To Be a **Good Company**

TOKIO MARINE
INSURANCE GROUP

Cyber Threats under COVID-19

コロナ禍におけるサイバー攻撃の脅威

2021年11月10日

東京海上日動火災保険株式会社
IFFCO-TOKIO GENERAL INSURANCE CO. LTD.
萩原 圭介

IFFCO-TOKIO
GENERAL INSURANCE
Muskurate Raho

TOKIO MARINE
INSURANCE GROUP

Today's Agenda

1. Covid-19下におけるリスクへの影響
2. バーチャル世界におけるサイバー脅威
3. 基本的な自己防衛策
4. サイバーリスクのリスクマネジメント
5. サイバーリスク保険

Covid-19下におけるリスクへの影響

全世界における経済の停滞	働き方の劇的な変化	暫定的な制度と新たな申請スキーム	アジアにおけるサイバーの脅威
• 商取引の減少 • キャッシュフロー問題 • サプライチェーン問題	• 在宅勤務 • 従業員の健康問題 • ITセキュリティ対策 • 雇用契約内容見直し	• 監督省庁からの対策要請と速やかな履行 • 新たな制度（暫定的制度？）や申請スキームの導入 • 監視体制の強化	• Remote環境をターゲットにしたソーシャルエンジニアリング • ハッカーによる企業のITの脆弱性への攻撃 • マルウェア感染

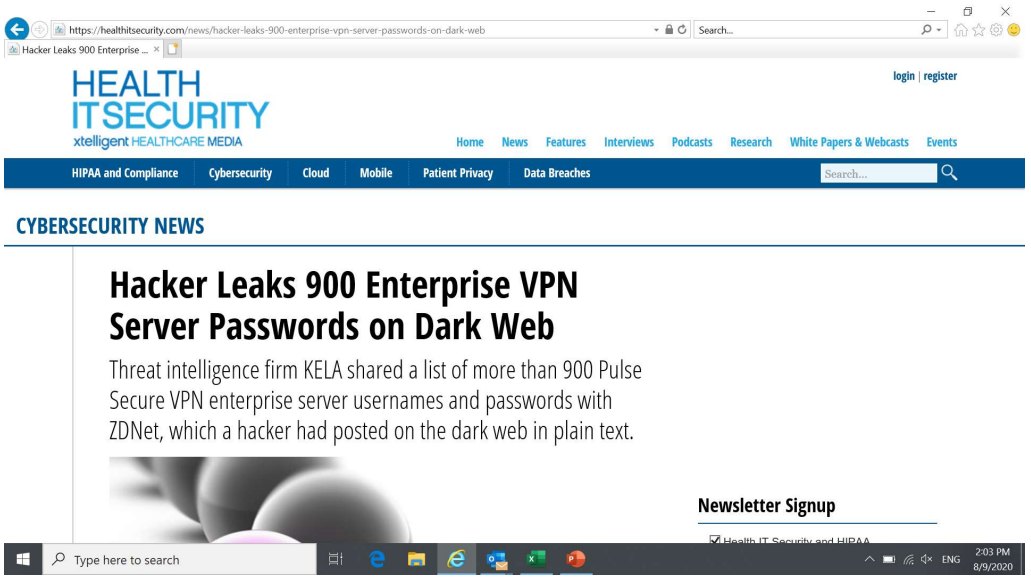
バーチャル世界におけるサイバー脅威

August 2020 – Russian Hacker
it is reported by KELA* that a Russian speaking Hacker has published a list of plaintext usernames and passwords, along with IP addresses for more than 900 Pulse Secure VPN enterprise servers.
KELA: Israel based Cyber Intelligent company

900以上の企業のパルスセキュアVPNとユーザー名・パスワードおよびIPアドレスが公開された

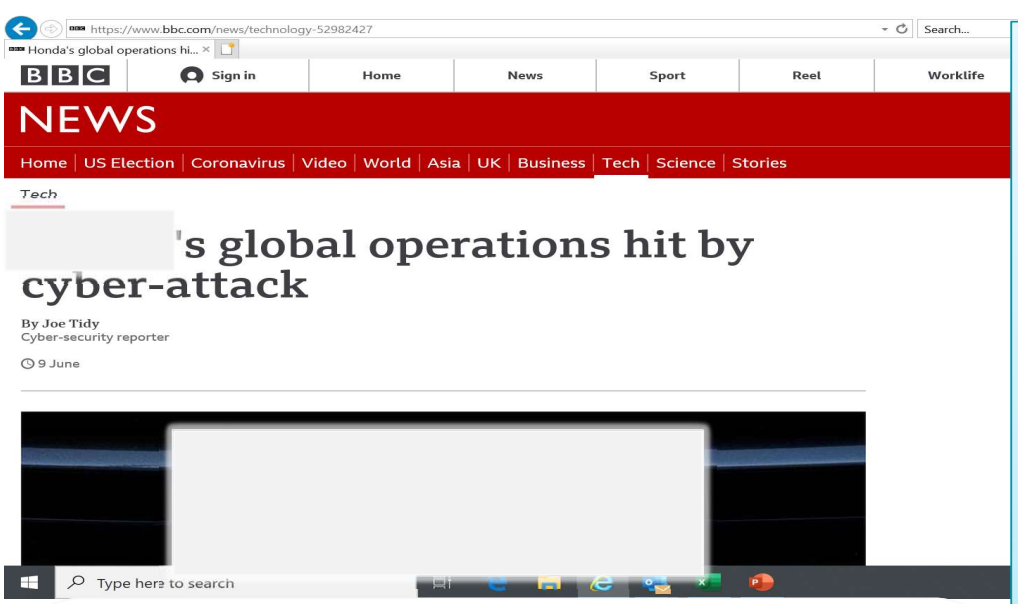
According to a review, the list includes:
- IP addresses of Pulse Secure VPN servers
- Pulse Secure VPN server firmware version
- SSH keys for each server
- A list of all local users and their password hashes
- Admin account details
- Last VPN logins (including usernames and cleartext passwords)
- VPN session cookies

これらの情報はハッカーフォーラムに掲載され、多くのハッカーが企業ネットワークへ侵入し、莫大な身代金を要求



list has been shared on a hacker forum that is frequented by multiple ransomware gangs.
For example, the REvil (Sodinokibi), NetWalker, Lockbit, Avaddon, Makop, and Exorcist ransomware gangs have threads on the same forum, and use it to recruit members (developers) and affiliates (customers).
Many of these gangs perform intrusions into corporate networks by leveraging network edge devices like Pulse Secure VPN servers, and then deploy their **ransomware payload and demand huge ransom demands.**

バーチャル世界におけるサイバー脅威



2020年某日発生したサイバーアタックにより、重要なシステムならびに社内メールシステムが使用不可となり、米国を中心に全世界の複数工場の生産停止を余儀なくされた。
当該マルウェアは〇〇〇のみを標的とし、ファイルを暗号化し身代金を要求するものであった。

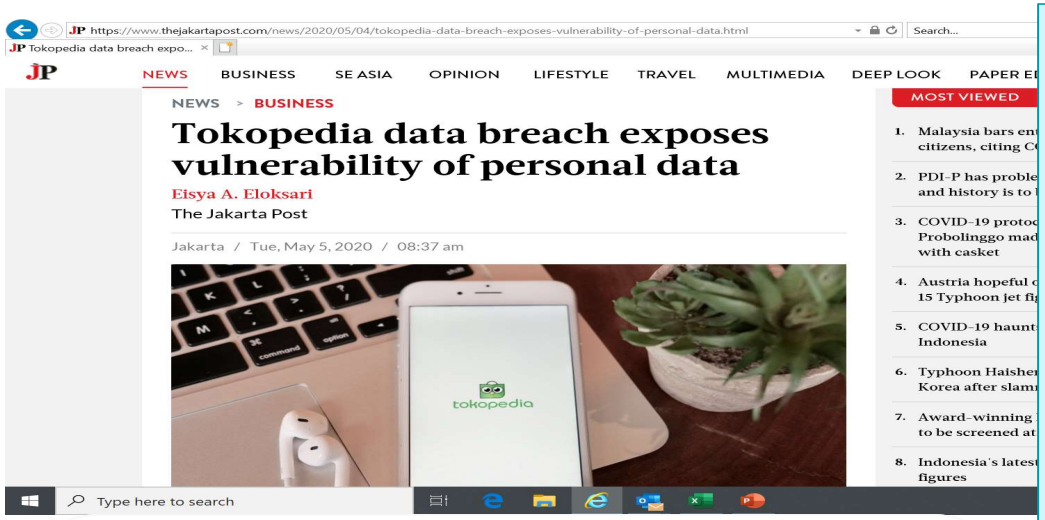
〇〇〇 MOTORS - 2020

〇〇〇 Motor was likely specifically targeted by the malware that brought several plants to a halt this month as sophisticated cyberattacks further highlight the need for organizations to protect themselves.

The company's network came under a file-encrypting ransomware attack 〇〇, disrupting production at 〇〇 factories in the U.S. and elsewhere. Essential systems, as well as internal email, were rendered unusable.

"The malware was made to encrypt files and demand a ransom only in 〇〇〇's internal environment," by analysist of Mitsui Bussan Secure Directions.

バーチャル世界におけるサイバー脅威



1,500万人のTokopediaユーザー情報を取得したとする匿名Twitterが投稿され、氏名・住所・誕生日などの重要情報が流出したことが判明。また同匿名者はユーザーのパスワードを解明すべく支援を求めた。
のちの調べにより、9,100万人の顧客情報が闇サイト上でわずかUSD5,000にて販売されていることが判明。

Jakarta, Tokopedia, May 2020

Data breach monitoring firm Under the Breach published a Twitter post on Saturday showing screenshots from an unnamed individual who claimed he had acquired the personal details of 15 million Tokopedia users during a March 2020 hack on the e-commerce site.

According to the screenshots, which show names, emails and birthdays, the hacker alleges he or she is in possession of a much bigger user database and asks for assistance to "crack" users' passwords.

Under the Breach, which monitors cyber crime, said on Sunday the hacker had updated the post to offer the details of 91 million users for "$5,000 on the Darknet". The firm shared a screenshot of the hacker's proposed offer posted online.

バーチャル世界におけるサイバー脅威

サイバー犯罪の目的とは?

- 身代金要求
- 不正行為– quasi CEO, etc
- 特定可能な個人情報
- 企業の機密情報やデータの取得
- 政治的問題
- 自己顕示欲

犯人は一体誰？

- Police report?
- Regulations?
- 国外？どこからハッキングしているのか？

インドにおけるサイバーリスク

インドの2020年度コロナ期間中のサイバー攻撃は前年比300%上昇。

300 % *rise in cyber attacks in India in 2020 Covid Times , govt tells Parliament*

2020年度の製造業に対するサイバー攻撃件数はインドはアジア地域で二番目に多い。同エネルギー部門においてはインドはアジアで最多。

India, NHAI , 2020/2021

NHAI had reported a cyber attack on its email server and had said that prompt action resulted in no data loss. It had shut down its server then as a precaution.

Server Shutdown across the company for weeks

India National Airline, 2021

A cyberattack on systems at airline data service provider SITA resulted in the leaking of personal data of passengers of the Airline . The leaked data was collected between August 2011 and February 2021

Last 10-year Personnel Data Compromised

インドにおけるサイバーリスク（過去事例）

No	内容
事例1	南インドの銀行2行、デリーの製造会社2社、アンドラ警察のPC100台にランサムウェアによる被害発生。使われたのは「The Shadow Broker」（ハッカー団体）がアメリカ国家安全保障局から盗んだツール「Eternal Blue」が変形したもの。
事例２	カルナタカ州のブロードバンドのネットワークがマルウェアによる被害を受けた。6万個のモデムに影響を及ぼしネット接続不可になった。
事例３	レストラン検索サービス会社Zomatoが2017年５月にハッキングされたことを公表。1700万人の個人情報が盗まれた。
事例４	コスモス銀行へのマルウェア攻撃が2018月10日～13日の間に2回に分けて行われた。攻撃第1波では複数国から約12億7,000万円が盗まれ、第2波ではデビットカードを使ってインド全土で約2億2,000万円近く引き出された。22ヶ国という世界規模の攻撃。

世界のサイバー巨額損害事例

1. 半導体メーカー　マルウェア感染による生産ラインの全停止

半導体メーカーA社の製造工場で、マルウェアが原因で生産ラインが停止。USBメモリを経由し、装置のアップデートに使用した機器からマルウェアが侵入。

最終ラインで品質検査を行う検査装置がマルウェア感染したため、本来不良品として判定すべきものが検出されず。発生当初、感染源がわからず次々と飛び火、最終的に生産ラインを全停止。

1ヶ月間の操業停止を余儀なくされ、300億円超の売上機会を失った。

2. 海運事業者　ランサムウェア感染による操業停止

コンテナ海運事業者B社は、ランサムウェア“NotPetya”の被害を受けた。

4ヶ国の拠点の注文処理に支障が出て76港の一部で輸送遅延等の影響が数週間にわたり続いた。IT対応として、4,000台の新規サーバー、45,000台の新規PC、2,500のアプリケーションのインストールを行った。

業務中断による損失、IT復旧費用、業務関連費用等合計は2.5億USDから3億USD。

基本的な自己防衛策

最新版の（アップデートされた）ソフトウェアを使用する

WannaCryのケースにおいては、サポート期間が終了していたWidows XPやWindows Server2003を標的に行われた。これは最新のセキュリティパッチが行われないことを意味しており、極めて脆弱な状態であったことを意味している。よって常に最新版のアップデートされたソフトウェアを使用することを徹底することが必要である。

海賊版/不正ソフトウェアやデバイス使用について制限もしくは禁止をすること

専門家はアジアでの海賊版または不正ソフトのダウンロードや使用が非常に多く、かねてより警笛を鳴らしてきた。著作権の問題にとどまらず、海賊版のソフトウェアの使用によりコンピューターシステムへ甚大なダメージをもたらす危険性が指摘されており、それは海賊版ソフトウェアがマルウェアに感染している可能性がある為である。
従業員が所有している個人のUSBを会社PCへ接続した際にマルウェアが拡散したという事例も多く報告されており、これにより会社のPC、サーバー、ネットワークが影響を受けたこともある。その結果、会社のサーバーに保存されている重要データが流出していまうリスクが顕在化する。

基本的な自己防衛策

ネットワークへのアクセスに関する制御・制限

ソフトウェアのアップデートやウィルス対策ソフトの他に、Emailやウェブサイトへのアクセスを制限するといった社内ルールの制定が防止策として考えられる。
例えば、E-mailのアクセスをInternalメールサーバーシステムのみへ制限する、もしくはビジネスに関係の無いウェブサイトへのアクセスをブロックするといった対策が考えられる。
さらにビジネス用途での使用であってもファイルのオンライン上での受け渡しを行うサイト（Drop Box等）へのアクセスを禁じるという制限も考えられる。一般的にこのようなフリーソフトはセキュリティが脆弱であると仮定することが重要。

そして必要に応じて、機密情報はネットワークに接続されているPCやサーバーには保管せず、オフラインのPCにのみ保存しておくという対策を講じることも有効。

基本的な自己防衛策

ソーシャルエンジニアリング攻撃に対する定期的なTraining

昨今、多くの国々でソーシャルエンジニアリング攻撃が日増しに増加してきており、その手法もより巧妙になってきている。そうした中で、詐欺であることを見極めるのが極めて難しくなってきている為、定期的かつ継続的な従業員への研修が極めて重要であり、「何かこのメールおかしい」と感じる感覚を醸成させる必要がある。

サイバー事案が発生した際の対応について

PCやサーバー、ネットワークへのセキュリティを強化し準備周到にしていたとしても、サイバー攻撃のレベルは常に進化しており、完全にその危険性を排除することは不可能といえる。
従って、サイバー攻撃が起こった際にどのように対応するのか準備しておくことが非常に重要である。会社のブランドイメージを守るためにどのように対応するのか、例えば影響を受けた顧客・関係者への声明をどのように行うかなど準備をすることでレピュテーションコントロールを図ることが求められる。

被害を受けた際のコストの想定

実際にサイバー被害を受けた場合、どの程度の被害額になるのかを想定しておくことを強く推奨する。コンピューターシステムが全てダウンし、オペレーション継続が不可能になるという最悪のシナリオで、システム不全中に操業が出来ないことによる機会損失（利益損失）、調査費用、システムの復旧費用など諸々を考慮し算出しておくことで、会社としてのリスクの定量化・可視化をすることが重要。

Loss Scenario 1

Auto Parts Manufacturer

(Company profile)
Turn Over: INR 750 Cr
# of Employees: 400

サイバーインシデント

工場の組立ラインを制御する会社のコンピュータシステムがランサムウェアに感染した。
同社ではバックアップシステムとリカバリープロトコルを維持していたため、48時間以内に業務が完全に再開された。

Estimated Losses incurred by the Company

- **Operation Shut Down: 48 hours**
- **Income Loss: INR 2.5 Cr**
- **IT Forensic/restoration Costs: INR 0.8 Cr**

Loss Scenario 2

E-commerce

(Company Profile)
Turn Over: INR 2,500 Cr
# of Employees: 800

サイバーインシデント

ハッカーが同社サーバーへの不正アクセスを行い、ウェブサイトを改変しマルウェアを配置。サイト利用者の個人情報が盗まれた。

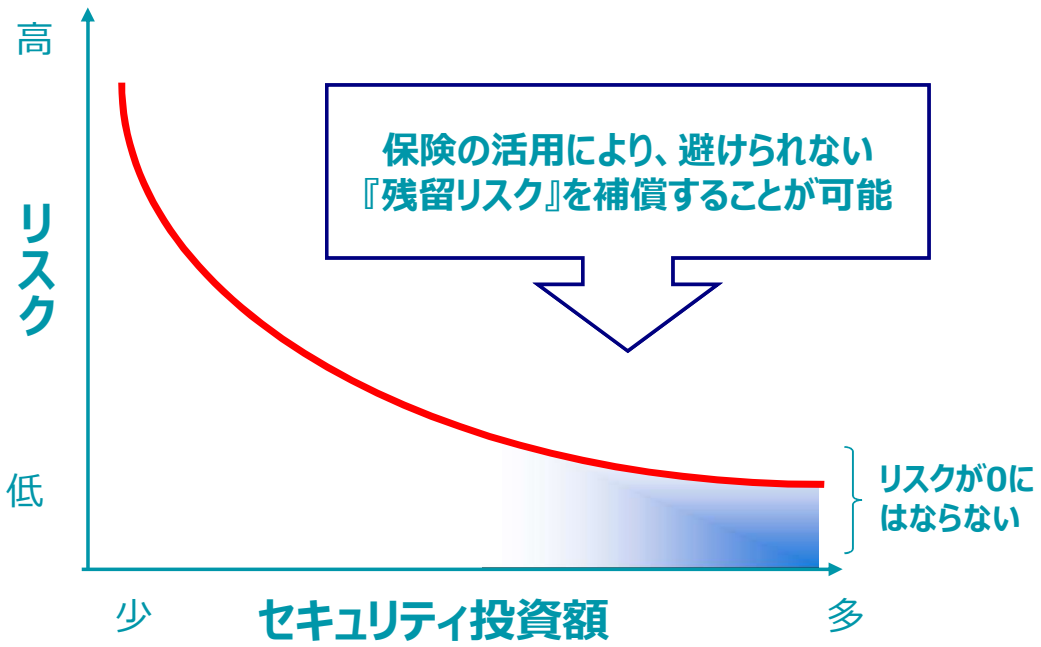
Estimated Losses incurred by the Company

- **Website Shut Down:** 10 days
- **Income Loss:** INR 3 Cr
- **IT Forensic/restoration Costs:** INR 1 Cr
- **Extra costs for manpower:** INR 0.3 Cr

サイバーリスクのリスクマネジメント

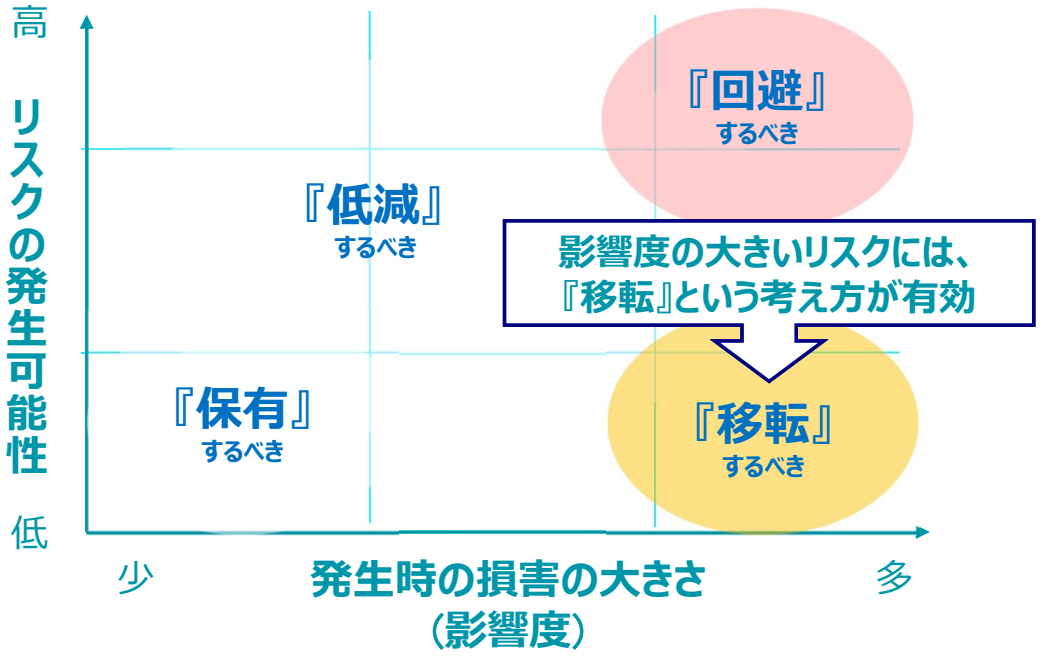
リスクマネジメントの選択肢の１つとして、保険活用は有効な手段

＜リスクとセキュリティ投資額の関係＞



✓どれだけセキュリティ対策に投資をしても、サイバーリスクをゼロにすることは出来ないといわれています。

＜リスクコントロールの考え方＞



✓リスクの発生可能性を下げたとしても、発生した場合の影響が大きいリスクに対しては、リスクの『移転』が有効です。
✓サイバーリスク保険は、リスクの『移転』に効果的な手段です。

サイバーリスク保険

- **<u>サイバーインシデント発生時の緊急対応</u>**
  - ・24時間365日のホットラインサービスで初診・相談に対応

- **<u>ITフォレンジック/調査費用と原状回復費用</u>**
  - ・24時間365日対応のホットラインサービスで相談した後、IT専門家による可及的速やかな処置は必要
  - ・IT専門家のフォレンジック及び復旧サービスによって発生した費用を補償

- **<u>「業務停止」に伴い発生した収入損害を補償</u>**

注：ご契約内容により、免責事項が適用される場合あり

サイバーリスク保険

個人情報の漏洩が発端となり、更なる損失を被る可能性あり

➢ **<u>当局の調査</u>**

・当局がデータ漏洩の原因調査や措置を講じる場合あり
→調査への対応費用を補償

➢ **<u>届出及び公示対応</u>**

・当局が会社に対し、漏洩事故に関連して被災者への通知を命じることがある
（日本のようなケース）
・また漏洩事故に関する届け出も求められるケースもあり
・公示のための費用を当保険にて補償

注：ご契約内容により、免責事項が適用される場合あり

サイバーリスク保険（主な補償内容）

コンピュータ鑑識

逸失利益

データ回復費用

監督官庁調査対応費用

告知･公示費用

第三者賠償

標準的な補償パッケージ

補償内容		
第三者賠償	セキュリティー侵害・個人情報漏洩に起因するもの	セキュリティー侵害・個人情報漏洩に起因して被保険者が被る民事上の賠償金や防御費用など
復旧費用・対策費用等の補償	個人情報漏洩に関する監督官庁からの調査・課徴金など	個人情報漏洩や個人情報保護に関する法律・規制違反により監督官庁などから調査を受けた場合の対応費用など
	危機管理費用	セキュリティー侵害・個人情報漏洩に起因して被保険者が被る法律への対応費用（公告など）、クレジットカードの与信監視システムやＰＲ費用など
	サイバー恐喝	被保険者のコンピュータへの不正侵入により被保険者のデジタル情報を損壊または漏洩するなどのサイバー恐喝に対する対応費用や身代金など
	デジタル・アセットの消失	サービス妨害攻撃やウイルス、不正アクセスや不正使用により被保険者の保有するデジタルアセットが損傷、変質、盗まれたまたは破壊された際に係る復旧費用
	逸失利益やコスト	サービス妨害攻撃やウイルス、不正アクセスや不正使用などにより被保険者のコンピュータシステムの一部損壊または全壊により被保険者が被る逸失利益や損失拡大防止費用など

ご清聴有難うございました。

IFFCO-TOKIO
GENERAL INSURANCE
Muskurate Raho

＜お問合せ先＞

IFFCO-TOKIO General Insurance

萩原　圭介（はぎわら　けいすけ）

Mobile：+91-93115-68134

Email: khagiwara@iffcotokio.co.in