Legal Wire

pillsbury

Japan Practice

Vol. 27 / November 2016

ニューヨーク州、多くの課題をもたらすサイバーセキュリティの規則を発表

奈良房永（日本語版監修）

ブライアン・E・フィンチ、メルセデス・K・タンストル

広範な調査と検討を経て、ニューヨーク州金融サービス局（New York State Department of Financial Services、以下「DFS」）は金融機関（銀行、証券、保険会社など）に対するほぼ最終版のサイバーセキュリティ要件（Cybersecurity Requirements for Financial Service Companies）を発表しました。この DFS サイバーセキュリティ規則は適用範囲が非常に広範囲であるため、今後金融機関が運用の安全性を図る上で重大な影響を及ぼすことになるでしょう。

この DFS サイバーセキュリティー規則を正しく履行するのは並大抵のことではないでしょう。この規則では、広く知られているものから比較的特異なものまで、サイバーセキュリティに関わるさまざまな社内規則と運用ルールの実行が規定されています。また、対象となる組織は取引関係のある第三者に対してもほぼ同レベルの厳格なサイバーセキュリティコントロールを求めることとされており、その点も負担となるでしょう。さらに、対象企業の取締役および役員は、この規則を会社が遵守していることを毎年保証するよう求められています。このように、今回のサイバーセキュリティ規則は、精査の対象となることが容易に予想できるでしょう。

本稿では DFS サイバーセキュリティー規則について、どのような取引先や業者が規制の対象となるか、現状の規則で詳細が説明されていない点は何か、民事責任となり得る問題を回避しつつ法人としてこの規則を遵守するためにとるべき方策は何か、といった点を明らかにしていきます。

I. DFS サイバーセキュリティー規則の概要

DFS が今回発表したサイバーセキュリティ規則は、これまでで最も包括的かつ大がかりな内容となっています。2017 年より、対象となる企業は、広範囲にわたるサイバーセキュリティ計画および方針の設定、トレーニング体制、リスク分析と脆弱性評価、事故対応能力、およびその他の管理体制を構築することを求められています。さらにこの規則はサイバーセキュリティに関する方針、手順そしてさまざまなテスト計画と評価を定期的に行い、更新するよう求めています。要するに、この規則は対象となる 2000 近い企業に対して、これまでになかった重要な（そして費用がかかるであろう）義務を課すものです。

この規制は対象となる組織を銀行法、保険法または金融サービス法に基づいて、免許、登録、設立、認証、許可、認可などを受けて運用されているすべての法人、と定義しています。但し、過去 3 年につき、顧客数が平均 1000 人以下、年間総所得が各年 500 万ドル以下、年度末総資産が 1000 万ドル以下の場合は、適用対象外となっています。

この規則では次のような要件を満たさなければなりません。

- 情報システムと非公開情報（業務に関連するすべての情報、対象組織が受け取った情報、ヘルスケア情報、および個人を特定する情報）を保護するため、明文化されたサイバーセキュリティ計画を作成して実行すること。この規則特有のサイバーセキュリティ計画の項目として次のものを含む。
    - 容量と処理効率計画
    - システム運用と稼働率に関する懸念
    - システムとネットワークのセキュリティーとその監視
    - システムとアプリケーションの開発とその品質保証
    - 警備・施錠設備および空調設備
    - 納入業者および第三者プロバイダーの管理
- サイバーセキュリティ計画全体について、年に最低一度は取締役会（またはそれに同等の経営組織）で見直した上で、上級幹部役員による承認を受けなければならない。
- 事故対応計画を作成し実行する。
- 最高情報セキュリティー責任者（CISO）を設け、半年に1度、会社のサイバーセキュリティの全体的状況を、取締役会またはこれに同等する場に報告しなければならない。
- 対象組織はサイバーセキュリティ担当者を雇うか、「資格のある第三者を利用して要件を満たす」ようにしなければならない。
- 年に1度の侵入テストとリスク評価に加え、四半期毎の脆弱性評価と定期的な訓練を実施しなければならない。
- サイバーセキュリティの監査記録は少なくとも 6 年保管しなければならない。
- サイバーセキュリティ計画は、アプリケーションソフトやアプリについてセキュリティ対策を施すものでなければならない。
- 取引関係にある第三者のサイバーセキュリティ方針と手続きは、正式に記録として残さなければならない。第三者のセキュリティー方針は、最低限次の要件を満たさなければならない。
    - 第三者取引先のサイバーセキュリティのリスク評価
    - 第三者取引先が従うべきサイバーセキュリティ手順を特定し、これを遵守しているかについてのデューデリジェンス

- 第三者取引先セキュリティ対策の年次見直しと評価
- 第三者取引先との契約には下記項目を含むこと
  - マルチファクター認証の採用
  - 暗号化
  - サイバーセキュリティ事故発生時の即時通報
  - 第三者取引先のサイバーセキュリティ体制に対する監査を実行する権利
  - 第三者取引先から規制対象組織に提供されるサービスと製品がサイバーセキュリティの脅威に対応している旨の、当該第三者による表明保証
  - システムとアプリケーション開発およびその品質保証
  - 警備・施錠設備および空調設備
- 「サイバーセキュリティ事故」（既遂、未遂に関わらず、また成功・不成功に関わらず、情報システムおよびそのシステムに保存されているデータに対する不正なアクセス、妨害、不正操作と定義される）は、その発生から 72 時間以内に DFS に報告されなければいけない。（下線強調は著者による）

この規則は 180 日の猶予期間を設けていますが、規制対象組織は 2018 年 1 月 15 日以降、DFS 局長宛てに「遵守保証書」を提出しなければなりません。

II. 疑問点と懸念

この規則は「常識的な」サイバーセキュリティ対策で構成されているとみることも可能でしょう。この規則のうち、その多くは納得できるものである一方、規制対象組織にとっての難題は、規則によって課せられる義務が非常に細かいものからきわめて曖昧なものまである点です。以下にこの規則に関わる疑問点の例をいくつかあげましょう。

①「サイバーセキュリティ事故」の定義があまりにも広い

上に述べたように、この規制はサイバーセキュリティ事故を「既遂、未遂に関わらず、また成功・不成功に関わらず」、情報システムおよびそのシステムに保存されているデータに対する不正なアクセス、妨害、不正操作と定義しています。そのような事故が起きた場合、その発生から 72 時間以内に DFS に報告されなければなりません。

一読する限り、どれほど下手に計画され実行されたかにかかわらず、ほとんどすべてのサイバーアタックが「サイバーセキュリティ事故」に当てはまります。規制上報告義務の対象となる、実質的にシステムに影響を及ぼす「合理的な可能性」がどのような場合に認められるかについては何の説明もなく、DFS が非常に広範でかつ随意な「合理的」という定義を前提としていることは容易に想像できます。

規制対象組織は、（そうでないと証明されるまでは）何がサイバーセキュリティ事故にあたるかという点について、DFS が極めて広義に判断する傾向が強いことを前提としなければなりません。組織によっては日々何十万回（もしかすると何百万回）もサイバーアタックの標的になる場合があり、その通知を行うこと自体が会社にとって重い負担となる可能性があります。

② 第三者取引先のサイバーセキュリティ規則遵守に責任を持つことはほとんど不可能

納入業者・第三者取引先の安全対策は、すべてのセキュリティプログラムにとっても重要な点であり、DSF がここを指摘するのは当然でしょう。しかし、規制対象組織が第三者取引先のサイバーセキュリティに関して負う義務は非常に重く、金融機関がこの責任を全うすることは、現実的には困難と思われます。特に、大規模な取引先が相手である場合、この規則の要求項目のすべてを満たすことは難しいでしょう。

第三者取引先の安全対策で最も厄介な項目は 500.11(b)(5)条です。同条は、規制対象組織が、サービス提供者である第三者から「規制対象組織に提供するサービスと製品は、対象会社の情報システムまたは非公開情報を害するサイバーセキュリティの脅威に対応していることの表明と保証」を取り付けなければならない、という要件です。

そのような表明を取り付けることが難しいのは経験上明らかであり、またもしそのような表明を取得しても、意味のあることではないでしょう。それは、サイバーアタックが至るところで行われており、どんなシステムでも何らかのマルウェア（不正ソフトウェア）に侵されているのが当たり前になっているためです。FireEye 社などによる調査は、最も先進的な組織の情報システムであっても、何らかのマルウェアが稼働時間の 95%以上の確率で存在しているという状況を示しています。そのため 500.11(b)(5)条が求める表明に同意するような第三者としての取引先を探し出すことは極めて困難であり、そのような表明に対する信頼性も低下することとなります。

また、500.03(a)(10)条は「警備・施錠設備および空調設備」に関連する明文化された方針や手順にも注意が必要と定めている点にも留意する必要があります。これらのシステムを管理するのは規制対象組織ではなくビルの所有主なので、この要件も現実的には問題となります。規制対象組織は、どのようなサイバーセキュリティ方針と手順がこの条項の要件を満たすかを定めるだけではなく、第三者であるビルの所有主にそれを遵守させる方法を考え出さなければなりません。規制対象組織とビルの所有主の間で、この規則の実施にあたって発生する多額の改修費用をどちらが負担するか、深刻なもめ事の原因とになるでしょう。

③ 規則の「情報システム」の定義に問題あり

DFS のサイバーセキュリティ規則における「情報システム」の定義は、「電子情報を収集、処理、保守、使用、分配、普及そして売却するために接続された電子情報機器群、また工業／加工制御システム、電話交換および構内交換システムそして空調コントロールシステム」を含みます。

長文の定義ですが、どこまでこの規則の対象となるかは不明瞭です。例えば、規制対象会社はビデオ会議システム、文書管理プログラム、外付け記憶装置を情報システムの一部とみなすべきでしょうか。次第にこれらの点が明らかになっていくでしょうが、より明確な説明が必要であることに間違いありません。

④ 内部調達あるいは外部委託

規制対象組織の多くは、内部の人員を使って大部分これに対応できるでしょう。一部の規制対象組織は、外部のサポートを求めることにより自社のリスクの一部を軽減できるかもしれません。選択の余地なく、サイバーセキュリティ計画を設計、実施するために、外部のサービス提供会社に全面的に委託せざるを得ない規制対象組織もあるでしょう。これは、DFS が承認するサイバーセキュリティ計画を策定するための能力が社内にない、これを育てる時間がない、といったケースにおいて考えられます。

いずれの場合も、規制対象組織にとっての課題は、セキュリティ計画をどこに頼むかという判断のみでなく、そうすることにより DFS の基準を満たすことができるかという難しい問題への対応です。なぜならばサイバーセキュリティのサービス提供会社は数多くありますが、その実効性を判断する手段は少ないからです。さらに、サイバーセキュリティで評判の良い会社には依頼が殺到し、コストと納期に問題が生じる可能性があります。

規制対象組織で外部業者の利用を考えている場合は、どの部分を組織内で行い、どの部分を外部に委託するのかとの判断を即座に始めるべきでしょう。また、入札と調達に関する厳格な手順を作成し、契約締結の全過程においてその手順のとおり手続きが行われたことを示す記録を保存しておくべきです。

⑤ 取締役と幹部役員にとっての懸念

取締役会で会社のサイバーセキュリティ計画をレビューしなければならないというのは、珍しいことではなく、実際に多くの取締役会でこれを実行しており、特別委員会やサイバーセキュリティに関する専門知識を持った役員を加えているところもあるほどです。最高情報セキュリティー責任者（CISO）や最高情報責任者（CIO）がトップ経営者会議やサイバーセキュリティに関する取締役会で定期的に報告することもごく一般的になってきており、法務部長や経営最高責任者がサイバーセキュリティ計画の作成に関わることもあります。

しかし、この規制の要件が規制対象組織のサイバーセキュリティ計画の設計と実施に影響を与える可能性があります。つまり、この規制により、取締役や幹部は、単に規制を遵守する計画の策定のみではなく、策定する計画が DFS の定める不明瞭な基準を充足するかどうか、さらにその計画が「妥当かつ充分」であるかどうかを検討すべき立場におかれることとなります。問題は、サイバーセキュリティ計画が「妥当」または「充分」であるかどうかを定める基準が、ほとんど皆無に近い状況にあることです。特に問題なのは、完璧なサイバーセキュリティを備えることができるという前提に基づいている点です。完璧なサイバーセキュリティは存在しないため、取締役や幹部役員は、DFS に対して何らかの表明をする前に、自らの組織のセキュリティー計画が技術的かつ法的に堅固なものであることを確実するべきです。

III. DFS のサイバーセキュリティ規制の遵守をし易くするために安全法（SAFETY ACT）を活用

DFS のサイバーセキュリティ規則が多くの面で曖昧である一方で、規制対象組織が包括的なサイバーセキュリティ計画を有していることを示す手段はすでに存在します。それは安全法（SAFETY Act）です。安全法（Support Anti-terrorism by Fostering Effective Technologies Act: 効果的技術促進による反テロリズム支援法）は、賠償責任を管理するための法律で、2002 年国家安全保障法の一部として成立したものです。

安全法の下では、サイバーセキュリティ製品やサービスまたは方針／計画を、所持、販売または設置する会社（自らのサイバーセキュリティ方針と計画を策定する会社を含む）が、連邦国土安全保障省に対して、民事訴訟における損害賠償の上限や免責など、特定の責任を制限することを申請することができます。安全法による保護は、当該セキュリティープログラムとその方針が、現実的、効果的であり、有効な品質保証を伴っていると認めた場合にのみ、国土安全保障省によって与えられます。審査は徹底しており、認可された保護は通常 5 年間有効です。

DFS 規則（または他の法律）に基づいて設定されるプログラムや実行手順のすべては、国土安全保障省により安全法の保護を目的とした評価を受ける可能性があります。即ち、規制対象組織が

設定した自社のサイバーセキュリティ計画、トレーニング計画、危機評価、さらには第三者サービス提供会社の選定過程についても、安全法の保護を得ることが可能になるということです。規制対象組織が安全法に基づいた保護を得ている場合には、DFS 規則により義務付けられている計画と方針を実際に合理的に実行し堅固な遵守計画に基づいて継続的に更新しているという、強力な証拠になります。何故ならこれらの事項は安全法の保護を受ける為に必須の項目でもあるからです。

安全法の保護を受けていても、DFS 規則の法的責任が免除されるわけではないことに留意しなければなりません。安全法は、これに基づく保護をそのような目的のために使用することを、明確に禁止しています。ただ、DFS は各組織のサイバーセキュリティプログラムの有効性の根拠を問い質してくるでしょうから、そのような場合規制対象組織が安全法で認められたサイバーセキュリティ計画を有していると示すことがどれだけ強力な後ろ盾となるかということは、一考に価します。

IV. DFS サイバーセキュリティ規則は今後長期にわたる課題

ニューヨークのサイバーセキュリティ規制は、今後修正・変更されることは間違いないでしょう。また、他の州も似たような規制を設定することが予想されます。このため規制対象組織は、既存の情報漏洩通知義務と同様に、州ごとに異なる規制に対応しなければならないことになります。

DFS の要件はなくなりはしません。規制の対象となる企業は、なるべく早く遵守計画策定の準備を始めるべきでしょう。そしてこの分野の専門弁護士と密に協力し、自社が妥当なサイバーセキュリティプログラムの設定していることを示せるように準備し、十分で包括的なサイバーセキュリティプログラムのさらなる証拠として安全法が役立つものとなっているかどうかの見直しを行うことをお勧めします。

本稿の内容に関する連絡先

奈良房永
1540 Broadway
New York, NY 10036-4039
212.858.1187
fusae.nara@pillsburylaw.com

Brian E. Finch
1200 Seventeenth Street, NW
Washington, DC 20036
202.663.8062
brian.finch@pillsburylaw.com

Mercedes K. Tunstall
1200 Seventeenth Street, NW
Washington, DC 20036
202.663.8118
mercedes.tunstall@pillsburylaw.com

Legal Wire 配信に関するお問い合わせ

古在 綾
Japan Practice Program Administrator
akozai@pillsburylaw.com