Deloitte.
デロイト トーマツ

Cybersecurity Insights 2023：金融機関におけるサイバーセキュリティ予算の現状、およびベンチマーク

Cybersecurity insights 2023：金融機関におけるサイバーセキュリティ予算、およびベンチマーク

デロイトが2023年6月に実施した「金融機関におけるサイバーセキュリティ調査」で調査対象となった61の金融機関の回答から、3つの重要な傾向が明らかになっています。

- サイバーセキュリティ予算は過去数年に比べて制約されていますが、基本的な課題対応が優先順位の上位を占めている状況です。
- デジタルトランスフォーメーション（DX）対応が各組織におけるサイバーセキュリティの最重要課題である一方、規制対応に関するプレッシャーも高まっており重要度が増しています。
- サイバーセキュリティ部門は技術的な課題だけでなく、ビジネスへの影響やリスクへの注力が一層求められています。この動きは「ビジネスにおける、サイバーセキュリティの戦略的役割の高まり」を示しています。

サイバーリスク管理業務はかつてないほどに困難なものになっています。デロイトの2023年金融機関におけるサイバーセキュリティ調査では、最高情報セキュリティ責任者（CISO）、最高情報責任者、CEOおよび経営幹部に対し、業界基準に沿ったサイバーセキュリティ運用を推進する際に役立つ知見を提供しています。

サイバーセキュリティ
年間支出／収益

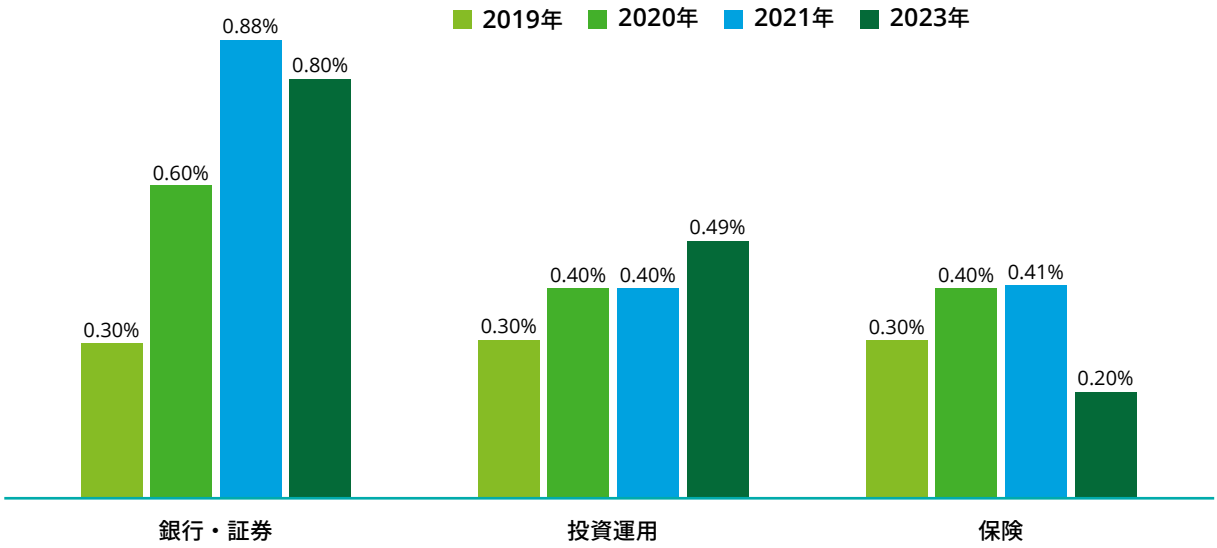
0.72%
2021年

0.54%
2023年

厳しい予算の中でもサイバーセキュリティの優先度は高いままだが、基本的な課題対応に留まっている

ビジネス要件や規制の影響からのプレッシャーによりサイバーセキュリティプログラムの成熟が求められる一方で、金融機関全体の支出削減により、CISOは予算のプレッシャーに直面しています。結果として、銀行・証券部門、保険部門における「収益に占めるサイバーセキュリティ予算の割合」は減少していました。投資運用部門では、総収益に対し支出は微増でした。

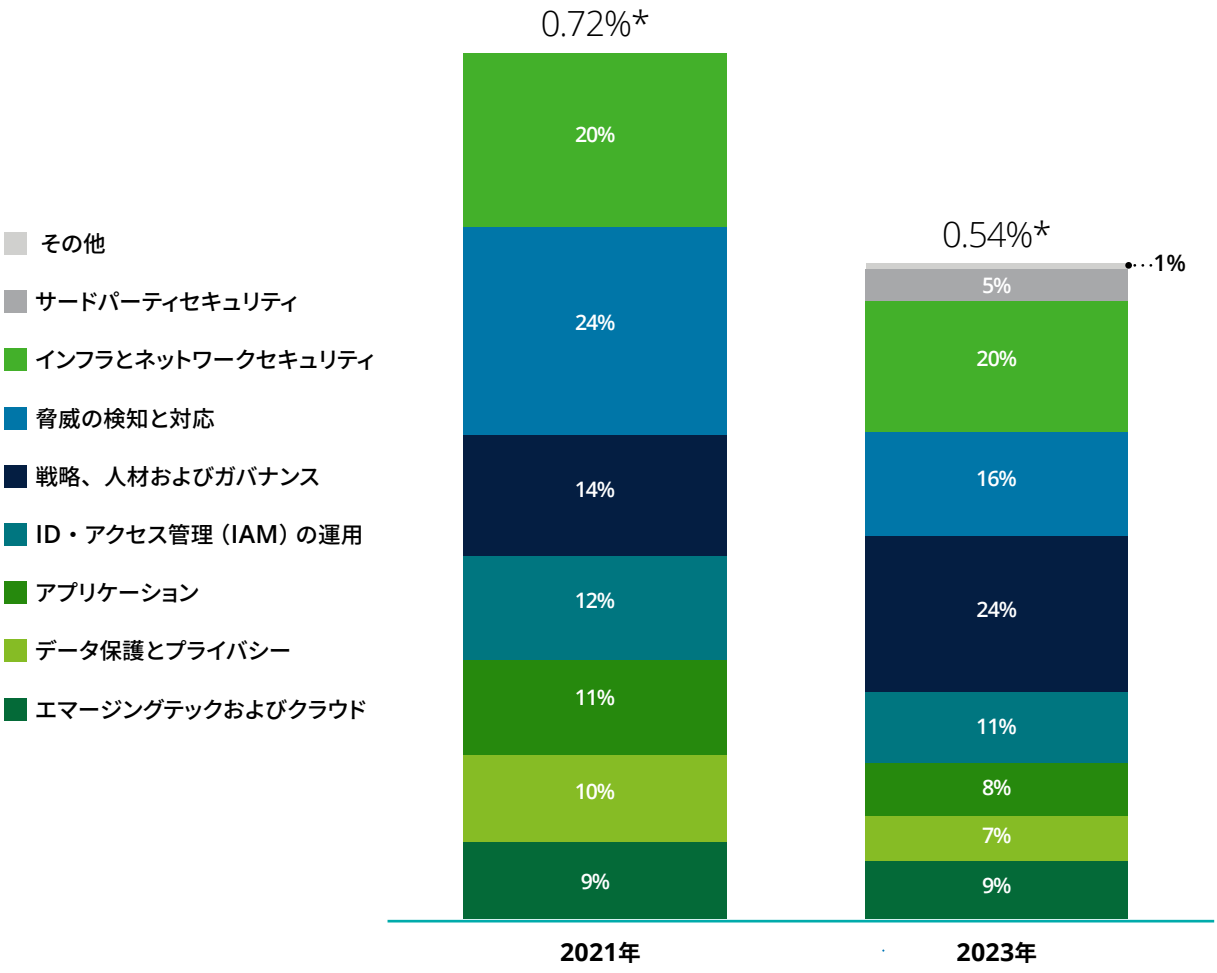
図1：貴組織の収益に占めるサイバーセキュリティ予算の割合は何パーセントですか。



出所：2023年金融機関におけるサイバーセキュリティ調査（Deloitte & Touche LLP）、2021年サイバーの将来に関する調査（Deloitte Global）、2019年および2020年サイバーベンチマーキング調査（DeloitteおよびFS-ISAC（Financial Services Information Sharing and Analysis Center））不動産セクターについては「2021年0.54%、2023年0.10%」でしたが、2023年の回答数は1件のみであり、この比較は有効ではありません。

図1により示されたサイバーセキュリティ予算のうち、優先される支出先の大部分は2020年・2021年から大きく変わらず、インフラとネットワークセキュリティ、脅威の検知と対応、戦略とガバナンス、そしてID・アクセス管理の運用が占めています。

図2：貴組織における今年度のサイバーセキュリティ全体予算のうち、次の分野に配分された割合は何パーセントですか。

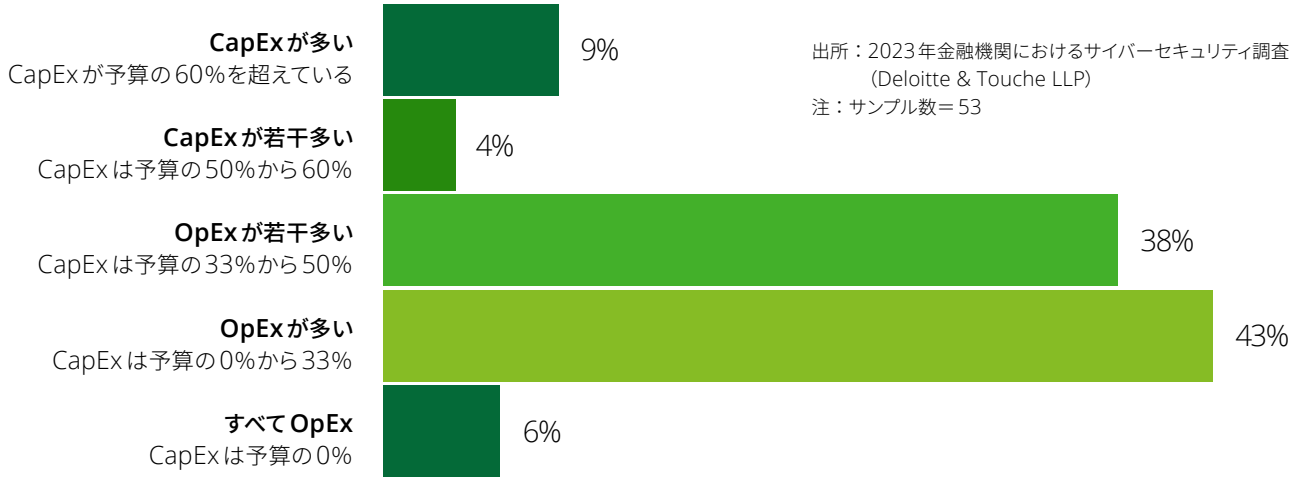


*収益に占めるサイバーセキュリティ年間支出の割合を示す

注：クラウド移行、統合、DevSecOpsは「エマージングテックおよびクラウド」に含まれます。サイバートランスフォーメーションは「戦略、ガバナンスおよび人材・教育」に含まれます。インフラセキュリティおよびIoT・ICS・OTは「インフラとネットワークセキュリティ」に含まれます。2023年の調査では2021年の調査で使用した項目を上記のように統合しました。

資本的支出（CapEX）と事業運営費（OpEx）を比較しても、従来通り基本的な要素を重視していることがわかります。多くの金融機関において、大半のサイバーセキュリティ支出は設備投資ではなく事業運営に充てられています。回答した金融機関の87%で事業運営費が資本的支出を上回りました。金融機関の中には、変革型投資には配分せず、運営のみに専念している回答者も6%いました。サイバーセキュリティが経営課題において中心的な役割を担う一方、組織は基本的な課題への対応に終始しているということがわかります。

図3：貴組織のサイバーセキュリティ予算のうち、資本的支出（CapEX）または事業運営費（OpEx）に配分された割合は何パーセントですか。

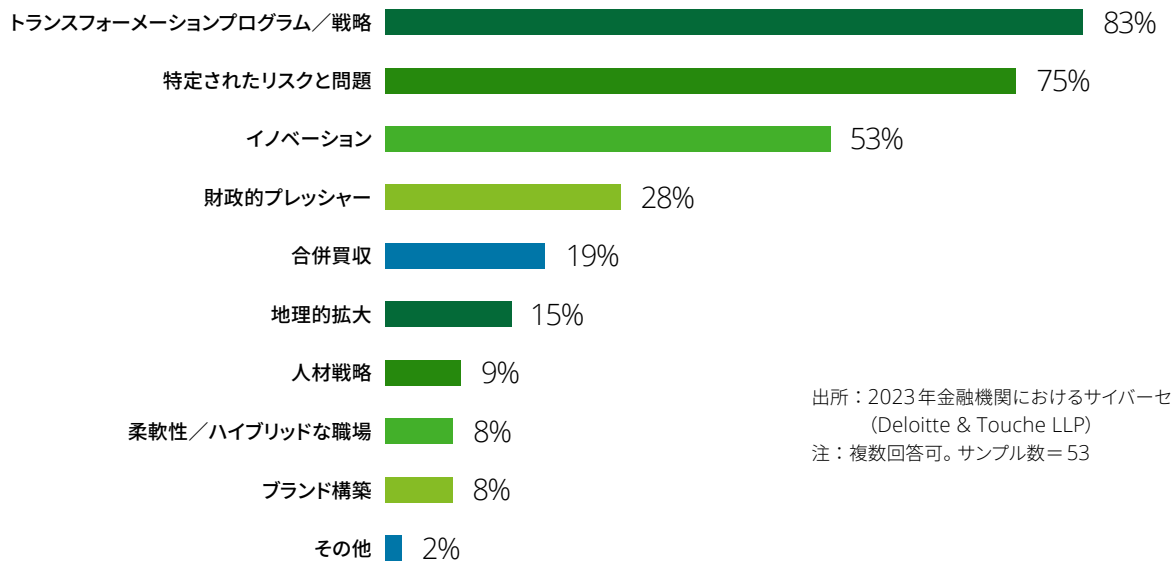


出所：2023年金融機関におけるサイバーセキュリティ調査（Deloitte & Touche LLP）
注：サンプル数＝53

サイバーセキュリティにおいてDXと規制に関するプレッシャーが最重要課題

リスク管理において、サイバーセキュリティがますます重要視されるなか、CISOが担う戦略もますます組織の幅広いニーズに対応する必要性が増加しています。2023年の調査では、サイバーセキュリティ対策を実現するための重要な推進要因として、2つの経営課題が明らかになりました。

図4：貴組織でセキュリティの強化を必要とするビジネス上の考慮事項の上位3つは何ですか。

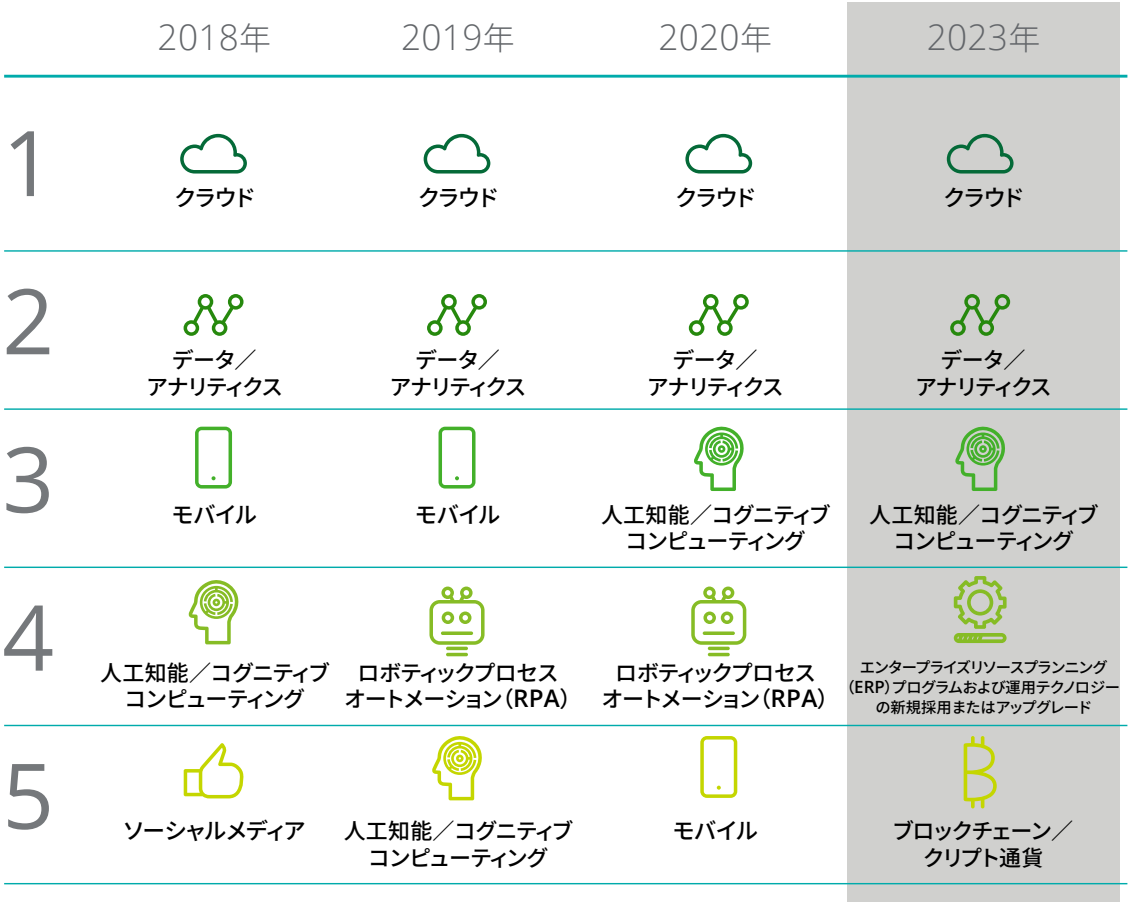


出所：2023年金融機関におけるサイバーセキュリティ調査（Deloitte & Touche LLP）
注：複数回答可。サンプル数＝53

DX：金融機関にとって新たな技術の導入はビジネスの発展やコスト管理に不可欠です。COVID-19のパンデミックの余波が沈静化する中、企業はDX戦略を具体化しながら推進しており、サイバーセキュリティは新たなプロセスやシステムの構築に盛り込まれています。

また、調査結果をみると、DXの最優先事項はこれまでと変わらずクラウドコンピューティングであり、第2位も前年同様、集約型データアナリティクスの使用増加が続いています。人工知能への関心も高まっており、CISOが対応すべき新たな課題とも認識されています。

図5：貴組織のDXにおける優先事項のうち、上位5つは何ですか。



出所：2023年金融機関におけるサイバーセキュリティ調査（Deloitte & Touche LLP）、2021年サイバーの将来に関する調査（Deloitte Global）、2019年および2020年サイバーベンチマーキング調査（DeloitteおよびFS-ISAC（Financial Services Information Sharing and Analysis Center））
注：サンプル数＝53

リスク低減：規制当局はますますサイバーセキュリティのリスクに焦点を当てており、これにより金融機関は特定されたリスクに対してより一層注意を払うようになっています。監査での指摘事項といった特定のリスクや、規制課題への対応についてもサイバーセキュリティ支出の主な要因となっており、新規のデジタル投資と比肩しています。

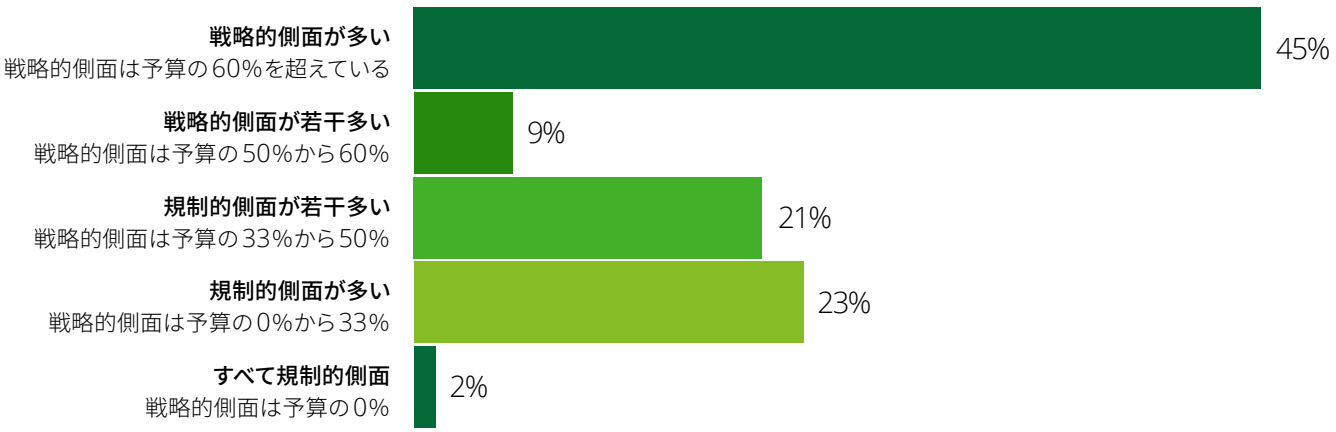
2023年7月26日、米国証券取引委員会は、すべての公開企業に対し、サイバー攻撃などの問題についてより迅速かつ包括的な報告を義務付ける新たな規制を導入することを発令しました。また、証券会社、ディーラー、投資会社や登録投資顧問などの金融機関は、顧客の記録や情報を保護するための予防策や情報漏洩時のインシデント対応プログラムの作成または更新を新たに求められる可能性があります。こうした動きを踏まえると、規制によるプレッシャーが今後ますます増大することは明らかといえます。

参考：「2023年、米国証券取引委員会は上場企業によるサイバーセキュリティリスク管理、戦略、ガバナンス、インシデント開示に関する規則を採択」https://www.sec.gov/news/press-release/2023-139

サイバーリスクの高まりと規制上のプレッシャーという2つの要素はスパイラルを作り出しています。新たなテクノロジーがビジネスプロセスに導入されるたびに規制は強化されます。規制当局はこれまでクラウドデータやクラウドサービスに関連するリスクに注意を払ってきましたが、人工知能やコグニティブコンピューティングによるサイバーへの懸念も、近いうちにさらに注目を集めるようになるでしょう。

リスク低減の重要性が高まっていることは、金融機関の支出に表れています。2023年に調査対象となった金融機関の46%が、サイバーセキュリティ予算の半分以上は規制に起因するものであると回答し、戦略的側面を優先していると回答した54%に匹敵する結果となりました。

図6：貴組織のサイバーセキュリティ予算のうち、規制上の優先事項ではなく戦略的優先事項によって配分された割合は何パーセントですか。
（回答した組織の割合）



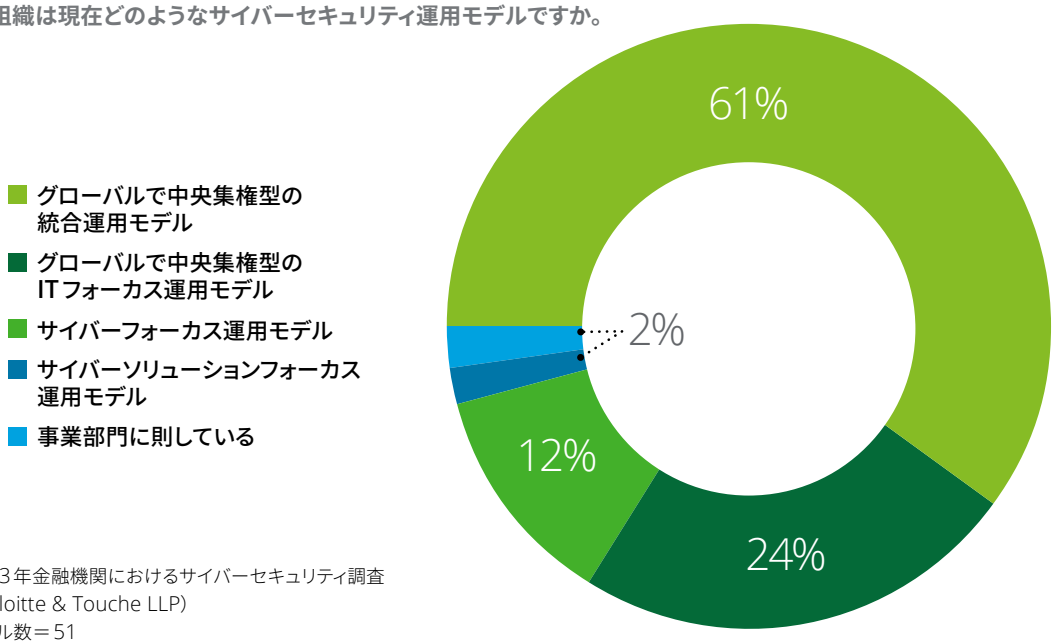
出所：2023年金融機関におけるサイバーセキュリティ調査（Deloitte & Touche LLP）
注：サンプル数＝53

サイバーセキュリティ組織の中央集権化が進行

2020年にデロイトが発行したレポート「Reshaping the Cybersecurity Landscape（日本版：サイバーセキュリティ展望を再構築）」では、サイバーセキュリティの戦略的な重要性を理解するためには、ビジネス戦略にどのような影響を与えるかを含め、IT以外にも目を向ける必要がある、と指摘しています。2023年の調査では、多くの組織がこのメッセージを重く受け止めていることが示されています。回答した金融機関の大半は、自社のサイバーセキュリティ組織はグローバルで中央集権型の統合運用モデルを採用していると述べています。

- グローバル：組織の地理的な拠点にまたがっているサイバーセキュリティ組織が存在することを指します。
- 中央集権型：ひとつのサイバーセキュリティ組織がすべてのビジネスラインにサービスを提供していることを指します。またはこの組織がすべてのビジネスラインに導入すべき中心的な方針や基準を定義します。
- 統合：ビジネスへの影響、リスクや人材も含め、テクノロジー／ITだけではなくサイバーセキュリティの全ての側面に焦点を当てる組織が存在することを指します。

図7：貴組織は現在どのようなサイバーセキュリティ運用モデルですか。

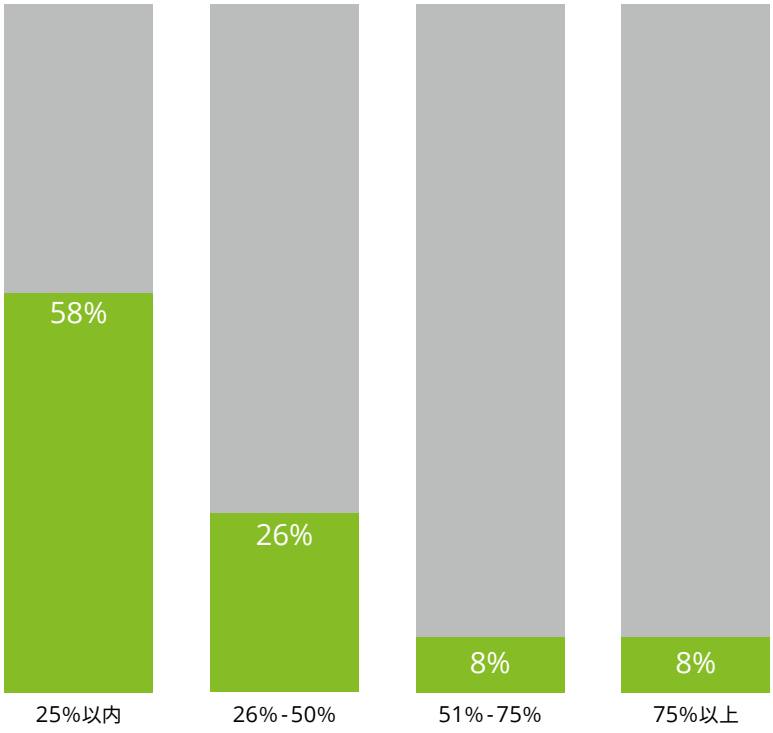


出所：2023年金融機関におけるサイバーセキュリティ調査（Deloitte & Touche LLP）
注：サンプル数＝51

2番目に多い運用モデルは、ITにフォーカスしたグローバルな中央集権型で、サイバーセキュリティの一部の側面をより広範なビジネス組織が対応しています。事業部門ごとにサイバーセキュリティ機能が分かれている運用モデルであると回答した金融機関は2%のみでした。

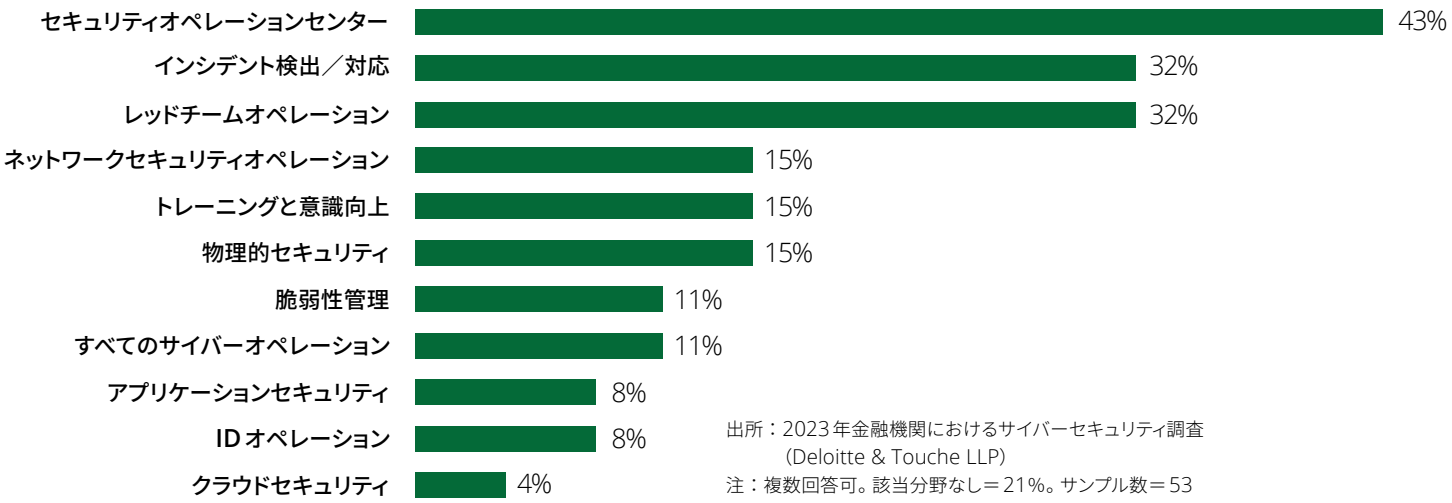
CISOは依然として業務の多くを外部委託に依存しており、回答者の42%が自組織のサイバーセキュリティ予算のうち25%以上を外部委託費用として支出していると回答しています（図8）。一方、サイバーセキュリティ運用を一切外部委託していないと回答した金融機関も21%ありました（図9）。委託先分野としてはセキュリティオペレーションセンターが最も多く、次にインシデント検出と対応、そして「レッドチームオペレーション」と続いています。クラウドセキュリティについては、ほぼすべての金融機関が社内で維持したいと考えています。

図8：貴組織のサイバーセキュリティ予算のうち、外部委託には何パーセントを配分していますか。



出所：2023年金融機関におけるサイバーセキュリティ調査（Deloitte & Touche LLP）
注：サンプル数＝53

図9：次のサイバーセキュリティ分野のうち、貴組織で外部委託しているのはどの分野ですか（例：外部管理サービス）。

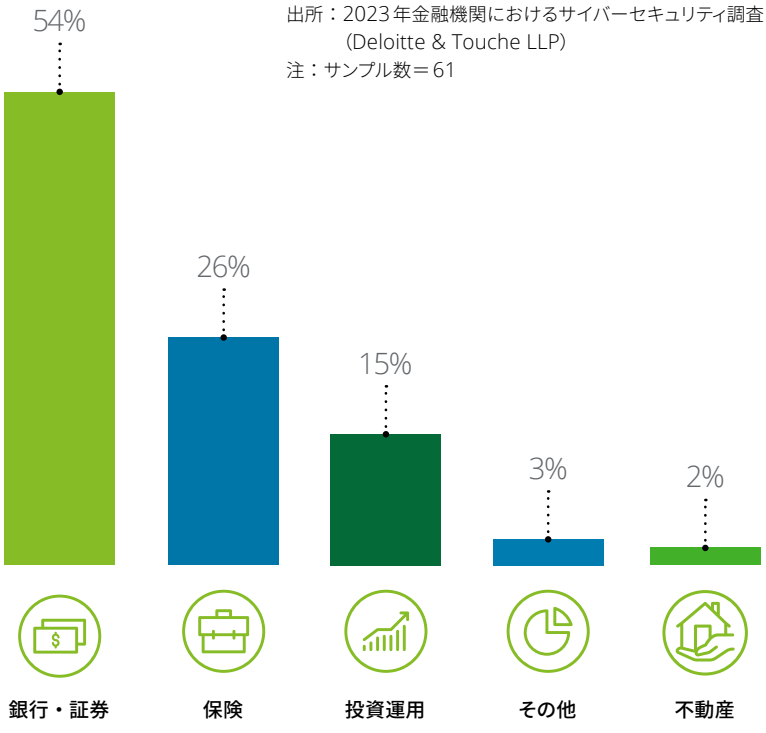


出所：2023年金融機関におけるサイバーセキュリティ調査（Deloitte & Touche LLP）
注：複数回答可。該当分野なし＝21%。サンプル数＝53

本調査について

2023年金融機関におけるサイバーセキュリティ調査は、金融サービス業界にサイバーセキュリティ運用の規模、重要性や機能に関するベンチマークを提供する目的で、2023年6月、Deloitte & Touche LLPによって実施しました。主に銀行・証券分野における合計61の金融機関の回答を基にまとめています。

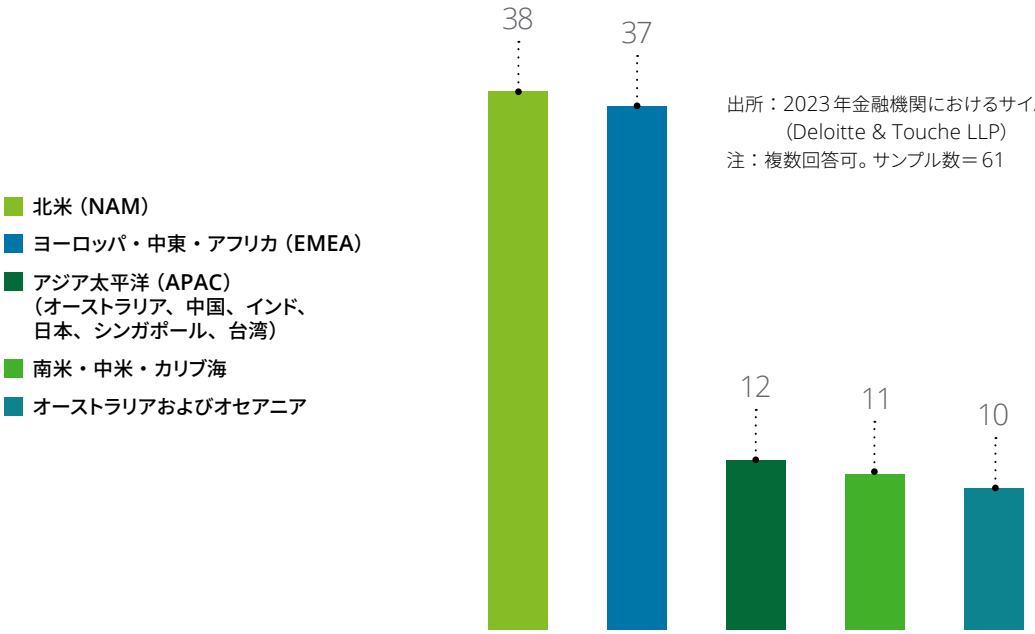
図10：貴組織の主要な事業セクターは何ですか。



出所：2023年金融機関におけるサイバーセキュリティ調査（Deloitte & Touche LLP）
注：サンプル数＝61

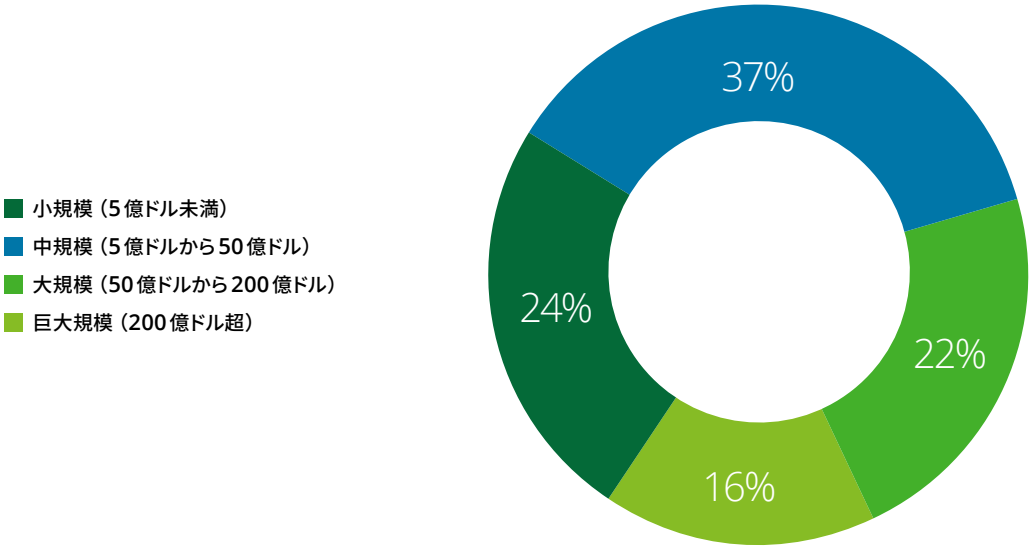
回答した大半の金融機関が北米またはヨーロッパ・中東・アフリカ（EMEA）市場で事業を展開しています（図11）。また、あらゆる規模の金融機関が含まれていますが、収益が5億ドルから50億ドルの「中規模」と回答した金融機関が最も多くなりました。

図11：貴組織はどの地域で事業運営を行っていますか。



出所：2023年金融機関におけるサイバーセキュリティ調査
（Deloitte & Touche LLP）
注：複数回答可。サンプル数＝61

図12：貴組織の総収益を教えてください。



出所：2023年金融機関におけるサイバーセキュリティ調査（Deloitte & Touche LLP）
注：サンプル数＝49。端数処理により、内訳の和は100%にならない場合があります。

問い合わせ先：

Julie Bernard
Principal
Deloitte & Touche LLP

juliebernard@deloitte.com

Meghana Kanitkar
Managing Director
Deloitte & Touche LLP

mkanitkar@deloitte.com

Steve Rampado
Partner – Cyber Leader
Deloitte Canada

srampado@deloitte.ca

Nick Seaver
Partner
Deloitte UK

nseaver@deloitte.co.uk

野見山 雅史
Masafumi Nomiyama
COO
デロイト トーマツ サイバー合同会社

masafumi.nomiyama@tohmatsu.co.jp

縣 和平
Kazuhira Agata
パートナー
デロイト トーマツ サイバー合同会社

kazuhira.agata@tohmatsu.co.jp

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ リスクアドバイザリー合同会社、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT弁護士法人およびデロイト トーマツ グループ合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市に約2万人の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト、www.deloitte.com/jpをご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTLおよびDTTLの各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTLはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務・法務などに関連する最先端のサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来175年余りの歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの45万人超の人材の活動の詳細については、www.deloitte.comをご覧ください。

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301