News Release

NTT Communications

2016 年 2 月 1 日

国内 ISP として初めて、
マルウェアによる情報漏洩から利用者を守る
「マルウェア不正通信ブロックサービス」の無料提供を開始

～お客さまによるお申し込みも設定も不要、不正通信を判別して自動ブロック～

NTT コミュニケーションズ（略称:NTT Com）は、インターネット接続サービス「OCN」の利用者など[*1]を対象に、2016 年 2 月 1 日より「マルウェア不正通信ブロックサービス」を無料で提供開始します。

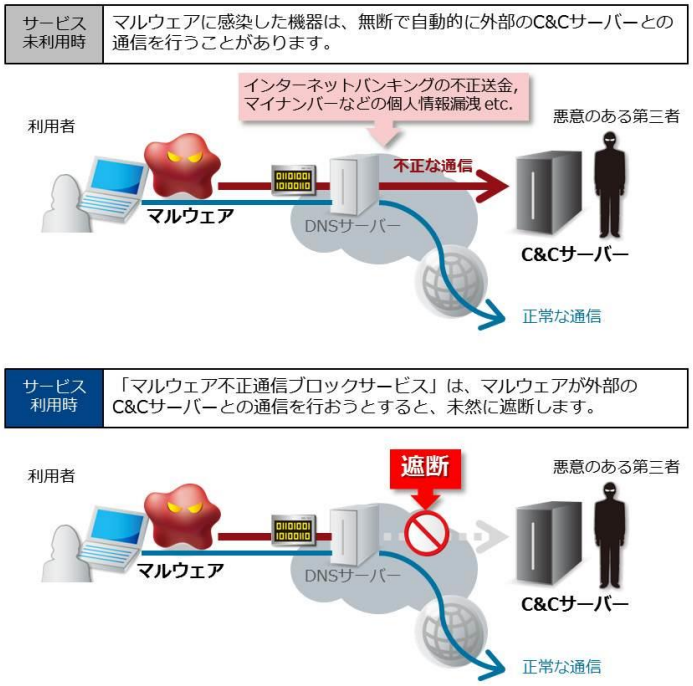
「マルウェア」とは、パソコンなどの機器に損害を与えることを目的に、悪意をもって作られたソフトウェアやコード類の総称です[*2]。マルウェアに感染したパソコンなどの機器は、悪意のある第三者が設置した外部の C&C サーバー[*3]と通信を行い、インターネットバンキングにおける不正送金や、マイナンバーやパスワードなどの個人情報漏洩といった被害をもたらす可能性があります。

本サービスは、マルウェアが外部の C&C サーバーと通信を行おうとすると、通信の内容(宛先情報)からそれを検知[*4]し、アクセスを遮断[*5]することでお客さまの被害を防ぐものです。

このように、通信の宛先情報に基づいて不正な通信をブロックするサービスを提供することは、国内の事業者として初めての試みです。

なお、お客さまによるお申し込みや設定は一切不要で、対象サービスをご利用のすべてのお客さまに対して無料で提供します。

<サービスイメージ図>



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

1. 背景

マルウェアによるセキュリティ上の被害は増加の一途をたどっています。例えば、マルウェアを悪用したサイバー犯罪の一つであるインターネットバンキングの不正送金について、国内の被害額は2015年上半期約15億円4,400万円と過去最悪の金額に達しています(警察庁調べ)。不正な通信の被害を避けるためには、利用者が個々にセキュリティ対策を行う必要がありますが、感染していても気づかないような挙動をするものも多く、対策を浸透させるのは容易ではありません。

これをうけNTT Comは、国内最大のインターネット接続サービス「OCN」をはじめとした対象サービスをご契約いただいているお客さまに、より安全・安心にインターネットをご利用いただくため、お客さまがお申し込みや設定をすることなく、また無料でご利用いただけるマルウェア対策サービスを提供します。このような取り組みは、国内ISPとして初めてです。

2. サービス詳細

マルウェアに感染したパソコンなどの機器が、悪意のある第三者が設置した外部のC&Cサーバーと、お客さまに被害をもたらす可能性がある不正な通信を行おうとする場合に、ネットワーク側で機械的・自動的に検知・遮断を行うことにより、未然に被害発生を防止するサービスです。

なお、本サービスにおいて検知・遮断のために参照する情報の範囲は、業界団体のガイドライン[*6]に準じています。また、参照するのは通信の宛先情報のみであり、お客さまが通信している情報の具体的な中身は参照しません。

お申し込み	不要
設定	不要 NTT Comのネットワークにて対策を行うため、お客さまによる設定は不要です。
利用料金	無料

本サービスによってマルウェアに感染していることが検知されたお客さまに対しては、NTT Comから通知を行います。

【個人のお客さま向けのサービス】

「OCNメール」にて通知。今後、会員サポートページにおいてもご確認を可能にする予定。

【企業のお客さま向けのサービス】

今後、ご契約者向けポータルサイトにてご確認を可能にする予定[*7]。

3. 提供開始日

2016年2月1日(月)

4. 「マルウェア不正通信ブロックサービス」の適用対象サービス

NTT Com の参照用 DNS サーバー[*8] を利用されているお客さまに対し自動適用されます。
主な対象サービスは以下の通りです。

【個人のお客さま向けのサービス】
「OCN 光」
「OCN 光 with フレッツ」
「OCN 光 「フレッツ」」
「OCN for ドコモ光」
「OCN ADSL」
「OCN ダイヤルアクセス」
「OCN モバイル ONE」

【企業のお客さま向けのサービス】
「OCN 光」
「OCN 光「フレッツ」」
「OCN 光サービス(F)」
「OCN ADSL アクセス」
「OCN モバイル ONE for Business」
「OCN モバイル スタンダード d」
「OCN バーチャルコネクトサービス」
「DNS サービス」
「Arcstar Universal One」インターネット接続オプション（GW 型/拠点型）
「Group-VPN」インターネット接続オプション

詳細な情報については、以下の Web サイトに掲載します。
【個人のお客さま向け】
「マルウェア不正通信ブロックサービス」
http://security.ocn.ne.jp/info/malware/

【企業のお客さま向け】
・企業向け OCN をご利用の方はこちら
「マルウェア不正通信ブロックサービス」
http://www.ocn.ne.jp/business/security/malware/
・「Arcstar Universal One」をご利用の方はこちら
「VPN サービス　Arcstar Universal One インターネット接続機能」
http://www.ntt.com/vpn/data/op_internet.html

*1: 対象サービスは「4. 「マルウェア不正通信ブロックサービス」の適用対象サービス」をご参照ください。
*2: 「ウイルス」や「ワーム」もマルウェアの一種です。
*3: Command and Control server のこと。悪意のある第三者が管理し、マルウェアに感染した機器などに遠隔指令を出すことで、セキュリティ上の被害をもたらす。
*4: 検知は機械的・自動的なものであり、NTT Com が利用者のアクセス先情報を恣意的に閲覧するものではありません。
*5: C&C サーバーへのアクセスを遮断します。その他の Web サイトの閲覧やメール利用等についてのアクセスは遮断しません。
*6:「インターネットの安定的な運用に関する協議会」が 2015 年 11 月 30 日に制定した「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン(第 4 版)」
*7: ご契約者向けポータルサイトにおけるご確認が可能になる以前の期間においては、お手数ですが NTT Com のカスタマサポートセンターもしくは営業担当者までお問い合わせください。
*8: 対象サービスをご利用であっても、OCN の DNS サーバーを参照しない設定にされているお客さまは本サービス適用の対象外となります。

○個人のお客さまからのお問い合わせ
https://support.ntt.com/ocn/inquiry/input/pid220000038y