IWASAKI GAKUEN

メモ

情報セキュリティ基礎

メモ

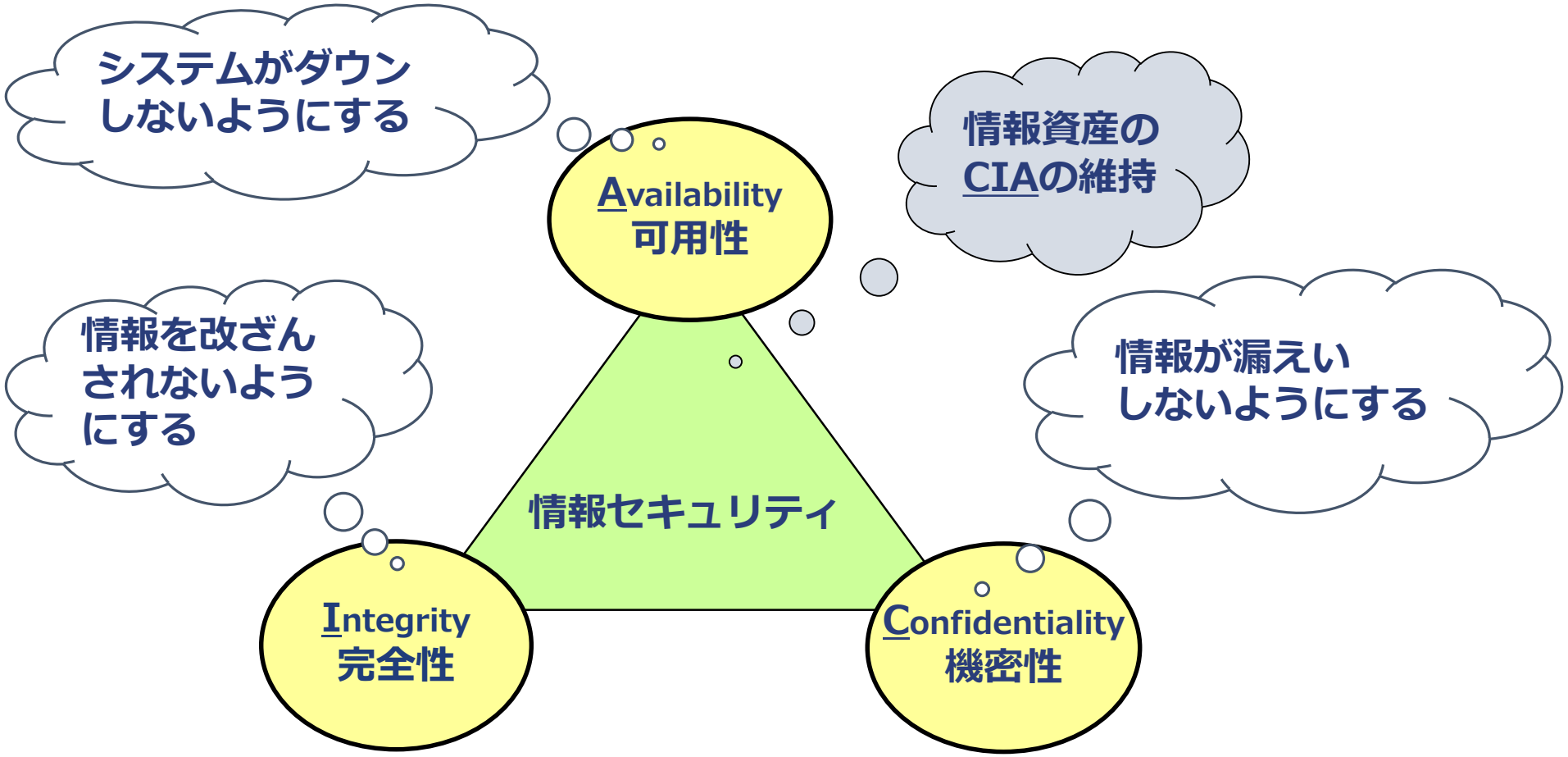
第1週. 情報セキュリティ概説

1-1. 情報セキュリティの概念

メモ

「情報セキュリティ」とは

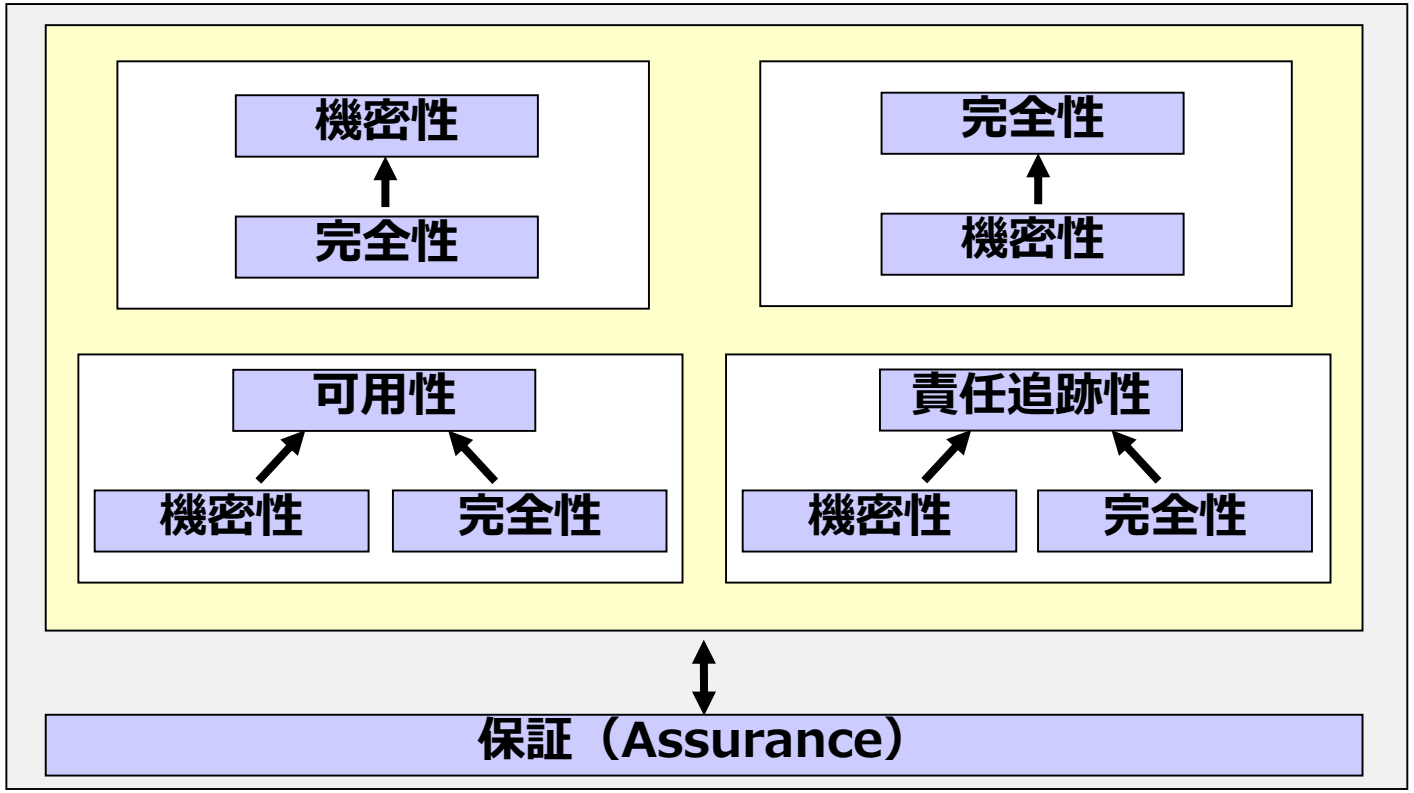
「情報セキュリティ」とは、「CIA（機密性、完全性、可用性）の維持」のための活動です。



メモ

情報セキュリティの相互依存関係

・セキュリティの要件は、相互依存関係にある
・その他の要件を考慮せずに、1つの要件のみ達成することはできない



～「ITセキュリティのための基本テクニカルモデル 」（NIST SP800-33）

メモ

情報セキュリティ対策のアプローチ

メモ

情報セキュリティにおける3つの対策

防 止	FWなどによる防止 相互牽制などによる抑止	「防止」ができたかどうかの確認には「検出」が必要
検 出	モニタリング(リアルタイム) 点検・監査（事後）	「防止」できないものは「検出」が必要。
対 応	回復・復旧、追跡、見直し エスカレーション、保証	「対応」できるためには「検出」が必要。

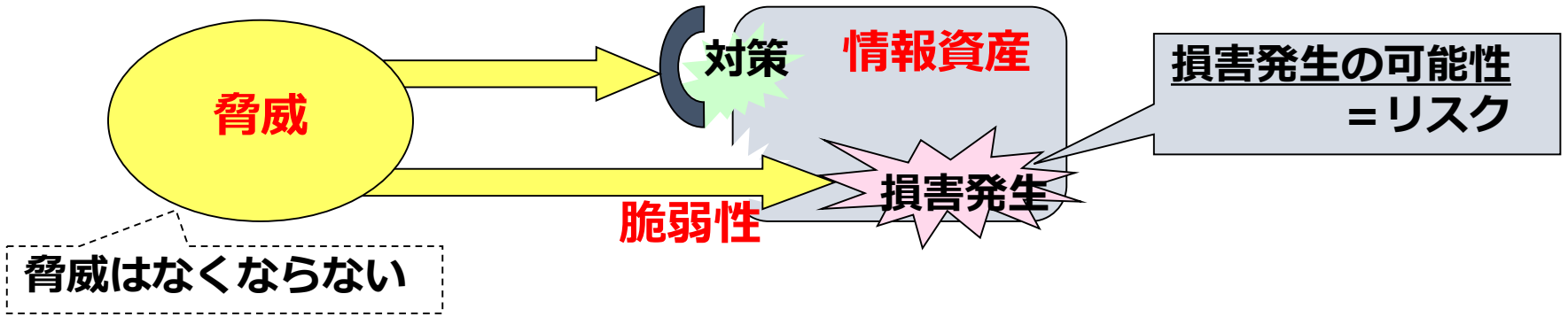
「防止」だけでは、バランスが取れた情報セキュリティ対策はできない。

1-2. 脅威と脆弱性

メモ

「脅威」とは

「脅威」とは、「組織に損害を与える可能性の『潜在的な原因』」のことです。



メモ

「脅威」の分類

悪意ある者による攻撃

盗難、ソーシャルエンジニアリング、不正アクセス、ウイルス、データの改ざん、盗聴、なりすまし、など

＝ **意図的脅威**

ヒューマンエラーや障害

紛失、盗難、操作ミス、会話からの情報漏えい、ファイル交換ソフトにおける情報漏えい、システム障害、ネットワーク障害

＝ **偶発的脅威**

災害

地震、パンデミック、火災、水害、荒天（雷、ひょう、雨、雪）、竜巻、異常気温、高湿度、建物の崩落

＝ **環境的脅威**

メモ

「脆弱性」とは？

脆弱性とは、セキュリティ上の問題箇所のことです。

・ソフトウェア製品の本来の機能や性能を損なう原因となり得る箇所

・不適切な運用により、セキュリティが維持できなくなっている状態

■脅威と脆弱性の関係

脆弱性 × 脅　威 → 被害・影響（インシデント）

メモ

主な「脆弱性」

■ソース/構造上の問題

- SQLインジェクション
- ディレクトリトラバーサル
- クロスサイトスクリプティング(XSS)
- クロスサイトリクエストフォージェリ(CSRF) など。

■設定・運用上の問題

- セッション管理の不備
- HTTPSの不適切な利用
- HTTPヘッダインジェクション
- メール不正中継 など。

メモ

1-3. 情報セキュリティインシデント

メモ

「情報セキュリティ10大脅威(組織)」

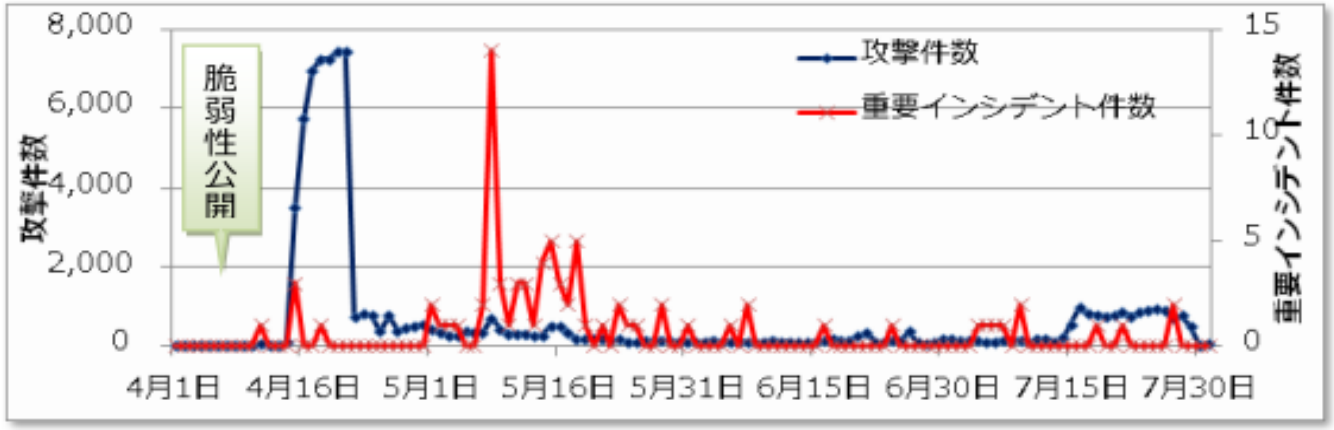
1	標的型攻撃による情報流出
2	ランサムウェアによる被害
3	ウェブサービスからの個人情報の窃取
4	サービス妨害攻撃によるサービスの停止
5	内部不正による情報漏えいとそれに伴う業務停止
6	ウェブサイトの改ざん
7	ウェブサービスへの不正ログイン
8	IoT機器の脆弱性の顕在化
9	攻撃のビジネス化（アンダーグラウンドサービス）
10	インターネットバンキングやクレジットカード情報の不正利用

～「2017年版 10大脅威 」
https://www.ipa.go.jp/security/vuln/10threats2017.html

メモ

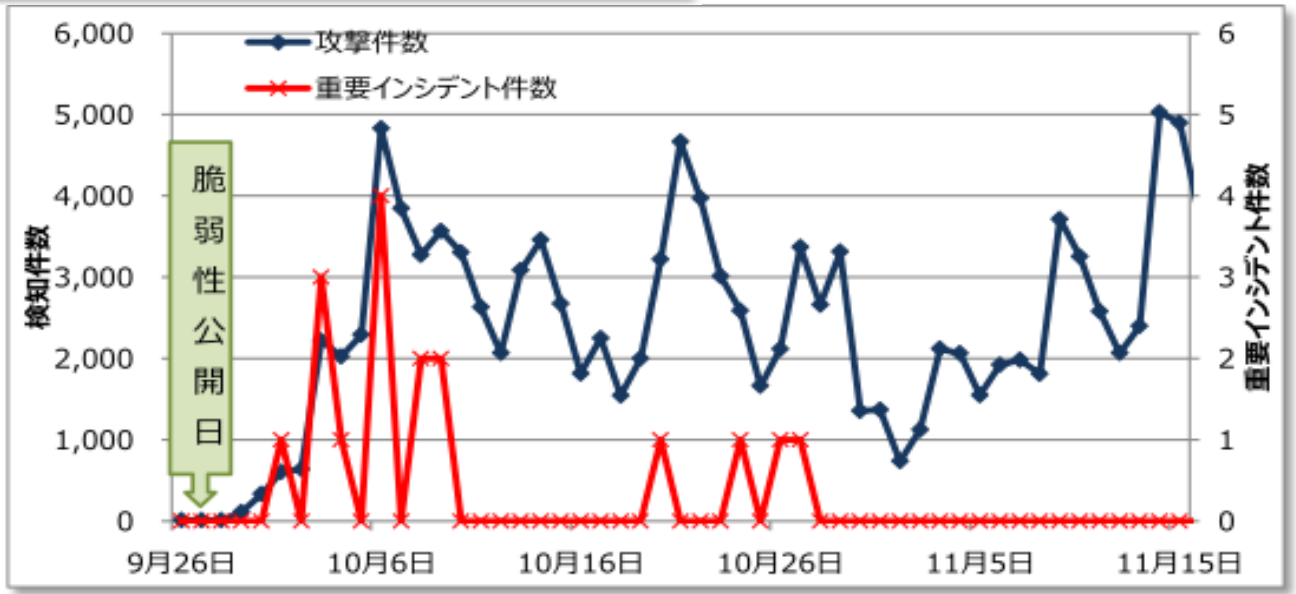
脆弱性を突く攻撃の傾向

脆弱性が公開されてからわずかな期間で攻撃が開始される。



OpenSSLにおける脆弱性を用いた攻撃件数推移
http://www.lac.co.jp/security/report/index.html

GNU bashにおける脆弱性を用いた攻撃件数推移
http://www.lac.co.jp/security/report/index.html



メモ

脆弱性を突く攻撃の例

» 2014年05月02日 09時17分 更新

XP狙いの攻撃を米国で観測：

IEの脆弱性を修正する緊急アップデート公開、XPにも「特例」で提供

米マイクロソフトは米国時間の2014年5月1日（日本時間5月2日）、Internet Explorer 6～11に存在する深刻な脆弱（ぜいじゃく）性を修正するセキュリティ更新プログラム（MS14-021）を緊急公開した。特例としてWindows XP向けも含まれている。

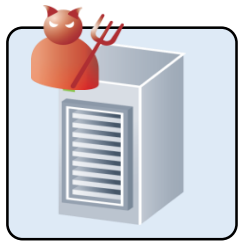
[高橋睦美，@IT]

米マイクロソフトは米国時間の2014年5月1日（日本時間5月2日）、Internet Explorer（IE）6～11に存在する深刻な脆弱（ぜいじゃく）性を修正するセキュリティ更新プログラム（MS14-021）を緊急公開し、Windows Updateなどを通じて配布を開始した。さらに「特例」として、4月9日（日本時間）でサポートが終了したWindows XPおよびIE 6用にもパッチを提供する。

パソコンの異常終了、マルウェア感染、不正な操作などの被害

悪意あるコンテンツ仕掛けたWebサイト

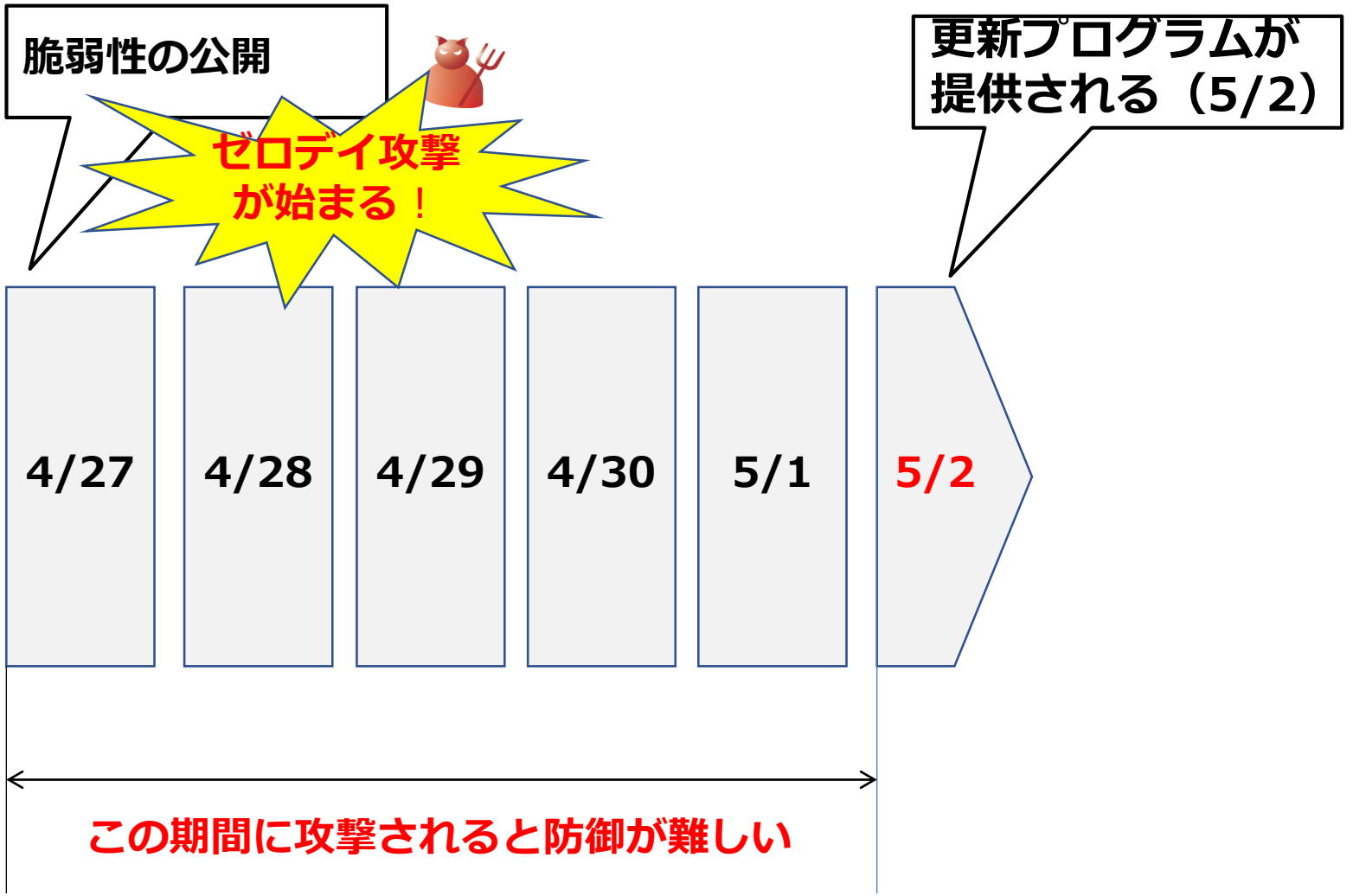
脆弱性があるIEでアクセス



パソコンの異常終了、ウイルス感染、不正な操作などの被害

メモ

ゼロデイ攻撃


脆弱性の公開
ゼロデイ攻撃
が始まる！
更新プログラムが
提供される（5/2）
4/27
4/28
4/29
4/30
5/1
5/2
この期間に攻撃されると防御が難しい

メモ

1-4. 情報セキュリティリスクの分析

メモ

リスクアセスメントの全体プロセス：リスク分析

メモ

「情報資産」とは？

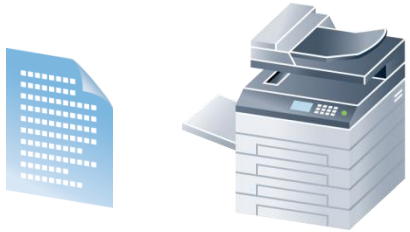
「情報資産」とは、情報セキュリティにおける保護の対象のこと。

「情報資産」はさまざまな形状をしており、その性質を理解し、適切に扱い、保護しなければなりません。

情報資産の例

電子媒体

印刷物



設備

パソコン

会話や電子メール

人

メモ

情報資産の評価の例

「情報資産」は、何が存在し、どの程度の価値を持つものかは、その組織によって異なる。

価値評価	金銭・機会損失（短期）	金銭・機会損失（中長期）	信用・ブランド損失
1.非常に小さい	当期経営にほとんど影響はない	中長期な経営には影響はない	ほとんど影響がない
2.小さい	当期経営に軽微な影響(当期利益の1%以下)を及ぼす	中長期な経営には影響はない	限定された人に対して影響が及ぶ
3.中程度	当期経営に影響(当期利益の3%以下)を及ぼす	中長期な経営にはほとんど影響はない	多くの人に対して影響が及ぶ
4.大きい	当期経営に重大な影響(当期利益の10%未満)を及ぼす	2年程度の経営には影響が及ぶ	限定された人に長期的な悪いイメージが残る
5.非常に大きい	当期経営に極めて重大な影響(当期利益の10%以上)を及ぼす	3年以上の経営には影響が及ぶ	多くの人に長期的な悪いイメージが残る

影響度の評価基準例～「情報セキュリティプロフェッショナル教科書」、JNSA教育部会

メモ

脅威・脆弱性の識別の例

脆弱性の分類	脆弱性の例	関連する脅威の例
環境、施設	ドア、窓などの物理的保護の 欠如	盗難
	不安定な電源設備	停電、誤作動
	災害を受けやすい立地条件	洪水、地震、災害
ハードウェア	温湿度変化に影響を受けやすい	故障、誤作動
	記憶媒体のメンテナンス不足	故障、情報漏洩
ソフトウェア	仕様書の不備	ソフトウェア障害、誤作動
	アクセスコントロールの欠如	なりすまし、改竄、情報漏洩
	不適切なパスワード	不正アクセス、改竄、情報漏洩
	監査証跡（ログ管理）の欠如	不正アクセス
	バックアップコピーの欠如	復旧不能
・・・・・・・・・・	・・・・・・・・・・	・・・・・・・・・・

メモ

リスク分析の例

リスク分析手法のバリエーション

- 定性的リスク分析（例：FTA – Fault Tree Analysis ）
- 定量的リスク分析（例：ALE – Annual Loss Expectancy ）
- ベースラインアプローチ
- 詳細リスク分析
- 組み合わせアプローチ など

定量的リスク分析手法の例

年次損失予測（ALE） = 単一損失予測（SLE） × 年次発生頻度（ARO）

リスクレベル算定ロジックの例

リスクの大きさ = 資産価値 × 脅威インパクト × 脆弱性の度合い

メモ

1-5. 情報セキュリティリスクの対応

メモ

リスクアセスメントの全体プロセス：リスク対応

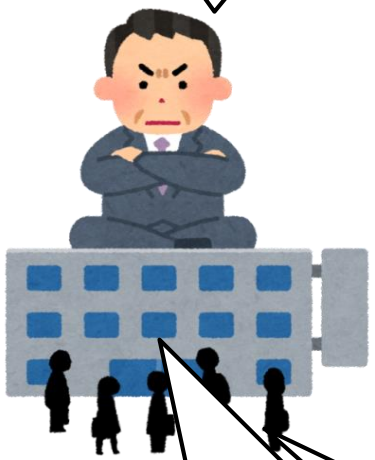
メモ

インシデントの被害や影響

問い合わせ窓口の設置と運用

原因と影響の調査

ネットワークやシステムの停止による業務効率の低下



代替サービス等の手配

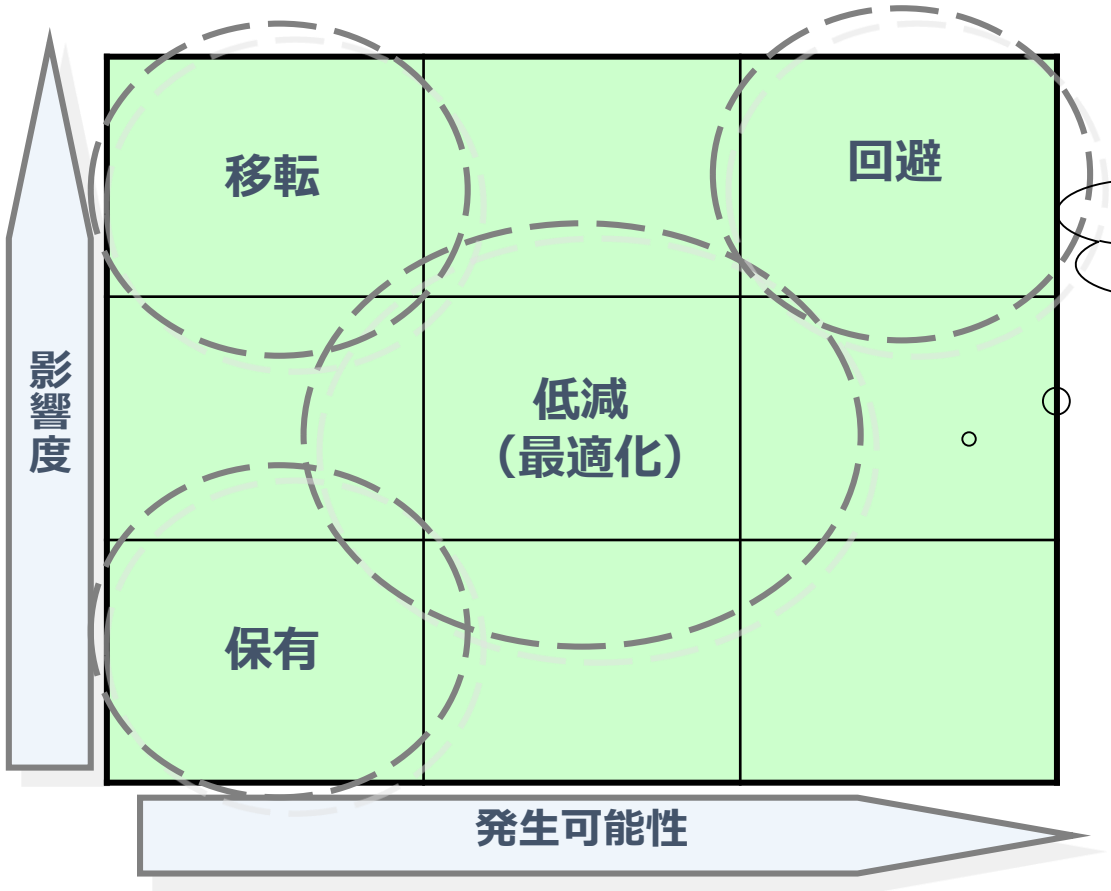
ブランド・イメージの低下

詐欺などによる2次被害

メモ

リスク評価・対応：リスクマトリックス

影響度や発生可能性を考慮して、「リスク対応」を選択する。
いくら「リスク対応」をしても、リスクは「0」にはならない。



「影響度」「発生可能性」の高いリスクの低減・移転・回避を実施

メモ

「リスク対応」と「リスク受容」

○リスク対応

・リスク回避： リスクの有る状況に巻き込まれないようにする意思決定、又はリスクのある状況から撤退する行為。

・リスク低減（リスク最適化）： リスクに関連して、好ましくない結果及びその発生確率最小化し、かつ、好ましい結果及びその発生確率を最大化するプロセス。（リスクに伴う発生確率もしくは好ましくない結果又はそれら両方を小さくするために取られる行為）

・リスク移転 ：リスクに関して、損失の負担又は利益の恩恵を他者と共有すること。（リスクに関して、損失の負担を他者と共有すること）

・リスク保有：あるリスクからの損失の負担又は利得の恩恵の受容

○リスク受容

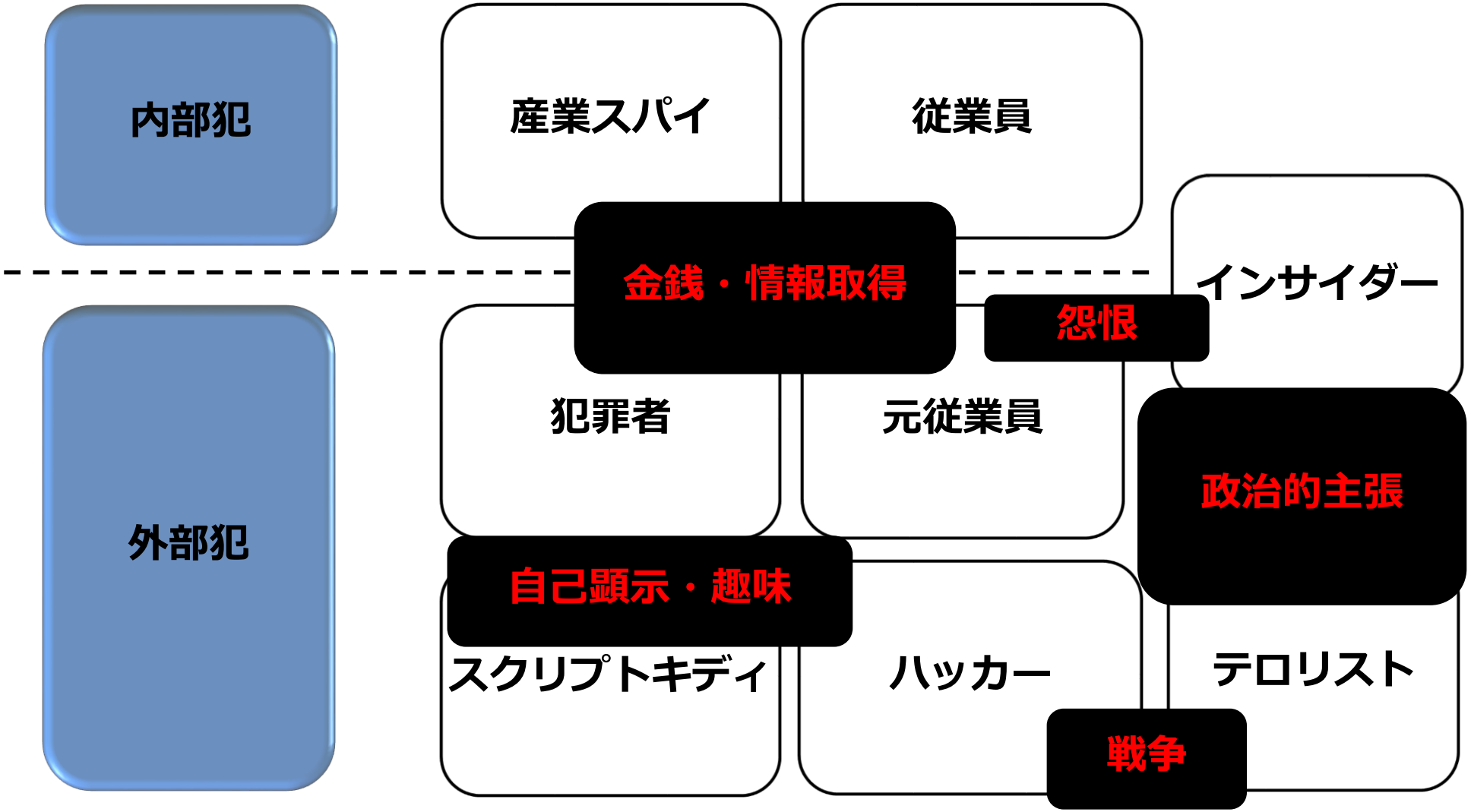
「リスク受容」とは、リスク対応で残ったリスクを受け入れること。

メモ

1-6. 攻撃者の種類

メモ

攻撃者の種類


内部犯
外部犯
産業スパイ
従業員
金銭・情報取得
インサイダー
怨恨
犯罪者
元従業員
政治的主張
自己顕示・趣味
スクリプトキディ
ハッカー
テロリスト
戦争

メモ

攻撃の「動機・機会・手段(MOM)」

IWASAKI GAKUEN

メモ

不正は、「動機」「機会」「手段」の3要素の結びつきにより発生する

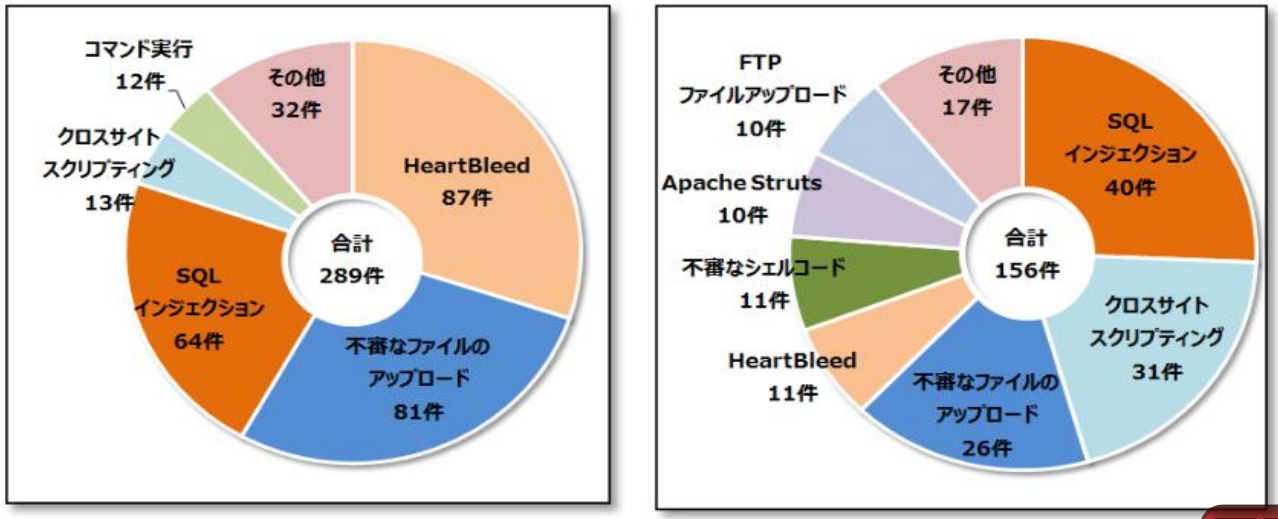
動機 Motive	**不正行為によって何らかの利益が得られる**
機会 Opportunity	**不正行為が可能な状態 タイミングが存在する状態**
手段 Means	**不正行為が可能な方法・手段が存在する状態**

この3要素の全て、もしくは一部をなくすことで、セキュリティ対策の効果が高まる

MO(Modus Operandi;手口)

不正を完遂するための手口であり、
不正時の経験から得られる行動パターンである。
一番効果的な手口を学ぶまで、その手口は変化する。

FBI Law Enforcement Bulletin　https://www.ncjrs.gov/pdffiles1/Digitization/134597NCJRS.pdf



a. 2015 年 7～9 月　　b. 2015 年 10～12 月

不正(攻撃)の手口は常に変化する

インターネットからの攻撃通信による重要インシデントの内訳

JSOC insight vol.11　http://www.lac.co.jp/security/report/2016/05/17_jsoc_01.html

メモ

1-7. 不正行為者の特徴

メモ

不正行為者のプロファイリング

　不正行為者には、ある程度の共通した行動特性がある。

　不正行為が行われた場合は、何らかの「前兆」や「痕跡」がある。

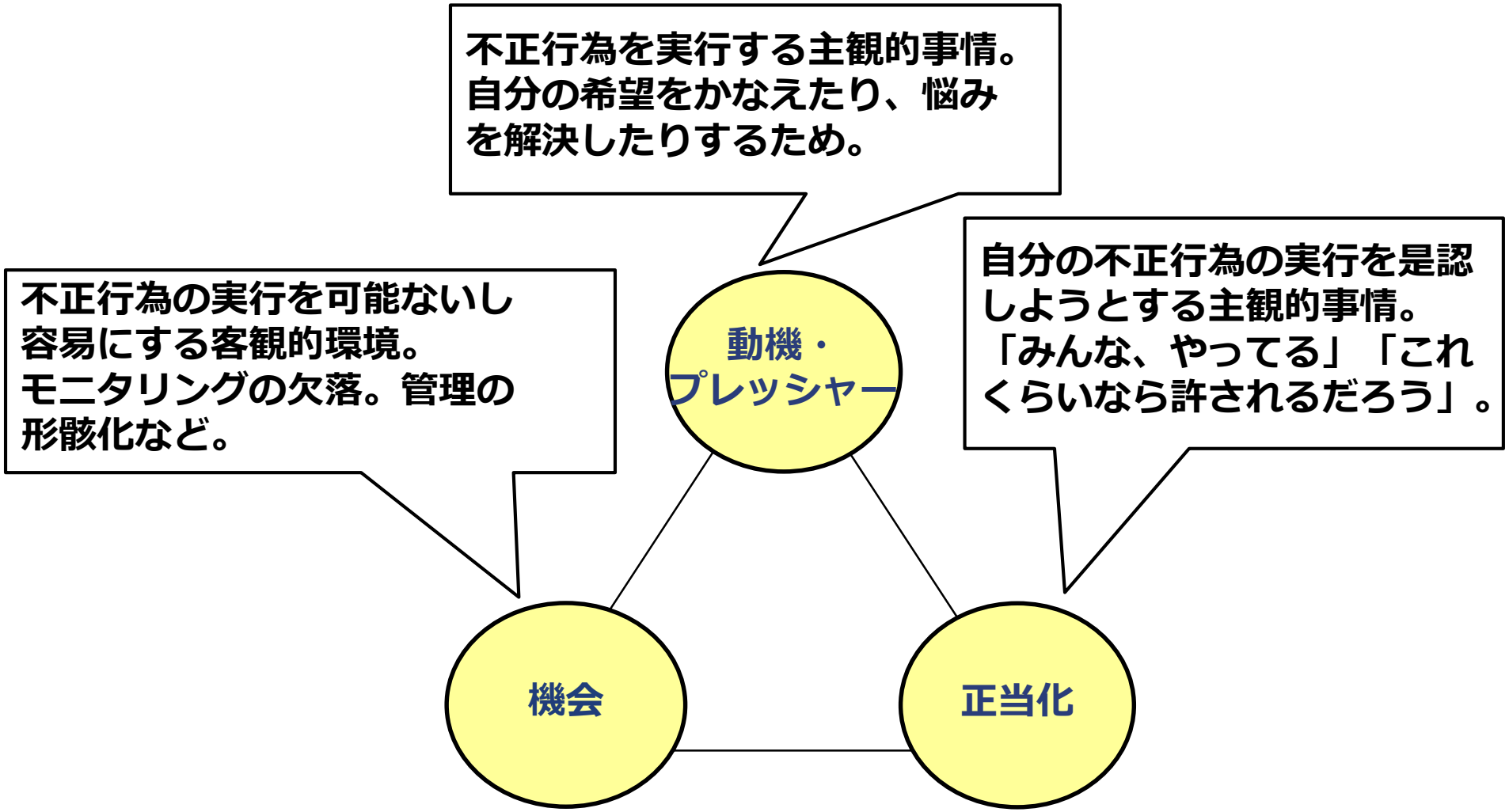
メモ

不正行為者の特徴

・今までに、所属組織や周囲にウソをついていた。（または、あまり話したがらない）
・経歴の詐称
・転職者の場合、以前の職場の退職理由の詐称
・不正を行う動機が存在する
・金銭的に困っている
・組織や内部の人間に、不満を持っている

メモ

「不正のトライアングル」



メモ

1-8. 攻撃者・不正行為者の目的

メモ

サイバー攻撃の主な目的

金銭

不満・怨み

諜報活動

メモ

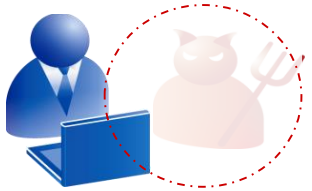
そして、攻撃が見えなくなる

金銭・諜報活動目的の攻撃

攻撃が見えづらくなる

攻撃者

不正アクセスやウイルスで、ひっそり、重要情報を盗むぞ。



攻撃に気づきにくくなる。

メモ

サイバー攻撃で狙われる情報

研究

調査

技術

「個人情報」だけが狙われているのではない。

メモ

1-9. 攻撃の全体的プロセス

メモ

サイバー攻撃の一般的プロセス

IWASAKI GAKUEN

1. 情報収集
   nslookupやwhoisコマンド、検索サービス等を使い攻撃対象のIPアドレスやネットワークレンジを調査
2. 偵察行為
   攻撃対象にポートスキャン等を行い稼動サービスや使用しているソフトウェア等を調査
3. 侵入・攻撃
   パスワードクラックや脆弱性の悪用により、侵入、攻撃(重要情報取得、コマンド実行)等を実施
4. 事後処理
   侵入の隠蔽(ログ改ざん)、踏み台として悪用、次回の侵入に使用する裏口の作成等を実施

メモ

侵入・攻撃

プロセスの全体像	情報収集	偵察行為	侵入・攻撃	事後処理

概要	ターゲットに攻撃を実行する	
攻撃の種類	侵入	使用不能攻撃
	権限昇格	破壊・汚染
攻撃元による分類	リモート攻撃	ネットワーク越しに攻撃を実行
	ローカル攻撃	ログイン状態から攻撃を実行
攻撃の様相による分類	能動的攻撃	攻撃者自らが、攻撃を仕掛ける
	受動的攻撃	罠を仕掛けて、攻撃対象が罠にかかるのを待つ

メモ

事後処理

プロセスの全体像

情報収集 → マッピング → 侵入・攻撃 → **事後処理**

概要	侵入に成功したホスト上で目的を達成するほか、次回以降の侵入に備えてコントロールを確実に掌握し、侵入の痕跡を消去する	
侵入後の行動パターンの例	データ奪取	目的のデータファイルや、アカウント情報が含まれるファイル（パスワードファイルなど）を奪取する
	データ改ざん	データファイル、ログデータ、プログラムファイル、システム設定やアカウントの追加・変更等を実施する
	バックドア設置	次回以降よりスムーズに侵入できるようにするための裏口（バックドア）を設置する
	不正中継	侵入したシステムを踏み台として別システムを攻略する

メモ

1-10. 攻撃のプロセスモデル

メモ

「サイバーキルチェーン」モデル

サイバー攻撃における攻撃者の一連の行動を、軍事行動に当てはめて示したモデル。

早期段階で攻撃を検知し、サイバーキルチェーンを断ち切ることで被害を防ぐことが可能となる。

メモ

「サイバーキルチェーン」の各段階

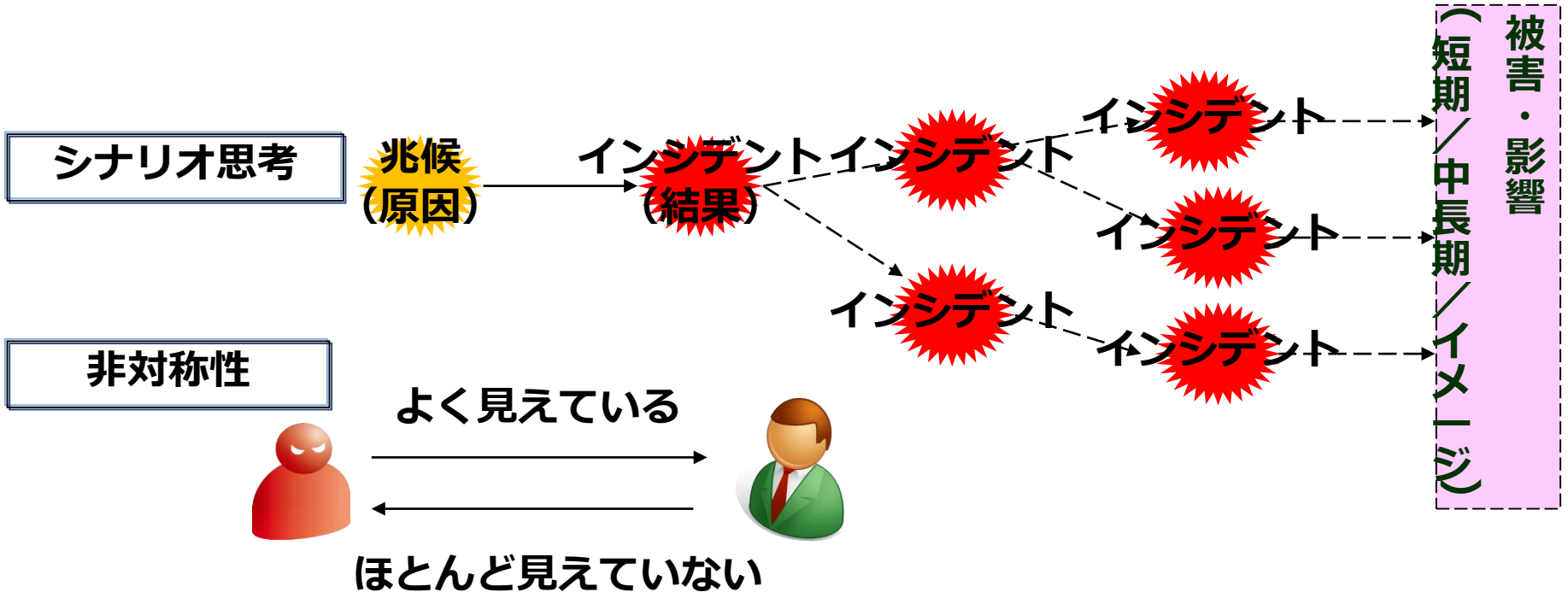
攻撃の段階	概　要
1.偵察	インターネットなどから組織や人物を調査し、対象組織に関する情報を取得する。
2.武器化	エクスプロイトやマルウェアを作成する。
3.デリバリ	なりすましメール（マルウェアを添付）を送付する。 なりすましメール（マルウェア設置サイトに誘導）を送付し、ユーザにクリックするように誘導する。
4.エクスプロイト	ユーザにマルウェア添付ファイルを実行させる。 ユーザをマルウェア設置サイトに誘導し、脆弱性を使用したエクスプロイトコードを実行させる。
5.インストール	エクスプロイトの成功により、標的がマルウェアに感染する。
6.C&C	マルウェアとC&Cサーバを通信させて、感染PCを遠隔操作する。新たなマルウェアやツールのダウンロードにより、感染拡大や内部情報の探索を試みる
7.目的の実行	探し出した内部情報を、加工（圧縮や暗号化等）した後、情報を持ち出す

メモ

攻撃者や攻撃をより理解するために

「敵」を知る。「敵の手口」を知る。そして、「脅威」や「インシデント」の連鎖関係を知ることが、セキュリティ対策をする上で重要となる。

・シナリオ思考（多くの不確実性要素のある中でも、予測し、対応する能力）
・非対称性（不正／攻撃をする側との見え方の違い）への適応



メモ