なんちゃってCSIRTを抜け出したい

- SIM3による成熟度評価 -

Internet week 2020

2020年11月25日

小村　誠一

なんちゃってCSIRTって？

- 何も起きないから何もしない
- 作ったあと、見直しをしていない
- メンバと連絡方法以外は決まってない。
  インシデントは発生してからどうするか考える

なんちゃってCSIRTを抜け出したい！

CSIRTをどう改善すればいいか言えますか？

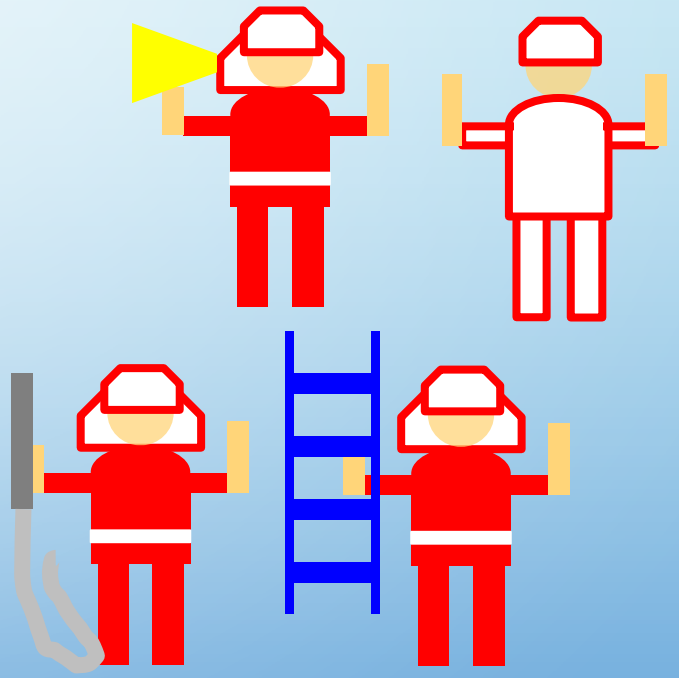
答えられない理由は？

CSIRTの状況を知らない

どう改善すればいいか知らない

CSIRTの状況を知るって、どうやったらいいの？！

- CSIRTの形、構成
- メンバとする人材
- メンバが使う道具、環境
- どう活動するか



SIM3とは

SECURITY INCIDENT MANAGEMENT
MATURITY MODEL

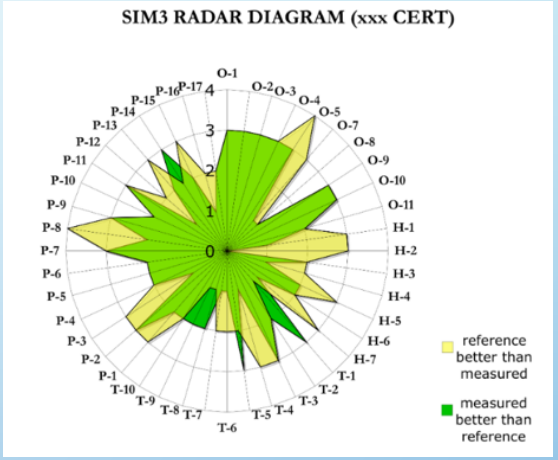
CSIRTマネジメントの
成熟度を評価し、改善に活用

SIM3の構成

1. 組織、人材、ツール、プロセスの分野、44の測定項目
   例）役務：CSIRTとして行う活動とその提供法を決めること
2. 項目の文書化、承認、評価改善に基づくレベル分け

SIM3の成熟レベル	
0	未定義・不明
1	認識しているが文書化していない
2	文書化しているが責任者の承認を得ていない
3	文書化し責任者が承認済み
4	3に加え、評価・改善を実施

SIM3の評価チャート



☆★全ての項目が4でなければならないということではない★☆

3. 各項目において必ず実施しなければいけない最低条件

EUでのSIM3活用

EUの一機関、ENISAがCSIRTのセルフチェック用の文書を開発

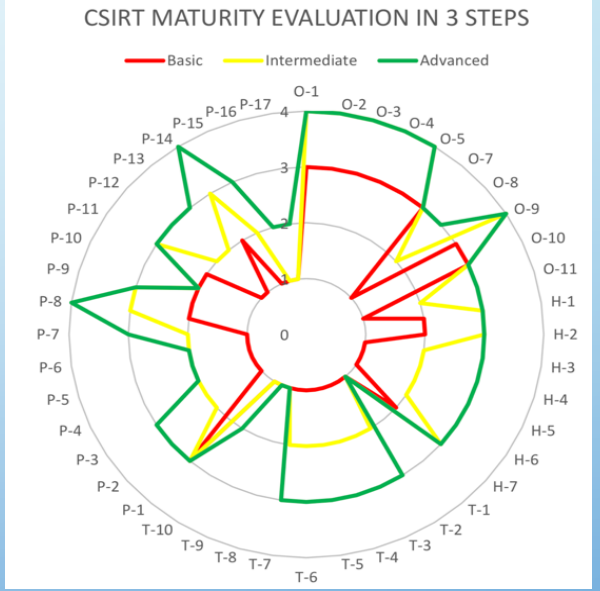
- 目的

  EU加盟国のナショナルCSIRTの成熟度向上

- 方法

  セルフチェック、およびペアチェック法

- 項目は3ステップとも同じであり、違いはレベルのみ
- 全項目がレベル1以上



CSIRTの形を整理するポイントが列挙

項番	項目	概要
O-1	任命	上位のマネジメント層からCSIRTメンバに任命されているか
O-2	Constituency	CSIRTの「クライアント」、CSIRTが守る部署や対象機器など
O-3	権限	CSIRTの目的を達成する為に、Constituencyへの実施が認められている行為
O-4	責任	CSIRTの目的を達成する為に、Constituencyへの実質が期待されていること
O-5	役務	CSIRTとして行う活動とその提供法を決めること
O-6	【なし】	
O-7	約款(SLA)	CSIRTが提供する役務の期待されるレベルを決めること
O-8	インシデント分類体系	インシデントの記録時に利用可能な分類体系とその適用法
O-9	CSIRT間連携	既存の他CSIRTと適切に構築された協力関係における位置付けや役割を決めること
O-10	組織体系	CSIRTを統括する文書にO-1からO-9を全て整合させること
O-11	セキュリティポリシ	CSIRTの運用に関わるセキュリティ体系を決めること

O-3 権限

CSIRTが目的を達成するために、および役割を完遂するための権限を有している／活動が認められている必要がある

システム停止などを行うような直接的な権限以外にも、助言を然るべき権限を持つ者に行う権限などの間接的な権限も含む

O-3 権限 レベル別回答事例

0. CSIRTが持つ権限について、考えたことや議論したことがない
1. いくつかの権限を用いて、業務を遂行しているが、
   明文化できていない
2. チームが持つ権限や裁量を文書化している
3. チームが持つ権限を文書化し、上位マネジメントが承認している
4. 3.に加え、定期的に権限が相応しいか、見直しを実施している

O-3: 権限が決まっていなかったら？

何が困る？　　困らない？

人材

メンバの行動指針や人材配置、スキルセット、トレーニング、外部連携などの7件の成熟パラメータ

項番	項目	概要
H-1	行動指針・服務規程・倫理規定	仕事外を含め、専門家としてどのように行動するかに関するCSIRTメンバーの規則やガイドラインの文書類
H-2	稼働の弾力性	CSIRTの職員数を決める際には、病気、休暇、離職などの可能性を考慮し要員を確保していること
H-3	スキルセット	CSIRTの仕事に必要なスキルセットを決めていること
H-4	内部トレーニング	新しいメンバーの訓練および既存メンバーのスキル向上のために（種類を問わず）内部トレーニング
H-5	外部の技術トレーニング	スタッフが外部の技術トレーニングを受けられる制度
H-6	コミュニケーショントレーニング	スタッフが外部の（人的）コミュニケーションまたはプレゼンテーショントレーニングを受けられる制度
H-7	対外連携	他のCSIRTと交流を持ち、可能な時にはCSIRT間連携やCSIRTコミュニティに貢献すること

H-5:（外部の）技術トレーニング

- あなたのCSIRTでは、メンバーが業務に関連した技術トレーニングを受ける機会を提供しているか？
- このトレーニングは、通常は外部トレーニングを指している。外部トレーニングには、例えばTRANSITS、ENISA CSIRT TRAININGや、CERT/CCやSANSをはじめとする機関から有償で提供される外部トレーニングなどが挙げられる。組織が大きい場合には、そのようなトレーニングも（一部は）内部で受けられることがある

ツール

Constituencyが使用するシステム構成情報や冗長化された電話回線、メールなどのコミュニケーション手段、インシデントの予防、検知、対応のためのツール等の10件の成熟パラメータ

項番	項目	概要
T-1	IT資産リスト	Constituencyが通常利用するHW、SW等からなるIT資産リスト
T-2	情報ソースリスト	脆弱性情報、脅威情報およびスキャン情報を入手するための情報ソースリスト
T-3	統合電子メールシステム	CSIRTの全てのメールが（少なくとも）一つの格納場所に保管され、全てのCSIRTメンバーが閲覧できるメールシステム
T-4	インシデント管理システム	インシデントを登録し管理するため、チケット管理や状況管理等のインシデント管理システム
T-5	耐性のある電話環境	代替手段も含めて、稼働時間と故障からの復旧時間がCSIRTのサービス要求条件を満たす電話環境
T-6	耐性のある電子メール環境	代替手段も含めて、稼働時間と故障からの復旧時間がCSIRTのサービス要求条件を満たす電子メール環境
T-7	耐性のあるインターネットアクセス環境	代替手段も含めて、稼働時間と故障からの復旧時間がCSIRTのサービス要求条件を満たすインターネットアクセス環境
T-8	インシデント防止ツール群	Constituencyにおけるインシデント発生防止を目的としたツール群
T-9	インシデント検知ツール群	インシデントが発生した時、あるいは発生しそうな時にインシデントを検知することを目的とするツール群
T-10	インシデント対応ツール群	インシデント発生後に、その解決を目的するツール群

T-2　情報ソース

あなたのCSIRTは、脆弱性／動向／スキャン情報を得るための情報源（情報フィード、WEBサイト、新聞、ツイート等）のリストを保管しているか？リストがある場合、情報源の重要度についても把握する必要がある。例として、一次、二次、三次情報源に分けるなど

プロセス

インシデント対応や防止、エスカレーションなどの17件の成熟パラメータ

項番	項目	概要
P-1	経営層へのエスカレーション	上位マネジメント、または顧客の経営層レベルへのエスカレーション
P-2	広報機能へのエスカレーション	CSIRTが所属する組織の広報機能へのエスカレーション
P-3	法務機能へのエスカレーション	CSIRTが所属する組織の法務機能へのエスカレーション
P-4	インシデント防止プロセス	CSIRTがどのようにインシデントを防止するか、関連するツール等の利用法を含めて決めること
P-5	インシデント検知プロセス	CSIRTがどのようにインシデントを検知するか、関連するツール等の利用法を含めて決めること
P-6	インシデント対応プロセス	CSIRTがどのようにインシデントを解決するか、関連するツール等の利用法を含めて決めること
P-7	特定のインシデントプロセス	フィッシングや著作権侵害のような特定のインシデントの取り扱いを決めること
P-8	監査/フィードバックプロセス	自己評価や外部監査、内部監査、その後のフィードバックにより、CSIRTがどのように体制や運用を評価するか決めること

プロセス

（続き）

項番	項目	概要
P-9	緊急連絡プロセス	緊急時にどのようにCSIRTへ連絡するか決めること
P-10	E-mailやWebプレゼンスのベストプラクティス	次の２点を決めること (1)CSIRTまたはCSIRTに報告すべきタイミングと内容を知る関係者が、セキュリティに関係するメールボックスの包括的なエイリアスを取り扱う方法 (2)Webサイトの公開法
P-11	機密情報取り扱いプロセス	CSIRTが機密情報を含むインシデントレポートや報告をどのように取り扱うか決めること
P-12	情報ソースプロセス	CSIRTが情報ソースをどのように取り扱うか決めること
P-13	啓蒙活動プロセス	インシデント対応とは関連がないが、CSIRT組織の認知向上や意識向上のためにConstituencyへどのような啓蒙活動を行うか決めること
P-14	報告プロセス	管理層やCISO等への報告をどのように行うか決めること
P-15	統計情報プロセス	インシデントの分類(0-8参照)にもとづき、どのようなインシデント統計情報をConstituencyや外部に開示するか決めること
P-16	会議プロセス	CSIRT内部の会議を定義すること
P-17	CSIRT連携プロセス	CSIRTが同じような立場のCSIRTや"上位の"CSIRTとどうのように活動するかを決めること

P-1 経営層へのエスカレーション

緊急性と重要性が高いインシデントまたは脅威が発生した場合に、できるだけ迅速かつ直接的にコンスティテュエンシー上層部に知らせる/警告するプロセスがあるか？

コンスティテュエンシーが親組織の外部にあり、より独立した組織で存在している場合、それらのすべてにエスカレーションする必要がある。

このような性質のエスカレーションは、営業時間内だけでなく、常時有効である必要がある。また、エスカレーションプロセスを有効にするには、エスカレーションプロセスをできるだけ短くする必要がある。

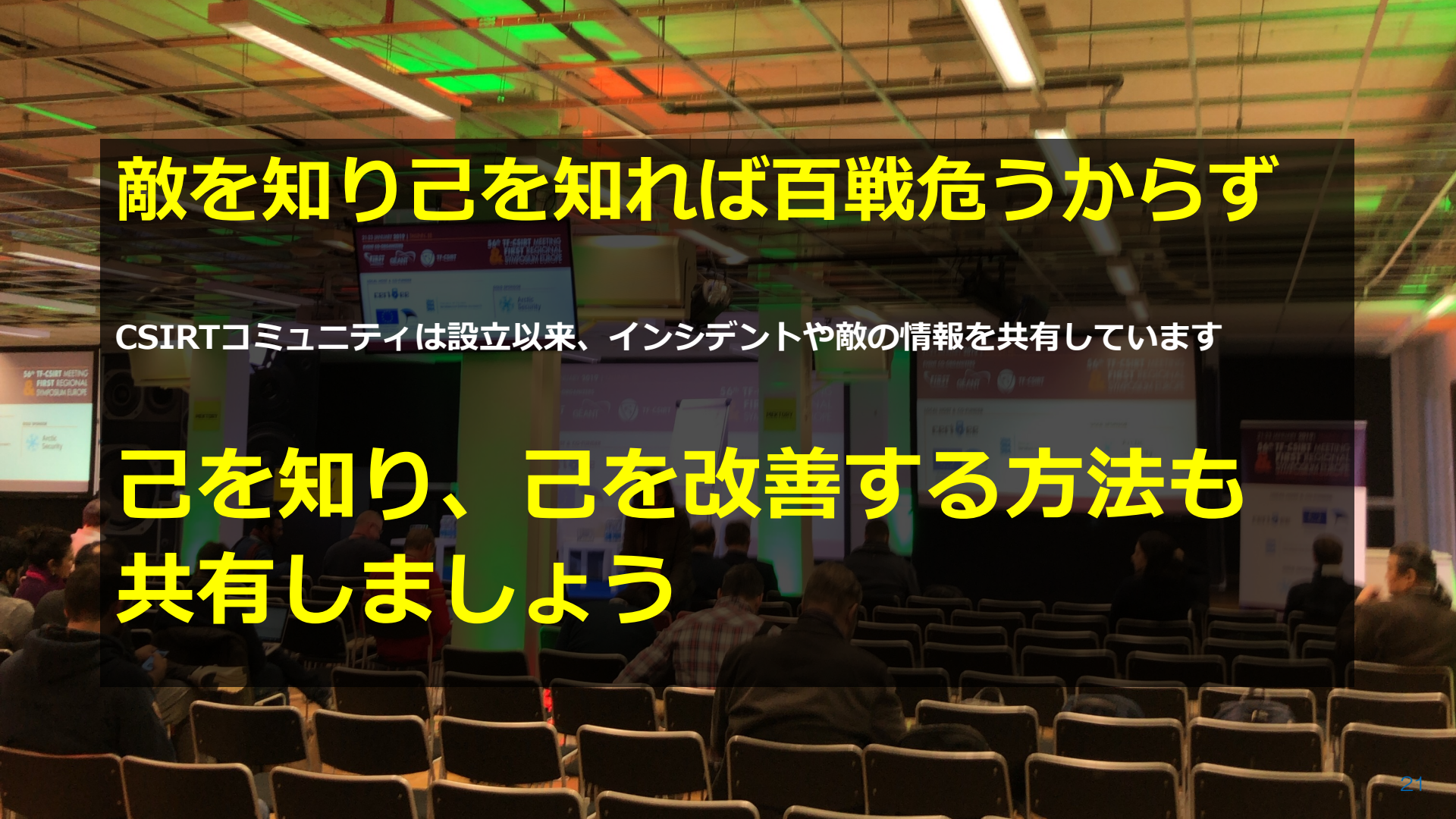
SIM3のレベル

SIM3の成熟レベル	
0	未定義・不明
1	認識しているが文書化していない
2	文書化しているが責任者の承認を得ていない
3	文書化し責任者が承認済み
4	3に加え、評価・改善を実施

レベル3の良い点は？、問題点は？

良い点

問題点



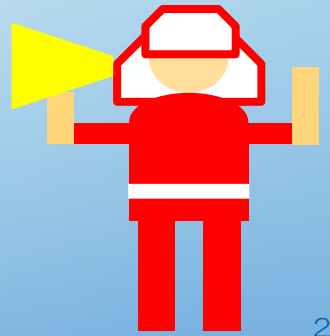
敵を知り己を知れば百戦危うからず

CSIRTコミュニティは設立以来、インシデントや敵の情報を共有しています

己を知り、己を改善する方法も共有しましょう

状況整理の観点や改善法が整理されている

どうしたいか考えるのは
会社やあなた



DIZEKUJE

DANK U WELL

DANKE SHOEN

THANK YOU VERY MUCH

どうも　ありがとう