第3週. サイバー脅威の主な手口・後編

メモ

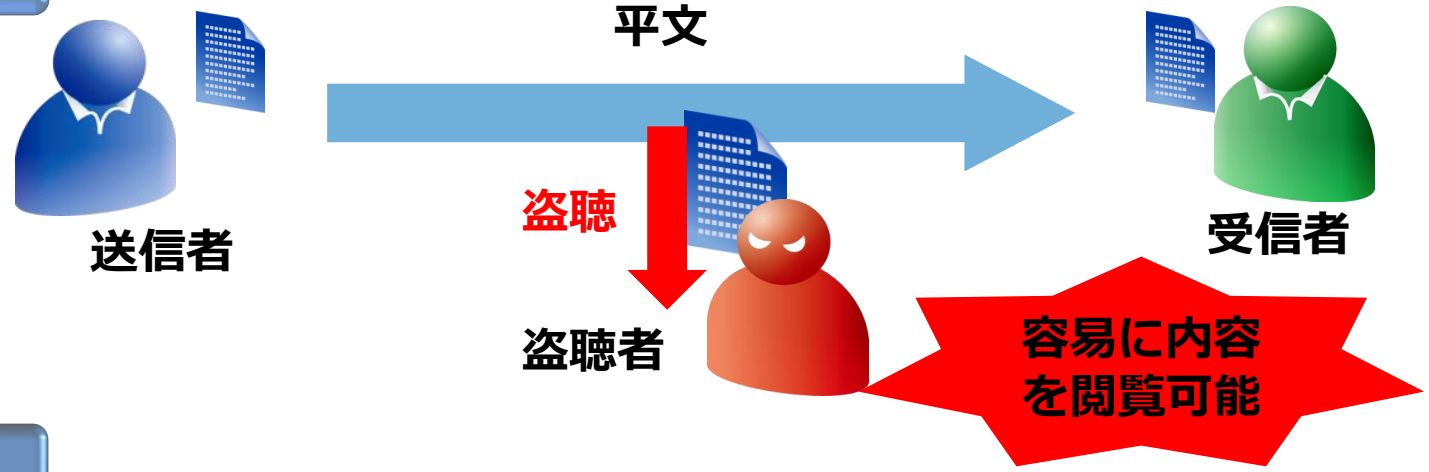
3-1. 盗聴(1)

メモ

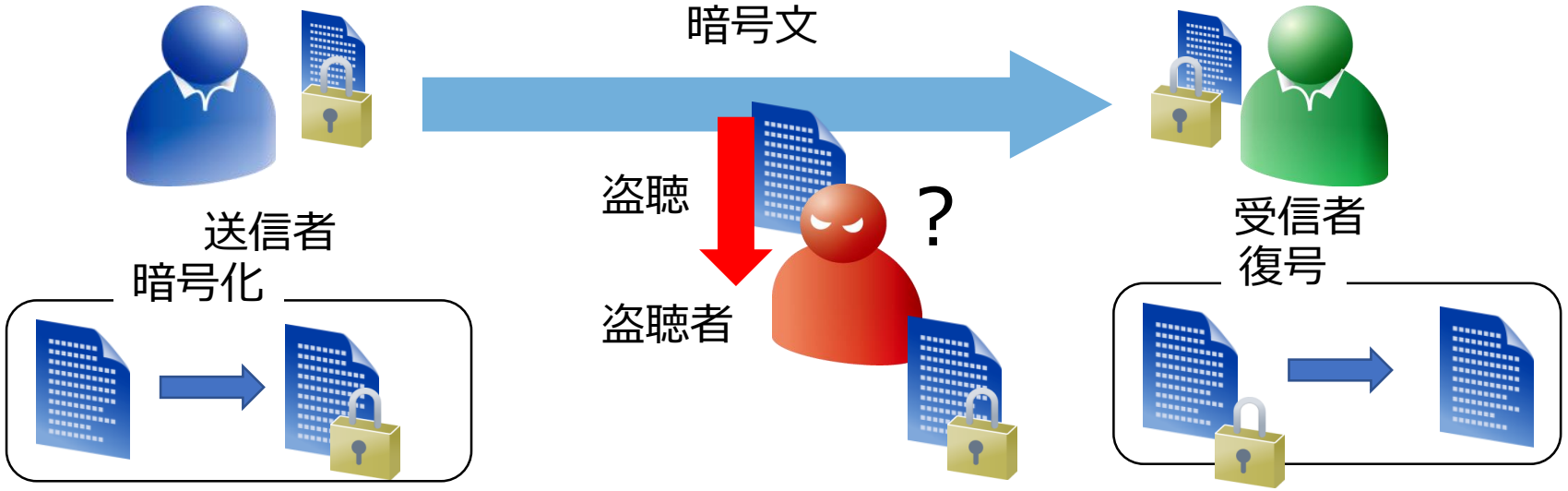
盗聴：暗号化されていない通信を狙う

メモ

平文通信

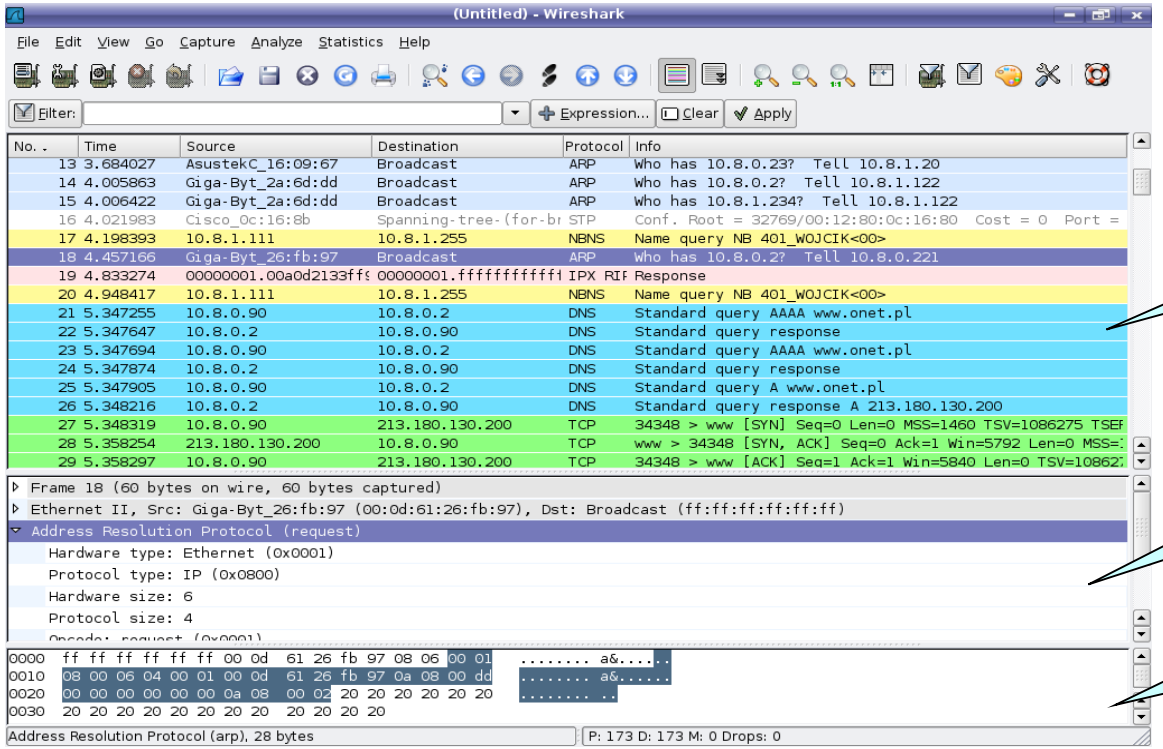


暗号通信



パケットキャプチャー

・パケットアナライザーを使用することで、ネットワークを流れるパケットを捕捉し、分析することができ、悪用すれば「盗聴」となる



キャプチャしたパケットの一覧。時間順に並んでいる。

プロトコル階層別に解析して表示された詳細画面。

16進法で表示された詳細画面。

http://www.wireshark.org/

メモ

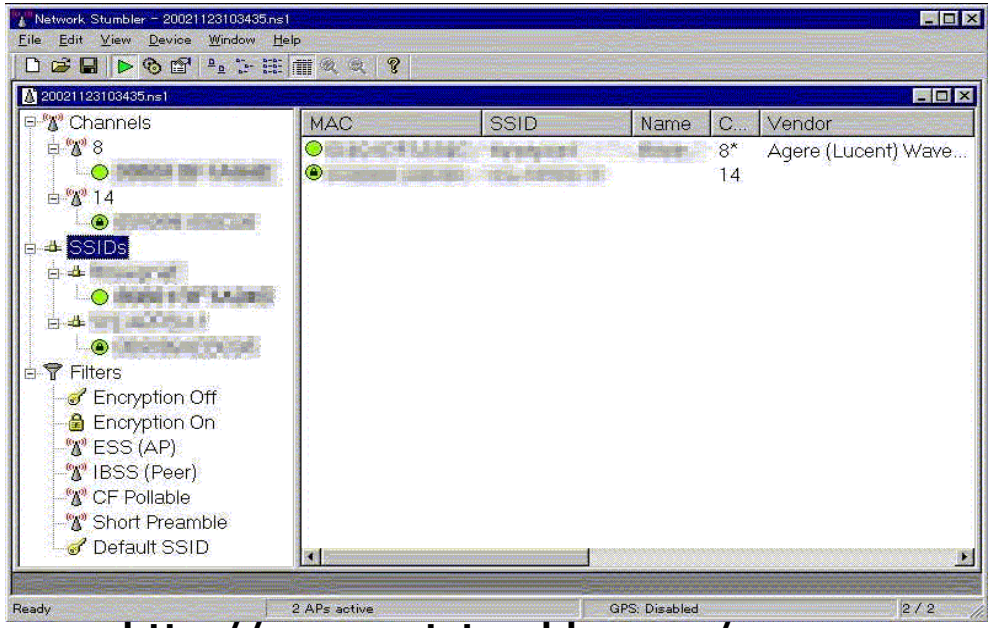
3-2. 盗聴(2)

メモ

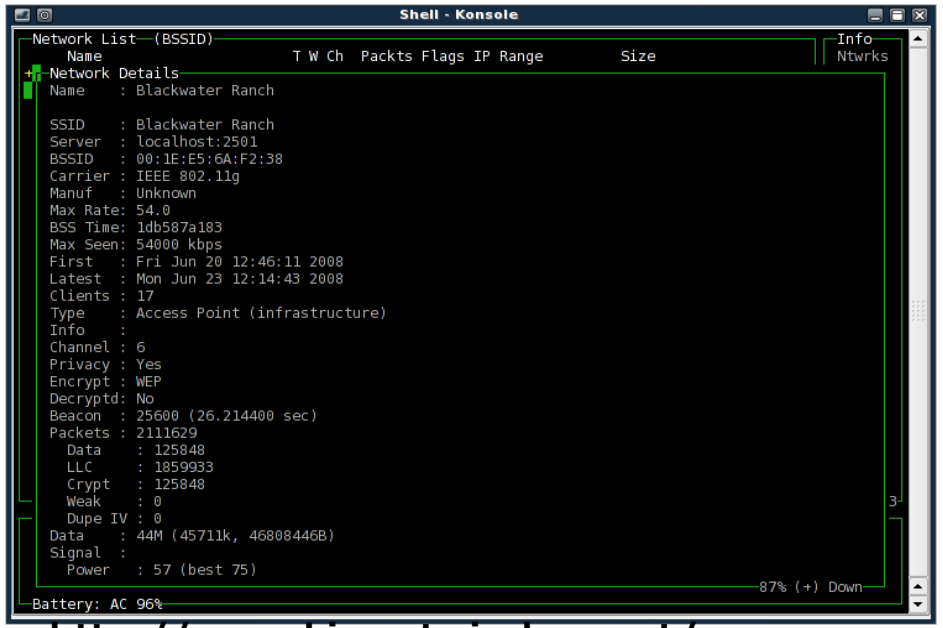
無線ネットワークのスキャンツール

無線ネットワークのスキャンツールを利用して、セキュリティの設定のないアクセスポイントがないかどうか、電波がどこまで届いているか、ESSID、WEP、MACアドレス制限などの基本的なセキュリティ対策ができているかどうか、などをテストする。

主なツールには、「NetStumbler」「Kismet」などがある。



http://www.netstumbler.com/



http://www.kismetwireless.net/

メモ

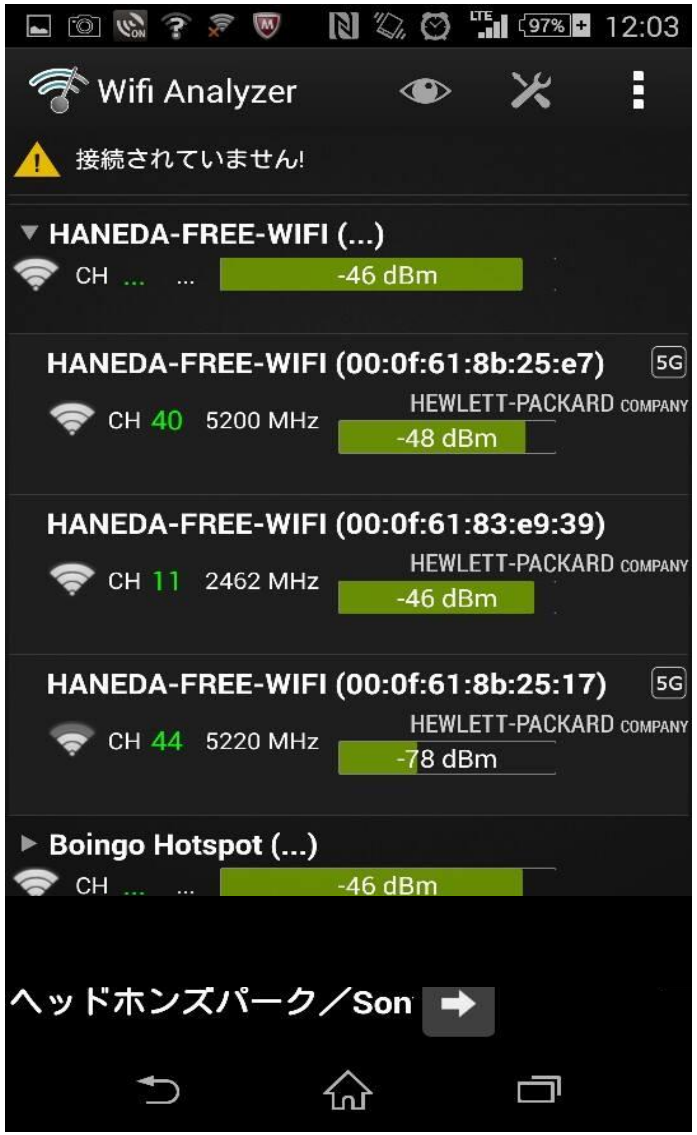
「ウォードライビング」

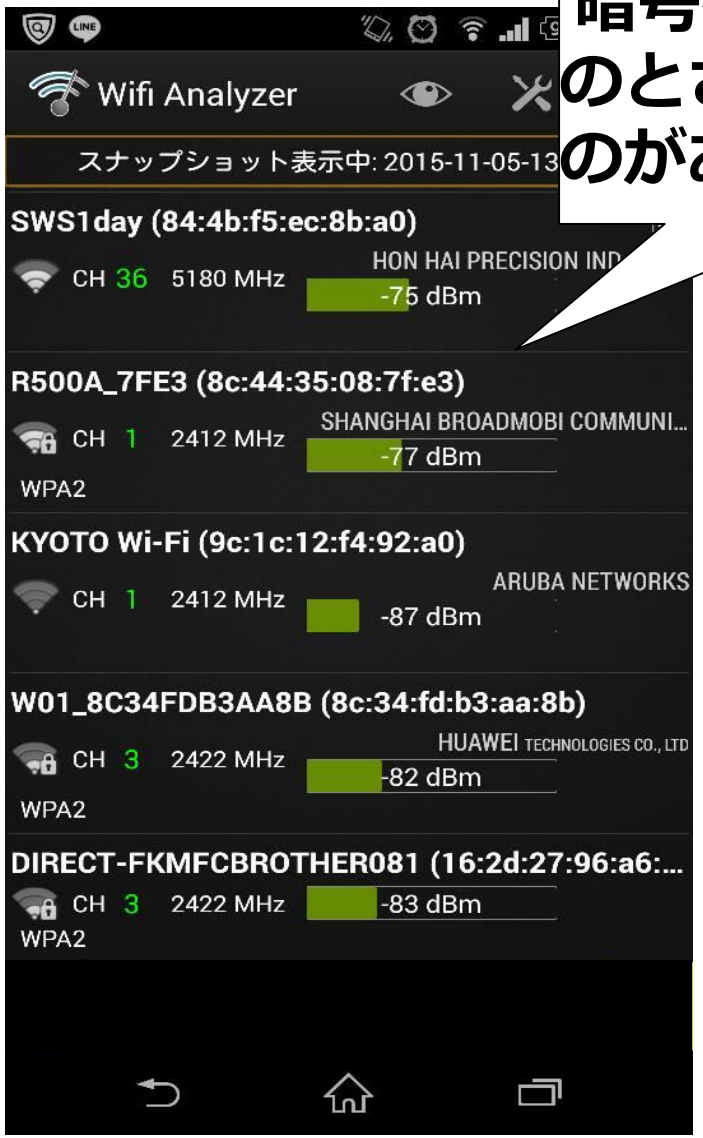
ツールにより、アクセスポイントのMACアドレスSSID (ESS-ID)、ネットワークの名称使用している周波数のチャンネル、無線ＬＡＮカードのチップセットのベンダー（メーカー）名、WEP暗号の使用 / 未使用、インフラストラクチャ / アドホックモード、信号のレベル（強弱）、電波のノイズレベル、などを知ることができる。

GPSなどと組みあわせ、「ウォードライビング」なども行われる。

メモ

公衆アクセスポイントの通信





暗号化されているものとされていないものがある

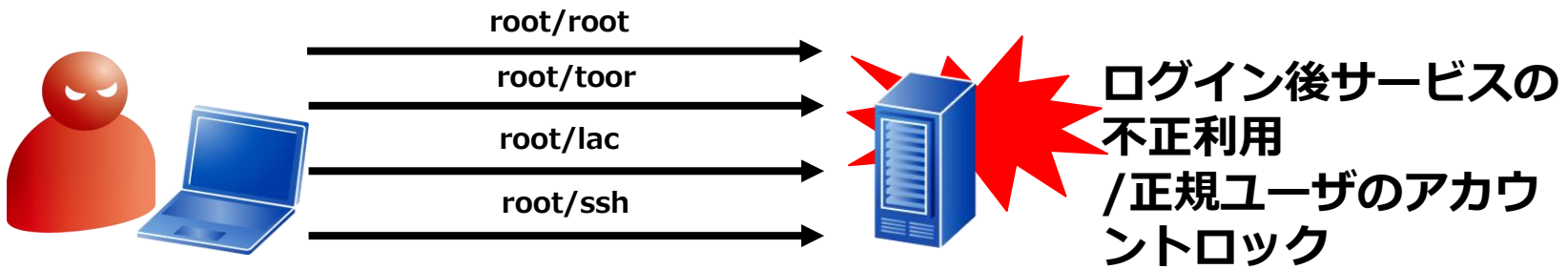
メモ

3-3. パスワード解読(1)

メモ

パスワード解読

パスワード認証が施されている、サービスやアプリケーションに接続し使用されているアカウント名/パスワードの組み合わせを調査する攻撃



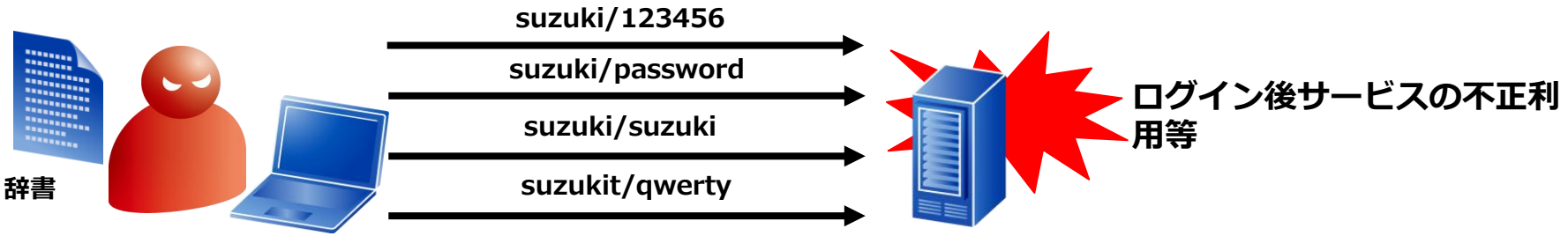
総当り(ブルートフォース)攻撃
あるアカウントに英数字・記号全ての組合わせのパスワードを入力する攻撃

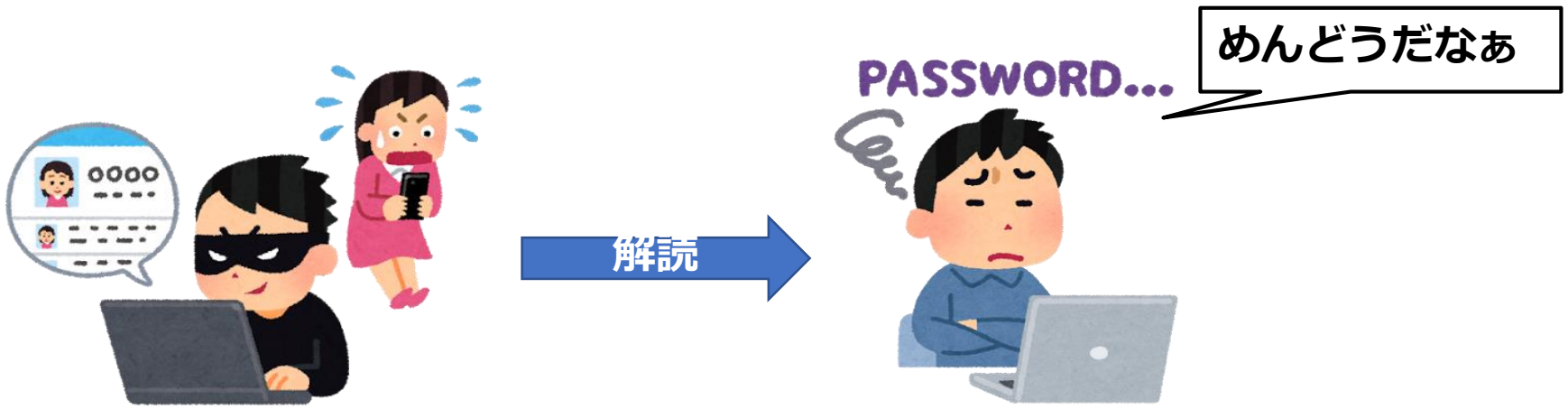
逆総当り(リバースブルートフォース)攻撃
アカウントロックを防ぐため、1つのパスワードで次々にアカウント名を変えてログインを試みる攻撃

メモ

「辞書攻撃」

製品やインターネットのサービスなどでデフォルト（初期設定）で使用されている、または、ユーザーがよく使いそうなログインIDとパスワードの組み合わせを「辞書」として準備し入力する攻撃





メモ

3-4. パスワード解読(2)

メモ

パスワードの強度

IPA コンピュータウイルス・不正アクセスの届出状況[2008年9月分および第3四半期]について

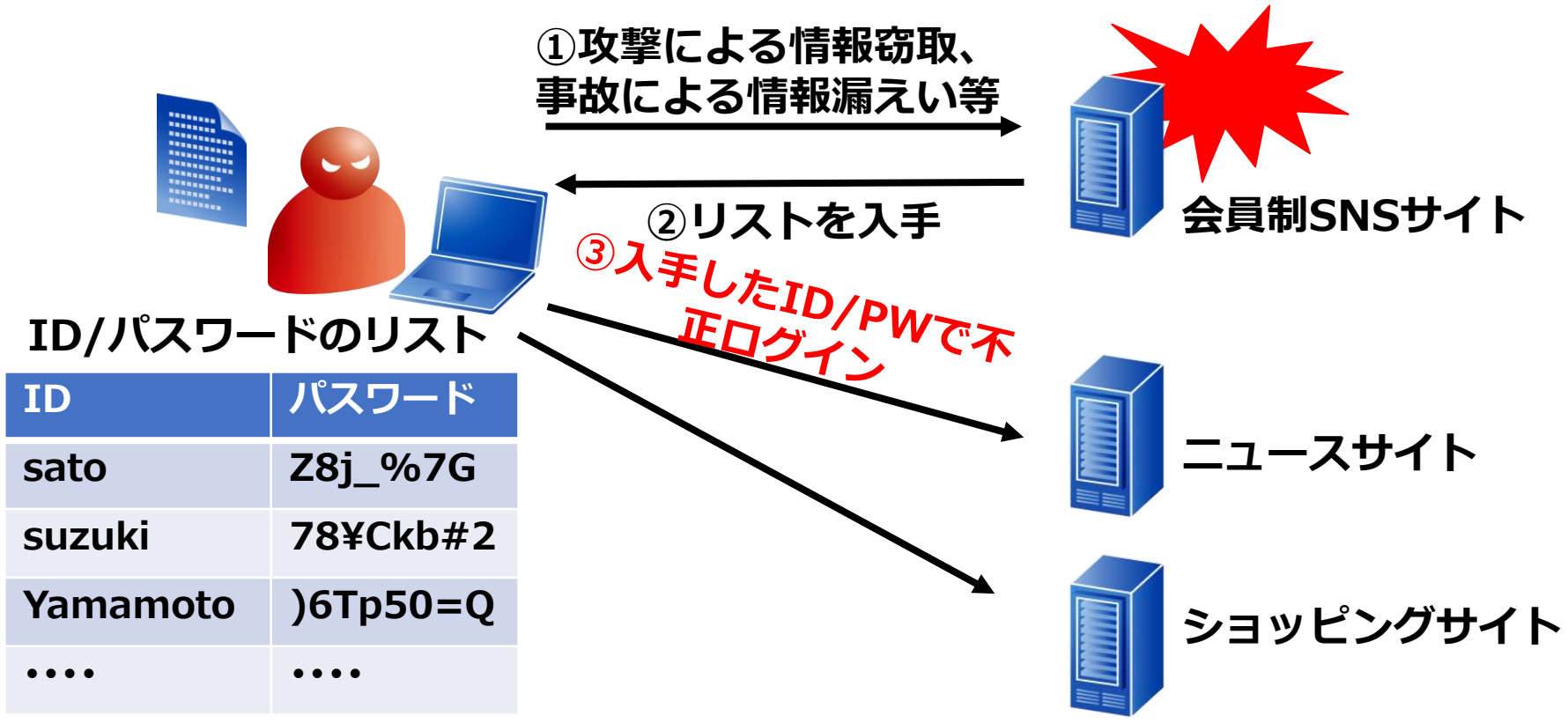
使用する文字の種類	使用できる文字数	最大解読時間			
		入力桁数			
		4桁	6桁	8桁	10桁
英字 (大文字、小文字区別し)	26	約3秒	約37分	約17日	約32年
英字(大文字、小文字区別あり) + 数字	62	約2分	約5日	約50年	約20万年
英字(大文字、小文字区月あり)+記号	93	約9分	約54日	約1万年	約1千万年

※すべての組み合わせを試すために必要な時間を計算。記号は31文字使用できるものとした。使用パソコンOS：Windows Vista Business 32bit版、プロセッサ：Intel Core 2 Duo T7200 2.00GHz、メモリ：3GB

メモ

「リスト型攻撃」

別のWebサイトなどから入手したユーザーIDとパスワードのリストを使って不正ログインを試行するする攻撃



ID/パスワードのリスト

ID	パスワード
sato	Z8j_%7G
suzuki	78¥Ckb#2
Yamamoto	)6Tp50=Q
….	….

メモ

3-5. マルウェア(1)

メモ

マルウェアの種類

・「マルウェア」とは、重要データの破壊や奪取、リソース消費、コンピュータの遠隔操作等を意図した、”悪意あるプログラム”の総称である。

・別称としてコンピュータウイルス、不正プログラムなどと呼ばれる。

マルウェアは、その特性や挙動からいくつかの類型に分類できる。

ウイルス	ワーム	トロイの木馬	rootkit
ボット	キーロガー	スパイウェア	ダウンローダー

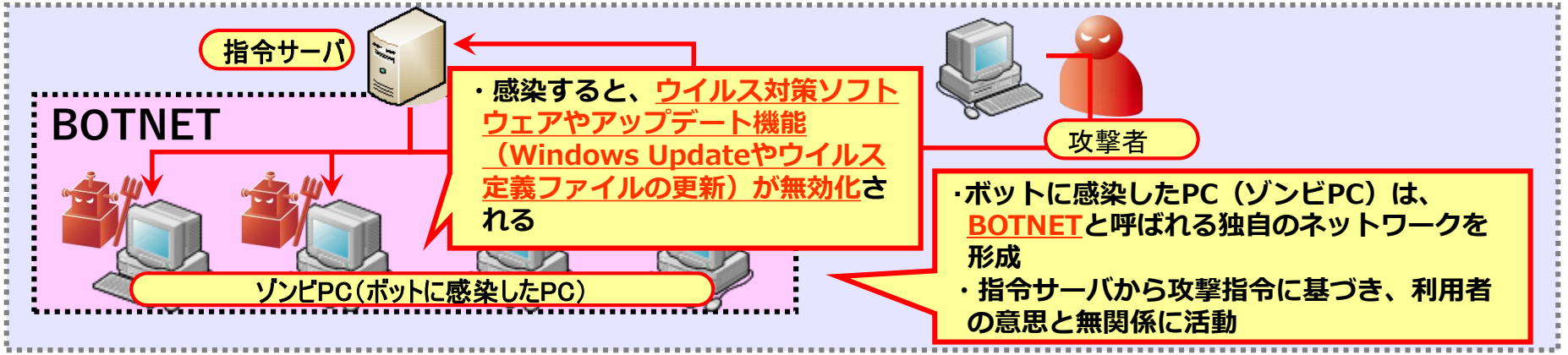
メモ

ボット （BOT）

・コンピュータを悪用することを目的に作られた悪性プログラム。
・攻撃者は、インターネットを通じて感染コンピュータを外部から遠隔操作することが可能。
・迷惑メールの大量配信、特定サイトへの攻撃等の迷惑行為をはじめ、コンピュータ内の重要情報を盗み出すスパイ活動を行う。

混入経路

ワームやウイルスの感染形態と同様
・ファイル経由、ネットワーク経由で感染活動が行われる



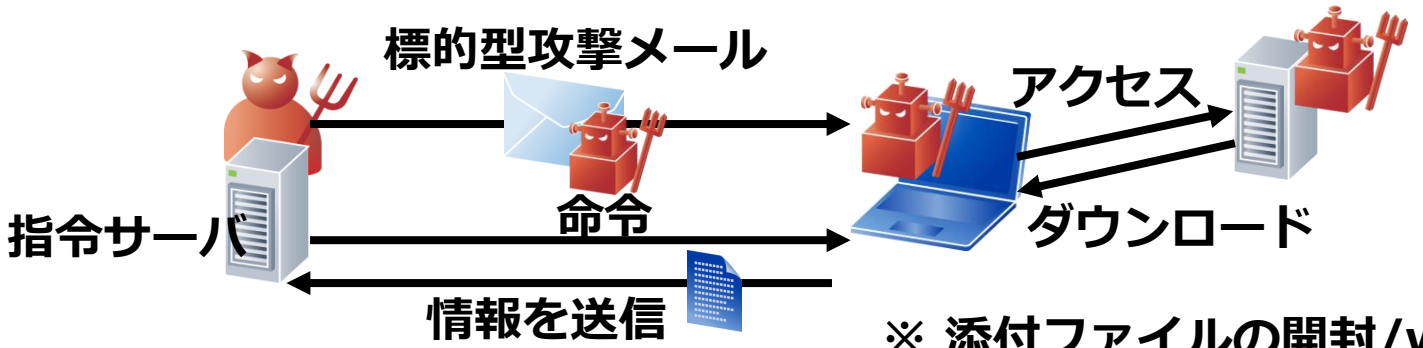
メモ

3-6. マルウェア(2)

メモ

「標的型攻撃」とは

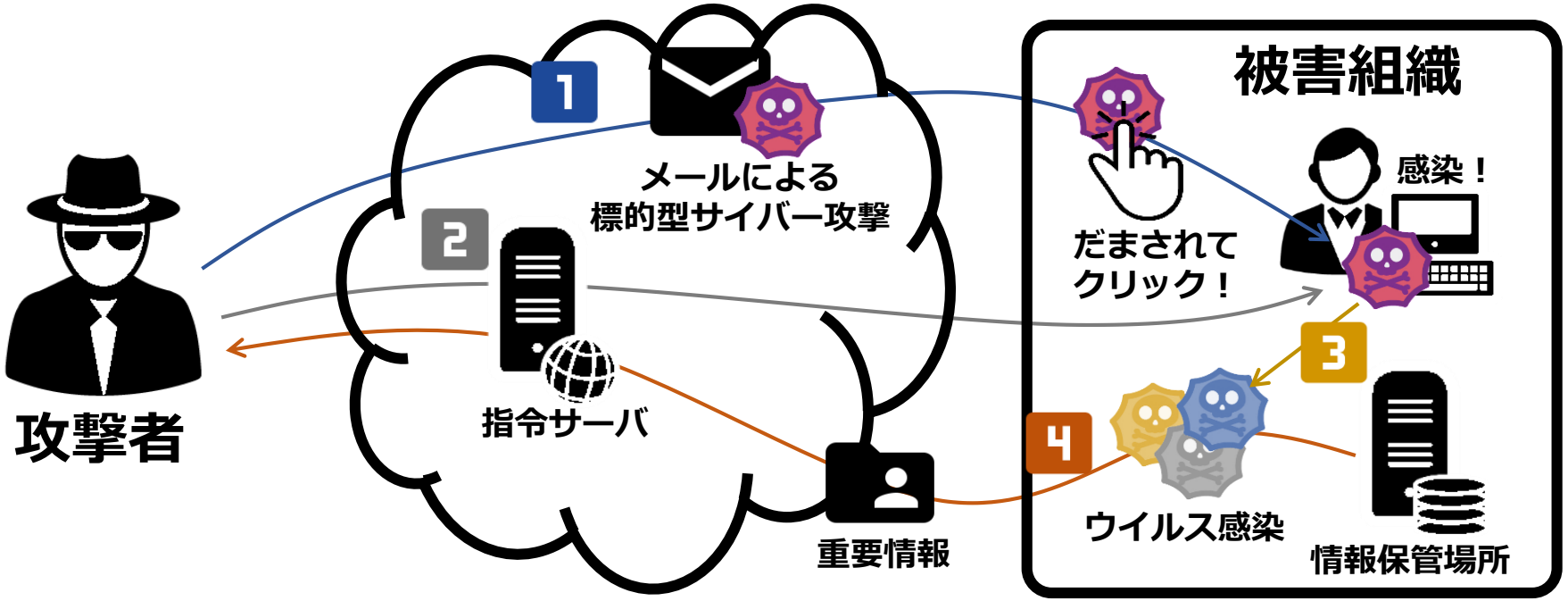
「標的型攻撃（Targeted Attack）」とは、特定の組織内の情報を狙って行われるサイバー攻撃の一種。
　メールの添付ファイルやウェブサイトを利用してPCにマルウェアを感染させ、遠隔操作し重要情報を窃取する攻撃。



※ 添付ファイルの開封/webサイトへのアクセスにより感染

メモ

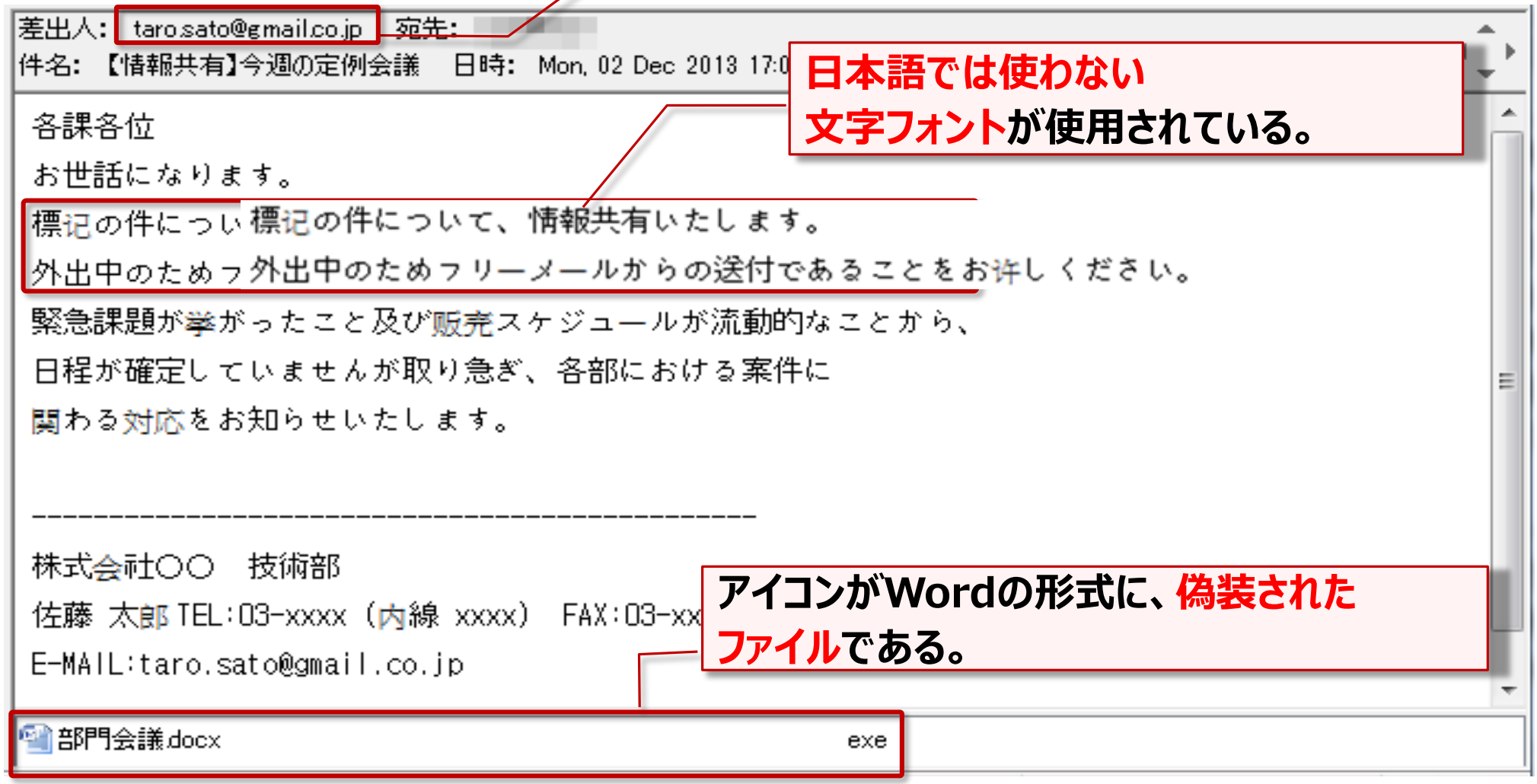
「標的型攻撃」の流れ


1
メールによる
標的型サイバー攻撃
2
指令サーバ
攻撃者
重要情報
被害組織
だまされて
クリック！
感染！
3
4
ウイルス感染
情報保管場所

メモ

「標的型攻撃」メールの例

社内から送信されたような本文であるが、
メールアドレスがフリーメールアドレスである。



日本語では使わない
文字フォントが使用されている。

アイコンがWordの形式に、偽装された
ファイルである。

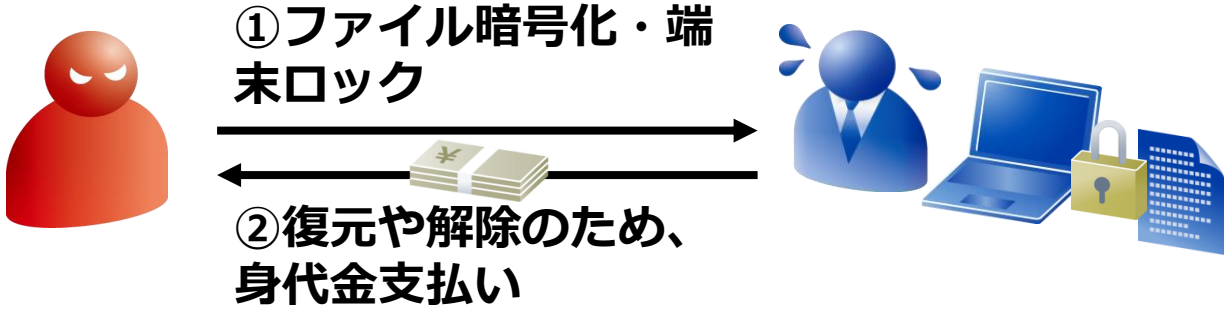
メモ

3-7. マルウェア(3)

メモ

ランサムウェア(Ransomware)

端末内のファイルの暗号化やロックにより、閲覧・編集・実行をできなくする。その復元や解除のために「身代金(Ransom)」を払うことを要求する機能を持つマルウェア(Malware)。



メモ

＜事例＞「WannaCry」:2017年5月

～IPAセキュリティセンター

メモ

ランサムウェア:身代金の要求

元に戻したければ、
金を払え！

払わなければ、
ファイルをさらす！

「JSOC INSIGHT vol.11」～ラック、2016年5月17日
http://www.lac.co.jp/security/report/pdf/20160517_jsoc_m001t.pdf

メモ

3-8. マルウェア(4)

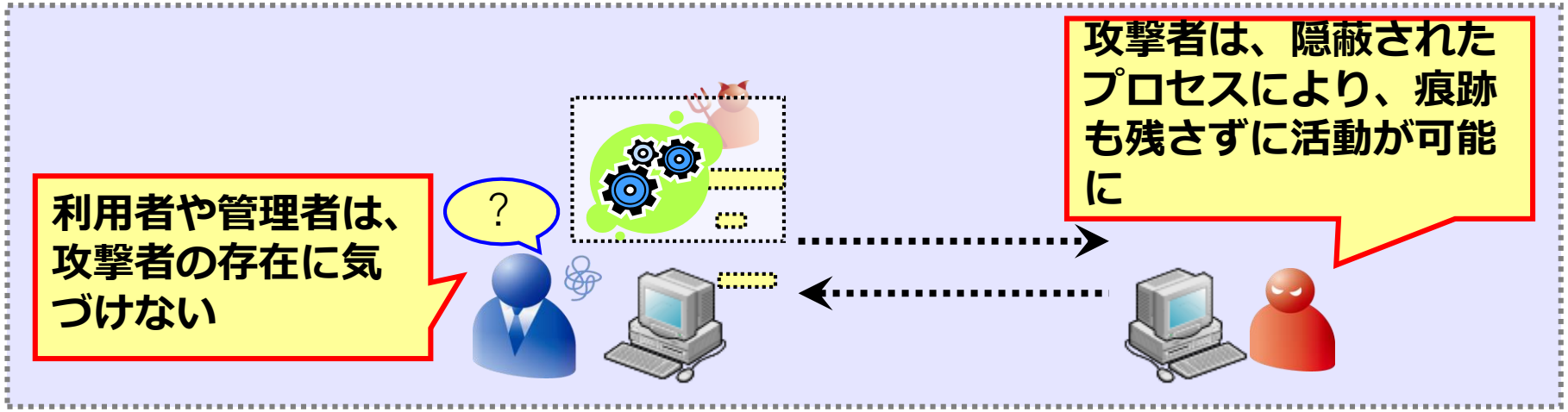
メモ

ルートキット（rootkit）

攻撃者が次回の侵入を容易にするツールや、ログ削除ツール、攻撃者（セッション、ネットワーク接続、ファイル、プロセス他）の存在を隠蔽するツールなどが含まれる。

混入経路

侵入に成功した攻撃者による設置、媒体からの混入

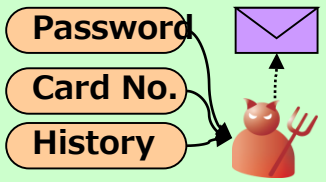


メモ

その他のマルウェア

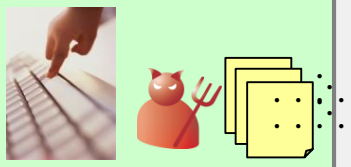
メモ

スパイウェア



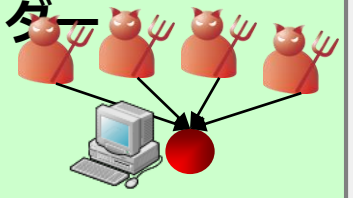
・利用者のプライバシー情報を収集し、外部に送信するプログラム
・フリーソフトとともに導入されるケースが多い
・アンチウイルスソフトで検知されず、削除が困難なケースもある

キーロガー



・利用者のキーストローク（キーボード入力）をひそかに記録し、外部に送信するプログラム
・他の不正プログラム（ウイルス・ワーム・トロイの木馬・スパイウェア・BOT）が一機能として持っているケースが多い

ダウンローダー



・インターネット上の（悪意ある）Webサイトから、不正プログラムをダウンロード・インストールするプログラム
・形態は様々であり、Webサイトにアクセスしただけで自動実行されるJavascriptやActiveXコントロールの形態をとるものもある。

3-9. その他の脆弱性を突く攻撃

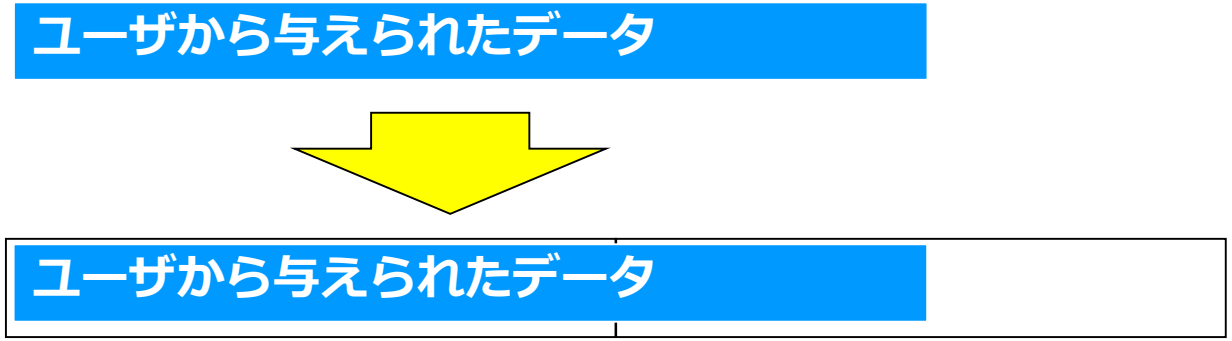
メモ

バッファオーバーフロー攻撃

・データをバッファへコピーする際、コピー元のサイズが、コピー先のバッファのサイズより大きい場合、構わず関係のないメモリ領域を上書きする。

・データのコピーなどでメモリ領域が壊れてしまった状態を、バッファオーバーフロー状態という。

・サイズチェックをせずに、文字列コピーをすることで、バッファオーバーフロー状態に陥ることが多い。



関係のないBuffer2の領域を上書きしてしまう

メモ

SQLインジェクション

メモ

正常な例

利用者

ID:yamada
PW:pw001

Select * from USER where
ID= ‘yamada’ and pass= ‘pw001’

Webサーバ

DBサーバ

Yamadaユーザの情報を含むページ

Yamadaユーザの情報

攻撃例

攻撃者

ID:111’ OR ‘A’=‘A’; --
PW:111

Select * from USER where
ID= ‘111’ OR ‘A’=‘A’; --’ and pass= ‘111’

Webサーバ

DBサーバ

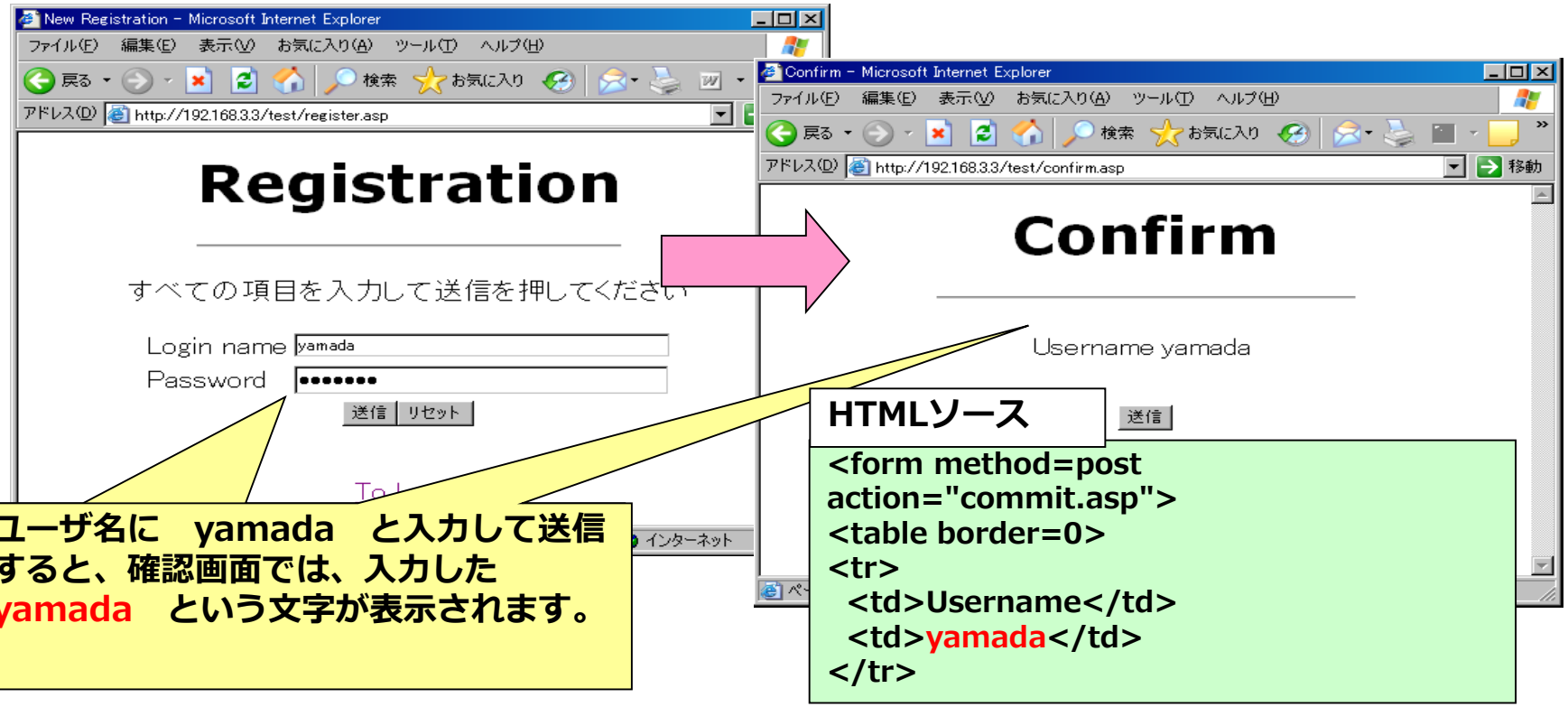
全ユーザの情報を含むページ

全ユーザの情報

クロスサイトスクリプティング(1)

攻撃対象がサーバではなく、ユーザのWebブラウザ。攻撃者は利用者のWebブラウザ上に悪意のスクリプトを送り込み、実行させる。

正常な例



ユーザ名に　yamada　と入力して送信すると、確認画面では、入力した yamada　という文字が表示されます。

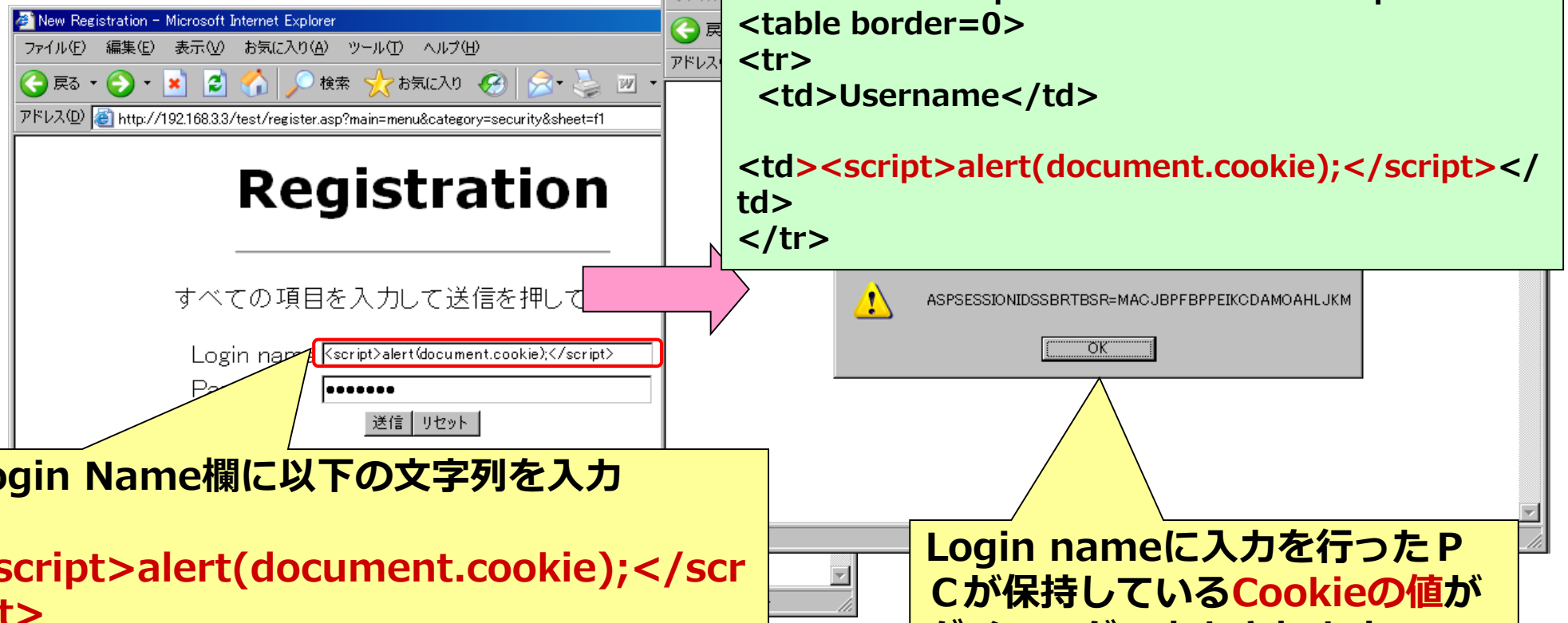
HTMLソース

```
<form method=post
action="commit.asp">
<table border=0>
<tr>
  <td>Username</td>
  <td>yamada</td>
</tr>
```

メモ

クロスサイトスクリプティング(2)

攻撃例



HTMLソース

```
<form method=post action="commit.asp">
<table border=0>
<tr>
  <td>Username</td>

<td><script>alert(document.cookie);</script></
td>
</tr>
```

Login Name欄に以下の文字列を入力

**<script>alert(document.cookie);</scr
ipt>**

alert() ： ダイアログを表示する命令
document.cookie ： Cookieの値

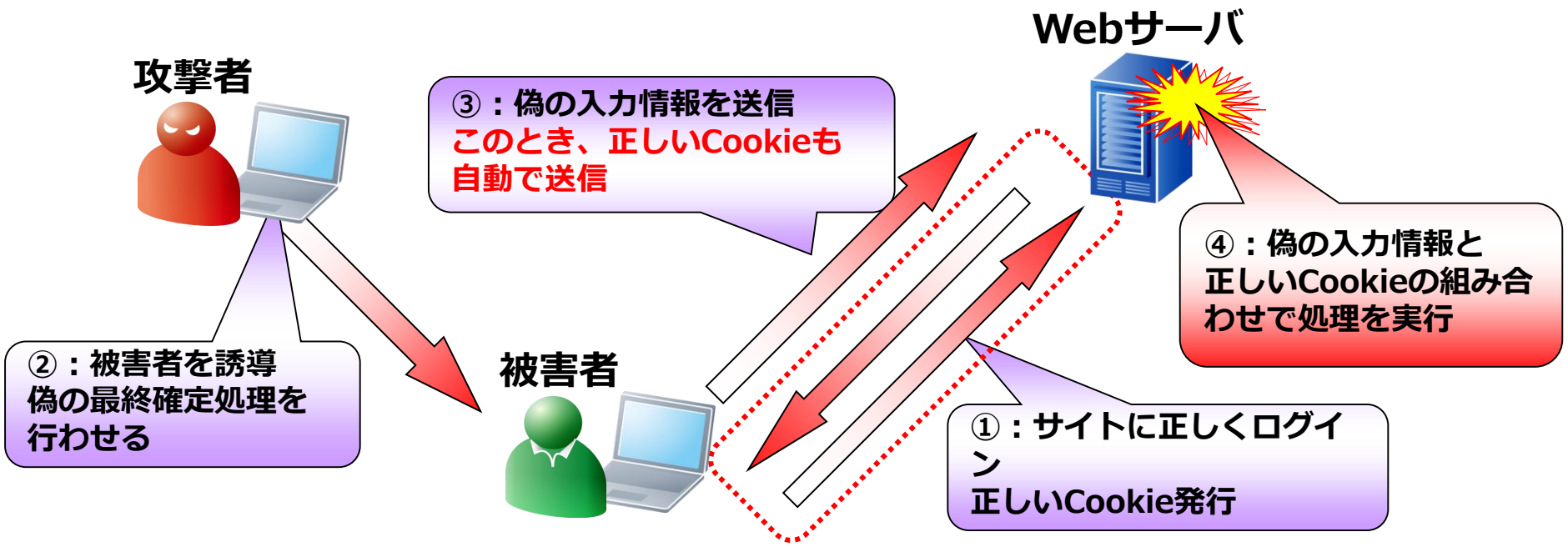
Login nameに入力を行ったＰＣが保持しているCookieの値がダイアログで出力されます。

メモ

クロスサイトリクエストフォージェリ（CSRF）

・主にCookieやBasic認証などブラウザが自動的に送信するパラメータでセッション管理を行っているWebシステムで発生

・一般的な脅威は、「なりすまし」
・強制的に攻撃者の指定した動作を「正常動作のように」実行してしまう



メモ

3-10. ソーシャルエンジニアリング

メモ

「ソーシャルエンジニアリング」とは

　攻撃や不正行為をするために必要となる重要な情報を、IT技術を使用せずに盗み出す方法。

　その多くは人間の心理的な隙や行動のミスにつけ込みだますもの。

メモ

ソーシャルエンジニアリングの手法

なりすまし

誰かになりすます
- 企業の役員
- システム管理者
- テールゲート

など

コミュニケーション

巧みなコミュニケーション
- 会話、電話
- メール
- blog、BBS

など

詐欺

相手をだます
- 信頼性
- 脅迫
- 緊急性

など

盗み見

情報収集を行う
- ごみ箱あさり
- ショルダーサーフィン
- 付箋を盗み見る

など

メモ

ソーシャルエンジニアリングの例

・なりすましにより、電話でパスワードを聞きだす
・肩越しにキー入力を見る(ショルダーハッキング)
・ゴミ箱をあさり、重要書類やメディアを探す(トラッシング)
・偽の緊急連絡先を用意する。
　⇒トラブル時に、焦らせ攻撃者に情報を伝えさせる。
・SNSのIDやアカウント情報を掲示板に書き込む。
　⇒攻撃者のアカウントに連絡させる

あらかじめ仕掛けをしておき、ターゲットがその仕掛けを踏むことで、
情報を盗み出すことも。

メモ

3-11. 内部不正

メモ

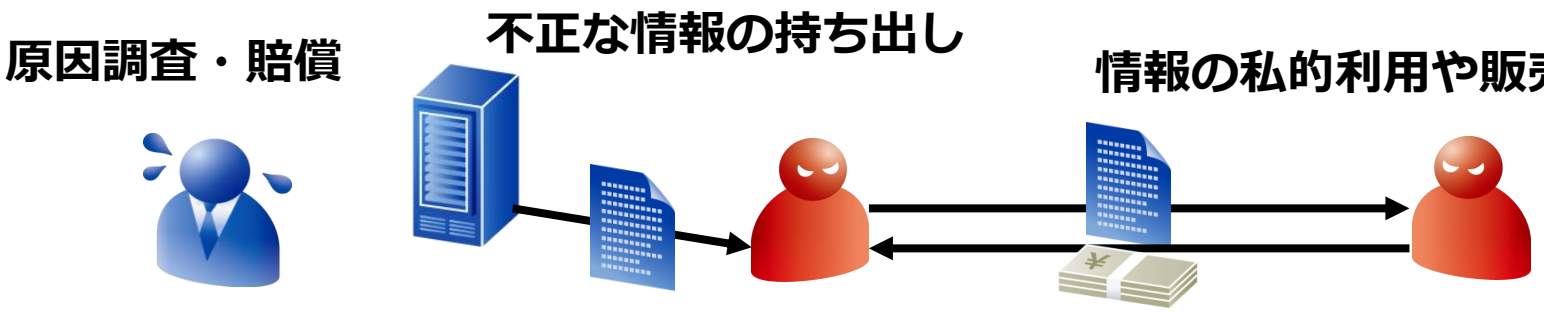
主な人的脅威

分　類	内　容
違反・不正	意図的にルールを破る違反行為
怠慢	不正目的ではないが、決められた内容を実施しない
不注意	ついうっかりのミス、エラー
その他	やり方が違う、遅い、など。リテラシーやスキル不足

メモ

内部不正の例

**金銭の取得や私的利用のために、内部犯が組織内にある情報を取得する。
情報の流出が発覚すると、原因調査、賠償などの対応により業務が停止する場合がある。**



<発生要因>

- 職場環境や処遇の不満
- アクセス権限の不適切な付与
- システム操作記録と監視の未実施

メモ

不正行為の分類

	分類	概要	不正行為の例
1	システム破壊 (IT Sabotage)	特定個人、組織（組織のデータ、システム、日常業務を含む）に損失を与えるという意志に基づいた悪意ある行動	システムの破壊・改ざん
2	知的財産の窃盗 (theft of IP)	機密や知財に関連する情報などを組織から盗み出す	顧客情報等の職務で知りえた情報の持ち出し
3	システム悪用 (fraud)	組織の財やサービスをごまかし(deception)やペテン(trickery)で手に入れる	個人情報を売買するなど職務で知りえた情報の目的外利用
4	意図しない内部不正 (Unintentional Insider Threat)	悪意のない内部者が、誤った相手に電子メール・FAXを送信する、誤ってインターネット上に公開する、紙媒体や可搬記録媒体を紛失・廃棄・盗難される	うっかりミスや不注意によるルールや規則の違反
5	その他 (miscellaneous)	上記にあてはまらないケース	上記以外のなんらかのルールや規則の違反

「内部不正による情報セキュリティインシデント実態調査-調査報告書-」IPAセキュリティセンター、2016年3月

メモ