News Release

2017 年 9 月 25 日

高精度な悪性サイト情報サービス
「Active Blacklist Threat Intelligence」の提供を開始

～日本で今起きているサイバー攻撃情報を活用した防御力の強化～

NTT コミュニケーションズ株式会社(以下：NTT Com)は、総合リスクマネジメントサービス WideAngle のマネージドセキュリティサービスにおいて、新メニュー「Active Blacklist Threat Intelligence」（アクティブ ブラックリスト スレット インテリジェンス）の提供を、2017 年 9 月 25 日より開始します。

本メニューでは、日本の企業や官公庁のお客さま向けに実施しているセキュリティ監視業務から収集した、国内で今起きているサイバー攻撃に使われている悪性サイト情報（以下：ブラックリスト）をリアルタイムに提供します。お客さまは、最新のブラックリストを自社のネットワーク機器へ自動的に取り込むことで、新しく発見された悪性サイトへの通信遮断を速やかに設定でき、自社が被害にあう前に対策を講ずることができます。

1.背景

昨今、攻撃者は従来のウイルス対策などの方法では検知できない未知のウイルスや悪性サイトを準備し、メールや Web サイト経由でサイバー攻撃を行い、機密情報を窃取します。これらの、新しいサイバー攻撃への対策としては、ウイルスなどの侵入を許した後の対応が中心であり、情報流出に発展するリスクが生じるため、緊急対応に追われるという状況がありました。また、サイバー攻撃は国や地域によって傾向が違う一方で、日本に特化したブラックリストが乏しく、日本を標的にしたサイバー攻撃への防御力にも課題がありました。

2.サービス概要

今回、NTT Com が提供する、高精度な悪性サイト情報サービス「Active Blacklist Threat Intelligence」（アクティブ ブラックリスト スレットインテリジェンス）では、国内の企業や官公庁に導入されているセキュリティ機器などで検知したサイバー攻撃情報をセキュリティオペレーションセンターの分析基盤に収集、独自の手法で悪性サイト情報を精査し、ブラックリスト化します。最新で精度の高いブラックリストをお客さまのネットワーク機器に自動取り組み可能な形式でリアルタイムに提供することにより、お客さまは新しく発見された悪性サイトとの通信を速やかに遮断できます。日本の企業や官公庁が狙われる可能性の高い新しいサイバー攻撃に対して予防型の対策を講ずることができ、自社の ICT 環境の防衛力を強化できます。

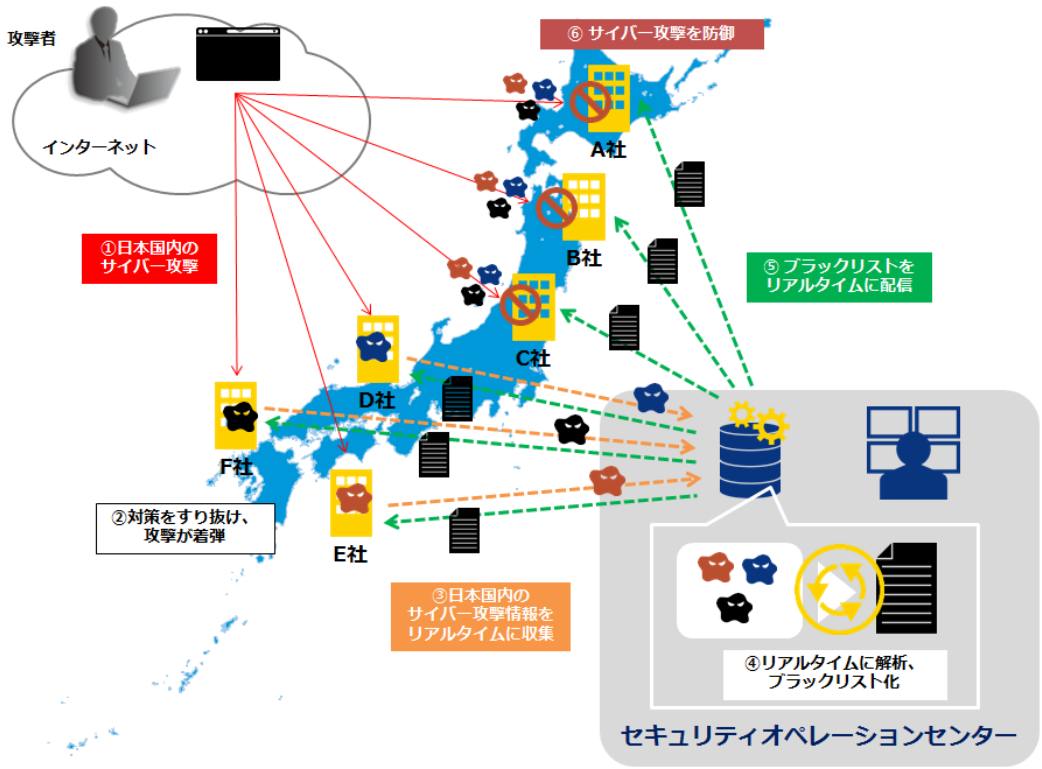
NTT コミュニケーションズ株式会社　広報室
NTT Communications Corporation　Public Relations Office
〒100-8019　東京都千代田区内幸町 1-1-6
1-1-6 Uchisaiwai-cho, Chiyoda-ku, Tokyo 100-8019, Japan
Tel (03)6700-4010 International +81 3 6700 4010

特長① 日本の企業や官公庁に最適なブラックリストをリアルタイムにアップデート

国内の企業や官公庁に設置しているセキュリティ機器などにて、今起きているサイバー攻撃の情報を検知し、リアルタイムにブラックリスト化するため、日本の企業や官公庁を狙ったサイバー攻撃への予防型の対策として有効です。

特長② 高精度なブラックリストがより多くの悪性サイトへの通信を遮断

NTT Com が提供する悪性サイト情報と市販製品を比較すると、5%～30%の情報が市販製品では検知できていない独自に精査し収集した情報です。さらに無害なサイト情報は除外することで、高精度なブラックリストを提供します。お客さまは、より多くの悪性サイトへの通信を遮断でき、誤判定による正常な通信の遮断を回避できます。



<今起きているサイバー攻撃情報をリアルタイムに共有するイメージ>

3. 提供範囲および提供開始日

日本および海外にて 2017 年 9 月 25 日より提供開始

※海外への提供は、日本国内にてご契約されているお客さまに限ります。

4. 提供価格（税別）

初期費用：0 円、月額費用 320,000 円

※Arcstar Universal One 経由でのブラックリスト配信となります。
※連携対象機器は、以下の通りです。詳細な機種名やバージョンは別途お問い合わせください。
・パロアルトネットワークス社[*1]の次世代ファイアウォール
・シマンテック社[*2]のプロキシサーバ
・マカフィー社[*3]のプロキシサーバ
・デジタルアーツ社[*4]の i-FILTER[*5]
・オープンソースのプロキシサーバ（Squid）

5.今後の予定

NTT Com は、すでに提供済のアドバイザリーサポート（2017 年 7 月 19 日サービス開始）に加えて、お客さま内の様々な組織で設置している ICT システムの情報をあらかじめデータベース化しておき、脆弱性情報が公開された際、該当するシステムを自動抽出し、システム管理者に随時通知する「脆弱性マネジメントプラットフォーム（仮称）」（開発中）など、お客さま CSIRT の運用を支援するスレットインテリジェンス提供を強化します。

6.その他

本サービスは、NTT Communications Forum 2017（2017 年 10 月 5 日～6 日、ザ・プリンス パークタワー東京）にてご紹介します。
http://www.ntt.com/business/go-event.html

*1 パロアルトネットワークス社は、米国に本社を持ち、サイバー攻撃から数多くの企業、行政機関、プロバイダを防御する次世代セキュリティのリーディングカンパニーです。先進的なセキュリティプラットフォームにより、お客さまのビジネス展開やデータを防御します。

*2 シマンテックコーポレーション（NASDAQ: SYMC）はサイバーセキュリティ業界をリードする世界的企業です。さまざまな場所に保管されている大切なデータを守るため、企業や政府機関、個人のお客様を支援しています。エンドポイントからクラウド、インフラまでを高度な攻撃から守るため、世界中の企業がシマンテックの戦略的統合ソリューションを選択しています。また、世界中で 5 千万以上の個人やご家庭が、自宅などで使用するデバイスそしてデジタルライフを守るために、ノートンと LifeLock 社の製品を使用しています。シマンテックのサイバーインテリジェンスネットワークは民間が運営するネットワークとしては世界最大規模を誇ります。このネットワークが、先進的な脅威をいち早く発見し、お客様を守ります。詳しくは https://www.symantec.com/ja/jp/ をご覧ください。

*3 マカフィー社は世界最大規模の独立系サイバーセキュリティ企業です。業界、製品、組織、そして個人の垣根を超えて共に力を合わせることで実現する、より安全な 世界を目指し、企業そして個人向けのセキュリティ ソリューションを提供しています。詳細は http://www.mcafee.com/jp/ をご覧ください。

*4 デジタルアーツ社は、フィルタリング技術を核に、製品の企画・開発・販売・サポートまでを一貫して行う情報セキュリティ企業です。「i-FILTER」は国産初の Web フィルタリングソフトとして業界最大級のデータベースと、世界 27 の国と地域で特許を取得したフィルタリングテクノロジー「ZBRAIN」により、業務中の閲覧が不適切な Web サイトを高い精度で遮断するほか、Web メールの利用や掲示板の書き込みなどといった、Web 経由の情報漏洩を防ぐとともに、その内容を記録・確認・保存することが可能なソリューションです。

*5 バージョン 9 での対応となります。