



株式会社セキュアイノベーション 会社紹介

- **会社概要**
- **沿革**
- **サービス領域**
- **対策マトリクス**
- **取り扱い製品**
- **アライアンス事例**
- **サービス紹介**



会社概要

会社名	株式会社セキュアイノベーション Secure Innovation Inc. (略称：SIV)
設立	2015（平成27）年 10月 21日
資本金等	1億2,100万円（資本金1億,100万円、資本準備金2,000万円）
主な出資者	沖縄振興開発金融公庫、グローバルセキュリティエキスパート株式会社、株式会社ベリサーブ、伊藤忠テクノソリューションズ株式会社、株式会社クレスコ、株式会社QTnet、株式会社りゅうせき、九州電力株式会社、栗田智明 他
代表取締役	栗田 智明
取締役	金城 夏樹 鉢嶺 光 神山 吉衛門 金 智美 原 伸一（グローバルセキュリティエキスパート株式会社 代表取締役副社長）
従業員数	134人（2026年4月20日現在）
所在地	沖縄県那覇市上之屋一丁目18番36号 沖縄映像センタービル3F TEL:098-943-2718 第2オフィス：沖縄県那覇市上之屋一丁目18番17号 カーサ上之屋 3階
東京オフィス	東京都中央区日本橋1丁目13番1号 日鉄日本橋ビル3階
名古屋オフィス	愛知県名古屋市中川区尾頭橋四丁目13番7号 名古屋ビジネスインキュベータ金山503
大阪オフィス	大阪府大阪市中央区道修町4-1-1 武田御堂筋ビル 2F 206号室
福岡オフィス	福岡県福岡市中央区渡辺通二丁目4番8号 福岡小学館ビル5F サービスオフィス福岡薬院18号室
事業内容	<ul style="list-style-type: none">・情報セキュリティシステムの設計、構築、運用監視、診断、ログ分析・セキュリティ人材の育成、派遣事業・システム開発・サイト制作/運営・BPO事業 ・地域活性化事業



主な取引先

官公庁・行政機関、電力会社（東証プライム）、SIer（東証プライム）
インターネット関連会社（東証プライム）、グループホールディングス（東証プライム）
コンサルファーム、クレジット会社、システム開発会社
通信・インフラ会社、広告代理店、情報通信システム会社、リスクマネジメント会社
金融関連会社（銀行・保険会社・信用組合）、病院・クリニック、人材派遣会社
出版会社、学習塾、コンビニエンスストア、社団法人（公益・一般）
認証機関、IoT機器メーカー、自動車メーカーグループ会社 他

所属団体

サイバーセキュリティ協議会 / Center for Internet Security(CIS) / 公益社団法人沖縄県情報産業協会
那覇商工会議所 / ISCO(沖縄ITイノベーション戦略センター) / デジタル・フォレンジック研究会 正会員
公益社団法人日本通信販売協会 賛助会員 / 組込みシステム産業振興機構 一般会員 / 日本カード情報セキュリティ協議会

許可・認定等

JIS Q 27001:2014(ISO/IEC 27001:2013) ISMS認定(登録番号 IS127) [本社・東京オフィス・名古屋オフィス取得]
JASA情報セキュリティサービス基準審査登録
・脆弱性診断サービス(登録番号: 019-0022-20) ・セキュリティ監視運用サービス(登録番号: 019-0022-40)
・機器検証サービス(登録番号: 019-0022-50) ・情報セキュリティ監査サービス(登録番号: 019-0022-10)
労働派遣事業(許可番号: 派47-300169)

主な保有資格

※2026年5月現在

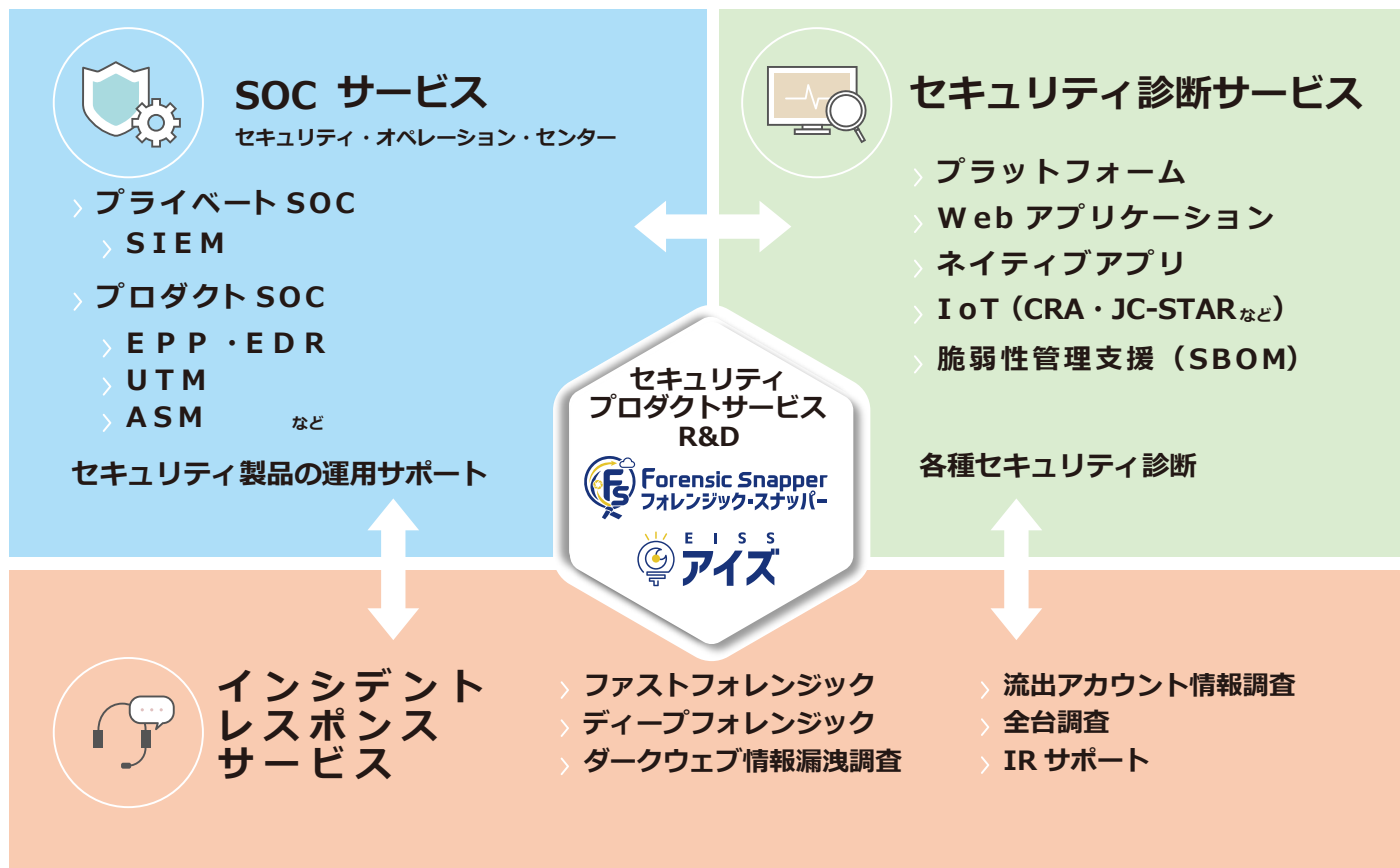
- ・IPA 情報処理安全確保支援士
- ・IPA 応用情報技術者試験
- ・Splunk Enterprise Security Certified Admin
- ・Splunk Enterprise Certified Admin
- ・Splunk Core Certified Power User
- ・Splunk Cloud Certified Admin
- ・Splunk Certified Cybersecurity Defense Analyst
- ・SecuriST 認定ネットワーク脆弱性診断士
- ・SecuriST 認定Webアプリケーション脆弱性診断士
- ・OSCP (Offensive Security Certified Professional)
- ・Microsoft Certified: Security Operations Analyst Associate
- ・Microsoft Certified: Cybersecurity Architect Expert
- ・Microsoft Certified: Azure Solutions Architect Expert
- ・Microsoft Certified: Azure Security Engineer Associate
- ・Microsoft Certified: Azure DevOps Engineer Expert
- ・Microsoft Certified: Azure Developer Associate
- ・Microsoft Certified: Azure Administrator Associate
- ・GCFE (GIAC Certified Forensic Examiner)
- ・eJPT (eLearnSecurity Junior Penetration Tester)
- ・ECIH (EC-Council Certified Incident Handler)
- ・CompTIA PenTest+
- ・CompTIA CySA+
- ・CISSP (Certified Information Systems Security Professional)
- ・CISA (Certified Information Systems Auditor)
- ・CHFI (Computer Hacking Forensic Investigator)
- ・CEH (EC-Council Certified Ethical Hacker)
- ・CND (Certified Network Defender)
- ・CCFH (CrowdStrike Certified Falcon Hunter)
- ・CCFR (CrowdStrike Certified Falcon Responder)
- ・CCFA (CrowdStrike Certified Falcon Administrator)
- ・AWS Certified Solutions Architect - Associate
- ・AWS Certified Developer - Associate



2015/10	セキュアイノベーション設立
2016/01	ベンチャー企業スタートアップ支援事業に採択
2016/03	資本金を3100万円に増資
2017/09	中小企業向けWEBアプリケーション診断サービス開始
2018/01	沖縄県内中小企業向けSOCサービス開始
2018/06	沖縄県新産業研究開発支援事業に採択
2018/07	資本金および資本準備金を8100万円に増資
2018/09	中小企業向けセキュリティサービス開始、SOMPOリスクアマネジメント社と共同企画による
2020/04	自社研究開発を行ったセキュリティ製品「EISS」（アイズ）を販売開始
2020/09	経済産業省&独立行政法人情報処理推進機構（IPA）が推進する令和2年度中小企業サイバーセキュリティ対策支援体制構築事業へ（サイバーセキュリティお助け隊事業）実施事業者として参画
2020/10	資本金および資本準備金を1億6100万円に増資
2021/10	福岡オフィス新設

2021/11	自社研究開発製品「EISS（アイズ）」が「第15回ASPIC IoT・AIクラウドアワード2021」支援業務系ASP・SaaS部門「先進技術賞」を受賞
2022/03	名古屋大学と車載イーサネットの分野における共同研究を開始
2023/09	伊藤忠テクノソリューションズ株式会社からの出資及びセキュリティ事業協業
2023/12	グローバルセキュリティエキスパート株式会社の持分比率変更及び資本業務提携
2023/12	株式会社クレスコ・株式会社QTnetと資本業務提携
2024/04	大阪オフィス新設
2025/03	株式会社りゅうせきとの資本業務提携
2025/04	九州電力株式会社の資本参画
2026/04	本社第2オフィス開設
2026/05	自社研究開発を行ったセキュリティ製品「Forensic Snapper（フォレンジック・スナッパー）」販売開始

当社は「SOCの構築・運用」「セキュリティ診断」「インシデントレスポンス」をサービスの柱としており、その3つの領域で培ったノウハウから自社プロダクトの開発、販売を行っております。







SOC ではSIEM やUTM・EDR・次世代アンチウイルスソフト等、多くのセキュリティ製品の構築・運用に対応しており、インシデントレスポンスを含め連携しながらお客さまに寄り添ったサービスをご提供いたします。

また、セキュリティ診断・SOC・IoTセキュリティおよびリスクアセスメントは経済産業省が定めた「**情報セキュリティサービス基準**」に適合しており、客観的に評価いただいております。











対策マトリクス

近年、複数のセキュリティを施してサイバー攻撃の脅威に備える「**多層防御**」が重要となっています。組み合わせ方によって、より強固なセキュリティ対策を実現させることができますので、現状の把握からサイバー攻撃に備えて最適な対策をご提案いたします。

	ネットワーク	Webアプリケーション	エンドポイント [PC端末]
 弱点の把握 セキュリティ 状況の把握	サイバーセキュリティリスクアセスメント 自社全体のセキュリティ対策状況を把握したい		
	プラットフォーム診断 ネットワークのセキュリティ状況を把握したい	Webアプリケーション診断 Webサイト環境のセキュリティ状況を把握したい	Windowsセキュリティ構成 フレームワーク設定チェック エンドポイントのセキュリティ状況を把握したい
 防御策 攻撃を防ぐ	UTM(統合脅威管理) ネットワークへの攻撃を防ぎたい	クラウド型WAF Webサイトへの攻撃を防ぎたい	アンチウイルスソフト エンドポイントへの攻撃を防ぎたい
	クラウド型サーバセキュリティ サーバへの攻撃を防ぎたい		
 被害軽減策 攻撃/改ざん検知	SIEM(ログ管理分析) 攻撃を検知したい	改ざん検知 SIEMは全てのカテゴリで有効施策となります。	EDR / EISS / ログ管理分析
 事後対処策	デジタルフォレンジック/ダークウェブ情報漏洩調査 / 流出アカウント調査 攻撃されてしまった際の法的根拠となる証拠保全の検討や、情報漏洩・流出を確認したい		
その他	脆弱性管理 (SBOM) ソフトウェアの構成や脆弱性を 可視化・管理したい	ASM 公開されているIT資産に存在する 脆弱性等のリスクを検出・評価したい	EASYクラウドバックアップ 被害にあった際にデータを復元したい
	サイバーセキュリティ コンサルティング セキュリティ対策への 継続的なアドバイスや支援を依頼したい	IoT/車載セキュリティ IoTセキュリティ (CRA/RED/JC-STAR等) や 車載機器のセキュリティ状況を把握したい	情報セキュリティ教育 自社従業員のセキュリティ教育したい

取り扱い製品 (抜粋)

※この他の製品をご希望の際にはお問い合わせください。

<p>ログ収集分析ツール</p>	 a CISCO company SIEM	 SIEM	 ログ分析
<p>ネットワークセキュリティ (UTMなど)</p>	 UTM	 UTM	
<p>Webアプリケーションファイアウォール (WAF)</p>		 クラウド型WAF	
<p>エンドポイント製品 (アンチウイルスソフト、EDRなど)</p>	 AURORA Protect  AURORA Endpoint Defense EPP・EDR	 EPP	 Microsoft Defender for Endpoint EDR
	 EPP・EDR	 ログ管理分析	
<p>その他</p>	 EASY クラウドバックアップ	 標的型メール訓練	 Capy Security for All



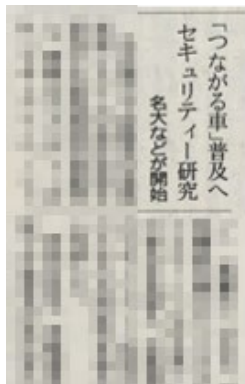
名古屋大学

2022年04月【共同研究】

セキュアイノベーション、名古屋大学と車載イーサネットの分野における共同研究を開始

昨今の自動車分野の技術向上に伴い、より高いセキュリティ基準の取り組みが必要とされる中、本分野における研究で高い知見を持つ 名古屋大学 倉地亮 特任准教授をアドバイザーとして迎え、車載イーサネット分野について共同研究を行います。

今後、両者の共同研究の下、車載イーサネット分野における研究を通して得られたセキュリティ研究成果をもとに、評価ツールの開発や研究成果を学会やシンポジウムで発表を行う等、自動車分野におけるセキュリティ技術向上への貢献、またはそれに伴ったより安心、より安全性の高い車載セキュリティに寄与することを目指し、取り組んでまいります。



中日新聞 2022年4月6日掲載



日刊自動車新聞 2022年4月14日掲載



琉球新報 2022年4月17日掲載

日経業界地図の掲載について

日本経済新聞社が毎年発行している「日経業界地図」に当社がサイバーセキュリティ業界を代表する企業として、**5年連続**で「クラウド/SaaS」部門に掲載されました。

著者：日本経済新聞社
出版社：日経BP 日本経済新聞出版
2025年8月20日発行『日経業界地図 2026年版』



2021年8月24日発行 『日経業界地図2022年版』
2022年8月20日発行 『日経業界地図2023年版』
2023年8月23日発行 『日経業界地図2024年版』
2024年8月28日発行 『日経業界地図2025年版』

止まらないランサムウェア、人材不足も深刻化

ソフトウェア
パソコンなどにインストールし、外部からのウィルスの侵入や感染を防ぐソフト

ZenmuTech	トレンドマイクロ	ブロードコム
チェック・ポイント・ソフトウェア・テクノロジーズ	マカフィー	
タニウム	デジタルアーツ	マイクロソフト
イーセット	カスヘルスキー	
ソースネクスト	ジェン・デジタル	

個人が主な対象

アプライアンス
社内外のネットワークの「境界点」に置き、外部からの不正な攻撃を防ぐ装置

ブレイクベリ	A10ネットワークス	ケイトネットワークス	シスコシステムズ
ジュニパーネットワークス	ハロアルトネットワークス	フォーティネット	

クラウド/SaaS
ネットワーク内に監視ソフトウェアを用意する防衛システム

セットスカー	アカマイテクノロジーズ	クラウドフレア	クラウドストライク
グーグル	データドッグ	セキアインベーション	サイバーセキュリティクラウド

マネージド・セキュリティサービス (MSS)
企業などの信頼システムを総合的に監視・防御するサービス

インターネットイニシアティブ (IIJ)	IBM	アクセンチュア	
セコム	SBテクノロジー	NRI セキュアテクノロジーズ	
NEC	NTTセキュリティホールディングス	キヤノンITソリューションズ	
エムオーテックス	ソフォス	サイバーリズ	日立ソリューションズ
デルテクノロジーズ	デロイトトーマツ サイバー	日立システムズ	
PwC	ヒューレット・パッカード・エンタープライズ (HPE)	Sky	
三井物産セキュアディレクション	ファイア・アイ	富士通	ラック

サイバー保険
サイバー攻撃による被害を想定した損害保険

あいおいニッセイ同和損害保険	AIG 損害保険	損害保険ジャパン
東京海上日動火災保険	三井住友海上火災保険	
共栄火災海上保険	大同火災海上保険	日新火災海上保険

「ランサムウェア」の被害が拡大している。ランサムウェアは、システムを停止させ、その後引金を引く身代金を要求する攻撃手法であり、2024年にKADOKAWA、カンオ計算機、25年に東海大学が被害を受けた。サイバー攻撃に対するグローバルの体制強化も進む。警察庁が22年にサイバー警察局を設置したほか、防衛省は17年度までにサイバー関連部隊を4000人にまで拡充する計画。日本政府は、サイバーセキュリティ政策を指す「国家サイバー統括室」を25年に立ち上げた。国民ともに専門人材の不足が深刻化しており、育成のための体制づくりが急がれる。（日経BPM 総合研究所）

【ランサムウェア】の被害が拡大している。ランサムウェアは、システムを停止させ、その後引金を引く身代金を要求する攻撃手法であり、2024年にKADOKAWA、カンオ計算機、25年に東海大学が被害を受けた。サイバー攻撃に対するグローバルの体制強化も進む。警察庁が22年にサイバー警察局を設置したほか、防衛省は17年度までにサイバー関連部隊を4000人にまで拡充する計画。日本政府は、サイバーセキュリティ政策を指す「国家サイバー統括室」を25年に立ち上げた。国民ともに専門人材の不足が深刻化しており、育成のための体制づくりが急がれる。（日経BPM 総合研究所）

業界規模 セキュリティソフトウェアの国内市場規模：5,861億100万円(2024年、IDC Japan)

キーワード 【総動的サイバー防衛】 外部からの通信を常に監視することで攻撃の手先を察知し、危機と判断した際には攻撃を無力化するための措置を講じること。国内では関連法が2025年5月に成立、27年までには完全施行する。

「日経業界地図2026年版」©Nikkei Inc., 2025 無断複製転載を禁じます。

「日経業界地図」48 クラウド/SaaS 49 サイバーセキュリティ 50 ソフトウェア

7

サイバーセキュリティ

ポイント

- ランサムウェア被害、拡大
- 日本政府の体制強化などの一方で、人材不足が深刻に

※書影および誌面については、日経BP社より許可を得て掲載しています。

① サイバーセキュリティリスクアセスメント

セキュリティ対策を推進するにあたって、自社の状態を把握する必要があります。**戦略・技術的対策・組織的対策の3つの視点で有効性を評価し、セキュリティリスクの全体像を可視化。**今後の対策優先度をご提示します。

- ✓ ご要望やご懸念に応じ、最適なアセスメントをご提案
- ✓ 様々なフレームワークとガイドラインを用いて実施
- ✓ ご提出する報告書は、ランク付けや定量評価で表現し、事前知識のない方でも理解しやすくご提供

② セキュリティ脆弱性診断

再診断が1回無料！
(Webアプリケーション診断)

診断対象に外部から擬似攻撃を行い、対象に潜む脆弱性や潜在要因を診断し、レポート確認いただけるサービスです。**現状のリスクを把握して、効果的な対策に繋げるためにも、継続的に続けることが重要となります。**

- ✓ プラットフォーム診断・Webアプリケーション診断を実施
- ✓ 経産省「情報セキュリティサービス基準」登録済み
- ✓ 認定脆弱性診断士の資格保持者多数

③ UTM (統合脅威管理) マネージドセキュリティ



UTMは、複数のセキュリティ機能を一元化で運用管理を行う機器です。ファイアウォールの機能に加え、IDS/IPSやアンチウイルスなどの外部攻撃をブロックするだけでなく、内部からのアクセス制限による情報漏洩のリスク低減、内部端末間のウイルス拡大対策が可能です。



- ✓ お客様の環境や目的に応じた機器をご提案
- ✓ 経産省「情報セキュリティサービス基準」登録済み

④ Cloud One – Workload Security™ マネージドセキュリティ

サーバの多層防御を実現するクラウド型総合サーバセキュリティサービス「Cloud One – Workload Security™」を、当社が初期設定から運用までをワンストップで、安定したマネージドセキュリティサービスを提供いたします。

- ✓ 自社内で専任の人材や体制構築、教育・人材採用等の負担をかけず利用可能
- ✓ 保護対象のセキュリティ要件に合わせたプラン提供

⑤ SOC (Security Operation Center)

SOCとは、ネットワークやデバイスを監視しサイバー攻撃の検出や分析、対応策のアドバイスを行う組織を意味し、SIV-SOCは当社セキュアイノベーションがセキュリティ診断など豊富な経験で培った分析や知見をもとにお客様のシステム運用・対策をサポートするサービスです。

- ✓ 24/365体制によるSOCサービスをご提供
- ✓ 運用を支援することでセキュリティ製品本来の強度を維持する事が可能

⑥ Splunk (SIEM) 構築・運用



SIEM製品としてログを管理し、自動的に分析を行う事が可能なソリューションです。あらゆるデータをもとにITセキュリティにおける難しい課題解決やビジネスにおける挑戦を支援するツールとして活用でき、**分析主導型セキュリティ**をご提供いたします。

- ✓ ログを管理・分析した環境が必要な状況でご活用可能
- ✓ プライベートSOCの構築、運用を支援
- ✓ SOCの豊富な実績で得られた知見をもとにサービスをご提供

⑦ Microsoft Product MSS (マネージドセキュリティサービス) ・ Sentinel ・ Defender Solution

有資格者が揃うセキュリティ専門SOCチームがMicrosoft社の各プロダクト (Sentinel ・ Defender Solution等 (SIEM/EDR機能など)) の監視・分析をサポート。適切かつ安全な運用で会社の資産・情報を守ります。

- ✓ 24/365体制でアラート/インシデントの分析・通知
- ✓ チューニングや報告書提出が標準プランに含まれる
- ✓ セキュリティ担当の負担軽減
- ✓ Sentinelは構築から実施することも可

⑧ EISS (アイス)

30日間無料お試し可能

月額あたり150円で導入可能なエンドポイントセキュリティサービスです。PC端末における操作を定期的に記録・分析することにより、サイバー攻撃の挙動や痕跡を検知し、「**自ら早期発見できる状況**」を作り、早期の対処による被害の軽減化を目的としています。

- ✓ ログ管理ツールとして活用可能
- ✓ ご利用中のアンチウイルスソフトと併用して利用可能
- ✓ Windowsセキュリティ構成のフレームワーク設定のマクロ有効化等のチェックが可能

⑨ secuWAF (クラウド型WAF)

3か月間無料お試し可能

外部脅威によるWebサイトへの攻撃を遮断して防ぐサービスです。クラウドサービスであるため、コスト面、導入&運用手間についても、アプライアンス型（機器設置等）よりも負担が少なくWebサイトの防御が可能となります。

- ✓ WAFの機能だけではなく「検知分析機能」もプラン追加可能
- ✓ 「総流量プラン」「帯域保証プラン」など予算・目的に合わせて設定可能
- ✓ 簡易脆弱性診断（TOPページのみ）付プランあり



⑪ Deep Instinct マネージドセキュリティ



防御率99%、未知のマルウェアやゼロデイ攻撃などの脅威を予測し、PCやサーバ機器等への侵入をリアルタイムに検知し未然に防ぐことが可能な次世代型AIアンチウイルスです。ライセンス提供や導入支援、SOCによる運用面なども含めてご提供いたします。

- ✓ ディープラーニングを活用した「予測脅威防御」
- ✓ スマホなど様々なOSに対応
- ✓ 導入、構築、SOCによる運用までワンストップでご提供

⑩ Aurora Protect/Endpoint Defense マネージドセキュリティ

99%の防御率を誇るアンチウイルスソフトです。人工知能（AI）を活用した予測防御型ソフトで、その強かさから機密情報を保持する大手企業や金融機関等でも活用されており、しっかり攻撃を防御したい方にお勧めです。

※旧Cylance PROTECT/OPTICS

- ✓ 自己学習のためリスト更新による挙動の重たさがなく、端末への負担が少ない
- ✓ 99%という検知率は、第三者機関（AVTEST等）に評価された信頼性のある数値

⑫ デジタルフォレンジック



情報漏洩などのインシデントが発生した際、証拠保全等を目的として原因調査を行うため、パソコン内部等に保存されているデジタルデータをもとに、専門技術者が原因調査を行うサービスです。

- ✓ 賠償請求のために必要な法的証拠として、証明できる能力を持たせる調査を実施
- ✓ 内容をヒアリングしながらお客様のご予算、期間など要望に応じた調査プランをご提案

13 流出アカウント情報調査

サイバー空間に流出しているログイン情報を調査し、対応方法を提示する情報調査サービスです。原則2020年に遡り、過去から流出しているサービス顧客の流出・漏洩情報を調査・確認します。短期間での調査が可能。

- ✓ Webドメイン、サブドメイン、メールドメインを調査
- ✓ エビデンスを含めた確認レポートを提出
- ✓ 流出が確認できなければ費用はかかりません

14 ダークウェブ情報漏洩調査



サイバー攻撃により盗まれた**お客様の機密情報等**が闇サイト群「**ダークウェブ**」等で出回った可能性がないかを調査するサービスです。ダークウェブ上へ情報が掲載されるタイミングを予測するのは困難なため、定期調査プランもご提供しております。

- ✓ お客様のご予算に合わせたキーワード選定もサポート
- ✓ スレットインテリジェンス専門企業と提携
- ✓ サイバー保険、デジタルフォレンジックもご提案可能

15 IoTセキュリティ診断



IoT機器に対するお客様のセキュリティ課題を解決できるよう、お客様のご要望に合わせて試験範囲を選択できるプランを用意した、IoT機器向けのセキュリティ診断サービスです。

- ✓ 欧州規約であるCRA/RE指令/EN 18031/ETSI EN 303 645等に沿っているかテスト検査をご提供
- ✓ 認証機関と提携しているため、認証から技術面までワンストップで相談可能
- ✓ ファームウェアの脆弱性診断等も提供可能
※オプション

16 車載セキュリティ



自動車のセキュリティ対策として義務化が開始したUNECE規則**UN-R 155（サイバーセキュリティ管理システム：CSMS）**、**UN-R 156（ソフトウェアアップデート管理システム：SUMS）**や、**ISO/SAE21434に準じたセキュリティ評価・試験**を行うサービスです。

- ✓ 認証機関のビューローベリタスジャパン株式会社と提携しているため、認証から技術面までワンストップで相談可能

17 ONEKEY



バイナリひとつで製品の自動解析を行うSaaSプラットフォームツールです。AIベースの解析で、手動で5日を要する解析をわずか30分で分析可能。Professional とEnterprise プランを用意している。

- ✓ SBOM（Software Bill of Materials）の自動生成
- ✓ ソースコードは不要。バイナリファームウェアイメージで動作
- ✓ 脆弱性リアルタイム監視

18 EASYクラウドバックアップ



初期費用なし、クラウド型サービスなので機器の準備も必要なく、お手軽にバックアップの仕組みを導入いただけます。サイバー攻撃を受けた際、普段からのバックアップで早期にデータ復旧できる仕組みを作っておくことで被害を軽減させます。

- ✓ 利用容量でのプラン選択のため、利用台数無制限
- ✓ ファイル単位だけでなく、アプリケーションやアカウント、OSまるごとなど多くのバックアップ形式に対応

19 情報セキュリティ教育

LRM社の情報セキュリティ教育クラウドサービス「セキュリオ」を活用し、当社が培ってきた専門的な知見で独自の運用サービスを合わせたサービスです。eラーニング、標的型攻撃メール訓練の配信もアウトソースでき、セキュリティ担当者の負担を軽減できます。

- ✓ セキュリオの導入実績は1,300社以上
- ✓ 提出する報告書は、訓練の結果だけでなく客観的な総評もレポート

20 【プラスセキュリティ】セキュリティ教育サービス受講プログラム

GSX社の教育セキュリティ人材育成プログラムを提供しています。IT企業・SIer向けに、SEA/J、SecuriST、EC-Council、CISSPなど、目的や対象者に応じて幅広いセキュリティ資格を用意しています。

- ✓ 技術者育成トレーニングや入門・新入社員向けなど幅広いターゲット層に対応するプログラムメニュー。
- ✓ 営業・事業企画向けやIT規格向けもあり、業種を問わず企業人として役立つ知識が身に付きます

②① PHISHNET/25

フィッシングサイトやなりすましなどのサイバーリスクを検知・可視化し、テイクダウンまで支援するクラウド型サイバーセキュリティサービスです。企業・組織への攻撃やブランド侵害を防ぎます。

- ✓ 日本語フィッシングサイトを中心に検知/テイクダウンを行う為のクラウドサービス
- ✓ 付帯情報やブランドの悪用、SNSの書き込みや情報漏洩有無の確認も可能
- ✓ フィッシングのプロセスの多くに対応

②② DMARC/25 Analyze

膨大な XML 形式の認証結果情報（DMARCレポート）を、集計・可視化して解析し、大切なお客様をだまそうとする、なりすましメールへの対策を支援するサービスです。

- ✓ 日本国内のデータセンターでのデータ保存、サービス提供
- ✓ グローバルな情報収集ネットワークに基づく幅広い知見
- ✓ 日本の電子メール業界で長年活躍しているエキスパートによるコンサルティング

②③ ASM

公開されているIT資産に存在する脆弱性・リスクをASMで可視化。

月額サービスで継続して脆弱性の監視・分析・対処が可能。また、ワンショット（単発）もご利用いただけるので、低コストで自社のIT資産を把握することも可能です。

- ✓ 脆弱性などからリスクをスコアリング
- ✓ 優先的に対処が必要となる資産を決めて対応
- ✓ 優先度に基づきリスク低減、受容策の対応

②④ Forensic Snapper フォレンジック・スナッパー

高度なデジタルフォレンジック知識や専用機器を必要とせず、誰でも簡単に導入・運用が可能。平時から「解析可能な状態」を維持する自社開発製品。

導入することで、ユーザーのみならず、フォレンジックを実施するベンダー側にもメリットがあります。

- ✓ 対応手順の未確立による現場の混乱、ミスをなくす
- ✓ 専門知識がなくても重要データを即時確保する
- ✓ 迅速なトリアージにより総調査コストを抑える

お問い合わせ


資料請求やお見積依頼など、お気軽にお問い合わせください。
担当からすぐにご連絡いたします。

お問い合わせフォーム

<https://www.secure-iv.co.jp/contact>



 pr@secure-iv.com

 **098-943-2718**

受付時間 9:00~18:00 (土日祝祭日を除く)