経済産業省
Ministry of Economy, Trade and Industry

10・11月号
October / November 2016

METI Journal

［経済産業ジャーナル］

進めてる？

サイバーセキュリティ対策

第２特集

2020年には30兆円が目標！

世界に飛び出せ！ ニッポンのインフラ

Special Report

変化が望まれる株主総会プロセス
企業と株主・投資家との対話促進に向けて

リスクマネジメントの心得

慶應義塾大学
名誉教授
土居範久さん

どいのりひさ／慶應義塾大学名誉教授、(独) 科学技術振興機構社会技術研究開発センター参与。日本学術会議副会長、文部科学省次世代スーパーコンピュータ戦略委員会主査、総務省情報通信技術分科会会長などを歴任。現在、CSSCサイバーセキュリティ演習実行委員長、日本セキュリティ監査協会会長など。情報処理学会名誉会員。日本ソフトウェア科学会名誉会員。

経済協力開発機構(OECD)では、1992年に「情報システムのセキュリティのためのガイドライン」を採択しています。このガイドラインはOECD加盟国の法制度の基盤として広く採用されています。

近年、情報セキュリティに係る事件・事故が日常茶飯になってきたので、経済および社会の繁栄のために信頼あるオープンなデジタル環境を築き利用するためには、政府、官民の組織において高度なセキュリティリスクマネジメントを行う必要があるという方向に舵を切り替えた勧告が2015年9月に採択され、このガイドラインに取って代わりました。

“リスク”はISOでは「目的に対する不確かさの影響」と定義しています。「影響」とは「期待されていることから、好ましい方向および／または好ましくない方向に乖離すること」です。つまり、常識とは異なり、“負のリスク”だけではなく“正のリスク”があるということです。情報セキュリティにおいては“負のリスク”を想定していますが、リスクマネジメントを行う際にはこの点を十分心得ておく必要があります。

第１特集 進めてる？

04 サイバーセキュリティ対策

METI Journal

Contents 10・11 月号

編集・発行／経済産業省大臣官房広報室
東京都千代田区霞が関１丁目３番１号
TEL.03-3501-1511（代表）
編集協力／株式会社コンセント

METI Journal Facebookページ

METI Journal ヘルプページ

CLICK! をクリックするとより詳しい情報にアクセスできます。

第２特集

14 世界に飛び出せ！ ニッポンのインフラ

進めてる？

サイバーセキュリティ対策

毎日の暮らし・ビジネスにおいて、今、IT機器やインターネットは不可欠な存在。
ただし、便利さや手軽さの裏側には、リスクや危険が潜んでいるのが世の常です……。
あなたや、あなたの会社が被害に遭う前に、始めませんか？
サイバーセキュリティ対策！

大事なのは分かるけれど、何から始めたらいいか……」。サイバーセキュリティ対策というと、そんなふうに思っている人もきっと少なくないはずです。しかし現実には、サイバー攻撃の件数は増加傾向。特定の企業や組織を狙った標的型の攻撃も当たり前になってきていて、“人ごと”ではいられない状況です。

まして最近は、さまざまな機器やシステムがインターネットとつながって作動するIoTも進展。人の目が届きづらいところで、知らぬ間に被害が広がるケースも出てきており、企業としても、個人としても、見過ごすことはできません。

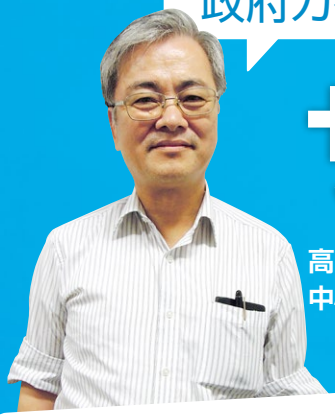
サイバーセキュリティ対策にいくらお金をかけても、それは直接的に利益を生まないことがほとんどでしょう。とはいえ、個人情報や技術情報が流出したり、工場等の制御システムが被害を受けたりしたら、取り返しがつかない事態を招くこともある。また、仮に自動運転や医療の分野でIoT機器が攻撃を受けるようなことがあれば、それは人命にもかかわります。やはりITの活用とそのセキュリティ対策は、クルマの両輪として考えなければなりません。

そこで経済産業省などは、「何から始めたらいいか……」の声に応えるため、2つのガイドラインを策定、公表しています。1つは「サイバーセキュリティ経営ガイドライン」。経営者が意識すべきポイントなどをまとめたものです。もう1つは「IoTセキュリティガイドライン」。こちらは、利用者を含めたIoT機器、システムの関係者に対策への認識を促す内容となっています。

次ページ以降では、それらのガイドラインにも触れながら、サイバー攻撃への対処法、サイバーセキュリティ対策の実践例などを紹介していきます。それら最新の情報を参考に、ぜひ、今後のセキュリティ強化を考えてみてください。

政府ガイドライン策定の専門家に聞く

サイバーセキュリテ



高まるサイバー攻撃の脅威に、どう対応していけばいいのか。政府の対策ガイドライン作成でも中心的な役割を果たした東京電機大学の佐々木良一先生にポイントを聞きました。

多様化・巧妙化するサイバー犯罪

近年、サイバー犯罪の悪質化がさらに進んでいます。科学技術庁のサイトが不正アクセスで改ざんされ、サイバー攻撃が世間の耳目を集めた2000年当初は、ハッカーが不特定のサイトを面白半分に攻撃するというものが大半でした。しかし、イランの核燃料施設へのサイバー攻撃があった2010年頃から、経済的利益を得る目的や国家の指示により重要インフラや企業などを狙った標的型のサイバー攻撃が増えています。

攻撃の手口も、標的企業の社員が関心を持ちそうな内容を装った複数のメールを送信し、誰か一人が添付ファイルを開封すると被害がLANでつながった社内のコンピュータすべてに及ぶなど巧妙になりました。しかも、機密情報を盗み出す従来型の犯罪に加え、データの改変でシステムに誤作動を起こしたり、企業のシステムを使えなくして原状復帰と引き替えに代金を要求するなど、犯罪の形態も多様化し、被害の額も大きくなっています。

サイバー犯罪は原価が安く、足がつきにくいことから“割のよい犯罪”とされ、組織的な犯行が増えています。今後も攻撃は、さらに厳しくなっていくといえるでしょう。

経営者自身のコミットが重要

サイバーセキュリティへの投資はリターンが見えにくいため、これまで企業等で対応が進んでいるとは言えませんでした。しかし実際に機密情報が流出した企業では、ブランドの失墜に加え、対応にも数十億から数百億円のコストがかかるなど、その影響は大きくなります。だからこそ、まずは経営者がリスクを認識し、自らコミットして対策を進めることが大切です。

IoTの経営者・開発担当者・利用者が気をつけたいポイント

供給企業の経営者
- 経営者として、IoTがサイバー攻撃を受けた場合の影響の大きさをまず理解する
- IoTのセキュリティ確保について、自ら対策にコミットしていく

機器・サービスの開発担当者
- 不特定多数との接続や長期使用を前提にしたセキュリティ設計を行う
- 最初からしっかり対策を行うほうが低コストであることを理解する

一般利用者
- IDやパスワードを初期設定のままにせずしっかり設定しなおす
- 使用していない機器の電源を切り、廃棄する際はデータを消す

例えば、セキュリティパッチが配信されたらきちんと適用してパソコンやサーバーのOS・ソフトウェアを更新する、パスワードを高度化するといった安価な対策を取るだけでもリスクは軽減します。また、不正メールの見極めによる侵入予防、社内のネットワーク分離での侵入拡大抑制、ファイアーウォールによる外部への情報流出防止などを合わせた多層防御ができれば安全性もより高まるでしょう。リスクを分析し、コストと効果を検討しながら自社に合った方法を選ぶといいと思います。

IoTの安全確保も大きな課題です。センサーなどのIoT機器のなかには、セキュリティ対応するには性能に限りがあるものも多く、耐用年数も長く、長期にわたって監視が行き届かない状態になりやすいものがあります。また昨年、遠隔ハッキングで自動車のブレーキが利かなくなるという実験結果も報道されましたが、乗っ取りで誤作動が起きれば社会への影響も大きい。機器やサービスを供給する企業の経営者は、そうしたIoTの性質を理

イ対策の鉄則

佐々木良一さん
東京電機大学教授。同大学サイバーセキュリティ研究所所長。内閣官房サイバーセキュリティ補佐官。日立製作所での研究開発などを経て現職へ。日本セキュリティ・マネジメント学会前会長。

CLICK! ●東京電機大学 未来科学部 情報メディア学科 情報セキュリティ研究室

解した上で、セキュリティや開発の担当者と対策を進める必要があります。まずIoT化の必要性を判断し、IoT化するなら不特定の相手とつながり、長期間使用する前提でしっかりしたセキュリティ設計を行う。最初からチップに必要機能を組み込むなどしておけば、安全装置を後付けしたり、問題が起きて対応するよりコストも安く済みます。大きな可能性を持つIoTで高い安全性が実現できれば、それが競争力につながると考えていただくといいと思います。

政府の指針も生かしセキュリティを考える

政府も対策の指針として、「サイバーセキュリティ経営ガイドライン」、「IoTセキュリティガイドライン」の2つを公表しました。

セキュリティ対策での経営者の役割について読みやすくまとめた前者は、昨年春に特殊法人での大規模なデータ流出が起きた影響もあって多くの方にお目通しいただき、社長レベルでセキュリティ対策を進める文化の浸透に寄与できたと感じています。また後者は、経済産業省と総務省が協力し、経営者・開発担当者・利用者など幅広い層に向け、製品のライフサイクル全体に対応した包括的な指針を初めて出したもの。この指針をもとに、自動車、医療機器など産業分野ごとの議論が行われているとも聞いています。

最近は各社の意識も高まり、有事の際の証拠にもなるアクセス記録(ログ)の保管が大きな流れになっています。サイバーセキュリティの緊急事態対応チーム(CSIRT／CERT)を持つ企業も増えました。技術面でもログ解析で異常時にはアラートを発するソフトなどが登場しています。一方で攻撃方法も進化し、今後はAIを搭載したウィルスが出る可能性も高い。2020年には530億個の機器がネットワークに接続されるといわれており、IoT化が進むなかで対策を取らずにいればそれだけリスクも上がります。そうしたなかでは、最新情報の収集・共有や地道な対策を続け、新たな脅威に対応していくことが必要。2つのガイドラインが、多くの人がサイバーセキュリティについて考え、議論を深めるきっかけになればと考えています。

サイバーセキュリティ経営ガイドライン CLICK!

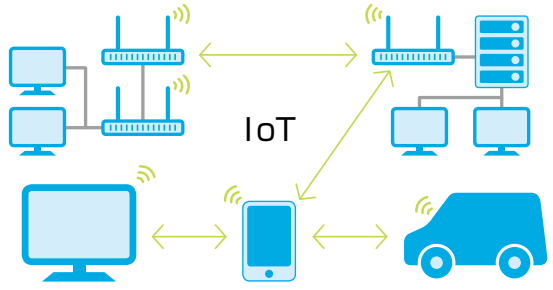
ビジネスに不可欠なITの安全性を確保すべく、政府が経営者に向けて発行した初のセキュリティ対策指針。サイバー攻撃のリスクと対策の必要性、経営者が最低限認識すべき3原則、管理の枠組みづくりや事前対策、攻撃を受けた場合の重要10項目などが分かりやすくまとまっている。

経営者が認識すべき3原則

- 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
- 自社のみならず、ビジネスパートナーを含めた対策が必要
- 平時及び緊急時のいずれにおいても、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

IoTセキュリティガイドライン CLICK!

IoTのセキュリティ対策についての包括的ガイドライン。経営者・開発担当者・利用者など幅広い対象に向け、リスク分析や対策方針の策定、機器・サービスの設計から製造、運用・保守までIoT供給の全過程における留意点、IoTを利用する際の注意点などをまとめている。



サイバーセキ最前

日立製作所

社内認定制度もつくり セキュリティ人財を育成

日立グループでは“情報セキュリティ人財”の存在を重視。社内認定制度なども創設し、その発掘や育成に力を注いでいます。人財像については、経済産業省によるITスキル標準をベースに、未知の攻撃に対応できる「高度セキュリティ人財」、既知の攻撃に対応できる「システム開発運用をまとめるセキュリティ人財」、「展開されたセキュリティ対策を実施する人財」の3つに分類。それぞれに必要な教育と演習を実施しています。

CLICK! ●日立製作所 情報セキュリティ報告書2016

NEC

委託先と一体となってセキュリティを強化

NECグループは、業務委託先を情報セキュリティ対策状況のレベルに応じて分類。適切なレベルの委託先を選定することでリスクの低減を図っています。また委託先に対して、毎年、書類点検や訪問点検も行い、その結果を個別にフィードバック。委託先が自身のセキュリティ水準を確認できるようにもしています。さらには全国で情報セキュリティ説明会も開催し、NECグループとしての対策を伝えるなど、多面的な取り組みを推進中です。

CLICK! ●NEC 情報セキュリティ報告書2016

東京ガス

CSMSの認証取得でLNG基地を守る

万一、制御システムの障害によってガスの供給がストップすれば、社会的影響は計り知れない——。東京ガスは日立LNGガス基地においてCSMS※の認証を取得しました。既存の基地でもセキュリティ確保に努めていたものの、今回の認証取得により、そのレベルや課題をより客観的に確認できるようになりました。さらにPDCAを回す仕組みもいっそう充実。外部環境が変化しても、継続的にセキュリティを維持できる体制を整えています。

※Cyber Security Management System。国際電気標準会議(IEC)が規定した国際標準IEC 62443-2-1。

CLICK! ●東京ガスグループ CSMS認証取得事例

富士通

ガイドラインに準拠した基本方針をいち早く策定

富士通は、「サイバーセキュリティ経営ガイドライン」に準拠した「富士通グループ情報セキュリティ基本方針」を新たに策定。ウェブサイトなどを通じて、その内容を公表しています。あわせて、情報セキュリティ体制において、リスク・コンプライアンス委員会の下に最高情報セキュリティ責任者（CISO）を設置。グローバルな情報セキュリティ体制の見直しも行い、各種施策等の確実な実行を目指しています。

CLICK! ●富士通グループ 情報セキュリティ基本方針

ユリティ線！

「これから本格的な対策を」と考えたとき、他社の事例は大いに参考になるはず。先行する各社が独自に取り組むサイバーセキュリティ対策をピックアップしました。

大成建設

CSIRTを立ち上げ緊急時の体制を拡充

大成建設は建築業界で初めて、日本シーサート協議会加盟の組織内CSIRT「T-SIRT」を発足。従来、情報企画部で行っていたインシデント対応などを担わせるとともに、緊急時の対応体制を拡充しています。T-SIRTは、社長室直下の情報企画部と情報系グループ会社である大成情報システムのメンバーから構成される仮想的な組織体。図面や顧客情報を共有する協力会社や専門工事業者へも技術的な支援を行っています。

CLICK! ●大成建設 Taisei-SIRT

大日本印刷

実例に基づくシナリオでリアルな訓練ができる

事業活動で大量の個人情報を取り扱う大日本印刷。同社は、その中で培った情報漏えい阻止などのノウハウをもとに、セキュリティ技術者の訓練システムを構築。企業等に提供しています。特徴は、実例に基づく攻撃シナリオによるリアルな防御トレーニングが可能なこと。1チーム4人単位で訓練でき、リーダーがメンバーの役割やタスクを設定したり、次の行動を指示したり――。チーム力とリーダシップを同時に養える仕組みとなっています。

CLICK! ●大日本印刷

［ IPA（独立行政法人 情報処理推進機構）］

企業規模の大小にかかわらず サイバーセキュリティは経営課題！

リスクを熟知する現場が、今、伝えたいこと

――経済産業省とIPAで策定した「サイバーセキュリティ経営ガイドライン」には、どんなメッセージが込められているのでしょうか。

サイバーセキュリティを経営戦略上の問題ととらえ、**経営者自らが指揮して対策を取ってほしい**、との思いです。例えば、対策にどの程度投資するか、セキュリティ強化をいかに自社の優位性としてアピールするか。これらの決定には、まさに経営判断が求められます。サイバーセキュリティ対策は、**企業のリスクマネジメントの一環**なのです。

――中小企業向けのガイドラインの改訂も進めているとのことですが。

IPAの調査で、規模の小さい企業ほど対策に不備があることが浮き彫りになったためです。例えば、**小規模企業の過半数が社員の私物端末の業務利用を認めている一方、端末のパスワード設定の実施割合は全体平均より低い傾向に**あります。

2009年の策定以来、初めてとなる今回の改訂では、モバイルやクラウドの進展、またマイナンバー制度などの法規制の変化にも対応する計画です。さらに自社の診断シートのほか、マネジメントサイクルの構築・運用のための「資産管理台帳」や「脅威別対策一覧」などのツールも付録として用意する予定です。

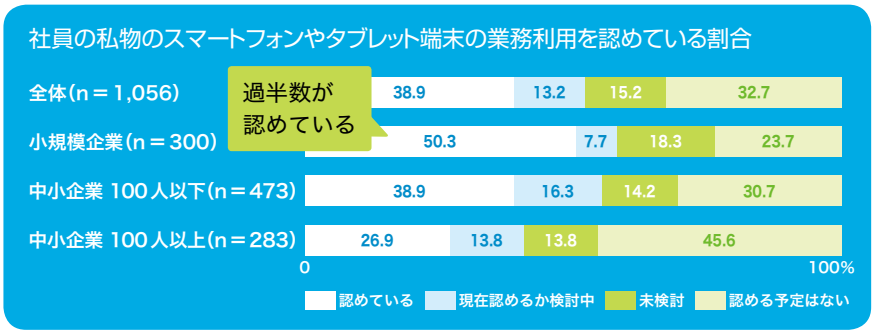
――さまざまな分野でIoT製品が普及してきています。安全性を確保するには何が必要でしょうか。

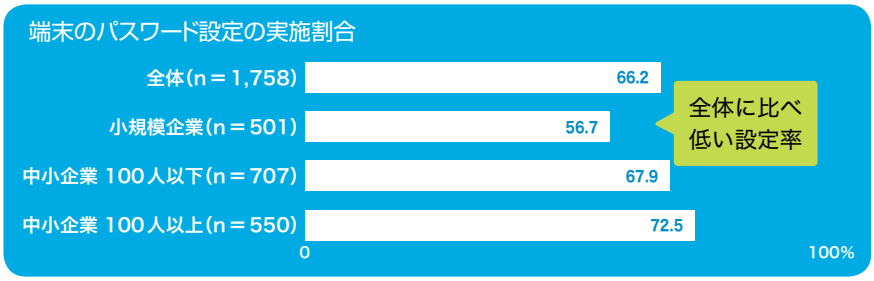
製品やシステムの開発時にそのリスク要因をどれだけ網羅できるかが鍵となるでしょう。その上で、**あらかじめ安全・安心を維持するための仕組みを組み込んでいくことが重要です。**とはいえ、多くの技術者は専門性を追求する中で、横断的、俯瞰的な視点を持ちにくいのが現実。広範な視野を持つ技術者の育成が課題です。

――社会全体のサイバーセキュリティ対策を強化するため、IPAとしてはどんな活動を行っていきますか。

「サイバーセキュリティ経営ガイドライン」が公表されて以来、それが企業などで議論の的になっている一方で、「対策の具体的なイメージがわかない」との声もいただいています。今後は、**各重点項目の実施手順を具体的に記載した解説書をつくるなど**して、経営者、管理職、社員のコミュニケーション促進を後押しできればと考えています。

中小企業における情報セキュリティ対策





「2015年度 中小企業における情報セキュリティ対策に関する実態調査」報告書（IPA）

【IPA】複雑・膨大化する情報社会システムの安全性・信頼性の確保による“頼れるIT社会”の実現に向け、IT施策の一端を担う政策実施機関。ミッションとして「情報セキュリティ」「情報処理システムの信頼性向上」「IT人材育成」を掲げている。「情報セキュリティ白書2016」の発行なども行う。

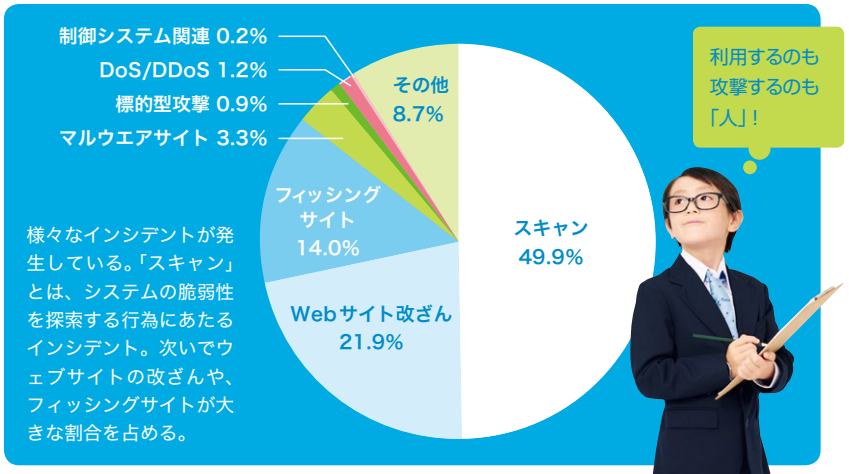
CLICK! ●情報処理推進機構

日々、コンピュータウイルスや不正アクセスなどのインシデントと向き合い、その対応に取り組んでいる国内の２大専門機関に、サイバーセキュリティ対策について「ぜひ知っておいてほしいこと」を話してもらいました。

［ JPCERT/CC（一般社団法人 JPCERTコーディネーションセンター）］

インシデントを“自分ごと”としてとらえ基本的な対策を怠らないことが大事

インシデント件数のカテゴリ別割合（2015年4月～2016年3月）



――サイバー攻撃が巧妙かつ複雑なものになっているといわれます。実態をどのように見ていますか。

攻撃側が組織化してきているといわれ始めたのが10年ほど前。そして、攻撃が社会に及ぼすダメージが顕在化してきたのが５年ほど前からです。その中で確かに攻撃の技術は高度化していますが、もう一つ見逃せないのは**社会全体のITへの依存度が急速に高まっている点。**ITが社会活動、企業活動の基盤となっていくにしたがって、攻撃の対象や手法の幅が広がっているのが現状です。

――具体的な対策のポイントについて聞かせてください。

まずOSなどのアップデートやセキュリティソフトの導入はしっかり行うこと。**基本的な対策を怠らなければ、かなりの攻撃を防げることを知ってほしい**と思います。

現実には、アップデート前の状態でシステムを稼働させていたり、不審なメールの添付ファイルを開いてしまったり……。そうした不備を突かれているケースが非常に多いのです。

――セキュリティ対策を進める際の姿勢や意識面についてアドバイスはありますか。

日々のインシデントなどを**“自分ごと”としてとらえることが大事。**万一、企業がサイバー攻撃を受け、その被害が取引先や顧客にまで及ぶようなことがあれば、世間からの信頼や評判は大きく低下してしまいます。しかしながら、これまで攻撃を受けたことのない企業が甚大な被害を具体的にイメージするのは簡単ではありません。その意味では、インシデントを自分ごととしてとしてとらえて、対応していくことが評価されるような社会をつくっていくことも重要だと思います。

――最後に、これから対策を本格的に始めようという企業や個人に一言お願いします。

サイバー攻撃を仕掛けるのも、受けるのも「人」。対策を考える際は、それを頭に入れておくことが大切です。セキュリティ機器やソフトを導入するにあたっても、ITの利用者ができる限り早く異変に気付くためにはどうしたらいいか、攻撃者を素早く捕捉するためには何が必要か――。そうした視点が欠かせません。

そのためにも、組織のセキュリティ対策については**「事前準備」が重要。**インシデントが発生した場合の体制やマニュアルを予め整備しておくことが有効です。被害が一気に拡大するサイバー攻撃への対応において**“スピード”は大事な要素となるでしょう。**

【JPCERT/CC】インターネットを介して発生する侵入やサービス妨害等について、情報の収集や発信、対応の支援、また再発防止のための対策の検討や助言などを技術的な立場から実施。特定の政府機関や企業からは独立した中立の組織として、日本の情報セキュリティ対策の向上に積極的に取り組んでいる。

CLICK! ●JPCERT コーディネーションセンター

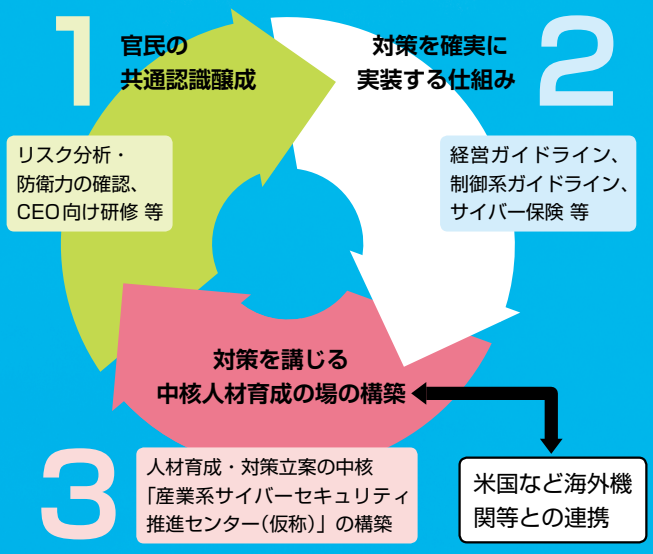
官民一体で重要インフラを サイバー攻撃から守る!

社会活動を支えるインフラがサイバー攻撃を受ければ、影響、被害は甚大です。
年々高まるその脅威へどう対応すべきか――。国と企業等が連携する最新の取り組みについて紹介します。

例えば2015年、ウクライナの電力会社がサイバー攻撃を受け、大規模停電が発生しました。もちろん日本でも、そうした攻撃があれば社会的混乱や経済的損害は避けられず、人命も危機にさらされる――。国家の安全保障の面からも、サイバーセキュリティ強化は必須です。

潤沢な軍事予算を持つ米国やイスラエルでは、軍や情報機関のニーズに応える形で技術と人材が育ってきましたが、状況の異なる日本では、インフラの安定的な運用を担う企業と政府が協調し、必要な投資がなされる社会システムの構築が大事。そこで、両者が意識を共有し、ガイドライン策定やサイバー保険などの制度を通して対策を推進する仕組みを設け、実際に対策を継続する人材を育てるというサイクルをつくることを目指しています。

サイバーセキュリティ対策を進めるサイクル



人材育成の中核を担う 産業系サイバーセキュリティ推進センターの役割

【産業系サイバーセキュリティ推進センター】
企業等でサイバーセキュリティ対策の中核となる人材を官民が連携して育成する拠点。模擬プラントを使った演習なども行う。

模擬プラントを用いた検証や演習、対策立案

日々高度化するサイバー攻撃からインフラや産業基盤を守るためには、実際の攻撃を想定した実践的な訓練が必要。そのため、情報系システムから制御システムまでシステム全体を備えた模擬プラントを設置。ホワイトハッカーや研究者などの専門家とともに、攻撃から早期にシステム復旧する演習や、安全性・信頼性の検証などを通じて実践力を養成する。米国関連省庁との共同演習やイスラエルの企業・省庁との人材交流など海外との連携も推進し、最新の知見を得る。

模擬プラントを用いたサイバー演習の様子

実システムの安全性などの検証と対策立案

企業が導入を計画する制御システムやIoT機器の安全性・信頼性について、依頼ベースで調査を行う。ベンダー企業、ユーザー企業、専門家がチームを組み、安全性・信頼性の検証と、その向上のために必要な対策立案を行う。

攻撃情報の収集・研究

ネットワーク、制御システム、犯罪心理学など幅広い分野の研究者の知見を結集し、新たな攻撃手法を収集、分析、研究することによって攻撃トレンドをつかむことで、対策強化に役立てる。

ガイドラインの公表はゴールではない。課題を取り入れ、発展させていきます！

各種ガイドラインの策定や施策の推進、人材の育成などを通して、激化するサイバー攻撃から、産業や生活の重要インフラを守る――。そうした活動への思いについて、経済産業省の担当者が語ります。

市ノ渡 社会のIoT化など進むなかで、重要インフラや産業システムを標的としたサイバー攻撃が、国や企業の大きな脅威になっています。当課ではこの新たなリスクから社会基盤を守るサイバーセキュリティの強化に、ガイドラインの策定や各種対策の推進などを通じて取り組んでいます。

石見 昨年末に公表された「サイバーセキュリティ経営ガイドライン」は、国として初となる経営者を対象としたセキュリティ指針です。日本は海外に比べると、サイバー攻撃に対する経営層の関心が薄いという調査結果もありますが、サイバー攻撃で情報が漏洩したり、業務が停滞したりすれば企業へのダメージも大きい。経営者の方々に、こうした問題を経営リスク、自らの課題として考えてもらえるよう留意しました。

市ノ渡 また本年7月公表の「IoTセキュリティガイドライン」では、汎用性を持たせることを意識しながら、IoTに関する初の指針を示しました。

森川 IoTの分野では日々新しい技術が開発され、機器への実装が進んでいます。そうした状況のなかで、IoT機器を製造する企業の経営者や開発担当者、情報セキュリティベンダー、一般利用者といった多様な人たちにとって価値のある指針を策定するには、“ネットにつながるリスク”とIoTの未来像を見据え、それぞれが自らの立場で考えを深める共通の土台になるようなものにする。これが大切だと考えていました。

現場の意見をもとに指針を進化させていく

石見 「サイバーセキュリティ経営ガイドライン」の公表後、経営者の方から「委託の情報システム会社に、ガイドラインに沿った対応ができているか確認してみた」など多数の反響をいただいてます。報道されるサイバー事故は大規模な組織や企業のものが中心ですが、近年は安全対策が不十分になりがちな中小企業を狙うハッカーも増えています。企業規模を問わず対策はすべきものだと考えていただきたいですね。

森川 「IoTセキュリティガイドライン」へのパブリックコメントの多さに、IoTに対する期待と不安の大きさを実感しました。指針の公表はゴールではなく、その普及や対策もしっかり進めることが重要。またガイドライン自体も「ver 1.0」というバージョン名があるとおり、今後の課題を取り入れながら発展させていくべきものとなっています。時々の問題をしっかり把握しながら検討を続けていきたいと心しています。

市ノ渡 ガイドラインを進化させるには、やはり現場の方たちの意見が欠かせません。またIoTやFinTechの普及でサイバー攻撃から守るべき対象が広がるなか、対策を担うセキュリティ担当者の育成を進める必要もあります。東京五輪が行われる2020年、第4次産業革命を経た2030年という節目に向けて、日本の産業のコアを支える人材と基盤づくりに関われることに、強いやりがいを感じています。

商務情報政策局
サイバーセキュリティ課
（左から）
課長補佐　石見賢蔵
課長補佐　市ノ渡佳明
係長　森川淳

今年6月、情報セキュリティ政策室から体制を増強して課となったサイバーセキュリティ課では、重要インフラをはじめとする企業等のサイバーセキュリティ対策の強化を図るための施策を進めている。

世界に飛び出せ！ニッポンのインフラ

2020年には30兆円が目標！

急速な都市開発と経済成長により、新興国を中心とした世界のインフラ需要は膨大です。しかし、日本はその機会を活かし切れていないのが現状です。日本のインフラを普及させるためには、一体何が必要なのでしょうか――。

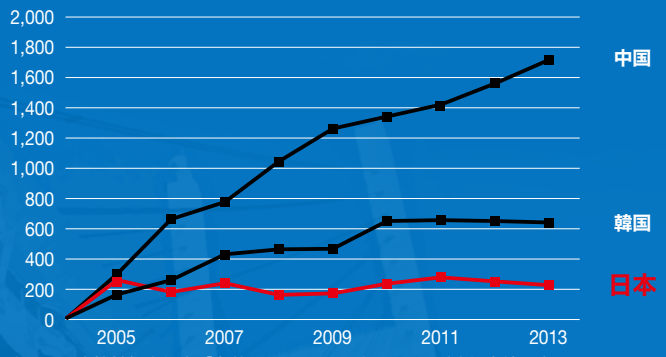
世界中に広がる新興国の急速な都市化や経済発展により、世界のインフラ需要は急伸しています。米国のコンサルティング会社であるマッキンゼーは、2013～30年までに世界がインフラに投資する金額の累計を57兆ドルと試算。産業分野によっては日本国内の需要も頭打ちの状態ですから、関連企業であれば、この膨大な市場を見逃す手はありません。

しかし、各国のインフラ輸出の推移を示した「海外プラント・エンジニアリング成約実績」（右上）のグラフを見ると、日本は05～13年にかけてほぼ横ばいで、年々増加している世界のインフラ需要を取り込めていないことが分かります。国によってこのグラフに反映するインフラの対象が若干異なるため、単純な比較はできませんが、韓国や中国は毎年右肩上がりになっています。

国もこうした状況を打開するべく、13年には内閣官房長官が議長を務める閣僚級の会合「経協インフラ戦略会議」を立ち上げ、インフラ輸出などについて総合的に議論してきました。14年の第4回会議では「インフラシステム輸出戦略」を決定し、その中で20年の受注目標を約30兆円（10年は10兆円受注）に設定。目標を達成するための支援策なども次々に打ち出しています。

公的支援を上手に活用しながら、すでに世界に飛び出している企業も少なくありません。次のページからは、海外で活躍している企業の先進事例を紹介するとともに、現在国が実施している支援体制などについても解説していきます。

海外プラント・エンジニアリング成約実績

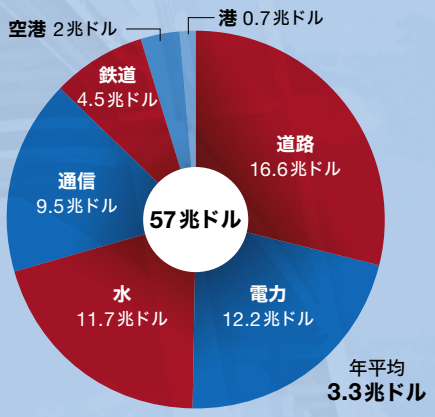


出典：日本機械輸出組合「海外プラントエンジニアリング成約実績調査」

国別の海外プラント・エンジニアリング契約の金額の推移。日本がほぼ横ばいなのに対し、韓国は約4倍、中国は6倍近くに拡大している。

マッキンゼー（2013年）世界のインフラ投資額の累計（2013-30年）

マッキンゼーが試算した2013～30年までに世界が必要とするインフラ投資額の累計。道路や電力、水関連の需要が高いことが分かる。



インフラ

IHI
インフラシステム

トルコのイズミット湾に同国最長の長大吊橋を建設

株式会社IHIインフラシステム 取締役 イズミットプロジェクト部 部長　**川上 剛司さん**

IHIインフラシステム(IIS)は、IHI時代を含めると橋梁事業で約130年の歴史を持っています。そんなIISがこのほど、トルコ共和国のイズミット湾を横断する同国最長の長大吊橋を建設しました。この橋は、トルコ最大の都市イスタンブールと第三の都市イズミルを結ぶ高速道路の一部。全長は2907メートルに及び、1550メートルという中央径間※の長さは世界4位です。経済産業省や国土交通省、外務省などの支援のもと、官民一体となった受注戦略が功を奏しました。

地震大国のトルコでは、日本の耐震技術や品質へのこだわりなどは重宝されましたが、高品質を生み出す日本のとび職人の厳しい働き方を、マイペースなトルコ人スタッフに理解してもらうのは大変でした。ですが、「特殊なのはむしろ日本人の方だ」と考えて粘り強く指導を続けた結果、発注元からは「IISでなければ、この短い工期でこれほど完成度の高い施工はあり得なかっただろう」という言葉をいただき、トルコ道路庁や銀行団などからも高い評価を受けました。

海外事業で大切なのは、治安や経済事情はもちろん、現地スタッフの特性まで、まずは相手国について幅広く知ることです。その上で「短時間で正確かつ美しく」といった日本が誇るこだわり部分を出していく。このこだわりが、世界との競争に勝ち抜くカギになります。

CLICK! ●IHIインフラシステム

※橋の中央部分にある主塔から主塔までの距離

フロントランナーに聞いた！
世界を支えるニッポンの品質

英国の鉄道2幹線に高速鉄道車両を納入

株式会社日立製作所 鉄道ビジネスユニット経営企画本部 本部長付　**尾島 啓文さん**

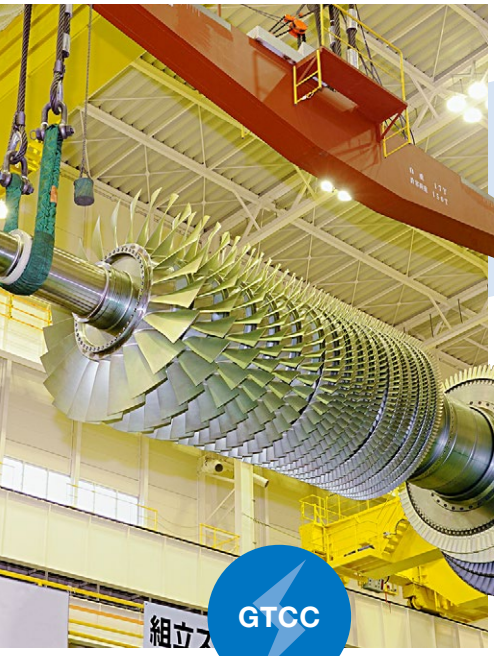
日本トップレベルの鉄道システムサプライヤーである日立製作所ですが、輸出はアジアなどが中心で、欧州への事例は21世紀に入るまでほとんどありませんでした。2009年に英国で初めて納入した高速列車Javelinが、12年のロンドンオリンピック・パラリンピックの主要交通機関として観客や関係者約240万人をトラブルなく輸送。これを機に欧州における日立の評価が高まりました。

そして今回の都市間高速鉄道計画――。国の公的支援を活用して受注したこのプロジェクトには、ロンドンを起点とする2幹線への新車両の納入と、その後の保守契約が含まれています。新車両は、車体が軽量アルミ製であるほか、省エネ技術を駆使した駆動システムを採用するなど環境に配慮。ディーゼルエンジン付き発電機も装備しているため、非電化区間でも走行が可能です。この新車両の製造工場を現地に設け、約730人の雇用を創出する予定にもなっています。

納期や予算を厳守する仕事ぶりなどが現地で高く評価されていますが、そこに至るまでは長い道のりでした。規格や認証が日本に比べて厳格な欧州では、規格に合致していることを立証するために大変な時間と労力を要します。そのような状況下で成功を収めるには、リスクを覚悟した上での長期的な戦術眼が必要です。

CLICK! ●日立製作所

英国鉄道
日立製作所



GTCC

ガスタービン・コンバインド
サイクル発電プラント

三菱日立パワーシステムズ

「おもてなし」で世界NO.1を目指す信頼性の高い火力発電システム

三菱日立パワーシステムズ株式会社 取締役 常務執行役員 営業本部長　**河相 健さん**

三菱日立パワーシステムズ（MHPS）は、2014年に三菱重工業と日立製作所の火力発電システム事業を統合し、同分野で世界No.1プレーヤーになることを目指してスタートしました。これまでに、世界70カ国以上にわたり、約700台のガスタービン、約1200台の蒸気タービンなどの火力発電関連製品を納入しています。海外での火力発電所建設プロジェクトでは、円借款に加え、JBIC様やNEXI様からファイナンス面で支援を頂く場合もあり、最近の事例では、バングラデシュやタンザニアの発電所建設プロジェクト向けに、高効率のガスタービンや蒸気タービンを供給する計画です。

火力発電設備は、他の社会インフラ製品と同様に、高い信頼性が求められます。当社では、製品の研究開発、設計、製造、納入後のサービスを一貫して行うことにより、信頼性の高い発電設備を提供しています。また、自社内に大型ガスタービンの実証発電設備を持つことにより、新製品の信頼性を確保しています。さらに、ICT技術を活用した発電所の保守、運用サービスの提案や、当社製品のユーザー様同士による情報交換会の開催などを通して、顧客密着型の「おもてなし」サービスを提供しています。

CLICK! ●三菱日立パワーシステムズ

事例集でほか先進事例もチェック！

日本のインフラ投資の実例はこのほかにもたくさんあります。それらを「エネルギー」「鉄道」「水」などの分野ごとにまとめた「質の高いインフラ投資」事例集がこのほど発表されました。このページで紹介する4つの事例と合わせ、こちらもぜひ参考にしてください。

CLICK! ●「質の高いインフラ投資」事例集

フィリピンのマニラで下水処理場を建設中

JFEエンジニアリング株式会社 アクアソリューション本部 海外事業部 営業部　**黒岩 綾子さん**

JFEエンジニアリングでは、環境、エネルギー、橋梁など、さまざまな分野のインフラ案件を世界各地で手がけています。フィリピンのマニラを中心としたエリアでは、特に上下水分野に注力しており、現在も約30万人分の下水を処理するプラントを建設中です。この施設で29件目となります。

当社は、日本の下水処理場で最も多く採用されている標準活性汚泥法をベースに、現地の気候や地形に合わせて省エネ・省スペースを追求した独自の浄化プロセスを確立。加えて運転費用や維持管理費などのライフサイクルコストを意識した提案により、競争力を高めています。

とはいえ、海外での工事は簡単ではありません。営業として特に気をつけたいのは契約約款の取り決め。国によって法律や基準、慣例なども異なりますから、契約までにあらゆるリスクを分析し、譲れない条件に関しては粘り強く交渉しなければなりません。

また、海外でのプロジェクトを成功に導くためには、優秀な現地スタッフを獲得し、その能力を最大限引き出すことが不可欠です。権限委譲などでスタッフのモチベーションを向上させることはもちろんですが、まずは継続的に案件を受注すること。そうしてスタッフを長期的な視野で育成することが大切になります。

CLICK! ●JFEエンジニアリング

フィリピン
下水処理
施設

JFE
エンジニアリング

国も全力支援！

ニッポンが誇る充実のサポート体制

14ページでも触れましたが、日本のインフラ輸出の拡大に向け、国は2013年3月に「経協インフラ戦略会議」を設置しました。この会議は、議長を務める内閣官房長官を筆頭に、副総理兼財務大臣、総務大臣、外務大臣、経済産業大臣、国土交通大臣、経済再生担当大臣のほか、適宜必要な関係大臣が出席する会合です。設立から今年8月までに26回開催され、今後のインフラ輸出拡大の方向性を示した「インフラシステム輸出戦略」や、支援制度を抜本的に改善・拡充し、総理より発表した「質の高いインフラパートナーシップ」「質の高いインフラ輸出拡大イニシアティブ」などを次々にとりまとめています。

支援制度には、「リスクマネー」「制度改革」「人材育成」という大きく分けて3つの観点があります。リスクマネーに関しては、世界全体のインフラ案件に対して今後5年間で総額2000億ドルを供給することを決めました。制度面では、円借款の手続きを迅速化するとともに、新興国からのニーズが高いドル建て借款などを新たに創設。また、企業への投融資を行う関係機関の機能強化を行うなど、さまざまな改革を進めています。

人材育成に関しては、入札における決め手がスピードや価格になりがちな開発途上国の政府関係者に対して、質の高いインフラのメリットを説明。ライフサイクルコストや安全性、リスクに対する強じん性といった観点への理解を促進します。そのほか現地企業の生産能力をアップさせる体制を整えるとともに、実務を担当する現地スタッフの育成も支援します。

インフラ輸出を検討しているなら、これらの優遇措置を使わない手はありません。あなたの企業に必要な支援は何か――。以下にそれぞれの要点をまとめました。

伊勢志摩サミットでもG7がインフラに言及！

5月にはここ日本で「G7伊勢志摩サミット」が開かれました。世界経済や政治問題などを協議するこの首脳会談の場でも“質の高いインフラ投資”は議題として取り上げられ、首脳宣言における主要経済アジェンダの1つとなったほか、「質の高いインフラ投資の推進のためのG7伊勢志摩原則」という成果文書としても示されました。

伊勢志摩原則では、質の高いインフラとしてのポイントを5つ挙げています。1つ目は、プロジェクト全期間を通じて効果的なガバナンスが形成された上で、ライフサイクルコストから見た経済性、リスクに対する強じん性などが確保されていること。2つ目は現地での雇用創出。3つ目は社会・環境面への配慮。4つ目は国家や地域の開発戦略との整合性の確保で、最後5つ目は官民連携を通じた効果的な資金動員の促進です。

こうしたポイントを押さえたインフラ投資が、世界の持続的な成長にとって重要と各国首脳が認めました。世界的なインフラの需給ギャップによって、ぜい弱性を有するインフラが広がることを懸念しているのです。今後G7以外の国や国際開発金融機関などに対しても、この原則に沿ったインフラ投資を働きかけていくとしています。

このように、日本が得意とする質の高いインフラが求められる土壌は、世界に着々と広がりつつあるといえます。

経協インフラ戦略会議が決定した重要施策

リスクマネー

5年で2000億ドル！エリアや対象も拡大

JICA（国際協力機構）、JBIC（国際協力銀行）、NEXI（日本貿易保険）、JOIN（海外交通・都市開発事業支援機構）、JICT（海外通信・放送・郵便事業支援事業）、JOGMEC（石油天然ガス・金属鉱物資源機構）という関係機関を通じ、今後5年間で総額約2000億ドルを供給。利用できるエリアはアジアから全世界に、対象は資源エネルギーなどを含む広義のインフラ案件にそれぞれ拡大しています。

制度改革

大幅な機能強化で支援内容が充実

これまで5年ほどかかっていた円借款の手続きを最短1年半に短縮。ドル建て借款、金利が優遇されるハイスペック借款などを創設しました。また、NEXIの投資保険期間の上限を15年から30年に引き延ばすとともに、融資保険、投資保険、短期輸出保険に関しては、相手国の政治・経済・社会変化などに伴うカントリーリスクのカバー率をすべて100％にまで拡大しています。

人材育成

発注者と労働者双方を育成支援

インフラを発注する開発途上国の政府関係者などを日本に招聘。日本の強みでもある質の高いインフラに対しての理解を深めてもらうとともに、国家や地域における経済的・総合的政策立案能力と、経営面でのメリット理解促進による評価能力の向上をサポートします。また、プロジェクトの設計や運営、保守といった現地での幅広い実務に携わるスタッフの育成も支援していきます。

CLICK! ●質の高いインフラパートナーシップ
CLICK! ●質の高いインフラパートナーシップのフォローアップ
CLICK! ●質の高いインフラ輸出拡大イニシアティブ

貿易経済協力局 通商金融・経済協力課 戦略輸出室
（左から）大山一成さん　佐飛昴さん　岡林俊起さん
棚橋忠司さん　村瀬洋行さん
戦略輸出室は、経済産業省におけるインフラ輸出の司令塔として、関係省庁・機関と連携し、各種支援ツールを活用して日本のインフラ輸出を促進しています。

経済産業省｜担当者の声

世界規模のインフラ争奪戦で勝ち抜くために

政府は今、インフラ輸出にかつてないほど注力しています。それはこの1年間の取組でも明確です。2015年5月から2016年5月にかけて、安倍総理大臣は、計3回ものインフラ輸出促進に関する新たな取組を発表。政府関係機関が率先して、今後5年間で2,000億ドルものリスクマネーを供給することや、ドル建ての借款創設や、サブ・ソブリン（地方公共団体等）向けの新たな円借款の創設など、円借款を創設した1958年以来の大改革を行いました。

また、総理大臣・関係閣僚らによる海外への“インフラの売り込み”も活発に行っています。2013年～2015年の3年間だけでも350件 を超えるトップセールスを行いました。特に、昨年末には、インドにおいて、日本の新幹線方式の採用に合意しました。これは、日本の新幹線輸出に大きな弾みとなりました。また、インドネシアのタンジュンプリオク港の拡張工事に係る林大臣（当時）のトップセールスに、実際に私も同行しました。現在、同案件は、最終合意に向けた調整段階にあります。

世界のインフラ受注競争は今後更に激化していくことが想定されますが、日本の質の高いインフラの輸出拡大のため、オールジャパンでの取組を一層強力に進めていきたいと思います！（岡林）

変化が望まれる株主総会プロセス

企業と株主・投資家との対話促進に向けて

経済産業省では、中長期的な企業価値創造による経済の好循環を実現すべく、
企業と株主・投資家が建設的な対話が行える環境を整備することを目的として、
株主総会プロセスの電子化について検討を行っています。

企業と株主・投資家との対話は重要

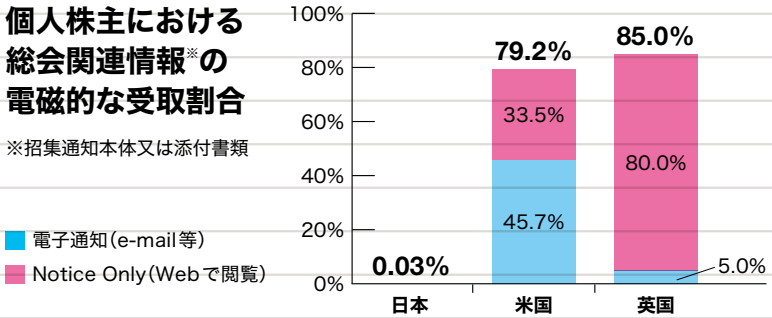
第４次産業革命を見据え、未来に向けた投資を増やしていくには、企業による果敢な経営判断に加え、成長資金を拠出する投資家の存在も重要です。そして、企業による成長の果実がリターンとして投資家に還元されることは、実は、国民一人一人の資産形成にとっても重要です。というのも、皆さんの年金積立金は、運用会社などのプロの投資家により、国内外の株式などに投資されているからです。

投資家が企業と対話を行い、中長期的な企業価値の向上を促すことで、持続的なリターンを確保し、広く国民に還元していく。そうした好循環を実現すべく、経済産業省は、企業と株主・投資家が共に持続的な成長を目指して対話を行える環境整備に向け、検討を重ねてきています。例えば、株主総会における議決権行使は、株主たる投資家が投資先企業の経営に適切に関与していく上で重要です。しかし、日本では、株主総会の議案を検討できる期間が実質３日等と極めて短いなど、諸外国と比べて非効率であると指摘されています。

これを解決する手段の一つが「電子化」です。

1 個人株主における総会関連情報※の電磁的な受取割合

※招集通知本体又は添付書類



出典：日本／「旬刊商事法務　株主総会白書2015年版」(商事法務研究会、2015.12/1臨時増刊号)のデータを元に試算
米国／「“Analysis of Distribution and Voting Trends Fiscal year Ending June 30,2015”,Broadridge」
英国／Prism Cosec社(www.prismcosec.com)発行の“Prism Briefing”2015年8月12日付を参照

日本では電子化が進んでいない

今日、国際的には、株主総会プロセスの電子化が進んでおり、米国や英国では、招集通知等の受取も、議決権行使も、それぞれ70～90％程度が電子的に行われています。しかし、日本では未だに株主への招集通知等の提供は紙媒体での送付が原則となっており、招集通知等の受取は1％未満（→**1**）、議決権行使は10％程度しか電子化されていません（→**2**）。

紙媒体では印刷、封入、郵送などに時間がかかるため、株主が議案情報を受け取るタイミングは遅くなってしまいます。さらに、議決権行使も書面が主流となると、集計作業等に要する時間の分だけ議案への賛否について考える期間は短くなってしまいます。

2 議決権の電子行使の状況（議決権個数ベース）

米国（2013年）		機関投資家……98％　個人株主……73％ （個人：郵送による投票率は20％、電話による投票率は7％）
英国		機関投資家……9割以上
ドイツ		機関投資家……7割以上
日本（2015年）		機関投資家＋個人株主……10.9％ （ICJ経由の電子行使率は議決権行使個数全体の9.4％）

出典：米国／Broadridge+PwC,“Proxy Pluse,first edition 2014”
英国・ドイツ／英Makinson Cowell社、独VIP社に対するヒアリング等からあずさ監査法人が作成
日本／全国株懇連合会「株主総会等に関する実態調査集計表」（平成27年10月）から作成

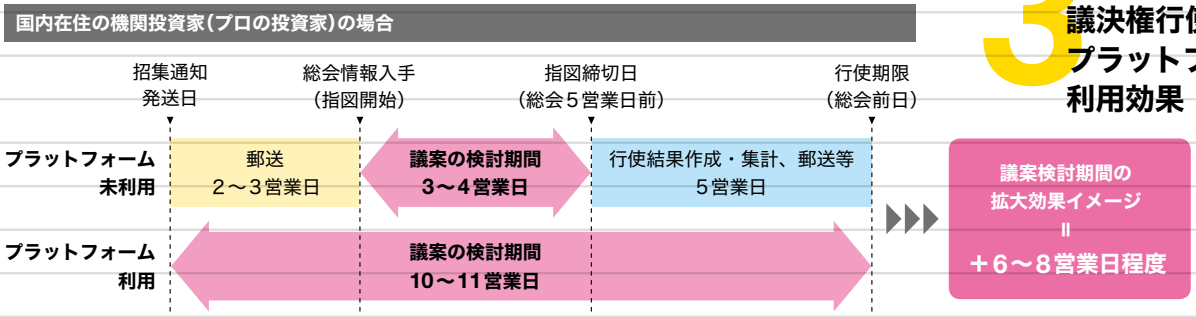
※機関投資家とは、顧客から拠出された大量の資金を使って株式や債券で運用を行う「プロの投資家」のこと。

一方で、変化の兆しも

そのような中、ここ最近、招集通知等を発送する前の段階でウェブサイト等に開示するという自主的な取組みが上場会社の約7割に普及しており、注目されます。しかし、発送する1日前にウェブ開示する企業が多いのも現状です。

また、日本でも、電子的に招集通知の受取や議決権行使ができるプラットフォームが運営されており、このプラットフォームに参加する上場会社も近年増加しています。これを投資家が利用すると議案の検討期間は約1～2週間拡大（→**3**）しますが、事務の複線化などを理由として、十分使われるには至っていません。

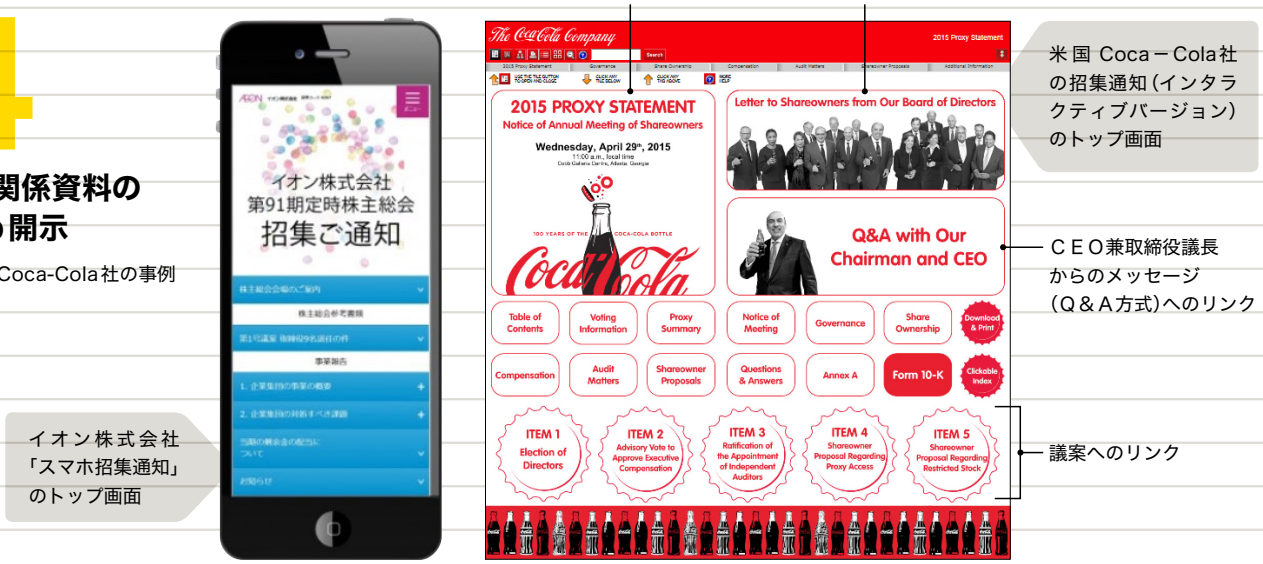
3 議決権行使電子プラットフォームの利用効果



4

総会関係資料のWeb開示

イオン、Coca-Cola社の事例



電子化するとこんなにたくさんのメリットが！

株主総会プロセスの電子化には、投資家が責任を持って議決権行使を行う上で必要となる時間的余裕を確保できるといった効果以外にもメリットがあります。

最近の株主総会では、例えば米国のコカコーラのように招集通知のビジュアルを魅力的にして情報を見つけやすい形で提供したり、イオンのように招集通知の閲覧や議決権行使をスマートフォンで行えるようにしたりなどの工夫が見受けられます（→4）。ウェブ上で情報が提供されれば、株主は、紙に印刷された分厚い書類を読むよりも情報を検索し易くなります。経営陣や役員候補者からのメッセージ動画が提供されれば、会社をより身近に感じることもできるでしょう。

また、ウェブであれば、会社側も、反対の多い議案についてタイムリーに情報発信を行うことで、議案に理解を求めやすくなります。このように、紙の世界からの解放は、情報提供やコミュニケーションの充実効果をもたらすと期待されます。加えて、環境負荷軽減効果もあります。

そこで、本年４月に公表された「株主総会プロセスの電子化促進等に関する研究会」の報告書は、電子化による対話充実効果が広く行き渡るよう、招集通知等に関して、個別に株主の承諾を得ることなく、ウェブ上で提供できる情報の範囲を拡大し原則電子提供とする「新たな電子提供制度」の創設を提言しています。また、招集通知の受取から議決権行使を一括して行える情報プラットフォームの利用環境の整備に向け、関係者が検討を進めることも提言しています。

「新たな電子提供制度」の創設〜招集通知に添付される書類の原則電子化

「新たな電子提供制度」のイメージは、株主総会の日時等が記載された招集通知本体は書面で届く一方で、事業内容や財務諸表などが記載された添付書類はウェブで閲覧するというものです。添付書類を「紙でみたい」という場合は、自ら印刷するか、企業側に書面で提供するよう要請することが必要になります。

株主からの書面請求への対応は、今後の制度設計上の論点の１つです。書面請求に応じる義務を法令上規定すべきとの指摘がある一方で、約4割の企業実務担当者がデジタルデバイド問題を電子化の課題（→**5**）と捉えており、そもそも会社には株主との良好な関係を構築したいというインセンティブがあることも踏まえると、自主対応に委ねてもよいという見解もあります。書面請求への対応が義務化されると、法的リスクや事務コストの観点から、これまでどおり書面で一括送付することとなり、電子化による株主全体の効用が得がたくなるのではないか、例えばコーポレートガバナンス・コードのようなソフトローで対応を求めるのも一案ではないか、との指摘もあります。

いずれにせよ、インターネット利用の更なる普及など、今後の環境変化に応じて電子提供を行う範囲や手続きを柔軟に変えていけるよう、企業に選択肢を与える方向で制度を整備していくことが重要です。

対話先進国の実現に向けて

株主総会プロセスの電子化は、政府の成長戦略の最重要課題であるコーポレートガバナンス改革の鍵となる施策としても位置づけられています。

昨今、対話促進に向けた取り組みは徐々に進展しつつあります。しかし、日本の関係者に長年の慣習が根強く残っていることも事実です。事業活動や資金調達のグローバル化が進み、海外投資家による日本株の保有割合も増加している中、国際的な潮流も無視できません。長年培かわれてきた実務や慣行を変えるには時間も労力もかかりますが、株主総会プロセスの電子化を契機として、国際的にも遜色ない「対話先進国」たる環境が構築されるよう、経済産業省としても引き続き取り組んでいきます。

CLICK! ●株主総会プロセスの電子化促進等に関する研究会

5 招集通知添付書類の提供の原則電子化について、実務面で考えられる課題

複数回答。自由記載欄の内容を事務局で分類したもの。

回答	件数	割合
書面請求対応等に関する管理コストの問題	117	41.5%
高齢者などのデジタルデバイド問題	116	41.1%
議決権行使率の低下	18	6.4%
電子化を選択制とすることの課題（義務化すべき）	14	5.0%
⋮		
全体	282	100.0%

出典：経済産業省・東京株式懇話会「招集通知のWEB開示等に関するアンケート調査」（平成27年11月実施）

あいうえお
かきくけこ
さしすせそ
たちつてと
なにぬねの
はひふへほ
まみむめも
やゆ　よ
らりるれろ
わ　　を
ん

いまを読み解く

今号の 経済キーワード

from METIPEDIA CLICK!

経協インフラ戦略会議

【けいきょう・いんふら・せんりゃく・かいぎ】

我が国企業によるインフラ・システムの海外展開等を支援するとともに、我が国の海外経済協力に関する重要事項を議論し、戦略的かつ効率的な実施を図るために開催している会合（議長：内閣官房長官、構成員：経済産業大臣を始めとする関係閣僚）。「インフラ輸出戦略」をとりまとめている他、2016年5月には「質の高いインフラ輸出拡大イニシアティブ」を決定した。

CSIRT

【しーさーと】

Computer Security Incident Response Team。情報漏えいや不正アクセスなどのセキュリティ上の問題が発生したことを検知又は報告を受けた際に、原因分析、影響範囲調査、再発防止策などの解決に向けた対応及び調整を行う組織。

Stuxnet

【すたっくすねっと】

2010年にイランのウラン濃縮工場の制御システムに感染した不正なソフトウェア（いわゆるマルウェア）。2000年当初は攻撃者が不特定のサイトを狙う事例が大半だったが、これを機に、インフラやプラントの制御システムを狙った攻撃への対応が課題として浮上した。

経済産業省
Ministry of Economy, Trade and Industry

経済産業ジャーナル 2016年10・11月号

発行人／経済産業省
〒100-8901 東京都千代田区霞が関1丁目3番1号
http://www.meti.go.jp/

アンケートに回答する　メールマガジンに登録する　バックナンバー