2020 年 7 月 2 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（第 2 報）

NTT コミュニケーションズ(以下 NTT Com)は、当社への不正アクセス事案について 5 月 28 日に公表（「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」、以下 第 1 報）しましたが、その後の調査結果についてお知らせいたします。

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しており、誠に申し訳ございません。あらためて心よりお詫び申し上げます。

1. BHE/ECL サービス管理セグメント経由での工事情報管理サーバーへの不正アクセス

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 Cloud（以下 ECL）オプションサービス」※2）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事象について、AD 運用サーバー（以下 サーバーA）、運用サーバー（以下、サーバーB）、サーバーC のフォレンジック調査※3 の結果、6 月 19 日に、第 1 報でお知らせした 621 社に加え、83 社に関する工事情報などが流出した可能性があることが判明しました。新たに判明したお客さまについては、当社より順次報告を行うなどの対応をしています。

なお、海外を含むクラウドサービスの提供やサービス品質に影響はございません。また、個人向けサービスのお客さまに関する情報は含まれておりません。

2. 社内ファイルサーバーへの不正アクセス

第 1 報でお知らせした社内サーバー群への不正操作履歴についてその後の調査を進めた結果、6 月 2 日に一部の社内ファイルが流出した可能性があることが判明しました。影響を受けたお客さまには、当社より報告を行いました。

また、上記の調査過程において、新たに VDI※4 サーバー経由で、一部の社内ファイルサーバーへの不正アクセスが確認され、社内ファイルが閲覧された可能性があることが 5 月 26 日に判明しました。

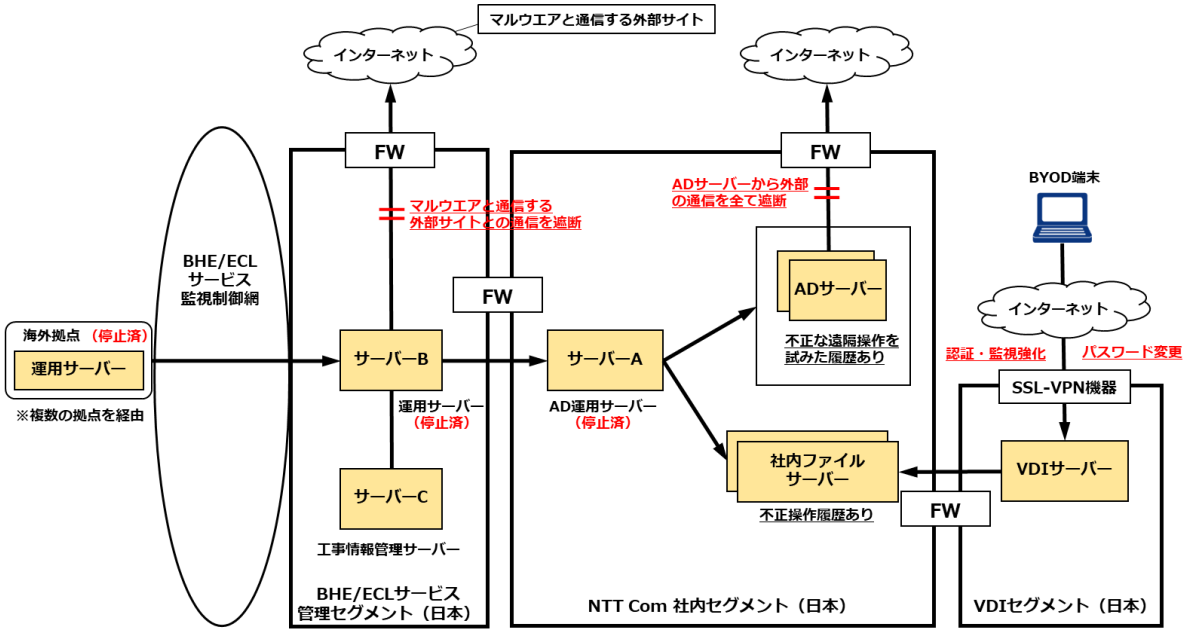
5 月 26 日にリモートアクセスを利用した BYOD※5 端末からの不正アクセスが判明したため、すべての BYOD 端末とシンクライアント専用端末のリモートアクセス環境を即時停止すると同時に、予防保全として全社員のパスワード変更を実施しました。さらに、リモートアクセス時の認証や監視の強化を実施しており、現在社員アカウントの不正利用は発生しておりません。

窃取された、正当なアカウントとパスワードが用いられたことから、攻撃者が閲覧した可能性のある情報の特定に時間を要しましたが、フォレンジック調査やアクセス履歴の分析の結果、影響を受けた可能性があるお客さまは 188 社であり、当社より順次報告を行っております。

なお、個人向けサービスのお客さまに関する情報は含まれておりません。

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】



3. 今後の対応

今回の事象を踏まえ、影響範囲の特定に時間を要したなりすまし攻撃への対策として、攻撃者の振る舞いを可視化する UEBA[※6] を導入し、侵入検知までの時間短縮を図るとともに、再発防止に向けてエンドポイントセキュリティを強化する EDR[※7] の導入や、ゼロトラスト[※8] を基本とするセキュリティ対策をさらに加速させます。

加えて、社内ファイルサーバーにおける情報管理ポリシーの徹底を図るとともに、セキュリティ対策の有効性を検証する Red Team[※9] を強化し、社内 IT/OT[※10] に対する TLPT[※11] を継続的に実施することで、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 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： 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。

※4： VDI（Virtual Desktop Infrastructure）とは、仮想デスクトップ基盤と呼ばれ、デスクトップ環境を仮想化させて、PC のデスクトップ環境をサーバー上に集約し、サーバー上で稼働させる仕組み。

※5： BYOD（Bring Your Own Device）とは、社員の私用端末を業務に使用することです。

※6： UEBA（User and Entity Behavior Analytics）とは、ユーザーの行動分析を行い、リスクを早期に検知する手法です。

※7： EDR（Endpoint Detection and Response）とは、ユーザーが利用する PC やサーバー（エンドポイント）における不審な挙動を検知し、迅速な対応を行うことです。

※8： ゼロトラストとは、社内は安全であるという前提の下に境界だけを守るのではなく、社内外すべてが信頼できないことを前提とした、情報セキュリティ対策の概念です。

※9： Red Team とは、企業や組織へセキュリティ攻撃を実行し、企業や組織が攻撃に適切に対応できるかの評価や改善提案を行う社内の独立したチームのことです。

※10： OT（Operational Technologies）とは、電力などのライフラインに関わる社会インフラを提供するシステムを最適に動かすための「制御・運用技術・設備」です。

※11： TLPT（Threat Led Penetration Test）とは、攻撃シナリオにもとづいて疑似的な攻撃を行うことで、セキュリティ対策状況を評価する手法です。