証券コード:2467

株式会社バルクホールディングス
2021年3月期第２四半期　決算説明資料

2020年11月16日

Contents

2021年3月期第2四半期 連結業績等

第2四半期連結決算のポイント①

◆売上高は625百万円（前期比▲13百万円、▲2.1％）
マーケティングリサーチ及びセキュリティトレーニングにおいて、新型コロナウイルスの影響を受けたもののセキュリティ認証コンサル、AI脆弱性診断、セールスプロモーションが堅調に推移

►セキュリティ事業　　256百万円（前期比+63百万円、+32.8%）
【主な要因】
・セキュリティ対策ニーズの高まりを受け、AI脆弱性診断などのサイバーセキュリティ分野の売上が増加、情報セキュリティ規格のコンサルティング売上も堅調に推移
・トレーニング売上は前期並み。新型コロナウイルスの影響を受け、集合型研修の開催を一時停止（CYBERGYM TOKYO赤坂アリーナは6月より稼働再開）

►マーケティング事業　375百万円（前期比▲69百万円、▲15.6%）
【主な要因】
・マーケティングリサーチ部門は、新型コロナウイルスの影響による顧客の予算削減、プロジェクト延期等により、売上・受注が減少
・セールスプロモーション・広告代理部門は、主要顧客である大手スーパーマーケットや大手食品メーカーからの売上・受注が引き続き堅調に推移

第1四半期連結決算のポイント②

◆セキュリティ事業にかかる米国資産の減価償却費について

子会社SCH社が米国に保有するトレーニングアリーナ運営用資産（以下「対象資産」）について、2020年３月期末時点の簿価でサイバージム社に売却予定。

一方で、日本会計基準の適用により、対象資産の減価償却費が引き続き計上されており、当該費用として当第2四半期において43百万円を計上。

対象資産の売却が完了した時点で、2020年4月以降に計上した対象資産の減価償却費と同額の固定資産売却益を計上予定であることから、当該減価償却費を控除した各段階利益が実質的な損益の状況。

► 2020年7月以降、SCHの米国部門における減価償却費以外の固定費も大きく減少し、月次損益は大幅に改善。

主な取り組み状況等

◆CYBERGYMトレーニング

►日米において官公庁・大手企業など含め200社以上の企業が受講

►CYBERGYM東京アリーナでは、毎月多くのカスタマイズトレーニングを実施し、フル稼働に近い状況（新型コロナウイルス感染拡大の影響により5月末日まで一時休止、6月からは予定通りフル稼働）

►クラウド型サブスクリプションモデルのeラーニングメニューを開発・提供開始（成長戦略における中核ソリューションとして今後、順次プログラムを拡充）

◆CYBERGYMトレーニングの販売パートナー契約状況

►㈱テクノプロ、㈱インターネット総合研究所、 ㈱ソリトンシステムズ、扶桑電通㈱、㈱昌新、㈱富士通ラーニングメディア、㈱クロスポイントソリューション、ニュートラル㈱などに拡大

◆脆弱性診断『ImmuniWeb®AI Platform』の提供実績

► 2020年10月までに600件超の診断実績

◆脆弱性診断『ImmuniWeb®AI Platform』のリセラー契約状況

►リセラー契約先20社以上（国内SI企業、セキュリティ企業等と契約）

連結P/L概要①

◆売上高
マーケティングリサーチ及びセキュリティトレーニングにおいて、新型コロナウイルスの影響を受けたもののセキュリティ認証コンサル、AI脆弱性診断、セールスプロモーションが堅調に推移した結果、売上高は微減にとどまり、売上総利益は8.9%増加

◆販管費
前年同期と比べ事業規模自体は拡大しているものの、経費削減により13.5%減少

◆各段階利益
新型コロナウイルスの影響を受けたことや、マーケティングリサーチ部門及び脆弱性診断部門の収益が下期偏重であることなどから、営業利益以下の各段階利益において損失計上

（単位：百万円）

（連結）	2021/3月期2Q			2020/3月期2Q
	金額	増減額	前年同期比	金額
売上高	625	▲13	▲2.1%	638
売上総利益	190	+16	+8.9%	174
販管費	402	▲21	▲13.5%	465
営業損失(▲)	▲211	+78	—	▲290
経常損失(▲)	▲236	+247	—	▲484
親会社株主に帰属する四半期純損失（▲）	▲246	+250	—	▲496

連結P/L概要②

【ご参考】

◆米国資産の減価償却費を控除した場合の連結業績

（単位：百万円）

（連結）	2021/3月期 2Q			2020/3月期 2Q
	金額	増減額	前年同期比	金額
売上高	625	▲13	▲2.1%	638
売上総利益	231	+56	+32.4%	174
販管費	400	▲64	▲14.0%	465
営業損失(▲)	▲168	+121	—	▲290
経常損失(▲)	▲193	+291	—	▲484
親会社株主に帰属する四半期純損失（▲）	▲202	+294	—	▲496

連結B/S概要

◆流動資産　：現預金が113百万円増加した一方で受取手形・売掛金が70百万円減少したことなどにより69百万円の増加
◆固定資産　：減価償却等により77百万円の減少
◆流動負債　：社債の償還などにより100百万円の減少
◆純資産　：第5回・第6回新株予約権の行使により資本金及び資本剰余金がそれぞれ176百万円増加した一方で、四半期純損失246百万円を計上したことなどにより92百万円の増加
◆自己資本比率：以上の結果、自己資本比率は10.9ポイント増加

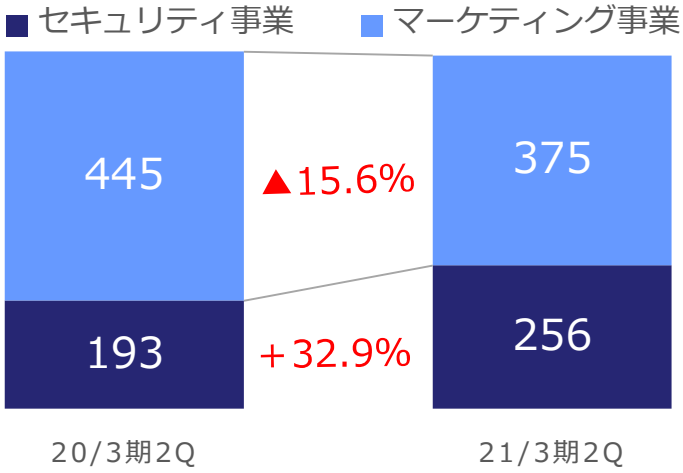
（単位：百万円）

（連結）	2020/3月末	2020/9月末		
	金額	金額	増減額	前期末比
流動資産	393	462	69	117.7%
固定資産	518	441	▲77	85.1%
繰延資産	21	14	▲7	66.5%
総資産	934	919	▲14	98.4%
流動負債	603	503	▲100	83.4%
固定負債	131	124	▲7	94.6%
純資産	198	290	+92	146.5%
自己資本比率	20.6%	31.5%	+10.9	—

セグメント別業績

◆セキュリティ事業
・セキュリティ対策ニーズの高まりを受け、AI脆弱性診断などのサイバーセキュリティ分野の売上が増加、情報セキュリティ規格のコンサルティング売上も堅調に推移
・トレーニング売上は前期並み。新型コロナウイルスの影響を受け、集合型研修は当初予定どおりに開催できず。(CYBERGYM TOKYO赤坂アリーナは6月より稼働再開)

◆マーケティング事業
・マーケティングリサーチ部門は、新型コロナウイルスの影響による顧客の予算削減、プロジェクト延期等により、売上・受注が減少
・セールスプロモーション・広告代理部門は、主要顧客である大手スーパーマーケットや大手食品メーカーからの売上・受注が引き続き堅調に推移



（単位：百万円）

（連結）	2021/3月期 2Q			2020/3月期 2Q
	金額	増減額	前年同期比	金額
セキュリティ事業	256	+63	+32.9%	193
マーケティング事業	375	▲69	▲15.6%	445

連結業績推移

（単位：百万円）

※18/3期における売上高の前期比大幅減は子会社2社（住宅関連事業、IT事業）の売却による

2021年3月期通期業績見通し

セキュリティトレーニング、脆弱性診断サービスとも、受注・引合いの推移状況、リモートワークの急速な普及等による市場のさらなる拡大傾向を踏まえ、順調な事業拡大を想定。既存ソリューションのうち、セキュリティ認証コンサル、セールスプロモーションは、新型コロナウイルスによる影響はあるものの、強固な事業基盤により、堅調な推移を見込む。マーケティングリサーチは、新型コロナウイルス感染拡大の影響による顧客の予算削減やプロジェクト延期等の影響で当初想定を下回って推移しているが、マーケティング事業の事業領域において、技術革新、経済・社会の在り方変化等による新たなニーズが拡大しており、この取り込みを推進。（LINE公式アカウントの運用支援を開始し受注案件を積み上げ中）
また、サイバージム社とのグローバルでの共同事業戦略の見直しにより、サイバーセキュリティ事業を米国で展開するために負担していた費用が大幅に軽減。

（単位：百万円）

（連結）	2021/3月期			2020/3月期
	金額	増減額	前年同期比	金額
売上高	1,706	＋353	126.1%	1,353
営業利益	14	＋581	―	△567
経常利益	6	＋1,141	―	△1,135
親会社株主に帰属する当期純利益	4	＋1,324	―	△1,320
1株当たり当期純利益	0.41	＋146.85	―	△146.44

サイバーセキュリティ分野の主な実績及び今後①

◆サイバーアリーナの提供・運営支援

►㈱インターネット総合研究所内にCYBERGYM新宿アリーナがオープン(2019年８月)

►㈱クロスポイントソリューションとアリーナ提供契約を締結(2020年8月)、同社との合弁会社㈱クロスポイントセキュリティジムを設立(2020年10月、持分法適用関連会社)がCYBERGYM八重洲アリーナをオープン(2020年11月)

►2021年3月期中に、海外ではアジア、国内では関東及び関西でのオープンを予定

◆サイバーセキュリティトレーニング

►毎月1回、Cyber Defense Essentialsオープン講座を開始

►CYBERGYM'S Zero to Heroプログラムの提供を開始

►組織内レッドチーム構築プログラムの提供を開始

►OT/IoT向けトレーニングの提供を開始

►セキュア開発トレーニングの提供を開始

►クラウド型サブスクリプションモデルのeラーニングを開発・提供

（今後、順次プログラムを拡充）

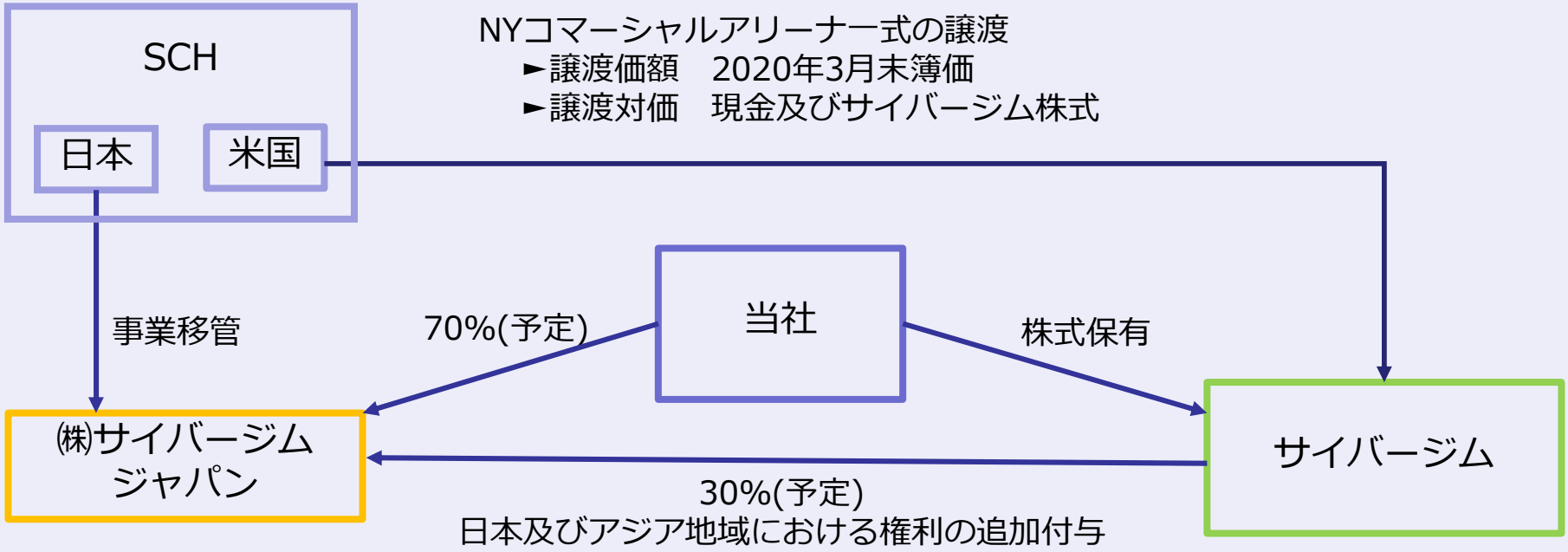
サイバーセキュリティ分野の主な実績及び今後②

◆サイバーセキュリティ関連のその他ソリューション

- ►『ImmuniWeb® AI Platform』によるAIセキュリティ診断の提供を開始
- ►AIを用いた制御システム向け初期障害検出サービス『SIGA Platform』の提供を開始
- ►NIST（米国セキュリティ基準）対応支援サービスの提供を開始
- ►SOC（セキュリティ監視センター）の立ち上げに向けて準備中
- ►cybereasonEDR（Endpoint Detection and Response）の提供を開始
- ►トータルセキュリティソリューションを提供するため、セキュリティトレーニング、脆弱性診断、セキュリティ認証コンサルをベースとして、高付加価値ソリューションを有するパートナーとの関係を拡大（P24参照）

サイバージム社とのグローバルでの共同事業戦略の見直しについて

◆サイバージム社との間で覚書を締結（2020年6月2日公表）
米国でのセキュリティトレーニング事業展開のために保有するライセンス・設備等の譲渡、日本国内での合弁会社設立



►SCH社の米国部門における固定費の大幅削減、日本及びアジアにおける権利強化
→迅速な業績の改善と成長の実現
►譲渡対価の一部としてサイバージム社株式を取得
→サイバージム社への出資比率を高めることで、中長期的なリターンを享受
►サイバージム社は中核拠点として米国でアリーナを保有・運営

投資先の状況 ～CyberGym Control Ltd.（イスラエル）～

CYBERGYM

https://www.cybergym.com/

CYBERGYM AMSTERDAM
スキポール空港内

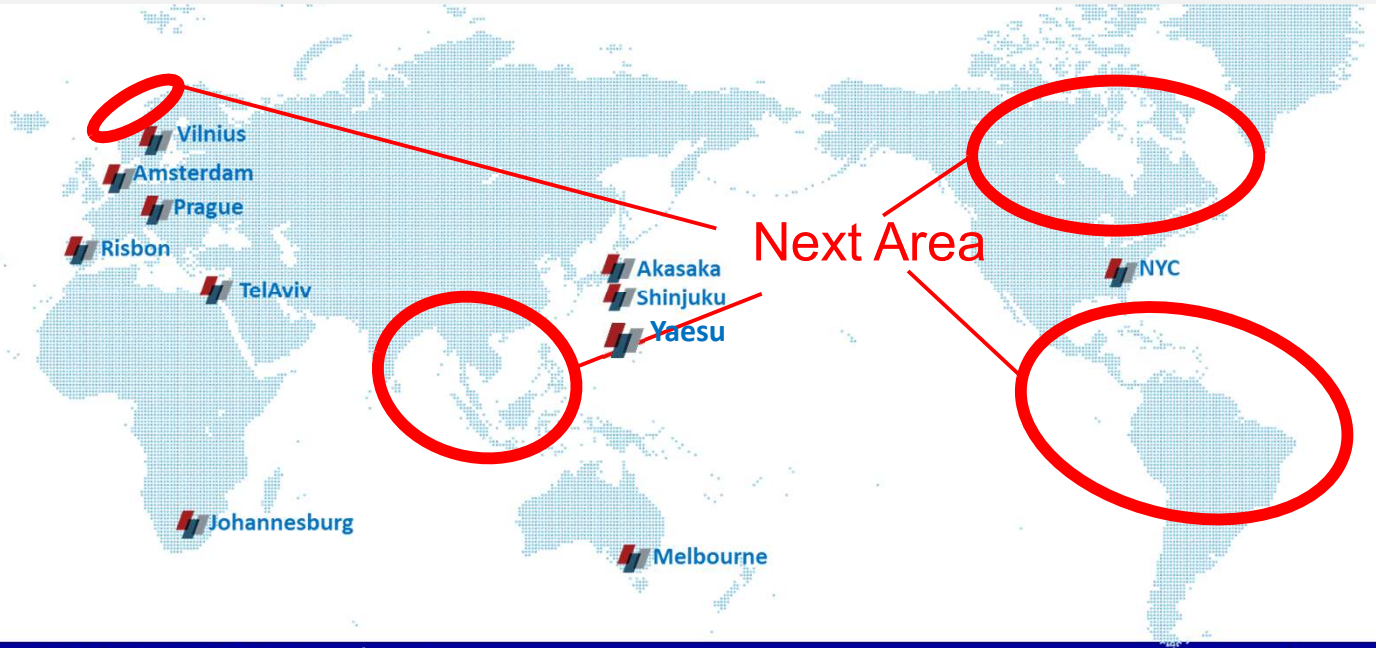
ハポアリム銀行との
調印セレモニーの様子

►**グローバルなサイバーアリーナ網を拡充**
・イスラエル、チェコ、ポルトガル、リトアニア、オーストラリア、アメリカ、日本、南アフリカ、オランダにアリーナ開設
・東南アジア、欧州、中米でのアリーナ開設も準備中
・その他にも複数の新規プロジェクトが世界各国で進行中

►**米国Cybint社と提携し、高等教育機関向け『Cyber Centers of Excellence助成金プログラム』を提供開始**

►**イスラエル最大手銀行のハポアリム銀行と提携、金融セクター向けサイバーアリーナの開設・運営などに関する戦略的パートナーシップを締結**

WCWA（World Cyber Warfare Arena）



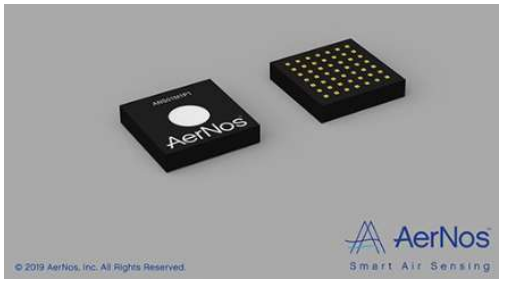
投資先の状況 ～ AerNos,Inc.（米国） ～

AerNos
http://www.aernos.com/

カーボンナノチューブを用いたMEMSに高度なデータサイエンス技術を組み合わせることで、空気中などにある様々な種類のガスをリアルタイムで同時に検知する極小かつ高精度なナノガスセンサーを開発販売

２年連続受賞！

世界最大級の先端テクノロジー見本市
「CES2020（米ラスベガス、2020年1月7日～10日）」
にて、CES 2020 Innovation Awardsを受賞
（Tech for a Better World部門）



AerNos AerSIP

【AerIoT】

空気清浄機、エアコン、スピーカー、街灯等の組込み用センサー

→グローバルで展開する大手家電メーカー向けに
量産化のための生産ラインを準備中

AerIoT

【AerBand】

高血糖及び低血糖の症状を検出するウェアラブルセンサー

→段階的に出荷を開始


AerBand

バルクグループの事業戦略について

サイバーセキュリティ市場の現状

公共性の高いインフラは近年、IT化が加速しており、サイバー攻撃の脅威に直面。
インターネットの普及で、あらゆるモノや世界が繋がり、生活が便利になった反面、デジタルデータ量も急増し、サイバー攻撃被害が増加し、世界のサイバーセキュリティ市場は2021年には2,024億米ドルに達するとの報道もなされている。また、国内においてもセキュリティ人材の不足が深刻な問題となっており、経済産業省の報告では、本年までにおよそ20万人もの人材が不足すると推測

想定される重要インフラ分野での主な障害

情報通信 通信・放送の停止	**政府・行政** 行政サービスの支障
金融 預金の払い戻し、 融資の遅延・停止	**医療** 医療機器の誤作動
航空 安全運航への支障	**水道** 水供給の停止 水質維持の支障
空港 セキュリティ低下,遅延・停止	**物流** 輸送の遅延・停止 貨物の追跡支障
鉄道 列車の安全輸送の支障	**化学** プラントの停止 製品供給の停止
電力 電力供給の停止	**クレジット** カード情報の漏洩 決済の遅延・停止
ガス ガス供給の停止 プラントの安全運用への支障	**石油** 石油の供給停止 安全運転への支障

最近のサイバー攻撃被害等の一例

【2019年12月】
米国SNS企業、2.7億人分のユーザー情報が流出

【2020年１月】
大手電機メーカー、サプライチェーン攻撃により本社や主要拠点のPC・サーバに不正アクセス

【2020年１月】
大手電機メーカー、防衛事業部門にて不正アクセス被害

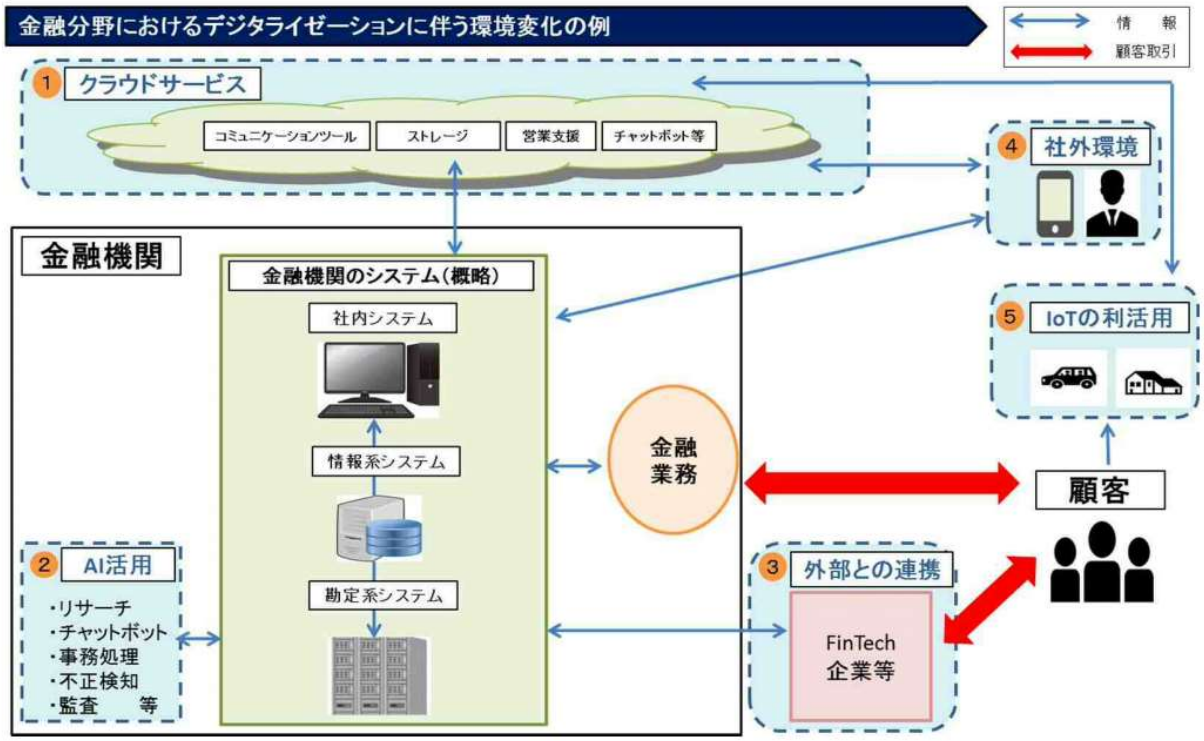
【2020年１月】
米国インフラ企業、ランサムウェアにより天然ガス施設が稼働停止

【2020年６月】
大手自動車メーカー、身代金要求ウイルスに感染し、一部工場で生産停止

【2020年11月】
コロナワクチン研究にサイバー攻撃

技術革新による企業インフラの変化

【図表１：金融分野におけるデジタライゼーションに伴う環境変化の例（銀行）】



（資料）金融庁

出典：金融分野のサイバーセキュリティレポート 令和元年6月　（金融庁）
https://www.fsa.go.jp/news/30/20190621_cyber/cyber_report.pdf

WEBサイト

モバイルアプリ

ネットバンク

ATM

各種IoTデバイス

エンドポイント

クラウド

10年前は企業システムの入り口と出口を守っていれば十分であったが、スマートフォン・タブレット・ノートパソコンの普及、Wifiスポットの普及、プリンタやIPカメラのインターネット化により企業の侵入経路は爆発的に拡大。今後、IoT、５G、制御システム(OT)のオープン化が進むことでさらに拡大する見込み

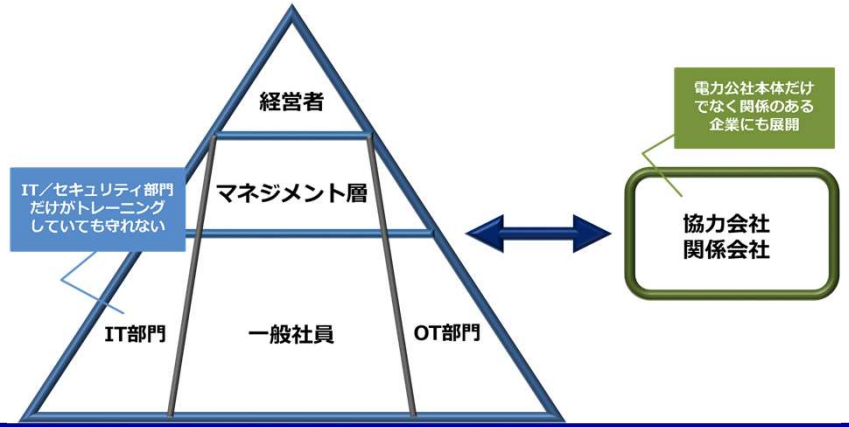
イスラエル電力公社のサイバーアタックの現状

2018年IECへのサイバー攻撃

- 年間2億回以上
- 月平均1,700万回
- 最高月間攻撃数7,000万回（2017年5月）
- イスラエル電力公社（IEC)は99.85%政府保有のイスラエルで唯一の電力事業者
- 25か所の火力（石炭・石油）・天然ガス発電所を保有。イスラエル経済の全セクターに対して発電、送電及び配電事業を展開

未知のマルウェア・攻撃手法が1,000件～3,000件/月
アタックの一部を防御出来ず、侵入を受ける

それでも重要インフラを守ることが出来ている理由は？



経営層から一般社員まで全社員
12,000人中7,000人のトレーニング実施
（CYBERGYMが実施）

サイバージム社の強み

◆様々な重要インフラセクターにおけるグローバルかつ高度な知識・ノウハウ

►毎月1,700万件のサイバー攻撃に対峙するIECの経験
►8200部隊やNSAなどにおいて実践経験を有する高い技術・ノウハウを有するチーム
►各国のサイバーインシデント発生時から72時間以内に分析し、トレーニング化
►エネルギーセクター、銀行セクターの主要企業との強固な連携

◆実践経験に基づく独自開発のトレーニングプログラム

►IT環境だけではなくOT環境にも焦点
►顧客のセクター、システム、ハードウェア、担当業務範囲、レベル等に応じて高度にカスタマイズ可能なトレーニングプログラム
►事前にプログラム化されたサイバー攻撃ではなく、顧客に応じてカスタマイズしたトレーニング環境に対して行われるオンタイムの攻撃
►ハンズオンアプローチによる実践的なトレーニング
►セキュリティ・プロダクトやツールのみならず、オペレーションプロセスや企業の方針、人的要因等を加味した上で、組織としての体制構築もサポート

◆サイバーアリーナをプラットフォームとした高付加価値ソリューション

セキュリティ事業のソリューションマップ

株主総会・取締役会

省庁・業界団体

CEL

セキュリティに関する善管注意義務（Fiduciary duty）

脅威調査 → 法令遵守 → 機関設計 → 危機管理 → 評価 → 認証 → 保険 → 開示 → 立証

CIO	CISO	Audit

ITインフラ	OTインフラ	セキュア開発	診断	訓練 危機対応	モニタリング	評価	トレーニング	認証 コンプライアンス
Endpoint	ICS	Secure By Design	脆弱性診断	レッドチーム	マネージドセキュリティ	従業員eラーニングセキュリティ理解度テスト	経営層	Pマーク
Email	SCADA	S-SDLC	ペネトレーションテスト	CyberKill Chain	SoC	標的型メール訓練	非エンジニア社員	ISMS
Webapp	PLC	DevSecOps	金融機関	CSIRT	EDR	内部統制	IT/OT/IoT	GDPR
SPapp	HMI	Agile	自動車車載システム				SoC	NIST
Network			スマート家電				Pentester	
WebServer			スマートホーム				レッドチーム	
SW			ブロックチェーン					
HW								
顧客DB								
決済DB								

CEL　CYBERGYM　VLC VALUE CREATE

当社グループは世界的に人材の足りない『重要インフラ・OT・IoT・5G』などのセキュリティ新領域における人材を確保することで、クライアント企業の企業価値の保全と向上に貢献。重要インフラ企業の経営層から現場エンジニアまでトータルでソリューション提供ができる競合企業は少ない。

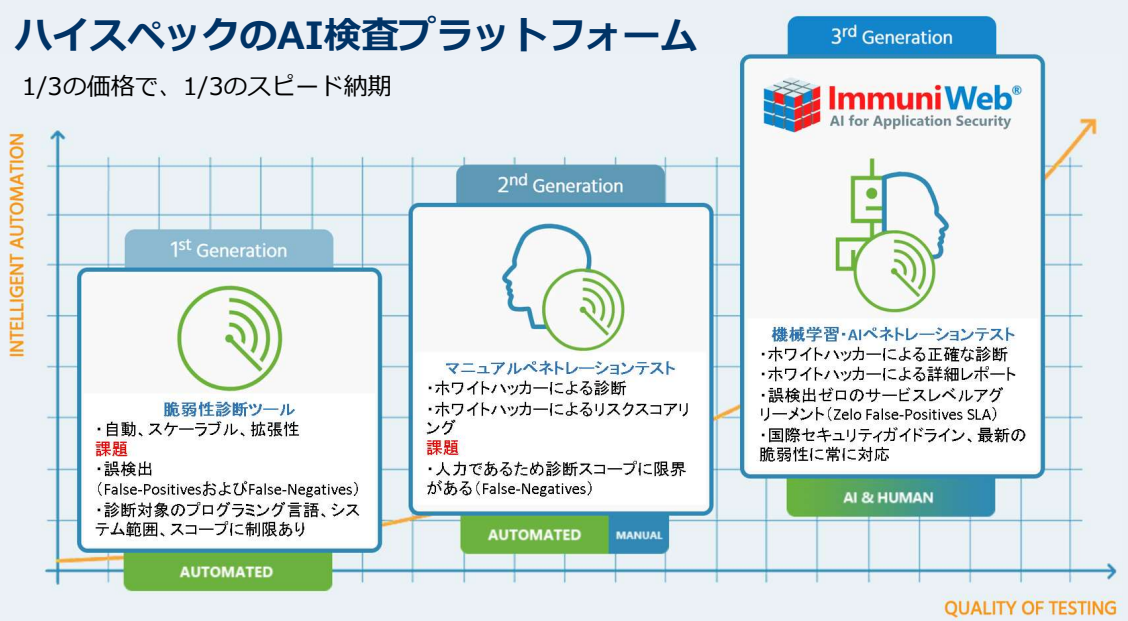
セキュリティ事業のソリューション戦略

►グループの既存顧客・見込顧客リストは大企業（主にSCH、CEL）から中小・ベンチャー企業（主にバルク、CEL）までを網羅。
成長戦略として、この販売チャネルを活用しクロスセル・アップセルを実現するため、顧客ニーズを満たすセキュリティ
ソリューションを大幅に拡充。

セキュリティトレーニングの主なメニュー

トレーニング名	概要	対象者	日数	金額
Cyber Defense Essentials	実際のサイバー攻撃を体験し、複数の検出・監視ツールを駆使してサイバーインシデントを検出し、その初期分析を行うためのスキルを習得	IT担当者 情報セキュリティ担当者 SOCアナリスト	2日間	250,000円/1人 1名から参加可能
Management Workshop	・実際のサイバー攻撃シナリオの体験とサイバー攻撃時の意思決定を実践しながら、緊急事態や危機管理のマネジメントを体験する ・最新のサイバー攻撃の事例を学ぶ	トップレベルの意思決定者及びマネジメント層	半日	300,000円
SIEM Intrusion Detection Training	・SIEMとそのデータソースを最適にしながら、サイバー攻撃を特定できる ・システム侵入やデータ侵害の検出と分析をしSIEMのルールを最適化する	情報セキュリティ担当者 SOCアナリスト	3日間	450,000円/1人 4名以上
Penetration Test	・脆弱性診断やペネトレーションテストで使用する様々なツールを使用して、対象システムやネットワークの弱点を調査及び特定する ・侵入成功後に実際に被害が発生し得る影響についても把握できるように	IT担当者 情報セキュリティ担当者 SOCアナリスト 脆弱性診断	5日間	700,000円/1人 4名以上
Forensics Training	Forensicの能力を身につける	IT担当者 情報セキュリティ担当者	5日間	1,000,000円/1人
Zero to Hero	・CSIRTやSOCメンバーとして、第一線で活躍ができる技術力や判断力をサイバー攻撃の実践を通じて身につける ・セキュリティ全般の知見を広め、インシデントレスポンスやフォレンジック能力を高める	IT担当者 情報セキュリティ担当者	2ヶ月	2,500,000円/1人 3名以上
Basic ICS Distribution Defense	PLCや設備（発電プロセス）のモデルを使い、SCADA環境におけるサイバー攻撃を体験する	OT担当者	2日間	500,000円/1人
Spy Chip Hack **（日本では未実施）**	サードパーティーサプライヤーの脆弱性を使用したサイバーインシデントを確認する	IT担当者 インシデントレスポンスチーム	2日間	700,000円/1人

脆弱性診断『ImmuniWeb®AI Platform』



2016年米Frost&Sallivan社調査：WEB セキュリティテスト市場《最も革新的なポジション》
2017年米Gartner社調査：中堅企業のセキュリティ診断市場におけるCool Vendor選出
2018年SC Awards Europe：サイバーセキュリティ市場における機械学習・AI活用No.1評価

機械学習・AIを活用し、膨大なテストを短期間で完了させることが可能
①世界各国の法制度・ガイドラインに準拠（NIST、GDPR、PCIDSS、HIPAAなど）
②国際的な脆弱性規格に準拠（CVE、CVSSなど）
③ハッカーの攻撃手法を網羅（OWASP Top10, CWE/SANS Top25など）

ImmuniWebは160以上のクラウドマシンを組み合わせたハイスペックのバーチャルプラットフォーム、短時間で高速、網羅的にアプリケーションを巡回し、優先度の高い順にAIでスクリーニングした診断を実現。このプラットフォームをいち早く無料で公開したことにより、グローバル通算で4000万件のWEBサイト検査実績、50万件のスマートフォンアプリ検査実績を保有し、この点は他の製品を圧倒。大手ベンダのAI検査プラットフォームに比べても上位評価。

CEL TLPT※シリーズ　一覧

	プラン名	内容	期間	見積方法
1	CEL Discovery	WEB、モバイル、IoT（IPカメラ、複合機、VoIPシステム・IP電話、ルータなど）、クラウド、ダークウェブ上の漏洩アカウントなど外部からの調査。年間プランではCSIRTチームの業務をサポート	10営業日～	プロジェクトスコープに応じてお見積り
2	CEL Assessment	①ネットワーク・プラットフォーム診断 ②WEBアプリケーション診断・モバイル・IoT診断 ③おまとめプラン	10営業日～	プロジェクトスコープに応じてお見積り
3	CEL Evaluation	WannaCry、Stuxnet、Emotetなどの典型的なマルウェアの挙動や高度持続型攻撃（APT）をシミュレーション。オンサイトでPCを3台お借りして端末がマルウェアに汚染した場合の影響範囲をシミュレーション（マルウェアはインストールせず、セキュリティスペシャリストが手動＋ツールで診断を実施）。MITRE ATT&CK Matrixを参考とした評価を実施。導入済みのセキュリティ製品の検知状況や有効性を評価	10営業日～	プロジェクトスコープに応じてお見積り
3.1	CEL Evaluation Blackbox	名刺一枚の情報から企業のITネットワーク、OTネットワークに侵入（CEL Evaluationのブラックボックステスト） ☑拠点確立、権限昇格、ネットワーク構成図および機密情報の取得 ☑開発環境、R&D部門、IT管理者権限、産業制御機器などへの侵入を想定 ※リモートからのAPT攻撃を想定 ※物理的な攻撃に対する評価はオプション。施設内侵入、無線Wifi、マウス、キーボード、USB、ドローンなどを用いた攻撃	2～3か月	プロジェクトスコープに応じてお見積り
4	CEL Governance	NIST CSF、NIST SP800-171、NIST SP800-53、ISO27001、CSMS、NIST Framework for Improving Critical Infrastructure Cybersecurity、IPA推奨項目などを参考とした組織のセキュリティ体制評価	10営業日～	プロジェクトスコープに応じてお見積り
5	CEL TLPT	CEL Discovery/CEL Assessment/CEL Evaluation/CEL Governanceを含む診断パッケージ。重要インフラの経営上のサイバーリスクを網羅的に検査	2～3か月	プロジェクトスコープに応じてお見積り
6	CEL Outsourcing	EDR、SIEM、ログ監視の人材不足に対応。お客様インフラ状況に応じてセキュリティスペシャリストが社内セキュリティ環境修正やCSIRTチームのインシデントレスポンスを支援。PC端末、サーバ、IoT端末、OT機器などSoC業務のアウトソーシング	1か月～	プロジェクトスコープに応じてお見積り

❑主な市場の変化
金融庁が民間事業者に対して脅威ベースのペネトレーションテストを推奨。年に１回のアプリケーション検査を指示
省庁・独立行政法人がアプリケーション開発に際して納品前のセキュリティ検査を仕様書にて定義
各大手企業グループがアプリケーションに対する年1回のセキュリティ検査をセキュリティガイドラインに追加

・CELが省庁入札資格を取得　省庁調達資格番号0000192892
・CELが経済産業省・情報処理推進機構（IPA）が進める情報セキュリティサービス基準台帳登録認可を取得　台帳登録番号 019-0031

※*TLPT（Threat-Led Penetration Test）：サイバーセキュリティ対策が有効に機能するかを評価する手法で、「脅威ベースのペネトレーションテスト」と訳し、テスト対象企業ごとに脅威の分析を行い、個別にカスタマイズしたシナリオに基づく実践的な侵入テスト*

バルクグループトピックス

トピックス

◆第5回・第6回新株予約権（2020年1月24日発行決議）の行使による資金調達状況（2020年10月末）

【資金使途】子会社への出資及び融資、M&A及び資本・業務提携資金、人件費等の運転資金

回　　号	第５回 (行使価額修正条項付)	第６回 (行使価額修正選択権付※)	合計
発行新株予約権数	10,781個 (1,078,100株)	8,085個 (808,500株)	18,866個 (1,886,600株)
行　使　数	10,781個 (1,078,100株)	7,107個 (710,700株)	17,888個 (1,788,800株)
未行使残高	－	978個 (97,800株)	978個 (97,800株)
行使による調達額	217百万円	144百万円	361百万円

※2020年6月17日に当該選択権を行使し、同月18日より行使価額修正型に転換

【2020年1月24日発行決議ファイナンスによる資金調達実現額】

種　　類	新株式	新株予約権	合計
調達金額	61百万円	366百万円	427百万円

※同時に第2回無担保社債も発行し、アップフロントで60,000千円を調達。新株予約権の行使による調達分により全額繰上償還済み。

トピックス

◆Strategic Cyber Holdings LLC（2020年4月9日公表）
新入社員向けライブ配信型トレーニングプログラムの開始

テレワーク導入が要請されるなか、4月からの新入社員についても在宅勤務を適用する組織が増加。そこで、子会社SCHがCYBERGYM TOKYOにおいて新入社員などを対象とするサイバーセキュリティの基礎知識プログラムを新たに提供。
このプログラムでは、CYBERGYM講師によるLIVE配信講義を1社毎に個別に実施。

【プログラム内容】

1. サイバーセキュリティとは
2. ハッカーの考え方を学ぶ
3. 世界のサイバー攻撃の事例

トピックス

◆株式会社CEL（2020年4月9日公表）「経済産業省 情報セキュリティサービス基準台帳」に登録

子会社CELが経済産業省策定の情報セキュリティサービス基準に合格し、
脆弱性診断サービス事業者として台帳登録承認。

情報セキュリティサービス基準台帳登録内容

事業者名：	株式会社 CEL
事業者登録番号：	019-0031
サービスの種別：	脆弱性診断サービス
サービスの登録番号：	019-0031-20
サービス名：	CEL TLPT シリーズ

トピックス

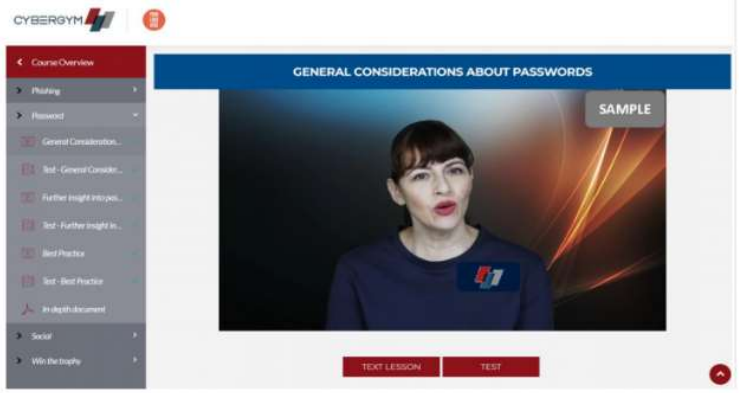
◆Strategic Cyber Holdings LLC（2020年4月16日公表）クラウド型eラーニング『定額制サイバーセキュリティトレーニング』を提供開始

CYBERGYM TOKYOにおいて、サイバージム社と連携し、業務従事者全般を対象とするクラウド型eラーニングによるサイバーセキュリティトレーニングの定額制メニューを2020 年７月より提供

【トレーニングの構成】

1. First Session 9 プログラム、総合確認テスト
2. Second Session 21 プログラム、総合確認テスト
3. Third Session 9 プログラム、総合確認テスト

<本トレーニングのイメージ>　※日本語による提供



トピックス

◆株式会社バルク（2020年4月22日公表）
助成金対応/テレワーク導入・運用コンサルティングサービス提供開始
～新型コロナウイルス対策や激変する働き方への対応を支援～

子会社バルクにおいて、企業等組織におけるテレワークの導入・運用をサポートするため、
新規導入及び運用支援コンサルティングの提供を開始

トピックス

◆CyberGym Control Ltd.（2020年4月23日公表）Microsoft社の Microsoft®Azure™プラットフォームによる専門トレーニングのリモート提供を開始

セイバーセキュリティ分野における共同事業パートナーのサイバージム社が、Microsoft Corporationと連携し、同社のクラウドプラットフォーム『Microsoft®Azure™』を通じたサイバーセキュリティトレーニングのリモート提供を開始。

サイバージム社の大幅な事業拡大に向けた経営戦略に基づく諸施策の一環。
子会社SCHは、日本での中核的な役割を担い、より一層グローバルで革新的なサイバーセキュリティトレーニングを幅広く多数の受講者向けに提供。

これまでの専門トレーニングは、サイバーアリーナ内において集合・実地型で実施。
OTトレーニングなど物理的な専用機器を必要とするプログラムを除き、
リモート環境において、より多数の受講者がホワイトハッカーや専門トレーナーによる効率的かつダイレクトな各専門トレーニングを受講することが可能に。

サイバーセキュリティ専門部署以外の要員も対象とするクラウドベースの多様なトレーニングプログラムの展開を通じて、より多くの受講者向けに、それぞれのレベルに適したサイバーセキュリティに関する知識・スキルの習得機会を提供。

トピックス

◆Strategic Cyber Holdings LLC（2020年4月23日公表）
【テレワーク企業必見】サイバーセキュリティ動画を無料配信

CYBERGYM TOKYOは、新型コロナウイルス感染症対策として、テレワークを緊急導入する企業・団体が急増し、多くの組織にとって初めての取り組みとなるなか、CYBERGYM TOKYOのトレーナーがサイバーセキュリティの観点からテレワークにおけるポイントを簡潔に説明した動画を無料配信。

【本サービスの概要】

配信期間：2020 年 4 月 23 日～5 月 6 日

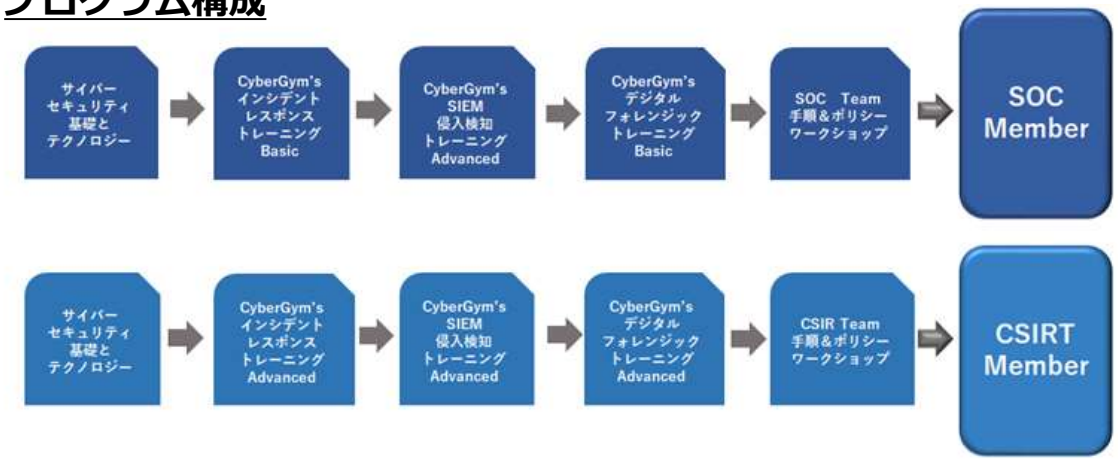
所要時間：30 分

トピックス

◆Strategic Cyber Holdings LLC（2020年4月27日公表）「CYBERGYM’s Zero to Hero program」が経済産業省『第四次産業革命スキル習得講座』に認定

CYBERGYM TOKYOと共同事業パートナーのサイバージム社において開発された
サイバーセキュリティ専門家養成講座。
「CYBERGYM’s Zero to Hero program」が、CYBERGYM TOKYOを申請者として
経済産業省の『第四次産業革命スキル習得講座』に認定。

プログラム構成



トピックス

◆株式会社バルク（2020年4月27日公表）「新型コロナ感染予防対策実施把握調査」提供開始

新型コロナウイルス感染症対策として、在宅勤務、テレワークを緊急導入される企業が急増し、環境の変化による従業員の勤務状態や健康状態を把握し予防することが、企業として急務に。子会社バルクではこれまでのリサーチサービスのノウハウを活かしたパッケージの提供を開始。

活用のポイント

- **具体的な予防対策**
  勤務環境の問題や健康状態の不調を早期に発見することにより予防が可能。
- **感染予防の意識向上**
  調査実施により、従業員は改めて感染予防対策について再認識。
- **コミュニケーションとしての活用**
  不便な環境下で、設問回答や意見を書き込むことで不満や不安を共有。

トピックス

◆Strategic Cyber Holdings LLC（2020年4月27日公表）
サイバーセキュリティ専門トレーニングのリモート提供を開始

CYBERGYM TOKYOが共同事業パートナーのサイバージム社と連携し、
CYBERGYMトレーニングのリモート提供を開始。

サイバージム社は大幅な事業拡大に向けた経営戦略に基づく一貫としてMicrosoft Corporationと連携し、同社のクラウドプラットフォーム『Microsoft®Azure™』を通じたCYBERGYMトレーニングのリモート提供を開始。

これに伴い、サイバージム社のパートナーとして日本において中核的役割を担う子会SCHのCYBERGYM TOKYOにおいて、国内向けCYBERGYMトレーニングのリモート提供を開始。(2020年5月より)

► 中長期的な事業拡大の中核ソリューションとしても期待。メニュー拡充に向け開発を推進。

トピックス

◆Strategic Cyber Holdings LLC（2020年7月6日公表）セキュア開発トレーニングプログラム『Secure coding for developers』を提供開始

CYBERGYM TOKYOが、日本国内において、セキュア開発向けサイバーセキュリティトレーニングプログラムを 2020 年 8 月より提供開始。

製品やシステムを開発する際にはサイバーセキュリティを盛り込んだセキュア開発が今やグローバルスタンダードとなり、日本国内においてもセキュア開発手法を習得したエンジニアの育成が最重要課題。

本トレーニングでは、セキュアな製品を完成させるまでの一連の概念と開発手法の習得を目的とする実践形式を豊富に組み込んだプログラムを提供。

トピックス

◆国内サイバーアリーナの新設(2020年7月15日・８月11日・10月6日公表）
当社と株式会社クロスポイントソリューション(CP-SOL社)間において
サイバーセキュリティ教育事業会社の共同設立で基本合意。
CP-SOLとSCH間においてアリーナ提供契約等を締結。

＜共同事業会社＞
CP-SOL社と当社の合弁会社として株式会社クロスポイントセキュリティジムを
10月に設立。CYBERGYMアリーナによるサイバーセキュリティ教育事業を展開。
親会社はCP-SOL社、当社の持分法適用関連会社

＜アリーナの提供＞
SCH→CP-SOL社
※それぞれ契約上の地位をSCHは新設の当社子会社㈱サイバージムジャパンに、
CP-SOL社は、同社の子会社となる上記共同事業会社に移転予定

＜アリーナの概要＞
名　　称　：CYBERGYM八重洲アリーナ
開設場所　：東京都中央区
開設日　　：2020年11月

►アリーナ提供・保守売上によるストック収益が拡大。これに加え、高稼働が
期待される本アリーナの収益を持分法により取り込み。

トピックス

◆株式会社バルク（2020年9月8日公表）
クラウド型IT資産管理ソリューション『ISM CloudOne』の取扱いを開始

子会社バルクが情報セキュリティ認証取得・運用支援コンサルティングやテレワーク導入・運用支援コンサルティングにおけるソリューションの一環として、
クオリティソフト株式会社が提供するクラウド型 IT 資産管理ソリューション
『ISM CloudOne』の取扱いを開始。

『ISM CloudOne』とは
・管理者の運用負担を軽減するエンドポイントセキュリティ管理ツール。
リモートワークにも対応し、社内や外出先で利用するあらゆる端末（PC・スマートデバイス）の一元管理を実現。管理対象は物理OS・仮想OSにも対応し、操作ログや外部デバイスの利用制御機能による内部不正対策や勤怠管理にも有効。
・クラウド型資産管理サービス市場において、トップシェアを5年連続して維持、これまでの導入実績は65,000社以上。

► 『ISM CloudOne』は、バルク社の情報セキュリティ認証取得・運用支援コンサルティングやテレワーク導入・運用支援コンサルティング等との親和性が非常に高く、これをバルクソリューションに組み入れることで、顧客負担を軽減し、有効な情報セキュリティ管理体制の構築・運用を強力にサポート。

トピックス

◆株式会社バルク（2020年10月13日公表）
システム性能監視のアイビーシー社と業務提携
～性能監視とAIによる脆弱性診断でシステムの可用性と安全性を担保～

子会社バルクとアイビーシー株式会社（以下「IBC」）は、IBCが開発・販売するシステム情報管理ソフトウェア『System Answer G3』および次世代MSPサービス『SAMS』と、バルクが提供する機械学習・AIを用いた脆弱性診断サービス『Immuni Web®』を相互に自社サービ スと組み合わせて提供することにより、顧客システムの可用性と安全性を担保するソリューションを展開することで合意。

企業経営を支えるICTインフラは、新型コロナウィルス対策によるリモートワークの急増やクラウド利用の促進などニューノーマル時代に向けた働き方改革により、今まで以上に可用性と安全性を担保した運用が必須。
『System Answer G3』および次世代MSPサービス『SAMS』は、サーバーやネットワーク、クラウドに展開された企業システムの性能情報を監視・ 管理することで、障害の予兆検知や機器の増強計画策定などを支援し、ICTインフラの快適な継続利用を可能に。

►システムの性能監視に長年取り組んできた専門 ベンダーであるIBCとAIによる脆弱性診断で評価の高いバルクが業務提携を行うことにより、企業経営を支えるICTインフラの可用性と安全性を兼ね備えたシステム運用をワンストップで提供し、高品質なICTインフラの性能監視と脆弱性診断を迅速かつ安価に実現。

トピックス

◆株式会社サイバージムジャパン（2020年10月20日公表）ニュートラル社とサイバーセキュリティトレーニング・セキュリティ診断の販売等サイバーセキュリティ分野で業務提携

子会社サイバージムジャパンはニュートラル株式会社（以下「ニュートラル社」）とニュートラル社の顧客基盤及び販売ネットワークを活用したサイバーセキュリティ教育・トレーニング、セキュリティ診断等のサイバージムソリューションにかかる販売提携契約を締結。

ニュートラル社は、「デジタルトランスフォーメーション」の時代に日本が抱える人口減少・高齢化、エネルギー問題、インフラ老朽化など多くの課題に対するソリューションを提案し、ICT 技術と豊富な実績で、中部東海圏企業の成長を支え、地域社会の発展に貢献。

►ニュートラル社の保有する名古屋・大阪・静岡・金沢エリアにおける幅広い販売網を通じて、サイバージムジャパンのサイバーセキュリティソリューションを提供することが可能に。

トピックス

◆株式会社CEL（2020年11月16日公表）
米EnterpriseSecurity誌よりマネッジドセキュリティサービスプロバイダー分野アジア太平洋地域Top10に選出

当社子会社CELが、米「EnterpriseSecurity」誌よりマネッジドセキュリティサービスプロバイダー分野でアジア地域Top10に選出。

EnterpriseSecurityは欧米及びアジア地域にて約12万部発行されているセキュリティ大手専門誌。毎年購読者や顧客を対象とした市場調査を実施しており、今回の調査では企業での決裁権を持つCIO、CISOやセキュリティ専門家の推薦をもとに急成長しているアジア太平洋地域のセキュリティサービス事業者として選出。

免責事項

本資料に記載されている当社の予想、見通し、目標、計画、戦略等の将来に関する記述は、本資料作成の時点で当社が合理的であると判断する情報に基づき、一定の前提（仮定）を用いており、マクロ経済動向及び市場環境や当社グループの関連する業界動向、その他種々の要因により、実際の業績はこれらの予想・目標等と大きく異なる可能性があります。

当社は、これらの将来の見通しに関する事項を常に改定する訳ではなく、またその責任も有しません。

なお、本資料は投資判断のご参考となる情報の提供を目的としたもので、投資勧誘を目的として作成したものではありません。本資料利用の結果生じたいかなる損害についても、当社は一切責任を負いません。

ＩＲ及び本資料に関するお問い合わせ

株式会社バルクホールディングス
IR担当

TEL：03-5649-2500