

Cyber Security Market Report



HATASE HOLDINGS Co., Ltd.
CEO & Owner Kyosuke Hatase
Research, Advisory, Asset Management
Fund: 22 Jan 2015
Capital: 50,000,000 JPY
7-13-6 GINZA TOKYO JAPAN

株式会社HATASE HOLDINGS
代表取締役 畑瀬 匡甫(100%オーナー)
リサーチ、アドバイザリー、持ち株の管理・運用
設立日：2015年1月22日
資本金：5000万円
所在地：東京都中央区銀座7丁目13-6 サガミビル

Cyber Security Market

サイバーセキュリティ業界は世界的にも、日本の政策としても、日本企業の経営課題としても、注目が集まっており、セクター全体の企業価値が高まると考えた。その根拠を示す。

□2015年9月4日「サイバーセキュリティ戦略について」の閣議決定において、「サイバーセキュリティ関連産業の振興」、「我が国企業の国際展開のための環境整備」といった国家戦略の方向性が示された。

5.1.2 セキュリティマインドを持った企業経営の推進

連接融合情報社会における企業経営に当たっては、従前からのサイバーセキュリティ確保のための取組はもとより、新たなビジネスの創出等のためにも、これまで以上に、セキュリティリスクの把握や経営資源に係る投資判断を適切に行い、製品・サービスへのセキュリティ機能の実装の推進、セキュリティ人材の育成、組織能力の向上等を図ることが必要となってくる。

このため、我が国企業において、セキュリティマインドを持った企業経営を浸透させることを目指し、以下の取組を実施する。

(1) 経営層の意識改革

企業の経営層が、事業の基盤として用いるシステムや営業秘密の事業戦略上の価値・役割を認識して活用することは、企業経営において不可欠なものである。また、高いレベルのセキュリティ品質が確保された製品・サービスを市場に投入し、新たなビジネスを創出する経営判断に当たり、サイバーセキュリティに関する素養が企業経営層の必須能力となりつつある。こうした社会の変化をより多くの企業経営層が的確に認識し、セキュリティ対策はやむを得ない「費用」ではなく、より積極的な経営への「投資」であるとの認識を醸成していくことは、我が国の経済社会の活力の向上及び持続的発展のために必要である。このため、サイバーセキュリティを経営上の重要課題として取り組んでいることが市場や出資者といったステークホルダーから正当に評価される仕組みや資金調達等の財務面で有利となる仕組みの構築、認識醸成のための官民が一体となった啓発活動を実施する。

また、各企業が、事業戦略としてサイバーセキュリティを確保していくためには、経営層において、セキュリティに関する最高責任者を置くことが必要となる。このため、CISO(Chief Information Security Officer)の機能が各企業の経営層に確実に位置付けられるよう、官民で連携して促す。

(2) 経営能力を高めるサイバーセキュリティ人材の育成

サイバーセキュリティの考え方や能力を、企業経営において使いこなすためには、経営層と実務者層の双方が、経営戦略やサイバーセキュリティに関する課題や解決の方向性を共有する必要がある。このため、経営層の示す経営方針を理解し、サイバーセキュリティに係るビジョンの提示や、実務者層との間のコミュニケーションの支援を行う橋渡し人材層の育成を推進する。

また、企業経営や事業戦略において、サイバーセキュリティ確保のための取組が不可欠になるにつれ、企業の内部人材としてサイバーセキュリティ人材を育てていく必要性が高まっている。このため、サイバーセキュリティを担う実務者層、橋渡し人材層、セキュリティリスクを含む企業

のリスクマネジメントに責任を有する経営層といったキャリアパスを考慮した長期的な人材育成や人事評価の在り方について検討し、経営層に訴求する取組を展開する。

(3) 組織能力の向上

接続融合情報社会においては、製品・サービスにセキュリティを取り込んでいくことが、企業の競争力強化に貢献し、企業活動の維持・発展の基盤となることから、企業における製品・サービスの関係者がセキュリティ・バイ・デザインを共通の価値として認識することを促していく。また、営業秘密保護や事業継続の観点から、リスク分析に基づく組織運営を行うよう促していくなど、有効な経営の在り方を発信・推進する。組織の壁を越えたサプライチェーン全体でセキュリティを向上するための方策を講じていく。

さらに、企業における深刻な事業リスクであるサイバー攻撃等の事象への対応能力の向上に当たっては、インシデントの検知・対応の窓口機能を有するCSIRT(Computer Security Incident Response Team)の設置・運用、迅速な対応・復旧に向けた計画やツールの整備、演習の実施、対外説明機能の強化等が有用であることから、こうした取組を促し、名実ともに充実を図る。加えて、経営層のリーダーシップの下での体制整備、最新のサイバー攻撃の手口や被害の状況等を踏まえた有効な対策、情報開示等の在り方についてサイバーセキュリティに係る経営のガイドライン等により企業に対して発信していくとともに、それを踏まえた企業の取組が第三者認証等により客観的に評価される仕組みを確立していく。また、対策の際の課題、ベストプラクティス、最新の脅威情報やインシデント情報等の共有のため、サイバーセキュリティについて知見を有する独立行政法人、ISAC (Information Sharing and Analysis Center)を含むインシデント情報共有・分析機能を有する機関等を積極的に活用しつつ、情報共有のためのプラットフォーム構築等、民間・官民間における一層の情報共有網の拡充を進める。

5.1.3 セキュリティに係るビジネス環境の整備

我が国のIoT産業6を含む情報通信技術を活用した関連産業が国際競争力を有し、もって我が国経済をけん引していくとともに、我が国が自立的にサイバーセキュリティの確保を行う能力を有していくためには、我が国において、サイバーセキュリティ関連産業が成長産業となるような環境整備を行っていくほか、あらゆるビジネスの基盤となる公正な市場環境の整備を行っていく必要がある。このため、我が国企業のセキュリティ確保及び国際競争力強化の基盤となるビジネス環境の整備に向けて、以下の取組を実施する。

(1) サイバーセキュリティ関連産業の振興

IoT産業等の関連産業の成長に伴い、今後、コンサルティングや人材育成ビジネスを含むサイバーセキュリティ関連産業に対する需要が一層増加することが見込まれる。このため、我が国において、サイバーセキュリティ産業がこうした需要を捉え、成長産業となるよう、国内外で大規模に活躍できる企業やベンチャー企業の育成等によりこれを振興していく。

まず、サイバー関連情報に係るグローバルな情報収集網や、こうした情報の分析・提供能力を有する産業の振興のため、政府系ファンドの活用によりサイバーセキュリティ分野への大規模かつ集中的な投資を行うなどにより、我が国のサイバーセキュリティ関連産業のリーディングケースを確立する。

また、単独で十分なセキュリティ環境を実現することが困難な中小企業等についてはセキュリティが確保されたクラウドサービスを活用することが有効であると考えられるため、クラウドサービスに関するセキュリティ監査等の普及を促進させていく。

加えて、変化が激しく機動性の求められるサイバーセキュリティ分野においては、革新的な新規事業や技術開発に挑戦するベンチャー企業等の活性化が重要である。このため、サイバーセキュリティ分野において、政府系ファンドの活用によるベンチャー企業同士の国際的な交流を含む共同研究開発等の促進、公的研究機関とベンチャー企業との共同研究開発の促進、研究開発成果を活用したベンチャー企業の育成等の取組を行う。

さらに、サイバーセキュリティに関連する産業の振興に向けて制度の見直しを柔軟に検討していく必要がある。このため、例えば著作権法におけるセキュリティ目的のリバースエンジニアリングに関する適法性の明確化や、所要の制度の見直しについて検討を行う。

(2) 公正なビジネス環境の整備

イノベーションが絶えず生まれ、企業収益につながる経済システムを構築するためには、企業における基幹技術、製造ノウハウといった技術情報の価値を守ることが必要不可欠である。このため、企業の知的財産の漏えい防止及びこれが侵害された場合の措置を強化するための法整備、啓発活動、実践的な訓練・演習等を実施していく。また、セキュリティを理由に国際的な貿易のルールに不適切な影響を及ぼす措置に対しては、国際的な連携の下、厳格に対処する。

(3) 我が国企業の国際展開のための環境整備

我が国のIoT産業やサイバーセキュリティ関連産業が、国際競争力を有し、もって成長産業として我が国経済をけん引していくためには、国際的なルール等に我が国の立場を十分に盛り込んでいくことが重要である。このため、制御装置等を含むIoTシステムのセキュリティに係る国際的な標準規格や評価・認証制度の国際的な相互承認への枠組み作りについて、産学官が一体となり、国際的議論を主導していくほか、我が国のベストプラクティスの国際的な共有・展開を図る。

また、我が国のIoT産業やサイバーセキュリティ関連産業の国際展開に当たっては、IoTシステムで生成・流通されるデータのセキュリティを始め、海外の社会基盤におけるセキュリティの確保が不可欠となる。このため、我が国と経済的結びつきの深い東南アジア諸国連合(ASEAN)諸国等において必要な制度整備の支援、普及啓発活動等を行う。

加えて、近年、我が国企業の国際展開等に伴い、いわゆるサプライチェーン・リスクへの対策も重要となってきている。このため、サプライチェーン・リスクへの対策として、例えば必要な研究開発や、ASEAN諸国等の国・地域との協力を推進する。

出所) 平成27年9月4日 閣議決定「サイバーセキュリティ戦略について」

<https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf>

□G7においても、サイバーセキュリティに関するガイドラインが発表されている。

出所) G7 FUNDAMENTAL ELEMENTS OF CYBERSECURITY FOR THE FINANCIAL SECTOR

https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

図表 3 Global Cybersecurity Index における日本のウィークポイント

#	Member State	GCI Score	Cybersecurity metrics	Incentive mechanisms	Public-private partnership
1	Singapore	0.925	Leading	Leading	Leading
2	United States of America	0.919	Leading	Leading	Maturing
3	Malaysia	0.893	Leading	Leading	Leading
4	Oman	0.871	Leading	Leading	Leading
5	Estonia	0.846	Leading	Maturing	Maturing
6	Mauritius	0.830	Leading	Leading	Leading
7	Australia	0.824	Leading	Maturing	Initiating
8	Georgia	0.819	Leading	Leading	Leading
8	France	0.819	Maturing	Leading	Maturing
9	Canada	0.818	Leading	Maturing	Leading
10	Russian Federation	0.788	Leading	Leading	Leading
11	Japan	0.786	Initiating	Initiating	Initiating

【凡例】 Leading Maturing Initiating

Cybersecurity metrics (評価基準) : 国レベルのサイバーセキュリティ成熟度評価基準を定め、定期的に定量的に評価するもの

Incentive mechanisms (インセンティブの仕組み) : 自国のサイバーセキュリティに対する動機付けや支援

Public-private partnerships (官民連携) : 官民が協力して、インシデント予防や対応に協力する仕組み

□官民提携で日本は出遅れているが、上記の政策もあり、日本企業にとっては事業機会が大きくなると考えられる。

出所) 一般社団法人 日本サイバーセキュリティ・イノベーション委員会

諸外国におけるサイバーセキュリティの情報共有に関する調査

<https://www.j-cic.com/pdf/report/>

CybersecurityInformationSharingSurvey-20180309(JP).pdf

□経済産業省、内閣サイバーセキュリティセンター、独立行政法人 情報処理推進機構が連携して各業界へのサイバーセキュリティの底上げを図る

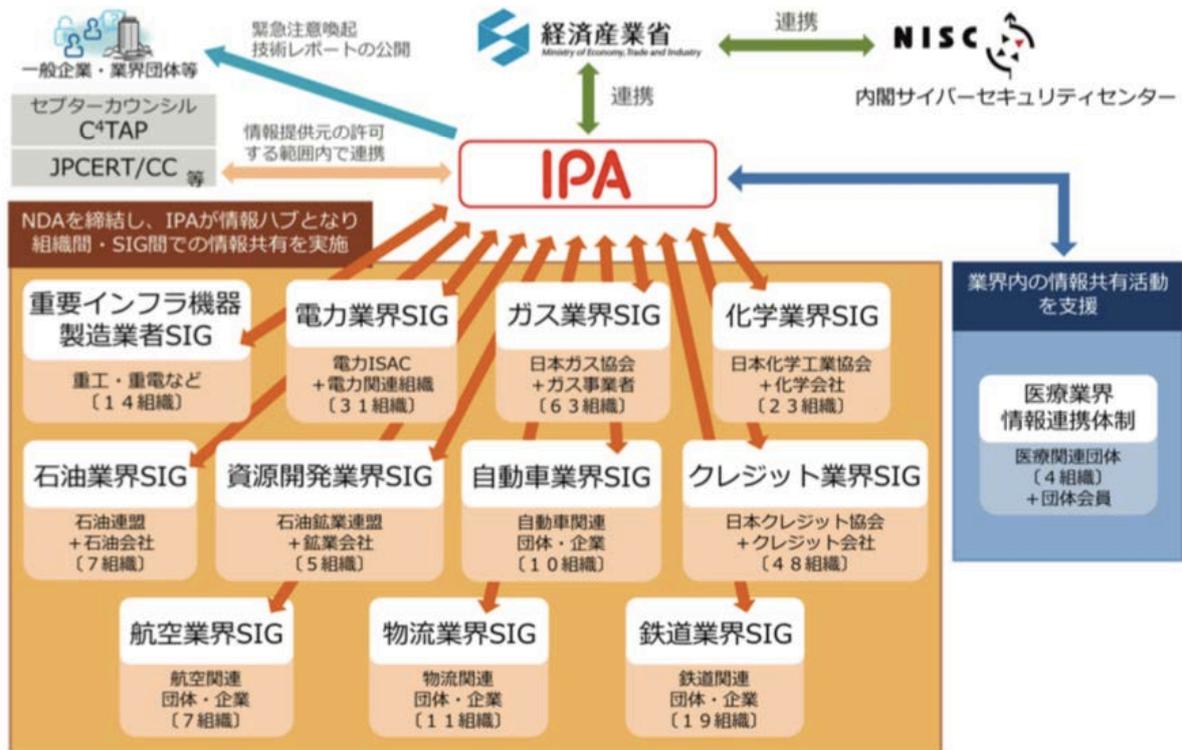
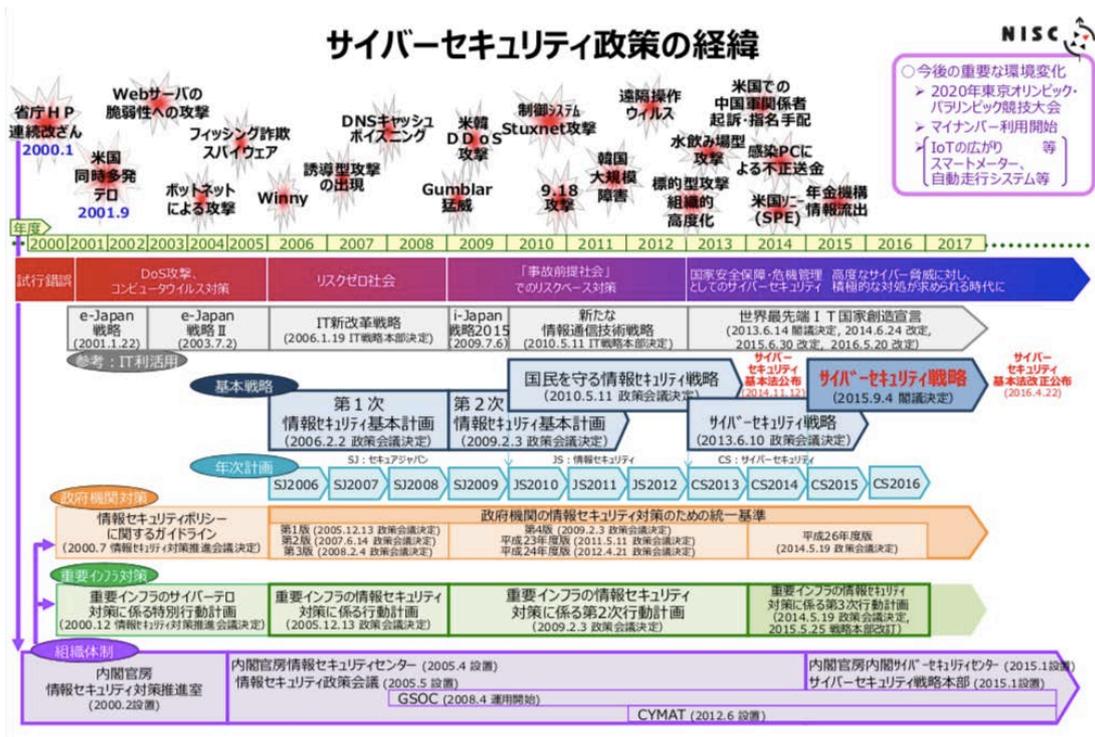


図 1 J-CSIP の体制図

出所) サイバー情報共有イニシアティブ(J-CSIP) 運用状況 [2018 年7月~9月]

<https://www.ipa.go.jp/files/000069662.pdf>

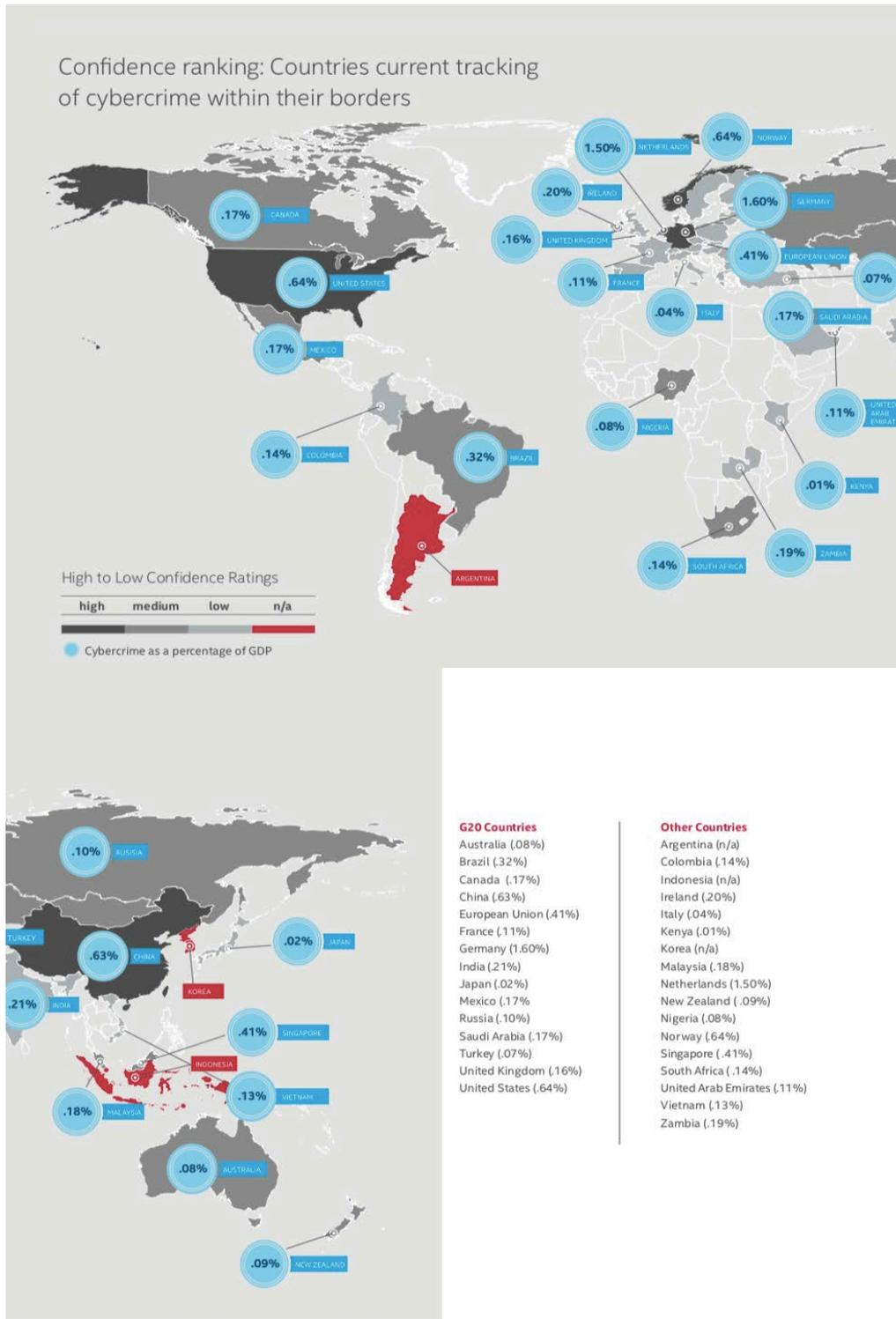
□サイバーセキュリティ政策の経緯として、2020年の東京オリンピックに向けて法整備と具体的な施策を急がなければならない。



出所) 我が国のサイバーセキュリティの概要

http://www.soumu.go.jp/main_content/000463592.pdf

□米国のシンクタンクである戦略国際問題研究所（CSIS：Center for Strategies and International Studies）の調査レポートによると、サイバー犯罪による世界全体の経済的被害額を3750億～5750億ドルと試算している。これは世界のGDPの0.5～0.8%に相当する。世界的な課題である。



出所) Net Losses: Estimating the Global Cost of Cybercrime

https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

CRESTにおけるサイバーセキュリティレポート。

CREST is an international not-for-profit accreditation and certification body that represents and supports the technical information security market.



出所) CREST

<https://www.crest-approved.org/index.html>

出所) CBEST Implementation Guide

<https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf>

□サイバーセキュリティ分野へ投資するファンドの業績が好調で、まだ株価が上がってない日本企業の中に、このようなパフォーマンスが期待できる銘柄があると考えた。

成長が期待される サイバーセキュリティ市場

■インターネット活用の拡大や個人情報保護規制への対応によるセキュリティ対策需要増加などを背景に、今後もサイバーセキュリティ市場は拡大していくと期待されています。
 ■サイバーセキュリティ関連企業の株価は、情報技術株式を上回って堅調に推移し、売上高も2桁成長を続けてきました。

拡大するサイバーセキュリティ市場

世界のサイバーセキュリティ市場規模予測
(億米ドル)

出所：statistaのデータを基に三菱UFJ国際投信作成
期間：2016年～2021年、年次 ※全て予測値です。

成長が期待されるサイバーセキュリティ関連企業

サイバーセキュリティ関連企業* パフォーマンス (左) と売上高成長率 (右)

出所：Datastreamのデータを基に三菱UFJ国際投信作成 期間：左→2012/12/31～2018/3/14、日次 右→2013年～2017年、年次
 ※左図は、前年度比で表示しています。また、世界情報技術株式は指数のトータルリターンを基に算出しています。
 ※計算期間が異なる場合は、結果も異なる点にご注意ください。
 *サイバーセキュリティ関連企業は、2018年2月末時点の当ファンド購入銘柄とここでは定義しています。パフォーマンスは各銘柄のトータルリターンの単純平均を使用しています。売上高成長率は各銘柄の年次成長率の単純平均です。

日本のサイバーセキュリティに関する当初予算

325.8億円	498.3億円	598.9億円	727.5億円
平成27年度	平成28年度	平成29年度	平成30年度

平成30年度は、東京オリンピック・パラリンピックに向けた態勢の整備やIoTについてのセキュリティ対策の予算などを新たに計上

※内閣サイバーセキュリティセンターの発表資料を基に三菱UFJ国際投信作成

※「本資料で使用する数値について」および「本資料でご覧いただきたい事項」を必ずご確認ください。
 ※上記は、過去の業績・状況または作成時点での見込み・分析であり、将来の市場環境の変動や運用状況・成果を予測・保証するものではありません。また、為替・税金・手数料等を考慮しておりません。

当ファンドの運用状況

■設定後約8ヵ月で為替ヘッジなしは18%、為替ヘッジありは23%上昇しています (2018/3/14時点)。

為替ヘッジなし

課税前分配金再投資換算基準価額と純資産

為替ヘッジあり

課税前分配金再投資換算基準価額と純資産

期間：2017/7/13 (設定日)～2018/3/14、日次
 ※基準価額 (円) (右軸) は、課税前分配金再投資換算後のものです。※課税前分配金再投資換算基準価額は、当ファンドの各日、各投資先(課税前)をその分配金再投資したと仮定して算出したものであり、三菱UFJ国際投信が公表している基準価額とは異なります。

※「本資料で使用する数値について」および「本資料でご覧いただきたい事項」を必ずご確認ください。
 ※上記は、過去の業績・状況または作成時点での見込み・分析であり、将来の市場環境の変動や運用状況・成果を予測・保証するものではありません。また、為替・税金・手数料等を考慮しておりません。

出所) 三菱UFJ国際投信株式会社 サイバーセキュリティ株式オープン
https://www.am.mufj.jp/text/261647_180402.pdf

□近年のサイバーセキュリティ重大事件を参考に、サイバーセキュリティ対策の被害額と対策にかかる費用を予測し、対策をする企業が増えるだろう。

2016年の10大セキュリティ事件ランキング（マカフィー）

順位	セキュリティ事件（時期）	認知度（%）
1	振り込め詐欺／迷惑電話による被害（1年を通して）	51.7
2	大手金融機関やクレジットカード会社などをかたるフィッシング（1年を通して）	36.9
3	人気のPokemon GOをかたる偽アプリを発見（2016年7月）	35.8
4	公共無線LANのセキュリティ問題（1年を通して）	33.4
5	国際的ハッカー集団「アノニマス」による日本への攻撃（2015年10月～2016年2月）	28.9
6	米連邦捜査局（FBI）が米アップルに対して、銃乱射事件の犯人が使っていたiPhoneのロック解除を要請、プライバシーの問題に注目が集まる（2016年2月）	28.9
7	米ヤフーで、国家が関与するとみられるサイバー攻撃を2014年に受け、5億人以上の個人情報が流出（2016年9月）	28.9
8	JTBで、旅行商品をインターネット販売する子会社が標的型攻撃のメールからマルウェアに感染、最大約793万人分の個人情報が流出した可能性（2016年6月）	28.3
9	ランサムウェア（身代金ウイルス）の被害（1年を通して）	28.0
10	佐賀県で、県立学校の情報システムが不正アクセスを受け、個人情報を含むファイル約15万3000件が漏えい、17歳の少年が逮捕される（2016年6月）	21.6

順位	セキュリティ事件（時期）	認知度（%）
1	ランサムウェア「WannaCry / WannaCrypt（ワナクライ）」の大規模な攻撃が世界中で確認され、国内でも製造や運輸などの業界で被害が発生（2017年5月）	36.7
2	Amazonをかたるフィッシングメール／「Amazon」の利用者を狙ったフィッシング攻撃が発生／大手宅配業者の商品の発送や宅配便のお知らせを装った偽メールが増加（2016年11月～2017年1月）	36.2
3	無線LANの暗号化規格であるWPA2の脆弱性（KRACK / KRACKs）が発見される（2017年10月）	32.8
4	米Yahoo!で、不正アクセスにより最終的に30億人以上のユーザー個人情報が漏えいしていたことが判明（2017年10月）	32.3
5	ランサムウェアや遠隔操作ウイルスの作成、フリーマーケット アプリへのマルウェア関連情報の出品など、中高生によるサイバー犯罪で逮捕者が続出（2017年6月～9月）	27.2
6	Appleを装い、アカウント情報を詐取するフィッシング攻撃が確認される（2017年2月）	26.0
7	女優や女性アイドルなどの芸能人が画像を保存するなどしていたインターネットサーバーに不正にログインしたとして、無職の男を書類送検（2017年4月）	23.0
8	防衛省と自衛隊の情報基盤がサイバー攻撃を受けたとの報道（2016年11月）	20.4
9	女性タレントや女性アイドルらの電子メールサービスなどに不正接続したとして、大手新聞社の社員を逮捕（2016年11月）	19.3
10	日本マクドナルドのシステムがマルウェアに感染し、外部に向けて大量のバケットを発信して通信を圧迫、商品購入時のポイントサービスが利用不能に（2017年6月）	18.8

表 1：2017年 個人情報漏えいインシデント 概要データ【速報】

漏えい人数	519万 8,142人
インシデント件数	386件
想定損害賠償総額	1,914億 2,742万円
一件当たりの平均漏えい人数	1万 4,894人
一件当たり平均損害賠償額	5億 4,850万円
一人当たり平均損害賠償額	2万 3,601円

表 2：2017年 個人情報漏えいインシデント トップ10

No.	漏えい人数	業種	原因
1	118万 8,355人	製造業	不正アクセス
2	67万 6,290人	公務	不正アクセス
3	59万 7,452人	情報通信業	不正アクセス
4	37万 1,200人	情報通信業	不正アクセス
5	19万 9,169人	公務	不正アクセス
6	19万人	サービス業	管理ミス
7	18万 4,981人	公務	管理ミス
8	16万 3,000人	公務	紛失・置忘れ
9	14万 408人	情報通信業	不正アクセス
10	13万 1,936人	卸売業, 小売業	不正アクセス

© Copyright 2018 NPO Japan Network Security Association (JNSA)
2/8

出所) NPO法人 日本ネットワークセキュリティ協会

2017年 情報セキュリティインシデントに関する報告書【速報版】

https://www.jnsa.org/result/incident/data/2017incident_survey_sokuhou_ver1.1.pdf

□重大セキュリティインシデントとして、最大規模の個人情報漏洩で会ったベネッセホールディングスを参考にする。

事件発生年月	2013年12月から情報の不正な持ち出しが始まる。2014年7月9日に事件発覚。
損害範囲	進研ゼミをはじめとする教育サービスの登録者の個人情報である、保護者氏名、子どもの氏名、子どもの性別、子どもの生年月日、住所、出産予定日、メールアドレス、合計3504万件が流出した。
原因	ベネッセホールディングスの再委託先であるエンジニアの派遣社員が、会社からの貸与PCに個人のスマートフォンを充電するために接続した際に、データの移行が可能であると気づいた。その社員のギャンブルによる借金300万円の返済の目的で、約20回にわたりデータの持ち出しが行われた。複数の名簿屋に売られた個人情報は、ジャストシステム、ECC、全国の学習塾、予備校、着物販売店などに転売され、その後、ベネッセ会員に各社からのダイレクトメールが届いたことを不審に思ったベネッセ会員からの問い合わせにより、事件が発覚した。
直接被害	2014年4月期の有価証券報告書に、260億円の特別損失を計上した。内訳は、顧客会員への補償が200億円、お詫びの文章の発送、事件の調査、セキュリティ対策に60億円であった。
間接被害	1年間で94万人の会員が流出した。翌年の2015年3月期の業績は、営業収益は146億円から93億円に36%減少、当期純利益は106億円の黒字から20億円の赤字に減少。
経営者の責任追及	福島保副会長と明田英治取締役が引責辞任。原田永幸会長兼社長は業績悪化の責任を取り2年後に辞任。
訴訟	約1万人の「被害者の会」により集団訴訟を受けている。また被害者180人がベネッセホールディングスと関連会社に1478万円（一人当たり3～10万円）の損害賠償請求。株主代表訴訟で元取締役6名に対して260億円の訴訟を提起。

出所) ベネッセホールディングス 第61期 有価証券報告書
<http://pdf.irpocket.com/C9783/SAip/pPe1/Hwba.pdf>

樋口晴彦 ベネッセ顧客情報漏えい事件の事例研究
https://ci.nii.ac.jp/els/contentscinii_20180624102242.pdf?id=ART0010513157

以上のデータから、サイバーセキュリティ業界は成長すると考え、このセクターから比較優位性の高い企業を選定することとした。

Industry Analysis

サイバーセキュリティ関連の上場企業には下記のような企業が存在する。

2158 フロンテオ

<http://www.fronteo.com>

▶売上5期連続成長。しかし3期連続赤字で、今期は黒字転換

▶東証マザーズ上場。時価総額315億円(2018/11/22時点)

▶東証一部上場のサイバーセキュリティ企業である株式会社フォーカスシステムズが7.8%保有の大株主

▶ディスカバリは米国民事訴訟で被告・原告の双方が審理前に証拠を開示する制度です。特に、電子データを取り扱う作業はeディスカバリと呼ばれます。当社は、アジアにおけるeディスカバリ総合支援企業のパイオニアとして、証拠となりうる電子データの特定、証拠保全からデータの処理、ドキュメントレビュー、提出データ作成にいたるまでワンストップでサービスを提供しております。

▶フォレンジックサービスとは、情報漏洩や内部不正等の問題が生じた際に、顧客からの依頼を受けて提供された

パソコン等を、いつ、誰が、どのようなことをしたのか不正調査の観点から調査し、調査結果を顧客へ提供するサービスです。また、当社グループは日本発のデジタルフォレンジックソフトウェアとして独自の人工知能「KIBIT」を搭載した「Lit i View XAMINER(リットアイビューエグザミナー)」の販売を行っております

▶「KIBIT Email Auditor(キビットイメールオーディター)」、特許調査・分析システム「KIBIT Patent Explorer(キビットパテントエクスプローラ)」、ビジネスデータ分析システム「KIBIT Knowledge Probe(キビットナレッジプローブ)」等のソフトウェア販売、運営サポートをはじめ、企業内データ解析を様々な角度から行っております。

▶当社独自の人工知能「KIBIT」を搭載したコミュニケーションロボット「Kibiro(キビロ)」の開発および販売、

人工知能「KIBIT」を活用したデジタルコミュニケーションに関するソリューションの提供を行っております。

▶医療機関や民間企業をサポートすることを目的とした子会社である株式会社FRONTEOヘルスケアを中心に、ヘルスケア関連ビッグデータの利活用を促進することを目的に独自開発をした人工知能エンジン「Concept Encoder (コンセプトエンコーダー)」を活用することで、医療現場の業務改善をサポートするソフトウェアやシステム、また医師の診断を支援する機器の開発および販売を行っております。

情報漏洩や内部不正などの問題が発生した際の調査業務

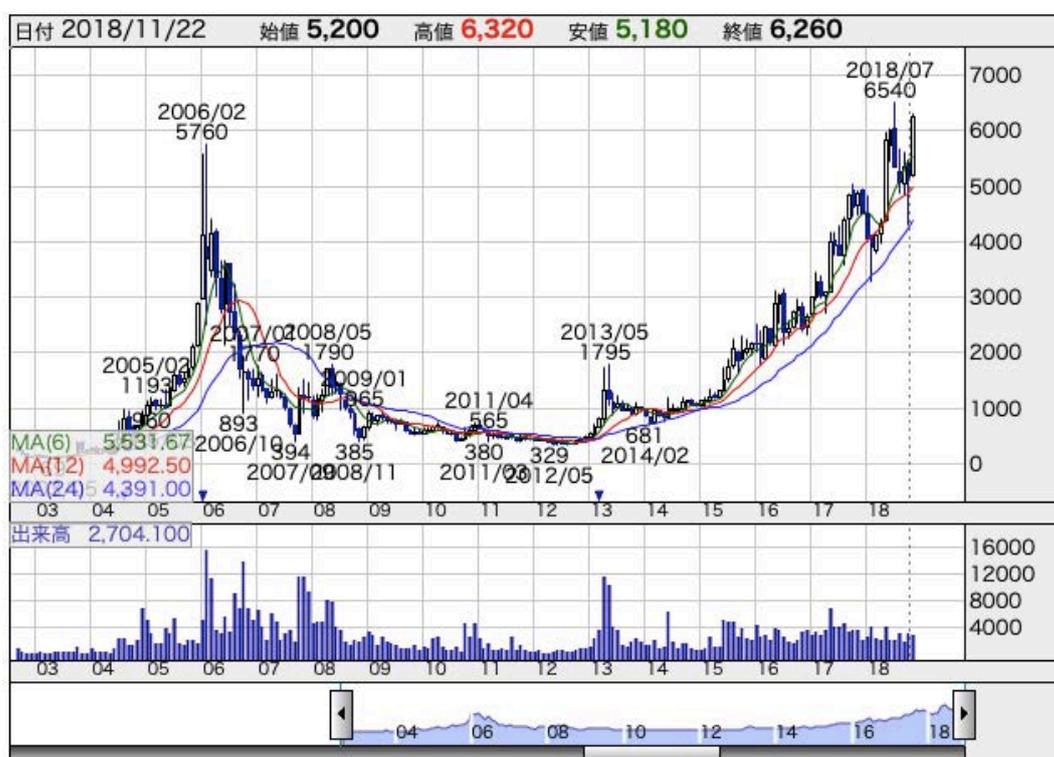
2326 デジタルアーツ

<https://www.daj.jp>

▶5期連続で売上成長、利益成長、純資産増加

- ▶ 株価は6年で20倍成長
- ▶ 東証一部上場。時価総額884億円(2018/11/22時点)
- ▶ 売上総利益率が80%と高い
- ▶ 当社グループは、当社および連結子会社4社により構成され、Webセキュリティ、メールセキュリティ、およびファイル暗号化・追跡ソリューションの企画・開発・販売等を主要な事業としております。
- ▶ インターネットセキュリティ関連ソフトウェア、アプライアンス製品（特定用途の電子機械）の企画、開発、販売
- ▶ 「FinalCode」(ファイル暗号化・追跡ソリューション)の開発・販売
- ▶ 情報セキュリティコンサルティング等
- ▶ 日経ビジネスONLINEの取材に答える創業者 道具 登志夫氏

<https://business.nikkeibp.co.jp/atcl/report/15/269655/092800001/>



2327 新日鉄住金ソリューションズ

<https://www.nssol.nssmc.com>

- ▶ 情報システムのコンサルティング。主に、IT資産分析、評価、IT戦略・ロードマップ、全社アーキテクチャ検討、IT組織、事業課題に関するIT施策検討、プロジェクト構想、IT投資事後評価、情報システム基盤統合・最適化、クラウド等新規技術採用検討、データマイニング、統計モデル化、データ統合検討
- ▶ 業務・流通システムソリューション。主に、自動車・自動車部品、電機・精密機器、機械・エンジニアリング、鉄道・電力、食品・飲料、ネット・メディア・サービス、一般消費財、流通・小売、医薬、旅行などの業界に提供している
- ▶ 金融ソリューション。統合市場系業務ソリューション「TSSummit」、ディーリングフロント・ミドル・バックシステムなど。ALM・原価計算、統合収益・リスク管理「BancMeasure」

シリーズ、信用リスク、バーゼル対応(新BIS規制)・IFRS対応など。ストラクチャリング・シミュレーション、住宅ローン証券化、情報配信サービス、コモディティリスク管理「Ratispherd」など。最新のオープンシステム技術を用いた情報系統DBなど信頼性の高いシステム基盤構築、レガシーリエンジニアリングなど。外為インターネットサービス「CrossMeetz」、金融機関財務関連情報提供サービス「BancMonitorContrast」、ATMローン事業向け与信判定サービスなど。

- ▶ 5期連続で売上、利益、純資産が成長
- ▶ 東証一部上場。時価総額3049億円(2018/11/22時点)
- ▶ 新日鐵住金(株)が61.29%保有の大株主



2467 バルクホールディングス

<https://www.vlcholdings.com>

- ▶ サイバーセキュリティトレーニング施設の設立・運営
- ▶ プライバシーマーク認定取得や ISO27001 認証取得
- ▶ 2018年に大幅は役員変更と事業内容の変更を行った
- ▶ 名証セントレックス。時価総額36億円(2018/11/22時点)

3021 パシフィックネット

<http://www.prins.co.jp>

- ▶ IT機器の導入、運用、管理、使用後の機器の廃棄までをワンストップでサポートを行うLCM（ライフサイクルマネジメント）事業
- ▶ LCM事業で、回収し、データ消去したIT機器を中古販売業者への販売
- ▶ 観光地のガイドで使われるイヤホンガイドの製造、レンタル、販売、保守サービス。完全子会社の株式会社ケンネットが国内シェア90%を占める

3040 ソリトンシステムズ

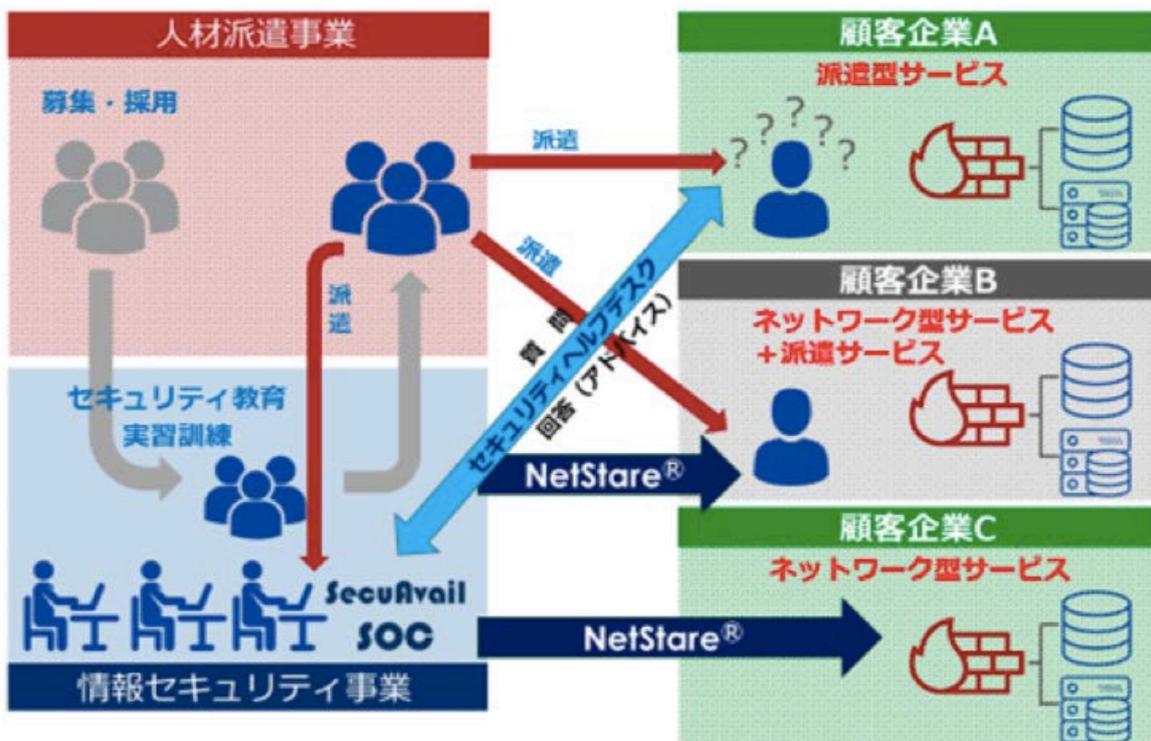
<https://www.soliton.co.jp>

- ▶情報漏洩対策、ログオン認証、アクセス制御、スパムメール対策、サイバーセキュリティ対策などの製品の開発、販売
- ▶スマートデバイスの業務利用のためのセキュリティ対策の構築、販売
- ▶企業向けクラウドサービス・企業向けネットワークインテグレーション・VoD(ビデオ・オン・デマンド)システムの構築・運用
- ▶中国、シンガポール、アメリカ、デンマーク、オランダに子会社を持ち、セキュリティ製品を海外へ販売している
- ▶前期売上164億円のうち、ITセキュリティセクターの売上は155億円
- ▶東証一部。時価総額181億円(2018/11/22時点)
- ▶代表取締役 鎌田 信夫氏およびその資産管理会社である有限会社Zen-Noboksの保有株式を合わせると44.55%の筆頭株主となる

3042 セキュアヴェイル

<http://www.secuavail.com>

▶当連結会計年度に情報セキュリティ技術者の派遣に特化した人材派遣会社「株式会社キャリアヴェイル」を設立し、情報セキュリティ技術者を派遣するだけでなく、情報セキュリティ事業の既存顧客への従来のネットワーク型サービスに情報セキュリティ技術者派遣サービスを合わせたハイブリッド型のビジネスモデルをご提案できるようになりました。



- ①セキュリティ(ソフト)マネジメントに属するコンポーネント
 - i.緊急セキュリティ対応

お客様のセキュリティ機器やアプリケーション等に対する、外部からの不正アクセスなどの攻撃の有無を24時間365日体制で監視し、万が一不正アクセスを検知した場合には、2時間以内に緊急の対応を行います。

ii.最新セキュリティ技術対応

外部からの不正侵入を防御するため、常に最新のセキュリティ事情に対応し続け、脅威を及ぼす可能性がある発信元からの侵入を直前でブロックするなど、定期的な情報の更新等による強固でハイレベルなセキュリティオペレーションを行っています。

iii.ログ管理/分析

自社開発のソフトウェア「LogStare®(ログステア)」を用いて、ネットワークデバイスから出力される日常のセキュリティログを様々な角度から分析し、問題の発生リスクを早期に発見して、トラブルが発生しにくい環境やネットワーク機器構成の実現に努めています。

iv.問い合わせ対応

内外の専門教育を実施し、高度な知識を備えたエンジニアにより、24時間365日体制でセキュリティ機器やシステム、ソフトウェアに対する様々な問い合わせに迅速に対応しています。

②システム機器(ハード)マネジメントに属するコンポーネント

i.障害復旧支援

ネットワーク機器に物理的な障害が発生した場合には、お客様に負荷をおかけすることなく、代替機の手配から当初のネットワーク・セキュリティ環境を再構築するなど、論理復旧まで一貫して対応します。

ii.システム運用

性能監視及び稼働監視によって把握したシステム上の問題点を改善し、常に最適なパフォーマンスを維持するための提案を行い、設定変更やルール変更などの具体的な対策を実施しています。

iii.セキュリティ機器監視

お客様のネットワークシステムに当社独自の運用監視システムを用いてアクセスし、24時間365日体制で、お客様のセキュリティ機器やアプリケーション等に対する外部からの不正アクセスなどの攻撃の有無を監視しております。

iv.保護対象機器監視

ネットワーク機器やシステムの稼働状況を24時間365日監視して性能状態、パフォーマンス状態を把握し、正常に応答があるか、ダウンしているかなどの把握を行います。さらに、システム上で問題が発生する前にその問題点を検知し、適切な対策を立案しております。

③情報セキュリティ技術者の派遣事業

当連結会計年度に、情報セキュリティ技術者派遣に特化した人材派遣事業会社「株式会社キャリアヴェイル」を設立したことにより、セキュリティシステムの導入支援、運用サービスを行いながら、お客様ごとの環境や事情に応じた施策をご支援する為に情報セキュリティ技術者を派遣することが可能になりました。

④運営体制の充実

当社グループのサポート体制は、24時間365日での稼働監視を実現しています。また、コンピュータシステム専用として建築された、自家発電装備、耐震性、漏水防止性、防火性等に優れたビルに、データセンター機能を有するセキュア・デリゲーション・センター(SDC)を設置し、万が一の場合にもお客様にご迷惑をお掛けしないサポート体制の確立に万全を期しております。

▶JASDAQグローバル上場。時価総額33億円(2018/11/22時点)

3054 ハイパー

<https://www.hyperpc.co.jp>

▶サーバー、コンピュータ、プリンタ、トナー、周辺機器の販売

▶ネットワークインフラ、電話配線、オフィスレイアウト、エルプデスク運営、デジタルコンテンツの制作

▶アスクルの代理店業務

▶中小企業様向けセキュリティシステム等の製造・企画・販売、ITコンサルティング、セキュリティ対策

▶情報通信機器販売事業とアスクルエージェント事業の収益が90%以上を占めており、サイバーセキュリティ企業の要素は小さい

▶JASDAQスタンダード上場。時価総額46億円(2018/11/22時点)

3356 テリロジー

<http://www.terilogy.com/index.html>

▶ルータ、無線LANなどの情報通信機器の販売、ネットワークインフラの設計、構築

▶モニタリング業務：トラフィックデータの収集、解析、可視化

▶アプリケーションの性能を監視するクラウドサービス

▶2016年10月21日 カナダWedge Networks社と国内販売代理店契約を締結! ~サービス事業者向けクラウドUTMプラットフォームと法人向けAI搭載の 独自特許技術による統合セキュリティアライアンスを販売開始~

http://www.terilogy.com/ir/pdf/WedgeNetworks_terilogypressnews2016.pdf

▶2016年10月21日 米国Tempered Networks社と国内独占販売契約を締結。既存ネットワークから隔離・隠蔽するステルスネットワークを実現する製品の販売開始

~ネットワークセキュリティプロトコル(HIP)を採用し、簡単な設定操作で安全なプライベートオーバレイネットワークを実現~

http://www.terilogy.com/ir/pdf/TemperedNetworks_terilogypressnews2016.pdf

▶**Tempered Networks社**

<https://www.temperednetworks.com>

▶2016年11月16日 イスラエルKELA社と販売代理店契約を締結。ダークネットでやり取りされる脅威情報を検知するスレットインテリジェンスサービスを提供

<http://www.terilogy.com/product/kela/index.html>

▶2016年11月16日 「イスラエルの最新鋭諜報テクノロジーが、訓練不足の日本のセキュリティ”頭脳”を補完する」インタビュー記事掲載

http://www.terilogy.com/product/kela/pdf/kela_interview01.pdf

▶2018年10月12日 テリロジーワークス、日本サイバーディフェンス社と サイバーセキュリティ教育事業に関するアライアンス契約を締結 ~最先端のサイバーセキュリティに関する教育プログラムの提供

http://www.terilogy.com/product/cyberthreatintelligence/pdf/terilogy_pressnews2018_1012.pdf

▶JASDAQスタンダード。時価総額228億円(2018/11/22時点)

事業部門	主要製品分野
ICT部門	<ul style="list-style-type: none"> ・ネットワーク機器（スイッチ、ルータ、無線LAN、DNS/DHCP等） ・次世代ストレージ製品 ・テレビ会議システム製品
セキュリティ部門	<ul style="list-style-type: none"> ・ネットワークセキュリティ製品（ファイアウォール、侵入検知・防御、情報漏えい対策等） ・セキュリティ認証基盤 ・ワンタイムパスワード製品 ・フォレンジック（自社開発製品（nonentun）と他社製品との連携によるログ収集・分析・可視化）
モニタリング部門	<ul style="list-style-type: none"> ・自社開発製品（nonentun） ・ネットワーク運用・管理・監視機器
グローバル部門	<ul style="list-style-type: none"> ・パートナーを經由して自社開発製品（nonentun）を市場に提供
サービス部門	<ul style="list-style-type: none"> ・プロダクト保守 ・クラウド性能監視サービス（CloudImage）
ソリューションサービス部門	<ul style="list-style-type: none"> ・リアルタイム映像通訳サービス（みえる通訳） ・クラウド管理型マネージドVPNサービス（MRA VPN Zero-Con） ・ウェブ会議サービス（MRA Video Conference） ・法人向けインターネット接続サービス（MRA光） ・高速モバイルデータ通信サービス（MRAモバイル） ・レンタルサーバサービス（ITPARK）

3676 デジタルハーツHD

<https://www.digitalhearts-hd.com>

- ▶ソフトの動作テストをして不具合を検知するデバック業務
- ▶総合ゲーム情報サイト「4Gamer.net」等を運営し、広告、プロモーションを行う
<https://www.4gamer.net>
- ▶東証一部上場。時価総額367億円(2018/11/22時点)

3692 FFRI

<https://www.ffri.jp>

- ▶各種セキュリティ対策製品をサブスクリプションライセンス（期限付きの使用権）もしくはパーペチュアルライセンス（無期限の使用権）により販売している。標的型攻撃対策製品「FFRI yarai」、マルウェア（不正な動作を招くウイルスやコード）自動解析ツール「FFRI yarai analyzer」といった製品を提供している
- ▶官公庁やセキュリティ感度の高い企業に対して、サイバーセキュリティ対策の受託開発
- ▶東証マザーズ上場。時価総額298億円(2018/11/22時点)

3762 テクマトリックス

<https://www.techmatrix.co.jp/index.html>

- ▶ネットワークやサーバーの運用・監視及びネットワークエンジニアの派遣、セキュリティ製品やストレージ製品の販売
- ▶システム開発、アプリケーション・パッケージ、テスト・ソリューションに加えて、クラウドサービス(SaaS)等様々なアプリケーション・サービスを提供

▶積極的に新しいビジネスの立ち上げを行い、IT需要の変化を先取りする取り組みを行いました。◇情報基盤事業

第1四半期連結会計期間

- ・メール添付ファイル自動無害化ソリューション「Votiro Auto Mail Link with matriXgate」の販売を開始
- ・クロス・ヘッド株式会社が、米国Palo Alto Networks, Inc.のAmazon Web Services(AWS)上で動作する仮想化バージョン「VM-Series」の販売及び構築サービスの提供を開始
- ・クロス・ヘッド株式会社が、フィンランドのF-Secure Corporationのセキュリティの脆弱性診断ソフトウェア「RADAR」を利用した「クロス・ヘッド脆弱性診断サービス」の提供を開始
- ・沖縄クロス・ヘッド株式会社が、JBサービス株式会社と協業し、データセンター機器の状態を遠隔監視する「OCH POWER」の提供を開始

第2四半期連結会計期間

- ・クロス・ヘッド株式会社が、学校法人高宮学園代々木ゼミナールが運営する代ゼミライセンススクールにて「ITパスポート試験対策講座」の提供を開始
- ・沖縄クロス・ヘッド株式会社が、日本インターネットエクスチェンジ株式会社と連携し、沖縄県内においてIXポートサービスを提供するJPIX沖縄を開始
- ・米国Menlo Security社のWeb分離・無害化プラットフォーム製品「Menlo Security Isolation Platform」のオンプレミス版の提供を開始
- ・セキュリティ運用監視サービス「.: TRINITY <トリニティ>」において、米国Palo Alto Networks, Inc.がAmazon Web Services(AWS)環境向けに提供している仮想化次世代ファイアウォール「VM-Series on AWS」のセキュリティ運用監視サービスを開始
- ・米国Palo Alto Networks, Inc.が提供する次世代ファイアウォールと、当社のクラウドサービス「テクマクラウド」を連携させた新サービスとして、マイクロソフト社のメール等のクラウド版グループウェアサービスOffice 365 通信の自動制御サービスの提供を開始

第3四半期連結会計期間

- ・クロス・ヘッド株式会社が、内部不正による情報漏洩の抑止に有効なセキュリティソリューション「Ekran System」の提供を開始
- ・クロス・ヘッド株式会社が、株式会社イーセクターと連携し、ソフトウェアロボットによる業務代行ソリューション「ROBOWARE」の取扱いを開始
- ・沖縄クロス・ヘッド株式会社が、自社の「nas2cloud Plus(ナスツークラウドプラス)」と、日本ヒューレット・パッカー株式会社が提供する「HPE ProLiant」を組み合わせた中堅・中小企業向けのバックアップソリューションの提供を開始
- ・沖縄クロス・ヘッド株式会社が、株式会社アシストと協業し、情報漏洩対策サービス「ダブルブラウザ・ソリューション」の提供を開始
- ・沖縄クロス・ヘッド株式会社が、横河レンタ・リース株式会社と共同で、働き方改革ソリューションサービスの提供を開始
- ・セキュリティ運用監視サービス「.: TRINITY <トリニティ>」において、マカフィー株式会社が提供するセキュリティ脅威の可視化を行う統合ログ管理ソリューション「McAfee Security Information and Event Management」の導入から運用までをワンストップで実現する「TRINITY セキュリティ監視サービス for McAfee SIEM」の提供を開始



- ・無害化システムが標準搭載された、教育委員会向けファイル受け渡しシステム「Votiro Auto SFT Plus」の提供を開始
- ・セキュリティ運用監視サービス「.:TRINITY <トリニティ>」において、米国Palo Alto Networks, Inc.が提供する次世代エンドポイント※9セキュリティ「Traps」を対象としたセキュリティ運用監視サービス「TRINITY セキュリティ運用監視サービス for Traps」の提供を開始
- ・デジタルアーツ株式会社が提供するメールセキュリティ製品「m-FILTER」と当社の無害化ソリューションを組み合わせた「Votiro AutoSFT Plus for m-FILTER」の提供を開始

当第4四半期連結会計期間

- ・沖縄クロス・ヘッド株式会社が、日本オラクル株式会社が販売するオラクルデータベース専用のディザスタリカバリー(災害復旧)サービス「OCH POWER BCP パッケージ」の提供を開始
- ・クロス・ヘッド株式会社が、Amazon Web Services(AWS)が提供するクラウド型コンタクトセンターサービス「Amazon Connect」を活用した、コンタクトセンターサービス「Managed Connect Service」の販売を開始

- ▶ 5期連続売上成長、4期連続純利益成長している
- ▶ 株価は6年で10倍成長
- ▶ 東証一部上場。時価総額385億円(2018/11/22時点)

3776 ブロードバンドタワー

<https://www.bbtower.co.jp>

(1) コンピュータプラットフォーム事業 当社を中心とするコンピュータプラットフォーム事業では、「データセンター」、「クラウド・ソリューション」、「データ・ソリューション」、「その他」にサービス区分し、それぞれ展開しております。各サービスの内容は次のとおりであります。

1 データセンター(データセンター、ネットワークプロバイダー)

データセンター用不動産(データセンタービル)を賃借し、同不動産内にデータセンター設備(通常運用時の電力供給設備、非常時バックアップ用バッテリー設備(無停電電源装置)、非常用電源設備(小型のディーゼル発電機、またはガスタービン発電装置))、情報通信機器(ルータ・スイッチ類、LAN、情報通信セキュリティ機器)等を設置して、インターネット情報提供サービスを提供する事業者の保有するコンピュータ機器(サーバ)をラック内に収容すると共に、当社の情報通信機器を通じて通信事業者(キャリア等)の通信回線と接続し、以下の設備等を提供しております。

- ・スペースの提供
- ・通信回線
- ・電力
- ・コンピュータ機器運用受託
- ・同上各サービスの周辺設備

2 クラウド・ソリューション

当社内データセンターにある当社の保有するコンピュータ資源を顧客に貸し出しております。また、当社と販売提携している他社製クラウドサービスの再販、クラウド利用に関するサービスを提供しております。

3 データ・ソリューション

当社が代理店権を有するストレージ装置の販売、大容量ストレージに蓄積されたデータを分析・加工するシステム構築、データ分析、加工するサービスを提供しております。

4 その他

クラウドを中心とした技術を強化するため、当社内に設置したCloud&SDN研究所を中心に、SDN、NFV、OpenStackを活用した技術の研究開発を行っております。(SDN:Software Defined Networking、NFV:Network Functions Virtualization、OpenStack:オープンソースで開発されているクラウド環境構築用のソフトウェア群)

(2) IoT/AIソリューション事業

株式会社エーアイスクエア(以下、AI2)、株式会社IoTスクエア(以下、IoTスクエア)、グローバルIoTテクノロジーベンチャーズ株式会社(以下、GiTV)、GiTV Fund Investment,L.P.、BBTOWER SANDIEGO INC.(以下、BBT SD)を中心に事業を行っております。

株式会社IoTスクエアでは、IoT事業及び新規事業を行っており、AI2は、自然言語解析技術を活用したAIソリューションをコンタクトセンターやヘルプデスク向け等に提供しております。

GiTVは業務執行組合員として、国内外のIoT先端技術ベンチャー企業へ出資するため、グローバルIoTテック1号投資事業組合を組成しベンチャー企業へ投資を実行してはりましたが、本年1月に新たにケイマン籍のファンドであるGiTV Fund I Investment,L.P.を組成し、これに伴い、グローバルIoTテック1号投資事業組合については清算を行いました。

(3) メディアソリューション事業

IoTスクエアは、コンシューマー向け動画配信サービス、ネットシネマ等も展開しております。また、ジャパンケーブルキャスト株式会社は、主に日本全国のケーブルテレビ事業者及び番組供給事業者向けの通信ネットワーク事業を行っております。

なお、当社が行っていたコンシューマー向け動画配信サービス、ネットシネマ等は、新設分割により昨年10月2日付けでIoTスクエアに移管しております。

▶東証JASDAQスタンダード上場。時価総額164億円(2018/11/22時点)

3788 GMOクラウド

<https://ir.gmocloud.com>

- ▶共同ホスティング業務（サーバーを複数のユーザーで共有することで、複数ユーザーが遠隔地での操作が可能）
- ▶専用ホスティング業務（会社専用のサーバーをカスタムする）
- ▶仮想専用サーバーVPS（仮想サーバーに複数のユーザーがログインでき、それぞれに専用のOSがあるため、ユーザーごとに自由にソフトを利用できる）
- ▶SSLサーバ証明書発行（①サイトの実在性証明：サイトの運営組織が実在し、ドメイン名の使用権があることを、サイバートラストが信頼される第三者機関として証明します。②WebブラウザとWebサーバ間で暗号化通信を行い、個人情報、クレジットカード番号などが第三者に盗み見られないようにします。）
- ▶シンガポール、イギリス、アメリカ、フィリピン、ベルギー、ロシア、中国、インドに子会社
- ▶親会社はGMOインターネット持ち株比率51.8%
- ▶東証一部上場。時価総額415億円(2018/11/22時点)

3837 アドソル日進

▶IoTシステム事業においては、デバイス制御(センシング、OSを含む)からネットワーク、大規模インフラ、クラウドシステム迄をカバーする総合エンジニアリング企業として、その全域をワンストップにて提供しています。更に、PMP(Project Management Professional)人材を活用したプロジェクト管理に強みを持ち、国内地方や中国・ベトナム企業との分散開発体制と、これを支える当社独自ソリューションの開発、拡充、及び提供に注力しています。

一方、他社との差別化を明確化するソリューション開発にも注力しており、「セキュリティ」、「GIS (Geographic Information System:地理情報システム)」、「センサ・ネットワーク」、「ID認証セキュリティ」等、新たな価値の創造に継続的に取り組むことに加え、将来当社の事業活動において必要になると予想される先端技術や、生産性向上としてソフトウェア開発における生産技術の革新(賢く価値を生み出す開発モデルの実現)の為に研究・開発を推進しています。

- ▶5期連続で純利益成長
- ▶6年で株価14倍
- ▶東証一部上場。時価総額181億円(2018/12/14時点)



3857 ラック

<https://www.lac.co.jp>

(1)セキュリティソリューションサービス事業(SSS事業)

・セキュリティコンサルティングサービス

情報セキュリティ対策の計画立案からリスクアセスメント、情報セキュリティポリシーの策定・導入・運用管理、情報セキュリティ監査までの一貫したサービスを提供しております。また、セキュリティに関わる緊急事態に対して支援する緊急対応サービスや復旧・恒久対策支援、不正な外部への情報流出やパソコンのウィルス感染などによる情報漏えいなどを調査・分析し、組織内からの情報流出・情報漏えいの可能性を評価するサービスの提供のほか、グローバルな情報セキュリティ教育を標準とし、実践的情報セキュリティ教育の支援を行っております。

・セキュリティ診断サービス

Webアプリケーションや稼働中のサーバ、ネットワーク機器、データベースなどの脆弱性を診断するサービスを提供しております。診断の結果、検出された脆弱性や想定されるリスクレベル、求められる対策などについて詳細に報告することで、お客様のシステムを安全に保つための支援を行っております。

・セキュリティ運用監視サービス

セキュリティ監視センター「ジャパン セキュリティ オペレーション センター(JSOC)」にて、お客様のネットワークを24時間365日リアルタイムに監視するサービスを提供しております。また、各種セキュリティ製品の導入 サービス、セキュリティを考慮したサーバの設定やアップデートを行うなど、堅牢なセキュアサーバを構築するサービスを提供しております。

・セキュリティ製品販売

セキュリティソリューションサービスに付随するセキュリティ関連製品の販売を行っております。

・セキュリティ保守サービス

販売したセキュリティ関連製品の保守サービスを提供しております。

(2)システムインテグレーションサービス事業(SIS事業)

・開発サービス

大型汎用コンピュータの基本となる基盤系システムや顧客の個別ニーズに応じた業務系アプリケーションシステムの設計・開発からシステム稼働後の保守サービスまでを行っております。汎用コンピュータ分野での基盤系システムの設計・開発は、汎用コンピュータおよびオペレーティング・システム(OS)の知識と開発、運用、保守の経験が必要とされる分野で、大手都市銀行をはじめとする金融機関や官公庁など、高い信頼性が求められるシステムの開発を行っております。

・HW/SW販売

IT活用を支えるシステム基盤となるサーバ、ストレージおよび付随製品など、お客様の多様なニーズにお応えできる幅広い情報システム製品(ハードウェアおよびソフトウェア)の販売を行っております。

・IT保守サービス

販売した製品(ハードウェアおよびソフトウェア)の保守サービスを提供するとともに、IT設備工事を含むネットワーク基盤の設計・構築から、機器の導入展開、運用監視にいたる幅広いサービスを提供しております。

・ソリューションサービス

インターネット/イントラネット環境における豊富な経験と最新のIT技術を活かした各種ソリューションサービスを提供しております。また、データセンターにおいてクラウドサービスをはじめとする各種アウトソーシングサービスを提供しております。

▶2017年10月24日 サイバートラスト株式会社への資本参加

<http://v4.eir-parts.net/v4Contents/View.aspx?cat=tdnet&sid=1521390>

▶2018年1月15日 デジタルソリューションへの資本参加

<http://v4.eir-parts.net/v4Contents/View.aspx?cat=tdnet&sid=1544627>

▶2018年2月5日 KDDI株式会社との合併会社を設立に関する基本合意

<http://v4.eir-parts.net/v4Contents/View.aspx?cat=tdnet&sid=1551280>

▶2018年11月7日 第2四半期報告書

http://v4.eir-parts.net/v4Contents/View.aspx?cat=yuho_pdf&sid=2765027

①セキュリティソリューションサービス事業(SSS事業)

セキュリティコンサルティングサービスは、顧客常駐型サービスは横ばいであったものの、緊急対応サービスが堅調に推移し、売上高は13億16百万円(前年同期比6.6%増)となりました。セキュリティ診断サービスは、主力のWebアプリケーション診断とともに、スマートフォンアプリケーション診断が好調に推移し、売上高は9億23百万円(同38.3%増)となりました。

セキュリティ運用監視サービスは、前年同四半期にはなかった株式会社アジアリンクの組み入れおよび中部地域大手製造業向け運用監視サービスの売上計上、ならびに既存案件の契約更新が堅調に推移したことにより、売上高は25億85百万円(同50.9%増)となりました。

セキュリティ製品販売は、クラウドに対応した高度な機能を備えた製品等の販売が好調に推移し、売上高は13億64百万円(同16.3%増)となりました。

セキュリティ保守サービスは、堅調な既存案件の更新需要はあるものの、売上高は6億16百万円(同0.6%減)となりました。

この結果、SSS事業の売上高は68億7百万円(同25.8%増)、セグメント利益は8億92百万円(同76.2%増)となりました。

②システムインテグレーションサービス事業(SIS事業)

主力ビジネスである開発サービスは、中核となっていた大手銀行業向けは大幅減となったものの、旅行業や人材派遣業など銀行業以外の案件が好調に推移したことにより、売上高は70億21百万円(前年同期比0.2%増)となりました。HW/SW販売は、クラウドサービス活用などによる需要縮小に加え、前年同期には大型案件があり伸長したものの当四半期は同様の案件がなかったことにより、売上高は9億45百万円(同60.3%減)となりました。IT保守サービスは、前期のHW/SW販売が低調であったことにより、売上高は23億2百万円(同4.3%減)となりました。ソリューションサービスは、子会社の株式会社ジャパン・カレントが提供するデジタルマーケティングサービスの売上増はあったものの、アプリケーションパフォーマンス管理ソリューションの売上減により、売上高は6億79百万円(同4.5%減)となりました。

この結果、SIS事業の売上高は109億49百万円(同12.5%減)、セグメント利益はのれん償却額等の販管費減などもあり12億13百万円(同11.0%増)となりました。

売上高は前期と比較してほぼ横ばいだが、売上の構成がセキュリティコンサルティング、診断、運用監視サービスに大きく変化している。



▶ 株価は8年で10倍

▶ 東証JASDAQスタンダード上場。時価総額417億円(2018/11/22時点)

3858 ユビキタスAIコーポレーション

<https://www.ubiquitous-ai.com/news/2017/002781.html>

▶ 安心、安全なIoT環境の実現に必須である組み込みネットワーク及びセキュリティ技術、様々な機器の中でのデータの増大という課題に対処するためデータ管理の効率化に寄与する軽量で高速なデータベース製品、LinuxやAndroidの採用でますます複雑化する機器を「いつでも」使えるようにOSの高速起動を実現する高速起動製品を提供しております。

▶ さらに、IoT時代に向けて、クラウドサービスで様々なデバイスを接続するIoTクラウドプラットフォーム等を展開しております。

▶ また、当社グループである、エンジニアリングサービスの提供を行う株式会社エム、海外の組み込みソフトウェアの専門技術商社である株式会社イーアイコーポレーションと連携し、幅広い市場への多種の商材、サービスを提供しております。

▶ 通信機器、ワイヤレス通信機器、スマートハウス用通信機器

▶ 2017年10月24日 サイバートラストとユビキタス、IoT機器向けの脆弱性診断サービスにおける協業を開始 ～IoT機器自体のサイバーセキュリティ確保を推進～

<https://www.ubiquitous-ai.com/news/2017/002808.html>

▶ サイバートラスト株式会社

<https://www.cybertrust.ne.jp>

※サイバートラスト株式会社(非上場会社)はソフトバンク・テクノロジー株式会社が74.5%保有する子会社であり、ソフトバンク・テクノロジー株式会社はソフトバンク・インターナショナル合同会社が54.26%保有する子会社である。

▶2018年10月24日 ユビキタスAIコーポレーションと米国Beyond Security社、IoT機器の脆弱性・セキュリティ検証のための新ツールの共同開発に合意 ～擬似的にIoT機器、車載機器へのサイバー攻撃シナリオを作成、機器メーカーが自社で対象機器の防御力を確認可能に～

<https://www.ubiquitous-ai.com/news/2018/002910.html>

▶Beyond Security社

<https://www.beyondsecurity.com>

http://www.beyondsecurity.jp/beyond_experience.html (日本語)

▶東証JASDAQスタンダード上場。時価総額75億円(2018/11/22時点)

3927 フーバーブレイン

<https://www.fuva-brain.co.jp>

▶情報セキュリティソリューション事業

▶データ回復/暗号化技術

▶マルウェア対策

▶PC業務ログ監視

▶セキュリティソフトの製作、販売、OEM製品

▶2期連続で売上が減少し、経常赤字だったが、今期より黒字転換

▶2018年8月14日 代表取締役と常務取締役が辞任し、興水 英行氏が代表取締役社長に就任

<https://ssl4.eir-parts.net/doc/3927/tdnet/1624045/00.pdf>

▶興水 英行氏はフォンティス興水会計事務所の代表で、事業再生で15年の経験あり

<http://fontis-limited.com/partner/>

▶東証マザーズ上場。時価総額86億円(2018/11/22時点)

3967 エルテス

<https://eltes.co.jp>

▶SNSや掲示板をAIと専任アナリストで観測、分析、報告

▶内部者による不正会計、情報漏洩をデータに現れる人の動きで分析、検知する

▶サイバーセキュリティではないが、分析、検知の考え方、事業方針が似ている

▶累計650社を超える導入実績を持つ。創業来の「コンサルティングサービス」は、ソーシャルリスクに関する危機発生後に、速やかに顧客が適切な対応を取れるようにアドバイスを行うサービスであり、リスクが顕在化している企業や組織に対しては、リスクの鎮静化に向けた緊急対応コンサルティングと事後のレピュテーション回復(及びブランド再構築)に向けたサービスを提供している。一方、「モニタリングサービス」は、ソーシャルリスクの発生を早期に検知及び把握するもので、24時間365日、Twitter等のSNSやネット掲示板といったソーシャルメディア上の投稿を分析し、リスクの予兆があれば緊急通知の実施や対応方法のアドバイスを行い、危険投稿がなければ日報で報告するサービスである(月報でのトレンド報告を含む)。同社では、創業来の主力である「コンサルティングサービス」から、リスク予防型で契約継続率の高い「モニタリングサービス」へのシフトを進めている。

▶主力の「ソーシャルリスク関連サービス(ソーシャルリスクモニタリングサービス)」の月額課金は40万円程度、「内部脅威検知サービス」は50万円程度とみられる。なお、顧客数の拡大のためには、新規顧客の獲得と継続率の維持・向上が重要である。継続率は80%から90%の高い水準を確保しているもようである。

<http://contents.xj-storage.jp/xcontents/AS80619/51b1884f/2cda/435d/b737/fee9231c0668/20180816100450677s.pdf>

- ▶ 5期連続売上高成長。平均成長率40%
- ▶ 東証マザーズ上場。時価総額112億円(2018/11/22時点)

3968 セグエグループ

<https://segue-g.jp>

- ▶ WiFiルータ、LAN、マルウェア対策機器
- ▶ セキュリティ脆弱性診断、管理
- ▶ サイバー攻撃検知、分析
- ▶ ITシステムの構築に必要なセキュリティ製品及びITインフラ製品を、米国をはじめとする海外メーカーより代理店として輸入するほか、国内において他の代理店から調達し、主に販売パートナーを通じて国内の顧客(エンドユーザー)に販売しております。また、自社開発製品として、内部ネットワークと外部(インターネット等)ネットワークを分離し、外部からの脅威を防ぐインターネット分離ソリューション「SCVX」を販売しております。
- ▶ ソリューションプロダクト事業として単に製品の販売を行うのみでなく、エンドユーザーが求める要件に合致するITシステムを設計し、その構築を行うサービスを、主に販売パートナーを通じて
- ▶ エンドユーザーに提供しております。

常駐・遠隔によるシステムの運用や監視等のサービス、エンジニア派遣サービス等を行っております。

- ▶ 売上総利益率が20-25%と低い
- ▶ 4期連続売上、利益成長
- ▶ 東証JASDAQスタンダード上場。時価総額90億円(2018/11/22時点)

4288 アズジェント

<https://www.asgent.co.jp>

- ▶ ネットワークセキュリティ関連商品の販売、および、コンサルティング
- ▶ 2018年10月17日 アズジェントのセキュリティ3製品がSOMPOリスクマネジメントのセキュリティサービスに採用

<https://www.asgent.co.jp/press/releases/2018/20181017-001352.html>

https://sompo-rc.co.jp/news/2018/20181016_1.pdf

- ▶ 東証JASDAQスタンダード上場。時価総額67億円(2018/11/22時点)

4203 野村総研

<https://www.nri.com/jp>

(コンサルティング)

経営・事業戦略及び組織改革等の立案・実行を支援する経営コンサルティングのほか、ITマネジメント全般にわたるシステムコンサルティングを提供しています。

[主要な関係会社] ASG Group Limited

(金融ITソリューション)

主に証券業や保険業、銀行業等の金融業顧客向けに、システムコンサルティング、システム開発及び運用サービスの提供、共同利用型システム等のITソリューションの提供を行っています。

[主要な関係会社] NRIプロセスイノベーション(株)、(株)だいこう証券ビジネス、(株)DSB情報システム

(産業ITソリューション)

流通業、製造業、サービス業や公共向けに、システムコンサルティング、システム開発及び運用サービス等の提供を行っています。

[主要な関係会社]NRIシステムテクノ(株)、Brierley & Partners, Inc.、ASG Group Limited、SMS Management & Technology Limited

(IT基盤サービス)

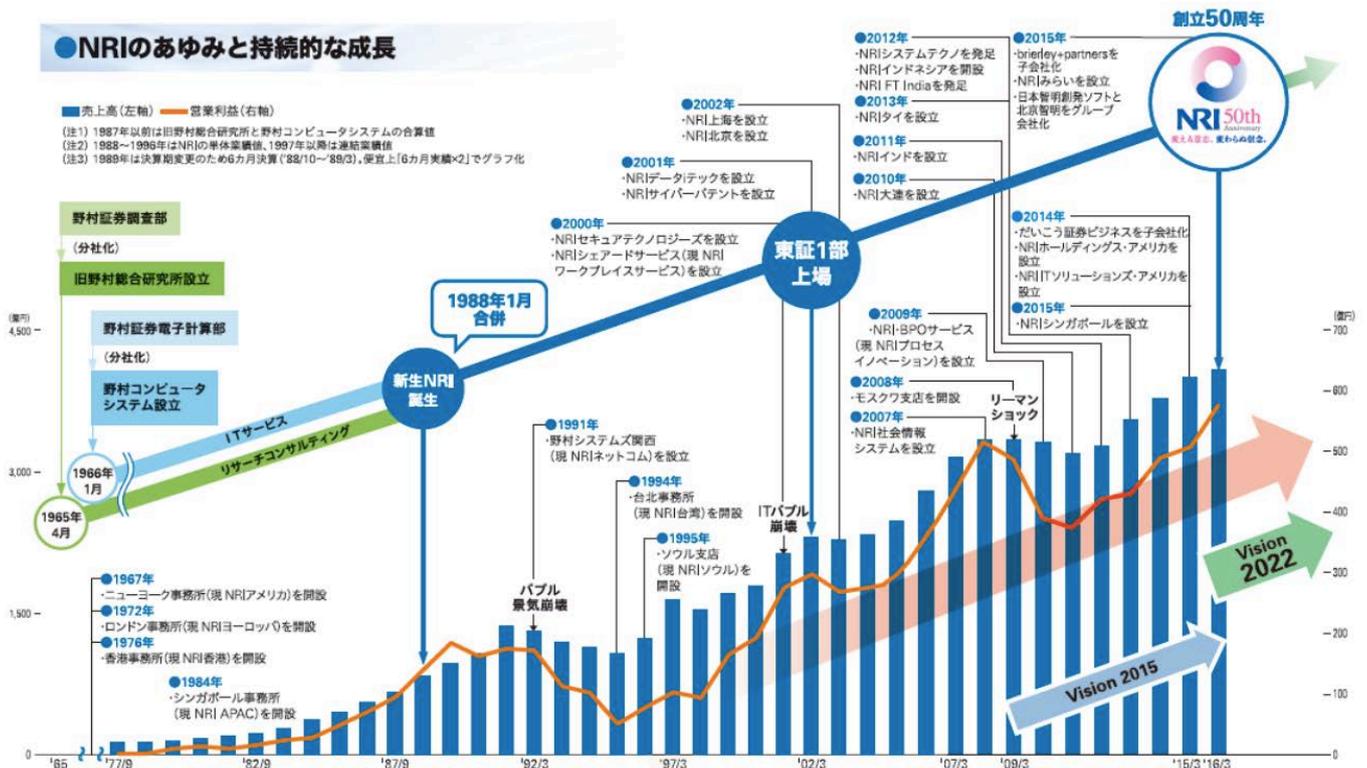
主に金融ITソリューションセグメント及び産業ITソリューションセグメントに対し、データセンターの運営管理 やIT基盤・ネットワーク構築等のサービスを提供しています。また、様々な業種の顧客に対してIT基盤ソリューションや情報セキュリティサービスを提供しています。このほか、ITソリューションに係る新事業・新商品の開発に向けた研究や先端的な情報技術等に関する研究を行っています。

[主要な関係会社] NRIセキュアテクノロジーズ(株)、NRIデータテック(株)

(その他)

上記報告セグメントに含まれない事業セグメントであり、システム開発や運用サービスの提供を行う子会社などがあります。

[主要な関係会社] NRIネットコム(株)



これらのほか、その他の関係会社として野村ホールディングス(株)があり、また、関係会社以外の主な関連当事者として野村証券(株)があります。当社グループ及び関連会社は、これらに対してシステム開発・製品販売及び運用サービス等の提供を行っています。

- ▶ 5期連続売上、利益成長。前期売上4714億円、当期純利益551億円
- ▶ 野村HDが27.6%、野村ファシリティーズが8.9%保有の大株主
- ▶ 東証一部上場。時価総額1兆2449億円(2018/11/22時点)

4344 ソースネクスト

<https://www.sourcenext.com>

- ▶ ソフトウェアの企画、開発、販売
- ▶ セキュリティ対策ソフトの販売

ZERO ウイルスセキュリティ：2003年より自社ブランドのセキュリティ対策ソフトとして展開し、2006年には、業界慣習を打破して年間更新料を廃止しました。シリーズ全体の累計ユーザー登録数は、1000万人となっております。

ZERO スーパーセキュリティ：2011年より発売しているZEROシリーズの高性能モデルです。国際的な第三者機関、AV-comparativesの「Product of the Year2017」を受賞するなど世界最高レベルの性能を誇るBitdefender社のエンジンを搭載しています。

- ▶ Androidアプリ、ハガキアプリ、PDF、語学学習
- ▶ 自動通訳機「POCKETALK(ポケットーク)」がヒット中
- ▶ 5期連続売上成長、3期連続純利益成長
- ▶ 5年で株価4.5倍に成長
- ▶ 東証一部上場。時価総額828億円(2018/11/22時点)



4386 SIG

<https://www.sig-c.co.jp>

▶官公庁、地方自治体へのシステム開発（年金、人事、給与など）

▶セキュリティサービスでは、米国SecuGen社の製品を始め、セキュリティホール探索や実際に侵入や攻撃を試みるペネトレーションテスト等に用いる脆弱性対策ツール等、セキュリティ商材の販売と、その設計・構築・保守・運用までの一元的なサービスを提供しています

▶米国SecuGen社

<https://secugen.com>

▶2018年6月に上場したばかり

▶東証JASDAQスタンダード上場。時価総額47億円(2018/11/22時点)

4398 ブロードバンドセキュリティ

(1) セキュリティ監査

① セキュリティ監査

当社はクレジットカード業界におけるグローバルセキュリティ基準であるPCI DSS(※2)の監査資格(QSA：Qualifid Security Assessor)を法人として保有しており、クレジットカードデータを取り扱っている企業に対して、セキュリティ監査を実施しています。

また、企業がPCI DSS準拠監査を通過するために、実際の姿とあるべき姿にしがいがあがる場合には、それが何であり（GAP分析）、どう対処するべきかといったコンサルティングサービスを提供しています。

② コンサルティングサービス

現状の情報セキュリティの分析から対策すべきポイントの抽出、社内体制や情報システムの改善施策とその実現まで、お客様のなすべき目標を明確にかかげ、企業の情報セキュリティ強化に向けた体制作りを、社内ルール及び情報システム両方の視点から支援するコンサルティングサービスを提供しています。

(2) 脆弱性診断サービス

企業のWebサイトに対し、当社のエンジニアが、外部からの侵入や、内容の書き換えが可能かどうか、疑似攻撃をかけることで、Webサイトの安全性を診断するサービスを提供しています。

(3) 情報漏洩IT対策サービス

当社のサーバ群や独自に開発したソフトウェアなどを使用し、企業の情報漏洩対策（予防、監視、発見、遮断等）のためのサービスを提供しています。具体的には以下の8つのサービスとなります。

① セキュリティ機器マネージドサービス

24時間365日体制でお客様の代わりに様々なセキュリティ機器を運用・監視するサービスであり、それらを総称して「マネージドサービス」と呼んでいます。その中心になるのがSOC（Security Operation Center）であり、SOCは地震やその他災害が発生した場合においても業務を継続できるインターネットデータセンターの中に設置されています。

② セキュリティメールサービス

企業が安全かつ安心してメールをご利用いただけるように設計された様々な機能を搭載した

クラウド型のサービスです。例えば、添付使用の自動暗号化、不正なメールを防止するフィルターの設置、悪性添付ファイルの自動停止など、企業ユースに特化したサービスを提供しております。クラウド型のため、利用者は大きな初期投資なくメールシステムを利用することができます。

③マルウェア検知サービス

クラウド型のウィルス検知サービスです。マルウェアと呼ばれる悪性ウィルスのうち、未知のウィルスに対しては一般的なアンチウィルスソフトでは予防することができません。そのため当社では、未知のウィルスへの感染の可能性のあるファイルを一度仮装領域に展開し、コード自体を読み込んでウィルスに感染しているかどうかを判定するクラウド型のウィルス対策検知サービスを提供しています。このタイプの対策は、判定の専門性などの面で一般事業会社での内製化は困難であり、専門家でないと判断できない場合が多々あります。ここにクラウド型のサービス提供のメリットがあり、当社のサービスは分析・報告まではセットになっている点が大きな特徴です。

④標的型メール攻撃サービス（開封率調査）

顧客企業が「標的型メール攻撃(※3)」にどの程度耐性を持つのかを調査するサービスであります。具体的には当社が攻撃者になりすまし、悪性ウィルスを添付した偽のメールを送り、その会社で何人(何%)の社員が開封してしまうかを調べるサービスです。

⑤ウィルス感染チェックサービス

マルウェア感染の有無を確認するサービスです。過去のプロキシサーバ(※4)のログ(通信結果が保存されたデータ)を解析することによりチェックする方法、ハッシュ(※5)解析と呼ばれる方法、上記で述べたマルウェア検知サービスを一定期間だけ提供することで外部通信を調査し、感染をチェックする方法等、顧客の状況に合わせてチェックするサービスを提供しています。

⑥SIEM(※6)構築及び運用サービス

ウィルスに感染した際、外部に送信される前にその動きを検知して漏えいを防ぐためのサービスである。これはファイヤウォール(※7)やIPS(※8)などのネットワーク機器や、ソフトウェアやアプリケーションが出力するイベントログを一元的に保管して管理し、相関分析することにより、リアルタイムで不審なトラフィックを検知、感染端末を特定し、漏洩する前に遮断するというセキュリティポリシー管理とコンプライアンス支援を行うサービスです。

⑦フォレンジック(※9)サービス（緊急駆けつけサービス）

万が一企業が情報漏洩を起こしてしまった場合に、速やかにネットワークから当該端末やサーバを切り離して、それ以上情報が漏洩しないようにし、感染経路の特定(原因調査)および漏洩した情報の特定、影響範囲の特定等、企業が行うべき様々な漏洩対応に関するサポートを行うサービスです。

⑧インターネット分離クラウドサービス

マルウェア対策の一環として、業務用システムとインターネットを利用するWeb閲覧やメール送受信を異なる環境に置き、業務用システムを悪意あるプログラムから守る「インターネット分離」をクラウド型で提供するサービスです。

※1 マルウェア：不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称。悪意のあるソフトウェアをマルウェア(malware=malicious「悪意がある」とsoftware「ソフトウェア」を組み合わせた造語)と呼び、ウィルスもマルウェアに含まれる。

※2 PCI DSS：Payment Card Industry Data Security Standardの略で、国際カードブランド

5社（American Express、Discover、JCB、Master Card、VISA）が共同で設立したPCI SSC（PCI Security Standard Council）により、運用・管理されているカード情報セキュリティの国際統一基準の名称。

Payment Card Industry Data Security Standard Council

<https://ja.pcisecuritystandards.org/minisite/env2/>

※3 標的型メール攻撃：特定のターゲットに絞ってメールなどでサイバー攻撃を仕掛ける「標的型攻撃」。その多くがメールを利用して行われるため「標的型メール攻撃」と呼ばれる。

※4 プロキシサーバ：内部のネットワークとインターネットの境界で動作し、両者間のアクセスを代理して行うこと。プロキシは「代理」という意味。ネットワーク内におけるインターネットの出入り口をプロキシサーバ経由に限定することで、通信内容を一括してプロキシサーバ側でチェックすることが可能。クライアントコンピュータは直接インターネットにつながるのではなく、不正アクセスや侵入防止を防ぐことができ、セキュリティ向上目的で用いられる。

※5 ハッシュ：メッセージを特定するための暗号化技術。

※6 SIEM：Security Information and Event Managementの略で、ファイアウォールやIPSなどのセキュリティ機器、ソフトウェアやアプリケーションが出力するイベント情報を一元的に保管して管理し、脅威となる事象を把握するテクノロジー。

※7 ファイアウォール：社内ネットワークとインターネットの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システムなどのこと。

※8 IPS：Intrusion Prevention Systemの略で、サーバやネットワークの外部との通信を監視し、侵入の試みなど不正なアクセスを検知して攻撃して未然に防ぐシステムのこと。

※9 フォレンジック：情報漏洩や不正アクセスなど、コンピュータが関わる犯罪が起きた際に、コンピュータ本体に記録された電子データを収集・分析して、証拠とするための技術のこと。

▶2018年9月に上場したばかり

▶SBIホールディングスのグループ会社であり、SBIホールディングスが78.28%を保有している。

▶5期連続売上成長し、2期前から黒字転換

▶東証JASDAQスタンダード上場。時価総額108億円(2018/11/22時点)

4662 フォーカスシステムズ

▶官公庁及び関係機関・地方自治体及び関連機関等の公共機関並びに銀行・保険等の金融機関向けのソフトウェアの開発、ハードウェア、ネットワークを含む情報システム全体の構築、情報化に関わるコンサルティング

▶防衛省関連システムの共通運用基盤整備に係るソフトウェア等の製品導入と保守サービス、インターネットを介したサイバー攻撃対策に有効なデジタルフォレンジック等の製品販売や調査サービス、トレーニング

▶2017年6月1日 サイバー犯罪の証拠データ分析の高速処理化に向け、フォーカスシステムズと日本マイクロソフトが連携

<https://www.focus-s.com/focus-s/media/20170601.pdf>

▶東証一部上場。時価総額180億円(2018/11/22時点)

4704 トレンドマイクロ

<https://virusbuster.jp/vb/trial/sem/mac.htm>

▶当社の企業集団は、コンピュータセキュリティ対策製品の開発、販売及び関連サービスの提供を行っている当社ならびに北米、欧州、アジア・パシフィック、中南米地域の子会社と、関連会社としてモバイルデバイスプラットフォームサービスプロバイダであるGeneral Mobile Corporation等により構成されております。

(1) コンピュータセキュリティ対策製品の開発、販売に関する事業

コンピュータセキュリティ対策製品群の名称

PCクライアント製品 LANサーバ製品 インターネットサーバ製品 統合製品 その他製品

(2) その他の事業

モバイルデバイスプラットフォームおよびモバイルインターネットサービスにおけるトータルソリューションを提供するGeneral Mobile Corporationにより、コンピュータセキュリティ対策製品の開発、販売に関する事業以外の事業が行われております。

▶代表取締役Eva Chen氏はForbes Asiaの「50 Power Businesswomen (アジアで最も有力な女性企業家トップ50)」に選出されている著名女性経営者

https://www.trendmicro.com/ja_jp/about/leaders.html

▶2018年11月15日 NEC、トレンドマイクロ、三井住友海上 サイバー保険付帯の「仮想パッチによるサーバ脆弱性対策サービス」を開発

https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20181107-01.html

▶2018年9月5日 トレンドマイクロとMoxaが産業用IoT向けアプリケーションのセキュリティで提携

https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20180905-01.html

▶MOXA 日本語サイト

<https://japan.moxa.com>

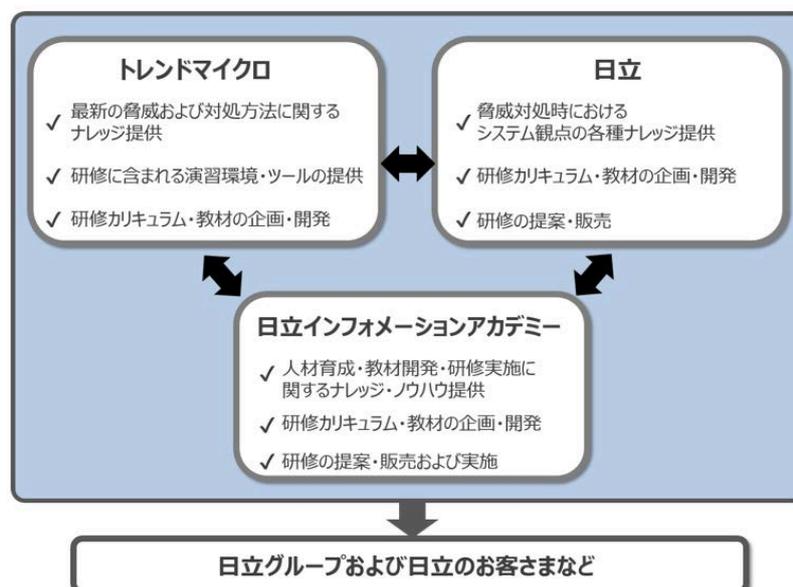
▶2018年8月28日 「セキュリティインシデントに関する被害コスト調査」を発表

https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20180828-01.html

上記のような調査レポートの報告が豊富

▶2018年6月6日 日立とトレンドマイクロが、サイバーセキュリティ分野における人材育成の協業に合意

https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20180606-01.html





- ▶ 5期連続売上成長
- ▶ 売上総利益率が80%と高い
- ▶ 6年で株価3倍
- ▶ 東証一部上場。時価総額8838億円(2018/11/22時点)

4726 ソフトバンク・テクノロジー

<https://www.softbanktech.co.jp>

セグメント	サービス区分	主なサービスの内容	主な事業会社の名称
報告 セグメント	デジタル マーケティング	<ul style="list-style-type: none"> ・ ECサイト運営代行サービス、フロントセットの開発・販売及びウェブフロントサービスの提供 ・ ウェブサイトの構築、アクセスログ解析ツール、データ解析及びコンサルティングサービスの提供 	<ul style="list-style-type: none"> ・ ソフトバンク・テクノロジー(株) ・ フォントワークス(株) ・ ㈱環
	プラットフォーム ソリューション	<ul style="list-style-type: none"> ・ IT基盤の構築と運用保守サービス、リナックスソリューションの提供 ・ 脆弱性診断テストや標的型攻撃対策サービス、電子証明書を利用した認証や暗号化サービスの提供 	<ul style="list-style-type: none"> ・ ソフトバンク・テクノロジー(株) ・ サイバートラスト(株) (注)
	クラウドシステム	<ul style="list-style-type: none"> ・ 情報システムの開発と運用保守サービス、タブレット端末やスマートフォン、ロボット用アプリケーションの開発 ・ 情報システムのクラウド移行支援、親和性の高い自社クラウドサービスの提供 	<ul style="list-style-type: none"> ・ ソフトバンク・テクノロジー(株) ・ MSLUIS(株) ・ アソラテック(株) ・ リデン(株)

(注) 2017年10月1日付で、サイバートラスト(株)はミラクル・リナックス(株)に吸収合併されております。またミラクル・リナックス(株)は、同日付でサイバートラスト(株)へ商号変更しております。

- ▶ ECサイトの運営代行
- ▶ 弱性診断テスト、電子証明書を利用した認証や暗号化
- ▶ ソフトバンクグループが54.3%を保有する親会社
- ▶ 東証一部上場。時価総額437億円(2018/11/22時点)

4847 インテリジェントウェイブ

<https://www.iwi.co.jp>

- ▶ 金融業界向けシステム開発
- ▶ 盗難カード、偽造カードの不正利用検知
- ▶ セキュリティ対策ソフトの販売
- ▶ 当社は、クレジットカード会社、銀行、証券会社等、金融業界の特定の業務に密接に関与するシステム開発を主要な事業領域としていますが、社会環境の変化や情報通信技術の進化に伴い、顧客の業務運用やシステム投資の需要も変化しており、こうした変化に対応するだけでなく成長機会として積極的に活かしていく方針です。

当社は、既存の事業領域においては、顧客の期待を超える品質のシステムをソリューションとして提供することで、顧客との信頼関係を更に強固に維持していきます。そのうえで、社会や技術の環境変化を事業機会として、顧客の様々な業務分野へ積極的なシステム提案を行うことで、当社の事業領域を拡大していく方針です。クレジットカードだけでなく、プリペイド、デビットからICカードやスマートフォンを利用した決済業務を完遂するために必要なネットワーク接続や、カードの使用認証の機能分野において、当社は豊富な経験と実績を保有していますが、こうした事業上の強みを伸ばし、事業領域を更に拡大するために必要な新製品やサービスを早期に開発し、顧客へ提供することで、当社事業を継続的に成長させる方針です。

- ▶ 2018年11月21日 個人投資家向け資料より。下記の情報セキュリティ製品を販売している

<https://contents.xj-storage.jp/xcontents/AS00585/0d88c58b/0fea/4d89/ad4e/d876799656e5/20181122102725203s.pdf>

Road to 10B

情報セキュリティ製品の販売



点から面へソリューション拡大

攻撃対策		内部犯行		外部からのサイバー攻撃		
脅威		内部情報漏洩	侵入 脆弱性攻撃 標的型攻撃	ランサム等 Malware対策	手動による攻撃操作 横展開/汚染	大量のログデータに 隠れた脅威
攻撃を検知	CWAT					
管理者への通知	自社製品		Palo Alto Networks社	illusive networks社	SecBI社	
レポート フォレンジック	CWAT		Traps	Deceptions Everywhere	SecBI	
動作を止める			eyeShare™			
インシデント対応 外部連携			ayehu社			イスラエル発の製品
運用監視支援 SOC支援			eyeShare			
事前対策		脆弱性診断ツール		ユーザ・パスワード管理		
内容		OS/Network診断	Web脆弱性診断		特権アカウント管理	
セキュリティ管理 PCI DSS対応	Rapid7社(米国) RAPID7 Nexpose/Metasploit	UBsecure社(国産) VEX		CyberArk Software社 CyberArk PAS		

- ▶大日本印刷が50.6%を保有する親会社
- ▶東証二部上場。時価総額224億円(2018/11/22時点)

6050 イー・ガーディアン

<https://www.e-guardian.co.jp>

- ▶SNSでの誹謗中傷や不適切コメントの管理、分析、運用
 - ▶ビットコインの本人認証サービスの提供
 - ▶ソーシャルゲームの新規案件の獲得、
 - ▶広告審査、入稿管理、広告枠の管理、広告ライティング
 - ▶WEBサービスを運用する法人に対して、一般利用者から投稿されたコメント、画像、動画に違法性、不適切、誹謗中傷がないかどうか監視し、目視件数に応じた報酬をもらっている
 - ▶風評調査業務
 - ▶CS業務。ソーシャルゲームのユーザーからの退会の処理、メールや電話によるテクニカルサポート、ヘルプデスク対応
 - ▶オンラインゲームを使っているユーザーからの要望への対応、パトロール業務、不正ツールの取り締まり
 - ▶デバック業務。ゲームの動作チェック、文字化け、レイアウト
 - ▶2017年11月24日 2017年9月期 決算説明会資料
- <https://www.e-guardian.co.jp/ir/pdf/2017年9月期決算説明会資料.pdf>
- ▶5期連続売上、純利益成長。5期で2倍
 - ▶東証一部上場。時価総額254億円(2018/11/22時点)

6088 シグマクシス

<https://www.sigmaxyz.com>

■ビジネス戦略策定支援及びシステム構築・運用支援サービス

下記の能力を組み合わせ、企業が事業戦略を策定・実行して成果を出すための支援を行います。

- ・事業戦略策定
- ・事業運営マネジメント
- ・IT計画策定
- ・ITサービスマネジメント
- ・セキュリティ
- ・システムアセンブリング
- ・小売事業改革
- ・製薬事業改革
- ・物流事業改革
- ・公共事業改革

■プログラム&プロジェクトマネジメント支援サービス

下記の能力を組み合わせ、プロジェクトの成果を出すために必要となる、プログラムおよびプロジェクトマネジメントの支援を行います。

- ・プロジェクトマネジメント

- ・ベンダー(外注先)マネジメント
- ・ステークホルダー(利害関係者)マネジメント
- ・チェンジ(変革)マネジメント
- ・インテグレーション(統合)マネジメント
- ・高速開発マネジメント

■デジタル変革支援サービス

下記の能力を組み合わせ、デジタル技術を用いて新たな企業競争力を生み出す事業変革支援を行います。

- ・人工知能&アナリティクス
- ・IoT&ロボティクス
- ・クラウドソリューション
- ・サービスデザイン
- ・デジタルアーキテクチャー設計
- ・構築

■イノベーション組織への変革支援サービス

下記の能力を組み合わせ、イノベーションによる新たな価値を生み出す組織づくりの支援を行います。

- ・ビジョンフォレスト(アートを使った組織変革アプローチ)/変革リーダー
- ・ラボ(次世代変革リーダーの育成 プログラム)
- ・イノベーション創発組織デザイン
- ・ビジネスイノベーション支援

■M&A戦略・アドバイザー及び価値算定サービス

金融機関、投資銀行の出身者、そして経営コンサルティングのプロフェッショナルによって構成されるチームで M&A戦略立案、M&Aアドバイザー、そしてPMI(Post Merger Integration : 経営統合)までをワンストップで支援を行います。

- ▶三菱商事が32.9%を保有する親会社
- ▶4期連続売上、純利益成長
- ▶東証一部上場。時価総額216億円(2018/11/22時点)

8023 大興電子

<https://www.daikodenshi.jp>

- ▶OA機器、電子計算機、電子通信機器の開発、販売、施工、保守
- ▶富士通特約店で売上3位
- ▶米政府で18年間破られていない実績を誇るAppGuard

<https://www.daikodenshi.jp/solution/appguard/>

- ▶AppGuardを提供しているBlue Planet-works社

<https://www.blueplanet-works.com/contents/solution/>

- ▶AppGuardは、内閣サイバーセキュリティセンター (NISC) 「政府機関等の対策基準策定のためのガイドライン」に適合した製品

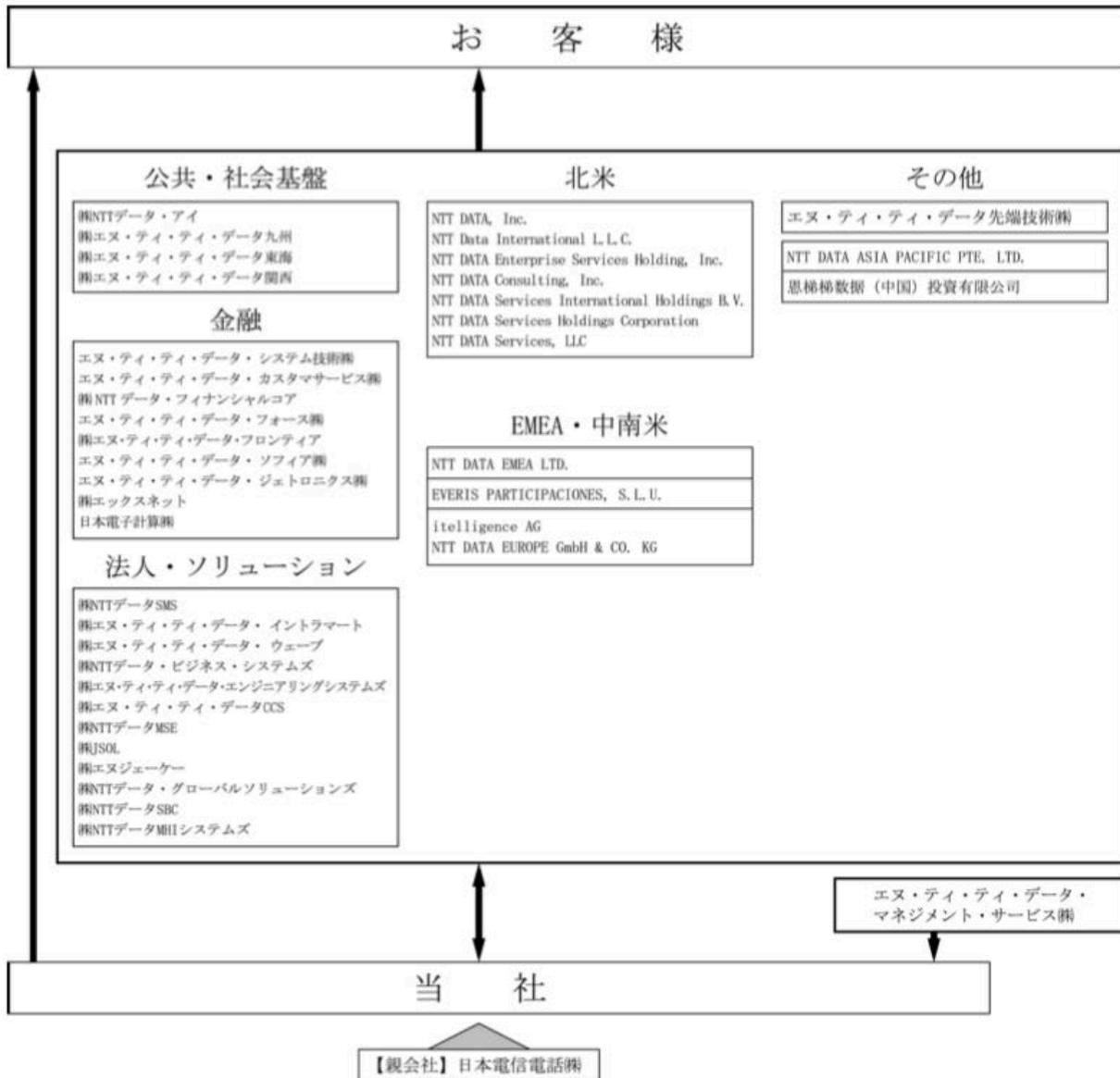
<https://www.blueplanet-works.com/contents/news/detail.html#/posts/126>

- ▶東証二部上場。時価総額92億円(2018/11/22時点)

<p>個別受注生産管理システム</p> <p>rBOM</p> <p>▶ 詳しくはこちらから</p>	<p>調達支援ソリューション</p> <p>PROCURE SUITE</p> <p>▶ 詳しくはこちらから</p>	<p>帳票配布・データ交換ツール</p> <p>EdiGatePOST</p> <p>▶ 詳しくはこちらから</p>	<p>クラウド型情報配信ソリューション</p> <p>i-Compass</p> <p>▶ 詳しくはこちらから</p>
<p>専門店向けMD/POSシステム</p> <p>Retail Focus</p> <p>▶ 詳しくはこちらから</p>	<p>新しい概念のセキュリティ技術</p> <p>APPGUARD</p> <p>▶ 詳しくはこちらから</p>	<p>マイナンバーセキュリティ</p> <p>D's GUARDIAN</p> <p>▶ 詳しくはこちらから</p>	<p>モバイルでありながらセキュアな通信</p> <p>D's モバイル</p> <p>▶ 詳しくはこちらから</p>
<p>セキュリティソリューション</p> <p>セキュリティ</p> <p>▶ 詳しくはこちらから</p>	<p>AI/IoTの取り組み</p> <p>AI/IoTの取り組み</p> <p>▶ 詳しくはこちらから</p>	<p>RPAの取り組み</p> <p>DAiKO-RPA</p> <p>▶ 詳しくはこちらから</p>	<p>働き方改革</p> <p>働き方改革</p> <p>▶ 詳しくはこちらから</p>
<p>取扱製品一覧</p> <p>取扱製品一覧</p> <p>▶ 詳しくはこちらから</p>	<p>法人様向けECサイト</p> <p>おカフベス</p> <p>PC・周辺機器など40万点の品揃え</p> <p>▶ 詳しくはこちらから</p>		

9163 NTTデータ

<http://www.nttdata.com/jp/ja/>



▶2018年10月31日 グローバルセキュリティ動向四半期レポート（2018年度 第2四半期）

[http://www.nttdata.com/jp/ja/news/information/2018/pdf/](http://www.nttdata.com/jp/ja/news/information/2018/pdf/NTTDATA_FY2018_2Q_SecurityReport.pdf)

[NTTDATA_FY2018_2Q_SecurityReport.pdf](http://www.nttdata.com/jp/ja/news/information/2018/pdf/NTTDATA_FY2018_2Q_SecurityReport.pdf)

サイバーインシデントの詳細が報告されているレポート

▶5期連続売上成長

▶NTTが54.1%を保有する親会社

▶東証一部上場。時価総額1兆7994億円(2018/11/22時点)

Business of VLC

株式会社バルクHDのは下記の事業を行っている。

グループ会社一覧

 <p>株式会社バルク セキュリティ事業： コンサルティングサービス マーケティング事業： マーケティングリサーチサービス</p> <p>プライバシーマークやISO27001の認定・認証取得支援等を行う情報セキュリティコンサルティングサービス及び調査企画・設計・分析・レポートまでのフルサポートを特徴としたマーケティングリサーチサービスなどを提供しております。</p> <table border="1"><tr><td>資本金：100百万円</td><td>設立：2007年3月</td></tr><tr><td>代表者：伊倉 宏之</td><td>保有比率：100%</td></tr></table> <p>WEB SITE</p>	資本金：100百万円	設立：2007年3月	代表者：伊倉 宏之	保有比率：100%	 <p>株式会社マーケティング・システム・サービス マーケティング事業： セールスプロモーション、広告代理</p> <p>主に食品に関連した流通業界、メーカー、物流会社などに対し、各種セールス企画、キャンペーン企画及びその事務局運営、イベント企画、店頭配布用フリーペーパーの立案作成並びに各種ノベルティの制作など幅広い領域においてプロモーション活動の支援サービスを提供しております。</p> <table border="1"><tr><td>資本金：10百万円</td><td>設立：2005年8月</td></tr><tr><td>代表者：青木 慎博</td><td>保有比率：100%</td></tr></table> <p>WEB SITE</p>	資本金：10百万円	設立：2005年8月	代表者：青木 慎博	保有比率：100%
資本金：100百万円	設立：2007年3月								
代表者：伊倉 宏之	保有比率：100%								
資本金：10百万円	設立：2005年8月								
代表者：青木 慎博	保有比率：100%								
 <p>Strategic Cyber Holdings LLC (米国) セキュリティ事業： サイバーセキュリティトレーニングサービス</p> <p>イスラエルのCyberGym Control Ltd.との共同事業会社であり、サイバーセキュリティトレーニング施設の運営・提供、その他サイバーセキュリティ関連サービス・製品の提供を行ないます。</p> <table border="1"><tr><td>資本金：1.47百万米ドル</td><td>設立：2018年1月</td></tr><tr><td>代表者：石原 紀彦</td><td>持分比率：100%</td></tr></table> <p>WEB SITE</p>	資本金：1.47百万米ドル	設立：2018年1月	代表者：石原 紀彦	持分比率：100%	 <p>株式会社CEL セキュリティ事業： サイバーセキュリティソリューションサービス</p> <p>EBサービス、スマホアプリ、Eコマース、ブロックチェーン事業者をはじめとする成長IT企業の企業価値向上を目的として、情報資産に関する脅威調査、脆弱性診断、ペネトレーションテスト、マネジドセキュリティ、SoCなどのサイバーセキュリティサービスを提供しています。</p> <table border="1"><tr><td>資本金：30百万円</td><td>設立：2018年9月</td></tr><tr><td>代表者：田中翔一朗</td><td>保有比率：100%</td></tr></table> <p>WEB SITE</p>	資本金：30百万円	設立：2018年9月	代表者：田中翔一朗	保有比率：100%
資本金：1.47百万米ドル	設立：2018年1月								
代表者：石原 紀彦	持分比率：100%								
資本金：30百万円	設立：2018年9月								
代表者：田中翔一朗	保有比率：100%								

関連会社

 <p>CyberGym Control Ltd. (イスラエル) サイバーセキュリティサービスの提供</p> <p>重要インフラ事業者向けに分野ごとに構築した模擬システムを使いサイバー攻撃に対応するための実践的な訓練サービスその他サイバーセキュリティ関連サービス・製品の提供を行っております。</p> <p>WEB SITE</p>	 <p>AerNos, Inc. (米国) ガスセンサーの開発・販売</p> <p>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ガスセンサーの開発販売を行っております。</p> <p>WEB SITE</p>
---	---

1【主要な経営指標等の推移】

(1) 連結経営指標等

回次	第20期	第21期	第22期	第23期	第24期
決算年月	2014年3月	2015年3月	2016年3月	2017年3月	2018年3月
売上高 (千円)	1,693,543	2,060,187	2,250,145	1,712,841	1,008,551
経常利益 (千円)	24,476	49,211	69,042	23,176	19,935
親会社株主に帰属する当期純利益 又は親会社株主に帰属する当期純 損失 (△) (千円)	15,724	△15,938	51,270	6,723	42,909
包括利益 (千円)	16,751	△10,978	57,040	11,238	42,029
純資産額 (千円)	655,590	644,611	701,652	712,890	714,255
総資産額 (千円)	1,310,447	1,409,744	1,424,130	910,860	962,277
1株当たり純資産額 (円)	84.92	82.79	89.63	90.53	95.19
1株当たり当期純利益又は 1株当たり当期純損失 (△) (円)	2.41	△2.13	6.84	0.90	5.73
潜在株式調整後1株当たり 当期純利益 (円)	-	-	-	-	-
自己資本比率 (%)	48.6	44.0	47.2	74.5	74.1
自己資本利益率 (%)	3.1	-	7.9	1.0	6.2
株価収益率 (倍)	82.9	-	24.8	147.1	52.9
営業活動による キャッシュ・フロー (千円)	66,700	33,257	122,495	△45,541	△15,516
投資活動による キャッシュ・フロー (千円)	△62,787	771	9,267	△867	△195,448
財務活動による キャッシュ・フロー (千円)	62,489	56,907	△14,391	85,979	50,145
現金及び現金同等物の期末残高 (千円)	322,587	413,524	530,896	570,466	409,647
従業員数 (人)	59	68	64	52	36
(ほか、平均臨時雇用者数)	(3)	(3)	(3)	(3)	(2)

(1) コンサルティング事業

①情報セキュリティコンサルティング

プライバシーマーク認定コンサルティングやISO27001 (ISMS) 認証コンサルティング等の取得・更新・運用支援をはじめとする情報セキュリティ強化のための各種コンサルティングサービスを提供しております。

a. プライバシーマーク制度

プライバシーマーク制度とは、日本工業規格JISQ5001 (個人情報保護に関するコンプライアンス・プログラムの要求事項) に適合していることを審査・認定し、その証明として、プライバシーマークというロゴマークの使用を許諾する制度であり、財団法人日本情報処理開発協会 (JIPDEC) が、その運用を行っております。

b. ISO27001 (ISMS) 適合性評価制度

ISMS適合性評価制度とは、全業種を対象に、国際的に整合性のとれた情報セキュリティマネジメント基準に適合していることを審査・認定し、その証明としてISMS認定シンボルというロゴマークの使用を許諾する制度であり、財団法人日本情報処理開発協会 (JIPDEC) が、その運用を行っております。

(主な関係会社) 株式会社バルク

②サイバーセキュリティソリューション

サイバーセキュリティトレーニングサービス、脆弱性診断サービス等のサイバーセキュリティソリューションサービスを提供しております。

(主な関係会社) Strategic Cyber Holdings LLC、株式会社バルク

(2) マーケティング事業

①マーケティングリサーチ

新製品等開発のためのユーザーニーズ調査、ブランドイメージ調査、CS (顧客満足度) 調査、ES (従業員満足度) 調査、Q1浸透度調査、Webサイト調査及びその他各種意識調査、並びにこれらに関する分析サービス等を提供しております。

インターネット調査、グループインタビュー調査、街頭調査及び訪問面接調査等の各種調査手法によるクライアントのニーズに合わせたオーダーメイド型の調査・分析サービスの特徴としております。

(主な関係会社) 株式会社バルク

②セールスプロモーション、広告代理

主に食品関連の小売業界、メーカー、物流企業に対して、各種セールス企画、キャンペーン企画及びその事務局運営、イベント企画、販促用フリーペーパーの企画制作、ノベルティ制作等の幅広い領域でセールスプロモーション活動の支援等を行っております。

(主な関係会社) 株式会社マーケティング・システム・サービス

ほとんどのサイバーセキュリティ業界の企業がマルウェア対策ソフトの販売などを行っている中で、バルクHDはサイバーセキュリティのトレーニング事業を行っている。また、サイバーセキュリティ対策の本場である、アメリカ、イスラエルの企業との提携を進めている。

Board Member of VLC

バルクホールディングスと関連会社には以下のような役員陣が在籍している。

代表取締役 石原 紀彦 氏

2018年1月1日に代表取締役に就任。

ゴールドマン・サックス証券出身

<https://www.goldmansachs.com/japan/>

Forbes JAPANを発行している株式会社アトミックメディアの元代表取締役CEOで、現在は席を高野真氏に譲っている。

当時のIR)

https://atomixmedia.co.jp/pdf/BL_from_atomixmedia0623.pdf

株式会社アトミックメディア

<https://atomixmedia.co.jp>

成長戦略総合研究所の社外取締役

<http://www.rigs.co.jp/members.html>

みやこキャピタル株式会社の取締役

<https://www.miyakocapital.com>

子会社Strategic Cyber Holdings LLCのCEO

<https://www.cybergym.com/ja/>

父親の石原邦夫氏は、東京海上日動火災保険相談役、経団連副会長、日米経済協議会会長、東京急行電鉄監査役、日本郵政社外取締役、国土審議会会長代理、日本情報システム・ユーザー協会会長。東京海上ホールディングス及び東京海上日動火災保険の初代社長・会長や日本損害保険協会会長、経済同友会副代表幹事、三菱東京UFJ銀行取締役、NHK経営委員会委員長などを歴任。

<https://ja.wikipedia.org/wiki/石原邦夫>





取締役 松田 孝裕 氏

株式会社ソフトブレイン（東証一部上場）の元代表取締役
<http://www.softbrain.co.jp>

成長戦略総合研究所の取締役
<http://www.rigs.co.jp/members.html>

株式会社ティ・エムコンサルティング代表取締役
<http://t-m-consulting.com/index.html>

ソフトブレインは松田氏が入社(2003年)から代表取締役(2005年)に株価が約11倍になっている。



取締役 田中 翔一郎 氏

Tanaakk株式会社 代表取締役
<http://tanaakk.co.jp>

GFX CEO
<http://gfxfoundation.com/?lang=en>

バルクホールディングスの子会社である株式会社
CELの代表取締役
[http://v4.eir-parts.net/v4Contents/View.aspx?
cat=tdnet&sid=1623327](http://v4.eir-parts.net/v4Contents/View.aspx?cat=tdnet&sid=1623327)



以下は新役員の略歴など

候補者番号	氏名 (生年月日)	略歴、地位、担当及び重要な兼職の状況	所有する 当社の 株式数
1	石原 紀彦 (1977年 5 月 4 日生)	<p>2001年 4 月 ゴールドマン・サックス・アセット・マネジメント株式会社入社</p> <p>2004年 8 月 ゴールドマン・サックス証券株式会社入社</p> <p>2009年 2 月 日本コアパートナー株式会社取締役副社長</p> <p>2011年 1 月 株式会社アトミックスメディア取締役</p> <p>2011年 3 月 サンインベストメント合同会社設立 代表社員(現任)</p> <p>2013年 9 月 みやこキャピタル株式会社取締役(現任)</p> <p>2014年 4 月 サンインベストメント株式会社設立 代表取締役(現任)</p> <p>2014年 6 月 株式会社アトミックスメディア代表取締役</p> <p>2017年 3 月 株式会社アトミックスメディア取締役</p> <p>2017年 6 月 当社取締役</p> <p>2018年 1 月 当社代表取締役社長(現任)</p> <p>2018年 1 月 Strategic Cyber Holdings LLC Chairman of the Board & CEO(現任)</p> <p>(重要な兼職の状況)</p> <p>Strategic Cyber Holdings LLC Chairman of the Board & CEO</p> <p>サンインベストメント合同会社 代表社員(非常勤)</p> <p>サンインベストメント株式会社 代表取締役(非常勤)</p> <p>みやこキャピタル株式会社 取締役(非常勤)</p>	11,800株
2	五十嵐 雅人 (1972年 8 月18日生)	<p>1996年 4 月 垂細証券印刷株式会社(現 株式会社プロネクサス)入社</p> <p>2001年 1 月 ナスダック・ジャパン株式会社入社</p> <p>2002年11月 ディー・ブレイン証券株式会社入社</p> <p>2004年 4 月 IPO証券株式会社(現 株式会社アイネット証券)入社</p> <p>2007年 8 月 同社取締役</p> <p>2008年 9 月 IPOキャピタルパートナーズ株式会社設立 代表取締役社長</p> <p>2010年 1 月 ユナイテッドベンチャーズ株式会社入社</p> <p>2012年 2 月 当社入社 経営企画室長</p> <p>2012年 6 月 当社取締役管理本部長兼経営企画室長(現任)</p> <p>2013年 4 月 株式会社マーケティング・システム・サービス 取締役(現任)</p> <p>2014年 2 月 株式会社ハウスバンクインターナショナル取締役</p> <p>2014年 6 月 株式会社ヴィオ取締役</p> <p>2018年 1 月 株式会社バルク取締役(現任)</p> <p>2018年 1 月 Strategic Cyber Holdings LLC Board member(現任)</p> <p>(重要な兼職の状況)</p> <p>株式会社バルク 取締役(非常勤)</p> <p>株式会社マーケティング・システム・サービス 取締役(非常勤)</p> <p>Strategic Cyber Holdings LLC Board member(非常勤)</p>	5,900株
3	西澤 岳志 (1966年 3 月29日生)	<p>1989年 9 月 株式会社協和銀行(現 株式会社りそな銀行)入社</p> <p>2000年 9 月 株式会社イージーユーズ(現 アキナジスタ株式会社)入社</p> <p>2001年 4 月 同社代表取締役社長</p> <p>2009年 4 月 株式会社プロフィットメディア(現 株式会社 Buying)設立 代表取締役(現任)</p> <p>2009年 8 月 株式会社ウィザーズプラス設立 代表取締役社長(現任)</p> <p>2011年12月 株式会社ライフステーション取締役(現任)</p> <p>2012年 6 月 当社社外取締役(現任)</p> <p>2012年 9 月 西澤管財株式会社設立 代表取締役社長(現任)</p> <p>(重要な兼職の状況)</p> <p>株式会社ウィザーズプラス 代表取締役社長</p> <p>西澤管財株式会社 代表取締役社長</p> <p>株式会社Buying 代表取締役</p> <p>株式会社ライフステーション 取締役</p>	1,020,200株

新役員の略歴など

候補者 番号	氏 名 (生年月日)	略歴、地位、担当及び重要な兼職の状況	所有する 当社の 株式数
4	<p style="text-align: center;">ひらやま つよし 平山 剛 (1980年 8 月 1 日生)</p>	<p>2004年 4 月 株式会社ピラミッドフィルム入社 2007年 6 月 監査法人トーマツ(現 有限責任監査法人トーマツ)入所 2009年12月 公認会計士登録 2009年12月 弁護士登録 2009年12月 平山剛公認会計士事務所設立 代表(現任) 2010年 1 月 伊藤 見富法律事務所/モリソンフォースター 外国法事務弁護士事務所入所 2012年10月 株式会社オモロキ取締役(現任) 2015年 1 月 株式会社ブレイブソフト取締役 2015年 3 月 タイラカ総合法律事務所設立 代表(現任) 2015年 4 月 慶應義塾大学総合政策学部非常勤講師 2017年 6 月 当社社外取締役(現任) 2018年 3 月 株式会社A P P r o g 取締役(現任) (重要な兼職の状況) タイラカ総合法律事務所 代表 平山剛公認会計士事務所 代表 株式会社オモロキ 取締役 株式会社A P P r o g 取締役</p>	1,900株
5	<p style="text-align: center;">【新任】 まつだ たかひろ 松田 孝裕 (1960年 5 月20日生)</p>	<p>1983年 4 月 富士通株式会社入社 2003年11月 ソフトブレーション株式会社入社 2004年 3 月 同社取締役副社長 2005年 6 月 同社代表取締役社長 2008年 6 月 ティ・エムコンサルティング株式会社設立 代表 取締役(現任) 2011年 4 月 コムチュア株式会社常務取締役 2012年 5 月 株式会社エアウィーヴ取締役副社長 2014年 9 月 同社代表取締役社長 2017年 9 月 ナイスパス株式会社代表取締役(現任) (重要な兼職の状況) ティ・エムコンサルティング株式会社 代表取締役 ナイスパス株式会社 代表取締役</p>	一株
6	<p style="text-align: center;">【新任】 たなか しょういちろう 田中 翔一朗 (1987年 7 月30日生)</p>	<p>2010年 7 月 SAPジャパン株式会社入社 2012年 3 月 オートノミー株式会社(現 日本ヒューレット・ パッカード株式会社)入社 2013年 7 月 Tanaakk株式会社設立 代表取締役社長(現任) (重要な兼職の状況) Tanaakk株式会社 代表取締役社長</p>	20,000株

Shareholder of VLC

(6) 【大株主の状況】

2018年3月31日現在

氏名又は名称	住所	所有株式数 (株)	発行済株式(自己 株式を除く。)の 総数に対する所有 株式数の割合 (%)
村松 澄夫	千葉県流山市	1,210,000	16.1
西澤管財株式会社	東京都中央区銀座4丁目9番8号	1,000,000	13.3
株式会社MHcapital	東京都港区海岸1丁目2番20号	992,000	13.2
J P capital株式会社	東京都港区赤坂9丁目5番26号	900,000	12.0
西岡 将基	東京都荒川区	240,000	3.2
株式会社DAWNCAPITAL	東京都港区海岸1丁目1番1号	120,200	1.6
中辻 哲朗	京都市下京区	100,000	1.3
有限会社アート緑化	埼玉県飯能市中居134-1	74,900	1.0
細羽 強	広島県福山市	70,000	0.9
幅 昭義	東京都新宿区	63,200	0.8
計	—	4,770,300	63.7

(5) 【大株主の状況】

2018年9月30日現在

氏名又は名称	住所	所有株式数 (株)	発行済株式(自己 株式を除く。)の 総数に対する所有 株式数の割合 (%)
西澤管財株式会社	東京都中央区銀座四丁目9番8号	1,000,000	11.50
村松 澄夫	千葉県流山市	916,700	10.54
日本トラスティ・サービス信託銀行 株式会社	東京都中央区晴海1丁目8-11	204,900	2.36
松井証券株式会社	東京都千代田区麹町1丁目4番地	198,900	2.29
カブドットコム証券株式会社	東京都千代田区大手町1丁目3番2号	128,600	1.48
米田 豊	東京都杉並区	100,100	1.15
金本 康来	大阪市阿倍野区	95,000	1.09
株式会社SBI証券	東京都港区六本木1丁目6番1号	80,000	0.92
米田 研介	東京都杉並区	72,500	0.83
有限会社アート緑化	埼玉県飯能市中居134-1	72,100	0.83
計	—	2,868,800	33.00

1. 筆頭株主：西澤管財株式会社（1,000,000株）。代表取締役の西澤岳志氏はバルクHDの社外取締役である。また株式会社ウィザーズプラスの代表取締役を兼任している。

<https://www.wizardz-plus.jp/saiyo/>

2. 第二位：村松澄夫氏（916,700株）。バルクHDの創業者であり、経営安定の観点から長期保有を目的としているが、経営陣および事業内容が一変したため持ち株の売却を進めている。

3. 代表取締役石原 紀彦氏は普通株式を10,900株保有している。また、払込価格100円、行使価格300円の新株予約権で899,200株保有しており、行使すると合計910,100株となり、第3位の株主になる。行使期間は2019年7月1日～2023年6月30日まで。

なお、バルクHDの発行済株式総数は8,694,000株である。

Consideration of IR

株式会社バルクHDの適時開示に対して以下のような解釈をし、取引に反映させた。

2017年12月22日

CyberGym Control Ltd.との共同事業に関する独占的ライセンス契約締結等のお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1541357/00.pdf>

1. ライセンス締結の目的

当社はサイバージム社との間で、共同事業体を通じて重要インフラストラクチャーセクターの民間企業及び政府機関等に対してサイバー攻撃に対応するためのトレーニング施設(コマーシャルアリーナ※1)を米国ニューヨーク州に開設すること、並びにサイバージム社独自開発のサイバー環境を模したトレーニング施設(ハイブリッドアリーナ※2)を米国及び日本で販売・サービス提供を行うこと。

※1 コマーシャルアリーナ

重要インフラストラクチャーの複数セクターを対象とするサイバーセキュリティトレーニングのフルパッケージサービスを提供する大型のトレーニング施設となります。コマーシャルアリーナ内には、対象セクターに対応する模擬施設、ハードウェア及びソフトウェアなどが構築され、サイバーセキュリティのスペシャリストで構成される攻撃側の RED TEAMや防衛側をサポートする WHITE TEAM などが配備されます。

※2 ハイブリッドアリーナ

特定顧客・特定セクターを対象とした小型のトレーニング施設であり、主に顧客の社内又は設備内に設置されます。なお、ハイブリッドアリーナ向けのサービス等は、コマーシャルアリーナを通じて提供されます。

2. 共同事業としてのライセンス契約の概要

(1)締結日 2017年12月22日

(2)当初支出金額 500万米ドル(詳細については下記3.を参照)

(3)ライセンス契約に基づく共同事業の内容

- ①米国ニューヨーク州へのコマーシャルアリーナの設置・運営。同アリーナによる他のハイブリッドアリーナ向けサービス提供
- ②日本及び米国(オクラホマ州及びテキサス州を除く)の顧客に対するサイバーセキュリティサービスの提供、ハイブリッドアリーナの販売
- ③サイバージム社がサイバーセキュリティ関連情報のリアルタイム相互共有を目的としたサイバーストリックを立ち上げた際における同グリッドへの参加

上記の共同事業を展開するため、サイバージム社は共同事業会社に対してアリーナ等の販売・設置、並びにノウハウ、情報及びソフトウェアの提供を行い、共同事業会社が顧客向けにサイバーセキュリティトレーニングサービスの提供やハイブリッドアリーナの販売を行います。

CyberGym Control Ltd.

<https://www.cybergym.com/ja/company/>

は、イスラエル電力公社 (Israel Electric Corporation) とイスラエルのサイバーセキュリティコンサルタントであるCyber Control社とのジョイントベンチャーです。イスラエル電力公社は日常的に数えきれないほどのサイバー攻撃に直面している年間売上77億米ドルにも達する企業であり、Cyber Control社はNISA (国家情報安全保障庁) のメンバーとセキュリティ専門家によって設立されたイスラエルのサイバーセキュリティ分野におけるリーディングカンパニーです。

イスラエル電力公社 (Israel Electric Corporation)

<https://www.iec.co.il/en/pages/default.aspx>

イスラエル電力公社はイスラエルで唯一の電力会社であるため平均的に一日6000回以上のハッキングを受けている。そのため世界TOPクラスのサイバーセキュリティ対策をとっている企業でもある。

→このIRで株価が180円(12/22終値)から430円(1/9終値)に高騰。新規事業への期待と、イスラエル電力公社とCyberGym Control Ltd.との協業による売上向上を予測した個人投資家の買いが入ったと思われる。このIRからバルクHDがサイバーセキュリティ業界で成長し、企業価値向上するストーリーが始まった。

雑誌『CIO APPLICATIONS』にて、CyberGym Control Ltd.が2018年のサイバーセキュリティ企業のTop25社に選ばれた。

<https://www.cioapplications.com/vendors/top-25-cybersecurity-companies-2018-rid-79.html>



米国の政府機関に導入され18年間破られていないという実績を誇るセキュリティソフトウェア会社のAppgurd

<https://www.appguard.us>

時価総額190億ドルのサイバーセキュリティ大手のpalo Alto networks

<https://www.paloaltonetworks.com>

といった、企業がTo25に入った。



CyberGym Control : An Innovative Approach Tackling Cyberattacks

<https://www.cioapplications.com/vendor/cybergym-control-an-innovative-approach-to-tackling-cyberattacks--cid-1699-mid-97.html>

CEOであるOfir Hasonのコメントが掲載されている。

2018年1月3日

CyberGym has announced the establishment of WCWA - a global cyber warfare arena and the construction of a training arena in New York

<https://www.cyberreadyusa.com/single-post/2018/01/02/Cybers-has-announced-the-establishment-of-WCWA---a-global-cyber-warfare-arena-and-the-construction-of-a-training-arena-in-New-York>

CyberGym社はWCWAの設立を発表しました。これはグローバルなサイバー対策の場であり、そのトレーニング施設をニューヨークに建設する予定です。

2018年1月31日

(適時開示の経過) CyberGym Control Ltd.との共同事業会社の設立に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1549239/00.pdf>

新会社名：Strategic Cyber Holdings LLC

事業目的：サイバーセキュリティトレーニング施設の運営・提供

その他サイバーセキュリティ関連サービス・製品の提供

WCWA(World Cyber Warfare Arena)への参加

<https://www.cyberreadyusa.com/single-post/2018/01/02/Cybers-has-announced-the-establishment-of-WCWA---a-global-cyber-warfare-arena-and-the-construction-of-a-training-arena-in-New-York>

Strategic Cyber Holdings LLCのボードメンバー

役職	氏名	主な兼職
Chairman of the Board & CEO	石原 紀彦	当社代表取締役社長
Board member	Ofir Hason	サイバージム社 CEO
Board member	五十嵐 雅人	当社取締役管理本部長
Board member	遠藤 典子	株式会社NTTドコモ社外取締役
Board member	Yosi Shneck	イスラエル電力公社 Senior Vice President Information, Security and Communication Group サイバージム社 Chairman of Steering Committee



Ofir Hason氏
CyberGym Control Ltd.のCEO
<https://www.cybergym.com/ja/company/>



遠藤 典子 氏
株式会社NTTドコモ（東証一部）取締役。
https://www.nttdocomo.co.jp/corporate/about/outline/endo_noriko.html

株式会社アインホールディングス（東証一部）社外取締役。
<https://www.ainj.co.jp/about/group.html>



Yosi Shneck氏
イスラエル電力公社 Senior Vice President Information
<https://www.iec.co.il/en/pages/default.aspx>

サイバージム社 Chairman of Steering Committee
<https://www.cybergym.com/ja/company/>

サイバー攻撃やコンピューターテクノロジーで40年以上の経験
<http://asia.cybertechconference.com/node/1228>

2018年2月19日 Forbes JAPANの記事

イスラエル8200部隊出身の起業家が描く「サイバークリッド構想」

<https://forbesjapan.com/articles/detail/19798/1/1/1/1/1>

世界で最もサイバー攻撃を受けているイスラエル電力公社「IEC」。同社の経験を生かして創業したのが、サイバー防衛のトレーニング企業「CyberGym（サイバージム）」である。

同社はイスラエルをはじめ、ヨーロッパ各国にサイバーアリーナと呼ばれる訓練施設を設置している。2017年11月にはオーストラリアにも開設。17年末には南アフリカ、18年にはアメリカおよび日本での開設を予定しており、世界中のタイムゾーンに拠点を持つ計画だ。グローバルなサイバー防衛ネットワーク「CyberGrid（サイバークリッド）」の構築を進めている。

今回、サイバージムを立ち上げたオフィール・ハソンCEOにイスラエルのサイバーセキュリティ事情、そして「サイバークリッド」の意義について聞いた。

—日本でもサイバー攻撃に対する危機意識は高まっている。20年夏季オリンピックを迎える前にできることは？

ハソン：オリンピックは世界中のハッカーが注目している。大会だけでなく、日本のインフラを攻撃しようとするだろう。まずはその意識で準備を進めることが必要だ。

世界中で起きているサイバー攻撃の状況把握やパターンの解析、実際の事例に触れてみることで意識は向上する。それを戦略的な行動に移し、組織として備えるべき。セキュリティ担当者だけでなく、一般従業員、経営陣それぞれの責任範囲を明確化することが重要だ。

—「サイバークリッド構想」では、トレーニングに加え、各サイバーアリーナを連携させ、情報の収集・発信を行うという。その狙いとは？

ハソン：重要なのは敵を知ること。攻撃の動機、それは個人情報やIP（知的財産）の獲得、システムに損害を与えて会社の評判を傷つける、などさまざまだ。

サイバー攻撃から自社のシステムや資産を守るソリューションは多数あるが、それは何もテクノロジーには限らない。実際、サイバー攻撃による被害の原因は95%以上が人的要因による。WannaCry（ワナクライ）やPETYA（ペトヤ）の例では、企業側が使っていたサイバー攻撃対策のテクノロジー自体に問題はなかった。担当者の対応が間違っていたわけでもない。

だが組織として対応する用意ができておらず、損害が大きくなった。攻撃を認識したときに取締役会でどのように意思決定するか、メディア対応をどうするかなど、準備が必要だ。ボクシングのように、日々のトレーニングやスパーリングは欠かせない。テクノロジーはサイバー攻撃の重要な一部だが、全部ではない。

—ハッカーは相手をどう攻撃するのか。

ハソン：ハッカーが企業をサイバー攻撃しようと思ったら、まずは企業の調査や、SNSを通じて意思決定者や技術者の略歴と特徴を調べるだろう。まず、彼らが何をしているかを学ぶことから始める。テクノロジーは調査した内容に基づき、攻撃する際の手段でしかない。

最初の重要なステップはテクノロジーではなく、人的要因。つまり、ファイアウォールをハッキングすることではなく、ターゲットを取り巻く“ソーシャルエンジニアリング”なのだ。

—具体的に取るべき対策とは？

ハソン：ふつうの人には、ハッカーの思考回路は理解できない。ただ彼らの考え方に従って訓練を積むことは可能だ。

顧客はトレーニングを通じて、ハッカーが次に何を仕掛けてくるかを予測できるようになる。我々の顧客は、ワナクライやペトヤなどのサイバー攻撃では被害を受けていない。すべて組織として防御できている。

私たちはサイバー攻撃の発生後、72時間以内に実際のコードを解析し、トレーニングメニューを用意する。だから顧客は何をすべきか分かるのだ。

—サイバグリッド構想は、それを世界レベルに広げたものなのか。

ハソン：サイバグリッドを通じて世界中のタイムゾーンでの情報アクセスを可能にすることで、レスポンス時間の短縮に努めている。そのため、日本にもトレーニング施設を開設する予定だ。イスラエルの経験を生かし、日本市場に我々のソリューションを提供する。

損害の要因となる人的要因を最小化するためには、人材のトレーニングが最も効果的だ。ROI（投資利益率）を考えても、サイバー攻撃による実際の被害への対応をしたり、防御プロダクトを導入することのみで準備したりするより、人材を訓練した方が投資効率はよい。

最近、ニュアンスという会社がサイバー攻撃で、1億500万ドルの被害を受けた。我々のトレーニングはそんなにはかからない。トレーニングはコストではなく、投資と考えるべきなのだ。

オフィール・ハソン◎イスラエルのサイバーセキュリティ企業「CyberGym」の共同創業者兼CEO。イスラエル国防軍のサイバー攻撃・防御の精鋭部隊である8200部隊出身。イスラエル政府NISA（National Information Security Authority）で経験を積みサイバーセキュリティ関連の会社を2度起業した後、2013年にイスラエル電力公社とCyberGymを創業した。

2018年2月21日

当社連結子会社による株式会社アクロホールディングスとの業務提携に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1559570/00.pdf>

当社連結子会社であるバルク社は、主要事業として情報セキュリティ等のコンサルティング事業を展開しており、プライバシーマーク認定取得やISO27001 認証取得に関する支援等を中心として、情報セキュリティ体制の構築やサイバーセキュリティを含む情報セキュリティ等に関するコンサルティングサービスを提供しております。特に、プライバシーマーク認定取得のコンサル

ティングにおいては国内トップクラスの1,800件以上の支援実績を有し、業界のリーディングカンパニーとなっております。

一方で、アクロ社は、傘下や出資先に50社を超えるIT企業を有しているほか、多数のIT企業向けに様々な経営支援を行っており、アクログループ間における緊密な連携とその広範なネットワークを活かした多様なITソリューションの提供や営業支援等を強みとしております。

AI・IoT・ビッグデータなどの利活用が拡大し、セキュリティリスクが急速に高まるなかで、IT及びセキュリティへの対応は企業経営における最重要課題となっており、このたびの業務提携によって、相互の顧客に対して、より付加価値の高いIT・セキュリティソリューションを提供することが可能となるとともに、営業協力等の各種協業を行うことで、双方の業績向上と事業のさらなる発展が期待されることから、両者間において本業務提携について合意に至りました。

2018年4月9日

(開示事項の変更・経過)CyberGym Control Ltd.との共同事業及び追加ファイナンスの状況に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1571207/00.pdf>

前回開示におきましては、サイバージムからのNYコマーシャルアリーナー式購入資金及び事業運営資金を用途としたSCH社における追加ファイナンスを2018年3月末を目途に実施する予定としておりましたが、SCH社の事業戦略に関する最適なストラクチャーの協議・検討が完了し、具体的な内容が決定した段階で速やかに開示いたします。

なお、2018年6月頃を予定しているSCH社によるNYコマーシャルアリーナの開設・サービス開始日に関しては、追加ファイナンスの実行の有無にかかわらず、NYコマーシャルアリーナー式の購入資金及び当初の事業運営資金につき一時的に当社の自己資金で賄うことも可能な状況であることから、現時点において変更はありません。

→このIRで株価が231円(4/9終値)から901円(4/19終値)まで高騰。NYコマーシャルアリーナでのサイバーセキュリティトレーニング事業への期待。

2018年4月19日

主要株主である筆頭株主の異動に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1573608/00.pdf>

村松澄夫氏が1,210,000株を一部売却し、現在は989,000株(第三位)

西澤管財株式会社が1,000,000株(筆頭株主)。また代表取締役の西澤岳志氏はバルクホールディングスの社外取締役である。

<http://www.kabupro.jp/edp/20180418/S100CT65.pdf>

4/12、4/19の出来高が100万株を超えた。

2018年5月18日

イスラエル大手ベンチャーキャピタル Vertex Ventures Israel ゼネラルパートナーのデイビッド・ヘラー氏(Mr. David Heller)が当社米国子会社SCHのアドバイザリーボードメンバーに就任

<http://www.vlcholdings.com/wp/wp-content/uploads/2018/05/PR20180518.pdf>

このたびSCH社のアドバイザリーボードメンバーに就任したデイビッド・ヘラー氏(Mr. David Heller)は、イスラエル大手ベンチャーキャピタルVertex Ventures Israelのゼネラルパートナー

を務めております。ヘラー氏は、これまで20年以上に渡って日本の企業や投資家とイスラエルのハイテク企業の架け橋としての役割を担って参りました。

Vertex Ventures Israelが投資活動を行うイスラエルでは、米国のシリコンバレー同様に革新的な発想や技術をもつ先進的な企業が数多く生まれており、世界的な企業がR&Dの中心的な開発拠点を同国に開設しております。特にサイバーセキュリティ分野、バイオテック分野などのハイテク分野の技術に定評がありますが、同社はその中でもサイバーセキュリティを注力分野の一つとしており、2017年にはその実績を高く評価され、



Geektime 2017 Reportにおいて、イスラエルのサイバーセキュリティ投資におけるリーディング・インベスター1位にランクされました。

Vertexはこれまで、2014年にNASDAQに上場したCyberArk(CYBR)、2017年11月にContinentalが買収したArgus Cyber Security、2017年2月にPalo Alto Networksが買収したLightCyberにおいて、最初の投資家としてその成長に貢献し、それ以外にもIndegy、Cylus、Axoniusといったサイバーセキュリティ企業に積極的に出資をしております。

ヘラー氏のアドバイザリーボード参加により、同氏の当該分野での幅広い知見やイスラエルでのテクノロジー企業とのネットワークが、サイバーセキュリティトレーニングをはじめとする様々なサイバーセキュリティソリューションの提供において、サービス・製品の付加価値向上に資するものと確信しております。当社グループとしては、サイバージム社と連携し、サイバーアリーナをプラットフォームとした上で、イスラエル企業をはじめとする世界の最先端技術を常に模索し、お客様をサイバー攻撃から全力で守るべく、最適なサイバーセキュリティソリューションの提供を目指します。

■デイビッド・ヘラー氏(Mr. David Heller)プロフィール

イスラエルの大手ベンチャーキャピタル、Vertex Ventures Israelのゼネラルパートナー。日本の投資家向けのイスラエルで最初のベンチャーキャピタルファンドの設立及び運営の経験も持ち、イスラエル国内外でベンチャーキャピタル投資の分野で20年以上にわたり広範囲に活躍。エルサレムのヘブライ大学で法学士を取得後、イスラエルでは、法律事務所のパートナーとして、M&A取引を専門とし、アジア関連の取引担当を務めた。また、京都大学で法学修士を取得後、日本の弁護士事務所にも在籍。

※WCWA(World Cyber Warfare Arena)

WCWAは、世界中の専門家から継続的にサイバーセキュリティの情報収集を行い、知識、トレーニング、防衛方法をメンバーに対して提供するグローバルネットワークです。メンバーは、WCWAに接続することで、知識と技術のギャップを埋めることができます。WCWAには、今後、さまざまな規模の企業、政府機関、研究機関、学術機関およびスタートアップ企業などの参加が見込まれております。また、SCH社が米国ニューヨーク州に設立するサイバーアリーナは、イスラエルやオーストラリアのアリーナと同様に多業種向けのサービスを配備する最大規模のアリーナとなり、世界各地をつなぐサイバージムのWCWAに最重要拠点の一つとなる予定です。

David Heller

<http://www.vertexventures.co.il/team/>

Vertex Ventures Israel
<http://www.vertexventures.co.il>

2018年5月29日

取締役及び監査役選任議案並びに監査役の辞任に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1594191/00.pdf>

2018年6月8日

『Jupiter(ジュピター)プロジェクト』を主宰するビーオービー株式会社とのサイバーセキュリティ分野における業務提携に関するお知らせ

<http://www.vlcholdings.com/wp/wp-content/uploads/2018/06/PR20180608.pdf>

BOB社は、企業のセキュリティインシデントを防ぐべく、人工知能(AI)を活用したサイバー攻撃からの防御、内部情報漏洩を自動的に防ぐ仕組み、高い匿名性と防御力を持った独自のブロックチェーンといった3つの独自の技術を包括的に組み合わせ、企業や公的機関に高度なセキュリティソリューション「ジュピターセキュリティ」を提供するために、「Jupiter(ジュピター)プロジェクト※」を立ち上げ、各界の有識者と共同で推進しております。

当社としては、本業務提携を通じて、ブロックチェーン業界における情報共有及びサイバーセキュリティに対する意識やリテラシーの向上といった啓蒙を行うとともに、同業界へのサイバーセキュリティソリューションの提供が期待できるものと考えております。また、BOB社においても当社グループ及びパートナーが有するサイバーセキュリティのノウハウと技術を採用することで事業強化や競争力の強化を期待しております。

今後、両者間の協業や人材交流を通じて、最適な相互協 なお、ジュピタープロジェクトにおける、当社グループといたしましては、あらゆる環境において“お客様をサイバークライムから守る”力関係を構築してまいります。

開発、製造、販売、人材戦略に至るまで幅広い見地に対応したサイバーセキュリティチームのアドバイザーとして、当社代表の石原紀彦が参画する予定です。

3. 業務提携の相手先の概要

- (1) 名称 ビーオービー株式会社（英文表記：BOB inc.）
- (2) 所在地 東京都千代田区丸の内 2-3-2 郵船ビルディング 1 階
- (3) 代表者の役職・氏名 代表取締役 澤田 幸人
- (4) 設立年月日 2017 年 11 月 9 日
- (5) 事業内容
 - ◆経営支援
 - ◆サイバーセキュリティ
 - ◆システム開発
 - ◆仮想通貨に関するコンサルティング
- (6) 資本金 1,100 万円
- (7) 当社との関係 資本関係、人的関係、取引関係はありません。また、関連当事者への該当事項もありません。
- (8) URL <https://www.bobinc.jp/>

Jupiter(ジュピター)プロジェクト公式サイト

<http://jupiter-ico.com/japanese/>

Jupiter(ジュピター)プロジェクトの詳細

<https://hyip-information.com/ico/>

<https://hyip-information.com/ico/%e3%82%b8%e3%83%a5%e3%83%94%e3%82%bf%e3%83%bcjupiter%e3%81%ae%e4%bb%ae%e6%83%b3%e9%80%9a%e8%b2%a8ico%ef%bc%81%e5%a4%8f%e9%a0%83%e4%b8%8a%e5%a0%b4%e4%ba%88%e5%ae%9a%ef%bc%81%e5%86%85%e5%ae%b9/>

2018年6月12日

第24期 定期株主総会招集ご通知

<https://ssl4.eir-parts.net/doc/2467/tdnet/1600116/00.pdf>

株式会社ソフトブレン（東証一部上場）の元代表取締役の松田 孝裕氏が新任した。

<http://www.softbrain.co.jp>

13年に渡り企業価値向上アドバイザーを行なっているTanaakk株式会社の代表取締役の田中 翔一朗氏が新任した。

<http://tanaakk.co.jp>

→これらのIRで、株価631円（5/29終値）から1848円（6/14最高値）に高騰。新任役員への期待。

2018年6月15日 日本産経新聞の記事

イスラエル電力公社が東京五輪に向けて日立製作所などの日本企業に技術者を派遣

<https://www.sankei.com/world/news/180615/wor1806150010-n1.html>

2012年のロンドン五輪では2億回を超えるサイバー攻撃を受けており、マルウェアは現在では毎週300～500個も開発されている。

2018年6月15日

当社子会社Strategic Cyber Holdings LLCによる日本第1号のハイブリッドアリーナのオープンに関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1602303/00.pdf>

このたび、サイバージムとの共同事業について、日本市場における本格展開を図るため、米国子会社SCHがサイバーセキュリティトレーニングサービスの提供拠点として、日本第1号のハイブリッドアリーナ※2 を開設することとなりました。本アリーナでは、経営層に対するワークショップや、顧客のオペレーション環境、技術環境に応じてカスタマイズされたハンズオントレーニングの受講が可能となります。

当施設でのサイバーセキュリティトレーニングサービスの提供を通じて、日本企業が日々増大するサイバー攻撃に対処するための適切な組織構築を支援いたします。

<名称> CyberGym Tokyo

<所在地> 東京都港区赤坂 1 丁目 14 番地 11 号 HOMAT ROYAL 1F

<オープン日> 2018年8月1日(水曜日)

※1 **コマーシャルアリーナ** 重要インフラストラクチャーの複数セクターを対象とするサイバーセキュリティトレーニングのフルパッケージサービスを提供する大型のトレーニング施設となります。コマーシャルアリーナ内には、対象セクターに対応する複数の模擬施設、ハードウェア及び専用ソフトウェアなどが構築され、サイバーセキュリティのスペシャリストで構成される攻撃側の RED TEAM や防衛側をサポートする WHITE TEAM などが配備されます。

※2 **ハイブリッドアリーナ** 主に顧客の社内又は設備内に設置される小型のサイバーセキュリティトレーニング施設です。WHITE TEAM が配備され、主な設備はハードウェア及び専用ソフトウェア等となります。なお、RED TEAM によるサービスは、コマーシャルアリーナからリモート提供されます。

2018年6月25日

第三者割当による第3回新株予約権(行使価額修正条項付)及び第4回新株予約権(行使価額修正選択権付)並びに無担保社債(私募債)の発行に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1603589/00.pdf>

マッコーリー・バンク・リミテッド(以下、「割当予定先」といいます。)を割当先とする第三者割当の方法による第3回及び第4回新株予約権(以下、総称して「本新株予約権」といいます。)並びに無担保社債(私募債)(以下、「本社債」といいます。)の発行を行うことを決議いたしましたので、お知らせいたします。

[新株予約権]

- ・割当日 平成30年7月11日
- ・発行株数 1,490,000株
- ・行使価格修正条件 前取引日の終値の90%の価格
- ・希薄化率 19.88% 発行済株式総数7,494,000株を分母とする

[無担保社債]

- ・社債の総額 250,000,000円
- ・振込期日 平成30年7月11日
- ・償還期日 平成31年7月10日(満期一括償還)
- ・利率 付さない。

[募集の目的]

当社は、サイバーセキュリティトレーニングサービス等のサイバーセキュリティ分野における共同事業を行うことについて、イスラエルの同分野におけるリーディングカンパニーである Cyber Gym Control Ltd.社(以下、「サイバージム社」といいます。)との間で、平成29年11月9日付で基本合意し、同12月22日付で独占的ライセンス契約を締結しました。その後、本共同事業のために平成30年1月31日付でサイバージム社との共同事業会社として、米国に当社子会社 Strategic Cyber Holdings LLC(以下、「SCH」といいます。)を設立し、各種サイバーセキュリティトレーニングアリーナの運営準備やマーケティング活動を共同で推進しております。本共同事業の遂行において、平成30年6月25日付「(開示事項の経過)CyberGym Control Ltd.との共同事業及び追加ファイナンスの状況に関するお知らせ」に記載のとおり、SCHが米国NY州に開設するコマーシャルアリーナ一式の購入資金の一部、及び新設会社であるSCHにおいて事業基盤が確立され、安定的に収益を獲得できるようになるまでの運転資金として、当社はSCHに対して出資及び融資による資金支援を行う予定です。

[調達資金の融資]

当社は、本社債の発行により調達する250百万円に本新株予約権の行使による調達額50百万円を加えた300百万円を、サイバージム社との共同事業会社として平成30年1月に米国に新設した当社子会社SCHに対して、追加出資として約165百万円、貸付金として約135百万円の資金支援を行う予定です。

当社グループといたしましては、M&A及び資本・業務提携に関わる資金・費用として、過去5年間の実績金額及び検討案件における1件あたりの金額が数千万円から数億円であったことを踏まえ、3件から8件程度の複数案件向けの資金・費用として1,017百万円を充当する予定です。

→このIRで、株価1070円(6/25終値)から657円(6/27終値)まで下落。株の希薄化を懸念した個人投資家の売りだと思われる。

2018年6月25日

(開示事項の経過) **CyberGym Control Ltd.との共同事業及び追加ファイナンスの状況に関するお知らせ**

<https://ssl4.eir-parts.net/doc/2467/tdnet/1603590/00.pdf>

SCHによる「CyberGym NYC」のサイバージムからの取得資金500万米ドルの未払い残代金128万米ドル(支払済みの222万米ドルと納入元であるサイバージム社による現物出資分の150万米ドルを除いた金額)とSCHの事業基盤が確立され、安定的に収益を獲得できるようになるまでの運転資金について、当社の自己資金に加え、当社が資金調達を行うことで、これをSCHに追加出資及び融資することといたしました。

2018年6月27日

主要株主の異動に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1605908/00.pdf>

株式会社MH capitalが992,000株(3/31時点)→754,100株(6/19時点)→503,000株(6/28時点)に減少させ、松村邦夫、西澤管財株式会社、JPcapital株式会社に続き第4位になった。

→6/6、6/12～6/29までの平均の出来高は100万株を超えた。

<https://96ut.com/stock/jikei.php?code=2467&year=2018>

2018年7月2日

2018年3月期 有価証券報告書

https://ssl4.eir-parts.net/doc/2467/yuho_pdf/S100DK8R/00.pdf

2018年7月4日

コーポレート・ガバナンスに関する報告書

<https://ssl4.eir-parts.net/doc/2467/tdnet/1607895/00.pdf>

コーポレートガバナンス・コードの基本原則を全て実施しております。

外国人持ち株比率10%未満

2018年7月19日

サイバーセキュリティ分野における業務提携先であるCyberGym Control Ltd.への出資に向けた基本合意書締結に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1611588/00.pdf>

当初方針を変更し、SCHへの当社の出資比率を維持するため、資金支援は当社が直接行うこととなりました。SCHの持分比率は、現時点で当社が100%となっておりますが、サイバージムが30%分の持分取得オプションを保有しているため、当社によるSCHへの追加出資が完了しサイバージムが持分取得オプションを行使した段階で当社が70%、サイバージムが30%となる予定です。

また、上記方針変更に伴い、その必要資金を確保するため、2018年6月25日付「第三者割当による第3回新株予約権(行使価額修正条項付)及び第4回新株予約権(行使価額修正選択権付)並びに無担保社債(私募債)の発行に関するお知らせ」(以下、「2018年6月25日付ファイナンス開示」)に記載のとおり、同年7月11日を払込日として当社においてファイナンスを実施いたしました。

2018年7月19日

サイバーセキュリティトレーニング施設「CyberGym NYC」本日ニューヨークにオープン!

<http://www.vlcholdings.com/wp/wp-content/uploads/2018/07/PR20180719.pdf>

このたび、SCHを主体として、開設準備を進めてまいりましたサイバーセキュリティトレーニング施設「CyberGym NYC」をニューヨークに開設する運びとなり、このオープンを記念いたしまして、7月18日(米国時間)に、米国内外から多くの主要関係者や政府関係者にご出席いただき、テープカットセレモニー、サイバーアリーナの内覧会およびカクテルパーティを執り行いました。

内覧会では、実際のサイバー攻撃が体験可能なサイバーアリーナ内の説明や最先端の技術を使用した設備についてご説明させていただきました。



当社代表兼 SCH 代表の石原紀彦と来賓の方々とのテープカットシーン



ニューヨークのトレーニング施設 (SOC Room, Classroom, Red Room)



2018年8月10日

クリプトアセットアドバイザー事業を目的とする子会社設立に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1623327/00.pdf>

当該新設子会社では、ブロックチェーン技術を用いて独自の経済圏を確立し、企業価値を向上する手法(クリプトエコノミクス)に着目し、暗号技術および分散型台帳技術を用いた経済圏の確立手法に関するデータおよびノウハウを蓄積すると同時に、クリプトアセットを管理するうえで不可欠となるサイバーセキュリティへの対策に関して、当社が業務提携しております CyberGym Control Ltd. (以下「サイバージム社」)との連携により、ブロックチェーン応用システム、仮想通貨交換業者およびコールドウォレット提供事業者、ICO事業者※5 に対してサイバー・フィジカル・セキュリティ対策ソリューションを提供する計画です。

→旬な材料である仮想通貨、ブロックチェーン関連の新設子会社のIRだったが、第1四半期決算短信が良くなかったこともあり、株価にはあまり影響せずだった。

2. 新設子会社の概要

(1)名称	CEL LTD. (Crypto Economics Lab)	
(2)所在地	未定	
(3)代表者の役職・氏名	Chairman of the Board&CEO 田中翔一郎 (当社取締役)	
(4)事業内容	・クリプトアセットにかかわるサイバーセキュリティリスクに関するアセスメント及びトレーニング、コンサルティング、モニタリングサービスの提供 ・クリプトアセットを活用した企業価値向上アドバイザー	
(5)資本金	未定	
(6)決算期	3月31日	
(7)設立年月日	2018年9月中(予定)	
(8)持分比率	当社100%	
(9)当社と当該子会社との関係	資本関係	当社の100%出資子会社となります。
	人的関係	当社取締役が当該子会社の代表者を、当社代表取締役石原紀彦及び取締役五十嵐雅人が当該子会社の Board Member を兼任する予定であります。
	取引関係	新設会社のため該当事項はありません。

3. 経営体制(予定)

当該新設子会社の代表者には当社取締役の田中翔一郎が就任し、当社業務提携先であるサイバージム社 CEO の Ofir Hason 氏もボードメンバーに参加する予定であります。

役職	氏名	主な兼職
Chairman of the Board & CEO	田中 翔一郎	当社取締役
Board member	石原 紀彦	当社代表取締役社長
Board member	五十嵐 雅人	当社取締役管理本部長
Board member	Ofir Hason	CyberGym Control Ltd. CEO

2018年8月10日

2019年3月期 第1四半期決算短信(日本基準)(連結)

<https://ssl4.eir-parts.net/doc/2467/tdnet/1623328/00.pdf>

2018年8月13日

2019年3月期 第1四半期報告書

https://ssl4.eir-parts.net/doc/2467/yuho_pdf/S100DXQR/00.pdf

当第1四半期連結会計期間から、コア事業の明確化等を目的として、報告セグメントの名称をコンサルティング事業からセキュリティ事業に変更しており、以下の前年同四半期比較及び分析については、変更後の区分に基づいて記載しております。

また、当第1四半期連結会計期間より、サイバージム社との共同事業会社である子会社 Strategic Cyber Holdings LLC(以下、「SCH社」)を連結の範囲に含めております。当社の決算月3月に対してSCH社の決算月は12月であり、仮決算を行わずに連結することから、SCH社の業績は概ね3ヶ月遅れで当社の連結業績に反映されます。

2018年8月30日

サイバーセキュリティ分野における業務提携先であるCyberGym Control Ltd.への出資に係るクロージングに関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1626763/00.pdf>

本日付でクロージングプロセスが完了いたしましたので、お知らせいたします。

また、当社代表取締役社長の石原紀彦がサイバージムのアドバイザリーボードメンバーに就任しCyberGym Control Ltd.の経営に参画いたします。

本件出資により、当社とサイバージム間の連携関係はさらに強化されますが、当社は同社との強固な連携をベースにサイバーセキュリティ分野における事業拡大を推進いたします。

2018年9月3日

(開示事項の経過)クリプトアセットアドバイザリー事業を目的とする子会社設立に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1627537/00.pdf>

公表いたしましたとおり、本日付でクリプトアセットアドバイザリー事業を主な目的とする子会社を設立いたしましたので、下記の通りお知らせいたします。

1. 新設子会社の概要

(1)名称	株式会社 CEL (CEL LTD.) ※
(2)所在地	東京都港区赤坂一丁目 14 番 11 号
(3)代表者の役職・氏名	代表取締役社長 田中翔一郎
(4)主な事業内容	・クリプトアセットにかかわるサイバーセキュリティリスクに関するアセスメント及びトレーニング、コンサルティング、モニタリングサービスの提供 ・クリプトアセットを活用した企業価値向上アドバイザー
(5)資本金	30,000 千円
(6)決算期	3月31日
(7)設立年月日	2018年9月3日
(8)出資比率	当社 100%

※CELはCrypto Economics Labの略称です。

役職	氏名	主な兼職	四半期純利益			
			2019年3月期	2018年3月期	2019年3月期	2018年3月期
代表取締役社長	田中 翔一郎	当社取締役				
取締役	石原 紀彦	当社代表取締役社長				
取締役	五十嵐 雅人	当社取締役管理本部長				
監査役	奥山 琢磨	当社常勤監査役				
アドバイザーボードメンバー	Ofir Hason	CyberGym Control Ltd. CEO				

(2) 連結財政状態

	総資産		純資産		自己資本比率	1株当たり純資産
	百万円	百万円	百万円	百万円	%	円 銭
2019年3月期第1四半期	1,000	691	690	714	69.0	92.10
2018年3月期	962	714	713		74.1	95.19

(参考) 自己資本 2019年3月期第1四半期 690百万円 2018年3月期 713百万円

2018年9月10日

サイバートラスト株式会社との協業に係る合意書締結に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1628918/00.pdf>

本日付でサイバートラスト株式会社(本社:東京都港区、代表取締役社長 眞柄泰利、以下「サイバートラスト社」とサイバーセキュリティ分野における協業に係る合意書を締結いたしましたので、下記の通りお知らせいたします。

当社グループといたしましては、本件協業により、サイバートラスト社を通じて同社の顧客向けにサイバーセキュリティトレーニングを中心とした各種サイバーセキュリティサービスの提供を目指すとともに、サイバートラスト社への直接のサービス提供も期待しております。これに加え、当社グループの顧客向けソリューションにサイバートラスト社の技術・サービスを組み合わせることで、サービスの拡充や攻撃の検知から防御・対策までの一貫した迅速なサービス提供など、当社グループソリューションの付加価値をさらに高めることが可能となります。

また、両者の保有する人材・技術・ノウハウ等の経営資源を活かすことで、サイバー脅威に対してよりの確に対処するための組織的なソリューション開発も推進して参ります。

※サイバートラスト株式会社(非上場会社)はソフトバンク・テクノロジー株式会社が74.5%保有する子会社であり、ソフトバンク・テクノロジー株式会社はソフトバンク・インターナショナル合同会社が54.26%保有する子会社である。

3. 相手先の概要

(1) 名称	サイバートラスト株式会社	
(2) 所在地	東京都港区六本木一丁目9番10号	
(3) 代表者の役職・氏名	代表取締役社長 眞柄 泰利	
(4) 設立年月日	2000年6月1日	
(5) 事業内容	IoT事業、Linux/OSS事業、認証・セキュリティ事業	
(6) 資本金	4億7,008万円	
(7) 大株主及び持株比率	ソフトバンクテクノロジー株式会社 74.5%	
(8) 当社との関係	資本関係	該当事項はありません。
	人的関係	該当事項はありません。
	取引関係	該当事項はありません。
	関連当事者への該当状況	該当事項はありません。
(9) URL	https://www.cybertrust.co.jp/	

https://www.softbanktech.co.jp/-/media/corporate/corp/pdf/ir/upload_file/library_03/4726_yh201803_4q.pdf?la=ja-JP&rev=64b16662b08c449185643d7369a281b0

2018年9月12日

革新的エンドポイントセキュリティ製品「AppGuardR」の取扱い開始に関するお知らせ

<https://www.vlcan.com/wsys/wp-content/uploads/2018/09/0b816114f0eb536a6fb4f1cb27839d45.pdf>

当社は、PCIホールディングス株式会社の子会社である Safer Connected World 株式会社(本社:東京都、代表者:代表取締役 原口直道、以下「SCW 社」といいます。)とリセラー契約を締結し、同社の販売するエンドポイントセキュリティ製品「AppGuardR(アップガード)」の取扱いを開始いたしました。

このたび提供を開始する「AppGuardR」は、“システムの正しい動作と機能をまもること”を目的とした新概念のセキュリティ製品であり、米国の政府機関で使用され、18年以上破られていないという実績を有しています。マルウェア自体※の検出・駆除による攻撃を防止する従来のセキュリティ製品とは異なり、“システムへの動作を監視・隔離すること”で、課題となっている未知のマルウェアへの対策も解決し、サイバー攻撃から企業を守ることを可能にする製品です。

当社では「AppGuardR」をセキュリティソリューションの一部に加えることで、既存の情報セキュリティコンサルティングサービスの提供先を含むセキュリティ意識の高い、大企業から中小企業までの幅広い顧客向けに、よりセキュアな環境を提供してまいります。

※:マルウェア 不正かつ有害に動作させる意図で作成された悪質なソフトウェアやコードの総称(コンピュータウイルス・ワームなど)

▶AppGuardを提供しているBlue Planet-works社

<https://www.blueplanet-works.com/contents/solution/>

▶AppGuardは、内閣サイバーセキュリティセンター (NISC)「政府機関等の対策基準策定のためのガイドライン」に適合した製品

<https://www.blueplanet-works.com/contents/news/detail.html#/posts/126>

■契約相手先の概要

- (1) 名称 Safer Connected World 株式会社
- (2) 所在地 東京都港区虎ノ門1-21-19 東急虎ノ門ビル5階
- (3) 代表者の役職・氏名 代表取締役 原口 直道
- (4) 設立年月日 2018年6月1日
- (5) 事業内容
 - 「AppGuard®」および関連製品ならびに付帯サービスの提供
- (6) 資本金 1,000万円
- (7) 株主 PCIホールディングス株式会社(東証一部、コード3918) 90%
株式会社Blue Planet-works 10%
- (8) URL <https://ag.safercw.co.jp/>

2018年10月9日

主要株主の異動に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1634224/00.pdf>

JPcapital株式会社は2014年以前より900,000株を長期保有していた第四位の主要株主であったが、9月30日時点で保有株式を0株にした。

→このIRを受けて、708円(10/9終値)だった株価が翌日には660円(10/10安値)まで下落。

2018年10月15日 (CyberGYMのIR)

《満席につき受付終了》サイバーセキュリティトレーニング『Cyber Defense Essentials 2 days -supports hybrid-』を開催します (11/20・21)

<http://cybergym.tokyo/89/>

CYBERGYM TOKYOにおきまして、『Cyber Defense Essentials 2 days -supports hybrid-』を開催します。

ハンズオンの時間を多く設けたトレーニングを1名様からお申込みいただける集合型の日程をご用意しました。

当日はイスラエルのホワイトチームが来日しての直接指導、およびイスラエルのレッドチームとリアルタイムで繋ぎ実際に最先端のサイバーアタック攻防を実体験していただけます。

《トレーニング概要》

日時：2019年11月20日(火)・21日(水) 9:30~17:30

場所：東京都港区1-14-11 CYBERGYM TOKYO アリーナ

費用：250,000円/1名

2018年10月19日

サイバージム社CEOのオフィール・ハソンが一般社団法人 日本経済団体連合会の『サイバーセキュリティに関する懇談会』にて講演いたしました

<https://www.vlcholdings.com/wp/wp-content/uploads/2018/10/PR20181019.pdf>



『サイバーセキュリティに関する懇談会』の様子

2018年10月26日

サイバージム社『Spy Chip Hack』攻撃に対するセキュリティトレーニングを開発

<https://www.vlcholdings.com/wp/wp-content/uploads/2018/10/PR20181026.pdf>

サイバーセキュリティ分野における共同事業パートナーであるイスラエルCYBERGYM(サイバージム)社は、高度なフォレンジック分析と報告された攻撃シナリオの複製品を利用し、サプライチェーンとインフラストラクチャのセキュリティに関する不安を解決するトレーニングソリューションの提供を開始いたします。

このトレーニングプログラムは、某国の諜報機関が、AppleやAmazonなどの世界的に重要な民間インフラストラクチャ企業や米軍や米諜報部隊において使用されているサーバーに監視チップをインストールしたというメディアの主張に応じて開発されたものです。

ハッカーによるこの攻撃は、ハードウェアサプライチェーン内のサプライヤを通して実施されたという点が重要であり、この点を考慮し、サイバージムのイスラエルR&Dセンターでは、複雑なハードウェアベースの攻撃に対して防御する効果的な戦略を組織に提供するトレーニングプログラムを開発いたしました。

2018年10月30日

GFX Cross-Loyalty Network Officially Launches, Rewards Members with Registration Incentives

<https://www.media-outreach.com/release.php/View/7077#Contact/>

GFX Cross-Loyalty Networkが登録インセンティブを持つメンバーに報酬を与えると正式発表

報酬についての説明動画

http://m.youku.com/video/id_XMzg5NDYzNjQ4OA==.html?spm=a2h3j.8428770.3416059.1&source=https%3A%2F%2Fwww-businessinsider-sg.cdn.ampproject.org%2F



2018年10月31日

ジュピタープロジェクト株式会社との業務提携解消に関するお知らせ

<https://www.vlcholdings.com/wp/wp-content/uploads/2018/10/PR20181031.pdf>

イスラエルのサイバージム社を中心とするアライアンス先との連携を通じたセキュリティ・ソリューションの開発やサービス内容が具体化する中で、当社グループのブロックチェーン関連セキュリティ事業におけるアライアンス戦略の最適化をはかる必要性等が生じたことから、本業務提携を解消することといたしました。

これに伴い、当社は、本業務提携契約の定めに従い、翌11月末日を解約日とする解約通知書をジュピター社に対して本日付で提出いたしました。

2018年11月1日 (CyberGYMのIR)

《満席につき受付終了》サイバーセキュリティトレーニング『Cyber Defense Essentials 2 days -supports hybrid-』を開催します (12/25・26)

<http://cybergym.tokyo/68/>

CYBERGYM TOKYOにおきまして、『Cyber Defense Essentials 2 days -supports hybrid-』を開催します。

ハンズオンの時間を多く設けたトレーニングを1名様からお申込みいただける集合型の日程をご用意しました。

当日はイスラエルのホワイトチームが来日しての直接指導、およびイスラエルのレッドチームとリアルタイムで繋ぎ実際に最先端のサイバーアタック攻防を実体験していただけます。

《トレーニング概要》

日時：2019年12月25日 (火) ・26日 (水) 9:30~17:30

場所：東京都港区1-14-11 CYBERGYM TOKYO アリーナ

費用：250,000円/1名

2018年11月9日

当社子会社である株式会社バルクと株式会社ソリトンシステムズとの情報セキュリティ分野におけるパートナー契約の締結に関するお知らせ

https://www.vlcholdings.com/wp/wp-content/uploads/2018/11/PR20181109_1.pdf

株式会社バルクは、プライバシーマーク認定取得やISO27001認証取得に関する支援等を中心として、情報セキュリティ体制の構築やサイバーセキュリティを含む情報セキュリティ等に関するコンサルティングサービスを提供しております。特に、プライバシーマーク認定取得のコンサルティングにおいては国内トップクラスの2,000件以上の支援実績を有し、業界のリーディングカンパニーとなっております。

一方で、ソリトンは、日本のITネットワーク黎明期から企業ネットワークの構築や、情報セキュリティ分野ではサイバーセキュリティ対策をはじめネットワーク制御や認証、クラウドサービス、情報漏洩対策などに関する自社製品群を開発し、国内、国外の企業にサービス提供する独立系メーカーです。

(3040)株式会社ソリトンシステムズ

<https://www.soliton.co.jp>

東証一部上場、時価総額194億円、前期売上164億円、事業内容は下記

セグメントの名称	主な営業種目	会社名
ITセキュリティ	<ul style="list-style-type: none">・情報漏洩対策、ログオン認証、アクセス制御、スパムメール対策、サイバーセキュリティ対策などの製品の開発・販売・スマートデバイスの業務利用の為にセキュリティ対策の構築・販売・企業向けクラウドサービス・企業向けネットワークインテグレーション・VoD(ビデオ・オン・デマンド)システムの構築・運用	当社 索利通ネットワークシステム(上海)有限公司 Soliton Systems Singapore Pte.Ltd Soliton Systems, Inc. Soliton Cyber & Analytics, Inc. Soliton Systems Development Center Europe AS, Gritech AS (株)オレガ (株)データコア Militus Inc.
映像コミュニケーション	<ul style="list-style-type: none">・モバイル回線による高品質のリアルタイム画像伝送システム「Smart-telecaster」の開発・販売	当社 Soliton Systems Europe N.V. (株)LaboLive
エコ・デバイス	<ul style="list-style-type: none">・アナログ・デジタル混合半導体デバイスの開発・販売・組み込み特殊処理エンジンの開発・販売	当社 Y Explorations, Inc

2018年11月9日

当社子会社である株式会社バルクが3000社以上の支援実績を節目として、2018年12月3日に「バルクユーザー会」を東京ドームホテルにて開催致します

https://www.vlcholdings.com/wp/wp-content/uploads/2018/11/PR_20181109.pdf

2018年11月12日

米国カリフォルニア州ロサンゼルス市におけるコマーシャルアリーナの開設に向けた基本合意書締結に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1648135/00.pdf>

当社子会社であるStrategic Cyber Holdings LLC(以下、「SCH」といいます。)は、米国現地時間2018年11月8日、当社グループの共同事業パートナーであり出資先でもあるCybergym Control Ltd.(本社:イスラエル、ハデラ市、共同創設者兼CEO:Ofir Hason(オフィール・ハソン)/以下、「サイバージム」といいます。)と共同で、重要インフラ向けサービスを提供する米国企業(本社:米国カリフォルニア州ロサンゼルス市)と、コマーシャルアリーナの販売及びサービス提供に関する基本合意書を締結いたしましたので、下記のとおりお知らせいたします。

(1) Sales agreement (先方とSCH間で締結)

コマーシャルアリーナの販売契約

(2) Licensing agreement (先方とサイバージム間で締結)

サイバージムの商標その他知的財産権の使用にかかる契約

(3) Service level agreement (先方とSCH及びサイバージムの三者間で締結)

年間のメンテナンス、サポート及びライセンスにかかる契約

※相手先の名称及び本件基本合意の詳細につきましては、守秘義務等により非開示とさせていただきます。 2.LA コマーシャルアリーナの概要

名称:CYBERGYM LA(仮称)

開設予定地:米国カリフォルニア州ロサンゼルス市内

3.今後の日程

(1) 本件基本合意書に係る SCH 取締役会決議日及び本件基本合意書締結日

2018年11月8日

(2) 最終契約締結日(予定)

2019年1月末までを目処

(3) CYBERGYM LA の設置(予定)

2019年中旬を目処

2018年11月13日

2019年3月期 第2四半期決算短信〔日本基準〕(連結)

<https://ssl4.eir-parts.net/doc/2467/tdnet/1649071/00.pdf>

セキュリティ事業において、業務提携先であるイスラエルの CyberGym Control Ltd.(以下、「サイバージム社」との共同事業において、サイバーセキュリティトレーニング施設として米国NY コマーシャルアリーナ※1(CYBERGYM NYC)を2018年7月に、東京ハイブリッドアリーナ※2(CYBERGYM TOKYO)を同年8月にそれぞれ開設し、サイバーセキュリティトレーニングサービスの提供を開始いたしました。

また、サイバージム社との本共同事業を推進するなかで、両者において本共同事業に対する戦略上の位置付けが高まり、サイバージム社との共同事業会社である子会社Strategic Cyber Holdings LLC(以下、「SCH社」)の資本政策を含む事業戦略に関する最適なストラクチャーについて十分な検討を行った結果、SCH社の資金支援等及びその他必要資金の確保を目的として、2018年7月にマッコーリー・バンク・リミテッドを割当先とする第三者割当による無担保社債及び新株予約権を発行いたしました。

このような状況のなか、サイバージム社において、グローバル戦略の強化及び事業拡大のための体制強化・人員 拡張、事業展開のための設備投資等を目的として、エクイティファイナンスによる資金調達を実施することとなり、引受先として主要パートナーである当社に対して打診があったことから、本共同事業の戦略的重要性やサイバーセキュリティ分野での事業展開におけるサイ

バージム社との連携強化の重要性に鑑み、当社は同年8月30日に500万米ドルを同社に出資いたしました。

その他、今後のグローバル経済のなかで重要な役割を担うことが期待される分散型台帳技術において、この技術に不可欠となるサイバーセキュリティへの対策に関して、サイバージム等の各アライアンス先との連携により、ブロックチェーン応用システム並びに仮想通貨交換業者、コールドウォレット提供事業者、ICO及びSTO事業者向けにサイバー・フィジカル・セキュリティ対策ソリューションを提供するため、新設子会社として株式会社CELを2018年9月に設立いたしました。

(百万円未満切捨て)

1. 2019年3月期第2四半期の連結業績 (2018年4月1日～2018年9月30日)

(1) 連結経営成績 (累計)

(%表示は、対前年同四半期増減率)

	売上高		営業利益		経常利益		親会社株主に帰属する 四半期純利益	
	百万円	%	百万円	%	百万円	%	百万円	%
2019年3月期第2四半期	457	△6.2	△38	—	△39	—	△45	—
2018年3月期第2四半期	487	△50.9	9	△55.4	12	△37.2	6	△45.2

(注) 包括利益 2019年3月期第2四半期 △36百万円 (—%) 2018年3月期第2四半期 11百万円 (△15.7%)

	1株当たり 四半期純利益	潜在株式調整後 1株当たり 四半期純利益
	円 銭	円 銭
2019年3月期第2四半期	△5.77	—
2018年3月期第2四半期	0.85	—

(2) 連結財政状態

	総資産	純資産	自己資本比率	1株当たり純資産
	百万円	百万円	%	円 銭
2019年3月期第2四半期	1,909	1,609	84.2	184.98
2018年3月期	962	714	74.1	95.19

(参考) 自己資本 2019年3月期第2四半期 1,608百万円 2018年3月期 713百万円

2018年11月14日

2019年3月期 第2四半期報告書

https://ssl4.eir-parts.net/doc/2467/yuho_pdf/S100EL05/00.pdf

主要株主が大きく変更した。

(5) 【大株主の状況】

2018年9月30日現在

氏名又は名称	住所	所有株式数 (株)	発行済株式(自己 株式を除く。)の 総数に対する所有 株式数の割合(%)
西澤管財株式会社	東京都中央区銀座四丁目9番8号	1,000,000	11.50
村松 澄夫	千葉県流山市	916,700	10.54
日本トラスティ・サービス信託銀行 株式会社	東京都中央区晴海1丁目8-11	204,900	2.36
松井証券株式会社	東京都千代田区麹町1丁目4番地	198,900	2.29
カブドットコム証券株式会社	東京都千代田区大手町1丁目3番2号	128,600	1.48
米田 豊	東京都杉並区	100,100	1.15
金本 康来	大阪市阿倍野区	95,000	1.09
株式会社SBI証券	東京都港区六本木1丁目6番1号	80,000	0.92
米田 研介	東京都杉並区	72,500	0.83
有限会社アート緑化	埼玉県飯能市中居134-1	72,100	0.83
計	—	2,868,800	33.00

創業者の村松澄夫氏(1,210,000株→916,700株)、株式会社MH capital(992,000株)、JP capital株式会社(900,000株)、西岡将基氏(240,000株)、株式会社DOWN CAPITAL(120,200株)、中辻哲郎氏(100,000株)など、現在の経営に関与していない主要株主が一部もしくは全部売却している。逆に、新しい主要株主が台頭してきている。

日本トラスティ・サービス信託銀行(204,900株)は、三井住友トラストHDとりそな銀行の共同出資会社で、投資信託や年金基金のお金を間接的に運用する資産管理業務を行なっている。つまり、バルクHDも機関投資家にも買われるような銘柄として認められたと言える。

また、松井証券(198,900株)、カブドットコム証券(128,600株)、SBI証券(80,000株)が保有する株は、信用取引の貸し株に充てられるため、バルクHDが信用銘柄として差出せるほどの信用性を認められたと考えられる。

日本トラスティ・サービス信託銀行

<https://www.japantrustee.co.jp/corporate/business.html>

新しい主要株主は以下である。

米田豊氏(100,100株)は兵庫教育大学の副学長。米田研介氏(72,500株)は同じく東京都杉並区在住であることから親族だと思われる。バルクHDとの関係は不明。

金本康来氏(95,000株)は(社)日本リノベーション・マネジメント協会の理事。株式会社シーエムシー。株式会社エアーテック代表取締役。バルクHDとの関係は不明。

2018年11月15日 (CyberGYMのIR)

サイバーセキュリティトレーニング『Cyber Defense Essentials 2 days -supports hybrid-』を開催します (1/22・23)

<http://cybergym.tokyo/40/>

CYBERGYM TOKYOにおきまして、『Cyber Defense Essentials 2 days -supports hybrid-』を開催します。

ハンズオンの時間を多く設けたトレーニングを1名様からお申込みいただける集合型の日程をご用意しました。

当日はイスラエルのホワイトチームが来日しての直接指導、およびイスラエルのレッドチームとリアルタイムで繋ぎ実際に最先端のサイバーアタック攻防を実体験していただけます。

《トレーニング概要》

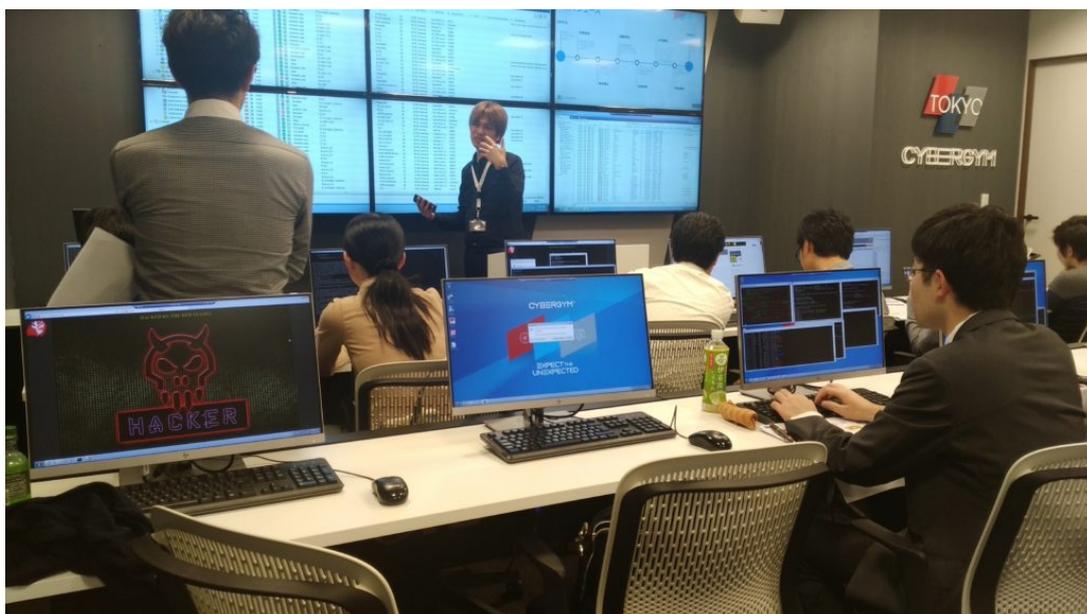
日時：2019年1月22日(火)・23日(水) 9:30~17:30

場所：東京都港区1-14-11 CYBERGYM TOKYO アリーナ

費用：250,000円/1名

2018年11月26日 (CyberGYMのIR)

IPA産業サイバーセキュリティセンターの受講生の皆さまがトレーニングを体験受講されました
<http://cybergym.tokyo/54/>



11月22日（木）に独立行政法人情報処理推進機構 産業サイバーセキュリティセンターの受講生の皆さまが 弊社サイバーセキュリティトレーニングを体験受講されました。トレーニングを通じ、実践的なサイバー攻撃を実感できたと評価を頂戴しました。

2018年11月27日

仮想通貨GFXがBitPoint APECに上場。CISOであった田中翔一朗氏がGFXのCEOに就任。

GFX web site

<http://gfxfoundation.com/?lang=en>

BITPOINT-APEC web site

<https://www.bitpoint-apec.com/index>

→上場後497円(11/27終値)から620円(12/3終値)まで上昇。

2018年11月30日

当社子会社SCH が『Cybertech Tokyo 2018』(2018/11/29-30)に出展しました。

<https://www.vlcholdings.com/wp/wp-content/uploads/2018/11/PR20181130.pdf>

サイバージム社CEOのオフィール・ハソンも出席し、サイバーセキュリティ上の諸課題に取り組む国内企業・団体等のみなさまに対して、イスラエル、米国、日本、ヨーロッパ等のCYBERGYM拠点・ネットワークを通じたグローバルサポート体制や最先端のサイバーセキュリティ・ディフェンスソリューション等をご紹介します。

また、SCHのボードメンバーでもあるイスラエル電力公社CISO(Chief Information Security Officer)・サイバージム社Chairman of Steering CommitteeのYosi Shneck氏が、『危機管理』と題して講演しました。



2018年12月3日 (CyberGYMのIR)

株式会社FiNC Technologiesにて経営幹部向けサイバーセキュリティマネジメントセミナーを実施しました

<http://cybergym.tokyo/92/>

2018年11月30日、株式会社FiNC Technologiesにて、CYBERGYM ISRAEL CEO Ofir Hason ならびにCYBERGYM NYC/TOKYO CEO石原紀彦が同社経営幹部の皆さまを対象としたマネジメントセミナーを実施しました。

本セミナーでは、現在のサイバー環境における最新情報から基礎知識、そして会社経営にあたって自社のサイバーセキュリティにおけるリスクや必要な取り組みについて詳細に紹介し、インシデントが発生した際に経営幹部がこれらの知識を持って迅速かつ確かな意思決定を行う必要がある旨を強調しました。

また、インシデントの95%には何らかの人為的なミスが絡んでいることにも触れ、組織全体における各階層・各部門に見合ったサイバーセキュリティトレーニングの必要性を説きました。

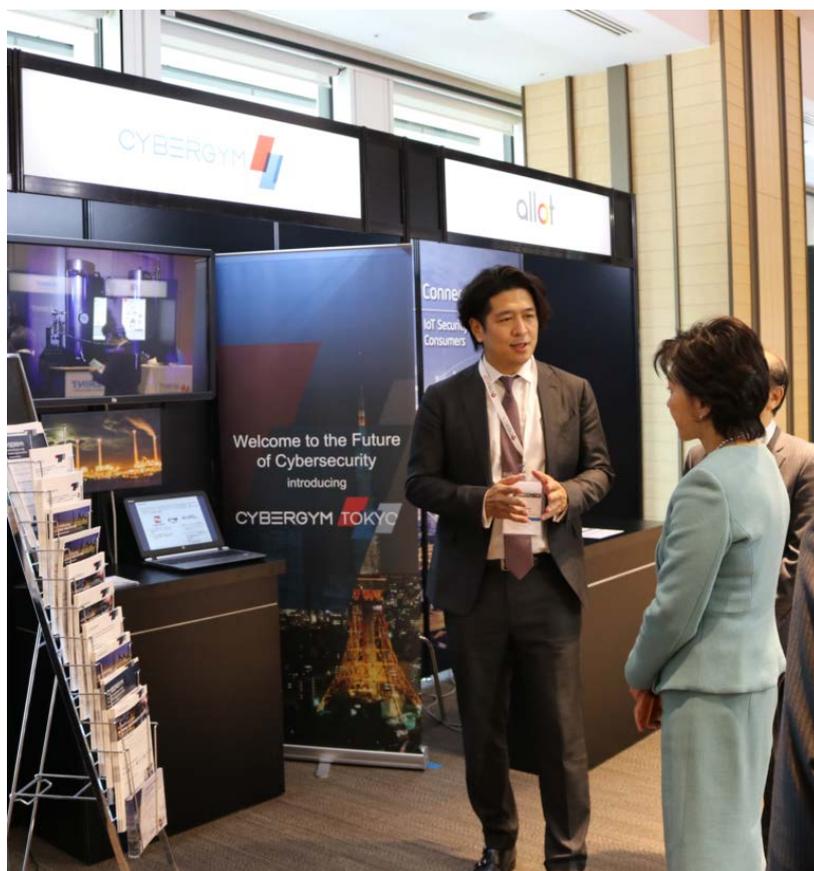
2018年12月3日 (CyberGYMのIR)

CYBER TECH TOKYO 2018に出展しました

<http://cybergym.tokyo/24/>

2018年11月29日・30日に開催されたCYBER TECH TOKYO 2018にCYBERGYMが出展し、多くの方々にブースへお越しいただきました。

また、総務省 佐藤ゆかり副大臣もCYBERGYMブースをご視察されました。



2018年12月5日

サイバーセキュリティ国際会議『サイバー・イニシアチブ東京 2018』（2018/12/11-12 開催）において、当社代表取締役社長の石原紀彦が講演いたします。

<https://www.vlcholdings.com/wp/wp-content/uploads/2018/12/PR20181205.pdf>

この講演では、IT 環境に加えて、重要インフラや工場・設備の OT(Operation Technology)環境でも具体的なサイバー攻撃のリスクが高まってきていること、企業経営上の最重要課題の一つであるサイバーセキュリティ対策として、世界で実際に発生した攻撃シナリオを再現し、実践的なトレーニングを行うことが非常に有効であることなどについてご説明させていただく予定です。

2018年12月17日（CyberGYMのIR）

CYBER INITIATIVE TOKYO 2018で弊社CEO石原が講演しました

<http://cybergym.tokyo/30/>

2018年12月11日・12日に虎ノ門ヒルズフォーラムで開催された『CYBER INITIATIVE TOKYO 2018』におきまして、『日本企業の経営視点から見た実践的サイバー防衛訓練の必要性 The CYBERGYM value from management point of view』と題し、藤原 洋氏とともに弊社 CEO 石原紀彦が講演しました。



2018年12月25日 (CyberGYMのIR)

サイバーセキュリティトレーニング『Cyber Defense Essentials 2 days -supports hybrid-』を開催します (2/19・20)

<http://cybergym.tokyo/98/>

CYBERGYM TOKYOにおきまして、『Cyber Defense Essentials 2 days -supports hybrid-』を開催します。

ハンズオンの時間を多く設けたトレーニングを1名様からお申込みいただける集合型の日程をご用意しました。

当日はイスラエルのホワイトチームが来日しての直接指導、およびイスラエルのレッドチームとリアルタイムで繋ぎ実際に最先端のサイバー攻撃攻防を実体験していただけます。

《トレーニング概要》

日時：2019年2月19日(火)・20日(水) 9:30~17:30

場所：東京都港区1-14-11 CYBERGYM TOKYO アリーナ

費用：250,000円/1名

2019年1月3日

AerNos Nano-Gas Sensors to Power Wearable Alert Devices for People with Diabetes

http://www.aernos.com/press/AerNos_Nano-Gas_Sensors_to_Power_Wearable_Alert_Devices_for_People_with_Diabetes.html

San Diego, California -- (January 3, 2019) – AerNos Inc. today announced that its nanotechnology based gas sensors will be incorporated in a new wearable alert device that will detect certain exhaled gases indicative of hypoglycemic and hyperglycemic diabetic episodes. Using a non-invasive, always-on alert system, AerBetic will enable a higher quality of life for the more than 460 million people worldwide diagnosed with

diabetes. AerBetic will be demonstrated during CES 2019 in AerNos booth 42349, Sands Expo, January 8 – 11 in Las Vegas.

AerNos Inc.は本日、ナノテクノロジーベースのガスセンサーが、低血糖および高血糖の糖尿病エピソードを示す特定の呼気ガスを検出する新しいウェアラブル警告装置に組み込まれることを発表しました。非侵襲的な常時警戒システムを使用したAerBeticは、世界中で糖尿病と診断された4億6000万人以上の人々のために、より質の高い生活を可能にします。AerBeticはCES 2019の間に1月8日から11日までラスベガスで開催されるSands ExpoのAerNosブース42349で展示されます。

2019年1月8日

サイバーセキュリティトレーニング 『CyberGym's Zero to 'Hero'』 プログラムのご案内

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/01/PR20190108.pdf>

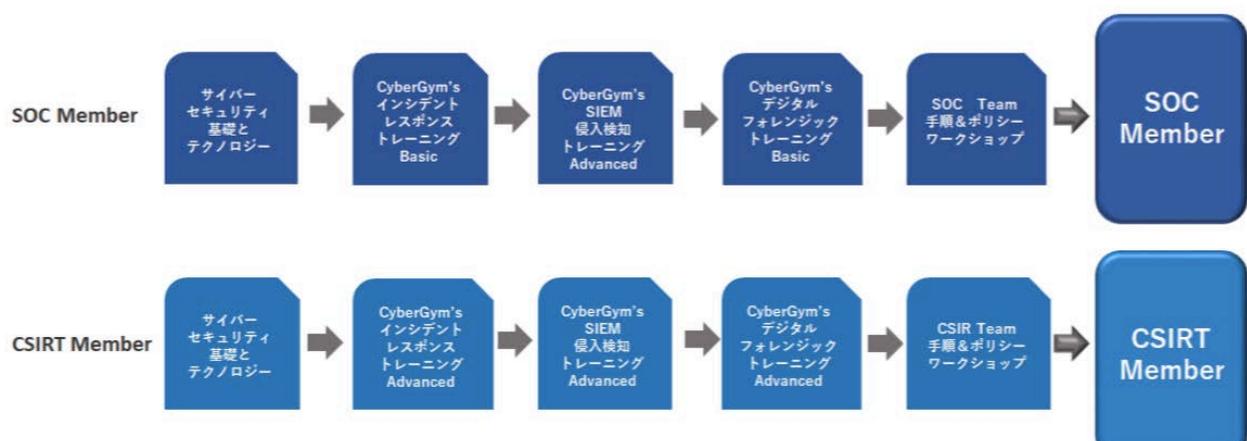
高度情報化社会においてサイバー攻撃による脅威は日々変化し、巧妙化が進んでいます。また、その被害も拡大・長期化し、深刻化する傾向にあることから、サイバーセキュリティは経営上の最重要課題の一つとなっています。一方で、2016年に経済産業省が公表した調査結果において、日本国内の情報セキュリティ人材は2020年には約19.3万人が不足すると推計されています。

このような背景と有力企業・団体の強いニーズを踏まえ、上記人材需要を充足するハイレベルなサイバーセキュリティ人材の供給を目指し、SCHにおいて、『CyberGym's Zero to 'Hero'』プログラムを開発いたしました。

本プログラムはSOC及びインシデント対応を担い得るハイレベルなチームメンバーの育成を目的としており、カリキュラムの各ステージは、講義形式と実践形式のプログラムで構成されています。CYBERGYMホワイトチームがサイバーセキュリティに関する専門的かつ広範な知識を体系的に提供し、これにCYBERGYMレッドチームによる模擬サイバー攻撃への対処を交えた実践演習を効果的に組み合わせることで、複雑化・巧妙化するサイバー攻撃に対して実践的な対応・調査能力を持つ人材を育成いたします。

また、各企業・団体の業種・業態や内部方針・プロセスに合わせた、それぞれの脅威モデルに基づく実際の攻撃シナリオを用いたトレーニングを組み込むことも可能であり、より実践的な能力を備えた即戦力人材の獲得を強力に支援いたします。

【本トレーニングの流れ】



プログラム名 : CyberGym'S Zero to 'Hero'

価格(税抜き) : 1名 100万円～

実施期間 : 2か月～

2019年1月8日

当社出資先であるAerNos 社が CES 2019 Innovation Awardsを受賞

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/01/PR20190108-2.pdf>

当社出資先である米国の次世代ガスセンサーメーカーAerNos,Inc.が、2019年1月8日～11日に開催される世界最先端の技術見本市「CES 2019(Consumer Electronics Show)※」(開催地:米国ラスベガス)に昨年に引き続き出展いたします。

このCES2019において、AerNos 社開発製品の『AerloT』は、CES 2019 Innovation Awards(Tech for a Better World 部門)を受賞いたしました。

AerNos社プレスリリース: <http://www.aernos.com/news-press-releases.html>

AerloTは、様々なアプリケーションや業界向けにリアルタイムの大気モニタリングを実現させ、スマート家電、車内環境制御システム、ドローン、空気清浄などのサードパーティ製IoTデバイスに組み込むことが可能な画期的なナノガスセンサーモジュールです。

※出展社数が約 4,000 社にも上るCESは、世界中の民生機器テクノロジー業界の関係者が参加する世界最大規模の最新技術・製品の見本市・展示会であり、約50年にわたり、次世代の革新的テクノロジーの市場投入の可能性を探る場として、かつイノベーターや画期的な技術を実証する場としての役割を果たしております。

公式サイト: <https://www.ces.tech/>

2019年1月10日 (CyberGYMのIR)

CYBERGYM CEOのOfir Hasonが 『Industry Era 10 BEST CEOs of 2018』 に選ばれました

<http://cybergym.tokyo/107/>

当社グループのサイバーセキュリティ分野における事業パートナーであるサイバージム社 (イスラエル (イスラエル、CyberGym Control Ltd.) のCEOであり、当社子会社 (Strategic Cyber Holdings LLC、(株)CEL) のボードメンバーを兼任するOfir Hason (オフィール・ハソン) 氏が、『Industry Era 10 BEST CEOs of 2018』 に選出されました。



『Industry Era』は、ベンチャー・中小企業の保有する革新的な技術・サービスを、経営者・マネジメント層向けに紹介するグローバルテクノロジーマガジンです。

2019年1月11日（株式会社バルクのIR）

経営幹部向けサイバーセキュリティマネジメントセミナー実施に関するお知らせ

<https://www.vlcan.com/wsyz/wp-content/uploads/2019/01/ed0b6239e323f25da150e7b148b7570e.pdf>

当社は、当社グループ会社 Strategic Cyber Holdings LLC(米国)を通じて、当社お取引先である株式会社FiNC Technologies(本社:東京都千代田区)の経営幹部の皆様向けに、サイバーセキュリティマネジメントセミナーを実施しましたので、その概要についてご紹介させていただきます

2018年11月30日、当社お取引先である株式会社 FiNC Technologies にて、CYBERGYM ISRAEL CEO Ofir HasonおよびCYBERGYM NYC/TOKYO CEO石原紀彦を講師として、同社の経営幹部の皆様を対象としたマネジメントセミナーを実施させていただきました。

本セミナーでは、サイバー環境における最新情報から基礎知識、そして会社経営にあたって自社のサイバーセキュリティにおけるリスクや必要な取り組みについて詳細に紹介し、インシデントが発生した際に経営幹部がこれらの知識を持って迅速かつ確かな意思決定を行う必要がある旨を強調しました。また、インシデントの95%には何らかの人為的なミスが絡んでいることにも触れ、組織全体における各階層・各部門に見合ったサイバーセキュリティトレーニングの必要性を説かせていただきました。

2019年1月16日

株式会社CELがKeypair Inc.(韓国・英国)と国内独占販売契約を締結 世界初の非接触カード型仮想通貨ウォレットと店舗向け決済ソリューションを提供

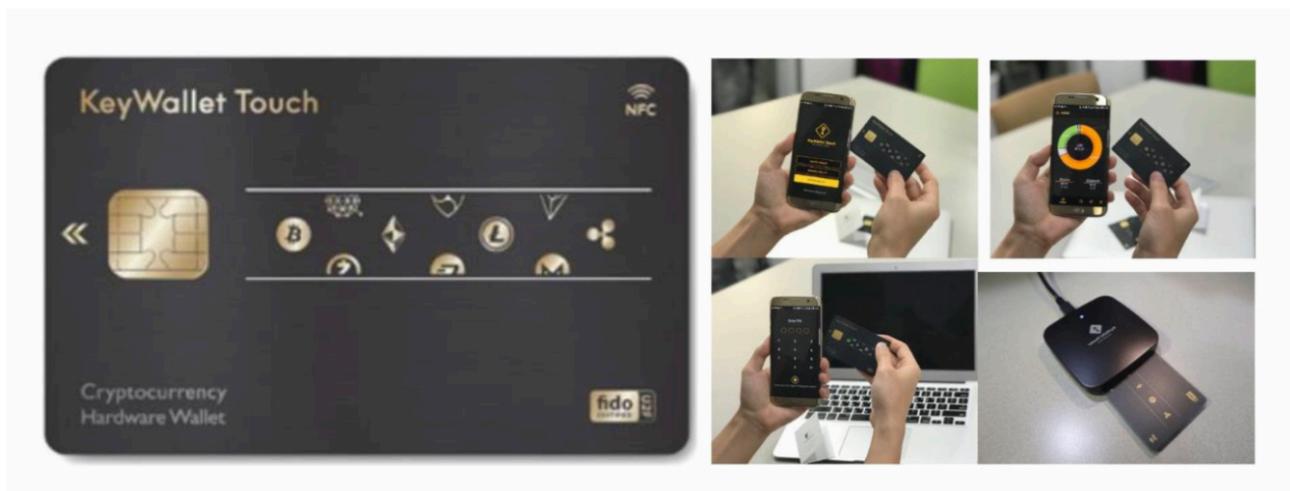
<https://www.vlcholdings.com/wp/wp-content/uploads/2019/01/PR20190116.pdf>

Keypair 社は、2012年に数社の事業売却実績を持つシリアルアントレプレナーであるKevin Lee 氏と、暗号学博士号を持つ Korea University 非常勤教授 JY Lee氏によって創業されたグローバル・フィンテック企業です。

Keypair社は、セキュリティチップ、ハードウェアおよびソフトウェアの独自の技術・特許と調達経路を保有し、同社の開発した SmartOne Card※は SHINHAN CARD、Kookmin Bank、Hana Bank、WOORI BANKおよびNH BANKなどの韓国大手金融機関に納品され、認証カードで韓国国内No.1シェアを有しています。また、同社が韓国国内で特許を有するNFC開発技術は大韓民国金融監督院(Korea Financial Supervisory Service)にて業界標準として認定されています。

大韓民国国家情報院(National Intelligence Service)、Samsung などのパートナーを有するKeypair社は、独自のセキュリティチップ製造技術を生かし、韓国国内最大手の電力会社にスマートメーターのセキュリティチップを納品するなどその事業を展開してきましたが、昨年6月に、セキュリティチップ搭載型のNFC対応カード型仮想通貨ウォレット『KeyWallet Touch』を全世界に向けて販売開始しました。販売開始以降、韓国、米国、スイス、台湾、シンガポールおよび日本など、すでにグローバルで20社を超える企業にその技術を提供しております。

※SmartOneCard



Keypair 社が開発した NFC(Near Field Communication)、PKI-based HSM(Public Key Infrastructure based Hardware Security Module)、FIDO U2F(Fast IDentity Online Universal 2nd Factor)、OTP(One Time Password)が一体となった認証カードおよび端末。

KeyWallet Touchは、世界初であり現在世界で唯一のNFC搭載カード型ハードウォレットであり、Bitcoin、BitcoinCash、Ethereum、ERC20 トークン、Ripple、Litecoin、Monacoin および NEM といった各種仮想通貨を安全に保管することができます。利用者は、スマートフォンまたは PCのアプリケーションを利用することで簡単に残高の照会や通貨管理をすることができます(将来的には仮想通貨のウォレット内交換機能も追加予定)。

セキュリティに関しては、Common Criteria EAL5+、FIDO U2F、KCMVPおよびKorea Certificationといった国際的に高水準な認証を取得し、政府機関や重要インフラ企業においても導入が可能なセキュリティ基準をクリアしております。

CEL社は、Keypair社の日本総代理店として、宣伝広告、販売、カスタマーサポートおよび国内各事業者との連携を主導し、非接触型 NFC カードウォレットおよびウォレットアプリ(iOS、Android、Windows、Mac 版)、店舗向け決済端末・決済アプリを順次提供してまいります。小売店、家電量販店および飲食店チェーン各社に設置されている既存のNFCリーダーとのAPI連携についても、国内仮想通貨交換業者との共同開発を予定しております。



会社名:Keypair Inc.

所在地:169, Yeoksam-ro, Gangnam-gu, Seoul

XnTree Ltd. Level 39, One Canada Square, Canary Wharf, London, E14 5AB

代表者:CEO Kevin Ck Lee

<https://www.keypair.co.uk/>

<http://keywalletpro.io>

2019年1月18日

サイバーセキュリティトレーニング『Cyber Defense Essentials 2 days -supports hybrid-』を開催します (3/26・27)

<http://cybergym.tokyo/112/>

CYBERGYM TOKYOにおきまして、『Cyber Defense Essentials 2 days -supports hybrid-』を開催します。

ハンズオンの時間を多く設けたトレーニングを1名様からお申込みいただける集合型の日程をご用意しました。

当日はイスラエルのホワイトチームが来日しての直接指導、およびイスラエルのレッドチームとリアルタイムで繋ぎ実際に最先端のサイバーアタック攻防を実体験していただけます。

《トレーニング概要》

日時：2019年3月26日（火）・27日（水） 9：30～17：30

場所：東京都港区1-14-11 CYBERGYM TOKYO アリーナ

費用：250,000円/1名

2019年1月28日

(開示事項の経過) 当社連結子会社による米国LAコマーシャルアリーナにかかる販売契約及び運用サポート等契約の締結に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1665210/00.pdf>

1.本件契約の概要

(1)Sales agreement(相手先とSCH間で締結)

コマーシャルアリーナの販売契約

(2)Licensing agreement(相手先とサイバージム間で締結)

サービステリトリー等のライセンス契約

(3)Service level agreement(相手先とSCH及びサイバージムの三者間で締結)

コマーシャルアリーナ納入後の継続的メンテナンス及びサポート等にかかる契約

※相手先の名称及び本件契約の詳細につきましては、守秘義務等により非開示とさせていただきます。

2.LAコマーシャルアリーナの概要

名称：CYBERGYM LA(仮称)

開設予定地：米国カリフォルニア州ロサンゼルス市内

設置予定時期：2019年7月～8月

3.今後の見通し

本件により、SCHにおいてコマーシャルアリーナの販売による収益と運用サポート等による継続的収益が発生することで翌期以降における当社グループの業績への寄与が見込まれます。今後、本件において開示すべき事項が生じましたら速やかに開示いたします。

2019年1月29日

当社子会社Strategic Cyber Holdings LLC 株式会社インターネット総合研究所とハイブリッドアリーナの販売等協業に向け基本合意

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/01/PR20190129.pdf>

当社子会社の Strategic Cyber Holdings LLC(本社:米国デラウェア州、代表者:CEO 石原紀彦、以下「SCH」といいます。)は、このたび、2019年1月29日付にて、株式会社インターネット総合研究所(本社:東京都新宿区、代表者:代表取締役所長 最高経営責任者 藤原洋)/以下「IRI」といいます。)と、ハイブリッドアリーナの販売及びライセンス 供与、並びに本アリーナを通じた協業に向けた基本合意書を締結いたしましたので、下記のとおりお知らせいたします。

記

1.本件の概要

IRI グループは、国内のインターネットの普及促進を担ってきたIRIを中心に、5G(第5世代移動通信システム)対応可能なデータセンター事業をコアに各種プラットフォーム事業を展開する株式会社ブロードバンドタワー、国内最大級のインターネット技術の統合イベント「INTERROP TOKYO」など情報通信分野を中心とした最先端の科学技術を伝えるイベント主催・運営事業を展開する株式会社ナノオプト・メディアなどの事業会社で構成されております。また、IRIの親会社であるInternet Research Institute Ltdは、イスラエル・テルアビブ証券取引所の上場企業です。

一方で、SCHは、当社と事業パートナーである Cybergym Control Ltd.(本社:イスラエル ハデラ市、代表者:共同創設者兼CEO, Ofir Hason/以下「サイバージム」といいます。)の共同事業会社であり、サイバーセキュリティ専用トレーニング施設として、**米国ニューヨークに『CYBERGYM NYC』(コマーシャルアリーナ)を、東京赤坂に『CYBERGYM TOKYO』(ハイブリッドアリーナ)**を開設し、サイバージムとの連携により、実践的かつ体系的なセキュリティトレーニングサービスを提供しております。

本件取組みでは、CYBERGYM TOKYOの第2サイトとして、**新宿区にハイブリッドアリーナ(以下「新宿アリーナ」といいます。)**を開設し、新宿アリーナを通じた協業を行う予定です。具体的には、SCHがIRIに対してサイバージムのハイブリッドアリーナを販売し、IRIによる新宿アリーナの運営をホワイトハッカーの提供やプロモーション活動などでサポートいたします。新宿アリーナでは、IRIグループ等の顧客に対してサイバーセキュリティトレーニングサービスを提供するとともに、IRIグループ内におけるホワイトハッカーなどのサイバーセキュリティスペシャリストの育成をはかります。また、本件協業としてSCHは、IRI グループとの新たなセキュリティソリューション等の開発、共同営業、相互の顧客紹介、技術者人材の交流・相互補完なども予定しております

2.ハイブリッドアリーナの概要

名称：未定

開設予定地：東京都新宿区

3.本件当事者の概要

(1) 相手方(IRI)の概要

1 名称：株式会社インターネット総合研究所

2 所在地：東京都新宿区西新宿一丁目6番1号新宿エルタワー12階

3 代表者の役職・氏名：代表取締役所長 最高経営責任者 藤原 洋

4 設立年月日：2017年10月5日

5 事業内容：コンサルティング事業、インキュベーション事業

6 当社との関係：資本関係、人的関係、取引関係はありません。また、関連当事者への該当事項もありません。

(2) 当社子会社(SCH)の概要

1 名称：Strategic Cyber Holdings LLC

2 所在地：850 New Burton Road, Suite 201, Dover, DE 19904

3 代表者の役職・氏名：CEO 石原紀彦

4 設立年月日：2018年1月31日

5 事業内容：サイバーセキュリティトレーニングサービスの提供など

6 当社との資本関係：当社100%出資(サイバージムが30%分の持分取得権を保有)

4.今後の日程

(1)本件基本合意書締結日

2019年1月29日

(2)本契約等締結予定日 (2019年3月末までを目処に以下の契約締結に向けた協議を行うことを予定しております。)

1 Sales agreement (IRIとSCH間で締結)

ハイブリッドアリーナの販売契約

2 Licensing agreement (IRIとSCH及びサイバージムの三者間で締結)

サイバージムの商標その他知的財産権の使用にかかる契約

3 Service level agreement (IRIとSCH及びサイバージムの三者間で締結)

ハイブリッドアリーナ納入後の継続的メンテナンス、サポート及びライセンスにかかる契約

4 その他本件協業に関する契約 (IRIとSCH間で締結)

(3) 新宿アリーナの設置・開設予定日

2019年7月～8月頃を目途

株式会社インターネット総合研究所 (Internet Research Institute Ltd.)

<https://www.iri.co.jp>

2019年1月29日

Cybergym Control Ltd.社がCyber reason社との戦略的コラボレーションを発表

<http://cybergym.tokyo/127/>

当社事業パートナーのCybergym Control Ltd. (イスラエル) のCEO Ofir Hasonが、エンドポイントセキュリティ企業であるCyber reason CEOのLior Div氏とともに、2019年1月28日にCYBERTECH 2019 Tel Avivのイベントにおいて、戦略的コラボレーションを実施すると発表しました。



Cyber reason

<https://www.cybereason.co.jp>

2019年2月4日

当社子会社 Strategic Cyber Holdings LLC(CYBERGYM TOKYO) テクノプロ・デザイン社とサイバーセキュリティエキスパートの育成事業で協業

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/02/PR20190204.pdf>

当社子会社のStrategic Cyber Holdings LLC(東京都港区、CEO石原紀彦、以下「SCH」)は、CYBERGYM TOKYOにおいて、国内最大規模の技術系人材サービスを提供する株式会社テクノプロ(東京都港区、代表取締役社長 西尾保示)の最大規模の社内カンパニーであるテクノプロ・デザイン社と、サイバーセキュリティエキスパートの育成・派遣事業で協業し、双方の顧客に対し共同でサイバーセキュリティに関連したサービスの提供を行うことで合意しました。なお、本協業において育成するサイバーセキュリティエキスパートの人員数として、まずは2020年6月までに100名規模を目指します。

◆テクノプロ・デザイン社

技術系人材サービスを手がける株式会社テクノプロの最大規模の社内カンパニーであるテクノプロ・デザイン社は、2017年6月末現在、機械、電気・電子、組込制御などの分野を中心に6,167名の正社員(無期雇用)技術者を擁し、大手メーカーを中心に製造業、情報産業など700を超すお客様の研究開発・設計開発の現場で技術サービスを提供しています。

URL:<http://www.technopro.com/design/>

◆テクノプロ・グループ

テクノプロ・グループは国内120以上の拠点に14,346名(2017年6月末時点)の技術者・研究者を擁する日本最大の技術系人材サービス企業グループです。機械、電気・電子、情報システム、化学、バイオ、医薬、建築、土木など、日本の産業界で必要とされているほぼすべての技術領域をカバーする専門領域の幅広さが評価され、国内外で1,800以上の企業・大学・研究機関に技術を軸とした各種のサービスを提供しています。

URL:<http://www.technproholdings.com/>

2019年2月14日

2019年3月期通期連結業績予想の修正に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1676992/00.pdf>

1. 2019年3月期通期連結業績予想数値の修正 (2018年4月1日～2019年3月31日)

	売上高	営業利益	経常利益	親会社株主に 帰属する 四半期純利益	1株当たり 四半期純利益
前回発表予想 (A) (2018年5月14日公表)	百万円 1,387 ～1,254	百万円 70 ～△31	百万円 72 ～△29	百万円 △12 ～△60	円 銭 △1.60 ～△8.00
今回修正予想 (B)	1,027	△374	△380	△392	△47.27
増減額 (B - A)	△360 ～△227	△444 ～△343	△452 ～△351	△380 ～△332	
増減率 (%)	△26.0 △18.1	-	-	-	
(ご参考)前期実績 (2018年3月期)	1,008	15	19	42	5.73

2019年2月14日

2019年3月期 第3四半期決算短信〔日本基準〕(連結)

<https://ssl4.eir-parts.net/doc/2467/tdnet/1676994/00.pdf>

(百万円未満切捨て)

1. 2019年3月期第3四半期の連結業績(2018年4月1日～2018年12月31日)

(1) 連結経営成績(累計)

(%表示は、対前年同四半期増減率)

	売上高		営業利益		経常利益		親会社株主に帰属する 四半期純利益	
	百万円	%	百万円	%	百万円	%	百万円	%
2019年3月期第3四半期	744	△5.0	△204	—	△208	—	△221	—
2018年3月期第3四半期	784	△46.3	19	△45.3	22	△30.1	13	△14.0

(注) 包括利益 2019年3月期第3四半期 △248百万円(—%) 2018年3月期第3四半期 18百万円(3.7%)

	1株当たり 四半期純利益	潜在株式調整後 1株当たり 四半期純利益
	円 銭	円 銭
2019年3月期第3四半期	△27.18	—
2018年3月期第3四半期	1.74	—

(2) 連結財政状態

	総資産	純資産	自己資本比率	1株当たり純資産
	百万円	百万円	%	円 銭
2019年3月期第3四半期	1,864	1,397	74.9	160.58
2018年3月期	962	714	74.1	95.19

(参考) 自己資本 2019年3月期第3四半期 1,396百万円 2018年3月期 713百万円

2. 配当の状況

	年間配当金				
	第1四半期末	第2四半期末	第3四半期末	期末	合計
	円 銭	円 銭	円 銭	円 銭	円 銭
2018年3月期	—	0.00	—	0.00	0.00
2019年3月期	—	0.00	—	—	—
2019年3月期(予想)	—	—	—	0.00	0.00

(注) 直近に公表されている配当予想からの修正の有無: 無

3. 2019年3月期の連結業績予想(2018年4月1日～2019年3月31日)

(%表示は、対前期増減率)

	売上高		営業利益		経常利益		親会社株主に帰属 する当期純利益		1株当たり 当期純利益
	百万円	%	百万円	%	百万円	%	百万円	%	円 銭
通期	1,027	1.9	△374	—	△380	—	△392	—	△47.27

(注) 直近に公表されている業績予想からの修正の有無: 有

2019年2月14日

2019年3月期 第3四半期報告書

https://ssl4.eir-parts.net/doc/2467/yuho_pdf/S100F800/00.pdf

2019年2月18日

株式会社CELがHigh-Tech Bridge SA(スイス・米国)と国内独占販売契約を締結 機械学習・AIを
応用した脆弱性診断・ペネトレーションテストサービスを提供

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/02/PR20190218.pdf>

2019年2月15日付けで、当社100%子会社である株式会社CEL(以下「CEL社」)は、High-Tech Bridge SA(以下「HTB社」)との間で、日本国内における『ImmuniWeb® AI Platform』販売に関する独占契約を締結いたしました。

『ImmuniWeb® AI Platform』は、HTB社のアプリケーションセキュリティテスト自動化ソリューションの総称であり、CEL社は本契約を通じて、機械学習・AIの応用により品質・スピード・コスト競争力を兼ね備えた脆弱性診断・ペネトレーションテストサービスを日本国内において独占的に提供いたします。

HTB社は、2007年にセキュリティエンジニアであるIliia Kolochenko氏によりスイスで創業されたグローバル・AST事業者※1であり、Barracuda (NYSE: CUDA)、F5® (NASDAQ: FFIV)、Imperva® (NYSE: IMPV)、Qualys(NASDAQ: QLYS)、PwC(スイス・シンガポール)とテクノロジーパートナーとして提携し、4つの有料AIセキュリティサービス『ImmuniWeb® AI Platform』※2とSSL Security Test、Website Security Test、Phishing Test、Mobile App Security Testの4つの無料AIセキュリティテストサービスを提供しております。HTB社は、英国セキュリティアセスメント認証機関によるCREST※3認証を保持し、2016年にはWEBセキュリティテスト市場において米Frost&Sullivan社より最も革新的なリーダーポジションとしての評価を受け、2017年には米Gartner社よりCool Vendor選出、2018年には機械学習・AIを用いたサイバーセキュリティソリューションとしてSC Award Europeで最優秀賞を受賞し、米IDC社よりMobile Application Security Testing (MAST) 市場におけるイノベーターとして選出されました。

※1 AST(Application Security Testing)事業者:

WEBサイト・スマートフォンアプリ・イントラネットなどのアプリケーションおよびインフラストラクチャを対象としてセキュリティ検査を行う事業者

※2 『ImmuniWeb® AI Platform』に含まれる4つのAIセキュリティサービス:

—ImmuniWeb®Discovery <https://www.htbridge.com/immuniweb/discovery/>

WEBアプリ、スマートフォンアプリ、API、クラウド、ドメイン、SSLなど、自社が保有する資産を可視化し、HackabilityスコアとAttractivenessスコアにより管理の優先順位付けを行うサービス

—ImmuniWeb®On-Demand <https://www.htbridge.com/immuniweb/ondemand/>

WEB サイトセキュリティ、プライバシー、コンプライアンスの検査および監査を目的として WEB アプリケーション、WEB サーバ、API、WAF(WEB アプリケーションファイヤーウォール)のテストを行うサービス

—ImmuniWeb®Continuous <https://www.htbridge.com/immuniweb/continuous/>

WEBサイトセキュリティ、プライバシー、コンプライアンスのモニタリングサービス。24時間365日定期的にアプリケーションを監視するセキュリティオペレーションセンター(SoC)サービス

—ImmuniWeb®MobileSuite <https://www.htbridge.com/immuniweb/mobile/>

iOSおよびAndroidアプリに対して、プログラム、バックエンドサーバ、API、プライバシー、暗号化のテストを行うサービス

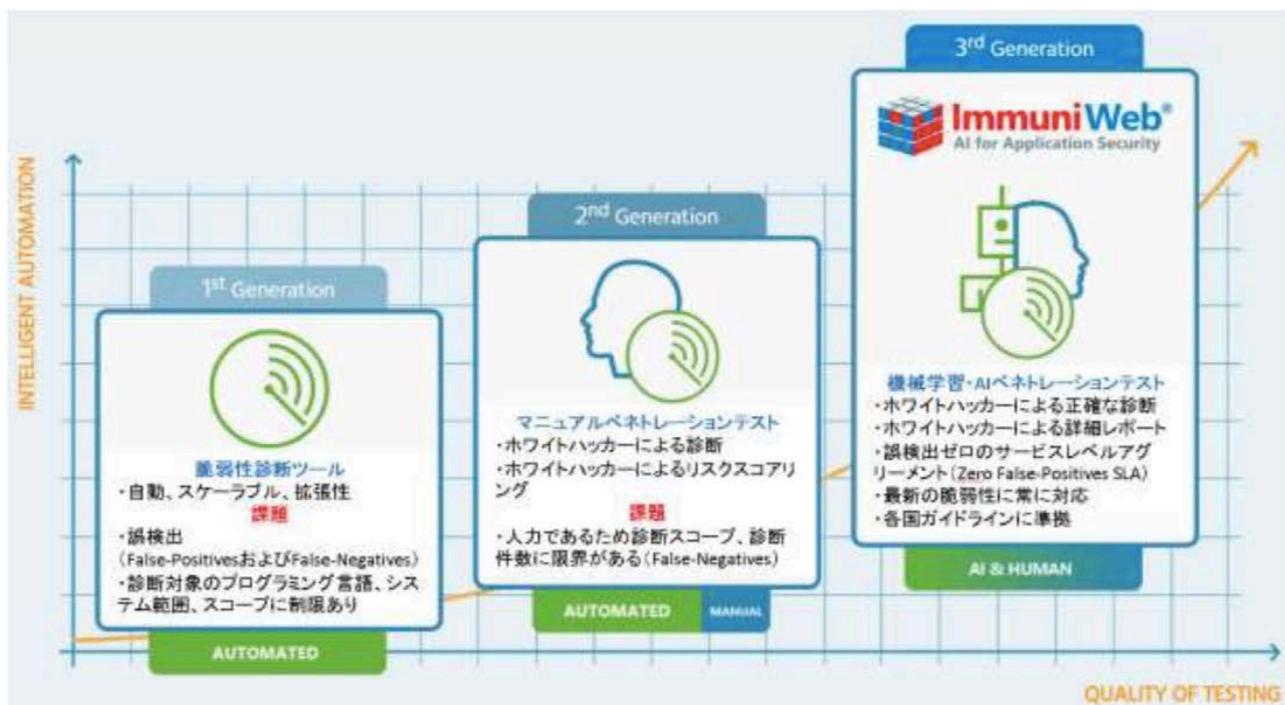
※3 CREST(The Council of Registered Ethical Security Testers):

英国の情報セキュリティ認定機関およびその認証制度

なお、アプリケーションセキュリティアセスメントをグローバルで実施する際には各国ガイドラインや各国法に準拠する必要がありますが、HTB社は米国NIST※4、英国CREST、EU-GDPR※5などの各国ガイドラインおよび法制度、PCIDSS※6、HIPAA※7などの国際的な業界規格に準拠した調査・診断・報告を行っており、PwC TVM Framework※8の一部として158か国を超えるグローバル企業にソリューションを提供しています。

また、現在、世界中で毎日350,000件の最新マルウェアが報告されています(AV-TEST Institute 調べ)、米MITRE社が発表している共通脆弱性識別子であるCVE※9は1999年から現在にいたるまで11万種類以上報告され、2018年には16,555種類のCVEが登録されています。

HTB 社はCVEをはじめとして、CWE※10、CVSS※11 といったセキュリティ報告の国際規格および、OWASP Top 10※12、CWE/SANS Top 25※13、PCI DSS 3.2.1, Requirements 6.5.1-6.5.10※14 といった国際脆弱性検査標準に依拠した調査・診断・報告を行っています。



※4 NIST(National Institute of Standards and Technology): アメリカ国立標準技術研究所

※5 EU-GDPR(EU General Data Protection Regulation): EU一般データ保護規則

※6 PCIDSS(Payment Card Industry Data Security Standard):

国際ペイメントブランド5社(アメリカンエクスプレス、Discover、JCB、マスターカード、VISA)が策定したカード情報セキュリティの国際統一基準

※7 HIPAA(Health Insurance Portability and Accountability Act of 1996):

医療情報の電子化の推進とそれに関するプライバシー保護やセキュリティ確保について定めた米国の法律

※8 PwC TVM(PricewaterhouseCoopers Threat and Vulnerability Management) Framework:

世界4大会計事務所・総合コンサルティングファームである英プライスウォーターハウスクーパース社のセキュリティコンサルティングフレームワーク

参照: <https://www.htbridge.com/immuniweb/partners/TAP/>

※9 CVE(Common Vulnerabilities and Exposures):

共通脆弱性識別子。個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体のMITRE社が採番

※10 CWE(Common Weakness Enumeration): 共通脆弱性タイプ一覧。MITRE社が採番

※11 CVSS(Common Vulnerability Scoring System):

共通脆弱性評価システム。米 FIRST(Forum of Incident Response and Security Teams)が採番

※12 OWASP Top 10:

世界的なオープンソースコミュニティであり米国政府認定NPOである OWASP(Open Web Application Security Project)が発表している脆弱性リスト

※13 CWE/SANS Top 25: 米MITRE社と米SANS Institute社が共同で発表している脆弱性リスト

※14 PCI DSS 3.2.1, Requirements 6.5.1-6.5.10:

米PCI SSC(Payment Card Industry Security Standards Council)が公表している世界中の企業が決済カードデータを保護するための基準

このような膨大な情報を扱う専門家であるホワイトハッカー人材は、情報セキュリティ業界において希少な存在であるとともにグローバル企業間での人材争奪戦も激しく、大手企業であっても増員が難しいとされています。HTB社はセキュリティに関する膨大なデータ処理と、国際的なホワイトハッカー人材不足という課題を解決するために、機械学習・AIをアプリケーション脆弱性診断およびペネトレーションテストに応用しました。

HTB社の『ImmuniWeb® AI Platform』を使用することで、従来のセキュリティアセスメント手法に比べてより包括的で高品質な診断(検出率240%増)が可能になるとともに、従来の手法に比べて3倍のスピードで調査・診断・報告が完了し、コスト(人件費×必要時間の金銭換算値)は170%削減されます。また、サービス品質を高めるためにHTB社はクライアントとゼロフォースポジティブ(誤検出ゼロ)のサービスレベルアグリーメントを締結し、米Gartner社の顧客満足度調査である peerinsightsTMで5点満点中4.6点を獲得しています。(2019年2月15日時点)

グローバルのアプリケーションセキュリティ市場は、2017年の2.79 Billion USDから2022年には9 Billion USDまで拡大する見込みであり、年平均成長率は26.4%という急成長市場です(RESEARCH AND MARKETS 調べ)。あらゆるサイバー攻撃のうち6割はWebアプリケーション経由であり(Verizon 調べ)、アプリケーションセキュリティを素早く、低予算で強化できるかという点が企業の実質的なセキュリティ能力向上の課題となっています。

CEL社は国内成長IT企業に対する自社内のホワイトハッカー人材の提供サービスを強化するためにHTB社と連携し、バルクグループが保有する3,000社を超える成長企業顧客に対してHTBソリューションを提供する予定です。また、CEL社はHTB社に寄せられる1日平均グローバル100件を超える見込み客からの問い合わせのうち、日本国内案件に関する対応を行います。CEL社は当社グループであるSCH社が『CYBERGYM's Zero to Hero』※15を通して育成するセキュリティエンジニア人材を活用し、急成長するアプリケーションセキュリティ市場において各チャネルパートナーと協業して市場開拓を行う予定です。

当社グループは、あらゆる環境において“お客様をサイバークライムから守る”ことを重要な使命としており、その実現のためにサイバーセキュリティ分野の各テーマに一つずつ取り組んでまいり所存です。今後も、様々な先端技術を導入し、各事業パートナーとの最適な連携関係を構築することで、株主価値の最大化を目指してまいります。

※15 CYBERGYM's Zero to Hero:

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/02/PR20190204.pdf>

参照: Strategic Cyber Holdings LLC(CYBERGYM TOKYO) テクノプロ・デザイン社とサイバーセキュリティエキスパートの育成事業で協業



会社名: High-Tech Bridge SA

<https://www.htbridge.com/>

所在地: World Trade Center II 29, Route de Pré-Bois, CH-1215 Geneva

代表者: Ilia Kolochenko

2019年2月19日

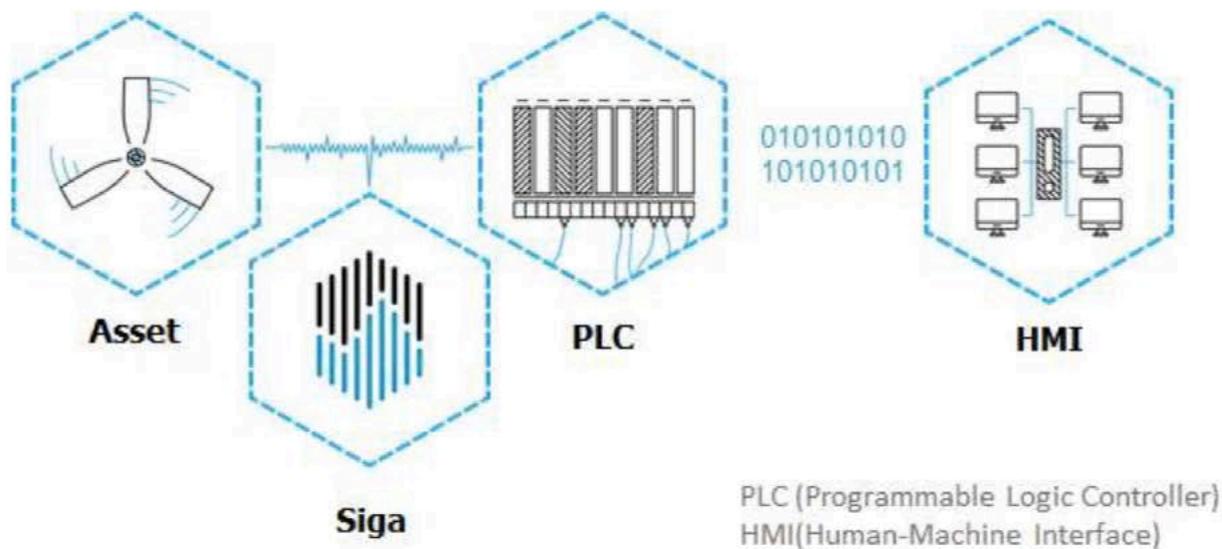
当社子会社Strategic Cyber Holdings LLC 『SIGA Platform』によるAIを用いた制御システム向け初期障害検出サービスの提供開始

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/02/PR20190219.pdf>

当社子会社Strategic Cyber Holdings LLC(米国デラウェア州・東京都港区、CEO石原紀彦、以下「SCH社」)は、日本国内及び米国において、OTソリューションとして、SIGA OT Solutions(イスラエル、CEO Amir Samoiloff)の『Siga Platform』によるAIを用いた産業制御システム向け初期障害検出サービスの提供を開始します。なお、SCH社は本サービスの日本における独占的取扱事業者です。

『SIGA Platform』は、センサーやアクチュエータ※1などのエンドポイントインフラとPLC※2(プログラマブルロジックコントローラ)のネットワークの中間地点に設置されたデータログ取得ハードウェア端末とサーバーにインストールされた専用のソフトウェアの組み合わせで稼働します。『SIGA Platform』を活用することで、既存の産業制御システムを停止させることなく、PLCで処理される前の電気信号をAI・マシンラーニングにより検知・解析し、ICS(インシデント・コマンド・システム)における脅威を即座に特定することが可能となり、異常の初期兆候の的確なモニタリングが実現します。

制御機器・システムの正確でリアルタイムな状態把握を可能とする本サービスは、イスラエル電力公社をはじめとする政府機関及び企業での実績が評価され、世界各国で導入されています。国際的イベントが増える中、日本は制御機器やIoT機器のサイバー攻撃に対する対策が不十分であり、日本のユーティリティ企業においてもこの分野の解決策に大きく寄与するものです。



※1.アクチュエータ 入力されたエネルギーもしくはコンピュータが出力した電気信号を物理的運動に変換する機械・電気回路を構成する機械要素

※2.PLC(プログラマブルロジックコントローラ) プログラムで定められた順序や条件などに従って設備や機械の動きを制御する装置

◆SIGA OT Solutions

SIGA OT Solutions社は、2014年にイスラエルで設立されたグローバルセキュリティ企業です。同社経営陣の重要インフラセキュリティに対する知見とその革新的なサービスは電力発電所・水力発電所・石油プラント・化学プラント・ビルディングシステムなどを運営する多くのグローバル企業に採用されており、2018年には米IT調査会社Gartnerによって『Cool Vendors in Industrial IoT and OT Security』に選出されています。

2019年2月22日

第三者割当による第4回新株予約権(行使価額修正選択権付)に係る行使価額の修正決定に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1679055/00.pdf>

当社が2018年7月11日に発行いたしました第4回新株予約権(行使価額修正選択権付)の全部に関して、当該行使価額修正選択権を行使し、行使価額を修正することを決定いたしましたので、下記のとおりお知らせいたします。

(1)	銘 柄 名	株式会社バルクホールディングス第4回新株予約権
(2)	発行新株予約権数(潜在株式数)	2,900個(290,000株)
(3)	修正前行使価額	1,200円
(4)	修正後行使価額	各修正日の前取引日の名古屋証券取引所における当社普通株式の終値(同日に終値がない場合には、その直前の終値。)の90%に相当する金額の小数第3位未満の端数を切上げた金額
(5)	修正事由	本新株予約権の発行要項第10項に規定された行使価額の修正条項の適用によるものです。
(6)	修正日	2019年2月25日
(7)	修正日前日までの行使個数(潜在株式数)	一個(一株)
(8)	未行使個数(潜在株式数)	2,900個(290,000株)
(9)	調達資金の用途	本新株予約権が行使された場合に払い込まれる資金は、以下の用途に充当する予定です。 ①M&A及び資本・業務提携に関わる資金・費用 ②人件費等の運転資金

※ 修正後の行使価額が463円(以下「下限行使価額」といいます。)を下回る場合には、行使価額は下限行使価額となります。

(10) 行使価額の修正を行う理由

当初行使価額及び本新株予約権発行日以降現在までにおける株価動向、並びに資金調達の迅速性及び必要調達額について総合的に勘案した結果、行使価額の修正を行うこととしました。

2019年2月22日

重要インフラサイバーセキュリティコンファレンス2019にて講演・出展しました

<http://cybergym.tokyo/172/>

2月21日に、品川で開催されました『重要インフラサイバーセキュリティコンファレンス2019』に出展しました。

CYBERGYM TOKYOのブースでは、各種サイバーセキュリティトレーニングのご紹介、ならびにSIGA社CEOのAmir Samoiloff氏による『SIGA Platform』のデモンストレーションを実施しました。重要インフラを対象としたイベントということもあり、AIを用いたOT制御向けの同サービスに関心の高い企業の方々にも多数お立ち寄り頂きました。

更に、CYBERGYM TOKYOからイベントの最後を飾る『Special Night Session』を提供させて頂き、イスラエル電力公社のChairman Yiftah Ron-Tal氏による招待講演が行われました。世界屈指の膨大な量のサイバー攻撃を受けながら、公社として国の重要インフラを担う企業のトップによる講演には、当初予定されていた会場に加えてサテライト会場も用意され、日本のサイバーセ

セキュリティを担う最前線の皆さまに大勢ご来場いただきました。公演中は熱心にメモを取りながらご聴講されている方が多くいらっしゃるなど、ここでも国内におけるサイバーセキュリティの重要性の高まりがこの上ない状況になっていることが表れている雰囲気となりました。

《招待講演の様子》



イスラエル電力公社 Chairman Yiftah Ron-Tal氏



満席の会場の様子

イスラエル電力公社 Chairman Yiftah Ron-Tal氏

https://en.wikipedia.org/wiki/Yiftah_Ron-Tal

2019年2月22日

CYBERGYM EXECUTIVE FORUM 2019を開催しました

<http://cybergym.tokyo/163/>

2月20日に、ホテルオークラ東京において『CYBERGYM EXECUTIVE FORUM 2019』を開催しました。

当日は満席の方々にご来場いただき、弊社代表の石原紀彦から昨年8月の東京アリーナ(赤坂)を開設以来ご支援・ご愛顧を賜っております皆さまへの御礼をお伝えする挨拶から始まりました。第一部ではイスラエル電力公社のChairman Yiftah Ron-Tal氏を招いての特別講演を行いました。

サイバー先進国であるイスラエルの中でも最も多いサイバー攻撃を受けている企業のトップによる講演は、同社における緊迫感のあるサイバーセキュリティ現場のイメージ映像から始まり、万全を期してもなお100%を防ぐことが出来ないサイバー攻撃に対する最大の解決策は「人」であり、そのトレーニングを欠かすことは出来ないと繰り返し強調されました。国の重要インフラを担いながら日々膨大なサイバー防衛を実施している企業のトップによる講演の内容は大変説得力があり、ご聴講された皆さまも熱心に耳を傾けていらっしゃいました。

その後、そのイスラエル電力公社のサイバーセキュリティ教育を担っているCYBERGYMのCEO Ofir Hasonが、実際に導入されているトレーニングをはじめ、最新のサイバーセキュリティトレーニングの情報を皆さまにご紹介しました。それに続き、弊社代表石原紀彦からアメリカ及び日本におけるCYBERGYMの最新状況をお伝えし、『SIGA Platform』の新規展開を発表いたしました。



Ron-tal氏からCYBERGYM TOKYOへ、イスラエル電力公社のプラント模型が贈られるサプライズがありました



2019年2月25日

株式会社CELがCYBAVO Pte.,Ltd.(シンガポール・台湾)と協業 ホワイトハッカー人材を国内成長企業に提供

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/02/PR20190225.pdf>

当社100%子会社である株式会社CEL(以下「CEL社」)は、CYBAVO Pte.,Ltd.(以下「CYBAVO社」)とサイバーセキュリティ分野における協業を開始します。

CYBAVO社は2018年にセキュリティ専門家のPaul Fan氏、Tim Hsu氏、Thomas Lim氏により共同創業されたデジタルアセットセキュリティ企業です。Paul Fan氏はアンチウイルスソフト大手である360 Security Guardの元ゼネラルマネージャーであり、Tim Hsu氏は台湾最大のハッカーコンテストであるHITCONの設立者で、近年は1,000名を超えるホワイトハッカーがHITCONに参加しています。また、Thomas Lim氏は国際的に著名なハッカーカンファレンスであるSyscanおよびセキュリティ調査会社COSEINCの設立者であり、Black HatやDEF CONをはじめとするサイバーセキュリティカンファレンスでの研修・講演の提供実績を有しています。CYBAVOチームはTrendmicro、Taiwan Mobileなどのテクノロジー企業、台湾法務部調査局(MJIB)などの政府諜報機関出身者、セキュリティにおける著名な実績を持つ経営陣によって構成され、Tesla、Facebook、Volkswagen、VIVOTEKをはじめとしたグローバル企業の自動運転車、Webアプリケーション、IPカメラ、ドローンなどのセキュリティに関する脆弱性を発見・報告してきました。

また、CYBAVO社はセキュリティ能力世界第2位※と評価されているCobinhoodのセキュリティコンサルティングを実施しており、安全な鍵管理と金融機関水準のプロセス管理をスケーラブルに実現できる『CYBAVO VAULT』を開発、ブロックチェーン業界における先進的な実績を生み出しています。

CEL社はすでに省庁、電力会社、IT企業などが保有するWebサイト、スマートフォンアプリ、イントラネットに対してセキュリティ診断サービスを提供していますが、日本国内はペネトレーションテストやセキュアバイデザインを推進する人材に乏しいため、CYBAVO社のような海外の先端テクノロジー人材を有する企業と協業することで、日本国内のセキュリティ需要拡大に対応してまいります。

会社名: CYBAVO Pte.,Ltd.

所在地: 102F PASIR PANJANG ROAD #08-02 SINGAPORE

9F, No.415,Sec.4,Xinyi Rd.,Taipei, TAIWAN

代表者:Paul Fan

事業内容:Cryptocurrency storage and management, enterprise wallet, cryptocurrency security. <https://www.cybavo.com/>



2019年2月25日

【申込受付中/4月16日(火)・17日(水)】サイバーセキュリティトレーニング『Cyber Defense Essentials 2 days -supports hybrid-』を開催します

<http://cybergym.tokyo/201/>

CYBERGYM TOKYOにおきまして、『Cyber Defense Essentials 2 days -supports hybrid-』を開催します。

ハンズオンの時間を多く設けたトレーニングを1名様からお申込みいただける集合型の日程をご用意しました。

当日はイスラエルのホワイトチームが来日しての直接指導、およびイスラエルのレッドチームとリアルタイムで繋ぎ実際に最先端のサイバーアタック攻防を実体験していただけます。

《トレーニング概要》

日時：2019年4月16日（火）・17日（水） 9：30～17：30

場所：東京都港区1-14-11 CYBERGYM TOKYO アリーナ

費用：250,000円/1名

2019年2月26日

第三者割当による第4回新株予約権(行使価額修正選択権付)の大量行使に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1679719/00.pdf>

当社が2018年7月11日に発行いたしました第4回新株予約権(行使価額修正選択権付)に関し、2019年2月1日から同年2月26日までの期間において、行使価格737.1円で50,000株を行使しました。未行使の新株予約権は2,400個(24万株)となります。

2019年2月28日

第三者割当による第4回新株予約権(行使価額修正選択権付)の大量行使に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1680555/00.pdf>

当社が2018年7月11日に発行いたしました第4回新株予約権(行使価額修正選択権付)に関し、2019年2月27日から同年2月28日までの期間において、行使価格647.1円で75,000株を行使しました。未行使の新株予約権は1,650個(16万5000株)となります。

2019年3月1日

第三者割当による第4回新株予約権(行使価額修正選択権付)の月間行使状況に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1681154/00.pdf>

当社が2018年7月11日に発行いたしました第4回新株予約権(行使価額修正選択権付)に関し、2019年2月における月間行使状況につきまして、下記のとおりお知らせいたします。

(1)	銘 柄 名	株式会社バルクホールディングス第4回新株予約権
(2)	対象月間の交付株式数	125,000株
(3)	対象月間に行使された新株予約権の数及び発行総数に対する行使比率	1,250個(発行総数の43.10%)
(4)	対象月の前月末時点における未行使新株予約権数	2,900個
(5)	対象月の月末時点における未行使新株予約権数	1,650個

(6) 対象月間における行使状況

行使日	交付株式数		行使価額(円)	行使された新株予約権の数(個)
	新株(株)	移転自己株式(株)		
2月1日(金)～ 2月22日(金)	—	—	1,200	—
2月25日(月)	—	—	817.2	—
2月26日(火)	50,000	—	737.1	500
2月27日(水)	—	—	710.1	—
2月28日(木)	75,000	—	647.1	750

2019年3月1日

当社子会社Strategic Cyber Holdings LLC 『組織内レッドチーム構築・育成・運用支援サービス』の提供開始

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/03/PR20190301.pdf>

当社子会社Strategic Cyber Holdings LLC(米国デラウェア州・東京都港区、CEO 石原紀彦、以下「SCH社」)は、日本国内において、サイバー防衛にかかる『組織内レッドチーム※構築・育成・運用支援サービス』の提供を開始します。

高度情報化社会において、サイバー攻撃は日々変化し、巧妙化が進み脅威は増えています。また、その被害も拡大・長期化し深刻化する傾向にあることから、サイバーセキュリティは経営上の最重要課題の一つとなっています。このサイバーセキュリティ上の諸課題を洗い出し、適切に対処する必要があることから、多数の企業・団体において外部のホワイトハッカーによるペネトレーションテストや脆弱性診断が行われており、また、大企業等の一部では外部のレッドチームによるサイバーインシデント演習も実施されています。当社グループでも最先端の技術や膨大な経験・ノウハウを有する国内外のパートナーと緊密に連携し、これらのサービスを提供しておりますが、サイバー攻撃に備えて、より堅牢な体制を整備し、かつ、実際のサイバー攻撃発生時に、よりフレキシブルに対処することで事業活動への影響を最小化するためには、外部のホワイトハッカーの利用に加え、組織内レッドチームを構築することが非常に効果的です。

それぞれの組織における事業活動、組織、人員、設備、業務フローおよび社内ルールなどの社内環境を熟知した組織内レッドチームを編成し、このチームが内部不正やヒューマンエラーも考慮した様々なサイバー攻撃のシミュレーションを行うことで、外部のホワイトハッカーの利用では判明しなかった組織に内在する脆弱性が明らかとなり、実際のサイバー攻撃に対して、より有効な対処が可能となります。なお、サイバー攻撃の手法には、システム上の侵入だけではなく、人的・物理的な侵入もあり、情報収集・初期侵害から任務遂行までの8つの段階(下図参照)で構成されることから、レッドチームにはサイバーセキュリティの高度な知見・スキルだけではなく、リーガル、アタッカーマインド、コミュニケーション等を含めた総合的な知見・スキルが求められます。

※レッドチーム 攻撃・防御演習において、攻撃を仕掛ける側をレッドチーム、防御する側をブルーチームと呼びます。



SCH社の共同事業パートナーであるCyberGym Control Ltd.(イスラエル、CEO Ofir Hason、以下「サイバージム社」)は、サイバーセキュリティ分野で世界最高レベルにあるとされるイスラ

エルにおいて技術を確立し、その技術力およびノウハウをベースとするサイバーセキュリティトレーニングソリューションをグローバルに提供しております。

この高度な技術力、サイバーセキュリティトレーニングの豊富な実績およびノウハウ、ならびに自社の強力なレッドチームを背景としたサイバージム社のレッドチーム組成ノウハウを最大限に活用し、SCH社は、主に国内の大企業等向けに組織内レッドチームの構築・育成・運用支援サービスを提供します。

なお、本サービスのリリースは、機密レベルや社会インフラとしての重要性の高さから外部のホワイトハッカーの利用が制限される国内大手インフラ企業など、複数の大企業等からの強いニーズを受けたものです。また、当社グループとしては、現時点において、国内で同様のサービスを提供する他の事業者は存在しないものと認識しております。

当社グループは、お客様をサイバー攻撃から全力で守るべく、サイバージム社を中心とする各事業パートナーと緊密に連携し、最適なサイバーセキュリティソリューションの提供を目指します。

2019年3月4日

第三者割当による第4回新株予約権(行使価額修正選択権付)の大量行使に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1681559/00.pdf>

当社が2018年7月11日に発行いたしました第4回新株予約権(行使価額修正選択権付)に関し、2019年3月1日から同年3月4日までの期間において、行使価格672.3円で50,000株を行使しました。未行使の新株予約権は1,150個(11万5000株)となります。

2019年3月5日

(訂正)第三者割当による第4回新株予約権(行使価額修正選択権付)の大量行使に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1681878/00.pdf>

2019年3月4日に公表いたしました「第三者割当による第4回新株予約権(行使価額修正選択権付)の大量行使に関するお知らせ」の内容に訂正すべき事項がありましたので、下記のとおりお知らせいたします。

対象月の前月末時点における発行済株式数：

誤 8,694,000株（うち自己株数:-株）

正 8,819,000株（うち自己株数:-株）

2019年3月5日

第三者割当による第4回新株予約権(行使価額修正選択権付)の大量行使に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1681880/00.pdf>

当社が2018年7月11日に発行いたしました第4回新株予約権(行使価額修正選択権付)に関し、2019年3月5日において、行使価格725.4円で75,000株を行使しました。未行使の新株予約権は400個(4万株)となります。

2019年3月6日

第三者割当による第4回新株予約権(行使価額修正選択権付)の大量行使、行使完了及び月間行使状況に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1682127/00.pdf>

当社が2018年7月11日に発行いたしました第4回新株予約権(行使価額修正選択権付)に関し、2019年3月6日において、行使価格760.5円で40,000株を行使しました。また、当該新株予約権

は、本日をもって行使が全て完了いたしましたので2019年3月の月間行使状況につきましても、併せてお知らせいたします。

2. 月間行使状況

(1) 銘柄名	株式会社バルクホールディングス第4回新株予約権
(2) 対象月間の交付株式数	165,000株
(3) 対象月間に行使された新株予約権の数及び発行総数に対する行使比率	1,650個（発行総数の56.89%）
(4) 対象月の前月末時点における未行使新株予約権数	1,650個
(5) 現時点における未行使新株予約権数	一個

(6) 対象月間における行使状況

行使日	交付株式数		行使価額（円）	行使された新株予約権の数（個）
	新株（株）	移転自己株式（株）		
3月1日（金）	—	—	651.6	—
3月4日（月）	50,000	—	672.3	500
3月5日（火）	75,000	—	725.4	750
3月6日（水）	40,000	—	760.5	400

2019年3月7日

3月6～8日『Security Days Spring 2019 Tokyo』に出展しています

<http://cybergym.tokyo/214/>

6日には『ICS/SCADAにおけるサイバージムのセキュリティーソリューション』と題した講演を行い、満員のご聴講の皆さまへ向けて、今後特にサイバー攻撃の急増が予想されるICS/SCADAにおけるセキュリティーソリューションと、トレーニングの解説を行いました。

2019年4月1日

当社子会社Strategic Cyber Holdings LLCと株式会社インターネット総合研究所とのハイブリッドアーナの販売等協業にかかる契約締結予定日に関するお知らせ

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/04/PR20190401.pdf>

2019年1月29日付「当社子会社Strategic Cyber Holdings LLC、株式会社インターネット総合研究所とハイブリッドアーナの販売等協業に向け基本合意」にて公表いたしましたとおり、当社連結子会社Strategic Cyber Holdings LLC(本社:米国デラウェア州、代表者:CEO石原紀彦/以下「SCH」といいます。)は、株式会社インターネット総合研究所(本社:東京都新宿区、代表者:代表取締役所長 最高経営責任者 藤原洋/以下「IRI」といいます。)と、サイバーセキュリティ専用トレーニング施設『ハイブリッドアーナ』の販売及びライセンス供与、並びに本アーナを通じた協業に向けた基本合意書を締結いたしました。

(1) 基本合意書締結日

2019年1月29日

(2) 本契約締結日(予定)

2019年4月8日

(3) 本件ハイブリッドアリーナの開設地、設置・開設日(予定)

東京都新宿区に2019年7月～8月頃を目途として設置・開設

2019年4月2日

株式会社ショーケースと業務提携契約を締結 第一弾として、当社子会社CELが同社とサイバーセキュリティ分野におけるサービス連携を開始

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/04/PR20190402.pdf>

当社は、本日2019年4月2日付けで、株式会社ショーケース(東京都港区六本木、代表取締役社長:永田 豊志、以下「ショーケース社」)との間で、主にサイバーセキュリティ分野およびマーケティング分野におけるソリューションの共同開発や販売協力等を行うため、業務提携契約を締結しました。

本業務提携の第一弾として、ショーケース社が機械学習・AI を活用した脆弱性診断サービス『ZEIJAX』の提供を開始し、当社連結子会社である株式会社CEL(東京都港区赤坂、代表取締役社長:田中 翔一郎、以下「CEL社」)がこれをサポートします。

<ショーケース社『ZEIJAX』サービスについて>

ZEIJAX は、Web サイト、Webアプリケーション、スマートフォンアプリケーションを対象として、高品質で高速な脆弱性診断およびペネトレーションテストを行うサービスです。

当サービスはセキュリティ診断に機械学習・AI・RPA を活用し、グローバルで収集される脆弱性データ、脅威情報と3800万回以上の Web サイトに対するセキュリティ診断により培われたアルゴリズムを活用しつつ、ホワイトハッカー(サイバーセキュリティ技術者)による誤検出ゼロの品質保証が付与された診断報告書を提供します。

セキュリティ性においては、米国NIST*1、HIPAA*2、英国CREST*3、欧州GDPR*4などの各国ガイドラインおよび法制度、PCIDSS*5などの国際的な業界規格、CVE*6、CWE*7、CVSS*8 といったセキュリティ報告の国際規格および、OWASP Top 10*9、CWE/SANS Top25*10 といった国際脆弱性検査標準に準拠した調査・診断・報告を実施しますので、安心してご利用いただけます。

また、他のソリューションに比べ迅速なプロジェクト遂行が可能となるため、診断に必要な期間は国内サービスの1/3、コストも1/3程度に削減され、脆弱性診断スコープは3倍と高品質のサービスを提供できます。

*1 National Institute of Standards and Technology(アメリカ国立標準技術研究所)

*2 Health Insurance Portability and Accountability Act(医療保険の携行・責任に関する法律)

*3 The Council of Registered Ethical Security Testers(英国の侵入テストのための業界団体)

*4 General Data Protection Regulation(EU 一般データ保護規則)

*5 Payment Card Industry Data Security Standard(PCI データセキュリティスタンダード)

*6 Common Vulnerabilities and Exposures(共通脆弱性識別子)

*7 Common Weakness Enumeration(共通脆弱性タイプ一覧)

*8 Common Vulnerability Scoring System(共通脆弱性評価システム)

*9 Open Web Application Security Project Top10(最重大 Web アプリケーションリスク TOP10)

*10 Common Weakness Enumeration/SysAdmin,Audit, Network, Security(プログラミングエラーTop25)

なお、CEL社は、機械学習・AIの応用により品質・スピード・コスト競争力を備えた脆弱性診断・ペネトレーションテストサービスを提供するため、High-Tech Bridge SA(米国・スイス、代表

者:Ilia Kolochenko、以下「HTB 社」)との間で、日本国内における『ImmuniWeb® AI Platform』*11販売に関する独占契約を締結しております。CEL社とHTB社との独占契約の内容、HTB社の概要、取り組みの目的など詳細につきましては、当社が2019年2月18日付けで公表いたしました「株式会社CELがHigh-Tech Bridge SA(スイス・米国)と国内独占販売契約を締結 / 機械学習・AIを応用した脆弱性診断・ペネトレーションテストサービスを提供」をご参照ください。

*11 『ImmuniWeb® AI Platform』(HTB 社アプリケーションセキュリティテスト自動化ソリューションの総称)

当社グループは、様々な先端技術を導入し、各事業パートナーとの最適な連携関係を構築することで、株主価値の最大化を目指してまいります。



会社名 :株式会社ショーケース(Showcase Inc.) 東証 1 部 証券コード:3909

所在地 :東京都港区六本木 1-9-9 六本木ファーストビル 14F

代表者 :代表取締役社長 永田 豊志

事業内容:①マーケティングSaaS事業:クラウド型のWebマーケティング支援サービス「Navicast」シリーズとセキュリティ対策サービス「Protech」シリーズ提供ほか ②広告・メディア事業:独自のDMPによるオンライン広告サービスと「bitWave」をはじめとする自社メディア運営 ③新領域事業:RPA による業務自動化支援、業界特化型SaaSなど ④投資事業(株式会社 Showcase Capital):国内外における技術ベンチャーへの投資事業 ⑤人材事業(株式会社レーザービーム):人材紹介事業、各種業務支援

URL :<https://www.showcase-tv.com>



会社名 :株式会社CEL(CEL LTD.)

所在地 :東京都港区赤坂1-14-11

代表者 :代表取締役社長 田中翔一郎

株主 :株式会社バルクホールディングス 100%

事業内容:サイバーセキュリティリスクアセスメント事業

URL :<https://celab.co.jp/>



会社名 :High-Tech Bridge SA

所在地 :World Trade Center II 29, Route de Pré-Bois, CH-1215 Geneva

代表者 :Iliia Kolochenko

事業内容:Global provider of web and mobile security testing and security ratings

URL :<https://www.htbridge.com/>

2019年4月8日

当社子会社 Strategic Cyber Holdings LLC

IRI/BBT グループ代表の藤原洋氏がアドバイザーリーボードメンバーに就任

https://www.vlcholdings.com/wp/wp-content/uploads/2019/04/PR20190408_2.pdf

藤原氏は、インターネット黎明期からの豊富な実績・経験、サイバー環境や IT に関する幅広く高い見識を有しており、これらの分野における有識者として、これまでに数々の要職を歴任しております。また、同氏は第 4 次産業革命が進展するなかで、国内産業のIoT・AI技術を適用したビジネスモデルへの転換を最重要視し、IRI/BBT グループでは、業界のなかで先駆けて、これらの技術基盤となる5Gインフラを活用し、第4次産業革命を先導するテクノロジー環境を提供しております。さらに、同氏は日本のサイバーセキュリティを中心とするテクノロジー・パートナー国としてイスラエルとの連携を重視しており、IRIの持株会社としてInternet Research Institute Ltdをイスラエルに設立し、2018年8月にアジア企業初のテルアビブ証券取引所への株式上場を実現させました。

SCHのアドバイザーリーボードメンバーには、有識者として2018年5月にデイビッド・ヘラー氏※1が、同年8月にフランク J・シルフォ氏※2がそれぞれ就任しており、これに藤原氏が加わることで、第4次産業革命を契機とする飛躍的な成長に向けた有益な助言や、サイバーセキュリティ事業との親和性の高いIRI/BBTグループとの連携強化等が期待でき、SCHの事業基盤がさらに強化されます。

なお、本件と並行して、IRIとSCH及びサイバージム間において、本日付でサイバーセキュリティ専用トレーニング施設「ハイブリッドアリーナ(東京都新宿区)」の共同運営等にかかる諸契約を締結しております。この共同事業にはBBTも参画し、当事者間の連携による事業拡大を目指します。

◆藤原氏略歴

藤原 洋(ふじわら ひろし)氏

1954年福岡県生まれ。1977年京都大学理学部卒業。東京大学工学博士(電子情報工学)

<現職>

(株)ブロードバンドタワー 代表取締役会長兼社長CEO

(一財)インターネット協会 理事長・IoT推進委員長

(株)インターネット総合研究所 代表取締役所長

(株)ナノオプト・メディア 代表取締役社長

慶應義塾大学環境情報学部特別招聘教授、SBI大学院大学副学長

<主な経歴>

日本アイ・ビー・エム(株)、(株)日立エンジニアリング、(株)アスキーを経て、1996年12月(株)インターネット総合研究所を設立。同社代表取締役所長に就任、2008年7月(株)ナノオプト・メディア代表取締役社長に就任、2012年4月(株)ブロードバンドタワー代表取締役会長兼社長CEO に就任。現在、(一財)インターネット協会理事長、慶應 義塾大学環境情報学部特別招聘教授、SBI 大学院大学副学長を兼務。2011年4月独立行政法人宇宙航空研究開発機構(JAXA)宇宙科学評議会評議員、2013年12月総務省ICT新事業創出推進会議構成員、2014年1月同省電波政策ビジョン懇

談会構成員、2016年10月同省新世代モバイル通信システム委員会構成員(現任)、2018年12月同省デジタル変革時代のグローバルICT戦略懇談会構成員(現任)に就任。

<代表著書>

1998年『ネットワークの覇者』日刊工業新聞社、2009年『科学技術と企業家の精神』岩波書店、2010年『第4の産業革命』朝日新聞出版、2014年『デジタル情報革命の潮流の中で～インターネット社会実現へ向けての60年自分史～』アスペクト、2016年『日本はなぜ負けるのか～インターネットが創り出す21世紀の経済力学～』インプレスR&D、2018年『全産業「デジタル化」時代の日本創生戦略』PHP研究所、『数学力で国力が決まる』日本評論社、他多数。

※1.デイビッド・ヘラー氏(Mr. David Heller)

イスラエルの大手ベンチャーキャピタル、Vertex Ventures Israelのゼネラルパートナー。日本の投資家向けのイスラエルで最初のベンチャーキャピタルファンドの設立及び運営の経験も持ち、イスラエル国内外でベンチャーキャピタル投資の分野で20年以上にわたり広範囲に活躍。エルサレムのヘブライ大学で法学士を取得後、イスラエルでは法律事務所のパートナーとして、M&A取引を専門とし、アジア関連の取引担当を務めた。また、京都大学で法学修士を取得後、日本の弁護士事務所にも在籍。

※2.フランク J・シルフォ氏(Mr.Frank J.Cilluffo)

米国ジョージワシントン大学アソシエイトヴァイスプレジデント兼サイバー&国土安全保障センター長。元米国国土安全保障担当大統領補佐官。また、米国大統領諮問委員会(National Council of Advisors)議長のほか、国家安全保障諮問委員会をはじめとする米国政府及び非営利団体が主催するさまざまな国家安全保障関連委員会の委員などの要職を歴任。

2019年4月8日

当社子会社Strategic Cyber Holdings LLC 株式会社インターネット総合研究所とハイブリッドアリーナの販売等協業にかかる 契約を締結し、ブロードバンドタワーが本事業に参画

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/04/PR20190408.pdf>

2019年1月29日付「当社子会社 Strategic Cyber Holdings LLC、株式会社インターネット総合研究所とハイブリッドアリーナの販売等協業に向け基本合意」にて公表いたしましたとおり、当社連結子会社Strategic Cyber Holdings LLC(本社:米国デラウェア州、代表者:CEO 石原紀彦/以下「SCH」といいます。)は、株式会社インターネット総合研究所(本社:東京都新宿区、代表者:代表取締役所長 藤原洋/以下「IRI」といいます。)と、サイバーセキュリティ専用 トレーニング施設『ハイブリッドアリーナ』の販売及びライセンス供与、並びに本アリーナを通じた協業に向けた基本合意書を締結いたしました。

1.本件契約の概要

(1) 両社が主催するサイバーセキュリティなどの教育・トレーニングの相互販売 (2) ソリトンによる SCH 向け顧客紹介

2019年5月8日

当社子会社Strategic Cyber Holdings LLC株式会社ソリトンシステムズと販売提携、サイバーセキュリティ教育・トレーニングなどセキュリティソリューションの提供で協業

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/05/PR20190508.pdf>

1.本件契約の概要

(1) 両社が主催するサイバーセキュリティなどの教育・トレーニングの相互販売

(2) ソリトンによるSCH向け顧客紹介



株式会社ソリトンシステムズ（1979年設立、東証1部）

1979年の設立以来、ソリトンはIT・エレクトロニクス業界にあって、常に新しい技術トレンドを見据え、いくつもの「日本で初めて」を実現してきました。近年は、認証を中心としたITセキュリティからサイバー対策製品まで、また、携帯電話回線やWi-Fiを利用したハイビジョン・レベルの映像伝送システムなどに取り組んでおります。国産メーカーとして、オリジナルの「もの創り」、「独創」にこだわった製品とサービスを提供しております。

<https://www.soliton.co.jp/>

2019年5月15日

決算発表予定日に関するお知らせ

決算発表は明日に延期しました。

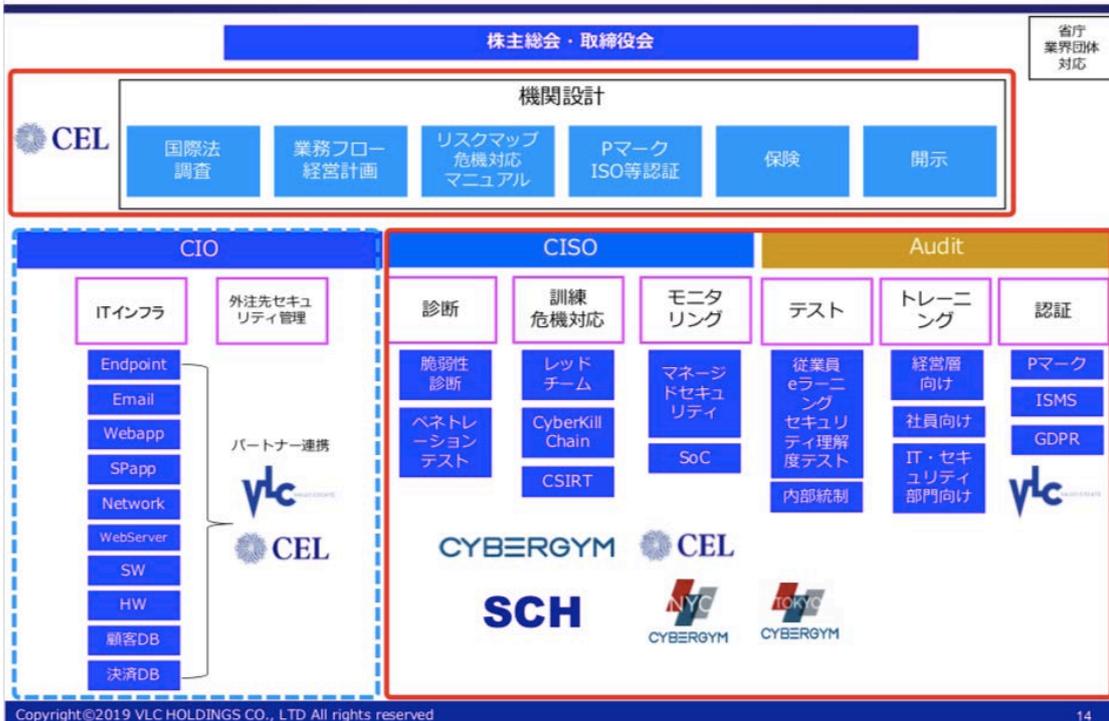
<https://ssl4.eir-parts.net/doc/2467/tdnet/1709031/00.pdf>

2019年5月16日

株式会社バルクホールディングス 2019年3月期 決算説明資料

<https://ssl4.eir-parts.net/doc/2467/tdnet/1709455/00.pdf>

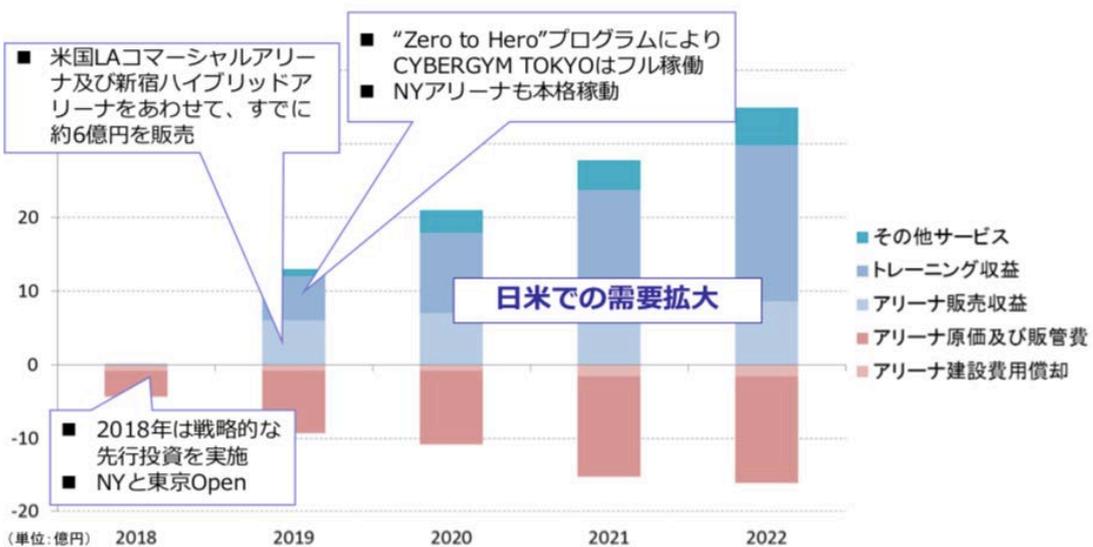
セキュリティ事業のサービスマップ



SCHの収益モデル



アリーナの販売（継続サポート）、アリーナでのトレーニング提供、その他付加価値の高いサービス提供が収益の源泉。2018年に先行投資を実施。市場での需要拡大は更に加速しており、2019年から本格的に収益に貢献



◆Keypair Inc.（韓国・英国）と国内独占販売契約を締結し、世界初の非接触カード型仮想通貨ウォレットと店舗向け決済ソリューションを提供（19/1/16）

CELと韓国Keypair Inc. との間で、日本国内における KeyWallet Touch とKeypair 社が開発する店舗向け仮想通貨決済ソリューションの販売に関する独占契約を締結。大韓民国国家情報院（National Intelligence Service）、Samsung などのパートナーを有するKeypair 社は、2018年6月に、セキュリティチップ搭載型の NFC 対応カード型仮想通貨ウォレット『KeyWallet Touch』を、全世界に向けて販売開始。販売開始以降、韓国、米国、スイス、台湾、シンガポールおよび日本など、すでにグローバルで 20 社を超える企業にその技術を提供



Copyright©2019 VLC HOLDINGS CO., LTD All rights reserved

19

◆米国LAコマーシャルアリーナにかかる販売契約及び運用サポート等契約の締結（19/1/28）

本件契約の概要

- (1) Sales agreement（相手先と SCH 間で締結）
コマーシャルアリーナの販売契約
- (2) Licensing agreement（相手先とサイバージム間で締結）
サービスエリア等のライセンス契約
- (3) Service level agreement（相手先と SCH 及びサイバージムの三者間で締結）
アップグレード・保守メンテナンス等の継続運用サポート

LA コマーシャルアリーナの概要

名称： CYBERGYM LA（仮称）

開設場所：米国カリフォルニア州
ロサンゼルス市内

開設予定：2019年7月～8月



アリーナイメージ

Copyright©2019 VLC HOLDINGS CO., LTD All rights reserved

20

◆テクノプロ・デザイン社とサイバーセキュリティ・エキスパートの育成事業で協業（19/2/4）

SCHが国内最大規模の技術系人材サービスを提供する(株)テクノプロの最大規模の社内カンパニーであるテクノプロ・デザイン社と、サイバーセキュリティエキスパートの育成・派遣事業で協業し、双方の顧客に対して、共同でサイバーセキュリティに関連したサービスの提供を行うことで合意。「CyberGym's Zero to 'Hero」をベースとした実践的かつ体系的なトレーニングをテクノプロ・デザイン社のエンジニアに提供

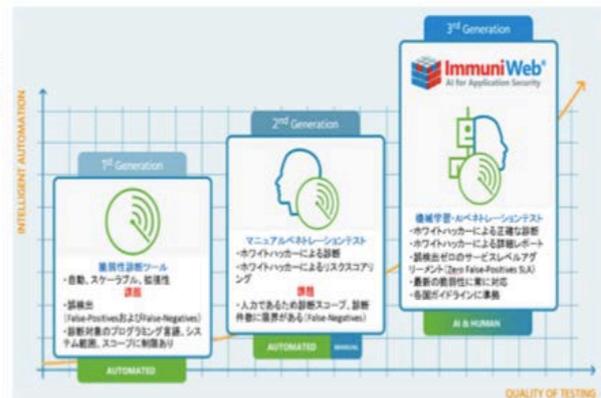
2020年6月までに100名規模のサイバーセキュリティエキスパートの育成を目指す



◆ High-Tech Bridge SA（スイス・米国）と国内独占販売契約を締結 ～機械学習・AIを応用した脆弱性診断・ペネトレーションテストサービスを提供～（19/2/18）

CELがスイスのハイテック・ブリッジ社とセキュリティサービス「ImmuniWeb AI Platform」の国内独占販売契約を締結。ハイテック・ブリッジ社はWEBセキュリティテストで国際的に高い評価を誇る企業。機械学習・AIの応用した脆弱性診断・ペネトレーションテストサービスを日本国内で独占的に提供

他のソリューションに比べ迅速にプロジェクト遂行が可能になるため、診断期間に必要な時間は国内サービスの1/3、コストも1/3程度に削減され、脆弱性診断スコープは3倍と高品質のサービスを提供を実現

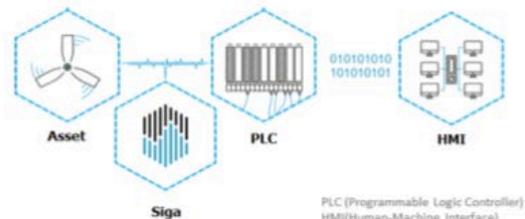


◆『SIGA Platform』による AI を用いた制御システム向け 初期障害検出サービスの提供開始 (19/2/19)

SCHは、日本国内及び米国において、OTソリューションとして、SIGA OT Solutions (イスラエル) の『Siga Platform』によるAIを用いた産業制御システム向け初期障害検出サービスの提供を開始。なお、SCHは本サービスの日本における独占的取扱事業者

◆SIGA OT Solutions

SIGA OT Solutions社は、2014年にイスラエルで設立されたグローバルセキュリティ企業。同社経営陣の重要インフラセキュリティに対する知見とその革新的なサービスは電力発電所・水力発電所・石油プラント・化学プラント・ビルディングシステムなどを運営する多くのグローバル企業に採用されており、2018年には米IT調査会社Gartnerによって『Cool Vendors in Industrial IoT and OT Security』に選出



◆ショーケース社と業務提携し、CELが同社とサイバーセキュリティ分野におけるサービス連携を開始 (19/4/2)

CELとショーケース社の協業で、機械学習・AIを活用した脆弱性診断サービス「ZEIJAX」の提供を開始

他のソリューションに比べ迅速にプロジェクト遂行が可能で、診断期間に必要な時間は国内サービスの1/3、コストも1/3程度に削減され、脆弱性診断スコープは3倍と高品質のサービス提供が実現

高い品質と実績



◆インターネット総合研究所とハイブリッドアリーナの販売等協業にかかる契約を締結、ブロードバンドタワーも本事業に参画（19/4/8）
◆IRI/BBT グループ代表の藤原洋氏がSCHのアドバイザーボードメンバーに就任（19/4/8）

【アリーナ販売】SCH→IRI

【運営サポート】SCH/CG社→IRI

→ホワイトハッカーの提供とプロモーション支援

【サービス提供】IRI/BBT→顧客

【サイバーセキュリティスペシャリストの育成】
SCH/CG社→IRI/BBTグループ内エンジニアを育成

ハイブリッドアリーナの概要

名称：未定

開設場所：東京都新宿区

開設予定：2019年7月～8月頃を目途



◆ソリトンシステムズと販売提携、サイバーセキュリティ教育・トレーニングなどセキュリティソリューションの提供で協業（19/5/8）

SCHとソリトン社との間でサイバーセキュリティ分野を中心とする教育・トレーニングの販売提携契約、並びにソリトン社の顧客基盤及び販売ネットワークを活用したSCHソリューションの紹介契約を締結

【具体的な協業の概要】

- ・両社が主催するサイバーセキュリティなどの教育・トレーニングの相互販売
- ・ソリトン社によるSCH向け顧客紹介

【ご参考】

◆株式会社ソリトンシステムズとの情報セキュリティ分野におけるパートナー契約の締結（18/11/9）
ハルクにおいて、ソリトン社とそれぞれが提供する情報セキュリティ分野におけるサービスを相互の顧客に対して販売し、サービスラインナップの拡充を図る



2019年5月16日

2019年3月期 決算短信〔日本基準〕(連結)

<https://ssl4.eir-parts.net/doc/2467/tdnet/1709457/00.pdf>

(百万円未満切捨て)

1. 2019年3月期の連結業績(2018年4月1日~2019年3月31日)

(1) 連結経営成績

(%表示は対前期増減率)

	売上高		営業利益		経常利益		親会社株主に帰属する当期純利益	
	百万円	%	百万円	%	百万円	%	百万円	%
2019年3月期	1,050	4.2	△380	-	△398	-	△411	-
2018年3月期	1,008	△41.1	15	△39.9	19	△14.0	42	538.2

(注) 包括利益 2019年3月期 △408百万円 (-%) 2018年3月期 42百万円 (274.0%)

	1株当たり 当期純利益	潜在株式調整後 1株当たり当期純利益	自己資本 当期純利益率	総資産 経常利益率	売上高 営業利益率
	円 銭	円 銭	%	%	%
2019年3月期	△49.43	-	-	-	-
2018年3月期	5.73	-	6.2	2.1	1.5

(参考) 持分法投資損益 2019年3月期 0百万円 2018年3月期 2百万円

(2) 連結財政状態

	総資産	純資産	自己資本比率	1株当たり純資産
	百万円	百万円	%	円 銭
2019年3月期	1,961	1,441	73.5	160.38
2018年3月期	962	714	74.1	95.19

(参考) 自己資本 2019年3月期 1,440百万円 2018年3月期 713百万円

(3) 連結キャッシュ・フローの状況

	営業活動による キャッシュ・フロー	投資活動による キャッシュ・フロー	財務活動による キャッシュ・フロー	現金及び現金同等物 期末残高
	百万円	百万円	百万円	百万円
2019年3月期	△290	△886	1,090	322
2018年3月期	△15	△195	50	409

2. 配当の状況

	年間配当金					配当金総額 (合計)	配当性向 (連結)	純資産配当 率(連結)
	第1四半期末	第2四半期末	第3四半期末	期末	合計			
2018年3月期	円 銭	円 銭	円 銭	円 銭	円 銭	百万円	%	%
2019年3月期	-	0.00	-	0.00	0.00	-	-	-
2020年3月期(予想)	-	0.00	-	0.00	0.00	-	-	-

3. 2020年3月期の連結業績予想(2019年4月1日~2020年3月31日)

(%表示は通期は対前期同四半期増減率)

	売上高		営業利益		経常利益		親会社株主に帰属する当期純利益		1株当たり 当期純利益
	百万円	%	百万円	%	百万円	%	百万円	%	円 銭
通期	2,394	127.8	101	-	99	-	57	-	6.56

※当社は年次での業績管理を行っていることから、当期より第2四半期(累計)の連結業績予想開示を省略いたします。

2019年5月28日

当社子会社Strategic Cyber Holdings LLC『OT向けサイバーセキュリティトレーニング』の提供を開始

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/05/PR20190528.pdf>

本トレーニングでは、トレーニングアリーナ内に設けた設備や制御機器を対象にレッドチーム※2が、下記のような複雑かつ最先端のサイバー攻撃を仕掛けます。受講者の皆さまには、攻撃シナリオの理解とその防御、攻撃を受けた場合の影響などについて、実践的かつ体系的な知識・スキルを習得して頂きます。

ートレーニングにおいて実行されるサイバー攻撃の例ー

- ・ 誤った監視データを送信することによって、HMI※3と PLC※4間で通信異常を起こす。
- ・ ITネットワークから分散ネットワークにアクセスし、PLCに偽コマンドを送信し、設備に誤った信号を送る。
- ・ PLCのIPアドレスを変更する。
- ・ HMIへDOS 攻撃を仕掛け、HMIに誤った情報を表示する。
- ・ HMIにウィルスを仕掛け、身代金を要求する。

※1.OT(Operational Technology)…社会インフラにおいて、必要な製品や設備、システムを最適に動かすための制御・運用技術

※2.レッドチーム…攻撃・防御演習において、攻撃側をレッドチーム、防御側をブルーチームと呼びます。

※3.HMI(Human Machine Interface)…デバイスの各工程を制御、監視、管理、視覚化するための装置やソフトウェアの総称

※4.PLC(Programmable Logic Controller)…制御装置の一種



Kinetic Modelの詳細:



※5.SCADA (Supervisory Control And Data Acquisition) …産業制御システムの種類

※6.Kinetic Model…動態模型

2019年5月29日

投資損失引当金の計上に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1714511/00.pdf>

当社の連結子会社であるStrategic Cyber Holdings LLCに対する出資について、先行投資による同社の純資産額の減少を踏まえ、投資損失引当金を計上いたします。当社といたしましては、すでに受注済みの複数の大型案件もあることなどから、今後、同社の業績は向上するものと判断しておりますが、財務健全性の観点から、当該子会社株式に対する投資 損失引当金繰入額167百万円を特別損失として計上することといたしました。

2019年6月5日

取締役人事に関するお知らせ

<https://ssl4.eir-parts.net/doc/2467/tdnet/1718376/00.pdf>

1. 取締役候補者

(1) 取締役候補者

氏名	新役職名	現役職名	選任の種別
石原 紀彦	代表取締役社長	同左	重任
松田 孝裕	取締役	同左	重任
田中 翔一朗	取締役	同左	重任
遠藤 典子	社外取締役	-	新任

(注) 1.各取締役候補者と当社との間には、特別の利害関係はありません。

2.社外取締役候補者の遠藤典子氏は、2018年1月より、当社子会社であるStrategic Cyber Holdings LLCの非業務執行役員を務めております。

(2) 新任取締役候補者の略歴等

氏名 (生年月日)	略歴等	所有 株式数
遠藤典子 (1968年5月6日生)	1994年6月 株式会社ダイヤモンド入社 2004年4月 国立大学法人九州大学東京事務所長・ディレクター兼務 2006年4月 株式会社ダイヤモンド週刊ダイヤモンド編集部副編集長 2013年9月 国立大学法人東京大学政策ビジョン研究センター客員研究員 2015年4月 学校法人慶應義塾大学大学院政策・メディア研究科特任教授(現任) 2016年6月 株式会社NTTドコモ社外取締役(現任) 2018年1月 Strategic Cyber Holdings LLC Board member(現任) 2018年7月 株式会社アインホールディングス社外取締役(現任) (重要な兼職の状況) 学校法人慶應義塾大学大学院政策・メディア研究科特任教授 株式会社NTTドコモ社外取締役 株式会社アインホールディングス社外取締役 Strategic Cyber Holdings LLC Board member(非常勤)	-株

2. 就任予定日

2019年6月27日(木)

2019年6月10日

2019年定時株主総会招集通知

<https://ssl4.eir-parts.net/doc/2467/tdnet/1719782/00.pdf>

議案及び参考事項

第1号議案 取締役4名選任の件

取締役全員（6名）は、本総会終結の時をもって任期満了となります。つきましては、取締役4名の選任をお願いするものであります。

取締役候補者は、次のとおりであります。

候補者番号	氏名 (生年月日)	略歴、地位、担当及び重要な兼職の状況	所有する 当社の 株式数
1	石原 紀彦 (1977年5月4日生)	2001年4月 ゴールドマン・サックス・アセット・マネジメント株式会社入社 2004年8月 ゴールドマン・サックス証券株式会社入社 2009年2月 日本コアパートナー株式会社取締役副社長 2011年1月 株式会社アトミックメディア取締役 2011年3月 サンインベストメント合同会社設立 代表社員(現任) 2013年9月 みやこキャピタル株式会社取締役(現任) 2014年4月 サンインベストメント株式会社設立 代表取締役(現任) 2014年6月 株式会社アトミックメディア代表取締役 2017年3月 株式会社アトミックメディア取締役 2017年6月 当社取締役 2018年1月 当社代表取締役社長(現任) 2018年1月 Strategic Cyber Holdings LLC Chairman of the Board & CEO(現任) 2018年9月 株式会社CEL取締役(現任) (重要な兼職の状況) Strategic Cyber Holdings LLC Chairman of the Board & CEO サンインベストメント合同会社 代表社員(非常勤) サンインベストメント株式会社 代表取締役(非常勤) 株式会社CEL 取締役(非常勤)	17,000株

候補者番号	氏名 (生年月日)	略歴、地位、担当及び重要な兼職の状況	所有する 当社の 株式数
2	松田 孝裕 (1960年5月20日生)	1983年4月 富士通株式会社入社 2003年11月 ソフトブレーション株式会社入社 2004年3月 同社取締役副社長 2005年6月 同社代表取締役社長 2008年6月 ティ・エムコンサルティング株式会社設立 代表取締役(現任) 2011年4月 コムチュア株式会社常務取締役 2012年5月 株式会社エアウィーヴ取締役副社長 2014年9月 同社代表取締役社長 2018年6月 当社取締役(現任) 2018年11月 Strategic Cyber Holdings LLC日本支社代表(現任) (重要な兼職の状況) Strategic Cyber Holdings LLC 日本支社代表 ティ・エムコンサルティング株式会社 代表取締役(非常勤)	一株
3	田中 翔一郎 (1987年7月30日生)	2010年7月 SAPジャパン株式会社入社 2012年3月 オートノミー株式会社(現 日本ビューレット・パカード株式会社)入社 2013年7月 Tanaakk株式会社設立 代表取締役社長(現任) 2018年6月 当社取締役(現任) 2018年9月 株式会社CEL代表取締役社長(現任) (重要な兼職の状況) 株式会社CEL 代表取締役社長 Tanaakk株式会社 代表取締役社長(非常勤)	16,500株

招集ご通知より

候補者番号	氏名 (生年月日)	略歴、地位、担当及び重要な兼職の状況	所有する 株式数
4	【新任】 遠藤 典子 (1968年5月6日生)	1994年6月 株式会社ダイヤモンド入社 2004年4月 国立大学法人九州大学東京事務所長・ディレクター兼務 2006年4月 株式会社ダイヤモンド 週刊ダイヤモンド編集部副編集長 2013年9月 国立大学法人東京大学政策ビジョン研究センター客員研究員 2015年4月 学校法人慶應義塾大学大学院政策・メディア研究科特任教授(現任) 2016年6月 株式会社NTTドコモ社外取締役(現任) 2018年1月 Strategic Cyber Holdings LLC Board member(現任) 2018年7月 株式会社アインホールディングス社外取締役(現任) (重要な兼職の状況) 学校法人慶應義塾大学大学院政策・メディア研究科特任教授 株式会社NTTドコモ 社外取締役 株式会社アインホールディングス 社外取締役 Strategic Cyber Holdings LLC Board member(非常勤)	一株

第2号議案 監査役2名選任の件

本定時株主総会終結の時をもって、監査役清水勝士氏は任期満了となり、また、監査役野口基宏氏が辞任されますので、新たに監査役2名の選任をお願いするものであります。

また、本議案に関しましては、監査役会の同意を得ております。

監査役候補者は、次のとおりであります。

候補者番号	氏名 (生年月日)	略歴、地位及び重要な兼職の状況	所有する 株式数
1	【新任】 平山 剛 (1980年8月1日生)	2004年4月 株式会社ピラミッドフィルム入社 2007年6月 監査法人トーマツ(現 有限責任監査法人トーマツ)入所 2009年12月 公認会計士登録 2009年12月 弁護士登録 2009年12月 平山剛公認会計士事務所設立 代表(現任) 2010年1月 伊藤 見富法律事務所/モリソンフォスター 外国法事務弁護士事務所入所 2012年10月 株式会社オモロキ取締役(現任) 2015年1月 株式会社プレイブソフト取締役 2015年3月 タイラカ総合法律事務所設立 代表(現任) 2015年4月 慶應義塾大学総合政策学部非常勤講師 2017年6月 当社社外取締役(現任) (重要な兼職の状況) タイラカ総合法律事務所 代表 平山剛公認会計士事務所 代表 株式会社オモロキ 取締役	2,800株
2	【新任】 小松 祐介 (1974年7月2日生)	1997年6月 公認会計士大浦俊一事務所入所 2001年6月 税理士登録 2001年7月 小松祐介税理士事務所(屋号 アークス総合会計事務所)設立 代表(現任) 2005年2月 KTAX株式会社代表取締役(現任) 2016年5月 東洋通信工業株式会社監査役(現任) (重要な兼職の状況) アークス総合会計事務所 代表 KTAX株式会社 代表取締役 東洋通信工業株式会社 監査役	一株

第3号議案 取締役の報酬額改定の件

現在の取締役の報酬額は、2001年6月29日開催の第7期定時株主総会において、年額80百万円以内とご承認いただき今日に至っておりますが、その後の経済情勢の変化等諸般の事情を考慮し、取締役の報酬額を200百万円以内（うち社外取締役分は30百万円以内）と変更させていただきたいと存じます。

なお、取締役の報酬額には、従来どおり使用人兼務取締役の使用人分給与は含まないものとしたと存じます。

以上

主要株主が入れ替わった。日本トラスティサービス信託銀行株式会社がいなくなり、新たに第5位(1.5%)で株式会社HATASE HOLDINGSがでランクイン。

2. 会社の株式に関する事項（2019年3月31日現在）

(1) 発行可能株式総数 25,288,000株

(2) 発行済株式の総数 8,984,000株

(注) 2018年7月11日付で発行した第3回及び第4回新株予約権（第三者割当）が、当事業年度において全数行使されたことにより、発行済株式の総数は1,490,000株増加しております。

(3) 株主数 4,968名

(4) 大株主

株主名	持株数	持株比率
西澤管財株式会社	1,000,000株	11.1%
村松澄夫	916,700株	10.2%
松井証券株式会社	194,700株	2.2%
株式会社SBI証券	134,100株	1.5%
株式会社HATASE HOLDINGS	133,500株	1.5%
米田豊	111,000株	1.2%
カブドットコム証券株式会社	109,700株	1.2%
マネックス証券株式会社	80,000株	0.9%
金本康来	76,500株	0.9%
米田研介	76,200株	0.8%

2019年7月1日

2019年3月期 有価証券報告書

https://ssl4.eir-parts.net/doc/2467/youho_pdf/S100GDZX/00.pdf

2019年7月4日

共同事業パートナーであるCYBERGYM社が ニューヨーク州電力公社等とパートナーシップを締結

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/07/PR20190704.pdf>

ニューヨーク州プレスリリース(抄訳)

2019年7月1日付「クオモ知事、ニューヨークとイスラエルの一連の経済開発パートナーシップを発表」

先週のSolidarity Tripの結果、UAV/ドローン(無人偵察機)、交通機関、エネルギー、サイバーセキュリティ、金融技術および医療 技術と研究にフォーカスしたパートナーシップを締結することとなった。17のイスラエル企業が、6つのニューヨーク州の機関およびその他のパートナーと協力して、双方の革新と経済的関係を強化。

複数ある共同発表の中で、サイバーセキュリティに関しては、「ニューヨーク州立大学のニューヨークとイスラエル国土安全保障とサイバーセキュリティパートナーシップ拡大」および「金融技術(FinTech)協力に関するニューヨークとイスラエルの間の協定」が挙げられており、これに関連してオフィール・ハソンは下記のようにコメントしています。

「CyberGymがニューヨークのエネルギー市場における主要企業であるニューヨーク州電力公社と提携することを光栄に思います。この提携はCyberGymがニューヨークでの拠点を拡大する糧になると同時に、私どもがサポートさせて頂くことでニューヨークの電力企業のサイバーセキュリティレベルも大幅に向上することになります。私どもは今回の覚書の締結によって、ニューヨークにおけるサイバーセキュリティ製品への追加投資が不要となり、長期計画のもとにより安全な市民生活をもたらすものと確信しています。」

2019年7月8日

当社子会社Strategic Cyber Holdings LLC

東芝ITサービス株式会社へAIを用いた『SIGA Platform』を供給

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/07/PR20190708.pdf>

1.本件の目的

SCH は、サイバーセキュリティ分野において世界最高レベルのイスラエルで技術を確立しているCyberGym Control Ltd.(イスラエル ハデラ市、CEO Ofir Hason、以下「CYBERGYM」)との提携により、サイバーセキュリティ専用トレーニング施設を日本及び米国において運営し、実践的かつ体系的なトレーニングを提供するとともに、クライアントがセキュアなビジネス運営を行うためのソリューションとして、『SIGA Platform』をはじめとする各種サイバーセキュリティサービス・コンサルティングを提供しています。

一方で、東芝 IT サービスは長年にわたり実績と信頼を築いてきた24時間365日の全国保守サービス体制による経験とノウハウをベースに、安全で快適なネットワーク環境の構築からセキュリティ、ファシリティサービス、幅広いシステム導入支援、お客さまのビジネスを守り続けるシステム運用・監視サービスまで、IoT時代に対応したワンストップで付加価値の高い各種サービスを提供しています。

本供給を通じて、サイバーセキュリティ分野において、両社の独自の強み・ノウハウを基盤に、全てのモノがインターネットに繋がるIoTの時代を迎えるいま、より付加価値の高いソリューションサービスを確立することで事業拡大が期待できます。SCHにおいては、特に国内における『SIGA Platform』の導入拡大を目指します。

2.本サービスの概要

『SIGA Platform』はセンサーやアクチュエータ※1などのエンドポイントインフラとPLC※2(プログラマブルロジックコントローラ)のネットワークの中間地点に設置されたデータログ取得ハードウェア端末とサーバーにインストールされた専用のソフトウェアの組み合わせで稼働します。

『SIGA Platform』を活用することで、既存の産業制御システムを停止させることなく、PLCで

処理される前の電気信号をAI・マシンラーニングにより検知・解析し、ICS(インシデント・コマンド・システム)における脅威を即座に特定することが可能となり、異常の初期兆候の的確なモニタリングが実現します。

制御機器・システムの正確でリアルタイムな状態把握を可能とする本サービスは、イスラエル電力公社をはじめとする政府機関及び企業での実績が評価され、世界各国で導入されています。国際的イベントが増える中、日本は制御機器やIoT機器のサイバー攻撃に対する対策が不十分であり、日本のユーティリティ企業においてもこの分野の解決策に大きく寄与するものです。

尚、SCHとSIGA OT Solutions(イスラエル、CEO Amir Samoiloff)との間で、日本国内における『SIGA Platform』によるサービスに関する独占契約を本年2月に締結しています。

※1.アクチュエータ: 入力されたエネルギーもしくはコンピュータが出力した電気信号を物理的運動に変換する機械・電気回路を構成する機械要素

※2.PLC(プログラマブルロジックコントローラ): プログラムで定められた順序や条件などに従って設備や機械の動きを制御する装置

東芝ITサービス株式会社

東芝 IT サービスは、IT 機器から IoT 機器まで社会の様々なシステムに関わるサービスを提供する会社であり、高度化するシステムに対し長年培った技術力と実績があります。多様化するお客様ニーズに応えるため、ライフサイクルに沿った 6つのサービスユニットと様々なサービスを組み合わせ、日本全国の 100 を超えるサービス拠点からお客様にフィットしたユニファイドサービスとして 24 時間 365 日、サービスを提供しています。

<https://www.it-serve.co.jp/>

2019年7月18日

株式会社CELがBAP Inc.(ベトナム)とオフショア開発で協業 セキュリティ検査後のシステム開発需要に対応

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/07/PR20190718.pdf>

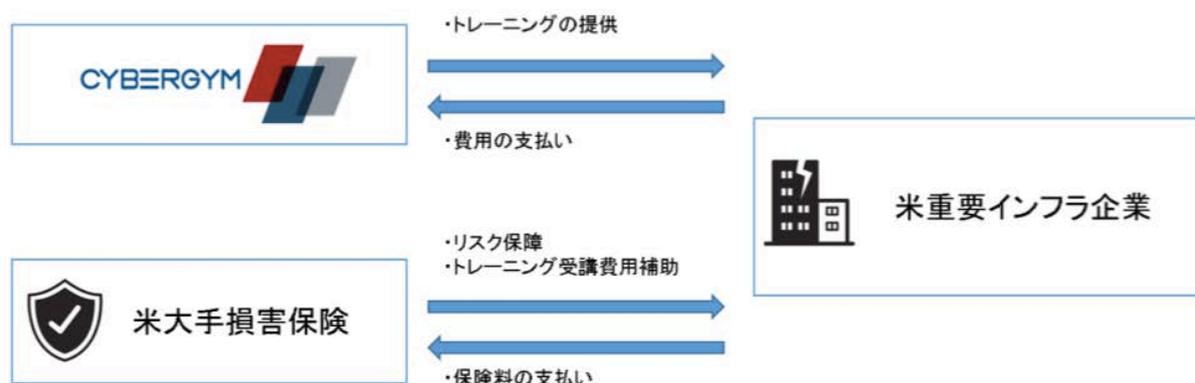
BAP社は2016年に株式会社サイバーエージェント出身のシニアソフトウェアエンジニアであった Dao Ngoc Thanh氏により設立されました。ハノイ工科大学をはじめとしたベトナム国内の優秀な学生を集め、2019年7月現在で160名のエンジニアを抱えるオフショア開発企業です。業務システム(SAP ERP、Salesforce)、WEBアプリケーション、モバイルアプリケーション、ゲームなど、多岐にわたるシステムの開発実績を持ち、日本国内の大手会計事務所や大手情報通信企業に採用されています。

また、当社グループとして、米国、欧州、アジアはセキュリティにおける需要の高成長が期待される重要な市場であることから、各国のテクノロジー企業と連携することにより、各地域の重要インフラ企業等へのソリューション提供を可能とする体制を構築し、その強化と拡大を進めています。

BAP社が本拠地を置くベトナムにおいても、VNR500と呼ばれるベトナム国TOP500の影響力を持つ企業は、日本国内の大手企業と比較しても遜色ないほどの高成長と情報通信分野への投資を実施しており、当社グループとして、今後同地域での需要への対応を計画しています。

2019年7月22日

Strategic Cyber Holdings LLCが米大手損害保険会社と協業 サイバーセキュリティ保険一体型トレーニングの提供で提携



当社子会社Strategic Cyber Holdings LLC(以下「SCH」)は、米国CYBERGYM NYCにおいて米大手損害保険会社と協業し、サイバーセキュリティ保険と一体となったCYBERGYMトレーニングの提供を開始いたしました。CYBERGYM NYCのターゲット顧客である重要インフラ企業は、保険会社による費用補助が受けられることから、サイバートレーニングを受講し易くなります。一方で、保険会社においても、サイバートレーニングを通じて被保険者の対処能力が強化されることから、トレーニング費用の補助額を大幅に上回るサイバー攻撃に起因する損害補償額の低減が期待できます。本ソリューションの当初の設計は、米大手電力会社を対象としておりますが、電力会社をはじめとして、米国の重要インフラ企業などを対象とするサイバーセキュリティ保険一体型のトレーニングを今後提供してまいります。また、SCHは日本市場向けにも同様のソリューション導入を目指します。

なお、米国のサイバー保険市場は2020年までに年間保険料収入ベースで56億ドル規模に成長すると予測されており、業界を問わず米国で情報漏洩被害に遭った企業の平均被害総額は735万ドルで、情報漏洩インシデントの47%は悪意のあるサイバー攻撃によるものであることが明らかになっています。(※JETRO/IPA調べ)

※「米国におけるサイバー保険の現状」JETRO/IPA ニューヨーク <https://www.ipa.go.jp/files/000062714.pdf>

2019年7月24日

[コーポレートガバナンスに関する報告書](#)

<https://ssl4.eir-parts.net/doc/2467/tdnet/1733434/00.pdf>

2019年8月14日

[当社子会社 Strategic Cyber Holdings LLC](#)

[米国市場での ImmuniWeb® AI Platform および SIGA Platform の提供開始](#)

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/08/PR20190814.pdf>

当社子会社のStrategic Cyber Holdings LLC(東京都港区、CEO 石原紀彦、以下「SCH」)は、日本国内のセキュリティ市場における先端ソリューションの成功事例をグローバルに展開するため、米国において『ImmuniWeb® AI Platform』および『SIGA Platform』の提供を開始いたします。

なお、当社子会社の株式会社CELは『ImmuniWeb® AI Platform』の日本における独占的取扱事業者※1であり、SCHは『SIGA Platform』の日本における独占的取扱事業者※2となっております。

※1(2019年2月18日付プレスリリース) 株式会社CELがHigh-Tech Bridge SA(スイス・米国)と国内独占販売契約を締結 機械学習・AI を応用した脆弱性診断・ペネトレーションテストサービスを提供

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/02/PR20190218.pdf>

※2(2019年2月19日付プレスリリース) 当社子会社Strategic Cyber Holdings LLC 『SIGA Platform』によるAIを用いた制御システム向け初期障害検出サービスの提供開始

https://www.vlcholdings.com/wp/wp-content/uploads/2019/02/PR20190219_2.pdf

2019年8月14日

2020年3月期 第一四半期報告書

https://ssl4.eir-parts.net/doc/2467/yuho_pdf/S100GSBS/00.pdf

回次	第25期 第1四半期 連結累計期間	第26期 第1四半期 連結累計期間	第25期
会計期間	自 2018年4月1日 至 2018年6月30日	自 2019年4月1日 至 2019年6月30日	自 2018年4月1日 至 2019年3月31日
売上高 (千円)	223,816	312,363	1,050,835
経常損失(△) (千円)	△14,549	△140,173	△398,189
親会社株主に帰属する四半期(当期)純損失(△) (千円)	△15,420	△143,712	△411,150
四半期包括利益又は包括利益 (千円)	△23,170	△169,762	△408,018
純資産額 (千円)	691,085	1,271,978	1,441,740
総資産額 (千円)	1,000,930	1,764,704	1,961,544
1株当たり四半期(当期)純損失(△) (円)	△2.06	△16.00	△49.43
潜在株式調整後1株当たり四半期(当期)純利益 (円)	—	—	—
自己資本比率 (%)	69.0	72.0	73.5

2019年8月14日

2020年3月期 第一四半期決算短信〔日本基準〕（連結）

<https://ssl4.eir-parts.net/doc/2467/tdnet/1745569/00.pdf>

（百万円未満切捨て）

1. 2020年3月期第1四半期の連結業績（2019年4月1日～2019年6月30日）

（1）連結経営成績（累計）

（％表示は、対前年同四半期増減率）

	売上高		営業利益		経常利益		親会社株主に帰属する 四半期純利益	
	百万円	%	百万円	%	百万円	%	百万円	%
2020年3月期第1四半期	312	39.6	△147	—	△140	—	△143	—
2019年3月期第1四半期	223	△6.4	△15	—	△14	—	△15	—

（注）包括利益 2020年3月期第1四半期 △169百万円（－％） 2019年3月期第1四半期 △23百万円（－％）

	1株当たり 四半期純利益	潜在株式調整後 1株当たり 四半期純利益
	円 銭	円 銭
2020年3月期第1四半期	△16.00	—
2019年3月期第1四半期	△2.06	—

（2）連結財政状態

	総資産	純資産	自己資本比率	1株当たり純資産
	百万円	百万円	%	円 銭
2020年3月期第1四半期	1,764	1,271	72.0	141.48
2019年3月期	1,961	1,441	73.5	160.38

（参考）自己資本 2020年3月期第1四半期 1,271百万円 2019年3月期 1,440百万円

2. 配当の状況

	年間配当金				
	第1四半期末	第2四半期末	第3四半期末	期末	合計
	円 銭	円 銭	円 銭	円 銭	円 銭
2019年3月期	—	0.00	—	0.00	0.00
2020年3月期	—	—	—	—	—
2020年3月期（予想）	—	0.00	—	0.00	0.00

（注）直近に公表されている配当予想からの修正の有無：無

3. 2020年3月期の連結業績予想（2019年4月1日～2020年3月31日）

（％表示は、対前期増減率）

	売上高		営業利益		経常利益		親会社株主に帰属 する当期純利益		1株当たり 当期純利益
	百万円	%	百万円	%	百万円	%	百万円	%	円 銭
通期	2,394	127.8	101	—	99	—	57	—	6.56

（注）1. 直近に公表されている業績予想からの修正の有無：無

2. 当社は年次での業績管理を行っていることから、第2四半期（累計）の連結業績予想開示を省略しております。

2019年8月14日

2020年3月期 第一四半期決算説明資料

<https://ssl4.eir-parts.net/doc/2467/tdnet/1745574/00.pdf>

第1四半期連結決算のポイント



◆売上高は前年同期比39.6%増で着地、既存事業は堅調に推移し、新規事業の売上も計上開始

●セキュリティ事業は、40.0%の増収

【主な要因】

- ・既存のコンサルティング分野が堅調に推移し、新設子会社SCH及びCELの売上が計上開始
- ・サービス開始により当四半期中において稼働が上昇。現在の東京アリーナの稼働率は100%超
- ・㈱テクノプロとサイバーセキュリティ人材の育成・派遣事業における協業契約を締結
- ・SIGA OT Solutions（イスラエル）の『SIGA Platform』によるAIを用いた産業制御システム向け初期障害検出サービスを日本における独占的取扱事業者として提供開始
→2019年7月に東芝ITサービス㈱向けに本サービスを供給開始し、東芝グループとは様々な形での協力を模索中
- ・ImmuniWeb®AI Platformを国内独占提供するCELが既存セキュリティ診断業者を含む15社とリセラー契約を締結し、拡販体制を整備

●マーケティング事業は、39.5%の増収

【主な要因】

- ・セールスプロモーション分野にて、前期からの積極的な営業開拓による新規顧客の獲得に成功し、大幅増収

◆先行投資の影響で販管費が増加し、営業損失を計上

- ・安定的な収益や中長期の受注拡大を期待できる大口・優良顧客の開拓、並びに最適なソリューション提供に向けた良質なパートナーとの関係構築等の足場固め等に経営資源を重点的に投下
- ・サイバーセキュリティの重要性・市場潜在性の理解向上、当社グループのブランド認知向上のため、各種イベントにおける出展・講演やセミナーの企画・実施等のプロモーション活動に注力
- ・中長期的な企業価値の向上を目指し、最先端の技術及びノウハウ等の獲得・新規事業開発のため、資本提携、業務提携及びM&A等の推進・模索並びに市場調査等の先行投資を引き続き積極的に実施

Copyright©2019 VLC HOLDINGS CO., LTD All rights reserved

4

◆『OT向けサイバーセキュリティトレーニング』の需要が拡大

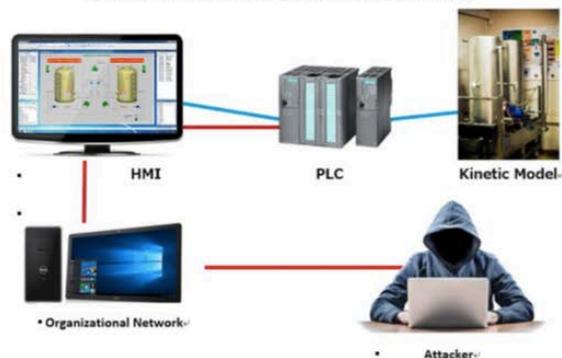
重要インフラ施設や工場において用いられる産業制御システムは、サイバー攻撃の脅威に本格的に直面しており、実効性のあるセキュリティ対策が必要となっております。

そのような中、本サービスは、国内の重要インフラ施設関連事業者や大手製造業など多くの顧客から強い要望を受け開発された「OT向け実践的サイバーセキュリティトレーニングサービス」です。

CYBERGYM SCADA Extensionの論理構成図

トレーニングアリーナ内に設けた設備や制御機器を対象に攻撃チームが、複雑かつ最先端のサイバー攻撃を仕掛けます。

本トレーニングでは攻撃シナリオの理解とその防御、攻撃を受けた場合の影響などについて、実践的かつ体系的な知識・スキルの習得が可能。



Copyright©2019 VLC HOLDINGS CO., LTD All rights reserved

17

2019年8月27日

当社子会社Strategic Cyber Holdings LLC(CYBERGYM TOKYO) サイバーリーズン・ジャパンとサイバーセキュリティ人材育成で協業

<https://www.vlcholdings.com/wp/wp-content/uploads/2019/08/PR20190827.pdf>

子会社のStrategic Cyber Holdings LLC(東京都港区、CEO 石原紀彦、以下「SCH」)は、CYBERGYM TOKYOにおいて、サイバーリーズン・ジャパン株式会社(本社:東京都港区、取締役CEO:シャイ・ホロヴィッツ、以下「サイバーリーズン・ジャパン」)と協業し、両社が有する最先端のノウハウと実績、経験値を融合した新たなサイバー攻撃対策のトレーニングメニューを共同で開発し、2019年10月上旬より提供を開始します。

ITやデジタルが社会に浸透し、デジタル・トランスフォーメーションが急速に進行している昨今、サイバー攻撃は日々巧妙化し、その脅威・被害は深刻化する傾向にあります。一方で、2016年に経済産業省が発表した調査結果では、2020年に情報セキュリティ人材が19万3000人不足すると予想されるなど、企業や組織では深刻なセキュリティ人材の不足が懸念されています。

このような状況をふまえ、最先端かつ実践的な“強いサイバーセキュリティ人材”を育成するためにCYBERGYM TOKYOを運営するSCHとAI(人工知能)を活用したサイバー攻撃対策プラットフォーム「Cybereason」を日本市場向けに提供するサイバーリーズン・ジャパンは、サイバーリーズンのMSSパートナー向けトレーニング、サイバーリーズンの導入企業のセキュリティ担当者向けトレーニングなどを共同で開発・提供することによって、お客様、パートナー様、双方で不足していると言われる高度なサイバーセキュリティ人材を短期に育成し、お客様のデジタル・トランスフォーメーションを安心・安全に推進し、様々な価値創造を実現する事を支援します。

また、SCHは、エンドポイントセキュリティソリューション「Cybereason EDR」の販売において、サイバーリーズン・ジャパンとパートナー契約を締結し、CYBERGYM TOKYOのインシデント対応トレーニングでの「Cybereason EDR」の活用やトレーニング受講者への「Cybereason EDR」の導入を支援します。

SCHは、サイバーリーズン・ジャパンと共にお客様のシステムを安全に保護する最適なトータルセキュリティソリューションの提供で協力し、さらなるセキュリティビジネスの拡大を図ります。



サイバーリーズン・ジャパン株式会社(2016年3月設立)

「Cybereason」は、サイバー攻撃から企業や団体のシステムを安全かつ確実に保護するサイバーセキュリティ対策プラットフォームで、企業・団体内の膨大なデータをあらゆる角度から深く分析する機械学習エンジンとグラフ処理システムを構築、提供します。次世代アンチウイルス(NGAV)、ランサムウェア対策、悪意のあるPowerShellへの対策、EDR機能を搭載するフルスタックの振る舞い検知型ソリューションである「Cybereason」は、これまでにない脅威を可視化し、複雑化する高度なサイバー攻撃を阻止する力をお客様へ提供しています。

<https://www.cybereason.co.jp>

2019年9月2日

当社子会社バルクがISO審査員研修機関のグローバルテクノ社とサイバーセキュリティ分野で提携

https://www.vlcholdings.com/wp/wp-content/uploads/2019/09/PR20190902_01-1.pdf

グローバルテクノ社は、ISO研修で27年の実績を持つ、日本最大級のISO研修機関であります。1992年の創業以来、ISO審査員研修コース受講者数24,294人、ISO内部監査員養成コース受講者数62,404人(2018年10月末現在)を輩出する業界のリーディングカンパニーです。近年は、ISO27001、プライバシーマーク、クラウドセキュリティなどのマネジメントシステム研修コースも提供。また、グループ会社にはISO審査を行う国際システム審査もあり、ISOの多分野で活躍中です。

このたびの業務提携契約の締結により、両社がそれぞれ提供する情報セキュリティ分野におけるサービスを相互の顧客に対して販売することで、顧客により高い付加価値を提供できるとともに、両社の顧客基盤の拡大、営業効率の向上、事業のさらなる発展が期待できるものと考えております。

業務提携の内容等

- ①共同企画による「サイバーセキュリティ講座」の開設、その他相互の経営資源を活かした新規事業・サービス等の創出
- ②それぞれが提供するサービス等にかかる相互の顧客紹介、販売
- ③共同提案、セミナー共催等の営業活動における協業

【相手先の概要】

会社名 :株式会社グローバルテクノ

所在地 :東京都新宿区下落合1-5-22

代表者 :代表取締役社長 砂川 清榮 事業内容:ISO審査員研修事業、ISOに関連するコンサルティングサービス等 URL :<https://www.gtc.co.jp/>

2019年9月2日

当社子会社Strategic Cyber Holdings LLC扶桑電通株式会社と販売提携、サイバーセキュリティ診断の提供で協業

https://www.vlcholdings.com/wp/wp-content/uploads/2019/09/PR20190902_2-1.pdf

扶桑電通は「ソリューション」、「ネットワーク」、「ファシリティ」の3つの事業を核に、システムやネットワークに関する提案から設計・施工・運用・保守まで一貫したソリューションを全国54カ所の拠点で展開しており、中でも「ソリューション」の分野では、長年培ってきたシステム開発、構築ノウハウをベースにした多彩なオリジナルパッケージ群を販売しています。本件取組みを通じて、サイバーセキュリティ分野において、両社の経営資源や独自の強み・ノウハウを活かすことで双方の事業拡大が期待できます。SCHにおいては、特に扶桑電通の顧客基盤やネットワークを通じたセキュリティ診断ソリューションの販売拡大を目指します。

本件の主なサービス

機械学習・AIの応用により品質・スピード・コスト競争力を兼ね備えた脆弱性診断・ペネトレーションテストサービス『ImmuniWeb® AI Platform』を本件の主なソリューションサービスとして取り扱います。尚、当社子会社の株式会社CELとHigh-Tech Bridge SA(米国・スイス、代表者: Iliia Kolochenko)との間で、日本国内における『ImmuniWeb® AI Platform』販売に関する独占契約を本年2月に締結しており、既に当社グループを通じて国内でも多数の企業に提供を行っています。



扶桑電通株式会社(1948年3月設立)

扶桑電通は、「ネットワーク」「ソリューション」「ファシリティ」の3つの事業を柱として、全国54か所の拠点に要員を配し、クライアントの業務についてのコンサルティングからシステム的设计・開発・施工・運用・保守までをワンストップでサービス提供しています。

<https://www.fusodentsu.co.jp/>

2019年9月

Comparative Advantages

株式会社バルクHDの比較優位性は以下のような点である。

- 1、役員陣
- 2、提携している企業
- 3、セキュリティ業界での事業戦略
- 4、現在の時価総額
- 5、株主や機関投資家
- 6、
- 7、
- 8、
- 9、

Link

□内閣サイバーセキュリティセンター

<https://www.nisc.go.jp>

□一般社団法人 日本サイバーセキュリティ・イノベーション委員会

<https://www.j-cic.com>

□NIST アメリカ国立標準技術研究所

<https://www.nist.gov>

□CREST

<https://www.crest-approved.org/index.html>

□IPA 独立行政法人情報処理推進機構

<https://www.ipa.go.jp/cyberj/>

□IPA 独立行政法人 情報処理推進機構 企業のCISOやCSIRTに関する実態調査 2017

<https://www.ipa.go.jp/files/000058850.pdf>

□NPO法人 日本ネットワークセキュリティ協会

<https://www.jnsa.org>

□2016年9月4日 サイバーセキュリティについての閣議決定

<https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf>

□2016年3月 今後のサイバーセキュリティ政策について

http://www.meti.go.jp/shingikai/sankoshin/shinsangyo_kozo/pdf/007_04_02.pdf

□諸外国のサイバーセキュリティ政策

http://www.soumu.go.jp/main_content/000488150.pdf

□2017年1月30日 我が国のサイバーセキュリティの概要

http://www.soumu.go.jp/main_content/000463592.pdf

□2017年3月3日 サイバーセキュリティ研究開発骨子について

http://www.soumu.go.jp/main_content/000488157.pdf

□2015年3月 ニュートン・コンサルティング 企業の情報セキュリティ開示に関する調査

https://www.nisc.go.jp/inquiry/pdf/kaiji_honbun.pdf

- 2018年7月25日 サイバーセキュリティ2018 サイバーセキュリティ戦略本部
<https://www.nisc.go.jp/active/kihon/pdf/cs2018.pdf>

- 2018年7月27日 サイバーセキュリティ戦略
<https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf>

- 金融庁 金融分野におけるサイバーセキュリティ
<https://www.fsa.go.jp/policy/cybersecurity/index.html>

- NEC サイバーセキュリティグローバルトレンド
<https://jpn.nec.com/cybersecurity/journal/02/globaltrend02.html>

- 2017年1月 ダボス会議 Advancing Cyber Resilience Principles and Tools for Boards
http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf

- NISC サイバーセキュリティ戦略 2018の概要
<http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-cs2018-gaiyou.pdf>

- FISC 金融情報システムセンター
<https://www.fisc.or.jp>

- 一般社団法人JPCERT コーディネートセンター
<https://www.jpccert.or.jp>

- 一般社団法人JPCERT コーディネートセンター 研究・調査レポート
<https://www.jpccert.or.jp/research/>

- OWASP
https://www.owasp.org/index.php/Main_Page

- PRACTIAL REVERSE ENGINEERING
<https://repo.zenk-security.com/Reversing%20.%20cracking/Practical%20Reverse%20Engineering.pdf>

- KPMGコンサルティング株式会社 制御システムにおけるサイバーリスクマネジメント態勢の確立と事例紹介
https://www.jpccert.or.jp/present/2018/ICS2018_04_KPMG.pdf

- 三菱シーケンサ はじめてのシーケンサ入門編
<http://www.mitsubishielectric.com/fa/assist/satellite/data/jy997d41501e.pdf>

- KeyWallet Pro
<http://www.keywalletpro.io/>

□ISO Technical Committees

<https://www.iso.org/technical-committees.html>

□サイバー保険by損害保険ジャパン日本興亜

http://www.soumu.go.jp/main_content/000536248.pdf

□Long term growth

http://group30.org/images/uploads/publications/G30_LongtermFinanceEconGrowth.pdf

□パランティアテクノロジー

https://www.principle-c.com/column/global-marketing/palantir-technologies/#_1669646376.1541469965

□2018.10.15オウケイウェイブがパランティアテクノロジーとの協業に向けて株式取得

<https://www.okwave.co.jp/press/20181015-3/>

□VCGTF Virtual Currency Governance Task Force 国際標準化ワーキンググループ

<https://vcgtf.github.io>

□Frank J. Cilliaffo

<https://cchs.gwu.edu/Frank-J-Cilluffo>

Associate Vice President at The George Washington University

(ジョージ・ワシントン大学の副学長)

Special Assistant to the President for Homeland Security

□White and case

<https://www.whitecase.com>

□White and case Japan

<https://www.whitecase.com/ja/law/asia-pacific/japan#about>

1987年創業の外資系弁護士事務所

□法律事務所ZeLo

<http://zelojapan.com>

日本ブロックチェーン協会(JBA)では、本日2017年11月21日付けで新たなリーガルアドバイザーとして法律事務所ZeLoの小笠原 匡隆弁護士にご就任いただきました。

http://jba-web.jp/archives/20171122_new_regal_advisor

□小笠原 匡隆『ブロックチェーンビジネスとICOのフィジビリティスタディ』(2018.10.31)

<https://www.shojihomu.co.jp/publication?publicationId=7118786>

□田村二郎研究会 慶應義塾大学法学部法律学科

<http://jironet.info>

□平成28年2月6日 日本を支える鉄道・航空におけるサイバー攻撃の脅威

http://www.jterc.or.jp/journal/bn/pdf/no72_symposium01.pdf

NISCの監視では各省庁に年間400万件、8秒に1回の割合で不審な通信を受けている

また拡散型攻撃ではなく、標的型攻撃の割合が4割に登る

2015年にサイバーセキュリティ基本法が施行されたが、サイバーセキュリティという用語が使われたのはこの法案が初めて

NISCによる第三者監査は、セキュリティポリシーのPDCAが適切に循環しているかをチェックする『マネジメント監査』と、NISCが疑似的なハッカーになって各省庁の情報システムの中に入って脆弱性をあぶり出し、必要な対策を練るための『ペネトレーションテスト(侵入テスト)』の2種類を行う

2012年のロンドン五輪では2億回を超えるサイバー攻撃があった

□DDoS攻撃

<https://www.shadan-kun.com/blog/measure/2160/>

□The Power of Intangibles

<https://sfmagazine.com/post-entry/may-2017-the-power-of-intangibles/>

□CSIS Center for Strategic & International Studies

<https://www.csis.org/>

□2014年6月 Net Loss : Estimating the Global Cost of Cybercrime by intel security

https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

サイバークライムによる世界の経済的被害額を3750~5750億ドルと推計している。これは世界のGDPの0.5~0.8%に相当する。

□2018年2月21日 Economic Impact of Cybercrime - No Slowing Down by McAfee

https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email

2018年2月21日の調査レポートで、経済的被害額を4450~6000億ドルへと上方修正している。

□Disruptive technologies: Advances that will transform life, business, and the global economy | McKinsey

<https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies>

デジタルイノベーションによって2025年までに世界で14~33兆ドルの経済的価値が生み出され可能性があると考えられる。

□Guide to Cybersecurity Due Diligence in M&A Transactions

<https://www.americanbar.org/products/inv/book/297711517/>

米ヤフーは個人情報流出により、ベライゾンによる買収価格が3億5000万ドルもディスカウントされた。

□National Cyber Security Strategy 2016-2021

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

「英国の安全と経済的繁栄の将来はデジタル基盤に依存している。我々世代にとっての挑戦は、サイバー脅威に対してレジリエントで、かつ機会の最大化とリスクマネジメントに関わる知識と能力を兼ね備えた、繁栄するデジタル社会を作り上げることである」と宣言している。by横浜信一『経営とサイバーセキュリティ』

□Report on Securing and Growing The Digital Economy

<https://iapp.org/resources/article/report-on-securing-and-growing-the-digital-economy/>

米国では、今後10年超にわたるサイバーセキュリティ政策を大統領に提言すべく組成された国家サイバーセキュリティ強化委員会(Commission on Enhancing National Cybersecurity)が2016年に発表されたこのレポートにおいて、「技術の相互接続がデジタル経済にもたらす膨大な利益を認識して、大統領は当委員会にレポート作成を指示した」と述べている。by横浜信一『経営とサイバーセキュリティ』

□横浜信一『経営とサイバーセキュリティ』(2018)

<https://eb.store.nikkei.com/asp/ShowItemDetailStart.do?itemId=D2-00265130B0>

□経済産業省&(独)情報処理推進機構 サイバーセキュリティ経営ガイドラインVer2.0

http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf

□2018年5月28日 IDC Japan株式会社の市場予測

<https://www.idcjapan.co.jp/Press/Current/20180528Apr.html>

セキュリティ製品の2017~2022年の平均市場成長率は3.9%、2022年には3602億円
セキュリティサービスの2017~2022年の平均市場成長率は5.4%、2022年には9870億円

□2018年6月15日 アイ・ティ・アールによる市場予測

<http://www.atmarkit.co.jp/ait/articles/1806/15/news053.html>

アイ・ティ・アール (ITR) は2018年6月14日、国内サイバーセキュリティサービスの市場規模について、実績と予測を発表した。

2017年度の売上金額は対前年度比13.8%増の約2750億円。2018年度も引き続き堅調に伸び、対前年度比12.7%増の約3100億円になると見込む。2017年度から2022年度までの年平均成長率 (CAGR) は8.4%で、2022年度には4100億円を超えると予測した。

□Payment Card Industry Data Security Standard Council

<https://ja.pcisecuritystandards.org/minisite/env2/>

□一般財団法人 日本サイバー犯罪対策センター (JC3)

<https://www.jc3.or.jp>

□Dark Webの謎に迫る | INFORIUM | NTTデータ

https://inforium.nttdata.com/trend_keyword/266.html

□2016年 企業経営のためのサイバーセキュリティの考え方

https://www.nisc.go.jp/active/kihon/pdf/keiei_gaiyou.pdf

□2017年4月18日 サイバーセキュリティ人材育成プログラム

<https://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf>

□NICT-情報通信研究機構

<https://www.nict.go.jp>

□日・イスラエル投資協定 2017年10月5日効力発生

<https://www.mofa.go.jp/mofaj/files/000236608.pdf> (協定)

<https://www.mofa.go.jp/mofaj/files/000236611.pdf> (概要)

□情報セキュリティ白書2018 2018年7月17日公開

<https://www.ipa.go.jp/security/publications/hakusyo/2018.html>

□JNSA NPO日本ネットワークセキュリティ協会

<https://www.jnsa.org>

□Black Hat

<https://www.blackhat.com>

□2018年6月13日 情報セキュリティインシデントに関する調査報告書【速報版】 JNSA

https://www.jnsa.org/result/incident/data/2017incident_survey_sokuhou_ver1.1.pdf

□サイドチャネル攻撃に対する安全性評価の研究動向とEMV カード固有の留意点

<https://www.imes.boj.or.jp/research/papers/japanese/kk34-4-6.pdf>

□総務省が誇るカーボン・ナノチューブ関連研究

https://www.aist.go.jp/Portals/0/resource_images/aist_j/aistinfo/aist_today/vol11_07/vol11_07_full.pdf

□主要国の研究開発戦略 (2018年)

<https://www.jst.go.jp/crds/pdf/2017/FR/CRDS-FY2017-FR-01.pdf>

□2016年3月31日 一般社団法人 JPCERT コーディネーションセンター

高度サイバー攻撃(APT)への備えと対応ガイド ~企業や組織に薦める一連のプロセスについて

<https://www.jpccert.or.jp/research/20160331-APTguide.pdf>

□FireEye

<https://www.fireeye.jp>

□Lockheed Martin Corporation

<https://www.lockheedmartin.com/en-us/index.html>

□Australian Cyber Security Centre (ACSC)

<https://acsc.gov.au/index.html>

□2018年12月18日 一般社団法人JPCERTコーディネーションセンター 2017年度CSIRT構築
および運用における実態調査

https://www.jpccert.or.jp/research/20181218_CSIRT-survey2017.pdf

□PWC 諸外国の「驚異ベースのペネトレーションテスト(TLPT)」に関する報告書

<https://www.fsa.go.jp/common/about/research/20180516/TLPT.pdf>

□AT Kearney 加熱するデジタル人材の獲得競争

<https://www.atkearney.co.jp/documents/4409500/7908849/>

War_for_Digital_Talents_160323.pdf/2438c817-6679-45c4-bc70-14abb47b6c09?

fbclid=IwAR3HV_yXwbhp6EAfRMw9Fb8hbsqHhOQyPFau6D6eucAzJbRzBj1ccOYnKDI

□School of Advanced Military Studies United States Army Command and General Staff
College Fort Leavenworth, Kansas 2017

Cyber Attacks and the Legal Justification for an Armed Response

<https://www.hsdl.org/?>

view&did=804021&fbclid=IwAR1BbCVArrK7XK76QuNSNQX6wpWASfAUGlrPSZMTUy7
_J5UYDwTmizTqaPg

□PRACTICAL REVERSE ENGINEERING

<https://repo.zenk-security.com/Reversing%20.%20cracking/>

Practical%20Reverse%20Engineering.pdf?

fbclid=IwAR2iVkpNCLHz0syfhqq3wDzIXA7xgfWf4EP09LXWc_v_wQr5qoH6ZWmu8Ac

□国際規格の歴史とその広がり

<http://www.hmt.u-toyama.ac.jp/socio/lab/sotsuron/99/takeuchi/4.html?>

fbclid=IwAR1Xp62hdSS6kitjEpr-AI5EnZRYI7Rr871MO0eQ_UatyiyZFfHc4sEJuXI

□Prime Minister's Office National Cyber Directorate National Cyber Security Authority
Cyber Defense Methodology for an Organization

[https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4.pdf?](https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4.pdf?fbclid=IwAR0VOXQ2ExselxVsY0L_3MSVr83iE_TiyRPI2ILZBsQe9jub3cjxt3N7TvY)

[fbclid=IwAR0VOXQ2ExselxVsY0L_3MSVr83iE_TiyRPI2ILZBsQe9jub3cjxt3N7TvY](https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4.pdf?fbclid=IwAR0VOXQ2ExselxVsY0L_3MSVr83iE_TiyRPI2ILZBsQe9jub3cjxt3N7TvY)

□UNC School of Law. Toward a Cybersecurity Policy Model : Israel National Cyber Bureau Case Study

[https://scholarship.law.unc.edu/cgi/viewcontent.cgi?](https://scholarship.law.unc.edu/cgi/viewcontent.cgi?referer=https%3A%2F%2Fwww.google.co.jp%2F&httpsredir=1&article=1283&context=ncjolt&fbclid=IwAR3D27fr6aCqEwcXrbBin5L9mLpuMy8caZKVnurPSCahcZZTJjdcMksCu90)

[referer=https%3A%2F%2Fwww.google.co.jp%2F&httpsredir=1&article=1283&context=ncjolt&fbclid=IwAR3D27fr6aCqEwcXrbBin5L9mLpuMy8caZKVnurPSCahcZZTJjdcMksCu90](https://scholarship.law.unc.edu/cgi/viewcontent.cgi?referer=https%3A%2F%2Fwww.google.co.jp%2F&httpsredir=1&article=1283&context=ncjolt&fbclid=IwAR3D27fr6aCqEwcXrbBin5L9mLpuMy8caZKVnurPSCahcZZTJjdcMksCu90)

□ASSA Androidアプリのセキュリティ設計・セキュアコーディングガイド

[https://www.jssec.org/dl/android_securecoding.pdf?](https://www.jssec.org/dl/android_securecoding.pdf?fbclid=IwAR12Zxr8Hw6e1e1gKxzrqI5Smxerqz7MjpOutnaNC3yRanznt35PzFcDFv4)

[fbclid=IwAR12Zxr8Hw6e1e1gKxzrqI5Smxerqz7MjpOutnaNC3yRanznt35PzFcDFv4](https://www.jssec.org/dl/android_securecoding.pdf?fbclid=IwAR12Zxr8Hw6e1e1gKxzrqI5Smxerqz7MjpOutnaNC3yRanznt35PzFcDFv4)

□IJJ Mimikatz実行痕跡の発見手法

[https://www.ijj.ad.jp/dev/tech/techweek/pdf/171108_02.pdf?](https://www.ijj.ad.jp/dev/tech/techweek/pdf/171108_02.pdf?fbclid=IwAR0Wzf_zaVBM4eDmSaNqP9OUOvN6bwZjuXqdKhF3thRoByQhzcjfyGQ-thl)

[fbclid=IwAR0Wzf_zaVBM4eDmSaNqP9OUOvN6bwZjuXqdKhF3thRoByQhzcjfyGQ-thl](https://www.ijj.ad.jp/dev/tech/techweek/pdf/171108_02.pdf?fbclid=IwAR0Wzf_zaVBM4eDmSaNqP9OUOvN6bwZjuXqdKhF3thRoByQhzcjfyGQ-thl)

□税務大学校 論叢第88号 平成29年6月 仮想通貨の税務上の取扱い

[https://www.nta.go.jp/about/organization/ntc/kenkyu/ronsou/88/05/05.pdf?](https://www.nta.go.jp/about/organization/ntc/kenkyu/ronsou/88/05/05.pdf?fbclid=IwAR1g_8MWOduXiOhn56Oca7F9tZuG2gqo6pKd0kEDIU8xWeaWJKV4XYI9sHU)

[fbclid=IwAR1g_8MWOduXiOhn56Oca7F9tZuG2gqo6pKd0kEDIU8xWeaWJKV4XYI9sHU](https://www.nta.go.jp/about/organization/ntc/kenkyu/ronsou/88/05/05.pdf?fbclid=IwAR1g_8MWOduXiOhn56Oca7F9tZuG2gqo6pKd0kEDIU8xWeaWJKV4XYI9sHU)

□JBAA 日本ビジネス航空協会 ビジネス航空（ビジネスジェット）とは？

[https://www.jbaa.org/wp/wp-content/uploads/2016/11/Business-Aviation-Introduction-R5.pdf?](https://www.jbaa.org/wp/wp-content/uploads/2016/11/Business-Aviation-Introduction-R5.pdf?fbclid=IwAR2I6tmoujQtObBlnafAtvzgSawABOZTbjeB2m4xZBLgwldx3NYiA4uDRZE)

[fbclid=IwAR2I6tmoujQtObBlnafAtvzgSawABOZTbjeB2m4xZBLgwldx3NYiA4uDRZE](https://www.jbaa.org/wp/wp-content/uploads/2016/11/Business-Aviation-Introduction-R5.pdf?fbclid=IwAR2I6tmoujQtObBlnafAtvzgSawABOZTbjeB2m4xZBLgwldx3NYiA4uDRZE)

□2017 Global Security Index(GSI)

[https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf?](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf?fbclid=IwAR3tBMjsMV481dJcdDY4a60lx7h8S3-9mYjwx5CabLIPcC8X_jTIVzLn-uo)

[fbclid=IwAR3tBMjsMV481dJcdDY4a60lx7h8S3-9mYjwx5CabLIPcC8X_jTIVzLn-uo](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf?fbclid=IwAR3tBMjsMV481dJcdDY4a60lx7h8S3-9mYjwx5CabLIPcC8X_jTIVzLn-uo)

□The Journal of Academic Social Science Studies

[https://www.jasstudies.com/Makaleler/2029641765_32-Bariş%20ÇELİKTAŞ.pdf?](https://www.jasstudies.com/Makaleler/2029641765_32-Bariş%20ÇELİKTAŞ.pdf?fbclid=IwAR01P_n3ajGVeseRMawnkIPFHjgMudoqedNbFI0u9osqV5Q3TppqAP1sBpfg)

[fbclid=IwAR01P_n3ajGVeseRMawnkIPFHjgMudoqedNbFI0u9osqV5Q3TppqAP1sBpfg](https://www.jasstudies.com/Makaleler/2029641765_32-Bariş%20ÇELİKTAŞ.pdf?fbclid=IwAR01P_n3ajGVeseRMawnkIPFHjgMudoqedNbFI0u9osqV5Q3TppqAP1sBpfg)

□Fire Eye. APT30 AND THE MECHANICS OF A LONG-RUNNING CYBER ESPIONAGE OPERATION

<https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf>

□中国の対ネット新兵器・巨砲「The Great Cannon」の仕組みとは

[https://gigazine.net/news/20150413-china-great-cannon/?](https://gigazine.net/news/20150413-china-great-cannon/?fbclid=IwAR2UmlfuKt4cgdxshR5JhMPcW0Z9CuD93IE0xsCx7AK39kPgg6gcSCcq218)

[fbclid=IwAR2UmlfuKt4cgdxshR5JhMPcW0Z9CuD93IE0xsCx7AK39kPgg6gcSCcq218](https://gigazine.net/news/20150413-china-great-cannon/?fbclid=IwAR2UmlfuKt4cgdxshR5JhMPcW0Z9CuD93IE0xsCx7AK39kPgg6gcSCcq218)

□Crypto assets task force: final report

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf?fbclid=IwAR1GBgtRm0BWcF6CvtnxDUR_BS9-FPyQJSIfjvNHNmsC3HZ3iKyuGCy_aeY

□Mckinsey Quarterly 2018 November 4

https://www.mckinsey.com/~media/McKinsey/McKinsey%20Quarterly/Digital%20Newsstand/2018%20Issues%20McKinsey%20Quarterly/Q4-2018_McK-Quarterly-Full-Issue.ashx?fbclid=IwAR1BG_9HUQeaBForEvuhwfPA055kKWNWUv3tfUqdycl3SULHd49mytj0Kz4

□数字で見る防衛省 自衛隊

http://www.mod.go.jp/j/publication/book/pamphlet/pdf/sujidemiru_h2912.pdf?fbclid=IwAR2CC2n1FYhrjxYRDdeEADllooNCYV7k1G2HBkH_txxo9HUJVsCZFNOMDfE

□Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information | OPA | Department of Justice

https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion?fbclid=IwAR2va8lkhTQE9i2v8Rg9URTKSQ_DuGsftdQGzf1q3LS3uHa__CSo0NEtDKI

□The Best of Books 2018

https://www.foreignaffairs.com/lists/2018-12-14/best-books-2018?utm_campaign=daily_soc&utm_source=fb&utm_medium=social&fbclid=IwAR1rUXz8MV4SZUhR1EINMxFZEMVCCNRhCa-ARv9rCM3Kg2AROuQP7v0kr20

□2018中国游戏市场规模2144.4亿元，同比增长仅5.3%，占全球游戏市场约23.6%-游戏陀螺 | 关注游戏创业，为游戏创业服务

https://www.youxituoluo.com/518174.html?from=timeline&isappinstalled=0&fbclid=IwAR37Kq-Jrse4LHNAwb2hgmht9ke4D3gCE9d1rPk1ntD6z218VW1tGs_nwfU

□JEITA 平成29年度情報セキュリティ調査報告書 -経営とセキュリティに関する調査-

https://home.jeita.or.jp/upload_file/20180809181822_Xo509Mkrcv.pdf?fbclid=IwAR02kXsn2UrD5KBMKHxQqKb_nyZw6oSHREghOmzXzXkebl3fFmeEH0hem5k

□This is what the financial sector can do to fight cyber attacks | World Economic Forum

https://www.weforum.org/agenda/2018/06/estimating-cyber-risk-for-the-financial-sector?fbclid=IwAR0eXQYUgzdKieANg48y_yWMcofVlkvV8atIC45-vA8h-6iFGjBWfg7tIQM

□MANDIANT APT1 Exposing One of China's Cyber Espionage Units

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf?fbclid=IwAR2CKp-Grmg4QaQN2b_XFH1yDyghdMio6NKd6wQxn64_iKqml06f2DwWKnM

□Security Report Gives A or A- Rating to 16% of Major Crypto Exchanges, None Get A+

<https://cointelegraph.com/news/security-report-gives-a-or-a-rating-to-16-of-major-crypto-exchanges-none-get-a>

□第242回NRIメディアフォーラム 共通ポイント社会の未来像～増える共通ポイント、進むマルチポイント化～

<https://www.nri.com/-/media/Corporate/jp/Files/PDF/knowledge/report/cc/mediaforum/2016/forum242.pdf?fbclid=IwAR248pZtEU4BQuoStOICDUUwPgg4jHu1xHa2kP-EaA6Y0bH2auz3KlcV4gk>

□Five emerging cyber-threats to worry about in 2019 - MIT Technology Review

<https://www.technologyreview.com/s/612713/five-emerging-cyber-threats-2019/?fbclid=IwAR3PHtUTKKKnG8bmuHaZ5DL09ZG1D1t17apDudb7BhMwmAMNk3jGH7EAudo>

□Chinese hackers allegedly stole data of more than 100,000 US Navy personnel - MIT Technology Review

https://www.technologyreview.com/the-download/612655/chinese-hackers-allegedly-stole-data-of-more-than-100000-us-navy-personnel/?fbclid=IwAR1ezMTIDs4pm-ml_WDpBLt0vvbBami7bagg89fCO-v21ZqhfM2HD__w4Jak

□The Crypto Valley's Top 50 The Blockchain in Switzerland & Liechtenstein analyzed and visualized Zug, 10 October 2018

https://cvvc.com/application/files/8415/3918/0658/CVVC_Insights_TOP50.pdf?fbclid=IwAR3g0hEd8fiO2O5P2prd4je7G-f4FbtP7Jg2_RmdnW-31qXovL_6DFYnC9Q

□EUROPIAN CENTRAL BANK EUROSISTEM TIBER-EU FRAMAWORK

https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf?fbclid=IwAR3t0bMonc05vEsv-OBUsyib728UmycdIBM77tn9LBfT0jOJ1t_q5BkXS2k

□EUROPIAN CENTRAL BANK EUROSISTEM TIBER-EU Framework

https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf?fbclid=IwAR2G-fa0oN5LVRzggGgTeXU_A9-jHcCTLCPp6SoMsteGLON32WNCPeNQJtOA

□EUROPIAN CENTRAL BANK EUROSISTEM TIBER-EU White Team Guidance
<https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf?fbclid=IwAR0gWAZWLI-urdHPqWyk6nUbVCIP08DnAiBJ8IQxOMFXypFSkqEXcb3UKIQ>

□Charlie Munger: Full Transcript of Daily Journal Annual Meeting 2018
http://latticeworkinvesting.com/2018/02/19/charlie-munger-full-transcript-of-daily-journal-annual-meeting-2018/?fbclid=IwAR0bBjvJuihHQsGKWzgi6n4j3DEJ0wghf2DRxaBSA-OCMPyOkPNzh3Ne_Qw

□共通脆弱性識別子CVE概説：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/CVE.html?fbclid=IwAR1YQUKBYMvKgsXFEr3P4xqHhP3Z5L0_Cz-UpqZ278Q4DDmyJ2tEzFUEMM

□セキュリティ設定共通化手順SCAP概説：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/SCAP.html?fbclid=IwAR0sjVaz2gZCVV7MaO6E_wydwvEDJIYbVcLS5x4Pxulr5IS3YhvDCP-zvkk

□セキュリティ検査言語OVAL概説：IPA 独立行政法人 情報処理推進機構
<https://www.ipa.go.jp/security/vuln/OVAL.html?fbclid=IwAR2Nyp-vDg1K-ssg9AvTgzdW4oc1Ya613ntx0ri7fbyPTDZiJS-OOJRZNOU>

□The ITU National cybersecurity Strategy Guide
https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf?fbclid=IwAR3EDHnzJ49rRgZTT2kU56ib5QYJ6i7_9_SJnEWUTAOoQVqILCsW4ngs9hg

□Cybersecurity Insiders 2018 Application Security Report - Whitepaper | Tenable®
https://jp.tenable.com/whitepapers/cybersecurity-insiders-2018-application-security-report?utm_campaign=00015656&utm_promoter=tenable-pr&utm_medium=8-28-18-press-release&utm_content=2018-appsec-report&fbclid=IwAR2qGYMB3696i1ioKNwGR-wvg6lIG4xA9nHT1esdhWkFZvJjUEdPX9ayBq4

□Salesforce Cybersecurity Insiders Application security report 2018
https://na53.salesforce.com/sfc/p/#300000000pZp/a/f200000017YL/EHuYZh0t0s_hEhMi4s9M4HLb7Q4H7w7flfeOzqkK9W4

□All About Security Clearances
https://www.state.gov/m/ds/clearances/c10978.htm?fbclid=IwAR2B5wo66LO65tmgynO5zJSty_kZ_W1PDavrK1VILYlgn3B9dlQs6QmYdlc

□ASVの要件(PCISSCのプログラムガイドVer1.2より)

[https://www.jcdsc.org/doc/20120126_asv.pdf?
fbclid=IwAR3lLzDtHiWQp2HcqnDjFmUOXjX6ldrAdurZXQ7XuNGwi8XNxCLGf-xD3R8](https://www.jcdsc.org/doc/20120126_asv.pdf?fbclid=IwAR3lLzDtHiWQp2HcqnDjFmUOXjX6ldrAdurZXQ7XuNGwi8XNxCLGf-xD3R8)

□JNSA 国内情報セキュリティ市場2017年度調査報告(速報値)

[https://www.jnsa.org/result/2018/surv_mrk/data/2017_mrkreport_sokuhou.pdf?
fbclid=IwAR1EtgsgN_1UAWQ3Vv6RTjrHloJ13Q1yQKCruLyYrRKleLsziG9S694SJxY](https://www.jnsa.org/result/2018/surv_mrk/data/2017_mrkreport_sokuhou.pdf?fbclid=IwAR1EtgsgN_1UAWQ3Vv6RTjrHloJ13Q1yQKCruLyYrRKleLsziG9S694SJxY)

□平成30年10月31日 産業サイバーセキュリティ研究会 ワーキンググループ 1(制度・技術・標準化) ビルサブワーキンググループ ビルシステムにおける サイバー・フィジカル・セキュリティ対策ガイドライン(β版・差し替え版)

[http://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/
wg_building/pdf/20180903_01.pdf?fbclid=IwAR09-n_ZKgT0ZuvvVNkWOGrI0Dif5Z-
l87jBULZxxBoTolmuFMok7W7_Zc](http://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/pdf/20180903_01.pdf?fbclid=IwAR09-n_ZKgT0ZuvvVNkWOGrI0Dif5Z-l87jBULZxxBoTolmuFMok7W7_Zc)

□Machine Learning for Cybersecurity 101

[https://towardsdatascience.com/machine-learning-for-
cybersecurity-101-7822b802790b?
fbclid=IwAR1TLOWpnFOUvSr4PmCOk17PjkKeOnO7_XzMxKscYcXTeO1ypt73LPVjD_I](https://towardsdatascience.com/machine-learning-for-cybersecurity-101-7822b802790b?fbclid=IwAR1TLOWpnFOUvSr4PmCOk17PjkKeOnO7_XzMxKscYcXTeO1ypt73LPVjD_I)

□Browse cve vulnerabilities by date

[https://www.cvedetails.com/browse-by-date.php?fbclid=IwAR3CxP-Ad5AA8a-
UnNkPwckatlObzi3-y-o1u0kLrid2hrU3bZ3WvKKxlu4](https://www.cvedetails.com/browse-by-date.php?fbclid=IwAR3CxP-Ad5AA8a-UnNkPwckatlObzi3-y-o1u0kLrid2hrU3bZ3WvKKxlu4)

□CVE - Towards a Common Enumeration of Vulnerabilities

[https://cve.mitre.org/docs/docs-2000/cerias.html?
fbclid=IwAR12Tcllsp5IAOIJZcRvsO5B-6ZUZD3UjsMrczbtGyRz1NwUYj5afcbSB1ug](https://cve.mitre.org/docs/docs-2000/cerias.html?fbclid=IwAR12Tcllsp5IAOIJZcRvsO5B-6ZUZD3UjsMrczbtGyRz1NwUYj5afcbSB1ug)

□制御系システムのセキュリティ (4) 最終号 -制御系システムの認証制度- | NTTデータ先端技術株式会社

[http://www.intellilink.co.jp/article/column/sec-controlsys04.html?fbclid=IwAR0iOaThOLI-
FHxIMKWvSWvvGa28ym_Gll9FX5ioyMEe-rHyn5jwAJCqk8Q](http://www.intellilink.co.jp/article/column/sec-controlsys04.html?fbclid=IwAR0iOaThOLI-FHxIMKWvSWvvGa28ym_Gll9FX5ioyMEe-rHyn5jwAJCqk8Q)

□"動く"半導体で、様々な機器の小型・軽量・高性能化を実現 | NEDOプロジェクト実用化ドキュメント

[https://www.nedo.go.jp/hyoukabu/articles/201316omron/index.html?
fbclid=IwAR3SpN3IK4ZLuDvVrKJ2XVJDUo5zXF8NdyCrULvMBr9fB-FiTica_19yZJM](https://www.nedo.go.jp/hyoukabu/articles/201316omron/index.html?fbclid=IwAR3SpN3IK4ZLuDvVrKJ2XVJDUo5zXF8NdyCrULvMBr9fB-FiTica_19yZJM)

□ICSとは？保護の手段は？ | カスペルスキー公式ブログ

[https://blog.kaspersky.co.jp/what-is-ics/18596/?
fbclid=IwAR2n1i8BYuUc29j8BFPAYaosYfDzaytsL3ZX-SF9VhO2SGm4D1NN9IO0d08](https://blog.kaspersky.co.jp/what-is-ics/18596/?fbclid=IwAR2n1i8BYuUc29j8BFPAYaosYfDzaytsL3ZX-SF9VhO2SGm4D1NN9IO0d08)

□How to Fool an ADC. or how to hide the destruction of a turbine with the help of DSP

<https://www.blackhat.com/docs/eu-16/materials/eu-16-Gonzalez-How-To-Fool-An-ADC-Part-II-Or-Hiding-Destruction-Of-Turbine-With-A-Little-Help-Of-Signal-Processing.pdf?fbclid=IwAR0PHlxzjQrtVbzbGALUTN-9cYTGE0BFJmpul8VqQz7RT2crIP3mnJkKt5al>

□PCI Security Standard Council. PCI DSS Quick Reference Guide

https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?fbclid=IwAR3L-FCeWLZ95rXBGWRzLPgCREsPq1jMrQx3T6ztq5o3SjCdYFgwMLhZEYI

□Whole Product Dynamic “Real-World” Protection Test Consumer Products

https://www.av-comparatives.org/wp-content/uploads/2018/07/avc_prot_2018a_en.pdf?fbclid=IwAR2Hs_iw79ICzz4zzDsz_MDfJfZ3eibj0_NckRcN-jZmigc4wmDTVHdLOK8

□CYBER THREAT REAL TIME MAP

https://cybermap.kaspersky.com/?fbclid=IwAR2NcskDZ8pZ6FIDIG9aDKIgKcUN7A_2ryC5JrRYm5bR3IyCWNPHvC302xU

□SANS Institute: Reading Room - Industrial Control Systems / SCADA

<https://www.sans.org/reading-room/whitepapers/ICS/paper/36327>

□F5 LABS 2018 Application Protection Report

https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/F5Labs_2018_Application_Protection_Report.pdf?fbclid=IwAR1oGeFV_uU3jyy0c0-1kx5L-tDRPxZdjcVEbjQaSoNJaadhEePrOPgERtg

□産業用コントローラ 入出力モジュールの冗長化

https://www.toshiba.co.jp/tech/review/2011/06/66_06pdf/f03.pdf?fbclid=IwAR2mepHS3ofD_3ooDtcWsPoCY379ezye2qmyz5NtGU-PAiM51BZXCMg5coU

□Green Lights Forever: Analyzing the Security of Traffic Infrastructure

https://jhalderm.com/pub/papers/traffic-woot14.pdf?fbclid=IwAR2KTUif34XXJkRZ11sd-SzeP8s_MYyhAiPU9Vp1h2XyzmJFfcKelHBH-So

□2017年7月 民間航空分野における 先進的な無線システムの研究開発

http://www.soumu.go.jp/main_content/000502406.pdf?fbclid=IwAR1Shw-JPtDPimNqv4IgmOOpjDrEOhRSk8_grsq-vHrAaBTSwxKTmbEeQg8

□昭和57年7月 最近の航空機の計測と操縦システム

https://www.jstage.jst.go.jp/article/sicej11962/21/7/21_7_691/_pdf?fbclid=IwAR3KeeJVJWNxn7AxrUomi26RF5QavVhxrRGDcFkV-JGZ_m5F_LIU7LO6LvQ

□botify

<https://www.botify.com>

□サイバーセキュリティ.com サイバー攻撃の件数など統計情報

[https://cybersecurity-jp.com/cybersecurity-guide/14641?](https://cybersecurity-jp.com/cybersecurity-guide/14641?fbclid=IwAR0REwkPWGsCjJ3F8IB94eJHh2k70f4lyZuqh77_kf5QzzcGWOkgR3pQMoE#i)

[fbclid=IwAR0REwkPWGsCjJ3F8IB94eJHh2k70f4lyZuqh77_kf5QzzcGWOkgR3pQMoE#i](https://cybersecurity-jp.com/cybersecurity-guide/14641?fbclid=IwAR0REwkPWGsCjJ3F8IB94eJHh2k70f4lyZuqh77_kf5QzzcGWOkgR3pQMoE#i)

□Kali Linux Revealed

[https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf?](https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf?fbclid=IwAR3Y1mbrW8zI0Fja2hXRcnlWA9mf_pLIZWcxADR702H11CnoRPYfREz0eB8)

[fbclid=IwAR3Y1mbrW8zI0Fja2hXRcnlWA9mf_pLIZWcxADR702H11CnoRPYfREz0eB8](https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf?fbclid=IwAR3Y1mbrW8zI0Fja2hXRcnlWA9mf_pLIZWcxADR702H11CnoRPYfREz0eB8)

□Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers

[https://www.exploit-db.com/?fbclid=IwAR37z14GH1gBXvqUC4aaJ_y-](https://www.exploit-db.com/?fbclid=IwAR37z14GH1gBXvqUC4aaJ_y-hbrFZsk04BsCGFB91WC1riHwEcyOqwzYZP4)

[hbrFZsk04BsCGFB91WC1riHwEcyOqwzYZP4](https://www.exploit-db.com/?fbclid=IwAR37z14GH1gBXvqUC4aaJ_y-hbrFZsk04BsCGFB91WC1riHwEcyOqwzYZP4)

□Facial recognition, AI and big data poised to boost Chinese public safety - People's Daily Online

[http://en.people.cn/n3/2017/1017/c90000-9280772.html?](http://en.people.cn/n3/2017/1017/c90000-9280772.html?fbclid=IwAR0FgfaxYBn9vso7WI6YB7B3w7xOZHCrAbD8qeakkIDwsIEQPezTg5XhF4M)

[fbclid=IwAR0FgfaxYBn9vso7WI6YB7B3w7xOZHCrAbD8qeakkIDwsIEQPezTg5XhF4M](http://en.people.cn/n3/2017/1017/c90000-9280772.html?fbclid=IwAR0FgfaxYBn9vso7WI6YB7B3w7xOZHCrAbD8qeakkIDwsIEQPezTg5XhF4M)

□2019年2月22日 国内800万件のアカウント情報流出が判明、ダークウェブに出現した約27億件の巨大漏えいファイル群「Collection#1」事件 - INTERNET Watch

<https://internet.watch.impress.co.jp/docs/news/1171134.html>

□Payment Card Industry(PCI) データセキュリティ基準

[https://ja.pcisecuritystandards.org/_onelink_/pcisecurity/en2ja/minisite/en/docs/](https://ja.pcisecuritystandards.org/_onelink_/pcisecurity/en2ja/minisite/en/docs/PCI_DSS_v3%202_JA-JP_20180801.pdf?fbclid=IwAR0157U1Dw-TDJNmKEmralcRuEBW_efABjeb7QkoPXNRTYwSI0Ute8bmGE8)

[PCI_DSS_v3%202_JA-JP_20180801.pdf?fbclid=IwAR0157U1Dw-](https://ja.pcisecuritystandards.org/_onelink_/pcisecurity/en2ja/minisite/en/docs/PCI_DSS_v3%202_JA-JP_20180801.pdf?fbclid=IwAR0157U1Dw-TDJNmKEmralcRuEBW_efABjeb7QkoPXNRTYwSI0Ute8bmGE8)

[TDJNmKEmralcRuEBW_efABjeb7QkoPXNRTYwSI0Ute8bmGE8](https://ja.pcisecuritystandards.org/_onelink_/pcisecurity/en2ja/minisite/en/docs/PCI_DSS_v3%202_JA-JP_20180801.pdf?fbclid=IwAR0157U1Dw-TDJNmKEmralcRuEBW_efABjeb7QkoPXNRTYwSI0Ute8bmGE8)

□SANS CWE/SANS最も危険なプログラミングエラーTOP 25

[https://www.sans.org/media/](https://www.sans.org/media/top25_japanese.pdf?fbclid=IwAR0BYyVvmXn_QyUOg8515eDUOxvZyo_WLWowJr42r2-1S0IJRm4uJk_V28o)

[top25_japanese.pdf?fbclid=IwAR0BYyVvmXn_QyUOg8515eDUOxvZyo_WLWowJr42r2-](https://www.sans.org/media/top25_japanese.pdf?fbclid=IwAR0BYyVvmXn_QyUOg8515eDUOxvZyo_WLWowJr42r2-1S0IJRm4uJk_V28o)

[1S0IJRm4uJk_V28o](https://www.sans.org/media/top25_japanese.pdf?fbclid=IwAR0BYyVvmXn_QyUOg8515eDUOxvZyo_WLWowJr42r2-1S0IJRm4uJk_V28o)

□TorFlow

[https://torflow.uncharted.software/?fbclid=IwAR1yJsP64MsZCjxylkBHruWmCF-Pq6s8-](https://torflow.uncharted.software/?fbclid=IwAR1yJsP64MsZCjxylkBHruWmCF-Pq6s8-QV86CM6IT5_qTKCg0vFpzywX1Y#?ML=4.21875,41.11246878918088,3&C=us,USA)

[QV86CM6IT5_qTKCg0vFpzywX1Y#?ML=4.21875,41.11246878918088,3&C=us,USA](https://torflow.uncharted.software/?fbclid=IwAR1yJsP64MsZCjxylkBHruWmCF-Pq6s8-QV86CM6IT5_qTKCg0vFpzywX1Y#?ML=4.21875,41.11246878918088,3&C=us,USA)

□ソリトン Security White Paper 2019

[https://www.soliton.co.jp/special/csa1902/WP_CSA-1902A.pdf?fbclid=IwAR10c3r3W-](https://www.soliton.co.jp/special/csa1902/WP_CSA-1902A.pdf?fbclid=IwAR10c3r3W-WnWE9asFrpLQIm0Anb7LS7oS8NumcWmLkObmliRq96Muk30Nc)

[WnWE9asFrpLQIm0Anb7LS7oS8NumcWmLkObmliRq96Muk30Nc](https://www.soliton.co.jp/special/csa1902/WP_CSA-1902A.pdf?fbclid=IwAR10c3r3W-WnWE9asFrpLQIm0Anb7LS7oS8NumcWmLkObmliRq96Muk30Nc)

□Bug Bounty - Hacker Powered Security Testing | HackerOne

[https://www.hackerone.com/?](https://www.hackerone.com/?fbclid=IwAR3mQRngTYaF75vGZ2B5U3wF6WWPVYJiMHqKI90pcm7HKB5PHG_nrmom3Uo)

[fbclid=IwAR3mQRngTYaF75vGZ2B5U3wF6WWPVYJiMHqKI90pcm7HKB5PHG_nrmom3Uo](https://www.hackerone.com/?fbclid=IwAR3mQRngTYaF75vGZ2B5U3wF6WWPVYJiMHqKI90pcm7HKB5PHG_nrmom3Uo)

□The North Korea Strategic Dilemma President/CEO Pacific Tech Bridge

[https://www.canon-igs.org/event/report/171031_Paul_presentation.pdf?](https://www.canon-igs.org/event/report/171031_Paul_presentation.pdf?fbclid=IwAR3o9G0hOh_76Qg0txKa5Z7oi37GwUCSPRj8YJgsZnqnub-hO6QruDz0Yss)

[fbclid=IwAR3o9G0hOh_76Qg0txKa5Z7oi37GwUCSPRj8YJgsZnqnub-hO6QruDz0Yss](https://www.canon-igs.org/event/report/171031_Paul_presentation.pdf?fbclid=IwAR3o9G0hOh_76Qg0txKa5Z7oi37GwUCSPRj8YJgsZnqnub-hO6QruDz0Yss)

□Julian Assange, CrowdStrike, and the Russian Hack That Wasn't – American Greatness

[https://amgreatness.com/2018/07/13/julian-assange-crowdstrike-and-the-russian-hack-that-wasnt/?fbclid=IwAR2cJ9J9Avq5VadbbT0bfhrKI1IQ9CO8Y7N8TEXwh-](https://amgreatness.com/2018/07/13/julian-assange-crowdstrike-and-the-russian-hack-that-wasnt/?fbclid=IwAR2cJ9J9Avq5VadbbT0bfhrKI1IQ9CO8Y7N8TEXwh-PgnNCgZSMkLcnzQ-l)

[PgnNCgZSMkLcnzQ-l](https://amgreatness.com/2018/07/13/julian-assange-crowdstrike-and-the-russian-hack-that-wasnt/?fbclid=IwAR2cJ9J9Avq5VadbbT0bfhrKI1IQ9CO8Y7N8TEXwh-PgnNCgZSMkLcnzQ-l)

[PgnNCgZSMkLcnzQ-l](https://amgreatness.com/2018/07/13/julian-assange-crowdstrike-and-the-russian-hack-that-wasnt/?fbclid=IwAR2cJ9J9Avq5VadbbT0bfhrKI1IQ9CO8Y7N8TEXwh-PgnNCgZSMkLcnzQ-l)

□経済財政分析ディスカッション・ペーパー 近年の労働分配率の低下の要因分析

[https://www5.cao.go.jp/keizai3/discussion-paper/dp183.pdf?](https://www5.cao.go.jp/keizai3/discussion-paper/dp183.pdf?fbclid=IwAR3xpgEBuu3nb9TiAmeRVNgyqc8-i_QSUTjLAovihDkfbQU4pKiRo8WFSL8)

[fbclid=IwAR3xpgEBuu3nb9TiAmeRVNgyqc8-i_QSUTjLAovihDkfbQU4pKiRo8WFSL8](https://www5.cao.go.jp/keizai3/discussion-paper/dp183.pdf?fbclid=IwAR3xpgEBuu3nb9TiAmeRVNgyqc8-i_QSUTjLAovihDkfbQU4pKiRo8WFSL8)

□Bank of England CBEST Intelligence-Led Testing Implementation Guide

[https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-](https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide?fbclid=IwAR2qQiN1BuMMB-UBm35TETf43PqGlrN-a2R5B9bVoBRJjkj-TIWHunzIX-c)

[continuity/cbest-implementation-guide?fbclid=IwAR2qQiN1BuMMB-](https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide?fbclid=IwAR2qQiN1BuMMB-UBm35TETf43PqGlrN-a2R5B9bVoBRJjkj-TIWHunzIX-c)

[UBm35TETf43PqGlrN-a2R5B9bVoBRJjkj-TIWHunzIX-c](https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide?fbclid=IwAR2qQiN1BuMMB-UBm35TETf43PqGlrN-a2R5B9bVoBRJjkj-TIWHunzIX-c)

□Bank of England CBEST Intelligence-Led Testing Understanding Cyber Threat Intelligence Operations

[https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-](https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations?fbclid=IwAR2gKzcDte8SdbUmQmW-2k83pGDBKB3vd8A-dFo-CYB9JDKu4G_7xwbL6ds)

[continuity/understanding-cyber-threat-intelligence-operations?](https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations?fbclid=IwAR2gKzcDte8SdbUmQmW-2k83pGDBKB3vd8A-dFo-CYB9JDKu4G_7xwbL6ds)

[fbclid=IwAR2gKzcDte8SdbUmQmW-2k83pGDBKB3vd8A-dFo-CYB9JDKu4G_7xwbL6ds](https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations?fbclid=IwAR2gKzcDte8SdbUmQmW-2k83pGDBKB3vd8A-dFo-CYB9JDKu4G_7xwbL6ds)

□FesRAMP PENETRATION TEST GUIDANCE

[https://www.fedramp.gov/assets/resources/documents/](https://www.fedramp.gov/assets/resources/documents/CSP_Penetration_Test_Guidance.pdf?fbclid=IwAR2S5bqRL3djt_aESv5CzL6z6bqWJv54Kj-Y2SlakHweELZxfT7rqDq-gZI)

[CSP_Penetration_Test_Guidance.pdf?](https://www.fedramp.gov/assets/resources/documents/CSP_Penetration_Test_Guidance.pdf?fbclid=IwAR2S5bqRL3djt_aESv5CzL6z6bqWJv54Kj-Y2SlakHweELZxfT7rqDq-gZI)

[fbclid=IwAR2S5bqRL3djt_aESv5CzL6z6bqWJv54Kj-Y2SlakHweELZxfT7rqDq-gZI](https://www.fedramp.gov/assets/resources/documents/CSP_Penetration_Test_Guidance.pdf?fbclid=IwAR2S5bqRL3djt_aESv5CzL6z6bqWJv54Kj-Y2SlakHweELZxfT7rqDq-gZI)

□NIST Technical Guide to Information Security Testing and Assessment

[https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf?](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf?fbclid=IwAR33nVO_3-5y82ANe7kCdvj6BE4IWZvmLobBoNEN9tm10z2lQQ_oeDho6Y8)

[fbclid=IwAR33nVO_3-5y82ANe7kCdvj6BE4IWZvmLobBoNEN9tm10z2lQQ_oeDho6Y8](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf?fbclid=IwAR33nVO_3-5y82ANe7kCdvj6BE4IWZvmLobBoNEN9tm10z2lQQ_oeDho6Y8)

□Cybercrime is increasing and more costly for organizations | CIO

[https://www.cio.com/article/3386417/cybercrime-is-increasing-and-more-costly-for-](https://www.cio.com/article/3386417/cybercrime-is-increasing-and-more-costly-for-organizations.html?fbclid=IwAR0cJIVmlSajbc-iEK794aldl226fW-JTFKSBdLxrX5qCSS_pN73Ha7HRpl)

[organizations.html?fbclid=IwAR0cJIVmlSajbc-iEK794aldl226fW-](https://www.cio.com/article/3386417/cybercrime-is-increasing-and-more-costly-for-organizations.html?fbclid=IwAR0cJIVmlSajbc-iEK794aldl226fW-JTFKSBdLxrX5qCSS_pN73Ha7HRpl)

[JTFKSBdLxrX5qCSS_pN73Ha7HRpl](https://www.cio.com/article/3386417/cybercrime-is-increasing-and-more-costly-for-organizations.html?fbclid=IwAR0cJIVmlSajbc-iEK794aldl226fW-JTFKSBdLxrX5qCSS_pN73Ha7HRpl)

□Dillon Gage | The most diverse company in the Precious Metals Industry
https://dillongage.com/?fbclid=IwAR3e2U_s_kXTH2xFLw9OclB8VMhjTp8o-zi0YZleRt6OlwZDsQjZXzww1CA

□The Cordell Institute for Policy in Medicine & Law | Washington University in St. Louis
<https://cordellinstitute.wustl.edu/?fbclid=IwAR0Frh8NYm13h9nBXxev74bZLX5soBP576RtYeJtmuk8L4aW6lOR5fgkmVo>

□Chinese scientists have put human brain genes in monkeys—and yes, they may be smarter - MIT Technology Review
https://www.technologyreview.com/s/613277/chinese-scientists-have-put-human-brain-genes-in-monkeysand-yes-they-may-be-smarter/?utm_campaign=the_download.unpaid.engagement&utm_source=hs_email&utm_medium=email&utm_content=71618860&_hsenc=p2ANqtz-8TRdjJ4jobJLmS_QlvqCtCwwrhHeq1rgdUatfDhpgVEwtZ4vw8h4AQoiQkn8moeJDs2-Ju1ZTREugHMeOKdElia_N-SA&_hsmi=71618860&fbclid=IwAR1rtfiCalGIHeJiSKYm0D-saJyZNfVSkKDwCFjN4ny3bdwvy8yXpZMWC58

□Lessons for the Cyber Battlefield from the Early Nuclear Era's Single Integrated Operating Plan
https://www.fdd.org/wp-content/uploads/2019/01/fdd-report-cyber-siop.pdf?fbclid=IwAR0petMZBYPmJ4E3pMwXUrc81I9itX4guzpSKamCK257_KmNkQ5AS3lwY9A

□英国のEU脱退（ブレグジット）に向けた日本企業の留意点
https://www.jetro.go.jp/ext_images/_Reports/01/63e5b8fb0ea6b7c8/20180024.pdf?fbclid=IwAR03-3O-csRI--ssuJy-PJbjXe-gldS5tZZnpxvbrz3VYw0xYb6A3H0wEtA

□新世代モバイル通信システム委員会 技術検討作業班における検討状況
http://www.soumu.go.jp/main_content/000536171.pdf?fbclid=IwAR2HYfFDsNXf2bmaU4rOKGvprxv6y1hZH38YijGjQbqGaCPCiSSuKvYCqY0

□警察政策学会資料 第94号 米国における行政傍受に関する法体系と解釈運用
[http://asss.jp/report/警察政策学会資料094\(米国における行政傍受に関する法体系と解釈運用\).pdf?fbclid=IwAR1DHbbGllrQ4Z1z9pMgvS-yZFma6exp2HhsEF1FNA-myU2Huba5Toph1g](http://asss.jp/report/警察政策学会資料094(米国における行政傍受に関する法体系と解釈運用).pdf?fbclid=IwAR1DHbbGllrQ4Z1z9pMgvS-yZFma6exp2HhsEF1FNA-myU2Huba5Toph1g)

□National Security Strategy of United States of America December 2017
https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf?fbclid=IwAROC3MSOSWrs3D4MzT24M_QRRfTmyj6MhQ7P6pQqD4DIN_JNqvLlSkbnN48

□アクセンチュア 資産運用会社のビジネスモデルに関する調査研究 2018/3/30

[https://www.gpif.go.jp/investment/research_2017_3_.pdf?
fbclid=IwAR0_J2e7F6CSAitGXx07cfckB7ZFxJFx9xyMQA3upyUBpkWZoNIMdalOUpA](https://www.gpif.go.jp/investment/research_2017_3_.pdf?fbclid=IwAR0_J2e7F6CSAitGXx07cfckB7ZFxJFx9xyMQA3upyUBpkWZoNIMdalOUpA)

□Charlotte Training May 2019 - The National Cyber-Forensics and Training Alliance
[https://www.ncfta.net/charlotte-training-may-2019/?
fbclid=IwAR0iWbhrWvCQoWpPe7Pid2BDTKZCxVi0M4oC47D6UMhYbaWQ-ao3cR9aFDc](https://www.ncfta.net/charlotte-training-may-2019/?fbclid=IwAR0iWbhrWvCQoWpPe7Pid2BDTKZCxVi0M4oC47D6UMhYbaWQ-ao3cR9aFDc)

□Goldman Sachs The World of Games eSports from Wild West to Mainstream
[https://www.goldmansachs.com/insights/pages/infographics/e-sports/report.pdf?
fbclid=IwAR3xf9L4k4Kpw8cSgU98MDm8F4auw2N3WiHJ67XmbsTdR1ICMODsT0vcHbk](https://www.goldmansachs.com/insights/pages/infographics/e-sports/report.pdf?fbclid=IwAR3xf9L4k4Kpw8cSgU98MDm8F4auw2N3WiHJ67XmbsTdR1ICMODsT0vcHbk)

□Goldman Sachs Presentation to Bernstein Strategic Decisions Conference
[https://www.goldmansachs.com/investor-relations/presentations/2018-sanford-
bernstein-conference-PDF.pdf?
fbclid=IwAR2c5RDWK1IF0XMFAOcmsUt80WC3YDSjL4tHGt5VcUcKVJWY342YmYm_XB
A](https://www.goldmansachs.com/investor-relations/presentations/2018-sanford-bernstein-conference-PDF.pdf?fbclid=IwAR2c5RDWK1IF0XMFAOcmsUt80WC3YDSjL4tHGt5VcUcKVJWY342YmYm_XBA)

□Australian Strategic Policy Institute - Mapping China's Tech Giant
[https://chinatechmap.aspi.org.au/?fbclid=IwAR2wJrydCOxSLZhtDcA-Dcj1o-
kgJLilf6JERf7f_1megF1WQ5oSBevrdyY#/map/](https://chinatechmap.aspi.org.au/?fbclid=IwAR2wJrydCOxSLZhtDcA-Dcj1o-kgJLilf6JERf7f_1megF1WQ5oSBevrdyY#/map/)

□拡大するサイバーセキュリティー市場 | 地域・分析レポート - 海外ビジネス情報 - ジェトロ
<https://www.jetro.go.jp/biz/areareports/2018/1fb2ecd606c590e5.html>

□サイバー攻撃リアルタイム可視化ツール集
<https://cybersecurity-jp.com/software-tool/15011>

□MAP | Kaspersky Cyberthreat real-time map
<https://cybermap.kaspersky.com>

□NICTERWEB 2.0
<https://www.nicter.jp/atlas>

□Digital Attack Map
[http://www.digitalattackmap.com/
#anim=1&color=0&country=ALL&list=0&time=18065&view=map](http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18065&view=map)

□FireEye Cyber Threat Map
<https://www.fireeye.jp/cyber-map/threat-map.html>

□シスコ 2018 年次サイバーセキュリティーレポート
https://www.cisco.com/c/dam/m/ja_jp/offers/183/sc-04/cisco-acr2018-ja.pdf

□サイバー保険とは | サイバー保険 | 日本損害保険協会

<http://www.sonpo.or.jp/cyber-hoken/about/>

□NICTER 観測レポート 2018 国立研究開発法人 情報通信研究機構

サイバーセキュリティ研究所 サイバーセキュリティ研究室

http://www.nict.go.jp/cyber/report/NICTER_report_2018.pdf

□Least Cyber Safe Countries (Rank)

<https://datawrapper.dwcdn.net/rx0QK/4/>

□Nokia Threat Intelligence Report – 2019

<https://blog.drhack.net/wp-content/uploads/2018/12/>

Nokia_Threat_Intelligence_Report_White_Paper_EN.pdf

□2019 State of Malware provided by Malware bytes Labs

<https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf>

□Wiretapping End-to-End Encrypted VoIP Calls: Real-World Attacks on ZRTP

<https://www.ibr.cs.tu-bs.de/papers/schuermann-popets2017.pdf>

□2016年12月16日 VoIPセキュリティの基礎 ~IP電話システムを安心・安全に利用するコ

ツ~ | CIAJ 一般社団法人 情報通信ネットワーク産業協会

<https://www.ciaj.or.jp/ciaj-wp/wp-content/uploads/2016/12/>

bcb9cc4353a5052075d1458ab5e415bf.pdf

□NTT CERT サイバーセキュリティ アニュアルレポート 2018

http://www.ntt.co.jp/sc/media/NTTannual2018_j_web_lock.pdf

□IoTのセキュリティ ~ハッカーによる攻撃の現状と対策ポイント~ 2015年12月11日 重要生活機

器連携セキュリティ協議会 事務局長 伊藤 公祐

<https://www.nic.ad.jp/ja/materials/after/20151211/20151211-itou.pdf>

□平成28年度 内外一体の経済成長戦略構築にかかる 国際経済調査事業 (サイバー国際経済に関する調査) 調査報告書 平成29年3月 株式会社三菱総合研究所

https://www.meti.go.jp/meti_lib/report/H28FY/290775.pdf

□平成29年度 委託調査報告書 HP掲載一覧

https://www.meti.go.jp/meti_lib/report/H29FY/itakuichiranH29FY.pdf

□インターネット総合研究所のイスラエル上場*と今後のIRI/BBTowerグループの展開について | 藤原洋のコラム

<https://ameblo.jp/bbtower-ceo/entry-12400019587.html>

□ネットワーク通信 (LANとTCP/IP)

[https://www.ei.fukui-nct.ac.jp/~t-saitoh/edu/internet/net-lan.pdf?](https://www.ei.fukui-nct.ac.jp/~t-saitoh/edu/internet/net-lan.pdf?fbclid=IwAR2HI4CjmpcX6h4Za40mc9GzMDdEZ72urEhQcsqMvJsLBduwWnUprJ9hPKY)

[fbclid=IwAR2HI4CjmpcX6h4Za40mc9GzMDdEZ72urEhQcsqMvJsLBduwWnUprJ9hPKY](https://www.ei.fukui-nct.ac.jp/~t-saitoh/edu/internet/net-lan.pdf?fbclid=IwAR2HI4CjmpcX6h4Za40mc9GzMDdEZ72urEhQcsqMvJsLBduwWnUprJ9hPKY)

□OWASP テスティングガイド 2008第3版 日本語版

[https://www.owasp.org/images/1/1e/OTGv3Japanese.pdf?fbclid=IwAR0R0dW-](https://www.owasp.org/images/1/1e/OTGv3Japanese.pdf?fbclid=IwAR0R0dW-z1j4D_DCyQ4732VFKj-UqG7_9T2e6MLBXJwWOGbap7gEfSlcc)

[z1j4D_DCyQ4732VFKj-UqG7_9T2e6MLBXJwWOGbap7gEfSlcc](https://www.owasp.org/images/1/1e/OTGv3Japanese.pdf?fbclid=IwAR0R0dW-z1j4D_DCyQ4732VFKj-UqG7_9T2e6MLBXJwWOGbap7gEfSlcc)

□FFRI NFCとセキュリティ

[https://www.ffri.jp/assets/files/monthly_research/MR201301_NFC_Security.pdf?](https://www.ffri.jp/assets/files/monthly_research/MR201301_NFC_Security.pdf?fbclid=IwAR2J2YQrPhcVV92PJD13_rJymfFwmDoZyahGI6skGM0ysInCKVTKWkAEj6Y)

[fbclid=IwAR2J2YQrPhcVV92PJD13_rJymfFwmDoZyahGI6skGM0ysInCKVTKWkAEj6Y](https://www.ffri.jp/assets/files/monthly_research/MR201301_NFC_Security.pdf?fbclid=IwAR2J2YQrPhcVV92PJD13_rJymfFwmDoZyahGI6skGM0ysInCKVTKWkAEj6Y)

□Near Field Communication (NFC) Technology, Vulnerabilities and Principal Attack Schema

[https://resources.infosecinstitute.com/near-field-communication-nfc-technology-](https://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/?fbclid=IwAR0aNsulhVFbilxsbGkcS22y6C9sFrIhrOp727fGkW5PXBjizqz8UoUvn--A#gref)

[vulnerabilities-and-principal-attack-schema/?fbclid=IwAR0aNsulhVFbilxsbGkcS22y6C9sFrIhrOp727fGkW5PXBjizqz8UoUvn--A#gref](https://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/?fbclid=IwAR0aNsulhVFbilxsbGkcS22y6C9sFrIhrOp727fGkW5PXBjizqz8UoUvn--A#gref)

□Prof. Eviatar Matania | Mobile

[https://en-social-sciences.m.tau.ac.il/profile/eviatarm?](https://en-social-sciences.m.tau.ac.il/profile/eviatarm?fbclid=IwAR2u41IUvzKI2XtVqXkV2EtroTN_iRIS4sXy-giwo48xNU_f-5ADGwdbkIE)

[fbclid=IwAR2u41IUvzKI2XtVqXkV2EtroTN_iRIS4sXy-giwo48xNU_f-5ADGwdbkIE](https://en-social-sciences.m.tau.ac.il/profile/eviatarm?fbclid=IwAR2u41IUvzKI2XtVqXkV2EtroTN_iRIS4sXy-giwo48xNU_f-5ADGwdbkIE)

□Wiretapping End-to-End Encrypted VoIP Calls: Real-World Attacks on ZRTP

[https://www.ibr.cs.tu-bs.de/papers/schuermann-popets2017.pdf?](https://www.ibr.cs.tu-bs.de/papers/schuermann-popets2017.pdf?fbclid=IwAR0nyjj5SuY7jrGfoO8dpOqL_dE26N3in-zbVgqOPGDeJearTmE_X79qUvA)

[fbclid=IwAR0nyjj5SuY7jrGfoO8dpOqL_dE26N3in-zbVgqOPGDeJearTmE_X79qUvA](https://www.ibr.cs.tu-bs.de/papers/schuermann-popets2017.pdf?fbclid=IwAR0nyjj5SuY7jrGfoO8dpOqL_dE26N3in-zbVgqOPGDeJearTmE_X79qUvA)

□MANDIANT APT1 Exposing One of China's Cyber Espionage Units

[https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-](https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf?fbclid=IwAR2CKp-Grmg4QaQN2b_XFH1yDyghdMio6NKd6wQxn64_iKqml06f2DwWKnM)

[report.pdf?fbclid=IwAR2CKp-Grmg4QaQN2b_XFH1yDyghdMio6NKd6wQxn64_iKqml06f2DwWKnM](https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf?fbclid=IwAR2CKp-Grmg4QaQN2b_XFH1yDyghdMio6NKd6wQxn64_iKqml06f2DwWKnM)

□The ITU National cybersecurity Strategy Guide

[https://www.itu.int/ITU-D/cyb/cybersecurity/docs/](https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf?fbclid=IwAR3EDHnzJ49rRgZTT2kU56ib5QYJ6i7_9_SJnEWUTA0oQVqILCsW4ngs9hg)

[ITUNationalCybersecurityStrategyGuide.pdf?](https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf?fbclid=IwAR3EDHnzJ49rRgZTT2kU56ib5QYJ6i7_9_SJnEWUTA0oQVqILCsW4ngs9hg)

[fbclid=IwAR3EDHnzJ49rRgZTT2kU56ib5QYJ6i7_9_SJnEWUTA0oQVqILCsW4ngs9hg](https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf?fbclid=IwAR3EDHnzJ49rRgZTT2kU56ib5QYJ6i7_9_SJnEWUTA0oQVqILCsW4ngs9hg)

□Five emerging cyber-threats to worry about in 2019 - MIT Technology Review

[https://www.technologyreview.com/s/612713/five-emerging-cyber-threats-2019/?](https://www.technologyreview.com/s/612713/five-emerging-cyber-threats-2019/?fbclid=IwAR3PHtUTKKKnG8bmuHaZ5DL09ZG1D1t17apDudb7BhMwmAMNk3jGH7EAu)

[fbclid=IwAR3PHtUTKKKnG8bmuHaZ5DL09ZG1D1t17apDudb7BhMwmAMNk3jGH7EAu](https://www.technologyreview.com/s/612713/five-emerging-cyber-threats-2019/?fbclid=IwAR3PHtUTKKKnG8bmuHaZ5DL09ZG1D1t17apDudb7BhMwmAMNk3jGH7EAu)
do

