経営課題であるサイバーリスク
—— IT部門だけで対応できるリスクではない

PwCあらた有限責任監査法人
システム・プロセス・アシュアランス部
パートナー　**綾部 泰二**

はじめに

サイバーセキュリティと聞くと、セキュリティ部門やIT部門で対応すべきリスクと認識されている方もまだまだ多いのではないでしょうか。本稿では、サイバーインシデントへの対応や対応状況によっては経営者の責任、企業への格付け評価に影響があることに触れながら、サイバーリスクが経営課題であることを解説します。

1 インシデント対応から理解する

各企業が生産性の向上や新たなビジネスの創出のためにデジタルトランスフォーメーション（DX）を推進し、またコロナ禍への対応としてリモートワークを急激に導入した昨今において、サイバーリスクが顕在化する機会は飛躍的に増大したと想定すべきでしょう。

まずは公開データに基づいて、サイバーインシデントの傾向を把握しておきましょう。**図表1**からも分かるように、最近のサイバーインシデントの傾向として次の3点が挙げられます。

① ランサムウェアによる被害
② 不正アクセス
③ 内部犯行

近年その被害が急増しているランサムウェアは、主に身代金を目的としてシステムを暗号化、もしくはデータを搾取する悪意のあるプログラムですが、金銭を要求する攻撃者に対してどのように対応するかという問題があり、その対応はIT部門やセキュリティ部門の通常の役割を超えるものと想定されます。そのため、会社のポリシーとしてこのような身代金要求には応じないとの意思をあらかじめ決定しておくことが必要です。

身代金要求に応じない場合には、システムが暗号化されたままになったり、搾取されたデータが公開されたりすることが想定されます。そのような場合に必要な対応は以下のとおりです。

(1) システムが暗号化される場合

暗号化されるシステムにもよりますが、システムが復旧されるまで業務をいかに維持すべきかをあらかじめ検討してお

図表1：最近発生したサイバーインシデント

年月	被害組織	概要	攻撃手段
2021年1月	A社	技術情報を持ち出し、転職先企業へ提供した疑い	内部犯行
2021年2月	B社	サイバー攻撃により、水酸化ナトリウムの濃度を通常の100倍超に変更	不正アクセス
	SaaSサービス利用企業	設定ミスにより、複数企業で住民・顧客情報などが漏洩	設定ミス
2021年3月	C社	国際航空情報通信機構（SITA）の旅客系システムへ不正アクセス	不正アクセス
2021年4月	多数	偽名で日本国内レンタルサーバーを契約し、国内約200の組織へサイバー攻撃などに悪用した疑い	不正アクセス（ITサプライチェーン）
2021年5月	D社	ランサムウェア感染のためパイプラインの操業が停止し、約100 GBのデータ漏洩が発生	ランサムウェア
	E社	サイバー攻撃を受け3TBの機密データがリークサイトで公開	ランサムウェア
	F社	テスト環境で利用する「Codecov」への不正アクセスにより、同社ソースコードの一部および約2万8000件の同社顧客情報が漏洩	不正アクセス（ITサプライチェーン）
2021年6月	Webサービス提供会社	大手ITベンダーが提供する共有システムへの不正アクセスにより、政府をはじめとする利用組織から情報漏洩相次ぐ	不正アクセス（ITサプライチェーン）
	G社	食肉加工大手の支社システムがランサムウェア感染。バックアップをもとに復旧するも、身代金として約12億円を支払う	ランサムウェア
	非営利団体組織	2020年4月にランサムウェア攻撃の被害を受けていたことが報道された。被害端末約60台の全面入れ替えを行い復旧	ランサムウェア
2021年7月	H社顧客	自社の顧客企業がランサムウェアに感染	ランサムウェア（ITサプライチェーン）
	I社	ランサムウェア感染のため、企業情報および個人情報の一部が流出	ランサムウェア

出所：公開情報をもとにPwC作成

く必要があります。

あるインシデントにおいては、バックアップを含む大量のデータが暗号化されました。この影響により、被害を受けた企業は決算発表や四半期報告書の提出を延期せざるを得ない状況に陥りました。

（2）搾取されたデータが公開される場合

搾取されたデータの内容を把握できないとインシデントに対応できません。データオーナーがユーザー部門であることから、その対応はユーザー部門が中心となって行うと想定されます。また漏洩データがビジネスパートナーから預託を受けているデータであったり、顧客情報であったりする場合は、その対応はより複雑性を増すことが想定されます。

このように、上記（1）と（2）の対応からも、IT部門やセキュリティ部門だけで対応できるものではないことが分かります。

また、ITサプライチェーン経由の感染、つまり自社またはビジネスパートナーがランサムウェアに感染したことで2次被害が生じたケースがある点には留意が必要です。ITサプライチェーンの被害事例は取引先に留まりません。いわゆるSaaSサービスを提供している企業が感染することで、当該サービスを利用している企業も被害に遭うというケースが発生しています。このため、取引先のサイバーリスクへの対応状況についても理解し、一定水準以上の対応を取っている企業と取引を行うなどの対応が必要です。

このような対応を実行するには、既存の取引先へのアセスメントや、定期的な更新が必要です。これらはセキュリティ担当部門によって推進されるべきですが、実際にビジネスパートナーを管理している部門の協力も不可欠です。

インシデントに対応するときだけでなく、サイバーリスクの発生可能性を低減する際にもIT部門やセキュリティ部門だけでは対応は不十分ということになります。

2 インシデントに対する責任から理解する

インシデントが発生した場合、企業がその責任を問われるケースもあります。そのような事例は国内でも起きていますが、国外においてはその傾向は顕著で、グローバル展開している企業においては特に留意が必要です。

責任が問われる結果としてCEO退任、役員報酬返上といった対応を取らざるを得ないケースがあります。場合によっては被害者から訴訟を提起される、刑事事件に発展して有罪判決を受けるといった可能性もあります。企業が有罪判決を

受けた事例を1つご紹介しましょう。

ある企業ではセキュリティインシデントの公表を予定していました。そのことを事前に知る立場にあったある従業員は株価下落による損失回避を目的として、公表前に自身が保有する自社株を売り抜けたのですが、インサイダー取引と認定されて有罪判決を受けたのです。この事例のような、インシデント情報を知り得る従業員や役員の自社株売却については、制限を設けるなどの措置が必要であることは明らかです。

以上のように、インシデント発生時にはさまざまな部門が対応に関与します。インシデント発生時に関与が想定される部門を事前に特定することは難しく、IT部門やセキュリティ部門だけで対応できる問題ではありません。

3 企業の格付け機関の評価項目から理解する

セキュリティ対策をはじめとする非財務情報の開示は、機関投資家の各種企業格付けに影響を与えています。例えばある格付け機関によると、多数の非財務情報の評価項目としてプライバシーへの対応やデータセキュリティに関し全体の評価に反映させているとのことです。ここで企業から情報が得られない場合には、評価は最低スコアになることもあると言われています。

このようにサイバーリスクへの対応は、非財務情報の開示項目として企業価値に影響を及ぼすものであることから、当該対応もIT部門やセキュリティ部門を超えて全社的に対応しなければならないことが分かります。

4 最後に

ここまでインシデントへの対応、インシデント発生後の責任、そしてサイバーリスク対応の開示といった観点から、サイバーリスクを経営課題として捉えるべきである点について解説してきました。いずれのケースにおいてもIT部門やセキュリティ部門のみの対応ではなく、複数の部門による横断的な対応が求められる課題であるとご理解いただけたのではないでしょうか。

このような部門横断的な課題への対応には、トップマネジメントによるリードが必要です。ぜひ今一度、サイバーリスクへの対応という観点から、インシデントの発生が自社の利害関係にどのようなインパクトを及ぼすかを整理し、現状の体制で十分であるかどうかを検討してみてください。また、将来にわたってサイバーリスクを防ぐための「戦略」を立案し、実行することが必要です。事業戦略、特にデジタルやデータを活用した戦略を立案する際には、サイバーリスクへの対応を当該戦略の一要素として検討すべきでしょう。また、次々と登場するマルウェアの脅威に対抗するためにも、「何を守るのか」を明確にした上で戦略を立案・実行し、対応いただければと思います。

綾部 泰二（あやべ たいじ）

PwCあらた有限責任監査法人　システム・プロセス・アシュアランス部
パートナー

2006年CISA（公認情報システム監査人）、2001年にPwCへ参画。以後、セキュリティやITガバナンス等のリスクマネジメント業務に多数従事。2019年7月よりPwC Japanグループのサイバーセキュリティ Co-Leaderを務める。共著に『クラウド・リスク・マネジメント』（同文舘出版）、『経営監査へのアプローチ――企業価値向上のための総合的内部監査10の視点』（清文社）がある。