[CCDS]サーティフィケーションプログラム

IoT機器に対するリスク分析のガイド

一般社団法人
重要生活機器連携セキュリティ協議会

プロセス全体の流れ

■ステップ1－1．脅威分析
　1）システム構成図を用いた想定脅威の検討
　2）CCDS-STRIDEモデルによる脅威分類の実践

■ステップ1－2．対策立案
　3）リスク対策のためのフレームワーク活用
■ステップ1－3．検証手法の検討
　4）仮説の検証～検証ツールや検証手法を選定する

■ステップ２-1．リスク評価～レベル定義
　1）リスク評価の実施

手順②：守るべき情報、資産を明確化する

■守るべき資産の分析～守るべき資産とは？

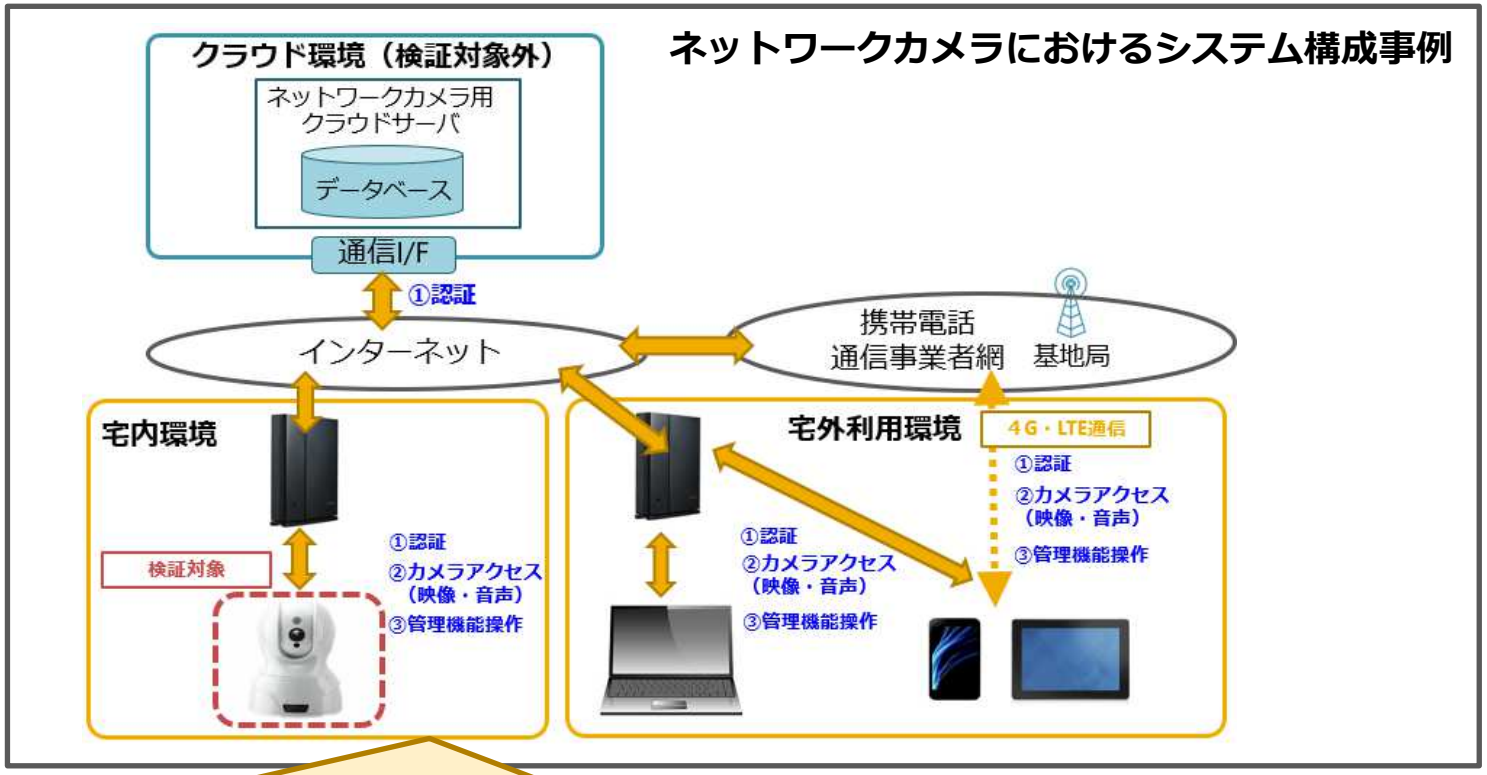
分類	具体事例
個人情報	氏名、生年月日等、個人を識別可能な情報
機密情報	企業にとって外部への開示を予定していない情報
金融資産	金銭（現金取扱い端末等）
金融資産に紐づくデータ	クレジットカード番号、銀行口座番号等
設定情報	ネットワークの設定情報、アクセス権限等
ログ情報	実際にやり取りされる通信データやクライアント、サーバの情報等
セキュリティ情報	アクセス用のID、Password情報や、電子証明書、暗号鍵等
機器本体	対象となるDUT機器本体
プログラムコード (ソフトウェア、ファームウェア)	対象DUTに含まれるソフトウェアやファームウェアなどのソースコード
健康、人命（※）	機器の利用にかかわるユーザの物理的安全性

※IoTに必要な「情報セキュリティ」に不足している考え方
・物理的安全（特に人命）を資産として考える
・人命に対する脅威を最優先として捉える
・コンプライアンス、製造物責任法（PL法）の順守

手順③：攻撃経路を分析する

■攻撃経路の分析

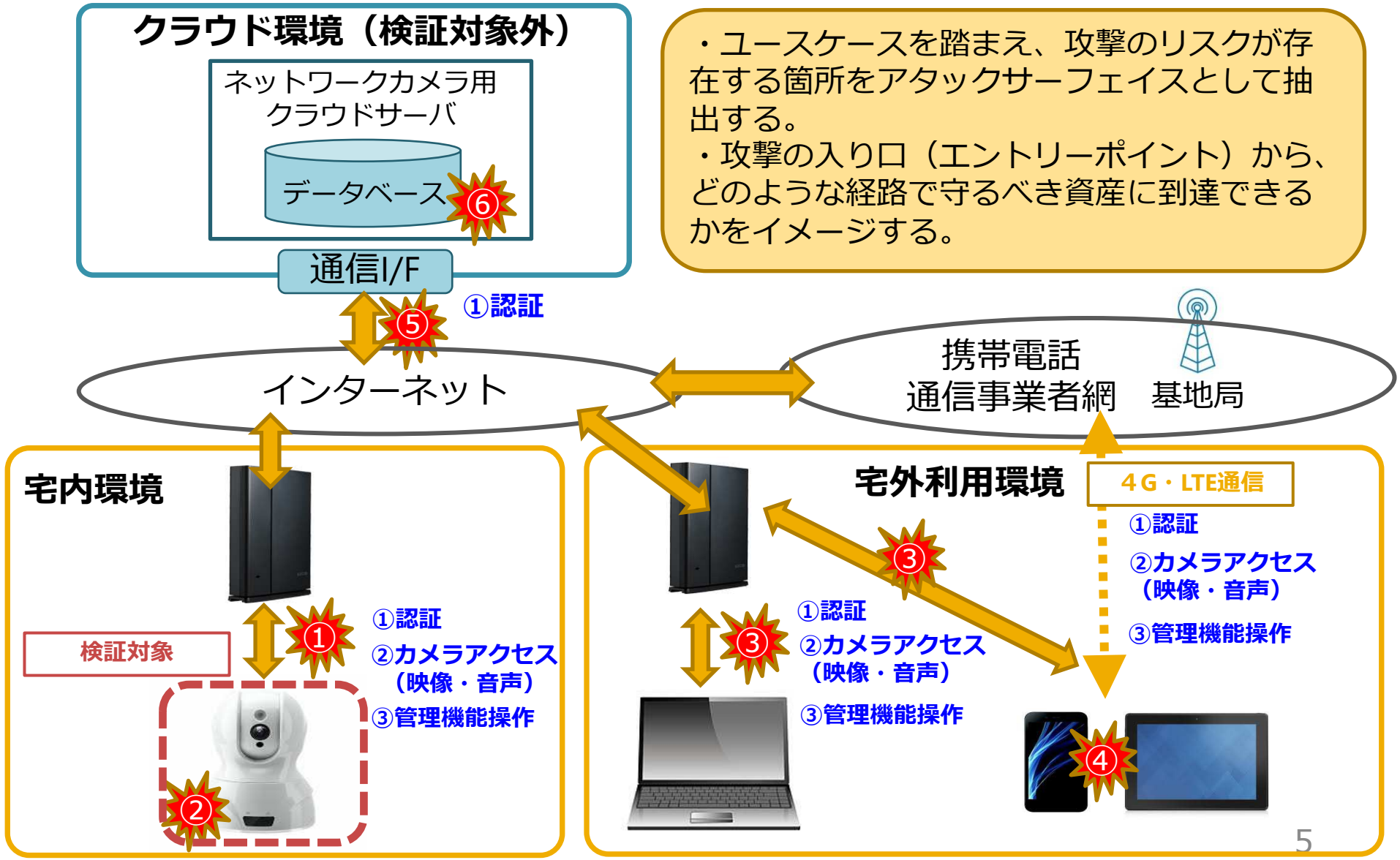
・システム構成図の中で、データの入出力やインタフェースを踏まえ、
攻撃の入口（エントリーポイント）やアタックサーフェイスの分析を行う。



攻撃者の視点で考える！
・どこに自分が欲しい資産（情報）があるのか
・そのためにはどこから攻撃するのが一番効率的（簡単）なのか

手順③：攻撃経路を分析する

■ネットワークカメラを事例としたエントリーポイント、アタックサーフェースの抽出



手順④：想定脅威の具体事例の検討

システム構成図で想定された各攻撃ポイント（AS＝アタックサーフェース）※について、具体的な脅威を分析していく。　※AS: ✸ マークが想定される攻撃ポイント

■システム構成において想定される具体的な脅威例（ネットワークカメラ）

対象範囲	攻撃ポイント	想定される具体的な攻撃	影響を受ける守るべき資産	脅威分類（後述）
カメラ本体	AS①	インターネット経路における通信情報、認証情報の漏洩、窃取	・認証情報 ・通信経路上のデータ	情報の暴露
	AS②	カメラの管理機能に対する不正アクセス（設定変更）	・管理機能上の設定情報 ・録画データ	不正アクセス
		カメラ機能、SDカード記録情報への不正アクセス	・録画データ	不正アクセス
		攻撃者によるカメラの踏み台利用		踏み台
PC用ソフトウェア	AS③	インターネット経路における通信情報、認証情報の漏洩、窃取	・認証情報	情報の暴露
スマートフォン・タブレット用アプリ	AS④	スマートフォン、タブレットアプリの個人情報の漏洩、窃取	・スマートフォン、タブレット内の連絡先等個人情報（アプリ連携のパーミッション）	情報の暴露
クラウドサーバ	AS⑤	インターネット経路における通信情報、認証情報の漏洩、窃取	・認証情報	情報の暴露
	AS⑥	ネットワークカメラサーバへの不正アクセス	・録画データ（クラウド保存をサポートしている場合） ・アップデート用のソフトウェア ・認証情報 ・復号鍵（秘密鍵）	不正アクセス

～～～～～以下、省略～～～～～～～

手順⑤：CCDS-STRIDEモデルによる脅威の分類

・STRIDEモデルなど活用して、各エントリーポイントの想定脅威を抽出、分類する

■STRIDE　脅威モデルによる分類

脅威名称	英語表記	説明
なりすまし	**S**poofing	コンピューターに対し、他のユーザーを装うこと
データの改ざん	**T**ampering with Data	権限なしでデータを改ざんし、データの完全性を失わせること
否認	**R**epudiation	ユーザーがあるアクションを行ったことを否認し、相手はこのアクションを証明する方法がないこと
情報の暴露(漏洩)	**I**nformal Disclosure	アクセス権限を持たない個人に情報が公開されること
サービス不能	**D**enial of Service	正規のユーザがサーバやサービスにアクセスできないこと
権限の昇格	**E**levation of Privilege	権限のないユーザーがアクセス権限を得ること

手順⑤：CCDS-STRIDEモデルによる脅威の分類

■STRIDEにCCDSで脅威を追加したモデル

脅威名称	英語表記	説明
なりすまし（偽装）	**S**poofing	コンピューターに対し、他のユーザーや機器を装うこと
データの改ざん	**T**ampering with Data	権限なしでデータを改ざんし、データの完全性を失わせること
否認	**R**epudiation	ユーザーがあるアクションを行ったことを否認し、相手はこのアクションを証明する方法がないこと
情報の暴露(漏洩)	**I**nformal Disclosure	アクセス権限を持たない個人に情報が公開されること
サービス不能(DoS)	**D**enial of Service	正規のユーザがサーバやサービスにアクセスできないこと ※DDoS攻撃やジャミングによるサービス妨害など
権限の昇格	**E**levation of Privilege	権限のないユーザーがアクセス権限を得ること
不正アクセス	Unauthorized access	アクセス権限を持たない者にアクセスされること
マルウェア感染	Malware infection	他の機器への汚染源になる。ランサムウェアなどにより業務妨害を受けること
踏み台	Stepping stone attack	他の機器へ不正アクセス等を行う際の中継地点として使用されること
不正改造(HW/SW)	Tampering with device	不正（違法）なハード、ソフトウェアの改造により、内部データを抜き取ったり、脆弱性の要因を組み込まれること
未知の脆弱性	Unknown Vulnerabilities	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性のこと

手順⑥：必要なセキュリティ対策のリストアップ

保護すべき資産への想定脅威に対して、どのような対策が必要であるかを分析し、対策名として整理する。

■ネットワークカメラにおけるセキュリティ対策の検討例

対象範囲	攻撃ポイント	想定される具体的な攻撃	影響を受ける守るべき資産	脅威分類	対策名
カメラ本体	AS①	インターネット経路における通信情報、認証情報の漏洩、窃取	・認証情報 ・通信経路上のデータ	情報の暴露	通信経路暗号化
	AS②	カメラの管理機能に対する不正アクセス（設定変更）	・管理機能上の設定情報 ・録画データ	不正アクセス	脆弱性対策
					セキュア開発
					ユーザ認証
		カメラ機能、SDカード記録情報への不正アクセス	・録画データ	不正アクセス	脆弱性対策
					セキュア開発
		攻撃者によるカメラの踏み台利用		踏み台	脆弱性対策
					セキュア開発
PC用ソフトウェア	AS③	インターネット経路における通信情報、認証情報の漏洩、窃取	・認証情報	情報の暴露	通信経路暗号化
スマートフォン・タブレット用アプリ	AS④	スマートフォン、タブレットアプリの個人情報の漏洩、窃取	・スマートフォン、タブレット内の連絡先等個人情報（アプリ連携のパラメータ）	情報の暴露	アプリ側の脆弱性対策 ※要個別対応
					アプリ側のセキュア開

～～～～～以下、省略～～～～～～～

参考）脅威別のセキュリティ対策一覧①

脅威	セキュリティ対策名
なりすまし（偽装）	サーバ認証
	メッセージ認証（デジタル署名）
データの改ざん	通信経路暗号化
	メッセージ認証（セキュアハッシュ）
否認	デジタル署名
情報の暴露（漏洩）～通信経路上	通信経路暗号化
	サーバ認証
	ユーザ認証
	データ二次利用禁止

脅威	セキュリティ対策名
情報の暴露（漏洩）～HW(SW)	データ暗号化
	出荷状態リセット
	セキュア消去
	耐タンパ―H/W
	耐タンパ―S/W
	遠隔消去
サービス不能	DoS対策
	FW（ファイアウォール）機能
	電磁波（ジャミング）対策
権限の昇格	脆弱性対策
	サーバセキュリティ
	セキュア開発
	IDS/IPS
	ユーザ認証
	ログ分析

参考）脅威別のセキュリティ対策一覧②

※CCDS追加項目に対するセキュリティ対策

脅威	セキュリティ対策名
不正アクセス	脆弱性対策
	サーバセキュリティ
	セキュア開発
	FW（ファイアウォール）機能
	ユーザ認証
	遠隔ロック
	ログ分析
マルウェア感染	脆弱性対策
	セキュア開発
	フィルタリング
	アンチウィルス
	仮想パッチ
	ホワイトリスト制御
	ソフトウェア署名

脅威	セキュリティ対策名
踏み台	脆弱性対策
	サーバセキュリティ
	セキュア開発
	IDS/IPS
	ユーザ認証
	ログ分析
不正改造（HW/SW）	ソフトウェア署名
	セキュア開発
	出荷状態リセット
	セキュア消去
	耐タンパ―HW
	耐タンパ―SW
未知の脆弱性	－

参考）セキュリティ対策の機能・目的①

対策名	機能・目的
脆弱性対策	開発段階での脆弱性混入を防止する。運用段階で検出された脆弱性を解消する。
セキュア開発	実装時にセキュアプログラミングを実施する。また、セキュリティテストを実施したことを確認の上で出荷する。
サーバセキュリティ	サーバのセキュリティ（設定情報を含む）を定期的に確認し、問題があれば修正する。
FW 機能	接続先を IP アドレス・ポート番号で制限する。
サーバ認証	クライアントがサーバを認証することにより、サーバへの成りすましを防止する。
フィルタリング	信頼できないウェブサイトへのアクセスを禁止する。また、信頼できないアドレスからのメール受信を拒否する。
IDS/IPS	入出力データを監視し、不正アクセスの検知、抑止を行う。
DoS 対策	DoS（DDoS）攻撃を遮断するための対策を実施する。
アンチウイルス	ウイルスを検知・除去して、ウイルス感染を防止する。
仮想パッチ	ソフトウェア更新等が実施できず、脆弱性を完全に除去できない場合、脆弱性を突いた攻撃を前段にてブロックする。（WAFによる対策など）
ユーザ認証	利用者を認証することにより、利用者の成りすましによる脅威を防止する。可能であれば、複数の認証要素を組み合わせた多要素認証技術を採用することが望ましい。
メッセージ認証	通信相手から送信されたメッセージを認証することにより、通信相手への成りすましによる偽メッセージ送信や、メッセージの改ざんを防止する。

参考）セキュリティ対策の機能・目的②

対策名	機能・目的
通信路暗号化	データの通信路を暗号化し、通信路上のデータが漏えいしたとしても、無価値化する（攻撃者にとって無意味なものとする）。また、通信路上でのデータの改ざんを検知する。
データ暗号化	データ自体を暗号化し、仮に蓄積時または通信時のデータが漏えいしたとしても、無価値化する（攻撃者にとって無意味なものとする）。
データ二次利用禁止	データの目的外利用を禁止し、二次利用先からの漏えいを防止する。
ホワイトリスト制御	予め許可したプログラム以外の動作を禁止し、ウイルス感染を防止する。
ソフトウェア署名	署名されたソフトウェアの動作のみ許可し、ウイルス感染したソフトウェアや不正改造されたソフトウェアの動作を防止する。
出荷時状態リセット	IoT 機器を出荷時状態にリセットして、データや出荷後の設定を全て削除する。
セキュア消去	記録していた場所から復元不可能な様にした上で、データを消去する。
耐タンパーH/W	筐体開封を検知して内部情報を自動消去する等、ハードウェア技術を用いて、内部構造や記憶しているデータの解析を困難とする。
耐タンパーS/W	プログラムやデータ構造の難読化等、ソフトウェア技術を用いて、内部構造や記憶しているデータの解析を困難とする。
遠隔ロック	遠隔操作により IoT 機器の機能をロックし、第三者による不正利用を防止する。
遠隔消去	遠隔操作により IoT 機器内のデータを消去し、情報漏えいを防止する。
ログ分析	各種ログを分析することで、不正アクセスを検知し、何が行われたかを突き止める。

手順⑦：対策フレームワークの活用と具体化

・セキュリティ対策の具体的な対策内容を、Online Trust Alliance（OTA）の「OTA IoT Trust Framework」[参考資料：3-1]や、OWASPの「OWASP Top 10 IoT Vulnerabilities」[参考資料：３-２]等のフレームワークを参考に検討し、対応する対策番号を記載する。

■ネットワークカメラにおけるセキュリティ対策の検討例（OTA,OWASP）

対象範囲	攻撃ポイント	想定される具体的な攻撃	影響を受ける守るべき資産	脅威分類	対策名	OTA分類	OWASP分類
カメラ本体	AS①	インターネット経路における通信情報、認証情報の漏洩、窃取	・認証情報 ・通信経路上のデータ	情報の暴露	通信経路暗号化	1，2，3	4，8
	AS②	カメラの管理機能に対する不正アクセス（設定変更）	・管理機能上の設定情報 ・録画データ	不正アクセス	脆弱性対策	[redacted]	
					セキュア開発	2，7	3，4，5，6
					ユーザ認証	[redacted]	
		カメラ機能、SDカード記録情報への不正アクセス	・録画データ	不正アクセス	脆弱性対策	[redacted]	
					セキュア開発	2，7	3，4，5，6
		攻撃者によるカメラの踏み台利用		踏み台	脆弱性対策	[redacted]	
					セキュア開発	2，7	3，4，5，6
PC用ソフトウェア							

～～～～～以下、省略～～～～～～～

手順⑦：対策フレームワークの活用と具体化

①Online Trust Alliance（OTA）の対策フレームワーク

参考資料：3A-1）「OTA IoT Trust Framework」

⇒31項目（Update July 12 , 2016）

[文書構成]

	対策観点	項目数
1	デバイス、アプリケーション、クラウドサービスのセキュリティ	10項目
2	ユーザアクセスと資格情報	5項目
3	プライバシー　透明性と開示	16項目

[概要]

「Online Trust Alliance」はオンラインの信頼性を向上させる事を目的としたアメリカの非営利団体である。このフレームワークはIoT機器向けの対策として、メールを含む通信プロトコルやアクセス権限管理、プライバシー保護のための遵守事項等、幅広い範囲に渡って記載されている。どちらかと言えば、セキュリティを強化するための実装やサービス要件も含まれており、評価・検証用としては、やや使いにくい印象。

手順⑦：対策フレームワークの活用と具体化

②OWASPの対策フレームワーク

参考資料：３A-２）「OWASP Top 10 IoT Vulnerabilities」

⇒10項目、※57の小項目

[文書構成]

	対策観点	項目数
1	セキュリティが確保されていないWebインターフェイス	5項目
2	不十分な認証	10項目
3	セキュリティが確保されていないネットワークサービス	3項目
4	暗号化されていないトランスポート	4項目
5	プライバシーに関する懸念	6項目
6	セキュリティが確保されていないクラウドインターフェイス	6項目
7	セキュリティが確保されていないモバイルインターフェイス	6項目
8	不十分なセキュリティ設定	5項目
9	セキュリティが確保されていないソフトウェア/ファームウェア	6項目
１０	物理的セキュリティの脆弱さ	6項目

手順⑧：リスク評価の実施

ステップ1で分析した想定脅威に対して、後述の手法を用いたリスク評価を行い、検証・対策優先度の参考指標とする

■ネットワークカメラにおけるリスク評価の対象例

対象範囲	攻撃ポイント	想定される具体的な攻撃	影響を受ける守るべき資産	脅威分類	対策名
カメラ本体	AS①	インターネット経路における通信情報 認証情報の漏洩、窃取	想定脅威①⇒　リスク評価を実施		通信経路暗号化
		カメラの管理機能に対する不正アクセ （設定変更）	・管理機能上の設定情 想定脅威②⇒　リスク評価を実施 ・録画データ		脆弱性対策 セキュア開発 ユーザ認証
	AS②	カメラ機能、SDカード記録情報への不 正アクセス	想定脅威③⇒　リスク評価を実施 ・録画データ		脆弱性対策 セキュア開発
		攻撃者によるカメラの踏み台利用	想定脅威④⇒　リスク評価を実施		脆弱性対策 セキュア開発
PC用ソフトウェア	AS③	インターネット経路における通信情報 認証情報の漏洩、窃取	想定脅威⑤⇒　リスク評価を実施		通信経路暗号化
スマートフォン・タブレット用アプリ	AS④	スマートフォン、タブレットアプリの個 人情報の漏洩、窃取	・スマートフォン、タブレット内の連絡先等 想定脅威⑥⇒　リスク評価を実施 のパーミッション）		アプリ側の脆弱性対策 ※要個別対応 アプリ側のセキュア開発 ※要個別対応

リスク評価とは

事象の重要度、緊急度を数値化したもの

（先述のレポート記載項目「重要度(Severity)」と同意で、優先度(Priority)は重要度の値を基に設計側が判断する）

リスク評価手法のひとつ「CVSS v3 」について

CVSSとは：深刻度を計る数値　(Common Vulnerability Scoring System)

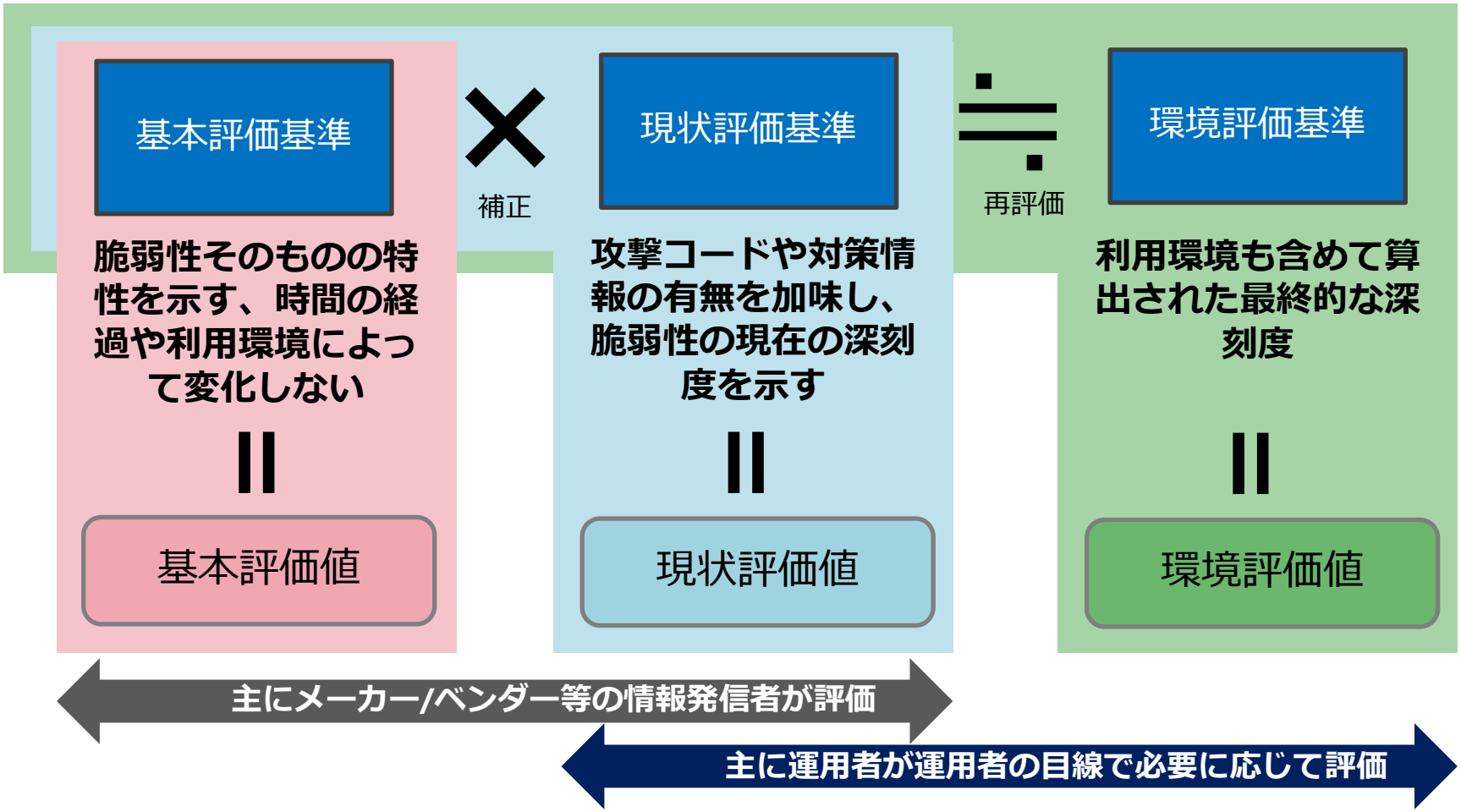
定量化する事で問題の深刻度・対応緊急度を判断する為の共通の材料として扱う（改修優先度の判断材料にもなる）

深刻度は5段階評価

深刻度	スコア
緊急	9.0 ～ 10.0
重要	7.0 ～ 8.9
警告	4.0 ～ 6.9
注意	0.1 ～ 3.9
なし	0

CVSSの特徴

各評価基準による算出のロジック



CVSS v3の計算手法　[基本評価基準]

①基本評価基準の計算因子（配布資料：CVSS 因子解説参照）

機密性への影響
×
完全性への影響
×
可用性への影響

情報セキュリティの3要素への影響
各特性が損なわれる影響がある可能性を
「高い＞低い＞ない」の3段階で数値化する

調整前影響度

×

スコープ変更

影響の広がりを判断
なし　or　あり（値UP）

影響度

攻撃元区分　どこから攻撃できるのか
×
攻撃条件の複雑さ　特定の条件を満たした時だけ攻撃されるのか
×
必要な特権レベル　攻撃に権限が必要かどうか ※スコープ変更ありなら評価値UP
×
ユーザ関与レベル　ユーザによるアクションが必要か

各状況の掛け合わせで
数値を出す

攻撃容易性

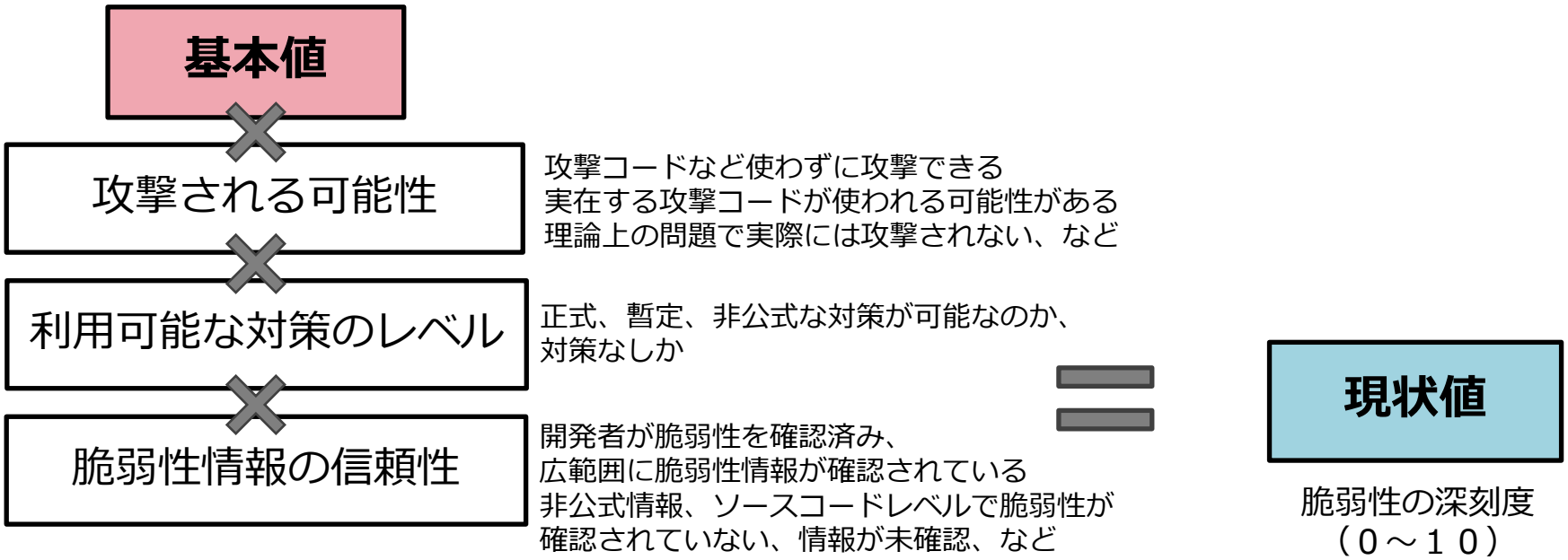
＝

脆弱性の深刻度
（０～１０）

基本値

CVSS v3の計算手法　[現状評価基準]

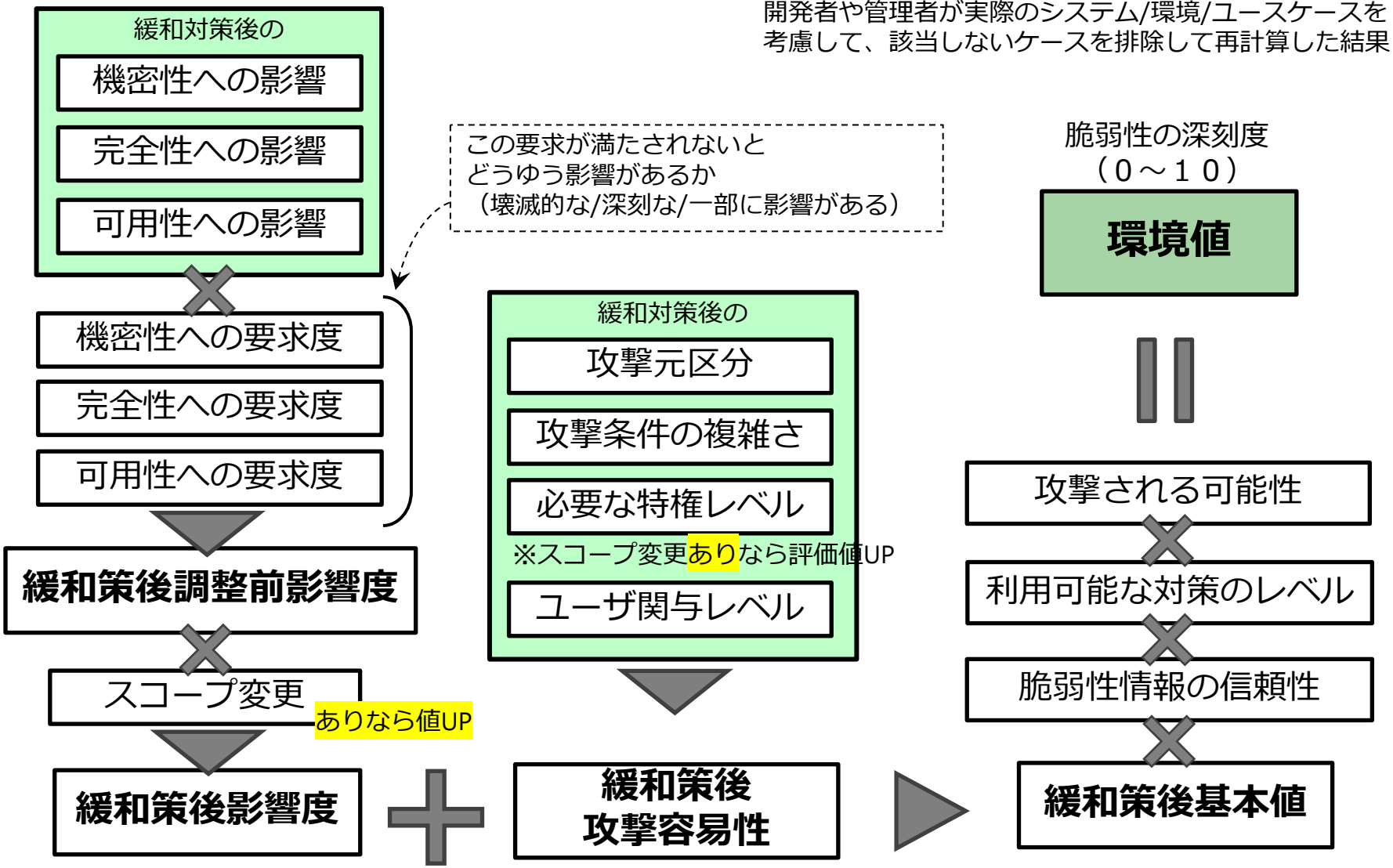
②現状評価基準の計算因子



CVSS v3の計算手法　[環境評価基準]

③環境評価基準の計算因子

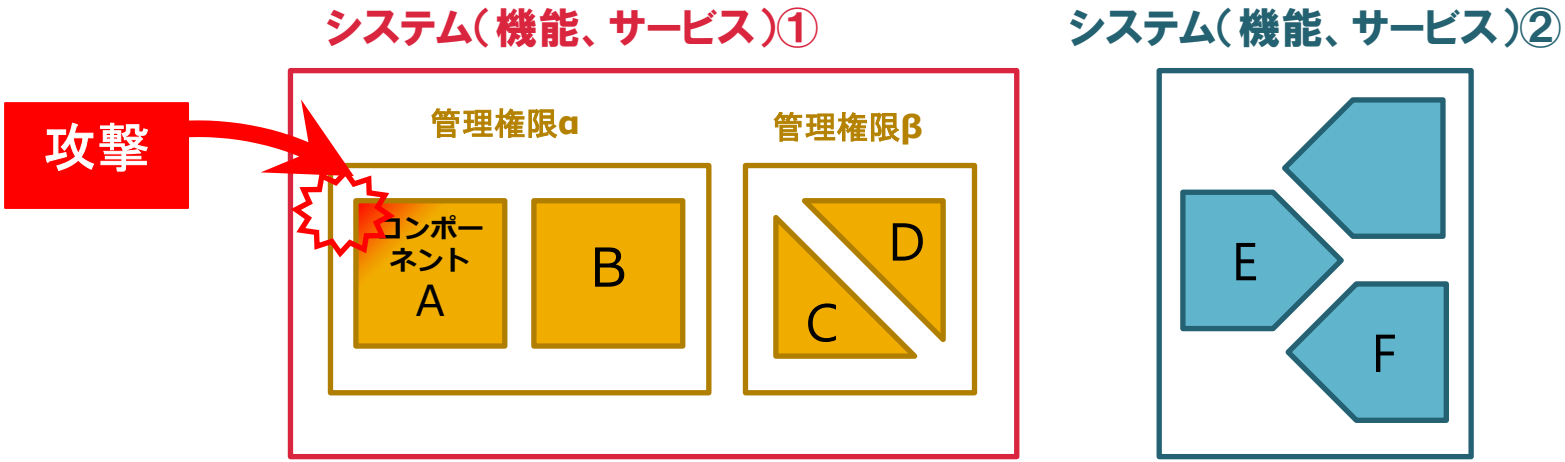
緩和対策後とは、
開発者や管理者が実際のシステム/環境/ユースケースを
考慮して、該当しないケースを排除して再計算した結果



CVSS v3の計算因子　スコープについて

スコープとは

システムやサービスはいくつものソフトウェアのパートが集まって成り立っているが、その一部の脆弱性のあるパートが攻撃された際に、影響が攻撃を受けたパートに留まる（または同じ管理権限のパートに留まる）か、それ以外に影響を及ぼすかを評価値に反映させる因子



影響がA、またはBに留まる　⇒スコープ変更無し

影響が他の管理権限のC、DまたはE、Fに及ぶ　⇒スコープ変更あり