Deloitte.
デロイト トーマツ

シートベルトをお締めください：

航空機のイノベーションを支えるデジタルリスク管理術

サイバー攻撃の議論には、いつも盗まれたクレジットカードデータ、個人情報の流出、なりすまし被害などが取り上げられる。しかし、現在の企業を狙ったサイバー攻撃は、従業員や顧客データの窃取といったレベルをはるかに超えたものとなっている。新しいタイプのサイバー攻撃では、知的財産、戦略プラン、著名人の情報などを標的とする以外にも、運用上の混乱や企業資産の損害、公共インフラや安全に対する深刻な脅威を狙って実行される。これらは、従来の「ハッカー」やサイバー犯罪者とは異なり、競合関係、またはハクティビストによって行われる。現状では本格的なサイバーテロリズムと見なされることはないものの、その対象範囲や考えられる影響を考慮すると、いずれサイバーテロリズムやサイバー戦争の領域に突入することは間違いない。

今やサイバー上のリスク対策は、企業データの保護や、データの機密性、完全性、可用性の維持だけに存在するものではない。サイバー上のリスクは、企業によってはビジネスリスクとなり、IT分野のみに委ねられる問題ではなくなっている。日々繰り返されるサイバー攻撃は、企業にとって、業務妨害や回復困難なダメージを与えらることとなり、航空業界に至っては、生命を危険に晒す可能性すらある。1日10万フライトを運航し、高度3万7千フィートを飛びながら何百万もの人を安全に運ぶ航空会社は、標的となるリスクが非常に高いと言える。航空関連企業の経営者らは、自社が標的になることを懸念している。

イノベーションとの関係

アメリカ経済における航空業界の重要性は、軽んじることはできない。民間航空の成長率は、アメリカ経済全体の成長を上回っており、2012年の国勢調査の集計データを見ると、航空業界はGDP（国民総生産）の5.4%を占め、経済活動全体の1.5兆ドルに貢献し、1,180万人の雇用を支援している（※1）。業績が加速する背景には、多くの分野と同様、技術革新がある。航空業界は、新規の収益源を求め、インターネットによる技術革新を採用した。それによって、業務効率の向上、個人向けの細かいカスタマイズによる顧客ニーズへの対応が可能となった。しかし、その結果もたらされたのが、サイバーリスクに対する増々の不安である。

※1. The Economic Impact of Civil Aviation on the U.S. Economy（アメリカ経済における民間航空の経済的影響）」、アメリカ合衆国運輸省、連邦航空局（2014年6月）

デジタル航空機の台頭

IP対応の新世代航空機は、「e-Enabled」やデジタル航空機と呼ばれることがある。デジタル航空機は航空業界の「スマートデバイス」で、操縦室からキャビン、地上での業務を大きく変えた。航空技術や携帯型デジタル時代によって促進されたこれら新規イノベーションによって、航空業界は長年の課題だった燃料消費の最適化、メンテナンス効率の向上、スケジュール設定の改善、GateLink（PKI）、電子フライトバッグ（EFB）、航空機空地データ通信システム（ACARS）（※2）、次世代の航空管制などの機能を通じたリアルタイム品質データへのアクセスができるようになった。航空機のIP対応によるメリットは明白で、広く浸透したが、同時に下記に示す通り、リスクも存在する。

図1：航空分野の新しい技術的イノベーションが抱える潜在的なリスク

ボーイング777の後継機でワイドボディ機の新ボーイング787ドリーマー、エアバスA380や新A350XWBは、すでにデジタル対応している。ボーイング737や777などの古い世代の民間航空機やエアバスA320ファミリにも、デジタル機能が実装され始めている。最新の民間航空機は実質、何百万もの出張客や旅行客を毎日運ぶ、リモートかつコンピュータ制御可能なデバイスという、空飛ぶ産業制御システムになった。各航空機は相互接続された情報技術システムで、複雑かつハッキングの可能性を抱えながら運用されており、フライト指示の提供、航空機のウェイト/バランス問題の確認、他航空機の位置の特定、悪天候の回避などを、フライバイワイヤーや従来の空地システムを使って行っている。

※2. ACARS、Wikipedia.org（http://en.wikipedia.org/wiki/Aircraft_Communications_Addressing_and_Reporting_System）（2015年3月21日）

残存する既知の脅威

一方で、従来のサイバーリスクも未だ残っている。航空業界の主要な販売プラットフォームは、eコマースだ。高度なオンライン販売チャネルや報酬プログラムを開発した結果、航空会社はビジネス業務や販売促進をインターネットベースのデータ交換に依存するようになった。サウスウエスト航空やジェットブルー航空は、サードパーティのオンライン旅行代理店（OTA）を完全に避ける形で、搭乗券のほぼ100％を直販している。ロイヤリティプログラムIDや決済カード情報（PCI）は、顧客と予約情報とを紐づけるために利用される。これら情報は空港内のキオスク、ユーザの携帯デバイス、搭乗ゲートのキオスクなどに保存され、エグゼクティブクラブのメンバーシップ、座席のアップグレード、手荷物チェックインサービス、その他さまざまなサービスを介してアクセスすることができる。搭乗ゲートのキオスクまたは自動キオスクは、個人を識別可能な情報（PII）の一部を使って顧客のプロフィールや旅行プランへアクセスできる。個人を特定可能な情報がひとつ流出する、または初歩的なソーシャルエンジニアリング攻撃が実行されれば、攻撃者は特定の個人がどこからどこへ旅行し、いつ到着し、さらにはどのゲートに到着するかなどの正確な情報を入手できる可能性がある。スパイ、ストーカー、誘拐犯にこうした情報が渡ってしまうと、搭乗客の安全は脅かされ、航空会社にとっては新たな法的責任が課されることになる。すでに航空会社では、フリークエントフライヤーのアカウント情報のなりすましや、ロイヤリティプログラムのポイント盗難などへの対応に追われている。それに加えて、一般的には操作が難しいセキュリティ制御アプリケーションについても、継続的に使い勝手のバランスをとっていく必要がある。

重要インフラとしての航空業界

2013年2月、オバマ大統領は大統領令13636号「重要インフラストラクチャのサイバーセキュリティの改善」を発行し、その中で航空業界は重要インフラ区分に指定された。大統領令には、アメリカ国立標準技術研究所（NIST）に対し、既存の標準、ガイドライン、ベストプラクティスをベースに、利害関係者と協力して自主参加型フレームワークを構築し、重要インフラへのサイバーリスクを軽減するよう指示があった。1年後、NISTは「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」1.0版を公開し、サイバーセキュリティ関連リスクを管理するための優先付けができ、柔軟かつコスト効果が高く、繰り返し適用可能なアプローチを提供した。アメリカ政府によって航空業界への対応が優先付けられた結果、同分野への注目が集まり、重要な議論が活発化した。一方で、民間航空機の設計および運行の両方における包括的かつ効果的なプログラムへの議論は、まだ多く残されている。

新たな脅威へ先手を打つには

効果的なサイバーリスクプログラムは、企業が晒される固有のサイバー脅威またはサイバー脅威の状況を検討した上で、広範に管理されたサイバーリスクフレームワークを通じて現実的な目標を設定できる必要がある。どのような環境も完璧な安全はなく、ましてや費用対効果が高い安全を実現する方法などはそうはない。企業はデータ、アプリケーション、インフラストラクチャを守るために合理的な手順を踏むだけでなく、攻撃が成功した場合の被害を最小限に抑え、出来る限り早く通常業務に戻れるようにしなければならない。サイバーリスクを効果的に管理するには、企業は次の要素が必要となる。

- **予防：既知および未知の脅威から重要な資産を守る**
- **発見：脅威に対する意識を保ち、敵対活動を検知する**
- **事後対応：インシデント発生から素早く回復する**

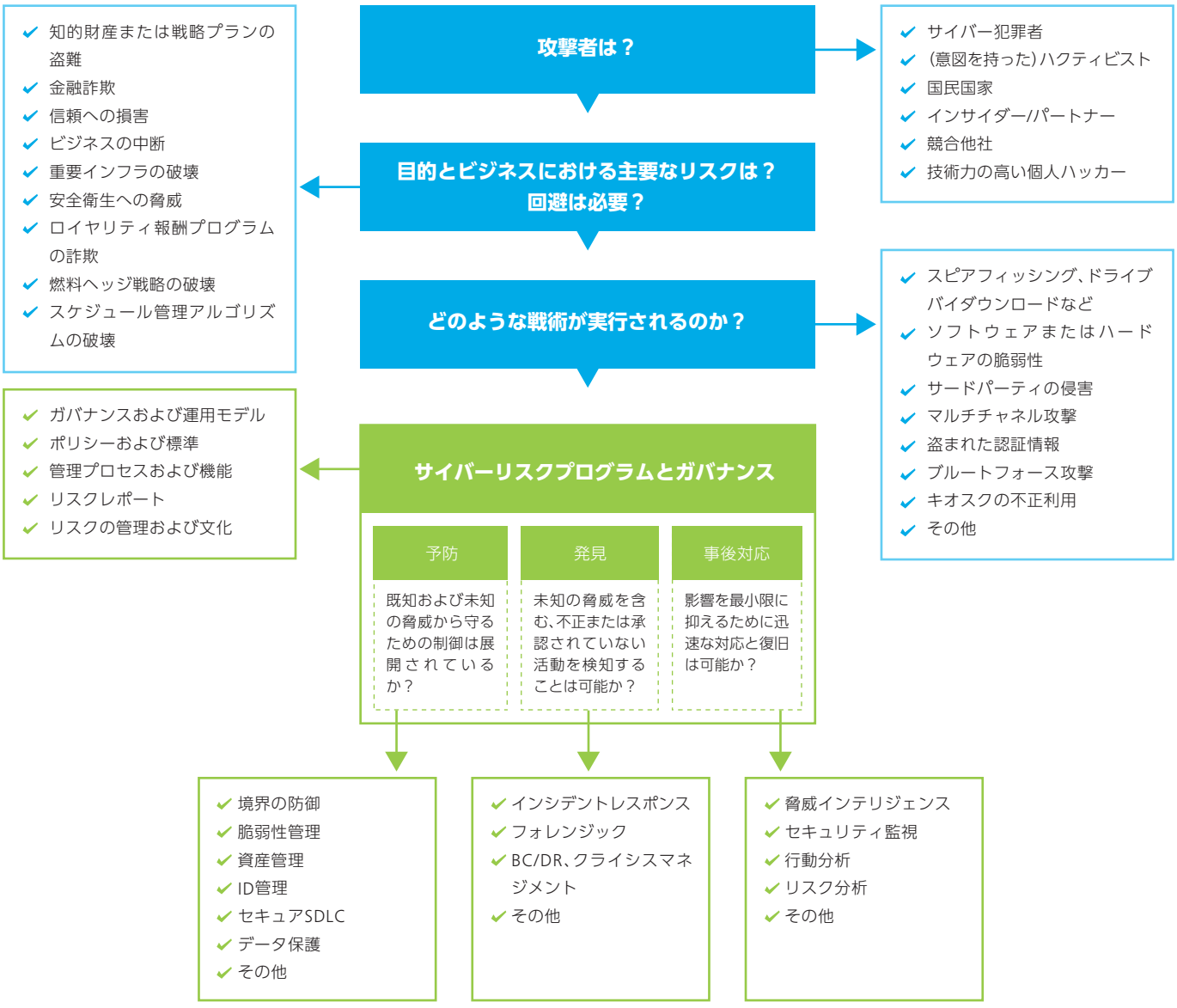

図2：攻撃者、攻撃理由、攻撃方法を理解する

予防：エコシステム全体を既知および未知の脅威から守る

効果的なセキュリティプログラムでは、企業全体で既知および未知の脅威から重要資産を守るために、継続的に対策を見直す必要がある。予約確認でクレジットカード番号の利用を廃止することはできないかもしれないが、トークン化技術を使ってクレジットカード番号、社会保障番号、既知の旅行者ID、パスポート番号などのデータがシステム全体で増殖することを防ぐことはできる。顧客は、搭乗券の発行、座席変更やアップグレードの申請、予約など、さまざまな認証がモバイルから実行できることを望んでいる。こうしたモバイルトラフィックを暗号化し、顧客の認証を自動化するとき、公開鍵インフラストラクチャ（PKI）技術を利用することができる。これにより、顧客に意識させることなくモバイルでのやりとりの安全性を高めることができる。このほか、業務部門は多様なサービスを提供するためにサードパーティと急速に提携しているが、こうしたベンダが特定のIT資産へアクセスできるようにする必要がある。フェデレーション技術では、機密性の高い内部ディレクトリを公開することなく、またサードパーティのIDや認証情報の管理を負担することなく、ビジネスパートナーに対して安全にリソースへのアクセスを提供できる。

発見：予防的な可視性および状況の認識

不正侵入が発生する可能性はゼロにはならない。攻撃を防ぐには、もはやシステムのパッチ適用や侵入検知システムのシグネチャ更新のような従来のシンプルな対策では対応できない。攻撃を素早く検知・特定することは、発生しうる損害を食い止める上で重要だ。こうしたサイバー脅威への対策では、重要なアプリケーションに対する検知機能と、ID管理やネットワークアクセス制御などのセキュリティ技術の両方にセキュリティオペレーションセンター（SOC）を取り入れることが、企業が警戒を怠ることなく対処するための中核的な能力となる。SOCが真の効果を発揮するには、インシデントの発生を監視し、評価、エスカレーションするコンピュータセキュリティインシデントレスポンスチーム（CSIRT）のサポートが必要となる。また、SOCでは誤検知を削減し、容量分析やフォレンジック分析のためのログストレージを最適化するために、継続的に使用例を改善する必要がある。多くの場合、SOCは複数の業界、警察、政府による情報共有および分析センター（ISAC）などの高度脅威情報に基づき、未知の脅威を特定する。たとえば、非営利組織の航空ISAC（A-ISAC）では、世界中の航空事業、業務、サービスを守るための航空業界向け機能を提供する目的で設立されている。

事後対応：インシデント発生時の復旧機能

事業上の性質や搭乗客の安全という潜在的リスクから、航空会社の大半はインシデントレスポンスと危機管理に熟達している。しかし、サイバー攻撃がもたらす脅威はこうしたリスクとはまったく異なる。場合によっては、航空業界が経験した従来の安全問題よりもはるかに複雑で、対応範囲を超えることもある。そういった新しい脅威には、サイバー・ウォー・ゲーミングを通じて攻撃シナリオへの対応を訓練し、備えることができる。サイバー・ウォー・ゲーミングの「机上訓練」では、企業で実際に発生した、または発生しうる脅威を模倣し、企業がどれだけ効果的に対応できるかを理解する。訓練は、ビジネスリーダー、技術チーム、弁護士、警察や独立系サードパーティといった外部組織など、組織の全レベルに対応し、ほとんどの場合は甚大な労力が必要となる業務復旧への取り組みにおいて、どれだけ効果的に関与できるかを評価することができる。一般的に、訓練を実施して判明する最も多い問題は、取締役会の対応への不慣れと準備不足、組織内の多くの部門間における連携不足だ。

成功要因としてサイバーリスクへの取り組みを位置付けるための実例を作る

効果的かつ投資を受けた、予防、発見、事後対応といったサイバープログラムは、経営層レベルでの可視化が重要となる。サイバーリスクはビジネスリスクであり、航空会社がビジネス上の決定において、企業全体のリスクを評価する際に検討すべき課題だ。知識のあるCISOやCSOであれば、サイバーリスクプログラムを単にコンプライアンスを維持するための必要悪としてではなく、成功要因として位置付けることができる。それぞれの投資は関連する費用対効果検討書を付けて、企業リスクの削減とビジネス上のメリットの両方を明確に特定、定量化するべきである。検討書に記載する内容としては、顧客体験の向上、プロビジョニングおよびガバナンスのプロセスの自動化による業務効率の改善、トークン化技術の採用による機密データへの高額かつ義務的なセキュリティ制御の回避、外部ベンダとのパートナー連携を支援する高い俊敏性の提供などが挙げられる。

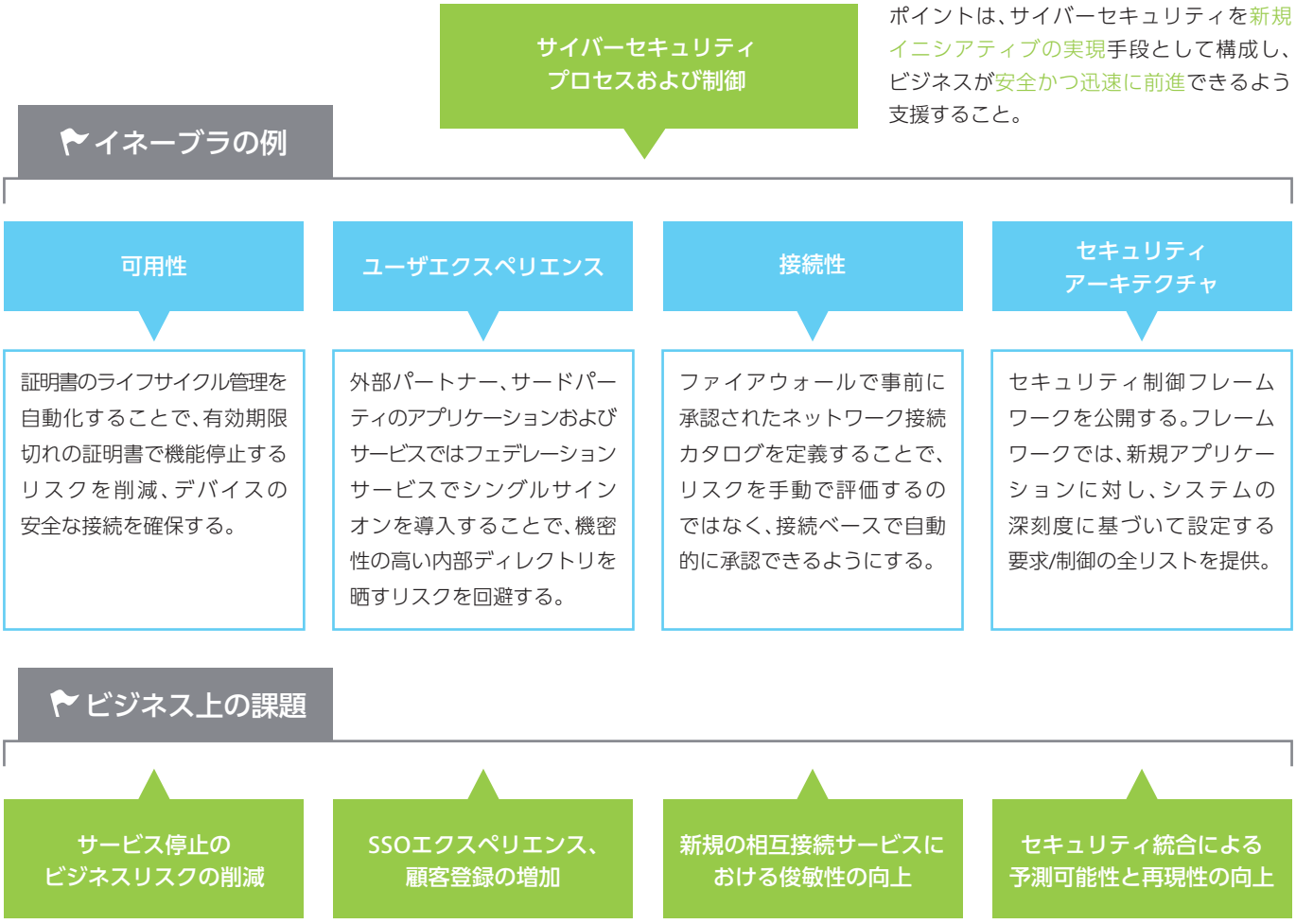

図3:サイバーリスク投資によるビジネス上の潜在的なメリット

経済的利益は、直接的な場合もある。たとえば、保険会社は十分開発されたセキュリティプログラムに対して、サイバー保険の割引を提供している。これは、一般経費や管理費から直接純損失へと流れるため、コスト削減につながる。

航空業界のような、密度が高く競争が厳しい業界では、効率、マージン、顧客体験を改善する新しい技術を誰もが模索しており、堅牢なサイバーリスクプログラムの目標は組織を高速かつ安全に推進させることにある。このようなプログラムは、新技術をメインストリームに採用、導入する適切なプロセスや手順が展開されていることを保証することで、ビジネスのイニシアティブを促進するだけでなく、加速させることが可能となる。

上層部を動かす - カギは経営層の支援と企業ガバナンスにある

サイバーセキュリティは、企業リスクとして毎回の経営者会議で議論されるべき課題だ。取締役会はサイバーセキュリティを理解するべきで、会議ではセキュリティ全体の状況と併せて定期的かつ継続的なサイバーリスクの確認を実施する必要がある。もうひとつ主要な実践方法として、「リスク管理委員会」の設置が挙げられる。委員会は、内部監査、航空管制、保険、法務、情報セキュリティを含む複数の部門のトップで構成し、定期的に会議を開き、サイバーリスクについて議論する。

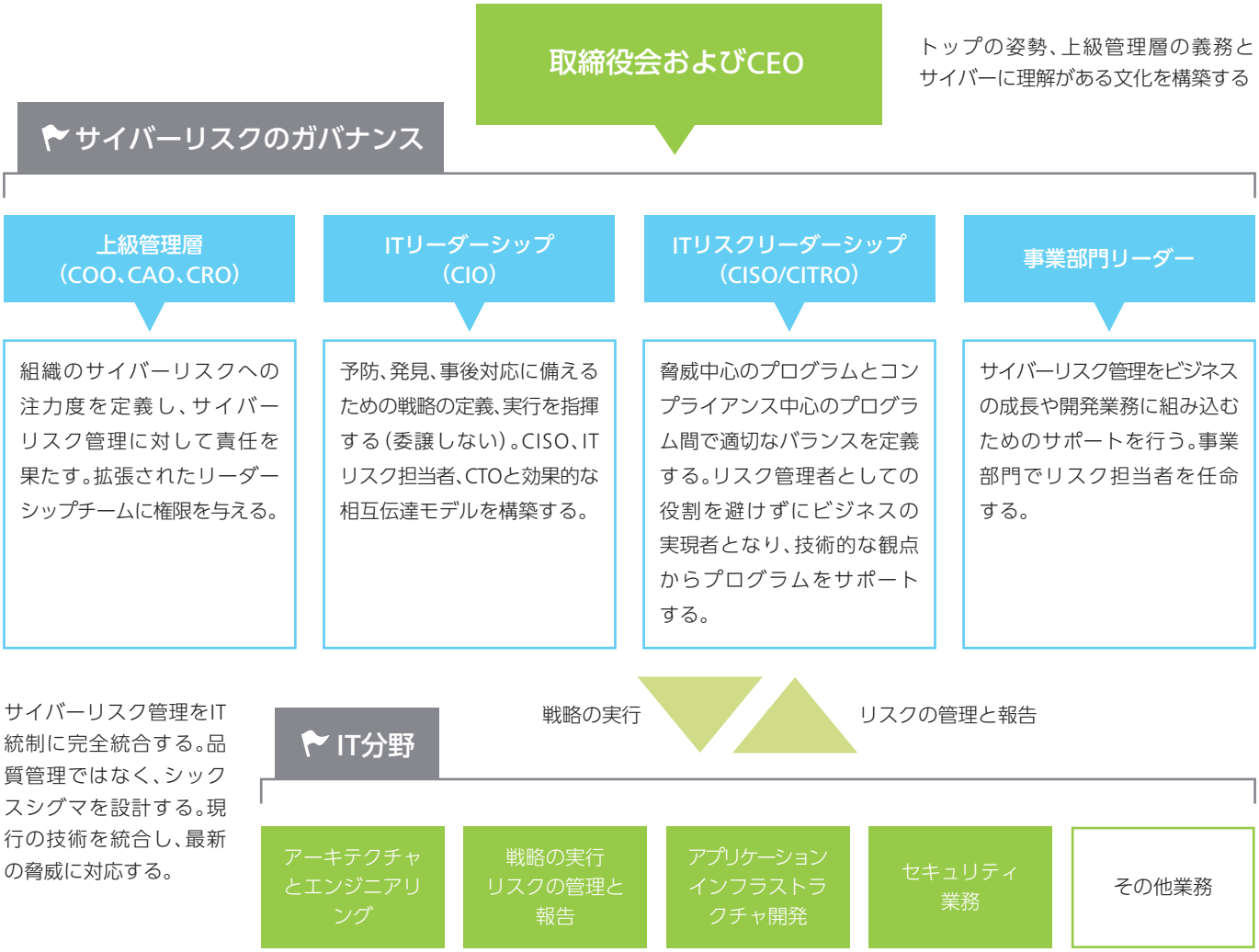

図4：サイバーリスクのガバナンス構造と経営層による支援

サイバーリスクプログラムをビジネスイノベーションの「シートベルト」に

従来の脅威が継続する現在、航空業界は技術革新の恩恵を受ける一方で、新規に登場し進化を続けるサイバーリスクにも対応する必要がある。今やサイバーリスクの被害は、データのプライバシー侵害やコンプライアンスの罰則の範囲を超え、最悪の場合、搭乗者の安全性だけでなく、最終的には組織自体の存続性をも脅かす可能性がある。多くの人はサイバーセキュリティに対し、前進を遅らせる「必要悪」と見ているが、必ずしもそうとは限らない。

サイバーセキュリティをシートベルトに例えることは、適切といえる。シートベルトは安全を追加することで高速での移動を可能にする。同様に、堅牢なサイバーセキュリティプログラムに投資することで、企業は技術革新を通じてビジネスの競争力を高め、成長を促進しながら、同時に関連リスクに対処することができる。そして、今やネットワーク内に航空機と搭乗者の情報を抱える航空会社は、今一度「ネットワークは本当に十分防御できているか」考えてみて欲しい。

CONTACTS

Guy Langford

Vice Chairman,
U.S. Travel, Hospitality & Leisure Leader
Deloitte & Touche LLP
(212) 436-3020
glangford@deloitte.com

Vikram Kunchala

Director
Deloitte & Touche LLP
(713) 982-2807
vkunchala@deloitte.com

Edward W. Powers

National Managing Principal
Cyber Risk Services
Deloitte & Touche LLP
(212) 436-5599
epowers@deloitte.com

丸山 満彦

パートナー
サイバーリスクサービス
デロイト トーマツ リスクサービス株式会社
090-6492-3648
mitsuhiko.maruyama@tohmatsu.co.jp

注: 本資料はデロイト トーマツ リスクサービス株式会社が翻訳したものです。原文については英語版をご参照ください。
http://www2.deloitte.com/content/dam/Deloitte/us/Documents/consumer-business/us-cb-aviation-cyber-risk-report-04222015.pdf

国内ネットワーク

有限責任監査法人トーマツ

東　京　〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル　Tel:03-6213-1112
大　阪　〒541-0042　大阪府大阪市中央区今橋4-1-1 淀屋橋三井ビルディング　Tel:06-4560-6021
名古屋　〒450-8530　愛知県名古屋市中村区名駅3-13-5 名古屋ダイヤビルディング3号館　Tel:052-565-5517
福　岡　〒810-0001　福岡県福岡市中央区天神1-4-2 エルガーラ　Tel:092-751-1517

デロイト トーマツ リスクサービス株式会社

本　社　〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル　Tel:03-6213-1300