IDC
ANALYZE THE FUTURE

スポンサー:
Recorded Future

**著者**:
Harsh Singh
Martha
Vazquez

2018 年 8 月

# Recorded Future により組織のセキュリティ脅威への対応効率と投資効率が上昇

## ビジネス価値のハイライト

**284%**
3 年後の ROI

**32%**
IT セキュリティチームを効率化

**4 か月**
で投資回収

**10 倍**
驚異の特定を高速化

**22%**
多くのセキュリティ脅威を事前に特定

**86%**
計画外ダウンタイムを低減

**100 万ドル**
セキュリティ侵害毎の罰金/科料回避額

**63%**
驚異解決をスピード化

## エグゼクティブサマリー

黎明期の脅威情報セキュリティサービス(TISS)市場といえば、IT 環境の脆弱性や脅威に関する複数のデータフィードや情報源の収集でした。ところがここ 3〜5 年で TISS 市場は単なる複数の情報源からのデータフィードから IT 環境に流入するデータのコンテキスト情報も含むように発展しました。今日では、脅威情報(TI)サービスはデータを活用して TI アナリストに深い分析を提示しています。IDC では TISS を、単なるデータフィードのみならず脆弱性や脅威をめぐる追加コンテキスト情報を含み、反復情報(過去の経験や失敗を将来の計画立案に取り組むプロセス)を活用するものと定義しています。脅威情報はデータポイントを超える情報にとどまらず、組織に提示しているデータに関して意思決定に実用的な推奨も提供する必要があります。脅威情報では履歴に基づいて傾向を特定し、天気予報のようにストーリー性を以て組織のセキュリティ方針に関する戦略的判断に容易に役立てられるようなものでなければなりません。

Recorded Future は TISS 市場のベンダとして、機械学習と人手による分析を組み合わせてリアルタイムで関連性のあるデータを作成するオールインワンの普遍的 TI ソリューションを提供します。その技術は機械学習と自動化を基盤としており、ここ数年で同社は専門家をチームに加え、コンテキストの詳細情報も提供しています。Recorded Future の技術は、セキュリティアラートやインシデントのコンテキストに関する膨大なデータを人の手で調べ、組織のセキュリティリスクを判断しようとすればさらに調査が必要になるのに対して、時間を節減し効率を上げるべく構築されました。

IDC は、Recorded Future を IT セキュリティの脅威情報に活用している数々の組織を取材しました。取材の結果明らかになったのは、Recorded Future のソリューションを IT セキュリティ組織全体で活用することにより、相当な便益を実現しているということでした。



IDC
ANALYZE THE FUTURE

IDC の算出では、下記によりこれら組織が実現している便益は、1 組織当たり年間 80 万 6000 米ドル相当（組織内 IT セキュリティチーム人員 1 人当たり 3 万 9368 米ドル）でした。

- IT セキュリティチーム全体（運用、調査、レポート編集、脅威解決担当要員を含む）の生産性向上を推進
- 組織への影響が拡大する前に脅威を積極的に叩く時間をセキュリティチームに提供
- セキュリティ侵害毎に損害となる違反や科料の回避を支援

# 現況概要

今日のサイバー脅威を見渡せば、敵は一層狡猾になり組織に申告な課題をもたらしています。セキュリティチームは APT（高度で持続的な脅威）やゼロデイ攻撃の先手を打とうと努力しても、目立たないように侵入速度を低下しながら標的に複数のテクニックやツールを駆使する未知の攻撃者に先回りされ続けています。代表的なファイヤウォールやシグネチャベースのマルウェア対策ソリューションも効果はあるものの、今日の悪意ある脅威に後れを取らないようにするのに必ずしも適しているわけではありません。依然としてシグネチャベースの手法を頼みの綱とする企業もあるものの、多くがセキュリティ業務に脅威情報サービスを取り込み、分析と予測によってリスクや潜在的な業務の混乱を緩和に役立てようとしています。

データフィードをネットワークに統合するセキュリティツールをインストールしても、組織の多くは流入する情報をどうすべきか認識していません。脅威情報の意味や組織にもたらす便益を理解していない場合が多いのです。IT 環境に流入するデータ量は膨大なため、組織は却って効果的な判断をするにはどうすればよいかと当惑し、混乱しています。データフィードを申し込んだはよいものの、どの脅威が最も重要性が高いのかを詳細に分析して調査し、判別しても深刻に受け止めるべき脅威なのか、組織としてどう進めばよいかを実際に分析して判断する要員がいない場合もあります。

TISS 市場は比較的新しいものの、過去数年で順調に伸びてきました。2017 年には 13 億米ドル規模に達しました。2016 年から 2021 年には 11.2%の CAGR（複合年間成長率）が見込まれます。TISS 市場は、組織が投資、データや知的財産の保護に努めるにつれ拡張を続けます。組織全体への脅威プロファイルに先手を打つのは、新たな脅威に門戸を開く IoT（モノのインターネット）、SDN（Software defined networks）やクラウドコンピューティングの進歩によりますます難しく、複雑になりつつあります。その結果として、組織はセキュリティ分析から具体的で実用的なデータを構築し、敵との戦いに役立てるように TISS ベンダと提携する機会を利用しているのです。

# RECORDED FUTURE

Recorded Future は、ベンダとして世界中の組織に普遍的な脅威情報ソリューションを提供しています。これまで触れたテーマの1つで、意思決定に実用的なコンテンツを提供するデータで脅威情報を構成する必要性を論じました。今日の組織は膨大なデータを収集し、そのデータの意味や、真の脅威がどこにあるかを理解するのに奮闘しています。セキュリティインシデントを読み解くには時間と専門技術を要します。そこに Recorded Future が役立ちます。Recorded Future は、継続フィード、オープンソースやダークウェブ情報、アナリストレポートを組み合わせて統合した情報を提供し、単一プラットフォームにデータを集約します。Recorded Future の脅威情報は機械学習と人間の専門知識を組み合わせてリアルタイムで現実の問題に直結したデータを作成します。さらに、ここ数年の間に同社ではチームに専門家を投入してコンテンツの詳細分析を提供するようになりました。Recorded Future の技術は、SIEM（セキュリティ情報イベント管理）システムや脆弱性スキャナ等の機器から流入するセキュリティインシデントの可能性を人手で調べ、その後時間をかけて最も深刻な脆弱性やセキュリティインシデントを判断する時間を節減し、効率を上げるために構築されました。現実の脅威を示すイベントを読み解くのに加え、IT セキュリティチームは環境に流入する大量のアラートも優先順位付けしなければなりません。Recorded Future の TI 製品を利用すれば、どの脅威が最重要であるかを評価して即座に緩和したりパッチを当てたりすることができます。

セキュリティチームが何十万もの外部ソースから提供される大量の脅威データや脆弱性データを調査するのは、言語を解読し、クロス相関させ、徹底調査をして脅威データが何を意味するのか、どの脅威データが組織に関連があるのかを判断しなければならないため困難を極めます。Recorded Future のソリューションは機械学習と自動化を活用することで、技術ソース、技術研究、オープンソース、クローズド/ダークソースからデータを取り込むことができます。Recorded Future の最新プラットフォームである Fusion は、さらにサードパーティのフィードや内部の脅威データをはじめとする顧客ソースも取り込むことができます。Recorded Future のソリューションは、このような大量のリソースを取り込んでデータを一か所に集約して分析します。この普遍的な TI ソリューションの中で、自然言語処理によりあらゆる言語を処理し、リアルタイムで脅威アクターや標的、マルウェア等に関連する言葉を迅速に特定することができます。本ソリューションはオントロジーを用いて階層的関係を表し、データを整理します。例えば、ある組織がフランスで脅威を調査していればシステムは自動的にフランス国内のすべての市町村に関連する脅威を含めます。

Recorded Future は点と点をつないで脅威アクター、TTP（戦術、テクニック、手順）、IOC（侵害の兆候）に関連する情報を顧客に提示します。例えば、顧客が特定の IP アドレスの詳細を知りたい場合には、編集済みのレポート（インテリジェンスカード）をリアルタイム情報と共にオンデマンドで

引き出すことができるため、貴重なコンテキスト情報を提供します。インテリジェンスカードは、最上位の攻撃ベクター、企業内に存在するかもしれない感染した技術、関連する IOC を一覧化して提供します。さらに顧客は具体的要件や関心領域にカスタマイズしたオンデマンドレポートや週次レポートを要求して、セキュリティリスクやその他のセキュリティ脅威分析を判断することもできます。

Recorded Future の TI サービスのもう一つの重要な特徴は、セキュリティ環境内でも統合が可能なことです。前にも触れたように SIEM システムと脆弱性スキャナを統合することはできますが、他の多くのセキュリティ機器も脅威情報の消費を目的に統合することができます。さらに、複数のソリューションを統合してセキュリティ運用、インシデント対応、脆弱性管理や経営陣等様々なIT セキュリティ担当者をサポートすることも可能です。セキュリティ運用チームでは、Recorded Future はトリアージュの迅速化、手作業による調査時間の低減、未知の脅威の発見を助け、アラートのリスクレベルの判断やイベントの優先順位付けに役立ちます。インシデント対応チームでは、ソリューションはインシデントに関するリアルタイムの豊富なコンテキスト情報を提供するため手作業による調査の必要性や誤検出の特定に無駄に費やしていた時間を最小化し、応答時間を短縮するのに役立ちます。脆弱性管理チームは、流入する大量の脆弱性情報の優先順位や優先的にパッチを当てるべき脆弱性を判断することができるようになります。さらに優先順位付けをスピード化するには、インテリジェンスカードにリスクスコアが提供されるため、特定イベントに関連するリスクレベルの迅速な把握に役立ちます。それほど詳細な情報を要しない経営陣もハイレベルレポートやダッシュボードを見れば、セキュリティリスクの全容の把握に十分な情報が表示されます。

取材に回答した Recorded Future の顧客は Recorded Future の TI サービスや、この TI サービスが効率化や作業効率の拡大にいかに役立ったかを熱心に語っていました。顧客はソリューションが持つリアルタイム分析提供能力へのコメントとして、IT環境に流入するセキュリティインシデントについて良い判断ができるようになったため作業効率が上がったと語っていました。また、コスト効果や効率、統合のしやすさ、可視性の広がり、最新のセキュリティインシデントに関する実用的な情報についても触れていました。

# RECORDED FUTURE のビジネス価値

## 調査対象の構成

IDC は、本調査で 6 組織を対象に取材し、参加者に Recorded Future のソリューション導入による IT 業務やセキュリティ業務、ビジネス、コストへの影響について様々な定量的、定性的質問を行いました。表 1 はこれら組織の企業特性を示しています。

調査対象の企業規模には巨大企業から中小規模の組織まで多様性を持たせました。この結果、平均従業員基盤は 5 万 1725 人となっています。すべての企業で IT の存在感は顕著であり、IT 人員平均 4072 人が社内ユーザ平均合計 4 万 3292 人をサポーとしていました。調査対象企業はすべて米国を拠点としていました。さらに業界セグメントも金融サービス、車載機器、製造、情報技術と幅広く取り混ぜています。

表 1 取材対象組織の構成

| | 平均 | 中央値 |
|---|---|---|
| 従業員数 | 51,725 | 17,500 |
| IT要員人数 | 4,072 | 880 |
| ITサービスユーザ数 | 43,292 | 17,500 |
| 業務用アプリケーション数 | 742 | 475 |
| 接続機器数 | 64,100 | 36,250 |
| 年間収益 | 62 億米ドル | 19 億米ドル |
| 国 | 米国 (6) | |
| 業界 | 金融サービス (3)、車載機器、製造、情報技術 | |

*n=6 出典: IDC, 2018*

## Recorded Future の活用

今日のビジネス環境では一流のセキュリティ機能が IT 業務にもビジネス事業運営にも不可欠です。IT 部門やセキュリティチームは、脅威データの収集と分析を自動化して先行的なセキュリティをリアルタイムで提供する分析主導のソリューションを必要としています。

IDC が取材した企業は、組織の IT インフラやデータへの脅威や攻撃数の増加に対処するためにこのような機能の導入が必要だと強調していました。取材に応じた組織は IDC に Recorded Future のソリューションは優れたリアルタイム通知とインサイトを提供し、セキュリティ問題を監視し、対処する役に立ったと述べていました。調査参加者が代替手段に比べて Recorded Future を選択した多数の理由の一部を紹介します。

- **コスト効率の高いセキュリティ強化:**「Recorded Future はセキュリティエンジニア正規職員 2 人分より割安で、当社組織全体で既存のセキュリティ作業すべての関連情報分析とレポートへのアクセスを増やし、改善します」
- **ベンダインサイトの改善:**「Recorded Future はベンダと取引する際のリスクなどインサイトを提供します。当社の購買部がベンダを評価する際に、これまで財務報告書は使っていましたがサイバーチェックをすることは考えてもいませんでした。一度やってみたところ、『いったいどういう会社なんだ』というリアクションがありました」
- **セキュリティプロセスの自動化推進:**「戦略目標の 1 つにセキュリティ検出と対応への自動化機能の実装推進があります。Recorded Future はこれにぴったりはまり、当社のネットワークベースのファイヤウォールやエンドポイントセキュリティを補完します」

調査対象企業の利用パターンの全体像を描くために、IDC は調査参加者が Recorded Future のプラットフォームをどのように導入しているか、また、IT 環境やネットワーク環境の詳細についても情報を収集しました。例えば、表 2 に示すように全企業の業務用アプリケーションの平均数は 322 で、社内ユーザ数は 3 万 1617 人と多数でした。表 2 は Recorded Future のソリューションの活用に関しても追加メトリックスを提供しています。

## 表 2 組織の Recorded Future 使用環境

| | 平均 | 中央値 |
|---|---|---|
| 支店/拠点数 | 238 | 200 |
| 社内ユーザ数 | 31,617 | 10,800 |
| 業務用アプリケーション数 | 322 | 155 |
| サポート対象収益 | 88% | 100% |

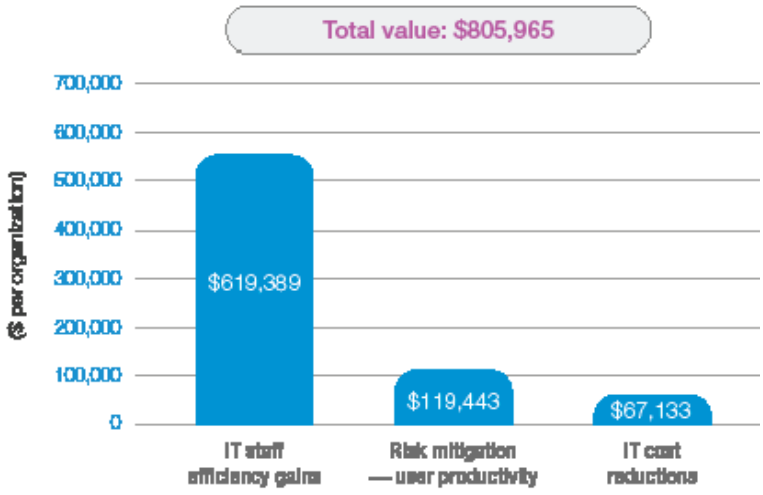
*n=6 出典: IDC, 2018*

# Recorded Future のビジネス価値

参加組織は、Recorded Future から受信する情報が現実の問題に直結していてタイムリーな理由として、主に、機械学習/人工知能により脅威関連情報の生成が自動化されていることと、可視性と適時性により脅威の意識が改善されていることの 2 つを挙げていました。潜在的な脅威の調査や修正に膨大な時間を割かずに、組織はセキュリティの脅威や懸念に先行的なアプローチを取れるようになります。IDC は、顧客や参加企業は 1 組織当たり年間平均 80 万 6000 米ドル相当の便益を以下の領域で達成できると算出しています（図1参照）。

- **IT 要員の生産性における利点:** IT セキュリティチームは時間のかかる調査やレポート編纂から解放され、重要なセキュリティ業務にかかれるようになります。一方で、セキュリティ解決チームは脅威の侵入予測に多くの時間をかけられるようになるため、先手を打てるようになります。IDC ではこれら組織が 1 組織当たり 61 万 9389 米ドル相当（社内 IT セキュリティチーム要員毎に 3 万 462 米ドル相当）の生産性利益を実現していると算出しました。
- **リスク緩和 — ユーザ生産性の便益:** 組織は、業務に影響を及ぼすセキュリティ侵害による計画外のダウンタイムが減ったと報告していました。これによる生産性利得を IDC では 1 組織当たり 19 万 9443 米ドル（社内 IT セキュリティチーム要員毎に 5874 米ドル）とはじき出しています。
- **IT コストの削減:** 取材に答えた組織は IDC に外部レポートやコンサルティング費用が節減できたと申告していることから、IDC はこれが 1 組織当たり 6 万 7133 米ドル相当（社内 IT セキュリティチーム要員毎に 3302 米ドル相当）と推定しています。

## 図 1 組織当たりの平均年間便益




*出典: IDC, 2018*

## *IT セキュリティ業務の効率化*

調査参加者は、Recorded Future ソリューションの導入によってセキュリティチームが効率化されたと語っていました。これには、脅威情報の編集と脅威調査手順の 2 つの重点領域での改善が含まれます。その結果、セキュリティチームはソリューションを活用して先行的に問題に取り組めるようになっています。

Recorded Future のソリューションは、人手に比べて脅威情報に機械学習の規模と速度を活用できるように構築されています。Recorded Future は、脅威情報を IT 組織が導入する他のソリューションにも統合できるように API を提供しているため、組織は時間の節減を達成することができます。

調査参加者は、効率化を推進した特性を次のように説明していました。

- **既存のセキュリティソリューションの改善:**「Recorded Future はデータのエンリッチメントを行います。私が都合する情報で Recorded Future を使うとはるかに多くの情報が得られます。例えば、ドメイン監視にドメインツールを使っていますが、これを Recorded Future に接続すると特定の IP アドレスが不審な活動に関わっていたという情報も得られます」
- **正確なレポート:**「Recorded Future のオンデマンドレポート…は精確で、驚くほど詳細にわたっています。そのうえ納期も早いです。レポートのデータは非常に実用的で貴重です」
- **実際性があり実用的な情報:**「当社製品に関する最新情報を定期的に受け取っていますが、『今日のニュース』のようなハイレベルのレポートもいいですね。Recorded Future により有益な情報がきちんと増えてきました。経営幹部にとっては朝、会議前にレポートがあると助かります。Recorded Future は読み込める貴重な情報を出してくれます」

これらの引用からも Recorded Future がセキュリティチームの様々なレベルに影響を及ぼしていることがわかります。表 3 は、セキュリティ脅威情報編纂作業の生産性に Recorded Future がもたらした影響について具体的な改善測定値を示しています。セキュリティチーム要員の工数が 34% 改善したことは特筆に値します。

表 3 セキュリティレポート編纂作業の生産性に及ぼした影響

| | Recorded Future 導入前 | Recorded Future 導入後 | 差分 | 利益 (%) |
|---|---|---|---|---|
| 脅威情報編纂要員に及ぼした影響（正規職員数換算） | 6.1 | 4.1 | 2.0 | 34 |
| セキュリティチーム要員の年間工数（時間数） | 564 | 375 | 189 | 34 |
| レポート編纂の工数費 | $610,200 | $405,400 | $204,800 | 34 |

*出典: IDC, 2018*

取材に応じた組織は IDC に対して、Recorded Future ソリューションにより自動的に編纂されるようになったため脅威情報チームが脅威を手作業で検索する必要がなくなったと述べました。この便益は大きく、脅威調査の所要時間を激減します。

これについてある調査参加者が次のように言及しました。「Recorded Future のお陰で潜在的脅威に関してはるかに意味のあるデータを生成できるようになり、あらゆることを明確に把握できるようになりました。以前は特定のイベントを手作業で検索しなければなりませんでしたが、Recorded Future はもっと多くの情報源からデータを引き込めます。これがなければ Google やソーシャルメディアなどから潜在的活動を選り分けなければならないところでした」
問題特定の迅速化については別の参加者も次のように語っています。「Recorded Future はインシデント対応に関してはセキュリティに特化しています。インシデントの発見も速くなり、当社ネットワークにはなく出回っているインシデントにも対応して修正できるようになりました」

表 4 は脅威調査プロセスの生産性に及ぼした影響の改善測定基準を示しています。例えばこうした作業の全体工数が平均して 13%改善しました。

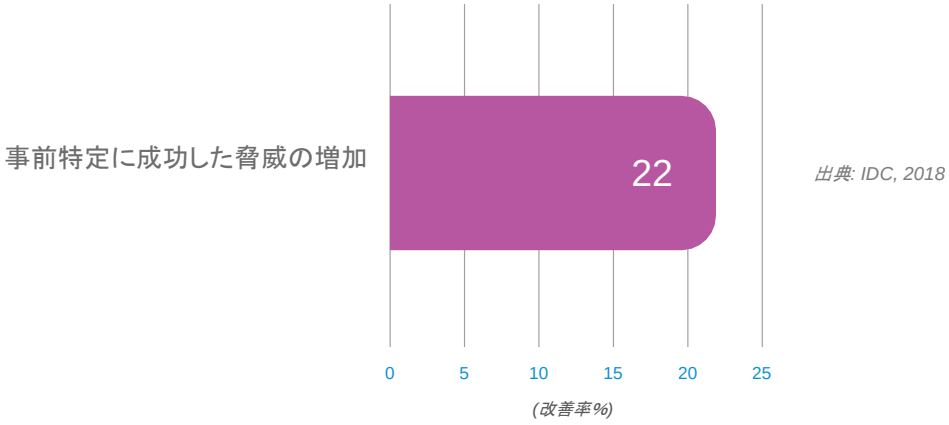
## 表 4 脅威調査要員の生産性に及ぼした影響

| | Recorded Future 導入前 | Recorded Future 導入後 | 差分 | 利益(%) |
|---|---|---|---|---|
| 脅威調査要員に及ぼした影響（正規職員数換算） | 18.2 | 15.7 | 2.4 | 13 |
| セキュリティチーム要員の年間工数（時間数） | 1681 | 1455 | 226 | 13 |
| レポート編纂の工数費 | $1,818,600 | $1,574,000 | $244,600 | 13 |

*出典: IDC, 2018*

調査対象組織の全体的なセキュリティ課題にはもう一つ、組織に影響が及ぶ前に多くの脅威を突き止めたいというものでした。ある組織は次のように言及しました。「Recorded Future は当社リスクプロファイルの評価に役立ちます。会社が大きくなって新たな技術を買収し、新たな領域に拡がったことから、当社が新参者である分野では既存ビジネスにはあったようなセキュリティインフラを持ち合わせていない場合がありますが、Recorded Future により脅威の監視ができています」
図 2 に示すように、このような組織では、脅威が及ぶ前に検出できる脅威が 22%増えています。

## 図 2 脅威の解決




出典: IDC, 2018

表 5 は、Recorded Future のサービスを導入し使用した結果、チームの生産性にどのような影響を及ぼしたかを示しています。これらの組織では潜在的に影響力の強い脅威の特定にかかった日数が Recorded Future 導入前の 0.4 日前から Recorded Future 導入後には約 4.1 日前と、10 倍速く突き止められるようになりました。ここで時間を節減できたことで、セキュリティ解決チームも平均して脅威を 63%速く解決できます。こうした時間の節約の結果—脅威がタイムリーに可視化できるようになったことで—セキュリティ解決チームの生産性は平均して 78%改善しました。

## 表 5 セキュリティ解決要員の生産性に及ぼした影響

| | Recorded Future 導入前 | Recorded Future 導入後 | 差分 | 利益(%) |
|---|---|---|---|---|
| 影響力が強くなる前に脅威特定にかかった時間(日数) | 0.4 | 4.1 | 3.7 | 1,000 |
| 問題解決の所要時間(時間数) | 15.6 | 5.7 | 9.9 | 63 |
| 脅威調査要員に及ぼした影響(正規職員数換算) | 2.4 | 0.5 | 1.9 | 78 |
| セキュリティチーム要員の年間工数(時間数) | 223 | 50 | 173 | 78 |
| セキュリティ解決の工数費 | $241,100 | $54,000 | $187,400 | 78 |

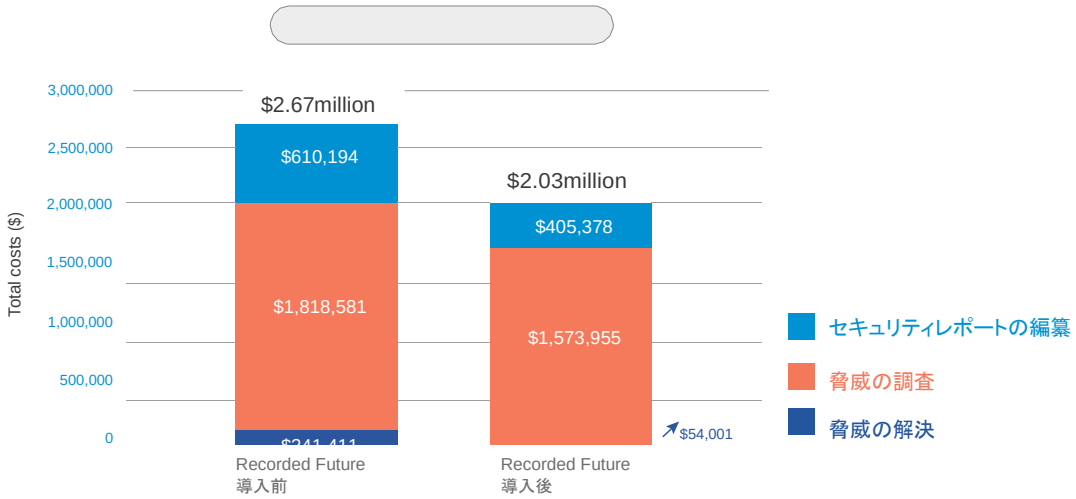
Source: IDC, 2018

生産性の向上は総運用コストにからむ便益に結び付きます。図 3 に示すようにセキュリティチームのコストへの影響はこれまで論じてきた 3 つの重要領域に関連付けられます。

- セキュリティレポートの編纂
- 脅威の調査
- 脅威の解決

図 3 に示すように、IT セキュリティチームのコストは Recorded Future 導入後 32%低減しました。

## 図 3 IT セキュリティチームの総時間コストへの影響




*出典: IDC, 2018*

### *リスク緩和への影響*

今日のビジネス環境では計画外のダウンタイムは事業部門の生産性に致命的です。調査参加者は IDC に、Recorded Future のソリューションにより計画外のダウンタイムのインスタンスがいかに減ったかを語りました。

セキュリティチームは重大な問題に発展する前に脅威をうまく処理できるようになったため、計画外のダウンタイムを阻止できています。これは、セキュリティ関連の計画外のダウンタイムの影響を受けるユーザ数とユーザ当たりのインシデント経験数を減った結果です。

表 6 に示すように組織はセキュリティ脅威関連の計画外のシャットダウンによって失われたエンドユーザの生産性を 86%取り戻すことができました。

## 表 6 計画外のダウンタイムが及ぼした影響

| | Recorded Future 導入前 | Recorded Future 導入後 | 差分 | 利益（%） |
|---|---|---|---|---|
| 計画外シャットダウンによる生産性喪失の影響の正規職員数換算 | 2.1 | 0.3 | 1.8 | 86 |
| セキュリティチーム要員 1 人当たりの年間時間数 | 193 | 27 | 166 | 86 |
| 年間の生産性損失価値 | $145,800 | $20,300 | $125,600 | 86 |

*出典: IDC, 2018*

情報筋によると、2018 年に米国企業がデータ漏洩毎に支払った額は世界の他国企業よりもはるかに多かったとのことです。現実に侵害が起こると金銭がリスクにさらされたり、大いに喧伝されるデータ窃盗のリスク、また実体は伴わなくとも評判や顧客の喪失という厄介な問題を伴う場合もあります。

リスクの緩和はこうしたコストの削減手段です。実際のまたは潜在的なセキュリティ脅威の処理の信頼性が増したことにより、調査対象組織の全体リスクが低減しました。この利点について、ある調査参加者は「Recorded Future によって可視性が改善されました。インシデント数に変化はありませんがリスクレベルは変わりました」とコメントしました。

表 7 に示すように、Recorded Future のソリューションを導入して使用するようになった後のリスク緩和影響は多大で、顧客は 1 回の侵害当たり平均 103 万 3300 ドルの潜在的損失を回避できています。

## 表 7 リスク緩和に及ぼした影響

| | 1 組織当たり |
|---|---|
| 侵害 1 回当たりの潜在的損失 | $1,033,300 |
| 科料/罰金の減額 | 2% |

*Source: IDC, 2018*

# ROI 分析

表 8 は、参加組織による Recorded Future の利用に関する便益とコストの IDC による分析結果を示しています。IDC は 3 年間でこれらの組織は Recorded Future のソリューションに割引現在価値にして平均 50 万米ドル（セキュリティチーム要員 1 人当たり 2 万 4656 米ドル）を投資すると推定しています。その見返りとして、IDC ではこれらの顧客は割引現在価値にして 1 組織当たり 192 万米ドル（セキュリティチーム要員 1 人あたり 9 万 4639 米ドル）の便益を実現すると予想しています。これにより ROI は 284%となり、4 か月で投資の元が取れることになります。

表 8 ROI 分析

| | 1 組織当たり | セキュリティチーム要員 1 人当たり |
|---|---|---|
| 便益（割引現在価値） | $1.92 million | $94,639 |
| 投資（割引現在価値） | $0.50 million | $24,656 |
| 正味現在価値（NPV） | $1.42 million | $69,983 |
| 投資利益率（ROI） | 284% | 284% |
| 回収機関 | 4 か月 | 4 か月 |
| Discount rate | 12% | 12% |

*出典: IDC, 2018*

# 課題と機会

脅威情報の活用に当たっての課題の 1 つは、それがどういうものであるか、どのように使うかを学習することです。大抵の場合、エンドユーザは脅威情報データの受信を望みますがそのデータから貴重なインサイトを構築する方法がわかっていません。複数のソースから生のデータフィードを受信しても利用価値のあるデータにはなりません。エンドユーザはそのデータが会社にどういう意味があるか、何か心配するべきものであるかを知る必要があります。脅威フィードやその他の脅威データの重要性は、セキュリティ侵害の兆候の収集にとどまらず、企業がセキュリティ方針や組織内で検出されたイベントに関して決断をするのに役立つような実用的なコンテンツにもあるのです。

TISS 市場では多くのベンダがフィードのみを提供していますが、フィードには履歴情報や脅威の傾向、評価された初期の兆候をめぐるコンテキスト情報といった肝心な情報が入っていません。今日の組織は依然として受信した情報をどうするか、手持ちの情報でどのように決断するかで奮闘している段階です。

Recorded Future はこうした課題を事業機会に変えて TISS 市場に算入したプロバイダです。そのソリューションには何十もの脅威フィードにサーフェス、ディープ、ダークウェブデータに加え専門家による分析が集約され、関連する脅威情報をリアルタイムで提供します。新たなプラットフォームである Fusion は他のサードパーティのフィードや顧客の固有データも統合するため、ソリューション自体が企業のワンストップショップになります。豊富な外部の脅威情報と内部データを組み合わせて企業が情報に基づいたセキュリティ判断をできるようにする役に立っていることから、TSS 市場に大変革をもたらしました。

# 要約と結論

概して今日の組織は大量のデータを収集しそのデータが何を意味するか、真の脅威であるかを理解することに奮闘している段階です。セキュリティインシデントを読み解くには時間と専門知識を要します。そこに Recorded Future が役に立ちます。取材の過程で収集した顧客データに基づけば、Recorded Future の脅威情報の顧客では IT セキュリティチーム全体で要員の生産性と効率化を期待できます。ソリューションは、発生しているセキュリティ脅威に対して IT チームの視野を広げ、最新の脅威について戦略的決断を下す支援をします。Recorded Future は組織に普遍的な脅威情報プラットフォームを提供できることから、データを収集し、リアルタイムで分析し、顧客に実用的な判断に必要となるリアルな情報を提供して他のベンダのサービスと差別化しています。この結果、この調査に参加した組織は 3 年間で 284%という目覚ましい投資利益率を達成したのです。

# APPENDIX

## 分析手法

IDC 標準の ROI 分析手法を本プロジェクトに活用しました。この手法では、モデルの基盤として Recorded Future の現行ユーザから収集したデータを基盤にしています。Recorded Future を活用している組織の取材に基づき、IDC は 3 段階のプロセスで ROI と回収期間を算出しました。

1. **Recorded Future の効果に関する事前事後評価を用いて取材で定量的な便益情報を収集。** この調査で、便益には要員の工数節減、生産性便益や運用費の削減が含まれていました。

2. **取材に基づいて完全な投資(3 年総コスト分析)プロファイルを作成。** 投資には Recorded Future の利用に関する初期費用と年間費用に加え、移行、計画、コンサルティング、要員やユーザトレーニングに関する追加コストも含むことができます。

3. **ROI と回収機関を算出。**IDC では、組織による Recorded Future 使用レポートに関して 3 か年にわたって便益と投資のキャッシュフローに減価償却を適用した分析を実績しました。ROI は、投資額の正味現在価値（NPV）と割引現在価値の割合です。回収期間は、累積利益が初期投資と等しくなるポイントで割り出しています。

IDC は、回収機関と ROI の算出をいくつかの想定に基づいておこなっています。それを下にまとめます。

- 時間的価値に給与負担額（給与＋（給付金と諸経費の 28%）を乗算して効率と生産性向上による節減を定量化します。この分析の目的においては IDC は取材した組織の地理的位置情報に基づいて IT 要員の平均年間俸給として平均 10 万米ドル、IT 以外の要員の平均年間俸給として平均 7 万米ドルの想定を用いました。IDC では従業員は年間に 1880 時間（40 時間×47 週）勤務すると想定しています。
- 3 年間にわたる節減の正味現在価値では、取り逃した機会費用を考慮し、12%の利益を生む投資商品に元金を投資していれば実現していただろう金額を差し引いて算出しています。これは想定資金コストと想定利益率双方を考慮に入れています。
- さらに IT ソリューションには開発期間が伴うため、ソリューションの完全な便益は開発期間中には提供されません。この現実を取り込むために、IDC では便益を月割計算したうえで初年節減額から導入期間を差し引いています。

*注記: 本文書内のすべての数字は丸めてあるため正確ではない可能性があります。*

IDC Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com



## IDC について

International Data Corporation（(IDC）は IT、通信、消費者向け技術市場の市場情報やアドバイザリーサービス、イベントの世界一のプロバイダです。IDC は IT の専門家、事業経営者や投資業界が技術の購入や事業戦略に関して事実に基づいた意思決定をできるように支援しています。IDC の 1100 人以上のアナリストが世界 110 か国の技術や産業分野の市場機会に関してグローバル、地域別、国別の専門知識を提供しています。50 年にわたり、IDC はお客様が主な事業目標を達成できるように支援してまいりました。IDC は世界第 1 位の技術メディア、研究、イベント会社 IDG の子会社です。