ソフトウェア管理：セキュリティ責務と新たなビジネス機会

BSA
グローバル
ソフトウェア調査
2018年6月

目次

はじめに

世界的に、販売追跡、帳簿管理、市場ターゲット選定、顧客とのコミュニケーション、パートナーとの協業、更には生産性の向上など、企業が日常業務を実行する上で、ソフトウェアは最も広く使用される不可欠なツールになっています。躍進的な技術の発展により、ソフトウェアの能力は一層高まっており、各種組織ではこれまで以上にソフトウェアを媒介に、ビジネスの仕方を改善し、収益を向上し、そして競争力を強化しています。

一方で、現状、ユーザーが最先端テクノロジーを活用しようと試みても、マルウェアの侵入を含めたセキュリティ上の脅威に直面しています。マルウェアの感染にはライセンスのない不正ソフトウェアの使用が深く関連していることが、次第に明確になっています。そのため、多くのCIOは、ライセンスのない不正ソフトウェアの使用が費用を増大させることを認識し始め、ソフトウェア管理の改善のための現実的な対策措置を講じています。

こうした問題が引き起こす影響や経済的機会の損失を把握するため、BSAがIDCとの協力で実施した「グローバルソフトウェア調査」では、世界の110以上の国や地域のパーソナルコンピューターにインストールされているライセンスのない不正ソフトウェアの数と資産価値について、定量的に調査を実施しました。その結果、数多くのCIOは、ライセンスのない不正ソフトウェアの使用がセキュリティ上のリスクを生じさせている事を理解しているにもかかわらず、今なおパーソナル コンピューターにインストールされているソフトウェアの37%もが、ライセンスの許諾を得ていない不正使用でした。

この報告によると、サイバー攻撃上のセキュリティリスクが話題となっている今日、組織は自らのネットワークにあるソフトウェアを再評価し、ライセンスのな

主要なトレンドと調査結果

- 不正ソフトウェアの使用は、わずかながら減少していますが、まだまだ蔓延しています。
- CIOは、不正ソフトウェアはリスクをともない、費用がかかることに既に気が付いています。
- ソフトウェア規則の遵守は、今や経済の発展を可能にする要因であり、セキュリティ上の必須の課題です。
- 今日、組織はソフトウェア管理を改善し、重要な利益を得るために意義あるステップを取ることが不可欠です。

不正ソフトウェアの使用に関する詳細な分析から、ソフトウェアの管理方法を改善するために強力な対策を実施している企業は、セキュリティリスクを低減し、収益性を向上し、且つ使用停止時間を短縮しながら、ビジネスの機会を増やすための強力な新しいツールを導入していることがわかりました。

主要な発見

い不正使用を取り除く対策を、重要な最初のステップとして実行しなければならない事は、明らかです。そうすることで、有害なサイバー攻撃のリスクを低減し、収益向上につなげることができます。

ライセンス許諾を得ていないソフトウェアは、わずかながら減少しているものの、依然として広く使用されているのが現状です。世界的には、この2年間で不正ソフトウェアのインストールは2ポイント減少していますが、今もこうしたソフトウェアの使用は世界規模で広く見られ、パーソナル コンピューターの37%にインストールされています。ライセンスのない不正ソフトウェアの商業的な価値も全般的には低下していますが、調査対象となった国々の過半数では、ライセンスのない不正ソフトウェアのインストール率が、いまだに50%を超えています。この高い不正使用比率のために、定評あるテクノロジーを利用する事で得られる経済的な価値の提供が遅延しているだけでなく、企業の収益向上を妨げ、次なるセキュリティリスクをも内包しています。

CIOは、ライセンスのない不正ソフトウェアはリスクがあり、費用がかかることに既に気付いています。現在、組織がライセンスのない不正ソフトウェアの パッケージを入手またはインストール、あるいは不正ソフトウェアが入っているパーソナル コンピューターを購入すると、3回に1回はマルウェアに遭遇する危険性があります。マルウェアの攻撃を受けると、その企業の経済的な損失は平均で240万ドルにものぼり、解消までには50日を要します。感染することで、その会社の業務が中断するだけでなく、ビジネスのデータが失われる場合もあるので、企業のブランドや評判にも深刻な影響を及ぼします。ライセンスのない不正ソフトウェアに関連するマルウェアが引き起こすコスト自体も、増大しています。今では感染したコンピューター1台につき、その企業のコスト負担は10,000ドルを超え、全世界の企業数で合算すると、そのコストは毎年3,590億ドル前後にも達します。現在、CIOが自社のネットワーク上で使用するソフトウェアを完全にライセンスが付与されたものに転換する第一の理由は、マルウェアによるセキュリティ上の脅威を回避するためです。

ソフトウェア規則の遵守は、今や、経済的な発展を可能にする大きな要因であり、セキュリティ上の必須の課題でもあります。マルウェアの被害に関連したコストが増大する中、ビジネスリーダーたちは完全にライセンスが付与され、最新バージョンにアップデート可能なソフトウェアを採用するようになってきました。こうしたバージョンアップの更新は、深刻なマルウェアの侵入やデータの漏えい、その他のセキュリティ リスクに対する主要な防御措置となっています。更に、組織全体のソフトウェアの管理能力を強化することで、利用停止時間を短縮し、大幅な収益向上を可能にできる事を理解するリーダーたちが増えています。実際、IDCは、企業が現実的な処置を講じてソフトウェア管理を向上させれば、収益を最大で11%向上させることができると推定しています。

組織は有効な措置を施すことで、ソフトウェア管理を向上させ、大きな利益を上げることができます。こうした利益享受を目的に、企業はソフトウェア資産管理（SAM）のベストプラクティスを実施することで、ソフトウェア資産管理を強化し、テクノロジーをさらに活用することが可能になります。SAMにより、CIOは、自社のネットワーク上で使用しているソフトウェアがすべて完全にライセンスが付与された、合法的なものであることを確認できるだけでなく、疲弊を伴うサイバーリスクを低減し、生産性を向上し、利用停止時間

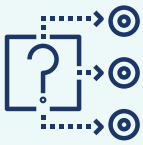
を低減させ、更にはライセンス管理を集中化してコストを削減できます。幾つかの調査によれば、頑強なSAMとソフトウェア ライセンスの最適化プログラムを実施すれば、組織の年間ソフトウェア経費は最大で30%ほど削減できることが、わかっています。[1]

マルウェアの脅威は今では、史上最大のレベルに達しています。日々、毎秒、新たな8つの脅威が発生しています。

マルウェアのインパクト

企業が不正ソフトウェアを入手またはインストールする際に、およそ3回に1回の確率でマルウェアに遭遇しています。

不正ソフトウェアに関わるマルウェアの対処には、感染したコンピューター1台当たり10,000ドル以上の費用がかかり、世界全体では3590億ドル以上になります。



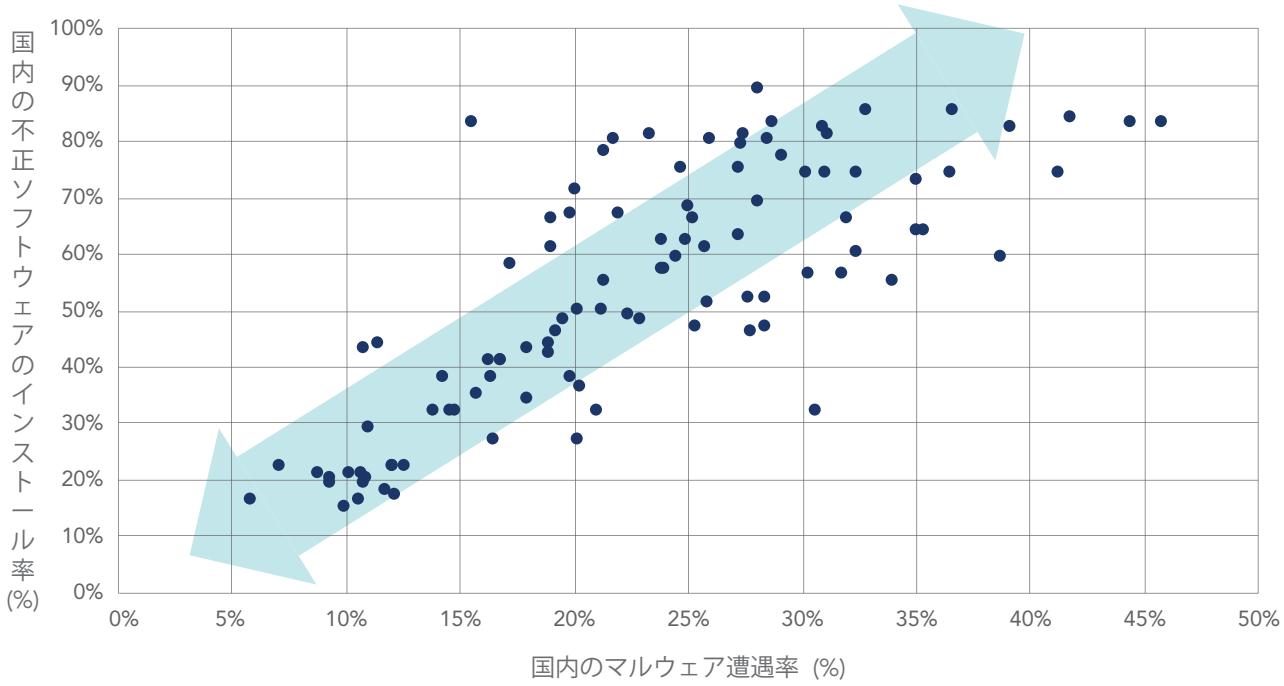
ユーザの68%とCIOの48%が、不正ソフトウェアを使用しない主な3つの理由の1つにマルウェアを選択しています。

CIOは、不正ソフトウェアにおけるマルウェアの脅威の最大の懸念事項に、企業や個人のデータの喪失、システムの停止、ネットワークの停止、システムのマルウェア駆除コストなどを上げています。

これらの影響を軽減するために、ライセンスソフトウェアの使用に関して正式な書面によるポリシーを表明しているCIOの数は、2015年度の41%から今年度は54%に急増しています。しかし、雇用者は35%しか正式な書面によるポリシーを認識しておらず、このことは教育上の重大なギャップを示唆しています。

プロアクティブな取り組みを進めている企業は、ソフトウェアコンプライアンスを20%増加させることで企業の利益を11%向上させることができるとしています。これは調査対象となった平均的なサイズの企業において50万ドル以上増加することを意味します。

不正ソフトウェアの使用とマルウェアとの遭遇には強い関連性がある



出典: IDC

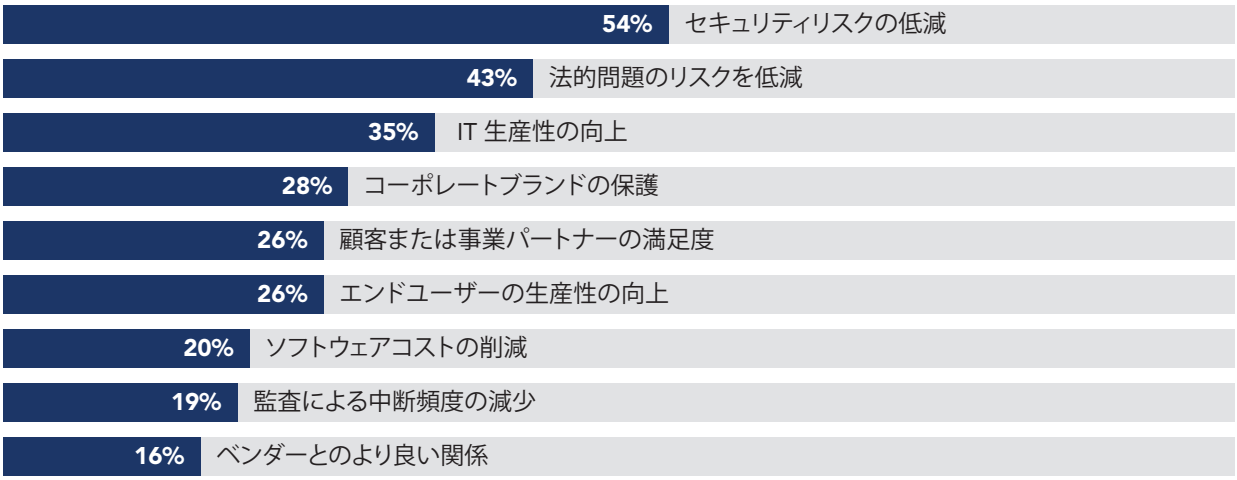
マルウェアによる侵略性、経費、消耗性は、増大し続けています。

全世界の消費者、企業、および国々は、最新テクノロジーの潜在能力を管理し活用しようとする試みが、マルウェアの潜在的かつ深刻な脅威により妨げられていることをますます実感しています。こうしたマルウェアの脅威は今では、史上最大のレベルに達しています。日々、毎秒、新しい8つの脅威が発生しています。[2] マルウェアの発生頻度が高まるだけでなく、その破壊力も強大化しています。そして、対応に要する費用もリソースも増大しています。

マルウェアによる攻撃は、頻度も攻撃の巧妙性も増しています。[3] 例として2016年には、データ漏えいが15件発生し、1,000万以上のIDが盗難に遭遇しました。2013年の件数と比較すると、ほぼ二倍に増えています。[4] こうした攻撃は大企業だけではなく、あらゆる規模の企業や消費者に及んでいます。実際、2015年には世界のサイバー攻撃の43%は、従業員数が250人未満の小規模な企業に対するものでした。[5] サイバー犯罪者たちは、モバイル ネットワークをも攻撃対象にしています。モバイル デバイス用の各種マルウェアは、昨年、54%も増大し、毎日24,000件もの有害なモバイル アプリがブロックされています。[6]

更に、そうした攻撃がもたらす被害金額も増大しています。マルウェア攻撃を受けると、企業は平均で240万ドルの損失を被ります。[7] 感染すると、その度に業務に使用停止時間が生じて利益を失い、生産性が低下し、そして、ビジネス機会喪失となり、被害を緩和するために追加のIT人件費が必要になります。感染により使用停止時間が生じたり、ビジネス データが喪失することから、企業のブランドや評判に深刻な被害をもたらします。その上、困ったことには、こうした感染による経済的コストは増大を続けており、2014年比では20%増加しています。マルウェア関連の対策のため、今では全世界で、毎年6,000億ドルもの金額が費やされています。これは、全世界のGDPの0.8%に相当します。[8]

CIOは、強力なソフトウェアコンプライアンスから得られる最大の利点を報告



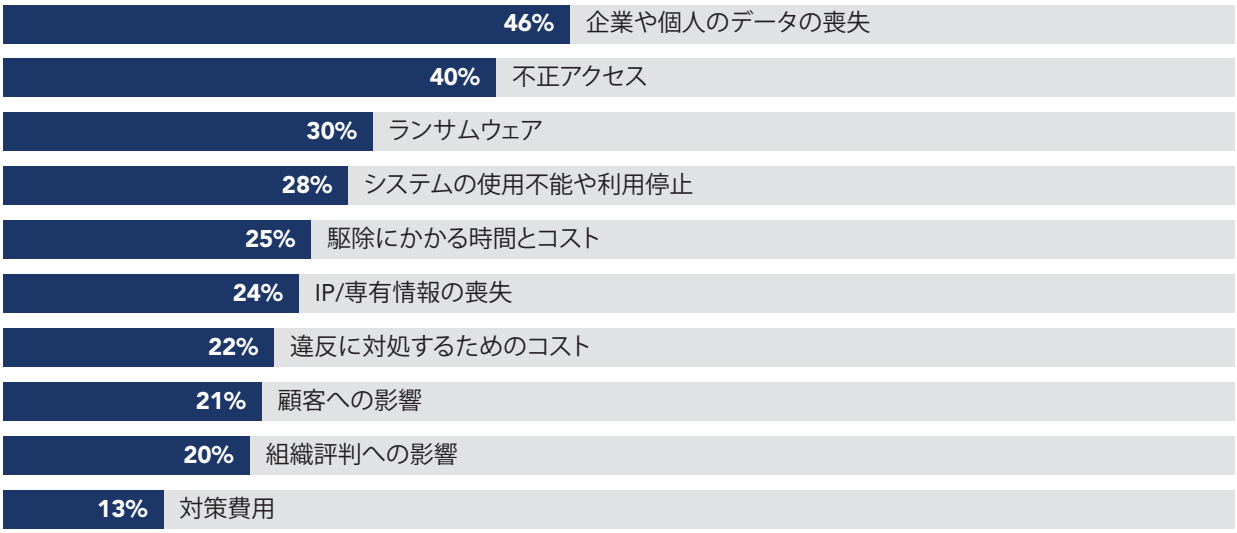
対策をさらに難しくしている要因として、マルウェア攻撃は検出も解消も困難なものが多いのです。組織が１件のマルウェア攻撃を検出するためには、平均で243日かかり、[9] 解決するためには、最大で50日を要します。[10]

(5ページに続く)

マルウェア感染は、ライセンスのない不正ソフトウェアに関連

マルウェア感染がライセンスのない不正ソフトウェアの使用と密接に結びついていることは、次第に明らかになりつつあります。ライセンスのない不正ソフトウェアの使用率が高いほど、大きな被害を及ぼすマルウェアへ感染する確率も高くなります。

企業は、不正ソフトウェアからのマルウェアの影響を最も懸念



しかし、確かな関連性にも関わらず、ライセンスのない不正ソフトウェアの使用は、今も驚くほど一般的に広がっています。世界的に、ソフトウェアの多くがライセンスが付与されていない状況で使用されています。実に6つの地域のうち4つ、つまりアジア太平洋、中央・東ヨーロッパ、中東・アフリカ、ラテン アメリカで、パーソナル コンピューターに搭載されているソフトウェアの過半数はライセンス許諾を得ていません。(12-13ページ参照)

ライセンスのない不正ソフトウェアとマルウェア感染とのつながりを考えると、これは深刻なサイバー攻撃のリスクです。IDCの推定によれば、ライセンスのない不正パッケージ ソフトウェアを入手したり、そうしたソフトの入っているコンピューターを購入する組織がマルウェア被害にあう確率は、1/3 (29%) にも達します。

その関連性は、統計的に証明されています。世界の国々で、ライセンスのない不正ソフトウェアの使用とマルウェアとの遭遇との間には、一貫した相関関係があります(r-0.78)。実際のところ、ある国でどの程度のマルウェア感染があるかは、その国でライセンス付与のない不正ソフトウェアがどの程度広く使用されているかで、予想できるのです。

CIOは、この関連性を既に理解しています。強固なソフトウェア ライセンス管理とコンプライアンスを実施することの最大の利点は何かという質問に対して、CIOの54%が 、完全にライセンスされたソフトウェアを使用する第一の理由として、セキュリティ リスクの低減を挙げています。

CIOは、マルウェアとライセンスのない 不正ソフトウェアの関連性を最も懸念しています。これには、正当な理由があります。マルウェア感染による被害がいかに深刻かを、CIOは直接的に理解しているのです。調査対象となったCIOは、ライセンスのない不正ソフトウェアに付きまとうマルウェアに関連する第一の懸念事項として、データの盗難を挙げています (46%)。更に、自社のネットワークへの不法アクセス (40%) や、ランサムウェアの可能性への対処 (30%)、システムの使用不能や停止時間 (28%)、ネットワークの感染を防止するための時間と費用 (25%) も理由として挙げています。またCIOは、こうした被害が1回きりのものとは限らないことも、理解しています。実際、この調査対象の5社に1社 (19%) は、2~3か月に一度はネットワーク、ウェブサイト、コンピューターの使用不能を経験していると回答しています。そして、セキュリティに関連した使用不能の原因として、最も多いものは、エンドユーザーのコンピュー

ソフトウェアの規則の遵守は今や、経済の発展を可能にする要因であり、セキュリティ上の必須の課題でもあります。

ターからのマルウェアでした（56%）。ライセンスのない不正ソフトウェアは、たびたび攻撃される対象となります。

上述のように、こうした事態が発生すると、破壊的な被害を招きます。今では1つの企業がサイバー攻撃とその事後処理に要する費用は、感染したコンピューター1台当たり10,000ドルを超えています。従って、ライセンスが付与されたソフトウェアを入手する費用の何百倍もの費用になります。コンピューター自体の価格よりも、はるかに大きなものです。IDCの推定では、ライセンスのない不正ソフトウェアに関連する企業のマルウェア対策には、年間で3,600億ドル近くがかかります。

マルウェアのリスク、深刻な現実問題に発展

ソフトウェア資産管理を行わず、ライセンスのない不正ソフトウェアを使用したことで、世界的に巨大なセキュリティ上の悪影響が発生しています。ライセンスのない不正ソフトウェアの使用率が高い国々では、特に顕著です。例えば、

- 中国では使用されているソフトウェアの何と66%に正規のライセンスがありません。そのため、他国よりも深刻なマルウェア攻撃を経験しており、機能不全にまで陥る体験をした中国の組織は、40,000と推定されています。例えば、ある1つのマルウェア攻撃が、パッチできない、且つライセンスのないソフトウェアに急速に広がっています。清華大学のような高名な研究機関が機能不全に陥り、また中国石油公司の全中国のガソリンスタンドで電子支払いシステムが停止し、中国銀行のATMがダウンし、更には中国電信や海南航空など大手企業の業務にも悪影響が出るなど、その数は枚挙にいとまがありません。フィンランドのサイバーセキュリティ企業F-Secure の報告によれば、中国にはライセンスのない不正ソフトウェアを使用しているコンピューターが多数あり、この破壊的な攻撃を広げてしまいました。[11] 北京に本社のあるテクノロジー企業のシニアネットワーク エンジニアの指摘によれば、「中国でのこの攻撃の被害者の大半は、ライセンスを得ていない不正ユーザーでした」[12]
- ロシアもライセンスのない不正ソフトウェアの使用率が62%と高く、しかもその商業価値は12億ドルと大きく、最近、あるマルウェア攻撃で大変な被害を体験しました。2017年、マルウェア攻撃のためロシア保健省がマヒし、国営のロシア鉄道、警察を運営する内務省、テレコム企業のメガフォンなども次々と機能不全に陥りました。プラハ国際関係研究所の上級研究員の指摘によれば、ロシアでこのマルウェア感染が拡大したのは、「旧式のソフトウェアを使っ

ていただけでなく、旧式の海賊版を使用していたことによる」とのこと。

ビジネスの重要な機能に不正ソフトウェアを使っている人たち、ソフトウェア資産管理システムを配備していない人たち、そしてライセンスのない不正ソフトウェアに関連するマルウェアに感染するリスクのある人たちに依存している組織は、こうした脅威の範囲と影響の大きさに警鐘を鳴らすべきです。




ライセンスのないPCソフトウェアのインストール率と商業価値

アジア太平洋							
	18%	20%	21%	23%	$540	$579	$743	$763
	84%	86%	87%	90%	$226	$236	$197	$147
	64%	66%	66%	67%	$18	$19	$13	$25
	66%	70%	74%	77%	$6,842	$8,657	$8,767	$8,902
	38%	41%	43%	43%	$277	$320	$316	$232
	56%	58%	60%	63%	$2,474	$2,684	$2,911	$2,930
	83%	84%	84%	86%	$1,095	$1,145	$1,463	$1,467
	16%	18%	19%	21%	$982	$994	$1,349	$1,875
	51%	53%	54%	55%	$395	$456	$616	$657
	16%	18%	20%	22%	$62	$66	$78	$99
	83%	84%	85%	86%	$267	$276	$344	$278
	64%	67%	69%	70%	$388	$431	$444	$338
	27%	30%	32%	33%	$235	$290	$344	$255
	32%	35%	38%	40%	$598	$657	$712	$815
	77%	79%	83%	84%	$138	$163	$187	$86
	34%	36%	38%	37%	$254	$264	$305	$293
	66%	69%	71%	72%	$714	$738	$869	$852
	74%	78%	81%	81%	$492	$598	$620	$395
その他のアジア太平洋諸国	87%	87%	91%	91%	$442	$491	$763	$589
アジア太平洋諸国合計	**57%**	**61%**	**62%**	**60%**	**$16,439**	**$19,064**	**$21,041**	**$20,998**
中央・東ヨーロッパ							
	74%	73%	75%	75%	$10	$10	$10	$6
	85%	86%	86%	88%	$17	$18	$26	$26
	81%	84%	85%	87%	$50	$90	$103	$67
	82%	85%	86%	87%	$59	$76	$173	$87
	61%	63%	65%	66%	$24	$24	$21	$15
	57%	60%	63%	64%	$72	$78	$101	$102
	50%	51%	52%	53%	$48	$49	$64	$74
	32%	33%	34%	35%	$149	$150	$182	$214
	41%	42%	47%	48%	$16	$16	$20	$25
	63%	64%	65%	66%	$15	$15	$19	$22
	81%	84%	90%	91%	$22	$25	$40	$52
	36%	38%	39%	41%	$104	$107	$127	$143
	74%	73%	74%	76%	$62	$89	$136	$123
	48%	49%	53%	54%	$22	$23	$29	$32
	50%	51%	53%	54%	$35	$37	$47	$44
	83%	86%	90%	90%	$35	$36	$57	$45
	74%	76%	78%	79%	$6	$6	$7	$7
	46%	48%	51%	53%	$415	$447	$563	$618
	59%	60%	62%	63%	$151	$161	$208	$207
	62%	64%	62%	63%	$1,291	$1,341	$2,658	$3,227
	66%	67%	69%	72%	$51	$54	$70	$104
	35%	36%	37%	40%	$51	$55	$67	$68
	41%	43%	45%	46%	$28	$30	$41	$51
	80%	82%	83%	84%	$108	$129	$444	$647
その他の中央・東ヨーロッパ諸国	86%	87%	89%	90%	$69	$70	$105	$127
中央・東ヨーロッパ合計	**57%**	**58%**	**61%**	**62%**	**$2,910**	**$3,136**	**$5,318**	**$6,133**
ラテンアメリカ							
	67%	69%	69%	69%	$308	$554	$950	$657
	79%	79%	79%	79%	$94	$98	$95	$59
	46%	47%	50%	53%	$1,665	$1,770	$2,851	$2,848
	55%	57%	59%	61%	$283	$296	$378	$382
	48%	50%	52%	53%	$241	$281	$396	$295
	58%	59%	59%	58%	$80	$90	$98	$62
	75%	76%	75%	76%	$74	$84	$73	$93
	68%	68%	68%	68%	$132	$137	$130	$92
	80%	81%	80%	80%	$61	$63	$72	$58
	78%	79%	79%	79%	$165	$169	$167	$116
	75%	75%	74%	73%	$32	$36	$38	$24
	49%	52%	54%	57%	$760	$980	$1,211	$1,249
	81%	82%	82%	79%	$20	$23	$23	$9
	71%	72%	72%	72%	$112	$117	$120	$74
	83%	84%	84%	83%	$76	$89	$115	$73
	62%	63%	65%	67%	$190	$210	$249	$209
	67%	68%	68%	68%	$51	$57	$74	$85
	89%	88%	88%	88%	$317	$402	$1,030	$668
その他のラテンアメリカ諸国	82%	83%	84%	84%	$296	$331	$352	$406
ラテンアメリカ合計	**52%**	**55%**	**59%**	**61%**	**$4,957**	**$5,787**	**$8,422**	**$7,459**

中東・アフリカ								
	82%	83%	85%	84%	$70	$84	$102	$83
	52%	54%	53%	54%	$32	$34	$27	$23
	80%	79%	79%	80%	$22	$23	$20	$16
	80%	82%	82%	83%	$20	$21	$9	$9
	59%	61%	62%	61%	$64	$157	$198	$172
	85%	85%	86%	86%	$107	$120	$116	$172
	27%	29%	30%	31%	$165	$161	$177	$192
	79%	80%	80%	81%	$21	$22	$24	$16
	55%	56%	57%	58%	$32	$34	$35	$31
	74%	76%	78%	78%	$99	$113	$128	$85
	57%	58%	58%	59%	$86	$94	$97	$72
	69%	70%	71%	71%	$61	$65	$65	$52
	90%	90%	89%	90%	$66	$65	$50	$60
	52%	54%	55%	57%	$6	$7	$7	$7
	64%	65%	66%	66%	$52	$57	$69	$91
	80%	80%	81%	82%	$123	$232	$287	$251
	60%	60%	60%	61%	$56	$59	$65	$36
	47%	48%	49%	50%	$64	$72	$77	$62
	38%	39%	39%	40%	$2	$2	$1	$1
	47%	49%	50%	51%	$356	$412	$421	$449
	74%	75%	77%	78%	$12	$12	$9	$9
	32%	33%	34%	35%	$241	$274	$385	$564
	73%	74%	75%	74%	$39	$49	$66	$51
	56%	58%	60%	62%	$208	$291	$504	$526
	32%	34%	36%	37%	$210	$226	$230	$208
	88%	87%	87%	89%	$10	$11	$9	$15
	80%	81%	81%	82%	$4	$4	$3	$3
	89%	90%	91%	92%	$7	$7	$4	$4
	83%	84%	85%	86%	$364	$419	$484	$363
	85%	84%	85%	87%	$478	$569	$640	$536
中東・アフリカ合計	**56%**	**57%**	**59%**	**58%**	**$3,077**	**$3,696**	**$4,309**	**$4,159**
北米								
	22%	24%	25%	27%	$819	$893	$1,089	$1,141
	41%	41%	42%	42%	$27	$28	$27	$44
	15%	17%	18%	19%	$8,612	$9,095	$9,737	$9,773
北米合計	**16%**	**17%**	**19%**	**19%**	**$9,458**	**$10,016**	**$10,853**	**$10,958**
西ヨーロッパ								
	19%	21%	22%	23%	$121	$131	$173	$226
	22%	23%	24%	24%	$182	$190	$237	$252
	44%	45%	47%	48%	$14	$14	$19	$19
	20%	22%	23%	24%	$167	$176	$224	$222
	22%	24%	24%	25%	$166	$171	$208	$210
	32%	34%	36%	37%	$1,996	$2,101	$2,685	$2,754
	20%	22%	24%	26%	$1,566	$1,720	$2,158	$2,265
	61%	63%	62%	61%	$173	$189	$220	$343
	44%	46%	48%	48%	$12	$10	$12	$17
	29%	32%	33%	34%	$79	$87	$107	$144
	43%	45%	47%	48%	$1,278	$1,341	$1,747	$1,945
	17%	19%	20%	20%	$20	$21	$30	$33
	43%	44%	44%	43%	$4	$4	$5	$7
	22%	24%	25%	27%	$448	$481	$584	$644
	21%	23%	25%	27%	$159	$178	$248	$289
	38%	39%	40%	40%	$137	$145	$180	$245
	42%	44%	45%	44%	$859	$913	$1,044	$1,216
	19%	21%	23%	24%	$260	$288	$397	$461
	21%	23%	24%	25%	$399	$448	$469	$514
	21%	22%	24%	26%	$1,421	$1,935	$2,019	$1,943
西ヨーロッパ合計	**26%**	**28%**	**29%**	**32%**	**$9,461**	**$10,543**	**$12,766**	**$13,749**
全世界合計	**37%**	**39%**	**43%**	**42%**	**$46,302**	**$52,242**	**$62,709**	**$63,456**

ソフトウェア資産管理により、サイバーリスクを低減し収益を向上

完全なライセンス許諾のあるソフトウェアだけを使用すれば、サイバーリスクを低減できることは、明白です。その対策として、国際的に認められた「標準」もあります。国際標準化機構（ISO）では最近、SAMを改定しましたが、それはソフトウェアも含むIT資産管理（ITAM）全般の枠組みとなるものです。[14]

最近の実例が示すように、ISOに準拠したSAMは、セキュリティ強化のための強力なツールです。アメリカではEquifax社が、数か月前から自社のサーバーの1つに脆弱性があることを知りながら、その修正を怠り、史上最大級のデータ漏えいを招きました。同社が被った被害は推定で4億3,900万ドルにのぼり、同社のCEOとCIOが辞任に陥る結果となりました。[15] 専門家による報告によれば、同社がSAMのシステムを使用してApacheソフトウェアの全ての実態を追跡していれば、この漏えいは回避できたであろう、とのことです。[16] 不正ソフトウェアの使用を避けることでマルウェアとの接触を最小限に抑えることは重要ですが、この実例から分かるように、ライセンスが正しく付与されたソフトを使っている場合でも、適切なSAMシステム管理を配備しておくことは不可欠です。

SAMがあると、ソフトウェアが完全なライセンスを受けており、しかもビジネスのニーズに合致して最適化されていることを確認できますので、使用停止時間の削減と収益向上という形で、利益につながります。更に、SAMは、企業が使用しているソフトウェアがビジネスのニーズに最適であることを確認し、またクラウド サービスなどの新しいテクノロジーを活用するので、企業としてはソフトウェアを最大限に活用できます。これらを併用すれば、組織は効率性を向上させ、コストも削減できます。頑強なSAMプログラムを導入すれば、組織は年間のソフトウェア関連費用を30%も削減できることが、各種の研究から判明しています。[17]

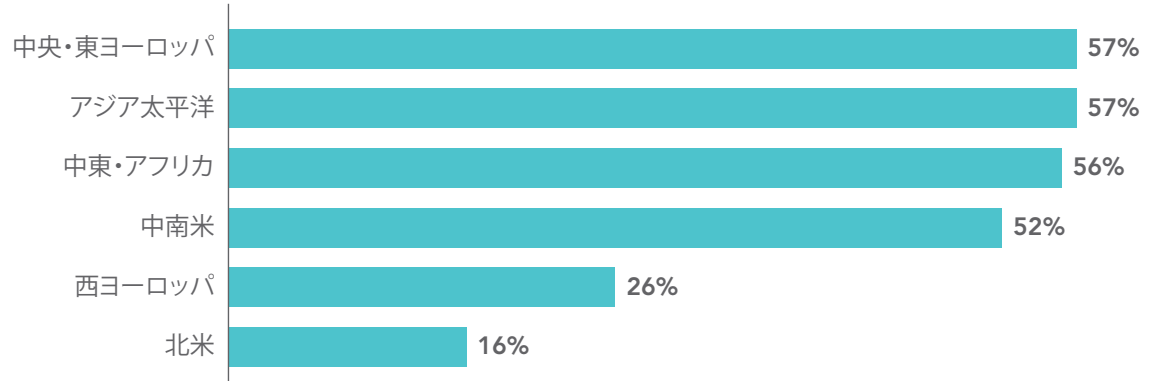
この調査から、SAMには投資するだけの価値が十分あることも判明しています。回答者情報に基づきIDCが試算したところ、ソフトウェアのコンプライアンス率を20%向上する（例えば、ライセンスのないソフトの比率を24%から19%に下げる）だけで、年間収益が8,300万ドルの企業であれば（調査対象企業の平均）利益を何と11%も伸ばせることが判明しました。こうした目を見張る採算性の向上は、ソフトウェアのコンプライアンス率を20%高めるために必要な経費の29倍に相当します。[18]

世界に広がる実例

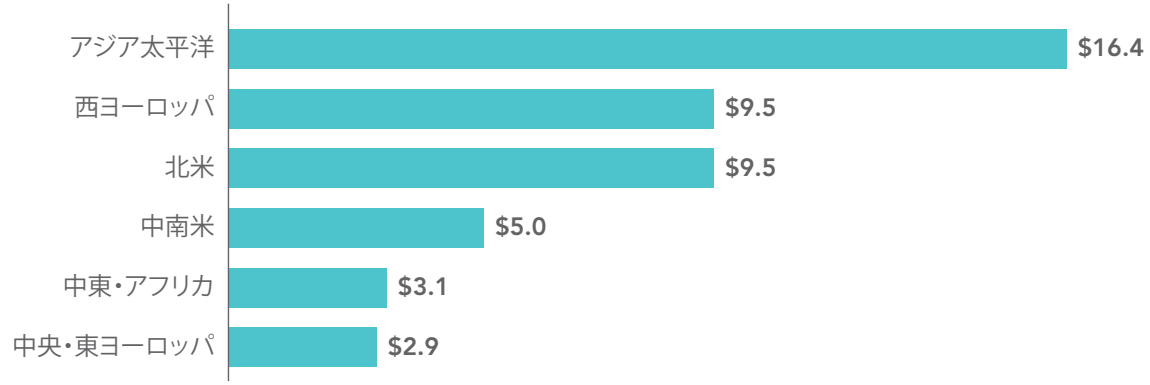
ドイツでの例：

OSIインターナショナル フーズは、12,000人を超える従業員数を誇る企業ですが、ソフトウェアのより効果的なライセンス取得モデルを実施することで、ライセンス取得後のコストを30%以上削減しました。[19]

ライセンスのないソフトウェア使用率の平均値



ライセンスのないソフトウェア使用の商業価値（10億ドル）



ロシアでの例：

バルティカ ブリューワリーズは、8つの醸造所を有するロシアの大手ビールメーカーで、物理的サービスとクラウド サービスの両方を組み合わせています。同社ではSAMプログラムを開始してITインフラの最適化を実施。ビジネス用アプリケーションをクラウドに移すことで、年間100,000ドルを節約しました。[20]

英国での例：

ロンドンにあるレハンプト大学では、SAMプロジェクトに基づいてロードマップを作成し、もはや使用していない従来からのソフトウェアと、ライセンス期間を超えたソフトウェアを特定しました。これにより同大学では経費を節約。新しいバージョンで能力が高く、且つセキュリティにも優れたテクノロジーへの投資に充てました。このプロジェクトの全工程期間で、500万ドルを節約できるものと見積っています。[21]

アメリカでの例：

政府機関にも利点。例えばNASAでは、各部署でSAMのベスト プラクティスを導入し、この6年間で1億ドル以上を節約しています。[22] NASAでは、デジタル化を事業全体に導入することで、わずかな先行投資でより大きな利点を得ることができました。市民からの税金を節約したことになります。

第1段階

信頼できるデータ

第1段階は、自社が保有するものを完全に把握し、包括的に管理できるようにします。まず、ソフトウェアライセンス契約を遵守できるように、システム上のソフトウェアを評価します。ライセンス管理に加えて、この段階を経ることで組織は変更管理、データ管理、セキュリティ管理に必要なプロセスの開発が可能です。

第2段階

ライフサイクル インテグレーション

第2段階は、第1段階を踏まえ、仕様、取得、展開、リリース、導入、運用、廃棄までIT資産のライフサイクル全体にわたる管理を改善することで、企業の効率性とコスト効率の向上に役立ちます。

第3段階

最適化

第3段階は、契約や財務管理などの部門ごとに焦点を当てることで、企業の効率性とコスト効率の向上に役立ちます。

政府機関が行えるステップ

最新の技術に主導される進歩を最大限に活用する企業に起因する膨大な新規雇用、税の拡大、経済的利益を享受するために、政府機関はライセンスされていないソフトウェアの使用率を減少させ、経済セクターにより高い弾力性をもたらす共通理解と具体的な手順を示すことができます。

1 模範を示して指導する。

政府機関は世界最大のソフトウェアユーザーです。すべての組織と同様、リスクを低減し、技術的説明責任を強化し、SAMプラクティスを採用することで利益を得ることができます。政府はまた、国有企業、請負業者、サプライヤーの間でSAMとライセンスソフトウェアの使用を促進することができます。

2 教育と認知の向上。

政府機関、会計および監査の専門家、業界のコンサルタント、事業者団体、ビジネス組織は、ソフトウェアライセンスの規則遵守とライセンスのないソフトウェアをインストールし使用することの危険性について組織に対して教育する必要があります。

3 法律の現代化で新たな技術革新を主導。

クラウドコンピューティングの登場とネットワーク化されたモバイルデバイスの普及により、ソフトウェアは革新的な新しい方法で保管、提供、そして使用されています。政策立案者は形式や提供方法にかかわらず、それらの保護を保証すべきです。

4 権利行使を助成する環境作り。

政府は法的枠組みが救済のための効果的手段となることを確実にし、ソフトウェアの著作権侵害を減少させるように、ステークホルダー間の協力を促進すべきです。

ソフトウェアの利点を拡大して享受するため、政府が現実的な処置を講ずることが可能に

政府は、実施できる、また実施すべき各種の措置に加えて、権限の範囲内で常識的で具体的な段階を踏襲しながら、ライセンス許諾のない不正ソフトウェアの比率を下げ、そして政府内の経済関連部門の緊急時の際の回復能力を高めることができます。こうした政府主導のプロアクティブな試み（15ページで詳細説明）としては、模範例の提示・共有、ソフトウェア資産管理の向上、契約のある政府関連機関における合法的なソフトウェア使用など、が挙げられます。

政府によるこうした動きを支援するため、BSAでは便利なガイドを作成しました。政府が自らのソフトウェア資産管理を向上させるために活用できます。[23]
政府自らが、合法的なソフトウェアしか使用しないこと、また合法的なソフトウェアのみを使用している企業としか契約を締結しないことを明示することで、民間・公共の両部門において合法的なソフトウェアを使用する動きを強固に、且つ明確に誘導できます。

グローバルなトレンド

全世界で、何年にも渡る啓蒙・教育活動と法執行、そしてソフトウェア資産管理の利点に関する啓蒙・教育活動の進展により、ライセンスのない不正ソフトウェアの使用が、幾分減少しています。2015年から2017年にかけて、世界での不正ソフトウェアの比率は2%減少し、39%から37%になりました。ライセンス許諾の無い不正ソフトウェアの商業価値は、通貨ベースで、世界では8%下落し、463億ドルになりました。

不正ソフトウェア使用率の低下の一因としては、PCの出荷量の減少もありますが、IDCの推定によると低下分のおよそ60%は、ソフトウェアに関するコンプライアンスの強化によるものです。この数値から、ソフトウェアを取り巻くコンプライアンス強化がビジネスにとっても有益である事を理解している人が、今では多くなっていることが窺えます。こうした進展にも関わらず、調査対象となった各市場に出回っているソフトウェアの過半数は ライセンスのないものです。継続した一層の努力が必要なことは、明らかです。

全ての地域でライセンスのない不正ソフトウェアの使用比率は低下したものの、著しい低下は新興市場以外で顕著でした。一方、新興市場での不正ソフトウェアの使用比率は、異常とも言える61%に達しています。こうした市場が世界のライセンスのない不正ソフトウェアで占める比率は、2015年の70%から、2017年には75%に拡大しています。

世界レベルでは、不正ソフトウェアの使用比率は、101の市場で低下しており、拡大したのは6つの市場だけでした。2017年、この比率は12の国では3%減少しました。[24] 中国とベトナムでは4ポイント低下していますが、この両国は当初、不正ソフトウェアの比率が高い状況でした。2017年のその比率を2015年の比率で割った数値率で見ると、最大の減少は先進国で見られ、米国、オーストラリア、オーストリア、日本、ルクセンブルグ、ニュージーランド、シンガポール、スウェーデンはいずれも10%以上の下げを示しています。こうした国々は、サイバーセキュリティの面においても、経済的な利点を得ています。

いかなる地域でも、不正ソフトウェアの比率が下がれば、その利点を享受

アジア太平洋：ここではソフトウェアの57%がライセンス許諾を得ておらず、2015年から4ポイント減少しているものの、地域全体で見るとライセンスのない比率は、アジア太平洋地域が世界で最も高くなっています。このため、この地域でのライセンスのない不正ソフトウェアの商業価値は164億ドルにも達し、こうした不正ソフトウェアの全世界での商業価値の1/3を占めています。これは、他のいかなる地域よりも大きなものです。アジア太平洋地域では、商業価値で68億ドル相当のライセンスなしの不正ソフトウェアが中国だけから出回っています。

中央・東ヨーロッパ：中央・東ヨーロッパ地域もアジア太平洋と並んで、ライセンスのない不正ソフトウェア使用の全体的比率が高く、57%に達しています。2015年からの低下率も、1%だけでした。この地域で、ライセンスのない不正ソフトウェアがどの程度使用されているかには大きな違いが生じています。不正ソフトウェアの使用率がこの地域で最も高いのはアルメニアで、85%です。第2位がモルドバの83%、第3位がベラルーシの82%です。これに対して、チェコ共和国はこの地域では最低の32%、2番目に低いのはスロバキアの35%です。しかしロシアでのこうした不正ソフトウェアの商業価値は13億ドルにのぼり、この地域でのライセンスのない不正ソフトウェアの使用ではロシアが現在も最大のシェアを占めています。

中東とアフリカ：中東とアフリカでは、不正ソフトウェアの全体的比率は1%低下し、56%になりました。一方、2つの市場では1%増大し、他の4つの市場では比率に変化がありませんでした。この地域の比率は、世界で最も悪い結果となったアジア太平洋地域よりも、1%低いだけです。この地域の中には、不正ソフトウェアの使用比率が世界でも特に高い幾つかの国が存在し、リビアが90%、ジンバブエが89%です。これに対しUAE（32%）、南アフリカ（32%）、イスラエル（27%

）は、ライセンス許諾を得ている合法的なソフトウェアの利点を享受しています。

ラテン アメリカ：ラテンアメリカ地域のソフトウェアの52%には、ライセンス許諾が存在していません。2015年の調査から、3ポイント減少しています。ソフトウェア
の商業価値は、50億ドル近くに達しています。特に比率の高い国々としては、89%のベネズエラ、世界で第2位）、81%のニカラグア、80%のエルサルバドルがあります。これに対しブラジルは46%、コロンビアは 48%、メキシコは49%で、ライセンスのない不正ソフトウェアの比率が小さく、その利点を上手く得ることに成功しています。またメキシコは、2015年からライセンスのない比率が3ポイント低下しています。今のところブラジルがこの地域で最も比率が低くなっていますが、市場規模として最大の国でもあるため、不正ソフトウェアの商業価値のうち、17億ドルを占めるまでに至っています。この地域では、最大規模です。

西ヨーロッパ：西ヨーロッパ全体では、ライセンスのないソフトの比率は2ポイント低下し、26%に下がりました。最も低下幅が大きかったのはアイルランドで、3ポイントの低下で、ライセンスのない不正ソフトウェアの比率は29%になりました。ギリシャはこの地域では依然として 例外的な存在で、ライセンスのない不正ソフトウェアの使用比率が61 %と飛び抜けて高い状況です。この地域の幾つかの国々では、不正ソフトウェアの比率を世界でも最低レベルに抑制するよう努めており、商業用ソフトウエアの価値を最大限に活用し、サイバーセキュリティのリスクを低減しています。17%のルクセンブルグ、19%のスウェーデン、19%のオーストリア、 20%のデンマークとドイツ、21%のスイスといった国々です。調査対象となった20か国のうち16か国において、2015年から 2ポイント以上の低減を達成しました。

北米：北米地域全体では、引き続き世界の各地域と比較すると不正ソフトウェアの使用比率は16%と最小レベルを維持しています。市場規模が巨大であるため、こうしたソフトウェの商業価値は現在も大きく、95億ドルに達しています。

ソフトウェア資産管理：組織をリスクから守り、価値を向上する方法

企業レベルにおいては、世界的にも適用できる優れたベスト プラクティスが存在し、それを活かすことでテクノロジー資産から得られる利点を最大化し続け、不正ソフトウェア使用によるマルウェアのリスクを低減できます。各種調査によると、強固なソフトウェア資産管理（SAM）プログラムを実施すれば、年間のソフトウェア関連コストを最大で30%近くまで節約できることが、判明しています。[25]

2017年版のISO/IEC 19770-1標準では、ISOに準拠したSAMの効果的なシステム導入を実施するための包括的なアプローチを定めています。この標準を導入することで、3層からなる段階的実施すべてに関して、連続的なプロセスの改善を実現できます。この段階的アプローチによって、組織は適切に実装を展開できます。この標準では、業界標準のプロセス全体において各層の適用を検討しています。そして、このプロセスは以下の4段階で構成されています。(1) 選択した各層に合わせた、包括的な導入プランの作成、(2) プランを優れた管理能力を持って実行、(3) プランの進捗状況の評価、(4) 必要に応じてプランを調整し、継続的に改善を確保。

クラウド化への移行に向けた機会の加速化

クラウドは、現世代のテクノロジーの中でも、最も革新をもたらすコア技術の1つとして拡大しています。コンピューティング リソースの売買や導入のあり方に大きな革命をもたらすものです。小規模企業から現在急成長中の企業まで、以前であれば大企業しか利用できなかったテクノロジーを、誰でもが利用可能です。今では企業が利用できるデジタル化に向けたクラウドベースのサービスは、量・質、そして多様性のいずれにおいても爆発的に増大しています。平均的な企業が利用するクラウド ベースのアプリケーションの件数は、この3年間で3倍に増えたと推定されています。[26] 多くの場合、インターネット経由で利用できるクラウドサービスの内容は、従来のソフトウェアの機能を大幅に強化したものです。実際、IDCの推定では、現在の世界でのソフトウェアの機能のうち、22%はクラウドで提供されています。

こうしたクラウド サービスに企業が殺到している状況には、コストの削減や柔軟性の向上、複雑性の軽減、そしてセキュリティの強化という魅力的な可能性が網羅されていることが背景にあります。

- クラウドは、コスト効率において卓越：IT組織がクラウドへの移行に成功した場合、大型のデータ センターを運営し、宅内で殆んどのアプリケーションをホスティングしている同業他社の平均値と比べ、ITコストを21%削減できます。[27]先進的な企業によると、クラウドの活用により高額な資本投下を回避し、ITコストを軽減できます。ここでの資本投下は、例えば、既存のハードウェア等のインフラをアップグレードし、保守する際に必要となるコストです。クラウドでは必要なリソースにだけ料金を払う（サブスクリプション）ので、組織は一層コストの削減が可能です。しかもインターネット経由で利用できるコンピューティングとストレージ容量は、ほぼ無制限です。
- クラウドはセキュリティに優れ、柔軟:さらにクラウドはその独特なアーキテクチャーにより、従来にはない柔軟性を実現しています。コンピューティング用リソースの売買や導入方法を変更しただけでなく、いかなるデバイスからでも、また世界中のどこからでもアプリケーションを利用できるためです。一部のユーザーにとって、クラウドの最大の利点とは従来のモデルに比較してセキュリティが大幅に向上することです。クラウドのプロバイダーはセキュリティ上の脅威がどこにあるかを広範に見渡し、早期にリスクを特定し、高度なセキュリティ テクノロジーを配備しています。個々の顧客が自費で配備できるセキュリティよりも、高度な技術です。更に、リスクの脅威から防御する最先端テクノロジー、固定および移動通信両方のデータ暗号化、アップデートの自動化などを提供して、新たに発見されたリスクの脅威からシステムを保護します。上記のような能力を組み合わせることで、データの回復力を高め、組織のセキュリティを強化します。
- SAMにより、クラウドに移行する機会を実現：クラウド化により、事業全体で新規のデジタル化を推進するなど、かつて経験したことのない潜在的な可能性を享受できます。SAM は、クラウドへの移行を加

終了ノート

[1] "Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices," Gartner (July 19, 2016), available at www.gartner.com/newsroom/id/3382317 and "Demonstrating the Business Value of Software Asset Management and Software License Optimization," Gartner, available at http://imagesrv.gartner.com/media-products/pdf/flexera/flexera_issue1.pdf.

[2] McAfee Labs Threat Report (March 2018), available at https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2018.pdf.

[3] "Cyber-Attacks Occurring More Frequently and With Greater Sophistication, NTT Security Report Finds," Security InfoWatch (August 9, 2017), available at www.securityinfowatch.com/press_release/12358487/cyber-attacks-occurring-more-frequently-and-with-greater-sophistication-ntt-security-report-finds.

[4] *Internet Security Threat Report*, Symantec (April 2017), available at www.symantec.com/security-center/threat-report.

[5] In 2015, 43 percent of cyber-attacks worldwide were against small businesses with less than 250 workers. Elizabeth MacDonald, "Cyber Attacks on Small Businesses on the Rise," *Fox Business* (April 26, 2016), available at www.foxbusiness.com/features/cyber-attacks-on-small-businesses-on-the-rise.

[6] *Internet Security Threat Report*, Symantec (April 2017), available at www.symantec.com/security-center/threat-report.

[7] Ponemon Institute, *2017 Cost of Cyber Crime Study*, available at www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

[8] "Global Cybercrime Costs Top $600 Billion," DarkReading (February 21, 2018), available at https://www.darkreading.com/attacks-breaches/global-cybercrime-costs-top-$600-billion-/d/d-id/1331106.

[9] M-Trends 2013: Attack the Security Gap, Mandiant (2013), available at https://www.fireeye.com/current-threats/annual-threat-report/mtrends/rpt-2013-mtrends.html.

[10] Ponemon Institute, *2017 Cost of Cyber Crime Study*, available at www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

[11] Paul Mozur, "China, Addicted to Bootleg Software, Reels From Ransomware Attack," *New York Times* (May 15, 2017), available at www.nytimes.com/2017/05/15/business/china-ransomware-wannacry-hacking.html.

[12] "China's Fondness for Pirated Software Raises Risks in Attack," *Phys Org* (May 16, 2017), available at https://phys.org/news/2017-05-china-fondness-pirated-software.html.

[13] "Jakub Kroustek, a malware researcher with Avast, a security software company in the Czech Republic, said in a blog post that Russia was the most-affected country so far [from a malware attack]."Elizabeth Dwoskin and Karla Adam, "More Than 150 Countries Affected by Massive Cyberattack, Europol Says," *Washington Post* (May 14, 2017), available at https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html.

[14] International Organization for Standardization, *ISO/IEC 19770-1:2017 Information Technology—IT Asset Management*, available at www.iso.org/standard/68531.html.

[15] "Equifax Breach to Cost Total of $439M," PYMNTS (March 5, 2018), available at www.pymnts.com/news/security-and-risk/2018/equifax-cost-275m/.

[16] "How Could ITAM Have Helped the Equifax CIO?" *The ITAM Review* (October 19, 2017), available at www.itassetmanagement.net/2017/10/19/equifax-itam/.

[17] "Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices," Gartner (July 19, 2016), available at www.gartner.com/newsroom/id/3382317 and "Demonstrating the Business Value of Software Asset Management and Software License Optimization," Gartner, available at http://imagesrv.gartner.com/media-products/pdf/flexera/flexera_issue1.pdf.

[18] These important benefits are derived from the combination of better security by reducing malware that may accompany unlicensed software, fewer disruptive audits that take precious time to respond to, reduced legal risks around license compliance violations, better IT productivity by eliminating outdated or unsupported software, more trusted brand identity by avoiding risky behavior, and better relationships with vendors.

[19] With a more effective licensing model in place, OSI reduced costs by more than 30 percent and achieved 100 percent compliance with Microsoft guidelines. See "OSI International Foods Increases Software License Visibility and Reduces Costs by 30 Percent," Microsoft Customer Solution Case Study, available at http://download.microsoft.com/download/7/F/1/7F18B556-BC4D-4B5C-BAB8-9386515BF1EB/Germany-OSI_International_Foods.doc.

[20] Baltika conducted a SAM project that now saves them $100,000 per year in the workstation, software, and servers. See "Baltika Breweries Unlocks the Power of Microsoft Technologies Through SAM," YouTube, available at www.youtube.com/watch?v=yocvl9nl8o0&feature=youtu.be; and "Software Asset Management Customer Evidence," Microsoft, available at www.microsoft.com/en-us/sam/customers.aspx.

[21] "University of Roehampton Benefits From Azure Migration Through Microsoft SAM," YouTube, available at https://www.youtube.com/watch?v=hAHHvZ_8zz4&feature=youtu.be; and "Software Asset Management Customer Evidence," Microsoft, available at https://www.microsoft.com/en-us/sam/customers.aspx.

[22] Using a specialized SAM tool and other strategies, the space agency uncovered software consolidation opportunities. For NASA, it meant eliminating duplicate software licenses and negotiating better prices for the software it already buys. "How NASA Saved $100 Million on Software Licenses," *FedTech* (February 23, 2017), available at https://fedtechmagazine.com/article/2017/02/how-nasa-saved-100-million-software-licenses.

[23] See BSA | The Software Alliance, *Government Guide for Software Asset Management*, available at www.bsa.org/~/media/Files/Tools_And_Resources/Guides/SoftwareManagementGuide/SoftwareManagementGuide_Government.pdf.

[24] Azerbaijan, Belarus, Bulgaria, Georgia, Hong Kong, Ireland, Mexico, Moldova, Philippines, Singapore, South Korea, and Thailand.

[25] "Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices," Gartner (July 19, 2016), available at www.gartner.com/newsroom/id/3382317 and "Demonstrating the Business Value of Software Asset Management and Software License Optimization," Gartner, available at http://imagesrv.gartner.com/media-products/pdf/flexera/flexera_issue1.pdf.

[26] Ajmal Kohgadai, "12 Must-Know Statistics on Cloud Usage in the Enterprise," SkyHigh Networks, available at https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise/.

[27] "Cloud Users Enjoy Significant Savings," Computer Economics (April 2016), available at https://www.computereconomics.com/article.cfm?id=2185.

[28] Case Study: A Confident Move to the Cloud for the University of Roehampton," available at https://www.civica.com/globalassets/7.document-downloads/2.uk-docs/case-studies/roehampton-case-study.pdf.

BSA | ザ・ソフトウェア・アライアンスについて

BSA | ザ・ソフトウェア・アライアンス (www.bsa.org) は、政府やグローバル市場において、世界のソフトウェア産業を代表する主唱者です。BSAの会員は、世界で最もイノベーティブな企業で構成されており、経済を活性化させ、現代生活を向上させるソフトウェア・ソリューションを創造しています。

ワシントンDCに本部を置き、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・プログラムを先導し、技術革新の推進とデジタル経済の成長を推進する公共政策を提唱しています。

www.bsa.org

BSA Worldwide Headquarters
20 F Street, NW
Suite 800
Washington, DC 20001

+1.202.872.5500
@BSAnews
@BSATheSoftwareAlliance

BSA Asia-Pacific
300 Beach Road
#25-08 The Concourse
Singapore 199555

+65.6292.2072
@BSAnewsAPAC

BSA Europe, Middle East & Africa
65 Petty France
Ground Floor
London, SW1H 9EU
United Kingdom

+44.207.340.6080
@BSAnewsEU