Secureworks

年間1,400件以上のインシデント対応から導く、XDRのあるべき姿

妥協ないオープン性を誇るTaegis™ XDR/MXDRとは

セキュアワークス株式会社
代表取締役社長
廣川 裕司

戦略プログラムディレクター
三科 涼

Secureworks

ビジョン

デジタル（DX）社会に欠かせない
サイバーセキュリティ企業になること

ミッション

常に一歩先を行くことでサイバー
犯罪者に打勝ち、人類の進歩を
確かにしお客様のビジネスを守る

Secureworks®

セキュアワークスの概要

Nasdaq
(SCWX)

卓越した検知力

比類なき対応力

妥協ないオープン性

高い保護力とROI

$499Mドル 過去12か月の売上[1]	**～80か国** 事業を展開する国数	**4800+** 顧客数	**2400名** 従業員数
20年以上 脅威インテリジェンスと セキュリティリサーチ年月	**175以上** 監視する 攻撃者グループ数	**～3000件** 年間の インシデント対応数と セキュリティテストの実施数	
～98% MITRE ATT&CK フレームワークのカバー範囲	**4,700億** **イベント** 1日に処理するイベント数	**25+ペタバイト** Taegis™ に蓄積された データ量	
100以上 すぐに利用できる Taegis™の統合機能	**CRN** ★★★★★ 5-star：セキュリティ ベンダーに格付け	**413%** セキュアワークスの お客様の平均ROI	

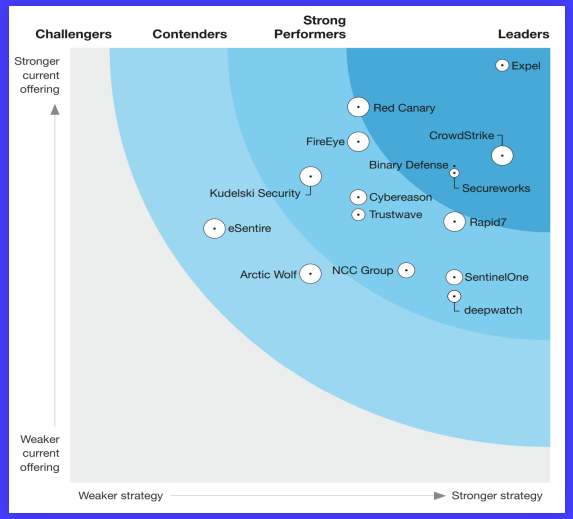
1 Revenue as of FY23 Q2 Earnings
2 The Forrester Wave™ in Managed Detection and Response, Q1 2021
3 IDC MarketScape: U.S. Managed Detection and Response Services 2021 Assessment (doc # US48129921, August 2021
4 Frost & Sullivan 2021 Global XDR Customer Value Leadership Award

Secureworks®

業界のリーダーとして認知される セキュアワークス

Forrester

MDR（ Managed Detection and Response）Wave分野でリーダに選出**



IDC

U.S. MDR MarketScape 2021年、リーダーに選出*

Frost & Sullivan

Taegis™XDRが 2021 Customer Value Leadership Award を受賞

IDC

Incident Response & Readiness 分野で MarketScape のグローバルリーダーを獲得

* In 2020, Gartner graduated the Gartner Managed Security Services Magic Quadrant to a Gartner MSS Market Guide that does not rank vendors. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER and MAGIC QUADRANT are registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved. This recognition does not reflect the current market scenario. This Magic Quadrant was last published in 2019. Due to change in the market, the Magic Quadrant report was retired and Gartner published a Market Guide for Managed Security Services.

** The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

***IDC MarketScape: U.S. Managed Detection and Response Services 2021 Assessment (doc # US48129921, August 2021) IDC MarketScape vendor analysis model is designed to provide an overview of the competitive fitness of ICT suppliers in a given market. The research methodology utilizes a rigorous scoring methodology based on both qualitative and quantitative criteria that results in a single graphical illustration of each vendor's position within a given market. The Capabilities score measures vendor product, go-to-market and business execution in the short-term. The Strategy score measures alignment of vendor strategies with customer requirements in a 3-5-year timeframe. Vendor market share is represented by the size of the icons.

Secureworks

サイバーセキュリティ対応の情勢

現状では立ちゆかない

2.9M サイバーセキュリティの専門家・人材不足は　世界で290万人

87% ランサムウェアインシデント数は日本でも上半期昨年の87%も急拡大

＊（日本の警察庁調べ）

36.1% 昨年ランサムウェア被害を経験した日本企業は全企業の36.1%に上る**

$20B 2020年のランサムウェア被害（支払いコスト）額は
全世界で200億ドル（2兆8000億円）に上る

Free ダークウェブではハッキングツールが無償で取引されている

**March 2022

Source: ESG, Five Threat Detection and Response Technologies are Coming Together, 2019; CriticalStart, The Impact of Security Alert Overload, 2020; The Third Annual Study on the State of Endpoint Security Risk Ponemon Institute© Research Report, Sponsored by Morphisec, January 2020; Top10VPN.com; PurpleSec.us; https://www.japantimes.co.jp/news/2022/09/15/national/crime-legal/ransomeware-attacks-rise/ ; https://www.nippon.com/en/japan-data/h01294/

Secureworks

セキュアワークス
日本戦略

日本の市場規模

IDCによる向こう５年間の予測, May 27, 2022

140 JPY / USD

CY2021	IT 市場	CY2026
19兆2353億円	――CARG +4.1%――→	**23兆　555億円**

主な成長要因　：　5G, IoT, Cloud, ビックデータ→　DX

CY2021	サイバーセキュリティ市場	CY2026
7323億円	――CARG +3.8%――→	**8763億円**
ソフトウェア　4300億円	+4.1%	5317億円
サービス　2963億円	+3.1%	3446億円

主な成長要因: 高度なサイバー攻撃、 クラウド･DXの浸透によるセキュリティホールの拡大など

Secureworks

日本を取り巻くサイバー脅威の実情（止まない攻撃）

2022 IPA 情報セキュリティ10大脅威 (*)

1位（昨年1位）	ランサムウェアによる攻撃	↑
2位（昨年2位）	標的型攻撃による機密情報の窃取	↑
3位（昨年4位）	サプライチェーンの弱点を悪用した攻撃	↑
4位（昨年3位）	テレワーク等のニューノーマルな働き方を狙った攻撃	↓
5位（昨年6位）	内部不正による情報漏えい	↓
6位（昨年10位）	脆弱性対策情報の公開に伴う悪用増加	↑
7位（NEW）	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	↑
8位（昨年5位）	ビジネスメール詐欺による金銭被害	↓
9位（昨年7位）	予期せぬIT基盤の障害に伴う業務停止	↓
10位（昨年9位）	不注意による情報漏えい等の被害	↓

インシデント年表（2020年～2022年）

2022年 ランサムウェアがサイバー攻撃最大脅威

No. 2 APT
No. 3 サプライチェーン弱点を悪用した攻撃
No. 4 テレワーク 環境狙った攻撃 5. 内部情報漏洩

2021年 ランサムウェア（身代金要求型サイバー攻撃）多発し始めた

2020年 APT（標的型サイバー攻撃）が暗躍した年

コロナ禍でのテレワーク環境（VPN）・脆弱性をつく不正アクセス・攻撃も加速
例：Microsoft Exchangeサーバ、AD、F5 Big IPなど脆弱性をついた攻撃多発

＊ 出典：https://www.ipa.go.jp/security/vuln/10threats2022.html

なぜセキュアワークスか？

業界最高レベルの実績
評価と顧客ベース

世界標準・デファクトスタンダード、グローバルトップレベルのNISTのフレームワークでEnd-to-End対応

NIST（国商務省下の標準化団体）CSF（2014年公開、2018年改訂）のフレームワークコア
2018年の改訂では、「サプライチェーンリスク」が追加＝より「全体感」が重要視

特定/Identify	防御/Protect	検知/Detect	対応/Response	復旧/Recovery

これまで重視されてきた対策 → NIST CSFで重視する対策のコア

SRC/CRC
サイバー・リスク・コンサルティング
徹底的なテスト/Red Team

MSS（マネージド・セキュリティ・サービス）
24/365 グローバル拠点を網羅
アラート・レポーティング

IR・IMR
インシデント対応

◆ SRCコンサル・テスト、MDR監視、IMRインシデント対応・復旧まで
一貫したサイバーセキュリティ対応
世界トップベンダー『セキュアワークス』のグローバル契約が日本で可能

Secureworks

日本事業拡大・成長のモメンタム　過去3年

1. **事業規模の大幅拡大：市場の成長を遥かに上回る**
2. **日本IT市場浸透効果**
   - 日本市場　顧客総数　　大幅増加（Unique LOGO グループ会社）
   - MSS サブスクリプション顧客数　　大幅増加（Unique LOGOグループ会社）
   - 社名変更による知名度向上　　Secureworks K.K. ➡ セキュアワークス株式会社
3. **サイバーセキュリティ市場における存在感・影響力**
   - 主要メディア掲載：日経・日経BP、ZDNet、マイナビ、週刊BCN、IT Leader、ITMediaなど
   - パートナーコミュニティ大幅拡大実現：GPPモデルの展開推進（リセラーに注力）
     - 戦略リセラーパートナー
     - 地域特化パートナー
     - 特定市場

成長戦略＃1

『戦略的顧客・案件増大と地域拡大』

- SEUG（ユーザ会）発足 5月25日第一回総会
  ”セキュリティ業界初のユーザー会” 発足
- 主要業種 トップ3顧客の獲得を狙う
- グローバル・DXリーダー企業への深堀営業促進
- 西日本営業強化とローカルキングユーザーの獲得

SEUG: Secureworks Enterprise Users Group – セキュアワークス エンタープライズ ユーザーグループ

成長戦略＃2

『パートナー事業の大幅拡大』

・GPPモデルの浸透と拡大

リセラー ➡ 戦略リセラー
2Tier Distribution、テクノロジーパートナー対応強化検討
MSSPの採用検討

・ 戦略パートナー増加とエンゲージ深耕:

GPPモデルを梃子とした主要製品拡販の
パートナモデルの深耕を促進し
事業相互拡大連携、戦略的幹部会合

成長戦略＃3

『最先端ソリューション投入・需要喚起』

- **11月1日より『Taegis XDR・MXDR』 投入**
- IRソリューション充実：IMR、脅威ハンティング
- 各種テストの拡充：ペンテストから Red Team まで

IR: Incident Response, IMR: Incident Management Retainer

2022年　セキュアワークス日本事業にとって重要なマイルストーン（節目）

Secureworks

セキュアワークス・ジャパン 2.0
成長戦略

セキュアワークス日本事業さらなる成長を狙う事業戦略

ミッション: 攻撃者の先を行き、人類の進歩を確かにし日本のお客様を守る

お客様の成功・事業拡大・経済/IT発展

国策でもある『DX with サイバーセキュリティ』の実現

成長戦略 1

戦略顧客・大型案件
グローバル・DX企業
業界Top1-3顧客
新規業種及び
地域カバレッジ拡大

成長戦略 2

パートナ-事業の大幅拡大
1) Dell Technologies
2) リセラーパートナー
3) MSSPパートナー
4) Tier Model検討
事業計画を共有する.
戦略GPPパートナー拡大

成長戦略 3

最先端ソリューション投入
需要を大きく喚起する
- MXDR製品投入
- IRソリューション充実：
  IMR、脅威ハンティング
- 各種テストの拡充：
  ペンテストから
  Red Team Testまで

成長戦略 4
GPTW・組織の強化

組織の拡大・強化（採用）
GPTW
リーダーシップ養成
.

成長戦略 5
業務効率の向上
Operational Excellence

働き方改革・外部サービス向上

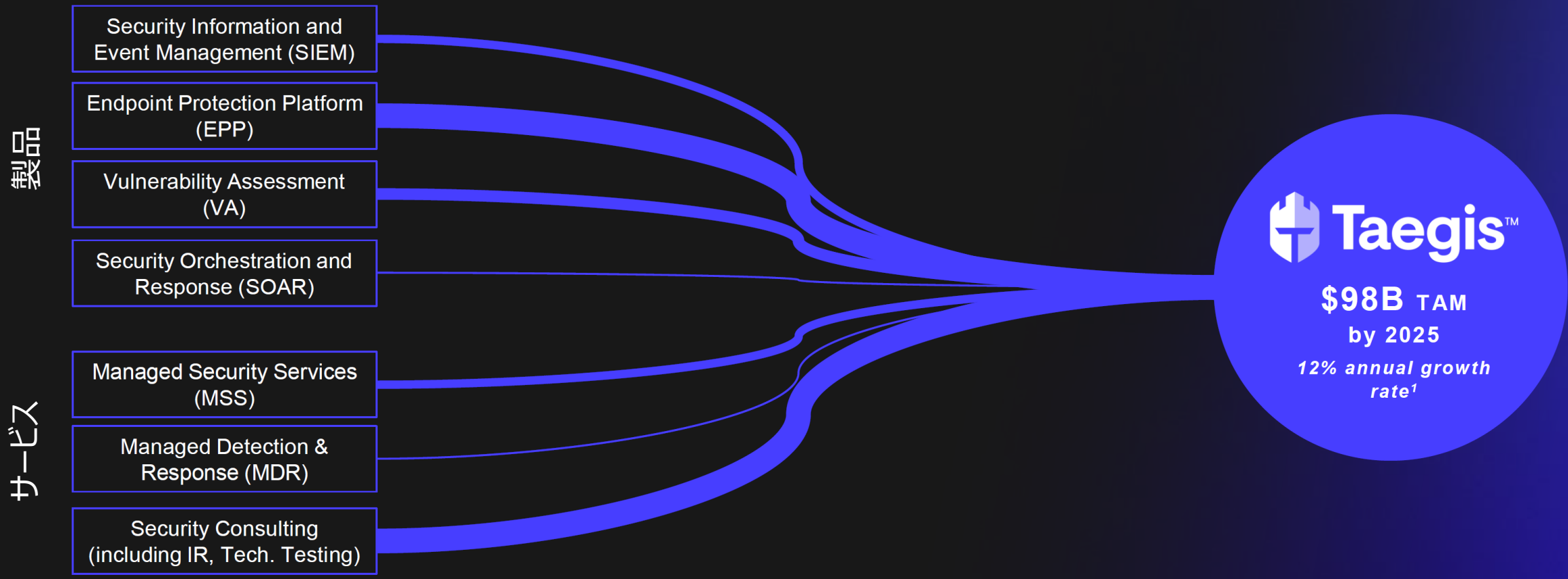
セキュアワークス ・ジャパン2.0 成長戦略

FY23 WW Business Strategy: (1) Cloud Native CS Solutions (2) Partner Leverage Model (3) Security Community Leveraged Response to Adversaries / Threat Actors

Secureworks

XDR Expanded Market Coverage

エンドポイント、ネットワーク、クラウド、Eメール、コンテナ等の市場全体にアクセス可能



*1） 市場規模情報ソース：*Gartner Forecast: Information Security and Risk Management, Worldwide, 2019-2025, 2Q21 update.* TAM規模は脆弱性診断, SIEM, SOAR, EPPソフトウェア, マネージドセキュリティ, MDR, セキュリティコンサルティングサービスを含む。

Taegis™

テイジス

T（echnology） + aegis （shield, defend）

技術 ＋ 盾

（ae·gis） In classical art and mythology, it is an attribute of Zeus and Athena, usually represented as a shield.

古典学や神話学において、主神ゼウス・女神アテーナの属性
一般的に『盾』を意味する

なぜセキュアワークスか？　（本年11月1日より）

業界最高レベルの実績、評価と顧客ベース

世界標準・デファクトスタンダード、グローバルトップレベルのNISTのフレームワークでEnd-to-End対応

NIST（国商務省下の標準化団体）CSF（2014年公開、2018年改訂）のフレームワークコア
2018年の改訂では、「サプライチェーン リスク」が追加＝より「全体感」が重要視

特定/Identify | **防御/Protect** | **検知/Detect** | **対応/Response** | **復旧/Recovery**

これまで重視されてきた対策　→　NIST CSFで重視する対策のコア

SRC/CRC
サイバー・リスク・コンサルティング
徹底的なテスト/Red Team

Taegis™ XDR & ManagedXDR

24/365 グローバル領域を網羅するXDRソリューション

1. 卓越した検知（Detection）
2. 比類なき対応（Response）
3. 妥協ないオープン性
4. 高い投資収益率ROI（Return of Investment）

IR・IMR
インシデント対応

◆ SRCコンサル・テスト、XDR監視、IMRインシデント対応・復旧まで
一貫したサイバーセキュリティ対応
世界トップベンダー『セキュアワークス』のグローバル契約が日本で可能

Secureworks

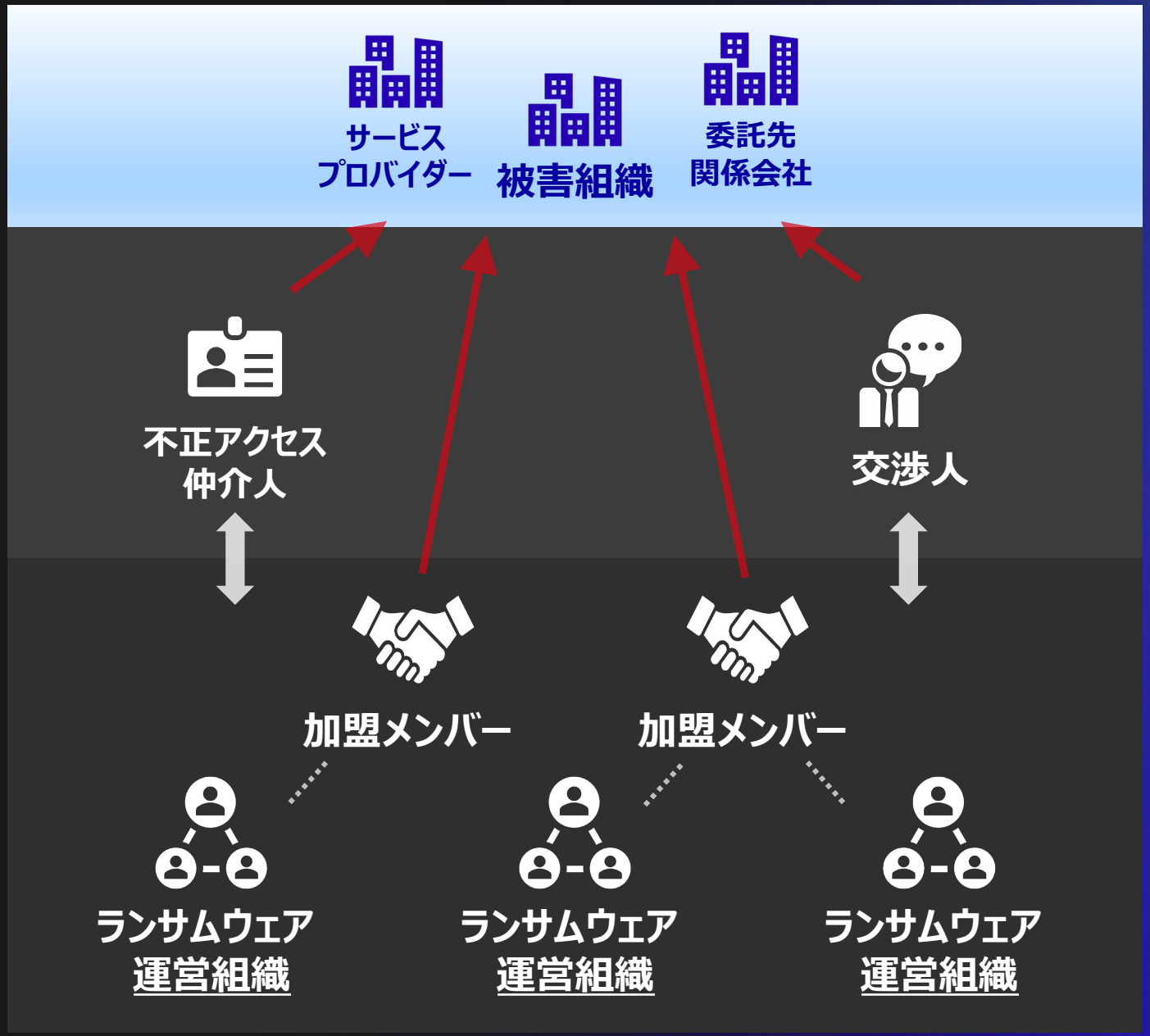
ランサムウェアを軸とした犯罪エコシステムの変化

Secureworks®

ランサムウェア エコシステム

分業の発展により被害深刻化

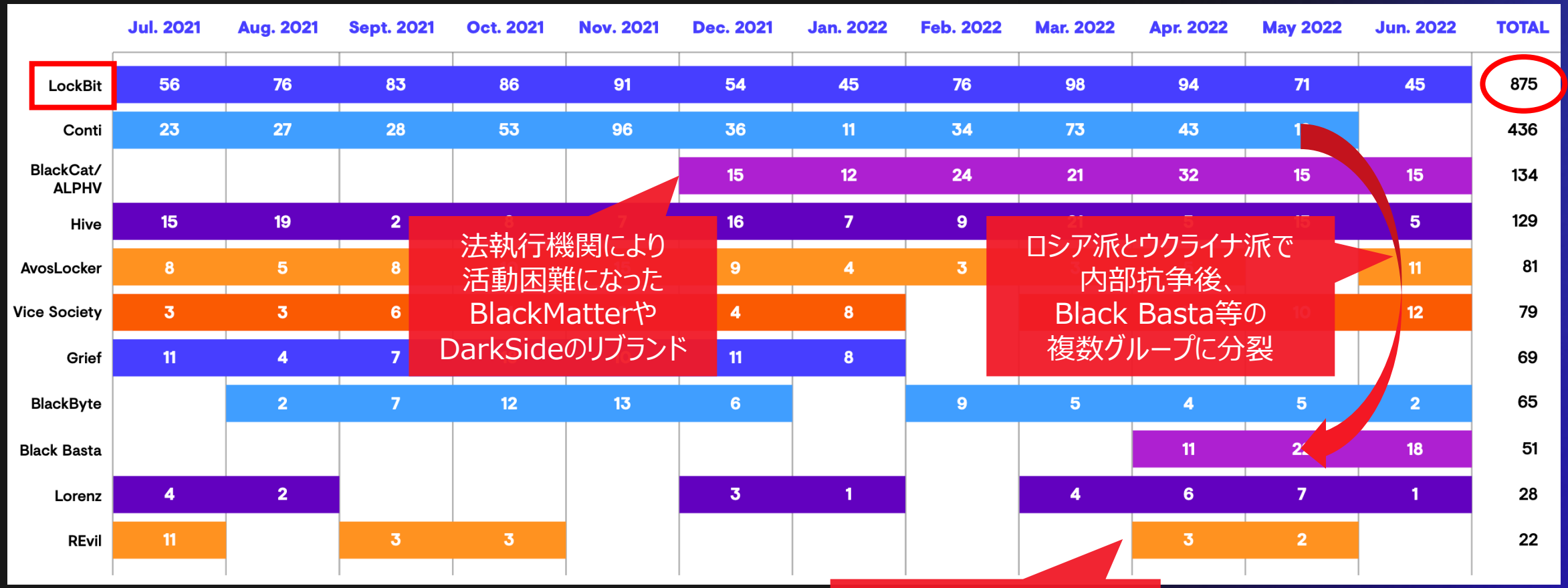
- **運営組織（Operator）：**
  ランサムウェア開発・ビジネス運営
- **加盟メンバー（Affiliates）：**
  運営組織と契約し侵害実務を担当
- **不正アクセス仲介人（IAB）：**
  不正アクセス情報の提供
- **交渉人：**
  被害組織との金銭交渉などを担当



Secureworks

増え続ける暴露型ランサムウェアの被害

LockBit の活動が顕著、日本も複数企業が被害に



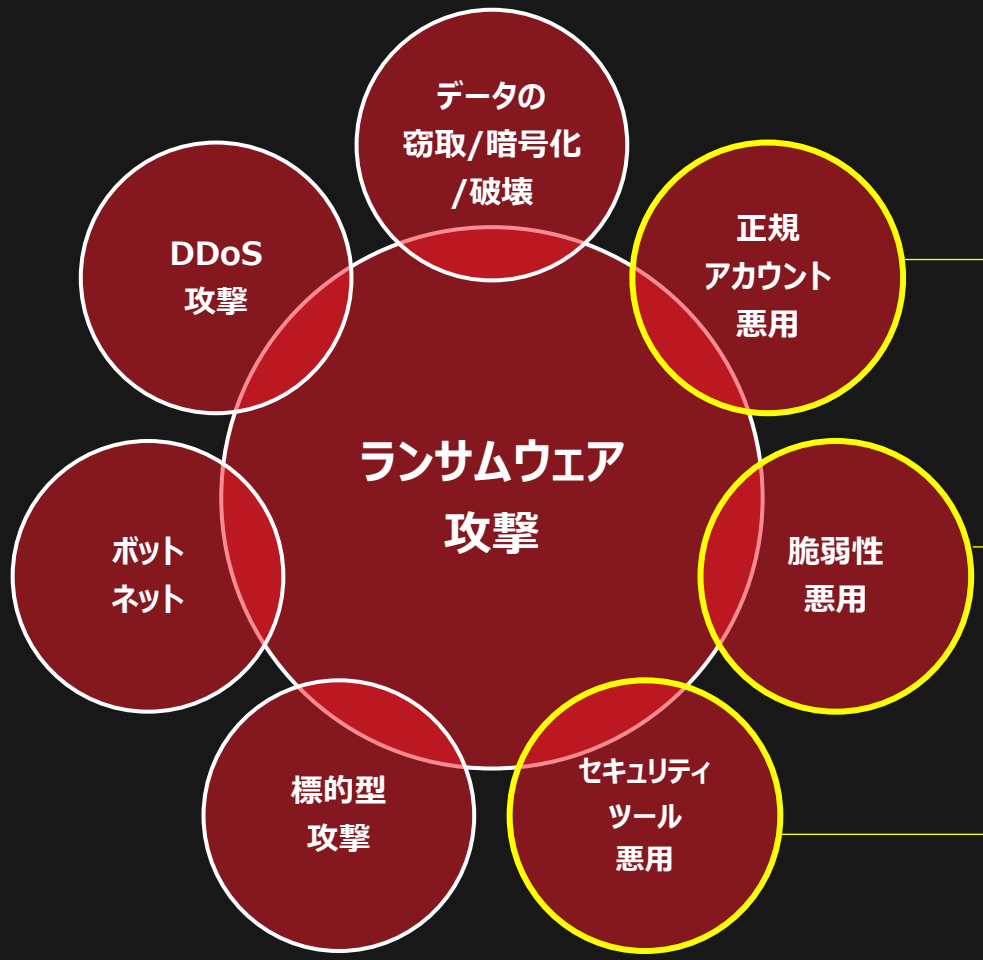
主要なランサムウェアグループによる各月のリークサイト掲載件数

ブランドを残しつつ
休止と復活を繰り返す

Secureworks

業界・業種・規模問わず狙われる

Opportunistic Compromise, Targeted Deployment… “Low-Hanging Fruit”



近年顕著な攻撃傾向

- ブルートフォース攻撃
- 売買された正規アカウント
- RDP / VPN サービス

- インターネットからアクセス可能な機器（VPN機器など）
- 公開サーバ（OS / アプリ）

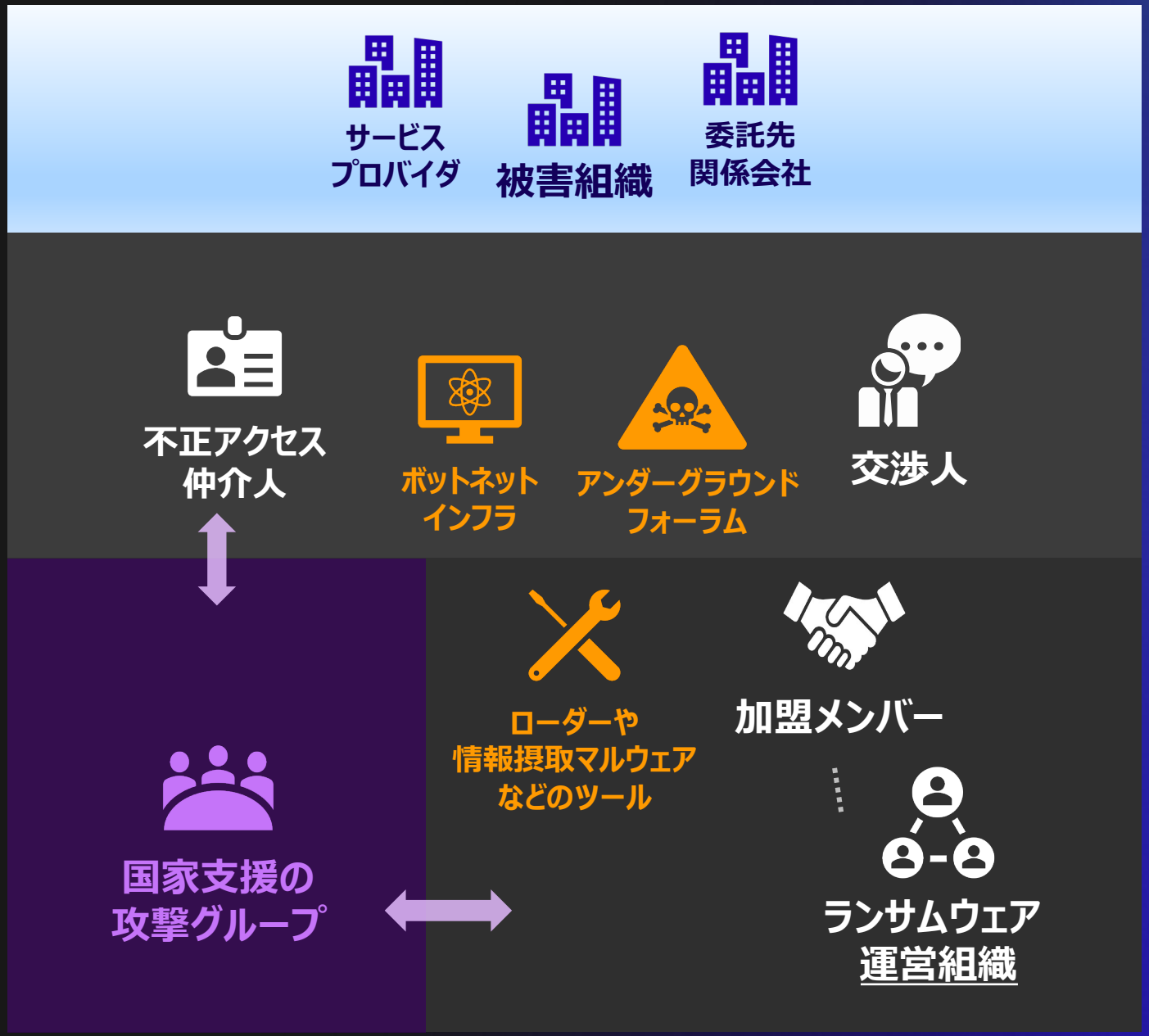
- Cobalt Strike
- 認証情報窃取ツール（Nirsoft / Mimikatzなど）

Secureworks®

エコシステムの水面下で見える変化

利害が結びつくサプライチェーン

- **アンダーグラウンドフォーラム**：
  不正アクセスのための情報やツール売買
- **ボットネットインフラ**：
  Emotet などのインフラを借用
- **目的特化のツール深刻化**：
  ローダーや情報摂取マルウェアなど
- **国家支援攻撃グループ**
  ツールや攻撃対象情報などを共有



Secureworks

様々な思惑で活動する国家支援の攻撃グループ

Secureworks®

ロシアの攻撃グループの主な活動

- 軍事作戦支援、認知した敵への執拗な攻撃、世界中の事業体への諜報活動が主な活動
- 2022年はウクライナの政府機関と国家の重要なインフラを標的
- 以下の業種を狙ったロシアの対外情報組織およびそれらの攻撃グループによるサイバー作戦を確認

航空

ソフトウェア
サプライチェーン

エネルギー
制御系システム

テレコミュニケーション

政府系

防衛系

衛星通信

選挙キャンペーン

Secureworks

中国の攻撃グループの主な活動

- 知的財産、貿易機密、ビジネスの機密情報を狙って長年活動
- 中国の5か年計画や産業重点分野に係る広い範囲の業界を標的としている
- 過去3年間で、セキュアワークスでは以下の業種への攻撃を確認

農業　食品　エネルギー　航空

エンジニアリング　製造業　防衛関連サプライチェーン　製薬・バイオテクノロジー

Secureworks

国家も関与するランサムウェア攻撃の例

国やグループによって目的も異なる

BRONZE STARLIGHT

- 中国のランサムウェアグループ
  - 中国の標的型攻撃グループと攻撃手法を共有
- ランサムウェアを目くらましとして使用している可能性がある

目的は機密情報の窃取

COBALT MIRAGE

- イランのランサムウェアグループ
  - ランサムウェアを使わない暗号化手法を使用する

目的は金銭

Secureworks

国家支援のグループそれぞれの思惑

脅迫による金銭獲得

COBALT MIRAGE など

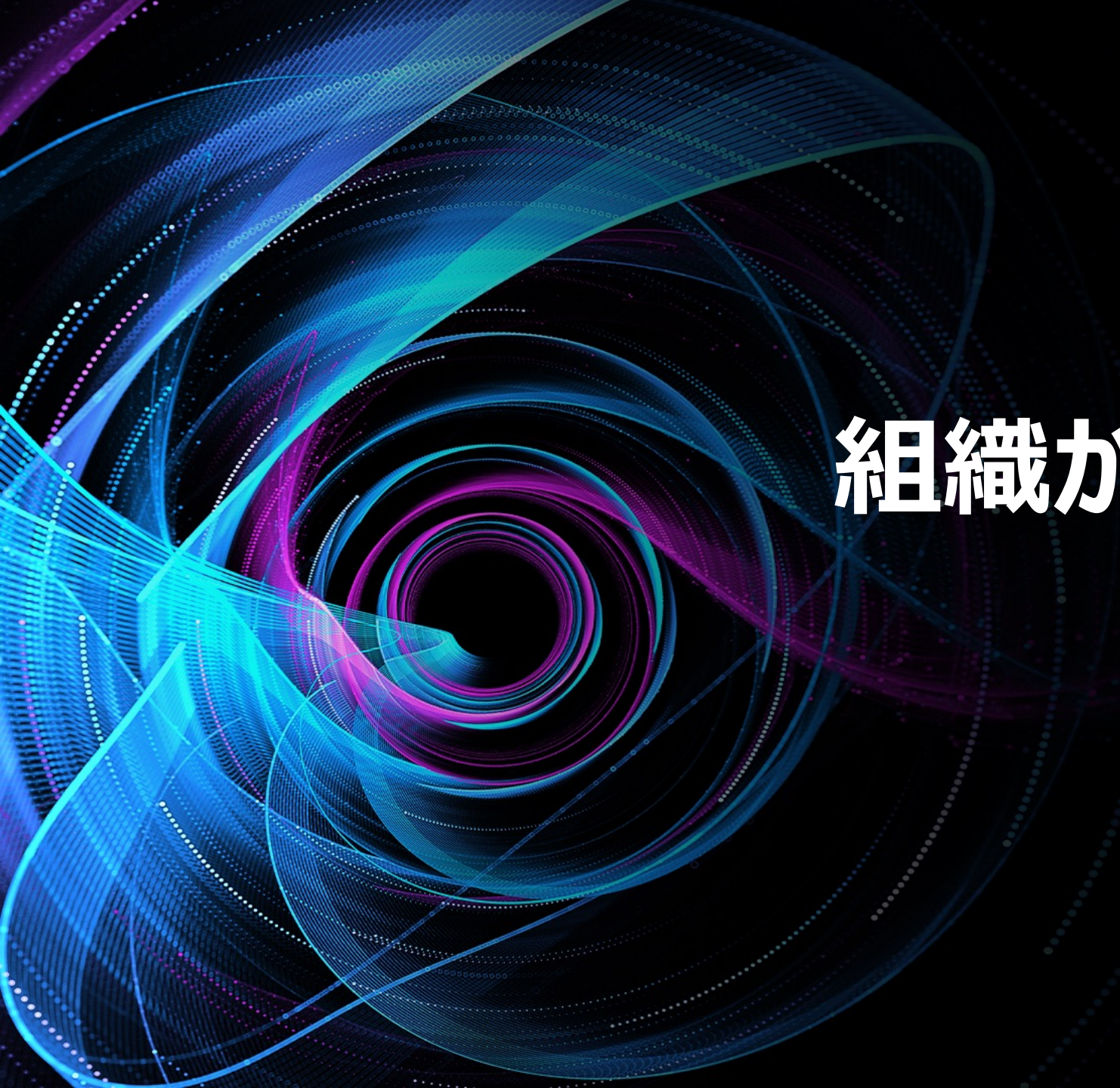
情報窃取のための偽装・証拠隠滅

BRONZE STARLIGHT など

サービス妨害や破壊工作

IRON VIKING など

Secureworks®

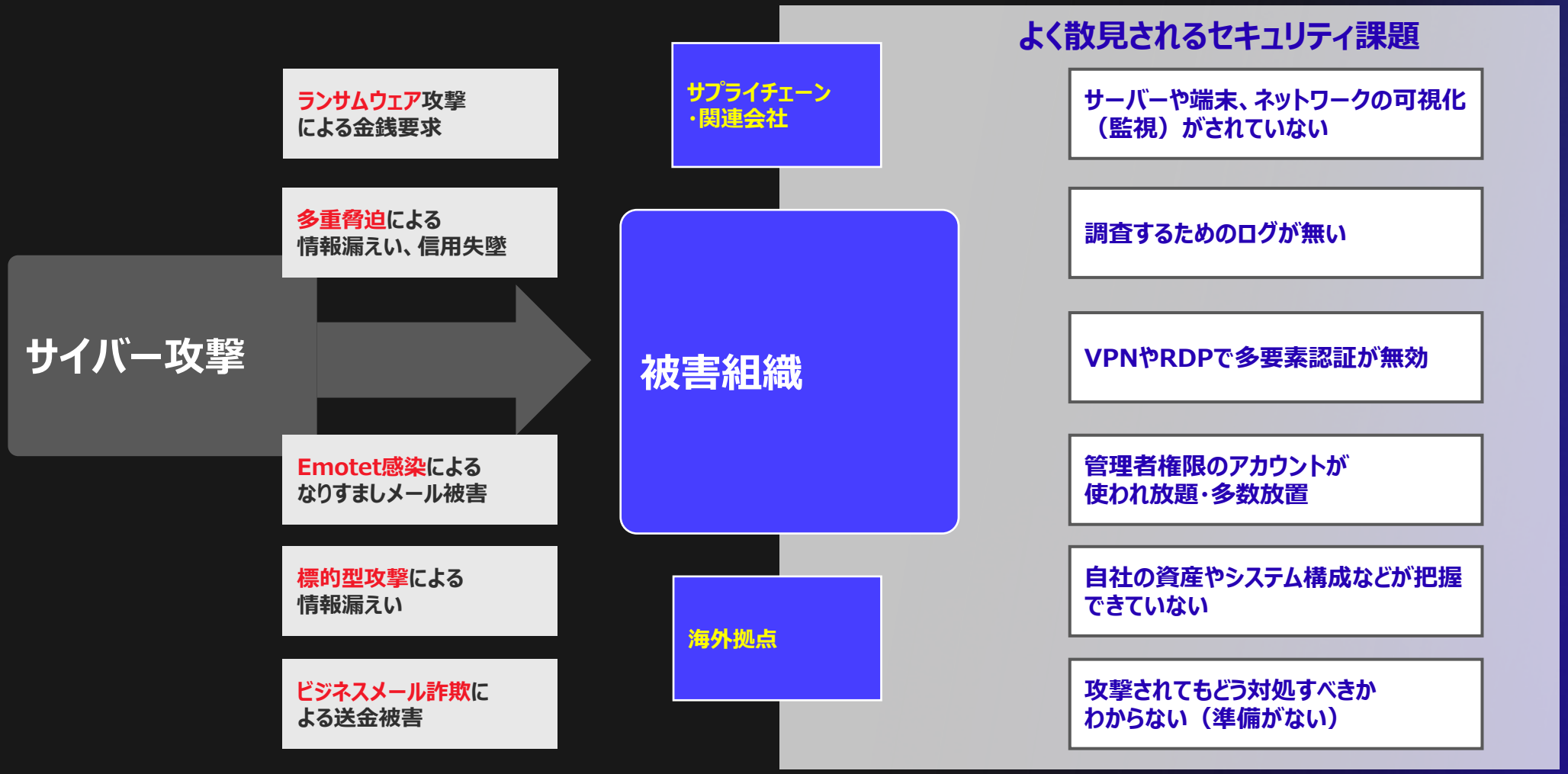


組織が直面する現実と次の一手

Secureworks®

勢いと複雑さを増すサイバーセキュリティ

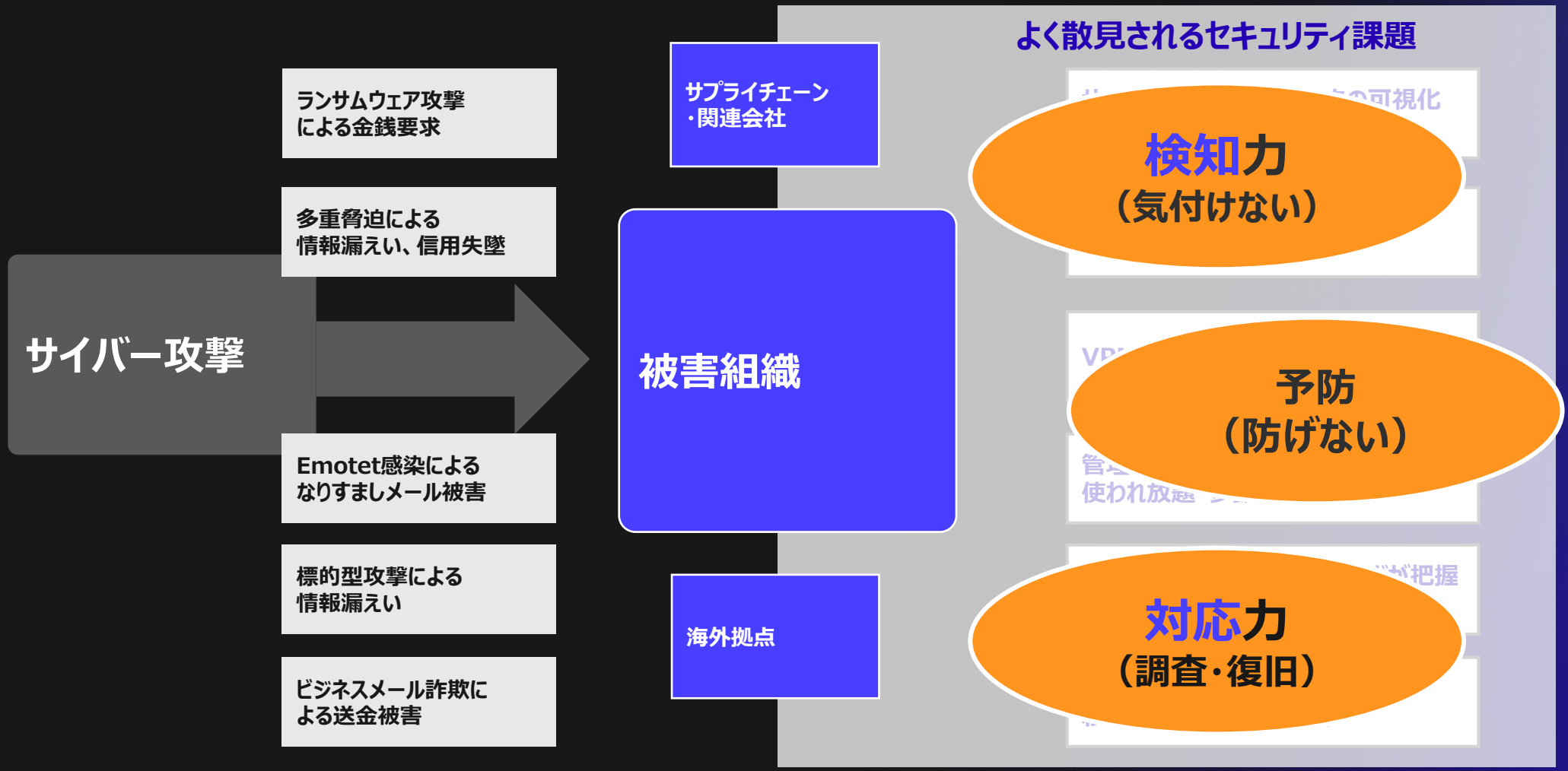
攻撃者が常に優勢な状況



Secureworks

組織の課題も増加の一途

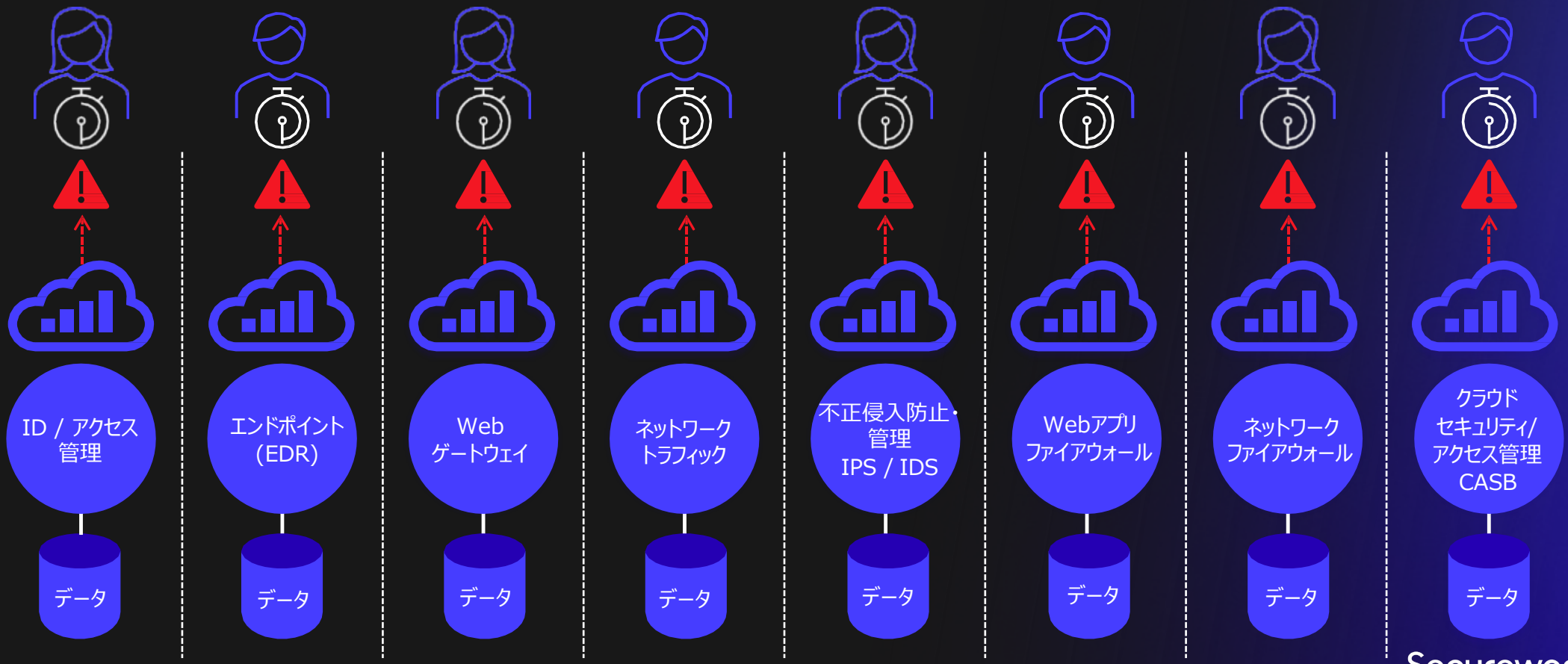
ヒト・モノ・カネの問題に直結



Secureworks

サイロ化されたセキュリティ運用管理の限界

- サイバー攻撃の高度化・複雑化により導入するセキュリティ製品は増えるばかり
- アラートの多発や誤検知対応、製品ごとに異なる管理コンソールやオペレーション
- 増え続ける“ログ“に対する悩み、リソースやスキルの枯渇



Secureworks®

Source: Enterprise Management Associates, InfoBrief: A Day in the Life of a Cyber Security Pro, 05/17/17

4.5日

2022年の「ランサムウェア」インシデント
において、侵入されてから組織内で
暗号化されるまでの平均時間

検知して対処するための猶予期間は”数日”

Secureworks®

次世代セキュリティ対策の生命線

XDR

eXtended Detection & Response

XDR

Extended Detection and Response

Gartner® Market Guide for Extended Detection and Response*では、今後のXDRマーケットの成長について以下のように予測している。

*"**By year-end 2027, XDR will be used by up to 40% of end-user organizations** to reduce the number of security vendors they have in place, up from **less than 5% today**."*

* https://www.gartner.com/en/documents/4007995

- 要するに「**予防**」「**検知**」「**対応**」を飛躍的に向上させる**統合プラットフォーム**
- **検知**するまでの平均時間（MTTD）および**対応**するまでの平均時間（MTTR）の**最小化**が目的のひとつ
- XDRで期待される主な機能
  - **多種多様**なセキュリティ製品の**データの集約と相関による一元的な可視化**
  - **拡張可能**なデータ処理（クラウド）と**機械学習**による検知精度の向上
  - 分析とトリアージ対応処理の**自動化**
  - インシデント対応の調査や脅威ハンティング活動が行える、**コラボレーションできる環境**

Secureworks®

Taegis™
テイジス

2022年11月1日より日本にて販売開始

Taegis™ XDR & ManagedXDR

Taegis ManagedXDR

セキュアワークスの専門家が24時間365日に渡り、Taegis™ プラットフォームを駆使した検知、詳細調査、インシデント対応などをご支援するサービス

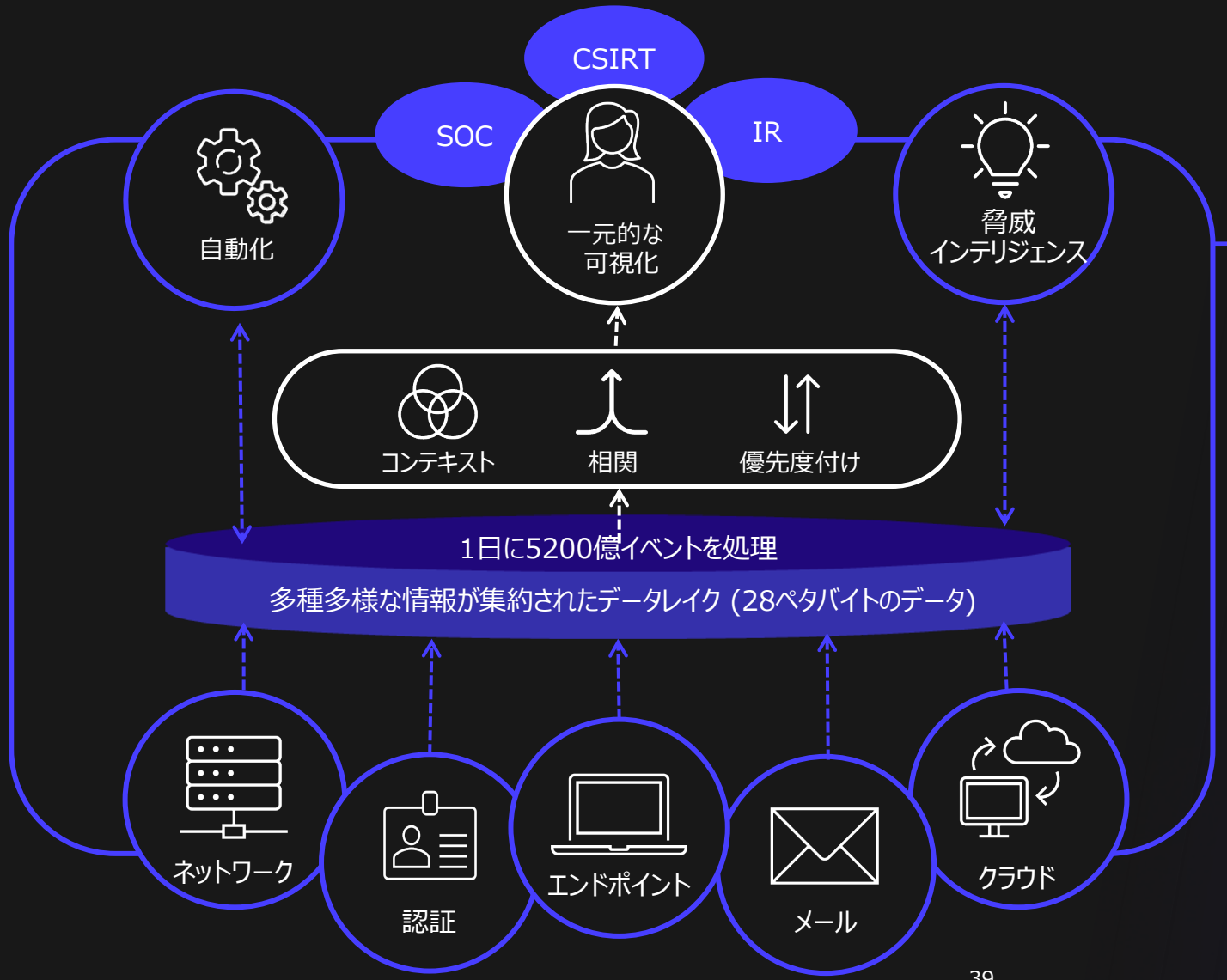
Taegis XDR

お客様主体あるいは弊社を必要に応じて活用いただくなど、お客様のニーズに併せて柔軟に設計されたTaegis™ プラットフォームに搭載されたXDR SaaS アプリケーション

Taegis

セキュアワークスがこれまで20年以上培ってきた叡智を詰め込んだ、次世代クラウドネイティブのプラットフォーム

Taegis™ プラットフォームの全体像



XDR導入の主な効果

- ✓ サイバー脅威の一元的可視化
- ✓ 既知・未知の脅威を検知
- ✓ アラートのノイズ軽減
- ✓ 豊富な脅威インテリジェンス
- ✓ 自動化によるリソース負荷軽減
- ✓ 連携容易な共用プラットフォーム
- ✓ 早期の脅威根絶
- ✓ 高い費用対効果

Secureworks

サイバー脅威の一元的可視化の重要性

点で見えていた脅威を面でとらえるアプローチ

28ペタバイトのデータレイク

毎日5200億件のイベントを処理

380万以上のエンドポイントを管理

事実：イベントの60%はエンドポイント以外のソースから発生

Secureworks

Taegisの強み

卓越した検知力

比類なき対応力

妥協ないオープン性

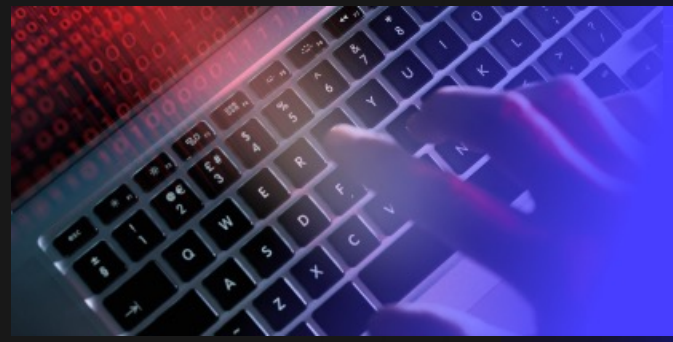
高い費用対効果（ROI）

Secureworks®

サイバーセキュリティ業界を牽引するセキュアワークスとしての役割

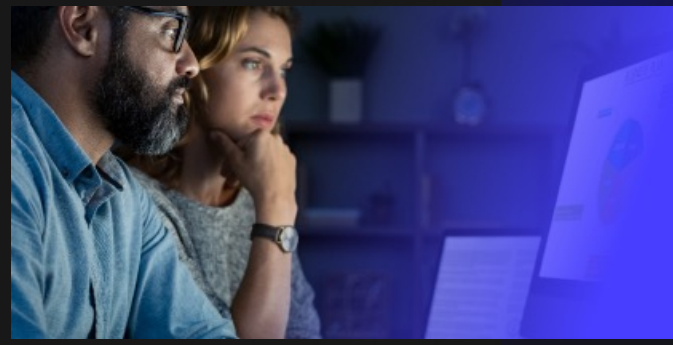
セキュリティ専門家による
セキュリティ専門家・従事者のための
ソリューションを提供

“We deliver solutions by security experts for security experts to drive customer value”



リスク提言

セキュリティ投資の
最適化



セキュリティの
人材不足を打開

最後にアンケートにご協力ください

QRコードを読み込んで、アンケートへのご回答をお願いします

https://forms.office.com/r/RhTBHnKZRx

Secureworks®