AMIYA

攻めのサイバーセキュリティ

セキュリティ投資がいかに収益を増大させるか？

監修
京都大学経済学研究科教授
坂出 健（さかで たけし）

Supervisor
監修

京都大学
経済学研究科教授
坂出 健（さかで たけし）

京都大学経済学研究科教授（国際経済安全保障）。中曽根平和研究所研究員として経済産業省経済安全保障調査委託事業有識者会議委員など務める。2023 GTCF International Workshop on Human Rights in the Digital Age (in Taipei) にて報告「Variety of Digital Democracy from the Asian View of Human Being」。著　書 The British Aircraft Industry and American-led Globalisation, 1943-82 (Routledge, 2022) にてアメリカ経済史学会賞（鈴木圭介賞）受賞。

目次 Index

はじめに ……2
サイバー攻撃のリスク ……3
サイバー攻撃の被害 ……5
サイバーセキュリティ投資 ……7
「攻め」のサイバー攻撃対策・セキュリティ投資 ……9
経営者にわかりやすくサイバーセキュリテイ投資の必要性を伝えるには？ …… 12
おわりに …… 13
セキュリティの自動化で、誰もが安全を享受できる社会へ …… 14

はじめに

サイバー攻撃リスクの増大と想定される被害額・復旧コストについては
周知のことになっていることとおもいます。
とはいえ、こうしたサイバーリスクに全社的に取り組むにはなかなか腰が重い、
現場では必要性が認識されているが経営者・経営陣には、
サイバーセキュリティ対策・投資は「コスト増大」として認識されるにとどまり、
どこか他人事のように優先順位が低いままである場合があります。
そこでこのホワイトペーパーでは、サイバー攻撃のリスクとコストの関係を整理し、
いかにサイバーセキュリティ投資が御社の収益増大に直結する投資になるのか、
また、いかに経営者・経営陣にサイバーセキュリティ投資の必要性を伝えるか、
解説します。
つまり、これまでの「受け身」のサイバーセキュリティ対策から
収益・企業価値増大をもたらす「攻め」のサイバーセキュリティ投資への
発想の転換についてお伝えします。

第1章　サイバー攻撃のリスク

近年、企業規模にかかわらずサイバー攻撃が劇的に増大しています。サイバー攻撃の種類も、マルウェア、ランサムウェア、フィッシング、DoS攻撃、SQLインジェクション、ゼロデイ攻撃など多様化・進化してきています。

背景には、企業活動にますますIT技術が浸透するようになってきている一方、社会はプライバシーに敏感になり、企業に対して個人情報管理に責任を求めるようになってきていることが挙げられます。

サイバー攻撃の目的には、ランサムウェアなどを利用した金銭の直接的な詐取、愉快犯が行う好奇心を満足させるような技術や理論の検証、あるいは、他の目的で、民間企業の情報システムや個人のパソコン、スマートフォンなどの端末に不正に侵入し、重要な内部情報を盗んだり、裏で監視し続けたりすることなどがあります。

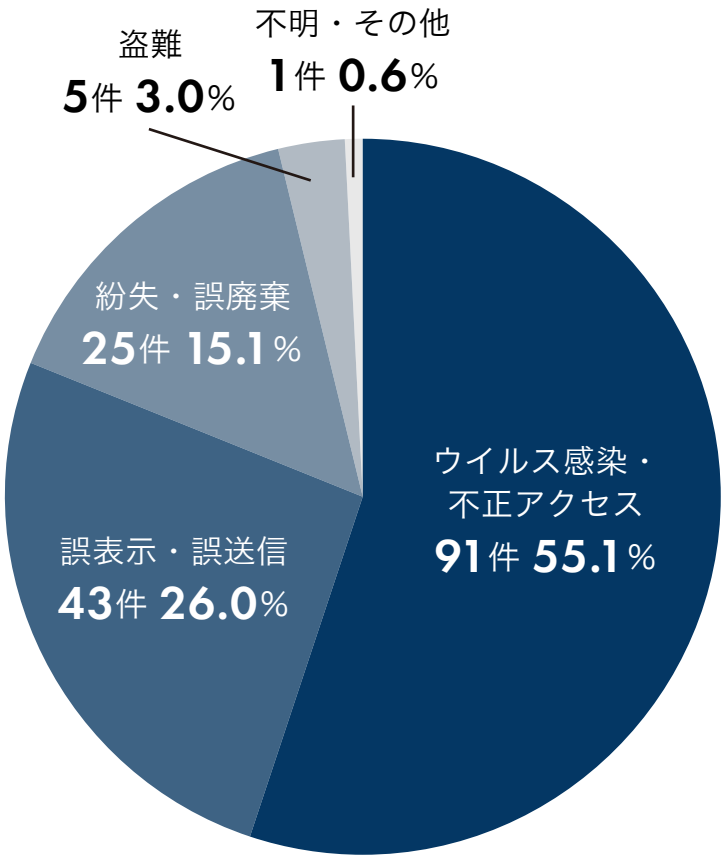
第1章　サイバー攻撃のリスク

企業の内部情報のなかでも、顧客情報などの個人情報は企業の重要な資産ですが、個人情報漏洩は企業経営の最大のリスクの一つとなっています。

情報漏洩の原因としては、誤操作、紛失・置き忘れ、管理ミス、などといった人為的なものももちろんまだまだ色濃く残るものの、昨今はやはり「ウイルス感染・不正アクセス」などといったサイバー攻撃によるものが55.1%と、その大半を占めています。そしてサイバー攻撃によって個人情報が漏洩すると、その規模・影響がきわめて大きくなってしまうのも特徴です。

重要な技術・重要な情報を持つにも関わらず、必要なセキュリティ対策をとっていない組織・企業が社会にはまだまだ多く存在し、このような企業が狙われる傾向にあるようです。

情報漏えい・紛失事故件数　原因別



東京商工リサーチ調べ

参考：『個人情報漏えい・紛失事故 2年連続最多を更新 件数は165件、流出・紛失情報は592万人分 ～ 2022年「上場企業の個人情報漏えい・紛失事故」調査 ～』より引用
https://www.tsr-net.co.jp/data/detail/1197322_1527.html

第2章　サイバー攻撃の被害

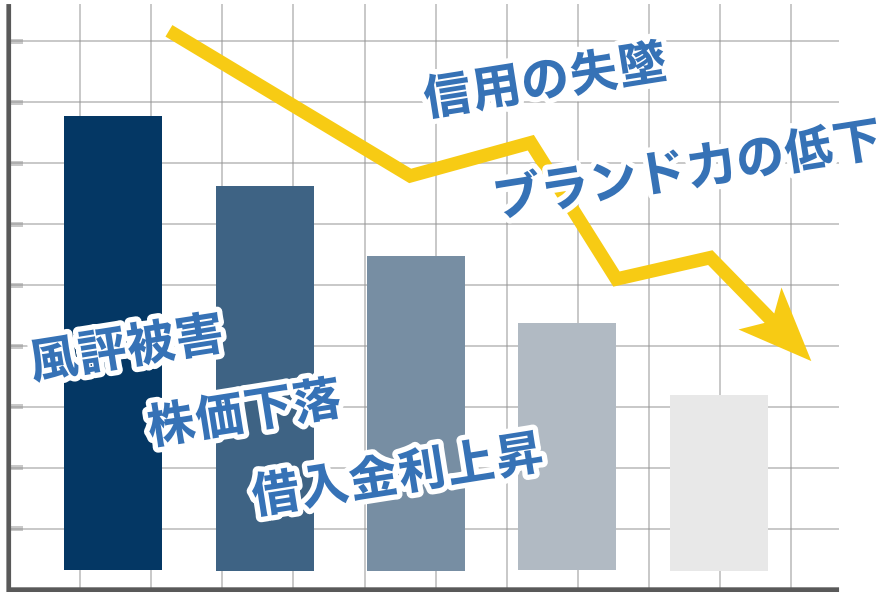
サイバー攻撃による企業の被害は、直接的には、ランサムウェアの身代金・ネットバンクからの盗難のような金銭被害、原因・被害状態の調査・解析費用、操業停止による逸失利益・費用、顧客・マスコミ対応などの公開費用があります。それだけではなく、「会社のブランド・信用」という企業の最も貴重な財産も失われることになります。顧客離れ、売り上げ減少、株価下落、借入金利上昇が起こり、風評対策・ブランド回復には多額の費用と長期の時間が必要となります。

金銭被害
ランサムウェア等による身代金・ネットバンクからの盗難など

調査・解析/復旧費用
原因･被害状況の調査費や､復旧費用､再発防止策実行の為の費用など

逸失利益
創業停止による利益損失や、被害者・取引先への損害賠償金支払いなど

公開費用
謝罪会見の開催費用や、被害者への告知費用など



Point　サイバー攻撃被害は、その後の事業継続にも大きな影響を及ぼす

第2章　サイバー攻撃の被害

そして、サイバー攻撃による経済的損害は今後ますます増大する傾向にあります。その事情を米国戦略国際問題研究所 (CSIS) は、2016 年の報告書「サイバー犯罪の経済的インパクト」で、次のように分析しています。

第一に、サイバー犯罪者は新しい技術を採用するが、防御側が一歩遅れという非対称性があり、
第二に、ネット利用者が増大し、サイバー犯罪のターゲットになっている、
第三に、北朝鮮等サイバー犯罪の中心となる犯罪センターが増加している、
第四に、サイバー犯罪で窃取した情報等の現金化が容易化している、
第五に、サイバー犯罪に用いるツールがダークウェブで多数取引され、クラウドベースで犯罪ツールを提供するサイトも多数でてきた、などです。

つまり、第一章で見たようにサイバーインシデントの発生リスクは増大(↑)し、第二章でみたように被害額も増大(↑)していきます。これを簡略な式にすると次のようになります。

式 1

サイバーインシデント発生確率（↑） × **サイバーインシデント被害額（↑）** ＝ **今後のサイバー攻撃脅威は悪化の一途をたどる**

それでは、この飛躍的に上昇する傾向にあるサイバー攻撃被害を未然に防ぐサイバーセキュリティ対策を、高精度かつ比較的安価に実施するにはどうしたらしたらいいのでしょうか？

第3章　サイバーセキュリティ投資

情報セキュリティ対策には、大きく①技術的②物理的③組織的④人的の四つの角度からすすめる安全管理措置があります。

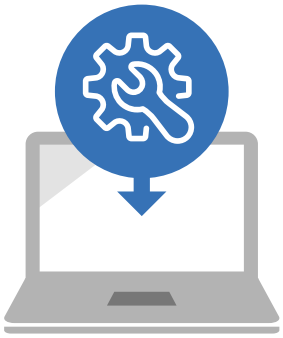
①は主に、IT セキュリティツールを使用して情報を守ることに主眼があります。

②の物理的側面―防犯対策、入退室管理、盗難防止、書類廃棄など、実体的セキュリティは今後ともその重要性がなくなりません。

③組織面は、情報セキュリティに関する組織や手順を策定し、社員に周知することを指します。

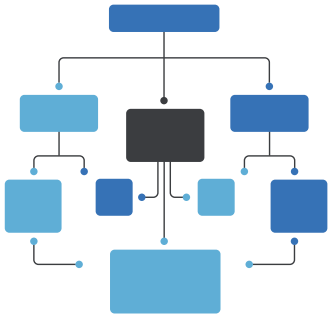
④人的側面は、社員のセキュリティ講習教育訓練・e ラーニング等が含まれます。

情報セキュリティ対策の強化に欠かせない4つの視点



① 技術的

② 物理的



③ 組織的

④ 人的

第3章　サイバーセキュリティ投資

新たな攻撃方法が次々に生まれているので、必要なサイバーセキュリティ対策は年々増加しています。そのため、サイバーセキュリティ担当者の負担も増加しますが、その反面でサイバーセキュリティ人材は不足しています。

そのため対策効率化のためのAIの活用やその一分野である機械学習等を活用した対策のための作業の自動化を進める必要性があります。つまり今後、こうした情報セキュリティの高精度化・コスト低減・ユーザーフレンドリー性をすすめるには AI・自動化ベースが切り札になります。AI 自動化をすすめることで、よりシンプルで扱いやすい高水準のセキュリティを享受することができ、その結果、①リスクの最小化、②追加コストの最小化がすすみます。

Point　これからのセキュリティには、AI・自動化ベースが切り札

第4章　「攻め」のサイバー攻撃対策・セキュリティ投資

サイバー攻撃対策・セキュリティ投資は、これから成長を続ける企業にとって、リラクタントな（渋々の）「必要出費」にとどまるものではありません。むしろ、セキュリティ投資は重要なビジネス・チャンスです。

現在、国内外で個人データの取り扱いに関する規制が強化されつつあります。この分野で先進的なEUでは、「EU一般データ保護規則」（GDPR：General Data Protection Regulation）という、個人データ保護やその取り扱いについて詳細に定められたEU域内の各国に適用される法令が2018年5月25日に施行されています。EU圏の企業・団体と取引のある日本企業はすでにGDPRの適合する必要に迫られています。こうした傾向はEUだけでなく世界的に強化する傾向にあるといえます。

つまり、個人データ・セキュリティ基準をクリアした企業には、そうでない企業より競争優位が獲得され、基準をクリアした先進的な「ホワイト」企業同士の取引・入札にもビジネス・チャンスが広がるのに対し、逆に、基準に対して「グレー」「ブラック」な企業は市場からの退出を迫られることになります。

また、セキュリティ対策の情報開示自身も企業価値向上につながります。

実際に、総務省が公表している「サイバーセキュリティ対策情報開示の手引き」（下図参照）でも、サイバーセキュリティ対策の情報開示は企業にも様々なメリットがあると明記しています。

なお、付言すれば、サイバーセキュリティ対策の情報開示は企業の立場からすれば、以下のような効果も期待できる。

- ✓ サイバーセキュリティ対策の情報開示を目指すことによって、開示内容に対応するよう、自社、子会社、業務委託先、調達先等のサイバーセキュリティ対策強化の取組が進展することが期待される。
- ✓ ステークホルダーからの信頼と高い評価を得て、自社の社会的評価や自社の商品・サービスのブランド価値の向上につながることが期待される。
- ✓ 対外的な情報開示が社内や子会社・グループ会社、外部委託先のサイバーセキュリティ対策の意識向上の観点に寄与するなど、関係者に対する啓蒙・啓発の観点からの効果が期待される。
- ✓ ISAC（Information Sharing and Analysis Center）などの情報共有コミュニティでの情報共有や、同業他社の開示情報の参照を通じ、自社のサイバーセキュリティ対策強化の契機になることが期待される。

参考：総務省『サイバーセキュリティ対策情報開示の手引き（P8）』より引用 https://www.soumu.go.jp/main_content/000630516.pdf

第4章　「攻め」のサイバー攻撃対策・セキュリティ投資

企業のサイバーセキュリティ対策に関する情報開示には次の三段階があります。
第一者開示の段階は、企業内の情報共有です。第二者開示は、サプライチェーンを構成する取引先など限られた範囲での情報共有です。第三者開示は、企業から市場に対する開示で、その企業がサイバー攻撃のリスクを的確に把握して対策を講じているので、事業継続などの観点からみて経営リスクが低いと判断することができるようになります。
こうした段階を踏むことで、企業の市場価値は上昇していきます。
まとめると、以下のような式となります。

式1

サイバーインシデント発生確率（↑）× サイバーインシデント被害額（↑）＝ 今後のサイバー攻撃脅威は悪化の一途をたどる

このままでは危ない

セキュリティを投資と捉える

式2

適切なセキュリティ対策の実施により
（サイバーインシデント発生確率（↓）× サイバーインシデント被害額（↓））× AI自動化の活用により セキュリティ対策費用（↓）× セキュリティ対策の情報開示により ビジネスチャンス（↑）＝ 収益増大・企業価値増大

ピンチがチャンスに

Point　セキュリティは、もはや【コスト】ではなく【投資】である

第5章　経営者にわかりやすく
サイバーセキュリテイ投資の必要性を伝えるには？

上記のようなサイバーセキュリティ対策の必要性はサイバーセキュリティ担当者・現場では認識されているのですが、その予算的・人員的必要性が経営者・経営陣に共有されない場合が多いのが実情です。それでは、経営者・経営陣にサイバーセキュリティ投資の必要性を伝えるにはどうしたらいいのでしょうか？

そのためには、まず前述の式1・式2のロジックを、各社の事情に応じた当てはめ、修正・追加をし、経営陣が好む①リスト化②ストーリー化③図式化④数値化などのプレゼンをしてみたらどうでしょうか。

おわりに

サイバーセキュリティ投資は企業にとって「受け身」の重荷でなく、「攻め」の企業経営に必須の「競争手段」なのです。この発想転換をサイバーセキュリティ担当者・現場だけでなく、全社的に浸透させることによって御社の貴重な財産である個人情報・技術情報をサイバー攻撃から堅守し、企業ブランドを保持し、さらには新たなビジネス・チャンス、収益・企業価値増大をもたらすことができます。

参考文献

谷脇康彦『サイバーセキュリティ』(岩波新書、2018)
松原実穂子『サイバーセキュリティ』(新潮社、2019)

AMIYA's Mission

セキュリティの自動化で、誰もが安全を享受できる社会へ

株式会社網屋では、「セキュリティの自動化」を目指しAIテクノロジーや
独自のクラウドネットワーク技術を活用した様々なセキュリティ製品やサービスを開発・製造・販売しています。
すべての人がサイバー攻撃のターゲットとなる時代に、すべての人が高水準のセキュリティを受けられる社会を実現したい。
それが私たちのアイデンティティです。

人口減少が進む今、網屋が果たす役割。求められるのは、テクノロジーによる「自動化」

AMIYA's Service

ログ管理

ALog

複雑なログをわかりやすく管理。AIと高度な分析機能で効果の見えるログ管理を実現。

詳細はこちら

クラウドCSIRTサービス

セキュサポ

当社のセキュリティ専門チームがお客様の環境全体を監視し、ランサムウェア攻撃をはじめとした一連のサイバー攻撃への対策を包括代行。

詳細はこちら

脆弱性診断サービス

セキュリティ監査サービス

Data Security
データセキュリティ事業

Security Service
セキュリティサービス事業

AMIYA
サイバーセキュリティプロバイダ

Network Security
ネットワークセキュリティ事業

Security Education
セキュリティ教育事業

クラウドネットワークインフラ

Network All Cloud®

煩わしいネットワーク構築や、導入後の運用や障害対応までをクラウド上のサポートセンターが代行。

詳細はこちら

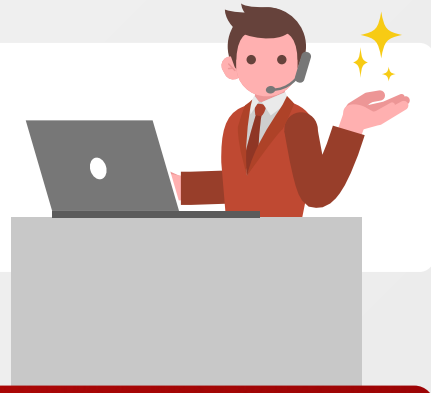
サイバーセキュリティトレーニング

経営層から一般社員、エンジニアまで網羅的なサイバーセキュリティトレーニングで組織のセキュリティレベル向上をサポート。

詳細はこちら

まずはセキュリティについてお気軽にご相談下さい。

電話	メール	フォーム
03-6822-9996	bv-sales@amiya.co.jp	お問い合わせフォーム



緊急でお困りの方は下記へご連絡ください。

緊急インシデント対応サービス

緊急インシデント対応サービスは、事業継続を脅かすセキュリティインシデントの被害を最小化するために、
素早い原因特定・状況把握、調査・分析を行い復旧に向けて、総合的に支援するサービスです。

今すぐ電話で相談する

03-6822-9909

（平日 9:00 ～ 18:00）

または

お問い合わせフォームから相談する

こんなインシデントに対応します

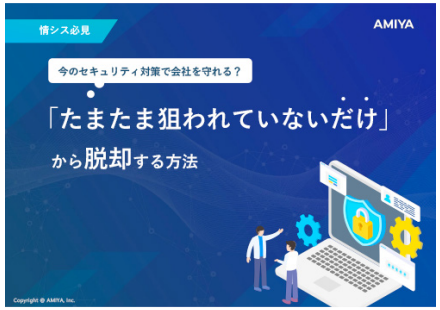
- 怪しいメールを開いてしまった…
- データが暗号化されてしまった…
- 第三者より情報漏えいの指摘があった…
- 知らないうちにWeb サイトが書き換わっている

網屋では、様々なセキュリティホワイトペーパーを無料で配布しています。

【弁護士監修】
法的観点で見るインシデント対応

サイバー攻撃や不正アクセスなどのサイバーインシデントの発生時、企業には法的にどのような対応が必要になるか。弁護士蔦大輔氏監修のもとわかりやすく解説しています。

資料をダウンロード



今のセキュリティ対策で会社を守れる？
「たまたま狙われていないだけ」から脱却する方法

新たな働き方の普及、様々なクラウドサービスの台頭、柔軟なデータ活用……現代のビジネスを取り巻く要素や課題と、その効果的な対策について解説します。

資料をダウンロード

サイバー攻撃の被害は
Active Directoryで最小化する！

あらゆるサイバー攻撃が AD を経由することに着目し、内部対策の中でも AD をテーマに、AD における対策や AD のログ管理などを解説していきます。

資料をダウンロード

Secure the Success.

網屋の事業は、セキュリティ。

セキュリティ製品やサービスを自ら開発・製造・販売する、セキュリティの総合プロバイダです。

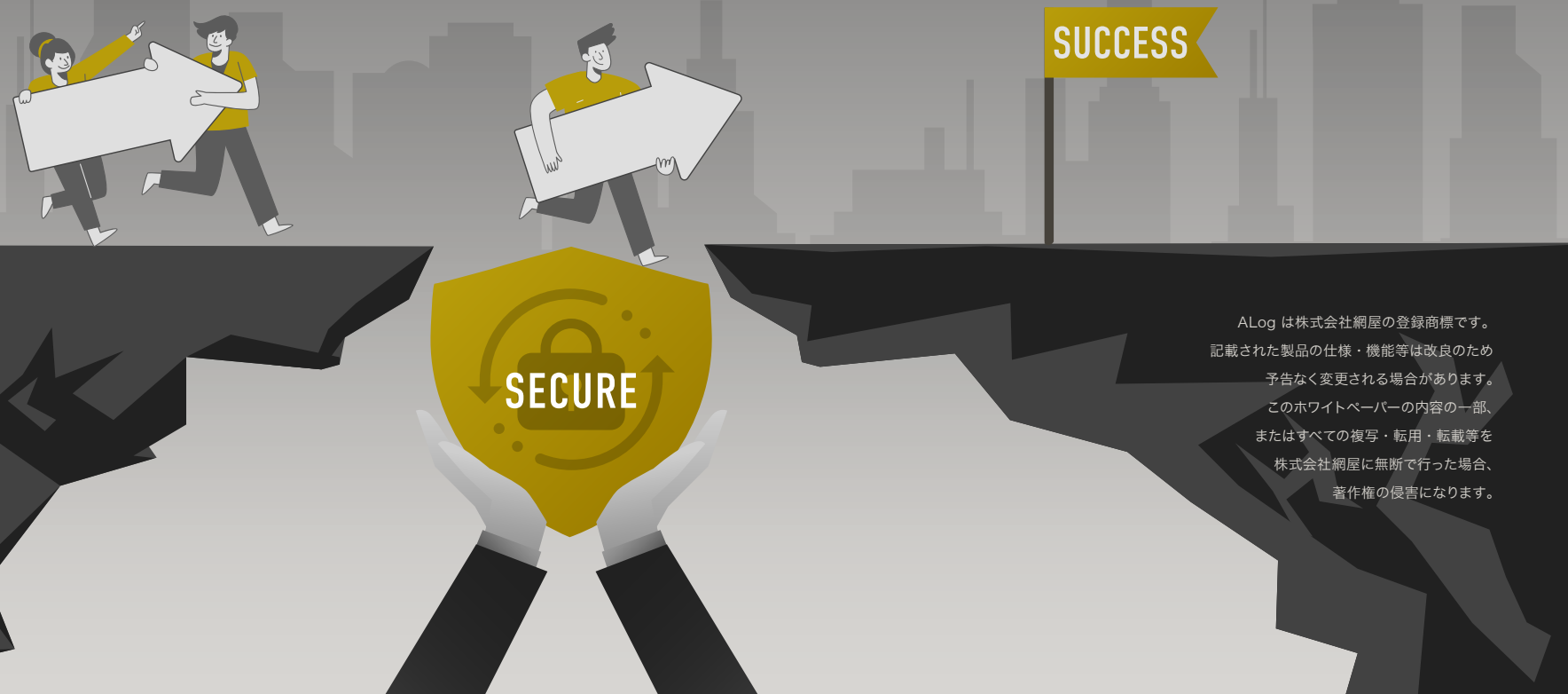
サイバー攻撃は、経済的余裕度に関係なく、全ての事業法人がターゲットになります。

サイバー攻撃の脅威を「セキュリティの自動化」で解決し、

高水準のセキュリティを誰でも享受できる社会を創りたい。

それが私たちのアイデンティティです。

AMIYA



株式会社 網屋

https://www.amiya.co.jp/

〒103-0007
東京都中央区日本橋浜町3-3-2
トルナーレ日本橋浜町 11F
TEL: 03-6822-9999
FAX: 03-6822-9998

ALog は株式会社網屋の登録商標です。
記載された製品の仕様・機能等は改良のため
予告なく変更される場合があります。
このホワイトペーパーの内容の一部、
またはすべての複写・転用・転載等を
株式会社網屋に無断で行った場合、
著作権の侵害になります。