# CSIRT MT

## セキュリティインシデント管理を
## 効率化するCSIRT MT

～クラウド型で早期にインシデント管理が可能に～

**CONFIDENTIAL**

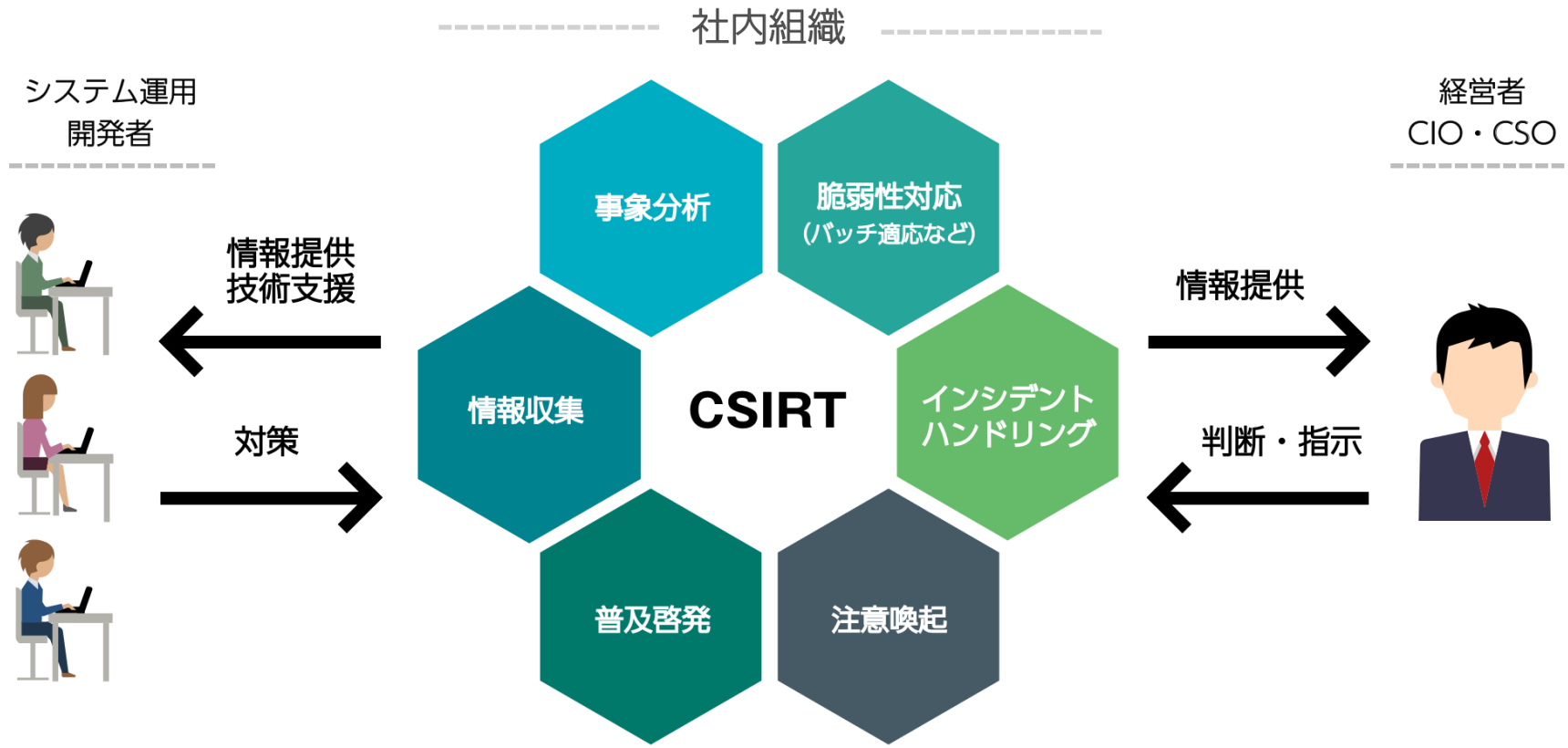


GRCS™

# CSIRTとは

CSIRT MT

シーサート (CSIRT: Computer Security Incident Response Team) とは、コンピュータセキュリティにかかるインシデントに対処するための組織の総称です。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をします。（日本シーサート協議会Webサイトより）




GRCS

# CSIRTの必要性

CSIRT MT

セキュリティ対策の考え方を以下5つの機能と定義した場合、従来型セキュリティ 対策は「防御」を主体とした位置付けになります。 今後のセキュリティ対策は、「検知」以降の技術的対応体制の構築を行いますが、前提として守るべき資産の特定等、各組織で「特定」に対する検討が必要です。


- 資産管理
- ビジネス環境
- ガバナンス
- リスクアセスメント
- リスク管理戦略

- アクセス制御
- 意識向上およびトレー ニング
- データセキュリティ
- 情報を保護するための プロセスおよび手順
- 保守
- 保護技術

- 異常とイベント
- セキュリティの継続的なモニタリング
- 検知プロセス

- 対応計画の作成
- 伝達
- 分析
- 低減
- 改善

- 復旧計画の作成
- 改善
- 伝達

引用元：重要インフラのサイバーセキュリティを向上させるためのフレームワーク 1.0版
米国国立標準技術研究所 (National Institute of Standards and Technology)
https://www.ipa.go.jp/security/publications/nist/ 従来型セキュリティ対策 CSIRTで明確化される対策

GRCS

# CSIRT機能を支援するソリューション群

CSIRT MT

多くの企業が整備できていない、CSIRTに必要な各種機能をご提供いたします。

| CSIRTの機能として備えている項目 | 実装割合 | 対応ソリューション名 |
|---|---|---|
| インシデントに対する初動対応 | 41.6% | CSIRT MT |
| インシデントの調査及び分析 | 40.6% | |
| 外部機関や関係者への連絡・調整 | 29.9% | |
| 再発防止策の策定 | 28.7% | |
| 脆弱性情報ハンドリング | 50.6% | CSIRT MT ＆ 脆弱性TODAY |
| 情報セキュリティ関連情報の収集・分析 | 72.6% | 脆弱性TODAY |
| セキュリティ監査・評価 | 66.6% | アセスメントサービス |
| セキュリティツールの管理・運用 | 55.4% | SOCサービス |
| インシデントの検知 | 44.4% | |
| 情報セキュリティ対策に関する教育、啓発 | 55.1% | 教育サービス |
| 訓練・演習の実施 | 33.4% | 教育・演習サービス |
| 社内外からのインシデント報告窓口 | 38.2% | |
| 社外組織との連携窓口 | 31.4% | |
| インシデント後の対外公表、法的対応 | 26.4% | |

GRCS

IPA：企業のCISOやCSIRTに関する実態調査2016 ― データ集 ― より

# CSIRTMTのご紹介と
# インシデント管理の効率化

# 製品コンセプト

CSIRT MT

これからの組織にとってクリティカルなCSIRT運用を

## 高度化・自動化・見える化します

製品監修　満永拓邦氏
（一般社団法人CSIRTトレーニングセンター　代表理事）

CSIRTの運用において組織内のインシデント対応状況の共有や、脆弱性情報の管理は不可欠な機能です。それらの機能を併せ持つ「CSIRT MT」の展開は、CSIRTの対応能力の向上に大きく寄与するものと期待しています。

GRCS

# CSIRT MTが解決する課題

CSIRT MT

- インシデント対応の整備ができていない
  - 対応フローが未整備、要員により品質が異なる、再発防止策の検討が不十分

→ 実用的な管理項目とフローによる品質の統一化

- 脆弱性情報への対応が追いついていない
  - 自社資産とのマッチングが大変、対応のトラッキングができていない

→ 要対応の脆弱性が自動表示・サーバ単位で進捗管理が可能

- 経営層・グループ会社・グローバルの子会社との情報共有
  - 情報の吸い上げが出来ていない、地域・時差・言語の壁

→ ダッシュボードでリアルタイム表示、クラウド・多言語対応

- Excel・メールベースでのやりとりのため情報がバラバラ
  - 対応のスピードが落ちる、情報の蓄積とナレッジ化が出来ていない

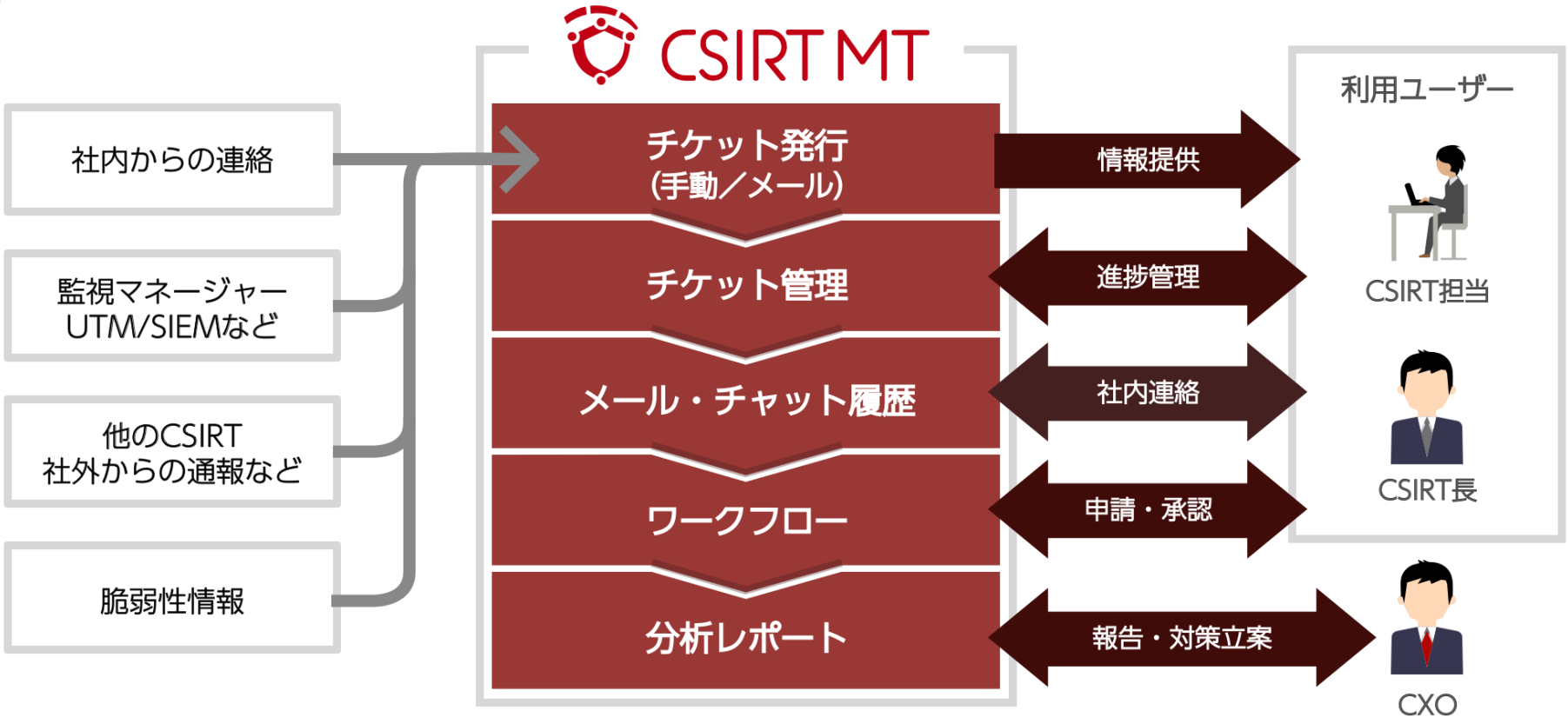
→ メール自動連携、関連チャット・メールの一括管理

GRCS

# CSIRT MTのご利用イメージ

CSIRT MT

CSIRTやSOC運用に最適化した、チケット管理と情報共有のための
クラウドアプリケーションです。




GRCS

# CSIRT MTの導入効果

CSIRT MT

## 高度化と工数削減

インシデントと脆弱性のハンドリングに関わるCSIRT運用品質の高度化と工数・対応時間削減

## 情報共有

ダッシュボードにより状況が一目瞭然。個々のシステムの対応状況もリアルタイムで把握可能。

## カスタマイズ

対応ステップを自社用にカスタマイズし必要な承認やメールの送信内容も自由に設定可能

## サンプルの実装

実用的なインシデント対応のチェックリスト等をサンプルとしてご提供*

## 簡単な導入

クラウドサービスの為サーバ等の準備やインストールが不要。グローバル対応（日/英）。

## レポート出力

CSIRTの運用状況について、独自の切り口で自由にカスタマイズしてレポートを作成可能

脆弱性TODAY

**連携**

脆弱性TODAYとの連携で自社資産に関連する脆弱性情報がリアルタイムに更新*

*CSIRT MTのライセンス費用に加えて別途ご購入が必要となります。

GRCS

# サービス提供形態

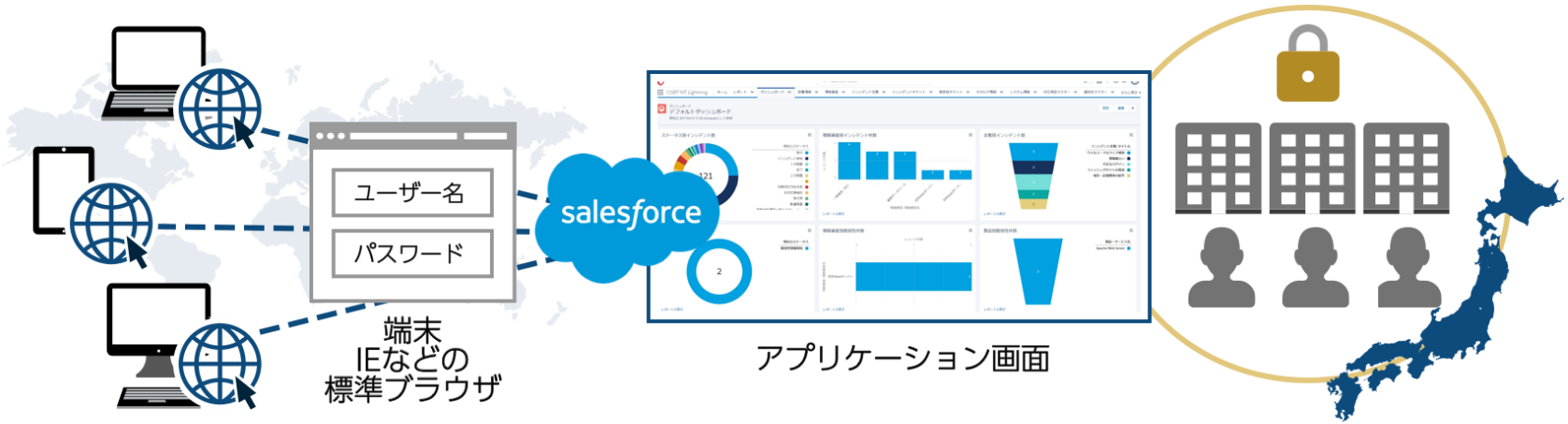
CSIRT MT

エリア

普段お使いのWebブラウザから海外など離れた拠点からも利用可能です。

セキュリティ

お客様環境（組織）ごとにデータやユーザは区分され、セキュリティ面も心配はありません。データも日本国内のデータセンターに保管されます。




プラットフォーム

株式会社セールスフォース・ドットコムが提供するプラットフォームである、「Salesforce App Cloud」上で動作します。

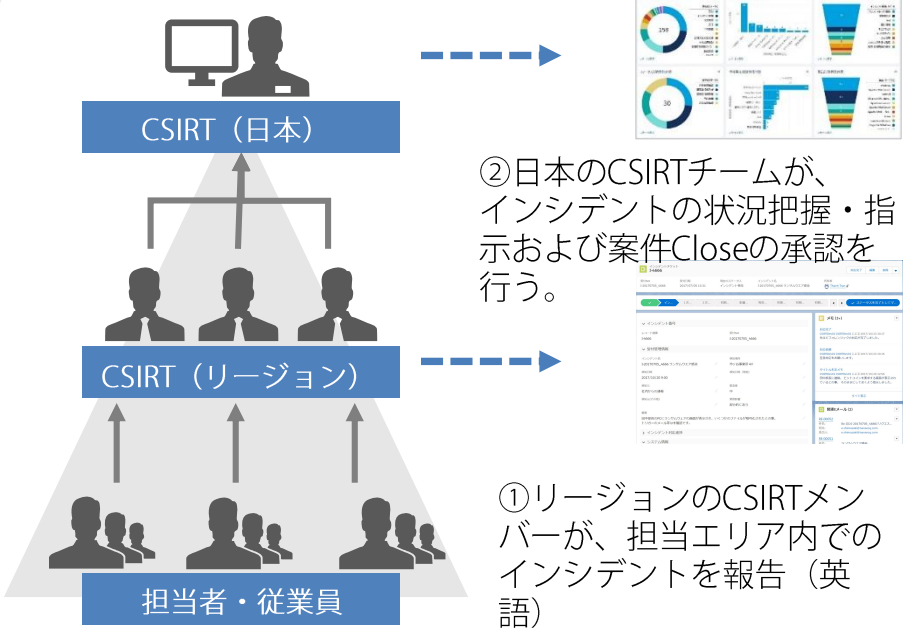
GRCS

# 事　例

# ユースケース

CSIRT MT

## A. グローバル企業（インシデント対応）



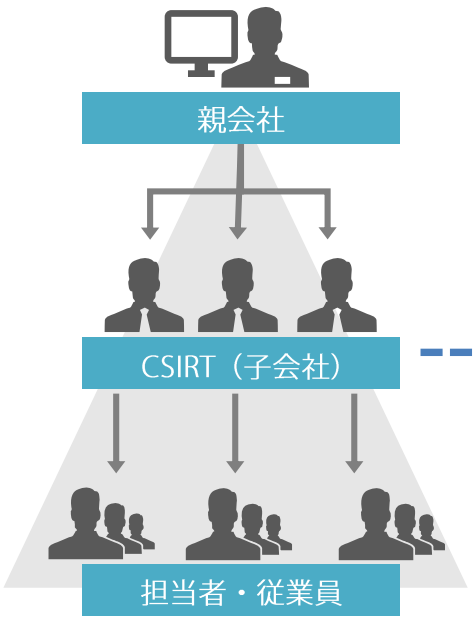



②日本のCSIRTチームが、インシデントの状況把握・指示および案件Closeの承認を行う。



①リージョンのCSIRTメンバーが、担当エリア内でのインシデントを報告（英語）

## B. グループ企業（脆弱性対応）




①親会社から定期的に脅威情報・脆弱性情報を提供

②子会社で各情報に対して、自社での該当有無と、対応の進捗確認を実施し、親会社に報告。

GRCS

# 機能詳細

# インシデント管理機能

CSIRT MT

インシデント対応における調査項目を網羅したチケット管理をメインに、関係者への通知、行うべき項目のチェックリスト、進捗状況やファイルを随時追記していくメモ＆添付ファイル等の必要機能をすべて一元化しています。



GRCS

# 脆弱性情報管理機能

CSIRT MT

日々発表される脆弱性情報や脅威情報をチケットとして登録し、システム構成情報とマッチしたチケットに対して、パッチ適用などの対策の進捗を管理。該当IT資産や承認者への承認依頼、関係者への通知等の機能をすべて一元化します。

脆弱性チケット
製品・サービス名が有効の脆弱性チケット

42 個の項目・並び替え基準: レコード連番・検索条件: 製品・サービス名が有効の脆弱性チケット・最終更新 数秒前

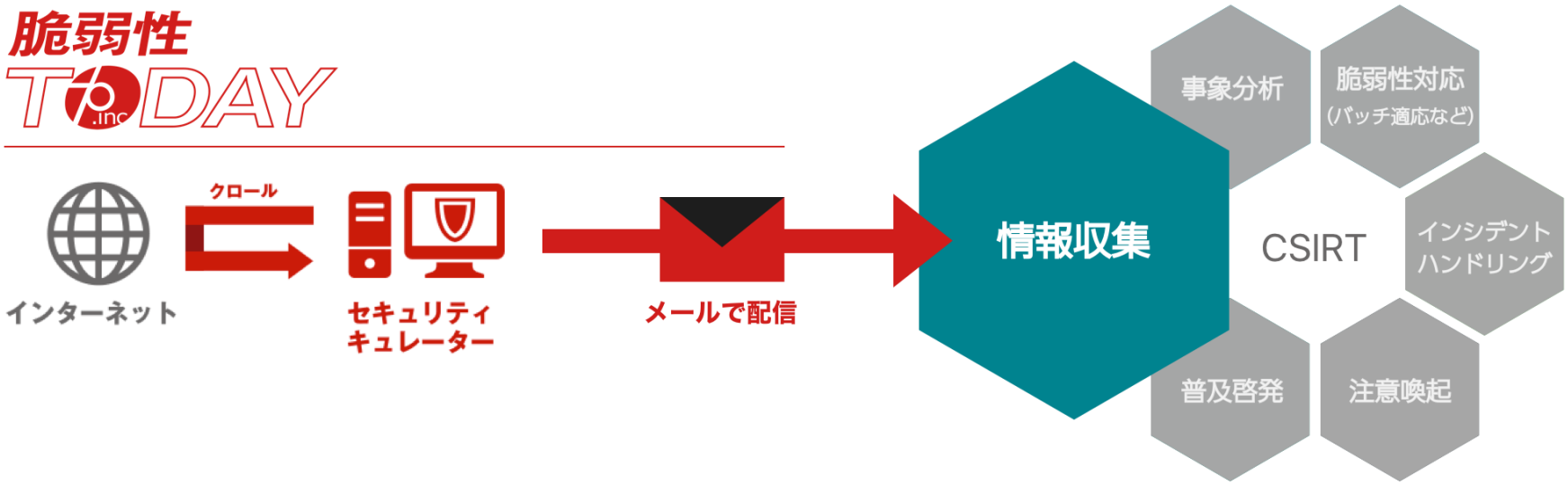
| | レコード連... | 脆弱性名称 | 製品・サービス名 | 現在のステータス | 最終更新日 |
|---|---|---|---|---|---|
| 1 | VT-0002 | ECサイトに攻撃が検出された | アマゾンサイト | 脆弱性情報入手 | 2017/05/1( |
| 2 | VT-0989 | Google Android Qualcomm コンポーネントにお.. | Android | 対応依頼 | 2017/04/2( |
| 3 | VT-1001 | Google Android Qualcomm コンポーネントにお.. | Android | 脆弱性情報入手 | 2017/05/0: |
| 4 | VT-1026 | V-20170424_1026 Mozilla Thunderbird におけ... | Mozilla Thunder... | 脆弱性情報入手 | 2017/04/2( |
| 5 | VT-1027 | V-20170425_1027 Oracle Java for Red Hat Ent... | Oracle Java for R.. | 脆弱性情報入手 | 2017/04/2: |
| 6 | VT-1028 | V-20170425_1028 Linux Kernel におけるローカ.. | Linux | 対応依頼 | 2017/05/1: |
| 7 | VT-1029 | V-20170425_1029 Skype for Windows におけ... | Skype for Windo.. | 対象有無確認 | 2017/04/2: |
| 8 | VT-1030 | V-20170425_1030 WordPress 用 Spider Event ... | Spider Calendar | 脆弱性情報入手 | 2017/04/2: |
| 9 | VT-1039 | Google Android における権限昇格の脆弱性 (20... | windows | 脆弱性情報入手 | 2017/05/2: |


GRCS

# 脆弱性TODAYとの連携

CSIRT MT

脆弱性情報日次配信サービス「脆弱性TODAY」は、日々作業が煩雑な脆弱性情報収集を弊社コンサルタントが行い、更に整理し当日午後に配信するサービスです。
国内外のセキュリティ最新情報を毎日、いち早く収集する事によりCSIRTの運用を大きくサポート。また、予めCSIRT　MTに登録された情報資産にマッチする脆性を自動で検知し、初動もスムーズに進めることが可能です。




GRCS

# レポート＆ダッシュボード機能

CSIRT MT

標準で経営層向けとCSIRTの現場向けダッシュボードを実装。いつでも瞬時に状況把握が可能。また、運用状況に関するレポートも「お客様ごとの切り口」で簡単に作成でき経営層への報告業務を支援します。


レポート
インシデント対応所要時間

編集

合計レコード数
158

| インシデントチケット: レコード連番 | インシデント名 | 検知日時 | インシデントチケット: 最終更新日 | PROCESSED DAYS | PROCESSED HOURS | フェーズ |
|---|---|---|---|---|---|---|
| I-4123 | I-20170411_4123 フィッシングサイト | 2017/04/11 12:00 | 2017/04/11 | 84 | 1,991 | 受付 |
| I-4122 | I-20170411_4122 ウイルス感染 | 2017/04/11 12:30 | 2017/04/11 | 63 | 1,510 | 受付 |
| I-4121 | I-20170411_4121 PCシャットダウン起動不可 | 2017/04/11 12:00 | 2017/04/11 | 53 | 1,270 | 緊急体制 |
| I-4137 | I-20170412_4137 abc | - | 2017/04/12 | 40 | 964 | 受付 |
| I-4117 | I-20170411_4117 社外への情報漏洩 | 2017/04/11 12:00 | 2017/04/11 | 38 | 916 | 受付 |
| I-4139 | I-20170412_4139 ウイルス感染 | 2017/04/12 12:00 | 2017/04/12 | 37 | 887 | トリアージ |
| I-4138 | I-20170412_4138 ウイルス感染 | 2017/04/12 12:00 | 2017/04/12 | 35 | 842 | 受付 |
| I-4133 | I-20170412_4133 不正アクセス検知 | 2017/04/12 12:00 | 2017/04/12 | 31 | 740 | 受付 |
| I-4132 | I-20170412_4132 DoS攻撃 | 2017/04/12 12:00 | 2017/04/12 | 21 | 499 | トリアージ |
| I-4141 | I-20170413_4141 ウイルス感染 | 2017/04/11 12:00 | 2017/04/13 | 21 | 504 | 受付 |

GRCS

# 脆弱性TODAYのご紹介

# サービス概要

CSIRT MT

本サービスは、毎日公開される脆弱性情報をメールで日次配信するサービスです。サービスの概要は以下の通りです。

## 製品の特長

1. 収集した脆弱性情報をメール等によりあらかじめ指定した担当者に送信して報告します
2. 当日朝に発表された脆弱性を同日午後に配信します（土日祝日を除く）
3. 国内だけでなく、海外の製品の脆弱性についても対象に含めております
4. 脆弱性の情報には製品名・該当バージョン・深刻度を示す指標を含んでいます
5. テキストデータに加えて、CSV形式など、パッケージ等への取込みが容易な形式でも提供します

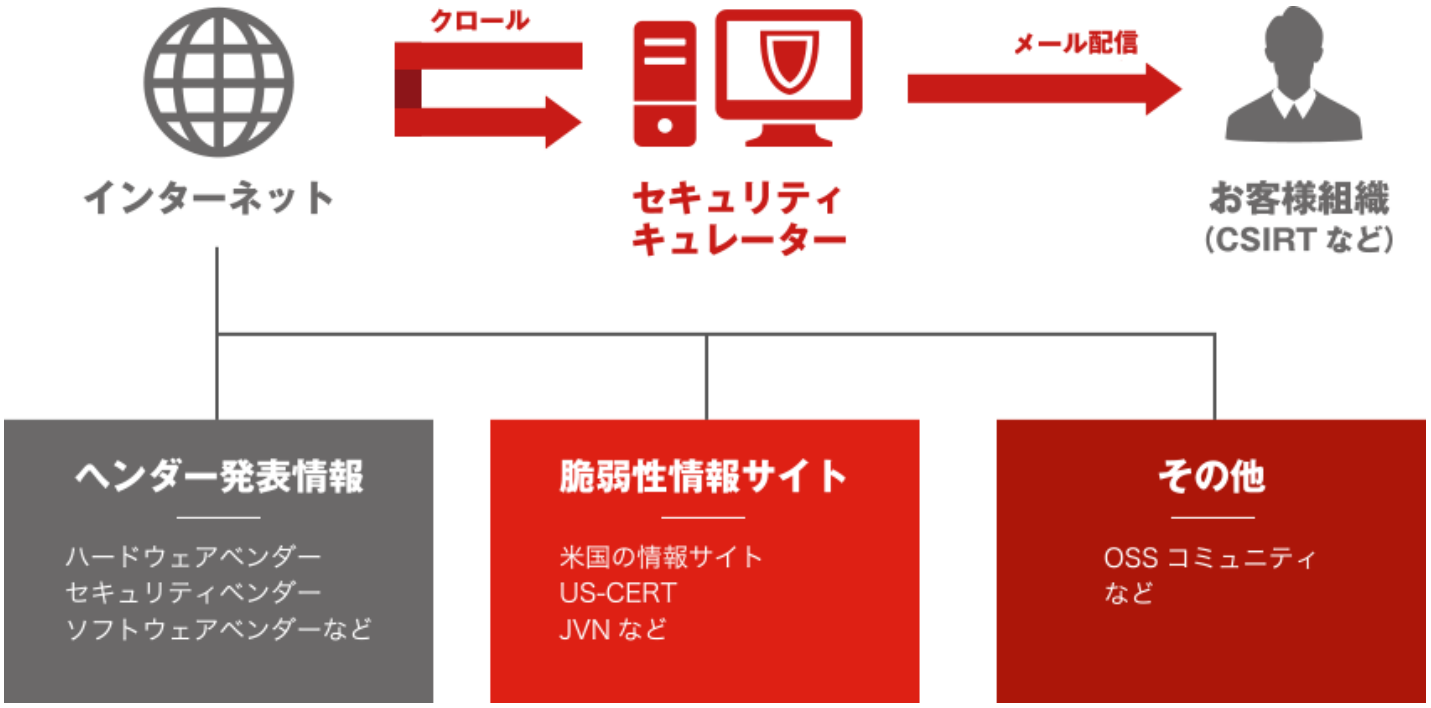
本サービスは、「一般社団法人CSIRTトレーニングセンター」の監修とご協力を頂いております。

GRCS

# サービス提供形態

CSIRT MT

GRCSのコンサルタントが毎日インターネット上で発表・公開される脆弱性情報を収集・整理して、当日午後にメールでレポートを配信するサービスです。




※平日の日本時間午前6時までに発表・公開されている情報を対象にしています

GRCS

# サービスの特長

CSIRT MT

本サービスの特長と優位性を以下に記します。

**速報性**

毎日報告される脆弱性情報を素早く収集するためには、英語圏のポータル・サイトやベンダー・サイトを参照することが必須となります。それらのサイトをくまなく巡回し、日本時間で午前６時までに公表された脆弱性情報を、数時間のうちに収集／分析／整理し、午後にご提供しています。

**網羅性**

数多くのサイトをツールなどを利用して参照することで、重要な情報を見落とすことなく収集しています。各ベンダーのサイトおよび、US—CERTやJVNなどのポータル・サイトを含む、30以上のWebサイトをカバーし、オープンソース・コミュニティから提供される情報も網羅しています。

**正確性**

独自のツールを開発／運用することで人的ミスを極力排除し、正確な情報の提供を実現しています。また、重要な情報であるCVSSスコアに関しても、前述のツールで自動的に計算することで、より正確な情報の提供を目指しています。

**利便性**

膨大なセキュリティ情報を活用し、システムを安全に運用していくユーザーの視点に立って、利便性の高いレポートを目指しています。CVE／CWE／CVSSだけではなく、リモートやローカルに分類される攻撃区分、エクスプロイト・コードやソリューションの有無、参照サイトURLなどを、簡潔にまとめています。

# レポートに含まれる内容

CSIRT MT

本サービスで配信されるレポートおよびCSVファイルには以下の項目が含まれます。

| 項目名 | 概要 |
|---|---|
| 製品・サービス名 | 脆弱性が発表された製品またはサービスの名称です。 |
| 製品・サービスベンダー | 製品またはサービスの提供元です。 |
| 脆弱性が存在するversion | 脆弱性が該当する製品またはサービスのバージョン情報です。 |
| CVE | 米国MITREが採番している脆弱性情報の識別子です。 |
| CWE | 米国MITREが発表しているソフトウェアにおけるセキュリティ上の弱点（脆弱性）の種類を識別するための共通の基準です。 |
| CVSSv3スコア | 統一された基準で算定される脆弱性の評価基準です。<br>攻撃を受ける条件や難易度、影響の大きさなどにより決定されます。 |
| 緊急性判断材料 | 緊急性が高い場合、その判断根拠を記載しています。 |
| 攻撃成功の条件 | 攻撃を受ける条件や手法を記載しています。 |
| 想定される影響 | 攻撃を受けた場合の影響を記載しています（情報漏洩がある、サービスが停止するなど）。 |
| 対策方法 | 公開されているワークアラウンドまたはパッチの情報です。 |
| 情報元 | ベンダーが提供している情報のリンク先です。 |

※未発表の情報などが一部含まれない場合があります。

GRCS

# 配信イメージ

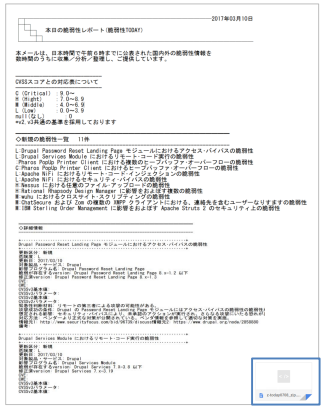
CSIRT MT

本サービスで配信イメージは下記の通りです。

1.情報配信（GRCS）

＊配信システム(Salesforce)

2.メール受信

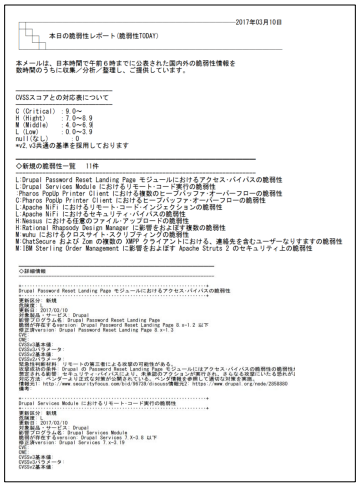


3.ダウンロード

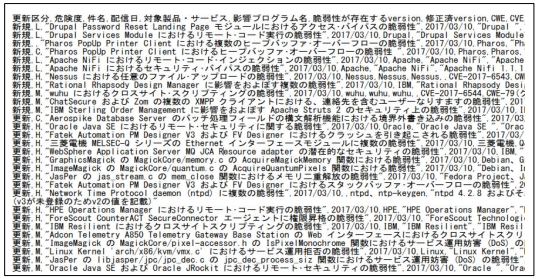
メール
添付ファイル

4.展開　＊メール本文と同様の内容

①テキストファイル（.txt）



②CSV（.csv）



GRCS

# 構成内容

テキストファイル及びCSVファイルの構成は、下記の通りです。

①テキストファイル（.txt）　＊メール本文と同様の内容

2017年03月10日

本日の脆弱性レポート(脆弱性TODAY)

本メールは、日本時間で午前６時までに公表された国内外の脆弱性情報を
数時間のうちに収集／分析／整理し、ご提供しています。

CVSSスコアとの対応表について

C (Critical) : 9.0～
H (Hight) : 7.0～8.9
M (Middle) : 4.0～6.9
L (Low) : 0.0～3.9
null(なし) : 0
*v2, v3共通の基準を採用しております

サマリー

◇新規の脆弱性一覧　11件

L:Drupal Password Reset Landing Page モジュールにおけるアクセス･バイパスの脆弱性
L:Drupal Services Module におけるリモート･コード実行の脆弱性
:Pharos PopUp Printer Client における複数のヒープバッファ･オーバーフローの脆弱性
C:Pharos PopUp Printer Client におけるヒープバッファ･オーバーフローの脆弱性
L:Apache NiFi におけるリモート･コード･インジェクションの脆弱性
L:Apache NiFi におけるセキュリティ･バイパスの脆弱性
H:Nessus における任意のファイル･アップロードの脆弱性
H:Rational Rhapsody Design Manager に影響をおよぼす複数の脆弱性
M:wuhu におけるクロスサイト･スクリプティングの脆弱性
M:ChatSecure および Zom の複数の XMPP クライアントにおける、連絡先を含むユーザーなりすますの脆弱性
M:IBM Sterling Order Management に影響をおよぼす Apache Struts 2 のセキュリティ上の脆弱性

詳細情報

◇詳細情報

+----------+
Drupal Password Reset Landing Page モジュールにおけるアクセス･バイパスの脆弱性
+----------+
更新区分: 新規
危険度: L
更新日: 2017/03/10
対象製品・サービス: Drupal
影響プログラム名: Drupal Password Reset Landing Page
脆弱が存在するversion: Drupal Password Reset Landing Page 8.x-1.2 以下
修正済version: Drupal Password Reset Landing Page 8.x-1.3
CVE:
CWE:
CVSSv3基本値:
CVSSv3パラメータ:
CVSSv2基本値:
CVSSv2パラメータ:
緊急性判断材料: リモートの第三者による攻撃の可能性がある。
攻撃成功の条件: Drupal の Password Reset Landing Page モジュールにはアクセス･バイパスの脆弱性の脆弱性
想定される影響: セキュリティ･バイパスにより、未承認のアクションが実行され、さらなる攻撃にいたる恐れが
対応方法: ベンダーより正式な対策が公開されている。ベンダ情報を参照して適切な対策を実施。
情報元1: http://www.securityfocus.com/bid/96739/discuss情報元2: https://www.drupal.org/node/2858880
備考:

+----------+
Drupal Services Module におけるリモート･コード実行の脆弱性
+----------+
更新区分: 新規
危険度: L
更新日: 2017/03/10
対象製品・サービス: Drupal
影響プログラム名: Drupal Services Module
脆弱が存在するversion: Drupal Services 7.x-3.8 以下
修正済version: Drupal Services 7.x-3.19
CVE:
CWE:
CVSSv3基本値:
CVSSv3パラメータ:
CVSSv2基本値:

詳細情報

②CSV（.csv）

項目名

更新区分,危険度,件名,配信日,対象製品・サービス,影響プログラム名,脆弱性が存在するversion,修正済version,CWE,CVE
新規,L,"Drupal Services Module におけるリモート･コード実行の脆弱性",2017/03/10,Drupal,"Drupal Services Module
新規,,"Pharos PopUp Printer Client における複数のヒープバッファ･オーバーフローの脆弱性",2017/03/10,Pharos,"Ph
新規,C,"Pharos PopUp Printer Client におけるヒープバッファ･オーバーフローの脆弱性 ",2017/03/10,Pharos,Pharos,
新規,L,"Apache NiFi におけるリモート･コード･インジェクションの脆弱性",2017/03/10,Apache,"Apache NiFi","Apache
新規,L,"Apache NiFi におけるセキュリティ･バイパスの脆弱性",2017/03/10,Apache,"Apache NiFi","Apache Nifi 1.1.1
新規,H,"Nessus における任意のファイル･アップロードの脆弱性",2017/03/10,Nessus,Nessus,Nessus,,CVE-2017-6543,CW
新規,H,"Rational Rhapsody Design Manager に影響をおよぼす複数の脆弱性",2017/03/10,IBM,"Rational Rhapsody Desi
新規,M,"wuhu におけるクロスサイト･スクリプティングの脆弱性",2017/03/10,wuhu,wuhu,wuhu,,CVE-2017-6544,CWE-79(
新規,M,"ChatSecure および Zom の複数の XMPP クライアントにおける、連絡先を含むユーザーなりすますの脆弱性",201
新規,M,"IBM Sterling Order Management に影響をおよぼす Apache Struts 2 のセキュリティ上の脆弱性",2017/03/10,I
更新,C,"Aerospike Database Server のバッチ処理フィールドの構文解析機能における境界外書き込みの脆弱性",2017/03
更新,H,"Oracle Java SE におけるリモート･セキュリティに関する脆弱性",2017/03/10,Oracle,"Oracle Java SE ","Orac
更新,H,"Fatek Automation PM Designer V3 および FV Designer におけるクラッシュを引き起こされる脆弱性",2017/03/
更新,H,"三菱電機 MELSEC-Q シリーズの Ethernet インターフェースモジュールに複数の脆弱性",2017/03/10,三菱電機,C
更新,H,"WebSphere Application Server MQ JCA Resource adapter の潜在的なセキュリティの脆弱性",2017/03/10,IBM,"
更新,H,"GraphicsMagick の MagickCore/memory.c の AcquireMagickMemory 関数における脆弱性",2017/03/10,Debian,G
更新,H,"ImageMagick の MagickCore/quantum.c の AcquireQuantumPixels 関数における脆弱性",2017/03/10,"Debian,
更新,H,"JasPer の jas_stream.c の mem_close 関数におけるメモリ二重解放の脆弱性",2017/03/10,"Fedora Project,
更新,H,"Fatek Automation PM Designer V3 および FV Designer におけるスタックバッファ･オーバーフローの脆弱性",2
更新,H,"Network Time Protocol daemon (ntpd) に複数の脆弱性",2017/03/10,,ntpd、ntp-keygen,"ntpd 4.2.8 およびそ
(v3が未登録のためv2の値を記載)"
更新,H,"HPE Operations Manager におけるリモート･コード実行の脆弱性",2017/03/10,HPE,"HPE Operations Manager","
更新,H,"ForeScout CounterACT SecureConnector エージェントに権限昇格の脆弱性",2017/03/10,"ForeScout Technologi
更新,M,"IBM Resilient におけるクロスサイトスクリプティングの脆弱性",2017/03/10,IBM,"IBM Resilient","IBM Resil
更新,M,"Adcon Telemetry A850 Telemetry Gateway Base Station の Web インターフェースにおけるクロスサイトスクリ
更新,M,"ImageMagick の MagickCore/pixel-accessor.h の IsPixelMonochrome 関数におけるサービス運用妨害 (DoS) の
更新,M,"Linux Kernel 'arch/x86/kvm/vmx.c' におけるサービス運用拒否の脆弱性",2017/03/10,Linux,"Linux Kernel","
更新,M,"JasPer の libjasper/jpc/jpc_dec.c の jpc_dec_process_siz 関数におけるサービス運用妨害 (DoS) の脆弱性"
更新,M,"Oracle Java SE および Oracle JRockit におけるリモート･セキュリティの脆弱性",2017/03/10,"Oracle","Ora

詳細情報

# 情報ソースについて

CSIRT MT

情報ソースは非公開とさせて頂いております。
参考までに6月分でカバーしたベンダー（OSS含む）と脆弱性件数は下記の通りとなります。

| ■メーカー等 | 件数 |
|---|---|
| IBM | 137 |
| Cisco | 56 |
| Microsoft | 40 |
| RedHat | 18 |
| Wiewshark | 16 |
| GNU | 14 |
| Apache | 12 |
| Google | 11 |
| ImageMagick | 10 |
| Linux | 10 |
| Adobe | 10 |
| EMC | 8 |
| HPE | 8 |
| Lenovo | 7 |
| Juniper | 5 |
| Apple | 2 |
| Trend Micro | 2 |

（以下略）

| ■プログラム | 件数 |
|---|---|
| Linux Kernel | 20 |
| GNU binutils | 14 |
| Wireshark | 12 |
| Microsoft Edge | 11 |
| IBM Sterling B2B Integrator | 11 |
| ImageMagick | 10 |
| Microsoft Windows | 10 |

（以下略）

■全体（新規・更新）
6月732件（配信計22日）

GRCS

# 製品デモ

# 価　格

# ライセンス価格

CSIRT MT

CSIRT MTにログインできるユーザー数に応じた、ユーザーライセンス（年間契約）となります。

| ユーザー数 | 月額 | 年額 |
|---|---|---|
| 5～20名まで | 1ユーザー　9,000円 | 1ユーザー　108,000円 |
| 21名～以上 | ご相談ください | |

※販売価格は税抜き金額となります。
※添付できるファイルの総サイズは1ユーザーあたり2GBまでの制限があります。
　これを超過する場合は追加料金が発生します。
※Salesforce本体のライセンスの購入は必要ありません。
※最小5ユーザーからのご契約となります。

アカデミック向け価格を検討中

GRCS

# 導入・コンサルティングサービス

CSIRT MT

CSIRT MTの導入およびその前段階となるCSIRT組織、対応フロー、チェックリストの作成など、ご要望に応じて柔軟に対応させていただきます。

| 種別 | 価格 | 主な内容 |
|---|---|---|
| 導入支援サービス | 300,000円～ | 項目・レイアウトのカスタマイズ、レポート・ダッシュボードの作成など |
| トレーニングサービス | ご相談ください | 管理者向けの製品設定やレポート作成等に関するトレーニング |
| インシデント対応チェックリスト（詳細） | | 製品付属の「ウイルス対策」以外の、「不審なメール」「DoS攻撃」などインシデント種別に応じた対応チェックリスト |
| CSIRTコンサルティングサービス | | CSIRTの立ち上げ支援、対応フローの整備、IT資産洗い出し、各種文書・規定の整備など |

※販売価格は税抜き金額となります。
※価格は参考価格となります。詳細なご要件をお伺いの上、別途正式御見積をご提示します。

GRCS

# 会社紹介

# GRCS会社概要

CSIRT MT

| | |
|---|---|
| ■ 会　社　名 | 株式会社GRCS（ジーアールシーエス） |
| ■ 住　　所 | 東京都千代田区五番町1-9MG市ヶ谷ビルディング9F |
| ■ 代　表　者 | 代表取締役社長兼CEO　佐々木　慈和 |
| ■ 事業内容 | IT-GRC・セキュリティ関連ソリューション事業 |
| ■ 設　　立 | 2005年3月1日（2018年3月1日商号変更） |
| ■ 資　本　金 | 1億円（2017年11月30日） |
| ■ 許　可　等 | 有料職業紹介事業許可証（13-ユ-301890） |
| | 特定労働者派遣事業（特13-318092） |
| ■ 所属団体 | 一般社団法人日本CISO協会 |
| | 日本カード情報セキュリティ協議会（運営委員） |

# 製品・クラウドサービス

CSIRT MT

| | | |
|---|---|---|
| 企業経営における<br>リスク管理ソリューション<br>GRC | RiskOrganizer | 企業全体のリスク管理、ISO31000対応 |
| | SUPPLIER RISK MT | 外部委託先リスクマネジメントクラウドサービス |
| | RSA Archer GRC Platform | GRCの統合管理を実現 |
| サイバーセキュリティ<br>リスク管理ソリューション<br>CSIRT・教育 | CSIRT MT | CSIRTに必要な機能を実装したクラウドサービス |
| | 脆弱性TODAY | 脆弱性情報日次配信サービス |
| | ユニプラス | ゲーム学習型教育クラウドサービス |
| インシデント検知・可視化<br>ソリューション<br>検知・フォレンジック | RSA NetWitness | ネットワークフォレンジック・インシデント検知 |
| | DARKTRACE | AIを利用した機械学習によるインシデント検知 |
| 次世代型エンドポイント保護<br>ソリューション<br>EDR・DLP | DIGITAL GUARDIAN | 次世代データ・プロテクション・プラットフォーム |
| | Bromium | 次世代MicroVMエンドポイントプロテクション |
| | CYLANCE | 機械学習を利用したエンジンでマルウェアを検知 |

GRCS

# コンサルティングサービス

CSIRT MT

企業経営における
リスク管理コンサルティング
GRC

サイバーセキュリティ
リスク管理コンサルティング
CSIRT・教育

インシデント検知・可視化
コンサルティング
検知・フォレンジック

次世代型セキュリティ
製品導入
エンドポイント・SIEM

| | |
|---|---|
| グローバルガバナンス | 規定策定・法令対応 |
| リスク管理効率化 | 全社リスクアセスメント |
| 各種認証取得支援 | ISMS、PCIDSS、個人情報保護 |
| セキュリティ監査・アセスメント | PIN Security、３Dセキュア |
| CSIRT構築・運用支援 | 組織立ち上げ、運用改善、アドバイザリ |
| エンジニア教育 | CSIRT研修、標的型メール対応 |
| エンタープライズパケット分析 | インシデント分析、レポート |
| 脆弱性検査 | ネットワーク、サーバ、アプリケーションの検査 |
| SOC構築・運用 | 構築・運用および定期レポート報告 |
| エンドポイント製品導入 | 次世代型エンドポイント製品の導入 |
| SIEM構築・導入 | SIEM製品およびオープンソースの導入 |

GRCS

デモのご用命および無償トライアル利用のお申し込み先

GRCS™

www.grcs.co.jp

株式会社GRCS　営業担当

電話：03-6272-9191
メールアドレス：info@ml.grcs.co.jp
URL：https://www.grcs.co.jp