cybozu

クラウドセキュリティとオープンカルチャー

～サイボウズの取り組み、コミュニティ活動の価値～

松本 純 (Jun Matsumoto)

サイボウズ株式会社 セキュリティ室 / Cy-SIRT

日本シーサート協議会(NCA) 運営委員、地区活動委員

セキュリティ・キャンプ協議会 理事、副会長

cybozu

Q: 白浜シンポジウムに、どの様に来ましたか？

1. 出張（自分で予算を確保）
2. 出張（誰かが予算を確保）
3. 自腹（自己研鑽、旅行、趣味）
4. その他

お話しすること

- サイボウズのセキュリティの取り組み
  - 開発/運用での取り組み、認証/監査対応
  - セキュリティチェックの課題
  - 企業理念を踏まえたセキュリティ業務の取り組み
- コミュニティ活動の取り組みと思い
  - 日本シーサート協議会、セキュリティ・キャンプ協議会、OWASP KANSAI

cybozu

松本 純

(758254)

(010430)

- 北海道旭川市出身
  - 旭川高専 (システム)制御情報工学科
- 1994/4～ 株式会社カプコン
- 2022/4～ サイボウズ株式会社 セキュリティ室 / Cy-SIRT
- OWASP KANSAI 運営、IPA 情報セキュリティ10大脅威 選考会
  日本シーサート協議会 (NCA) 運営委員、地区活動委員
  セキュリティ・キャンプ協議会 理事、副会長
- 複業：セキュリティ対策のご支援、講演

cybozu

職歴1: 株式会社カプコン (1994/4～2022/3)

1994～	ゲームプログラム開発	開発
2001～	システム管理、オンラインサービス開発、ヘルプデスク	開発
2011～	セキュリティ（グローバルWebサイトのセキュリティ診断）	情シス
2013～	ゲームセキュリティ（チート/不正コピー対策）	開発
2015～	セキュリティ対策情報収集、CSIRT構築、NCA加盟	開発
2020～	インシデント対応、その後の対策強化	開発 セキュリティ

cybozu

職歴2: サイボウズ株式会社 (2022/4～)

2022～	セキュリティ監査対応（SOC2レポート：kintone.com）
	セキュリティ対策に関する情報収集、社内発信
	社外コミュニティ活動への参加、運営支援 日本シーサート協議会 (NCA)、セキュリティ・キャンプ協議会
	セキュリティに関する情報交換の場作り（SaaSセキュリティの会）
	…

cybozu

趣味など

- サイクリング（運動→食べて±0）
- コミュニティ勉強会/シンポジウム（参加+運営）、旅行
- 音楽鑑賞（クラシック、ジャズ、フュージョン、聖飢魔Ⅱ）
- 2022/8～、大阪/旭川の2拠点生活

サイボウズ 会社概要 (2023年12月末時点)

名称	**サイボウズ株式会社**（東証プライム 4776）
事業内容	**「グループウェア」**の開発・運用・販売
創業	1997年8月（愛媛県松山市にて3名で創業）
所在地	東京都中央区日本橋2-7-1 東京日本橋タワー
拠点	東京、札幌、仙台、大宮、横浜、名古屋、大阪、広島、松山、福岡 アメリカ, 中国, 台湾, ベトナム, マレーシア, オーストラリア, タイ
資本金	613百万円
業績	連結売上 25,432百万円 (経常利益 3,579百万円)
従業員数	連結 1,276名

サイボウズについて

会社の理念「チームワークあふれる社会を創る」

- チーム：共通の理想を持つ集団
- チームワーク：理想に向かって集団が行動すること
- **情報共有で チームメンバが「効率よく、楽しく」働ける**
  →チームワークがあふれている状態、そんな会社を増やしたい！

kintone　Garoon

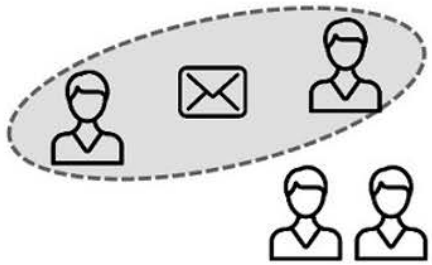
サイボウズ Office　メールワイズ Mailwise

「情報伝達」と「情報共有」

cybozu

情報伝達

相手を選んで、情報を伝達する。
それ以外の人は情報を知らない。



メール、メッセンジャー、ビデオ会議など

情報共有

プライバシーとインサイダーを除き、
すべての情報を共有する。

グループウェア、社内SNSなど

情報格差は、権力差や対立、組織の壁、経済格差を生む。
情報格差をなくすことで、一人ひとりの主体性を引き出せる。

https://japan.zdnet.com/article/35150903/2/

サイボウズ 災害支援プログラムとは？

https://cybozu.co.jp/efforts/disaster-support/

支援内容： 災害復旧・復興のための活動に、サイボウズが提供する
すべてのクラウドサービスを**半年間無償提供**

対象　： 災害の復旧・復興に関わる団体

支援内容　： **約20社のパートナー**による連携サービスや構築支援を提供

パートナー　：

※一部抜粋

支援内容： **被災地や遠隔地からのリモートでIT支援**
（システム構築、データ整備、IT機器の無償提供　等）

メンバー　： サイボウズの社員約40名が所属（2024年3月末時点）

https://news.mynavi.jp/article/newsinsight-279/

kintone

cybozu

利用者コミュニティを盛り上げる活動

- 利用事例や活用アイディアを組織を超えて共有
- 導入事例、業務改善プロセス、失敗や工夫から学ぶ
- 100社あれば100通りの使い方

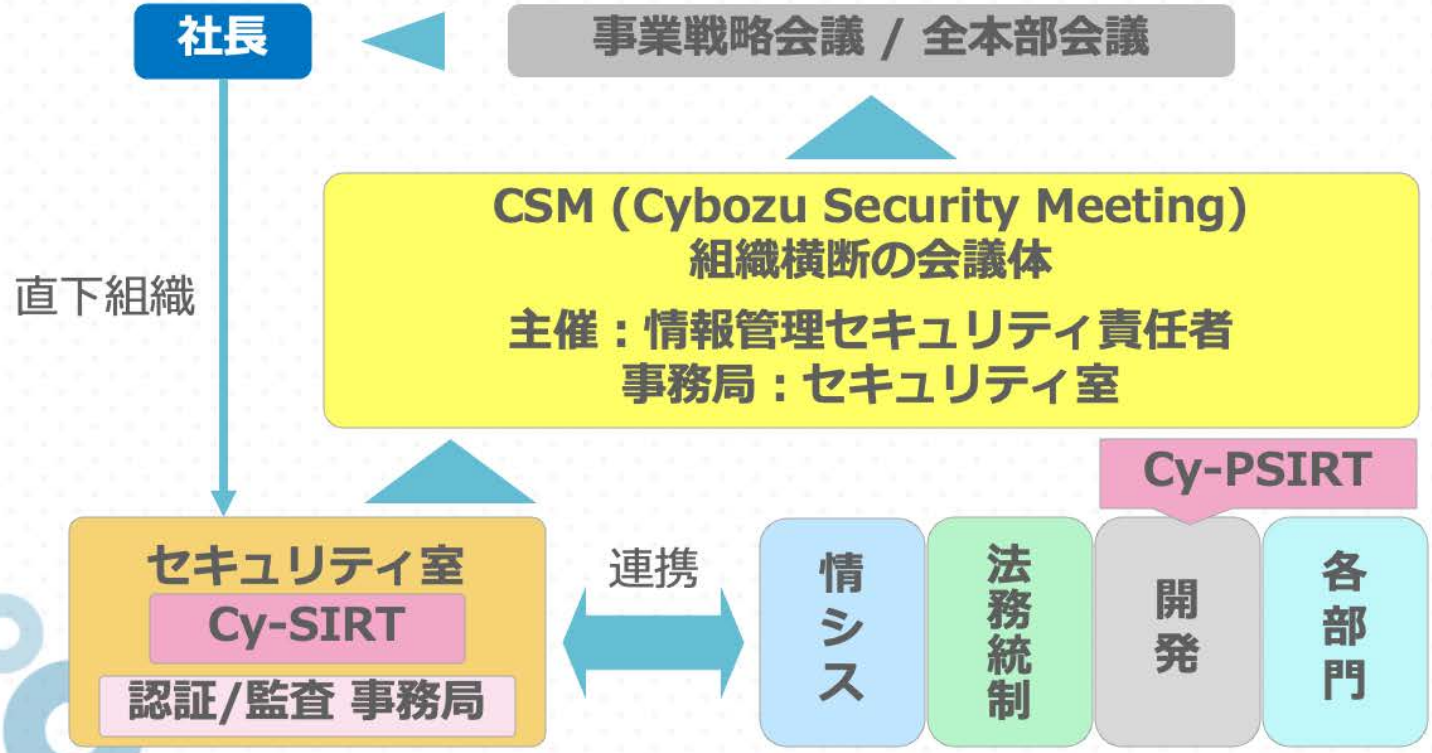
kintone hive

セキュリティに関する体制 経緯

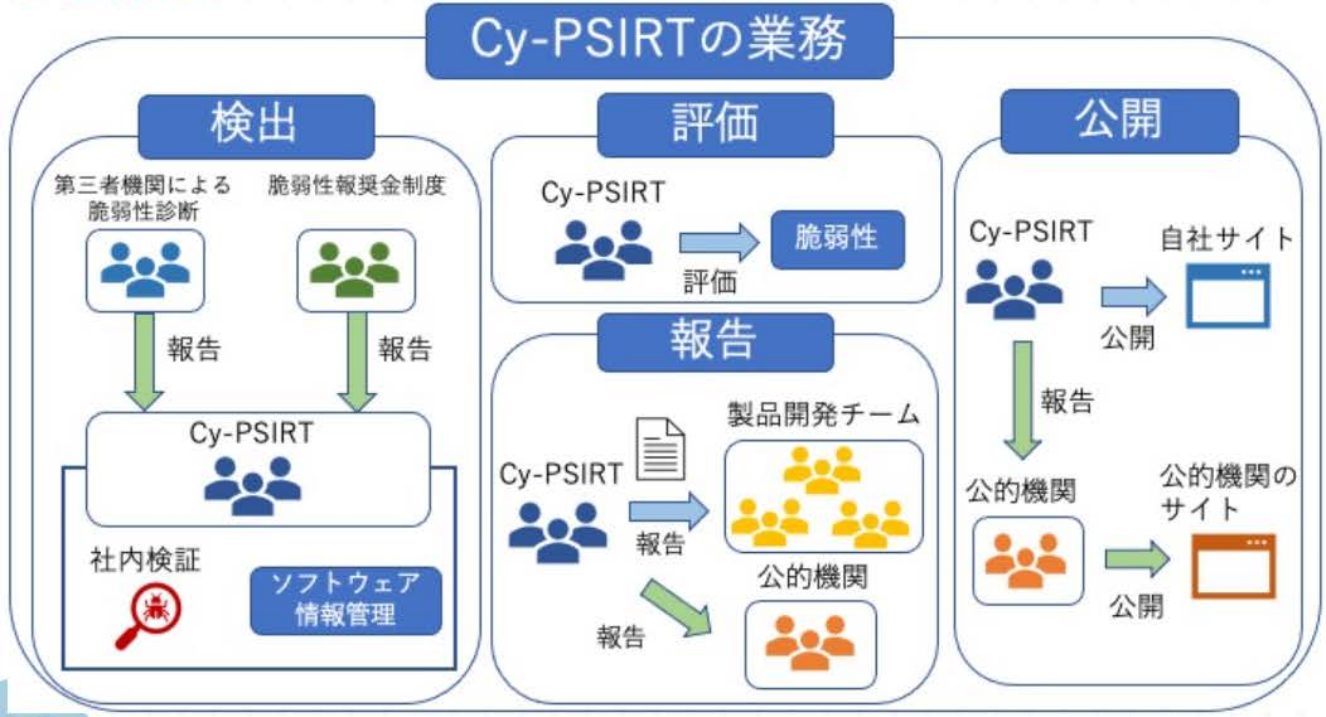
Cy-SIRT

2002年	製品の脆弱性ハンドリングを開始
2006年	PSIRTを設立 組織的に脆弱性に取り組む体制を構築
2011年	クラウドサービスをリリース（cybozu.com） PSIRTを強化しCy-SIRTに（製品+全社のセキュリティ）
2016年	セキュリティ室（全社セキュリティ）を新設 社員教育、社内からの相談窓口、セキュリティマネジメント(認証/監査)

セキュリティに関する体制



Cy-PSIRT



https://blog.cybozu.io/entry/2021/10/08/170000

cybozu

脆弱性報奨金制度（バグバウンティ）

- 善意のエンジニア（バグハンター）の多様な視点による検証
- 報告内容を知見として蓄積、製品の堅牢化に活用
- 2014年スタート
  - 報告1,715件、711件認定、報奨金約6,350万円 (2023年まで)
- バグハンターコミュニティの活性化にも注力
  - ポイント・ランク制度、バグハンター合宿

https://cybozu.co.jp/products/bug-bounty/

脆弱性報告および認定をリアルタイムで行う「サイボウズ バグハンター合宿 2023」結果発表

9名の社外バグハンターが参加。2日間で52件の脆弱性を報告、うち36件を認定

2023.11.20　サイボウズ株式会社

ポスト　シェアする 0　ダウンロード（1.6 MB）

サイボウズ株式会社（本社：東京都中央区、代表取締役社長：青野慶久、以下サイボウズ）は、2023年11月18日（土）～19日（日）の2日間で行われた、kintone（キントーン）、Garoon（ガルーン）などのサイボウズ製品の脆弱性報告および認定をリアルタイムで行う「サイボウズ バグハンター合宿 2023」において、52件の脆弱性が報告され、うち36件が認定されたことをお知らせいたします。

https://topics.cybozu.co.jp/news/2023/11/20-18568.html

ソフトウェア情報管理（OSS管理）

- 開発チームから、OSS利用一覧をPSIRTに提出
- PSIRTでOSS管理台帳を作り、日々アップデート情報を監視
  - 新しいバージョン、脆弱性情報、 EOLチェック…
- 以前は手動対応で毎月45人月、今はツール活用で10人月
  - ツールを最大限活用し、効率よくセキュリティ業務を行う

yamory 脆弱性管理クラウド

ログイン お問い合わせ 資料ダウンロード

サービス詳細 導入事例 セミナー ブログ お知らせ よくあるご質問 セキュリティ個別相談

サイボウズ株式会社様

yamoryがない状態には戻りたくない。OSSの脆弱性管理工数を月35人日削減

https://yamory.io/case/cybozu

セキュリティ室 (Cy-SIRT) 業務

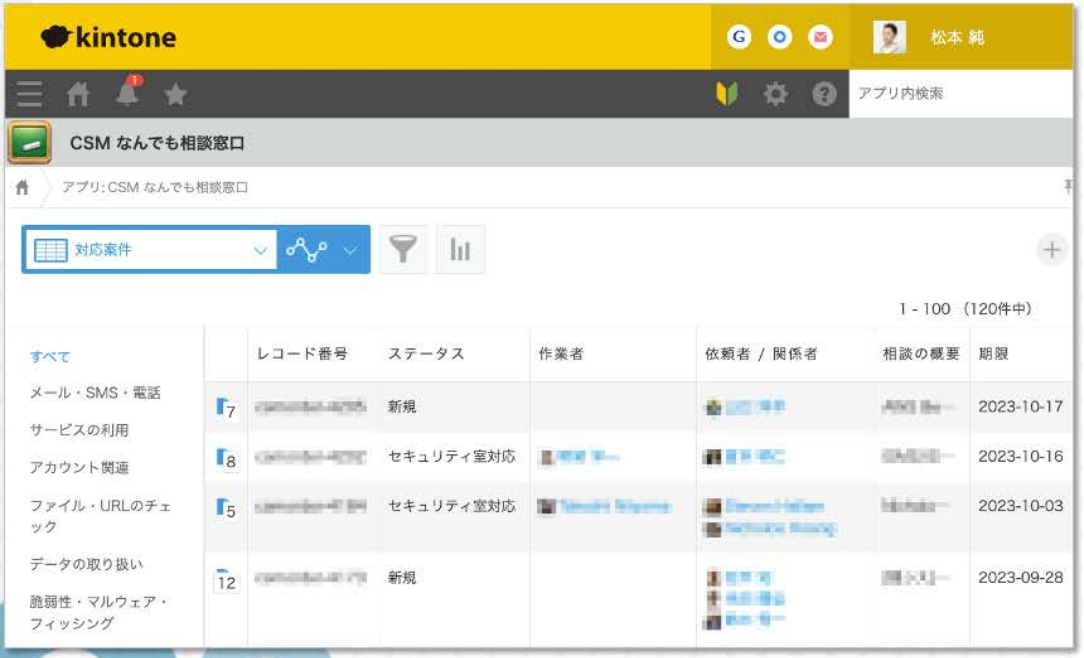
セキュリティに関する**専門知識**に基づき、
各事業部で行うセキュリティ施策に対して**支援**する

インシデント対応支援	セキュリティ情報収集	外部機関との連携
セキュリティ教育	セキュリティ相談会議運営	セキュリティマネジメント

セキュリティ室 認証/監査 対応

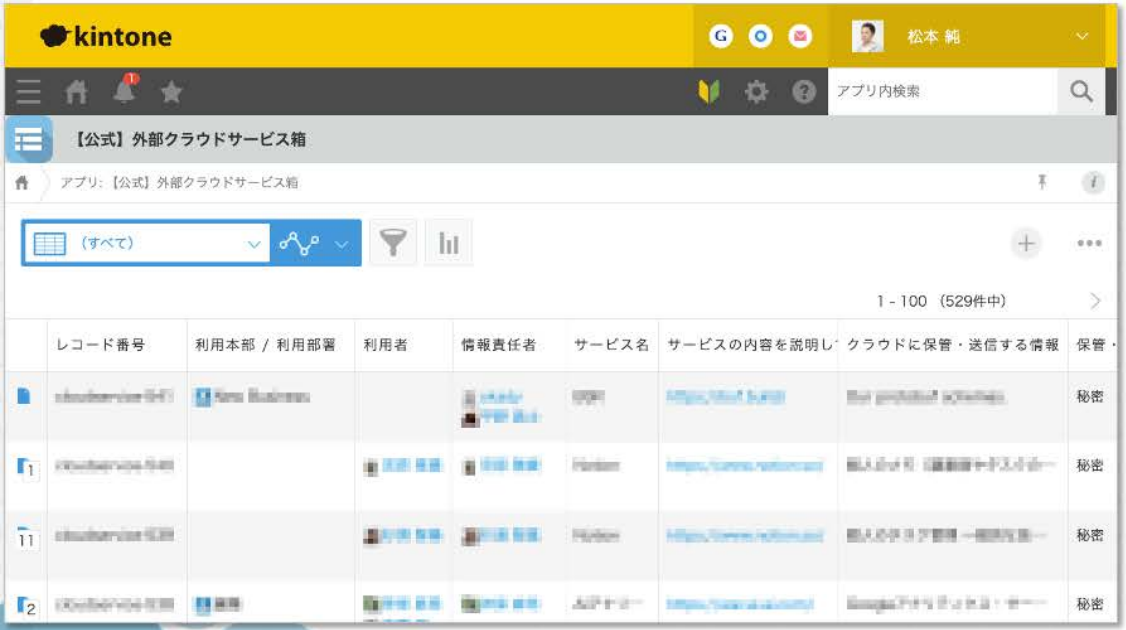
- ISMS
  - 2011年、ISO 27001 取得
  - 2019年、ISO 27017 取得（クラウドセキュリティ認証）
- ISMAP
  - 2021年、ISMAPクラウドサービスリストに掲載
- SOC2
  - 2023年、SOC2 Type1報告書 受領

業務効率化 事例1: セキュリティ相談窓口



- セキュリティルールの確認
- インシデントかも…
- 怪しいメールの受信
- ISMSやISMAPについて確認
- クラウドサービス利用相談

事例2: クラウドサービスの利用申請、管理



- 利用したいサービスの申請
  - セキュリティチェック実施
  - 利用判定
- 管理台帳→棚卸にも

事例3: 認証/監査対応

- 監査法人とのやりとりをkintoneスペースに集約
  - 記述内容の検討
  - 証跡の提出、確認

作り易い&使い易いアプリで、効率的に管理する

- ノーコードツールで、簡単にWebアプリを作れる
  - 例：申請→承認（ワークフロー）→記録（データベース）
    - 過去の申請内容を蓄積/公開→簡単に申請できる or 自己解決
    - そのまま管理台帳に、棚卸もアプリで簡単に（確認記録を残す）
- **日々使いながら、容易に改善できる**
- **業務を効率化し、より良いセキュリティ施作を提供**

現場で開発できる vs ガバナンスの課題

- ノーコードツールは、業務担当者自身が業務に必要なシステムを容易に開発できる
- 一方で利用部門や対象業務が増えると、アプリの品質確保やリスク管理のためのルールやガバナンスが課題に…

cybozu

kintone ガバナンスガイドライン

利用状況や会社の組織/風土を踏まえ、攻めと守りのバランスを考慮したガバナンスをどの様に構築するか、ポイントを紹介

https://kintone.cybozu.co.jp/jp/governance_guideline/

cybozu

セキュリティチェックシート 利用目的

- 発注元が委託先のリスクアセスメントを行い、リスクに応じた使い方を意思決定する（自社ポリシとの適合/乖離をチェック）
  - クラウドサービス事業者として
    - お客様に、サイボウズのクラウドサービスを利用いただく際に
  - クラウドサービス利用者として
    - サイボウズ社員が、他社クラウドサービスを利用する際に

セキュリティチェックシート 対応方法

- クラウドサービス事業者のドキュメントを調査し **自分で記入**
- 自社のチェックシートをクラウド事業者に送り **回答を依頼**
  - セキュリティの取り組みや、標準的なチェックシートを公開し、認証/監査を受けていても…
- セキュリティ評価サービスの活用

cybozu

標準セキュリティチェックシートを公開、評価サービスを案内

- **経済産業省：クラウドサービス利用のための情報セキュリティマネジメントガイドライン**

  経済産業省が発行する「クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年版」をもとに、よくある質問などを追記したチェックシートを公開しています。

  ダウンロード

- **セキュリティ評価プラットフォーム「Assured（アシュアード）」**

  サイボウズのクラウドサービスのセキュリティ情報は、クラウドサービスのリスク評価情報を集約するプラットフォーム「Assured（アシュアード）」からもリクエストいただけます。

  セキュリティ評価をリクエスト

https://www.cybozu.com/jp/

経済産業省 ガイドライン版（抜粋）

1 情報セキュリティのための方針群			
1	経営陣によって承認された情報セキュリティに関する基本方針を定めた文書があること。また、該当文書を全従業員及びクラウドサービス利用者に明示すること。	○	経営層に承認されたクラウドサービスに関するセキュリティの基本方針（https://www.cybozu.com/jp/terms/security.html）及び社内セキュリティに関する従業員が遵守すべき社内規程（情報セキュリティ規則等）を定めております。 当方針は、全従業員には、社内規程として周知し、クラウドサービス利用者には、当社ホームページに公開しております。 ▼ISMS基本方針 https://www.cybozu.com/jp/terms/security.html
2	情報セキュリティに関する基本方針を定めた文書は、定期的またはクラウドサービス提供に関係する重大な変更が生じた場合に、レビューすること。	○	情報セキュリティマネジメントシステム（以下、「ISMS」）を構築し、情報セキュリティ保全活動を効果的に推進するために、クラウドサービスに関するセキュリティの基本方針を定め、定めた通りに実施運用し、監査及び見直しを行う仕組みを確立しております。 また、経営層によって承認されたクラウドサービスに関するセキュリティの基本方針は、ISMSにおいて、経営者によって毎年及び重大な変化が発生した場合に見直しております。
2 情報セキュリティのための組織			
1 内部組織			
1	経営陣は、情報セキュリティに関する取り組みについての責任及び関与を明示し、組織内におけるセキュリティを積極的に支持・支援を行うこと。	○	当社グループの内部統制についての基本方針にて、経営者、監査役、従業員の行動指針を明らかにし、クラウドサービスに関するセキュリティの基本方針にて、業務に携わる役員、社員が継続的に情報セキュリティ対策を推進することを宣言しております。 ▼内部統制の基本方針 https://cybozu.co.jp/company/internal-control/ ▼ISMS基本方針 https://www.cybozu.com/jp/terms/security.html また、情報セキュリティマネジメントシステム（以下、「ISMS」）を構築し、情報セキュリティ保全活動を効果的に推進するために、クラウドサービスに関するセキュリティの基本方針を定め、定めた通りに実施運用し、監査及び見直しを行う仕組みを確立しております。 さらに、当社経営層によって承認されたクラウドサービスに関するセキュリティの基本方針は、ISMSにおいて、経営者によって毎年及び重大な変化が発生した場合に見直しております。

- 組織
- 開発体制
- 運用体制
- 法律対応
- 利用規約
- その他

セキュリティチェックシート 事業者の対応

そもそも、サイボウズにおいてセキュリティチェックシートによる課題とは、どのようなものだったのだろうか。この点について萩澤氏は以下のように説明する。

「当社では お客さまとのセキュリティチェックシートのやり取りが2018年に260件、2019年に360件、2020年に420件、2021年には480件 と年々増加の一途をたどっていました。また、設問数は多いものだと500問ほどあり、必ずしもクラウドサービスのセキュリティチェックではない観点も含まれていました。さらに、納期も短いほか、即答できる体制を整備することは難しく、回答方法も設問によっては他部署とのコミュニケーションが必要となるなど、煩雑になっていました。3～4人で対応していましたが、私自身も専門の職種ではないため他のメンバーに継続してもらうのは大変だと感じていました」（萩澤氏）

https://news.mynavi.jp/techplus/article/20220804-2414576/

セキュリティチェックシート 悩み

事業者

- 認証を取得したり、標準的なチェックシートなど様々な情報を公開しているが、各社のチェックシートへの記入を求められる

利用者

- セキュリティチェックシートの回答を断られる場合もある
  - ○○万USD 以上の契約なら対応します
  - チェックシートの回答は有料です（良い取り組みかも…）

セキュリティ評価サービス

- 事業者
  - 評価サービスのチェックシートに一度回答することで、複数の利用者からの問い合わせに対応できる
- 利用者
  - セキュリティ評価の開示をWebから申請、結果を閲覧
  - よくある項目はほぼある→簡単に自社シートにマッピングできる

セキュリティ評価プラットフォーム「Assured」、サイボウズ株式会社の活用事例を公開

～Assuredを活用したセキュリティ情報開示で、セキュリティチェック対応工数25%削減～

・通常業務の傍らで、年間500件以上、月150時間のセキュリティチェックシート対応に追われる

・外部からのセキュリティ情報開示依頼機能の追加により、多くの企業への広がりを期待

・セキュリティチェックシートの課題に対する社会の注目の高まりが利用の後押しに

・Assuredによりセキュリティチェック対応工数25%削減を実現

・Assuredを通じたセキュリティ情報開示・取得が当たり前の世の中になってほしい

・自社サービスのセキュリティ向上にも寄与

https://prtimes.jp/main/html/rd/p/000000632.000034075.html

cybozu

企業理念 (Purpose, Culture)

公明正大

理想への
共感

多様な
個性を重視

自立と議論

チームワークあふれる
社会を創る

チームの生産性と働く人の幸福度を両立するチームワークを
ITツールによって実現し、世界中に広げていくこと。
それがサイボウズの目指す理想であり、存在意義です。
存在意義を支える基盤として、4つの文化というものがあります。
これはサイボウズのメンバーが共通して重視している価値観で、
採用のカルチャーフィットを測る基準にもなっています。

https://cybozu.co.jp/recruit/about/philosophy/

セキュリティの業務も企業理念に沿って

理想への共感

- 「規則なのでダメです！」で済まさず、**自主的に実施してもらえるように**

多様な個性の重視

- さまざまな**業務形態、働き方**に応じた対応

公明正大

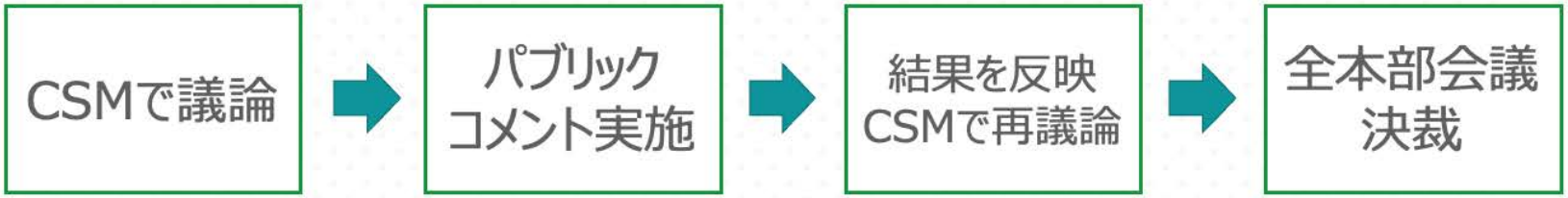
- **インシデント報告してくれたことを尊重**、報告し易い空気を醸成

自律と議論

- **幅広く議論**して、ルールやセキュリティ対策を検討

関係者だけでルールを定めず、社員から意見を求める

- 社員の利便性、業務の可用性を重視
- 社員の**セキュリティ施策への共感を高める**ことが重要



まとめ：セキュリティの取り組み

- 効率的なOSS管理、外部知見を得る（バグバウンティ）
- セキュリティチェック、認証/監査対応を効率化したい！
  - 基準の異なる複数の認証/監査、しかも毎年更新…
  - セキュリティチェック、より効率的な手法に変えていきましょう！
- オープンなカルチャーで組織を変える！
  - 失敗を隠さず 正直に報告できる風土（公明正大）
  - セキュリティ部門だけでルールを決めない

外部セキュリティ団体への参加、情報共有

IPA

JPCERT CC

CSIRT
日本シーサート協議会

JNSA

ISOG-J

一般社団法人
ソフトウェア協会

SECURITY CAMP

SecHack365
SECURITY+HACKATHON 365 DAYS

フィッシング対策協議会
Council of Anti-Phishing Japan

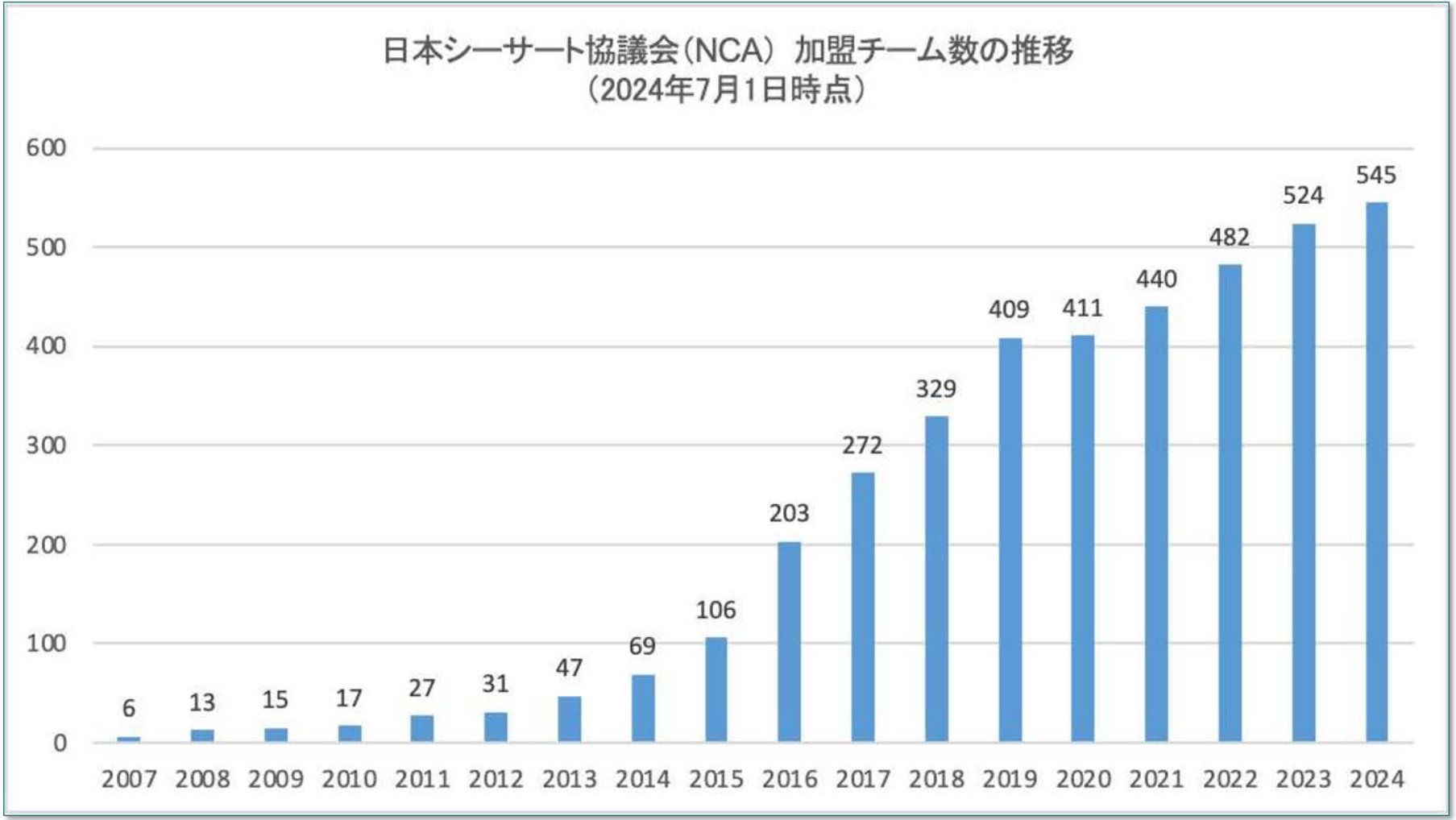
- 他にも、地域のIT/セキュリティイベントの協賛、参加

なぜ外部団体と積極的に交流するのか？

- セキュリティインシデントは、自社だけで対応することが困難
  - 攻撃手法の多様化・高度化・複雑化
  - 1社で蓄積できるノウハウは限られている
  - **万一のインシデント対応には、組織を超えた連携が必要**
- 各組織の経験やノウハウを共有し、効果的なセキュリティ対策に活用 →皆で底上げを図りたい！

日本シーサート協議会 (NCA)

- https://www.nca.gr.jp/
- セキュリティ対策の情報交換、共助の場
  - 年会費：従業員1000名未満 6万円、1000名以上 12万円
  - 入会金：3万円
- 他組織のセキュリティ対策やインシデント対応事例、WG成果物を、自組織のセキュリティ対策に効率よく活用
- **地域/組織を超えて、同じ課題と戦う仲間や専門家と知り合う場**


日本シーサート協議会（NCA） 加盟チーム数の推移
（2024年7月1日時点）
600
500
400
300
200
100
0
6
13
15
17
27
31
47
69
106
203
272
329
409
411
440
482
524
545
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024

セキュリティ・キャンプ 協議会

- 「とがったセキュリティ人材」を発掘・育成する事業
  - 2004年から20年続く
- 12～22歳の生徒/学生が、選考を経て受講
- 現役技術者が直接指導、法律や倫理も教える
- 全国大会（夏期 6日間）
- 地方大会（2024年 13回）

cybozu

セキュリティ・キャンプ 協議会 ミッションステートメント

良い仲間と出会えるコミュニティを大切にします

- 高い技術と、技術を正しく使う倫理を育む
- ダークサイドに落ちない、「良い仲間」と繋がる

持続・発展させるためのエコシステムの形成を目指します

- 受講生が講師や運営メンバに、講師同士も交流し学ぶ
- 地域/組織を超えた育成の場

サイボウズとセキュリティ・キャンプの関わり

- スポンサー（2013年～）
  - グループウェア 無償提供 (kintone)
- 講師
  - **7名**
- 受講生の入社（全国大会+地方大会）
  - **9名（PSIRT、開発、運用、採用）**

cybozu

セキュリティ・キャンプ 多くのスポンサーに支えられてます！

OWASP (Open Worldwide Application Security Project)

セキュリティに関する課題を解決する国際的コミュニティ

アメリカ政府認定NPO、世界中に200以上の支部

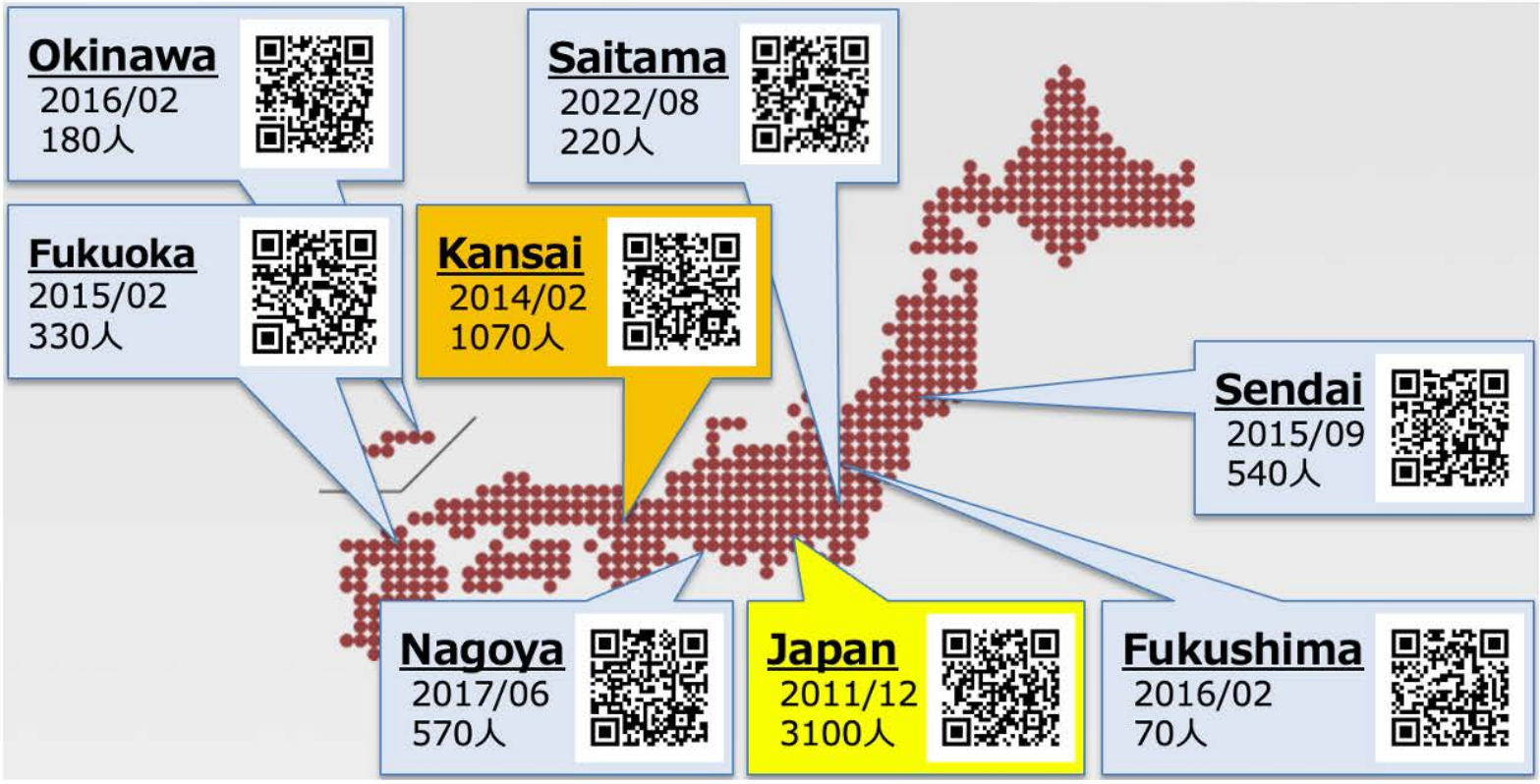
OWASP KANSAIは、日本で2番目に発足した支部

2014年3月から大阪・京都・神戸・奈良で勉強会を開催（10年間で30回～）

Webアプリ、モバイル、IoT、LLMなどの開発/利用で
注意すべき脆弱性と対策をまとめたドキュメント
https://owasp.org/Top10/ja/

みんなの力で Open
世界中で Worldwide
つくられたもんの Application
セキュリティを Security
何とかする活動 Project

OWASP 日本国内に8支部



各地域に、組織を超えてセキュリティの相談できる場がある！

コミュニティ活動 参加のメリット

- **組織を超えて相談/研鑽できる仲間と出会える**
  - 1人セキュリティ担当で、社内に相談できる人が居ない…
- 効果的な情報収集
  - 幅広い業界との意見交換、同業他社とのベンチマーク
- LTや発表で、資料作成・プレゼンに慣れる

コミュニティ活動 運営に加わるメリット

- **組織を超えて相談/研鑽できる仲間と出会える**
- イベント企画/運営を経験できる
  - 企画、調整、告知、集客、設営、受付、司会、進行
- コミュニティ運営＝組織運営
- 本業以外での満足感、充実感

テーマと趣旨

第28回サイバー犯罪に関する白浜シンポジウム テーマ

激変する環境、複雑化するサイバー犯罪にどう立ち向かうのか？

≪趣旨≫

閉域網に守られて安全だったはずの工場や病院などがコロナ禍で加速したクラウド化により見えないところでインターネットと接点をもち、ランサムウェアなどによるサイバー攻撃の被害を受けています。
自治体情報セキュリティクラウドと3層の分離・分割で守られてきた自治体では、αモデルからβ、β'モデルへの移行や、LGWANからのインターネット接続へという変化がおきています。
また現場部門主体のDXによるクラウド活用の副作用として情報システムがシャドウIT化し、情報システム部門のコントロールの外に置かれてしまうという事態が発生しています。
さらに生成AIの登場は業務の効率化に資する一方、思いがけない情報漏洩、フェイク情報の生成、詐欺行為への活用を始めとする「サイバー犯罪の効率化」という大きな環境の変化をもたらしました。
今回のシンポジウムではこのような環境の激変に伴う、サイバー犯罪の複雑化にどう立ち向かうのか、その現状と将来について議論します。

過去開催

第26回開催
第25回開催
第24回開催
第23回開催
第22回開催
第21回開催
第20回開催
第19回開催
第18回開催
第17回開催
第16回開催
第15回開催
第14回開催
第13回開催

「コンピュータ犯罪に関する白浜シンポジウム」の思い出

帝塚山学院大学情報メディア学
科特任教授　中野秀男

2018年5月27日

1997年5月に始まった白浜のコンピュータ犯罪シンポジウムも時代の流れで名称も変え、コンテストも併設されるなど益々盛んになっている。事務局の臼井さんから思い出話を書いて欲しいと言われたので、今年も過去招待講師として招待されたので、そのお礼も兼ねて、過去のメールやパワポを探し出しながら書いてみたい。シンポ以外に話を盛ってねと依頼されたので、中野流でパラパラと書いてみます。

まとめ：コミュニティ活動を繋いでいく、広げていく

- 白浜シンポジウムのコミュニティ、日本のセキュリティ担当者のコミュニティを広げていきましょう！
  - 組織、地域、世代を超えて
  - 所属組織でも、世代や部署、異動を越えて
    - 予算化、思いを伝える
- **白浜で、気軽に相談できる仲間を増やしていきましょう！**

cybozu

宣伝：コミュニティ活動にオフィスを貸し出します

サイボウズ セキュリティ室 X (Twitter)

- https://twitter.com/CybozuSecurity
- 少人数で頑張るCSIRTを応援したい
  セキュリティの仕事にチームワークを！
- セキュリティ業務や今関心のあるトピックを発信
- セキュリティに興味を持ってもらいたい、事業会社のセキュリティチームの活動を知ってほしい