実務解説

米国M&Aにおけるサイバーセキュリティ，データプライバシーの実務

Mayer Brown LLP
ニューヨーク州弁護士　ジョゼフ・カステルチーオ
TMI総合法律事務所
弁護士・イリノイ州弁護士　田中健太郎

世界中でサイバーセキュリティおよびデータプライバシー（以下「サイバーセキュリティ等」という）に関する関心が強まっており，これらに関する議論が活発になされているが，日本では，M&Aの文脈においてこれらの問題点を中心に検討した論考は必ずしも多くないように思われる。サイバーセキュリティ等に関する問題は，小さな綻びが広範囲かつ壊滅的な被害を企業に及ぼすリスクを含んでいること等から，企業価値に大きな影響を与える可能性があるため，M&Aの文脈において，これらの問題を検討することの重要性が増してきている。

本稿では，米国実務をふまえ，M&Aにおけるサイバーセキュリティ等に係るリスクのうちいくつかのポイントを紹介するが，これらは日本においても当てはまる部分も多いことから，M&Aに関わる実務家にとっての一助になれば幸いである。

I M&Aにおける サイバーセキュリティ等の重要性

サイバーセキュリティはごく一部の企業にとっての問題に過ぎないと考えている方もいるかもしれないが，ハッカー等は，サイバー攻撃の対象になるとは考えられていない企業や対象にあえて攻撃することがあるため，あらゆる企業がサイバー攻撃のリスクに晒されているといえる。たとえば，ハッカー等は，企業情報そのものではなく，企業のインフラやシステムから利益を得ることを試みたり，複数の関連性のないネットワークを同時に攻撃し，それらを利用して，混乱を招き，情報搾取，金銭要求等を行うこともある。さらに，ハッカー等は，銀行口座等の機密性の高い企業情報にアクセスするための情報を取得するために，それほど機密性の高くないタイプのオンラインアカウント（ソーシャルメディアのアカウントを含む）を標的とすることもある。また，ハッカー等が付随的な被害が発生することを考慮していないため，直接的にサイバー攻撃の対象となっていなかったとしても，企業がサイバー攻撃の影響を付随的・間接的に受ける可能性もある[1]。そのため，すべての会社がサイバー攻撃の対象になり，またはサイバー攻撃の影響を受ける可能性があることから，あらゆるM&A取引において，サイバーセキュリティを検討項目に含めて考えるべきである。

[1] たとえば，歴史上最大規模のマルウェア攻撃の1つであるNotPetya攻撃は，当時ウクライナの大半の企業が利用していた税務・会計ソフトの欠陥を悪用したため，エネルギー会社から銀行，送電網といった広範な範囲に悪影響を及ぼした。

また，企業が収集・活用するデータの重要性が増していることから，M&A取引においても，個人情報を含むデータに適用される法令を正確に理解することが重要になってきている。 特に，さまざまな種類のデータを取り扱っている場合やデータを収集，使用もしくは保存している国が異なる場合には，関連する規制を正確に理解し，これに対応することは困難を要するため，デューデリジェンス（以下「DD」という）においてこれらの規制の遵守状況を把握する必要がある。

以上のとおり，サイバーセキュリティ等の問題は，ITまたはセキュリティチームによる検討事項にとどまらず，企業価値に重大な影響を与える可能性があることから，取締役会，経営戦略部およびM&Aの担当部署において，M&A取引を実施するに際して当該リスク分析の優先順位を高めて検討する必要がある。

Ⅱ チェックポイント

1 コンプライアンス・プログラム

(1) 重要性

サイバーセキュリティ等に関する規制は多数存在するが，絶えず進化し，一部規制内容が重複し，ときには矛盾することもあることから，それらの規制内容を正確に理解することは必ずしも容易ではない。また，その規制対象が極めて広範な範囲におよび，違反時に高額な罰則が科されることもある。たとえば，欧州一般データ保護規則（General Data Protection Regulation，以下「GDPR」という）は，世界中の企業に，GDPRに準拠したコンプライアンス・プログラムの実施を要求しているが，仮にこれらの企業がGDPRに違反した場合には，１件当たり全世界収益の最大４％または20,000,000ユーロのうち高額な罰金が科される可能性がある[2]。

GDPRおよび同種の規制を遵守するためには，充実したコンプライアンス・プログラムが欠かせないが，当該コンプライアンス・プログラムは，M&Aを成功させるうえでも非常に重要である。具体的には，対象会社の不十分なコンプライアンス・プログラムが多額の罰則につながるだけでなく，企業の成長を鈍化させ，シナジーの喪失や取引の基礎となった前提を覆す事態を生じさせる等，M&Aに対して重大な悪影響を与える可能性があることから，検討する必要性が高い。

(2) 買主のコンプライアンス・プログラムの適用

買主が，充実したコンプライアンス・プログラムを有し，GDPRやその他の規制に積極的に取り組んでいる場合には，既存のコンプライアンス・プログラムを対象会社にそのまま適用すれば足りると思われるかもしれないが，以下のような理由から，このような単純な対応では不十分なものとなるおそれがある。

- 対象会社のシステムが，買主のコンプライアンス・プログラムのもとで機能しない可能性。
- 対象会社が，買主が現在事業を行っていない国または法域で事業を営んでいる結果，買主に現在適用されている規制よりもより強力な規制を遵守しないといけない可能性。
- 買主のコンプライアンス・プログラムは，対象会社の事業内容に鑑みて，適切な規模に調整する必要が生じる可能性[3]。
- 対象会社のコンプライアンス・プログラムに買主が自社のものに取り入れたいと考える点が含まれている可能性。

(3) DD

このような買主と対象会社のコンプライア

[2] そのほかにも，California Consumer Privacy Act of 2018等の規制があげられる。

[3] なお，このようなコンプライアンス・プログラムの更新・調整は定期的に行われるが，M&Aの文脈では，M&A取引およびその後の統合計画の一部として，他の改訂事項とあわせて検討されるべきである。

ンス・プログラムの齟齬に対応するために，買主は，潜在的なリスクをDDの過程で顕出し，特定する必要がある。

スケジュールの関係等からDDにおいてすべての項目を調査することが実務上困難または不可能な場合もあるが，そのような場合であっても，たとえば以下のような重要事項については確認・検討すべきである。

- 対象会社に存在するプライバシーポリシーやコンプライアンス・プログラムの基本的な水準の調査。
- プライバシーポリシーやコンプライアンス・プログラムを主に管轄する部署の担当責任者（コンプライアンス担当役員や，情報セキュリティ担当役員等）が存在するか，存在する場合にどの程度の経験を有する者かの調査。
- 関連するすべての法域において，最新の法令に沿っていない，または法令遵守を無視したプラクティスまたはコンプライアンス・プログラムの有無・内容の調査（買主および対象会社の事業拠点がある場所に限られない）。
- 対象会社のコンプライアンス内で矛盾するプラクティスおよび買主と対象会社のコンプライアンス・プログラムで矛盾するプラクティスの有無・内容の調査。
- コンプライアンス・プログラムに遵守した取扱いがなされているかの調査[4]。

これらのリスクは，コストを発生させるだけでなく，取引の遅延を生じさせ，スケジュール全体のなかで重要なマイルストーンの達成に悪影響を与える可能性がある。そのため，買主は，早い段階からこれらの項目についての調査に着手し，潜在的なリスクの有無・内容を把握することが重要である。そして，買主は，これらの項目に関するDDの結果をふまえて，統合計画を作成するに際して，予期せぬ遅延が生じないように留意する必要がある。

2 データプライバシー

⑴ 重要性

業界の垣根を越えて，ビジネスにおけるデータプライバシーの重要性が増していることから，ビジネスによって収集・使用されるデータをM&A取引によって取得することが，M&Aを実施する目的の１つになってきている。最も，買主は，対象会社が顧客からデータを収集し，保存したタイミングのプライバシーポリシーを精査することなく，安易にM&Aによって取得することになるデータを用いて収益化を実現することができると考えるべきではない。

買主は，M&Aを成功させるために，DDを通じてデータを利活用できる範囲を正確に把握する必要がある。

⑵ DD

そのため，データプライバシーに関連するDDを行うにあたっては以下のようなポイントを確認することが肝要であろう[5]。

- データの入手経路（消費者から提供されたものか，顧客から提供されたものか等）。
- データの種類（いわゆるセンシティブ情報が含まれていないか）。
- データに提供される準拠法の確認（データが組成された国，データを提供した者が居住する国の確認）。
- データ漏えいの有無・内容およびそれに対する対処方法，同種事案発生の有無等。
- データ漏えい保険の有無・内容。

また，データプライバシーに係る権利内容は，データが収集された時点で効力を有していたプライバシーポリシーによって規律されるが，当該プライバシーポリシーの内容に優先して適用される法令が存在することもある。

加えて，プライバシーポリシーは，時間の経過とともに変更されることも多いことから，

[4] 特に対象会社の企業文化を理解することが重要である。いかに充実したコンプライアンス・プログラムが存在したとしても，それが遵守されないのであれば，多額の制裁金のおそれのある違反や継続的な違反につながってしまうのである。

[5] なお，ヘルスケア等，特定の業界においてはデータに係る特殊な規制が存在する可能性がある。

対象会社が，異なる時期に異なるプライバシーポリシーに基づいて収集したデータについて，異なる権利義務を有する可能性がある。

したがって，DDにおいては，特定のデータに適用されるプライバシーポリシーを特定し，会社の有する権利義務の内容を正確に確認することが重要になる。これらの権利・義務の内容によっては，スムーズな統合を妨げ，買主のデータの使用を制限し，将来の統合計画に悪影響を与え，ひいてはM&A取引によるシナジーが最大化することを妨げる可能性がある[6]。また，買主は，対象会社がプライバシーポリシーの内容に従った取扱いをしていると安易に信じるべきではなく，DDの過程において，実際の運用状況についても確認する必要がある[7]。

⑶ プライバシーポリシーに対するアプローチ

M&Aの実行後，買主は対象会社のプライバシーポリシーについて，以下のいずれかの方法で対応することが考えられる。

- 対象会社が顧客からデータを取得した際のプライバシーポリシーを維持し，当該規制内容に従った取扱いを継続する。
- データの提供者から許可を得たうえで，顧客のデータを活用または共有する方法に重大な変更を加える。

米国では，統合前に収集されたデータに関連するプライバシーポリシーを変更するためには，新しい取扱いに対する顧客の（能動的な）承諾が必要になる。また，これらの顧客から将来収集されるデータの取扱いまたは活用法の変更にあたっては，変更通知およびこれらを受け入れるための十分な機会を提供することが必要になる（単に既存のプライバシーポリシーやユーザー規約を改訂するだけでは不十分である）。

3 サイバーセキュリティ

⑴ 重要性

サイバー攻撃は，世界中のどこでも事業に対する日常的な脅威になっている。M&Aは，企業の防御活動に綻びを生じさせ，ハッカー等が企業のネットワークにアクセスする機会を与えることから，当該企業がサイバー攻撃を受ける可能性を高める。

当然のことながら，この種のサイバー攻撃がもたらす可能性のある悪影響は多く存在するが，そのうちの一部を紹介すると次頁の**【図表】**のとおりである。このようにサイバーセキュリティは会社の企業価値に大きな影響を与えることから，サイバーセキュリティ対策がどの程度十分に整備されているかがM&A取引における価格決定にも大きな影響を与え得るため，M&Aにおける重要性は高い。

⑵ M&Aにより高まるサイバーセキュリティ・リスク

また，M&Aに関連するアクションの多くは，サイバー攻撃に対する企業の脆弱性が増加することにつながる。たとえば，報道や規制当局への届出の公表やプレスリリースが，サイバー攻撃につながることがある。ハッカー等は，取引に関与している企業が機密データや情報を送信していることを知っていることから，上級執行役員またはアドバイザーに攻撃対象を集中することができる。

⑶ DD

DDを実施するにあたっては，特に①サイ

[6] 連邦取引委員会（FTC）は，M&Aに関連する企業向けにプライバシーポリシーに関するガイドラインを公表しているが，FTCは，合併または同様の取引によって，データ収集時に有効に存在していたプライバシーポリシーの有効性に影響を与えないとしている。

[7] 当該リスクを検討するにあたっては，対象会社の企業文化を理解することが重要である。

【図表】サイバー攻撃がもたらす悪影響

データ，機密情報および／または信頼の喪失，知的財産の盗難	たとえば，知的財産が奪われた結果として，企業は当該知的財産を独占することができなくなり，当該知的財産は海外の競合企業の手に渡ることがある。これにより，将来の収益の減少やレピュテーションの低下等，さまざまなコストや損害が発生する可能性がある。漏えいした機密情報から生じるこれらの損害を定量化し，または回復することは困難または不可能である可能性もある。
取引価値の喪失	VerizonによるYahoo!の買収は，取引価値が喪失した著名なケースである。2016年に，Verizonは検索事業とEメール事業を含むYahoo!の主要事業を48億ドルで買収すると発表した。ところが，契約書締結からクロージングまでの期間において，Yahoo!がサイバー攻撃の被害に２度遭っていたことが明らかになった。このサイバー攻撃の結果，20億を超えるYahoo!アカウントのパスワードやその他の情報が公表され，Yahoo!の株主が受け取るはずであった金額が３億5,000万ドル減少した。
金銭の喪失	会社の銀行口座にアクセスするための情報を取得したハッカー等は，（海外または追跡不可能な口座への）送金を行ったり，銀行口座自体にアクセスするおそれがある。
株価の下落	当然のことではあるが，有害なサイバー被害のニュースは，会社の株価に重大な悪影響を与えることが統計上明らかになっている。

バーセキュリティに関するガバナンス（監視体制，管理担当者，対応手順等の整備状況，担当取締役が積極的な役割を担っているか等），②委託先（ソフトウェアやサービスプロバイダー等）の管理体制（十分なセキュリティ対策が実施されているか否か等），③サイバー保険の有無・内容等を検討することがポイントとなる[8]。

⑷ M&Aにあたっての留意点

攻撃者がネットワークセキュリティーを侵害するために，取引チームの個人を標的にするといった手法をとることがあるため，案件に関与するすべてのメンバーが，サイバーセキュリティ・リスクとそれに対する対応方法を正確に理解している必要がある。また，情報共有にあたっては，外部のアドバイザーとの関係だけでなく，社内でも機密性の高い情報のやりとりについては暗号化することも考えられる。これによって，会社のシステムが危険にさらされた場合であっても，侵害が発見される前に侵害の影響を軽減するための追加のセキュリティを構築することが可能になる。

また，買主は，自社と対象会社のITインフラを統合する前に，自社ネットワークに統合するデータ，ソフトウェアおよびハードウェアの内容を正確に理解する必要がある。対象会社のシステムが脆弱である場合，この脆弱な部分が統合されたことによって，買主のシステムが脆弱性を有したまま稼働してしまう可能性がある。買主が対象会社のシステムに関して適切な水準で安全性が図られていると確認できない場合には，システムが適切に修復されるまで各システムを個別に作動させる必要がある点にも留意する必要がある。

顕出されたリスクに対する一般的な対応方法

前記でもM&Aを実施するにあたって留意すべき点等を簡単に論じたが，M&A取引において，当事者がサイバーセキュリティ等のリスクを軽減するための対処方法として以下のような一般的な対応を講じることも考えられる。

[8] たとえば，米国の多くの企業は，サイバー保険に加入しているケースが多い。サイバー保険はサイバー攻撃による損失を補償することから，その保険内容を確認することは重要であるが，サイバー保険には企業がサイバー侵害を受けることを防ぎ，または緊急時への対応をサポートするサービスが付随していることが多いため，サイバー保険に加入しているか否かはガバナンス体制の整備状況を確認する意味でも重要である。

1　表明保証

まず，非公開会社を対象会社とする取引を行う場合には，サイバーセキュリティ等に係るリスクを買主から売主に転換するために，M&Aの契約書において，売主にサイバーセキュリティ等に関する表明保証をさせ，表明保証違反による損害が顕在化した場合に，買主から売主に対して補償請求をすることができるよう交渉することが考えられる[9]。ただし，売主との交渉力の差によってはこれらの条項を規定することが難しい場合もあり，補償期間，買主が認識し，または認識し得たリスクに関する取扱い等についても売主側と激しい交渉がなされることも多い。

2　誓約事項・前提条件

次に，買主は，売主に対して，契約締結後クロージングまでの間に，誓約事項として，一定の対応を義務づけたり，一定の対応が完了していることを前提条件とすることを求めることが考えられる。具体的には，買主が特定の問題を発見した場合に，売主に対して，クロージングまでに当該問題を解決することを誓約事項として義務づけ，また，それを前提条件とすることが考えられる[10]。

3　保険の活用

さらに，サイバーセキュリティ等に起因したリスクに対処するために，売主，対象会社および買主が，サイバー保険およびデータ漏えい保険に加え，表明保証保険を活用することも検討に値する。表明保証保険はM&A取引において一般的に用いられることが多くなってきているが，当該保険によって，保険会社が，売主による表明保証違反に関連したリスクの一部を引き受けることになるため，売主の表明保証違反が表明保証保険の適用対象である場合，保険会社が買主に損失の一部を補填することができる。したがって，売主がサイバーセキュリティ等に係る表明保証に違反した場合も当該リスクを表明保証保険によって補填することができる可能性がある。

＊　　＊　　＊

以上のとおり，M&Aの文脈において，サイバーセキュリティ等を検討することの重要性に加え，それぞれのリスクの概要および対処方法の概要について解説した。M&Aという重大な経営判断をするにあたっては，リスクを正確に理解したうえで，当該リスクを軽減するためのソリューションの有無・内容をあわせて検討することが重要である。サイバーセキュリティ等に関連したリスクの検討・分析が不十分であったことを理由に，誤った経営判断につながらないためにも，本稿がM&Aに関わる日本の実務家の一助になれば幸いである。

Joseph Castelluccio（ジョゼフ・カステルチーオ）
Mayer Brown LLP.パートナー（米ニューヨークオフィス）。ジョージタウン大学およびブルックリンロースクール卒業。投資銀行で勤務した経験も有する。日本企業を含むグローバル企業に対して，テクノロジー，保険，金融サービス，工業，化学，インフラ部門を含む幅広い業界におけるM&A，ジョイントベンチャー等の企業法務に係る助言を行う。

田中健太郎（たなか　けんたろう）
TMI総合法律事務所。日本国弁護士，イリノイ州弁護士。中央大学およびミシガンロースクール卒業。2018年7月から2019年6月までMayer Brown LLP，7月からHOUTHOFF（アムステルダム）で研修中。M&A，フランチャイズを中心に企業法務全般を取り扱い，これらに関する多数の論文・書籍の執筆を行う。

[9] さらにサイバーセキュリティ等に係るリスクが大きい場合等には，買主の認識の有無にかかわらず，通常の補償条項よりも長期の期間，契約書による上限のない形で特別補償請求を認める規定を設けることが考えられる。

[10] ただし，問題の重要性や問題解決に係る時間軸に応じて，クロージングまでにこのような対応を求めることが現実的でない場合には，表明保証の対象にするにとどめることも考えられる。