2023.5.1

中国風険消息〈中国関連リスクニュース〉 <2023.No .1>

チャットツールの業務利用に伴うリスクと対策について

【要旨】
◆ 中国では日常生活のみならず、業務上でもチャットツールが多用されている。
◆ 中国の日系企業では、ウィーチャット（日本でいう LINE に似たサービス）に代表されるチャットツールの業務利用について悩みを抱える経営者が少なくない。
◆ 本稿では、チャットツールの業務での利用方法、これに伴うリスクについて事例を交えて紹介し、企業が実施すべき対策について述べる。

１．チャットツールに関する日系企業の悩み

（１）チャットツールとは

チャットツールは、パソコンやスマートフォンを介してコミュニケーションを行うアプリケーション（以下、アプリ）のひとつである。常に携帯しているスマートフォンでリアルタイムでコミュニケーションを取ることができるうえ、伝統的なビジネスメールのように形式的・一方的なメールではなく、実際に会話するようなざっくばらんなコミュニケーションが好まれる傾向にあるため、より早いテンポでやり取りを進めることができる。また、グループを作成して複数人で情報共有したり、画像や動画を送受信することも容易である。

中国では、チャットツールは日常生活のみならず、業務利用においても、欠かすことができないものとなっており、中でも「ウィーチャット（微信）」は最も広く普及しているチャットツールの一つである。

（２）チャットツールの業務利用に伴うリスク

日本企業の多くは、社内外とのコミュニケーションにおいて、会社が用意するメールアドレスを用いた正式なコミュニケーションを好む傾向がある。全ての送受信記録を会社が管理することにより、情報の記録、整理、バックアップ等の管理を適切に実施できるほか、なんらかの問題が発生した場合にも、トレーサビリティを確保し、原因究明や再発防止の検討を行えるといったメリットがある。添付ファイルにパスワードを掛けなければ社外に発信できないといったセキュリティ対策も講じやすい。

一方で、中国の多くの企業（日系含む）では、チャットツールで社外の取引先と連絡をとり、業務に関連するファイルを送受信するといった対応が、ごく日常的に行われている（取引先との初対面の場において、名刺ではなく、チャットツールの ID を交換する場面もよく見かける）。多くの場合、個人アカウントを利用しているため、やり取りの内容や送受信するファイルの内容を、管理者が把握することは困難である。会社としてメール情報を記録する、バックアップを取るといった対応ができないため、社外とのやり取りを継続する中で、情報の欠落や不確実性が生じるリスクもある。

そのため、チャットツールの業務利用を会社として認めた場合（黙認も含む）、チャットを通じた不用意な情報の送受信の中で、重要情報が流出する恐れがある。誤送信のようなヒューマンエラーのほか、故意・悪意による重要情報の不適切な授受、ユーザーである社員が新しい会社へ転職するにあたり、元の会社の既存顧客の情報を持ち出すといった例もある。また、管理者にとっては、チャット内容を随時把握するのは困難であるため、万が一顧客対応を長期間にわたって放置する社員がいたとしても、適切な管理が行えない。

（3）チャットツールの業務利用を禁止すべきか

このように、チャットツールの業務利用には、会社にとって様々なリスクが想定されるため、中国の日系企業では、これを禁止したいと考える経営者が少なくない。また、実際に業務ルールとして使用を禁止しているケースもある。しかしながら、前述のような中国の現在のビジネス習慣に照らすと、「業務利用禁止」ルールに実効性を持たせるのは極めて難しい。「ウィーチャット」に代表されるチャットツールは、人々の生活に深く浸透しており、こちらからの情報発信を会社メールに限定したとしても、相手方からチャットツールで返信があったり、顧客から「会社メールでなく、チャットツールで資料を送付してほしい」といった要望を受けることもしばしばあるからである。このような利用実態を考慮せず、業務パソコンへのチャットツールアプリのダウンロードやスマートフォンの業務利用を禁止すると、会社に内緒でチャットツールを利用し続ける社員の増加に繋がる恐れがある。

したがって、会社として現実に即したセキュリティ対策を講じるには、チャットツールの利用を一律に禁止するのではなく、利用に伴うリスクについて社員に周知するとともに、最低限遵守すべきルールを設定して徹底させるといった対応が、より現実的であると考えられる。

2．中国におけるチャットツールの利用状況とリスク事例

（1）チャットツールの利用状況

中国で多く用いられているチャットツールには、ウィーチャットや DingTalk（釘釘）等がある。日常的なコミュニケーションのほか、企業の宣伝・広告手段としても活用が進んでいる。中国で代表的なチャットツールは表１のとおり。

表１　代表的なチャットツール

名称	開発元	主な用途	アクティブユーザー数
ウィーチャット (微信)	テンセント	チャット、企業間の情報交換 商品やサービスの広告宣伝等	13.13 億人①
DingTalk (釘釘)	アリババ グループ	チャット、出勤管理、タスク管理等	6 億人、企業 2300 万社②
Lark (飛書)	バイトダンス	社内コミュニケーション、スケジュール管理、ドキュメント共同編集	611 万人③

① 情報の出典：http：//stock.hexun.com/2023-03-22/208055173.html

② 情報の出典：www.ithome.com/0/664/012.htm

③ 情報の出典：https：//36kr.com/newsflashes/1699631220506629

これらのツールをビジネスに活用する主な場面として、以下が考えられる。

表２　チャットツールの活用場面

場面	詳細
チームワーク	チーム内のタスク調整、情報共有に活用できる。特に遠隔地間、時差がある場合のコミュニケーションにおいて利便性が高い。
社内連携	社内のスケジュール共有、タスクの進捗確認、フィードバック等をタイムリーに行うことができる。
顧客とのコミュニケーション	ファイルの送受信、自社情報の案内、技術サポートの提供、受発注等を行うことができる。
商品・サービスの宣伝	チャットツール内のミニプログラムに、自社製品・サービスを掲載することができる。フォロワー数が増えれば、より関心を集めやすくなるといった SNS ならではの相乗効果も期待できる。

これらのツールの利用が進むにつれ、中国でもセキュリティ対策も注目されつつある。自社社員がチャットツールを使用する際に、会社の機密情報を外部に漏洩させる、ユーザー個人が虚偽広告や詐欺による被害を受けるケースも発生しており、企業としてもデータ管理や情報保護、社内ルール整備などの対策が求められる。

（2）企業にとってのリスク

チャットツールの業務利用が企業に及ぼすリスクとして、以下が考えられる。

① 情報漏洩リスク

ウィーチャットには、不特定多数に公開されるインターネットサイトやブログサイトとは異なり、公式アカウント（公衆号）や動画アカウント（視頻号）等といった、公開先を限定した情報発信を行うプライバシー機能がある。ただし、この機能により完全なプライバシーが確保されると誤解すると、思わぬ情報漏洩に繋がりかねない。チャットツールの基本的な性質はオープンである。全ての情報がオープンなネットワーク上でやり取りされ、保存されていることに注意する必要がある。万が一、社員がチャットツールを通じて情報漏洩を引き起こした場合には、社員個人が民事上・刑事上の責任を負うだけでなく、雇用する企業も、政府から処罰（罰金・業務停止を課される等）を受ける可能性がある。市場における信用低下や顧客離れといった二次的な損害に繋がる恐れがある。

事例：

- 2017 年、銀行社員がチャットツールを通じて顧客の個人情報を漏洩させた。銀行は監督管理機構による処分、改善命令を受けた。
- 2018 年、医師が患者のカルテを特定メンバー内のグループチャットに投稿したところ、患者のプライバシーを侵害する行為であるとして世間の批判を受けた。
- 2020 年 11 月、宅配会社の社員（5 名）が、社内の物流システムにログインできる ID を 1 日 500 元で不正に貸し出した。不正ログインした第三者がユーザー情報（発送者・配達先の住所、氏名、電話番号等）を盗み出した。流出した情報は 40 万件超におよび、被害額は 120 万元超に達した。
- 2022 年 4 月、地方政府職員が上級機関から機密文書を受け取った。速やかに関係者に情報伝達する必要があったため、「機密」部分を隠した状態で文書をグループチャットに投稿したところ、情報漏洩に繋がった。

② サイバー攻撃リスク

チャットツールは、多数のユーザーがグローバルなネットワークで繋がる仕組みであるため、サイバー攻撃を受けるリスクが高いといえる。ハッカーは様々な方法でチャットツールを攻撃して、直接的にメールアドレス、氏名、業務に関する重要な情報の入手を試みるだけでなく、標的会社の社内ネットワークを攻撃し、機密資料の窃取を試みることもある。

サイバー攻撃を受けて情報漏洩が発生した場合には、直接的な被害に加えて、ネット上での情報管理の甘さについて批判を受け、大きく会社の評判を落とす恐れもある。

表３　サイバー攻撃に伴う代表的なリスク（企業）

リスク	詳細
セキュリティの脆弱性	どのソフトウェアにもセキュリティ上の脆弱性が存在する可能性がある。ハッカーに脆弱性を突かれ、チャットアプリのインターフェイスや特定機能が攻撃されると、ウイルスに感染する（機密情報が漏洩する）。
リモートコードの脆弱性	コードの脆弱性を突かれ、攻撃者が悪意あるコードを実行すると、システムが不正に制御され、機密情報が漏洩する。
マルウェア攻撃	チャット機能で届いた悪質なリンク、ファイル、ソフト等にユーザーがアクセルすると、コンピュータにマルウェアがインストールされ、ユーザー情報の漏洩やデバイスの不正な遠隔操作に繋がる。
ソーシャルエンジニアリング攻撃	人の心の隙を狙った巧妙な手口にユーザーが騙されると、チャットツールのID・パスワードが流出する可能性がある。特定ユーザーになりすました第三者が他ユーザーに接触し、情報を騙し取る。
フィッシング攻撃	ハッカーがチャットツール内の公式ウェブサイトを偽造する、ツール管理者を装ってシステムメッセージやメールを送信することにより、騙されたユーザーのID・パスワードが流出する可能性がある。また、悪質なリンクをクリックすると、機密情報が漏洩する恐れもある。
ウィーチャットミニプログラム（公衆号）	ミニプログラムを利用する際は、個人情報（氏名、生年月日、GPS位置情報等）へのアクセス承認を要するケースが多い。ハッカーの攻撃により、ミニプログラムから関連情報が大量に漏洩する可能性がある。また、画像を文字変換するミニプログラムでは、変換の過程で情報がインターネットサーバーにアップロードされるため、データを窃取される恐れがある。
ファイル転送アシスタント機能	端末間での情報共有に利用する機能であるが、実際にはデータが端末やインターネット上に保存される。バックアップの削除を行った端末に対し、悪意ある第三者がアクセスすることにより、データが漏洩する。

事例：

- 2018 年 4 月、テック企業がチャットツールを用いたフィッシング攻撃を受けた。攻撃者はチャットツールのインタフェースを偽造し、不正なリンクをクリックさせる手口で社員 ID・パスワードを窃取した。甚大な情報漏洩に繋がった恐れがある。
- 金融サービスプラットフォーム業者は、ミニプログラム上で「ミニプログラムに友達を招待すると、1,000 元相当の品物を 1 元で購入できる」という内容のキャンペーンを実施した。キャンペーン開始直後にハッカーが自動攻撃ツールを開発し、最終的には割引サービスの恩恵を全て、ハッカーが不正取得した。
- 2020 年 2 月、市営企業の社員が機密文書を社内で共有する際に、チャットツール内の画像認識アプリで文書をスキャンし、文字データに変換した（機密文書の撮影・転送は禁止されている）。その後、当該データを機密性の低いサーバに送信したところ、アプリの保守スタッフが不正にこれらのデータを取得し、インターネット上にアップロードしたため、情報漏洩に繋がった。
- 2021 年 3 月、ある区の職員 A が機密文書を携帯電話で撮影した後、画像データをチャットツールで銀行社員 B に送付した。社員 B は、受領した画像データ（情報漏洩に配慮し、文書番号を削除済）を同様に友人 C に転送した。その後、友人 C が友人関係のグループチャットに画像データを投稿したところ、機密文書が広範囲に漏洩・拡散することとなった。

（3）ユーザー個人にとってのリスク

セキュリティ対策が不十分な場合には、チャットツールを使用する個人においても、企業と同様のリスクが生じる可能性がある。

表４　サイバー攻撃に伴う代表的なリスク（個人）

リスク	詳細
口座情報の窃取	フィッシングサイト、マルウェアなどの様々な手段でアカウント情報を窃取し、ユーザーの口座情報、チャット記録、アクセス記録等の機密情報を入手する。
個人情報の漏洩	チャットツールでは写真、マイク、位置情報へのアクセス権限が開放されているケースが多い。不正アクセスにより個人情報が漏洩し、悪用される可能性がある。
金銭の窃取	フィッシングサイト・ウイルスなどを送り付け、チャットアプリ上の決済パスワードを盗むことにより、ユーザーの残高を別口座に移動させる。

事例：

- 2019 年 7 月、A 氏がチャットツールを通じ、「銀行カードが凍結されました。凍結を解除するため、パスワードを入力してください」という内容のメッセージを受信した。A 氏は指示通りにパスワードを入力し、8,800 元の振込を行った。その後の警察の調査により、ハッカーが偽の銀行サイトを装ったフィッシング詐欺であることが判明した。
- 2019 年 8 月、B 氏が SNS にチャットツール（グループチャット）のスクリーンショットを投稿した。投稿内容は、「ある駐車場に数百台のシェアサイクル（自転車）が保管されており、現場を訪れた人は自由に自転車を持って帰ることができる」といったものであった。メディアも注目する話題となったが、実際のところ、この情報は事実ではなかった。このスクリーンショットは、ハッカーが個人のチャットツールから不正に盗み、加工して発信したものであった。個人の所有するデータが流出し、騒動に至った事例である。

３．業務でチャットツールを利用する際のリスク対策

業務でチャットツールを利用する際のリスク対策について、５つの観点から説明する。

（１）ハード対策

チャットツールを業務上で使用する際は、ビジネス利用を前提としたセキュリティ対策が講じられているビジネス専用の仕様のものを利用することをお勧めする。企業ウィーチャット（企業微信）、DingTalk（釘釘）がこれに相当する。これらのツールに関するセキュリティ機能は表５のとおり。

表５　ビジネス専用チャットツールのセキュリティ機能

SNS	セキュリティ機能	セキュリティ認証
企業ウィーチャット（企業微信）	転送・保存時に、内部データを暗号化する。	ISO 27001 情報セキュリティマネジメントシステム認証
	指紋、顔認証、OTP などのセキュリティ認証方式を採用する（非認証ユーザーはアクセス不可）。	中国レベル保護３級認定
	組織部門、社員に対して異なるデータ権限を設定する。	C ５認定、ドイツ連邦情報セキュリティ局(BSI)が公表したクラウドサービスのセキュリティ認定基準
	端末を紛失した場合には、データを遠隔操作で破棄する。	―
DingTalk（釘釘）	ログイン時に、ユーザー名・パスワードの入力に加え、SMS 認証コードなどの二次認証方式を採用する。	ISO27001 情報セキュリティマネジメントシステム認証
	メッセージが送信中・保存中に盗まれる、改ざんされることがないよう、データ暗号化技術を採用する。	CMMI5 評価認定
	組織管理者がツール内の構成、権限、アプリ、部門などの情報の管理・制御を行う、管理者機能を設定する。	国家商務部機密登録
	日常操作、ユーザー操作、クライアントのバージョンなどを監視・分析し、異常動作を検出する。異常が見られた場合には、速やかに警告・対処を行う。	―

（２）ソフト対策

ハード対策だけでは、情報攻撃やサイバー攻撃を完全に防ぐことはできない。したがって、ハード対策と合わせて、ソフト対策を講じることが重要である。社員の行動、情報管理、設備の使用等に関するルールを設定し、社員に周知する必要がある。

ソフト対策（社内ルール整備等）のポイントは表６のとおり。

表６　ソフト対策（社内ルール整備等）のポイント

リスク対策	詳細
情報の重要度	チャットツールの業務利用を認める場合には、社内に専任の情報管理者を選任する必要がある。取扱い可能な情報は、「一般情報」までにとどめ、国家秘密、業務秘密、顧客情報、商業秘密、プライバシー情報等は、取り扱いを厳禁とする。
データ分類	取扱うデータの性質に応じて「機密レベル」を設定し、機密レベルに応じた相応の安全対策を講じる。機密レベルの高い情報は、チャットツールでの送受信を禁止するだけでなく、暗号化、バックアップなどの対策を徹底する。
権限管理	管理者は部門・社員の役割に応じて、アクセス権限をきめ細かく管理する必要がある。不要なデータへのアクセスを制限し、情報漏洩リスクを予防する。
パスワード保護	ID の乗っ取りを防止するため、チャットツールの ID・パスワードの定期的な変更を徹底させる（数字、文字、記号をいずれも含む安全性の高いパスワードとすること）。ID・パスワードの使い回しは厳禁とする。画面上を指でなぞるジェスチャーパスワードの活用も有効的である。 公共の場、安全性が確保できないネットワーク環境では、パスワードを入力させないことも重要である。
公共 WiFi	公共の場で提供される非認証の WiFi ネットワーク、暗号化されていない WiFi ネットワーク、「88888888」といった単純なパスワードで接続できる WiFi は使用しない（ネットワーク管理者やハッカーに情報を傍受される、ハッキング・情報窃取の被害にある可能性あり）。
不明なリンクのクリック	チャットツール内のコンテンツに表示される不審な広告、宣伝リンクを不用意にクリックしない。必要に応じて、アンチウイルスプログラムでシステムをスキャンし、安全を確保する。プライバシー設定で「漂流瓶」、「揺一揺」、「附近的人」等、悪意を持った第三者の接近を招く機能をオフにする。
ログ監視	システムログを常時監視し、ログデータを分析することにより、システム内の異常動作を早期に発見する必要がある。セキュリティ・インシデントに速やかに対応できるよう、不審な挙動を自動監視・識別・報告できる仕組みを設ける。

（３）緊急時対応

情報漏洩やサイバー攻撃を完全に予防することは困難であるため、万が一の場合に備えて、被害拡大を防止するための緊急時対応についても検討しておく必要がある。以下にそのポイントを説明する。

表７　緊急時対応のポイント

リスク対策	詳細
①　検知	報告すべき「異常」の定義、報告ルートを明確化する。
②　初期対応	感染の恐れがある端末・ネットワークを隔離するための対応手順を明確化する。システムダウン、ネットワーク停止の判断基準を設定する。日本本社、公安等に報告する基準を設定する。
③　調査・分析	原因調査と影響範囲を明確にする特定のプロセスでは、外部専門家を起用するための判断基準を検討しておく。被害を受けた情報の重要度・ビジネスへの影響について事業部門を巻き込んで分析する。
④　情報開示・顧客対応	対外発表の要否に関する判断基準、対外発表項目を事前に検討しておく。情報漏洩の被害を受けた顧客への対応方針と対応要領を整理する。
⑤　復旧・再発防止	システム・データの復旧方針のみならず、再発防止対策も同時に検討する。

（4）社員教育・訓練

ルールを定めても、社員に徹底されずセキュリティ意識の向上に繋がらなければ意味がない。定期的に教育や訓練を行うことが重要である。

表８　社員教育・訓練のポイント

リスク対策	詳細
安全教育	社員に対して定期的にサイバーセキュリティや情報漏洩リスクに関する研修を行う。研修は全員参加かつ理解度テストを行うことが望ましい。
抜き打ち検査	重点検査項目の 1 つとして、抜き打ち検査をおこない、スマートフォンや業務パソコンの利用状況、重要情報の取扱い情報をチェックする。
フィッシング攻撃訓練	チャットツール内のプラットフォームを利用して、社員を対象としたフィッシング攻撃訓練を行う。偽のリンクやその他の形態の電子通信を送信し、社員が不用意にクリックしないかを点検する。
サイバー攻撃訓練	サイバー攻撃を受けた想定下で、緊急時対応に関するシミュレーション訓練を実施する。対応ルールや対応能力の実効性を検証・評価する。

（5）ユーザー個人の対策

各社員が保有するスマートフォンなどの端末にも以下のようなセキュリティ対策を実施させる必要がある。

表９　ユーザー個品の対策のポイント

リスク対策	詳細
バージョン更新	スマートフォンのシステムとソフトウェアを適切なタイミングでアップグレードすることにより、既知の脆弱性を修正し、セキュリティを向上させることができる。スマートフォンの Root、Jailbreak と呼ばれる行為は、安全性の低下を招くため、厳禁とする。
アプリのインストール	アプリをダウンロードする際は、公式アプリストア、またはその他の信頼できるチャネルを利用する。アプリのインストール前に、アプリが要求するアクセス権限の範囲を慎重に確認する。プライバシー関連の権限を不必要に開放しない。
PC の保護	チャットツールの PC 版をインストールする場合には、その PC に以下のセキュリティ対策を講じる。 ウイルス対策ソフトやファイアウォールの導入、不特定多数の人が利用できないようなパスワード設定、OS とアプリケーションの適切なタイミングでの更新、チャットツール利用時のログイン異常へのアラート等。

４．まとめ

本稿では、中国で発生した重大な情報漏洩、サイバー攻撃の事例をもとに、企業が講じるべき対策のポイントを説明した。こういった事例の主要な原因は、アプリの技術的な欠陥、ヒューマンエラーなど様々である。これらのリスクに対策を講じるためには、技術面、管理面、運用ルール面、法律面などを含め、全面的な検討・対応を進める必要がある。本稿で述べた対策がチャットツールを安全に業務利用する上での一助となり、情報セキュリティ事故の低減に繋がれば幸いである。

以　上

参考資料：

1. 和讯网新闻　http：//stock.hexun.com/2023-03-22/208055173.html
2. IT 之家新闻　https：//www.ithome.com/0/664/012.htm
3. 36 氪　https：//36kr.com/newsflashes/1699631220506629
4. 网易新闻　https：//www.163.com/dy/article/HMFNQMM00514D3UH.html
5. 搜狐新闻　https：//www.sohu.com/a/492876948_161795
6. 保密观”微信公众号：微信泄密又出新案例
   https：//www.12371.cn/2021/11/19/ARTI1637277436721109.shtml
7. 永安在线报告：基于微信小程序生态体系的黑灰产研究报告　https：//zhuanlan.zhihu.com/p/408514439

インターリスク上海　コンサルティング部　高級経理　張若亭