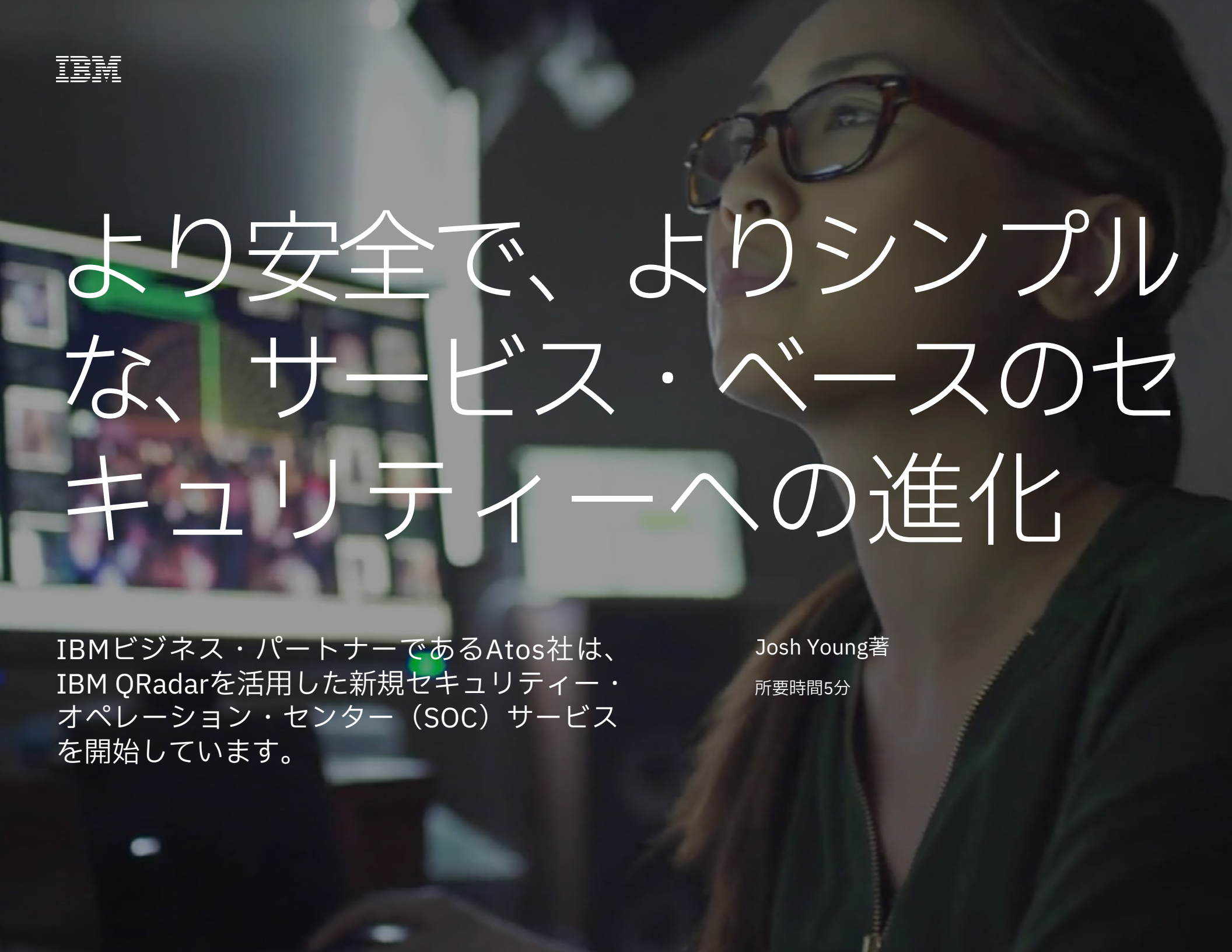


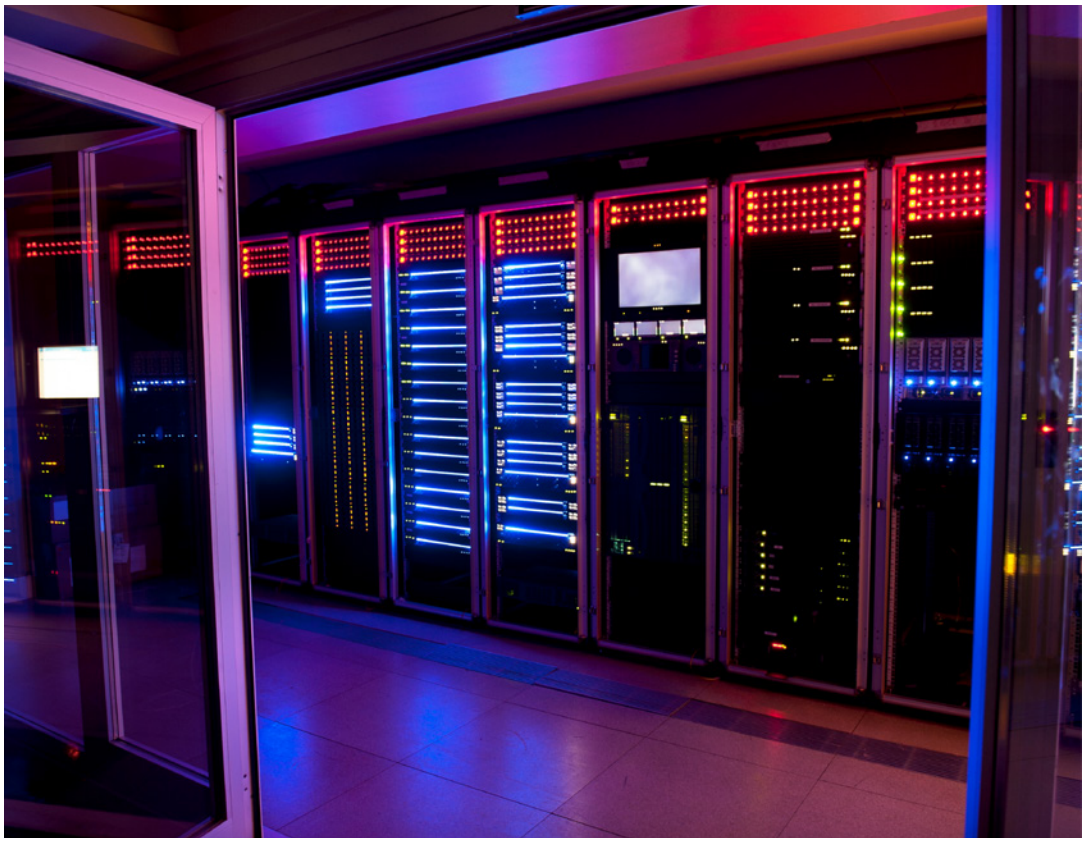
より安全で、よりシンプルな、サービス・ベースのセキュリティーへの進化

IBMビジネス・パートナーであるAtos社は、IBM QRadarを活用した新規セキュリティー・オペレーション・センター（SOC）サービスを開始しています。

Josh Young著

所要時間5分

サイバー犯罪者に休日はありません。そのためITセキュリティーは、いつでもすぐに攻撃を検知し、回避できるよう備えておく必要があります。しかし多くの企業にとって、24時間体制のセキュリティー管理チームを編成することは現実的ではなく、経済的にも困難です。



Atos中国のビッグデータ＆セキュリティー責任者であるCheng Cai He氏は次のように説明しています。「この20年間で、セキュリティーやデータ漏洩の脅威が増していることは、誰もが実感していることだと思います。そして、攻撃のタイプ、つまりウイルスの種類は、中国地域で急速に進化してきています。」

この事態に対応するため、Atos社のお客様の多くは新しいセキュリティー機器や製品に多額の投資を始めていました。しかし、これらの製品はうまく統合されていないことが多く、ユーザーを保護する能力には限界がありました。

「効率性があまりにも悪かった」とCheng Cai氏は言います。「製造業をはじめとする企業から、どうすれば確実

に様々なセキュリティー製品を連携して機能させられるのかという質問が寄せられることが増えてきました。そこで、私たちはクラウド・ベースのセキュリティー・オペレーション・センター（SOC）サービスの構築を検討し始めました。」

この時点でSOCは中国市場では存在感を増していました。そして、SOCサービスを通じて、Atos社はお客様のセキュリティー・データをより集中的に管理し、全体的なネットワークの正常性と安定性をあらゆる角度から確認できるようになっていました。

「以前はSOCといえば、どれも各企業が構築したものでした」とCheng Cai氏は言います。「そうしたSOCは投資額が多額になるため、それほど多くはありませんでした。あらゆる種類のセキュリティー装置を購入する必要がありますし、年中無休の24時間体制で保護を実現するには、専門のサポートチームに投資する必要があります。」

SOCサービスにかかる費用は

約1.5 FTE未満

社内にスタッフを配置する場合は、7～8 FTE（フルタイム社員1名の仕事量相当）が必要

中小規模のお客様に

24時間365日

のセキュリティーの監視と保護を提供します

また一方で、サービス・ベースのアプローチを選択することで、Atos社は、大規模なITプロジェクトに投資する資金を持たない中小企業にもSOCのメリットを拡大できるようになりました。さらに、SOCサービスを複数のエンド・ユーザー環境に簡単に配信するために、Atos社はクラウドを活用した配信モデルを常用せざるを得ませんでした。

「中国のクラウド産業は、ここ5年で非常に成熟しました。」とCheng Cai氏は言います。「そして、お客様の多くはIT資産をオンプレミスからクラウドに移行しています。しかし、この移行は少し複雑です。なぜなら、重要な情報とお客様の個人データを国外に転送することを禁止するデータ保護法を全員が遵守する必要があるからです。そのため、新しいサービスのクラウド・ソリューションは中国の国内でホストする必要がありました。」

「セキュリティーやデータ侵害の脅威が増大していることは周知のとおりです。そして、攻撃のタイプ、つまりウイルスの種類は、中国地域で急速に進化してきています。」

Cheng Cai He氏、ビッグデータ＆セキュリティー責任者、
IBMビジネス・パートナーの中国Atos社

新しい技術と 新しい機能を 新しい形で届ける

Atos社は、同社の計画したSOCサービスの提供方法の検討に入る中で大規模なマーケティング分析を行い、このオファリングに対する顧客の要件と期待を調査しました。同時に、新しいSOCを構築するために信頼できるセキュリティー製品とツールの検討を開始しました。

Atos社はIBMのビジネス・パートナーでもあるため、すぐにIBMのテクノロジーに候補を絞り、とりわけ関心を寄せたのがIBM Security® QRadar® XDRスイートでした。このプラットフォームでの概念検証（POC）が成功すると、同社は新しいSOCサービスのセキュリティー情報とイベント管理（SIEM）のニーズを監督するために、IBM Security QRadar SIEMソリューションを

選択しました。一方、中国ではAWSが、必要なクラウド環境を整えています。

そして、QRadarテクノロジーは、Atos社に顧客ネットワークの全体像を提供し、AIを活用した脅威検知とログ分析とともに監視を行います。「すべてを見ることができます。」とCheng Cai氏は付け加えます。「お客様のネットワーク全体を把握できます。優先事項とそ

うでない事項が分かるため、大変に便利です。」

QRadarの導入を効率化して、お客様のオンボーディングを円滑に進められるように、Atos社はIBM® Embedded Solution Agreement（ESA）を締結しました。「4月にESAに署名しました」とCheng Cai氏は振り返ります。「QRadar製品を当社のオファリングに標準装備することで、ライセンス交付がより簡単になりました。また、IBMとのパートナーシップがより強固なものになり、より一層の緊密な連携が実現しています。」

新サービスは2022年8月に完成し、当初はパイロット段階でAtos社の既存のお客様3社と協力していました。その翌月、一般向けのAtos SOCサービスを正式に開始しました。

「北京のIBMイノベーション・センターで2つのワークショップを開催し、そこでSOCサービスのデモを公開しました。そこでの議論を踏まえて、当社のオファリング・カタログをさらに充実させています。」とCheng Cai氏は話しています。

「[QRadar]では、すべてを見渡すことができます。お客様の状況を把握し、優先事項とそうでない事項が分かるため、大変に便利です。」

Cheng Cai He氏、ビッグデータ＆セキュリティー責任者、IBMビジネス・パートナーの中国Atos社

IBMをお勧めする理由

「QRadarは当社のSIEMにとって正しい選択であることがわかりました」とCheng　Cai氏は説明します。「それは、中国政府から課せられた、私たちが遵守する必要のある各種の方針および規制要件とすでに統合されていたからです。また、お客様はSOCプラットフォームを導入した初日からご使用いただけます。」

「この10年間、QRadarとIBM Securityが Gartner Magic Quadrantに常にランクインしていることにも感心していました。お客様にクラス最高のサービスを提供するためには、クラス最高のセキュリティー製品が必要です」と同氏は続けます。

Atos社はIBMビジネス・パートナーとして、過去数年間にわたって築いてきたグローバル・ビジネスとの既存の関係も重視しています。「Atos社はIBMと長い間パートナー関係にあります」と、Cheng Cai

氏は言います。「しかし、これは中国国内でIBMと連携した2つ目のプロジェクトにすぎません。外部からの支援で新しいソリューションを推進する場合、その相手企業の協力と信頼が全体のオペレーションを成功させるための重要な鍵となることが分かっていました。そして、IBMはその信頼関係を築いてくれました。」

Cheng Cai氏は、この信頼関係という気持ちの重要性を強調しました。「私たちはITサービスを基盤とする企業で、IBM Chinaにはセキュリティー・サービス・チームが存在します。したがって、場合によっては、実際にIBMと競合する立場に立つこともあります。しかし、グローバル・ビジネスでこれまで築いてきたお互いの関係と、今回のプロジェクトでの直接得られた経験から、私たちは完全に信頼できるパートナーであることを確信しました。」

シンプルに提供、包括的に保護

Atos社は、この新しいSOCサービスにより、中小規模の中国企業に包括的で堅牢なセキュリティー監視・管理を手ごろな価格で提供することができます。

Cheng Cai氏によれば、「当社の価格設定では、SOCサービスを1～1.5フルタイム当量（FTE）で提供しています。しかし、一般的な企業が独自の内部SOCを構築するには、7～8人の専任チームが必要となります。24時間365日のサービスを提供しようとすれば、すべてのセキュリティー製品を用意するための多大な設備投資が必要となるところ、それが必要ない点で、私たちは競争上の優位性が得られます。」

「さらに、脅威もセキュリティー技術も非常に急速に進化しています」と、Cheng Cai氏は続けます。「したがって、常に方針や技術を更新していく必要があります。しかし、SOCでは、当社がそれをお手伝いしています。当社は市場で先駆的なサービスを提供し、お客様のお力になります。」

内蔵AIと自動化機能を持つQRadarプラットフォームは、より迅速にイベントを特定し、解決することを支援します。「これらの攻撃には、スピードがすべてです」と、Cheng Cai氏は述べます。「異常な行動をいち早く識別し、すばやく隔離することで、侵害によって引き起こされる損害の可能性を低く抑えることができます。」

Atos SE社について

IBMのビジネス・パートナーであるAtos社（ibm.comの外部リンク）は、ITコンサルタント・サービス、デジタル・セキュリティー・ソリューション、脱炭素化オファリングのグローバル・プロバイダーです。フランスのパリに本社を置き、世界71カ国に拠点を持ち、11万2000人以上の従業員を雇用しています。

ソリューション・コンポーネント

- IBM® Embedded Solution Agreement
- IBM Security® QRadar® XDR
- IBM Security QRadar SIEM

© Copyright IBM Corporation 2022. 日本アイ・ビー・エム株式会社 〒103-8510 東京都中央区日本橋箱崎町19-21

米国で作成、2022年10月

IBM、IBM ロゴ、ibm.com、IBM Security、および QRadar は、世界中の多くの法域で登録されている International Business Machines Corp. の商標です。その他の製品名およびサービス名は、IBMまたは他社の商標である可能性があります。IBM の商標の最新リストは、ウェブ上の http://www.ibm.com/legal/copytrade からご参照いただけます。

Microsoft、Windows、Windows NT、Windows のロゴは、米国、その他の国、またはその両方におけるMicrosoft Corporation の登録商標です。

本書は最初の発行日時点における最新情報を記載しており、IBMにより予告なしに変更される場合があります。IBMが事業を展開しているすべての国で、すべての製品が利用できるわけではありません。

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。本書の情報は「現状のまま」で提供されるものとし、明示または黙示を問わず、商品性、特定目的への適合性、および非侵害の保証または条件を含むいかなる保証もしないものとします。IBM製品は、IBM所定の契約書の条項に基づき保証されます。

お客様は自己の責任で関連法規を順守しなければならないものとします。IBMは法律上の助言を提供することはなく、また、IBMのサービスまたは製品が、お客様においていかなる法を順守していることの裏付けとなることを表明し、保証するものでもありません。

適切なセキュリティーの実践に関するステートメント。ITシステム・セキュリティーには、企業内外からの不適切なアクセスに対する予防、検出および対応などにより、システムと情報を保護することが含まれます。不適切なアクセスは、情報の改ざん、破壊、悪用、誤用、または他者への攻撃への使用を含む、システムの損傷または誤用につながるおそれがあります。ITシステムや製品は絶対にセキュアであると捉えるべきではなく、不適切な使用やアクセスを防止する上で絶対に効果のある、製品、サービス、セキュリティ対策は1つもありません。IBMのシステム、製品およびサービスは、合法的で包括的なセキュリティー・アプローチの一部として設計されているため、必然的に運用手順が追加されることになります。また、他のシステム、製品、またはサービスが最も効果的である場合もあります。IBMでは、いずれの当事者による不正行為または違法行為により、いかなるシステム、製品もしくはサービス、またはお客様の企業に対して影響が及ぶことはないことを保証するものではありません。