FUTURE

脆弱性管理と組織組成：
- X.1060で考える、脆弱性管理の機能 -

2024年02月03日

フューチャー株式会社
CyberSecurityInnovationGroup
井上圭

TLP:GREEN

概要

脆弱性対応と、それを行う組織について X.1060を用いて考えてみようと思います。
学生の方は企業セキュリティの全体像をなんとなく見てみる、社会人の方は現状の確認と改善に使える話と思われます。

1. 脆弱性管理してますか？
   - なぜ必要？何をするの？
   - “対応”ではなく“管理”なのは何故？
2. 企業における標準的な脆弱性管理
   - 一般的なフローと、企業での運用
   - 理想と現実
3. 企業におけるセキュリティ対応組織と、脆弱性管理の位置づけ
   - 脆弱性管理と、その他の活動
4. 脆弱性管理を、X.1060で考える
   - 脆弱性管理に関する、必要な“機能”
5. まとめ

Note
- なるべく理解しやすいように簡略化している部分があるため、一部説明を省略している部分があります。
- また、脆弱性対応の全体像を示しますが、経営層の意思等も関係してくるため、SOC/CSIRT目線での見え方で記載しています。
- 本講演内容すべてについて、わたくし個人の意見であり、弊社および弊社製品等とは無関係です。組織の意見でもありません。

自己紹介

井上圭

■ フューチャー株式会社
- サイバーセキュリティイノベーショングループ
  - ✓ シニアコンサルタント

■ 業務概要
- セキュリティコンサルタント（？）
- 脆弱性管理製品FutureVuls 営業、サポート、トレーニング
- JNSA, ISOG-J, NCA 加盟
- 講演等
  - ✓ NICT サイバーコロッセオ,CodeBlue OpenTalks,Janog52, InternetWeek2023、OWASP Capter、NCA AnnualConference etc
- 勉強会主催
  - ✓ 脆弱性対応勉強会、Vuls祭り etc

■ その他
- バイク3台所有（V-TwinMagna/GRPM(JC92)/CB-150R）
- サウナ・スパ健康アドバイザー 資格保有
- 水風呂が心の支え
- 「脆弱性対応勉強」主催
- セキュリティの「温泉地シンポジウム」4か所、全てバイクで踏破(2023)

Vuls
Agentless Vulnerability Scanner for Linux/FreeBSD

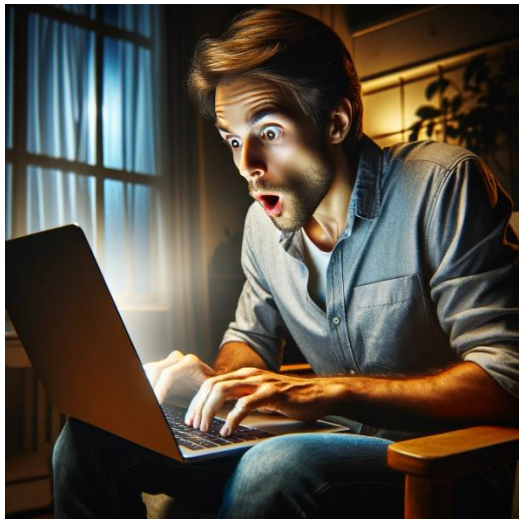
Future Vuls
継続的な脆弱性管理のFutureVuls


ISOG-J WG6 撮影

TLP:GREEN

1. 脆弱性対応、していますか？

システムを運用する場合、脆弱性管理が業務の一環として必要になります。



そもそも、何故、脆弱性管理が必要なのでしょうか。

- ■ ソフトウェアやライブラリは、ある日突然、脆弱性が発見される
  - ➢ 経年劣化ではなく、”見つけられてしまう“
  - ➢ その為、「ある日突然脆弱性が発見される」ように見える

放置するとどうなるのでしょうか。

- ■ 悪用される場合も、悪用されない場合もある
  - ➢ 悪用されないのは運が良いだけ、悪用される可能性（=リスク）が存在し、リスクは高低様々
- ■ 悪用された場合、何らかの被害が発生する
  - ➢ サービスが（不便になる|停止する）、それにより顧客に不利益を起こす
  - ➢ それらの対処として、金銭保証や社会的信用低下などにより、事業に影響が出る（最悪、倒産など）
- ■ 悪用されなかった場合、何も起こらない
  - ➢ あくまで一時的な物であり、将来にわたって”何も起こらない”事が保証されているわけではない

脆弱性によりもたらされる「リスク」を低減する為、脆弱性管理が必要です。

■ そもそも「リスク」とは？

- 一般的に「リスク＝脅威×脆弱性×資産価値」と言われています
- 脆弱性管理という観点では、以下のように解釈します
  - ✓ 脅威　　：対象の脆弱性に対する、攻撃者の動向やExploitの有無など、悪用される可能性
  - ✓ 脆弱性　　：脆弱性それ自体の危険性
  - ✓ 資産価値　：対象となるシステムの資産価値（提供するサービスの価値、事業への影響度合い）

ソフトウェアの脆弱性の危険度が高くとも、
資産価値や脅威が少なければ、全体としては
“非常に危険ですぐに対応が必要”「ではない」
と判断できる。

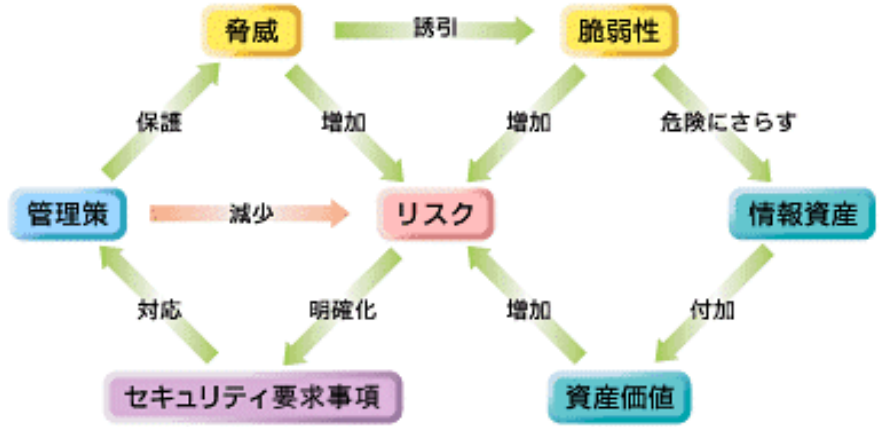
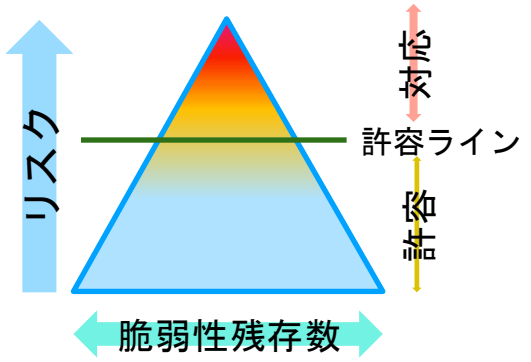


図2 情報資産、脆弱性、脅威の識別とその因果関係（参照 GMITS Part1）

https://atmarkit.itmedia.co.jp/ait/articles/0210/17/news001.html

■ 脆弱性「管理」とは

- 実運用上、「すべての製品」を「直ぐに修正」できるわけではない
  - ✓ 数の多さ、対応するための時間や人員、無停止が求められる、等がある
- 許容できる脆弱性も存在する
  - ✓ 例：「ローカルコンソールにキーボードをつなぎ、ESCを連打するとログインできてしまうバグ」は、本当に危険なのか？
- 目的は、リスクを減らす（下げる）こと
  - ✓ リスクが許容できる場合は、全ての脆弱性に「対応（＝アップでデートや修正）」する必要はない
- リスクが管理できていれば良いので、残存する脆弱性を「管理」で来ていればよい
  - ✓ 故に、脆弱性「対応」ではなく、脆弱性「管理」



全てに対応できるわけではない

＝ 事業に影響のある”可能性が高い”ものを排除することで、事業リスクを減らす。

2. 企業における標準的な脆弱性管理

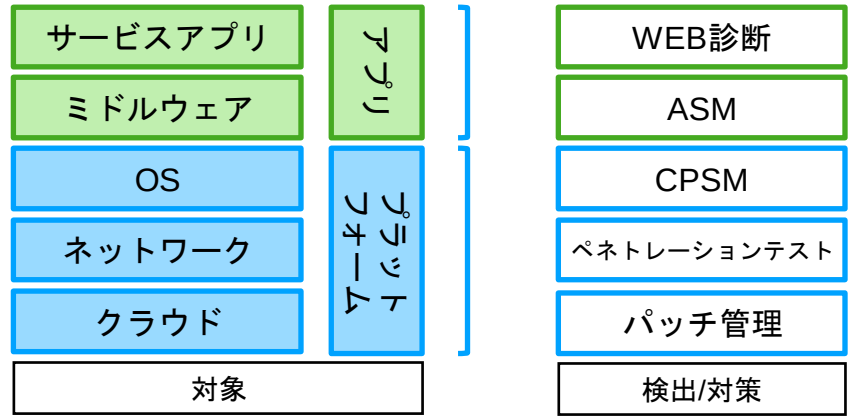
企業において、脆弱性管理として「対応すべき脆弱性」のみを選択して対応しています。

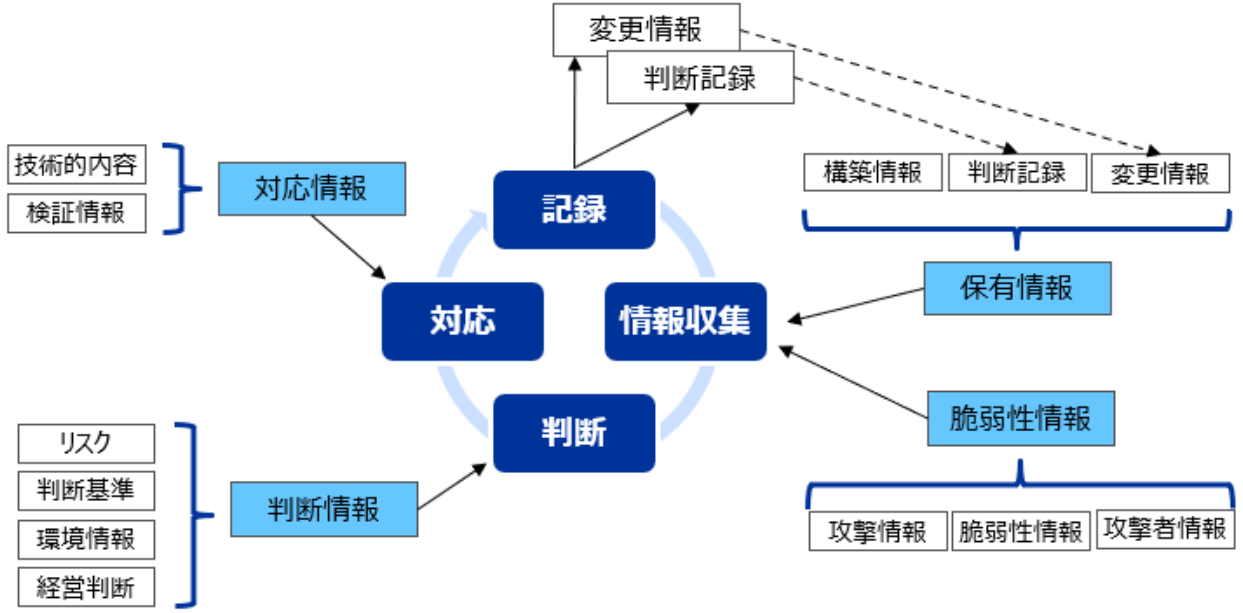
■ 脆弱性をどのように認識するのか

- 対象から
  - ✓ ペネトレーションテスト、WEB診断、プラットフォーム診断
- 方法から
  - ✓ アクティブに、パッシブに

■ どのように「選択」するのか

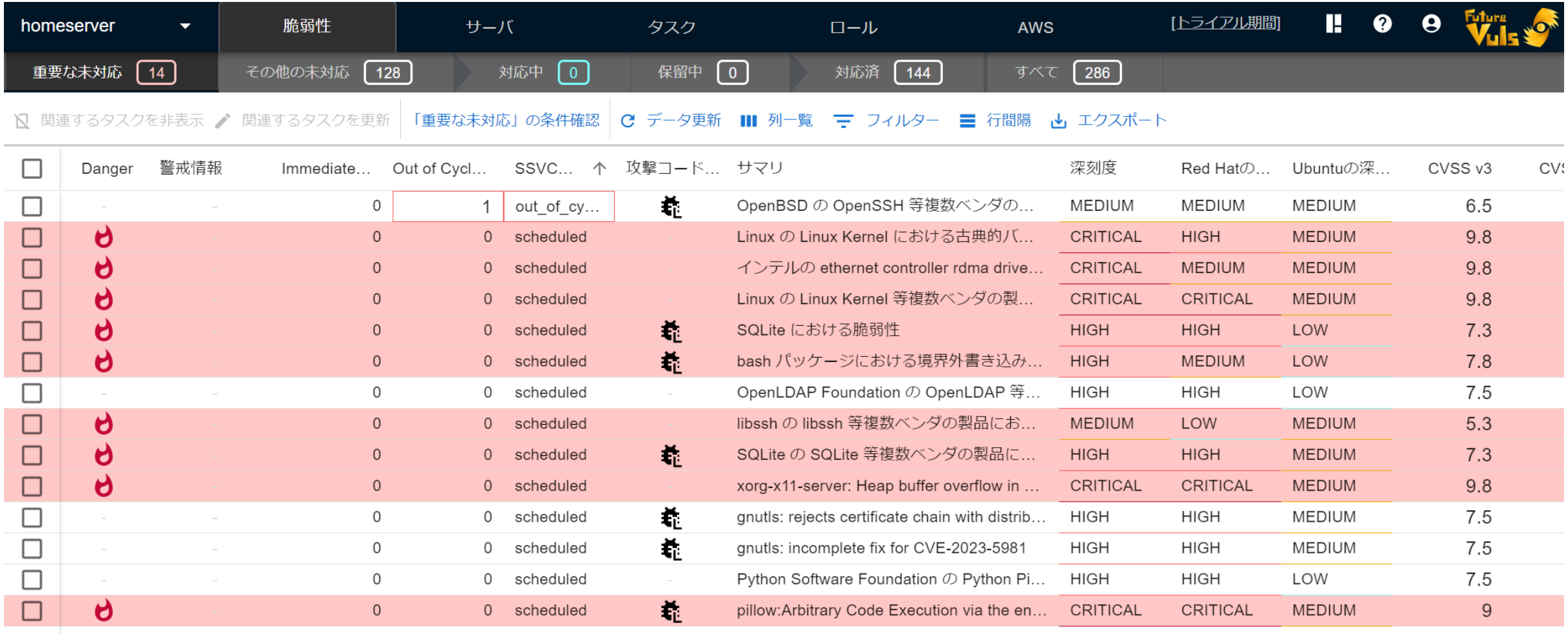
- CVSS BaseScoreやその他の指標を用いて、基準値のポリシーを用いて判断
  ＝トリアージ





TLP:GREEN

脆弱性管理ツールで、脆弱性を一元管理することも多いです。



Danger	警戒情報	Immediate…	Out of Cycl…	SSVC…	攻撃コード…	サマリ	深刻度	Red Hatの…	Ubuntuの深…	CVSS v3	CVS
-	-	0	1	out_of_cy…		OpenBSD の OpenSSH 等複数ベンダの…	MEDIUM	MEDIUM	MEDIUM	6.5	
	-	0	0	scheduled	-	Linux の Linux Kernel における古典的バ…	CRITICAL	HIGH	MEDIUM	9.8	
	-	0	0	scheduled	-	インテルの ethernet controller rdma drive…	CRITICAL	MEDIUM	MEDIUM	9.8	
	-	0	0	scheduled	-	Linux の Linux Kernel 等複数ベンダの製…	CRITICAL	CRITICAL	MEDIUM	9.8	
	-	0	0	scheduled		SQLite における脆弱性	HIGH	HIGH	LOW	7.3	
	-	0	0	scheduled		bash パッケージにおける境界外書き込み…	HIGH	MEDIUM	LOW	7.8	
-	-	0	0	scheduled	-	OpenLDAP Foundation の OpenLDAP 等…	HIGH	HIGH	LOW	7.5	
	-	0	0	scheduled	-	libssh の libssh 等複数ベンダの製品にお…	MEDIUM	LOW	MEDIUM	5.3	
	-	0	0	scheduled		SQLite の SQLite 等複数ベンダの製品に…	HIGH	HIGH	MEDIUM	7.3	
	-	0	0	scheduled	-	xorg-x11-server: Heap buffer overflow in …	CRITICAL	CRITICAL	MEDIUM	9.8	
-	-	0	0	scheduled		gnutls: rejects certificate chain with distrib…	HIGH	HIGH	MEDIUM	7.5	
-	-	0	0	scheduled		gnutls: incomplete fix for CVE-2023-5981	HIGH	HIGH	MEDIUM	7.5	
-	-	0	0	scheduled	-	Python Software Foundation の Python Pi…	HIGH	HIGH	LOW	7.5	
	-	0	0	scheduled		pillow:Arbitrary Code Execution via the en…	CRITICAL	CRITICAL	MEDIUM	9	

TLP:GREEN

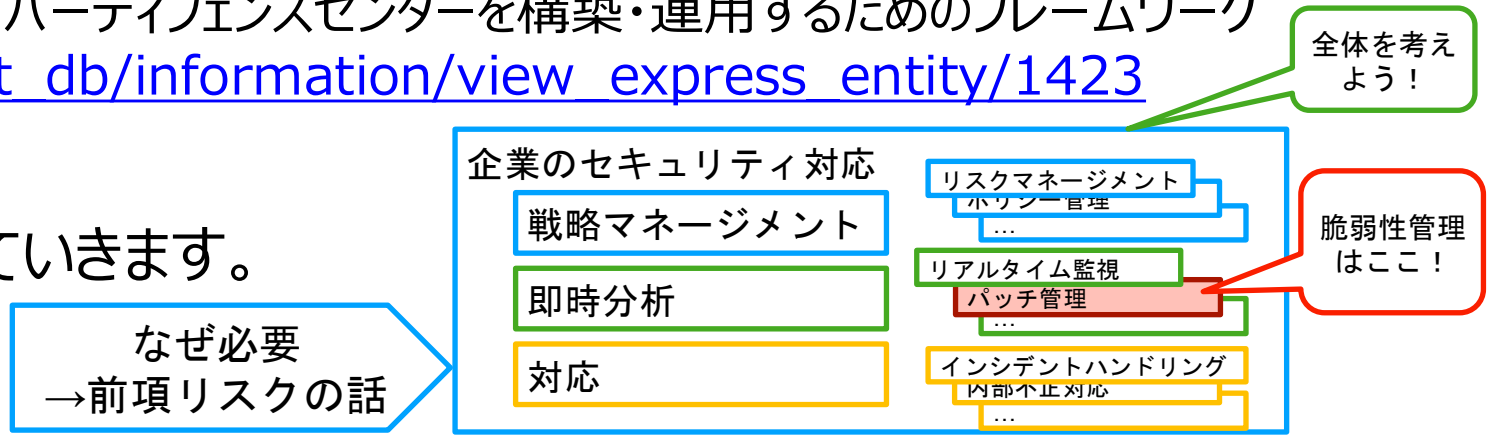
3. 企業におけるセキュリティ対応組織と、脆弱性管理の位置づけ

脆弱性管理は、企業全体のセキュリティ対応活動の中の一つの手段でしかありません。
企業が行うべきセキュリティ対応の全体像から、脆弱性管理の位置づけを確認します。

企業が行うべきセキュリティ対応は、以下のような資料が参考になります。

- ISOG-J:セキュリティ対応組織の教科書
  - https://isog-j.org/output/2023/Textbook_soc-csirt_v3.html
- ITU-T:X.1060 Framework for the creation and operation of a cyber centre
  - https://www.itu.int/rec/T-REC-X.1060-202106-I
  - 日本語版に相当するものは TTC：サイバーディフェンスセンターを構築・運用するためのフレームワーク https://www.ttc.or.jp/document_db/information/view_express_entity/1423

今回は ITU-T X.1060 を中心にみていきます。



TLP:GREEN

X.1060とは

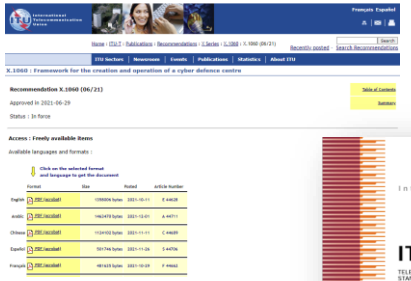
■ ITU-T

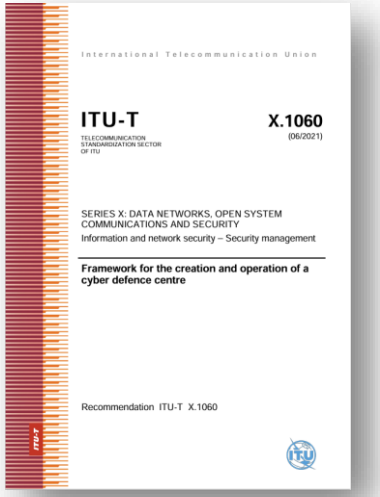
- 国際連合の専門機関の一つで、国際電気通信連合（ITU:International Telecommunication Union）に存在する、電気通信に関する部門。国際標準の策定などを担っている。

■ X.1060

- 上記ITU-Tの勧告として公開された、セキュリティ対応を行う組織（CDC：Cyber Defense Centre）を構築するためのフレームワーク

世界標準で使える、CDCの共通言語、という認識でよいと思います。





参考：

- JPCERT/CC Eyes: ITU-T X.1060サイバーディフェンスセンターについてのワークショップをアフリカで開催
  - ✓ https://blogs.jpcert.or.jp/ja/2023/03/CDCWorkshop.html
- TTC標準草案
  - ✓ https://www.ttc.or.jp/application/files/4416/3850/7173/2021_3Q_01.pdf

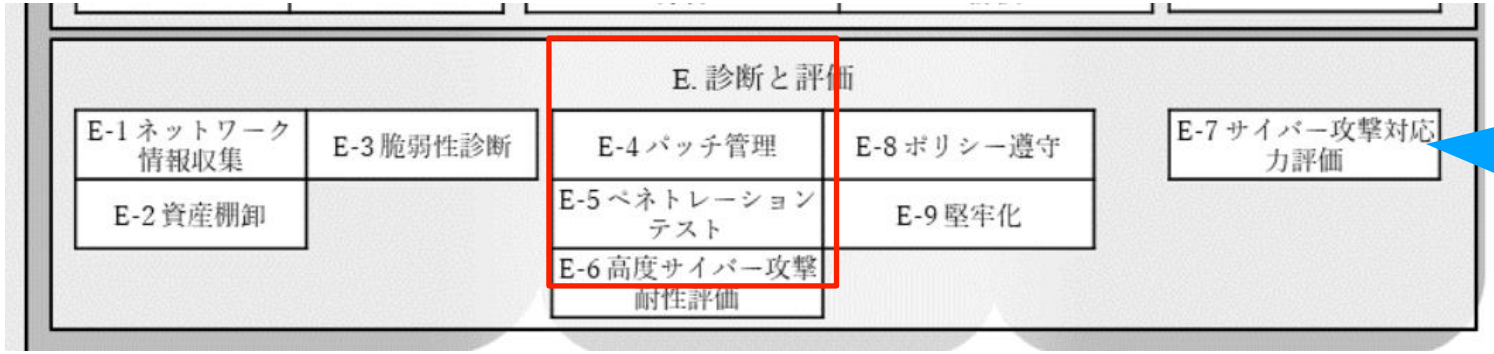
TLP:GREEN

X.1060（日本語化されたJT-X1060）の肝となる部分は、おおよそ以下の図となります。

■ CDCサービス

- CDCとして実装するべきサービス
- カテゴリーごとに、サービスリストがある

今回の脆弱性管理は、E.パッチ適用、を中心にみてみます。



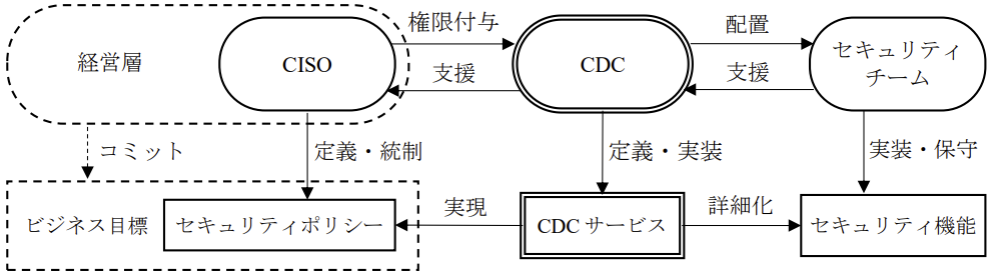


図 1　CDC の運営における関係者とその役割

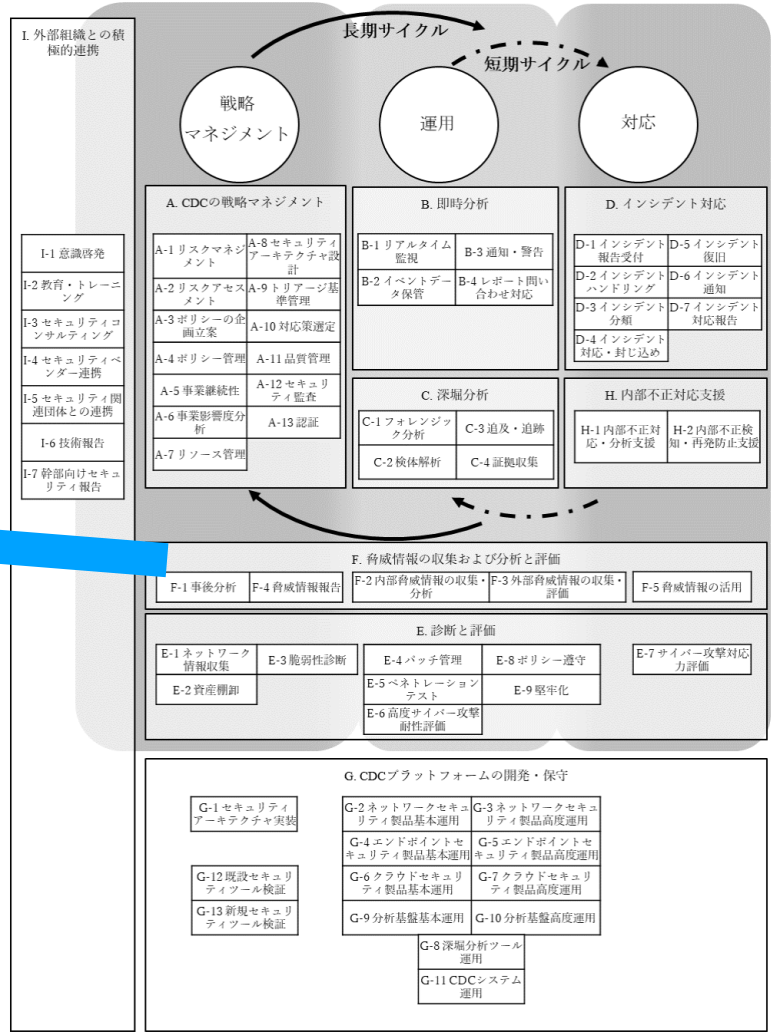


図 8　CDC サービスカテゴリー

説明画像

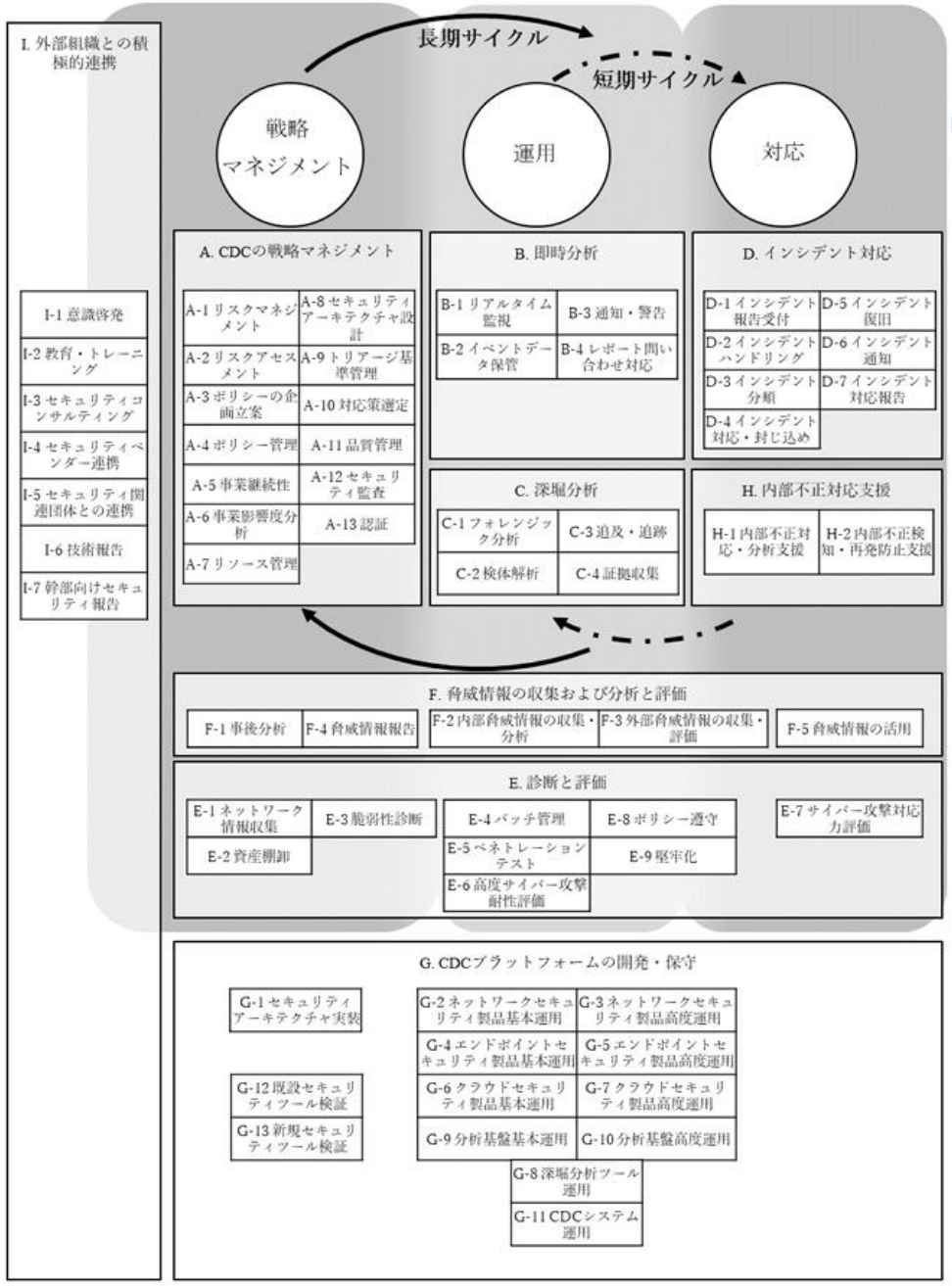


図 8　CDC サービスカテゴリー

4. 脆弱性管理を、X.1060で考える

脆弱性管理を、X.1060と併せて考え、
組織の機能として何が必要なのかを考えて
みます。

- ■ 分類
  - ➢ 直接影響のある機能
  - ➢ 間接的に影響のある機能
    - ✓ 直接影響がある物に影響
    - ✓ 組織全体に影響
- ■ 何を検討するのか
  - ➢ 誰が、どのタイミングで、どの精度で実施するのか
  - ➢ 必要か/不要か、アウトソースか/インソースか

初の試みなので、もう少し検討したほうがいいかもしれません。
これにより、SOC/CSIRTの機能改善のヒントになるかもしれません。

…ならないかもしれません。。

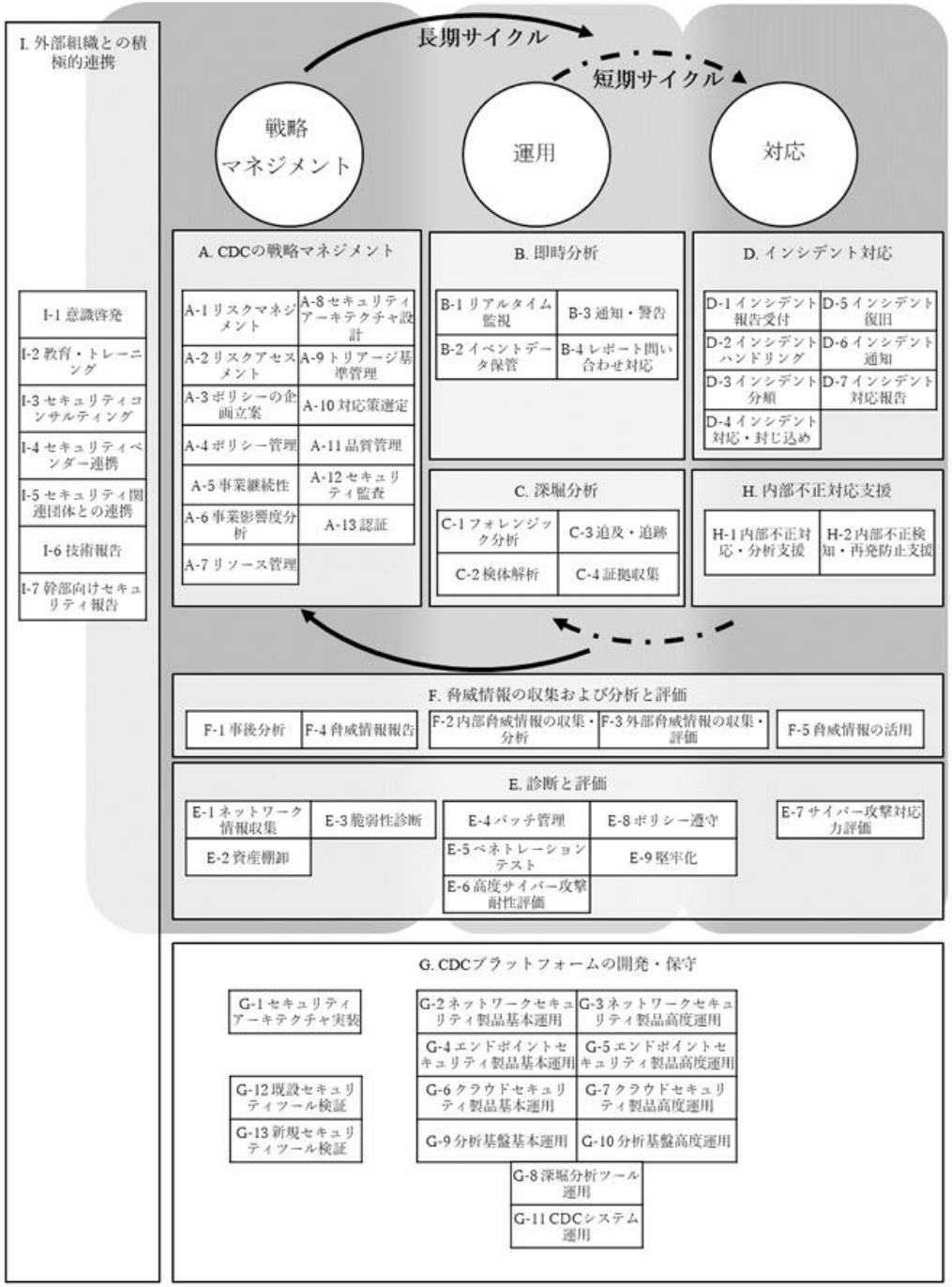
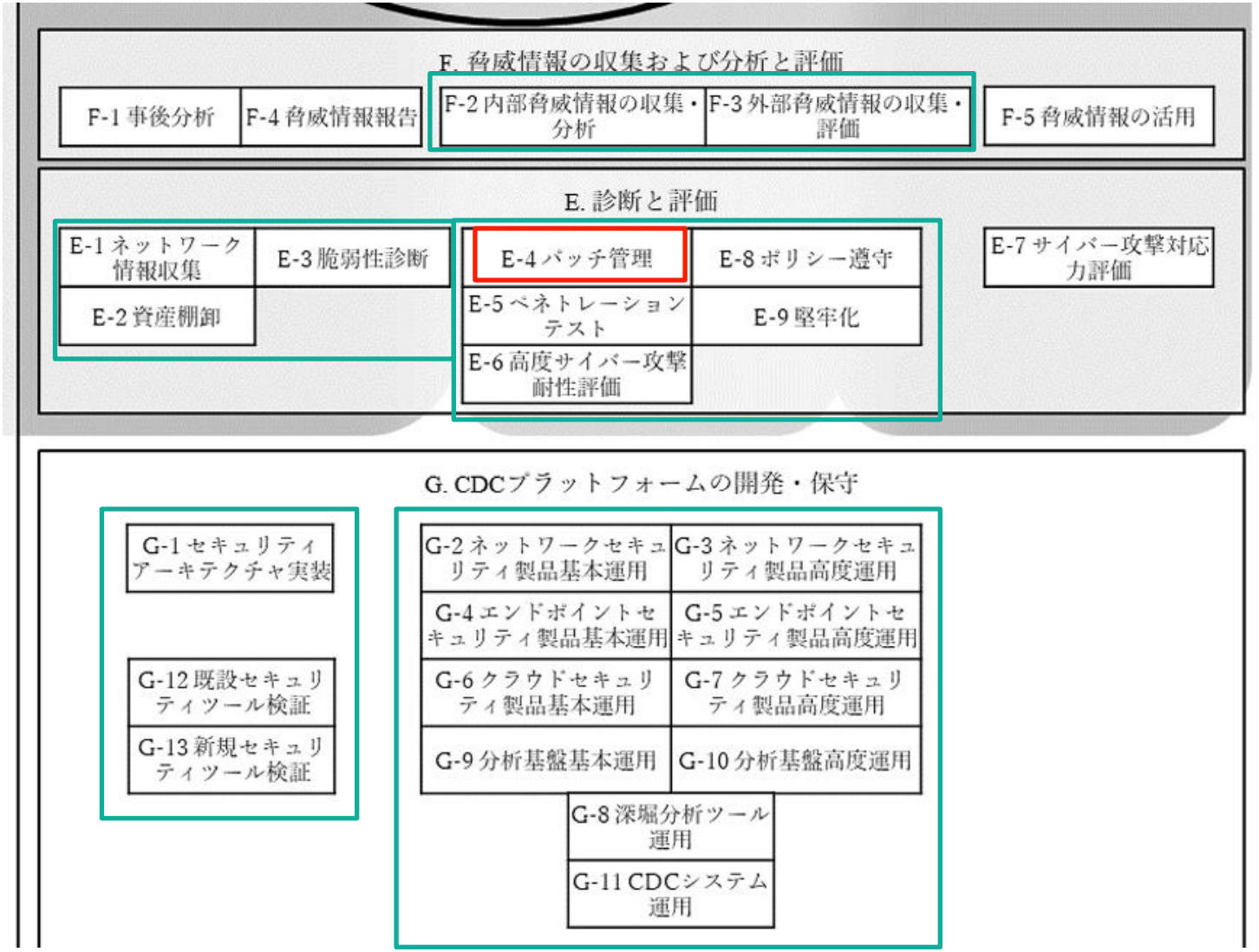


図 8　CDC サービスカテゴリー

TLP:GREEN

■ 直接影響のある機能

- ➢ F. 脅威情報の収集及び分析と評価
  - ✓ 発見した脆弱性についての詳細
  - ✓ 脆弱性があるという情報
- ➢ E. 診断と評価
  - ✓ 脆弱性を認識するための活動
    - ◆ 診断、評価
  - ✓ 脆弱性管理
    - ◆ パッチ適用、堅牢化
- ➢ G CDCプラットフォームの開発・保守
  - ✓ ツール選定から実証
  - ✓ 脆弱性管理のプラットフォーム保守運用



4. 脆弱性管理を、X.1060で考える

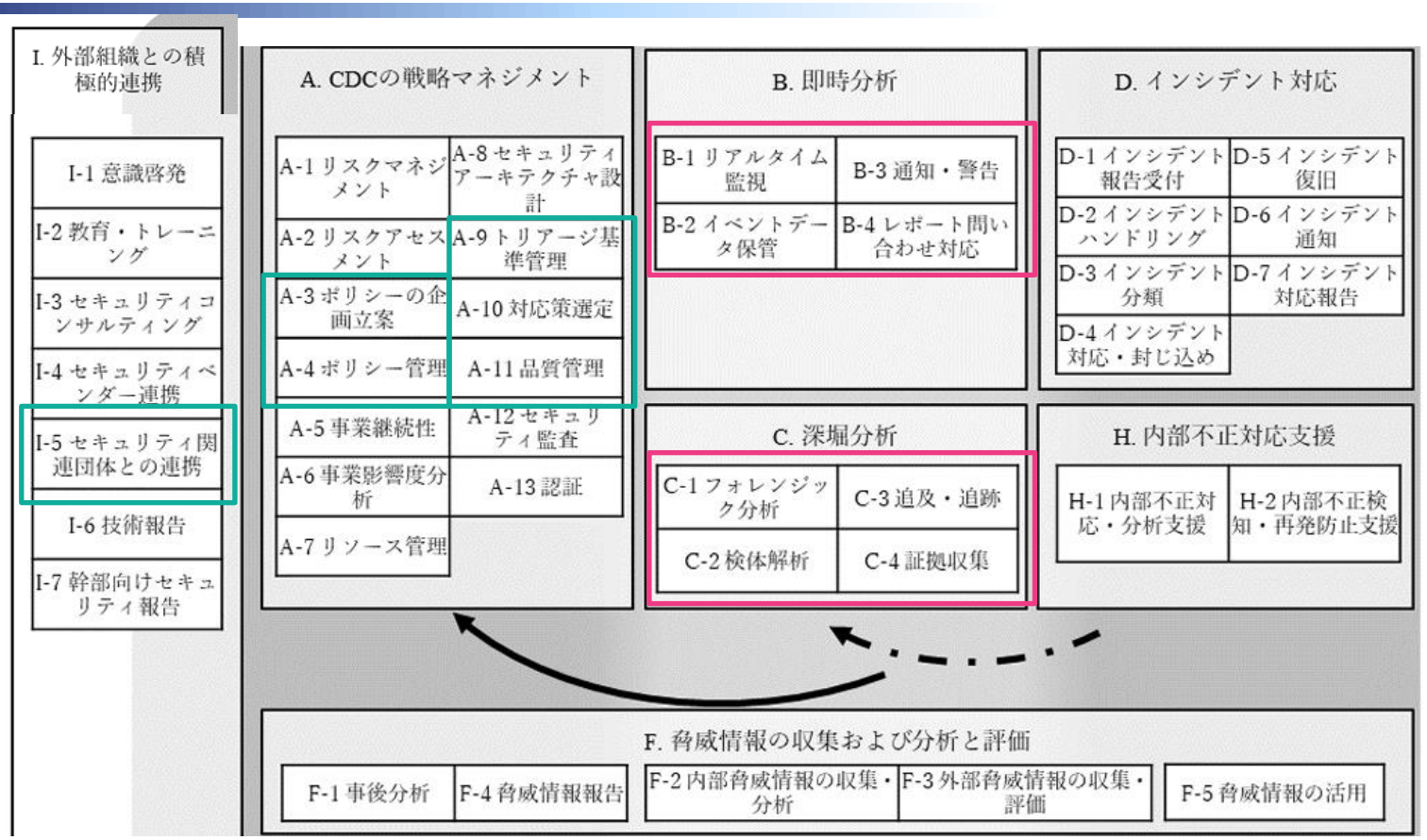
FUTURE

■ 間接的に影響のある機能

- A. CDCの戦略マネジメント
  - ✓ トリアージポリシーの策定
    - ◆ ポリシーの企画立案管理
  - ✓ 対応の標準化
    - ◆ 対応策選定、品質管理
- I. 外部組織との積極的連携
  - ✓ 脆弱性情報などの情報源として
    - ◆ セキュリティ関連団体との連携

■ 既知の攻撃の認識

- B. 即時分析
  - ✓ 監視や保管ログでの攻撃有無の確認
- C. 深堀分析
  - ✓ 上記で得られた可能性を、より詳細に確認



TLP:GREEN

6. まとめ

FUTURE

- 企業活動として、脆弱性対応は必要
- 脆弱性対応は、組織のCDCの提供する機能の一つであり、全体像を忘れないでね
  - 何を目的に脆弱性対応をしているのか、を忘れずにいるともう少し楽に判断できるかもしれません
- その為、脆弱性対応の為には組織として、追加の機能を実装する必要があるかもしれない
  - 必要な機能で、弱い/不足している部分は無いか。アウトソースで実現するのも有効
  - そこら辺の判断等は、ISOG-J セキュリティ対応組織の教科書 を参考にする

to. 学生の方

- WEB診断やペネトレーションなどの「技術」が、実際の仕事や社会ではどこで使われ、どのように組織のセキュリティに寄与しているかという全体像を考えると、やりたいことや面白いことを見つけられるかもしれません。

第一部、完

バズった(?)ので告知

リモート側には%d人も居るので、
バズったと言って過言ではない！

02月-03月18日まではサイバーセキュリティ月間の為、様々なイベントがあります。

- 2024-02-09（金曜）（現地開催）
  - 出張版 脆弱性対応勉強会 #05（名古屋）
    - ✓ https://zeijyakuseitaioukenkyukai.connpass.com/event/306261/
    - ✓ 下記OWASP758Dayの前日イベントとして、適当に私がお話する会
      - ◆ OWASP Nagoyaのご協力により、市民活動推進センターをお借りします
- 2024-02-10（土曜）（現地開催）
  - OWASP Nagoya Chapterミーティング第33回 / OWASP 758 Day 2024
    - ✓ https://owaspnagoya.connpass.com/event/305686/
    - ✓ 「未知の情報セキュリティ脅威に備えるために」がテーマ
      - ◆ にゃん☆たく氏と私が講演します
- 2024-02-16（金曜）（現地/リモート）
  - Vuls祭り#9
    - ✓ https://vuls-jp.connpass.com/event/304423
    - ✓ 脆弱性対応などをする人たちに有益な情報を共有する場
      - ◆ JPCERT/CC様、NTTデータグループ様、Vuls開発者などが講演します

TLP:GREEN

DS-201_政府情報システムにおけるセキュリティリスク分析ガイドライン

～ベースラインと事業被害の組み合わせアプローチ～

FUTURE

表２－１ セキュリティリスク分析手法の比較

リスク分析手法	長所	短所
ベースライン アプローチ	・決められた対策要件をチェックすることにより、作業の工数は大きくない。 ・既存の基準をもとにしているので、あるレベルの評価の目安としては利用できる。	・対策基準に対する適合レベルのチェックであり、自分のシステムの状況に沿ったリスク分析にはなっていない。 ・事業被害を起こさない裏づけには間接的にしかならない。 ・未実施の対策群があった場合、自分のシステムに沿った選択基準が得られない。
非形式的 アプローチ	・経験値を活用するので、属人的ではあるが工数は小さい。	・リスク分析にはなっていない。 ・起こりうる脅威、あるいは新たな脅威に対しての対応が困難である。 ・属人的であり、継続的なセキュリティレベルの向上は困難である。
詳細リスク分析	・自分のシステム自体に対する、正確なリスク分析が可能である。 ・一度実施すると、それをベースに継続的なセキュリティレベルの向上が可能となる。	・システムの規模や手法によっては、かなりの工数がかかることがある。 ・リスク分析の結果の評価に技量を要する。また、技量を持つ評価者のアサインが難し

5

リスク分析手法	長所	短所
	・セキュリティ投資の優先順位等、組織として戦略的に検討していくことができる。	い。※
組み合わせ アプローチ	・上記、各手法の長所の取り込みの可能性である。 ・上記、各手法の短所の改善の可能性がある。	・どう組み合わせるのか、それぞれのシステムや事業者によって異なってくるが、その指針は示されていない。

（出典）ＩＰＡ「制御システムのセキュリティリスク分析ガイド　第２版」より作成

※下線の箇所は、出典に対して本ガイドラインとして追記した箇所

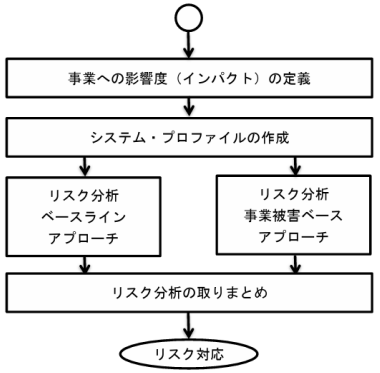


図２－１　本ガイドラインのリスク分析のプロセス

表２－２ リスク分析のプロセスの実施事項

8

プロセス	実施事項
事業への影響度（インパクト）の定義	事業の影響度を定義し、それぞれのリスク分析で共通した基準とする。
システム・プロファイルの作成	システムの利用形態や特性・特質を分析しプロファイルを作成する。作成したプロファイルはそれぞれのリスク分析で使用する。
リスクアセスメント	リスク特定、リスク分析及びリスク評価のプロセス全体。
ベースライン アプローチ	対象システムにあったセキュリティ管理策をチェックすることにより、確保すべきセキュリティレベルを達成するためのセキュリティ対策要件を分析する。
事業被害ベース アプローチ	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りリスク分析を実施する。
リスク分析の取りまとめ	２つのリスク分析の結果から、設定したセキュリティレベルを達成するセキュリティ対策を取りまとめる。

表３－２　事業リスクの種類

#	事業リスクの種類 Impacts per Category
①	利用者に不便、苦痛を与える、又は事業を所管する機関等が信頼を失う Potential impact of inconvenience, distress, or damage to standing or reputation:
②	利用者に金銭的被害を与える、機関等に賠償責任が生じるなど財務上の影響を与える Potential impact of financial loss:
③	機関等の活動計画や公共の利益に対して影響を与える Potential impact of harm to agency programs or public interests:
④	利用者の個人情報などの機微な情報が漏洩する Potential impact of unauthorized release of sensitive information:
⑤	利用者の身の安全に影響を与える Potential impact to personal safety:
⑥	法律に違反する The potential impact of civil or criminal violations is:

（出典）NIST SP 800-63-3「Digital Identity Guidelines（電子的認証に関するガイドライン）」より作成

表３－３．事業への影響度の定義

影響度	内容
高位 (High)	当該リスクの影響による損失が、組織の運営、組織の資産、又は個人に致命的又は壊滅的な悪影響を及ぼすと予想される

12

中位 (Moderate)	当該リスクの影響による損失が、組織の運営、組織の資産、又は個人に重大な悪影響を及ぼすと予想される
低位 (Low)	当該リスクの影響による損失が、組織の運営、組織の資産、又は個人に限定的な悪影響を及ぼすと予想される
非該当 (NA)	該当しない　または　当該リスクによる影響がないと予想される

（出典）「連邦政府の情報および情報システムに対するセキュリティ分類規格（連邦情報処理規格 FIPS 199）」より作成

表３－４　事業への影響度の定義

#	事業リスク Impacts per Category	影響度	影響度の定義
①	利用者に不便、苦痛を与える、又は事業を所管する機関等が信頼を失う	高位	深刻または重大かつ長期的な不便、苦痛、損害。この影響は、特に深刻な影響や多くの利用者に影響するレベル
		中位	相当かつ短期間ないしは限定的だが長期間の不便、苦痛、損害
		低位	限定的かつ短期間の不便、苦痛、損害
②	利用者に金銭的被害を与える、機関等に賠償責任が生じるなど財務上の影響を	高位	重大または致命的な経済的損失または賠償責任
		中位	相当な経済的損失または賠償責任
		低位	些細でとるに足らない経済的損失または賠償責任

13

#	事業リスク Impacts per Category	影響度	影響度の定義
	与える		
③	機関等の活動計画や公共の利益に対して影響を与える	高位	組織の運用や資産、公共の利益への致命的な悪影響（長期間の機能停止または深刻な損害）
		中位	組織の運用や資産、公共の利益への相当な悪影響（長期間の機能低下または著しい損害）
		低位	組織の運用や資産、公共の利益への限定的な悪影響（処理効率の低下または軽微な損害）
④	利用者の個人情報などの機微な情報が漏洩する	高位	情報の不当な開示が、組織活動、組織資産、または個人に致命的または壊滅的な悪影響を及ぼすことが予想されうる(FIPS 199)
		中位	情報の不当な開示が、組織活動、組織資産、または個人に重大な悪影響を及ぼすことが予想されうる(FIPS 199)
		低位	情報の不当な開示が、組織活動、組織資産、または個人に限定的な悪影響を及ぼすことが予想されうる(FIPS 199)
⑤	利用者の身の安全に影響を与える	高位	重傷または死亡のリスク
		中位	医療治療を必要とする怪我のリスク
		低位	治療を必要としない軽傷
⑥	法律に違反する	高位	特に重要とされている民事上又は刑事上の違反のリスク
		中位	法執行の対象となる可能性のある民事上又は刑事上の違反のリスク
		低位	法執行の対象とならない性質の民事上又は刑事上の違反のリスク

（出典）NIST SP 800-63-3「Digital Identity Guidelines（電子的認証に関するガイドライン）」より作成

TLP:GREEN

TLP:GREEN

Appendix

FUTURE

■ X.1060

- ITU-T : X.1060 Framework for the creation and operation of a cyber defence centre
  - ✓ https://www.itu.int/rec/T-REC-X.1060-202106-I
- TTC : JT-X1060 - サイバーディフェンスセンターを構築・運用するためのフレームワーク
  - ✓ https://www.ttc.or.jp/document_db/information/view_express_entity/1423

■ 日本の参考資料

- ISOG-J : セキュリティ対応組織の教科書 第3.1版（2023年10月）
  - ✓ https://isog-j.org/output/2023/Textbook_soc-csirt_v3.html
- 経済産業省 : サイバーセキュリティ経営ガイドライン
  - ✓ https://www.meti.go.jp/policy/netsecurity/mng_guide.html