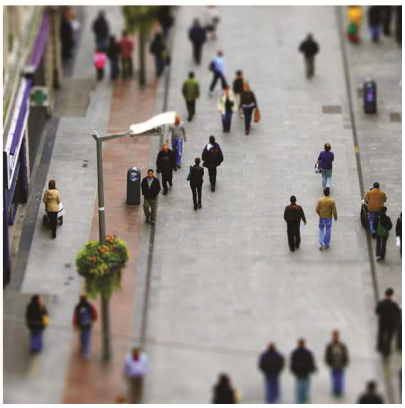
Threat Intelligence White Paper

猛威を振るうリスト型攻撃への対策はあるか？

2013 年 7 月



免責事項

本文書の著作権は Dell SecureWorks に帰属し、Dell SecureWorks は本文書またはここに含まれる如何なる情報を無断で転用、流用、転載することを禁じます。Dell SecureWorks は本資料およびここに含まれるいずれかの内容そのもの、またはこれを信頼することによって生じる如何なる損害に対し（予見できたか、直接的または間接的か、必然的か偶然か、特殊か典型的か、懲罰的かによらず）特定の責任を負うものではありません。

本文書で利用されている標、名称、製品名は各社の商標、商号または商品名です。Dell およびその関係各社はこれらの誤記や誤表示など、不作為による誤りについて責任を負うものではありません。

目次

リスト型攻撃の猛威

某有名 SNS サービスから会員情報が漏洩

不正アクセス事件の発生が止まらない。

LINE サービスの公開から約 2 年となる 7 月 23 日に世界 2 億ユーザーを達成したことを発表した LINE 社（旧 NHN Japan）は、そのわずか数日前の 7 月 19 日、同社が運営する NAVER サービス（NAVER まとめ、N ドライブ、NAVER Photo Album、pick、cafe）の会員情報が外部からの不正アクセスにより流出した可能性があることを公表した。

同社の調査によると、7 月 17 日 20 時 51 分から 18 日 10 時 57 分まで、会員データベースを管理しているサーバーに外部から不正アクセスがあった痕跡を発見したという。流出した可能性がある情報は、NAVER サービス会員の E メールアドレス、ハッシュ化されたパスワード、アカウント名などで、実に 169 万 2496 件にのぼる会員の情報が外部へ流出した可能性がある。

なお、漏洩した可能性がある情報のうち、パスワードはハッシュ化されているため高度な解読技術がなければ即座に悪用することは困難だと考えられるが、同社では今回の不正アクセスを受けて新しいパスワード設定機能を設置し、流出した可能性のある会員へパスワードを再設定するようにメールで呼びかけている。

続発する不正アクセス被害

振り返ると、2013 年 4 月上旬～6 月上旬のたった 2 ヶ月間で、公表されているだけでも下表 1 に示すように非常に多くの企業が不正ログインの被害を受けている。

最近でも、前述した LINE 社の NAVER サービス以外に、任天堂のクラブニンテンドーが 1545 万回を超える不正アクセスがあったことを 7 月 5 日に発表し、その後 7 月 9 日にはコナミデジタルエンタテインメントが KONAMI ID ポータルサイトにおいて 394 万回を超える不正アクセスがあり、そのうち 35 万件ほどが実際に不正ログインに成功していたことを発表している。

図表 1

企業名	サービス名	公表日	不正アクセス数	不正ログイン数
NTT レゾナント	goo	2013/4/3	不明	108,716 件
イーブックイニシアティブジャパン	eBook Japan	2013/4/5	2,821 件	779 件
カルチュア・コンビニエンス・クラブ	T サイト	2013/4/5	不明	299 件

東日本電信電話	フレッツ光メンバーズクラブ	2013/4/10	約 24,000 件	77 件
東日本旅客鉄道	My JR-EAST	2013/4/17	約 26,000 件	97 件
エムティーアイ	mopita	2013/4/22	不明	5,450 件
ディノス	ディノスオンラインショップ	2013/5/8	約 1,110,000 件	約 15,000 件
資生堂	ワタシプラス	2013/5/17	約 240,000 件	682 件
イード	インサイド	2013/5/21	不明	2,515 件
三越伊勢丹ホールディングス	三越オンラインショッピング	2013/5/25	5,202,002 件	8,289 件
阪急阪神百貨店	阪急・阪神オンラインショップ	2013/5/29	不明	2,382 件
ハピネット	ハピネット・オンライン	2013/6/3	不明	9,609 件

狙われる『リスト』

これまで、オンラインサービスに対する不正アクセスの多くは、『総当たり攻撃（ブルートフォースアタック）』と呼ばれる手法を通じて行われており、これは悪意のハッカーなどの攻撃者がパスワードクラッキングツールなどを活用して辞書に載っている文字列やランダムな英数字の組み合わせを一つずつ高速に試していくことで、主に平易な単語や短いパスワードを使っているアカウントへ “あわよくば” 不正ログインしようというものだった。

しかし、最近続発している不正アクセス被害は、こうした総当たり攻撃では見られないような高確率で不正ログインに成功しているケースも多い。下表 2 を見てほしい。これは eBookJapan 社が自社に対する不正アクセス被害の調査を行った際の資料であるが、たった 1 度のログイン試行で不正ログインに成功していた例が 386 件もある。

図表 2

ID あたり PW 試行回数	該当 ID 数
1	386
2	347
3	37
4	4
5	5

これはどういうことか。冒頭で紹介した NAVER サービスの事件から遡ること 2 か月、ヤフーは 5 月 23 日に、5 月 17 日に公表した Yahoo! JAPAN ID 約 2,200 万件の漏洩事件において、約 148 万件については ID に加えてハッシュ化されたパスワードと、パスワードリセットに使われる秘密の質問の一部が流出した可能性が高いと発表している。

つまり悪意の攻撃者はこうした有名オンラインサービスから膨大なアカウントとパスワードの組み合わせリストを盗み出し、そのまま別のオンラインサービスへの不正ログインに転用しているのだと考えられる。

シンプルだが抜群の攻撃力

多くのオンラインサービスはアカウント名として E メールアドレスを採用しており、サービスごとにパスワードを変えるほどセキュリティ意識の高い利用者はまだまだ少ない。そして特定のオンラインサービスから漏洩したアカウントとパスワードのリストは、既にそのサービス上で有効に使われていたものであり、その利用者が他のオンラインサービスでも同じアカウントやパスワードを使用している可能性はかなり高い。

そのため、ひとたびどこかのオンラインサービスから有効なアカウントや E メールアドレスとパスワードのリストが漏洩すると、ハッカーコミュニティなどで流通しているリストを入手した攻撃者は、いとも簡単に様々なオンラインサービスへ不正ログインできてしまうわけである。

このように、実際にどこかのサービスで利用されているアカウントとパスワードの “リスト” を不正に入手し、それを悪用して不正ログインを試みることから、この種の不正アクセスは『リスト型攻撃』や『リスト型アカウントハッキング』などと呼ばれ、オンラインサービスを提供する企業やセキュリティ業界などを中心に、警戒が強まっている。

リスト型攻撃への対処

従来型の対策では防げない

従来型の『総当たり攻撃（ブルートフォースアタック）』と呼ばれる攻撃手法であれば、辞書に載っている文字列やランダムな英数字の組み合わせを、いわば “あてもなく” 一つずつ試していくため、相当数の試行をしなければ不正ログインに成功する確率は極めて低い。このため、例えば一定時間内に連続して 5 回以上パスワード入力に失敗すると、当該アカウントでのログインを一時停止するというアカウントロックアウト機能が有効であった。

しかしながら『リスト型攻撃』では、たった数回の試行、場合によっては 1 回の試行で不正ログインに成功してしまう可能性があるため、不正ログイン数の上限に達してアカウントがロックアウトされてしまう前に、攻撃者は正規の利用者としてサービスにログインし、個人情報などを盗み取ることができてしまう。

侵入検知システムによる検出も困難

アカウントロックアウトが無意味であれば、ネットワークやシステムに対する不正侵入を検知する IDS (Intrusion Detection System) や IPS (Intrusion Prevention System) などのシステムによる検出はできないだろうか。侵入検知システムは既知の攻撃パターンに該当する通信パケットを見つけ出すことで不正アクセスを検知する。つまり、アクセス先のシステムに不具合を引き起こすような不正なデータが通信パケットに含まれていれば不正と判断して警告を出したりアクセスを遮断したりすることもできるが、リスト型攻撃による不正アクセスは、通信内容からしてみれば正規のユーザーが普通にログインしようとしているとしか見えないため、残念ながらこれを防ぐための有効な手立てとはならない。

それでは、Web アプリケーションを不正な攻撃から保護する WAF (Web Application Firewall) はどうだろうか。WAF は保護対象のアプリケーションの脆弱性を悪用するような不正なスクリプトやコマンドを送りつけることで、アプリケーションの誤動作を発生させたり、セキュリティ機能を回避したりする攻撃を防止する。したがって、こちらもやはり正規のログインと何ら変わらない方法で行われるログイン試行を防ぐことはできない。

処方箋としての二要素認証

こうなるともはや八方塞がりで打つ手なし、と思われるかもしれないが、効果的な対処方法がないわけではない。もちろん、オンラインサービスの利用者がサービスごとに異なるアカウントとパスワードの組み合わせを確実に利用するように徹底できれば多くの被害を防ぐことができるはずであり、それを啓蒙するのもサービス提供者の責務の一環とも言えるが、ここではサービス提供者やサイトの運営者が採るべき技術的対応について述べたい。

まず対策として挙げられるのは、いわゆる “二要素認証” である。二要素認証は、文字通りアカウントを認証する際に二つの情報を利用することであり、通常は従来のパスワードに加えてトークンデバイスや生体情報、端末固有の識別情報などが使われる。最近では Google が Gmail アカウントへの不正アクセス多発を受けて、ログイン時にはパスワードの入力に加え、利用者固有の携帯端末へ送信されるパスコードを入力しなければログインできないようにする対策を講じている。

このように、パスワードに加えてサービスの利用者本人しか持ちえない、または知りえない情報をログイン時に要求することで、たとえ悪意の攻撃者が正当なアカウントとパスワードのリストを入手できたとしても、サービスの利用者本人以外がログインすることはできないため、リスト型攻撃への有効な対策であると言える。

ただし、この二要素認証の実装は、サービス提供者側にはトークンデバイスや新たな認証システムに関する追加のメンテナンスコストが必要となり、利用者側にもトークンデバイスを持ち歩く手間や特定の端末からしかアクセスできないなど利便性の観点でデメリットがある。なお、特定端末からのアクセスに限定する形で二要素認証を実装する場合、毎回二要素での認証を要求するのではなく、端末側に前回ログインした履歴情報を保管しておく Cookie が存在しない場合や、Cookie の有効期限が切れた場合だけ二要素での認証を必要とすることで、セキュリティ強度を低下させることなく利用者側の手間も軽減することができる。

こうしたコスト負担や利便性における制約をどうしても許容できない場合、リスト型攻撃を未然に防ぐことは難しくなるかもしれないが、システムへのログイン状況をモニタリングすることで、攻撃の兆候をできる限り早い段階で検知して攻撃元を特定し、当該の攻撃元からのアクセスを遮断する、といった対処は可能である。

ログから兆候をあぶり出す

システムやアプリケーションへのログイン状況をモニタリングすることでリスト型攻撃の兆候をあぶり出すには、正規の利用者によるログインとリスト型攻撃によるログインとの違いを見極める必要がある。ログインを受け付けるシステムやアプリケーション側から見ると、リスト型攻撃による一つ一つのログイン操作は技術的に正規のものと変わらないため検出が難しいということは前段で述べた通りであるが、少し広い視野でログイン傾向を観察することで浮かんでくる正規ログインとの違いがある。

例えば、リスト型攻撃の場合、ある特定の端末から膨大なアカウントに対するログインが短期間で同時多発的に発生しているということが挙げられる。職場や家族の間で同一の端末を共有している場合、2 つや 3 つのアカウントに対するログインが同一端末から発生することはあるかもしれないが、1 時間以内に 100 以上のアカウントに対するログイン試行が一つの端末から発信されているとなると、正規のログイン環境ではありえないとみて差し支えない。したがって、特定ホスト（IP アドレス）から一定期間内に一定数以上のログイン試行があった場合、当該端末からリスト型攻撃が発生しているとみて、ネットワーク機器や Web アプリケーションで当該端末からのアクセスを遮断するように設定する、という流れでの対処は可能となる。

また、そもそも普段サービスを提供している中ではありえないほどのログインが突発的に発生するということも挙げられる。三越オンラインショッピングの例では、5 月 6 日～23 日の 17 日間で不正ログイン試行が約 520 万件あったことが同社調べで判明しているが、このオンラインサービスの会員数は約 73 万人であるため、もしこのログイン試行が正規のものであったとすると、全会員が 2 週間ほどの期間に 7 回以上、つまり 2 日に 1 回はログイン試行していることになる。もちろん普段からこれだけリピート率の高いログイン数を誇っているのであればこの上ないことだが、実際にログインに成功しているのは 8,000 件ほどであり、ほとんどがログインに失敗している。そのため同社もこれを異常事態として認識し、オンラインショッピングサイトを一時閉鎖するに至っている。したがって、Web サイトやシステムに対するログイン試行がピーク時よりもさらに上回るような状態が数時間または数日間続くようであれば、リスト型攻撃やブルートフォース攻撃による不正アクセスを受けている可能性が高いとみて、発信元を特定してアクセスを遮断するなどの対処に移ることができる。

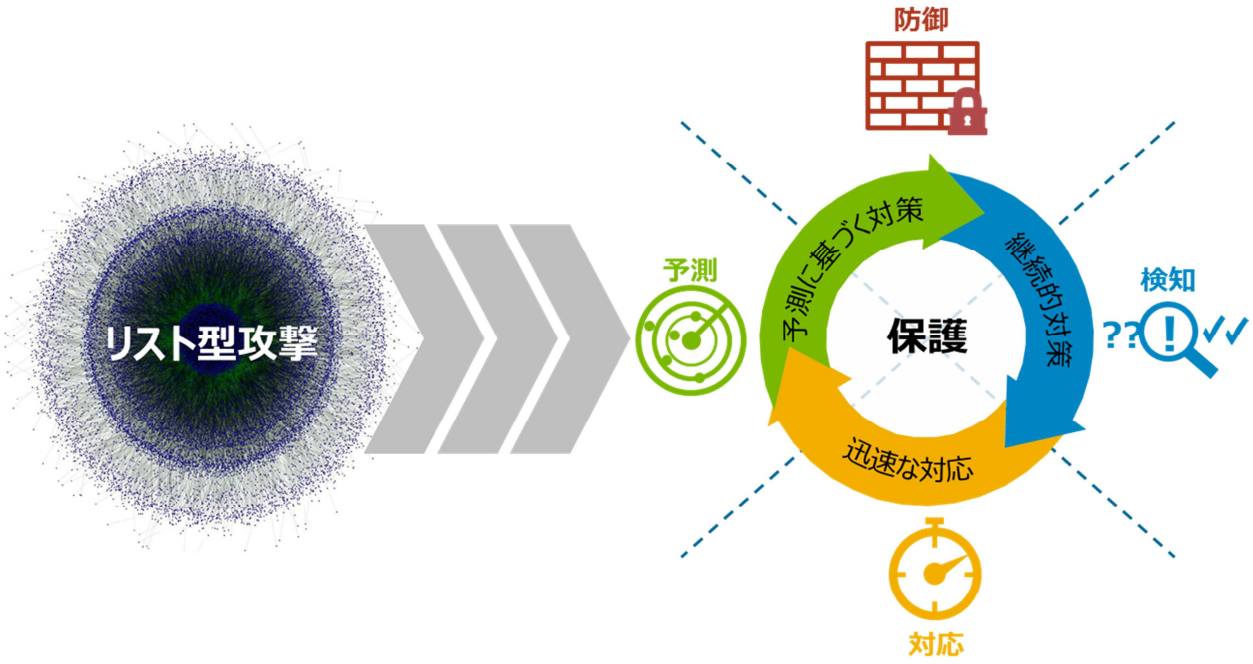
リスト型攻撃対策ソリューション

対策に必要な 4 つの柱

正規ログインとの区別がつきにくく、いつ発生するかもわからないリスト型攻撃に対して、場当たり的な対策や対症療法的な対応だけでは自社の顧客、サービス、システムを保護することはできない。内外のリスク環境の変化や進化する脅威に目を光らせることで攻撃の兆候を『予測』し、リスクの深刻度と保護対象の重要度に応じて『防御』対策を実装する必要がある。すべての情報資産やシステムへの攻撃を完全に防御することは困難であるため、防御対策をすり抜けてくる攻撃をモニタリングして『検知』し、実際に攻撃が検出された場合はあらかじめ定められた体制と手順に沿って速やかに『対応』すべきである。

この『予測』『防御』『検知』『対応』がリスト型攻撃対策に必要な 4 つの柱であり、下図 3 のように、これらが適切に連携することですべての対策の効果が最大限に発揮されると考えられる。

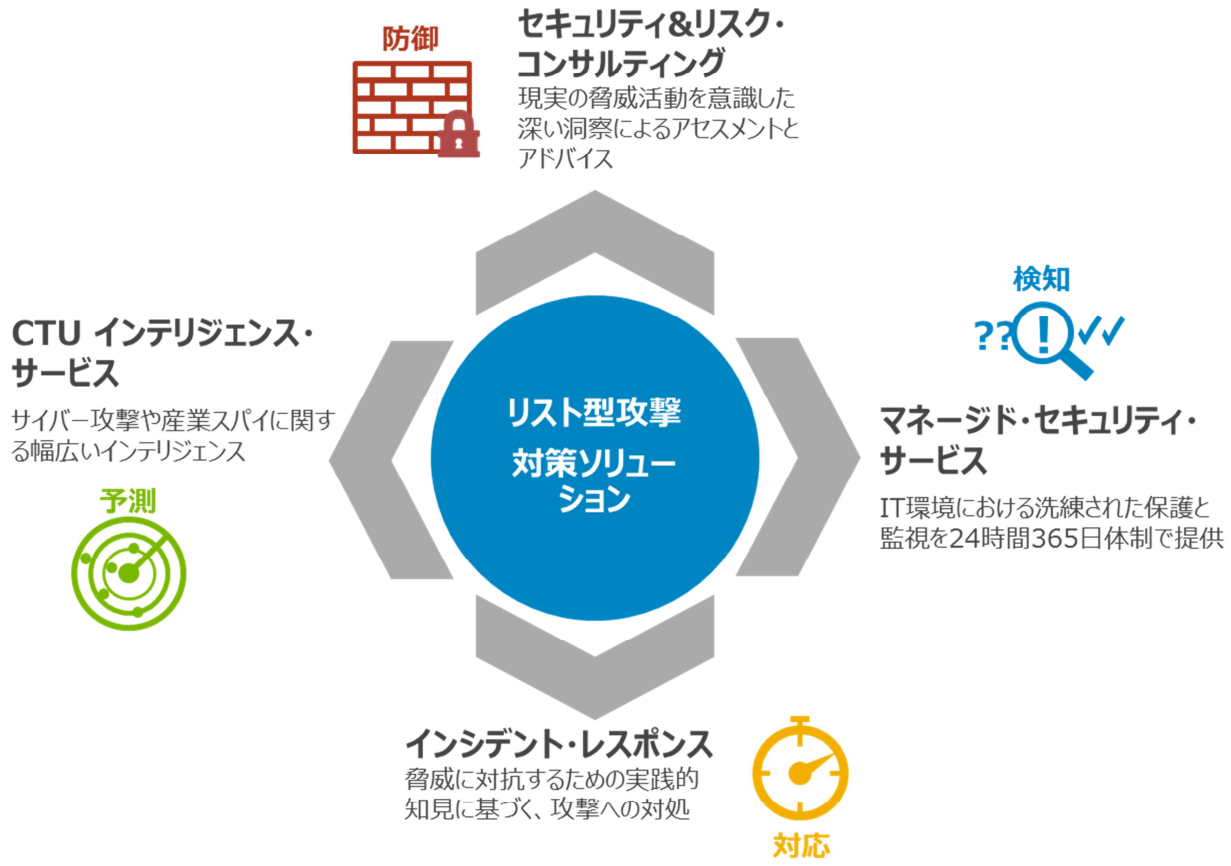
図表 3



Dell SecureWorks のソリューション

Dell SecureWorks は、下図 4 に示す通り、リスト型攻撃対策に必要な 4 つの柱それぞれに対応するソリューションを網羅的に提供しています。

図表 4



CTU インテリジェンス・サービス

Dell SecureWorks の Counter Threat Unit (CTU)は、セキュリティ分野で広く知られている優秀な専門家やグローバル企業、軍事機関、警察当局など様々な経歴を有する研究員で構成される世界有数のセキュリティ調査研究チームです。CTU は、グローバルな脅威の可視化、独自仕様のツールセット、卓越した専門知識を活かして脅威の状況を積極的に監視し、新たに出現しつつある脅威とゼロデイ脆弱性を詳細に分析します。

CTU が日々蓄積しているこうしたインテリジェンスは、以下のような各種サービスを通じてお客様にリスト型攻撃の『予測』に役立つ情報や知見を提供します。

- Threat Intelligence – アカウント・パスワードリスト漏洩事件や、リスト型攻撃の発生状況など、最新のセキュリティインシデントや脅威の傾向に関するアドバイザリーを提供します。
- 攻撃元データベース – C&C (Command & Control) サーバーやボットネットなど、リスト型攻撃の発信元となる可能性があるホストの IP アドレス情報などを提供します。

セキュリティ&リスク・コンサルティング

Dell SecureWorks のセキュリティ&リスク・コンサルティング (SRC) サービスの提供が開始されたのは 2004 年であり、以来セキュリティ、リスク、およびコンプライアンスのニーズを抱えたお客様から絶えず信頼を寄せていただいた結果、SRC サービスで対応したコンサルティング契約はこれまで 5,500 件以上にのぼっています。 Dell SecureWorks では、セキュリティ関連の多彩な経歴を持ち、高度な認定資格を備えたセキュリティのプロフェッショナルだけを採用しています。当社のコンサルタントたちは、監査、公式リスク分析、コンプライアンス、ガバナンス、その他のビジネスに主眼を置いた業務について順次トレーニングと業務経験を積み、あらゆるセキュリティサービスに精通しています。

SRC のコンサルタントは、以下のような各種サービスを通じてお客様によるリスト型攻撃への『防御』対策の実装を支援します。

- リスクアセスメント – お客様環境における現状のセキュリティ対策を評価し、リスト型攻撃に対して脆弱な点を洗い出して推奨改善案を提供します。
- 対策ポリシー策定 – リスト型攻撃対策を実装するにあたって必要なセキュリティポリシー、運用ポリシー、パスワードポリシーなどの策定または改訂に関する推奨案を提供します。
- 対策実装支援 – リスト型攻撃対策に有効な二要素認証やログモニタリングの実装にあたり、お客様環境に最適な製品やソリューションの検討や導入構成、実装方法などについて専門的見地からのアドバイスとプロジェクト管理を提供します。

マネージド・セキュリティ・サービス

Dell SecureWorks のマネージド・セキュリティ・サービス (MSS) は、世界 7 か所のセキュリティ・オペレーション・センター (SOC) から 3,000 社以上のお客様に対して IT セキュリティに関する多彩なマネージド・サービスを 24 時間 365 日休

むことなく提供しています。Dell SecureWorks 独自仕様によるセキュリティ専用プラットフォームである脅威対策プラットフォーム（CTP）では、10 万台を超える Firewall、IDS/IPS、アンチウイルスなどのデバイスから発生する一日 350 億件以上のイベントに対するフィルタリング、関連付け、および分析を行っています。

MSS は、以下のようなセキュリティデバイスの監視と分析を通じてお客様環境に対するリスト型攻撃の『検知』を支援します。

- セキュリティデバイスの監視 – Firewall、IDS/IPS、アンチウイルス、次世代型 Firewall、Web アプリケーション Firewall など
- セキュリティ分析 – 脆弱性管理、セキュリティイベント管理、ログ管理、SOC アナリストによる分析など

インシデント・レスポンス

Dell SecureWorks のインシデント・レスポンス (IR) サービスは、セキュリティ＆リスク・コンサルティングサービスの一環として提供され、セキュリティインシデント発生時の初動駆け付けによるトリアージから被害調査、詳細なデジタル・フォレンジックによる原因究明まで、お客様環境におけるインシデント発生から収束に必要なすべての作業と活動を支援するための体制と専門知識を有しています。Dell SecureWorks が提供するインシデント・レスポンスサービスでは、専門家として認定されたフォレンジック調査員やインシデント調査員が、社内外で開発されたフォレンジック専用ツールや業界ベストプラクティス、その他専門技術などの高度な技術を駆使して解析を行います。

IR に関する専門技術とノウハウは、以下のような各種サービスを通じてお客様環境におけるリスト型攻撃への『対応』を支援します。

- 初動トリアージ – リスト型攻撃によるインシデント発生直後に調査員が現場に急行し、被害発生状況の確認と証拠の保全を実施します。
- フォレンジック解析 – リスト型攻撃によって被害を受けたシステムのディスクやメモリイメージを複製し、調査ラボでマルウェアによる攻撃やデータ漏洩の有無などを解析します。
- インシデント対応シミュレーション – リスト型攻撃を受けた場合に迅速かつ適切な対応ができるかどうか、お客様環境におけるインシデント対応体制と手順の成熟度を確認するための演習を実施し、推奨改善案を提供します。

Dell SecureWorks の特徴

Dell SecureWorks は 70 ヶ国に 3,000 以上のお客様を抱え、世界トップクラスの情報セキュリティサービスで市場をリードするプロバイダです。 Dell SecureWorks のサービスはあらゆる規模の組織にご利用いただいており、資産保護、コンプライアンスの向上、コスト削減を実現しています。 受賞歴のあるセキュリティの専門知識とカスタマサポートを併せて提供する Dell SecureWorks は、情報セキュリティサービスのトッププロバイダです。 Dell SecureWorks の従業員数は、現在 1,300 名以上にのぼります。

Dell SecureWorks の歴史

Dell SecureWorks は、インターネットの脅威から組織を保護することを目的として、1999 年に設立されました。 業界のパイオニアである Dell SecureWorks は、高度なテクノロジーとセキュリティ分野での卓越した経験を組み合わせ、受賞歴のある広範な情報セキュリティサービスを組織に提供することによって、急成長を遂げてきました。 2011 年 2 月の Dell Inc.による買収以降も、セキュリティの新しい機能、テクノロジー、および能力を獲得するために多額の投資を続けています。

Dell SecureWorks では、現在の市場における最も優秀なセキュリティ研究者、セキュリティアナリスト、およびセキュリティコンサルタントの採用に努めています。 トップクラスの人材を獲得することに力を入れ、その人材に必要なツールとトレーニングを提供する一方、研究者、アナリスト、コンサルタント同士が緊密な意思疎通を図るという企業文化も促進しています。 こうした取り組みが、お客様に大きなメリットをもたらすものと考えています。

Managed Security Services

Dell SecureWorks の IT セキュリティに関する多彩なマネージド・サービスは、あらゆる規模の組織にご利用いただいています。 Dell SecureWorks の IT セキュリティサービスは、ネットワーク全体の保護を提供し、ネットワーク境界、重要な内部資産、データ、リモートユーザー、顧客、パートナーを保護します。

Dell SecureWorks の独自仕様によるセキュリティ専用プラットフォームである脅威対策プラットフォーム（CTP）では、企業の顧客ベース全体に渡って毎日 300 億件以上のイベントのフィルタリング、関連付け、および分析を行っています。 マネージド IPS/IDS、ファイアウォール管理、ログ監視、セキュリティ監視、脆弱性管理など、数多くのサービスを提供しています。

Dell SecureWorks の Managed Security Services（MSS）はさまざまな賞を獲得し、表彰も数多く受けています。 最近では、Dell SecureWorks は Gartner の MSSP 部門の Magic Quadrant でリーダーの評価を獲得し

（2011 年 11 月）、Forrester Wave でもリーダーの評価を獲得しました（2012 年 3 月）。また、2012 年、2011 年、2009 年、2008 年、2007 年、2006 年には SC Magazine の「Best Managed Security Service」（最優秀マネージド・セキュリティ・サービス）賞を受賞し、2011 年には SC Magazine のヨーロッパにおける「Best MSSP」（最優秀 MSSP）賞を受賞しました。

詳細については、次の Web サイトを参照してください。www.secureworks.com/it_security_services/

Counter Threat Unit 調査チーム

Dell SecureWorks Counter Threat Unit（CTU）調査チームの第一の目標は、CTU の調査機能とインテリジェンス機能を Dell SecureWorks の業務のあらゆる面で活用して、Dell SecureWorks のお客様の利益を保護することにあります。

CTU は、グローバルな脅威の可視化、独自仕様のツールセット、卓越した専門知識を活かして脅威の状況を積極的に監視し、新たに出現しつつある脅威とゼロデイ脆弱性を詳細に分析します。CTU では、取得した知識を活かして現在の MSS のお客様を保護するための対応策を開発し、さらなる脅威インテリジェンス機能をお客様に提供すると共に、通常のユーザーが直面する脅威についても広く情報を提供します。CTU の調査機能とインテリジェンス機能は、デルのセキュリティ・オペレーション・センターやセキュリティコンサルティングチームとも共有されます。

CTU は世界トップクラスのチームであり、現在のセキュリティ分野で広く知られている優秀な専門家も数名在籍しています。こうした専門の研究者たちは、民間企業、軍事、インテリジェンス、警察当局など、さまざまな経歴の持ち主です。

詳細については、次の Web サイトを参照してください。www.secureworks.com/research

セキュリティ&リスクコンサルティングサービス

Dell SecureWorks セキュリティ&リスクコンサルティングサービス（SRC）サービスの提供が開始されたのは、2004 年です。一部のお客様から提起された独自の課題を解決するため、最初のセキュリティコンサルタントチームが設立されたことがきっかけとなりました。当時のコンサルタントたちは、セキュリティ&リスク・コンサルティング業務が、Dell SecureWorks を現在のような情報セキュリティサービスプロバイダへと成長させるために大きな役割を果たすと考えていました。これ以降、SRC サービスで対応したコンサルティング契約は 5,500 件以上にのぼっています。Dell SecureWorks には、セキュリティ、リスク、およびコンプライアンスのニーズを抱えたお客様から絶えず信頼を寄せていただいており、今年だけで 1,500 件もの契約を完了できると予想されています。

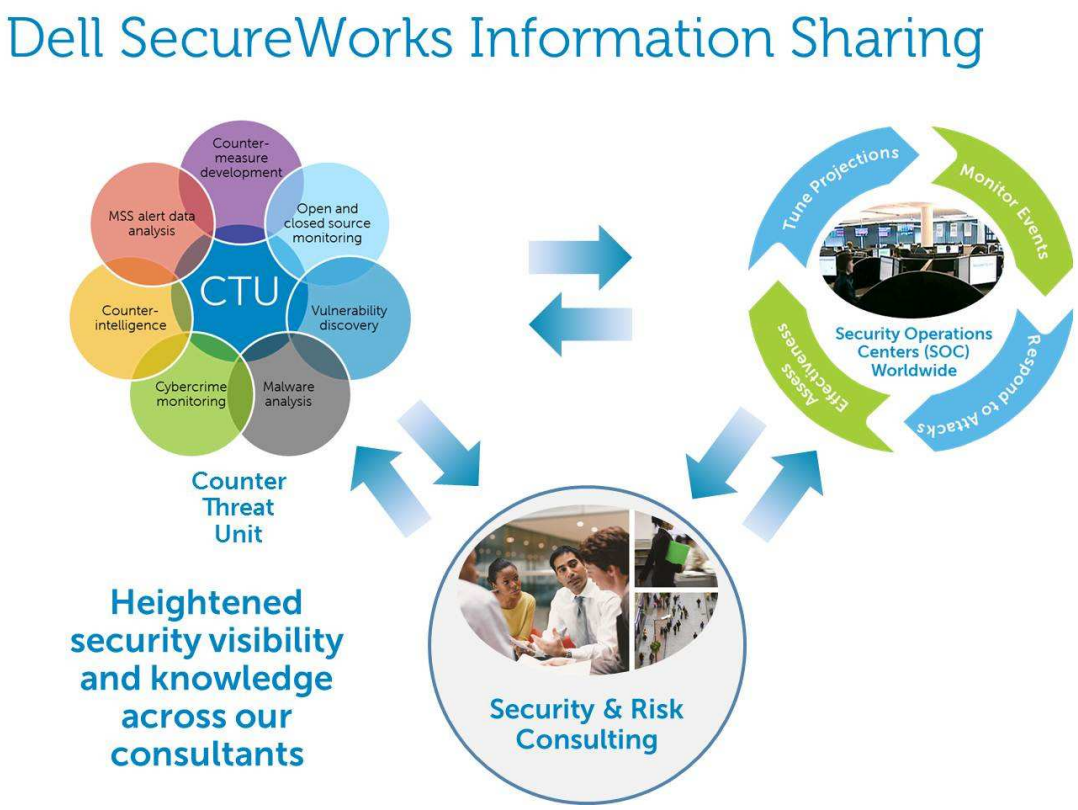
SRC サービスでは、お客様のセキュリティ、リスク、およびコンプライアンスのニーズに対応するため、さまざまなサービスポートフォリオをご用意しています。

Dell SecureWorks のセキュリティコンサルタントは、お客様の脆弱性の特定と実際のビジネスリスクの評価、PCI、HIPAA、GLBA、FISMA、ISO 27002 などのコンプライアンス義務のより効率的で効果的な遂行、お客様の環境に適したデバイスのセキュリティおよび管理プログラムの作成を支援します。また、お客様のチームでは対処が難しいセキュリティ侵害が発生した場合には、その復旧も支援します。

詳細については、次の Web サイトを参照してください。www.secureworks.com/consulting

情報の共有

Dell SecureWorks では、社内業務のあらゆる面で高度な相互コミュニケーションを促進しています。それにより、社内のセキュリティ研究者、アナリスト、セキュリティコンサルタントたちが、新しい脅威や悪者が用いる戦術、技法、手順（TTP）について、また、私たちがこの「無法地帯」で直面している事柄について、最新の情報を把握してより適切な準備と対応ができるように努めています。このような情報共有の企業文化は、当社のチームのセキュリティ能力を高め、当社のお客様の保護強化にも役立つと考えています。 さらに、セキュリティコンサルタントに対して、業務の過程で適切な情報をお客様と共有するよう働きかけています。



Dell SecureWorks の所在地

Dell SecureWorks の本社は、ジョージア州アトランタにあります。その他にも、イリノイ州シカゴ、サウスカロライナ州マートルビーチ、ロードアイランド州プロビデンスに加え、 さらに英国のロンドンとエジンバラにもオフィスがあります。 Dell SecureWorks のサービスは、米国内 5 ヶ所（ジョージア州アトランタ、イリノイ州シカゴ、サウスカロライナ州マートルビーチ、ロードアイランド州プロビデンス、テキサス州プラーノ）にある耐障害性に優れた SOC と、世界 2 ヶ所（英国のエジンバラ、インドのノイダ）にある SOC から提供されます。 Dell SecureWorks はこれらを拠点として、世界中のお客様にサービスを提供しています。

Dell SecureWorks の提携

Dell SecureWorks は、常に最新の脅威と脆弱性の状況に対応できるよう、世界各国の組織と公式および非公式の提携関係を結んでいます。 Dell SecureWorks は、次の組織に加盟しています。

- APWG（Anti-Phishing Working Group）
- CERT（Computer Emergency Response Team）
- CWFI（Cyber Warfare Forum Initiative）
- CyberCop Network

- FBI Citizens' Academy
- FIRST（Forum of Incident Response and Security Teams）
- FTC（連邦取引委員会）
- Imperva PartnerSphere Cloud Alliance Program
- ISA（Internet Security Alliance）
- ISC（Internet Systems Consortium）
- MAPP（Microsoft Active Protections Program）
- NCFTA（National Cyber-Forensics & Training Alliance）
- SANS（SysAdmin, Audit, Network, Security）
- 米国 司法省、国防総省、エネルギー省
- 米国 ECTF（Secret Service Electronic Crimes Task Force）
- ZDI（Zero Day Initiative）

Dell SecureWorks の Threat Intelligence White Paper 『猛威を振るうリスト型攻撃への対策はあるか？』をご覧いただき、誠にありがとうございます。

ホワイトペーパーの内容または当社サービスについてのお問い合わせは、こちらのフォームからご連絡ください。