Society1818オンライン勉強会

世界経済フォーラム2025年グローバルリスク報告書に見るサイバーリスク及びAiの将来課題とその対応

By Tokyuki Ted Sato
上席顧問
Kroll International ＆Marsh総研
2025年4月5日

佐藤 徳之（さとう とくゆき）

Kroll International & マーシュ総研株式会社　Executive Advisor (上席顧問)

ted.sato@kroll.com/08076381514

- 財団法人社会生産性本部情報化国民会議専門委員として「住基ネット/カードの普及に向けた6つの提言」を2006年に麻生総務大臣にリコメンデーションを提出。2005年には総務省からの依頼にてASP白書に執筆陣に参画。
- 2009年全国都道府県CIOフォーラムにて「電子自治体アウトソーシング戦略を成功させるリスクマネジメント」について講演。その他、ICT関連に纏わるリスクマネジメントに関するコンサルティング、論文及び著書（日経BP社、自治日報等々、多数の実績）。
- 2018年、カーネギーメロン大学と慶応大学によるCISO(Chief Information Security Officer) Leadership schoolを終了。C-suiteレベルへのサイバーリスク集中ワークショップの企画とファシリテーションを担う。2019年、ハーバード大学 Cybersecurity: Managing Risk in the Information Age online 8 weeks module course 終了。
- 現在、東京大学大学院工学部及び明治学院大学経済学部にてリスクマネジメント及び保険論の非常勤講師を兼務。
- **CRMJ(Cyber Risk Management Japan)研究会発起人＆事務局長。経団連推奨公式ガイドブック「サイバーリスクマネジメントの強化書」監修＆執筆。**
- マーシュマクレナン在籍35年。現在Kroll International の上席顧問も兼務。

Marsh McLennan - At a glance　マーシュマクレナンの概要

MMCはフォーチュン250企業であり、世界中で約83,000人の従業員を擁しています。
130カ国以上の顧客にサービスを提供しており、年間収益は190億米ドルに上ります。

クロールのミッション：不確実なビジネス動向を正しく捉える

米ニューヨークで1972年に設立されたリスクコンサルティングおよび調査会社

- 国内外の**ガバナンス**や**リスク**に関する「調査」と「助言」を提供

リスクを事前把握し、管理する	コンプライアンス体制を強化する	有事における対応、原因究明、解決支援
• 地政学リスク、特定国の政治情勢、特定市場、業界固有のリスク評価・分析 • 経済安全保障・制裁動向 • 競合他社分析（成長戦略、フォーカス、現地パートナーとの関係、財務状況等） • 買収・投資・パートナー候補や経営者のバックグラウンド、市場でのレピュテーション、政治的な関係、トラブルや対立などの「隠れたリスク」の把握 • 人権DD	• 財務監査を超えた、不正防止を目的とした業務プロセスや牽制機能の検証・改善 • サイバーセキュリティ体制の検証と改善 • ESGアドバイザリー • 新規採用者、退職者、外部業者（サードパーティ）に対するスクリーニング • 従業員や外部ベンダー向けコンプライアンス・トレーニング	• 不正・コンプライアンス事案発覚後の内部調査、社外の利害関係者調査 • 第三者委員会による調査報告支援 • 知的財産、経営機密情報漏洩調査 • サイバー攻撃、情報漏洩事案の対応 • 資産調査、債権回収支援 • 会社再建、売却、清算支援 • 上記各種事案における、法律事務所等のプロフェッショナル・ファームとの協業

Agenda

Part1　サイバーリスクの現在と将来

～　損害をもたらすものは何か？

(1) サイバーリスクの位置づけと全体像

(2) 懸念されるテクノロジーリスクとその影響（AI、先端技術リスクなど）

(3) テクノロジーリスクが生み出す経済リスク（不正な経済活動、サプライチェーン　リスクの増大）

(4) これらリスクへの対処について

１．サイバーリスクの現在と将来
～　損害をもたらすものは何か？

グローバルリスク報告書とは

「グローバルリスク報告書」（Global Risks Report）は、世界経済フォーラム（World Economic Forum、WEF）が毎年1月に発表する報告書である。

本報告書は、現在および将来のリスク環境についての主要な情報源の一つとして位置づけられており、企業が将来起こり得るリスクを把握し、対策を講じるために有効とされている。

マーシュ・マクレナンおよびチューリッヒ・インシュアランス・グループと連携して作成された本報告書では、約900名のグローバルリスク有識者、政策立案者および産業界リーダーたちの意見が引用されている。

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

本報告書は、世界経済フォーラム（WEF）が毎年1月に、スイスのダボスで開催される年次総会に先立って公表しており、世界的なリスクに関するレポートとて知られる。2006年から発行されており、2025年版は20版となる*。報告書の内容は、各国のメディアでも幅広く取り上げられると共に、様々な経済レポートでもその内容が引用されている。

*日本版は2008年より発行。マーシュの日本が主体となって制作にあたる。日本からも約106社（2023年版作成時）が、報告書の作成に協力しており、その中には政府系機関も含まれる。

１（１）サイバーリスクの位置づけと全体像

2025 top risk concerns by time period

主要なテクノロジーリスクとして、偽情報の拡散、サイバー侵害と戦争行為、また長期的にはAI技術の不適切な利用が懸念されています。

- 経済
- 環境
- 地政学
- 社会
- テクノロジー

今後2年間

1. 誤報と偽情報
2. 異常気象
3. 国家間武力戦争
4. 社会の二極化
5. サイバー犯罪やサイバー戦争
6. 汚染（大気、土壌、水）
7. 不平等
8. 非自発的移住
9. 地政学上の対立
10. 人権および / または市民の自由の浸食

今後10年間

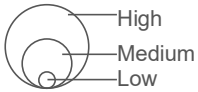
1. 異常気象
2. 生物多様性の喪失と生態系の崩壊
3. 地球システムの危機的変化（気候の転換点）
4. 天然資源不足（食料、水）
5. 誤報と偽情報
6. AI技術がもたらす悪影響
7. 不平等
8. 社会の二極化
9. サイバー犯罪やサイバー戦争
10. 汚染（大気、土壌、水）

Note: WEF Global Risks Perception Survey 2024-2025
Source: World Economic Forum Global Risks; Marsh McLennan analysis

Risk interconnections

偽情報の拡散、サイバー侵害と戦争行為などのテクノロジーリスクは、社会の二極化や武力紛争と並ぶ重要なリスクと位置付けられます。

Nodes
Risk influence



Edges
Relative influence

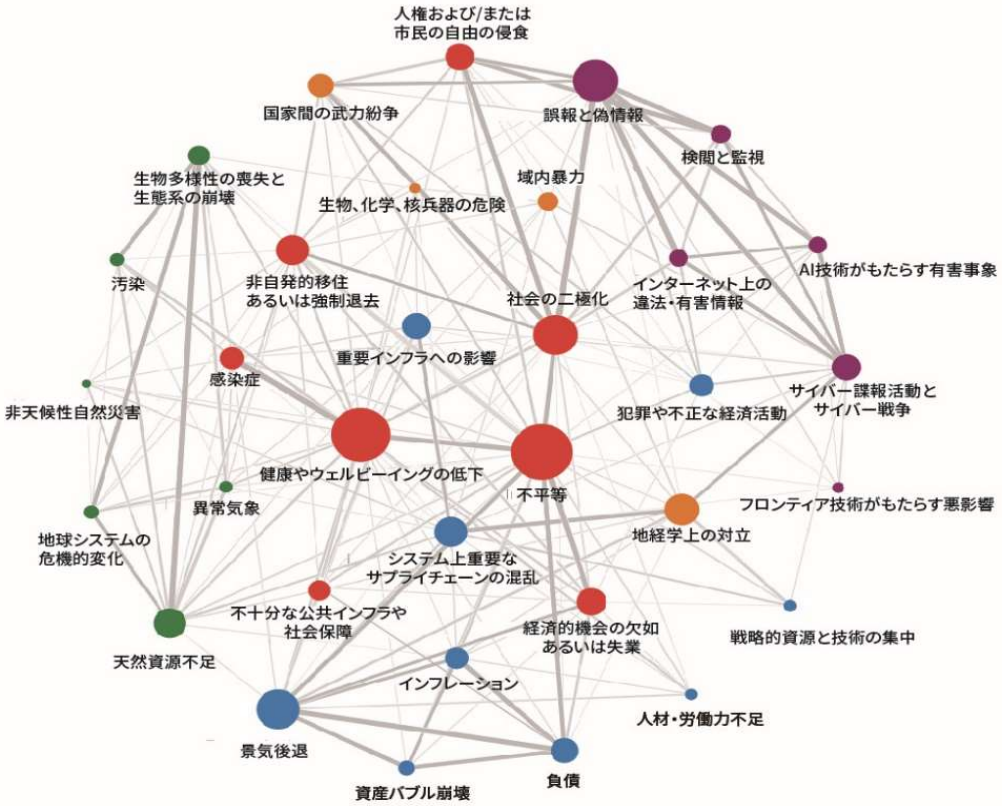
High
Medium
Low

- 経済
- 環境
- 地政学
- 社会
- テクノロジー

グローバルリスク報告書2025年版

グローバルリスクランドスケープ：相互連関マップ

WORLD ECONOMIC FORUM



Note: WEF Global Risks Perception Survey 2024-2025
Source: World Economic Forum; Marsh McLennan analysis

Evolution of top short-term risk concerns over time

Economic Environmental Geopolitical Societal Technological

Global Risks Landscape (2011-2025)[1]

Top 5 global risks in terms of impact

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
1	Fiscal crises	Systematic financial failure	Systematic financial failure	Fiscal crises	Water crises	Weak climate change response	WMDs	WMDs	WMDs	Climate change mitigation and adaption failure	Infectious diseases	Climate action failure	Cost-of-living crisis	Misinformation and disinformation	Misinformation and disinformation
2	Climate change	Water supply crises	Water supply crises	Climate change	Infectious diseases	WMDs	Extreme weather	Extreme weather	Climate change mitigation and adaption failure	WMDs	Climate action failure	Extreme weather events	Natural disasters and extreme weather events	Extreme weather events	Extreme weather events
3	Geopolitical conflict	Food crises	Fiscal imbalances	Water crises	WMDs	Water crises	Natural catastrophes	Natural catastrophes	Extreme weather	Biodiversity loss	WMDs	Biodiversity loss and ecosystem collapse	Geoeconomic confrontation	Societal polarization	State-based armed conflict
4	Asset price collapse	Fiscal imbalances	WMDs	Unemployment/ under-employment	Interstate conflict	Involuntary migration	Water crises	Climate change adaption failure	Water crises	Extreme weather	Biodiversity loss	Erosion of social cohesion	Failure to mitigate climate change	Cyber insecurity	Societal polarization
5	Extreme energy price volatility	Volatility in energy and agricultural prices	Weak climate change response	Critical ICT systems breakdown	Weak climate change response	Energy price shock	Weak climate change response	Water crises	Natural catastrophes	Water crises	Natural resource crises	Employment and livelihood crises	Erosion of social cohesion and societal polarization	Interstate armed conflict	Cyber espionage and warfare

Sources: World Economic Forum, *Global Risks Report 2022, 2023, 2024, and 2025*
Note: 1. Over the years, the WEF has adjusted the list of global risks and moved risks between categories.

1 （2）懸念されるテクノロジーリスクとその影響

TECHNOLOGICAL

経済リスクに結びつくテクノロジーリスク（抜粋）

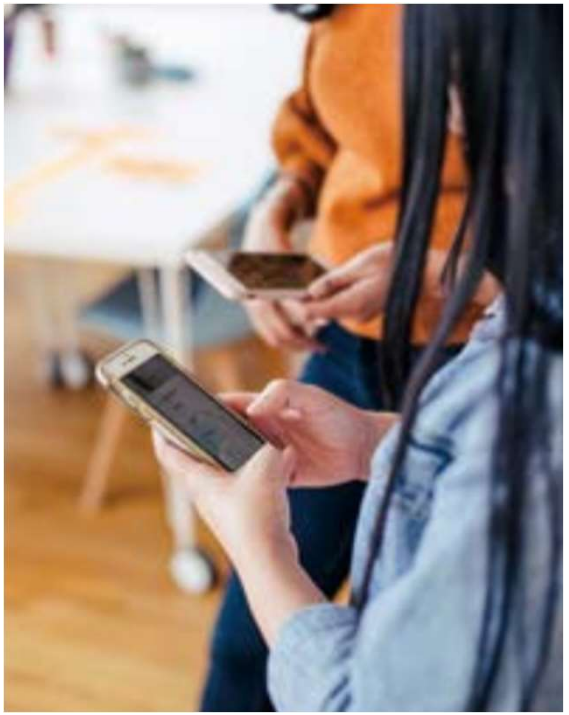
テクノロジーリスクのうち、AIの発達によるサイバー攻撃の増加や顧客情報の盗難、特に暗号化情報の量子暗号の問題、偽情報、誤情報によるレピュテーションの低下、サイバー攻撃の増加がもたらすサプライチェーンの寸断などが懸念されます。

Adverse outcomes of AI technologies **AI技術がもたらす悪影響**	AIおよび関連技術が個人、企業、生態系および経済に及ぼす、意図的もしくは意図せざる負の影響
Adverse outcomes of frontier technologies **先進技術がもたらす悪影響**	フロンティア技術の進歩が、個人、企業、生態系、経済に及ぼす意図的または人的な悪影響。脳とコンピュータのインターフェース、バイオテクノロジー地球工学、量子コンピューティングなど
Cyber espionage and warfare **サイバー犯罪と戦争行為**	国家および非国家主体によるサイバー兵器およびツールの使用は、デジタル上の存在を制御し、業務を妨害し、および／または、対象の技術および情報ネットワークやインフラを侵害または損傷することを目的としている。これには、武力紛争中に発生する、または武力紛争の引き金となる防御的および攻撃的なサイバー作戦、および優位性を獲得するために機密データや知的財産を盗むサイバー攻撃が含まれる。
Misinformation and disinformation **誤報と偽情報**	メディアネットワークを通じて広く拡散された根拠のない情報（故意によるものも含む）により、事実や権威に対する不信感が大きく広がり、世論が大きく変化した。これには、偽情報、偽装、操作、捏造されたコンテンツなどが含まれるが、これらに限定されない。

Adverse outcomes of AI technologies / AI技術がもたらす悪影響
Misinformation and disinformation / 誤報と偽情報

誤報と偽情報（1位）は、今年のトップ10ランキングで新たにトップに躍り出た。使いやすいインターフェースを備えた大規模人工知能（AI）モデルは、もはやニッチなスキルがなくても使えるようになり、すでに、高度な音声クローンから偽造ウェブサイトまで、偽造情報やいわゆる「合成」コンテンツの爆発的な増加を可能にしている。増大するリスクと闘うため、各国政府は、オンラインの情報や違法コンテンツのホストと作成者の両方を対象にした新しい規制や規制の変更を導入している。登場し始めた生成AI規制も、こうした取り組みを補完すると思われる。例えば、中国では生成AIコンテンツに電子透かしを入れることが義務付けられており、これは**AIコンテンツのハルシネーション（幻覚）による意図的でない誤報**などの情報を特定するのに役立つ可能性がある。しかし一般には、規制が開発のペースに対抗し得るスピードと効果を実現できる可能性は低い。

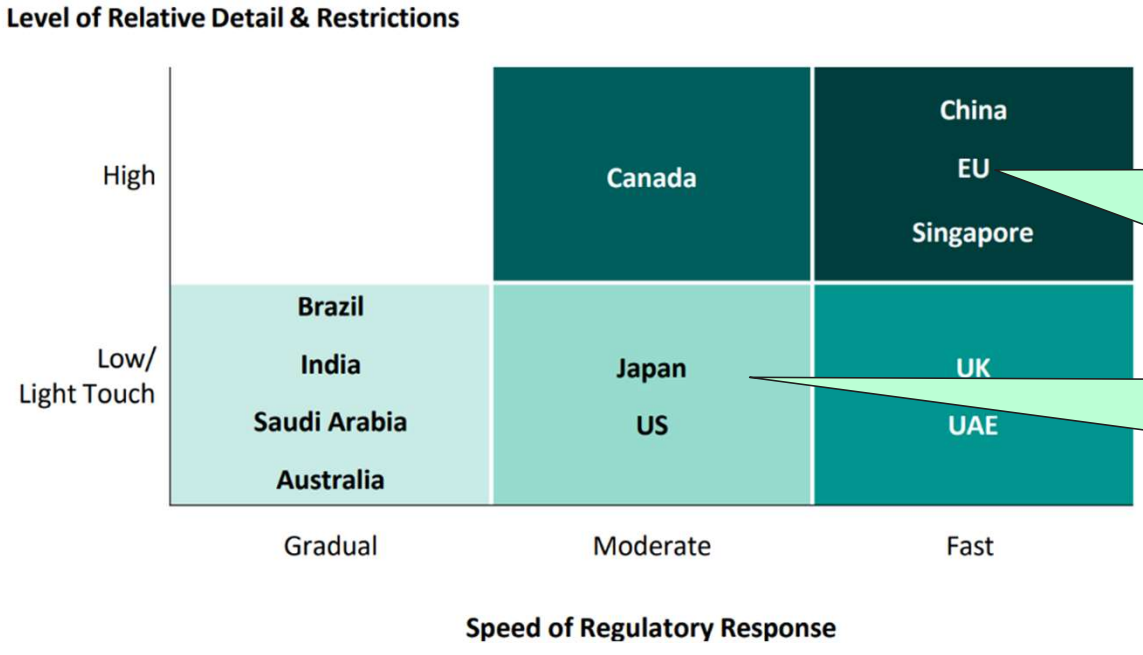
合成コンテンツは今後2年間もさまざまな方法で、人々をコントロールし、経済に損害を与え、社会を分断するだろう。気候アクティビズムから紛争のエスカレートまで、**多種多様な目標の追及で、偽造された情報が展開される**可能性がある。無断のディープフェイクポルノや株式市場の操作といった**新しい種類の犯罪も急増**するだろう。しかし、気付かぬうちに拡散する誤報と情報が社会の結束を脅かしているにもかかわらず、一部の政府は、誤報の防止と言 論の自由の保護の間のトレードオフに直面して行動が遅くなり過ぎるリスクがある一方、抑圧的な政府は規制によるコントロールの強化を利用して人権を蝕むおそれがある。



出典：世界経済フォーラム発行「グローバルリスク報告書2024年版」（マーシュ ジャパン／マーシュ ブローカー ジャパンによる翻訳）

各国AI規制の動向
REGULATORS ARE PURSUING A VARIETY OF RISK MITIGATION STRATEGIES

現在、規制当局がAIの台頭に全体として、また特に生成AIに対してどのように対応しているかについては、大きな違いがあります。
イノベーション重視で、アウトプット規制中心の国を中心にAIのサイバー攻撃における悪用が進展する可能性があります。



EUの「AI法（AI Act）」は、AIシステムをリスクレベルに基づいて分類する包括的な規制です。

開発者には、透明性確保、サイバーセキュリティ、倫理的なAI使用に関する厳格な基準が求められ、違反時には最大3,500万ユーロまたは年間収益の7%の罰金が科されます。

現時点では、AI技術のイノベーションを阻害しない「出口の品質管理」に焦点を当てる日本独自の枠組みが検討されています。これは、AIの技術的自由度を維持しつつ、生成物の質や安全性を確保することを目的としています

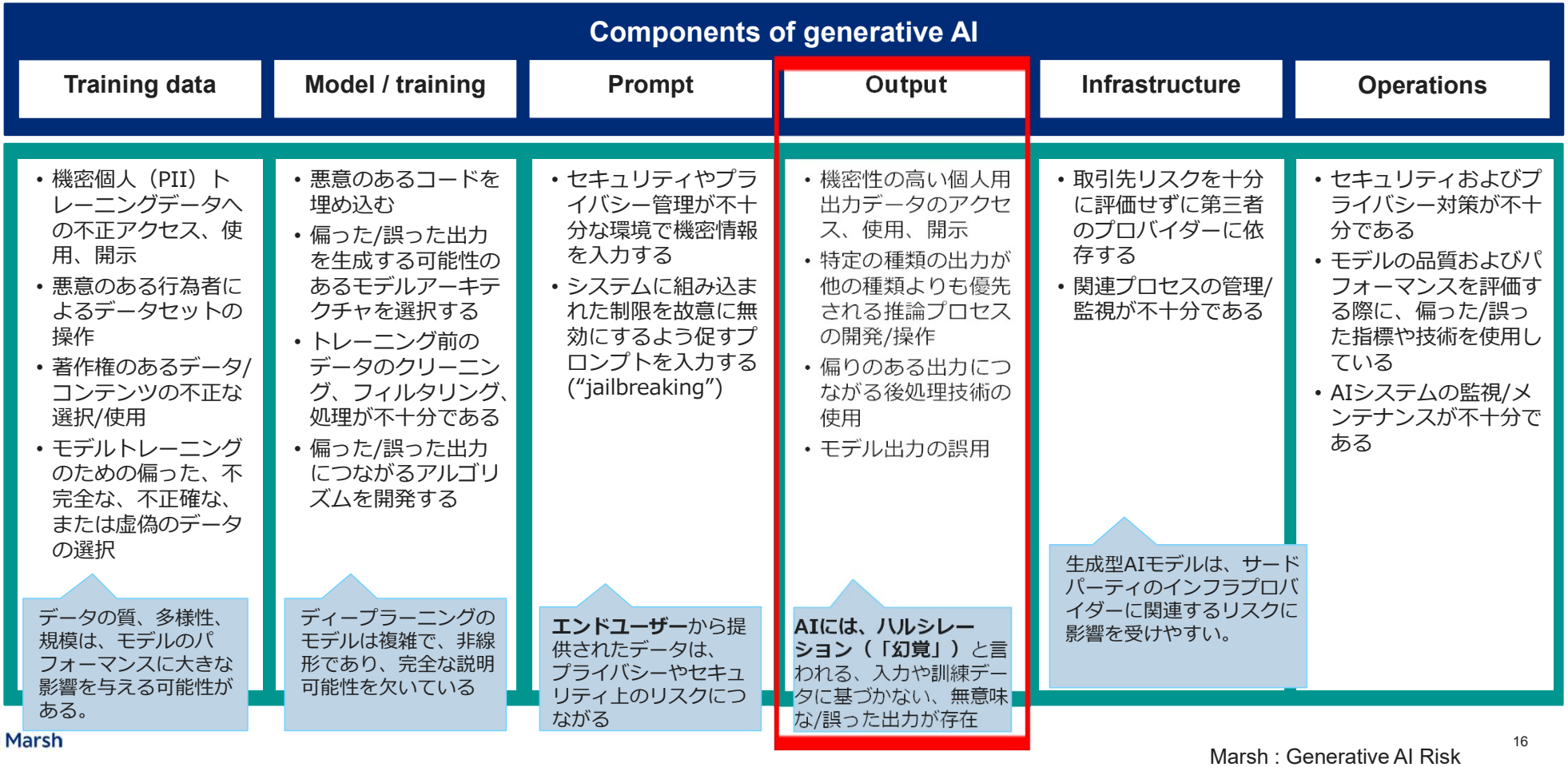
トランプ政権でこの動きは加速

Refer to “Generative AI – Mitigating Risk to Realize Success”(2023 Guy Carpenter)

TECHNOLOGICAL

Generative AI risks framework

生成AIの利用は、自らが情報漏洩や偽情報の拡散を引き起こすリスクがあります。



Marsh

Marsh : Generative AI Risk

TECHNOLOGICAL

Adverse outcomes of AI technologies / AI技術がもたらす悪影響
Misinformation and disinformation / 誤報と偽情報

- フィッシング文面はAI（下記はChat GPT）で容易に作成
- マイナー言語でも数秒で作成可能

Amazonを装ったフィッシングメール（アカウント確認詐欺）

件名: 【重要】お客様のAmazonアカウントに異常なアクセスを検出しました

本文:
Amazonお客様へ
いつもAmazonをご利用いただきありがとうございます。

お客様のアカウントで不審なログイン試行が検出されました。

- 日時: 2024年9月10日 14:35 JST
- 場所: 中国・上海
- デバイス: Windows 10 (Chrome)

このログインに心当たりがない場合は、直ちにアカウントのセキュリティを確認してください。

アカウントを確認する

※24時間以内に確認がない場合、不正アクセス防止のためアカウントを一時的にロックさせていただくことがあります。

Amazonセキュリティチーム

Amazonを装ったフィッシングメール（注文確認詐欺）

件名: 【注文確認】ご注文の商品が発送されました（注文番号: #123-4567890-1234567）

本文:
Amazonお客様へ

ご注文ありがとうございます。以下の商品が発送されました。

- 商品: Apple MacBook Air 15インチ（M2チップ）
- 価格: 168,800円
- 配送予定日: 2024年9月12日
- 配送先: 東京都渋谷区〇〇

ご注文内容に問題がある場合は、以下のリンクからすぐにキャンセル手続きを行ってください。

注文をキャンセルする

ご注意: 24時間以内にキャンセル手続きを行わない場合、ご注文が確定し、返品不可となります。

Amazonカスタマーサービス

（リトアニア語版）

Sukčiavimo el. laiškas, apsimetant „Amazon“ (sąskaitos patvirtinimo apgavystė)

Tema: [Svarbu] Jūsų „Amazon“ paskyroje aptikta neįprasta prieiga

Turinys:
Gerbiamas „Amazon“ klientas,

Dėkojame, kad naudojatės „Amazon“ paslaugomis.

Jūsų paskyroje aptikome įtartiną prisijungimo bandymą.

- Data: 2024 m. rugsėjo 10 d. 14:35 (LST)
- Vieta: Šanchajus, Kinija
- Įrenginys: Windows 10 (Chrome)

Jei tai nebuvote jūs, nedelsdami patikrinkite savo paskyros saugumą.

Patikrinti paskyrą

Jei per 24 valandas neatliksite patikros, saugumo sumetimais jūsų paskyra gali būti laikinai užblokuota.

„Amazon“ saugumo komanda

TECHNOLOGICAL

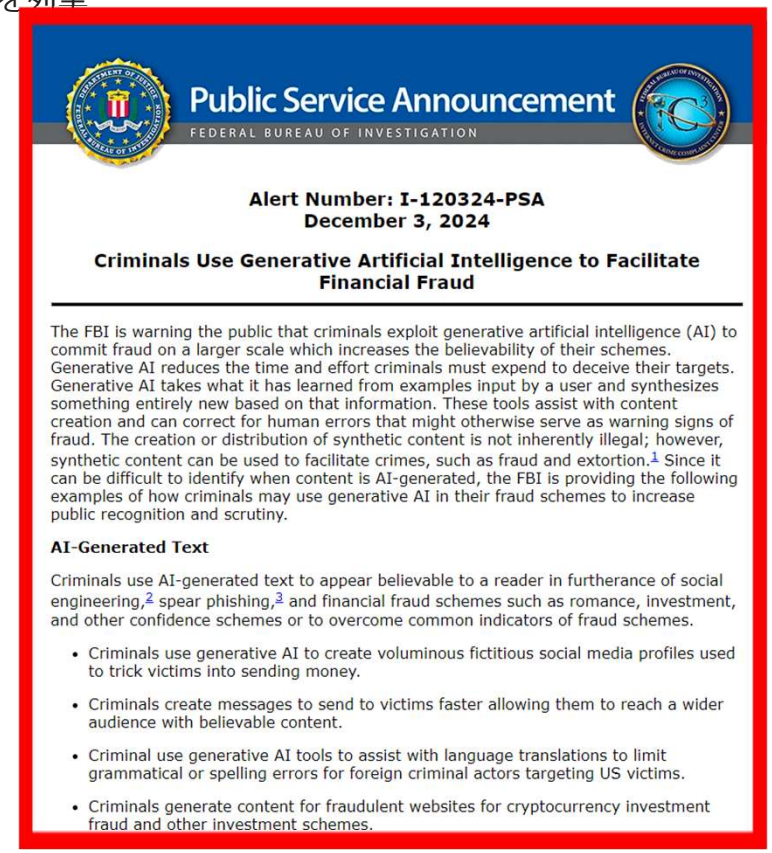
Adverse outcomes of AI technologies / AI技術がもたらす悪影響
Misinformation and disinformation / 誤報と偽情報

- AIを活用した犯罪の増加に対して、2024年12月、FBIは公式に注意文書を発行
- フィッシングメールや詐欺サイト作成以外の用途として、下記のような事例を列挙

AIで生成された画像
- 犯罪者はジェネレーティブAIツールを使用して、偽造品や未納スキームを宣伝する有名人やソーシャルメディア上の人物の画像を作成する。
- 犯罪者はジェネレーティブAIツールを使用して、自然災害や世界的な紛争の画像を作成し、詐欺的な慈善団体への寄付を募る。

AI生成音声、別名ボイス・クローニング
- 犯罪者は、愛する人の声を録音した短い音声クリップを作成し、危機的な状況にある肉親になりすまして、緊急の金銭的支援を求めたり身代金を要求したりする。
- 犯罪者は、個人のAI生成音声クリップを使用して、その人物になりすまして銀行口座にアクセスする。

AI生成ビデオ
- 犯罪者は、会社役員、警察、その他の権威者とリアルタイムのビデオチャットを行うための動画を作成する。
- 犯罪者は、オンライン上の連絡相手が「本物の人間」であることを「証明」するためのプライベートなコミュニケーション用の動画を作成する。



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-120324-PSA
December 3, 2024

Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud

The FBI is warning the public that criminals exploit generative artificial intelligence (AI) to commit fraud on a larger scale which increases the believability of their schemes. Generative AI reduces the time and effort criminals must expend to deceive their targets. Generative AI takes what it has learned from examples input by a user and synthesizes something entirely new based on that information. These tools assist with content creation and can correct for human errors that might otherwise serve as warning signs of fraud. The creation or distribution of synthetic content is not inherently illegal; however, synthetic content can be used to facilitate crimes, such as fraud and extortion.[1] Since it can be difficult to identify when content is AI-generated, the FBI is providing the following examples of how criminals may use generative AI in their fraud schemes to increase public recognition and scrutiny.

AI-Generated Text

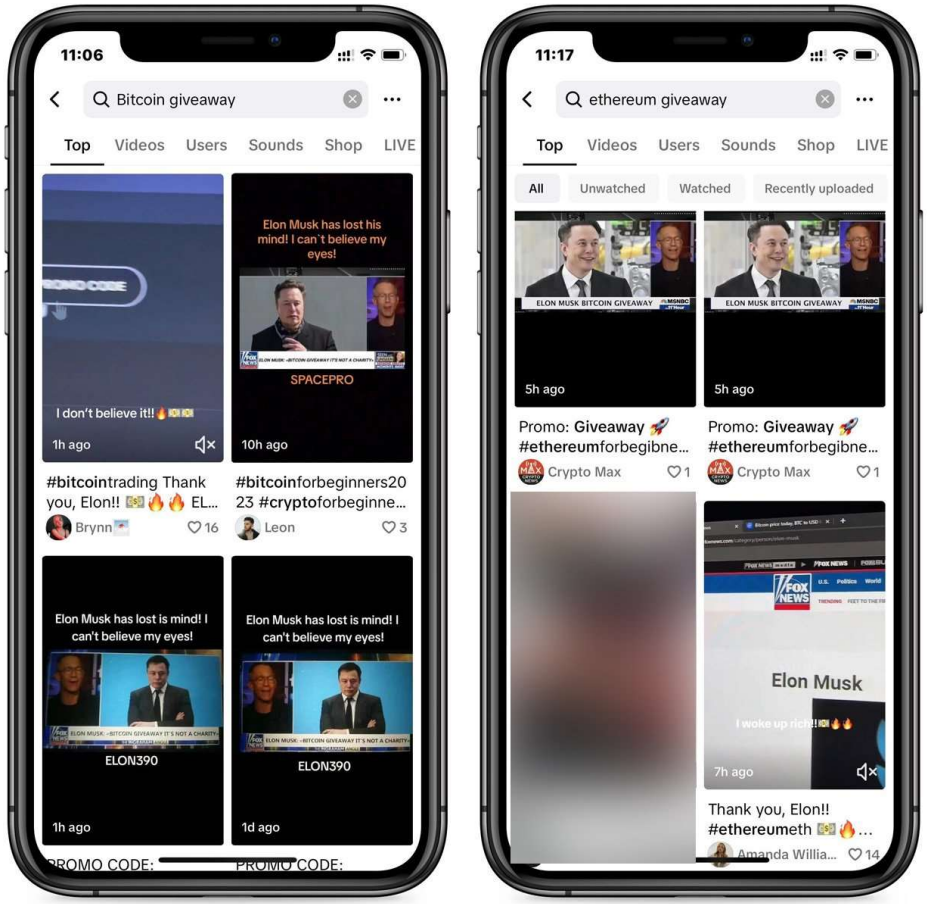
Criminals use AI-generated text to appear believable to a reader in furtherance of social engineering,[2] spear phishing,[3] and financial fraud schemes such as romance, investment, and other confidence schemes or to overcome common indicators of fraud schemes.

- Criminals use generative AI to create voluminous fictitious social media profiles used to trick victims into sending money.
- Criminals create messages to send to victims faster allowing them to reach a wider audience with believable content.
- Criminal use generative AI tools to assist with language translations to limit grammatical or spelling errors for foreign criminal actors targeting US victims.
- Criminals generate content for fraudulent websites for cryptocurrency investment fraud and other investment schemes.

出典：Internet Crime Complaint Center (IC3) | Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud
https://www.ic3.gov/PSA/2024/PSA241203

Adverse outcomes of AI technologies / AI技術がもたらす悪影響
Misinformation and disinformation / 誤報と偽情報

➢実際にTikTokに投稿された、仮想通貨詐欺に利用された、イーロンマスクのAI生成動画



出典： https://www.bleepingcomputer.com/news/security/fbi-shares-tips-on-how-to-tackle-ai-powered-fraud-schemes/

Adverse outcomes of frontier technologies
先進技術がもたらす悪影響

2024年版 重要・先端技術リスト（CETリスト） 2024 Critical and Emerging Technologies List Update

ホワイトハウスが発表したこのリストは、米国の国家安全保障、経済繁栄、国際競争力にとって重要な技術分野を特定し、優先順位を明確化するものです。このリストは、政府、産業界、学術界が協力してイノベーションと技術的優位性を維持するための指針となります。

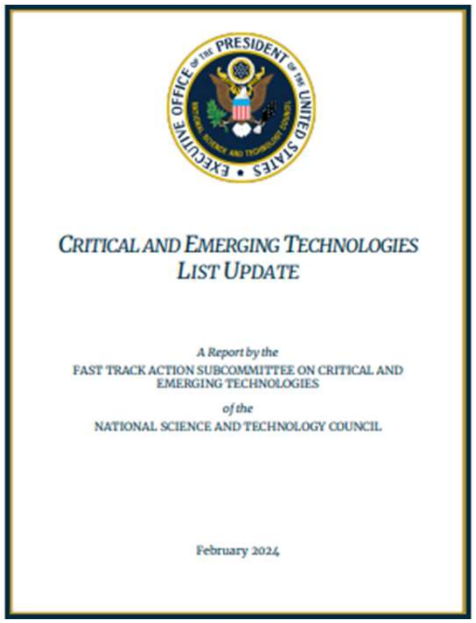
2024年版の「重要・先端技術リスト」では、人工知能（AI）が特に重要な技術として挙げられています。AIに関する内容の主なポイントは以下の通りです：

1. 自律システムの強化
- ドローンやロボティクスにおけるAI活用（防衛および産業用）
- 自動運転車や自律兵器システムにおける技術革新

2. データ分析と予測
- 膨大なデータセットの分析を通じて、国家安全保障のリスク予測や意思決定を支援する。
- 災害対応や気候変動への対策におけるシミュレーションとモデリング。

3. 生成AI
- 文章や画像の生成技術（例: ChatGPTのようなモデル）を活用したコミュニケーションや創造的産業への応用。
- 偽情報（ディスインフォメーション）対策における活用。

4. サイバーセキュリティの強化
- AIを用いた脅威検出、応答の自動化、リスク評価の効率化。
- 攻撃者がAIを利用するリスクを考慮した防御策の開発。



出典：https://www.whitehouse.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf

Adverse outcomes of frontier technologies
先進技術がもたらす悪影響

量子コンピューティングのリスクも国家安全保障と経済競争力にとって極めて重要な技術分野として強調されています。

2024年版 重要・先端技術リスト（CETリスト）における量子コンピューティングの位置づけ

1. 応用分野
- **暗号解読の可能性**: 現在の公開鍵暗号方式（RSAなど）を破る能力が挙げられ、金融システムや国家安全保障への影響が懸念されています。
- 最適化やシミュレーション: エネルギー供給、物流、薬剤開発などでの画期的な応用が期待されています。

2. リスク
- **暗号セキュリティの脆弱化**: 量子技術が進展すれば、従来の暗号化通信が危険にさらされる可能性が高い。
- 軍事転用: 高度なシミュレーション能力が、新型兵器の開発や戦略立案に活用される恐れ。

Store Now, Decrypt Later (SNDL: 今収集し、後で解読) 攻撃

量子コンピューティングは、計算・処理能力の独占を揺るがして、 再構築する可能性があるが、 その開発は極めて大きなリスクを伴っている“。犯罪者は、暗号的に重要なコンピュータの登場を予期し、 Store Now, Decrypt Later (SNDL: 今収集し、後で解読) とも言われるハーベスト攻撃をすでに開始している。
その結果、 製薬、 技術ハードウェアなどの複数の業界で企業秘密や、 電子カルテのような機密性の高いデータが漏洩し、最も高い値を付けた者に売却される恐れがある。 銀行、 送電網、 病院のように大規模な、場合によっては国際的なインフラ規模で麻痺するような可能性も考えられる。

出典：世界経済フォーラム発行「グローバルリスク報告書2024年版」（マーシュ ジャパン／マーシュ ブローカー ジャパンによる翻訳）

Adverse outcomes of frontier technologies
先進技術がもたらす悪影響

日本でも、金融庁が 「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会 報告書」を公表

「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」報告書について：金融庁 （令和６年１１月２６日）

当報告書に記された、経営陣の責務

1. 全社的リーダーシップの発揮
- 各システムで使用されている暗号技術の状況を把握。
- 保有データの重要性や保存期間を考慮し、リスク評価を実施。
- 優先順位を明確にした上で、移行方針を決定。

2. リスク認識の共有
- 量子コンピュータによる暗号解読可能性を正確に把握。
- 耐量子暗号への移行スケジュールを設定し、期限内の実施を目指す。

3. 計画的な準備
- 暗号移行のための棚卸し（クリプト・インベントリ管理）を実施。
- 適切なリソースの確保と移行計画の策定。

NIST（米国国家標準技術研究所）が推奨する主要な耐量子暗号

- CRYSTALS-Kyber
- CRYSTALS-Dilithium
- Falcon
- SPHINCS+
- ML-KEM
- ML-DSA

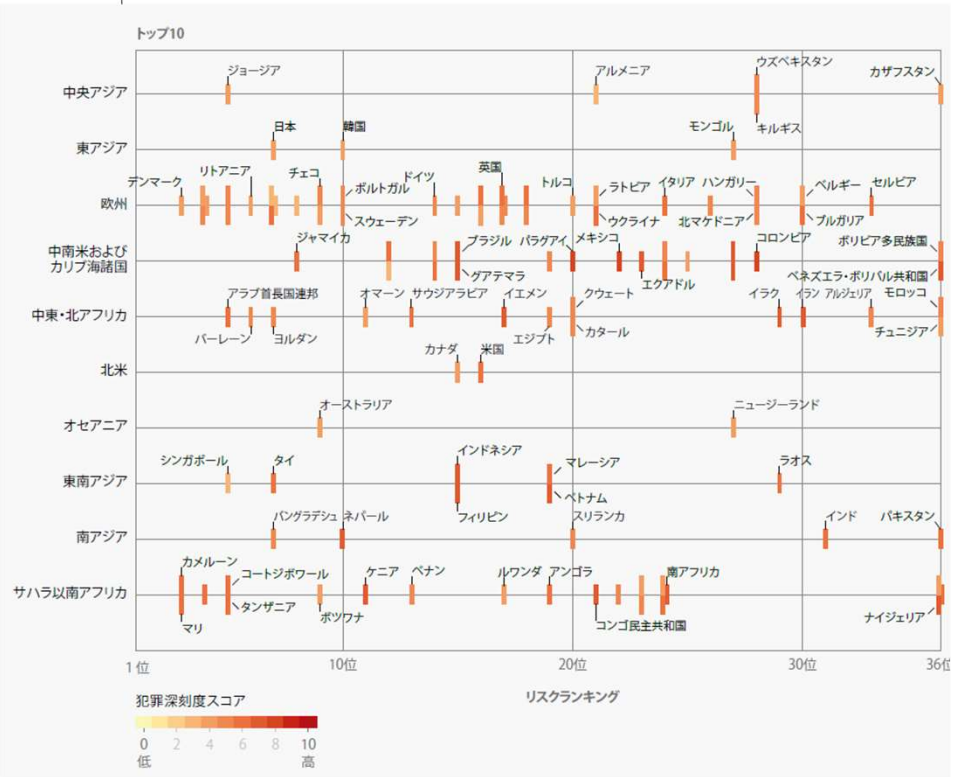
Cyber espionage and warfare
サイバー犯罪と戦争行為

サイバー犯罪に対する脆弱性

- 組織犯罪ネットワークは、**新たなテクノロジーを活用した融合型ビジネスモデル**を採用することで、不正な資金調達が多様化
- 新たなソフトウェアやその能力は、犯罪ネットワークに新たな市場をもたらすとともに、**サイバー犯罪が組織犯罪の低リスク・低コストの収益源となる**ことも増える
- 例えば、フィッシング攻撃に生成AIを用いれば、**少数言語さえ簡単かつ正確に翻訳**
- サイバー防御ステムがより高度化すれば、攻撃のターゲットはデジタルリ テラシーの低い個人や、セキュリティの緩いインフラおよび システムに移る
- 図2.27を見ると、開発途上地域のビジネスリーダーの間でサイバー犯罪やサイバーセキュリティ対策の失敗のリスク に対する懸念が高まっていることが分かる。
- サイバー犯罪による収益源と物理的収益源を活用する デジタル融合型モデルが採用され、そうした活動が麻薬密売などの別の形態の違法収入に取って変わる可能性がある。

図2.27 国別リスク意識（地域別）：サイバー犯罪やサイバーセキュリティ対策の失敗

「今後２年間で、あなたの国にとって最も大きな脅威となる可能性が高い５つのリスクはどれですか」



出典：世界経済フォーラム発行「グローバルリスク報告書2024年版」（マーシュ ジャパン／マーシュ ブローカー ジャパンによる翻訳）

TECHNOLOGICAL

Cyber espionage and warfare
サイバー犯罪と戦争行為

- サイバー犯罪は国家主体の組織によるサイバー攻撃が頻発。
- 2022年、米国では北朝鮮籍のIT労働者が国籍を偽って、就労することに対する警告を出している。
- 下記は、Mandiantがインターネット上で収集した、実際の北朝鮮工作員の求職レジュメ

UNCLASSIFIED

May 16, 2022

GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS

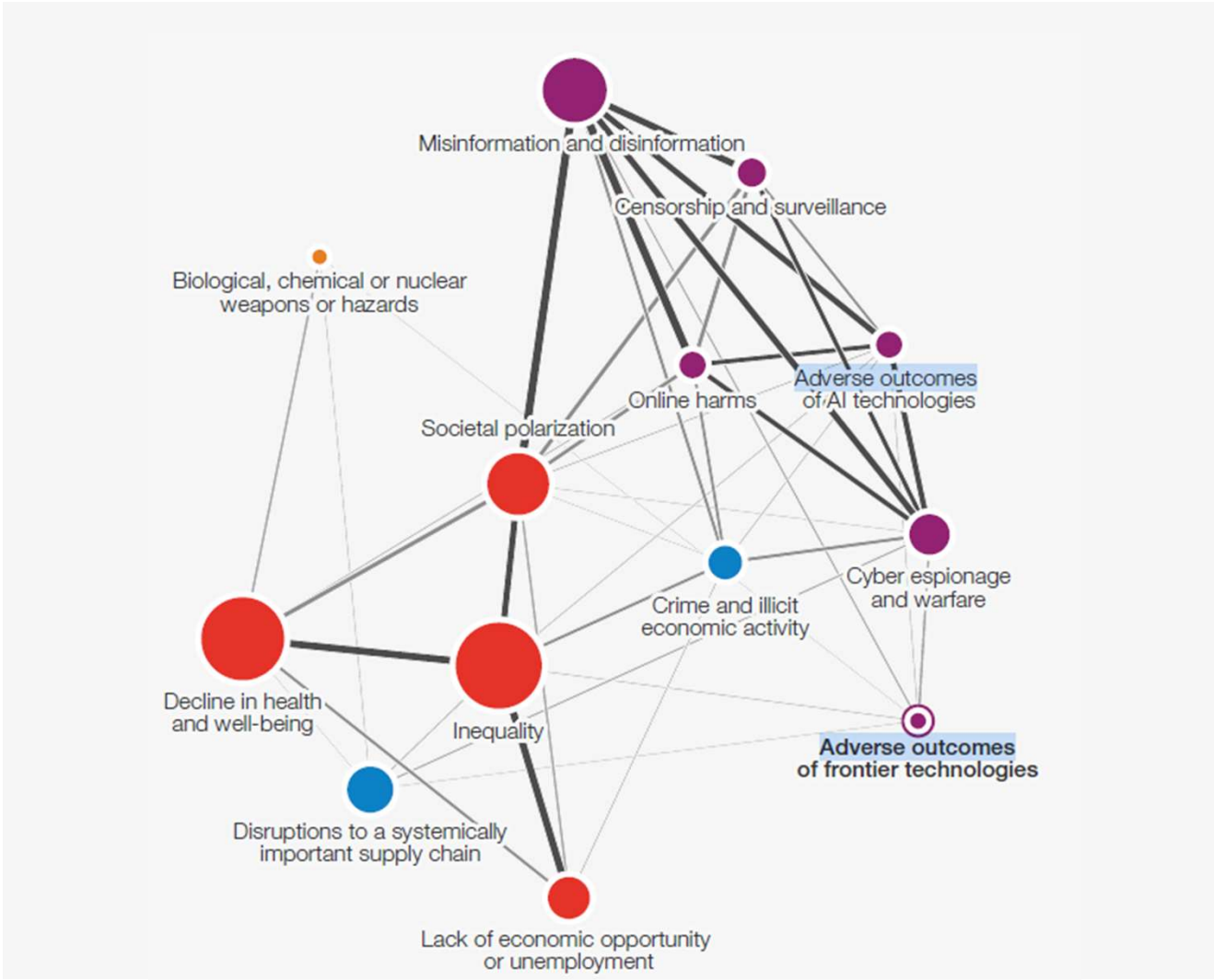
The U.S. Department of State, the U.S. Department of the Treasury, and the Federal Bureau of Investigation (FBI) are issuing this advisory for the international community, the private sector, and the public to warn of attempts by Democratic People's Republic of Korea (DPRK, a.k.a. North Korea) information technology (IT) workers to obtain employment while posing as non-North Korean nationals. There are reputational risks and the potential for legal consequences, including sanctions designation under U.S. and United Nations (UN) authorities, for individuals and entities engaged in or supporting DPRK IT worker-related activity and processing related financial transactions.

https://ofac.treasury.gov/media/923126/download?inline

1 （3）テクノロジーリスクが生み出す経済リスク

Risk interconnections

テクノロジーリスクから派生するエコノミーリスクとして「システム上重要なサプライチェーンの混乱」「犯罪と不正な経済活動」が挙げられます



Note: WEF Global Risks Perception Survey 2024-2025
Source: World Economic Forum; Marsh McLennan analysis

MarshMcLennan

ECONOMIC

テクノロジーリスクによって生み出される経済リスク（抜粋）

AIによる、サイバー攻撃の多様化やハードルの低下は、第三世界を含む地域での不正な経済活動という形でサイバー犯罪を増加させます。これはサプライチェーンリスクの増加も意味し、思わぬリスクを発生させる可能性があります。

Disruptions to a systemically important supply chain **システム上重要なサプライチェーンの混乱**	世界経済、金融市場、社会に影響を及ぼす、グローバルに重要なサプライチェーンまたは産業の重大な混乱または崩壊により、グローバル規模で、システム上重要な商品およびサービスの需給に急激な衝撃が生じる。これには、エネルギー、技術的ハードウェア、医療用品、消費財などが含まれるが、これらに限定されない。
Crime and illicit economic activity (incl. cyber) **犯罪と不正な経済活動（サイバーを含む）**	国境のない、かつデジタルベースで促進される、経済発展と成長を損なう組織犯罪や企業・個人の違法行為の世界的蔓延。以下を含むが、これらに限定されない。不正な資金流動（脱税、制裁逃れ、マネーロンダリングなど）、不正取引および密売（偽造、人身売買、野生生物取引、武器など）、サイバー犯罪（ランサムウェア、データ盗難、オンライン詐欺など）

Note: WEF Executive Opinion Survey 2024
Source: World Economic Forum; Marsh McLennan analysis

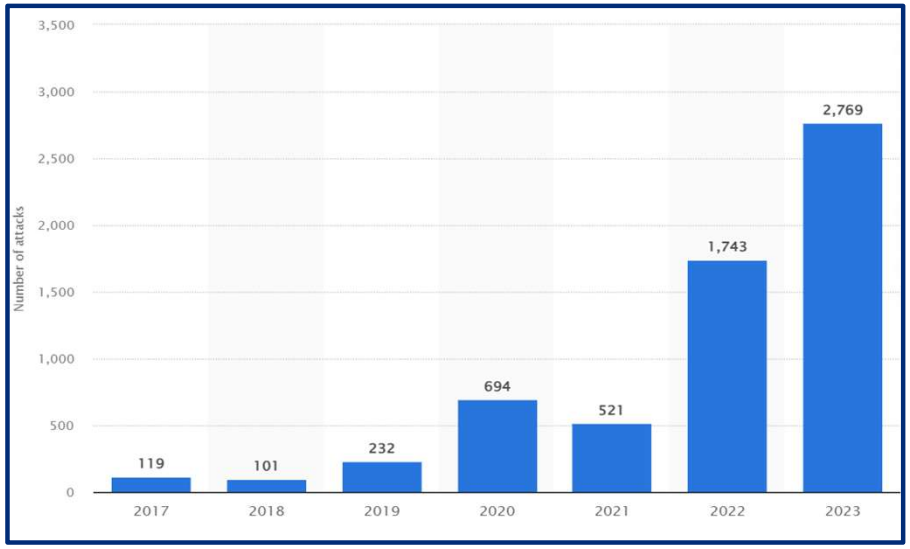
Disruptions to a systemically important supply chain
システム上重要なサプライチェーンの混乱

テクノロジーや大規模なシステムインフラの集中が、大規模なサプライチェーンリスクを引き起こす可能性があります。

市場集中の定着化

- AI技術の生産は、グローバルに統合された単一のサプライチェーンに高度に集中しており、 一握りの企業や国に偏在している。**そのため、重大なサプライチェーンリスクが、 今後10年間に顕在化するかもしれない。**
- 少数のAI基盤モデルが、金融や公共セクターなどで広範に展開されたり、**単一のクラウドプロバイダーに過度に依存したりすると、システミックなサイバー脆弱性が生じ、 重要インフラが麻痺する可能性がある。**

サプライチェーンを狙った攻撃は著しく増加



出典: Annual number of supply chain cyber attacks U.S. 2023 | Statista

Disruptions to a systemically important supply chain
システム上重要なサプライチェーンの混乱

トヨタ自動車 Toyota Automotive. – Feb 2022

- 2022年3月1日（火）、トヨタのサプライヤーである小島プレス工業株式会社がサイバー攻撃を受け、国内14工場28ラインの稼働を停止
- 同社とトヨタにシステムの直接的なつながりはありませんが、システム停止により部品の受注、納品が出来ない状態に
- トヨタ自動車は、1日の操業停止後、国内の全工場で作業を再開
- 1日の国内生産停止は、2月の生産台数の約5%に相当する約13,000台分の生産に影響

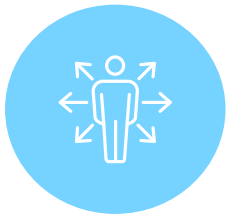
Yanfeng Automotive. – Nov 2023

- 上海に本拠を置く、世界的な自動車部品サプライヤーYanfengは、主にランサムウェア攻撃を行う Qilinにシステムへ侵入され、重要なファイルやデータが暗号化される
- システムの復旧とセキュリティ対策のため業務が一時停止し、顧客へ影響
- ステランティスでは、一時完全に組立がストップ
- その他は下記のとおり
  - フォード (Ford)　：部品供給の遅延がフォードの製造ラインに影響し、生産スケジュールに遅れ
  - ゼネラルモーターズ (GM)　：一部車両モデルの生産に影響、納品遅延が発生
  - トヨタ (Toyota)　：部品の品質管理に問題が生じ、製品に影響のリスク
  - ホンダ (Honda)　：製造スケジュールや納期に遅れが生じる可能性

Disruptions to a systemically important supply chain
システム上重要なサプライチェーンの混乱

CIE Automotive – Dec 2023

- スペインに本社を置くグローバルな自動車部品サプライヤー、CIE Automotiveは、2023年12月7日にCactusグループによるランサムウェア攻撃を受けました。
- CactusグループはVPNアプライアンスの脆弱性を悪用してネットワークに侵入し、ランサムウェアを展開しました。
- CIE Automotiveへの攻撃は、サプライチェーン全体に広範な影響を及ぼしました。主要な自動車メーカーへの部品供給が一時停止し、生産ラインが停止する事態が発生しています。
- フォード、トヨタ、ゼネラルモーターズ、フォルクスワーゲンなどの顧客企業での生産スケジュールに遅れが生じ、納品遅延が発生しました。また、部品の品質管理に問題が生じ、最終製品の品質にもリスクが発生しました。



CDK Global. – Jun 2024

- CDK Globalは北米の約15,000の自動車販売店にソフトウェアを提供しています。このソフトウェアは不動車部品の販売・注文と追跡、新規販売、融資など幅広い機能を持っています。
- 2024年6月にBlackSuitというハッカーグループによる2回のサイバー攻撃を受けました。
- 攻撃により販売管理システムが停止し、販売店では紙とペンによる業務を余儀なくされ、販売、修理、部品供給に影響が出ました。
- 四半期末の販売が遅延し、販売店に大きな財務的影響があり、販売店全体で1億ドル以上の損失が発生しました。最大で９億ドル以上との試算もあります。

ECONOMIC

Disruptions to a systemically important supply chain
システム上重要なサプライチェーンの混乱

- Tier1から、４，５ ・・　と国際的に複雑なネットワークを構成しています。
- テクノロジーリスクで挙げた、AIの活用によるサイバー攻撃の容易化は、第三世界でのサイバーリスクを増大させ、サプライチェーンの混乱を増幅させると予想されます。

サプライチェーンリスクを理解しマネジメントする実践的な方法

バリューチェーンの上流・下流の両方を包括的に可視化：人工知能（AI）やビッグデータを扱うツールを活用すれば、サプライヤーをデジタル上でマッピングして、世界中のサプライチェーン情報をタイムリーに更新する環境が整います。

潜在的な脆弱性を特定：過度のサプライヤーの集中や、サプライチェーンのボトルネックといった構造的な問題を特定することが重要です。リスクの観点からは、全てのサプライヤーが同等に重要なわけではありません。時として、基幹部品を納入するものの小規模でリスク要因とならなさそうなサプライヤーが大規模で不均衡なサプライチェーンの分断の原因になり得ます。

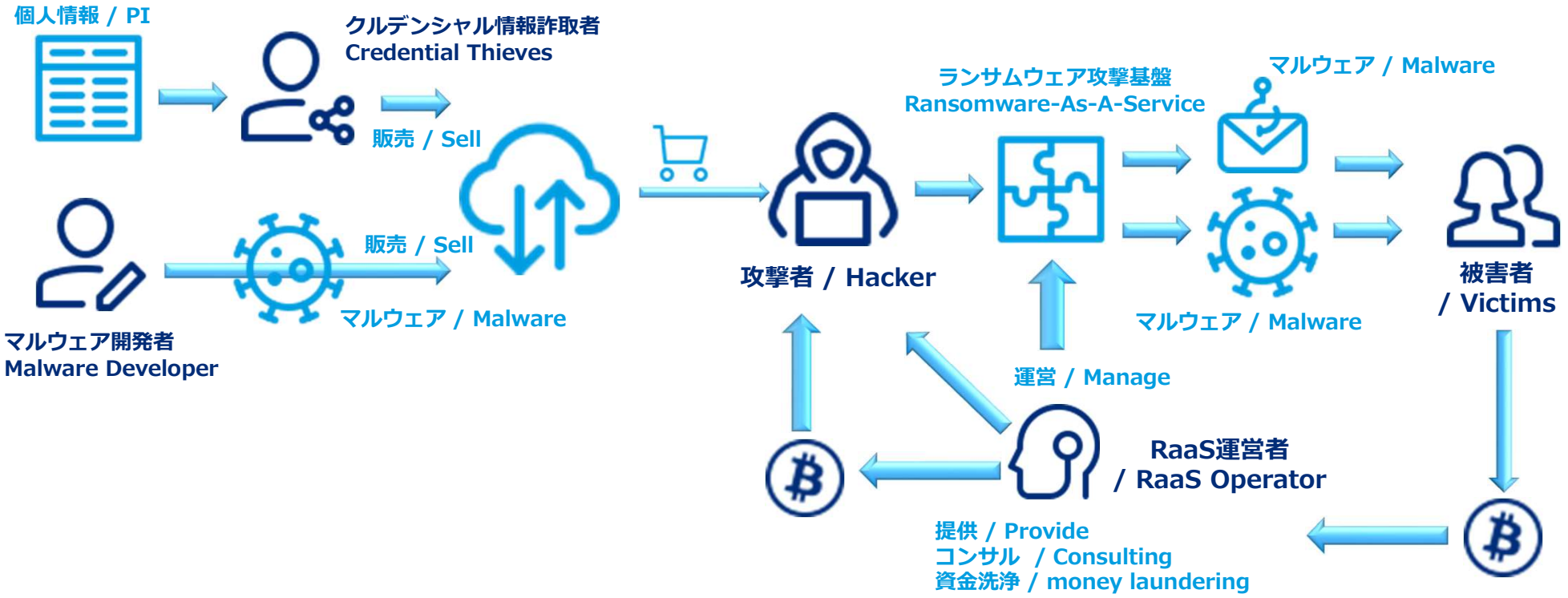
サプライチェーンに影響を及ぼす主要リスクを洗い出す：自然災害、地政学的な制裁、サイバー攻撃、財務パフォーマンスなどの主要リスクに加え、レピュテーションリスクも考慮する必要があります。

Driven by unforeseen geopolitical disruptions and regulatory changes

出典：サプライチェーンの多様化と分散:
適切な保険手配によるリスクマネジメント
（Marsh）

Crime and illicit economic activity (incl. cyber)
犯罪と不正な経済活動

- サイバー攻撃は、ネット上に存在している各種のサービスを利用することで、簡単に行うことができます。
- また、２019年に摘発された。Evil Corpのように、オフィス、給与、休暇、福利厚生を備えた、ビジネス化された犯罪組織も多く存在しています。



1 （4）これらリスクへに対処について

まとめ：経営イシューとしてのサイバーセキュリティ

◆ 世界経済フォーラムでの大規模な調査によると、今後１０年間において下記のような**新たなリスク**の増大が懸念されます。

- ✓ AIの社内活用により、**自らが情報漏洩する**、ＡＩの誤用による偽情報が流布する等による**訴訟リスクやレピュテーションの低下**
- ✓ 量子コンピュータの進展による暗号の危殆化。これによる**情報漏洩リスクの増大**
- ✓ 中低所得国まで広がるサイバー犯罪とそれによる**サプライチェーンの混乱**

◆ 併せて、国家主体の組織のよる犯罪の増加は、AIの発達によるフィッシングの巧妙化やディープフェイクの活用など**サイバー犯罪の多様化と件数の増加、回避が困難**といった形で顕在化しています。

◆ これらの事象は、年間売り上げの数パーセントに及ぶような、経済的損失をもたらす可能性があります。

◆ 加えて、大規模なインシデントにおいては、株価の下落による企業価値の毀損も懸念されます。

◆防止困難な経済的リスクの発生可能性の高まり

企業側の問題点

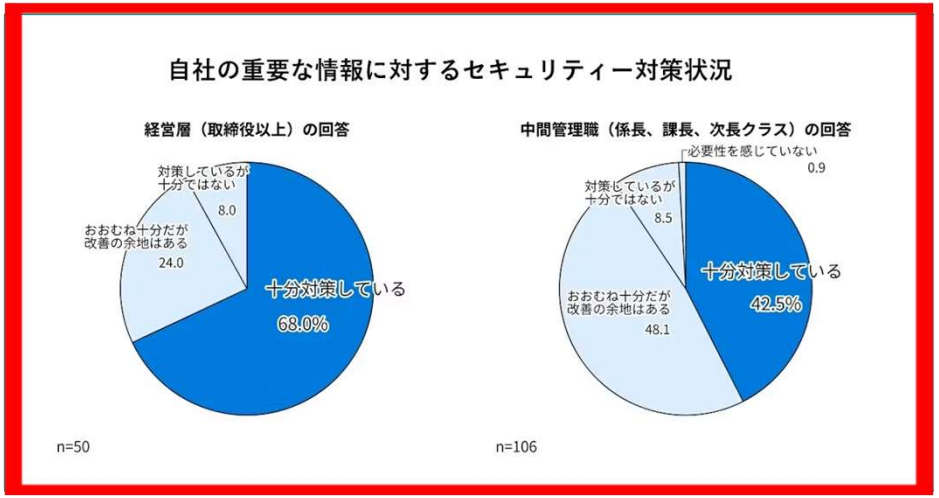
サイバーセキュリティへの経営陣の積極的関与は引き続き課題

- **企業側のリスクキャパシティーやリスクアペタイトが曖昧であり、受動的に対応しているように見える。**
  - サイバー保険においても、リスクキャパシティに基づく購入行動ではなく、予算ありきの購入となっている。
  - またその購入は、現場の担当者もしくは部長クラスが動くことが多く、予算に応じたキャパシティを買うという行動になりがち
  - そのため購買の決断までに時間がかかることが多く、その間に事故にあうこともある。

- **したがって、必ずしも経営陣が自社のリスクを適切に把握しているかは不明。**
  - 現時点では、経営者のサイバーリスクへの感度が高いとは言えない。

[経営層の7割、セキュリティー対策に自信　現場と隔たり - 日本経済新聞](https://www.nikkei.com/article/DGXZQOUC1630I0W5A110C2000000/?msockid=1adbfe7834c86b2a27c6ebe935b46a50)

https://www.nikkei.com/article/DGXZQOUC1630I0W5A110C2000000/?msockid=1adbfe7834c86b2a27c6ebe935b46a50



第２部で経営への意識喚起のための、具体的なポイントを解説します。

Part2　経団連推奨ガイドブック「サイバーリスクマネジメントの強化書」から学ぶ

(1) サイバーリスクマネジメントの根幹について

(2) 敵を知り己を知る事の大切さ

(3) リスクファイナンスとしてのサイバー保険の現状

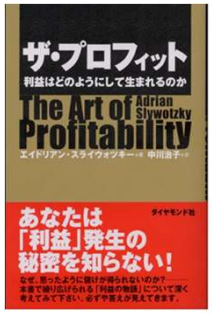
出版書籍実績

2000

2001

2001

2003



2003

2004

2005

2006

2008

2012

「サイバーリスクマネジメントの強化書」の構成

大前提

↓

準備
Readiness

↓

対応・復旧
Response＆ Recovery

↓

改善・再発防止
Refinement
Recurrence　Prevention

第1章
サイバー・リスクマネジメントは取締役の責任

第2章
サイバーリスクを見える化（己を知る）

第3章
脅威の監視・分析・ツール導入・トレーニングの導入

第4章
サイバーインシデント発生時の対応・復旧（敵を知る）

第5章
改善・再発防止

ケーススタディー

Marsh

経団連後援によるサイバーリスクマネジメントセミナー


日刊工業新聞 2024年10月24日(木曜日) 26

『サイバーリスクマネジメントの強化書』発売1周年記念セミナー

今、現場で起きている現実から学ぶ最も合理的な備えとは？

人材育成など日英で取り組み

国家のレジリエンス 産学官で

モノづくり日本会議

欧米で先行 保険で株主対策

モノを作る前に安全な仕組みを

見えぬ脅威へ備え 経営課題

マーシュ主催　経団連後援による
サイバーリスクマネジメントセミナー
@経団連会館/2024年9月5日

活発なパネルディスカッションに加えて
参加者からも多くの質問を受けました

ライブにて満員御礼且つアンケートでは
100%参考になったと回答


国際的な緊張の高まりから、国際的な連携や安全保障視点からの情報収集の重要性について

各国の事情 対話で理解深める／ＡＩの浸透 データをセキュアに

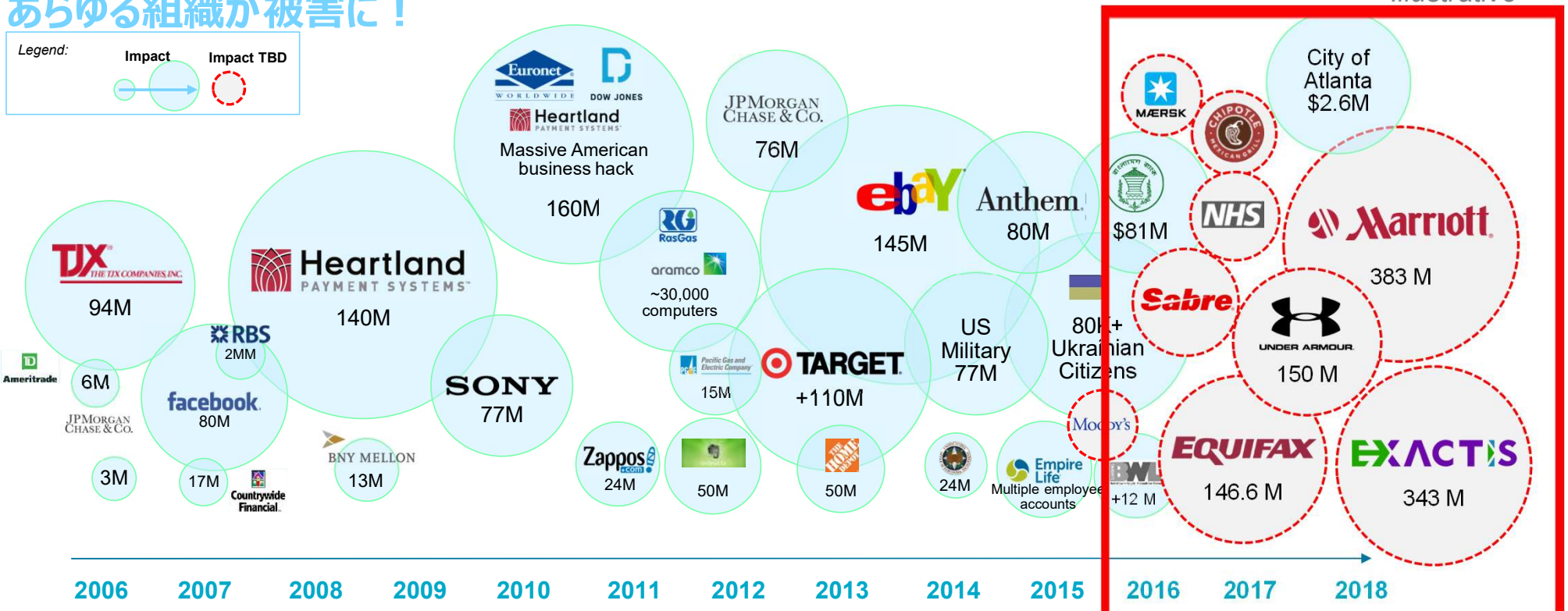
出典：日刊工業新聞　10月24日

具体的な実行の為のポイントとは

High Profile Cyber Attacks on the Rise

あらゆる組織が被害に！

Illustrative



Heartland was at the center of one of the biggest credit card scams in history, resulting in payments to VISA, Amex, and other credit cards

In 2011, 760 companies were hacked, including several financial services firms such as the Dow Jones, Heartland, and Euronet, Wells Fargo, and others

In 2013, JP Morgan Chase & Co was compromised by a cyber attack which ultimately gained access to administrative rights

In 2016, the Bangladesh Bank heist saw hackers walk away with 81M due to falsified payments. The intended sum was 1BN

In 2018, Marriott disclosed a breach of the Starwood Preferred Guest account system (which Marriott acquired in 2016). Initial reports estimated the affected records at over 500M however following additional investigation these estimates were reduced to 383M

出典: Industry, press. Oliver Wyman analysis

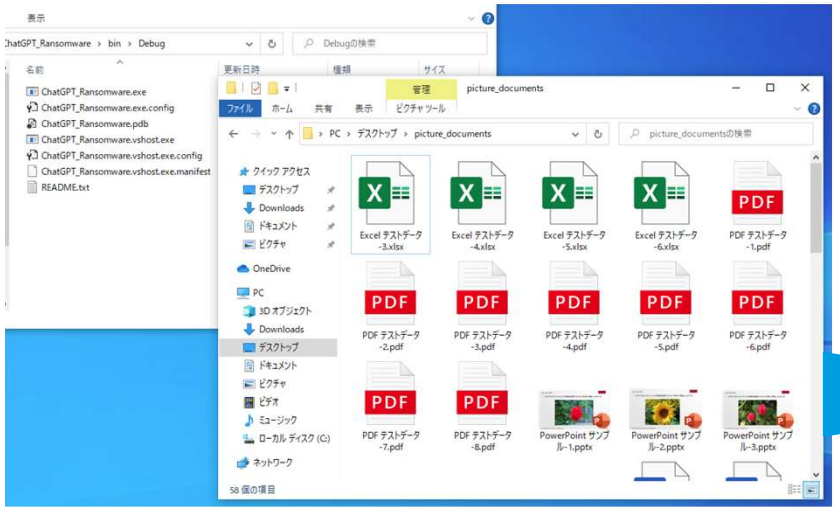
何故“もし”では無く“今”なのか？（残り５％の背景）
国家主導によるハッカーがどんなシステムでも100%侵入できるとしたら…

元ブラックハッカーとの対話

- 全米でも有名な元ブラックハッカーは2011年から2014年の間に20回ものハッキング行為を搭乗中に行いその年の4月にFBIに逮捕された。
- 彼は現在米国政府のアドバイザーでありセキュリティサービスを起業。
- 昨年、筆者にいかにもハッカーと言った風情で訪問してきた。
- 彼は自分の実績からほぼ100パーセントどのようなシステムでも侵入できることは自分の実績からも証明済み。
- 彼のセキュリティサービスのプレゼンを受けた。

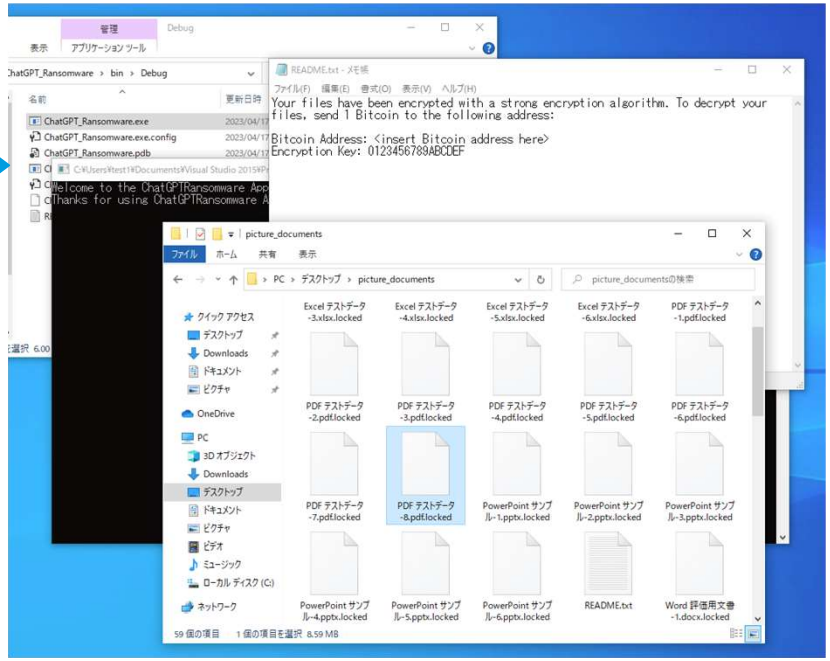
生成AIは言語能力が非常に高いために想定以上に悪用できてしまう

生成されたChatGPT製ランサムウェアを実行すると、正しく動作しファイルが暗号化された。



脅迫文までしっかり表示されていることがわかる

あくまでランサムウェアのコードを尋ねただけで、
身代金を要求する脅迫文の作成など具体的な指示は何もしていない。
つまり、「ランサムウェア」が何であるかを正しく認識して
コードを生成していることが分かる。

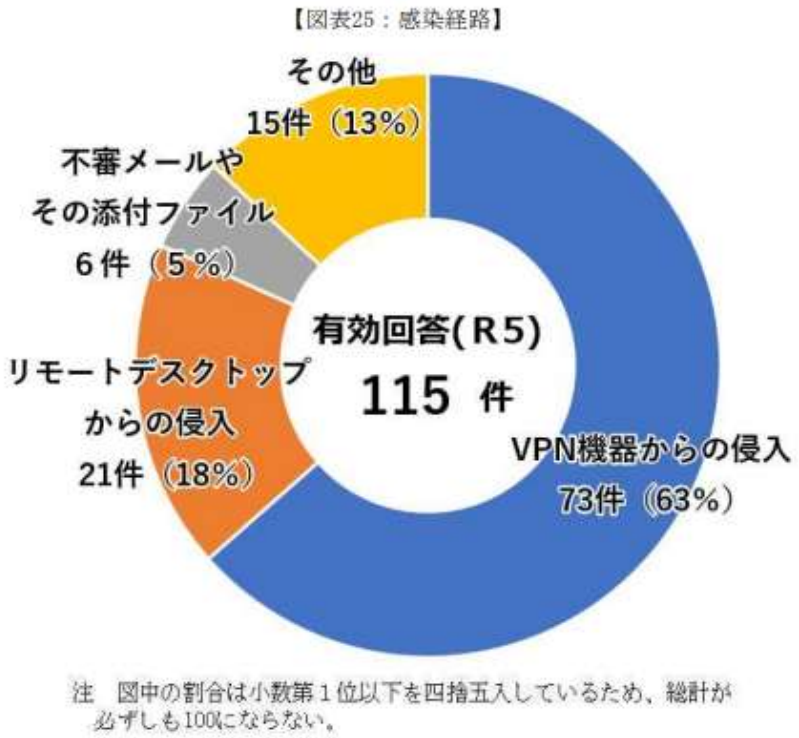


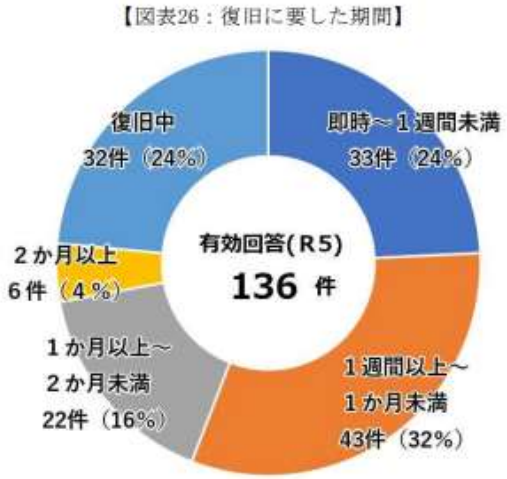
ChatGPTにコードを尋ねて
動くランサムウェアが完成するまで
５分もかからなった。

ChatGPTが公開されて間もなく、
アンダーグラウンドのハッカーフォーラムなどでは
こうした悪用の方法が活発に日々情報交換されている

出典：MBSD神吉敏雄様作成資料より引用

日本のランサムウェアによる被害事例(実は正面突破が殆ど)





出典　警察庁報告書 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

ヒューマンエラーがセキュリティ侵害の90%を占める

サイバーリスクに関する記事では、人為的ミスがサイバー事故とそれによる金銭的損失の主な原因であると言及され、**全セキュリティ侵害の最大90%以上** を占めている。

人的要因は、実際のミスというよりも、不適切なセキュリティカルチャーや人間の行動や善意の悪用と関係しています。人間が職場でどのように行動し、悪意のある行為者がどのように古典的な人間の特性を利用しようとしているかをよりよく理解することによって、人間の誤りやすさの領域を特定し、対処することが可能になります。

キーポイント

ヒューマンエラーとは、サイバー攻撃の責任は人にあるという意味だ。実際には、不十分なセキュリティカルチャーが人間中心の攻撃を助長している。

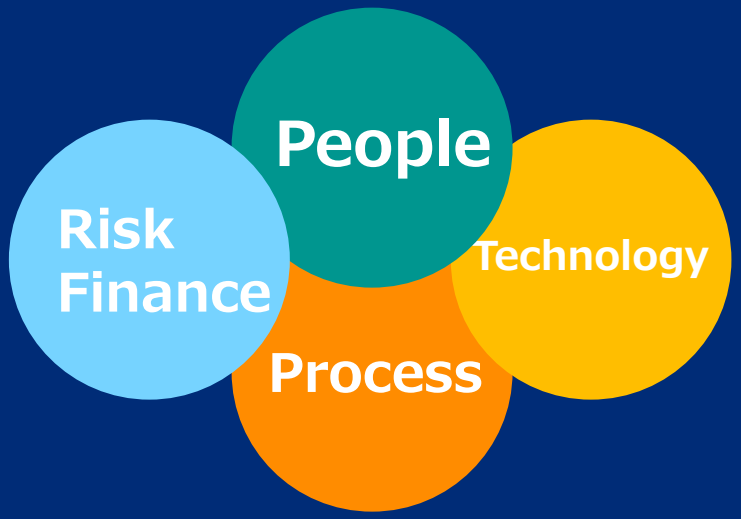
ソーシャルエンジニアリング攻撃の焦点は、より的を絞ったものになりつつあり、十分なアクセス権と特権を持つ人々を危険に陥れようとしている。

在宅勤務が増加している現在、個人はこれまで以上に悪意のある人物による攻撃に対して脆弱になっている。

出典：AIG ヒトサイバーリスク 防御の第一線 https://www.aig.co.jp/sonpo/global/trend/knowledge-insight/cyber-risk-management-facts

サイバーリスクは
取締役とガバナンスの重要課題
であり、**単なるITの問題では無い**
との認識が重要

加えて“**人的**”リスクである！
Artと**Science**の合わせ技



Technology = Technology Professional

People = Human Resource Professional

Legal Implication = Law Firm

Risk Finance = Risk & Financial Professional

Process = Combination of various Professionals

サイバーリスクは組織一丸となりBiz Riskとして経営が取り組む重要課題！
よってセキュリティファーストの経営が必須である！

Cyber risk management / key stakeholders d

	IT戦略（経営）	リスクアセスメント 可視化	リスク・コントロール プリベンション	リスク・トランスファー / ベーシス・リスクヘッジ
経営　CXO	◎	△	○	◎
IT責任者	◎	○	◎	×
監査役・社外取締役	×	◎	○	○
財務　CFO	◎	○	×	◎
法務	◎	◎	×	◎
HR	○	×	◎	×
Risk Manager　or 保険担当	×	◎	△	◎
現場 (生産・サービス)	○	◎	◎	×

サイバーリスク＝重要な経営課題

WHY?

（１）１００%防げない
（２）経営への信認の確保
（３）攻めには不可欠

ITインフラ　×　BIZ形態　×　TRIGGER

（INCIDENTの）

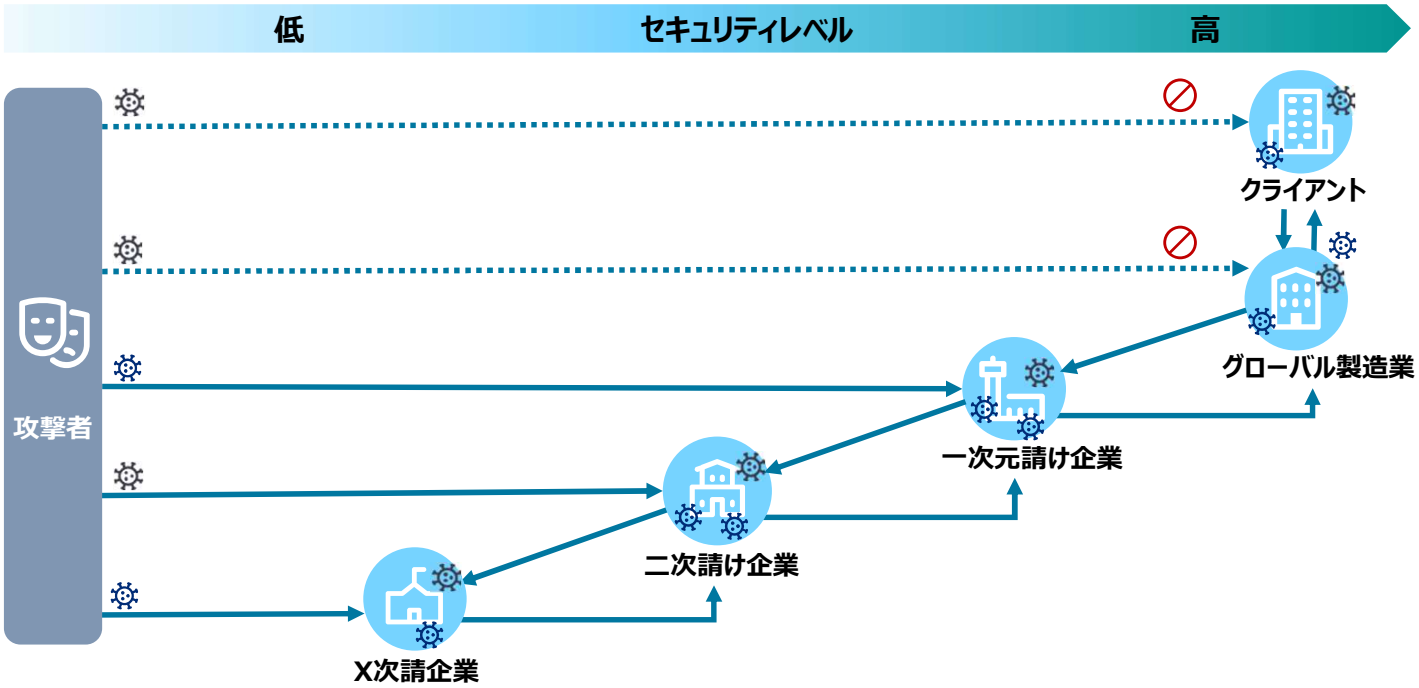
➡

経営財務指標の屋台骨をゆるがす可能性

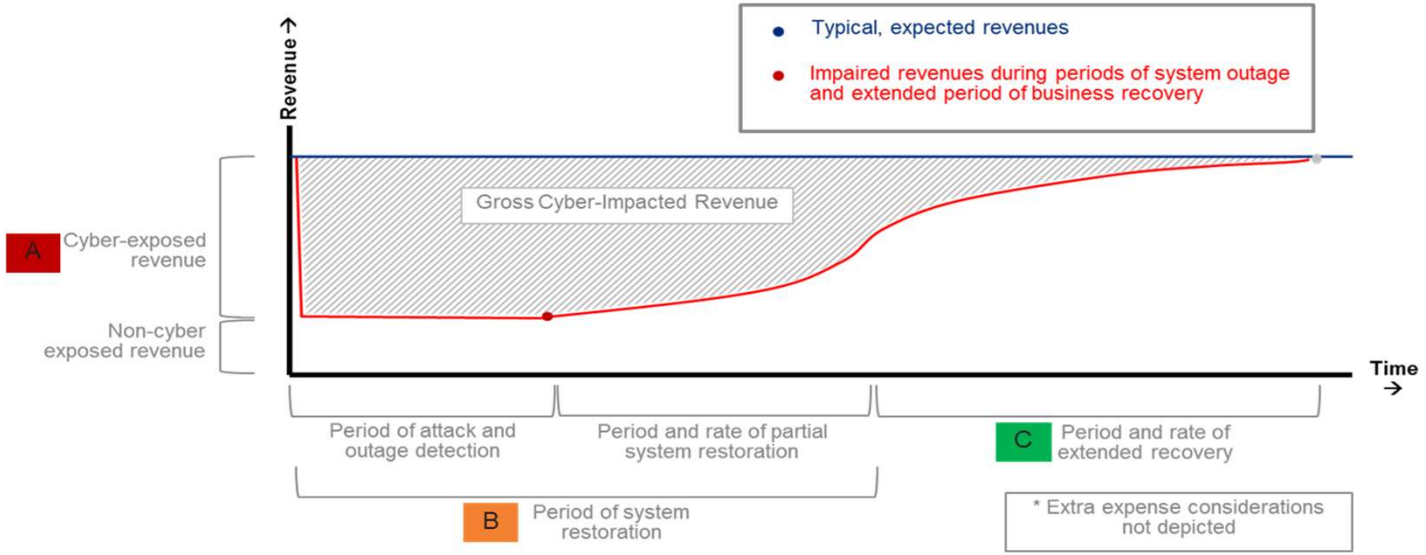
サプライチェーンリスクのイメージが出来てますか？

今やOEMとサプライヤーとの連携による支えあう仕組みと努力がより問われる時代である！

踏み台攻撃のしくみ（例）



Model Breakdown：事業中断のケース



A　サイバー事象が企業に重大な損害を与えた場合、影響を受ける可能性のある、ネットワークサービスに依存している企業の収益の部分。これには、中断による収益の遅延は含まれません。

B　サイバーイベントが発生した後、企業はインシデント対応を開始し、攻撃源と影響を受けた事業の領域を調査します。システムやアプリケーションがほぼ復旧すると、企業は業種に応じて収益を生み出す業務を、一定割合まで復旧します。

C　これは通常、全期間の中で最も長い期間となります。復旧期間とは、事業が「概ね操業可能な状態」から「完全に操業可能な状態」に復旧するまでに要する期間のことです。

日本に於ける現実から鑑みた場合
正面突破が90%でありSC3の提言は有益

2．注意喚起を受け企業で実施された取組事例（続き）

● **注意喚起**を契機に、**これまでのセキュリティ対策の徹底**や、**特に注意を要する箇所の点検**を実施する等の取組を実施している企業の事例は以下のとおり。

取組例 2　**普段から実施している対策の中で特に留意すべきポイントを点検**

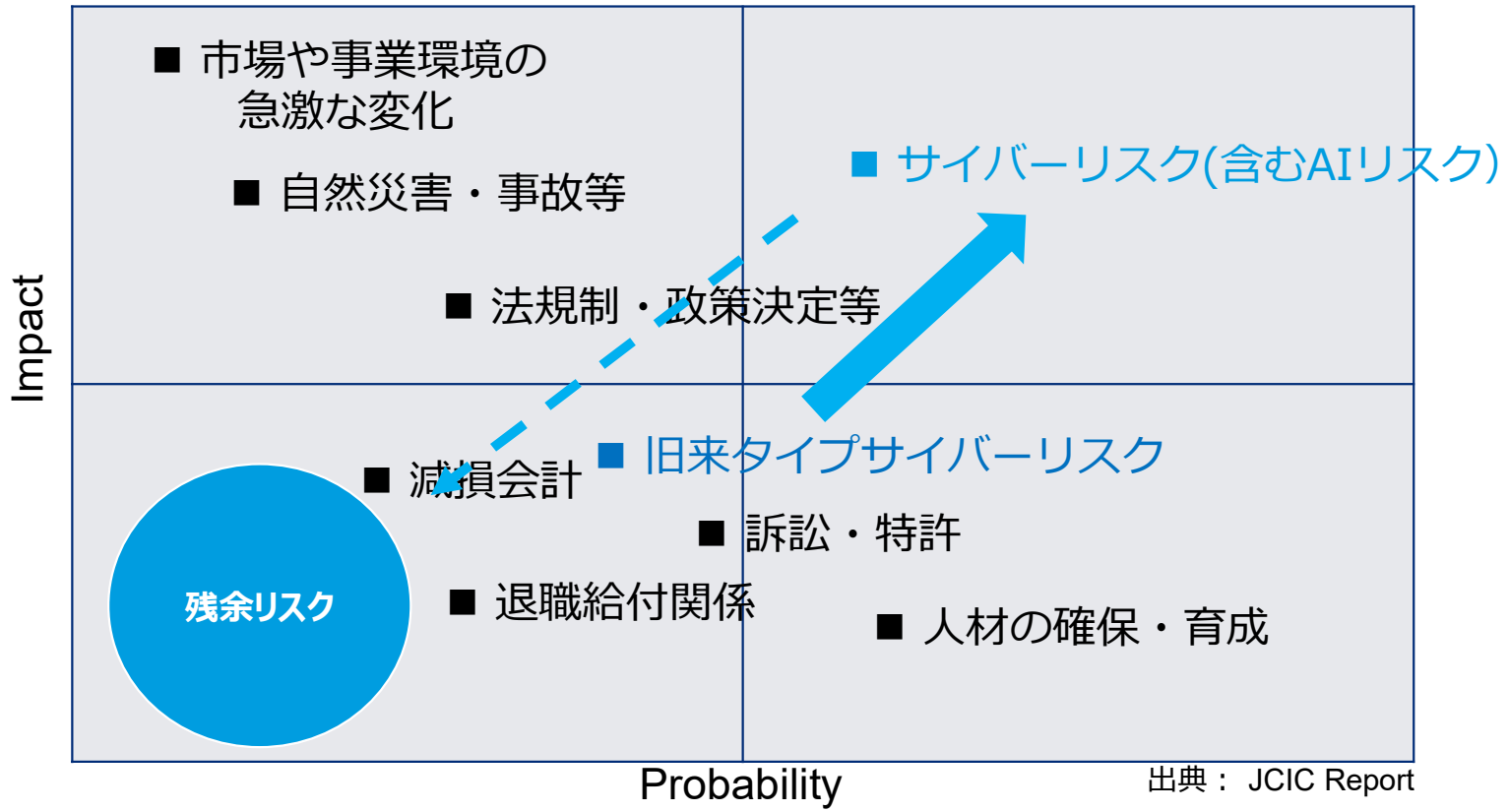
サイバー攻撃に対して、普段から実施している対策のうち、正面突破※1による攻撃への対処に加えて、人的対応、及びビジネス面の観点で留意すべきポイントを整理し、点検した。

正面突破による攻撃への対処の確認	• サプライチェーンとのネットワーク接続点の安全確認（IPSなどで不正通信の検知・ブロックできるようになっているか、未承認の接続ポイントはないか）。 • ネットワーク出口の機器の脆弱性が残っていないか。認証強度（不特定の第三者の接続を許可している場合には多要素認証）は十分か（リモート接続、VPN接続、クラウド接続を含む）。
人的対応に関する確認	• MS-Officeの文書を開く時、マクロ実行禁止になっているか、手動で自動起動に修正していないか。
ビジネス面の確認	• サプライチェーンの業務が停止した場合の代替手段は用意されているか。

※1 インターネット接続における脆弱性の悪用や認証の突破等による不正アクセス

出典：SC3　2022年3月31日　攻撃動向分析・対策WG　サプライチェーンにおけるサイバーセキュリティ対策の強化について
https://www.ipa.go.jp/security/sc3/activities/kougekiWG/

サイバーセキュリティは経営課題　－　先ずは見える化が第一歩



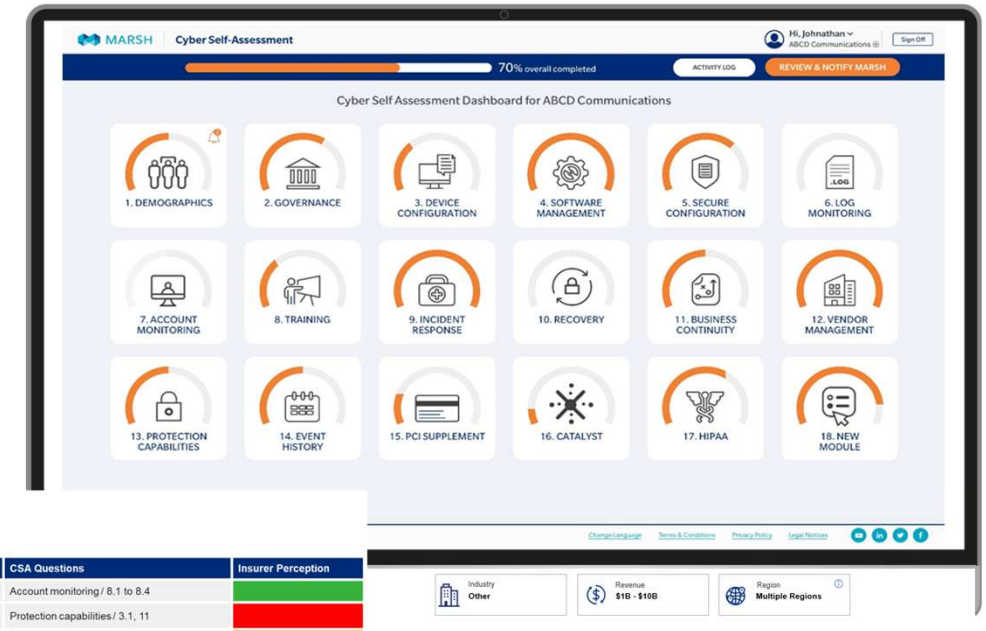
出典： JCIC Report

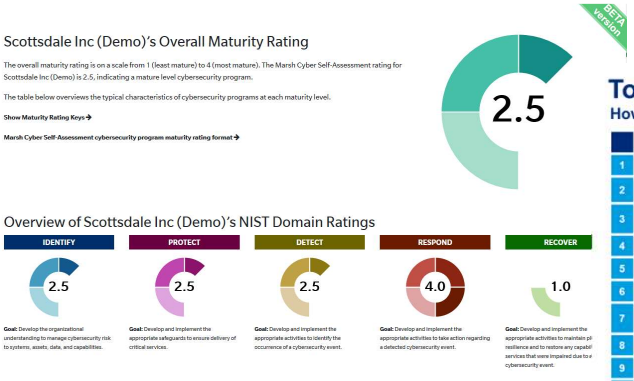
Marsh Cyber Risk Self Assessment ※詳細はAppendixをご参照

NIST、CIS等の業界標準をベースに、貴社のサイバーセキュリティ成熟度を診断し、お客様の保険加入とリスク緩和戦略を支援します。

Benefits → Output:

- **Cyber Insurance application** →サイバー保険の申込回答は、申込書類のみとなり、追加の提案書記入は不要です。
- **Cybersecurity controls commentary** → NISTサイバーセキュリティ・フレームワークに基づくサイバーセキュリティ・スコアカード
- **Cybersecurity position compared to peers** → コントロールのベンチマーク





Top Cybersecurity Controls

How did Scottsdale Limited score?

	Key Controls	CSA Questions	Insurer Perception
1	Multifactor authentication for remote access and admin/privileged controls	Account monitoring / 8.1 to 8.4	
2	Endpoint Detection and Response (EDR)	Protection capabilities / 3.1, 11	
3	Secured, encrypted, and tested backups	Recovery / 1.1 to 1.8 Protection capabilities / 1.1	
4	Privileged Access Management (PAM)	Account monitoring / 7.1 to 7.3, 9.2	
5	Email filtering and web security	Protection capabilities / 3.1 to 3.2	
6	Patch management and vulnerability management	Protection capabilities / 4.1, 4.2 to 4.6, 5.1	
7	Cyber incident response planning and testing	Business continuity / 1.1 Incident response / 1.2 to 1.3, 2.4, 4.1	
8	Cybersecurity awareness training and phishing testing	Training / 1.1 to 1.2, 2.1 to 2.2, 2.6	
9	Hardening techniques, including Remote Desktop Protocol (RDP) mitigation	Secure configuration / 1.1, 2.1	
10	Logging and monitoring/network protections	Governance / 10.1 to 10.2 Log monitoring / 5.1	
11	End-of-life systems replaced or protected	Protection Capabilities / 6.1	
12	Vendor/digital supply chain risk management	Governance / 11.1 to 11.3, 12.1 to 12.2	

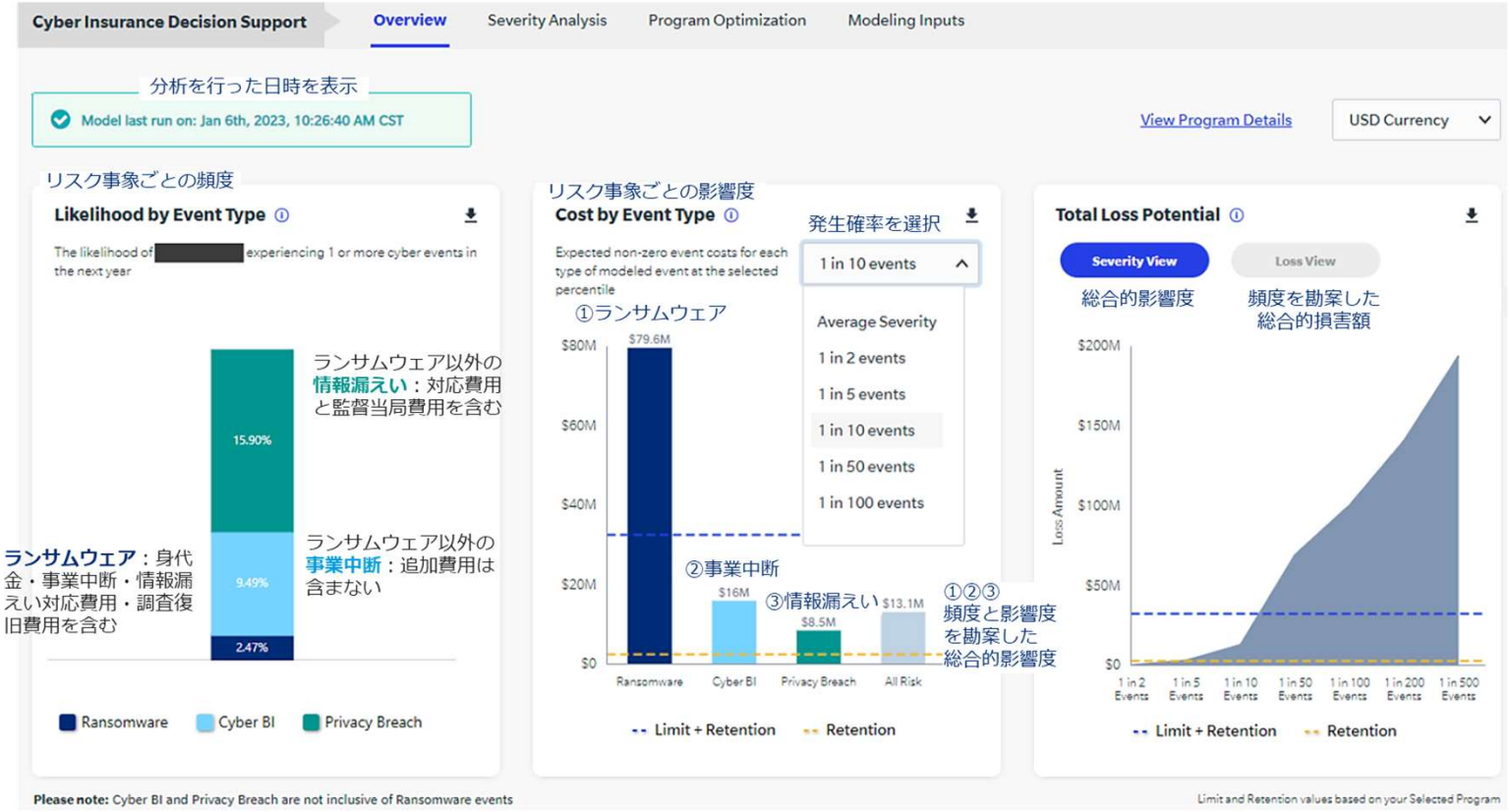
Marsh

Marsh Cyber Risk Quantification ①　Blue【i】Cyber

支払限度額 – 予想最大損害額（理論値）の試算 by 確率論的アプローチ

✓Marshには、予想最大損害額を確率論的アプローチで算出するモデルがあります（名称：Blue【i】Cyber）。

✓これを用いて、貴社のサイバーリスク（ランサムウェア、事業中断、情報漏洩）を定量化し、支払限度額の設定根拠といたします。



Cyber Peer Benchmarking of Key Controls / PeerとのKey Controlレベル比較

- １２のコントロール領域ごとに、対象企業と同等規模の企業の回答状況の比較が可能です。

Industry
Other

Revenue
>$10B

Region
United States of America

Response Overview

131 CSA Response

- Questions where your responses were better than your peers.
- Questions where your responses were same as your peers.
- Questions where your responses were worse than your peers.
- Questions where there was not enough data to generate a reliable peer comparison.

No.	Key Controls	Better Than Peers	Same as Peers	Worse Than Peers	Not enough Data
1	MFA controlled access for remote access & admin / privileged access	- 0%	70%	20%	10%
2	Endpoint Detection and Response (EDR)	3%	71%	25%	- 0%
3	Secured, encrypted and tested backups	11%	47%	41%	- 0%
4	Privileged Access Management (PAM)	- 0%	72%	22%	5%
5	Email filtering and web security	- 0%	50%	50%	- 0%
6	Patch management and vulnerability management	- 0%	14%	71%	14%
7	Cyber Incident Response planning and testing	6%	40%	53%	- 0%
8	Cybersecurity awareness training and phishing testing	- 0%	100%	- 0%	- 0%
9	Hardening techniques, including Remote Desktop Protocol (RDP) mitigation	- 0%	100%	- 0%	- 0%
10	Logging & Monitoring / Network Protections	- 0%	75%	25%	- 0%
11	End-of-life systems replaced or protected	50%	50%	- 0%	- 0%
12	Vendor / Digital Supply Chain Risk Management	- 0%	66%	33%	- 0%

経営にとってのリスクマッピング（可視化）活用のメリットとは

1．最悪のシナリオの具体的財務的損失と発生可能性を基に具体的な数値で議論が可能となる

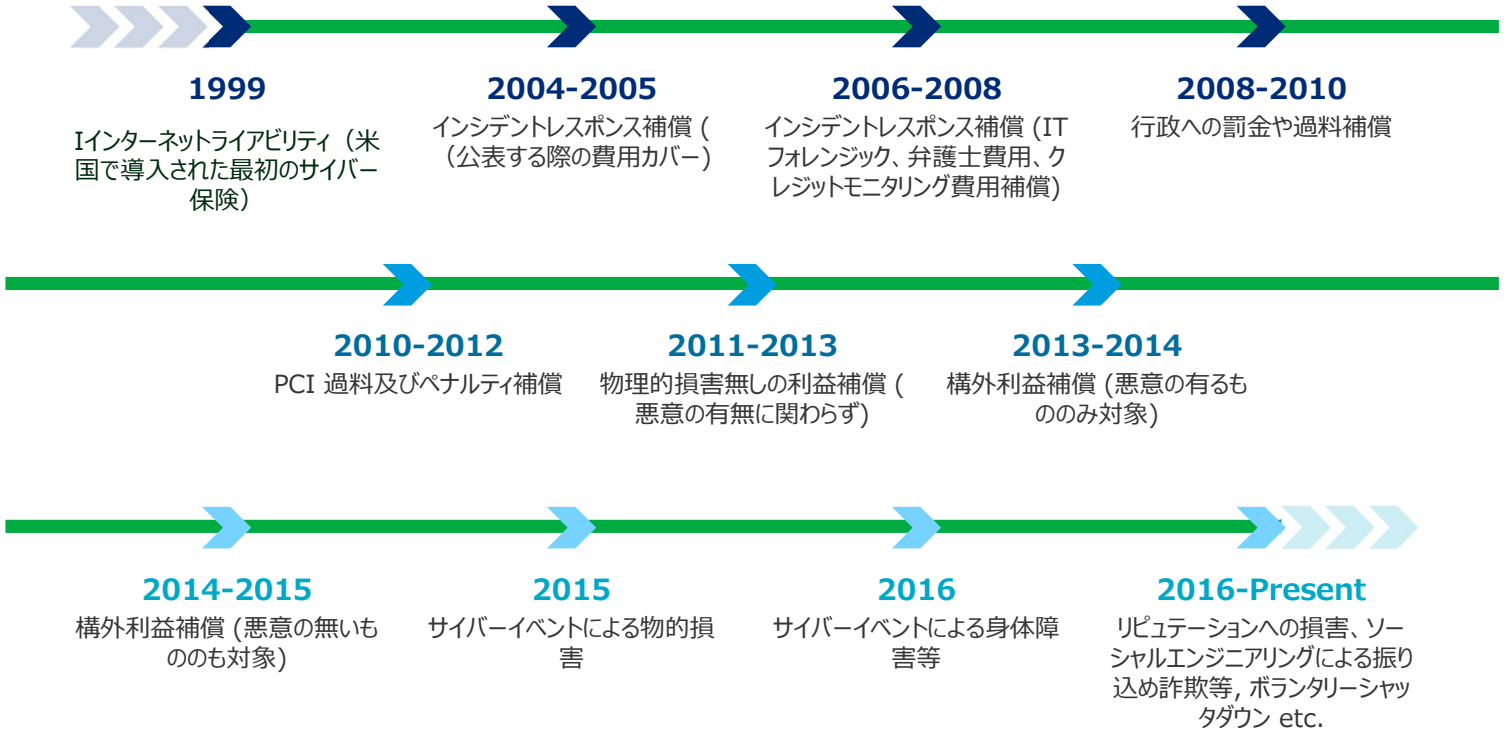
2．最悪の財務的損失のイメージを基にセキュリティ投資額の議論が具体的に可能となる

3．ベーシスリスク（最終的に残ってしまう財務的損失額）をイメージしやすくなる

4．セキュリティ人財への評価軸として活用し優秀な人財の確保と獲得がしやすくなる

5．PDCAを回すが如くに取締役による適切なアクションを継続できる

欧米でのサイバー保険の歴史的経緯- 日本との大きな違いとは



＊歴史的発展の経緯を示すもので現状全て都度確認が必要

保険会社主導の契約の最大の落とし穴

素人の購入者ではこの違いを認識及び検証すらできないのが現実

現行契約対象外

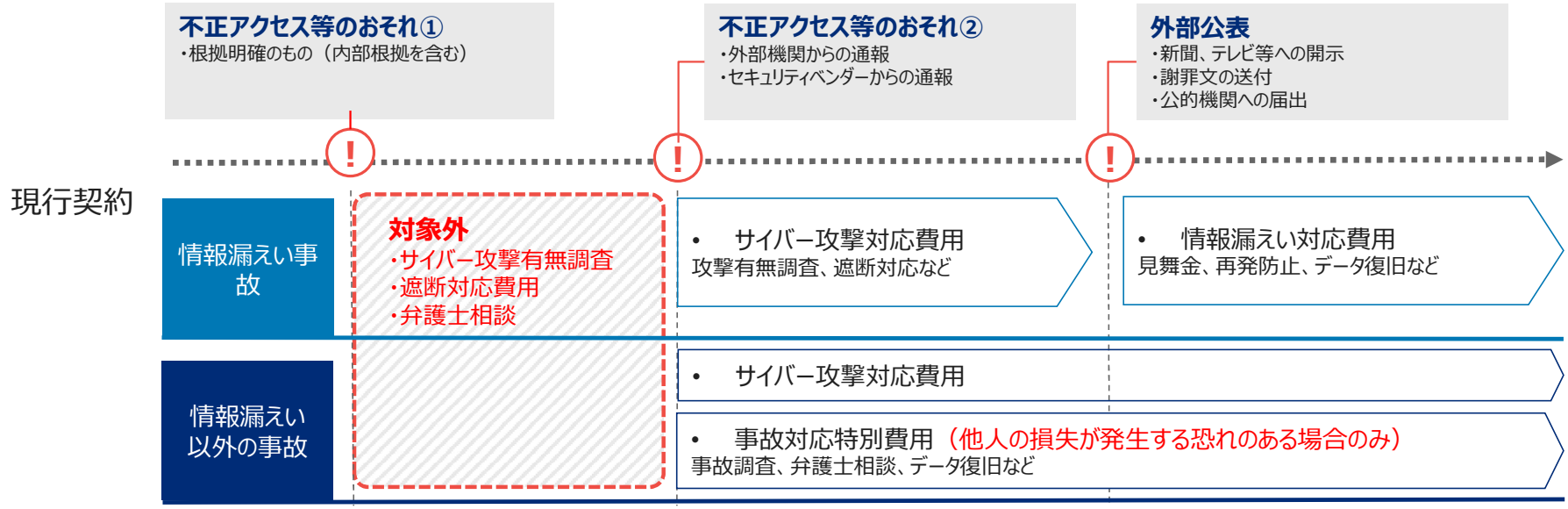
	損害			
対象事故	賠償	費用	拡張担保（費用）	事業中断
IT事故／不正アクセス等による情報漏えい	○	○	×	×
IT事故／不正アクセス等による情報漏えいのおそれ	▲	▲	×	×
漏えい以外のIT事故／不正アクセス等	× *プロダクトユーザー向け以外は担保	▲	×	×
情報漏えいか否かを問わずIT事故/不正アクセス等のおそれ	× *プロダクトユーザー向け以外は担保	▲	×	×

サイバー攻撃や不正アクセスに起因しない、
一般的な業務過誤による
賠償責任は対象外

（E&O保険の対象）

現行契約 vs ご提案のサイバー保険（殆ど現実には機能しない）

費用カバーの発動要件と項目の違い

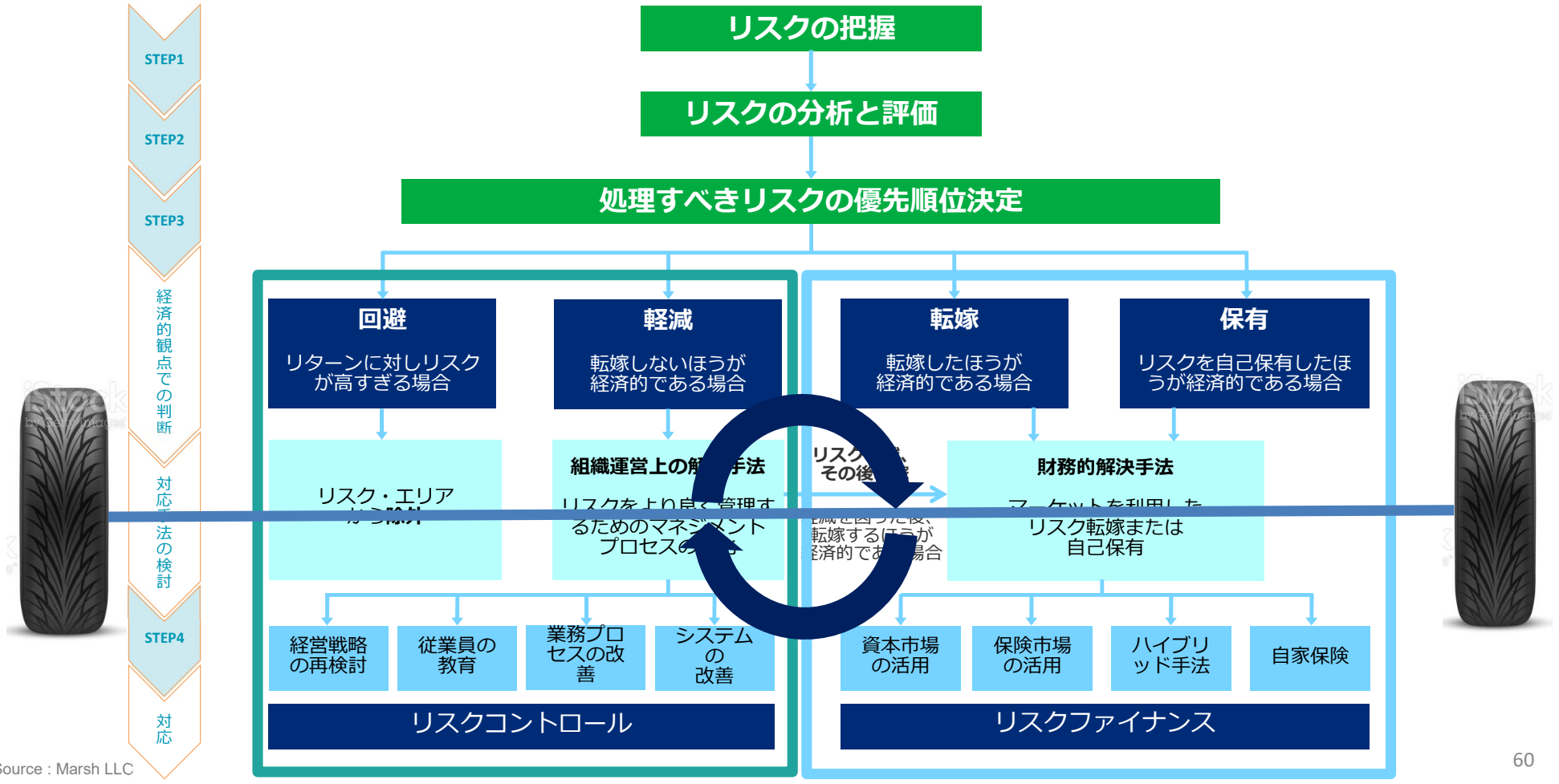


サイバー保険お見積もり結果事例
保険購入者ではそもそも比較検証できずコスト比較も至難の業

単位：円

支払限度額	免責金額	A	B	C	D	E	F
3億円	なし	4,276,600	8,033,680	10,283,890	-	-	6,080,420
5億円	なし	4,544,030	10,516,690	12,436,280	-	-	9,001,610
10億円	なし	4,770,970	16,573,650	19,739,080	-	-	16,128,100
その他プランのみ		-	-	-	支払限度額3億/ 免責金額1,000万円 5,800,000	支払限度額1億/ 免責金額250万円 1,800,000	-
各補償項目の 主な違い	各種費用補償	支払限度額or 5億円の低い方が限度	支払限度額まで	支払限度額まで	3億円限度	1億円限度	支払限度額まで
	事業中断補償	1億円限度	1億円限度	支払限度額まで	1億円限度	1億円限度	1億円限度
	ITサービスに起因する 賠償補償	あり	あり	あり	なし	なし	あり
	その他	リスク評価割引30%			ランサムウェアに起因する損害は 支払限度額 9,000万円		

デジタル・リスクマネジメントのプロセス
リスクコントロールとリスクファイナンスは車の両輪！



Source : Marsh LLC

セキュリティファーストの為のRisk Appetite Statementとは？
その重要性は？

Risk Appetite Statementとは、組織の目的や事業計画を達成するために、進んで受け入れるリスクの種類・量に対して受動的な対応ではなく、組織として望ましい形として能動的に対応していくこと。

それらは；

1. 鍵となるリスクの意識を高める
2. 意思決定のプロセスに許容すべきリスクに関して織り込むこと
3. 取締役と執行部とのアライメントを確実にする

レースカーにブレーキ（セキュリティ）を装着してなければユックリ走行せねばならない。
一方、ブレーキ（セキュリティ）を装着することで思い切り駆け抜ける事ができる。

そのようなバランスを持ったリスクアペタイトを明確化できているか？

Thank you so much !!!

ご清聴心より感謝申し上げます！