Marsh

建設業界における サイバー・セキュリティ

包括的で費用対効果の高い保険ソリューション

White Paper

建設業界における サイバーリスクの状況

デジタル化が進むアジアの建設業界では、サイバー・セキュリティに関するインシデントやサイバー攻撃による企業の財務的損失の増加をはじめ、甚大な被害が発生しています。

ランサムウェア攻撃に関する調査1において、2020年から2021年にかけて世界的に最も多く標的にされたのは建設業界であり、製造業、金融、ヘルスケア業界よりも上位にランクされています。また、2022年のIBMの調査では、2021年には世界の中でアジアが標的となる場合が最も多く、組織へのサイバー攻撃のうち26%となったことが判明しました。[2]

さらに、建設会社は一般にキャッシュフローが高いため、サイバー犯罪に狙われやすいとされており、高額な支払いが生じる下請け業者やサプライヤーも多いため、建設業界はスピアフィッシング（特定の個人、組織、企業を標的とした電子メールや電子コミュニケーションの詐欺の一種）の標的になっています。[3]

同時に、建設会社の基幹システムやサポートシステムの一部として採用された新しいテクノロジーも、サイバー・セキュリティの改善を伴っていないことが多いため、結果として、サイバー攻撃や悪質な犯罪者が侵入するためのアクセスポイントをさらけ出してしまっているとも言えるのです。これは、アジアの企業の68%が自社のサイバーレジリエンスに自信を持っているものの、約半数（48%）が、サイバーハイジーン（サイバー衛生）の実践に関してはまだ改善の余地があることを認めている、という事実を裏付けています（Marsh-Microsoftによる「サイバーレジリエンスの現状」レポートより）。

建設業界における脆弱性

電子的に保有・共有・更新されるBIM（ビルディング・インフォメーション・モデリング）とプロジェクト管理ツール

自動機械・ロボティクス

IoT（モノのインターネット）機器 / SCADA（監視制御・データ収集）システム

協力会社やサプライチェーンベンダーと共有する情報およびビジネスクリティカルなシステム

ITシステム（給与計算など）のサポート

コンピュータシステムに保存された重要な設計・図面

アクセスポイント

また、建設業界では従業員が流動的であるため、機密情報や専有情報へのアクセス管理が困難であることも、サイバーリスク上昇の要因となっています。会社や顧客のデータを保護するために必要なサイバー衛生の実践と必要な手順を確実に実行するために、建設会社は、スタッフや特権ユーザー（データやビジネスにとって重要な情報にアクセスできる人など）の審査やトレーニングなどの重要なサイバー・セキュリティ・コントロール（cybersecurity control）を実施するためのガイダンスが必要とされています。

1 Ransomware statistics: Who is targeted the most? Nordlocker (2021). https://nordlocker.com/ransomware-attack-statistics/
2 IBM (2022). X-Force Threat Intelligence Index 2022 https://www.ibm.com/downloads/cas/ADLMYLAZ
3 National Cyber Security Centre (2023). Cyber security for construction businesses https://www.ncsc.gov.uk/guidance/cyber-security-for-construction-businesses

建設業界のサイバー・インシデントとデータ侵害

一般に、収益が大きい大手建設会社ほど頻繁にサイバー攻撃を受けると考えられていますが、中小企業もサイバー・セキュリティの手順や管理が十分でない場合があるため、脆弱性が高い状況です。近年、世界で起きた建設業界に対するサイバー・インシデントやデータ侵害の顕著な例は次の通りです。

企業	年間売上高（想定）	サイバー攻撃の種類	攻撃の内容	被害結果
フランスの建設（資材）製造会社	478億米ドル	ランサムウェア（NotPetya）	17日間システムがオフライン	売上高で約2億5千万ユーロ、営業利益で8千万ユーロの損失
米国建設会社	9百万米ドル	ビジネスメール詐欺（BEC）	顧客からの請求書と称する電子メールを受信し、別の住所への送付依頼を受領	偽の請求書に対して21万米ドル以上の小切手送付
スイスの建設機械製造会社	38億米ドル	情報漏えい	企業はセキュリティ侵害による全拠点でのデータ盗難を公表したが、6百万米ドルに上る身代金の支払いは拒否	同社の事業予算、受注請求書類、銀行取引明細書を含む約4GBのデータの流出
米国建設会社	5千万米ドル	情報漏えい	同社が加入している医療保険制度に関連する情報への不正アクセス	従業員の機密データ流出後、サイバー攻撃が判明、システムをオフライン化し、独立系コンピュータ・フォレンジック会社に依頼

サイバー・インシデントやデータ侵害の根本的な原因には、以下のような外部要因と内部要因の両方が含まれます。

1

悪意のある攻撃
（ランサムウェアやマルウェアを含む）

2

不十分なセキュリティ管理

3

システムの不具合

4

従業員に関連した原因

- 不注意
（パスワードの紛失、ノートPCの盗難など）
- モビリティ（安全でないネットワークの使用）
- 不満のある現従業員、元従業員

建設業におけるサイバーリスクの影響について

適切なサイバー・セキュリティ対策が行われていない場合、サイバー・インシデントやデータ侵害は、数週間から数か月間発見されず、組織への被害と悪影響はさらに拡大する可能性があります。それにより、建設会社が受ける影響は、業務、人材、環境、財務、風評など多岐にわたります。

ダウンタイム
建設業界は、スケジュール通りにプロジェクトを遂行することが重要です。会社のソフトウェアや設備がサイバー攻撃を受けると、プロジェクトの遅延や事業中断につながる可能性が高くなります。

知的財産の侵害
企業が機密性の高い設計図や(電気機械などの)構造図を所有している場合、これらの漏えいにより、大きな風評被害や訴訟へ発展する可能性があります。

入札データの漏洩
入札戦略への不適切なアクセスにより、競争力の優位性や入札機会やプロジェクト自体の喪失につながる可能性があります。

労働者の負傷
設備機器の破壊や、物理的な制御が効かなくなった場合、労働者や第三者の負傷につながる可能性があります。

事業コスト
告知、身代金の支払い、法的サービス、データ復旧、事業中断による損失など、セキュリティ障害やプライバシー侵害に対処するための費用

秘密情報の漏洩
コンピュータセキュリティの障害に起因する、従業員、顧客、規制当局などの第三者への賠償責任

サイバー保険はサイバーリスクに適切に対応できるのか

進化する様々なサイバー脅威に直面する建設会社は、従来の保険契約に付帯されるサイバー免責や、サイバーリスクに起因する財物損害に対する保険会社の引受意欲が限定的なハードマーケット下では、サイバーリスクに対する保険ヘッジがより困難になってきているのが現状です。

工事保険の中核である**コンストラクション・オールリスク（CAR）**保険は、建設中の本体工事や仮設工事に対する物理的な損害のすべてのリスク（免責事項を除く）をカバーしています。保険会社は一貫して、LMA5400およびLMA5401条項によりCAR保険のサイバー・インシデントに対する完全な免責を規定しています。免責の範囲は以下の通りです。

免責事項[4]	LMA5400	LMA5401
サイバー・アクト：電子機器へのアクセスまたは使用に関わる不正、悪意によるもの、または犯罪行為に関連する損失または損害	不担保	不担保
サイバー・インシデントその1：電子機器へのアクセスまたは使用に伴う誤操作または不作為に関連した損失または損害	不担保	不担保
サイバー・インシデントその2：電子機器へのアクセス不能、または使用不能に関連する損害	不担保	不担保
データの使用不能または機能低下に伴う損失または損害	不担保	不担保
データの交換・復元	不担保	不担保
データの価値	不担保	不担保
ライトバック（復活担保）に関するシナリオ[5]	**LMA5400**	**LMA5401**
サイバー・インシデントに起因する火災や爆発による財物損害を補償	サイバー・アクトやデータ免責が優先される場合がある	不担保
サイバー・インシデントに起因する火災や爆発による事業中断を補償	不担保	不担保
保険補償対象のリスクにより電子機器が使用不能になった場合の財物保険または事業中断を補償	不担保	不担保

LMA5400およびLMA5401条項の免責文言は、サイバーリスクの原因（マルウェアやデータ漏洩など）ではなく、起こりうる結果に基づいており、免責が有効になるためには因果関係ではなく「関連性」だけが必要となります。CAR保険における制約は、操業開始遅延保険（付保している場合）の補償にも影響します。Marshは、新たなサイバー攻撃の状況により保険会社の見解が変化している分野を以下のように特定しました。

- 第三者賠償責任 (TPL)
- 工場および設備 (P&E)
- テロまたはポリティカルバイオレンス (PV)
- 海上貨物

4 https://insurance-endorsements.com/lma5400-and-lma5401-cyber-and-data-endorsements/
5 https://insurance-endorsements.com/lma5400-and-lma5401-cyber-and-data-endorsements/

サイバーリスクのリスクギャップを埋める

従来の保険では補償できないサイバーリスクが多くあることと、データを「財物」とみなし、破損したデータを「財物損害」とみなす判例がないことから、あらゆる業界の企業がリスクギャップに対処すべく、サイバーリスクに特化した保険の重要性を認識しています。

多くのサイバー保険は、第三者への賠償責任に加え、自社（被保険者）が被る非物的財物の損害に対する補償も提供しています。
しかし、その他の補償に関しては、大きなばらつきがあります。したがって、サイバー保険を購入する企業は、以下のような側面について補償が提供されるかどうか、またどの程度の範囲で補償されるか把握しなければなりません。

- **恐喝に対する費用**
- **データの消失と復元**
- **インシデントレスポンス費用**
- **情報漏えい賠償責任**
- **セキュリティ障害による賠償責任**
- **事業中断と臨時費用**
- **クレジット情報、個人情報のモニタリング**
- **規制措置**

最適なサイバー保険のあり方

サイバーリスク軽減のために保険の最適解を特定する最初のステップとして、自社のリスクとセキュリティ・プログラムの成熟度を評価する、**「マーシュ・サイバー・セルフアセスメント（英語版）」**を受けることをお薦めします。
日本語版については準備ができ次第、マーシュジャパンのWEBページより公開する予定です。

米国国立標準技術研究所（NIST）のサイバー・セキュリティの枠組に準拠して開発され、高度なデータと分析に支えられたマーシュ・サイバー・セルフアセスメントは、組織のサイバー・セキュリティ・コントロール、テクノロジー、人材について保険市場をリードする分析を提供します。

マーシュ・サイバー・セルフアセスメントは自社が晒されているサイバーリスクをマッピングすることで、リスクマネジメントの意思決定を正確に伝え、保険を含むリスクコストを最適化し、同時にサイバー保険の見積もり手続き簡素化というメリットも提供いたします。

マーシュ・サイバー・セルフアセスメントの主な特徴

- **無料**
  すべての企業に無料で提供され、自己診断の完了時にレポートが提供されます
- **安全性**
  使いやすいウェブベースのインターフェースで、アクティブ・ディレクトリ・コントロールや転送時・保存時のデータ暗号化など、業界をリードするセキュリティ・プロトコルを備えています
- **共有性**
  複数の関係者によるプラットフォームへの同時回答や記入を可能にし、1つのアプリケーションを効率よく、かつ重複やミスを回避しながら作成することができます。
- **包括的**
  サイバー・セキュリティの成熟度の全容を把握し、同業他社に対するサイバー・コントロールのベンチマークを行うと同時に、リソース配分に関する関係者の議論を促進することが可能です。
- **実用的**
  レポートにはリスクスコアが含まれており、サイバーリスクに対する脆弱性に積極的に対処することが可能です。
- **専門家との連携**
  マーシュのサイバーリスクおよび保険の専門家と連携し、レポートの理解を深め、リスクおよび保険のアプローチを調整し、保険会社と交渉することができます。

サイバー保険の活用とクレーム処理のニーズへの対応

お客様のニーズに沿った適切かつ競争力のあるリスクソリューションを実践し、サイバー・インシデントが発生した場合の保険クレーム処理について、信頼できるパートナーから支援を得ることができます。マーシュのサイバープラクティスのグローバルなプレゼンス、複数の専門分野にまたがるチーム、深い技術的専門知識、そしてオーダーメイド型のアプローチを活用することで、補償の拡充や大規模事故に備えたサイバー保険の調達、既存契約における特定の免責事項の復活担保などのメリットを享受することができます。

サイバーリスクが流動的で絶えず進化していることも、企業にとって課題となっています。保険約款の書きぶりによって、保険でカバーされる範囲やそれに伴う自社のコストが異なるため注意を要します。専門的な知識を持ち合わせているマーシュのクレームアドバイザリー部門が保険金請求の各種手続について支援します。

組織のサイバーリスクレジリエンスを高め、最適化されたサイバーリスクおよび保険に関する洞察とソリューションによって貴社が競争優位に立てるよう、マーシュの担当者にお問合せいただくか、マーシュ・サイバー・セルフアセスメントをお試しください。

本レポートに関するお問合せは以下までお願いいたします。

マーシュ ジャパン株式会社
03 6775 6001（代表）
Jp.Info-MJ@marsh.com

マーシュ ブローカー ジャパン株式会社
03 6775 6100代表）
Jp.Info-MBJ@marsh.com

〒107-6216 東京都港区赤坂9-7-1 ミッドタウン・タワー
www.marsh.com/jp/ja

About Marsh

保険仲介とリスクマネジメントの世界的リーディングカンパニーであるマーシュは、45,000名以上の従業員が130か国でデータに基づくリスクソリューションとアドバイザリーサービスに従事しています。マーシュは、リスク、戦略および人的資本の分野におけるグローバルなコンサルティング・ファームであるマーシュ・マクレナン（ニューヨーク証券取引所上場：MMC）の一員です。マーシュ・マクレナンの年間総収入は200億米ドル以上、マーシュのほか、ガイ・カーペンター、マーサーおよびオリバー・ワイマンを傘下に各分野で業界をリードし、お客様を支援しています。詳細情報については、marshmclennan.com, LinkedIn、Twitterをご覧ください。