IPA Better Life with IT

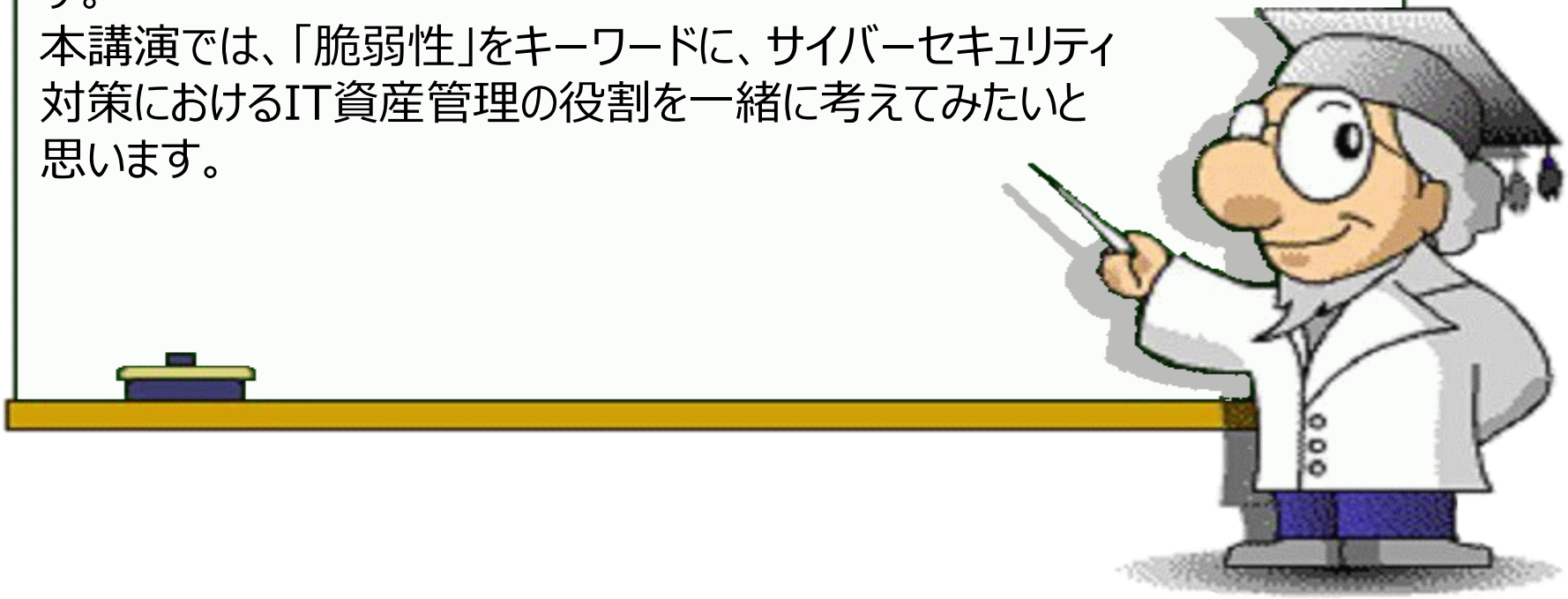
IT資産管理と サイバーセキュリティ対策

2018/10/04

独立行政法人 情報処理推進機構 (IPA)
技術本部セキュリティセンター
情報セキュリティ技術ラボラトリー
寺田真敏

目次

サイバー攻撃に対するセキュリティ施策において、脆弱性などを含む、サイバーセキュリティリスクの把握は、重要な課題のひとつとなっています。
(独)情報処理推進機構(IPA)では、脆弱性関連情報を配布するためのJVN脆弱性対策基盤、効果的な施策を実施するためのセキュリティリスク分析など、各種サイバーセキュリティ対策のための取組を推進しています。
本講演では、「脆弱性」をキーワードに、サイバーセキュリティ対策におけるIT資産管理の役割を一緒に考えてみたいと思います。



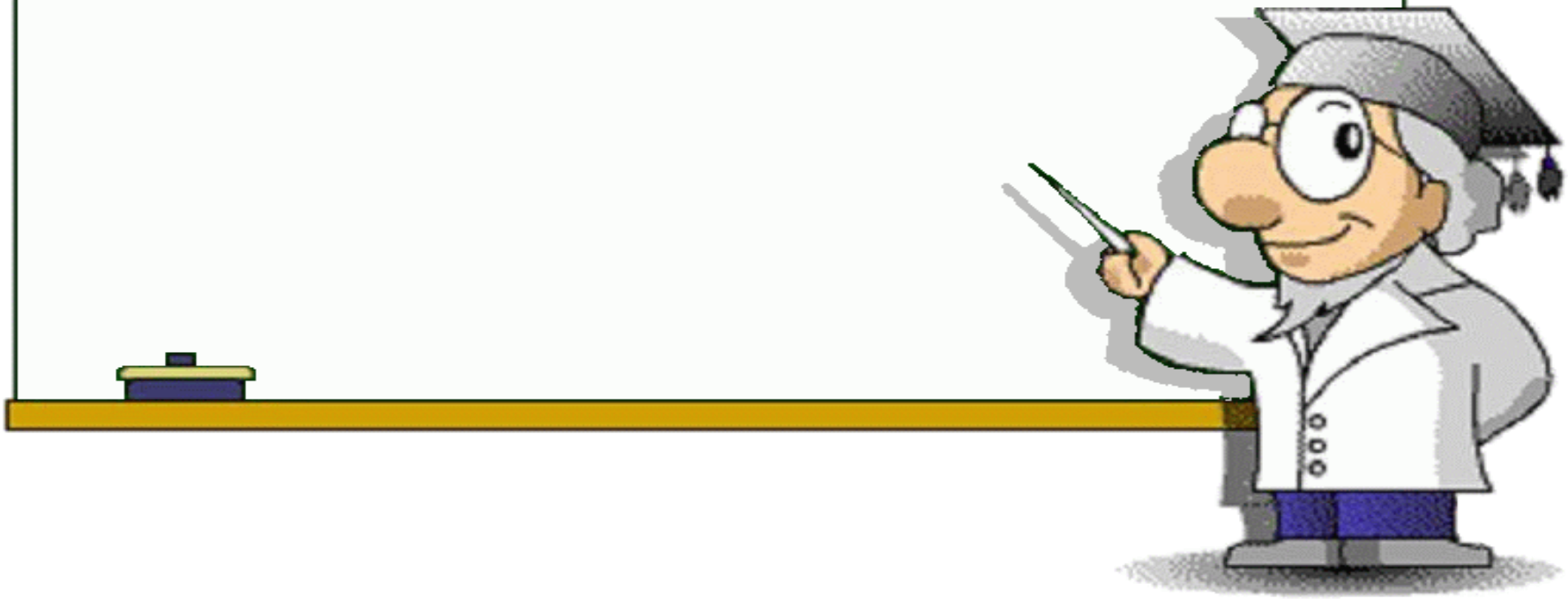
情報セキュリティ10大脅威 2018

- 2017年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から選出

昨年	個人	順位	組織	昨年
1位	インターネットバンキングやクレジットカード情報等の不正利用	1位	標的型攻撃による被害	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	2位
7位	ネット上の誹謗・中傷	3位	ビジネスメール詐欺による被害	ランク外
3位	スマートフォンやスマートフォンアプリを狙った攻撃	4位	脆弱性対策情報の公開に伴う悪用増加	ランク外
4位	ウェブサービスへの不正ログイン	5位	脅威に対応するためのセキュリティ人材の不足	ランク外
6位	ウェブサービスからの個人情報の窃取	6位	ウェブサービスからの個人情報の窃取	3位
8位	情報モラル欠如に伴う犯罪の低年齢化	7位	IoT機器の脆弱性の顕在化	8位
5位	ワンクリック請求等の不当請求	8位	内部不正による情報漏えい	5位
10位	IoT機器の不適切な管理	9位	サービス妨害攻撃によるサービスの停止	4位
ランク外	偽警告によるインターネット詐欺	10位	犯罪のビジネス化(アンダーグラウンドサービス)	9位
	インターネット上のサービスを悪用した攻撃(10)	ランク外へ	ウェブサイトの改ざん(6) ウェブサービスへの不正ログイン(7) 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(10)	

目次

- 脆弱性とは
- 脆弱性対策　～情報収集に役立つキーワード～
- 変化点：IT管理からリスク/危機管理へ
- サイバーセキュリティ対策におけるリスク分析実施のススメ



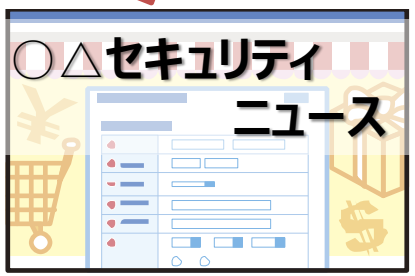
最近、
脆弱性という言葉を耳にしませんか？

Struts2の脆弱性突く不正アクセス、4年前にもStruts2で被害(2017)

WordPressの脆弱性突く攻撃が激増、
6万以上のWebサイトで改ざん被害(2017)

CPUの脆弱性対策 半数以上で実施(2018)

新聞から

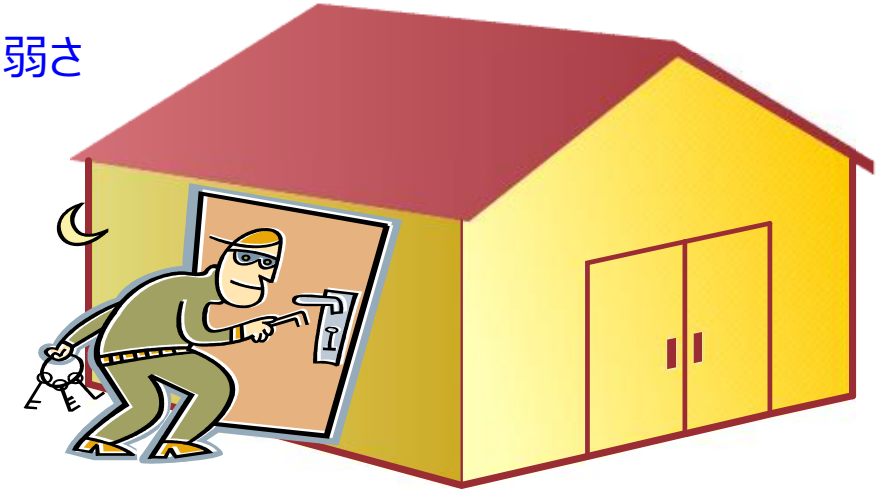


ウェブニュースから

脆弱性とは・・・

ウイルス対策と脆弱性対策は、同じではありません。
なぜなら、脆弱性は、鍵穴の劣化、鍵そのものの”弱さ”だからです。これは、鍵が付いていない、鍵をかけていないのと同じことです。

【脆弱性】
鍵穴の劣化、鍵そのものの弱さ

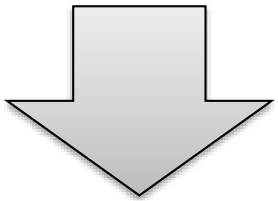


【ウイルス対策】
警備員

いくら、警備員を配置(ウイルス対策ソフトを導入)しても、警備員がよそ見するなどの隙(攻撃者は検知されないテクニックを駆使)を利用すれば、脆弱性を利用して侵入できてしまいます。

脆弱性とは・・・

- 脆弱性の定義
  脆弱性とは、ソフトウエア製品やウェブアプリケーション等において、コンピュータ不正アクセスやコンピュータウイルス等の攻撃により、その機能や性能を損なう原因となり得るセキュリティ上の問題箇所
  (出典：情報セキュリティ早期警戒パートナーシップガイドライン)

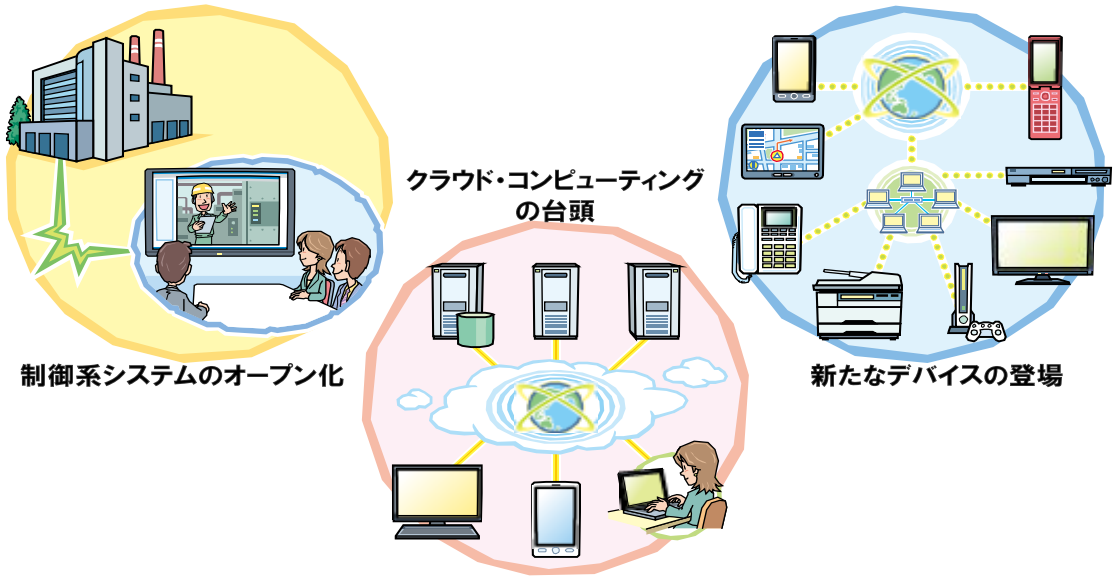


言い換えれば

- 攻撃によりシステムが攻略される可能性
- セキュリティ被害をもたらす危険要素
- 攻撃を受ければ被害、受けなければ無害

脆弱性を取り巻く環境の変化
～様々な分野に広がっていく脆弱性～

- デバイスのスマート化、制御系のオープン化により、新たな分野で、新たな脆弱性が発見され続けている。



- 情報システム脅威：情報窃取、破壊、妨害
- メディカルデバイスの脅威：身体への影響懸念
- 制御系システムの脅威：社会インフラへの影響

脆弱性を取り巻く環境の変化
～海外では脆弱性売買が行われている～

- 脆弱性発見者に報奨金を支払う制度が一般化

- 大手製品ベンダ、大手ウェブサービスベンダなどが採用
- 脆弱性種別によっては、最大10万$の報奨金
- 脆弱性発見を専門とする企業出現(ビジネス化)
- 報奨金を競うコンテストも開かれて

脆弱性を取り巻く環境の変化
～振り返り 2014年～

- 2014年4月
  OpenSSLの情報漏えいを許してしまう脆弱性 ～ Heartbleed問題 ～
- 2014年4月
  Apache Strutsの任意のコード実行を許してしまう脆弱性
- 2014年9月
  GNU bashの脆弱性 ～ shellshock問題 ～
- 2014年10月
  SSL通信の暗号文の解読を許してしまう脆弱性 ～ POODLE問題 ～

脆弱性対策には、システム、資産、データ、機能に対するサイバーセキュリティリスクの管理(リソース把握・管理)が必要であることが再認識された。

脆弱性を取り巻く環境の変化
～振り返り 2017年～

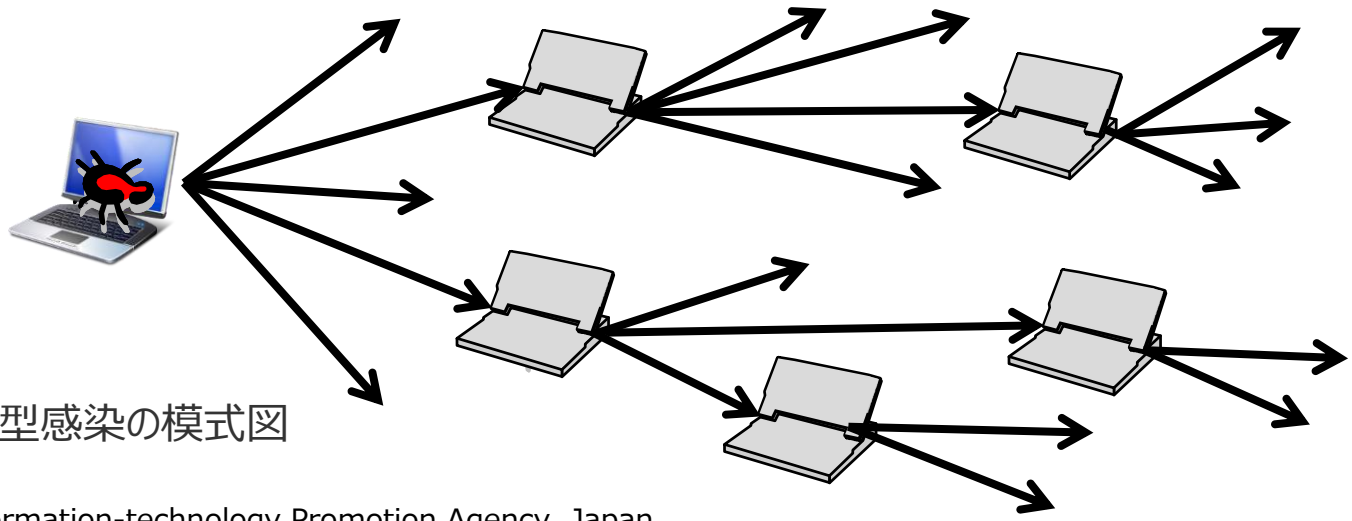
- 2017年3月
  Apache Struts 2の任意のコード実行を許してしまう脆弱性
- 2017年5月
  ランサムウェアWannaCryの流布
  2017年3月にセキュリティ更新プログラムがリリースされた
  「MS17-010：Windows SMBv1の任意のコード実行を許してしまう脆弱性」を悪用

脆弱性対策には、システム、資産、データ、機能に対するサイバーセキュリティリスクの管理(リソース把握・管理)が必要であることが再認識された。

脆弱性を取り巻く環境の変化
～ランサムウェアWannaCryの流布～

- 世界的な不正プログラムの感染被害

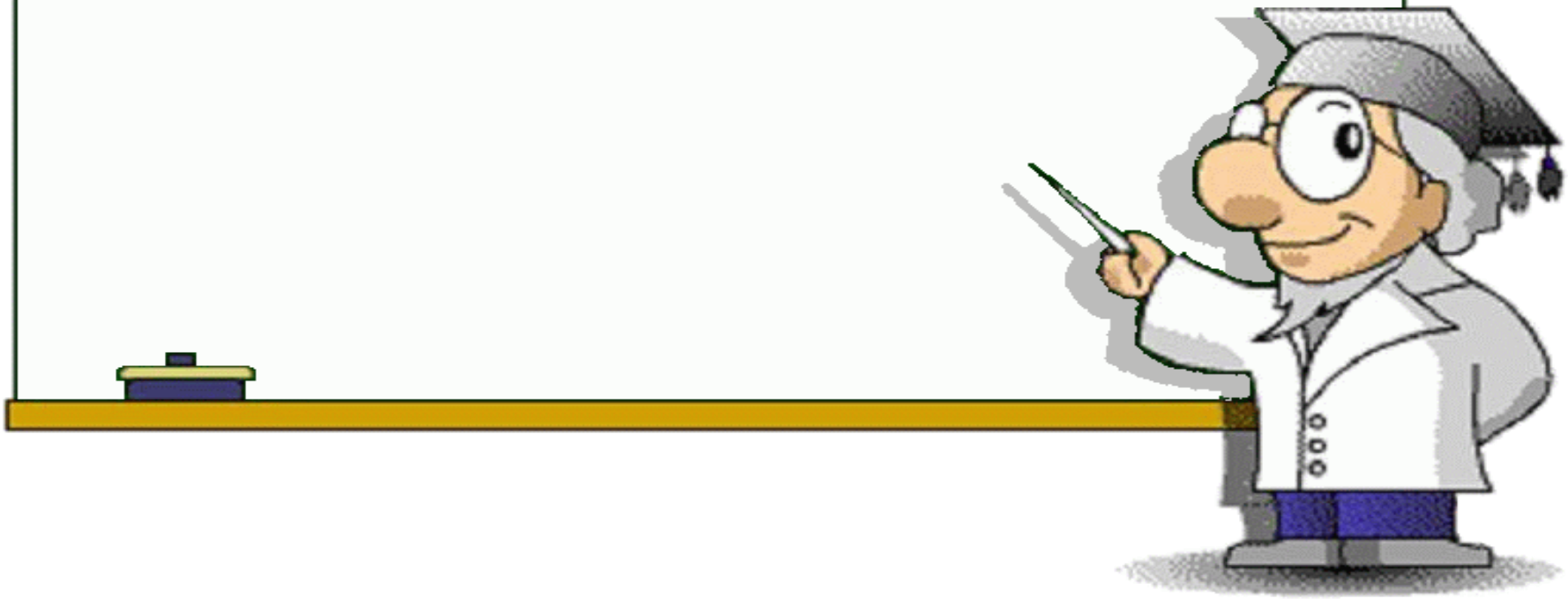
	約15年前(2000-2003)	現在(2017)
種類	W32/CodeRed I/II(2001年7月) W32/Nimda(2001年9月) W32/SQLSlammer(2003年1月) W32/MSBlaster(2003年8月)	WannaCry(2017年5月)
機能	自己増殖型感染(ネットワーク型ワーム)	自己増殖型感染(ネットワーク型ワーム) ランサムによるファイル暗号化



自己増殖型感染の模式図

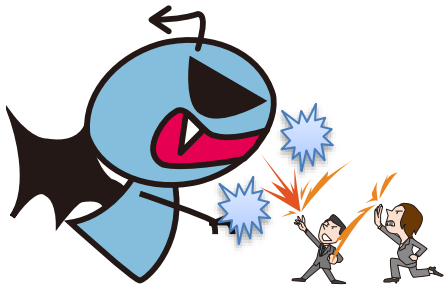
目次

- 脆弱性とは
- **脆弱性対策　～情報収集に役立つキーワード～**
- 変化点：IT管理からリスク/危機管理へ
- サイバーセキュリティ対策におけるリスク分析実施のススメ



脆弱性対策

- 脆弱性を放置すると自組織に重大な被害が発生する危険性は大きくなる。



「彼を知り己を知れば百戦殆うからず」

脆弱性(彼)と対策のための関連情報を知っておくことが
適切な対応につながる。

脆弱性対策

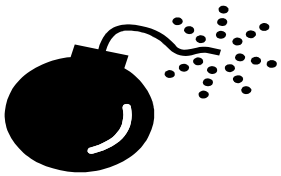
情報収集に役立つ
キーワードについて知ろう

脆弱性関連情報の収集
～脆弱性と攻撃の関係～

- 脆弱性を構成する要素(脆弱性関連情報)

＜攻撃方法＞
脆弱性を悪用するプログラムや
それらの使い方

＜脆弱性情報＞
脆弱性の性質及び特徴を示す情報



攻撃コード
(Exploit)

脆弱性を攻撃する

＜検証方法＞
脆弱性が存在することを
調べるための方法

脆弱性を含んだ
ソフトウエア

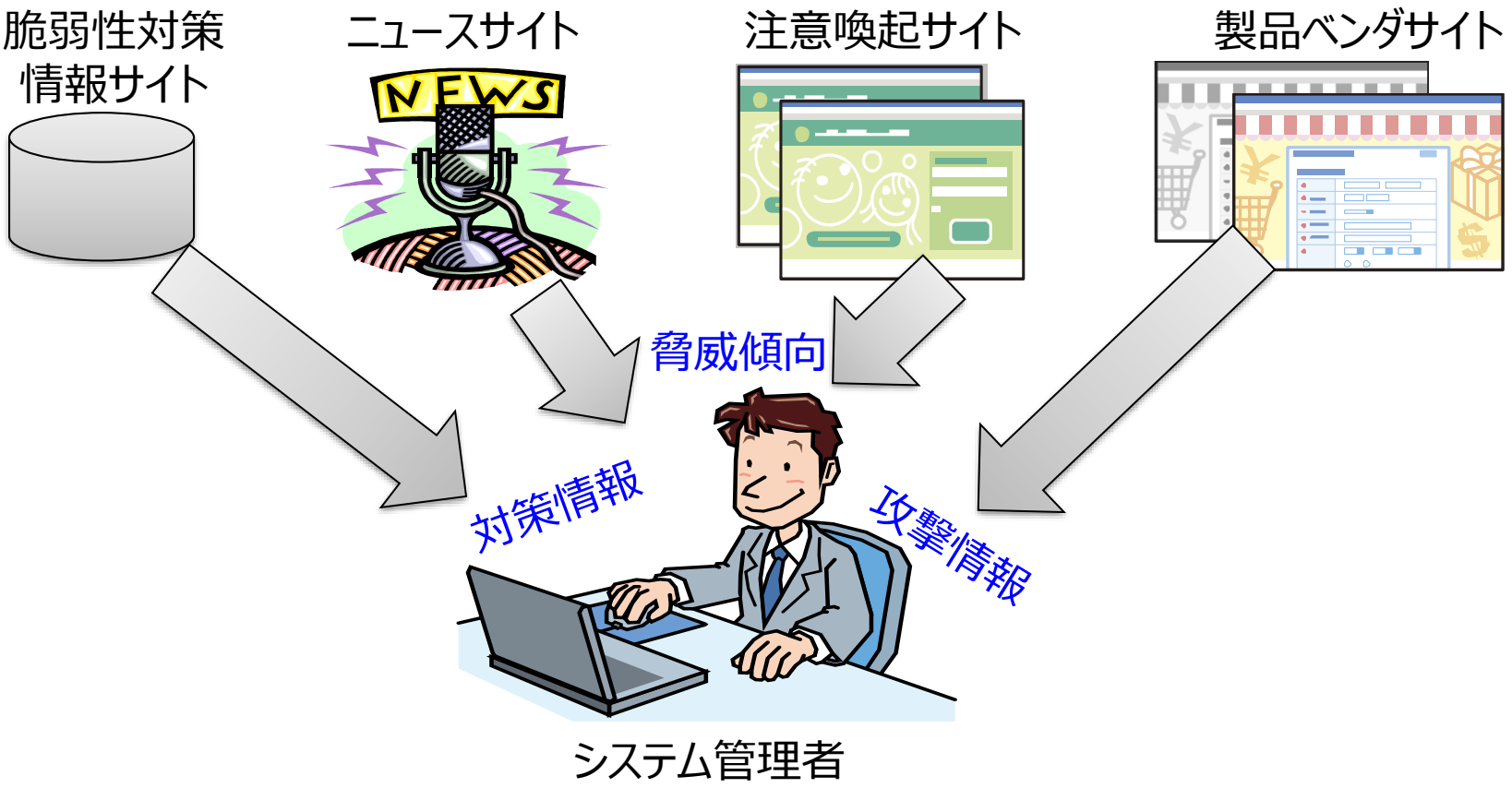
脆弱性を除去する

対策情報/プログラム

＜対策方法＞
脆弱性から生じる問題を
回避するまたは解決を図る方法

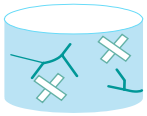
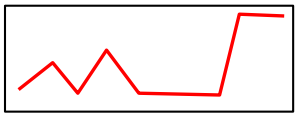
脆弱性関連情報の収集
～外部の情報を収集し、自組織の対策に役立てる～

- 脆弱性関連情報の収集とは?
  脆弱性対策の判断要素となる情報を収集すること



脆弱性関連情報の収集
～対策判断の為に、どのような情報を掴めば良いのか？～

- 情報種別と対策の考え方
  迅速に対策を実施する為に判断材料となる情報を収集

対象情報	情報の意味合い	活用例
脆弱性対策情報 	被害を受けるポテンシャル	●脆弱性の深刻度の調査 ●当該製品の脆弱性対策
攻撃情報 	実施・発生している事象	●自組織の対策状況のチェック ●攻撃有無のチェック
脅威傾向 	攻撃者の狙い・傾向	●中期的なセキュリティ対策の立案

脆弱性関連情報の収集
～効率的に進める為に有効なキーワード～

- 脆弱性対策情報、注意喚起、ニュース記事等でも使用されているキーワード

・・・脆弱性を一意に識別する番号

・・・脆弱性の影響度を評価する指標

CVE
～脆弱性を一意に識別する番号～

- **Common Vulnerabilities and Exposures**
  共通脆弱性識別子
  プログラム上のセキュリティ問題に一意の番号(CVE識別番号)を付与して管理する仕組み

CVE識別番号の構成

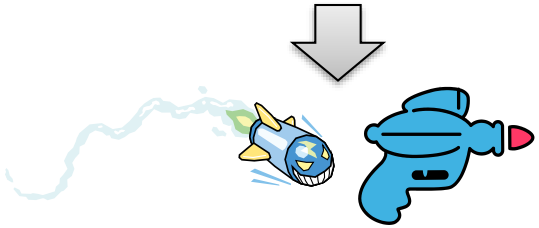
西暦　連番

CVE-2014-1000
CVE-2014-10000
CVE-2014-100000
CVE-2014-1000000

CVSS
～脆弱性の影響度を評価する指標～

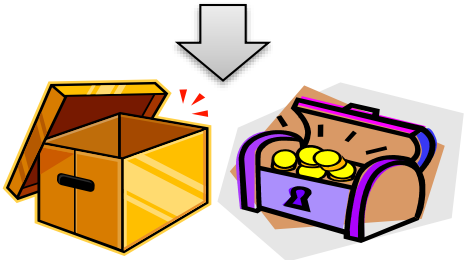
- **Common Vulnerability Scoring System**
  共通脆弱性評価システム
  攻撃状況やシステムの重要度を加味して脆弱性の深刻度を表す仕組み

＝ 「技術的な特性」 × 「脅威の大きさ」 × 「情報資産の価値」
＝ 「基本評価基準」 × 「現状評価基準」 × 「環境評価基準」



何が引き起こされるのか?

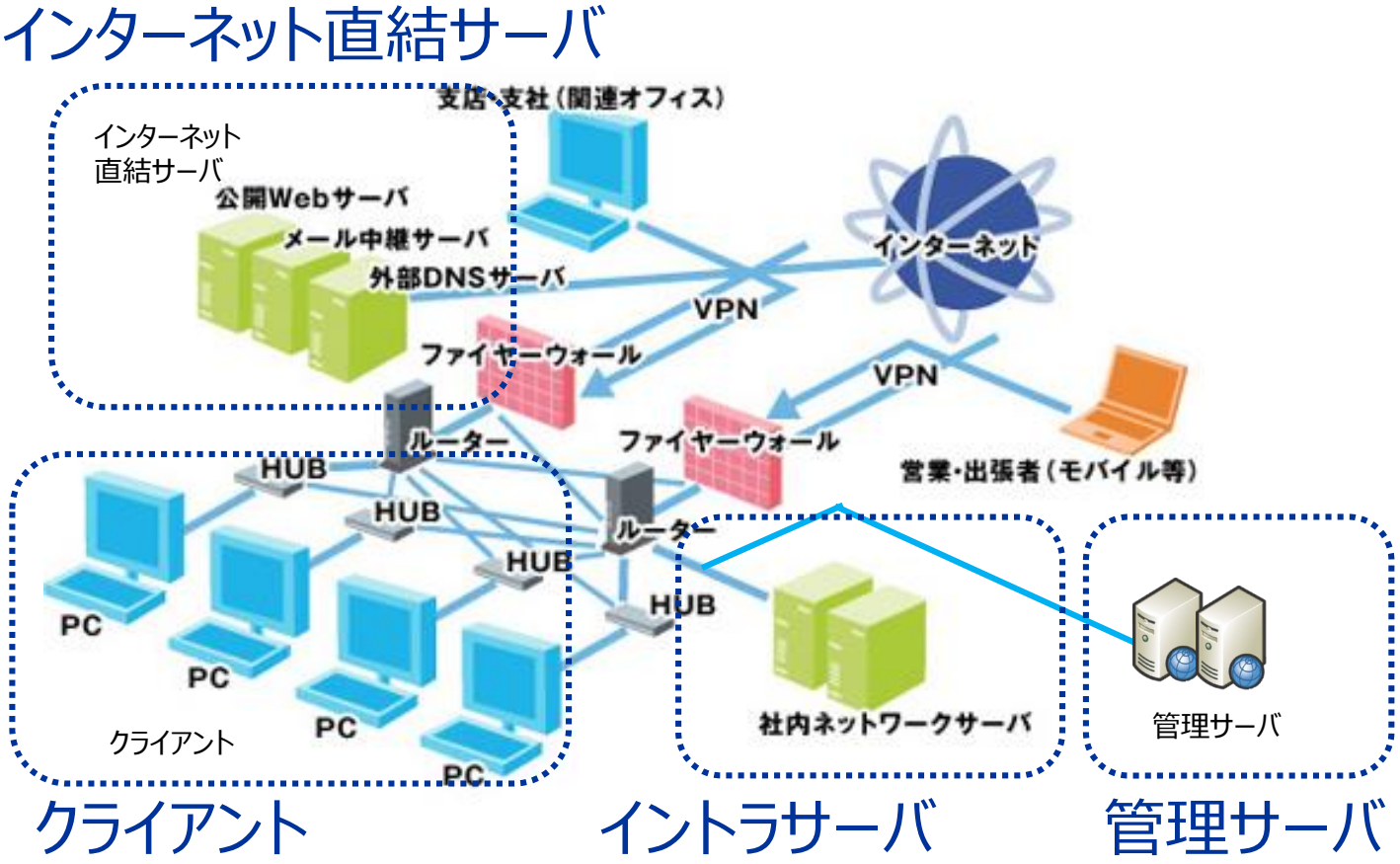
既に攻撃されている?
対策パッチは出ている?



システムの重要度は?

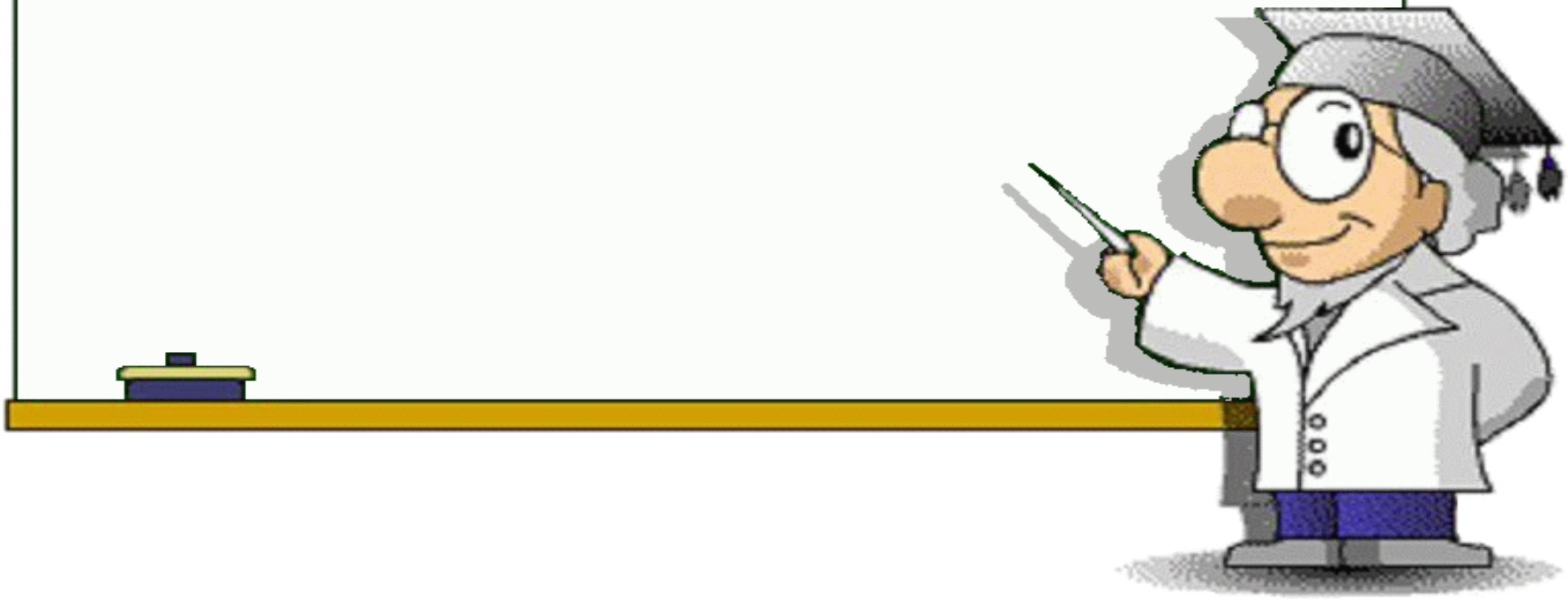
脆弱性関連情報の収集
～効率的に進める為に有効なキーワード～

- リソース把握・管理ができていないと、「効率的に進める為に有効なキーワード」の効果も半減してしまう。



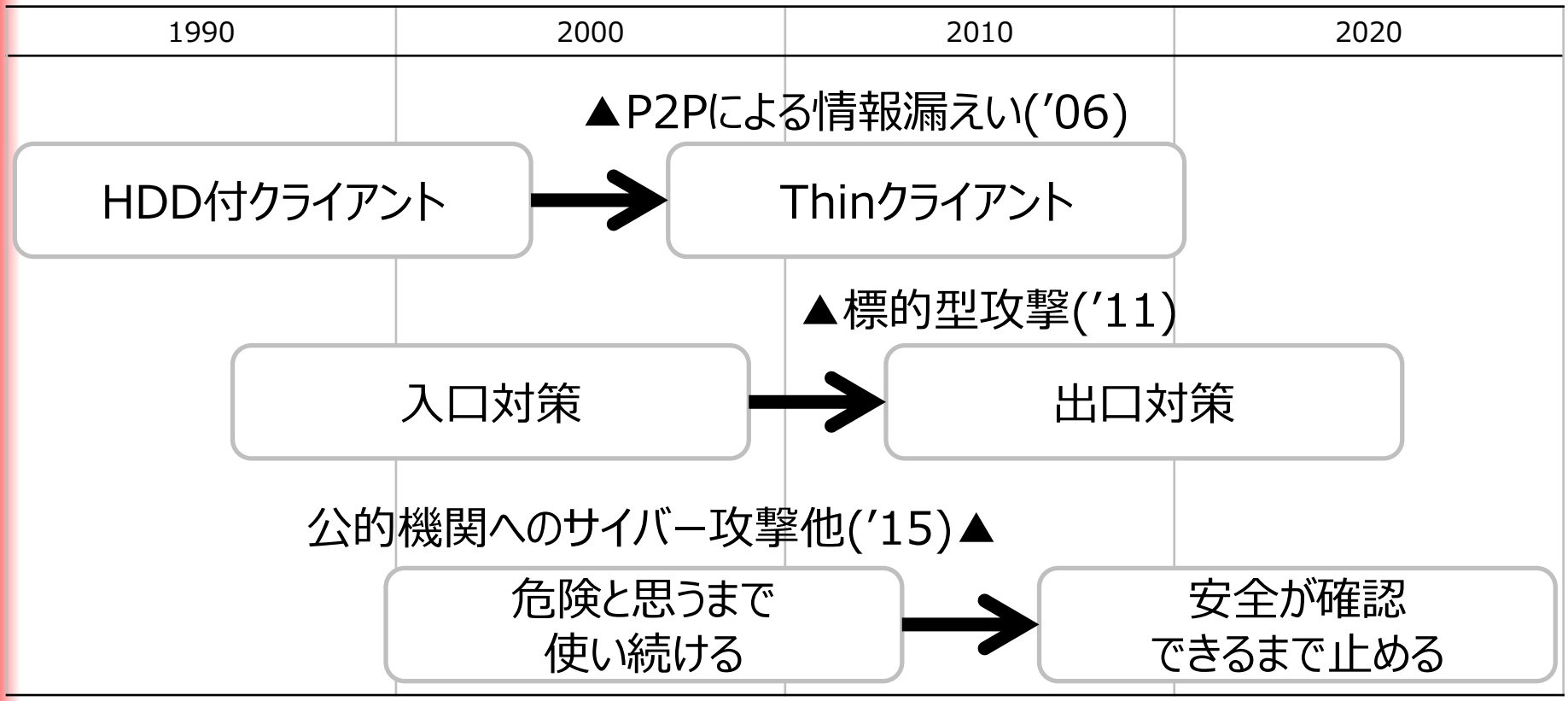
目次

- 脆弱性とは
- 脆弱性対策　～情報収集に役立つキーワード～
- **変化点：IT管理からリスク/危機管理へ**
- サイバーセキュリティ対策におけるリスク分析実施のススメ



「安全が確認できるまで止める」という考え方

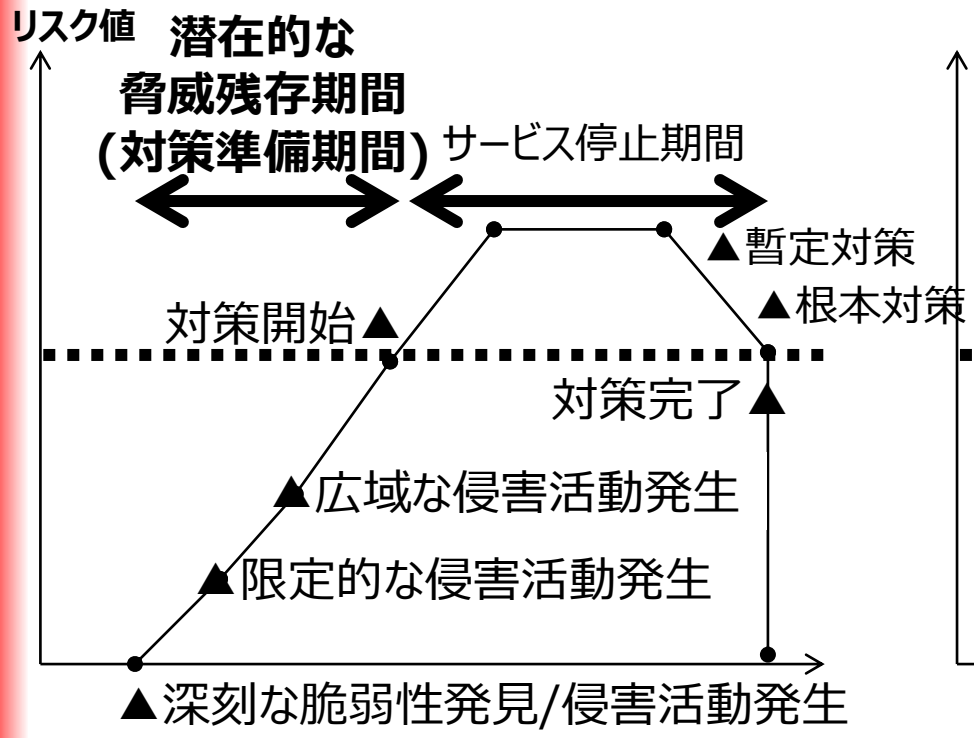
- 影響の大きなインシデントが発生すると対策アプローチに大きな変化が見られる



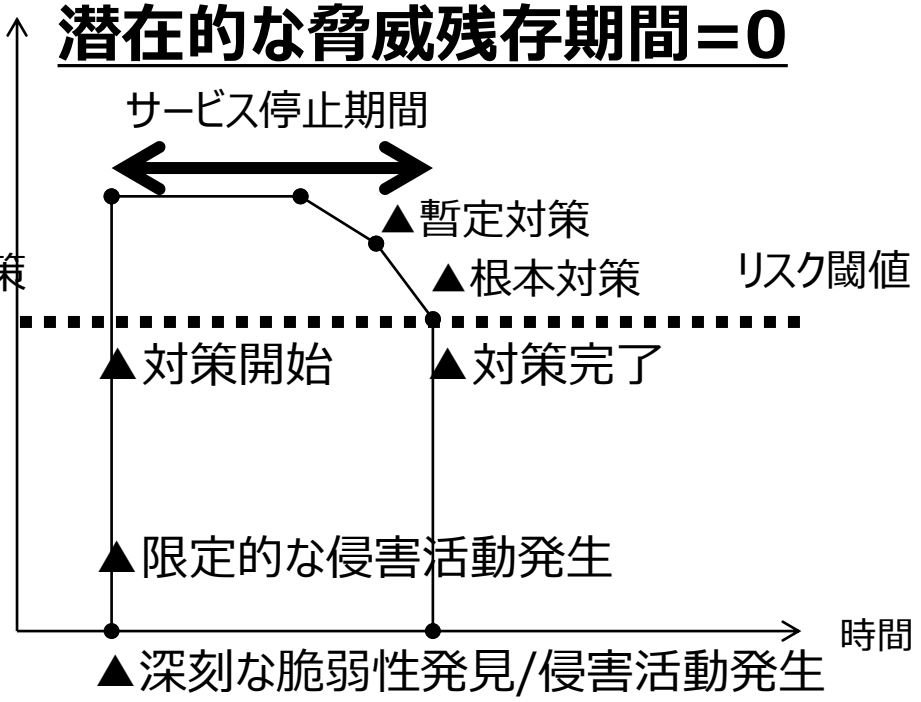
「安全が確認できるまで止める」という考え方

- 影響の大きなインシデントが発生すると対策アプローチに大きな変化が見られる

危険と思うまで使い続ける

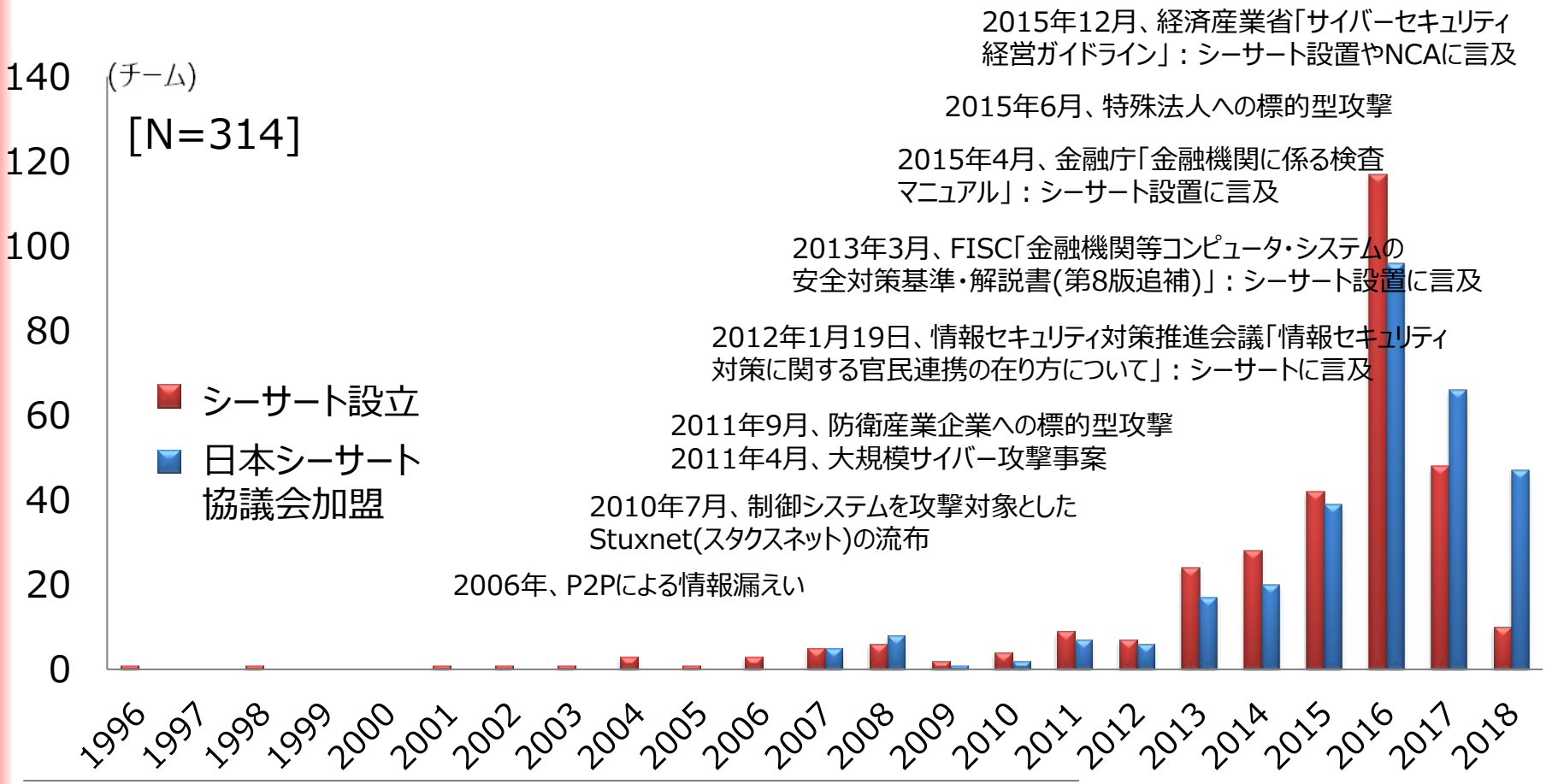


安全が確認できるまで止める



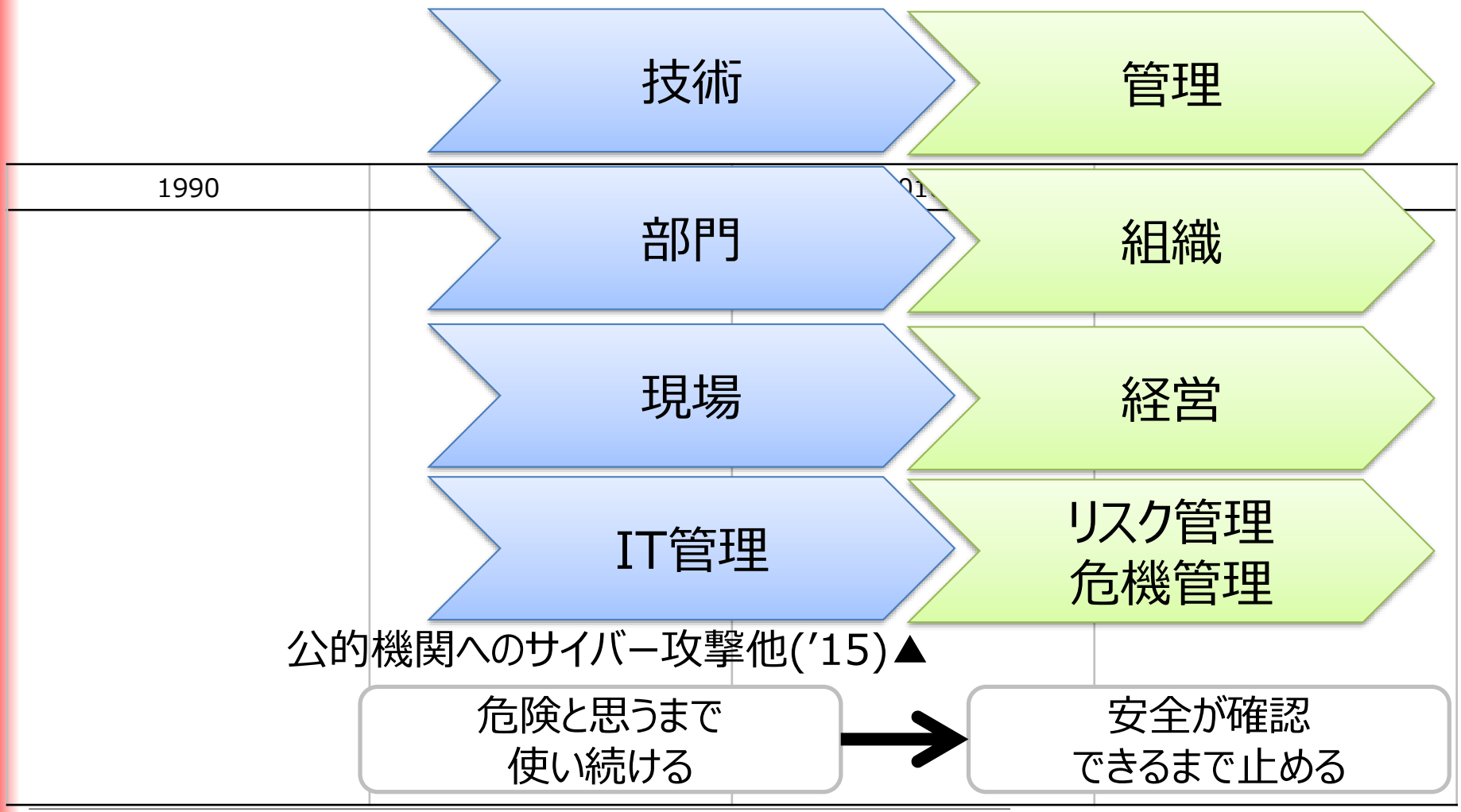
「安全が確認できるまで止める」という考え方

- 2013年以降、シーサート設立と加盟が急速に進んでいる。



[URL] 日本シーサート協議会加盟組織一覧について
http://www.nca.gr.jp/member/index.html

サイバー攻撃対応における考え方の変化
～IT管理からリスク/危機管理へ～



[URL]　組織管理者のための見えないサイバー攻撃リスクへの心構え
https://digitalforensic.jp/wp-content/uploads/2018/03/community2017-03kamata.pdf

サイバーセキュリティマネジメント
～サイバーセキュリティフレームワーク～

- 2014年2月、米国立標準技術研究所(NIST)から公開
- サイバーセキュリティ対策を「特定」、「防御」、「検知」、「対応」、「復旧」の5つの機能に分類

機能	概要
特定	システム、資産、データ、機能に対するサイバーセキュリティリスクの管理に必要な理解を深める。
防御	重要インフラサービスの提供を確実にするための適切な保護対策を検討し、実施する。
検知	サイバーセキュリティイベントの発生を検知するための適切な対策を検討し、実施する。
対応	検知されたサイバーセキュリティイベントに対処するための適切な対策を検討し、実施する。
復旧	レジリエンスを実現するための計画を策定・維持し、サイバーセキュリティイベントによって阻害されたあらゆる機能やサービスを復旧するための適切な対策を検討し、実施する。

[URL]　重要インフラのサイバーセキュリティを向上させるためのフレームワーク
https://www.ipa.go.jp/security/publications/nist/

サイバーセキュリティマネジメント
～サイバーセキュリティフレームワーク～

- 2014年2月、米国立標準技術研究所(NIST)から公開
- サイバーセキュリティ対策を「特定」、「防御」、「検知」、「対応」、「復旧」の5つの機能に分類

機能	カテゴリー	概要
特定	資産管理	組織が事業目的を達成することを可能にするデータ、職員、デバイス、システム、施設を特定し、事業目標と自組織のリスク戦略との相対的重要性に応じて管理している。
	ビジネス環境	自組織のミッション、目標、利害関係者、活動を理解し、優先順位付けを行っている; この情報はサイバーセキュリティ上の役割、責任、リスク管理上の意思決定を伝達するために使用される。
	ガバナンス	自組織に対する規制、法律、リスクと、自組織の環境、運用上の要求事項を管理しモニタリングするためのポリシー、手順、プロセスを理解しており、サイバーセキュリティリスクの管理者に伝達している。
	リスクアセスメント	企業は自組織の業務(ミッション、機能、イメージ、評判を含む)、自組織の資産、個人に対するサイバーセキュリティリスクを把握している。
	リスク管理戦略	自組織の優先順位、制約、リスク許容度、想定を定め、運用リスクの判断に利用している。

サイバーセキュリティマネジメント
～サイバーセキュリティ経営ガイドライン～

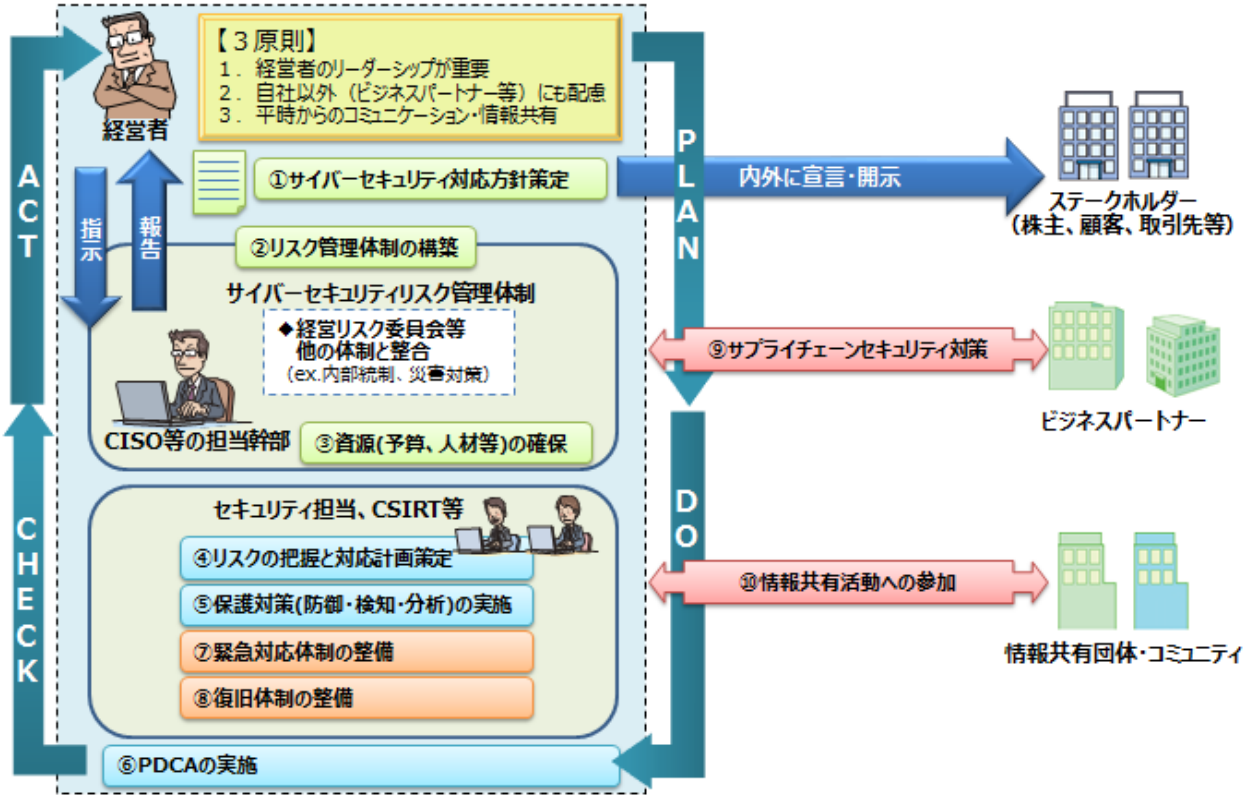
IPA

- 2015年12月、経済産業省から公開、企業の経営者を対象としたサイバーセキュリティ対策を推進するためのガイド
  - 経営者が認識する必要のある「3原則」、経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部(CISO等)に指示すべき「重要10項目」を記載
  - 3原則
    1. 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
    2. 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要
    3. 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

[URL] サイバーセキュリティ経営ガイドライン
http://www.meti.go.jp/policy/netsecurity/mng_guide.html

サイバーセキュリティマネジメント
～サイバーセキュリティ経営ガイドライン～

- 2015年12月、経済産業省から公開、企業の経営者を対象としたサイバーセキュリティ対策を推進するためのガイド
  - 重要10項目



サイバーセキュリティマネジメント
～サイバーセキュリティ経営ガイドライン～

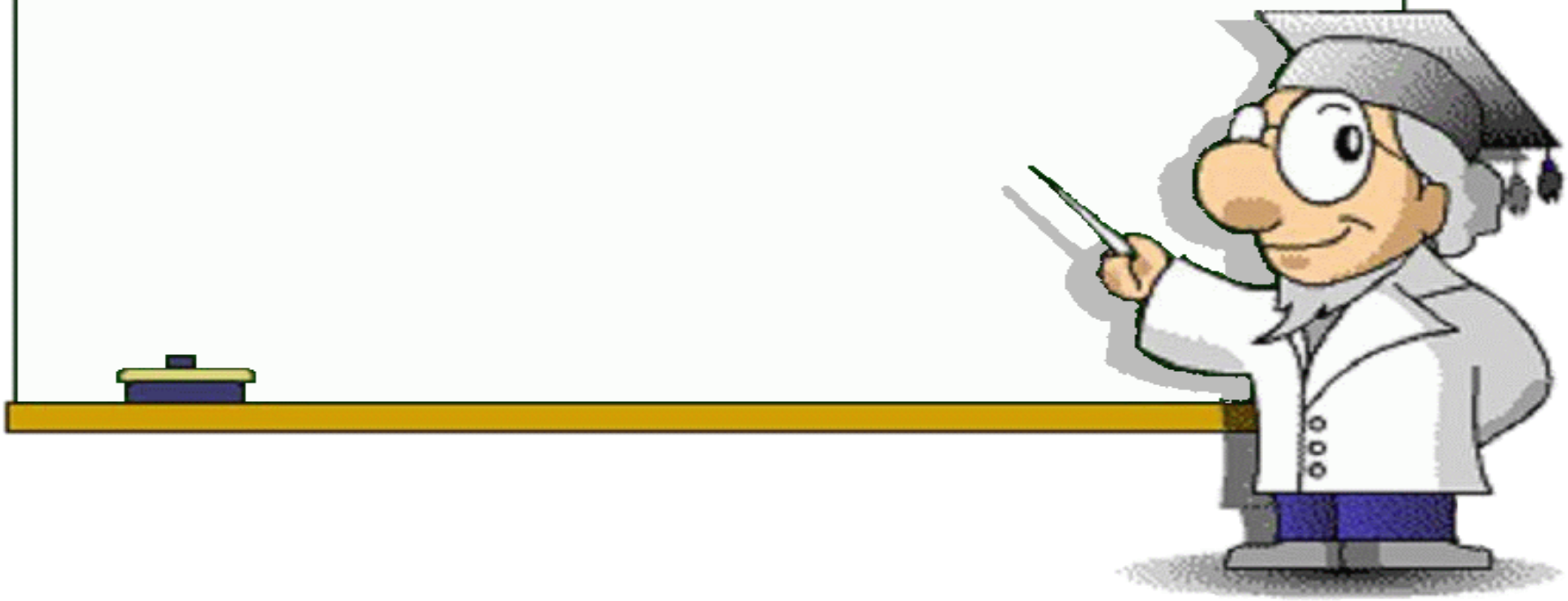
- 2015年12月、経済産業省から公開、企業の経営者を対象としたサイバーセキュリティ対策を推進するためのガイド
  - 経営者が認識する必要のある「3原則」、経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部(CISO等)に指示すべき「重要10項目」を記載

指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

経営戦略の観点から守るべき情報を特定させた上で、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、リスクに対応するための計画を策定させる。その際、サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策も検討した上で、残留リスクを識別させる。

目次

- 脆弱性とは
- 脆弱性対策　～情報収集に役立つキーワード～
- 変化点：IT管理からリスク/危機管理へ
- サイバーセキュリティ対策におけるリスク分析実施のススメ



サイバー攻撃と戦う兵法
～セキュリティリスク分析の重要性～

IPA

中国、春秋時代の軍事戦略家、孫武の兵法書『孫子』に示された名句に「彼を知り己を知れば百戦殆うからず」がある。サイバー攻撃時代において、敵＝脅威(攻撃者を含む)、己＝自組織と置き換えてみると、セキュリティ対策において効果的な施策を実施するための教えとなる。
リスク分析は、
　己を知り、敵を知れば、百戦殆うからず
を実践する、サイバーセキュリティ時代の兵法である。

「リスク分析」　＝　①②③を評価指標に、事業リスクを明確にするプロセス

① 評価対象(資産や事業)の価値(重要性)、想定される被害の規模・影響
② 評価対象に対して想定される脅威とその発生の可能性
③ 想定される脅威が生じた際の受容可能性(評価対象の脆弱性、対策不備)

リスク分析の重要性と有効性

① 実効的なリスクの低減の実現
② 効果的なセキュリティ投資の実現(追加対策、有効なテスト箇所の抽出)
③ PDCAサイクルの確立とセキュリティの維持向上を継続するためのベース

制御システムの
セキュリティリスク分析ガイド

- 具体的な手順を解説、テンプレート、チェックリスト等を提供
  https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

【ガイド本編の目次】

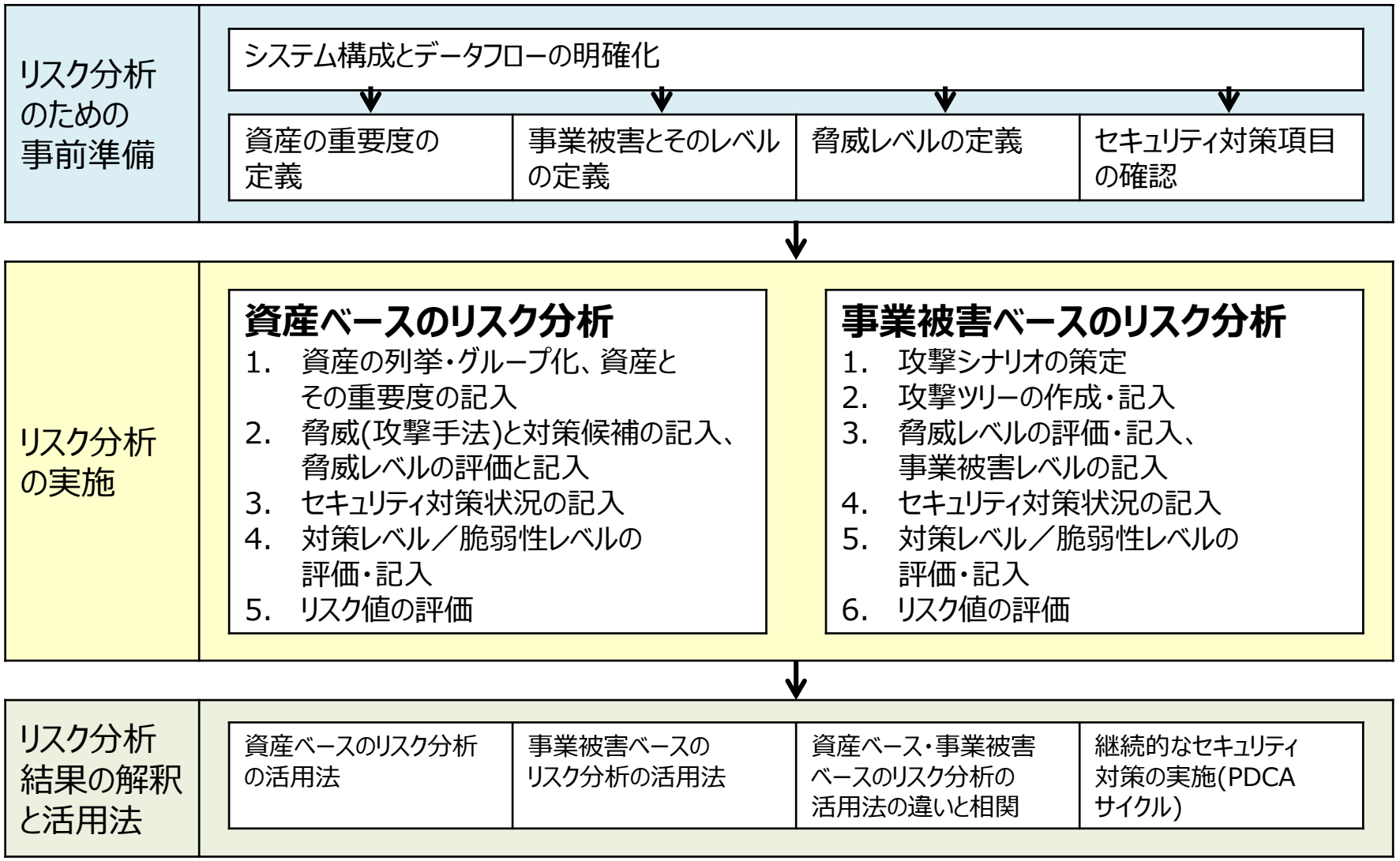
ガイド本編

350頁

別冊
(分析例フルセット)

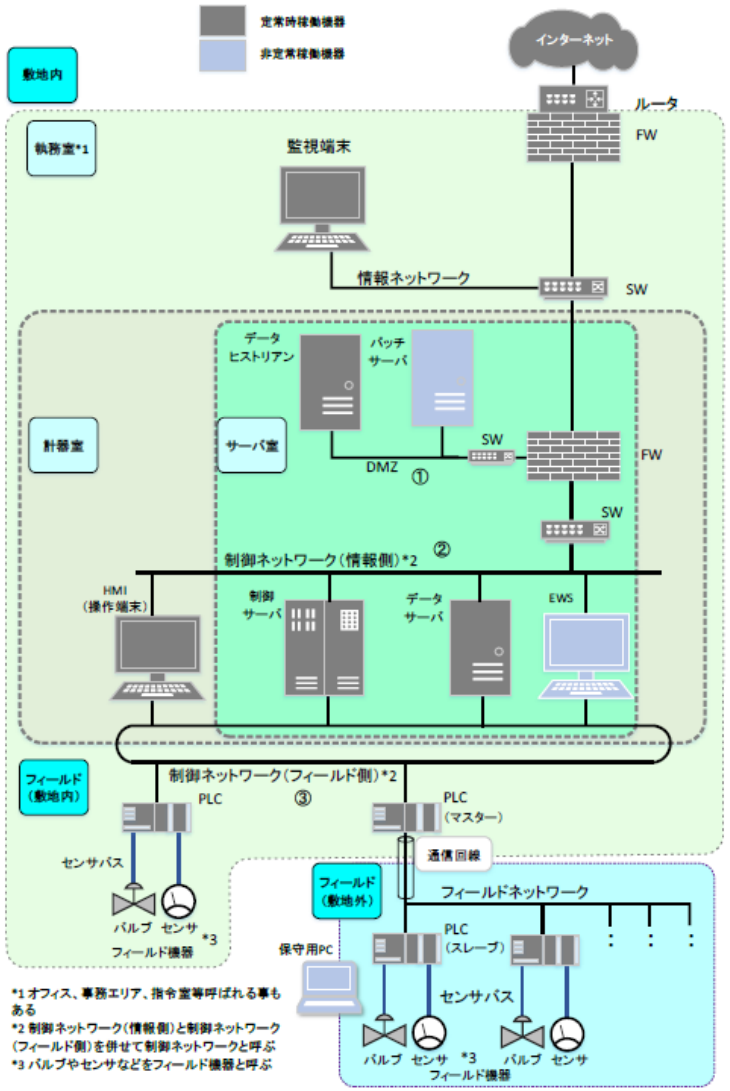
70頁

リスク分析の作業手順


リスク分析のための事前準備
システム構成とデータフローの明確化
資産の重要度の定義
事業被害とそのレベルの定義
脅威レベルの定義
セキュリティ対策項目の確認
リスク分析の実施
資産ベースのリスク分析
1. 資産の列挙・グループ化、資産とその重要度の記入
2. 脅威(攻撃手法)と対策候補の記入、脅威レベルの評価と記入
3. セキュリティ対策状況の記入
4. 対策レベル／脆弱性レベルの評価・記入
5. リスク値の評価
事業被害ベースのリスク分析
1. 攻撃シナリオの策定
2. 攻撃ツリーの作成・記入
3. 脅威レベルの評価・記入、事業被害レベルの記入
4. セキュリティ対策状況の記入
5. 対策レベル／脆弱性レベルの評価・記入
6. リスク値の評価
リスク分析結果の解釈と活用法
資産ベースのリスク分析の活用法
事業被害ベースのリスク分析の活用法
資産ベース・事業被害ベースのリスク分析の活用法の違いと相関
継続的なセキュリティ対策の実施(PDCAサイクル)

リスク分析の作業手順
～事前準備：システム構成とデータフローの明確化～

- 資産の洗い出し
- システム構成の明確化、論理化
  - 分析範囲の決定
  - 分析用アーキテクチャの明確化
  - 資産とその付帯情報の整理
  - 分析対象とする資産の絞り込み(グループ化と除外)
  - ロケーションと資産の配置
  - 各資産の接続情報の記述
- データフローの明確化
  - データの流れのシステム構成図へのマッピング



リスク分析の作業手順
～事前準備：資産の重要度、事業被害とそのレベルの定義～

防御側の視点からリストアップ

- 資産の重要度
  - 資産ベースのリスク分析における評価指標の一つ
  - システム資産としての価値、攻撃によって想定される事業被害や事業継続性への影響を考慮した評価点(1：低～3：高)
- 事業被害レベル
  - 事業被害ベースのリスク分析における評価指標の一つ
  - 脅威によって生じる事業被害の評価点(1：小～3：大)
- 事業被害
  - 組織の事業の安定的な運営や継続を阻害する事象・状況
  - 発生時の被害範囲や会社経営上の打撃を基に各事業者にて定義

リスク分析の作業手順
～事前準備：脅威レベル、脆弱性レベルの定義～

攻撃側の視点からリストアップ

- 脅威レベル
  - 2種類のリスク分析における評価指標の一つ
  - それぞれのリスク分析において、想定する脅威が発生する可能性の評価点(1：低～3：高)
- 脆弱性レベル
  - 2種類のリスク分析における評価指標の一つ
  - それぞれのリスク分析において、発生した脅威を受け入れる可能性の評価点(1：低～3：高)

リスク分析の作業手順
~リスク分析の実施~

IPA

- リスク分析の手法と特徴

#	分析手法			工数	効果
1	ベースラインアプローチ			小	△
2	非形式的アプローチ			小	×
3	詳細リスク分析	資産ベース		中	○
		シナリオベース	アタックツリー・アナリシス(ATA)	大	○
			フォールトツリー・アナリシス(FTA)	大	○
4	組み合わせアプローチ			大	◎

- アタックツリー・アナリシス(ATA)：攻撃者視点で、トップダウンに、誰が、どこから、どのルートを経由して被害発生を引き起こしうるかのシナリオをツリーとして構成していく方法
- フォールトツリー・アナリシス(FTA)：被害(インシデント等)事象を起点として、ボトムアップに、その被害に至る１ステップ前の攻撃事象を想起しながらツリーとして構成していく方法

リスク分析の作業手順
~リスク分析の実施~

- **資産ベースのリスク分析　＜己を知る＞**

  保護すべきシステムを構成する資産を対象に、各資産(サーバ、端末、通信機器等)に対して、その重要度(価値)、想定される脅威、脆弱性の３つを評価指標として、リスク分析を実施。

  ⇒　資産に対して網羅的に脅威と対策状況を評価可能

- **事業被害ベースのリスク分析　＜敵を知る＞**

  保護すべきシステムにおいて実現されている事業やサービスに対して、回避したい事業被害を定義し、発生した際の事業被害のレベル、その被害を起こしうる攻撃シナリオによる脅威、そのシナリオに対する脆弱性(そのシナリオの受容可能性)の３つを評価指標として、リスク分析を実施。

  ⇒　一次攻撃脅威から、連鎖して事業被害に繋がる攻撃を、
  　　評価可能(ATAとFTAの利点を融合)

  ⇒　**机上でのペネトレーションテスト**

リスク分析の作業手順
~リスク分析結果の解釈と活用法~

- リスク分析結果の解釈及び活用のねらい
  - セキュリティ上の弱点を発見し、サイバー攻撃に対するリスクを低減するため、分析結果として得られたリスク値を可能な限り低減する。

- リスク値の活用
  - リスクの把握
  - 改善箇所の抽出、選定
  - リスクの低減
  - リスクの低減効果の確認
  - セキュリティテストの対策箇所の抽出、特定

最後に

日々の脆弱性関連情報の収集だけではなく、
IT資産管理と連携させた対策を進めることで、
サイバーセキュリティリスクの管理を加味した脆
弱性対策を実現していく必要があります。
脆弱性に対して適切な対応をとっていきましょう。


IPA
Better Life
with IT