2024 年 10 月号

金融分野におけるサイバーセキュリティに関するガイドライン

森・濱田松本法律事務所
弁護士　林 浩美
TEL. 03 5220 1811
hiromi.hayashi@mhm-global.com
弁護士　湯川 昌紀
TEL. 03 6266 8764
masaki.yukawa@mhm-global.com
弁護士　蔦 大輔
TEL. 03 6266 8769
daisuke.tsuta@mhm-global.com

Ⅰ. はじめに

2024 年 10 月 4 日、金融庁は、「金融分野におけるサイバーセキュリティに関するガイドライン」（以下「金融分野ガイドライン」といいます。）に係るパブリックコメントの結果を公表し、同日から適用を開始しました。

金融分野ガイドラインは、従来の監督指針や事務ガイドラインに記述されていたサイバーセキュリティに関する記述を独立させ、かつ、従来より詳細な規定としたものとなっており、「基本的な対応事項」と「対応が望ましい事項」に分けて対応事項が定められています。

金融分野をはじめとする重要なインフラ分野に関しては、サイバーセキュリティ戦略本部において推進している重要インフラに係る施策（重要インフラのサイバーセキュリティに係る行動計画）のほか、2024 年 5 月から、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）に基づく基幹インフラ制度の本格運用が開始されました。

また、経済安全保障の文脈では、国家安全保障戦略（2022 年 12 月閣議決定）において、「重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める」こととされ、これを受けて、内閣官房「サイバー安全保障分野での対応能力の向上に向けた有識者会議」において、重要なインフラにおけるインシデント報告の義務化を含めた検討が行われています。

そのような中で策定された金融分野ガイドラインは、他の重要インフラ・基幹インフラ分野の事業者はもちろん、それ以外の事業者にとっても参考になるものと思われるため、本レターにおいては、その概要を紹介いたします。

Ⅱ. ガイドラインの概要

金融分野ガイドラインでは、下表のような「基本的な対応事項」及び「対応が望ましい事項」が示されています。「基本的な対応事項」は、金融機関等が一般的に実施する必要のある基礎的な事項、「対応が望ましい事項」は、金融機関等の規模・特性等を踏まえるとインシデント発生時に、地域社会・経済等に大きな影響を及ぼしうる先において実践することが望ましいと考えられる取組みや、他国の当局又は金融機関等との対話等によって把握した先進的な取組み等の大手金融機関及び主要な清算・振替機関等が参照すべき優良事例を指すとされています。なお、下表では、特に留意すべきと思われる部分のみ要約しておりますので、詳細については金融分野ガイドラインをご参照ください。

	基本的な対応事項	対応が望ましい事項
サイバーセキュリティ管理態勢の構築	・取締役会等によるサイバーセキュリティ管理基本方針の策定 ・サイバーセキュリティ管理態勢のレビュー（少なくとも１年に１回） ・サイバーセキュリティリスクの状況、リスク評価及び取組計画の進捗状況の経営陣[1]への報告 ・サイバーセキュリティの規程及び業務プロセスの整備及び見直し（少なくとも１年に１回） ・リスク管理部門からのサイバーセキュリティ管理の実施状況の取締役会等への報告 ・サイバーセキュリティをテーマとした内部監査の実施、取締役会等への報告	・各部門の役割分担の明確化や外部専門家を利用した検証の仕組みを構築 ・統合的リスク管理の一部として位置づけ、リスク選好度[2]、リスク耐性度[3]を設定 ・サイバーセキュリティに関する取組みの公表 ・担当部署から経営陣への１年に２回の KPI[4]及び KRI[5]の報告 ・CISO の配置 ・リスク管理部門及び内部監査部門への専門性のある職員の配置
サイバーセキュリティリスクの特定	・情報資産管理 ・ハードウェア及びソフトウェアを適切に管理するための手続・台帳等の整備、最新の状態を網羅的に把握できるようにすること ・脅威情報、脆弱性情報の収集・分析、収集元及び収集・分析の方法の見直し（少なくとも１年に１回） ・リスク評価（少なくとも１年に１回、それに加えて重大な脅威や脆弱性が判明した場合や新規商品又はサービスの提供時）	・管理対象外の情報資産や未承認のクラウドサービスを特定して、適切に対応（管理対象とする又は使用中止等） ・ソフトウェア部品表（SBOM）の整備 ・重要な業務[11]を特定し、重要な業務を継続するために必要な組織内の人員、設備、システム、サードパーティの相互依存度を考慮したリスク評価 ・ペネトレーションテストは VPN 網、内部環境も対象とする ・脅威ベースのペネトレーションテスト（TLPT）の定期的実施

[1] パブコメ回答 27 番にて、「経営陣」は、会社法上の役員（業法において読み替える場合を含む）が該当し、「経営陣等」には、執行役員及びそれに準ずる責任者が含まれるとされている。
[2] リスク選好度（リスクアペタイト）とは、自社の戦略目標や事業計画を実現するために、リスクキャパシティ（組織が許容できる最大のリスク量）の範囲内において、進んで受け入れるリスクの種類と総量のこと。
[3] リスク耐性度（リスクトレランス）とは、リスク選好度（リスクアペタイト）を設定した上で、重要な業務と特定した金融サービスについて、未然防止策を尽くしてもなお、業務中断が必ず生じることを前提に最低限維持すべき水準のこと。金融分野ガイドラインでは、参考として、金融庁「オペレーショナル・レジリエンス確保に向けた基本的な考え方」（令和５年４月）が引用されている。
[4] パフォーマンス指標。金融分野ガイドラインでは、例として、標的型メール訓練の報告率、脆弱性対応率、情報資産棚卸進捗率、トレーニング受講率等が挙げられている。
[5] リスク指標。金融分野ガイドラインでは、例として、サイバー攻撃試行件数、監査指摘件数、インシデント件数、未対応の脆弱性件数等が挙げられている。
[11] 金融分野ガイドライン脚注 12 において、その中断が金融機関等の業務又は利用者もしくは金融システムに著しい悪影響を生じさせるおそれのある金融サービスと定義されている。

	・リスク評価については内部ネットワークセグメントも対象とする[6] ・リスク評価の結果に基づくリスク対応計画の策定、経営陣への定期的報告 ・ハードウェア・ソフトウェア等の脆弱性管理に係る手続等の策定、見直し ・パッチ適用等の対応期限を設定する（例外的にパッチ適用を実施しない場合には経営陣等[7]からの承認を必要とする） ・重要なサードパーティ[8]が保有するシステムの脆弱性対応の管理 ・脆弱性診断及びペネトレーションテストの定期的実施[9] ・定期的な演習・訓練を実施[10]	・内部人材によるペネトレーションテストの実施 ・テストベンダーの交代要否の検討
サイバー攻撃の防御・検知	・認証及びアクセス権の付与に係る方針及び規程等の策定、定期的見直し ・第三者による不正行為を阻止するための仕組みや取組みの活用[12] ・経営陣を含む全ての役職員に対する教育・研修の定期的な実施 ・インシデント対応及び復旧計画における役割及び運用手順に関する教育・研修の、関係する役職員に対する定期的な実施 ・情報の重要度に応じたデータ分類とその保護（適切な暗号化、認証、秘匿化、アクセス制御等） ・システム及び情報の重要度に応じたバックアップ要件等を含むバックアップに関する規程等の整備・実装 ・ログの取得・監視・保存のための手続の策定、定期的レビュー[13] ・サービスの企画・設計段階でセキュリティ要件を組み込むこと（セキュリティ・バイ・デザイン） ・サイバー攻撃の端緒の検知のための監視[14]・分析・報告に係る手続等の策定、見直し	・DLP[15]の導入 ・安全な開発手法を製品開発に取り入れている事業者から提供される安全なプロダクトを選定すること ・サプライチェーンのリスク評価において、ハードウェアに関するサイバーセキュリティリスクを評価対象とすること ・ハードウェアの調達基準にセキュアな調達のための基準を設けること ・DDoS/DoS 攻撃対策、DNS 対策、代替通信経路の制御 ・開発環境及びテスト環境の本番環境からの分離 ・ネットワークセグメントの細分化によるマルウェアの水平移動の阻止 ・攻撃の初期段階検知のための仕組み（おとりアカウントやサーバの利用）の導入 ・常時監視 ・SIEM[16]等を活用した分析

[6] パブコメ回答 9 番にて、一般論として、ゼロトラストは、防御、検知に限らず推奨されているとされている。
[7] パブコメ回答 142 番にて、状況に応じて、CISO といった然るべき責任者による承認を想定しているとされている。
[8] 金融分野ガイドライン脚注 26 において、自組織として業務運営上重要と認識しているサードパーティと定義されている。
[9] パブコメ回答 155 番にて、定期的に実施としているが、一律の頻度は示さないとされている。
[10] パブコメ回答 168 番にて、具体的な最低頻度は示さないとされている。
[12] パブコメ回答 180 番、181 番にて、フィッシングによるものとみられる不正送金の被害が増加していることを踏まえ、送信ドメイン認証を計画的に導入することが重要とされている。
[13] パブコメ回答 184 番にて、バックアップの期間や頻度、ログの保存期間等について、金融機関等で定義すべきと回答されているが、特定非営利活動法人日本セキュリティ監査協会「サイバーセキュリティ対策マネジメントガイドライン Ver2.0」において、ログの保存期間は 1 年以上とすることが望ましいとされている旨付言されている。
[14] 金融分野ガイドラインによれば、監視の対象にはクラウドサービスの責任分界に応じて当該サービスも含めること、クラウド事業者のシステム監視状況を同事業者から提供されるレポート等により確認することも監視にあたるとされている。
[15] DLP(Data Loss Prevention)とは、機密情報等を特定し、監視・保護するツールのこと。
[16] SIEM(Security Information and Event Management)とは、ファイアウォールや IDS/IPS、プロキシ等から出力されるログやデータを一元的に集約し、それらのデータを組み合わせて相関分析を行うことにより、ネットワークの監視やサイバー攻撃やマルウェア感染等のインシデントを検知することを目的とするツールのこと。

サイバーインシデント対応及び復旧	・インシデント対応計画及びコンティンジェンシープランの、サイバー攻撃の種別ごとの策定 ・他機関にとっても有効となる攻撃技術情報について、機密情報を除いた上で、必要に応じ、金融ISACやJPCERT/CC等の情報共有機関に共有すること[17] ・実際の封じ込めに当たって、情報漏えいによる再発及び二次的被害の可能性が危惧される場合には、発生を防ぐための対策を実施すること	・大規模な被害が生じるサイバーインシデントに対応するためのコンティンジェンシープランの整備 ・封じ込めの際に、対応によって影響の生じる可能性のあるサードパーティに適切に通知を行うこと[18]
サードパーティリスク管理	・サードパーティを管理するための台帳等の整備・維持 ・サードパーティのデューデリジェンスの実施 ・サイバーセキュリティに関する事項をサードパーティとの契約等に定めること	・重要なサードパーティがそのサードパーティを管理する能力、サプライチェーンリスク、集中リスク等の定期的なモニタリング ・重要なサードパーティの事業撤退、業務停止、契約関係の終了等への備え

Ⅲ. 金融機関等における対応

上記のとおり、金融分野ガイドラインは、「基本的な対応事項」を金融機関等が一般的に実施する必要のある基礎的な事項としており、社内の管理態勢の整備や見直し（特に、少なくとも１年に１回見直すとされている項目について前回見直しから期間が経過していないか）の確認が必要になると思われます。また、サードパーティとの間では、セキュリティ要件に関する事項や教育・研修の実施について契約を見直すことが必要になることも想定されます。

他方、「基本的な対応事項」と「対応が望ましい事項」のいずれについても一律の対応を求めるものではなく、金融機関等が、自らを取り巻く事業環境、経営戦略及びリスクの許容度等を踏まえた上で、サイバーセキュリティリスクを特定、評価し、リスクに見合った低減措置を講ずること（いわゆる「リスクベース・アプローチ」を採ること）が求められるとされています[19]。このため、サイバーセキュリティリスクの特定・評価、「基本的な対応事項」と「対応が望ましい事項」の対応状況を確認した上で、新たに実施するべき事項を決めていくことが必要になると思われます。

なお、リスク評価について、少なくとも１年に１回、それに加えて重大な脅威や脆弱性が判明した場合や新規商品又はサービスの提供時に行うことが「基本的な対応事項」とされていることもあり、一度リスク評価を行ってリスク対応を決めたとしても、その後の時間の経過や状況の変化に応じて見直しを行うことも必要になると思われます。

---

[17] 金融分野ガイドラインでは、参考として、内閣サイバーセキュリティセンター「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和５年３月８日）が挙げられている。

[18] 金融分野ガイドラインでは、金融情報システムセンター「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書（第４版）」（令和６年１月）を参照するようにとされている。

[19] パブコメ回答 13 番、32 番等では、検査・モニタリングでの対応や行政処分の対象となるかについて、一般論として、行政上の対応は、個別・具体的な状況に応じて検討すべきものとの回答がされている。また、パブコメ回答 22 番では、金融庁が金融機関等に対して実施を求めているサイバーセキュリティセルフアセスメントについて、金融分野ガイドラインと整合させる形で自己点検票の見直しを行う予定とされている。

セミナー情報

- セミナー　『サイバーセキュリティへの脅威とインシデント対応の法律実務～ケースを元に具体的な対応を解説～』
  - 開催日時　2024 年 11 月 5 日（火）10:00～12:00
  - 講師　蔦 大輔
  - 主催　株式会社金融財務研究会

- セミナー　『第 4 回 NIKKEI Privacy Conference～ユーザー目線を意識したプライバシー施策とテック～』
  - 開催日時　2024 年 11 月 7 日（木）13:00～16:45
  - 講師　岡田 淳
  - 主催　NIKKEI Privacy Conference 事務局

- セミナー　『【司法試験受験生・ロースクール生／若手弁護士対象・無料】サイバーセキュリティ分野の最前線を走る 3 名の弁護士が解説する、新規分野を切り拓く方法』
  - 開催日時　2024 年 11 月 28 日（木）17:00～18:00
  - 講師　蔦 大輔
  - 主催　Business & Law 合同会社

- セミナー　『日本 DPO 協会 第 33 回個人情報保護セミナー「プライバシーとテクノロジーをめぐる議論の現在地」』
  - 開催日時　2024 年 11 月 28 日（木）15:00～16:00
  - 講師　岡田 淳
  - 主催　一般社団法人日本 DPO 協会

文献情報

- 論文　「〈特集 1〉サイバーセキュリティ サイバーセキュリティ法制の概観と課題」
  - 掲載誌　ジュリスト No.1599
  - 著者　蔦 大輔（単著）

- 論文　「Japan's DPA publishes interim summary of amendments to data protection regulations」
  - 掲載誌　International Association of Privacy Professionals (IAPP)
  - 著者　田中 浩之、塩崎 耕平（共著）

- 論文　「クロスセクター・サイバーセキュリティ法（第 9 回）サイバーセキュリティ×危機管理―外部からのサイバー攻撃を念頭に」
  掲載誌　NBL No.1270
  著者　山内 洋嗣、蔦 大輔、今泉 憲人、門田 航希（共著）

- 論文　「Data Localization Laws: Overview (Japan)」
  掲載誌　Practical Law
  著者　田中 浩之、蔦 大輔、嶋村 直登（共著）

- 論文　「なりすまし・不正ログインの犯人への法的措置と当局への報告等」
  掲載誌　UNITIS
  著者　蔦 大輔、嶋村 直登（共著）

- 論文　「〈特集 経済安全保障のゆくえ〉基幹インフラ審査制度―サプライチェーン・サイバーセキュリティ」
  掲載誌　ジュリスト No.1601
  著者　蔦 大輔、新井 雄也（共著）

- 論文　「〈特集 通常国会で制定・改正された重要法律～そのポイントと実務への影響～〉セキュリティ・クリアランス制度創設とその背景―民間企業に何が求められるか」
  掲載誌　会社法務 A2Z No.208
  著者　梅津 英明、蔦 大輔、滝口 浩平、新井 雄也（共著）

- 論文　「対話で理解する」「学びを実務へ」情報管理のエッセンス（1）情報管理に係る法令の全体像」
  掲載誌　会社法務 A2Z No.208
  著者　田中 浩之、蔦 大輔、北山 昇、塩崎 耕平（共著）

- 論文　「個人情報保護法の次回改正に向けた中間整理に見る、漏えい等対応の実務上の課題」
  掲載誌　UNITIS
  著者　蔦 大輔（単著）

NEWS

- 蔦 大輔 弁護士のインタビューが、UNITIS の『ランサムウェア身代金は払っていいのか？ 法令や判断基準、事前策を弁護士が解説』と題した記事に掲載されました

- 蔦 大輔 弁護士のインタビューが、UNITIS の『ダークウェブに流出した情報の取得・拡散は違法？ 抵触する法律や企業の対応策を弁護士が解説』と題した記事に掲載されました

- 蔦 大輔 弁護士のインタビューが、UNITIS の『ランサムウェア被害時にとるべき初動・広報対応を弁護士が解説』と題した記事に掲載されました

- 増田 雅史 弁護士が NFT 部会 法律顧問として策定に関与した「NFT ビジネスに関するガイドライン 第 3 版」が、一般社団法人日本暗号資産ビジネス協会（JCBA）より公表されました

- 【重要】当事務所または当事務所の弁護士・スタッフ名を騙った詐欺にご注意ください

  世当事務所を騙り出会い系詐欺などの被害相談を受けると宣伝するウェブサイトが確認されました。当事務所は、このようなウェブサイトに一切関係がございません。ウェブサイト記載の連絡先に連絡することのないようお願い申し上げます。

  また、当事務所の弁護士名を騙り被害弁償をする等の電話やメールを送っている事例が確認されました。当事務所は、このような事件には一切関係がございません。

  当事務所または当事務所の弁護士・スタッフ名を名乗る者からのお心当たりのない連絡を受けた場合は、すぐには応じず、相手の身元を十分にご確認ください。また、併せて下記連絡先までお知らせくださいますようお願い申し上げます。

  なお、当事務所の弁護士が、連絡を差し上げた事案について、当事務所の他の弁護士・秘書・スタッフ、他のオフィスなどには連絡しないように伝えることはありません。
  そのようなことを伝えられた場合は、基本的に詐欺であるとご理解下さい。

  森・濱田松本法律事務所
  Tel: 03-5220-1800（総合案内）（9 時 00 分～17 時 00 分）
  E-mail: mhm_info@mhm-global.com

➢ 横浜オフィス業務開始のお知らせ

横浜オフィスは、弁護士法人森・濱田松本法律事務所の従事務所として、2024 年 8 月 19 日より、正式に業務を開始いたしました。

横浜オフィスには、コーポレート・ガバナンスを含めた会社法全般、スタートアップ支援、M&A、訴訟・紛争等の分野において豊富な経験を有する河島 勇太 弁護士及び髙津 洸至 弁護士が所属し、東京オフィスをはじめとする他の国内拠点に加えて、クロスボーダーの M&A やアジア進出などの業務につきましては、ニューヨーク・北京・上海・シンガポール・バンコク・ホーチミン・ハノイ・ジャカルタ・ヤンゴン・マニラの各海外拠点及び提携事務所、当事務所所属の弁護士が滞在する各国の法律事務所と密に連携し、神奈川県のクライアントの皆様の近くで、きめ細やかに最先端のリーガル・サポートを提供してまいります。

➢ AI 法務プラットフォーム「LegalOn Cloud」における「MORI HAMADA ライブラリー」提供開始のお知らせ

森・濱田松本法律事務所（以下「MHM」）は、株式会社 LegalOn Technologies（本社：東京都渋谷区 代表取締役 執行役員・CEO：角田望、以下「LegalOn Technologies 社」）が提供する、法務業務全体を包括的に支援する AI 法務プラットフォーム「LegalOn Cloud」において MHM が作成する法務コンテンツを搭載した「MORI HAMADA ライブラリー」の提供を 9 月 12 日より開始したことをお知らせいたします。

LegalOn Cloud において MHM が提供する「MORI HAMADA ライブラリー」では、まずは、M&A や国際取引に関するひな形、各種会社法関連書類、それらに付随する解説記事などの法務コンテンツを搭載する予定です。M&A 関連や国際取引などのより複雑かつ高い専門性が求められる案件について、必要な書式・解説を提供することで企業法務を支援いたします。これにより、複雑かつ専門性の高い案件での適切な契約リスクのコントロールや、スピード感のある対応を支援できるものと考えております。

MHM はクライアントの皆さまに対し、今後も業務に役立つ実用的な法務コンテンツを提供し、企業法務の支援を行ってまいります。

➢ 法律業界向けの生成 AI に関する Harvey 社とのパートナーシップについて

森・濱田松本法律事務所（以下「MHM」）は、法律業界向け生成 AI ソリューションのグローバル・プラットフォームとして業界をリードする Harvey 社と提携することになりましたので、お知らせいたします。

本提携により、MHM は、日本における Harvey 社のオープンエンド API の独占的使用権、同社の革新的な新製品である Vault（生成 AI で強化された大規模データセットのレビュー機能）へのアクセス権、その他の同社のプラットフォームへのアクセス権を有することとなります。MHM は、アジアに本拠を置く Harvey 社の初めてのパートナーとなります。

当事務所のマネージングパートナーである飯田 耕一郎 弁護士のコメント：「当事務所は、法律業界をリードする生成 AI プラットフォームを提供している Harvey 社と戦略的パートナーシップを締結することで、更に、当事務所の業務における最先端のテクノロジーの利活用を推進する所存です。国内外の拠点において AI の利活用を進めることにより、当事務所のリーガル・サービスを強化し、クライアントの皆様に更なる付加価値を提供して参ります。Harvey 社との協業を通じて、AI の利活用の更なる可能性を追求することを楽しみにしております。」

Harvey 社の CEO である Winston Weinberg 氏のコメント：「MHM との提携は、当社にとって、日本及びアジアに進出する重要な一歩となります。このパートナーシップは、卓越性、革新性、顧客重視のサービスという共通の価値観の上に成り立っています。MHM の信頼に感謝するとともに、日本及びアジアにおいて AI を活用した優れたリーガル・ソリューションを提供するために協力できることを楽しみにしています。」

MHM は、Harvey 社とのパートナーシップを通じて、地域、業務、言語を問わず、文書レビュー、デューデリジェンス、調査業務等において、生成 AI の活用を更に推進し、クライアントの皆様に対し、より一層質の高い法務サービスを提供することができるよう目指して参ります。