情報セキュリティの動向と台湾における情報セキュリティ・スタートアップのブレイクスルーの方向性

TAcc+ 計画分析チーム
東京本部貿易経済部仮訳

2020 年は、全世界で新型コロナウイルス感染症の感染拡大による衝撃を受け、各業界では、外部環境によるあおりを受け、あらゆる経営モデルへのシフトが次々と生じた。また、これにより企業のデジタルトランスフォーメーションが加速したと同時に、情報セキュリティに対する意識が高まった。これによってゼロトラストというトレンドが情報セキュリティの新たなスタンダードとなり、各組織は、無停止連続稼働の防御態勢を整えていく必要がある。同時に、リモートユーザーがセキュリティ保護において直面する業務上のリスクを整理して明確化する必要がある。ここから将来、情報セキュリティへのニーズが、デジタルトランスフォーメーションの進展に伴って高まっていくであろうことが分かる。

（1）近年における情報セキュリティの展開のトレンド

2021 年のガートナー（Gartner）の報告では、新型コロナウイルス感染症の大流行後、在宅勤務により、情報セキュリティ環境が重大な変化に直面しており、これに伴って予防戦略にも変化が生じ、感染拡大後のニューノーマルの形成に伴い、各組織は、リモートユーザーの情報セキュリティにおけるニーズと、セキュリティ保護において直面する業務上のリスクについて、さらに踏み込んで整理し明確化する必要があると指摘されている。ガートナーは、今年の情報セキュリティとリスクのトレンドにおいては、情報セキュリティのエコシステムにおいて現在進行中の戦略転換が顕在化していると述べている。これは、長期的に見ると業界全体に広範な影響をもたらすとともに、巨大な破壊的潜在力を有するものである。トレンドについての観察を以下に列挙する。

- サイバーセキュリティメッシュ：分散化の進む企業において、最も必要な場所に安全性の配置と展開が可能となる。
- ネットワークに精通した取締役会：CVE（共通脆弱性識別子、情報セキュリティにおける脆弱性やインデントのリスト）や複雑なセキュリティ設定がますます増えており、これに伴い、取締役会は、サイバーセキュリティをさらに重視するようになってきている。
- サプライヤーのインテグレーション：情報セキュリティの現状として、現在、情報セキュリティのリーダーが多くのツールを持ちすぎているため、さらなるインテグレーションが必要である。
- ID 優先の安全性：感染拡大により、組織の完全（又は大部分の）リモート化が生じており、このトレンドは既に極めて重要なものとなっている。
- デバイス ID を重要な情報セキュリティ機能とする管理：組織は、人以外の実体の増加に直面している。これは、デバイス ID の管理が、既に情報セキュリティ戦略における重要な構成部分となっていることを意味している。一例として電気自動車については、車の所有者の追跡が困難である。以前は刻印されたエンジン番号で認証を行っていた。なぜなら、エンジンは高価で変造が困難だったからである。しかし、電気自動車の電池は安価であるため、車の所有者の識別においては、当人認証の他、車体上での認証装置について業界内で構想中

である。いくつかの自動車メーカーでは、PUF（Physically Unclonable Function）を使用した認証について討議がなされており、これは速やかに解決が望まれる課題である。
・リモートワークの常態化：現在、64％の従業員が在宅勤務を行うことができ、5分の2は実際に在宅勤務を実施している。
・破壊と攻撃のシミュレーション:セキュリティ制御の有効性、配置に関する問題及び検査機能に関して、問題の発見をサポートする。
・プライバシーのコンピューティング技術の増強：信頼を受けていない環境においても、安全なデータ管理、共有、越境データ移動及び分析を実現できる。

（2）新型コロナウイルス感染症の感染拡大に伴う影響

台湾で最も代表的な情報セキュリティ企業である趨勢科技は、2020年上半期に、合計で278億回を超える脅威を遮断した。これは前年同時期と比較して10億回増加しており、そのうち93％は電子メールを介した拡散であった。その他、ビジネスメール詐欺（Business Email Compromise、BEC）の検出数は2019年下半期と比較して19％増加した。その一因として、詐欺集団が、在宅勤務者がソーシャル・エンジニアリングに遭いやすいという弱点を狙って攻撃を試みたことが挙げられる。

McAfee Labsの報告では、悪意のあるソフトウェアの脅威数の平均は1分当たり588件となったことが観察され、2020年第3四半期までの期間で、1分当たり169件（40％）増加した。第4四半期の平均数は1分当たり648件で、1分当たり60件（10％）増加した。

2020年5月4日、台湾中油がランサムウェアによる攻撃を受け、同年には、チェコ共和国第2の都市であるブルノの大学病院がランサムウェアによる攻撃を受けた。検疫は、当初予定されていた1日を超え、数日かかってようやく完了し、セキュリティ対策業務に重大な影響が及んだ。趨勢科技は、ランサムウイルスの犯罪グループは、注目を集め、価値の高い目標に照準を定めて攻撃していると分析している。

米国のCovewareおよびニュージーランドのEmsisoftは2020年3月に、新型コロナウイルス感染症が世界的に拡大し始めた中、ランサムウェアの攻撃を受けた医療機関のために無料サポートを提供すると発表した。これには、ランサムウェアの分析サポート、デコードツールの無料開発、さらにはハッカーとの交渉代理や、システム回復サポートが含まれている。

カナダのバンクーバーで開催が予定されていたPwn2Own脆弱性発見コンテストでは、オンライン開催に変更となった他、脆弱性のある攻撃対象としてコンテスト参加者の利用が特に集中したのは3大OSであった。これにより、大量の従業員が在宅勤務を行っていることから、パソコンもハッカーが狙いを定める最重要目標となっていることが顕在化した。ハッカーは、防御力の脆弱な家庭用コンピュータや家庭用無線ネットワークを通じて、会社のネットワークに侵入する新たな方法を開発するであろう。

コロナウイルスの感染拡大も、製品開発のスピードに影響を及ぼしている。例えば､Googleは、ChromeとChrome OSについて、従来のスピーディーなリリース戦略を中止し、現行のバージョン80の脆弱性対策に集中して、後継バージョンの発表を一時的に見合わせると発表した。当初2020年3月末にリリース予定であったバージョン81は、これにより一時中断となり、リリースは2020年4月に延期された。マイクロソフトも、2020年5月からソフトウェアアップデート戦略を打ち出し、オプション機能部分の提供を取りやめる予定であると発表している。

また、昨年有名となったSolarWinds Orion情報セキュリティ事件からは、悪意のある組織がソフトウェアサプライチェーンの脆弱性を利用して攻撃を行うというトレンドが形成されていることを見て取ることができる。

オンライン会議ツールやコラボレーションツールの急増も、悪意のある相手による新たな攻撃技術の創造を誘引している。彼らは証明書を盗み取り、コラボレーションツールを足掛かりに、ユーザーがシェアする機密データにアクセスしている。

（3）情報セキュリティ領域のスタートアップとスタートアップ投資のトレンド

CBInsightsは、サイバーセキュリティ分野でポテンシャルのある14のスタートアップ企業をまとめている。情報セキュリティ分野に打ち込む志のある台湾の起業家は、このまとめを通じて、他の人がどのような新興分野に切り込んでいるか観察することができる（表1を参照）。例えば、ソースからフェイクニュースを防止すること、各国におけるプライバシー基準に違反しないようプライバシーデザインを行うこと、AIの運用を通じて使用行為の異常を検出して攻撃インシデントを発見し、Patch protectionでソフトウェアへの侵入を自動的に防止する。Zero-trust Networkingでは、厳格な方法で感染を未然に防ぎ、Bot-Assisted DefenseではAI等のロボットを利用して情報セキュリティ防御のサポートを行う。Multi-Cloud Securityも、近年大量の資金が投入されている、課題の多い分野である。特に、5Gネットワークは既にソフトウェアによる仮想ネット

表1　サイバーセキュリティに変化をもたらす可能性のあるスタートアップ企業

サイバーセキュリティ分野	スタートアップ企業
Medical Device Security	ordr / MEDIGATE
Container Security	anchore / CAPSULE8
Outsourced Data Protection	evervault / VERY GOOD SECURITY
Multi-Cloud Security	CLOUDKNOX / orca security
Bot-Assisted Defense	SECURITI.ai / respond
Zero-Trust Networking	ZERO Networks / perimeter 81
Credential Stuffing Defense	kasada / Arkose Labs
Patch Protection	AUTOMOX / ForAllSecure
Third-Party Risk Management	axis security / SecZetta
Anomalous Behavior Detection	Abnormal Security / AWAKE
Privacy by Design	CONCENTRIC / TRANSCEND
Password-less Verification	passbase / BEYOND IDENTITY
Decentralized Digital Identities	evernym / bitkey
Disinformation Detection	yonder / Astroscreen

出典：CBInsights

ワーク（SDN）環境にあり、ソフトウェアを通じて多くの5G基地局が統合されている。同様の概念は、将来においても、ソフトウェアを使用した情報セキュリティ防御のインテグレーションが進み、仮想ネットワーク機能（VNFs）を利用し、ネットワークノード階層の機能をいくつかの機能ブロックに分割して、それぞれソフトウェアの方式で実装するため、ハードウェアのフレームワークに拘束されなくなる。Container Securityは既に主流となっており、その他にもMedical Device Securityは個人のフィジカルデータを収集するよう要求している。この他にも、情報セキュリティ保護に関する多くのニーズが存在する。

Smart money社は、業界で比較的優れた投資実績のあるVC（ベンチャーキャピタル）であり、彼らの投資先や方向性を観察することで、クラウドファウンディング市場で有望視されている分野を把握することができる。これは、シリコンバレーにおいて、大企業やスタートアップチームが継続的に注目しつつ留意しなければならない指標となっている。表2の2020年の情報セキュリティSmart Money社投資分析を参考にすると、引き続きCloud securityが近年における最大分野となっている。その次にData protection、Identity-based security、脅威intelligence、Network securityが含まれており、これらはいずれもSmart money社が非常に注目している分野である。

（4）情報セキュリティ分野における政治的環境

・欧州委員会は、2020年12月15日に「デジタルサービス法」と「デジタル市場法」の草案を提出した。前者の目的は、よりセキュアなデジタル空間を構築し、デジタルサービスユーザーの権利を保護することにあり、後者については、デジタル市場の公平な競争とイノベーションのための環境を保護することにある。

・EUの一般データ保護規則GDPR（25 May 2018）では、最高で2,000万ユーロ又は企業の全世界での売上の4%の罰金を課すことができる。

・行政院国家発展委員会は2020年に「個人情報保護法」の改正作業を実施し、「個人情報保護専門機関」を成立させた。これにより、2020年にGDPRの適合性認定を取得し、台湾の国内企業がEUとの間で個人情報の越境データ移動を自由に行うことができるようになり、企業の経営コストが削減され、競争力

表2　Smart Money社が投資する情報セキュリティ分野の分析

サイバーセキュリティ分野	投資シェア
Cloud security	18%
Data protection	11%
Identity-based security	11%
Threat intelligence	10%
Network security	10%
Other	9%
Email security	8%
Website security	7%
Privacy	6%
Connected devices（IoT）security	5%
Endpoint security	5%

出典：CBInsights

が高まることが期待されている。

・米国食品医薬品局（Food and Drug Administration, FDA）は2016年12月28日に、「医療機器のサイバーセキュリティの市場投入後の管理」（Postmarket Management of Cybersecurity in Medical Devices）を発布し、市場投入後の医療機器の管理の一部とした。

・米国カリフォルニア州では（カリフォルニア州消費者プライバシー法,（CCPA））が2020年1月1日に発効した。

・米国国防総省は2020年1月31日に、2020年9月末までに、国防総省の一部の競争入札で契約した請負業者に対して、サイバーセキュリティ認証の取得を要求すると発表した。この認証は、Cybersecurity Maturity Model Certification, CMMCに基づいており、請負業者はプロジェクトの機密性に基づき、それぞれ異なる安全認証を取得しなければならない。

・イスラエルのCheck Pointは2019年6月の統計データを発表した。その結果によると、台湾企業が悪意のあるソフトウェアによる攻撃を受ける割合は、全世界の4倍から数十倍になるとのことである。特に、米中貿易戦争の開始後、中国からの攻撃が明らかに増加している。

・内政部は、44億台湾ドルを拠出し、当初2020年10月にNew eID（IC身分証）への全面的な切り替えを実施し、将来「デジタル個人識別」を実施するためのツールとすることを予定していた。カードのICの内容、データの読み取り、データベース接続等の状況についてはまだ規定されておらず、潜在的なプライバシーのリスクが存在する。

・韓国の国会では、2020年3月にAct on Reporting and Use of Specific Financial Information Billの改正案が可決され、暗号資産の運営企業（仮想通貨の取引プラットフォーム、電子マネー業者及びICO等の業者を含む）に対して、情報セキュリティマネジメントシステム（Information Security Management System, ISMS）認証の取得が求められるようになった。

台湾の情報セキュリティ・スタートアップのブレイクスルーにおける方向性

台湾の工業技術研究院の調査によると、台湾の情報セキュリティ産業の生産額は、2016年から2019年の間、351.7 → 393.5 → 439.4 → 493.4億台湾ドルで推移した。台湾の情報セキュリティ産業は、2000年にネットワーク通信産業が飛躍的な発展を遂げた際のファイアーウォールのニーズに始まり、2019年まで発展を続け、参入業者は324社、従業者数は約8,800人に上る。業務類型は3つの大分類に区分され、各類の生産額の占有率は、モジュールとハードウェアで51.4%、ソフトウェアで9.7%、代理及び情報セキュリティサービスで38.9%を占める。

ハードウェアは、台湾が優位性を有する分野であり、全世界の80％を超えるサイバーセキュリティハードウェアプラットフォームは台湾で製造されている。また、自国の情勢に起因して、また情報通信産業大国として、台湾は各国のハッカーからの挑戦やテストの対象となり、ハッカーとの攻防の実戦において、少なからぬ経験や人材を蓄積してきた。加えて、自国の情勢におけるニーズ、情報セキュリティ及び国家安全保障により、台湾は情報セキュリティ産業における発展において、その他の国と比較してより切迫した動機や情報通信のバックグラウンドにおける優位性を有するようになった。

しかし、台湾本土の市場はあまりに小さいため、規格の制定者となることは困難である。そのため、

ソフトウェアの占有率は少なく、また世界の情報セキュリティ市場のソフトウェア占有率における比較的大きな分布に比べると、台湾の情報セキュリティ産業の生産額分布はかなり大きな差がある。これに取って代わるのが、情報セキュリティサービスの成長性の高さであり、サービスの範囲も運営監視、クラウド資産管理、検出やフォレンジック、コンサルティング、システムプランニングと設置が含まれる。さらには企業の情報セキュリティ意識の継続的向上により、社内でリソースが不足している企業は、外部委託方式を採用し、これに関係する運営管理サービス業者又はシステムインテグレータの発展は比較的健全であるといえる。

（1）台湾の情報セキュリティにおけるビジネスチャンス

IDC は、台湾の情報セキュリティ市場の規模が、2019 年の 4 億 6,000 万 US ドルから、2023 年には 8 億 2,000 万 US ドルに成長するであろうと予測している。そのうち、情報セキュリティサービス（Service）市場が急速に成長し、年平均成長率は 21％に上り、情報セキュリティソフトウェア及び情報セキュリティ設備の市場は、小幅な成長を維持している。

iThome が台湾企業に対して行った調査結果の示すところによると、直近 4 年間における自社の情報セキュリティ保護に対する企業の信頼度は、2018 年で 62.9 ポイント、2019 年で 61.4 ポイント、2020 年で 63.8 ポイント、2021 年で 62.4 ポイントという結果であり、長期にわたりちょうど合格ラインの水準を維持している。企業が情報セキュリティ事件に直面した場合、8.4％の企業は 1 時間以内に回復できると回答し、1 日以内に回復できると回答した企業は 61.4％、1 週間以内に回復できると回答した企業は 23.3％であった。それ以降は順に 2 週間以内：5.1％、1 ヶ月以内：1％、3 ヶ月以内：0.5％、半年以内：0.3％と回答している。

ガートナーの報告が示すところによると、全世界の情報セキュリティ市場の規模は、全世界の IT 支出の約 3.32％を占め、かつ、占有率は引き続き上昇傾向にある。台湾は、IT 設備の製造大国であるが、情報セキュリティ産業の発展においては、本土の市場があまりに小さい上に、情報セキュリティソフトウェアの開発において、先進国と比較して落差があることが課題となっている。加えて、顧客は、情報セキュリティ業者を医者のようにみなしている。腕の良い医者には多くの人が群がるものであり、かつ、複雑な管理を簡略化するため、一度購入した製品とサービスから十分な保証が受けられることを期待するものであるから、産業特性上、単独作戦を講じる小規模な情報セキュリティ業者にとっては不利である。そのため、展開においては、比較的遠回りで総合的な手段を講じる必要がある。

（2）台湾の情報セキュリティのスタートアップが直面する問題

A. あらゆる産業が直面している複雑な IT 環境

全ての産業において、自らの業務に関係のある専門知識があり、IT 環境も、各産業の実務運営におけるニーズに合わせて配置される。各種 IT デバイス間のリンクやインテグレーションの応用方法も、各産業における習慣化された作業フローが暗黙的に含まれており、加えて、情報セキュリティの防御技術がそもそも多元的でありかつ時間の経過とともに進歩するものであるため、情報セキュリティ分野への進出を希望する台湾企業にとっては、各産業において必要とされるソリューションが全て同じとは限らず、かつ、各種情報セキュリティ技術同士の間で効果的なインテグレーションが必要となり、さもなければ良好な防御効果が生まれないという課題が生じる。

医療及び小売業を例に取ると、CBInsights が、

Healthcare、Retail と関係のある情報セキュリティ業者をそれぞれ整理し、同時に、その産業特性に応じ、以下の表の 15 種類に分類を行ったところ、表 3 に見られる通り、医療、小売関連の情報セキュリティ業者は 15 種類に分類され、そのうち名称が完全に一致するものは 10 種類存在した。Data Privacy（HIPAA）と Consumer Data Privacy、Third-Party Risk と Third-Party / Supply Chain Risk については、名称の一部が一致していた。しかし、産業特性に合わせて名称を設定しても、同一の基準が存在するわけではない。例えば、Data Privacy に関して医療産業で重視されるのは HIPAA への適合性である。しかし、小売業においては、消費者保護が重視される。小売業は医療産業と比較して、Third-Party リスクの他に、Supply Chain リスクを特に重視する。上記の 2 つにはそれぞれ、自らの産業特性に応じた 3 種類の分類がある。さらに比較すると、同一の分類名に属する医療及び小売関連の情報セキュリティ業者も完全に同一ではなく、かつ、15 種類の防御技術をカバーできる業者を探し出すことはほぼ不可能である。これは、IT 環境の複雑な状況を裏付けるものとなっている。

B. 情報セキュリティの創業者の多くは技術畑出身であり、マーケティング又は販売能力に必ずしも長けていない

情報セキュリティについて、複雑な IT 環境、防御ニーズの継続的増加、多数存在する競合製品やサービス、情報セキュリティに対する企業の経営陣の理解度の低さ、信頼や信用の確立には時間を要すること、顧客に対する大量の教育と防御意識の強化が必要であること、多くの企業が情報セキュリティを全体戦略に組み込んでおらず、又は優先順位を低く定めていること、顧客は統合されたソリューションを期待していること、攻防技術が日進月歩で変化していくこと、といった課題が立ちはだかっていることを考慮すると、多くのマンパワー、時間やリソースを投入して潜在顧客や既存顧客とのコミュニケーションを図り、良好なビジネスモデルをプランニングする必要があるため、産業特性上、1 社単独での展開には適さない。しかし、台湾の情報セキュリティ関連のスタート

表 3　CBinsights による、医療と小売産業に関係する情報セキュリティ業者の分類

医療（Healthcare）	小売（Retail）
Cloud Security	Cloud Security
Data Security	Data Security
Data Privacy（HIPAA）	Consumer Data Privacy
Endpoint Security	Endpoint Security
Human Element	Human Element
Managed Security	Managed Security
Network Security	Network Security
Secure Collaboration	Secure Collaboration
SIEM	SIEM
Third-Party Risk	Third-Party / Supply Chain Risk
Vulnerability Mgmt.	Vulnerability Mgmt.
Website Security	Website Security
IAM	Digital Brand Protection
Medical Device Security	E-Commerce Experience Fraud
Threat Intelligence	In-Store & Supply Chain IoT Security

出典：CBinsights

アップ企業の中心的メンバーの多くは技術畑出身であり、潜在的顧客群や提携パートナー、製品やサービスのユーザー、管理者、投資者等との交流や双方向のコミュニケーションをどのように行うかについての経験に乏しい。

C. 台湾で情報セキュリティの自主研究開発能力を有している業者の多くは、現時点で小規模企業である

国家発展委員会産業発展処の資料に基づき、台湾の情報セキュリティ業者の分布状況と規模は表4の示す通りである。ここから以下のことが観察できる。台湾の情報セキュリティ業者の規模は、情報セキュリティ運営管理サービス、終端装置及びモバイルデバイスの防御が上位2位を占め、1社当たりの平均売上高は3億台湾ドルを超える。これに対して、情報セキュリティサポートサービス、情報セキュリティシステムのインテグレーション及び設置業者の1社当たりの平均売上高は1億台湾ドルを下回る。全体として、1社当たりの平均売上高は約1億5000万台湾ドルであり、規模は総じて大きいものではなく、1社単独での展開のみに頼るとすると、成長のスピードには必然的に限界が生じる。

D. 台湾のベンチャーキャピタルは、リスク回避のため遅い順番での投資を希望する

資訊工業策進会資安科技研究所は、全世界における情報セキュリティ関連スタートアップが合併・買収される確率が引き続き増加していると指摘している。この現象の背後には、情報セキュリティ関連の大企業が、継続してCVC投資又はスタートアップの買収を通じて自社のソリューションを充実させていることが主な原因の一つであることを示している。FINDITウェブサイトは、2020年のCVCのサイバーセキュリティに対する投資がかなり活気を帯びていると分析しており、投資件数も、前年度と比較して13%成長して140件にまで増加し、投資総額も31%と大幅に増加して38億USドルにまで増加した。これは、巨額取引を含む件数が12件に倍増したことが一因として挙げられる。台湾のベンチャーキャピタル

表4　台湾の情報セキュリティ産業分布と平均規模

情報セキュリティ産業分布	売上高（億台湾ドル）	件数	1社当たりの平均売上高（台湾ドル）
終端装置及びモバイルデバイスの防御	108	31	348,387,097
サイバーセキュリティ	139.5	53	263,207,547
データとクラウド応用セキュリティ	26.5	24	110,416,667
IoTセキュリティ	20	13	153,846,154
情報セキュリティ運営管理サービス	50.3	13	386,923,077
情報セキュリティ検査、フォレンジック、コンサルティングサービス	61.7	48	128,541,667
情報セキュリティシステムのインテグレーション及び設置	83.8	132	63,484,849
情報セキュリティサポートサービス	3.3	12	27,500,000
全体	493.4	324	152,283,951

出典：国家発展委員会産業発展処

も遅い順番で投資することに慣れており、かつ回収のタイミングに関する期待も比較的短いため、この環境下にあるスタートアップは、成功した際に外国の大企業から買収されやすく、CVC を受け入れない場合、より長い時間を要して生存可能な市場を探さなければならない可能性がある。VC による資金調達を通じて自社の研究開発能力を強化するという試みを実践するのも容易ではないため、いかにして最善の成長戦略を制定するかについては、慎重なプランニングが必要である。

上記の考察をまとめると、台湾の業者は情報セキュリティ製品を自主開発する際に多くの課題に直面し、事業展開においては比較的遠回りで総合的な手法を講じる必要がある。台湾の情報セキュリティ産業の発展は、相対的なボトルネックに直面しており、これは主に、多くの人がハッカーやアンチウイルスソフトについて認知しているだけで、この２つが情報セキュリティの全てであると考えていることに起因している。台湾の情報セキュリティ産業関連の統計と、主流となっている国際的情報セキュリティ産業の統計との間には落差がある。また、現在の米中関係の対立と競争の激化により、中国大陸で製造された情報セキュリティ製品に対する欧米諸国の懸念も大幅に増加しており、さらに、台湾自身の国家安全保障について考慮すると、現在、客観的な環境においては、情報セキュリティの発展に適した環境を形成するにあたって台湾にとって最良の参考となるのはイスラエルであろう。