金融セクターのランサムウェアに対するレジリエンスに関するG7の基礎的要素（仮訳）

ランサムウェアの発達と急増は、金融機関が現在直面している課題のなかで最も重大なもののひとつである。ランサムウェアは、侵害された情報システムを恐喝目的で操作し、身代金の要求が満たされるまで、被害者が当該システムや当該システムに保存されているデータを全く使用できないようにする[1]。ランサムウェアは、その性質上、被害者の業務継続能力に影響を及ぼす。金融セクターにとって、ランサムウェアは容認できないリスクをもたらし得る。

ランサムウェア攻撃は、その使用が利益をもたらさなくなるまで停止しない可能性がある。金融機関は、攻撃が生じる前に、ランサムウェアへのレジリエンスを確保するために必要な措置を講じることが重要である。その際には、金融機関に直接的又は間接的なランサムウェアリスクをもたらし得る、特に重要なサードパーティプロバイダについてのリスクも考慮すべきである。これらの課題に対処することで、金融機関が業務を維持すること及び攻撃者がランサムウェア攻撃による利益追求を継続する動機となり得る身代金の支払いを回避することに資する。

本文書は、金融機関にランサムウェアの脅威に対処するためのハイレベルな構成要素を提供する。これは規範的ではなく、拘束力を持つものではなく、G7メンバー全体を通じて実施されている現在の政策アプローチ、業界に対するガイダンス及びベストプラクティスを取り込むことを意図している。本文書は、主に民間セクターの金融機関及びその特に重要なサードパーティプロバイダに焦点を当てる一方で、金融当局が自らの内部におけるランサムウェアによる被害を低減する活動及び金融セクターのレジリエンスを高めるための取組みにも利用できる。

ランサムウェアに対するレジリエンスを作り出すための過程は、多くの場合、金融機関がサイバーインシデントに備え既に実施している過程と同様であるべきである。本「金融セクターのランサムウェアに対するレジリエンスに関するG7の基礎的要素」文書は、2016年に公表した「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」文書と整合している。元の文書で示された各要素について、本文書はランサムウェアの脅威に対処するために必要な、検討すべき事項を述べる。

1 本文書の目的上、用語の定義は別段の定めがない限り、金融安定理事会(FSB)のサイバー・レキシコンを参照する。FSBサイバー・レキシコン(2018年)の改訂が進行中であり、改訂版は2023年に公表される予定である。改訂版には、合意されたランサムウェアの定義が含まれる予定だが、2018年版のレキシコンには独立した定義がなかった。

要素１：サイバーセキュリティ戦略及びフレームワーク

ランサムウェアに対するレジリエンスを金融機関のサイバーセキュリティ戦略及びフレームワークに組み込むこと。

包括的なサイバーセキュリティ戦略及びフレームワークは、あらゆる組織のあらゆるサイバー・セキュリティ・プログラムに不可欠な構成要素である。ランサムウェアのリスクは、金融機関が検討する他の脅威とともに、統合された包括的なアプローチによって最善の取扱いがなされる。

成功したランサムウェア攻撃の大部分は、組織内の不適切なサイバー衛生の実践により生じた欠陥と関係している。これには、強力な認証行為の欠如、エンドユーザーへの不十分なサイバーセキュリティ及びフィッシング対策教育、不適切な資産管理、効果的なネットワークセグメンテーションの欠如、又は特に重要な資産に対する遅滞した若しくは不完全な脆弱性のパッチ適用が含まれる。これらの脆弱性は通常、金融機関のサイバーセキュリティ戦略及びフレームワークの中で対処される。

要素２：ガバナンス

実効的なガバナンス態勢を通じ、ランサムウェアが組織に及ぼす広範な影響に対する実効的な連携を確保すること。

ランサムウェアのインシデントが組織のIT部門に限定されることは稀であり、むしろ、ビジネス運営、法令及び規制の遵守体制、マーケティング並びに広報業務に係る機能に大きな影響を及ぼす。意思決定過程の全体にランサムウェアに対する計画を盛り込んだ、強力な企業のサイバーセキュリティ・ガバナンスを構築することが重要である。このような準備には、取締役レベルでの監視及び事業ユニット間の高いレベルの調整が含まれる。ガバナンスの議論では、資産追跡、データ分類及びバックアップ戦略、演習、脆弱性診断、エンドユーザーに対するサイバーセキュリティ教育のような問題が取り上げられる可能性があり、これらはすべて、ランサムウェア及びその他のサイバー脅威からの保護のために重要である。ランサムウェア関連の、上級管理者レベルでのガバナンスに係る議論の、さらなる重要なトピックは、以下のとおりである。

身代金要求に対する計画　―G7各国は、一般的に身代金の支払いに否定的であり、それは犯罪の企てへの資金提供を助長し、継続的な悪意ある行いに対する意図しない誘因を与える可能性があるためである。秘密鍵を入手できない可能性や、その鍵を用いたデータ復元が受け容れ難いほど遅い又は不完全となる可能性を考えると、身代金の支払いは復元データへのアクセスを保証しない。攻撃者は、ランサムウェア攻撃で取得した機密データの複製を保持することもあり、被害者に対する継続的な影響力をもたらす可能性がある。

身代金の支払いは、国の政策又は業界の基準によって妨げられる場合がある。経済制裁対象に指定された事業体への支払いを伴う場合のように、場合によっては、身代金の支払いが法的に禁止されることもある。金融機関は、ランサムウェアのインシデントが発生する前に、それぞれの法域の法律についてあらためて調査することを検討すべきである。金

融機関は、潜在的な制裁リスクを評価するために、攻撃者又はランサムウェアに係る支払いの受取人について特定が困難な可能性があることも考慮すべきである。

事業継続計画 ―ランサムウェアのインシデントは、特に重要な情報システムを長期間にわたって停止させ、特に重要な業務運営に大きな影響を及ぼす可能性がある。組織内のサイバーセキュリティ専門家は、事業継続計画の考慮事項における他の運用上の構成要素と緊密に連携することで恩恵を得る。事業継続計画にはランサムウェアに係るシナリオを含めることを検討すべきである。

コミュニケーション計画 ―内部及び外部のコミュニケーション計画は、上級管理者レベルの協議を通じて対処することが最適なもう一つの項目である。金融機関は、その業務の中核的な部分において信頼に大きく依存している。金融機関は、適時かつ効果的なコミュニケーションを通じて対処できるように、主要なステークホルダー・グループの関心及び懸念を予め理解したいと考えるであろう。これには、顧客、取引先、従業員、監督当局者及び公衆一般が含まれ得る。

これらのグループは、ランサムウェアのインシデントにより、その影響を受けた金融機関がサービスを継続して提供する能力並びに口座保有及び個人・企業データのセキュリティに及ぼす影響について懸念を持ち得る。彼らはまた、支払要求への金融機関の対応に関して疑問を持ち得る。

組織横断的な計画 ―金融セクター内のランサムウェアインシデントは、個別金融機関への大きな影響に加え、他の金融セクター事業体とその顧客まで広範にわたる大きな影響を及ぼす可能性がある。ランサムウェアリスクに対処できる健全な体制を構築する上で、金融機関、業界団体、金融当局は重要な役割を果たしている。効果的な組織横断的計画は、様々なレベルの意思決定のための役割、責任、及び調整メカニズムを明確に特定することとなる。これらには、規制当局、法執行機関及びサイバーセキュリティ機関、保険提供者、緊急対応チーム、更にはバーチャル資産サービス提供者などの新たな利害関係者を含む、多様な利害関係者のグループが含まれ得る。

要素３：リスク及び統制策の評価

ランサムウェアリスクに対する統制策を確実に実践すること。

金融機関は、ランサムウェアのリスク及び既存のサイバーセキュリティフレームワークにおけるリスクに対応するための統制策を評価すること、並びにサイバー脅威の入口となりうるサードパーティプロバイダ（ストレージや電子メールなどのクラウドサービスを含む）の特定によって恩恵を得る。金融機関は、サードパーティのサイバーセキュリティ慣行及び自身が経験し得るあらゆるインシデントを認識することにより恩恵を得る。

金融機関は、保険契約への加入を通じて、ランサムウェアリスクへの部分的な対処策を求めることができる。保険契約は、一定のランサムウェア関連の損失、特に復旧に係る損失から企業を保護することができる。また、多くの契約では、侵害に対する指導、攻撃者とのコミュニケーション、広報、及びフォレンジックなど、幅広い対応リソースへのアク

セスを提供している。保険契約は、強力なサイバー衛生及び効果的なランサムウェア対策計画に代わるものではなく、実際、多くの保険会社は、保険引受プロセスの一環でこれらの証明を求める。保険契約には、制限、免責額及びサブリミット、並びに免責条項が含まれ、通常、金銭的損失の全額をカバーしない。例えば、風評やコンプライアンスへの影響など、ランサムウェアによる深刻な負の結果に対しては、保険をかけることが極めて困難である。

要素４：モニタリング

潜在的なランサムウェアの挙動に係る一連の兆候をモニタリングすること。

ランサムウェア活動の兆候は、金融機関が情報システム上で悪意のある、又は異常な活動を検知するために構築している不正侵入検知システム及び関連システムを通じて、最善に特定される。組織が外部のランサムウェアによる脅威の追跡に使用でき、また、傾向の特定に資することができる多様な情報源がある。これらの情報源には、とりわけ法執行及びサイバーセキュリティ機関、業界団体並びにサードパーティのセキュリティプロバイダーによって発行された脅威報告やインテリジェンスの提供が含まれる。

要素５：インシデント対応

ランサムウェアインシデントに対応するために策定した計画を実践すること。

金融機関によるランサムウェアへの対応は、複数のレベルで協調して業務を行う場合において、最も効果的となるであろう。金融機関は、ランサムウェアによる影響の様々な側面を反映した多様なシナリオを使った訓練を通じて、組織的対応を強化するため、継続した努力を行うことが重要である。

ランサムウェアインシデントは犯罪に該当しかねず、適切な権限を持つ当局との調整が必要な場合がある。金融機関は、インシデント中の連携が容易になるよう、ランサムウェアインシデントに先立って、適切な法執行機関、国家安全保障機関及び規制当局との関係を確立することから恩恵を得る。法域によっては、金融機関は、ランサムウェアインシデントを示す可能性のある疑わしい活動を権限ある当局へ報告をし得る、又はしなければならない。

多くの組織は、ランサムウェア対応活動の支援をサードパーティに依存することとなる。サードパーティの活用により、組織は、ランサムウェアへの対応経験を重ねた、訓練された担当者のサポートを通じて、迅速に対応能力を強化できる。ただし、金融機関は、広範なインシデントの場合には、同時に複数の組織からこれらのサービスへの需要が高まりうることも認識すべきである。したがって、金融機関は、対応計画の一環として、代替となり得るプロバイダの特定を検討し得る。

金融機関は、自身の特定のシステムに影響を与えないインシデントであっても対応するよう求められる場合がある。ランサムウェアの支払いは、仮想通貨交換業者を含む金融機関を通じて行われることが多い。金融機関は、ランサムウェアに係る疑わしい取引の届出を含む、マネー・ローンダリング及びテロ資金供与対策に関する義務を遵守することを通じて、ランサムウェアの脅威から金融システムを保護する上で重要な役割を果たしている。

さらに、各国は、犯罪者による金融サービスへのアクセス及び悪用を抑制するために、特に仮想資産に関して、金融活動作業部会基準を実施すべきである。

要素６：インシデントからの復旧

ランサムウェアによるインシデントで損なわれた可能性のある機能を回復するための手順を実践すること。

ランサムウェアインシデントからの回復に不可欠な要素は、システム及びデータのバックアップ及び復元である。データバックアップ戦略を策定する上で、金融機関は、通常のバックアップ実務をかいくぐり又は妨害するランサムウェア主体の能力を考慮すべきである。金融機関は、ランサムウェア主体がバックアップデータの感染を試みようとしているかもしれず、かつ、ランサムウェア攻撃自体が明らかになるよりもかなり前から感染を開始しているかもしれないことを考慮すべきである。これによって、金融機関のシステムを再感染させずにデータを復元することが困難になり得る。また、データが適切にバックアップ及び復元されていたとしても、攻撃者は、データが公開される危機にさらされていると恐喝する目的で、窃取したデータを保有する可能性がある。

金融機関は、ランサムウェアへのレジリエンスをもたらす特徴を備えたバックアップ戦略を検討すべきである。これらのソリューションには、保存されたデータの改変、削除、又は暗号化を防止するシステムが含まれ得る[2]。これらには、より頻繁なバックアップ、より長い期間のバックアップ保持、オフラインバックアップ並びにオンプレミス及びオフプレミスの様々なシステムにわたるデータ保持手法の冗長性といった取組みも含まれる。

対応活動と同様に、事前にバックアップをテストするとともに、データの復元並びに特に重要なユーザーアカウント及びソフトウェアの適切な目標時間内での再インストールを訓練し、検証した金融機関は、ランサムウェア攻撃からの復旧を最善に行えるだろう。データの復元は、特に大規模なデータセットの場合には困難であることで知られており、金融機関がバックアップから復元する際に予期せぬ問題に直面する可能性がある。

法執行機関の捜査官が必要とする可能性があるため、金融機関にとって、その回復プロセスを慎重に文書化することが重要である。また、金融機関が将来のインシデントに適用する可能性がある教訓を確認し、及び文書化することも重要である。

要素７：情報共有

ランサムウェアのインシデント及び情勢に関するデータ、情報、及び／又は知識を組織内外の必要な関係者と共有すること。

ランサムウェアの活動は、多くの場合、悪意ある主体、対象となる業界、使用される戦術及びその他の要因に基づいたパターンに従う。金融機関は、状況認識を向上させるためにこれらのパターンを理解するよう努めるとともに、修正に資する共通の脆弱性及び新たな侵害指標を継続的に監視するべきである。

2 これらの品質の一部又は全部を備えたバックアップ技術は、「イミュータブル」と呼ばれることがある。

法域によっては、ランサムウェア攻撃についての報告を義務付ける制度が存在する場合がある。金融機関は、インテリジェンス及び情報共有ネットワーク（例：金融分野のサイバーセキュリティインシデント対応チーム（CSIRT）及び情報共有・分析センター（ISAC））等の然るべき能力のある団体に報告することも考慮すべきである。

要素８：継続的な知見獲得

過去のインシデントから知見を得ることで、ランサムウェアに対するレジリエンスを高めること。

すべてのサイバーセキュリティ問題と同様、ランサムウェアに対する効果的な対処には、継続的な学習アプローチの採用が必要となる。ランサムウェア攻撃は、高度な攻撃に対しての一般的なサイバー衛生の欠如に起因することが多いため、金融機関は、システムへの不正アクセスにつながり、及びランサムウェアが悪用し得る脆弱性を生み出す可能性のあるフィッシング、ソーシャルエンジニアリングその他の攻撃の影響を受けやすいエンドユーザーの教育に、追加リソースの投入を検討すべきである。さらに、対抗技術が進化しているのと同じく、ランサムウェアの脅威は絶えず進化している。金融機関は、脅威環境におけるこれらの変化を追跡し、健全な慣行の遵守を確認するためシステムログを頻繁にレビューし、また、障害が特定された場合にはプロセスと構成を改善することで、ランサムウェアに対するレジリエンスを確保することができる。