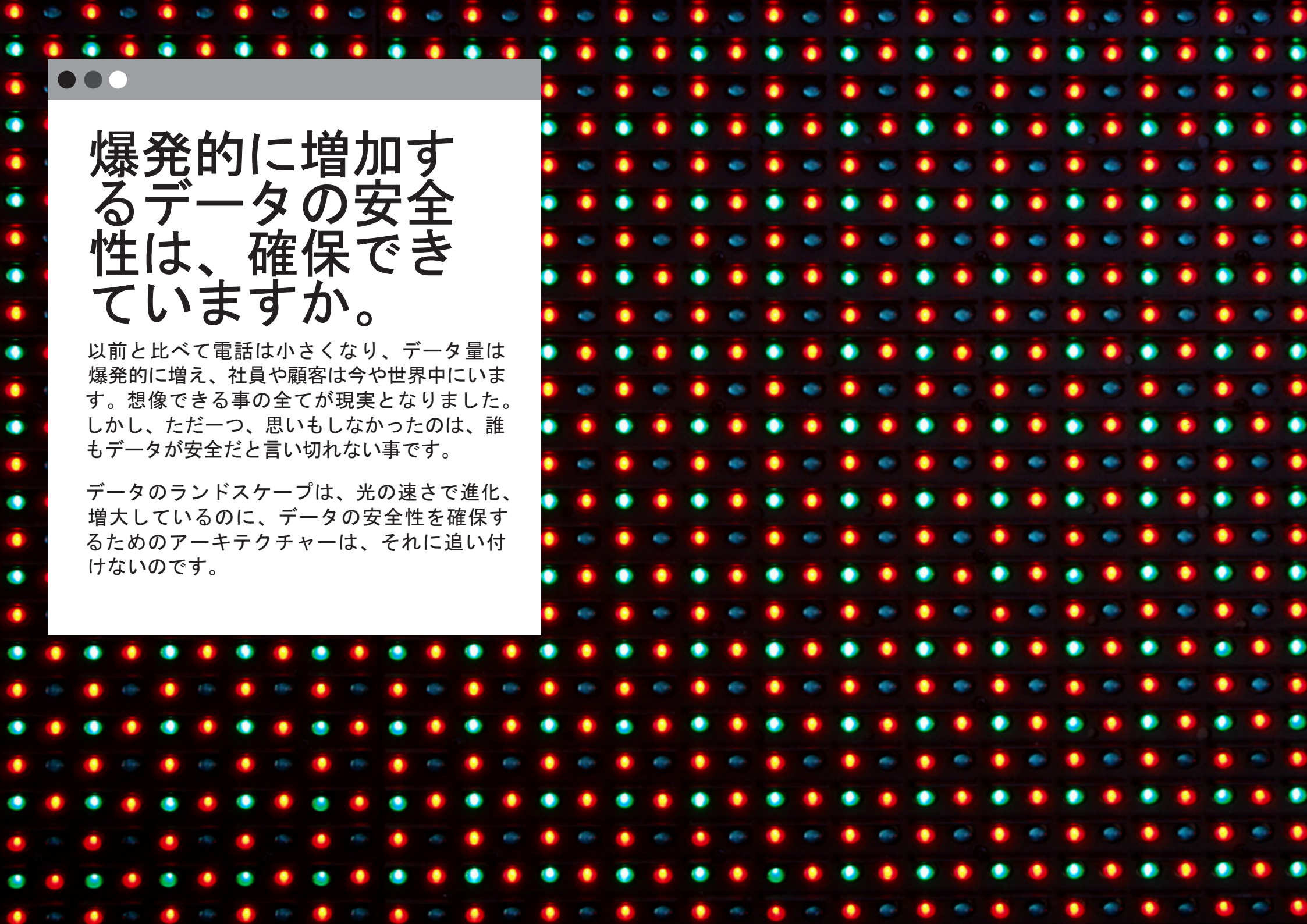
informatica

データ中心型セキュリティ

データ新時代の新しい課題



爆発的に増加するデータの安全性は、確保できていますか。

以前と比べて電話は小さくなり、データ量は爆発的に増え、社員や顧客は今や世界中にいます。想像できる事の全てが現実となりました。しかし、ただ一つ、思いもしなかったのは、誰もデータが安全だと言い切れない事です。

データのランドスケープは、光の速さで進化、増大しているのに、データの安全性を確保するためのアーキテクチャーは、それに追い付けないのです。

状況は最悪です。過去2年間だけでも、以下のような結果です。

Ebay – 1億4,500万件のレコード消失

Target – 7,000万件のレコード消失

Adobe – 1億5,200 万件のレコード消失

Evernote – 5,000 万件のレコード消失[1]

ハッカーは賢くなり、データ侵害は増え、脅威はあらゆる方向からやってきます。問題が膨らむ一方で、データの安全を担う企業は追いかけるのに必死です。

安全か安全でないかを含め、あらゆるデータが企業の枠や方針を超えて飛び交う中で、徐々に見えてきた事実があります。それは、企業の境界線だけにフォーカスした既存のネットワークベースのデータセキュリティアーキテクチャーは、もはや通用しないということです。ファイアウォールの穴が広がった訳ではありません。データは遠くまで移行し、ファイアウォールの中だけに留まらなくなったという事です。

今日、前代未聞の大量データが、全く異なるテクノロジー基盤上の様々な場所を行き来し、そのスピードと範囲は加速しています。巨大化した脅威に対処するには、既存のデータセキュリティレベルでは事足りないのです。


改革が必要です！

問題の根源

既存のデータセキュリティモデルの限界

既存のデータセキュリティアーキテクチャーは、データセンター内にありオンプレミスのデータを保護することを目的としています。つまり、データ規模が小さく、常に監視され、そこから動かないことが前提です。また、社員がリモートからデータにアクセスする際には、適切な（しかし常に機能するとは限らない）セキュリティ制御システムを使用して、企業のネットワークにログオンすることも前提です。

結局は、データを防御の壁で包囲し、それを固守しているだけです。

一方、実世界では・・・

データは、クラウド上の膨大な数のアプリケーションから流出し、社員や顧客が持ち歩いている膨大な数のモバイルデバイスに配信されています。このため、データは巨大化し、保護することは非常に困難な課題となりました。少し前までは、データを一元管理して制御し、安全性を確保していたのに、今やデータが増加し過ぎてコントロール不能になり、非常にリスクの高い状況にあります。

2013年で既に、デジタルの世界に存在するデータのビット数は、宇宙に存在する星の数に匹敵していました[2]。（さらに、企業が新しいデータを発掘するスピードは、天文学者が新たな星を発見するよりもはるかに速いのです。なぜなら今の時代、データこそが黄金の宝だからです。）

つまり、いくらデータセンターの包囲網を固めても、セキュリティは理論的に過ぎません。なぜなら、このようなセキュリティシステムには2つの致命的な欠陥があるからです。

1.データは増加し、移動するという事実を無視している

データ新時代で最も特徴的なのは、データの発生元と送信先が爆発的に多様化したことです。クラウドサービスとモバイル技術が一般化したことで、運用データの量とスピードが急激に増加しました。しかし、こうしたデータは、ファイアウォールでは保護しきれません。

さらに悪いことに、コンプライアンスという重要な問題が無視されています。規制は国によってかなり異なります。ロンドンの本社からインドの開発センターにデータを移動するだけで、データプライバシーに関するいくつもの法律に抵触する恐れがあります。

2.包囲網の内側で起こっている現実を無視している

セキュリティ侵害の50%が、社内で発生している今日[3]、データセンターのファイアウォールをいくら強化しても無意味です。

意図的あるいは単なる人的ミスであれ、管理者や包囲網の内側にいる契約社員が、あらゆるデータへのアクセス権を持っていれば、重大な損害を被るリスクがあります。

そもそもデータ処理のために雇用している社員に対して、データの取り扱いを禁止できないのが問題です。現在のデータセキュリティアーキテクチャーでは、取り扱うデータが増えるほど、リスクも増大します。

悪循環を断ち切るには

新しいデータのランドスケープの基本的特性を無視した既存のセキュリティアーキテクチャーは、大胆な攻撃者の高度な脅威から企業を守ることはできません。攻撃を受けてから対策を講じるような受け身の姿勢が招く悪循環を断ち切るには、全く新しいセキュリティアプローチが必要です。

データ中心型セキュリティ

データ新時代のセキュリティを見据えたビジョン

現在のセキュリティアーキテクチャーは、昔の企業とデータの関係を前提にしているため、全く役に立たないことが多々あります。新しいモデルを導入するなら、データは、企業の生命線として鼓動し、増加しながら生き続けるということを念頭に置かなければなりません。

これを「データ中心型セキュリティ」と呼び、次のように定義します。

データ中心型セキュリティとは、データが移動するエンドポイントやネットワーク、アプリケーションなどを保護するのでなく、データそのものを保護する事です。

つまり、ニーズに応じてデータが自由に移動できるよう、セキュリティも共に移動します。データの増加を抑止、進歩の速度を低下させるようなセキュリティではなく、データがどこに保管され、どこに送信されても、データを最大限に活用できるようなセキュリティです。

データ中心型セキュリティとは

データセキュリティの新たなアプローチを採用するには、次に挙げる4つのプロセスを（現時点では困難でしたが）上手に取り入れなければなりません。

1. 機密データの所在を認識する

自社の機密データがどこに保管されているか自信を持って答えられる企業は全体のわずか16%です[4]。この数字だけ見ても、不安な程に少ない企業しか対応できていませんが、さらに、データを適切にプロファイリングして適切な機密レベルに分類できるのも、たったこれだけの企業しかいないのです。

機密データに接続し、発掘、場所を確認、分類するのは、非常に重要なプロセスです。また、再利用可能なプロセスであり、技術的にも地理的にも依存しないように設定しなければなりません。

2. データのセキュリティ対策を評価する

全てのデータが同じという訳ではありません。データ中心型セキュリティモデルでは、機密データのリスクのレベルを判断する必要があります。つまり、どのユーザーがデータへのアクセス権を持つのか、どんな操作をするのかをモニタリングし、そのデータを保護するために、どのようなセキュリティ対策を講じているかについて、常に把握しておかなければなりません。

3. データを保護する

データ中心型セキュリティでは、データに個別のルールを定義する必要があります。最も詳細なレベルでは、あるユーザーに対してデータをマスキングし、別のユーザーには、完全にブロックするといったことを意味します。そのためには、データがどこで増加しても追跡できるような厳格なデータガバナンスポリシーを適用する方法を知っておく必要があります。

4. データ侵害を検出する

データ中心型セキュリティモデルでは、データがポリシーに準拠していないことを認識できなければなりません。従来のようにログファイルを使って問題の発生個所を探しているようでは手遅れです。プロアクティブに侵害を検出することが重要です。


シフトしましょう
非常に簡単な3つの初め
のステップ

データ中心型セキュリティへの移行は、既存の対策を利用し続けることはできますが、ほとんどの企業が、アプローチとテクノロジーを大幅に改革しなければなりません。

幸いにも、セキュリティモデルをデータ中心に移行するために今すぐ始められる基本的な方法があります。

1. 非運用環境では、本番用データを使わない。

本番用データを、一貫したルールでマスキングをせずに、テストやトレーニングに使用すると、データ漏えいのリスクが高まります。特にテストチームに、契約社員や請負業者、海外の組織が含まれている場合は要注意です。そもそもデータ処理のために雇用している社員に対して、データの取り扱いを禁止できないのが問題です。現在のデータセキュリティアーキテクチャーでは、取り扱うデータが増えるほど、リスクも増大します。

2. データへの不正アクセスを阻止する。

データベース管理者の70%が、未だに全データへのアクセス権を持っています。データ中心型セキュリティモデル導入の第一歩としtて、DBAや外部契約社員が、承認されたデータ以外にアクセスできないように、まずは動的な役割ベースのマスキングを実施しましょう。つまり、業務に必要なデータしか見れないようにするのです。

3. 機密データへのアクセスを監視する。

現在、役割や場所に基づくアクセス制御を行っている企業は全体の41%に過ぎません[4]。データ中心型モデルに移行するためには、ユーザーやデータの場所に応じて、誰が機密データにアクセスできるかを、常に監視し監査するプロセスが必要です。これにより、疑わしいアクセスパターンが検出された際に、自動的に対策となるアクションを実行することができます。

コラボレーションの義務

データアーキテクトとセキュリティアーキテクトが、連携すべき理由

データ中心型モデルへの移行に伴う一般的な傾向は、サイロを解消することです。データや部門のサイロ化は、真実の断片化を招く大きな原因となるからです。

データ中心型セキュリティモデルへ転換するには、これまで交流のなかった人々、つまりデータアーキテクトとセキュリティアーキテクトが連携しなければなりません。

セキュリティアーキテクトがデータアーキテクトの周りに難攻不落の防御線を築いていた時代には、両者が協業する必要はありませんでした。しかし新しいデータのランドスケープで白日の下にさらされる今、互いに協力しないような事は許されません。

考えを共有する

セキュリティアーキテクトは、オープンエンタープライズ内をデータが行き来できるような柔軟性を尊重する姿勢を養う必要があります。

一方、データアーキテクトは、場所を問わず、全てのデータセキュリティを保護するために何が必要かを理解しなければなりません。そうすれば、アプリケーションとユーザーの間でデータが増加してもセキュリティポリシーを強化することができます。

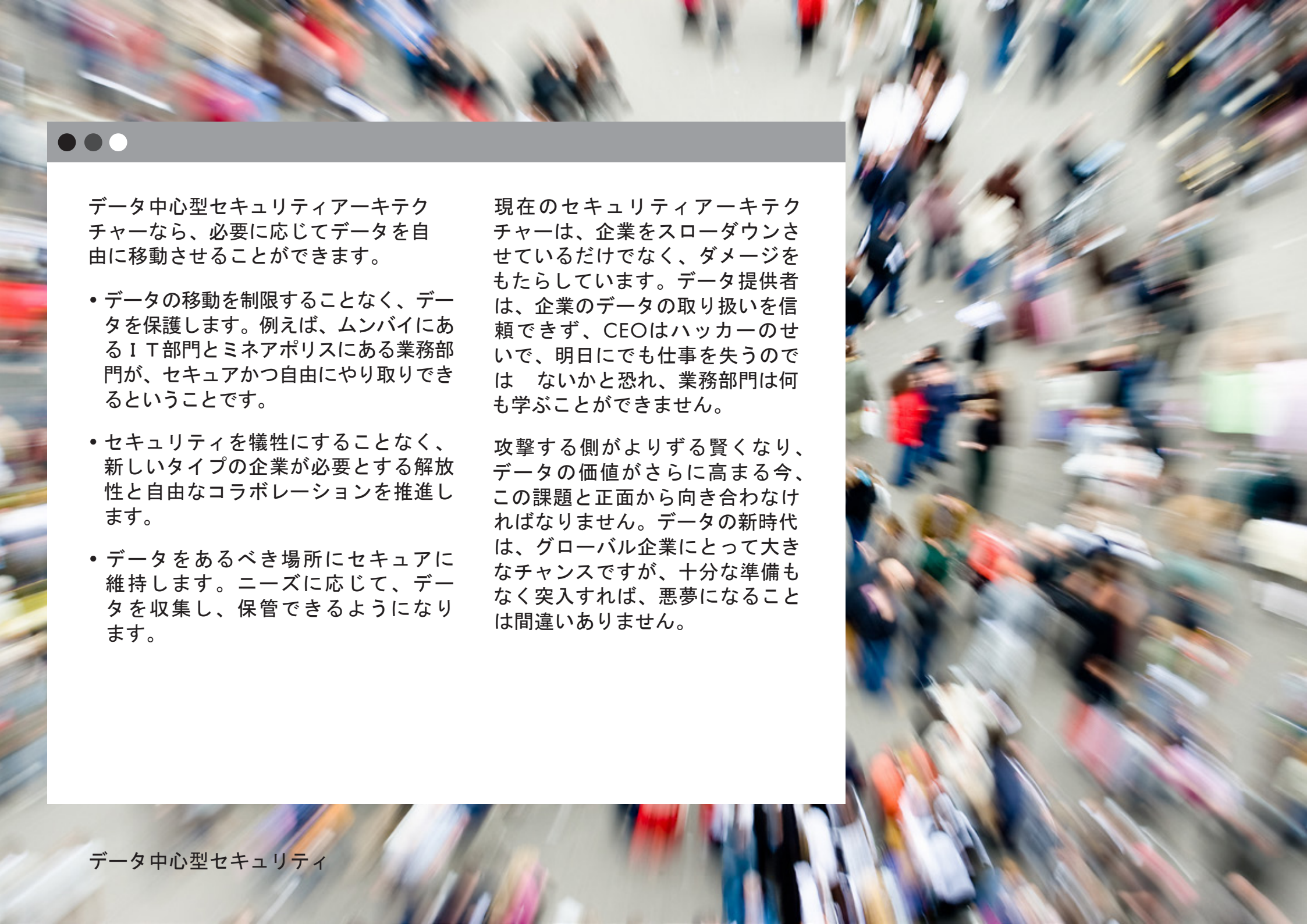
両者の協力関係が早く立ち上がれば、企業の基盤もより強くなります。

二度と侵害されないために

データ中心型セキュリティが重要な理由

データのランドスケープは、一夜にしてその様相を変えました。今後もその変化のスピードは加速し続けるでしょう。

コンプライアンスとセキュリティを妥協せずにコントロールを勝ち取った企業こそが、新しいパラダイムの支配者となります。



データ中心型セキュリティアーキテクチャーなら、必要に応じてデータを自由に移動させることができます。

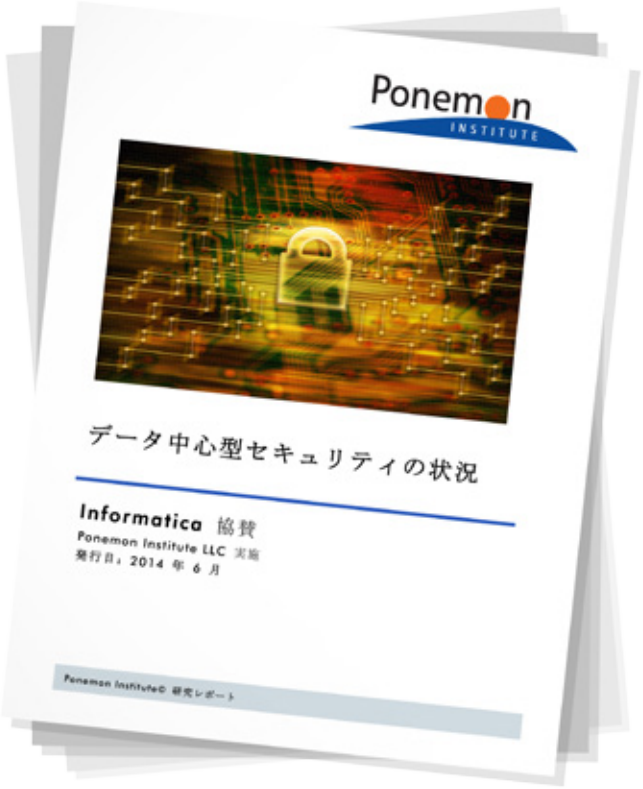
- データの移動を制限することなく、データを保護します。例えば、ムンバイにあるＩＴ部門とミネアポリスにある業務部門が、セキュアかつ自由にやり取りできるということです。
- セキュリティを犠牲にすることなく、新しいタイプの企業が必要とする解放性と自由なコラボレーションを推進します。
- データをあるべき場所にセキュアに維持します。ニーズに応じて、データを収集し、保管できるようになります。

現在のセキュリティアーキテクチャーは、企業をスローダウンさせているだけでなく、ダメージをもたらしています。データ提供者は、企業のデータの取り扱いを信頼できず、CEOはハッカーのせいで、明日にでも仕事を失うのでは　ないかと恐れ、業務部門は何も学ぶことができません。

攻撃する側がよりずる賢くなり、データの価値がさらに高まる今、この課題と正面から向き合わなければなりません。データの新時代は、グローバル企業にとって大きなチャンスですが、十分な準備もなく突入すれば、悪夢になることは間違いありません。

参考資料

データ中心型セキュリティの標準を定義する一環として、PonemonInstituteは、下記のレポートで企業がデータの脅威にどのように対応しているかについて説明しています。



「データ中心型セキュリティの状況」をご覧下さい。

Informatica について

Informaticaは、製品やサプライヤー、顧客に関するビジネス上重要なデータの完全かつ正確に把握できるビューを提供することで、企業がデータ中心にビジネスできるように支援します。

お問い合わせ下さい。

informatica

IN18_0614_2658

出典

1. World's Biggest Data Breaches, Version 1.07, May 2014,
   http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

2. The Digital Universe of Opportunities、EMC Digital Universe、IDC、
   http://www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf

3. Data Security Statistics, Kroll Cyber Security, 2011,
   http://www.krollcybersecurity.com/resources/data-security-resources/data-security-statistics.aspx

4. The State of Data-Centric Security, Ponemon Institute, June 2014