WEBアプリケーション脆弱性スキャンニングサービス

～あなたのWEBサイトは乗っ取られてませんか？～

◎イスラエルGamaSec社製品のご案内(2016年10月27日)

GamaSecJapan　大田佳一郎
らぼ･コミスペ　藤森慎太郎

GamaSec
Trusted Website Security

GamaSec社の製品

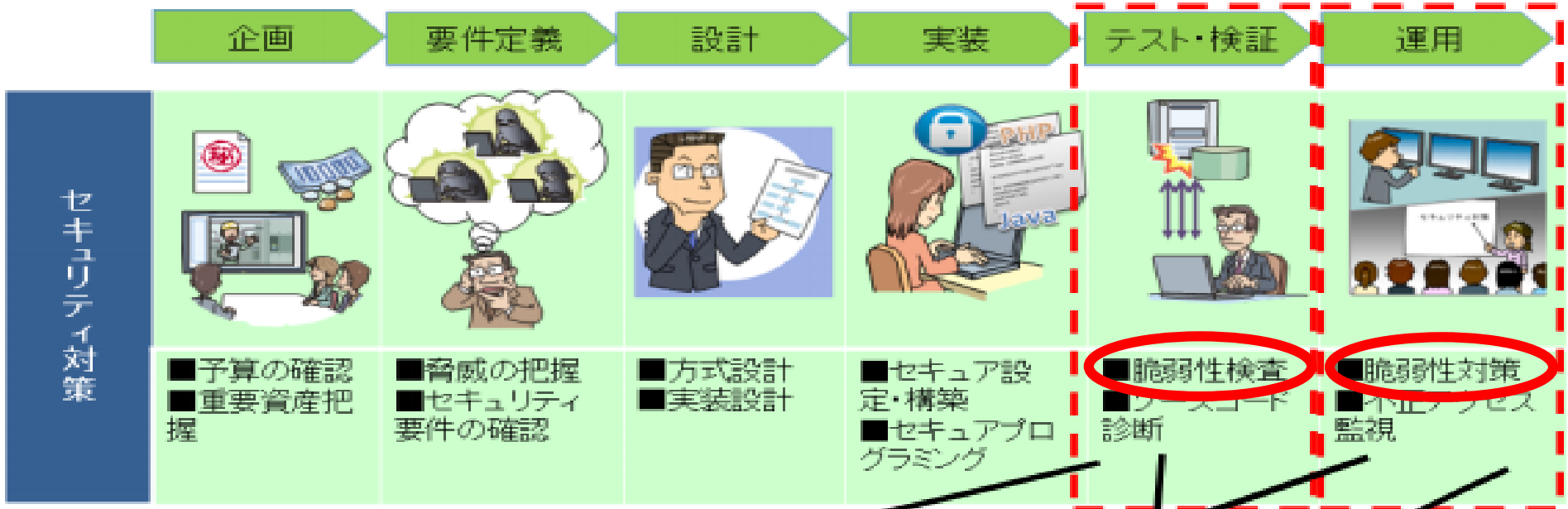
クラウド型脆弱性診断

	製品名	製品概要
1	GamaScan	脆弱性診断を毎月１回1年間行います。(ダース契約といいます。)
2	GamaWare	マルウェアの存在を1年間毎日診断します。
3	GamaShield	GamaScanとGamaWareの組み合わせで対策を行います。
4	GamaScan(シングル)	ワンショットの脆弱性診断です。開発会社および監査時向けです。
5	Gama　Penetration	ご要望に応じたペネトレーション試験を行います。(イスラエルとの調整あり)

脆弱性検査ツールの活用フェーズ

GamaSec Trusted Website Security

IPA著 「ウェブサイトにおける脆弱性検査手法（ウェブアプリケーション編）」(2016年9月28日改訂版)より抜粋



品質向上 GamaScan

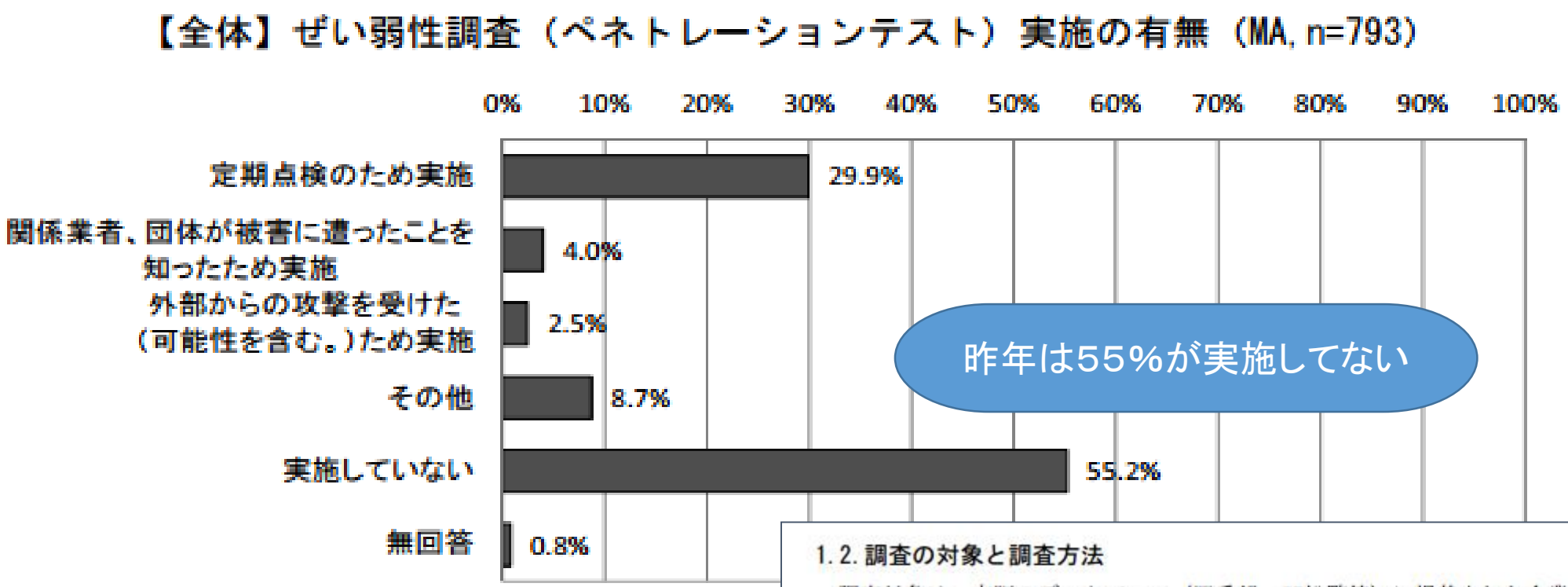
納品検収 GamaScan (シングル)

運用 GamaWare GamaScan (ダース)

OSS オワスプ ジャパン

SECURED gamasec.com 09-OCT-2016

脆弱性診断の実施状況



昨年は55%が実施してない

1. 2. 調査の対象と調査方法

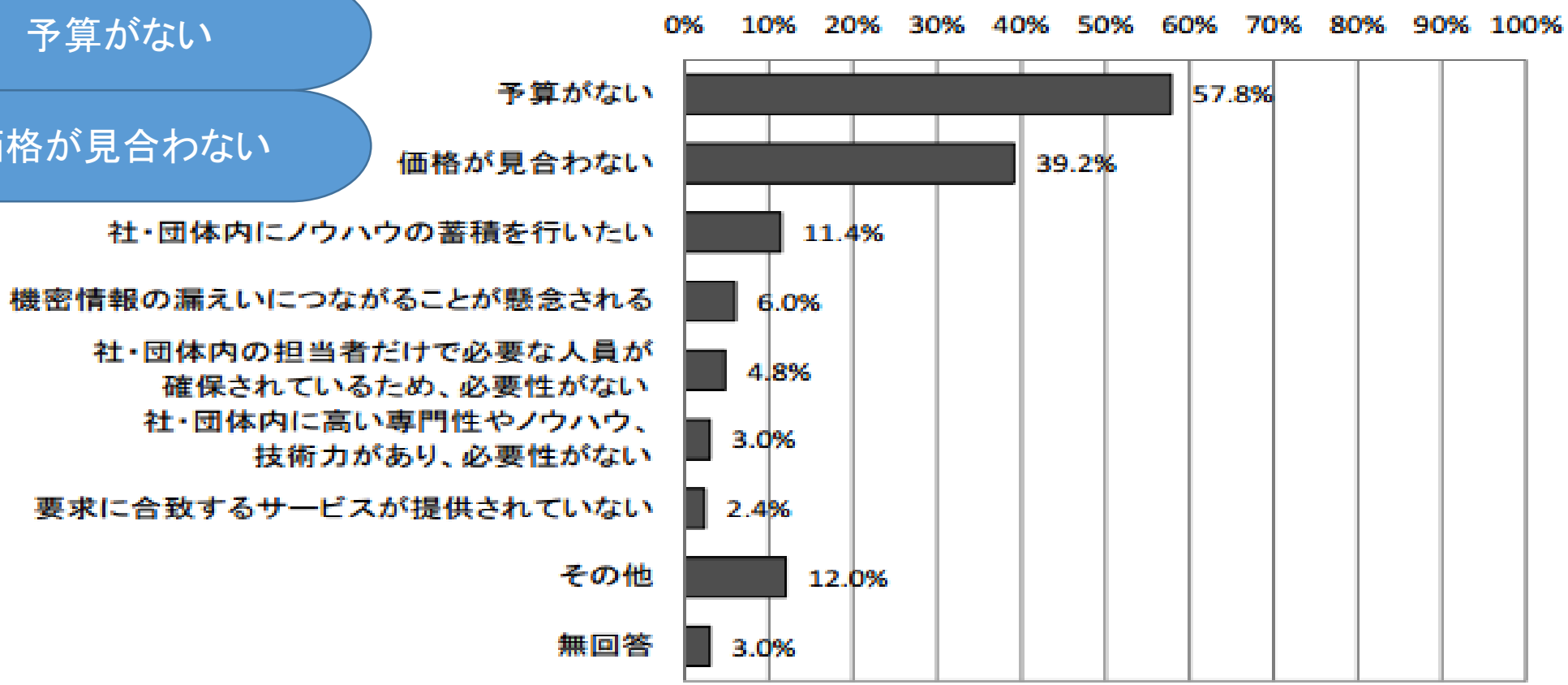
調査対象は、市販のデータベース（四季報、IT総覧等）に掲載された企業、教育機関（国公立、私立の大学等）、医療機関、地方公共団体（県・市町村等）、独立行政法人（教育機関及び医療機関に掲げるものを除く。）、特殊法人から特定の業種、地域に偏りのないよう3, 050件を無作為に抽出した。

警察庁生活安全局情報技術犯罪対策課著 「不正アクセス行為対策等の実態調査　調査報告書　平成27年10月」より抜粋

脆弱性診断の実施しない理由

予算がない

価格が見合わない



警察庁生活安全局情報技術犯罪対策課著 「不正アクセス行為対策等の実態調査　調査報告書　平成27年10月」より抜粋

脆弱性診断の相場

製品名	1回あたりの価格	期間	特記事項
一般既成製品	数十万円～数百万円	一か月以上	ページ数の制約があるところもある。 打合わせ時間および試験環境構築時間を要す。 運用中は、システム停止が必要。
GamaScan	¥20,000以下	数日	ページ数の規定なし クラウドによる検査 運用中もシステム停止等の制限なし

※但し、GamaSec社のペネトレーションテストの場合は、項目による見積もりが必要であり、打ち合わせ等の時間がかかります。

GamaSec社について

GamaSec社は、WebサイトおよびWebアプリケーションの脆弱性を診断するSaasソリューションを提供するイスラエルの会社です。

軍事技術

イスラエル国（軍）が要求する規格をクリアした技術を使用しています。

AI技術

リアルタイムで対応し続けるためAI技術を用いて、シミュレーションシナリオを随時更新しています。

だが、日本安全保障・危機管理学会主任研究員の新田容子氏は言う。

「イスラエル軍のサイバー部門は米露にも伍す優秀さで知られています。同国は官民一体でセキュリティ技術を開発、輸出するなど、日本の一歩も二歩も先に行っています」

デイリー新潮（**2016年4月7日号 掲載**）より抜粋

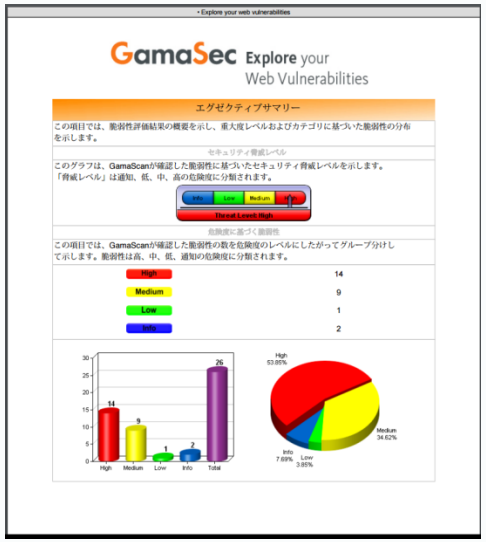
脆弱性監査実績

全世界で500,000ドメイン超の脆弱性監査実績

GamaSecの設立以降、**イスラエル政府系機関**をはじめ、アプリケーション、ウェブサイトを持った、世界的なグローバル企業がGamaScanを利用しています。

例

GamaScan報告書
（日本語表記）



https://drive.google.com/drive/folders/0B0P_WWAQov7seXNFbGVRakcxdDQ?usp=sharing

日本政府のサイバーテロ対策について（抜粋）

日本政府のセキュリティ対策

サイバーセキュリティ戦略本部著「サイバーセキュリティ2016」(2016.08..31)より抜粋

政策の3本柱

経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

国際社会の平和・安定及び我が国の安全保障

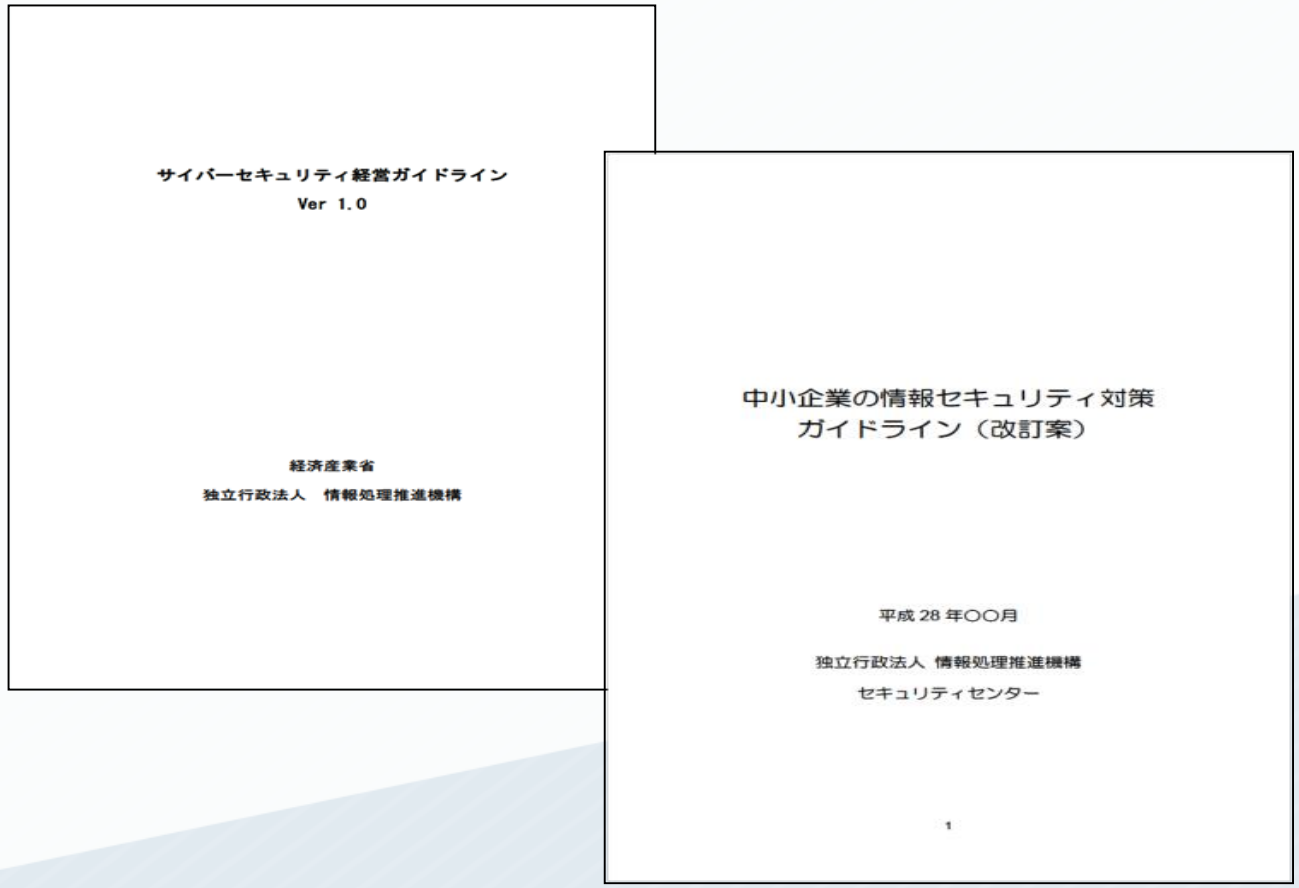
～ サイバー空間における積極的平和主義 ～

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

■セキュリティマインドを持った企業経営の推進

➢ サイバーセキュリティ経営ガイドラインの普及【経済産業省】



営業秘密官民フォーラム
および営業秘密保護の対策推進

(2) 公正なビジネス環境の整備

(ア)経済産業省において、産業界と協力し、企業情報の漏えいに関して、サイバー攻撃など今後ますます高度化・複雑化が予想される最新の手口や被害実態などの情報の共有を行う場として、関係省庁とも連携し「営業秘密官民フォーラム」を開催する。

(イ)経済産業省において、企業の情報漏えいの防止に資するため、「秘密情報の保護ハンドブック～企業の価値向上に向けて～」についての普及啓発を図る。

(ウ)経済産業省において、IPAを通じて、営業秘密保護に関する対策等を推進するため、組織における内部不正防止のためのガイドラインの普及促進を図る。

サイバーセキュリティ戦略本部著「サイバーセキュリティ2016」(2016.08..31)より抜粋

不正競争防止法では、企業が持つ秘密情報が不正に持ち出されるなどの被害にあった場合に、民事上・刑事上の措置をとることができます。そのためには、その秘密情報が、不正競争防止法上の「営業秘密」として管理されていることが必要です。

情報リスクの数値化方法

GamaSec Trusted Website Security

IPA著「中小企業の情報セキュリティ対策ガイドライン（改訂版）平成28年」より抜粋

情報のリスク値

＝

情報の資産価値

指標		3	2	1
(a)対象となる情報資産の重要度（資産価値）	機密性	漏えいが企業の存続を左右する	漏えいが企業の業務に重大な影響を及ぼす	漏えいしても大きな影響なし
	完全性		改ざんが企業の業務に重大な影響を及ぼす	改ざんがあっても大きな影響なし
	可用性		情報が利用不可で業務に重大な影響あり	利用できなくても大きな影響なし

×

驚異の発生頻度

(b)脅威がどの程度起こりうるか（発生確率や頻度）	通常の状態で発生する（いつ発生してもおかしくない）	特定の状況で発生する（年に数回程度）	通常では発生しない（数年に1回未満）

×

脆弱性

(c)被害を生じさせるきっかけ（脆弱性）	ある（ほぼ無防備）	一部残存（部分的対策）	ほぼない（対策済み）

サーバーセキュリティの成長産業化 および情報セキュリティ投資促進

サイバーセキュリティ戦略本部著「サイバーセキュリティ2016」(2016.08..31)より抜粋

(1) サイバーセキュリティ関連産業の振興

(ア)経済産業省において、NEDO等の支援事業や政府系ファンドによるベンチャー企業や国内外で大規模に活躍できる企業の育成など、サイバーセキュリティの成長産業化に取り組む。

(イ)総務省及び経済産業省において、クラウドセキュリティガイドライン、クラウドセキュリティ監査制度の普及促進を行う。

(ウ)経済産業省において、中小企業における情報セキュリティ投資を促進するための施策を推進する。

(エ)文部科学省において、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に関する措置を速やかに講ずる。

サーバーセキュリティ対策ガイドラインの普及およびサイバーセキュリティ保険

GamaSec
Trusted Website Security

1.2. セキュリティマインドを持った企業経営の推進

(1) 経営層の意識改革

(ア)内閣官房及び金融庁において、上場企業におけるサイバー攻撃によるインシデントの可能性等について、米国の証券取引委員会（SEC）における取組等を参考にしつつ、事業等のリスクとして投資家に開示することの可能性を検討し、結論を得る。その際、関連情報の共有など開示するインセンティブを促すための仕組みの在り方についても併せて検討し、結論を得る。

(イ)経済産業省において、経営層がサイバーリスクを経営上の重要課題として把握し、設備投資、体制整備、人材育成等経営資源に係る投資判断を行い、組織能力の向上を図るために、説明会等を通じて、サイバーセキュリティ経営ガイドラインの普及を図る。

(ウ)経済産業省において、企業のサイバーセキュリティ対策を推進するため、サイバーセキュリティ保険など、情報の保護が必要となる政府の補助事業や研究開発事業等の採択に際して、上記のサイバーセキュリティ経営ガイドラインや第三者認証取得など企業のサイバーセキュリティ対策への取組を、加点要素等として考慮する仕組みなどのインセンティブ策を検討する。

サイバーセキュリティ戦略本部著「サイバーセキュリティ2016」(2016.08..31)より抜粋

サイバー犯罪への対策の強化

GamaSec
Trusted Website Security

(3) サイバー犯罪への対策

(ア)警察庁において、新たな手口の不正アクセスや不正プログラム（スマートフォン等を狙ったものを含む。）の悪用等急速に悪質巧妙化するサイバー犯罪の取締りを推進するため、サイバー犯罪捜査に従事する全国の警察職員に対する部内研修及び民間企業への講義委託の積極的な実施、官民人事交流の推進、技術的に高度な民間資格の活用等、サイバー犯罪への対処態勢を強化する。

サイバーセキュリティ戦略本部著「サイバーセキュリティ2016」(2016.08..31)より抜粋

法的罰則

	法律（略称）	罰則
1	不正アクセス禁止法	3年以下の懲役又は100万円以下の罰金
2	威力業務妨害罪	3年以下の懲役又は50万円以下の罰金
3	電子計算機損壊等業務妨害罪	5年以下の懲役又は100万円以下の罰金

※　GamaScanは、許可されたWEBにしか脆弱性診断を実施しません。

今後の普及活動について

GamaSec
Trusted Website Security

（１）各県に代理店および全国販売店を作ります。
　　代理店は、主に自治体向けに展開するためです。
　　全国販売店は、希望する企業向けです。

（２）ITコーディネータ等の企業経営コンサルへの提供
　　専門家向けにGamaScanシングルの提供を考えています。

（３）開発会社向け
　　納品等の品質向上のために使用してください。
　　条件等は別途調整とします。

（４）クラウド製品提供企業
　　クラウドによるサービス提供会社への提供

契約条件

1．販売ノルマなし
2．月締めまとめ請求(当月払い)
3．商圏しばり一応なし
4．不正アクセスはしない
詳細は調整にて

脆弱性診断の問合わせ先

GamaScan（シングル）

九州復興支援価格 ￥12,000(税込)　11月末までの申込み

OPENスクエア宛

メール：sales_os@opensquare.co.jp

お申込み後、らぼ・コミスペ社よりご連絡させて頂きます。