



Incubate advanced technology

SSL認証書自動管理ソリューション NeoCertManager

2025年12月

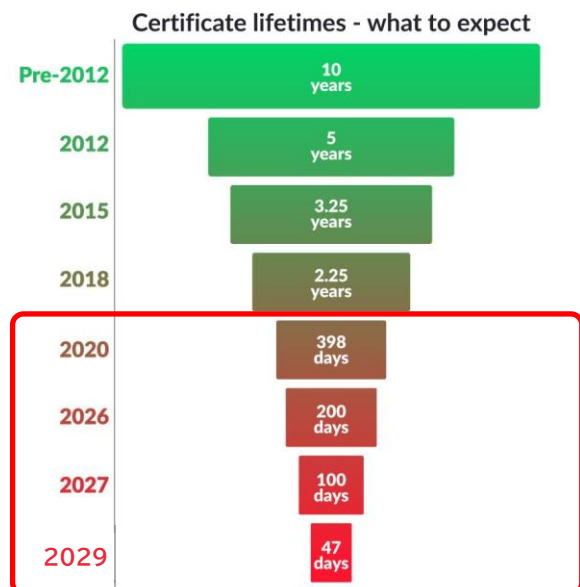
株式会社Cho&Company

目次

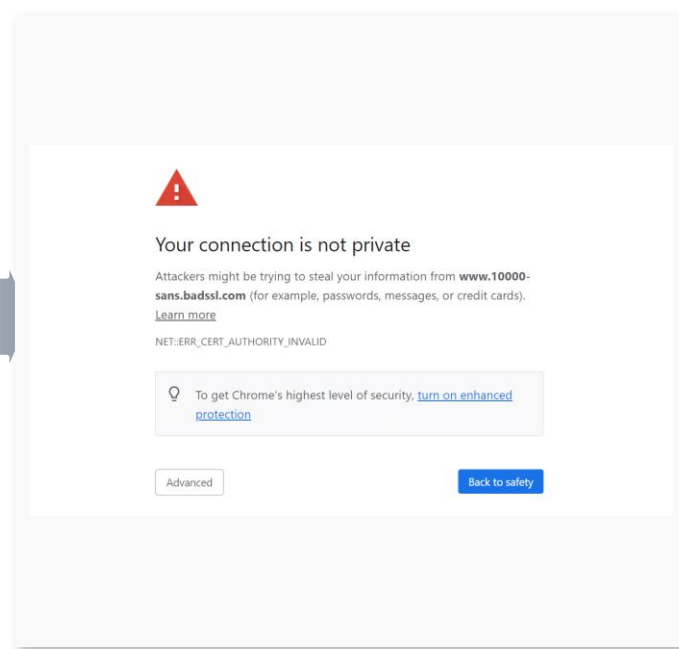
1. SSL証明書管理の現況
2. NeoCertManagerについて
3. NeoCertManagerの主な機能

SSL証明書管理の現況(SSL/TLS証明書の有効期間の短縮)

- Google、MSなどで構成されたCA/Bフォーラムのポリシー変更により証明書の有効期間が短縮
- 今年基準で最大398日の証明書有効期間は、**2029年には47日と短縮予定**
- 世界中のドメインは2億以上と推定されており、ほとんどが証明書を使用している
- 証明書管理業務が増加することで業務負荷によるヒューマンエラー発生、サービス障害時の企業イメージと信頼性の低下



有効期間の短縮



サービス障害の増加



信頼度低下

SSL証明書管理の現況(システム)

- SSL証明書の自動管理で企業のセキュリティ管理効率を向上させる重要なツール
- グローバルCA企業が独自に証明書管理システムを販売中だが、クラウド方式で国内セキュリティ環境に適用不可
- 国際鍵管理標準KMIPを準用する独自開発ソリューションベース(NKM、NeoKeyManager)

他社ソリューション



- 無料で利用可能
- オープンソースによるセキュリティの脆弱性
- 独自の開発力がないと設置、運用不可



- CA機関で直接扱ってセキュリティ性に優れ
- クラウドベースで金融、公共、通信など適用不可
- マニュアル提供のみ、技術支援不可
- 高コストライセンス



当社ソリューション



TC Members

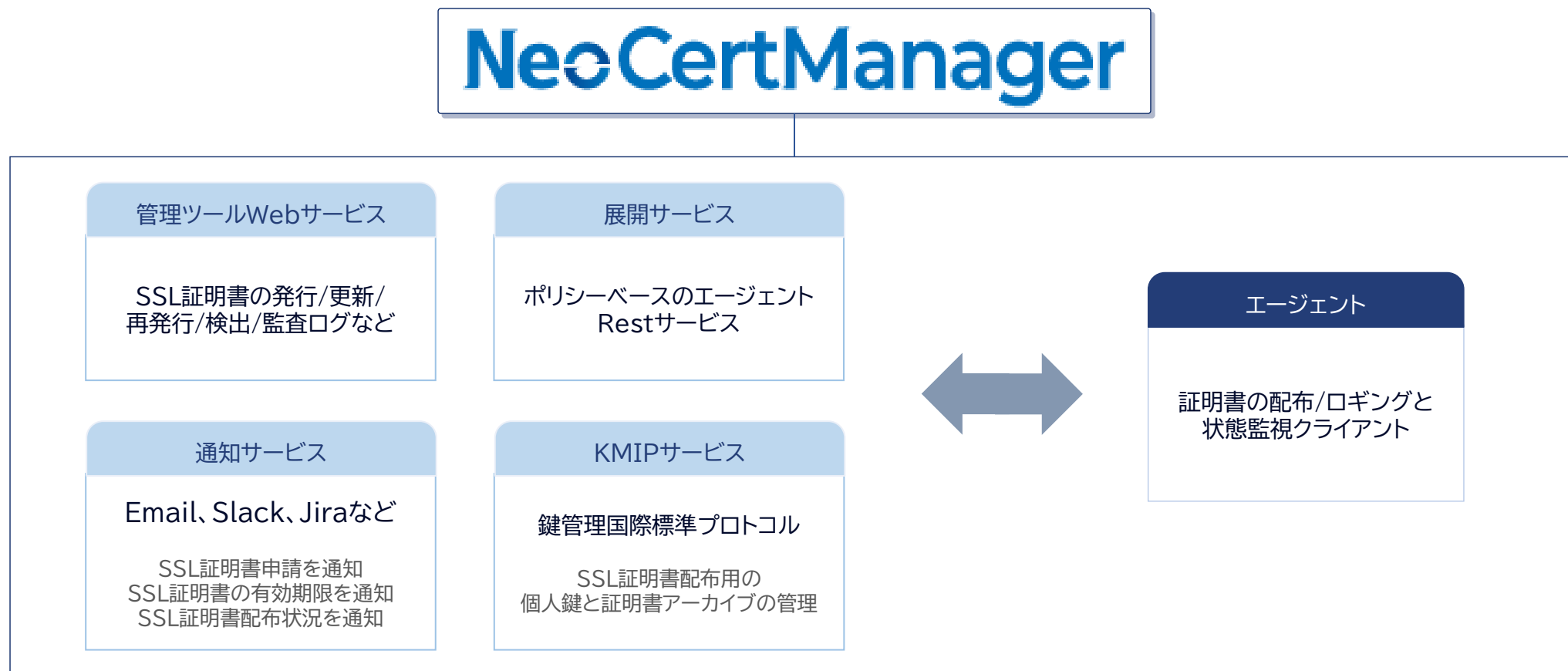


- 国際鍵管理標準KMIP 3.0準用
- 国内RA機関と連動してグローバルCA証明書をサポート
- 独自開発のKMSベースで安全な鍵管理
- 証明書(Selfsign)発行
- お客様の環境に合わせた構築
- カスタマイジングのサポート
- 障害発生時の迅速な対応



NeoCertManagerについて

- 国際鍵管理標準KMIPを準用する自社開発ソリューション(NKM、NeoKeyManager)
- 鍵管理ソリューションKMSの技術力と構築経験をもとに開発したソリューションでグローバルCA企業と競争
- 顧客のIT環境に合わせたカスタマイズ可能な構築型ソリューションで、金融、公共、通信、製造あらゆる対象に適用可能



NeoCertManagerについて

- NeoCertManagerは、お客様に合わせた構築が可能な独自開発ソリューション
- FIPS 140-2 Lv3認定HSM 搭載、最高のセキュリティを維持しながら利便性と活用性を最大化

NeoCertManager

活用性

Total Package

NKMソリューション+管理サーバー
統合構築

Discovery

内部証明書の現状を把握

利便性

対応

即時の技術支援、障害対応

クイック発行

認証 承認後、証明書の即時発行

セキュリティ

On-Premise

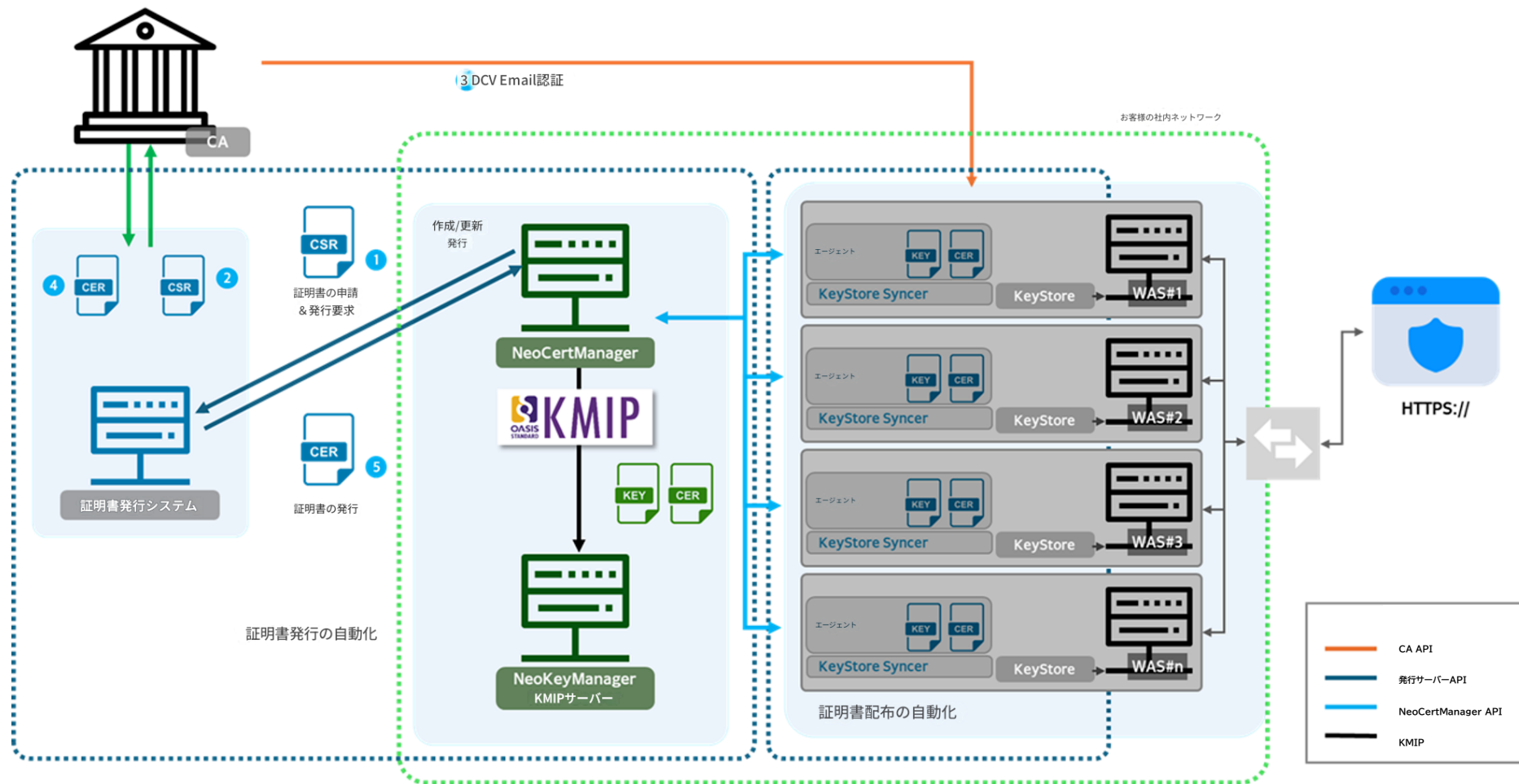
内部構築型ソリューションによる
安定性の確保とセキュリティ脅威の縮小

HSM Duplex機器

証明書と秘密鍵の暗号化、保存

NeoCertManagerについて

- NCMはお客様の内部環境にインストールされ、証明書の閲覧、更新、配布プロセスを自動的に管理
- グローバルCA機関の証明書を自動/手動で発行



NeoCertManagerについて

- 顧客のウェブシステムと連動するためのクライアントエージェント、SDK提供、当社技術人材が直接設置対応
- SSL証明書が必要な3rd party Webファイアウォール、Webサーバー製品との連動テスト



NeoCertManagerについて

- すべての証明書は**FIPS 140-2 Level 3** と **国際CC認証**を取得した**HSM**を通じて安全に分離保管

HSM認証の現状



【国際CC認証】

【FIPS 140-2 Level3認証】

HSMの安全性レベル

Level	説明
Level 1	<ul style="list-style-type: none">基本的なセキュリティ要件について評価された製品物理的なセキュリティは要求されず、主にソフトウェア暗号化モジュールの評価
Level 2	<ul style="list-style-type: none">暗号モジュールとハードウェア部門でセキュリティ適合性評価を実施物理的な機器の解体防止などに対する対策を講じなければならない
Level 3	<ul style="list-style-type: none">製品の分解を防ぐための断片的な方策と積極的な対策の提示可否を評価する不正アクセスなどの不当な方法の変更または誤用を検出した場合、デバイスは主要なセキュリティ変数を削除
Level 4	<ul style="list-style-type: none">物理的な保護が困難な環境を考慮して評価クラウドなどの新しい鍵管理サービスや製品に適用するためのレベル

【FIPS 140-2 Lv.3認証HSM搭載】

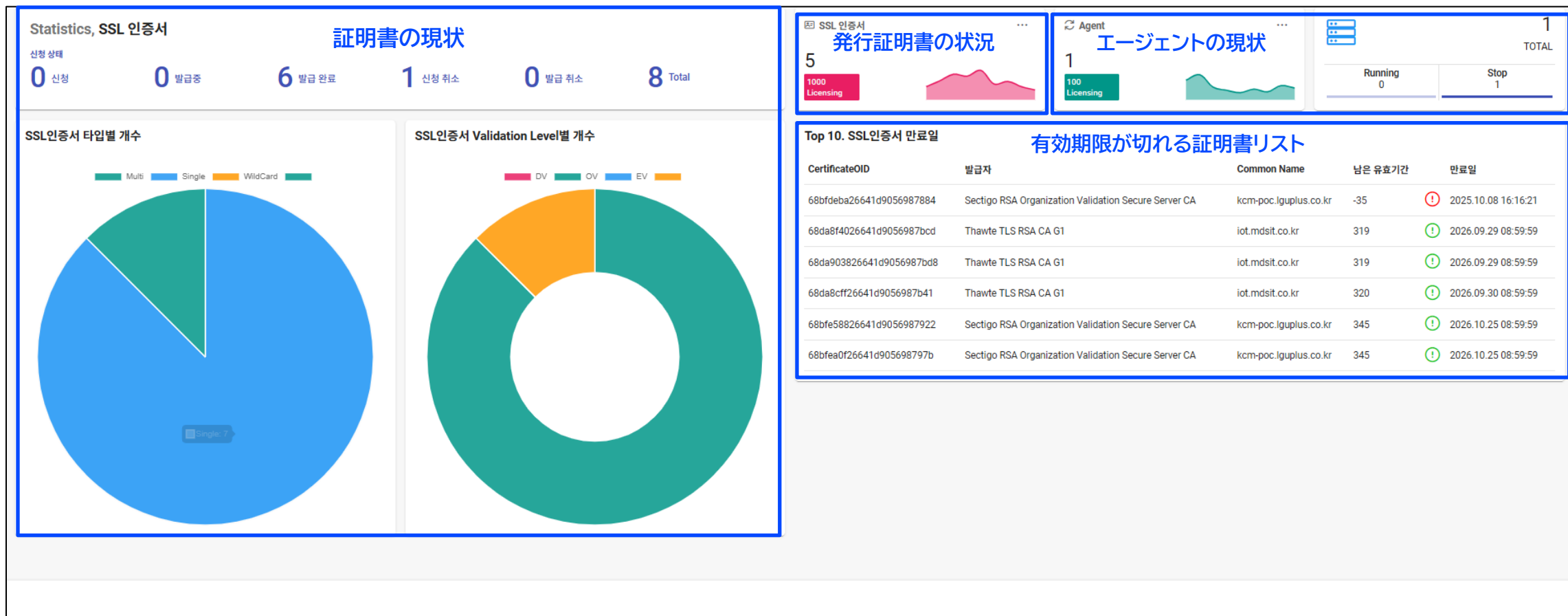
NeoCertManagerについて

- ・ NCMは、SSL証明書の閲覧、更新、展開、監視、通知などのライフサイクル全体を効果的に管理する機能を提供します。



NeoCertManager 主な機能

- NCMは、全社的な証明書統合管理のための直感的なダッシュボードを提供します
- 証明書の申請 現況、エージェントの動作可否、月別有効期限ドメイン確認



NeoCertManager 主な機能

- 主な機能-スキャン(Discovery)

ネットワークのインストールされた証明書を見つけて管理できるスキャン機能

- ✓WebサーバーおよびL / BにインストールされているSSL証明書をスキャン
- ✓すべてのベンダーの証明書を検、表示(CN値、発行CA、発行日、有効期限)
- プライベートCA/認定CAナビゲーション

The image displays three overlapping screenshots of the 'Discovery' (ディスカバリー) interface in NeoCertManager. The top-left screenshot shows the 'Host Name / IP Address' (ホスト名/IPアドレス) tab selected, with input fields for 'Host Name / IP Address' (ホスト名/IPアドレス*) and 'Port (Enter key input)' (Port (エンターキー入力)*), and a 'Connection Timeout (Second per resource)' (接続タイムアウト(Second per resource)*) field. The top-right screenshot shows the 'File Upload' (ファイルのアップロード) tab selected, with a '+ Choose' button and a 'Connection Timeout' field. The bottom-center screenshot shows the 'IP Address Range' (IPアドレス範囲) tab selected, with input fields for 'Range Start IP Address' (範囲 Start IP アドレス*) and 'Range End IP Address' (範囲 End IP アドレス*), and 'Connection Timeout' and 'Port' fields. All screenshots include a search bar at the top and a 'Connection Timeout' field on the right. The bottom-right corner of each screenshot features three buttons: a green search button, a yellow refresh button, and a red close button.

NeoCertManager 主な機能

- 主な機能-自動更新とデプロイ (Auto Renewal & Deployment)

期限切れ予定の証明書を自動更新、発行

✓最初の証明書:管理者から申請または登録が必要

✓更新証明書:有効期限確認後、NCMを介して自動更新

>有効期限前に更新できるスケジュール設定可能ex。10日前

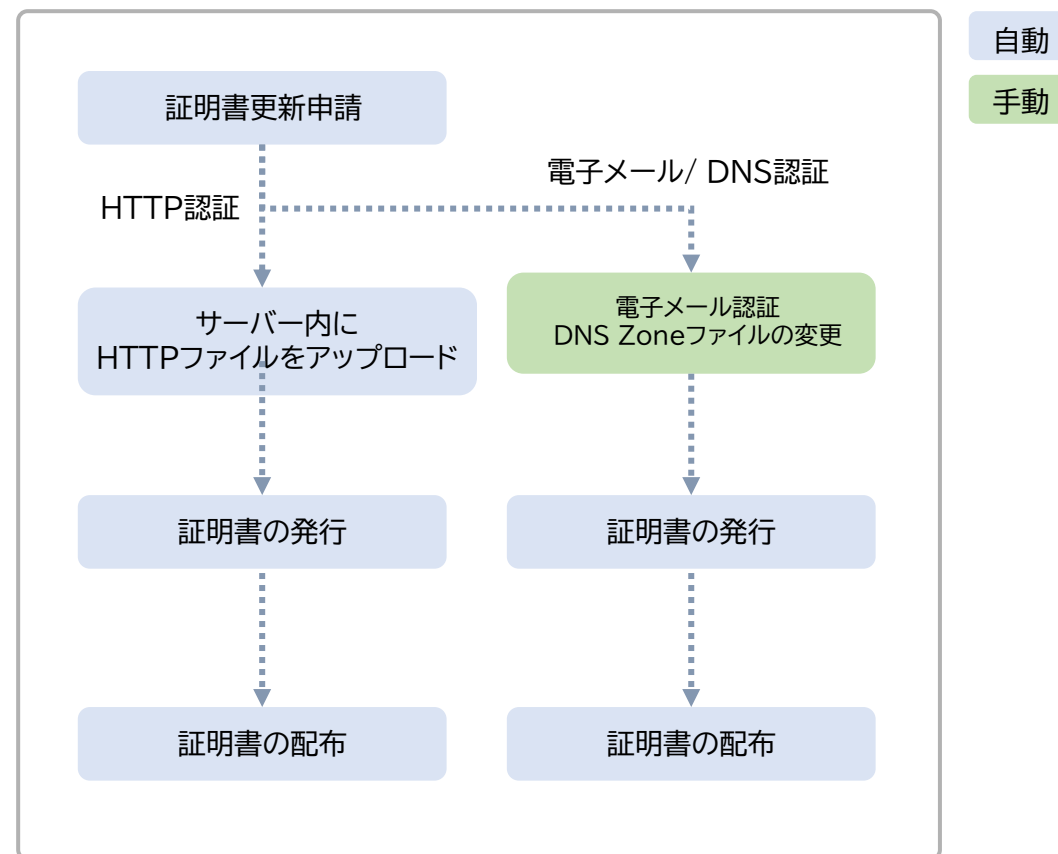
✓要請時に、中間管理者承認後に更新できる機能有

✓認証方式

1)Email:手動認証

2)DNS(CNAME / DNS TXT):手動認証

3)HTTP認証: 自動認証による証明書の発行



NeoCertManager 主な機能

• 主な機能-自動更新とデプロイ (Auto Renewal & Deployment)

✓ 証明書ステータスチェック後、発行された証明書を登録されているサーバー内に自動展開

✓ NCMで配布サーバーを登録、登録されたサーバーと証明書をマッチング

1) 配布先サーバの一時パスへ証明書をアップロード

2) 証明書の反映: 新しい証明書に変更

3) 証明書のロールバック: インストール中にエラー(接続エラーまたはfingerprint値の不一致)が発生した場合、古いSSL証明書として保持

엔드포인트 수정

2cf19459eb3b1a8f09289353fe6f4f2d37dd40df

IP주소 * 192.168.15.160 Port * 8444 DNS Name * 3e18a00f1dae.ngrok-free.app ☐ Check 디스커버리

배포 정책 설정

SSL 즉시 적용 ☒

Web Root * /var/www/html

Web Server * APACHE-SSL (selected), Apache-SSL, IBM HTTP Server, iPlanet, Oracle(OHS), SAP Web Application Server

Object 종류	Upload File	Install File
PrivateKey	ssl-cert-test.key	/etc/ssl/private/ssl-cert
Certificate	ssl-cert-test.pem	/etc/ssl/certs/ssl-cert-test.pem

Post Policy: sudo systemctl reload apache2

Object 종류: 선택, jks, AllJks

対応WebServer

- APACHE-SSL
- IBM HTTP Server
- Iplanet
- Oracle(OHS)
- SAP Web Application Server
- Tomcat
- Cisco 3000 시리즈 VPN 콘센트레이터
- Microsoft IIS 7.x & later
- WebtoB
- WebLog
- NginX
- AWS
- Jboss
- Haproxy
- MonitorappWAF

NeoCertManager 主な機能

- 主な機能-通知と記録 (Notification & Record)

- 1) 証明書の有効期限と配布状況通知

- ✓ Eメール、Slack、Rest対応
 - ✓ 通知ポリシー設定機能: 証明書の有効期限、証明書発行ステータス、自動更新、配布サーバーのステータス
 - ✓ SMTPによる送信メールの設定
 - ✓ 多数の通知受信者登録が可能(メール参照機能あり)

The image displays two screenshots of the NeoCertManager web interface, specifically the 'Notification Client Setup' (通知受信クライアントの作成) and 'Certificate Notification Settings' (証明書通知の設定) pages.

Left Screenshot: Notification Client Setup

- Navigation:** SMTP設定, 通知受信クライアント (selected), スケジュールポリシー/通知ポリシー
- Form Fields:**
 - OID: [Input Field]
 - 通知受信クライアント名: [Input Field]
 - 再試行制限数*: [Input Field]
 - 受信方法*: [Dropdown Menu with options: REST (selected), REST, EMAIL]
 - 詳細受信方法: ☐ N/A, ☒ SLACK, ☐ JIRA
 - 受信URL*: [Input Field]
 - 認証トークン: [Input Field]
 - 説明: [Input Field]
 - 通知の受信クライアント名の受信方法: ☐
 - test_email: [Input Field]
 - EMAIL: [Input Field]
 - タイプ: 参照Emailアドレス, 受信Emailアドレス
- Buttons:** 保存 (Save)

Right Screenshot: Certificate Notification Settings

- Navigation:** SMTP設定, 通知受信クライアント (selected), スケジュールポリシー/通知ポリシー
- Form Fields:**
 - 証明書の有効期限通知: ☒
 - サイクル (Cron式): [Input Field]
 - 有効期限基準日: [Input Field]
 - 通知受信クライアント: [Dropdown Menu]
 - 自動更新: ☒
 - field.RequestRW 基準日: [Input Field]
 - 通知受信クライアント: [Dropdown Menu]
 - 証明書発行ステータスチェック: ☒
 - サイクル (Cron式): [Input Field]
 - 通知受信クライアント: [Dropdown Menu]
 - 配布サーバーの状態チェック: ☒
 - サイクル (Cron式): [Input Field]
 - 通知受信クライアント: [Dropdown Menu]
- Buttons:** ヘルプ (Help)

NeoCertManager 主な機能

主な機能-通知と記録 (Notification & Record)

証明書ログ管理機能

✓ 監査ログとメニューアクセスログの照会

Agent デプロイログ

共通名: Request IP: イベントタイプ: 結果状態: 作成日:

역성 내리받기

エージェントからの展開履歴を自動保存

イベントタイプ	Request IP	CertificateOID	共通名	結果状態	理由	結果メッセージ	作成日
Certinstall	192.168.15.160(8444)	68bfdeba26641d9056987884	kcm-poc.lguplus.co.kr	Success			2025.09.09 17:28:23
Certupload	192.168.15.160(8444)	68bfdeba26641d9056987884	kcm-poc.lguplus.co.kr	Success			2025.09.09 17:24:23
Wait	192.168.15.160			Fail	AuthenticationNotSuccessful	この証明書は登録されていません。 (2cf19459e b3b1a8f09289353fe64f2d37d40df)	2025.09.09 17:20:23
Wait	192.168.15.160			Fail	AuthenticationNotSuccessful	この証明書は登録されていません。 (2cf19459e b3b1a8f09289353fe64f2d37d40df)	2025.09.09 17:18:23
Wait	192.168.15.160			Fail	AuthenticationNotSuccessful	この証明書は登録されていません。 (2cf19459e b3b1a8f09289353fe64f2d37d40df)	2025.09.09 17:16:23
Wait	192.168.15.160			Fail	AuthenticationNotSuccessful	この証明書は登録されていません。 (2cf19459e b3b1a8f09289353fe64f2d37d40df)	2025.09.09 17:14:23
Wait	192.168.15.160			Fail	AuthenticationNotSuccessful	この証明書は登録されていません。 (2cf19459e b3b1a8f09289353fe64f2d37d40df)	2025.09.09 17:12:23
Wait	192.168.15.160			Fail	AuthenticationNotSuccessful	この証明書は登録されていません。 (2cf19459e b3b1a8f09289353fe64f2d37d40df)	2025.09.09 17:10:23
Wait	192.168.15.160			Fail	AuthenticationNotSuccessful	この証明書は登録されていません。 (2cf19459e b3b1a8f09289353fe64f2d37d40df)	2025.09.09 17:08:23
Wait	192.168.15.160			Fail	AuthenticationNotSuccessful	この証明書は登録されていません。 (2cf19459e b3b1a8f09289353fe64f2d37d40df)	2025.09.09 17:06:23

TOTAL 33.

<< 1 2 3 4 > 10

監査ログ

ユーザーID: 理由: 結果メッセージ: イベントタイプ: 詳細イベントタイプ: 結果状態: 作成日:

역성 내리받기

ユーザーアクセス監査ログの自動生成

イベントタイプ	サブタイプ	Request IP	結果状態	理由/結果メッセージ	作成日	ユーザーID
ユーザー管理	削除	192.168.15.11	Success		2025.11.12 19:18:06	kcm_test_15_25
ユーザー管理	作成	192.168.15.11	Success		2025.11.12 19:14:07	homepage_admin
ユーザー管理	ログイン	192.168.15.11	Success		2025.11.12 19:12:58	homepage_admin
ユーザー管理	ログイン	192.168.15.11	Failed	[AuthenticationNotSuccessful] RequiresOTPCredential	2025.11.12 19:12:49	homepage_admin
ユーザー管理	ログアウト	192.168.15.11	Success		2025.11.12 19:12:43	homepage_admin
ユーザー管理	修正	192.168.15.11	Success		2025.11.12 19:12:43	
ユーザー管理	ログイン	192.168.15.11	Success		2025.11.12 19:12:17	homepage_admin
ユーザー管理	作成	192.168.15.11	Success		2025.11.12 19:11:52	kcm_test_15_25
グループ管理	作成	192.168.15.11	Success		2025.11.12 19:11:03	kcm_test_15_25
ユーザー管理	ログイン	192.168.15.11	Success		2025.11.12 19:05:40	kcm_test_15_25

TOTAL 190.

<< 1 2 3 4 5 > 10

NeoCertManager 主な機能

- 4段階でアカウント別の権限管理機能を提供して、セキュリティを強化

メニュー		トップマネージャ (ADMIN)	グループマネージャ (GROUP ADMIN)	グループユーザー (GROUP USER)	監査マネージャ (AUDITOR)
ホーム	ダッシュボード	v	v	v	v
環境設定	インストール情報				
	一般環境	v			
	リソース	v			
	通知ポリシー	v			
Discovery	証明書スキャン	v	v	v	
証明書の登録	証明書の発行	v	v		
	証明書発行ログ	v	v		v
	証明書の登録	v	v		
展開管理	展開管理	v	v	v	
	展開ログ	v	v	v	v
	展開サーバーの管理	v	v	v	
ログ	各ログ	v	v	v	v

お問い合わせ

株式会社Cho&Company

- web: www.cho-co.jp
- e-mail: sales@cho-co.jp

