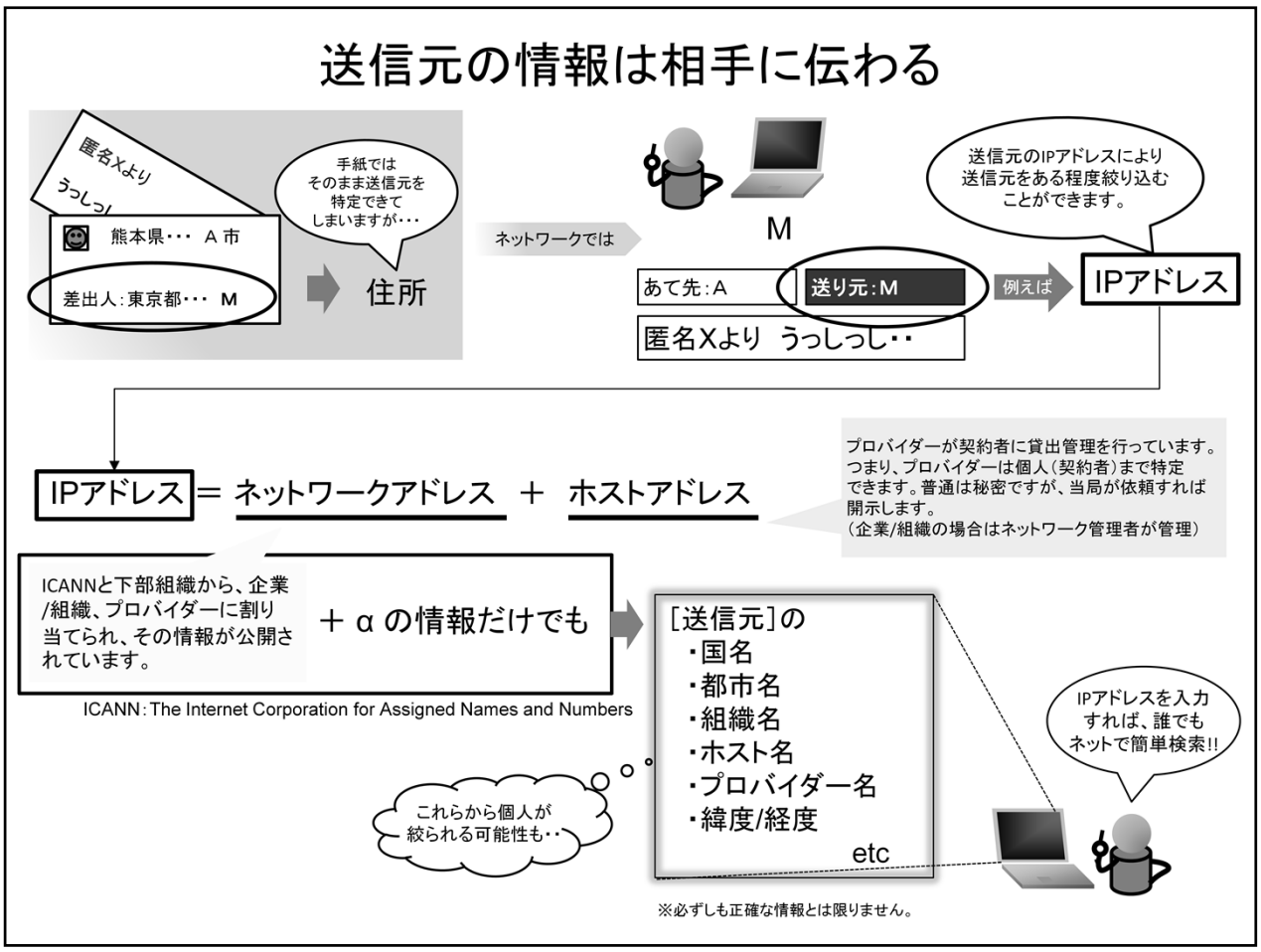


相手に伝わる送信元の情報には様々なものがありますが、基本となる情報は、IPアドレスです。IPアドレスは、基本的には世界に2つと同じ番号が存在しないように管理された番号で、インターネット上でコンピュータを一意に特定する情報です。

このIPアドレスは、2つの情報から成り立っています。このうちネットワークアドレスと呼ばれる情報を調べることで、コンピュータが所属している組織の名前や、プロバイダー名などを簡単に知ることができます。ネットワークアドレスは、電話番号でいう「市外局番」や「市内局番」と同じような意味を持ちます。電話番号のうち、先頭にある「市外局番」や「市内局番」を見れば、どの地域から発信されたかを推測することができます。

また、自宅などがプロバイダーを経由してインターネットで接続されている場合は、IPアドレスそのものを、プロバイダーから貸してもらっているイメージになります。つまり、プロバイダーは何時何分に何番のIPアドレスを、どの契約者に貸し出したかを把握しています。通常は、この情報は開示されていませんので、誰が何番のIPアドレスを使用していたかは、第三者には不明ですが、警察や裁判所からの依頼に応じて、開示されることもあります。この情報を参照することで、送信元コンピュータひいては送信操作を行った人間を絞り込んでいくことができます。

パーミッションの確認

【「許可」(パーミッション)の一例】

許可に表示される項目名	許可内容	パーミッション名
ネットワーク通信 (完全なインターネットアクセス)	情報を外部のサーバに送信することを許可します。	INTERNET
電話/通話 (携帯のステータスとIDの読み取り)	通話状態、電話番号、個体識別情報(IMEI)、国際移動体加入者識別番号(IMSI)などの情報を読み取ることを許可します。	READ_PHONE_STATE
個人情報 (連絡先データの読み取り)	連絡先データを読み取りことを許可します。	EAD_CONTACT
ハードウェアの制御 (画像と動画の撮影)	カメラによる撮影と撮影データの読み取りを許可します。	CAMERA

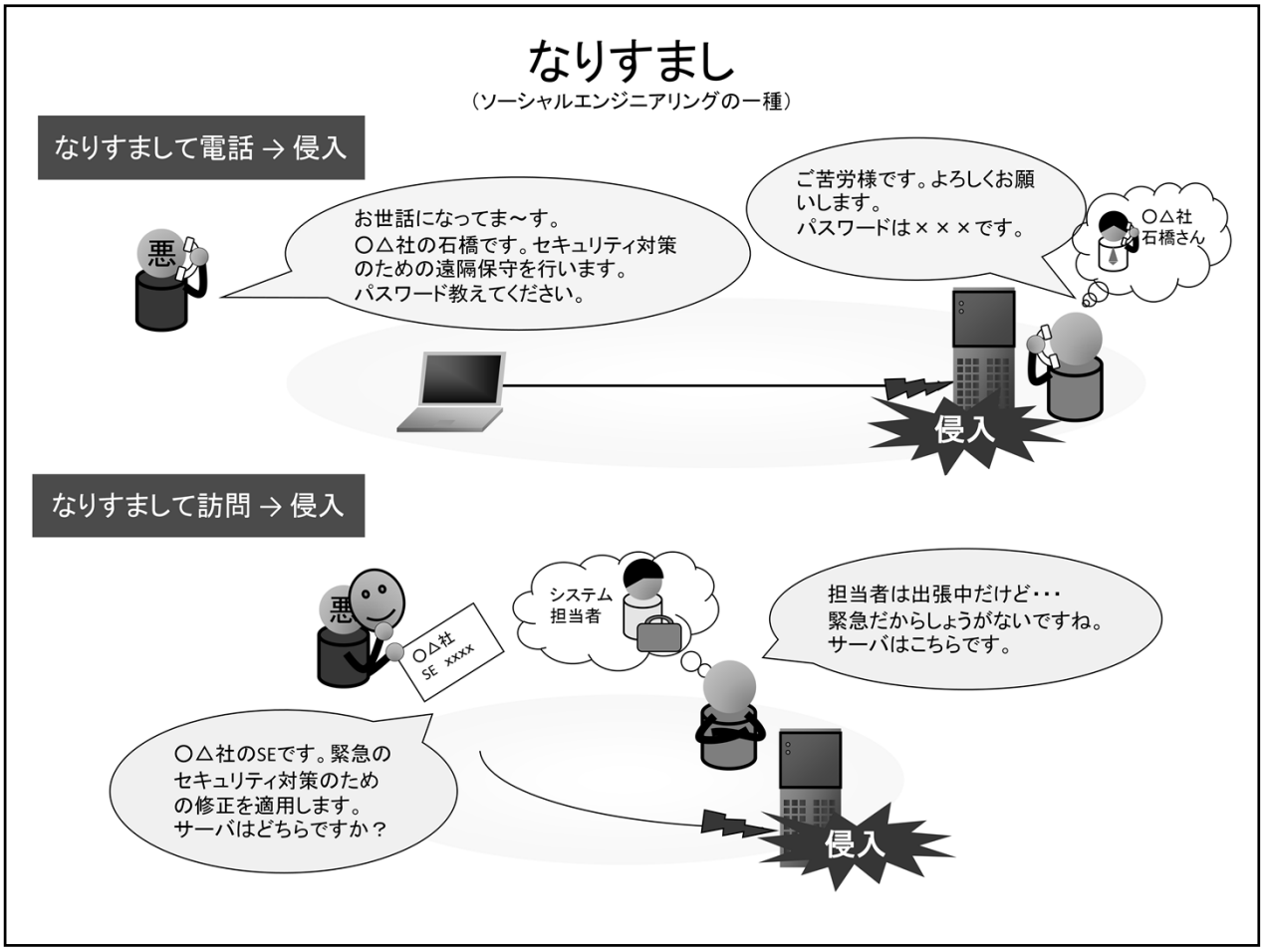
アプリケーションから、パーミッションで許可した権限以外の要求が行われると、Android OSは、その要求を拒否するため、アプリケーションは異常終了し動作できません。これにより、利用者が意図しないデータへのアクセスや通信を防ぐことができます。

しかし、この仕組みを知らずに、インストール時に要求された権限を確認せずインストールし実行してしまうと、思わぬ問題が発生します。また、権限は一つだけでも脅威になりうるもののありますが、組み合わせに対する注意も必要です。

例えば、「ネットワーク通信」と「電話/通話」を許可しているアプリケーションは、利用しているAndroid携帯の電話番号などを、インターネットに送信することができることになります。「ネットワーク通信」と「個人情報」が許可されていると、連絡先データがインターネットに送信できます。すなわち、知り合いの名前と電話番号などの個人情報が流出する可能性があります。

また、クーポンアプリなどに、「ハードウェアの制御」などが許可を要求している場合もあります。

アプリケーションの動作上、必要な場合がほとんどですが、中にはウィルスやマルウェアなどが、必要以上の許可を要求して、情報漏洩などを行う場合もあります。



ここでのなりすましは、ソーシャルエンジニアリングの一つとして「なりすまし」を指しています。オレオレ詐欺のようなものをイメージしてください。

簡単なものでは、電話によるなりすましがあります。電話では顔が見えないため、正当な利用者の名前を名乗るだけで、簡単になりすますことができます。

例えば、普段は交流のない役員クラスの名前を名乗り、さらに高圧的な態度をとることで、冷静な対応ができないように電話してくる場合などがあります。また、システム担当者が不在であるのを見計らって、直接、企業を訪れて、サーバへの不正アクセスを図る場合もあります。