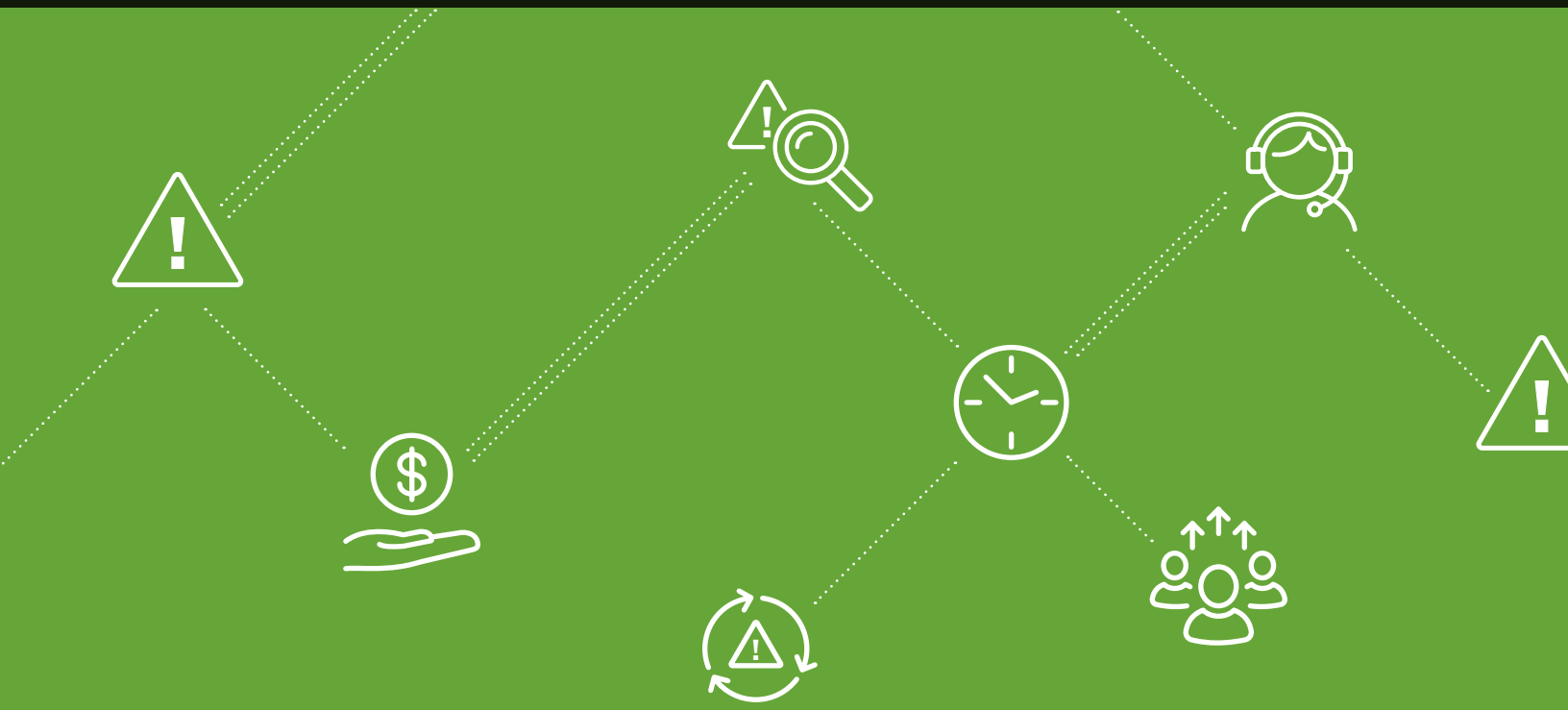
splunk> | quocirca

研究分析

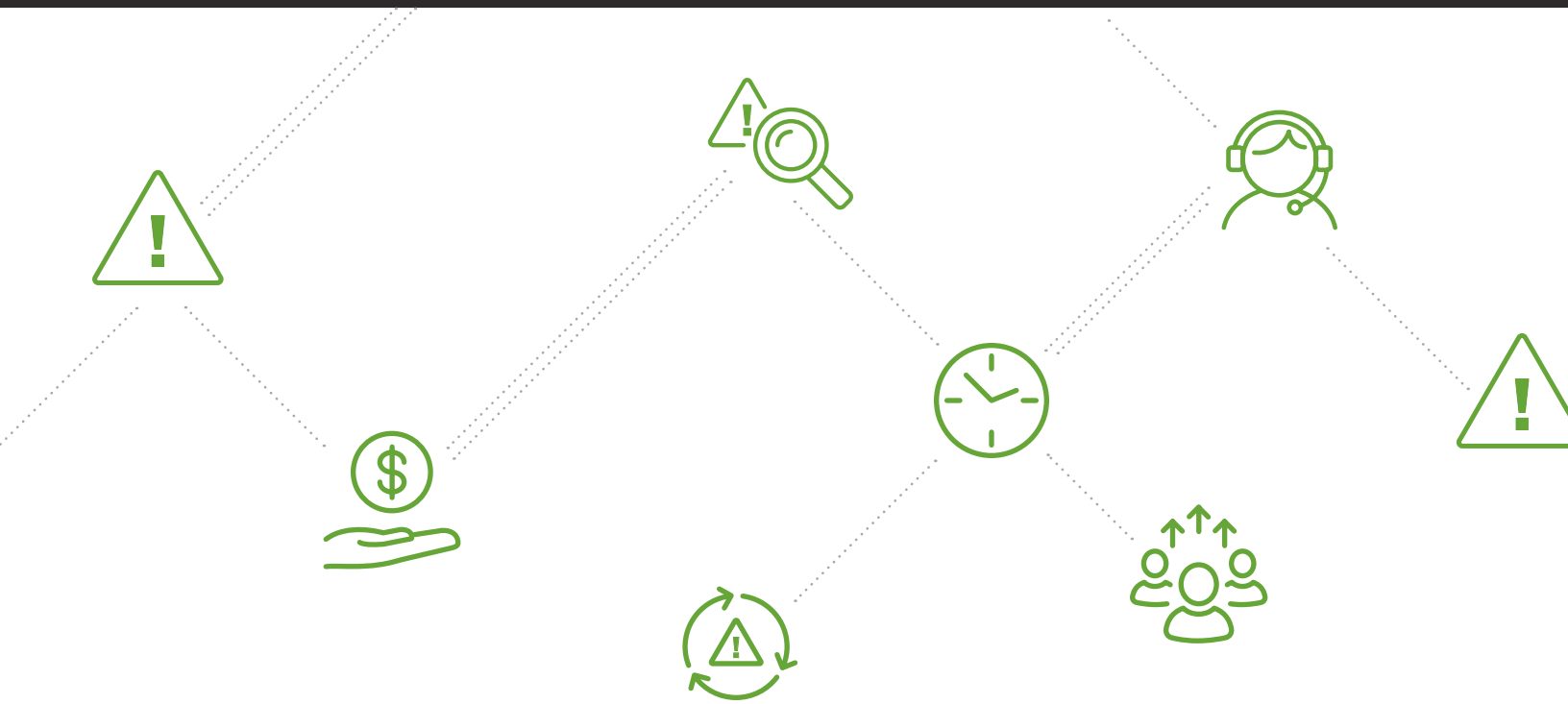


損害対策

重大な IT インシデントの影響

Bob Tarzey (Quocirca 社アナリスト兼ディレクター)

2017 年 11 月



損害対策

重大な IT インシデントの影響

Bob Tarzey (Quocirca 社アナリスト兼ディレクター)
2017 年 11 月

IT インシデントは業種を問わず企業に年間数百万ドルものコストをもたらします。ひとたびインシデントが発生すると、IT スタッフは対応に追われて通常業務が滞り、その影響は IT 部門を超えて企業全体の生産性や顧客の利便性にも及びます。

企業では平均で週に数百件のインシデントが発生しています。インシデントの発端となる IT システムおよび IT インフラストラクチャでは膨大な量のイベントデータが生成されます。関連する IT システムからこれらのデータを幅広く収集して分析すれば、インシデントを早期かつ効率的に検出し、より効果的に問題を解決して、平均修復時間を短縮することができます。さらに、これらのデータは問題の再発を防ぐための根本原因分析にも役立ちます。IT インシデント対応の時間を短縮すれば、IT スタッフはシステムの保守作業よりもデジタルイノベーションの推進に集中して取り組むことができます。

エグゼクティブサマリー

IT インシデントと重大インシデント

企業では 1 カ月あたり平均約 1,200 件の IT インシデントがログに記録され、そのうち 5 件ほどが重大インシデントに該当します。これらのインシデントにつながる大量のイベントデータを処理し、対応の優先順位を決めるのは困難な作業です。しかし、70% の企業が重大インシデントによって自社の信頼が低下したことがあると回答していることから、インシデントを早期に検出して影響を最小限に抑えることは喫緊の課題といえます。

重大インシデントの IT コストとビジネスコスト

重大インシデント 1 件あたりの IT コストは平均 36,326 ドルで、さらにインシデントの影響によるビジネスコストが平均 105,302 ドル発生します。この 2 つのコストは相関関係にあることから、イベント管理やインシデント管理に不備があると、IT コストが上がるだけでなく業務運営にも悪影響を及ぼすことがわかります。

検出、修復、根本原因分析の平均時間

80% の企業がインシデントの平均検出時間を短縮する余地があると考えています。検出時間の短縮は問題の早期解決と業務への影響の抑制につながります。重大インシデントの平均修復時間は 5.81 時間ですが、そもそも管理するインシデントが少なければ修復時間も減らせるはずです。その後の根本原因分析にかかる時間は平均 7.23 時間で、根本原因の特定率は 65% です。

無意味なインシデント

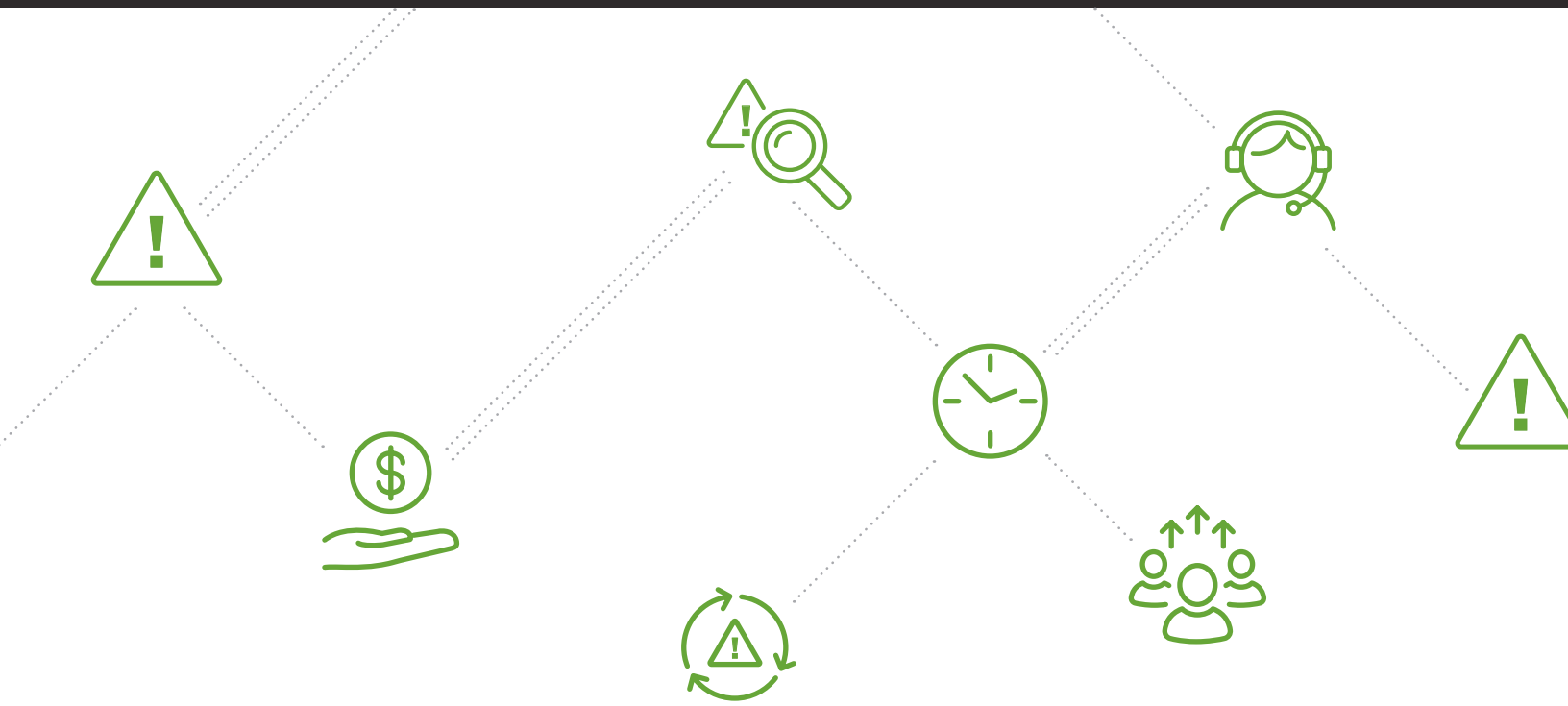
インシデントの重複と再発は根強い問題です。インシデントの重複とは、特定の問題について複数のインシデントが生成されることです。97% の企業でイベント管理プロセスの不備によりインシデントの重複が発生しており、すべてのインシデントの 17.2% が重複しています。また、96% の企業で効果的な根本原因分析によって過去のインシデントから学んでいないためにインシデントが再発しており、再発によるインシデントは全体の 13.3% を占めています。

IT インフラストラクチャの可視性

イベントログを記録してインシデントを識別するための IT インフラストラクチャの監視にも改善の余地があり、80% の企業が監視に死角があると回答しています。監視の死角はインシデントの検出と調査の遅延につながります。しかし、IT システムやそれを監視する IT ツールが複雑化しているために、多くの企業では IT インフラストラクチャ全体を包括的かつ十分に把握できていないのが現状です。

大量イベントの処理とイベント管理

IT 監視ツールによって生成される大量のイベントを処理するのは容易ではありません。52% の企業が何とか管理している状態で、13% は苦戦し、1% は手に負えていないと回答しています。イベント管理プロセスを適切に整備して大量イベントを余裕を持って管理できている企業では、インシデントの平均検出時間が短く、インシデントの重複や再発も少ない傾向にあります。



はじめに

このレポートでは、大量の IT インシデントと、その中でも特に業務プロセスの中断につながりユーザーや顧客に悪影響を及ぼす可能性のある重大インシデントの量が企業に与える影響について、最新の調査結果をご紹介します。そこから、IT 監視ツールによって生成される大量のイベントデータの処理、インシデントの再発防止、インシデントの平均検出時間 (MTTD) と平均修復時間 (MTTR) の短縮に必要な対策について考察します。また、根本原因分析によるインシデントの再発防止効果についても説明します。インシデントを早期に検出できれば、それに連鎖して起こる問題の影響を軽減して、IT 部門とそのユーザーである業務部門のインシデントコストを同時に削減できます。

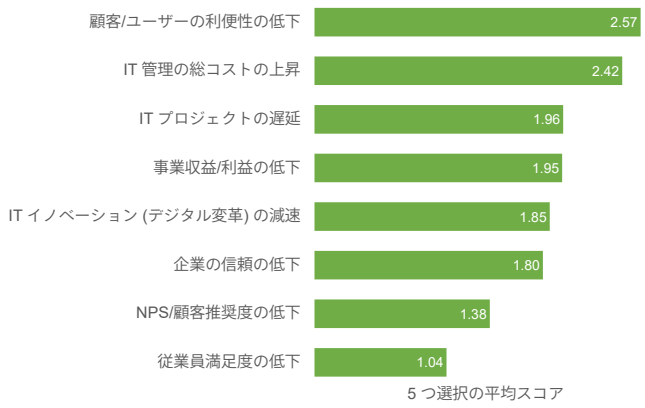
調査は、米国、日本、シンガポール、オーストラリア、スウェーデン、オランダ、ドイツ、フランス、英国の 9 カ国で、さまざまな規模と業種の企業を対象に行われました (詳細は付録を参照)。

IT インシデントと重大インシデント

企業の IT インフラストラクチャは IT 依存度の高まりとともにますます複雑化しています。競争力を維持するために新しいデジタル技術を取り入れなければならないというプレッシャーから、仮想化、コンテナ化、クラウドサービスといった新しいレイヤーが次々と IT インフラストラクチャに追加されています。しかしそれはユーザーの不満と余計なビジネスコストを生み出し、最終的には企業の信頼低下につながることもあります。

調査によると、インシデントがもたらす影響の中で多くの企業が特に懸念しているのは、ユーザーの利便性の低下とプロジェクトの遅延です (図 1)。IT 管理チームは問題を解決して適時に保守作業を行うために、IT インフラストラクチャ監視ツールによって生成されるすべてのイベントデータをフィルタリングして、何が本質的な問題かを判断する必要があります。しかし、ノイズをより分けて重要な問題を識別するのは容易ではありません。検出と対応が遅れれば、小さな問題が重大なインシデントに発展してしまう可能性もあります。

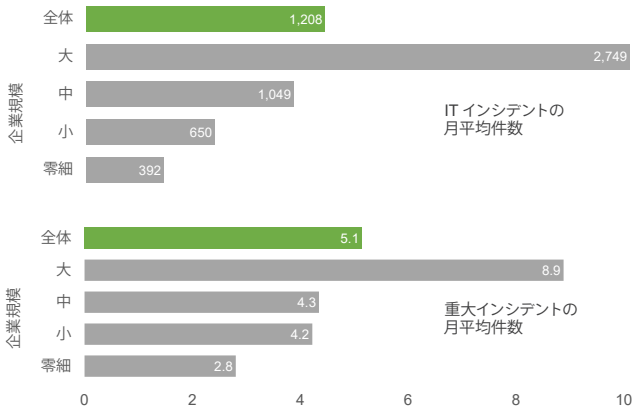
図 1：IT インシデントがもたらす影響の中で特に懸念されること



企業では重大インシデントが 1 カ月あたり 5.1 件発生

重大なインシデントには最高レベルの優先度を割り当てる必要があります (サービスデスクのシステムで「重大度 1」、「優先度 1」、「P1」などのラベルを付けます)。企業では 1 カ月あたり平均約 1,200 件のインシデントがログに記録され、そのうち 5.1 件が重大インシデントに該当します (図 2)。70% の企業が過去に重大インシデントによって自社の信頼が低下したことがあると回答しています。重大インシデントとそうでないインシデントを見極めるのは IT チームにとっても難しく、優先順位付けをできるだけ効果的に行うには適切なツールの助けが必要です。

図 2：ログに記録される IT インシデントと重大インシデントの月平均件数



70% の企業が重大インシデントによって自社の信頼が低下したことがあると回答

重大インシデントのコスト

重大インシデント 1 件あたりの IT コストは平均 36,326 ドルです。それに加えて平均 105,302 ドルのビジネスコストが発生します (図 3)。この 2 つのコストは相関関係にあることから、インシデント管理に不備があると、IT コストが上がるだけでなく、業務運営にも悪影響を及ぼすことがわかります。

重大インシデント 1 件あたりの IT コストは平均 36,326 ドル

重大インシデント 1 件あたりのビジネスコストは平均 105,302 ドル

重大インシデント 1 件あたりの総コストは平均 141,628 ドル

MTTD は、問題が最初に発生した時点からそのインシデントを特定するまでの平均時間を指します。MTTD が長い企業ほど重大インシデントの IT コストが上がります (図 4)。これは、イベント管理プロセスの初期段階で見つかった問題がインシデント管理までどのようにエスカレーションされるかを示しています。

インシデントの件数も IT コストを押し上げる要因となります。インシデントの対応件数が最も多い企業の IT コストは最も少ない企業の 4 倍以上に及びます。件数によるコストへの影響は、インシデントの重複または再発の件数と IT コストの関係にも表れています (図 5)。重複や再発が多く発生する原因は、イベント管理とインシデント管理の不備に加えて、効果的な根本原因分析を通して失敗から学ぶことができていないことにあります。

では、重大インシデントのコストを削減するにはどうすればよいでしょうか?今回の調査では、インシデントの早期検出とインシデント調査プロセスの効率改善が IT インシデントの影響軽減に寄与することが明らかになりました。また、効果的な根本原因分析がインシデントの再発防止に役立つこともわかりました。これらの対策を実行すれば、インシデントの IT コスト、そしてその結果として生じるビジネスコストと業務運営への損害を軽減できるはずです。

図 3：重大インシデント 1 件あたりの平均 IT/ ビジネスコスト

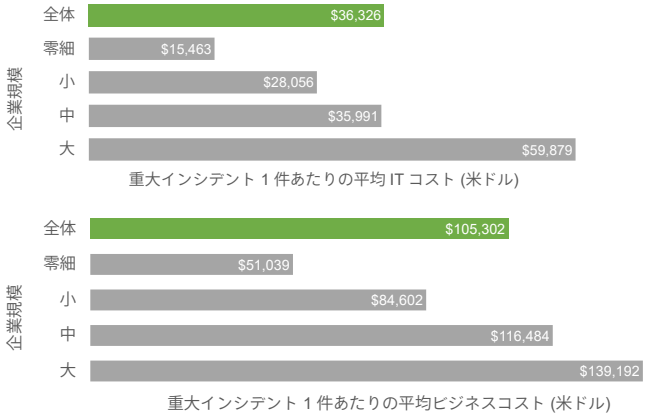


図 4：重大インシデントの MTTD と IT コストの関係

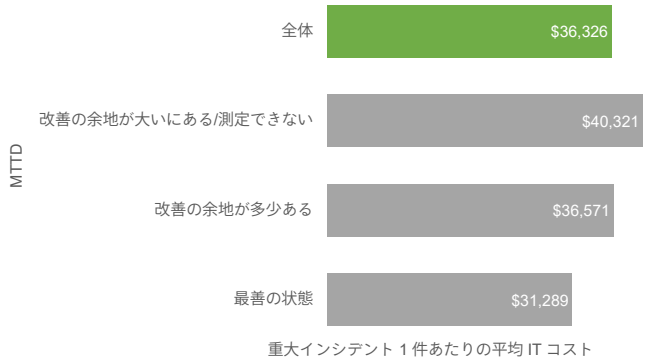
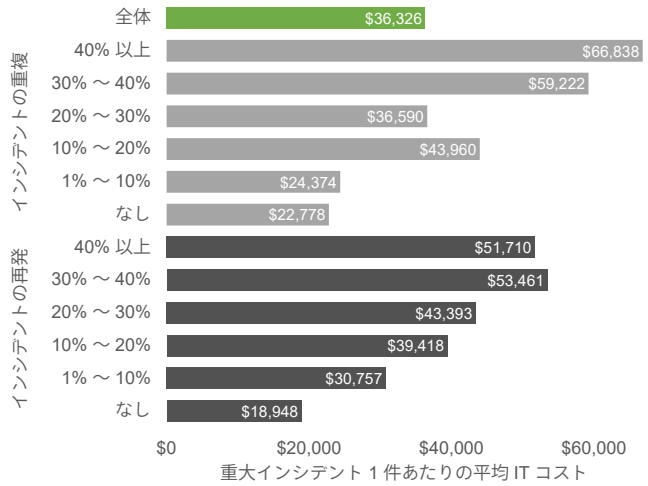


図 5：インシデントの重複 / 再発と重大インシデントの IT コストの関係



インシデント対応

インシデント対応では、まず、自動イベント管理システムを通じて、または IT スタッフやエンドユーザー、顧客からの報告によって、インシデントを検出しなければなりません。80% の企業が MTTD を改善する余地があると考えており、MTTD が最善の状態であると回答したのはわずか 20% でした。ただし、IT 監視ツールによって生成される大量のイベントデータを余裕を持って管理できている企業に限ると、最善の状態であると回答した割合は 2 倍以上に増えます (図 6)。

80% の企業が MTTD の改善余地があると考えている

IT チームは、業務プロセスに与える影響の大きさに基づいてインシデントを優先順位付けする必要があります。そのためには、IT インフラストラクチャを可視化して、IT 運用担当者があらゆるコンポーネントの状態を把握、分析できるようにすることが必要です。

検出後は、問題解決とインシデントの終了プロセスに入ります。MTTR は、インシデントが検出された時点から、問題を修復して解決済みとするまでの平均時間を示します。重大インシデントの MTTR は多くの企業にとって重要な指標です。重大インシデントの MTTR は全体で平均 5.81 時間ですが、重複や再発による不必要なインシデントが増えると MTTR も長くなります (図 7)。

重大インシデントの MTTR は全体で平均 5.81 時間

図 6：大量イベントへの対応と平均検出時間 (MTTD) の関係

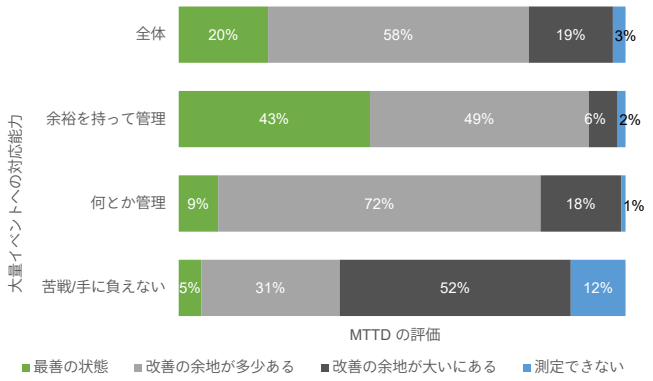
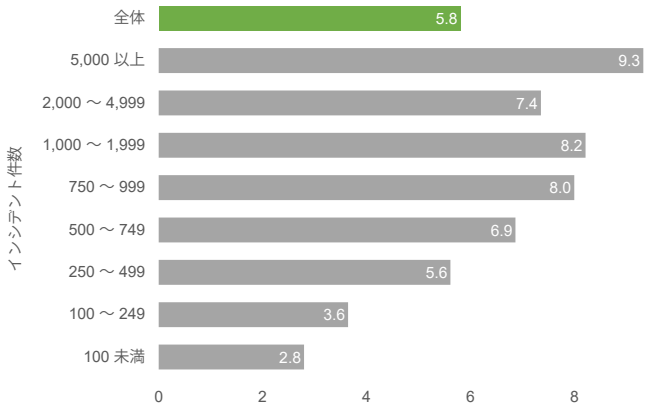


図 7：重大インシデントの件数と平均修復時間 (MTTR) の関係



大インシデントの対応に当たるのは、多くの場合、IT 管理の従来分野を担当するチームです (図 8)。IT 管理の懸念事項に関する最新調査でセキュリティがトップに挙げられていることを考えれば、IT セキュリティチームが深く関与するのは当然といえます (図 9)。セキュリティに関するインシデント (DoS 攻撃やランサムウェア感染など) やデータ漏えいにつながる可能性のあるインシデントは、通常、重大と見なされます。

重大インシデントの対応に当たるチームの平均人数は 6 人です (図 10)。特定のインシデント対応に必要なスキル範囲は企業の規模を問わずほぼ同じであるため、企業の規模によるチーム人数の差はほとんどありません。インシデント調査のために集められるチームは SME (特定分野の専門家) で構成されるため、その人数を減らすのは難しいでしょう。IT インフラストラクチャの可視性を高めることは、IT スタッフが自身の権限を越えるインフラストラクチャ領域のデータにアクセスできるようにする際に役立ちます。

図 8：重大インシデントの対応における各種 IT チームの関与度

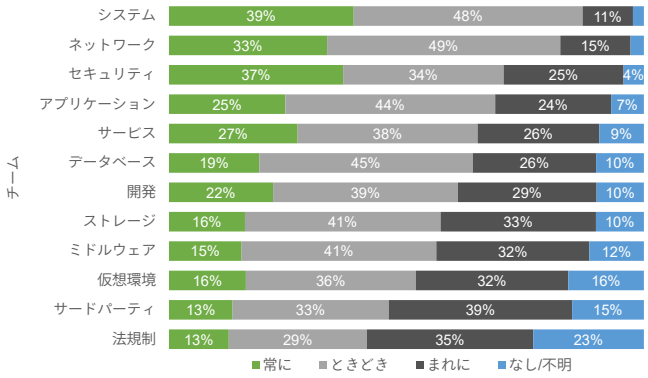


図 9：IT 管理全般に関する懸念事項

効果的な根本原因分析による重大インシデントのコスト削減

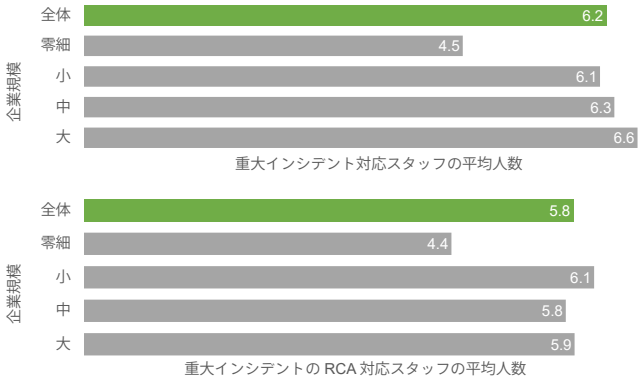
インシデントを早期に検出、修復できれば、その分インシデントが発生した根本的な原因の調査を早く開始できます。この調査は根本原因分析 (RCA) と呼ばれ、IT インフラストラクチャ管理の継続的な改善とインシデントの再発防止に欠かせません。RCA の平均時間は 7.23 時間で、根本原因の特定率は 65% です。RCA でも担当チームの平均人数は約 6 人です (図 10)。

RCA の平均時間は 7.23 時間

根本原因の特定率は 65%

RCA でほぼ常に原因を特定できていると回答した企業は、特定率が 50% と回答した企業に比べて、インシデントの再発件数がおよそ 3 分の 1 に抑えられています。再発の防止は、IT インシデントの総コスト削減につながります。

図 10：重大インシデントの v 解決に当たる IT スタッフの人数



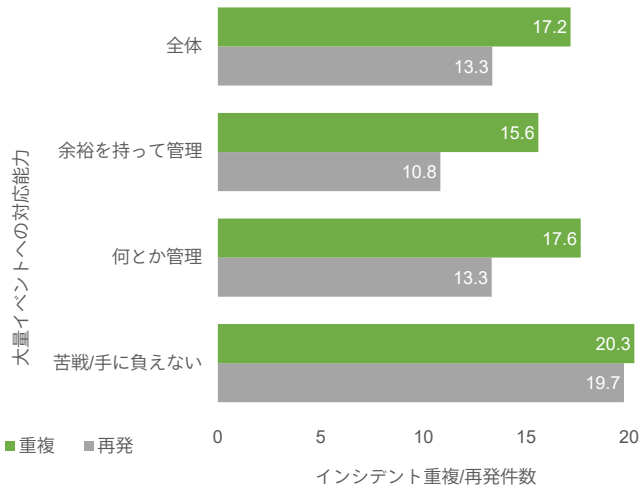
大量イベントの処理とイベント管理

3 分の 2 の企業が、イベント管理プロセスの中で IT 監視ツールによって生成される大量のイベントの処理が問題になっていると考え、20% がそもそもイベント管理プロセスが存在しないと回答しています。66% の企業が大量イベントの処理を課題と認識し、そのうち 52% が何とか管理している状態で、13% が苦戦し、1% が手に負えていません。

66% の企業が大量イベントの処理を課題と認識し、そのうち 52% が何とか管理している状態で、13% が苦戦し、1% が手に負えていない

一方で、大量のイベントに対応できている企業ではインシデントの重複と再発の件数がいずれも少なくなっています (図 11)。対応能力を高めるには、イベント管理プロセスとそれをサポートするツールを適切に整備することが重要です。たとえば、IT インフラストラクチャの可視性を高めれば、イベントの優先順位を効果的に判断できるようになります。イベント管理プロセスに不備があると、誤報を生み、後続のインシデント管理プロセスに無用な重圧を与えて、問題の検出と解決を遅らせる要因となります。

図 11：大量イベントへの対応能力とインシデント重複 / 再発件数の関係



無意味なインシデント

IT インフラストラクチャが複雑で包括的な可視性が確保されていないと、インシデントの重複が発生しやすくなります。サービスデスクによって同じ問題が複数回ログに記録され、ひどい場合には複数の IT チームが同じインシデントの対応に当たることになります。インシデントの重複は 97% の企業で発生しており、およそ 5 分の 1 (17.2%) の企業ではすべてのインシデントが重複しています。

インシデントの重複は 97% の企業で発生しており、17.2% の企業ではすべてのインシデントが重複している

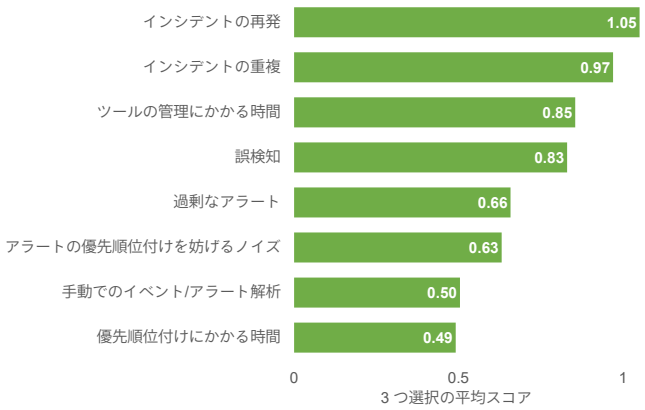
予兆と思われるインシデントに対応して急場をしのいでも、効果的な根本原因分析を行って対策をとらないと、過去の問題から得た経験が活かされず同じインシデントが再発する可能性が高まります。96% の企業が過去のインシデントから学んでいないためにインシデントが再発していると回答しており、再発によるインシデントは全体の 13.3% を占めます。

96% の企業が過去のインシデントから学んでいないためにインシデントが再発していると回答しており、再発によるインシデントは全体の 13.3% を占める

インシデントの重複や再発の影響を過小評価してはいけません。企業では無意味なインシデント (重複) や回避可能なインシデント (再発) が 1 カ月あたり平均 374 件発生しており、大規模企業ではその数が 852 件にも及びます。これによって無駄な修復作業やコストが発生することになります。原因はやはりイベント管理プロセスとインシデント管理プロセスの不備にあります。

IT 管理チームはこの問題を認識しており、IT 運用の効率に影響を及ぼす問題としてインシデントの重複と再発が上位に挙げられています (図 12)。この問題を解決すれば、ログに記録される IT インシデント (およびインシデント調査にかかる時間) を 3 分の 1 ほど削減できる可能性があります。

図 12：IT 運用の効率に影響を及ぼす問題



IT インフラストラクチャの可視性

IT インフラストラクチャの可視性を高めるツールを導入すれば、インシデントの早期検出と調査が可能になり、根本原因分析の効果も上がります。ただし可視化の実現範囲はさまざまで、IT プロセス全体の包括的な可視性が極めて良いまたは良いと回答した企業は最も少なく、45% にとどまります (図 13)。

全体として、サーバー、ストレージ、ネットワークといった従来分野では可視性が高く、クラウドコンピューティング、コンテナ、モバイルといった次世代技術の分野では低い傾向にあります。これは、ビジネスに求められる変化のスピードに管理能力が追いついていないことを示しています。IT の運用状況やエンドユーザーの利用状況を可視化して包括的に把握できなければ、顧客やユーザーの利便性といった、IT インシデントで最も懸念される影響を防ぐのが難しくなります。

図 13 の結果から、全体の可視性スコアを計算できます (計算方法は付録を参照)。最大を 4 とする可視性の平均は 2.56 で、改善の余地が大いにあることを示しています。調査対象となった全インフラストラクチャで可視性が完全に確保されていると回答した企業はわずか 2.5% で、0.7% の企業ではいずれのインフラストラクチャも可視化されていませんでした。

調査対象となった全インフラストラクチャで可視性が完全に確保されていると回答した企業はわずか 2.5% で、0.7% の企業ではいずれのインフラストラクチャも可視化されていない

企業が使用している監視ツールの数は平均 19.8 個で、中には 100 個に達するという大規模企業もありました。しかし、80% の企業が監視に死角があると回答しています。死角を減らすには、効果的な監視体制を構築して可視性を高めることが重要です。

可視性を高めれば、インシデントの重複や再発を減らすこともできます。可視化はインシデント検出プロセスの改善策として見過ごされがちな点です (図 14)。また、インシデントの根本原因分析にかける時間を増やし、過去の問題から学んで再発を防止することも、インシデントを減らす効果があります。

図 13：IT インフラの可視性

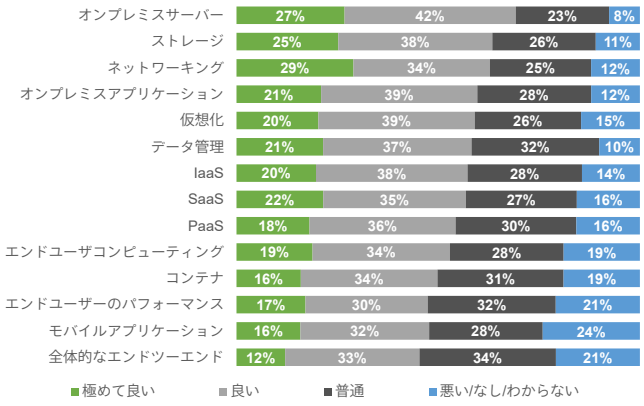
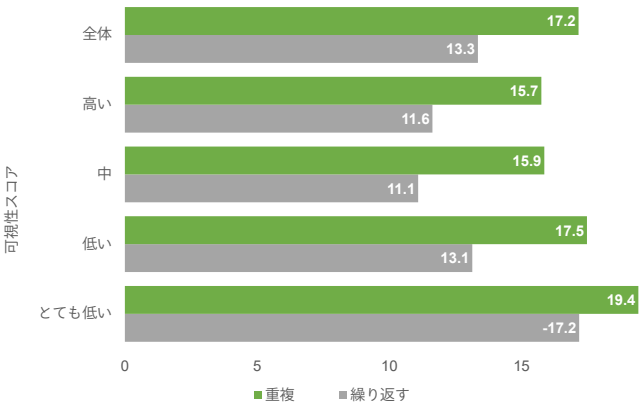
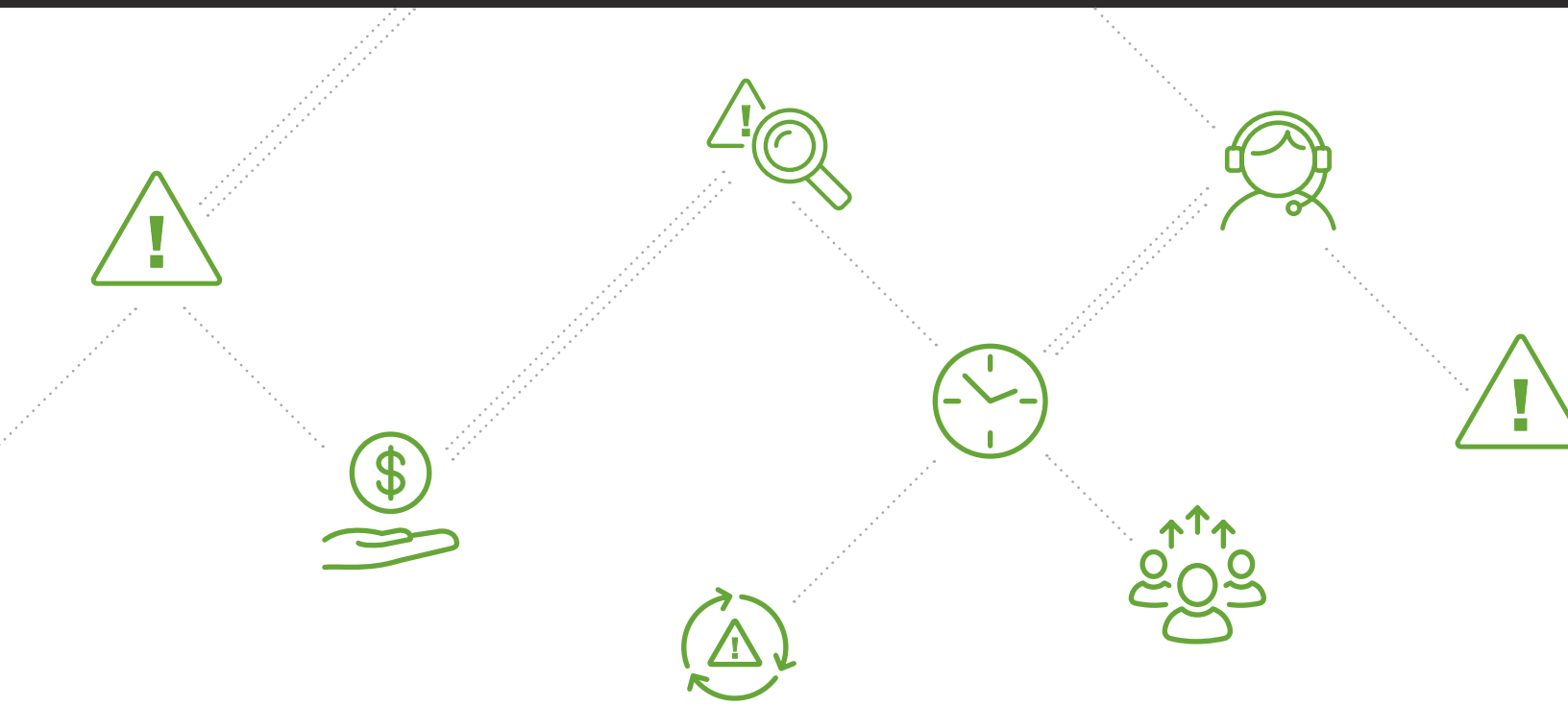


図 14：可視性と重複インシデントの繰り返し





まとめ

IT 部門は、企業の競争力を維持するために、ユーザーや顧客向けの高品質なデジタルサービスを短期間で開発することが求められていますが、IT コストを抑えつつこれを実現する必要もあります。

IT が複雑化するにつれてインシデントを効率的に管理することが難しくなり、結果として IT 部門にもそのユーザーである業務部門にも必要以上のコストが発生しています。デジタル主導のプロセスへの依存度が高まる現在、IT インシデントの管理プロセスの不備はユーザーや顧客に大きな影響を及ぼし、最終的には企業の信頼低下につながることもあります。

重大な IT インシデントへの対応は、IT 部門が最優先で取り組むべき課題です。管理プロセスとそれを支える IT インフラストラクチャを包括的に可視化するツールの導入は必須です。ツールを活用して、IT インシデントをすばやく検出、調査し、根本原因分析を効率的に行って、必要最小限の人数で問題解決に当たることが重要です。これらの取り組みを実現すれば、IT コストだけでなく、IT インシデントがもたらすより大きなビジネスコストと業務への影響も大幅に軽減できます。

こちらをクリックすると、企業の重大 IT インシデントのコストを計算できます。

付録

図 1、9、12 のスコアの計算方法

質問に関して、回答者には該当する選択肢の中から最も該当する順に 3 つまたは 5 つ選んでもらいます。計算時に各選択に次のスコアを割り当てます。

5 つ選択する場合 (図 1、9)

- 選択 1 = 5 (最重要の問題)
- 選択 2 = 4 (2 番目に重要な問題)
- 選択 3 = 3 (3 番目に重要な問題)
- 選択 4 = 2 (4 番目に重要な問題)
- 選択 5 = 1 (5 番目に重要な問題)
- 未選択 = 0

3 つ選択する場合 (図 12)

- 選択 1 = 3 (最重要の問題)
- 選択 2 = 2 (2 番目に重要な問題)
- 選択 3 = 1 (3 番目に重要な問題)
- 未選択 = 0

これらのスコアから各選択肢の加重平均を割り出して、レポート全体で使用したさまざまな問題の懸念や影響の大きさを表しています。回答者に選択を順位付けしてもらうことで、懸念や影響の大きさの違いが明確になっています。

図 13 のデータに基づく可視性スコアの計算方法

インフラストラクチャ全体の可視性スコアは、図 13 の回答で「極めて良い」= 4、「良い」= 3、「普通」= 2、「悪い」= 1、「なし / わからない」= 0 のスコアを割り当ててから、全体の平均スコアを割り出すことによって計算しています。

為替レート

金額に関する調査結果はすべて米ドル単位で示しています。調査では現地通貨で回答してもらい、それを以下の為替レートで米ドルに換算しています (1 米ドルあたり)。

- シンガポール：1.36 ドル
- 日本：112 円
- オーストラリア：1.28 ドル
- スウェーデン：8.05 クローナ
- ユーロ圏：0.85 ユーロ
- 英国：0.76 ポンド

調査対象

調査はすべてシニア IT マネージャーに回答してもらいました。対象となった国と業種および企業規模の内訳を下の図に示します。調査の実行は Quocirca の調査パートナーである Vanson Bourne 社に依頼しました。

調査対象

調査はすべてシニア IT マネージャーに回答してもらいました。対象となった国と業種および企業規模の内訳を下の図に示します。調査の実行は Quocirca の調査パートナーである Vanson Bourne 社に依頼しました。

図 15：ビジネス規模別の国数

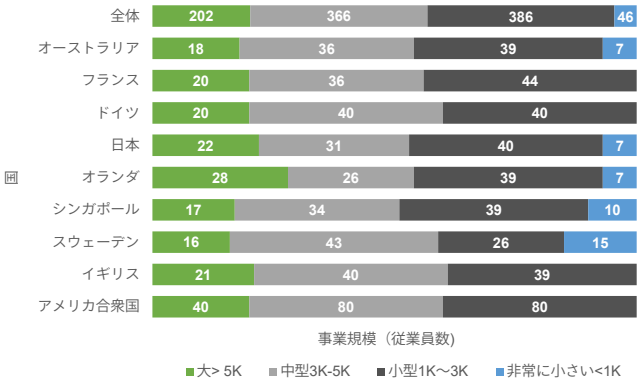
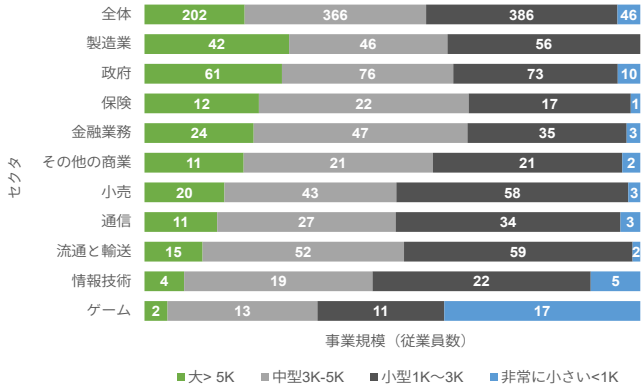


図 16：ビジネス規模別ビジネスセクター



splunk>

SPLUNK について

Splunk Inc. (NASDAQ: SPLK) は、機械学習によってデータから答えを導き出します。お客様は、市場をリードする Splunk の機械学習ソリューションを利用し、IT や IoT (モノのインターネット)、セキュリティ上の難問を解決しています。何百万というユーザーが積極的に利用している Splunk で、「ひらめき」や「気付き」を見つけてみませんか。

www.splunk.com

quocirca

QUOCIRCA について

Quocirca は、英国に本社を置く調査分析会社です。IT に関する意思決定に携わる人を対象とした無料コンテンツを提供しています。その多くは、ヨーロッパ、アメリカ、アジアで幅広い IT 業界団体の支援を受けて行う一次調査に基づいています。Quocirca のコンテンツは、特定の製品ではなく企業の中での IT の使用について、独立した立場で書かれています。Quocirca はメディアとの関係も深く、その記事やレポートは数百万人のインフルエンサーや意思決定者に読まれています。

www.quocirca.com

splunk> | quocirca

詳細はこちら www.splunk.com/ja_jp/talk-to-sales.html
〒 100-0004 千代田区大手町 1-1-1 大手町パークビルディング 8 階

www.splunk.com/ja_jp
splunkjp@splunk.com

WP-Splunk-Quocirca-Cost-of-Critical-IT-Incidents-JA-201712