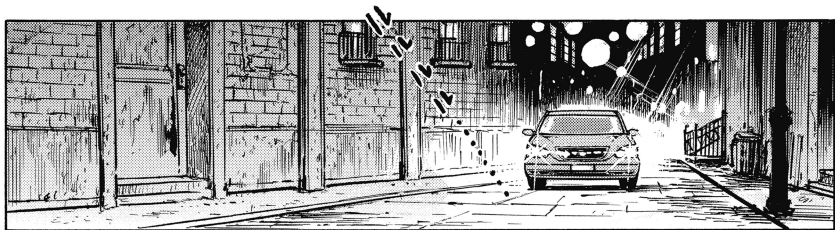
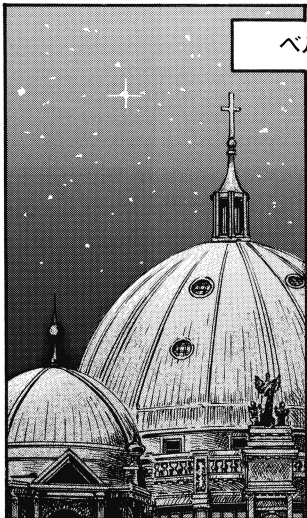


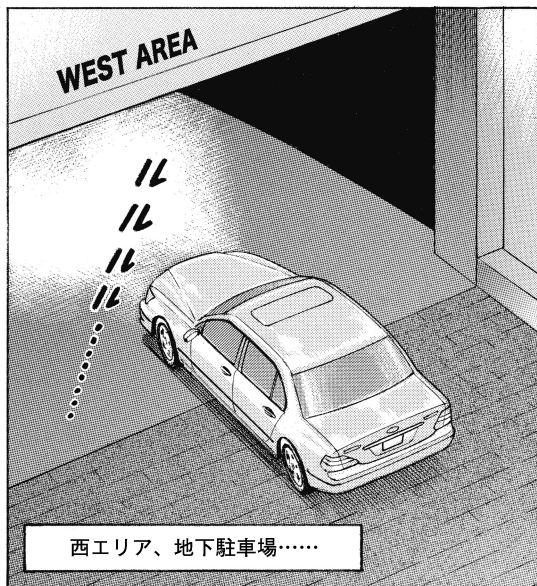
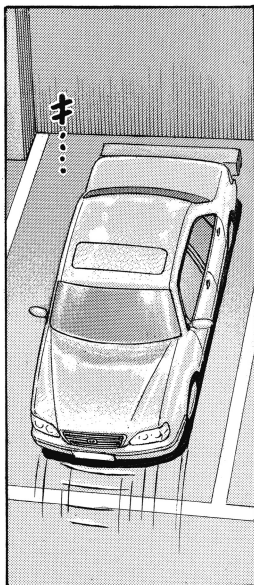


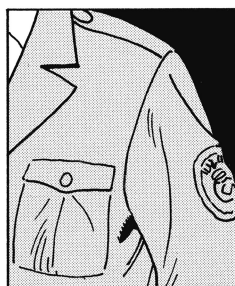
PART 8 オフィスの安全対策の死角

ベルリン——ドイツ——

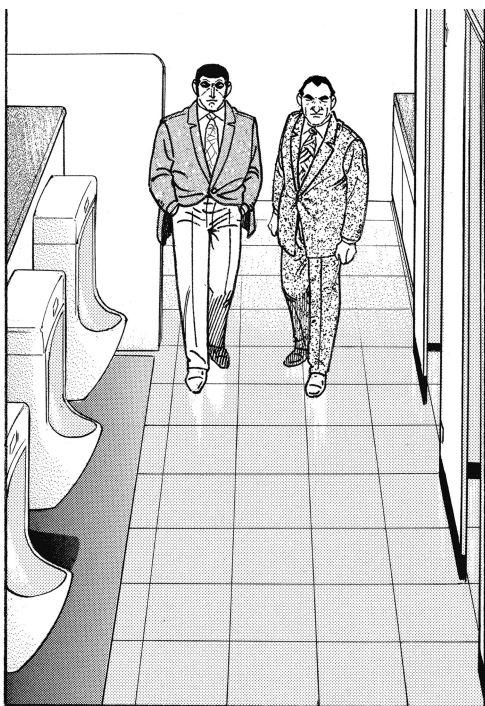
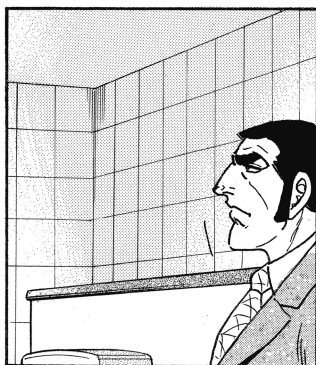


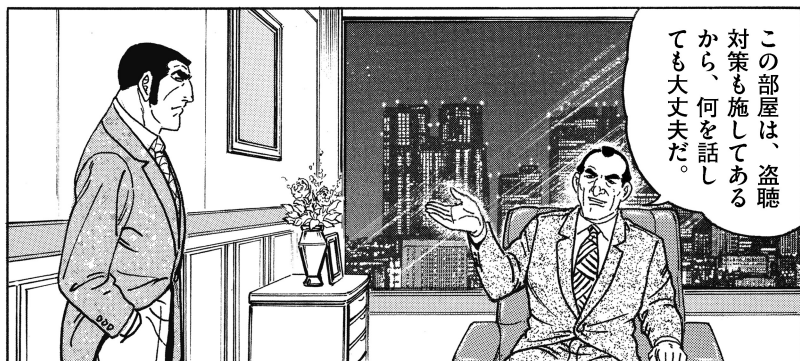




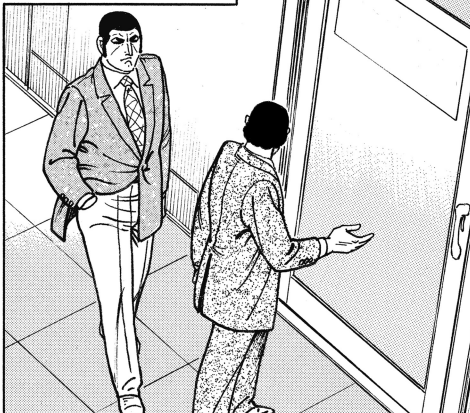








3ヶ月後、共同物産ベルリン支店……



うむ……
実によく分析
されている！
これは、
他の支社の
安全対策マニユ
アルのひな形になる
だろう！



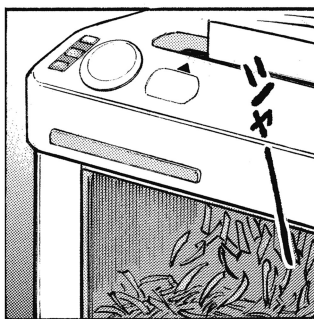
3か月間調査した
結果、まず、これ
だけはやっておく
べき安全対策を
まとめた。

おお、
それは素晴ら
しい！



ところで、
この報告書は
他にコピーは
あるのかね？

これを
「Gマニユアル」
として我が社の
トップシークレッ
ト扱いにしよう。



8 長期滞在時の注意事項 その2

(1) オフィスの安全対策

長期滞在時には、現地に拠点を設ける、もしくは既に設置してあるオフィスを利用してビジネスを進めていくこととなります。1日の主要な時間を過ごすオフィスの安全対策には、住宅の安全対策同様に気を配ることが重要です。

(ア) オフィスを新設する場合

オフィスを新しく設ける場合、安全対策の観点からどのような点を考慮すべきでしょうか？例えば、治安環境や治安機

関の信頼性、テロ対象となりそうな施設の有無など所在地・周辺エリアの安全性、建物・駐車場の構造、雑居ビルであれば他の入居企業の情報、通勤経路の安全性、費用・利便性などを考慮するのが一般的です。加えて、建物自体の耐震性についても十分注意する必要があります。建築業者の能力が劣る場合もあるので、いつ、誰が建設した建物なのか、その業者の信頼性は高いのか、などについても可能な範囲で吟味する必要があります。

(イ) すでにあるオフィスを継続して使用する場合

既にオフィスがある場合には、一通り

の安全対策が講じられていることが一般的です。ただし、住宅同様その対策で十分かという点に関しては自ら確認し判断する必要があります。オフィス周辺の治安状況は設置時と比べて変化していないか、周辺でどのような事件が起きているかなどについて、最新の情報を入手したうえで安全対策を更新することが大切です。

(ウ) 具体的な対策

住宅の項目でも言及した通り、犯罪者は比較的侵入しやすい場所をターゲットにする傾向があります。近隣のオフィスがどのような安全対策をとっているかを

調べ、周囲と比べて自社の安全対策が同等以上であるかを確認することが大切です。例えば、入館者の確認は確実にされているか、警備体制は十分か、警備業者の信頼性は問題ないか、などについて確認を行います。また、監視カメラ、侵入センサー、通信手段などについても、自分自身でテストを行い、緊急時に機能することを確かめておくことが重要です。

オフィスの安全対策においても、住宅同様3つの防衛線を想定して対策を考えることは有効な方法です。

(115ページのチェックリストを参照)

(エ) 情報の管理

「行動を予知されない」というのは安全のための三原則の一つですがオフィスの安全対策でも同様の注意が必要です。例えば、役員や関係者の行動、来客などの情報管理を徹底し、必要最小限のメンバーのみで共有することが、危機を避けることにつながります。

具体的には、情報管理の責任者を決める、情報の取り扱い規定を定める、P C等の持ち出しをチェックするなど体制を整えます。情報共有に関しては、駐在員の動きに関する情報(日程、所在など)について社内の必要最小限の関係者のみが把握し、現地スタッフにはできる限り

周囲と比べて同等以上の安全対策が出来なければ、先ずお前の所が狙われる。



間際のタイミングで通知する体制とするなど、管理に気を配ることが重要です。

(2) 現地情勢にあつた対策を

オフィスの安全対策は、現地の情勢を

十分考慮したものであることが必要です。「これだけやれば大丈夫!」といった一律で

適用できる安全対策はありません。現地の治安情勢に応じてどのような警備体制を設けるか、どのような警備機材を設置するかを個別に判断していきます。

また、現地情勢はささいな

ことで大きな変化が生じる場合があります。日常的に関連情報をモニターしながら、最新の情勢分析に応じて安全対策を更新していくことが大切です



プロは決して自分の手を相手に預けるようなことはしない。

(第1巻『アロスの咆哮』より)

(参考) 自社マニュアル作成のための滞在中チェックリスト

1 テロ・治安情勢に係る情報収集／分析・評価 (本社・現地共通)	YES	NO
☐ ニュース（現地であれば、現地ニュース、CNN、BBC、インターネット情報等）などの公開情報を毎日確認しているか。	☐	☐
☐ 外務省海外安全ホームページに掲載されている進出国及び周辺国の渡航情報、進出国所在の在外公館（日本大使館・総領事館）のホームページを毎日確認しているか。	☐	☐
☐ 「在留邦人向けメールマガジン」に登録しているか。	☐	☐
☐ 外務省から「広域情報」が発出されたら、その背景等について必ず分析・評価しているか。	☐	☐
☐ 情報収集／分析・評価を専門に行うスタッフを指名・配置・育成しているか。	☐	☐
☐ 本社と現地の情報共有体制は確立しているか。	☐	☐
(本社)		
☐ 社内で情報の分析・評価をできる体制にない場合、危機管理会社等から分析・評価の提供を受けているか。	☐	☐
(現地)		
☐ 在外公館の担当や他の進出（日系）企業と定期的に安全対策を含め情報共有を行っているか。（在外公館作成の「安全の手引」入手を含む）	☐	☐
☐ 現地治安当局と良好な関係を日頃から構築し、情報を入手しているか。	☐	☐
☐ ニュース等の一般情報に加え、信頼できる情報ソースを複数確保しているか。	☐	☐
☐ 情報ソースから得た情報の信頼性を定期的に評価しているか。	☐	☐
☐ 現地職員と良好な関係を構築し、常日頃から必要な情報を入手できるような状況にあるか。	☐	☐

	YES	NO
☐ 進出地域の文化、宗教、社会等の特徴についても情報収集を行っているか（書籍等の関連資料の収集等）。また、それを事務所内で共有しているか。	☐	☐
☐ 日常と異なる状況が生じた時、それを異変として認識しているか。（スーパーの商品が極端な品不足になっている、いつもは渋滞の道路が空いているなど）。	☐	☐
2 情報管理（セキュリティ） （本社・現地共通）		
☐ 情報セキュリティに関する社内規則を定め、本社と現地事務所における情報管理（セキュリティ）責任者を指名しているか。	☐	☐
☐ 社内文書、電子データ、CD、USBメモリ等の扱いに関する社内規定を設けているか。	☐	☐
☐ 社内事務で取り扱う情報は、不必要な持ち出し・複写・配布をしないよう義務付けているか。	☐	☐
☐ 現地の情報の要管理対策区域への携帯電話、カメラ等の持ち込みを制限しているか。	☐	☐
☐ 駐在員および現地職員の私用電子機器（PC、携帯電話等）の現地事務所／工場／サイトに於ける使用に関する規制を設けているか。	☐	☐
☐ 必要と判断した場合には、電子データのパスワードによる保護や暗号化等の手段を講じているか。	☐	☐
☐ 席を離れる際には、パソコン画面をロックし、盗み見、不正利用を防止しているか。また、CD、USBメモリ等の外部記録媒体を机上等に放置したままにしていないか。	☐	☐
☐ 現地職員の社用PC、携帯電話の使用状況を管理しているか。	☐	☐
☐ 秘密度の高い情報は、外部への電子メールやPCのハードディスクへの保存を禁止しているか。	☐	☐

	YES	NO
☐ 秘密度の高い文書、CD、USBメモリ等は施錠可能なキャビネット等で管理しているか。	☐	☐
☐ 秘密度の高い情報を業務のために事務所外へ持ち出す場合に、情報管理（セキュリティ）責任者の許可を得ているか。	☐	☐
☐ 社内の情報機器（PC等）を業務のために事務所外へ持ち出す場合に、情報管理（セキュリティ）責任者の許可を得ているか。	☐	☐
☐ CD、USBメモリ等、外部記録媒体を廃棄する場合、物理的に破壊するか、データ消去ソフトウェア等を使用しているか。	☐	☐
☐ 駐在員の動きに関する情報（日程、所在等）については社内の必要最小限の関係者のみが把握しているか。現地職員に対する通知は、できる限りぎりぎりのタイミングでなされているか。	☐	☐
☐ 駐在員の動きに関する情報（日程、所在等）を飲食店等の社外で話題にしないよう、情報を知りうる人すべてに対して周知徹底しているか。	☐	☐
☐ 脅威度の高い地域では、ウェブサイト上や名刺に社員の顔写真を掲載しないような対策をとっているか。	☐	☐
☐ 盗聴の危険性が高い地域では、盗聴防止用の機器を使用しているか。	☐	☐
☐ 本社及び現地事務所における情報セキュリティの監査を定期的に行っているか。	☐	☐
3 駐在員／現地施設の予防措置		
(1) 駐在員の予防措置		
(本社)		
☐ 駐在員に対して派遣国の治安情勢について、外務省の渡航情報の案内を含め、派遣前に十分な説明を行っているか。	☐	☐
☐ 派遣前に駐在員及びその家族に対して安全対策について説明しているか。	☐	☐
☐ 危険地への派遣者を人選する際に候補者の健康状態を確認し、持病など健康に不安がある場合は派遣を避けるように配慮しているか。	☐	☐

	YES	NO
(現地)		
☐ 駐在員赴任時の在留届提出、帰任時の帰国・転出届提出を徹底しているか。	☐	☐
☐ 生活面（住居、車での移動等）の心構えを指導しているか。	☐	☐
☐ 現地の宗教的又は習慣的な禁忌について指導しているか。	☐	☐
(2) 現地施設の予防措置		
☐ 脅威評価を踏まえ、脅威度の高い施設から一定の距離を置いた場所に事務所・工場・工事サイトの場所を選定しているか。	☐	☐
☐ 周辺の治安状況をチェックしたか。隣に空き家はないか。犯罪多発地域に隣接していないか。	☐	☐
☐ 現地施設の安全対策は周辺の施設の安全対策と比べて同等以上か。	☐	☐
☐ 雑居ビルに事務所がある場合など、隣接するオフィス等の調査を行っているか。	☐	☐
☐ 受付、出入口に24時間体制で警備員が配置されているか。	☐	☐
☐ 警備会社及び警備員の信頼性について十分な調査を行っているか。	☐	☐
☐ 緊急時に備えて複数の通報手段が確保されているか。（警報装置、サイレン、構内放送、電話・メールの同報等）	☐	☐
☐ 侵入探知センサー、警報装置を設置し、時々テストしているか。	☐	☐
☐ 監視カメラは設置されているか。	☐	☐
☐ 警備員とのコミュニケーションは適確にとれているか。	☐	☐
☐ 外部業者、訪問者へのセキュリティチェックは十分か。	☐	☐