セキュリティインシデント報告・対応規程

1. 趣旨

2. 対象者

3. 対象

4. 遵守事項

5. 運用確認事項

6. 平時の準備

7. 対応フロー

    7-1. 事象の検知

    7-2. 初動対応・応急処置

    7-3. 調査・封じ込め

    7-4. 報告・公表

    7-5. 抑制措置・復旧

    7-6. インシデントタイプ別の対応手順

8. インシデントからの学習

9. 改訂

1. 趣旨

本規程は、セキュリティインシデントが発生した場合及びセキュリティインシデントの発生と疑われる場合、適切な連絡経路を通じて極力速やかに報告し、定められた手順に従って迅速に対応し、環境の復旧が速やかになされることと、発生した事態から問題点や改善点などに対する学習を行い、継続的な再発防止が行われることを目的とする。

当社におけるセキュリティインシデントとは次のような事態を指す。

（１）セキュリティに対する侵害例 データベースへのハッキングによる不正アクセスでの情報漏洩・データ改ざん。従業員による情報漏洩。ウイルス・マルウエア感染、DoS攻撃、記録媒体等の紛失 等

（２）システム・ネットワークの故障・損壊

例 電源異常、熱暴走、天災による機器損壊 等

2. 対象者

当社の全従業員。

3. 対象

当社の従業員が業務遂行のため利用するすべてのソフトウェア、ハードウェア。

4. 遵守事項

システム管理者又は EC 管理者の同意・承認の元、未然に防げなかった事態が発生した際に、事態の可及的速やかな収拾と被害や影響範囲を最小にするために、平時からの取

組と組織・役割の責任の明確化・伝達方法・事態の評価と対応及び再発防止を含む学習についての取り組みを明確にする。

5. 運用確認事項

インシデント発生時における対応方法について、セキュリティインシデントを検知して処理するための計画や Runbook を作成し、あらかじめ報告及び復旧等に向けた手順を作成しているか定期的に確認する。主要なインフラストラクチャまたはシステムの変更があった場合もこれに該当する。

また、インシデント対応実施後に再発防止策、対応手順の改善が行われているか、確認する。

（１）定期的（年１回）にリスクの評価と管理プロセス内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

これには、既知のリスクを追跡するための潜在的な脅威や脆弱性、ならびに可能性や影響の評価が含まれるが、これらに限定しない。

対応計画の変更を求める者は、システム管理者又は EC 管理者に申請しなければならない。システム管理者又は EC 管理者は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

（２）定期的（半年に１回）、または主要なインフラストラクチャまたはシステムの変更後は、計画を確認し検証をおこなう。

主要なインフラストラクチャまたはシステムの変更とは、下記の事を指す。

・システム変更：ソフトウェアのアップグレードやパッチ適用、ハードウェアの変更、新しいシステムの導入、既存システムの大幅な改良など

・コントロール：システムやプロセスの管理・監視方法に変更がある場合など

・運用環境：サーバーの配置、ネットワーク構成、データセンターの立地変更など、システムが動作する環境の変更など

・リスクレベル：新たな脅威の出現、既知のリスクの増大など

・サプライチェーン：製品やサービスの供給元、製造元などの変更が行われた場合など

・6. 平時の準備

セキュリティインシデントが発生した場合、あるいは発生が疑われる場合は速やかにセキュリティインシデントの分析、封じ込め、原因の根絶、復旧が可能となるよう以下の準備作業を行い、関係者に周知・徹底する。

（１）想定するセキュリティインシデントの具体的な対応手順を第 7 項に策定する。対応手順には、次の事項を含む。

- 組織の内部及び外部機関との協力関係の明記
- 組織の内外への必要な連絡先の明記

（２）システム管理者又は EC 管理者は、策定した対応手順でセキュリティインシデントに対応可能となるよう、定期的に訓練を行い、併せて対応手順に問題がないか確認を行い、対応手順に問題があれば是正する。

（３）システム管理者又は EC 管理者は、各システムの復旧優先度を決定しなければならない。復旧優先度の決定は、対象システムにおいて運用される業務の停止許容時間を観点において行う。

7. 対応フロー

セキュリティインシデントが発生した際の基本的な対応フローは第 7-1 項から順に、第 7-5 項までを行う。

セキュリティインシデントの種類・規模によっては省略、順序変更を行う。

なお、セキュリティインシデントに関する情報は、システム管理者又は EC 管理者のもと、一元的に収集、管理する。

7-1. 事象の検知

事象の検知、発見は以下にて判断する。

- 情報漏洩の兆候となる不正アクセスが起きた場合

・　　具体的な情報漏洩の事実を確認した場合

・　　UTM 管理のセキュリティ会社からの情報提供があった場合

・　　その他外部からの情報提供があった場合

・　　システムのアラートや異常検知が報告された場合

・　　システムが通常通り動作しない場合

・　　機器トラブルが起きた場合

事象の検知した場合速やかにシステム管理者又は EC 管理者に報告する。連絡先は以下の通り。

・　　代表取締役社長　渡部 正行

TEL:0852-52-6688 Mail: tokyoshoes@tkshoes.co.jp

・　　EC 管理者： 伊藤 佳彦

TEL: 080-7416-7024　Mail: y.ito@tkshoes.co.jp

・　　システム管理者：北垣 剛志

TEL: 070-131-7229　Mail: tkita@tkshoes.co.jp

7-2. 初動対応・応急処置

システム管理者又は EC 管理者は報告を受けたらすぐにインシデント対応体制を取る。システムの被害状況、稼働状況の確認を行い、異常があれば下記優先度にて復旧にあたること。

（１）優先度高：サーバー、顧客情報及び物流に関連する管理システム

（２）優先度中：（１）以外の管理システム

（３）優先度低：管理システム以外のハードウェア、ソフトウェア

情報が未だ外部からアクセスできる状態であれば情報の隔離とネットワークの遮断、サービスの停止などを行い、被害の拡大や二次被害を防ぐこと。不正アクセスや不正プログラムなどの可能性がある場合は、あとから侵入ルートなどの原因調査を行う観点で、システム上の証跡を消さないようにする。発見が外部からの情報提供によるものだった場合は、相手の連絡先やどこからどのような情報を得たのか聞き取りを行う。取引先情報が含まれる場合には取引先に報告し、取引先の意向に沿った対応を行う。

7-3. 調査・封じ込め

セキュリティインシデントの情報の整理。事実関係を裏付ける情報や証拠の確保。特定したセキュリティインシデントの原因に基づく対応を取る。被害の拡散を防止し、被害箇所の原因の根絶、防御、修復を行う。

- セキュリティインシデントの発生状況及び対応状況に関する情報
- 顧客及び取引先等利害関係者の影響等に関する情報
- 自社のビジネス活動再開に関する情報

各セキュリティインシデントを調査し、第 8 項に基づき再発防止の為の文書を作成する。

7-4. 報告・公表

情報漏洩が起こった際は、代表者または管理者が関係各所への報告を行う。

個人情報が漏洩した場合、またその恐れがある場合は、個人情報保護法に準拠した対応を行い、関係各所への報告を行う。

連絡先は以下の通り。

- 個人情報保護委員会 TEL : 03-6457-9685
- 楽天 : 050-5533-1899
- Yahoo : (Mail)https://support.yahoo-net.jp/form/s/PccDeveloper
- Amazon (24 時間以内)：(Mail)3p-security@amazon.com
- 影響のある顧客個人 : 発生時に分かりうる連絡先
- 影響のある取引先 : 取引先の通常の連絡先
- ホームページにて公表 : https://www.shoes-i.net/

機器トラブルや天災によりサービスが一時停止する場合は必要な連絡先にのみ事象を報告。被害が当社で完結している場合は、関係各所への報告・公表は省略可能。

Amazon が関係するセキュリティインシデントについては、Amazon からの書面による依頼がない限り、Amazon に代わって規制当局や購入者と対話することはできないものとする。

また 7-3 項にて作成した文書については、証拠や記録の保全を維持し関係各所の要求に応じて提出を行う。

代表者または管理者は、現地で適用される法律に従って関連する政府または規制機関に通知することについては、開発者が全責任を負うこととする。

7-5. 抑制措置・復旧

拡大防止と復旧のための措置を取る。個人情報漏洩の場合には専用の相談窓口を設けてなんらかの被害がある場合にはその内容を聞き取り、対応を行うこと。再発防止に向けた取組みが完了した管理システム・ハードウェア・ソフトウェア・サービスから復旧させ、通常業務へ戻る。

7-6. インシデントタイプ別の対応手順

（1）データベースのハッキング

a. 事象の検知: データベースの不正アクセスや異常なシステムの動作が検出された際には、システム管理者又は EC 管理者に報告する。

b. 初動対応・応急処置: 代表者または管理者は、検知した不正アクセスに対し、直ちにインシデント対応体制を敷き、被害の詳細と現在の稼働状況を確認する。必要に応じて、データベースのアクセスを一時的に制限または停止する。

c. 調査・封じ込め: ハッキングがどのように行われたか調査し、その脆弱性を特定し、対策を実施する。被害箇所の修復及び防御強化を行う。

d. 報告・公表: 法的義務に基づき、影響を受けた個人や組織、関連機関にハッキングの発生を報告する。AWS を使用したシステムやサービスがわずかでも関係している可能性がある場合は、24 時間以内にメールにて通知を行う。再発防止策を文書化し、必要に応じて公開する。

e. 抑制措置・復旧: ハッキングの影響を受けたデータベースの運用を一時的に停止し、修復とセキュリティ対策の強化を行う。その後、安全が確認されたら、データベースを再稼働する。

（2）不正アクセス

a. 事象の検知: 不正アクセスが確認された場合、その情報をシステム管理者又は EC 管理者に報告する。

b. 初動対応・応急処置: 不正アクセスのソースを特定し、そのソースからのアクセスを遮断する。影響を受けたアカウントのパスワードを変更するなどの応急処置を行う。

c. 調査・封じ込め: 不正アクセスの原因を調査し、それに基づいた対策を実施する。再発防止策を文書化する。

d. 報告・公表: 不正アクセスの報告を関連機関や影響を受けた個人に行う。必要に応じて、公表も行う。また AWS を使用したシステムやサービスがわずかでも関係している可能性がある場合は、24 時間以内にメールにて通知を行う。

e. 抑制措置・復旧: セキュリティ対策の強化と修復を行った後、安全を確認したうえで、通常の業務に戻るかどうかを判断する。

（3）データ漏洩

a. 事象の検知: データ漏洩が確認された場合、その事実をシステム管理者又は EC 管理者に報告する。

b. 初動対応・応急処置: 漏洩した情報の種類を特定し、可能な限り漏洩したデータの隔離を試みる。システムのアクセスを制限または一時的に停止し、二次被害を防ぐ。

c. 調査・封じ込め: データ漏洩の原因を調査し、その漏洩経路を封じ込む。被害箇所の修復及び再発防止策を文書化する。

d. 報告・公表: 法的義務に基づき、影響を受けた個人や組織、関連機関にデータ漏洩の発生を報告する。AWS を使用したシステムやサービスがわずかでも関係している可能性がある場合は、24 時間以内にメールにて通知を行う。再発防止策を文書化し、必要に応じて公開する。

e. 抑制措置・復旧: データ漏洩の影響を受けたシステムの運用を一時的に停止し、修復とセキュリティ対策の強化を行う。その後、安全が確認されたら、システムを再稼働する。

8. インシデントからの学習

セキュリティインシデントの対応後、同様のセキュリティインシデントの再発防止、および対応手順の不備等について改善を行う。

（１）システム管理者又は EC 管理者は、セキュリティインシデントへの対応が完了した後、発生したインシデントの説明、修復アクション、関連する修正プロセス、システムコントロールを文書化し記録しなければならない。

（２）システム管理者又は EC 管理者は、調査結果をもとに再発防止計画を作成しなければならない。また対応手順の不備、または良かった点を整理し、対応手順を改善する項目も記載する。

再発防止計画作成時には、技術的側面と組織的側面の両方に留意する。

（３）再発防止計画は、すべての従業員に周知され、適切に実施されなければならない。

（４）システム管理者又は EC 管理者は、一連の記録を保管、管理しなければならない。