

The
Software
Alliance

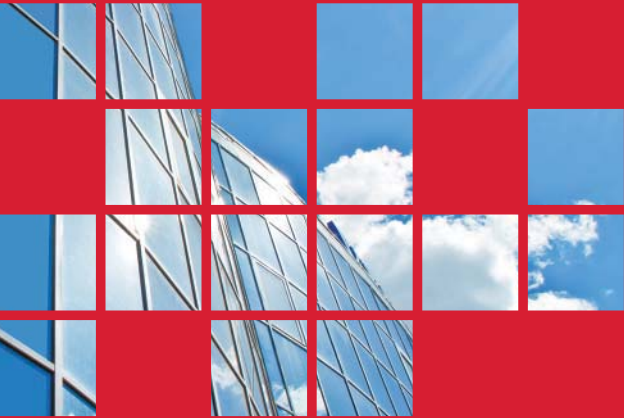
BSA

ライセンス コンプライアンスによる 機会獲得

BSA グローバルソフトウェア調査

2016年5月





目次

主な動向と調査結果	1
強い相関：マルウェアと不正ソフトウェア	4
世界動向	5
PC にインストールされたソフトウェアの不正コピー率および不正ソフトウェア総額	6
クラウドコンピューティングの一環として必要とされる効果的なソフトウェア資産管理	9
調査方法	10
サイバーリスクから組織を適切に保護する	14
BSA The Software Alliance (BSA ザ・ソフトウェア・アライアンス) について	16



主な動向と調査結果

多くの産業や人々の取り組みにおいて、ソフトウェアは人が創造力を発揮するための最も重要な出発点となります。革新的な考えを持つ人は、アプリケーションやクラウドコンピューティングなど常に変化しているイノベーションとソフトウェアの活用により、何十億という人々の生活に多大な恩恵をもたらしています。

ソフトウェアの進歩とユビキタス化の結果として、サイバーセキュリティが世界中の企業や組織にとって一番の懸念事項になることが考えられます。理由は、以下の通りです。

- 2015年、4億3,000万件の新しいマルウェアが検出されました。これは2014年の数字から36%上昇しています¹。
- 組織は7分ごとに何らかのかたちで、マルウェアの攻撃を受けています²。
- 2015年、データ侵害により5億を超える個人情報データが盗まれたり、失われたりしました³。

組織が直面するこのようなサイバー攻撃の損害は侮ることができません。調査会社のIDCによると、2015年のサイバー攻撃による世界的な損害額は4,000億ドルを上回っています。

サイバー攻撃により企業は莫大な経済的損害を受ける可能性があります。それに加えて企業はその評判に傷がついたり、顧客の信頼を失ったりする可能性があります。「2016年インターネットセキュリティ脅威レポート (2016 Symantec Internet Security Threat Report)」では、1回のサイバー攻撃だけでも「企業の評判と信頼性に重大な損害が与えられる可能性がある」と述べられています。

サイバーセキュリティに対処するために必要な最初のステップは、組織内部に目を向けることです。まず、企業は自社のネットワークに何がインストールされているかを把握する必要があります。また、ネットワークで実行されているソフトウェアが正規品であり使用許諾を得ていることを確認する必要があります。不正ソフトウェアや使用許諾を得ていないソフトウェアの使用とマルウェアからの攻撃には非常に強い関連があるため、非常に重要なステップです（ページ4の「強い関連：マルウェアと不正ソフトウェア」を参照）。企業は正規ソフトウェアを使用するよう取り組むことにより、サイバーリスクを大幅に軽減することができます。

¹ 2016年インターネットセキュリティ脅威レポート、第21号、5ページ (<https://www.symantec.com/security-center/threat-report>)。

² *Fighting Cybercrime with Actionable Insights*、IBM Corporation、2014 (<http://www.slideshare.net/IBMBDA/infographic-fighting-cybercrime-with-actionable-insights>)。

³ 2016年インターネットセキュリティ脅威レポート、第21号、54ページ (<https://www.symantec.com/security-center/threat-report>)。

リスクを認識しているにもかかわらず、危険な行為が依然として存在する

個人ユーザ、IT 管理者、企業ユーザを対象とした今回のグローバルソフトウェア調査では、不正ソフトウェアの利用によるサイバーセキュリティの危険を十分に認識している国際社会の実態が描かれました。また、不正ソフトウェアをまだ使用している企業の割合が驚くほど高いことも明らかになりました。

世界各国の CIO は、ネットワークで必ず正規ソフトウェアを使用する大きな理由が不正ソフトウェアによるセキュリティ脅威を回避することと認識していました。また、世界のどの地域においても、最も懸念されることはこのようなセキュリティインシデントに関連して発生するデータ損失であると CIO は述べています。

このようなリスクを認識しているのは CIO だけではないということが重要です。個人ユーザや社員に対する広範な調査では、調査対象者の 60% が仕事において正規ソフトウェアを使用する

大きな理由として、不正ソフトウェアによるセキュリティリスクの懸念を挙げています。またデータ損失に関して強い懸念も示しており、このようなセキュリティリスクが十分に理解されています。しかしながら、危険な行為が阻止されていないのが現状です。

自社のネットワーク上にどのようなソフトウェアが、アップロードされ使用されているかを把握することは企業にとって不可欠です。しかし、実際には社員が非正規ソフトウェアのインストールとその使用の割合に対して、大きな認識の差が存在しています。CIO は社員の 15% が会社のパソコンにソフトウェアをアップロードしていると推測していますが、実際にはその約 2 倍の社員が会社のパソコンに非正規ソフトウェアをアップロードしていると述べています。

さらに、グローバルソフトウェア調査では以下のことが判明しました。

- 2015 年、世界中の PC にインストールされたソフトウェアのうち、適切な使用許諾を得ていないソフトウェアは 39% でした。状況は、2013 年に BSA が実施した前回のグローバル調査で示された 43% からわずかに改善したのみです。
- デジタル環境の厳格な管理が必要な業界においても、不正使用の割合は驚くほど高いと判明しました。銀行、保険、証券業界における不正使用の世界的割合は 25% と、4 つのソフトウェアのうちの 1 つが不正使用であることが調査により判明しました。
- CIO の 49% が不正ソフトウェアの使用によるマルウェアによるセキュリティ脅威を認めています。

ソリューション：ソフトウェア資産管理と社員教育

ソフトウェア資産を管理していない企業は不要なリスクを負うだけでなく、コスト削減の機会も失います。ソフトウェア資産を注意深く管理することで効率性を大幅に改善できる可能性があります。**ソフトウェアを適切に管理し、ライセンス数が多すぎるアプリケーションや未使用のソフトウェアなど、見落としがちな非効率性を取り除くことで、実際にコストを 25% も削減できることが研究によって示されています。**

重大なリスクが緩和されるとともに大幅なコスト削減を実現することで、組織は経営と収益に好影響を及ぼす大きな機会を得ることができます。

幸いにも、これを行うための統制方法がすでに確立されています。それはソフトウェア資産管理 (SAM) です (15 ページで説明する 4 つのステップから成る行動アクション計画を参照)。SAM を効果的に導入している組織には、ネットワークに何がインストールされているかを示すインベントリや、ソフトウェアの購入、インストール、更新、使用停止に関する規程とプロセスを持ち、ソフトウェアの使用

ソフトウェアを適切に管理し、ライセンス数が多すぎるアプリケーションや未使用のソフトウェアなど見落としがちな非効率性を排除することで、コストを 25% も削減できます。

にソフトウェアのニーズを合わせます。効果的な SAM は他の堅実な管理規程などと同様にビジネスに取り込まれています。

規程と手法だけでは十分ではありません。調査で強調されているように最良の規程があっても、規程

とその重要性について従業員が教育されていない場合、失敗してしまいます。

効果的な SAM と十分な従業員教育を積極的に組み合わせることで、企業は安全性、コスト効率、効果を高める機会をとらえることができます。

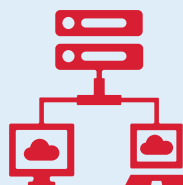
不正ソフトウェア：実態



2015 年、サイバー攻撃に対して企業がかけたコストは 4,000 億ドルを超えました。



サイバー攻撃と不正ソフトウェアの使用には強い相関関係が存在します（ページ 4 の「強い相関：マルウェアと不正ソフトウェア」を参照）。



非常に多くの CIO がネットワークを管理していません。また、実際に、不正ソフトウェアがどれだけインストールされているかを大幅に過小評価しています。



26% の従業員が業務で使用するコンピュータに外部ソフトウェアをインストールしていることを認め、84% が複数の不正プログラムをインストールしていることを認識しています。



モバイルデバイスの使用が増大しているにもかかわらず、個人のモバイルデバイスを業務で接続することに関して、70% の企業が非公式の規程しかない、またはそのような規程が一切ないと報告しました。

強い相関：マルウェアと不正ソフトウェア

マルウェアは組織にとって大きな問題ですが、その主な原因の1つは不正ソフトウェアです。

BSA が新しいグローバルソフトウェア調査の一環として実行した分析によると、不正 PC ソフトウェアの割合が高いほど、攻撃対象を弱体化させるマルウェアの攻撃をユーザが高い確率で受けることが確認されました。

調査結果は、回帰分析（変数間の関係を推定するための統計プロセス）の結果を表しています。この調査結果では、マルウェアと不正ソフトウェアの間に非常に強い正の相関が示されました。

具体的には、0.78 の相関係数が示されました（1.0 が完全な相関を表す）。例えば他の相関と比べた場合、

教育と所得水準の相関は 0.77、国の法令順守とその国の IT 洗練度の相関は 0.79 を示しています。相関が 1.0 に近づくほど、調査の対象である 2 つの変数間の関係が強くなり、一方の値からもう一方の値を予測できるようになります。

この結果は 2015 年前半の IDC の調査を裏付けています。この調査でも、不正ソフトウェアの使用が「マルウェア

の攻撃を予測する強力な要因である」こと、および「因果関係を示す経験的証拠がある」ことが確認されています。

セキュリティ環境への脅威と損害が増大するにつれ、CIO は不正ソフトウェアとサイバーリスクの関係にしっかりと向き合って、細心の注意を払う必要があります。

Symantec の最新のインターネットセキュリティ脅威レポートの調査結果に示されているとおり、サイバーセキュリティの脅威は増えています。

- 2015 年は、毎日 100 万を超える新しい脅威が生まれました。
- 2015 年、ランサムウェア攻撃が 35% 増加しました。
- 2015 年、標的型攻撃の 65% が中小規模の組織を狙ったものでした。リソースの少ないこのような組織では、多くの場合、ベストプラクティスが導入されていません。

このような攻撃には高いコストがかかります。業界の推定によると、サイバー攻撃を受けると、平均で 1,100 万ドルのコストが組織にかかります。IDC は、組織がサイバー攻撃からの副次的影響に対応するために費やしたコストは昨年 1 年間だけで 4,000 億ドルを超えたと見積もっています。

財務的なコストをはるかに上回る、そしておそらくさらに破壊的であり、組織を弱体化させる可能性がある影響は、評判に傷がつくことです。IBM が昨年実施した業界調査によると、61% の組織が、データ盗難とサイバー犯罪が組織の評判に対する最大の脅威であると述べています。

この調査結果は、不正ソフトウェアの使用に関連する目に見えない大きなコストがあることを強調しており、不正ソフトウェアの使用により組織がそのサイバーリスクに対して無意識のうちに扉を開いている可能性があることを示しています。また、この調査結果は第一防衛線を制定することも主張しています。つまり、非正規のソフトウェアや不正ソフトウェアを誰も取得できないようにして、さらに、ソフトウェアを定期的に更新し、セキュリティパッチを入手直後に適用します。これを行わない場合、重大な問題が発生する可能性があります。

BSA が新しいグローバルソフトウェア調査の一環として実施した分析によると、不正 PC ソフトウェアの割合が高いほど、攻撃対象を弱体化させるマルウェアの攻撃を高い確率で受けることが確認されました。

世界動向

サイバーセキュリティが世界中の企業およびその他の組織にとって最大の懸念になりました。10年以上にわたって不正ソフトウェアの使用が43%から39%に僅かながらも減少したのは、この懸念と他の要因（適切なSAMの重要性に対する認識が高まったこと、長年にわたる教育と施策など）によるものです。

同時に、サイバーセキュリティの脅威についての懸念が高まってきたことに加えて、このような脅威に対する組織の脆弱性と不正ソフトウェアの使用との関係に対する認識も高まってきました。今年の調査では、例えば、個人ユーザと従業員の60%が、不正ソフトウェアを使用しない一番の理由としてマルウェアによるセキュリティ脅威を挙げました。

不正ソフトウェアの使用が世界的に減少（恒常ドルベースで4%）するのに伴って、不正ソフトウェアの総額が522億ドルに減少しました。

この前向きな動きにもかかわらず、調査の対象となった116のマーケットのうち72のマーケットでは、2015年にインストールされた総PCソフトウェアの半数以上が不正ソフトウェアであり、47のマーケットでは、75%以上が不正ソフトウェアでした。やるべきことは依然としてたくさんあります。

地域別ハイライト

2015年はすべての地域で、不正ソフトウェアの割合が低下しました。他よりも大きく低下した地域もあります。一般に、地域の割合は大国に影響されます。アジア太平洋地域では中国、ラテンアメリカではブラジルです。

場合によって逆説的效果も見られます。中国では4%の低下が見られましたが、アジア太平洋全体では1%のみの低下に留まり、61%になりました。これは、この地域のPC市場における中国のシェアが高まり、平均が全体的に引き上げられたためであり、中国の全体的な不正コピー率が地域全体の不正コピー率を依然として上回っているためです。

ラテンアメリカではこれとは逆の現象が見られます。ブラジルで3%、メキシコで2%の低下が見られましたが、これらは地域の平均を4%低下させる

個人ユーザと社員の60%が、不正ソフトウェアを使用しない一番の理由としてマルウェアによるセキュリティ脅威を挙げました。

(ページ8に続く)

PC にインストールされたソフトウェアの不正コピー率および不正ソフトウェア総額

	不正コピー率				不正ソフトウェア総額 (単位: 百万ドル)			
	2015	2013	2011	2009	2015	2013	2011	2009
アジア太平洋								
オーストラリア	20%	21%	23%	25%	\$579	\$743	\$763	\$550
バングラデシュ	86%	87%	90%	91%	\$236	\$197	\$147	\$127
ブルネイ	66%	66%	67%	67%	\$19	\$13	\$25	\$14
中国	70%	74%	77%	79%	\$8,657	\$8,767	\$8,902	\$7,583
香港	41%	43%	43%	47%	\$320	\$316	\$232	\$218
インド	58%	60%	63%	65%	\$2,684	\$2,911	\$2,930	\$2,003
インドネシア	84%	84%	86%	86%	\$1,145	\$1,463	\$1,467	\$886
日本	18%	19%	21%	21%	\$994	\$1,349	\$1,875	\$1,838
マレーシア	53%	54%	55%	58%	\$456	\$616	\$657	\$453
ニュージーランド	18%	20%	22%	22%	\$66	\$78	\$99	\$63
パキスタン	84%	85%	86%	84%	\$276	\$344	\$278	\$166
フィリピン	67%	69%	70%	69%	\$431	\$444	\$338	\$217
シンガポール	30%	32%	33%	35%	\$290	\$344	\$255	\$197
韓国	35%	38%	40%	41%	\$657	\$712	\$815	\$575
スリランカ	79%	83%	84%	89%	\$163	\$187	\$86	\$77
台湾	36%	38%	37%	38%	\$264	\$305	\$293	\$227
タイ	69%	71%	72%	75%	\$738	\$869	\$852	\$694
ベトナム	78%	81%	81%	85%	\$598	\$620	\$395	\$353
その他	87%	91%	91%	90%	\$491	\$763	\$589	\$303
合計	61%	62%	60%	59%	\$19,064	\$21,041	\$20,998	\$16,544
中央・東ヨーロッパ								
アルバニア	73%	75%	75%	75%	\$10	\$10	\$6	\$8
アルメニア	86%	86%	88%	90%	\$18	\$26	\$26	\$14
アゼルバイジャン	84%	85%	87%	88%	\$90	\$103	\$67	\$52
ベラルーシ	85%	86%	87%	87%	\$76	\$173	\$87	\$55
ボスニア	63%	65%	66%	66%	\$24	\$21	\$15	\$14
ブルガリア	60%	63%	64%	67%	\$78	\$101	\$102	\$115
クロアチア	51%	52%	53%	54%	\$49	\$64	\$74	\$71
チェコ	33%	34%	35%	37%	\$150	\$182	\$214	\$174
エストニア	42%	47%	48%	50%	\$16	\$20	\$25	\$19
ジョージア	84%	90%	91%	95%	\$25	\$40	\$52	\$54
ハンガリー	38%	39%	41%	41%	\$107	\$127	\$143	\$113
カザフスタン	73%	74%	76%	78%	\$89	\$136	\$123	\$74
ラトビア	49%	53%	54%	56%	\$23	\$29	\$32	\$24
リトアニア	51%	53%	54%	54%	\$37	\$47	\$44	\$31
マケドニア	64%	65%	66%	67%	\$15	\$19	\$22	\$15
モルドバ	86%	90%	90%	91%	\$36	\$57	\$45	\$28
モンテネグロ	76%	78%	79%	81%	\$6	\$7	\$7	\$11
ポーランド	48%	51%	53%	54%	\$447	\$563	\$618	\$506
ルーマニア	60%	62%	63%	65%	\$161	\$208	\$207	\$183
ロシア	64%	62%	63%	67%	\$1,341	\$2,658	\$3,227	\$2,613
セルビア	67%	69%	72%	74%	\$54	\$70	\$104	\$67
スロバキア	36%	37%	40%	43%	\$55	\$67	\$68	\$65
スロベニア	43%	45%	46%	46%	\$30	\$41	\$51	\$39
ウクライナ	82%	83%	84%	85%	\$129	\$444	\$647	\$272
その他	87%	89%	90%	88%	\$70	\$105	\$127	\$56
合計	58%	61%	62%	64%	\$3,136	\$5,318	\$6,133	\$4,673
ラテンアメリカ								
アルゼンチン	69%	69%	69%	71%	\$554	\$950	\$657	\$645
ボリビア	79%	79%	79%	80%	\$98	\$95	\$59	\$40
ブラジル	47%	50%	53%	56%	\$1,770	\$2,851	\$2,848	\$2,254
チリ	57%	59%	61%	64%	\$296	\$378	\$382	\$315
コロンビア	50%	52%	53%	55%	\$281	\$396	\$295	\$244
コスタリカ	59%	59%	58%	59%	\$90	\$98	\$62	\$33
ドミニカ	76%	75%	76%	77%	\$84	\$73	\$93	\$66
エクアドル	68%	68%	68%	67%	\$137	\$130	\$92	\$65
エルサルバドル	81%	80%	80%	80%	\$63	\$72	\$58	\$46
グアテマラ	79%	79%	79%	80%	\$169	\$167	\$116	\$74
ホンジュラス	75%	74%	73%	74%	\$36	\$38	\$24	\$17
メキシコ	52%	54%	57%	60%	\$980	\$1,211	\$1,249	\$1,056
ニカラグア	82%	82%	79%	79%	\$23	\$23	\$9	\$5
パナマ	72%	72%	72%	73%	\$117	\$120	\$74	\$42
パラグアイ	84%	84%	83%	82%	\$89	\$115	\$73	\$29
ペルー	63%	65%	67%	70%	\$210	\$249	\$209	\$124
ウルグアイ	68%	68%	68%	68%	\$57	\$74	\$85	\$40
ベネズエラ	88%	88%	88%	87%	\$402	\$1,030	\$668	\$685
その他	83%	84%	84%	83%	\$331	\$352	\$406	\$430
合計	55%	59%	61%	63%	\$5,787	\$8,422	\$7,459	\$6,210

ライセンスコンプライアンスによって機会をとらえる：BSA グローバルソフトウェア調査

	不正コピー率				不正ソフトウェア総額 (単位：百万ドル)			
	2015	2013	2011	2009	2015	2013	2011	2009
中東・アフリカ								
アルジェリア	83%	85%	84%	84%	\$84	\$102	\$83	\$55
バーレーン	54%	53%	54%	54%	\$34	\$27	\$23	\$21
ボツワナ	79%	79%	80%	79%	\$23	\$20	\$16	\$11
カメルーン	82%	82%	83%	83%	\$21	\$9	\$9	\$7
エジプト	61%	62%	61%	59%	\$157	\$198	\$172	\$146
イラク	85%	86%	86%	85%	\$120	\$116	\$172	\$129
イスラエル	29%	30%	31%	33%	\$161	\$177	\$192	\$148
コートジボワール	80%	80%	81%	79%	\$22	\$24	\$16	\$14
ヨルダン	56%	57%	58%	57%	\$34	\$35	\$31	\$26
ケニア	76%	78%	78%	79%	\$113	\$128	\$85	\$66
クウェート	58%	58%	59%	60%	\$94	\$97	\$72	\$62
レバノン	70%	71%	71%	72%	\$65	\$65	\$52	\$46
リビア	90%	89%	90%	88%	\$65	\$50	\$60	\$25
モーリシャス	54%	55%	57%	56%	\$7	\$7	\$7	\$4
モロッコ	65%	66%	66%	66%	\$57	\$69	\$91	\$64
ナイジェリア	80%	81%	82%	83%	\$232	\$287	\$251	\$156
オマーン	60%	60%	61%	63%	\$59	\$65	\$36	\$39
カタール	48%	49%	50%	51%	\$72	\$77	\$62	\$50
レユニオン	39%	39%	40%	40%	\$2	\$1	\$1	\$1
サウジアラビア	49%	50%	51%	51%	\$412	\$421	\$449	\$304
セネガル	75%	77%	78%	78%	\$12	\$9	\$9	\$5
南アフリカ	33%	34%	35%	35%	\$274	\$385	\$564	\$324
チュニジア	74%	75%	74%	72%	\$49	\$66	\$51	\$44
トルコ	58%	60%	62%	63%	\$291	\$504	\$526	\$415
アラブ首長国連邦	34%	36%	37%	36%	\$226	\$230	\$208	\$155
イエメン	87%	87%	89%	90%	\$11	\$9	\$15	\$10
ザンビア	81%	81%	82%	82%	\$4	\$3	\$3	\$2
ジンバブエ	90%	91%	92%	92%	\$7	\$4	\$4	\$4
その他アフリカ	84%	85%	86%	86%	\$419	\$484	\$363	\$260
その他中東	84%	85%	87%	88%	\$569	\$640	\$536	\$294
合計	57%	59%	58%	59%	\$3,696	\$4,309	\$4,159	\$2,887
北米								
カナダ	24%	25%	27%	29%	\$893	\$1,089	\$1,141	\$943
プエルトリコ	41%	42%	42%	46%	\$28	\$27	\$44	\$46
米国	17%	18%	19%	20%	\$9,095	\$9,737	\$9,773	\$8,390
合計	17%	19%	19%	21%	\$10,016	\$10,853	\$10,958	\$9,379
西ヨーロッパ								
オーストリア	21%	22%	23%	25%	\$131	\$173	\$226	\$212
ベルギー	23%	24%	24%	25%	\$190	\$237	\$252	\$239
キプロス	45%	47%	48%	48%	\$14	\$19	\$19	\$16
デンマーク	22%	23%	24%	26%	\$176	\$224	\$222	\$203
フィンランド	24%	24%	25%	25%	\$171	\$208	\$210	\$175
フランス	34%	36%	37%	40%	\$2,101	\$2,685	\$2,754	\$2,544
ドイツ	22%	24%	26%	28%	\$1,720	\$2,158	\$2,265	\$2,023
ギリシャ	63%	62%	61%	58%	\$189	\$220	\$343	\$248
アイスランド	46%	48%	48%	49%	\$10	\$12	\$17	\$11
アイルランド	32%	33%	34%	35%	\$87	\$107	\$144	\$125
イタリア	45%	47%	48%	49%	\$1,341	\$1,747	\$1,945	\$1,733
ルクセンブルク	19%	20%	20%	21%	\$21	\$30	\$33	\$30
マルタ	44%	44%	43%	45%	\$4	\$5	\$7	\$7
オランダ	24%	25%	27%	28%	\$481	\$584	\$644	\$525
ノルウェー	23%	25%	27%	29%	\$178	\$248	\$289	\$195
ポルトガル	39%	40%	40%	40%	\$145	\$180	\$245	\$221
スペイン	44%	45%	44%	42%	\$913	\$1,044	\$1,216	\$1,014
スウェーデン	21%	23%	24%	25%	\$288	\$397	\$461	\$304
スイス	23%	24%	25%	25%	\$448	\$469	\$514	\$344
英国	22%	24%	26%	27%	\$1,935	\$2,019	\$1,943	\$1,581
合計	28%	29%	32%	34%	\$10,543	\$12,766	\$13,749	\$11,750
全世界合計	39%	43%	42%	43%	\$52,242	\$62,709	\$63,456	\$51,443
EU	29%	31%	33%	35%	\$11,060	\$13,486	\$14,433	\$12,469
BRICs*	64%	67%	70%	71%	\$14,452	\$17,187	\$17,907	\$14,453

*BRICs：ブラジル、ロシア、インド、中国

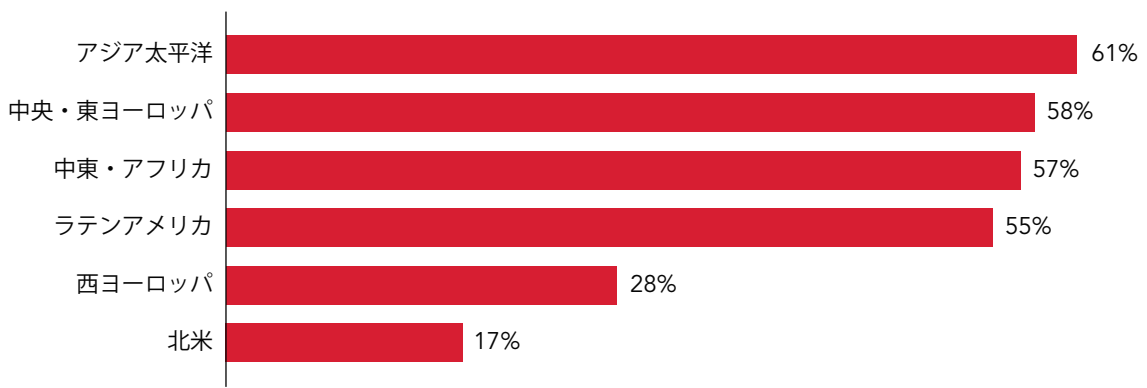
のに十分なものであり、地域の平均は 55% になりました。これは、この 2 つの国の不正コピー率の平均が地域の平均よりも低かったためです。

2013 年からの最も顕著な変化が中央・東ヨーロッパで見られます。ロシアでは、不正コピー率が 2% 上昇し、恒常ドルベースでの総額が 2013 年から 50% 低下しました。これは、ルーブルの切り下げによるものであり、実際の低下幅 (4%) とは根本的に異なります。

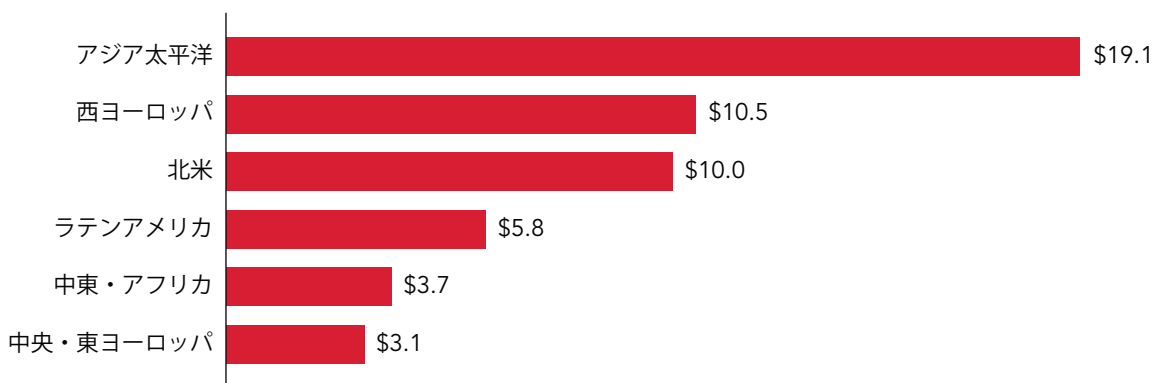
その他の地域別ハイライト：

- 北米の不正コピー率は 17% で、世界で最も低い不正コピー率を維持しています。ただし、不正ソフトウェアの総額は 100 億ドルと、極めて大きいものでした。
- 西ヨーロッパ全体の不正コピー率は、1% 低下して 28% になりました。
- 中東・アフリカ全体では、不正使用率が 2% 低下して 57% になりました。

不正コピー率の平均値



不正ソフトウェア総額 (10 億ドル)



クラウドコンピューティングの一環として必要とされる効果的なソフトウェア資産管理 (SAM)

クラウドコンピューティングは組織に莫大な利益をもたらす可能性があります。クラウドコンピューティングを使用することで、スタートアップ企業や個人ユーザ、公共団体、小規模企業を問わず、すべてのユーザがテクノロジーに迅速で効率的かつ規模を拡大してアクセスできます。そして、これらのサービスにより、今までにない高い接続性、生産性、競争力への扉が開かれました。

クラウドコンピューティングの重要性が高まる一方、効果的なソフトウェア資産管理 (SAM) システムの維持、および組織内のソフトウェアとクラウドサービスのライフサイクルの管理が求められます。SAM は、莫大な利益をもたらすベストプラクティスです。

クラウドサービスは従来の分散型ソフトウェアとは異なりますが、クラウドでもソフトウェアのライフサイクル管理を同様に行う必要があります。組織は、どのクラウドベースソフトウェアに対して使用権限を与えたかと、そのソフトウェアの実際の使用状況について把握しておく必要があります。クラウドサービス経由で付与した使用権限を最大限に活用しない場合、組織から生み出される価値が限定される可能性があります。SAM についての検討事項を適切に対処せずにクラウドコンピューティングを使用すると、コストおよびリスク分析に関連する重大な誤りを引き起こす可能性があります。

ネットワーク上のクラウドサービスの利用範囲を把握していない場合、組織に重大なリスクをもたらす懸念が残ります。例えば、商用目的ではないサービスの使用や、内部の機密データを外部ネットワークに公開するサービスの許可、違法なクラウドサービスプロバイダが提供するサービスなどです。

クラウドセキュリティ企業の SkyHigh Networks 社による最近の調査では、平均的な大企業がネットワーク全体で使用しているクラウドサービスの数は 1,100 を上回ることが明らかになっています。また同調査では、多くの組織がクラウドサービスプロバイダの承認について公式な規程を保有していないことや、クラウドサービスプロバイダとの契約時に従業員が正規のプロセスに従っていないことが指摘されてい

ます。正規のプロセスが存在しない場合、信頼できるプロバイダからのみクラウドベースソフトウェアを購入できるよう、SAM プログラムを適用することが重要です。

クラウドサービスを利用する組織にとって、ログイン資格情報の共有はさらに別のリスクを産む場合があります。新しいグローバルソフトウェア調査の結果によると、ログイン資格情報の共有が広まり、増加していることが明らかになりました。

調査では、ユーザの 58% が商用クラウドソフトウェアサービスのログイン資格情報を共有していることが確認されました。さらに、10 人のユーザのうち 1 人以上が組織以外の誰かとログイン資格情報を共有していました。ログイン資格情報を別のユーザと共有したユーザの 72% が、時々または頻繁に共有を行っていたことが示されています。

通常、クラウドサービスはサブスクリプションに基づいており、個々のユーザに割り当てられます。別のユーザと共有するものではありません。効果的なソフトウェア資産管理システムがあれば、使用許諾条項と、クラウドサービスにアクセスしているユーザ数を監視できます。

少なくとも、ログイン資格情報の共有に関する問題の一部は、組織内での教育が不十分であることや、正規の規程が存在しないことに起因している可能性があります。調査では、回答者の 42% が、ログイン資格情報の共有に関して非正規の規程しかない、またはそのような規程が一切ないと述べています。

クラウドコンピューティングは、高度なテクノロジーへのアクセスを一般に広めるための比類のない機会を提供します。組織内で不可欠な SAM の促進することで、この新しいテクノロジーを効果的に組み込みながら、リスクを軽減することができます。

サイバー関連の脅威およびログイン資格情報の共有が世界的に増大しつつある現在、リスクを軽減するためのこの取り組みはもはやベストプラクティス以上のもので、唯一のプラクティスと言えます。

多くの組織がクラウドサービスプロバイダの承認に関して正規の規程を持っていません。また、クラウドサービスプロバイダとの契約時に従業員が正規プロセスに従っていません。

調査方法

BSA グローバルソフトウェア調査は、任意の年における PC にインストールされた不正ソフトウェアの数と価値を調査するもので、今回は 2015 年を対象としています。BSA は報告書の作成に際し、世界有数の独立系調査会社である IDC とともに、世界中で使用されている正規および不正ソフトウェアを測定、把握、評価しました。

調査では、182 種類の離散的なデータ入力を収集し、116 の市場の PC とソフトウェアの傾向を評価しています。

不正ソフトウェアの使用のような違法行為の規模と範囲を正確に測定することは極めて困難です。本調査は、世界の著作権侵害の最も洗練された評価のひとつと考えられていますが、BSA とその協力企業はデータの信頼性を改善する新しい方法を常に模索しています。2011 年には、2 人の著名な IT 経済研究者とともに入力データを精密化するとともに、不正ソフトウェアの使用の推定精度を可能な限り高めるためにいくつかの改修を行いました。

ソフトウェアユーザの世界規模調査

今回の BSA グローバルソフトウェア調査の重要な構成要素のひとつが、2016 年の初めに IDC が実施した、20,000 人を超える個人と企業の PC ユーザに対する世界規模の調査です。地域内の代表的な市場、IT 洗練度のレベル、地理的・文化的多様性を考慮して 32 の市場を選び、オンラインまたは電話による調査を実施しました。さらに同時に 22 カ国、2,200 人の IT 管理者に対しても調査を実施しました。

調査は、たとえば、各国の「ソフトウェア搭載数」を決めるためにも使われます。ソフトウェア搭載数とは、商用ソフトウェア、オープンソースプログラム、それらの混在したプログラムなど、PC ごとにインストールされるソフトウェアの数を意味します。回答者には、前年に自分の PC にインストールしたソフトウェアパッケージの数と種類、新規とアップグレードの比率、ソフトウェアが PC の付属品か、新規の PC にインストールしたか、2015 年以前の PC にインストールしたかなどを尋ねます。これらの質問の対象は個人と企業のユーザの両方です。

さらに、知的財産、不正ソフトウェアの使用、その他の新しい技術的問題に関する社会の傾向や行動も評価します。この評価により、調査年ごとに、世界中の不正ソフトウェアの使用に隠れている動態についての最新の見解を得ることができます。

調査対象国は、回を重ねるごとに対象範囲が最大になるよう順番に選んでいます。11 の優先市場は調査周期ごとに同時に調べ、52 の国は 2～3 周期に少なくとも 1 回の調査を実施します。残りの国は、その回に応じて選定します。どの任意の調査周期でも、合計の調査対象は、インストールされているソフトウェアの総数の 85% 以上、有償ソフト

ウェアの約 90% に達しており、ほとんどの市場は 3 年の調査周期ごとに少なくとも 1 回調査対象となります。

インストールされたソフトウェアの不正コピー率の計算

BSA は 2003 年以來、IT 産業の市場統計・予測大手である IDC とともに、インストールされたソフトウェアの不正コピー率と総額を調査してきました。

以下に、各国の不正コピー率と総額を算出する基本的な方法を示します。

1. 個人と企業ユーザが対象年にインストールした PC ソフトウェアの総数を決定します。
2. 対象年に有償で入手した数量および正規に取得した数量（オープンソース、無償ライセンスなど）を決定します。これも、個人と企業ユーザに分けて調査します。
3. 総数から正規数を差し引き、不正ソフトウェアの総数を求めます。総数の把握後、インストールした全ソフトウェアに対する比率として、不正コピー率を算出します。

$$\begin{aligned}
 & \text{不正コピー率} \\
 & = \\
 & \frac{\text{不正ソフトウェア数}}{\text{インストールされたソフトウェア総数}} \\
 & \times \\
 & \frac{\text{ソフトウェアがインストールされた PC 台数}}{\text{PC1 台当たりのソフトウェア数}} \\
 & = \\
 & \text{インストールされたソフトウェア総数}
 \end{aligned}$$

インストールされたソフトウェアの総数（分母）を計算するために、各国に何台の PC があるか、そしてその PC のうち、その年に何台の PC にソフトウェアがインストールされたかを調べます。IDC は、「PC トラッカー」と呼ばれる、92 カ国をカバーする四半期ごとの調査製品でこの情報を追跡します。残りの数カ国は、当該調査のために年に 1 回調査されます。

個人用と企業用の PC の数がわかれば、調査で収集したソフトウェア搭載数データを使って、各国でインストールされた正規と不正ソフトウェアの総数が計算できます。

調査対象以外の国のソフトウェア搭載数を推定するために、IDC はクラスタ分析技法を用いて搭載数を変化させながら各国に共通の特性を見つけ、その特性を使って調査対象以外の国に搭載数を割り当てます。さらに、調査した国の既知のソフトウェア搭載数と、国際電気通信連合 (ITU) が発行する新興市場の尺度 (ICT 開発指標) 上の当該国のスコアとの相関を調べ、グループに分けて調査対象以外の国との比較により、割り当てた搭載数の妥当性を確認します。

不正ソフトウェアの総数（分子）を求めるのに必要となる、正規に取得したソフトウェアの市場規模の把握には、IDC が保有する約 80 カ国のソフトウェア市場データを利用しています。また、約 20 カ国以上については、個別に調査を実施します。残りの数カ国に関しては、当該調査のために年 1 回の調査を行います。これらの調査により、正規に取得したソフトウェアの市場規模が把握できます。ソフトウェアの総額は、個人と企業のユーザについて別に求めます。

ソフトウェアの市場規模をソフトウェアの数量に変換するには、各国の個人用と企業用の PC ソフトウェアの平均価格が必要です。これは、小売り、ボリュームライセンス、OEM、無償、オープンソースなどのソフトウェア価格の国別のマトリクスと、セキュリティ、OA、オペレーティングシステムなどの製品のマトリクスによって得られます。

IDC の価格情報は、IDC の価格トラッカーと各地のアナリストの調査によって得られます。また、OEM 对小売り、個人対企業などの重み付けは IDC の調査によって決まります。この 2 つのマトリクスを掛け合わせることで、各種ソフトウェアの最終的な加重平均単価が得られます。

正規ソフトウェアの総数を求めるために、IDC では以下の式を用います。

$$\begin{aligned} & \text{ソフトウェアの市場規模} \\ & \div \\ & \text{ソフトウェアの平均単価} \\ & = \\ & \text{正規ソフトウェア総数} \end{aligned}$$

2011 年に IDC はソフトウェアの平均単価の計算の妥当性を確認するために、いくつかの対策を講じました。25 カ国のアナリストチームが、カテゴリ別とユーザ別（個人、企業）のソフトウェア価格および取得方法の種類（小売り、ボリュームライセンス、無償、オープンソースなど）の評価に関する情報を提供し、IDC の計算で得られた値のクロスチェックを実施しました。情報を集める国を毎年順番に変えることにより、ソフトウェア単価を定期的に見直すことで、業界が得た収益から正規ソフトウェアの総数をより正確に推定することが可能になります。

最後に、ソフトウェア総数から正規ソフトウェア総数を引けば、その年にインストールされた不正ソフトウェア総数が得られます。

$$\begin{aligned} & \text{インストールされたソフトウェア総数} \\ & - \\ & \text{正規ソフトウェア総数} \\ & = \\ & \text{不正ソフトウェア総数} \end{aligned}$$

このようなプロセスにより、基本的な不正コピー率を算出するための基礎データが得られます。

不正ソフトウェアの総額計算

不正ソフトウェアの総額は、不正ソフトウェアの使用規模を示す別の指標になり、ソフトウェアの使用状況の年ごとの変化を比較するうえで重要です。

総額は、IDC がソフトウェアの平均単価を求めるときと同じ価格カテゴリを使って計算します。つまり、小売り、ボリュームライセンス、OEM、無償、オープンソース、個人、企業などです。ソフトウェアの平均単価は、店舗での小売価格より低くなります。

インストールされたソフトウェアの総数、正規と不正のソフトウェアの数、ソフトウェアの平均単価がわかれば、不正ソフトウェアの総額が計算できます。



調査対象ソフトウェア

BSA グローバルソフトウェア調査では、PC 上で動作する不正ソフトウェアの数を算出します。PC には、デスクトップ、ラップトップのほか、ネットブックなどのより小型のポータブルデバイスが含まれます。

ソフトウェアには、オペレーティングシステム、システムソフトウェア（データベースやセキュリティのパッケージ）、業務用アプリケーション、および個人用アプリケーション（ゲーム、個人用資産管理、リファレンスソフトなど）が含まれます。調査は、正規の無償ソフトウェアおよびオープンソースソフトウェアが利用可能であることも考慮しています。オープンソースソフトウェアは、共通使用のためにパブリックドメインとしてライセンスされるものです。基本的には無償ですが、市販品の中で扱われることもあります。

一方、タブレットおよびスマートフォンにインストールされるソフトウェアは含まれません。さらに、サーバおよびメインフレーム上で動作するソフトウェア、ルーチン型のデバイスドライバや無料ダウンロードが可能なユーティリティ（スクリーンセーバなど）も含まれません。これらは、有償ソフトウェアに取って代わるものではなかったり、通常、ユーザがソフトウェアだと認識していなかったりするためです。

本調査では、PC にインストールされるソフトウェアに置き換わることが可能なサービス (SaaS) やパース (PaaS) などのクラウドコンピューティングサービスを含めています。また、ライセンス適法化プログラムの一環として、たとえば学校に配布するために政府にバルクで売られるようなソフトウェアも含めています。

為替レートの影響

2009 年以前の総額表に記載されているドルの値は、1 年前のレートで計算されていました。たとえば、2007 年の不正ソフトウェアの総額は、前年との比較を容易にするために 2006 年のレートで計算した値でした。2009 年に、BSA は調査した年の為替レートを使う方法に変更しました。このため、2009 年の総額は 2009 年のレート、2015 年の総額は 2015 年のレートで計算されました。以前の総額を現在のドルの値で再計算することはありません。

これは、時間経過に伴う総額の変化を評価する際に重要です。変化の一部は実際の市場の動的变化や年ごとの為替レートの変動に依存するためです。

たとえば、2013 年の不正ソフトウェア総額を、2013 年の為替レートの代わりに 2015 年の為替レートで米国ドルに換算すると、出版時の値より 13% 低くなります。

サイバーリスクから組織を適切に保護する

サイバーリスクの管理は複雑ですが、最初のステップが非常に重要です。企業の独自のネットワーク内で何がインストールされ実行されているかを把握し、ソフトウェアが正規品であり完全な使用許諾を得ていることを確認する作業です。

この最初のステップを実行しない場合、深刻な結果が生じる可能性があります。IDCの調査では、不正ソフトウェアの存在とマルウェアの攻撃を受ける可能性との間に強い正の相関が確認されました。

IDCの調査では、不正ソフトウェアの存在とマルウェアの攻撃を受ける可能性との間に強い正の相関が確認されました。

サイバーセキュリティのリスクは、2013年の拡大COSOフレームワーク（世界的に認められた内部統制の標準）に勧告が含められたほどの重大な懸念事項です。この勧告は、ソフトウェアライセンスのコンプライアンスを含め、テクノロジーの正規使用に関する内部統制を導入するよう企業に求めるものでした。

また、国際標準化機構（ISO）と国際電気標準会議（IEC）もSAMに特化した標準を発行しました。

SAMプログラムは不可欠なものです。SAMプログラムは、コンプライアンスを継続的に維持し、リスクにさらされることを最小限に抑え、この非常に重要な資産から最大限の利益を得ることができるような方法で、企業がソフトウェアを適切に管理できるよう設計されています。

今すぐに適用できる4つのステップから成る行動計画



**ステップ1：
評価を実施する**

適切に使用許諾を得ているかどうかを評価するために使用できる、信頼性のある一貫したデータを収集し、管理します。

- ネットワーク上で実行されているソフトウェアを見つけます。
- そのソフトウェアが必要かどうかを確認します。
- ネットワークで実行されているすべてのソフトウェアが正規品であり適切な使用許諾を得ているかどうかを確認します。



**ステップ2：
自社の事業ニーズに合わせる**

現在および将来の事業ニーズを適切なライセンスモデルに一致させます。

- クラウドのサブスクリプションなど、コスト効率が高くなる可能性がある新しいライセンス形式を調べます。
- 可能なコスト削減方法を確認します（ベンダーが許可する場合、ライセンスの再利用など）。
- ソフトウェア使用許諾契約の保守条項をより適切に活用し、費用に対して適切な価値が得られるようにします。



**ステップ3：
規程と手順を確立する**

企業のITライフサイクルに渡ってSAMが役割を果たすようにします。ISOに準じたSAMを効果のあるものにするには、企業のITインフラストラクチャをサポートする手法と、SAMプロセスをサポートする管理が必要です。

- ソフトウェアの実行基盤となるプラットフォームの選択をサポートする記録と、調達プロセスをサポートする記録を使って、管理された方法でソフトウェアを取得します。
- 企業内にインストールされたソフトウェアの現在の保守もサポートする管理された方法でソフトウェアをインストールします。
- 使用しなくなったハードウェアからソフトウェアを削除し、企業内ですべてのライセンスを適切に再配置します。
- ソフトウェアパッチを定期的にインストールし、アップグレードを適切なタイミングで実行します。



**ステップ4：
事業に統合する**

SAMが事業全体に統合され、サポートすることを確認します。

- ITのライフサイクルだけでなく、企業内の関連するすべてのライフサイクル活動にSAMを組み入れます。
- ステップ1で構築したデータ管理プロセスを改良します。
- ソフトウェアの適切な使用方法のほか、ソフトウェアに関する行動が組織に与える影響（法的、財務的、評判上の影響）を従業員が確実に理解するようにします。

BSA | The Software Alliance (BSA | ザ・ソフトウェア・アライアンス) 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・ソリューションを創造しています。

ワシントン DC に本部を構え、世界 60 カ国以上で活動する BSA は、正規ソフトウェアの使用を促進するコンプライアンスプログラムの開発、技術革新の発展とデジタル経済の成長を推進する公共政策の支援に取り組んでいます。



www.bsa.org

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