セキュリティリスク対策
プランニングサービスのご説明

株式会社神戸デジタル・ラボ

Proactive Defense

Kobe Digital Labo

情報セキュリティ上のリスクとは何か

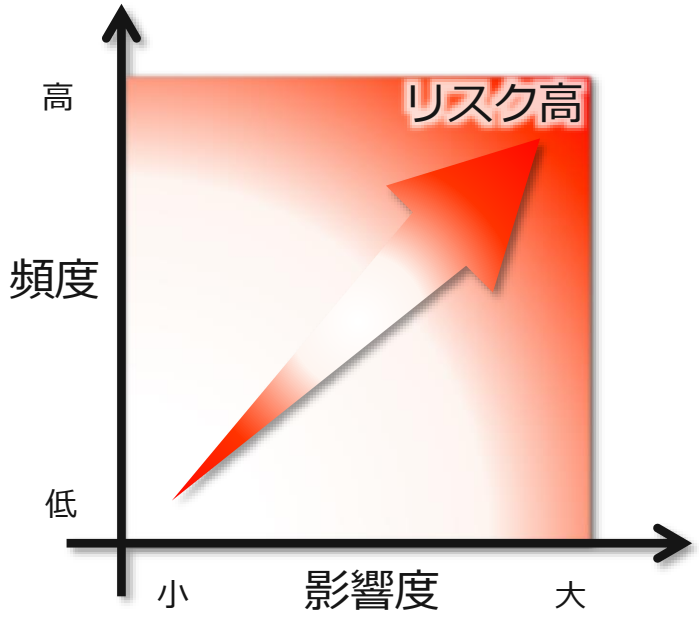
情報資産への脅威を「頻度」と「影響度」で評価したもの

が情報セキュリティ上のリスクです。

頻度	脅威（不正アクセス等による攻撃、人的ミス等による事故）が発生する頻度
影響度	脅威が発生した際に必要な対応の規模

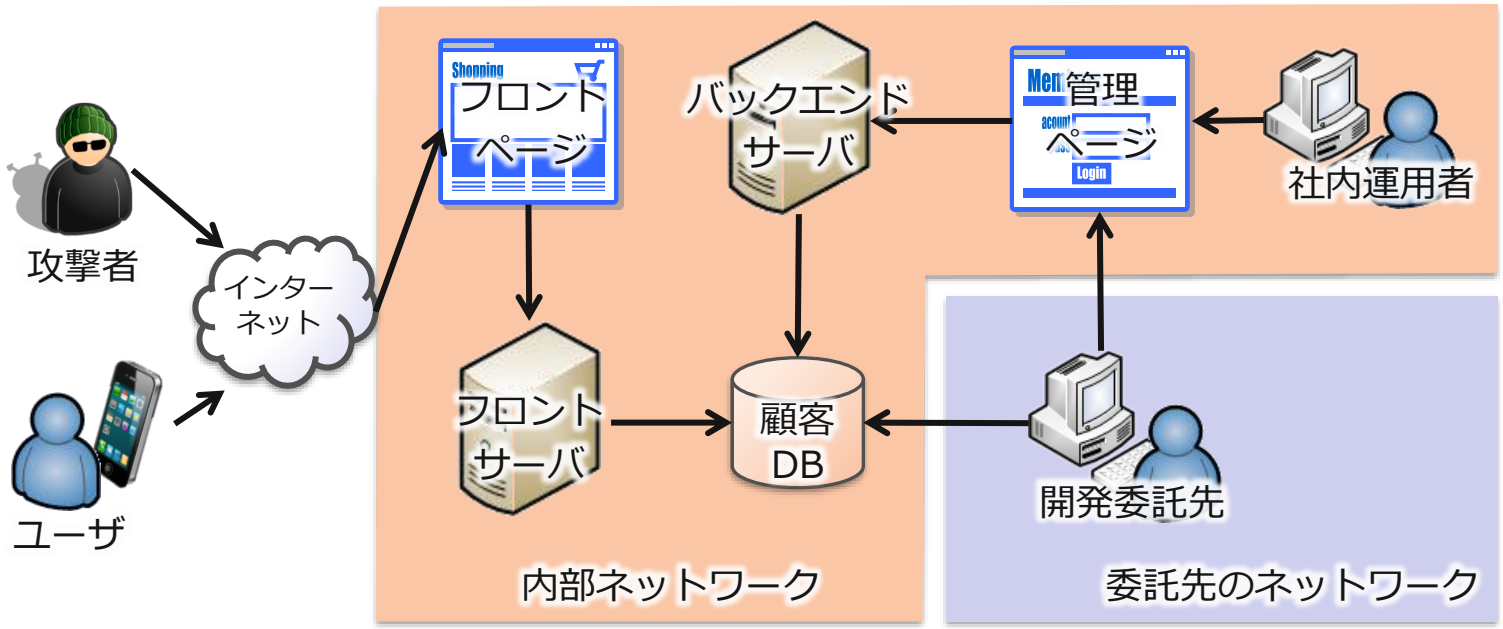
例えば、右のグラフのように、脅威の頻度が高く、影響度も大きい場合は、リスクが高いと言えます。

このリスクを洗い出すことによって、情報資産を運用する上でセキュリティの対応が必要な箇所を明らかにすることができます。



サービス概要

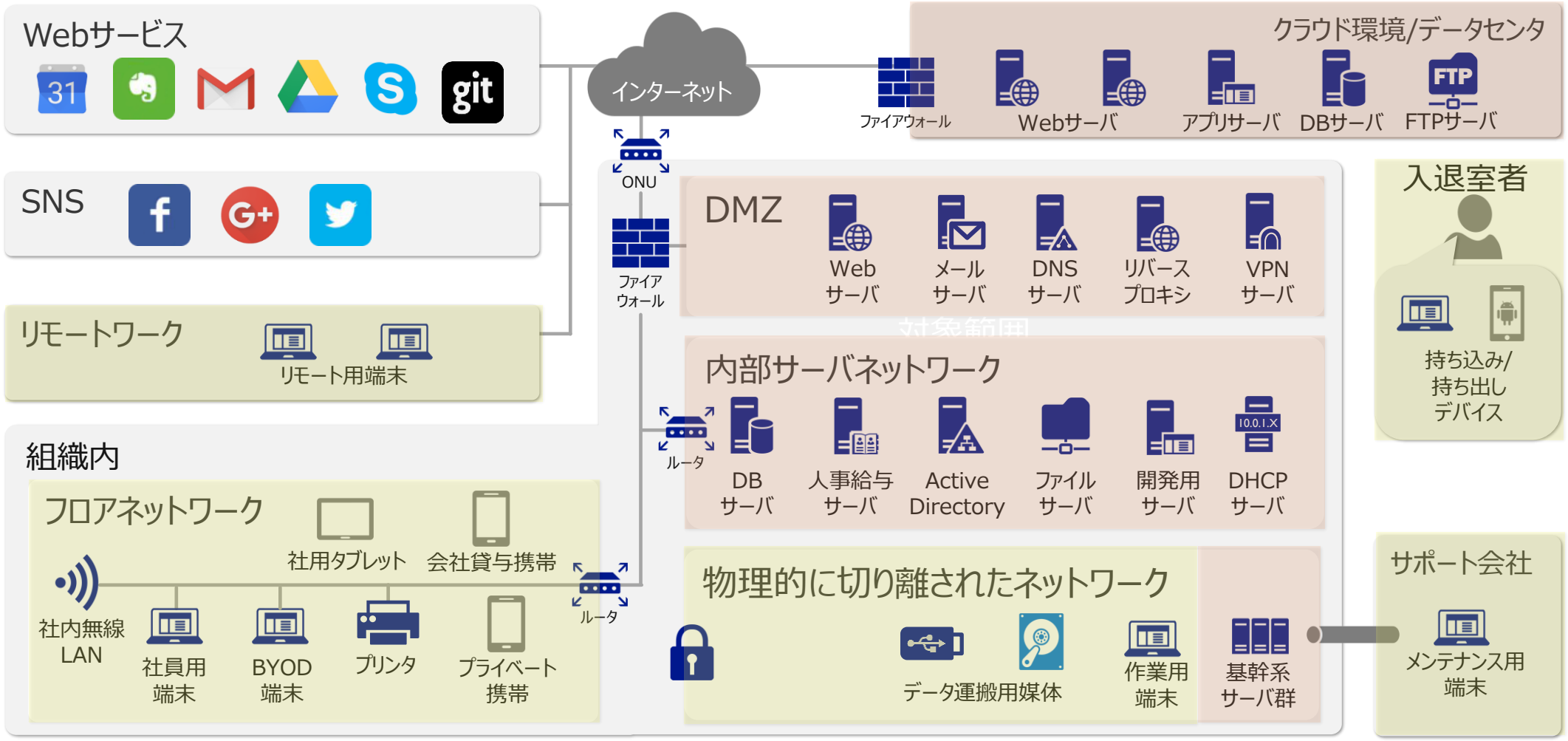
セキュリティリスク対策プランニングサービスは、システムとそれに関わる組織に対するリスクを洗い出し被害想定金額を算出した上で、今後のセキュリティ対策の方針、優先度を提案し、それに見合った必要な予算を明らかにします。



人、モノ、運用からリスクを分析し、
必要な対応をご提案します

サービス適用範囲

本サービスでは、JIS Q 27002に沿ってシステムとその運用をヒアリングベースで評価するコンサルティングとなります。以下の ■ で網掛けされた箇所にあるシステム群が主なサービス適用範囲となります。また、■ で網掛された、システムにアクセス可能な端末や担当者とその運用もサービス適用範囲となります。



サービスを利用するメリット

セキュリティ対応の進め方、迷っていませんか？

1．リスクがたくさんありそうだ！でも、どこがうちにとって一番リスクが高いのか分からない。今年も手をつけられない・・・

起こりうる攻撃の頻度と発生時被害に加え、システムの**売上への寄与と資産の規模**から、**貴社におけるリスクの高さを**見積もります。

2．セキュリティ対策をしたい！でも、何を対策すれば良いかわからない。とりあえず世間で事件が起こったものから対策しよう・・・

リスク（＝優先度）の高いものから**短期的な対策、長期的な対策に分けて提案**します。事件性にとらわれず対策の計画をたてられます。

3．セキュリティ対策のための予算を確保したい！でも、予算化するための理由が言えない。毎年予算が通らない・・・

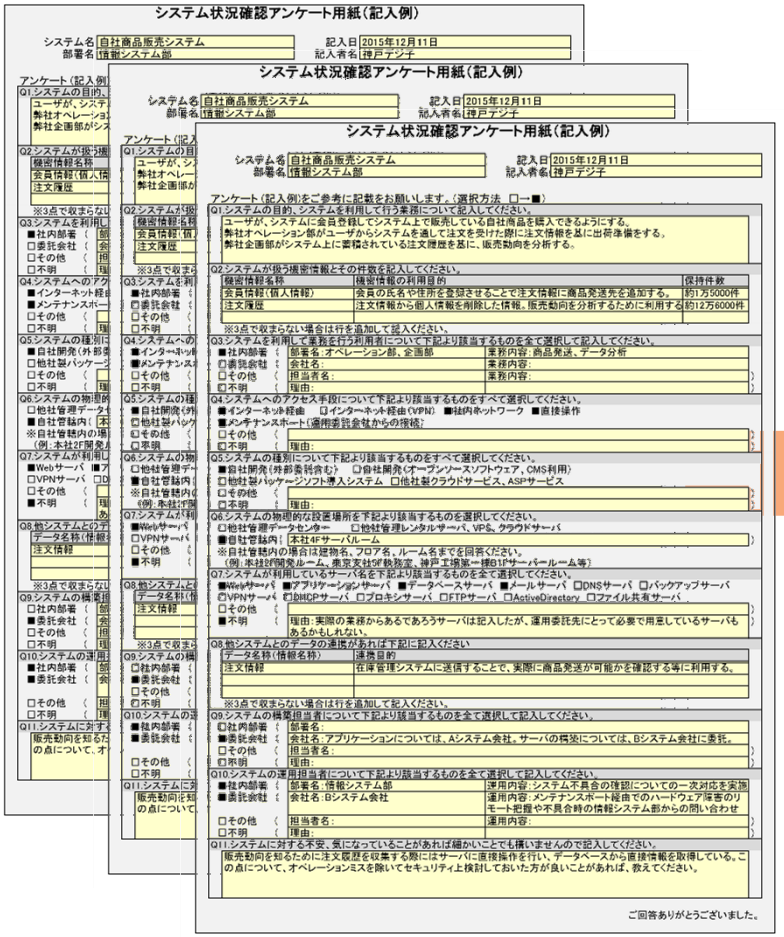
実際に情報漏洩が発生した際の**被害金額を算出**しますので、予算を投じない場合の具体的な危険性を訴えることができます。**また、運用対処でも対策可能なものはその方法も提案**するので必要最低限の予算を検討することもできます。

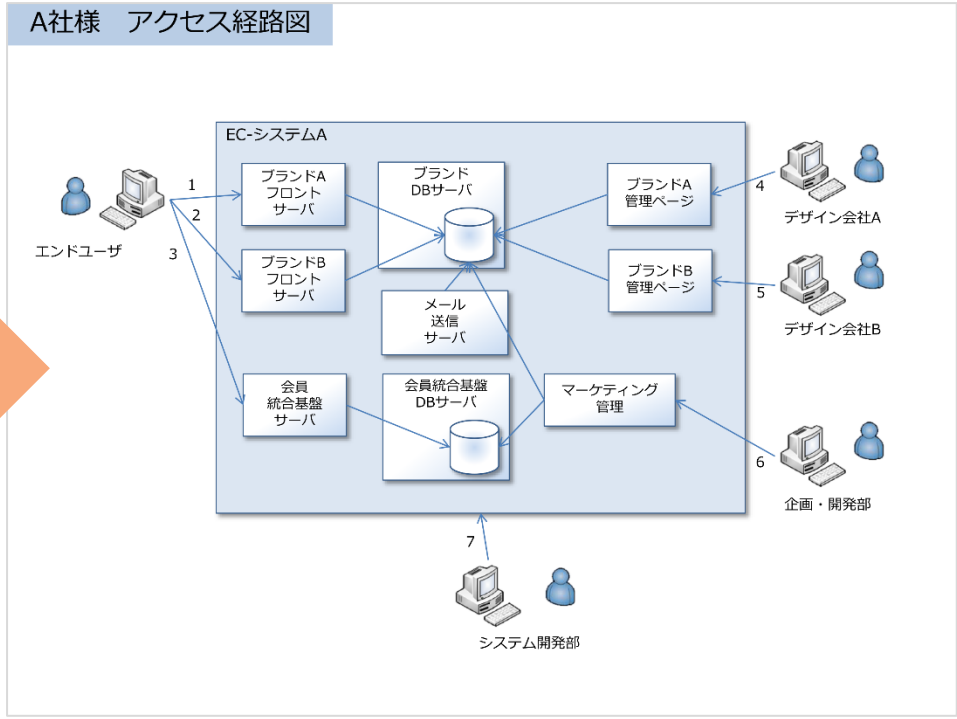
サービスの流れ

フェーズ	弊社作業	お客様作業	内容
1.全体像とアクセス経路の把握	システム状況確認アンケート、ヒアリングシートの送付 アクセス経路図の作成	システム状況確認アンケートとヒアリングシートへのご記入	お見積り時にリスク評価をするシステムを選定し、選定したシステムに対して、状況確認を行うためにアンケートを行います。これにより、システム全体像から各システムへの不正アクセスの経路を明らかにします。また、リスク評価のためのヒアリングシートを事前に送付し、可能な範囲で記入し、返信いただきます。
2.ヒアリングによるリスク評価	ヒアリング、アクセス経路図の確認 リスク評価、対策検討	未回答項目について組織内への確認	アクセス経路図と事前記入いただいたヒアリングシートを基に、各システムの機能や扱うデータを理解している人を対象にヒアリングを行い、各システムが様々な経路からの不正アクセスに対して何らかしらの対応がなされているか確認し、リスクを評価していきます。ヒアリング時に即座に答えられない項目については、お客様の組織内や担当ベンダーに確認の上後日回答いただきます。
3.高リスク事象への対策提案	評価結果、対策案確認		リスク評価の結果、高リスクの事象については対策検討をし、提案致します。
4.報告書作成	報告書作成 報告書確認		今までの作業内容をまとめ、加えて、対策を実施しない場合の被害想定金額の算出と、今までの事故事例を記載した報告書を作成します。
5.報告会の実施	経営層向け報告会実施		特に経営層に対して必要な予算を共有することを目的として、報告書の内容を基にリスクの詳細や必要な対策等を報告します。

サービスの流れ - 1.全体像とアクセス経路の把握

システム状況確認アンケートによって、システムの特性や扱っているデータの情報種別とシステム間の関係性を把握します。これにより、システム全体像を明らかにし、不正アクセスの経路を洗い出します。





サービスの流れ - 2.ヒアリングによるリスク評価

ヒアリングシートを基に各脅威に対する対応状況をヒアリングします。「抑止・予防策」の有無を確認することで、脅威の頻度を下げる対応ができているかを評価し、「回復策・検知策」の有無を確認することで、脅威発生時の影響を下げる対応ができているかを評価します。これにより各脅威の一般的に考えられるリスクをどの程度下げる働きができているか明らかにすることができます。また、対応のなされていないリスクは必然的に高リスク事象として洗い出されます。

1.リスク分析ヒアリングシート(システム用)(サンプル)

No	脅威	手段	対策種別	質問事項
1	サーバへの攻撃	なりすましや総当たり攻撃による不正ログイン	抑止・予防策	パスワードは、複雑なもの(八桁以上、パスワード世代管理、三種類以上の文字種の使用)を設定するようになっていますか。また、そのようなルールがありますか？
2				システムの利用者の認証について、1利用者、1IDとなっています
3				
4				
5				
6				
7				
8		権限		

2.リスク分析結果(サンプル)

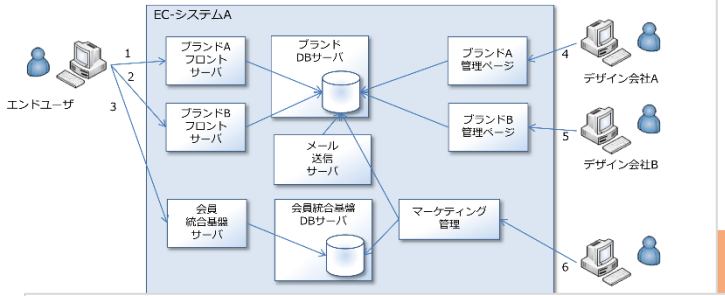
No	システム名	アクター						アクセス手段	脅威				対策状況		
		外部			内部				脅威の手段	発生頻度	影響内容	脅威発生時の影響度	予防・抑止策	予防・抑止策を実施している現状の脅威発生頻度	検知策
		一般利用者	開発担当会社	運用担当会社	特定利用者	開発担当者	運用担当者								
1	○○システム	○	○	○	○	●	●	社内ネットワーク	サーバへの攻撃:なりすましや総当たり攻撃による不正ログイン	中	サーバの乗っ取りによる、Webサイト改ざん、バックドア設置等ログインした権限で可能なことすべてが可能。	高	・明文化されたルールがあり、それに沿って複雑なパスワードを設定している。	低	・ログインログを取得し、ログイン失敗時にはアラートをにしている。
2	○○システム	○	○	○	○	●	●	社内ネットワーク	サーバへの攻撃:権限を越えた操作、管理者権限での操作ミス、悪意ある操作	中	サーバの乗っ取りによる、Webサイト改ざん、バックドア設置等ログインした権限で可能なことすべてが可能。	高	・サーバ上のファイルについては、社内ルール上特定の領域にはアクセス権限を設定している。 ・管理者アカウントは申請時のみ払い出しを行い、利用後はパスワードを変更している。	低	・操作ログを取得しているアカウントの操作ログにつウント返却後にログ内容をる。
	○○システム	○	○	○	○	●	●	社内ネットワーク	サーバへの攻撃:通信の盗聴	低	サーバへのログイン情報の搾取。	高	・シェルによるサーバへのアクセスはSSL通信による暗号化を行っている。	低	検知策なし
	○○システム	●	○	○	○	○	○	インターネット経由	サーバへの攻撃:OSやミドルウェアの既知の脆弱性を突いた攻撃	高	サーバの乗っ取りによる、Webサイト改ざん、バックドア設置等サーバ内で可能なことすべてが可能。	高	・明文化されたルールがあり、それに沿って定期的にサーバのアップデートやミドルウェアに対するパッチを適用している。 ・サーバリリース時、設定変更時にプラッ	低	・ホスト型IDSを設置し、やWebアプリケーションのている。問題があれば連ルでアラートが通知され
	○○システム							インターネット経由	Webアプリケーションへの攻撃:						

※一般的にリスクへの対応策として、攻撃を思いとどまらせる抑止策、攻撃するハードルを上げる予防策、攻撃発生を早期に知る検知策、攻撃によって発生した被害から通常状態へ戻すための回復策、これら４つが検討・実施していることが理想とされています。

サービスの流れ - 3.高リスク事象への対策提案

リスク評価の結果洗い出された高リスク事象について最も優先度の高い対策**3つ**を検討し、対策一覧にまとめます。この際に、作成したアクセス経路図も確認しながら検討します。これにより、システム毎の対策だけではなく、あるポイントに機器を導入することで複数の高リスク事象に対する一括した対策も提案できます。提案内容は機器導入等で解決できるシステム的な対策と、設定変更やルールによって解決できる運用的な対策それぞれを提案します。また、システム的な対策については大よその費用感も提示します。これによりリスクを低減するための必要予算が明らかになります。

A社様　アクセス経路図



2.リスク分析結果(サンプル)

No	システム名	アクター							アクセス手段	脅威		影響		予防・即止策
		外部			内部									
		一般利用者	開発担当会社	運用担当会社	特定利用者	開発担当者	運用担当者			脅威の手段	発生頻度	影響内容	脅威発生時の影響度	
1	○○システム	○	○	○	○	●	●		社内ネットワーク	サーバへの攻撃：なりすましや総当たり攻撃による不正ログイン	中	サーバの乗っ取りによる、Webサイト改ざん、バックドア設置等ログインした権限で可能なことすべてが可能。	高	・明文化されたルールがあり、沿って複雑なパスワードを設定する。
2	○○システム	○	○	○	○	●	●		社内ネットワーク	サーバへの攻撃：権限を超えた操作、管理者権限での操作ミス、悪意ある操作	中	サーバの乗っ取りによる、Webサイト改ざん、バックドア設置等ログインした権限で可能なことすべてが可能。	高	・サーバ上のファイルについてルール上特定の領域にはアクを設定している。 ・管理者アカウントは申請時のしを行い、利用後はパスワードている。
	○○システム	○	○	○	○	●	●		社内ネットワーク	サーバへの攻撃：通信の盗聴	低	サーバへのログイン情報の搾取。	高	・シェルによるサーバへのアク通信による暗号化を行っている
	○○システム	●	○	○	○	○	○		インターネット経由	サーバへの攻撃：OSやミドルウェアの既知の脆弱性を突いた攻撃	高	サーバの乗っ取りによる、Webサイト改ざん、バックドア設置等サーバ内で可能なことすべてが可能。	高	・明文化されたルールがあり、沿って定期的にサーバのアップミドルウェアに対するパッチを適る。 ・サーバリリース時、設定変更
	○○システム								インターネット経由	Webアプリケーションへの攻撃：				

◆リスク高以上の対策

No.	詳細	分析結果	対策案	導入によるデメリット
1	【サーバへの攻撃】 OSやミドルウェアの脆弱性	端末は環境が異なるために、動作検証が難しく、セキュリティパッチやバージョンアップは一部を除いて実施できていない。セキュリティパッチが適用されないことで既知の脆弱性を攻撃するマルウェアに侵入されるなどのリスクが高くなる。	①HP社 「TippingPoint」 http://www8.hp.com/jp/ja/software-solutions/ngips-intrusion-prevention-system/ 仮想パッチとなるIPSを導入し、クライアントPCの対策は行わない方式。XP等のサポート終了したOSも対応可能。	・攻撃の遮断を行う設定の場合、誤検知停止のデメリットがありうる。 ・ゲートウェイ型で導入した場合、通信化する可能性がある。 ・ネットワーク障害が発生した場合、調てしまう。
			②体制の見直し【運用による対策】 ・情報システム管理規定に「随時パッチ適用が実施可能な運用体制」記載すること。 ・当該管理規定に準じてパッチ管理を実施すること。 ・サービスベンダーに対しても当該運用規定に準じて、導入当初からパッチ管理が運用できる体制を契約内容にもり込むこと。 ・既存のサーバについては、手作業で危険な脆弱性について個別にサーバの動作検証を行ってパッチやOSアップデートを適用していく。	・パッチ管理の体制が必要となり、維持必要となる。 ・パッチ管理が適用できないサービスベするので、サービスによっては適用できる。また、適用できるケースでもサービス割高になる可能性がある。
	【…】 …の暗号化	広域網を使用しているので、内部ネットワーク内を流れる通信データの暗号化は実施していない。標的型攻撃が成功した際や内部犯行の際に通信データが傍受されれば、生データが漏えいする。		
3	無線LANからの侵入	無線LANはTKIPである。TKIPはWPA2であっても脆弱性がある。通信データの漏えいや成りすましによる侵入の可能性がある。 WEPが推奨されているが、WEPは高いリスクが存在し、数秒でWEPキーが解析される。通信データの漏えいや成りすましによる侵入の可能性がある。	①WEPについては、セキュリティガイドラインを見直して、無線LANの推奨暗号方式をWEPからWPA2(AES)に変更する。【運用による対策】	・WPA2(AES)に対応していない機器をきなくなる。機材の買い直しなどのコスがある。
			③AirTight Networks 社 「SpectraGuard Enterprise」 http://www.marubeni-sys.com/sec/airtight/products/sge.html Wireless IPS(侵入検知／防止システム)であるAirTight Networks 社のSpectraGuard Enterpriseを導入し、無線LANに接続する機器を登録することで、登録外の機器を接続できない様にすることができる。 ①、②の実施後にさらにセキュリティレベルを高める目的で実施する。	・誤検知により、正規の機器が無線LANる可能性がある。 ・新規に無線LANへ接続する場合、管理登録する必要があり、利用者が自由にきなくなる。
	【アプリへの攻撃】	外部公開サーバに対して、WAF・IPS・IDSがない。個人情報がな…	①SST社 「Scutum」 https://www.scutum.jp/	・誤検知によりWebサーバへのアクセス能性がある。

サービスの流れ - 4.報告書の作成

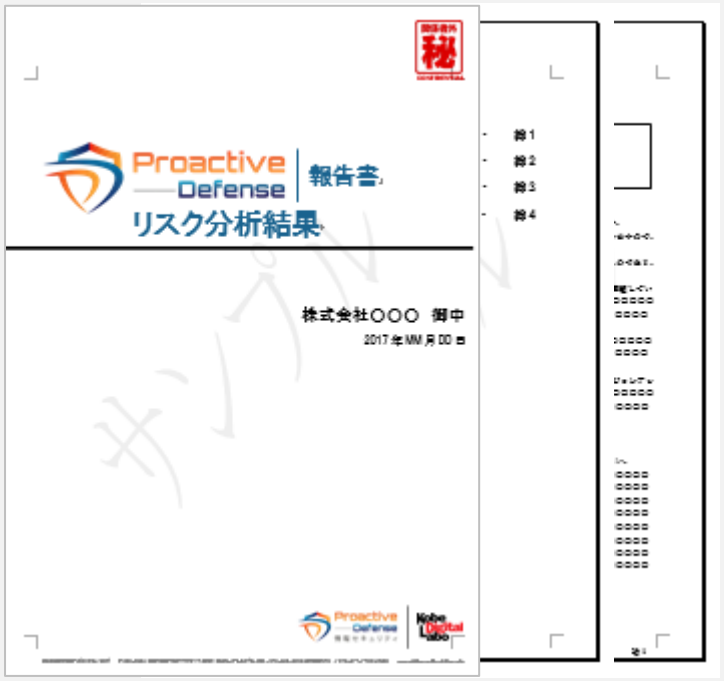
今までの作業内容をまとめ、対策一覧に記載の対策を実施せずに攻撃を受けて情報漏えいした際の被害想定金額を算出結果と事故事例を加えて報告書を作成します。これにより、対策一覧に記載の対策費用と被害想定金額を併記することによって、経営層に向けて、どちらを選択するか促すことができるようになります。

◆リスク高以上の対策

No.	詳細	分析結果	対策案	導入によるデメリット
1	【サーバへの攻撃】 OSやミドルウェアの脆弱性	端末は環境が異なるために、動作検証が難しく、セキュリティパッチやバージョンアップは一部を除いて実施できていない。セキュリティパッチが適用されないことで既知の脆弱性を攻撃するマルウェアに侵入されるなどのリスクが高くなる。	①HP社 「TippingPoint」 http://www8.hp.com/jp/ja/software-solutions/ngips-intrusion-prevention-system/ 仮想パッチとなるIPSを導入し、クライアントPCの対策は行わない方式。XP等のサポート終了したOSも対応可能。	・攻撃の遮断を行う設定の場合、誤検知停止のデメリットがありうる。 ・ゲートウェイ型で導入した場合、通信の化する可能性がある。 ・ネットワーク障害が発生した場合、調査してしまう。
			②体制の見直し【運用による対策】 ・情報システム管理規定に「随時パッチ適用が実施可能な運用体制」記載すること。 ・当該管理規定に準じてパッチ管理を実施すること。 ・サービスベンダーに対しても当該運用規定に準じて、導入当初からパッチ管理が運用できる体制を契約内容にもり込むこと。 ・既存のサーバについては、手作業で危険な脆弱性について個別にサーバの動作検証を行ってパッチやOSアップデートを適用していく。	・パッチ管理の体制が必要となり、維持必要となる。 ・パッチ管理が適用できないサービスベするので、サービスによっては適用できる。また、適用できるケースでもサービス割高になる可能性がある。
2	【ネットワークへの攻撃】 通信の暗号化	広域網を使用しているので、内部ネットワーク内を流れる通信データの暗号化は実施していない。標的型攻撃が成功した際や内部犯行の際に通信データが傍受されれば、生データが漏えいする。		
3	無線LANからの侵入	無線LANはTKIPである。TKIPはWPA2であっても脆弱性がある。通信データの漏えいや成りすましによる侵入の可能性がある。 WEPが推奨されているが、WEPは高いリスクが存在し、数秒でWEPキーが解析される。通信データの漏えいや成りすましによる侵入の可能性がある。	①WEPについては、セキュリティガイドラインを見直して、無線LANの推奨暗号方式をWEPからWPA2(AES)に変更する。【運用による対策】	・WPA2(AES)に対応していない機器をきなくなる。機材の買い直しなどのコスがある。
			③AirTight Networks 社 「SpectraGuard Enterprise」 http://www.marubeni-sys.com/sec/airtight/products/sge.html Wireless IPS(侵入検知／防止システム)であるAirTight Networks 社のSpectraGuard Enterpriseを導入し、無線LANに接続する機器を登録することで、登録外の機器を接続できない様にすることができる。 ①、②の実施後にさらにセキュリティレベルを高める目的で実施する。	・誤検知により、正規の機器が無線LANる可能性がある。 ・新規に無線LANへ接続する場合、管理登録する必要があり、利用者が自由にきなくなる。
	【アプリへの攻撃】	外部公開サーバに対して、WAF・IPS・IDSがない。個人情報がなければ情報漏えいの危険性はないが、改ざんやサービス停止等の	①SST社 「Scutum」 https://www.scutum.jp/	・誤検知によりWebサーバへのアクセス能性がある。

サービスの流れ - 5.報告会の実施

最終的に報告書を基に報告会を実施し、経営層に向けたリスクの危険性や必要な予算を共有し、現場、経営層双方が理解した計画を立案できるための下地作りとなるよう報告します。また、報告書から派生して確認したい質問についてもこの報告会で解消します。



費用と期間

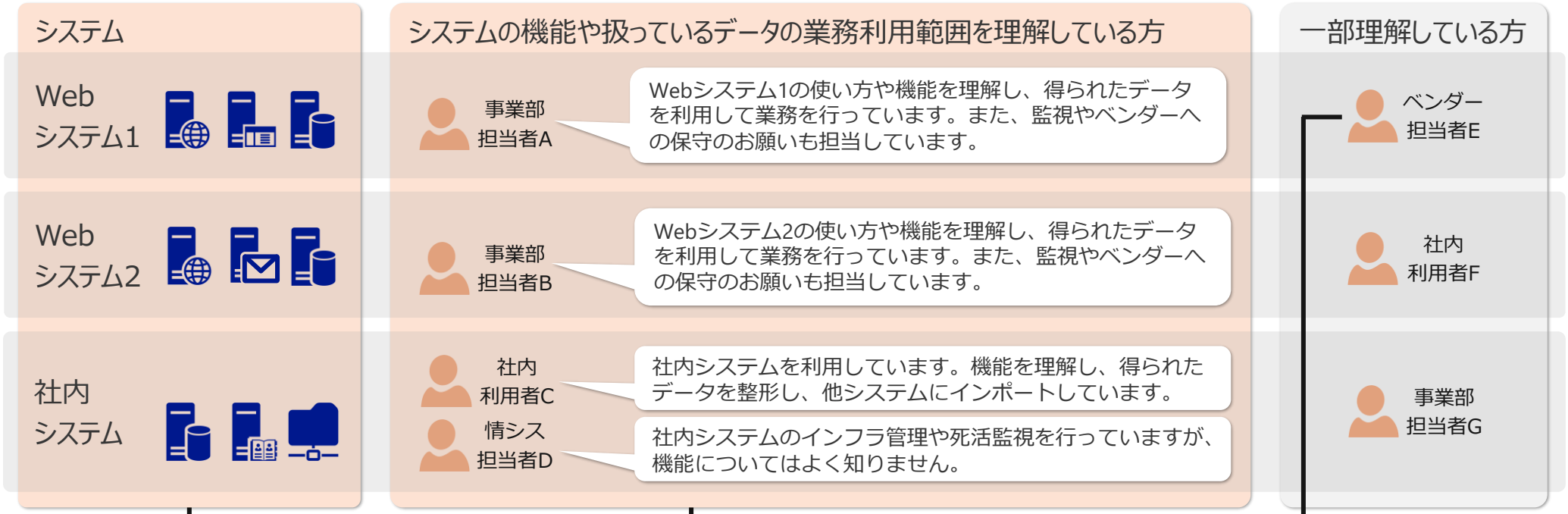
		Standard	Lite
目的		調査内容に対して、経営層向けに報告資料をまとめ、**予算化や分析結果報告の支援**を実施します。	流出した場合に被害が大きくなる情報資産に対して、**対応すべき対策とその手段を把握**できます。
成果物	アクセス経路図	○	○
	リスク一覧	○	○
	対策一覧(3つ)	○	○
	被害想定金額	○	-
	事故事例	○	-
	経営層に向けた報告書	○	-
報告会（※交通費別）		○	○
基本費用（**※5人までのヒアリングを含む**）		385万円	275万円
ヒアリング対象者追加費用		55万円	44万円
期間		1か月以上	2週間～1か月
オプション			
情報資産の把握		55万円	

通常はStandardをご利用いただいていますが、お客様のセキュリティ予算が確保されており、対策の一覧と優先度までわかれば今後の対策が可能であれば、Liteをご利用ください。ただし、Liteでは報告書は提出されませんのでその点予めご了承ください。

Proactive Defense

ヒアリング対象者のカウント方法

「システムの機能や扱っているデータの業務利用範囲を理解している方」をヒアリング対象者とします。そのため、1つのシステムについて、複数の担当者にヒアリングしないとシステムの内容を把握できない場合はそれぞれカウントします。カウントした内容を見積もりシートにまとめてお見積り致します。
この際、ヒアリング対象者数5人が基本費用に含まれます。また、6人目からは追加費用にて対応致します。



見積もりシート

No	システム名称	システム概要	ヒアリング対象者	管理・運用ベンダーの有無	機密情報の有無（※可能な範囲でお願いします）				
					社外個人情報の有無	特許情報・技術情報の有無	組織内の個人情報の有無	その他の機密情報の有無	大まかな件数
例1	Webシステム1	弊社の社外向けホームページ	事業部担当者A	○	○	×	×	×	
例2	Webシステム2	弊社のリクルート用サイト				×	×	×	
例3	社内システム	全社グループウェア、人事給与システム				×	○	○	
例4	同上	同上	情シス担当者D						

Proactive Defense

CONFIDENTIAL

お見積りに必要となる情報

前ページに記載しました通り、お見積りにあたり以下の情報資産に関する情報が必要となるためご準備ください。もし、情報資産の把握ができない場合は、「プランと価格」に記載のオプションプラン「情報資産の把握」をご利用ください。下記情報を含む情報資産の把握から実施致します。

情報資産に関する項目	説明
システム名称	情報資産を扱うシステムの名称を記入ください。
システム概要	システムの目的、システムを利用して行う業務を記入ください。
ヒアリング対象者	システムの機能や扱っているデータの業務利用範囲を理解している方をヒアリング対象者として選出して記入ください。一つのシステムに対して、機能によって担当者が異なる場合や、アプリケーションとインフラで担当者が異なる場合は、それぞれ記入してください。
管理、運用部門（ベンダー）の有無 ※可能な限りで大丈夫です	お見積りに直接的に関連するわけではありませんが、社内、外部委託先ベンダーがあれば記入ください。本サービスの過程でベンダー側にも確認が必要な場合があるため、可能な範囲で結構ですので記入いただけると助かります。
機密情報の有無、件数 ※可能な限りで大丈夫です	お見積りに直接的に関連するわけではありませんが、機密情報の件数によって分析対象のシステムに優先度をつけることができるようになります。これにより、今回予算的に全体のリスク評価をすることが難しい場合にシステムを絞って本サービスを適用することができるようになります。

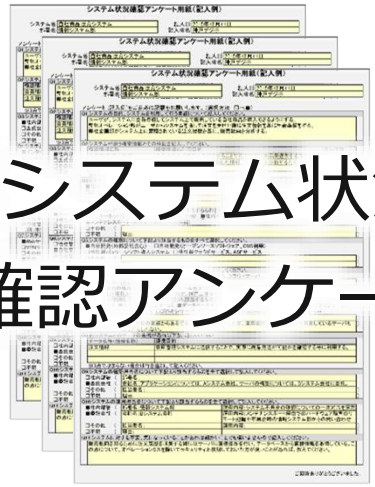
オプションについて

リスク対策プランニングを利用されるお客様の担当者様が、組織内で扱っているシステムの全貌がつかめない場合等、リスク評価をする対象を選定できず、見積もりシートの作成が困難な場合にご利用ください。

お客様に代わって、情報資産管理台帳の確認や、現場担当者やシステムを利用して業務担当者に直接ヒアリングを行い、想定されるシステムと保持する機密情報を明らかにします。

No	システム名称	システム概要	ヒアリング対象者	管理・運用ベンダーの有無	社外個人情報の有
例1	Webシステム1			○	○
例2	Webシステム2		事業部担当者	×	○
例3	社内システム	全社グループウェア、人事給与システム	社内利用者C	×	×
例4	同上	同上	情シス担当者D		

見積もりシート



システム状況
確認アンケート

（参考）サービス適用範囲毎のセキュリティリスク

No	範囲	リスク
1	リモートワーク	リモートワーク環境のセキュリティ対策が整備されていないことによって、そのネットワーク内に同居している他端末がウイルス感染した場合に二次被害の対象となるリスクがあります。また、監視の少ない環境下であるが故に、リモートワーク従事者によって機密情報がリモートワーク端末より持ち出されてしまうリスクがあります。
2	クラウド環境 /データセンタ	一般的にWebサービス等が運用されるため、サービスに対する、アプリケーション、プラットフォーム双方への攻撃の標的となるリスクがあります。Webサービスへの成りすましログインや、データベース、パスワード等の漏えい、Webページの改ざん、サービスの停止等が考えられます。
3	DMZ	外部向けに提供しているWebサイト等がクラウド環境/データセンタと同様のリスクを負います。また、DMZ内に不正侵入された場合に、内部ネットワークへの更なる侵入等二次被害のリスクがあります。
4	フロアネットワーク	標的型攻撃、水飲み場攻撃、ソーシャルエンジニアリング、マルウェア感染済みのデバイスの接続等の攻撃によって、端末がマルウェアに感染し、端末上に保存された機密情報が漏えいするリスクやランサムウェアによって暗号化されるリスクがあります。また、端末が乗っ取られた場合に内部ネットワークへの更なる侵入の踏み台にされる等のリスクがあります。
5	内部サーバ ネットワーク	内部犯行や、DMZや端末内に侵入したマルウェアからのアクセス等によって、機密情報が漏えいするリスクがあります。また、ランサムウェアによって機密情報が暗号化されるリスクがあります。
6	物理的に切り離された ネットワーク	基本的に、ネットワークを伝って攻撃されるリスクは低いですが、業務に関連するサポート会社の入室等があるため、不特定多数の者によるデータ運搬用媒体や作業用端末を伝って攻撃されるリスクが高まります。例えば、マルウェア感染済みのデータ運搬用媒体や作業用端末によって二次被害の対象となるリスクや、内部犯行等による情報漏えいのリスクが考えられます。
7	入退室者	組織内への入室者が保持するデバイスがマルウェア感染済みである場合、二次被害の対象となるリスクがあります。また、退室者によって、情報が持ち出された場合には、保存されたデバイスの紛失等により機密情報が漏えいするリスクがあります。
8	サポート会社	仮にサポート会社の端末がマルウェア感染した場合に、物理的に切り離されたネットワーク等も含め、メンテナンス用にひかれた回線によって侵入され、二次被害の対象となるリスクがあります。また、サポート会社の内部犯行等による情報漏えいのリスクが考えられます。

Kobe Digital Labo ITで未来を創る

- 記載されている会社名および製品名は、各社の商標または登録商標です。
- 当資料は予告なく変更する場合があります。

株式会社 神戸デジタル・ラボ

本社
〒650-0034 神戸市中央区京町72番 新クレセントビル
TEL： 078-955-9682（セキュリティ事業部）/ 078-327-2280（代表）
FAX： 078-327-2278

ホームページ
弊社サイト：https://www.kdl.co.jp/
Proactive Defense 専用サイト：http://www.proactivedefense.jp/

SNS
Facebook：ProactiveDefense
Twitter：KDL_Security

Proactive Defense