BSA The Software Alliance

ソフトウェアライセンスの不備が誘発するリスクと対策

目次

はじめに

企業がビジネスを進めるうえで、コンプライアンスの重要性が増しています。コンプライアンスは、法令を順守し、企業倫理、社会常識を守りながら、企業の社会的責任を果たしていくことです。コンプライアンスを徹底し、リスクを適切に管理することは、健全で効率的な企業経営の実現につながります。コンプライアンスの結果として、企業価値が高められる時代になったと言ってよいでしょう。

これはソフトウェアライセンスについても共通することです。ソフトウェアのライセンスコンプライアンスとは、ライセンスを適切に管理することで、社内や取引先の知的財産権の侵害を防ごうという取り組みのことです。ソフトウェアは目に見えず、同じものを簡単にコピーすることができます。そうした特性もあってか、ソフトウェアのライセンスは、しばしばないがしろにされがちです。

ソフトウェアのライセンスをないがしろにすればどうなるでしょうか。適切なライセンス管理を怠れば、企業価値の低下を招きます。さらに、社内で不正コピーを当たり前のように使っていると、従業員のモラルや責任感も低下します。実際、私が受ける相談のなかには「社内で不正コピーが使われていることに不満を感じている」という声も多くあります。こうした声に経営者が耳を貸さなかった結果、人材が流出するケースも少なくありません。

もろちん、ライセンスが管理されていない状況を放置することは、損害賠償や刑事罰の対象になります。BSAの情報提供窓口に寄せられた不正コピー情報を端緒として、4億円を超える損害賠償を支払わざるを得なかったケースも実際に出ています。こうしたさまざまなリスクを回避するためにも、いまこそ適切なソフトウェアライセンス管理が必要です。

大切なことは、管理不在は大きなリスクであり、その責任は経営者個人にも求められるということです。経営層がこれを十分に理解して、自分の意識を変えていく必要があります。本ハンドブックでは、ソフトウェアライセンスとは何か、経営に対してどんな影響があるのか、適切に管理するための基本は何かをまとめました。ソフトウェアのライセンスコンプライアンスを知り、企業価値を高める手立てとしてください。

BSA | ザ・ソフトウェア・アライアンス日本担当顧問
TMI総合法律事務所　パートナー
弁護士　石原　修

ソフトウェアライセンスとは何か?

ソフトウェアは、PCやプリンタなどのハードウェアと違って、目に見えない無形資産ですが、コンピュータプログラムとして、著作権で保護されています。ソフトウェアを利用する場合、著作権で保護されているのだということを意識することが大切です。モノとソフトウェアを買う場合をそれぞれ考えてみましょう。

モノを買う場合、たいていは店舗などで商品を買って、自宅や会社などに運び、壊れるまで使い続けます。モノの所有権は、購入者に移ります。捨てたり譲ったりすることも所有者が決めることができます。まさに、"自分のもの"となるわけです。

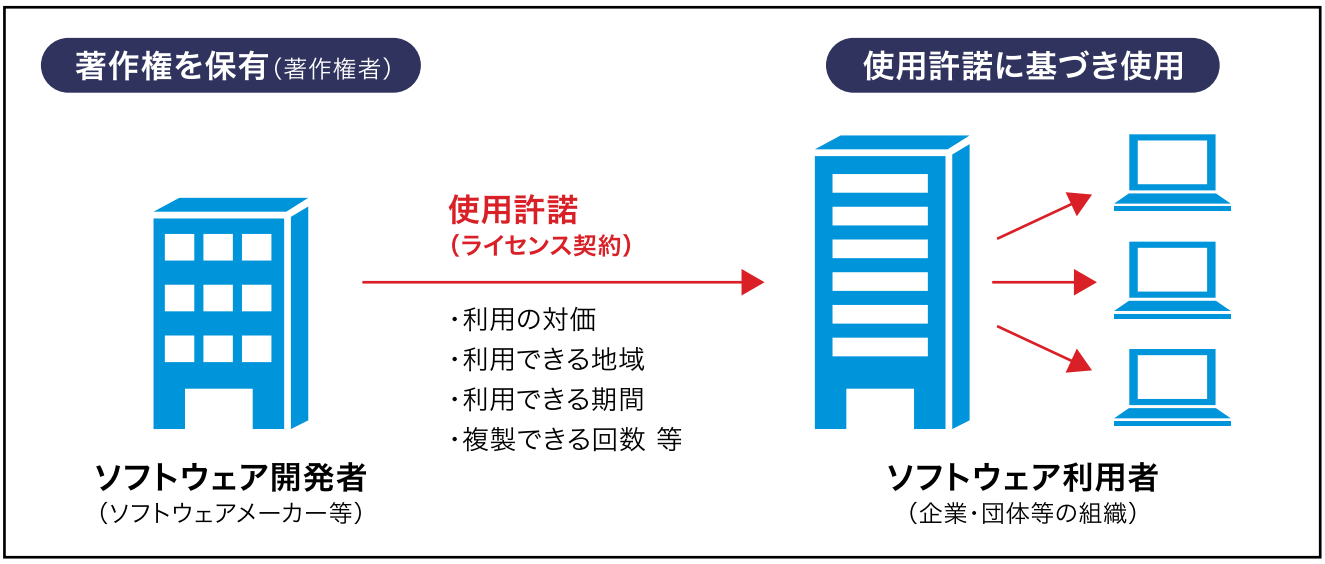
一方、ソフトウェアを買う場合、所有権に相当する著作権が購入者に移ることはありません。ソフトウェアを使うためには、著作権を保有する人(著作権者)から使ってもよいという許諾を得る必要があります。ソフトウェアを買うことは、モノを買うのでなく、この「使ってもよいという許諾」を買うということです。ソフトウェアの著作権は"自分のもの"にはならず、著作権者からの許諾のもとに、ソフトウェアを使用する権利を取得するという契約になるのです。【図1－1】

このように、著作権を保有するメーカーなどからソフトウェアを利用しても良いという許諾を受けることをソフトウェアライセンスと呼びます。ソフトウェアライセンスでは、ソフトウェアの利用範囲を「使用許諾契約書」などに明示します。たとえば、インストール可能な台数や使い方、試用期間の制限などです。これらの内容は、メーカー、製品種別、購入形態(パッケージ、ダウンロード、ライセンスプログラム)などにより異なるのが普通です。ソフトウェアを使い続けるということは、著作権者の使用許諾に従ったソフトウェアライセンスを守るということにほかなりません。

では、ソフトウェアライセンスを守らなかったらどうなるでしょうか。たとえば、使用許諾契約書に明示されたインストール可能な台数を超えてインストールしたとします。この場合、不正コピー、すなわち複製権という著作権の1つを侵害したことになるのです。

こうした不正コピーは、ビジネスを進めるうえでも大きなリスクです。どんなリスクがあるのかを【図1－2】にまとめました。一次的には、不正コピー

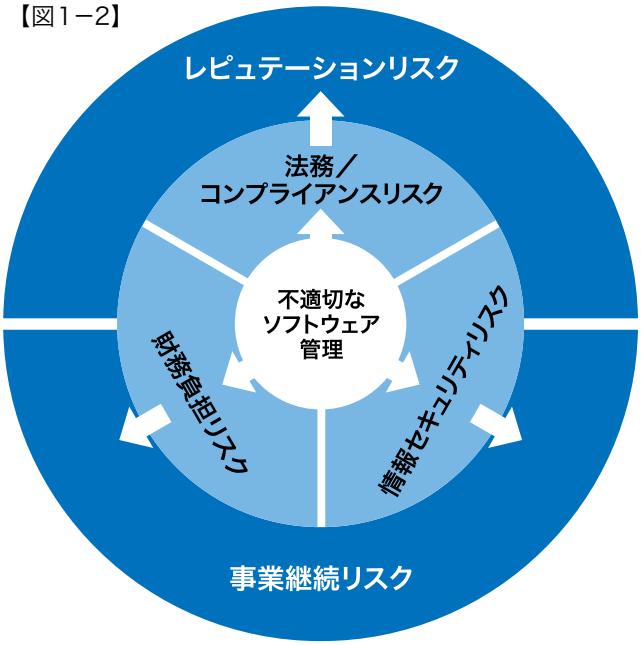
【図1－1】



発覚時の賠償請求や刑事罰といった法務／コンプライアンスリスク、ウイルス感染や個人情報漏洩といった情報セキュリティリスク、取締役や監査役自身が負う個人責任リスクがあります。さらに、二次リスクとして、いわゆる風評被害などのレピュテーションリスク、顧客離れや取引停止といった事業継続リスクがあります。こうして見ると、範囲が広範で連鎖的に起こることがわかります。

ポイントは、こうしたリスクは、ソフトウェア管理を漫然と放置した場合に起こるという点です。では、次に、この点を詳しく見ていくことにしましょう。

【図1−2】



弁護士メモ

「買ったのだから自由に使ってもよい」は大きな誤解!

ソフトウェアに関してよくある誤解は「お金を出して買ったのだから、あとは自由に使ってよい」というものです。実際には、ソフトウェアは著作物であり、音楽や映画のCD/DVDと同じように、著作権で保護されています。たとえば、DVDを許可なくダビングすれば違法になるように、ソフトウェアを許可なくコピーやインストールすれば違法になります。コピーやインストールといった複製は著作権者だけができる行為で、複製する場合は著作権者の許諾（ライセンス）が必要です。ソフトウェアは、「自由に使ってよい」のではなく「著作権者の許諾の範囲内で使う」ものなのです。

よくある誤解として「正規品を購入すれば不正は起きない」というものもあります。ここでポイントになるのは、複数のPCにソフトウェアをインストールする行為は複製にあたるということです。「1回しかインストールできない」というライセンスに反して、複数のPCにインストール（複製）すれば、著作権の侵害です。正規品であっても、使用制限を超えてインストールすれば違法になるということです。

また、不正コピーは、実際に行為を行った人だけの問題ではないという点も見過ごされがちです。経営者は、ソフトウェアを適切に管理する責任があります。管理を社員任せにするなど、漫然と放置していれば、通常の過失で会社に対する個人責任を、重過失があればソフトウェアメーカーに対する個人責任も問われます。社内で不正コピーが行われていないかを管理することは、経営者自らが積極的に関与・推進すべき課題なのです。

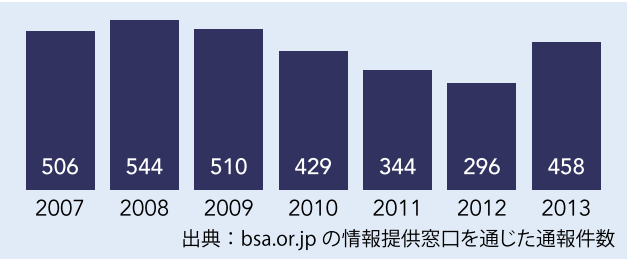
不十分なライセンス管理に潜むリスクと

ソフトウェアライセンスの管理は、コンプライアンスという目的だけでなく、さまざまなビジネスリスクの回避につながります。では、ソフトウェア管理を漫然と放置した場合、どのようなリスクを被るのでしょうか。また、代償としてどのくらいの金額を支払うことになるのでしょうか。3、4ページで見たリスクのなかから、不正コピー発覚時の損害賠償請求や刑事罰のケースについて、詳しく見ていきましょう。

不正コピーが発覚するきっかけは、そのほとんどが通報窓口への通報です。コンプライアンスに対する意識が高まるなか、不正コピーに敏感な従業員が増えています。従業員は、健全な職場で働きたいという願いから、社内で行われている不正コピーの実態を告発します。実際、【図2－1】のように、BSAへの情報提供件数はここ数年でも平均400件ほどで推移しています。また、BSAが期間限定で行った、不正コピー解決につながる有力情報に対し最大100万円の報奨金を提供する「報奨金プログラム」には大きな反響が寄せられました。ソフトウェアライセンス管理は、重要な経営課題の1つなのです。

不正コピーの事例として、刑事罰を受けるケース、民事で損害賠償をしたケース、民事で和解したケースの3つを紹介します。

【図2−1】
日本における組織内不正コピーの通報件数推移



出典：bsa.or.jp の情報提供窓口を通じた通報件数

法務リスク 1　刑事罰：著作権侵害の最高量刑

著作権侵害の刑事罰は、行為者に対して10年以下の懲役、1,000万円以下の罰金、またはその両方が課せられます。そして、企業/自治体などの社員・職員が、業務で著作権を侵害した場合は、その法人に3億円以下の罰金が課せられます。窃盗（万引き）の場合は、行為者のみが10年以下の懲役または50万円以下の罰金で、法人罰はありませんから、いかに重い罪であるかが、おわかりいただけるでしょう。

著作権侵害の刑事罰（最高量刑）

行為者	組織（企業や団体等）
懲役10年以下 罰金1,000万円以下 または両方（併科可）	罰金3億円以下

法務リスク 2　民事事案：訴訟による損害賠償

民事訴訟例としては、これまでに大きな2つの判例があります。1つは、ある司法試験予備校のケースで、損害賠償額は約8500万円（東京地方裁判所2001年5月判決）。もう1つは、コンピュータスクールのケースで、損害賠償額は約4000万円（大阪地方裁判所2003年10月判決）。いずれも、ビジネスソフトを不正コピーしており、著作権侵害による損害賠償です。

民事訴訟例（損害賠償）

判例 1	判例 2
司法試験予備校事件 約8,500万円 東京地方裁判所 2001（H13）年5月16日判決	コンピュータスクール事件 約4,000万円 大阪地方裁判所 2003（H15）年10月23日判決

法務リスク 3　民事事案：和解による損害賠償

民事で和解による損害賠償のケースも増えています。これらは決して大企業だけの問題ではありません。例えば従業員500名以下の損害賠償金額（種別）のトップ5は、約4億4,000万円（ソフトウェア開発）、約1億4,000万円（金融）、約1億4,000万円（製造）、約1億円（デザイン）、約1億円（情報・通信）といずれも1億円を超える高額です。こうした数字を見るだけでも、不正コピーの代償が財務的な負担となり、企業経営を大きく圧迫することがわかります。

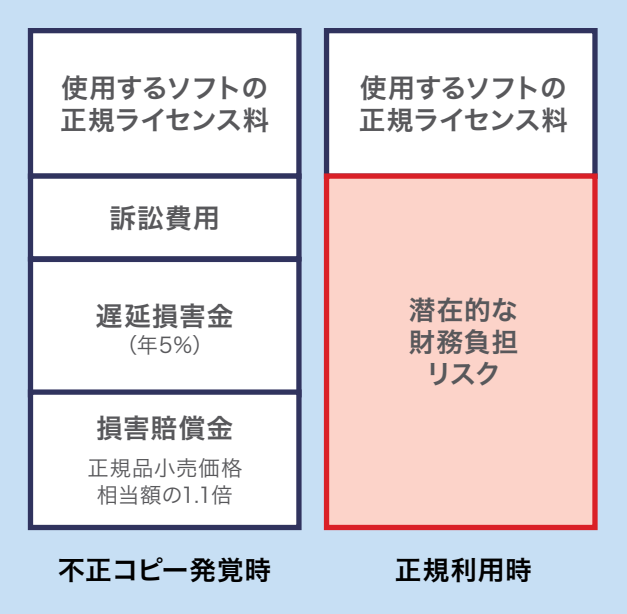
従業員数 500 名以下の企業における不正コピーでの損害賠償額 TOP 5

	損害賠償額	業種
1	約4億4,000万円	ソフトウェア開発
2	約1億4,000万円	金融
3	約1億2,000万円	製造
4	約1億円	デザイン
5	約1億円	情報・通信

その代償

ここで注意すべきなのは、損害賠償額は、ソフトウェアを正規に購入し利用する場合の支出よりも高くなるということです。正規利用時は、当然のことながら、使用するソフトの正規ライセンス費用しかかかりません。一方、不正コピーの利用が発覚した時は、それに加えて、損害賠償金と遅延損害金が加わります。損害賠償金は、正規品小売価格相当額（実際の購入額ではない）の1.1倍で、遅延損害金はインストール時から年5%です【図2−2】。しかも、損害賠償を支払ったら不正コピーが利用出来るようになるわけでなく、全て削除（アンインストール）する義務を負いますので、新たに正規に購入する必要があります。このように、不正コピーには、潜在的な財務負担が伴うのです。

【図2−2】**損害賠償金額の算出**



弁護士メモ

安易なアンインストールは証拠隠滅罪の可能性も

ご紹介した2つの事件は、いずれも民事訴訟の前に証拠保全の手続を行っています。裁判所が著作権者の申立に対し証拠保全の決定をすると、裁判官が、当該組織に行き、各ＰＣにインストールされているソフトウェアの種類や数、ライセンス証書の有無などについて証拠保全手続きを実施します。この手続で明らかとなる不正コピー数などが裁判で重要な証拠となります。その際に、実際に検証していないPCについても侵害行為があったと推認すること（司法試験予備校事件）や、痕跡がなくても使用状況から不正コピーがあったと推察すること（コンピュータスクール事件）があります。たとえば、前者の例では、検証した83台に不正コピーがあったため、同じスクール内に存在するが時間が足りず検証出来なかった136台のPCについても同じ量の不正コピーがあると推認しました。証拠保全手続きは限られた時間で行われるため、検証できなかったPCについても認めてもらう必要があるのです。

コンピュータスクール事件では、「従業員の不正コピーを漫然と放置したこと」「不正コピーの防止に関する管理体制が不備であったこと」の2点を重過失として認定し、代表取締役の個人責任も認めています。社内における不正コピー防止のための体制不備を漫然と放置した代表者の責任が認定された初めての判決です。

社内監査などにより社内で不正コピーを見つけたときの留意点としては、安易にアンインストール（削除）しないことが挙げられます。不正コピーがＰＣにインストールされている状態は、著作権侵害被疑事件の重要な証拠ですので、アンインストールすると証拠隠滅罪に該当する可能性があります（刑法第104条）。不正コピーが発見されたら、すぐにソフトウェアメーカーに相談することが適切な対応です。

適切なライセンス管理と、予防・改善策

ソフトウェアを利用するうえでは、ライセンス管理を適切に行うことが重要です。では、適正なライセンス管理とはどういうことでしょうか。まずは、社内に存する全てのコンピュータに番号を振り把握することが求められます。これは、企業のセキュリティ管理や、IT資産管理、財務データの信頼性、情報セキュリティの適切な運用などの前提にもなるものです。ライセンス管理だけでなく、社内のIT資産を棚卸して、経営を可視化するといった視点からも重要な手続きであると言えます。

実際のライセンス管理の手順きは、全てのコンピュータを把握した上で、以下のようになります。

1. インストール調査

「ソフトウェア管理台帳」を整備し、
企業内のすべてのパソコンに
インストールされているソフトウェアの
種類と数を全部把握する

2. 保有ライセンス調査

ソフトウェアライセンスの最新の保有状況を
記録する「保有ライセンス管理台帳」を整備し、
企業で保有するすべての
ソフトウェアライセンスを把握する

3. 差分把握

「ソフトウェア管理台帳」と
「保有ライセンス管理台帳」を突合させ、
すべてのインストール数と
保有ライセンス数の差分を把握する

4. ライセンスの適正化

ライセンス不足が生じていた場合は、
当該ソフトウェアベンダーに相談するなどし、
適正化を行う。

としてのソフトウェア資産管理

ライセンス管理を行ううえでは、ソフトウェア資産管理（Software Asset Management: SAM）という考え方を踏まえておくことが大切です。ソフトウェア資産管理では、ライセンス管理に加えて、以下のような取り組みを進めます。

- **管理方針・規定の整備**
- **管理体制の整備**
- **定期的な棚卸しをともなう管理台帳の更新**
- **第三者による定期的な外部監査**

これらを行うことで、ライセンス不足の予防や再発防止につながるのです。

弁護士メモ

ライセンス管理に欠かせないのは経営者のコミットメント

実際に社内でどんなソフトウェアが使われているのか。これを把握するのはかなり大変な作業です。IT部門であっても、即座に答えられないことが多いのではないでしょうか。システムの規模が大きかったり、部門ごとにIT予算を持っている場合などはなおさらです。IT部門が社内の状況を把握しきれなくなるのです。そこでカギになるのが経営者のコミットメントです。IT部門やシステム担当者だけでインストール調査を進めれば、部門の壁や非協力的な社員によって調査を阻まれることが考えられます。これを避けるには調査を阻止させないだけの力強い後ろ盾が必要です。一方で、IT資産の棚卸しにより潜在リスクが可視化されます。時には経営陣による経営判断が必要な深刻なリスクが発見される可能性もあります。こうしたことからも、まずは、経営者自らが意識を改革し、ライセンス管理にコミットすること。そして、その決意を管理者や担当者だけでなく全社員に示せば、社内全体に“ライセンス管理に協力すべきだ”という気運が高まります。これは強力な推進力になります。

また、単にライセンス管理のための体制を作ればよいというわけではありません。定期的な外部監査を含めた、PDCAサイクルをまわすことが重要です。

さらに、近年では、サプライチェーンの不正にも注意を払う必要がでてきました。たとえば、多くの企業でコンプライアンスの一環として「CSR調達」のガイドラインを設けるようになりました(たとえばJEITA『サプライチェーンCSR推進ガイドブック』参照)。ライセンスについて、納入先のコンプライス条件に抵触していないかを確認する必要があります。たとえば、外注先が不正コピーを使って制作物を納品していないかといったケースです。また、世界各国の政府は、不正コピー使用により世界貿易で不公正な優位性を確保することに懸念を抱いています。不正コピーを使うことで不公正な競争をうながし、ペナルティが課せられることもあります。現地法人での不正コピーの調査なども必要です。

まとめ

最後に、“漫然と放置”しないための「5つのポイント」と「5つの誤解・落とし穴」を紹介します。
自社の取り組みの状況にあわせて、利用してください。

5つのポイント

ポイント① 経営層が自ら意識を改革すること

ポイント② 基本台帳（管理台帳）が存在すること

ポイント③ （定期的な棚卸に基づき）台帳の情報を更新するルールが存在すること

ポイント④ ルールが遵守されていることが検証されていること（第三者の監査の活用等）

ポイント⑤ 「不一致」が見つかった場合に適法な手段により是正されること

5つの誤解・落とし穴

誤解・落とし穴 1　管理者がいるから大丈夫？

・管理者は著作権やライセンスを熟知していない場合がある
・定期的な棚卸しやレビュー、外部監査を行っていない場合がある
・管理者からの報告内容が正しいと言える裏付けがない場合がある

誤解・落とし穴 2　インストール制限をしているから大丈夫？

・制限をすり抜けインストールされるソフトウェアやウイルスの存在がある

誤解・落とし穴 3　管理ツールを導入しているから大丈夫？

・ネットワークに接続されていない端末の情報は収集できない
・把握できるソフトウェアの範囲は、ツールごとに異なる
・ツールはソフトウェア資産管理の一部の役割を果たすにすぎない

誤解・落とし穴 4　部門ごとにしっかり管理しているから大丈夫？

・部門ごとの管理者が正しく管理しているチェック機能がなければ万全ではない
よくある話として、インストールに必要なIDやインストールキーなどが部門内で共有されているケースも

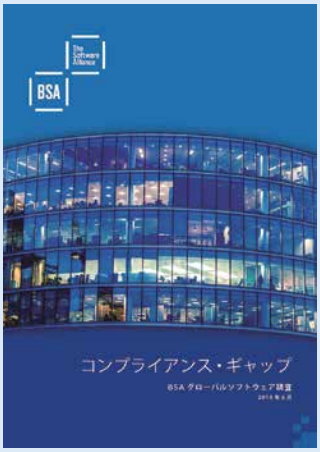
誤解・落とし穴 5　業者にまかせているから大丈夫？

・契約主体はあくまでエンドユーザとソフトウェアベンダーであり、業者が責任をもつものではない
・納品物が仕様通りかどうかをチェック（検収）する機能はあるか
・キッティング業者が不正なインストールCDを使用しているケースもある

BSAについて

BSA | The Software Alliance（BSA | ザ・ソフトウェア・アライアンス）は、グローバル市場において世界のソフトウェア産業を牽引する業界団体です。BSAの加盟企業は世界中で最もイノベーティブな企業を中心に構成されており、経済の活性化とより良い現代社会を築くためのソフトウェア・ソリューションの創造に年間数千億円もの投資を行っています。世界各国の政府との意見交換、著作権をはじめとする知的財産権の保護ならびに教育啓発活動を通じて、BSAはデジタル社会の拡大とそれを推進する新たなテクノロジーへの信頼の構築に努めています。

BSAの主な活動には、法制度および重要政策に関する政府への提言（アドボカシーアジェンダ）と不正対策活動（不正対策アジェンダ）があり、日本では不正商品対策協議会（ACA）や一般社団法人コンピュータソフトウェア著作権協会（ACCS）等の業界団体や関係官庁とも積極的に協力しながら活動しています。



団体概要

団　体　名：BSA | The Software Alliance（BSA | ザ・ソフトウェア・アライアンス）
拠　　点：【本部】米国ワシントンDC / Worldwide Headquarters
【支部】英国ロンドン / BSA EMEA（Europe, Middle East & Africa）
シンガポール / BSA Asia
設　　立：1988年
代　　表：ビクトリアA. エスピネル　プレジデント兼最高経営責任者（CEO）
ホームページ：【本部】www.bsa.org（英語）
【日本】www.bsa.or.jp

www.bsa.or.jp

BSA Worldwide Headquarters

20 F Street, NW
Suite 800
Washington, DC 20001

T: +1.202.872.5500
F: +1.202.872.5501

BSA Asia-Pacific

300 Beach Road
#25-08 The Concourse
Singapore 199555

T: +65.6292.2072
F: +65.6292.6369

BSA Europe, Middle East & Africa

2 Queen Anne's Gate Buildings
Dartmouth Street
London, SW1H 9BP
United Kingdom

T: +44.207.340.6080
F: +44.207.340.6090

Argentina Australia Belgium Brazil Canada Chile China Colombia Czech Republic Denmark France Germany Greece India Indonesia Israel Italy Japan Malaysia Mexico Netherlands Panama Peru Poland Russia South Africa South Korea Spain Taiwan Thailand Turkey Vietnam