# 2010年度データ漏洩/侵害調査報告書

ベライゾン ビジネスRISKチームによる分析研究
協力: アメリカ合衆国シークレットサービス

## エクゼクティブサマリー

データ漏洩／侵害はある意味、指紋と共通点が多いと言えます。いずれも同じものは二つとなく、また形状や線、輪郭を分析することによって多くのことが分かります。指紋分析の主な価値は、事件などで残った指紋の主を特定できることにあります。この点を考えると何百、何千という指紋の種類を分析することにメリットを得られることはほとんどありません。一方、多数のデータ侵害を分析することには大きなメリットがあります。調べれば調べるほど、データ侵害を防ぐ態勢を整えることができるからです。

アメリカ合衆国シークレットサービス（USSS）も当然ながら、データ侵害の調査と抑止に高い関心を持っています。この理由から、USSSでは、2010年版データ漏洩／侵害調査報告書への協力が決定されました。この協力によりUSSSの数百のデータ侵害事例が追加され、分析可能な事例数が大幅に増加しました。本報告書では、USSSの活動を付録として2例収録しています。一つは、オンライン犯罪者コミュニティに関するケース、もう一つはサイバー犯罪の訴追に関するケースです。このUSSSの協力を通じて、世界中の組織や個人にさらに有益な情報が提供できると私達は考えています。USSSの関係者にRISKチームの感謝の意をここに記させていただきます。

「データ漏洩／侵害調査報告書（DBIR）」は6年間分の漏洩／侵害事件を網羅した報告書で、2009年度に発生したデータと今回のUSSSからのデータを合計すると、今まで扱ったデータ漏洩／侵害は事例数で900以上に達し、被害を受けたレコード数は9億件を超えます。これまでの調査を通じて得られた教訓は実に多く、その内容を読者の皆さんと共有させていただく機会があることに感謝しています。本調査の目的はこれまでと同様、読者が所属する企業や組織において事業計画やセキュリティ対策を策定する上でその一助として活用していただくことにあります。以下に挙げるのは、報告書の要点と主な分析結果です。

### データ漏洩／侵害の背後にいるのは誰か？

- 70% が外部原因によるもの（-9%）
- 48% がインサイダーによるもの（+26%）
- 11% にビジネスパートナーが関与（-23%）
- 27% が複数の実行者が関与（-12%）

上述のように、本年度の報告書にはUSSSの事例が取り込まれており、そのため分析結果に若干の影響はありましたが、世界的な傾向には大きな変化はありませんでした。まず、2009年に発生した事例のうち、大半の侵害は組織的犯行によって行われ、また、ほぼすべてのデータ窃盗（98%）が被害者組織外の犯罪組織または犯罪者による事件によるものでした。一方、インサイダーによるデータ侵害はUSSSの事例で多く見られ、結果として全体の数値が高く上昇しています。本年度の調査で、部内者による犯罪がこれまでになく「よく見えるようになった」と言えます。ビジネスパートナーが関係した漏洩／侵害は、昨年度も減少傾向にありましたが本年度も減り、2004年以降、過去最低の割合を記録しました。

### データ漏洩／侵害はどのようにして発生するか？

表にあるように、2009年に発生したデータ漏洩／侵害の中では、権限の不正使用によるものが最上位を占め、これはインサイダーによる侵害が増加したことに関連しています。次にハッキングとマルウェアですが、どちらも衰えを見せていません。それぞれ上位の2位と3位を占めており、ハッキングまたはマルウェアによって侵害されたデータは、全侵害データの95%を超えています。このことは、脆弱な認証情報、認証情報の盗難、SQLインジェクション、データキャプチャー、カスタマイズされたマルウェアによる侵害が相変わらず続いており、企業などが情報資産の保護に苦慮していることを示しています。ソーシャルエンジニアリング（フィッシングなど）による侵害は2倍を超える増加を見せ、物理的攻撃（窃盗、機器の改ざん、盗み見など）は数パーセントの増加にとどまりました。

- 48% が権限の不正使用によるもの（+26%）
- 40% がハッキング（-24%）
- 38% がマルウェア（同）
- 28% がソーシャルエンジニアリング（+16%）
- 15% が物理的攻撃を介して発生（+6%）

## どのような共通点があるか？

**98%** がサーバーに置かれていたデータ（-1%）

**85%** の攻撃は、技術的に高度とは思われない（+2%）

**61%** が第三者が発見（-8%）

**86%** の被害者で、ログファイルに侵害の証拠が残されていた

**96%** の侵害は、初歩または中級レベルの統制を実施していれば回避できたと考えられる（+9%）

**79%** の被害者はクレジットカード業界のセキュリティ基準（PCI DSS）への準拠義務があったにもかかわらず未準拠

これまでと同じく、ほぼ全ての漏洩／侵害されたデータはサーバー上またはアプリケーション上から被害を受けていました。これは、侵害の恐れのあるデータが実際に侵害される傾向があることを表しており、この傾向は本年度も同じでした。攻撃の難易度については、高度な攻撃は少ないのですが、これまでと同じく高度な攻撃によって侵害されたレコードの割合は非常に大きく、全侵害レコードの約90%を占めています。高度な攻撃は少なかったという調査結果から、基本的な低コストの内部統制の体制さえ敷いていれば大半の漏洩／侵害は防止できたと言えます。物事は、あとでよく分かるといいますが、教訓も同じです。犯人が常に先手を打つわけではありません。知識が増えれば、それだけ準備の完成度も高まります。準備もそうですが、一般に企業はインシデント（漏洩事故）の発見と対応にも依然として悠長です。侵害の多くは外部の第三者が発見しており、それも発生してから、かなりの時間が経過しています。

本報告書の結論部分に本年度の新しい推奨事項を追加しましたが、右記の推奨事項は、本報告書の初版からこれまで提唱しているものと似ています。繰り返し記載するのは、目の前にあるこれまでの調査と分析結果から、これらの全ての事項が未だに有効であると言えるからです。

この報告書を作成するときにいつも思い起こさせられるのは、弊社にはデータの処理や分析に必要なツールが揃っているということです。ここで大事なのは、作業に最も適したツールを選ぶと同時にツールの切れ味を鈍らせないように、また錆びさせないように注意することです。証拠はいつ発生したかを示してくれるはずですが、これを怠った途端、敵につけこまれる隙を与えてしまうのです。

認証情報を不正に利用したデータ漏洩・侵害事例は多く、これは大きな問題です。昨年の報告書では、デフォルトの認証情報の悪用が目立ちました。本年度は、脆弱な認証情報の悪用と認証情報の盗難が顕著となってきています。この傾向が強かったのは、大半のユーザーに過剰な権限が与えられていることをアタッカーが知っているためと思われます。また、企業がユーザーの行動を十分に監視していないことをアタッカーが知っていたからかもしれません。もしくは、認証情報の悪用が、内部に侵入するのに一番簡単な方法だったかもしれません。理由はどうであれ、何らかの対処が必要です。悪人と善人、つまり不正なユーザーと正規のユーザーとを見分けられなければ、どんなに防御が堅固であっても無意味となってしまうからです。

マルウェアの検出と感染の防止は、年々困難になってきています（特にシステムがアタッカーの手に渡った後は困難です）。そのため、マルウェアに感染したときでも、その後の被害をできるだけ抑えなければならず、この場合、アウトバウンドトラフィックをフィルタリングし、制限することで被害をかなり軽減することができます。

最後に、ログの監視（というより「発掘」という表現の方が適切かもしれません）は大いに価値があり、これは強調しすぎることはありません。ログにはなにかしらの痕跡や徴候が残されており、必要なのは徴候を見つける力を付けることだけです。

## 軽減（解決）対策で重点を置くべき領域は？

- ✔ 不要なデータを削除し、残っているデータを監視・管理する。
- ✔ 必要な管理基準が満たされているかどうか確認する。
- ✔ 上記を再度、チェックする。
- ✔ ウェブアプリケーションのテストとレビューを行う。
- ✔ ユーザーアカウントを監査し、特権ユーザーの行動を監視する。
- ✔ アウトバウンドトラフィックの選別を行う。
- ✔ イベントログを監視し、内容をチェックする。

## メソドロジー

科学の役割は自然世界の物事の「仕組み “How” 」を説明すること、とよく言われます。これは的確な表現であると同時に、複雑なデータ侵害事件を調査し、事実の究明に努めている関係者全員への激励でもあります。ベライゾンも、コンピュータ犯罪における物事の「仕組み」の解明に継続して取り組んでおり、本2010年度データ漏洩／侵害調査報告書（DBIR）は3冊目（補足報告書を含めると5冊目）の報告書となります。

科学的研究の場合、当然のことながら、収集・分析するデータに一貫性のあることが基本の一つです。データ漏洩／侵害調査報告書においても、メソドロジーは厳格な基準をもとに分析をおこなっていますが、完全に一貫性があるとは言えないかもしれません。具体的には、最初の2008年度の報告書（DBIR）は、前年のデータに基づいて作成したものではなく、ベライゾンが保有する過去4年間（2004年～2007年）のデータをまとめて作成した「回顧」報告書でした。データの範囲は広かったのですが、中には古いデータもあり、その関係からいくぶん限界がありました。そして、2009年度DBIRでは、2008年度とは異なり前年のデータが使用され、より最新の傾向が見られるようになりました。分析内容も前年度よりも細かくなっており、新たな分析項目も追加されました。本年度のDBIRの場合も、当初は2009年度DBIRの方法を踏襲し一貫性を維持する予定でした。データの一貫性は、分析を行う場合に確かに価値があります。しかしながら、本DBIRの最終の目標は、一貫性ではなく知識です。「仕組み」を理解し、説明することが目標です。

*USSSの協力によりデータの量が増え、そのためデータ侵害に対する視野が広がったばかりでなく、新たな視点で分析ができるようになりました。後述の説明にあるように、ベライゾンの事例データとUSSSの事例データでは多くの類似点が見られましたが、幾つかの重要な相違点も見つかりました。*

上記の理由から、2010年度DBIRでは方針を変更し、今回初めて「外部」のデータ（ただし信頼性は極めて高い）を追加することにしました。具体的には、アメリカ合衆国シークレットサービス（USSS）の協力によってUSSSのデータ（および専門知識）を得られることになり、これは実に歓迎すべきことでした。この協力によりデータ漏洩／侵害に対する視野が広がったばかりでなく、新たな視点で分析ができるようになりました。ベライゾンの事例データとUSSSの事例データでは類似点も多く見られましたが、重要な相違点もありました。ベライゾンとUSSSのどちらのデータも分析に有益であり、これらを活用することで「仕組み」を理解し、説明するという上記の目標に近づくことができると考えています。

ベライゾンの漏洩／侵害事例データとUSSSの漏洩／侵害事例データを統合するという作業は、両者にとって時間と労力を要する作業でした。いかにこの作業をおこなったかは後に追記しております。

### ベライゾンのデータ収集メソドロジー

分析に使用したデータは、2010年度DBIRの場合も基本的には今までと同じです。つまり、2004年以降、また直前の年（2009年）にベライゾンが実施したフォレンジック調査で得られた直接証拠をデータとし、分析を行いました。分析では、主に2009年のデータを使用しましたが、2004年以降の累積データもすべて参照しました（複数年の傾向分析などに使用）。ベライゾンの調査対応（IR）チームが扱ったケースの中には、漏洩・侵害と確認されなかったものもありましたが、確認された事故・事件のデータだけを採用しました。入力の信頼性と一貫性を確保するため、調査担当者は全員、ベライゾンエンタープライズリスク／インシデントシェアリング（VERIS）フレームワークを用いて事例データと関連情報を記録しました。VERISを使って記録された情報は、その後、RISKインテリジェンスチームに渡され、検証と分析が行われました。また、安全のため、企業や機関、個人の身元が判明する可能性のある情報はすべてケースデータから削除されました。

## USSSのデータ収集メソドロジー

前述のように、今年度は方針を変更しUSSSのデータを追加しました。ここで読者の中には、それでは過去の報告書と、データの一貫性がなくなってしまうのではないか、と考える方もいらっしゃるかもしれませんが、そうではありません。理由は次のとおりです。まず、データの記録・収集に関しては、USSSの方法はベライゾンと若干異なっていました。そこで、USSSではVERISフレームワークをベースとしたアプリケーションを作成し、データを入力しました。次に、まずUSSSが2008年と2009年の2年間[1]に扱った数千というデータ漏洩・侵害事件と事故から、組織（企業・機関）で発生し[2]、かつ漏洩・侵害の事実が確認されたケースのデータだけに絞り込みました。さらに、その中から、ベライゾンがフォレンジックス調査を行わなかったケースだけを抽出しました[3]。その後、上記の事例についてそれぞれ、資料をUSSSから取り寄せるとともに、実際にケースを担当したUSSS調査員に、そのケースのデータの入力を依頼しました。USSS調査員は、調査資料のほか、データ侵害を受けた企業・機関、またフォレンジックス調査会社から提出された報告書を参考にするとともに、現場での経験も加味してデータを入力しました。最終的に、257件のデータ漏洩・侵害のケースデータが抽出され、本報告書のデータとして追加されることになりました。257件のケースデータは、特定の企業や機関、個人を識別できる情報はすべて削除された後、ベライゾンのRISKインテリジェンスチームに提供され分析が行われました。

最後に、本報告書は、世界のすべての企業・機関で発生したすべてのデータ漏洩・侵害ケースを対象とした調査結果ではないことを繰り返し述べさせていただきます。本報告書ではベライゾンとUSSSの両方のデータを使用しているため、どちらか一方のデータを使用したときに比べ（推定上）、より現実を反映した結果が表れているといえますが、データはあくまで「サンプル」です。また、本報告書の分析結果の多くは一般傾向として適切と考えていますが（この自信は年々高まっています）、それでも偏向は存在します。しかしながら、そうであっても、本報告書には、有効かつ明確な事実を含む、豊富な情報が記載されています。いかなる調査や研究でも言えることですが、どの分析結果をいかに活用するかは、最終的には読者に任されています。

### VERISについて

VERISは、共通言語を使ってセキュリティインシデントに関する情報を記録できるフレームワークで、構造化形式、また反復可能な形式で情報を入力できます。「誰が、何にまたは誰かに、どの様なことをして、結果はどうなったか」という物語風に情報を入力すると一定形式のデータ（本報告書に記載されているようなデータ）に変換されます。ベライゾンでは、DBIRのデータ収集方法について質問を受けることが多く、また今以上にセキュリティインシデントに関する情報をより多くの企業・方々と共有したいと考えていることから本年、VERISを公開しました。VERISは無料で使用できます。VERISの概要については弊社ウェブサイト[4]に掲載されていますが、VERIS（完全版）は、VERISコミュニティwiki[5]より入手可能です。弊社のウェブサイトとVERISコミュニティには本報告書で使用している用語や調査背景を説明する参考情報も掲載されています。

1 本報告書に追加したUSSSのケースデータは、2008年と2009年のものです。ただし、2008年のデータのうち70件を超えるケースは、2007年に発生し、その後、USSSが2008年に扱ったデータ漏洩／侵害のデータです。70件を超えるケースのデータはサンプルとして十分な量であるため、3年間の傾向分析に使用しました。その場合、2007年のデータと2008年のデータを分けて扱っています。

2 USSSが調査した窃盗と詐欺に関わる事件の中には、本報告書に追加しなかったケースデータも多くあります。たとえば、個人に対する窃盗や詐欺であって、企業・機関、もしくは企業・機関の資産が関係しない事件のデータは追加しませんでした。また、データが盗まれた後に発生した犯罪事件（「ホワイトプラスチック詐欺」やアイデンティティ窃盗）のデータも本報告書の調査対象には含まれていません。

3 ベライゾンが調査担当した事件にUSSSが何らかの形で関わっていること場合があります（特に規模の大きい事件）。このような事件では、データの重複を避けるためUSSS側のデータを除外しました。つまり、ベライゾンとUSSSが同じ事件を扱った場合、ベライゾンのデータが本報告書のデータとして使用されています。

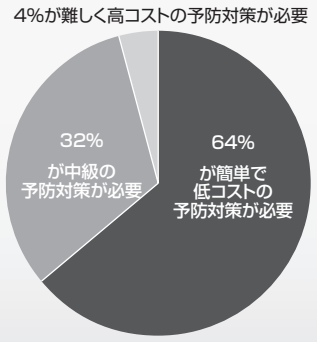
4 http://www.verizonbusiness.com/resources/whitepapers/wp_verizon-incident-sharing-metrics-framework_ja_xg.pdf

5 https://verisframework.wiki.zoho.com/

## 結論と推奨事項

2009年に発生した攻撃を全体的に見ると、攻撃の技術的レベルは以前より若干上がっているものの、防止対策の難度は逆に下がっています。実際、全データ侵害のうち、高難易度で高コストの防止対策が必要とされたデータ侵害は4%に過ぎませんでした（図42）。図43は、具体的な推奨防止対策を分類したものです。図で分かるように、新たな防止対策の導入や購入というより、全データ侵害の40%は既存の資産の設定を変更することで、また26%は既存の運用手順を変更することによって防止できるという結果が出ています。この傾向は、これまでと同様です。

図42. 推奨される予防対策の費用と漏洩／侵害に占める割合*




* ベライゾンのケースデータのみ

セキュリティ管理に関して重要な教訓が一つあります。敵は常に巧妙で情報収集に長けています。しかし、この分析調査を行う際に常に思い起こさせられるのは、私達には調査と分析に必要なツールを持っているということ。そしてここで大事なのは、作業に適した正しいツールを選ぶと同時にツールの切れ味を鈍らせないように、また錆びさせないように注意することです。これを怠った途端、証拠はいつ発生したかを示してくれますが、敵につけこまれる隙を与えてしまうのです。

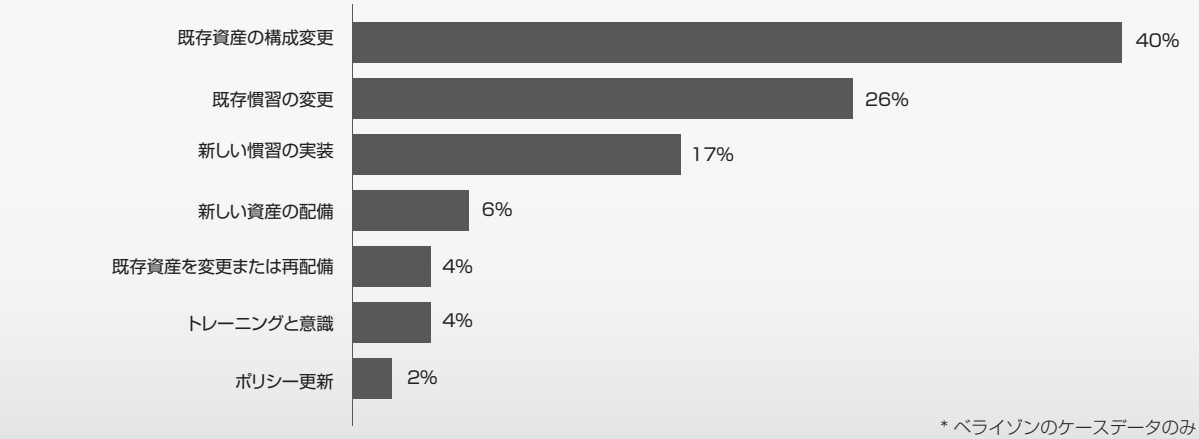
本調査報告書（DBIR）には推奨項目を記載してありますが、実効性の高いものを考案するのは年々難しくなってきています。考えてみればレポートの分析結果は、年ごとに徐々に変化し進化しますが、まったく新しくなったり一変したりすることは稀と言えるでしょう。推奨は、分析結果に基づいているのですから、分析結果が変わらなければ推奨措置も変わらないのは当然です。必要であれば、多数の推奨事項を盛り込んだリストを作り、提供することもできますが、このようなリストは他からも入手できるでしょう。弊社の関心は、数ではなくメリットにあります。今回、2009年の分析結果をもとに、新たな推奨事項をいくつか案出し（これまでの事項の拡張案も含め）、下記に掲載しました。もちろん、2008年度と2009年度のDBIR、また2009年度補足版に記載されている推奨事項も継続的に推奨してまいります。

**権限を持つユーザーの数を減らし、監視する：** USSSから提供されたデータにより、本年から部内者による侵害のデータが増えました。部内者、特に特権ユーザーの管理は簡単ではありませんが、実証済みの対策はいくつかあります。以下に列挙します。信用していても確認を行います。試用期間中の社員をしっかりスクリーニングし、問題が発生する前に対処します。ユーザーに必要以上の権限を与えないようにし（これは特に重要）、職務の分担を行います。適切な指示（会社のポリシーと規定の周知）と監督（ポリシーなどを遵守しているかどうかの確認）がおこなわれるよう体制を整えます。特権ユーザの作業はすべてログし、管理・経営部門に報告されるように設定します。特権ユーザが予定に無い使用を行った場合、アラームが発動し、調査を実施します。

**「ささいな」ポリシー違反に注意する：** 部内者による違反に関しては、会社のポリシーに対する社員の「ささいな」違反と重大な不正行為との間には相関性があり、このことは今までにでも何度か触れています。この理論は、いわば「サイバー犯罪における割れた窓理論（軽微な犯罪を放置しておくと深刻な犯罪に発展するという理論）」と呼べます。そのため、社員のポリシー違反に注意するとともに適宜、相応の対策をとる必要があります。ケースデータの分析によれば、社員のコンピュータに不法なコンテンツやポルノなどが見つかった場合（もしくは不適切な行動が見受けられた場合）、それは将来、データ侵害に発展する恐れがあることを示す徴候です。時折発生する不正行為にその都度対応するより、このような徴候を積極的に監視し注意するほうがはるかに効果的です。

**認証情報の盗難を防ぐ措置を講じる：** 2009年の事例データでは、企業・機関のシステムへの不正アクセスの方法として、認証情報を盗んでアクセスするという方法が最も多く見られました。2009年に単に増加したのか、またはトレンドだったのかに関わらず、認証情報の盗難に対して何らかの方策を講じる必要があります。何よりも最優先されなければならないのは、まず、システムが認証情報捕捉マルウェアに感染しないように注意します。また、必要に応じて2ファクター認証を使用します。そのほか可能であれば、システムの使用可能時間を制限したり、IPブラックリスティング（業務に関係のないIPアドレスをブロック単位または領域単位でブロックします）を行ったり、管理作業のための接続を制限したりします（たとえば、内部の特定のコンピュータからのみ接続できるようにします）。さらに、「直近のログイン履歴」バナーを使用したり、認証情報の盗難が疑われる場合、パスワードを変更したり、その旨を報告するように社員に指導することも有効です。

図43. 推奨される軽減対策の分類と漏洩／侵害に占める割合*




* ベライゾンのケースデータのみ

**アウトバウンドネットワークトラフィックの監視とフィルタリングを行う：** ほとんどの企業では、少なくともインターネットからインバウンドトラフィックについては、一定レベルのフィルタリングを行っています。一般に企業では、外部には内部に入れてはならないものが多く存在する、という（正しい）考えを持ってこの処理を行っています。そして多くの企業が忘れてしまうのが、外部に出してはならないものが内部に多く存在しているということです。これによって外部へのフィルターリングに関心が向けられず、おろそかになることも少なくありません。ベライゾンの調査によると、アウトバウンド・トラフィックのフィルタリングは基本的に必要とされています。データ漏洩／侵害では多くの場合、一連のイベントが発生している間、データが外部に流れたり、外部に対して通信や接続が実行されます。このような状態を防止することで、連鎖を断ち切り、結果的にデータ侵害を終わらせることができます。アウトバウンド・トラフィックの監視、状態の把握、管理を行うことで、侵害行為が軽減される可能性が大きく向上します。

**イベント監視とログ分析の方法を見直し、改善する：** 現在のイベント監視とログ分析の手順を見直すことは、有効な対策です。これは、本報告書の次の分析結果からも裏付けられます。（1）大半の攻撃では、侵害を受けた企業・機関は、データ侵害されるまでに数日以上が経過している、（2）侵害が発見されるまでには、かなりの時間がかかる、（3）侵害の発見者の多くは、侵害を受けた企業・機関以外の者である、（4）最後に、ほぼ全ての被害者企業・機関のログには、侵害の証拠が残っている。このような結果を見ると、イベント監視やログ分析が不十分であり、その方法や手順を変更しなければならないことが分かります。まず、すべてを「リアルタイム」機能に頼ることはやめます。たとえば、IDS/IPSだけで防御するのは不可能です。IDS/IPSなどのほか、ログを活用します。つまり、ログをバッチ処理し、内容をよく分析します。その際、細部（針）より、全体（干し草の山）に注目します。この作業は、手間も費用も多くかけずに、たとえば、ログの行数や長さをカウントし、値が許容値を超えたらアラートが出力されるような簡単なスクリプトを作成します。最後に、異常を発見した際に迅速に対応するための人員の確保と、必要なツール、また十分な手順の整備をおこないます。このアプローチは、メリットも大きく、時間や労力、費用もそれほどかかりません。

**インシデント情報を共有する：** この推奨事項は、最後の推奨対策であると同時に本報告書の結びの段落といえます。本報告書が証明していますが、インシデント情報の共有は現在、安全かつ効率よく行うことができ、情報の信頼性も確かです。弊社が提供するセキュリティプログラムの有効性は、弊社が取り入れるプラクティス（慣習）に依存すると考えています。そして、プラクティスは、私達の意思決定に依存し、意思決定は、私達が真実であると考えている信念に依存しています。私達が持つ信念は、現在持つ知識に基づき、現在の知識は私達が入手する情報によって、そして、私達が入手する情報は、情報を収集し、分析し、共有する誰かに左右されることになります。この依存関係の連鎖を考えた際、私達のセキュリティプログラムの有効性は共有しようとしている情報に左右されると言っても良いでしょう。弊社ではこの活動を重視して継続して推し進め、情報の共有にご協力いただく企業・人員を募っております。

本報告書をご一読いただき、誠にありがとうございました。

verizonbusiness.com/jp

verizonbusiness.com/socialmedia verizonbusiness.com/thinkforward