How to make your SOC/CSIRT team more trustworthy?: ISOG-J Maturity Model and self-checking tool

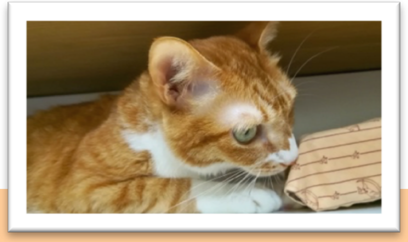
Yasunari Momoi momo@iij.ad.jp
Internet Initiative Japan Inc. / ISOG-J

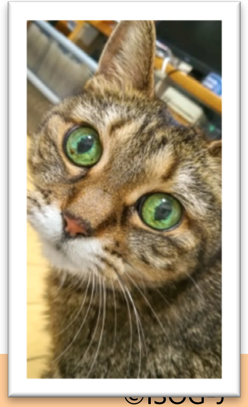
Agenda

- about me
- what is ISOG-J?
  - past ISOG-J activities
- building security team
  - documents and frameworks
- improving your security team using the viewpoint of operation
  - introduce some ISOG-J's documents and tools
  - some interest points of evaluating results
- Cybersecurity information sharing

About me

- momo: Yasunari Momoi
  - Internet Initiative Japan Inc., IIJ-SECT member
  - Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division
  - Facebook ymomoi Twitter @sbg
- Security, SOC/CSIRT, Software Developer, Server/Network Engineer
  - Develop some managed security services, operators dashboard, software tools for analyzing security logs, etc…
- Acting as a CSIRT member
  - FIRST, FIRST Japan Teams, NCA (Nippon CSIRT Association)
  - ISOG-J, ICT-ISAC
- Special Interest
  - local foods, Heavy Metal, cats





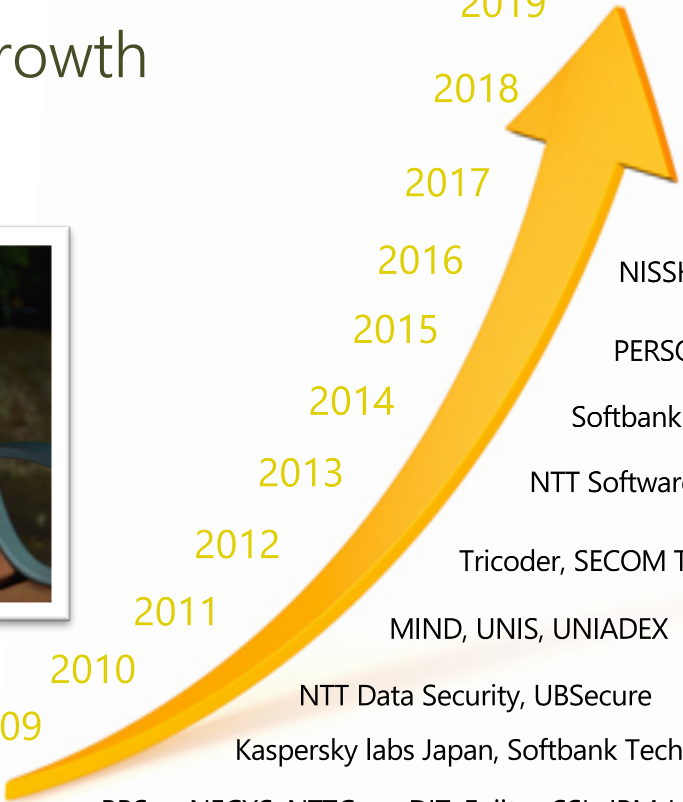
WHAT IS ISOG-J?

What is ISOG-J

- the Information Security Operation providers Group Japan
  - established 2008
  - ISOG-J is a professional community for security operation providers
  - a forum to share information about security operation and resolve common issues.
- ISOG-J's pronunciation is "ee-sog-jay"
  - the meaning is "Got to hurry, Japan!"
- http://isog-j.org/e/

ISOG-J member growth

50 membership organizations (2019-08)



2019

SST, FUJI SOFT, Kawaguchi Sekkei, DIGITAL HEARTS, Hitachi, Persol Process & Technology, Lepidum, Mitsubishi Electric

2018

GSX, NRI Secure, JRI, Marubeni OKI, Net One Systems, PFU, PwC, KOANKEISO, SecureWorks Japan

2017

2016

NISSHO ELECTRONICS, Recruit Technologies, KDL

2015

PERSOL Technology Staff, Cybozu

2014

Softbank mobile, NES

2013

NTT Software, SecureSoft

2012

Tricoder, SECOM Trust Systems, SCSK

2011

MIND, UNIS, UNIADEX

2010

NTT Data Security, UBSecure

2009

Kaspersky labs Japan, Softbank Technology

2008

BBSec, NECXS, NTTCom, DIT, Fujitsu SSL, IBM Japan

established

IIJ, IIJ Technology, NTT Data, NEC, NTT, Hitachi Systems, Fujitsu, MBSD, NRI Secure, LAC

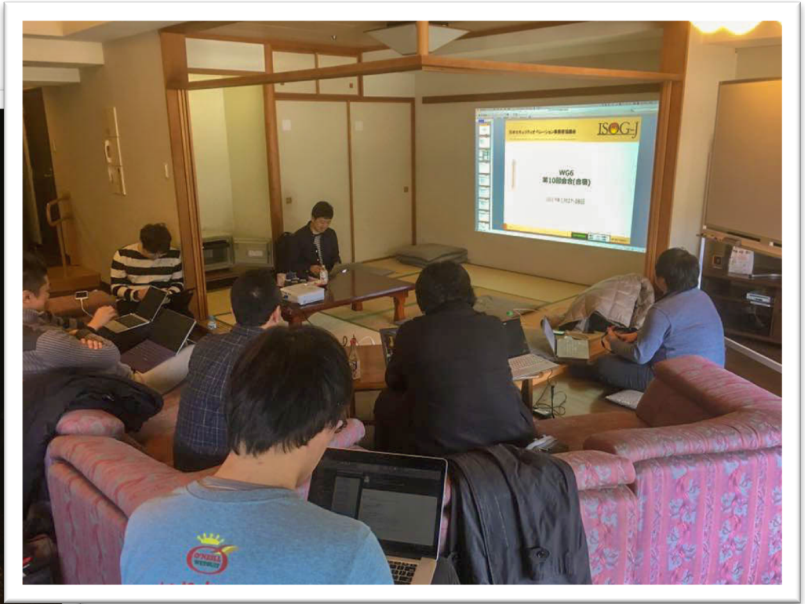
Activities of ISOG-J Working Groups (1)

- Security Operation Guideline WG (WG1)
  - collaborates with OWASP Japan Chapter
  - creates Pentesters' skill map and syllabus
  - Web app vulnerability assessment guideline / security requirement
- Security Operation Technology WG (WG2)
  - to promote friendship among the members
  - hold internal seminars of technical topics, then drink together
  - we call these timetable "sub part" and "main part"
    - It's ok to join only "main part"😎

KILKENNY
KILKENNY

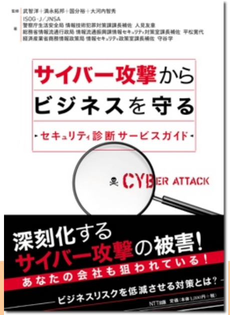
Activities of ISOG-J Working Groups (2)

- Security Operation-related Laws Research WG (WG3)
  - research the laws and systems related to the SOC business
  - Handy Compendium of Information Security Laws in Japan
- Security Operation Recognition and Propagation WG (WG4)
  - to improve of the recognition of the security operations
  - event and publicity planning
- Security Operations Chaos WG (WG Rock!(6))
  - discussing any issues on security operation chaos
  - taking an acronym: SOC


ISOG-J
WG6
第10回会合(合宿)

Past ISOG-J publications (1)

- 2008 Service map of Managed Security Services (listed up and categorized)
- 2009 Guidelines to choose Managed Security Service
  - How to choose the Managed Security Service that fits your organization
- 2011 Survey report on IPv6 readiness of security equipment
- 2011 Handy Compendium of Information Security Laws in Japan
  - Revised in 2012 and 2015
- 2013 How to defend your business – a guide for security assessment service (book)



監修 武智洋＋満永拓邦＋国分裕＋大河内智秀

著 ISOG-J／JNSA
警察庁生活安全局 情報技術犯罪対策課課長補佐 人見友章
総務省情報流通行政局 情報流通振興課情報セキュリティ対策室課長補佐 平松寛代
経済産業省商務情報政策局 情報セキュリティ政策室課長補佐 守谷学

サイバー攻撃から
ビジネスを守る
・セキュリティ診断サービスガイド・

深刻化するサイバー攻撃の被害！
あなたの会社も狙われている！
ビジネスリスクを低減させる対策とは？

NTT出版 定価（本体1,800円＋税）

Past ISOG-J publications (2)

- 2014 Skillmap and syllabus of web pentesters (with OWASP Japan Pentester Skillmap Project JP)
- 2016,2017 Skillmap and syllabus of platform pentesters / Guideline for web application penetration testing (with OWASP Japan Pentester Skillmap Project JP)
- 2018,2019 Web app vulnerability assessment guideline / security requirements (with OWASP Japan Pentester Skillmap Project JP)

But these publications are…

- All written in Japanese
- Because most SOC/CSIRT members in Japan prefer Japanese readings

BUILDING SECURITY RESPONSE TEAM

ISOG-J is...

- A community for security operation providers
- Each company provides services for customers

How to build your security response team?

- Many good documents already available
  - textbooks, guides, frameworks...
- Documents that have a good reputation in Japan
  - CSIRT Services Framework (FIRST)
  - CSIRT Guide, CSIRT for Management Layer (JPCERT/CC)
  - What is CSIRT?, CSIRT Human Resource (NCA)
  - Cybersecurity Framework (NIST)
  - SIM3 (Open CSIRT Foundation)
  - Cybersecurity Management Guidelines (METI)

Why difficult?

- Security response organization/team has various forms
- All situations vary from organization to organization
  - scale, structure, staff composition, budgets
  - industry, a type of business
  - existing services, professionals
- What is the organization aiming for in the future?

Classify and organize them from the viewpoint of operations

- We broke down security operations into services
  - categorized them into roles afterward
- Summarize using these roles and services
  - flows during security response
  - interactions between roles or services

- Textbook for Security Response Organization (SOC/CSIRT)
  - …but only in Japanese, sorry
- Handbook for Security Response Organization (SOC/CSIRT)
  - the summarized version of the textbook

Past ISOG-J publications related to SOC/CSIRT

- 2015 Self-check sheet: prepare for information security incident response (for beginners)
  - Easy-to-read, very short summary
- 2016 Overview of SOC member roles and required skills
- 2016 Textbook for Security Response Organization (SOC/CSIRT) ver.1.0
- 2017 Textbook for Security Response Organization (SOC/CSIRT) ver.2.0 (with self-check sheet)
- 2017,2018 6Ws on cybersecurity information sharing for enhancing SOC/CSIRT ver.1.0
  - “6Ws” is “5W1H” in Japanese
- 2018,2019 Handbook for Security Response Organization (SOC/CSIRT)

HANDBOOK FOR SECURITY RESPONSE ORGANIZATION (SOC/CSIRT)

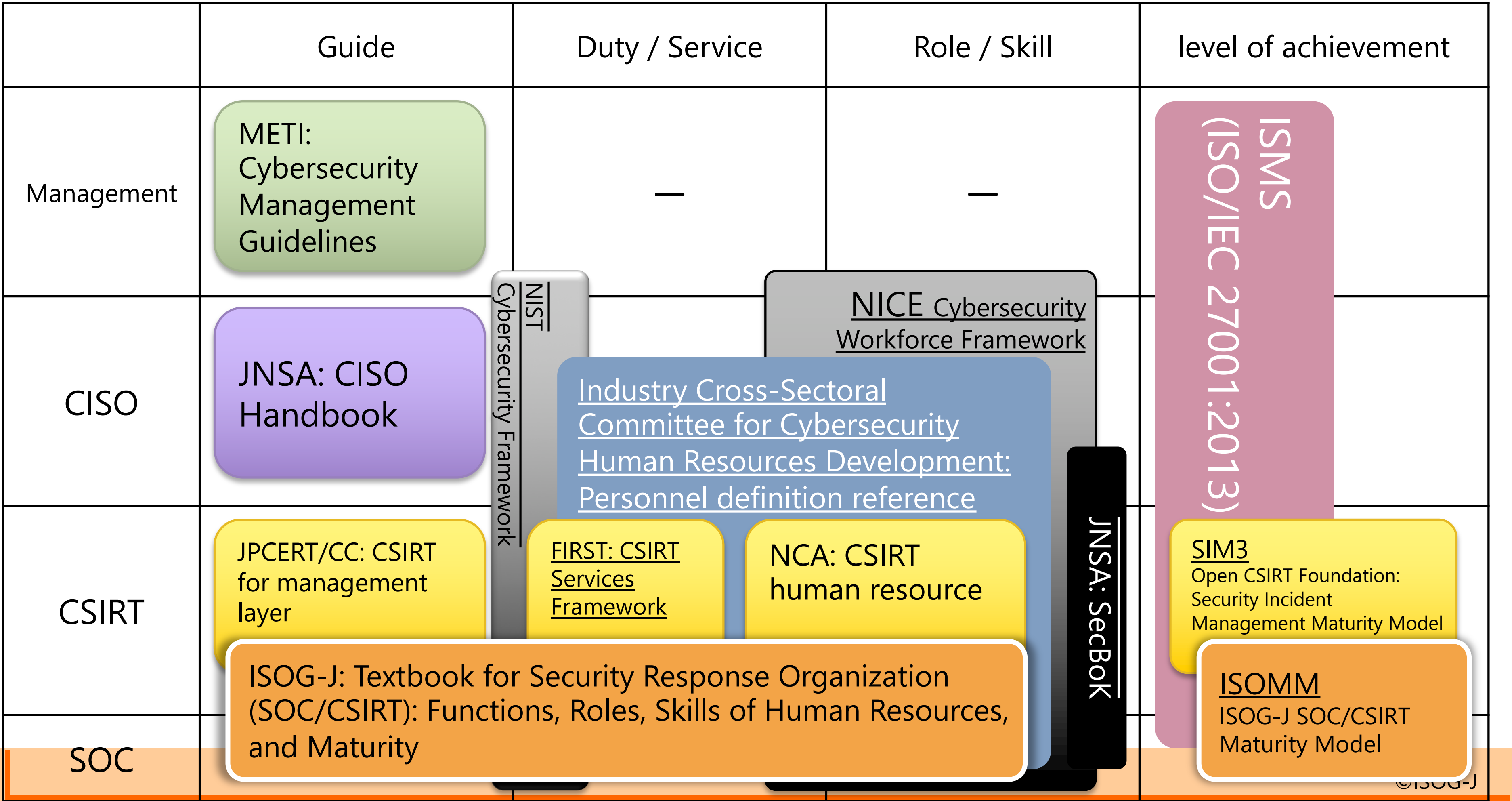
What is "Security Response"?

Security Response…

- Even the same thing looks different from each others viewpoint
  - if you are the Owner, CSO/CISO, Division director, Manager, Security team leader, SOC operator, etc.

↓

Understand that thinking is different depending on their position; refer to the appropriate guidelines for each



Guide

Duty / Service

Role / Skill

level of achievement

Management

CISO

CSIRT

SOC

METI: Cybersecurity Management Guidelines

—

—

ISMS (ISO/IEC 27001:2013)

NIST Cybersecurity Framework

NICE Cybersecurity Workforce Framework

JNSA: CISO Handbook

Industry Cross-Sectoral Committee for Cybersecurity Human Resources Development: Personnel definition reference

JNSA: SecBoK

JPCERT/CC: CSIRT for management layer

FIRST: CSIRT Services Framework

NCA: CSIRT human resource

SIM3 Open CSIRT Foundation: Security Incident Management Maturity Model

ISOG-J: Textbook for Security Response Organization (SOC/CSIRT): Functions, Roles, Skills of Human Resources, and Maturity

ISOMM ISOG-J SOC/CSIRT Maturity Model

Security Response Organization includes

SOC (Security Operation Center) + **CSIRT**

Which team provides which security roles depend on each organization

We categorized the operations of security response organizations in detail and defined

9 roles

and

54 services

The **9 roles**

A) Managing Security Response Organization/Team

B) Real-time Analysis

C) Deep Analysis

D) Incident Response

E) Assessment of the Achieved Security Level

F) Threat Information Collection, Analysis, and Evaluation

G) Systems Development and Operation

H) Supporting Organization Governance and Threats Response

I) Collaborating with Other Organizations

The **54 services**

A. Managing Security Response Organization/Team

A-1 Overall direction
A-2 Triage criteria management
A-3 Action policy management
A-4 Quality management
A-5 Measuring the effect of security responses
A-6 Resource management

B. Real-time Analysis

B-1 Basic real-time analysis
B-2 Advanced real-time analysis
B-3 Gathering information for triage
B-4 Reporting real-time analysis result
B-5 Answering inquiries on the report

C. Deep Analysis

C-1 Network forensics
C-2 Digital forensics
C-3 Malware sample analysis
C-4 Analysis of the whole attack
C-5 Preservation of evidence

D. Incident Response

D-1 Incident help desk
D-2 Incident management
D-3 Incident analysis
D-4 Remote operation
D-5 On-site operation
D-6 Internal collaboration
D-7 External collaboration
D-8 Incident response report

E. Assessment of the Achieved Security Level

E-1 Monitoring network information
E-2 Asset management
E-3 Vulnerability management and response
E-4 Automatic vulnerability assessment
E-5 Manual vulnerability assessment
E-6 Assessment of defense capability against APT attack
E-7 Assessment of response capability on cyber attack

F. Threat Information Collection, Analysis, and Evaluation

F-1 Internal threat intelligence collection and analysis
F-2 External threat intelligence collection and evaluation
F-3 Reporting collected threat intelligence
F-4 Threat intelligence utilization

G. Systems Development and Operation

G-1 Basic operation of network security devices
G-2 Advanced operation of network security devices
G-3 Basic operation of endpoint security products
G-4 Advanced operation of endpoint security products
G-5 Deep analysis tool operation
G-6 Basic operation of analysis platform
G-7 Advanced operation of analysis platform
G-8 Verifying existing security products and tools
G-9 Investigating and developing brand new security products and tools
G-10 Operates business systems

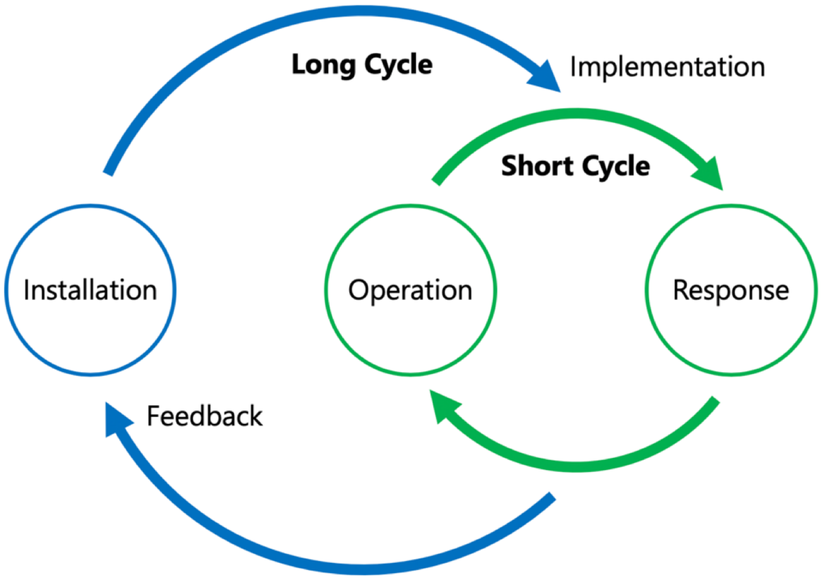
H. Supporting Organization Governance and Insider Threats Response

H-1 Collection and management of audit information for organization governance
H-2 Support for investigating and analyzing insider threats
H-3 Support for detecting and preventing insider threats

I. Collaborating with Other Organizations

I-1 Raising members' security awareness
I-2 Security training implementation and support for members
I-3 Acting as a security advisor for organization members
I-4 Human resource recruitment and development for security operation
I-5 Collaborating with security vendors
I-6 Collaborating with other security organizations

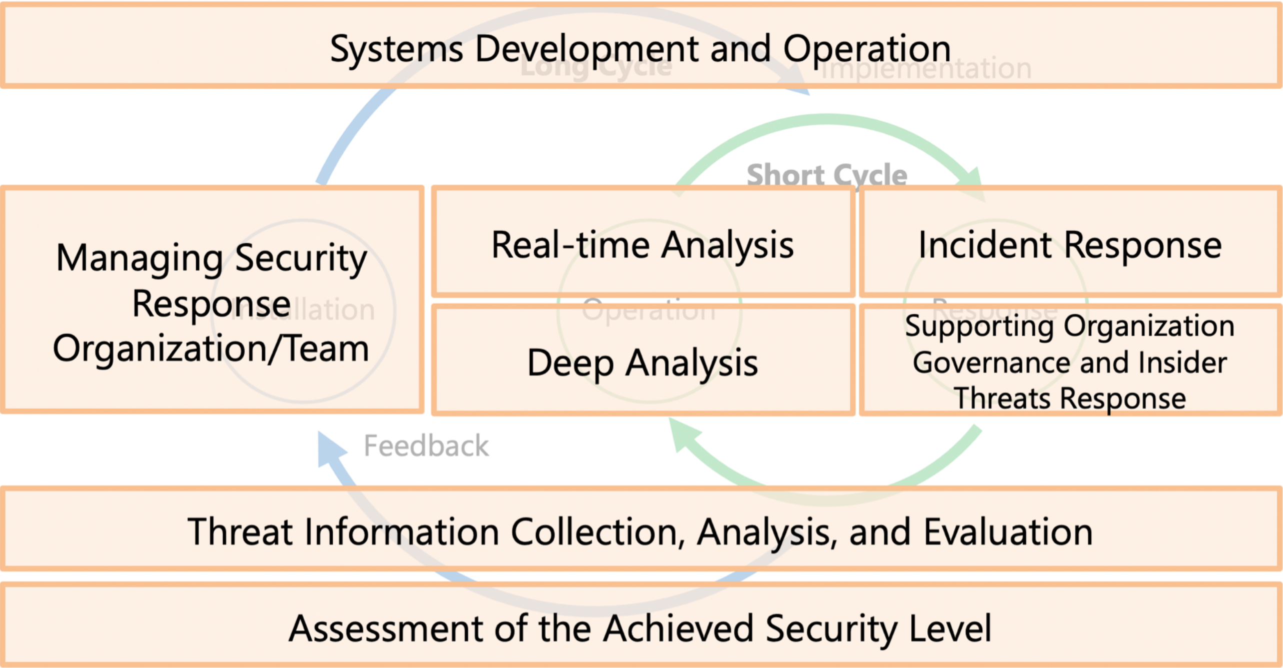
What is the security response?



Installation	Phase for considering and installing security policy and supporting system that are mandatory to operate security team
Operation	Phase for checking if the implemented system is working as intended and maintaining daily (normal) operation status to monitor and find potential incidents
Response	Phase for responding to incidents that are found internally or reported from external parties

ISOG-J *"Handbook for Security Response Organization (SOC/CSIRT)"*

What is the role during security response?



Systems Development and Operation

Managing Security Response Organization/Team

Real-time Analysis

Incident Response

Deep Analysis

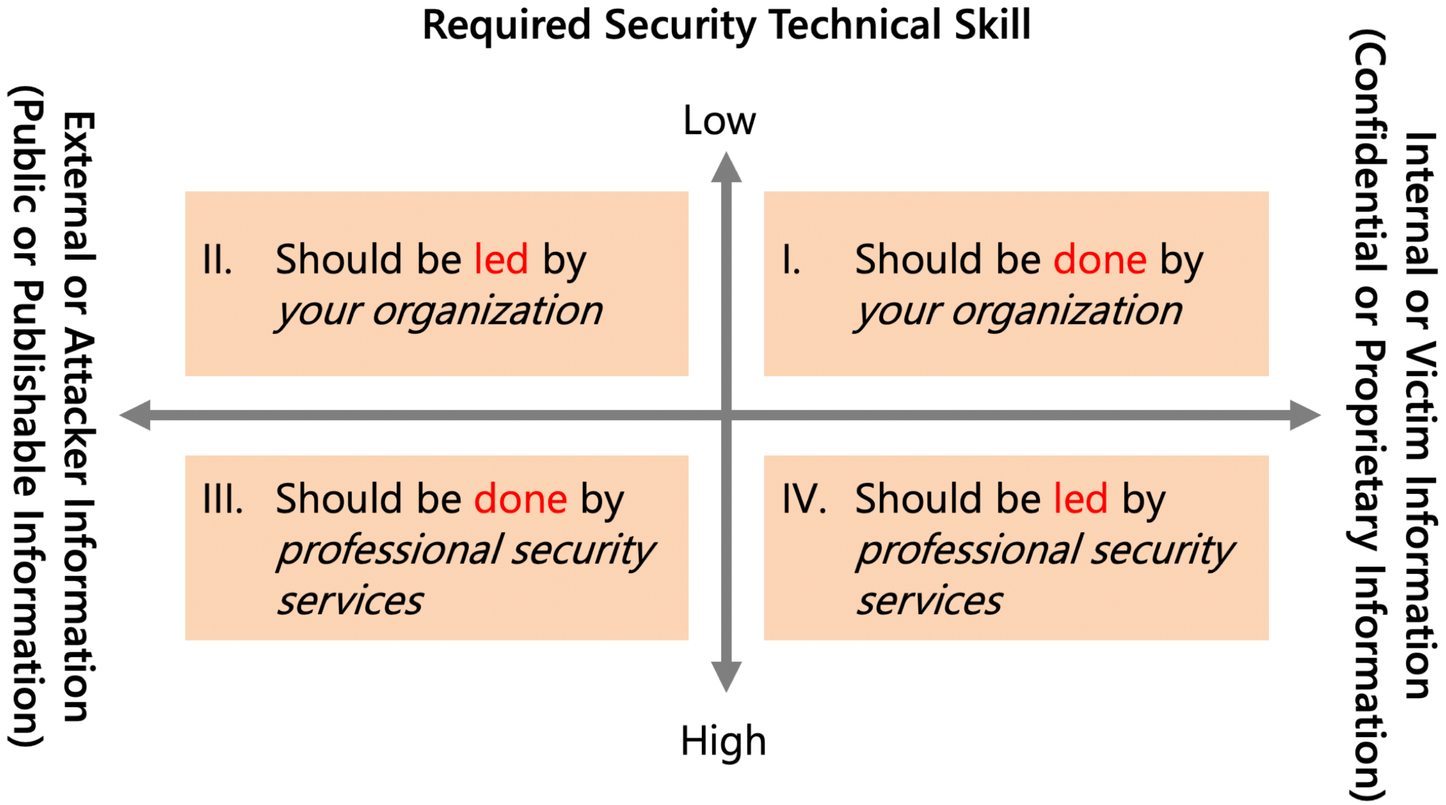
Supporting Organization Governance and Insider Threats Response

Threat Information Collection, Analysis, and Evaluation

Assessment of the Achieved Security Level

ISOG-J *"Handbook for Security Response Organization (SOC/CSIRT)"*

Security response organization services quadrant chart



Required Security Technical Skill

Low

High

External or Attacker Information
(Public or Publishable Information)

Internal or Victim Information
(Confidential or Proprietary Information)

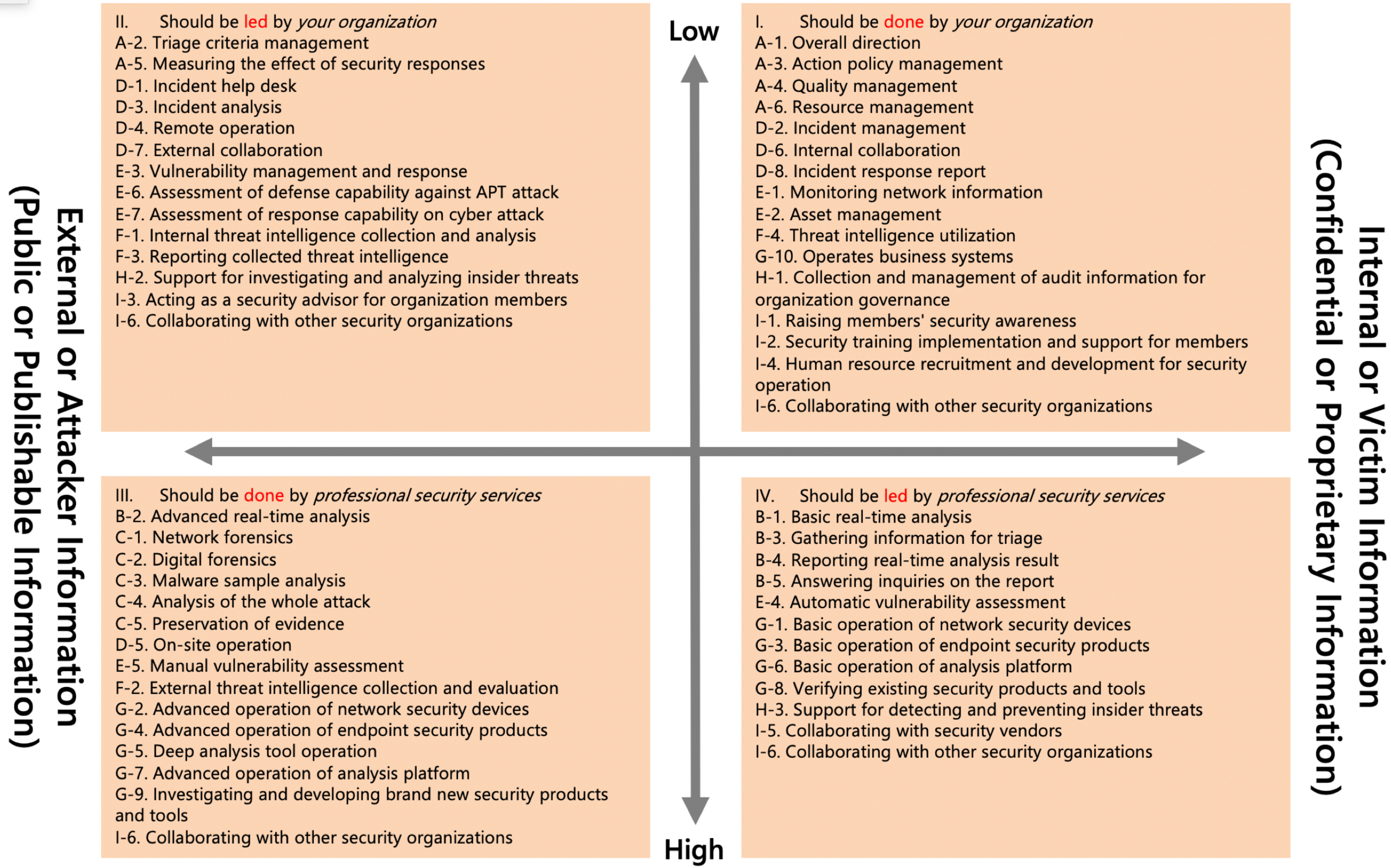
II. Should be led by *your organization*

I. Should be done by *your organization*

III. Should be done by *professional security services*

IV. Should be led by *professional security services*

Required Security Technical Skill


Low
High
External or Attacker Information
(Public or Publishable Information)
Internal or Victim Information
(Confidential or Proprietary Information)

II. Should be led by *your organization*
A-2. Triage criteria management
A-5. Measuring the effect of security responses
D-1. Incident help desk
D-3. Incident analysis
D-4. Remote operation
D-7. External collaboration
E-3. Vulnerability management and response
E-6. Assessment of defense capability against APT attack
E-7. Assessment of response capability on cyber attack
F-1. Internal threat intelligence collection and analysis
F-3. Reporting collected threat intelligence
H-2. Support for investigating and analyzing insider threats
I-3. Acting as a security advisor for organization members
I-6. Collaborating with other security organizations

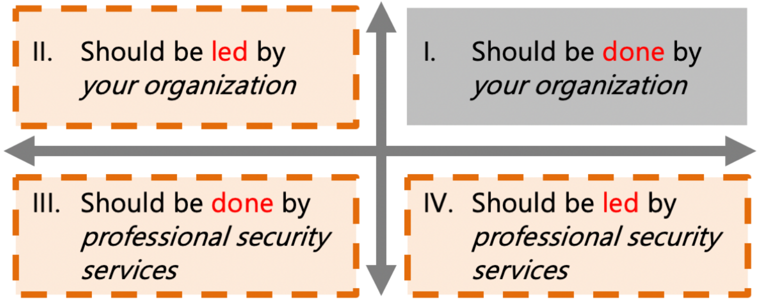
I. Should be done by *your organization*
A-1. Overall direction
A-3. Action policy management
A-4. Quality management
A-6. Resource management
D-2. Incident management
D-6. Internal collaboration
D-8. Incident response report
E-1. Monitoring network information
E-2. Asset management
F-4. Threat intelligence utilization
G-10. Operates business systems
H-1. Collection and management of audit information for organization governance
I-1. Raising members' security awareness
I-2. Security training implementation and support for members
I-4. Human resource recruitment and development for security operation
I-6. Collaborating with other security organizations

III. Should be done by *professional security services*
B-2. Advanced real-time analysis
C-1. Network forensics
C-2. Digital forensics
C-3. Malware sample analysis
C-4. Analysis of the whole attack
C-5. Preservation of evidence
D-5. On-site operation
E-5. Manual vulnerability assessment
F-2. External threat intelligence collection and evaluation
G-2. Advanced operation of network security devices
G-4. Advanced operation of endpoint security products
G-5. Deep analysis tool operation
G-7. Advanced operation of analysis platform
G-9. Investigating and developing brand new security products and tools
I-6. Collaborating with other security organizations

IV. Should be led by *professional security services*
B-1. Basic real-time analysis
B-3. Gathering information for triage
B-4. Reporting real-time analysis result
B-5. Answering inquiries on the report
E-4. Automatic vulnerability assessment
G-1. Basic operation of network security devices
G-3. Basic operation of endpoint security products
G-6. Basic operation of analysis platform
G-8. Verifying existing security products and tools
H-3. Support for detecting and preventing insider threats
I-5. Collaborating with security vendors
I-6. Collaborating with other security organizations

Insource or Outsource patterns

Minimum insource



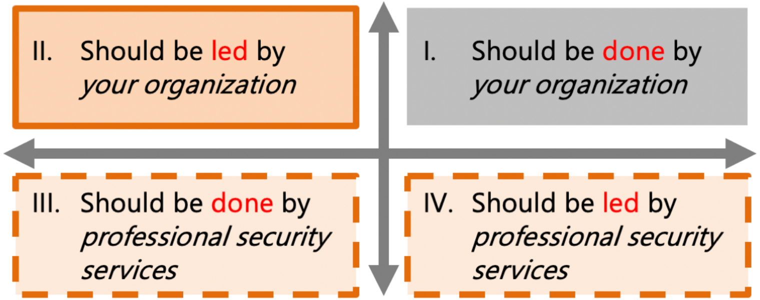
II. Should be led by *your organization*

I. Should be done by *your organization*

III. Should be done by *professional security services*

IV. Should be led by *professional security services*

Hybrid insource/outsource



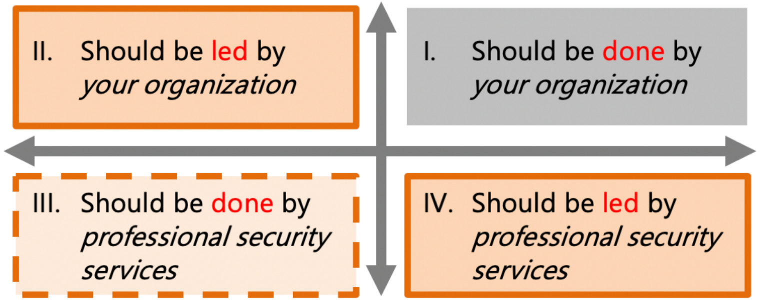
II. Should be led by *your organization*

I. Should be done by *your organization*

III. Should be done by *professional security services*

IV. Should be led by *professional security services*

Minimum outsource



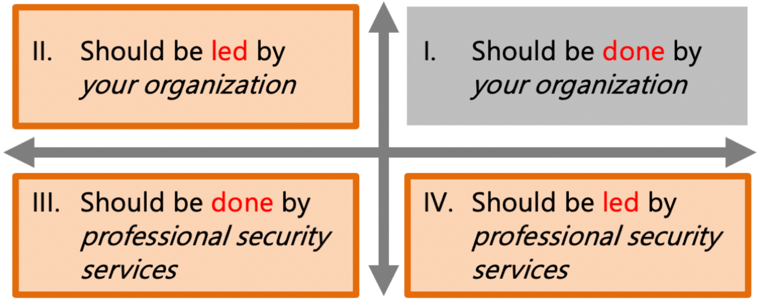
II. Should be led by *your organization*

I. Should be done by *your organization*

III. Should be done by *professional security services*

IV. Should be led by *professional security services*

Full insource



II. Should be led by *your organization*

I. Should be done by *your organization*

III. Should be done by *professional security services*

IV. Should be led by *professional security services*

Strength of Security Response Organization

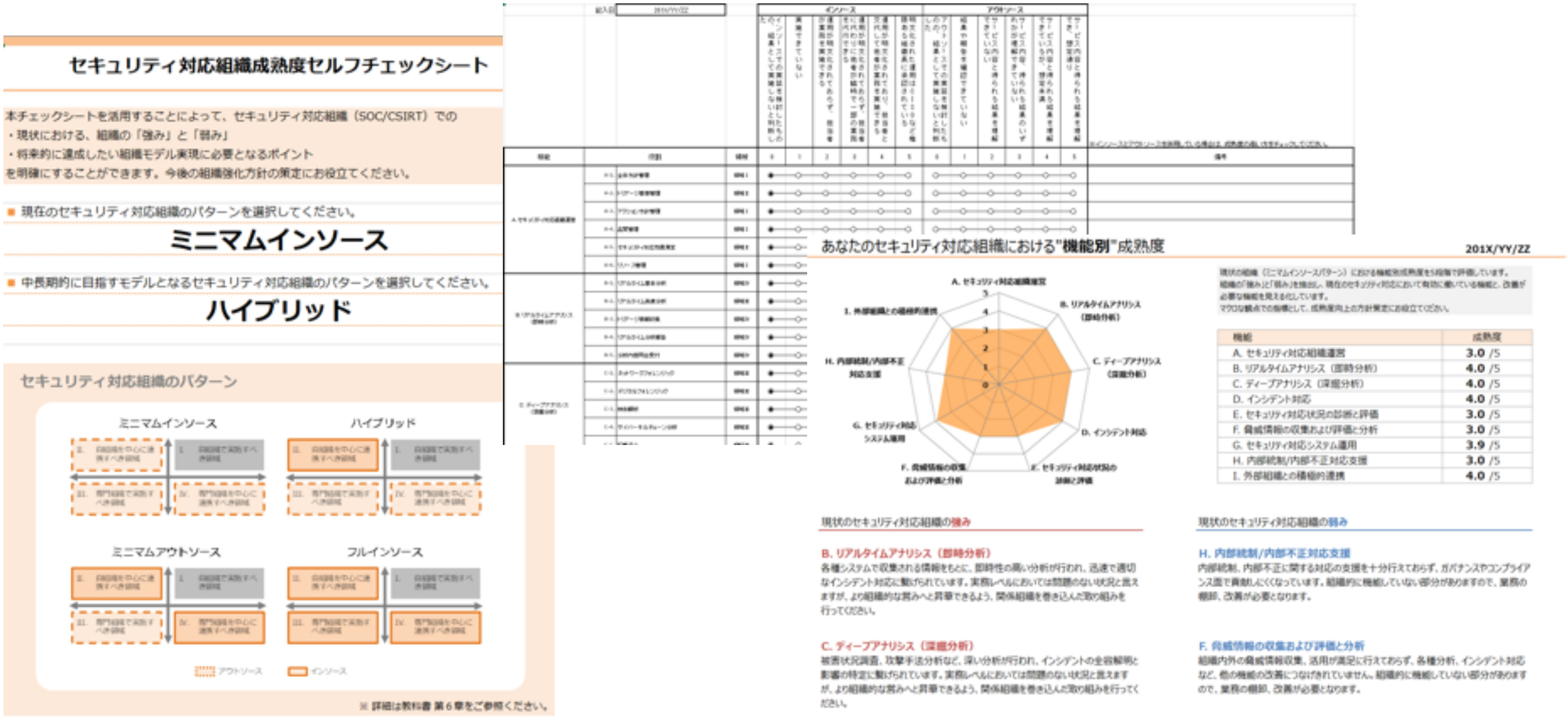
||

Whether each role can be performed continuously by the team

How to measure your security response organization?

Security Response Organization Maturity Level Self-check Sheet

ISOMM (ISOG-J SOC/CSIRT Maturity Model)



セキュリティ対応組織成熟度セルフチェックシート

本チェックシートを活用することによって、セキュリティ対応組織（SOC/CSIRT）での
・現状における、組織の「強み」と「弱み」
・将来的に達成したい組織モデル実現に必要となるポイント
を明確にすることができます。今後の組織強化方針の策定にお役立てください。

■ 現在のセキュリティ対応組織のパターンを選択してください。

ミニマムインソース

■ 中長期的に目指すモデルとなるセキュリティ対応組織のパターンを選択してください。

ハイブリッド

セキュリティ対応組織のパターン

ミニマムインソース
ハイブリッド
ミニマムアウトソース
フルインソース
I. 自組織で実施すべき領域
II. 自組織を中心に連携すべき領域
III. 専門組織で実施すべき領域
IV. 専門組織を中心に連携すべき領域
アウトソース
インソース

※ 詳細は教科書 第６章をご参照ください。

記入日
201X/YY/ZZ
インソース
アウトソース

あなたのセキュリティ対応組織における"機能別"成熟度

201X/YY/ZZ

A. セキュリティ対応組織運営
B. リアルタイムアナリシス（即時分析）
C. ディープアナリシス（深掘分析）
D. インシデント対応
E. セキュリティ対応状況の診断と評価
F. 脅威情報の収集および評価と分析
G. セキュリティ対応システム運用
H. 内部統制/内部不正対応支援
I. 外部組織との積極的連携
0
1
2
3
4
5

現状の組織（ミニマムインソースパターン）における機能別成熟度を5段階で評価しています。
組織の「強み」と「弱み」を抽出し、現在のセキュリティ対応において有効に働いている機能と、改善が必要な機能を見える化しています。
マクロな観点での指標として、成熟度向上の方針策定にお役立てください。

機能	成熟度
A. セキュリティ対応組織運営	3.0 /5
B. リアルタイムアナリシス（即時分析）	4.0 /5
C. ディープアナリシス（深掘分析）	4.0 /5
D. インシデント対応	4.0 /5
E. セキュリティ対応状況の診断と評価	3.0 /5
F. 脅威情報の収集および評価と分析	3.0 /5
G. セキュリティ対応システム運用	3.9 /5
H. 内部統制/内部不正対応支援	3.0 /5
I. 外部組織との積極的連携	4.0 /5

現状のセキュリティ対応組織の強み

B. リアルタイムアナリシス（即時分析）
各種システムで収集される情報をもとに、即時性の高い分析が行われ、迅速で適切なインシデント対応に繋げられています。実務レベルにおいては問題のない状況と言えますが、より組織的な営みへと昇華できるよう、関係組織を巻き込んだ取り組みを行ってください。

C. ディープアナリシス（深掘分析）
被害状況調査、攻撃手法分析など、深い分析が行われ、インシデントの全容解明と影響の特定に繋げられています。実務レベルにおいては問題のない状況と言えますが、より組織的な営みへと昇華できるよう、関係組織を巻き込んだ取り組みを行ってください。

現状のセキュリティ対応組織の弱み

H. 内部統制/内部不正対応支援
内部統制、内部不正に関する対応の支援を十分行えておらず、ガバナンスやコンプライアンス面で貢献しにくくなっています。組織的に機能していない部分がありますので、業務の棚卸、改善が必要となります。

F. 脅威情報の収集および評価と分析
組織内外の脅威情報収集、活用が満足に行えておらず、各種分析、インシデント対応など、他の機能の改善につなげられていません。組織的に機能していない部分がありますので、業務の棚卸、改善が必要となります。

https://isog-j.org/output/2017/Textbook_soc-csirt_v2.1_maturity-checklist.xlsx

HOW TO USE ISOMM

Steps to use ISOMM

1. Understand the security response cycle, roles & services
2. Decide which roles/services you want to provide within your organization
3. Know the current status of your insource/outsource style
4. Determine the goal of your insource/outsource style
5. Check the current status using the self-check sheet
6. Decide what to improve based on the results

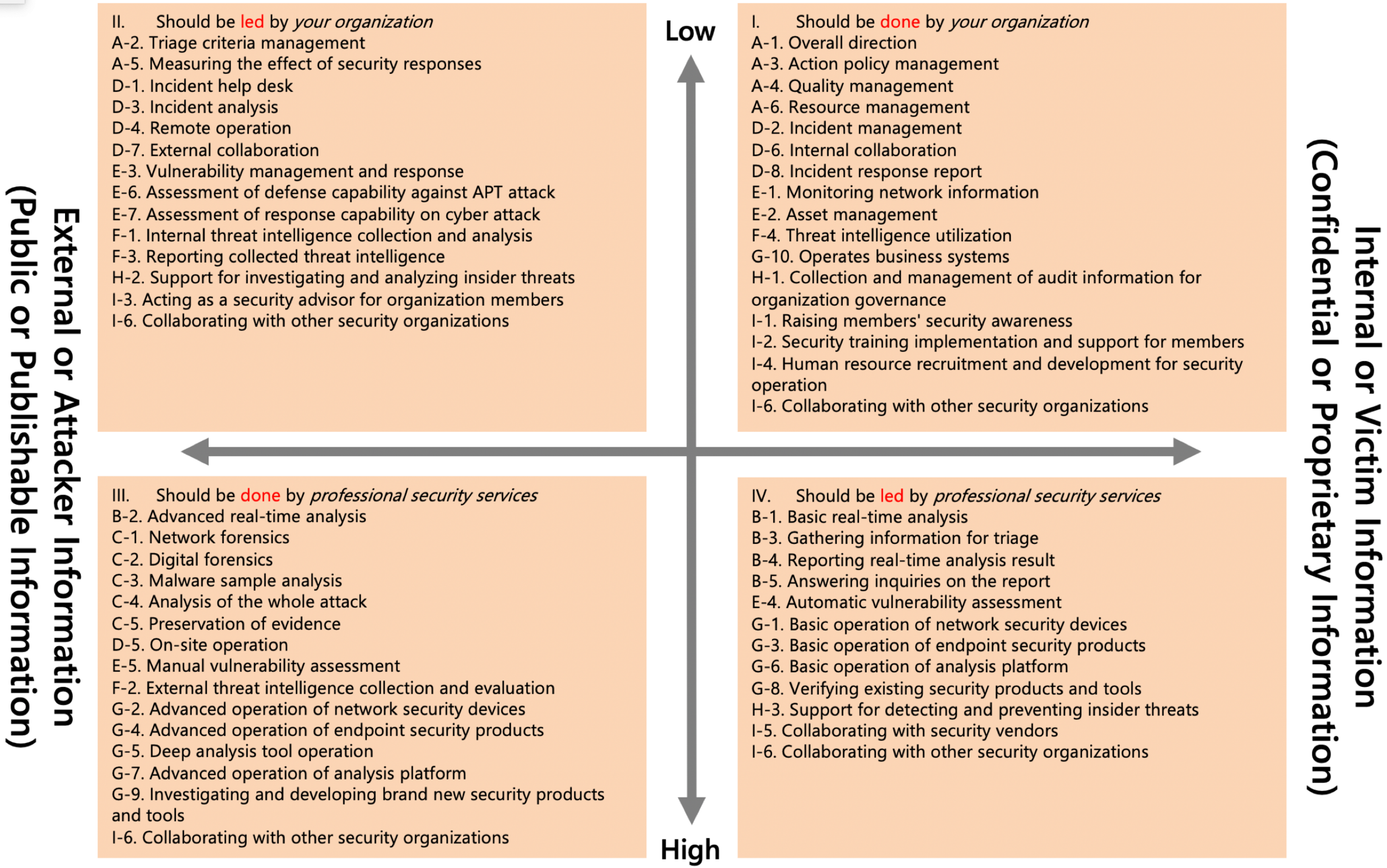
Steps to use ISOMM

1. **Understand the security response cycle, roles & services**
2. Decide which roles/services you want to provide within your organization
3. Know the current status of your insource/outsource style
4. Determine the goal of your insource/outsource style
5. Check the current status using the self-check sheet
6. Decide what to improve based on the results

Steps to use ISOMM

1. Understand the security response cycle, roles & services
2. **Decide which roles/services you want to provide within your organization**
3. Know the current status of your insource/outsource style
4. Determine the goal of your insource/outsource style
5. Check the current status using the self-check sheet
6. Decide what to improve based on the results

Required Security Technical Skill



Low

High

External or Attacker Information
(Public or Publishable Information)

Internal or Victim Information
(Confidential or Proprietary Information)

II. Should be led by *your organization*
A-2. Triage criteria management
A-5. Measuring the effect of security responses
D-1. Incident help desk
D-3. Incident analysis
D-4. Remote operation
D-7. External collaboration
E-3. Vulnerability management and response
E-6. Assessment of defense capability against APT attack
E-7. Assessment of response capability on cyber attack
F-1. Internal threat intelligence collection and analysis
F-3. Reporting collected threat intelligence
H-2. Support for investigating and analyzing insider threats
I-3. Acting as a security advisor for organization members
I-6. Collaborating with other security organizations

I. Should be done by *your organization*
A-1. Overall direction
A-3. Action policy management
A-4. Quality management
A-6. Resource management
D-2. Incident management
D-6. Internal collaboration
D-8. Incident response report
E-1. Monitoring network information
E-2. Asset management
F-4. Threat intelligence utilization
G-10. Operates business systems
H-1. Collection and management of audit information for organization governance
I-1. Raising members' security awareness
I-2. Security training implementation and support for members
I-4. Human resource recruitment and development for security operation
I-6. Collaborating with other security organizations

III. Should be done by *professional security services*
B-2. Advanced real-time analysis
C-1. Network forensics
C-2. Digital forensics
C-3. Malware sample analysis
C-4. Analysis of the whole attack
C-5. Preservation of evidence
D-5. On-site operation
E-5. Manual vulnerability assessment
F-2. External threat intelligence collection and evaluation
G-2. Advanced operation of network security devices
G-4. Advanced operation of endpoint security products
G-5. Deep analysis tool operation
G-7. Advanced operation of analysis platform
G-9. Investigating and developing brand new security products and tools
I-6. Collaborating with other security organizations

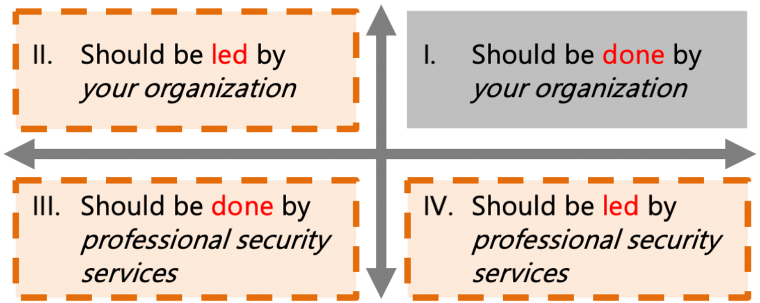
IV. Should be led by *professional security services*
B-1. Basic real-time analysis
B-3. Gathering information for triage
B-4. Reporting real-time analysis result
B-5. Answering inquiries on the report
E-4. Automatic vulnerability assessment
G-1. Basic operation of network security devices
G-3. Basic operation of endpoint security products
G-6. Basic operation of analysis platform
G-8. Verifying existing security products and tools
H-3. Support for detecting and preventing insider threats
I-5. Collaborating with security vendors
I-6. Collaborating with other security organizations

Steps to use ISOMM

1. Understand the security response cycle, roles & services
2. Decide which roles/services you want to provide within your organization
3. **Know the current status of your insource/outsource style**
4. **Determine the goal of your insource/outsource style**
5. Check the current status using the self-check sheet
6. Decide what to improve based on the results

Insource or Outsource patterns

Minimum insource



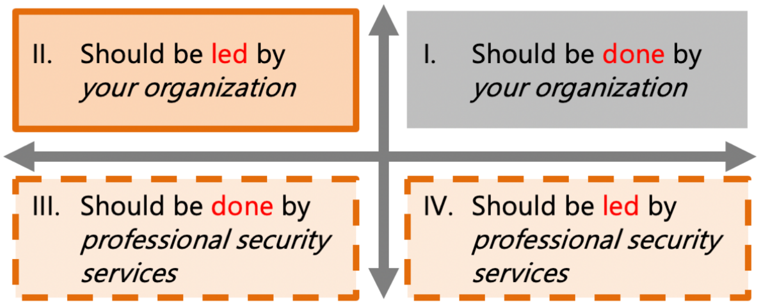
II. Should be led by *your organization*

I. Should be done by *your organization*

III. Should be done by *professional security services*

IV. Should be led by *professional security services*

Hybrid insource/outsource



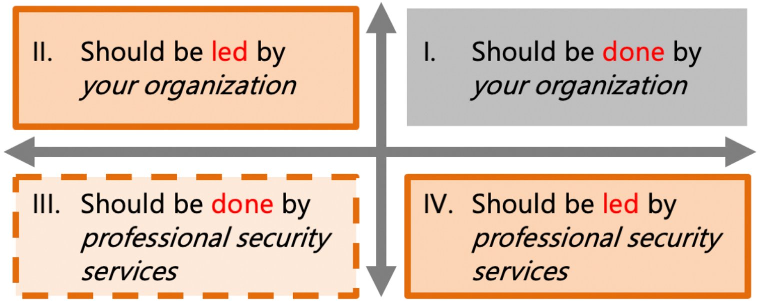
II. Should be led by *your organization*

I. Should be done by *your organization*

III. Should be done by *professional security services*

IV. Should be led by *professional security services*

Minimum outsource



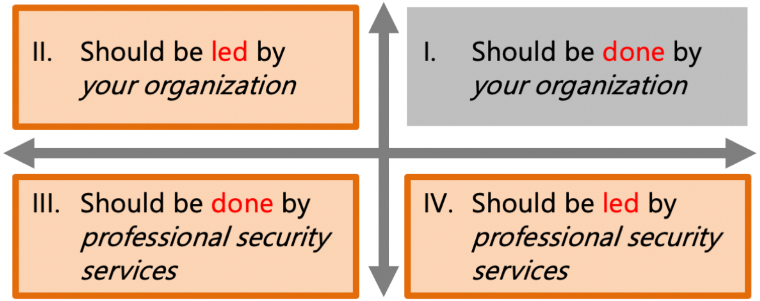
II. Should be led by *your organization*

I. Should be done by *your organization*

III. Should be done by *professional security services*

IV. Should be led by *professional security services*

Full insource

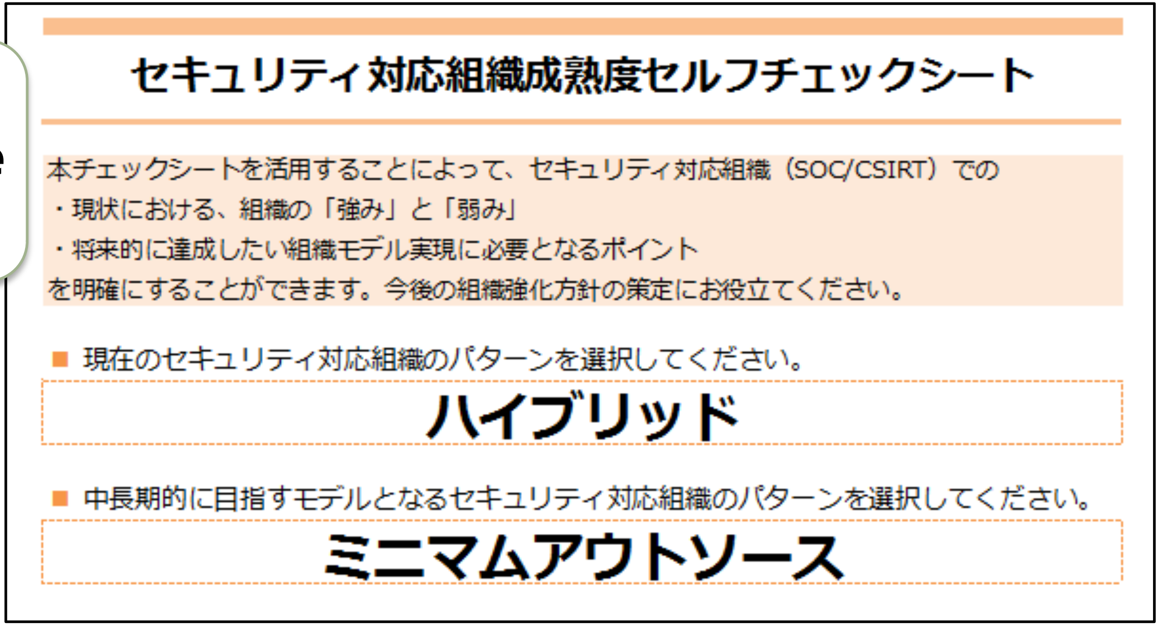


II. Should be led by *your organization*

I. Should be done by *your organization*

III. Should be done by *professional security services*

IV. Should be led by *professional security services*



セキュリティ対応組織成熟度セルフチェックシート

本チェックシートを活用することによって、セキュリティ対応組織（SOC/CSIRT）での
・現状における、組織の「強み」と「弱み」
・将来的に達成したい組織モデル実現に必要となるポイント
を明確にすることができます。今後の組織強化方針の策定にお役立てください。

■ 現在のセキュリティ対応組織のパターンを選択してください。

ハイブリッド

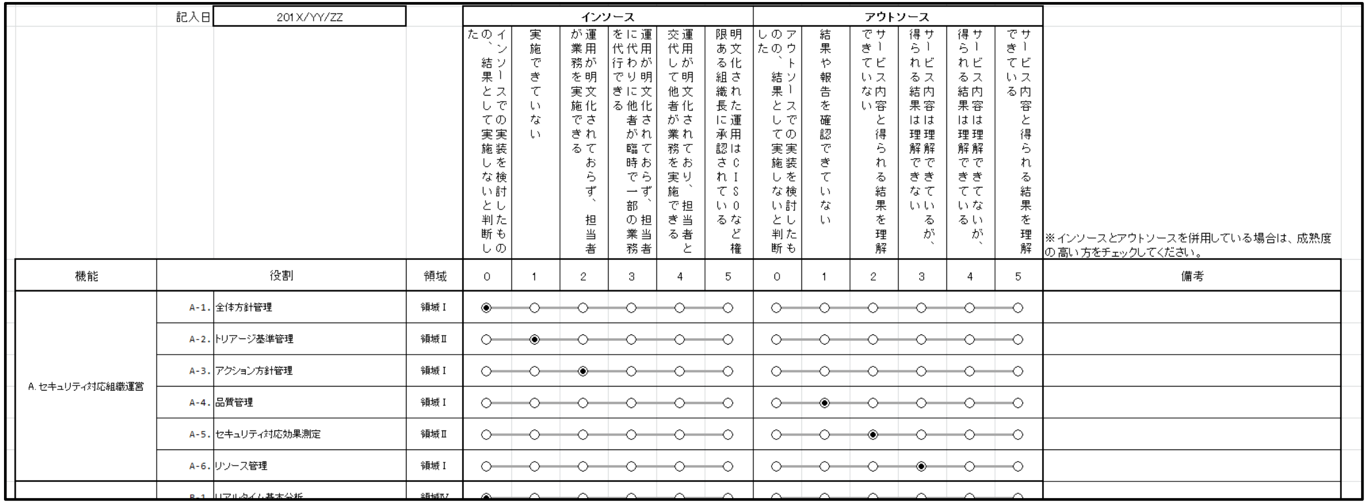
■ 中長期的に目指すモデルとなるセキュリティ対応組織のパターンを選択してください。

ミニマムアウトソース

Select the current pattern and target pattern

Steps to use ISOMM

1. Understand the security response cycle, roles & services
2. Decide which roles/services you want to provide within your organization
3. Know the current status of your insource/outsource style
4. Determine the goal of your insource/outsource style
5. **Check the current status using the self-check sheet**
6. Decide what to improve based on the results



	記入日	201X/YY/ZZ		インソース						アウトソース						
				インソースでの実装を検討したものの、結果として実施しないと判断したもの	実施できていない	運用が明文化されておらず、担当者が業務を実施できる	運用が明文化されておらず、担当者に代わりに他者が臨時で一部の業務を代行できる	運用が明文化されており、担当者と交代して他者が業務を実施できる	明文化された運用はCISOなど権限ある組織長に承認されている	アウトソースでの実装を検討したものの、結果として実施しないと判断したもの	結果や報告を確認できていない	サービス内容と得られる結果を理解できていない	サービス内容は理解できているが、得られる結果は理解できていない	サービス内容は理解できていないが、得られる結果は理解できている	サービス内容と得られる結果を理解できている	※インソースとアウトソースを併用している場合は、成熟度の高い方をチェックしてください。
機能	役割		領域	0	1	2	3	4	5	0	1	2	3	4	5	備考
A. セキュリティ対応組織運営	A-1.	全体方針管理	領域Ⅰ	●	○	○	○	○	○	○	○	○	○	○	○	
	A-2.	トリアージ基準管理	領域Ⅱ	○	●	○	○	○	○	○	○	○	○	○	○	
	A-3.	アクション方針管理	領域Ⅰ	○	○	●	○	○	○	○	○	○	○	○	○	
	A-4.	品質管理	領域Ⅰ	○	○	○	○	○	○	○	●	○	○	○	○	
	A-5.	セキュリティ対応効果測定	領域Ⅱ	○	○	○	○	○	○	○	○	●	○	○	○	
	A-6.	リソース管理	領域Ⅰ	○	○	○	○	○	○	○	○	○	●	○	○	
	B-1.	リアルタイム基本分析	領域Ⅳ	●	○	○	○	○	○	○	○	○	○	○	○	

Rate each service on the measure of an **insourcing** or **outsourcing** scale

Scoring chart

	Insourcing	Outsourcing
0	Do nothing as a result of consideration	Do nothing as a result of consideration
1	Knowing and not doing, or not knowing anything	Not confirm the results and the reports, or not knowing anything
2	A few people can do operations, but not documented	Not understand the services and the results
3	Several people can do operations, but not documented	Not understand the services or the results
4	Team members can do operations by referring to documents	The service quality and benefits are lower than expected or not sufficient
5	Team members can do operations by referring to documents that authorized by responsible persons (ex. CISO, managers…)	The services and the benefits are as expected, and confirm the reports and the results

Some useful tips about the self-check

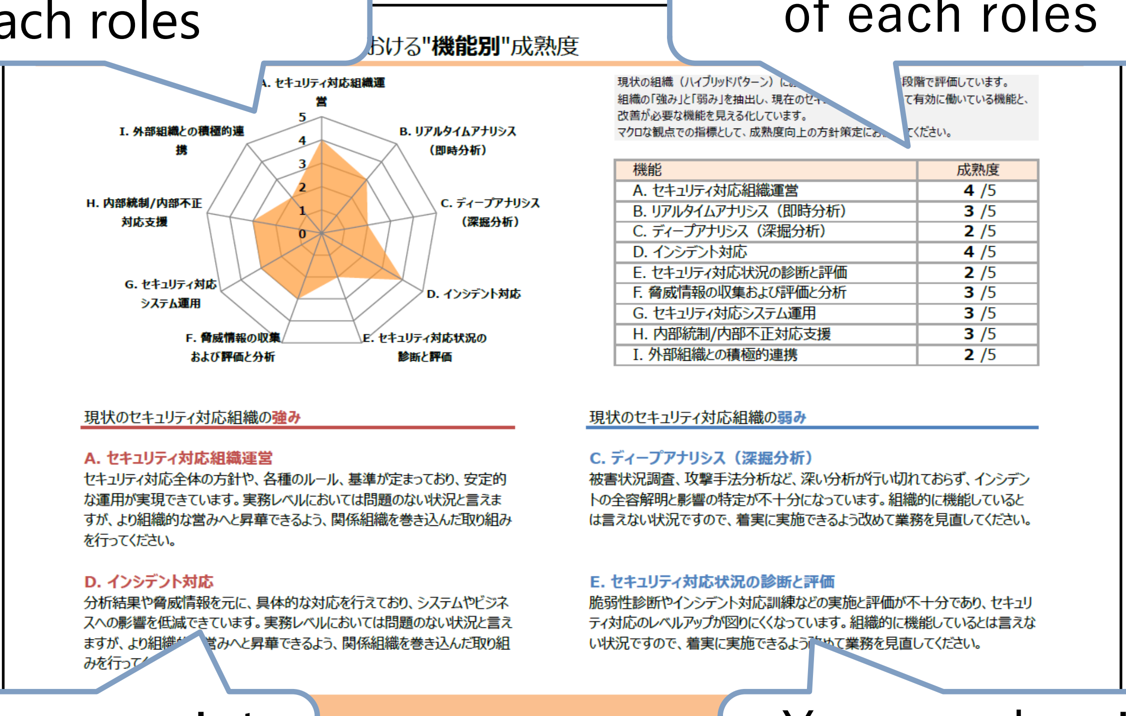
- 1 point if you do nothing without considering the item
- 1 point if you do not know the item or do not think about it
- The score changes depending on your position
  - Rate these items as you think to visualize differences between positions
- Self-check is to visualize things you did not know or could not do, so do not be afraid to rate a low score

Steps to use ISOMM

1. Understand the security response cycle, roles & services
2. Decide which roles/services you want to provide within your organization
3. Know the current status of your insource/outsource style
4. Determine the goal of your insource/outsource style
5. Check the current status using the self-check sheet
6. **Decide what to improve based on the results**

Radar chart: your scores of each roles

Table: your scores of each roles



おける"**機能別**"成熟度

A. セキュリティ対応組織運営
B. リアルタイムアナリシス（即時分析）
C. ディープアナリシス（深掘分析）
D. インシデント対応
E. セキュリティ対応状況の診断と評価
F. 脅威情報の収集および評価と分析
G. セキュリティ対応システム運用
H. 内部統制/内部不正対応支援
I. 外部組織との積極的連携
5
4
3
2
1
0

現状の組織（ハイブリッドパターン）に
段階で評価しています。
組織の「強み」と「弱み」を抽出し、現在のセキ
て有効に働いている機能と、
改善が必要な機能を見える化しています。
マクロな観点での指標として、成熟度向上の方針策定にお
てください。

機能	成熟度
A. セキュリティ対応組織運営	**4** /5
B. リアルタイムアナリシス（即時分析）	**3** /5
C. ディープアナリシス（深掘分析）	**2** /5
D. インシデント対応	**4** /5
E. セキュリティ対応状況の診断と評価	**2** /5
F. 脅威情報の収集および評価と分析	**3** /5
G. セキュリティ対応システム運用	**3** /5
H. 内部統制/内部不正対応支援	**3** /5
I. 外部組織との積極的連携	**2** /5

現状のセキュリティ対応組織の**強み**

A. セキュリティ対応組織運営

セキュリティ対応全体の方針や、各種のルール、基準が定まっており、安定的な運用が実現できています。実務レベルにおいては問題のない状況と言えますが、より組織的な営みへと昇華できるよう、関係組織を巻き込んだ取り組みを行ってください。

D. インシデント対応

分析結果や脅威情報を元に、具体的な対応を行えており、システムやビジネスへの影響を低減できています。実務レベルにおいては問題のない状況と言えますが、より組織　営みへと昇華できるよう、関係組織を巻き込んだ取り組みを行って

現状のセキュリティ対応組織の**弱み**

C. ディープアナリシス（深掘分析）

被害状況調査、攻撃手法分析など、深い分析が行い切れておらず、インシデントの全容解明と影響の特定が不十分になっています。組織的に機能しているとは言えない状況ですので、着実に実施できるよう改めて業務を見直してください。

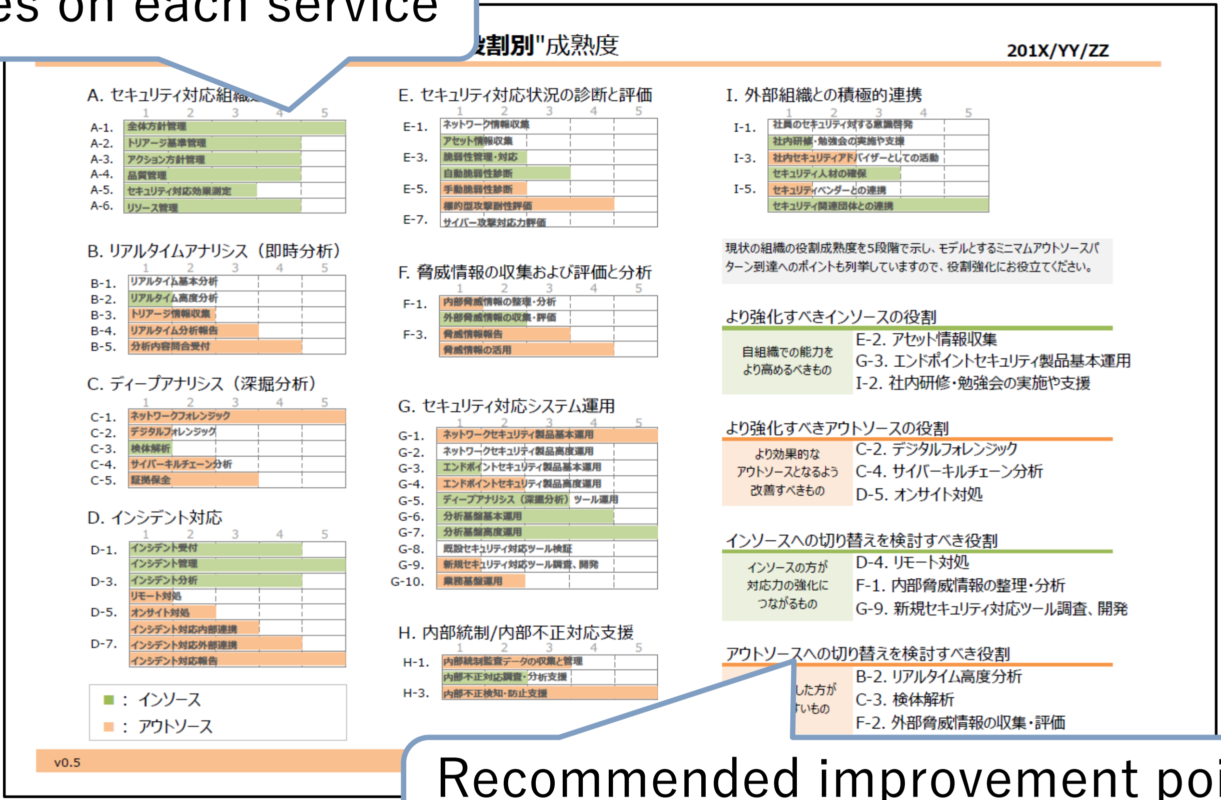
E. セキュリティ対応状況の診断と評価

脆弱性診断やインシデント対応訓練などの実施と評価が不十分であり、セキュリティ対応のレベルアップが図りにくくなっています。組織的に機能しているとは言えない状況ですので、着実に実施できるよう改めて業務を見直してください。

Your strong point: high maturity

Your weak point: low maturity

Your scores on each service



役割別"成熟度

201X/YY/ZZ

A. セキュリティ対応組織

- A-1. 全体方針管理
- A-2. トリアージ基準管理
- A-3. アクション方針管理
- A-4. 品質管理
- A-5. セキュリティ対応効果測定
- A-6. リソース管理

B. リアルタイムアナリシス（即時分析）

- B-1. リアルタイム基本分析
- B-2. リアルタイム高度分析
- B-3. トリアージ情報収集
- B-4. リアルタイム分析報告
- B-5. 分析内容問合受付

C. ディープアナリシス（深掘分析）

- C-1. ネットワークフォレンジック
- C-2. デジタルフォレンジック
- C-3. 検体解析
- C-4. サイバーキルチェーン分析
- C-5. 証拠保全

D. インシデント対応

- D-1. インシデント受付
- インシデント管理
- D-3. インシデント分析
- リモート対処
- D-5. オンサイト対処
- インシデント対応内部連携
- D-7. インシデント対応外部連携
- インシデント対応報告

🟩 ： インソース
🟧 ： アウトソース

E. セキュリティ対応状況の診断と評価

- E-1. ネットワーク情報収集
- アセット情報収集
- E-3. 脆弱性管理・対応
- 自動脆弱性診断
- E-5. 手動脆弱性診断
- 標的型攻撃耐性評価
- E-7. サイバー攻撃対応力評価

F. 脅威情報の収集および評価と分析

- F-1. 内部脅威情報の整理・分析
- 外部脅威情報の収集・評価
- F-3. 脅威情報報告
- 脅威情報の活用

G. セキュリティ対応システム運用

- G-1. ネットワークセキュリティ製品基本運用
- G-2. ネットワークセキュリティ製品高度運用
- G-3. エンドポイントセキュリティ製品基本運用
- G-4. エンドポイントセキュリティ製品高度運用
- G-5. ディープアナリシス（深掘分析）ツール運用
- G-6. 分析基盤基本運用
- G-7. 分析基盤高度運用
- G-8. 既設セキュリティ対応ツール検証
- G-9. 新規セキュリティ対応ツール調査、開発
- G-10. 業務基盤運用

H. 内部統制/内部不正対応支援

- H-1. 内部統制監査データの収集と管理
- 内部不正対応調査・分析支援
- H-3. 内部不正検知・防止支援

I. 外部組織との積極的連携

- I-1. 社員のセキュリティ対する意識啓発
- 社内研修・勉強会の実施や支援
- I-3. 社内セキュリティアドバイザーとしての活動
- セキュリティ人材の確保
- I-5. セキュリティベンダーとの連携
- セキュリティ関連団体との連携

現状の組織の役割成熟度を5段階で示し、モデルとするミニマムアウトソースパターン到達へのポイントも列挙していますので、役割強化にお役立てください。

より強化すべきインソースの役割

自組織での能力を より高めるべきもの	E-2. アセット情報収集 G-3. エンドポイントセキュリティ製品基本運用 I-2. 社内研修・勉強会の実施や支援

より強化すべきアウトソースの役割

より効果的な アウトソースとなるよう 改善すべきもの	C-2. デジタルフォレンジック C-4. サイバーキルチェーン分析 D-5. オンサイト対処

インソースへの切り替えを検討すべき役割

インソースの方が 対応力の強化に つながるもの	D-4. リモート対処 F-1. 内部脅威情報の整理・分析 G-9. 新規セキュリティ対応ツール調査、開発

アウトソースへの切り替えを検討すべき役割

した方が いもの	B-2. リアルタイム高度分析 C-3. 検体解析 F-2. 外部脅威情報の収集・評価

v0.5

Recommended improvement points to work on next

The characteristic of analysis results by this tool

- Immediately after the staff changes, the score is often low
- If the operators and the engineers is self-checking, the score often lower. If the managers and the leaders self-checking, the scores often higher
- Outsourced services have higher scores

Lightweight and easy-to-use tool

- Anyone who belongs to a security organization can self-checking your organization's current status
  - Visualize gaps felt by the type of occupation or individual differences
  - Determine if there is a lack of service for security response in your organization
- Compare with assessment results from third parties
- No improvement can be made without checking the current status
  - use ISOMM!

CYBERSECURITY INFORMATION SHARING

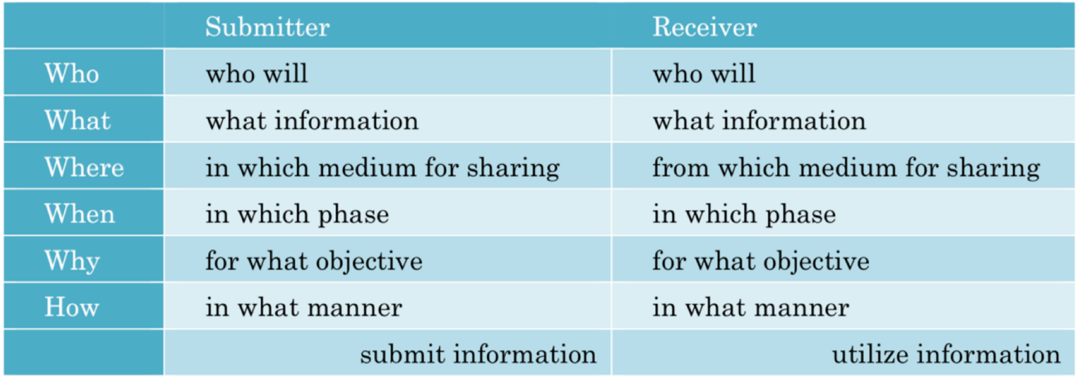
Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT

- Released!
  - The referral destination documents are only in Japanese
    - we will make summary of necessary parts in English
- Please send us your comments!

download here https://goo.gl/qoCHtn
or from http://isog-j.org/e/

the point of this Six Ws document

- the basics of security information sharing for members of SOC/CSIRT
- Why mismatches when sharing information?
  - We went back to the basics and thought



	Submitter	Receiver
Who	who will	who will
What	what information	what information
Where	in which medium for sharing	from which medium for sharing
When	in which phase	in which phase
Why	for what objective	for what objective
How	in what manner	in what manner
	submit information	utilize information

Table 1：Six Ws in cybersecurity information sharing

Phasing incident handling triggered by shared information

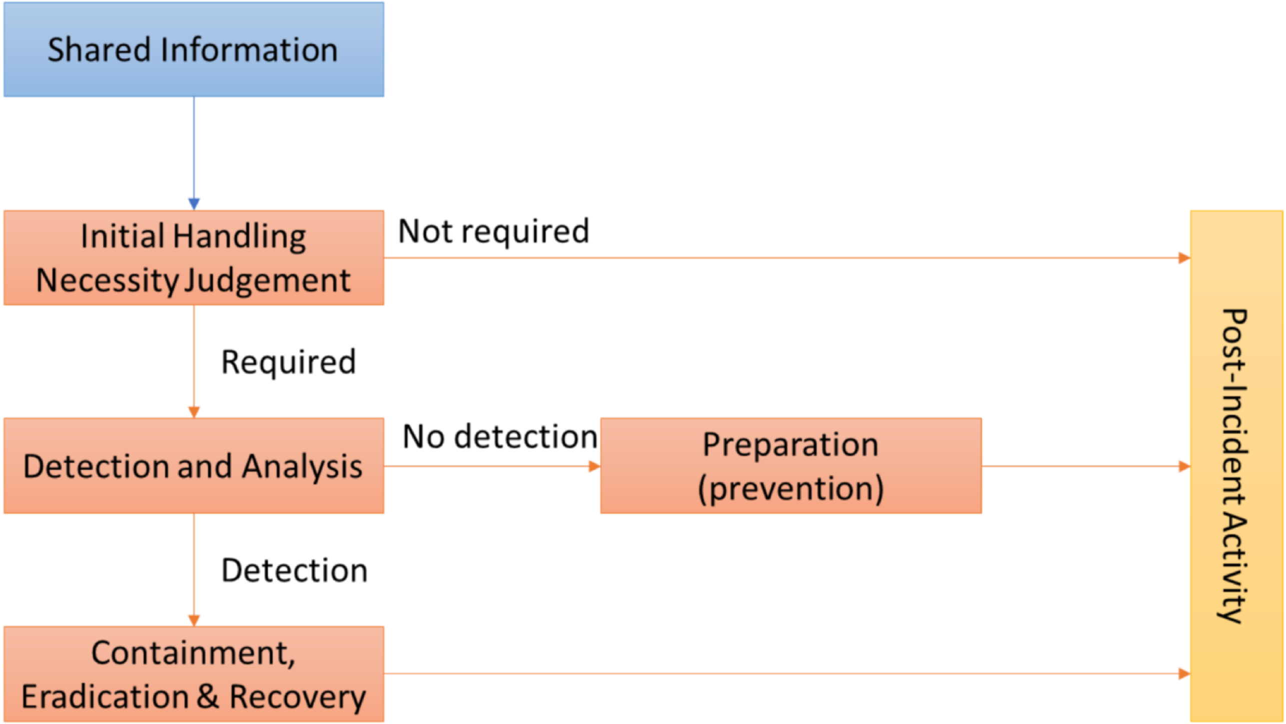
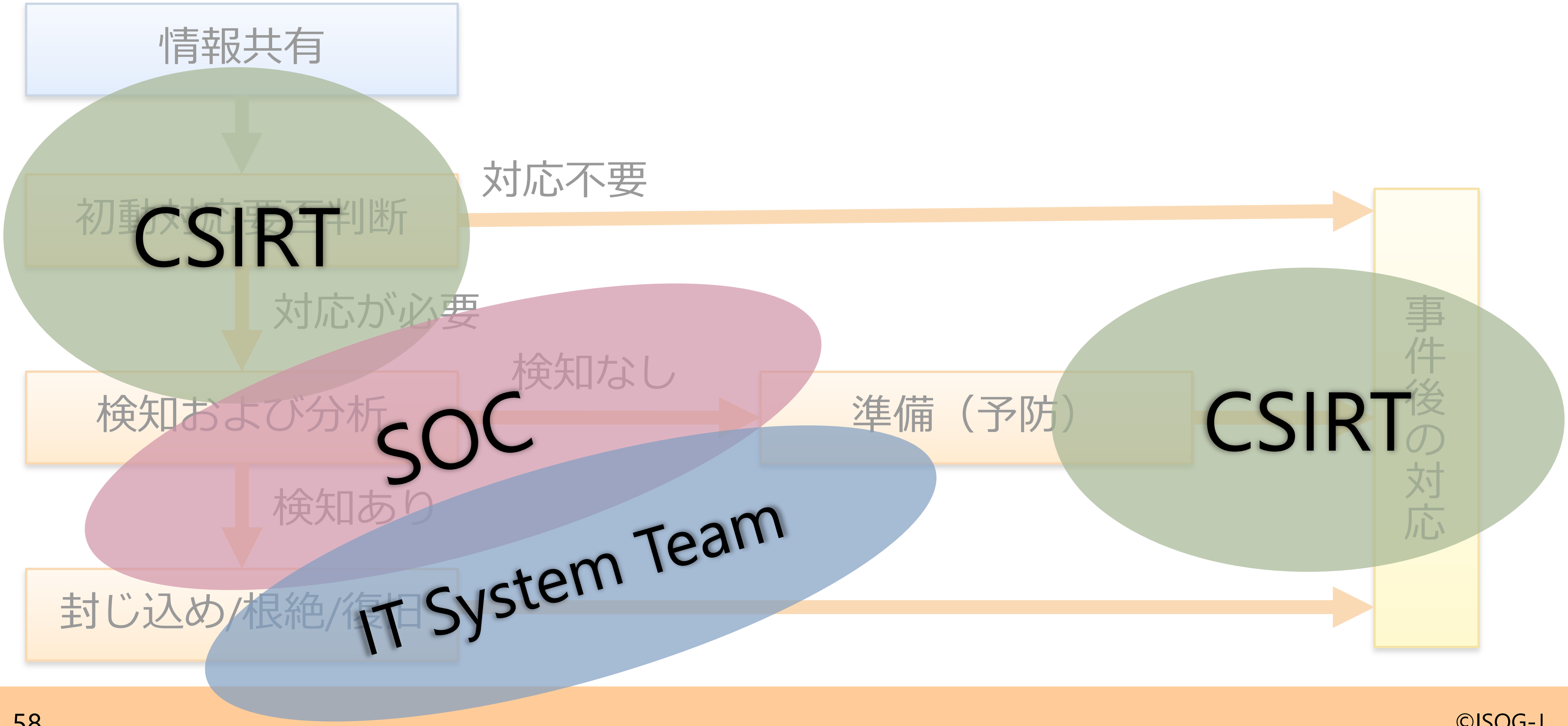
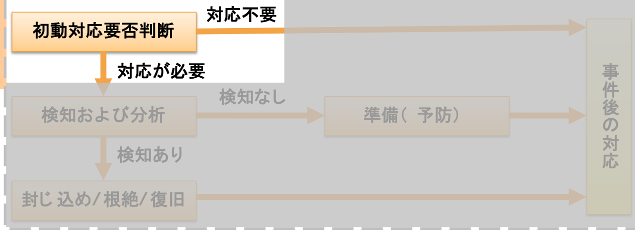


Figure 3：Incident handling triggered by shared information

The roles responsible for each phase are different





When	Determine if action is required
Why	Is our organization affected?

Vulnerability information (What)

- vulnerability identifier
  - CVE or patch number
- affected systems
  - system type
  - version
  - conditions (e.g. configuration)
- can security products prevent it?

Attacking related information (What)

- name that specifies the attack
  - campaign
  - malware/incident name
- target of attack
- attack vector
  - from where the attack comes

Information sharing triangle

- Take just two out of the three!
  - Fast, Accurate, Comprehensive

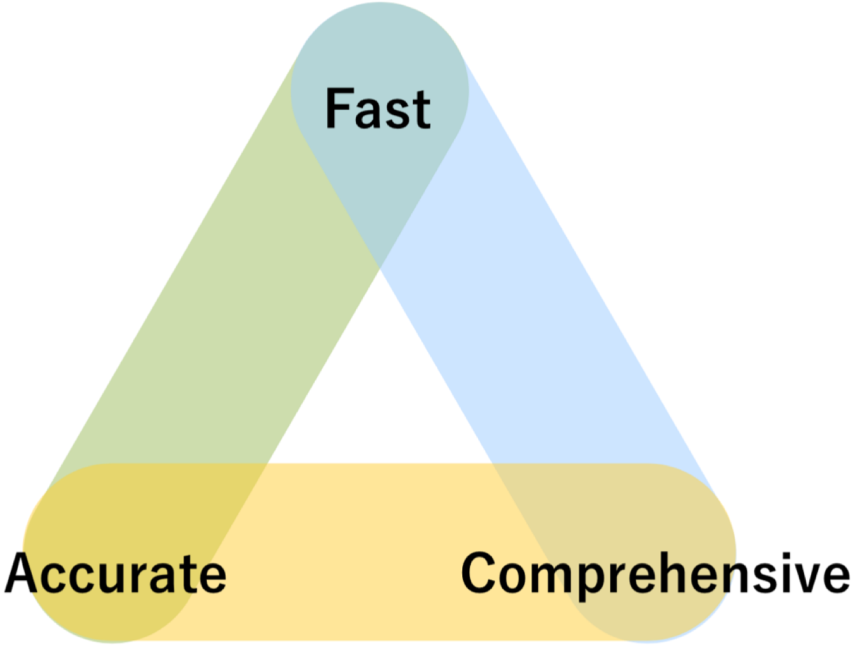


Figure 4 : Triangle in information sharing

27th Annual FIRST Conference (2015), Lightning Talk: "Four Easy Pieces", Tom Millar (US-CERT, NIST)

OVERALL SUMMARY

Thanks!

- ISOG-J released Handbook for Security Response Organization (SOC/CSIRT)
  - You can use ISOMM and self-checking tool for measure your security response team
- ISOG-J discussed information sharing on cybersecurity from the fundamentals and summarized it.
- Release soon! Please send us your comments!

https://isog-j.org/e/