LINEを利用するにあたってのリスク管理について

（1）LINEのセキュリティー

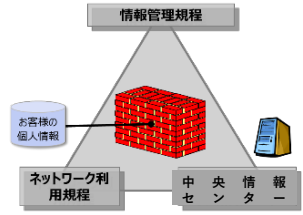
弊社は業務上のリスクを想定し、リスクの発生を抑制するための対策、体制を講じます。
また万が一リスクが顕在化し、具体的な危機が発生した場合の対処方法を以下に定めます。

①電子決済サービスの不正利用、利用者情報の流出

WEBアプリケーションの利用において、各利用者の情報を不正なアクセスから防ぐため以下のような対策を取っております。

＊電子決済はオンタイムで店舗管理画面、事務局管理画面で、確認可能です。同一人物の同時刻複数決済など不正が疑われる決済があれば事務局より店舗へ事実確認、不正となれば顧客決済凍結し本人連絡し返済を求めます。GTEでも同じ方法で管理運行し摘発しています。

	保護要件	
1	なりすまし防止	・IDとパスワード認証による不正ページアクセス防止 ・cookieとサーバサイドセッションによる不正ページアクセス防止
2	盗聴防止	・TLS通信による暗号化
3	改ざん防止	・Webアプリケーションに対する書込み権限の限定、及びFirewallによる制御、 公開鍵認証を利用したコンテンツ更新
4	暗号化通信	・TLS通信による暗号化
5	通信プロトコル制御	・Firewallにより制御
6	通信量制御	・ロードバランサにより制御
7	ハッキング対策	・Web Application Firewall (WAF) やFirewallにより防衛
8	ウィルス対策	・コンテナによる差分検証・環境の定期初期化により対処



※リアルタイムで通信を不正アクセス防御システムで監視し、緊急性のレベルにより、即時・日次・月次で対応を検討します。
また、FireWallログについては３年間保管しております。
※コンピュータ緊急対応センター(JPCERT/CC）、情報処理振興事業協会セキュリティセンター（IPA/ISEC） の情報より対応を行っております。

（2）リスク管理

② 書類の誤操作や電子メールの誤送信等による個人情報の漏えい

PC等のセキュリティ管理及び不正アクセス管理を徹底します。また、電子メールの送信の際は最新の注意を払い、第三者同士への送信には、BCC欄を利用します。

③ 書類の不適切管理による紛失

個人情報を含め書類は事務局内にて施錠管理とし、社外への持出を禁止します。
個人情報管理簿により、保有している情報を一元管理します。

④ 機器の操作誤り等による電子データの棄損や処理誤り

重要情報を含む機器の扱いは部門長のみ権限とし、二重チェックによる事故の防止に努めます。

⑤ 弊社の情報管理について

弊社では、「情報管理規程」「ネットワーク利用規程」を遵守し、個人情報保護法および弊社個人情報保護方針に基づく「個人情報の取扱いについて」に従った取扱いを行っております。個人情報を入手した目的や条件以外での一切の使用をいたしません。また、「情報センター」は24時間体制の専門要員と高度なネットワークセキュリティを融合させたシステムビルにて万全な管理を行っております。社員教育としても、定期的な研修（Eラーニング含む）にてルールの徹底を継続して計っています。
万が一、リスクが発生した場合は、社内規定に則し迅速且つ正確に対処し、対象者及び奈良県様へ速やかにご報告いたします。

弊社では2006年3月に
個人情報保護のマネジメント規格
「プライバシーマーク」を取得いたしました。

10450055(08)

（3）LINEのセキュリティー・別途詳細

(1)なりすまし防止(ユーザ及びサーバ認証)

1、本システムにおける認証パターン
本システムは下記#1の認証を基本としております。ただし、一般に公開するコンテンツに関しては#0の認証となります。
オプションとして2，3の認証を付加することが可能です。

#	パターン	
0	サーバ認証	・TLS通信によるサーバー認証
1	サーバ認証＋IDパスワード認証	・TLS通信によるサーバー認証に加え、 個別に発行されたID,パスワードによる認証と 認証情報をもとにしたセッション管理を実施
2	＋IDパスワード認証	・クライアント証明書認証を利用し、 証明書が登録されているPCからのみの認証する。
3	＋IP制限	・事前登録されているIPアドレスでのみ認証する。

2、DBのおけるデータアクセスについて
・DB内のデータについては、各利用者のログインIDにて対象データを判断し、かつ、ユーザーID・パスワード等、前途の認証にて与えられた権限を絞ることにより、表示可能該当データのみを表示します。そのため、認証情報が漏洩されない限り、データが他の人に見えることはありません。また、ID、パスワードが漏洩した可能性がある場合、ユーザIDやパスワードの変更により不正アクセスをブロックすることができます。

3、XSS対策
【 XSS(クロスサイトスクリプティング ）】
悪意を持った第三者よりサイト内のプログラムに渡されたHTMLタグやスクリプトを、閲覧者のブラウザに送り、そのコンピュータで実行させて しまう脆弱性のこと。この脆弱性を利用すると、Webセッションの監視から、第三者への情報の転送、個人情報の含まれたクッキーを読み 取ったり上書きしたりすることができ、またそのサイトを 訪れるたびに実行される永続的なコードであることもあります。
・アプリケーションにて、入力データや引渡しデータ内にHTMLタグやスクリプトコード、SQL 文などが無いかをチェックします。
・アプリケーション上での入力データの引き渡しは必ずフレームワークによるサニタイズ処理を挟み、入力変数を直接出力する関数の利用を禁じ、また検知する仕組みを導入しています。
・作成されたアプリケーションに問題ないかチェックするため、第三者機関のアプリケーション脆弱 性検査を受けており、発見された問題点については対応を行っております。

4、OS、Webサーバソフトの対処
・利用しているOS、ミドルウェア、Webサーバソフトに対して、 全てのセキュリティ ホール情報の収集と対処を行ないます。(コンピュータ緊急対応センター(JPCERT/CC)、
情報処理振興事業協会セキュリティセンター(IPA/ISEC)を基本とします。)
・設定に問題ないかチェックするため、第三者機関の脆弱性検査(擬似攻撃)を受けており、発見さ れた問題点に ついては対応を行っております。

(2)盗聴防止のための暗号化

・盗聴防止対策として、TLS設定による通信データの暗号化を実施致しております。
【 TLS (Transport Layer Security) 】
インターネット上で使われるwwwなどのデータを暗号化し、プライバシーに関わる情報や企業秘密などを安全に送受信する仕組み。
電子認証機関の発行するサーバ証明書を使用することによって次の点が証明できます。
・〈サイトの正当性〉ドメインの所有者が持つサーバであることを確認できます。

(3) 不正アクセス(通信プロトコル制御、通信量制御、ハッキング対策)

Firewallにてインターネットから DBへの不正アクセスを遮断します。
またウェブサーバーの不要なポートへのアクセスを遮断します。
WebApplicationFirewall(WAF)により、アクセスを監視し、不審なアクセスをブロック、アクセスパターンを保全しております。
またロードバランサ及び、SSLアクセラレー タを使用し、Webサーバーの安定稼動をサポートします。
【 ロードバランサ(負荷分散装置 ）】
多くのサーバに要求を分散して送信し、各サーバが快適な応答速度を保つことを目的に外部ネットワークからの要求を転送する装置。
【 SSLアクセラレータ 】
SSL/TLSによる暗号通信で送受信される膨大なデータの復号化処理を高速に行う専用装置。

(4) ウィルス対策

本システムが受信するファイル・メールは直接サーバーに保存されることなく、マネージドサービスに直接渡され、
ウィルスや不正プログラムが処理されます。また、万一不正プログラムが侵入した場合も、サーバー環境はコンテナ技術を用いて定期的に初期化されますので被害の拡大を最小限に防ぐことができます。