セキュリティへの取り組み（1/2）

運営のプロとして、ゲームをセキュリティ脅威から守り検知、復旧まで網羅的な対策に取り組んでいます

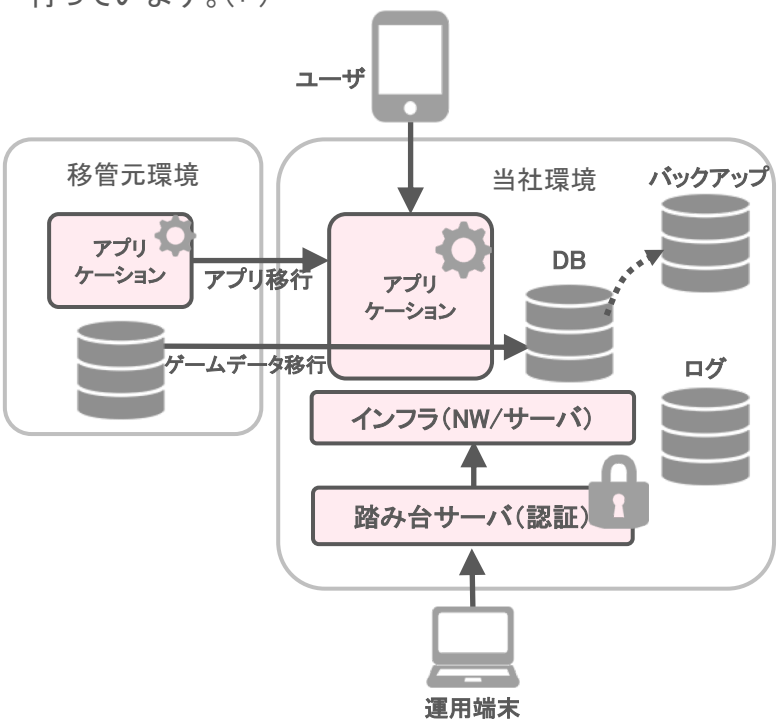
ゲーム運営のパターンとセキュリティ対策

当社の主力事業であるゲーム運営には、システム稼働環境に応じて2種類のパターンがあり、各パターンに対してセキュリティ規格に基づいた対策に取り組んでいます。(*1)

- システムを当社環境に移行し、システム運用含めてゲーム運営を行う
- システムの移行が難しいことから、開発元環境上のシステムに対してゲーム運営を行う

セキュリティ対策詳細（当社環境へシステムを移行する場合）

当社環境に移行して運営するゲームシステムに対して、セキュリティインシデントからの防御、インシデント発生時の検知、対応、復旧を行うために、以下に代表されるセキュリティ対策を行っています。(*2)



ポリシー/ドキュメント整備

- セキュリティポリシーを定め社内外に周知しています(*3)
- インシデント対応手順を定め、他社インシデント状況なども踏まえて定期的に見直しています

安全なネットワークの構築

- 外部からのアクセスは、ユーザからのゲーム利用アクセス、管理者からの管理アクセス等、必要最低限の通信のみを許可しています

強固なアクセス制御

- 管理アクセスは担当するゲームタイトルのみに制限し、必ず踏み台サーバを経由して認証を行っています
- アカウントは個人ごとに作成し多要素認証を行っています
- 移行前から利用しているシステムのアカウントを無効化しています

脆弱性への対応

- サーバと端末にウィルス対策ソフトを導入しています
- 移行したアプリケーションに対して、コードレビューや脆弱性診断を行い脆弱性に対処しています

ネットワークの監視

- ログやセキュリティイベントを取得し監視しています
- システムのログを取得しセキュリティ事故発生時に証跡として利用します

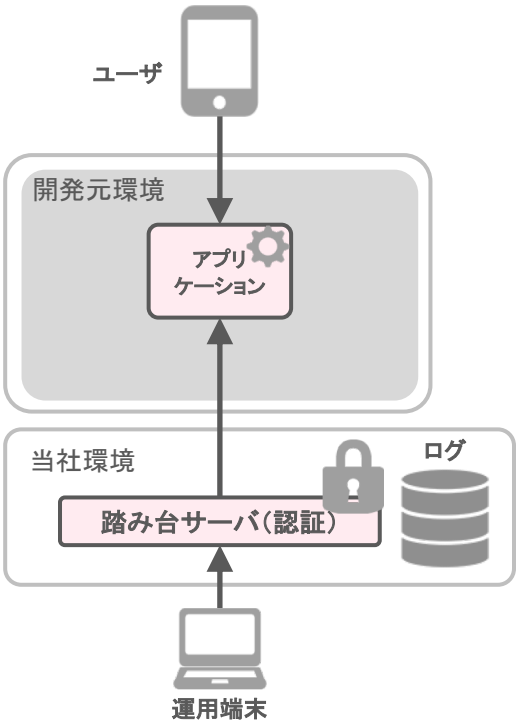
データ保護

- データの定期的なバックアップを取得して別ストレージ上に保存し、アクセス権限を分けて管理しています
- ソースコードはバージョン管理を行い、ゲーム稼働環境とは独立した環境に保存しています

セキュリティへの取り組み（2/2）

セキュリティ対策詳細（開発元環境のシステムを運営する場合）

開発元環境へのアクセスや当社が管理する運用端末など、当社にてコントロール可能な対象に関して、以下に代表されるセキュリティ対策を行っています。(*4)



ポリシー/ドキュメント整備

- セキュリティポリシーを定め社内外に周知しています(*3)
- インシデント発生時における、当社管理環境に関する対応手順を定めています

強固なアクセス制御

- 開発元環境へのアクセス毎に、専用の踏み台サーバを設けています
- 運用端末の送信元アドレスと、利用アカウントを必要最低限に制限しています
- 運用で利用するアカウントは個人ごとに作成し、多要素認証を行っています

脆弱性への対応

- 当社が運営するアプリケーションに対して、コードレビューを行い脆弱性に対処しています
- 踏み台サーバと運用端末にウィルス対策ソフトを導入し最新状態に更新しています

ネットワークの監視

- 踏み台サーバのアクセスログを取得しセキュリティ事故発生時に証跡として利用します

参考

(*1) システムの実装・運用寄りのセキュリティ規格をベースとした「セキュリティガイドライン」を社内で定め、ガイドライン内容に沿った対策を行っています。

(*2) 本資料に記載したセキュリティ対策内容は各構成の代表的な対策の一例であり、環境に応じて変更になる可能性があります。

(*3) セキュリティポリシーでは、本書に記載されている「事業内容に対する具体的なセキュリティ対策」のみならず、以下のような、企業全体としてのセキュリティへの取り組み概要を記載しています。

- グリー株式会社と協力した社内体制の整備
- 定期的な従業員の教育
- 外部委託先のセキュリティ対策管理
- 継続的なポリシーの改善　等

(*4) 当社の責任範囲は、運用端末から当社環境内の踏み台サーバまでのシステム及びネットワーク、また開発元環境上にて当社が運営を行うゲームアプリケーションを想定しています。本責任範囲は、環境に応じて変更になる可能性があります。