2020 年 5 月 28 日

当社への不正アクセスによる情報流出の可能性について

NTT コミュニケーションズ(以下 NTT Com)は、当社の設備が攻撃者からの不正アクセスを受けたことを 5 月 7 日に検知し、一部の情報が外部に流出した可能性があること（以下 本事象）を 5 月 11 日に確認しました。

社内調査の結果、当社の一部サービス（「Biz ホスティング エンタープライズ（以下 BHE）」[※1]、「Enterprise Cloud1.0（以下 ECL1.0）オプションサービス」[※2]）に関する工事情報管理サーバーおよび、当社の社内業務で利用しているサーバー群（以下 社内サーバー群）において、一部の情報が外部に流出した可能性があることが判明しました。

現時点においては、踏み台となったサーバーの停止などの初動措置を終えておりますが、影響を受けた可能性があるお客さまには、順次連絡を差し上げております。あわせて、再発防止に向けた対応を実施しております。

また、個人のお客さまに関する情報は含まれておりません。

関係者の皆さまには、多大なご迷惑およびご心配をお掛けすることとなり、誠に申し訳ございません。心よりお詫び申し上げます。

1. 不正アクセス検知後の当社対応経緯

5 月 7 日にシステム主管部門が、当社 Active Directory[※3]（以下 AD）サーバーに対し、不正な遠隔操作を試みたログを検知し、同日に当該の遠隔操作の踏み台となった社内セグメントの AD 運用サーバー（以下 サーバーA）を緊急停止しました。その後、調査を開始し、サーバーA へのアクセス元の BHE/ECL1.0 サービス管理セグメントにある運用サーバー（以下 サーバーB）を緊急停止し、社内セグメントの AD サーバーから外部への通信を全て遮断しました。また、マルウエアと通信する外部サイトとの通信を遮断しました。

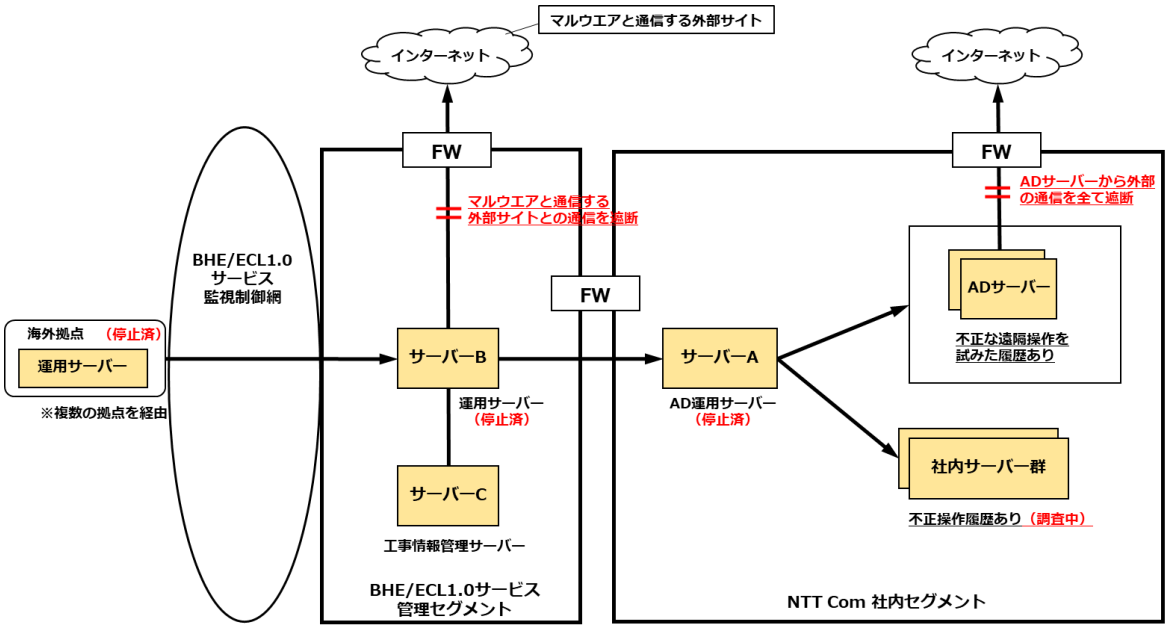
その後、社内サーバー群のアクセスログを解析した結果、不審なアクセスがあり一部の情報が流出した可能性があることが 5 月 11 日に判明しました。

また、今回の不正アクセスによる情報流出の恐れのあるルートは、サーバーB 経由であったため、サーバーB のフォレンジック調査[※4]を実施しました。その結果、BHE/ECL1.0 サービス管理セグメントの工事情報管理サーバー（以下 サーバーC）に不正アクセスされた形跡があることが判明しました。サーバーC のアクセスログを解析した結果、サーバーC に保管されていたファイルが流出した可能性があることが 5 月 13 日に判明しました。

なお、侵入経路を調査した結果、サーバーB がある BHE/ECL1.0 サービス管理セグメントに接続されている海外拠点（シンガポール）への攻撃および侵入をきっかけとして、日本のサーバーB に到達したことが判明しています。

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 東京都千代田区大手町 2-3-1 大手町プレイスウエストタワー
OTEMACHI PLACE WEST TOWER 2-3-1 Otemachi, Chiyoda-ku, Tokyo 100-8019, Japan
Tel (03)6700-4010 International +81 3 6700 4010

【発生事象概要図】



2. お客さまへの影響

現時点で、流出の可能性が判明している情報は以下のとおりです。本事象の影響を受けた可能性があるお客さまには、順次連絡を差し上げております。

・サービス管理セグメントの工事情報管理サーバー（サーバーC）から、サービスに関する工事情報などが流出した可能性があるお客さま数：　621 社

3. 今後の対応

BHE は、ご利用中のお客さまの環境を新サービスへ移行しておりました。このたび、移行に伴って撤去を控えていたサーバーB、海外の運用サーバー、ならびに一部の通信経路が、攻撃者の侵入経路として利用されたと考えております。

今後の対策として、新サービスへ移行中の設備に対しても、物理的な撤去が終わるまでは最新の攻撃手法に対応可能なセキュリティ対策を適用し、またお客さまが利用停止される都度、不要な通信経路の停止を徹底いたします。引き続き社内サーバー群の調査を行うとともに、再発防止のためのセキュリティ対策、監視体制のさらなる強化を進め、より一層のサービス品質の向上を図ってまいります。

新たにお知らせすべき内容が判明した場合、速やかに情報を開示してまいりますが、個別のお客さまに関する情報の開示は、機密保持の観点から差し控えさせていただきます。ご理解賜りますよう、よろしくお願い申し上げます。

※1：Biz ホスティング　エンタープライズとは、企業の ICT 基盤向けクラウドサービスで、一部のオプションサービスを除き、2018 年 3 月にサービス提供を終了しています。

※2：今回対象となる ECL　1.0 オプションサービスには、マネージドオプション、コロケーション接続、構築サポートなどが含まれます。

※3：Active Directory とは、Windows パソコンの機能やユーザ情報を管理するために、Windows Server に設けられた機能です。

※4：フォレンジック調査(デジタル・フォレンジック)とは、サイバー攻撃などの犯罪に対し、パソコンや通信機器など電子機器全般に残されたアクセスログなどの電子的証跡を調査し、証拠の保全を行ったり被害状況を分析したりする技術や手法です。