

Hinemos機能紹介 セキュリティ

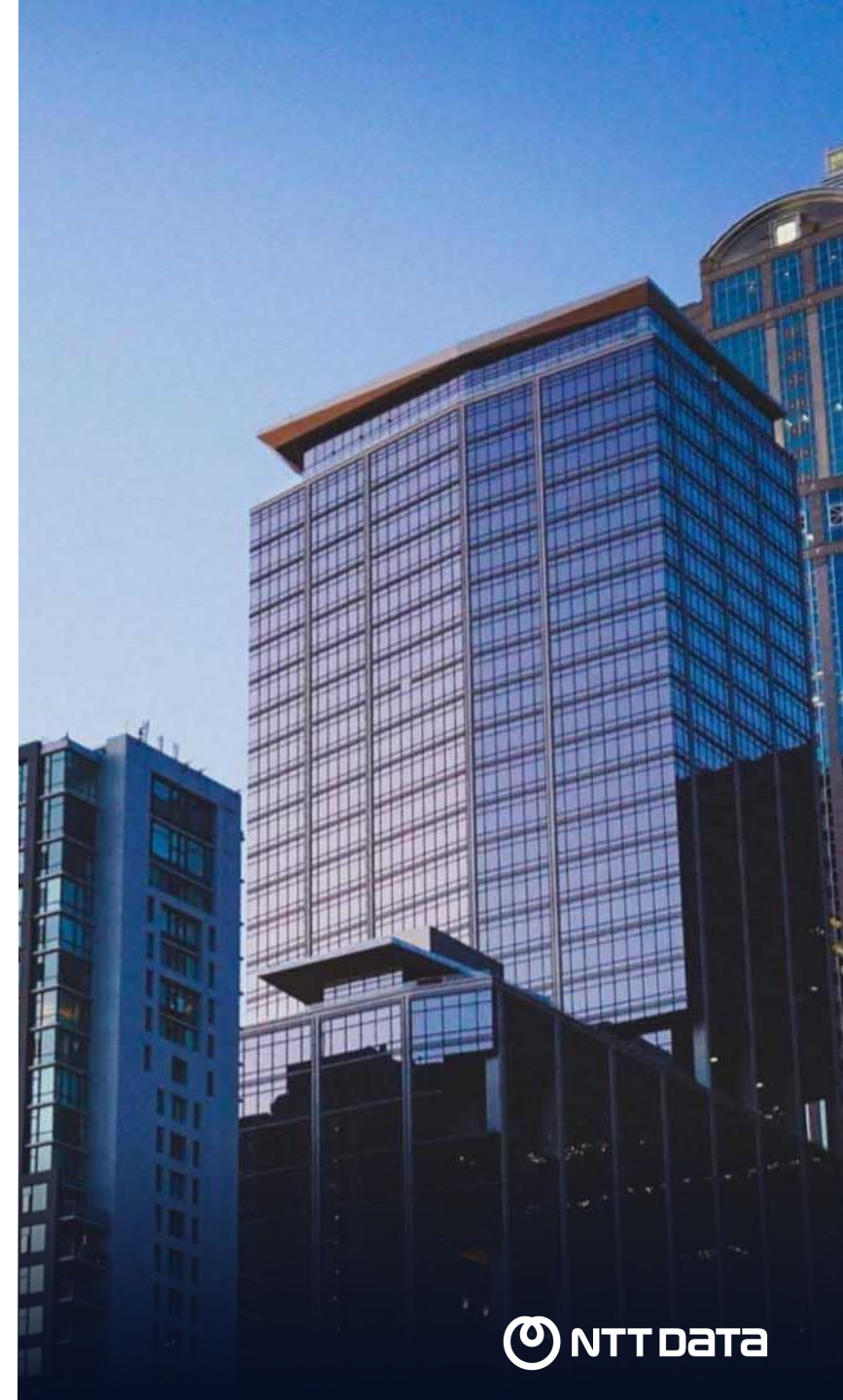
株式会社NTTデータ先端技術

© 2025 NTT DATA INTELLILINK Corporation



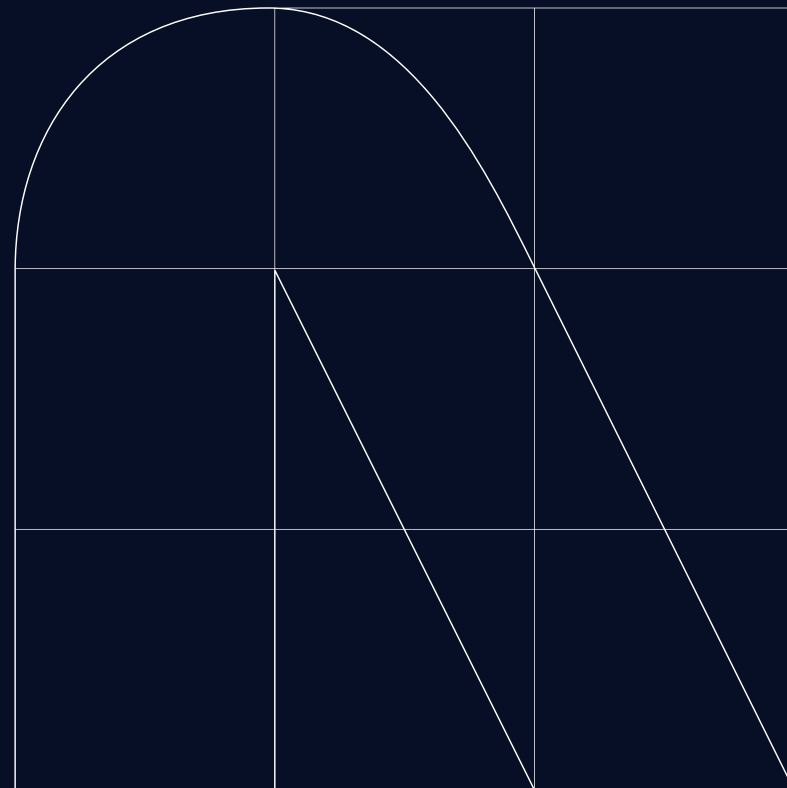
INDEX

1. 脆弱性とサイバー攻撃
2. Hinemos セキュリティオプション ネットワーク診断オプションのご紹介
3. Hinemos セキュリティオプション アプリケーション診断オプションのご紹介
4. ご相談・お問合せ



01

脆弱性とサイバー攻撃



脆弱性によるサイバーセキュリティの脅威

脆弱性による脅威は、IPAの10大脅威で、3年連続トップ10にランキング

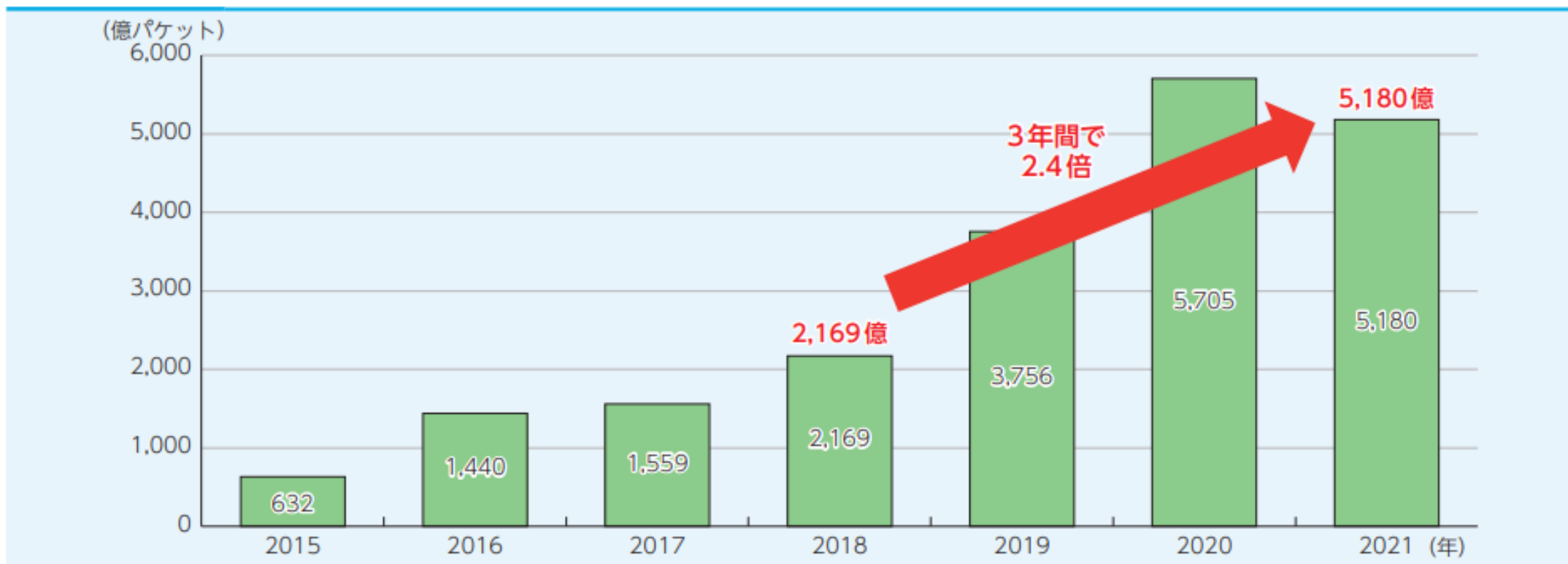
順位	10大脅威2023/組織	10大脅威2022/組織	10大脅威2021/組織
1位	ランサムウェアによる被害	ランサムウェアによる被害	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃	標的型攻撃による 機密情報の窃取	標的型攻撃による 機密情報の窃取
3位	標的型攻撃による 機密情報の窃取	サプライチェーンの弱点を悪用した攻撃	テレワーク等のニューノーマルな働き方を狙った攻撃
4位	内部不正による情報漏えい	テレワーク等のニューノーマルな働き方を狙った攻撃	サプライチェーンの弱点を悪用した攻撃
5位	テレワーク等のニューノーマルな働き方を狙った攻撃	内部不正による情報漏えい	ビジネスメール詐欺による 金銭被害
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	脆弱性対策情報の公開に伴う悪用増加	内部不正による情報漏えい
7位	ビジネスメール詐欺による 金銭被害	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	予期せぬIT基盤の障害に伴う業務停止
8位	脆弱性対策情報の公開に伴う悪用増加	ビジネスメール詐欺による 金銭被害	インターネット上のサービスへの不正ログイン
9位	不注意による情報漏えい等の被害	予期せぬIT基盤の障害に伴う業務停止	不注意による情報漏えい等の被害
10位	犯罪のビジネス化（アンダーグラウンドサービス）	不注意による情報漏えい等の被害	脆弱性対策情報の公開に伴う悪用増加

出典：行政独立法人情報処理推進機構(IPA)「情報セキュリティ10大脅威」を元に作成

サイバーセキュリティ上の脅威が増大

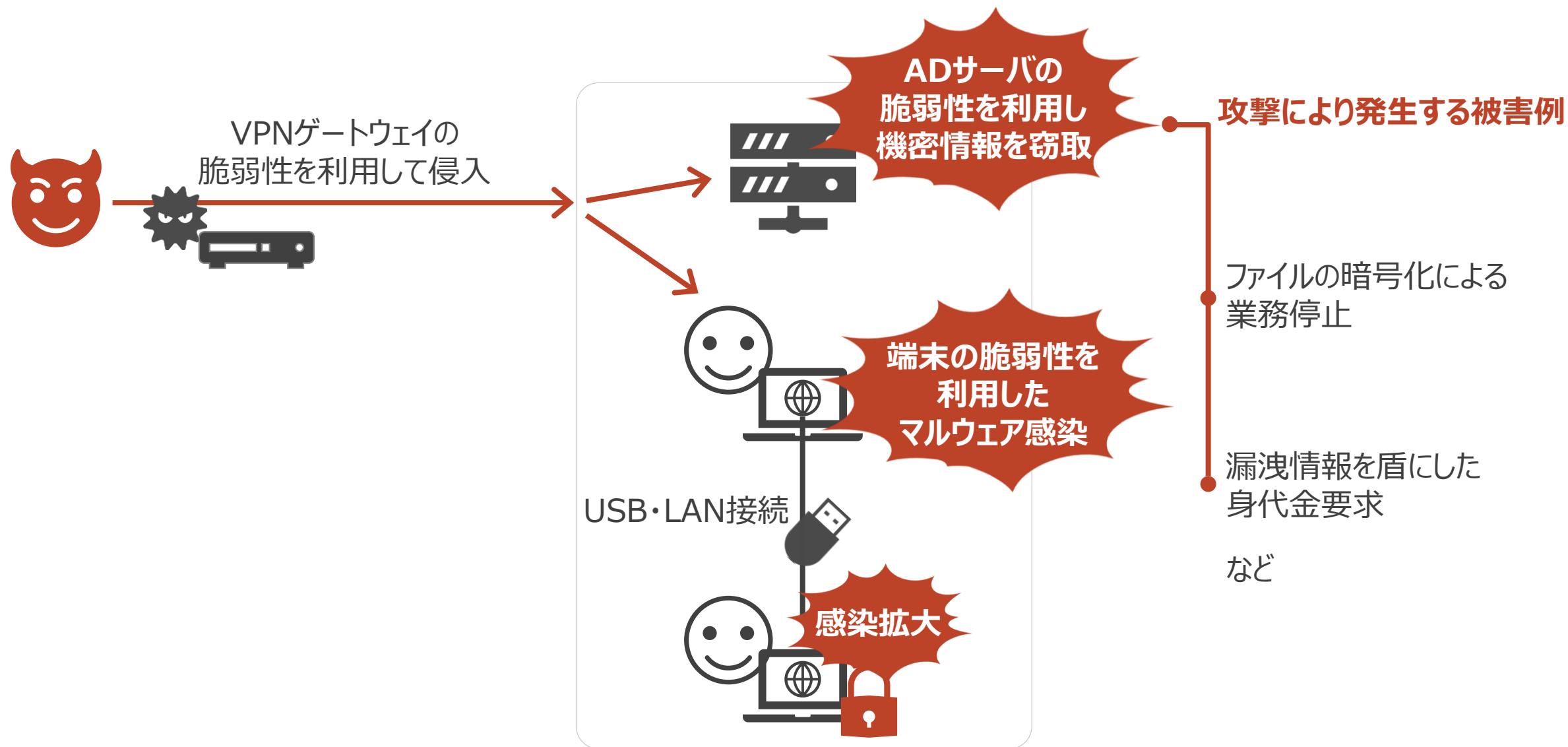
攻撃関連通信が3年間で2.4倍に増加。システムの脆弱性を利用し攻撃に成功する可能性が高まっている。

NICTERにおけるサイバー攻撃関連の通信数の推移



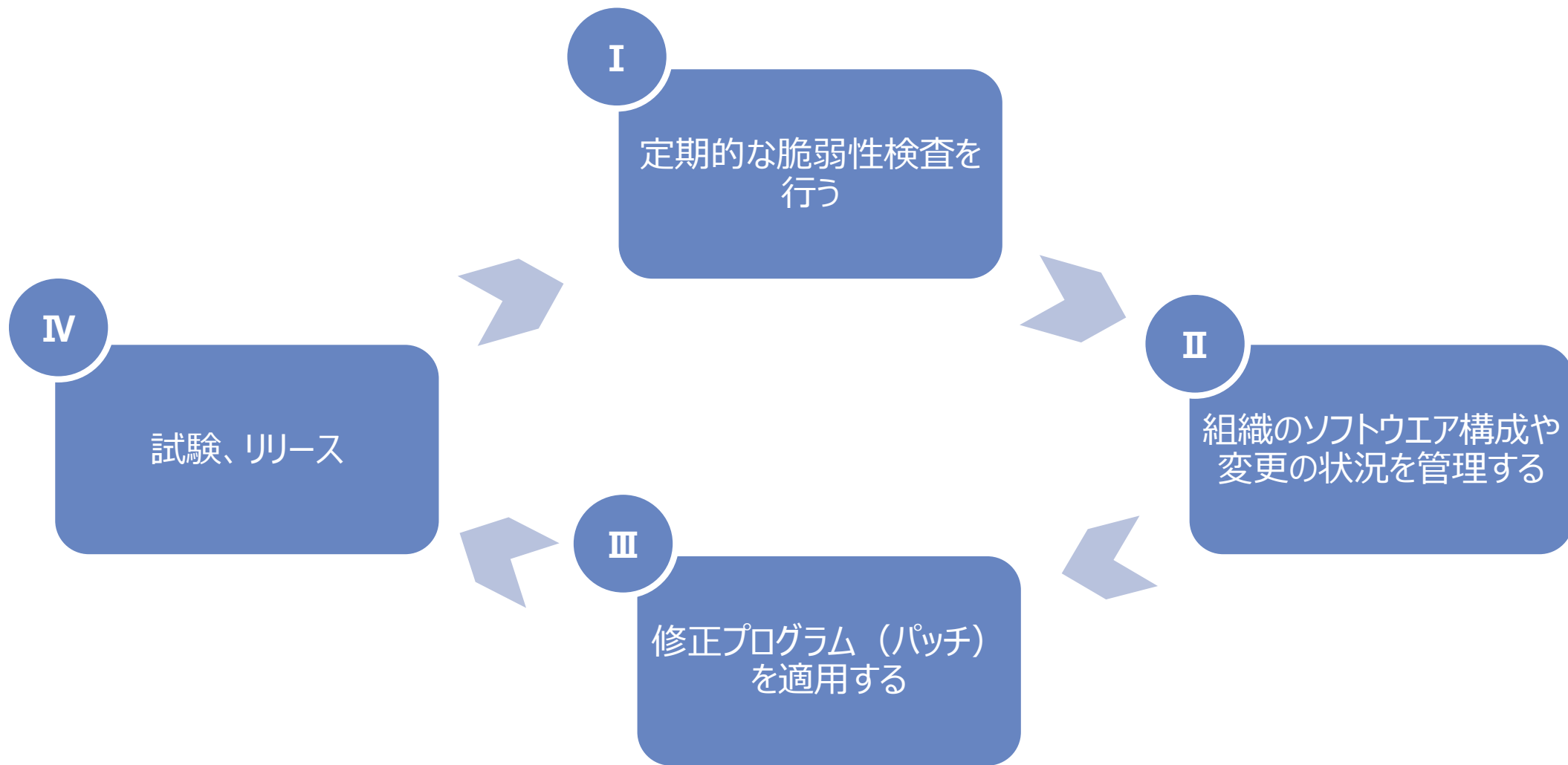
出典：総務省 令和4年版 情報通信白書（NICT「NICTER観測レポート2021」を基に作成）

脆弱性を悪用した攻撃例



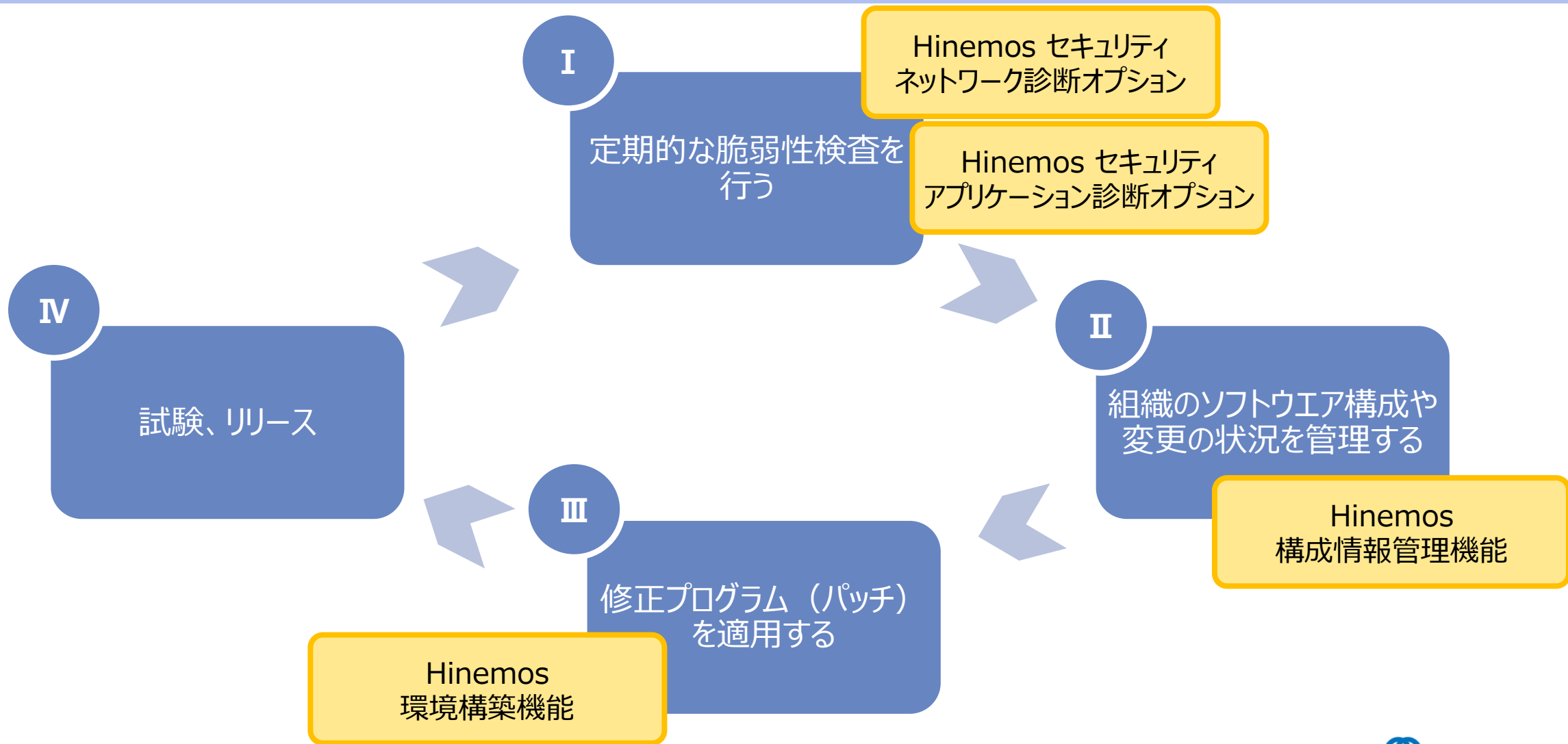
脆弱性とその対策について

運用段階における「脆弱性対策」は主に以下のようなものが求められています。



脆弱性とその対策について

Hinemosでは以下の機能で運用段階の脆弱性を対策します。

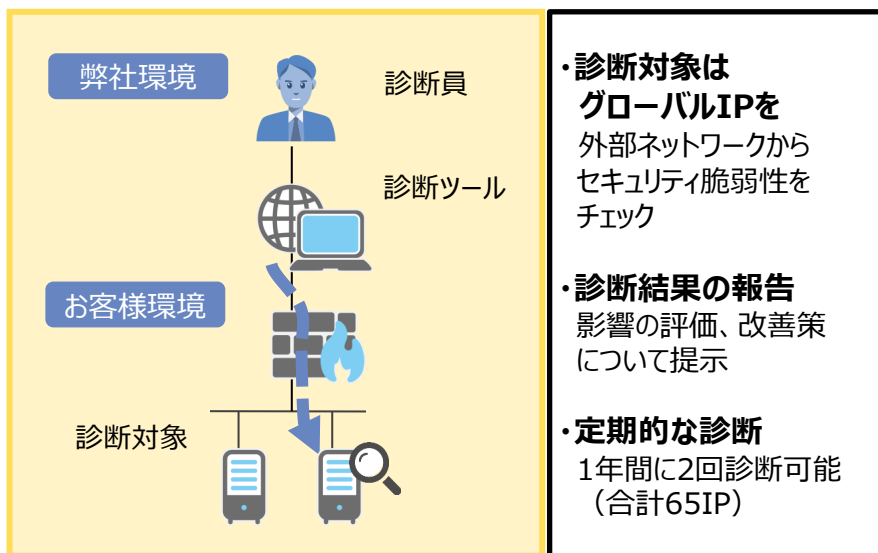


Hinemos セキュリティオプション

セキュリティ運用に必要なセキュリティ情報の配信サービスとネットワーク/アプリケーション診断を提供します。

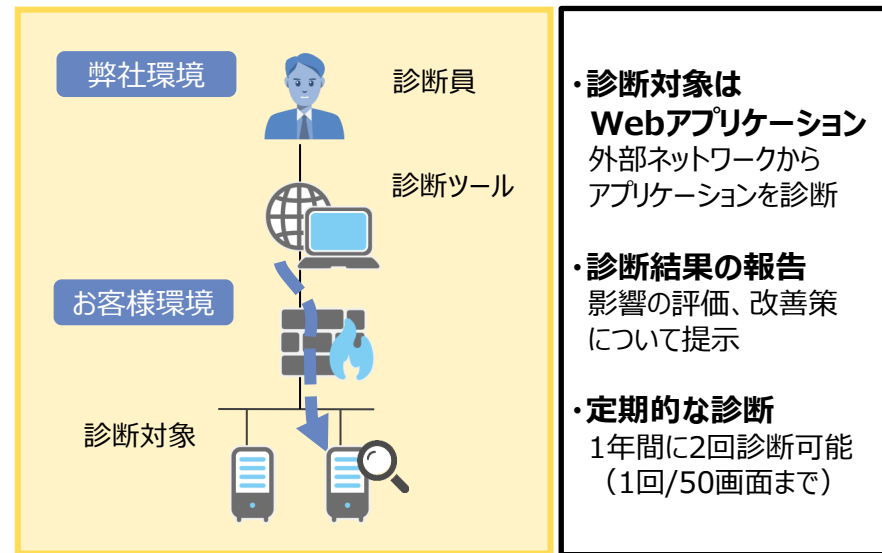
Hinemosセキュリティ ネットワーク診断オプション

ネットワークシステムを検査し、
セキュリティの問題点を洗い出します



Hinemosセキュリティ アプリケーション診断オプション

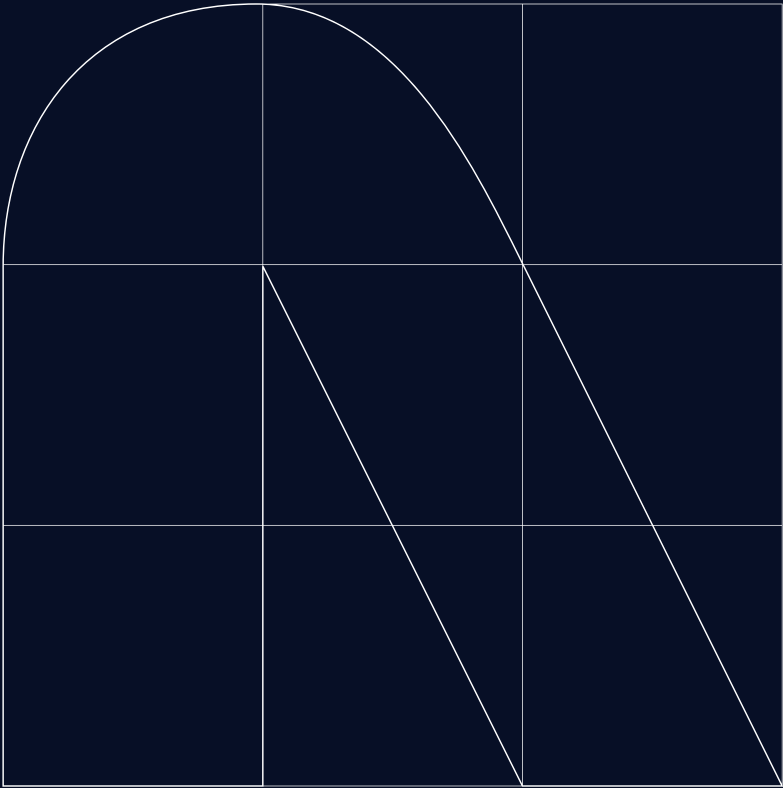
Webアプリケーションを検査し、
セキュリティの問題点を洗い出します



セキュリティプロセスとIT運用管理を統合したセキュリティ運用を実現

02

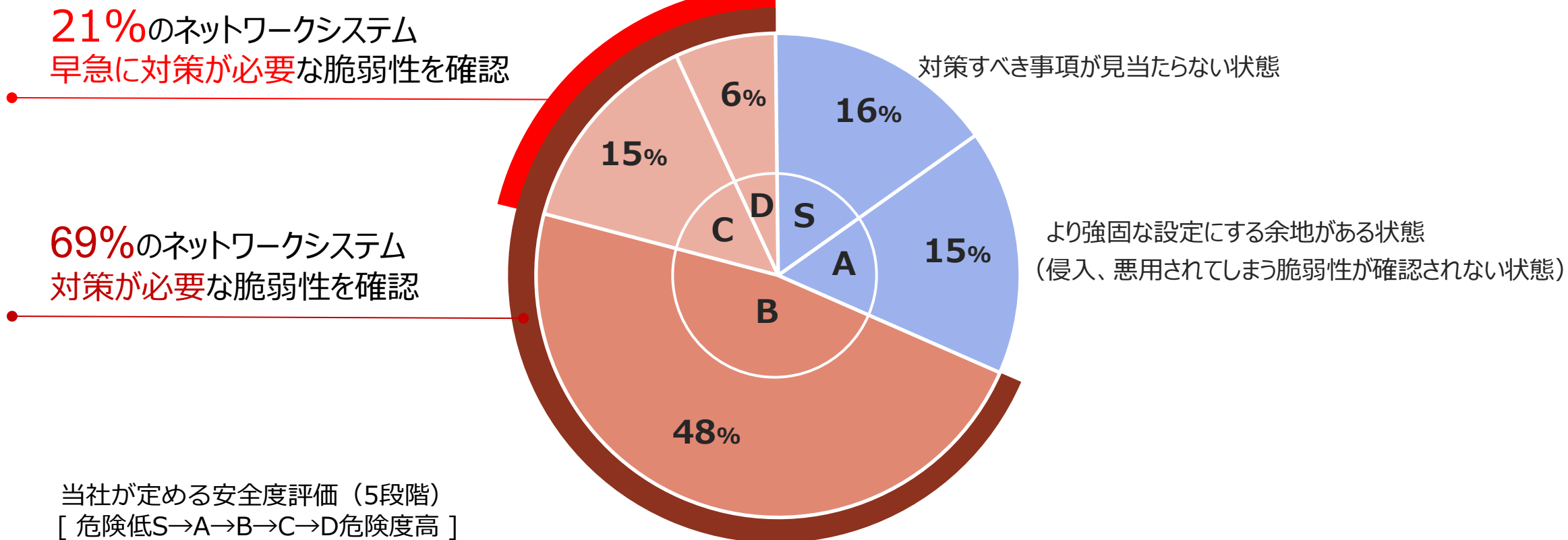
Hinemos セキュリティ ネットワーク診断オプションのご紹介



サーバやネットワークの問題点を「見える化」

NTTデータ先端技術によるネットワーク診断の対象となったネットワークシステムの内、
69%のネットワークシステムに対策を必要とする脆弱性が確認されています。

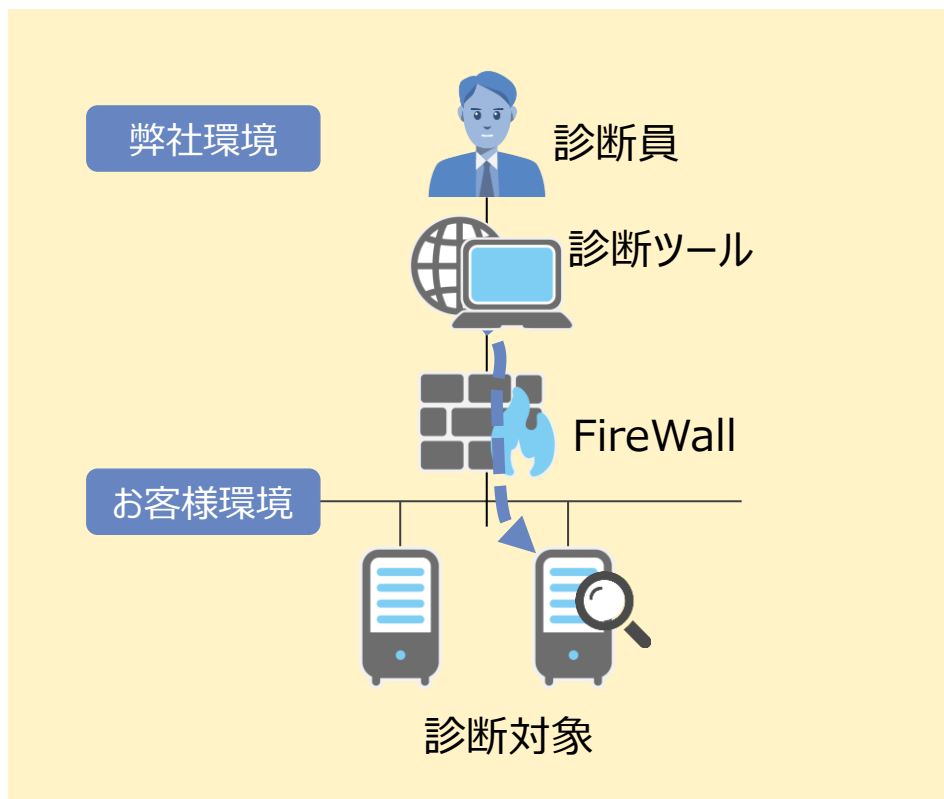
診断対象となったネットワークシステムの評価



サイバー攻撃による被害を未然に防ぐためには、
問題点（セキュリティ上の脆弱性）の早期発見と対策が重要です！！

サービス内容

ネットワークシステム（ネットワーク機器、サーバー）を検査し、セキュリティの問題点がないかを明確にします。
セキュリティ事故が起きないようにシステム改善を支援します。



診断内容

有償の脆弱性検査ツールを用いて、外部ネットワークからグローバルIPを診断対象とし、セキュリティ脆弱性を洗い出します。

診断結果報告

確認された脆弱性については、システムに及ぼす影響の評価、改善策について提示します。

診断回数

Hinemos セキュリティ ネットワーク診断オプションは、ご契約期間中、1年間に2回、65IPまで実施いただけます。

診断結果レポートでは、危険度ごとに色分けされたわかりやすい表示に加え、検出された脆弱性の詳細説明が確認できます。



わかりやすい危険度表示

192.243 Summary					
Critical	High	Medium	Low	Info	Total
8	2	4	3	25	42
Details					
Severity	Plugin Id	Name			
Critical	153584	Apache < 2.4.49 の複数の脆弱性			
Critical	34460	サポートされていない Web サーバーの検出			
Critical	11793	Apache < 1.3.28 の複数の脆弱性 (DoS, ID)			
Critical	153583	Apache < 2.4.49 の複数の脆弱性			
Critical	11915	Apache < 1.3.29 の複数のモジュールローカルオーバーフロー			
Critical	161948	Apache 2.4.x < 2.4.54 の複数の脆弱性			
Critical	158900	Apache 2.4.x < 2.4.53 の複数の脆弱性			
Critical	15555	Apache mod_proxy のコンテンツ長のオーバーフロー			
High	31654	Apache < 1.3.37 の mod_rewrite LDAP プロトコルの URL 処理オーバーフロー			
High	11137	Apache < 1.3.27 の複数の脆弱性 (DoS, XSS)			
Medium	90317	SSH の弱いアルゴリズムのサポート			
Medium	31408	Apache < 1.3.41 の複数の脆弱性 (DoS, XSS)			
Medium	11213	HTTP TRACE / TRACK メソッドが可能			
Medium	17696	Apache HTTP Server の 403 エラーページの UTF-7 でエンコードされた XSS			
Low	153953	SSH の弱い鍵交換アルゴリズムが有効			
Low	70658	SSH サーバーの CBC モード暗号が有効			
Low	71049	SSH の弱い MAC アルゴリズムが有効			
Info	66334	Patch Report			
Info	110723	資格情報が提供されていません			
Info	22964	サービスの検出			
Info	45590	共通プラットフォーム列挙 (CPE)			
Info	11936	OS の識別			
Info	149334	SSH パスワード認証の受け入れ			
Info	117886	OS Security Patch Assessment 利用不可			
Info	10881	SSH Protocol Versions Supported			

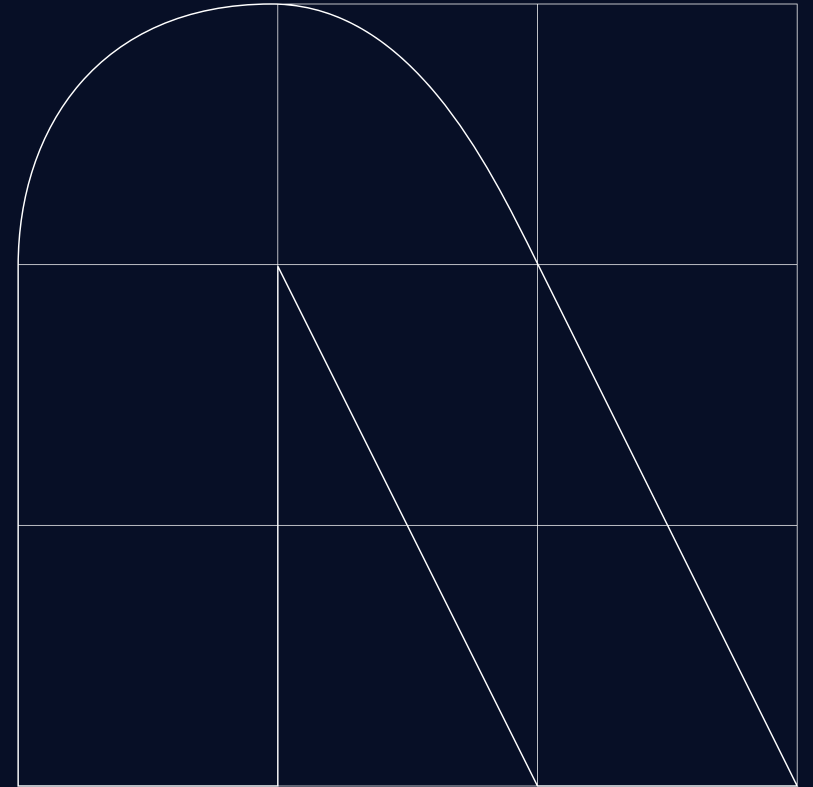


脆弱性の詳細説明や一般的な解決策

17696 - Apache HTTP Server の 403 エラーページの UTF-7 でエンコードされた XSS	
Synopsis	
リモートホストで実行されている Web サーバーにクロスサイトスクリプティング脆弱性があります。	
Description	
バナーによると、リモートホストで実行されているバージョンの Apache HTTP Server が、クロスサイトスクリプティング (XSS) 攻撃に使用されることがあります。特別に作り上げられたリクエストを作成することで、UTF-7 でエンコードされたスクリプトコードを 403 応答ページに注入し、XSS 攻撃を引き起こすことができます。これは、実際には RFC 2616 に適合しないことによって発生する Web ブラウザの脆弱性です (CVE-2008-2168 を参照)。Apache HTTP Server は脆弱ではありませんが、デフォルト構成では、脆弱なブラウザで、適合しない悪用可能な動作がトリガされることがあります。	
See Also	
https://seclists.org/bugtraq/2008/May/109	
https://seclists.org/bugtraq/2008/May/166	
Solution	
Apache HTTP Server 2.2.8 / 2.0.63 / 1.3.41 または以降にアップグレードしてください。これらのバージョンでは、脆弱な Web ブラウザでの悪用を防止するデフォルト構成設定が使用されます。	
Risk Factor	
Medium	
Vulnerability Priority Rating (VPR)	
3.3	
CVSS v3.0 Base Score	
6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)	
CVSS v3.0 Temporal Score	
5.9 (E:P/RL:O/RC:C)	
CVSS Base Score	
4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)	
CVSS Temporal Score	
3.4 (E:POC/RL:OF/RC:C)	
References	
CVE	CVE-2008-2168

03

Hinemos セキュリティ アプリケーション診断オプションのご紹介

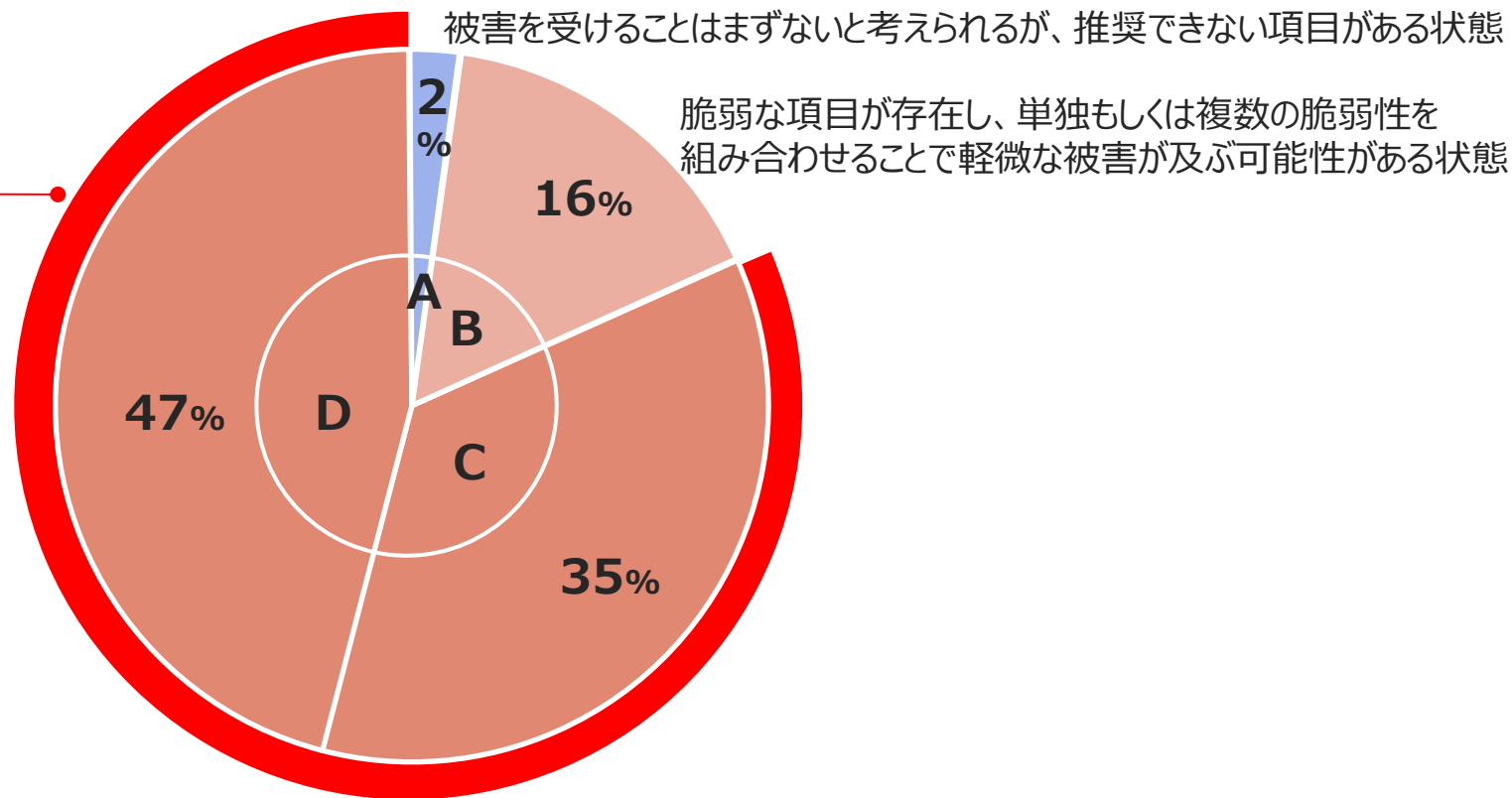


Webアプリケーションの問題点を「見える化」

NTTデータ先端技術によるWebアプリケーション診断の対象となったWebアプリケーションの内、
82%のWebアプリケーションに対策を必要とする脆弱性が確認されています。

診断対象となったWebアプリケーションの評価

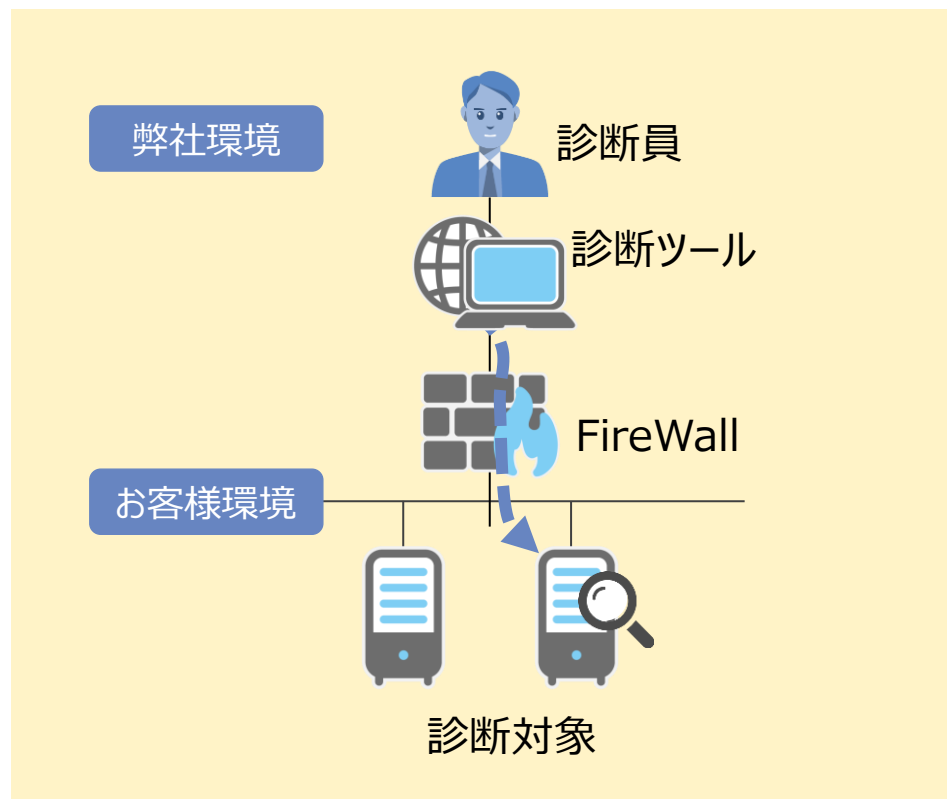
82%のWebアプリケーション
対策が必要な脆弱性を確認



サイバー攻撃による被害を未然に防ぐためには、
問題点（セキュリティ上の脆弱性）の早期発見と対策が重要です！！

サービス内容

Webアプリケーションを検査し、セキュリティの問題点がないかを明確にします。
セキュリティ事故が起きないようにシステム改善を支援します。



診断内容

有償の脆弱性検査ツールを用いて、外部ネットワークからFQDNを診断対象とし、セキュリティ脆弱性を洗い出します。

診断結果報告

確認された脆弱性については、システムに及ぼす影響の評価、改善策について提示します。

診断回数

Hinemos セキュリティ Webアプリケーション診断オプションは、ご契約期間中、1年間に2回、50画面/1回まで実施いただけます。

診断結果レポートとして、検出された脆弱性の発見箇所や詳細説明に加えて、画面遷移図もご提示します。



脆弱性の発見箇所や詳細説明

スクリーンショット

脆弱性が見つかった箇所

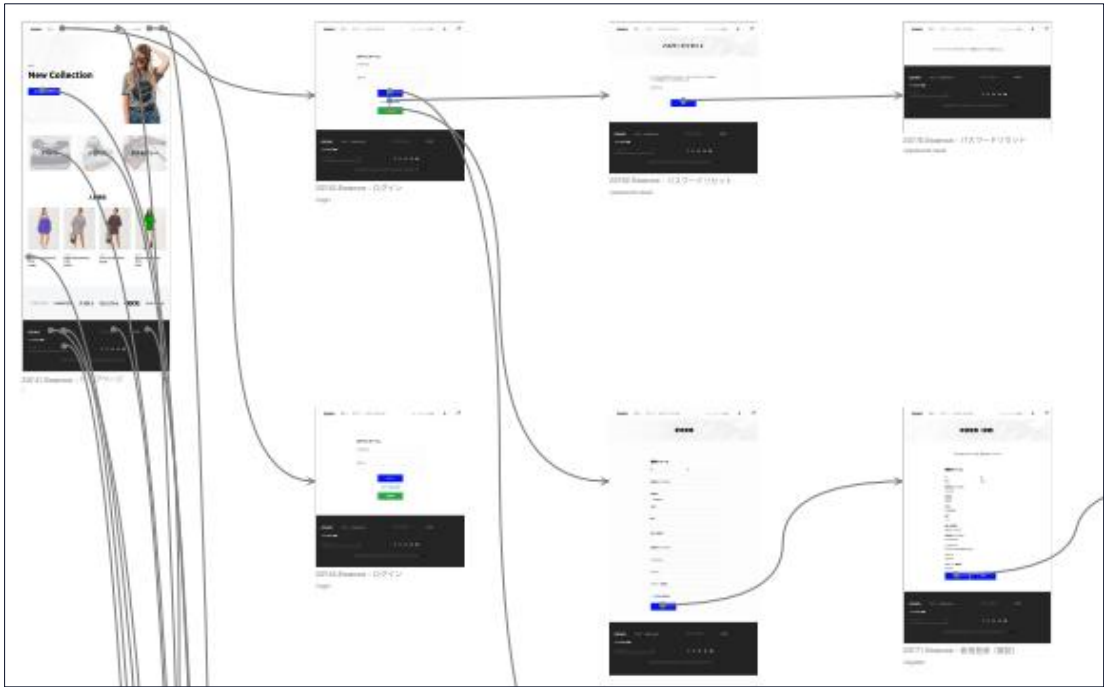
20771.Essence - 新規登録（確認）(POST <http://example.com:3333/register>)

パラメータ情報

タイプ	パラメータ名	正常値	操作値	検知理由
-----	--------	-----	-----	------



診断対象サイトの画面遷移図

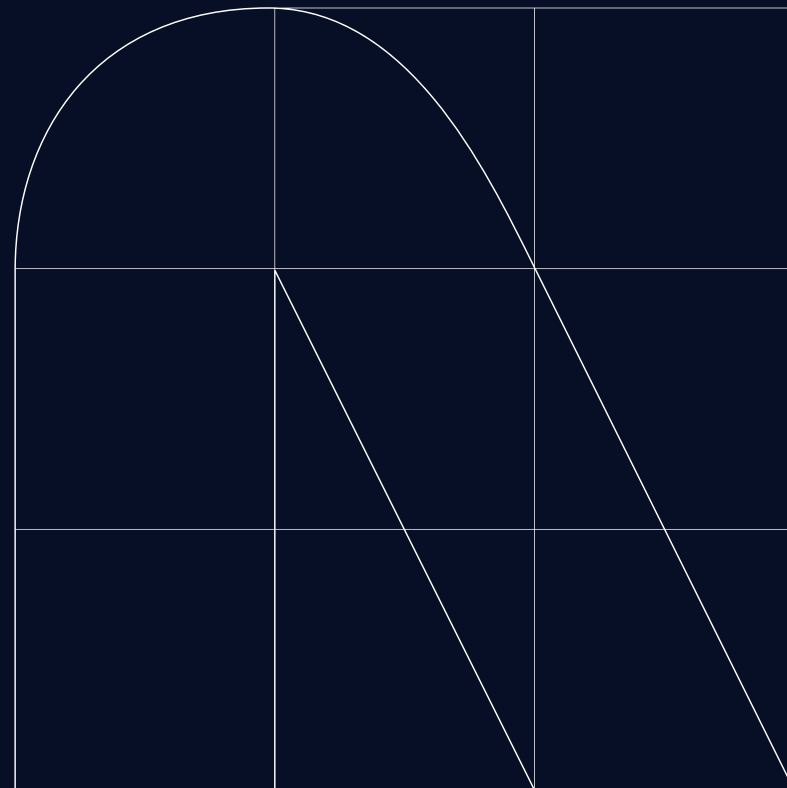


- システム管理も昨今様々なサービスと連携する中で脆弱性を狙ったサイバー攻撃に晒される脅威が増大してきています。
- Hinemosでは構成情報管理機能により、組織のソフトウェア構成や変更の状況を管理することが可能です。
- Hinemos セキュリティ ネットワーク診断オプションではネットワークシステムを検査し、セキュリティの問題点を確認、システム改善を支援します。
- Hinemos セキュリティ アプリケーション診断オプションではWebアプリケーションを検査し、セキュリティの問題点を確認、システム改善を支援します。

Hinemos セキュリティオプションを活用して
さらなる業務の改善を行いましょう！

04

ご相談・お問合せ



お問い合わせはこちら

まずは下記よりお問い合わせください。

Hinemosに関するお問合せ

お気軽にお問い合わせください。

Hinemosポータルサイト

URL : <https://www.hinemos.info/contact>

Hinemos



お待ちしているのに！

