Dell SecureWorks

SecureWorks

包括的な IT セキュリティ サービス Dell SecureWorks とは

Dell SecureWorksは、サイバー スレット インテリジェンスを活用し、世界中の何千ものお客様の脅威を予見し、継続的に保護しています。

Counter Threat Unit™（CTU）リサーチ チームのインテリジェンスにより強化されたDell SecureWorksの IT セキュリティ サービスは、脅威を予見し、プロアクティブな防御を実現する御支援を致します。

また、サイバー攻撃を継続的に検知して阻止し、万が一のセキュリティ侵害発生時には、より迅速なリカバリをサポート致します。

「Dell SecureWorksのサービスを利用したことで、組織の重要事項に集中できるようになりました。Dell SecureWorksによる、インテリジェンスと　エンジニアリングサポートを活用することで、現状のリソース内で継続的なセキュリティ強化を行うことが出来るようになりました。」

大手航空宇宙および防衛企業のIT責任者

効果的な情報セキュリティ対策を導入するためには、新たな脅威からの防御は勿論、新しいテクノロジーの採用や日常業務の管理、そして無数の規則や規制へのコンプライアンスの維持も考慮しなければなりません。これに加えて、熟練したセキュリティ スタッフを探して人員を確保したり、予算とリソースの最適な配分方法を決定したりする作業も必要になります。ITセキュリティ部門が頻繁にパンク寸前になるのも、これでは無理のない話です。

デルは、お客様が直面する課題を熟知しています。そのため、多くの組織からパートナーとして選ばれ、Dell SecureWorksを採用いただいています。情報セキュリティサービスのポートフォリオを幅広く取り揃えているデルにお任せいただければ、お客様のセキュリティ部門は最も重要な案件にリソースを集中させることができます。デルのセキュリティ専門スタッフが、お客様のセキュリティ部門の一員として業務を行い、社内のセキュリティやコンプライアンスの現状とのギャップを埋めて体制を強化、そしてリスクの削減に関わる業務をサポートいたします。

独自のサイバー スレット インテリジェンスの活用により脅威を可視化し高度なサービスを提供

サイバー スレット インテリジェンスが、デルのあらゆるサービス ポートフォリオを支えています。グローバルな脅威の可視化を行う中で、Dell SecureWorksのCounter Threat Unit（CTU）リサーチ チームが解析したスレット インテリジェンスは、セキュリティ デバイスのシグネチャやポリシー、攻撃者のブラックリスト、およびイベントの相関分析に適用されています。加えて、攻撃者と攻撃手法に関する脅威情報を、デルのセキュリティ アナリスト、セキュリティ コンサルタント、およびインシデント レスポンス担当者がオープンなフィードバック ループを通じて積極的に共有します。その結果、お客様はデルの全てのサービス ポートフォリオで、より的確で効果的なサポートを受けることができます。デルは、お客様が直面しているビジネス課題の本質を理解し、その問題に有効なセキュリティ戦略、リスク戦略、およびコンプライアンス戦略を提案いたします。

Dell SecureWorksは、ガートナー社の「Magic Quadrant for Global MSSPs」[1]で、
リーダー クアドラントに位置付けられています。

Dell SecureWorks の包括的な IT セキュリティ サービス

Dell SecureWorks のサービスをご利用いただくことで、お客様のIT環境は、進化し続ける脅威へのセキュリティとコンプライアンス体制を強化し、リスクを削減することができます。

マネージド セキュリティ サービス

- 24×7 セキュリティ監視
- エンドポイント監視
- セキュリティ デバイス管理
- ログ管理
- セキュリティ情報管理
- 脆弱性管理
- Web App スキャニング
- Enterprise iSensor
- SIEM 管理
- 高度なセキュリティ対策機器の監視&管理
- サーバーの監視&保護

マネージド セキュリティ サービスの強みは、24時間365日お客様を攻撃から守ることができる独自仕様の管理テクノロジー、認定セキュリティ アナリスト、および極めて高度なスレット インテリジェンスにあります。

デルのセキュリティ アナリストは、お客様のセキュリティ部門チームの一員として業務を行い、組織全体のIT環境を監視し脅威の検知に努めます。デルは、お客様固有の環境に合わせてカスタマイズしたサービスをお届けします。

また、オプションとして様々なサービスを柔軟にご提供いたします。

セキュリティ & リスク コンサルティング

- ネットワーク & Web App テスト
- クラウド セキュリテ
- モバイル セキュリティ
- コンプライアンス&認証
- ポリシー開発&実装
- 専門家の常駐
- セキュリティ啓発トレーニング ソリューション
- Red Team テスト

セキュリティ & リスク コンサルティングチームは、その専門技術と分析能力を通じて、お客様のセキュリティ体制の強化、リスクの軽減、コンプライアンスの推進、および運用効率の向上を支援します。

デルのコンサルタントは、幅広く詳細な専門知識と様々なセキュリティ資格を有しており、技術の高さにおいて業界トップクラスです。

スレット インテリジェンス

- 特定の脅威に対する解析
- 脅威、脆弱性情報およびアドバイザリ情報の提供
- マイクロソフト更新プログラムの分析
- 毎週のインテリジェンス報告
- インテリジェンス ブリーフィング
- マルウェアの分析
- CTU サポート
- 攻撃者DBの提供
- 特的の脅威の追跡

スレット インテリジェンスによって、ネットワークの末端まで脅威が可視化されます。
今日のサイバー空間は脅威にあふれていますが、デルは、お客様の組織にとって重要となる世界的なトレンドや脅威発生の状況に関する警告を出すことができます。
組織や管理職を故意に標的にしている恐れのある攻撃者があれば、それを特定するうえでもスレット インテリジェンスは有効です。
防御の提案をするだけではなく、攻撃者を事前に阻止できるようサポートします。

インシデント レスポンス

- PFI：PCISS 認定のフォレンジック調査認定機関
- インシデント・ハンドリングと管理
- CSIRP 開発
- CSIRP ギャップ分析
- DDoS 対策
- 標的型攻撃対策
- 対応シュミレーション
- デジタル・フォレンジック調査
- 特定の脅威に対する対応

インシデント レスポンス & デジタル フォレンジック サービスは、脅威を急速に封じ込めた上で根絶の実施を行うので、組織のセキュリティ侵害に被る時間と影響を最小限に留めることができます。

デルの"インテリジェンス"である サイバー スレット インテリジェンスおよびグローバルな可視化を活用し、最も複雑で大規模なセキュリティインシデントを見据えた予防と対策、そしてリカバリができる体制を整えてください。

デルのIT情報 セキュリティ サービスの詳細については、www.secureworks.jp をご覧ください。
Dell SecureWorksのセキュリティ セキュリティスペシャリストにご相談の場合は、
Eメール DSWRX_JP_Sales@dell.com にご連絡ください。

Dell SecureWorksについて

Dell SecureWorksは、サイバー スレット インテリジェンスを使用して、世界中の何千もの組織を、予測可能で継続的な応答型プロテクションで保護しています。Counter Threat Unit（CTU）リサーチ チームの英知によって強化されたDell SecureWorksの情報セキュリティ サービスは、組織がプロアクティブに防御を固める支援をいたします。また、サイバー攻撃を継続的に検知して阻止し、セキュリティ侵害からより迅速にリカバリができるようサポートいたします。

1 ガートナー社「Magic Quadrant for Global MSSPs」Kelly M. Kavanagh、2014年2月26日

DELL SecureWorks

Dell SecureWorks Security & Risk Consulting Services

セキュリティ & リスク コンサルティング サービス

Dell SecureWorks のセキュリティ&リスク コンサルティングサービスではその専門技術と分析能力を通じて、お客様のセキュリティ体制の強化、 リスクの軽減、コンプライアンスの推進、および運用効率の向上を支援致します。

Dell SecureWorksのコンサルタント

Dell SecureWorks のセキュリティ コンサルタントは、情熱を持ち、高度な資格と認定を受けたセキュリティの専門家です。また、技術面の厳しい審査に合格し、継続的に行われるセキュリティのトレーニングや講習を受けています。

デルは、セキュリティの知識を持っているだけでなく、リ スク管理やお客様のビジネスプロセスについても語ることができ、業界用語を使わずにビジネス向けの言葉でお客様と話すことができるセキュリティコンサルタントを探し求めています。

効果的なITセキュリティ対策を実現する業務には、新しいテクノロジーの採用、日常業務の管理、コンプライアンスの維持だけでなく、新たな脅威から組織を保護することも含まれます。
これに加えて、熟練したセキュリティスタッフを探して人員を確保したり、予算とリソースを最適なかたちで割り当てたりする作業も必要になります。この状況では、IT セキュリティグループに大きな負荷がかかるのも当然といえます。

デルのコンサルタントは高度な資格を有しており、技術の高さにおいて業界 トップクラスです。
デルのセキュリティコンサルタントは、お客様のセキュリティ防御のテストと改善、適用要件へのコンプライアンスの評価、セキュリティプロセスの効率化、新しいセキュリティ対策の計画と開発を支援し ます。

高度なサイバー スレット インテリジェンスに基づくセキュリティ & リスク マネジメント サービス

サイバー スレット インテリジェンスが、デルのあらゆるサービス ポートフォリオを支えています。
グローバルな脅威の可視化を行う中で、Dell SecureWorksのCounter Threat Unit（CTU）リサーチ チームが解析したスレット インテリジェンスは、セキュリティ デバイスのシグネチャやポリシー、攻撃者のブラックリスト、およびイベントの相関分析に適用されています。
加えて、攻撃者と攻撃手法に関する脅威情報を、デルのセキュリティ アナリスト、セキュリティ コンサルタント、およびインシデント レスポンス担当者がオープンなフィードバック ループを通じて積極的に共有します。
デルのセキュリティコンサルタントが、このインテリジェンスを、あらゆる取り組みに反映することで、お客様は、より的確で効果的なサポートを受けることができます。

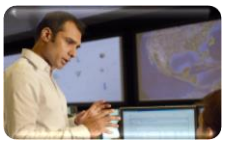
Dell SecureWorks のセキュリティ&リスク コンサルティングサービスでは、独自の専門技術、経験、および視点を通じて、お客様のセキュリティ、リスク、およびコンプライアンスに関する懸案事項に対処します。

Dell SecureWorks Security & Risk Consulting Services

現実のサイバー攻撃を熟知した、深い洞察によるアセスメントとアドバイスを提供致します。

CTU インテリジェンス

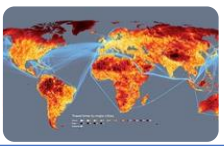
柔軟性の高い アプローチ



業種固有の 専門知識

Big Data を活用する 独自のテクノロジー

全世界をカバー するセキュリ ティ運用



全員が有資格の セキュリティ 専門家

Dell SecureWorks が持つ能力・技術をサービスに反映

1．**グローバルで対応：**世界70ヶ国、5,000件を超えるサービス実績

2．**全員が有資格の専門家：**全世界で、1,000人以上のエキスパート

3．**独自のメソドロジ：**経験に裏付けられた、洗練されたフレームワーク

4．**CTUリサーチの解析結果を活用：**最新の脅威に対し、実践的な対策を提示

5．**柔軟な対応：**お客様の環境に応じて最適なサービス形態を提供

テスト & アセスメント	コンプライアンス サービス	セキュリティ レジデンシー	セキュリティ & ガバナンス プログラム開発	セキュリティ アーキテクチャ & デザイン

ストラテジック コンサルティング & アドバイザリ

ペネトレーション テスト (基本および完全)	脆弱性 アセスメント	Web API テスト	CUNA	ガバナンス、リスク、コンプライアンス	クラウド セキュリティ 戦略 コンサルティング	セキュリティ ヘルス チェック
物理セキュリティ アセスメント	脆弱性 検出	Web サービス テスト	EI3PA	インシデント レスポンス	企業情報 セキュリティ	セキュリティ アーキテクチャ アセスメント
Red Team テスト	ウォー ダイヤリング	無線セキュリティ テスト	FFIEC/GLBA	セキュリティ管理	CSIRP 開発	セキュリティ アーキテクチャ & デザイン
リモート ソーシャル エンジニアリング	Web App セキュリティ アセスメント		FISMA	MSS 統合付加価値サービス	内部監査支援	
モバイル アプリ セキュリティ アセスメント	モバイル デバイス 利用リスク アセスメント	クラウド ベンダー セキュリティ アセスメント	HIPAA/HITECH/ 実践活用	セキュリティ オペレーション	モバイル セキュリティ 戦略 & ロードマップ	
企業情報 セキュリティリスク アセスメント	ネットワーク セキュリティ アーキテクチャ レビュー	第三者 デューデリジェンス /ベンダー管理	ISO 2700X	セキュリティ プログラム 管理	セキュリティ啓発 プログラム	
情報セキュリティ アセスメント	ネットワーク&システム セキュリティ アセスメント		NIST	SOC 開発	セキュリティ ポリシー レビュー & 開発	
			PCI			

セキュリティ 啓発 トレーニング ソリューション (CISO Office)

オンデマンド セキュリティ トレーニング	セキュリティ 啓発 ニーズ アセスメント	セキュリティ 啓発プログラム開発	カスタム セキュリティ トレーニング サービス	フィッシング 模擬訓練	セキュリティ管理 啓発プログラム

Dell SecureWorks のIT情報 セキュリティ サービスの詳細については、www.secureworks.jp をご覧ください。
Dell SecureWorks のセキュリティ セキュリティスペシャリストにご相談の場合は、
Eメール DSWRX_JP_Sales@dell.com にご連絡ください。

DELL SecureWorks

Dell SecureWorks Managed Security Services

マネージド セキュリティ サービス

Dell SecureWorks は、70 を超える国々の 4,000 社を上回るお客様のITインフラを、サイバー上の脅威から保護する為に常時、休むことなく監視し続けています。

世界 8 拠点のセキュリティ オペレーションセンター(SOC)で、日々760 億を超えるサイバーイベントを処理する Dell SecureWorks は、

- ✓ **情報資産の保護**
- ✓ **コンプライアンスの改善**
- ✓ **コストの削減**

において、あらゆる規模のお客様から信頼を得ています。

現代のサイバーセキュリティの脅威を対抗するには、適切な計装、情報、および経験が必要です。簡単に聞こえるかもしれませんが、正確な調整が必要となります。
セキュリティスタッフは膨大なデータをより分け、実際の脅威を特定して対応する必要があります。多くの組織には、細かく調整したセキュリティプログラムを年中無休で維持するための時間、資金、人員が不足しています。

Dell SecureWorks は、情報セキュリティ インフラストラクチャの管理において、70 か国以上、4,000 社以上のクライアントから信頼を得ています。デルのサービスをご利用いただくことで、優れたグローバルな脅威に対する可視性と、1,000 名を越える認定セキュリティ専門家の経験をご活用いただけます。

高度なサイバー スレット インテリジェンスに基づく マネージド セキュリティ サービス

スレット インテリジェンスは、デルのあらゆるサービス ポートフォリオを支えています。Dell SecureWorks の Counter Threat Unit™（CTU™）のリサーチチームが収集&解析したインテリジェンスは、グローバルな脅威の可視化を活用し、組織が 直面する脅威に関するさまざまな背景情報として提供されます。

また、デルのセキュリティ研究者およびセキュリティ オペレーションセンターのセキュリティアナリストは、攻撃者と攻撃手法に関するインテリジェンスを、オープンなフィードバックループを通じて積極的に共有します。その結果、クライアントは、セキュリティインシデント発生時に、より的確で効果的なサポートを受けることができます。

カウンター スレットプラットフォーム（CTP）

カウンタースレットプラットフォームはDell SecureWorks 専用のマネージド セキュリティ サービスプ ラットフォームで、脅威からお客様をインテリジェ ントに防御します。
CTP はマルチテナントの分散アーキ テクチャを搭載しており、数十億件のイベントを分析し、 世界各国の数千社にのぼるクライアントを保護しています。

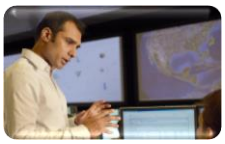
Dell SecureWorksは、ガートナー社の「Magic Quadrant for Global MSSPs」[1]で、
リーダー クアドラントに位置付けられています。

Dell SecureWorks Managed Security Services

膨大な監視ポイントと攻撃者の監視を通じて、グローバルの可視化でお客様を守り管理コストを削減する

CTU インテリジェンス

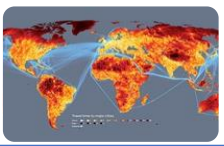
柔軟性の高いアプローチ



業種固有の専門知識

Big Data を活用する独自のテクノロジー

全世界をカバーするセキュリティ運用



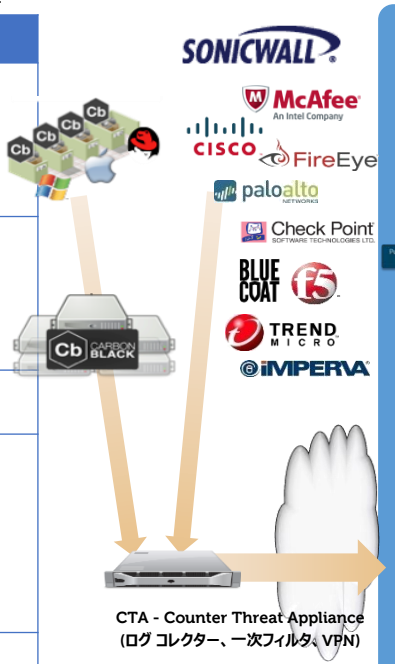
全員が有資格のセキュリティ専門家

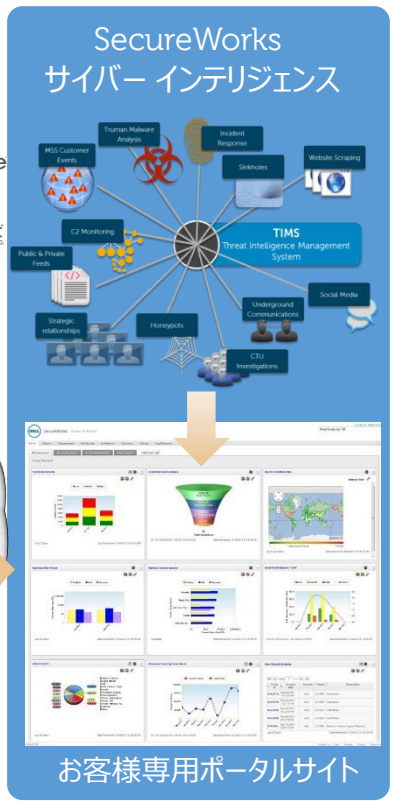
Dell SecureWorks が持つ能力・技術をサービスに反映

1. **グローバルで対応：**世界70ヶ国、4,000社以上のお客様にサービス
2. **マルチベンダーで、幅広い監視対象：**最新の機器にも迅速に対応
3. **人の目で判断を下す：**単なる、機械的な振り分けとは違う
4. **相関分析：**複数の対象を監視し相関分析し攻撃者の意図を明らかに
5. **事前の対抗措置：**攻撃者情報を解析し事前にお客様へ対応を促す

主要な監視&管理対象セキュリティ機器一覧

分類	ベンダー	モデル
Firewall	Check Point Cisco Juniper McAfee Sidewinder Nokia	Firewall-1 Firefly, Power-1, IPxx, 2xxx, 4xxx, 12xxx PIX Netscreen, SSG Secure Firewall IP XXX
IDS/IPS	Cisco IBM ISS McAfee Sourcefire(NG) Tipping Point Dell	IDS/IPS Proventia-G, GX I, M 3Dxxxx iSensor
Malware Protection	FireEye	WebMPS, EmailMPS
NGFW/UTM	Cisco Check Point IBM ISS Juniper Dell Fortinet PaloAlto Networks	ASA UTM Proventia Mxx, MXxxxx SRX SonicWALL SuperMassive, NSA, TZ Fortigate PA
WAF	Citrix f5 Imperva	NetScaler Application Security Manager SecureSphere
Endpoint (PC)	Bit9	Carbon Black





※注
- MSSでサポートしている「主要な」ベンダー・モデルを記載しております。
- 機能によっては現状サポートできていないものもございます。
- 詳細および最新のサポート状況については個別にお問い合わせいただくようお願い致します。

Dell SecureWorks のIT情報 セキュリティ サービスの詳細については、www.secureworks.jp をご覧ください。
Dell SecureWorks のセキュリティ セキュリティスペシャリストにご相談の場合は、
Eメール DSWRX_JP_Sales@dell.com にご連絡ください。

1 ガートナー社「Magic Quadrant for Global MSSPs」Kelly M. Kavanagh、2014年2月26日

DELL SecureWorks

Dell SecureWorks Incident Response & Forensics Services

インシデント レスポンス & デジタル フォレンジック サービス

Dell SecureWorks のインシデント レスポンス & デジタル フォレンジックサービスは、脅威を急速に封じ込めて根絶するため、セキュリティ侵害を被る時間とその影響を最小限に留めることができます。

高度なサイバー スレット インテリジェンスおよびグローバルな可視化を活用し複雑で大規模なセキュリティ インシデントを見据えた予防と対策、そしてリカバリができる体制の整備をご検討ください。

セキュリティ侵害が発生してから、セキュリティ インシデントに対する準備不足に気付いても手遅れです。セキュリティ インシデントは危機的状況であり、対応を担うITスタッフに大きなプレッシャーを与えます。実証済みの対応計画や戦略がなければ、ITスタッフは、明確な指示や優先度が分からないままに、ストレスを感じながら重大な判断を下さなければなりません。

このような状況下では、容易に誤った判断を招き、インシデントにかかる時間およびその影響を長引かせることになります。Dell SecureWorksは、インシデント レスポンスの計画と分析から緊急インシデント レスポンスおよびフォレンジックに至る、さまざまなインシデント レスポンスおよびデジタル フォレンジックのサービスを提供します。

セキュリティ侵害が発生した場合、Dell SecureWorksをご利用いただくことで、被害を最小限に抑え、破損したデータを修復し、法的措置に備えて証拠を保存できます。

高度なサイバー スレット インテリジェンスに基づくインシデント レスポンス

スレット インテリジェンスは、デルのあらゆるサービス ポートフォリオをサポートします。Dell SecureWorksのCounter Threat Unit™（CTU™）のリサーチチームが構築したインテリジェンスでは、グローバルな脅威の可視化を活用し、組織が直面する脅威に関するさまざまな背景情報を提供します。
また、デルのセキュリティ研究者およびインシデント レスポンス セキュリティコンサルタントは、脅威の攻撃者と攻撃手法に関するインテリジェンスを、オープンなフィードバックループを通じて積極的に共有します。
マルウェア分析およびリバース エンジニアリングにより、脅威に関するさらなるインテリジェンスと詳細な背景情報が得られます。その結果、クライアントは、セキュリティ インシデント発生時により的確で効果的なレスポンス サポートを受けることができます。

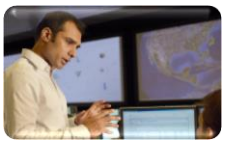
Dell SecureWorksのインシデント レスポンス　サービスでは、攻撃元の手口に関してデルが持つ高度なインテリジェンスを駆使して個々の対応に当たります。このインテリジェンスには、脅威の目的、 脅威の背後に潜む人物、およびお客様の環境から脅威の元を根絶する方法といった貴重なコンテキストが含まれています。

Dell SecureWorks Incident Response & Forensics Services

脅威に的確に対応した実践的知見に基づく、攻撃への対処を実現するインシデント レスポンス サービス

CTU インテリジェンス

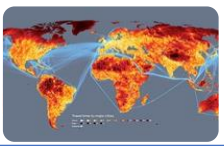
柔軟性の高いアプローチ



業種固有の専門知識

Big Data を活用する独自のテクノロジー

全世界をカバーするセキュリティ運用



全員が有資格のセキュリティ専門家

Dell SecureWorks が持つ能力・技術をサービスに反映

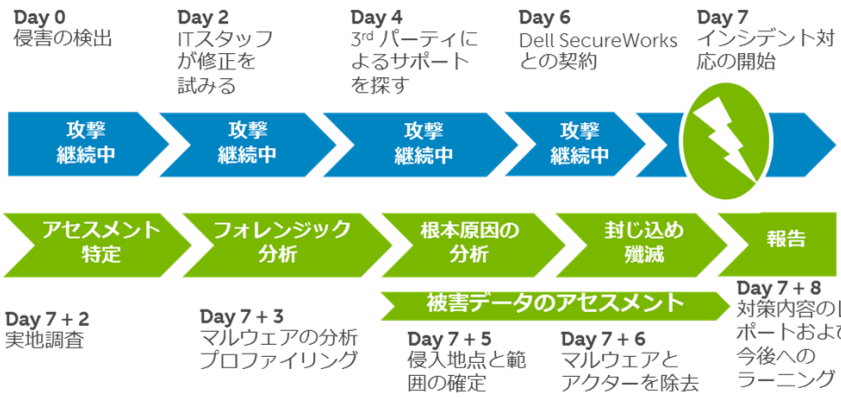
侵害の発生に備えてインシデント対応計画を策定しておき、侵害への対応を支援する外部のコンサルタントを起用することで、侵害を受けたレコード1件あたりのコストを最大55ドル削減できます。

Ponemon Institute
2013 Cost of Data Breach Study
（データ侵害による2013年の損害コストの調査）
（米国では、28,765件のレコードが標準的な顧客情報その他の機密情報などのデータ侵害の対象）

何が
どのように
侵害されたか
特定し

脅威を
封じ込め
食い止め

徹底的に
削除し
リトライを
防御



包括的なインシデント レスポンス サービス

セキュリティ インシデントの発生前、発生中、そして発生後までエンドツーエンドのサービスを提供します。

セキュリティ侵害に対する準備

- CSIRP 作成
- CSIRP ギャップ分析
- DoSへの準備
- 公開計画
- 高度な脅威への準備
- 机上訓練（演習）
- コンプライアンスの統合

セキュリティ侵害への対処

- インシデント処理
- デジタル フォレンジック調査
- インシデント管理
- マルウェア分析

インシデント対応の後

- 根絶＆回復
- 事後分析
- 文章化

法律、規制やコンプライアンスに関するレポート条件を満たす

インシデント対応のリテーナー・サービス

Dell SecureWorks のIT情報 セキュリティ サービスの詳細については、www.secureworks.jp をご覧ください。
Dell SecureWorks のセキュリティ セキュリティスペシャリストにご相談の場合は、
Eメール DSWRX_JP_Sales@dell.com にご連絡ください。

DELL SecureWorks