information

# 米国における サイバー攻撃 対策義務の動向

**近時、サイバー攻撃対策の重要性が叫ばれる中、米国では最近具体的な指針および法案が公表され、注目を集めている。**


デビボイス・アンド・プリンプトン
ワシントンDC・デラウエア州弁護士
ルーク・デムボスキー

ニューヨーク州弁護士
ジム・パストーレ

弁護士・ニューヨーク州弁護士
青山 直美


制作／レクシスネクシス・ジャパン広告出版部

## ランサムウェアに関する指針

米国保健福祉省（DHHS）は、2016年7月にランサムウェア（身代金要求型コンピュータウィルス）に関する指針を発表した。この指針は、ランサムウェアによる攻撃を受けることを防止するために採るべき対策と、攻撃を受けてしまった際に必要な対処の仕方を定めており、ヘルスケア業界を対象とするものであるが、他の業界においても大いに参考とすべきもとなっている。対策として有効と考えられるのみならず、他業を管轄する当局もDHHSの見解に習う可能性が高いからである。

ランサムウェアに感染すると、コンピュータに保存されたデータにアクセスできなくなり、データを回復したければ金銭（身代金＝ransom）を支払うよう要求するメッセージが表示される。メールに添付されたファイルやリンクをクリックすることで感染するケースが多い。2016年に入って世界中で毎日4000件ものランサムウェア攻撃が行われているといわれており、前年比3倍増の件数である。

要求される金額は比較的小さいことが多く、支払いをすればデータへのアクセスを回復できることが多いようである。中には、まるでインターネット通販業者のように、事後に被害者にアンケートへの回答を求め、約束どおりきちんとデータを回復する「信頼のおける」ハッカーであるという口コミ評価を発表している者までいるという。しかし、最近は、より多額の金銭の支払いに応じることができそうであったりコンピュータシステムへの依存度の高かったりする者（大手の法律事務所や病院など）がターゲットとして選ばれ、被害に遭う傾向にあるという。

ランサムウェア攻撃は犯罪であることから、これまで被害者側がどうすべきであったかという側面には、あまり焦点が当たっていなかった。多くの州法では、一定の漏洩の事実があった場合に被害者への開示義務を定めているが、ランサムウェア攻撃を受けても個人情報等のデータが漏洩しなければ適用されないことが多い。また、米国連邦取引委員会はサイバーセキュリティ対策の不備が法律違反になり得るという立場をとっているが、これまでのところ、それを理由にランサムウェア攻撃を受けた被害者の責任を追及することはしていない。

しかし、今回の指針は、米国の医療保険の携行性と責任に関する法律（The Health Insurance Portability and Accountability Act：HIPPA）に基づく既存の安全規則の定めるサイバーセキュリティ対策が、次のとおりランサムウェアについても適用されることを明確にした。

①ランサムウェア被害時の対応および被害から回復するための指針・手続（例えば、頻繁なバックアップ、バックアップを使っての定期的な回復テスト、バックアップまでもが被害を受けることを防ぐためシステムから隔離しオフラインの状態にしておくこと

**Luke Dembosky**
16年初めまで米国司法省国家安全保障担当検事として、最先端のサイバーセキュリティ案件を数多く扱った経験を活かし、企業にアドバイスを行う。ワシントンDCオフィス所属。



に金融機関を対象としたサイバー攻撃対策に関する法案を発表した。金融機関の顧客を保護するための対策・対処義務を定めるものである。

この法案は連邦の銀行監督当局および連邦金融機関検査協議会（FFIEC）の示す方向と同一のところを目指すものであるが、既存の他の州レベルの規則よりもかなり充実し、規則として成立すれば金融機関にとっては遵守のハードルが上がることになろう。

FFIECのサイバーセキュリティ評価ツールや米国国立標準技術研究所のサイバーセキュリティ・フレームワークでは、企業が自ら行うリスク判断に従い対策を講じることを求め、各企業に裁量の余地を残しているのに対し、NYDFSの法案では、広範にわたる事項につき、採るべき技術的対策やガバナンスのルールを具体的に細かく定めている。今後、連邦および他の州当局が同様の規制を導入する際には、この法案が参考にされると思われるため、注視が必要である。

この法案は、ニューヨーク州で金融サービス業法の規制対象となる法人（銀行、保険会社等）の義務を定めるが、顧客数が3年間1000未満のもの、年間総収入が3年間500万ドル未満のもの、年度末の総資産（関連会社の資産を含む）が1000万ドル未満のものには適用がない。

保護の対象には、業務・営業上の情報、顧客の個人情報など非公表の情報がすべて含まれる。情報保護に関する多くの法令が個人を特定できる情報のみを対象としているのとは大きく異なる。

具体的な義務として定められているものをいくつか挙げると次のとおりである。

**Naomi Aoyama**
91年東京大学法学部卒業。94年弁護士登録。99年シカゴ大学ロースクール修士号（LL.M.）取得。99年よりニューヨークオフィスにてM&A、合弁案件等に従事。15年に帰国し、東京オフィスを開設。

**●通報義務**
通常の営業に大きく影響する可能性があると合理的に判断される事象または非公表の事実に影響を与える事象を発見してから、72時間以内にNYDFSに通報しなければならない。72時間というのは、これまでにない迅速性を要求するものである。

**●毎年の報告**
この規則を遵守していることを毎年報告しなければならない。

**●対策計画の策定**
保護すべき情報を特定し、アクセス権、非常事態への対処、モニタリング等14の項目についての方針を定めた総合的な計画を作成しなければならないのみならず、これを取締役会等が毎年見直さなければならない。

**●アクセス制限**
これまでも推奨されていた情報の暗号化、パスワード等の認証要件の複数化、アクセス権の制限と閲覧履歴の記録等を今後は義務とする。

**●取引先の管理**
取引先のサイバーセキュリティ対策の状態を確認したり、取引先に情報の暗号化や情報漏洩の通知義務などを負わせるための契約条項を用意したりしておかなければならない。

**Jim Pastore**
当事務所にて5年間知的財産権訴訟に携わった後、米国検察官としてコンピュータ犯罪の訴追等を5年間担当。14年ニューヨークオフィスに復帰。

## ニューヨーク州のサイバー規制法案

ニューヨーク州金融監督局（NYDFS）は2016年9月に金融機関を対象としたサイバー攻撃対策に関する法案を発表した。金融機関の顧客を保護するための対策・対処義務を定めるものである。

この法案は連邦の銀行監督当局および連邦金融機関検査協議会（FFIEC）の示す方向と同一のところを目指すものであるが、既存の他の州レベルの規則よりもかなり充実し、規則として成立すれば金融機関にとっては遵守のハードルが上がることになろう。

FFIECのサイバーセキュリティ評価ツールや米国国立標準技術研究所のサイバーセキュリティ・フレームワークでは、企業が自ら行うリスク判断に従い対策を講じることを求め、各企業に裁量の余地を残しているのに対し、NYDFSの法案では、広範にわたる事項につき、採るべき技術的対策やガバナンスのルールを具体的に細かく定めている。今後、連邦および他の州当局が同様の規制を導入する際には、この法案が参考にされると思われるため、注視が必要である。

この法案は、ニューヨーク州で金融サービス業法の規制対象となる法人（銀行、保険会社等）の義務を定めるが、顧客数が3年間1000未満のもの、年間総収入が3年間500万ドル未満のもの、年度末の総資産（関連会社の資産を含む）が1000万ドル未満のものには適用がない。

保護の対象には、業務・営業上の情報、顧客の個人情報など非公表の情報がすべて含まれる。情報保護に関する多くの法令が個人を特定できる情報のみを対象としているのとは大きく異なる。

具体的な義務として定められているものをいくつか挙げると次のとおりである。

**●通報義務**
通常の営業に大きく影響する可能性があると合理的に判断される事象または非公表の事実に影響を与える事象を発見してから、72時間以内にNYDFSに通報しなければならない。72時間というのは、これまでにない迅速性を要求するものである。

**●毎年の報告**
この規則を遵守していることを毎年報告しなければならない。

**●対策計画の策定**
保護すべき情報を特定し、アクセス権、非常事態への対処、モニタリング等14の項目についての方針を定めた総合的な計画を作成しなければならないのみならず、これを取締役会等が毎年見直さなければならない。

**●アクセス制限**
これまでも推奨されていた情報の暗号化、パスワード等の認証要件の複数化、アクセス権の制限と閲覧履歴の記録等を今後は義務とする。

**●取引先の管理**
取引先のサイバーセキュリティ対策の状態を確認したり、取引先に情報の暗号化や情報漏洩の通知義務などを負わせるための契約条項を用意したりしておかなければならない。