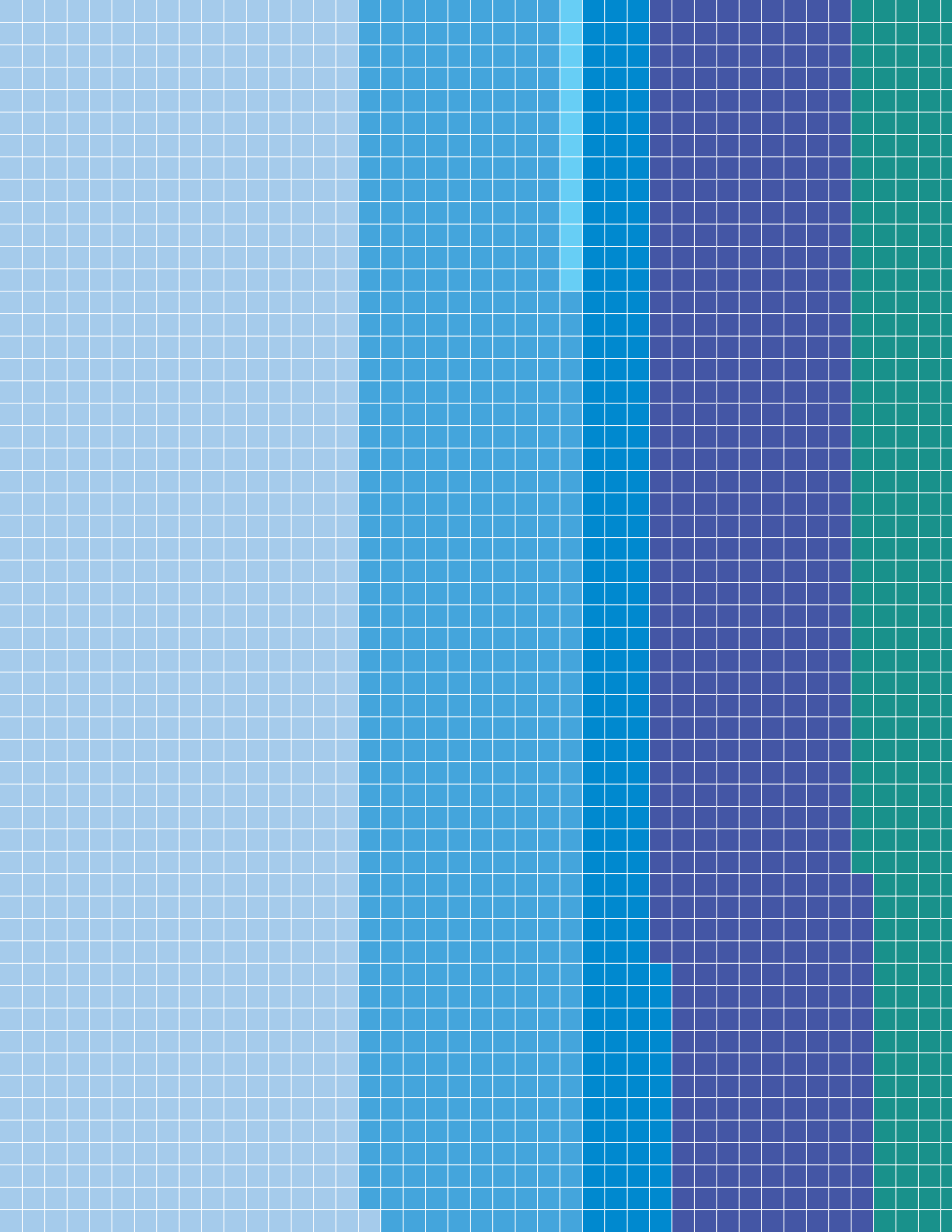
DBIR

2020

# データ漏洩/侵害調査報告書

## エグゼクティブサマリー

verizon



# 3,950件の漏洩/侵害

色分けされたこれらの小さな四角いブロックは、今年のレポートで取り上げた16の業界と世界の4つの地域を表現したものです。各ブロックはおよそ1件の漏洩/侵害を表し（正確には1.04件）、業種と地域の両方を併せて、合計4,675個のブロックで表しています。

また、今年度の調査では過去最高の合計157,525件のインシデントを分析しましたが、そのうち32,002件が当社の品質基準を満たしていました。この報告書でのデータの網羅性は非常に高く、単色の表紙とは対照的に、データ駆動型のリソースであるDBIRの使命がここに強調されています。ページをめくって調査結果をご覧ください。

# 目次

# データとインサイトを活用して常に脅威に備える

脅威の現状を詳細に把握できれば、データのセキュリティを高められるようになり、セキュリティ侵害で紙面を賑わすリスクを減らすことができます。ベライゾンがデータ漏洩/侵害調査報告書（DBIR）を発行している理由はここにあります。13回目の発行となる今年の報告書は、これまでで最も多い81に上る企業の協力を得て作成されました。2020年版のDBIRをまとめるにあたって、DBIRチームは32,002件のセキュリティインシデントを分析し、うち3,950件で漏洩や侵害の発生を確認しています。今回の報告書では、これまで以上に業種別のデータに注目しているほか、新たに地理的な観点からも分析を行っています。

**報告書のハイライトを是非ご覧ください。また、このサマリーを同僚の皆様にご紹介ください。報告書の全文をダウンロードいただくと、現在存在する様々な脅威の現状を詳細に把握できる内容になっています。**

**32,002**

**DBIRチームは、32,002件のセキュリティインシデントを分析し、うち、3,950件で侵害の発生を確認しています。**

### 分析の質の向上に向けた継続的な取り組み

DBIRチームは、インシデントや漏洩/侵害を分類および分析するためのVocabulary for Event Recording and Incident Sharing（VERIS）フレームワークを絶えず拡張しており、今年は、MITRE社のATT&CKとCenter for Internet SecurityのCritical Security Controls（CIS CSC）とのマッピングを行いました。そして、このマッピングを利用して分析を強化し、分析した内容をより大規模なセキュリティコミュニティでも利用できるようにしています。

# 分析の要約

**図1.** 情報漏洩の被害者は誰か?

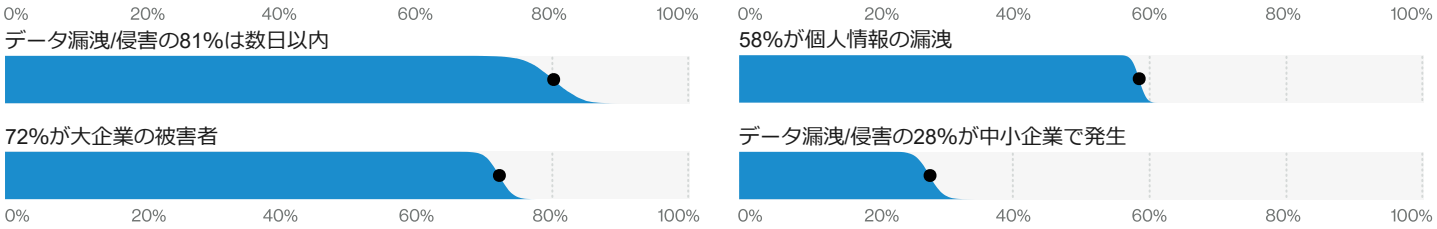



**図2.** 攻撃の背後にいるのは誰か?

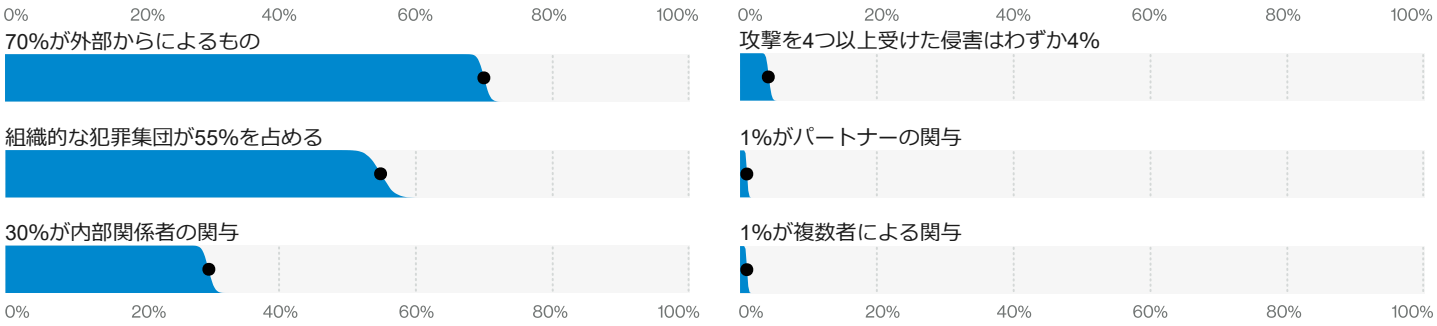
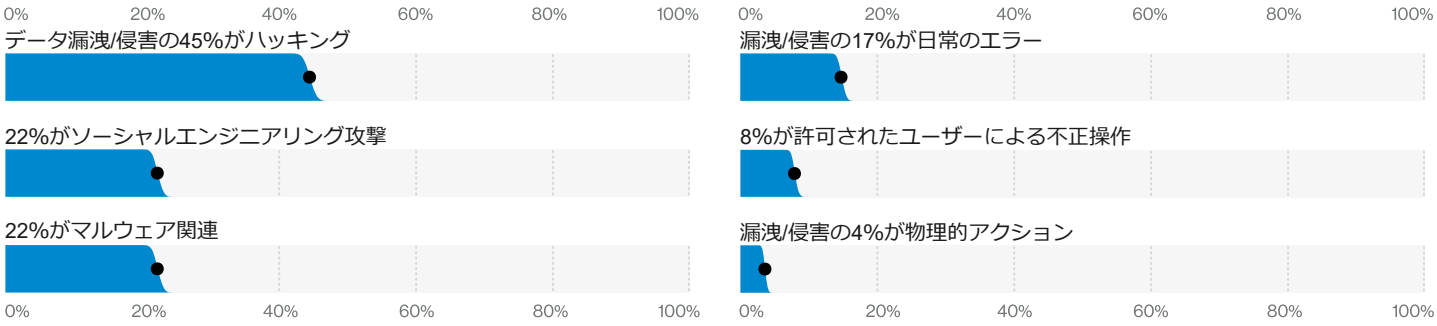



**図3.** どのような手法がとられているか?



# 重要なポイント

## 誤った通説を正す

### ほとんどのデータ漏洩/侵害は外部からの攻撃によって発生

データ漏洩や侵害の原因として最も多いのは内部の関係者による不正行為に関係するものであると多くの人が考えていますが、DBIRのデータによれば、従来と同様に依然として外部からの攻撃のほうがずっと多く確認されており、その証拠に本年の報告書における漏洩/侵害の70%は外部からの攻撃によるものです。

### ほとんどのデータ漏洩/侵害が、金銭を奪うことをその目的としている

サイバースパイ活動はマスコミを賑わすものの、本年のデータではそのような行為による漏洩や侵害の割合はわずか10%にとどまっており、依然として、その大部分（86%）は、金銭目的であるとしています。また、最近取り上げられることの多い高度な脅威もわずか4%であるにすぎません。

## 攻撃者とその手口に目を向ける

### 同じ手口が何度も使われている

認証情報の盗取、フィッシングやビジネスメール詐欺などのソーシャル攻撃、ユーザーのミスに乗じた攻撃が、データ漏洩/侵害の大部分（67%以上）の要因を占めています。これらの手口はその有効性が明らかになっているため、攻撃者に繰り返し使用されています。ほとんどの企業ではセキュリティ活動の大部分は、これら3つの手口に対する対策に重点を置くべきです。

### どこにでも存在するランサムウェア

現在、ランサムウェアはマルウェアインシデントの27%を占めており、18%の企業が少なくとも1つのランサムウェアを過去にブロックしています。どの企業もランサムウェアを無視できる余裕はありません。

### Webアプリを標的とする攻撃が増加

Webアプリを標的にした攻撃はデータ漏洩/侵害の43%を占めており、その数は昨年の2倍以上になっています。ワークフローがクラウドサービスへと移行するなかで、当然のことながら、攻撃者もその動きに追随しています。機密情報の窃取を目的としてWebアプリを狙った攻撃で最も頻繁に使われるのは、盗み取った認証情報を使用したり、総当たり攻撃で認証情報を割り出したりする手口であり、その割合は80%を超えています。一方、同様の攻撃で脆弱性を狙ったものは20%もありません。

### 増加する個人情報データの漏洩

個人情報データが従来にも増して漏洩や侵害の被害を受けるようになっており、その報告の数もこれまで以上に多くなっています。数が増えているのは多くの場合、情報漏洩に関する規制に起因しています。いずれにしても、個人情報データに関する漏洩/侵害の割合は58%に達しており、昨年のデータの約2倍になっています。この個人情報データにはメールアドレスや氏名、電話番号、住所などのデータが含まれており、これらのデータはメールの中身や構成に不備のあるデータベースから見つけ出すことができます。

### 新規の法律や法改正に伴う報告件数の増加

本年のDBIRからは内部のミスに起因するデータ漏洩や侵害が数多く発生していることが確認できます。その数は昨年が424件であったの対し、今年は881件になっています。人間が完全でないことは当然のことながら、本年の報告でこれだけ件数が増加したのはミスの数が単純に増えたというよりも、新たな法律の制定や既存の法律の改定に伴い、事故報告の要件が厳しくなったことに起因すると考えられます。

## 歓迎すべき傾向

### ツールのブロック性能が向上

セキュリティツールは進化しており、一般的なマルウェアの攻撃はブロックすることができます。DBIRのデータによれば、トロイの木馬型のマルウェアは2016年にデータ漏洩や侵害全体の50%弱を占めるまでになりましたが、これをピークに以後、減少に転じ、昨年ではその割合はわずか6.5%になっています。マルウェアをサンプリングしたところ、その45%がドロッパー、バックドア、キーロガーのいずれかに該当しました。この種類の脅威は未だ数多く存在するものの、その大部分は問題なくブロックできるようになっています。

### 多くの企業が適切にパッチを適用

今回の報告書では脆弱性を突くエクスプロイト攻撃に関係するデータ侵害は5%未満しか確認されませんでした。また、ベライゾンのデータセットではこの種の攻撃を頻繁に行う攻撃者は確認できませんでした。さらに、ベライゾンのセキュリティ情報とイベント管理（SIEM）では脆弱性を突くエクスプロイト攻撃に関係する事故は2.5%しか存在しませんでした。このデータが示すように、ほとんどの企業が適切にパッチを適用するようになっており、そのような企業の数は増え続けています。

しかし、一見するとパッチの適用がスムーズに進んでいるように見えますが、一方で、資産管理の不備に隠れて大きな問題が潜んでいる可能性があります。弊社の調査によれば、ほとんどの企業でインターネットに接続された資産が5つ以上のネットワークにわたって存在しており、このうちに忘れたまま一度もパッチが適用されていない資産があると、それがセキュリティホールとなる危険があります。

**27%**

**ランサムウェアは現在、マルウェアのインシデントの27%を占めています。**

**データ漏洩/侵害において特に頻繁に使われる手口として、認証情報の盗取、ユーザーのミスに乗じた攻撃、ソーシャル攻撃の3つがあります。在宅勤務の従業員は特にこれらの攻撃に対して脆弱です。不確実な要素の多い現在の環境では、このような的を絞ったセキュリティ対策が効果を発揮します。**

# 業種別のハイライト

**規模や業種に関係なく、どの企業もサイバー攻撃のリスクにさらされています。しかし多くの場合、最も遭遇する確率の高い攻撃のタイプは企業ごとに違いがあります。効果的に防御を行いセキュリティ予算を最大限に活用するためには、大局的に状況を把握すると同時に、個々の業種で最も使用されている攻撃の手口を理解することが必要です。本年の報告書では調査対象の業種の区分を16まで増やしました。また、企業の大小で脅威の内容がどう違うのかの分析も行いました。なお、企業の分類には北米産業分類システム（NAICS）のコードを利用しました。**

## 宿泊および飲食業（NAICS 72）

この業種のデータ漏洩/侵害は、もはや過去にその大部分を占めていたPOS関係の攻撃によるものではありません。漏洩や侵害の要因としては、複数のアクションタイプがほぼ均一に影響しており、具体的にはマルウェアやユーザーのミスに乗じた攻撃、盗み取った認証情報を使ったハッキングなどが挙げられます。この業種では金銭目的のハッカーによるクレジットカードの情報を狙った攻撃が頻繁に確認されています。

| | |
|---|---|
| **頻度** | インシデント125件、確認されたデータの暴露92件 |
| **上位3つのパターン** | 「クライムウェア」、「Webアプリケーション攻撃」、「POSへの侵入」がデータ漏洩/侵害全体の61%を占める |
| **攻撃者** | 外部（79%）、内部（22%）、複数の関係者（2%）、パートナー（1%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（98%）、二次的動機（2%）（漏洩/侵害） |
| **侵害されたデータ** | 決済情報（68%）、個人情報（44%）、認証情報（14%）、その他（10%）（漏洩/侵害） |
| **上位3つの対策** | ネットワークポート、プロトコル、サービスの制限と制御（CSC 9）、境界防御（CSC 12）、データ保護（CSC 13） |

## 芸術、娯楽およびレクリエーション業（NAICS 71）

この業種では、Webアプリケーションを標的とした攻撃によるデータ漏洩や侵害が多く発生しています。また、DoS攻撃における1秒あたりのビット数がデータセット全体と比較して多くなっているほか、ソーシャルエンジニアリング攻撃やユーザーのミスに乗じた攻撃も多く確認されています。

| | |
|---|---|
| **頻度** | インシデント194件、確認されたデータの暴露98件 |
| **上位3つのパターン** | 「Webアプリケーション攻撃」、「多種多様なエラー」、「その他全て」がデータ漏洩/侵害の68%を占めている |
| **攻撃者** | 外部（67%）、内部（33%）、パートナー（1%）、複数の関係者（1%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（94%）、自己都合（6%）（漏洩/侵害） |
| **侵害されたデータ** | 個人情報（84%）、医療情報（31%）、その他（26%）、決済情報（25%）（漏洩/侵害） |
| **上位3つの対策** | 境界防御（CSC 12）、セキュアな設定（CSC 5、CSC 11）、セキュリティ意識向上トレーニングプログラムの実施（CSC 17） |

## 建設業（NAICS 23）

この業種では、Webアプリケーションを標的とする攻撃やソーシャルエンジニアリング攻撃の被害が発生しているほか、窃取した認証情報を悪用する手口も依然として問題になっています。ただし、建設業ではパッチの適用率が全業種の平均よりも高く、従業員のセキュリティ関連のミスの数が驚くほど低く抑えられています。

| | |
|---|---|
| **頻度** | インシデント37件、確認されたデータの暴露25件 |
| **上位3つのパターン** | 「その他の全て」、「Webアプリケーション攻撃」、「クライムウェア」がインシデント全体の95%を占めている |
| **攻撃者** | 外部（95%）、内部（5%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（84%～100%）、怨恨（0%～16%）（漏洩/侵害）[1] |
| **侵害されたデータ** | 個人情報、認証情報 |
| **上位3つの対策** | セキュアな設定（CSC 5, CSC 11）、境界防御（CSC 12）、アカウントの監視およびコントロール（CSC 16） |

## 教育サービス業（NAICS 61）

この業種では、データ漏洩/侵害の28%はフィッシング攻撃に起因しており、一方、窃取した認証情報を悪用したハッキングによる侵害が23%発生しています。また、インシデントデータのうち、マルウェア感染の約80%をランサムウェアが占めています。この業種では、フィッシング攻撃を受けた場合の報告の面で不備があり、データ侵害を受けた企業は迅速な対応ができていません。

| | |
|---|---|
| **頻度** | インシデント819件、確認されたデータの暴露228件 |
| **上位3つのパターン** | 「その他全て」、「多種多様なエラー」、「Webアプリケーション攻撃」がデータ漏洩/侵害の81%を占めている |
| **攻撃者** | 外部（67%）、内部（33%）、パートナー（1%）、複数の関係者（1%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（92%）、愉快犯（5%）、自己都合（3%）、スパイ活動（3%）、二次的動機（2%）（漏洩/侵害） |
| **侵害されたデータ** | 個人情報（75%）、認証情報（30%）、その他（23%）、内部情報（13%）（漏洩/侵害） |
| **上位3つの対策** | セキュリティ意識向上トレーニングプログラムの実施（CSC17）、境界防御（CSC12）、セキュアな設定（CSC5、CSC11） |

## 金融および保険業（NAICS 52）

この業種でのデータ漏洩/侵害は、金銭目的の外部攻撃者に起因するものが63%を占め、内部の関係者による金銭目的の犯行によるものが18%、内部の関係者のミスに起因するものが9%存在します。また、窃取した認証情報でWebアプリケーションを攻撃する漏洩や侵害も繰り返しこの業種を悩ませています。内部の人間に起因する漏洩/侵害は、悪意のあるアクションによるものから悪意のないヒューマンエラーによるものへと内容が変わりつつあります。ただし、影響は変わらず大きな被害をもたらしています。

| | |
|---|---|
| **頻度** | インシデント1,509件、確認されたデータの暴露448件 |
| **上位3つのパターン** | 「Webアプリケーション攻撃」、「多種多様なエラー」、「その他全て」がデータ漏洩/侵害全体の81%を占めている |
| **攻撃者** | 外部（64%）、内部（35%）、パートナー（2%）、複数の関係者（1%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（91%）、スパイ活動（3%）、怨恨（3%）（漏洩/侵害） |
| **侵害されたデータ** | 個人情報（77%）、その他（35%）、認証情報（35%）、銀行情報（32%）（漏洩/侵害） |
| **上位3つの対策** | セキュリティ意識向上トレーニングプログラムの実施（CSC17）、境界防御（CSC12）、セキュアな設定（CSC5、CSC11） |

## 医療および社会福祉業（NAICS 62）

この業種では、金銭目的の犯罪者グループによるランサムウェア攻撃が頻繁に確認されています。また、インシデントデータセットを見ると、資産の盗難や消失も依然として問題になっています。基本的なヒューマンエラーが未だに存在し、その数も少なくありません。エラーのタイプで最も多いのは、配信に関するエラーであり、一方で企業内部でのユーザーによるエラーは減少しています。

| | |
|---|---|
| **頻度** | インシデント798件、確認されたデータの暴露521件 |
| **上位3つのパターン** | 「Webアプリケーション攻撃」、「多種多様なエラー」、「その他全て」がデータ漏洩/侵害の72%を占めている |
| **攻撃者** | 外部（51%）、内部（48%）、パートナー（2%）、複数の関係者（1%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（88%）、愉快犯（4%）、自己都合（3%）（漏洩/侵害） |
| **侵害されたデータ** | 個人情報（77%）、医療情報（67%）、その他（18%）、認証情報（18%）（漏洩/侵害） |
| **上位3つの対策** | セキュリティ意識向上およびトレーニングプログラム（CSC17）、境界防御（CSC12）、データ保護（CSC13） |

## 情報産業（NAICS 51）

この業種では、Webアプリケーションの脆弱性を突いた攻撃や盗取した認証情報を悪用した攻撃が数多く確認されています。依然としてヒューマンエラーが漏洩/侵害発生の大きな要因になっており、クラウドデータベースの構成の不備がエラーの大半を占めています。また、この業種では依然として、DoS攻撃の増加が問題になっています。

| | |
|---|---|
| **頻度** | インシデント5,741件、確認されたデータの暴露360件 |
| **上位3つのパターン** | 「Webアプリケーション攻撃」、「多種多様なエラー」、「その他全て」がデータ漏洩/侵害の88%を占めています。 |
| **攻撃者** | 外部（67%）、内部（34%）、複数の関係者（2%）、パートナー（1%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（88%）、スパイ活動（7%）、愉快犯（2%）、怨恨（2%）、その他（1%）（漏洩/侵害） |
| **侵害されたデータ** | 個人情報（69%）、認証情報（41%）、その他（34%）、内部情報（16%）（漏洩/侵害） |
| **上位3つの対策** | セキュアな設定（CSC 5、CSC 11）、継続的な脆弱性管理（CSC 3）、セキュリティ意識向上トレーニングプログラムの実施（CSC 17） |

## 製造業（NAICS 31-33）

製造業は、パスワードダンパーマルウェアや盗取した認証情報を使用してシステムに侵入したり、データを盗み出したりする外部からの攻撃を受けています。攻撃のほとんどは金銭目的の攻撃ですが、この業種ではスパイ活動を目的とした攻撃も相当な数が確認されています。また、従業員がアクセス権限を悪用してデータを不正に持ち出すケースも依然として問題になっています。

| | |
|---|---|
| **頻度** | インシデント922件、確認されたデータの暴露381件 |
| **上位3つのパターン** | 「クライムウェア」、「Webアプリケーション」、「特権の悪用」が漏洩/侵害の64%を占めています。 |
| **攻撃者** | 外部（75%）、内部（25%）、パートナー（1%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（73%）、スパイ活動（27%）（漏洩/侵害） |
| **侵害されたデータ** | 認証情報（55%）、個人情報（49%）、その他（25%）、決済情報（20%）（漏洩/侵害） |
| **上位3つの対策** | 境界防御（CSC12）、セキュリティ意識向上トレーニングプログラムの実施（CSC17）、データ保護（CSC13） |

## 鉱業、採石業、石油・ガス採掘業（NAICS 21）および公益事業（NAICS 22）

漏洩/侵害のタイプは多岐にわたりますが、インシデントデータの多くはフィッシングやなりすましなどのソーシャル攻撃に関するものです。ただし、データの漏洩は確認されませんでした。オペレーションテクノロジー（OT）資産に関係するスパイ活動を目的とした攻撃やインシデントも、この業種では問題になっています。

| | |
|---|---|
| **頻度** | インシデント194件、確認されたデータの暴露43件 |
| **上位3つのパターン** | 「その他全て」、「Webアプリケーション攻撃」、「サイバー諜報活動」がデータ漏洩/侵害の74%を占めている |
| **攻撃者** | 外部（75%）、内部（28%）、複数の関係者（2%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（63%～95%）、スパイ活動（8%～43%）、自己都合/その他/二次的動機（各0%～17%）、恐怖/愉快犯/怨恨/イデオロギー（各0%～9%）（漏洩/侵害）[1] |
| **侵害されたデータ** | 認証情報（41%）、個人情報（41%）、その他（35%）、内部情報（19%）（漏洩/侵害） |
| **上位3つの対策** | セキュアな構成（CSC 5、CSC 11）、境界防御（CSC 12）、セキュリティ意識向上トレーニングプログラムの実施（CSC 17） |

## その他のサービス業（NAICS 81）

その他のサービスには、様々な種類のビジネスが含まれており、パーソナルサービスや修理サービス、非営利の宗教法人や公益団体などがあります。金銭目的の外部からの攻撃が最も多く、Webアプリケーションを標的にした攻撃がデータ漏洩/侵害の39%を占めています。この業種では、従業員のミスも問題になっており、特に構成やデリバリーの不備が目立っています。認証情報もよく狙われる標的ですが、最も盗まれることが多いのは個人情報データです。

| | |
|---|---|
| **頻度** | インシデント107件、確認されたデータの暴露66件 |
| **上位3つのパターン** | 「Webアプリケーション攻撃」、「多種多様なエラー」、「その他全て」が漏洩/侵害の83%を占めています。 |
| **攻撃者** | 外部（68%）、内部（33%）、複数の関係者（2%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（60%～98%）、スパイ活動（0%～28%）、自己都合/恐怖/愉快犯/怨恨/その他/二次的動機（各0%～15%）（漏洩/侵害）[1] |
| **侵害されたデータ** | 個人情報（81%）、その他（42%）、認証情報（36%）、内部情報（25%）（漏洩/侵害） |
| **上位3つの対策** | 境界防御（CSC 12）、セキュリティ意識向上トレーニングプログラムの実施（CSC 17）、セキュアな設定（CSC 5、CSC 11） |

## 専門的・科学的・技術的サービス業（NAICS 54）

この業種では、金銭目的の攻撃者が認証情報を盗み、それを利用してWebアプリケーションインフラストラクチャに攻撃を仕掛ける事例が後を絶ちません。不正アクセスに利用されるのは、フィッシングやなりすましといったソーシャルエンジニアリングの手口がほとんどです。また、この業種は定期的にDoS攻撃を受けています。

| | |
|---|---|
| **頻度** | インシデント7,463件、確認されたデータの暴露326件 |
| **上位3つのパターン** | 「Webアプリケーション攻撃」、「その他全て」、「多種多様なエラー」がデータ漏洩/侵害の79%を占めている |
| **攻撃者** | 外部（75%）、内部（22%）、パートナー（3%）、複数の関係者（1%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（93%）、スパイ活動（8%）、イデオロギー（1%）（漏洩/侵害） |
| **侵害されたデータ** | 個人情報（75%）、認証情報（45%）、その他（32%）、内部情報（27%）（漏洩/侵害） |
| **上位3つの対策** | セキュアな設定（CSC 5、CSC 11）、セキュリティ意識向上とトレーニングプログラムの実施（CSC 17）、境界防御（CSC 12） |

## 公務（NAICS 92）

この業種では、ランサムウェアが大きな問題となっており、金銭目的の攻撃者は広範な政府関係機関を標的としてのランサムウェア攻撃を仕掛けています。また、政府・公共機関では配信や構成のミスが依然として多く存在します。

| | |
|---|---|
| **頻度** | インシデント6,843件、確認されたデータの暴露346件 |
| **上位3つのパターン** | 「多種多様なエラー」、「Webアプリケーション」、「その他全て」がデータ漏洩/侵害の73%を占めている |
| **攻撃者** | 外部（59%）、内部（43%）、複数の関係者（2%）、パートナー（1%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（75%）、スパイ活動（19%）、愉快犯（3%）（漏洩/侵害） |
| **侵害されたデータ** | 個人情報（51%）、その他（34%）、認証情報（33%）、内部情報（14%）（漏洩/侵害） |
| **上位3つの対策** | セキュリティ意識向上トレーニングプログラムの実施（CSC17）、境界防御（CSC12）、セキュアな設定（CSC5、CSC11） |

# 不動産業、レンタルおよびリース業（NAICS 53）

この業種では、盗み取った認証情報を利用してWebアプリケーションを攻撃する事例が頻繁に確認されています。ソーシャルエンジニアリング攻撃も多数確認されており、この攻撃では攻撃者は資産の移転のプロセスに自身の情報を埋め込み、自らの銀行口座に直接金銭を振り込ませようとします。他の多くの業種と同様に、この業種でも構成の不備がセキュリティに影響を及ぼしています。

| | |
|---|---|
| **頻度** | インシデント37件、確認されたデータの暴露33件 |
| **上位3つのパターン** | 「Webアプリケーション攻撃」、「その他全て」、「多種多様なエラー」がデータの漏洩/侵害の88%を占めている |
| **攻撃者** | 外部（73%）、内部（27%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（45%～97%）、自己都合/スパイ活動（各0%～40%）、恐怖/愉快犯/怨恨/イデオロギー/その他/二次的動機（各0%～21%）（漏洩/侵害）[1] |
| **侵害されたデータ** | 個人情報（83%）、内部情報（43%）、その他（43%）、認証情報（40%）（漏洩/侵害） |
| **上位3つの対策** | セキュアな設定（CSC 5、CSC 11）、セキュリティ意識向上トレーニングプログラムの実施（CSC 17）、境界防御（CSC 12） |

# 小売業（NAICS 44-45）

この業種では、データ漏洩/侵害の主な要因として、eコマースアプリケーションを標的とした攻撃が圧倒的多数を占めています。この業種の企業は主要な業務をWebに移行し続けていますが、犯罪者もその動きに追随しています。この業種で長年にわたり主要な問題になっていたPOS関連のデータ漏洩や侵害は、Webへの移行の影響を受けて減少し続け、2019年のDBIRで最も件数が少なくなりました。標的となるデータタイプとしてはクレジットカードの情報が一般的ですが、個人情報や認証情報も狙われることが少なくありません。

| | |
|---|---|
| **頻度** | インシデント287件、確認されたデータの暴露146件 |
| **上位3つのパターン** | 「Webアプリケーション攻撃」、「その他全て」、「多種多様なエラー」がデータ漏洩/侵害の72%を占めている |
| **攻撃者** | 外部（75%）、内部（25%）、パートナー（1%）、複数の関係者（1%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（99%）、スパイ活動（1%）（漏洩/侵害） |
| **侵害されたデータ** | 個人情報（49%）、決済情報（47%）、認証情報（27%）、その他（25%）（漏洩/侵害） |
| **上位3つの対策** | 境界防御（CSC12）、セキュアな設定（CSC5、CSC11）、継続的な脆弱性管理（CSC3） |

# 運輸および倉庫業（NAICS 48-49）

この業種を標的にしているのは、Webアプリケーションに攻撃を仕掛ける金銭目的の犯罪者集団です。一方で、制御機能のない大規模なデータベースを構築してしまうといったような従業員のミスも繰り返し問題になっています。このような要素にフィッシングやなりすましといったソーシャルエンジニアリングの手口を加えると、この業種で発生している大部分の漏洩/侵害の要因がカバーされます。

| | |
|---|---|
| **頻度** | インシデント112件、確認されたデータの暴露67件 |
| **上位3つのパターン** | 「その他全て」、「Webアプリケーション攻撃」、「多種多様なエラー」がデータ漏洩/侵害の69%を占めている |
| **攻撃者** | 外部（68%）、内部（32%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（74%～98%）、スパイ（1%～21%）、コンビニエンス（0%～15%）（漏洩/侵害）1 |
| **侵害されたデータ** | 個人（64%）、認証情報（34%）、その他（23%）（漏洩/侵害） |
| **上位3つの対策** | 境界防御（CSC 12）、セキュリティ意識向上トレーニングプログラムの実施（CSC 17）、セキュアな設定（CSC 5、CSC 11） |

# 中小企業（SMB）に関する詳細な分析

**中小企業（SMB）と大企業ではデータ漏洩や侵害の内容に違いがありますが、クラウドへの環境の移行やWebベースの無数のツールの登場、ソーシャル攻撃の拡大に伴い、その違いは小さくなっています。SMBがビジネスモデルを調整していくなかで、犯罪者も自身のアクションを変更してその歩調を合わせており、最短のルートで最も容易に攻撃を成し遂げられる方法を選択しています。**

| | 小規模（従業員数1,000人未満） | 大規模（従業員数1,000名以上） |
|---|---|---|
| **頻度** | インシデント407件、確認されたデータの暴露221件 | インシデント8,666件、確認されたデータの暴露576件 |
| **上位3つのパターン** | 「Webアプリケーション攻撃」、「その他全て」、「多種多様なエラー」がデータの漏洩/侵害の70%を占めている | 「その他全て」、「クライムウェア」、「特権の悪用」がデータ漏洩/侵害の70%を占めている |
| **攻撃者** | 外部（74%）、内部（26%）、パートナー（1%）、複数の関係者（1%）（漏洩/侵害） | 外部（79%）、内部（21%）、パートナー（1%）、複数の関係者（1%）（漏洩/侵害） |
| **攻撃者の動機** | 金銭目的（83%）、スパイ活動（8%）、愉快犯（3%）、怨恨（3%）（漏洩/侵害） | 金銭目的（79%）、スパイ活動（14%）、愉快犯（2%）、怨恨（2%）（漏洩/侵害） |
| **侵害されたデータ** | 認証情報（52%）、個人情報（30%）、その他（20%）、内部情報（14%）、医療情報（14%）（漏洩/侵害） | 認証情報（64%）、その他（26%）、個人情報（19%）、内部情報（12%）（漏洩/侵害） |

# 地域別の分析

**今年のDBIRでは初めて、地域別のデータ分析を行いました。**

**図4.** 北アメリカ

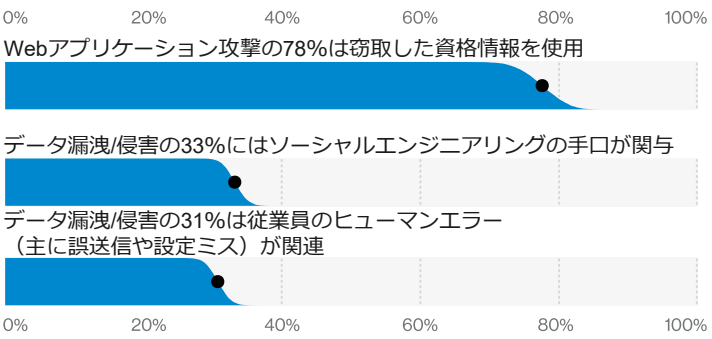



**図5.** 欧州・中東・アフリカ

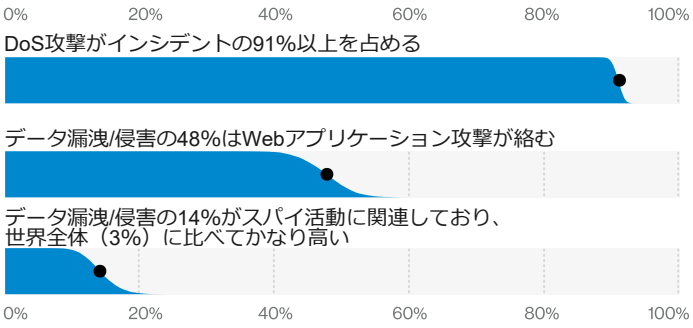



**図6.** アジア太平洋地域

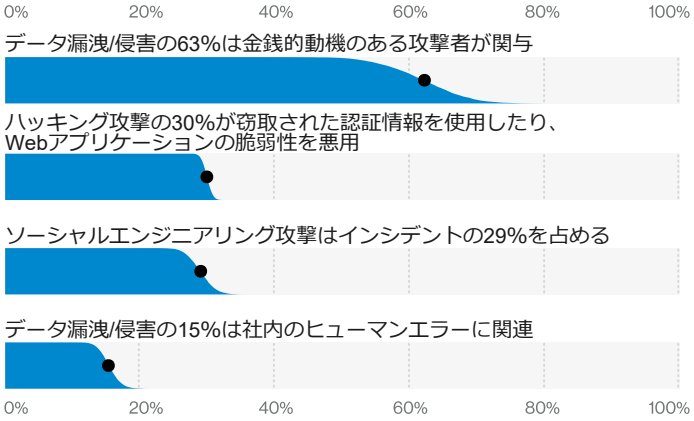
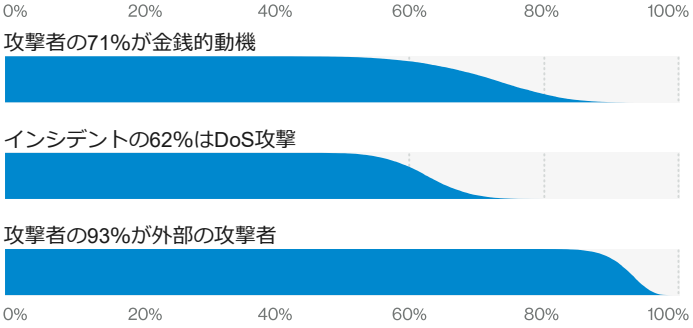



**図7.** ラテンアメリカとカリブ海地域



# ベストプラクティス

**本年のDBIRでは、分析結果をCenter for Internet Security管理と連携させて、DBIRのデータを実際のセキュリティ活動に活かす手法を提供いたします。弊社のデータ分析から、ほとんどの企業で有用であると判断した上位の管理手法の内容を示します。**

### 脆弱性の継続的な管理（CSC 3）

この手法を使用すると、コードベースの脆弱性などを特定、修正できます。また、この手法は構成の誤りを見つけるうえでも大いに役立ちます。

### セキュアな構成（CSC 5、CSC 11）

目的の機能を実現するために必要なサービスやアクセス権限だけでシステムを構成します。また、それを検証します。

### メールとWebブラウザの保（CSC 7）

危険の多いインターネット環境でユーザーを保護できるよう、ブラウザやメールクライアントをロックダウンします。

### ネットワークポート、プロトコル、サービスの制限および制御（CSC 9）

システムで公開する必要のあるサービスやポートを把握し、これらのへのアクセスを制限します。

### 境界の保護（CSC 12）

ファイアウォールだけでなく、ネットワークの監視やプロキシ、多要素認証などの対策も考慮します。

### データの保護（CSC 13）

機密情報のインベントリの管理、機密データの暗号化、承認されたクラウドプロバイダーやメールプロバイダーだけにアクセスを制限することで機密情報へのアクセスを制御します。

### アカウントの監視（CSC 16）

認証情報が盗まれた場合、対象のユーザーアカウントを企業全体でロックダウンして、認証情報を悪用されないようにします。また、このカテゴリに適しているソリューションは多要素認証です。

### セキュリティ啓発/トレーニングプログラムの実施（CSC 17）

悪意のある攻撃や不注意から発生する漏洩/侵害に関するトレーニングをユーザーに実施します。

# 常に最新の情報を入手して脅威に備える

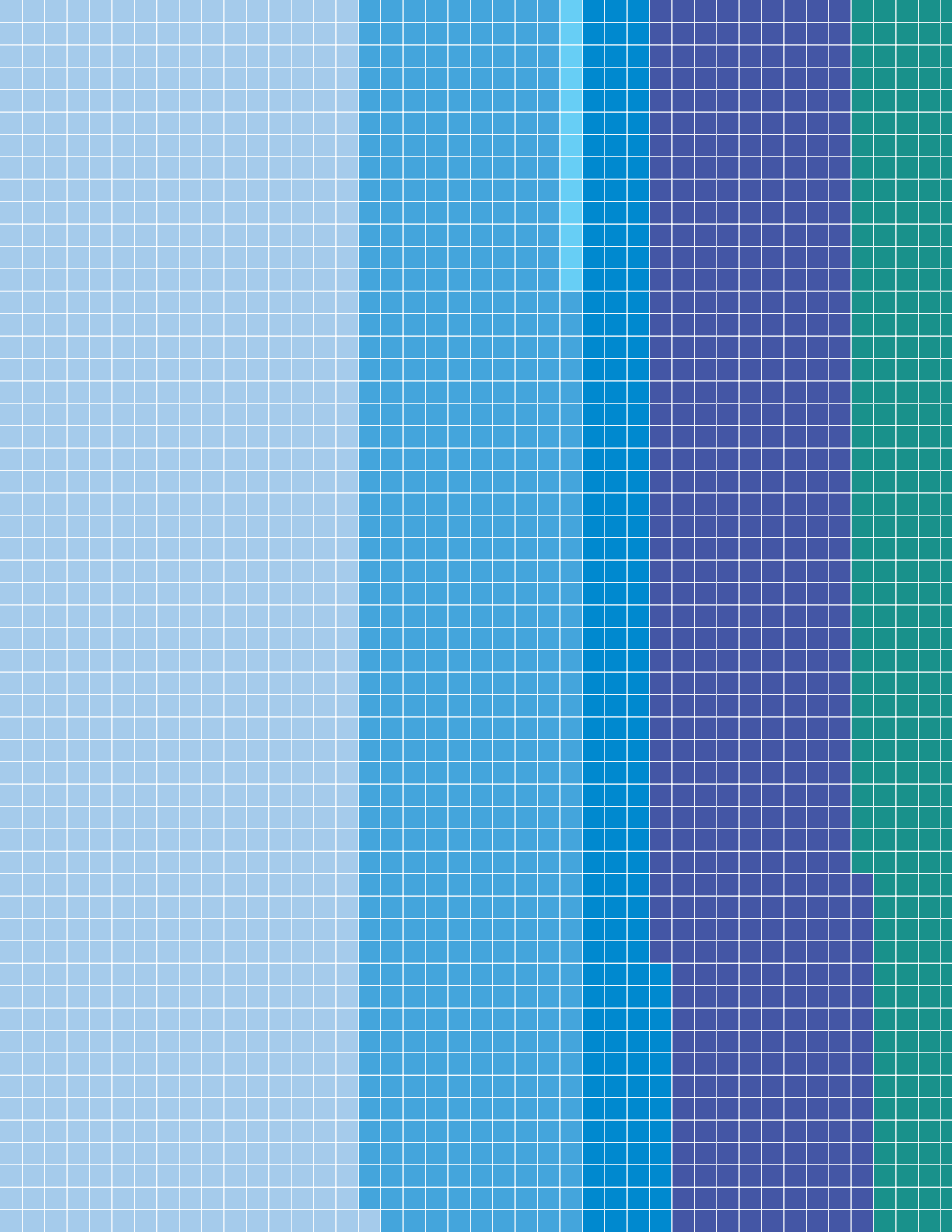
**現代の脅威に対処するためには、信頼できるソースから提供されるインテリジェンスが欠かせません。完全版のDBIRでは、攻撃者や攻撃のアクション、攻撃のパターンについて詳しく説明しており、これらの内容はセキュリティの体制を整える場合や、企業内でセキュリティのトレーニングを行う際に役立ちます。企業を脅威から保護するために必要なインテリジェンスを是非ご活用ください。**

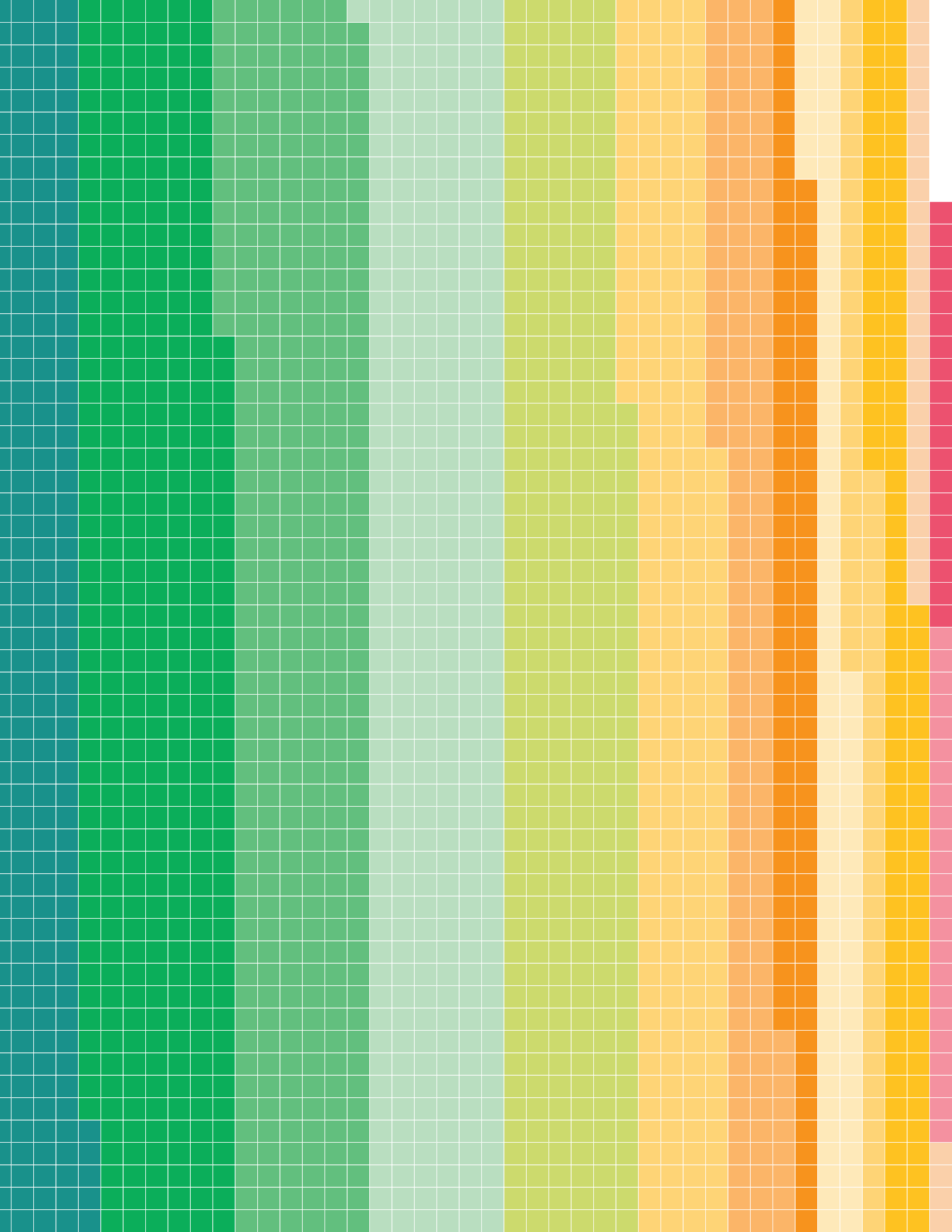
**2020年版のDBIRの全文は、verizon/com/dbirからご覧いただけます。**

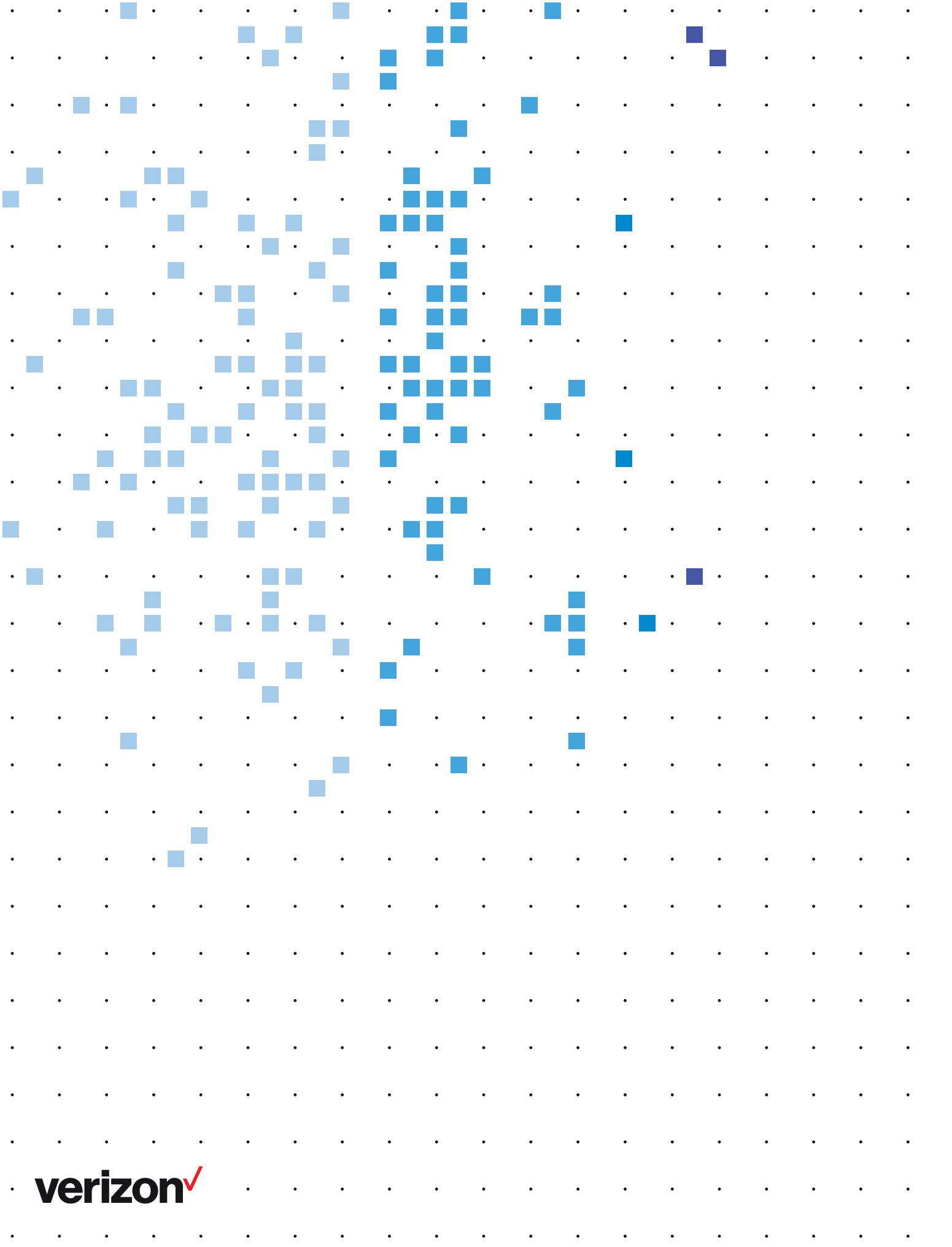
### 次回の調査に是非ご協力ください

DBIRは数十の企業の協力を得てまとめられています。来年の報告書では是非お客様も情報をご提供ください。DBIRに関するご意見はdbir@verizon.comにお送りいただくか、@VZDBIRでツイートしていただくことができます。また、VERIS GitHubのページ（https://github.com/vz-risk/veris）も是非ご覧ください。

1 この資料ではサンプル数が比較的少ないため、このセクションに関する信頼性の幅を明確にするために、様々なパーセンテージを使用しています。このアプローチの詳細については、報告書の全文をご覧ください。






verizon