KEIZAI DOYUKAI

「Cyber Security Everywhere」時代

～経営者の８つのアクションと政府への６つの提言～

2024 年 10 月 23 日

公益社団法人　経済同友会

目次

本提言のサマリー

「Cyber Security Everywhere」時代
～経営者の８つのアクションと政府への６つの提言～

Ⅰ　はじめに

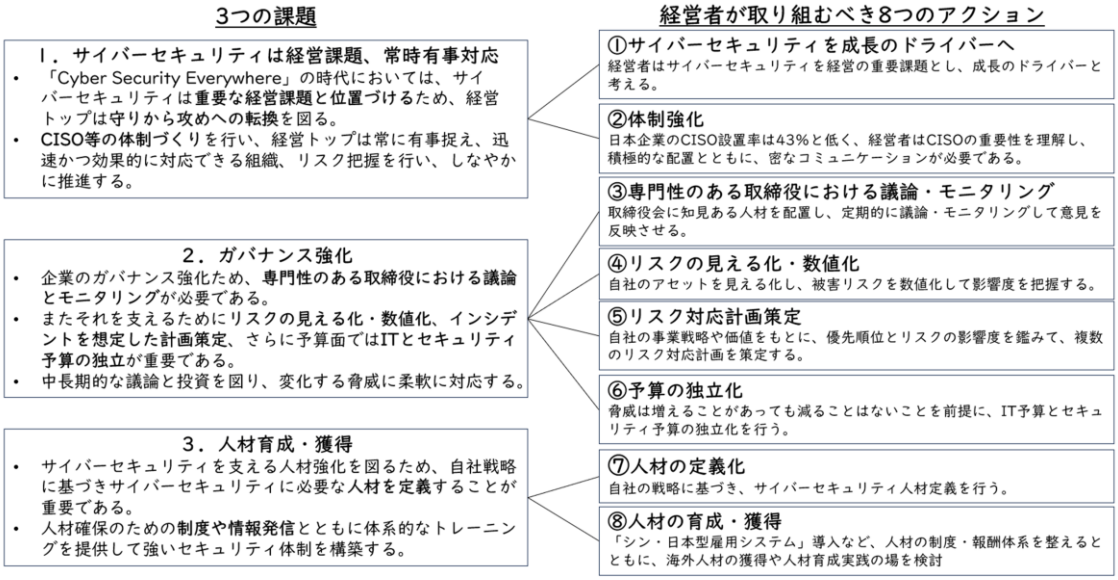
- 時代は「Cyber Security Everywhere」に突入した。
- 世界市場の地政学や地殻変動に影響をもたらしたウクライナ危機の発端は衛星通信システムや変電所へのサイバー攻撃である。また、近年、わが国への中国や北朝鮮等からのサイバー攻撃は増加しており、その手法は一段と巧妙化、高度化、複雑化、組織化している。
- 企業が DX を更に推進するためには、サイバーセキュリティの強化・体制構築が不可欠である。
- 「Cyber Security Everywhere」時代に突入したという認識のもと、企業経営者が行動すべき８つのアクションと政府が進めるべき６つの提言について考え方を示す。

Ⅱ　サイバーセキュリティにおける現状認識

- 外部環境変化ではアタックサーフェイスの増加、サイバー犯罪エコシステムの成熟化・複雑化、IT 及び AI 発展による攻撃の高度化、地政学リスクの高まりが挙げられる。
- 企業では、サイバー攻撃の件数増加、事業のサービス停止・廃止、サイバーセキュリティ人材不足が顕在化している。
- さらに欧米諸国は近年サイバーセキュリティの強化に向けて法整備化を加速している。

Ⅲ　経営が取り組むべき８つのアクション

・　３つの課題から経営者が取り組むべき８つのアクションを以下のように示す。



Ⅳ　政府への６つの提言

・　政府への６つの提言は①能動的サイバー防御の早期導入・NISC の司令塔機能強化②重要インフラ事業者への報告義務化・新たな官民連携組織の創設③人材育成④情報開示⑤サイバーセキュリティ産業の振興⑥サイバー保険である。

・　NISC 内に新たな組織体を創設し、「give and take」の概念とともに、定期的な会合、ワークショップ、官民の人材交流などを図るべきである。

・　政府主導で人材定義と可視化、サイバーセキュリティ教育における民間人材の積極的な登用、高専、大学、大学院の人材において質、量を広げる必要である。

・　サイバーセキュリティに関する重要情報の正確かつタイムリーな開示を行うことを念頭に、有価証券報告書への記載義務化を検討すべきである。

・　高品質な国産セキュリティ製品、サービス供給強化が必要である。

・　サイバー保険は政府主導でデータ集約、分析等、サイバー保険によるリスク評価の枠組みとしての選択肢を作るべきである。

Ⅴ　おわりに

・　業界や個々の企業が連携し、経営者集団としてサイバーセキュリティ強化を支援し、「Cyber Security Everywhere」時代を生き抜き、企業が持続的に成長できるよう、取り組みを一層加速させていく。

Ⅰ　はじめに

時代は「Cyber Security Everywhere」に突入した。

サイバースペースの可能性の拡がりは、情報へのアクセス民主化や人的ネットワーク拡大、新しい経済機会の創出等を実現した。一方、サイバー攻撃や偽情報の蔓延などにより大きな危機に直面している。例えば、世界市場の地政学や地殻変動に影響をもたらしたウクライナ危機の発端は衛星通信システムや変電所へのサイバー攻撃であると言われている。また、近年、わが国への中国や北朝鮮等からのサイバー攻撃は増加しており、その手法は一段と巧妙化、高度化、複雑化、組織化している。

他方、わが国経済は持続的・構造的な賃上げの実現や「金利のある世界」の回帰のなかで、企業は成長投資の加速化や DX（デジタル・トランスフォーメーション）によるビジネスモデルの変革および高付加価値な製品・サービスの創出が求められ、持続的成長に向けて動き出す兆しがある。グローバルな経済活動の中で企業が DX を更に推進するためには、サイバーセキュリティの強化・体制構築が不可欠であり、企業の社会的責任を果たす上でも重要である。

本提言では、「Cyber Security Everywhere」時代に突入したという認識のもと、グローバルなサイバーセキュリティの動向およびわが国の現状・課題を踏まえて、特に影響度が大きい大企業を中心とした企業の経営者[1]が行動すべき８つのアクションと政府への６つの提言を示す。

Ⅱ　サイバーセキュリティにおける現状認識

１　外部環境変化

(1) アタックサーフェイスの増加

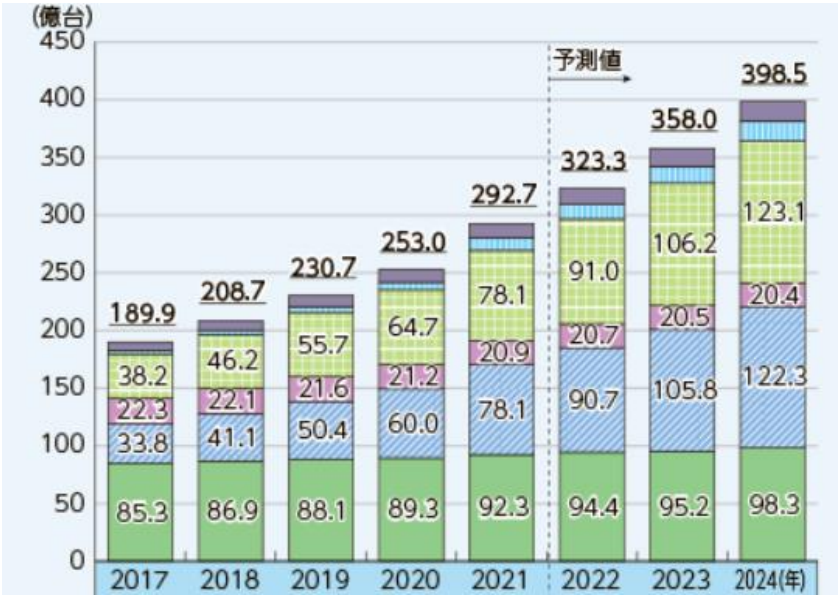
ビジネス上の競争力の確保や顧客向けのサービスの付加価値向上、あるいは業務プロセスの改善や柔軟な働き方を実現するための企業 DX の加速[2]に伴い、情報システムの利用及びクラウド等の活用は拡大している。「世界の IoT デバイス数の推移及び予測」によれば、アタックサーフェイスは 2024 年には約 399 億

[1] 中小企業におけるサイバーセキュリティの強化を図る必要があるものの、論点を明確にするために、本提言からはスコープ外とする。

[2] DX に取組んでいる企業（「全社戦略に基づき、全社的に DX に取組んでいる」「全社戦略に基づき、一部の部門で DX に取組んでいる」「部署ごとに個別で DX に取組んでいる」の合計）の割合は 2021 年度の 55.8%から 73.7%に増加し、着実に DX が企業に浸透している。（出所：IPA「DX 動向 2024」）

台であり、2019 年と比較して 1.7 倍に拡大しており（図表１）、サイバー空間の利用拡大等に伴う、侵入口が増加している。

図表１：アタックサーフェイスの増加



（出所：令和４年情報通信白書　世界の IoT デバイス数の推移と予測）

(2) サイバー犯罪エコシステムの成熟化・複雑化

近年のサイバー攻撃は１つの組織ではなく、分業化が進んでいる。例えば、マルウェア開発、認証状況販売、暗号化、実行者などがある。さらに、異なる専門性を有する犯罪者同士が補完しあい、かつ、相互に利益を享受するようなエコシステムの成熟化・複雑化により、ランサムウェアインシデント等のサイバー攻撃の被害を増大させている。

(3) IT 及び AI 発展による攻撃の高度化

SNS 普及により個人情報の入手が容易となり、なりすましメッセージも頻繁になっている。また、高度な翻訳サービスより攻撃者が標的組織に送る文章も自然なものになっている。さらに生成 AI が登場し、WormGPT など倫理的な制約なく、サイバー犯罪者に対して効率的なサイバー攻撃を支援するために設計された生成 AI ツール（マルウェアの自動生成など）の出現もある。AI 発展により、攻撃の自動化や効率化など急速にサイバー攻撃の敷居が下がると共に、より高度化される可能性があると考えられる。

（4）地政学リスクの高まり

ロシアによるウクライナ侵攻では重要インフラを妨害するサイバー攻撃などのハイブリット型の脅威が顕在化した。軍事侵攻開始の１年以上前から、ウクライナ政府や重要インフラ等の情報システムやネットワークに侵入し、破壊的なサイバー攻撃等を開始することで、軍事侵攻前にウクライナ政府と軍の連絡の要である「衛星通信網」に対する攻撃を実施した[3]。

また国連安全保障理事会北朝鮮制裁委員会の専門家パネルが作成した年次報告書では 2017 年～2023 年、暗号資産関連企業にサイバー攻撃を繰り返し、約30億ドルを搾取した疑いがあり[4]、搾取した資金は核・弾道ミサイル開発等の資金に充てられていると指摘している。

２　企業におけるサイバーセキュリティの状況

（1）サイバー攻撃の件数増加

わが国のサイバー攻撃の現状は、国立研究開発法人情報通信研究機構（NICT）が運用している大規模サイバー攻撃観測網（NICTER）のダークネット観測で確認された 2023 年のサイバー攻撃関連の通信数（パケット）の年間総数は約6,197 億パケットと 2015 年の約 632 億パケットと比較して 9.8 倍となっているなど、過去最高の通信数を記録している[5]（図表２）。

また警察庁のサイバー企画課によれば、令和６年上期都道府県の警察から警察庁に報告のあった企業・団体等におけるランサムウェア件数は 128 件であり、令和４年上半期以降、高い水準で推移し深刻な状況である[6]。

---

[3] 欧州宇宙政策研究所「The War in Ukraine from a Space Cybersecurity Perspective」
[4] 外務省　国連安保理北朝鮮制裁委員会専門家パネル 2023 年最終報告書の概況（2024 年 3 月 21 日）
[5] 総務省「令和６年情報通信白書　サイバー攻撃関連の通信数の推移」
[6] 警視庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2024 年 9 月 19 日）

図表２：サイバー攻撃関連の通信数（パケット）

（出所：令和６年情報通信白書　サイバー攻撃関連の通信数の推移）

（2）サービス停止・廃止の現実

サイバーセキュリティ対策が脆弱な企業においては、不正アクセス等による機密情報流失だけでなく、事業のサービス停止、廃止が起こっている。

例えば、ある小売業の事例では、不十分な認証機能が原因で全国の利用者等が金銭的な被害を受け、サービス廃止となった。さらに、あるエンターテインメント業の事例では、当該グループへのランサムウェア攻撃に起因した情報漏洩により、サービスの停止になり、企業業績の悪化にも繋がっている。

（3）サイバーセキュリティ人材不足

わが国の約９割の企業においてサイバーセキュリティ人材が不足している[7]。海外主要国の企業では、セキュリティ業務の標準化、自動化、省力化を実践することでセキュリティ統制レベルを保ちつつ人材不足の課題を克服しており、人材不足を課題としているのは日本企業だけとの指摘もある。サイバー攻撃のリスクが増大する中で、早急な対策が必要である。

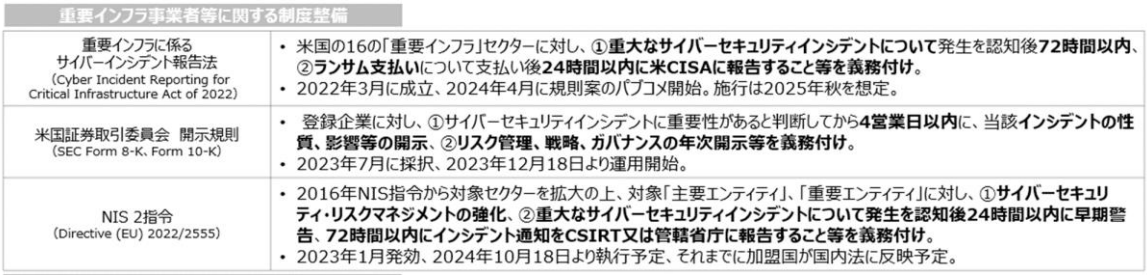
３　サイバーセキュリティにおける国際的な動向

欧米を中心に重要インフラ事業者等におけるサイバーセキュリティ対策の強化に関する法整備が加速度的に進んでいる（図表３）。

一方でわが国においては、サイバー攻撃を受けた場合、重要インフラ事業者への報告義務化を定めた法律はない。

7　NRI セキュアテクノロジーズ「企業における情報セキュリティ実態調査 2023」

図表３：サイバーセキュリティの国際動向



重要インフラ事業者等に関する制度整備	
重要インフラに係るサイバーインシデント報告法 (Cyber Incident Reporting for Critical Infrastructure Act of 2022)	• 米国の16の「重要インフラ」セクターに対し、**①重大なサイバーセキュリティインシデントについて**発生を認知後**72時間以内**、**②ランサム支払い**について支払い後**24時間以内に米CISAに報告すること等を義務付け**。 • 2022年3月に成立、2024年4月に規則案のパブコメ開始。施行は2025年秋を想定。
米国証券取引委員会 開示規則 (SEC Form 8-K、Form 10-K)	• 登録企業に対し、①サイバーセキュリティインシデントに重要性があると判断してから**4営業日以内**に、当該**インシデントの性質、影響等の開示**、**②リスク管理、戦略、ガバナンスの年次開示等を義務付け**。 • 2023年7月に採択、2023年12月18日より運用開始。
NIS 2指令 (Directive (EU) 2022/2555)	• 2016年NIS指令から対象セクターを拡大の上、対象「主要エンティティ」、「重要エンティティ」に対し、**①サイバーセキュリティ・リスクマネジメントの強化**、**②重大なサイバーセキュリティインシデントについて発生を認知後24時間以内に早期警告、72時間以内にインシデント通知をCSIRT又は管轄省庁に報告すること等を義務付け**。 • 2023年1月発効、2024年10月18日より執行予定、それまでに加盟国が国内法に反映予定。

（出所：第８回産業サイバーセキュリティ研究会資料より事務局作成）

Ⅲ　経営者が取り組むべき８つのアクション

１　サイバーセキュリティを成長ドライバーへ

めまぐるしく変化する現代のビジネス環境では、サイバーセキュリティリスクを適切に理解し対処することが不可欠だ。サイバー攻撃のリスクは年々増加しており、ビジネスのみならず企業の存続に重大な影響を与える可能性がある。そのため、経営トップがサイバーセキュリティリスクに対する危機感をもち、重要な経営課題と認識するべきである。サイバーセキュリティを成長ドライバーとして位置づけ、守りの対策から攻めの戦略へと転換を図る必要がある。

具体的には、サイバーセキュリティを取締役会のアジェンダとして設定する。他社で発生したサイバー攻撃による被害を経営トップが理解し、自社組織で発生した場合を想定することが必要である。

２　体制強化

サイバーセキュリティの体制を図るため、CISO（最高情報セキュリティ責任者）等の体制づくりをすべきである。特に企業における情報セキュリティを統括する責任者であるCISOは、企業や組織内の情報資産を守るべく、セキュリティポリシーの策定やセキュリティリスクの管理・対策などを最前線で業務を行う役割を持つ。CISO はセキュリティに関する技術的側面と、経営に関する意思決定を行うマネジメント的側面を併せ持つ必要がある。しかし日本の上場企業でのCISO設置は43%であり、グローバルの中では少ない[8]。

[8]　世界中の会社を対象とした「フォーチュングローバル500」のトップ100社のCISO設置は63%、米国企業を対象とした「フォーチュン 500」のCISO設置は89%である（出所：Nordvpn https://nordvpn.com/ja/blog/ciso-ownership-ratio/）

具体的には、経営トップは自組織にCISOを設置するとともに、取締役や役員クラスに任命する。重大なインシデントを想定し、CISO が事業停止を行うことができる権限を与える。CISO や事業責任者等と常にリスクや課題を共有し、定期的なコミュニケーションを図り、PDCA サイクルを図ることを行うことが必要である。

３　専門性のある取締役による議論とモニタリング

サイバーセキュリティにおけるガバナンスを強化するため、専門性のある取締役による議論とモニタリングをすべきである。サイバーセキュリティに関する全社的な戦略や方針について議論されている会議体として、取締役会で議論されている企業は 1.5%と非常に少ない[9]。さらに社外取締役を含む、サイバーセキュリティに知見のある人材を配置している企業はまだまだ多くない。

具体的には、自社の事業に精通し、執行側に対して能動的に質問できる取締役人材を配置する。取締役会での議論とともに、執行側に対してサイバーセキュリティ対応について定期的にモニタリングを行う。また取締役会の意見を踏まえて、執行側がサイバーセキュリティの対応を見直すなどの関係性を構築することが必要である。

例えば、ソニーでは社外取締役の中で IT／テクノロジーやリスク管理の経験・専門性を有する２名を情報セキュリティ担当として配置している。また社外取締役と執行側では月次会議を行っているとともに、取締役会では年間数回に渡り議論をしている。

４　リスクの見える化・数値化

自社のアセットを見える化、管理するとともに、被害リスクの数値化し、事業の影響度を把握すべきである。そのためには守るべき情報やシステム等の特定や把握が必要である。

インシデント発生時に生じる損害としては、事故対応損害、賠償損害、法令損害、無形損害が考えられる。例えば、サイバーリスクの数値化モデル[10]を参考にし、経営の共通言語である「金額」を用いて議論することも有用である。

---

[9] IPA「企業の CISO 等やセキュリティ対策推進に関する実態調査」(2020 年 3 月 25 日)
[10] 一般社団法人　日本サイバーセキュリティ・イノベーション委員会「サイバーリスク数値化モデル」

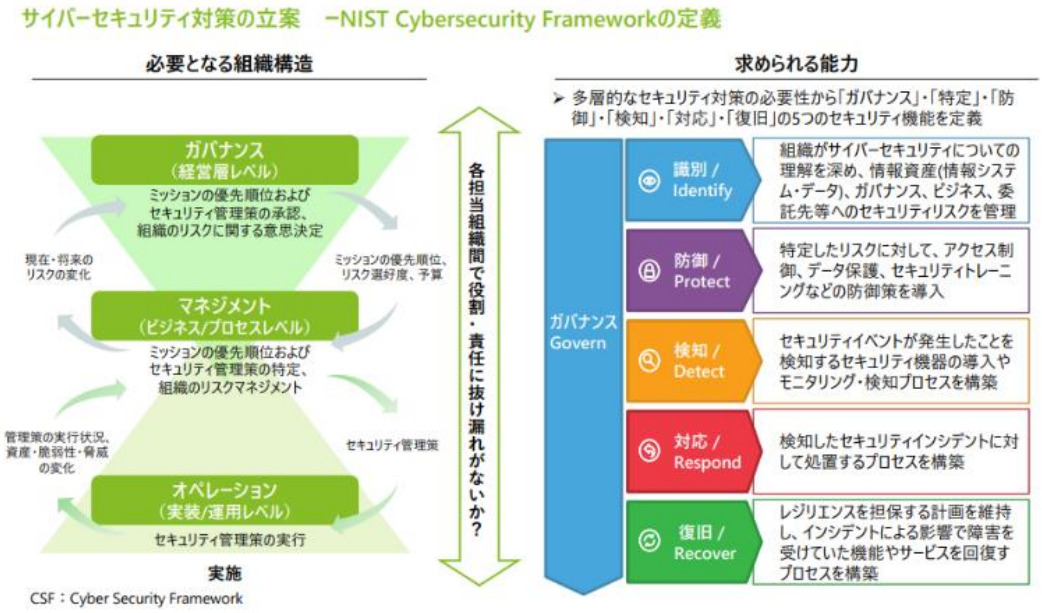
５　リスク対応計画策定

常時有事であることを考えると、経営トップはあらかじめ有事に備えたリスク対応計画策定をすべきである。

具体的には、自社の事業戦略や価値をもとに、優先順位やリスクの影響度を鑑みて、実際のサイバー攻撃を想定し、複数のプランを策定する。プラン策定においては、経営レベル、事業レベル、運用レベルで役割を決め、関係者と連携しながら、策定することが必要である。

例えば、「NIST Cybersecurity Framework」をもとに３層モデル×５機能の考え方が参考になる（図表４）。

図表４：NIST Cybersecurity Framework の定義



（出所： 企業の DX 推進委員会第２回会合　デロイト トーマツ サイバー作成資料）

６　予算の独立化

経営トップは「脅威は増えることがあっても、減ることはない」ということを前提に、IT 予算とサイバーセキュリティ予算を独立させるべきである。また自社のサイバーセキュリティ戦略をもとに具体的なリスクの低減や回避、さらには事業への影響度を加味しながら、中長期的な投資をする必要がある。

具体的には、サイバーセキュリティ予算を単なるコストとせず、将来の利益を守る投資と考える。サイバーセキュリティ投資を事業の基盤作りや顧客から

の信頼により企業成長の柱になると考え、ひいてはWACC[11]を下げ、DCF法による企業価値向上につながりうると考えることが必要である。

７　人材の定義化

「Ⅱ　サイバーセキュリティにおける現状認識」－「２　企業におけるサイバーセキュリティの現状」－「(3) 人材不足」で確認したとおり、サイバーセキュリティ人材不足が課題になる中において、サイバーセキュリティの人材における役割、必要な知識及びスキル等人材定義をすべきである。

具体的には、経済産業省のデジタルスキル標準[12]を活用し、自組織の事業環境や戦略に合わせて、役割やスキルを定義するために参考にすることも有用である。

８　人材育成・獲得

昨今の人手不足を考えると制度や賃金体系についても検討する必要がある。経済同友会ではこれまで内部労働市場を活性化させるためには、「シン・日本型雇用システム[13]」を導入・定着し、成長事業へ人材を集中させることが可能になっていなければならないと主張してきた。IT 人材とりわけ、サイバーセキュリティについては海外人材を含む獲得を考えると、終身雇用を前提としない内部育成・ポテンシャル重視や職務等級制度および役割等級制度（ミッショングレード制)、成果報酬等が必要になってくる。

さらに海外人材獲得には、制度や賃金体系以外にも外部発信も重要である。例えば、メルカリでは、セキュリティチームの３分の２は海外人材を占めているが、海外人材の活躍をエンジニアブログ等で発信しており、大いに参考になる。

また人材育成においては、個社で行うことに限界がある。経済同友会では、経営者自らこの課題に向き合い、企業のサイバーセキュリティ人材強化に向けて、企業や大学等と連携して具体的施策を検討していく。

---

[11] WACC：Weighted Average Cost of Capital

[12] 経産省「デジタルスキル標準」における「DX 推進スキル標準」の人材類型の定義にサイバーセキュリティ人材について記載がある

[13] 経済同友会「シン・日本型雇用システム」導入を突破口に、外部労働市場の真の活性化を―民間主導でリスキリングをあらゆる個人に開放せよ―（2023 年 4 月 21 日）

Ⅳ　政府への６つの提言

１　能動的サイバー防御の早期導入・NISC の司令塔機能強化

「Cyber Security Everywhere」時代となった現実とともに、現在、政府の有識者会議が議論している安全保障や重大なサイバー攻撃の恐れのある場合、未然に排除、侵害拡大を防止する能動的サイバー防御を早期に導入すべきである。そのためには、官民連携の強化、通信情報の利用、アクセス・無害化について速やかに取り組みをするべきである。

能動的サイバー防御の早期導入に向けて、内閣サイバーセキュリティセンター（NISC）は、司令塔機能の強化が必須である。現在、NISC は「サイバーセキュリティの確保に関する施策の企画及び立案並びに総合調整」の役割を担っているが、今後は各府省庁のサイバーセキュリティ部門との連携を一層強め、サイバー安全保障分野の政策を一元的に総合調整する機能を有するべきである。また各府省庁のサイバーセキュリティ部門人材を NISC へ兼務することや各府省庁のサイバーセキュリティ部門が物理的に同じ執務室で協働することも検討すべきである。

２　重要インフラ事業者への報告義務化・新たな官民連携組織の創設

サイバーセキュリティにおいて情報は最も重要なファクターである。現状政府は、必要な情報を民間企業から得られているとは言い難い。また民間企業はレピュテーションリスク等を不安に感じ、情報を十分に出さず、負のスパイラルとなっている。したがって重要インフラ事業者への報告義務化を早期に導入するべきである。

そのため、NISC 内に新たな官民連携の組織体を創設するべきである（図表５）。新たな官民連携の組織体は「give and take」の概念を念頭に、情報収集・提供、インシデント対応支援、リスクコミュニケーションなどの機能をもつ組織とする。また定期的な会合やワークショップを開催し、参加企業間の情報や意見交換を促進するとともに、官民との人材交流を行い、信頼関係の構築を図る。組織設置にあたっては、米国の共同サイバー防衛連携（JCDC）、英国のインダストリー100（i100）、豪州のサイバー脅威情報共有（CTIS）など諸外国の事例は参考にするべきである。

政府から民間企業等へ提供する情報については、経営層の意識決定に有用な情報提供を実施すべきである。情報としては、「攻撃者の主体、目的、背景」、

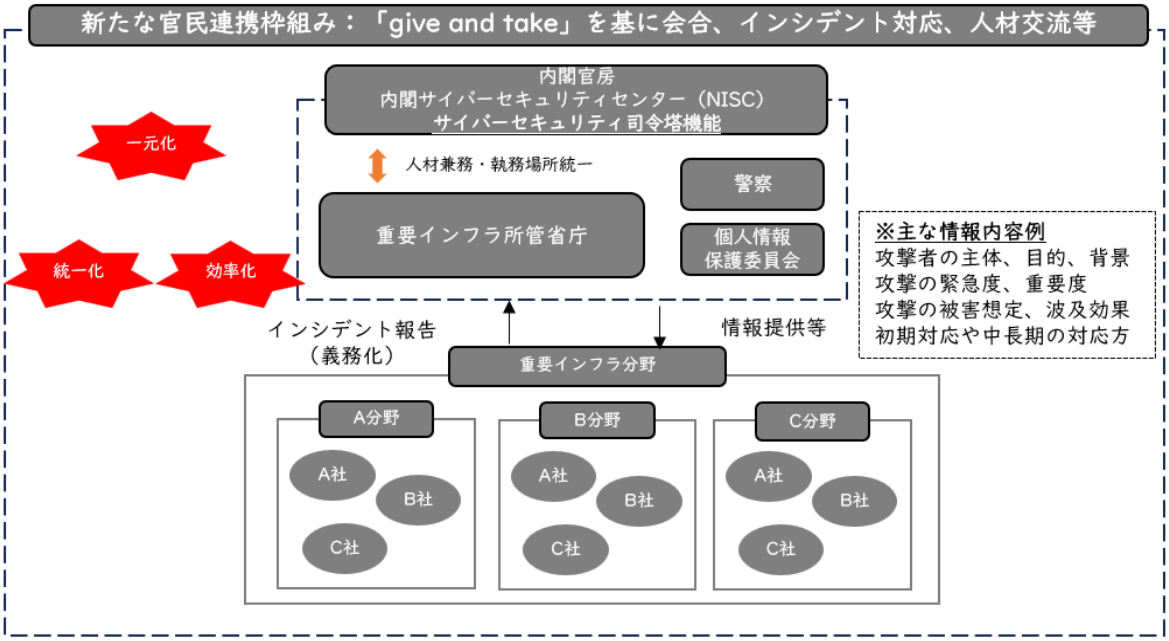
「攻撃の緊急度、重要度」、「攻撃の被害想定、波及効果」、「初期対応や中長期の対応方」が例として挙げられる。

経済同友会は 2024 年２月に「セキュリティ・クリアランス法制に関する意見[14]」 をしたが、セキュリティ・クリアランス制度の適切な設計や運用を求めるとともに、情報提供においても十分に活用すべきである。

民間企業等から政府へのインデント報告は現状、各業法やガイドライン等に基づき、各事業者の監督官庁へ行われているが、リアルタイム性が欠けている。そのためインシデント報告先の一元化を行うべきである。

また監督官庁等により、報告内容や形式が異なる。そのため、報告フォーマットの統一に加えて、報告や集約が一元化できる仕組みを行い、効率性を上げるべきである。

図表５：新たな官民連携組織のイメージ



３　人材育成

（1）サイバーセキュリティ人材定義と可視化

「デジタル田園都市国家構想」はデジタル人材育成について 2022 年度からの５年間で 230 万人と定めているが、とりわけサイバーセキュリティ人材が重要である。

[14] 経済同友会　セキュリティ・クリアランス法制に関する意見（2024 年 2 月 22 日）

サイバーセキュリティの人材強化について産官学の共通認識をするためにも、諸外国の事例や国内の動きを参考に、政府主導でサイバーセキュリティ人材定義と可視化を検討すべきである。また人材定義と可視化とともに教育機関と連携する必要がある。

取り組みにあたっては、米国と欧州の事例は大いに参考するべきである。米国では、NICE サイバーセキュリティ労働力フレームワーク（NIST. SP.800-181）にて業務、知識、技術の定義している。さらに National Centers of Academic Excellence in Cybersecurity (NCAE-C)プログラムにて米国教育機関のサイバーセキュリティに関する学位認証を行っている。欧州では、欧州サイバーセキュリティ技能フレームワーク（ECSF）によりサイバーセキュリティの役割、能力、スキル、知識に関する共通理解、スキル認知促進を実施している。また、Cyber HEAD にて EU 及び EFTA 諸国におけるサイバーセキュリティ高等教育データベースを行い、web 上での大学の見える化もしている。

(2) 教育機関の質と量の拡充

サイバーセキュリティのリテラシー向上や人材育成・確保の視点からも初等教育段階から中等教育までセキュリティ教育を実施すべきである。

その際、民間の専門人材を活用し、生徒の指導と共に教員の研修など知識・スキル向上を行うべきである。

また、セキュリティ人材の即戦力、さらには CISO などのトップ人材を増やすべく、高専、大学、大学院の人材育成を強化するため、質、量を広げる必要がある。例えば、豪州で導入しているサイバーアカデミーを参考にサイバーセキュリティを専門に学べる仕組みを検討すべきである。

４　情報開示：有価証券報告書への記載義務

経営側、執行側、投資家側の各々が有効なコミュニケーションをとるために、サイバーセキュリティに関する重要情報の正確かつタイムリーな開示（適時開示）を行うことを念頭に、有価証券報告書への記載義務を検討するべきである。またコーポレートガバナンスコードにサイバーセキュリティに関する方策を明確に記載すべきである。

米国では 2023 年に上場企業に対し、①サイバーセキュリティのリスク管理と戦略、ガバナンスに関する一定の情報を Form 10-K（年次報告書）において開示すること、および②顧客情報への不正アクセス等のサイバーセキュリティ・インシデントが発生した場合、当該インシデントを重要と判断した時点から原則 ４営業日以内に Form 8-K（臨時報告書）で開示することを義務化している。

わが国においてもこうした事例を参考に速やかに取り組むべきである。

５　サイバーセキュリティ産業の振興

わが国の情報セキュリティ製品市場（売上高）は、2022 年度は前年比 19.8%増の 5,254 億 5,400 万円[15]と堅調に伸長している。しかしながら、外資系企業のシェアが５割を超えており、わが国のサイバーセキュリティ製品の多くを海外企業に依存している。そのため、同盟国や同志国と連携しながら、高品質な国産セキュリティ製品、サービス供給を強化すべきである。さらに、それらを海外展開し、その利益を新たな研究開発や人材育成に充当するなどのエコシステムを構築する。

加えて耐量子計算機暗号への対応もする必要があるため、政府主導で民間ともに取り組みについてロードマップを描くべきである。

６　サイバー保険

世界のサイバーセキュリティ保険市場は年々拡大し、2024 年度では 200 億ドルを超えると想定されている。しかしわが国のサイバーセキュリティ保険市場は約 300 億円の規模と言われ、市場規模が小さく、かつ日本企業のサイバー保険加入率は 7.8%[16]と欧米に比べ低い。

サイバー保険は新たな分野であるため、各保険会社だけではデータが不足している状況である。政府主導でデータ集約、分析、ルール作りをして、サイバー保険によるリスク評価の枠組みとしての選択肢を作るべきである。加えて、有価証券報告書の義務付けと合わせることで、中長期的にはサイバー保険を加入していることが、サイバーセキュリティ対策を行っている１つの指標になることで、WACC の低減や企業価値向上にも繋がるであろう。

Ⅴ　おわりに

あらゆる場面でサイバー攻撃の脅威と対峙する「Cyber Security Everywhere」時代になった現実を経営トップ自身が深く認識すべきである。

「他社で起きているだけでサイバー攻撃は自分たちには関係ない」、「情報システム部門がしっかりやっている」、「サイバーセキュリティ対策のコストだけ

---

[15] 総務省「令和６年情報通信白書　サイバーセキュリティの動向」

[16] 日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020」（2020 年 12 月）

がかさみ、効果が見えない」という声がある。しかし、戦争でサイバー攻撃が使われ、サイバー攻撃により搾取された資金がミサイル開発の原資になるなどわが国の脅威になっている。企業においてもサイバー攻撃を受け、サービス停止、損失発生など影響が発生している。

一方で、グローバルを見ると、欧米諸国は近年サイバーセキュリティの強化に向けて法整備化を加速している。

さらに生成 AI を含む AI などテクノロジーの進化はサイバーセキュリティの領域でも脅威になるだろう。

政府においては、サイバーセキュリティ戦略、サイバー安全保障分野での対応能力の向上に向けた有識者会議など施策や議論を進めているところではあるが、本提言も踏まえた施策を迅速に検討・実行することを期待する。その際、民間企業等とのコミュニケーションを図りながら進めることを強く望む。

他方、民間においては、個別企業での取り組みのみならず、業界を横断した連携も重要である。

本会は、業界や個々の企業が連携し、経営者が集団としてサイバーセキュリティの取り巻く状況の理解、危機感を醸成する活動やベストプラクティスを広げることで「Cyber Security Everywhere」時代を生き抜き、企業が持続的に成長できるよう、取り組みを一層加速させていく所存である。

以上

2024年10月

企業のDX推進委員会

（敬称略）

委員長

伊　藤　穰　一	（デジタルガレージ　取締役　・千葉工業大学　学長）
上野山　勝　也	（PKSHA Technology　代表取締役）
鈴　木　国　正	（インテル　取締役会長）

副委員長

青　木　千栄子	（シー・ブルー　代表取締役）
今　田　素　子	（メディアジーン　代表取締役ＣＥＯ）
高　田　幸　徳	（住友生命保険　取締役 代表執行役社長）
高　橋　隆　史	（ブレインパッド　取締役会長）
山　中　雅　恵	（ロート製薬　取締役チーフトランスフォーメーションオフィサー）

アドバイザー

伊　藤　益　光	（デロイト トーマツ サイバー　パートナー）

委員

會　田　武　史	（RevComm　代表取締役）
青　木　邦　哲	（ＡＳＪ　取締役社長）
青　木　　寧	（高島　社外取締役）
赤　林　富　二	（ニッセイ・リース　取締役会長）
吾　郷　康　人	（山九　取締役副社長）
浅　沼　章　之	（淺沼建物　取締役社長）
足　立　洋　子	（ＳＢＩ証券　専務取締役）
有　田　喜一郎	（群栄化学工業　取締役社長執行役員）

有　田　礼　二　　（東京海上日動火災保険　常勤顧問）

石　井　智　康　　（石井食品　取締役社長）

石　黒　不二代　　（ペガサス・テック・ホールディングス　取締役）

石　塚　茂　樹　　（ソニーグループ　社友）

石　塚　達　郎　　（タダノ　取締役）

石　塚　雅　洋　　（スーパーナース　取締役社長）

石　橋　さゆみ　　（ユニフロー　取締役社長）

伊　藤　　昇　　（日本アイ・ビー・エム　専務執行役員）

伊　藤　秀　俊　　（イノピスホールディングス　取締役社長）

井　上　裕　美　　（日本アイ・ビー・エム　取締役）

今　井　斗志光　　（豊田通商　副社長ＣＴＯ）

今　泉　泰　彦　　（構造計画研究所ホールディングス　社外取締役）

入　江　仁　之　　（アイ＆カンパニー　取締役社長）

岩　井　一　郎　　（ＩＣＭＧ　Ｄｉｇｉｔａｌ　執行役員）

岩　崎　俊　博　　（T.IWASAKI　取締役社長）

岩　本　修　司

岩　本　敏　男　　（ＮＴＴデータグループ　シニアアドバイザー）

宇　井　隆　晴　　（日本レジストリサービス　取締役）

植　地　卓　郎　　（アリックスパートナーズ・アジア・エルエルシー　日本代表）

宇　治　則　孝　　（技術同友会　代表理事）

臼　井　　努　　（京西テクノス　取締役社長）

内　永　ゆか子　　（ＧＲＩ　取締役社長）

浦　上　　彰　　（リョービ　取締役社長）

榎　本　英　二　　（野村不動産ホールディングス　執行役員）

遠　藤　弘　暢

大　賀　昭　雄　　（東通産業　取締役社長）

大久保　和　孝	（大久保アソシエイツ　取締役社長）
大久保　秀　夫	（フォーバル　取締役会長）
大　倉　正　幸	（ソミック石川　取締役副社長）
大　越　いづみ	（チェンジホールディングス　執行役員）
太　田　　寛	（シグマクシス・ホールディングス　取締役社長）
大　塚　博　行	（ジャパン・アクティベーション・キャピタル　取締役社長＆ＣＥＯ）
大　西　佐知子	（日本電信電話　常務取締役 常務執行役員）
大　西　　徹	（かんぽ生命保険　取締役兼代表執行役副社長）
大　野　　誠	（インテル　取締役社長）
大　橋　光　博	（Groundcover Consulting　代表取締役）
大　森　美　和	（ＡＡＪクリエーションズ　代表取締役）
岡　田　直　樹	（フジクラ　代表取締役 取締役社長ＣＥＯ）
奥　谷　禮　子	（ＣＣＣサポート＆コンサルティング　取締役会長）
奥　村　康　彦	（パナソニック コネクト　執行役員 シニア・ヴァイス・プレジデント）
小　椰　博　史	（ソニーネットワークコミュニケーションズ　エグゼクティブ・フェロー）
小　野　健　二	（日本アイ・ビー・エム　執行役員）
糟　谷　敏　秀	（東京ガス　代表執行役副社長）
片　倉　正　美	（ＥＹ新日本有限責任監査法人　理事長）
片　山　智　弘	（セガ エックスディー　取締役 執行役員）
葛　谷　幸　司	（ＢＩＰＲＯＧＹ　取締役専務執行役員）
川　上　登　福	（経営共創基盤　共同経営者（パートナー）マネージングディレクター）
川　上　結　子	（日本アイ・ビー・エム　執行役員）
川　﨑　博　子	（ＥＮＥＯＳホールディングス　取締役 取締役会議長）
川　添　雄　彦	（日本電信電話　取締役副社長 副社長執行役員）
河　野　昭　彦	（パナソニック コネクト　執行役員 アソシエイト・ヴァイス・プレジデント ・ＣＩＯ）

河　原　茂　晴	（河原アソシエイツ　代表 公認会計士（日本ならびに米国））
木　内　文　昭	（マクアケ　取締役）
木　島　葉　子	（実践女子学園　理事長）
北　野　泰　男	（キュービーネットホールディングス　取締役社長）
草　川　麗　子	（アイセル　取締役社長）
久保田　正　崇	（ＰｗＣ　Ｊａｐａｎグループ　グループ代表）
熊　谷　亮　丸	（大和総研　副理事長 兼 専務取締役）
栗　島　　聡	（ＮＴＴコムウェア　相談役）
桑　田　　始	（ＪＥＣＣ　取締役社長）
高　乗　正　行	（双日　顧問）
児　玉　哲　哉	（日本サイバーディフェンス　取締役）
後　藤　匡　洋	（野村證券　取締役副社長）
小　林　永　朋	（カネソウ　取締役）
小　林　洋　子	（宇宙航空研究開発機構（ＪＡＸＡ）　監事）
小　原　教　仁	（ファイザー　執行役員）
小　宮　義　則	（ＩＨＩ　エグゼクティブ・フェロー）
斉　藤　　剛	（味の素　取締役　執行役常務 Chief Transformation Officer(CXO)）
斎　藤　由希子	（日本マクドナルド　取締役・執行役員兼ＣＰＯ）
齋　藤　洋　平	（フューチャー　取締役ＣＴＯ）
坂　井　和　則	（TOPPANホールディングス　取締役副社長執行役員）
堺　　和　宏	（日本電気　執行役　Corporate SEVP 兼 Co-COO）
坂　口　英　治	（シービーアールイー　取締役会長兼ＣＥＯ）
坂　下　智　保	（富士ソフト　取締役社長執行役員）
坂　本　和　彦	
桜　井　伝　治	（日本情報通信　取締役社長）
櫻　井　祐　記	（富国生命保険　常勤顧問）

佐　谷　　進　　（プロレド・パートナーズ　代表取締役）

佐　藤　久　美　　（コスモ・ピーアール　取締役社長）

佐　藤　　司　　（サークレイス　取締役会長兼社長）

佐渡友　裕　之　　（プロティビティ　マネージングディレクター）

澤　　正　彦　　（出光興産　取締役副社長　副社長執行役員）

澤　田　千　尋　　（コムチュア　代表取締役 社長執行役員）

椎　名　　茂　　（ＵＭＩ　取締役会長）

椎　野　孝　雄　　（キューブシステム　取締役（社外））

ステファン・ジヌー　　（エアバス・ジャパン　取締役社長）

島　田　俊　夫　　（CAC Holdings　特別顧問）

下　野　雅　承　　（日本アイ・ビー・エム　名誉顧問）

神　宮　由　紀　　（フューチャー　取締役）

杉　浦　英　夫　　（有限責任監査法人トーマツ　マネージングディレクター）

杉　野　尚　志　　（レイヤーズ・コンサルティング　代表取締役ＣＥＯ）

鈴　木　啓　太　　（日本精工　取締役 代表執行役専務・ＣＦＯ）

鈴　木　正　敏　　（ServiceNow Japan　執行役員社長）

須　藤　憲　司　　（Kaizen Platform　代表取締役）

諏　訪　暁　彦　　（ナインシグマ・ホールディングス　取締役社長）

関　　マサエ　　（ＩＩＭヒューマン・ソリューション　取締役社長）

関　　正　樹　　（みずほ証券　取締役会長）

瀬　山　昌　宏　　（インターエックス　取締役社長）

千　田　哲　也　　（日本郵便　取締役社長兼執行役員社長）

相　馬　剣之介　　（森トラスト　取締役）

曽　谷　　太　　（ソマール　取締役社長）

反　町　雄　彦　　（東京リーガルマインド　取締役社長）

平　　皓　瑛　　（ＳＭＢＣクラウドサイン　取締役）

高　橋　弘　二	（大日精化工業　取締役社長）
髙　橋　悠　人	（レバテック　代表執行役社長）
高　畑　　勲	（インフィニオンテクノロジーズジャパン　取締役 最高財務責任者）
瀧　原　賢　二	（日清製粉グループ本社　取締役社長）
田久保　善　彦	（グロービス経営大学院大学　常務理事）
田　尻　克　至	（ＳＯＭＰＯホールディングス　執行役員専務）
多　田　雅　之	（アルファパーチェス　取締役　社長 兼 ＣＥＯ）
巽　　達　志	（住友商事　執行役員）
田　中　　潤	（ウイングアーク１ｓｔ　代表取締役 社長執行役員CEO）
田　中　淳　一	（ジェンパクト　取締役社長）
田　中　孝　司	（ＫＤＤＩ　取締役会長）
田　中　豊　人	（Ｂｌｕｅ　Ｌａｂ　取締役社長）
田　中　若　菜	（リンクトイン・ジャパン　日本代表）
田　沼　千　秋	（グリーンハウス　取締役社長）
種　市　順　昭	（東京応化工業　代表取締役 取締役社長）
玉　塚　元　一	（ロッテホールディングス　取締役社長ＣＥＯ）
田　村　修　二	（日本貨物鉄道　相談役）
塚　田　亮　一	（アシアル　取締役）
津　上　晃　寿	
塚　本　英　彦	（日本信号　取締役社長）
塚　本　　恵	（デジタルソサエティフォーラム　代表理事）
堤　　浩　幸	（アマゾン ウェブ サービス ジャパン　常務執行役員）
角　田　賢　明	（ジャスト　取締役社長）
出　張　勝　也	（オデッセイ コミュニケーションズ　取締役社長）
ポール・デュプイ	（Take-5 Global　取締役社長）
徳　永　優　治	（エゴンゼンダー　パートナー）

富　田　純　明　　（日進レンタカー　取締役会長）

鳥　越　慎　二　　（アドバンテッジリスクマネジメント　取締役社長）

中　島　史　雄　　（ユアサM&Ｂ　取締役専務執行役員）

中　嶋　康　晴　　（キッコーマン　常務執行役員）

長　瀬　玲　二　　（長瀬産業　特別顧問）

中　防　　保　　（レイヤーズ・コンサルティング　代表取締役ＣＯＯ）

中　俣　　力　　（日本郵政　常務執行役）

中　村　哲　也　　（日本タタ・コンサルタンシー・サービシズ　副社長執行役員）

中　村　壮　秀　　（アライドアーキテクツ　取締役社長）

中　山　克　成　　（ベース　取締役社長）

永　山　妙　子　　（ＦＲＯＮＴＥＯ　取締役）

中　山　泰　男　　（セコム　特別顧問）

楢　﨑　浩　一　　（ＳＯＭＰＯホールディングス　グループCDO 執行役専務）

南　部　智　一　　（住友商事　取締役 副会長）

西　　恵一郎　　（富士通　ＳＶＰ　ＣＥＯ室長）

西　島　剛　志

野　田　由美子　　（ヴェオリア・ジャパン　取締役会長）

野　中　賢　治　　（ﾏｯｷﾝｾﾞｰ･ｱﾝﾄﾞ･ｶﾝﾊﾟﾆｰ･ｲﾝｺｰﾎﾟﾚｲﾃｯﾄﾞ･ｼﾞｬﾊﾟﾝ　シニア・パートナー）

橋　本　祥　生　　（コンカー　取締役社長）

橋　本　孝　之　　（日本アイ・ビー・エム　名誉相談役）

橋　本　英　知　　（ベネッセホールディングス　専務執行役員）

橋　本　優　希　　（キョウデン　取締役）

羽田野　彰　士　　（テルモ　顧問）

濱　　逸　夫　　（ライオン　相談役）

濱　田　奈　巳　　（コカ･コーラボトラーズジャパンホールディングス　社外取締役）

早　坂　宣　則　　（アイネックス　取締役社長）

林　　郁	（デジタルガレージ　代表取締役 兼 社長執行役員グループＣＥＯ）
林　　信　秀	（日本経済調査協議会　理事長）
原　　一　将	（マクニカホールディングス　取締役社長）
原　　雄　介	（デンソー　上席執行幹部）
原　田　典　子	（ＡＩ　ＣＲＯＳＳ　代表取締役ＣＥＯ）
樋　口　智　一	（ヤマダイ食品　取締役社長）
樋　口　泰　行	（パナソニック コネクト　取締役 執行役員 プレジデント・ＣＥＯ）
平　井　康　文	（楽天グループ　副社長執行役員）
平　石　洋　子	（ファイザー　執行役員）
平　澤　　潤	（協栄産業　取締役社長）
平　野　大　介	（マイスターエンジニアリング　取締役社長）
福　田　達　男	（新時代戦略研究所（ＩＮＥＳ）　主任研究員）
福　田　　譲	（富士通　執行役員 ＥＶＰ ＣＤＸＯ，ＣＩＯ）
藤　井　　剛	（富士通　Ｃｏ－Ｈｅａｄ）
藤　木　貴　子	（グーグル　上級執行役員　マネージングディレクター）
藤　重　貞　慶	（ライオン　特別顧問）
藤　原　和　彦	（ソフトバンク　取締役専務執行役員ＣＦＯ）
藤　原　総一郎	（長島・大野・常松法律事務所　マネージング・パートナー）
藤　原　　遠	（ＮＴＴデータ先端技術　取締役社長）
舩　橋　　元	（ＩＣＭＧ　取締役社長）
船　橋　　仁	（ＩＣＭＧ　取締役会長）
古　川　　厚	（パナソニック コネクト　執行役員 ヴァイス・プレジデント）
星　　久　人	（ベネッセホールディングス　特別顧問）
程　　近　智	（ベイヒルズ　代表取締役）
堀　　新太郎	（ベインキャピタル・プライベート・エクイティ・ジャパン．LLC シニア アドバイザー）
前　野　伸　幸	（ホットスケープ　代表取締役）

牧　浦　真　司　（商工組合中央金庫　取締役）

正　西　康　英　（ラキール　取締役 上席執行役員）

間　下　直　晃　（ブイキューブ　取締役会長 グループＣＥＯ）

増　田　健　一　（アンダーソン・毛利・友常法律事務所外国法共同事業　パートナー）

益　戸　宣　彦　（ＲＢＧパートナーズ　マネージング・パートナー）

増　山　美　佳　（増山 ＆Ｃｏｍｐａｎｙ　代表）

松　林　知　史　（ティルフ・マネジメント　代表）

三　嶋　英　城　（ＳＭＢＣクラウドサイン　取締役社長）

湊　　宏　司　（イトーキ　取締役社長）

南　　昌　宏　（りそなホールディングス　取締役兼代表執行役社長兼グループＣＥＯ）

三　原　寛　人　（昭芝製作所　取締役社長）

宮　川　純一郎　（全日空商事　取締役社長）

三　宅　茂　久　（税理士法人山田＆パートナーズ　統括代表社員）

宮　崎　達　三　（ミライト・ワン　取締役専務執行役員）

牟　田　正　明　（トランスコスモス　取締役共同社長）

村　上　　努　（日本政策投資銀行　取締役常務執行役員）

村　瀬　龍　馬　（ＭＩＸＩ　取締役　上級執行役員）

室　元　隆　志　（サントリーホールディングス　常務執行役員）

森　　浩　志　（三菱ＵＦＪ銀行　取締役専務執行役員ＣＬＯ）

森　　正　勝　（国際大学　特別顧問）

森　岡　　琢　（ジェムコ日本経営　取締役社長）

森　川　　智　（ヤマト科学　取締役社長）

森　川　徹　治　（アバントグループ　取締役社長グループＣＥＯ）

矢　口　敏　和　（グローブシップ　取締役社長）

山　内　雅　喜　（ヤマトホールディングス　参与）

山　極　清　子　（ｗｉｗｉｗ　会長）

山　口　明　夫	（日本アイ・ビー・エム　取締役社長執行役員）
山　口　公　明	（セントケア・ホールディング　取締役）
山　口　修　治	（電通グループ　dentsu Japan データ&テクノロジー プレジデント）
山　口　有希子	（パナソニック コネクト　取締役 執行役員 シニア・ヴァイス・プレジデント・CMO）
山　田　哲　矢	（ラックス建設　代表取締役）
横　山　　文	（OXYGY　エグゼクティブアドバイザー）
吉　田　雅　俊	（日税ホールディングス　取締役会長）
吉　丸　由紀子	（積水ハウス　取締役）
脇　坂　克　也	（東武トップツアーズ　取締役副社長執行役員）
脇　山　保　生	（明治安田生命保険　執行役員）

以上234名

事務局

菅　原　晶　子	（経済同友会　常務理事）
針　替　孝　之	（経済同友会　政策調査部　マネジャー）
森　山　武　尊	（経済同友会　政策調査部　調査役）
児　島　健太郎	（経済同友会　政策調査部　マネジャー）