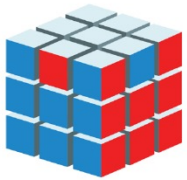
開演までしばらくお待ちください。

TANAAKK

TANAAKK



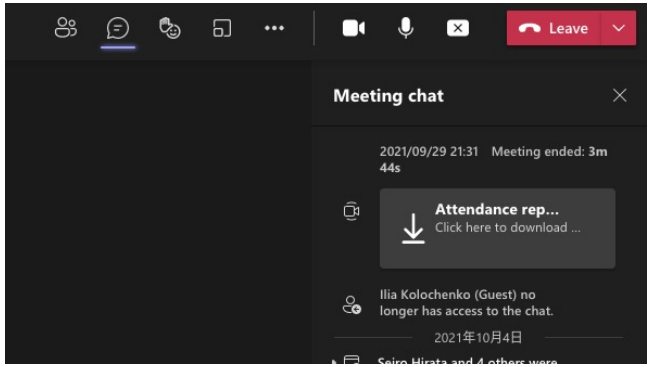
ImmuniWeb®

AI for Application Security

WEBINER勉強会概要

時間	内容	進行
16:00-16:05	開会 開会挨拶	事務局 木村 Tanaakk田中
16:05-17:00	ImmuniWeb®AI Platformの急速な伸びとPT-as-a-Serviceのセキュア開発への組み込み	イリヤ・田中 通訳 小林 ゲスト中本
17:00-17:30	国内法令・判例と商慣習に見るPT-aaSの市場性	Tanaakk青木
17:30-18:00	世界におけるPT-aaS市場、RegTech市場の伸びとセキュリティ監査に関する米国法令・ガイドラインの現状	大江橋平田
	閉会 開会挨拶	事務局 木村 Tanaakk田中

セミナー中にご質問がある場合はTeamsチャットに投稿してください。
ご意見・次回開催ご要望はアンケートフォームより投稿してください。
Tanaakk×ImmuniWeb勉強会アンケートフォーム
https://forms.office.com/r/26fB0GPUSM



ImmuniWeb®AI Platformの急速な伸びと
PT-as-a-Serviceのセキュア開発への組込

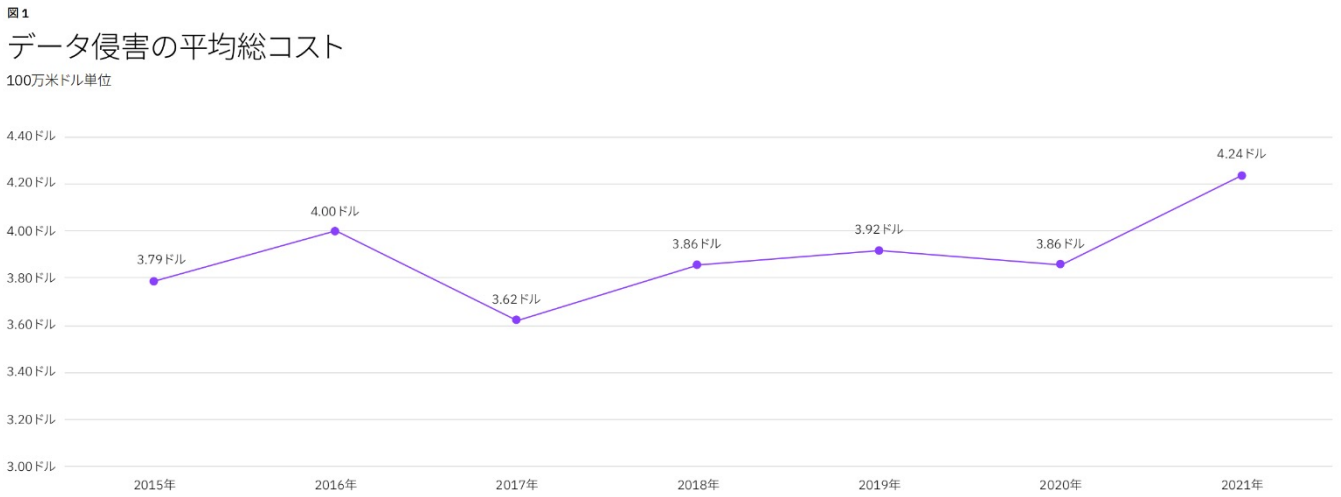
投影のみ

Tanaakk株式会社 創業者CEO田中翔一朗
ImmuniWeb SA 創業者CEOイリヤコロチェンコ

国内法令・判例と商慣習に見るPT-aaSの市場性

Tanaakk株式会社管理本部長 弁護士 青木正芳

データ侵害時のコスト



出所：IBM「2021年 データ侵害の コストに関する 調査レポート」

・データが侵害された場合の平均コストは年々増加しており、2021年の調査では、424万ドルとなっている（アメリカの平均は905万ドル,日本は469万ドル）

・侵害コストの内訳

①罰金・制裁金②企業価値の毀損③リーガルコスト④復旧コスト

・ 総合サイバーセキュリティ企業の論説では、「業界の専門家の間では、組織がサイバー上の侵害や攻撃に直面するのは、「If」の問題ではなく、「When」の問題であるというのが一般的な見解」とされる

※実際、Cyber Security.comでは、毎日ようにサイバーインシデントが報告されている

→セキュリティのリスクは、どの企業も危険にさらされていると考えるべき

ベネッセ事件

◆事件発生時：2014年７月９日

◆事件内容

・ベネッセの情報処理系子会社「シンフォーム」の派遣エンジニアが、データベース上の顧客データを持ちだし、複数の名簿業者に売却（最大2070万件の情報流出の恐れ）

・当該行為者は数百万円の利益を得た

◆法的問題点（リーガルコスト）

・刑事（個人の責任）：不正競争防止法違反（営業の秘密の複製、開示）

→懲役２年６ヶ月、罰金300万円（東京高裁：平成29年３月21日）

・民事：一人あたりシンフォームに対し3300円の賠償（東京地裁平成2018年12月27日）

※複数訴訟があり、損害なしと認定されたものもある

なお、ベネッセの役員に対する株主代表訴訟は、棄却（岡山地裁平成３０年９月12日）

◆その他問題点

①責任部署にいた取締役が引責辞任

②企業価値の毀損

ベネッセの売り上げ７％減、営業損益が前年期の39億1000万円の黒字から、４億3000万円の赤字に（出典不明）

③復旧コスト

「シンフォーム」を解散し「ベネッセインフォシェル」へ再編

※一人あたり500円程度で解決する事案が多い（機密性が高いものは３万円程度とされるものも）

個人情報の流出の特殊性

TANAAKK

◆外部不経済との類似性

・外部不経済

市場を通じて行われる経済活動の外側で発生する不利益が、個人、企業に悪い効果を与えること（引用：ブリタニカ国際大百科事典 小項目事典）

Ex:公害、騒音

・政府の介入

市場で解決できない問題を、汚染物質の排出規制や、エンジン音の規制など、政府が介入し、市場の不完全性を補完する

・個人情報の流出の特徴

集めた個人情報に対してセキュリティ対策をして、そのコストを販売価格に乗せると、価格の面で他社より競争力がなくなる恐れ

一方、消費者にとって一人一人の情報流出は、大きな問題となりえず、企業に対して交渉力を持ち得ない

しかし、個人情報が流出することで、特殊詐欺の対象になったり、不当な営業活動を受けたり、個人のプライバシーが侵害する恐れ

GDPR（General Data Protection Regulation：一般データ保護規則）

TANAAKK

◆概要

・2016年にGDPRが採択され、2018年５月に施行された

・個人情報の管理者・処理者に、個人情報の取扱の安全性の確保、取扱活動の記録、侵害時の通知などの義務を定めている

・義務違反や個人情報の流出があった場合、（1）「最大1000万ユーロ、または全世界年間売上高の2％のどちらか高い方」（2）「最大2000万ユーロ、または全世界年間売上高の4％のどちらか高い方」（重い義務違反）

◆これまでの運用実績

・2020年1月28日以降の約1年間で報告された罰金の総額は1億5850万ユーロ（約200億円）である（直近20ヶ月の罰金総額は、GDPRの施行日からの20ヶ月総額に比較して39%増加している）

（出所：DLA Piper: "DLA Piper GDPR fines and data breach survey: January 2021"）

・有名な罰金事例は以下の表の通り

社名	日付	事件の概要	罰金額※
Google	2019年1月	クッキーを、利用者の同意なく送付し、その情報を利用	5000万ユーロ
British Airways	2020年10月	５０万人の顧客情報流出	2200万ユーロ
Amazon	2021年7月	現在詳細は不明	７億4600万ユーロ

※但し、これらの額は、悪質性等を判断し、その後減額されることもあるようである

CCPA

◆アメリカ全体について
・個人情報に関する包括的な連邦法は存在せず、金融（Gramm-Leach-Billey Financial Modernization Act of 1999） 、医療(Health Insurance Portability and Accountability act of 1996)など各分野の業法で、規制されている
◆カルフォルニア州の規制
・2020年1月、カリフォルニア州で、包括的な個人情報に関する規定である
CCAP(California'sComsumerPrivacy Act)が施行された
・ポイント
個人情報が流出した場合、消費者一人あたり損害額を100ドルから750ドル以下と推定される（実害が大きい場合は実害の額）
→オプト-アウトのクラスアクションが可能（損害賠償額が莫大になる恐れ）
　10万人のデータが流出すると、最低でも1000万ドルの賠償金となる
・域外適用
　カリフォルニア州の消費者の個人情報を保有していると、域外適用される恐れあり
◆訴訟の在り方
実際に訴訟を行い、規制を明確化させる文化
①CCPAが発効する前の2019年9月16日から2019年11月11日だが、Salesforceがマルウェアに感染したことにより、Hanna Anderssonのウェブサイトにアクセスした消費者の個人情報が盗まれるリスクが高まったと訴訟を提起
②2020年2月18日、セキュリティおよびスマートホーム企業のRing社に対して、、Ring社が適切なセキュリティを実装していなかったこと、及び消費者の個人情報を同意なしに未承認の第三者と共有したと主張しています（opt -outできることを消費者に通知する必要がある）

個人情報保護法の改正

・2022年が４月施行予定の、改正個人情報保護法87条では、これまで法人に対する罰金も個人と同様「50万円以下」の罰金とされいたが、法人に対し「１億円以下」の罰金を課すことができることになる
・具体的には、
①個人情報保護委員会の命令に従わない場合（同法83条、同法42条２項、同条３項）
②役職員が会社内で構築された個人情報を不正な目的で盗用した場合（同法84条）

現行法の個人情報保護法の条文

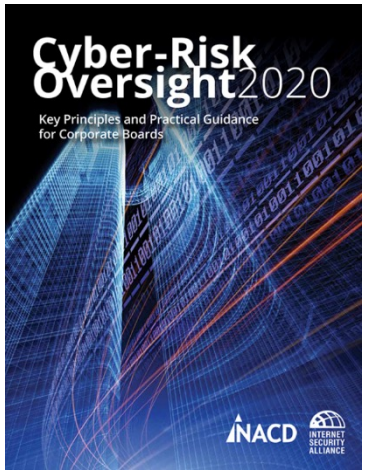
第87条　法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関して、第83条から第85条までの違反行為をしたときは、行為者を罰するほか、その法人又は人に対しても、各本条の罰金刑を科する。
２　法人でない団体について前項の規定の適用がある場合には、その代表者又は管理人が、その訴訟行為につき法人でない団体を代表するほか、法人を被告人又は被疑者とする場合の刑事訴訟に関する法律の規定を準用する。

※８３条、８４条、８５条は、個人が規律に従わない場合の罰金を定めその額は、50万から３０万円以下である

改正法の個人情報保護法の条文

第八十七条　法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関して、次の各号に掲げる違反行為をしたときは、行為者を罰するほか、その法人に対して当該各号に定める罰金刑を、その人に対して各本条の罰金刑を科する。
一　第八十三条及び第八十四条　一億円以下の罰金刑
二　第八十五条　同条の罰金刑
2　法人でない団体について前項の規定の適用がある場合には、その代表者又は管理人が、その訴訟行為につき法人でない団体を代表するほか、法人を被告人又は被疑者とする場合の刑事訴訟に関する法律の規定を準用する。

日本商慣習



「Director's Handbook on Cyber-Risk Oversight」の2020年度版

「サイバーリスクハンドブック（取締役向ハンドブック）」

◆新しい制度の輸入傾向

・日本は、リスクの問題を自国発進で考えるより、アメリカやヨーロッパで発生した問題や規制を輸入する傾向にある

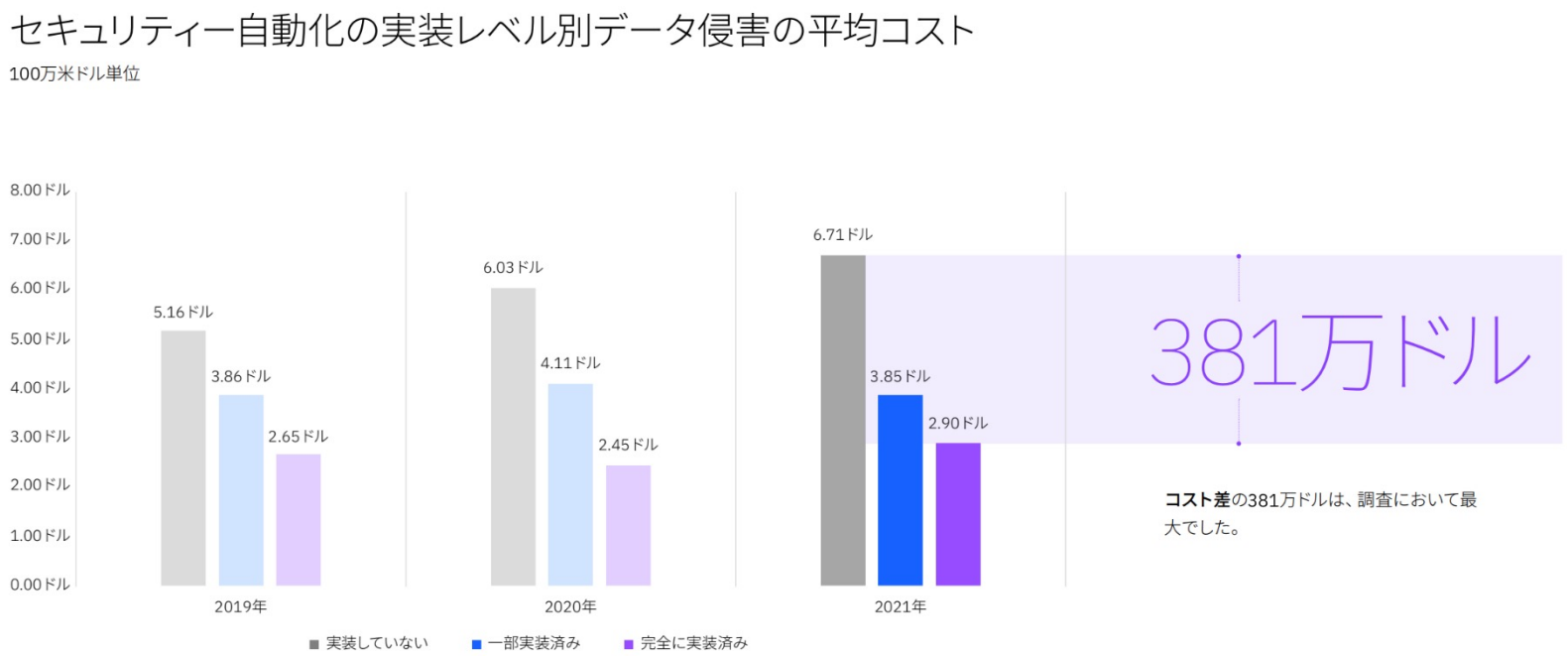
Ex 2014年に米国取締役協会が「Director's Handbook on Cyber-Risk Oversight」を作成すると、経団連がこれを元に「サイバーリスクハンドブック（取締役向ハンドブック）」を2019年に作成

◆意思決定手続

・売上 1 兆円超える企業は、サイバーセキュリティに対し、グループ会社を統合的に、リスクから想定される必要となるコストをかけ始めている

・一方、上場企業の内中規模な企業は、サイバーセキュリィの予算は、各企業の情報システム部門の決済権限内にあり、そこから捻出する必要がある場合が多い

侵害時のコスト（自動化と自動化していない場合の比較）



出所：IBM「2021年 データ侵害の コストに関する 調査レポート」

・セキュリティを完全自動化している企業は、自動化を導入していない企業と比べ、平均で侵害時のコストが381万ドル低い（一部自動化においても、286万ドル低い）

・ セキュリティーAI/自動化を完全に実装している組織では、ライフサイクルは合計で247日であり、セキュリティーAI/自動化が一切実装されていない組織にライフサイクル合計は324日である（データ侵害のライフサイクルの差は77日）（一部セキュリティーAI/自動化実装のライフサイクルは289日）

※人手による入力を必要とするプロセスでは、多くの場合、何十ものツールや複雑で統合されていないシステムがあり、それらの間でデータは共有されていない（平均すると、調査対象の組織は34のセキュリティー・ツールを使用していました）（ IBM「2021年 データ侵害の コストに関する 調査レポート」からの引用）。

事業モデルの設計８条件

TANAAKK

1	XaaSであること	IaaS/PaaS/SaaSなど、月額課金のサブスクリプションビジネスで、必要なものが丸ごと提供されるというサービスの形
2	フリーミアムな課金体系	メール登録と認証だけで簡単に始めることが可能で営業マンとの会話を交わさずとも使用を開始できる。プロダクトがニーズに合う場合はすぐに課金開始できる。価格とサービスは常に計測され改善される。
3	決済方法	決済オプションはクレジットカード、後払い、掛け売り、振り込み、キャリア決済などオプションが多様であること
4	互換性	シングルサインオンやアプリケーションの相互接続性、シェアの高いプロダクトとのAPI連携など
5	スケーラブルなDevSecOps構成	事業の成長を見据えて、プラットフォームはトランザクションの柔軟な拡大や縮小に適したプラットフォームを選択。セキュア開発が実現できる運用体制を選択。
6	データアナリティクス	ユーザのブラウザ利用、アプリ利用やアプリサーバー、データベース、WEBサーバの負荷などあらゆるデータは計測され、最適化されます
7	人材が集まること	市場規模が大きく、市場成長性が高いエリアで、上記ビジネスモデルを構築することにより、スキルセットの調達可能性が上がります。
8	投資家が集まること	市場規模と市場成長性を兼ね、予測可能性の高いグロースシステムを持つ事業は好意的な投資対象になり得ます。

フリーミアム

TANAAKK

	Dropbox	LinkedIn	NYTimes.com	Spotify
WHAT IT IS	A cloud storage and file-sharing service	A social media site for professional networking	A digital, enhanced version of the print newspaper	A music streaming and downloading service
WHAT'S FREE	2 GB of storage, with up to 16 GB more for referring friends	Creating a profile, making connections, basic communication	10 articles a month	Unlimited music, interspersed with ads
WHAT'S PREMIUM	100 GB of storage for $9.99 a month	Advanced searches and communication, starting at $19.95 a month	Full access, starting at $3.75 a week	Downloads and ad-free streaming for $9.99 a month
HOW MANY USE IT	More than 200 million users (free and premium)	277 million users (free and premium) at the end of 2013	53.8 million visitors in December 2013; 760,000 subscribers	24 million users, of whom 6 million are subscribers

ハーバードビジネスレビューによると、Freemium(フリーミアム）とは無料で使用開始できて、ヘビーユーザにサブスクリプションで課金し、ユーザーの声を拾い集めながらサービスラインナップおよび価格を継続的にテストして、収益拡大する事業モデルのこと。ドロップボックス、リンクドイン、ニューヨークタイムズ、スポティファイなどが例に挙げられる。Microsoft、Google、Amazonもこのモデルを採用。

小括

・サイバーインシデントは必ず起こるものであるとの指摘もあり、更に発生すると多額の代償を払う必要がある
・個人情報の流出は、外部不経済の問題の一つとも考えられ、EUやアメリカ（カルフォルニア州）では、多額の制裁金を課す規制となっている
・日本においても情報流出についての規制は厳しくなりつつある・日本の会社の予算規模に合わせた、適切なサイバーセキュリティ商品を提案する必要がある
・その際、サイバーリスクやコストについて認識不足の場合があるので、その点も喚起し、真の企業の価値の向上を提案する必要がある
・今後、サイバーセキュリティの分野は実績や効率性の観点から、AIを利用したツールが世界的に大きな流れになると考えられる

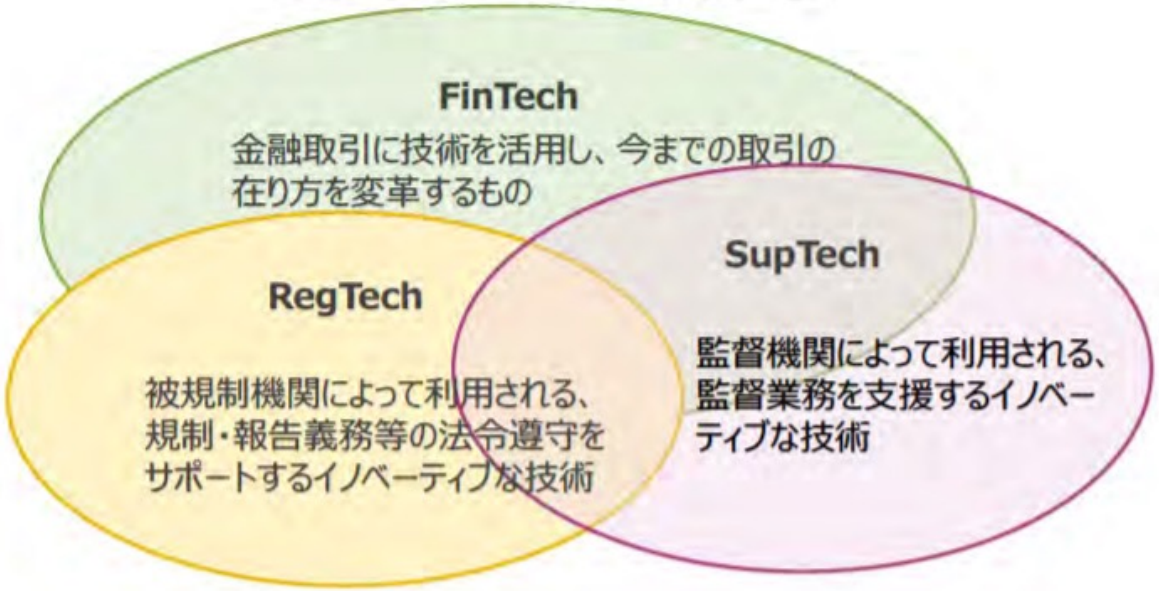
RegTech市場の伸びと
セキュリティ監査に関する米国法令・ガイドラインの現状

Tanaakk株式会社顧問
弁護士法人大江橋法律事務所
弁護士　平田省郎

Regtechとは

- 確立した定義はまだないが、国際決済銀行（BIS）の定義に従えば、以下の通り

図表 1 BIS による RegTec、SupTech の定義



- Regtechの活用により、規制を受ける民間法人においてのコンプライアンスコストの削減、正確適切な規制対応を行われることが期待されている。

Regtechの分類

分野	内容
レポーティング	ビッグデータ解析、リアルタイム報告、 クラウドを利用した自動的なデータ抽出・提供および規制報告
リスクマネジメント	コンプライアンス及び規制リスクの抽出、 リスク評価と将来リスク（脅威）の予測
ID管理・コントロール	カウンターパーティデューデリジェンス、KYC手続、 不正行為防止のためのスクリーニングと検出
コンプライアンス	現時点の法令順守状況と今後の規制の導入見込みを リアルタイムで監視・追跡
トランザクション モニタリング	リアルタイムのトランザクション監視と監査のためのソリューション。 ブロックチェーン技術と暗号通貨による分散型台帳の利点を活用。

※DeloitteのRegtech Universeの分類による。
https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html

- 個人情報に関する意識の高まり
  ビッグデータの活用が盛んになる中で、個人情報保護に対する意識も高まり、各国で法制度化が進んでいる。日本の個人情報保護法はもちろん、EUのGDPRやアメリカのカリフォルニア州のCCPAなどがその代表例。

- 各国における金融行政の複雑化
  リーマンショック以後、金融機関への規制の強化とそれに伴うコンプライアンス費用の肥大化した。例えば、ゴールドマン・サックスの報告によるとコンプライアンス費用は、2009年の70億ドルから2014年には100億ドルへと急速に増加していっている。

Regtechに関する関心の高まり（各国当局の動き）

- 近年、各国当局においても、Regtechに関する取り組みを本格化し、Regtechを推進している

  - イギリス

    Financial Conduct Authority（FCA。金融行動監視機構） と Bank of England（BOE）が、RegTech に関する 政府としての取組み方針を公表。特にFCAは2015年頃から積極的にRegtechの推進を行っている。

  - アメリカ

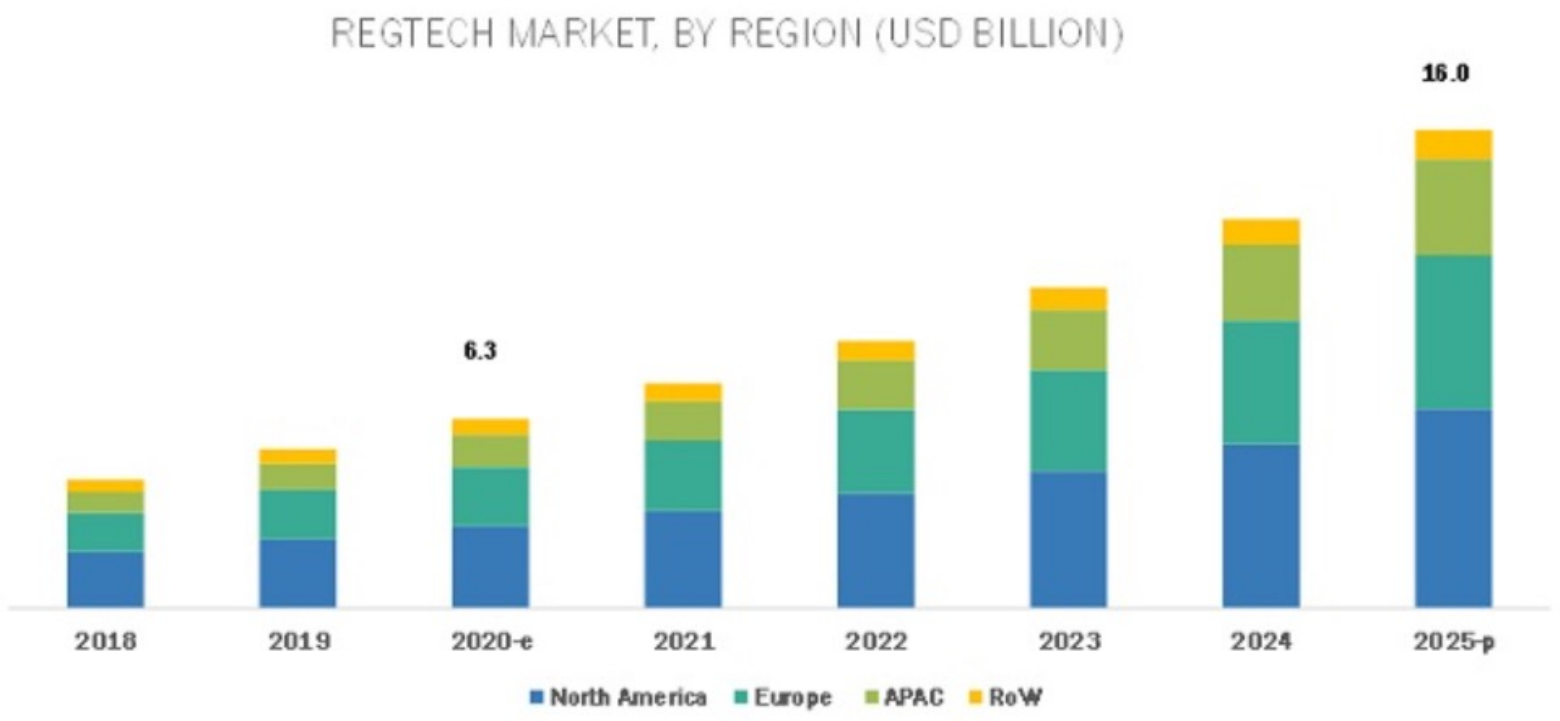
    2017年から、U.S. Commodity Futures Trading Commission（米商品先物取引委員会）が「CFTC Innovation Initiative」と題した、金融分野における技術変化の受入を目指す取組みを始めている。

  - フランス

    Autorité des Marchés Financiers（AMF。金融市場庁）が2018年に策定した「#Supervision2022 Strategic Plan」において、RegTechなどの金融イノベーションの積極的なモニタリングを行うことを表明。

Regtechの市場規模

●RegTech市場の規模は、2020年の63億米ドルから2025年には160億米ドルまで、年平均成長率（CAGR）20.3%で成長すると予想されている。



Source: MarketsandMarkets Analysis

EUの個人情報保護規制（GDPR：General Data Protection Regulation）

- 2018年5月25日に施行。
- 個人データ（Personal data）の処理(processing)と移転(transfer)に関するルールを規定したもの。
- 個人データの範囲は、「識別された、または識別可能な自然人（データ主体）に関するすべての情報）をいい、一般的にいえば、日本の個人情報保護法上の「個人情報」の範囲よりも広い。
- 地理的適用範囲
  欧州経済領域（EEA）域内の管理者または処理者に適用されるだけでなく、EEA域内に拠点のない管理者または処理者であっても、EEA域内のデータ主体に対する物品又はサービスの提供と関連する場合などにも適用あり。
- 制裁金
  制裁金の額は、最大で、全会計年度における全政界における売上高の４％になる。このため、巨額の制裁金リスクがある。
  施行以降、制裁金が課された実例も多数存在しており、つい最近（2021年8月）では、アマゾンがルクセンブルク当局から約970億円の制裁金を科されている。

アメリカ（FTC Act）

- FTC Act とは
  - Federal Trade Commission Actのことであり、一種の消費者保護を定めた連邦法。
  - 消費者を保護するために事業者の「不公正または欺瞞的な（unfair or deceptive）」行為または慣行を禁止する法律であり、消費者の個人情報の収集、処理、保護および開示についても、適用される。
  - その適用対象は広く、米国でビジネスを行う企業または個人に適用される。

- 規制内容
  - 消費者個人の権利または事業者の義務を具体的に規定するものではないが、不公正または欺瞞的な個人情報の取扱いを禁止することにより、実質的に、個人情報関連規制として機能していると言われている。
  - たとえば、FTC Actには、事業者が個人情報保護のための安全管理措置を講じず、個人を識別可能な情報を誰でもアクセス可能な状態に置いた場合などには、不公正な個人情報の取扱いであるとして、同法に違反する可能性がある

    例）Zoomの事例（2021年）

    実際はセキュリティが脆弱であるにもかかわらず利用者にはセキュリティを確保していると説明していたことが、不公正かつ欺瞞的なプライバシー・セキュリティに関する慣行であるとして、FTC Actに違反するとされた事件

アメリカ（HIPAA/GLBA）

- HIPAA （Health Insurance Portability and Accountability Act）
  電子化した医療情報に関するプライバシー保護・セキュリティ確保について定めた連邦法。

- GLBA（Gramm-Leach-Bliley Act）
  個人を識別可能な非公開の財務情報の取扱いに関し、金融機関を規制する連邦法。

- 主な規制

規制内容	GLBA	HIPPA
個人情報取得時の通知	必要	必要
第三者開示への同意取得	規定なし （オプトアウトは可能）	必要
個人情報へのアクセス権等	規定なし	アクセス権あり。
データセキュリティプログラム	一定の安全管理措置が必要	個人情報保護方針及び手続の確立が必要

アメリカ（SHIELD Act)

- SHIELD Act とは
  - NY州法
  - SHIELD Actは、事業者に対する義務を規定するにとどまり、CCPAのように消費者の権利を規定するものではない。

- 規制内容
  - データ侵害通知義務
    一定の事業者が保持するニューヨーク州居住者の個人情報に関するシステムのセキュリティの侵害が認められる場合、当該事業者に、①当該個人情報において特定される個人、および②ニューヨーク州の司法長官等に対して、当該侵害の事実を通知する義務を課している。
  - データセキュリティプログラムの確立義務
    個人情報のセキュリティ、機密性および完全性を保護するための合理的な安全管理措置（データセキュリティプログラム。データの破棄も含みますが、これに限りません）の策定、実行および維持を行う義務。
  - 違反の効果
    データ侵害通知の違反は最低5000ドル（最大25万ドル）
    データセキュリティプログラム確立義務の違反は5000ドル

アメリカ（NISTの定める指針）

- NISTとは
  National Institute of Standards and Technology（米国国立標準技術研究所）は米国商務省傘下の研究機関であり、様々な技術標準を定めている。

- NISTの定める指針
  法令ではないため、原則として法的拘束力はない。しかし、米国政府と取引を行う業者にはこれらの指針の順守が求められており、サイバーセキュリティ業界の業界標準としての位置づけを有している。

- SP 800-171 Rev.2
  NISTが開発した包括的なサイバーセキュリティとデータ保護のフレームワークであり、米国連邦政府に属する、いわゆるCUI（Controlled Unclassified Information）を、第三者であるコントラクターが保管または処理する際に、拡大するサプライチェーン攻撃から保護することを目的とする。「アクセス制御」、「緊急時対応計画」など項目ごとにチェックリストが定められている。

企業概要

組織概要・沿革

企業名	Tanaakk株式会社
本店所在地	〒100-0005 東京都千代田区丸の内2丁目3番2号1階
技術研究所	Tanaakk株式会社 仙台技術研究所 〒983-0036 宮城県仙台市宮城野区苦竹3-1-6 Tanaakk Vietnam Lab 10F, 81 Quang Trung – Hai Chau – Da Nang
創業年月日	2013年7月3日
資本金	1億円
代表取締役	田中翔一朗
グループ会社	Tanaakk法律事務所、Tanaakkファシリティーズ株式会社

取引先 （五十音順・敬称略）	株式会社アグリトリオ（武蔵精密工業関連会社） 株式会社アンファン（学校法人河合塾グループ） 株式会社朝日興産（竹中工務店関連会社） 株式会社サーキュレーション（マザーズ 7379） サントリー食品インターナショナル株式会社(TYO:2587) ジヤトコ株式会社（日産自動車株式会社（東証一部 7201）関連会社） 大日本印刷株式会社（東証一部 7912） 株式会社竹中工務店 東北電力株式会社（東証一部 9506） 東急建設株式会社（東証一部 1720） 株式会社平賀（東証JASDAQ 7863） 前田建設工業株式会社（東証一部 1824） 前田道路株式会社（東証一部 1883） 株式会社パソナJOBHUB（パソナグループ（東証一部 2168）関連会社） 株式会社フジタ（大和ハウス（東証一部 1925）関連会社） 株式会社丸山運送 武蔵精密工業株式会社（東証一部 7220 本田技研工業関連会社） 株式会社メディアドゥ（東証一部 3678） 株式会社モバイルブック・ジェーピー（大日本印刷関連会社） ユナイテッド・スーパーマーケット・ホールディングス株式会社（ 東証一部3222）
調達先 （五十音順・敬称略）	Apple Japan合同会社（アメリカ） Atlassian,Inc（オーストラリア） アドビ株式会社（アメリカ） アマゾンウェブサービスジャパン株式会社（アメリカ） ImmuniWeb SA（スイス） 株式会社NTTテクノクロス GitHub Inc.（アメリカ） グーグル合同会社（アメリカ） Cloud Academy Inc.（イギリス） Crunchbase Inc（アメリカ） さくらインターネット株式会社 サーブコープ東京株式会社（オーストラリア） GMOインターネット株式会社 Semrush Inc（アメリカ） 株式会社CEL 株式会社セールスフォース・ドットコム（アメリカ） 株式会社帝国データバンク 株式会社東京商工リサーチ 日本マイクロソフト株式会社（アメリカ） 株式会社バルク BAP Solution Japan株式会社（ベトナム） Lucid Software Inc（アメリカ）

TANAAKK

〒100-0005
東京都千代田区丸の内二丁目 3 番 2 号郵船ビルディング 1 階
Tanaakk株式会社 Tel 03−5533−8771 Fax 03−5533−8772
URL https://tanaakk.co.jp E-mail jp@tanaakk.co.jp