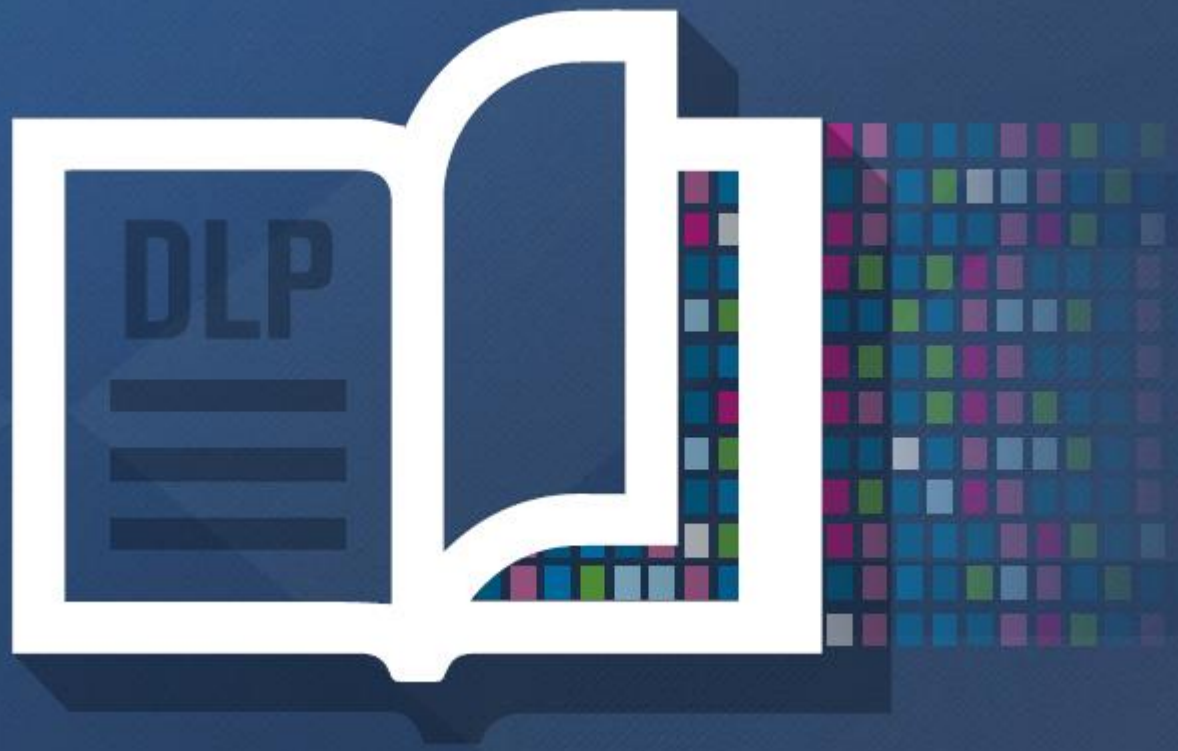
DLP (Data Loss Prevention) 徹底ガイド（見本）



DLP(Data Loss Prevention)徹底ガイドは、Digital Guardian社の「THE Definitive GUIDE TO DATA LOSS PREVENTION」の抄訳です。

DLPの定義

“DLPは、停止/稼動時において、データのリアルタイムスキャニングを実施し、既存のポリシー定義に反しているもの、ポリシーに違反しているものの特定、ならびに事前に定義した、被害抑制のためのアクション-例えば、ユーザや管理者に警告したり、疑わしいファイルに対する検疫、データの暗号化もしくは、外部へ送信されるトラフィックのブロックなどを自動的に行うシステムを指す。

-451 Research,”The Data Loss Prevention Market by the Numbers,” July 2015

DLPの基本

何？：一言でいうと、DLPは重要なデータの詐取や紛失を防ぐためのツールやプロセスなどの技術セットです。

どうやって？：DLPは組織の重要なデータを以下のように検知・保護します。

- 稼動中、利用時もしくは停止時のデータスキャン
- 保護が求められる重要なデータの特定
- 被害抑制のためのアクション-アラーム・検疫・ブロック・暗号化
- コンプライアンス・監査、調査・分析、インシデントへの対応などのためのレポートの提供

何故？：例えば従業員のミスや、悪意のある行為があなたのデータを危険にさらすため。

DLPの利用対象

顧客規模：米国フォーチューン・グローバル500内の大企業は、DLPにおよそ15年の投資を行っています。今日のDLPは中堅企業においても重要なセキュリティ戦略を提供しています。

産業：過去に、DLPは規制が多い産業である、金融サービス ヘルスケア、製造、エネルギー、そして政府組織などにおいて、用いられてきました。しかし、新たな活発的な侵入者は、これらの産業にとどまらずに、幅広い産業をそのターゲットにしています。

50%

の組織が

なんらかのDLPを利用しています。またガートナーの予想によると2018年には、90%に上るとしています。

（Gartner “Magic Quadrant for Enterprise Data Loss Prevention”, 1 February.2016, Brian Reed and Neil Wynne)

DLPが必要ですか？

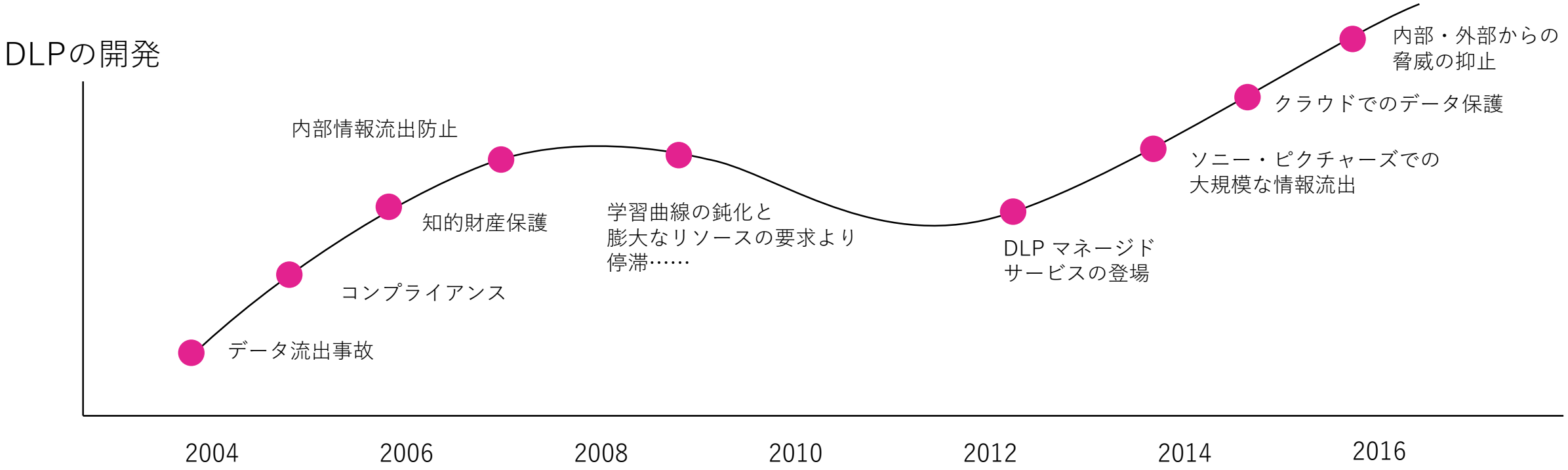
これらの一般的な項目が、あなたの組織に何かしら当てはまる場合は、DLPはお役に立つはずです。

DLPの項目チェックリスト

目的・対象	内容・状況	当てはまる場合はチェック
個人情報の保護やコンプライアンスの実践	個人を特定するような情報や、個人の医療記録や、支払い記録などの保護や秘匿性を政府や行政機関から求められているような場合。	☐
知的財産権の保護	組織が価値のある知的財産や、取引情報、秘匿情報などを持っており、悪意のある従業員が故意に情報を流出・破棄したり、偶然に無関係の従業員などに情報が共有された結果、重大な金銭的なブランドイメージの損失が発生するおそれがある場合。	☐
	組織の内部ネットワークへの侵入を図ろうとしたり、従業員など内部関係者と偽って、重要なデータを盗もうとする、競合他社や外国からの標的とされている場合。	☐
ビジネスパートナー間のコンプライアンス	組織が他社とパートナーシップを締結し、そのパートナーの知的財産を保護しなくてはならない場合。万が一その情報が流出・紛失した場合などに、多額の賠償をパートナーにしなければならない場合。	☐
	お客様が、組織と取引を進めるにあたり、組織内の情報保護のシステムが信頼に足りうるシステムを備えているかどうか、確認を求められているような場合。	☐

DLPはあらたなステージへ

DLPはユーザの多大な期待と興味をもってマーケットに登場してきました。ファースト世代のDLPはコストと導入の複雑さゆえに停滞しましたが、
度重なる大規模な情報流出事故や、DLP as Service(クラウドサービス）などの登場になり、DLPの機能はクラウド対応やATPの機能を実装し、
DLPは新たな発展のステージへと突き進んでいます。



DLPに関する３つの誤解

今日のDLPはより洗練され、自動化され、より多くの企業に受け入れられるものとなってきています。
DLPに対する“過剰な期待と幻滅の繰り返し”という時期を乗り越え、残るわずかな誤解を解消するに至りました。

誤解1:
DLPの管理と維持には多大なリソースがかかる？

過去のDLPは確かにそのとおりでした。
しかし最新のDLPは管理と維持に多大なリソースを費やす必要がなくなりました。自動化と、クラウド上のDLPサービス展開は、これまで大きな負荷とされていた、構築や設定、モニタリングや、チューニングなどの各種作業を軽減することを可能にしています。

誤解2:
DLPの“成果”を確認するのに18ヶ月もかかる。

DLPの導入成果を確認するのに、長い時間が必要といったことは過去のものになっています。
組織は導入の成果を、年単位や月単位ではなく、導入後数日で確認することができるようになっています。今日のDLPはモジュラー型となり、データ保護のプログラムを常にアップデートすることを可能にしています。

誤解3:
DLPは最初にポリシーを定義しないといけない。

今日のDLPは、必ずしも最初にポリシーを定義するといった必要はありません。コンテキスト認識型DLPは、データの使用率や動作といった情報をまず収集し、その結果を元に管理者が適切なポリシーを適用することを可能にしています。

クラウド利用により保護すべきデータは“いたるところ”に

クラウドの利用は、データの管理を非常に困難にしています。管理者の監視が及ばないところで、重要なデータが企業内LANからクラウドへと転送される……
組織のクラウド利用は、まさに大きな転換点を迎えています。

69%

の組織が

クラウドの導入が、セキュリティの管理と運用をより複雑化していると回答しています。

62%

の組織が、モバイルコンピューティングの導入が、セキュリティの管理と運用をより複雑化していると回答しています。

3割以上

の組織が、クラウドサービスを審査するにあたり、組織内のセキュリティエキスパートの関与がないという調査結果がでています。

80%

クラウドサービスの80%は事業部門のプロジェクト向け購入され、事業部門による直接管理またIT部門による管理を利点と見ています。

50%以下

クラウド上で実行するアプリケーションを定義している組織の割合。

わずか5割

クラウド上で利用するアプリケーションに関する契約と承認に関するガイドラインを制定している組織の割合

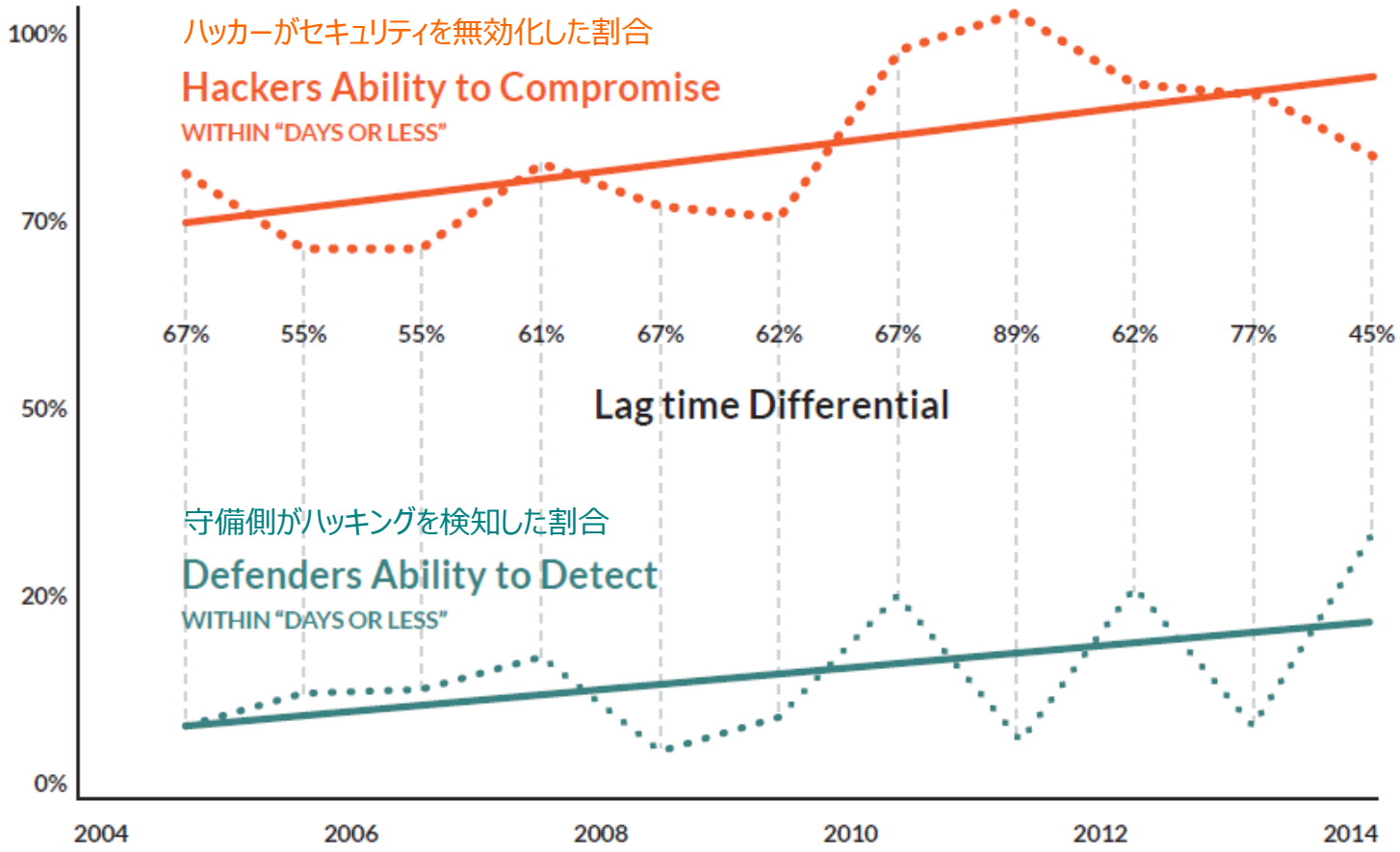
組織のデータは常に狙われています

攻撃と検知の間には大きなギャップが…

（このチャート）は攻撃者が数日以内で対象に何回侵入できたか（オレンジ線）を示し、守備者は、同じ時間枠で何回その攻撃を検知したか（青色線）を比較したものです。
残念なことに、数日内に攻撃を検知できたグラフは、侵入できたグラフに比べて非常に下回っていることがわかります。

さらに悪いことに、この2つの線は、この10年にわたり明確な差異があり、攻撃者と、守備者の間の「ギャップ」が広がっていることがわかります。これは、セキュリティ業界の一つの大きな問題を示しているものだと認識しています。

-Verizon 2015 Data Breach Investigations Report-



VERIZON 2015 DATA BREACH INVESTIGATHIONS REPORT

情報漏えいは”頻繁”にそして”大規模”に

まだデータ保護に懐疑的ですか？このページをご覧ください。

79,790
セキュリティ事故
“事故”とは、情報資産の秘匿性・整合性・可用性が、損なわれたイベントを指しています。

2,122
データ漏洩
第三者に対してデータの漏洩があったこと確認した事件の割合は増え続けています。

10億
のデータ損失

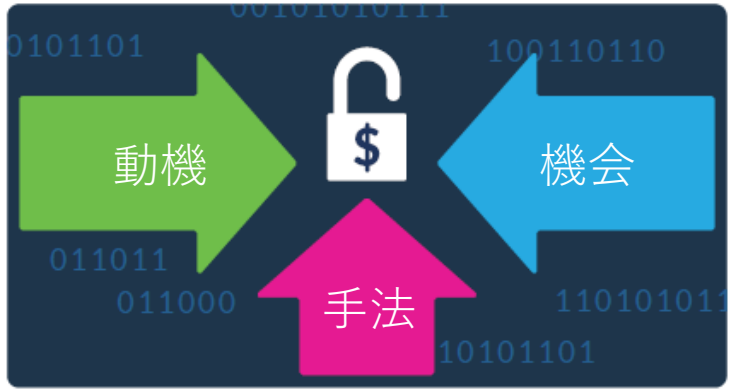
$154
盗まれた1レコードあたりの損失金額

+56%
“特許”などの知的財産が盗まれた割合（2014年比）

$3.79百万
わずか一度の情報漏えいで、回復にかかる平均コスト

sources: Verizon Data Breach Investigations (VBDIR) Report 2015; Ponemon Institute’s “2015 Annual Study: U.S. Cost of a Data Breach”; PWC “The Global State of Information Security® Survey 2016”)

データ窃取を分析する



手法： ツール、リソース、そしてスキルを攻撃者が手に入れた場合セキュリティアラートを回避する能力を取得したことになります。

動機： 国の支援：軍事情報や政策、経済情報の獲得のため
サイバー犯罪：金を稼ぐために必要なあらゆる手法を用います。
思想的な動機：犯罪者自身の思想目的を促進するため、など。

機会： タイミングとターゲットに関する情報は、攻撃者に対して侵入する確立を増加させます。攻撃者はあらゆる情報を利用して、彼らの目的を達成します。

具体的なデータ窃取事例

顧客データへのハッキングが、数週間のうちに、利益が約100億円消し去る。

英国の通信事業者“Talk Tlak”は、2014年の末、ハッキングの被害をうけ、150,000件の顧客データが流出。
被害額は日本円にして約100億近い損害に。

知的財産データ窃取が、企業競争力と、株主の利益を消し去る。

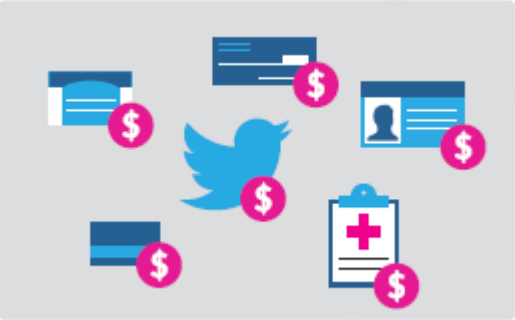
American Superconductors Corporation(AMSC)は中国の経済スパイ活動の標的にさらされました。AMSCは巨大なタービンをコントロールするシステムとプログラムを開発し、中国政府が背後で支援する、Sinovel Wind Groupとタービンを自社製造するためにパートナー契約を結びました。AMSCはそれが生みだす利益を、$50百万から$500百万とみていたものの、Sinovel Storeが知的財産をすべて窃取し独自にタービンを製造し始めたために、ASMCはその利益を失いました。ASMCはSinovelを相手に訴訟を起こし、係争中となっています。

プライバシーの漏洩が、多額の罰金の支払いと、組織の評判を失墜させることに。

The Feinstein Institute for Medical Research は患者13,000人の情報が入ったラップトップが盗まれたことにより、$3.9百万の罰金を支払うことに。

盗まれたデータの“価格”が上がっている事実

サイバー犯罪から利益を得るための地下マーケットには、盗まれたデータを売るための詳細な価格とパッケージモデルが用意されています。



このような「ダークウェブ」は違法行為と販売行為に用いられ、サイバー窃盗団に対して、データを販売するためのグローバルなマーケットを提供しています。

窃取されたデータは「ダークウェブ」で販売が可能となっており、あらゆるデータが、その価値によって価格が定義されています。
盗まれた情報がその価格に応じて販売されていることがわかります。

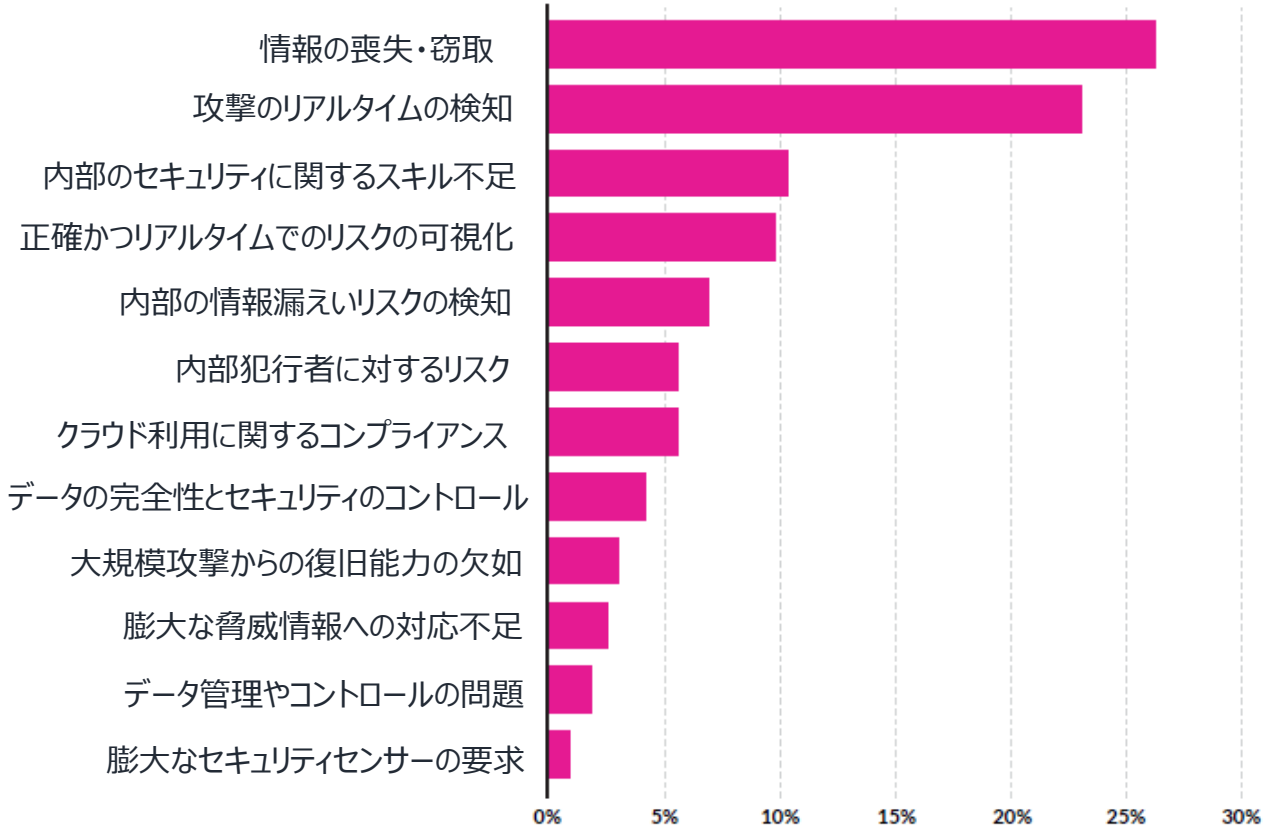
このような複雑な地下マーケットにて販売される大量のプライベートデータを見るにつけ、DLP導入の重要性がわかります。

偽造の運転免許証	$100-150
ソーシャルメディアのアカウント	$50
カードデータの基本情報（支払いアカウント番号、カード認証コード、有効期限）	$5-12 個人あたり（US） $25-30（EU）
上記に加え、請求先住所、個人認証番号（PIN）、社会保障番号（SSN）、生年月日（DOB）	$30(US) $45(EU)
銀行口座情報（ユーザー名とパスワード）＄2,000以上の預金がある場合	$190　口座あたり
銀行口座情報（ユーザー名とパスワード）＄6,000以上の預金がある場合	$500 口座あたり
銀行口座情報（ユーザー名とパスワード）＄20,000以上の預金がある場合	$1,200
患者の医療情報または生命保険のアカウント情報（含む、PIN,SSN,DOB）	$50 個人あたり
偽造され、かつ利用できる社会保障番号カード	$250-400
公共料金支払いに利用できる、完全な個人情報プロファイル	$350

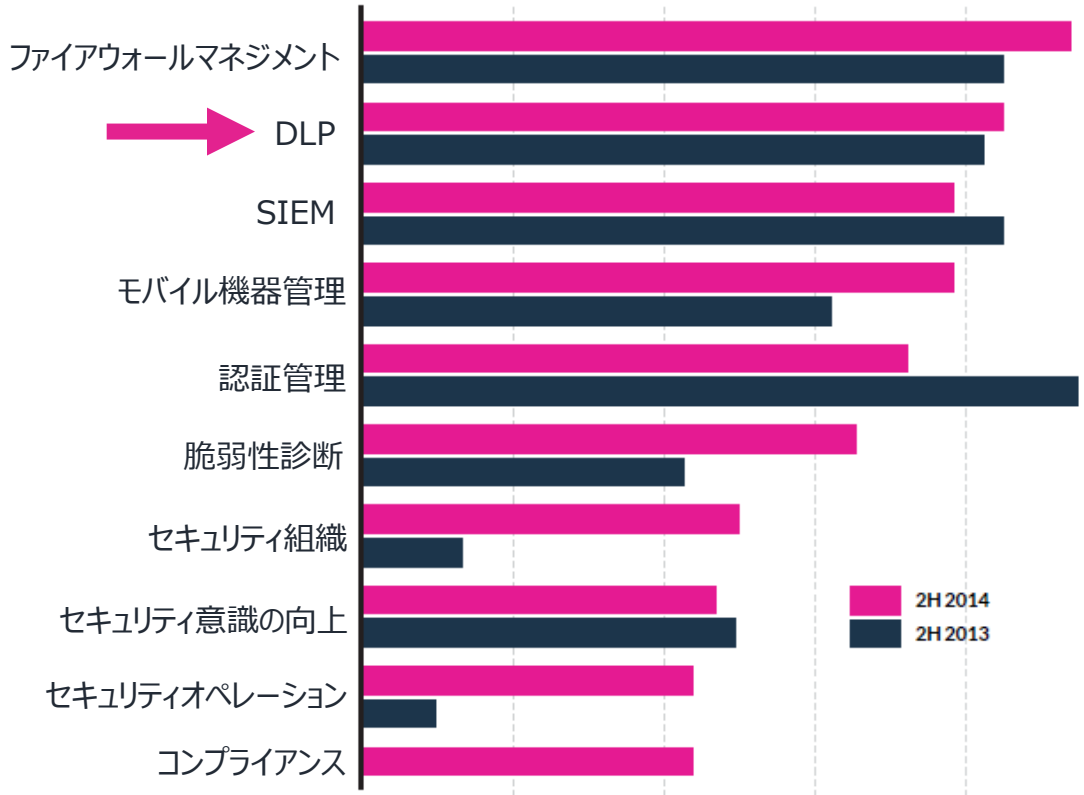
ランキングの中のDLP

“データの喪失や窃取への懸念”が次の12ヶ月でもっともトップに

【質問】次の12ヶ月で、情報セキュリティでもっとも懸念な事項は何ですか？

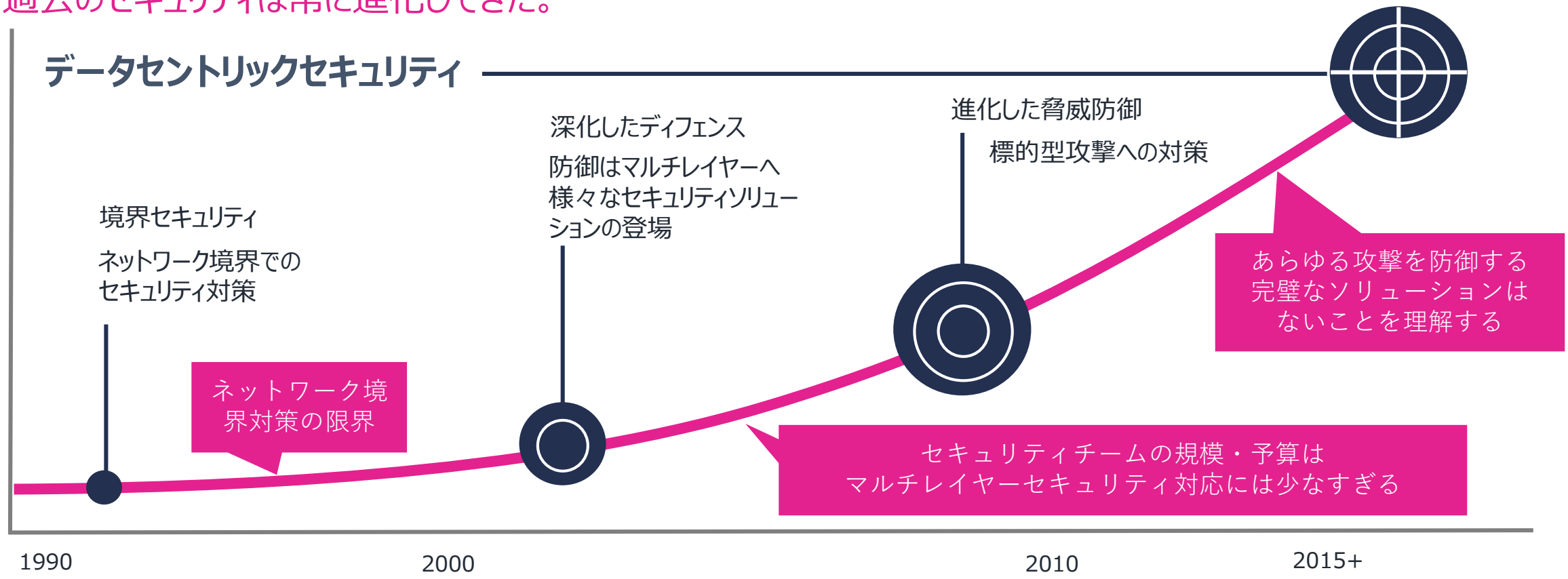


DLPが20のセキュリティプロジェクトのカテゴリーの中で2位に



すべてのトレンドは“データセントリック”へ

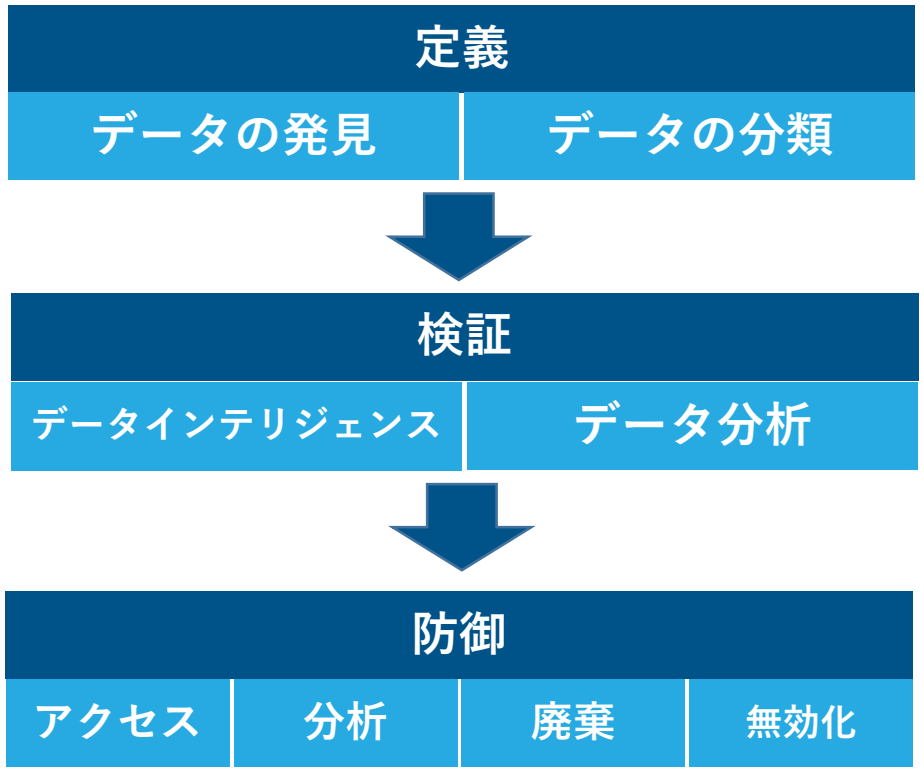
過去のセキュリティは常に進化してきた。



つまり、DLPはデータセントリックセキュリティの礎です。

“データセントリック”セキュリティフレームワーク

企業が“データセントリックセキュリティ”を行うには手助けが必要です。Forresterはそのためのフレームワークを作成しました。“データセキュリティ&フレームワーク”はデータのコントロールと安全性の確保の課題に対して、“定義”、“検証”、“防御”といった3つのステップに分解しています。これらのステップにより、企業は企業内のデータについて理解をすることができ、適切なリソースを配置することができ、重要なデータについて効果的に防御することを可能にします。



定義：データの発見と各種データの分類を行います。

検証：データインテリジェンス（そのデータからデータに関する情報を抽出し、その情報をデータを保護するために役立てること）。データ分析（プロアクティブにデータを保護するためのデータ分析を行うこと）

防御：データを守るためには、たった4つの手段しかありません。
アクセスのコントロール、データの利用パターンの分析と侵入に対する予防、
不要になったデータの廃棄。窃取されたデータを暗号化して、不正利用を防止することです。

(ソース: The Future Of Data Security And Privacy: Growth And Competitive Differentiation, Forrester Research, Inc., July 10, 2015)

ステップ1

守るべき主要なデータが”何“であるのか特定する

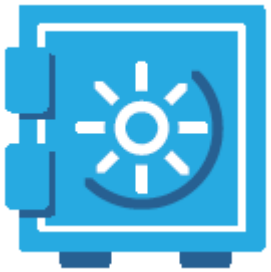
DLPプロジェクトを実行する前にもっとも重要な検討はあなたの組織が持つ主要なデータが「何」であるのかを、特定することです。
一般的に、組織がDLPを利用する場合には、次の３つのうちの1つであるといえます。

規制や法律を遵守

HIPAA PCI GLBA Gramm-Leach-Bliley Act

*改正個人情報保護法
*マイナンバー　など

知的財産を保護する



ビジネスパートナーとのコンプライアンス遵守

資料請求は……

この続きの↓

- DLPを行うための正しいアプローチを検討する。
- データ保護のための事業計画
- DLPを購入しよう！
- DLP導入を成功に導くために

に関する資料のお問い合わせは、

【お問い合わせフォーム】：

www.crosshead.co.jp/contact/digitalguardian/confirm_dg_guide.php

もしくは

【メールアドレス】：

secsales@crosshead.co.jp

まで、ご連絡ください。

DLP(Data Loss Prevention)徹底ガイドは、Digital Guardian社の「THE Definitive GUIDE TO DATA LOSS PREVENTION」の抄訳です。
オリジナル（英語）版は、https://digitalguardian.com/resources/whitepapersからダウンロードすることが可能です。