Fast, Frank, and Friendly
Financials ISAC Japan

ＩＳＡＣの活用について

ISACの２つの柱

➢ コレクティブ・インテリジェンス

- ✓ 攻撃者は組織化され、多くある弱点の１つを狙ってくればよい。
- ✓ 圧倒的に攻撃側が有利な環境下、１つの組織で適切な対応を行うことは極めて難しい。
- ✓ 各組織のバイアスを少なくする効果もある。
- ✓ 信頼のあるコミュニティの中で培われた集合知はお金では買えない。

➢ リソースシェアリング

- ✓ 更に進んで、教育、演習、最近では制度への対応のグッド・プラクティスをシェア。
- ✓ 不正送金へのティップスを含めた対応方法。
- ✓ 今後のPQC、AIへの対応。

（２）暗号資産交換業者への不正な送金への対策事例 イメージ

＜A.暗号資産交換業者の判定方法＞

① 金融庁「暗号資産交換業者登録一覧」を確認
https://www.fsa.go.jp/menkyo/menkyoj/kasoutuka.pdf

② 取引ログから、上記から想定される振込先を「カナ名義」で検索し、利用されている口座を確認、対象リストを作成する

課題１：取引量が少ないと網羅性のあるリストを作成できない

課題２：暗号資産交換業者の社名（カナ名義）が短い場合は、一般事業者もヒットしてしまう
→カナ名義のあいまい判定のみでは、誤判定リスクあり

シェアリングの例２：APIセキュリティ

◆APIへの攻撃事例

- Dropboxの事例（APIキーが盗まれた事例）
- Kerasの事例（API脆弱性）

◆APIセキュリティ強化のポイント

- APIを提供する場合には「標準」に準拠すること
- OAuth2.0、OpenID Connect1.0、FAPI2.0
- APIの可視化、モニタリング
- API管理基盤の活用

シェアリングの例3：教育

■ スキルアップWGのコンテンツ

座学・ゲーム　読み物　座学＋演習　座学＋ディスカッション　演習

超初級
初任者向け

初級
IT・セキュリティの基礎

中級
個別・応用分野、インシデント対応総合演習

【A010】
基礎の基礎

【A020】
ABCSIRT
インシデント対応
カードゲーム

【B010】
Linux
基礎

【B020】
Windows
基礎

【B030】
IT基礎
①②

【B040】CAMP
ハンズオン形式の基礎学習

【C010】
IT基礎
③

【C020】
インシデント
初動調査入門

【B031】ミニ勉強会(DNS、暗号他)

【B050】脆弱性対応勉強会

【B060】しくじり事例から学ぶ

【B070】サイバーセキュリティ対策勉強会

Cyber Quest

【D010】
サイバークエスト
（技術チーム）

【C030】
サイクエミニ
（技術チーム）

【C031】
サイクエBLUE
（技術チーム）

【D010】
サイバークエスト
（管理チーム）

【C030】
サイクエミニ
（管理チーム）

【C031】
サイクエBLUE
（技術チーム）

【E010】経営層向け教材（経営層用・担当者用）

スキルマップ／スキルチェックシート（スキル状況の可視化ツール）

シェアリングの例4：内部監査

情報共有会

内部監査WGメンバーの事例共有、最新トレンドに関するディスカッション、監査お悩み相談	
成果	✓ 全11回実施（≒月次） ✓ 内外の最新動向の共有・ディスカッションを通してレベルアップに貢献

分科会

【分科会①】2022年度に作成した「サイバーセキュリティ監査ガイド」の分冊となる、“**実践編**”の作成	
成果	✓ 執筆7名、レビュー等支援6名にて作成 ✓ 全68ページの「サイバーセキュリティ監査ガイド（実践編）」をリリース（2024年4月）

【分科会②】勉強会の開催	
成果	✓ 2023年度、計4回の勉強会を開催 ✓ 延べ250名超が参加

【分科会③】クラウドチェックリストの作成	
成果	※他WGとコラボ企画を進めたものの2023年度中での具体的な成果物なし

シェアリングの例5：成熟度評価

Fast, Frank, and Friendly
Financials ISAC Japan

IDENTIFY 識別 | PROTECT 防御 | DETECT 検知 | RESPOND 対応 | RECOVER 復旧

GOVERN ガバナンス
GV.OC：組織コンテキスト
GV.RM：リスク管理戦略
GV.PO：ポリシーと手続
GV.RR：役割分担

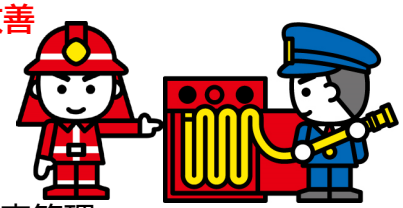
①新設+IDから移動

~~ID.GV：ガバナンス~~
~~ID.RM：リスク管理戦略~~

PR.AT：意識向上・訓練

②新設(集約)

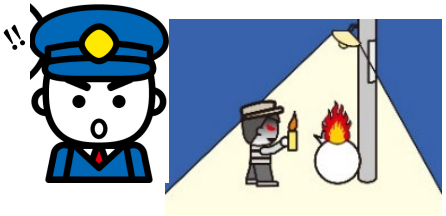
ID.IM：改善



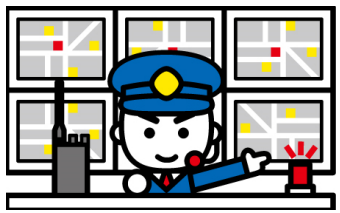
ID.AM：資産管理
~~ID.BE：ビジネス環境~~
ID.RA：リスク評価
ID.SC：サプライチェーン管理

PR.AA~~C~~：ID管理・認証・アクセス制御
PR.DS：データセキュリティ
~~PR.MA：保守~~
~~PR.IP：情報保護プロセス・手順~~
~~PR.PT：保護技術~~
PR.PS：プラットフォームセキュリティ
PR.IR：技術インフラレジリエンス

DE.AE：~~異常とイベント~~有害イベント分析
DE.CM：~~セキュリティの~~継続的なモニタリング
~~DE.DP：検知プロセス~~

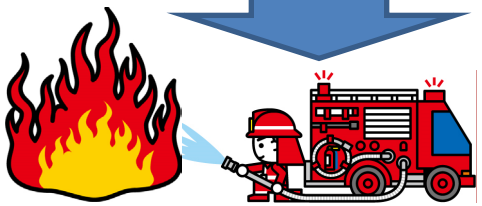


④分解



RS.MA~~RP~~：インシデント対応管理計画
RS.CO：インシデント報告・コミュニケーション
RS.AN：インシデント分析

⑤広範

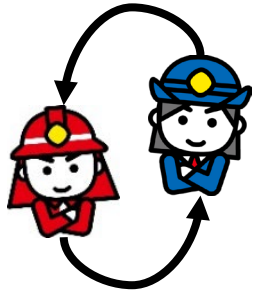


RS.MI：インシデントの低減
~~RS.IM：改善~~

③分解+新設(セキュリティアーキ等)

⑤拡張(バックアップ等)

RC.RP：復旧計画
~~RC.IM：改善~~
RC.CO：インシデント復旧コミュニケーション



付録　~2023年度の概況と今後の展望~

日本の金融機関において、2023年度は重要な動きを見せています。金融庁は、中小金融機関向けに開始した**CSSA（サイバーセキュリティ自己評価ツール）**を、保険や証券業界にも拡大し、サイバー評価の浸透を図っています。一方、大手金融機関では評価ツールのシフトが進んでいます。具体的には、FFEICCATから**CRIProfileへの移行**が進行中であり、この変化は米国金融機関のスタンダードに関連しています。

22年5月に制定された**経済安全保障推進法**に基づき、大手地銀や都銀においては、23年はサイバーレジリエンスの観点から外部委託の事前審査の枠組み作りが進められました。今後は、重要システムを委託する際には、**リスク管理措置**をサプライヤーに提示する運用が本格的に開始されます。

グローバルの動向と展望に目を向けると、22年に改定を発表した**NISTCSFv2.0**へのディスカッションが進み、23年6月にドラフト版が公開、24年2月に正式版が公開されました。24年度はこれに関連付けされるNISTシリーズや主な評価ツールの改訂が続きます。

高まる**地政学リスク**を背景に、米国で防衛関連の機密情報を保護するNISTSP800-53やNISTSP800-171がサイバーセキュリティ基準として注目されています。また、情報セキュリティの国際規格である**ISO27001**も新たなサイバーセキュリティ要件を追加し、22年に5年ぶりに大改訂されました。現在、3年間の移行期間中です。

一部の超巨大IT企業は、グローバルベースで大量のデータを保有しており国家レベルの力を持つ存在として金融監督機関からの警戒が強まっています。分散化を含めた**サードパーティ管理の要請**が活発化してきています。

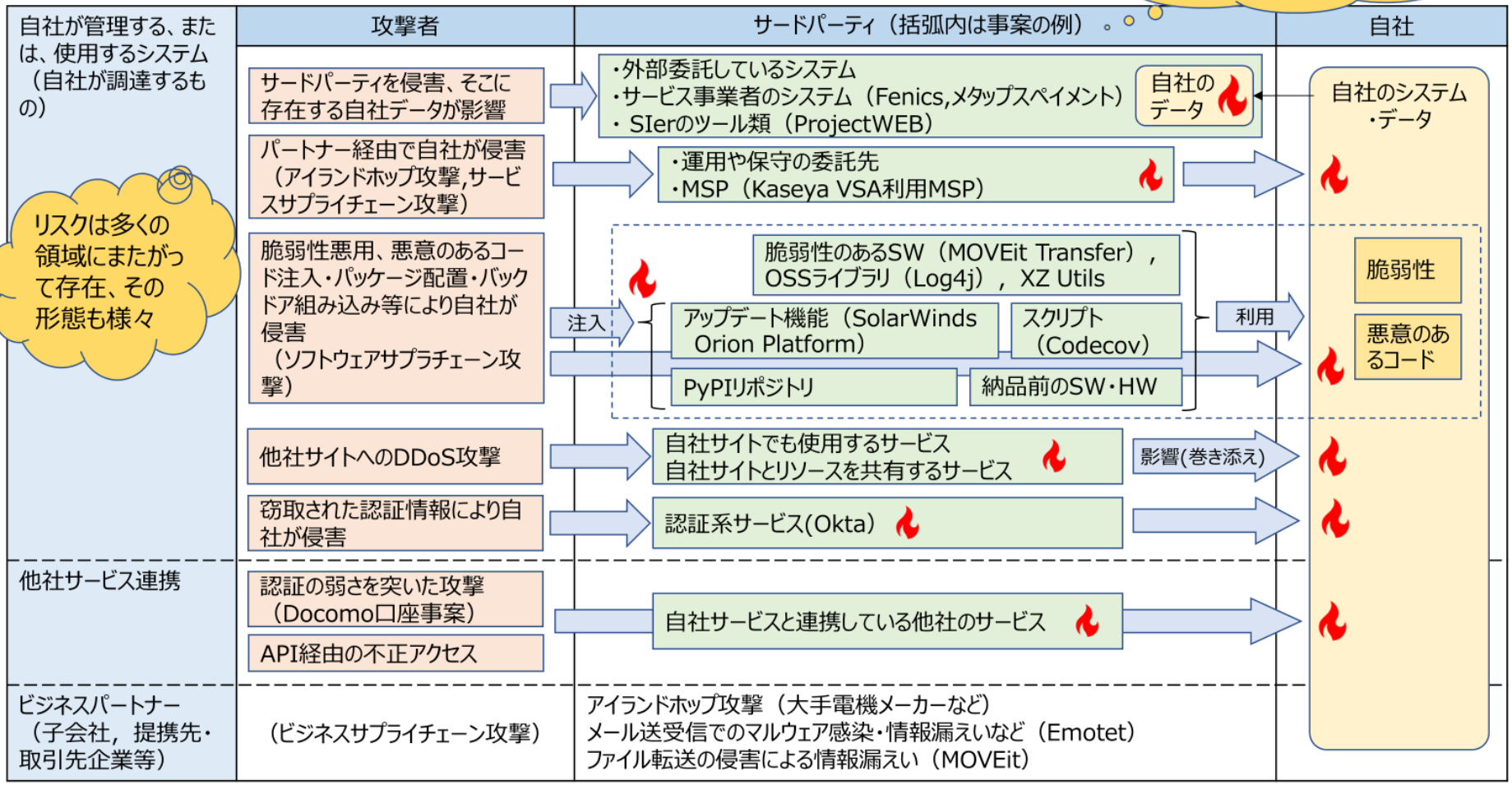
さらに、生成AIやディープフェイクの急速な技術進歩により、フィッシング詐欺などに**AIが悪用**されるケースが増える見込みです。金融機関においても顧客をサイバー犯罪、デジタル詐欺から保護する備えがますます重要視されており、セキュリティ評価ツールの今後にも影響を与えるでしょう。

※Chat-GPT4に『おしゃれなエッセイ風文章』に変更するようオーダーしました。

シェアリングの例７：サードパーティリスクの類型

サードパーティサイバーリスクの視点での脅威シナリオの類型（例）

サードパーティへの依存度が高まっている



シェアリングの例８：Daily脆弱性情報＆セキュリティ・ニュース

20240513_Daily脆弱性情報

* 【☆9.9(v3)】Veeam Service Provider Console 7.0.0.18899/8.0.0.19236 未満におけるリモート・コード実行の脆弱性
* 【★9.8(v3)】Tinyproxy (light-weight HTTP/HTTPS proxy daemon) 1.10.0/1.11.1 における解放済みメモリの使用の脆弱性
* 【★High】Google Chrome for Mac/Linux/Windows における脆弱性と 124.0.6367.91/92 へのアップデート
* 【High】Trend Micro Antivirus One for Mac (antivirus/monitoring) 3.10.3 以下におけるコード・インジェクションの脆弱性
* 【8.6(v4)】Linux Kernel (open source Unix-like operating systems) 5.19.9 以下における解放済みメモリの使用の脆弱性
* 【☆8.4(v3)】Pterodactyl Wings (server control plane) 1.11.11 以下におけるファイル／ディレクトリに対する外部からの不正参照の脆弱性
* 【8.1(v3)】IBM AIX などにおける権限昇格の脆弱性
* 【★7.5(v3)】F5 BIG-IP (application delivery controllers with LTM and DNS) 17.1.0 以下におけるサービス運用妨害の脆弱性
* 【☆7.4(v3)】F5 BIG-IP Next Central Manager 20.0.1/20.0.2 における不適切な暗号の脆弱性
* 【☆6.5(v3)】F5 BIG-IP (application delivery controllers with LTM and DNS) 15.1.9 以下におけるメモリ・リークの脆弱性
* 【★6.5(v3)】Open-Xchange OX App Suite (email/calendar/cloud storage/office document) 8.21 以下における XSS の脆弱性
* 【☆6.4(v3)】Pterodactyl Wings (server control plane) 1.11.11 以下における不適切なアクセス制御の脆弱性
* 【☆6.3(v4)】F5 BIG-IP (application delivery controllers with LTM
* 【★6.3(v3)】Red Hat Enterprise Linux などに影響をおよぼす gstream
* 【6.2(v3)】IBM Watson CloudPak for Data Data Stores における情報漏
* 【★6.1(v3)】WordPress Yoast SEO Plugin 22.5 以下における XSS の脆
* 【★6.1(v3)】Pterodactyl Panel (game server management panel) 1.11.
* 【☆5.3(v4)】F5 BIG-IP Next および F5 BIG-IP における不適切なイニシ
* 【☆5.3(v4)】F5 BIG-IP Next および F5 BIG-IP の Configuration util
* 【★5.3(v3)】Aruba ArubaOS (Network Management Software) 8.10.0.10
* 【☆5.3(v4)】MediaWiki (collaboration and documentation platform)
* 【☆5.3(v4)】MediaWiki (collaboration and documentation platform)

4.セキュリティ・ニュースについて　CSIRT-TC

セキュリティ・ニュースができるまで

海外メディア
Bleeping Computer
The Hacker News
Security Week
Security Online
Security Affairs
Help Net Security
Info Security
Dark Reading
…

CISA KEV
JPCERT/CC
Exploit-DB

記事／情報の選別、カテゴライズ
・速さ：各メディアを毎日4~5回クロール
・信憑性：一次ソースへのリンク
・一定量の情報が提供されるサイト
・統計系：HelpNetSecurity
・深堀り系：InfoSecurity／DarkReading

記事の翻訳・要約
・15分程度で
読める文量に要約

WordPress
DeepL
Google T

配信
・平日（月~金）AM
・翌日／翌々日の配信（努力目標）
・1日あたり6~7件

脆弱性レポート
＋ インシデント情報

気になる脆弱性リスト
→ WGで報告

17

今後のテーマ１：PQC対応

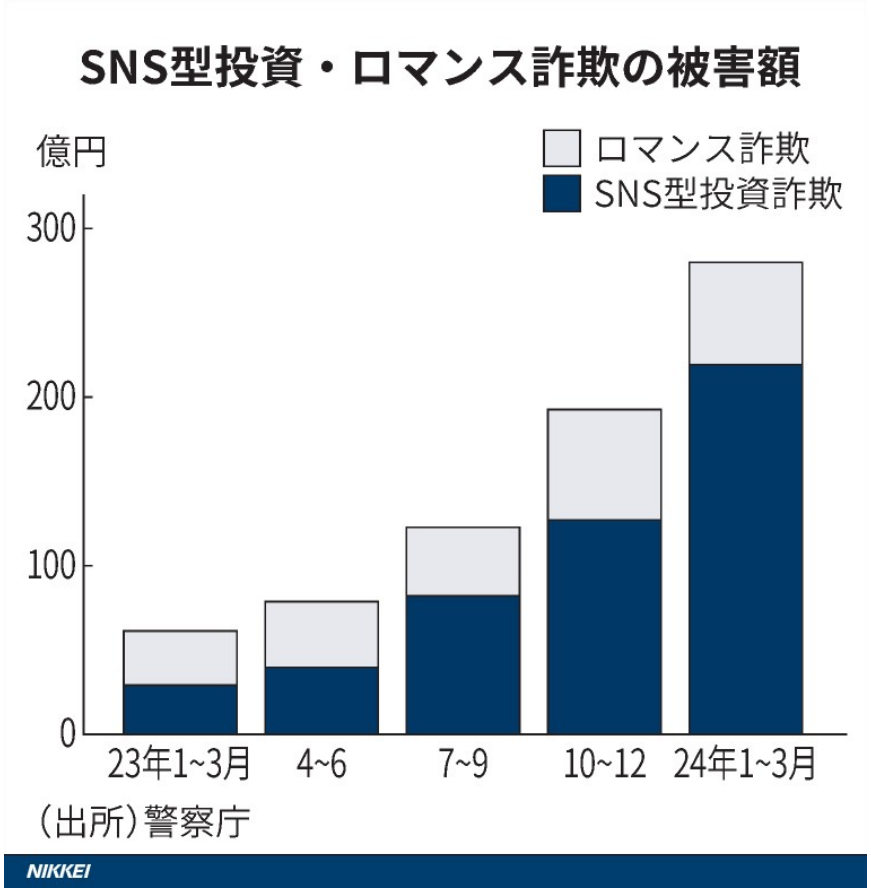
◆PQC

- ●量子コンピュータの実用化により、特にRSA等の非対称暗号が脆弱になると言われており、それに対応したPQC（耐量子コンピュータ暗号）への移行が求められている。

◆論点がいまひとつ明確でない中

- ●どんなリスクがあるのか
- ●いつから/いつまでに対応すべきか
- ●何を対応すべきか
- ●どのように対応すべきか

今後のテーマ２：特殊詐欺について



2024年5月16日日本経済新聞より

2024年4月24日NHKより

今後のテーマ２：特殊詐欺について

【重要】SBI証券およびSBIグループ各社を装った偽アカウント、偽広告にご注意ください

Facebook、Instagram、X(旧Twitter)、LINE等のSNSにおいて、当社、SBIグループ各社および役職員の公式アカウントを装った偽アカウントや偽広告の配信が確認されています。

とくに弊社代表の北尾吉孝を装った偽アカウントや偽広告を複数確認しており、十分にご注意くださいますようお願い申し上げます。

また、一部のWEBサイトやアプリでも同様の偽広告が確認されています。

偽アカウントおよび偽広告は、不正サイトへの誘導、個人情報の取得および悪用、詐欺被害に遭う可能性等がございますのでアクセスされないようご注意ください。

公式SNSアカウントは以下のとおりです。

北尾 吉孝公式Facebookアカウント
https://www.facebook.com/yoshitakakitao

SBI証券HPより

参考例②（実際に無断転載されたサムネイル等）

・2023年3月・8月 FacebookやInstagram等のSNSにおいて本協会コンテンツを無断転載し、LINEグループや情報商材販売サイトに誘導している事例。

※ 以下、実際に無断転載されたサムネイル等

本協会が、LINEグループへの参加を促したり情報商材を販売したりすることは一切ございませんのでご注意ください。

・2017年2月 証券会社の社員を騙った者から「日証協の役員に金銭を渡す必要があることから、指定の銀行口座に金銭を振り込め」という指示があり、振り込んでしまった事例。

・2016年11月 日本証券業協会返還部（または返還業務部等）の役職員を騙った者から、通報者の持っている未公開株の返金に関する電話があった事例。

・2016年10月 日本証券業協会の役職員を騙った者から、通報者の持っている社債を高値で買取る旨の電話があった事例。

・2016年1月 日本証券業協会の役職員を騙った者から、未公開株式詐欺の被害者に、被害回復を行うための手数料と称して金銭を要求する電話があった事例。

少しでも怪しいと思った場合には、直ぐにやり取りを中断して、以下のような方法で証券会社へご確認ください。

日本証券業協会HPより

今後のテーマ２：特殊詐欺について

2023 CRIME TYPES continued

By Complaint Loss

Crime Type	*Loss*	*Crime Type*	*Loss*
Investment	$4,570,275,683	Extortion	$74,821,835
BEC	$2,946,830,270	Employment	$70,234,079
Tech Support	$924,512,658	Ransomware*	$59,641,384
Personal Data Breach	$744,219,879	SIM Swap	$48,798,103
Confidence/Romance	$652,544,805	Overpayment	$27,955,195
Data Breach	$534,397,222	Botnet	$22,422,708
Government Impersonation	$394,050,518	Phishing/Spoofing	$18,728,550
Non-payment/Non-Delivery	$309,648,416	Threats of Violence	$13,531,178
Other	$240,053,059	Harassment/Stalking	$9,677,332
Credit Card/Check Fraud	$173,627,614	IPR/Copyright and Counterfeit	$7,555,329
Real Estate	$145,243,348	Crimes Against Children	$2,031,485
Advanced Fee	$134,516,577	Malware	$1,213,317
Identity Theft	$126,203,809		
Lottery/Sweepstakes/Inheritance	$94,502,836		

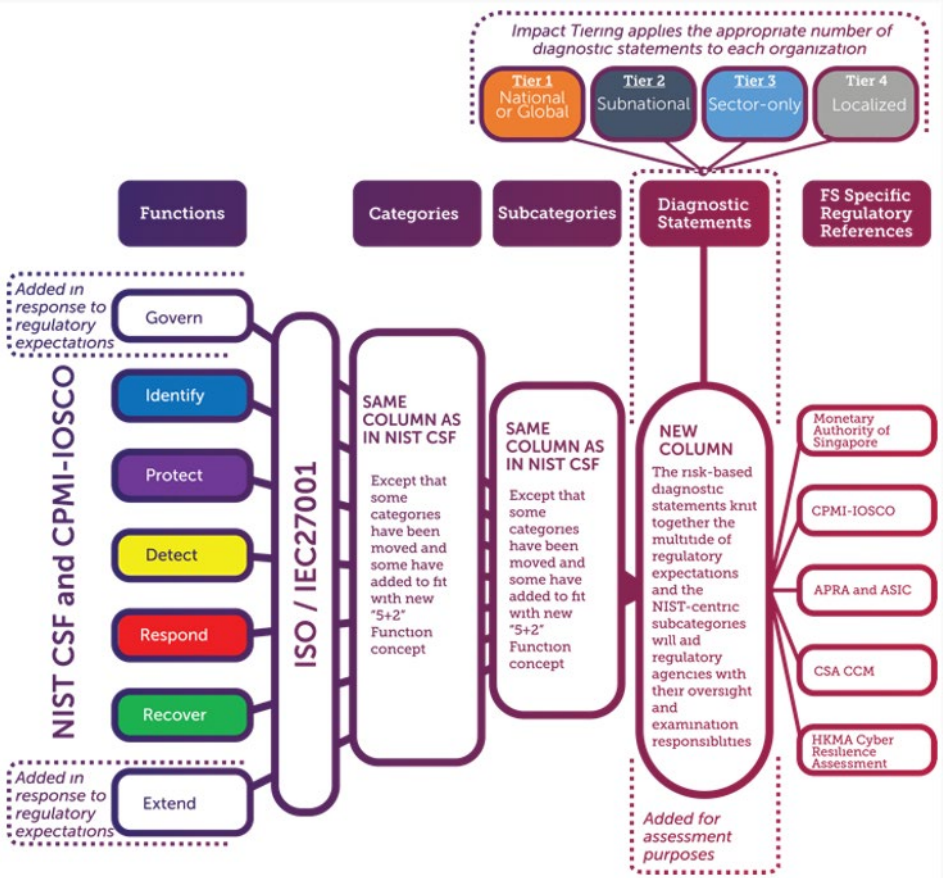
*Descriptors***			
Cryptocurrency	$3,809,090,856	Cryptocurrency Wallet	$1,778,399,729

*Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by an entity. In some cases, entities do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what entities report to the FBI via the IC3 and does not account for the entity direct reporting to FBI field offices/agents.

FBI Internet Crime Report 2023 (IC3, 2024)より

- ✓ USでは桁違いの被害
- ✓ unauthorizedとauthorizedの補償

今後のテーマ２：当局対応とアカウンタビリティ



Cyber Security Institute HPより

Format for Incident Reporting Exchange (FIRE): A possible way forward

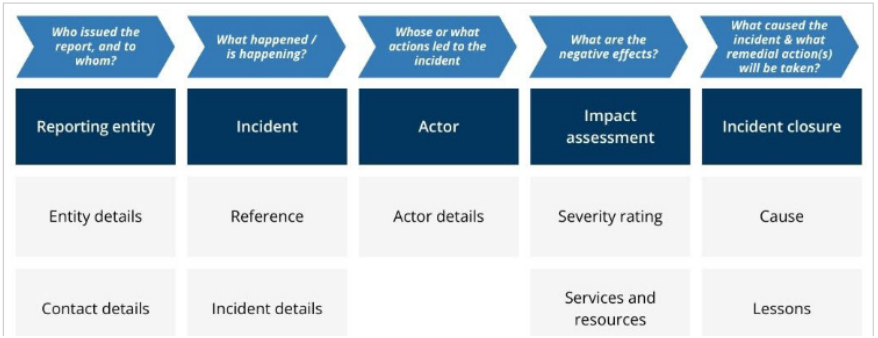
Available as: PDF

13 April 2023

> The FIRE concept promotes common information elements and requirements for incident reporting, whilst remaining flexible to a range of implementation practices.

As part of its work to achieve greater convergence in cyber incident reporting (CIR), the FSB found that there is a high degree of commonality in the types of information that authorities require financial institutions to report under existing CIR frameworks. Seeing potential to leverage on these similarities to explore greater convergence, the FSB consulted on a concept for developing a common format for incident reporting exchange (FIRE) to collect incident information from FIs and that authorities could use for information sharing.

This report reflects the public feedback received on the FIRE concept. It outlines the potential benefits, risks and costs, and discusses how the FSB will take forward the development of FIRE.



Financial Stability Board HPより