サイバーセキュリティからみたデータガバナンス

杉山一郎　EY 新日本有限責任監査法人
GIAC Certified Forensic Analyst

◆ *Summary* ◆

ランサムウェア等のサイバー攻撃による影響が拡大の一途をたどり，事業継続や財務報告等にも影響を及ぼし始めている。また，データの利活用とともに個人データの侵害等に対する規制が強まっている。このような状況を踏まえ，本稿では DX が進むなかで増加するサイバーセキュリティリスクの視点から見たデータガバナンスの重要性について考察する。

《は じ め に》

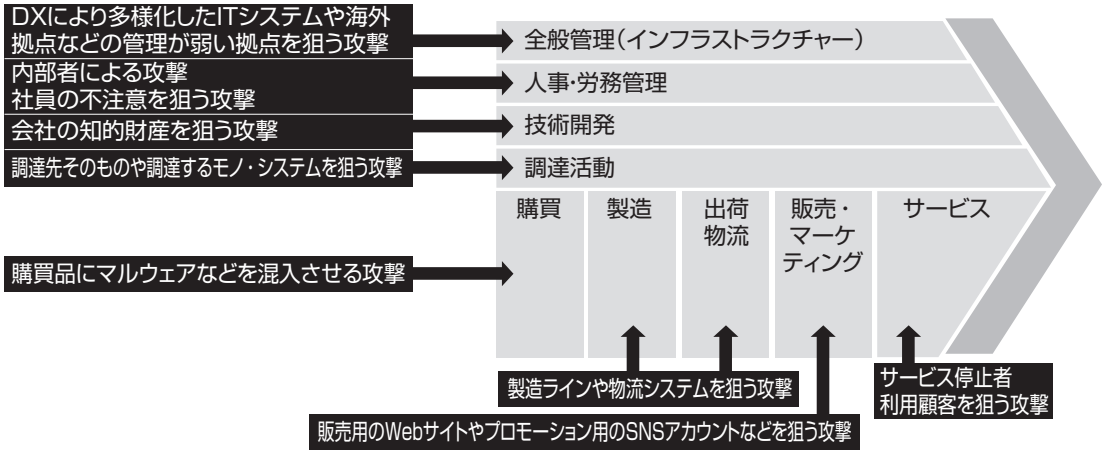
企業のデジタル化により業務で取り扱われる情報量が増加したことに加えて，ビジネスプロセス変革により事業における IT の役割も増えたことで，組織外部からのサイバー攻撃による情報漏えいや資産の毀損などのサイバーリスクも同時に増加している。これまでは対岸の火事だと思っていたサイバーインシデントが，ついに自社でも発生したという方が読者の中にもいるのではないだろうか。サイバーインシデントは無形資産の破壊や不正送金による直接的な毀損だけでなく，企業の事業継続や信頼にも影響を及ぼし始め，最近ではサイバー攻撃により財務報告に甚大な影響を受けた事例が各国で報告されている。

たとえば，昨今急増しているランサムウェア攻撃の場合，被害企業はシステムや重要データの暗号化により停止してしまった事業を再開するための対応に限らず，個人情報・営業秘密・知的財産などの重要な情報の漏えいおよび毀損などの影響範囲の確認，財務報告を構成する情報の完全性の検証，ステークホルダーへの報告など，様々な対応に追われることとなる。このような危機的な状況は他のサイバー攻撃によっても発生しうるので，DX 推進下において企業が進めるデータドリブン型経営やオペレーショナルエクセレンスなどの企業戦略に大きな影響を与えかねない。たとえば，前者については判断のもととなるデータが侵害され完全性や可用性が損なわれてしまうことで，適切なデータ分析が行えなくなるだろうし，場合によっては機密性の侵害によりプライバシー関連法の罰則や漏えい被害者からクラスアクション（集団訴訟）のリスクなども生じてしまう。このような状況を踏まえて，本稿では近年重要視されているデータガバナンスの中でもサイバーセキュリティなどのデータ利活用時のリスク管理について触れたい。

Ⅰ　サイバー攻撃の件数および事業への影響が増加する理由

端的に言えば，２つの理由があると考えて

〔図表〕サイバー攻撃は企業の様々な側面を標的としている



いる。1つ目が「サイバー攻撃のベクトルが企業活動の様々な側面に向かっているが，企業の防御が追いついていない」という点である（図表）。これはデータガバナンスの重要性の高まりとも深く関係する。企業がデジタルデータの活用や多様な働き方などを実現するために導入した新たなテクノロジーが結果として攻撃の対象を増やしており，それに対する防御が追いついてない状況を一部生み出している。「新しいテクノロジー導入時にセキュリティ部門へ相談するルールがない」「新しいテクノロジーにより増加した管理対象データが保有するリスクが適切に評価されていない」など理由は様々であり，このような課題について頭を悩ませているCISOやCIOは多いのではないだろうか。また，新しいテクノロジー導入時にはサイバーセキュリティ以外にも内部リスクなどに配慮した物理的なセキュリティにも留意する必要があるが，この点に対する意識の低さも攻撃件数や影響範囲の拡大に多少なりとも影響していると考える。

2つ目は「サイバー攻撃を行う犯罪者が，攻撃ツールの入手から別の攻撃により流出したシステム等の認証情報の購入，ランサムウェアを通じ取得した仮想通貨の資金洗浄まで幅広いサービスをダークウェブ等の闇市場で容易に利用できてしまう，サイバー犯罪のエコシステムの進化」という点が挙げられる。ローコストハイリターンのおいしいビジネスが攻撃者のモチベーションをあげ，サイバー犯罪の数を増やしたり，デジタルに依拠するビジネスの様々な側面を狙うことで別のサイバー犯罪ビジネスモデルが生まれたりしているのが現状であり，昨今のランサムウェアを悪用した犯罪のモデル（Ransomware as a Service）もその1つとなる。実際にランサムウェア以外にも株価下落（空売り）を狙っ

Profile

すぎやま・いちろう◇EY新日本有限責任監査法人 Forensic事業部 プリンシパル。デジタルフォレンジックの分野において15年以上の業務経験を持ち，2014年からEY Japan Forensicsにてサイバーインシデント対応，eDiscovery対応，インフォメーションガバナンスなどを主な取扱い分野とするフォレンジック・テクノロジーの責任者を務める。

てサイバー攻撃を請け負うようなサービスモデルも報告されている。

Ⅱ　サイバーリスクへの基本的な対応アプローチ

多様化・複雑化するサイバー攻撃に対してどのようなアプローチが有効であるか，サイバー攻撃がもたらすサイバーリスクの構成要素に従って，「攻撃する側の視点（脅威）」と「防御する側の視点（脆弱性と資産）」から考えてみたい。

攻撃をする側，つまり攻撃者は何らかの意図（情報窃取，破壊等）と攻撃に必要な能力（ハッキング，マルウェア等）を持ち，攻撃の機会を見計らって標的組織に攻撃を仕掛けてくる。近年はこのような脅威（攻撃者）に関する情報を積極的に入手し，セキュリティ対策につなげていく「脅威インテリジェンス」をセキュリティ活動に取り入れる組織が増えている。脅威は本来組織では対策が困難なサイバーリスクの構成要素であり，後述する防御側の視点中心のアプローチが企業のセキュリティ活動の中心となることが多かった。しかしながら，防御視点中心のアプローチには対応リソースの限界などがあるため，この限界をカバーできる可能性があるアプローチとして，この脅威インテリジェンスの活用が着目されている。脅威インテリジェンスは本稿のメインテーマであるデータガバナンスとの関連性は高くないため，詳細は割愛するが，セキュリティ対策の不備などが悪用され，万が一にも機密情報が漏えいした場合に備えた監視などに有用であるほか，攻撃の動向を把握し先回りして対策を打てるなど，今後重要となるアプローチであることはお伝えしておきたい。

たとえば，昨今のランサムウェア攻撃において悪用されることが多いVPN（Virtual Private Network）機器などインターネットからアクセス可能な企業のネットワーク機器の認証情報，あるいは認証情報なしでアクセス可能な脆弱な機器の一覧などは攻撃者のコミュニティにおいて取引されていることが少なくない。脅威インテリジェンスの活動を通じて，このような情報の流通を先回りし，把握して対策を実施し，攻撃を回避するといったことが期待できる。なお，このような脅威インテリジェンスの活用は，これから説明する自社が保有するデータ資産の保護やデータ管理上の脆弱性対策が一定程度できていることが必要となることには留意いただきたい。

さて，本題となる防御側の視点からのアプローチについて考えたい。このアプローチは企業が保有する重要なデータ資産の特定とその保護策（セキュリティ）の欠点となる脆弱性の管理をどのように行い，サイバーリスクを減らしていくかを検討し，実施していく。

このアプローチでは，以下の３つのプロセスの実施を検討する。

① 企業として避けるべき事態から守るべき重要な情報資産を特定する
② 特定した重要な情報資産の脆弱性を把握し，リスク管理を行う
③ リスクが顕在化し，最悪の事態あるいはそれを予見させる事態となった場合の対応策を索定する（インシデント調査，訴訟等）

それぞれ，少し補足する。まず①については，すべての情報資産からリスクを特定する網羅的なアプローチよりもビジネス全体を俯

瞰して避けるべき事態から重要な情報資産を見出すアプローチとしている。これは，サイバー攻撃の範囲が広範にわたっており，その対象となるシステムや情報が増加していることに鑑みるとシステムやビジネスの相互関係を踏まえ俯瞰的に捉える必要があると考えるからだ。また，業種などビジネスの構成要素により異なるが，一般的に重要な情報資産としては営業秘密，個人情報，医療情報，知的財産情報，インサイダー情報などが挙げられる。それぞれが関連法などにより保護されているだけでなく，その情報に係る関係者やシステムが複数存在することに留意が必要である。重要資産の理解が必要な例を１つ挙げる。昨年末にFBIが，一部のランサムウェア攻撃を行う集団が企業合併などを控えている企業を狙っていると警告している(1)。企業合併などの時間的な制約がある企業の関連情報を暗号化し，株価下落を恐れる企業に対して身代金支払を迫っているということのようだ。攻撃者が標的にとっての重要なイベントから効果の高い攻撃手法などを分析していることが推測されるが，防御側も攻撃者同様に重要なイベントに影響を与える事象から保護すべき重要資産の特定が必要であるといえるのではないだろうか。

次に②の脆弱性について補足する。一般的に脆弱性というとデータの保管や処理を行うソフトウェアやハードウェアなどの技術的な脆弱性を思い浮かべる方が多いかと思うが，ここで言う脆弱性は技術的な脆弱性に加えて，ビジネスプロセス上の脆弱性（例：ソフトウェア更新ルールや特権利用時の承認プロセスの未整備）や従業員などの人の脆弱性も含めている。これらの重要資産を保護するうえでの脆弱性の対応についてあるべき姿をベストプラクティスやセキュリティガイドラインを参考にし，自社の実態との乖離状況を分析するギャップ分析アプローチが一般的に利用される。

最後の③のプロセスは①②に比べると，日本企業は進んでいない印象を持っているが，サイバー攻撃が事業に与える影響が拡大しており，実際にサイバーインシデントが発生すると短時間で事業再開時期や身代金支払など様々な意思決定が求められるだけなく，ステークホルダーへの適時の情報開示の対応まで求められる必要があることに鑑みると，非常に重要なプロセスであることがわかる。本年４月に施行された改正個人情報保護法では，個人情報漏えい時の委員会への報告のタイミングについて，当該事態を知った時点からおおむね３～５日の速報，30日以内の確報を求めているが，昨今のサイバー攻撃が与える影響範囲の広がりやサイバー攻撃の痕跡の残りにくさなどを考えると，事前の準備なしではこの改正法の要件に従った時間軸での対応は難しい。さらに時間的制約は法律だけでなく，攻撃者からも掛けられる。たとえば，昨今のランサムウェア攻撃は企業のデータを暗号化する前に窃取し，そのデータの暴露に対して脅迫行為を行う。攻撃者が指定した数日程度の短い時間内に身代金が支払われない場合，インターネット上に公開するといった脅迫である。このような時間的制約を掛けられる中でしっかりと事実確認をし，その確認結果に基づく復旧およびステークホルダーへの情報開示を行うためにも③のプロセスは重要となる。

なお，身代金支払については，わが国の現

行法では直接罰する法律はない一方で，犯罪者への資金提供につながるほか，そもそもそのような事態に陥ってしまったセキュリティ対策など不備について善管注意義務違反となる可能性も否定できず，原則支払うという選択肢はないと思われる。ランサムウェア攻撃により重要なデータやシステムが破壊され事業継続が困難となり，身代金支払を検討せざるを得ない状況とならないよう，セキュリティの強化が望まれる。

Ⅲ　サイバーセキュリティとデータガバナンス

前置きが長くなってしまったが，前述の①～③のプロセスの実施において前提となり重要となるのが，企業に散在するデータを統一的に整理し，そのデータが持つ情報特性に応じたリスク管理を行うデータガバナンスである。なぜ，データガバナンスが有効となるのか，平時と有事の両面から見た情報管理から整理したい。

まず，有事の側面から整理する。既述のとおり，サイバー攻撃により個人情報などの漏えいなどが発生した場合，各国のプライバシー関連法などで定められた期限内での報告が必要となる。その際にどの法律要件が適用されるかは企業が保有するデータが持つ情報やそのデータの保管場所などにより変わり，インシデント後の整理では間に合わないため，インシデント前の整理が望まれる。特に海外で事業展開されている企業においては当該国のプライバシー関連規制について，「対象となるデータの範囲」「インシデント発生時の通知義務要件」「域外適用」「国内移転の可否」「国内保存義務」「データの移転などに際して必要な手続」などの点について事前に確認しておくほうがよい。また，外部からのサイバー攻撃というよりは内部関係者による犯行を見据えた対応となるが，営業秘密のように法律上の保護を受けるためにインシデント以前から適切な取扱いが求められる情報があることにも留意が必要である。そのような情報の侵害が生じ，調査によりその行為を立証しようとしても，そもそも情報が適切に管理されていないと期待した結果を得られずに終わる可能性があることに留意する必要がある。

有事の際に調査対象となる証拠データの保全についても情報管理の観点で留意したほうがよい点がある。証拠データについて，「完全性（改ざんされていないか）」「網羅性（関連性のあるデータを保全できているか）」「追跡可能性（証拠データはどのように扱われたのか）」の３点が特に重要となり，いずれも有事の段階で確保しようとしても難しいため，企業が新たにサードパーティー製のサービスやシステムを導入する段階でこの点に留意する必要がある。たとえば，欧米のクラウドサービスにはインシデントや訴訟に備えたデータやログ保管に関する追加のオプションが備わっていることが多いが，日本企業では広く利用されていない印象があり，実際にこのようなオプションが無効化されており調査上必要なデータが取得できず調査を断念した事案を聞くことが多い。また，従業員の私物デバイスの業務利用を認めている企業で発生したインシデントにおいて，当該デバイスの調査が必要となったが，調査への同意を得られずに調査できなかったという事例も少なくない。外部からのサイバー攻撃に限らず，営業秘密

などの重要資産の保護の観点からも従業員の私物デバイスの利用を認めている場合は，有事において企業データが格納されるデバイスとして調査協力のため提出することへの同意を取得しておくことが望まれる。

次に平時における情報管理について整理する。既述のとおり，有事対応以前に平時の段階から適切な情報管理を求める規制が増えている。このような規制に対して適切に対応していくことが平時における情報管理で重要な点の１つとなるが，対応のポイントとしては「組織横断での」情報管理が挙げられる。

組織には様々な場所にデータが散在し，それぞれのデータには部門が異なるオーナーが存在する。データガバナンスの主目的である組織横断でのデータ利活用の実現時にも大きな障壁となる部門の壁がセキュリティのための情報管理においても課題となる。冒頭でも触れたとおり，サイバー攻撃のベクトルが組織の様々なプロセス，つまりそこで扱われるデータに向いていることを考えると，各部門で扱われる情報やデータに対しては統一的なセキュリティを行う必要がある。少なくとも新しいテクノロジー導入やデータ戦略においてセキュリティ部門が相談を受けないという状況は回避しなければならないし，企業がDX 推進している環境下においてはなおさらである。

《おわりに》

ここまでサイバー攻撃の影響範囲，サイバーリスクを最小化するためのアプローチ，情報管理の重要性についてデータガバナンスとの関連性も踏まえて記載してきた。

最後にデータガバナンスの主要なテーマであるセキュリティやコンプライアンス等のリスク管理について，古くから検討されているインフォメーションガバナンスのアプローチについても紹介したい。

日本でデータガバナンスが着目される以前からデジタルフォレンジックや eDiscovery（米国民事訴訟における電子証拠開示）の世界では，訴訟等における電子情報開示や法的に保護された文書の保管義務，リスク管理などに対応するために，企業内のデータが持つ情報のライフサイクル管理としてインフォメーションガバナンスの重要性が認知され，特に訴訟対応の多いグローバル系企業で取り組まれている。このインフォメーションガバナンスはデータガバナンスの中でもサイバーセキュリティやコンプライアンス上のリスク管理部分と重複するため，インフォメーションガバナンスで利用されているアプローチがデータガバナンスのセキュリティルール等の作成において有用と考える。

インフォメーションガバナンスでは，最初に組織がどのようなデータを作成・受領・収集しているかを理解し，その用途・保管場所の理解を進める。具体的には，データインベントリの構築が最初のステップとなる。企業全体に散在するデータが持つ情報やコンテキストから企業が順守すべき法律等の要件を理解し，その利用状況や保管場所の適切性を検討していく。特にプライバシー関連規制においては，データの保管場所の適切性の評価，情報所有者からの削除等の要求，データ移転時の適切な処置を行う必要があるため，利用状況や保管の実態把握が重要となる。また，GDPR などの法規制で要求されるデータマッピングは継続的にメンテナンスされる必要が

あるため，データインベントリの構築時にはこの点にも留意が必要である。

次にサイバーセキュリティやコンプライアンスに深く関係する，データの保護と侵害等のイベントへの対応について現状を知り，改善を進めていく。自明だが漏えいしたデータは犯罪者に悪用されたり，インターネット上で公開されたりするリスクがある。また，大規模なデータ侵害事案によるレピュテーションの低下は長期にわたり企業の収益に影響を与える可能性がある。プライバシー関連情報を取り扱うシステムについてはデザイン段階からプライバシーに配慮するなど，ビジネスやテクノロジーの導入にプライバシー保護等のセキュリティが常に組み込まれるように企業文化を醸成することが重要であり，知的財産などの他の情報に対する取扱いも同様である。また，保護以外にもその侵害の兆候を検知する仕組みや侵害が発生した際に事前に確認した要件を満たすためのインシデント対応プログラムの整備も忘れてはならない。インシデント発生時に情報の開示を期待するのは当局だけではなく，顧客・株主・取引先などと広範にわたる。それぞれのステークホルダーに対して適切に情報開示するには，それぞれのステークホルダーに対峙する社内関係者との連携が不可欠であり，インフォメーションガバナンスなどの組織横断での情報管理を維持する理由の１つである。なお，高度なサイバーセキュリティのテクノロジーにより，インシデント対応のオペレーションの多くが自動化されることがあるが，組織内連携やステークホルダーへの情報開示などの対応は経営層を中心とした社員が行う必要があることに留意いただきたい。

最後にデータの保管期間と廃棄ポリシーの策定・見直しを行う。プライバシー規制，ビジネスニーズ，訴訟やその他法規制を考慮し，企業はデータの種別の保管期間を定期的に見直す必要があるが，急速なプライバシー規制の変化やデータの分散化などを考慮すると，レコード・マネジメント・システムの活用など組織全体に適用可能な包括的なアプローチを検討する必要がある。また，不必要なデータ廃棄は情報漏えいによるプライバシー侵害リスクの低減や訴訟対応などの法的コストの削減につながるため，保管要件の期間を超えたデータは速やかに削除する。

以上の３つの大きなプロセスを回していくことが，インフォメーションガバナンスの基本的なアプローチとなる。すでにある程度類似の取組みを行っているという組織については，記録・情報管理に携わるプロフェッショナルが集まる非営利団体である ARMA International が発刊する，企業のインフォメーションガバナンスの成熟度を５段階で評価する Information Governance Maturity Model を参照し，自組織で不足している領域から取組みを始めてみてもよいと思う。なお，同モデルで成熟度評価の対象としているのは，Accountability・Transparency・Integrity・Protection・Compliance・Availability・Retention・Disposition となっており，先に述べたインフォメーションガバナンスの基本的アプローチの内容を網羅している。

（注）

⑴　https://www.ic3.gov/Media/News/2021/211101.pdf