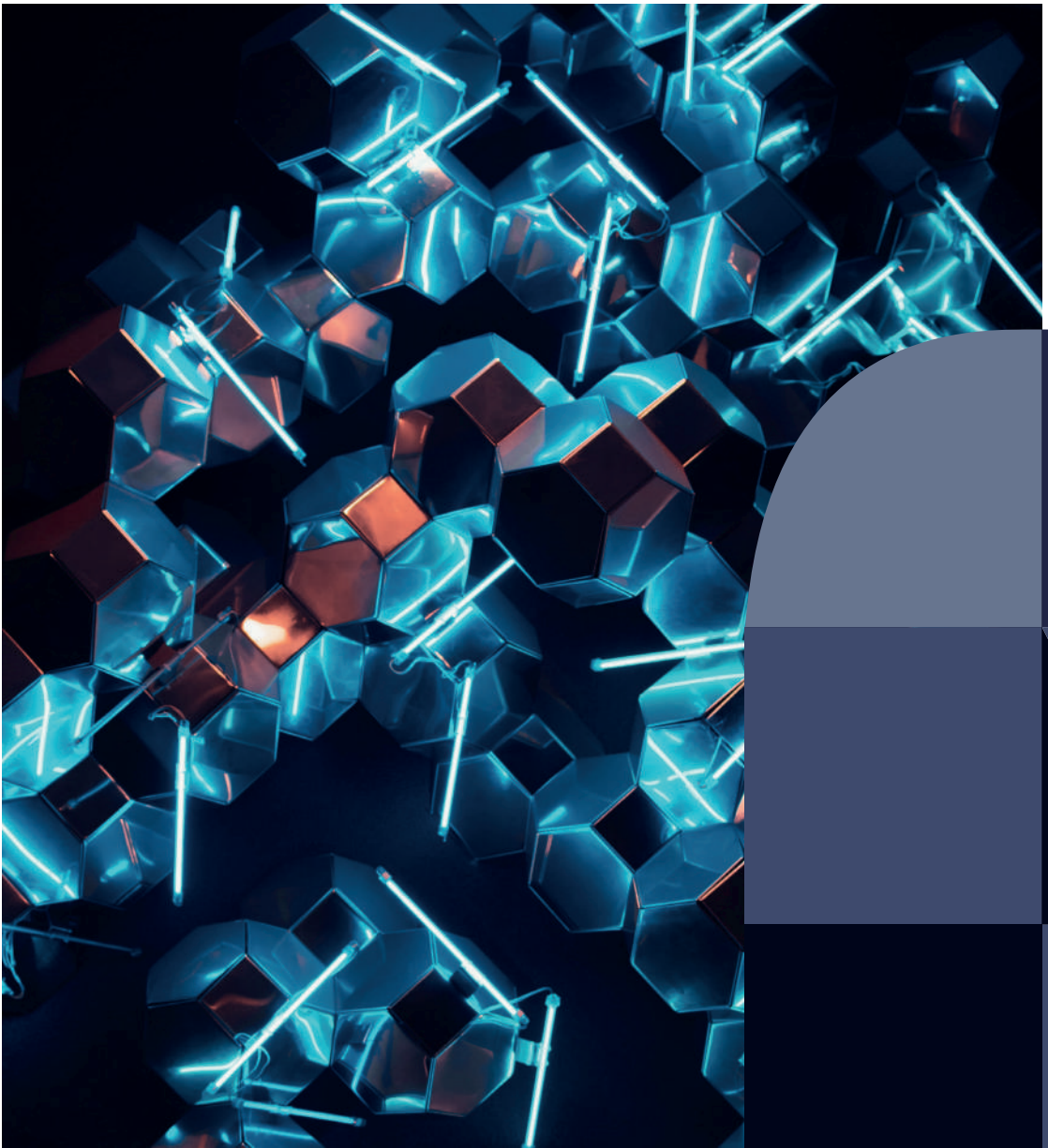
NTT DATA
Trusted Global Innovator

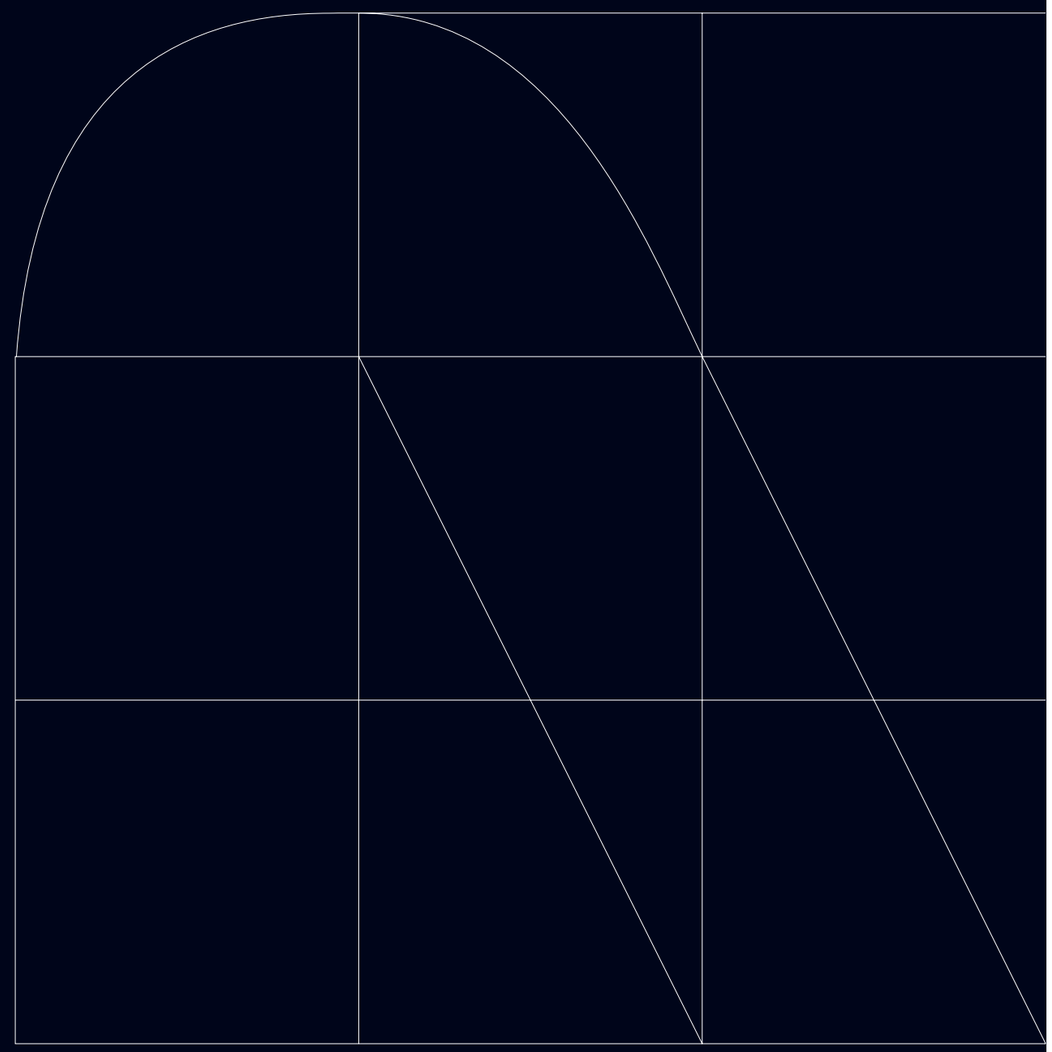
スマートなデータドリブン型保険の時代のセキュリティ強化

サイバーセキュリティの課題
ソートリーダーシップ



目次

3 概要
7 はじめに
8 保険業界のサイバーセキュリティについてのビジョン
12 デジタル化が進んでいる背景
13 _ デジタル成熟度という観点：完全デジタル化に向けての組織の活動
14 _ デジタル化という文脈のなかでのセキュリティの役割
15 _ DevOpsとセキュリティ：開発および導入のサイクル初期におけるセキュリティの組み込み
16 データドリブン型保険：プライバシーとセキュリティに対する保険会社の対応
17 _ サイバー攻撃のターゲットとしての保険会社
22 _ 保険のセキュリティを確保する
25 _ 保険会社の信用と評判を高める：クライアントにとっての透明性の重要さ
26 保険におけるサイバーセキュリティのベストプラクティス
27 _ 人中心のリスク管理
29 _ サイバー攻撃に対する保険業界の対応例
30 NTT DATAのサービスとユースケース
31 _ 保険会社が必要とするセキュリティの機能と管理
32 _ NTT DATAのサービス
33 _ ユースケース（匿名）
34 結び



概要

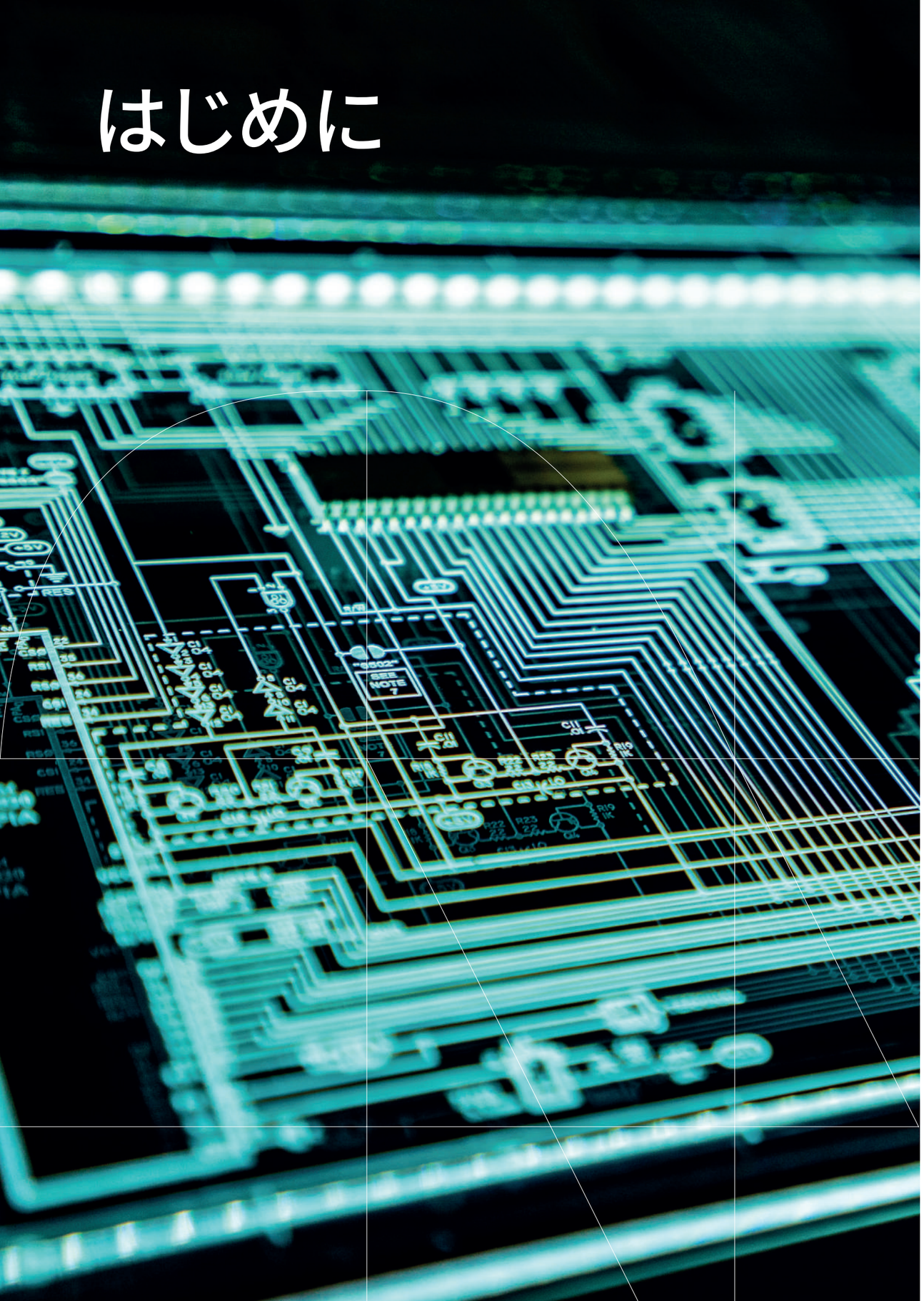
1. 保険は、サイバーセキュリティ攻撃の主要なターゲットの1つとなっています。そのため、この業界の企業は保険の商品およびサービスのセキュリティを確保するとともに、企業が保存している個人情報のデータプライバシーを改善することが望まれています。

2. 保険業界は、サイバーセキュリティ上の4つの主要な課題に直面しています。クラウドのセキュリティ、データドリブン型ビジネス、スマート化と自動化、およびデジタルワークフォースが、その4つの課題となります。これら課題は、セキュリティアジェンダにおいて、保険会社が強く意識すべき優先事項です。

3. サイバー脅威に対処するときには、予防と準備がきわめて重要となります。MAPFRE、CNA、SegurCaixaおよびChubbなどが、サイバーエマージェンシー対応計画の優れた一例となっています。

4. NTT DATAは、サイバーセキュリティ関連のエンドツーエンドのコンサルティングとサービスを行っています。これらのなかには、戦略、セキュリティ、ガバナンスとリスク管理、設計によるプライバシーとセキュリティ、リモート監視と迅速な対応、サイバーソリューション、およびサイバーセキュリティについての意識付けと人材提供などが含まれています。

はじめに



保険業界がデータドリブン型ビジネスになり、業界で活動している企業が、実用的なリアルタイムデータを活用することが必要であることを理解するにつれ、サイバー犯罪のターゲットとなるものも増加します。

保険会社は、ハッカーおよび国家の明確な興味の対象になり得る、膨大な量のクライアント情報を手元に持っています。そうなると、サイバーセキュリティが保険にとっての最大の課題の1つのとなり、保険会社は意思決定の際にそのことを優先事項とします。

それと並行して、保険会社のデジタルジャーニーでは、処理を自動化し、会社の業績全体に価値をもたらさない労働時間を削減する必要性がますます高まっています。この解決策は、インテリジェントなツールの実装か、リスクを検知および緩和する人間の努力のいずれかとなります。どちらのオプションでもセキュリティが不可避な、議論の余地のない前提となっていなければなりません。

さらに、ビジネスとテクノロジーの間のギャップが埋まりつつあり、保険会社は、サイバーセキュリティがビジネスリスクになっているということを理解しています。つまり、サイバーセキュリティはもはや当たり前のものでもなく、あるいは重要度の落ちる懸念のいずれでもあり得なくなっています。現在、CISO（最高セキュリティ責任者）たちは、最重要の意思決定に対する責任を負っており、他の重役たちと協力し合い、先頭に立って予期しなかった業務リスクに向き合っています。

進行中の変更事項と保険契約者からのきわめて厳しい要求に上記のすべてが加わることにより、このサイバーシナリオには十分な議論と継続的なテストが必要となります。

NTT DATAは、その保険対応能力とセキュリティに対する包括的なアプローチによって、現在のホワイトペーパーに記されている専門性と知識を活用し、この喫緊の事柄に関する一連の傾向、課題およびベストプラクティスを提供いたします。このレポートでは、テクノロジーとデータプライバシーが生き残りのために必要とされている時代で発展するために、保険会社が着目すべき、さまざまな領域および分野の機会、保険関連のサイバーセキュリティについての概要がハイライトされています。

保険業界のサイバーセキュリティについてのビジョン

サイバーセキュリティは、デジタルトランスフォーメーションを進めている現在の保険会社の大きな課題です。保険会社が保存しているデータの量が増えれば増えるほど、国家およびアタッカーにとっての価値が高まります。個人情報の場合は、なおさらです。

自社のサービス内容、業務および経営にテクノロジーを組み込むという世界的な課題に加えて、企業は、予期せぬイベントに対応するという、業界をクロスしたジレンマも認識しておく義務があります。これらのイベントには、パンデミック、自然災害、気候変動、第三者リスク、ESG関連リスク、またはこの文書のテーマであるサイバー攻撃といった、潜在的なリスクをもたらす可能性のある、予想不能な状況が含まれています。新しい業務上のリスクはこれらの予期せぬ状況から生まれており、業界の商品および製品についてもこれらのリスクを考慮する必要があります。これらの商品は保険会社によってアップデートされなければならず、保険会社には、これらの事柄に対して迅速に対応できる体制を整えることが求められています。

サイバーセキュリティには、保険会社が注意を払うべき、4つの共通する課題があります。それらは、以下の通りとなります。

クラウドのセキュリティ
ここ数年、クラウドへの移行が保険会社の優先事項となっており、クラウドのセキュリティが、企業のリスク管理アジェンダのトップに置くべきものとして浮かび上がってます。クラウドへの移行で業務を最適化するためには、保険会社は生産性とセキュリティのバランスをとる必要があります。これらの新しいテクノロジーは、新しい機能の提供および社内インフラストラクチャの拡大を新たな規模へと拡大させ、組織を間違いなく助けますが、セキュリティ基準を考えたアプローチをしないと、好ましくない結果を招くことになります。

しかし、企業が好むハイブリッドおよびマルチクラウド環境でのセキュリティ管理は複雑で、パブリックウラウドプロバイダー、プライベートクラウドプロバイダーを通じて、およびオンプレミスにおいての導入のいずれをもシームレスに機能させる方法とツールが必要となります。

データドリブン型ビジネス
現在、顧客データをもとにした戦略計画および意思決定を経営の基盤とする場合、保険会社は顧客のことを気にかけ、配慮する必要があります。保険会社は、より迅速に行動し、現代のこのような環境で競争上の優位をもたらす可能性のある他の勢力に遅れをとらないようにするため、データインテリジェンスを行うものになる必要があります。保険会社はできる限り機敏でいなければならず、機会だけでなく、この状況で絶えず出現するリスクにも迅速に順応する必要があります。

完全にデータ主導型の企業になることができたところは、売上増加、効率向上および利益率の改善が可能になっています。しかし、データ依存型になると、データのコンプライアンス、ガバナンス、データプライバシー、弾力性、監査などを対象とした、総合的な戦略を策定することが不可欠となります。

スマート化と自動化
電子メール、ウィルスやマルウェア対策、アプリケーションセキュリティ、データ暗号化、ネットワークとファイアウォールのセキュリティ、VPNなどのツールを効果的に実装していても、アラートやインシデントが発生した場合には、セキュリティという点では人間の介入がやはり必要となるでしょう。

さらに、ツールが改善されて誤検出を排除できるようになっても、あまりに多くの誤検出が検知されると、人間の手間が必要となります。

インテリジェントなテクノロジーを使って、時間のかかる繰り返しの多いタスクを自動化することによって、サイバーセキュリティチームは、より生産的な活動に注力できるようになり、正式な手順によって、修正可能な欠陥を識別できるようになります。同様に、自動化によってツールの標準化が容易になり、大きな出費につながる、膨大な種類のセキュリティツールの使用および実装を避けられるようになります。

セキュリティの自動化は、さまざまなサイバー環境での脅威の識別、エキスパートのアナリストが事前に定めていた意思決定方法に従った、潜在アラートのトリアージ、およびこれらの脅威に対応するための行動の判断で成り立っています。これらすべてが、人間が介入する必要なしに、数秒で行われなければなりません。これによって、時間のかかる、繰り返しの多い行動に費やす時間がはるかに少なくなり、さらに最適化されます。

デジタルワークプレイス

リモートワークが全世界の会社に広がっているというのは、目新しいことではありません。多くの社員がオフィス以外の場所で仕事をするようになり、ペリメータ・セキュリティ、パスワードおよび手動での許可管理に依存する従来のセキュリティ手法は、古くなっているだけでなく、不十分であることが証明されています。テレワーカーが、フィッシング、マルウェアおよびパスワード攻撃などのサイバー脅威のターゲットとなることが増えています。そのため、企業、とくに機密性がきわめて高いデータを使って仕事をしている保険業界の会社は、将来の問題発生を回避するための、ふさわしいセキュリティ手順を導入しなければなりません。

この点に関して、保険会社は、自社のロールベースアクセス制御（RBAC）の手法をすでに実施しているほか、リモートワークプレイスのセキュリティを強化する際の優先事項としてゼロトラストアプローチを採用しています。

これにより、組織のネットワーク、あるいはローカル、クラウドまたはハイブリッドのネットワークのいずれにつながっているのであれば、すべての従業員が、アプリケーション、データおよび文書にアクセスする際に認証、許可および検証されることが保証されるようになります。

保険会社がサイバーセキュリティアジェンダで真っ先に優先すべきことを分析すると、これらが「4大課題」となります。上記が「4大課題」となるのは、保険会社のサイバーセキュリティアジェンダにおける優先事項を分析する場合です。これら優先事項には、組織が焦点を当てるべき、不可欠な経営上および業務上の行動が伴います。さらに、経営と業務を横断した、会社内の中央集権的な行動も必要となります。セキュリティは顧客向き、内向きの諸刃の剣で、会社が顧客に提供しなければならないものでありながら、配慮していることを保証しなければならない内向きの施策でもあります。

デジタル化が進んでいる背景

デジタル成熟度という観点：完全デジタル化に向けての組織の活動

これまでの期間、保険会社は、顧客およびサプライヤーとの長期的な関係を維持するという目的でデジタルテクノロジーに移行してきており、市場投入までの時間に優れた新しい商品やマーケットを展開して、株主により高い価値をもたらしています。コンシューマライゼーションについてのマーケットでの既存のトレンド、利益率についての圧力およびエコシステムの統合とともに、パンデミックがリモートワークとオンラインでのステークホルダーエンゲージメントをもたらし、その結果、保険会社は、デジタルチャネルとバリューチェーンの自動化に加えて、通信テクノロジーを導入するようになっています。

デジタルテクノロジーのこのような緊急的な成熟は、商品とサービスのパーソナライゼーション、リアルタイムでの配慮と監視、仮想的なチーム管理およびスマートワーキングといった機会を保険ビジネスにもたらしているのは確かです。しかし、デジタル化に向けた、このような急速な動きにより、保険業界に対するサイバーアタックの成功率を高めることにもなっています。

現在、保険会社は、デジタルチャネルのセキュリティとデータの保護だけでなく、レガシーテクノロジーのセキュリティに対する責任を負うようになっています。多くの保険会社は、ビジネスプロセスにおいて、今もデジタルとレガシーのテクノロジーを組み合わせています。それにも関わらず、[1]世界規模の大手保険会社200社を対象としたACORDによる最近の調査によれば、真の意味でバリューチェーンをデジタル化させている保険会社は25%未満となっています。

このデジタル化という状況のなかでのセキュリティの役割

好調な成長指向の企業は、デジタル化戦略を導入し、デバイスと人の接続を促進しているはずです。ただし、同時に自社の情報システムの安全性を油断なく観察して行動を起こしているはずです。

保険会社は、履歴情報、専門業務賠償責任保険（PII）、財務および健康についての情報といった、保険契約者についての詳細な情報を集める必要があります。これらの情報によって、保険契約者がサイバー犯罪のターゲットになるのは疑いようもないからです。
保険での主要なサイバー犯罪には、ランサムウェア、ソーシャルエンジニアリング（フィッシングなど）、サービス拒否（DoS）攻撃、完全なサービス中断、データ漏洩および侵害があります。

この点を考慮すると、サイバーリスクがこの業界にとっての最大の業務リスクとなっているため、サイバーセキュリティが保険業界のビジネスにとって不可欠なものとなっています。これまで、サイバーセキュリティは、CIOの組織内で扱われ、そのために優先順位が相反するときも、サイバーセキュリティのための予算とリソースが限定されているセキュリティ組織内でのITリスクと見なされていました。

もっとも、多くの保険会社は現在、新たに登場しているサイバー脅威と業界に対するリスクを根拠として、サイバーセキュリティはビジネスリスクであると理解しています。修正された組織構造では、CISOがCEOの直属となっています。サイバーセキュリティリスクの管理には、予算およびリソースに対する取締役レベルの支援が頻繁に行われており、保険会社はサイバーセキュリティの対処に戦略的なアプローチをとっています。従来のコンプライアンスと「チェックリスト」を使うようなマインドセットから、ソフトウェアのライフサイクルの初期からサイバーリスクを能動的に管理するという変化が起こっています。

最上位の意思決定者として、CISOは他の重役たちとともに、最初にサイバーリスクアセスメントを実施し、さまざまな保険ビジネスに潜んでいるかもしれない脆弱性をマッピングして、潜在的な損害を査定しなければなりません。その後、対応戦略がサイバー緊急事態対応プランの形式で実施され、サイバー攻撃の発生時にとるべき、具体的な行動が案内されなければなりません。

好調な成長指向の企業は、デジタル化戦略を導入し、デバイスと人の接続を促進しているはずです。同時に、自社の情報システムの安全性を観察して、行動を起こしています。

サイバーリスクがこの業界にとっての最大の業務リスクとなっているため、サイバーセキュリティが保険業界のビジネスにとって不可欠なものとなっています。

DevOpsとセキュリティ：開発および導入のサイクル初期におけるセキュリティの組み込み

それぞれの保険会社はさまざまなな方法でDevOpsプロセスを実装できる程度の自由さはあり、明示されたルール、関連の責任および所有権を定める責任をも負っています。DevSecOpsを導入する程度に発展し、開発ライフサイクルの初期からセキュリティを組み込んでいる会社もあります。さらに、アプリケーションのローンチがプロセスの各フェーズで加速しており、アイデンティティ管理、ファイアウォールまたは脆弱性スキャンといった、いくつかのセキュリティ機能が実行されています。

プロセスのあらゆる段階でセキュリティの脆弱性をチェックする以外にも、DevSecOpsは、保険会社向けの、その他の優れた利点も活用します。これらの利点によって、保険金請求の処理と正確な見積もり提出、非効率的なプロセスの自動化による無駄な労働時間の削減と高品質な商品の作成、あるいは法規制の遵守が可能になり、競争上の優位を得ることができます。DevSecOpsの処理により、データを実用的なセットに変えることも可能になるため、エラーが減ります。それと同時に、役に立つ分析と実施可能なフィードバックが生成され、よく構造化されたコードが保証されるため、導入を成功させることができます。

ただし、その反面、DevSecOpsは、いくつかの課題に直面するかもしれません。セキュリティプロセスに関与する従業員の場合、その可能性が高まります。[2]Gartnerによれば、開発者の再トレーニングが明らかに必要となっていますが、保険会社が、DevOps開発者に対して「情報セキュリティの古い、重々しい、チェックポイントを中心としたプロセスを強制」するのはできないことです。その代わりに、「CI/CD」ツールチェーンとプロセスの全体にわたって、継続的なセキュリティ保証をシームレスに組み込むのだと心に留めておく必要があります。

アナリストが言うには、DevSecOpsも同様に、マインドセットと開発の文化プロセスが変わりつつあるようで、セキュリティスキャンを使った、1回限りのゲートチェックから、継続的なセキュリティ保証プロセスへと移行しています。

もっとも、脆弱性ゼロのアプリケーションを作成するという発想が開発者の足かせとなっているため、Gartnerでは、開発者が、脅威モデリングを通じて識別された、最も重要なセキュリティに集中するように推奨しています。

さらに、ソフトウェアライフサイクルでのセキュリティに対する当社のアプローチは、ソフトウェア開発ライフサイクルの各フェーズで実行されなければならず、セキュリティについて要件と制御をすべて定めているセキュアな開発モデル（OWASP SAMMをもとにしたもの）を実装することが基本となっています。このモデルから、プロジェクトのセキュリティ監督を行う、セキュリティオフィス、ならびにセキュリティチャンピオンプロファイル（チーム内のセキュリティコーディネーター）の導入をもとにして、組織のセキュリティ構造が作られます。

このセキュリティオフィスは、プロジェクトまたは会社のCI/CD内でセキュリティ制御を統合させ、各フェーズでプロジェクトの実施すべきセキュリティ制御を定める役割を負います。これらのテストをセキュリティチャンピオンとともに実施および監督し、検知されたリスクに対するアクションプランを決定するのが、セキュリティオフィスの責任となります。

このプロセスの全体がダッシュボードを通じて監視されていなければならず、それによって、その状況のために生成された、セキュアな開発モデルという観点から、それぞれのプロジェクトおよび/またはセキュリティチャンピオンのコンプライアンスレベルが分析できるようになっていなければなりません。この方法により、ノンコンプライアンスとなっている領域を検知し、適切な方法で対策を講じることが可能になります。

自動化は、実施される制御の数を拡大できるようにするツールですが、私たちの考えでは、そのレベルのリスクを緩和するためのカギとなるのは、管理です。

データドリブン型保険：プライバシーとセキュリティに対する保険会社の対応

サイバー攻撃のターゲットとしての保険会社

すでに見てきたように、デジタルトランスフォーメーションは多くのことを保険業界にもたらしています。データ中心のアプローチにより、新しい収益源の創生、正確な引受、リスクの削減、最適化およびパーソナライズされた顧客とパートナーの関係が可能になります。
顧客エクスペリエンスの改善と取引のスピードアップに向けた取り組みにより、保険業界は、データを業界のまさに中心に据えることによって、アプリケーション開発と自動化に焦点を当てるようになっています。データと自動化は保険を「よりスマート」にし、その結果、データ分析の結果を反映した料金の迅速な調整と損害可能性の傾向特定が可能になっています。自動車のスマートセンサーまたは個人向けフィットネスデバイスは、健康保険または自動車保険に影響を与える可能性のある、ライフスタイルについての遠隔測定を提供しています。プライバシーに関する消費者の大きな懸念は、より安い保険料への希望によって相殺されるかもしれません。デジタルへの依存が高まることにより、保険はより大きな成功を収められますが、増加するサイバーリスクに晒されることもあります。そのため、保険業界はこの課題に立ち向かおうとしています。消費者は、保険会社が自分たちのデータを安全かつ適切に、プライバシー要件に整合するかたちで取り扱っているという、より大きな保証を必要としています。

ただし、保険業界のデジタルトランスフォーメーションは、レガシーのシステムと手作業の比率が高いプロセスが障害となっています。パンデミックがこの状況を浮かび上がらせており、保険のプロセスとシステムのデジタル化についての注目が高まっています。[3]Gartner の記事「How Leading Insurance Companies Manage Legacy Modernization（大手保険会社がレガシーの近代化をいかに管理しているか）」によれば、デジタル成熟度が高い保険会社は、デジタル成熟度が低い会社に比べて、コアシステムの近代化目標において計画を上回る可能性が2倍になっています。ただし、保険会社のおよそ50%では、コアシステムの50%以上でレガシーのシステムを活用しています。Gartnerでは、IT予算の65%がビジネスの「保守運用」に割り当てられていることも発見しています。もっとも大きな成功を収める保険会社とは、自動化を導入し、効率的でパーソナライズされたサービスを提供できる保険会社となるでしょう。

保険で真っ先に優先すべきこととしてセキュリティを考えた場合、以下のような課題が立ちはだかります。

増大する、規制当局からの圧力

私たちがオープンインシュアランスに向かっているという状況下では特にテクノロジーの進歩は、とても速いペースで進んでいます。さらに、保険業界の規制も同じような速さと強度で進んでいます。当社の[4]「InsurTech Global Outlook 2022：保険規制」でお知らせしたように、保険業界に直接的および間接的に影響を与える規制は数多くあります。そのなかには、ローカルで適用されるものではあるものの、Solvency または IFRS 17のように国際的なものもあり、他の多くは国または州を対象としたものとなっています。
それにも関わらず、世界中の保険会社は、既知の攻撃だけでなく、その後に誕生したすべての規制に適合する必要性にも影響されています。

世界中の多くの国または連邦の政府は、悪意のある者から消費者のデータを保護する目的だけでなく、保険会社の事業運営で消費者のデータが悪用されるのを防ぐ目的でも、データプライバシー法を制定しています。これらのプライバシー規制に従わない場合、保険会社は制裁金という民事責任を問われる可能性があり、さらに評判を損なうことにより、新しい顧客の引き留めおよび獲得が困難になります。そのため、これらの法律に従い、消費者のデータを保護することは、保険会社の最優先事項となります。

消費者のデータを保護していることを確認するために保険会社ができることは、自身の地域で施行されているプライバシー規制についての認識があるかどうか、[5]FIPSの指針に合致したデータの使用について内部の関係者を教育しているかどうか、セキュリティ態勢を向上しているかどうか、さらにデータプライバシーに対する消費者の懸念を認識し、それに対処しているかどうかを確認するということになります。

1. データプライバシーと保護についての規制

ここ数年、人々のデータのアクセスおよび処理について、さまざまな法律が施行されています。それぞれの国の状況が違うため、これらすべてが異なった対象範囲を持っているのは間違いありません。個人データを扱う際に企業が果たさなければならない義務ということになると、より制限の厳しいルールとなっている場合もあれば、それほど要件が厳しくなっていない場合もあります。

これまで作られてきた、もっとも重要はプライバシー法は、欧州の**EU一般データ保護規則（Data Protection Regulation：GDPR）**で、これは2016年に施行されましたが、2018年5月25日まで適用されませんでした。それ以降、この規則の基準に則った、その他の法律が数多く世界中で策定されるようになり、欧州連合の住民の個人データを使って業務を行っている、すべての企業に対して、データの適切な使用を保証するために、厳しいプロトコルを適用することが求められています。

全世界に関わるものではあるものの、GDPRがデータプライバシーに関係する唯一の規則というわけではありません。北米では、**1999年金融サービス近代化法（Financial Modernisation Act of 1999）**とも呼ばれる**グラムリーチブライリー法（Gramm-Leach-Bliley：GLBA）**により、米国の金融機関（商業銀行、投資銀行、証券会社および保険会社）が顧客の個人情報を取り扱う方法が定められています。

一方、カナダでは、民間部門の組織を対象とした連邦プライバシー法である**個人情報保護および電子文書法（PIPEDA）**が制定されています。

中南米では、**ブラジルの個人データ保護についての一般法**が代表的な法律となっており、アジア大陸では多くの国がそのための法律を定めており、**韓国の個人情報保護法**、中国の**個人情報保護法**、あるいはタイの **個人情報保護法**などがあります。**日本の場合は、個人情報の保護に関する法律**が2022年に改正されています。

そのため、プライバシーという点に関して言えば、規制によって大きな違いがあります。国または地域によって、さまざまな重要さおよび厳しさを持った規格が必要とされています。しかし、確かなことは、これらの法律はすべて、企業がより積極的にデジタルプラットフォームを使い、製品またはサービスを売り出そうとしているなかで、企業によるデータ使用から人々の権利をよりしっかりと保護することを目指しているということです。

保険会社の場合も、上記の法律または規制に従っていることを保証しなければならないため、状況は他のセクターとそれほど異なっていません。これを実現するために、保険会社は、独自のソリューションを開発することも、あるいはサードパーティーとの提携を活用することもできます。通常、このサードパーティーは、テクノロジーの応用によって、規則セキュリティおよびコンプライアンスの要件またはニーズを満たす方法を熟知しているものとなります。ただし、保険会社は、自社の膨大な量のデータを処理および管理する責任を負っているクラウドサービスプロバイダーのような、他の大きなパートナーも持たなければなりません。

2. リスク管理と規制

2020年9月、欧州議会と欧州委員会は、EUの金融サービスセクターでのデジタル オペレーショナル レジリエンスについての法制に関する草案を提出しました。将来の法律となる**デジタル オペレーショナル レジリエンスに関する規制（Digital Operational Resilience Act：DORA）**は、保険会社および再保険会社を含む金融セクターの情報通信テクノロジー（ICT）に関係するリスク要件を強化およびアップデートし、これら業界のすべての関係者が共通のシステムのもとで業務を行い、特定のテクノロジーの使用から派生するリスクを避けられるようにすることを目的としています。

DORAは、金融システムのすべての参加者が、サイバーアタックおよび他のリスクを緩和するための必要な保護手段を持つようにすることを目指しています。立案されている法制では、企業はICT関連のあらゆる種類の脅威およびディスラプションに耐えられるようになることが求められるでしょう。この立案では、クラウドサービスプロバイダーのような、重要なサードパーティーのプロバイダーを対象とした監視フレームワークも導入されます。

その目的は、潜在的にきわめて重要な存在であるICTサービスプロバイダーを含む、この業界のすべてのメンバーが、サイバーアタックと他のタイプのリスクと戦えるようになるための必要な手続きを定めることにあります。そのため、企業は、サービス妨害のようなデジタル脅威およびその影響に対処できることを示さなければなりません。新しい法律は企業（銀行および保険会社）を対象とするだけでなく、上記の企業にサービスを提供する企業にも効力が拡大することも目指していますので、クラウドサービスプロバイダーのような、重要なプロバイダーにもこのルールは適用されます。

この法律の斬新な点の1つは、さまざまな規定に広く分岐している、この件に関する現状の法律との調和がとられるということです。

他方、この草案の提出からは、欧州保険・企業年金監督局（European Insurance and Occupational Pensions Authority：EIOPA）、欧州銀行監督局（European Banking Authority）および欧州証券市場監督局（European Securities and Markets Authority：ESMA）がその準備に積極的に参加してきたことから、各機関の集約という目的も見られます。

脅威の発見とリスクの定量化をより早く行う必要性
予期せぬイベントが増えれば増えるほど、その影響を予見し、損害を受ける前に、適切に行動することについて考慮しなければなりません。しかし、これらの予測不可能な状況がより頻発に起こっており、リスクと脆弱性をより早く検知する必要が高まっています。まったく不明というわけではないものの、迅速な行動をとるためにはより注意が必要という状況にも、同じことがあてはまります。気候変動はその一例でしょう。

不透明な状況が拡大しているなか、リスクを検知する必要が高まっています。保険組織は、リスクの検知、定量化および緩和を急速に行う仕組みを必要としています。そのため、企業が起こり得るリスクを自主的に監視するなかで、すべての関係者がコミュニケーションリスクを緩和するために、リスク管理の文化に参画していることを確認しなければなりません。さらに、リスクが実体化すれば、保険会社は効果的な対応および復旧を行う必要があります。

一般的に使用されているリスク緩和ツールには、低リスクと高リスクの可能性があるシステムの概観を容易にするリスク評価フレームワーク (RAF) や、確率マトリックス、SWOT、根本原因分析などがあります。

好ましくないイベントが起こる可能性を下げることは可能です。通常業務への迅速な復帰は、ガバナンス、リスク管理およびコンプライアンス（GRC）

プラットフォーム上で事業継続計画を管理し、ITと事業目的を整合させながら、リスクを管理し、規制コンプライアンスに対する要件を満たすことで、可能となります。

これによって、事業の中断を計画に織り込むことができ、それによって、その頻度と影響を抑制することができます。

事業継続は、同じようなシンプルな方法とサードパーティーを使うことによって評価することができます。資産の利用可能性および重要性を判断するには、リスクアセスメントを行うのがいいでしょう。次のステップは、資産、管理およびポリシーを結びつけて、リソースの依存度を調査および確認することです。事業への影響を評価し、ディスラプションによる財務への影響を判断しましょう。GRCプラットフォームが、復旧チームのメンバーが会社を去った場合に対処する必要がある領域を明らかにするでしょう。

不正とマネーロンダリング

カスタマイズされたCXの必要性と保険マーケットでの競争が高まるにつれ、不正およびマネーロンダリングといった不正目的のものも増えています。当社の[6]2022 Insurance Visionで証明されているように、悪意のある目的を相手にした世界的な戦いが、保険業界の3大課題の1つとなっています。

保険業界にとって、不正はまだ潜伏中であり、COVID-19危機によって、より多くの関わりと注目を得る一方となっています。[7]Coalition Against Insurance Fraudは、不正によって米国の業界はすべての保険種目にわたって800億ドルの損害を被っていると試算しています。

業界全体でバリューチェーンのSTPへの注目が高まっていますが、そのためにはデータおよび機械学習/AIテクノロジーを活用した、リアルタイムでの不正検知が必要となります。パンデミック中は、車両および商業用不動産の使用が減り、重要性の低いサービス業界が一時的にシャットダウンされていたにもかかわらず、不正が増加しました。

不正の増加は利益率に直接的な影響を及ぼし、保険契約者の保険料が上がることになります。保険会社は、不正行為の初期検知については、機械学習/AIテクノロジーへの移行を進めています。

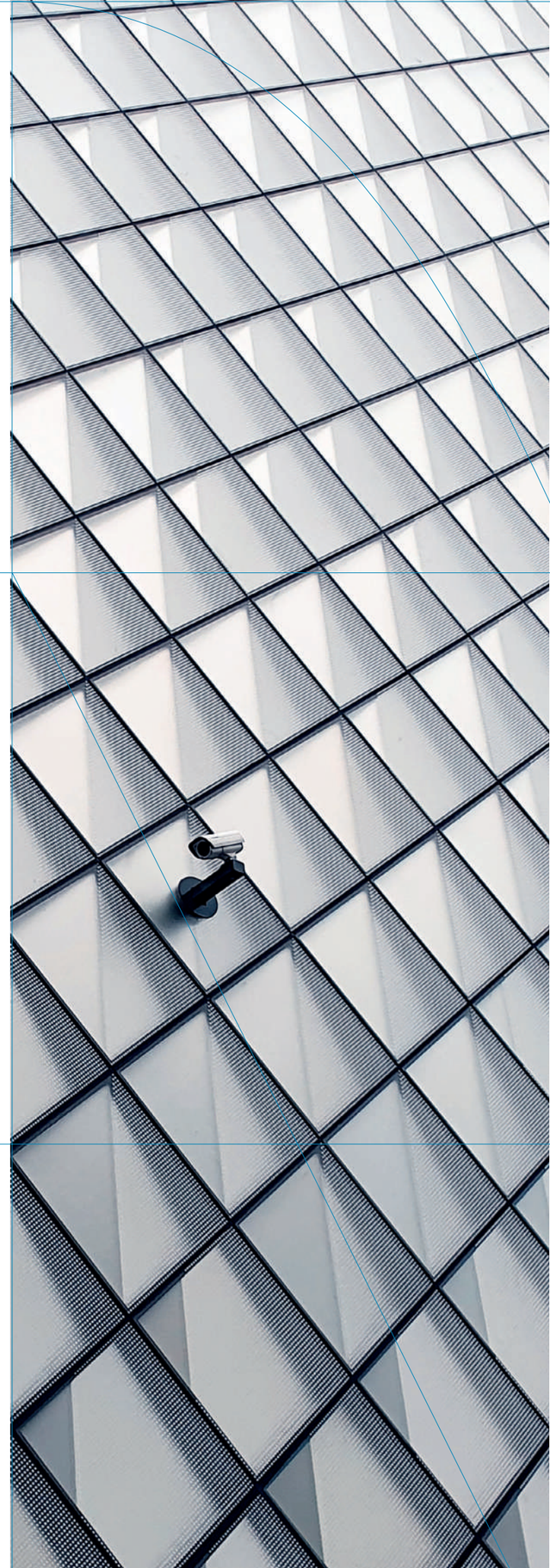
サイバー攻撃

潜在的なサイバー脅威となる主要な領域には、顧客のポータル、クレジットカード取引、クラウドのデータストレージ、B2BとB2Cのポータル、データレイク、規制によるリスク、アプリケーションを狙った攻撃、セキュリティ制御および保険の詳細などのクライアント情報があります。

ハクティビストはイデオロギーを理由として保険加害者を狙っていると知られており、B2C保険契約者の個人情報も、詳細な情報が多く含まれているため、国家の支援を受けた脅威アクターにとって有用です。保険会社に違反があると、サイバー犯罪者は、保険契約の詳細およびサイバーセキュリティー保険顧客のセキュリティ基準を知ることができ、その後に盗まれた情報を使って不正またはサイバー攻撃を行えるようになります。国家の支援を受けた脅威アクターは、インテリジェンスおよび捜査活動でも、盗まれた情報を使用することができます。

国家の支援を受けたインテリジェンスサービスは、集めた個人情報を検索可能なデータベースに取り込むことで、それに対する標的型のクエリを実行し、さらなる攻撃ベクトルが可能となります。

アプリケーションを狙った攻撃も主要な脅威です。エラーは人間につきものですが、アプリケーションのコーディングにエラーが発生すると、組織への攻撃を可能にする脆弱性が生まれます。組織は、脅威のモデリングから始まり、侵入テストとウェブアプリケーションのファイアウォールを含む、すべてのサイクルを対象としたセキュリティ制御を構築する必要があります。



保険のセキュリティを確保する

上記のような課題と要件があるため、セキュリティは、保険業界にとってきわめて重要なものであり、組織にとっては必須のものとなっています。ただし、セキュリティにはさまざまな形状とサイズがあり、「どんなものにも通用するもの」という発想は組織では減りつつあります。

そのため、保険は以下のような方法でセキュリティを確保することができます。

設計によるセキュリティ
保険セクターは行動を起こし、製品およびサービスの開発ライフサイクルのすべての段階にサイバーセキュリティについての懸念を織り込み始めなければなりません。顧客エクスペリエンス、可用性、セキュリティまたはプライバシーについては、かなり考慮する必要があります。ビジネスを支えている、IT アーキテクチャの基盤は、最初に紹介したような、ゼロトラストのフレームワークになっていなければなりません。

データセキュリティ
完全にリスクフリーな職場の構築は不可能です。データの暗号化は、ゼロトラスト環境での使用、伝送および安心のためにセキュリティ上不可欠なものとなっています。きわめて重要な個人情報を保有および処理しているセクターでは、ポリシーベースの暗号化を実現する、Microsoft Information Protection のようなソリューションが欠かせません。

アイデンティティ
すべてのセキュリティの基本となるものはアイデンティティです。自社のシステムにアクセスしている人物が本当に適切なレベルの信頼を寄せられる人物であるかどうかを確認できないのであれば、信頼を築くことはできません。すべての保険会社は、真実とアイデンティティで構成されたアイデンティティソースを構築し、生成および削除が、特権を付与されているアカウントを中心に、安全に処理されていることを確認するという戦略に従うべきです。

パスワードのいらない認証
サイバー保険引受人は、適正なセキュリティ基準についての関心を高めつつあり、現在、これらの多くが多要素認証を必要としています。保険セクターが、内部での使用、ならびに B2C および B2B のエンゲージメントで、強固で、できればパスワードのいらない認証を推し進めているのは理解できます。

リスク管理と強固なガバナンス
リスク管理は保険のコアとなるものであり、したがって、サイバーリスクの管理が組織のエンタープライズリスク管理に組み込まれているべきです。サービスプロバイダーとなる、クラウドサービスプロバイダーやソフトウェアサービスプロバイダーといったサードパーティーの利用が増えることで、責任分担の枠組みが生まれるようになります。組織が最高の結果を出し、とろうとしているリスクに対抗できるようにするためには、すべてのアウトソーシング方法にしっかりとしたガバナンスレイヤがそなわっていることが必要となります。

ビジネス E メールのセキュリティ侵害とフィッシング攻撃
E メールは今もよくある攻撃ベクトルとなっています。私たちは、潜在的にリスキーである E メールをフィルターまたはハイライトするセキュリティ制御を可能にするテクノロジーによって、ユーザーがより良い決定を下せるようにすることができます。ビジネス E メールのセキュリティを高めるためには、DMARC、SPF および DKIM を組み合わせて使うのがいいでしょう。電子メールに [External] というマークを付けると便利であるだけでなく、Microsoft Teams または Google Chat といった IM での内部通信が奨励されるようになるかもしれません。また、フィッシングのテストを定期的に行い、低リスクの意思決定を奨励する、セキュリティ文化を育むようにしましょう。

ネットワークセキュリティは、保険販売がリモートで行われ、高度に分散しているという特性に左右されます。セキュアサービスエッジテクノロジーにより、費用の削減が可能になるとともに、強固なセキュリティ対策を施しながら、ベンダー管理に関係するリスクを抑制できるようになります。ゼロトラストネットワーキングのアプローチにより、すべてのネットワークトラフィックを暗号化および監視することで、機密全体をセキュアな状態に保てるようになります。

保険会社はリスクアセスメントによって潜在的な問題を把握し、顧客をできる限り保護しようとします。そのため、サイバー保険が、保険会社のなかでより一般的なものとなりつつあります。この保険により、サイバーセキュリティインシデントを原因とする損失から保険会社を保護することが可能になります。サイバー保険がより多くの保険会社に利用されるようになっており、セキュリティに対するクライアントの要求はますます厳しくなっています。成功したサイバー攻撃および国家の支援を受けたサイバー攻撃が検知されると、リスクが高まり、保険会社の実行すべき要件にも影響し、保険会社はその後に自らの組織に保険をかけることになります。

保険業界は支払いを減らす必要があり、そのまさに特性として、引受によってリスクの範囲が示され、潜在的な脆弱性に大きく晒されているクライアントは対象から除外されています。クライアントが多要素認証を行っていない場合、保険会社は損失を補うことがありません。これによって、企業が保険をかけ続けられるようになるために実装しなければならない、サイバーセキュリティ管理の普及が促進されています。

対処しなければならない現状の課題および要件があるため、セキュリティは保険業界にとってきわめて重要なものであり、組織にとっては必須のものとなっています。

サイバー保険が、顧客の保護を最大限に高めようとしている保険会社のなかで、より一般的なものとなりつつあります。

保険会社の信用と評判を高める：クライアントにとっての透明性の重要さ

潜在的顧客および既存の顧客による信頼を築くのは、保険業界にとって、つねに最大の懸案となっています。保険の特性、複雑な提案および価格モデルがクライアントの不信を招く原因となっているのかもしれません。

さらに、ユーザーがさまざまなタイプの会社だけでなく、マーケットや業界に個人データを伝えるかもしれないという懸念が高まっています。データドリブン型保険には、カスタマイズされたソリューションによる顧客エクスペリエンスの向上、既存の顧客のターゲット増加、リスクの正確な識別、ならびに保険の新しい対象といった、数多くの利点がありますが、顧客の懐疑の的ともなっています。

保険会社が透明性を保ち、保険契約についての明確で、ミスのない説明を行うようになるように求める消費者がどんどん増えています。こうなることで、消費者は、保険の対象と他の商品より優れている点を理解できるようになり、消費者エンゲージメントを高められるようになります。

しかし、保険会社は、どのようにすれば完全な透明性を保証でき、すべての消費者の信頼を得られるようになるのでしょうか。保険契約者に納得して貰うようになるには、以下を考慮する必要があります。

意思決定の過程でプライバシーとセキュリティーを最優先する
テクノロジーとビジネスは一体となって進歩します。セキュリティとビジネスもそうならなければなりません。プライバシーは全社的なレベルで達成され、他の重点イニシアティブに対するのと同じように、リーダーはセキュリティを理解し、セキュリティに注意を払わなければなりません。

システム、処理および運営をアップデートする
保険会社は既存の手順を発展させなければならないだけでなく、クライアントから得たデータを正しく使っていることを保証する、新しい手順も作り出さなければなりません。このことは、新しいインフラストラクチャおよび能力（人、財務およびテクノロジーの能力）の構築について考え始め、最大限の倫理的振る舞いを保証しながら、データを活用できるようにすることの必要性を示しています。

新しい規制に継続的に適応する
前に指摘した規則は、現在のサイバーセキュリティについての法規制全体の一部にすぎません。ただし、さまざまな地域の法人の規制は、この文書を読めばわかるように、進化しています。これら法人は、業界のテクノロジー、製品およびサービスの絶え間ない進化に積極的に適応しようとしています。そのため、保険会社は、求められる前に説明責任を果たさなければならず、そのことによって、データ活用とデータ倫理のバランスを保たなければなりません。

全体的には、既存の顧客と見込み客からの信頼を得るには、正直に真実を伝えることが最善の策となります。セルフサービスのUXとわかりやすい情報をユーザーに伝え、ユーザーのデータがいつ、どこで、どのように使用されるのかをわかりやすく伝え、完全に理解してもらえるようにすることで、保険会社はユーザーとの関係を構築できるようになるでしょう。

保険におけるサイバーセキュリティのベストプラクティス

人中心のリスク管理

人間に起因するリスクへの対処は、最も効果的であるのに過小評価されているリスク管理戦略の1つです。社員がフィッシングメールのリンクをクリックすることがよくあり、ソーシャルエンジニアリング攻撃中にアクセス権と情報を提供するように操られることもあります。これら社員は弱いパスワードを使っているかもしれませんし、悪意のあるハードウェアを偶然ダウンロードしたり、あるいはセキュリティインシデントを引き起こしやすいエラーに関係したりしているのかもしれません。これらのリスクを軽減するには、結局のところ、社員の適切な意識、知識および行動を生み出すしかありません。

[8]スタンフォード大学の人間のエラーについての研究 によれば、サイバー犯罪者はこのような弱点につけ込んで、機密情報をハッキングしようとしています。88%ものセキュリティ侵害は人間のミスが原因となっており、攻撃の37%ではEメールおよび手紙が侵害の根本的な原因として関わっていました。情報セキュリティ保護を強化するためには、企業は人に対する準備を高めることに焦点を当てなければなりません。投資および集中化が、ITインフラストラクチャ、制御およびCISO主導のプログラムを中心に継続されるべきですが、人的要因がかなりのリスクであることに変わりはありません。私たちは、組織が直ちに優先して、効果を及ぼすことのできるものとして、次のような3つの注目ポイントを上げています。

リーダーが足並みを揃え、上層部全体から可視化する
全体として、最高人材活用責任者および最高学習責任者の戦略およびビジネス目標と整合している必要があります。最高リスク責任者とのつながりをより綿密に、より公的なものにすることにより、文化、意識、およびその会社の全社的なリスクプロファイルをもとにしたトレーニングに着目した、人間中心の戦略との整合性が生まれます。

リスクをベースにした文化の組み込みは、トップより始まります。具体的なリスクについて教育を受けたリーダーは、責任ある代弁者となり、セキュリティの重要さを強調し、伝えることができます。企業は、経営陣が会議や毎日の行いのなかで率先してセキュリティの顔と声になるようにしなければなりません。

厳しい、不透明な時期にはなおさら、リスクマネージャーは、効率的なリスク管理プログラムのチャンピオンとして振る舞う機会を得ます。たとえば、新型コロナウィルス流行の初期、チームはリーダーに、指示、透明性、およびもっとも重要なこととなる計画を求めました。強いリーダーはこの機会を活かしてリスク評価を行い、顧客、組織の資産、関係者および社員を保護するための戦略を策定しました。

組織全体にわたってセキュリティの文化を構築する
ほとんどのリーダーは、社員の変化とコンプライアンスは、1日にして、あるいは1つのトレーニングプログラムで起こるわけではないと理解しています。その代わり、最良の企業は情報に対する意識とリスク重視のセキュリティを文化に組み入れていました。文化は信念と行動を、最高に設計された、制御できないレベルにまで引き上げます。振る舞いを呼び起こすという意味では、文化は、リスク全体を管理する上での「第4のディフェンスライン」になり得ます。そのため、長期的な振る舞いを育みたいと願うリーダーは、リスクが結果を左右すると認識しなければなりません。

持続可能な文化変容を実現させるための最初のステップは、意識喚起と教育です。組織のリスク意識喚起キャンペーンにより、動画やニュースレター、記事、その他のメディアを通じて、セキュリティ脅威と関連のリスクに対する可視性を高めることができます。次に、リーダーはデータのプライバシーとセキュリティを強化し、結果的に振る舞いを強化するためのポリシーと手順を導入しなけれななりません。最後に、組織は、データの保護と予防を含めた、リーダーの役割に合わせて、さまざまな性能管理プロセスを調整することができます。

巧妙なセキュリティ脅威を想定した没入型のトレーニングを実施する
社員の意識および振る舞いは、組織のコミュニケーションとトレーニングプログラムの質と適合性に依存しています。組織は、年に1回のスライド資料集を使ったプレゼンテーションを改善し、チームが現代のリスクに備えるための、人を惹きつける現実的なトレーニングを行わなければなりません。

ただし、リスクとコンプライアンスに関する義務的なトレーニングを行うだけでは十分ではありません。チームが情報を記憶し続けることをリーダーが望んだ場合、リーダーは順位表のようなゲーミフィケーション手法を大々的に採り入れ、好ましい振る舞いを広め、参加者を増やすことができます。トレーニングプログラムは人を惹きつける、今日的なものであるべきで、日付の決まっているEラーニングコースとは一線を画したものであるべきです。たとえば、シナリオにもとづくシミュレーションは、さまざまなセキュリティ脅威、ならびに前例のないシチュエーションで最善の対応をする方法についての意識を植え付けます。また、すべての社員が同じリスクプロファイルを持っているわけではないので、トレーニングはさまざまな役割およびチームに応じて行われるべきです。

さらに、個人的なものにすること。パーソナライズされたリスクトレーニングは、データ保護についての学びとリソースを強化します。これらのトレーニングセッションでは、社員は仕事以外の生活でのセキュリティ保護の重要さを理解し、職場のなかにこのマインドセットを持ち込むようになるかもしれません。この関連付け可能なコンテンツにより、社員は自身の個人データをよりセキュアにすることを学ぶようになるので、エンゲージメントを高めることができます。

サイバー攻撃に対する保険業界の対応例

サイバーセキュリティは、プライバシーに対する消費者の懸念が見えない点だけでなく、すでに落とし穴に落ちている企業があるという意味でも、世間の注目を浴びている事柄です。保険業界に対するサイバー攻撃の例は、巨大なグループと企業、および地方の業者の両方で、数多くあります。

たとえば、[9]米国のChubbが、2020年にサーバー攻撃を受け、サードパーティーのサービスプロバイダーによる情報への不正アクセスにより、保険契約者の個人データが盗まれました。ランサムウェアを使った同じような事例が、2021年に[10]CNAでもありました。スペインでも、類似のサイバー脅威の事例が[11]MAPFREと[12]SegurCaixaより報告されており、両者は2020年にランサムウェア攻撃を受けました。Pacific Specialty Insurance CompanyやAXAといった企業も、歴史的なサイバー攻撃の被害者となりました。

しかし、これらの事例を紹介することが重要なのは、サイバー攻撃の欠点とそれが生み出す困難な状況に光を当てるのではなく、これらの会社が脅威にどのように反応したかを示すことができるからです。

MAPFREの事例は、他の理由によって際立っています。なによりも先に、この会社自体が侵害があったことをクライアントと一般の人々に知らせ、それによって、会社の透明性と顧客の信頼を高めたからです。

次に、同社は関係機関（この場合はスペインデータ保護庁）に攻撃についての連絡を十分速やかに行い、その機関が徹底的な捜査を行い、フィッシングキャンペーンの可能性があると結論づけました。

さらに、スペインの保険会社が、攻撃への迅速な対応を実施しています。システム障害を検知すると7分以内に、MAPFREが影響力の高いプロトコルを発動して、インシデント管理手順を開始し、危機管理委員会を招集します。攻撃が実行されてから30分以内に、この会社はすでにデバイス、重要ではないサーバー、および分離されているいくつかのネットワークセグメントの多くを、すでにシャットダウンしていました。

企業のセキュリティチームの作業員は1晩中働き、ランサムウェアを見つけ、感染したデバイスのウィルスを除去しようとしました。7時間も経たないうちに、攻撃は制御され、解決されました。この話の結論はどういうことでしょう？ MAPFREは、このような攻撃（あるいは上記の他の攻撃）に備えていました。サイバー攻撃の際にすべきことを示したプロトコルと具体的な指示があったために、影響を大幅に抑制できたのは確かかもしれません。

NTT DATA のサービスとユースケース

保険会社が必要とするセキュリティの機能と管理

NTT DATA は、リスクリーダーが未来の保険組織に向けての準備を整えるなかで考慮すべき、いくつかの重要な活動を明らかにしています。それらは以下の通りです。

1. 組織または企業の戦略計画プロセスにリスクリーダーを参画させる。この活動により、リーダーは会社のリスク管理目標のうちのビジネス上の優先事項を議論できるようになります。リスクリーダーは、他の人が見逃すかもしれない、リスクまたは機会が潜んでいる可能性がある、新たな傾向についての見解を示すことも可能になります。

2. 組織の部署または機能ではなく、ビジネスユニットと一体化できるようにリスク機能を再構成する。従来のリスク機能は財務または業務と組み合わされていましたが、損害保険や生命保険の個人向け保険種目と組み合わせることにより、事業およびリスク対応部門は、ビジネス上の意思決定の初期段階でリスクの見通しについて採り上げることができるようになります。それにより、リスク機能は、第1のディフェンスラインを責任を持って配備する際に、ビジネス上の願望および課題について学ぶこともできるようになります。未来のリスク機能はよりビジネス指向になり、プロフィットセンターとして付加価値をもたらすようになるべきです。

3. 第1および第2のディフェンスラインでの役割および責任を明確に定義する。「3つのディフェンスライン」が普及しているにもかかわらず、その実装には今も課題があります。3つのディフェンスライン内の役割および責任の明確な定義が課題となっていることがよくあります。全社的なリスク管理である第2のディフェンスライン（SLOD）は、通常はビジネスユニットで構成されている第1のディフェンスライン（FLOD）と同じことをするのではなく、これらビジネスユニットを補完することを目指すべきです。

4. 先進のテクノロジーと高度な人材に投資する。ほとんどのリスク機能は、効果的なリスク管理に欠かせない高速データ処理を阻害するような手動のプロセス、またはレガシーのシステムを今も使っています。新しいテクノロジーにアップグレードすることにより、保険会社は、手動のタスクの自動化、データ処理の高速化、ならびにエクスポージャーの評価、リスクへの対応および制御性能の測定を行うための重要な洞察を生成できるようになります。組織は、問題が起きてからコンプライアンスチェックリストに頼るようなマインドセットから、最新のテクノロジーの活用によって効率性と効果が向上する、より機敏で、能動的かつ機能横断的な構造へリスク文化へとシフトすべきです。リスクリーダーがチームの強化を考えている場合は、ビジネス、分析、ならびに ESG、気候およびサイバー脅威などの機能を越えたリスクについての理解および専門知識を備えた人材を求めるようにしましょう。

NTT DATAの サービス

NTT DATAでは、サイバー攻撃および他の脅威のリスクを最小化および中立化させる最良の方法は、自社の機器、ネットワークおよびリソースをオンプレミスおよびクラウドの両方で保護する、専門的なソリューションを活用した包括的なアプローチを導入することだと考えています。

NTT DATAは、戦略についてのコンサルティング、セキュリティ対策の実装、リモート監視および技術コンサルティングなど、エンドツーエンドの多様なサービスを取り揃えており、これらサービスのすべてが当社パートナーが提供する、最高のサイバーセキュリティソリューションを活用しています。

全業界のクライアントのプロジェクトを通じて培われた経験、セキュリティオペレーションセンター（SOC）のネットワークおよびR&Dリソースを持つ当社は、各業界固有の知識および技術についての専門知識を活かし、サイバーセキュリティリスクからお客様を保護しています。

サイバーセキュリティサービスに対する当社のロードマップは、以下の5つの主要な行動指針にもとづいています。

戦略、セキュリティ、ガバナンスおよびリスク管理
当社は御社のビジネスリスクの識別および管理を行い、その国および業界固有のデータセキュリティとガバナンスに関する規制へのコンプライアンスを保証します。不透明性の削減およびより良い意思決定の実現は、NTT DATAにお任せください。

プライバシーと設計によるセキュリティ
当社の自動化されたセキュリティテスト、設計のDevSecOpsおよびRed Teamサービスにより、ソフトウェアアーキテクチャおよび製品のセキュリティを向上させることができます。

リモート監視とすばやい対応
当社のセキュリティオペレーションセンター（SOC）により、管理サービスの監視および識別、ネットワークアクセス制御、インシデント検知、ならびにクラウドでの対応の自動化が可能になります。

サイバーソリューション
当社のソリューションが実装される主要なエリアは、アイデンティティ管理、クラウド環境でのアクセス制御、産業向けサイバーセキュリティおよびデジタル詐欺対策となっています。

サイバーセキュリティについての意識と人材
NTT DATAは、サイバーセキュリティ関連のトピックについての継続的な学習方法と意識喚起コースを用意しており、これらのすべてが御社組織の習熟度にマッチしています。

ユースケース（匿名）

クライアントのニーズ
このルールリエンジニアリングプロジェクト(Rule Reengineering Project)では、クライアントは、南米および北米22か国で、ファイアウォールのセキュリティレーティングを改善する必要がありました。

NTT DATAからの支援
NTT DATAのサービスを活用し、クライアントは、さまざまな国のファイアウォールに適用される新しいポリシーの定義、計画および運用で構成されるプロジェクトをエンドツーエンドでアウトソーシングし、関係するさまざまな地域での組織化、ならびににビジネスへの影響を最小限に抑えるための各地域の調整を行いました。

結果と利益
プロジェクトが進行中の場合、当社は利益を数値化することができません。ただし、このセキュリティサービスは、以下のような管理グループでのITセキュリティレベルの向上を目指したものであり、これらの管理グループは素晴らしい効果を上げることが期待されています。

- 業務セキュリティ管理
- インフラストラクチャのシールディング管理
- 管理の識別および許可
- インシデント管理
- 脆弱性およびアップデートの管理

同様に、ITセキュリティサービスは、グループのセキュリティインフラストラクチャについての企業の成熟度を高めるため欠かせない、システムヘルスの健全性に関するプロジェクトの定義、計画、エラボレーション、デプロイおよび検証に焦点を当てています。これらはすべて、リスク管理アプローチを通じて行われます。

結び

保険業界は急速に成長し、絶えず変化しているのが明らかであり、絶えずテストされ、絶えず進化している業界でもあります。不透明さが管理不能であり続け、保険業界のどこにでも存在している要素となっているなか、セキュリティは優先的に焦点を当てられるものとなり続けるでしょう。

この業界の企業は、競争力を維持するために、絶えず変化する世界情勢に適応しなければなりません。そのためにとるべき行動は、このような厳しい時代に生き残る方法を模索しながら、世界およびマーケットの関連トレンドについて考慮するということになります。

セキュリティリーダーが意識し、それに対応するために行動しなければならないことがいくつかあります。それらは、ツール、方法論の使用、チームのエンゲージメント、情報の活用およびテクノロジーなど多岐にわたる場合があり、企業はそれに適応しなければなりません。ただし、保険のリーダーがこの文書で強調されていることで心に刻むべきことが4つあるとすれば、それは以下のようになるでしょう。

1. セキュリティは、テクノロジーを越えたビジネス上の課題です。セキュリティは、保険会社の意思決定を行うトップから最初に、できれば取締役会から最初に導入しなければなりません。

2. データプライバシーは、規制および顧客の両方から絶えず求められるでしょう。個人情報の透明性と倫理的な管理が、保険の契約プロセスにおいてエンドツーエンドで保証されなければなりません。

3. サイバーセキュリティは最終的なものではなく、門番的な役割を果たします。成熟化する前のきわめて早期の段階でサイバーセキュリティを取り入れ、潜在的な脅威と脆弱性を識別しなければなりません。

4. 上記を考慮すると、予防と対応準備が大きな意味を持つようになります。そのため、サイバー攻撃に直面したときのための、事前作成された、明確で、周知徹底されているプロトコルを持つことが、不可欠となります。。

業界横断および保険のセキュリティのエキスパートで構成された、当社のチームは、世界中の業界トレンドについての深い知識を持っているだけでなく、この分野のソートリーダーシップを構築するのに協力してきました。そのなかには、消費者の要求に対応し、絶えず登場するリスクにかかわらず成功するために、CISOおよび他の重役が短期的に、注視すべき分野が含まれています。これらの課題、利点、実例およびアドバイスにより、保険会社のリーダーがその分野における業界のエキスパートとなり、自動化された、データ主導型のセキュアな保険へと他のリーダーたちを導くことを当社は望んでいます。

NTT DATAは保険ビジネスについて専門知識を有しており、根本的な戦略ビジョンを構築し、保険会社がデジタル化への道のりでリーダーとなるための具体的な助言を提示することができます。複数セクターにわたるエキスパートとしての当社の役割を通じて、業界内の企業は、マーケットでのリーダーシップを強化し、保険会社の枠組みを越えるためのフレームワーク、ツールおよびソリューションを得ることができるでしょう。

参考資料

1. ACORD Insurance のデジタル成熟度についての研究（2022 版）https://www.acord.org/marketplace-pages/product-detail/acord-insurance-digital-maturity-study-(2022-edition)

2. DevSecOps で成功するための 12 の方法 https://www.gartner.com/doc/3978490?ref=clientFriendlyURL

3. 大手保険会社はレガシーの近代化をいかに管理しているか https://www.gartner.com/doc/4014359?ref=solrAll&refval=334260698

4. InsurTech Global Outlook 2022：保険規制 https://insurtech-insurance.nttdata.com/four-forces/regulations/intro

5. 情報についての公正な慣行 https://iapp.org/resources/article/fair-information-practices/

6. The 2022 Insurance Vision. 保険の範囲を超えて https://insurance.nttdata.com /thought-leadership/2023-vision/

7. 詐欺統計 https://insurancefraud.org/fraud-stats/

8. 会社のセキュリティが破られる原因となった失敗を理解する https://www.tessian.com/research/the-psychology-of-human-error/

9. 保険会社に対するサイバー攻撃：リスクを避ける方法 https://votiro.com/blog/cyber-attacks-against-insurance-companies-how-to-avoid-the-risks/

10. 10.3 月のサイバー攻撃のあと、CNA が 4,000 億ドルの身代金を支払い https://www.insurancejournal.com/news/national/2021/05/21/615373.htm

11. Mapfre、ランサムウェアのサイバー攻撃を受けたことを認める：「サービスの提供を続けるために、人間にできることはすべて行ってまいります」https://www.businessinsider.es/mapfre-reconoce-ser-victima-ciberataque-ransomware-698639

12.「ランサムウェア」攻撃がスペイン最大の保険会社に与えた影響 https://elpais.com/tecnologia/2020-10-16/asi-ha-afectado-un-ataque-de-ransomware-a-una-de-las-mayores-aseguradoras-de-espana.html

NTT DATA
Trusted Global Innovator

Natàlia Solé Riera
Head of Cloud + IM + Security at NTT DATA EMEAL

Enrique Bernao
Cybersecurity Manager at NTT DATA EMEAL

Sushila Nair
Vice President of Security Services at NTT DATA Services

Nutan Pandit
Practice Leader, Insurance Risk and Compliance at NTT DATA Services

NTT Groupの一員であるNTT DATAは、高い信頼を得ている、ITとビジネスサービスの世界的なイノベーターで、本社は東京にあります。当社は、コンサルティング、産業ソリューション、ビジネスプロセスサービス、IT近代化およびマネージドサービスを通じて、お客様のトランスフォーメーションを支援しています。NTT DATAにより、お客様ならびに社会は、デジタルの未来へと安心して移行することができます。当社は、お客様の長期的な成功を願っており、世界的な規模と地域のお客様への対応を組み合わせ、50以上の国で活動しています。詳細は、以下のウェブサイトをご覧ください。insurance.nttdata.com