

at home



at home

アットホーム株式会社

不動産会社および一般消費者に、インターネットを通じて日々大量の不動産情報を提供するサービスのほか、不動産業務を支援するさまざまな事業を展開しています。

所在地：東京都大田区西六郷4-34-12
 設立：1967年12月
 資本金：1億円
 従業員数：1,342名（2015年7月末現在）
 URL：http://athome-inc.jp/

（取材日：2015年8月）

POINT

パスワードの定期的な変更で
 特権ID利用ユーザを限定

1

パスワードの貸出し申請を
 していないユーザの
 不正なサーバアクセスを防止

2

パスワード申請・承認プロセス
 の導入で
 ユーザのセキュリティ意識が向上

3

セキュリティ強化と業務効率
 ハードルを1つ1つクリアしながら
 段階的に対策を実施

「特権ID管理は、社員の意識向上にもつながった」

不動産情報サービス企業のアットホーム株式会社では、情報セキュリティ強化の一環として、それまで社内各所で行われていた特権IDの固定パスワードによる利用の廃止を目指していました。これを実現するために同社が導入したのが、サーバの「パスワード貸出し」の仕組みを可能にする「CA Shared Account Manager (SAM)」でした。

課題

対策

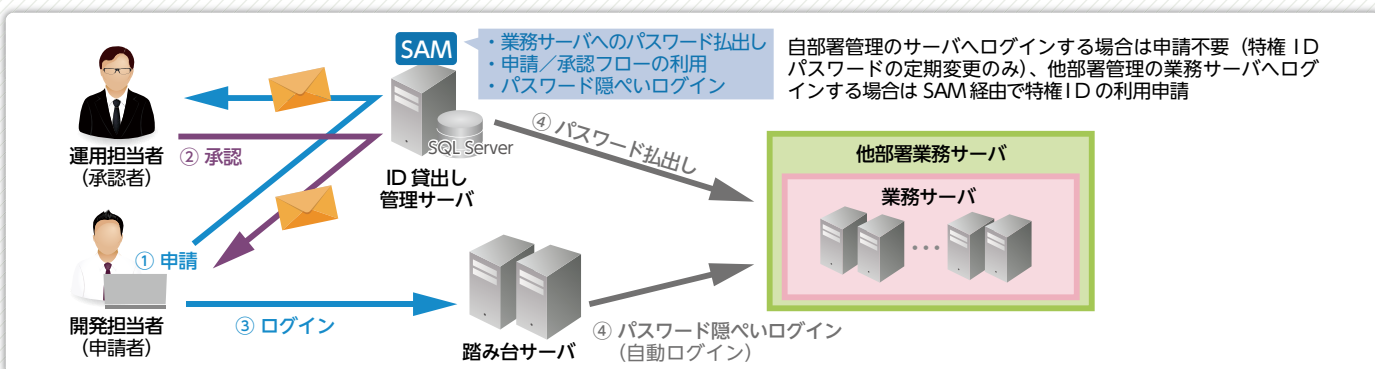
効果

- 固定パスワードのまま特権IDを共有することで潜在的な情報漏洩リスクが存在した
- 接続先のサーバを間違えて、意図しないサーバへ特権IDでログインし操作してしまうことがあった
- 社会インフラの一端を担うシステムのデータベースにはベンダーサポートが必須だった

- 特権IDのパスワード貸出しが可能なSAMを導入
- 特権IDのパスワードを定期的に変更することで、不正なサーバアクセスを防止
- 固定パスワードを利用した特権IDを前提に動作するプログラム用に、最小限の権限のみを付与したアカウントを別途作成

- 本番サーバへの不正なアクセスによる情報漏洩や事故のリスクを大幅低減
- 特権IDを利用した意図しないサーバへのログインを未然に防止できるようになった
- パスワード申請・貸出しプロセスの導入でユーザのセキュリティ意識が向上

システム概要



CA Shared Account Manager

膨大な量の情報を守るための 段階的なセキュリティ対策強化

不動産総合情報サイト「アットホーム」でおなじみのアットホーム株式会社（以下、アットホーム）。一般消費者向けサービスのほか、不動産会社向けの情報提供サービスや業務支援サービスなど、幅広い不動産ビジネスを展開しています。



宮之原 氏

同社が取り扱う物件情報の数は、不動産会社の間で流通するもので約830万件、一般消費者向けでは約1,930万件にも上ります。アットホーム情報システム部 情報管理室 管理運用グループ インフラ設計チーム チーム長 宮之原秀雄氏は、

これだけ膨大な量の情報を扱うに当たり、社外への情報漏洩を防ぐためのセキュリティ対策にかなり力を入れていると言います。

宮之原氏 標的型攻撃や内部犯行など、様々なセキュリティ脅威からお客様の情報や内部情報を守るために、経営陣をはじめ全社一丸となってセキュリティ対策の強化に取り組んでいます。ただし、セキュリティ対策の強化は、ときにユーザの生産性を落とすこともあります。そのため、一気にすべての対策を導入するのではなく、段階的に対策強化を進めています。

例えば、ユーザが本番サーバへアクセスする際に必ず特定のサーバを経由させて、ユーザが行ったすべての操作を記録する「踏み台サーバ」の導入もその一環でした。これにより、万が一インシデントが発生した際にその原因をさかのぼって調査できるとともに、ユーザに対する不正アクセスのけん制効果も期待できます。しかしこれはあくまでも事故が起こってしまった後の事後的な対策に過ぎず、次の段階としては不正アクセスやうっかりミスを事前に防ぐための対策が求められていました。

特権IDの定期的なパスワード変更 により不正アクセスを防止

アットホーム 情報システム部 情報管理室 管理運用グループ インフラ設計チーム 本杉直人氏によれば、本番サーバへのアクセス制御を見直すに当たって、差し迫った重要な課題は「特権IDの管理」にあったと言います。

本杉氏 本番サーバにログインして行われる作業のほとんどで、“administrator”や“root”といった管理者

権限を持つ特権IDが使われていました。しかもずっと同じパスワードを使っていたので、特権IDによる不正アクセスがセキュリティ事故を引き起こすリスクを長らく抱えていました。

そこでまずは、このリスクを回避するための対策を導入することになりました。そのための具体的なソリューションや製品を模索する中で、やがて有力候補として浮上ったのが、アシストの提案したセキュリティ製品「CA Shared Account Manager (SAM)」でした。

SAMは、本番サーバに代わってログインパスワードの管理と発行を行い、ユーザに対して「パスワードの貸出し」を行う製品です。ユーザは本番サーバにアクセスするには、必ず事前にSAMにアクセスして、ログインパスワードを申請・取得する必要があります。アクセスの際には、管理者による申請承認フローを組み込むこともでき、また毎回パスワードを自動的に変更することもできます。

こうした機能を使えば、特権IDの固定パスワードを廃止し、定期的にパスワードを変更してユーザに個別発行する運用が可能となります。これにより、特権IDによる本番サーバに対する不正アクセスは劇的に減るはずですが、アットホームにとっては、まさに打って付けの製品だったので。

本番サーバへの不用意なアクセスが招く セキュリティリスクを排除



當間 氏

アットホームは早速、アシストの協力のもとSAMの検証作業を行い、同社のニーズに合う製品であることを確認しました。正式にSAMの導入を決めた同社は、続いて本番導入へと作業を進めましたが、同社 情報システム部 情報管理室 管理運用グループ インフラ設計チーム 當間健太氏によると一部のユーザからは懸念の声も上がったと言います。

當間氏 システム運用管理ツールのジョブや、バッチ処理プログラムの中には、固定パスワードを使って特権IDとしてサーバにログインすることを前提に作られたものがありました。SAMを導入してパスワードを定期的に変更すると、これらが正常に動作しなくなるかもしれません。

こうしたリスクを回避するために、運用管理タスクやバッチ処理で必要な権限のみを付与した専用アカウントを、特権IDとは別に新たに作成することにし

ました。またSAMの適用も、すべてのサーバに対して一度に行うのではなく、システムの更改やサーバ新規導入時のシステム見直し作業に合わせて段階的に行うことにしました。これらの工夫で現場の導入ハードルを下げたおかげで、2015年5月から本番環境で無事SAMの運用をスタートさせることができました。

これにより、同社がもともと抱えていた特権IDの固定パスワードにまつわるセキュリティリスクは、ほぼ一掃されたと本杉氏は言います。

本杉氏 SAMの仕組み

を導入したことで、セキュリティリスクを一掃するとともに、これまで潜在的に抱えていた『間違った本番サーバへのアクセス』のリスクもなくなりました。また、SAMIによるパスワード申請のプロセスを導入したことで、軽い気持ちで不用意に本番サーバへアクセスするユーザもかなり減りました。セキュリティレベルは大幅に向上したと実感しています。



本杉 氏

今後は本番サーバログイン後の アクセス制御の仕組みを検討

アットホームでは現在約50台のサーバを対象に、SAMによるパスワード貸出しの仕組みを運用しています。社内にはまだ、SAMを適用していないサーバも存在するため、今後はこれらのサーバの更改タイミングを見計らって、順次SAMの適用範囲を広げていく予定だと言います。

また、早くもSAM導入に続く次のセキュリティ対策の検討も進められています。SAMはシステムに対するログインの制御を可能にしましたが、次はサーバにログインした後のアカウントの挙動を制御する「アクセス制御」の仕組みを、SAMの同系列製品「CA Privileged Identity Manager (PIM)」を使って実現できないか、検討を続けていると言います。

宮之原氏は、こうした計画を実現する上でも、今後ともアシストの支援には大いに期待していると述べます。

宮之原氏 これまでアシストさんには、製品開発元ベンダーとの間に入ってもらって様々な調整を行っていただきました。今後弊社がさらにセキュリティ対策を進化させていく上でも、是非そうした役割を引き続き期待したいと思います。

お問い合わせは **株式会社アシスト**

URL <http://www.ashisuto.co.jp/product/ac/> E-Mail ssj_info@ashisuto.co.jp

東 京 〒102-8109 東京都千代田区九段北4-2-1 市ヶ谷東急ビル TEL: 03-5276-5862 大 阪 〒530-0011 大阪市北区大深町4-20 グランフロント大阪タワーA 13F TEL: 06-6373-7113
札 幌 〒060-0003 札幌市中央区北3条西4-1-1 日本生命札幌ビル 13F TEL: 011-281-1161 広 島 〒730-0011 広島市中区基町12-3 COI広島紙屋町ビル 3F TEL: 050-3816-0974
仙 台 〒980-0013 仙台市青葉区花京院1-1-20 花京院スクエア 19F TEL: 050-3816-0970 福 岡 〒812-0013 福岡市博多区博多駅東2-6-1 九動筑紫通ビル 9F TEL: 092-481-7156
名古屋 〒460-0003 名古屋市中区錦1-11-11 名古屋インターシティ 4F TEL: 052-232-8211 沖 縄 〒900-0014 那覇市松尾1-10-24 ホークシティ那覇ビル4F TEL: 050-3816-0976
金 沢 〒920-0853 金沢市本町2-15-1 ボルテ金沢 8F TEL: 050-3816-0972

※本事例は取材時の内容に基づくものです。※製品内容は、予告なく変更される場合があります。※記載されている会社名、製品名は、各社の商標または登録商標です。 AX-025-OCT15