシデント対応、復旧、情報共有の要素を含むこと）。」を要求する。**

228. G7FE の 8 番目では、「サイバーに関する脆弱性・脅威は、それらに対処するためのベストプラクティスや技術標準が進化するのと同じように、急速に進化している」と述べている。したがって、「金融機関のサイバー・セキュリティ・ストラテジーとフレームワークは、金融セクター全体のそれと同じく、脅威やその統御環境の変化に対応し、利用者の意識を向上させ、実効的に資源を配分するために、定期的な見直しとアップデートを必要とする。」

A. 保険コアプリンシプルへの G7FE 要素 8 の位置付け

229. G7FE の 8 番目は、適切な情報、管理プロセスおよび客観的評価に基づいてフィードバックループを組み込むことを保険会社のリスク管理システムに要求する、ICP 16.10 に基づく全社的リスク管理の枠組みにおけるフィードバックループによって捕捉されうる。

B. 継続的学習に関する監督者への提言

230. サイバー・セキュリティの継続的学習に関しては、監督実務で以下をリスクベースかつプロポーショナルな方法にて奨励または反映することが適切となりうる。

a. 保険会社は、変化する脅威環境の中で継続的なサイバー・セキュリティを確保することを前提とした、サイバー・セキュリティの枠組みを採用すべきである。

b. 保険会社は、後手に回る統制を超え、将来のサイバー事象に対する先を見越した保護を含む、サイバー・リスク管理実務を実施すべきである。

c. 将来のサイバー事象の予測能力と予測は、ベースラインから逸脱した活動を分析することに基づく。保険会社は、予測能力を達成または取得し、複数の内外の情報源からデータを捕捉し、そのような専門知識をアウトソーシングすることを含め、行動およびシステム活動のベースラインを定義するように努めるべきである。（C/I 9.2.3）

d. サイバー脅威の急速な進化に遅れずに追従する上で実効的とするためには、サイバー・リスクのダイナミックな性質を利用して進化し、また、保険会社が自社のシステムに適切なセーフガードを導入する目的で、セキュリティの脅威および脆弱性を識別、評価、および管理できるようにする、適応型のサイバー・セキュリティ枠組みを導入すべきである。保険会社は、あらゆるレベルでの弾力性の姿勢が定期的かつ頻繁に再評価される、サイバー・リスクを認識する文化を浸透させることを目指すべきである。（C/I 9.1）

e. 保険会社は、回復力を高めるために、組織内外で発生したサイバー・イベントから重要な教訓を体系的に特定し、抽出すべきである。有用な学習ポイントは、使用された方法およびサイバー攻撃者が悪用した脆弱性の観点から、成功したサイバー侵入およびニアミスから得られることが多い。（C/I 9.1）

f. 保険会社は、技術の進展を積極的にモニターし、既存のおよび新しく開発されたサイバー攻撃の形態により実効的に対抗できる新しいサイバー・リスク管理プロセスに通じているべきである。保険会社は、そのような専門知識のアウトソーシングを含む、サイバー・セキュリティを維持するための技術とノウハウの獲得を検討すべきである。（C/I 9.2.1）

g. サイバー・リスクの定量化のための方法は、進展し続けるため、保険会社は、運用上の信頼性目標などの事前に定めた規準一式に対して、サイバー・セキュリティの成熟度を評価するための指標の使用を検討してもよい。保険会社はベンチマーキングにより、監査人の調査結果、経営監査、インシデント、ニアミス、テストおよび実習、ならびに外部および内部インテリジェンスを分析して関連付けることができる。（C/I 9.2.2）

C. 現行の実務の例

231. ドイツ。BaFin の IT 要件に関する回報によると、管理委員会は、組織上および運営上の IT 構造のための規制は、IT 戦略に基づいて決定されていること、および組織の活動およびプロセスにおけるあらゆる変化を可能な限り反映するために修正されることを確認する責任を有する。

232. カナダのケベック州。AMF の事業継続管理ガイドラインでは、保険会社が自社の事業継続計画の信頼性を定期的に検証することを推奨する。技術的および手続き的な変更だけでなく、従業員の役割および責任の変更は、計画の信頼性に影響する場合がある。したがって、その信頼性を定期的に確認することが重要である。 AMF は、事業継続の管理プロセスが、保険会社、外部当事者およびその環境に影響を及ぼすあらゆる変更を考慮に入れた動的なものであることを期待する。

233. さらに、保険会社が利用可能な AMF 自己評価ツールは、金融機関がサイバー・セキュリティの枠組み、その計画の策定および実施を担当する特定の人物を指名することを推奨している。保険会社は、事前に設定された頻度に従い、サイバー攻撃シミュレーション実習を使用した対応および回復計画の有効性を検証することを推奨する。最後に、重大なサイバー・インシデントが発生した後、事象の発生順序を文書化し、統制および管理プロセスの不備を特定し、回復計画を立てるために、事後調査が実施されるべきである[88]。

234. 英国。FCA は、インシデントにより継続的な学習の機会を得られるよう確保するために、技術の機能停止またはサイバー攻撃の対象となる規制対象の企業に対し、学んだ教訓の報告書および根本的原因の分析を定期的に要求する。事業継続計画は少なくとも年に一度は見直されるはずであり、また CCG イニシアティブにより、サイバー攻撃の対象となる企業の教訓を他の企業と共有することができる。

235. 米国。NAIC の保険データ・セキュリティ・モデル法のセクション 4G では、技術の変更、ネットワーク上に格納された情報の機密性の変更、情報の内的または外的な脅威および保険会社自身の事業変更に基づいて、情報セキュリティ・プログラムをモニター、評価および調整するよう保険会社に求める。

236. 審査官ハンドブックには、保険会社が情報共有グループおよび集団から、ならびに、過去のインシデントおよび違反から得た情報に関するセキュリティ・プログラムをどのように更新するかに関するテスト条項が含まれている。ハンドブックのガイダンスはまた、保険会社が自社のサイバー・セキュリティ・プログラムを継続的に更新する重要性を強調している。ガイダンスでは、失敗したサイバー・セキュリティ事象は、規制上の重大な影響（罰金、報告など）を及ぼすことがないものの、会社の役員が学

[88] AMF の「ビジネス継続性マネジメント指針」（2010 年 4 月），
https://lautorite.qc.ca/en/professionals/insurers/guidelines/

ぶべきで、かつ、セキュリティ・プログラムを強化できる方法を特定する好機として生かせる、重要な出来事を表すことを強調している。

237.NYDFS の『金融サービス会社に関するサイバー・セキュリティ要件』のセクション 500.05 は、サイバー・セキュリティ・プログラムの有効性を評価するために、自社のリスク評価に従って開発されたモニタリングおよびテストを実施することを保険会社に要求する。セクション 500.14 は、保険会社が全ての社員に対して定期的なサイバー・セキュリティ認識のための研修を提供することを要求する。

238.NYDFS の*『金融サービス会社に関するサイバー・セキュリティ要件』*のセクション 500.17 は、保険会社に対し、取締役会または上級役員により、規制の遵守を証明するよう求める。 保険会社が「重要な改善、更新または再設計を必要とする分野、システムまたはプロセスを特定した場合」、保険会社は、「そのような分野、システムまたはプロセスに対処するために、計画されている、および進行中の徳衛および是正の取組みを文書化する」よう求められる。

D. G7FE－要素 8 の結果の評価

239.G7FE の 8 番目については、G7 が提案する望ましい結果は次のとおりである。

240.**G7FEA 結果 1-基礎的要素（G7FE）が整備されている。**上記パラグラフ 72-73 で議論。

241. **G7FEA 結果 5 - 行動を促す文化がある。**上記パラグラフ 224-226 で議論。

4.0　事例研究—オランダ銀行

242.数年の間、オランダ銀行（DNB）は、保険セクターにおいて情報セキュリティの習熟度のレベルを評価するための枠組みを使用してきた。サイバー・セキュリティは、情報セキュリティの一部としてレビューされている。その枠組みは、COBIT に基づき、統制対象を含む 54 の選択は、情報セキュリティ監督（「DNB の評価枠組み」）の、認められたモデルを導いた保険業界との間の緊密な協議によってなされた。

243.毎年 DNB は、これらの規制に関する情報セキュリティが要求されるレベルに達する程度を判断するために、保険会社の選択において、情報セキュリティレビューを実施する。保険会社は、セクターの性質および具体的な機関のオペレーショナル統制が考慮に入れられる、原則に基づく評価の対象である。機関によるレビューのための毎年の選択は、フォローアップ評価および、以前は情報セキュリティレビューとして選択されていなかった機関に関する評価を構成する。後者はベースライン測定と呼ばれている。その意図は、習熟度が許容される最低基準に達するまでの 3 年間に 1 度各保険会社を取り扱うということである。保険会社自身が彼らの情報セキュリティの質を頻繁に評価し、必要な場合には、改善するための対処を行うことが期待される。保険会社は、そのように DNB 評価枠組みを使用することが可能である。

244.情報セキュリティのレベルを判断するために、要求される基準の概略を提供する DNB 評価枠組みは、COBIT に基づく習熟されたモデルを使用する。一般的に、保険会社統制は、—期間全体を通じて設計され、実効的なオペレーションがされていることを意味する—最低限レベル「3」の習熟度を有すべきである。これは、54 の統制の内の 51 個に適用される。リスク管理に関連する 3 個の統制については、レベル「4」の習熟度が要求される。

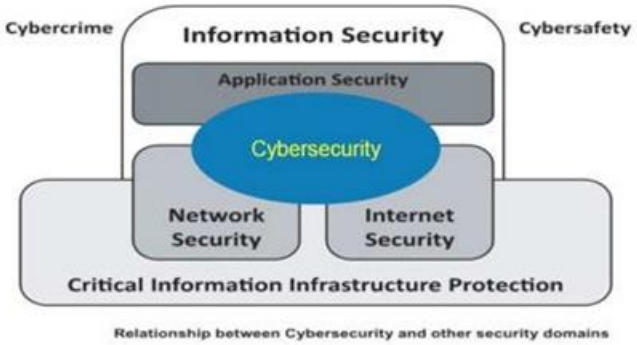
245.以下の表は、DNB 評価枠組みにおいて考慮される習熟度の定義を示す。

レベル	統制の定義
0	**存在しない**—文書がない。統制に関し認識および注意がない。
1	**初期／アドホック**—統制は（部分的に）定義されている一方で、統一された方法でない。実行方法は、個人による。
2	**反復可能、しかし直観的**－統制は、適切であり、構成、一貫して実行されているが非公式的な方法である。
3	**定義されている**—統制は文書化され構成および定式化された方法にて実行される。

	統制の実行は保証される。
4	**管理され、測定可能である**—統制の実効性は、必要に応じて定期的に評価および改善される。この判断は、文書化されている。
5	**最適化されている**—全社リスクおよび統制プログラムは、継続的かつ実効的な統制およびリスク問題の解決策を提供する。内部統制およびリスク管理は、企業実務に統合され、統制モニタリング、リスク管理、コンプライアンスの実施について完全な説明責任を有する自動化されたリアルタイムのモニタリングによって支えられる。統制評価は継続的であり、自己評価に基づき、ギャップおよび根源は分析の原因となる。従業員は、統制改善について積極的に参加している。

246.情報セキュリティに関する監督は、年ごとに選択された保険会社によって完成された自己評価を通して支えられ、その後、保険会社に立入る IT 専門の監督者のチームによって試される。

247.情報セキュリティレビューという枠組みの中で、DNB は、選択された保険会社に自己評価である DNB の評価枠組みを完成させるよう要求する。これらの保険会社は、DNB が情報セキュリティを十分に保証するために、重要であると考える習熟度を 54 個の統制に自主的に割り当てるよう要求される。さらに、DNB は、機関へ証拠書類にて割り当てる基準を具体化するよう、また独立した当事者または部門（好ましくは内部および独立した外部監査）が自己評価を有効化することを保証することを要求する。



Relationship between Cybersecurity and other security domains

248.IT 専門の監督者による立入り試験は、年度によって異なることがある統制の選択によって実行される。毎年、選択は、その年に調査の対象であった全ての保険会社に適用される。その調査チームは、最小限の「サイバーに関連する」統制が選択されることを確保する。評価は、（サイバー・セキュリティを含む）情報セキュリティ方針、サイバー・セキュリティのガバナンス、リスク評価、物理的なセキュリティ、システ

ム・セキュリティ、人材の訓練および認知、モニタリングおよびテスト、事象評価、コミュニケーション、業務の継続性および第三者機関を取り扱う。DNB は、割り当てられたスポット・チェックに基づく習熟度の妥当性を分析し、必要に応じてこれらのレベルの調整を行い、その公表された習熟度について調査する。

249. 習熟度が水準を下回っていることを、DNB によって最終的に決定づけられた事例において、DNB は、機関に対し改善計画を提出するよう要求する。DNB は、進行中の監督または具体的なリスク軽減プログラムを通して、これらの改善計画の具体化を監視する。

250. チャレンジ・セッションの終了後、自己評価の結果は、保険会社のためのフィードバックおよび追加的な監督の手段を決定するために、他の類似する金融機関の基準に従って評価される。さらに、自己評価の結果は、DNB のウェブサイトにおいて包括的な（匿名化された）形式にて表されている。2017 年の主な結果は以下の通りである：

- セクターにおける情報セキュリティの習熟度は、増加している；
- 情報セキュリティは、いまだ要求されたレベルに達していない；
- （全てのサービス提供者を含めた）チェーン全体を通じた情報セキュリティは、いまだ不十分である；
- IT リスク管理の質は、改善されなければならない；
- サイバー・コントロールに対する機関の明確な注意に関し、大きな変動がある；
- サイバー脅威のレベルは変化している；
- セクター内における、より強い協力が要求される。

5.0　保険会社のサイバー・セキュリティ実務を評価するアプローチ

251.上記セクション 3 は、G7FE8 要素に対応する、保険会社への実効的なアプローチの潜在的な構成に関するガイダンスを提案する。

252.管轄区域は、（適切であるならば、管轄区域および企業のサイバー習熟度ならびにプロポーショナリティ原則についての考慮を含む）セクション 3 に対応する実務、統制、望ましい結果に基づく監督者要件または期待値を発展させる場合がある。

253.本適用文書におけるこのセクションは、保険会社が進めているまたはコンプライアンスを示している、サイバー・セキュリティに対する期待の程度を評価するための、実効的なアプローチの公表についての考慮に対応する。

254.ここに使用されているように、評価は、「（i）意図した結果に対して評価された実績の判断および（ii）是正措置を含む、改善余地のある分野のフィードバックおよび提示の提供を目的として」[89]個々の保険会社または集合体としてのセクターの「サイバー・セキュリティ実務および統制に関する組織的な収集、レビューおよび情報の使用」を意味する。

255.期待されたサイバー・セキュリティの結果における保険会社の発展およびコンプライアンスを評価する手段を取るということは、監督者の重要な役割として考えられるべきである。そのような評価プログラムを発展させる中で、監督者は、以下に要約される G7FEA のパート B で提案された「評価要素」を考慮に入れるべきである。

256.利用可能な専門的知見および他のリソースによって、評価プログラムの一部構成要素を外部委託することは、適切である場合がある。

257.以下の特性を埋め込むことは、サイバー・セキュリティ評価を行う実効的なプログラムを計画および設計する際に考慮される場合がある。

A.　監督者／評価者　明確な評価対象の公表および保険会社に対するそれらの対象を伝達する。

[89] 「G7FEA」（p.3）

258.G7FEA に記述されているように、評価者が、「評価者および評価された企業の両方に動機の明白性を提供ならびに責任を負うことを促進させるために評価活動のための明白な目標を公表」することは、重要なことである[90]。

259.評価者および保険会社の両者は、評価の基準を理解すべきである—特に「レビューに基づくサイバー・セキュリティの側面」[91]例えば、監督者が本適用文書に記述されている保険セクターのサイバー・セキュリティに関する期待値を公表した場合、評価対象は、一部または全ての期待された実務および結果に対する保険会社の達成度を評価することとなる場合がある。

B. 監督者／評価者は、方法論および期待値を設定および伝達する。

260.G7FEA に記述されているように、評価者は、「サイバー・セキュリティ評価が行われる対象の明確およびある程度の期待値を公表」すべきであり、期待値は、評価が始まる前に保険会社に「伝達され、よって理解される」べきである[92]。

261.「評価者によって選択された方法論は、評価のもとに記された対象および企業の複雑性に対して調整される。評価の比率は、リスクに基づくアプローチを通じ、サイバー・リスクの複雑および動的な性質を考慮に入れることで達成されることができる。」[93]

C. 監督者／評価者は、ツールの選択に関し多様なツールキットおよび手続きを整備する。

262.G7FEA に記述されているように、評価者は、「評価によって求められた範囲または習熟度の具体的な幅、深さを反映するために」[94]に利用可能な評価技術および方法の範囲を設けるべきである。

263.全ての評価が必ずしもオンサイトである、または問題について同じ範囲を取り扱うというわけではない。例えば G7FEA は、サイバー・セキュリティ評価のための「ツールキット」は、その他の技術および方法の中で：デスクトップレビュー；自己評価；オンサイト検査；脅威に基づく侵入テスト；技術レビュー；論題レビューおよび活動を含む場合があると記す—そしてそれらのツールは、単体でまたは組み合わせて使用可能である。

---

90 「G7FEA」（p.4）
91 「G7FEA」（p.4）
92 「G7FEA」（p.4）
93 「G7FEA」（p.4）
94 「G7FEA」（p.4）

264.評価者は、理想的に確定した手続きを通じて、どのツールが特定の評価の対象として適切であるかについて判断すべきである。G7FEA は、選択手続きは「より幅広いセクターに対する企業の重要性および内在するリスク；評価の具体的な性質および範囲；評価に関して費やされるリソースおよび時間；ならびに求められたレベルの保証のような要素を使用」[95]すべきであると提示する。

D. 監督者／評価者は明確な発見および具体的かつ改善的な期待値を報告する。

265.G7FEA に記述されているように：「実効的なセキュリティ評価は、判断および行動をなすための有意義なアウトプットを行う。これは、将来の行動に導く明確な結論を組み立て、具体的な改善策および／または主題の発見を認識することを意味する[96]。

266.「主要な結論を描く際に、評価者は、観察されたプラクティスおよび達成された事項を要約するとともに集められた事実から浮かび上がる期待に反するギャップまたは欠点を特定する。評価者は、関連するあらゆるリスクまたはその他の問題およびその影響について記述する。総じて、評価のアウトプットは、価値の提供、意思決定のサポート、ならびに重要かつ持続的な改善に導くフィードバックを生む。」[97]

267.評価結果を監査および知識を共有することを考慮する。技術的能力および評価の質は、「実施された評価および採用された方法論の独立したレビュー（すなわち評価することおよび評価者）」ならびに「評価者による知識の共有；および評価者個人の評価」[98]を通して維持されることが可能である。

E. 監督者／評価者は、評価が信頼でき、かつ公正であることを保証する。

268.G7FEA に記述されているように、信用できるために、サイバー・セキュリティ評価は、確実かつ公正であるべきである。とりわけ評価者は、評価を行うに十分な技術的背景、業界知識および経験を有し、維持しなければならない。手続きは、評価のもとに保険会社に明白であり、また（上記の、評価のもとで保険会社に共有される）発見は、適切な範囲で秘密であるべきである。プロポーショナリティ原則もまたは公正さに関連する[99]。

---

95 「G7FEA」（p.4）
96 「G7FEA」（p.5）
97 「G7FEA」（p.5）
98 「G7FEA」（p.5）
99 「G7FEA」（p.5）

6.0 結び

269.2016 年の論点書に関し、本適用文書は、発展途上のプログラムの管理下にある保険会社が、サイバーにレジリエンスのある組織を発展および維持させるための必要性を適切に認識していることを確保するために、発展途上のプログラムにおいて監督者を支えるリソースとして意図している。

270.リスクベースかつプロポーショナリティ原則の適用を考慮に入れ、管轄区域の規制および監督は、過度にならずに ICP に一致する結果の達成に十分な解決策を許容し、管轄区域の具体的な条件および特徴に適合されるべきである。プロポーショナリティ原則にもかかわらず、また論点書に当初より記述されているように、「サイバーレジリエンスは、規模、特殊性、住所、または地理的範囲に関わらず、全ての保険会社によって達成されるべきである。」

271.そのようにすることは、挑戦的かつ進行中の試みへの努力を維持する。完全なサイバー・セキュリティの達成は、意欲的な目標であると認識することで、監督者は、適用文書にて言及されているように、専門家の（官民両セクターについての）業務にレバレッジをかけ、各法域内での保険会社のサイバーレジリエンスのための期待値を適正化し、保険会社がそのような期待値に責任を持つことについて重要な役割を有する。

272.保険会社が各管轄区域において保険契約者および政策立案者の機密性を保ち、保険セクターが国内外の金融システムの重要な要素として運営を継続するためには、監督者は、管轄区域下のシステムおよび顧客データの機密性、完全性、および有用性を保護するための基準、ツールおよび測定基準を発展および実施するために、本適用文書に記述されているような手順を検討する場合がある。

273.金融システム、各機関、および契約者をサイバー・セキュリティ・リスクから保護する際の監督者および責任ある保険会社の利害関係は、規定の分裂および重複を回避しながら、調整されている。したがって、規制者および保険会社の利害関係者間における協議および調整は、管轄区域が保険会社のサイバー・セキュリティ監督を発展および改善されるにつれて、促されるべきである。