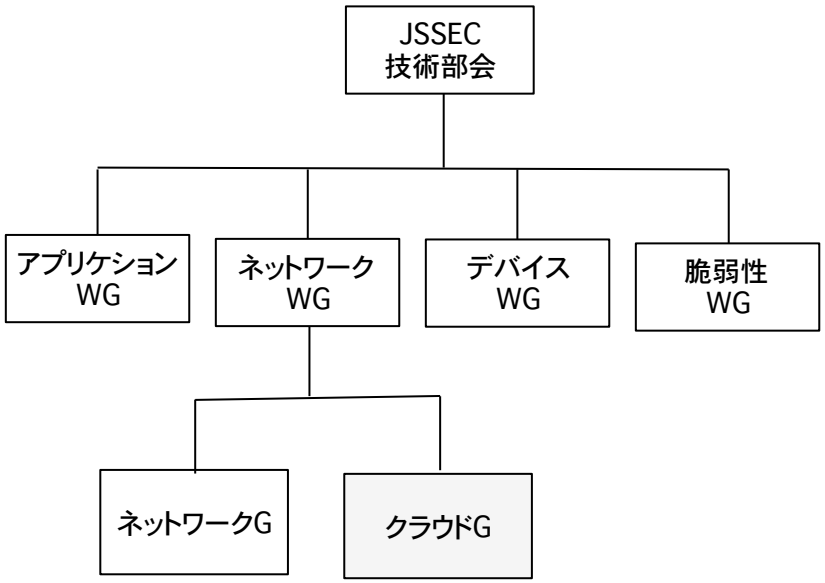
スマートフォンの業務クラウド利用における、端末からの業務データの情報漏洩を防ぐことを目的とした、企業のシステム管理者のための開発・運用管理ガイド

スマクラガイド

スマートフォンの
情報漏洩を考える

JAPAN SMARTPHONE SECURITY ASSOCIATION

一般社団法人日本スマートフォンセキュリティ協会技術部会 ネットワークWG クラウドG　文書番号JSSEC-TECN-CL-GD20130521-1



JSSEC技術部会の組織図と本ガイド執筆組織の位置づけ

JSSEC技術部会 ネットワークWG クラウドG

参加メンバー

リーダー：　株式会社コネクトワン 吉田 晋

メンバー：　アーンスト・アンド・ヤングアドバイザリー株式会社：倉永 英久
アルプスシステムインテグレーション株式会社：本多 規克
株式会社イーグリッド：野尻 泰正
株式会社NTTデータMSE：加藤 雅和
株式会社EMRESS SOFTWARE JAPAN：清水 健
株式会社神戸デジタル・ラボ：雲井 卓、バローズ ダニエル
株式会社CSIソリューションズ：中山 聡
シスコシステムズ合同会社：谷田部 茂
セコムトラストシステムズ株式会社
トレンドマイクロ株式会社：林 憲明、栃沢 直樹
一般社団法人日本オンラインゲーム協会：加治屋 繁久
日本電気株式会社：関 雄二
株式会社ネットマークス：相原 弘明
（会社名五十音順）

活動日

2012年 8/23, 9/21, 10/11, 10/30, 11/15, 12/17,
2013年 1/9, 1/29, 2/7

本ガイドの注意

※JSSECならびに執筆関係者は、本ガイドに関するいかなる責任も負うものではありません。全ては自己責任にて対策などをお願いします。
※本ガイドに登場する商品名・サービス名は、一般に各社の商標または登録商標です。
※社内文書などに引用する場合、著作権法で認められた引用の範囲内でご利用ください。また、その際は必ず出典を明記してください。
※本ガイドは発行日時点のものであり、記載された内容は今後変更の可能性があります。

目次

第一章 はじめに

第二章 FTA（故障の木解析）とは

第三章 FTAから導かれるスマートフォンからの情報漏洩26のケース

第四章 情報漏洩チェックに必要なセキュリティガイド

第五章 チェックリストの使い方（会社貸与端末とBYOD）

第六章 おわりに

第一章 はじめに

スマートフォンの業務クラウド利用における、端末からの業務データの情報漏洩を防ぐことを目的とした、企業のシステム管理者のための開発・運用管理ガイド

本ガイドの目的

日本スマートフォンセキュリティフォーラム（以下、JSSEC）では、2011年5月の発足以来、「スマートフォンやスマートタブレット（以下、スマートフォン）」の提供者／開発者／利用者などの、各企業が集まり、スマートフォンのセキュリティ向上に向けて様々な観点から調査・分析を行い、ガイドラインや提言の形で利用者などに公開してきました。

本ガイドは、スマートフォンの業務クラウド利用において、端末からの業務データの情報漏洩を防ぐことを目的とした、企業のシステム管理者のための開発・運用管理についてまとめました。

また本ガイドでは情報漏洩のリスク分析手法として、航空機などの信頼性工学の手法を取り入れました。日本の製造業が最も得意とする設計手法をスマートフォンのセキュリティ分析に適応したわけです。この手法のすぐれた点は漠然としたリスクではなく、理論的に発生し得るリスクを網羅して洗い出せることです。本当にAndroidは危険なのか、BYODは危険なのか、多くのシステム管理者が懸念するこれらの疑問の一つの解を本ガイドは提唱しています。

また自社のセキュリティ対策は必要十分なのか簡単に判断できるチェックリストもエクセルファイルとして本ガイドと同時にリリースされています。本ガイドとともにスマートフォンから業務システムを利用する際のセキュリティ対策として参考として頂き、業務効率の改善に貢献できれば幸いです。

ふうむむ。

本ガイドの構成

第二章 FTA（故障の木解析）とは

FTAと呼ばれる信頼性工学の設計手法について、なぜそれが情報漏洩対策に必要なのかを解説します。

第三章 FTAから導かれるスマートフォンからの情報漏洩26のケース

「どういう事象が組み合わさるとスマートフォンから業務クラウドの情報漏洩が発生するのか」というリスクの洗い出しを行います。信頼性工学設計で使われるFTAの手法を応用しています。

第四章 情報漏洩チェックに必要なセキュリティガイド

FTAによって洗い出されたリスクに対してどのような対策が必要か、ということと情報漏洩セキュリティを検討する上で必要な技術情報について解説します。

第五章 チェックリストの使い方（会社貸与端末とBYOD）

本ガイドと同時に配布されているチェックリストの使い方を述べています。会社貸与端末、個人所有端末（BYOD）などの視点から解説します。

自分のマスタデータ。

特定OS、特定機種に依存しない。

本ガイドの定義

「クラウド」「スマートフォン・スマートデバイス」の用語に様々な定義がありますが、本ガイドでは次のように定義します。

【クラウド】

1,クラウドとは「世界中どこからでも、どのOSどの端末からでも自分のデータにインターネット接続できる」というコンセプト”のこと。

2,クラウドにおいてはマスターデータは端末ではなくインターネット上に保存されることを基本とする。

3,従って以下のケースは本ガイドにおける【クラウド】とはしない。

－1 特定のOS、特定の機種からしかのみの接続を許可しないシステム。

－2 マスターデータを端末に保存する前提のシステム。

【スマートフォン・スマートデバイス】

スマートフォンおよびスマートデバイスとはクラウドへの接続を目的とした端末を指す。

【マルウェア】

ウイルス、スパイウェアなどの悪意のあるソフトウェアやプログラムの総称。

第二章 FTA（故障の木解析）とは

何が危険なのかを
知ることが第一歩

企業がスマートフォンを業務に利用する場合、セキュリティ的に安全なのか問題があるのかを判断することは非常に難しいといえます。その理由は、何がリスクであるかを定性的に洗い出すことが非常に難しいからです。

逆をいえば、何がセキュリティのリスクとして洗い出すことができれば、スマートフォンを業務利用として採用できるかどうか、きちんと定性的に判断することができます。

従来漠然と「BYODは危険だ。」とか、「AndroidはiOSに比べて危険だ」と判断していたことが、実はきちんと対策と施せば、危険を回避できるということがわかるかもしれませんし、あるいはやはりセキュリティ上カクカクシカジカという問題があるので採用ができない。ということがはっきり結論を出すことができます。

では潜在的なリスクを網羅的に洗い出す手法はあるのでしょうか。はい、あります。潜在リスクを洗い出す設計手法を信頼性工学設計と呼ばれます。そしてこの分野で最もよく知られている方法の一つにFTAがあります。

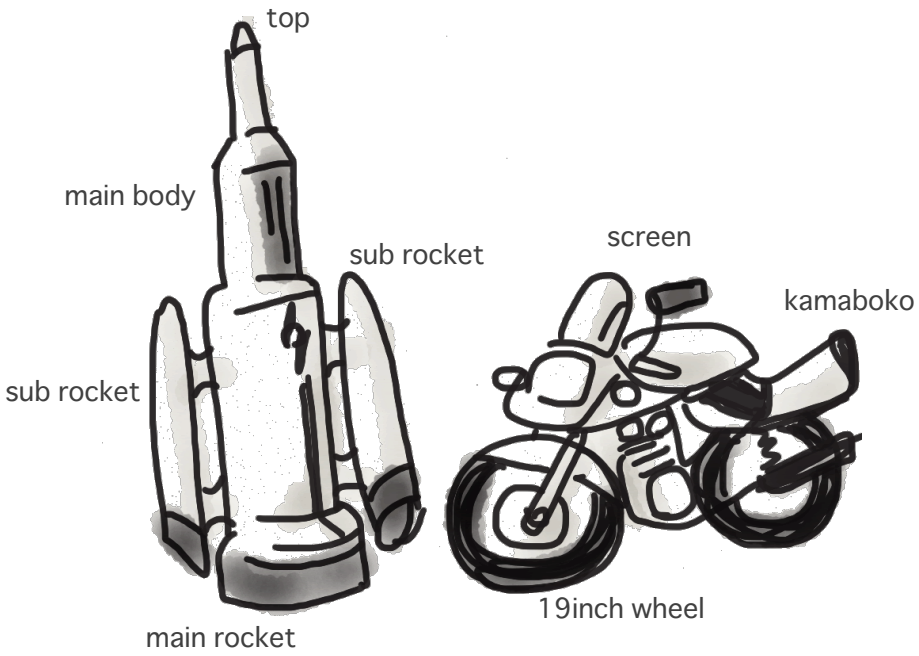
リスクを全部洗い出す

FTA（Fault Tree Analysis 故障の木解析）とは

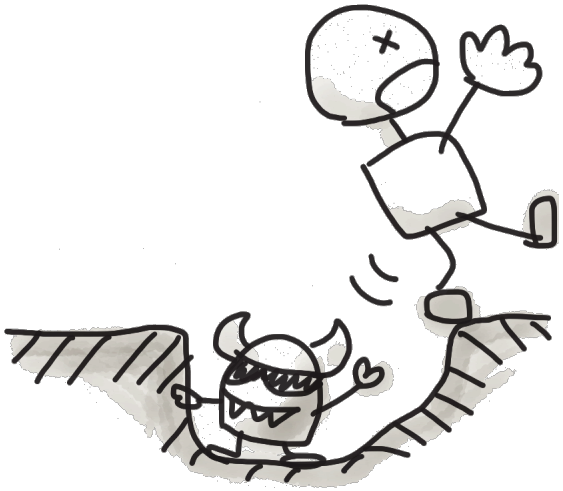
FTAとはシステム上で絶対起きてほしくない事象をトップ事象と想定し、その発生要因を上位のレベルから順次下位のレベルに論理展開した樹形図を作る設計手法です。

このFTAは1960年代に米空軍が大陸弾道ミサイル発射管制システムの信頼性を評価する手法としてベル研究所に委託したことが最初とされます。この手法はその後ボーイング社に引き継がれて完成されます。

今日では航空宇宙、原子力産業のほかに、自動車、電気製品、ソフトウェア、鉄道、建築、プラントなどで、システムの信頼性・保全性・安全性の解析に活用されていいます。



思い込みにはめられた。



ポイント1：
常識の落とし穴を見つける

FTAで最も重要なことは、「必ずトラブル事象が起こる」という視点で論理展開をしていく点です。

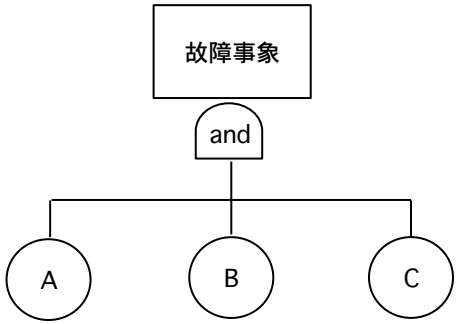
「必ずトラブルが起こる（例、必ずスマートフォンから情報漏洩が起きる）」。ではどういう事象が組み合わさるとそのトラブル事象が発生するか。という論理展開の視点がFTAです。この視点があるがゆえに、リスクの発生事象において網羅的な展開をすることが可能となります。

一般的にトラブル対策やセキュリティ対策は、最初に対策ありきで検討することが多くみられます。しかし対策を最初に脳内に想定してしまうと、その対策をすり抜けるリスクが見えなくなってしまうのです。これはどんなに熟練した設計者でも必ず陥る罠です。想定外を自分自身で想定することは非常に困難なのです。

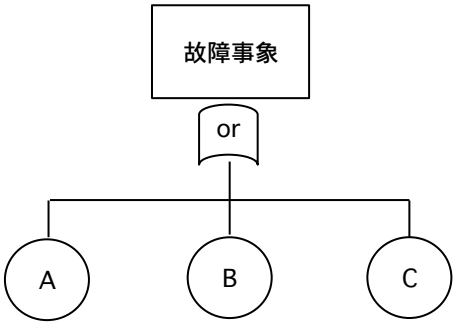
従って想定外を設計者自身が発見するために、「トラブルは必ず起こる」という視点で、リスクを論理展開することが効果的であるといえるのです。

ポイント2：必要十分な対策

FTAの特色は、そのトラブル事象が起きるの原因事象について、必ず「AND」か「OR」で展開していくということです。



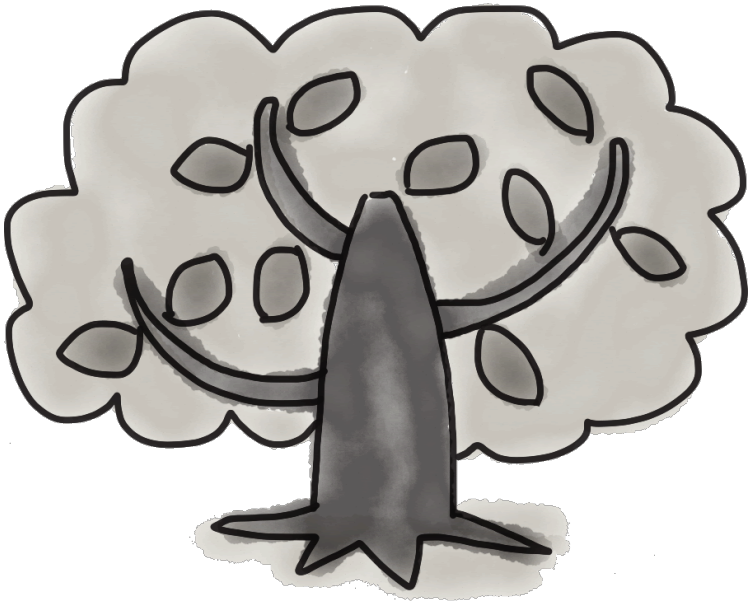
どれか一つ対策すれば防げる



三つとも対策しないと防げない

たとえば「故障事象」が発生する原因が「A事象」「B事象」「C事象」の3つが重ならないと起きないとします（AND条件）。その場合「A事象」「B事象」「C事象」のどれか一つが発生しないように対策するだけで、「故障事象」は発生しないといえます。
逆に「A事象」「B事象」「C事象」のどれか一つが起きれば発生するという場合（OR条件）は、その3つを全て対策しなければならない、ということがわかります。

つまりリスクの論理展開を行わず、設計者の思い込みだけで対策を検討すると、しなくてもリスク要因が変わらない不要な対策を施していたり、あるいは逆に本当はしなくてはならない対策がスッポリ抜けてしまう可能性があるわけです。しかしFTAによって、本当に必要十分な対策を検討することができるようになります。

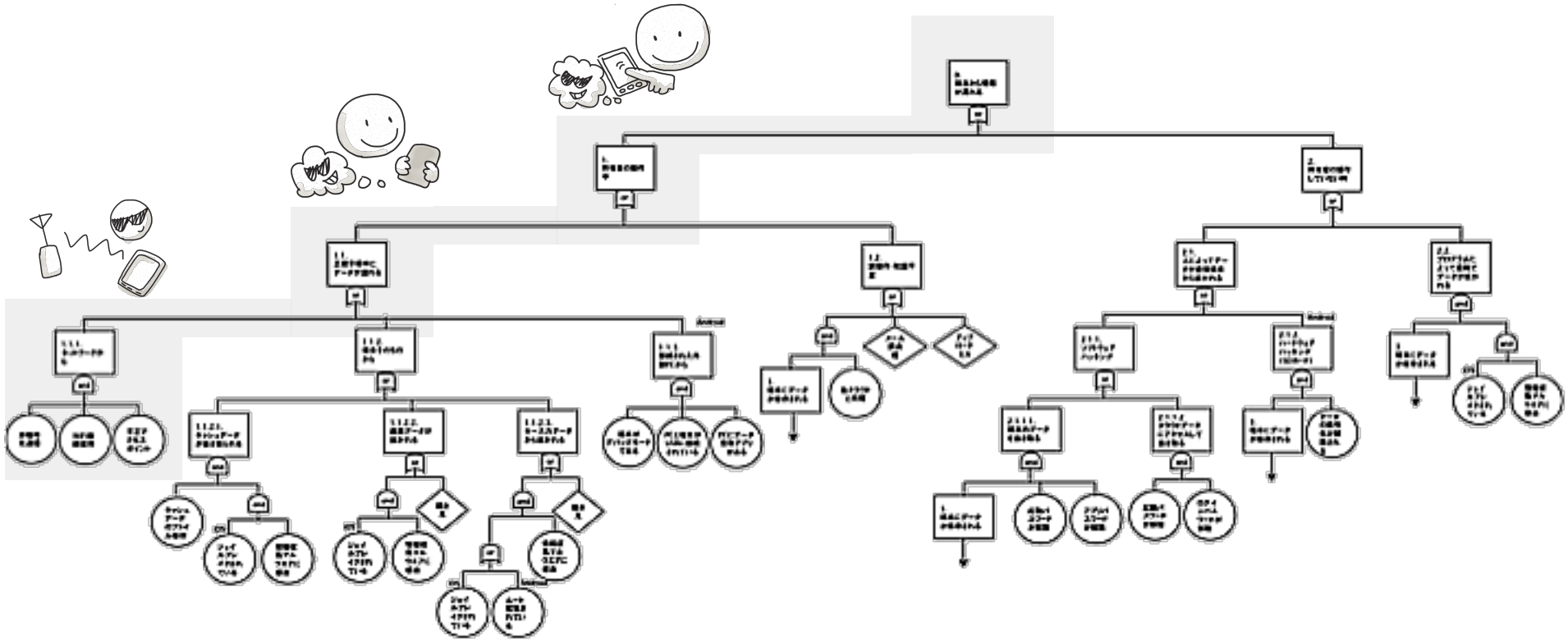


FTAの主な記号

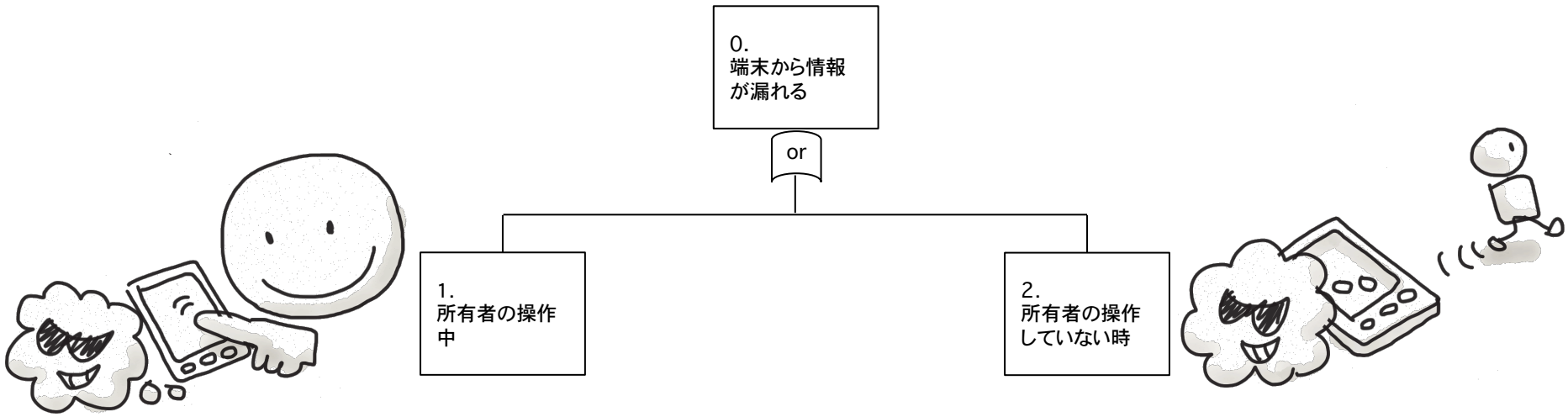
事象	欠陥や故障事象を表記します。
基本	これ以上展開できない事象を表記します。
非展開	情報不足や技術内容が不明確で展開を中断したときに使用します。
or	入力事象のいずれかが発生したときに出力事象が発生することを意味します。
and	入力事象がすべて発生したときに出力事象が発生することを意味します。

第三章
FTAから導かれるスマートフォンからの情報漏洩26のケース

スマートフォンの業務クラウド利用における端末からの業務データの情報漏洩FTA

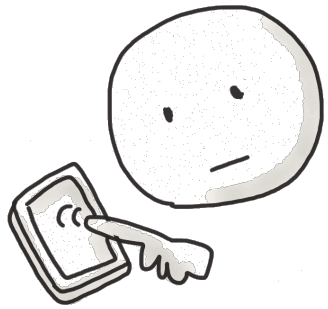


情報が漏洩する



端末操作中に

手から離れている間に



端末操作中に

1.
所有者の操作
中

or

1.1.
正規手順中に
データが漏れる

1.2.
誤操作・知識不
足

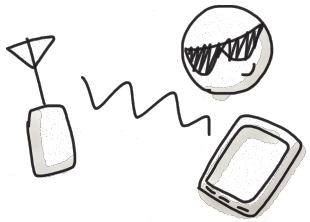
正規手順で
漏洩する

誤操作で
漏洩する

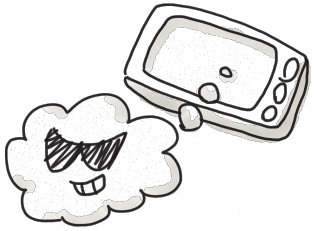
正規手順で

1.1.
正規手順中に
データが漏れる

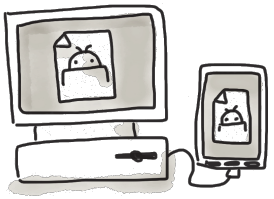
or



1.1.1.
ネットワークか
ら



1.1.2.
端末そのもの
から



1.1.3.
接続された外
部PCから

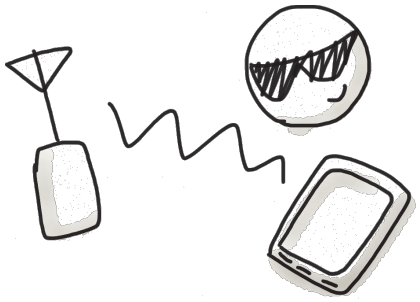
ネットワーク
から漏洩

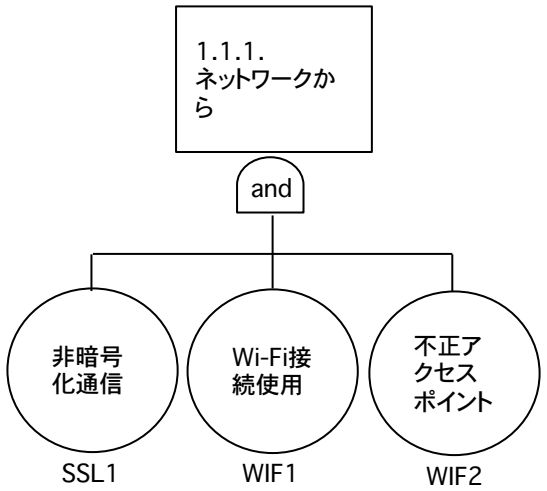
端末から
漏洩

外部PC
から漏洩

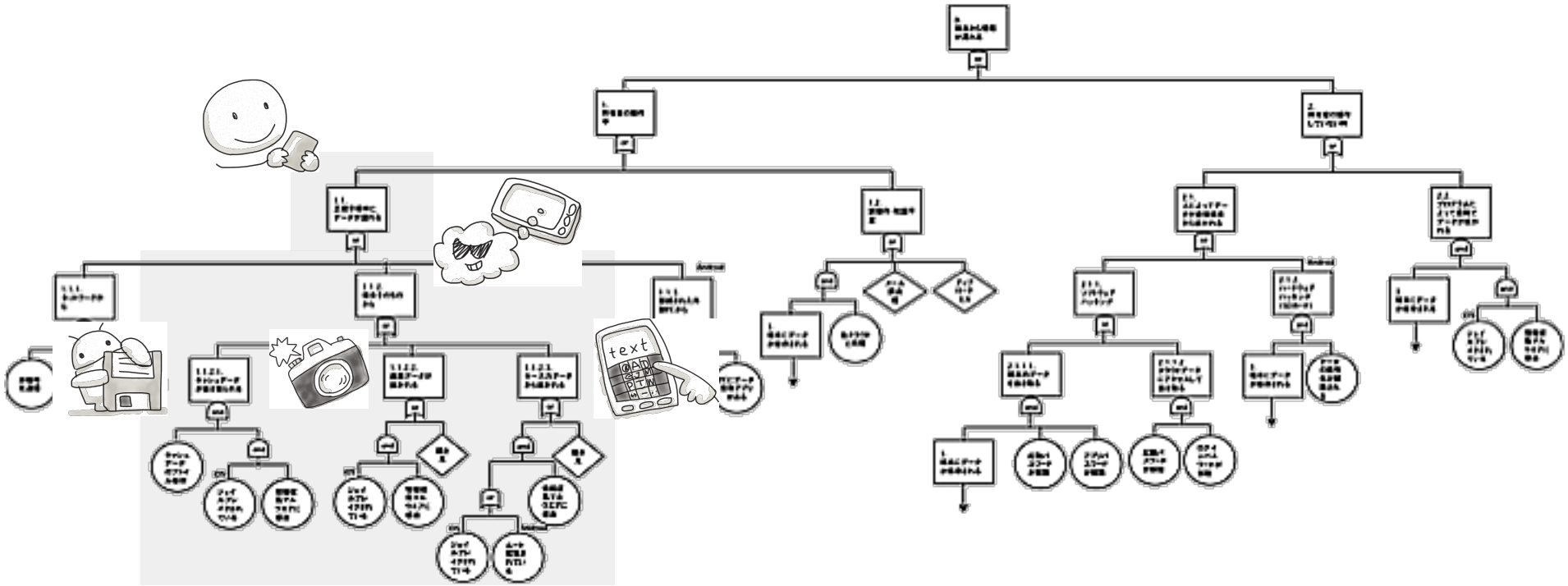
情報漏洩ケース1

なりすまし公衆無線LANから盗聴される





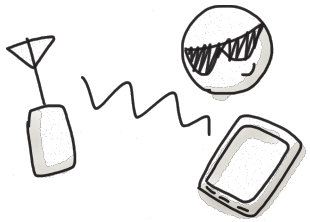
スマートフォンの業務クラウド利用における端末からの業務データの情報漏洩FTA



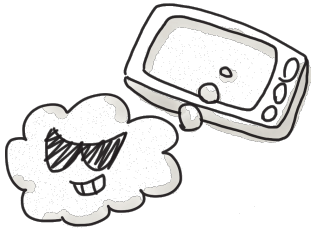
正規手順で

1.1.
正規手順中に
データが漏れる

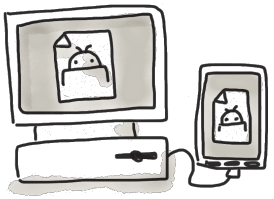
or



1.1.1.
ネットワークか
ら



1.1.2.
端末そのもの
から



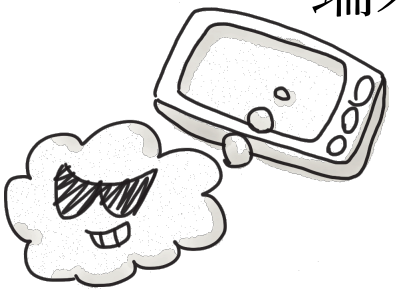
1.1.3.
接続された外
部PCから

ネットワーク
から漏洩

端末から
漏洩

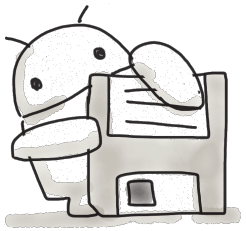
外部PC
から漏洩

端末から漏洩

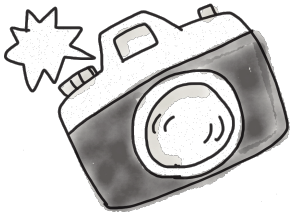


1.1.2.
端末そのものから

or

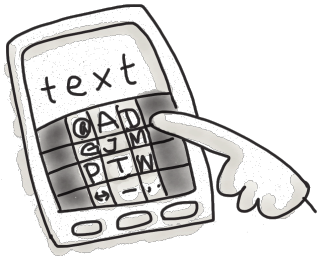


1.1.2.1.
キャシュデータが抜き取られる



1.1.2.2.
画面データが抜かれる

1.1.2.3.
キー入力データから抜かれる



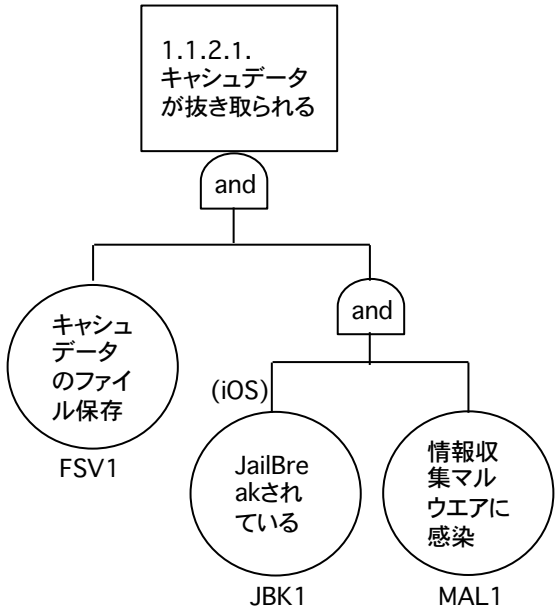
キャッシュデータが

スクリーンショットが

入力データが

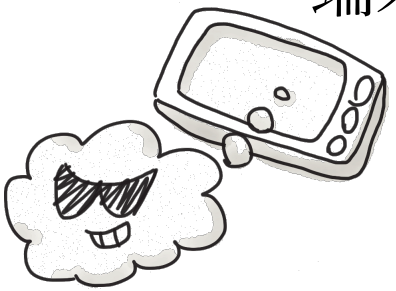
情報漏洩ケース2

アプリのキャッシュデータが
マルウェアにて抜き取られる①



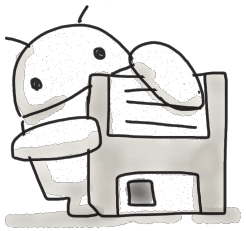
※ iOSはマルウェアに感染するためにはJailBreakされている前提があるので、JailBreakがand条件要素となります。→ P.86参照

端末から漏洩

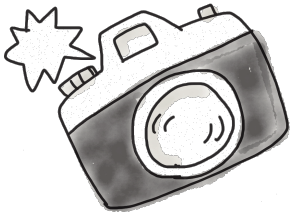


1.1.2.
端末そのものから

or

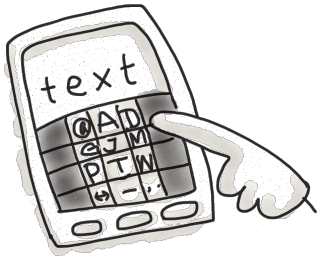


1.1.2.1.
キャシュデータが抜き取られる



1.1.2.2.
画面データが抜かれる

1.1.2.3.
キー入力データから抜かれる



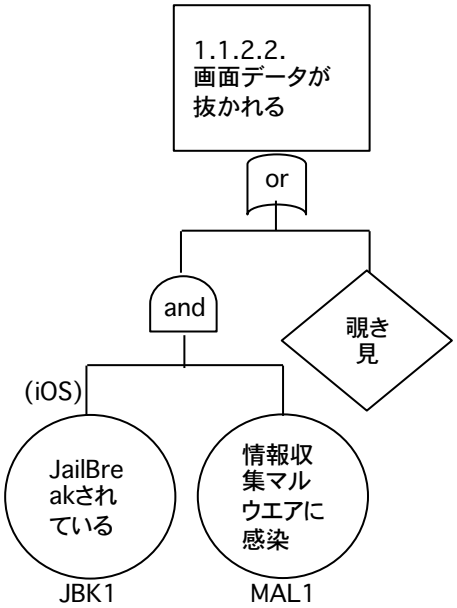
キャッシュデータが

スクリーンショットが

入力データが

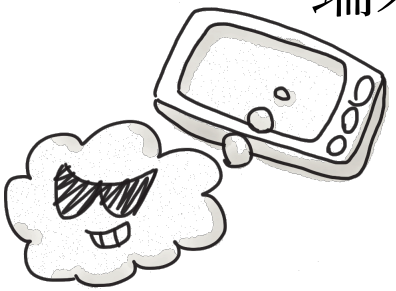
情報漏洩ケース3

操作中のスクリーンショットがマルウェアにて抜き取られる②



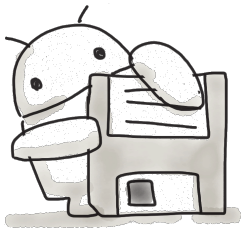
※ iOSはマルウェアに感染するためにはJailBreakされている前提があるので、JailBreakがand条件要素となります。→ P.86参照

端末から漏洩

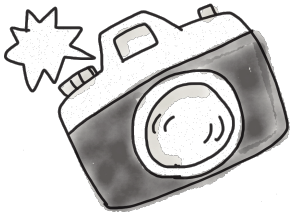


1.1.2.
端末そのもの
から

or

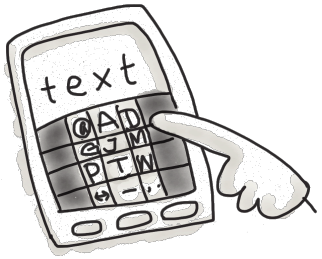


1.1.2.1.
キャシュデータ
が抜き取られる



1.1.2.2.
画面データが
抜かれる

1.1.2.3.
キー入力データ
から抜かれる



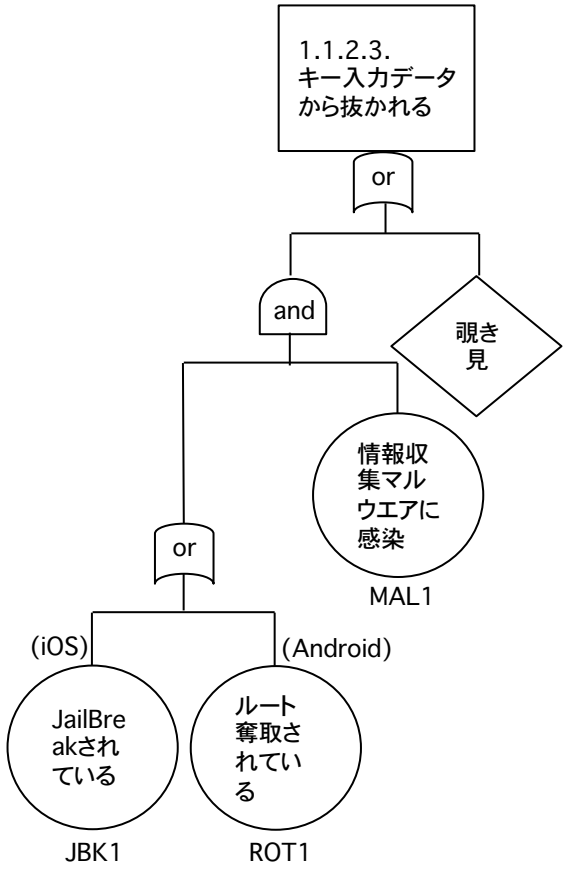
キャッシュ
データが

スクリーン
ショットが

入力
データが

情報漏洩ケース4

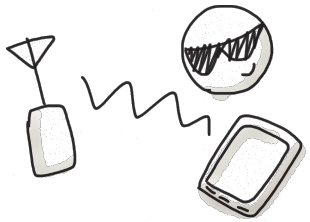
操作中の入力データが
マルウェアにて抜き取られる③



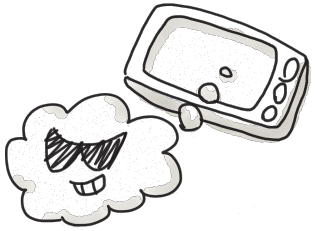
正規手順で

1.1.
正規手順中に
データが漏れる

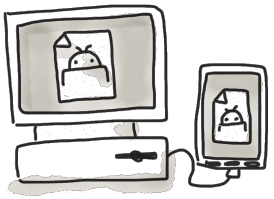
or



1.1.1.
ネットワークか
ら



1.1.2.
端末そのもの
から



1.1.3.
接続された外
部PCから

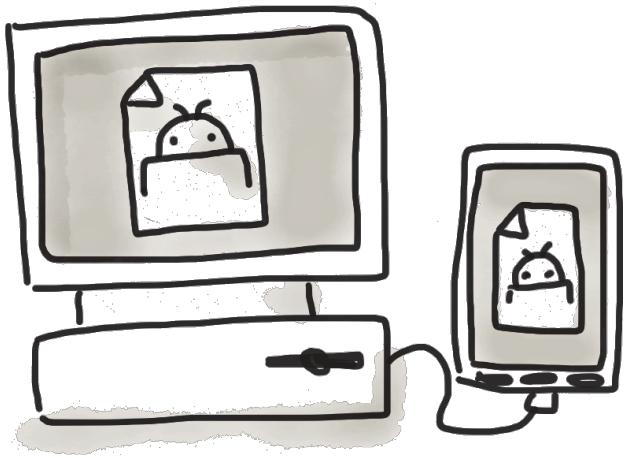
ネットワーク
から漏洩

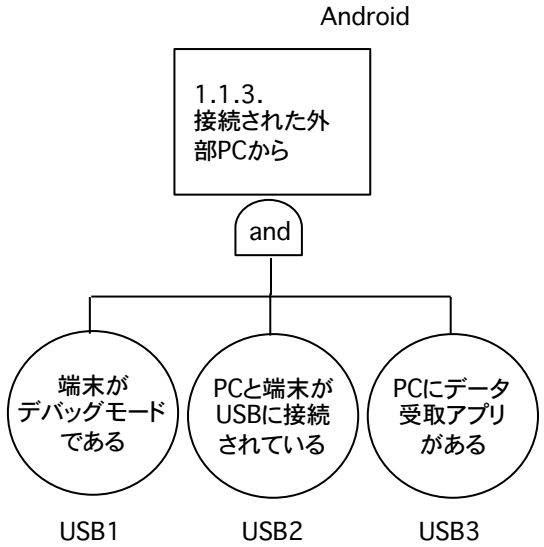
端末から
漏洩

外部PC
から漏洩

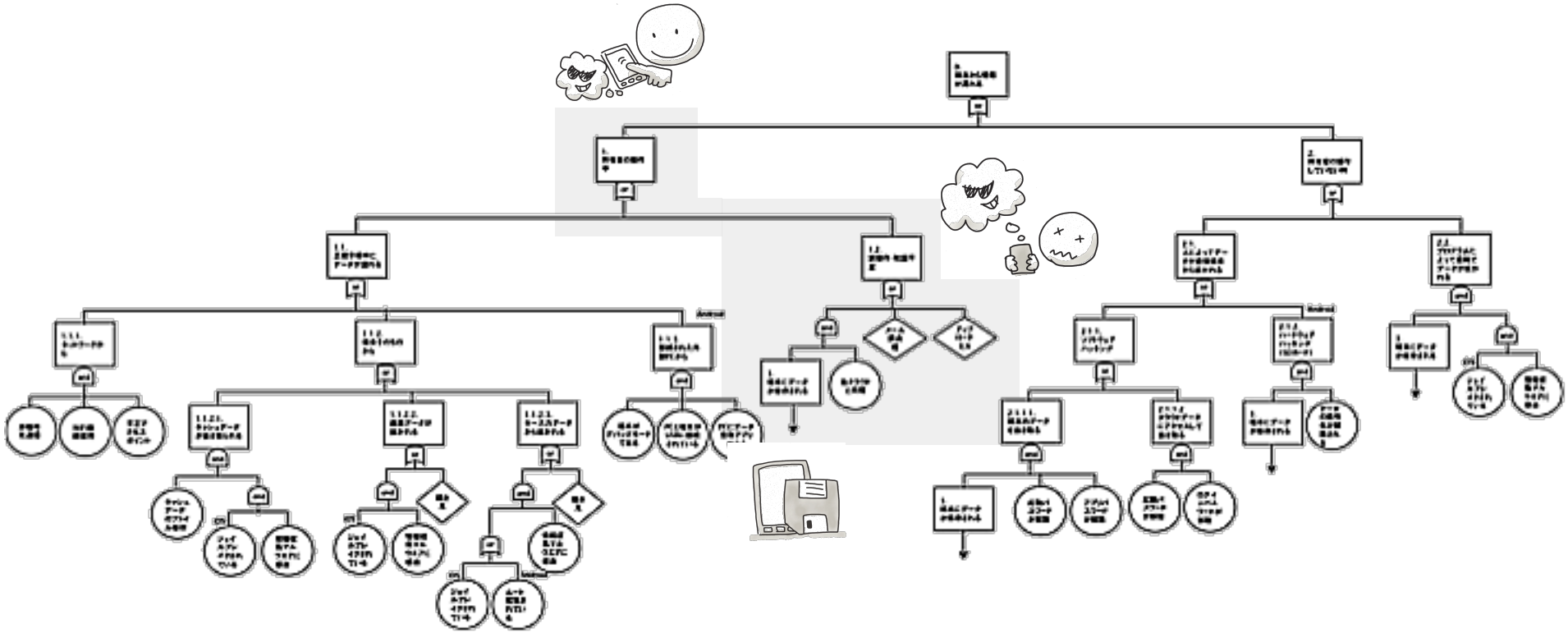
情報漏洩ケース5

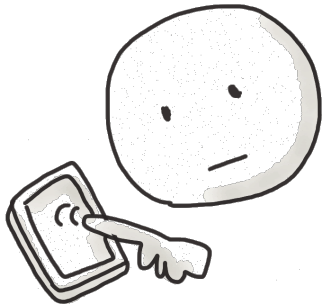
操作中の入力データが
外部PCに転送される





スマートフォンの業務クラウド利用における端末からの業務データの情報漏洩FTA





端末操作中に

1.
所有者の操作中

or

1.1.
正規手順中にデータが漏れる

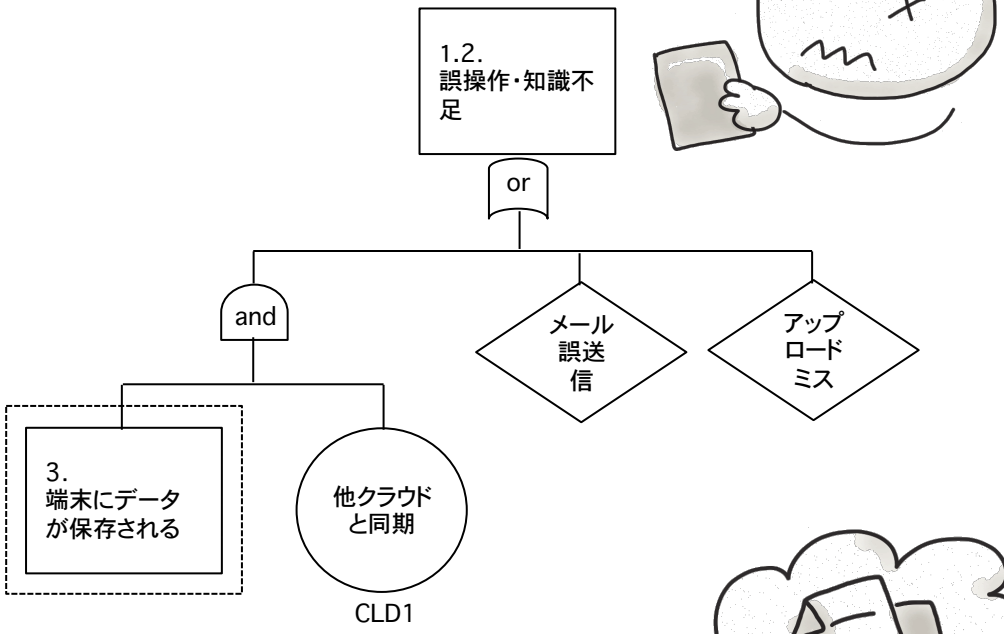
1.2.
誤操作・知識不足

正規手順で
漏洩する

誤操作で
漏洩する

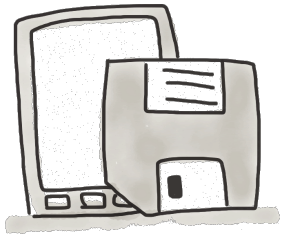
誤操作で

保存されていた
データが



勝手にアップ
ロードされる

データを保存する



3.
端末にデータ
が保存される

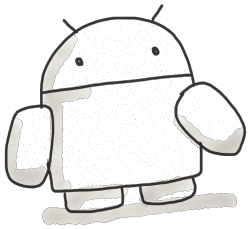
or

3.1.
アプリ機能とし
てデータが保
存される

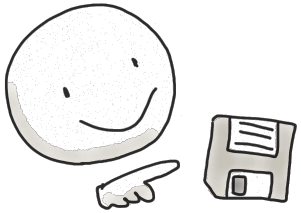
3.2.
アプリ機能外で
ユーザーが意
図的にデータを
保存する

3.3.
アプリ機能外で
ユーザーが意
図せずデータ
が保存される

アプリが



ユーザーが
意図して



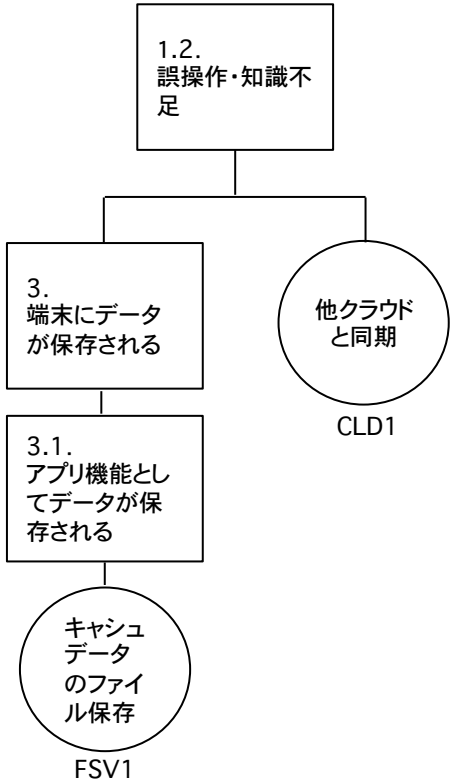
ユーザーが
意図せず

※ クラウド接続アプリはマスターデータは端末には保存しませんが、オフライン作業のために端末（SDカードなど）に一部キャッシュデータを保存する場合があります。本ケースではこのように仕様として端末に保存されるキャッシュデータを想定しています。

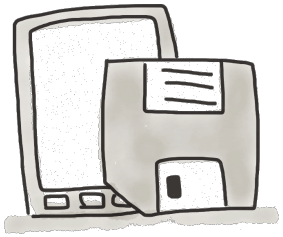
情報漏洩ケース6

アプリのキャッシュデータが、

他クラウドと同期して漏洩する①



データを保存する



3.
端末にデータ
が保存される

or

3.1.
アプリ機能とし
てデータが保
存される

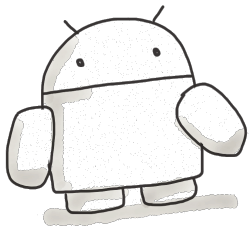
3.2.
アプリ機能外で
ユーザーが意
図的にデータを
保存する

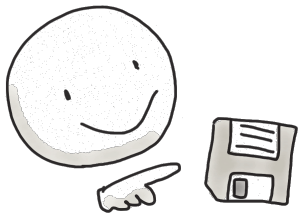
3.3.
アプリ機能外で
ユーザーが意
図せずデータ
が保存される

アプリが

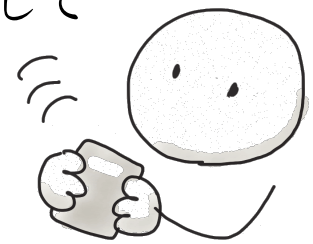
ユーザーが
意図して

ユーザーが
意図せず





ユーザーが意図して



3.2.
アプリ機能外でユーザーが意図的にデータを保存する

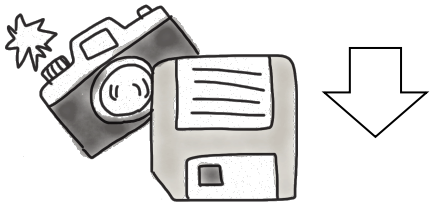
or

3.2.1.
端末デフォルトの保存機能使用

3.2.2.
非公式アプリによるデータ保存

3.2.3.
公式アプリによるデータ保存

端末機能で保存



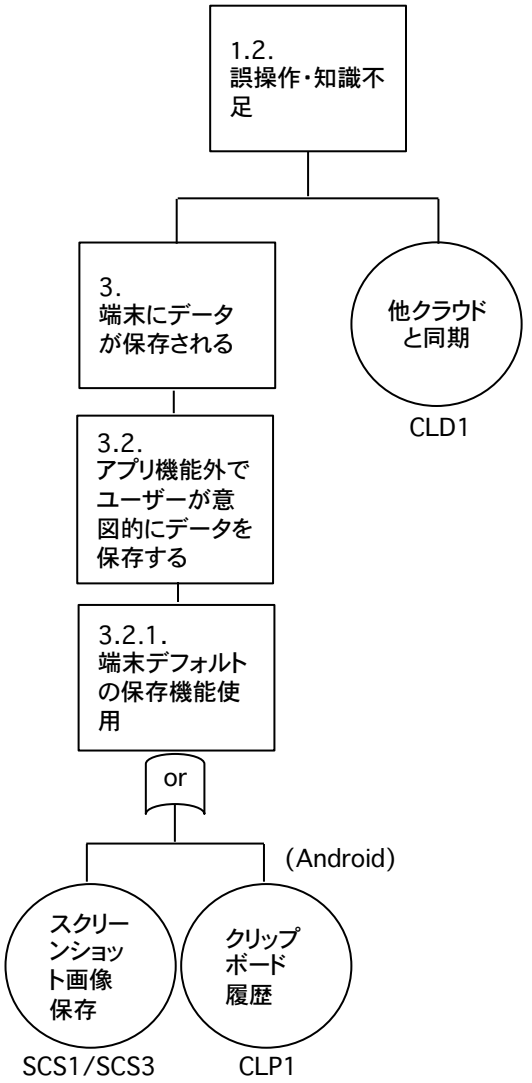
非公式アプリで保存

公式アプリで保存

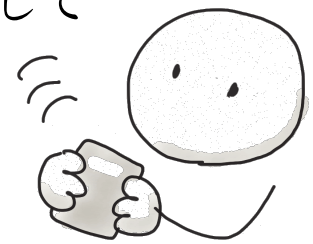
情報漏洩ケース7

端末機能で保存したデータが、

他クラウドと同期して漏洩する②



ユーザーが意図して



3.2.
アプリ機能外でユーザーが意図的にデータを保存する

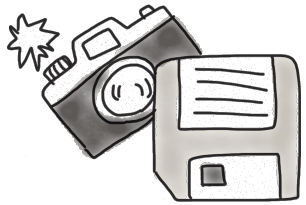
or

3.2.1.
端末デフォルトの保存機能使用

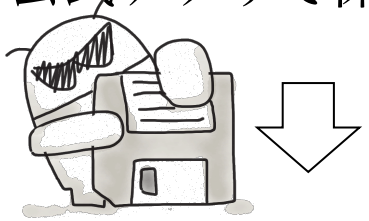
3.2.2.
非公式アプリによるデータ保存

3.2.3.
公式アプリによるデータ保存

端末機能で保存



非公式アプリで保存

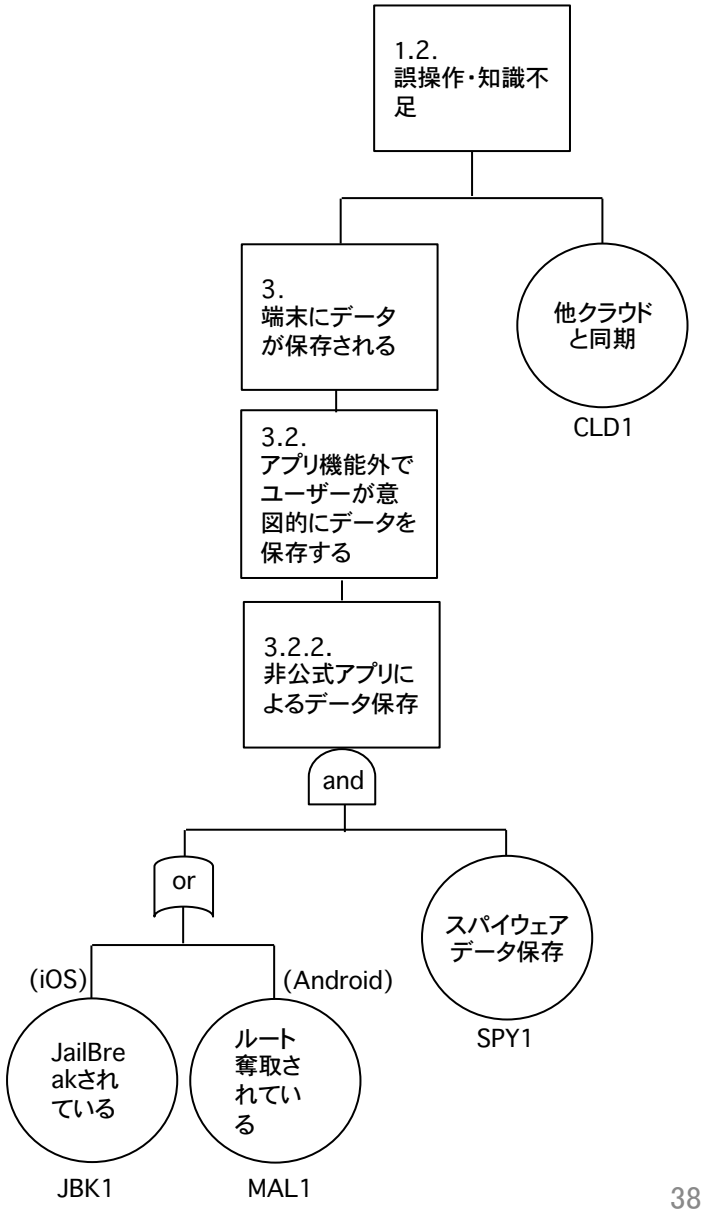


公式アプリで保存

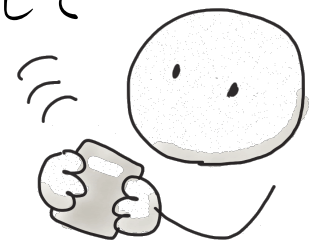
情報漏洩ケース8

非公式アプリによる保存データが

他クラウドと同期して漏洩する③



ユーザーが意図して



3.2.
アプリ機能外でユーザーが意図的にデータを保存する

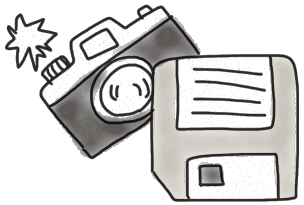
or

3.2.1.
端末デフォルトの保存機能使用

3.2.2.
非公式アプリによるデータ保存

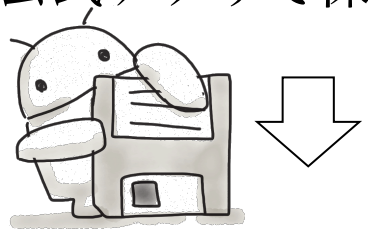
3.2.3.
公式アプリによるデータ保存

端末機能で保存



非公式アプリで保存

公式アプリで保存

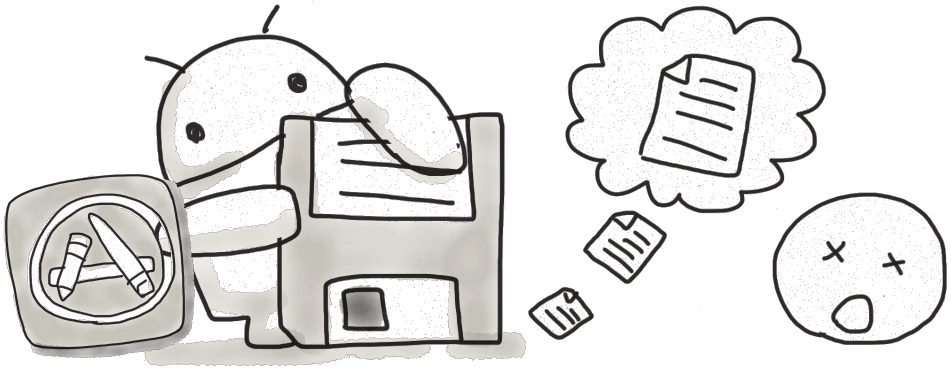


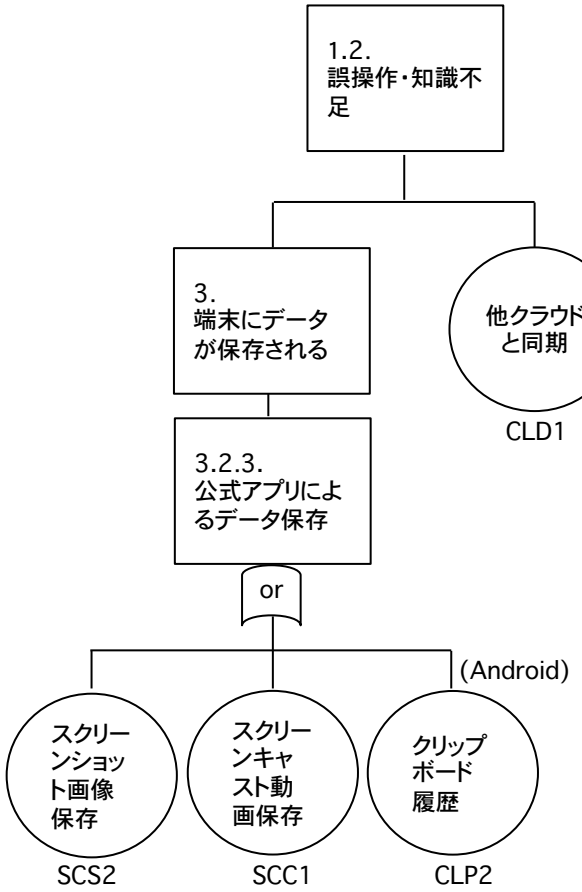
※ 公式アプリとはOSベンダーが提供しているアプリケーションを指します。
例）App Store, Google Play

情報漏洩ケース9

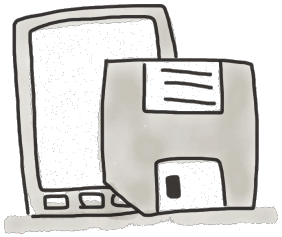
公式アプリによる保存データが、

他のクラウド同期して漏洩する④





データを保存する



3.
端末にデータ
が保存される

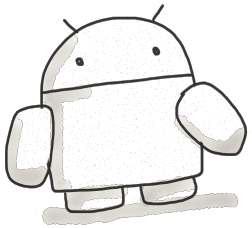
or

3.1.
アプリ機能とし
てデータが保
存される

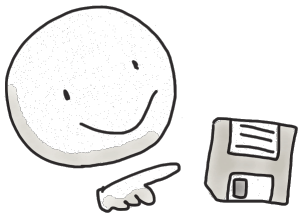
3.2.
アプリ機能外で
ユーザーが意
図的にデータを
保存する

3.3.
アプリ機能外で
ユーザーが意
図せずデータ
が保存される

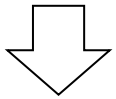
アプリが



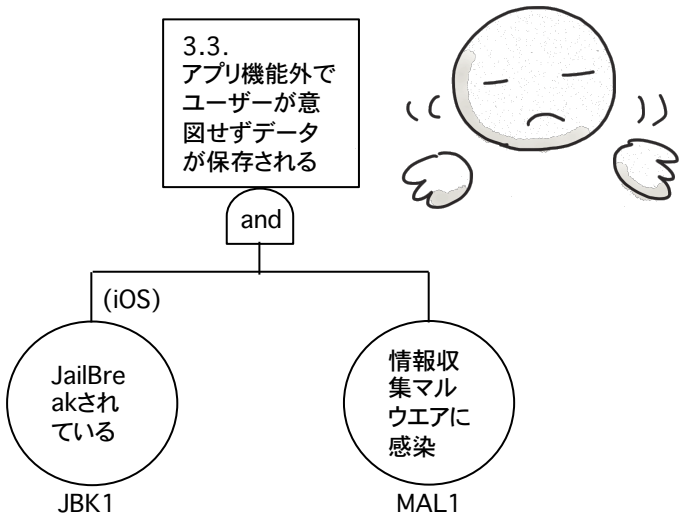
ユーザーが
意図して



ユーザーが
意図せず



ユーザーが意図せず



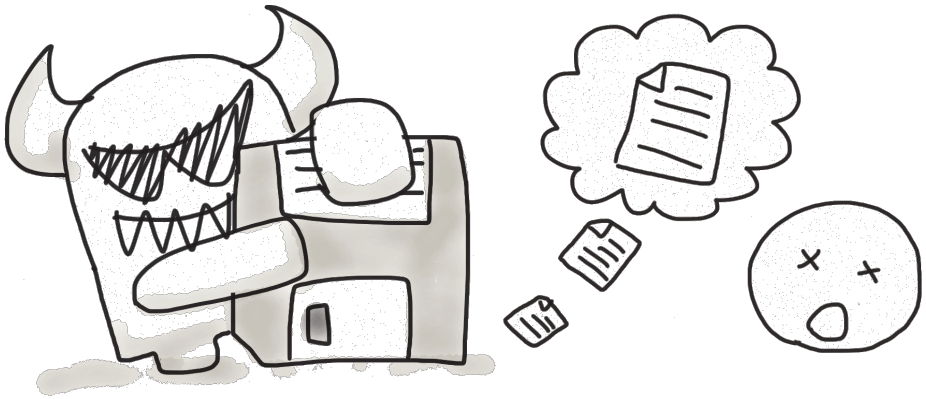
マルウェアが保存

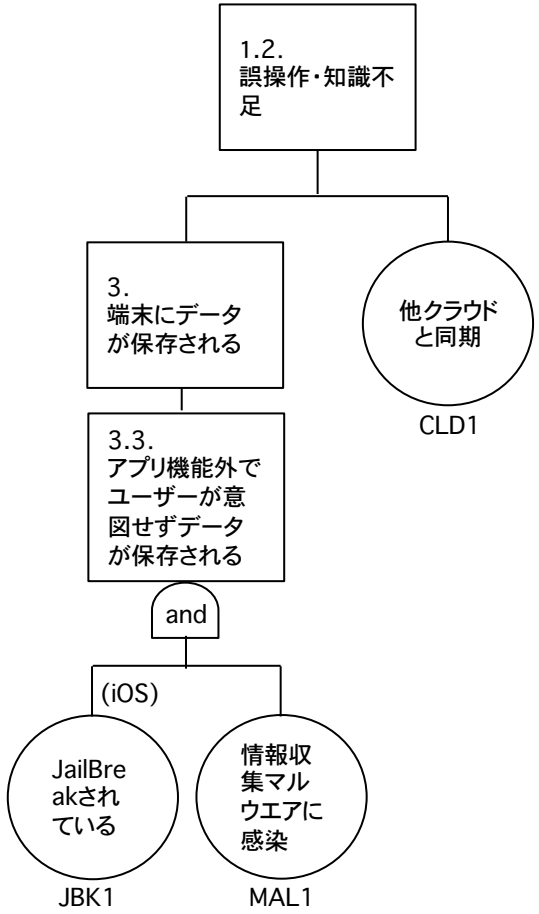
※ iOSはマルウェアに感染するためにはJailBreakされている前提があるので、JailBreakがand条件要素となります。→ P.86参照
※ ユーザーが意図せずデータが保存されるとは、スパイウェアの機能を有したマルウェアが技術的に可能であることから想定しています。→ P.82参照

情報漏洩ケース10

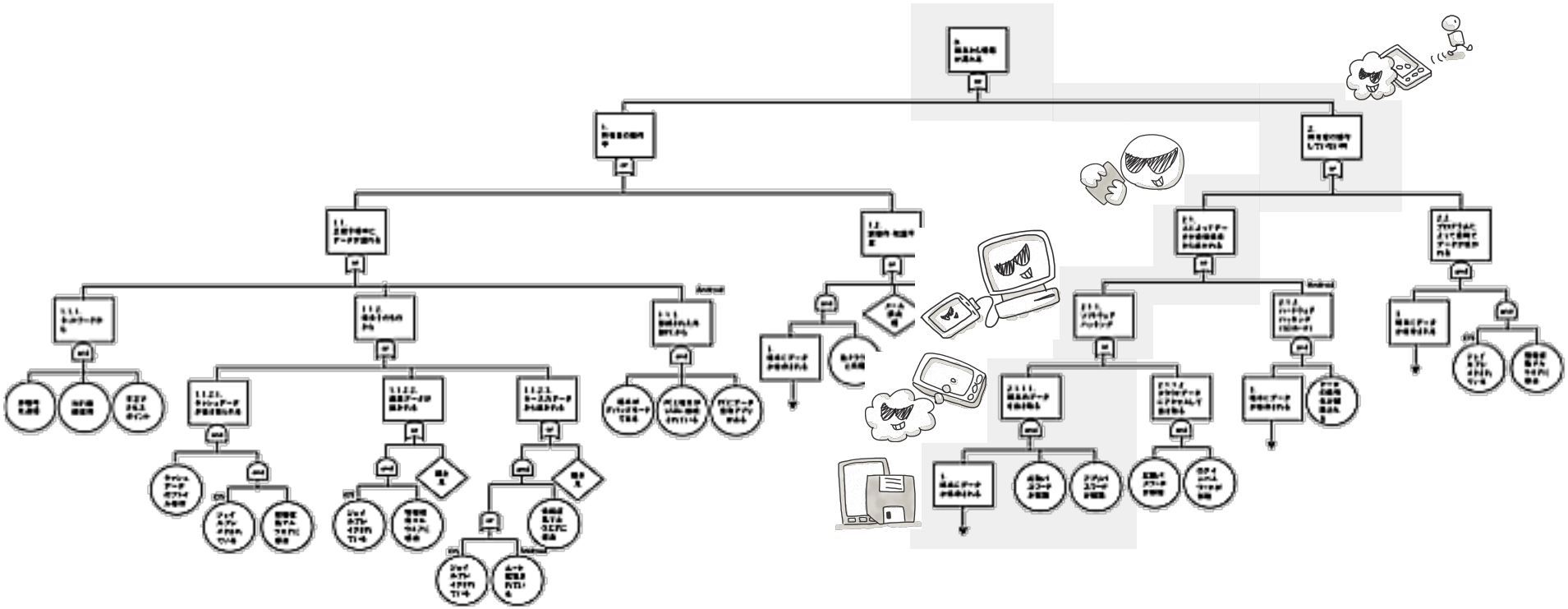
マルウェアが保存したデータが、

他クラウドと同期して漏洩する⑤

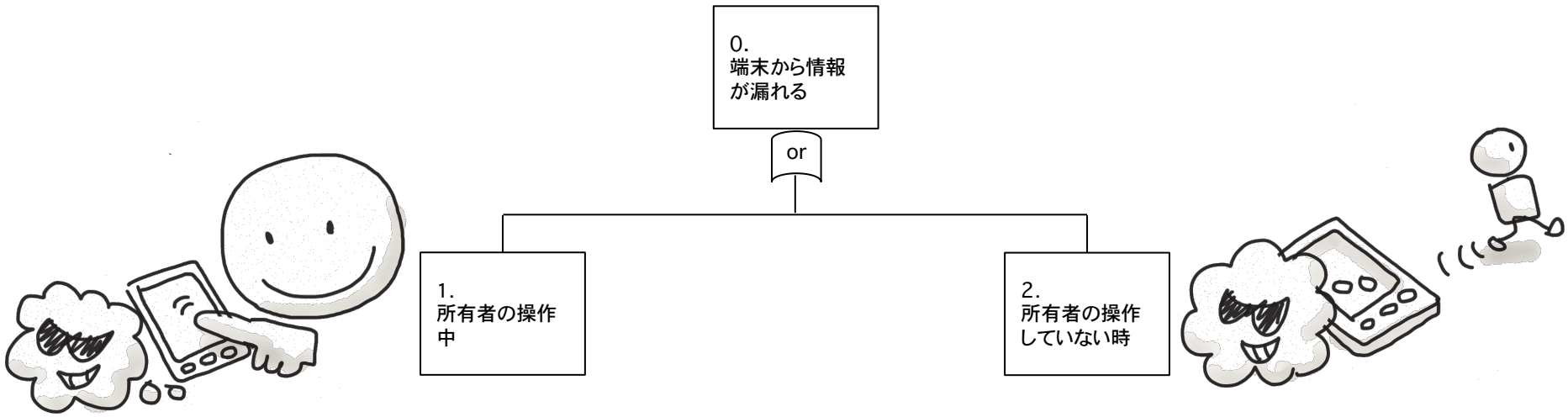




スマートフォンの業務クラウド利用における端末からの業務データの情報漏洩FTA

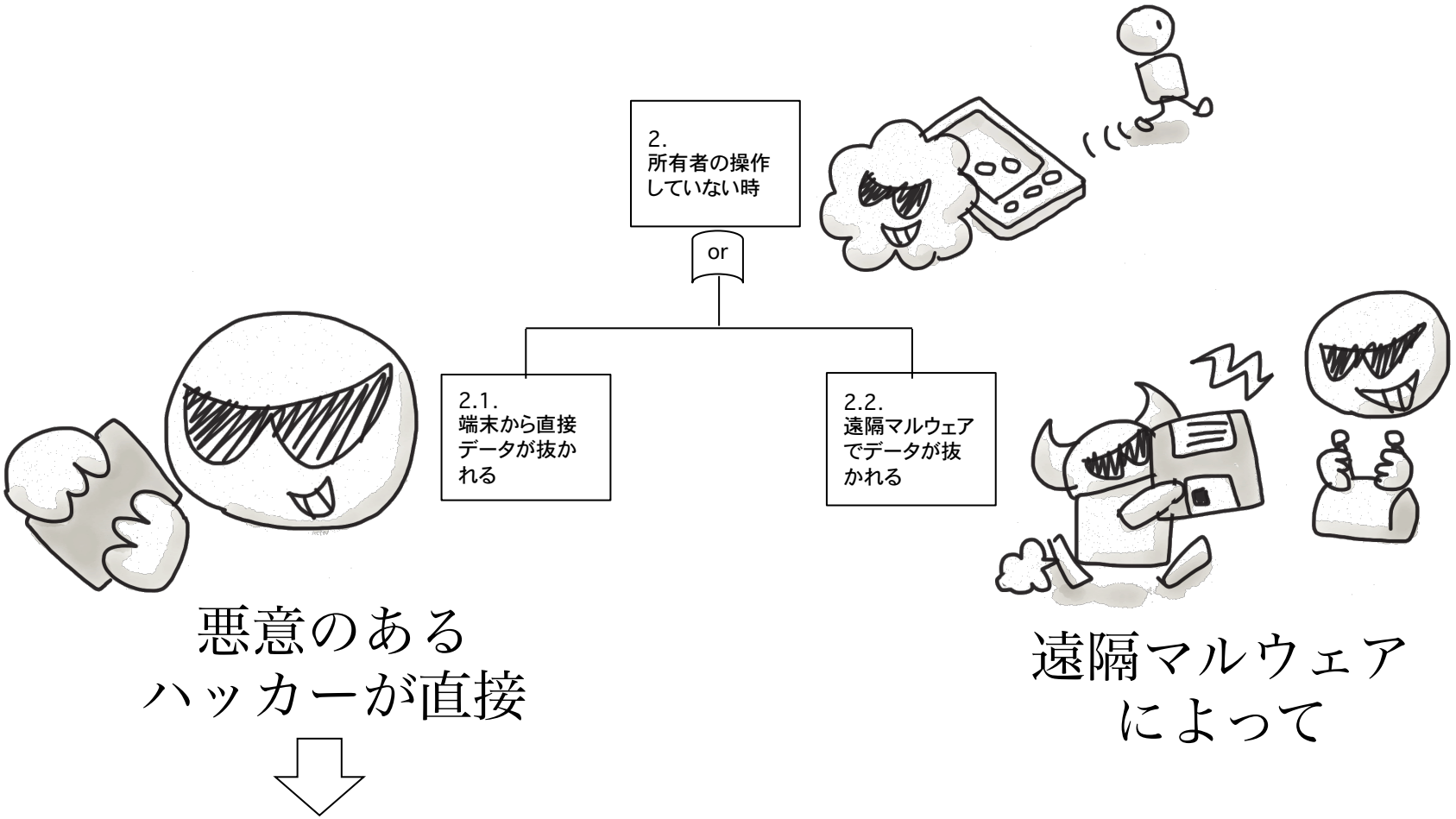


情報が漏洩する

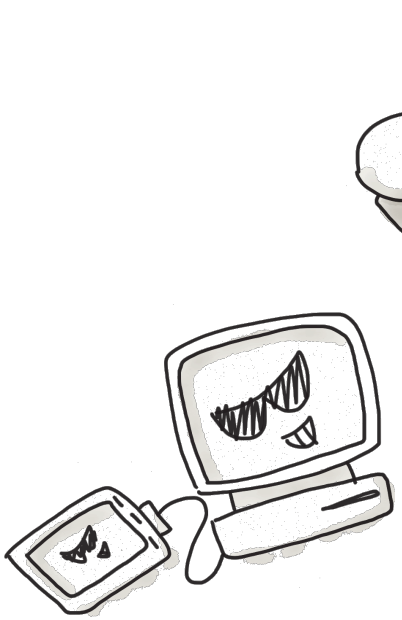


端末操作中に　　手から離れている間に

手から離れている間に


2.
所有者の操作
していない時
or
2.1.
端末から直接
データが抜か
れる
2.2.
遠隔マルウェア
でデータが抜
かれる
悪意のある
ハッカーが直接
遠隔マルウェア
によって

悪意のあるハッカーによって



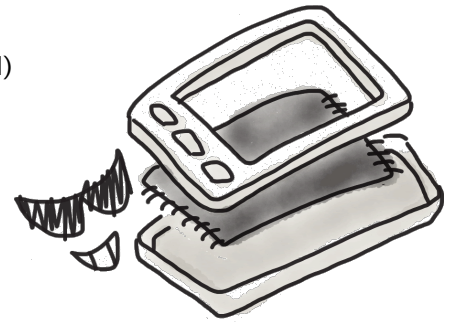
2.1.
人によってデータが直接端末から抜かれる

or

2.1.1.
ソフトウェアハッキング

(Android)

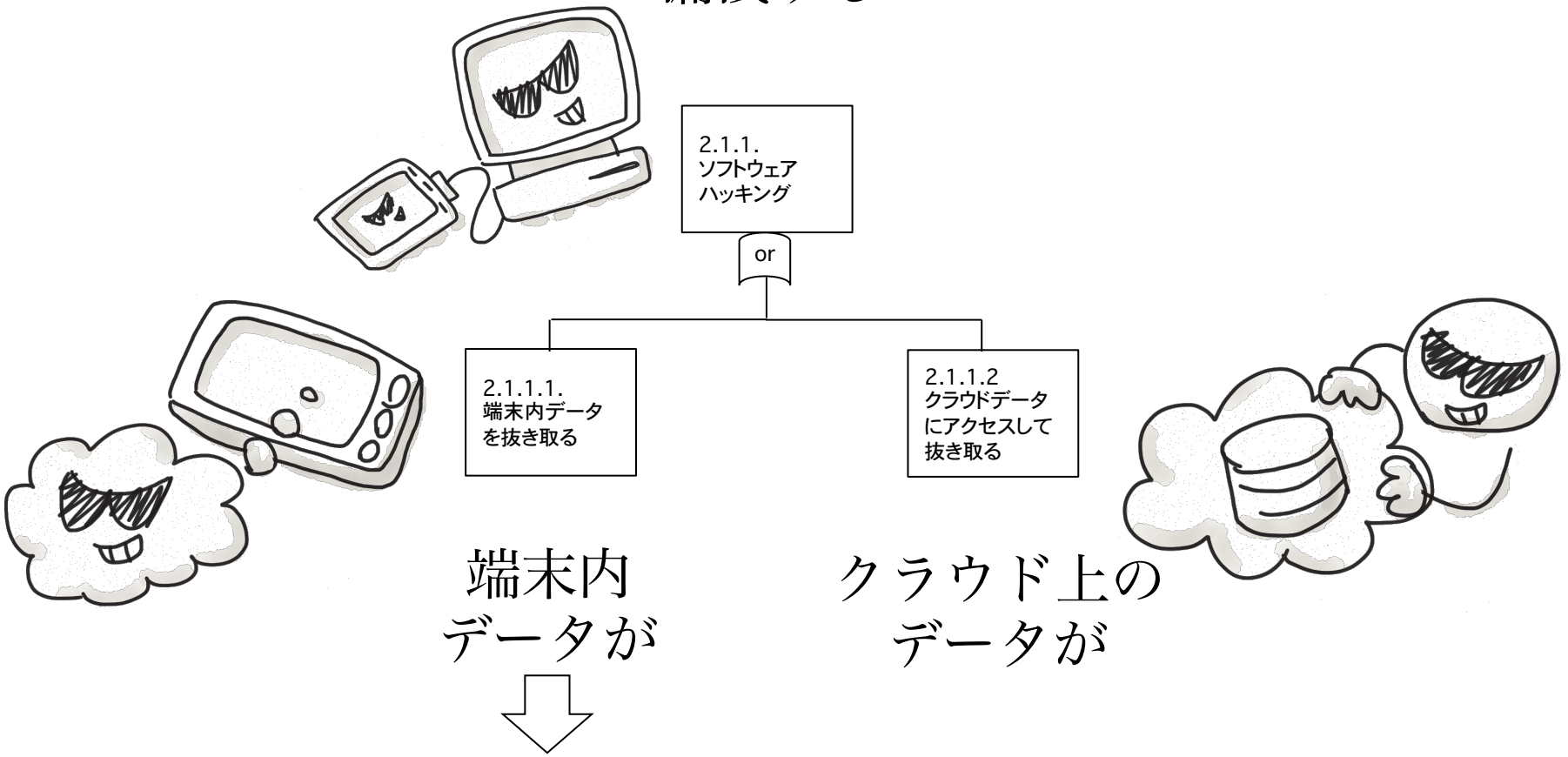
2.1.2.
ハードウェアハッキング
(SDカード)



端末が操作されて
漏洩する

SDカードが抜かれて
漏洩する

端末が操作されて
漏洩する



端末内データが

2.1.1.1.
端末内データを抜き取る

and

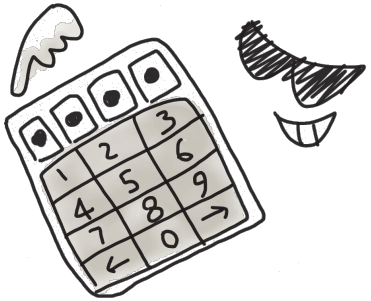
3.
端末にデータが保存される

起動パスワードが解除

PWD1

データの暗号化が解除

PWD2



端末に保存されたデータが

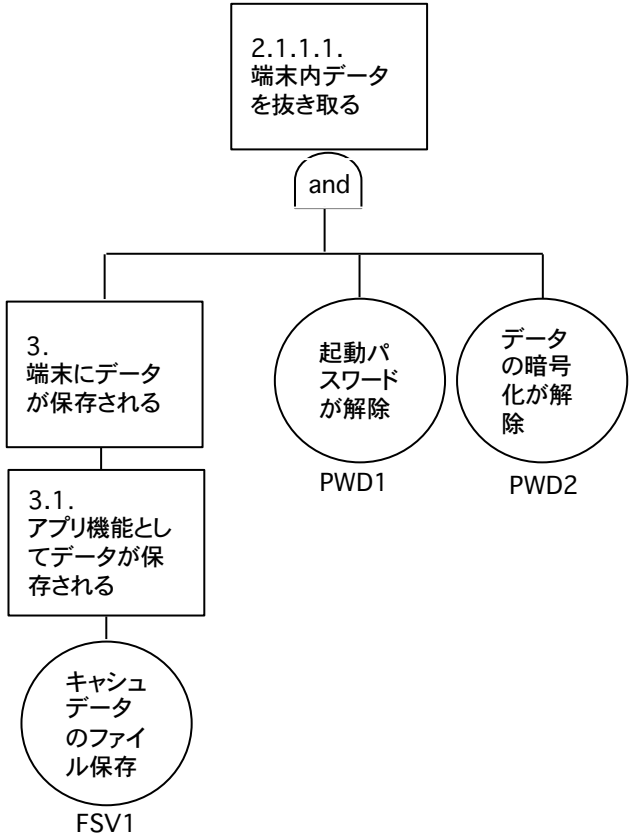
ハッキングされて盗み出される

情報漏洩ケース11～15へ

情報漏洩ケース11

アプリのキャッシュデータが、

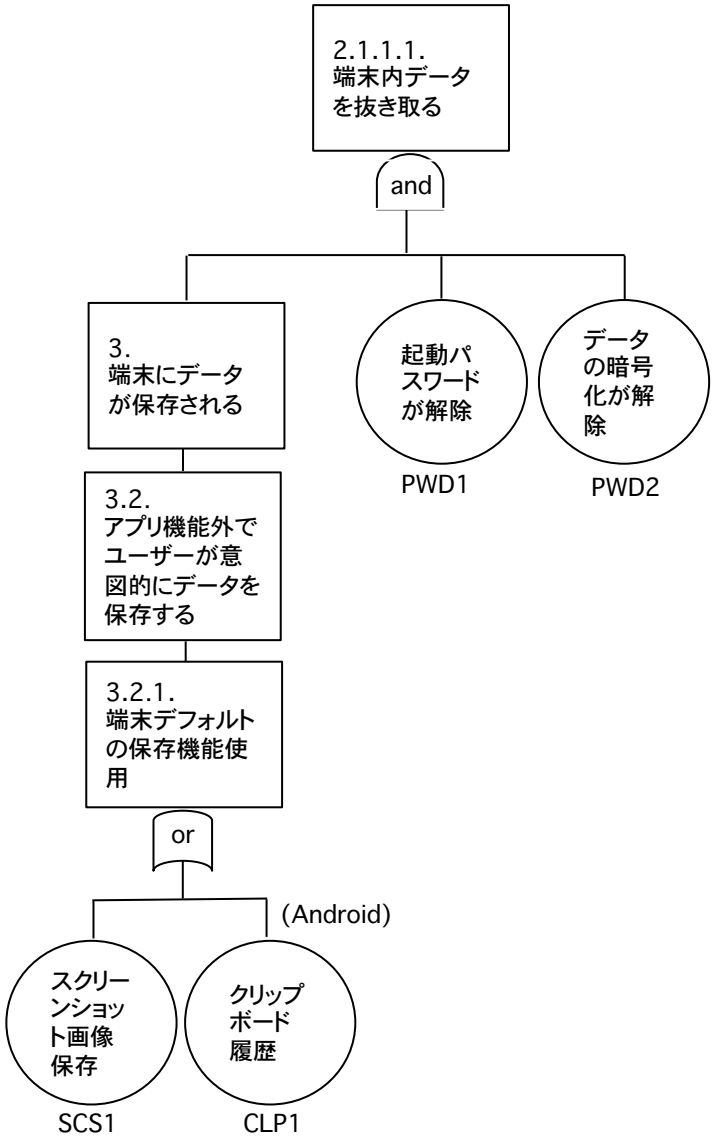
ハッキングされて盗み出される①



情報漏洩ケース12

端末機能で保存したデータが、

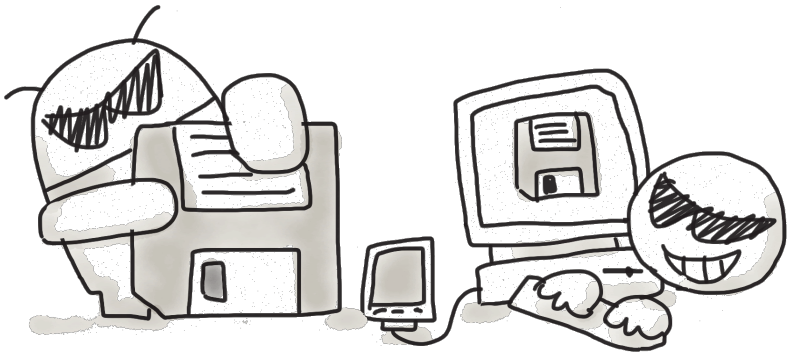
ハッキングされて盗み出される②

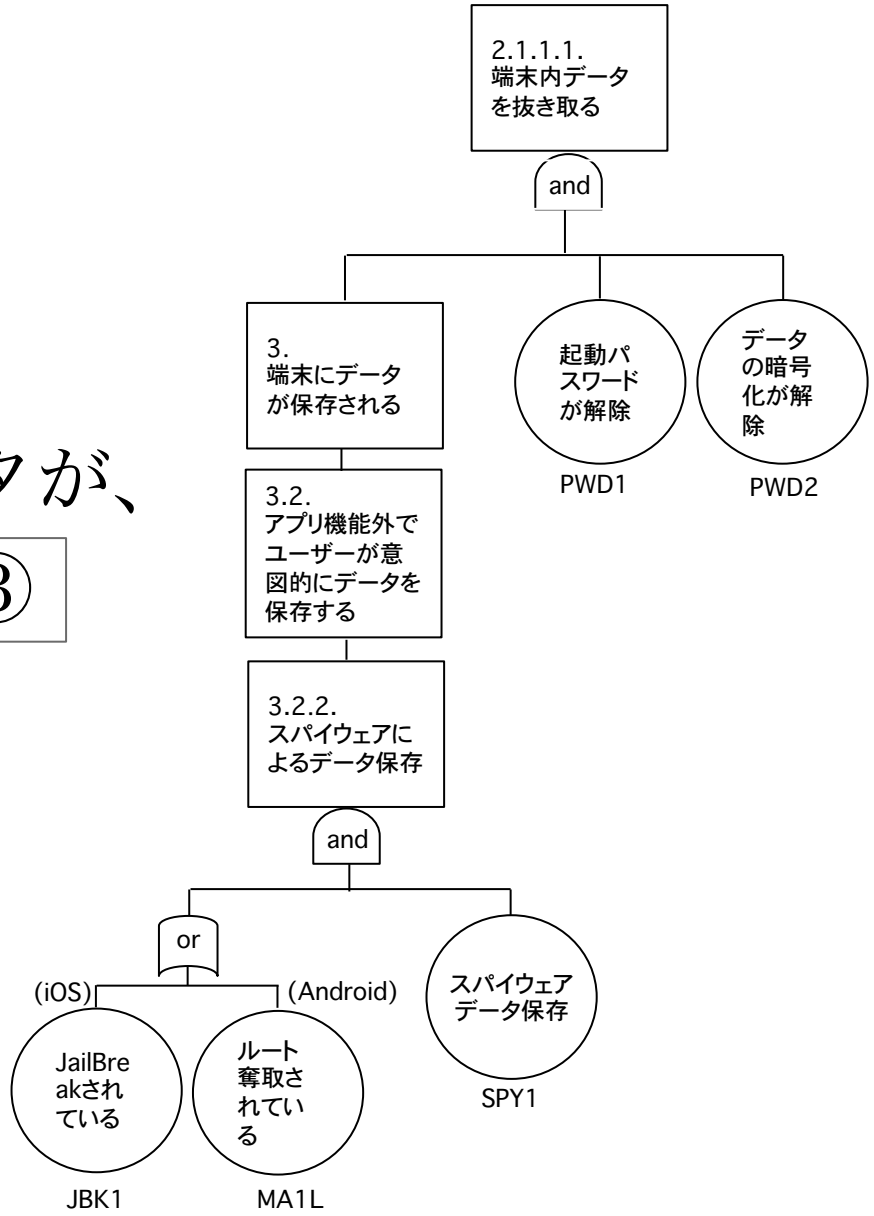


情報漏洩ケース13

スパイウェアが保存したデータが、

ハッキングして盗み出される③



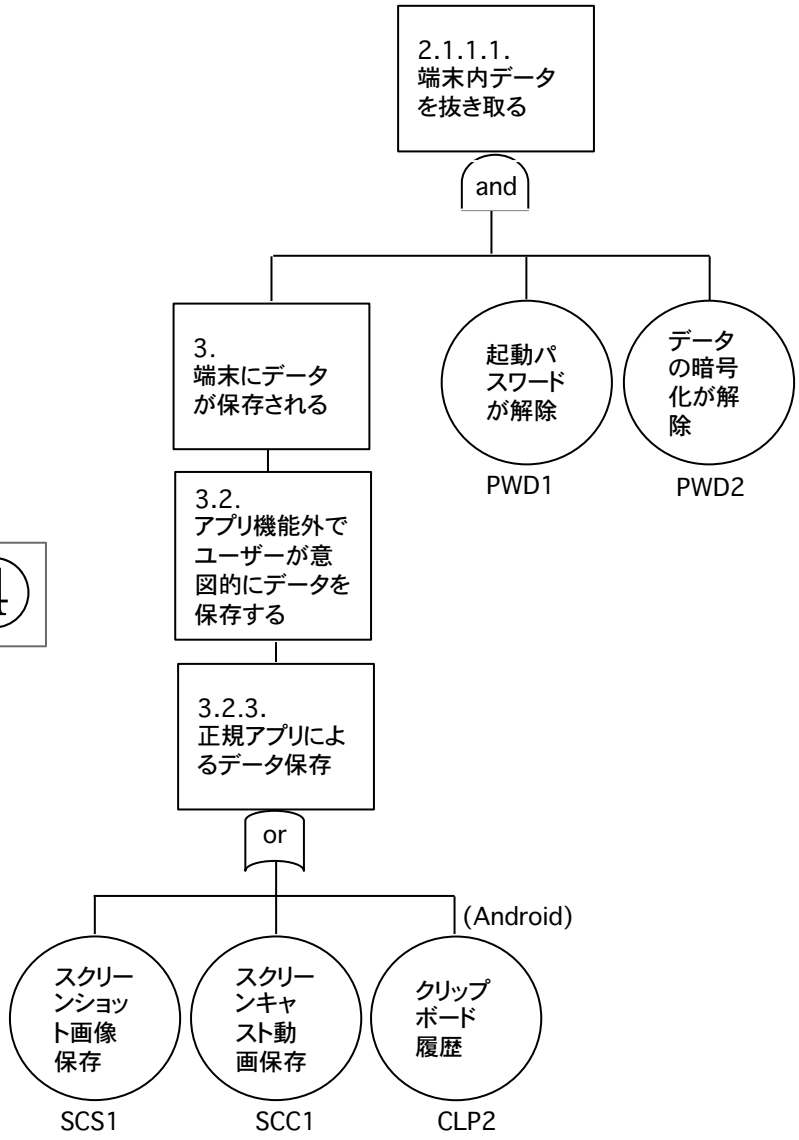


※ スパイウェアとマルウェアの違いはユーザーがインストールの意図に有無によって区別されます。スパイウェアは端末の所有者が操作中のデータを保存したり特定のサーバーに送信させることを意図して端末にインストールします。

情報漏洩ケース14

公式アプリで保存したデータが、

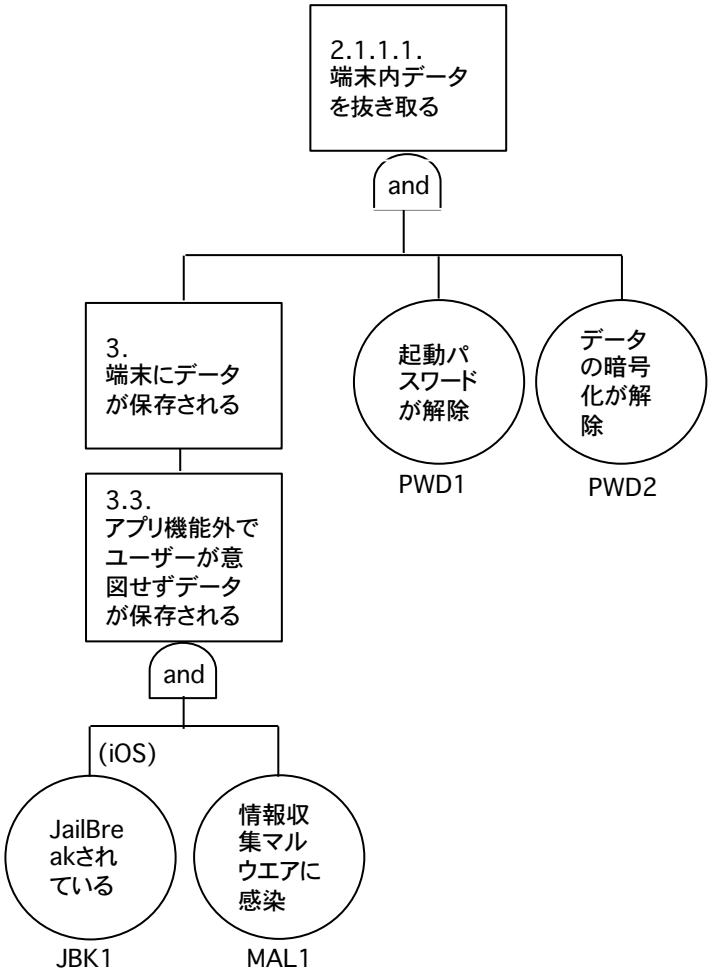
ハッキングされて盗み出される④



情報漏洩ケース15

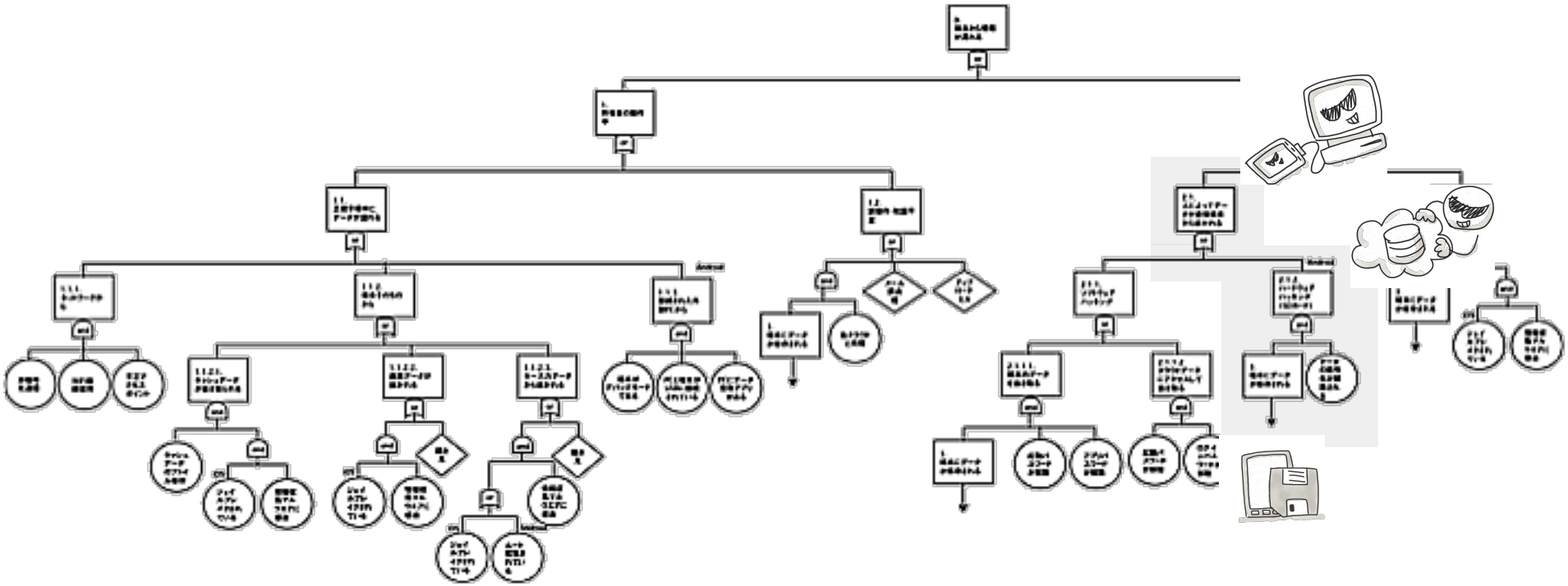
マルウェアが保存したデータが、

ハッキングされて盗み出される⑤

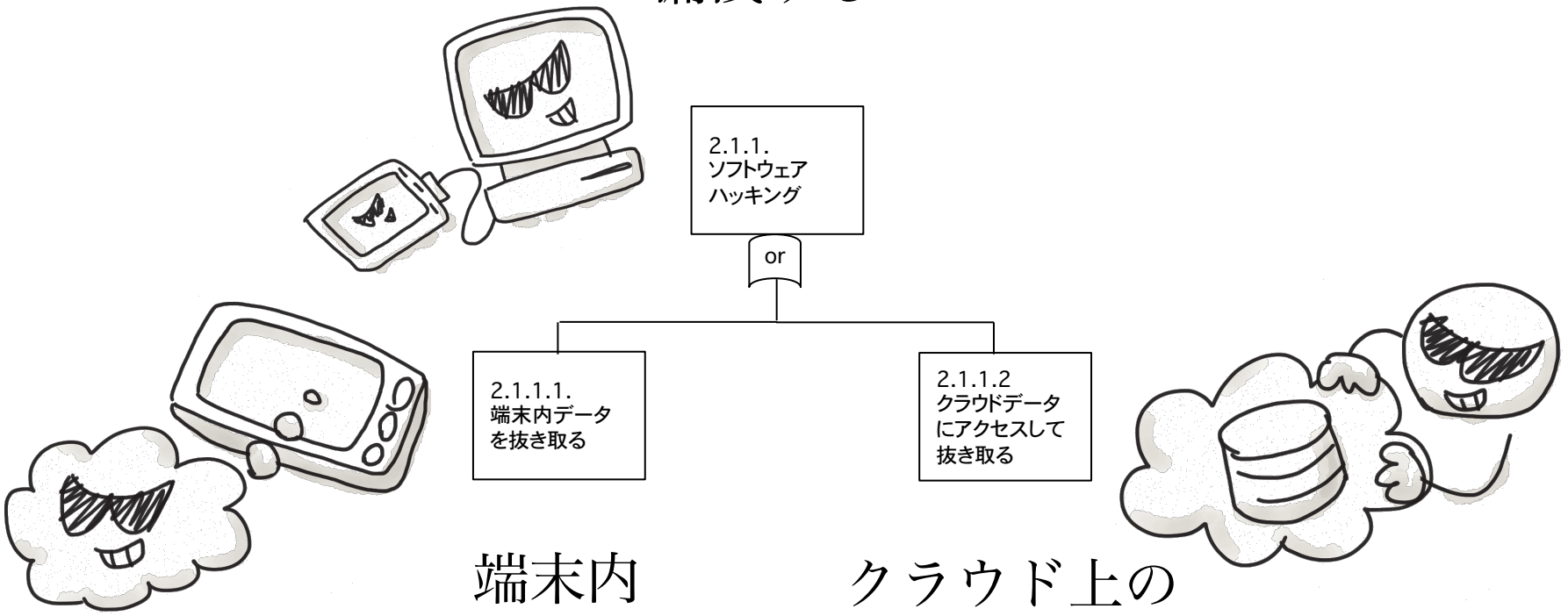


※ iOSはマルウェアに感染するためにはJailBreakされている前提があるので、JailBreakがand条件要素となります。→ P.86参照

スマートフォンの業務クラウド利用における端末からの業務データの情報漏洩FTA

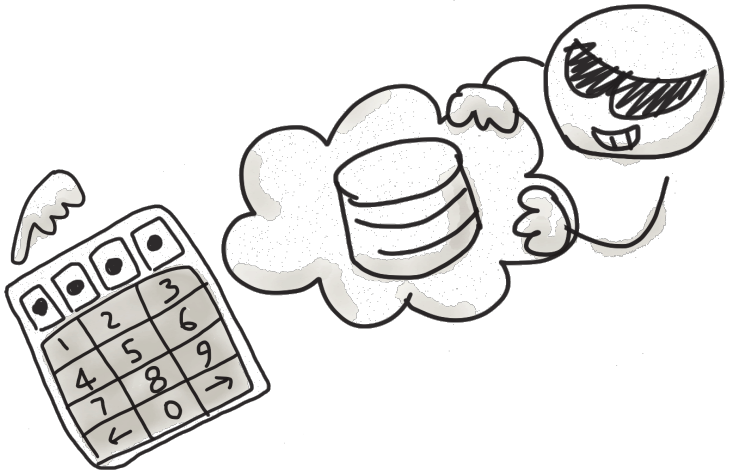


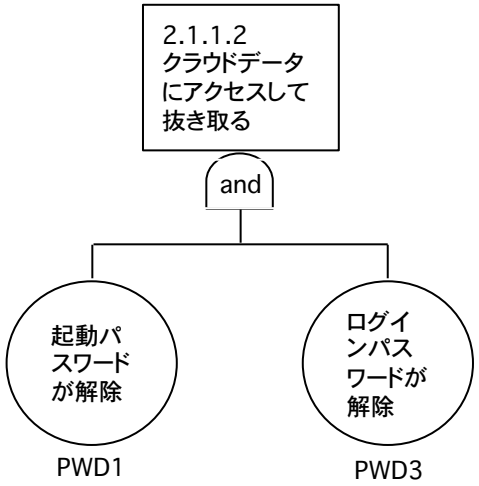
端末が操作されて
漏洩する



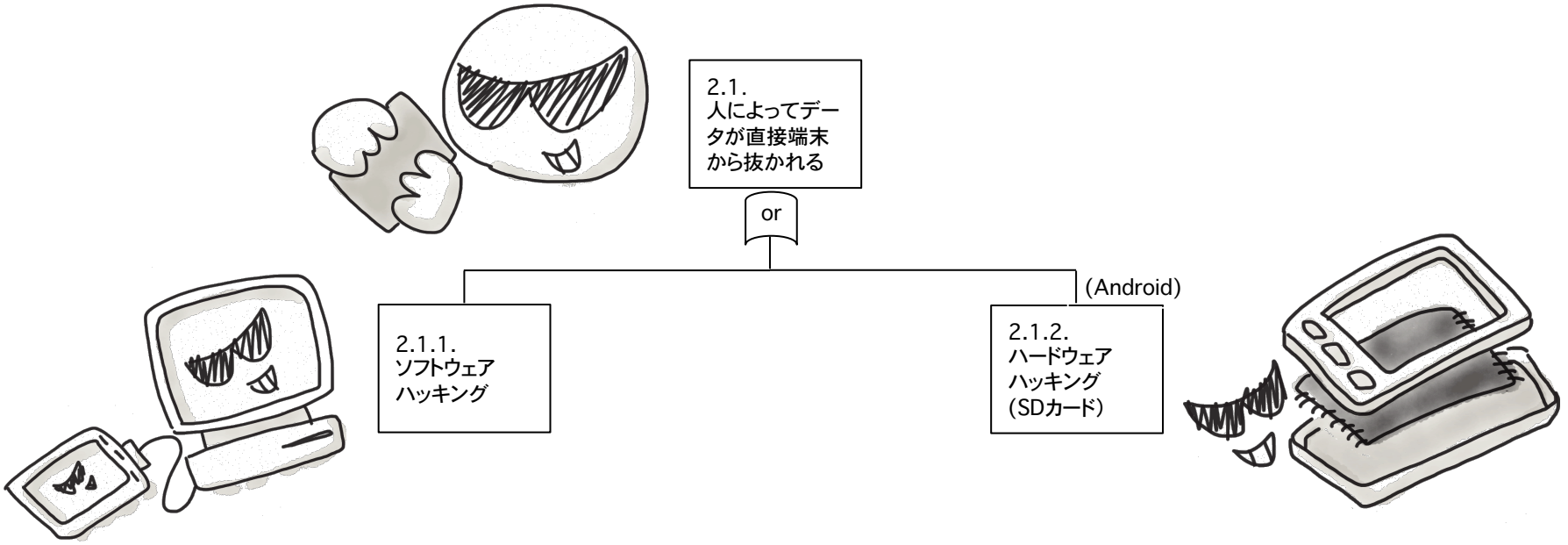
情報漏洩ケース16

クラウドへの
なりすましログインで
データを盗みだされる





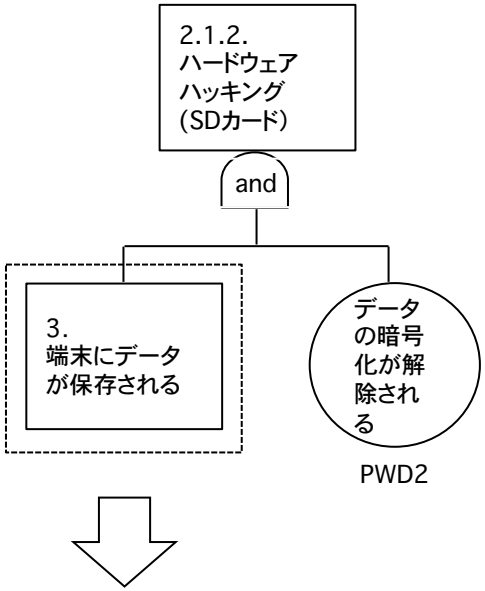
悪意のあるハッカーによって



端末が操作されて
漏洩する

SDカードが抜かれて
漏洩する

SDカードのデータが



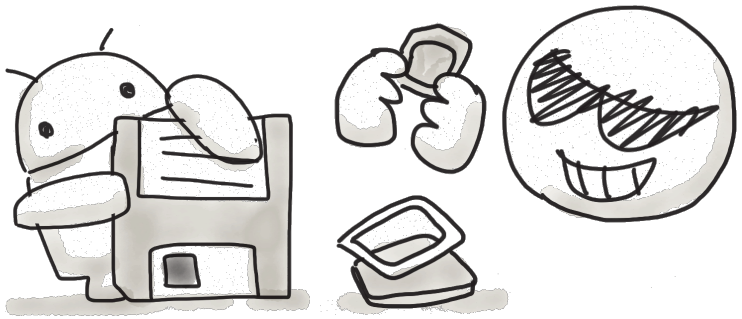
端末に保存されたデータが

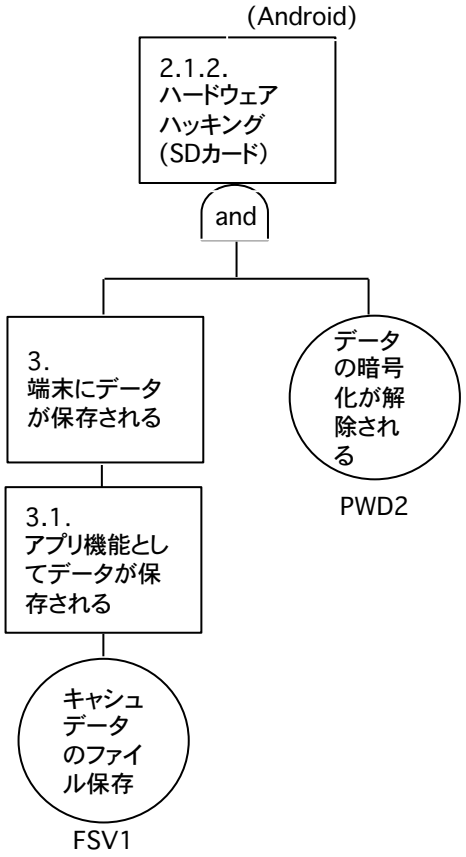
SDカードと共に抜き取られる

情報漏洩ケース17～21へ

情報漏洩ケース17

キャッシュ保存されたデータが SDカードと共に抜き取られる①



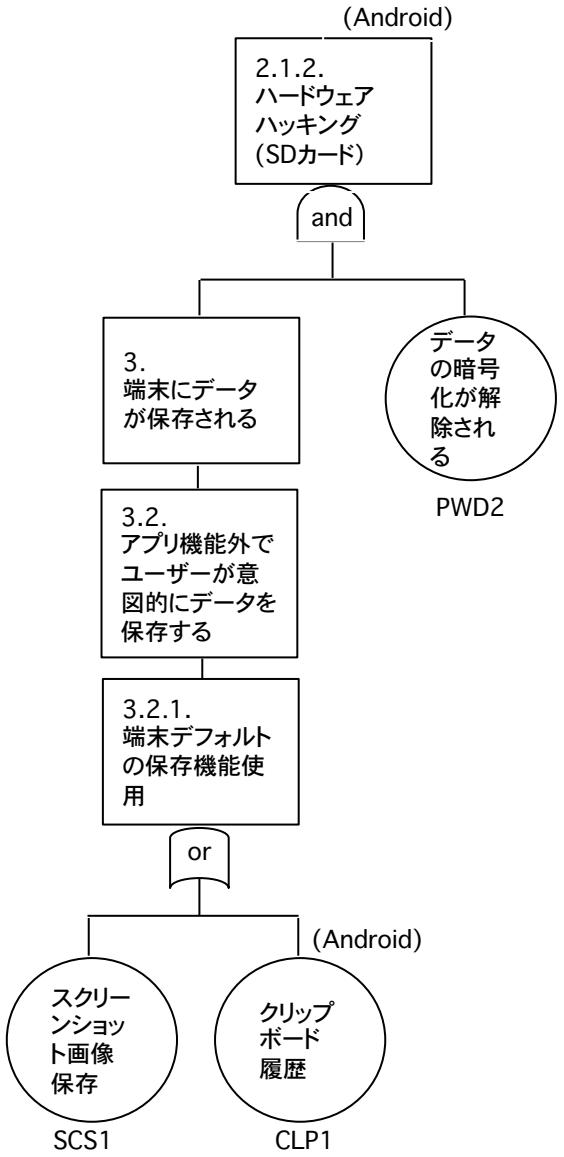


※ クラウド接続アプリはマスターデータは端末には保存しませんが、オフライン作業のために端末（SDカードなど）に一部キャッシュデータを保存する場合があります。
本ケースではこのように仕様として端末に保存されるキャッシュデータを想定しています。

情報漏洩ケース18

端末機能で保存したデータが、

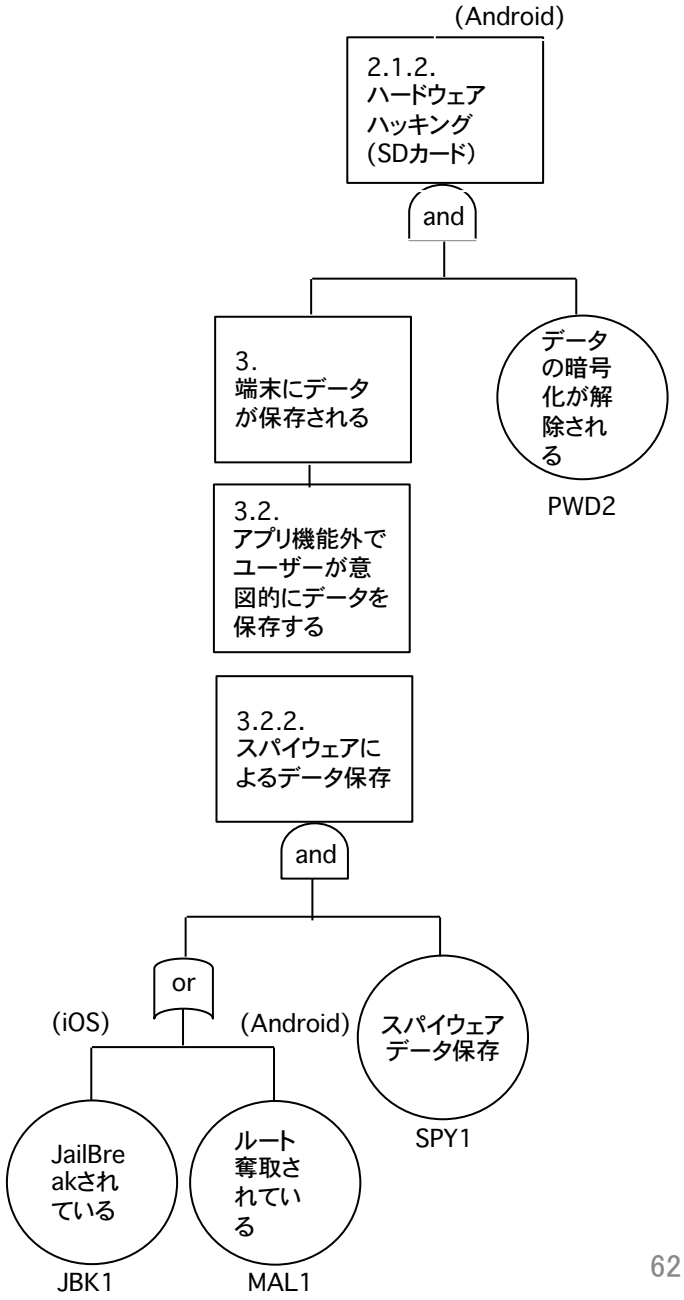
SDカードと共に抜き取られる②



情報漏洩ケース19

スパイウェアが保存していたデータ

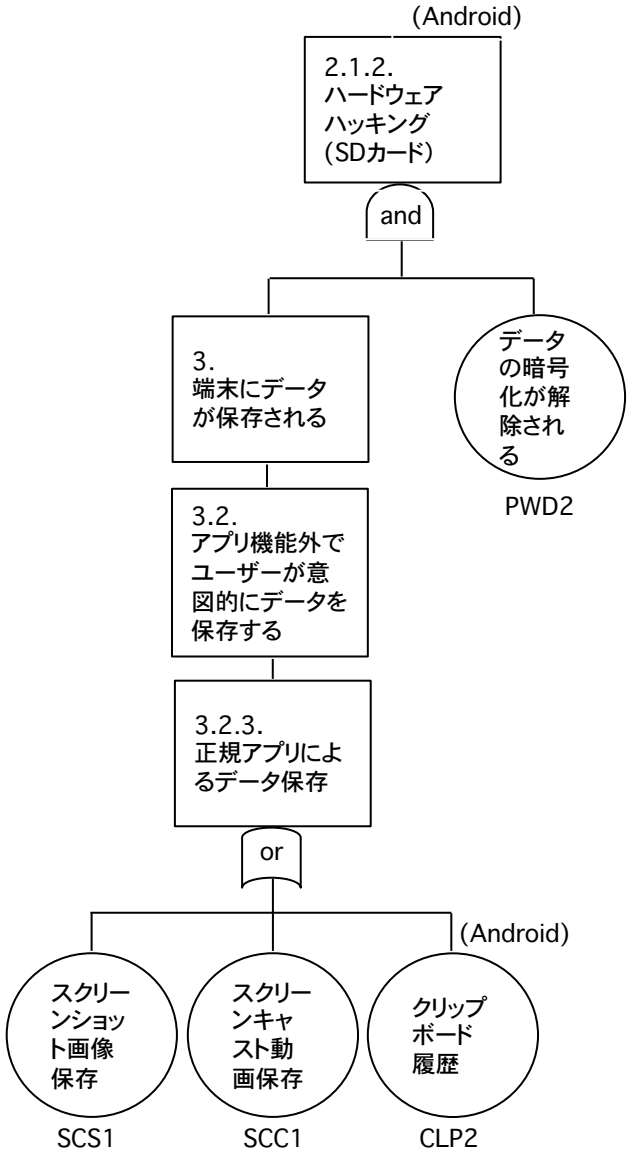
SDカードと共に抜き取られる③



情報漏洩ケース20

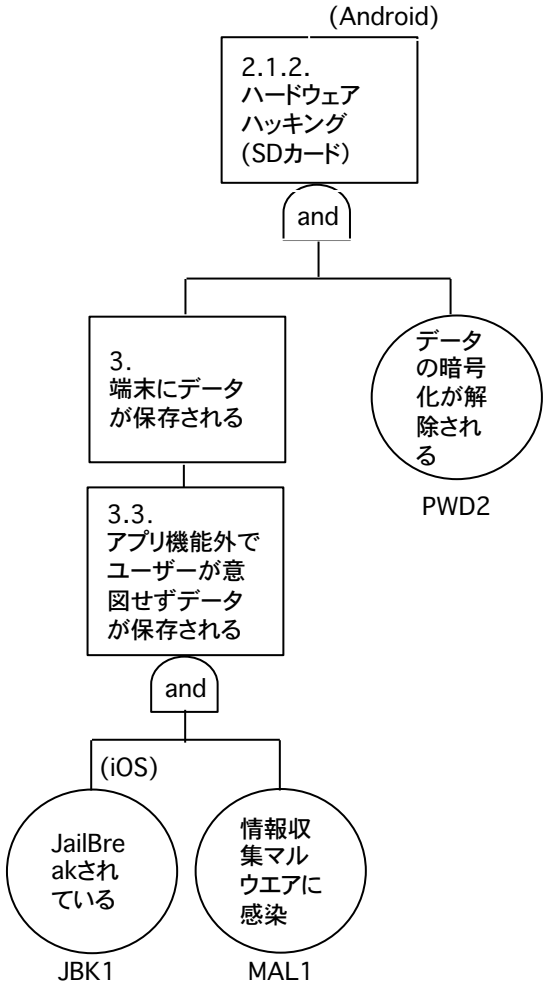
公式アプリで保存したデータが

SDカードと共に抜き取られる④



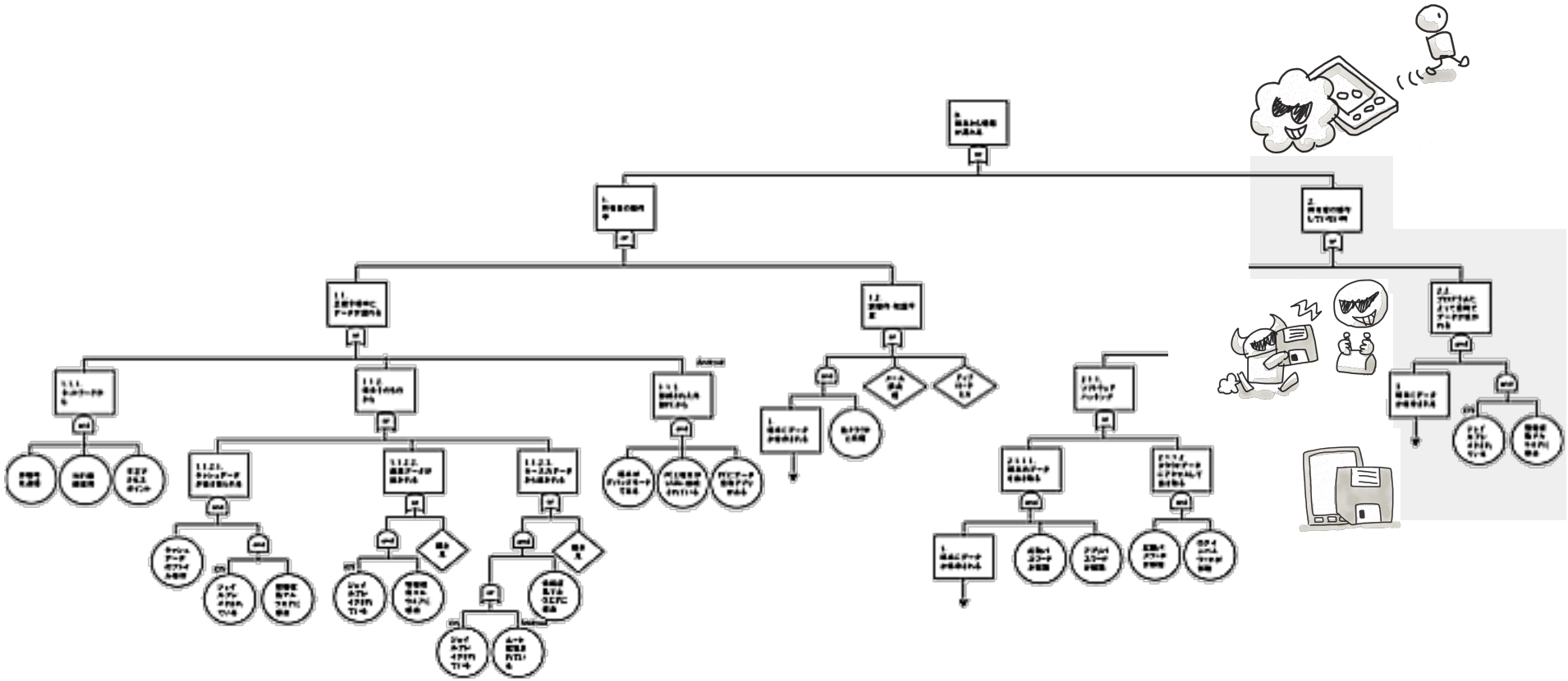
情報漏洩ケース21

マルウェアが勝手に保存したデータが SDカードと共に抜き取られる⑤

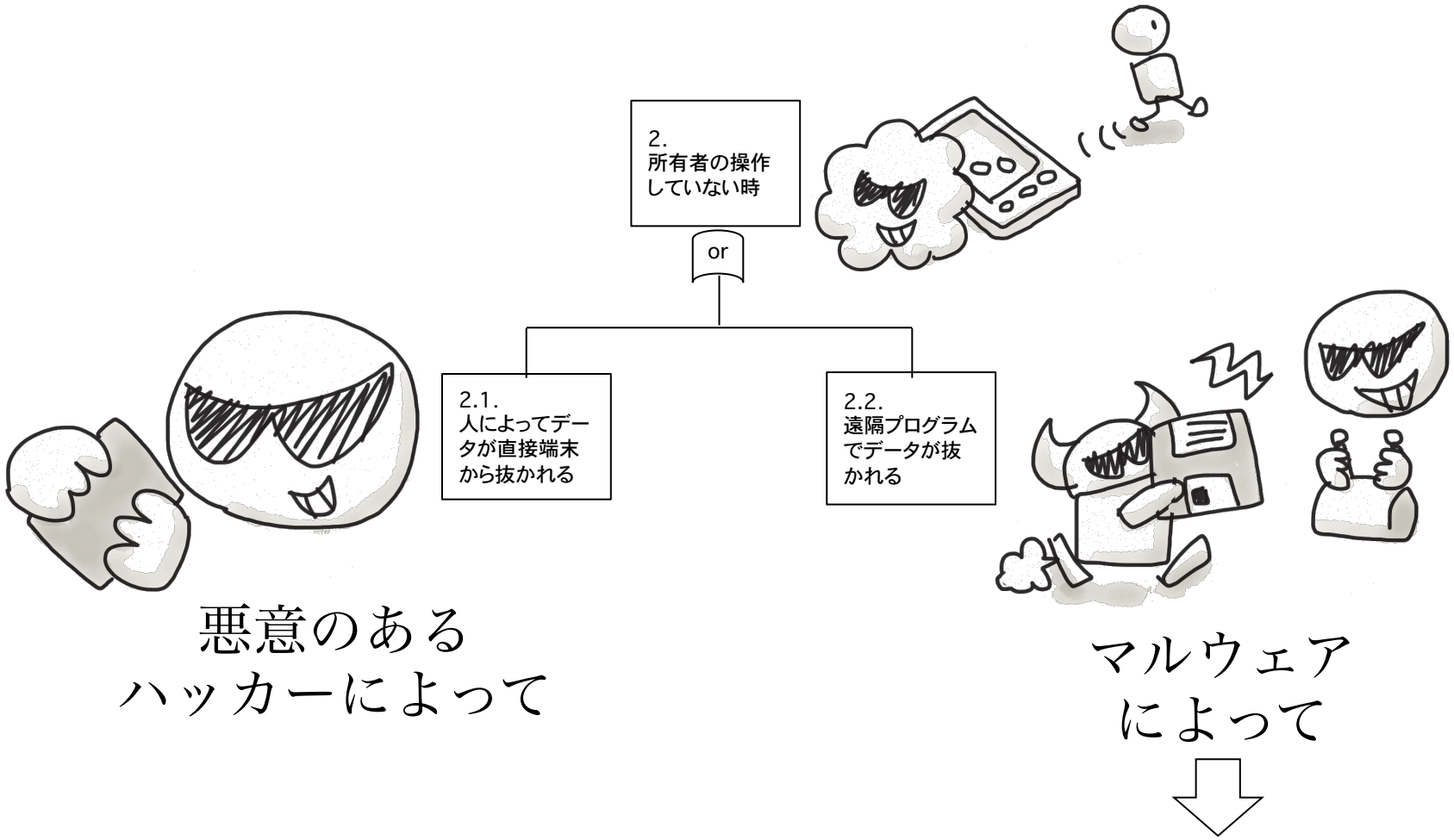


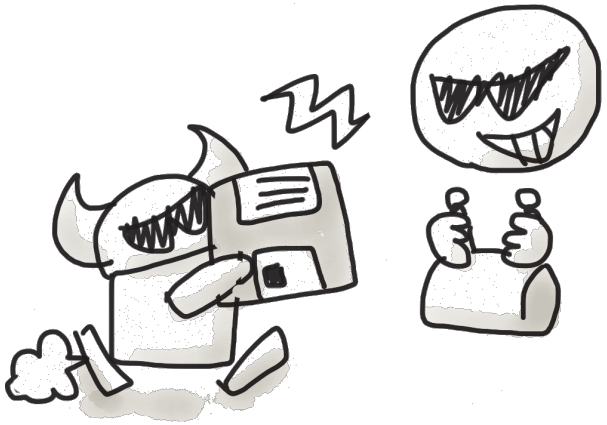
※ ユーザーが意図せずデータが保存されるとは、スパイウェアの機能を有したマルウェアが技術的に可能であることから想定しています。→ P.82参照

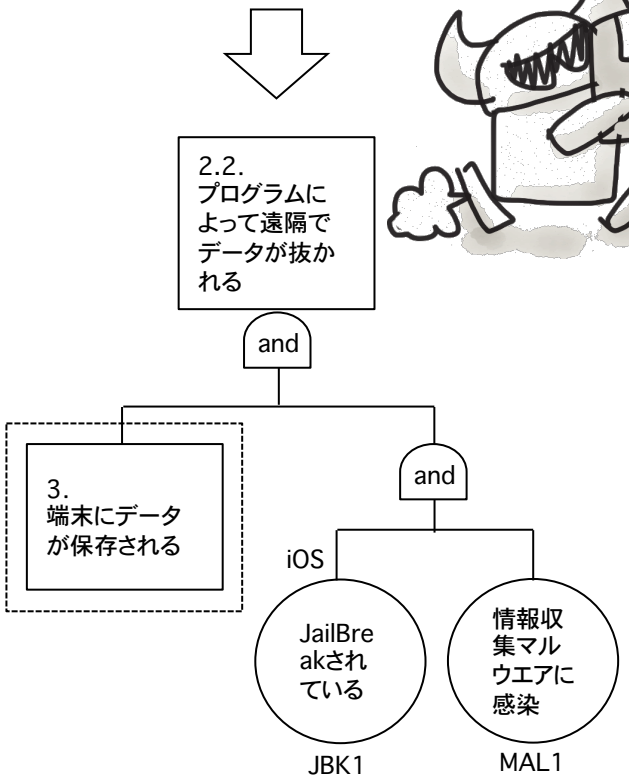
スマートフォンの業務クラウド利用における端末からの業務データの情報漏洩FTA



手から離れている間に


2.
所有者の操作
していない時
or
2.1.
人によってデー
タが直接端末
から抜かれる
2.2.
遠隔プログラム
でデータが抜
かれる
悪意のある
ハッカーによって
マルウェア
によって





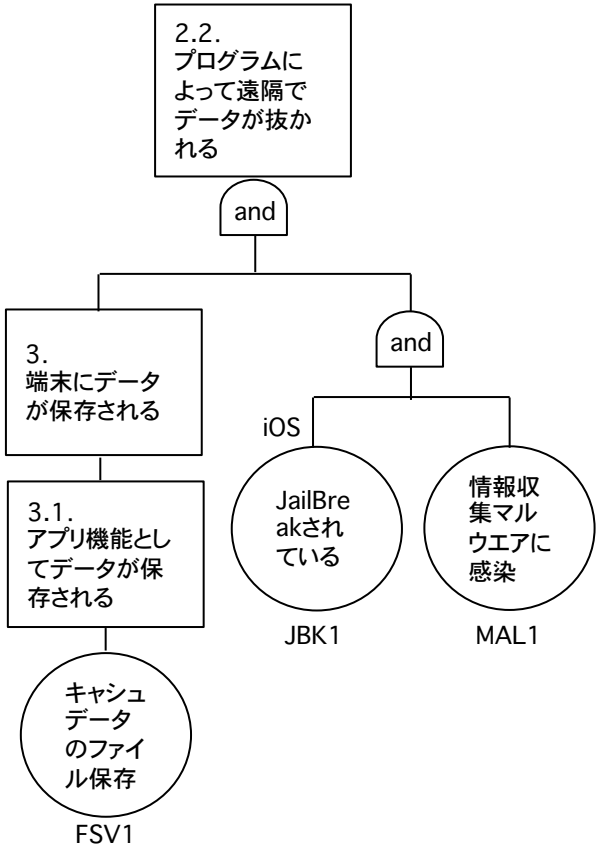
端末に保存されたデータが

遠隔マルウェア操作で抜き取られる

情報漏洩ケース22～26へ

情報漏洩ケース22

キャッシュ保存されたデータが
遠隔マルウェア操作で
抜き取られる①

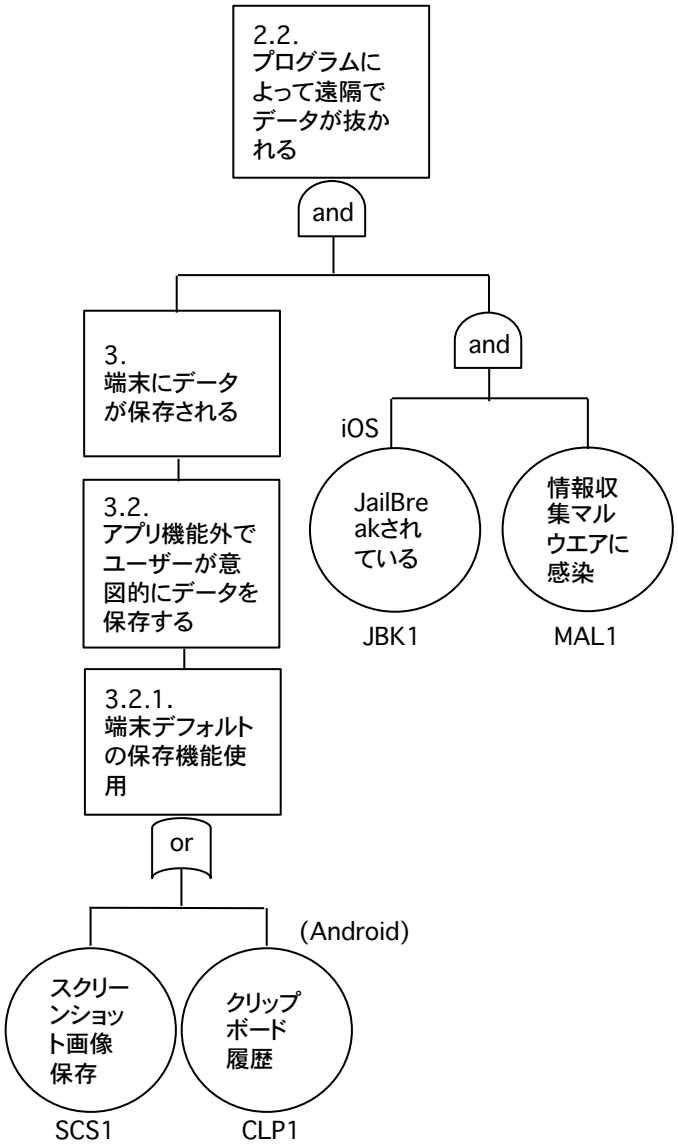


※ iOSはマルウェアに感染するためにはJailBreakされている前提があるので、JailBreakがand条件要素となります。→ P.86参照

情報漏洩ケース23

端末機能で保存したデータが

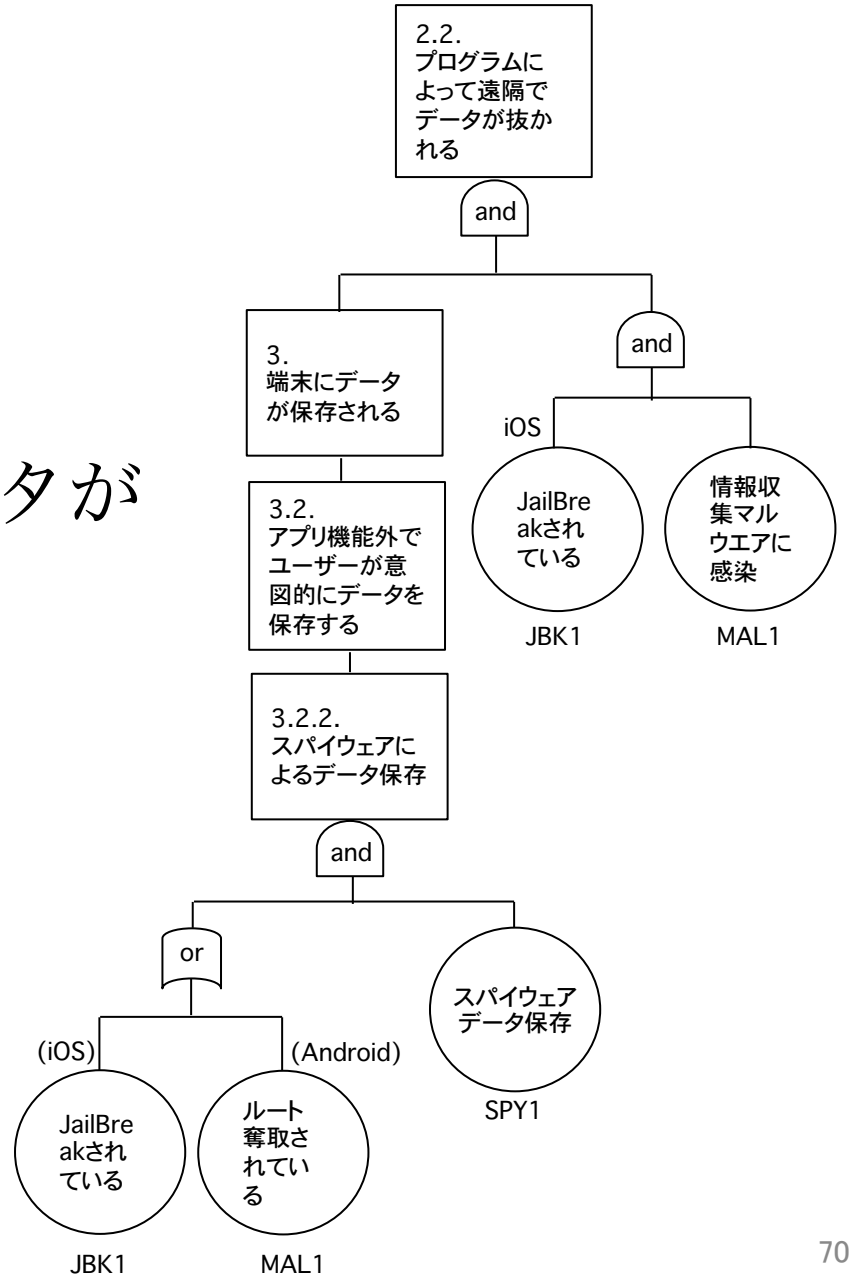
遠隔マルウェア操作で
抜き取られる②



情報漏洩ケース24

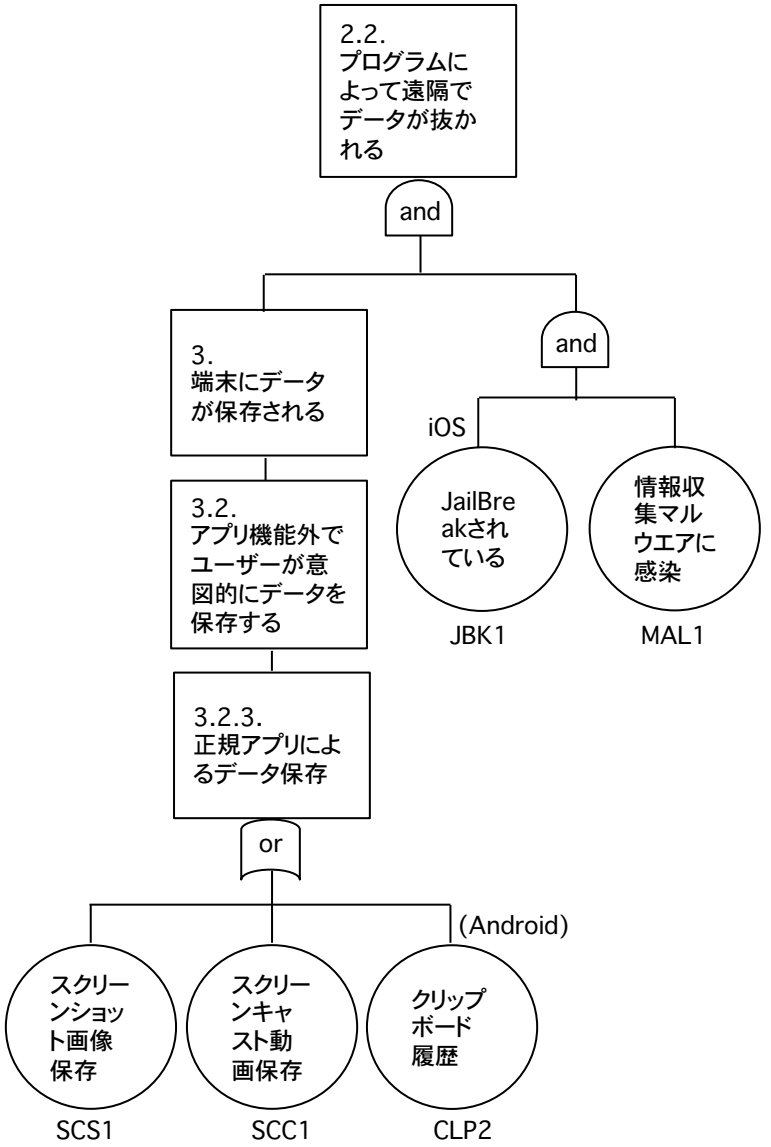
スパイウェアで保存されたデータが

遠隔マルウェア操作で
抜き取られる③



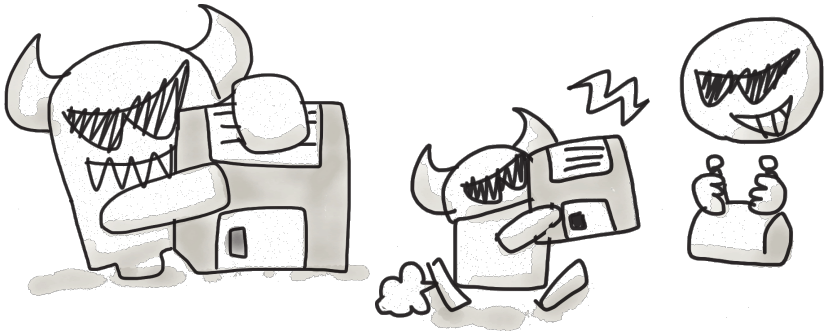
情報漏洩ケース25

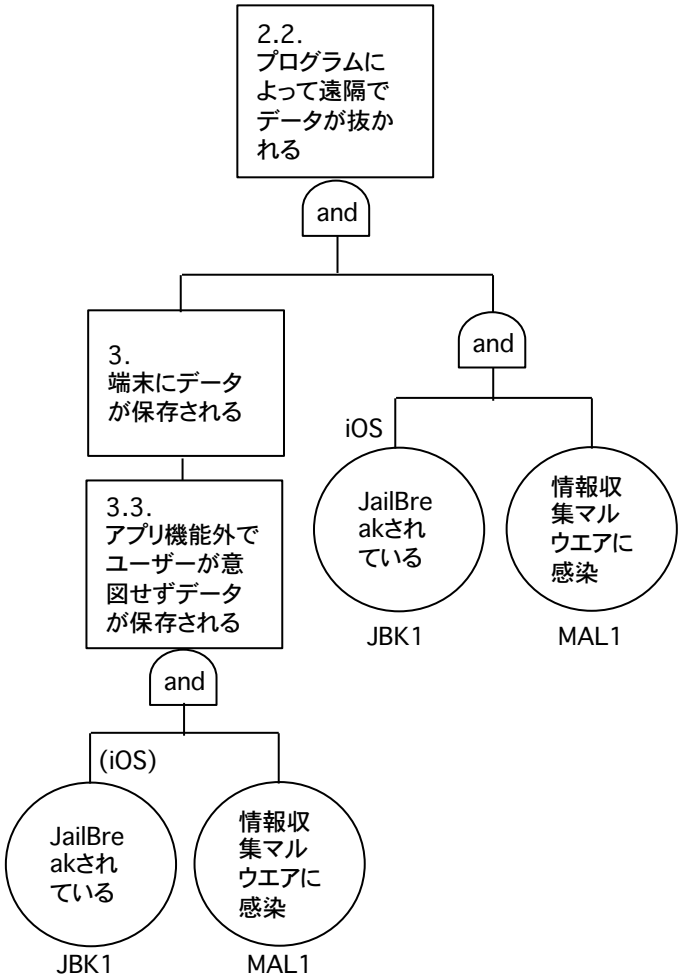
公式アプリが保存したデータが
遠隔マルウェア操作で
抜き取られる④



情報漏洩ケース26

マルウェアにて、
保存されていたデータが
遠隔マルウェア操作で
抜き取られる⑤





※ ユーザーが意図せずデータが保存されるとは、スパイウェアの機能を有したマルウェアが技術的に可能であることから想定しています。→ P.82参照

第四章 情報漏洩チェックに必要なセキュリティガイド

FTAが洗いだした22のチェックリスト項目

前章でFTAによって洗い出された30の情報漏洩のケースに対して、本章ではそれらを防ぐための22のチェックリストの内容について解説します。

チェックリスト項目は下記の4つのグループに分類されます。

1：マルウェアと不正改造関連
2：端末のデータ保存関連
3：パスワードの強度と運用関連
4：通信環境やクラウドサービス関連

マルウェア・不正改造関連

チェック	NO.	対策
☐	MAL1	マルウェアに感染した端末は業務クラウドに接続させないこと。
☐	ROT1	(Android) ルート奪取された端末は業務クラウドに接続させないこと。
☐	JBK1	(iOS) ジェイルブレイクした端末は業務クラウドに接続させないこと。

データ保存関連

チェック	NO.	対策
☐	FSV1	業務アプリにはキャッシュ保存機能を持たせないこと。
☐	SCS1	(iOS) MDMなどでスクリーンショット禁止の構成プロファイルの配布とインストールの監視を行うこと。
☐	SCS1	(iOS) 業務クラウド接続時にスクリーンショット禁止の構成プロファイルの有無をチェックすること。
☐	SCS2	(Android) 運用ルールにてスクリーンショットアプリを禁止し、MDMなどでインストールアプリを監視すること。
☐	SCS2	(Android) 業務クラウド接続時にスクリーンショットアプリの有無をチェックすること。
☐	SCS3	(Android) 業務クラウド接続中は、端末のスクリーンショット保存機能は無効にすること。
☐	SCC1	運用ルールにてスクリーンキャスト録画アプリを禁止し、MDMなどでインストールアプリを監視すること。
☐	SCC1	業務クラウド接続時にスクリーンキャスト録画アプリの有無をチェックすること。
☐	CLP1	運用ルールにてクリップボード履歴保存アプリを禁止し、MDMなどでインストールアプリを監視すること。
☐	CLP2	(Android) 運用ルールにてクリップボード履歴保存アプリを禁止し、MDMなどでインストールアプリを監視すること。
☐	CLP2	(Android) 業務クラウド接続時にクリップボード履歴保存アプリの有無をチェックすること。
☐	USB1	(Android) 業務クラウドへの接続時に端末がデバッグモードもしくはUSB接続の有無をチェックすること。
☐	KLG1	運用ルールにてキーロガーアプリを禁止し、MDMなどでインストールアプリを監視すること。
☐	KLG1	業務クラウド接続時にキーロガーアプリの有無をチェックすること。

パスワード関連

チェック	NO.	対策
☐	PWD1	運用ルールにて一定強度以上のパスワード設定を義務付けて、MDMなどでパスワード設定を監視すること。
☐	PWD1	業務クラウド接続時に一定強度以上のパスワード設定されてるかの有無をチェックすること。
☐	PWD2	キャッシュデータは充分な強度の鍵長さとロジックにて暗号化すること。
☐	PWD3	アプリにはキャッシュ保存機能を持たせないこと。

通信・クラウド関連

チェック	NO.	対策
☐	SSL1	業務クラウドの通信をSSLに限定すること。
☐	CLD1	運用ルールにて他のシステム同期アプリを禁止し、MDMなどでインストールアプリを監視すること。
☐	CLD1	業務クラウド接続時に他のシステム同期アプリの有無をチェックすること。

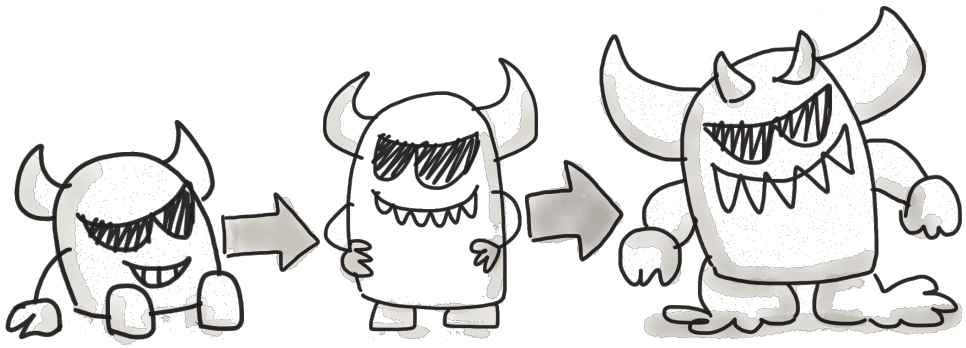
チェックリストの前に知っておくべきセキュリティガイド

1 ：マルウェアとOS不正改造

NO.	対策
MAL1	マルウェアに感染した端末は業務クラウドに接続させないこと。
ROT1	(Android) ルート奪取された端末は業務クラウドに接続させないこと。
JBK1	(iOS) JailBreakした端末は業務クラウドに接続させないこと。
SPY1	運用ルールにてスパイウェアを禁止し、MDMなどでインストールアプリを監視すること。
SPY1	業務クラウド接続時にスパイウェアの有無をチェックすること。

FTAによる情報漏洩リスクに対するチェックリストより

Androidマルウェア
進化の歴史



情報収集を目的として発達した手口と技術

Androidマルウェアは当初より端末内の情報収集することが目的の一つでした。

Android ver1.0 がリリースされた2008年9月には、すでに中国の電子科技大学から、機密情報収集して攻撃者に送信する「Android/StiffWeather.A」が発表されおり、Android OSも悪質なコードに対して脆弱性のリスクがあることが報告されました。

翌年2009年にはユーザーに気づかれず端末情報を収集する「Mobile Spy」がRatina X Studioよりリリースされました。このソフトの特徴はユーザーに気づかれずバックグラウンドでステルスモードで実行されるということです。

2010年8月には「FakerPlayer」と呼ばれるAndroid初のトロイの木馬が発見されました。ユーザーに気づかれず有償サービスに登録させるものでした。

2011年3月には「DroidDream」と呼ばれるマルウェアが発見されます。このマルウェアの脅威はOSのルート権限を奪取するだけでなく、公式のAndroidマーケット（現Google Play）で配布されたということです。

※参考サイト [1]

スマートフォンが
マルウェアに
かかりやすい理由

いかにユーザーをだますか

前述したようにマルウエア作成者は常にソーシャルエンジニアリング的な手法を模索しています。彼らの狙いは「いかにしてユーザにアプリをダウンロードさせ、インストールさせ、実行させるか」と言う点につきます。

よりセキュリティリテラシーが求められる

特にスマートフォンは以下の特徴があります。

1. 操作が直感的であるためPC操作が苦手なユーザーであっても簡単に使いこなすことができる。（結果的にマルウェアのリスクの認識が低いユーザーが相対的に多い傾向があると考えられる）
2. Web閲覧の延長のように容易に様々なアプリやコンテンツを収集することができる。（特にインストール時の、Windowsユーザーアカウント制御のような機構がない）

従ってスマートフォンを業務で利用する場合、このような安易なインストールを避けたり、マルウェア対策ソフトを積極的に利用するなど、ユーザの高いセキュリティ・リテラシーが求められます。

今後、スマートフォンの利用が拡大してゆく中で、現在PCで問題となっているAPT攻撃（Advanced Persistent Threat Attack）も、スマートフォンを標的にして移ってくる可能性も大いにあります。このような背景からも、ユーザのリテラシー向上を目指し、マルウエア対策を行う必要があります。

過去にあった漏洩事故。
将来あり得る漏洩事故。

セキュリティ・リスクを想定する二つの視点

セキュリティ・リスクの想定において必要なことは次の二点です。

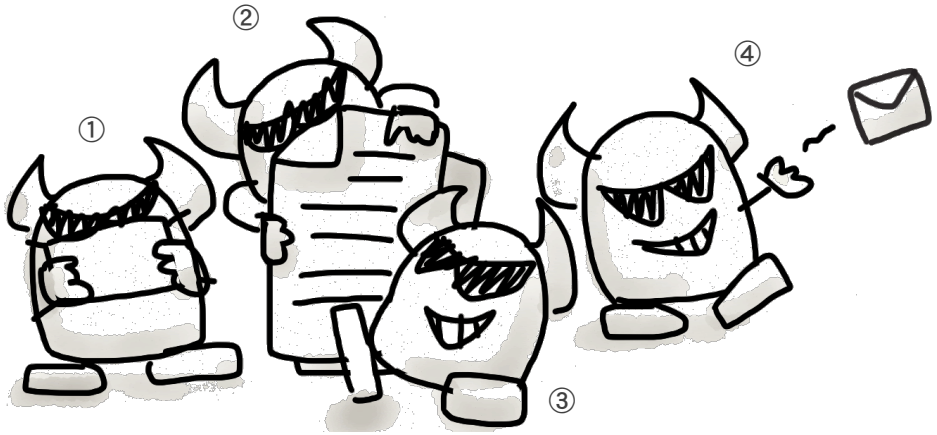
① 過去にどのようなセキュリティ・リスクが存在したか

過去発生したことは将来も条件を変えて発生する可能性があるということです。特にAndroidのマルウェアは前述したように初期の頃から端末内情報の収集と送信が目的の一つでした。従って過去にどういうマルウェアの手口が存在して、現在どのように進化し続けていくのかという情報は、将来発生しうるリスクを仮定するのに重要です。

② 技術的にどういうリスクが存在しえるか

過去にセキュリティ事故が発生していなくても、技術的にリスクとなり得ることが考えられる事柄については、やはりセキュリティの懸案として想定しておくべきです。
特にAndroidマルウェアは進化が早いため、現在存在していなくても技術的に起こりえる事象は対策を検討しておく必要があります。

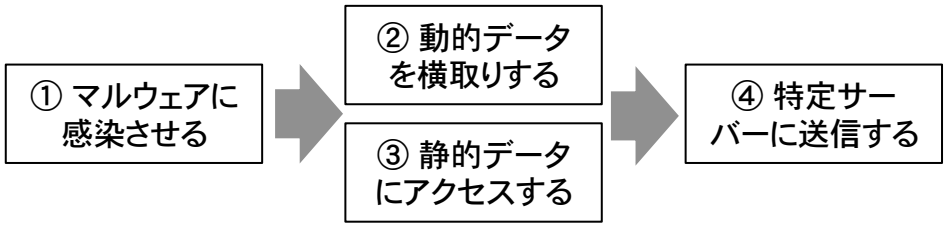
「感染させる。」
「横取りする。」
「アクセスする。」
「送信する。」



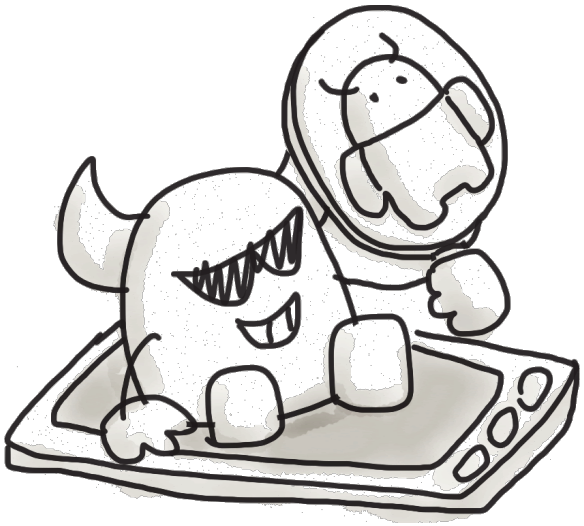
情報漏洩を生むマルウェアの4つの技術要素

本章では情報漏洩マルウェアを成立させるのに必要な次の4つの技術要素については以下に解説しています。

① マルウェアに感染させる。
　事例1：一般アプリなりすまし例。P.80
　事例2：ルート権限奪取例（キーロガーマルウェア感染条件）。P.81
　事例3：JailBreak例（iOSマルウェア感染条件）。P.86
② 閲覧・入力などの操作データを横取り一時保存する。（動的データ）
　事例1：公式アプリによるデータ横取り保存例。P.95
　事例2：データ横取り技術例。P.82
③ 正規に保存されている端末内データにアクセスする。（静的データ）
　事例1：マルウェアによる個人情報収集例。P.80
　事例2：ルート権限奪取例（SystemFileアクセス条件）。P.81
④ 取得したデータを特定のサーバに送信する。
　事例1：マルウェアによる情報漏洩送信例。P.80
　事例2：マルウェアによる端末遠隔操作例。 P.83, P.84



悪質マルウェアが
一般アプリになりすまし



一般アプリになりすまし隠れて個人情報を外部に送信

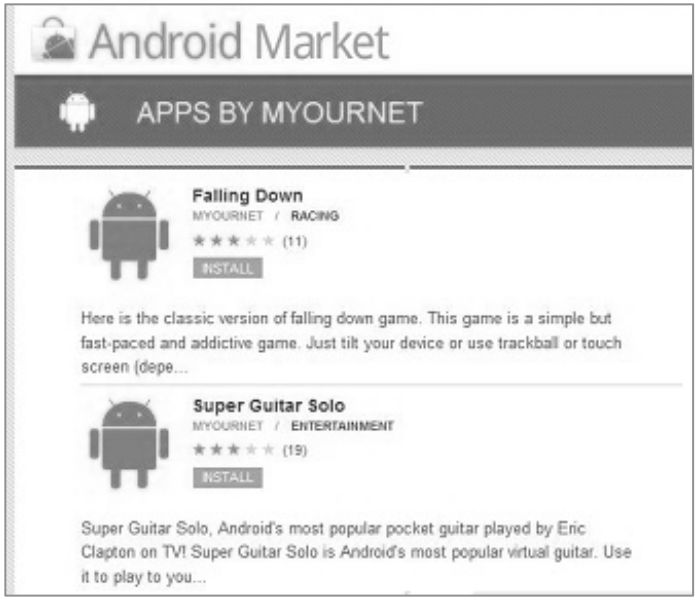
2011年3月に発見されたDroidDreamは公式のAndroidマーケット（現Google Play）で発見された最初のマルウェアでした。
国内における公式アプリなりすましマルウェアとしては2012年2月に発見された「The Movie」が有名です。このマルウェアは動画を再生しているバックグラウンドでアドレス帳データを特定のサーバーに送ります。数万～数百万件の個人情報が流出したと推定されます。

※参考サイト [2]

ルート奪取マルウェアは全ての権限を奪い取る

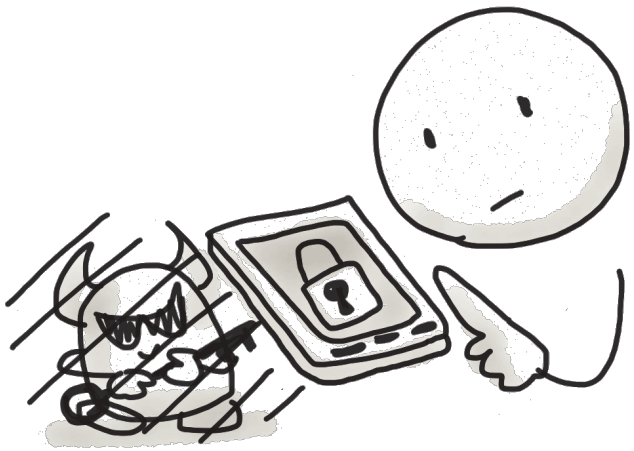
ルート奪取マルウェア

マルウェアにOSのルート権限を奪取された場合は、事実上あらゆることが可能です。
ルート権限を奪取すると保護されたSystemFileとして保護された情報にアクセスしたり、テキスト入力データなどの操作情報を抜き取ることが可能です。
またマルウェアが自分自身を隠してユーザーに感染していることを気づかせないこともできます。そして感染した後はマルウェア対策ソフトで削除することも不可能です。



※2011年3月に発見されたルート検出マルウェア「Droid Dream」と呼ばれる公式アプリ例。参考サイト [3]

ユーザーに気づかれず
情報抜き取るスパイウェア



未成年のスマートフォン操作監視用として売られているスパイウェア

スパイウェアはユーザーに気づかれず端末の操作内容を端末内に保存したり指定管理者に送信するアプリです。スパイウェアは位置情報、画面のスクリーンショット、SMS送信内容、Webサイト閲覧履歴などを取得することができます。「Mobile Spy(Android/iOS)」や「iKey Monitor (iOS)」といった製品が市販されており、保護者が未成年者にスマートフォンを与える時の監視ツールとして利用されています。これらの製品はAndroid端末のルート奪取や、iOS端末のJailBreakの必要があり、端末の管理者（利用者の保護者など）が意図的にインストール操作をする必要がありますのでマルウェアとはいえません。しかしこの技術を応用し、スパイウェアであることを隠して一般アプリになりすましたり、勝手にルート奪取やJailBreakする技術と組み合わせることで危険な「情報収集マルウェア」になる可能性があります。

※参考サイト [4] [5]

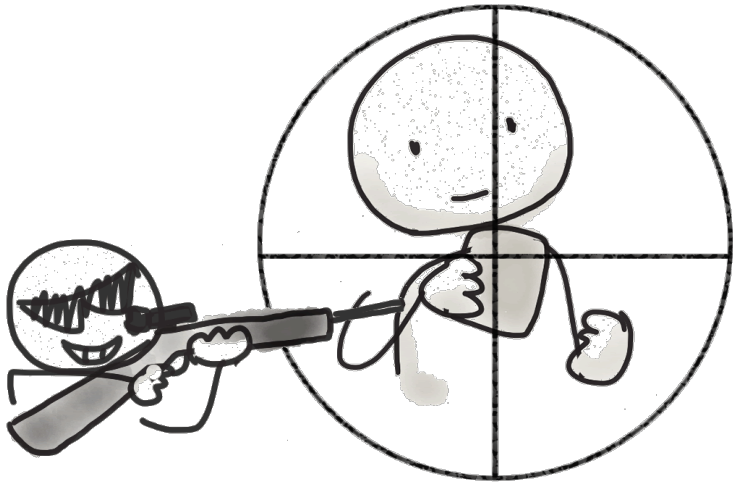
マルウェアで
端末自在に遠隔操作

ボット型マルウェア

ボットとは「ロボット」からネーミングされているように、外部から遠隔で操作されるマルウェアのことです。保存されているデータや、操作中のスクリーンショットデータやキー入力データを収集して特定のサーバーに送ることなども可能です。
※2010年12月に発見された「Geimini」が代表例です。

※参考サイト [6]

機密情報の漏洩を狙う標的型攻撃



特定組織の機密情報を狙う標的型攻撃

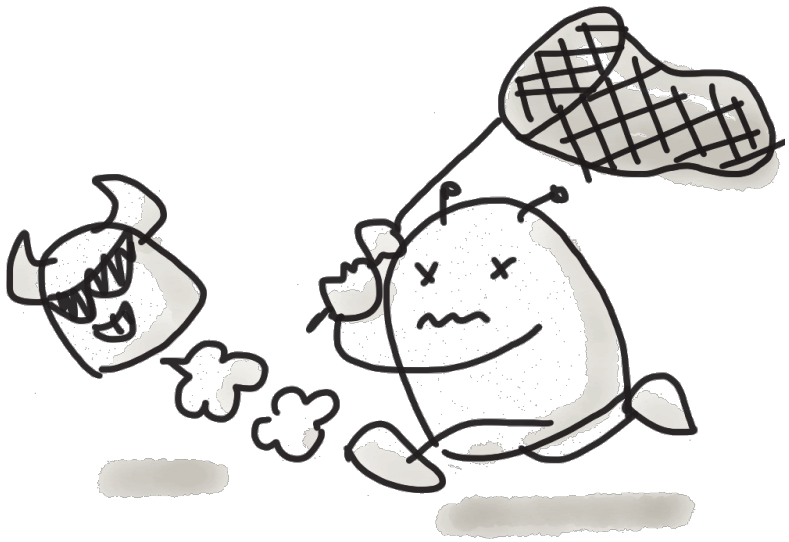
ここ数年危険性が指摘されているのが「標的型攻撃」と呼ばれる特定の組織を狙ったサイバー攻撃です。従来のコンピューターウイルスは愉快犯による犯罪も多く見られましたが、標的型攻撃の目標は特定の組織の情報を盗み出したり、システムを破壊することにあります。

Android端末を標的とした遠隔操作トロイの木馬

標的型攻撃とはその目的のために様々な手段が組み合わされるのが特徴です。TREND MICRO社のレポートによると持続型標的型攻撃の一貫としてすでにAndroid端末を標的としたマルウェアが開発され始めていると報告しています。（参考サイト[7]）
このアプリは現時点では開発初期段階とみられますが、次の機能を有してます。
① 端末に保存されている重要情報を探し出す。
② 奪取した情報を特定のサーバーに送信する。
③ 新しい不正プログラムをダウンロードさせる。

単なるスマートフォンの盗難や紛失と異なり、標的型攻撃の場合は明確に機密情報を奪取することが攻撃者の目的です。今後はスマートフォンの業務利用においても、標的型攻撃を視野に入れたセキュリティ対策が必要となると言えます。

BYODにおける
マルウェア対策ソフト管理



マルウェア対策ソフトの選び方

マルウェア対策ソフトをインストールしたとしても、端末を利用する社員がそれをアンインストールしたり、マルウェアを検知する定義ファイルの更新を怠ったり、スキャンを実行しなかったりすれば目的を果たすことができません。マルウェア対策ソフトを選ぶ場合においても重要なことは、定めたルール通りに確実に運用できる製品を選ぶことです。

①定評のあるマルウェア対策ソフトを選択する。

②マルウェア定義ファイルの自動更新機能や、悪質な「SMS/迷惑メール」や「Webサイトへの接続」への防御機能も有しているものを選択する。

※クラウド技術を利用した、最新の情報でのマルウェア評価技術（レピュテーション）など。

③集中管理型を選択する。

※スタンドアロン型は、運用がユーザー任せになるため有事の際に有効に働かない可能性があります。一方集中管理型は、各端末内のクライアントソフトを管理者がリモートで集中管理できるため、定められたセキュリティルールをユーザー端末に強制化することができます。

iOSがマルウェア感染するただ一つの条件

JailBreak

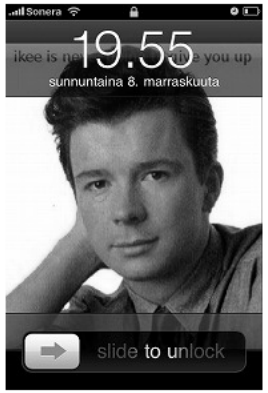
iOSのマルウェアは発見されていませんが、唯一の例外がJailBreak端末への感染です。JailBreakを行うとApp Storeで審査が通ったアプリ以外もインストールできるため、マルウェアにも感染する危険性が増します。社員のiOS端末はJailBreakさせないことが重要なセキュリティ対策です。
※2009年11月に発見された「Ikee」が代表的なマルウェアです。

「初のiPhoneワーム」をセキュリティ企業が発見

ロック解除したiPhoneに感染するワームが発見された。ソースコードも公開されており、さらなる亜種が登場するかもしれない。

[ITmedia]

セキュリティ企業F-Secureは11月8日、初のiPhoneワームを発見したと報告した。



このワームは「Ikee」という名前で、Jailbreak（iPhoneのロックを解除して好きなソフトを実行できるようにすること）したiPhoneのみに感染するという。このワームに感染すると、壁紙が歌手のリック・アストリーの写真に変わり、「ikee 3 件は君を離さない」というメッセージが表示される。

Ikeeは、Jailbreak済みだがデフォルトのrootログインパスワードを変更していないiPhoneを標的とする。感染するとSSHサービスを停止するため、再度感染することはない。このワームはIPアドレスをスキャンして脆弱なiPhoneを探すが、スキャンするアドレスはほとんどオーストラリアのもので、同国以外でIkeeの報告は確認されていないという。

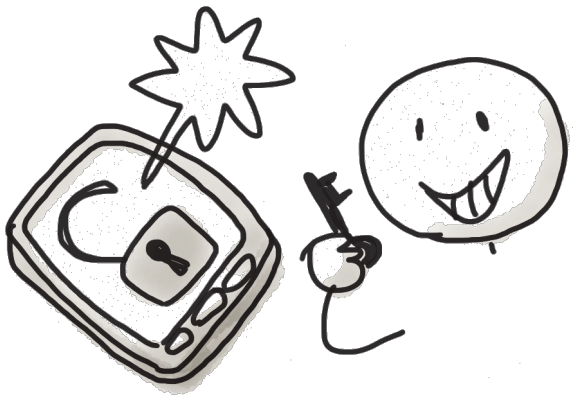
※参考サイト [8]

古いバージョンOSに残っている脆弱性

PDFスクリプト

iOS4.3.4以前のバージョンについてはPDFスクリプトの脆弱性が指摘されています。これにより悪意のあるスクリプトが埋め込んであるPDFを開くと、ユーザーが気づかないうちに端末がJailBreakされてしまう危険性があります。JailBreakに関する方法についてはハッカーとApple社のいたちごっこであり、ユーザーには脆弱性の対策が行われている最新のOSを推奨することが必要です。

セキュリティ対策の前提が崩れる不正改造



なぜJailBreakやルート奪取は危険なのか

OSの不正改造は、iOSの場合はJailBreak、Androidの場合はルート奪取と呼ばれます。いずれも一般ユーザーには解放されていないOSのルート権限を奪います。

このような不正改造は、大きく分けて次の二パターンがあります。
一つは前述のルート奪取マルウェア（P.81）や、OSの脆弱性をついたスクリプト（P.87）のようにユーザーが意図せず改造されてしまうケースです。
もう一つは専用ツールを使ってユーザーが不正改造を行うケースです。

いずれにせよルート権限が奪取されているとは、
① 本来なら検知できなはずの操作データを横取りすることができる。
② 本来ならアクセス権のないはずの保存データにアクセスできる。
③ ユーザーやシステム管理者の監視を逃れることができる。
という状態を指します。

スマートフォン業務利用における情報漏洩対策の多くは、OSが改造されていないことが前提です。従ってOS不正改造により上記①～③である可能性があるということは、これらの対策の前提がそもそも崩れるということを意味しています。

チェックリストの前に知っておくべきセキュリティガイド

２：端末のデータ保存関連

NO.	対策
FSV1	業務アプリにはキャッシュ保存機能を持たせないこと。
SCS1	(iOS) MDMなどでスクリーンショット禁止の構成プロファイルの配布とインストールの監視を行うこと。
SCS1	(iOS) 業務クラウド接続時にスクリーンショット禁止の構成プロファイルの有無をチェックすること。
SCS2	(Android) 運用ルールにてスクリーンショットアプリを禁止し、MDMなどでインストールアプリを監視すること。
SCS2	(Android) 業務クラウド接続時にスクリーンショットアプリの有無をチェックすること。
SCS3	(Android) 業務クラウド接続中は、端末のスクリーンショット保存機能は無効にすること。
SCC1	運用ルールにてスクリーンキャスト録画アプリを禁止し、MDMなどでインストールアプリを監視すること。
SCC1	業務クラウド接続時にスクリーンキャスト録画アプリの有無をチェックすること。
CLP1	運用ルールにてクリップボード履歴保存アプリを禁止し、MDMなどでインストールアプリを監視すること。
CLP2	(Android) 運用ルールにてクリップボード履歴保存アプリを禁止し、MDMなどでインストールアプリを監視すること。
CLP2	(Android) 業務クラウド接続時にクリップボード履歴保存アプリの有無をチェックすること。
USB1	(Android) 業務クラウドへの接続時に端末のUSB接続の有無をチェックすること。
USB2	(Android) 業務クラウドへの接続時に端末のデバッグモード有無をチェックすること。

FTAによる情報漏洩リスクに対するチェックリストより

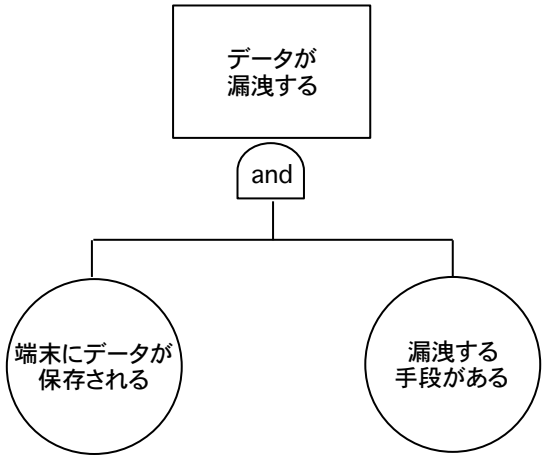
システム管理者が
想定していない
データ保存は要注意

端末データ保存の裏ワザはなぜ危険なのか。

FTAの解析によると、スマートフォン端末から業務データの情報漏洩が起こるには、データの横取りである動的なケースと、保存してあるデータを盗み出す静的なケースがあります。そして静的な情報漏洩のケースで必要なのが下記の二つのAND条件です。

① 業務データが端末に保存されていること。
② 保存されたデータが外部に漏れる手段があること。

もしシステム管理者が上記の①を対策しようとした時に、盲点となるのがデータ保存の裏ワザ方法です。
この章では、ユーザーが意図的に、あるいは意図せず誤操作で、業務データを端末に保存してしまうケースについて解説します。

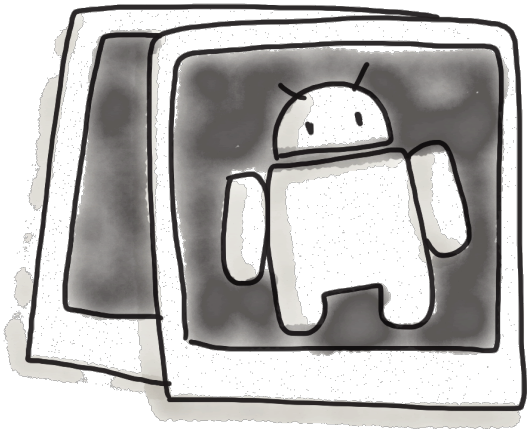


iPhone/iPadで
スクリーンショットを保存する

iOSスクリーンショット

電源ボタンとホームボタンを同時に長押しすることでスクリーンを画像データとしてアルバムに保存することができます。
これを禁止するには構成プロファイルにて「スクリーンショットを禁止する」設定としてユーザーの端末にインストールします。構成プロファイルはユーザーが勝手に削除できないように管理者パスワードでロックすることが可能ですが、端末の初期化と復元によって削除することも可能であるため、構成プロファイルの有無はシステムによって定期的にチェックする必要があります。

Androidで
スクリーンショットを保存する

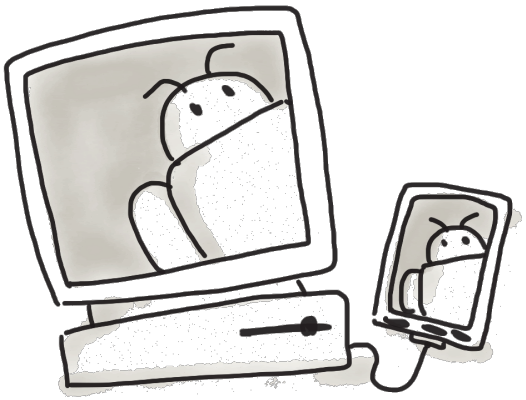


Androidスクリーンショット

多くの端末はそれぞれの方法にてiOSと同様にスクリーンショットをとり画像として保存することが可能です。Androidは構成プロファイルのようなセキュリティポリシーを一括で管理する設定はありません。またスクリーンショットを保存する方法もメーカーや機種により様々です。

※下記はSony Xperia Android4系におけるスクリーンショット保存例です。

パソコンに
スクリーンショットを転送する



Android PC転送スクリーンショット

端末をデバッグモードにしてPCにUSB接続すると端末のスクリーンを画像データとして取り込むことが可能です。(PCにはGoogle社が無料で配布しているAndroid SDKのDebug Monitorのインストールが必要です。)

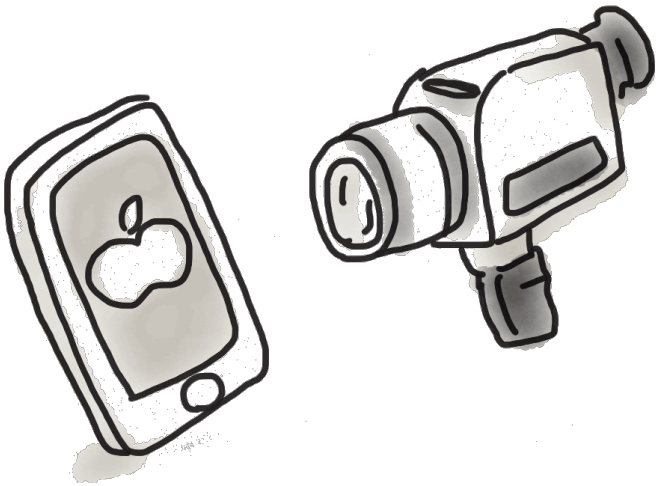
クリップボードデータが消えずに保存されている

Androidクリップボード保存

一般的にはクリップボードデータは直前の一つのみ保存されますが、Android端末の機種によってはクリップボードの履歴をファイルとして保存する機能があるものがあります。ユーザーがコピーした機密情報が消されないまま端末に保存されるリスクがあります。

※下記はSamsung Galaxy S2 Android 4系のクリップボード保存履歴例です。

端末のデータを保存する公式アプリたち



公式アプリデータ保存

各OSベンダーが運営する App Storeや Google Playなどで配布されている公式アプリにて操作データを端末に保存することができるアプリが配信されています。これらのアプリを使用すると機密情報が端末に保存されるリスクがあります。

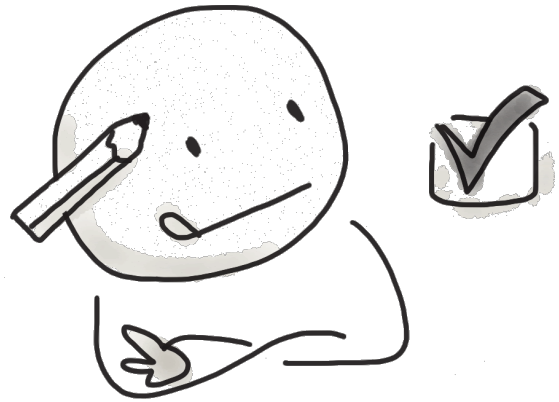
iOS: Display Recorder
スクリーンデータを動画として撮り保存することが可能です。

Android: ScreenShot UX
スクリーンショットを画像として任意のフォルダーに保存可能です。

Android: aNdClip
クリップボードの履歴をアプリ内に保存することができます。

チェックリストの前に知っておくべきセキュリティガイド

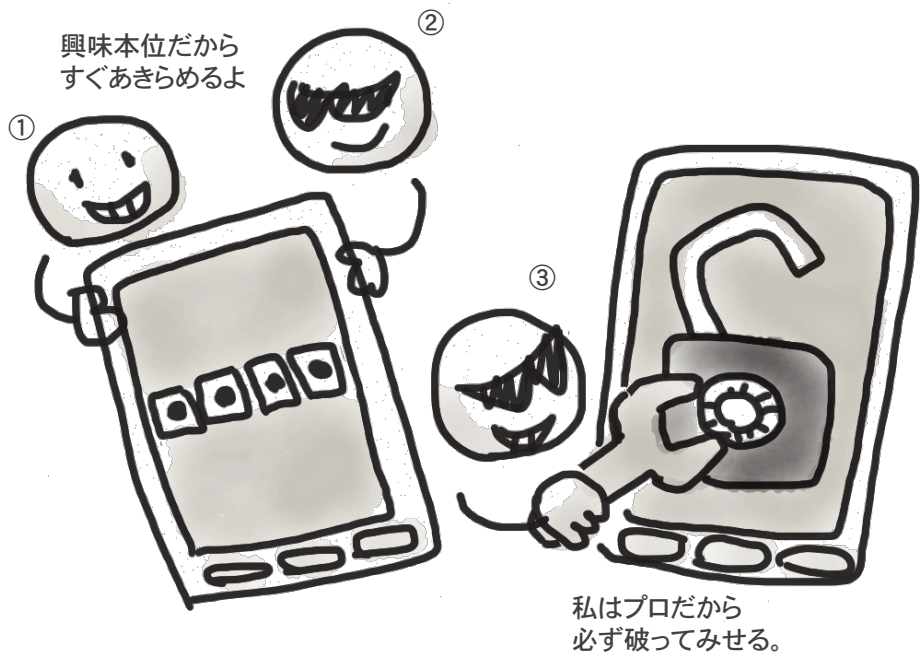
３：パスワードの強度と運用



NO.	対策
PWD1	運用ルールにて一定強度以上のパスワード設定を義務付けて、MDMなどでパスワード設定を監視すること。
PWD1	業務クラウド接続時に一定強度以上のパスワード設定されてるかの有無をチェックすること。
PWD2	キャッシュデータは充分な強度の鍵長さとロジックにて暗号化すること。
PWD3	業務クラウド側でなりすましログインに耐えうるパスワードポリシーにて運用を行うこと。

FTAによる情報漏洩リスクに対するチェックリストより

盗難・紛失の三つのケース



興味本位対策か? 専門ハッカー対策か?。

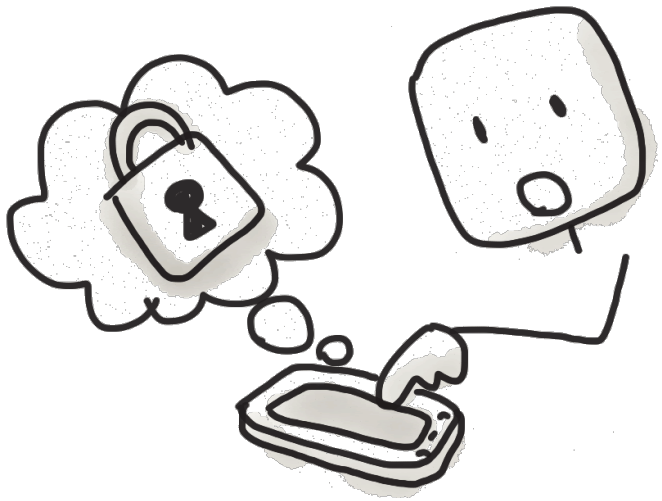
紛失したスマートフォンを拾ったり、あるいは特定のスマートフォンを盗難した場合に端末の情報をハッキングされる可能性はどのくらいあるのでしょうか。端末盗難および紛失でスマートフォンのパスワードが第三者に破られるケースは次の三つのケースが考えられます。

① 端末を拾った一般人が興味本位で中のデータにアクセスする。→ P.98
② 転売目的で盗取した犯人が初期化前に興味本位でデータにアクセスする。
③ 情報奪取目的で盗取した犯人が高度な専門ツールでデータ奪取する。→ P99, 100, 101

盗難・紛失のほとんどのケースは①および②です。③のケースは非常にまれではありますが、本当に高度な知識を持つ専門のハッカーにかかればスマートフォンのパスワードや暗号化は破られる可能性が高いのです。

昨今、特定の企業、団体、部署の機密情報を奪取する標的型ウイルスが増加傾向にあります。今後は同様に特定の企業、団体、部署の人間が所有するスマートフォンを情報奪取目的で盗難するケースが発生するかもしれません。そのような機密情報を扱う社員のスマートフォン利用では③のケースを想定すべきです。

拾った人の９６％が
端末内データを見ようとした



Androidパターンロックの脆弱性

2012年3月にシマンテックで行われた「ハニースティックプロジェクト」によりスマートフォンを拾った人がどういう行動をとるかという統計が取られました。結果は拾った人の50%が持ち主に返しましたが、しかし端末の内部のデータにアクセスしようとした人が96%でした。つまり持ち主に返そうという善意の人であっても、ほとんどの場合端末内のデータには一度はアクセスしようと試みたということです。
この事件結果により端末にはパスワードを強制化することが重要であることがわかります。

iOSは構成プロファイルによってパスワードのポリシーをより厳しく強制的に適用させることができます。一般的にiOS端末のパスワードは数字4桁ですが、英数字を含んだ長い桁数のパスワードや有効期限を設定することができます。また連続パスワード失敗でデータを初期化させることも可能です。（ただし初期化された端末はMDMの管理下からもはずれるためリモートワイプやロックも不可能になります）

Androidについては前述した「パターン解除」の他に「スワイプ・タッチ」「フェイスアンロック」などは使用させずPINの利用を強制させることで情報漏洩のリスクを下げることができます。

※参考文献 [9]

iOSキーチェーンの脆弱性

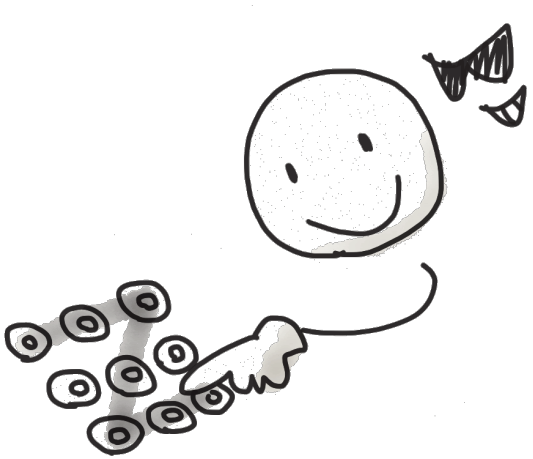
iOSキーチェーンの脆弱性

ドイツのフラウンホーファー研究所の報告ではiOSのキーチェーンに脆弱性について指摘されています。同研究所ではロックされた無改造のiPhoneのパスワードをハッキングする様子を動画としてYouTubeにアップしています。
悪意のあるハッカーにかかればiOSのキーチェーンを破ることができることが示唆されています。

また「Gecko iPhone Toolkit」のように一般に配布されているiOSのパスワード解除ツールもあります。

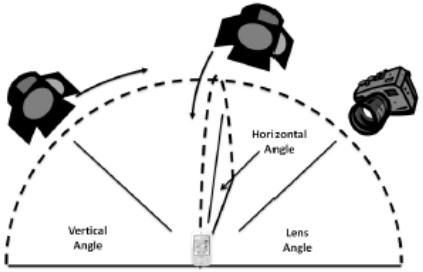
※参考サイト [10]

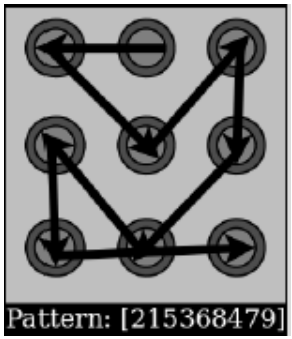
パターンロックの脆弱性



Androidパターンロックの脆弱性

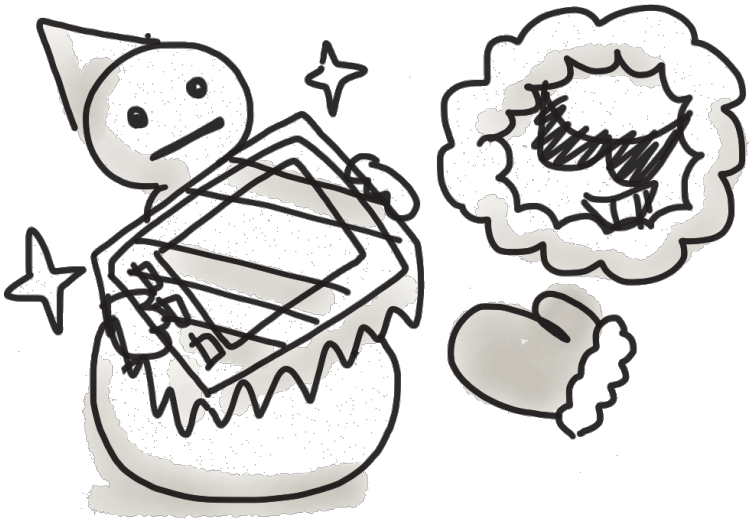
米ペンシルバニア大学の発表ではスクリーンの指紋の跡から約68%のパターンロックを解読できるといいます。
悪意のあるハッカーにかかれば、高い確率で起動時のパターンロックを破ることができることが示唆されています。





※参考文献 [11]

端末を凍らせて
暗号データを破る



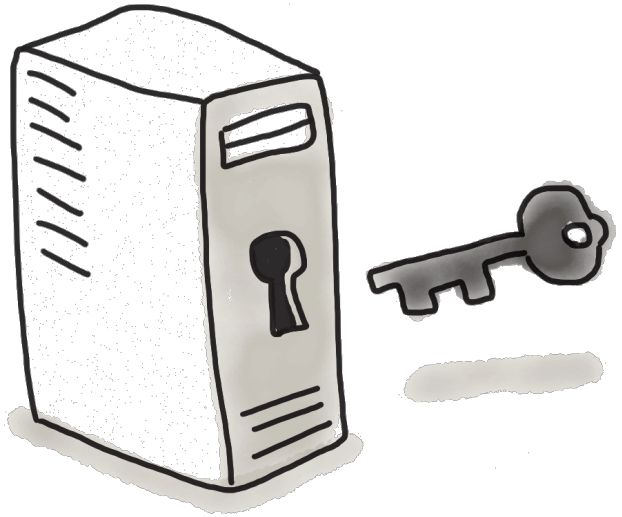
メモリーを冷却して暗号化を復号する「フロスト」

ドイツのフリードリッヒアレクサンダー大学のセキュリティチームは「フロスト」と呼ばれるハッキング手法により、スマートフォンの暗号化を無効化すると発表しました。
これは半導体は冷却すると情報が削除されるのに時間がかかる性質を利用し、メモリー内に残っていた暗号化情報を復元して取り出すというものです。これはデジタル・フォレンジックと呼ばれるパソコンに対して行われる犯罪調査の方法を応用したものです。

チームはこのフロストにより、Galaxy Nexus Android 4.0内の連絡先、写真、Web履歴などの解析に成功したと発表しています。

※参考文献 [12]

業務システムの
パスワードポリシー例



金融機関のパスワード強度

FISC（金融情報システムセンター）の安全対策基準ではパスワードについての運用は下記基準が推奨とされています。

技26
2.暗証番号・パスワード等は他人に知られないための対策を講ずること。
暗証番号・パスワードの利用等にあたっての安全対策上の機能としては、例えば以下のようなものがある。
(1) 暗証番号・パスワードにはNULLまたは少ない桁数を認めない機能
(2) 暗証番号・パスワードの使用に有効期間を設定し、有効期限近接時は、事前に変更要求を行う機能
(3) パスワードの変更にあたって前回もしくは以前と同一のパスワードの使用を認めない機能
(4) 特定の予測可能なパスワード(自分の会社名等)や不適切なパスワードを排他的に定義することができる機能
(5) アクセスの都度、アクセスに使用するパスワードを変更するワンタイムパスワードの機能

技36
IDの不正使用防止機能を設けること。
(1) ログオン中のタイムアウト システムにログオンしたまま一定時間操作が行われないIDを、強制的にログオフもしくは画面をロックする。
(2) 使用されていないIDの使用停止 一定期間システムに対してアクセスがないIDは、使用停止とする。
(4) パスワード入力失敗の回数制限 パスワードの入力を一定回数失敗した場合は、当該IDを一時的に使用不可とする。
(6) 総当り攻撃(ブルートフォース攻撃)への対策を講ずる。単にパスワード入力時のリトライ制限を設けるだけでなく、認証方式の特性を分析し、総当り攻撃が可能となるリスクに対応する。例えば想定されるリスクとして、パスワードを固定しユーザーIDを次々変化させてログオンを繰り返すことによるパスワードのリトライ制限の回避が考えられる。

※参考文献 [13]

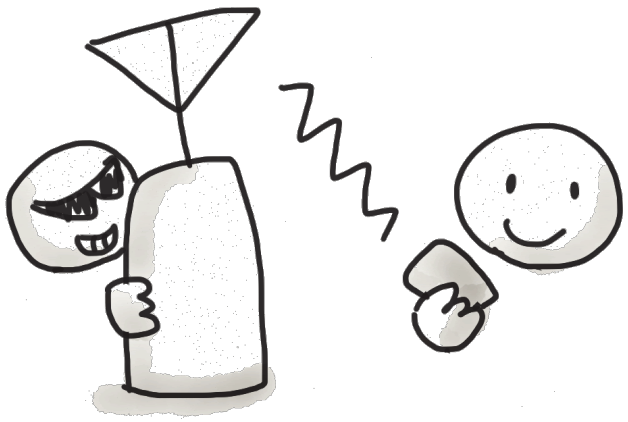
チェックリストの前に知っておくべきセキュリティガイド

４：ネットワークとクラウド

NO.	対策
SSL1	業務クラウドの通信をSSLに限定すること。
CLD1	運用ルールにて他のシステム同期アプリを禁止し、MDMなどでインストールアプリを監視すること。
CLD1	業務クラウド接続時に他のシステム同期アプリの有無をチェックすること。

FTAによる情報漏洩リスクに対するチェックリストより

なりすまし公衆Wi-Fiから情報が漏洩する



Wi-Fi自動接続

公衆無線LANのホットスポットになりすまして接続した端末とのデータのやり取りを傍受する犯罪をWfiフィッシングと呼びます。通信が暗号化されていない場合は、犯人はインターネットでやりとりした内容が盗むことが可能です。特にスマートフォンはWi-Fiの自動接続を有効にしていると、ユーザーが気づかず上記のようななりすましホットスポットに接続してしまうリスクがあります。

「米国ラスベガスで開催されたネットワーク機器の総合展示会「Interop 2005」で，無料の公衆無線LANサービスのAPになりすました不正APが見つかったのだ。発見した米エアーディフェンスによると，その不正APは接続 してきた端末に偽のページを表示。そのページのどの場所をクリックしても，ウイルスを自動的にダウンロードする仕組みになっていたという。」

※参考サイト [14]

個人向けクラウドサービスが機密情報を吸い上げる危険性

個人情報のデータ同期

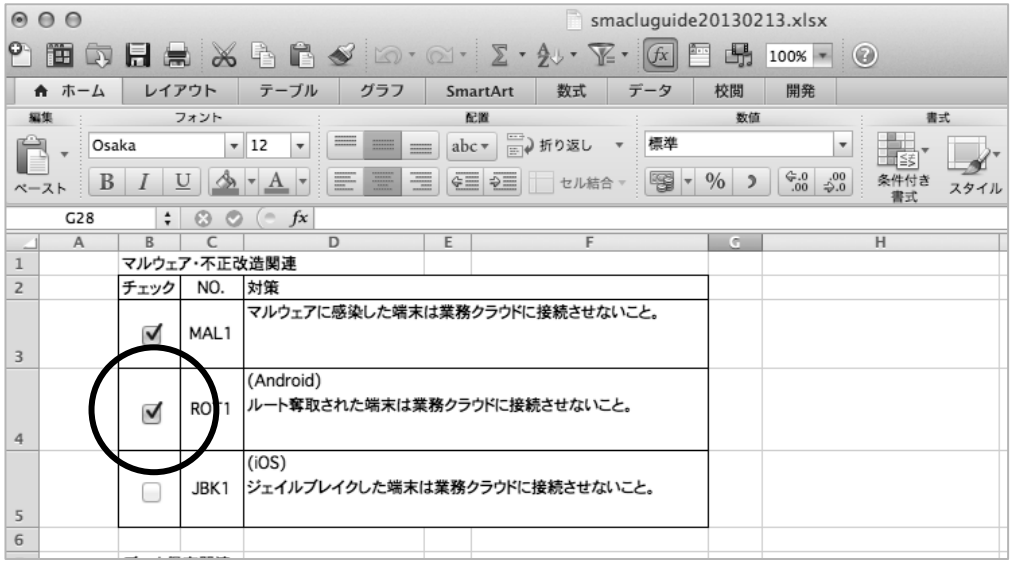
クラウドサービスによっては端末内に保存されたアドレス帳、予定表、画像などをクラウドと自動同期するものがあります。しかし場合によってはユーザーの設定ミスや認識不足により、意図せず端末データがクラウドにアップロードされるリスクがあるということです。

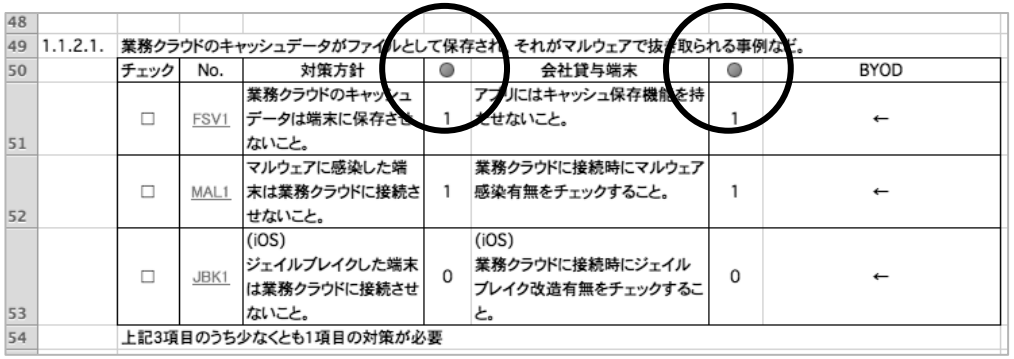
今後様々なクラウドサービスの端末内データの自動同期機能を実装することが考えられます。端末内にデータを保存させる場合はこれらのリスクに対しても考慮することが必要となります。

Facebook同期設定画面

Dropbox同期設定画面

第五章 チェックリストの使い方（会社貸与端末とBYOD）





チェックリストの使い方

添付のエクセルファイルにて、対策済みまたは対策予定のセキュリティの内容をチェックしてください。

それらの条件によって対策できている情報漏洩ケースについては緑色、対策が不十分な情報漏洩については赤色のアイコンが表示されます。

FTAによりANDの条件についてはどれか一つでも対策されていれば対策済みとなります。OR条件の場合は全ての対策が必要となります。

会社貸与端末とBYODの定義

会社貸与端末

会社貸与端末とは端末の管理主体者が企業のシステム管理者となります。多くのケースではMDMなどの端末管理ツールが適用され、必要な場合はシステム管理者が端末の状態を確認することができます。
このためユーザーは故意に端末やOSを改造したり、許可されないアプリケーションをインストールする危険性が低いと言えます。

BYOD（個人所有端末の業務利用）

個人所有端末は基本的には企業側が端末の管理をすることができません。したがってユーザーが端末やOSの不正改造や許可されないアプリケーションのインストールの危険性がありますから、BYODと呼ばれる個人所有端末の業務利用を許可する場合は、より情報漏洩に配慮したセキュリティ対策が必要となります。

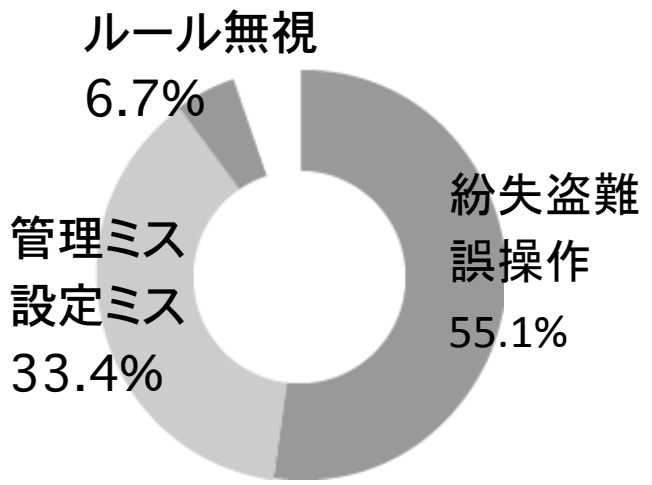
本チェックリストでは、ユーザーの故意の漏洩要素がない端末を「会社貸与端末」、故意の漏洩要素があり得る端末を「BYOD」と定義します。

情報漏洩における
両者のリスク要因の違い

会社貸与端末

会社貸与端末とBYODのセキュリティ上の一番の違いは、ユーザーがルール無視を行う敷居の高さであると言えます。MDMがインストールされている端末ではユーザーは常に「会社側に利用内容を把握されている」という抑止力が働いているからです。
しかしユーザーがルール無視や情報漏洩を意図しないミスが原因である情報漏洩は、会社貸与端末もBYODも条件は変わらないといえるでしょう。

※下記は情報漏洩事故の原因比率です。統計はスマートフォンに関わらず全般の内容ですが、情報漏洩を意図しないミスが原因である事故が多い傾向は、スマートフォンについても同様の傾向があると推定できます。



参考文献 [16]より作成

第五章 おわりに

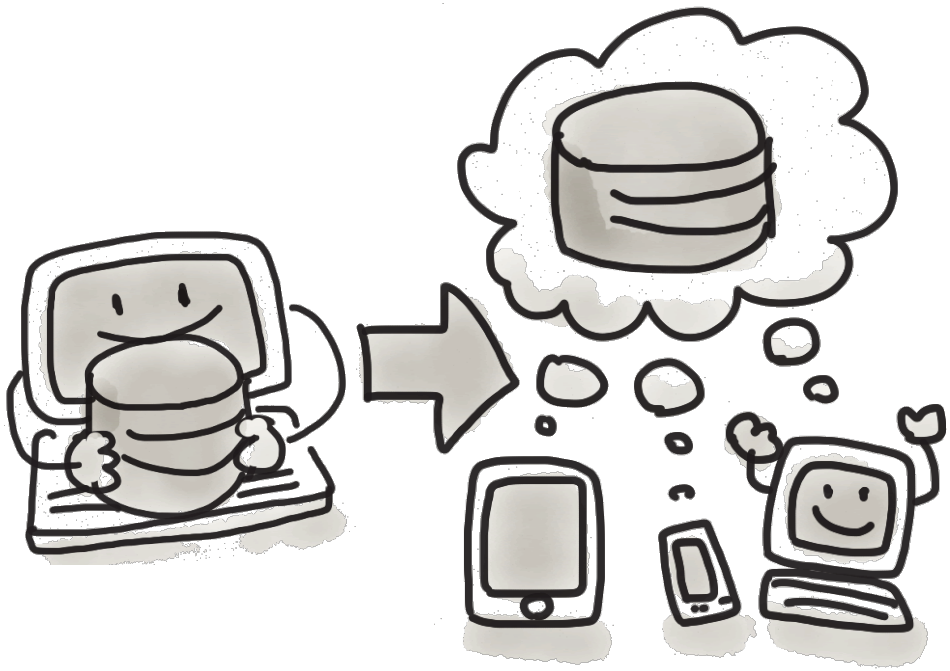
スマートフォンとクラウドの関係

私達の日常生活に浸透してきているIT文化は現在第三世代（クラウド世代）であるとみることができます。

第一世代は1970年代のパソコンの登場です。それまでメインフレームと呼ばれた大型コンピューターが小型化され家庭でも導入されるようになりました。

第二世代は2000年代から普及した常時接続のインターネットサービスです。家庭のパソコンがいつでもメールやWebで世界中に繋がるようになりました。

第三世代は2010年頃から普及し始めたクラウドサービスです。本ガイドの冒頭でも定義しましたがクラウドとは「端末の機種やOSを問わず、どこからでも自分のマスターデータにアクセスすることができる」というITコンセプトのことです。たとえサーバーがデータセンターではなく社内にあったとしても、端末のOSや機種を問わずアクセスできるシステムであれば、「オンプレミス・クラウド」と呼んでも良いクラウドシステムの一形態であると言って良いでしょう。
そしてスマートフォンはこのクラウドシステムへの接続端末として進化してきました。



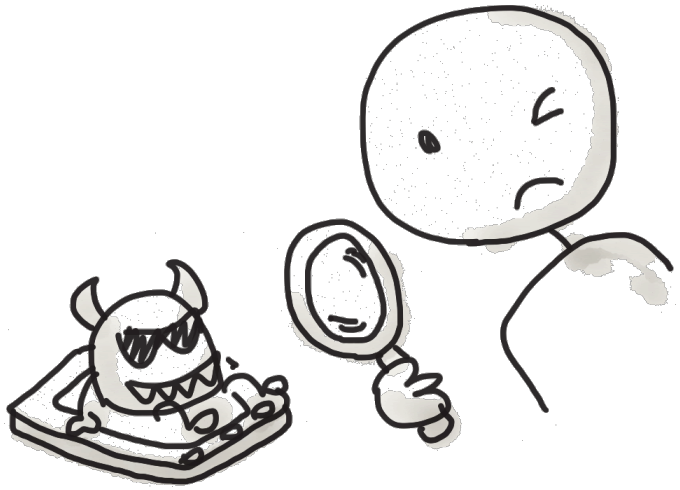
クラウド時代のスマートフォンセキュリティ

第一世代・第二世代のパソコン時代はストレージ容量が重要なスペックの一つでした。それはユーザーのマスターデータがパソコンの中に保存されるからです。

しかし第三世代のクラウド端末としてのスマートフォンはストレージ容量はユーザーにとって重要ではありません。なぜならマスターデータはクラウド上に保存されるからです。その代わりにスマートフォン端末に求められるのはクラウドシステムに接続しやすい大きなキレイな画面であり、操作性に優れたCPU能力であり太いインターネット回線です。

端末にマスターデータを持たないということは、当初私達が想像した以上に便利な世界でした。だれもが安価にいつでもインターネット繋がることができればでいるほど、マスターデータがクラウド上にあることが重要となります。

パソコン世代のセキュリティは「端末を管理すること」に主流が置かれました。しかしこれからは端末やOSに縛られないIT文化が主流になっていくことが想定されます。つまり企業側のセキュリティ意識も、パソコン時代の「端末管理」から、クラウド時代の新しいセキュリティコンセプトを視野に入れる必要が出てきつつあるといえます。



想定対策した事故は起きないという信頼性工学の基本

セキュリティを検討する上で一番大切なことは、何がリスクであるかを漏れなく洗い出すことです。
信頼性工学の基本は、「想定したことは発生しない」「想定しない事故が起こる」という考え方です。これは情報漏洩というセキュリティを検討する場合も共通します。

どういう対策をするかは企業のポリシーによります。対策にかかる費用や工数と、情報漏洩が起きた場合の損失でバランスを取るべきです。しかしどういうリスクがあり得るかということはリスクケースは漏れ無く洗い出されるべきです。
本ガイドではそのために「FTA(Fault Tree Analysis)」という手法を試みてみました。

クラウドシステムの接続端末としてのスマートフォンは、従来にない新しいIT文化の端末として進化しつつあります。果たして従来のパソコン文化の延長線のセキュリティ対策で十分なのか。もし不十分だとすると何が危ないのか。

それを検討するには「何が危ないのか」をまず漏れ無く洗い出すことが必要です。

継続的なリスク検討こそが安全性を維持する方法

今回スマートフォンの業務クラウド情報の漏洩対策として信頼性工学の手法を取り入れる試みを行いました。このガイドが多くの企業のシステム管理者の方々のお役に、少しでも立つことを願ってやみません。

FTAの真髄はリスクの洗い出しの検討を続けることにあります。リスク洗い出しに完成形はないからです。スマートフォンに関するセキュリティの技術は日々変化しています。それに伴い本ガイドも改定更新を続けたいと考えています。

参考サイト・参考文献

[1] McAfee「Android マルウェアの過去、現在、そして未来」
http://www.mcafee.com/japan/media/mcafeeb2b/international/japan/pdf/enterprise/wp_android-malware.pdf

[2] GIGAZINE「Androidの「the Movie」アプリで数万件～数百万件の個人情報が大量流出した可能性あり」
http://gigazine.net/news/20120413-android-the-movie

[3] KASPERSKY SECURELIST「Malware in the Android Market」
http://www.securelist.com/en/blog/11184/Malware_in_the_Android_Market

[4] iKeyMonitor公式サイト
http://global.ikeymonitor.com

[5] モバイルスパイ公式サイト
http://www.spy-mobile-phone.com/ja/

[6] TechCrunch Japan「Androidに初めてのボットネット型マルウェア（トロイの木馬）が出現」
http://jp.techcrunch.com/archives/20101229lookout-identifies-advanced-android-trojan-but-youre-probably-safe/

[7] Trend Labs SECURITY BLOG「Android端末を狙う標的型サイバー攻撃の兆候をLuckycat のインフラに確認」
http://blog.trendmicro.co.jp/archives/5940

[8] ITメディア・ニュース 2009年11月9日「「初のiPhoneワーム」をセキュリティ企業が発見」
http://www.itmedia.co.jp/news/articles/0911/09/news044.html

[9] Symantec「The Symantec Smartphone Honey Stick Project」
http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide_honeystick

[10] Fraunhofer SIT「Lost iPhone? Lost password !」
http://www.youtube.com/watch?v=uVGiNAs-QbY

[11] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith
Department of Computer and Information Science – University of Pennsylvania「Smudge Attacks on Smartphone Touch Screens」
http://static.usenix.org/event/woot10/tech/full_papers/Aviv.pdf

[12] FRIEDRICH-ALEXANDER UNIVERSITAT「FROST: Forensic Recovery Of Scrambled Telephones」
https://www1.informatik.uni-erlangen.de/frost

[13] 金融情報システムセンター「FISCガイドライン安全対策基準」

[14] Nikkei BP net「SAFETY JAPAN セキュリティの今を読み解く 10のキーワード 第三回 Wi-Fiフィッシング」
http://www.nikkeibp.co.jp/sj/2/column/u/03/

[15] NPO 日本ネットワーク・セキュリティ協会 セキュリティ被害調査ワーキンググループ「2011年 情報セキュリティインシデントに関する調査報告書 ～個人情報漏えい編～ 漏えい原因比率（件数）」
http://www.jnsa.org/result/incident/data/2011incident_survey_ver1.0.pdf

【日本スマートフォンセキュリティ協会】

スマートフォンセキュリティの最新情報については、
JSSECの Facebook, Twitter でも発信しています。
是非ご利用ください。

Face Book: http://www.facebook.com/JSSEC
Twitter: @jssec_org